番号	(新)ガバナンス基準	番号	(旧)ガバナンス基準
3.3.1	概要 情報セキュリティガバナンスは、評価、指示、モニタ及びコミュニケーションの各プロセスで構成される。次項以降において、各プロセスにおいて、ガバナンス主体及び各情報セキュリティマネジメントシステムの責任者が実行する内容を示す。	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
3.3.2	評価	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
–	(対応項なし)	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
3.3.2.1	ガバナンス主体は、以下を実行する。 ・事業に取り組む際の関連するリスク及び機会の確実な考慮 ・情報セキュリティに関する報告に対応するための、情報セキュリティマネジメントシステムにおける目的と優先度の規定	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
3.3.2.2	各情報セキュリティマネジメントシステムの責任者は、以下を実行する。 ・組織体の目的を適切に支援し、維持するような情報セキュリティの確立 ・重大な影響を伴う新規の情報セキュリティプロジェクトを実施する際の、組織体のガバナンス主体への承認依頼	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
3.3.3	指示	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
–	(対応項なし)	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
3.3.3.1	ガバナンス主体は、以下を実行する。 ・組織体全体の戦略の方向性と目的の設定 ・その組織体のリスク選好の決定 ・情報セキュリティ戦略の承認	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
3.3.3.2	各情報セキュリティマネジメントシステムの責任者は、以下を実行する。 ・適切な投資及び資源の配分の実施 ・組織体の目的に合致するように情報セキュリティの目的を調整 ・情報セキュリティに関する役割と責任の割当 ・情報セキュリティポリシーの規定	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)

番号	(新)ガバナンス基準	番号	(旧)ガバナンス基準
3.3.4	モニタ	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
–	（対応項なし）	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
3.3.4.1	ガバナンス主体は、以下を実行する。 ・各情報セキュリティマネジメントシステムの活動の有効性に関する報告の受領 ・組織体の優先度の文脈での、前項で報告された内容の評価 ・各情報セキュリティマネジメントシステムの責任者への優先度の伝達	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
3.3.4.2	各情報セキュリティマネジメントシステムの責任者は、以下を実行する。 ・情報セキュリティマネジメントシステム活動の有効性の評価 ・内部及び外部の要求事項への確実な適合の確保 ・組織体に関わる変化、法令及び規制の環境、並びに情報リスクへの潜在的影響の考慮 ・適切なパフォーマンス指標を選定し、組織的な観点から適切なタイミングで報告が実施されるよう要求を伝達 ・情報セキュリティの実績に関する結果のフィードバックを組織体の経営陣に提供 ・情報リスク及び情報セキュリティに影響する新規の開発についての、組織体の経営陣への注意喚起	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
3.3.5	コミュニケーション	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
–	（対応項なし）	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
3.3.5.1	ガバナンス主体は、以下を実行する。 ・外部の利害関係者を対象とする、組織体がその活動及び優先度の実態に見合った情報セキュリティのレベルを実践していることの報告 ・規制上の義務、利害関係者の期待及び情報セキュリティに関する組織体の要求事項の特定及び優先度の決定 ・注意及び決定が必要な問題についての、各情報セキュリティマネジメントシステムの責任者への助言 ・関連する利害関係者に向けた、情報セキュリティの優先度決定を支援するために採用すべき詳細な対象に関する指導 ・情報セキュリティに積極的な文化の奨励 ・スタッフ及びその他の人々を対象とする、情報セキュリティマネジメントシステムの適用範囲での責任を果たすための訓練とコミュニケーション	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
–	（対応項なし）	–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)
		–	(JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策)

番号	（新）マネジメント基準	番号	(旧)マネジメント基準
4.4.1	組織の役割、責任及び権限 [27001-5.3 / 5.1]	4.4.1	組織の役割、責任及び権限 [27001-5.3 / 5.1]
4.4.1.1	トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。 [27001-5.1b) / 5.1e) / 5.1f)] ・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する。 ・情報セキュリティマネジメントがその意図した成果を達成することを確実にする。 ・情報セキュリティマネジメントの有効性に寄与するよう人々を指揮し、支援する。 また、トップマネジメントがリーダーシップ及びコミットメントを発揮していることを以下により確認する。 ・経営会議等の議事録に、トップマネジメントの情報セキュリティマネジメントに関する意思、判断、指示等が記録されていること。 ・情報セキュリティ方針、情報セキュリティ目的及びそれを達成する計画を策定する際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・達成すべきセキュリティの水準として、リスクレベルをトップマネジメントが決定していること。 ・リスクレベルに応じて選択したセキュリティ管理策を実施させる際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・内部監査において確認すべき事項に、トップマネジメントが要求する情報セキュリティ要求事項等が含まれていること。 ・内部監査報告書やそれに基づく是正処置、マネジメントレビュー議事録等に、トップマネジメントの意思、判断、指示等が含まれていること。	4.4.1.1	トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。 [27001-5.1b) / 5.1e) / 5.1f)] ・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する。 ・情報セキュリティマネジメントがその意図した成果を達成することを確実にする。 ・情報セキュリティマネジメントの有効性に寄与するよう人々を指揮し、支援する。 また、トップマネジメントがリーダーシップ及びコミットメントを発揮していることを以下により確認する。 ・経営会議等の議事録に、トップマネジメントの情報セキュリティマネジメントに関する意思、判断、指示等が記録されていること。 ・情報セキュリティ方針、情報セキュリティ目的及びそれを達成する計画を策定する際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・達成すべきセキュリティの水準として、リスクレベルをトップマネジメントが決定していること。 ・リスクレベルに応じて選択したセキュリティ管理策を実施させる際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・内部監査において確認すべき事項に、トップマネジメントが要求する情報セキュリティ要求事項等が含まれていること。 ・内部監査報告書やそれらに基づく是正処置、マネジメントビュー議事録等に、トップマネジメントの意思、判断、指示等が含まれていること。
4.4.1.2	トップマネジメントは、組織の役割について、以下の責任及び権限を割り当て、組織内に伝達する。[27001-5.3] ・情報セキュリティマネジメントを、本管理基準の要求事項として適合させる。 ・情報セキュリティマネジメントのパフォーマンス評価をトップマネジメントに報告する。 また、組織の情報セキュリティマネジメントを本管理基準の要求事項に適合させるために不可欠な責任・権限を明確にしたうえで、それぞれに適切な割り当てが行われていることを確認する。責任・権限の例を以下に示す。 ・セキュリティ要求事項を盛り込んだ情報セキュリティ方針等の文書を策定する責任・権限 ・リスクアセスメントにおいて、リスクを運用管理する責任・権限をもつリスク所有者 ・セキュリティ要求事項を満たす管理策を教育、普及させる責任・権限 ・セキュリティ要求事項を満たしているか監査する責任・権限 ・各プロセスの結果及び効果をトップマネジメントに報告する責任・権限 ・各プロセスの結果及び効果を組織内に周知する責任・権限	4.4.1.2	トップマネジメントは、組織の役割について、以下の責任及び権限を割り当て、伝達する。[27001-5.3] ・情報セキュリティマネジメントを、本管理基準の要求事項として適合させる。 ・情報セキュリティマネジメントのパフォーマンス評価をトップマネジメントに報告する。 また、情報セキュリティマネジメントを本管理基準の要求事項に適合させるために、以下のような責任・権限を割り当てることを確認する。 ・セキュリティ要求事項を盛り込んだ情報セキュリティ方針等の文書を策定する責任・権限 ・リスクアセスメントにおいて、リスクを運用管理する責任・権限を持つリスク所有者 ・セキュリティ要求事項を満たす管理策を教育、普及させる責任・権限 ・セキュリティ要求事項を満たしているか監査する責任・権限 ・各プロセスの結果及び効果をトップマネジメントに報告する責任・権限 ・各プロセスの結果及び効果を組織内に周知する責任・権限
4.4.1.3	トップマネジメントは、その他の関連する管理層がその責任の領域においてリーダーシップを発揮できるよう、管理層の役割を支援する。[27001-5.1h)] ・その他の関連する管理層が、その職掌範囲、組織等において、リーダーシップを発揮できるよう、トップマネジメントは、管理層に、必要な権限を委譲していることを確認する。	4.4.1.3	トップマネジメントは、管理層がその責任の領域においてリーダーシップを発揮できるよう、管理層の役割を支援する。[27001-5.1h)] 管理層が、その職掌範囲、組織等において、リーダーシップを発揮できるよう、トップマネジメントは、管理層に、必要な権限を委譲していることを確認する。
4.4.2	組織及びその状況の理解 [27001-4.1]	4.4.2	組織及びその状況の理解 [27001-4.1]
4.4.2.1	組織は、組織の目的に関連し、かつ、情報セキュリティマネジメントの意図した成果を達成する組織の能力に影響を与える、以下の課題を決定する。[27001-4.1] ・外部の課題 ・内部の課題 これらの課題の決定とは、組織の外部状況及び内部状況の確定のことをいう。外部状況及び内部状況には、以下に例示するものが含まれ得る。 a) 外部状況 1) 国外、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 2) 組織の目的に影響を与える主要な原動力及び傾向 3) 外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 b) 内部状況 1) 統治、組織体制、役割及びアカウンタビリティ 2) 方針、目的及びこれらを達成するために策定された戦略 3) 資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） 4) 情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） 5) 内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 6) 組織文化 7) 組織が採択した規格、指針及びモデル 8) 契約関係の形態及び範囲	4.4.2.1	組織は、組織の目的に関連し、かつ、情報セキュリティマネジメントの意図した成果を達成する組織の能力に影響を与える、以下の課題を決定する。[27001-4.1] ・外部の課題 ・内部の課題 これらの課題の決定とは、組織の外部状況及び内部状況の確定のことをいう。外部状況及び内部状況には、以下のようなものが含まれる。 a) 外部状況 ・国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 ・組織の目的に影響を与える主要な原動力及び傾向 ・外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 b) 内部状況 ・統治、組織体制、役割及びアカウンタビリティ ・方針、目的及びこれらを達成するために策定された戦略 ・資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） ・情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） ・内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 ・組織文化 ・組織が採択した規格、指針及びモデル ・契約関係の形態及び範囲
4.4.3	利害関係者のニーズ及び期待の理解 [27001-4.2]	4.4.3	利害関係者のニーズ及び期待の理解 [27001-4.2]
4.4.3.1	組織は、利害関係者のニーズ及び期待を理解するために、以下を決定する。[27001-4.2] ・情報情報セキュリティマネジメントに関連する利害関係者 ・利害関係者に関連する要求事項 ・要求事項のうち、情報セキュリティマネジメントを通じて取り組むもの 利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含める場合もあるが、利害関係者には、以下に例示する人又は組織が含まれ得る。 ・組織内で情報セキュリティマネジメントプロセスを推進する役割・権限をもつ人又は組織。以下にその例を示す。 a) 情報セキュリティに関する方針等を策定する人又は組織(トップマネジメント等) b) セキュリティ管理策を全組織に徹底させる人又は組織(総務部、情報システム部等) c) 情報セキュリティ監査を行う人又は組織(監査室等) d) 組織内の情報セキュリティ専門家 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・所属するセキュリティ団体、協会	4.4.3.1	組織は、利害関係者のニーズ及び期待を理解するために、以下を決定する。[27001-4.2] ・情報セキュリティマネジメントに関連する利害関係者 ・利害関係者の、情報セキュリティに関連する要求事項 利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含めてもよいが、利害関係者には、以下のようなものが含まれる。 ・組織内で情報セキュリティマネジメントプロセスを推進する役割・権限を持つ人又は組織。例えば、以下のようなものをいう。 -情報セキュリティに関する方針等を策定する人又は組織(トップマネジメント等) -セキュリティ管理策を全組織に徹底させる人又は組織(総務部、情報システム部等) -情報セキュリティ監査を行う人又は組織(監査室等) -組織内の情報セキュリティ専門家 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・所属するセキュリティ団体、協会

番号	（新）マネジメント基準	番号	(旧)マネジメント基準
4.4.4	適用範囲の決定 [27001-4.3] 情報セキュリティマネジメントを確立、導入、運用、監視、レビュー、維持及び改善するために、まず適用範囲を明確にし、組織に合った情報セキュリティマネジメントを構築する基盤を整える。	4.4.4	適用範囲の決定 [27001-4.3]
		–	情報セキュリティマネジメントを確立、導入、運用、監視、レビュー、維持及び改善するために、まず適用範囲を明確にし、組織に合った情報セキュリティマネジメントを構築する基盤を整える。
4.4.4.1	組織は、情報セキュリティマネジメントの境界及び適用可能性を明確にし、適用範囲を決定する。[27001-4.3] ・組織は以下の点を考慮して適用範囲及び境界を定義する。 a) 自らの事業 b) 体制 c) 所在地 d) 資産 e) 技術の特徴 f) 外部及び内部の課題 g) 利害関係者の情報セキュリティに関連する要求事項 h) 組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係 ・情報セキュリティマネジメントの目的や目標は、組織の特徴によって異なる。 ・情報セキュリティマネジメントに対する要求事項はそれぞれの組織の事業によって、外部状況、内部状況の双方があり、これらを考慮して適用範囲を定義する。 a) 外部状況には、以下に例示するものが含まれ得る。 1) 国外、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 2) 組織の目的に影響を与える主要な原動力及び傾向 3) 外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 b) 内部状況には、以下に例示するものが含まれ得る。 1) 統治、組織体制、役割及びアカウンタビリティ 2) 方針、目的及びこれらを達成するために策定された戦略 3) 資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） 4) 情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） 5) 内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 6) 組織文化 7) 組織が採択した規格、指針及びモデル 8) 契約関係の形態及び範囲	4.4.4.1	組織は、情報セキュリティマネジメントの境界及び適用可能性を明確にし、適用範囲を決定する。[27001-4.3] a) 組織は以下の点を考慮して適用範囲及び境界を定義する。 ・自らの事業 ・体制 ・所在地 ・資産 ・技術の特徴 ・外部及び内部の課題 ・利害関係者の情報セキュリティに関連する要求事項 ・組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係 b) 情報セキュリティマネジメントの目的や目標は、組織の特徴によって異なる。 c) 情報セキュリティマネジメントに対する要求事項はそれぞれの組織の事業によって、外部状況、内部状況の双方があり、これらを考慮して適用範囲を定義する。 ・外部状況には、以下のようなものが含まれる。 －国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 －組織の目的に影響を与える主要な原動力及び傾向 －外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 ・内部状況には、以下のようなものが含まれる。 －統治、組織体制、役割及びアカウンタビリティ －方針、目的及びこれらを達成するために策定された戦略 －資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） －情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） －内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 －組織文化 －組織が採択した規格、指針及びモデル －契約関係の形態及び範囲
4.4.5	方針の確立 [27001-5.2 / 6.2 / 5.1]	4.4.5	方針の確立 [27001-5.2 / 6.2 / 5.1]
4.4.5.1	トップマネジメントは、以下を満たす組織の情報セキュリティ方針を確立する。[27001-5.2] ・組織の目的に対して適切であること。 ・情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組 ・情報セキュリティに関連して適用する要求事項を満たすことへのコミットメントを含むこと。 ・情報セキュリティマネジメントの継続的改善へのコミットメントを含むこと。 また、情報セキュリティ方針は情報セキュリティマネジメントにおける判断の基盤となる考え方を記載したものであり、組織の戦略に従って慎重に作成する。	4.4.5.1	トップマネジメントは、以下を満たす組織の情報セキュリティ方針を確立する。[27001-5.2] ・組織の目的に対して適切であること。 ・情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組 ・情報セキュリティに関連して適用する要求事項を満たすことへのコミットメントを含むこと。 ・情報セキュリティマネジメントの継続的改善へのコミットメントを含むこと。 また、情報セキュリティ方針は情報セキュリティマネジメントにおける判断の基盤となる考え方を記載したものであり、組織の戦略に従って慎重に作成する。
4.4.5.2	組織は、情報セキュリティ目的及びそれを達成するための計画を策定する。[27001-6.2] ・情報セキュリティ目的は、以下を満たすこととする。 a) 情報セキュリティ方針と整合していること。 b) （実行可能な場合）測定可能であること。 c) 適用される情報セキュリティ要求事項、並びにリスクアセスメント及びリスク対応の結果を考慮に入れること。 ・情報セキュリティ目的は、これを監視し、関係者に伝達し、必要に応じて更新し、文書化した情報として利用可能な状態にするとともに、情報セキュリティ目的を達成するための計画においては、以下を決定する。 a) 実施事項 b) 必要な資源 c) 責任者 d) 達成期限 e) 結果の評価方法	4.4.5.2	組織は、情報セキュリティ目的及びそれを達成するための計画を策定する。[27001-6.2] a) 情報セキュリティ目的は、以下を満たすこととする。 ・情報セキュリティ方針と整合していること。 ・（実行可能な場合）測定可能であること。 ・適用される情報セキュリティ要求事項、並びにリスクアセスメント及びリスク対応の結果を考慮に入れること。 b) 情報セキュリティ目的は、関係者に伝達し、必要に応じて更新するとともに、情報セキュリティ目的を達成するための計画においては、以下を決定する。 ・実施事項 ・必要な資源 ・責任者 ・達成期限 ・結果の評価方法
4.4.5.3	トップマネジメントは、以下によって、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。[27001-5.1a)] ・情報セキュリティ方針及び情報セキュリティ目的を確立すること。 ・情報セキュリティ方針及び情報セキュリティ目的は組織の戦略的な方向性と相矛盾しないこと。 また、情報セキュリティ方針は組織に伝えられるように文書化され、しかるべき方法で利害関係者が入手できるようにするとともに、トップマネジメントが情報セキュリティ方針にコミットした証拠を記録として保管する。記録の例を以下に示す。 ・文書化された情報セキュリティ方針への署名 ・情報セキュリティ方針が議論された会議の議事録 これらはトップマネジメントの責任を明確にするために実施する。	4.4.5.3	トップマネジメントは、以下によって、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。[27001-5.1a)] ・情報セキュリティ方針及び情報セキュリティ目的を確立すること。 ・情報セキュリティ方針及び情報セキュリティ目的は組織の戦略的な方向性と相矛盾しないこと。 また、情報セキュリティ方針は組織に伝えられるように文書化され、しかるべき方法で利害関係者が入手できるようにするとともに、トップマネジメントが情報セキュリティ方針にコミットした証拠を、以下のような記録をもって示す。 ・文書化された情報セキュリティ方針への署名 ・情報セキュリティ方針が議論された会議の議事録 これらはトップマネジメントの責任を明確にするために実施する。

番号	（新）マネジメント基準	番号	(旧)マネジメント基準
4.4.6	リスク及び機会に対処する活動 [27001-6.1]	4.4.6	リスク及び機会に対処する活動 [27001-6.1]
4.4.6.1	リスク及び機会を決定する。[27001-6.1.1] ・組織は、外部及び内部の課題、利害関係者の情報セキュリティに関連する要求事項を考慮し、以下のために対処する必要があるリスク及び機会を決定する。 a) 情報セキュリティマネジメントが、組織が意図した成果を達成する。 b) 望ましくない影響を防止又は低減する。 c) 継続的改善を達成する。 d) 当該決定の際、組織は、以下を計画する。 1) 決定したリスク及び機会に対処する活動 2) リスク及び機会に対処する活動の情報セキュリティマネジメントプロセスへの統合及び実施方法 3) リスク及び機会に対処する活動の有効性の評価方法 ・リスク及び機会に対処する活動の記録として、具体的な対処計画（実施時期、実施内容、実施者、実施場所、実施に必要な資源などを規定した計画）を作成していることを確認するとともに、当該計画を作成する際、各対処計画が、情報セキュリティマネジメントプロセスの一部として実施されるよう、考慮するとともに、当該対処の有効性を評価する方法（実施状況や実施したことによる効果を評価する方法）を作成していることも確認する。	4.4.6.1	リスク及び機会を決定する。[27001-6.1.1] a) 組織は、外部及び内部の課題、利害関係者の情報セキュリティに関連する要求事項を考慮し、以下のために対処する必要があるリスク及び機会を決定する。 ・情報セキュリティマネジメントが、組織が意図した成果を達成する。 ・望ましくない影響を防止又は低減する。 ・継続的改善を達成する。 当該決定の際、組織は、以下を計画する。 ・決定したリスク及び機会に対処する活動 ・リスク及び機会に対処する活動の情報セキュリティマネジメントプロセスへの統合及び実施方法 ・リスク及び機会に対処する活動の有効性の評価方法 b) リスク及び機会に対処する活動の記録として、具体的な対処計画（実施時期、実施内容、実施者、実施場所、実施に必要な資源などを規定した計画）を作成していることを確認するとともに、当該計画を作成する際、各対処計画が、情報セキュリティマネジメントプロセスの一部として実施されるよう、考慮するとともに、当該対処の有効性を評価する方法（実施状況や実施したことによる効果を評価する方法）を作成していることも確認する。
4.4.7	情報セキュリティリスクアセスメント [27001-6.1.2]	4.4.7	情報セキュリティリスクアセスメント [27001-6.1.2]
4.4.7.1	組織は、以下によって、情報セキュリティリスクアセスメントのプロセスを定め、適用する。[27001-6.1.2a) / 6.1.2b)] ・以下を含む情報セキュリティのリスク基準を確立し、維持する。 a) リスク受容基準 b) 情報セキュリティリスクアセスメントを実施するための基準 ・リスク受容基準に、以下を反映するよう、考慮する。 a) 組織の価値観 b) 目的 c) 資源 ・リスク受容基準を策定する際には、以下の点を考慮する。 a) 原因及び発生し得る結果の特質及び種類、並びにこれらの測定方法 b) 発生頻度 c) 発生頻度、結果を考える時間枠 d) リスクレベルの決定方法 e) 利害関係者の見解 f) リスク基準は、法令及び規制の要求事項、並びに組織が合意するその他の要求事項によって、組織に課せられるもの又は策定されるものもあること。 ・情報セキュリティリスクアセスメントを繰り返し実施した際に、以下の結果を生み出すこと。 a) 情報セキュリティリスクアセスメントの結果に、一貫性及び妥当性があること。 b) 情報セキュリティリスクアセスメントの結果が比較可能であること。 なお、情報セキュリティマネジメントにおけるリスクアセスメント手法には、定番といえるものがなく、それぞれの組織に適合したものを選択している場合が多いことから、必要に応じてツールを利用することなどが必要になる。	4.4.7.1	組織は、以下によって、情報セキュリティリスクアセスメントのプロセスを定め、適用する。[27001-6.1.2a) / 6.1.2b)] a) 以下を含む情報セキュリティのリスク基準を確立し、維持する。 ・リスク受容基準 ・情報セキュリティリスクアセスメントを実施するための基準 b) リスク受容基準に、以下を反映するよう、考慮する。 ・組織の価値観 ・目的 ・資源 c) リスク受容基準を策定する際には、以下の点を考慮する。 ・原因及び発生し得る結果の特質及び種類、並びにこれらの測定方法 ・発生頻度 ・発生頻度、結果を考える時間枠 ・リスクレベルの決定方法 ・利害関係者の見解 ・リスク基準は、法令及び規制の要求事項、並びに組織が合意するその他の要求事項によって、組織に課せられるもの又は策定されるものもあること。 d) 情報セキュリティアセスメントを繰り返し実施した際に、以下の結果を生み出すこと。 ・情報セキュリティリスクアセスメントの結果に、一貫性及び妥当性があること。 ・情報セキュリティリスクアセスメントの結果が比較可能であること。 なお、情報セキュリティマネジメントにおけるリスクアセスメント手法には、定番といえるものがなく、それぞれの組織に適合したものを選択している場合が多いことから、必要に応じてツールを利用するなどが必要になる。
4.4.7.2	組織は、以下によって、情報セキュリティリスクを特定する。[27001-6.1.2c)] ・情報セキュリティリスクアセスメントのプロセスを適用し、情報の機密性、完全性及び可用性の喪失に伴うリスクを特定する。 ・リスクを特定する過程において、リスク所有者を特定する。 ・リスクを特定する際には、以下について考慮する。 a) リスク源が組織の管理下にあるか否かに関わらず、リスク源又はリスクの原因が明らかでないリスクも特定の対象にすること。 b) 波及効果及び累積効果を含めた、特定の結果の連鎖を注意深く検討すること。 c) 何が起こり得るのかの特定に加えて、考えられる原因及びどのような結果が引き起こされることがあるのかを示すシナリオ d) 全ての重大な原因及び結果 e) 以下を特定すること。 1) リスク源 2) 影響を受ける領域、事象 3) 原因及び起こり得る結果 この段階で特定されなかったリスクは、今後の分析の対象から外されてしまうため、ある機会を追及しなかったことに伴うリスクも含め、リスクの包括的な一覧を作成する。	4.4.7.2	組織は、以下によって、情報セキュリティリスクを特定する。[27001-6.1.2c)] a) 情報セキュリティリスクアセスメントのプロセスを適用し、情報の機密性、完全性及び可用性の喪失に伴うリスクを特定する。 b) リスクを特定する過程において、リスク所有者を特定する。 c) リスクを特定する際には、以下について考慮する。 ・リスク源 が組織の管理下にあるか否かに関わらず、リスク源又はリスクの原因が明らかでないリスクも特定の対象にすること。 ・波及効果及び累積効果を含めた、特定の結果の連鎖を注意深く検討すること。 ・何が起こり得るのかの特定に加えて、考えられる原因及びどのような結果が引き起こされることがあるのかを示すシナリオ ・全ての重大な原因及び結果 ・以下を特定すること。 －リスク源 －影響を受ける領域、事象 －原因及び起こり得る結果 この段階で特定されなかったリスクは、今後の分析の対象から外されてしまうため、ある機会を追及しなかったことに伴うリスクも含め、リスクの包括的な一覧を作成する。
4.4.7.3	組織は、以下によって、情報セキュリティリスクを分析する。[27001-6.1.2d)] ・以下の手順によりリスク分析を行う。 a) 特定されたリスクが実際に生じた場合に起こり得る結果の分析を行う。 b) 特定されたリスクの発生頻度の分析を行う。 c) リスクレベルを決定する。 d) 特定した脅威やぜい弱性を基に、以下の点を考慮する。 1) セキュリティインシデントが発生した場合の事業影響度 2) セキュリティインシデントの発生頻度 3) 管理策が適用されている場合はその効果 ・リスク分析の際には、以下の点についても考慮する。 a) リスクの原因及びリスク源 b) リスクの好ましい結果及び好ましくない結果 c) リスクの発生頻度 d) リスクの結果及び発生頻度に影響を与える要素 なお、リスク分析は、状況に応じて、定性的、半定量的、定量的、又はそれらを組み合わせた手法で行うことが可能である。	4.4.7.3	組織は、以下によって、情報セキュリティリスクを分析する。[27001-6.1.2d)] a) 以下の手順によりリスク分析を行う。 ・特定されたリスクが実際に生じた場合に起こり得る結果の分析を行う。 ・特定されたリスクの発生頻度の分析を行う。 ・リスクレベルを決定する。 ・特定した脅威やぜい弱性を基に、以下の点を考慮する。 －セキュリティインシデントが発生した場合の事業影響度 －セキュリティインシデントの発生頻度 －管理策が適用されている場合はその効果 b) リスク分析の際には、以下の点についても考慮する。 ・リスクの原因及びリスク源 ・リスクの好ましい結果及び好ましくない結果 ・リスクの発生頻度 ・リスクの結果及び発生頻度に影響を与える要素 なお、リスク分析は、状況に応じて、定性的、半定量的、定量的、又はそれらを組み合わせた手法で行うことが可能である。
4.4.7.4	組織は、以下によって、情報セキュリティリスクを評価する。[27001-6.1.2e)] ・リスク分析の結果、決定されたリスクレベルとリスク基準との比較をする。 ・リスク対応のための優先順位付けを行う。 ・リスク評価の結果は今後の改善に利用するため保管する。 なお、リスク対応の優先順位を決定する際には、より広い範囲の状況を考慮し、他者が負うリスクの受容レベルについて考慮するとともに、法令、規制、その他の要求事項についても考慮する。	4.4.7.4	組織は、以下によって、情報セキュリティリスクを評価する。[27001-6.1.2e)] ・リスク分析の結果、決定されたリスクレベルとリスク基準との比較をする。 ・リスク対応のための優先順位付けを行う。 ・リスク評価の結果は今後の改善に利用するため保管する。 なお、リスク対応の優先順位を決定する際には、より広い範囲の状況を考慮し、他者が負うリスクの受容レベルについて考慮するとともに、法令、規制、その他の要求事項についても考慮する。

番号	（新）マネジメント基準	番号	(旧)マネジメント基準
4.4.8	情報セキュリティリスク対応 [27001-6.1.3]	4.4.8	情報セキュリティリスク対応 [27001-6.1.3]
4.4.8.1	組織は、情報セキュリティリスクアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。[27001-6.1.3a)] ・情報セキュリティリスク対応の選択肢には、以下が含まれる。 a) リスクを生じさせる活動を開始又は継続しないと決定することによるリスクの回避 b) ある機会を目的としたリスクの引受け又はリスクの負担 c) リスク源の除去 d) 発生頻度の変更 e) 結果の変更 f) （契約及びリスクファイナンス を含む）他者とのリスクの共有 g) 情報に基づいた意思決定によるリスクの保有 さらに、リスク対応の評価や改善に役立てるため、どの選択肢を選んだ場合も、その理由を明確にし、記載する。	4.4.8.1	組織は、情報セキュリティアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。[27001-6.1.3a)] 情報セキュリティリスク対応の選択肢には、以下が含まれる。 ・リスクを生じさせる活動を開始又は継続しないと決定することによるリスクの回避 ・ある機会を目的としたリスクの引受け又はリスクの負担 ・リスク源の除去 ・発生頻度の変更 ・結果の変更 ・（契約及びリスクファイナンス を含む）他者とのリスクの共有 ・情報に基づいた意思決定によるリスクの保有 さらに、リスク対応の評価や改善に役立てるため、どの選択肢を選んだ場合も、その理由を明確にし、記載する。
4.4.8.2	組織は、選定した情報セキュリティリスク対応の実施に必要な全ての管理策を決定する。[27001-6.1.3b)] ・リスク対応のための方針を決めた上で、管理策の目的（管理目的）及び管理策について検討する。以下を考慮しつつ、対応による効果と対応に必要な費用及び労力のバランスを取り、適切な情報セキュリティ対応の選択肢を選定する。 a) リスクの受容可能レベル b) 関連する法令 c) 規制や契約上の要求事項 d) その他の社会的責任 なお、具体的な管理策の選定においては、管理目的に対応した「管理策基準」から適切なものを選択するが、「管理策基準」はすべてを網羅しているわけではないので、組織の事業や業務などによってその他の管理策を追加してもよい。	4.4.8.2	組織は、選定した情報セキュリティリスク対応の実施に必要な全ての管理策を決定する。[27001-6.1.3b)] リスク対応のための方針を決めた上で、管理策の目的（管理目的）及び管理策について検討する。以下を考慮しつつ、対応による効果と対応に必要な費用及び労力のバランスを取り、適切な情報セキュリティ対応の選択肢を選定する。 ・リスクの受容可能レベル ・関連する法令 ・規制や契約上の要求事項 ・その他の社会的責任 なお、具体的な管理策の選定においては、管理目的に対応した「管理策基準」から適切なものを選択するが、「管理策基準」はすべてを網羅しているわけではないので、組織の事業や業務などによってその他の管理策を追加してもよい。
4.4.8.3	組織は、管理策が見落とされていないことを検証する。 [27001-6.1.3c)] ・必要な管理策の見落としがないか、管理策基準を参照するが、管理策基準に示す管理目的及び管理策以外の管理目的及び管理策が必要になった場合、他の管理目的及び管理策を追加することができる。	4.4.8.3	組織は、管理策が見落とされていないことを検証する。 [27001-6.1.3c)] 必要な管理策の見落としがないか、管理策基準を参照するが、管理策基準に示す管理目的及び管理策以外の管理目的及び管理策が必要になった場合、他の管理目的及び管理策を追加することができる。
4.4.8.4	組織は、情報セキュリティリスク対応計画を策定する。[27001-6.1.3e)] ・情報セキュリティリスク対応計画には、以下を含む。 a) 期待される効果を含む、対応選択肢選定の理由 b) 情報セキュリティリスク対応計画の承認者及び対応計画の実施責任者 c) 対応内容 d) 必要な資源 e) 費用・労力、制約 f) 後日の報告、監視に必要な要求事項 g) 対応工程における節目ごとの目標 h) 対応時期及び日程 ・情報セキュリティマネジメントにおいては最終的な承認をトップマネジメントが行っていることがほとんどであり、責任がトップマネジメントに集中している。一方で、情報セキュリティリスクアセスメント及びリスク対応については、責任及び権限をもつリスク所有者が、責任及び権限をもつ。リスク所有者は、トップマネジメント、又はトップマネジメントから任命され、責任及び権限が委譲された者であることが多いことから、情報セキュリティマネジメントにおいて、トップマネジメント及びリスク所有者が、どのような責任をもつかについて明確にする。	4.4.8.4	組織は、情報セキュリティリスク対応計画を策定する。[27001-6.1.3e)] a)情報セキュリティリスク対応計画には、以下を含む。 ・期待される効果を含む、対応選択肢選定の理由 ・情報セキュリティリスク対応計画の承認者及び対応計画の実施責任者 ・対応内容 ・必要な資源 ・費用・労力、制約 ・後日の報告、監視に必要な要求事項 ・対応工程における節目ごとの目標 ・対応時期及び日程 b) 責任及び権限について 情報セキュリティマネジメントにおいては最終的な承認をトップマネジメントが行っていることがほとんどであり、責任がトップマネジメントに集中している。 一方で、情報セキュリティリスクアセスメント及びリスク対応については、責任及び権限を持つリスク所有者が、責任及び権限を持つ。 リスク所有者は、トップマネジメント、又はトップマネジメントから任命され、責任及び権限が委譲された者であることが多いことから、情報セキュリティマネジメントにおいて、トップマネジメント及びリスク所有者が、どのような責任を持つかについて明確にする。
4.4.8.5	組織は、リスク所有者から、情報セキュリティリスク対応計画について承認を得、かつ、リスク所有者に、残留している情報セキュリティリスクを受け入れてもらう。[27001-6.1.3f)] ・すべてのリスクについて管理目的や管理策を選択した時点で、残留リスクについて明確にし、今後の対応計画を作成する。計画の作成においては以下の点について考慮する。 a) 技術的に対応可能になる時期 b) コスト的に対応可能になる時期 ・残留リスクについては、定期的に見直しを行い、必要に応じて、対応の対象とするとともに、リスク対応後の残留リスクについては、リスク所有者のほか、管理層やその他の利害関係者に認識させることを考慮する。また、リスク所有者の責任を明確にするために、承認された会議の議事録を正しく保管する。	4.4.8.5	組織は、リスク所有者から、情報セキュリティリスク対応計画について承認を得、かつ、リスク所有者に、残留している情報セキュリティリスクを受け入れてもらう。[27001-6.1.3f)] すべてのリスクについて管理目的や管理策を選択した時点で、残留リスクについて明確にし、今後の対応計画を作成する。計画の作成においては以下の点について考慮する。 ・技術的に対応可能になる時期 ・コスト的に対応可能になる時期 残留リスクについては、定期的に見直しを行い、必要に応じて、対応の対象とするとともに、リスク対応後の残留リスクについては、リスク所有者のほか、経営陣やその他の利害関係者に認識させることを考慮する。 また、リスク所有者の責任を明確にするために、承認された会議の議事録を正しく保管する。

番号	（新）マネジメント基準	番号	(旧)マネジメント基準
4.5	情報セキュリティマネジメントの運用 [27001-8]	4.5	情報セキュリティマネジメントの運用 [27001-8]
4.5.1	資源管理 [27001-7.1 / 5.1]	4.5.1	資源管理 [27001-7.1 / 5.1]
4.5.1.1	組織は、情報セキュリティマネジメントの確立、実施、維持及び継続的改善に必要な資源を決定し、提供する。[27001-7.1] ・管理目的を満たすためには、継続的に管理策を実施するとともに、人員の増加、システムの増加などの環境の変化に対応するために、適切な時期に適切に提供できるよう、経営資源を確保する。	4.5.1.1	組織は、情報セキュリティマネジメントの確立、実施、維持及び継続的改善に必要な資源を決定し、提供する。[27001-7.1] 管理目的を満たすためには、継続的に管理策を実施するとともに、人員の増加、システムの増加などの環境の変化に対応するために、適切な時期に適切に提供できるよう、経営資源を確保する。
4.5.1.2	トップマネジメントは、情報セキュリティマネジメントに必要な資源が利用可能であることを確実にするため、以下の資源を割り当てる。[27001-5.1c)] ・情報セキュリティマネジメントの各プロセスに必要な人又は組織 ・情報セキュリティマネジメントの各プロセスに必要な設備、装置、システム ・上記に必要な費用	4.5.1.2	トップマネジメントは、情報セキュリティマネジメントに必要な資源が利用可能であることを確実にするため、以下のような資源を割り当てる。[27001-5.1c)] ・情報セキュリティマネジメントの各プロセスに必要な人又は組織 ・情報セキュリティマネジメントの各プロセスに必要な設備、装置、システム ・上記に必要な費用
4.5.2	力量、認識 [27001-7.2 / 7.3 / 5.1]	4.5.2	力量、認識 [27001-7.2 / 7.3 / 5.1]
4.5.2.1	トップマネジメントは、有効な情報セキュリティマネジメント及びその要求事項への適合の重要性を伝達する。[27001-5.1d)] ・トップマネジメントは情報セキュリティマネジメントについて責任を負うが、実施においては組織全体の協力が必要であることを、情報セキュリティ方針と共に関係者に伝える。また、組織が同じ規定に従って同じ判断ができるように、情報分類等の基準を策定するが、個人情報のように組織によって解釈が一部異なる情報の場合は、一般的な考え方に加え、自社の考え方を明確にした上で、関係者に伝える。	4.5.2.1	トップマネジメントは、有効な情報セキュリティマネジメント及びその要求事項への適合の重要性を伝達する。[27001-5.1d)] トップマネジメントは情報セキュリティマネジメントについて責任を負うが、実施においては組織全体の協力が必要であることを、情報セキュリティ方針と共に関係者に伝える。 また、組織が同じ規定に従って同じ判断ができるように、情報分類等の基準を策定するが、個人情報のように組織によって解釈が一部異なる情報の場合は、一般的な考え方に加え、自社の考え方を明確にした上で、関係者に伝える。
4.5.2.2	組織は、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。[27001-7.2a)] ・情報セキュリティマネジメントに関係する業務及び影響のある業務を特定し、役割を明確にした業務分掌を作成する。これらの業務分掌においては以下の点を明確にする。 a) 役職名 b) 業務内容 c) 担当者の責任範囲 d) 業務に必要な知識 e) 業務に必要な資格 f) 業務に必要な経験 知識や資格、経験などは環境や目的の変化によって変更される可能性があるため、最新の情報となるように随時見直しを行う。	4.5.2.2	組織は、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。[27001-7.2a)] 情報セキュリティマネジメントに関係する業務及び影響のある業務を特定し、役割を明確にした業務分掌を作成する。これらの業務分掌においては以下の点を明確にする。 ・役職名 ・業務内容 ・担当者の責任範囲 ・業務に必要な知識 ・業務に必要な資格 ・業務に必要な経験 知識や資格、経験などは環境や目的の変化によって変更される可能性があるため、最新の情報となるように随時見直しを行う。
4.5.2.3	組織は、適切な教育、訓練又は経験に基づいて、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）が力量を備えられるようにする。[27001-7.2b)] ・適用される処置には、例えば、現在雇用している人々に対する教育訓練の提供、指導の実施、配置転換の実施などがある（教育や訓練などが間に合わないと判断される場合には相応の力量を有した要員の雇用が、また、社内業務との関連が少ない業務においては外部委託などがある。）。	4.5.2.3	組織は、適切な教育、訓練又は経験に基づいて、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）が力量を備えられるようにする。[27001-7.2b)] 適用される処置には、例えば、現在雇用している人々に対する教育訓練の提供、指導の実施、配置転換の実施などがある（教育や訓練などが間に合わないと判断される場合には相応の力量を有した要員の雇用が、また、社内業務との関連が少ない業務においては外部委託などがある。）。
4.5.2.4	組織は、必要な力量を身につけるための処置をとり、とった処置の有効性を評価する。[27001-7.2c)] ・必要な力量を身に着けるための処置としては、教育訓練が重要である。教育は「必要な知識を得させる」、訓練は「必要なスキル及び経験を得させる」ために実施する。教育の内容は一般的な脅威やぜい弱性などの知識だけではなく、業務上のリスクや、組織の特徴を反映した内容を盛り込むなど、実効性のある内容となるようにする。教育及び訓練を実施した結果、必要な力量が持てたかどうかを確認するための取組を実施する。取組の例を以下に示す。 a) 知識の確認テスト b) スキルの実習テスト c) チェックリストなどによるベンチマーク 実施結果については記録し、要員選択の客観性を確保する。	4.5.2.4	組織は、必要な力量を身に着けるための処置をとり、とった処置の有効性を評価する。[27001-7.2c)] 必要な力量を身に着けるための処置としては、教育訓練が重要である。教育は「必要な知識を得させる」、訓練は「必要なスキル及び経験を得させる」ために実施する。教育の内容は一般的な脅威やぜい弱性などの知識だけではなく、業務上のリスクについてなど、組織の特徴を反映した内容を盛り込むなど、実効性のある内容となるようにする。 教育及び訓練を実施した結果、必要な力量が持てたかどうかを確認するために、以下を実施する。 ・知識の確認テスト ・スキルの実習テスト ・チェックリストなどによるベンチマーク 実施結果については記録し、要員選択の客観性を確保する。
4.5.2.5	組織は、力量を常に把握し、その証拠として、適切な文書化した情報を組織が定めた期間保持する。[27001-7.2d)] ・教育、訓練については以下の例示を参考に検討し、定期的に実施する。 a) 教育、訓練基本計画 b) 教育、訓練実施計画 c) 確認テスト又は評価報告 ・教育や訓練の一部を免除する場合は、それがどの技能や経験、資格に当てはまるかを明確にし、それぞれの担当者について調査し、一覧にする。資格については有効期限などを明確にし、更新する。	4.5.2.5	組織は、力量を常に把握し、その証拠として、適切な文書化した情報を組織が定めた期間保持する。[27001-7.2d)] 教育、訓練については以下を検討し、定期的に実施する。 ・教育・訓練基本計画 ・教育・訓練実施計画 ・確認テスト又は評価報告 教育や訓練の一部を免除する場合は、それがどの技能や経験、資格に当てはまるかを明確にし、それぞれの担当者について調査し、一覧にする。資格については有効期限などを明確にし、更新する。
4.5.2.6	組織の管理下で働く人々は、情報セキュリティ方針を認識する。[27001-7.3a)] ・情報セキュリティの活動について、組織が定めた目的と重要性について、情報セキュリティ方針の通達や教育の一環として周知徹底することによって、管理策がなぜ実施されているのかについて関係者の理解を深める。	4.5.2.6	組織の管理下で働く人々は、情報セキュリティ方針を認識する。[27001-7.3a)] 情報セキュリティの活動について、組織が定めた目的と重要性について、情報セキュリティ方針の通達や教育の一環として周知徹底することによって、管理策がなぜ実施されているのかについての関係者の理解を深める。
4.5.2.7	組織の管理下で働く人々は、情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティマネジメントの有効性に対する自らの貢献を認識する。[27001-7.3b)] ・以下の点について組織の管理下で働く人々に伝えることによって、各人の役割及び情報セキュリティマネジメントの有効性に対する自らの貢献を明確にする。 a) 情報セキュリティマネジメントにおけるそれぞれの役割 b) 役割を実行するための業務と手順（異常を検知した場合の報告手順も含む。） c) これらが記載された文書の所在	4.5.2.7	組織の管理下で働く人々は、情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティマネジメントの有効性に対する自らの貢献を認識する。[27001-7.3b)] 以下の点について組織の管理下で働く人々に伝えることによって、各人の役割及び情報セキュリティマネジメントの有効性に対する自らの貢献を明確にする。 ・情報セキュリティマネジメントにおけるそれぞれの役割 ・役割を実行するための業務と手順（異常を検知した場合の報告手順も含む。） ・これらが記載された文書の所在
4.5.2.8	組織の管理下で働く人々は、情報セキュリティマネジメントの要求事項に適合しないことの意味を認識する。[27001-7.3c)]	4.5.2.8	組織の管理下で働く人々は、情報セキュリティマネジメントの要求事項に適合しないことの意味を認識する。[27001-7.3c)]

番号	（新）マネジメント基準	番号	(旧)マネジメント基準
4.5.3	コミュニケーション [27001-7.4]	4.5.3	コミュニケーション [27001-7.4]
4.5.3.1	組織は、情報セキュリティマネジメントに関連する内部及び外部のコミュニケーションを実施する必要性を決定する。[27001-7.4] ・内部及び外部のコミュニケーションを実施する際は、以下を考慮することとする。 a) コミュニケーションの内容 b) コミュニケーションの実施時期 c) コミュニケーションの対象者 d) コミュニケーションの方法 ・内部コミュニケーションでは、以下の例示を参考に、組織の情報セキュリティマネジメントの実施に不可欠な者と、適宜及び定期的なコミュニケーションを実施する。 a) トップマネジメント b) 情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者 c) 情報セキュリティマネジメントのパフォーマンスをトップマネジメント又は組織内に報告する権限者 d) 組織内の従業員 ・外部コミュニケーションでは、以下の例示を参考に、組織の情報セキュリティマネジメントの実施に不可欠な者と、必要に応じて、コミュニケーションを実施する。 a) 取引先、パートナー、サプライチェーン上の関係者 b) 親会社、グループ会社 c) 当該組織のセキュリティを監督する省庁、政府機関 d) 所属するセキュリティ団体、協会	4.5.3.1	組織は、情報セキュリティマネジメントに関連する内部及び外部のコミュニケーションを実施する必要性を決定する。[27001-7.4] a) 内部及び外部のコミュニケーションを実施する際は、以下を考慮することとする。 ・コミュニケーションの内容（何を伝達するか。） ・コミュニケーションの実施時期 ・コミュニケーションの対象者 ・コミュニケーションの実施者 ・コミュニケーションの実施プロセス b) 内部コミュニケーションでは、以下に示すような者と、適宜及び定期的なコミュニケーションを実施する。 ・トップマネジメント ・情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者 ・情報セキュリティマネジメントのパフォーマンスをトップマネジメント又は組織内に報告する権限者 ・組織内の従業員 c) 外部コミュニケーションでは、以下に示すような者と、必要に応じて、コミュニケーションを実施する。 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・所属するセキュリティ団体、協会
4.5.4	情報セキュリティマネジメントの運用の計画策定及び管理 [27001-8.1]	4.5.4	情報セキュリティマネジメントの運用の計画及び管理 [27001-8.1]
4.5.4.1	組織は、次に示す事項の実施によって情報セキュリティ要求事項を満たすため、リスク及び機会に対処する活動を実施するために必要なプロセスを計画し、実施し、かつ管理する。[27001-8.1] ・プロセスに関する基準の設定 ・その基準に従った、プロセスの管理の実施	4.5.4.1	組織は、情報セキュリティ要求事項を満たすため、リスク及び機会に対処する活動を実施するために必要なプロセスを計画し、実施し、かつ管理する。[27001-8.1]
		4.5.4.2	組織は、情報セキュリティ目的を達成するための計画を実施する。[27001-8.1]
4.5.4.2	組織は、計画通りに実施されたことを確信するために、文書化した情報を利用可能な状態にする。[27001-8.1] ・文書化した情報に、以下の情報が集められているかどうかを確認する。 a) 管理策の実施状況 b) 管理策の有効性 c) 管理策を取り巻く環境の変化 また、これらの情報を把握し判断する体制を構築する。	4.5.4.3	組織は、計画通りに実施されたことを確信するために、文書化した情報を保持する。[27001-8.1] 文書化した情報に、以下の情報が集められているかどうかを確認する。 ・管理策の実施状況 ・管理策の有効性 ・管理策を取り巻く環境の変化 また、これらの情報を把握し判断する体制を構築する。
4.5.4.3	組織は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置を講じる。[27001-8.1]	4.5.4.4	組織は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置をとる。[27001-8.1]
–	（対応項なし）	4.5.4.5	組織は、外部委託するプロセスを決定し、かつ、管理する。[27001-8.1]
4.5.5	情報セキュリティリスクアセスメントの実施 [27001-8.2 / 8.3]	4.5.5	情報セキュリティリスクアセスメントの実施 [27001-8.2 / 8.3]
4.5.5.1	組織は、以下のいずれかの場合において、情報セキュリティリスクアセスメントを実施する。[27001-8.2] ・あらかじめ定めた間隔 ・重大な変更が提案された場合 ・重大な変化が生じた場合	4.5.5.1	組織は、以下のいずれかの場合において、情報セキュリティリスクアセスメントを実施する。[27001-8.2] ・あらかじめ定めた間隔 ・重大な変更が提案された場合 ・重大な変化が生じた場合
4.5.5.2	組織は、情報セキュリティリスク対応計画を実施する。[27001-8.3] ・情報セキュリティリスク対応計画の実施においては、明確にされた個々の責任について全うしていることを確認するための方策を講じる。	4.5.5.2	組織は、情報セキュリティリスク対応計画を実施する。[27001-8.3] 情報セキュリティリスク対応計画の実施においては、明確にされた個々の責任について全うしていることを確認するための方策を講じる。
4.5.5.3	トップマネジメントは、情報セキュリティリスク対応計画のために十分な経営資源を提供する。 ・情報セキュリティリスク対応計画には相応の経営資源が必要になるところ、以下の点について考慮する。 a) 管理策の導入及び運用にかかる費用、人員、作業工数、技術 b) セキュリティインシデント発生時の一時対応にかかる費用 c) その他のリスク対応にかかる費用 運用においては管理策の効果測定などを実施するために必要な経営資源について考察し、予算化する。	4.5.5.3	トップマネジメントは、情報セキュリティリスク対応計画のために十分な経営資源を提供する。 情報セキュリティリスク対応計画には相応の経営資源が必要になるところ、以下の点について考慮する。 ・管理策の導入及び運用にかかる費用、人員、作業工数、技術 ・セキュリティインシデント発生時の一時対応にかかる費用 ・その他のリスク対応にかかる費用 運用においては管理策の効果測定などを実施するために必要な経営資源について考察し、予算化する。
4.6	情報セキュリティマネジメントの監視及びレビュー [27001-5.1 / 8.2 / 9 / 10.2]	4.6	情報セキュリティマネジメントの監視及びレビュー [27001-5.1 / 8.2 / 9 / 10.2]
4.6.1	有効性の継続的改善 [27001-10.2 / 8.2 / 9.2 / 9.3 / 5.1]	4.6.1	有効性の継続的改善 [27001-10.2 / 8.2 / 9.2 / 9.3 / 5.1]
4.6.1.1	組織は、以下を実施し、情報セキュリティマネジメントの適切性、妥当性及び有効性を継続的に改善する。[27001-10.2 / 8.2 / 9.2 / 9.3] ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・トップマネジメントによる定期的なマネジメントレビュー 継続的改善においては、これまで実施してきた管理策だけはなく、環境の変化に伴う新たな脅威やぜい弱性についても不適合を検出し処置する。	4.6.1.1	組織は、以下を実施し、情報セキュリティマネジメントの適切性、妥当性及び有効性を継続的に改善する。[27001-10.2 / 8.2 / 9.2 / 9.3] ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・トップマネジメントによる定期的なマネジメントレビュー 継続的改善においては、これまで実施してきた管理策だけはなく、環境の変化に伴う新たな脅威やぜい弱性についても不適合を検出し処置する。
4.6.1.2	トップマネジメントは、継続的改善を促進する。[27001-5.1g)] ・4.6.1.1.を実施するための、役割、責任及び権限を割り当て、実施するよう関係者に伝達する。	4.6.1.2	トップマネジメントは、継続的改善を促進する。[27001-5.1g)] 4.6.1.1.を実施するための、役割、責任及び権限を割り当て、実施するよう関係者に伝達する。

番号	（新）マネジメント基準	番号	(旧)マネジメント基準
4.6.2	パフォーマンス評価 [27001-9]	4.6.2	パフォーマンス評価 [27001-9]
4.6.2.1	組織は、以下を決定し、その結果の証拠として文書化した情報を利用可能な状態とするとともに、情報セキュリティパフォーマンス及び情報セキュリティマネジメントの有効性を継続的に評価する。[27001-9.1] ・必要とされる監視及び測定の対象（情報セキュリティプロセス及び管理策を含む。） ・妥当な結果を確実にするための、監視、測定、分析及び評価の方法（妥当と考えられる、比較可能で再現可能な結果を生み出す方法とする。） ・監視及び測定の実施時期及び頻度 ・監視及び測定の実施者 ・監視及び測定の結果の、分析（因果関係、相関関係を含む）及び評価の時期及び頻度 ・監視及び測定の結果の、分析及び評価の実施者 ・分析及び評価の結果に応じた対応措置 ・分析及び評価の結果の報告頻度	4.6.2.1	組織は、情報セキュリティパフォーマンス及び情報セキュリティマネジメントの有効性を継続的に評価し、以下を決定する。[27001-9.1] ・必要とされる監視及び測定の対象（情報セキュリティプロセス及び管理策を含む。） ・妥当な結果を確実にするための、監視、測定、分析及び評価の方法（比較可能で再現可能な結果を生み出す方法とする。） ・監視及び測定の実施時期及び頻度 ・監視及び測定の実施者 ・監視及び測定の結果の、分析（因果関係、相関関係を含む）及び評価の時期及び頻度 ・監視及び測定の結果の、分析及び評価の実施者 ・分析及び評価の結果に応じた対応措置 ・分析及び評価の結果の報告頻度
4.6.2.2	組織は、あらかじめ定めた間隔で内部監査を実施する。[27001-9.2a) / 9.2b)] ・内部監査を実施する際は、以下を確認する。 a) 以下に適合していること。 1) 情報セキュリティマネジメントに関して、組織自体が規定した要求事項 2) 本マネジメント基準の要求事項 b) 情報セキュリティマネジメントが有効に実施され、維持されていること。 ・内部監査は、管理策の有効性を総合的に確認するために定期的に実施し、計画及び結果について以下の文書で管理する。 a) 内部監査基本計画 b) 内部監査実施計画 c) 内部監査報告書 基本計画書では対象範囲、目的、管理体制及び期間又は期日について、実施計画では実施時期や実施場所、実施担当者及びその割当て並びに詳細な監査の手法についてあらかじめ決める。予定通り実施されたことを証明するためにも、実施報告書を作成する。 ・適合性の監査においては、以下の項目を対象に含む。 a) 関連する法令又は規制の要求事項 b) 情報セキュリティリスクアセスメントなどによって特定された情報セキュリティ要求事項 ・情報セキュリティマネジメントが有効に実施され、維持されていることの監査においては、以下の項目を対象に含む。 a) 管理策の有効性及び維持 b) 管理策が期待通りに実施されていること。	4.6.2.2	組織は、あらかじめ定めた間隔で内部監査を実施する。[27001-9.2a) / 9.2b)] a) 内部監査を実施する際は、以下を確認する。 ・以下に適合していること。 －情報セキュリティマネジメントに関して、組織自体が規定した要求事項 －本マネジメント基準の要求事項 ・情報セキュリティマネジメントが有効に実施され、維持されていること。 b) 内部監査は、管理策の有効性を総合的に確認するために定期的に実施し、計画及び結果について以下の文書で管理する。 ・内部監査基本計画 ・内部監査実施計画 ・内部監査報告書 基本計画書では対象範囲、目的、管理体制及び期間又は期日について、実施計画では実施時期や実施場所、実施担当者及びその割当て及び詳細な監査の手法についてあらかじめ決める。予定通り実施されたことを証明するためにも、実施報告書を作成する。 c) 適合性の監査においては、以下の項目を対象に含む。 ・関連する法令又は規制の要求事項 ・情報セキュリティリスクアセスメントなどによって特定された情報セキュリティ要求事項 d) 情報セキュリティマネジメントが有効に実施され、維持されていることの監査においては、以下の項目を対象に含む。 ・管理策の有効性及び維持 ・管理策が期待通りに実施されていること。
4.6.2.3	組織は、頻度、方法、責任及び計画策定に関する要求事項及び報告を含む、監査プログラムを計画、確立、実施及び維持する。[27001-9.2.2] ・ 内部監査プログラムを確立するとき、組織は、関連するプロセスの重要性及び前回までの監査の結果を考慮する。	4.6.2.3	組織は、頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持する。[27001-9.2c)] 監査プログラムでは、関連するプロセスの重要性及び前回までの監査の結果を考慮する。 監査は一度にすべての適用範囲について実施するだけではなく、範囲の一部のみを対象とする場合もあり、毎回の監査の目的を明確にし、適切な監査計画を実施することが重要であることから、監査プログラムの作成においては、以下の点を考慮する。 ・監査の目的と重点目標 ・対象となる監査プロセスの状況と重要性 ・対象となる領域の状況と重要性 ・前回までの監査結果
4.6.2.4	組織は、監査基準及び監査範囲を明確にする。[27001-9.2.2a)] ・監査プログラムでは全体的な監査の日程だけではなく、以下の内容について含める。 a) 監査の基準（以下の内容も含む。） 1) 目的、権限と責任 2) 独立性、客観性と職業倫理 3) 専門能力 4) 業務上の義務 5) 品質管理 6) 監査の実施方法 7) 監査報告書の形式 b) 監査の範囲 c) 監査の頻度又は時期 d) 監査の方法（個別の情報セキュリティ監査基準を作成し、内部監査、外部組織による監査のいずれにおいても、品質の高い監査を実施できるように準備を整える。）	4.6.2.4	組織は、監査基準及び監査範囲を明確にする。[27001-9.2d)] 監査プログラムでは全体的な監査の日程だけではなく、以下の内容について含める。 ・監査の基準（以下の内容も含む。） －目的、権限と責任 －独立性、客観性と職業倫理 －専門能力 －業務上の義務 －品質管理 －監査の実施方法 －監査報告書の形式 ・監査の範囲 ・監査の頻度又は時期 ・監査の方法（個別の情報セキュリティ監査基準を作成し、内部監査、外部組織による監査のいずれにおいても、品質の高い監査を実施できるように準備を整える。）
4.6.2.5	組織は、監査プロセスの客観性及び公平性を確実にする監査員の選定及び監査の実施を行う。[27001-9.2.2b)] ・監査人の選定においては監査基準に従い、以下の点を考慮する。 a) 外観上の独立性 b) 精神上の独立性 c) 職業倫理と誠実性 なお、内部の監査員の場合は、自らが従事している業務については自身で監査しないように、他の担当者を割り当てる。	4.6.2.5	組織は、監査プロセスの客観性及び公平性を確実にする監査員の選定及び監査の実施を行う。[27001-9.2e)] 監査人の選定においては監査基準に従い、以下の点を考慮する。 ・外観上の独立性 ・精神上の独立性 ・職業倫理と誠実性 なお、内部の監査員の場合は、自らが従事している業務については自身で監査しないように、他の担当者を割り当てる。
4.6.2.6	組織は、監査の結果を関連する管理層に報告することを確実にする。[27001-9.2.2c)]	4.6.2.6	組織は、監査の結果を関連する管理層に報告することを確実にする。[27001-9.2f)]
4.6.2.7	組織は、監査プログラムの実施及び監査結果の証拠として、文書化した情報を利用可能な状態にする。[27001-9.2.2] ・監査手順に以下の内容を反映させるとともに、文書化し、互いのコミュニケーションのために活用する。 a) 監査の計画・実施に関する責任及び要求事項 b) 結果報告・記録維持に関する責任及び要求事項 要求事項については監査品質を確保するための必須条件であり、責任者と監査人が同じ目的をもって監査を実施する。	4.6.2.7	組織は、監査プログラム及び監査結果の証拠として、文書化した情報を保持する。[27001-9.2g)] 監査手順に以下の内容を反映させるとともに、文書化し、お互いのコミュニケーションのために活用する。 ・監査の計画・実施に関する責任及び要求事項 ・結果報告・記録維持に関する責任と要求事項 要求事項については監査品質を確保するための必須条件であり、責任者と監査人が同じ目的をもって監査を実施する。

番号	（新）マネジメント基準	番号	(旧)マネジメント基準
4.6.3	マネジメントレビュー [27001-9.3]	4.6.3	マネジメントレビュー [27001-9.3]
4.6.3.1	トップマネジメントは、あらかじめ定めた間隔で、マネジメントレビューする。[27001-9.3] ・あらかじめ定められた間隔でマネジメントレビューを実施するために、以下の点について考慮するとともに、文書化する。 a) マネジメントレビュー基本計画 b) マネジメントレビュー実施計画 c) マネジメントレビューのための実施報告 基本計画書では目的及び実施時期について、実施計画では詳細な監査の手法についてあらかじめ決める。	4.6.3.1	トップマネジメントは、あらかじめ定めた間隔で、マネジメントレビューする。[27001-9.3] あらかじめ定められた間隔でマネジメントレビューを実施するために、以下の点について考慮するとともに、文書化する。 ・マネジメントレビュー基本計画 ・マネジメントレビュー実施計画 ・マネジメントレビューのための実施報告 基本計画書では目的及び実施時期について、実施計画では詳細な監査の手法についてあらかじめ決める。
4.6.3.2	トップマネジメントは、マネジメントレビューにおいて、以下を考慮する。[27001-9.3.2] ・前回までのマネジメントレビューの結果講じた処置の状況 ・情報セキュリティマネジメントに関連する外部及び内部の課題の変化 ・情報セキュリティマネジメントに関連する利害関係者のニーズ及び期待の変化 ・以下に示す内容を含めた、情報セキュリティパフォーマンスに関するフィードバック a) 不適合及び是正処置 b) 監視及び測定の結果 c) 監査結果 d) 情報セキュリティ目的の達成 ・利害関係者からのフィードバック ・情報セキュリティリスクアセスメントの結果及び情報セキュリティリスク対応計画の状況 ・継続的改善の機会 また、これらの情報を構成することが予想される活動及び事象を記録し、必要に応じて報告するとともに、緊急性が高いものについてはあらかじめ定義しておき、誰もが同じ判断をできるように基準を定める。	4.6.3.2	トップマネジメントは、マネジメントレビューにおいて、以下を考慮する。[27001-9.3] ・前回までのマネジメントレビューの結果とった処置の状況 ・情報セキュリティマネジメントに関連する外部及び内部の課題の変化 ・以下に示す内容を含めた、情報セキュリティパフォーマンスに関するフィードバック -不適合及び是正処置 -監視及び測定の結果 -監査結果 -情報セキュリティ目的の達成 ・利害関係者からのフィードバック ・情報セキュリティリスクアセスメントの結果及び情報セキュリティリスク対応計画の状況 ・継続的改善の機会 また、これらの情報を構成することが予想される活動及び事象を記録し、必要に応じて報告するとともに、緊急性が高いものについてはあらかじめ定義しておき、誰もが同じ判断をできるように基準を定める。
4.6.3.3	マネジメントレビューの結果には、継続的改善の機会及び情報セキュリティマネジメントのあらゆる変更の必要性に関する決定を含める。[27001-9.3.3] ・マネジメントレビューの結果を改善策に反映するために、以下の活動を実施し、改善策を検討する。 a) 情報セキュリティマネジメントの有効性の改善 b) 情報セキュリティリスクアセスメント及び情報セキュリティリスク対応計画の更新 c) 情報セキュリティマネジメントに影響を与える可能性のある内外の事象を考慮の上での手順及び管理策の修正 d) 必要となる経営資源の特定 e) パフォーマンス測定方法の改善 なお、改善策の立案においては、情報セキュリティリスク対応の選択肢を選択した際の記録を参考にする。	4.6.3.3	マネジメントレビューからのアウトプットには、継続的改善の機会及び情報セキュリティマネジメントのあらゆる変更の必要性に関する決定を含める。[27001-9.3] マネジメントレビューの結果を改善策に反映するために、以下の活動を実施し、改善策を検討する。 ・情報セキュリティマネジメントの有効性の改善 ・情報セキュリティリスクアセスメント及び情報セキュリティリスク対応計画の更新 ・情報セキュリティマネジメントに影響を与える可能性のある内外の事象を考慮の上での手順及び管理策の修正 ・必要となる経営資源の特定 ・パフォーマンス測定方法の改善 なお、改善策の立案においては、情報セキュリティリスク対応の選択肢を選択した際の記録を参考にする。
4.6.3.4	組織は、マネジメントレビューの結果の証拠として文書化した情報を利用可能な状態にする。[27001-9.3] ・マネジメントレビューの結果は次回のマネジメントレビューに活用されるため、実施内容と結果が分かるように具体的に記録する。	4.6.3.4	組織は、マネジメントレビューの結果の証拠として文書化した情報を保持する。[27001-9.3] マネジメントレビューの結果は次回のマネジメントレビューに活用されるため、実施内容と結果が分かるように具体的に記録する。
4.7	情報セキュリティマネジメントの維持及び改善 [27001-10]	4.7	情報セキュリティマネジメントの維持及び改善 [27001-10]
4.7.1	是正処置 [27001-10.2]	4.7.1	是正処置 [27001-10.1]
4.7.1.1	組織は、不適合が発生した場合、不適合の是正のための処置を取る。[27001-10.2] ・是正処置を取る際は、以下を実施する。 a) その不適合を管理し、是正するための処置 b) その不適合によって起こった結果への対処 c) 是正処置を手順どおりに実施するために、以下について文書化する。 1) 不適合の再発防止を確実にするために選択した処置の必要性の評価 2) 必要な是正処置の決定 3) 必要な是正処置の実施 4) 実施した処置の記録 5) 実施した是正処置のレビュー ・不適合は以下の活動によって検出される。 a) 定期的な情報セキュリティリスクアセスメント b) 定期的な情報セキュリティ内部監査 c) 定期的なマネジメントレビュー d) 不適合を手順どおりに検出するために、以下について文書化する。 1) 情報セキュリティマネジメントに対する不適合の特定 2) 情報セキュリティマネジメントに対する不適合の原因の決定 なお、単一の活動だけでは判断できない場合もあるので、複合的な結果の考察から不適合を検出する。	4.7.1.1	組織は、不適合が発生した場合、不適合の是正のための処置を取る。[27001-10.1a)] a) 是正措置を取る際は、以下を実施する。 ・その不適合を管理し、是正するための処置 ・その不適合によって起こった結果への対処 ・是正処置を手順どおりに実施するために、以下について文書化する。 －不適合の再発防止を確実にするために選択した処置の必要性の評価 －必要な是正処置の決定 －必要な是正処置の実施 －実施した処置の記録 －実施した是正処置のレビュー b) 不適合は以下の活動によって検出される。 ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・定期的なマネジメントレビュー ・不適合を手順どおりに検出するために、以下について文書化する。 －情報セキュリティマネジメントに対する不適合の特定 －情報セキュリティマネジメントに対する不適合の原因の決定 なお、単一の活動だけでは判断できない場合もあるので、複合的な結果の考察から不適合を検出する。
4.7.1.2	組織は、不適合が再発又は他のところで発生しないようにするため、その不適合の原因を除去するための処置を講じる必要性を評価する。[27001-10.2b)] ・必要性を評価する際は、以下を実施する。 a) その不適合のレビュー b) その不適合の原因の明確化 c) 類似の不適合の有無、又はそれが発生する可能性の明確化	4.7.1.2	組織は、不適合が再発又は他のところで発生しないようにするため、その不適合の原因を除去するための処置をとる必要性を評価する。[27001-10.1b)] 必要性を評価する際は、以下を実施する。 ・その不適合のレビュー ・その不適合の原因の明確化 ・類似の不適合の有無、又はそれが発生する可能性の明確化
4.7.1.3	組織は、必要な処置を実施する。[27001-10.2c)]	4.7.1.3	組織は、必要な処置を実施する。[27001-10.1c)]
4.7.1.4	組織は、講じた全ての是正処置の有効性をレビューする。[27001-10.2d)]	4.7.1.4	組織は、とった全ての是正処置の有効性をレビューする。[27001-10.1d)]
4.7.1.5	組織は、必要な場合には、情報セキュリティマネジメントの変更を行う。[27001-10.2e)]	4.7.1.5	組織は、必要な場合には、情報セキュリティマネジメントの変更を行う。[27001-10.1e)]
4.7.1.6	組織は、是正処置は、検出された不適合のもつ影響に応じたものとする。[27001-10.2]	4.7.1.6	組織は、是正処置は、検出された不適合のもつ影響に応じたものとする。[27001-10.1]
4.7.1.7	組織は、是正処置の証跡として、以下の文書化した情報を利用可能な状態にする。[27001-10.2f) / 10.2g)] ・不適合の性質及びそれに対して講じたあらゆる処置 ・是正処置の結果	4.7.1.7	組織は、是正処置の証跡として、以下の文書化した情報を保持する。[27001-10.1f) / 10.1g)] ・不適合の性質及びとった処置 ・是正処置の結果
4.8	文書化した情報の管理 [27001-7.5]	4.8	文書化した情報の管理 [27001-7.5]
4.8.1	文書化の指針 [27001-7.5.1]	4.8.1	文書化の指針 [27001-7.5.1]
4.8.1.1	組織は、情報セキュリティマネジメントが必要とする以下の情報を文書化する。[27001-7.5.1] ・情報セキュリティ方針 ・情報セキュリティ目的 ・情報セキュリティリスクアセスメントのプロセス ・情報セキュリティリスク対応のプロセス ・情報セキュリティリスクアセスメントの結果 ・情報セキュリティリスク対応計画 ・パフォーマンス測定の結果 これらの内容についてはどの文書に記載されていてもかまわないが、その内容を知る必要がある担当者には必ず伝わるように構成するとともに、知る必要性のない者が閲覧できないことを確実にする。	4.8.1.1	組織は、情報セキュリティマネジメントが必要とする以下の情報を文書化する。[27001-7.5.1] ・情報セキュリティ方針 ・情報セキュリティ目的 ・情報セキュリティリスクアセスメントのプロセス ・情報セキュリティリスク対応のプロセス ・情報セキュリティリスクアセスメントの結果 ・情報セキュリティリスク対応計画 ・パフォーマンス測定の結果 これらの内容についてはどの文書に記載されていてもかまわないが、その内容を知る必要がある担当者には必ず伝わるように構成するとともに、知る必要性のない者が閲覧できないことを確実にする。

番号	（新）マネジメント基準	番号	(旧)マネジメント基準
4.8.2	文書の作成・変更及び管理 [27001-7.5.2 / 7.5.3]	4.8.2	文書の作成・変更及び管理 [27001-7.5.2 / 7.5.3]
4.8.2.1	組織は、以下を行うことによって、文書化した情報を作成及び更新する。[27001-7.5.2] ・適切な識別情報の記述（例えば、表題、日付、作成者、参照番号） ・適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）の選択 ・適切性及び妥当性に関する、適切なレビュー及び承認 ・文書化した情報のライフサイクルの定義や、それに応じた処理ができるような手順の策定 ・文書を発行する前における、適正性のレビュー及び承認 ・必要に応じた、文書の更新及び再承認 ・廃止文書の誤使用の防止 ・廃止文書を何らかの目的で保持する場合における、廃止文書であることが分かる適切な識別情報の記述 ・法的及び規制の要求事項及び環境の変化に従い、定めた頻度での更新 また、これらのすべての活動が文書管理に反映されているか、またその活動が業務に大きな障害を与えていないかなどを考慮し、適切な文書管理手順を策定する。	4.8.2.1	組織は、以下を行うことによって、文書化した情報を作成及び更新する。[27001-7.5.2] ・適切な識別情報の記述（例えば、表題、日付、作成者、参照番号） ・適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）の選択 ・適切性及び妥当性に関する、適切なレビュー及び承認 ・文書化した情報のライフサイクルの定義や、それに応じた処理ができるような手順の策定 ・文書を発行する前における、適正性のレビュー及び承認 ・必要に応じた、文書の更新及び再承認 ・廃止文書の誤使用の防止 ・廃止文書を何らかの目的で保持する場合における、廃止文書であることが分かる適切な識別情報の記述 ・法的及び規制の要求事項及び環境の変化に従い、定めた頻度での更新 また、これらのすべての活動が文書管理に反映されているか、またその活動が業務に大きな障害を与えていないかなどを考慮し、適切な文書管理手順を策定する。
4.8.2.2	組織は、以下のことを確実にするために、情報セキュリティマネジメントで要求された、文書化した情報を管理する。[27001-7.5.3] ・文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態であること。 ・文書化した情報が十分に保護されていること（例えば、機密性の喪失、不適切な使用又は完全性の喪失からの保護）。 ・文書化した情報の配付、アクセス、検索及び利用 ・文書化した情報の読みやすさが保たれることを含む、保管及び保存 ・文書化した情報の変更の管理（例えば、版の管理） ・文書化した情報の保持及び廃棄 また、情報セキュリティマネジメントの計画策定及び運用のために組織が必要と決定した文書は、外部から入手したものであっても、必要に応じて、識別し、管理する。	4.8.2.2	組織は、以下のことを確実にするために、情報セキュリティマネジメントで要求された文書化した情報を、管理する。[27001-7.5.3] ・文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態であること。 ・文書化した情報が十分に保護されていること（例えば、機密性の喪失、不適切な使用及び完全性の喪失からの保護）。 ・文書化した情報の配付、アクセス 、検索及び利用 ・文書化した情報の読みやすさが保たれることを含む、保管及び保存 ・文書化した情報の変更の管理（例えば、版の管理） ・文書化した情報の保持及び廃棄 また、情報セキュリティマネジメントの計画及び運用のために組織が必要と決定した文書は、外部から入手したものであっても、必要に応じて、特定し、管理する。
4.9	情報セキュリティリスクコミュニケーション 利害関係者間の有効なコミュニケーションは、意思決定に大きな影響を与えることがある。情報セキュリティリスクコミュニケーションは、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間で情報セキュリティリスクに関する情報を交換、共有し、リスクを管理する方法に関する合意を得る。	4.9	情報セキュリティリスクコミュニケーション
		–	利害関係者間の有効なコミュニケーションは、意思決定に大きな影響を与えることがある。情報セキュリティリスクコミュニケーションは、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間で情報セキュリティリスクに関する情報を交換、共有し、リスクを管理する方法に関する合意を得る。
4.9.1	リスクコミュニケーションの計画	4.9.1	リスクコミュニケーションの計画
4.9.1.1	リスクコミュニケーション計画を策定する。 ・リスクコミュニケーション計画は、以下の２つに分けて策定し、文書化する。 a) 通常運用のためのリスクコミュニケーション計画 b) 緊急事態のためのリスクコミュニケーション計画 リスクコミュニケーション計画は、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間でどのようにコミュニケーションを図るかに留意し、以下の内容について含める。 1) 適切な利害関係者の参画による、効果的な情報交換／共有 2) 法令、規制及びガバナンスの要求事項の順守 3) コミュニケーション及び協議に関するフィードバック及び報告の提供 4) 組織に対する信頼を醸成するためのコミュニケーションの活用 5) 危機又は不測の事態発生時の利害関係者とのコミュニケーションの実施	4.9.1.1	リスクコミュニケーション計画を策定する。 リスクコミュニケーション計画は、以下の２つに分けて策定し、文書化する。 ・通常運用のためのリスクコミュニケーション計画 ・緊急事態のためのリスクコミュニケーション計画 リスクコミュニケーション計画は、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間でどのようにコミュニケーションを図るかに留意し、以下の内容について含める。 ・適切な利害関係者の参画による、効果的な情報交換／共有 ・法令、規制及びガバナンスの要求事項の順守 ・コミュニケーション及び協議に関するフィードバック及び報告の提供 ・組織に対する信頼を醸成するためのコミュニケーションの活用 ・危機又は不測の事態発生時の利害関係者とのコミュニケーションの実施
4.9.2	リスクコミュニケーションの実施	4.9.2	リスクコミュニケーションの実施
4.9.2.1	リスクコミュニケーションを実施する仕組みを確定する。 ・リスクに関する論議、その優先順位の決定及び適切なリスク対応、並びにリスク受容を行い、主要な意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の協調を得る仕組みを確定する。この仕組みでは次の事項を確実にする。 a) リスクマネジメントの枠組みの主要な構成要素、及びその後に行うあらゆる修正の適切な伝達 b) 枠組み、その有効性及び成果に関する適切な内部報告 c) 適切な階層及び時期に利用可能な、リスクマネジメントの適応から導出される関連情報の提供 d) 内部の利害関係者との協議のためのプロセス 仕組みには、適切な場合には、多様な情報源からのリスク情報について、まとめ上げるプロセスが含まれ、また、リスク情報の影響の受けやすさを考慮する必要がある場合もある。なお、この仕組みを設ける場として、委員会がある。	4.9.2.1	リスクコミュニケーションを実施する仕組みを確定する。 リスクに関する論議、その優先順位の決定及び適切なリスク対応、並びにリスク受容を行い、主要な意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の協調を得る仕組みを確定する。この仕組みでは次の事項を確実にする。 ・リスクマネジメントの枠組みの主要な構成要素、及びその後に行うあらゆる修正の適切な伝達 ・枠組み、その有効性及び成果に関する適切な内部報告 ・適切な階層及び時期に利用可能な、リスクマネジメントの適応から導出される関連情報の提供 ・内部の利害関係者との協議のためのプロセス 仕組みには、適切な場合には、多様な情報源からのリスク情報について、まとめ上げるプロセスが含まれ、また、リスク情報の影響の受けやすさを考慮する必要がある場合もある。なお、この仕組みを設ける場として、委員会がある。
4.9.2.2	リスクコミュニケーションを実施する。 ・リスクコミュニケーションは、次の点を達成するために、リスクマネジメントプロセスのすべての段階で継続的に実施する。 a) 組織のリスクマネジメント結果の保証を提供する b) リスク情報を収集する c) リスクアセスメントの結果を共有しリスク対応計画を提示する d) 意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の相互理解の欠如による情報セキュリティ違反の発生及び結果を回避又は低減する e) 意思決定を支援する f) 新しい情報セキュリティ知識を入手する g) 他の組織と協調しすべてのインシデントの結果を低減するための対応計画を立案する h) 意思決定者及び利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）にリスクについての責任を意識させる i) セキュリティ意識を改善する リスクコミュニケーションの実施においては、組織内の適切な広報又はコミュニケーション部門と協力し、リスクコミュニケーション関連の全タスクを調整して行う。	4.9.2.2	リスクコミュニケーションを実施する。 リスクコミュニケーションは、次の点を達成するために、リスクマネジメントプロセスのすべての段階で継続的に実施する。 ・組織のリスクマネジメント結果の保証を提供する ・リスク情報を収集する ・リスクアセスメントの結果を共有しリスク対応計画を提示する ・意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の相互理解の欠如による情報セキュリティ違反の発生及び結果を回避又は低減する ・意思決定を支援する ・新しい情報セキュリティ知識を入手する ・他の組織と協調しすべてのインシデントの結果を低減するための対応計画を立案する ・意思決定者及び利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）にリスクについての責任を意識させる ・セキュリティ意識を改善する リスクコミュニケーションの実施においては、組織内の適切な広報又はコミュニケーション部門と協力し、リスクコミュニケーション関連の全タスクを調整して行う。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.1	情報セキュリティのための方針群 統制目標：情報セキュリティ方針及びトピック固有の方針は、これを定義し、管理層が承認し、発行し、関連する要員及び関連する利害関係者に伝達し、認識させ、あらかじめ定めた期間で、及び重大な変化が発生した場合にレビューする。 目的：事業、法令、規制及び契約上の要求事項に従って、情報セキュリティに対する管理層の指示及び支援の継続的な適合性、適切性、及び有効性を確実にするため。		5.1	情報セキュリティのための方針群 管理策 情報セキュリティ方針及びトピック固有の方針は、これを定義し、管理層が承認し、発行し、関連する要員及び関連する利害関係者に伝達し、認識させ、あらかじめ定めた期間で、及び重大な変化が発生した場合にレビューする。 目的 事業、法令、規制及び契約上の要求事項に従って、情報セキュリティに対する管理層の指示及び支援の継続的な適合性、適切性、及び有効性を確実にするため。		5.1	情報セキュリティのための経営陣の方向性 管理目的：情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制に従って提示するため。
						5.1.1	情報セキュリティのための方針群 情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知する。 (脚注) 管理層には、経営陣及び管理者が含まれる。ただし、実務管理者（administrator）は除かれる。
						5.1.2	情報セキュリティのための方針群のレビュー 情報セキュリティのための方針群は、あらかじめ定めた期間で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューする。
5.1.1	情報セキュリティ方針を策定し、トップマネジメントが承認する。	組織は、方針群の最も高いレベルに、一つの情報セキュリティ方針を定める。この情報セキュリティ方針は、トップマネジメントが承認し、情報セキュリティの管理に対する組織の取組姿勢を示すものである。 情報セキュリティ方針は、次のものから得た出される要求事項を考慮に入れる。 a) 事業上の戦略及び要求事項 b) 規制、法令及び契約 c) 現在の及び予想される情報セキュリティのリスク及び脅威 情報セキュリティ方針には、次の事項に関する記載を含める。 a) 情報セキュリティの定義 b) 情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組み c) 情報セキュリティに関する全ての活動の指針となる原則 d) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメント e) 情報セキュリティマネジメントシステムの継続的な改善へのコミットメント f) 情報セキュリティマネジメントに関する責任の、定められた役割への割当て g) 逸脱及び例外を取り扱う手順 方針群のより低いレベルでは、情報セキュリティ方針は、情報セキュリティ管理策の実施を更に義務付けるために、必要に応じてトピック固有の方針によって支持する。トピック固有の方針は、一般に、組織内で対象とする特定のグループのニーズに対応するように、又は特定のセキュリティ領域を対象とするように構成される。 トピック固有の方針は、組織の情報セキュリティ方針に沿い、それを補完する。このようなトピックの例を次に示す。 a) アクセス制御 b) 物理的及び環境的セキュリティ c) 資産管理 d) 情報の転送 e) 利用者エンドポイント機器のセキュリティを保った構成及び取扱い f) ネットワークセキュリティ g) 情報セキュリティインシデント管理 h) バックアップ i) 暗号及び鍵管理 j) 情報の分類及び取扱い k) 技術的ぜい弱性の管理 l) セキュリティに配慮した開発 トピック固有の方針の作成、レビュー及び承認に関する責任は、関連する要員に、権限及び技術的力量のレベルに基づいて割り当てる。 レビューには、次ものの変化に応じた、組織の情報セキュリティ方針及びトピック固有の方針並びに情報セキュリティの管理に関する、改善の機会の評価を含める。 a) 組織の事業戦略 b) 組織の技術環境 c) 規制、法令及び契約 d) 情報セキュリティリスク e) 現在の及び予想される情報セキュリティの脅威の環境 f) 情報セキュリティ事象及びインシデントから学んだ教訓 情報セキュリティ方針及びトピック固有の方針のレビューは、マネジメントレビュー及び監査の結果を考慮する。 一貫性を維持するため、一つの方針を変更する場合は、他の関連する方針のレビュー及び更新を検討する。	5a-5.1.1	組織は、方針群の最も高いレベルに、一つの"情報セキュリティ方針"を定める。	手引に関連記載あり	5.1.1.1	組織は、経営陣によって承認され、組織の情報セキュリティ目的の管理に対する取組みを示すものとして、方針群の最も高いレベルに、一つの情報セキュリティ方針を定める。
			5a-5.1.2	情報セキュリティ方針は、次のものから得た出される要求事項を考慮に入れる。 a) 事業上の戦略及び要求事項	手引に関連記載あり	5.1.1.2	情報セキュリティ方針は、事業戦略によって生じる要求事項を取り扱う。
			5a-5.1.2	情報セキュリティ方針は、次のものから得た出される要求事項を考慮に入れる。 b) 規制、法令及び契約	手引に関連記載あり	5.1.1.3	情報セキュリティ方針は、規制、法令及び契約によって生じる要求事項を取り扱う。
			5a-5.1.2	情報セキュリティ方針は、次のものから得た出される要求事項を考慮に入れる。 c) 現在の及び予想される情報セキュリティのリスク及び脅威	手引に関連記載あり	5.1.1.4	情報セキュリティ方針は、現在の及び予想される情報セキュリティの脅威環境によって生じる要求事項を取り扱う。
			5a-5.1.3	情報セキュリティ方針には、次の事項に関する記載を含める。 a) 情報セキュリティの定義 b) 情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組み c) 情報セキュリティに関する全ての活動の指針となる原則	手引に関連記載あり	5.1.1.5	情報セキュリティ方針には、情報セキュリティに関する全ての活動の指針となる、情報セキュリティの定義、目的及び原則に関する記載を含める。
			5a-5.1.3	情報セキュリティ方針には、次の事項に関する記載を含める。 d) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメント e) 情報セキュリティマネジメントシステムの継続的な改善へのコミットメント	手引に関連記載あり	–	（対応項なし）
			5a-5.1.3	情報セキュリティ方針には、次の事項に関する記載を含める。 f) 情報セキュリティマネジメントに関する責任の、定められた役割への割当て	手引に関連記載あり	5.1.1.6	情報セキュリティ方針には、情報セキュリティマネジメントに関する一般的な責任及び特定の責任の、定められた役割への割当てに関する記載を含める。
			5a-5.1.3	情報セキュリティ方針には、次の事項に関する記載を含める。 g) 逸脱及び例外を取り扱う手順	手引に関連記載あり	5.1.1.7	情報セキュリティ方針には、逸脱及び例外を取り扱うプロセスに関する記載を含める。
			5a-5.1.5	方針群のより低いレベルでは、情報セキュリティ方針は、情報セキュリティ管理策の実施を更に義務付けるために、必要に応じてトピック固有の方針によって支持する。	手引に関連記載あり	5.1.1.8	方針群のより低いレベルでは、情報セキュリティ方針は、トピックに応じて定める個別方針 によって支持されるようにする。
			(5a-5.1.5参考)	トピック固有の方針は、一般に、組織内で対象とする特定のグループのニーズに対応するように、又は特定のセキュリティ領域を対象とするように構成される。	手引に関連記載あり	–	（対応項なし）
			5a-5.1.6	トピック固有の方針は、組織の情報セキュリティ方針に沿い、それを補完する。	手引に関連記載あり	–	（対応項なし）
			(5a-5.1.6参考)	このようなトピックの例を、次に示す。 a) アクセス制御	手引に関連記載あり	5.1.1.9	個別方針のトピックとして、アクセス制御を含める。
			(5a-5.1.6参考)	このようなトピックの例を、次に示す。 b) 物理的及び環境的セキュリティ	手引に関連記載あり	5.1.1.11	個別方針のトピックとして、物理的及び環境的セキュリティを含める。
			(5a-5.1.6参考)	このようなトピックの例を、次に示す。 d) 情報の転送	手引に関連記載あり	5.1.1.14	個別方針のトピックとして、情報の転送を含める。
			(5a-5.1.6参考)	このようなトピックの例を、次に示す。 e) 利用者エンドポイント機器のセキュリティを保った構成及び取扱い	手引に関連記載あり	5.1.1.12	個別方針のトピックとして、エンドユーザ関連のトピック（資産利用の許容範囲、クリアデスク・クリアスクリーン、情報転送、モバイル機器及びテレワーキング、ソフトウェアのインストール及び使用の制限）を含める。
			(5a-5.1.6参考)	このようなトピックの例を、次に示す。 f) ネットワークセキュリティ	手引に関連記載あり	5.1.1.18	個別方針のトピックとして、通信のセキュリティを含める。
			(5a-5.1.6参考)	このようなトピックの例を、次に示す。 h) バックアップ	手引に関連記載あり	5.1.1.13	個別方針のトピックとして、バックアップを含める。
			(5a-5.1.6参考)	このようなトピックの例を、次に示す。 i) 暗号及び鍵管理	手引に関連記載あり	5.1.1.17	個別方針のトピックとして、暗号による管理策を含める。
			(5a-5.1.6参考)	このようなトピックの例を、次に示す。 j) 情報の分類及び取扱い	手引に関連記載あり	5.1.1.10	個別方針のトピックとして、情報分類（及び取扱い）を含める。
			(5a-5.1.6参考)	このようなトピックの例を、次に示す。 k) 技術的ぜい弱性の管理	手引に関連記載あり	5.1.1.16	個別方針のトピックとして、技術的ぜい弱性の管理を含める。
			(5a-5.1.6参考)	このようなトピックの例を、次に示す。 j) 情報の分類及び取扱い	手引に関連記載あり	5.1.1.10	個別方針のトピックとして、情報分類（及び取扱い）を含める。
			(5a-5.1.6参考)	このようなトピックの例を、次に示す。 c) 資産管理 g) 情報セキュリティインシデント管理 l) セキュリティに配慮した開発	手引に関連記載あり	–	（対応項なし）
			5a-5.1.7	トピック固有の方針の作成、レビュー及び承認に関する責任は、関連する要員に、権限及び技術的力量のレベルに基づいて割り当てる。	手引に関連記載あり	5.1.2.1	各々の情報セキュリティのための方針には、その方針の作成、レビュー及び評価についての管理責任を与えられた責任者を置く。
			5a-5.1.8	レビューには、次ものの変化に応じた、組織の情報セキュリティ方針及びトピック固有の方針並びに情報セキュリティの管理に関する、改善の機会の評価を含める。 a) 組織の事業戦略 b) 組織の技術環境 c) 規制、法令及び契約 d) 情報セキュリティリスク e) 現在の及び予想される情報セキュリティの脅威の環境 f) 情報セキュリティ事象及びインシデントから学んだ教訓	手引に関連記載あり	5.1.2.2	情報セキュリティのための方針群のレビューには、組織の環境、業務環境、法的状況又は技術環境の変化に応じた、組織の情報セキュリティのための方針群及び情報セキュリティの管理への取組みに関する、改善の機会の評価を含める。
			5a-5.1.9	情報セキュリティ方針及びトピック固有の方針のレビューは、マネジメントレビュー及び監査の結果を考慮する。	手引に関連記載あり	5.1.2.3	情報セキュリティのための方針群のレビューでは、マネジメントレビューの結果を考慮し、反映する。
			5a-5.1.10	一貫性を維持するため、一つの方針を変更する場合は、他の関連する方針のレビュー及び更新を検討する。	手引に関連記載あり	–	（対応項なし）
5.1.2	トップマネジメントは、情報セキュリティ方針を、あらかじめ定めた期間及び重大な変化が発生した場合に承認する。	情報セキュリティ方針のいかなる変更もトップマネジメントが承認する。	5a-5.1.4	情報セキュリティ方針のいかなる変更もトップマネジメントが承認する。	手引に関連記載あり	5.1.2.4	改訂された情報セキュリティのための方針は、管理層から承認を得る。
5.1.3	情報セキュリティ方針を、関連する要員及び利害関係者に伝達する。	情報セキュリティ方針は、関連する要員及び利害関係者にアクセスでき、かつ、理解しやすい形で、伝達する。 必要な場合には、方針の受領者に、方針を理解したこと及びその順守に同意することの確認を求める。組織は、これらの方針文書について、組織のニーズを満たす形式及び名称を決定することが可能である。組織によって、情報セキュリティ方針及びトピック固有の方針を単一の文書にすることがある。組織は、トピック固有の方針に、標準、指令、方針、その他の名称を付けることがある。 情報セキュリティ方針を組織外に配布する場合には、秘密情報を不適切に開示しないように注意する。	5a-5.1.11	情報セキュリティ方針及びトピック固有の方針は、意図する読者にとって適切で、アクセスでき、かつ、理解しやすい形で、関連する要員及び利害関係者に伝達する。	手引に関連記載あり	5.1.1.21	トピック別の個別方針は、従業員及び関係する外部関係者にとって適切で、アクセス可能かつ理解可能な形式で伝達する（例えば、情報セキュリティの意識向上、教育及び訓練のプログラムに従う。）。
			5a-5.1.12	必要な場合には、方針の受領者に、方針を理解したこと及びその順守に同意することの確認を求める。	手引に関連記載あり	–	（対応項なし）
			(5a-5.1参考1)	組織は、これらの方針文書について、組織のニーズを満たす形式及び名称を決定することが可能である。	手引に関連記載あり	–	（対応項なし）
			(5a-5.1参考2)	組織によって、情報セキュリティ方針及びトピック固有の方針を単一の文書にすることがある。	手引に関連記載あり	–	（対応項なし）
			(5a-5.1参考3)	組織は、トピック固有の方針に、標準、指令、方針、その他の名称を付けることがある。	手引に関連記載あり	–	（対応項なし）
			5a-5.1.13	情報セキュリティ方針又はトピック固有の方針を組織外に配布する場合には、秘密情報を不適切に開示しないように注意する。	手引に関連記載あり	–	（対応項なし）
5.1.4	クラウドサービスの提供及び利用に当たした、情報セキュリティ方針を策定する。	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.2	情報セキュリティの役割及び責任 統制目標：情報セキュリティの役割及び責任は、組織のニーズに従って定め、割り当てる。 目的：組織内における情報セキュリティの実施、運用及び管理のために、定義され、承認され、理解される構造を確立するため。		5.2	情報セキュリティの役割及び責任 管理策 情報セキュリティの役割及び責任は、組織のニーズに従って定め、割り当てる。 目的 組織内における情報セキュリティの実施、運用及び管理のために、定義され、承認され、理解される構造を確立するため。		6.1	内部組織 管理目的：組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。
						6.1.1	情報セキュリティの役割及び責任 全ての情報セキュリティの責任を定め、割り当てる。
5.2.1	情報セキュリティ方針に従い、情報セキュリティの役割及び責任を定義し、割り当てる。	情報セキュリティの役割及び責任の割当ては、情報セキュリティ方針及びトピック固有の方針（5.1参照）に従って行う。 組織は、次の事項に関する責任を定義し、管理する。 a) 情報及びその他の関連資産の保護 b) 情報セキュリティプロセスの実施 c) 情報セキュリティのリスクマネジメント活動、特に残留リスクの受容（例えば、リスク所有者） d) 組織の情報及びその他の関連資産を使用する全ての要員	5a-5.2.1	情報セキュリティの役割及び責任の割当ては、情報セキュリティ方針及びトピック固有の方針に従って行う。	手引に関連記載あり	6.1.1.1	情報セキュリティの責任の割当ては、情報セキュリティのための方針群に従って行う。
			5a-5.2.2	組織は、次の事項に関する責任を定義し、管理する。 a) 情報及びその他の関連資産の保護 b) 特定の情報セキュリティプロセスの実施	手引に関連記載あり	6.1.1.2	個々の資産の保護に対する責任及び特定の情報セキュリティプロセスの実施に対する責任を定める。
			5a-5.2.2	組織は、次の事項に関する責任を定義し、管理する。 c) 情報セキュリティのリスクマネジメント活動、特に残留リスクの受容	手引に関連記載あり	6.1.1.3	情報セキュリティのリスクマネジメント活動に関する責任、特に残留リスクの受容に関する責任を定める。
			5a-5.2.2	組織は、次の事項に関する責任を定義し、管理する。 d) 組織の情報及びその他の関連資産を使用する全ての要員	手引に関連記載あり	–	（対応項なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.2.2	個人が責任をもつ各セキュリティ領域及び承認のレベルを定義し、情報セキュリティの役割をもつ個人に対してそれを伝達する。	個人が責任をもつ各セキュリティ領域を定義し、文書化し、伝達する。 承認のレベルを定義し、文書化する。 特定の情報セキュリティの役割をもつ個人は、その役割に必要な知識及び技能においてカ量をもつ。 その役割に関連し、その役割の責任を果たす上で必要な最新の動向に追随し続けるように支援される。	5a-5.2.5	個人が責任をもつ各セキュリティ領域を定義し、文書化し、伝達する。	手引に関連記載あり	6.1.1.7	個人が責任をもつ領域を規定する。
					手引に関連記載あり	6.1.1.9	個人が責任をもつ領域を規定するために、各資産又は情報セキュリティプロセスに対する責任主体の指定、及び/その責任の詳細の文書化を実施する。
			5a-5.2.6	承認のレベルを定義し、文書化する。	手引に関連記載あり	6.1.1.10	個人が責任をもつ領域を規定するために、承認レベルの規定及び/文書化を実施する。
			5a-5.2.7	特定の情報セキュリティの役割をもつ個人は、その役割に必要な知識及び技能においてカ量をもつ。	手引に関連記載あり	6.1.1.11	個人が責任をもつ領域を規定するために、情報セキュリティ分野における責任を果たせるよう、任命された個人が当該分野のカ量をもつこと、及び/最新の状況を把握するための機会が与えられるようにする。
			5a-5.2.8	その役割に関連し、その役割の責任を果たす上で必要な最新の動向に追随し続けるように支援される。	手引に関連記載あり	–	（対応項なし）
5.2.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.3	職務の分離 統制目標：相反する職務及び相反する責任範囲は、分離する。 目的：情報セキュリティ管理策の不正、誤り及び/又は盗みのリスクを軽減するため。		5.3	職務の分離 管理策 相反する職務及び相反する責任範囲は、分離する。 目的 情報セキュリティ管理策の不正、誤り及び/又は盗みのリスクを軽減するため。		6.1.2	職務の分離 相反する職務及び/責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離する。
5.3.1	どの職務及び責任範囲を分離する必要があるか定義し、分離する。	職務及び責任範囲の分離は、相反する可能性がある職務を一人の個人が自ら実行することを防ぐために、相反する職務を異なる個人に分離することを目的としている。次の事項は、分離が必要になる可能性のある活動の例である。 a) 変更の提案、承認及び実行 b) アクセス権の要求、承認及び付与 c) コードの設計、実装及びレビュー d) ソフトウェアの開発及び本番システムの管理 e) アプリケーションの使用及び管理 f) アプリケーションの使用及びデータベースの管理 g) 情報セキュリティ管理策の設計、監査及び保証 h) 承認又は許可を受ける申請者と当該承認等を行う許可権限者 i) 監査を受ける者とその監査を実施する者 分離の管理策の設計においては、共謀のおそれを考慮する。小さな組織では、職務の分離を実現するのは難しい場合がある。しかし、この原則は、実施可能な限り適用することが望ましい。 分離が困難である場合には、活動の監視、監査証跡、管理職による監督等の他の管理策を考慮する。 役割に基づくアクセス制御システムを使用する場合に、一人の個人に対して、相反する複数の役割を許可しないことを確実にするように注意する。 多数の役割がある場合、組織は、相反する役割を特定し、その除去を容易にするために自動化ツールの使用を考慮する。 役割を除去又は再割当てする場合のアクセスの問題を最小限にするために、役割は慎重に定義し、付与する。	5a-5.3.1	組織は、どの職務及び責任範囲を分離する必要があるかを決定する。	手引に関連記載あり	6.1.2.1	認可されていない状況又は検知されない状態で、一人で資産に対してアクセス、修正又は使用ができないように管理策を適用する。
			5a-5.3.2	分離の管理策の設計においては、共謀のおそれを考慮する。	手引に関連記載あり	6.1.2.3	管理策は、共謀のおそれを考慮して設計する。
			5a-5.3.3	分離が困難である場合には、活動の監視、監査証跡、管理職による監督等の他の管理策を考慮する。	手引に関連記載あり	6.1.2.4	職務の分離が困難である場合には、他の管理策（例えば、活動の監視、監査証跡、管理職による監督）を実施する。
			5a-5.3.4	役割に基づくアクセス制御システムを使用する場合に、一人の個人に対して、相反する複数の役割を許可しないことを確実にするように注意する。	手引に関連記載あり	–	（対応項なし）
			5a-5.3.5	多数の役割がある場合、組織は、相反する役割を特定し、その除去を容易にするために自動化ツールの使用を考慮する。	手引に関連記載あり	–	（対応項なし）
			5a-5.3.6	役割を除去又は再割当てする場合のアクセスの問題を最小限にするために、役割は慎重に定義し、付与する。	手引に関連記載あり	–	（対応項なし）
5.3.2	情報セキュリティ対策の運用において、以下の役割を兼務させない。 ・承認又は許可を受ける申請者と当該承認等を行う許可権限者 ・監査を受ける者とその監査を実施する者	特になし。	–	（統一基準由来）	令和7年版にて追加（情報セキュリティ管理基準以外の由来）	–	（対応項なし）
5.4	管理策の責任 統制目標：管理層は、組織の確立された情報セキュリティ方針、トピック固有の方針及び手順に従った情報セキュリティの適用を、全ての要員に要求する。 目的：管理層が、情報セキュリティにおける自らの役割を理解し、全ての要員が自らの情報セキュリティの責任を認識し、果たすことを確実にすることを目的として行動することを確実にするため。		5.4	管理策の責任 管理策 管理層は、組織の確立された情報セキュリティ方針、トピック固有の方針及び手順に従った情報セキュリティの適用を、全ての要員に要求する。 目的 管理層が、情報セキュリティにおける自らの役割を理解し、全ての要員が自らの情報セキュリティの責任を認識し、果たすことを確実にすることを目的として行動することを確実にするため。		7.2.1	経営陣の責任 経営陣は、組織の確立された方針及び手順に従った情報セキュリティの適用を、全ての従業員及び契約相手に要求する。
5.4.1	方針及び手順に従った情報セキュリティの適用を、全ての要員へ実施させることを、管理層の責任として定める。	管理層は、情報セキュリティ方針、トピック固有の方針、手順及び情報セキュリティ管理策に対する支援を実証する。 管理層の責任には、要員について、次の事項を確実にすることを含む。 a) 組織の情報及びその他の関連資産へのアクセスを許可する前に、情報セキュリティの役割及び責任について、要点を適切に伝える。 b) 組織内で、情報セキュリティについて要員に期待する役割を示す指針を提供する。 c) 組織の情報セキュリティ方針及びトピック固有の方針に従うことを指示する。 d) 組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する（6.3参照）。 e) 組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件、契約又は合意を順守する。 f) 継続的な専門教育を通じて、情報セキュリティに関する適切な技能及び資格を保持し続ける。 g) 実行可能な場合、情報セキュリティ方針、トピック固有の方針又は情報セキュリティのための手順への違反を報告するための、匿名の報告経路を提供する（例えば、内部通報）。これによって、匿名の報告を可能にする、又は報告者のアイデンティティに関する知識をその報告を扱う必要のある人だけが知ることを確実にする傾えをもつことを可能にする。 h) 組織のセキュリティ関連のプロセス及び管理策を実施するための、適切な資源及びプロジェクトを計画する時間を提供する。	5a-5.4.1	管理層は、情報セキュリティ方針、トピック固有の方針、手順及び情報セキュリティ管理策に対する支援を実証する。	手引に関連記載あり	7.2.1.8	経営陣は、情報セキュリティのための方針群、手順及び管理策に対する支持を実証し、手本となるように行動する。
			5a-5.4.2	管理職の責任には、要員について、次の事項を確実にすることを含む。 a) 組織の情報及びその他の関連資産へのアクセスを許可する前に、情報セキュリティの役割及び責任について、要点を適切に伝える。	手引に関連記載あり	7.2.1.1	経営陣の責任には、従業員及び契約相手に、秘密情報又は情報システムへのアクセスが許可される前に、情報セキュリティの役割及び責任について、要点を適切に伝える仕組みを整備することを含める。
			5a-5.4.2	管理職の責任には、要員について、次の事項を確実にすることを含む。 b) 組織内で、情報セキュリティについて要員に期待する役割を示す指針を提供する。	手引に関連記載あり	7.2.1.2	経営陣の責任には、従業員及び契約相手に、組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組みを整備することを含める。
			5a-5.4.2	管理職の責任には、要員について、次の事項を確実にすることを含む。 c) 組織の情報セキュリティ方針及びトピック固有の方針に従うことを指示する。	手引に関連記載あり	7.2.1.3	経営陣の責任には、従業員及び契約相手に、組織の情報セキュリティのための方針群に従うように動機付ける仕組みを整備することを含める。
			5a-5.4.2	管理職の責任には、要員について、次の事項を確実にすることを含む。 d) 組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成させる。	手引に関連記載あり	7.2.1.4	経営陣の責任には、従業員及び契約相手に、組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組みを整備することを含める。
			5a-5.4.2	管理職の責任には、要員について、次の事項を確実にすることを含む。 e) 組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件、契約又は合意を順守させる。	手引に関連記載あり	7.2.1.5	経営陣の責任には、従業員及び契約相手に、組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うように手引き仕組みを整備することを含める。
			5a-5.4.2	管理職の責任には、要員について、次の事項を確実にすることを含む。 f) 継続的な専門教育を通じて、情報セキュリティに関する適切な技能及び資格を維持させる。	手引に関連記載あり	7.2.1.6	経営陣の責任には、従業員及び契約相手に、適切な技能及び資格を保持し、定期的に教育を受けさせる仕組みを整備することを含める。
			5a-5.4.2	管理職の責任には、要員について、次の事項を確実にすることを含む。 g) 実行可能な場合、情報セキュリティ方針、トピック固有の方針又は情報セキュリティのための手順への違反を報告するための、匿名の報告経路を提供する。これによって、匿名の報告を可能にする、又は報告者のアイデンティティに関する知識をその報告を扱う必要のある人だけが知ることを確実にする傾えをもつことを可能にする。	手引に関連記載あり	7.2.1.7	経営陣の責任には、従業員及び契約相手に、情報セキュリティのための方針群又は手順への違反を報告するための、匿名の報告経路を提供する（例えば、内部告発）仕組みを整備することを含める。
			5a-5.4.2	管理職の責任には、要員について、次の事項を確実にすることを含む。 h) 組織のセキュリティ関連のプロセス及び管理策を実施するための、適切な資源及びプロジェクトを計画する時間を提供する。	手引に関連記載あり	–	（対応項なし）
5.5	関係当局との連絡 統制目標：組織は、関係当局との連絡体制を確立し、維持する。 目的：組織と、関係する法務、規制及び/監督当局との間で、情報セキュリティに関して適切な情報の流通が行われることを確実にするため。		5.5	関係当局との連絡 管理策 組織は、関係当局との連絡体制を確立し、維持する。 目的 組織と、関係する法務、規制及び/監督当局との間で、情報セキュリティに関して適切な情報の流通が行われることを確実にするため。		6.1.3	関係当局との連絡 関係当局との適切な連絡体制を維持する。
5.5.1	情報セキュリティに関して、適切な情報の流通が行われることを確実にするために、関係当局との連絡体制を確立し、維持する。	組織は、いつ、誰が関係当局（例えば、法執行機関、規制当局、監督官庁）に連絡するか、及び/特定した情報セキュリティインシデントをいかにして時機を失せずに報告するかを規定する。 関係当局との連絡は、これらの関係当局の現在及び/今後の期待（例えば、適用される情報セキュリティ規制）についての理解を促進するためにも用いる。	5a-5.5.1	組織は、いつ、誰が関係当局に連絡するか、及び/特定した情報セキュリティインシデントをいかにして時機を失せずに報告するかを規定する。	手引に関連記載あり	6.1.3.1	組織は、いつ、誰が関係当局（例えば、法の執行機関、規制当局、監督官庁）に連絡するかの手順を備える。
					手引に関連記載あり	6.1.3.2	法が破られと疑われる場合に、特定した情報セキュリティインシデントをいかにして時機を失せずに報告するかの手順を備える。
			5a-5.5.2	関係当局との連絡は、これらの関係当局の現在及び/今後の期待についての理解を促進するためにも用いる。	手引に関連記載あり	–	（対応項なし）
5.5.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.6	専門組織との連絡 統制目標：組織は、情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との連絡体制を確立し、維持する。 目的：情報セキュリティに関して適切な情報流通が行われることを確実にするため。		5.6	専門組織との連絡 管理策 組織は、情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との連絡体制を確立し、維持する。 目的 情報セキュリティに関して適切な情報流通が行われることを確実にするため。		6.1.4	専門組織との連絡 情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持する。
5.6.1	情報セキュリティに関して、適切な情報の流通が行われることを確実にするために、専門組織との連絡体制を確立し、維持する。	次の事項を達成する手段として、専門組織（情報セキュリティに関する研究会又は会議及び情報セキュリティの専門家による協会・団体）との連絡体制を確立し、維持する。 a) 厳適な慣行に関する知識を改善し、関係するセキュリティ情報に追随する。 b) 情報セキュリティ環境の理解が最新であることを確実にする。 c) 攻撃及び扒い弱性に関する早期警戒警報、勧告及びパッチを受理する。 d) 専門家から情報セキュリティの助言を得る。 e) 新しい技術、製品、サービス、脅威又は扒い弱性に関する情報を共有し、交換する。 f) 情報セキュリティインシデントを扱う場合の、適切な連絡窓口を提供する（5.24～5.28参照）。	5a-5.6.1	次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。 a) 厳適な慣行に関する知識を改善し、関係するセキュリティ情報に追随する。	手引に関連記載あり	6.1.4.1	厳適な慣行に関する認識を改善し、関係するセキュリティ情報を最新に保つ手段として、情報セキュリティに関する研究会又は会議へ参加する。
			5a-5.6.1	次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。 b) 情報セキュリティ環境の理解が最新であることを確実にする。	手引に関連記載あり	6.1.4.2	情報セキュリティ環境の理解が最新かつ完全であることを確実にする手段として、情報セキュリティに関する研究会又は会議へ参加する。
			5a-5.6.1	次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。 c) 攻撃及び扒い弱性に関する早期警戒警報、勧告及びパッチを受理する。	手引に関連記載あり	6.1.4.3	攻撃及び扒い弱性に関連する早期警戒警報、勧告及びパッチを受理する手段として、情報セキュリティに関する研究会又は会議へ参加する。
			5a-5.6.1	次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。 d) 専門家から情報セキュリティの助言を得る。	手引に関連記載あり	6.1.4.4	専門家から情報セキュリティの助言を得る手段として、情報セキュリティに関する研究会又は会議へ参加する。
			5a-5.6.1	次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。 e) 新しい技術、製品、サービス、脅威又は扒い弱性に関する情報を共有し、交換する。	手引に関連記載あり	6.1.4.5	新しい技術、製品、脅威又は扒い弱性に関する情報を共用し、交換する手段として、情報セキュリティに関する研究会又は会議へ参加する。
			5a-5.6.1	次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。 f) 情報セキュリティインシデントを扱う場合の、適切な連絡窓口を提供する。	手引に関連記載あり	6.1.4.6	情報セキュリティインシデントを扱う場合の、適切な連絡窓口を提供する手段として、情報セキュリティに関する研究会又は会議へ参加する。
5.7	脅威インテリジェンス 統制目標：情報セキュリティの脅威に関連する情報を収集及び分析し、脅威インテリジェンスを構築する。 目的：適切な/又り低減処置を講じることが可能となるように、組織の脅威環境についての認識をもつため。		5.7	脅威インテリジェンス 管理策 情報セキュリティの脅威に関連する情報を収集及び分析し、脅威インテリジェンスを構築することが望ましい。 目的 適切な/又り低減処置を講じることが可能となるように、組織の脅威環境についての認識をつため。		–	（対応項なし）
5.7.1	既存の又は新たな脅威に関する情報を収集及び分析するための目的を定める。	既存の又は新たな脅威に関する情報を、次の目的で収集し、分析する。 a) 脅威が組織に危害を及ぼすことを防止するために、十分な情報に基づく活動を支援する。 b) 脅威の影響を減らす。 脅威インテリジェンスは3階に分けることができ、これらの全てを考慮する。 a) 戦略的脅威インテリジェンス：変化する脅威の状況に関する高レベルの情報の交換（例えば、攻撃者の種類又は攻撃の種類） b) 戦術的脅威インテリジェンス：攻撃者が使う手法、ツール及び/技術に関する情報の交換 c) 運用上の脅威インテリジェンス：技術的特徴を含む特定の攻撃に関する詳細 脅威インテリジェンスの構築に必要な情報を提供するのに必要かつ適切な情報源を特定し、PR味し、選択する。	5a-5.7.1	既存の又は新たな脅威に関する情報を、次の目的で収集し、分析する。 a) 脅威が組織に危害を及ぼすことを防止するために、十分な情報に基づく活動を支援する。 b) 脅威の影響を減らす。	手引に関連記載あり	–	（対応項なし）
			5a-5.7.2	脅威インテリジェンスを構成する次の3階全てを考慮する。 a) 戦略的脅威インテリジェンス：脅威の動向に関する大局的な情報の交換 b) 戦術的脅威インテリジェンス：攻撃者が使う手法、ツール及び/技術に関する情報の交換 c) 運用上の脅威インテリジェンス：技術的特徴を含む特定の攻撃に関する詳細	手引に関連記載あり	–	（対応項なし）
5.7.2	目的を達成するために必要なインテリジェンス要件を定める。	脅威インテリジェンスは、次の事項を満たす。 a) 課題に応える（すなわち、組織の保護に関係する。）。 b) 十分な情報を含む（すなわち、脅威の状況に関する正確かつ詳細な理解を組織に提供する。）。 c) 状況認識を与えるような状況情報を含む（すなわち、事象の発生時間、場所、以前の経験及び同種の組織における傾向によって、情報に状況を加える。）。 d) 対応可能である（すなわち、組織が情報に基づいて迅速かつ効果的に対応可能である。）。	5a-5.7.3	脅威インテリジェンスは、次の事項を満たす。 a) 課題に応える（すなわち、組織の保護に関係する。）。 b) 十分な情報を含む（すなわち、脅威の状況に関する正確かつ詳細な理解を組織に提供する。）。 c) 状況認識を与えるような状況情報を含む（すなわち、事象の発生時間、場所、以前の経験及び同種の組織における傾向によって、情報に状況を加える。）。 d) 対応可能である（すなわち、組織が情報に基づいて迅速かつ効果的に対応可能である。）。	手引に関連記載あり	–	（対応項なし）
5.7.3	脅威インテリジェンス活動を実施する。	脅威インテリジェンス活動は、次の事項を含む。 a) 脅威インテリジェンスの構築の目的を確立する。 b) 脅威インテリジェンスの構築に必要な情報を提供するのに必要かつ適切な内部及び外部の情報源を特定し、PR味し、選択する。 c) 内部及び外部のいずれによらず、精選した情報源から情報を収集する。 d) 収集した情報を、分析に備えて処理する（例えば、情報を変換、形式化、又は要行うことによる）。 e) 情報を、それが組織にどのように関係し、意味をもつかを理解するために分析する。 f) 関係する個人に分析した結果を理解可能な形式で伝達し、共有する。 次の観点で分析し、組織が必要とする適切かリスク低減処理を講じるために使用す	5a-5.7.4	脅威インテリジェンス活動は、次の事項を含む。 a) 脅威インテリジェンスの構築の目的を確立する。 b) 脅威インテリジェンスの構築に必要な情報を提供するのに必要かつ適切な内部及び外部の情報源を特定し、PR味し、選択する。 c) 内部及び外部のいずれによらず、精選した情報源から情報を収集する。 d) 収集した情報を、分析に備えて処理する。 e) 情報を、それが組織にどのように関係し、意味をもつかを理解するために分析する。 f) 関係する個人に分析した結果を理解可能な形式で伝達し、共有する。	手引に関連記載あり	–	（対応項なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
		。 a) 脅威インテリジェンスの情報源から収集した情報を組織の情報セキュリティリスクマネジメントプロセスに反映する必要性があか否か。 b) ファイアウォール、侵入検知システム、マルウェア対策ソリューションなどの技術的な予防及び検知の管理策への追加の考慮事項とすべきか否か。 c) 情報セキュリティテストのプロセス及び手法への考慮事項とすべきか否か。 組織は、脅威インテリジェンス全体を改善するために、脅威インテリジェンスを他の組織と相互に共有する。	5a-5.7.5	脅威インテリジェンスを分析し、次のおりに使用する。 a) 脅威インテリジェンスの情報源から収集した情報を組織の情報セキュリティリスクマネジメントプロセスに含めるプロセスを実施することによって、 b) ファイアウォール、侵入検知システム、マルウェア対策ソリューションなどの技術的な予防及び検知の管理策への追加の入力として、 c) 情報セキュリティテストのプロセス及び手法への入力として。	手引に関連記載あり	–	（対応項なし）
			5a-5.7.6	組織は、脅威インテリジェンス全体を改善するために、脅威インテリジェンスを他の組織と相互に共有する。	手引に関連記載あり	–	（対応項なし）
5.8	プロジェクトマネジメントにおける情報セキュリティ 統制目標：情報セキュリティをプロジェクトマネジメントに組み入れる。 目的：プロジェクトのライフサイクル全体を通して、プロジェクトマネジメントにおいて、プロジェクト及び成果物に関連する情報セキュリティリスクに効果的に対処することを確実にするため。		5.8	プロジェクトマネジメントにおける情報セキュリティ 管理策 情報セキュリティをプロジェクトマネジメントに組み入れる。 目的 プロジェクトのライフサイクル全体を通して、プロジェクトマネジメントにおいて、プロジェクト及び成果物に関連する情報セキュリティリスクに効果的に対処することを確実にするため。		6.1.5	プロジェクトマネジメントにおける情報セキュリティ プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組む。
						14.1.1	情報セキュリティ要求事項の分析及び仕様化 情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含める。
5.8.1	情報セキュリティリスクへの対応をプロジェクトマネジメントに組み入れる。	プロジェクトマネジメントの一部として情報セキュリティリスクに対処することを確実にするために、情報セキュリティをプロジェクトマネジメントに組み入れる。これは、プロジェクトの複雑さ、規模、期間、分野又は適用領域にかかわらず、あらゆる種類のプロジェクトに適用可能である（例えば、中核事業プロセス、ICT、施設管理又はその他の支援プロセスのプロジェクト）。 プロジェクトマネジメントでは、次の事項を要求する。 a) 情報セキュリティリスクを、プロジェクトリスクの一部として、プロジェクトのライフサイクル全体を通じて、早い段階及び定期的にリスクアセスメント及びリスク対応を実施する。 b) 情報セキュリティ要求事項（例えば、アプケーションセキュリティの要求事項（8.26）、知的財産権を順守するための要求事項（5.32）など）は、プロジェクトの早い段階に対処する。 c) 内部及び外部への伝達の側面のセキュリティなど、プロジェクトの実行に伴う情報セキュリティリスク、プロジェクトのライフサイクル全体を通じて考慮し、処理する。 d) 情報セキュリティリスク対応の進捗状況及び活動の適切性を、あらかじめ定めた段階において、適切な人物又はガバナンス機関がフォローアップする。 プロジェクトに関連する情報セキュリティの責任及び権限を定義し、規定された役割に割り当てる。	5a-5.8.1	プロジェクトマネジメントの一部として情報セキュリティリスクに対処することを確実にするために、情報セキュリティをプロジェクトマネジメントに組み入れる。	手引に関連記載あり	6.1.5.1	情報セキュリティリスクがプロジェクトの中で特定及び対処されることを確実にするために、情報セキュリティを組織のプロジェクトマネジメント手法に組み入れ、プロジェクトの特性にかかわらず、一般にあらゆるプロジェクト（例えば、中核事業プロセス、IT、施設管理、その他のサポートプロセスのためのプロジェクト）に適用されるようにする
			（5a-5.8.1参考）	これは、プロジェクトの複雑さ、規模、期間、分野又は適用領域にかかわらず、あらゆる種類のプロジェクトに適用可能である。	手引に関連記載あり	–	（対応項なし）
			5a-5.8.2	用いるプロジェクトマネジメントでは、次の事項を要求する。 a) 情報セキュリティリスクを、プロジェクトリスクの一部として、プロジェクトのライフサイクル全体を通じて、早い段階及び定期的にリスクアセスメント及びリスク対応を実施する。 b) 情報セキュリティ要求事項には、プロジェクトの早い段階で対処する。	手引に関連記載あり	6.1.5.3	プロジェクトマネジメント手法においては、必要な管理策を特定するため、プロジェクトの早い段階で情報セキュリティリスクアセスメントを実施する。
					手引に関連記載あり	14.1.1.4	情報セキュリティ要求事項及び関連する プロセスの特定及び管理は、情報システムプロジェクトにその初期段階で統合する。
			5a-5.8.2	用いるプロジェクトマネジメントでは、次の事項を要求する。 c) 内部及び外部への伝達の側面のセキュリティなど、プロジェクトの実行に伴う情報セキュリティリスクを、プロジェクトのライフサイクル全体を通じて考慮し、処理する。	手引に関連記載あり	6.1.5.4	プロジェクトマネジメント手法においては、適用するプロジェクトマネジメントの方法論の全ての局面において、情報セキュリティを含める。
			5a-5.8.2	用いるプロジェクトマネジメントでは、次の事項を要求する。 d) 情報セキュリティリスク対応の進捗状況をレビュー し、対応の有効性を評価及び試験する。	手引に関連記載あり	6.1.5.5	全てのプロジェクトにおいて、情報セキュリティの組織への影響を明確にし、これを定期的にレビューする。
			5a-5.8.3	情報セキュリティの考慮及び活動の適切性は、あらかじめ定めた段階において、適切な人物又はプロジェクト運営委員会などのガバナンス機関がフォローアップする。	手引に関連記載あり	–	（対応項なし）
			5a-5.8.4	プロジェクトに関連する情報セキュリティの責任及び権限を定義し、規定された役割に割り当てる。	手引に関連記載あり	6.1.5.6	プロジェクトマネジメント手法で定められた役割を明確にするため、情報セキュリティに関する責任を定め、割り当てる。
5.8.2	プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項を定義する。	プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項は、情報セキュリティ方針、トピック固有の方針及び規制から順守すべき要求事項を導出することを含め、決定する。 プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項は、脅威のモデリング、インシデントのレビュー、ぜい弱性の深刻度の使用、緊急時対応計画策定などの活動から導き出すことができ、それによって、情報システムのアーキテクチャ及び設計を運用環境における既知の脅威から保護することを確実にする。 情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 a) どのような情報が関係する か（情報の決定）、それに対応する情報セキュリティのニーズは何か（分類、5.12参照）、及び適切なセキュリティの欠如から生じる可能性のある事業への潜在的な悪影響 b) 特に機密性、完全性及び可用性の観点から、関係する情報及びその他の関連資産に必要な保護のニーズ c) 認証の要求事項を導き出すための、エンティティが提示する識別情報に求める信頼又は保証のレベル d) 顧客及びその他の潜在的な業務上の利用者のほか、関係するプロジェクトメンバ、潜在的な運用スタッフ、外部供給者などの特権をもつ、又は技術をもつ利用者に対する、アクセスの提供及び認可のプロセス e) 利用者に対する、各自の義務及び責任の通知 f) トランザクションのログ取得及び監視、並びに否認防止の要求事項のような、業務プロセスに由来する要求事項 g) 他の情報セキュリティ管理策によって必要になる要求事項（例えば、ログ取得及び監視のインタフェース、情報漏えい検知システム） h) 組織の活動に適用される法令、規制及び契約上の条件の順守 i) 第三者との合意又は契約における関連セキュリティ箇条を含む、組織の情報セキュリティ計及びトピック固有の方針を満たす上で必要な、第三者に求める価値又は保証のレベル	5a-5.8.5	プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項は、情報セキュリティ方針、トピック固有の方針及び規制から順守すべき要求事項を導出することを含む、様々な方法を用いて決定する。	手引に関連記載あり	14.1.1.1	情報セキュリティ要求事項は、方針及び規則に由来する順守の要求事項、脅威のモデリング、インシデントのレビュー、又は ぜい弱性の限界の使用のような、様々な方法を用いて特定する。
			5a-5.8.6	プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項は、脅威のモデリング、インシデントのレビュー、ぜい弱性の深刻度の使用、緊急時対応計画策定などの活動から導き出すことができ、それによって、情報システムのアーキテクチャ及び設計を運用環境における既知の脅威から保護することを確実にする。	手引に関連記載あり	–	（対応項なし）
			5a-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 a) どのような情報が関係する か（情報の決定）、それに対応する情報セキュリティのニーズは何か、及び適切なセキュリティの欠如から生じる可能性のある事業への潜在的な悪影響	手引に関連記載あり	14.1.1.3	情報セキュリティ要求事項及び情報セキュリティ管理策には、関連する情報の業務上の価値、及びセキュリティが不十分だった場合に業務に及ぶ可能性のある悪影響を反映する。
			5a-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 b) 特に機密性、完全性及び可用性の観点から、関係する情報及びその他の関連資産に必要な保護のニーズ	手引に関連記載あり	14.1.1.8	情報セキュリティ要求事項においては、関連する資産の保護の要求、特に、可用性、機密性及び完全性に関する保護の要求を明確にする。
			5a-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 c) 認証の要求事項を導き出すための、エンティティが提示する識別情報に求める信頼又は保証のレベル	手引に関連記載あり	14.1.1.5	情報セキュリティ要求事項においては、利用者認証の要求事項を導き出すために、利用者が提示する識別情報に対して求める信頼のレベルを定める。
			5a-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 d) 顧客及びその他の潜在的な業務上の利用者のほか、関係するプロジェクトメンバ、潜在的な運用スタッフ、外部供給者などの特権をもつ、又は技術をもつ利用者に対する、アクセスの提供及び認可のプロセス	手引に関連記載あり	14.1.1.2	情報セキュリティ要求事項の特定作業の結果は、文書化し、全ての利害関係者によってレビュー、更新する。
					手引に関連記載あり	14.1.1.6	情報セキュリティ要求事項においては、業務上の利用者のほか、特権を与えられた利用者及び技術をもつ利用者に対する、アクセスの提供及び認可のプロセスを定める。
			5a-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 e) 利用者に対する、各自の義務及び責任の通知	手引に関連記載あり	14.1.1.7	情報セキュリティ要求事項においては、利用者及び運用担当者に対する、各自の義務及び責任の通知を明確にする。
			5a-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 f) トランザクションのログ取得及び監視、並びに否認防止の要求事項のような、業務プロセスに由来する要求事項	手引に関連記載あり	14.1.1.9	情報セキュリティ要求事項においては、トランザクションのログ取得及び監視、並びに否認防止の要求事項のような、業務プロセスに由来する要求事項を定める。
			5a-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 g) 他の情報セキュリティ管理策によって必要になる要求事項	手引に関連記載あり	14.1.1.10	情報セキュリティ要求事項においては、他のセキュリティ管理策によって義務付けられる要求事項を定める（例えば、ログ取得及び監視のインタフェース、情報漏えい検知システム）。
			5a-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 h) 組織の活動に適用される法令、規制及び契約上の条件の順守 i) 第三者との合意又は契約における関連セキュリティ箇条を含む、組織の情報セキュリティ計及びトピック固有の方針を満たす上で必要な、第三者に求める価値又は保証のレベル	手引に関連記載あり	–	（対応項なし）
5.8.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.8.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（SP800-53由来）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	14.1.1.23	情報システムの誤りメッセージは、悪意ある者にとって役立つ情報の開示にならないようにする。
5.9	情報及びその他の関連資産の目録 統制目標：情報及びその他の関連資産の目録を、それぞれの管理責任者を含めて作成し、維持する。 目的：組織の情報及びその他の関連資産を特定し、それらの情報セキュリティを維持し、適切な管理責任を割り当てるため。		5.9	情報及びその他の関連資産の目録 管理策 情報及びその他の関連資産の目録を、それぞれの管理責任者を含めて作成し、維持する。 目的 組織の情報及びその他の関連資産を特定し、それらの情報セキュリティを維持し、適切な管理責任を割り当てるため。		8.1	資産に対する責任 管理目的：組織の資産を特定し、適切な保護の責任を定めるため。
						8.1.1	資産目録 情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持する。
						8.1.2	資産の管理責任 目録の中で維持される資産は、管理する。
5.9.1	情報及びその他の関連資産の目録を作成し、維持する。	文書は、必要に応じて専用の目録又は既存の目録として維持する。 情報及びその他の関連資産は、正確で、最新に保たれ、一貫性があり、他の目録と整合している、情報及びその他の関連資産の目録の正確性を確実にするための選択肢は次のものを含む。 a) 資産目録に照らして、特定した情報及びその他の関連資産の定期的なレビューを実施する。 b) 資産の設置、変更又は除去のプロセスにおいて目録の更新を自動的に適用する。 資産の場所を、必要に応じて目録に含める。 目録は、情報及びその他の関連資産の単一のリストである必要はない。目録は組織において関係する機能が維持することが望ましいことを考えると、情報資産、ハードウェア、ソフトウェア、仮想マシン（VM）、施設、要員、力量、機能及び記録に関する目録などの、動的な目録の集まりとみなすことが可能である。 各資産は、それに関係する情報の分類に従って分類する（5.12参照）。 情報及びその他の関連資産の目録の粒度は、組織のニーズに適したレベルである。資産の性質上、情報のライフサイクルにおいて資産の特定のインスタンスが文書化できない場合がある。短期間だけ存続する資産の例として、ライフサイクルが短いVMインスタンスがある。 情報及びその他の関連資産のそれぞれに対し、情報セキュリティの観点から重要度を決定する。 特定した情報及び資産の分類（5.12参照）を決定する。	5b-5.9.1	組織は、情報及びその他の関連資産を特定し、情報セキュリティの観点からそれらの重要度を決定する。	手引に関連記載あり	8.1.1.1	組織は、情報のライフサイクルに関連し資産を特定し、その重要度を文書化する。
			5b-5.9.2	文書は、必要に応じて専用の目録又は既存の目録として維持する。	手引に関連記載あり	8.1.1.3	文書は、専用の目録又は既存の目録として維持する。
			5b-5.9.3	情報及びその他の関連資産は、正確で、最新に保たれ、一貫性があり、他の目録と整合している、情報及びその他の関連資産の目録の正確性を確実にするための選択肢は次のものを含む。 a) 資産目録に照らして、特定した情報及びその他の関連資産の定期的なレビューを実施する。 b) 資産の設置、変更又は除去のプロセスにおいて目録の更新を自動的に適用する。	手引に関連記載あり	8.1.1.4	資産目録は、正確で、最新に保たれ、一貫性があり、他の目録と整合していることを確実にするよう組みを整備する。
			5b-5.9.4	資産の場所を、必要に応じて目録に含める。	手引に関連記載あり	–	（対応項なし）
			（5b-5.9参考）	目録は、情報及びその他の関連資産の単一のリストである必要はない。目録は組織において関係する機能が維持することが望ましいことを考えると、情報資産、ハードウェア、ソフトウェア、仮想マシン（VM）、施設、要員、力量、機能及び記録に関する目録などの、動的な目録の集まりとみなすことが可能である。	手引に関連記載あり	–	（対応項なし）
			5b-5.9.5	各資産は、それに関係する情報の分類に従って分類する。	手引に関連記載あり	–	（対応項なし）
			5b-5.9.6	情報及びその他の関連資産の目録の粒度は、組織のニーズに適したレベルである。	手引に関連記載あり	–	（対応項なし）
			（5b-5.9.6参考）	資産の性質上、情報のライフサイクルにおいて資産の特定のインスタンスが文書化できない場合がある。短期間だけ存続する資産の例として、ライフサイクルが短いVMインスタンスがある。	手引に関連記載あり	–	（対応項なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.9.2	情報及びその他の関連資産の責任を明確にし、管理責任を個人又はグループに割り当てる。	特定した情報及びその他の関連資産について、各々の資産の管理責任を個人又はグループに割り当て、その上で分類を特定する（5.12及び5.13参照）。 資産の管理責任を時機を失せずに割り当てることを確実にするための プロセスを実施する。 資産を生成した時点、又は資産を組織に移転した時点で、管理責任を割り当てる。 現在の資産の管理責任者が職務を離れる又は変わる場合は、必要に応じて資産の管理責任を再割り当てる。 資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。 a) 情報及びその他の関連資産の目録を作成する。 b) 情報及びその他の関連資産を適切に分類し、保護する。 c) 分類を定期的にレビューする。 d) データベース、ストレージ、ソフトウェアの構成要素、サブ構成要素など、技術資産の構成要素を一覧表示し、ひも（紐）付ける。 e) 情報及びその他の関連資産の許容される利用に関する要求事項（5.10参照）を確立する。 f) アクセス制限が分類に対応し、有効であり、これを定期的にレビューする。 g) 情報及びその他の関連資産は、削除又は破棄する場合、セキュリティに配慮した方法で処理し、目録から削除する。 h) 資産の管理責任者が、資産に関連するリスクの特定及びマネジメントに関与する。 i) 資産の管理責任者が、情報を管理する役割及び責任をもつ要員を支援する。	5b-5.9.7	特定した情報及びその他の関連資産について、各々の資産の管理責任を個人又はグループに割り当て、その上で分類を特定する。	手引に関連記載あり	8.1.1.5	特定された各資産について、管理責任者を割り当て、分類する。
			5b-5.9.8	資産の管理責任を時機を失せずに割り当てることを確実にするためのプロセスを実施する。	手引に関連記載あり	8.1.2.1	資産の管理責任を時機を失せずに割り当てることを確実にするためのプロセスにおいて、資産が生成された時点、又は資産が組織に移転された時点で、適格な者（資産のライフサイクルの管理責任を与えられた個人及び組織）に管理責任を割り当てる。
			5b-5.9.9	資産を生成した時点、又は資産を組織に移転した時点で、管理責任を割り当てる。	手引に関連記載あり	8.1.2.1	【再】資産の管理責任を時機を失せずに割り当てることを確実にするためのプロセスにおいて、資産が生成された時点、又は資産が組織に移転された時点で、適格な者（資産のライフサイクルの管理責任を与えられた個人及び組織）に管理責任を割り当てる。
			5b-5.9.10	現在の資産の管理責任者が職務を離れる又は変わる場合は、必要に応じて資産の管理責任を再割り当てる。	手引に関連記載あり	–	（対応項なし）
			5b-5.9.11	資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。 a) 情報及びその他の関連資産の目録を作成する。	手引に関連記載あり	8.1.2.3	資産の管理責任者は、資産の目録を作成し、維持する仕組みを整備する。
			5b-5.9.11	資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。 b) 情報及びその他の関連資産を適切に分類し、保護する。	手引に関連記載あり	8.1.2.4	資産の管理責任者は、資産を適切に分類及び保護する仕組みを整備する。
			5b-5.9.11	資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。 c) 分類を定期的にレビューする。 d) データベース、ストレージ、ソフトウェアの構成要素、サブ構成要素など、技術資産の構成要素を一覧表示し、ひも（紐）付ける。 e) 情報及びその他の関連資産の許容される利用に関する要求事項を確立する。 f) アクセス制限が分類に対応し、有効であり、これを定期的にレビューする。	手引に関連記載あり	8.1.2.5	資産の管理責任者は、適用されるアクセス制御方針を考慮に入れて、重要な資産に対するアクセスの制限及び分類を定め、定期的にレビューする。
			5b-5.9.11	資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。 g) 情報及びその他の関連資産は、削除又は破棄する場合、セキュリティに配慮した方法で処理し、目録から削除する。	手引に関連記載あり	8.1.2.6	資産の管理責任者は、資産を消去又は破壊する場合に、適切に取り扱う仕組みを整備する。
			5b-5.9.11	資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。 h) 資産の管理責任者が、資産に関連するリスクの特定及びマネジメントに関与する。 i) 資産の管理責任者が、情報を管理する役割及び責任をもつ要員を支援する。	手引に関連記載あり	8.1.2.2	資産の管理責任者は、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。
5.9.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.10	情報及びその他の関連資産の許容される利用 統制目標：情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は、明確にし、文書化し、実施する。 目的：情報及びその他の関連資産を適切に保護し、利用し、取り扱うことを確実にするため。		5.10	情報及びその他の関連資産の許容される利用 管理策 情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は、明確にし、文書化し、実施する。 目的 情報及びその他の関連資産を適切に保護し、利用し、取り扱うことを確実にするため。		8.1.3	資産利用の許容範囲 情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施する。
						8.2.3	資産の取扱い 資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施する。
5.10.1	情報及びその他の関連資産の許容される利用に関する方針を策定する。	組織の情報及びその他の関連資産を利用する、又はそれらにアクセスする要員及び外部の利用者に対し、情報及びその他の関連資産を保護し、取り扱うための情報セキュリティ要求事項を認識させる。 要員及び外部の利用者は、どのような情報処理施設・設備の利用に対しても、責任をもつ。 組織は、情報及びその他の関連資産の許容される利用に関するトピック固有の方針を確立し、情報及びその他の関連資産を利用する又は取り扱う全ての人にそれを伝達する。 許容される利用に関するトピック固有の方針では、個人に期待する情報及びその他の関連資産の利用方法について、明確に指示をする。 トピック固有の方針には、次の事項を記載する。 a) 情報セキュリティの観点から見た、個人に期待する行動及び許容できない行動 b) 情報及びその他の関連資産について許可する利用及び禁止する利用 c) 組織が実行している監視活動	5b-5.10.1	組織の情報及びその他の関連資産を利用する、又はそれらにアクセスする要員及び外部の利用者に対し、情報及びその他の関連資産を保護し、取り扱うための情報セキュリティ要求事項を認識させる。	手引に関連記載あり	8.1.3.1	組織の資産を利用する又はアクセスできる従業員及び外部の利用者に対し、組織における情報や情報処理施設に関連する資産あるいは資源に関する情報セキュリティ要求事項について、認識させる。
			5b-5.10.2	要員及び外部の利用者は、どのような情報処理施設・設備の利用に対しても、責任をもつ。	手引に関連記載あり	8.1.3.2	従業員及び外部の利用者は、どのような情報処理資源の利用に対しても、また、利用者自身の責任の下で行ったいかなる利用に対しても、責任をもつ。
			5b-5.10.3	組織は、情報及びその他の関連資産の許容される利用に関するトピック固有の方針を確立し、情報及びその他の関連資産を利用する又は取り扱う全ての人にそれを伝達する。	手引に関連記載あり	–	（対応項なし）
			5b-5.10.4	許容される利用に関するトピック固有の方針では、個人に期待する情報及びその他の関連資産の利用方法について、明確に指示をする。	手引に関連記載あり	–	（対応項なし）
			5b-5.10.5	トピック固有の方針には、次の事項を記載する。 a) 情報セキュリティの観点から見た、個人に期待する行動及び許容できない行動 b) 情報及びその他の関連資産について許可する利用及び禁止する利用 c) 組織が実行している監視活動	手引に関連記載あり	–	（対応項なし）
5.10.2	情報及びその他の関連資産の許容される利用に関する規則及び取扱手順を整備し、実施する。	許容される利用の手順は、情報の分類（5.12参照）及び特定した汎欠に従って、情報のライフサイクル全体にわたって立案する。 許容される利用の手順の立案においては、次の項目を考慮する。 a) 分類のレベルに応じた保護の要求事項に対応するアクセス制限(5.12参照) b) 情報及びその他の関連資産の認可された利用者についての、記録の維持 c) 情報の一時的又は恒久的な複製についての、情報の原本の保護と整合性のあるレベルでの保護 d) 情報に関連する資産の、製造業者の仕様に従った保管（7.8参照） e) 記憶媒体（電子的又は物理的な）の全ての複製についての、認可された受領者の注意をひくような明確な表示（7.10参照） f) 情報及びその他の関連資産の破棄、並びにサポートされている削除方法の認可（8.10参照）	5b-5.10.6	許容される利用の手順は、情報の分類及び特定した汎欠に従って、情報のライフサイクル全体にわたって立案する。	手引に関連記載あり	8.2.3.1	情報を分類に従って取り扱い、処理し、保管し、伝達するための手順を作成する。
			5b-5.10.7	許容される利用の手順の立案においては、次の項目を考慮する。 a) 分類のレベルに応じた保護の要求事項に対応するアクセス制限	手引に関連記載あり	8.2.3.2	情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、各レベルの分類に応じた保護の要求事項に対応するアクセス制限に関する手順を含める。
			5b-5.10.7	許容される利用の手順の立案においては、次の項目を考慮する。 b) 情報及びその他の関連資産の認可された利用者についての、記録の維持	手引に関連記載あり	8.2.3.3	情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、資産の認可された受領者について、正式な記録を維持するための手順を含める。
			5b-5.10.7	許容される利用の手順の立案においては、次の項目を考慮する。 c) 情報の一時的又は恒久的な複製についての、情報の原本の保護と整合性のあるレベルでの保護	手引に関連記載あり	8.2.3.4	情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、情報の一時的又は恒久的な複製について、情報の原本と同等のレベルで保護するための手順を含める。
			5b-5.10.7	許容される利用の手順の立案においては、次の項目を考慮する。 d) 情報に関連する資産の、製造業者の仕様に従った保管	手引に関連記載あり	8.2.3.5	情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、IT 資産について、製造業者の仕様に従って保管するための手順を含める。
			5b-5.10.7	許容される利用の手順の立案においては、次の項目を考慮する。 e) 記憶媒体（電子的又は物理的な）の全ての複製についての、認可された受領者の注意をひくような明確な表示	手引に関連記載あり	8.2.3.6	情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、媒体の全ての複製について、認可された受領者の注意をひくように明確な印を付けるための手順を含める。
			5b-5.10.7	許容される利用の手順の立案においては、次の項目を考慮する。 f) 情報及びその他の関連資産の破棄、並びにサポートされている削除方法の認可（8.10参照）	手引に関連記載あり	–	（対応項なし）
5.11	資産の返却 統制目標：要員及び必要に応じてその他の利害関係者は、雇用、契約又は合意の変更又は終了時に、自らが所持する組織の資産の全てを返却する。 目的：雇用、契約、又は合意を変更又は終了するプロセスの一環として、組織の資産を保護するため。		5.11	資産の返却 管理策 要員及び必要に応じてその他の利害関係者は、雇用、契約又は合意の変更又は終了時に、自らが所持する組織の資産の全てを返却する。 目的 雇用、契約、又は合意を変更又は終了するプロセスの一環として、組織の資産を保護するため。		8.1.4	資産の返却 全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。
5.11.1	要員及びその他の利害関係者における雇用の変更及び終了において、前もって支給された全ての物理的及び電子的な資産の返却プロセスを整備し、実施する。	雇用の変更及び終了時のプロセスは、前もって支給された物理的及び電子的な資産（組織が所有するもの又は組織に預託されたもの）の全ての返却を含めて制定する。 要員及びその他の利害関係者が継続中の作業に重要な知識を保有している場合には、その情報を文書化し、組織に引き継ぐ。 要員及びその他の利害関係者が組織の装置・機器を購入する場合、又は個人所有の機器を用いる場合には、手順に従って、全ての関連する情報を追跡し、組織に返却し、装置・機器からセキュリティを保って削除することを確実にする（7.14参照）。 雇用の終了の予告期間中及びそれ以降、組織は、予告を受けた要員が認可を得ずに関連情報（例えば、知的財産）を複製することを防止する。 組織は、返却する全ての情報及びその他の関連資産を明確に特定し、文書化する。これには、次のものが含まれ得る。 a) エンドポイント機器 b) 可搬記憶装置 c) 専門機器 d) 情報システム、サイト及び物理的アーカイブ用の認証ハードウェア（例えば、機械式鍵、物理トークン及びスマートカード） e) 情報の物理的な複製	5b-5.11.1	雇用の変更及び終了時のプロセスは、前もって支給された物理的及び電子的な資産（組織が所有するもの又は組織に預託されたもの）の全ての返却を含めて制定する。	手引に関連記載あり	8.1.4.1	雇用の終了時の手続は、前もって支給された物理的及び電子的な資産（組織が管理責任をもつ又は組織に委託されたもの）の全ての返却を含める。
			5b-5.11.2	要員及びその他の利害関係者が組織の装置・機器を購入する場合、又は個人所有の機器を用いる場合には、手順に従って、全ての関連する情報を追跡し、組織に返却し、装置・機器からセキュリティを保って削除することを確実にする。	手引に関連記載あり	8.1.4.2	従業員及び外部の利用者が組織の設備を購入する場合、又は個人所有の設備を用いる場合には、手順に従って、全ての関連する情報を組織に返却し、設備からセキュリティを保って確実に消去する。
			5b-5.11.3	要員及びその他の利害関係者が継続中の作業に重要な知識を保有している場合には、その情報を文書化し、組織に引き継ぐ。	手引に関連記載あり	8.1.4.3	従業員及び外部の利用者が継続中の作業に重要な知識を保有している場合には、その情報を文書化し、組織に引き継ぐ。
			5b-5.11.4	雇用の終了の予告期間中及びそれ以降、組織は、予告を受けた要員が認可を得ずに関連情報を複製することを防止する。	手引に関連記載あり	8.1.4.4	雇用の終了の予告期間中は、雇用が終了する従業員及び契約相手が認可を得ずに関連情報（例えば、知的財産）を複製、削除することのないよう、組織が管理する。
			5b-5.11.5	組織は、返却する全ての情報及びその他の関連資産を明確に特定し、文書化する。	手引に関連記載あり	–	（対応項なし）
			（5b-5.11.5参考）	これには、次のものが含まれ得る。 a)顧用者エンドポイント機器 b)可搬記憶装置 c)専門機器 d)情報システム、サイト及び物理的アーカイブ用の認証ハードウェア e)情報の物理的な複製	手引に関連記載あり	–	（対応項なし）
5.12	情報の分類 統制目標：情報は、機密性、完全性、可用性及び関連する利害関係者の要求事項に基づく組織の情報セキュリティのニーズに従って分類する。 目的：組織における情報の重要度に従って、情報の保護のニーズを特定し、理解することを確実にするため。		5.12	情報の分類 管理策 組織は、情報の分類に関するトピック固有の方針を確立し、それを全ての関連する利害関係者に伝達する。 目的 組織における情報の重要度に従って、情報の保護のニーズを特定し、理解することを確実にするため。		8.2	情報分類 管理目的：組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。
						8.2.1	情報の分類 情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類する。
5.12.1	情報の分類や分類体系に関する方針を策定し、分類する。	組織は、情報の分類に関するトピック固有の方針を確立し、それを全ての関連する利害関係者に伝達する。 組織は、分類体系において、機密性、完全性及び可用性の要求事項を考慮する。 情報の分類及び関連する保護管理策では、情報を共有又は制限するため、情報の完全性を保護するため、及び可用性を保証するための事業上のニーズ、並びに情報の機密性、完全性及び可用性に関する法的要求事項を考慮する。情報以外の資産も、その資産に保管する情報、その資産で処理する情報、又は他の形で取り扱う若しくは保護する情報の分類に合わせて分類することが可能である。 情報の管理責任者は、その情報の分類に対してアカウンタビリティを負う。 分類体系には、分類の規則及びその分類を後にレビューするための基準を含める。 分類の結果は、ライフサイクルを通じた情報の価値、取扱いに慎重を要する度合い、及び重要度の変化に従って更新する。 分類は、情報の侵害が組織に与える影響のレベルによって決定することが可能である。分類体系で定義したそれぞれのレベルには、分類体系の適用において意味をもつ名称を付ける。 分類体系は、全員が情報及び扱当するその他の関連資産を同じ方法で分類できるよう、組織全体にわたって一貫し、組織の手順に含まれている。これによって、全員が保護に関する要求事項について共通した理解をもち、適切な保護を適用できるようになる。 情報共有を含む他の組織との合意は、他の組織から共有された情報の分類を特定し、分類レベルを解釈するための手順を含む。組織内で使用する分類体系は、レベルの名称が類似している場合でも、他の組織で使用する体系と異なる可能性がある。さらに、組織間で移動する情報は、分類体系が同じであっても、各組織の状況に依存して分類が異なる場合がある。異なる体系間の対応は、情報について同等の取扱い及び保護方法を探すことによって決定することが可能である。	5b-5.12.1	組織は、情報の分類に関するトピック固有の方針を確立し、それを全ての関連する利害関係者に伝達する。	手引に関連記載あり	–	（対応項なし）
			5b-5.12.2	組織は、分類体系において、機密性、完全性及び可用性の要求事項を考慮する。	手引に関連記載あり	8.2.1.4	情報の分類体系における保護レベルは、対象とする情報についての機密性、完全性、可用性及びその他の特性を分析することによって評価する。
			5b-5.12.3	情報の分類及び関連する保護管理策では、情報を共有又は制限するため、情報の完全性を保護するため、及び可用性を保証するための事業上のニーズ、並びに情報の機密性、完全性及び可用性に関する法的要求事項を考慮する。	手引に関連記載あり	8.2.1.1	情報の分類及び関連する保護管理策には、情報を共有又は制限する業務上の要求、及び法的要求事項を含める。
			5b-5.12.4	情報の管理責任者は、その情報の分類に対してアカウンタビリティを負う。	手引に関連記載あり	8.2.1.2	情報資産の管理責任者は、その情報の分類に対して責任を負う。
			5b-5.12.5	分類体系には、分類の規則及びその分類を後にレビューするための基準を含める。	手引に関連記載あり	8.2.1.3	情報の分類体系には、分類の規則及びその分類を時間が経ってからレビューするための基準を含める。
			5b-5.12.7	分類体系は、アクセス制御に関するトピック固有の方針と整合していて、組織のそれぞれの事業上のニーズに対応できる。	手引に関連記載あり	8.2.1.5	情報の分類体系は、アクセス制御方針と整合させる。
			5b-5.12.8	分類は、情報の侵害が組織に与える影響のレベルによって決定することが可能である。分類体系で定義したそれぞれのレベルには、分類体系の適用において意味をもつ名称を付ける。	手引に関連記載あり	8.2.1.6	情報の分類体系におけるそれぞれの保護レベルには、分類体系の適用において意味をなすような名称を付ける。
			5b-5.12.9	分類体系は、全員が情報及び扱当するその他の関連資産を同じ方法で分類できるよう、組織全体にわたって一貫し、組織の手順に含まれている。	手引に関連記載あり	8.2.1.8	情報の分類は、組織の プロセスに含め、組織全体にわたって一貫した論理的なものとする。
			（5b-5.12.9参考）	これによって、全員が保護に関する要求事項について共通した理解をもち、適切な保護を適用できるようになる。	手引に関連記載あり	8.2.1.7	情報の分類体系は、組織全体にわたって一貫させ、全員が情報及び関連する資産を同じ方法で分類 し、保護に関する要求事項について共通した理解をもち、適切な保護を適用できるようにする。
			5b-5.12.10	情報共有を含む他の組織との合意は、他の組織から共有された情報の分類を特定し、分類レベルを解釈するための手順を含む。	手引に関連記載あり	8.2.3.7	他組織との情報共有を含む合意には、その情報の分類を特定し、他組織からの又は他組織への分類ラベル及びアクセス制限の解釈を伝達するための手順並びにその解釈を支援する手順を含める。
5.12.2	分類の結果は、ライフサイクルを通じた情報の価値、取扱いに慎重を要する度合い、及び重要度の変化に従って分類の決定者や責任者に確認し、定期的に見直し更新する。	特になし。	5b-5.12.6	分類の結果は、ライフサイクルを通じた情報の価値、取扱いに慎重を要する度合い、及び重要度の変化に従って更新する。	管理策に関連記載あり	8.2.1.10	情報の分類の結果は、ライフサイクルを通じた、情報の価値、取扱いに慎重を要する度合い及び重要性の変化に応じて、更新する。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.13	情報のラベル付け 統制目標：情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施する。 目的：情報の分類の伝達を容易にし、情報の処理及び管理の自動化を支援するため。		5.13	情報のラベル付け 管理策 情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施する。 目的 情報の分類の伝達を容易にし、情報の処理及び管理の自動化を支援するため。		8.2.2	情報のラベル付け 情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施する。
5.13.1	情報の分類体系を反映した情報のラベル付けに関する手順を整備し、ラベル付けを実施する。	情報のラベル付けに関する手順は、あらゆる形式の情報及びその他の関連資産に適用できるものである。ラベル付けは、5.12で確立した分類体系を反映している。 ラベルは、容易に認識できる。 情報のラベル付けに関する手順では、記憶媒体の種類に応じて、情報がどのようにアクセスされるか又は資産がどのように取り扱われるかを考慮して、ラベルを添付する場所及びその添付方法に関する手引を示す。手順では、次の事項を定めることも可能である。 a) ラベル付けを省略する場合（例えば、作業負荷を減らすため、秘密でない情報のラベル付け） b) 電子的若しくは物理的手段、又はその他の形式で送信又は保存される情報のラベル付けの方法 c) ラベル付けが不可能な場合（例えば、技術的制約のため）の取扱いの方法 ラベル付け手法の例は次のものを含む。 a) 物理的ラベル b) ヘッダ及びフッタ c) メタデータ d) 透かし e) ゴムスタンプ デジタル情報は、特に機密性に関して、情報を特定し、管理し、制御するために、メタデータを活用する。メタデータは、情報の効率的かつ正確な検索を可能にする。メタデータは、付加した分類ラベルに基づいて、複数のシステムが連携し、決定を下すことを容易にする。 手順には、組織の情報モデル及びITアーキテクチャに沿って、情報にメタデータをどのように付けるか、どのラベルを使用するか、及びデータをどのように取り扱うことが望ましいかを記載する。 システムが情報をその情報セキュリティ特性に応じて処理するときに、関係する追加のメタデータをシステムで付加する。 要員及びその他の利害関係者に、ラベル付けに関する手順を認識させる。情報に正しくラベルを付け、それに応じて取り扱うことを確実にするために、全ての要員に必要な訓練を提供する。	5b-5.13.1	情報のラベル付けに関する手順は、あらゆる形式の情報及びその他の関連資産に適用できるものである。	手引に関連記載あり	8.2.2.1	情報のラベル付けに関する手順は、物理的形式及び電子的形式の情報及び関連する資産に適用できるようにする。
			5b-5.13.2	情報のラベル付けは、5.12で確立した分類体系を反映している。	手引に関連記載あり	8.2.2.2	情報のラベル付けは、8.2.1 で確立した分類体系を反映する。
			5b-5.13.3	情報のラベルは、容易に認識できる。	手引に関連記載あり	8.2.2.3	情報のラベルは、容易に認識できるようにする。
			5b-5.13.4	情報のラベル付けに関する手順では、記憶媒体の種類に応じて、情報がどのようにアクセスされるか又は資産がどのように取り扱われるかを考慮して、ラベルを添付する場所及びその添付方法に関する手引を示す。	手引に関連記載あり	8.2.2.4	情報のラベル付けに関する手順では、媒体の種類に応じて、情報がどのようにアクセスされるか又は資産がどのように取り扱われるかを考慮して、ラベルを添付する場所及びその添付方法に関する手引 を示す。
			（5b-5.13参考1）	手順では、次の事項を定めることも可能である。 a) ラベル付けを省略する場合 b) 電子的若しくは物理的手段、又はその他の形式で送信又は保存される情報のラベル付けの方法 c) ラベル付けが不可能な場合の取扱いの方法	手引に関連記載あり	–	（対応項なし）
			（5b-5.13参考2）	ラベル付け手法の例は次のものを含む。 a) 物理的ラベル b) ヘッダ及びフッタ c) メタデータ d) 透かし e) ゴムスタンプ	手引に関連記載あり	–	（対応項なし）
			5b-5.13.5	ディジタル情報は、特に機密性に関して、情報を特定し、管理し、制御するために、メタデータを活用する。	手引に関連記載あり	–	（対応項なし）
			5b-5.13.6	メタデータは、情報の効率的かつ正確な検索を可能にする。	手引に関連記載あり	–	（対応項なし）
			5b-5.13.7	メタデータは、付加した分類ラベルに基づいて、複数のシステムが連携し、決定を下すことを容易にする。	手引に関連記載あり	–	（対応項なし）
			5b-5.13.8	手順には、組織の情報モデル及びITアーキテクチャに沿って、情報にメタデータをどのように付けるか、どのラベルを使用するか、及びデータをどのように取り扱うことが望ましいかを記載する。	手引に関連記載あり	–	（対応項なし）
			5b-5.13.9	システムが情報をその情報セキュリティ特性に応じて処理するときに、関係する追加のメタデータをシステムで付加する。	手引に関連記載あり	–	（対応項なし）
			5b-5.13.10	要員及びその他の利害関係者に、ラベル付けに関する手順を認識させる。	手引に関連記載あり	8.2.2.5	従業員及び契約相手に、情報のラベル付けに関する手順を認識させる。
			5b-5.13.11	情報に正しくラベルを付け、それに応じて取り扱うことを確実にするために、全ての要員に必要な訓練を提供する。	手引に関連記載あり	–	（対応項なし）
			5b-5.13.12	取扱いに慎重を要する又は重要と分類される情報を含むシステム出力には、適切な分類ラベルを付ける。	手引に関連記載あり	8.2.2.6	取扱いに慎重を要する又は重要と分類される情報を含むシステム出力には、適切な分類ラベルを付ける。
5.13.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.14	情報の転送 統制目標：情報の転送の規則、手順又は合意を、組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備える。 目的：組織内及び外部の利害関係者との間で転送される情報のセキュリティを維持するため。		5.14	情報の転送 管理策 情報の転送の規則、手順又は合意を、組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備える。 目的 組織内及び外部の利害関係者との間で転送される情報のセキュリティを維持するため。		13.2	情報の転送 管理目的：組織の内部及び外部に転送した情報のセキュリティを維持するため。
						13.2.1	情報の転送 あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備える。
						13.2.2	情報転送に関する合意 合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱う。
						13.2.3	電子的メッセージ通信 電子的メッセージ通信に含まれた情報は、適切に保護する。
5.14.1	転送中の情報を保護するための方針を策定する。	組織は、情報の転送に関するトピック固有の方針を確立し、それを関連する全ての関係者に伝達する。 転送中の情報を保護するための規則、手順及び合意は、関連する情報の分類を反映する。 組織と第三者との間で情報を転送する場合、転送中の全ての形式の情報を保護するために、転送の合意（受信者の認証を含む。）を確立し、維持する（5.10参照）。 情報の転送は、電子的転送、物理的記憶媒体の輸送及び口頭での伝達によって行われる場合がある。 情報の口頭での伝達を保護するために、要員及びその他の利害関係者に対して、次の事項を行うことが望ましいことを留意させる。 a) 公共の場所又は安全でない通信チャネルを通じた口頭での秘密会話は、認可されていない者に聞かれる可能性があるので行わない。 b) 秘密情報を含んだメッセージを留守番電話又は音声メッセージに残さない。留守番電話又は音声メッセージに残したメッセージは、認可されていない者が再生する可能性、共有システムに保管される可能性又は誤ダイアルの結果、間違って保管される可能性があるからである。 c) 取扱いに慎重を要する会話においては、始めに注意事項を説明し、出席者に、これから伝える情報の分類レベル及び取扱いの要求事項を知らせる。	5b-5.14.1	組織は、情報の転送に関するトピック固有の方針を確立し、それを関連する全ての関係者に伝達する。	手引に関連記載あり	13.2.2.12	情報転送に関する合意においては、転送中の情報及び物理的媒体を保護するための方針、手順及び標準類を確立及び維持し、参照する。
			5b-5.14.2	転送中の情報を保護するための規則、手順及び合意は、関連する情報の分類を反映する。	手引に関連記載あり	–	（対応項なし）
			5b-5.14.3	組織と第三者との間で情報を転送する場合、転送中の全ての形式の情報を保護するために、転送の合意（受信者の認証を含む。）を確立し、維持する。	手引に関連記載あり	13.2.2.1	情報転送に関する合意に、送信、発送及び受領についての管理及び通知を行う責任を含める。
			5b-5.14.7	情報の口頭での伝達を保護するために、要員及びその他の利害関係者に対して、次の事項を行うことが望ましいことを留意させる。 a) 公共の場所又は安全でない通信チャネルを通じた口頭での秘密会話は、認可されていない者に聞かれる可能性があるので行わない。 c) 会話を開く際は、適切なレベルで音を遮断する。 d) 適切な部屋の管理策が実施されることを確実にする（例えば、防音、ドアを閉める。）。 e) 取扱いに慎重を要する会話においては、始めに注意事項を説明し、出席者に、これから伝える情報の分類レベル及び取扱いの要求事項を知らせる。	手引に関連記載あり	13.2.1.12	公共の場所、並びにセキュリティが確保されていない通信経路、出入りが自由なオフィス及び会議室では、秘密の会話はしないほうがよいことを要員に意識させる。
			5b-5.14.7	情報の口頭での伝達を保護するために、要員及びその他の利害関係者に対して、次の事項を行うことが望ましいことを留意させる。 b) 秘密情報を含んだメッセージを留守番電話又は音声メッセージに残さない。留守番電話又は音声メッセージに残したメッセージは、認可されていない者が再生する可能性、共有システムに保管される可能性、又は誤ダイアルの結果、間違って保管される可能性があるからである。	手引に関連記載あり	13.2.1.10	情報転送のために通信設備を利用するときに従う手順及び管理策には、留守番電話に残したメッセージの、認可されていない者による再生、共有システムに保管、又は誤ダイアルによる間違った先へ保管されることを防止するため、秘密情報を含んだメッセージを留守番電話に残さないことを含める。
5.14.2	全ての種類の情報の転送について、規則又は手順を整備する。	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 a) 転送する情報を、盗聴、認可されていないアクセス、複製、改ざん、誤った経路での通信、破壊及びサービス拒否から保護するために設計された管理策。これは、情報の分類に合ったそれぞれのレベルのアクセス制御、及び暗号技術の利用（8.24参照）など取扱いに慎重を要する情報を保護するために必要な管理策を含む。 b) 転送中の情報の受理記録を維持すること を含む、追跡可能性及び否認防止を確実にするための管理策 c) 該当する場合には、情報の管理責任者、リスク所有者、セキュリティ担当者及び情報管理者など、転送に関連する適切な連絡先の特定 d) 物理的記憶媒体の紛失又はデータの消失などの情報セキュリティインシデントが発生した場合の責任及び賠償義務 e) 取扱いに慎重を要する又は重要な情報に対する、合意したラベル付けシステム（ラベルの意味を適当に理解できること、及び情報を適切に保護することを確実にするもの）の使用 f) 転送サービスの信頼性及び可用性 g) 情報転送手段の許容される利用に関するトピック固有の方針又は指針（5.10参照） h) メッセージを含む全ての業務記録の保持及び破棄の指針 注記 業務記録の保持及び破棄に関しては、地域の法令及び規制が存在する場合がある。 i) 情報の転送に関連するその他の関連する法令、規制及び契約上の要求事項（5.31、5.32、5.33、5.34参照）の考慮（例えば、電子署名の要求事項） 合意については5.20.1供給者との合意にて、「物理的輸送又は論理的送信中に情報を保護するための情報の転送の管理策」が存在することから、本管理策においては「規則、手順」を対象とする。	5b-5.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 a) 転送する情報を、盗聴、認可されていないアクセス、複製、改ざん、誤った経路での通信、破壊及びサービス拒否から保護するために設計された管理策。これは、情報の分類に合ったそれぞれのレベルのアクセス制御、及び暗号技術の利用など取扱いに慎重を要する情報を保護するために必要な管理策を含む。	手引に関連記載あり	13.2.1.1	情報転送のために通信設備を利用するときに従う手順及び管理策には、転送する情報を、盗聴、複製、改ざん、誤った経路での通信及び破壊から保護するために設計された手順を反映する。
					手引に関連記載あり	13.2.1.6	情報転送のために通信設備を利用するときに従う手順及び管理策には、暗号技術の利用（例えば、情報の機密性、完全性及び真正性を保護するための暗号の利用）を含める。
					手引に関連記載あり	13.2.2.11	情報転送に関する合意に、容認できるアクセス制御のレベルを含める。
					手引に関連記載あり	13.2.2.13	情報交換に関する、いかなる合意における情報セキュリティの事項も、関連する業務情報の取扱いに慎重を要する度合いを反映する。
					手引に関連記載あり	13.2.3.1	電子的メッセージ通信のための情報セキュリティでは、組織が採用している分類体系に従った、認可されていないアクセス、改ざん又はサービス妨害からのメッセージを保護する。
			5b-5.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 b) 転送中の情報の受理記録を維持することを含む、追跡可能性及び否認防止を確実にするための管理策	手引に関連記載あり	13.2.2.2	情報転送に関する合意に、追跡可能性及び否認防止を確実にするための手順を含める。
			5b-5.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 d) 物理的記憶媒体の紛失又はデータの消失などの情報セキュリティインシデントが発生した場合の責任及び賠償義務	手引に関連記載あり	13.2.2.6	情報転送に関する合意に、情報セキュリティインシデントが発生した場合（例えば、データの紛失）の責任及び賠償義務を含める。
			5b-5.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 e) 取扱いに慎重を要する又は重要な情報に対する、合意したラベル付けシステム（ラベルの意味を適当に理解できること、及び情報を適切に保護することを確実にするもの）の使用	手引に関連記載あり	13.2.2.7	情報転送に関する合意に、取扱いに慎重を要する又は重要な情報に対する、合意されたラベル付けシステム（ラベルの意味を適当に理解すること、及び情報を適切に保護することを確実にするもの）の使用を含める。
			5b-5.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 f) 転送サービスの信頼性及び可用性	手引に関連記載あり	13.2.3.3	電子的メッセージ通信のための情報セキュリティでは、サービスの信頼性及び可用性を確保する。
			5b-5.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 g) 情報転送手段の許容される利用に関するトピック固有の方針又は指針	手引に関連記載あり	13.2.1.4	情報転送のために通信設備を利用するときに従う手順及び管理策には、通信設備の許容できる利用（物理的な扱いを含む。）について規定した方針又は指針を反映する。
			5b-5.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 i) 情報の転送に関連するその他の関連する法令、規制及び契約上の要求事項の考慮	手引に関連記載あり	13.2.1.7	情報転送のために通信設備を利用するときに従う手順及び管理策には、関連する国及び地域の法令及び規制に従った、全ての業務通信文（メッセージを含む）の保持及び処分に関する指針を反映する。
					手引に関連記載あり	13.2.1.13	情報転送サービスは、関連するいかなる法的要求事項についても順守する。
					手引に関連記載あり	13.2.3.4	電子的メッセージ通信のための情報セキュリティでは、法的考慮（例えば、電子署名のための要求事項）を含める。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.14.3	電子通信手段の使用について、規則又は手順を整備する。	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 a) 電子通信の利用を通じて伝送される可能性のあるマルウェアの検知及びそれに対する保護（8.7参照） b) 添付して通信する、取扱いに慎重を要する電子情報の保護 c) 通信において文書及びメッセージを誤った宛先又は番号に送信することの防止 d) 誰でも使える外部サービス（例えば、インスタントメッセージ、ソーシャルネットワーク、ファイル共有又はクラウドストレージ）を利用する際の、事前承認の取得 e) 公開されているアクセス可能なネットワークを通じて情報を転送するときの、より強固な認証レベル f) 電子通信手段に関連する制限（例えば、外部のメールアドレスへの電子メールの自動転送の防止） g) ショートメッセージサービス（SMS）又はインスタントメッセージで重要な情報を送信しないように要員及びその他の利害関係者に助言する。これは、これら(が)公共の場所で（したがって、認可されていない人に）読まれたり、又は適切に保護されていない装置・機器に保存されたりする可能性があるためである。 h) ファクシミリ又はそのサービスの利用に伴う、次の問題に関わる要員及びその他の利害関係者への助言 1) 組み込まれている記憶装置から受信文を取り出す、認可されていないアクセス 2) 特定の番号にメッセージを送る故意又は偶然のプログラミング 合意については5.20.1供給者との合意にて、「物理的輸送又は論理的送信中に情報を保護するための情報の転送の管理策」が存在することから、本管理策においては「規則、手順」を対象とする。	5b-5.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 a) 電子通信の利用を通じて伝送される可能性のあるマルウェアの検知及びそれに対する保護	手引に関連記載あり	13.2.1.2	情報転送のために通信設備を利用するときに従う手順及び管理策には、電子的メッセージ通信を通じて伝送される可能性のあるマルウェアを検出し、これらから保護するための手順を反映する。
			5b-5.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 b) 添付して通信する、取扱いに慎重を要する電子情報の保護	手引に関連記載あり	13.2.1.3	情報転送のために通信設備を利用するときに従う手順及び管理策には、添付形式として通信される、取扱いに慎重を要する電子情報の保護に関する手順を反映する。
			5b-5.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 c) 通信において文書及びメッセージを誤った宛先又は番号に送信することの防止	手引に関連記載あり	13.2.3.2	電子的メッセージ通信のための情報セキュリティでは、正しい送付先及びメッセージ送信を確実にする仕組みを整備する。
			5b-5.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 d) 誰でも使える外部サービスを利用する際の、事前承認の取得	手引に関連記載あり	13.2.3.5	電子的メッセージ通信のための情報セキュリティでは、誰でも使える外部サービス（例えば、インスタントメッセージ、ソーシャルネットワーク、ファイル共有）を利用する際の、事前承認を取得する。
			5b-5.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 e) 公開されているアクセス可能なネットワークを通じて情報を転送するときの、より強固な認証レベル	手引に関連記載あり	13.2.3.6	電子的メッセージ通信のための情報セキュリティでは、公開されているネットワークからのアクセスを制御する、より強固な認証レベルを決定する。
			5b-5.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 f) 電子通信手段に関連する制限	手引に関連記載あり	13.2.1.8	情報転送のために通信設備を利用するときに従う手順及び管理策には、通信設備の利用（例えば、外部のメールアドレスへの電子メールの自動転送）に関する管理策及び制限を反映する。
			5b-5.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 g) ショートメッセージサービス（SMS）又はインスタントメッセージで重要な情報を送信しないように要員及びその他の利害関係者に助言する。これは、これら(が)公共の場所で（したがって、認可されていない人に）読まれたり、又は適切に保護されていない装置・機器に保存されたりする可能性があるためである。	手引に関連記載あり	13.2.1.9	情報転送のために通信設備を利用するときに従う手順及び管理策には、秘密情報を漏えいしないように適切な予防策を講じることの、要員への助言を含める 。
			5b-5.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 h) ファクシミリ又はそのサービスの利用に伴う、次の問題に関わる要員及びその他の利害関係者への助言 1) 組み込まれている記憶装置から受信文を取り出す、認可されていないアクセス 2) 特定の番号にメッセージを送る故意又は偶然のプログラミング	手引に関連記載あり	13.2.1.11	情報転送のために通信設備を利用するときに従う手順及び管理策には、ファクシミリ又はそのサービスの利用に伴う問題（ファクシミリ)の受信文の取出し、検査への認可されていないアクセス、特定の番号にメッセージを送る故意又は偶然のプログラミング、誤ダイアル、又は間違って記憶した番号を用いることによる、誤った番号への文書及びメッセージの送付）について要員に意識させることを含める。
5.14.4	物理的記憶媒体の輸送について、規則又は手順を整備する。	物理的記憶媒体（紙を含む。）を輸送する場合、規則、手順及び合意には、次の事項も含める。 a) 輸送、受渡し及び受領を管理し、通知する責任 b) 伝票の正しい送付先及び送付を確実にすること c) 輸送中に発生する可能性が高い物理的損傷から、製造業者の仕様に従って内容物を保護すること（梱）包し、例えば、熱、湿気又は電磁界への露出など、記録媒体の再生を妨げる可能性のある環境要因からの保護。こん（梱）包及び送付のための最小限の技術標準の使用（例えば、不透明な封筒の使用）。 d) 管理簿が合意した、認可された信頼できる運送業者のリスト e) 運送業者を確認する規準 f) 輸送する記憶媒体内の情報の分散レベルに応じて、開封を明らかにする又は開封を防止する管理策（例えば、パック、コンテナ）の使用 g) 運送業者の識別情報を検証する手順 h) 情報の分散に応じた、輸送又は運送業者のサービスを提供する第三者の承認された一覧 i) 記憶媒体の内容及び適用した保護方法を特定するためのログを保持し、認可された受領者のリスト、輸送の責任窓口への発送時刻、及び宛先での受領時刻を記録する 合意については5.20.1供給者との合意にて、「物理的輸送又は論理的送信中に情報を保護するための情報の転送の管理策」が存在することから、本管理策においては「規則、手順」を対象とする。	5b-5.14.6	物理的記憶媒体（紙を含む。）を輸送する場合、規則、手順及び合意には、次の事項も含める。 c) 輸送中に発生する可能性が高い物理的損傷から、製造業者の仕様に従って内容物を保護すること（梱）包。例えば、熱、湿気又は電磁界への露出など、記録媒体の再生を妨げる可能性のある環境要因からの保護。こん（梱）包及び送付のための最小限の技術標準の使用。	手引に関連記載あり	13.2.2.3	情報転送に関する合意に、こん（梱）包及び送信に関する必要最小限の技術標準を含める。
					手引に関連記載あり	8.3.3.4	輸送される情報を格納した媒体を保護するために、輸送途中に生じるかもしれない物理的損傷から内容を保護（例えば、媒体の復旧効果を低減させる場合のある、熱、湿気又は電磁気にさらすといった環境要因からの保護）するために、こん（梱）包を十分な強度とし、また、製造業者の仕様にも従う。
			5b-5.14.6	物理的記憶媒体（紙を含む。）を輸送する場合、規則、手順及び合意には、次の事項も含める。 d) 管理簿が合意した、認可された信頼できる運送業者のリスト	手引に関連記載あり	8.3.3.1	輸送される情報を格納した媒体を保護するために、信頼できる輸送機関又は運送業者を用いる。
					手引に関連記載あり	8.3.3.2	輸送される情報を格納した媒体を保護するために、認可された運送業者の一覧について、管理者の合意を得る。
			5b-5.14.6	物理的記憶媒体（紙を含む。）を輸送する場合、規則、手順及び合意には、次の事項も含める。 e) 運送業者を確認する規準	手引に関連記載あり	8.3.3.3	輸送される情報を格納した媒体を保護するために、運送業者を確認する手順を導入する。
					手引に関連記載あり	13.2.2.5	情報転送に関する合意に、運送業者を確認する規準を含める。
			5b-5.14.6	物理的記憶媒体（紙を含む。）を輸送する場合、規則、手順及び合意には、次の事項も含める。 i) 記憶媒体の内容及び適用した保護方法を特定するためのログを保持し。認可された受領者のリスト、輸送の責任窓口への発送時刻、及び宛先での受領時刻を記録すること	手引に関連記載あり	8.3.3.5	輸送される情報を格納した媒体を保護するために、媒体の内容、適用された保護、並びに輸送の責任窓口への受渡時刻及び目的地での受取(時刻)の記録を特定するログを保持する。
5.14.5	電子メールサービスをクラウドサービス利用者に対して提供する場合、電子メールによる電子的メッセージ通信において、クラウドサービス利用者がSPF、DKIMのいずれかまたは両方による送信ドメイン認証技術の対策及び、DMARCによる送信側の対策を実施できるための機能又は利用者が設定するための情報を提供する。	クラウドサービス事業者は、電子メールによる電子的メッセージ通信において、クラウドサービス利用者がSPF、DKIMのいずれかまたは両方による送信ドメイン認証技術の対策及びDMARCによる送信側の対策を実施できるための機能又は利用者が設定するための情報を提供する。 a) SPF（sender policy Framework） b) DKIM（DomainKyes Identified Mail） c) DMARC（Domain-based Message Authentication Reporting and Conformance）	–	（統一基準由来）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	13.2.3.7.P	クラウドサービス事業者は、電子メールによる電子的メッセージ通信において、クラウドサービス利用者がSPF、DKIMのいずれかまたは両方による送信ドメイン認証技術の対策及び、DMARCによる送信側の対策を実施できるための機能又は利用者が設定するための情報を提供する。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.15	アクセス制御 統制目標：情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を、事業上及び情報セキュリティの要求事項に基づいて確立し、実施する。 目的：情報及びその他の関連資産への認可されたアクセスを行わせ、認可されていないアクセスを防ぐことを確実にするため。		5.15	アクセス制御 管理策 情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を、事業上及び情報セキュリティの要求事項に基づいて確立し、実施する。 目的 情報及びその他の関連資産への認可されたアクセスを行わせ、認可されていないアクセスを防ぐことを確実にするため。		9.1	アクセス制御に対する業務上の要求事項 管理目的：情報及び情報処理施設へのアクセスを制限するため。
						9.1.1	アクセス制御方針 アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビュー する。
						9.1.2	ネットワーク及びネットワークサービスへのアクセス 利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供する。
5.15.1	アクセス制御に関連する情報セキュリティ及び事業上の要求事項を踏まえたアクセス制御に関する方針及び規則を策定し、実施する。	情報及びその他の関連資産の管理責任者は、アクセス制御に関連する情報セキュリティ及び事業上の要求事項を決定する。 情報セキュリティ及び事業上の要求事項を考慮したアクセス制御に関する方針を定め、関連する全ての利害関係者に伝達する。 アクセス制御に関する方針では以下を含める a) ロのエンティティ、情報及びその他の関連資産にどの種類のアクセスを必要とするかの決定 b) アプリケーションセキュリティ（8.26参照） c) 物理的アクセス。これは適切な物理的入退管理策（7.2、7.3及び7.4参照）によって支援する必要がある。 d) 情報の配布及び認可（例えば、知る必要性の原則）、並びに情報のセキュリティ水準及び情報の分類（5.10、5.12及び5.13参照） e) 特権的アクセスの制限（8.2参照） f) 職務の分離（5.3参照） g) データ又はサービスへのアクセスの制限に関連する法令、規制及び契約上の義務（5.31、5.32、5.33、5.34及び6.3参照） h) アクセス制御機能の分離（例えば、アクセス要求、アクセス認可、アクセス管理） i) アクセス要求の正式な認可（5.16及び5.18参照） j) アクセス権の管理（5.18参照） k) ログ取得（8.15参照） アクセス制御規則は、関連するエンティティに対して、適切なアクセス権及び制限を定義し、対応付けすることによって実施する（5.16参照）。エンティティは、人間の利用者だけでなく、技術的又は論理的なケイテム（例えば、機械、装置・機器又はサービス）の場合がある。アクセス制御の管理を簡潔にするために、役割をエンティティのグループ化割り当てることが可能である。 アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。 a) アクセス権と情報分類との整合性 b) アクセス権と物理的境界のセキュリティのニーズ及び要求事項との整合性 c) エンティティに、使用が認められているネットワーク及びネットワークサービスを含む、情報及びその他の関連資産へのアクセスだけを提供するために、分散環境で利用可能な全ての種類の接続を考慮すること d) 動的アクセス制御に関連する要素又は要因をどのように反映できるかを検討すること。	5c-S.15.1	情報及びその他の関連資産の管理責任者には、アクセス制御に関連する情報セキュリティ及び事業上の要求事項を決定する。	手引に関連記載あり	9.1.1.1	資産の管理責任者は、資産に対する利用者のそれぞれの役割に対して、適切なアクセス制御規則、アクセス権及び制限を、アセットに伴う情報セキュリティリスクを反映した制御の詳細及び厳密さで決定し、利用者の認証を要求しないシステム及びサービスは認証を要求しない根拠と共に文書化する。
			5c-S.15.2	情報セキュリティ及び事業上の要求事項を考慮したアクセス制御に関するトピック固有の方針を定め、関連する全ての利害関係者に伝達する。	手引に関連記載あり	9.1.1.3	利用者及びクラウドサービス事業者には、アクセス制御によって達成する業務上の要求事項を明確に規定して提供する。
					手引に関連記載あり	9.1.2.1	ネットワーク及びネットワークサービスの利用に関し、方針を設定する。
			5c-S.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 b) アプリケーションセキュリティ	手引に関連記載あり	9.1.1.4	アクセス制御方針に、業務用アプリケーションのセキュリティ要求事項を反映する。
			5c-S.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 d) 情報の配布及び認可、並びに情報のセキュリティ水準及び情報の分類	手引に関連記載あり	9.1.1.5	アクセス制御方針には、情報の伝達及び認可に対する方針（例えば、知る必要性の原則、情報のセキュリティ水準、情報の分類）を含める。
			5c-S.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 e) 特権的アクセスの制限	手引に関連記載あり	9.1.1.14	アクセス制御方針に、特権的アクセスを認められた役割を含める。
			5c-S.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 g) データ又はサービスへのアクセスの制限に関連する法令、規制及び契約上の義務	手引に関連記載あり	9.1.1.7	アクセス制御方針には、データ又はサービスへのアクセスの制限に関連する法令及び契約上の義務を反映する。
			5c-S.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 h) アクセス制御機能の分離	手引に関連記載あり	9.1.1.9	アクセス制御方針に、アクセス制御における役割の分離（例えば、アクセス要求、アクセス認可、アクセス管理）の方針を含める。
			5c-S.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 i) アクセス要求の正式な認可	手引に関連記載あり	9.1.1.10	アクセス制御方針に、アクセス要求の正式な認可に対する要求事項を含める。
			5c-S.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 j) アクセス権の管理	手引に関連記載あり	9.1.1.12	アクセス制御方針に、アクセス権の削除の方針を含める。
			5c-S.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 k) ログ取得	手引に関連記載あり	9.1.1.13	アクセス制御方針に、利用者の識別情報及び秘密認証情報の利用及び管理に関する、全ての重要な事象の記録の保管を含める。
			5c-S.15.5	アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。 a) アクセス権と情報分類との整合性	手引に関連記載あり	9.1.1.6	アクセス制御方針は、システム及びネットワークにおける、アクセス権と情報分類の方針との整合性を考慮して定める。
			5c-S.15.5	アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。 b) アクセス権と物理的境界のセキュリティのニーズ及び要求事項との整合性	手引に関連記載あり	9.1.1.2	アクセス制御は、論理的アクセス制御と物理的アクセス制御の両面を考慮して決定する。
			5c-S.15.5	アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。 c) エンティティに、使用が認められているネットワーク及びネットワークサービスを含む、情報及びその他の関連資産へのアクセスだけを提供するために、分散環境で利用可能な全ての種類の接続を考慮すること	手引に関連記載あり	9.1.1.8	アクセス制御方針に、利用可能な全ての種類の接続を認識する分散ネットワーク環境におけるアクセス権の管理を含める。
					手引に関連記載あり	9.1.2.8	ネットワークサービスの利用に関する方針は、組織のアクセス制御方針と整合させる。
			5c-S.15.5	アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。 d) 動的アクセス制御に関連する要素又は要因をどのように反映できるかを検討すること	手引に関連記載あり	9.1.1.16	アクセス制御方針に、ゼロトラストアーキテクチャ（動的なアクセス制御）に関する要求事項を含める。
5.16	識別情報の管理 統制目標：識別情報のライフサイクル全体を管理する。 目的：組織の情報及びその他の関連資産にアクセスする個人及びシステムを一意に特定できるようにし、アクセス権を適切に割り当てることができるようにするため。		5.16	識別情報の管理 管理策 識別情報のライフサイクル全体を管理する。 目的 組織の情報及びその他の関連資産にアクセスする個人及びシステムを一意に特定できるようにし、アクセス権を適切に割り当てることができるようにするため。		9.2	利用者アクセスの管理 管理目的：システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。
						9.2.1	利用者登録及び登録削除 アクセス権の割当てを可能にするために、利用者の登録及び登録削除についての正式な プロセスを実施する。
5.16.1	識別情報のライフサイクル全体を管理するプロセスを整備し、管理する。	識別情報の管理におけるプロセスは、次の事項を確実にする。 a) 個人に割り当てられる識別情報の場合、特定の識別情報を使って実行した処理に関してその個人にアカウンタビリティを負わせることができるように、一つの識別情報は一人の個人にだけひも（紐）付ける。 b) 複数の人に割り当てられる識別情報（例えば、共有の識別情報）は、業務上又は運用上の理由で必要であり、そのための承認及び文書化をする場合にだけ許可する。 c) 人間以外のエンティティに割り当てられる識別情報は、適切に権限を分離し承認及び独立した継続的な監視の対象とする。 d) 識別情報が不要になった場合（例えば、関連するエンティティが削除された若しくは使用されなくなった場合、又は識別情報にひも（紐）付けされた人的組織を去った若しくは役割を変えた場合）、識別情報を時機を失せずに無効化又は削除する。 e) 特定の領域では、一つだけの識別情報を一つのエンティティに対応付ける［すなわち、同じ環境下で一つのエンティティに複数の識別情報を対応付けること（複数識別情報）は避ける。］。 f) 利用者識別情報及び認証情報の使用及び管理に関する全ての重要な事象の記録を保持する。 組織は、利用者識別情報に関連する情報の変更を取り扱う支援プロセスをもつ。このプロセスは、個人に関連する価値する文書の再検証を含む場合がある。	5c-S.16.1	識別情報の管理におけるプロセスは、次の事項を確実にする。 a) 個人に割り当てられる識別情報の場合、特定の識別情報を使って実行した処理に関してその個人にアカウンタビリティを負わせることができるように、一つの識別情報は一人の個人にだけひも（紐）付ける。	手引に関連記載あり	9.2.1.1	利用者IDを管理するプロセスに、利用者と利用者自身の行動とを対応付けること、及び利用者がその行動に責任をもつことを可能にする、一意な利用者ID の利用を含める。
			5c-S.16.1	識別情報の管理におけるプロセスは、次の事項を確実にする。 b) 複数の人に割り当てられる識別情報は、業務上又は運用上の理由で必要であり、そのための承認及び文書化をする場合にだけ許可する。	手引に関連記載あり	9.2.1.2	利用者IDを管理するプロセスに、共有ID の利用は、業務上又は運用上の理由であり要な場合に だけ許可し、承認し、記録することを含める。
			5c-S.16.1	識別情報の管理におけるプロセスは、次の事項を確実にする。 c) 人間以外のエンティティに割り当てられる識別情報は、適切に権限を分離した承認及び独立した継続的な監視の対象とする。	手引に関連記載あり	–	（対応策なし）
			5c-S.16.1	識別情報の管理におけるプロセスは、次の事項を確実にする。 d) 識別情報が不要になった場合、識別情報を時機を失せずに無効化又は削除する。	手引に関連記載あり	9.2.1.3	利用者IDを管理するプロセスに、組織を離れた利用者の利用者IDの、即座の無効化又は削除を含める。
			5c-S.16.1	識別情報の管理におけるプロセスは、次の事項を確実にする。 e) 特定の領域では、一つだけの識別情報を一つのエンティティに対応付ける。	手引に関連記載あり	–	（対応策なし）
			5c-S.16.1	識別情報の管理におけるプロセスは、次の事項を確実にする。 f) 利用者識別情報及び認証情報の使用及び管理に関する全ての重要な事象の記録を保持する。	手引に関連記載あり	–	（対応策なし）
			5c-S.16.2	組織は、利用者識別情報に関連する情報の変更を取り扱う支援プロセスをもつ。	手引に関連記載あり	–	（対応策なし）
			（5c-S.16.2参考）	このプロセスは、個人に関連する価値する文書の再検証を含む場合がある。	手引に関連記載あり	–	（対応策なし）
5.16.2	第三者が提供又は発行した識別情報を使用する場合、第三者の識別情報が必要な信頼レベルにあること及び関連するリスクを特定し、対応する。	第三者が提供し又は発行した識別情報（例えば、ソーシャルメディアのクレデンシャル）を使用する場合、組織は、必要な信頼レベル が第三者の識別情報にあり、関連するリスクを知り、十分に対応する。この対応は、第三者に関連する管理策（5.19参照）、及び認証情報に関連する管理策（5.17参照）を含む場合がある。	5c-S.16.3	第三者が提供し又は発行した識別情報を使用する場合、組織は、必要な信頼レベルが第三者の識別情報にあり、関連するリスクを知り、十分に対応する。	手引に関連記載あり	–	（対応策なし）
			（5c-S.16.3参考）	この対応は、第三者に関連する管理策、及び認証情報に関連する管理策を含む場合がある。	手引に関連記載あり	–	（対応策なし）
5.16.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.17	認証情報 統制目標：認証情報の割当て及び管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理する。 目的：適切なエンティティ認証を確実にし、認証プロセスの失敗を防ぐため。		5.17	認証情報 管理策 認証情報の割当て及び管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理する。 目的 適切なエンティティ認証を確実にし、認証プロセスの失敗を防ぐため。		9.2.4	利用者の秘密認証情報の管理 秘密認証情報の割当ては、正式な管理プロセスによって管理する。
						9.3	利用者の責任 管理目的：利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。
						9.3.1	秘密認証情報の利用 秘密認証情報の利用時に、組織の慣行に従うこと を、利用者に要求する。
						9.4.3	パスワード管理システム パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にするものとする。
5.17.1	認証情報の割当て及び管理のプロセスを整備し、管理する。	認証情報の割当て及び管理のプロセスは、次の事項を確実にする。 a) 個の秘密認証情報として登録プロセスやに自動的に生成される個人パスワード又は個人識別番号（PIN）は、推測不可能であり、各人に対して一意で、かつ、利用者は最初の使用後にそれを変更することが要求される。 b) 新規、更新又は仮の認証情報を発行する前に、利用者の本人確認の手順を確立する。 c) 仮の認証情報を含む認証情報は、セキュリティを保った方法（例えば、信頼できる保護された経路を通じて）で利用者に渡し、保護されていない（平文の）電子メールのメッセージその目的で利用することは避ける。 d) 利用者は、認証情報の受領を知らせる。 e) 業務がからが心定めた又は提供した初期設定の認証情報は、システム又はソフトウェアのインストール直後に変更する。 f) 認証情報の割当て及び管理に関する重要な事象の記録を保持し、記録に機密性を付与する。記録保持方法は、承認を受ける［例えば、承認されたパスワード管理ツール（password vault tool）を使用］。	5c-S.17.1	認証情報の割当て及び管理のプロセスは、次の事項を確実にする。 a) 個の秘密認証情報として登録プロセスやに自動的に生成される個人パスワード又は個人識別番号（PIN）は、推測不可能であり、各人に対して一意で、かつ、利用者は最初の使用後にそれを変更することが要求される。	手引に関連記載あり	9.2.4.3	秘密認証情報の割当ての正式な管理プロセスでは、利用者に各自の秘密認証情報を保持することを求める場合、最初に、セキュリティが保たれた個の秘密認証情報を発行し、最初の使用時にこれを変更させる。
					手引に関連記載あり	9.2.4.6	秘密認証情報の割当ての正式な管理プロセスでは、個の秘密認証情報は、一人一人に対して一意とし、推測されないものとする。
			5c-S.17.1	認証情報の割当て及び管理のプロセスは、次の事項を確実にする。 b) 新規、更新又は個の認証情報を発行する前に、利用者の本人確認の手順を確立する。	手引に関連記載あり	9.2.4.4	秘密認証情報の割当ての正式な管理プロセスでは、新規、更新又は個の秘密認証情報を発行する前に、利用者の本人確認の手順を確立する。
			5c-S.17.1	認証情報の割当て及び管理のプロセスは、次の事項を確実にする。 c) 個の認証情報を含む認証情報は、セキュリティを保った方法で利用者に渡し、保護されていない（平文の）電子メールのメッセージその目的で利用することは避ける。	手引に関連記載あり	9.2.4.5	秘密認証情報の割当ての正式な管理プロセスでは、個の秘密認証情報は、セキュリティを保った方法で利用者に渡す。外部関係者を通じて渡すことは保護されていない（暗号化していない）電子メールのメッセージを利用することは避ける。
			5c-S.17.1	認証情報の割当て及び管理のプロセスは、次の事項を確実にする。 d) 利用者は、認証情報の受領を知らせる。	手引に関連記載あり	9.2.4.7	秘密認証情報の割当ての正式な管理プロセスでは、利用者は、秘密認証情報の受領を知らせる。
			5c-S.17.1	認証情報の割当て及び管理のプロセスは、次の事項を確実にする。 e) 業務がからが心定めた又は提供した初期設定の認証情報は、システム又はソフトウェアのインストール直後に変更する。	手引に関連記載あり	9.2.4.8	秘密認証情報の割当ての正式な管理プロセスでは、業務がからが心定めた秘密認証情報は、システム又はソフトウェアのインストール後に変更する。
			5c-S.17.1	認証情報の割当て及び管理のプロセスは、次の事項を確実にする。 f) 認証情報の割当て及び管理に関する重要な事象の記録を保持し、記録に機密性を付与する。記録保持方法は、承認を受ける。	手引に関連記載あり	–	（対応策なし）
5.17.2	認証情報にアクセス又は使用する者に、機密性を保つために必要な事項を伝達する。	認証情報にアクセスする又はそれを使用する者に、次の事項を確実に行うよう助言する。 a) パスワードなどの秘密認証情報は機密を保つ。個人の秘密認証情報を他人と共有しない。複数の利用者に、又は個人でないエンティティにひも（紐）付けられている識別情報に対して使用する秘密認証情報は、認可された上だけ共有する。 b) 影響を受けた又は侵害された認証情報は、侵害の知らせ又はその他の兆候があれば、直ちに変更する。 c) パスワードを認証情報として使用する場合、例えば、次のような最適な慣行の推奨事項に従った強力なパスワードを選択する。 1) パスワードは、当人に関する情報（例えば、名前、電話番号、誕生日）から、他の者が容易に推測できる又は得られる事項に基づかない。 2) パスワードは辞書の単語又はそれらの組合せに基づかない。 3) 覚えやすいパスフレーズを使用し、英数字及び特殊文字を含めるようにする。 4) パスワードに最小限必要とする長さを定める。 d) 異なるサービス及びシステム間で同じパスワードを使用しない。 e) a)～d)の規則に従う義務が、雇用条件にも含まれている（6.2参照）。	5c-S.17.2	認証情報にアクセスする又はそれを使用する者に、次の事項を確実に行うよう助言する。 a) パスワードなどの秘密認証情報は機密を保つ。個人の秘密認証情報を他人と共有しない。複数の利用者に、又は個人でないエンティティにひも（紐）付けられている識別情報に対して使用する秘密認証情報は、認可された上だけ共有する。 b) 影響を受けた又は侵害された認証情報は、侵害の知らせ又はその他の兆候があれば、直ちに変更する。 c) パスワードを認証情報として使用する場合、例えば、次のような最適な慣行の推奨事項に従った強力なパスワードを選択する。 1) パスワードは、当人に関する情報から、他の者が容易に推測できる又は得られる事項に基づかない。 2) パスワードは辞書の単語又はそれらの組合せに基づかない。 3) 覚えやすいパスフレーズを使用し、英数字及び特殊文字を含めるようにする。 4) パスワードに最小限必要とする長さを定める。 d) 異なるサービス及びシステム間で同じパスワードを使用しない。 e) a)～d)の規則に従う義務が、雇用条件にも含まれている。	手引に関連記載あり	9.2.4.1	秘密認証情報の割当ての正式な管理プロセスでは、個人の秘密認証情報を秘密に保つ旨の文書への署名を、利用者に要求する。この署名文書は、雇用契約の条件に含める場合がある。
					手引に関連記載あり	9.2.4.2	秘密認証情報の割当ての正式な管理プロセスでは、グループの（すなわち、共用の）秘密認証情報はグループのメンバだけが秘密に保つ旨の文書への署名を、利用者に要求する。この署名文書は、雇用契約の条件に含める場合がある。
					手引に関連記載あり	9.3.1.1	全ての利用者に、秘密認証情報を秘密にしておき、関係当局の署名点の他者に秘密認証情報が漏えいしないよう助言する。
					手引に関連記載あり	9.3.1.3	全ての利用者に、秘密認証情報に対する危険の兆候が見られる場合には、その秘密認証情報を変更するよう助言する。
					手引に関連記載あり	9.3.1.4	全ての利用者に、秘密認証情報としてパスワードを用いる場合は、十分な最短文字数をもつ質の良いパスワードを選定するよう助言する（質の良いパスワードは、次の条件を満たすものとする。①覚えやすい。②当人の関連情報（例えば、名前、電話番号、誕生日）から、他の者が容易に推測できる又は得られる事項に基づかない。③辞書攻撃に対い弱でない（すなわち、辞書に含まれる語から成りたっていない）。④同一文字を連ねただけ、数字だけ、又はアルファベットだけの文字列ではない。⑤仮パスワードを発行する場合、最初のログオン時点で変更する。）。
					手引に関連記載あり	9.3.1.5	全ての利用者に、個人用の秘密認証情報を共有しないよう助言する。
					手引に関連記載あり	9.3.1.7	全ての利用者に、業務目的のものと業務目的でないものとに、同じ秘密認証情報を用いないよう助言する。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.17.3	パスワード認証を使用する場合は、機密性を保つために必要な機能を備えたものを利用する。	パスワードを認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 a) 利用者が自分のパスワードを選択及び変更できるようにし、入力エラーに対処するための確認手順を含める。 b) 優良な慣行の推奨事項［5.17.2c)参照］に従って強固なパスワードを使用させる。 c) パスワードは、最初のログイン時に利用者に変更させる。 d) 必要に応じて、例えば、セキュリティインシデントの後に、又は有効な識別情報（例えば、共有識別情報）のパスワードを知っている利用者の雇用の終了若しくは変更の時に、パスワードを変更させる。 e) 以前のパスワードの再利用を防止する。 f) 一般的に使われるパスワード、並びにハッキングされたシステムで侵害された利用者名及びパスワードの組合せの使用を防止する。 g) パスワードは、入力時に、画面上に表示しない。 h) パスワードは、保護した形態で保存し、伝達する。 パスワードの暗号化及びハッシュ化は、パスワードに関する承認された暗号技術に従って実行する（8.24参照）。	5c-S.17.3	パスワードを認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 a) 利用者が自分のパスワードを選択及び変更できるようにし、入力エラーに対処するための確認手順を含める。	手引に関連記載あり	9.4.3.2	パスワードの管理システムでは、利用者に自分のパスワードの選択及び変更を許可し、また、入力誤りを考慮した確認手順を組み入れる。
			5c-S.17.3	パスワードを認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 b) 優良な慣行の推奨事項に従って強固なパスワードを使用させる。	手引に関連記載あり	9.4.3.3	パスワードの管理システムでは、質の良いパスワードを選択させるようにする。例えば、強固なパスワードに必要な桁数や複雑さをもつパスワードとする。
			5c-S.17.3	パスワードを認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 c) パスワードは、最初のログオン時に利用者に変更させる。	手引に関連記載あり	9.4.3.4	パスワードの管理システムでは、パスワードは、最初のログオン時に利用者に変更させるようにする。
			5c-S.17.3	パスワードを認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 e) 以前のパスワードの再利用を防止する。	手引に関連記載あり	9.4.3.6	パスワードの管理システムでは、以前に用いられたパスワードの記録を維持し、再使用を防止する。
			5c-S.17.3	パスワードを認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 g) パスワードは、入力時に、画面上に表示しない。	手引に関連記載あり	9.4.3.7	パスワードの管理システムでは、パスワードは、入力時に、画面上に表示しないようにする。
			5c-S.17.3	パスワードを認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 h) パスワードは、保護した形態で保存し、伝達する。	手引に関連記載あり	9.4.3.9	パスワードの管理システムでは、パスワードは、保護した形態で保存し、伝達する。
5.17.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.18	アクセス権 統制目標：情報及びその他の関連資産へのアクセスは、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除する。 目的：情報及びその他の関連資産へのアクセスを、事業上の要求事項に従って定義し、認可することを確実にするため。		5.18	アクセス権 管理策 情報及びその他の関連資産へのアクセスは、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除する。 目的 情報及びその他の関連資産へのアクセスを、事業上の要求事項に従って定義し、認可することを確実にするため。		9.2.2	利用者アクセスの提供 全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者アクセスの提供についての正式なプロセスを実施する。
						9.2.5	利用者アクセス権のレビュー 資産の管理責任者は、利用者のアクセス権を定められた期間でレビューする。
						9.2.6	アクセス権の削除又は修正 全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正する。
5.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て及び無効化のプロセスを整備し、アクセス権の割り当て、変更及び削除する。	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスには、次の事項を含む。 a) 情報及びその他の関連資産の利用についての、その情報及びその他の関連資産の管理責任者からの認可の取得（5.9参照）。アクセス権について、管理職による承認を受けることが適切な場合もある。 b) 事業上の要求事項及び組織のアクセス制御に関するトピック固有の方針並びに規則の考慮 c) アクセス権の承認及び実施の役割の分離。並びに相反する役割の分離を含む、職務の分離の考慮 d) ある有り情報及びその他の関連資産にアクセスする必要がなくなった場合にアクセス権を削除する。特に、組織をさった利用者のアクセス権を特機を失せずに削除する。 e) 特に臨時要員、又は要員が必要とする一時的なアクセスについて、限られた期間の一時的アクセス権を与え、期限の日に取り消すことの考慮 f) 許可したアクセスのレベルが、アクセス制御に関するトピック固有の方針に適していること（5.15参照）、及び職務の分離（5.3参照）などその他の情報セキュリティ要求事項と整合していることの検証 g) 認可手順が問題なく完了した後にだけ、アクセス権を有効にする（例えば、サービス提供者がアクセス権を有効にする） h) 情報及びその他の関連資産にアクセスするために利用者識別子（ID、論理的又は物理的）に与えられたアクセス権の、一元的な記録の維持 i) 役割又は職務を変更した利用者のアクセス権の変更 j) 物理的及び論理的アクセス権の削除又は調整（鍵、認証情報、識別カード又は利用資格の削除、無効化又は交換によって行うことが可能である。） k) 利用者の論理的及び物理的アクセス権の変更の記録の維持	5c-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスには、次の事項を含む。 a) 情報及びその他の関連資産の利用についての、その情報及びその他の関連資産の管理責任者からの認可の取得	手引に関連記載あり	9.2.2.1	利用者ID に対するアクセス権の割当て及び無効化のプロセに、情報システム又はサービスの利用について、その情報システム又はサービスの管理責任者からの認可を得ていることの点検を含める。（アクセス権について、管理職から別の承認を受けることが適切な場合もある。）
			5c-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスには、次の事項を含む。 b) 事業上の要求事項及び組織のアクセス制御に関するトピック固有の方針並びに規則の考慮	手引に関連記載あり	–	（対応項なし）
			5c-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスには、次の事項を含む。 c) アクセス権の承認及び実施の役割の分離。並びに相反する役割の分離を含む、職務の分離の考慮	手引に関連記載あり	9.2.2.2	利用者ID に対するアクセス権の割当て及び無効化のプロセに、許可したアクセスのレベルが、アクセス制御方針に適していることの点検を含める。
				f) 許可したアクセスのレベルが、アクセス制御に関するトピック固有の方針に適していること、及び職務の分離などその他の情報セキュリティ要求事項と整合していることの検証	手引に関連記載あり	9.2.2.3	利用者ID に対するアクセス権の割当て及び無効化のプロセに、許可したアクセスのレベルが、職務の分離などその他の要求事項と整合していることの検証を含める。
			5c-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスには、次の事項を含む。 e) 臨時要員、又は要員が必要とする一時的なアクセスについて、限られた期間の一時的アクセス権を与え、期限の日に取り消すことの考慮	手引に関連記載あり	–	（対応項なし）
			5c-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスには、次の事項を含む。 d) ある有り情報及びその他の関連資産にアクセスする必要がなくなった場合にアクセス権を削除する。特に、組織をさった利用者のアクセス権を特機を失せずに削除する。 i) 役割又は職務を変更した利用者のアクセス権の変更	手引に関連記載あり	9.2.2.6	利用者ID に対するアクセス権の割当て及び無効化のプロセに、役割又は職務を変更した利用者のアクセス権の変更、及び組織を離れた利用者のアクセス権の即座の解除又は停止することを含める。
					手引に関連記載あり	9.2.6.1	雇用の終了時に、アクセス権を削除する必要があるかどうかを決定し、情報並びに情報処理施設及びサービスに関連する資産に対する個人のアクセス権を削除又は一時停止を行う。
			5c-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスには、次の事項を含む。 g) 認可手順が問題なく完了した後にだけ、アクセス権を有効にする	手引に関連記載あり	9.2.2.4	利用者ID に対するアクセス権の割当て及び無効化のプロセに、認可手順が完了するまで、（例えば、クラウドサービス事業者が）アクセス権を有効にしないことが確実になるよう定める。
			5c-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスには、次の事項を含む。 h) 情報及びその他の関連資産にアクセスするために利用者識別子（ID、論理的又は物理的）に与えられたアクセス権の、一元的な記録の維持 k) 利用者の論理的及び物理的アクセス権の変更の記録の維持	手引に関連記載あり	9.2.2.5	利用者ID に対するアクセス権の割当て及び無効化のプロセに、情報システム又はサービスにアクセスするために利用者ID に与えられたアクセス権の、一元的な記録の維持を含める。
			5c-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスには、次の事項を含む。 j) 物理的及び論理的アクセス権の削除又は調整	手引に関連記載あり	9.2.6.3	削除又は修正が望ましいアクセス権には、物理的な及び論理的なアクセスに関するものを含める。
5.18.2	物理的及び論理的なアクセス権の定期的なレビューを実施する。	物理的及び論理的なアクセス権の定期的なレビューでは、次の事項を考慮する。 a) 同じ組織内での何らかの変更後（例えば、異動、昇進、降格）又は退職後の利用者のアクセス権（6.1～6.5参照） b) 特権のアクセス権の認可 情報及びその他の関連資産への利用者のアクセス権は、雇用の変更又は終了の前に、次に示す1又は2の評価に基づいて、レビューし、調整又は削除する。 a) 雇用の終了又は変更が、利用者の側によるものか又は経営側によるものかどうか、及び雇用の終了の理由 b) 利用者の現時点の責任 c) 現在アクセス可能な資産の価値	5c-S.18.2	物理的及び論理的なアクセス権の定期的なレビューでは、次の事項を考慮する。 a) 同じ組織内での何らかの変更後又は退職後の利用者のアクセス権 b) 特権のアクセス権の認可	手引に関連記載あり	9.1.1.11	アクセス制御方針に、アクセス権の定期的なレビューに対する要求事項を含める。
					手引に関連記載あり	9.2.2.7	利用者ID に対するアクセス権の割当て及び無効化のプロセに、情報システム又はサービスの管理責任者による、アクセス権の定期的なレビューを含める。
					手引に関連記載あり	9.2.5.1	利用者のアクセス権は、定められた期間で見直す。
					手引に関連記載あり	9.2.5.2	利用者のアクセス権は、何らかの変更（例えば、昇進、降格、雇用の終了）があった後に見直す。
					手引に関連記載あり	9.2.5.3	利用者のアクセス権は、利用者の役割が同一組織内で変更された場合、そのアクセス権についてレビュー、削当てもし直す。
			5c-S.18.3	情報及びその他の関連資産への利用者のアクセス権は、雇用の変更又は終了の前に、次に示す1又は2の評価に基づいて、レビューし、調整又は削除する。 a) 雇用の終了又は変更が、利用者の側によるものか又は経営側によるものかどうか、及び雇用の終了の理由 b) 利用者の現時点の責任 c) 現在アクセス可能な資産の価値	手引に関連記載あり	9.2.6.2	雇用を変更した場合、新規の業務において承認されていない全てのアクセス権を削除する。
					手引に関連記載あり	9.2.6.6	情報及び情報処理施設に関連する資産へのアクセス権は、雇用の終了又は変更の前に、雇用の終了又は変更が、従業員若しくは外部の利用者の側によるものかは経営側によるものかどうか、及び雇用の終了の理由、従業員、外部の利用者、又は他の利用者の現時点の責任、現在アクセス可能な資産の価値の1又は2の評価に応じて、縮小又は削除する。
5.18.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.19	供給者関係における情報セキュリティ 統制目標：供給者の製品及びサービスの利用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施する。 目的：供給者関係において合意したレベルの情報セキュリティを維持するため。		5.19	供給者関係における情報セキュリティ 管理策 供給者の製品及びサービスの利用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施する。 目的 供給者関係において合意したレベルの情報セキュリティを維持するため。		15	供給者関係
						15.1	供給者関係における情報セキュリティ 管理目的：供給者がアクセスできる組織の資産の保護を確実にするため。
						15.1.1	供給者関係のための情報セキュリティの方針 組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化する。
5.19.1	供給者の製品又はサービスの利用に関連する方針を策定し、関連する全ての利害関係者に伝達する。	特になし。	5d-5.19.1	組織は、供給者関係に関するトピック固有の方針を確立し、関連する全ての利害関係者に伝達する。	管理策に関連記載あり	15.1.1.1	組織は、供給者による組織の情報へのアクセスに具体的に対処するため、方針において情報セキュリティ管理策を特定し、義務付ける。
5.19.2	供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するための プロセス及び手順を整備し、実施する。	組織は、供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するための プロセス及び手順を特定し、実施する。 供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するための プロセス及び手順は、組織によるクラウドサービス プロバイダの資源の利用にも適用する。 供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するための プロセス及び手順は、組織が実施するもの、並びに、供給者の製品若しくはサービスの利用の開始又は供給者の製品及びサービスの利用の終了に関して、供給者が実施することを組織が要求するものを含む。 プロセス及び手順に含まれる内容の例として、次がある。 a) 組織の情報の機密性、完全性及び可用性に影響を与える可能性のある供給者の種類（例えば、ICTサービス、物流、公益事業、金融サービス、ICT基盤の構成要素）の特定及び文書化 b) 情報、製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択する方法の確立（例えば、市場分析、顧客への照会、文書のレビュー、オンサイト評価、取得している認証を用いて） c) 適切な情報セキュリティ管理策を備えた供給者の製品及びサービスの評価及び選択、並びにそれらのレビュー。特に、供給者が実施する管理策の正確性及び完全性、それによって供給者の情報及び情報処理の完全性を確実にし、ひいては組織の情報セキュリティを確実にすること。 d) 供給者がアクセス、監視、管理又は使用する可能性のある組織の情報、ICT サービス及び物理的インフラストラクチャの定義 e) 組織の情報の機密性、完全性及び可用性に影響を与える可能性のある、供給者が提供するICT基盤の構成要素及びサービスの種類の定義 f) 次の事項に関連する情報セキュリティリスクの評価及び管理 1) 潜在的な悪意のある供給者の要員に起因するリスクを含む、組織の情報及びその他の関連資産の供給者による使用 2) 供給者が提供する製品（これらの製品で使用されるソフトウェア構成要素及びサプライチェーンを含む。）又はサービスの誤動作又は甘い弱性 g) 第三者のレビュー及び製品の妥当性確認を含む、供給者の種類ごと及びアクセスの種類ごとに確立した情報セキュリティ要求事項の順守の監視 h) 供給者の不順守の低減、これは監視を通じて検知されたか、又は他の手段によって検知されたかによらない。 i) 供給者の製品及びサービスに関連するインシデント及び不測の事態への対処。これには、組織及び供給者の両方の責任を含める。 j) 供給者の情報及び情報処理の可用性、並びにそれによって組織の情報の可用性を確実にするための、レジリエンスに関する対策、並びに必要な場合には、回復及び不測の事態に関する対策 k) 供給者の要員とやり取りする組織の要員を対象とした、職務に関する適切な規則、トピック固有の方針、プロセス、手順及び行動について、供給者の種類並びに供給者による組織のシステム及び情報へのアクセスのレベルに基づく、意識向上及び訓練 l) 情報、その他の関連資産及び移動が必要なその他のものの転送の管理、並びにその転送期間全体にわたって情報セキュリティの維持を確実にすること m) 次の事項を含む供給者関係のセキュリティに配慮した終了を確実にするための要求事項 1) アクセス権の回収 2) 情報の取扱い 3) 契約中に開発された知的財産の帰属の決定 4) 供給者又は内部委託の変更における情報の移行性 5) 記録管理 6) 資産の返却 7) 情報及びその他の関連資産のセキュリティに配慮した処分 8) 機密保持の要求の継続 n) 供給者の要員及び設備に期待する要員セキュリティ及び物理的セキュリティのレベル 組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実化を含める。 エンドポイント機能に係る供給者によるサポートには、供給者による利用方法の支援等のサポートやソフトウェアの更新に関らず、オープンソースソフトウェアにおけるセキュリティ更新の体制の維持等も含まれる。(8.1参照)	5d-5.19.2	組織は、供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するための プロセス及び手順を特定し、実施する。	手引に関連記載あり	15.1.1.2	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、組織が、自らの情報へのアクセスを許可する供給者の種類（例えば、IT サービス、物流サービス、金融サービス、IT 基盤の構成要素などの供給者）の特定及び文書化を含める。
			(5d-5.19.4参考)	プロセス及び手順に含まれる内容の例として、次がある。 a) 組織の情報の機密性、完全性及び可用性に影響を与える可能性のある供給者の種類の特定及び文書化 b) 情報、製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択する方法の確立 e) 組織の情報の機密性、完全性及び可用性に影響を与える可能性のある、供給者が提供するICT基盤の構成要素及びサービスの種類の定義 n) 供給者の要員及び設備に期待する要員セキュリティ及び物理的セキュリティのレベル	手引に関連記載あり	–	（対応項なし）
			(5d-5.19.4参考)	プロセス及び手順に含まれる内容の例として、次がある。 d) 供給者がアクセス、監視、管理又は使用する可能性のある組織の情報、ICTサービス及び物理的インフラストラクチャの定義	手引に関連記載あり	15.1.1.4	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、様々な供給者に許可される情報へのアクセスの種類の定義、並びにそのアクセスの監視及び管理を含める。
			(5d-5.19.4参考)	プロセス及び手順に含まれる内容の例として、次がある。 f) 次の事項に関連する情報セキュリティリスクの評価及び管理 1) 潜在的な悪意のある供給者の要員に起因するリスクを含む、組織の情報及びその他の関連資産の供給者による使用 2) 供給者が提供する製品（これらの製品で使用されるソフトウェア構成要素及びサプライチェーンを含む。）又はサービスの誤動作又は甘い弱性 h) 供給者の不順守の低減、これは監視を通じて検知されたか、又は他の手段によって検知されたかによらない。 i) 供給者の製品及びサービスに関連するインシデント及び不測の事態への対処。これには、組織及び供給者の両方の責任を含める。	手引に関連記載あり	–	（対応項なし）
			(5d-5.19.4参考)	プロセス及び手順に含まれる内容の例として、次がある。 g) 第三者のレビュー及び製品の妥当性確認を含む、供給者の種類ごと及びアクセスの種類ごとに確立した情報セキュリティ要求事項の順守の監視	手引に関連記載あり	15.1.1.6	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、それぞれの供給者及びアクセスに関して確立した情報セキュリティ要求事項が順守されているか否かを監視するためのプロセス及び手順（これには第三者のレビュー及び製品の妥当性確認も含まれる）を含める。
			(5d-5.19.4参考)	プロセス及び手順に含まれる内容の例として、次がある。 c) 適切な情報セキュリティ管理策を備えた供給者の製品又はサービスの評価及び選択、並びにそれらのレビュー。特に、供給者が実施する管理策の正確性及び完全性、それによって供給者の情報及び情報処理の完全性を確実にし、ひいては組織の情報セキュリティを確実にすること。	手引に関連記載あり	15.1.1.7	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、各当事者が提供する情報又は情報処理の完全性を確実にするための、正確さ及び完全さの管理を含める。
			(5d-5.19.4参考)	プロセス及び手順に含まれる内容の例として、次がある。 j) 供給者の情報及び情報処理の可用性、並びにそれによって組織の情報の可用性を確実にするための、レジリエンスに関する対策、並びに必要な場合には、回復及び不測の事態に関する対策	手引に関連記載あり	15.1.1.10	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、各当事者が提供する情報又は情報処理の可用性を確実にするための、対応力に関する取決め、並びに必要な場合には、回復及び不測の事態に関する取決めを含める。
			(5d-5.19.4参考)	プロセス及び手順に含まれる内容の例として、次がある。 k) 供給者の要員とやり取りする組織の要員を対象とした、職務に関する適切な規則、トピック固有の方針、プロセス、手順及び行動について、供給者の種類並びに供給者による組織のシステム及び情報へのアクセスのレベルに基づく、意識向上及び訓練	手引に関連記載あり	15.1.1.11	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、調達に関与する組織の要員を対象とした、適用される方針、プロセス及び手順についての意識向上訓練を含める。
					手引に関連記載あり	15.1.1.12	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、供給者の要員とやり取りする組織の要員を対象とした、関与及び行動に関する適切な規則（これは、供給者の種類、並びに組織のシステム及び情報への供給者によるアクセスのレベルに基づく）についての意識向上訓練を含める。
			(5d-5.19.4参考)	プロセス及び手順に含まれる内容の例として、次がある。 l) 情報、その他の関連資産及び移動が必要なその他のものの転送の管理、並びにその転送期間全体にわたって情報セキュリティの維持を確実にすること m) 次の事項を含む供給者関係のセキュリティに配慮した終了を確実にするための要求事項 1) アクセス権の回収 2) 情報の取扱い 3) 契約中に開発された知的財産の帰属の決定 4) 供給者又は内部委託の変更における情報の移行性 5) 記録管理 6) 資産の返却 7) 情報及びその他の関連資産のセキュリティに配慮した処分 8) 機密保持の要求の継続	手引に関連記載あり	15.1.1.14.B	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実化を含める。
5.19.3	供給者がその製品又はサービスを提供できなくなった場合に情報処理を継続するための手順を整備する。	代替の製品又はサービスの手配の遅延を回避するため、供給者がその製品又はサービスを提供できなくなった場合（例えば、インシデントのため、供給者が事業を行わなくなったため、又は技術の進歩によって一部の構成要素を供給しなくなったため）に情報処理を継続するための手順（例えば、事前に代替の供給者を特定しおく、又は常に代替の供給者も利用する。）を検討する。	5d-5.19.5	代替の製品又はサービスの手配の遅延を回避するため、供給者がその製品又はサービスを提供できなくなった場合に情報処理を継続するための手順を検討する。	手引に関連記載あり	15.1.1.9	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、供給者によるアクセスに伴うインシデント及び不測の事態への対処（これには、組織及び供給者の責任を含める）を含める。
5.20	供給者との合意における情報セキュリティの取扱い 統制目標：供給者関係の種類に応じて、関連する情報セキュリティ要求事項を確立し、各供給者と合意する。 目的：供給者関係において合意したレベルの情報セキュリティを維持するため。		5.20	供給者との合意における情報セキュリティの取扱い 管理策 供給者関係の種類に応じて、関連する情報セキュリティ要求事項を確立し、各供給者と合意する。 目的 供給者関係において合意したレベルの情報セキュリティを維持するため。		15.1.2	供給者との合意における情報セキュリティの取扱い 関連する全ての情報セキュリティ要求事項を確立し、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のための IT 基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意する。
5.20.1	供給者関係の種類に応じて、関連する情報セキュリティ要求事項を定義し、供給者と合意する。	関連する情報セキュリティ要求事項を満たすという両当事者の義務に関し、組織と供給者との間に明確な理解が得られることを確実にするために、供給者との合意を確立し、これを文書化する。 特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 a) 提供しスはアクセスされる情報の記載、及び提供方法又はアクセス方法の記載 b) 組織の分類体系に従った情報の分類（5.10、5.12及び5.13参照） c) 組織の分類体系と供給者の分類体系との間の対応付け d) 法令、規制及び契約上の要求事項［データ保護、個人識別可能情報（PII）の取扱い、知的財産権及び著作権に関する要求事項を含む。］、並びにこれらの要求事項を満たすことを確実にする方法についての記載 e) 契約の各当事者に対する、合意した一連の管理策（アクセス制御、パフォーマンスのレビュー、監視、報告及び監査を含む。）の実施の義務、及び供給者に対する、組織の情報セキュリティ要求事項の順守の義務 f) 情報及びその他の関連資産の許容される利用に関する規則。必要な場合、許容されない利用についての規則も含める。 g) 供給者の要員による組織の情報及びその他の関連資産の使用を認可する場合及びその認可を解除する場合の手順又は条件（例えば、組織の情報及びその他の関連資産を使用することが正当化される供給者の要員を特別に示す） h) 供給者のICT基盤に関する情報セキュリティ要求事項。特に、組織の事業上のニーズ及び以下各基準に基づき、個々の供給者との合意の基礎となる、情報の種類及びアクセスの種類それぞれについての最小限の情報セキュリティ要求事項 i) 調査事案が要求事項を満たさなかった場合の補償及び矯正 j) インシデント管理の要求事項及び手順（特に、インシデントからの回復中の通知及び協力） k) 特定の手順及び情報セキュリティ要求事項についての訓練及び意識向上に関する要求事項 l) 下請負業者が要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 1) 下請負供給者の使用に関する合意など、実施する必要のある管理策を含む、下請負契約に関する該当する規定（例えば、下請負供給者に対して供給者と同じ義務を負わせることの要求、下請負供給者のリストをもつこと及び変更前の通知の要求） m) 情報セキュリティに関する連絡先担当者も含む、関連する連絡先 n) 法的に許容される場合、供給者の要員の選考に関する要求事項。この要求事項には、選考を実施する責任、及び選考が完了しなかった場合又は選考の結果、疑い若しくは懸念が生じた場合に行う通知の手順も含める。 o) 供給者のプロセスに関連する情報セキュリティ要求事項についての第三者立証の証拠及び保証の仕組み。並びに管理策の有効性に関する独立した報告書 p) 合意に関する、供給者のプロセス及び管理策を監査する権利 q) 管理策の有効性について、報告書を定期的に提出する供給者の義務、及び報告書で提起された問題を適時に修正することに関する合意 r) 合意上の問題点の解決及び紛争解決のプロセス s) 組織のニーズに合わせたバックアップの提供（頻度及び機能並びに保管場所の点で） t) 主要設備と同じ機能にはさらされない代替設備（すなわち、災害回復サイト）の可用性を確実にすること、及び主要管理策が失敗した場合のフォールバック管理策（代替管理策）の考慮 u) 組織への事前通知を確実にする変更管理プロセスをもつこと、及び組織が変更を受け入れない可能性 v) 情報の物理的に含む物理的セキュリティ管理策 w) 物理的輸送又は論理的送信中に情報を保護するための情報の転送の管理策 x) 記録管理、資産の返却、情報及びその他の関連資産のセキュリティに配慮した処分、並びに機能的な機密保持義務を含む、合意締結時に定める終了条項 y) 供給者が保有している組織の情報を、不要になり次第、セキュリティに配慮して破壊する方法の規定 z) 契約の終了時に、別の供給者又は組織自らへの引継ぎの支援を確実にすること	5d-5.20.1	関連する情報セキュリティ要求事項を満たすという両当事者の義務に関し、組織と供給者との間に明確な理解が得られることを確実にするために、供給者との合意を確立し、これを文書化する。	手引に関連記載あり	15.1.2.1	関連する情報セキュリティ要求事項を満たすという両当事者の義務に関し、組織と供給者との間に誤解が生じないことを確実にするために、供給者との合意を確立し、これを文書化する。
					手引に関連記載あり	15.1.1.13	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報セキュリティに関する要求事項及び管理策を、両当事者が署名する合意書の中に記載する条件を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 a) 提供しスはアクセスされる情報の記載、及び提供方法又はアクセス方法の記載	手引に関連記載あり	15.1.2.2	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、提供し又はアクセスされる情報の記載、及び提供方法又はアクセス方法の記載を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 b) 組織の分類体系に従った情報の分類	手引に関連記載あり	15.1.2.3	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、組織の分類体系に従った情報の分類（必要な場合、組織の分類体系と供給者の分類体系との間の対応付け）を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 c) 組織の分類体系と供給者の分類体系との間の対応付け	手引に関連記載あり	15.1.2.3	【再】特定された情報セキュリティ要求事項を満たすために、供給者との合意には、組織の分類体系に従った情報の分類（必要な場合、組織の分類体系と供給者の分類体系との間の対応付け）を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 d) 法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすことを確実にする方法についての記載	手引に関連記載あり	15.1.2.4	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、法的及び規制の要求事項（データ保護、契約財産及び著作権に関する要求事項を含む）、並びにこれらの要求事項を満たすことを確実にする方法についての記載を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 e) 契約の各当事者に対する、合意した一連の管理策の実施の義務、及び供給者に対する、組織の情報セキュリティ要求事項の順守の義務	手引に関連記載あり	15.1.1.8	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、組織の情報を保護するために供給者に適用する義務の種類を含める。
					手引に関連記載あり	15.1.2.5	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、契約の各当事者に対する、合意した一連の管理策（アクセス制御、パフォーマンスのレビュー、監視、報告及び監査を含む）の実施の義務を含める。
					手引に関連記載あり	15.1.2.17	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、組織のセキュリティ要求事項を順守するという供給者の義務を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 f) 情報及びその他の関連資産の許容される利用に関する規則。必要な場合、許容されない利用についての規則も含める。	手引に関連記載あり	15.1.2.6	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、情報の許容可能な利用に関する規則（必要な場合、許容できない利用についての規則も）を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 g) 供給者の要員による組織の情報及びその他の関連資産の使用を認可する場合及びその認可を解除する場合の手順又は条件	手引に関連記載あり	15.1.2.7	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、組織の情報にアクセスする前には組織の情報を受領することが認められている供給者の要員のリスト、又は供給者の要員による組織の情報の取扱いを認めることが受領を認可する場合及びその認可を解除する場合の手順・条件、その リストの変更又はその認可の解除がある場合にその旨を組織に知らせることを含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 h) 供給者のICT基盤に関する情報セキュリティ要求事項。特に、組織の事業上のニーズ及び以下各基準に基づき、個々の供給者との合意の基礎となる、情報の種類及びアクセスの種類それぞれについての最小限の情報セキュリティ要求事項	手引に関連記載あり	15.1.1.5	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報の種類及びアクセスの種類ごとの最低限の情報セキュリティ要求事項で、組織の事業上のニーズ及び要求事項並びに組織のリスク プロファイルに基づく供給者との個々の合意の基礎となるものを含める。
					手引に関連記載あり	15.1.2.8	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、それぞれの契約に関連する情報セキュリティのための力計算を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 j) インシデント管理の要求事項及び手順（特に、インシデントからの回復中の通知及び協力）	手引に関連記載あり	15.1.2.9	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、インシデント管理の要求事項及び手順（特に、インシデントからの回復中の通知及び協力）を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 k) 特定の手順及び情報セキュリティ要求事項についての訓練及び意識向上に関する要求事項	手引に関連記載あり	15.1.2.10	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、インシデント対応手順、認可手順などの、特定の手順及び情報セキュリティ要求事項についての訓練及び意識向上に関する要求事項を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 l) 下請負供給者の使用に関する合意など、実施する必要のある管理策を含む、下請負契約に関する該当する規定	手引に関連記載あり	15.1.2.11	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、実施する必要のある管理策を含む、下請負契約に関する該当する規制を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 m) 情報セキュリティに関する連絡先担当者も含む、関連する連絡先	手引に関連記載あり	15.1.2.12	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、情報セキュリティに関する連絡先担当者も含む、合意における相手方の担当者を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 n) 法的に許容される場合、供給者の要員の選考に関する要求事項。この要求事項には、選考を実施する責任、及び選考が完了しなかった場合又は選考の結果、疑い若しくは懸念が生じた場合に行う通知の手順も含める。	手引に関連記載あり	15.1.2.13	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、必要に応じて、供給者の要員の選考に関する要求事項を含める（この要求事項には、選考を実施する責任、及び選考が完了しなかった場合又は選考の結果、疑い若しくは懸念が生じた場合に行う通知の手順も含める。）。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 o) 合意に関する、供給者のプロセス及び管理策を監査する権利	手引に関連記載あり	15.1.2.14	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、供給者が実施する、合意に関わるプロセス及び管理策を監査する権利を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 q) 管理策の有効性について、報告書を定期的に提出する供給者の義務、及び報告書で提起された問題を適時に修正することに関する合意	手引に関連記載あり	15.1.2.16	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、報告書で提起された問題を適時に修正することに関する管理策及び合意の有効性について、独立した報告書を定期的に提出する供給者の義務を含める。
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 r) 合意上の問題点の解決及び紛争解決のプロセス	手引に関連記載あり	15.1.2.15	特定された情報セキュリティ要求事項を満たすために、供給者との合意には、合意上の問題点の解決及び紛争解決のプロセスを含める。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
			(5d-5.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 i) 請負業者が要求事項を満たさなかった場合の補償及び是正 o) 供給者のプロセスに関連する情報セキュリティ要求事項についての第三者立証の証跡及び保証の仕組み、並びに管理策の有効性に関する独立した報告書 s) 組織のニーズに合わせたバックアップの提供（頻度及び種類並びに保管場所の点で） t) 主要設備と同じ脅威にはさらされない代替設備（すなわち、災害回復サイト）の可用性を確実にすること、及び主要管理策が失敗した場合のフォールバック管理策（代替管理策）の考慮 u) 組織への事前通知を確実にする変更管理プロセスをもつこと、及び組織が変更を受け入れない可能性 v) 情報の分類に合った物理的セキュリティ管理策 w) 物理的輸送又は論理的送信中に情報を保護するための情報の転送の管理策 x) 記録管理、義務の返却、情報及びその他の関連資産のセキュリティに配慮した処分、並びに継続的な機密保持義務を含む、合意締結時に定める終了条項 y) 供給者が保存している組織の情報を、不要になり次第、セキュリティに配慮して破壊する方法の規定 z) 契約の終了時に、別の供給者又は組織自らへの引継ぎの支援を確実にすること	手引に関連記載あり	–	（対応項なし）
5.20.2	供給者との合意の登録簿を作成し、維持する。	組織は、自らの情報がどこへ渡っているかを追跡するために、外部関係者との合意（例えば、契約、覚書、情報共有契約）の登録簿を作成し、維持する。 組織はまた、外部関係者との合意を定期的にレビューし、妥当性を確認し、更新して、それらが依然として必要であり、関連する情報セキュリティ条項によって目的に適合することを確実にする。	5d-5.20.2	組織は、自らの情報がどこへ渡っているかを追跡するために、外部関係者との合意の登録簿を作成し、維持する。	手引に関連記載あり	–	（対応項なし）
			5d-5.20.3	組織はまた、外部関係者との合意を定期的にレビューし、妥当性を確認し、更新して、それらが依然として必要であり、関連する情報セキュリティ条項によって目的に適合することを確実にする。	手引に関連記載あり	–	（対応項なし）
5.20.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.21	ICTサプライチェーンにおける情報セキュリティの管理 統制目標：ICT製品及びサービスのサプライチェーンに関連する情報セキュリティリスクを管理するための プロセス及び手順を定め、実施する。 目的：供給者関係において合意したレベルの情報セキュリティを維持するため。		5.21	ICTサプライチェーンにおける情報セキュリティの管理 管理策 ICT製品及びサービスのサプライチェーンに関連する情報セキュリティリスクを管理するための プロセス及び手順を定め、実施する。 目的 供給者関係において合意したレベルの情報セキュリティを維持するため。		15.1.3	ICTサプライチェーン 供給者との合意には、情報通信技術（以下「ICT」という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含める。
5.21.1	ICT製品及びサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセス及び手順を整備し、実施する。	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 a) ICT製品又はサービスの取扱に適用する情報セキュリティ要求事項を定める。 b) 供給者が組織に提供するICTサービスの一部を下請負契約に出す場合には、そのサプライチェーン全体に組織のセキュリティ要求事項を伝達するようにICTサービスの供給者に要求する。 c) ICT製品に関して、その製品に他の供給者又は他のエンティティ（例えば、下請負ソフトウェア開発者、ハードウェア構成要素供給者）から購入又は取得した構成要素が含まれる場合には、そのサプライチェーン全体に適切なセキュリティ慣行を伝達するようにICT製品の供給者に要求する。 d) ICT製品の供給者に、製品で使用しているソフトウェア構成要素を記載した情報を提供するよう要求する。 e) ICT製品の供給者に、自らの製品が実装するセキュリティ機能及びそのセキュリティに配慮した運用に必要な構成を説明する情報を提供するよう要求する。 f) 提供されたICT製品及びサービスが規定のセキュリティ要求事項を順守していることを確認するための、監視プロセス及び許容可能な監視方法を実施する。このような供給者レビュー方法の例に、侵入テスト、及び供給者の情報セキュリティ運用に関する第三者立証の検証又は妥当性確認がある。 g) 製品又はサービスの機能を維持するために重要な構成要素を特定し、文書化するプロセスを実施する。重要な構成要素に対しては、組織の外で作られる場合に必要とされる注意、精査及び厳なるフォローアップの強化が求められる。（例、供給者が製品又はサービスの構成要素を他の供給者に外部委託する場合。）。 h) 重要な構成要素及びその供給元が、サプライチェーン全体を通じて追跡可能であるという保証を得る。 i) 提供されるICT製品が期待どおりに機能し、予期しない又は好ましくない特性をもたないという保証を得る。 j) 供給者からの構成要素が真正のものであり、その仕様から変更されていないことを確実にするための プロセスを実施する。対象の例に、改ざん防止ラベル、暗号ハッシュ検証又はディジタル署名がある。仕様外の動作を監視することが、改ざん又は偽造を見つける手掛りとなる可能性がある。改ざんの防止及び検知は、設計、開発、統合、運用及び保守を含むシステム開発ライフサイクルの複数の段階で実施する。 k) ICT製品が、例えば、正式な認証又は共通基準承認アレンジメント（Common Criteria Recognition Arrangement）などの評価体系を通じて、必要なセキュリティレベルを達成していることの保証を得る。 l) サプライチェーンについての情報、並びに組織と供給者との間で生じる可能性のある問題及び妥協についての規則を定める。 m) ICT構成要素のライフサイクル及び継続的な使用、並びにこれに関連するセキュリティリスクを管理するための具体的なプロセスを実施する。このプロセスには、その構成要素が入手できなくなる（供給者が事業を営まなくなる、又は技術進歩によって供給者がその構成要素を提供しなくなる）というリスクを管理することも含まれる。代替供給者の特定、並びにソフトウェア及び/又は能力獲得に移転するプロセスを検討する。	5.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 a) ICT製品又はサービスの取扱に適用する情報セキュリティ要求事項を定める。	手引に関連記載あり	15.1.3.1	供給者との合意には、供給者関係に関する一般的な情報セキュリティ要求事項のほかに、ICT 製品及びサービスの取扱に適用する情報セキュリティ要求事項を定めることを含める。
			5d-5.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 b) 供給者が組織に提供するICTサービスの一部を下請負契約に出す場合には、そのサプライチェーン全体に組織のセキュリティ要求事項を伝達するようにICTサービスの供給者に要求する。	手引に関連記載あり	15.1.3.2	供給者との合意には、ICT サービスに関して、供給者が組織に提供するICT サービスの一部を下請負契約に出す場合には、そのサプライチェーン全体に組織のセキュリティ要求事項を伝達するよう供給者に要求することを含める。
			5d-5.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 c) ICT製品に関して、その製品に他の供給者又は他のエンティティから購入又は取得した構成要素が含まれる場合には、そのサプライチェーン全体に適切なセキュリティ慣行を伝達するようにICT製品の供給者に要求する。	手引に関連記載あり	15.1.3.3	供給者との合意には、ICT 製品に関して、その製品に他の供給者から購入した構成部品が含まれる場合には、そのサプライチェーン全体に適切なセキュリティ慣行を伝達するよう供給者に要求することを含める。
			5d-5.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 e) ICT製品の供給者に、自らの製品が実装するセキュリティ機能及びそのセキュリティに配慮した運用に必要な構成を説明する情報を提供するよう要求する。	手引に関連記載あり	14.1.1.13	製品の供給者との契約は、明確にされたセキュリティ要求事項を規定する。
			5d-5.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 f) 提供されたICT製品及びサービスが規定のセキュリティ要求事項を順守していることを確認するため、監視プロセス及び許容可能な監視方法を実施する。このような供給者レビュー方法の例に、侵入テスト、及び供給者の情報セキュリティ運用に関する第三者立証の検証又は妥当性確認がある。	手引に関連記載あり	15.1.3.4	供給者との合意には、提供されたICT 製品及びサービスが規定のセキュリティ要求事項を順守していることを確認するため、監視プロセス及び許容可能な監視方法を実施することを含める。
			5d-5.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 g) 製品又はサービスの機能を維持するために重要な構成要素を特定し、文書化するプロセスを実施する。重要な構成要素に対しては、組織の外で作られる場合に必要とされる注意、精査及び厳なるフォローアップの強化が求められる（例え、供給者が製品又はサービスの構成要素を他の供給者に外部委託する場合。）。	手引に関連記載あり	15.1.3.5	特に、直接の供給者が製品又はサービスの構成要素を他の供給者に外部委託する場合（製品又はサービスの機能を維持するために重要な構成要素に対しては、組織の外で作られる場合に注意及び精査の強化が求められるため）、供給者との合意には、重要な構成要素を特定するためのプロセスを実施することを含める。
			5d-5.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 h) 重要な構成要素及びその供給元が、サプライチェーン全体を通じて追跡可能であるという保証を得る。	手引に関連記載あり	15.1.3.6	供給者との合意には、重要な構成要素及びその供給元が、サプライチェーン全体を通じて追跡可能であるという保証を得ることを含める。
			5d-5.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 i) 提供されるICT製品が期待どおりに機能し、予期しない又は好ましくない特性をもたないという保証を得る。	手引に関連記載あり	15.1.3.7	供給者との合意には、提供されるICT 製品が期待どおりに機能し、予期しない又は好ましくない特性をもたないという保証を得ることを含める。
			5d-5.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 l) サプライチェーンについての情報、並びに組織と供給者との間で生じる可能性のある問題及び妥協についての情報を共有するための規則を定める。	手引に関連記載あり	15.1.3.8	供給者との合意には、サプライチェーンについての情報、並びに組織と供給者との間で生じる可能性のある問題及び妥協についての情報を共有するための規則を定めることを含める。
			5d-5.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 m) ICT 構成要素のライフサイクル及び継続的な使用、並びにこれに関連するセキュリティリスクを管理するための具体的なプロセスを実施する。このプロセスには、その構成要素が入手できなくなる（供給者が事業を営まなくなる、又は技術進歩によって供給者がその構成要素を提供しなくなる）というリスクを管理することも含める。	手引に関連記載あり	15.1.3.9	供給者との合意には、ICT 構成要素のライフサイクル及び継続的な使用、並びにこれに関連するセキュリティリスクを管理するための具体的なプロセスを実施することを含める。このプロセスには、その構成要素が入手できなくなる（供給者が事業を営まなくなる、又は技術進歩によって供給者がその構成要素を提供しなくなる）というリスクを管理することも含める。
			5d-5.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 d) ICT製品の供給者に、製品で使用しているソフトウェア構成要素を記載した情報を提供するよう要求する。 j) 供給者からの構成要素が真正のものであり、その仕様から変更されていないことを確実にするためのプロセスを実施する。対象の例に、改ざん防止ラベル、暗号ハッシュ検証又はディジタル署名がある。仕様外の動作を監視することが、改ざん又は偽造を見つける手掛りとなる可能性がある。改ざんの防止及び検知は、設計、開発、統合、運用及び保守を含むシステム開発ライフサイクルの複数の段階で実施する。 k) ICT製品が、例えば、正式な認証又は共通基準承認アレンジメント（Common Criteria Recognition Arrangement）などの評価体系を通じて、必要なセキュリティレベルを達成していることの保証を得る。	手引に関連記載あり	–	（対応項なし）
5.21.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.21.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.22	供給者のサービス提供の監視、レビュー及び変更管理 統制目標：組織は、供給者の情報セキュリティの活動及びサービス提供を定常的に監視し、レビュー、評価、変更を管理する。 目的：供給者との合意に沿って、合意したレベルの情報セキュリティ及びサービス提供を維持するため。		5.22	供給者のサービス提供の監視、レビュー及び変更管理 管理策 組織は、供給者の情報セキュリティの活動及びサービス提供を定常的に監視し、レビュー、評価し、変更を管理する。 目的 供給者との合意に沿って、合意したレベルの情報セキュリティ及びサービス提供を維持するため。		15.2	供給者のサービス提供の管理 管理目的：供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。
						15.2.1	供給者のサービス提供の監視及びレビュー 組織は、供給者のサービス提供を定常的に監視し、レビュー、監査する。
						15.2.2	供給者のサービス提供の変更に対する管理 関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む）を管理する。
5.22.1	供給者の情報セキュリティの活動及びサービス提供を監視し、レビューし、変更を管理する。	供給者のサービスを監視し、レビューし、変更管理することによって、次の点を確実にする。 a) 合意における情報セキュリティの条件の順守 b) 情報セキュリティのインシデント及び問題の適切な管理 c) 供給者のサービスの変更又は事業状況の変化がサービス提供に影響を与えないこと。 供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 a) 合意の順守を検証するために、サービスのパフォーマンスレベルを監視する。 b) 次の事項を含む供給者による変更を監視する。 1) 現在提供されているサービスの強化 2) 新しいアプケーション及びシステムの開発 3) 組織の購力計及び購手順の、変更又は更新 4) 情報セキュリティインシデントの解決及び情報セキュリティの改善のための、新たな又は変更した管理策 c) 次の事項を含む供給者サービスの変更を監視する。 1) ネットワークの変更及び強化 2) 新技術の利用 3) 新製品又は新しい版若しくはリリースの採用 4) 新たな開発ツール及び開発環境 5) サービス設備の物理的設置場所の変更 6) 下請負供給者の変更 7) 他の供給者への下請負契約 d) 供給者の作成したサービスの報告をレビューし、合意で求めている定期的な進捗会議を設定する。 e) 独立した監査人の報告書が入手できれば、これのレビュー併せて供給者及び下請負供給者の監査を実施し、特定された問題の追跡調査を行う。 f) 合意書並びに全ての附属の指針及び手順書の要求に従い、情報セキュリティインシデントの情報を提供し、その情報をレビューする。 g) 供給者の監査証跡、情報セキュリティ事象の記録、運用上の問題の記録、故障記録、障害履歴及び提供サービスに関連する事象の中断・阻害の記録をレビューする。 h) 特定された情報セキュリティ事象又はインシデントに対応し、管理する。 i) 情報セキュリティの ぱい 弱性を特定し、管理する。 j) 供給者とその供給者との間の供給者関係における情報セキュリティの側面をレビューする。 k) 供給者が、十分なサービス提供能力を維持すること、及び重大なサービスの不具合又は災害の後においても合意したサービス継続レベルが維持されることを確実にするように設計された実行可能な計画を維持すること（5.29、5.30、5.35、5.36及び6.14参照）。 l) 供給者が、順守をレビューし、合意の要求事項を実施する責任を割り当てることを確実にする。 m) 供給者が適切な情報セキュリティレベルを維持していることを定期的に評価する。	5d-5.22.1	供給者のサービスを監視し、レビューし、変更管理することによって、次の点を確実にする。 a) 合意における情報セキュリティの条件の順守	手引に関連記載あり	15.2.1.1	供給者のサービスを監視及びレビューすることによって、その合意における情報セキュリティの条件の順守、並びに情報セキュリティのインシデント及び問題の適切な管理を確実にする仕組みを整備する。
			5d-5.22.1	供給者のサービスを監視し、レビューし、変更管理することによって、次の点を確実にする。 b) 情報セキュリティのインシデント及び問題の適切な管理	手引に関連記載あり	15.2.1.15	組織は、報告プロセスを規定することで、セキュリティに関連した活動（例えば、変更管理、ぜい弱性識別、情報セキュリティインシデントの報告及び対応）の可視性を維持する。
			5d-5.22.1	供給者のサービスを監視し、レビューし、変更管理することによって、次の点を確実にする。 c) 供給者のサービスの変更又は事業状況の変化がサービス提供に影響を与えないこと。	手引に関連記載あり	–	（対応項なし）
			5d-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 a) 合意の順守を検証するために、サービスのパフォーマンスレベルを監視する。	手引に関連記載あり	15.2.1.2	供給者のサービスの監視及びレビューは、合意の順守を検証するために、サービスのパフォーマンスレベルを監視することを含める。
			5d-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 b) 次の事項を含む供給者による変更を監視する。 1) 現在提供されているサービスの強化 2) 新しいアプケーション及びシステムの開発 3) 組織の購力計及び購手順の、変更又は更新 4) 情報セキュリティインシデントの解決及び情報セキュリティの改善のための、新たな又は変更した管理策	手引に関連記載あり	15.2.2.2	供給者のサービス提供の変更に対する管理は、以下の4点を実施するために組織が行う変更を考慮して実施する。 1.現在提供されているサービスの強化 2.新しいアプケーション及びシステムの開発 3.組織の購力計及び購手順の、変更又は更新 4.情報セキュリティインシデントの解決及びセキュリティの改善のための、新たな又は変更した管理策
			5d-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 c) 次の事項を含む供給者サービスの変更を監視する。 1) ネットワークの変更及び強化 2) 新技術の利用 3) 新製品又は新しい版若しくはリリースの採用 4) 新たな開発ツール及び開発環境 5) サービス設備の物理的設置場所の変更 6) 下請負供給者の変更 7) 他の供給者への下請負契約	手引に関連記載あり	15.2.2.3	供給者のサービス提供の変更に対する管理は、以下の7点を実施するための供給者サービスにおける変更を考慮して実施する。 1.ネットワークに対する変更及び強化 2.新技術の利用 3.新製品又は新しい版・リリースの採用 4.新たな開発ツール及び開発環境 5.サービス設備の物理的設置場所の変更 6.供給者の変更 7.他の供給者への下請負契約
			5d-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 d) 供給者の作成したサービスの報告をレビューし、合意で求めている定期的な進捗会議を設定する。	手引に関連記載あり	15.2.1.3	供給者のサービスの監視及びレビューは、供給者の作成したサービスの報告をレビューし、合意で求めている定期的な進捗会議を設定することを含める。
			5d-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 e) 独立した監査人の報告書が入手できれば、これのレビュー併せて供給者及び下請負供給者の監査を実施し、特定された問題の追跡調査を行うこと。	手引に関連記載あり	15.2.1.4	供給者のサービスの監視及びレビューは、独立した監査人の報告書が入手できれば、供給者の作成したサービスの報告のレビュー併せて供給者の監査を実施し、特定された問題の追跡調査を行うことを含める。
			5d-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 f) 合意書並びに全ての附属の指針及び手順書の要求に従い、情報セキュリティインシデントの情報を提供し、その情報をレビューする。	手引に関連記載あり	15.2.1.5	供給者のサービスの監視及びレビューは、合意書並びに全ての附属の指針及び手順書の要求に従い、情報セキュリティインシデントの情報を提供し、その情報をレビューすることを含める。
			5d-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 g) 供給者の監査証跡、情報セキュリティ事象の記録、運用上の問題の記録、故障記録、障害履歴及び提供サービスに関連する事象の中断・阻害の記録をレビューする。	手引に関連記載あり	15.2.1.6	供給者のサービスの監視及びレビューは、供給者の監査証跡、情報セキュリティ事象の記録、運用上の問題の記録、故障記録、障害履歴及び提供サービスに関連する中断記録をレビューすることを含める。
			5d-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 h) 特定された情報セキュリティ事象又はインシデントに対応し、管理する。	手引に関連記載あり	15.2.1.7	供給者のサービスの監視及びレビューは、特定された問題の解決及び管理を実施することを含める。
			5d-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 j) 供給者とその供給者との間の供給者関係における情報セキュリティの側面をレビューする。	手引に関連記載あり	15.2.1.8	供給者のサービスの監視及びレビューは、供給者とその供給者との間の供給者関係における情報セキュリティの側面をレビューすることを含める。
			5d-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 k) 供給者が、十分なサービス提供能力を維持すること、及び重大なサービスの不具合又は災害の後においても合意したサービス継続レベルが維持されることを確実にするように設計された実行可能な計画を維持する。	手引に関連記載あり	15.2.1.9	供給者のサービスの監視及びレビューは、重大なサービスの不具合又は災害の後においても、合意したサービス継続レベルが維持されることを確実にするように設計された実行可能な計画とともに、供給者がサービス提供能力を維持することを確実にすることを含める。
			5d-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 l) 供給者が、順守をレビューし、合意の要求事項を実施する責任を割り当てる。	手引に関連記載あり	15.2.1.11	組織は、供給者が、順守状況のレビュー及び合意書における要求事項の実施について の責任を割り当てる。
5.22.2	供給者関係を管理及び監視する責任は、指定された個人又はチームに割り当て、監視するために十分な技術力及び人的資源を確保する。	供給者関係を管理する責任は、指定された個人又はチームに割り当てる。 合意書における要求事項、特に情報セキュリティに関する要求事項を満たしているかどうかを監視するために、十分な技術力及び人的資源を確保しておく。 サービスの提供において不完全な点があった場合は、適切な処置をとる。	5d-5.22.3	供給者関係を管理する責任は、指定された個人又はチームに割り当てる。	手引に関連記載あり	15.2.1.10	供給者関係を管理する責任は、指定された個人又はサービス管理チームに割り当てる。
			5d-5.22.4	合意書における要求事項、特に情報セキュリティに関する要求事項を満たしているかどうかを監視するために、十分な技術力及び人的資源を確保しておく。	手引に関連記載あり	15.2.1.12	組織は、合意書における要求事項、特に情報セキュリティに関する要求事項を満たしているかどうかを監視するために、十分な技術力及び人的資源を確保しておく。
			5d-5.22.5	サービスの提供において不完全な点があった場合は、適切な処置をとる。	手引に関連記載あり	15.2.1.13	組織は、サービスの提供において不完全な点があった場合に適切な処置をとる。
5.23	クラウドサービスの利用における情報セキュリティ 統制目標：クラウドサービスの調達、利用、管理及び利用終了のプロセスを、組織の情報セキュリティ要求事項に従って確立する。 目的：クラウドサービスの利用における情報セキュリティを規定し、管理するため。		5.23	クラウドサービスの利用における情報セキュリティ 管理策 クラウドサービスの調達、利用、管理及び利用終了のプロセスを、組織の情報セキュリティ要求事項に従って確立することが望ましい。 目的 クラウドサービスの利用における情報セキュリティを規定し、管理するため。			

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.23.1	ピアクラウドサービスの調達・利用・管理及び利用終了に関する方針を策定する。	組織はクラウドサービスの利用に関するトピック固有の方針を確立し、全ての関連する利害関係者に伝達する。 組織は、クラウドサービスの利用に伴う情報セキュリティリスクを管理する方法を定め、伝達する。これは、外部関係者が提供するサービスを、組織が管理する方法の既存の取組の拡張又はその一部である可能性がある（5.21及び5.22参照）。	5d-5.23.1	組織はクラウドサービスの利用に関するトピック固有の方針を確立し、全ての関連する利害関係者に伝達する。	手引に関連記載あり	–	（対応項なし）
			5d-5.23.2	組織は、クラウドサービスの利用に伴う情報セキュリティリスクを管理する方法を定め、伝達する。	手引に関連記載あり	–	（対応項なし）
			（5d-5.23.2参考）	これは、外部関係者が提供するサービスを、組織が管理する方法の既存の取組の拡張又はその一部である可能性がある。	手引に関連記載あり	–	（対応項なし）
5.23.2	ピアクラウドサービスの利用に伴う情報セキュリティ要求事項を定義する。	組織は次の事項を定義する。 a) クラウドサービスの利用に伴う全ての関係する情報セキュリティ要求事項 b) クラウドサービスの選定基準及びクラウドサービス利用の範囲 c) クラウドサービスの利用及び管理に関する役割及び責任 d) どの情報セキュリティ管理策をクラウドサービスプロバイダが管理し、どの情報セキュリティ管理策をクラウドサービスカスタマとしての組織が管理するか。 e) クラウドサービスプロバイダが提供する情報セキュリティ機能を取得し、利用する方法 f) クラウドサービスプロバイダが実施する情報セキュリティ管理策に関して保証を得る方法 g) 組織が複数のクラウドサービス、特に異なるクラウドサービスプロバイダのクラウドサービスを利用する場合に、管理策、インタフェース及びサービスの変更を管理する方法 h) クラウドサービスの利用に関連して発生する情報セキュリティインシデントを取り扱うための手順 i) 情報セキュリティリスクを管理するため、クラウドサービスの継続的な利用を監視し、レビュー、評価する組織の取組 j) クラウドサービスの出口戦略を含め、クラウドサービスの利用を変更又は停止する方法 取り扱う情報の移行及び取扱制限並びにクラウドサービス提供者との情報セキュリティに関する役割及び責任の範囲を踏まえて、クラウドサービスに求める情報セキュリティ対策を含むセキュリティ要件を定めること。 クラウドサービスの利用は、クラウドサービスプロバイダ、クラウドサービスカスタマである組織との間の、情報セキュリティに関する責任の共有及び分担、並びに共同作業を行う可能性がある。クラウドサービスプロバイダ、クラウドサービスカスタマである組織との両方の	5d-5.23.3	組織は次の事項を定義する。 a) クラウドサービスの利用に伴う全ての関係する情報セキュリティ要求事項 b) クラウドサービスの選定基準及びクラウドサービス利用の範囲 c) クラウドサービスの利用及び管理に関する役割及び責任 d) どの情報セキュリティ管理策をクラウドサービスプロバイダが管理し、どの情報セキュリティ管理策をクラウドサービスカスタマとしての組織が管理するか。 e) クラウドサービスプロバイダが提供する情報セキュリティ機能を取得し、利用する方法 f) クラウドサービスプロバイダが実施する情報セキュリティ管理策に関して保証を得る方法 g) 組織が複数のクラウドサービス、特に異なるクラウドサービスプロバイダのクラウドサービスを利用する場合に、管理策、インタフェース及びサービスの変更を管理する方法 h) クラウドサービスの利用に関連して発生する情報セキュリティインシデントを取り扱うための手順 i) 情報セキュリティリスクを管理するため、クラウドサービスの継続的な利用を監視し、レビュー、評価する組織の取組 j) クラウドサービスの出口戦略を含め、クラウドサービスの利用を変更又は停止する方法	手引に関連記載あり	–	（対応項なし）
5.23.3	定義された、ピアクラウドサービスの利用に伴う情報セキュリティ要求事項を踏まえ、合意をする。	クラウドサービスの合意は、多くの場合、事前に定義されており、交渉の余地はないことを踏まえ、全てのクラウドサービスについて、組織は、クラウドサービスプロバイダのクラウドサービスの合意をレビューする。 クラウドサービスの合意は、機密性、完全性、可用性及び情報の取扱いについての組織の要求事項、並びに、適切なクラウドサービスレベル目標及びクラウドサービスの定性的目標に言及する。 組織は、クラウドサービスの利用に関連するリスクを特定するために、関連するリスクアセスメントも実施する。 クラウドサービスの利用に関連する残留リスクは、組織の適切な管理層が明確に特定し、受容する。 クラウドサービスプロバイダと、クラウドサービスカスタマである組織との間の合意は、組織のデータ及びサービスの可用性を保護するために次の規定を含む。 a) アーキテクチャ及びインフラストラクチャに関する業界で認められた標準に基づくソリューションを提供する。 b) 組織の要求事項を満たすためにクラウドサービスのアクセス制御を管理する。 c) マルウェア監視及び保護ソリューションを実装する。 d) 組織の取扱いに関連を要する情報を、承認されている場所（例えば、特定の国又は地域）、又は特定の法域内若しくは特定の裁判権の下で処理し、保存する。 e) クラウドサービス環境で情報セキュリティインシデントが発生した場合に専用の支援を提供する。 f) クラウドサービスが、更に外部の供給者へ下請負契約されている場合に、組織の情報セキュリティ要求事項が満たされることを確実にする（又はクラウドサービスの下請負を禁止する。）。 g) 異なる法域にわたるディジタル証拠に関する法令及び規制を考慮して、ディジタル証拠を収集する際に組織を支援する。 h) 組織がクラウドサービスの利用を終了したいとき、適切な期間にわたって、適切な支援及びサービスを提供する。 i) クラウドサービスカスタマが利用するクラウドサービスプロバイダが提供する機能に基づいて、該当する場合に、データ及び構成情報の必要なバックアップを提供し、セキュリティを保った方法でバックアップを管理する。 j) サービスの提供中又はサービスの終了時に組織が要求する場合、クラウドサービスカスタマである組織が所有する構成ファイル、ソースコード、データなどの情報を提出し、返却する。 クラウドサービスを利用する組織は、クラウドサービスプロバイダと緊密な連絡を維持する。こうした連絡によって、クラウドサービスプロバイダ及びクラウドサービスカスタマである組織との両方が各サービスの特性を監視し、合意に含まれるユニットメントの不履行を取扱うサービス能力 を 可能にする。	5d-5.23.4	クラウドサービスの合意は、機密性、完全性、可用性及び情報の取扱いについての組織の要求事項、並びに、適切なクラウドサービスレベル目標及びクラウドサービスの定性的目標に言及する。	手引に関連記載あり	–	（対応項なし）
			5d-5.23.5	組織は、クラウドサービスの利用に関連するリスクを特定するために、関連するリスクアセスメントも実施する。	手引に関連記載あり	–	（対応項なし）
			5d-5.23.6	クラウドサービスの利用に関連する残留リスクは、組織の適切な管理層が明確に特定し、受容する。	手引に関連記載あり	–	（対応項なし）
			5d-5.23.7	クラウドサービスプロバイダと、クラウドサービスカスタマである組織との間の合意は、組織のデータ及びサービスの可用性を保護するために次の規定を含む。 a) アーキテクチャ及びインフラストラクチャに関する業界で認められた標準に基づくソリューションを提供する。 b) 組織の要求事項を満たすためにクラウドサービスのアクセス制御を管理する。 c) マルウェア監視及び保護ソリューションを実装する。 d) 組織の取扱いに関連を要する情報を、承認されている場所、又は特定の法域内若しくは特定の裁判権の下で処理し、保存する。 e) クラウドサービス環境で情報セキュリティインシデントが発生した場合に専用の支援を提供する。 f) クラウドサービスが、更に外部の供給者へ下請負契約されている場合に、組織の情報セキュリティ要求事項が満たされることを確実にする（又はクラウドサービスの下請負を禁止する。）。 g) 異なる法域にわたるディジタル証拠に関する法令及び規制を考慮して、ディジタル証拠を収集する際に組織を支援する。 h) 組織がクラウドサービスの利用を終了したいとき、適切な期間にわたって、適切な支援及びサービスを提供する。 i) クラウドサービスカスタマである組織が利用するクラウドサービスプロバイダが提供する機能に基づいて、該当する場合に、データ及び構成情報の必要なバックアップを提供し、セキュリティを保った方法でバックアップを管理する。 j) サービスの提供中又はサービスの終了時に組織が要求する場合、クラウドサービスカスタマである組織が所有する構成ファイル、ソースコード、データなどの情報を提出し、返却する。	手引に関連記載あり	–	（対応項なし）
			5d-5.23.9	クラウドサービスを利用する組織は、クラウドサービスプロバイダと緊密な連絡を維持する。	手引に関連記載あり	–	（対応項なし）
5.23.4	ピアクラウドサービスプロバイダから自組織へのサービス提供方法に対して、実質的にクラウドサービス利用者に影響を与える変更を行う前にピアクラウドサービスプロバイダが事前に通知することを、合意において要求するか検討し、記録に残す。	クラウドサービスカスタマである組織は、組織へのサービス提供方法に対して、実質的に顧客に影響を与える変更を行う前にクラウドサービスプロバイダが事前に通知することを合意において要求することが望ましいかどうかを、次の事項を踏まえて考慮する。 a) クラウドサービスの提供に影響するようなサービスを変更するような技術インフラストラクチャの変更（例えば、再配置、再構成、又はハードウェア若しくはソフトウェアの変更） b) 新しい地理的又は法的区域での情報の処理又は保存 c) ピアクラウドサービスプロバイダ又はその他の下請負業者の利用（既存の業者の変更又は新しい業者の利用を含む。）	5d-5.23.8	クラウドサービスカスタマである組織は、組織へのサービス提供方法に対して、実質的に顧客に影響を与える変更を行う前にクラウドサービスプロバイダが事前に通知することを合意において要求することが望ましいかどうかを、次の事項を含めて考慮する。 a) クラウドサービスの提供に影響するようなサービスを変更するような技術インフラストラクチャの変更 b) 新しい地理的又は法的区域での情報の処理又は保存 c) ピアクラウドサービスプロバイダ又はその他の下請負業者の利用（既存の業者の変更又は新しい業者の利用を含む。）	手引に関連記載あり	–	（対応項なし）
5.24	情報セキュリティインシデント管理の計画策定及び準備 統制目標：組織は、情報セキュリティインシデント管理のプロセス、役割及び責任を定め、確立し、伝達することによって、情報セキュリティインシデント管理を計画し、準備する。 目的：情報セキュリティ事象に関する伝達を含む、情報セキュリティインシデントへの迅速で、効果的で、一貫性があり、かつ、秩序のある対応を確実にするため。		5.24	情報セキュリティインシデント管理の計画策定及び準備 管理策 組織は、情報セキュリティインシデント管理のプロセス、役割及び責任を定め、確立し、伝達することによって、情報セキュリティインシデント管理を計画し、準備する。 目的 情報セキュリティ事象に関する伝達を含む、情報セキュリティインシデントへの迅速で、効果的で、一貫性があり、かつ、秩序のある対応を確実にするため。		16	情報セキュリティインシデント管理
						16.1	情報セキュリティインシデントの管理及びその改善 管理目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。
						16.1.1	責任及び手順 情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立する。
5.24.1	情報セキュリティインシデント管理プロセスを整備する。	組織は、適切な情報セキュリティインシデント管理プロセスを確立する。 情報セキュリティインシデント管理プロセスを確立する際には、次の事項を考慮する。 a) 連絡先を含め、情報セキュリティ事象を報告するための共通の方法を確立する（6.8参照）。 b) 管理、文書化、検知、トリージ、優先順位付け、分析、伝達及び利害関係者の調整を含む、組織が情報セキュリティインシデントを管理する機能を備えるためのインシデント管理プロセスを確立する。 c) 情報セキュリティインシデントを評価し、それに対応し、そこから学習する機能を組織が備えるためのインシデント対応プロセスを確立する。 d) 組織内で、情報セキュリティインシデントに関連する事項は、力量のある要員だけが取り扱えるように する。要員には、文書化した手順及び定期的な訓練を提供する。 e) インシデントに対応する要員に必要な訓練、認証及び継続的な専門能力開発を特定するプロセスを確立する。	5e-5.24.1	組織は、適切な情報セキュリティインシデント管理プロセスを確立する。	管理策に関連記載あり	–	（対応項なし）
			5e-5.24.3	情報セキュリティインシデント管理プロセスを確立する際には、次の事項を考慮する。 a) 連絡先を含め、情報セキュリティ事象を報告するための共通の方法を確立する。 b) 管理、文書化、検知、トリージ、優先順位付け、分析、伝達及び利害関係者の調整を含む、組織が情報セキュリティインシデントを管理する機能を備えるためのインシデント管理プロセスを確立する。 c) 情報セキュリティインシデントを評価し、それに対応し、そこから学習する機能を組織が備えるためのインシデント対応プロセスを確立する。 d) 組織内で、情報セキュリティインシデントに関連する事項は、力量のある要員だけが取り扱えるように する。そうした要員には、文書化した手順及び定期的な訓練を提供する。 e) インシデントに対応する要員に必要な訓練、認証及び継続的な専門能力開発を特定するプロセスを確立する。	手引に関連記載あり	16.1.1.2	情報セキュリティインシデント管理に関する管理層の責任及び手順について、確立する手順においては、以下の4点を確実にする。 1.組織内の情報セキュリティインシデントに関連する事項は、力量のある要員及び取り扱う。 2.セキュリティインシデントの対応と報告に関する助言と支援を提供する。 3.セキュリティインシデントを検知及び報告する場合の連絡先を定める。 4.情報セキュリティインシデントに関連した事項を取り扱う関係当局、外部の利益団体又は会議との適切な連絡（署吉、動吉、指示を含む。）を保つ。
			5e-5.24.6	これらの目的及び優先順位を満たすようにインシデント管理手順を実施する。	手引に関連記載あり	–	（対応項なし）
			5e-5.24.7	経営陣は、次の活動のためにそれぞれのシナリオ及び手順が作成され、実施されていることを考慮して、情報セキュリティインシデント管理計画の作成を確実にする。 a) 何が情報セキュリティインシデントに該当するかに関する基準に従った情報セキュリティ事象の評価 b) 情報セキュリティ事象及び情報セキュリティインシデントの監視、検知、分類、分析及び報告 c) インシデントの種類及びカテゴリに従った、対応及びエスカレーション、危機管理の発動及び継続計画の発動の可能性、インシデントからの管理された回復、並びに内部及び外部の利害関係者への伝達を含む、情報セキュリティインシデントの終結までの管理 d) 関係当局、外部の利益団体及び会議、供給者、顧客など、内部及び外部の利害関係者との調整 e) インシデント管理活動のログ取得 f) 証拠の取扱い g) 根本原因分析又は事後分析手順 h) 学んだ教訓及びインシデント管理手順又は一般的な情報セキュリティ管理策についての必要な改善の特定	手引に関連記載あり	16.1.1.1	情報セキュリティインシデント管理に関する管理層の責任及び手順について、組織において、以下の7点の手順が確定され、十分に伝達されることを確実にするために、管理層の責任を確立する。 1.インシデント対応の計画及び準備のための手順 2.情報セキュリティ事象及び情報セキュリティインシデントを監視、検知、分析及び報告するための手順 3.インシデント管理活動のログを取得するための手順 4.法的証拠を扱うための手順 5.情報セキュリティ事象の評価及び決定のための手順、並びに情報セキュリティ弱点の評価のための手順 6.対応手順（段階的取扱い、インシデントからの回復の管理、並びに内部及び外部の要員又は組織への通知） 7.内部及び外部の要員又は組織への指示に関する対応手順には、定めた時間内での指示の履行又は指示の発行元への不履行の程度の通知を含む。
5.24.2	情報セキュリティインシデント管理手順を実行するための役割及び責任を決定し、関連する内部及び外部の利害関係者に伝達する。	情報セキュリティインシデント管理手順を実行するための役割及び責任を決定し、関連する内部及び外部の利害関係者に伝達する。 クラウドサービス利用者は情報セキュリティインシデント管理の責任の割当て及び手順を定める。	5e-5.24.2	インシデント管理手順を実行するための役割及び責任を決定し、関連する内部及び外部の利害関係者に効果的に伝達する。	手引に関連記載あり	–	（対応項なし）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.24.3	情報セキュリティインシデント管理手順を整備する。	情報セキュリティインシデント管理の目的について、経営陣が同意している。 情報セキュリティインシデント管理について責任のある人々が、潜在的な結果及び重大度に基づく解決の時間枠を含む、組織が決めた情報セキュリティインシデントの取扱いの優先順位を理解していることを確実にする。 これらの目的及び優先順位を満たすようにインシデント管理手順を実施する。 経営陣は、次の活動のためにそれぞれのシナリオ及び手順が作成され、実施されていることを考慮して、情報セキュリティインシデント管理計画の作成を確実にする。 a) 何が情報セキュリティインシデントに該当するかに関する基準に従った情報セキュリティ事象の評価 b) 情報セキュリティ事象及び情報セキュリティインシデントの監視（8.15及び8.16参照）、検知（8.16参照）、分類（5.25参照）、分析及び報告（6.8参照）（人間又は自動的手段によって） c) インシデントの種類及びカテゴリに従った、対応及びエスカレーション（5.26参照）、危機管理の発動及び継続計画の発動の可能性、インシデントからの管理された回復、並びに内部及び外部の利害関係者への伝達を含む、情報セキュリティインシデントの終結までの管理 d) 関係当局、外部の利益団体及び会議、供給者、顧客など、内部及び外部の利害関係者との調整（5.5及び5.6参照） e) インシデント管理活動のログ取得 f) 証拠の取扱い（5.28参照） g) 根本原因分析又は事後分析手順 h) 学んだ教訓及びインシデント管理手順又は一般的な情報セキュリティ管理策についての必要な改善の特定	5e-5.24.4	情報セキュリティインシデント管理の目的について、経営陣が同意している。	手引に関連記載あり	16.1.1.4	情報セキュリティインシデント管理の目的について、経営陣の同意を得る。
			5e-5.24.5	情報セキュリティインシデント管理について責任ある人々が、潜在的な結果及び重大度に基づく解決の時間枠を含む、組織が決めた情報セキュリティインシデントの取扱いの優先順位を理解していることを確実にする。	手引に関連記載あり	16.1.1.5	情報セキュリティインシデント管理について責任ある人々に対し、組織が決めた情報セキュリティインシデントの取扱いの優先順位を確実に理解させる。
5.24.4	情報セキュリティインシデントの報告手順を整備する。	情報セキュリティ事象及び情報セキュリティインシデントの報告手順には、次の事項を含める。 a) 情報セキュリティ事象が発生した場合による処置（例えば、生じた誤動作、画面上の表示など）に関連する詳細全てを直ちに記録し、直ちに連絡先に報告し、協調した処置だけをとる。） b) 情報セキュリティインシデントを報告する際に要員が必要な全ての活動を実行できることを支援するためのインシデント書式の使用 c) 情報セキュリティ事象の報告吉に、その件が対処され、終結した後で、可能な限り結果を知らせることを確実にするための適切なフィードバックの手続 d) インシデント報告書の作成 インシデント管理手順を実施する際は、関連する利害関係者へ定められた時間内にインシデント報告する外部の要求事項（例えば、規制当局への侵害通知の要求事項）を考慮する。	5e-5.24.8	情報セキュリティ事象及び情報セキュリティインシデントの報告手順には、次の事項を含める。 a) 情報セキュリティ事象が発生した場合による処置 b) 情報セキュリティインシデントを報告する際に要員が必要な全ての活動を実行できることを支援するためのインシデント書式の使用 c) 情報セキュリティ事象の報告吉に、その件が対処され、終結した後で、可能な限り結果を知らせることを確実にするための適切なフィードバックの手続 d) インシデント報告書の作成	手引に関連記載あり	16.1.1.3	情報セキュリティインシデント管理に関する管理層の責任及び手順について、報告手順においては、以下の4点を含める。 1.情報セキュリティ事象が発生した場合に、報告作業を取り、報告する者が必要な全ての処置を忘れないよう手助けするための情報セキュリティ事象の報告書式の作成 2.情報セキュリティ事象が発生した場合による手順。例えば、詳細全て（不順守又は違反の形態、生じた誤動作、画面上の表示など）の記録を直ちにとる、直ちに連絡先に報告し、協調した処置だけをとる 3.セキュリティ違反を犯した従業員を処罰するために確立された正式な懲戒手続への言及 4.情報セキュリティ事象の報告者に、その件の処理が終結した後で結果を知らせることを確実にするための適切なフィードバックの手続
			5e-5.24.9	インシデント管理手順を実施する際は、関連する利害関係者へ定められた時間内にインシデント報告する外部の要求事項を考慮する。	手引に関連記載あり	–	（対応項なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.24.5	組織は、CSIRT（Computer Security Incident Response Team）を整備し、その役割を明確化する。	CSIRTに属する職員等として専門的な知識又は適性を有すると認められる者を選任する。 そのうち組織内における情報セキュリティインシデントに対処するための責任者として CSIRT責任者を置く。また、CSIRT内の業務統括及び外部との連携等を行う職員等及び役割を定める。 以下を例とする役割を定める。 a) CSIRTは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行う。 b) CSIRTは、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、関係への通報・連絡等を行う。 c) CSIRTは、情報セキュリティインシデントに関する対処状況を把握し、対処全般に関する指示、助言又は助言を行う。 d) CSIRTは、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システムセキュリティ責任者へ確認を指示する。 e) CSIRTは、情報セキュリティインシデントに関する対処の内容を記録する。	–	（統一基準由来）	令和7年版にて追加（情報セキュリティ管理基準以外の由来）	–	（対応項なし）
5.24.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.25	情報セキュリティ事象の評価及び決定 統制目標：組織は情報セキュリティ事象を評価し、それらを情報セキュリティインシデントに分類する方法を決定する。 目的：情報セキュリティ事象の効果的な分類及び優先順位付けを確実にするため。		5.25	情報セキュリティ事象の評価及び決定 管理策 組織は情報セキュリティ事象を評価し、それらを情報セキュリティインシデントに分類する方法を決定する。 目的 情報セキュリティ事象の効果的な分類及び優先順位付けを確実にするため。		16.1.4	情報セキュリティ事象の評価及び決定 情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定する。
5.25.1	情報セキュリティインシデント対応を目的とする情報セキュリティ事象の分類及び優先順位付けの体系を定義する。	インシデントの結果及び優先順位を特定するために、情報セキュリティインシデントの分類及び優先順位付けの体系について合意する。 体系には、事象を情報セキュリティインシデントに分類する基準を含める。	5e-5.25.1	インシデントの結果及び優先順位を特定するために、情報セキュリティインシデントの分類及び優先順位付けの体系について合意する。	手引に関連記載あり	16.1.4.1	連絡先の者は、合意された情報セキュリティ事象・情報セキュリティインシデントの分類基準を用いて各情報セキュリティ事象を評価し、その事象を情報セキュリティインシデントに分類するか否かを決定する。
5.25.2	情報セキュリティインシデントの分類及び優先順位付けの体系に基づき、情報セキュリティ事象を評価し、評価及び決定の結果を記録する。	連絡の窓口は、合意した体系を使用して、各情報セキュリティ事象を評価する。 情報セキュリティインシデントの調整及び対応に責任を負う要員は、評価を実行し、情報セキュリティ事象に関する決定をする。 評価及び決定の結果は、以後の参照及び検証のために詳細に記録しておく。	5e-5.25.5	評価及び決定の結果は、以後の参照及び検証のために詳細に記録しておく。	手引に関連記載あり	16.1.4.2	評価及び決定の結果は、以後の参照及び検証のために詳細に記録する。
5.26	情報セキュリティインシデントへの対応 統制目標：情報セキュリティインシデントは、文書化した手順に従って対応する。 目的：情報セキュリティインシデントへの効率的かつ効果的な対応を確実にするため。		5.26	情報セキュリティインシデントへの対応 管理策 情報セキュリティインシデントは、文書化した手順に従って対応する。 目的 情報セキュリティインシデントへの効率的かつ効果的な対応を確実にするため。		16.1.5	情報セキュリティインシデントへの対応 情報セキュリティインシデントは、文書化した手順に従って対応する。
5.26.1	情報セキュリティインシデントを、文書化した手順に従って対応する。	組織は、情報セキュリティインシデント対応に関する手順を確立し、それを全ての関連する利害関係者に伝達する。 情報セキュリティインシデントは、必要な力量をもつ指定されたチームが対応する（5.24参照）。 情報セキュリティインシデントへの対応策には、次の事項を含める。 a) インシデントの結果が拡がる可能性がある場合は、インシデントの影響を受けるシステムを含める。 b) 情報セキュリティインシデントの発生後、できるだけ速やかに証拠（5.28参照）を収集する。 c) 必要に応じて、危機管理活動及び場合によっては事業継続計画の発動を含むエスカレーションを行う（5.29及び5.30参照）。 d) 後で行う分析のために、関連する全ての対応活動を適正に記録することを確実にする。 e) 知る必要性の原則に従って全ての関連する内部及び外部の利害関係者に対し、情報セキュリティインシデントの存在又は関連するその詳細を伝達する。 f) 対応の有効性を改善し、他の組織への影響を最小限にする助けとするために、関係当局、外部の利益団体及び会議、供給者、顧客などの内部及び外部の関係者と調整する。 g) インシデントへの対処が漏りなく満んだ後、正式にそれを終了し、記録する。 h) 必要に応じて、情報セキュリティのフォレンジック分析を実施する（5.28参照）。 i) 根本原因を特定するために、インシデント後の分析を実施する。それが定められた手順に従って文書化され、伝達されることを確実にする（5.27参照）。 j) インシデントを引き起こし、インシデントの一因となり、又はインシデントの防止に失敗した管理策に関連するものを含む、情報セキュリティのぜい弱性及び弱点を特定し、管理する。 情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、組織の情報セキュリティ責任者に報告する。	5e-5.26.1	組織は、情報セキュリティインシデント対応に関する手順を確立し、それを全ての関連する利害関係者に伝達する。	手引に関連記載あり	–	（対応項なし）
			5e-5.26.2	情報セキュリティインシデントには、必要な力量をもつ指定されたチームが対応する。	手引に関連記載あり	16.1.5.1	情報セキュリティインシデントには、指定された連絡先、及び組織又は外部関係者の他の関係する要員が対応する。
					手引に関連記載あり	17.1.2.1	組織は、必要な権限、経験及び力量を備えた要員を用い、中断・障害を引き起こす事象に備え、これを軽減し、これに対処するための十分な管理構造を確実に設ける。
					手引に関連記載あり	17.1.2.2	組織は、インシデントを管理し、情報セキュリティを維持するための責任、権限及び力量を備えたインシデント対応要員を確実に任命する。
			5e-5.26.3	情報セキュリティインシデントへの対応策には、次の事項を含める。 a) インシデントの結果が拡がる可能性がある場合は、インシデントの影響を受けるシステムを含める。	手引に関連記載あり	–	（対応項なし）
			5e-5.26.3	情報セキュリティインシデントへの対応策には、次の事項を含める。 b) 情報セキュリティインシデントの発生後、できるだけ速やかに証拠を収集する。	手引に関連記載あり	16.1.5.2	対応策には、情報セキュリティインシデントの発生後、できるだけ速やかに証拠を収集することを含める。
			5e-5.26.3	情報セキュリティインシデントへの対応策には、次の事項を含める。 c) 必要に応じて、危機管理活動及び場合によっては事業継続計画の発動を含むエスカレーションを行う。	手引に関連記載あり	16.1.5.4	対応策には、必要に応じて、段階的取扱い（escalation）を行うことを含める。
			5e-5.26.3	情報セキュリティインシデントへの対応策には、次の事項を含める。 d) 後で行う分析のために、関連する全ての対応活動を適正に記録することを確実にする。	手引に関連記載あり	16.1.5.5	対応策には、後で行う分析のために、関連する全ての対応活動を適正に記録することを確実にすることを含める。
			5e-5.26.3	情報セキュリティインシデントへの対応策には、次の事項を含める。 e) 知る必要性の原則に従って全ての関連する内部及び外部の利害関係者に対し、情報セキュリティインシデントの存在又は関連するその詳細を伝達することを含める。	手引に関連記載あり	16.1.5.6	対応策には、知る必要性を認められている内部・外部の他の要員又は組織に対し、情報セキュリティインシデントの存在又は関連するその詳細を伝達することを含める。
			5e-5.26.3	情報セキュリティインシデントへの対応策には、次の事項を含める。 f) 対応の有効性を改善し、他の組織への影響を最小限にする助けとするために、関係当局、外部の利益団体及び会議、供給者、顧客などの内部及び外部の関係者と調整する。 h) 必要に応じて、情報セキュリティのフォレンジック分析を実施する。	手引に関連記載あり	–	（対応項なし）
			5e-5.26.3	情報セキュリティインシデントへの対応策には、次の事項を含める。 g) インシデントへの対処が漏りなく満んだ後、正式にそれを終了し、記録する。	手引に関連記載あり	16.1.5.8	対応策には、インシデントへの対応が漏りなく満んだ後、正式にそれを終了し、記録することを含める。
			5e-5.26.3	情報セキュリティインシデントへの対応策には、次の事項を含める。 i) 根本原因を特定するため、インシデント後の分析を実施する。それが定められた手順に従って文書化され、伝達されることを確実にする。	手引に関連記載あり	16.1.5.9	インシデントの根本原因を特定するために、インシデント後の分析を実施する。
			5e-5.26.3	情報セキュリティインシデントへの対応策には、次の事項を含める。 j) インシデントを引き起こし、インシデントの一因となり、又はインシデントの防止に失敗した管理策に関連するものを含む、情報セキュリティのぜい弱性及び弱点を特定し、管理する。	手引に関連記載あり	16.1.5.7	対応策には、インシデントの原因又はインシデントの一因であることが判明した情報セキュリティ弱点に対処することを含める。
5.27	情報セキュリティインシデントからの学習 統制目標：情報セキュリティインシデントから得られた知識は、情報セキュリティ管理策を強化し、改善するために用いる。 目的：将来のインシデントの起こりやすさ又は影響を減らすため。		5.27	情報セキュリティインシデントからの学習 管理策 情報セキュリティインシデントから得られた知識は、情報セキュリティ管理策を強化し、改善するために用いる。 目的 将来のインシデントの起こりやすさ又は影響を減らすため。		16.1.6	情報セキュリティインシデントからの学習 情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いる。
5.27.1	情報セキュリティインシデントから得た情報を、情報セキュリティ管理策の強化及び改善に使用する。	組織は情報セキュリティインシデントの形態、規模及び費用を定量化し、監視するための手順を確立する。 情報セキュリティインシデントの評価から得た情報は、次の目的で使用する。 a) インシデントのシナリオ及び手順を含むインシデント管理計画を強化する（5.24参照）。 b) 情報セキュリティリスクアセスメントを更新し、将来の同様のインシデントの起こりやすさ又は影響を減らすために必要な追加の管理策を決定し、実施するために、再発する又は重大なインシデント及びそれらの原因を特定する。これを可能にする仕組みには、インシデントの形態、規模及び費用に関する情報の収集、定量化及び監視を含む。 c) 発生し得るインシデントの事例、こうしたインシデントへの対応方法の事例、及び以後これらを回避するための方法の事例を示すことによって、利用者の意識向上及び訓練（6.3参照）を強化する。	5e-5.27.1	組織は情報セキュリティインシデントの形態、規模及び費用を定量化し、監視するための手順を確立する。	手引に関連記載あり	16.1.6.1	情報セキュリティインシデントの形態、規模及び費用を定量化及び監視できるようにする仕組みを備える。
			5e-5.27.2	情報セキュリティインシデントの評価から得た情報は、次の目的で使用する。 a) インシデントのシナリオ及び手順を含むインシデント管理計画を強化する。 b) 組織の情報セキュリティリスクアセスメントを更新し、将来の同様のインシデントの起こりやすさ又は影響を減らすために必要な追加の管理策を決定し、実施するために、再発する又は重大なインシデント及びそれらの原因を特定する。これを可能にする仕組みには、インシデントの形態、規模及び費用に関する情報の収集、定量化及び監視を含む。 c) 発生し得るインシデントの事例、こうしたインシデントへの対応方法の事例、及び以後これらを回避するための方法の事例を示すことによって、利用者の意識向上及び訓練を強化する。	手引に関連記載あり	16.1.6.2	情報セキュリティインシデントの評価から得た情報は、再発する又は影響の大きいインシデントを特定するために利用する。
5.28	証拠の収集 統制目標：組織は、情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための手順を確立し、実施する。 目的：懲戒処置及び法的処置の目的で、情報セキュリティインシデントに関連する証拠の一貫した効果的な管理を確実にするため。		5.28	証拠の収集 管理策 組織は、情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための手順を確立し、実施する。 目的 懲戒処置及び法的処置の目的で、情報セキュリティインシデントに関連する証拠の一貫した効果的な管理を確実にするため。		16.1.7	証拠の収集 組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用する。
5.28.1	懲戒処置及び法的処置のために情報セキュリティ事象に関連する証拠を取り扱う場合の手順を整備する。	懲戒処置及び法的処置のために情報セキュリティ事象に関連する証拠を取り扱う場合は、内部の手順を定めてそれに従う。 法的処置のために情報セキュリティ事象に関連して取り扱われる証拠は、関連する法域において受容される可能性を最大にするために、異なる幾つかの法域の要求事項を考慮する。 情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための証拠の管理に関する手順では、各種の記憶媒体、装置・機器及び装置・機器の状態（すなわち、電源が入っている か、切れている か）に従って、証拠の特定、収集、取得及び保存の指示を規定する。	5e-5.28.1	懲戒処置及び法的処置のために情報セキュリティ事象に関連する証拠を取り扱う場合は、内部の手順を定めてそれに従う。	手引に関連記載あり	16.1.7.1	懲戒処置及び法的処置のために証拠を取り扱う場合は、内部の手順を定め、それに従う。
			5e-5.28.2	法的処置のために情報セキュリティ事象に関連して取り扱われる証拠は、関連する法域において受容される可能性を最大にするために、異なる幾つかの法域の要求事項を考慮する。	手引に関連記載あり	16.1.7.12	懲戒処置及び法的処置に関連する幾つかの法域にまたがる証拠の利用の可能性を最大にするために、それらの異なる法域の要求事項を確認する。
			5e-5.28.3	情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための証拠の管理に関する手順では、各種の記憶媒体、装置・機器及び装置・機器の状態（すなわち、電源が入っている か、切れている か）に従って、証拠の特定、収集、取得及び保存の指示を規定する。	手引に関連記載あり	16.1.7.2	懲戒処置及び法的処置のために証拠を取り扱う手順では、各種の媒体、装置及び装置の状態（例えば、電源が入っている か、切れている か）に従って、証拠の特定、収集、取得及び保存のプロセスを規定する。
5.28.2	情報セキュリティ事象に関連する証拠を収集、取得及び保存する。	証拠は原則として、適切な国内法廷又は別の懲戒会議において受容される方法で収集し、次の事項を示す。 a) 記録は完全で、いかなる方法でも改ざんされていない。 b) 電子証拠の複製は原本と同一であることが確立される。 c) 証拠の収集元である情報システムは、証拠を記録した時点で正しく機能していた。 保存した証拠の価値を強化するために、入手可能であれば、要員及びツールの適格性を示す証明書又はその他適切な手段を追求する。 ディジタル証拠が組織の枠又は法域を越える場合、組織はお要とされる情報をディジタル証拠として収集することが法的に認められていることを確認する。	5e-5.28.4	証拠は原則として、適切な国内法廷又は別の懲戒会議において受容される方法で収集し、次の事項を示す。 a) 記録は完全で、いかなる方法でも改ざんされていない。 b) 電子証拠の複製は原本と同一であることが確立される。 c) 証拠の収集元である情報システムは、証拠を記録した時点で正しく機能していた。	手引に関連記載あり	16.1.7.4	懲戒処置及び法的処置のために証拠を取り扱う手順では、証拠の保全を行うプロセスを規定する。
			5e-5.28.5	保存した証拠の価値を強化するために、入手可能であれば、要員及びツールの適格性を示す証明書又はその他適切な手段を追求する。	手引に関連記載あり	16.1.7.10	保存された証拠の価値を強化するために、要員及びツールの適格性を示す証明書又はその他適切な手段を追及する。
			5e-5.28.6	ディジタル証拠が組織の枠又は法域を越える場合、組織はお要とされる情報をディジタル証拠として収集することが法的に認められていることを確認する。	手引に関連記載あり	16.1.7.11	懲戒処置及び法的処置に必要な法的証拠が、組織の枠又は法域を越える場合、組織はお要とされる情報を法的証拠として収集することが法的に認められていることを確認する。
5.28.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.29	事業の中断・阻害時の情報セキュリティ 統制目標：組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持するカ法を計画する。 目的：事業の中断・阻害時に情報及びその他の関連資産を保護するため。		5.29	事業の中断・阻害時の情報セキュリティ 管理策 組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画する。 目的 事業の中断・阻害時に情報及びその他の関連資産を保護するため。		17	事業継続マネジメントにおける情報セキュリティの側面
						17.1	情報セキュリティ継続 管理目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。
						17.1.1	情報セキュリティの継続の計画 組織は、困難な状況（adverse situation）（例えば、危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定する。
						17.1.2	情報セキュリティ継続の実施 組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持する。
						17.1.3	情報セキュリティ継続の検証、レビュー及び評価 確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、組織は、定められた間隔でこれらの管理策を検証する。
5.29.1	事業の中断・阻害時に情報セキュリティ管理策を適応させるための要求事項を定義する。	組織は、事業の中断・阻害時に情報セキュリティ管理策を適応させるための自らの要求事項を決定する。 情報セキュリティ要求事項は、事業継続マネジメントプロセスに含める。	5F-5.29.1	組織は、事業の中断・阻害時に情報セキュリティ管理策を適応させるための自らの要求事項を決定する。	手引に関連記載あり	17.1.1.2	組織は、事業継続及び災害復旧に関する計画を立てる場合に、情報セキュリティ要求事項を定める。
			5F-5.29.2	情報セキュリティ要求事項は、事業継続マネジメントプロセスに含める。	手引に関連記載あり	17.1.1.1	組織は、情報セキュリティの継続が事業継続マネジメント（以下「BCM」という。）プロセス又は災害復旧管理（以下「DRM」という。）プロセスに織り込まれているか否かを判断する。
5.29.2	中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するために、計画を策定する。	中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するために、計画を策定し、実施し、試験し、レビュー、評価する。 情報のセキュリティは、必要なレベル及び必要な時間内に復旧する。 組織は次の事項を実施し、維持する。 a) 事業継続計画及び/ICT継続計画における情報セキュリティ管理策、支援システム及び/ツール b) 事業の中断・阻害時に既存の情報セキュリティ管理策を維持するためのプロセス c) 事業の中断・阻害時に維持できない情報セキュリティ管理策を補う管理策	5F-5.29.3	中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するために、計画を策定し、実施し、試験し、レビュー、評価する。	手引に関連記載あり	17.1.2.3	組織は、経営陣が承認した情報セキュリティ継続の目的に基づいて、組織が中断・阻害を引き起こす事象を管理し、その情報セキュリティを既定のレベルに維持する場合の方法を計画及び手順に詳細に記して、計画、対応及び回復の文書化した手順を確実に策定し、これらを承認する。
			5F-5.29.4	情報のセキュリティは、必要なレベル及び必要な時間内に復旧する。	手引に関連記載あり	–	（対応項なし）
			5F-5.29.5	組織は次の事項を実施し、維持する。 a) 事業継続計画及び/ICT継続計画における情報セキュリティ管理策、支援システム及び/ツール	手引に関連記載あり	17.1.2.4	組織は、情報セキュリティ継続に関する要求事項に従って、事業継続又は災害復旧のための方針及び/手順、並びにこれらを支援するシステム及び/ツールにおける情報セキュリティ管理策を確立し、文書化し、実施し、維持する。
			5F-5.29.5	組織は次の事項を実施し、維持する。 b) 事業の中断・阻害時に既存の情報セキュリティ管理策を維持するためのプロセス	手引に関連記載あり	17.1.2.5	組織は、情報セキュリティ継続に関する要求事項に従って、困難な状況において既存の情報セキュリティ管理策を維持するための、プロセス及び/手順の変更並びにそれらの実施の変更を確立し、文書化し、実施し、維持する。
			5F-5.29.5	組織は次の事項を実施し、維持する。 c) 事業の中断・阻害時に維持できない情報セキュリティ管理策を補う管理策	手引に関連記載あり	17.1.2.6	組織は、情報セキュリティ継続に関する要求事項に従って、困難な状況において維持することが不可能な情報セキュリティ管理策を補うための管理策を確立し、文書化し、実施し、維持する。
5.29.3	中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するための計画を試験する。	5.29.2を参照	5F-5.29.3	【再】中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するために、計画を策定し、実施し、試験し、レビュー、評価する。	手引に関連記載あり	17.1.3.1	運用に関するものか、継続に関するものかを問わず、組織、技術、手順及び/プロセスの変更が、情報セキュリティ継続に関する要求事項の変更につながる場合、変更後の要求事項に照らして、情報セキュリティのためのプロセス、手順及び/管理策の継続性をレビューする。
					手引に関連記載あり	17.1.3.2	組織は、情報セキュリティ継続のためのプロセス、手順及び/管理策の機能が情報セキュリティ継続の目的と整合していることを確実にするために、これらの機能を実行し、試験する。
5.30	事業継続のためのICTの備え 統制目標：事業継続の目的及び/ICT継続の要求事項に基づいて、ICTの備えを計画し、実施し、維持し、試験する。 目的：事業の中断・阻害時に組織の情報及びその他の関連資産の可用性を確実にするため。		5.30	事業継続のためのICTの備え 管理策 事業継続の目的及び/ICT継続の要求事項に基づいて、ICTの備えを計画し、実施し、維持し、試験することが望ましい。 目的 事業の中断・阻害時に組織の情報及びその他の関連資産の可用性を確実にするため。		–	（対応項なし）
5.30.1	事業継続の目的及び/ICT継続の要求事項に基づいて、ICTの備えを計画する。	事業継続に関するICTの備えは、事業の中断・阻害時にも組織の目的が継続して満たされることを確実にするための、事業継続マネジメント及び/情報セキュリティマネジメントの重要な構成要素である。 ICT継続の要求事項を、事業影響度分析（BIA）の結果をもとに規定する場合、その/BIAプロセスでは、影響の種類及び/評価基準を用いて、製品及び/サービスを提供する事業活動の中断・阻害から生じる影響を経時的に評価する。 事業の中断・阻害の結果として生じる影響の大きさ及び/期間を用いて優先する活動を特定し、これに目標復旧時間（RTO）を設定した後、BIAでは、優先する活動の支援にどの資源が必要かを決定する。 優先する事業活動を支援する資源にもRTOを定め、これらの資源にの一部として/ICTサービスを含める。 ICTサービスに係るBIAを拡張して、事業の中断・阻害時の活動を支援するために必要な、ICTシステムのパフォーマンス、容量・能力の要求事項、及び/情報の目標復旧時点（RPO）を定めることが可能である。 事業の中断・阻害の結果として生じる影響の大きさ及び/期間を用いて優先する活動を特定し、これに目標復旧時間（RTO）を設定した後、BIAでは、優先する活動の支援にどの資源が必要かを決定する。 優先する事業活動を支援する資源にもRTOを定め、これらの資源にの一部として/ICTサービスを含める。 ICTサービスに係るBIAを拡張して、事業の中断・阻害時の活動を支援するために必要な、ICTシステムのパフォーマンス、容量・能力の要求事項、及び/情報の目標復旧時点（RPO）を定めることが可能である。 ICTサービスに関するBIA及び/リスクアセスメントの結果に基づいて、組織は、事業の中断・阻害の前、中断・阻害中及び/中断・阻害の後の選択肢を考慮したICT継続戦略を特定し、選択する。 組織は、次の事項を確実にする。 a) 事業の中断・阻害に備え、それを緩和し、それに対応するために、必要な責任、権限及び/力量をもつ要員が支援する適切な組織構造を備えている。 b) 組織が/ICTサービスの中断・阻害を管理する方法を詳述した、対応及び/復旧手順を含む/ICT継続計画について、経営陣による承認を得る。 c) ICT継続計画は、次のICT継続に関する情報を含む。 1) BIAで特定した事業継続の要求事項及び/目的を満たすためのパフォーマンス及び容量・能力の仕様 2) 優先するICTサービスそれぞれのRTO及び/それらの構成要素を復旧する手順 3) 情報として定義された優先するICT資源のRPO及び/情報を復旧する手順 組織が/ICTサービスの中断・阻害を管理する方法を詳述した、対応及び/復旧手順を含む/ICT継続計画について、経営陣による承認を得る。	5F-5.30.1	ICT継続の要求事項を、事業影響度分析（BIA）の結果をもとに規定する場合、その/BIAプロセスでは、影響の種類及び/評価基準を用いて、製品及び/サービスを提供する事業活動の中断・阻害から生じる影響を経時的に評価する。	手引に関連記載あり	–	（対応項なし）
			5F-5.30.2	事業の中断・阻害の結果として生じる影響の大きさ及び/期間を用いて優先する活動を特定し、これに目標復旧時間（RTO）を設定した後、BIAでは、優先する活動の支援にどの資源が必要かを決定する。	手引に関連記載あり	–	（対応項なし）
			5F-5.30.3	優先する事業活動を支援する資源にもRTOを定め、これらの資源の一部として/ICTサービスを含める。	手引に関連記載あり	–	（対応項なし）
			5F-5.30.4	ICTサービスに関するBIA及び/リスクアセスメントの結果に基づいて、組織は、事業の中断・阻害の前、中断・阻害中及び/中断・阻害の後の選択肢を考慮したICT継続戦略を特定し、選択する。	手引に関連記載あり	–	（対応項なし）
			5F-5.30.5	ICTサービスに必要な可用性レベルを満たし、重要なプロセスの中断又は失敗後に求められる時間内に回復するために、この戦略に基づいて計画を作成し、実装し、試験する。	手引に関連記載あり	–	（対応項なし）
			5F-5.30.6	組織は、次の事項を確実にする。 a) 事業の中断・阻害に備え、それを緩和し、それに対応するために、必要な責任、権限及び/力量をもつ要員が支援する適切な組織構造を備えている。 b) 組織が/ICTサービスの中断・阻害を管理する方法を詳述した、対応及び/復旧手順を含む/ICT継続計画について、次を実施する。 1) 演習及び/テストを通じた定期的な評価 2) 経営陣による承認 c) ICT継続計画は、次のICT継続に関する情報を含む。 1) BIAで特定した事業継続の要求事項及び/目的を満たすためのパフォーマンス及び/容量・能力の仕様 2) 優先するICTサービスそれぞれのRTO及び/それらの構成要素を復旧する手順 3) 情報として定義された優先するICT資源のRPO及び/情報を復旧する手順	手引に関連記載あり	–	（対応項なし）
5.30.2	事業継続の目的及び/ICT継続の要求事項に基づいて、ICTの備えの試験をする。	ICTサービスに必要な可用性レベルを満たし、重要なプロセスの中断又は失敗後に求められる時間内に回復するために、この戦略に基づいて計画を作成し、実装し、試験する。事業継続戦略は、一つ以上のソリューションから成る可能性がある。 組織が/ICTサービスの中断・阻害を管理する方法を詳述した、対応及び/復旧手順を含む/ICT継続計画について、演習及び/テストを通じた定期的な評価を実施する。	5F-5.30.5	ICTサービスに必要な可用性レベルを満たし、重要なプロセスの中断又は失敗後に求められる時間内に回復するために、この戦略に基づいて計画を作成し、実装し、試験する。	手引に関連記載あり	–	（対応項なし）
			（5F-5.30.5参考）	事業継続戦略は、一つ以上のソリューションから成る可能性がある。	手引に関連記載あり	–	（対応項なし）
5.31	法令、規制及び/契約上の要求事項 統制目標：情報セキュリティに関連する法令、規制及び/契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組を特定し、文書化し、また、最新に保つ。 目的：情報セキュリティに関連する法令、規制及び/契約上の要求事項の順守を確実にするため。		5.31	法令、規制及び/契約上の要求事項 管理策 情報セキュリティに関連する法令、規制及び/契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組を特定し、文書化し、また、最新に保つ。 目的 情報セキュリティに関連する法令、規制及び/契約上の要求事項の順守を確実にするため。		18	順守
						18.1	法的及び/契約上の要求事項の順守 管理目的：情報セキュリティに関連する法的、規制又は/契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。
						18.1.1	適用法令及び/契約上の要求事項の特定 各情報システム及び/組織について、全ての関連する法令、規制及び/契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。
						18.1.5	暗号化機能に対する規制 暗号化機能は、関連する全ての協定、法令及び/規制を順守して用いる。
5.31.1	組織の情報セキュリティに関連する全ての法令及び/規制を特定し、自らの事業の種類に対する要求事項を特定し、維持する。	法令、規制又は契約上の要求事項を含む外部の要求事項は、次の場合に考慮に入れる。 a) 情報セキュリティの方針群及び/手順の策定 b) 情報セキュリティ管理策の設計、実施又は変更 c) 内部のニーズ又は供給者との合意のために情報セキュリティ要求事項を設定するプロセスの一部として、情報及びその他の関連資産の分類 d) 情報セキュリティリスクアセスメントの実施、及び/情報セキュリティリスク対応活動の決定 e) 情報セキュリティに関連する役割及び/責任に従ったプロセスの決定 f) 組織、並びに供給を受ける製品及び/サービスの範囲に関係する、供給者の契約上の要求事項の特定 組織は、次の事項を行う。 a) 自らの事業の種類に対する要求事項を認識するために、組織の情報セキュリティに関連する全ての法令及び/規制を特定する。 b) 組織が次のとおりである場合に、関連する全ての国における順守を考慮する。 1) 他国で事業を行っている。 2) 法令及び/規制が組織に影響を与える可能性がある、他国の製品及び/サービスを利用している。 3) 法令及び/規制が組織に影響を与える可能性がある、法域との境界を越えて情報の移転を行う。 c) 変更に追随し、新しい法令を特定するために、特定した法令及び/規制を定期的にレビューする。 d) これらの要求事項を満たすための/プロセス及び/個々の責任を定義し、文書化する。D110 情報セキュリティに関する契約上の要求事項には、次のものに記載されている要求事項を含める。 a) 顧客との契約 b) 供給者との契約（5.20参照） c) 保険契約	5g-5.31.1	法令、規制又は契約上の要求事項を含む外部の要求事項は、次の場合に考慮に入れる。 a) 情報セキュリティの方針群及び/手順の策定 b) 情報セキュリティ管理策の設計、実施又は変更 c) 内部のニーズ又は供給者との合意のために情報セキュリティ要求事項を設定するプロセスの一部として、情報及びその他の関連資産の分類 d) 情報セキュリティリスクアセスメントの実施、及び/情報セキュリティリスク対応活動の決定 e) 情報セキュリティに関連する役割及び/責任に従ったプロセスの決定 f) 組織、並びに供給を受ける製品及び/サービスの範囲に関係する、供給者の契約上の要求事項の特定	手引に関連記載あり	18.1.1.1	各情報システム及び/組織について、全ての関連する法令、規制及び/契約上の要求事項を満たすための具体的な管理策及び/具体的な責任について定め、文書化する。
			5g-5.31.2	組織は、次の事項を行う。 a) 自らの事業の種類に対する要求事項を認識するために、組織の情報セキュリティに関連する全ての法令及び/規制を特定する。	手引に関連記載あり	18.1.1.2	管理者は、事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。
			5g-5.31.2	組織は、次の事項を行う。 b) 組織が次のとおりである場合に、関連する全ての国における順守を考慮する。 – 他国で事業を行っている。 – 法令及び/規制が組織に影響を与える可能性がある、他国の製品及び/サービスを利用している。 – 法令及び/規制が組織に影響を与える可能性がある、法域との境界を越えて情報の移転を行う。	手引に関連記載あり	18.1.1.3	組織が他の国で事業を営む場合には、管理者は、関連する全ての国における法令、規制及び/契約上の要求事項を順守する。
			5g-5.31.2	組織は、次の事項を行う。 c) 変更に追随し、新しい法令を特定するために、特定した法令及び/規制を定期的にレビューする。	手引に関連記載あり	–	（対応項なし）
			5g-5.31.2	組織は、次の事項を行う。 d) これらの要求事項を満たすための/プロセス及び/個々の責任を定義し、文書化する。	手引に関連記載あり	18.1.1.1	各情報システム及び/組織について、全ての関連する法令、規制及び/契約上の要求事項を満たすための具体的な管理策及び/具体的な責任について定め、文書化する。
			5g-5.31.4	情報セキュリティに関する契約上の要求事項には、次のものに記載されている要求事項を含む。 a) 顧客との契約 b) 供給者との契約 c) 保険契約	手引に関連記載あり	–	（対応項なし）
5.31.2	暗号化に関連する合意、法令及び/規制における要求事項への順守を確実にするための手順を整備する。	暗号化は、次の項目に関連する合意、法令及び/規制の順守を考慮に入れる。 a) 暗号機能を実行するためのコンピュータのハードウェア及び/ソフトウェアの、輸入又は輸出に関する規制 b) 暗号機能を追加するように設計されているコンピュータのハードウェア及び/ソフトウェアの、輸入又は輸出に関する規制 c) 暗号利用に関する規制 d) 暗号化された情報への、国の当局による強制的又は任意のアクセス方法 e) デジタル署名、e/シール及びデジタル証明書の有効性 暗号化は、多くの場合、国有の法的要求事項をニつ以上受ける。関連する法令及び/規制の順守を確実にするために、特に暗号化された情報又は暗号化ツールを法域の境界を越えて転送する場合、法的な助言を求めることが推奨される。	5g-5.31.3	暗号化は、次の項目に関連する合意、法令及び/規制の順守を考慮に入れる。 a) 暗号機能を実行するためのコンピュータのハードウェア及び/ソフトウェアの、輸入又は輸出に関する規制	手引に関連記載あり	18.1.5.1	関連する協定、法令及び/規制を順守するため、暗号機能を実行するためのコンピュータのハードウェア及び/ソフトウェアの、輸入又は輸出に関する規制を順守する。
			5g-5.31.3	暗号化は、次の項目に関連する合意、法令及び/規制の順守を考慮に入れる。 b) 暗号機能を追加するように設計されているコンピュータのハードウェア及び/ソフトウェアの、輸入又は輸出に関する規制	手引に関連記載あり	18.1.5.2	関連する協定、法令及び/規制を順守するため、暗号機能を追加するように設計されているコンピュータのハードウェア及び/ソフトウェアの、輸入又は輸出に関する規制を順守する。
			5g-5.31.3	暗号化は、次の項目に関連する合意、法令及び/規制の順守を考慮に入れる。 c) 暗号利用に関する規制	手引に関連記載あり	18.1.5.3	関連する協定、法令及び/規制を順守するため、暗号利用に関する規制を順守する。
			5g-5.31.3	暗号化は、次の項目に関連する合意、法令及び/規制の順守を考慮に入れる。 d) 暗号化された情報への、国の当局による強制的又は任意のアクセス方法	手引に関連記載あり	18.1.5.4	関連する協定、法令及び/規制を順守するため、内容の機密性を守るためにハードウェア又はソフトウェアによって暗号化された情報への、国の当局による強制的又は任意的アクセス方法を変える。
			（5g-5.31.3参考2）	関連する法令及び/規制の順守を確実にするために、特に暗号化された情報又は暗号化ツールを法域の境界を越えて転送する場合、法的な助言を求めることが推奨される。	手引に関連記載あり	18.1.5.5	関連する法令及び/規制の順守を確実にするために、法的な助言を求める。
					手引に関連記載あり	18.1.5.6	暗号化された情報又は暗号制御機能を、法域を越えて持ち出す前に、法的な助言を受ける。
5.31.3	提供するサービス上で取り扱われる情報に対して国内法以外の法令及び/規制が適用された結果、クラウドサービス利用者の意図しないまま当該利用者の管理する情報にアクセスされ、又は処理されるリスクを評価して外部委託先を選定し、必要に応じてクラウドサービス利用者が扱う情報が取り扱われる場所及び/契約に定める準拠法・裁判管轄を指定する。	当該事業者が提供するサービス上で取り扱われる情報に対して国内法以外の法令及び/規制が適用された結果、クラウドサービス利用者の意図しないまま当該利用者の管理する情報にアクセスされ又は処理されるリスクを評価して外部委託先を選定し、必要に応じてクラウドサービス利用者が扱う情報が取り扱われる場所及び/契約に定める準拠法・裁判管轄を指定する。	–	（統一基準由来）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	15.1.1.16.B	当該事業者が提供するサービス上で取り扱われる情報に対して国内法以外の法令及び/規制が適用された結果、クラウドサービス利用者の意図しないまま当該利用者の管理する情報にアクセスされ、又は処理されるリスクを評価して外部委託先を選定し、必要に応じてクラウドサービス利用者が扱う情報が取り扱われる場所及び/契約に定める準拠法・裁判管轄を指定する。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.31.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.31.5	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
						（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.31.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.31.7	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.32	知的財産権 統制目標：組織は知的財産権を保護するための適切な手順を実施する。 目的：知的財産権及び権利関係のある製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするため。		5.32	知的財産権 管理策 組織は知的財産権を保護するための適切な手順を実施する。 目的 知的財産権及び権利関係のある製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするため。		18.1.2	知的財産権 知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施する。
5.32.1	知的財産権及び権利関係のある製品の利用に関連する、法令、規制、契約上の要求事項の順守に関する方針とプロセスを策定する。	知的財産となり得るものを保護するために、次の事項を考慮する。 a) 知的財産権の保護に関するトピック固有の方針を定め、伝達する。 b) ソフトウェア製品及び情報製品のコンプライアンスにのっとった利用を定めた、知的財産権の順守の手順を実行する。 c) 著作権を侵害しないことを確実にするために、ソフトウェアは、知名度の高い、かつ、定評のある供給元だけを通して取得する。 d) 適切な資産登録簿を維持管理し、知的財産権の保護が求められている全ての資産を特定する。 e) 使用許諾を得ていることの証明及び証拠、手引などを維持・管理する。 f) 使用許諾で許可された最大利用者数又は資源数（例えば、中央処理装置（CPU）など）を超過しないことを確実にする。 g) 認可されていないソフトウェア及び使用許諾されている製品だけが導入されていることを確実にするためのレビューを行う。 h) 適切な使用許諾条件を維持・管理するための手順を定める。 i) ソフトウェアの処分又は他人への譲渡についての手順を定める。 j) 公衆ネットワークから又は外部供給元から入手するソフトウェア及び情報の使用条件を順守する。 k) 著作権法又は適用される使用許諾が認めている場合を除いて、商用記録（ビデオ、録音）を複製、他形式に変換、又は放利しない。 l) 著作権法又は適用される使用許諾が認めている場合を除いて、規格（例えば、ISO/IEC規格）、書籍、記事、報告書又はその他文書の全部又は一部を複写しない。	5g-S.32.1	知的財産となり得るものを保護するために、次の事項を考慮する。 a) 知的財産権の保護に関するトピック固有の方針を定め、伝達する。	手引に関連記載あり	–	（対応項なし）
			5g-S.32.1	知的財産となり得るものを保護するために、次の事項を考慮する。 b) ソフトウェア製品及び情報製品のコンプライアンスにのっとった利用を定めた、知的財産権の順守の手順を実行する。	手引に関連記載あり	18.1.2.1	ソフトウェア製品及び情報製品の合法利用を明確に定めた知的財産権順守方針を公表する。
					手引に関連記載あり	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			5g-S.32.1	知的財産となり得るものを保護するために、次の事項を考慮する。 c) 著作権を侵害しないことを確実にするために、ソフトウェアは、知名度の高い、かつ、定評のある供給元だけを通して取得する。	手引に関連記載あり	18.1.2.2	著作権を侵害しないことを確実にするために、ソフトウェアは、知名度の高い、かつ、定評のある供給元だけを通して取得する。
			5g-S.32.1	知的財産となり得るものを保護するために、次の事項を考慮する。 d) 適切な資産登録簿を維持管理し、知的財産権の保護が求められている全ての資産を特定する。	手引に関連記載あり	18.1.2.4	適切な資産登録簿を維持・管理し、知的財産権の保護が求められている全ての資産を特定する。
			5g-S.32.1	知的財産となり得るものを保護するために、次の事項を考慮する。 e) 使用許諾を得ていることの証明及び証拠、手引などを維持・管理する。	手引に関連記載あり	18.1.2.5	使用許諾を得ていることの証明及び証拠、マスタディスク、手引などを維持・管理する。
			5g-S.32.1	知的財産となり得るものを保護するために、次の事項を考慮する。 g) 認可されていないソフトウェア及び使用許諾されている製品だけが導入されていることを確実にするためのレビューを行う。	手引に関連記載あり	18.1.2.7	認可されていないソフトウェア及び使用許諾されている製品だけが導入されていることのレビューを行う。
			5g-S.32.1	知的財産となり得るものを保護するために、次の事項を考慮する。 h) 適切な使用許諾条件を維持・管理するための手順を定める。	手引に関連記載あり	18.1.2.8	適切な使用許諾条件を維持・管理するための方針を定める。
			5g-S.32.1	知的財産となり得るものを保護するために、次の事項を考慮する。 i) ソフトウェアの処分又は他人への譲渡についての手順を定める。	手引に関連記載あり	18.1.2.9	ソフトウェアの処分又は他人への譲渡についての方針を定める。
			5g-S.32.1	知的財産となり得るものを保護するために、次の事項を考慮する。 j) 公衆ネットワーク及び外部供給元から入手するソフトウェア及び情報の使用条件を順守する。	手引に関連記載あり	18.1.2.10	公衆ネットワークから入手するソフトウェア及び情報の使用条件に従う。
			5g-S.32.1	知的財産となり得るものを保護するために、次の事項を考慮する。 k) 著作権法又は適用される使用許諾が認めている場合を除いて、商用記録（ビデオ、録音）を複製、他形式に変換、又は放利しない。	手引に関連記載あり	18.1.2.11	著作権法が認めている場合を除いて、商用記録（フィルム、録音）を複製、他形式に変換、又は放利しない。
			5g-S.32.1	知的財産となり得るものを保護するために、次の事項を考慮する。 l) 著作権法又は適用される使用許諾が認めている場合を除いて、規格、書籍、記事、報告書又はその他文書の全部又は一部を複写しない。	手引に関連記載あり	18.1.2.12	著作権法が認めている場合を除いて、書籍、記事、報告書又はその他文書の全部又は一部を複写しない。
5.32.2	知的財産権及び権利関係のある製品の利用において、使用許諾で許可された最大利用者数又は資源数を超過しないことを確実にする。	特になし。	5g-S.32.1	【再】知的財産となり得るものを保護するために、次の事項を考慮する。 f) 使用許諾で許可された最大利用者数又は資源数を超過しないことを確実にする。	管理策に関連記載あり	18.1.2.6	使用許諾で許可された最大利用者数を超過しないことを確実にするための管理策を実施する。
5.33	記録の保護 統制目標：記録は、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。 目的：記録の保護及び可用性に関連する、法令、規制及び契約上の要求事項の順守、並びにコミュニティ又は社会の期待に応えることを確実にするため。		5.33	記録の保護 管理策 記録は、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護することが望ましい 目的 記録の保護及び可用性に関連する、法令、規制及び契約上の要求事項の順守、並びにコミュニティ又は社会の期待に応えることを確実にするため。		18.1.3	記録の保護 記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。
5.33.1	記録を保護するための方針を策定する。	組織は、自らの事業の状況及び自らの管理の要求事項が時間の経過とともに変化するため、記録の真正性、信頼性、完全性及び使用可能性を保護するための段階を踏む。 a) 記録の改変の防止を含む、記録の保存、受渡記録の取扱い及び記録の処分に関する指針を発行する。これらの指針は、記録管理及びその他の記録の要求事項に関する組織のトピック固有の方針に沿っている。 b) 記録及びそれらの記録の保持することが望ましい期間を明確にした保持計画を作成する。 具体的な組織の記録の保護について決定する場合は、組織の分類体系に基づき、その情報に適用されている情報セキュリティ分類を考慮する。 記録類は、記録の種類（例えば、会計記録、事業のトランザクション記録、人事記録、法務記録）によって、また、それぞれの種類を更に詳細に、保持期間、及び許容される物理的又は電子的な記憶媒体の種類によって分類する。	5g-S.33.1	組織は、自らの事業の状況及び自らの管理の要求事項が時間の経過とともに変化するため、記録の真正性、信頼性、完全性及び使用可能性を保護するために次の段階を踏む。 a) 記録の改変の防止を含む、記録の保存、受渡記録の取扱い及び記録の処分に関する指針を発行する。これらの指針は、記録管理及びその他の記録の要求事項に関する組織のトピック固有の方針に沿っている。	手引に関連記載あり	18.1.3.10	記録保護の目的を満たすため、組織内では、記録及び情報の保持、保存、取扱い及び処分に関する指針を発行する。
			5g-S.33.1	組織は、自らの事業の状況及び自らの管理の要求事項が時間の経過とともに変化するため、記録の真正性、信頼性、完全性及び使用可能性を保護するために次の段階を踏む。 b) 記録及びそれらの記録の保持することが望ましい期間を明確にした保持計画を作成する。	手引に関連記載あり	18.1.3.11	記録保護の目的を満たすため、組織内では、記録及びそれらの記録の保持期間を明確にした保持計画を作成する。
			5g-S.33.4	具体的な組織の記録の保護について決定する場合は、組織の分類体系に基づき、その情報に適用されている情報セキュリティ分類を考慮する。	手引に関連記載あり	18.1.3.1	具体的な組織の記録の保護について決定する場合は、組織の分類体系に基づき、その情報に適用されている分類を考慮して決定する。
			5g-S.33.5	記録類は、記録の種類によって、また、それぞれの種類を更に詳細に、保持期間、及び許容される物理的又は電子的な記憶媒体の種類によって分類する。	手引に関連記載あり	18.1.3.2	記録類は、記録の種類（例えば、会計記録、データベース記録、トランザクションログ、監査ログ、運用手順）によって、また、更にそれぞれの種類での保持期間及び許容される記憶媒体の種類（例えば、紙、マイクロフィッシュ、磁気媒体、光媒体）の詳細によって分類する。
5.33.2	記録を保存するシステムは、国、地域の法令、規制、該当する場合には、コミュニティ又は社会の期待も考慮に入れて、記録及びその保存期間を特定する。	記録を保存し、取り扱うシステムは、国又は地域の法令又は規制、及び該当する場合には、コミュニティ又は社会の期待も考慮に入れて、記録及びその保持期間の特定を確実にする。 記録の保持期間が終了した後、組織にとって必要ない場合には、そのシステムは、記録を適切に破棄できるようにする。	5g-S.33.2	記録を保存し、取り扱うシステムは、国又は地域の法令又は規制、及び該当する場合には、コミュニティ又は社会の期待も考慮に入れて、記録及びその保持期間の特定を確実にする。	手引に関連記載あり	18.1.3.8	データ保存及びデータ処理システムは、記録を確実に特定し、国又は地域の法令又は規制が適用される場合に定められている記録の保持期間を確実に特定する。
			5g-S.33.3	記録の保持期間が終了した後、組織にとって必要ない場合には、そのシステムは、記録を適切に破棄できるようにする。	手引に関連記載あり	18.1.3.9	保持期間が終了した後、組織にとって必要ない場合には、データ保存及びデータ処理システムは、記録を適切に破棄できるようにする。
5.33.3	記録を保護するための対策を実施する。	満たすべき要求に応じて、許容される時間枠内及び書式で、要求された記録を取り出すことができるよう、データ保存システムを選択する。 電子記憶媒体を選択する場合は、将来の技術変化によって読出しができなくなることを防ぐために、保持期間を通じて記録にアクセスできること（記憶媒体及び書式の読取り可能性）を確実にする手順を確立する。 記録を保持している期間中、記録の復号を可能にするために、暗号化したアーカイブ又はディジタル署名に用いた暗号鍵及び暗号プログラムも保持する（8.24参照）。 記録媒体の保存及び取扱いの手順は、記憶媒体の製造業者が示す推奨の仕様に従って実施する。 記録の保存に用いる媒体が劣化する可能性を考慮する。	5g-S.33.6	満たすべき要求に応じて、許容される時間枠内及び書式で、要求された記録を取り出すことができるよう、データ保存システムを選択する。	手引に関連記載あり	18.1.3.7	満たすべき要求に応じて、許容される時間枠内及び書式で、要求されたデータを取り出すことができるよう、データ保存システムを選択する。
			5g-S.33.7	電子記憶媒体を選択する場合は、将来の技術変化によって読出しができなくなることを防ぐために、保持期間を通じて記録にアクセスできること（記憶媒体及び書式の読取り可能性）を確実にする手順を確立する。	手引に関連記載あり	18.1.3.6	電子的記憶媒体を選択する場合は、将来の技術変化によって読出しができなくなることを防ぐために、保持期間を通じてデータにアクセスできること（媒体及び書式の読取り可能性）を確実にする手順を確立する。
			5g-S.33.8	記録を保持している期間中、記録の復号を可能にするために、暗号化したアーカイブ又はディジタル署名に用いた暗号鍵及び暗号プログラムも保持する。	手引に関連記載あり	18.1.3.3	保存した記録の暗号化又はディジタル署名に用いた暗号鍵及び暗号プログラムは、その記録期間を保存している期間中に記録の復号が可能なように、保管する。
			5g-S.33.9	記録媒体の保存及び取扱いの手順は、記憶媒体の製造業者が示す推奨の仕様に従って実施する。	手引に関連記載あり	18.1.3.5	記録の保存及び取扱いの手順は、媒体の製造業者の推奨の仕様に従って実施する。
			5g-S.33.10	記録の保存に用いる媒体が劣化する可能性を考慮する。	手引に関連記載あり	18.1.3.4	記録の保存に用いる媒体が劣化する可能性を考慮して記録の保存及び取扱いの手順を定める。
5.33.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.34	プライバシー及びPIIの保護 統制目標：組織は、適用される法令、規制及び契約上の要求事項に従って、プライバシー及びPIIの保護に関する要求事項を特定し、満たす。 目的：PIIの保護の情報セキュリティの側面に関連する法令、規制及び契約上の要求事項の順守を確実にするため。		5.34	プライバシー及びPIIの保護 管理策 組織は、適用される法令、規制及び契約上の要求事項に従って、プライバシー及びPIIの保護に関する要求事項を特定し、満たす。 目的 PIIの保護の情報セキュリティの側面に関連する法令、規制及び契約上の要求事項の順守を確実にするため。		18.1.4	プライバシー及び個人を特定できる情報（PII）の保護 プライバシー及び個人識別情報（PII）の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実に行う。
5.34.1	適用される法令、規制及び契約上の要求事項に従って、プライバシー及びPIIの保護に関する要求事項を特定し、対策を実施する。	組織は、プライバシー及びPIIの保護に関するトピック固有の方針を確立し、全ての関連する利害関係者に伝達する。 組織は、プライバシー及びPIIの保護のための手順を策定し、実施する。 組織は、プライバシー及びPIIの保護のために策定した手順を、PIIの処理に関わる全ての利害関係者に伝達する。 PIIを保護するための適切な技術的及び組織的対策を実施する。	5g-S.34.1	組織は、プライバシー及びPIIの保護に関するトピック固有の方針を確立し、全ての関連する利害関係者に伝達する。	手引に関連記載あり	18.1.4.1	プライバシー及びPII の保護に関する組織の方針を確立して実施する。
			5g-S.34.2	組織は、プライバシー及びPIIの保護のための手順を策定し、実施する。	手引に関連記載あり	18.1.4.2	プライバシー及びPII の保護に関する組織の方針は、PIIの処理に関与する全ての者に伝達する。
			5g-S.34.3	組織は、プライバシー及びPIIの保護のために策定した手順を、PIIの処理に関わる全ての利害関係者に伝達する。	手引に関連記載あり	–	（対応項なし）
			5g-S.34.7	PIIを保護するための適切な技術的及び組織的対策を実施する。	手引に関連記載あり	18.1.4.6	PII を保護するための適切な技術的及び組織的対策を実施する。
5.34.2	プライバシー及びPIIの保護に関する全ての法令及び規制の順守のための役割及び責任を割り当てる。	組織は、プライバシー及びPIIの保護のために策定した手順の順守、並びにプライバシー及びPIIの保護に関する全ての法令及び規制の順守のために、適切な役割、責任及び管理策を整備する。 プライバシー及びPIIの保護に関する責任者は、要員、サービス提供者及びその他の利害関係者に対して、それぞれの責任及び従うことが望ましい特定の手順について、手引を提供する。多くの場合、例えば、プライバシー担当役員のような一人の責任者を任命することによって最も達成される。 PIIの取扱いについての責任は、関連する法令及び規制を考慮に入れて処置する。	5g-S.34.4	組織は、プライバシー及びPIIの保護のために策定した手順の順守、並びにプライバシー及びPIIの保護に関する全ての法令及び規制の順守のために、適切な役割、責任及び管理策を整備する。	手引に関連記載あり	18.1.4.3	プライバシー及びPII の保護に関する組織の方針の順守、並びに人々のプライバシーの保護及びPII の保護に関する全ての法令及び規制の順守のために、適切な管理構造及び管理策を確立する。
			5g-S.34.5	プライバシー及びPIIの保護に関する責任者は、要員、サービス提供者及びその他の利害関係者に対して、それぞれの責任及び従うことが望ましい特定の手順について、手引を提供する。	手引に関連記載あり	18.1.4.4	プライバシー及びPIIの保護の責任者（例えば、プライバシー担当役員）は、管理者、利用者及びサービス提供者に対して、それぞれの責任及び従うことが望ましい特定の手順について、手引を提供する。
			5g-S.34.6	PIIの取扱いについての責任は、関連する法令及び規制を考慮に入れて処置する。	手引に関連記載あり	18.1.4.5	PII の取扱い、及びプライバシーの原則の認識を確実にすることについての責任は、関連する法令及び規制に従って処置する。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
5.35	情報セキュリティの独立したレビュー 統制目標：人、プロセス及び技術を含む、情報セキュリティ及びその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。 目的：組織における情報セキュリティ管理の取組の、継続的な適切性、十分性及び有効性を確実にするため。		5.35	情報セキュリティの独立したレビュー 管理策 人、プロセス及び技術を含む、情報セキュリティ及びその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。 目的 組織における情報セキュリティ管理の取組の、継続的な適切性、十分性及び有効性を確実にするため。		18.2	情報セキュリティのレビュー 管理目的：組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。
						18.2.1	情報セキュリティの独立したレビュー 情報セキュリティ及びその実施の管理（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。
5.35.1	情報セキュリティの定期的な独立したレビューを計画し、実施する。	組織は、情報セキュリティの独立したレビューを実施するためのプロセスをもつ。 管理策は、情報セキュリティの定期的な独立したレビューを計画し、実施する。 情報セキュリティの独立したレビューは、情報セキュリティ方針、トピック固有の方針、及びその他の管理策を含む、情報セキュリティの取組の改善の機会及び変更の必要性の評価を含む。 情報セキュリティの定期的な独立したレビューに加えて、組織は次の場合にも、独立したレビューの実施を検討する。 a) 組織に影響する法令及び規制が変わる。 b) 重大なインシデントが生じる。 c) 組織が新しい事業を開始する、又は現在の事業を変更する。 d) 組織が新しい製品若しくはサービスの利用を開始する、又は現在の製品若しくはサービスの利用を変更する。 e) 組織が情報セキュリティの管理策及び手順を大幅に変更する。	5g-5.35.1	組織は、情報セキュリティの独立したレビューを実施するためのプロセスをもつ。	手引に関連記載あり	18.2.1.1	経営陣は、情報セキュリティマネジメントの組織の取組みが、引き続き適切、妥当及び有効であることを確実にするために、独立したレビューを実施し、実施させる。
			5g-5.35.2	管理策は、情報セキュリティの定期的な独立したレビューを計画し、実施する。	手引に関連記載あり	–	（対応項なし）
			5g-5.35.3	情報セキュリティの独立したレビューは、情報セキュリティ方針、トピック固有の方針、及びその他の管理策を含む、情報セキュリティの取組の改善の機会及び変更の必要性の評価を含む。	手引に関連記載あり	18.2.1.2	独立したレビューは、改善の機会のアセスメントを含める。
					手引に関連記載あり	18.2.1.3	独立したレビューには、方針及び管理目的を含むセキュリティの取組みの変更について、その必要性の評価を含める。
			5g-5.35.10	情報セキュリティの定期的な独立したレビューに加えて、組織は次の場合にも、独立したレビューの実施を検討する。 a) 組織に影響する法令及び規制が変わる。 b) 重大なインシデントが生じる。 c) 組織が新しい事業を開始する、又は現在の事業を変更する。 d) 組織が新しい製品若しくはサービスの利用を開始する、又は現在の製品若しくはサービスの利用を変更する。 e) 組織が情報セキュリティの管理策及び手順を大幅に変更する。	手引に関連記載あり	–	（対応項なし）
5.35.2	情報セキュリティの独立したレビューを実施する個人・組織は、レビューの対象となる領域から独立した、レビューに関する経験や資格を保有する個人・組織が実施する。	情報セキュリティの独立したレビューは、レビューの対象となる領域から独立した個人・組織（例えば、内部監査の担当部署、独立した管理者、このようなレビューを専門に行う外部関係者）が実施する。 情報セキュリティの独立したレビューを実施する個人・組織は、適切な力量をもつ。 情報セキュリティの独立したレビューを実施する個人は、評価を行う上で独立性をもつことを確実にするため、権限をもつ系統に属さない。	5g-5.35.4	情報セキュリティの独立したレビューは、レビューの対象となる領域から独立した個人・組織が実施する。	手引に関連記載あり	18.2.1.4	独立したレビューは、レビューが行われる領域から独立した個人・組織（例えば、内部監査の担当部署、独立した管理者、このようなレビューを専門に行う外部関係者）が実施する。
			5g-5.35.5	情報セキュリティの独立したレビューを実施する個人・組織は、適切な力量をもつ。	手引に関連記載あり	18.2.1.5	独立したレビューは、適切な技能及び経験をもつ個人・組織が実施する。
			5g-5.35.6	情報セキュリティの独立したレビューを実施する個人は、評価を行う上で独立性をもつことを確実にするため、権限をもつ系統に属さない。	手引に関連記載あり	–	（対応項なし）
5.35.3	独立したレビューの結果は、レビューを実施した管理職及び適切な場合には、トップマネジメントに報告する。	情報セキュリティの独立したレビューの結果は、レビューを発議した管理職、及び、適切な場合には、トップマネジメントに報告する。 情報セキュリティの独立したレビューの記録は、維持する。	5g-5.35.7	情報セキュリティの独立したレビューの結果は、レビューを発議した管理職、及び、適切な場合には、トップマネジメントに報告する。	手引に関連記載あり	18.2.1.6	独立したレビューの結果は、記録し、レビューを発議した経営陣に報告する。
			5g-5.35.8	情報セキュリティの独立したレビューの記録は、維持する。	手引に関連記載あり	18.2.1.7	独立したレビューの結果の記録は、維持する。
5.35.4	独立したレビューにおいて、情報セキュリティマネジメントに対する組織の取組及び実施が十分でない場合に管理職は是正処置を指示する。	情報セキュリティの独立したレビューにおいて、情報セキュリティマネジメントに対する組織の取組及び実施が十分でない（例えば、文書化した目的及び要求事項が、情報セキュリティ方針及びトピック固有の方針（5.1参照）に記載された情報セキュリティに関する方向性に十分に適合していない、又はこれを順守していない。）ことが明確になった場合には、管理職は是正処置を発議する。	5g-5.35.9	情報セキュリティの独立したレビューにおいて、情報セキュリティマネジメントに対する組織の取組及び実施が十分でないことが明確になった場合には、管理職は是正処置を発議する。	手引に関連記載あり	18.2.1.8	独立したレビューにおいて、情報セキュリティマネジメントに対する組織の取組み及び実施が十分でない（例えば、文書化した目的及び要求事項が、情報セキュリティのための方針群に記載された情報セキュリティに関する方向性が十分に適合していない、又はこれを順守していない）ことが明確になった場合には、経営陣は是正処置の検討を指示する。
5.35.5	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.35.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.35.7	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.35.8	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.35.9	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
5.36	情報セキュリティのための方針群、規則及び標準の順守 統制目標：組織の情報セキュリティ方針、トピック固有の方針、規則及び標準を順守していることを定期的にレビューする。 目的：情報セキュリティを、組織の情報セキュリティ方針、トピック固有の方針、規則及び標準に従って実施し、運用することを確実にするため。		5.36	情報セキュリティのための方針群、規則及び標準の順守 管理策 組織の情報セキュリティ方針、トピック固有の方針、規則及び標準を順守していることを定期的にレビューする。 目的 情報セキュリティを、組織の情報セキュリティ方針、トピック固有の方針、規則及び標準に従って実施し、運用することを確実にするため。		18.2.2	情報セキュリティのための方針群及び標準の順守 管理者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューする。
5.36.1	管理者及びサービス、製品又は情報の管理責任者による、情報セキュリティ要求事項が満たされていることをレビューする方法を定める。	管理者及びサービス、製品又は情報の管理責任者は、情報セキュリティ方針、トピック固有の方針、規則、標準及びその他適用される規制で定められた情報セキュリティ要求事項が満たされていることをレビューする方法を特定する。 定めに従って効率的にレビューを行うため、自動的な測定ツール及び報告ツールの使用を考慮する。	5g-5.36.1	管理者及びサービス、製品又は情報の管理責任者は、情報セキュリティ方針、トピック固有の方針、規則、標準及びその他適用される規制で定められた情報セキュリティ要求事項が満たされていることをレビューする方法を特定する。	手引に関連記載あり	18.2.2.1	管理者は、方針、標準類及びその他適用される規制で定められた情報セキュリティ要求事項が満たされていることをレビューする方法を特定する。
			5g-5.36.2	定めに従って効率的に情報セキュリティのレビューを行うため、自動的な測定ツール及び報告ツールの使用を考慮する。	手引に関連記載あり	18.2.2.2	管理者は定めに従って効率的にレビューを行うため、自動的な測定ツール及び報告ツールを使用する。
					手引に関連記載あり	18.2.3.1	技術的順守は、技術専門家が後に解釈するための技術レポートを生成する自動ツールを活用してレビューする。
5.36.2	管理者及びサービス、製品又は情報の管理責任者がレビューする。	管理者及びサービス、製品又は情報の管理責任者が実施した レビュー及び是正処置の結果を記録し、また、その記録を維持管理する。 管理者の責任範囲に対して、情報セキュリティの独立したレビュー（5.35参照）が実施されるときは、管理職は、独立したレビュー実施者に対して、その結果を報告する。	5g-5.36.4	管理者及びサービス、製品又は情報の管理責任者が実施した情報セキュリティのレビュー及び是正処置の結果を記録し、また、その記録を維持管理する。	手引に関連記載あり	18.2.2.7	管理者が実施したレビュー及び是正処置の結果を記録する、また、その記録を維持・管理する。
			5g-5.36.5	管理者の責任範囲に対して、情報セキュリティの独立したレビューが実施されるときは、管理職は、独立したレビュー実施者に対して、その結果を報告する。	手引に関連記載あり	18.2.2.8	管理者の責任範囲に対して、独立したレビューが実施されるときは、管理者は、独立したレビュー実施者に対して、レビュー及び是正処置の結果を報告する。
5.36.3	レビューの結果、不順守を検出した場合、是正処置を実施する。	情報セキュリティのレビューの結果、何らかの不順守を検出した場合、管理者は、次の事項を行う。 a) 不順守の原因を特定する。 b) 順守を達成するための是正処置の必要性を評価する。 c) 適切な是正処置を実施する。 d) 是正処置の有効性を検証し、不備又は弱点を特定するために、講じた是正処置をレビューする。 情報セキュリティ要求事項の不順守に対する是正処置は、リスクに対して適切に、時機を失せずに完了する。 次に予定している情報セキュリティのレビューまでに完了しない場合、そのレビュー時に少なくとも進捗状況を取り上げる。	5g-5.36.3	情報セキュリティのレビューの結果、何らかの不順守を検出した場合、管理者は、次の事項を行う。 a) 不順守の原因を特定する。	手引に関連記載あり	18.2.2.3	管理者によるレビューの結果、何らかの不順守を検出した場合、管理者は、不順守の原因を特定する。
			5g-5.36.3	情報セキュリティのレビューの結果、何らかの不順守を検出した場合、管理者は、次の事項を行う。 b) 順守を達成するための是正処置の必要性を評価する。	手引に関連記載あり	18.2.2.4	管理者によるレビューの結果、何らかの不順守を検出した場合、管理者は、順守を達成するための是正処置の必要性を評価する。
			5g-5.36.3	情報セキュリティのレビューの結果、何らかの不順守を検出した場合、管理者は、次の事項を行う。 c) 適切な是正処置を実施する。	手引に関連記載あり	18.2.2.5	管理者によるレビューの結果、何らかの不順守を検出した場合、管理者は、適切な是正処置を実施する。
			5g-5.36.3	情報セキュリティのレビューの結果、何らかの不順守を検出した場合、管理者は、次の事項を行う。 d) 是正処置の有効性を検証し、不備又は弱点を特定するために、講じた是正処置をレビューする。	手引に関連記載あり	18.2.2.6	管理者によるレビューの結果、何らかの是正処置を実施した場合、管理者は、是正処置の有効性を検証し、不備又は弱点を特定するために、とった是正処置をレビューする。
			5g-5.36.6	情報セキュリティ要求事項の不順守に対する是正処置は、リスクに対して適切に、時機を失せずに完了する。	手引に関連記載あり	–	（対応項なし）
			5g-5.36.7	次に予定している情報セキュリティのレビューまでに完了しない場合、そのレビュー時に少なくとも進捗状況を取り上げる。	手引に関連記載あり	–	（対応項なし）
5.37	操作手順書 統制目標：情報処理設備の操作手順は、文書化し、必要とする要員に対して利用可能にする。 目的：情報処理設備の正確で、かつ、セキュリティに配慮した操作を確実にするため。		5.37	操作手順書 管理策 情報処理設備の操作手順は、文書化し、必要とする要員に対して利用可能にする。 目的 情報処理設備の正確で、かつ、セキュリティに配慮した操作を確実にするため。		12	運用のセキュリティ
						12.1	運用の手順及び責任 管理目的：情報処理設備の正確かつセキュリティを保った運用を確実にするため。
						12.1.1	操作手順書 操作手順は、文書化し、必要とする全ての利用者に対して利用可能とする。
5.37.1	情報処理設備における操作手順書を作成する。	例えば、次の場合に、情報セキュリティに関連する組織の操作活動の手順書を作成する。 a) 多くの人が同じ活動を行う必要がある場合 b) まれにしか行われない活動で、次に実行するときに手順を忘れている可能性が高い場合 c) 新たな活動で、正しく実行しないとリスクが生じる場合 d) 新しい要員に活動を引き継ぐ際 情報処理設備の操作手順には、次の事項を明記する。 a) 責任者 b) システムのセキュリティに配慮した導入及び構成 c) 情報の処理及び取扱い（自動化されたもの及び手動によるものを含む。） d) バックアップ（8.3参照）及びレジリエンス e) スケジュールに関する要求事項。これには、他のシステムとの依存関係を含む。 f) 作業中に発生し得る、誤り又はその他の例外状況の処理についての指示［例えば、ユーティリティプログラムの利用の制限（8.18参照）］ g) 操作上又は技術上の不測の問題が発生した場合の、外部のサポート用連絡先を含む、サポート用及びエスカレーション用の連絡先 h) 記憶媒体の取扱いに関する指示（7.10及び7.14参照） i) システムが故障した場合の再起動及び回復の手順 j) 監査証跡及びシステムログ情報（8.15及び8.17参照）並びにビデオ監視システム（7.4参照）の管理 k) 容量・能力、パフォーマンス及びセキュリティなどの監視手順（8.6及び8.16参照） l) 保守手順	5g-5.37.2	次の場合には、情報セキュリティに関連する組織の操作活動の手順書を作成する。 a) 多くの人が同じ活動を行う必要がある場合 b) まれにしか行われない活動で、次に実行するときに手順を忘れている可能性が高い場合 c) 新たな活動で、正しく実行しないとリスクが生じる場合 d) 新しい要員に活動を引き継ぐ際	手引に関連記載あり	12.1.1.1	情報処理設備及び通信設備に関連する操作（例えば、コンピュータの起動・停止の手順、インストール、設定、バックアップ、装置の保守、媒体の取扱い、コンピュータ室及びメールの取扱いの管理・安全）の手順書を、利用者の特権の有無を考慮して作成する。
			5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 a) 責任者	手引に関連記載あり	–	（対応項なし）
			5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 b) システムのセキュリティに配慮した導入及び構成	手引に関連記載あり	12.1.1.2	情報処理設備及び通信設備に関連する操作手順には、システムの運用前認可、導入及び構成（ベースライン構成を含む）、セキュリティ機能、管理機能の設定及び使用に関する既知のせい弱性を含む、操作上の指示を明記する。
			5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 c) 情報の処理及び取扱い（自動化されたもの及び手動によるものを含む。）	手引に関連記載あり	12.1.1.3	情報処理設備及び通信設備に関連する操作手順には、情報の処理及び取扱い（自動化されたもの及び手動によるものを含む）を含む、操作上の指示を明記する。
			5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 d) バックアップ及びレジリエンス	手引に関連記載あり	12.1.1.4	情報処理設備及び通信設備に関連する操作手順には、バックアップを含む、操作上の指示を明記する。
			5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 e) スケジュールに関する要求事項。これには、他のシステムとの依存関係を含む。	手引に関連記載あり	12.1.1.5	情報処理設備及び通信設備に関連する操作手順には、スケジュール作成に関する要求事項（他のシステムとの相互依存性、最も早い作業の開始時刻及び最も遅い作業の完了時刻など）を含む、操作上の指示を明記する。
			5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 f) 作業中に発生し得る、誤り又はその他の例外状況の処理についての指示	手引に関連記載あり	12.1.1.6	情報処理設備及び通信設備に関連する操作手順には、作業中に発生し得る、誤り又はその他の例外状況の処理についての指示（システムユーティリティの利用の制限）を含む、操作上の指示を明記する。
			5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 g) 操作上又は技術上の不測の問題が発生した場合の、外部のサポート用連絡先を含む、サポート用及びエスカレーション用の連絡先	手引に関連記載あり	12.1.1.7	情報処理設備及び通信設備に関連する操作手順には、必要な文書が入手できない場合及び操作上又は技術上の不測の問題が発生した場合の、外部のサポート用連絡先を含む、サポート用及び段階的取扱い（escalation）用の連絡先を含む、操作上の指示を明記する。
			5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 h) 記憶媒体の取扱いに関する指示	手引に関連記載あり	12.1.1.8	情報処理設備及び通信設備に関連する操作手順には、特別な出力及び媒体の取扱いに関する指示（特殊な用紙の使用、秘密情報の出力の管理（失敗した作業出力のセキュリティを保った処分手順を含む））を含む、操作上の指示を明記する。
			5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 i) システムが故障した場合の再起動及び回復の手順	手引に関連記載あり	12.1.1.9	情報処理設備及び通信設備に関連する操作手順には、システムが故障した場合の再起動及び回復の手順を含む、操作上の指示を明記する。
			5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 j) 監査証跡及びシステムログ情報並びにビデオ監視システムの管理	手引に関連記載あり	12.1.1.10	情報処理設備及び通信設備に関連する操作手順には、監査証跡及びシステムログ情報の管理を含む、操作上の指示を明記する。
			5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 k) 容量・能力、パフォーマンス及びセキュリティなどの監視手順	手引に関連記載あり	12.1.1.11	情報処理設備及び通信設備に関連する操作手順には、監視手順を含む、操作上の指示を明記する。
			5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 l) 保守手順	手引に関連記載あり	–	（対応項なし）
5.37.2	情報処理設備の操作手順書の変更は認可のもと実施する。	情報処理設備の操作手順書の変更は必要に応じてレビュー、更新する。 情報処理設備の操作手順書の変更は認可のもとで行う。 技術的に可能であれば、情報システムは、同一の手順、ツール及びユーティリティを用いて、首尾一貫した管理を行う。	5g-5.37.3	情報処理設備の操作手順書は必要に応じてレビュー、更新する。	手引に関連記載あり	–	（対応項なし）
			5g-5.37.4	情報処理設備の操作手順書の変更は認可のもとで行う。	手引に関連記載あり	12.1.1.12	システムの管理活動のための操作手順及び文書化手順は、正式な文書として取扱い、その手順書の変更は、管理職が認可する。
			5g-5.37.5	技術的に可能であれば、情報システムは、同一の手順、ツール及びユーティリティを用いて、首尾一貫した管理を行う。	手引に関連記載あり	12.1.1.13	情報システムは、技術的に可能な場合には、同一の手順、ツール及びユーティリティを用いて、首尾一貫した管理を行う。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
6.1	選考 統制目標：要員になる全ての候補者について経歴などの確認は、適用される法令、規制及び倫理を考慮に入れて、組織に加える前に、及びその後継続的に行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。 目的：全ての要員が、予定する役割に対して適格かつ適切であり、雇用中に適格かつ適切であり続けることを確実にするため。		6.1	選考 管理策 要員になる全ての候補者についての経歴などの確認は、適用される法令、規制及び倫理を考慮に入れて、組織に加える前に、及びその後継続的に行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。 目的 全ての要員が、予定する役割に対して適格かつ適切であり、雇用中に適格かつ適切であり続けることを確実にするため。		7	人的資源のセキュリティ
						7.1	雇用前 管理目的：従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。
						7.1.1	雇用前 全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。
6.1.1	要員になる候補者の確認の基準及び制約を定める。	選考手順には、要員になる候補者の確認のためのレビューの基準及び制約を定める（例えば、誰が選考するのか、また、この確認のためのレビューは、いつ、どのように、なぜ行うのか。）。	6a-6.1.7	選考手順には、要員になる候補者の確認のためのレビューの基準及び制約を定める。	予引に関連記載あり	7.1.1.9	手順には、確認のためのレビューの基準及び制約を定める（例えば、誰が選考するのか、また、この確認のためのレビューは、いつ、どのように、なぜ行うのか。）。
6.1.2	全ての候補者に対する選考プロセスにおいて、PII保護及び雇用に関する法令を考慮に入れて必要な確認を行う。	選考プロセスは、フルタイム、パートタイム及び臨時スタッフを含む全ての要員に対して実行する。 サービス供給者を通じて選考される個人に対して契約をする場合には、選考の要求事項を組織と供給者との間の合意に含める。 組織内である職位に付けることを検討している全ての候補者についての情報は、当該法域での適切な法令を考慮して収集し、扱う。 法域によっては、選考活動について、組織が候補者に事前に通知することが法的に必要な場合がある。 要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、次の事項を含む。 a) 満足のいく推薦状（例えば、業務及び人物に関する推薦状）の入手の可否 b) 応募者の履歴書の確認（完全であるか及び正確であるかの確認） c) 提示された学術上及び職業上の資格の確認 d) 公的証明書（例えば、パスポート又は適切な当局が発行したその他の許容可能な文書）の確認 e) 候補者が重要な役割を担う場合には、信用情報又は犯罪記録のレビューのような、より詳細な確認	6a-6.1.1	選考プロセスは、フルタイム、パートタイム及び臨時スタッフを含む全ての要員に対して実行する。	予引に関連記載あり	–	（対応項なし）
			6a-6.1.2	サービス供給者を通じて選考される個人に関して契約をする場合には、選考の要求事項を組織と供給者との間の合意に含める。	予引に関連記載あり	–	（対応項なし）
			6a-6.1.3	組織内である職位に付けることを検討している全ての候補者についての情報は、当該法域での適切な法令を考慮して収集し、扱う。	予引に関連記載あり	7.1.1.12	組織内である職位に付けることを検討している全ての候補者についての情報は、当該法域での適切な法令に従って収集し、扱う。
			（6a-6.1.3参考）	法域によっては、選考活動について、組織が候補者に事前に通知することが法的に必要な場合がある。	予引に関連記載あり	7.1.1.13	適用される法令によっては、選考活動について候補者へ、事前に通知する。
			6a-6.1.4	要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、満足のいく推薦状（例えば、業務についてのもの、人物についてのもの）の入手の可否の確認を行う。	予引に関連記載あり	7.1.1.1	関連があるプライバシー、PIIの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、満足のいく推薦状（例えば、業務についてのもの、人物についてのもの）の入手の可否の確認を行う。
			6a-6.1.4	要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、次の事項を含む。 b) 応募者の履歴書の確認（完全であるか及び正確であるかの確認）	予引に関連記載あり	7.1.1.2	関連があるプライバシー、PIIの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、応募者の履歴書の確認（完全であるか及び正確であるかの確認）を行う。
			6a-6.1.4	要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、次の事項を含む。 c) 提示された学術上及び職業上の資格の確認	予引に関連記載あり	7.1.1.3	関連があるプライバシー、PIIの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、提示された学術上及び職業上の資格の確認を行う。
			6a-6.1.4	要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、次の事項を含む。 d) 公的証明書の確認	予引に関連記載あり	7.1.1.4	関連があるプライバシー、PIIの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、公的証明書（パスポート又は同種の文書）の確認を行う。
			6a-6.1.4	要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、次の事項を含む。 e) 候補者が重要な役割を担う場合には、信用情報又は犯罪記録のレビューのような、より詳細な確認	予引に関連記載あり	7.1.1.5	関連があるプライバシー、PIIの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、信用情報又は犯罪記録のレビューのような、より詳細な確認を行う。
6.1.3	情報セキュリティに関する特定の役割のために雇用する場合、必要な確認を行う。	情報セキュリティに関する特定の役割のために雇用する場合、組織は、次の事項を確認する。 a) 候補者が、情報セキュリティに関するその役割を果たすために必要な力量を備えている。 b) 特に、その役割が組織にとって重要なものである場合は、候補者が、その役割を任せられる信頼できる人物である。 最初の発令で就く業務であろ、昇進して就く業務であるかにかかわらず、情報処理施設にアクセスすることがその担当者にとって必要になる場合、特にそれらの設備が秘密情報（例えば、財務情報、個人情報又は医療情報）を扱っているときには、組織は、より詳細な確認も検討する。	6a-6.1.5	情報セキュリティに関する特定の役割のために雇用する場合、組織は、次の事項を確認する。 a) 候補者が、情報セキュリティに関するその役割を果たすために必要な力量を備えている。	予引に関連記載あり	7.1.1.6	情報セキュリティに関する特定の役割のために雇用する場合、組織は、候補者が、情報セキュリティに関するその役割を果たすために必要な力量を備えていることを確認する。
			6a-6.1.5	情報セキュリティに関する特定の役割のために雇用する場合、組織は、次の事項を確認する。 b) 特に、その役割が組織にとって重要なものである場合は、候補者が、その役割を任せられる信頼できる人物である。	予引に関連記載あり	7.1.1.7	情報セキュリティに関する特定の役割のために雇用する場合、組織は、特に、その役割が組織にとって重要なものである場合は、候補者が、その役割を任せられる信頼できる人物であることを確認する。
			6a-6.1.6	最初の発令で就く業務であろ、昇進して就く業務であるかにかかわらず、情報処理施設にアクセスすることがその担当者にとって必要になる場合、特にそれらの設備が秘密情報を扱っているときには、組織は、より詳細な確認も検討する。	予引に関連記載あり	7.1.1.8	最初の発令で就く業務であろ、昇進して就く業務であるかにかかわらず、情報処理施設にアクセスすることがその担当者にとって必要になる場合、特にそれらの設備が秘密情報（例えば、財務情報、個人情報又は医療情報）を扱っているときには、組織は、より詳細な確認も検討する。
6.1.4	時機を失せずに要員になる候補者の確認を完了できない状況では、確認が終了するまで、リスク低減のための対策を実施する。	時機を失せずに要員になる候補者の確認を完了できない状況では、レビューが終了するまで、例えば、次のようなリスク低減のための管理策を実施する。 a) 業務研修の開始時期を遅らせる。 b) 企業資産の利用を遅らせる。 c) アクセスを限定した業務研修を実施する。 d) 雇用を終了する。 個人の役割の重要性に応じて、要員が適切であり続けることを確実にするための確認を定期的に繰り返す。	6a-6.1.8	時機を失せずに要員になる候補者の確認を完了できない状況では、レビューが終了するまで、例えば、次のようなリスク低減のための管理策を実施する。 a) 業務研修の開始時期を遅らせる。 b) 企業資産の利用を遅らせる。 c) アクセスを限定した業務研修を実施する。 d) 雇用を終了する。	予引に関連記載あり	–	（対応項なし）
			6a-6.1.9	個人の役割の重要性に応じて、要員が適切であり続けることを確実にするための確認を定期的に繰り返す。	予引に関連記載あり	–	（対応項なし）
6.2	雇用条件 統制目標：雇用契約書には、情報セキュリティに関する要員及び組織の責任を記載する。 目的：要員が、予定する役割における自らの情報セキュリティの責任を理解することを確実にするため。		6.2	雇用条件 管理策 雇用契約書には、情報セキュリティに関する要員及び組織の責任を記載する。 目的 要員が、予定する役割における自らの情報セキュリティの責任を理解することを確実にするため。		7.1.2	雇用条件 従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載する。
6.2.1	情報セキュリティに関する役割及び責任を含む雇用条件を定める。	要員の契約上の義務は、組織の情報セキュリティ方針及びその他の関連する方針を考慮に入れる。 場合に応じて、次の事項を明確にし、言及する。 a) 秘密情報へのアクセスが与えられる全ての要員が情報及びその他の関連資産へのアクセスが与えられる前に署名することが望ましい秘密保持契約書又は守秘義務契約書（6.6参照） b) 法的な責任及び権利（例えば、著作権法、データ保護に関連して制定された法令（5.32及び5.34参照）に関するもの） c) 要員によって実行される、情報の分類、組織の情報及びその他の関連資産の管理、並びに情報処理施設及び情報サービスの管理に関する責任（5.9及び5.13参照） d) 利害関係者から受け取った情報の扱いに関する責任 e) 要員が組織の情報セキュリティ要求事項に従わない場合による処置（6.4参照） 情報セキュリティに関する役割及び責任は、雇用前のプロセスにおいて候補者に伝達する。	6a-6.2.1	要員の契約上の義務は、組織の情報セキュリティ方針及びその他の関連するトピック固有の方針を考慮に入れる。	予引に関連記載あり	7.1.2.1	従業員又は契約相手の契約上の義務には、組織の情報セキュリティのための方針群を反映する。
			6a-6.2.2	場合に応じて、次の事項について明確にし、言及する。 a) 秘密情報へのアクセスが与えられる全ての要員が情報及びその他の関連資産へのアクセスが与えられる前に署名することが望ましい秘密保持契約書又は守秘義務契約書	予引に関連記載あり	7.1.2.2	従業員又は契約相手の契約には、秘密情報へのアクセスが与えられる全ての従業員及び契約相手による、情報処理施設へのアクセスが与えられる前の、秘密保持契約書又は守秘義務契約書への署名を含める。
			6a-6.2.2	場合に応じて、次の事項について明確にし、言及する。 b) 法的な責任及び権利	予引に関連記載あり	7.1.2.3	従業員又は契約相手の契約には、従業員又は契約相手の法的な責任及び権利（例えば、著作権法、データ保護に関連して制定された法律に関するもの）を明確にする。
			6a-6.2.2	場合に応じて、次の事項について明確にし、言及する。 c) 要員によって扱われる、情報の分類、組織の情報及びその他の関連資産の管理、並びに情報処理施設及び情報サービスの管理に関する責任	予引に関連記載あり	7.1.2.4	従業員又は契約相手の契約には、従業員又は契約相手によって扱われる情報の分類に関する責任、並びに従業員又は契約相手によって扱われる組織の情報、情報に関連するその他の資産、情報処理施設及び情報サービスの管理に関する責任を明確にする。
			6a-6.2.2	場合に応じて、次の事項について明確にし、言及する。 d) 利害関係者から受け取った情報の扱いに関する責任	予引に関連記載あり	7.1.2.5	従業員又は契約相手の契約には、他社又は外部関係者から受け取った情報の扱いに関する従業員又は契約相手の責任を明確にする。
			6a-6.2.2	場合に応じて、次の事項について明確にし、言及する。 e) 要員が組織の情報セキュリティ要求事項に従わない場合による処置	予引に関連記載あり	7.1.2.6	従業員又は契約相手の契約には、従業員又は契約相手が組織のセキュリティ要求事項に従わない場合による処置を含める。
			6a-6.2.3	情報セキュリティに関する役割及び責任は、雇用前のプロセスにおいて候補者に伝達する。	予引に関連記載あり	7.1.2.7	情報セキュリティに関する役割及び責任は、雇用前のプロセスにおいて候補者に伝える。
6.2.2	雇用契約書等を用いて、組織の要員と情報セキュリティに関する雇用条件の同意を得る。	組織は、要員が情報セキュリティに関する雇用条件に同意することを確実にする。 情報セキュリティに関する雇用条件は、情報システム及びサービスに関連する組織の資産に対する要員によるアクセスの特性及び範囲に応じて、適切なものとする。	6a-6.2.4	組織は、要員が情報セキュリティに関する雇用条件に同意することを確実にする。	予引に関連記載あり	7.1.2.8	組織は、従業員及び契約相手が情報セキュリティに関する雇用条件に同意することを確実にする仕組みを整備する。
			6a-6.2.5	情報セキュリティに関する雇用条件は、情報システム及びサービスに関連する組織の資産に対する要員によるアクセスの特性及び範囲に応じて、適切なものとする。	予引に関連記載あり	7.1.2.9	雇用条件は、情報システム及びサービスと関連する組織の資産に対する、従業員及び契約相手によるアクセスの特性及び範囲に応じて、適切なものとする。
6.2.3	法令、規制、情報セキュリティ方針又は情報セキュリティに関連する方針が変更された場合は、情報セキュリティに関する雇用条件をレビューする。	法令、規制、情報セキュリティ方針又はトピック固有の方針が変更された場合は、情報セキュリティに関する雇用条件をレビューする。 適切であれば、雇用の終了後も、定められた期間は、その雇用条件に含まれている責任を継続させる（6.5参照）。	6a-6.2.6	法令、規制、情報セキュリティ方針又はトピック固有の方針が変更された場合は、情報セキュリティに関する雇用条件をレビューする。	管理策に関連記載あり	–	（対応項なし）
			6a-6.2.7	適切であれば、雇用の終了後も、定められた期間は、その雇用条件に含まれている責任を継続させる。	予引に関連記載あり	7.1.2.10	雇用の終了後も、定められた期間は、その雇用条件に含まれている責任を継続させる。
6.3	情報セキュリティの意識向上、教育及び訓練 統制目標：組織の要員及び関連する利害関係者は、職務に関連する組織の情報セキュリティ方針、トピック固有の方針及び手順についての、適切な、情報セキュリティに関する意識向上プログラム、教育及び訓練を受け、また、定常的な更新を受ける。 目的：要員及び関連する利害関係者が自らの情報セキュリティの責任を意識し、それを果たすことを確実にするため。		6.3	情報セキュリティの意識向上、教育及び訓練 管理策 組織の要員及び関連する利害関係者は、職務に関連する組織の情報セキュリティ方針、トピック固有の方針及び手順についての、適切な、情報セキュリティに関する意識向上プログラム、教育及び訓練を受けることが望ましく、また、定常的な更新を受ける。 目的 要員及び関連する利害関係者が自らの情報セキュリティの責任を意識し、それを果たすことを確実にするため。		7.2.2	情報セキュリティの意識向上、教育及び訓練 組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受ける。
6.3.1	内部及び外部の要員の役割を含めた、情報セキュリティの意識向上プログラムを計画し、定期的に実施する。	情報セキュリティの意識向上、教育及び訓練プログラムは、保護すべき組織の情報及び情報を保護するために実施されている情報セキュリティ管理策を考慮に入れて、組織の情報セキュリティ方針、情報セキュリティ関連に関連する方針及び手順に沿って確立する。 情報セキュリティの意識向上、教育及び訓練は、定期的に実施する。 可能な場合、開始時の意識向上、教育及び訓練は、新しい要員、及び情報セキュリティに関する要求事項が大幅に異なる新たな職位又は役割に異動した者にも適用する。 知識が伝わったこと、並びに意識向上、教育及び訓練プログラムの有効性を確認するため、意識向上、教育及び訓練の活動終了時に、要員の理解の評価を行う。 情報セキュリティの意識向上プログラムは、要員に対し、情報セキュリティに関する各自の責任及びその責任を果たす方法について、認識させること を狙いとし、内部及び外部の要員（例えば、外部のコンサルタント、供給者の要員）を含む、組織における要員の役割を考慮に入れて、計画する。 意識向上プログラムの活動は、長期にわたり、できれば定期的に実施する。これによって、活動が繰り返され、新しい要員も対象となる。 意識向上プログラムの活動では、情報セキュリティインシデントから学んだ教訓を生かす。 意識向上プログラムには、キャンペーン、パンフレット、ポスター、会報、ウェブサイト、説明会、ブリーフィング、eラーニングモジュール、電子メールなど、適切な物理的又は仮想的な手段を通した多くの意識向上活動を含める。 情報セキュリティの意識向上には、例えば、次のような一般的な側面を含める。 a) 組織全体にわたる情報セキュリティに対する経営陣のコミットメント b) 情報セキュリティ計及びトピック固有の方針、基準、法令、規制、契約及び合意を考慮に入れた、適用される情報セキュリティの規則及び義務に関する精通度及び順守のニーズ c) 自身が行動したこと及び行動しなかったことに対する個人のアカウンタビリティ、並びに組織及び利害関係者に属する情報のセキュリティを保ち、これを保護することに対する一般的な責任 d) 情報セキュリティに関する基本的な手順（例えば、情報セキュリティ事象の報告（6.8）及び基本的な管理策（例えば、パスワードのセキュリティ（5.17）） e) 情報セキュリティに関連する事項についての追加の情報及び助言（情報セキュリティの意識向上に関する追加の資料も含む。）を得るための連絡先及び情報源 マルウェアに対する保護について、マルウェアに感染した電子メール、ファイル又はプログラムの受領、送信又はインストールを特定し、可能ならば軽減する方法について、全ての利用者に意識向上又は訓練を提供する。（8.7.6） ウェブへのアクセスを含む、オンライン資源のセキュリティを保全に適切な使用について、要員を訓練する。（8.23.2） オンライン資源のセキュリティを保全に適切な使用についての訓練には、組織の規則、セキュリティ上の懸念を報告するための連絡先、及び制限されたウェブ資源に正当な業務上の理由によってアクセスする必要がある場合の例外プロセスを含める。 ウェブサイトで、セキュリティが保たれないことを通知するブラウザアドイザ外を無効にしないことを確実にするように、要員を訓練する。	6a-6.3.1	情報セキュリティの意識向上、教育及び訓練プログラムは、保護すべき組織の情報及び情報を保護するために実施されている情報セキュリティ管理策を考慮に入れて、組織の情報セキュリティ方針、トピック固有の方針及び情報セキュリティの関連する手順に沿って確立する。	予引に関連記載あり	7.2.2.2	情報セキュリティの意識向上プログラムは、保護すべき組織の情報及び情報を保護するために実施されている管理策を考慮に入れて、組織の情報セキュリティの方針群及び関連する手順に沿って確立する。
			6a-6.3.2	情報セキュリティの意識向上、教育及び訓練は、定期的に実施する。	予引に関連記載あり	7.2.2.13	情報セキュリティの教育及び訓練は、定期的に実施するだけでなく、情報システムの変更に伴い必要に応じて実施する。
			6a-6.3.3	可能な場合、開始時の意識向上、教育及び訓練を、新しい要員、及び情報セキュリティに関する要求事項が大幅に異なる新たな職位又は役割に異動した者にも適用する。	予引に関連記載あり	7.2.2.14	最初の教育及び訓練は、新入社員だけでなく、情報セキュリティに関する要求事項が大幅に異なる新たな職位又は役割に異動した者にも適用し、その役割が始まる前に実施する。
			6a-6.3.4	知識が伝わったこと、並びに意識向上、教育及び訓練プログラムの有効性を確認するため、意識向上、教育及び訓練の活動終了時に、要員の理解の評価を行う。	予引に関連記載あり	–	（対応項なし）
			6a-6.3.5	情報セキュリティの意識向上プログラムは、要員に対し、情報セキュリティに関する各自の責任及びその責任を果たす方法について、認識させること を狙いとする。	予引に関連記載あり	7.2.2.1	情報セキュリティの意識向上プログラムは、従業員、及び関係する場合は契約相手に対し、情報セキュリティに関する各自の責任及びその責任を果たす方法について、認識させること を狙いとする。
			6a-6.3.6	意識向上プログラムは、内部及び外部の要員を含め、組織における要員の役割を考慮に入れて、計画する。	予引に関連記載あり	7.2.2.4	情報セキュリティの意識向上プログラムは、組織における従業員の役割、及び関係する場合には契約相手の認識に対する組織の期待を考慮に入れて、計画する。
			6a-6.3.7	意識向上プログラムの活動は、長期にわたり、できれば定期的に実施する。	予引に関連記載あり	7.2.2.5	情報セキュリティの意識向上プログラムの活動は、新しい従業員及び契約相手も対象とされるよう、長期にわたり、できれば定期的に計画する。
			6a-6.3.8	意識向上プログラムの活動では、情報セキュリティインシデントから学んだ教訓を生かす。	予引に関連記載あり	7.2.2.6	情報セキュリティの意識向上プログラムは、定期的に更新して組織の方針及び手順に沿って、情報セキュリティインシデントから学んだ教訓が生かされるようにする。
			6a-6.3.9	意識向上プログラムには、キャンペーン、パンフレット、ポスター、会報、ウェブサイト、説明会、ブリーフィング、eラーニングモジュール、電子メールなど、適切な物理的又は仮想的な手段を通した多くの意識向上活動を含める。	予引に関連記載あり	7.2.2.3	情報セキュリティの意識向上プログラムには、キャンペーン（例えば、情報セキュリティの日）、及びパンフレット又は会報の発行のような、複数の意識向上活動を含める。
					予引に関連記載あり	7.2.2.7	意識向上のための訓練は、（例えば、教室での訓練、通信教育、インターネットを利用した訓練、自己学習その他を含む、多様な手段を用いて、）組織の情報セキュリティの意識向上プログラムで必要とされる場合に実施する。
			6a-6.3.10	情報セキュリティの意識向上には、例えば、次のような一般的な側面を含める。 a) 組織全体にわたる情報セキュリティに対する経営陣のコミットメント	予引に関連記載あり	7.2.2.8	情報セキュリティの教育及び訓練には、組織全体にわたる情報セキュリティに対する経営陣のコミットメントの提示を含める。
			6a-6.3.10	情報セキュリティの意識向上には、例えば、次のような一般的な側面を含める。 b) 情報セキュリティ計及びトピック固有の方針、基準、法令、規制、契約及び合意を考慮に入れた、適用される情報セキュリティの規則及び義務に関する精通度及び順守のニーズ	予引に関連記載あり	7.2.2.9	情報セキュリティの教育及び訓練には、方針、規格、法令、規制、契約及び合意で定められた、適用される情報セキュリティの規則及び義務を熟知し、これを順守する必要性を含める。
			6a-6.3.10	情報セキュリティの意識向上には、例えば、次のような一般的な側面を含める。 c) 自身が行動したこと及び行動しなかったことに対する個人のアカウンタビリティ、並びに組織及び利害関係者に属する情報のセキュリティを保ち、これを保護することに対する一般的な責任	予引に関連記載あり	7.2.2.10	情報セキュリティの教育及び訓練には、自身が行動したこと及び行動しなかったことに対する個人の責任、並びに組織及び外部関係者に属する情報のセキュリティを保つ、これを保護することに対する一般的な責任を含める。
			6a-6.3.10	情報セキュリティの意識向上には、例えば、次のような一般的な側面を含める。 d) 情報セキュリティに関する基本的な手順	予引に関連記載あり	7.2.2.11	情報セキュリティの教育及び訓練には、情報セキュリティに関する基本的な手順（例えば、情報セキュリティインシデントの報告）及び基本的な管理策（例えば、パスワードのセキュリティ、マルウェアの制御、クリアデスク）を含める。
			6a-6.3.10	情報セキュリティの意識向上には、例えば、次のような一般的な側面を含める。 e) 情報セキュリティに関連する事項についての追加の情報及び助言（情報セキュリティの意識向上に関する追加の資料も含む。）を得るための連絡先及び情報源	予引に関連記載あり	7.2.2.12	情報セキュリティの教育及び訓練には、情報セキュリティに関連する事項についての追加的な情報及び助言（情報セキュリティの教育及び訓練に関する追加の資料も含む）を得るための連絡先及び情報源を含める。
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 m) マルウェアに感染した電子メール、ファイル又はプログラムの受領、送信又はインストールを特定し、可能ならば軽減する方法について、全ての利用者に意識向上又は訓練を提供する。	予引に関連記載あり	12.2.1.2	認可されていないソフトウェアの使用を禁止する正式な方針を確立し、定期的に見直しを行う。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
			8c-8.23.6	ウェブへのアクセスを含む、オンライン資源のセキュリティを保った適切な使用について、要員を訓練する。	手引に関連記載あり	–	（対応項なし）
			8c-8.23.7	オンライン資源のセキュリティを保った適切な使用についての訓練には、組織の規則、セキュリティ上の懸念を報告するための連絡先、及び制限されたウェブ資源に正当な業務上の理由によってアクセスする必要がある場合の例外プロセスを含める。			
			8c-8.23.8	ウェブサイトで、セキュリティが保たれないことを通知するブラウザアドバイザリを利用者が無効にしないことを確実にするように、要員を訓練する。	手引に関連記載あり	–	（対応項なし）
6.3.2	特定の技能及び専門知識を必要とする役割をもつ技術チームに対して、適切な訓練計画を策定し、定期的に実施する。	組織は、特定の技能及び専門知識を必要とする役割をもつ技術チームに対して、適切な訓練計画を特定し、準備し、実施する。 技術チームは、装置・機器、システム、アプリケーション及びサービスに必要なセキュリティレベルを構成し、維持する技能をもつ。 技術チームに不足している技能がある場合、組織は処置をとり、それを取得させる。 教育及び訓練プログラムは、様々な形式（例えば、講義又は自己学習、専門スタッフ又はコンサルタントによる指導（オンザジョブトレーニング）、スタッフ異動を活動に従事させるローテーション、既に熟練している人材の採用及びコンサルタントの雇用）を検討する。教室、遠隔教育、ウェブ利用、自習式、及びその他異なる提供手段が利用可能である。 技術要員は、会報及び雑誌を購読する、又は技術的及び専門的な向上を目的とした会議及びイベントに参加することによって、自らの知識を最新の状態に保つ。	6a-6.3.11	組織は、特定の技能及び専門知識を必要とする役割をもつ技術チームに対して、適切な訓練計画を特定し、準備し、実施する。	手引に関連記載あり	–	（対応項なし）
			6a-6.3.12	技術チームは、装置・機器、システム、アプリケーション及びサービスに必要なセキュリティレベルを構成し、維持する技能をもつ。	手引に関連記載あり	–	（対応項なし）
			6a-6.3.13	技術チームに不足している技能がある場合、組織は処置をとり、それを取得させる。	手引に関連記載あり	–	（対応項なし）
			6a-6.3.14	教育及び訓練プログラムは、様々な形式を検討する。	手引に関連記載あり	7.2.2.18	教育及び訓練を効果的に実施するためのプログラムでは、講義又は自己学習のように、多様な教育及び訓練の形式（例えば、手順書確認訓練又はシナリオ非提示型訓練）を考慮して、定める。
			（6a-6.3.14参考）	教室、遠隔教育、ウェブ利用、自習式、及びその他異なる提供手段が利用可能である。	手引に関連記載あり	–	（対応項なし）
			6a-6.3.15	技術要員は、会報及び雑誌を購読する、又は技術的及び専門的な向上を目的とした会議及びイベントに参加することによって、自らの知識を最新の状態に保つ。	手引に関連記載あり	–	（対応項なし）
6.3.3	情報セキュリティインシデントの対処手順が適切に機能することを訓練等により確認する。	訓練等には、実際に使用する機器を利用した「実機訓練」や、逐次の状況付与を受けて判断等を行う「ロールプレイング」、状況設定の上で手順の検証を行う「シミュレーション」といった大掛かりなものほか、より簡易な「ウォークスルー」や「机上チェック」といった手法が存在する。要員等の習熟度等に応じて、必要な訓練等を検討し実施することが考えられる。 5.24.1で策定された情報セキュリティインシデント管理プロセスに則った確認をする。	–	（統一基準由来）	令和7年版にて追加（情報セキュリティ管理基準以外の由来）	–	（対応項なし）
6.3.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
6.4	懲戒手続 統制目標：情報セキュリティ方針違反を犯した要員及びその他の関連する利害関係者に対して処置をとるために、懲戒手続を正式に定め、伝達する。 目的：要員及びその他の関連する利害関係者が情報セキュリティ方針違反の結果を理解すること、違反を抑止すること、及びそれを犯した要員及びその他の関連する利害関係者を適切に扱うことを確実にするため。		6.4	懲戒手続 管理策 情報セキュリティ方針違反を犯した要員及びその他の関連する利害関係者に対して処置をとるために、懲戒手続を正式に定め、伝達する。 目的 要員及びその他の関連する利害関係者が情報セキュリティ方針違反の結果を理解すること、違反を抑止すること、及びそれを犯した要員及びその他の関連する利害関係者を適切に扱うことを確実にするため。		7.2.3	懲戒手続 情報セキュリティ違反を犯した従業員に対して処置をとるため、正式かつ周知された懲戒手続を備える。
6.4.1	正式な懲戒手続として、違反の内容や性質に応じた段階別の対応を定め、関連する要員及びその他の利害関係者に伝達する。	正式な懲戒手続は、次のような要素を考慮した段階別の対応を定める。 a) 違反の内容（誰が、何を、いつ、どのように）及び重大さ、並びにその結果 b) 違反が意図的である（悪意がある）か、又は意図的でない（偶発的）か。 c) 最初の違反か又は繰り返されたものか。 d) 違反者は、適切に教育・訓練されていたかどうか。 懲戒手続は、情報セキュリティ方針違反が生じたことの事前の確認を待って開始する。 証拠の収集については5.28参照。 懲戒手続の対応は、関連する法令、規制、契約及び事業上の要求事項、並びに必要に応じてその他の要素を考慮に入れる。 懲戒手続を、要員及びその他の関連する利害関係者が情報セキュリティ方針、トピック固有の方針、及び情報セキュリティの手順に違反することを防ぐための抑止力として使うことも望ましい。意図的な情報セキュリティ方針への違反には、直ちに処置をとることが求められる場合がある。	6a-6.4.1	懲戒手続は、情報セキュリティ方針違反が生じたことの事前の確認を待って開始する。	手引に関連記載あり	7.2.3.1	懲戒手続は、情報セキュリティ違反が生じたことの事前の確認を待って開始する。
			6a-6.4.2	正式な懲戒手続は、次のような要素を考慮した段階別の対応を定める。 a) 違反の内容（誰が、何を、いつ、どのように）及び重大さ、並びにその結果 b) 違反が意図的である（悪意がある）か、又は意図的でない（偶発的）か。 c) 最初の違反か又は繰り返されたものか。 d) 違反者は、適切に教育・訓練されていたかどうか。	手引に関連記載あり	7.2.3.3	正式な懲戒手続は、違反の内容及び重大さ並びにその業務上の影響、最初の違反か又は繰り返されたものか、違反者は、適切に教育・訓練されていたかどうか、関連する法令、取引契約、その他の必要な要素を考慮した段階別の対応を定める。
			6a-6.4.3	懲戒手続の対応は、関連する法令、規制、契約及び事業上の要求事項、並びに必要に応じてその他の要素を考慮に入れる。	手引に関連記載あり	–	（対応項なし）
			6a-6.4.4	懲戒手続を、要員及びその他の関連する利害関係者が情報セキュリティ方針、トピック固有の方針、及び情報セキュリティの手順に違反することを防ぐための抑止力として使う。	手引に関連記載あり	7.2.3.4	懲戒手続を、従業員が情報セキュリティ違反（従業員による組織の情報セキュリティのための方針群及び手順への違反並びに他の全ての情報セキュリティ違反）を起こすことを防ぐための抑止力として使う。
			（6a-6.4.4参考）	意図的な情報セキュリティ方針への違反には、直ちに処置をとることが求められる場合がある。	手引に関連記載あり	–	（対応項なし）
6.5	雇用の終了又は変更後の責任 統制目標：雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、施行し、関連する要員及びその他の利害関係者に伝達する。 目的：雇用又は契約を変更又は終了する手続の一部として、組織の利益を保護するため。		6.5	雇用の終了又は変更後の責任 管理策 雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、施行し、関連する要員及びその他の利害関係者に伝達する。 目的 雇用又は契約を変更又は終了する手続の一部として、組織の利益を保護するため。		7.3 7.3.1	雇用の終了及び変更 管理目的：雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。 雇用の終了又は変更に関する責任 雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、その従業員又は契約相手に伝達し、かつ、遂行させる。
6.5.1	雇用終了又は変更時にどの情報セキュリティの責任及び義務を引き続き有効とするかを定め、関連する要員及びその他の利害関係者に伝達する。	雇用の終了又は変更を管理する手続では、終了又は変更後にどの情報セキュリティの責任及び義務を引き続き有効とすることが望ましいかを定める。 雇用の終了又は変更後の情報セキュリティの責任及び義務に、情報の秘密保持、知的財産及び取扱いましたその他の知識、並びにその他の秘密保持契約に含まれる責任を含める（6.6参照）。	6a-6.5.1	雇用の終了又は変更を管理する手続では、終了又は変更後にどの情報セキュリティの責任及び義務を引き続き有効とすることが望ましいかを定める。	手引に関連記載あり	7.3.1.1	雇用の終了に関する責任の伝達には、実施中の情報セキュリティ要求事項及び法的責任、並びに適切であれば、従業員又は契約相手の、雇用の終了以降の一定期間継続する、秘密保持契約及び雇用条件に規定された責任を含める。
			6a-6.5.2	雇用の終了又は変更後の情報セキュリティの責任及び義務に、情報の秘密保持、知的財産及び取扱いましたその他の知識、並びにその他の秘密保持契約に含まれる責任を含める。	手引に関連記載あり	–	（対応項なし）
6.5.2	雇用の終了又は変更後も引き続き有効な情報セキュリティの責任及び義務は、その個人（外部の要員を含む）の雇用条件、契約又は合意に含める。	雇用又は契約の終了後も引き続き有効な責任及び義務は、その個人の雇用条件（6.2参照）、契約又は合意に含める。個人の雇用の終了後、定められた期間継続するその他の契約又は合意も、情報セキュリティの責任を含む場合がある。 雇用の終了又は変更の手続は、供給者の要員、供給者との契約若しくは組織との仕事の終了が生じる場合、又は組織内で仕事の変更がある場合に、外部の要員（すなわち、供給者）にも適用する。 責任又は雇用の変更は、現在の責任又は雇用の終了と新しい責任又は雇用の開始との組合せとして管理する。 職務を去る又は職務が変わる個人がもつ情報セキュリティの役割及び責任を特定し、別の個人に移す。 変更及び運用の手順を要員、その他の利害関係者及び関連する連絡先担当者に（例えば、顧客及び供給者に）伝達するための手続を確立する。	6a-6.5.3	雇用又は契約の終了後も引き続き有効な責任及び義務は、その個人の雇用条件、契約又は合意に含める。	管理策に関連記載あり	7.3.1.2	雇用の終了後も引き続き有効な責任及び義務は、従業員又は契約相手の雇用条件に含める。
			（6a-6.5.3参考）	個人の雇用の終了後、定められた期間継続するその他の契約又は合意も、情報セキュリティの責任を含む場合がある。	手引に関連記載あり	–	（対応項なし）
			6a-6.5.4	責任又は雇用の変更は、現在の責任又は雇用の終了と新しい責任又は雇用の開始との組合せとして管理する。	手引に関連記載あり	7.3.1.3	責任又は雇用の変更は、現在の責任又は雇用の終了と新しい責任又は雇用の開始との組み合わせとして管理する。
			6a-6.5.5	職務を去る又は職務が変わる個人がもつ情報セキュリティの役割及び責任を特定し、別の個人に移す。	手引に関連記載あり	–	（対応項なし）
			6a-6.5.6	変更及び運用の手順を要員、その他の利害関係者及び関連する連絡先担当者に伝達するための手続を確立する。	手引に関連記載あり	–	（対応項なし）
			6a-6.5.7	雇用の終了又は変更の手続は、供給者の要員、供給者との契約若しくは組織との仕事の終了が生じる場合、又は組織内で仕事の変更がある場合に、外部の要員（すなわち、供給者）にも適用する。	手引に関連記載あり	–	（対応項なし）
6.6	秘密保持契約又は守秘義務契約 統制目標：情報保護に対する組織のニーズを反映する秘密保持契約又は守秘義務契約は、特定し、文書化し、定期的にレビューし、要員及びその他の関連する利害関係者が署名する。 目的：要員又は外部の関係者がアクセスできる情報の秘密保持のため。		6.6	秘密保持契約又は守秘義務契約 管理策 情報保護に対する組織のニーズを反映する秘密保持契約又は守秘義務契約は、特定し、文書化し、定期的にレビューし、要員及びその他の関連する利害関係者が署名する。 目的 要員又は外部の関係者がアクセスできる情報の秘密保持のため。		13.2.4	秘密保持契約又は守秘義務契約 情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビュー し、文書化する。
6.6.1	秘密保持契約又は守秘義務契約には、秘密情報を保護するための要求事項を含める。	秘密保持契約又は守秘義務契約には、法的に強制できる表現を用いて、秘密情報を保護するための要求事項を取り上げる。 組織の情報セキュリティ要求事項に基づいて、契約の条件は、取り扱われる情報の種類、その分類レベル、その使用及び当事者に許可されるアクセスを考慮して決定する。 秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 a) 保護する情報の定義（例えば、秘密情報） b) 秘密を無期限に又は情報が一般公開されるまで保持する必要がある場合も含めた、契約の有効期間 c) 契約終了時に要求する処置 d) 認可されていない情報開示を避けるための、署名者の責任及び行為 e) 情報、企業秘密及び知的財産の帰属、並びにこれらと秘密情報の保護との関係 f) 秘密情報の許可された利用範囲、及び情報を利用する署名者の権利 g) 高度に取扱いに慎重を要する状況における、秘密情報に関わる行為の監査及び監視の権利 h) 認可されていない開示又は秘密情報漏えいの、通知及び報告のプロセス i) 契約終了時における情報の返却又は破棄に関する条件 j) 契約の不順守が発生した場合に講じるべき処置 組織は、適用される法域における秘密保持契約又は守秘義務契約の順守を考慮に入れる（5.31、5.32、5.33及び5.34参照）。	6a-6.6.1	秘密保持契約又は守秘義務契約には、法的に強制できる表現を用いて、秘密情報を保護するための要求事項を取り上げる。	手引に関連記載あり	13.2.4.1	秘密保持契約又は守秘義務契約には、法的に強制できる表現を用いて、秘密情報を保護するための要求事項を取り上げる。
			6a-6.6.3	組織の情報セキュリティ要求事項に基づいて、契約の条件は、取り扱われる情報の種類、その分類レベル、その使用及び当事者に許可されるアクセスを考慮して決定する。	手引に関連記載あり	13.2.4.3	秘密保持契約又は守秘義務契約の当事者の種類、並びに当事者に許可される秘密情報のアクセス及び取扱いを考慮して、契約の要素を選定又は追加する。
					手引に関連記載あり	13.2.4.14	組織の情報セキュリティ要求事項に応じて、秘密保持契約又は守秘義務契約に必要な要素を含める。
			6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 a) 保護する情報の定義	手引に関連記載あり	13.2.4.4	秘密保持契約又は守秘義務契約には、保護される情報の定義（例えば、秘密情報）を含める。
			6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 b) 秘密を無期限に又は情報が一般公開されるまで保持する必要がある場合も含めた、契約の有効期間	手引に関連記載あり	13.2.4.5	秘密保持契約又は守秘義務契約には、秘密を無期限に保持する場合も含めた、契約の有効期間を含める。
			6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 c) 契約終了時に要求する処置	手引に関連記載あり	13.2.4.6	秘密保持契約又は守秘義務契約には、契約終了時に要求する処置を含める。
			6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 d) 認可されていない情報開示を避けるための、署名者の責任及び行為	手引に関連記載あり	13.2.4.7	秘密保持契約又は守秘義務契約には、認可されていない情報開示を避けるための、署名者の責任及び行為を含める。
			6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 e) 情報、企業秘密及び知的財産の帰属、並びにこれらと秘密情報の保護との関係	手引に関連記載あり	13.2.4.8	秘密保持契約又は守秘義務契約には、情報、企業秘密及び知的財産の所有権、並びにこれらの秘密情報の保護との関連を含める。
			6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 f) 秘密情報の許可された利用範囲、及び情報を利用する署名者の権利	手引に関連記載あり	13.2.4.9	秘密保持契約又は守秘義務契約には、秘密情報の許可された利用範囲、及び情報を利用する署名者の権利を含める。
			6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 g) 高度に取扱いに慎重を要する状況における、秘密情報に関わる行為の監査及び監視の権利	手引に関連記載あり	13.2.4.10	秘密保持契約又は守秘義務契約には、秘密情報に関する行為の監査及び監視の権利を含める。
			6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 h) 認可されていない開示又は秘密情報漏えいの、通知及び報告のプロセス	手引に関連記載あり	13.2.4.11	秘密保持契約又は守秘義務契約には、認可されていない開示又は秘密情報漏えいの、通知及び報告のプロセスを含める。
			6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 i) 契約終了時における情報の返却又は破棄に関する条件	手引に関連記載あり	13.2.4.12	秘密保持契約又は守秘義務契約には、契約終了時における情報の返却又は破棄に関する条件を含める。
			6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 j) 契約の不順守が発生した場合に講じるべき処置	手引に関連記載あり	13.2.4.13	秘密保持契約又は守秘義務契約には、契約違反が発生した場合にとるべき処置を含める。
			6a-6.6.5	組織は、適用される法域における秘密保持契約又は守秘義務契約の順守を考慮に入れる。	手引に関連記載あり	13.2.4.15	秘密保持契約又は守秘義務契約は、その法域において適用される法令及び規制の全てに従う。
6.6.2	秘密保持契約又は守秘義務契約は、供給者を含む利害関係者及び組織の要員との間で締結される。	秘密保持契約又は守秘義務契約は、利害関係者及び組織の要員との間で締結される。	6a-6.6.2	秘密保持契約又は守秘義務契約は、利害関係者及び組織の要員との間で締結される。	管理策に関連記載あり	13.2.4.2	秘密保持契約又は守秘義務契約は、外部関係者又は組織の従業員に適用する。
6.6.3	秘密保持契約又は守秘義務契約に関する要求事項は、定期的に及びこれら要求に影響する変化が発生した場合に、レビューする。	秘密保持契約又は守秘義務契約に関する要求事項は、定期的に及びこれら要求に影響する変化が発生した場合に、レビューする。	6a-6.6.6	秘密保持契約又は守秘義務契約に関する要求事項は、定期的に及びこれら要求に影響する変化が発生した場合に、レビューする。	管理策に関連記載あり	13.2.4.16	秘密保持契約又は守秘義務契約に関する要求事項は、定期的に及びこれら要求に影響する変化が発生した場合に、レビューする。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
6.7	リモートワーク 統制目標：組織の構外でアクセス、処理又は保存される情報を保護するために、要員が遠隔で作業をする場合のセキュリティ対策を実施する。 目的：要員が遠隔で作業をする場合の情報セキュリティを確実にするため。		6.7	リモートワーク 管理策 組織の構外でアクセス、処理又は保存される情報を保護するために、要員が遠隔で作業をする場合のセキュリティ対策を実施する。 目的 要員が遠隔で作業をする場合の情報セキュリティを確実にするため。		6.2.2	テレワーキング テレワーキングの場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施する。
6.7.1	リモートワーク活動を許可する組織は、関連する条件及び制限を定めたリモートワークに関する方針を策定する。	リモートワークは、組織の構外から組織の要員が作業し、ハードコピーで又はICT機器を通じて電子的に情報にアクセスするときに常に行われる、リモートワーク環境は、テレワーキング、コンピュータ端末を用いた在宅勤務（telecommuting）、柔軟な作業場（flexible workplace）、仮想的な作業環境、及び遠隔保守と呼ばれる環境を含んでいる。 注記記載によって異なる、地域の法令及び規制のため、この手引の全ての推奨事項が適用できるとは限らない。 リモートワーク活動を許可する組織は、関連する条件及び制限を定めたリモートワークに関するトピック固有の方針を発行する。 適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。 a) 要員が配置されている法域を含め、リモートワークの場所及び周辺環境の物理的セキュリティを考慮に入れた、リモートワークの場所における既存の又は新たに提案する物理的セキュリティ b) 施錠可能なファイリングキャビネット、場所間におけるセキュリティを保つべき移送、並びにリモートアクセス、クリアデスク、情報及びその他の関連資産の印刷及び廃棄、情報セキュリティ事象の報告に関する規則など、遠隔物理環境のための規則及びセキュリティの仕組み（6.8参照） c) 期待される物理的なリモートワーク環境 d) 次を考慮した、通信のセキュリティに関する要求事項 1) 組織のシステムへのリモートアクセスの必要性 2) 通信回線からアクセスし、通信回線を通過する情報の取扱いに慎重を要する度合い 3) システム及びアプリケーションの取扱いに慎重を要する度合い e) 個人所有の機器での情報の処理及び保管を支援する、仮想デスクトップアクセスなどリモートアクセスの使用 f) リモートワークの場所における、他者（例えば、家族、友人）による情報又は資源への認可されていないアクセスの脅威 g) 公共の場所における、他者による情報又は資源への認可されていないアクセスの脅威 h) 家庭のネットワーク及び公衆ネットワークの使用並びに無線ネットワークサービスの設定に関する要求事項又は制限 i) ファイアウォール及びマルウェアからの保護などのセキュリティ対策の使用 j) システムを遠隔で展開し、初期化するためのセキュリティに配慮した仕組み k) 組織のネットワークへのリモートアクセスを許可する場合に、単一要素認証の仕組みのもつ弱性を考慮に入れた、認証及びアクセス権限有効化のためのセキュリティに配慮した仕組み	6a-6.7.1	リモートワーク活動を許可する組織は、関連する条件及び制限を定めたリモートワークに関するトピック固有の方針を発行する。	手引に関連記載あり	6.2.2.1	テレワーキング活動を許可する組織は、テレワーキングを行う場合の条件及び制限を定めた方針を発行する。
			6a-6.7.2	適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。 a) 要員が配置されている法域を含め、リモートワークの場所及び周辺環境の物理的セキュリティを考慮に入れた、リモートワークの場所における既存の又は新たに提案する物理的セキュリティ	手引に関連記載あり	6.2.2.2	テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、建物及び周辺環境の物理的セキュリティを考慮に入れた、テレワーキングの場所の既存の物理的セキュリティの状況を考慮して定める。
			6a-6.7.2	適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。 b) 施錠可能なファイリングキャビネット、場所間におけるセキュリティを保つべき移送、並びにリモートアクセス、クリアデスク、情報及びその他の関連資産の印刷及び廃棄、情報セキュリティ事象の報告に関する規則など、遠隔物理環境のための規則及びセキュリティの仕組み	手引に関連記載あり	–	（対応項なし）
			6a-6.7.2	適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。 c) 期待される物理的なリモートワーク環境	手引に関連記載あり	6.2.2.3	テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、提案された物理的なテレワーキングの環境を考慮して定める。
			6a-6.7.2	適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。 d) 次を考慮した、通信のセキュリティに関する要求事項 －組織のシステムへのリモートアクセスの必要性 －通信回線からアクセスし、通信回線を通過する情報の取扱いに慎重を要する度合い －システム及びアプリケーションの取扱いに慎重を要する度合い	手引に関連記載あり	6.2.2.4	テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、組織の内部システムへの遠隔アクセスの必要性、通信回線からアクセスし、通信回線を通過する情報の取扱い慎重度及び内部システムの取扱いに関する慎重度を考慮した、通信のセキュリティに関する要求事項を考慮して定める。
			6a-6.7.2	適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。 e) 個人所有の機器での情報の処理及び保管を支援する、仮想デスクトップアクセスなどリモートアクセスの使用	手引に関連記載あり	6.2.2.5	テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、個人所有の装置で情報を処理及び保管できないようにする仮想デスクトップへのアクセスを考慮して定める。
			6a-6.7.2	適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。 f) リモートワークの場所における、他者による情報又は資源への認可されていないアクセスの脅威	手引に関連記載あり	6.2.2.6	テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、住宅環境を共有する者（例えば、家族、友人）による、情報又は資源への認可されていないアクセスの脅威を考慮して定める。
			6a-6.7.2	適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。 g) 公共の場所における、他者による情報又は資源への認可されていないアクセスの脅威	手引に関連記載あり	–	（対応項なし）
			6a-6.7.2	適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。 h) 家庭のネットワーク及び公衆ネットワークの使用並びに無線ネットワークサービスの設定に関する要求事項又は制限	手引に関連記載あり	6.2.2.7	テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、家庭のネットワークの使用及び無線ネットワークサービスの設定に関する要求事項又は制限を考慮して定める。
			6a-6.7.2	適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。 i) ファイアウォール及びマルウェアからの保護などのセキュリティ対策の使用	手引に関連記載あり	6.2.2.11	テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、マルウェアに対する保護及びファイアウォールの要件を考慮して定める。
			6a-6.7.2	適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。 j) システムを遠隔で展開し、初期化するためのセキュリティに配慮した仕組み	手引に関連記載あり	–	（対応項なし）
			6a-6.7.2	適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。 k) 組織のネットワークへのリモートアクセスを許可する場合に、単一要素認証の仕組みのもつ弱性を考慮に入れた、認証及びアクセス権限有効化のためのセキュリティに配慮した仕組み	手引に関連記載あり	–	（対応項なし）
6.7.2	リモートワーク活動に関するセキュリティ対策を実施する。	リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。 a) 組織の管理下にない個人所有の機器の使用を許さない場合には、リモートワーク活動のための適切な機器及び保管用具の提供 b) 許可した作業、保持することができる情報の分類、並びにリモートワークを行う者にアクセスを認可する内部システム及びサービスの定義 c) 遠隔で作業する者及び支援を提供する者のための訓練の提供。これは、遠隔で作業しつつセキュリティに配慮した方法で業務を行う方法を含む。 d) 機器画面のロック及び非アクティブ状態タイマー、機器の位置追跡の有効化、遠隔データ消去機能のインストールに関する要求事項など、セキュリティに配慮したリモートアクセス方法を含む、適切な通信機器の提供 e) 物理的セキュリティ f) 家族及び訪問者による機器及び情報へのアクセスに関する規則及び手引 g) ハードウェア及びソフトウェアのサポート及び保守の提供 h) 保険の提供 i) バックアップ及び事業継続のための手順 j) 監査及びセキュリティの監視 k) リモートワークが終了したときの、権限及びアクセス権の失効並びに機器の返却 情報システムへリモートアクセスする場合、多要素認証を行う。	6a-6.7.3	リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。 a) 組織の管理下にない個人所有の機器の使用を許さない場合には、リモートワーク活動のための適切な機器及び保管用具の提供	手引に関連記載あり	6.2.2.12	テレワーキングを行う場合に考慮すべき指針及び取決めには、組織の管理下にない個人所有の装置の使用を許さない場合には、テレワーキング活動のための適切な装置及び保管用具の用意に関する事項を含める。
			6a-6.7.3	リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。 b) 許可した作業、保持することができる情報の分類、並びにリモートワークを行う者にアクセスを認可する内部システム及びサービスの定義	手引に関連記載あり	6.2.2.13	テレワーキングを行う場合に考慮すべき指針及び取決めには、許可した作業、作業時間、保持してもよい情報の分類、並びにテレワーキングを行う者にアクセスを認可する内部システム及びサービスの定義に関する事項を含める。
			6a-6.7.3	リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。 c) 遠隔で作業する者及び支援を提供する者のための訓練の提供。これは、遠隔で作業しつつセキュリティに配慮した方法で業務を行う方法を含む。	手引に関連記載あり	–	（対応項なし）
			6a-6.7.3	リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。 d) 機器画面のロック及び非アクティブ状態タイマー、機器の位置追跡の有効化、遠隔データ消去機能のインストールに関する要求事項など、セキュリティに配慮したリモートアクセス方法を含む、適切な通信機器の提供	手引に関連記載あり	6.2.2.14	テレワーキングを行う場合に考慮すべき指針及び取決めには、安全な遠隔アクセス方法を含め、適切な通信装置の用意に関する事項を含める。
			6a-6.7.3	リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。 e) 物理的セキュリティ	手引に関連記載あり	6.2.2.15	テレワーキングを行う場合に考慮すべき指針及び取決めには、物理的セキュリティに関する事項を含める。
			6a-6.7.3	リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。 f) 家族及び訪問者による機器及び情報へのアクセスに関する規則及び手引	手引に関連記載あり	6.2.2.16	テレワーキングを行う場合に考慮すべき指針及び取決めには、家族及び訪問者による装置及び情報へのアクセスに関する規則及び手引を含める。
			6a-6.7.3	リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。 g) ハードウェア及びソフトウェアのサポート及び保守の提供	手引に関連記載あり	6.2.2.17	テレワーキングを行う場合に考慮すべき指針及び取決めには、ハードウェア及びソフトウェアのサポート及び保守の用意を含める。
			6a-6.7.3	リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。 h) 保険の提供	手引に関連記載あり	6.2.2.18	テレワーキングを行う場合に考慮すべき指針及び取決めには、保険の用意を含める。
			6a-6.7.3	リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。 i) バックアップ及び事業継続のための手順	手引に関連記載あり	6.2.2.19	テレワーキングを行う場合に考慮すべき指針及び取決めには、バックアップ及び事業継続のための手順を含める。
			6a-6.7.3	リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。 j) 監査及びセキュリティの監視	手引に関連記載あり	6.2.2.20	テレワーキングを行う場合に考慮すべき指針及び取決めには、監査及びセキュリティの監視に関する事項を含める。
			6a-6.7.3	リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。 k) リモートワークが終了したときの、権限及びアクセス権の失効並びに機器の返却	手引に関連記載あり	6.2.2.21	テレワーキングを行う場合に考慮すべき指針及び取決めには、テレワーキングが終了したとき、権限及びアクセス権の失効並びに装置の返却に関する事項を含める。
6.8	情報セキュリティ事象の報告 統制目標：組織は、要員が発見した又は疑いをもった情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設ける。 目的：要員が特定する可能性がある情報セキュリティ事象を、時機を失せず、一貫性をもって効果的に報告することを支援するため。		6.8	情報セキュリティ事象の報告 管理策 組織は、要員が発見した又は疑いをもった情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設ける。 目的 要員が特定する可能性がある情報セキュリティ事象を、時機を失せず、一貫性をもって効果的に報告することを支援するため。		16.1.2	情報セキュリティ事象の報告 情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告する。
						16.1.3	情報セキュリティ弱点の報告 組織の情報システム及びサービスを利用する従業員及び契約相手に、システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は、どのようなものでも記録し、報告するように要求する。
6.8.1	全ての利用者に、情報セキュリティ事象をできるだけ速やかに報告する責任のあること、情報セキュリティ事象の報告手順及び情報セキュリティ事象を報告する連絡先を伝達する。	情報セキュリティインシデントの影響を防止又は最小化するために、全ての利用者に、情報セキュリティ事象をできるだけ速やかに報告する責任のあることを認識させておく。 全ての利用者に、情報セキュリティ事象の報告手順及び情報セキュリティ事象を報告する連絡先を認識させる。 報告の仕組みは、できるだけ簡単で使いやすく、いつでも利用できるものとする。 情報セキュリティ事象には、インシデント、違反及び弱い領域を含める。 情報セキュリティ事象の報告を検討する状況には、次を含める。 a) 効果のない情報セキュリティ管理策 b) 情報の機密性、完全性又は可用性に関する期待に対する違反 c) ヒューマンエラー d) 情報セキュリティ方針、トピック固有の方針又は適用される標準の不順守 e) 物理的セキュリティ対策に対する違反 f) 変更管理プロセスを経ないシステム変更 g) ソフトウェア若しくはハードウェアの誤動作又はその他の異常なシステム挙動 h) アクセス違反 i) 弱い領域 j) マルウェア感染の疑い	6a-6.8.1	情報セキュリティインシデントの影響を防止又は最小化するために、全ての要員及び利用者に、情報セキュリティ事象をできるだけ速やかに報告する責任のあることを認識させておく。	手引に関連記載あり	16.1.2.1	全ての従業員及び契約相手に、情報セキュリティ事象をできるだけ速やかに報告する責任のあることを認識させておく。
					手引に関連記載あり	16.1.3.1	全ての従業員及び契約相手は、情報セキュリティインシデントを防止するため、情報セキュリティ弱点をできるだけ速やかに連絡先に報告する。
			6a-6.8.2	全ての要員及び利用者に、情報セキュリティ事象の報告手順及び情報セキュリティ事象を報告する連絡先を認識させる。	手引に関連記載あり	16.1.2.2	全ての従業員及び契約相手に、情報セキュリティ事象の報告手順及び情報セキュリティ事象を報告する連絡先を認識させる。
			6a-6.8.3	報告の仕組みは、できるだけ簡単で使いやすく、いつでも利用できるものとする。	手引に関連記載あり	16.1.3.2	情報セキュリティ弱点の報告の仕組みは、できるだけ簡単で使いやすく、いつでも利用できるようにする。
			6a-6.8.4	情報セキュリティ事象には、インシデント、違反及び弱い領域を含める。	手引に関連記載あり	–	（対応項なし）
			6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 a) 効果のない情報セキュリティ管理策	手引に関連記載あり	16.1.2.3	情報セキュリティ事象の報告には、効果のないセキュリティ管理策を含める。
			6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 b) 情報の機密性、完全性又は可用性に関する期待に対する違反	手引に関連記載あり	16.1.2.4	情報セキュリティ事象の報告には、情報の完全性、機密性又は可用性に関する期待に対する違反を含める。
			6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 c) ヒューマンエラー	手引に関連記載あり	16.1.2.5	情報セキュリティ事象の報告には、人による誤りを含める。
			6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 d) 情報セキュリティ方針、トピック固有の方針又は適用される標準の不順守	手引に関連記載あり	16.1.2.6	情報セキュリティ事象の報告には、個別方針又は指針の不順守を含める。
			6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 e) 物理的セキュリティ対策に対する違反	手引に関連記載あり	16.1.2.7	情報セキュリティ事象の報告には、物理的セキュリティの取決めに対する違反を含める。
			6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 f) 変更管理プロセスを経ないシステム変更	手引に関連記載あり	16.1.2.8	情報セキュリティ事象の報告には、管理されていないシステム変更を含める。
			6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 g) ソフトウェア若しくはハードウェアの誤動作又はその他の異常なシステム挙動	手引に関連記載あり	16.1.2.9	情報セキュリティ事象の報告には、ソフトウェア又はハードウェアの誤動作を含める。
			6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 h) アクセス違反	手引に関連記載あり	16.1.2.10	情報セキュリティ事象の報告には、アクセス違反を含める。
			6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 i) 弱い領域	手引に関連記載あり	–	（対応項なし）
			6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 j) マルウェア感染の疑い	手引に関連記載あり	–	（対応項なし）
6.8.2	全ての利用者に、疑いをもった情報セキュリティの弱い領域の立証や検査を試みないように要求する。	全ての利用者に、疑いをもった情報セキュリティの弱い領域の立証を試みないように要求する。弱い領域を検査することは、システムの不正使用の全てと見られる可能性があり、情報システム又はサービスに損傷を与える可能性もあり、それはディジタル証拠を破損又は不明瞭にする可能性がある。最終的に、検査した個人に法的責任が発生する可能性がある。	6a-6.8.6	要員及び利用者に、疑いをもった情報セキュリティの弱い領域の立証を試みないように要求する。	手引に関連記載あり	–	（対応項なし）
			(6a-6.8.6参考)	弱い領域を検査することは、システムの不正使用の全てと見られる可能性があり、情報システム又はサービスに損傷を与える可能性もあり、それはディジタル証拠を破損又は不明瞭にする可能性がある。最終的に、検査した個人に法的責任が発生する可能性がある。	手引に関連記載あり	–	（対応項なし）
6.8.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
6.8.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
6.8.5	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
7.1	物理的セキュリティ境界 統制目標：情報及びその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。 目的：組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷及び干渉を防ぐため。		7	物理的管理策		11	物理的及び環境的セキュリティ
			7.1	物理的セキュリティ境界 管理策 情報及びその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。 目的 組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷及び干渉を防ぐため。		11.1	セキュリティを保つべき領域 管理目的：組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。
						11.1.1	物理的セキュリティ境界 取扱いに重要な情報又はその他の関連資産への認可されていない物理的アクセス、損傷及び干渉を防ぐため、物理的セキュリティ境界を定め、かつ、用いる。
7.1.1	情報及びその他の関連資産のある領域に関する物理的セキュリティ境界を定め、保護する。	物理的セキュリティ境界について、次の事項を、必要な場合には、考慮し、実施する。 a) 境界内に設置している資産の情報セキュリティ要求事項に従って、セキュリティ境界並びにそれぞれの境界の位置及び強度を定める。 b) 情報処理設備を収容した建物又は敷地が物理的に適切な境界をもつ（すなわち、境界には隙間がなく、又は容易に侵入できる箇所がない。）。敷地内の屋根、壁、天井及び床は、堅固な構造物とし、外部に接する全ての扉を、開閉制御の仕組み（例えば、かんぬき、警報装置、錠）によって、認可されていないアクセスから適切に保護する。要員が不在のときには、扉及び窓を施錠し、窓（特に一階の窓）については外部からの保護を考慮する。換気口の位置も考慮する。 c) セキュリティ境界上にある全ての防火扉は、適切な標準が要求するレベルの抵抗力を確立するために、壁と併せて、警告、監視及び試験を行う。防火扉は、不具合が発生しても安全側に作動するように運用する。	7a-7.1.1	物理的セキュリティ境界について、次の事項を、必要な場合には、考慮し、実施する。 a) 境界内に設置している資産の情報セキュリティ要求事項に従って、セキュリティ境界並びにそれぞれの境界の位置及び強度を定める。	手引に関連記載あり	11.1.1.1	情報及び情報処理施設のある領域を保護するために、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に基づいて、それぞれの物理的セキュリティ境界の位置及び強度を定める。
			7a-7.1.1	物理的セキュリティ境界について、次の事項を、必要な場合には、考慮し、実施する。 b) 情報処理設備を収容した建物又は敷地が物理的に適切な境界をもつ（すなわち、境界には隙間がなく、又は容易に侵入できる箇所がない。）。敷地内の屋根、壁、天井及び床は、堅固な構造物とし、外部に接する全ての扉を、開閉制御の仕組みによって、認可されていないアクセスから適切に保護する。要員が不在のときには、扉及び窓を施錠し、窓（特に一階の窓）については外部からの保護を考慮する。換気口の位置も考慮する。	手引に関連記載あり	11.1.1.2	情報及び情報処理施設のある領域を保護するために、情報処理施設を収容した建物又は敷地の境界は、物理的に適正にする（すなわち、境界には隙間がなく、又は容易に侵入できる箇所がない）。具体的には、以下の点を行う。 1.敷地内の屋根、壁及び床は、堅固な構造物とする。 2.外部に接する全ての扉を、開閉制御の仕組み（例えば、かんぬき、警報装置、錠）によって、認可されていないアクセスから適切に保護する。 3.要員が不在のときには、扉及び窓を施錠する。 4.窓（特に一階の窓）については外部から保護する。
			7a-7.1.1	物理的セキュリティ境界について、次の事項を、必要な場合には、考慮し、実施する。 c) セキュリティ境界上にある全ての防火扉は、適切な標準が要求するレベルの抵抗力を確立するために、壁と併せて、警告、監視及び試験を行う。防火扉は、不具合が発生しても安全側に作動するように運用する。	手引に関連記載あり	11.1.1.5	情報及び情報処理施設のある領域を保護するために、以下の2点を行う。 1.セキュリティ境界上にある全ての防火扉は、該当する地域標準、国内標準及び国際標準が要求するレベルの抵抗力を確立するために、壁と併せて、警報機能を備え、監視し、試験する 2.防火扉は、その地域の消防規則に従って、不具合が発生しても安全側に作動するように運用する
7.2	物理的入退 統制目標：セキュリティを保つべき領域は、適切な入退管理策及びアクセス場所（受付など）によって保護する。 目的：組織の情報及びその他の関連資産に、認可された物理的アクセスだけがなされることを確実にするため。		7.2	物理的入退 管理策 セキュリティを保つべき領域は、適切な入退管理策及びアクセス場所（受付など）によって保護する。 目的 組織の情報及びその他の関連資産に、認可された物理的アクセスだけがなされることを確実にするため。		11.1.2	物理的入退管理策 セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護する。
						11.1.6	受渡場所 荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。また、認可されていないアクセスを避けるために、それらの場所を情報処理施設から隔す。
7.2.1	セキュリティを保つべき領域の物理的入退に関するセキュリティ対策を実施する。	荷物の受渡場所などのアクセス場所（受付など）、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。 可能な場合には、認可されていないアクセスを避けるために、それらの場所を情報処理施設から隔す。 物理的入退の管理策の実施については、次の事項を考慮する。 a) 敷地及び建物へのアクセスは、認可された要員だけに制限する。物理的領域へのアクセス権の管理プロセスに、認可の提供、定期的なレビュー、更新及び失効を含める（5.18参照）。 b) 全ての アクセスについて、物理的な記録簿又は電子形式の監査証跡を、セキュリティを保って維持及び監視し、全ての記録（5.33参照）及び取扱いに慎重を要する認証情報を保護する。 c) 情報を処理する又は保管する領域へのアクセスを管理するためのプロセス及び技術的な仕組みを確立し、実装する。認証の仕組みには、アクセスカード、生体認証、又はアクセスカード及び秘密の個人識別番号のような二要素認証の仕組みの使用を含め、慎重を要する領域へのアクセスには、二重のセキュリティドアの採用を検討する。 d) 要員が監視している受付エリア、又は敷地若しくは建物への物理的なアクセスを管理するその他の手段を設定する。 e) 入退の際に要員及び利害関係者の持ち物を検査し、確認する。 注記：持ち物の検査が可能か否かに関して、地域の法令及び規制が存在する可能性がある。 f) 全ての要員及び利害関係者に、何らかの形式の、目に見える証明書の着用を要求する。関係者が付き添っていない訪問者及び目に見える証明書を着用していない者を見かけた場合は、直ちにセキュリティ要員に知らせる。常勤の従業員、供給者及び訪問者を識別しやすくするために、容易に区別できるバッジの使用を検討する。 g) セキュリティを保つべき領域又は情報処理施設への、供給者の要員によるアクセスは、限定的かつ必要なときにだけ許可する。このアクセスは、認可を必要とし、監視する。 h) 複数の組織の資産を保持する建物の場合、物理的なアクセスのセキュリティには特別な注意を払う。 i) 物理的なインシデントの起こりやすさが高くなった場合に強化できるように物理的セキュリティ対策を設計する。 j) 非常口などの他の入退場所を、認可されていないアクセスから保護する。 k) 物理的な鍵又は認証情報（例えば、ロックコード、オフィス、部屋及び鍵キャビネットなどの設備のコンピーテーションロック）の管理を確実にし、記録簿又は毎年の鍵監査、及び物理的な鍵又は認証情報へのアクセスの管理を確実にするための鍵管理プロセスを設定する（認証情報の詳細については5.17参照）。	7a-7.2.1	荷物の受渡場所などのアクセス場所（受付など）、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。	手引に関連記載あり	–	（対応項なし）
			7a-7.2.2	可能な場合には、認可されていないアクセスを避けるために、それらの場所を情報処理施設から隔す。	手引に関連記載あり	11.1.1.7	情報及び情報処理施設のある領域を保護するために、組織が自ら管理する情報処理施設は、外部関係者が管理する施設から物理的に分離する。
			7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 a) 敷地及び建物へのアクセスは、認可された要員だけに制限する。物理的領域へのアクセス権の管理プロセスに、認可の提供、定期的なレビュー、更新及び失効を含める。	手引に関連記載あり	11.1.2.6	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、秘密情報を処理又は保管する領域へのアクセスを、認可された者だけに制限する。
					手引に関連記載あり	11.1.2.12	セキュリティを保つべき領域へのアクセス権は、定期的にレビューし、更新し、必要なときには無効にする。
			7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 b) 全てのアクセスについて、物理的な記録簿又は電子形式の監査証跡を、セキュリティを保って維持及び監視し、全ての記録及び取扱いに慎重を要する認証情報を保護する。	手引に関連記載あり	11.1.2.7	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、全てのアクセスについて、物理的な記録簿又は電子形式の監査証跡を、セキュリティを保って維持及び監視する。
			7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 c) 情報を処理する又は保管する領域へのアクセスを管理するためのプロセス及び技術的な仕組みを確立し、実装する。認証の仕組みには、アクセスカード、生体認証、又はアクセスカード及び秘密の個人識別番号のような二要素認証の仕組みの採用を含め、慎重を要する領域へのアクセスには、二重のセキュリティドアの採用を検討する。	手引に関連記載あり	11.1.2.5	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、適切なアクセス制御（例えば、アクセスカード及び秘密の個人識別番号のような、二要素認証の仕組みの導入）を実施する。
			7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 d) 要員が監視している受付エリア、又は敷地若しくは建物への物理的なアクセスを管理するその他の手段を設定する。	手引に関連記載あり	–	（対応項なし）
			7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 e) 入退の際に要員及び利害関係者の持ち物を検査し、確認する。	手引に関連記載あり	–	（対応項なし）
			7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 f) 全ての要員及び利害関係者に、何らかの形式の、目に見える証明書の着用を要求する。関係者が付き添っていない訪問者及び目に見える証明書を着用していない者を見かけた場合は、直ちにセキュリティ要員に知らせる。常勤の従業員、供給者及び訪問者を識別しやすくするために、容易に区別できるバッジの使用を検討する。	手引に関連記載あり	11.1.2.8	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、全ての従業員、契約相手及び外部関係者に、何らかの形式の、目に見える証明書の着用を要求する。
					手引に関連記載あり	11.1.2.9	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、関係者が付き添っていない訪問者及び目に見える証明書を着用していない者を見かけた場合は、直ちにセキュリティ要員に知らせる。
			7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 g) セキュリティを保つべき領域又は情報処理施設への、供給者の要員によるアクセスは、限定的かつ必要なときだけ許可する。このアクセスは、認可を必要とし、監視する。	手引に関連記載あり	11.1.2.10	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、セキュリティを保つべき領域又は秘密情報処理施設への、外部のサポートサービス要員によるアクセスは、限定的かつ必要なときだけ許可する。
					手引に関連記載あり	11.1.2.11	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、セキュリティを保つべき領域又は秘密情報処理施設への、全てのアクセスは認可を必要とし、監視する。
			7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 h) 複数の組織の資産を保持する建物の場合、物理的なアクセスのセキュリティには特別な注意を払う。	手引に関連記載あり	–	（対応項なし）
			7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 i) 物理的なインシデントの起こりやすさが高くなった場合に強化できるように物理的セキュリティ対策を設計する。	手引に関連記載あり	–	（対応項なし）
			7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 j) 非常口などの他の入退場所を、認可されていないアクセスから保護する。	手引に関連記載あり	–	（対応項なし）
			7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 k) 物理的な鍵又は認証情報の管理を確実にし、記録簿又は毎年の鍵監査、及び物理的な鍵又は認証情報へのアクセスの管理を確実にするための鍵管理プロセスを設定する。	手引に関連記載あり	–	（対応項なし）
7.2.2	物理的入退の訪問者に関するセキュリティ対策を実施する。	物理的入退の訪問者に関する管理策では、次の事項を考慮する。 a) 適切な手段によって訪問者のアイデンティティを認証する。 b) 訪問者の出入りの日時を記録する。 c) 特定の認可された目的で、かつ、領域のセキュリティ要求事項及び緊急時の手順に関する指示の下でだけ、訪問者にアクセスを許可する。 d) 明示的に例外が許可されない限り、全ての訪問者を監視する。 荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 a) 建物外部からの受渡場所へのアクセスは、特定の認可された要員に制限する。 b) 受渡場所は、配達要員が建物の他の場所に認可されていないアクセスをすることなく荷積み及び荷降ろしできるように設計する。 c) 受渡場所の外部扉は、制限領域への扉が開いているときにはセキュリティを保つ。 d) 入荷物は、受渡場所から移動する前に、爆発物、化学物質又はその他の危険物がないかを検査する。 e) 入荷物は、事業所へ持ち込むときに資産の管理手順（5.9及び7.10参照）に従って登録する。 f) 可能な場合には、入荷と出荷とは、物理的に分離した場所で扱う。 g) 入荷物は、輸送中に関封された痕跡がないかを検査する。関封の痕跡が見つかった場合には、直ちにセキュリティ要員に報告する。	7a-7.2.4	物理的入退の訪問者に関する管理策では、次の事項を考慮する。 a) 適切な手段によって訪問者のアイデンティティを認証する。	手引に関連記載あり	11.1.2.4	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、適切な手段によって、訪問者の識別情報を認証する。
			7a-7.2.4	物理的入退の訪問者に関する管理策では、次の事項を考慮する。 b) 訪問者の出入りの日時を記録する。	手引に関連記載あり	11.1.2.2	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、アクセス方事前に承認されている場合を除いて、全ての訪問者を監督する。
			7a-7.2.4	物理的入退の訪問者に関する管理策では、次の事項を考慮する。 c) 特定の認可された目的で、かつ、領域のセキュリティ要求事項及び緊急時の手順に関する指示の下でだけ、訪問者にアクセスを許可する。	手引に関連記載あり	11.1.2.3	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、訪問者には、特定され、認可された目的のためのアクセスだけを許可し、その領域のセキュリティ要求事項及び緊急時の手順についての指示を与える。
			7a-7.2.4	物理的入退の訪問者に関する管理策では、次の事項を考慮する。 d) 明示的に例外が許可されない限り、全ての訪問者を監督する。	手引に関連記載あり	11.1.2.1	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、訪問者の入退の日付及び時刻を記録し、定期的かつイベント発生又はイベントの兆候がある場合に、レビューする。
			7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 a) 建物外部からの受渡場所へのアクセスは、特定の認可された要員に制限する。	手引に関連記載あり	11.1.6.1	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、建物外部からの受渡場所へのアクセスは、識別及び認可された要員に制限する。
			7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 b) 受渡場所は、配達要員が建物の他の場所に認可されていないアクセスをすることなく荷積み及び荷降ろしできるように設計する。	手引に関連記載あり	11.1.6.2	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、受渡場所は、配達要員が建物の他の場所にアクセスすることなく荷積み及び荷降ろしできるように設計する。
			7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 c) 受渡場所の外部扉は、制限領域への扉が開いているときにはセキュリティを保つ。	手引に関連記載あり	11.1.6.3	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、受渡場所の外部扉は、内部の扉が開いているときにはセキュリティを保つ。
			7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 d) 入荷物は、受渡場所から移動する前に、爆発物、化学物質又はその他の危険物がないかを検査する。	手引に関連記載あり	11.1.6.4	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷物は、受渡場所から移動する前に、爆発物、化学物質又はその他の危険物がないかを検査する。
			7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 e) 入荷物は、事業所へ持ち込むときに資産の管理手順に従って登録する。	手引に関連記載あり	11.1.6.5	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷物は、事業所へ持ち込むときに資産の管理手順に従って登録する。
			7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 f) 可能な場合には、入荷と出荷とは、物理的に分離した場所で扱う。	手引に関連記載あり	11.1.6.6	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷と出荷とは、物理的に分離した場所で扱う。
			7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 g) 入荷物は、輸送中に関封された痕跡がないかを検査する。関封の痕跡が見つかった場合には、直ちにセキュリティ要員に報告する。	手引に関連記載あり	11.1.6.7	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷物は、輸送中に関封された痕跡がないかを検査する。関封の痕跡が見つかった場合には、直ちにセキュリティ要員に報告する。
7.3	オフィス、部屋及び施設のセキュリティ 統制目標：オフィス、部屋及び施設に対する物理的セキュリティを設計し、実装する。 目的：オフィス、部屋及び施設内の組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷、及び干渉を防ぐため。		7.3	オフィス、部屋及び施設のセキュリティ 管理策 オフィス、部屋及び施設に対する物理的セキュリティを設計し、実装する。 目的 オフィス、部屋及び施設内の組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷、及び干渉を防ぐため。		11.1.3	オフィス、部屋及び施設のセキュリティ オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する。
7.3.1	オフィス、部屋及び施設に関するセキュリティ対策を実施する。	オフィス、部屋及び施設のセキュリティを保つために、次の事項を考慮する。 a) 重要な施設は、一般の人のアクセスが避けられる場所に設置する。 b) 適用可能な場合、建物を目立たせず、その目的を示す表示は最小限とし、情報処理活動の存在を示すものは、建物の内外を問わず、一切表示しないことを確実にする。 c) 施設は、秘密の情報又は活動が外部から見えたり聞こえたりしないように構成する。該当する場合、電磁遮蔽も考慮する。 d) 秘密情報処理施設の場所を示す案内板、内線電話帳及びオンラインアクセス可能な地図は、認可されていない者に容易に利用可能とならないようにする。	7a-7.3.1	オフィス、部屋及び施設のセキュリティを保つために、次の事項を考慮する。 a) 重要な施設は、一般の人のアクセスが避けられる場所に設置する。	手引に関連記載あり	11.1.3.1	オフィス、部屋及び施設のセキュリティを保つために、主要な施設は、一般の人のアクセスが避けられる場所に設置する。
			7a-7.3.1	オフィス、部屋及び施設のセキュリティを保つために、次の事項を考慮する。 b) 適用可能な場合、建物を目立たせず、その目的を示す表示は最小限とし、情報処理活動の存在を示すものは、建物の内外を問わず、一切表示しないことを確実にする。	手引に関連記載あり	11.1.3.2	オフィス、部屋及び施設のセキュリティを保つために、建物を目立たせず、その目的を示す表示は最小限とし、情報処理活動の存在を示すものは、建物の内外を問わず、一切表示しないように設計する。
			7a-7.3.1	オフィス、部屋及び施設のセキュリティを保つために、次の事項を考慮する。 c) 施設は、秘密の情報又は活動が外部から見えたり聞こえたりしないように構成する。該当する場合、電磁遮蔽も考慮する。	手引に関連記載あり	11.1.3.3	オフィス、部屋及び施設のセキュリティを保つために、施設は、秘密の情報又は活動が外部から見えたり聞こえたりしないように構成する。（該当する場合、電磁遮蔽も含める）
			7a-7.3.1	オフィス、部屋及び施設のセキュリティを保つために、次の事項を考慮する。 d) 秘密情報処理施設の場所を示す案内板、内線電話帳及びオンラインアクセス可能な地図は、認可されていない者に容易に利用可能とならないようにする。	手引に関連記載あり	11.1.3.4	オフィス、部屋及び施設のセキュリティを保つために、秘密情報処理施設の場所を示す案内板及び内線電話帳は、認可されていない者が容易にアクセスできないようにする。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
7.4	物理的セキュリティの監視 統制目標：施設は、認可していない物理的アクセスについて継続的に監視する。 目的：認可されていない物理的アクセスを検知し、抑止するため。		7.4	物理的セキュリティの監視 管理策 施設は、認可していない物理的アクセスについて継続的に監視することが望ましい。 目的 認可されていない物理的アクセスを検知し、抑止するため。		–	（対応項なし）
7.4.1	認可されていないアクセス又は疑わしい行動を検知するため、監視システム（監視カメラ、検知器、警報器など）によりその建物を監視する。	物理的な施設は、監視システムによって監視する。これには、内部で又は監視サービス提供者が管理する、警備員、侵入者警報、監視カメラなどのビデオ監視システム、及び物理的セキュリティ情報管理ソフトウェアを含む場合がある。 重要なシステムを収容している建物へのアクセスは、認可されていないアクセス又は疑わしい行動を検知するために、次の手段によって継続的に監視する。 a）組織の施設の内部及び外部の慎重を要する領域へのアクセスを目視し、記録するために、監視カメラなどのビデオ監視システムを設置する。 b）関連する適用される標準に従って、侵入者警報を起動する次のような接触、音又は動きの検知器を設置し、それらを定期的に試験する。 1）パニック警報装置として使用するために、接触が発生又は適当されたときに警報を起動する接触検知器 2）物体が視野を通過したときに警報を起動する、赤外線技術に基づく動きの検知器 3）ガラスが割れる音に敏感に反応し、それを使用して警報を発し、セキュリティ要員に警告することができるセンサー c）全ての外部扉及びアクセス可能な窓を対象として、これらの警報を使用する。無人の領域は常に警報器を稼働させる。その他の領域（例えば、コンピュータ室又は通信室）も対象とする。 監視及び記録の仕組みは、特に要員の監視及び記録された映像の保持期間に関して、データ保護及びPII保護の法令を含む地域の法規制を考慮して使用する。	7a-7.4.1	物理的な施設は、監視システムによって監視する。	手引に関連記載あり	–	（対応項なし）
			（7a-7.4.1参考）	これには、内部で又は監視サービス提供者が管理する、警備員、侵入者警報、監視カメラなどのビデオ監視システム、及び物理的セキュリティ情報管理ソフトウェアを含む場合がある。	手引に関連記載あり	–	（対応項なし）
			7a-7.4.2	重要なシステムを収容している建物へのアクセスは、認可されていないアクセス又は疑わしい行動を検知するために、次の手段によって継続的に監視する。 a）組織の施設の内部及び外部の慎重を要する領域へのアクセスを目視し、記録するために、監視カメラなどのビデオ監視システムを設置する。 b）関連する適用される標準に従って、侵入者警報を起動する次のような接触、音又は動きの検知器を設置し、それらを定期的に試験する。 1）パニック警報装置として使用するために、接触が発生又は適当されたときに警報を起動する接触検知器 2）物体が視野を通過したときに警報を起動する、赤外線技術に基づく動きの検知器 3）ガラスが割れる音に敏感に反応し、それを使用して警報を発し、セキュリティ要員に警告することができるセンサー c）全ての外部扉及びアクセス可能な窓を対象として、これらの警報を使用する。無人の領域は常に警報器を稼働させる。その他の領域も対象とする。	手引に関連記載あり	–	（対応項なし）
			7a-7.4.9	監視及び記録の仕組みは、特に要員の監視及び記録された映像の保持期間に関して、データ保護及びPII保護の法令を含む地域の法規制を考慮して使用する。	手引に関連記載あり	–	（対応項なし）
7.4.2	監視システムの設計及び動画などの監視情報の機密性を維持する。	監視システムの設計は機密性を維持する。これは、漏えいすると、検知されずに侵入することが容易になるためである。 監視システムは、動画などの監視情報が、認可されていない人によってアクセスされることを防止するため、又はシステムが適時かつ無効にされることを防止するために、認可されていないアクセスから保護する。 警報システムの制御盤は警報付きの領域に配置する。 安全警報の場合は、警報を設定した人が簡単に出られるような場所に配置する。 制御盤及び検知器は不正防止（tamperproof）の仕組みをもつ。 システムは、意図したとおり作動していることを確実にするため定期的に試験する（システムの構成要素がバケツ型動の場合は特に試験が重要である）。	7a-7.4.3	監視システムの設計は機密性を維持する。	手引に関連記載あり	–	（対応項なし）
			7a-7.4.4	監視システムは、動画などの監視情報が、認可されていない人によってアクセスされることを防止するため、又はシステムが適時かつ無効にされることを防止するために、認可されていないアクセスから保護する。	手引に関連記載あり	–	（対応項なし）
			7a-7.4.5	警報システムの制御盤は警報付きの領域に配置する。	手引に関連記載あり	–	（対応項なし）
			7a-7.4.6	安全警報の場合は、警報を設定した人が簡単に出られるような場所に配置する。	手引に関連記載あり	–	（対応項なし）
			7a-7.4.7	制御盤及び検知器は不正防止（tamperproof）の仕組みをもつ。	手引に関連記載あり	–	（対応項なし）
			7a-7.4.8	システムは、意図したとおり作動していることを確実にするため定期的に試験する。	手引に関連記載あり	–	（対応項なし）
7.5	物理的及び環境的脅威からの保護 統制目標：自然災害及びその他の意図的又は意図的でない、インフラストラクチャに対する物理的脅威などの物理的及び環境的脅威に対する保護を設計し、実装する。 目的：物理的及び環境的脅威に起因する事象の結果を防止又は低減するため。		7.5	物理的及び環境的脅威からの保護 管理策 自然災害及びその他の意図的又は意図的でない、インフラストラチャに対する物理的脅威などの物理的及び環境的脅威に対する保護を設計し、実装する。 目的 物理的及び環境的脅威に起因する事象の結果を防止又は低減するため。		11.1.4	外部及び環境の脅威からの保護 自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用する。
7.5.1	物理的及び環境的脅威に対する保護を設計し、セキュリティ対策を実施する。	物理的及び環境的脅威がたらす潜在的な結果を特定するためのリスクアセスメントは、物理的な場所で重要な運用を開始する前に、及び定期的に実施する。 必要な物理的及び環境的脅威からの保護策を実施し、また、物理的及び環境的脅威の変化を監視する。 火災、洪水、地震、爆発、暴力行為、有毒廃棄物、環境排出物、その他の自然災害又は人的災害などの物理的及び環境的脅威から生じるリスクを管理する方法について、専門家の助言を得る。 物理的施設の場所及び建造物では、次のことを考慮に入れる。 a）適切な標高、水域、構造断層線など、現地の地形 b）政治不安、犯罪活動又はテロ攻撃を誘発する可能性が高い場所など、都市の脅威 リスクアセスメントの結果に基づいて、関連する物理的及び環境的脅威を特定し、次の状況のような例において適切な管理策の採用を考慮する。 a）火災：記憶媒体及び関連する情報処理システムの火災による損傷を防ぐために、火災を早期に検知し、警報を送信する又は消火システムを起動することができるシステムを設置し、構成する。消火は、周囲の環境に対して最も適切な物質を使用して実施する（例えば、閉鎖空間における ガス）。 b）洪水：記憶媒体又は情報処理システムを含む領域の床の下に、洪水を早期に検知できるシステムを設置する。洪水が発生した場合に水ポンプ又は同等の手段をすぐに利用できるようにする。 c）電気サージ：サーバ及びクライアントの両方の情報システムを電気サージ又は同様の事象から保護し、そのような事象の結果を最小化することができるシステムを採用する。 d）爆発物及び武器：取扱いに慎重を要する情報処理施設に入る要員、車両又は商品に対して、爆発物又は武器がないかランダムな検査を実施する	7a-7.5.1	物理的及び環境的脅威がたらす潜在的な結果を特定するためのリスクアセスメントは、物理的な場所で重要な運用を開始する前に、及び定期的に実施する。	手引に関連記載あり	–	（対応項なし）
			7a-7.5.2	必要な物理的及び環境的脅威からの保護策を実施し、また、物理的及び環境的脅威の変化を監視する。	手引に関連記載あり	–	（対応項なし）
			7a-7.5.3	火災、洪水、地震、爆発、暴力行為、有毒廃棄物、環境排出物、その他の自然災害又は人的災害などの物理的及び環境的脅威から生じるリスクを管理する方法について、専門家の助言を得る。	手引に関連記載あり	11.1.4.1	火災、洪水、地震、爆発、暴力行為、及びその他の自然災害又は人的災害からの損傷を回避する方法について、専門家の助言を得る。
			7a-7.5.4	物理的施設の場所及び建造物では、次のことを考慮に入れる。 a）適切な標高、水域、構造断層線など、現地の地形 b）政治不安、犯罪活動又はテロ攻撃を誘発する可能性が高い場所など、都市の脅威	手引に関連記載あり	–	（対応項なし）
			7a-7.5.5	リスクアセスメントの結果に基づいて、関連する物理的及び環境的脅威を特定し、次の状況のような例において適切な管理策の採用を考慮する。 a）火災：記憶媒体及び関連する情報処理システムの火災による損傷を防ぐために、火災を早期に検知し、警報を送信する又は消火システムを起動することができるシステムを設置し、構成する。消火は、周囲の環境に対して最も適切な物質を使用して実施する。 b）洪水：記憶媒体又は情報処理システムを含む領域の床の下に、洪水を早期に検知できるシステムを設置する。洪水が発生した場合に水ポンプ又は同等の手段をすぐに利用できるようにする。 c）電気サージ：サーバ及びクライアントの両方の情報システムを電気サージ又は同様の事象から保護し、そのような事象の結果を最小化することができるシステムを採用する。 d）爆発物及び武器：取扱いに慎重を要する情報処理施設に入る要員、車両又は商品に対して、爆発物又は武器がないかランダムな検査を実施する。	手引に関連記載あり	–	（対応項なし）
7.6	セキュリティを保つべき領域での作業 統制目標：セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実施する。 目的：セキュリティを保つべき領域にある情報及びその他の関連資産を、この領域で作業する要員による損傷及び認可されていない干渉から保護するため		7.6	セキュリティを保つべき領域での作業 管理策 セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実施する。 目的 セキュリティを保つべき領域にある情報及びその他の関連資産を、この領域で作業する要員による損傷及び認可されていない干渉から保護するため。		11.1.5	セキュリティを保つべき領域での作業 セキュリティを保つべき領域での作業に関する手順を設計し、適用する。
7.6.1	セキュリティを保つべき領域での作業に関するセキュリティ対策を実施する。	セキュリティを保つべき領域での作業のセキュリティ対策は、全ての要員に適用し、セキュリティを保つべき領域で行われる全ての活動を対象とする。 セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 a）要員には、セキュリティを保つべき領域の存在又はその領域内での活動を、知る必要性の原則に基づく範囲でだけ認識させる。 b）安全面の理由のため及び悪意のある活動の機会を低減するための両面から、セキュリティを保つべき領域での監督されていない作業は、回避する。 c）セキュリティを保つべき領域が無人のときは、物理的に施錠し、定期的に検査する。 d）画像、映像、音声又はその他の記録装置（例えば、エンドポイント機器に付いたカメラ）は、認可されたもの以外は許可しない。 e）セキュリティを保つべき領域でのエンドポイント機器の携行及び使用を適切に管理する。 f）見やすいように又はアクセスできるように緊急手順を掲示する。	7a-7.6.1	セキュリティを保つべき領域での作業のセキュリティ対策は、全ての要員に適用し、セキュリティを保つべき領域で行われる全ての活動を対象とする。	手引に関連記載あり	11.1.5.6	セキュリティを保つべき領域での作業に関する取決めは、セキュリティを保つべき領域で行われる全ての活動に適用する。
			7a-7.6.2	セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 a）要員には、セキュリティを保つべき領域の存在又はその領域内での活動を、知る必要性の原則に基づく範囲でだけ認識させる。	手引に関連記載あり	11.1.5.1	セキュリティを保つべき領域での作業に関する手順の設計においては、セキュリティを保つべき領域の存在又はその領域内での活動は、業務上知る必要のある要員にのみ知らせることを含める。
			7a-7.6.2	セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 b）安全面の理由のため及び悪意のある活動の機会を低減するための両面から、セキュリティを保つべき領域での監督されていない作業は、回避することを含める。	手引に関連記載あり	11.1.5.2	セキュリティを保つべき領域での作業に関する手順の設計に、安全面の理由のため及び悪意ある活動の機会を防止するための両面から、セキュリティを保つべき領域での監督されていない作業は、回避することを含める。
			7a-7.6.2	セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 c）セキュリティを保つべき領域が無人のときは、物理的に施錠し、定期的に検査する。	手引に関連記載あり	11.1.5.3	セキュリティを保つべき領域での作業に関する手順の設計に、セキュリティを保つべき領域が無人のときは、物理的に施錠し、定期的に点検することを含める。
			7a-7.6.2	セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 d）画像、映像、音声又はその他の記録装置は、認可されたもの以外は許可しない。	手引に関連記載あり	11.1.5.4	セキュリティを保つべき領域での作業に関する手順の設計に、画像、映像、音声又はその他の記録装置（例えば、携帯端末に付いたカメラ）は、認可されたもの以外は許可しないことを含める。
			7a-7.6.2	セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 e）セキュリティを保つべき領域での利用者エンドポイント機器の携行及び使用を適切に管理する。	手引に関連記載あり	11.1.5.5	セキュリティを保つべき領域での作業に関する取決めには、その領域で作業する従業員及び外部の利用者に対する管理策を含める。
			7a-7.6.2	セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 f）見やすいように又はアクセスできるように緊急手順を掲示する。	手引に関連記載あり	–	（対応項なし）
7.7	クリアデスク・クリアスクリーン 統制目標：書類及び取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定め、適切に実施させる。 目的：通常の勤務時間内及び時間外の、机、スクリーン及びその他のアクセス可能な場所にある情報への認可されていないアクセス、情報の消失及び損傷のリスクを低減するため。		7.7	クリアデスク・クリアスクリーン 管理策 書類及び取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定め、適切に実施させる。 目的 通常の勤務時間内及び時間外の、机、スクリーン及びその他のアクセス可能な場所にある情報への認可されていないアクセス、情報の消失及び損傷のリスクを低減するため。		11.2.9	クリアデスク・クリアスクリーン方針 書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用する。 （脚注）クリアデスクとは、机上に書類を放置しないことをいう。また、クリアスクリーンとは、情報をスクリーンに残したまま離席しないことをいう。
7.7.1	書類及び取外し可能な記憶媒体に対するクリアデスク及び情報処理施設に対するクリアスクリーンに関する方針を策定する。	組織は、クリアデスク・クリアスクリーンに関するトピック固有の方針を確立し、全ての関連する利害関係者へ伝達する。	7a-7.7.1	組織は、クリアデスク・クリアスクリーンに関するトピック固有の方針を確立し、全ての関連する利害関係者へ伝達する。	手引に関連記載あり	11.2.9.1	クリアデスク・クリアスクリーン方針において、組織の、情報分類、法的及び契約上の要求事項、並びにそれらに対応する リスク及び文化的側面を含める。
7.7.2	書類及び取外し可能な記憶媒体に対するクリアデスク及び情報処理施設に対するクリアスクリーンに関するセキュリティ対策を実施する。	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 a）取扱いに慎重を要する業務情報又は重要な業務情報（例えば、紙又は電子記憶媒体上の業務情報）は、必要のない場合、特にオフィスに誰もいないときには、施錠して（理想的には金庫、書庫又はセキュリティを備えた他の形態の収納用具に）保管しておく。 b）使用していないまたは施錠時には、施錠又はその他のセキュリティ手段によってエンドポイント機器を保護する。 c）エンドポイント機器は、施錠時には、ログオフ状態にしておか、又は利用者認証機能で管理されたスクリーン及びキーボードのロック機能によって保護しておく。全てのコンピュータ及びシステムは、タイムアウト又は自動ログアウト機能をも構成する。 d）印刷を実行した人に、プリンタ又は複合機からの出力をすぐに収集させる。印刷を実行した人だけが、プリンタの横に立ったときだけ、印刷物を得ることができる認証機能をもつプリンタを利用する。 e）取扱いに慎重を要する情報を含む文書及び取外し可能な記憶媒体をセキュリティを保って管理し、不要になった場合はセキュリティを保った処分の仕組みを使用してそれらを破棄する。 f）画面上のポップアップの設定に関する規則及び手引を確立し、伝達する（例えば、プレゼンテーション、画面共有の際、又は公共の場所においては、可能であれば新しい電子メール及びメッセージングのポップアップを抑止する。）。 g）不要になった場合には、ホワイトボード上及びその他の種類の掲示上の取扱いに慎重を要する情報又は重要な情報を消去する。 組織は、組織の資産（例えば、引き出し又は収納用具の後ろに落ちた文書など）を後に残さないことを確実にするため、退出する前に最後の清掃を行うことを含む、施設から退去する際の適切な手順をもつ。	7a-7.7.2	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 a）取扱いに慎重を要する業務情報又は重要な業務情報は、必要のない場合、特にオフィスに誰もいないときには、施錠して（理想的には金庫、書庫又はセキュリティを備えた他の形態の収納用具に）保管する。	手引に関連記載あり	11.2.9.2	取扱いに慎重を要する業務情報又は重要な業務情報（例えば、紙又は電子記憶媒体上の業務情報）は、必要のない場合、特にオフィスに誰もいないときには、施錠して（理想的には金庫、書庫又はセキュリティを備えた他の形態の収納用具に）保管する。
			7a-7.7.2	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 b）使用していないまたは施錠時には、施錠又はその他のセキュリティ手段によってエンドポイント機器を保護する。	手引に関連記載あり	11.2.9.3	コンピュータ及び端末は、施錠時には、ログオフ状態にしておか、又はパスワード、トークン若しくは類似の利用者認証機能で管理されたスクリーン及びキーボードのロック機能によって保護する。
			7a-7.7.2	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 c）利用者エンドポイント機器は、施錠時には、ログオフ状態にしておか、又は利用者認証機能で管理されたクリーン及びキーボードのロック機能によって保護しておく。全てのコンピュータ及びシステムは、タイムアウト又は自動ログアウト機能をも構成する。	手引に関連記載あり	11.2.9.4	コンピュータ及び端末は、利用しないときは、施錠、パスワード又は他の管理策によって保護する。
			7a-7.7.2	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 d）印刷を実行した人に、プリンタ又は複合機からの出力をすぐに収集させる。印刷を実行した人だけが、プリンタの横に立ったときだけ、印刷物を得ることができる認証機能をもつプリンタを利用する。	手引に関連記載あり	11.2.9.6	取扱いに慎重を要する情報又は機密扱い情報を含む媒体は、プリンタから直ちに取り出す。
			7a-7.7.2	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 e）取扱いに慎重を要する情報を含む文書及び取外し可能な記憶媒体をセキュリティを保って保管し、不要になった場合はセキュリティを保った処分の仕組みを使用してそれらを破棄する。	手引に関連記載あり	–	（対応項なし）
			7a-7.7.2	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 f）画面上のポップアップの設定に関する規則及び手引を確立し、伝達する。	手引に関連記載あり	–	（対応項なし）
			7a-7.7.2	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 g）不要になった場合には、ホワイトボード上及びその他の種類の掲示上の取扱いに慎重を要する情報又は重要な情報を消去する。	手引に関連記載あり	–	（対応項なし）
			7a-7.7.3	組織は、組織の資産を後に残さないことを確実にするため、退出する前に最後の清掃を行うことを含む、施設から退去する際の適切な手順をもつ。	手引に関連記載あり	–	（対応項なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
7.8	装置の設置及び保護 統制目標：装置は、セキュリティを保って設置し、保護する。 目的：物理的及び環境的脅威、並びに認可されていないアクセス及び損傷によるリスクを低減するため。		7.8	装置の設置及び保護 管理策 装置は、セキュリティを保って設置し、保護する。 目的 物理的及び環境的脅威、並びに認可されていないアクセス及び損傷によるリスクを低減するため。		11.2 11.2.1	装置 管理目的：資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。 装置の設置及び保護 装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、保護する。
7.8.1	装置を保護するためのセキュリティ対策を実施する。	装置を保護するために、次の事項を考慮する。 a) 装置は、作業領域への不必要なアクセスを最小限とし、認可されていないアクセスを回避するように設置する。 b) 取扱いに慎重を要するデータを扱う情報処理設備は、設備の使用中に認可されていない者が情報をのぞき見るリスクを低減するために、その位置を慎重に定める。 c) 潜在的な物理的及び環境的脅威［例えば、盗難、火災、爆発、ばい（煙）煙、水（又は給水の不具合）、しんあい（塵埃）、振動、化学的汚染、電力供給の妨害、通信妨害、電磁波放射、破壊］のリスクを最小限に抑えるための管理策を採用する。 d) 情報処理施設・設備の周辺での飲食及び喫煙に関する指針を確立する。 e) 情報処理施設・設備の運用に悪影響を与える可能性がある環境条件（例えば、温度、湿度）を監視する。 f) 全ての建物に、落雷からの保護を適用する。全ての電力及び通信の引込線に避雷器を装着する。 g) 作業現場などの環境にある装置には、特別な保護方法（例えば、キーボードカバー）の使用を考慮する。 h) 電磁波の放射による情報漏えいのリスクを最小限にするため、秘密情報を処理する装置を保護する。 i) 組織が管理する情報処理施設・設備を、組織が管理していない情報処理施設・設備から物理的に分離 装置には、情報処理施設・設備の技術補成要素、無停電電源装置（UPS）及びバッテリ、発電機、交流発電機及びコンバータ、物理的侵入検知システム及び層報装置、煙探知器、消火器、空調並びに非常機が含まれる。	7b-7.8.1 7b-7.8.1 7b-7.8.1 7b-7.8.1 7b-7.8.1 7b-7.8.1 7b-7.8.1 7b-7.8.1	装置を保護するために、次の事項を考慮する。 a) 装置は、作業領域への不必要なアクセスを最小限とし、認可されていないアクセスを回避するように設置する。 装置を保護するために、次の事項を考慮する。 b) 取扱いに慎重を要するデータを扱う情報処理設備は、設備の使用中に認可されていない者が情報をのぞき見るリスクを低減するために、その位置を慎重に定める。 装置を保護するために、次の事項を考慮する。 c) 潜在的な物理的及び環境的脅威のリスクを最小限に抑えるための管理策を採用する。 装置を保護するために、次の事項を考慮する。 d) 情報処理施設・設備の周辺での飲食及び喫煙に関する指針を確立する。 装置を保護するために、次の事項を考慮する。 e) 情報処理施設・設備の運用に悪影響を与える可能性がある環境条件を監視する。 装置を保護するために、次の事項を考慮する。 f) 全ての建物に、落雷からの保護を適用する。全ての電力及び通信の引込線に避雷器を装着する。 装置を保護するために、次の事項を考慮する。 g) 作業現場などの環境にある装置には、特別な保護方法（例えば、キーボードカバー）を使用する。 装置を保護するために、次の事項を考慮する。 h) 電磁波の放射による情報漏えいのリスクを最小限にするため、秘密情報を処理する装置を保護する。 装置を保護するために、次の事項を考慮する。 i) 組織が管理する情報処理施設・設備を、組織が管理していない情報処理施設・設備から物理的に分離する。	手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり	11.2.1.1 11.2.1.3 11.2.1.2 11.2.1.5 11.2.1.6 11.2.1.7 11.2.1.8 11.2.1.9 11.2.1.10 11.2.1.4	装置を保護するために、装置は、作業領域への不必要なアクセスが最小限になるように設置する。 装置を保護するために、認可されていないアクセス（遠隔操作による起動を含む。）を回避するよう、保管設備のセキュリティを保つ。 装置を保護するために、取扱いに慎重を要するデータ(を扱う)情報処理施設は、施設の使用中に認可されていない者が情報をのぞき見るリスクを低減するよう、その位置を慎重に定める。 装置を保護するために、潜在的な物理的及び環境的脅威［例えば、盗難、火災、爆発、ばい（煙）煙、水（又は給水の不具合）、しんあい（塵埃）、振動、化学的汚染、電力供給の妨害、通信妨害、電磁波放射、破壊］のリスクを最小限に抑えるよう管理策を採用する。 装置を保護するために、情報処理施設の周辺での飲食及び喫煙に関する指針を確立する。 装置を保護するために、情報処理施設の運用に悪影響を与えることがある環境条件（例えば、温度、湿度）を監視する。 装置を保護するために、全ての建物に、落雷からの保護を適用する。全ての電力及び通信の引込線に避雷器を装着する。 装置を保護するために、作業現場などの環境にある装置には、特別な保護方法（例えば、キーボードカバー）を使用する。 装置を保護するために、秘密情報を処理する装置は、電磁波の放射による情報漏えいのリスクを最小限にする。 装置を保護するために、特別な保護を必要とする装置は、それ以外の装置を分離するか、若しくは装置間に障壁を設ける。
7.9	構外にある資産のセキュリティ 統制目標：構外にある資産を保護する。 目的：構外にある装置・機器の紛失、損傷、盗難又は侵害、及び組織の業務の中断を防止するため。		7.9	構外にある資産のセキュリティ 管理策 構外にある資産を保護する。 目的 構外にある装置・機器の紛失、損傷、盗難又は侵害、及び組織の業務の中断を防止するため。		11.2.5 11.2.6	資産の移動 装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さない。 構外にある装置及び資産のセキュリティ 構外にある資産に対しては、構外での作業に伴って、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用する。
7.9.1	構外にある装置・機器を保護するためのセキュリティ対策を実施する。	組織が所有する装置・機器、及び個人が所有し組織のために用いる機器［私物機器の業務利用（BYOD）］を含む、情報を保管又は処理する、組織の構外で使用する装置・機器（例えば、モバイル機器）は全て保護する必要がある。構外にある装置・機器の使用は、管理者によって認可される。 組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。 a) 構外に持ち出した装置・機器及び記憶媒体は、公共の場所で、かつ、セキュリティが保たれない場所に無人状態で放置しない。 b) 装置・機器の保護［例えば、強力な電磁場、水、熱、湿度、ほこり（埃）にさらすことに対する保護］に関する製造業者の指示を常に守る。 c) 構外にある装置・機器を、複数の個人又は利害関係者の間で移動する場合には、その装置・機器の受渡記録を明記した記録（少なくとも、その装置・機器に対して責任を負う者の氏名及び組織を含むもの）を維持する。資産とともに移動する必要のない情報は、移動前にセキュリティを保って削除する。 d) 必要かつ実施可能な場合には、組織の構内から装置・機器及び媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する（5.14参照）。 e) 公共交通機関において機器（例えば、モバイル又はラップトップ）上の情報を見られること、及びのぞき見に関連するリスクに対して保護する。 f) 機器の位置追跡及び遠隔データ消去機能を実施する。 組織の構外に装置［アンテナ、現金自動預け払い機（ATM）など］を恒久的に設置すると、損傷、盗難又は侵受のリスクが高くなる可能性がある。これらのリスクは、場所によってかなり異なる可能性がある。装置を恒久的に設置する構外のそれぞれの場所に応じた最も適切な対策の決定には、リスクを考慮する。 装置を組織の構外に恒久的に設置する場合、次の事項を考慮する。 a) 物理的セキュリティの監視（7.4参照） b) 物理的及び環境的脅威からの保護（7.5参照） c) 物理的アクセス制御及び不正防止（tamper proofing）の管理策 d) 論理的アクセス制御	7b-7.9.1 7b-7.9.2 7b-7.9.2 7b-7.9.2 7b-7.9.2 7b-7.9.3 7b-7.9.4	構外にある装置・機器の使用は、管理者によって認可される。 組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。 a) 構外に持ち出した装置・機器及び記憶媒体は、公共の場所で、かつ、セキュリティが保たれない場所に無人状態で放置しない。 組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。 b) 装置・機器の保護に関する製造業者の指示を常に守る。 組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。 c) 構外にある装置・機器を、複数の個人又は利害関係者の間で移動する場合には、その装置・機器の受渡記録を明記した記録（少なくとも、その装置・機器に対して責任を負う者の氏名及び組織を含むもの）を維持する。資産とともに移動する必要のない情報は、移動前にセキュリティを保って削除する。 組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。 d) 必要かつ実施可能な場合には、組織の構内から装置・機器及び媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する 装置を恒久的に設置する構外のそれぞれの場所に応じた最も適切な対策の決定には、リスクを考慮する。 装置を組織の構外に恒久的に設置する場合、次の事項を考慮する。 a) 物理的セキュリティの監視 b) 物理的及び環境的脅威からの保護 c) 物理的アクセス制御及び不正防止（tamper proofing）の管理策 d) 論理的アクセス制御	手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり －	11.2.6.1 11.2.6.2 11.2.6.3 11.2.6.5 11.2.5.1 11.2.5.3 11.2.6.4 11.2.6.6 （対応項なし）	情報を保管及び処理する装置（組織が所有する装置、及び個人が所有し組織のために用いる装置）を組織の構外で用いる場合は、管理策の認可を得る。 構外に持ち出した装置及び媒体は、公共の場所に無人状態で放置しない。 構外にある装置の保護のために、装置の保護（例えば、強力な電磁場にさらすことに対する保護）に関する製造業者の指示を常に守る。 構外にある装置の保護のために、構外にある装置を、複数の個人又は外部関係者の間で移動する場合には、その装置の受渡記録を明記した記録（少なくとも、その装置に対して責任を負う者の氏名及び組織を含むもの）を維持する。 資産を構外に持ち出すことを許す権限をもつ従業員及び外部の利用者を特定し、承認する。 資産が構外に持ち出されていることを記録し、また、返却時に記録する。 構外にある装置の保護のために、在宅勤務、テレワーキング及び一時的サイトのような構外の場所についての管理策を、リスクアセスメントに基づいて決定し、状況に応じた管理策（例えば、施設可能な文書保管庫、クリアデスク方針、コンピュータのアクセス制御、セキュリティを保ったオフィスの通信）を適切に適用する。 リスク（例えば、損傷、盗難、侵受）は、場所によってかなり異なる場合があるため、それぞれの場所に応じた最も適切な管理策は、リスクを考慮して決定する。
7.10	記憶媒体 統制目標：記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理する。 目的：記憶媒体上の情報に対して認可された開示、変更、移動又は破棄だけがなされることを確実にするため。		7.10	記憶媒体 管理策 記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理する。 目的 記憶媒体上の情報に対して認可された開示、変更、移動又は破棄だけがなされることを確実にするため。		8.3 8.3.1 8.3.2 8.3.3	媒体の取扱い 管理目的：媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。 取外し可能な媒体の管理 組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施する。 媒体の処分 媒体が不要になった場合は、正式な手順を用いて、セキュリティを保って処分する。 物理的媒体の輸送 情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護する。
7.10.1	取外し可能な記憶媒体の管理に関する方針を策定し、管理する。	取外し可能な記憶媒体の管理において、次の事項を考慮する。 a) 取外し可能な記憶媒体の管理に関するポリシ及び管理の方針を確立し、取外し可能な記憶媒体を使用する又は取り扱う全ての人にポリシ及び管理の方針を伝達する。 b) 必要かつ実施可能な場合には、組織から記憶媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する。 c) 全ての記憶媒体は、情報の分類に従って安全でセキュリティが保たれた環境に保管し、製造業者の仕様に従って、環境の脅威（熱、水分、湿度、電場、経年劣化など）から保護する。 d) 情報の機密性又は完全性が重要な考慮事項である場合は、取外し可能な記憶媒体上の情報を保護するために、暗号技術を用いる。 e) 保管した情報がまだ必要な間に記憶媒体が劣化する又は交換されるため、読み出せなくなる前に情報を新しい記憶媒体に移し替える。 f) 価値の高い情報は、一度に損傷又は消失するリスクを上げるためにも、複数の複製を別の記憶媒体に保管する。 g) 情報を失う危険性を小さくするために、取外し可能な記憶媒体の登録を検討する。 h) 取外し可能な記憶媒体のポート［例えば、セキュアデジタル（SD）カードスロット及びユニバーサルシリアルバス（USB）ポート］は、組織にその利用について理由があるときだけ有効とする。 i) 取外し可能な記憶媒体を用いる必要がある場合、そのような記憶媒体への情報の転送を監視する。 j) 情報は、物理的な輸送中、例えば、郵便サービス又は宅配便で記憶媒体を送る場合に、認可されていないアクセス、不正使用又は破損に関して忧い頃である可能性がある。 媒体は紙の文書を含んでいる、物理的記憶媒体を輸送する場合には、5.14のセキュリティ対策を適用する。	7b-7.10.1 7b-7.10.1 7b-7.10.1 7b-7.10.1 7b-7.10.1 7b-7.10.1 7b-7.10.1 7b-7.10.1 7b-7.10.1 （7b-7.10.1参考）	取外し可能な記憶媒体の管理において、次の事項を考慮する。 a) 取外し可能な記憶媒体の管理に関するポリシ及び管理の方針を確立し、取外し可能な記憶媒体を使用する又は取り扱う全ての人にポリシ及び管理の方針を伝達する。 取外し可能な記憶媒体の管理において、次の事項を考慮する。 b) 必要かつ実施可能な場合には、組織から記憶媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する。 取外し可能な記憶媒体の管理において、次の事項を考慮する。 c) 全ての記憶媒体は、情報の分類に従って安全でセキュリティが保たれた環境に保管し、製造業者の仕様に従って、環境の脅威（熱、水分、湿度、電場、経年劣化など）から保護する。 取外し可能な記憶媒体の管理において、次の事項を考慮する。 d) 情報の機密性又は完全性が重要な考慮事項である場合は、取外し可能な記憶媒体上の情報を保護するために、暗号技術を用いる。 取外し可能な記憶媒体の管理において、次の事項を考慮する。 e) 保管した情報がまだ必要な間に記憶媒体が劣化する又は交換されるため、読み出せなくなる前に情報を新しい記憶媒体に移し替える。 取外し可能な記憶媒体の管理において、次の事項を考慮する。 f) 価値の高い情報は、一度に損傷又は消失するリスクを上げるためにも、複数の複製を別の記憶媒体に保管する。 取外し可能な記憶媒体の管理において、次の事項を考慮する。 g) 情報を失う危険性を小さくするために、取外し可能な記憶媒体の登録を検討する。 取外し可能な記憶媒体の管理において、次の事項を考慮する。 h) 取外し可能な記憶媒体のポートは、組織にその利用について理由があるときだけ有効とする。 取外し可能な記憶媒体の管理において、次の事項を考慮する。 i) 取外し可能な記憶媒体を用いる必要がある場合、そのような記憶媒体への情報の転送を監視する。 取外し可能な記憶媒体の管理において、次の事項を考慮する。 j) 情報は、物理的な輸送中、例えば、郵便サービス又は宅配便で記憶媒体を送る場合に、認可されていないアクセス、不正使用又は破損に関して忧い頃である可能性がある。 この管理策では、媒体は紙の文書を含んでいる、物理的記憶媒体を輸送する場合には、5b-5.14のセキュリティ対策を適用する。	手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり － 手引に関連記載あり	8.3.1.1 8.3.1.2 8.3.1.3 8.3.1.4 8.3.1.5 8.3.1.6 8.3.1.7 8.3.1.8 8.3.1.9 8.3.1.10 （対応項なし） －	取外し可能な媒体の管理のために、再利用可能な媒体を組織から移動する場合に、その内容がより後不要であるならば、これを復元不能とする。 取外し可能な媒体の管理のために、必要かつ実際的な場合には、組織から移動する媒体について、認可を要求する。 取外し可能な媒体の管理のために、組織から移動する媒体について、監査証跡の維持のために記録を保管する。 取外し可能な媒体の管理のために、全ての媒体は、製造業者の仕様に従って、安全でセキュリティが保たれた環境に保管する。 取外し可能な媒体の管理において、データの機密性又は完全性が重要な考慮事項である場合は、取外し可能な媒体上のデータを保護するために、暗号技術を用いる。 取外し可能な媒体の管理において、保管されたデータがまだ必要な間に媒体が劣化する前に媒体を交換するため、読み出せなくなる前にデータを新しい媒体に移動する。 取外し可能な媒体の管理において、価値の高いデータは、一度に損傷又は消失するリスクを上げるためにも、複数の複製を別の媒体に保管する。 取外し可能な媒体の管理において、データ消失の危険性を小さくするために、取外し可能な媒体の登録を含める。 取外し可能な媒体の管理のために、取外し可能な媒体のドライブは、その利用のための業務上の理由があるときだけ有効とする。 取外し可能な媒体の管理のために、取外し可能な媒体を用いる必要がある場合、媒体への情報の転送を監視する。 （対応項なし） （対応項なし）
7.10.2	記憶媒体のセキュリティを保った再利用又は処分の手順を整備し、セキュリティ対策を実施する。	認可されていない者に秘密情報が漏えいするリスクを最小化するために、記憶媒体のセキュリティを保った再利用又は処分の手順を確立する。 秘密情報を格納した記憶媒体の、セキュリティを保った再利用又は処分の手順は、その情報の取扱いや分類に応じたものとする。 記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 a) 秘密情報を含む記憶媒体を組織内で再利用する必要がある場合には、セキュリティを保ってデータ消去するか、又は再利用する前に記憶媒体をフォーマットする（8.10参照）。 b) 秘密情報を含む記憶媒体は、必要でなくなったときはセキュリティを保って処分する（例えば、内容を破壊、細断又はセキュリティを保って消去することなど）。 c) セキュリティを保った処分を必要とする可能性のある品目を特定する手順をもつ。 d) 多くの業者が、記憶媒体の収集及び処分サービスを提供している。十分な管理策及び経験をもつ適切な外部の供給者を選定することに、注意を払う。 e) 監査証跡を維持するために、取扱いに慎重を要する品目の処分を記録しておく。 f) 処分のために記憶媒体を集める場合、集積することによる影響に配慮する。取扱いに慎重を要する情報ではない情報でも、その量が集まると、取扱いに慎重を要する情報に変わる場合がある。 取扱いに慎重を要するデータ含んだ装置・機器が損傷した場合には、リスクアセスメントを実施し、修理又は廃棄に出すより先物理的に破壊する方が望ましい亦否かを決定する（7.14参照）。	7b-7.10.2 7b-7.10.3 7b-7.10.4 7b-7.10.4 7b-7.10.4 7b-7.10.4 7b-7.10.4 7b-7.10.4 7b-7.10.5	認可されていない者に秘密情報が漏えいするリスクを最小化するために、記憶媒体のセキュリティを保った再利用又は処分の手順を確立する。 秘密情報を格納した記憶媒体の、セキュリティを保った再利用又は処分の手順は、その情報の取扱いに慎重を要する度合いに応じたものとする。 記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 a) 秘密情報を含む記憶媒体を組織内で再利用する必要がある場合には、セキュリティを保ってデータを消去するか、又は再利用する前に記憶媒体をフォーマットする。 記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 b) 秘密情報を含む記憶媒体は、必要でなくなったときはセキュリティを保って処分する。 記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 c) セキュリティを保った処分を必要とする可能性のある品目を特定する手順をもつ。 記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 d) 多くの業者が、記憶媒体の収集及び処分サービスを提供している。十分な管理策及び経験をもつ適切な外部の供給者を選定すること、注意を払う。 記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 e) 監査証跡を維持するために、取扱いに慎重を要する品目の処分を記録しておく。 記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 f) 処分のために記憶媒体を集める場合、集積することによる影響に配慮する。取扱いに慎重を要する情報ではない情報でも、その量が集まると、取扱いに慎重を要する情報に変わる場合がある。 取扱いに慎重を要するデータを含んだ装置・機器が損傷した場合には、リスクアセスメントを実施し、修理又は廃棄に出すより先物理的に破壊する方が望ましい亦否かを決定する。	手引に関連記載あり 手引に関連記載あり － 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり 手引に関連記載あり －	8.3.2.1 8.3.2.2 （対応項なし） 8.3.2.3 8.3.2.4 8.3.2.6 8.3.2.7 8.3.2.8 （対応項なし）	認可されていない者に秘密情報が漏えいするリスクを最小化するために、媒体のセキュリティを保った処分のための正式な手順を確立する。 秘密情報を格納した媒体の、セキュリティを保った処分の手順は、その情報の取扱いに慎重を要する度合いに応じたものとする。 セキュリティを保った処分を必要とする品目を特定するための手順を定める。 媒体の収集並びに処分のサービスを提供する外部業者は、十分な管理策及び経験を持つ適切な契約相手を選択する。 監査証跡を維持するために、取扱いに慎重を要する品目の処分を記録する。 処分のために情報を含む媒体を集める場合、それらの情報が集積されることによる影響に配慮し、手順に含める。 （対応項なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
7.11	サポートユーティリティ 統制目標：情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保護する。 目的：サポートユーティリティの故障及び中断・阻害による情報及びその他の関連資産の消失、損傷若しくは侵害、又は組織の運用の中断を防止するため。		7.11	サポートユーティリティ 管理策 情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保護する。 目的 サポートユーティリティの故障及び中断・阻害による情報及びその他の関連資産の消失、損傷若しくは侵害、又は組織の運用の中断を防止するため。		11.2.2	サポートユーティリティ 装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。
7.11.1	情報処理施設・設備をサポートするユーティリティを保護するためのセキュリティ対策を実施する。	組織は、情報処理施設・設備をサポートするユーティリティ（例えば、電気、通信サービス、給水、ガス、下水、換気、空調）に依存している。そのため、組織は次の事項を行う。 a) ユーティリティを支援する装置を、関連する製造業者の仕様に従って構成し、操作し、保守することを確実にする。 b) ユーティリティが事業の成長及び他のサポートユーティリティとの相互作用に対応する能力を、定期的に評価することを確実にする。 c) ユーティリティを支援する装置が適切に機能することを確実にするために、定期的に検査し、試験することを確実にする。 d) 必要であれば、ユーティリティの不具合を検知するための警報装置を取り付ける。 e) 必要であれば、物理的な経路が異なる複数の供給元をユーティリティに備えることを確実にする。 f) ユーティリティを支援する装置がネットワークに接続されている場合、情報処理施設・設備から分離したネットワーク上にあることを確実にする。 g) ユーティリティを支援する装置を、必要な場合だけ、かつ、セキュリティを保った方法でだけインターネットに接続することを確実にする。 緊急連絡先の詳細を記載し、停止した場合に要員が利用できるようにする。 サポートユーティリティのための非常用の照明及び通信手段を備える。 非常口又は設備室の近く、電源、給水、ガス又はその他のユーティリティを遮断するための緊急スイッチ及び緊急バルブを設置する。	7b-7.11.1	組織は、情報処理施設・設備をサポートするユーティリティに依存している。そのため、組織は次の事項を行う。 a) ユーティリティを支援する装置を、関連する製造業者の仕様に従って構成し、操作し、保守することを確実にする。	手引に関連記載あり	11.2.2.1	サポートユーティリティ（例えば、電気、通信サービス、給水、ガス、下水、換気、空調）は、装置の製造業者の仕様及び地域の法的要求事項に適合しているものを採用する。
			7b-7.11.1	組織は、情報処理施設・設備をサポートするユーティリティに依存している。そのため、組織は次の事項を行う。 b) ユーティリティが事業の成長及び他のサポートユーティリティとの相互作用に対応する能力を、定期的に評価することを確実にする。	手引に関連記載あり	11.2.2.2	サポートユーティリティは、事業の成長及び他のサポートユーティリティとの相互作用に対応する能力を、定期的に評価する。
			7b-7.11.1	組織は、情報処理施設・設備をサポートするユーティリティに依存している。そのため、組織は次の事項を行う。 c) ユーティリティを支援する装置が適切に機能することを確実にするために、定期的に検査し、試験することを確実にする。	手引に関連記載あり	11.2.2.3	サポートユーティリティは、適切に機能することを確実にするために、定期的に検査及び試験する。
			7b-7.11.1	組織は、情報処理施設・設備をサポートするユーティリティに依存している。そのため、組織は次の事項を行う。 d) 必要であれば、ユーティリティの不具合を検知するための警報装置を取り付ける。	手引に関連記載あり	11.2.2.4	サポートユーティリティは、必要であれば、不具合を検知するための警報装置を取り付ける。
			7b-7.11.1	組織は、情報処理施設・設備をサポートするユーティリティに依存している。そのため、組織は次の事項を行う。 e) 必要であれば、物理的な経路が異なる複数の供給元をユーティリティに備えることを確実にする。	手引に関連記載あり	11.2.2.5	サポートユーティリティは、必要であれば、物理的な経路が異なる複数の供給元を確保する。
			7b-7.11.1	組織は、情報処理施設・設備をサポートするユーティリティに依存している。そのため、組織は次の事項を行う。 f) ユーティリティを支援する装置がネットワークに接続されている場合、情報処理施設・設備から分離したネットワーク上にあることを確実にする。 g) ユーティリティを支援する装置を、必要な場合だけ、かつ、セキュリティを保った方法でだけインターネットに接続することを確実にする。	–	（対応項なし）
			7b-7.11.2	サポートユーティリティのための非常用の照明及び通信手段を備える。	手引に関連記載あり	11.2.2.6	非常用の照明及び通信手段を備える。
			7b-7.11.3	非常口又は設備室の近く、電源、給水、ガス又はその他のユーティリティを遮断するための緊急スイッチ及び緊急バルブを設置する。	手引に関連記載あり	11.2.2.7	非常口又は設備室の近く、電源、給水、ガス又はその他のユーティリティを遮断するための緊急スイッチ及び緊急バルブを設置する。
7.12	ケーブル配線のセキュリティ 統制目標：電源ケーブル、データ伝送ケーブル又は情報サービスを支援するケーブルの配線は、傍受、妨害又は損傷から保護する。 目的：電源ケーブル及び通信ケーブルの配線に関連した、情報及びその他の関連資産の消失、損傷、盗難又は侵害、並びに組織の運用の中断を防止するため。		7.12	ケーブル配線のセキュリティ 管理策 電源ケーブル、データ伝送ケーブル又は情報サービスを支援するケーブルの配線は、傍受、妨害又は損傷から保護する。 目的 電源ケーブル及び通信ケーブルの配線に関連した、情報及びその他の関連資産の消失、損傷、盗難又は侵害、並びに組織の運用の中断を防止するため。		11.2.3	ケーブル配線のセキュリティ データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。
7.12.1	ケーブル配線のセキュリティを維持・保護するためのセキュリティ対策を実施する。	ケーブル配線のセキュリティのために、次の事項を考慮する。 a) 情報処理施設・設備に接続する電源ケーブル及び通信回線は、可能な場合には、地下に埋設する、又は床ケーブル保護装置、電柱など、これに代わる十分な保護手段を施す。ケーブルが地下にある場合は、偶発的な切断から保護する（例えば、外装電線管又はケーブルの存在を示す表示を利用し、）。 b) 干渉を防止するために、電源ケーブルは、通信ケーブルから隔離する。 c) 取扱いに慎重を要するシステムは重要なシステムために、次の追加の管理策の採用を検討する。 1) 外装電線管の導入、点検箇所・終端箇所の施設可能な部屋又は箱への設置及び鍵報装置の設置 2) ケーブルを保護するための電磁遮蔽の利用 3) ケーブルに取り付けられた認可されていない装置・機器を検知するための定期的な技術的探索及び物理的検査 4) 配線盤、端子盤及びケーブル室への管理されたアクセス（例えば、物理鍵又はPINを用いる。） 5) 光ファイバーケーブルの使用 d) ケーブル配線の物理的識別及び検査を可能にするために、ケーブルの各端に始点及び終点に関する十分な詳細情報をラベル付けする。 ケーブルに関するインシデント又は不具合から生じるリスクを管理する方法について、専門家の助言を求める。	7b-7.12.1	ケーブル配線のセキュリティのために、次の事項を考慮する。 a) 情報処理施設・設備に接続する電源ケーブル及び通信回線は、可能な場合には、地下に埋設する、又は床ケーブル保護装置、電柱など、これに代わる十分な保護手段を施す。ケーブルが地下にある場合は、偶発的な切断から保護する。	手引に関連記載あり	11.2.3.1	情報処理施設に接続する電源ケーブル及び通信回線は、地下に埋設するか、又はこれに代わる十分な保護手段を施す。
			7b-7.12.1	ケーブル配線のセキュリティのために、次の事項を考慮する。 b) 干渉を防止するために、電源ケーブルは、通信ケーブルから隔離する。	手引に関連記載あり	11.2.3.2	ケーブル間の干渉を防止するために、電源ケーブルは、通信ケーブルから隔離する。
			7b-7.12.1	ケーブル配線のセキュリティのために、次の事項を考慮する。 c) 取扱いに慎重を要するシステムは重要なシステムために、次の追加の管理策の採用を検討する。 1) 外装電線管の導入、点検箇所・終端箇所の施設可能な部屋又は箱への設置及び鍵報装置の設置 2) ケーブルを保護するための電磁遮蔽の利用 3) ケーブルに取り付けられた認可されていない装置・機器を検知するための定期的な技術的探索及び物理的検査 4) 配線盤、端子盤及びケーブル室への管理されたアクセス 5) 光ファイバーケーブルの使用	手引に関連記載あり	11.2.3.3	取扱いに慎重を要するシステムは重要なシステムために、以下の4点を行う。 1.外装電線管を導入し、点検箇所・終端箇所の施設可能な部屋又は箱へ設置する。 2.ケーブルを保護するための電磁遮蔽を利用する。 3.ケーブルに取り付けられた認可されていない装置の技術的探索及び物理的検査を実施する。 4.配線盤、端子盤及びケーブル室への管理されたアクセスを実施する。
			7b-7.12.1	ケーブル配線のセキュリティのために、次の事項を考慮する。 d) ケーブル配線の物理的識別及び検査を可能にするために、ケーブルの各端に始点及び終点に関する十分な詳細情報をラベル付けする。	手引に関連記載あり	–	（対応項なし）
			7b-7.12.2	ケーブルに関するインシデント又は不具合から生じるリスクを管理する方法について、専門家の助言を求める。	手引に関連記載あり	–	（対応項なし）
7.13	装置の保守 統制目標：装置は、情報の可用性、完全性及び機密性を維持することを確実にするために、正しく保守する。 目的：不十分な保守による、情報及びその他の関連資産の消失、損傷、盗難又は侵害、並びに組織の運用の中断を防止するため。		7.13	装置の保守 管理策 装置は、情報の可用性、完全性及び機密性を維持することを確実にするために、正しく保守する。 目的 不十分な保守による、情報及びその他の関連資産の消失、損傷、盗難又は侵害、並びに組織の運用の中断を防止するため。		11.2.4	装置の保守 装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。
7.13.1	装置を保守するためのセキュリティ対策を実施する。	装置の保守のために、次の事項を考慮する。 a) 装置は、供給者の推奨するサービスの頻度及び仕様に従って保守する。 b) 組織の保守プログラムを実施し、監視する。 c) 認可された保守要員だけが、装置の修理及び保守を実施する。 d) 故障と見られるもの及び実際の故障の全て、並びに予防及び是正のための保守の全てについての記録を保持する。 e) 装置の保守を計画する場合には、この保守を、要員が構内で行うのか、又は組織の外で行うのかを考慮して、適切な管理策を実施する。保守要員に適切な秘密保持契約を結ばせる。 f) 構内で保守を実施する場合は保守要員を監督する。 g) 遠隔保守のためのアクセスを認可し、管理する。 h) 情報を保有している装置を保守のために構外へ持ち出す場合は、構外にある資産のセキュリティ（7.9参照）の対策を適用する。 i) 保険において課される全ての保守要求事項を順守する。 j) 保守の後、装置を作動させる前に、その装置が改ざんされていないこと及び適切に機能することを確実にするために検査する。 k) 装置を処分するごとに決定した場合、装置のセキュリティを保った処分又は再利用（7.14参照）の対策を適用する。	7b-7.13.1	装置の保守のために、次の事項を考慮する。 a) 装置は、供給者の推奨するサービスの頻度及び仕様に従って保守する。	手引に関連記載あり	11.2.4.1	可用性及び完全性を継続的に維持することを確実にするために、装置は、供給者の推奨する期間及び仕様に従って保守する。
			7b-7.13.1	装置の保守のために、次の事項を考慮する。 b) 組織の保守プログラムを実施し、監視する。	手引に関連記載あり	–	（対応項なし）
			7b-7.13.1	装置の保守のために、次の事項を考慮する。 c) 認可された保守要員だけが、装置の修理及び保守を実施する。	手引に関連記載あり	11.2.4.2	可用性及び完全性を継続的に維持することを確実にするために、認可された保守要員の一覧を維持し、その保守要員だけが、装置の修理及び手入れを実施する。
			7b-7.13.1	装置の保守のために、次の事項を考慮する。 d) 故障と見られるもの及び実際の故障の全て、並びに予防及び是正のための保守の全てについての記録を保持する。	手引に関連記載あり	11.2.4.3	可用性及び完全性を継続的に維持することを確実にするために、故障と見られるもの及び実際の故障の全て、並びに予防及び是正のための保守の全てについての記録を保持し、レビューする。
			7b-7.13.1	装置の保守のために、次の事項を考慮する。 e) 装置の保守を計画する場合には、この保守を、要員が構内で行うのか、又は組織の外で行うのかを考慮して、適切な管理策を実施する。保守要員に適切な秘密保持契約を結ばせる。	手引に関連記載あり	11.2.4.4	可用性及び完全性を継続的に維持することを確実にするために、装置の保守を計画する場合には、この保守を、要員が構内で行うのか、又は組織の外で行うのかを考慮して、適切な管理策を実施する。その装置から秘密情報を消去する、又は保守要員が十分に信頼できる者であり、必要なアクセス権を有することを確かめる。
					手引に関連記載あり	11.2.4.5	可用性及び完全性を継続的に維持することを確実にするために、保険約款で定められた、保守に関する全ての要求事項を順守する。
			7b-7.13.1	装置の保守のために、次の事項を考慮する。 f) 構内で保守を実施する場合は保守要員を監督する。	手引に関連記載あり	–	（対応項なし）
			7b-7.13.1	装置の保守のために、次の事項を考慮する。 g) 遠隔保守のためのアクセスを認可し、管理する。	手引に関連記載あり	11.2.4.7	可用性及び完全性を継続的に維持することを確実にするために、遠隔保守は認可を必要とし、監視する。
			7b-7.13.1	装置の保守のために、次の事項を考慮する。 h) 情報を保有している装置を保守のために構外へ持ち出す場合は、構外にある資産のセキュリティの対策を適用する。	手引に関連記載あり	–	（対応項なし）
			7b-7.13.1	装置の保守のために、次の事項を考慮する。 i) 保険において課される全ての保守要求事項を順守する。	手引に関連記載あり	–	（対応項なし）
			7b-7.13.1	装置の保守のために、次の事項を考慮する。 j) 保守の後、装置を作動させる前に、その装置が改ざんされていないこと及び適切に機能することを確実にするために検査する。	手引に関連記載あり	11.2.4.6	可用性及び完全性を継続的に維持することを確実にするために、保守の後、装置を作動させる前に、その装置が改ざんされていないこと及び不具合を起こさないことを確実にするために検査する。
			7b-7.13.1	装置の保守のために、次の事項を考慮する。 k) 装置を処分するごとに決定した場合、装置のセキュリティを保った処分又は再利用の対策を適用する。	手引に関連記載あり	–	（対応項なし）
7.14	装置のセキュリティを保った処分又は再利用 統制目標：記憶媒体を内蔵した装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保てるよう上書きしていることを確実にするために、検証する。 目的：処分又は再利用する装置からの情報漏えいを防止するため。		7.14	装置のセキュリティを保った処分又は再利用 管理策 記憶媒体を内蔵した装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保てるよう上書きしていることを確実にするために、検証する。 目的 処分又は再利用する装置からの情報漏えいを防止するため。		11.2.7	装置のセキュリティを保った処分又は再利用 記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保つ上書きしていることを確実にするために、検証する。
7.14.1	装置の処分又は再利用する前に、セキュリティを保つための対策を実施する。	装置は、処分又は再利用する前に、記憶媒体が内蔵されているか否かを確かめるために検証する。 秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊、又はその情報を破壊、消去若しくは上書きする。 秘密情報又は著作権のある情報の消去又は上書きには、標準的な削除機能を利用するよりも、元の情報を媒体から取り出せなくする技術を利用する。記憶媒体のセキュリティを保った処分に関する詳細な手引については7.10を、情報の削除に関する手引については8.10を参照。 組織を特定する、又は情報の分類、管理責任者、システム若しくはネットワークの区別を示すラベル及び表示は、再販又は慈善団体への寄付を含む処分を行う前に除去する。 （上記の他、一部 JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	7b-7.14.1	装置は、処分又は再利用する前に、記憶媒体が内蔵されているか否かを確かめるために検証する。	手引に関連記載あり	11.2.7.1	装置は、処分又は再利用する前に、記憶媒体が内蔵されているか否かを確かめるために検証する。
			7b-7.14.2	秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊、又はその情報を破壊、消去若しくは上書きする。	手引に関連記載あり	11.2.7.2	秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊すること、又はその情報を破壊、消去若しくは上書きする。
			7b-7.14.3	秘密情報又は著作権のある情報の消去又は上書きには、標準的な削除機能を利用するよりも、元の情報を媒体から取り出せなくする技術を利用する。	手引に関連記載あり	11.2.7.3	秘密情報又は著作権のある情報を格納した記憶媒体の消去又は上書きには、標準的な消去又は初期化の機能を利用するよりも、元の情報を媒体から取り出せなくする技術を利用する。
			（7b-7.14.3参考）	秘密情報又は著作権のある情報の消去又は上書きには、標準的な削除機能を利用するよりも、元の情報を媒体から取り出せなくする技術を利用する。	手引に関連記載あり	–	（対応項なし）
			7b-7.14.4	組織を特定する、又は情報の分類、管理責任者、システム若しくはネットワークの区別を示すラベル及び表示は、再販又は慈善団体への寄付を含む処分を行う前に除去する。	手引に関連記載あり	–	（対応項なし）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり （情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
7.14.2	施設のリース終了時又は施設外への移転時に関するセキュリティ対策を実施する。	組織は、施設のリース終了時又は施設外への移転時に、アクセス制御、監視装置などのセキュリティ管理策の除去を検討する。これは、次のような要因に依存する。 a) 施設を元の状態に戻すリース合意 b) 次のテナントに対して、取扱いに慎重を要する情報を含むシステムが残されるリスクの最小化（例えば、利用者アクセスの記入、映像又は画像ファイル） c) 移転先の施設で管理策を再利用できること	7b-7.14.5	組織は、施設のリース終了時又は施設外への移転時に、アクセス制御、監視装置などのセキュリティ管理策の除去を検討する。	手引に関連記載あり	–	（対応項なし）
			（7b-7.14.5参考）	これは、次のような要因に依存する。 a) 施設を元の状態に戻すリース合意 b) 次のテナントに対して、取扱いに慎重を要する情報を含むシステムが残されるリスクの最小化 c) 移転先の施設で管理策を再利用できること	手引に関連記載あり	–	（対応項なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.1	利用者エンドポイント機器 統制目標：利用者エンドポイント機器に保存されている情報、処理される情報、又は利用者エンドポイント機器を介してアクセス可能な情報を保護する。 目的：利用者エンドポイント機器を使用することによってもたらされるリスクから情報を保護するため。		8.1	利用者エンドポイント機器 管理策 利用者エンドポイント機器に保存されている情報、処理される情報、又は利用者エンドポイント機器を介してアクセス可能な情報を保護する。 目的 利用者エンドポイント機器を使用することによってもたらされるリスクから情報を保護するため。		6.2	モバイル機器及びテレワーキング 管理目的：モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。
						6.2.1	モバイル機器の方針 モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用する。
						11.2.8	無人状態にある利用者装置 利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にする仕組みを整備する。
8.1.1	エンドポイント機器のセキュリティに関する方針、要求事項及び手順を整備する。	エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 a) エンドポイント機器が取扱い、処理、保存又は支援をすることが可能な情報の種類及び分類レベル b) エンドポイント機器の登録 c) 物理的保護についての要求事項 d) ソフトウェアのインストールの制限（例えば、システムの実務管理者が遠隔で管理する。） e) エンドポイント機器のソフトウェア（ソフトウェアの版を含む。）の要求事項及び更新の適用の要求事項（例えば、動的自動更新） f) 情報サービス、公衆ネットワーク、又はその他の構外ネットワークへの接続に関する規則（例えば、パーソナルファイアウォールの使用を求める。） g) アクセス制御 h) 記憶装置の暗号化 i) マルウェアからの保護 j) 遠隔操作による機器の無効化、データの消去又はロック k) バックアップ l) ウェブサービス及びウェブアプリケーションの使用 m) エンドユーザーの行動の分析（8.16参照） n) 取外し可能なメモリ装置を含む取外し可能な機器の使用、及び物理ポート（例えば、USB ポート）を無効化できる可能性 o) エンドポイント機器に分割機能がある場合は、その利用。これによって、組織の情報及びその他の関連資産（例えば、ソフトウェア）を、機器上の他の情報及びその他の関連資産からセキュリティを保って分離することが可能である。 ある情報が特に慎重な取扱いを要する場合に、エンドポイント機器を用いてその情報にアクセスは可能とするが、その機器には保存はできないようにするかどうかを検討する。その場合、機器に追加の技術的保護手段が必要になる可能性がある。例えには、オフライン作業のためのファイルのダウンロードの無効化、及びSDカードなどのローカルストレージの無効化を確実にすることがある。 組織は、エンドポイント機器のセキュリティのために次の事項に関する手順を確立する。 a) 機器の無線接続の構成（例えば、ぜい弱なプロトコルを無効化する。） b) 関連するトピック固有の方針に従って適切な帯域幅の無線又は有線接続を使用すること（例えば、バックアップ又はソフトウェア更新が必要であるため。） エンドポイント機器の盗難又は紛失に備えて、法令、規制、契約（保険を含む。）及び組織のその他のセキュリティ要求事項を考慮して、そのための手順を確立する。	8a-8.1.1	組織は、利用者エンドポイント機器のセキュリティを保全する構成及び取扱いに関するトピック固有の方針を確立する。	手引に関連記載あり	–	（対応項なし）
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 a) 利用者エンドポイント機器が取扱い、処理、保存又は支援をすることが可能な情報の種類及び分類レベル	手引に関連記載あり	–	（対応項なし）
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 b) 利用者エンドポイント機器の登録	手引に関連記載あり	6.2.1.3	モバイル機器の情報セキュリティ方針には、モバイル機器の登録を含める。
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 c) 物理的保護についての要求事項	手引に関連記載あり	6.2.1.4	モバイル機器の情報セキュリティ方針には、物理的保護についての要求事項を含める。
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 d) ソフトウェアのインストールの制限	手引に関連記載あり	6.2.1.5	モバイル機器の情報セキュリティ方針には、ソフトウェアのインストールの制限を含める。
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 e) 利用者エンドポイント機器のソフトウェア（ソフトウェアの版を含む。）の要求事項及び更新の適用の要求事項	手引に関連記載あり	6.2.1.6	モバイル機器の情報セキュリティ方針には、モバイル機器のソフトウェアのバージョン及びパッチ適用に対する要求事項を含める。
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 f) 情報サービス、公衆ネットワーク、又はその他の構外ネットワークへの接続に関する規則	手引に関連記載あり	6.2.1.7	モバイル機器の情報セキュリティ方針には、情報サービスへの接続の制限を含める。
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 g) アクセス制御	手引に関連記載あり	6.2.1.8	モバイル機器の情報セキュリティ方針には、アクセス制御を含める。
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 h) 記憶装置の暗号化	手引に関連記載あり	6.2.1.9	モバイル機器の情報セキュリティ方針には、暗号技術を含める。
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 i) マルウェアからの保護	手引に関連記載あり	6.2.1.10	モバイル機器の情報セキュリティ方針には、マルウェアからの保護を含める。
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 j) 遠隔操作による機器の無効化、データの消去又はロック	手引に関連記載あり	6.2.1.11	モバイル機器の情報セキュリティ方針には、遠隔操作による機器の無効化、データの消去又はロックを含める。
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 k) バックアップ	手引に関連記載あり	6.2.1.12	モバイル機器の情報セキュリティ方針には、バックアップを含める。
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 l) ウェブサービス及びウェブアプリケーションの使用	手引に関連記載あり	6.2.1.13	モバイル機器の情報セキュリティ方針には、ウェブサービス及びウェブアプリケーションの使用を含める。
			8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 m) エンドユーザーの行動の分析 n) 取外し可能なメモリ装置を含む取外し可能な機器の使用、及び物理ポートを無効化できる可能性 o) 利用者エンドポイント機器に分割機能がある場合は、その利用。これによって、組織の情報及びその他の関連資産を、機器上の他の情報及びその他の関連資産からセキュリティを保って分離することが可能である。	手引に関連記載あり	–	（対応項なし）
			8a-8.1.3	ある情報が特に慎重な取扱いを要する場合に、利用者エンドポイント機器を用いてその情報にアクセスは可能とするが、その機器には保存はできないようにするかどうかを検討する。	手引に関連記載あり	–	（対応項なし）
			（8a-8.1.3参考）	その場合、機器に追加の技術的保護手段が必要になる可能性がある。例えには、オフライン作業のためのファイルのダウンロードの無効化、及びSDカードなどのローカルストレージの無効化を確実にすることがある。	手引に関連記載あり	–	（対応項なし）
			8a-8.1.4	可能な限り、利用者エンドポイント機器の管理策に関する推奨事項を、構成管理又は自動化されたツールによって強制する。	手引に関連記載あり	–	（対応項なし）
			8a-8.1.9	組織は、利用者エンドポイント機器のセキュリティのために次の事項に関する手順を確立する。 a) 機器の無線接続の構成 b) 関連するトピック固有の方針に従って適切な帯域幅の無線又は有線接続を使用すること	手引に関連記載あり	–	（対応項なし）
			8a-8.1.6	利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧言する。 c) 公共の場所、オープンオフィス、集会所及びその他の保護されていない場所では、特別な注意を払って利用者エンドポイント機器を使用する。	手引に関連記載あり	6.2.1.14	公共の場所、会議室、その他保護されていない場所でモバイル機器を用いるときは、注意を払う。
			8a-8.1.6	利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧言する。 b) 利用者エンドポイント機器は、利用していない場合、物理的管理策及び論理的管理策を用いて、認可されていない利用から保護する。重要度の高い、取扱いに慎重を要する、又は影響の大きい業務情報が入っている機器を、無人の状態で放置しない。	手引に関連記載あり	6.2.1.15	モバイル機器に保管され、処理される情報について、認可されていないアクセス又は漏えい を防止するため、例えば、暗号技術の使用、秘密認証情報の使用の強制などの保護を実施する。
			8a-8.1.6	利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧言する。 d) 利用者エンドポイント機器を盗難から物理的に保護する。	手引に関連記載あり	6.2.1.16	モバイル機器は、盗難、特にどこか（例えば、自動車、他の輸送機関、ホテルの部屋、会議室、集会所）に置き忘れたときの盗難から、物理的に保護する。
			8a-8.1.7	利用者エンドポイント機器の盗難又は紛失に備えて、法令、規制、契約（保険を含む。）及び組織のその他のセキュリティ要求事項を考慮して、そのための手順を確立する。	手引に関連記載あり	6.2.1.17	モバイル機器の盗難又は紛失の場合の対策のために、法規制、保険及び組織の他のセキュリティ要求事項を考慮した特定の手順を確立する。
			8a-8.1.6	【再】利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧言する。 b) 利用者エンドポイント機器は、利用していない場合、物理的管理策及び論理的管理策を用いて、認可されていない利用から保護する。重要度の高い、取扱いに慎重を要する、又は影響の大きい業務情報が入っている機器を、無人の状態で放置しない。	手引に関連記載あり	6.2.1.18	重要度の高い、取扱いに慎重を要する又は影響の大きい業務情報が入っているモバイル機器は、無人の状態で放置しない。
8.1.2	エンドポイント機器を保護するための対策を実施する。	可能な限り、エンドポイント機器の管理策に関する推奨事項を、構成管理（8.9参照）又は自動化されたツールによって強制する。 エンドポイント機器を保護するためのセキュリティ要求事項及び手順、並びにそのセキュリティ対策を実施する自らの責任について、全ての利用者に認識させる。 エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧言する。 a) エンドポイント機器を必要がなくなったら、実行していたセッションからログオフ、サービスを終了する。 b) エンドポイント機器は、利用していない場合、物理的管理策（例えば、キーロック又は特殊ロック）及び論理的管理策（例えば、パスワードアクセス）を用いて、認可されていない利用から保護する。重要度の高い、取扱いに慎重を要する、又は影響の大きい業務情報が入っている機器を、無人の状態で放置しない。 c) 公共の場所、オープンオフィス、集会所及びその他の保護されていない場所では、特別な注意を払ってエンドポイント機器を使用する（例えば、他人が背後から読むことが可能な場合に秘密情報を読むことは避ける。また、プライバシースクリーンフィルタを使用する。）。 d) エンドポイント機器を盗難から物理的に保護する（例えば、自動車、他の輸送機関、ホテルの部屋、会議室、集会所において）。 個人所有の機器（BYODとしても知られる。）の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。 a) 機器の個人使用と業務上の使用とを区別する。このような区別を可能とし、個人所有の機器に保存された業務データを保護するためのソフトウェアの使用も含む。 b) 利用者が自らの義務（物理的保護、ソフトウェアの更新など）を受け入れた場合にだけ、業務情報にアクセスできるようにする。業務データについて明確な主張しないこと、及び機器の盗難若しくは紛失があった場合及びサービス利用の認可が取り消された場合に組織が遠隔操作でデータを消去することへの合意を含む。こうした場合、PII保護に関する法令を考慮することが望ましい。 c) 個人所有の機器で開発された知的財産権に関する紛争を防止するためのトピック固有の方針及び手順 d) 個人所有の機器へのアクセス（機械のセキュリティを検証する目的で、又は調査において）、これは法令で禁止されている場合がある。 e) 要員又は外部組織の利用者が個人で所有するエンドポイント機器上のクライアントソフトウェアについて、ライセンスを受ける責任を組織が負うことになる可能性があるソフトウェアライセンス契約 禁止事項の例を以下に示す。 a) 端末、OS、アプリケーション等の改造行為 b) 安全性が確認できないアプリケーションのインストール及び利用 c) 利用が禁止されているソフトウェアのインストール及び利用（利用を禁止するソフトウェアを定める場合） d) 許可されない通信回線サービスの利用（利用する回線を限定する場合） e) 第三者への端末の貸与 f) 利用承認を得ていないクラウドサービス等への機密情報のバックアップ g) 機密性の高い情報の取扱い	8a-8.1.5	利用者エンドポイント機器を保護するためのセキュリティ要求事項及び手順、並びにそのセキュリティ対策を実施する自らの責任について、全ての利用者に認識させる。	手引に関連記載あり	–	（対応項なし）
			8a-8.1.6	利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧言する。 a) 利用者エンドポイント機器を利用する必要がなくなったら、実行していたセッションからログオフし、サービスを終了する。	手引に関連記載あり	11.2.8.3	利用者に、必要がなくなったら、アプリケーション又はネットワークサービスからログオフするよう勧言する。
			8a-8.1.6	利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧言する。 b) 利用者エンドポイント機器は、利用していない場合、物理的管理策及び論理的管理策を用いて、認可されていない利用から保護する。重要度の高い、取扱いに慎重を要する、又は影響の大きい業務情報が入っている機器を、無人の状態で放置しない。	手引に関連記載あり	6.2.1.1	モバイル機器を用いる場合、業務情報が危険にさらされないことを確実にするために、特別な注意を払う。
					手引に関連記載あり	6.2.1.15	モバイル機器に保管され、処理される情報について、認可されていないアクセス又は漏えい を防止するため、例えば、暗号技術の使用、秘密認証情報の使用の強制などの保護を実施する。
					手引に関連記載あり	6.2.1.18	重要度の高い、取扱いに慎重を要する又は影響の大きい業務情報が入っているモバイル機器は、無人の状態で放置しない。
					手引に関連記載あり	11.2.8.4	利用者に、コンピュータ又はモバイル機器は、利用していない場合、キーロック又は同等の管理策（例えば、パスワードアクセス）によって、認可されていない利用から保護するよう勧言する。
			8a-8.1.6	【再】利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧言する。 c) 公共の場所、オープンオフィス、集会所及びその他の保護されていない場所では、特別な注意を払って利用者エンドポイント機器を使用する。	手引に関連記載あり	6.2.1.2	モバイル機器の情報セキュリティ方針は、保護されていない環境におけるモバイル機器を用いた作業のリスクを考慮して定める。
					手引に関連記載あり	6.2.1.14	公共の場所、会議室、その他保護されていない場所でモバイル機器を用いるときは、注意を払う。
			8a-8.1.6	【再】利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧言する。 d) 利用者エンドポイント機器を盗難から物理的に保護する。	手引に関連記載あり	6.2.1.16	モバイル機器は、盗難、特にどこか（例えば、自動車、他の輸送機関、ホテルの部屋、会議室、集会所）に置き忘れたときの盗難から、物理的に保護する。
			8a-8.1.8	個人所有の機器の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。 a) 機器の個人使用と業務上の使用とを区別する。このような区別を可能とし、個人所有の機器に保存された業務データを保護するためのソフトウェアの使用も含む。	手引に関連記載あり	6.2.1.21	モバイル機器の情報セキュリティ方針と、個人所有のモバイル機器の使用が許されている場合は、その方針及び関連するセキュリティ対策において、機器の私的な使用と業務上の使用とを区別する。（このような区別を可能とし、個人所有の機器に保存された業務データを保護するためのソフトウェアの使用も含む）
			8a-8.1.8	個人所有の機器の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。 b) 利用者が自らの義務（物理的保護、ソフトウェアの更新など）を受け入れた場合にだけ、業務情報にアクセスできるようにする。業務データについて明確な主張しないこと、及び機器の盗難若しくは紛失があった場合及びサービス利用の認可が取り消された場合に組織が遠隔操作でデータを消去することへの合意を含む。こうした場合、PII保護に関する法令を考慮する。	手引に関連記載あり	6.2.1.22	モバイル機器の情報セキュリティ方針で、個人所有のモバイル機器の使用が許されている場合は、その方針及び関連するセキュリティ対策において、エンドユーザ合意書に利用者が署名した場合にだけ、業務情報にアクセスできるようにする（エンドユーザ合意書には、利用者の義務（物理的な保護、ソフトウェアの更新など）についての確認、業務データに対する所有権を主張しないこと、及び機器の盗難若しくは紛失があった場合及びサービス利用の認可が取り消された場合に組織が遠隔操作でデータを消去することへの合意を含む。この方針では、プライバシーに関する法令を考慮する。）。
			8a-8.1.8	個人所有の機器の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。 c) 個人所有の機器で開発された知的財産権に関する紛争を防止するためのトピック固有の方針及び手順	手引に関連記載あり	6.2.2.8	テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、個人所有の装置の上で開発した知的財産の権利に関する論争を防ぐための方針及び手順を考慮して定める。
			8a-8.1.8	個人所有の機器の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。 d) 個人所有の機器へのアクセス（機械のセキュリティを検証する目的で、又は調査において）、これは法令で禁止されている場合がある。	手引に関連記載あり	6.2.2.9	テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、個人所有の装置へのアクセス（装置のセキュリティ検証のためのもの、又は調査期間中に行うもの）を考慮して定める。なお、このアクセスは、法令が禁じている場合がある。
			8a-8.1.8	個人所有の機器の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。 e) 要員又は外部組織の利用者が個人で所有する利用者エンドポイント機器上のクライアントソフトウェアについて、ライセンスを受ける責任を組織が負うことになる可能性があるソフトウェアライセンス契約	手引に関連記載あり	6.2.2.10	テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、従業員又は外部の利用者が個人的に所有するワークステーション上のクライアントソフトウェアの使用許諾について、組織が責任をもつことになる場合の、ソフトウェアの使用許諾契約を考慮して定める。
8.2	特権的アクセス権 統制目標：特権的アクセス権の割当て及び利用は、制限し、管理する。 目的：認可された利用者、ソフトウェア構成要素及びサービスだけに特権的アクセス権が与えられることを確実にするため。		8.2	特権的アクセス権 管理策 特権的アクセス権の割当て及び利用は、制限し、管理する。 目的 認可された利用者、ソフトウェア構成要素及びサービスだけに特権的アクセス権が与えられることを確実にするため。		9.2.3	特権的アクセス権の管理 特権的アクセス権の割当て及び利用は、制限し、管理する。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.2.1	特権のアクセス権の割当て及び利用を制限し、管理する。	特権のアクセス権の割当ては、アクセス制御に関するトピック固有の方針（5.15参照）に従って、認可プロセスによって管理する。 この管理策の実施については、次の事項を考慮する。 a) 各々のシステム又はプロセス（例えば、オペレーティングシステム、データベース管理システム、アプリケーション）の特権のアクセス権を必要とする利用者を特定する。 b) 特権のアクセス権を、アクセス制御に関するトピック固有の方針（5.15参照）に沿って、必要に応じて、かつ、事象ごとに、利用者に割り当てる（すなわち、特権的アクセスをより必要とする活動を実行するために必要な力量をもつ個人に対してだけ、かつその個人の職務上の役割のための最小限の要求に基づいて）。 c) 特権の認可プロセス（すなわち、誰が特権的アクセス権を承認することが可能かを決定するか、又は特権的アクセス権は認可プロセスが完了するまで許可しない。）及び割り当てた全ての特権の記録を維持する。 d) 特権のアクセス権の終了に関する要求事項を定め、実施する。 e) 利用者が、自らが特権的アクセス権をもっていること、及び自らがいつ特権的アクセスモードになっているかを認識することを確実にするための対策を講じる。考えられる対策としては、特別の利用者識別情報、利用者インタフェース設定、又は特別の装置の使用が含まれる。 f) 特権的アクセス権における認証の要求事項は、通常のアクセス権における要求事項よりも厳しくなる場合がある。特権的アクセス権を用いて作業を行う前に、再認証又は認証の格上げが必要になる場合がある。 g) 定期的に、また組織に何か変更があった後に、特権的アクセス権を用いて作業する利用者をレビューし、特権的アクセス権を用いた作業に関して、その利用者が職務、役割、責任及び力量の点でやも適格であるかどうかを検証する（5.18参照）。 h) 汎用の実務管理者ID（rootなど）の使用を避けるため、システムの構成管理機能に応じて、具体的な規則を確立する。そのようなIDの認証情報を管理し、保護する（5.17参照）。 i) 特権的アクセス権を永続的に許可するのではなく、承認された変更又は活動（例えば、保守活動又は一部の重要な変更）を実施するのに必要な時間枠だけ一時的な特権的アクセスを許可する。これはしばしばブレークグラス手順（break glass procedure）と呼ばれ、しばしば特権的アクセス管理技術において自動化されている。 j) 監査の目的で、システムへの全ての特権的アクセスのログを記録する。 k) 特権的アクセス権をもつ識別情報を複数の人で共有又は連携することはせず、特定の特権的アクセス権の割当てが許可された個別の識別情報を各人に割り当てる。特権的アクセス権の管理を簡素化するために、識別情報をグループ化することが可能である（例えば、実務管理者グループを定義することによって）。 l) 特権的アクセス権をもつ識別情報は、管理作業を実行するためだけに使用し、日常の一般的な職務（すなわち、電子メールの確認、ウェブへのアクセス）には使用しない（利用者はこれらの活動のために別の通常のネットワーク識別情報をもつ。）。	8a-8.2.1	特権的アクセス権の割当ては、アクセス制御に関するトピック固有の方針に従って、認可プロセスによって管理する。	手引に関連記載あり	9.2.3.1	特権的アクセス権の割当ては、関連するアクセス制御方針に従って、正式な認可プロセスによって管理する。
			8a-8.2.2	この管理策の実施については、次の事項を考慮する。 a) 各々のシステム又はプロセスの特権的アクセス権を必要とする利用者を特定する。	手引に関連記載あり	9.2.3.2	特権の割当ての正式な認可プロセスでは、各々のシステム又はプロセス（例えば、オペレーティングシステム、データベース管理システム、各アプリケーション）に関連した特権的アクセス権、及び特権的アクセス権を割り当てる必要がある利用者を特定する。
			8a-8.2.2	この管理策の実施については、次の事項を考慮する。 b) 特権的アクセス権を、アクセス制御に関するトピック固有の方針に沿って、必要に応じて、かつ、事象ごとに、利用者に割り当てる（すなわち、特権的アクセスをより必要とする活動を実行するために必要な力量をもつ個人に対してだけ、かつその個人の職務上の役割のための最小限の要求に基づいて）。	手引に関連記載あり	9.2.3.3	特権の割当ての正式な認可プロセスでは、特権的アクセス権を、アクセス制御方針に沿って、使用の必要性に応じて、かつ、事象に応じて、利用者に割り当てる。すなわち、利用者の職務上の役割のための最小限の要求事項に基づいて割り当てる。
			8a-8.2.2	この管理策の実施については、次の事項を考慮する。 c) 特権の認可プロセス（すなわち、誰が特権的アクセス権を承認することが可能かを決定するか、又は特権的アクセス権は認可プロセスが完了するまで許可しない。）及び割り当てた全ての特権の記録を維持する。	手引に関連記載あり	9.2.3.4	特権の割当ての正式な認可プロセスでは、割り当てた全ての特権の認可プロセス及び記録を維持する。
					手引に関連記載あり	9.2.3.5	特権の割当ての正式な認可プロセスでは、特権的アクセス権は、認可プロセスが完了するまで許可しない。
			8a-8.2.2	この管理策の実施については、次の事項を考慮する。 d) 特権的アクセス権の終了に関する要求事項を定め、実施する。	手引に関連記載あり	9.2.3.6	特権の割当ての正式な認可プロセスでは、特権的アクセス権の終了に関する要求事項を定める。
			8a-8.2.2	この管理策の実施については、次の事項を考慮する。 e) 利用者が、自らが特権的アクセス権をもっていること、及び自らがいつ特権的アクセスモードになっているかを認識することを確実にするための対策を講じる。考えられる対策としては、特別の利用者識別情報、利用者インタフェース設定、又は特別の装置の使用が含まれる。	手引に関連記載あり	–	（対応項なし）
			8a-8.2.2	この管理策の実施については、次の事項を考慮する。 f) 特権的アクセス権における認証の要求事項は、通常のアクセス権における要求事項よりも厳しくなる場合がある。特権的アクセス権を用いて作業を行う前に、再認証又は認証の格上げが必要になる場合がある。	手引に関連記載あり	–	（対応項なし）
			8a-8.2.2	この管理策の実施については、次の事項を考慮する。 g) 定期的に、また組織に何か変更があった後に、特権的アクセス権を用いて作業する利用者をレビューし、特権的アクセス権を用いた作業に関して、その利用者が職務、役割、責任及び力量の点でやも適格であるかどうかを検証する。	手引に関連記載あり	9.2.3.8	特権の割当ての正式な認可プロセスでは、特権的アクセス権を与えられた利用者の力量がその職務に見合っていることを検証するために、その力量を定期的にレビューする。
					手引に関連記載あり	9.2.5.5	特権の割当てを定められた間隔で点検して、認可されていない特権が取得されていないことを確認する。
					手引に関連記載あり	9.2.5.6	特権アカウントを変更する際は、定期的なレビューのために変更ログをとる。
			8a-8.2.2	この管理策の実施については、次の事項を考慮する。 h) 汎用の実務管理者IDの使用を避けるため、システムの構成管理機能に応じて、具体的な規則を確立する。そのようなID の認証情報を管理し、保護する。	手引に関連記載あり	9.2.3.9	特権の割当ての正式な認可プロセスでは、汎用の実務管理者ID の認可されていない使用を避けるため、システムの構成管理機能に応じて、具体的な手順を確立及び維持する。
			8a-8.2.2	この管理策の実施については、次の事項を考慮する。 i) 特権的アクセス権を永続的に許可するのではなく、承認された変更又は活動を実施するのに必要な時間枠だけ一時的な特権的アクセスを許可する。これはしばしばブレークグラス手順（break glass procedure）と呼ばれ、しばしば特権的アクセス管理技術において自動化されている。	手引に関連記載あり	–	（対応項なし）
			8a-8.2.2	この管理策の実施については、次の事項を考慮する。 j) 監査の目的で、システムへの全ての特権的アクセスのログを記録する。	手引に関連記載あり	–	（対応項なし）
			8a-8.2.2	この管理策の実施については、次の事項を考慮する。 k) 特権的アクセス権をもつ識別情報を複数の人で共有又は連携することはせず、特定の特権的アクセス権の割当てが許可された個別の識別情報を各人に割り当てる。特権的アクセス権の管理を簡素化するために、識別情報をグループ化することが可能である。	手引に関連記載あり	–	（対応項なし）
			8a-8.2.2	この管理策の実施については、次の事項を考慮する。 l) 特権的アクセス権をもつ識別情報は、管理作業を実行するためだけに使用し、日常の一般的な職務（すなわち、電子メールの確認、ウェブへのアクセス）には使用しない（利用者はこれらの活動のために別の通常のネットワーク識別情報をもつ。）。	手引に関連記載あり	9.2.3.7	特権の割当ての正式な認可プロセスでは、特権的アクセス権は、通常業務に用いている利用者ID とは別の利用者ID に割り当てる。特権を与えられたID からは、通常業務を行わない。
8.2.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
8.3	情報へのアクセス制限 統制目標：情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制限する。 目的：情報及びその他の関連資産への認可されたアクセスだけを確実にし、認可されていないアクセスを防止するため。		8.3	情報へのアクセス制限 管理策 情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制限する。 目的 情報及びその他の関連資産への認可されたアクセスだけを確実にし、認可されていないアクセスを防止するため。		9.4	システム及びアプリケーションのアクセス制御 管理目的：システム及びアプリケーションへの、認可されていないアクセスを防止するため。
						9.4.1	情報へのアクセス制限 情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限する。
8.3.1	情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関する方針に従って、制限を実施する。	アクセス制限の要求事項を満たすために、次の事項を考慮する。 a) 未知の利用者識別情報又は匿名の者による、取扱いに慎重を要する情報へのアクセスを許可しない。公開アクセス又は匿名アクセスは、取扱いに慎重を要する情報を含まない保管場所には許可する。 b) システム、アプリケーション及びサービスにもつ情報へのアクセスを制御するための構成の仕組みを提供する。 c) 利用者がアクセスできるデータを制御する。 d) どの識別情報又は識別情報のグループがどのアクセス権（読出し、書込み、削除、実行など）をもつかを制御する。 e) 取扱いに慎重を要するアプリケーション、アプリケーションデータ又はシステムを隔離するための、物理的又は論理的なアクセス制御を提供する。 次の場合には、組織にとって高い価値をもつ取扱いに慎重を要する情報を保護するための動的アクセス管理手法及びプロセスの採用を検討する。 a) 誰がどの期間、どのように情報にアクセスできるかを細かく制御する必要がある。 b) 情報を組織外の人々と共有し、誰がそれにアクセスできるかを制御する。 c) 情報の使用及び配布をリアルタイムで動的に管理する。 d) 認可されていない変更、複製及び配布（印刷を含む。）から情報を保護する。 e) 情報の使用を監視する。 f) 将来、調査が必要になった場合に備えて、情報の変更を記録する。 動的アクセス管理手法は、次の事項を含め、情報をそのライフサイクル（すなわち、作成、処理、保存、送信及び処分）を通じて保護する。 a) 次の事項を考慮して、個別の事例に基づき動的アクセス管理に関する規則を確立する。 1) 識別情報、装置・機器、場所又はアプリケーションに基づいてアクセス許可を与える。 2) 動的アクセス管理手法を用いてどの情報を保護する必要があるかを決定するために分類体系を活用する。 b) 運用、監視及び報告のプロセスを確立し、技術基盤を支援する。 動的アクセス管理システムは、次の方法によって情報を保護する。 a) 情報にアクセスする際に、認証、適切な資格情報又は証明書を要求する。 b) アクセスを、例えば、規定された時間枠（所定の日付以後、特定の日付までなど）に制限する。 c) 情報を保護するために暗号化を利用する。 d) 情報の印刷許可を定義する。 e) 誰が情報にアクセスし、その情報がどのように使用されたかを記録する。 f) 情報の悪用の試みが検知された場合に警報を上げる。	8a-8.3.1	情報及びその他の関連資産へのアクセスは、確立されたトピック固有の方針に従って制限する。	手引に関連記載あり	9.4.1.1	アクセスへの制限は、個々の業務用アプリケーションの要求事項に基づき、定められたアクセス制御方針に従う。
			8a-8.3.2	アクセス制限の要求事項を満たすために、次の事項を考慮する。 a) 未知の利用者識別情報又は匿名の者による、取扱いに慎重を要する情報へのアクセスを許可しない。公開アクセス又は匿名アクセスは、取扱いに慎重を要する情報を含まない保管場所にだけ許可する。	手引に関連記載あり	–	（対応項なし）
			8a-8.3.2	アクセス制限の要求事項を満たすために、次の事項を考慮する。 b) システム、アプリケーション及びサービスにもつ情報へのアクセスを制御するための構成の仕組みを提供する。	手引に関連記載あり	9.4.1.2	アクセス制限の要求事項を満たすために、アプリケーションシステム機能は不可欠な機能のみを提供し、その機能へのアクセスを制御するためのメニューを提供する。
			8a-8.3.2	アクセス制限の要求事項を満たすために、次の事項を考慮する。 c) 利用者がアクセスできるデータを制御する。	手引に関連記載あり	9.4.1.3	アクセス制限の要求事項を満たすために、利用者がアクセスできる機能、ポート、プロトコル、サービス、データを制御する。
			8a-8.3.2	アクセス制限の要求事項を満たすために、次の事項を考慮する。 d) どの識別情報又は識別情報のグループがどのアクセス権をもつかを制御する。	手引に関連記載あり	9.4.1.4	アクセス制限の要求事項を満たすために、利用者のアクセス権（例えば、読出し、書込み、削除、実行）を制御する。
			8a-8.3.2	アクセス制限の要求事項を満たすために、次の事項を考慮する。 e) 取扱いに慎重を要するアプリケーション、アプリケーションデータ又はシステムを隔離するための、物理的又は論理的なアクセス制御を提供する。	手引に関連記載あり	9.4.1.7	アクセス制限の要求事項を満たすために、取扱いに慎重を要するアプリケーション、アプリケーションデータ又はシステムを隔離するための、物理的又は論理的なアクセス制御を提供する。
			8a-8.3.3	次の場合には、組織にとって高い価値をもつ取扱いに慎重を要する情報を保護するための動的アクセス管理手法及びプロセスの採用を検討する。 a) 誰がどの期間、どのように情報にアクセスできるかを細かく制御する必要がある。 b) 情報を組織外の人々と共有し、誰がそれにアクセスできるかを制御する。 c) 情報の使用及び配布をリアルタイムで動的に管理する。 d) 認可されていない変更、複製及び配布（印刷を含む。）から情報を保護する。 e) 情報の使用を監視する。 f) 将来、調査が必要になった場合に備えて、情報の変更を記録する。	手引に関連記載あり	–	（対応項なし）
			8a-8.3.4	動的アクセス管理手法は、次の事項を含め、情報をそのライフサイクル（すなわち、作成、処理、保存、送信及び処分）を通じて保護する。 a) 次の事項を考慮して、個別の事例に基づき動的アクセス管理に関する規則を確立する。 1) 識別情報、装置・機器、場所又はアプリケーションに基づいてアクセス許可を与える。 2) 動的アクセス管理手法を用いてどの情報を保護する必要があるかを決定するために分類体系を活用する。 b) 運用、監視及び報告のプロセスを確立し、技術基盤を支援する。	手引に関連記載あり	–	（対応項なし）
			8a-8.3.5	動的アクセス管理システムは、次の方法によって情報を保護する。 a) 情報にアクセスする際に、認証、適切な資格情報又は証明書を要求する。 b) アクセスを、例えば、規定された時間枠に制限する。 c) 情報を保護するために暗号化を利用する。 d) 情報の印刷許可を定義する。 e) 誰が情報にアクセスし、その情報がどのように使用されたかを記録する。 f) 情報の悪用の試みが検知された場合に警報を上げる。	手引に関連記載あり	–	（対応項なし）
8.3.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.4	ソースコードへのアクセス 統制目標：ソースコード、開発ツール、及びソフトウェアライブラリへの読取り及び書込みアクセスを適切に管理する。 目的：認可されていない機能が入り込むことを防止し、意図しない又は悪意のある変更を回避し、価値の高い知的財産の機密性を維持するため。		8.4	ソースコードへのアクセス 管理策 ソースコード、開発ツール、及びソフトウェアライブラリへの読取り及び書込みアクセスを適切に管理する。 目的 認可されていない機能が入り込むことを防止し、意図しない又は悪意のある変更を回避し、価値の高い知的財産の機密性を維持するため。		9.4.5	プログラムソースコードへのアクセス制御 プログラムソースコードへのアクセスは、制限する。
8.4.1	プログラムソースコード及びプログラムソースライブラリへの読取り及び書込みのアクセスを管理する。	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 a) プログラムソースコード及びプログラムソースライブラリへのアクセスは、確立した手順に従って管理する。 b) ソースコードへの読取り及び書込みアクセスの許可は、業務上のニーズに基づき、変更又は悪用のリスクに対処するために管理し、かつ、確立された手順に従って行う。 c) ソースコード及び関連情報の更新、並びにソースコードへのアクセスの許可は、変更管理手順（8.32参照）に従って行い、かつ、適切な認可を得た後にだけ実施する。 d) 開発者にソースコード又はソースライブラリへの直接アクセスは許可せず、ソースコードに関する活動及び認可を管理する開発者ツールを通じて許可する。 e) プログラムリストは、セキュリティが保たれた環境で保持する。その環境では、読取り及び書込みアクセスを適切に管理し、割り当てる。 f) ソースコードへの全てのアクセス及び全ての変更について、監査ログを維持する。 プログラムソースコードの公開を意図している場合には、その完全性に保証を与える追加の管理策（例えば、ディジタル署名）の使用を考慮する。	8a-8.4.5	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 a) プログラムソースコード及びプログラムソースライブラリへのアクセスは、確立した手順に従って管理する。	手引に関連記載あり	9.4.5.3	プログラムソースコード及びプログラムソースライブラリは、確立した手順に従って管理する。
			8a-8.4.5	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 b) ソースコードへの読取り及び書込みアクセスの許可は、業務上のニーズに基づき、変更又は悪用のリスクに対処するために管理し、かつ、確立された手順に従って行う。	手引に関連記載あり	–	（対応項なし）
			8a-8.4.5	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 c) ソースコード及び関連情報の更新、並びにソースコードへのアクセスの許可は、変更管理手順に従って行い、かつ、適切な認可を得た後にだけ実施する。	手引に関連記載あり	9.4.5.8	プログラムソースライブラリの保守及び複製は、厳しい変更管理手順に従う。
			8a-8.4.5	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 d) 開発者にソースコード又はソースライブラリへの直接アクセスは許可せず、ソースコードに関する活動及び認可を管理する開発者ツールを通じて許可する。	手引に関連記載あり	9.4.5.5	プログラムソースライブラリ及び関連情報の更新、並びにプログラマへのプログラムソースの発行は、適切な認可を得た後にだけ実施する。
			8a-8.4.5	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 e) プログラムリストは、セキュリティが保たれた環境で保持する。その環境では、読取り及び書込みアクセスを適切に管理し、割り当てる。	手引に関連記載あり	9.4.5.6	プログラムリストは、セキュリティが保たれた環境で保持する。
			8a-8.4.5	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 f) ソースコードへの全てのアクセス及び全ての変更について、監査ログを維持する。	手引に関連記載あり	9.4.5.7	プログラムソースライブラリへの全てのアクセスについて、監査ログを維持する。
			8a-8.4.6	プログラムソースコードの公開を意図している場合には、その完全性に保証を与える追加の管理策の使用を考慮する。	手引に関連記載あり	9.4.5.9	プログラムソースコードの公開を意図している場合には、その完全性を保証するために役立つ追加的な管理策（例えば、ディジタル署名）を実施する。
8.4.2	ソースコード関連書類及び開発ツールへの読取り及び書込みのアクセスを管理する。	ソースコード、関連書類（例えば、設計書、仕様書、検証計画書、妥当性確認計画書）及び開発ツール（例えば、コンパイラ、ビルダ、統合ツール、テストプラットフォーム及びデスト環境）へのアクセスは、厳重に管理する。ソースコードについては、できればソースコード管理システムにおいて、コードを集中保管して管理することによってこれを達成することが可能である。 ソースコードへの読取りアクセス及び書込みアクセスは、必要に応じて要員の役割に基づいて制限する。例えば、ソースコードへの読取りアクセスは組織内で広く提供することはできるが、ソースコードへの書込みアクセスは、特権をもつ要員又は指定された管理責任者だけに認める。 コード部品を組織内の複数の開発者が使用する場合には、一元化したコードリポジトリへの読取りアクセスを提供する。 オープンソースコード又は第三者のコード部品の一元化した外部コードリポジトリへの書込みアクセスは制限する。	8a-8.4.1	ソースコード、関連書類及び開発ツールへのアクセスは、厳重に管理する。	手引に関連記載あり	9.4.5.1	プログラムソースコード及び関連書類（例えば、設計書、仕様書、検証計画書、妥当性確認計画書）へのアクセスは、認可されていない機能が入り込むことを防止し、意図しない変更を回避し、価値の高い知的財産の機密性を維持するために、厳重に管理する。
			（8a-8.4.1参考）	ソースコードについては、できればソースコード管理システムにおいて、コードを集中保管して管理することによってこれを達成することが可能である。	手引に関連記載あり	–	（対応項なし）
			8a-8.4.2	ソースコードへの読取りアクセス及び書込みアクセスは、必要に応じて要員の役割に基づいて制限する。	手引に関連記載あり	–	（対応項なし）
			（8a-8.4.2参考）	例えば、ソースコードへの読取りアクセスは組織内で広く提供することはできるが、ソースコードへの書込みアクセスは、特権をもつ要員又は指定された管理責任者だけに認める。	手引に関連記載あり	–	（対応項なし）
			8a-8.4.3	コード部品を組織内の複数の開発者が使用する場合には、一元化したコードリポジトリへの読取りアクセスを提供する。	手引に関連記載あり	–	（対応項なし）
			8a-8.4.4	オープンソースコード又は第三者のコード部品の一元化した外部コードリポジトリへの書込みアクセスは制限する。	手引に関連記載あり	–	（対応項なし）
8.5	セキュリティを保った認証 統制目標：セキュリティを保った認証技術及び手順を、情報へのアクセス制限、及びアクセス制御に関するトピック固有の方針に基づいて備える。 目的：システム、アプリケーション及びサービスへのアクセスを許可するときに、利用者又はエンティティをセキュリティを保って認証することを確実にするため。		8.5	セキュリティを保った認証 管理策 セキュリティを保った認証技術及び手順を、情報へのアクセス制限、及びアクセス制御に関するトピック固有の方針に基づいて備える。 目的 システム、アプリケーション及びサービスへのアクセスを許可するときに、利用者又はエンティティをセキュリティを保って認証することを確実にするため。		9.4.2	セキュリティに配慮したログオン手順 アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御する。
8.5.1	セキュリティを保った認証技術及び手順は、情報へのアクセス制限、及びアクセス制御に関する方針に基づいて、実施する。	利用者、ソフトウェア、メッセージ、及び/その他のエンティティが提示する識別情報を検証するために、適切な認証技術を選択する。 認証の強度は、アクセスする情報の分類に適したものを選択する。 強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、ディジタル証明書、スマートカード、トークン、生体認証などの認証方法を用いる。 重要な情報システムにアクセスするために、認証情報に追加の認証要素を加える（多要素認証とも呼ばれる。）。知識、所持物、生体情報など、複数の認証要素を組み合わせて使用することで、認可されていないアクセスの可能性を減らすことが可能である。特定の状況下においては、多要素認証に他の手法を組み合わせて、あらかじめ定義したルール及びパターンに基づく追加の要素も条件として要求することが可能である。このルール及びパターンには、通常と異なる場所からのアクセス、通常と異なる装置・機器からのアクセス、通常と異なる時間でのアクセスなどがある。 生体認証情報は、機密性が損なわれた場合は無効化する。 使用の条件（例えば、湿気又は加齢）によっては、生体認証が利用できないことに備えるため、生体認証は少なくとも一つの代替の認証手法をもつ。 ログオンの手順及び技術は、次の事項を考慮して実装する。 a) 認可されていない利用者に不必要な手助けを提供することを避けるために、取扱いに慎重を要するシステム又はアプリケーションの情報を、ログオン手順が正常に終了するまで表示しない。 b) システム、アプリケーション、又はサービスへのアクセスは、認可されている利用者に限定する"という一般的な警告を表示する。 c) ログオン手順中に、認可されていない利用者の助けとなるようなメッセージを表示しない（例えば、エラー状態が発生しても、システムからは、データの(どの部分が正しい)か又は関連っているかを示すことは望ましくない。）。 d) ログオン情報の妥当性確認は、全ての入力データが完了した時点で(だけ)行う。 e) 利用者名及びパスワードに関する総当たり攻撃でログオンしようとする試みから保護する（例えば、コンピュータ化人間を区別する完全に自動化された公開チューリングテスト（CAPTCHA）を使用する、あらかじめ定義した回数の試行失敗の後にパスワードリセットを要求する、又は最大2定めた回数のエラーの後に利用者をブロックする。）。 f) 失敗した試み及び成功した試みのログをとる。 g) ログオン制御への違反又は違反が試みられた可能性を検知した場合には、セキュリティ事象として取り上げる（例えば、誤ったパスワードの試行が特定の回数に達したときに利用者及び組織のシステム実務管理者に警告を送信する。）。 h) ログオンが成功裏に終了した時点で、次の情報を別の手段で表示又は送信する。 1) 前回成功裏にログオンできた日時 2) 前回のログオン以降、失敗したログオンの試みがある場合は、その詳細 i) 入力したパスワードを平文で表示しない。場合によっては、利用者のログオンを容易にするため、この機能を無効化する必要がある可能性がある（例えば、アクセシビリティのために、又はエラーの緩和によって利用者が打ちされないようにするために）。 j) ネットワークニファプログラムで構築されることを避けるため、ネットワークを介してパスワードを平文で通信しない。 k) リスクの高い場所（例えば、組織のセキュリティ管理外にある公共の場所又は外部の区域、利用者エンドポイント機器）では、特に、使用せずにあらかじめ定めた時間が経過したセッションを終了する。 l) リスクの高いアプリケーションのセキュリティを高め、認可されていないアクセスの危険性を低減するために、接続の継続時間を制限する。	8a-8.5.1	利用者、ソフトウェア、メッセージ、及び/その他のエンティティが提示する識別情報を検証するために、適切な認証技術を選択する。	手引に関連記載あり	9.4.2.1	利用者が提示する識別情報を検証するために、適切な認証技術を選択する。
			8a-8.5.2	認証の強度は、アクセスする情報の分類に適したものを選択する。	手引に関連記載あり	–	（対応項なし）
			8a-8.5.3	強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、ディジタル証明書、スマートカード、トークン、生体認証などの認証方法を用いる。	手引に関連記載あり	9.4.2.2.B	強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、暗号による手段、スマートカード、トークン、生体認証などの認証方法を用いる。
			8a-8.5.4	重要な情報システムにアクセスするために、認証情報に追加の認証要素を加える。	手引に関連記載あり	–	（対応項なし）
			（8a-8.5.4参考1）	知識、所持物、生体情報など、複数の認証要素を組み合わせて使用することで、認可されていないアクセスの可能性を減らすことが可能である。	手引に関連記載あり	–	（対応項なし）
			（8a-8.5.4参考2）	特定の状況下においては、多要素認証に他の手法も組み合わせて、あらかじめ定義したルール及びパターンに基づく追加の要素も条件として要求することが可能である。このルール及びパターンには、通常と異なる場所からのアクセス、通常と異なる装置・機器からのアクセス、通常と異なる時間でのアクセスなどがある。	手引に関連記載あり	–	（対応項なし）
			8a-8.5.5	生体認証情報は、機密性が損なわれた場合は無効化する。	手引に関連記載あり	–	（対応項なし）
			8a-8.5.6	使用の条件によっては、生体認証が利用できないことに備えるため、生体認証は少なくとも一つの代替の認証手法をもつ。	手引に関連記載あり	–	（対応項なし）
			8a-8.5.7	システム又はアプリケーションにログオンする手順は、認可されていないアクセスのリスクを最小限に抑えるように設計する。	手引に関連記載あり	9.4.2.3	システム又はアプリケーションへログオンするための手順は、認可されていないアクセスの機会を最小限に抑えるように設計する。
			8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 a) 認可されていない利用者に不必要な手助けを提供することを避けるために、取扱いに慎重を要するシステム又はアプリケーションの情報を、ログオン手順が正常に終了するまで表示しない。	手引に関連記載あり	9.4.2.4	ログオン手順では、認可されていない利用者に無用な助けを与えないために、システム又はアプリケーションについての情報の開示は、最小限にする。
					手引に関連記載あり	9.4.2.5	システム又はアプリケーションの識別子を、ログオン手順が正常に終了するまで表示しない。
			8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 b) "システム、アプリケーション、又はサービスへのアクセスは、認可されている利用者に限定する"という一般的な警告を表示する。	手引に関連記載あり	9.4.2.6	ログオン手順では、「コンピュータへのアクセスは、認可されている利用者に限定する」という警告を表示する。
			8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 c) ログオン手順中に、認可されていない利用者の助けとなるようなメッセージを表示しない。	手引に関連記載あり	9.4.2.7	ログオン手順中に、認可されていない利用者の助けとなるようなメッセージを表示しない。
			8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 d) ログオン情報の妥当性確認は、全ての入力データが完了した時点で(だけ)行う。	手引に関連記載あり	9.4.2.8	ログオン手順では、ログオン情報の妥当性検証は、全ての入力データが完了した時点で(だけ)行う。誤り条件が発生しても、システムからは、データの(どの部分が正しい)か又は関連っているかを指摘しない。
			8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 e) 利用者名及びパスワードに関する総当たり攻撃でログオンしようとする試みから保護する。	手引に関連記載あり	9.4.2.9	総当たり攻撃でログオンしようとする試みから保護する。
			8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 f) 失敗した試み及び成功した試みのログをとる。	手引に関連記載あり	9.4.2.10	ログオン手順では、失敗した試み及び成功した試みのログをとる。
			8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 g) ログオン制御への違反又は違反が試みられた可能性を検知した場合には、セキュリティ事象として取り上げる。	手引に関連記載あり	9.4.2.11	ログオン制御への違反又は違反が試みられた可能性が検知された場合には、セキュリティ事象として取り上げる。
			8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 h) ログオンが成功裏に終了した時点で、次の情報を別の手段で表示又は送信する。 1) 前回成功裏にログオンできた日時 2) 前回のログオン以降、失敗したログオンの試みがある場合は、その詳細	手引に関連記載あり	9.4.2.12	ログオンが成功裏に終了した時点で、①前回成功裏にログオンできた日時、②前回のログオン以降、失敗したログオンの試みがある場合は、その詳細を表示する。
			8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 i) 入力したパスワードを平文で表示しない。場合によっては、利用者のログオンを容易にするため、この機能を無効化する必要がある可能性がある。	手引に関連記載あり	9.4.2.13	ログオン手順では、入力したパスワードは表示しない。
			8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 j) ネットワークニファプログラムで構築されることを避けるため、ネットワークを介してパスワードを平文で通信しない。	手引に関連記載あり	9.4.2.14	ログオン手順では、ネットワークを介してパスワードを平文で通信しない。
			8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 k) リスクの高い場所では、特に、使用せずにあらかじめ定めた時間が経過したセッションを終了する。	手引に関連記載あり	9.4.2.15	ログオン手順では、リスクの高い場所（例えば、組織のセキュリティ管理外にある公共の場所又は外部の区域、モバイル機器）では特に、あらかじめ定めた条件に合致したセッションは終了する。
			8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 l) リスクの高いアプリケーションのセキュリティを高め、認可されていないアクセスの危険性を低減するために、接続の継続時間を制限する。	手引に関連記載あり	9.4.2.16	ログオン手順では、リスクの高いアプリケーションのセキュリティを高めるために接続時間を制限し、認可されていないアクセスの危険性を低減する。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.6	容量・能力の管理 統制目標：現在の及び予測される容量・能力の要求事項に合わせて、資源の利用を監視し調整する。 目的：情報処理施設、人的資源、オフィス及びその他の施設で必要とされる容量・能力の確保を確実にするため。		8.6	容量・能力の管理 管理策 現在の及び予測される容量・能力の要求事項に合わせて、資源の利用を監視し調整する。 目的 情報処理施設、人的資源、オフィス及びその他の施設で必要とされる容量・能力の確保を確実にするため。		12.1.3	容量・能力の管理 要求された主要なシステム資源の使用を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。
8.6.1	情報処理施設、人的資源、オフィス及びその他の施設の容量・能力に関する要求事項を定義する。	事業におけるシステム及び/プロセスの重要度を考慮に入れて、情報処理施設、人的資源、オフィス及びその他の施設の容量・能力に関する要求事項を特定する。 業務上必須のシステムについては、容量・能力の管理計画を文書化することを検討する。	8a-8.6.1	事業におけるシステム及び/プロセスの重要度を考慮に入れて、情報処理施設、人的資源、オフィス及びその他の施設の容量・能力に関する要求事項を特定する。	手引に関連記載あり	12.1.3.1	事業におけるシステムの重要度を考慮に入れて、その容量・能力に関する要求事項を特定する。
			8a-8.6.10	業務上必須のシステムについては、容量・能力の管理計画を文書化することを検討する。	手引に関連記載あり	12.1.3.8	業務上必須のシステムについては、容量・能力の管理計画を文書化することを検討する。
8.6.2	資源の利用を監視する。	システムの可用性及び/効率性の確保を確実にするため、また、必要な場合には、改善のために、システムの調整及び/監視を適用する。 適切な時点で問題を知らせるために、検知のための管理策を備える。 組織は、最大性能の要求事項を満たすのに十分なシステム容量・能力が利用できることを確認するために、システム及びサービスの負荷テストを実施する。 （上記の他、一部 JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	8a-8.6.2	システムの可用性及び/効率性の確保を確実にするため、また、必要な場合には、改善のために、システムの調整及び/監視を適用する。	手引に関連記載あり	12.1.3.2	システムの可用性及び/効率性を確実にするため、また、改善のために、システム調整及び/監視を適用する。
			8a-8.6.4	適切な時点で問題を知らせるために、検知のための管理策を備える。	手引に関連記載あり	12.1.3.3	適切な時点で問題を知らせるために、検知のための管理策を備える。
			8a-8.6.3	組織は、最大性能の要求事項を満たすのに十分なシステム容量・能力が利用できることを確認するために、システム及び/サービスの負荷テストを実施する。	手引に関連記載あり	–	（対応項なし）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
8.6.3	容量・能力に限界があると予測される場合は、容量・能力の増強又は需要の低減を実施する。	将来必要とされる容量・能力の予測では、新しい事業及び/システムに対する要求事項並びに組織の情報処理の能力についての現在の傾向及び/予測される傾向を考慮する。 入手に長い期間又は高額な費用が掛かる資源については、特別な注意を払うため、管理者、及び/サービス又は製品の管理責任者は、主要なシステム資源の使用を監視する。 システムセキュリティ及びサービスに脅威をもたらす可能性がある、潜在的な資源の制限及び/主要な要員への依存度合いを特定し、回避するために、管理者は、容量・能力に関する情報を用い、また、適切な処置を立案する。十分な容量・能力の提供は、容量・能力の増強又は需要の低減によって達成することが可能である。 容量・能力を増強するには、次の事項を考慮する。 a) 新しい要員を雇用する。 b) 新しい施設又は場所を取得する。 c) より強力な処理システム、メモリ及び/ストレージを取得する。 d) 容量・能力の課題に直接に応えるという特性があるクラウドコンピューティングを利用する。クラウドコンピューティングは、特定のアプリケーション及び/サービスで利用できる資源を要求に応じて迅速に拡張し、削減することを可能とする、弾力性及び/スケーラビリティをもっている。 組織の資源に関する需要を減らすために、次の事項を考慮する。 a) 古いデータの削除（ディスクスペース） b) 保持期間を満了したハードコピー記録の処分（棚スペースを空ける。） c) アプリケーション、システム、データベース又は環境の廃止 d) バッチのプロセス及び/スケジュールの最適化 e) アプリケーションコード及び/データベースへの照合せの最適化 f) 重要でない場合、大量の帯域を必要とするサービス（例えば、動画のストリーミング）に対する帯域割当ての拒否又は制限	8a-8.6.5	将来必要とされる容量・能力の予測では、新しい事業及び/システムに対する要求事項並びに組織の情報処理の能力についての現在の傾向及び/予測される傾向を考慮する。	手引に関連記載あり	12.1.3.4	将来必要とされる容量・能力の予測では、新しい事業及び/システムに対する要求事項並びに組織の情報処理の能力についての現在の傾向及び/予測される傾向を含める。
			8a-8.6.6	入手に長い期間又は高額な費用が掛かる資源については、特別な注意を払うため、管理者、及び/サービス又は製品の管理責任者は、主要なシステム資源の使用を監視する。	手引に関連記載あり	12.1.3.5	管理者は、特別な注意を払う必要のある主要なシステム資源（入手時間がかかるか又は費用がかかる資源）の使用を監視する。
			8a-8.6.7	システムセキュリティ及びサービスに脅威をもたらす可能性のある、潜在的な資源の制限及び/主要な要員への依存度合いを特定し、回避するために、管理者は、容量・能力に関する情報を用い、また、適切な処置を立案する。	手引に関連記載あり	12.1.3.7	システムセキュリティ及びサービスに脅威をもたらすおそれのある、潜在的なない（恐）路（bottlenecks）及び/主要な要員への依存度合いを特定し、回避するために、管理者は、上記の監視及び/傾向を特定した情報を利用して、適切な処置を立案する。
			(8a-8.6参考)	十分な容量・能力の提供は、容量・能力の増強又は需要の低減によって達成することが可能である。	手引に関連記載あり	–	（対応項なし）
			8a-8.6.8	容量・能力を増強するには、次の事項を考慮する。 a) 新しい要員を雇用する。 b) 新しい施設又は場所を取得する。 c) より強力な処理システム、メモリ及び/ストレージを取得する。 d) 容量・能力の課題に直接に応えるという特性があるクラウドコンピューティングを利用する。クラウドコンピューティングは、特定のアプリケーション及び/サービスで利用できる資源を要求に応じて迅速に拡張し、削減することを可能とする、弾力性及び/スケーラビリティをもっている。	手引に関連記載あり	–	（対応項なし）
			8a-8.6.9	組織の資源に関する需要を減らすために、次の事項を考慮する。 a) 古いデータの削除（ディスクスペース） b) 保持期間を満了したハードコピー記録の処分（棚スペースを空ける。） c) アプリケーション、システム、データベース又は環境の廃止 d) バッチのプロセス及び/スケジュールの最適化 e) アプリケーションコード及び/データベースへの照合せの最適化 f) 重要でない場合、大量の帯域を必要とするサービスに対する帯域割当ての拒否又は制限	手引に関連記載あり	–	（対応項なし）
8.7	マルウェアに対する保護 統制目標：マルウェアに対する保護を実施し、利用者の適切な認識によって支援する。 目的：情報及びその他の関連資産をマルウェアに対して保護することを確実にするため。		8.7	マルウェアに対する保護 管理策 マルウェアに対する保護を実施し、利用者の適切な認識によって支援する。 目的 情報及びその他の関連資産をマルウェアに対して保護することを確実にするため。		12.2	マルウェアからの保護 管理目的：情報及び/情報処理施設がマルウェアから保護されることを確実にするため。
						12.2.1	マルウェアに対する管理策 マルウェアから保護するために、利用者に適切に認識させること併せて、検出、予防及び/回復のための管理策を実施する。
8.7.1	情報及びその他の関連資産をマルウェアから保護する。	マルウェアに対する保護は、マルウェアの検出・修復ソフトウェア、情報セキュリティに対する認識、及び/システムへの適切なアクセス・変更管理についての管理策に基づく。適常、マルウェアの検出・修復ソフトウェアを単独で使用することは十分ではない。 マルウェアに対する保護については、次の手引を考慮する。 a) 認可されていないソフトウェアの使用を防止又は検出するための規則及び/管理策の実施［例えば、アプリケーションの許可リスト（すなわち、許可されたアプリケーションを示すリストの使用）］（8.19及び8.32参照） b) 悪意のあるウェブサイトであると知られている又は疑われるウェブサイトの使用を、防止又は検出するための管理策の実施（例えば、ブロックリスト） c) マルウェアに付け込まれる可能性のある弱い/弱性を減らす［例えば、技術的弱い/弱性管理によって（8.8及び8.19参照）］。 d) システム、特に重要な業務プロセスを支えるシステムのソフトウェア及び/データについて、定常的な自動化された妥当性確認の実施。承認されていないファイル又は認可されていない変更の存在を調査する。 e) 外部ネットワークから若しくは外部ネットワーク経由で、又は他の媒体を通じてファイル及び/ソフトウェア入手することにより/又に対する保護対策を確立する。 f) コンピュータ及び/電子記憶媒体をスキャンするための、マルウェアの検出・修復ソフトウェアの導入及び/定常的な更新。次の事項を含む定常的なスキャンを実施する。 1) ネットワーク経由又は何らかの形式の電子記憶媒体を通じて入手した全てのデータに対する、マルウェア検出のための使用前のスキャン 2) 電子メール及びインスタントメッセージングの添付ファイル及び/ダウンロードしたファイルに対する、マルウェア検出のための使用前のスキャン。このスキャンは、様々な場所（例えば、電子メールサーバ、デスクトップコンピュータ）で、及び/組織のネットワークの入口で実施する。 3) ウェブページに対するアクセスの際のマルウェア検出のためのスキャン g) リスクアセスメントの結果に基づき、かつ、次の事項を考慮して、マルウェアの検出・修復ツールの配置及び/構成を決定する。 1) 特に効果的である場合には、多層防御の原則。例えば、これはネットワークゲートウェイ（電子メール、ファイル転送、ウェブなどの様々なアプリケーションプロトコルにおける）、並びに利用者エンドポイント機器及び/サーバにおいて、マルウェアの検出につながる可能性がある。 2) 攻撃者がマルウェアを送り込むための回避技術（例えば、暗号化されたファイルの使用）、又はマルウェアの送信における暗号化プロトコルの使用 h) マルウェアに対する通常の管理策を、（注）回する可能性がある。保守及び/緊急時の手順中におけるマルウェアの入り込みの防止に注意を払う。 i) 例外承認権限、文書化した正当性の提示、及び/レビューの日付を含む、マルウェアに対する一部又は全ての対策の一時的又は恒久的な無効化を認可するプロセスを実施する。これは、マルウェアに対する保護によって通常の運用が中断・阻害される場合に必要になる可能性がある。 j) マルウェアの攻撃から回復するための適切な事業継続計画の策定。これには、必要な全てのデータ及び/ソフトウェアのバックアップ（オンラインとオフラインとの両方のバックアップを含む。）並び/に回復の対策を含める（8.13参照）。 k) 環境的な影響が生じる可能性のある環境の隔離 l) システム上でマルウェアに対する保護を扱う手順及び/責任の定義。これには、手順の使用、報告及び/マルウェア攻撃からの回復に関する訓練を含む。 m) マルウェアに感染した電子メール、ファイル又はプログラムの受信、送信又はインストールを特定し、可能なら/軽減する方法について、全ての利用者に意識向上及び/訓練（6.3参照）を提供する［n)及び/o)で収集され情報を、意識向上及び/訓練を最新状態に保つことを確実にするために使用することが可能である。］。 n) 定常的に新種のマルウェアに関する情報を収集するための手順の実施（例えば、メーリングリストへの登録及び/或はウェブサイトの確認） o) 誤告情報などマルウェアに関する情報が適格で正評のある情報源（例えば、信頼できるインターネットサイト、マルウェア検出ソフトウェアの供給者）から来ており、正確かつ役立つことを検証する。	8b-8.7.1	マルウェアに対する保護は、マルウェアの検出・修復ソフトウェア、情報セキュリティに対する認識、及び/システムへの適切なアクセス・変更管理についての管理策に基づく。	手引に関連記載あり	12.2.1.1	マルウェアに対する検出・修復ソフトウェア、情報セキュリティに対する認識、及び/システムへの適切なアクセス・変更管理、及び/外部からの不正通信の監視・分析に基づいた適当等の対処についての管理策により、マルウェアから保護する。
			(8b-8.7.1参考)	通常、マルウェアの検出・修復ソフトウェアを単独で使用することは十分ではない。	手引に関連記載あり	–	（対応項なし）
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 a) 認可されていないソフトウェアの使用を防止又は検出するための規則及び/管理策の実施	手引に関連記載あり	12.2.1.2	認可されていないソフトウェアの使用を禁止する正式な方針を確立し、定期的に見直しを行う。
					手引に関連記載あり	12.2.1.3	認可されていないソフトウェアの使用を防止又は検出するための管理策を実施（例えば、アプリケーションのホワイトリスト化）する。
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 b) 悪意のあるウェブサイトであると知られている又は疑われるウェブサイトの使用を、防止又は検出するための管理策の実施	手引に関連記載あり	12.2.1.4	悪意のあるウェブサイトであると知られている又は疑われるウェブサイトの使用を、防止又は検出するための管理策を実施（例えば、ブラックリスト）する。
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 c) マルウェアに付け込まれる可能性のある弱い/弱性を減らす。	手引に関連記載あり	12.2.1.6	マルウェアに付け込まれる可能性のある弱い/弱性を、技術的弱い/弱性管理などを通じて低減させる。
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 d) システム、特に重要な業務プロセスを支えるシステムのソフトウェア及び/データ一元について、定常的な自動化された妥当性確認の実施。承認されていないファイル又は認可されていない変更の存在を調査する。	手引に関連記載あり	12.2.1.7	重要な業務プロセスを支えるシステムのソフトウェア及び/データの、定めに従ったレビューを実施する。未承認のファイル又は認可されていない変更が含った場合には、正式に調査する。
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 e) 外部ネットワークから若しくは外部ネットワーク経由で、又は他の媒体を通じてファイル及び/ソフトウェア入手することにより/又に対する保護対策を確立する。	手引に関連記載あり	12.2.1.5	外部ネットワークから若しくは外部ネットワーク経由で、又は他の媒体を通じてファイル及び/ソフトウェアを入手することにより/又から保護し、どのような保護対策を行うことが望ましいかを示す組織の正式な方針を確立する。
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 f) コンピュータ及び/電子記憶媒体をスキャンするための、マルウェアの検出・修復ソフトウェアの導入及び/定常的な更新。次の事項を含む定常的なスキャンを実施する。 1) ネットワーク経由又は何らかの形式の電子記憶媒体を通じて入手した全てのデータに対する、マルウェア検出のための使用前のスキャン 2) 電子メール及びインスタントメッセージングの添付ファイル及び/ダウンロードしたファイルに対する、マルウェア検出のための使用前のスキャン。このスキャンは、様々な場所で、及び/組織のネットワークの入口で実施する。 3) ウェブページに対するアクセスの際のマルウェア検出のためのスキャン	手引に関連記載あり	12.2.1.8	予防又は定常作業として、コンピュータ及び/媒体を走査（scan）するために、マルウェアの検出・修復ソフトウェアの導入及び/定めに従った更新として、以下の3点を行う。 1. ネットワーク経由又は何らかの形式の記憶媒体を通じて入手した全てのファイルに対する、マルウェア検出のための使用前の走査。 2. 電子メールの添付ファイル及び/ダウンロードしたファイルに対する、マルウェア検出のための使用前の走査。この走査は、様々な場所（例えば、電子メールサーバ、デスクトップコンピュータ、組織のネットワークの入口）で実施する。 3. ウェブページに対するマルウェア検出のための走査。
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 g) リスクアセスメントの結果に基づき、かつ、次の事項を考慮して、マルウェアの検出・修復ツールの配置及び/構成を決定する。 1) 特に効果的である場合には、多層防御の原則。例えば、これはネットワークゲートウェイ、並び/に利用者エンドポイント機器及び/サーバにおいて、マルウェアの検出につながる可能性がある。 2) 攻撃者がマルウェアを送り込むための回避技術、又はマルウェアの送信における暗号化プロトコルの使用	手引に関連記載あり	–	（対応項なし）
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 h) マルウェアに対する通常の管理策を、（注）回する可能性がある。保守及び/緊急時の手順中におけるマルウェアの入り込みの防止に注意を払う。	手引に関連記載あり	–	（対応項なし）
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 i) 例外承認権限、文書化した正当性の提示、及び/レビューの日付を含む、マルウェアに対する一部又は全ての対策の一時的又は恒久的な無効化を認可するプロセスを実施する。これは、マルウェアに対する保護によって通常の運用が中断・阻害される場合に必要になる可能性がある。	手引に関連記載あり	–	（対応項なし）
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 j) マルウェアの攻撃から回復するための適切な事業継続計画の策定。これには、必要な全てのデータ及び/ソフトウェアのバックアップ（オンラインとオフラインとの両方のバックアップを含む。）並び/に回復の対策を含める。	手引に関連記載あり	12.2.1.10	マルウェアの攻撃から回復するための適切な事業継続計画を策定する。
					手引に関連記載あり	12.2.1.11	マルウェアの攻撃から回復するための適切な事業継続計画には、必要な全てのデータ及び/ソフトウェア、バックアップ及び/回復の手順を含める。
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 k) 環境的な影響が生じる可能性のある環境の隔離	手引に関連記載あり	12.2.1.14	環境的な影響が及ぶ可能性のある環境を隔離する。
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 l) システム上でマルウェアに対する保護を扱う手順及び/責任の定義。これには、手順の使用、報告及び/マルウェア攻撃からの回復に関する訓練を含む。	手引に関連記載あり	12.2.1.9	システムにおけるマルウェアからの保護、保護策の利用方法に関する訓練、マルウェアの攻撃の報告及び/マルウェアの攻撃からの回復に関する手順及び/責任を明確にする。
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 m) マルウェアに感染した電子メール、ファイル又はプログラムの受信、送信又はインストールを特定し、可能なら/軽減する方法について、全ての利用者に意識向上及び/訓練を提供する。	手引に関連記載あり	–	（対応項なし）
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 n) 定常的に新種のマルウェアに関する情報を収集するための手順の実施	手引に関連記載あり	12.2.1.12	常に情報を収集するための手順を実施（例えば、新種のマルウェアに関する情報を提供するメーリングリストへの登録又は/ウェブサイトの確認）する。
			8b-8.7.2	マルウェアに対する保護については、次の手引を考慮する。 o) 誤告情報などマルウェアに関する情報が適格で正評のある情報源から来ており、正確かつ役立つことを検証する。	手引に関連記載あり	12.2.1.13	マルウェアに関する情報を確認し、誤告情報が正確かつ役立つことを確実にするための以下の2つの手順を実施する。 1. 管理者は、曖昧さないぞらと真のマルウェアを識別するために、適切な情報源（例えば、定評のある行行物、信頼できるインターネットサイト、マルウェアの対策/ソフトウェア供給者）の利用を確実にする仕組みを整備する。 2. 監理者は、マルウェアではなく、いたずらの問題及び/それらを受け取ったときの対応について、全ての利用者に認識させる仕組みを整備する。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.8	技術的ぜい弱性の管理 統制目標：利用中の情報システムの技術的ぜい弱性に関する情報を獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価し、適切な手段をとる。 目的：技術的ぜい弱性の悪用を防止するため。		8.8	技術的ぜい弱性の管理 管理策 利用中の情報システムの技術的ぜい弱性に関する情報を獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価し、適切な手段をとる。 目的 技術的ぜい弱性の悪用を防止するため。		12.6	技術的ぜい弱性管理 管理目的：技術的ぜい弱性の悪用を防止するため。
						12.6.1	技術的ぜい弱性の管理 利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価する。さらに、それら関連するリスクに対処するために、適切な手段をとる。
						18.2.3	技術的順守のレビュー 情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューする。
8.8.1	技術的ぜい弱性を特定し、評価する。	組織は、効果的な技術的ぜい弱性管理の前提条件として、正確な資産の目録（5.9～5.14参照）をもつ。 資産の目録には、ソフトウェア業者、ソフトウェア名、版番号、配置状況（例えば、どのソフトウェアがどのシステム上に導入されているか。）、及びそのソフトウェアに責任のある組織内の担当者を含める。 技術的ぜい弱性を特定するために、組織は次の事項を考慮する。 a) 技術的ぜい弱性の管理に関連する役割及び責任を定め、確立する。技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性に関わるリスクアセスメント、更新、資産移動の追跡、及び要求される全ての調整責務が含まれる。 b) ソフトウェア及びその他の技術（組織の資産目録リスト[に基づく、5.9 参照）に関して、関連する技術的ぜい弱性を特定し、また、ぜい弱性を継続して認識するために用いる情報源を特定する。情報源の リストは、この目録を変更したとき、又は他の新しい若しくは有益な情報源を発見したときに更新する。 c) 情報システム（その構成要素を含む。）の供給者に、適用される契約に要求事項を含め、ぜい弱性の報告、取扱い及び開示を確実にすることを要求する。（5.20参照）。 d) ぜい弱性を特定し、ぜい弱性のパッチ適用が成功したかどうかを検証するために、使用している技術に適したぜい弱性スキャンツールを使用する。 e) ぜい弱性の特定を支援するため、力量が必[要]とされた者が、計画され、文書化された、再現可能な侵入テスト又はぜい弱性アセスメントを実施する。この活動はシステムのセキュリティを危うくする可能性があるため、注意を払う。 f) 第三者のライブラリ[及]びソースコードの使用について、ぜい弱性を追跡する。これはセキュリティに配慮したコーディングに含める（8.28参照）。 特定した技術的ぜい弱性を評価するために、次の手引を考慮する。 a) どのような対応及び修復活動が必要かを決定するために、報告書を分析及び検証する。 b) 潜在的な技術的ぜい弱性を特定したときは、それに伴うリスク及び講じるべき処置を特定する。 この処置は、ぜい弱性のあるシステムの更新又は他の管理策の適用を含む可能性がある。 組織は、次の事項のための手順及び能力を開発する。 a) 自らの製品及びサービス並[に]これらで使用している外部の構成要素について、ぜい弱性の存在を検知する。 b) 内部又は外部の供給元からぜい弱性報告を受け取る。 組織は、調査者及び他の人が問題を報告できるように、ぜい弱性の開示に関するトピック固有の方針の一部として公開連絡先を示す。 組織は、ぜい弱性の報告手順、オンライン報告書式を確立し、適切な脅威インテリジェンス又は情報共有の場を利用する。 組織は、ぜい弱性を適切に修復するために、組織における ぜい弱性の特定を支援する動機付けとして、報酬を提供するバグ報奨金プログラムの採用を検討する。 組織が力量のある業界団体又は他の利害関係者と情報を共有する。	8b-8.8.1	組織は、効果的な技術的ぜい弱性管理の前提条件として、正確な資産の目録をもつ。	手引に関連記載あり	12.6.1.1	技術的ぜい弱性（ソフトウェアの欠陥、誤った設定を含む。）の管理をサポートするために必要となる具体的な情報には、ソフトウェア業者、版番号、配置状況（例えば、どのソフトウェアがどのシステム上に導入されているか。）、及びそのソフトウェアに責任のある組織内の担当者を含める。
			8b-8.8.2	資産の目録には、ソフトウェア業者、ソフトウェア名、版番号、配置状況、及びそのソフトウェアに責任のある組織内の担当者を含める。	手引に関連記載あり	–	（対応項なし）
			8b-8.8.3	技術的ぜい弱性を特定するために、組織は次の事項を考慮する。 a) 技術的ぜい弱性の管理に関連する役割及び責任を定め、確立する。技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性に関わるリスクアセスメント、更新、資産移動の追跡、及び要求される全ての調整責務が含まれる。	手引に関連記載あり	12.6.1.3	技術的ぜい弱性の管理に関連する役割及び責任を定める。
					手引に関連記載あり	12.6.1.4	技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性に関わるリスクアセスメント、パッチの適用、資産移動の追跡、及び要求される全ての調整責務を含める。
			8b-8.8.3	技術的ぜい弱性を特定するために、組織は次の事項を考慮する。 b) ソフトウェア及びその他の技術に関して、関連する技術的ぜい弱性を特定し、また、ぜい弱性を継続して認識するために用いる情報源を特定する。情報源のリストは、この目録を変更したとき、又は他の新しい若しくは有益な情報源を発見したときに更新する。	手引に関連記載あり	12.6.1.5	技術的ぜい弱性を特定し、また、それらぜい弱性を継続して認識するために用いる情報資源（ぜい弱性検査ツールなど）を、ソフトウェア及びその他の技術（組織の資産目録リスト[に基づく）に対応させて特定する。
					手引に関連記載あり	12.6.1.6	技術的ぜい弱性の情報資源は、資産目録を変更したとき、又は他の新しい若しくは有益な資源を発見したときに更新を行う。
			8b-8.8.3	技術的ぜい弱性を特定するために、組織は次の事項を考慮する。 c) 情報システム（その構成要素を含む。）の供給者に、適用される契約に要求事項を含め、ぜい弱性の報告、取扱い及び開示を確実にすることを要求する。	手引に関連記載あり	–	（対応項なし）
				技術的ぜい弱性を特定するために、組織は次の事項を考慮する。 d) ぜい弱性を特定し、ぜい弱性のパッチ適用が成功したかどうかを検証するために、使用している技術に適した ぜい弱性スキャンツールを使用する。	手引に関連記載あり	–	（対応項なし）
			8b-8.8.3	技術的ぜい弱性を特定するために、組織は次の事項を考慮する。 e) ぜい弱性の特定を支援するために、力量が[必]要とされた者が、計画され、文書化された、再現可能な侵入テスト又はぜい弱性アセスメントを実施する。この活動はシステムのセキュリティを危うくする可能性があるため、注意を払う。	手引に関連記載あり	18.2.3.3	侵入テスト又は ぜい弱性アセスメントを用いる場合、このような作業は、システムのセキュリティを危うくするかもしれないことに注意する。
					手引に関連記載あり	18.2.3.4	侵入テスト又は ぜい弱性アセスメントは、計画し、文書化し、また、繰り返し実施するだけでなく、新たな ぜい弱性が確認され、報告された場合にも実施する。
					手引に関連記載あり	18.2.3.5	いかなる技術的順守のレビューも、力量があり、認可されている者によって、又はその者の監督の下で行い、実施する。
			8b-8.8.3	技術的ぜい弱性を特定するために、組織は次の事項を考慮する。 f) 第三者のライブラリ[及]びソースコードの使用について、ぜい弱性を追跡する。これはセキュリティに配慮したコーディングに含める。	手引に関連記載あり	–	（対応項なし）
			8b-8.8.9	特定した技術的ぜい弱性を評価するために、次の手引を考慮する。 a) どのような対応及び修復活動が必要かを決定するために、報告書を分析及び検証する。	手引に関連記載あり	–	（対応項なし）
			8b-8.8.9	特定した技術的ぜい弱性を評価するために、次の手引を考慮する。 b) 潜在的な技術的ぜい弱性を特定したときは、それに伴うリスク及び講じるべき処置を特定する。	手引に関連記載あり	12.6.1.8	潜在的な技術的ぜい弱性が特定されたときは、組織は、それと関連するリスク及びとるべき処置（例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用）を特定する。
			（8b-8.8.9参考）	この処置は、ぜい弱性のあるシステムの更新又は他の管理策の適用を含む可能性がある。	手引に関連記載あり	–	（対応項なし）
			8b-8.8.4	組織は、次の事項のための手順及び能力を開発する。 a) 自らの製品及びサービス並[に]これらで使用している外部の構成要素について、ぜい弱性の存在を検知する。 b) 内部又は外部の供給元からぜい弱性報告を受け取る。	手引に関連記載あり	–	（対応項なし）
			8b-8.8.5	組織は、調査者及び他の人が問題を報告できるように、ぜい弱性の開示に関するトピック固有の方針の一部として公開連絡先を示す。	手引に関連記載あり	–	（対応項なし）
			8b-8.8.6	組織は、ぜい弱性の報告手順、オンライン報告書式を確立し、適切な脅威インテリジェンス又は情報共有の場を利用する。	手引に関連記載あり	–	（対応項なし）
			8b-8.8.7	組織は、ぜい弱性を適切に修復するために、組織における ぜい弱性の特定を支援する動機付けとして、報酬を提供するバグ報奨金プログラムの採用を検討する。	手引に関連記載あり	–	（対応項なし）
			8b-8.8.8	組織が力量のある業界団体又は他の利害関係者と情報を共有する。	手引に関連記載あり	–	（対応項なし）
8.8.2	情報システムに関連するぜい弱性への対策を実施する。	必要に応じて、独立した評価機関がソフトウェアの変更を試験し、安当性を確認する。認可された全てのソフトウェアに、最新の承認済みパッチ及びアプリケーション更新を適用することを確実にするために、ソフトウェア更新管理プロセスを実装する。 変更が必要な場合は、元のソフトウェアを保持し、指定された複製に変更を適用する。 全ての変更は、必要に応じて将来のソフトウェアアップグレードに再適用できるように、完全に試験し、文書化する。 技術的ぜい弱性に対処するために、次の手引を考慮する。 a) 潜在的な技術的ぜい弱性の特定に対応して、適切に、かつ、時機を失せずに処置を講じる。関係する可能性のある技術的ぜい弱性の通知に対応するためのタイムラインを定義する。 b) 技術的ぜい弱性への対処の緊急性に応じて、変更管理に関する管理策（8.32参照）又は情報セキュリティインシデント対応手順（5.26参照）に従って、処置を実行する。 c) 正当な供給元（組織の内部又は外部の可能性がある）からの更新だけを使用する。 d) 更新を適用する前に、それが有効であること及び耐えられない副作用をもたらさないことを確実にするために、更新を試験し評価する［すなわち、更新が利用可能な場合、更新の適用に伴うリスクを評価する（ぜい弱性が引き起こすリスクを、更新を適用することのリスクと比較する。）。］。 e) リスクの高いシステムには最初に対処する。 f) 修復（一般にはソフトウェアの更新又は パッチ）を開発する。 g) 修復又は低減策が効果的であるかどうかを確認するために試験する。 h) 修復の真正性を検証する仕組みを提供する。 i) 利用可能な更新がない場合、又は更新を適用できない場合は、次のような他の管理策を検討する。 1) ソフトウェア業者又はその他の関連供給元が提案する回避策を適用する。 2) その ぜい弱性に関係するサービスは機能を停止する。 3) ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する（8.20～8.22参照）。 4) ぜい弱なシステム、装置・機器又はアプリケーションを、適切なトラフィックフィルタ（とAt仮想パッチ[と呼ばれる。）を導入して攻撃から保護する。 5) 実際の攻撃を検知するために、監視を強化する。 6) その ぜい弱性に対する認識を高める。 取[得]したソフトウェアについて、その業者がソフトウェアのセキュリティ更新に関する情報を定常的にリリース し、更新を自動的に適用する機能を提供している場合、組織は、自動更新を使用するかどうかを決定する。 監査ログは、技術的ぜい弱性管理で行われる全てのステップについて保持する。 技術的ぜい弱性の管理プロセスは、その有効性及び効率性を確実にするために、定常的に監視し、評価する。 技術的ぜい弱性に対する有効な管理プロセスは、インシデント管理活動と整合させる。 これは、ぜい弱性に関するデータをインシデント対応部署に伝達し、インシデントが発生した場合に実施する技術的手順を提供するためである。 組織が第三者のクラウドサービスプロバイダが提供するクラウドサービスを利用する場合、クラウドサービスプロバイダの資源の技術的ぜい弱性管理は、クラウドサービスプロバイダがの実施を確実に行うことを確認する。 クラウドサービスの利用に関する合意には、次を含める。 a) 技術的ぜい弱性管理に対するクラウドサービスプロバイダの責任 b) 技術的ぜい弱性に関するクラウドサービスプロバイダの対応を報告するプロセス（5.23参照） 一部のクラウドサービスの場合には、クラウドサービスプロバイダ及び[クラウドサービスカスタ]マにそれぞれの責任が存在する。例えば、クラウドサービスカスタマは、クラウドサービスにおいて使用する自身の資産のぜい弱性管理に責任がある。	8b-8.8.13	必要に応じて、独立した評価機関がソフトウェアの変更を試験し、安当性を確認する。	手引に関連記載あり	14.2.4.10	パッケージソフトウェアの変更が必要な場合には、変更は、独立した評価機関による試験を受け、正当性を証明する。
			8b-8.8.10	認可された全てのソフトウェアに、最新の承認済みパッチ及び[アプ]リケーション更新を適用することを確実にするために、ソフトウェア更新管理プロセスを実装する。	手引に関連記載あり	14.2.4.8	全ての認可されたソフトウェアに対して最新の承認済みパッチ及び[アプ]リケーションの更新を導入していることを確実にするために、ソフトウェアの更新管理手続を実施する。
			8b-8.8.11	変更が必要な場合は、元のソフトウェアを保持し、指定された複製に変更を適用する。	手引に関連記載あり	14.2.4.7	パッケージソフトウェアの変更が必要な場合、原本のソフトウェア保管し、指定された複製に対して変更を適用する。
			8b-8.8.12	全ての変更は、必要に応じて将来のソフトウェアアップグレードに再適用できるように、完全に試験し、文書化する。	手引に関連記載あり	14.2.4.9	将来のソフトウェア更新において、パッケージソフトウェアの変更を再び適用できるように、全ての変更は、十分に試験し、文書化する。
			8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 a) 潜在的な技術的ぜい弱性の特定に対応して、適切に、かつ、時機を失せずに処置を講じる。関係する可能性のある技術的ぜい弱性の通知に対応するためのタイムラインを定義する。	手引に関連記載あり	12.6.1.2	潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める。
					手引に関連記載あり	12.6.1.7	潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める。
			8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 b) 技術的ぜい弱性への対処の緊急性に応じて、変更管理に関する管理策又は情報セキュリティインシデント対応手順に従って、処置を実行する。	手引に関連記載あり	12.6.1.9	技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、とるべき処置を実行する。
			8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 c) 正当な供給元（組織の内部又は外部の可能性がある）からの更新だけを使用する。	手引に関連記載あり	12.6.1.10	正当な供給元からパッチを入手できる場合は、そのパッチを適用することに関連したリスク[を]評価する（ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。）。
			8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 d) 更新を適用する前に、それが有効であること及び耐えられない副作用をもたらさないことを確実にするために、更新を試験し、評価する。	手引に関連記載あり	12.6.1.11	パッチの適用前に、それらが有効であること及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価するとともに、利用可能なパッチがない場合は、以下の4点を実施する。 1.そのぜい弱性に関係するサービスは機能を停止する。 2.ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する。 3.実際の攻撃を検知するために、監視を強化する。 4.ぜい弱性に対する認識を高める。
			8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 i) 利用可能な更新がない場合、又は更新を適用できない場合は、次のような他の管理策を検討する。 1) ソフトウェア業者又はその他の関連供給元が提案する回避策を適用する。 2) その ぜい弱性に関係するサービスは機能を停止する。 3) ネットワーク境界におけるアクセス制御を調整又は追加する。 4) ぜい弱なシステム、装置・機器又はアプリケーションを、適切なトラフィックフィルタ（とAc仮想パッチ[と呼ばれる。）を導入して攻撃から保護する。 5) 実際の攻撃を検知するために、監視を強化する。 6) そのぜい弱性に対する認識を高める。	手引に関連記載あり	12.6.1.16	ぜい弱性が特定されていながら適切な対応策がない場合には、その状況に対処するための手順を定める。
			8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 e) リスクの高いシステムには最初に対処する。	手引に関連記載あり	12.6.1.14	技術的ぜい弱性は、リスクの高いシステムには最初に対処する。
			8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 f) 修復（一般にはソフトウェアの更新又はパッチ）を開発する。 g) 修復又は低減策が効果的であるかどうかを確認するために試験する。 h) 修復の真正性を検証する仕組みを提供する。	手引に関連記載あり	–	（対応項なし）
			8b-8.8.15	取[得]したソフトウェアについて、その業者がソフトウェアのセキュリティ更新に関する情報を定常的にリリース し、更新を自動的に適用する機能を提供している場合、組織は、自動更新を使用するかどうかを決定する。	手引に関連記載あり	–	（対応項なし）
			8b-8.8.16	監査ログは、技術的ぜい弱性管理で行われる全てのステップについて保持する。	手引に関連記載あり	12.6.1.12	修正パッチの適用、その他実施した全ての手順について監査ログを保持する。
			8b-8.8.17	技術的ぜい弱性の管理プロセスは、その有効性及び効率性を確実にするために、定常的に監視し評価する。	手引に関連記載あり	12.6.1.13	技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する。
			8b-8.8.18	技術的ぜい弱性に対する有効な管理プロセスは、インシデント管理活動と整合させる。	手引に関連記載あり	12.6.1.15	技術的ぜい弱性に対する有効な管理プロセスは、ぜい弱性に関するデータをインシデント対応部署に伝達し、インシデントが発生した場合に実施する技術的手順を準備するために、インシデント管理活動と整合させ、組織全体にわたってぜい弱性に対処する。
			（8b-8.8.18参考）	これは、ぜい弱性に関するデータをインシデント対応部署に伝達し、インシデントが発生した場合に実施する技術的手順を提供するためである。			
			8b-8.8.19	組織が第三者のクラウドサービスプロバイダが提供するクラウドサービスを利用する場合、クラウドサービスプロバイダの資源の技術的ぜい弱性管理は、クラウドサービスプロバイダがの実施を確実に行うことを確認する。	手引に関連記載あり	–	（対応項なし）
			8b-8.8.20	クラウドサービスの利用に関する合意には、次を含める。 a) 技術的ぜい弱性管理に対するクラウドサービスプロバイダの責任 b) 技術的ぜい弱性に関するクラウドサービスプロバイダの対応を報告する	手引に関連記載あり	–	（対応項なし）
			（8b-8.8.20参考）	一部のクラウドサービスの場合には、クラウドサービスプロバイダ及び[クラウドサービスカスタ]マにそれぞれの責任が存在する。例えば、クラウドサービスカスタマは、クラウドサービスにおいて使用する自身の資産のぜい弱性管理に責任がある。	手引に関連記載あり	–	（対応項なし）
8.8.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.9	構成管理 統制目標：ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティ構成を含む構成を確立し、文書化し、実装し、監視し、レビューする。 目的：ハードウェア、ソフトウェア、サービス及びネットワークが、必要とされるセキュリティ設定で正しく機能し、認可されていない変更又は誤った変更によって構成が変えられないことを確実にするため。		8.9	構成管理 管理策 ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティ構成を含む構成を確立し、文書化し、実装し、監視し、レビューすることが望ましい。 目的 ハードウェア、ソフトウェア、サービス及びネットワークが、必要とされるセキュリティ設定で正しく機能し、認可されていない変更又は誤った変更によって構成が変えられないことを確実にするため。		–	（対応項なし）
8.9.1	ハードウェア、ソフトウェア、サービス及びネットワークに関して、定義した構成を維持するプロセスの整備及びツールを定義し、実装する。	組織は、ハードウェア、ソフトウェア、サービス（例えば、クラウドサービス）及びネットワークに関して、新しく導入したシステム及び運用システムの存続期間にわたって、定義した構成（セキュリティ構成を含む。）を維持するためのプロセス及びツールを定義し、実装する。 全ての構成変更を良好に管理することを確実にするために、役割、責任及び手順を定める。 ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保つた構成のための標準テンプレートを次のように定義する。 a) 公開され、入手できる手引（例えば、業界及び独立したセキュリティ組織による認定のテンプレート）を使用する。 b) 十分なセキュリティレベルを決定するために、必要な保護のレベルを考慮する。 c) 組織の情報セキュリティ方針、トピック固有の方針、標準及びその他のセキュリティ要求事項を支援する。 d) 組織の状況において、セキュリティ構成の実現可能性及び適用可能性を考慮する。 ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保つた構成の標準テンプレートは、定期的にレビューすることに加えて、新しい脅威又はぜい弱性に対処する必要がある場合、又は新版のソフトウェア若しくはハードウェアを導入した場合に更新する。 ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保つた構成の標準テンプレートの策定に当たって、次の事項を考慮する。 a) 特権的又は実務管理者レベルのアクセス権をもつ識別情報の数を最小限にする。 b) 不必要な、使用されていない又はセキュリティが保たれていない識別情報を無効化する。 c) 不必要な機能及びサービスを無効化又は制限する。 d) 強力なユーティリティプログラム及び/又はストラバータ設定へのアクセスを制限する。 e) クロックを同期させる。 f) 初期パスワードなどの業者による初期認証情報を導入の直後に変更し、その他の重要なセキュリティ関連パラメータの初期状態をレビューする。 g) 既定の使用中断時間の後に、コンピューティング装置・機器から自動的にログオフするタイムアウト機能を作動させる。 h) 使用許諾の要求事項が満たされていることを検証する（5.32参照）。 ハードウェア、ソフトウェア、サービス及びネットワークについて決定した構成を記録し、全ての構成変更のログを維持する。これらの記録はセキュリティを保って保管する。これは、構成データベース又は構成テンプレートなど様々な方法で達成することが可能である。構成の変更は、変更管理プロセスに従う（8.32参照）。構成記録には、次の事項を含み得る。 a) 資産の最新の管理責任者又は連絡先情報 b) 構成の最終変更日 c) 構成テンプレートの版 d) その他の資産の構成との関係	8b-8.9.1	組織は、ハードウェア、ソフトウェア、サービス及びネットワークに関して、新しく導入したシステム及び運用システムの存続期間にわたって、定義した構成（セキュリティ構成を含む。）を維持するためのプロセス及びツールを定義し、実装する。	手引に関連記載あり	–	（対応項なし）
			8b-8.9.2	全ての構成変更を良好に管理することを確実にするために、役割、責任及び手順を定める。	手引に関連記載あり	–	（対応項なし）
			8b-8.9.3	ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保つた構成のための標準テンプレートを次のように定義する。 a) 公開され、入手できる手引を使用する。 b) 十分なセキュリティレベルを決定するために、必要な保護のレベルを考慮する。 c) 組織の情報セキュリティ方針、トピック固有の方針、標準及びその他のセキュリティ要求事項を支援する。 d) 組織の状況において、セキュリティ構成の実現可能性及び適用可能性を考慮する。	手引に関連記載あり	14.1.1.15	当該システムにおいて稼働するソフトウェア及びサービスと整合する製品のセキュリティ構成に関して、入手可能な手引を用いて、これを評価し、実施する。
			8b-8.9.4	ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保つた構成の標準テンプレートは、定期的にレビューすることに加えて、新しい脅威又はぜい弱性に対処する必要がある場合、又は新版のソフトウェア若しくはハードウェアを導入した場合に更新する。	手引に関連記載あり	–	（対応項なし）
			8b-8.9.5	ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保つた構成の標準テンプレートの策定に当たって、次の事項を考慮する。 a) 特権的又は実務管理者レベルのアクセス権をもつ識別情報の数を最小限にする。 b) 不必要な、使用されていない又はセキュリティが保たれていない識別情報を無効化する。 c) 不必要な機能及びサービスを無効化又は制限する。 d) 強力なユーティリティプログラム及び/又はストラバータ設定へのアクセスを制限する。 e) クロックを同期させる。 f) 初期パスワードなどの業者による初期認証情報を導入の直後に変更し、その他の重要なセキュリティ関連パラメータの初期状態をレビューする。 g) 既定の使用中断時間の後に、コンピューティング装置・機器から自動的にログオフするタイムアウト機能を作動させる。 h) 使用許諾の要求事項が満たされていることを検証する。	手引に関連記載あり	–	（対応項なし）
			8b-8.9.6	ハードウェア、ソフトウェア、サービス及びネットワークについて決定した構成を記録し、全ての構成変更のログを維持する。これらの記録はセキュリティを保って保管する。	手引に関連記載あり	–	（対応項なし）
			（8b-8.9.6参考1）	これは、構成データベース又は構成テンプレートなど様々な方法で達成することが可能である。	手引に関連記載あり	–	（対応項なし）
			（8b-8.9.6参考2）	構成の変更は、変更管理プロセスに従う。	手引に関連記載あり	–	（対応項なし）
			（8b-8.9.6参考3）	構成記録には、次の事項を含み得る。 a) 資産の最新の管理責任者又は連絡先情報 b) 構成の最終変更日 c) 構成テンプレートの版 d) その他の資産の構成との関係	手引に関連記載あり	–	（対応項なし）
8.9.2	構成を監視し、定期的にレビューする。	構成は、包括的なシステム管理ツール群（例えば、保守ユーティリティ、遠隔サポート、エンタープライズ管理ツール、パッケージ及び/又はアプリケーション）を用いて監視する。 構成設定を検証し、パスワードの強度を評価し、また、実施する活動を評価するために、定期的にレビューする。	8b-8.9.7	構成は、包括的なシステム管理ツール群を用いて監視する。	手引に関連記載あり	–	（対応項なし）
			8b-8.9.8	構成設定を検証し、パスワードの強度を評価し、また、実施する活動を評価するために、定期的にレビューする。	手引に関連記載あり	–	（対応項なし）
8.9.3	定期的なレビューの結果、逸脱を検知した場合には是正処置を実施する。	実際の構成を、定義した目標テンプレートと比較することが可能である。逸脱には、定義した目標構成を自動適用して、又は逸脱を手動で分析し、是正処置を講じて対処する。	8b-8.9.9	実際の構成を、定義した目標テンプレートと比較することが可能である。逸脱には、定義した目標構成を自動適用して、又は逸脱を手動で分析し、是正処置を講じて対処する。	手引に関連記載あり	–	（対応項なし）
8.10	情報の削除 統制目標：情報システム、装置又はその他の記憶媒体に保存している情報は、必要でなくなった時点で削除する。 目的：取扱いに慎重を要する情報の不用意な漏えいを防止し、情報の削除に関する法令、規制及び契約上の要求事項を順守するため。		8.10	情報の削除 管理策 情報システム、装置又はその他の記憶媒体に保存している情報は、必要でなくなった時点で削除することが望ましい。 目的 取扱いに慎重を要する情報の不用意な漏えいを防止し、情報の削除に関する法令、規制及び契約上の要求事項を順守するため。		–	（対応項なし）
8.10.1	情報システム、装置又はその他の記憶媒体に保存している情報は、時期を失せずに削除する。	取扱いに慎重を要する情報は、望ましくない開示のリスクを減らすために、必要な期間より長く保持しない。 システム、アプリケーション及びサービスに関する情報を削除する場合は、次の事項を考慮する。 a) 業務の要求事項に従い、また、関連する法令及び規制を考慮して、削除手法（例えば、電子的な上書き又は暗号化消去）を選択する。 b) 削除の結果を証拠として記録する（情報の削除の正式記録は、生じる情報漏えい事象の原因を分析するために役立つ。）。 c) 情報の削除を行うサービス提供者を利用する場合、サービス提供者から情報の削除の証拠を得る。 第三者が組織に代わってその情報を保存する場合、組織は、情報の削除に関する要求事項を第三者との合意に含め、サービスの実施中及び終了時に実行させることを検討する。 組織のデータ保持に関するトピック固有の方針に従い、また、関連する法令及び規制を考慮して、取扱いに慎重を要する情報は、必要がなくなったとき、次の方法で削除する。 a) 必要でなくなったとき、情報をセキュリティを保って破壊するようにシステムを構成する（例えば、データ保持に関するトピック固有の方針に従って定義した期間の後に、又は対象のアクセス要求に応じて）。 b) 古い版、複製及び一時ファイルは、それらがどこにあっても削除する。 c) 情報を恒久的に削除し、専門家が使う復旧ツール又はフォレンジックツールを使用しても情報が復旧できないことを確実にする助けとするために、広く認められた、セキュリティを保つた削除ソフトウェアを使用する。 d) 広く認められ、認定された、セキュリティを保つた廃棄サービス提供者を利用する。 e) 処分する記憶媒体の種類に適した処分の仕組みを使用する（例えば、ハードディスクドライブ及びその他の磁気記憶媒体の消磁）。 クラウドサービスを利用する場合、組織はクラウドサービスプロバイダが提供する削除手法が許容できるかどうかを検証し、許容できるならばそれを利用し、又はクラウドサービスプロバイダに情報の削除を要請する。 削除プロセスは、利用可能かつ適用可能な場合には、トピック固有の方針に従って自動化する。削除する情報の、取扱いに慎重を要する度合いに応じて、ログによって、削除プロセスが実行されたことを追跡又は検証することが可能である。 装置・機器を業者に返送するとき、取扱いに慎重を要する情報が意図せず漏えいすることを防止するために、装置・機器を組織の施設から出す前に、補助記憶媒体（例えば、ハードディスクドライブ）及びメモリを取り除くことによって、取扱いに慎重を要する情報を保護する。 組織はその装置・機器で取り扱う情報の分類に従って適切な手法を選択する（一部の装置・機器（例えば、スマートフォン）では、セキュリティを保った情報の削除は、装置・機器の破壊又は装置・機器に組み込まれている機能（例えば、工場出荷時の設定の復元）の使用によってだけ実施可能である。）。 記憶媒体を物理的に破壊し、同時にそこに含む情報を消去するために、7.14に記載する対策を適用する。	8b-8.10.1	取扱いに慎重を要する情報は、望ましくない開示のリスクを減らすために、必要な期間より長く保持しない。	手引に関連記載あり	–	（対応項なし）
			8b-8.10.2	システム、アプリケーション及びサービスに関する情報を削除する場合は、次の事項を考慮する。 a) 業務の要求事項に従い、また、関連する法令及び規制を考慮して、削除手法を選択する。 b) 削除の結果を証拠として記録する。 c) 情報の削除を行うサービス提供者を利用する場合、サービス提供者から情報の削除の証拠を得る。	手引に関連記載あり	–	（対応項なし）
			8b-8.10.3	第三者が組織に代わってその情報を保存する場合、組織は、情報の削除に関する要求事項を第三者との合意に含め、サービスの実施中及び終了時に実行させることを検討する。	手引に関連記載あり	–	（対応項なし）
			8b-8.10.4	組織のデータ保持に関するトピック固有の方針に従い、また、関連する法令及び規制を考慮して、取扱いに慎重を要する情報は、必要がなくなったとき、次の方法で削除する。 a) 必要でなくなったとき、情報をセキュリティを保って破壊するようにシステムを構成する。 b) 古い版、複製及び一時ファイルは、それらがどこにあっても削除する。 c) 情報を恒久的に削除し、専門家が使う復旧ツール又はフォレンジックツールを使用しても情報が復旧できないことを確実にするために、広く認められた、セキュリティを保つた削除ソフトウェアを使用する。 d) 広く認められ、認定された、セキュリティを保つた廃棄サービス提供者を利用する。 e) 処分する記憶媒体の種類に適した処分の仕組みを使用する。	手引に関連記載あり	–	（対応項なし）
			8b-8.10.5	クラウドサービスを利用する場合、組織はクラウドサービスプロバイダが提供する削除手法が許容できるかどうかを検証し、許容できるならばそれを利用し、又はクラウドサービスプロバイダに情報の削除を要請する。	手引に関連記載あり	–	（対応項なし）
			8b-8.10.6	削除プロセスは、利用可能かつ適用可能な場合には、トピック固有の方針に従って自動化する。	手引に関連記載あり	–	（対応項なし）
			8b-8.10.7	装置・機器を業者に返送するとき、取扱いに慎重を要する情報が意図せず漏えいすることを防止するために、装置・機器を組織の施設から出す前に、補助記憶媒体及びメモリを取り除くことによって、取扱いに慎重を要する情報を保護する。	手引に関連記載あり	–	（対応項なし）
			8b-8.10.8	組織はその装置・機器で取り扱う情報の分類に従って適切な手法を選択する。	手引に関連記載あり	–	（対応項なし）
			8b-8.10.9	記憶装置を物理的に破壊し、同時にそこに含む情報を消去するために、7b-7.14にある対策を適用する。	手引に関連記載あり	–	（対応項なし）
8.11	データマスキング 統制目標：データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有の方針及びその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用する。 目的：PIIを含む、取扱いに慎重を要するデータの開示を制限し、法令、規制及び契約上の要求事項を順守するため。		8.11	データマスキング 管理策 データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有の方針及びその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用することが望ましい。 目的 PIIを含む、取扱いに慎重を要するデータの開示を制限し、法令、規制及び契約上の要求事項を順守するため。		–	（対応項なし）
8.11.1	適用される法令や事業上の要求事項に従い、データマスキングの要件及び手法を特定する。	取扱いに慎重を要するデータ（例えば、PII）の保護が必要である場合、組織はデータマスキング、仮名化、匿名化又は含むデータマスキングの手法（データマスキング手法という。）を利用してそのデータを隠すことを検討する。 仮名化又は匿名化の手法では、次のことが可能である。 a) PIIのデータを隠する。 b) PII主体の真のアイデンティティ又はその他の取扱いに慎重を要する情報を偽装する。 c) PIIとPII主体のアイデンティティとの間のひも（紐）付けを他の取扱いに慎重を要する情報との間のひも（紐）付けを切る。 仮名化又は匿名化の手法を利用する場合、データが十分に仮名化又は匿名化されていることを検証する。 データの匿名化では、取扱いに慎重を要する情報の全ての要素に対して有効とするように考慮する。データの匿名化が適切に考慮されていない場合、ある人物が直接識別できるデータが匿名化されていても、間接的に識別を可能とする別のデータが存在して、その人物が識別できる場合がある。 データマスキング手法には、仮名化、匿名化のほかに、次を含む手法を考慮する。 a) データを暗号化する。 b) 文字をスルイ化又は消去する。 c) 数及び日付を変える。 d) 取扱いに慎重を要するデータのうち特定の値を別の値に置き換える。 e) 値そのハッシュ値に置き換える。	8b-8.11.1	取扱いに慎重を要するデータの保護が必要である場合、組織は仮名化、匿名化などを含むデータマスキングの手法を利用してそのデータを隠すことを検討する。	手引に関連記載あり	–	（対応項なし）
			8b-8.11.2	仮名化又は匿名化の手法を利用する場合、データが十分に仮名化又は匿名化されていることを検証する。	手引に関連記載あり	–	（対応項なし）
			8b-8.11.3	データの匿名化では、取扱いに慎重を要する情報の全ての要素に対して有効とするように考慮する。	手引に関連記載あり	–	（対応項なし）
			8b-8.11.4	データマスキング手法には、仮名化、匿名化のほかに、次を含む手法を考慮する。 a) データを暗号化する。 b) 文字をスルイ化又は消去する。 c) 数及び日付を変える。 d) 取扱いに慎重を要するデータのうち特定の値を別の値に置き換える。 e) 値そのハッシュ値に置き換える。	手引に関連記載あり	–	（対応項なし）
8.11.2	特定したデータマスキング手法を実装する。	データマスキング手法を実装する場合、次の事項を考慮する。 a) 利用者に必要最小限のデータだけを示すように照合せ（クエリ）及びマスクを設計する。 b) データセットの一部の記録に関して、利用者に一部のデータを見せないことが望ましい場合、データを難読化する仕組みを設計し、実装する（例えば、緊急の場合であっても、患者が自らの記録の全てを病院スタッフが見ることができることを望まない場合、病院スタッフには部分的に難読化したデータを提示し、そのデータが適切な治療に有用な情報を含む場合は、特定の役割をもつスタッフだけがアクセスできるようにする。）。 c) データを難読化する場合、データを難読化しているかどうかを利用者が知ることができないこと。PII主体が要求できるようにする（難読化の難読化。これは医療機器の利用され、例えば、血液検査の結果などの取扱いに慎重を要する情報が難読化されていることを、患者が意図に知られてしない場合などである。）。 d) 法令又は規制上の要求事項（例えば、処理中又は保管中に、支払いカードの情報をマスキングすることを要求する。）。 データマスキング、仮名化又は匿名化を利用する場合、次の事項を考慮する。 a) 処理するデータの使用法に応じた、データマスキング、仮名化又は匿名化の強度のレベル b) 処理するデータへのアクセス制御 c) 処理するデータの使用法に関する合意又は制限 d) PII主体を識別するために、処理するデータ他の情報と照合することの禁止 e) 処理するデータの提供及び受領の追跡	8b-8.11.5	データマスキング手法を実装する場合、次の事項を考慮する。 a) 利用者に必要最小限のデータだけを示すように照合せ（クエリ）及びマスクを設計する。 b) データセットの一部の記録に関して、利用者に一部のデータを見せないことが望ましい場合、データを難読化する仕組みを設計し、実装する。 c) データを難読化する場合、データを難読化しているかどうかを利用者が知ることができないこと を、PII主体が要求できるようにする。 d) 法令又は規制上の要求事項。	手引に関連記載あり	–	（対応項なし）
			8b-8.11.6	データマスキング、仮名化又は匿名化を利用する場合、次の事項を考慮する。 a) 処理するデータの使用法に応じた、データマスキング、仮名化又は匿名化の強度のレベル b) 処理するデータへのアクセス制御 c) 処理するデータの使用法に関する合意又は制限 d) PII主体を識別するために、処理するデータ他の情報と照合することの禁止 e) 処理するデータの提供及び受領の追跡	手引に関連記載あり	–	（対応項なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.12	データ漏えい防止 統制目標：データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存又は送信するシステム、ネットワーク及びその他の装置に適用する。 目的：個人又はシステムによる情報の認可されていない開示及び抽出を検出し、防止するため。		8.12	データ漏えい防止 管理策 データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存又は送信するシステム、ネットワーク及びその他の装置に適用することが望ましい。 目的 個人又はシステムによる情報の認可されていない開示及び抽出を検出し、防止するため。		–	（対応項なし）
8.12.1	データ漏えいのリスクへの対策を実施する。	組織は、データ漏えいのリスクを減らすために、次の事項を考慮する。 a）漏えいから保護する情報（例えば、個人情報、機微設定モデル及び製品設計）の特定及び分類 b）データ漏えいの経路・手段の監視（例えば、電子メール、ファイル転送、モバイル機器及び可搬記憶装置） c）情報の漏えいを防止するための処置（例えば、取扱いに慎重を要する情報を含むメールの検疫） データ漏えい防止ツールを、次の目的で使用する。 a）認可されていない開示のリスクがある取扱いに慎重を要する情報を特定し、監視する（例えば、利用者のシステム上の整理されていない情報）。 b）取扱いに慎重を要する情報の開示を検出する（例えば、信頼できない第三者のクラウドサービスに情報がアップロードされた場合、又は電子メールで送信された場合にこれらを検出する。）。 c）取扱いに慎重を要する情報を漏えいする利用者の行為又はネットワーク送信を阻止する（例えば、データベースエントリのスプレッドシートへのコピーを防止する。）。 組織は、組織の外部のサービス、装置・機器及び記憶媒体にデータをコピーして貼り付ける、又はアップロードする利用者の権限を制限する必要があるかどうかを判断する。 組織の管理外にデータをコピーして貼り付ける、又はアップロードする利用者の権限を制限する場合、データ漏えい防止ツール又は既存のツールの組合せなどの技術を導入する。 データの取り出しが必要な場合、利用者による取り出しを許可し、利用者に自らの行動にアカウンタビリティをもたせる役割を、データの管理責任者に与える。 画面のスクリーンショット又は写真を撮ることには、利用条件、訓練及び監査によって対応する。 データをバックアップする場合、暗号化、アクセス制御及びバックアップを保持する記憶媒体の物理的保護などの対策を使用して、取扱いに慎重を要する情報の保護を確実にする。 データ漏えい防止は、ちょう（諜）報活動の対象となる可能性がある、又はコミュニティにとって重要な可能性がある（地政学、人、財務、商取引、科学又はその他に関する）秘密情報を敵対者が情報収集活動によって取得することに対する保護も考慮する。 データ漏えい防止活動は、独立の活動又は敵対者の情報収集活動への対応のいずれかとして、敵対者の決定を混乱させる方策（真正の情報を偽の情報に置き換えることによる、リバースソーシャルエンジニアリング又は攻撃者を引き付けるハニーポットの使用がある。）も講じる。	8b-8.12.1	組織は、データ漏えいのリスクを減らすために、次の事項を考慮する。 a）漏えいから保護する情報の特定及び分類 b）データ漏えいの経路・手段の監視 c）情報の漏えいを防止するための処置	手引に関連記載あり	–	（対応項なし）
			8b-8.12.2	データ漏えい防止ツールを、次の目的で使用する。 a）認可されていない開示のリスクがある取扱いに慎重を要する情報を特定し、監視する。 b）取扱いに慎重を要する情報の開示を検出する。 c）取扱いに慎重を要する情報を漏えいする利用者の行為又はネットワーク送信を阻止する。	手引に関連記載あり	–	（対応項なし）
			8b-8.12.3	組織は、組織の外部のサービス、装置・機器及び記憶媒体にデータをコピーして貼り付ける、又はアップロードする利用者の権限を制限する必要があるかどうかを判断する。	手引に関連記載あり	–	（対応項なし）
			8b-8.12.4	組織の管理外にデータをコピーして貼り付ける、又はアップロードする利用者の権限を制限する場合、データ漏えい防止ツール又は既存のツールの組合せなどの技術を導入する。	手引に関連記載あり	–	（対応項なし）
			8b-8.12.5	データの取り出しが必要な場合、利用者による取り出しを許可し、利用者に自らの行動にアカウンタビリティをもたせる役割を、データの管理責任者に与える。	手引に関連記載あり	–	（対応項なし）
			8b-8.12.6	画面のスクリーンショット又は写真を撮ることには、利用条件、訓練及び監査によって対応する。	手引に関連記載あり	–	（対応項なし）
			8b-8.12.7	データをバックアップする場合、暗号化、アクセス制御及びバックアップを保持する記憶媒体の物理的保護などの対策を使用して、取扱いに慎重を要する情報の保護を確実にする。	手引に関連記載あり	–	（対応項なし）
			8b-8.12.8	データ漏えい防止は、ちょう報活動の対象となる可能性がある、又はコミュニティにとって重要な可能性がある秘密情報を敵対者が情報収集活動によって取得することに対する保護も考慮する。	手引に関連記載あり	–	（対応項なし）
			8b-8.12.9	データ漏えい防止活動は、独立の活動又は敵対者の情報収集活動への対応のいずれかとして、敵対者の決定を混乱させる方策も講じる。	手引に関連記載あり	–	（対応項なし）
8.13	情報のバックアップ 統制目標：合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェア及びシステムのバックアップを維持し、定期的に検査する。 目的：データ又はシステムの損失からの回復を可能にするため。		8.13	情報のバックアップ 管理策 合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェア及びシステムのバックアップを維持し、定期的に検査する。 目的 データ又はシステムの損失からの回復を可能にするため。		12.3 12.3.1	バックアップ 管理目的：データの消失から保護するため。 情報のバックアップ 情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査する。
8.13.1	組織のデータ保持及び情報セキュリティの要求事項に対応するために、バックアップに関する方針を策定する。	組織のデータ保持及び情報セキュリティの要求事項に対応するために、バックアップに関するトピック固有の方針を確立する。 インシデント又は記憶媒体の故障若しくは損失の後に、全ての重要な情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備える。 重要なシステム及びサービスに関するバックアップ対策は、災害に際してシステム全体を復旧させるために必要となる、システム情報、アプリケーション及びデータの全てを対象とする。 組織はクラウドサービスを利用する場合、クラウドサービス環境にある組織の情報、アプリケーション及びシステムのバックアップ情報を作成する。 組織は、クラウドサービスの一部として提供される情報バックアップサービスを利用する場合、バックアップの要求事項が満たされるかどうか、また、どのように満たされるかを特定する。 重要な業務情報の保持期間は、複製の保存に関するあゆる要求事項を考慮に入れて、決定する。 組織は、情報の保持期間が終了したら、バックアップに使用している記憶媒体にある情報の消除（8.10参照）、また、法令及び規制を考慮する。	8b-8.13.1	組織のデータ保持及び情報セキュリティの要求事項に対応するために、バックアップに関するトピック固有の方針を確立する。	手引に関連記載あり	12.3.1.1	バックアップ方針を確立し、情報、ソフトウェア及びシステムイメージのバックアップに関する組織の要求事項を定める。
			8b-8.13.2	インシデント又は記憶媒体の故障若しくは損失の後に、全ての重要な情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備える。	手引に関連記載あり	12.3.1.3	災害又は媒体故障の発生の後に、全ての重要な情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備える。
			8b-8.13.8	重要なシステム及びサービスに関するバックアップ対策は、災害に際してシステム全体を復旧させるために必要となる、システム情報、アプリケーション及びデータの全てを対象とする。	手引に関連記載あり	12.3.1.14	重要なシステム及びサービスに関するバックアップの取決めは、災害に際してシステム全体を復旧させるために必要となる、システム情報、アプリケーション及びデータの全てを対象とする。
			8b-8.13.9	組織はクラウドサービスを利用する場合、クラウドサービス環境にある組織の情報、アプリケーション及びシステムのバックアップ情報を作成する。	手引に関連記載あり	–	（対応項なし）
			8b-8.13.10	組織は、クラウドサービスの一部として提供されるバックアップサービスを利用する場合、バックアップの要求事項が満たされるかどうか、また、どのように満たされるかを特定する。	手引に関連記載あり	–	（対応項なし）
			8b-8.13.11	重要な業務情報の保持期間は、複製の保存に関するあゆる要求事項を考慮に入れて、決定する。	手引に関連記載あり	12.3.1.15	永久保存する複製物に関するあゆる要求事項を考慮に入れて、不可欠な業務情報の保管期間を決定する。
			8b-8.13.12	組織は、情報の保持期間が終了したら、バックアップに使用している記憶媒体にある情報の消除、また、法令及び規制を考慮する。	手引に関連記載あり	–	（対応項なし）
8.13.2	バックアップ計画を策定し、実装する。	バックアップに関するトピック固有の方針に対応するため、組織は、情報、ソフトウェア及びシステムをバックアップする方法について計画を作成し、実装する。 バックアップ計画を策定するときは、次の事項を考慮に入れる。 a）バックアップ情報の正確かつ完全な記録及び文書化したデータ復旧手順を作成する。 b）バックアップの範囲（例えば、フルバックアップ、差分バックアップ）、及びバックアップの頻度は、組織の事業上の要求事項（例えば、目標復旧時点、5.30参照）、関係する情報のセキュリティ要求事項、及びその情報の組織の継続的な運用に対する重要度を考慮して決定する。 c）バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた安全でセキュリティを保った場所に保管する。 d）バックアップ情報に対して、主事業所に適用されている標準と整合した、適切なレベルの物理的及び環境的保護（盗難及び5.1参照）を実施する。 e）バックアップに用いる媒体は、必要になった場合の緊急利用について信頼できることを確実にするために、定期的に試験する。バックアップデータで復旧する機能のテストは、バックアップ又はデータ復旧プロセスに失敗して、データに修復不能な損傷又は損失が生じることがないように、テストシステム上で行い、原本の記憶媒体に上書きしない。 f）特定したリスクに応じて、暗号化によってバックアップ情報を保護する（例えば、機密性が重要な状況において）。 g）バックアップを作成する前に、不注意によるデータ損失の検出を確実にするように注意する。	8b-8.13.3	バックアップに関するトピック固有の方針に対応するため、組織は、情報、ソフトウェア及びシステムをバックアップする方法について計画を作成し、実装する。	手引に関連記載あり	–	（対応項なし）
			8b-8.13.4	バックアップ計画を策定するときは、次の事項を考慮に入れる。 a）バックアップ情報の正確かつ完全な記録及び文書化したデータ復旧手順を作成する。	手引に関連記載あり	12.3.1.4	バックアップ情報の正確かつ完全な記録及び文書化したデータ復旧手順を作成する。
			8b-8.13.4	バックアップ計画を策定するときは、次の事項を考慮に入れる。 b）バックアップの範囲、及びバックアップの頻度は、組織の事業上の要求事項、関係する情報のセキュリティ要求事項、及びその情報の組織の継続的な運用に対する重要度を考慮して決定する。	手引に関連記載あり	12.3.1.5	バックアップの範囲（例えば、フルバックアップ、差分バックアップ）、及びバックアップの頻度は、組織の業務上の要求事項、関連する情報のセキュリティ要求事項、及びその情報の組織の事業継続に対しての重要度を考慮して決定する。
			8b-8.13.4	バックアップ計画を策定するときは、次の事項を考慮に入れる。 c）バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた安全でセキュリティを保った場所に保管する。	手引に関連記載あり	12.3.1.6	バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた場所に保管する。
			8b-8.13.4	バックアップ計画を策定するときは、次の事項を考慮に入れる。 d）バックアップ情報に対して、主事業所に適用されている標準と整合した、適切なレベルの物理的及び環境的保護を実施する。	手引に関連記載あり	12.3.1.7	バックアップ情報に対して、主事業所に適用されている標準と整合した、適切なレベルの物理的及び環境的保護を実施する。
			8b-8.13.4	バックアップ計画を策定するときは、次の事項を考慮に入れる。 e）バックアップに用いる媒体は、必要になった場合の緊急利用について信頼できることを確実にするために、定期的に試験する。バックアップデータで復旧する機能のテストは、バックアップ又はデータ復旧プロセスに失敗して、データに修復不能な損傷又は損失が生じることがないように、テストシステム上で行い、原本の記憶媒体に上書きしない。	手引に関連記載あり	12.3.1.8	バックアップに用いる媒体は、必要になった場合の緊急利用について信頼できることを確実にするために、定めに従って試験する。
					手引に関連記載あり	12.3.1.9	バックアップに用いる媒体の試験は、データ復旧手順の試験と併せて行い、必要なデータ復旧時間に照らし合わせて確認する。
					手引に関連記載あり	12.3.1.10	バックアップデータを復旧させる能力の試験は、バックアップ手順又はデータ復旧プロセスに失敗し、データに修復不能な損傷又は損失が発生した場合に備えて、原本の媒体とは書きするのではなく、専用の試験媒体を用いて行う。
			8b-8.13.4	バックアップ計画を策定するときは、次の事項を考慮に入れる。 f）特定したリスクに応じて、暗号化によってバックアップ情報を保護する。	手引に関連記載あり	12.3.1.11	機密性が重要な場合には、暗号化によってバックアップ情報を保護する。
			8b-8.13.4	バックアップ計画を策定するときは、次の事項を考慮に入れる。 g）バックアップを作成する前に、不注意によるデータ損失の検出を確実にするように注意する。	手引に関連記載あり	–	（対応項なし）
8.13.3	バックアップの実行を監視し、失敗した場合は適切に対処する。	バックアップの運用手順では、バックアップに関するトピック固有の方針に従って、バックアップの完全性を確保するために、その実行を監視し、計画したバックアップの失敗に対処する。	8b-8.13.5	バックアップの運用手順では、バックアップに関するトピック固有の方針に従って、バックアップの完全性を確保するために、その実行を監視し、計画したバックアップの失敗に対処する。	手引に関連記載あり	12.3.1.12	運用手順では、バックアップ方針に従って、バックアップの完全性を確保するために、その実行を監視し、計画されたバックアップの失敗に対処する。
8.13.4	個々のシステム及びサービスに関するバックアップ対策は、インシデント対応及び事業継続計画の目的を満たすことを確実にするために、定期的に試験する。	個々のシステム及びサービスに関するバックアップ対策は、インシデント対応及び事業継続計画の目的を満たすことを確実にするために、定期的に試験する（5.30参照）。 定期的な試験は、これを復旧手順のテストと組み合わせて、事業継続計画において必要とされる復旧時間に照らして確認する。	8b-8.13.6	個々のシステム及びサービスに関するバックアップ対策は、インシデント対応及び事業継続計画の目的を満たすことを確実にするために、定期的に試験する。	手引に関連記載あり	12.3.1.13	個々のシステム及びサービスに関するバックアップの取決めは、事業継続計画の要求事項を満たすことを確実にするために、定めに従って試験する。
			8b-8.13.7	定期的な試験は、これを復旧手順のテストと組み合わせて、事業継続計画において必要とされる復旧時間に照らして確認する。	手引に関連記載あり	–	（対応項なし）
8.13.5	クラウドサービス利用者に対し、当該利用者の資産（バックアップを含む）を管理するため、次のいずれかを提供する。 a）当該利用者の管理する資産を、記録媒体に記録する（バックアップを含む）前に暗号化し、当該利用者が暗号鍵を管理し消去する機能 b）当該利用者が、当該利用者の管理する資産を記録媒体に記録する（バックアップを含む）前に暗号化し、暗号鍵を管理し消去する機能を実装するために必要となる情報	特になし。	–	（統一基準由来）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	8.1.2.7.PB	クラウドサービス事業者は、クラウドサービス利用者に対し、当該利用者の資産（バックアップを含む）を管理するため、次のいずれかを提供する。 (a)当該利用者の管理する資産を、記録媒体に記録する（バックアップを含む）前に暗号化し、当該利用者が暗号鍵を管理し消去する機能 (b) 当該利用者が、当該利用者の管理する資産を記録媒体に記録する（バックアップを含む）前に暗号化し、暗号鍵を管理し消去する機能を実装するために必要となる情報
8.13.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
8.13.7	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.14	情報処理施設・設備の冗長性 統制目標：情報処理施設・設備は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。 目的：情報処理施設・設備の継続的な運用を確実にするため。		8.14	情報処理施設・設備の冗長性 管理策 情報処理施設・設備は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。 目的 情報処理施設・設備の継続的な運用を確実にするため。		17.2	冗長性 管理目的：情報処理施設の可用性を確実にするため。
						17.2.1	情報処理施設の可用性 情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。
8.14.1	業務上のサービス及び情報システムの可用性に関する要求事項を定義し、この要求事項を満たすために、適切な冗長性をもってシステムアーキテクチャを設計し、実装する。	組織は、業務上のサービス及び情報システムの可用性に関する要求事項を特定する。 組織は、この要求事項を満たすために、適切な冗長性をもってシステムアーキテクチャを設計し、実装する。 組織は、冗長な構成要素及び情報処理施設・設備を作動させる手順を計画し、実装する。冗長性は、情報処理施設・設備の一部又は全体を二重化させる（予備の構成要素をもつか、又は二つの全ての要素をもつ。）ことによって導入することが可能である。 冗長な構成要素及び処理施設・設備を作動させる手順では、冗長な構成要素及び処理活動を常に作動させておくか、又は緊急の場合に自動若しくは手動で作動させるかを定める。 冗長な構成要素及び情報処理施設・設備は、主たる構成要素及び情報処理施設・設備と同じセキュリティレベルをもつことを確実にする。 情報処理施設・設備の故障を組織に警告し、計画した手順を実行できるように、情報処理施設・設備を修理又は交換している間も、継続して可用性の維持を可能とする仕組みを設ける。 組織は、冗長システムを実装する場合、次の事項を考慮する。 a) インターネットサービス提供者など、ネットワーク及び重要な情報処理施設・設備の供給者、二者以上と契約する。 b) 冗長性のあるネットワークを使用する。 c) 冗長構成をとったシステムをもつ地理的に離れた二つのデータセンターを使用する。 d) 物理的に冗長性のある電力供給装置又は電源を使用する。 e) ソフトウェア構成要素の複数の並列インスタンスを、同じデータセンター内又は異なるデータセンターのインスタンス間で自動負荷分散によって使用する。 f) システムにおいて二重化した構成要素（例えば、CPU、ハードディスク、メモリ）をもつ、又はネットワークにおいて二重化した構成要素（例えば、ファイアウォール、ルーター、スイッチ）をもつ。	8b-8.14.1	組織は、業務上のサービス及び情報システムの可用性に関する要求事項を特定する。	手引に関連記載あり	17.2.1.1	組織は、情報システムの可用性に関する業務上の要求事項を特定する。
			8b-8.14.2	組織は、可用性の要求事項を満たすために、適切な冗長性をもってシステムアーキテクチャを設計し、実装する。	手引に関連記載あり	17.2.1.2	組織は、既存のシステムアーキテクチャを利用しても可用性を保証できない場合には、冗長な構成要素又はアーキテクチャを構築する。
			8b-8.14.3	組織は、冗長な構成要素及び情報処理施設・設備を作動させる手順を計画し、実装する。	手引に関連記載あり	–	（対応項なし）
			（8b-8.14.3参考）	冗長性は、情報処理施設・設備の一部又は全体を二重化させることによって導入することが可能である。	手引に関連記載あり	–	（対応項なし）
			8b-8.14.4	冗長な構成要素及び情報処理施設・設備を作動させる手順では、冗長な構成要素及び処理活動を常に作動させておくか、又は緊急の場合に自動若しくは手動で作動させるかを定める。	手引に関連記載あり	–	（対応項なし）
			8b-8.14.5	冗長な構成要素及び情報処理施設・設備は、主たる構成要素及び情報処理施設・設備と同じセキュリティレベルをもつことを確実にする。	手引に関連記載あり	–	（対応項なし）
			8b-8.14.6	情報処理施設・設備の故障を組織に警告し、計画した手順を実行できるように、情報処理施設・設備を修理又は交換している間も、継続して可用性の維持を可能とする仕組みを設ける。	手引に関連記載あり	–	（対応項なし）
			8b-8.14.7	組織は、冗長システムを実装する場合、次の事項を考慮する。 a) インターネットサービス提供者など、ネットワーク及び重要な情報処理施設・設備の供給者、二者以上と契約する。 b) 冗長性のあるネットワークを使用する。 c) 冗長構成をとったシステムをもつ地理的に離れた二つのデータセンターを使用する。 d) 物理的に冗長性のある電力供給装置又は電源を使用する。 e) ソフトウェア構成要素の複数の並列インスタンスを、同じデータセンター内又は異なるデータセンターのインスタンス間で自動負荷分散して使用する。 f) システムにおいて二重化した構成要素をもつ、又はネットワークにおいて二重化した構成要素をもつ。	手引に関連記載あり	–	（対応項なし）
8.14.2	一つの構成要素から別の構成要素への切替え（failover）が意図したとおりに動作することを試験する。	実施できる場合、できれば本番モードにおいて、一つの構成要素から別の構成要素への切替え（failover）が意図したとおりに動作することを確実にするために、冗長な情報システムを試験する。	8b-8.14.8	実施できる場合、できれば本番モードにおいて、一つの構成要素から別の構成要素への切替え（failover）が意図したとおりに動作することを確実にするために、冗長な情報システムを試験する。	手引に関連記載あり	17.2.1.3	組織は、一つの構成要素から別の構成要素への切替え（failover）による冗長の場合、それが意図したとおりに動作することを確実にするために、冗長な情報システムを試験する。
8.15	ログ取得 統制目標：活動、例外処理、過失及びその他の関連する事象を記録したログを取得し、保存し、保護し、分析する。 目的：事象を記録し、証拠を生成し、ログ情報の完全性を確実にし、認可されていないアクセスを防止し、情報セキュリティインシデントにつながる可能性のある情報セキュリティ事象を特定し、調査を支援するため。		8.15	ログ取得 管理策Ⅰ 活動、例外処理、過失及びその他の関連する事象を記録したログを取得し、保存し、保護し、分析する。 目的Ⅰ 事象を記録し、証拠を生成し、ログ情報の完全性を確実にし、認可されていないアクセスを防止し、情報セキュリティインシデントにつながる可能性のある情報セキュリティ事象を特定し、調査を支援するため。		12.4	ログ取得及び監視 管理目的：イベントを記録し、証拠を作成するため。
						12.4.1	イベントログ取得 利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。
						12.4.2	ログ情報の保護 ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護する。
						12.4.3	実務管理者及び運用担当者の作業ログ システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューする。
8.15.1	ログ特有の要求事項を定義し、ログ取得に関する方針を策定し、取得する。	組織は、ログを作成する目的、どのデータを収集し、ログに記録するか、及びログデータを保護し、取り扱うためのログ特有の要求事項を決定する。 ログ特有の要求事項は、ログ取得に関するトピック固有の方針に立脚せる。 活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。 a) 利用者ID b) システムの動作 c) 関係する事象の日時及び内容（例えば、ログオン、ログオフ） d) 装置・機器の識別情報、システムの識別子及び所在地 e) ネットワークアドレス及びプロトコル 次の事象について、ログ取得を検討する。 a) システムへのアクセスの、成功及び失敗した試み b) データ及び他の資源へのアクセスの、成功及び失敗した試み c) システム構成の変更 d) 特権の利用 e) ユーティリティプログラム及びアプリケーションの利用 f) アクセスされたファイル、及び重要なデータファイルの削除を含むアクセスの種類 g) アクセス制御システムが発した警報 h) セキュリティシステム（例えば、ウイルス対策システム、侵入検知システム）の起動及び停止 i) 識別情報の作成、変更又は削除 j) アプリケーションにおいて利用者が実行したトランザクション、特に二者が提供又は実行するサービス又は製品の場合がある。 インシデントの分析、署告及び調査のためにシステム間のログを関係付けられるように、全てのシステムが同期した時刻源（8.17参照）をもつことが重要である。	8b-8.15.1	組織は、ログを作成する目的、どのデータを収集し、ログに記録するか、及びログデータを保護し、取り扱うためのログ特有の要求事項を決定する。	手引に関連記載あり	–	（対応項なし）
			8b-8.15.2	ログ特有の要求事項は、ログ取得に関するトピック固有の方針に立脚せる。	手引に関連記載あり	–	（対応項なし）
			8b-8.15.3	活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。 a) 利用者ID	手引に関連記載あり	12.4.1.1	イベントログには、利用者IDを含める。
			8b-8.15.3	活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。 b) システムの動作	手引に関連記載あり	12.4.1.2	イベントログには、システムの動作を含める。
			8b-8.15.3	活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。 c) 関係する事象の日時及び内容	手引に関連記載あり	12.4.1.3	イベントログには、主要なイベントの日時及び内容（例えば、ログオン、ログオフ）を含める。
			8b-8.15.3	活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。 d) 装置・機器の識別情報、システムの識別子及び所在地	手引に関連記載あり	12.4.1.4	イベントログには、装置のID 又は所在地（可能な場合）、及びシステムの識別子を含める。
			8b-8.15.3	活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。 e) ネットワークアドレス及びプロトコル	手引に関連記載あり	12.4.1.11	イベントログには、ネットワークアドレス及びプロトコルを含める。
			8b-8.15.4	次の事象について、ログ取得を考慮する。 a) システムへのアクセスの、成功及び失敗した試み	手引に関連記載あり	12.4.1.5	イベントログには、システムへのアクセスの、成功及び失敗した試みの記録を含める。
			8b-8.15.4	次の事象について、ログ取得を考慮する。 b) データ及び他の資源へのアクセスの、成功及び失敗した試み	手引に関連記載あり	12.4.1.6	イベントログには、データ及び他の資源へのアクセスの、成功及び失敗した試みの記録を含める。
			8b-8.15.4	次の事象について、ログ取得を考慮する。 c) システム構成の変更	手引に関連記載あり	12.4.1.7	イベントログには、システム構成の変更を含める。
			8b-8.15.4	次の事象について、ログ取得を考慮する。 d) 特権の利用	手引に関連記載あり	12.4.1.8	イベントログには、特権の利用を含める。
			8b-8.15.4	次の事象について、ログ取得を考慮する。 e) ユーティリティプログラム及びアプリケーションの利用	手引に関連記載あり	12.4.1.9	イベントログには、システムユーティリティ及びアプリケーションの利用を含める。
			8b-8.15.4	次の事象について、ログ取得を考慮する。 f) アクセスされたファイル、及び重要なデータファイルの削除を含むアクセスの種類	手引に関連記載あり	12.4.1.10	イベントログには、アクセスされたファイル及びアクセスの種類を含める。
			8b-8.15.4	次の事象について、ログ取得を考慮する。 g) アクセス制御システムが発した警報	手引に関連記載あり	12.4.1.12	イベントログには、アクセス制御システムが発した警報を含める。
			8b-8.15.4	次の事象について、ログ取得を考慮する。 h) セキュリティシステムの起動及び停止	手引に関連記載あり	12.4.1.13	イベントログには、保護システム（例えば、ウイルス対策システム、侵入検知システム）の作動及び停止を含める。
			8b-8.15.4	次の事象について、ログ取得を考慮する。 i) 識別情報の作成、変更又は削除	手引に関連記載あり	–	（対応項なし）
			8b-8.15.4	次の事象について、ログ取得を考慮する。 j) アプリケーションにおいて利用者が実行したトランザクション	手引に関連記載あり	12.4.1.14	イベントログには、アプリケーションにおいて利用者が実行したトランザクションの記録を含める。
			（8b-8.15.4参考）	インシデントの分析、署告及び調査のためにシステム間のログを関係付けられるように、全てのシステムが同期した時刻源をもつことが重要である。	手引に関連記載あり	–	（対応項なし）
8.15.2	ログ情報の完全性を確実にするための対策を実施する。	特権的アクセス権をもつ利用者を含め、利用者は自らの活動のログを削除又は停止する権限をもたない。 特権を与えられた利用者に関するアカウンタビリティを維持するために、ログを保護及びレビューする。利用者は、その直接の管理下で、情報処理施設・設備に関するログを改変する可能性がある。 管理策は、次の事項を含む、ログ情報の認可されていない変更及びログ取得機能の運用上の問題から保護することを目指す。 a) 記録されたメッセージ形式の変更 b) ログファイルの編集又は削除 c) ログファイルを保持している記憶媒体の記録容量を超過した場合のイベント記録の不具合又は過去のイベント記録への上書き ログは保護することに、その手法として、次の使用を考慮する。 a) 暗号技術によるハッシュ化 b) 追加専用及び読取り専用ファイルへの記録 c) 公開透明性ファイル（第三者が確認できるようにすることで運用における透明性を確保することを目的とした公開されるファイル）への記録 ログは、データ保持に関する要求事項、又は証拠の収集及び保持（5.28参照）のための要求事項によって、保存が求められる場合がある。 組織がエラーのデバッグ又はトラブルシューティングを支援するために、システム又はアプリケーションのログを業者に送信する必要がある場合、利用者名、インターネットプロトコル、IPアドレス、ホスト名、組織名などの情報について、業者に送信する前に、可能な場合はデータマスキング手法（8.11参照）を使用してログの非識別化を行う。 イベントログは、取扱いに慎重を要するデータ及びPIIを含む可能性があるため、適切なプライバシー保護対策を講じる（5.34参照）。 組織が定める監査ログの保存要件に対応するために、監査ログングのストレージ容量を割り当てる。	8b-8.15.5	特権的アクセス権をもつ利用者を含め、利用者は自らの活動のログを削除又は停止する権限をもたない。	手引に関連記載あり	12.4.3.1	特権を与えられた利用者（システムの実務管理者及び運用担当者）に関する責任追跡性を維持するために、その作業を記録する。
			8b-8.15.6	特権を与えられた利用者に関するアカウンタビリティを維持するために、ログを保護及びレビューする。	手引に関連記載あり	12.4.3.2	特権を与えられた利用者（システムの実務管理者及び運用担当者）に関する責任追跡性を維持するために、その利用者の作業のログを保護する。
					手引に関連記載あり	12.4.3.3	特権を与えられた利用者（システムの実務管理者及び運用担当者）に関する責任追跡性を維持するために、その作業のログを定期的にレビューする。
			（8b-8.15.6参考）	利用者は、その直接の管理下で、情報処理施設・設備に関するログを改変する可能性がある。	手引に関連記載あり	–	（対応項なし）
			8b-8.15.7	管理策は、次の事項を含む、ログ情報の認可されていない変更及びログ取得機能の運用上の問題から保護することを目指す。 a) 記録されたメッセージ形式の変更	手引に関連記載あり	12.4.2.1	記録されたメッセージ形式の変更から保護する。
			8b-8.15.7	管理策は、次の事項を含む、ログ情報の認可されていない変更及びログ取得機能の運用上の問題から保護することを目指す。 b) ログファイルの編集又は削除	手引に関連記載あり	12.4.2.2	認可されていないログファイルの編集又は削除から保護する。
			8b-8.15.7	管理策は、次の事項を含む、ログ情報の認可されていない変更及びログ取得機能の運用上の問題から保護することを目指す。 c) ログファイルを保持している記憶媒体の記録容量を超過した場合のイベント記録の不具合又は過去のイベント記録への上書き	手引に関連記載あり	12.4.2.3	イベント記録の不具合又は過去のイベント記録への上書きを引き起こす、ログファイル媒体の記録容量超過の問題から記録を保護するため、イベント記録の生成中止などの手順を定める。
			8b-8.15.8	ログは保護することに、その手法として、次の使用を考慮する。 a) 暗号技術によるハッシュ化 b) 追加専用及び読取り専用ファイルへの記録 c) 公開透明性ファイルへの記録	手引に関連記載あり	–	（対応項なし）
			（8b-8.15.8参考）	ログは、データ保持に関する要求事項、又は証拠の収集及び保持のための要求事項によって、保存が求められる場合がある。	手引に関連記載あり	–	（対応項なし）
			8b-8.15.9	組織がエラーのデバッグ又はトラブルシューティングを支援するために、システム又はアプリケーションのログを業者に送信する必要がある場合、利用者名、インターネットプロトコル、IPアドレス、ホスト名、組織名などの情報について、業者に送信する前に、可能な場合はデータマスキング手法を使用してログの非識別化を行う。	手引に関連記載あり	–	（対応項なし）
			8b-8.15.10	イベントログは、取扱いに慎重を要するデータ及びPIIを含む可能性があるため、適切なプライバシー保護対策を講じる。	手引に関連記載あり	–	（対応項なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.15.3	ログ分析を実施する。	ログ分析は、侵害の可能性がある通常とは異なる活動又は異常な挙動を特定する助けとなるように、情報セキュリティ事象の分析及び解釈を含む。 事象の分析は、次の事項を考慮して実施する。 a) 分析を実施する専門家に必要な技能 b) ログ分析の手順の決定 c) 各セキュリティ関連事象の必要な属性 d) 既定の規則［例えば、セキュリティ情報及びイベント管理（SIEM）又はファイアウォールの規則、並びに侵入検知システム（IDS）又はマルウェアのシグネチャ］の使用を通じて特定される例外事象 e) 異常な活動及び挙動と比較する［利用者及びエンティティの挙動分析（UEBA）］、既知の挙動パターン及び標準ネットワークトラフィック f) 傾向分析又はパターン分析の結果（例えば、データ分析、ビッグデータ技術及び特定の目的の分析ツールを使用した結果） g) 利用可能な脅威インテリジェンス	8b-8.15.11	ログ分析は、侵害の可能性がある通常とは異なる活動又は異常な挙動を特定する助けとなるように、情報セキュリティ事象の分析及び解釈を含む。	手引に関連記載あり	12.4.1.18	利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、悪意のある第三者等からの不正侵入、不正操作等の有無について定期的に点検又は分析を実施する。
			8b-8.15.12	事象の分析は、次の事項を考慮して実施する。 a) 分析を実施する専門家に必要な技能 b) ログ分析の手順の決定 c) 各セキュリティ関連事象の必要な属性 d) 既定の規則の使用を通じて特定される例外事象 e) 異常な活動及び挙動と比較する利用者及びエンティティの挙動分析（UEBA）、既知の挙動パターン及び標準ネットワークトラフィック f) 傾向分析又はパターン分析の結果 g) 利用可能な脅威インテリジェンス	手引に関連記載あり	–	（対応項なし）
			8b-8.15.13	ログ分析は、次の事項を含む、異常な挙動を特定し、分析する助けとなる監視活動によって支援する。 a) 保護された資源［例えば、ドメインネームシステム（DNS）サーバ、ウェブポータル及び共有ファイル］への成功及び失敗したアクセスの試みをレビューする。 b) ボットネットのC2サーバ アンド コントロールサーバ（以下、C&Cサーバと表す。）への接続のような、悪意のあるサーバへのアウトバウンドネットワーク接続を特定するために、DNSログを確認する。 c) システム及びネットワーク内の異常な活動に関するサービス提供者からの使用状況報告（例えば、インボイス又はサービス報告）を調べる（例えば、活動のパターンをレビューする）。 d) より正確な検知及びインシデント分析を確実にするために、入口、出口などの物理的監視のイベントログを含める。 e) 効率的で非常に正確な分析を行えるように、ログを相互に関係付ける。	手引に関連記載あり	–	（対応項なし）
			8b-8.15.14	情報セキュリティインシデントの疑い、及び実際の情報セキュリティインシデントを特定し、要なる調査を行う。	手引に関連記載あり	–	（対応項なし）
8.15.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
8.16	監視活動 統制目標：情報セキュリティインシデントの可能性を評価するために、ネットワーク、システム及びアプリケーションについて異常な挙動がないか監視し、適切な処置を講じる。 目的：異常な挙動及び情報セキュリティインシデントの可能性を検出するため。		8.16	監視活動 管理策 情報セキュリティインシデントの可能性を評価するために、ネットワーク、システム及びアプリケーションについて異常な挙動がないか監視し、適切な処置を講じることが望ましい。 目的 異常な挙動及び情報セキュリティインシデントの可能性を検出するため。		–	（対応項なし）
8.16.1	監視の範囲及びレベルを定義する。	監視のために、次の事項を行う。 a) 監視の範囲及びレベルは、業務及び情報セキュリティの要求事項に従い、関連する法令及び規制を考慮して決定する。 b) 監視を記録する。 c) 監視記録は、定めた保持期間にわたって維持する。 監視システムに含めるものとして、次の事項を考慮する。 a) アウトバウンド及びインバウンドの、ネットワーク、システム及びアプリケーションのトラフィック b) システム、サーバ、ネットワーク装置、監視システム、重要なアプリケーションなどへのアクセス c) 重要な又は実務管理者が扱うシステム及びネットワークの構成ファイル d) セキュリティツールからのログ［例えば、ウイルス対策、IDS、不正侵入防止システム（IPS）、ウェブフィルタ、ファイアウォール、データ漏えい防止（DLP）］ e) システム及びネットワークの活動に関するイベントログ f) 実行しているコードがそのシステムでの実行を認可されていること、及びそれが改ざん（例えば、望ましくないコードを追加する再コンパイルによる改ざん）されていないことの確認 g) 資源（例えば、CPU、ハードディスク、メモリ、帯域幅）の使用及びそれらの動作状況 組織は、正常な挙動の基準を確立し、この基準に照らして異常を監視する。基準を確立する場合、次の事項を考慮する。 a) 通常時及びピーク時のシステムの使用率 b) 各利用者又は利用者グループの通常のアクセス時間、アクセスの場所、アクセスの頻度 監視システムは、次のような異常な挙動を特定するために、確立した基準に照らして構成する。 a) プロセス又はアプリケーションの計画外の終了 b) 既知の悪意のあるIP アドレスはネットワークドメイン（例えば、ボットネットのC&C サーバに関係するもの）から送信されるマルウェア又はトラフィックに典型的に伴う挙動 c) 既知の攻撃の特性（例えば、サービス妨害及びバッファオーバーフロー） d) 異常なシステム動作（例えば、キー入力のログ、プロセスインジェクション、及び標準プロトコルの使用に反する通信） e) ボトルネック及び過負荷（例えば、ネットワークの待ち行列、遅延レベル及びネットワーク上の通信の乱れ） f) システム又は情報への認可されていないアクセス又はその試み g) 業務アプリケーション、システム及びネットワークの認可されていないスキャン h) 保護された資源（例えば、DNS サーバ、ウェブポータル及びファイルシステム）への成功及び失敗したアクセスの試み i) 想定される挙動に対して、利用者及びシステムの異常な挙動	8b-8.16.1	監視のために、次の事項を行う。 a) 監視の範囲及びレベルは、業務及び情報セキュリティの要求事項に従い、関連する法令及び規制を考慮して決定する。 b) 監視を記録する。 c) 監視記録は、定めた保持期間にわたって維持する。	手引に関連記載あり	–	（対応項なし）
			8b-8.16.2	監視システムに含めるものとして、次の事項を考慮する。 a) アウトバウンド及びインバウンドの、ネットワーク、システム及びアプリケーションのトラフィック b) システム、サーバ、ネットワーク装置、監視システム、重要なアプリケーションなどへのアクセス c) 重要な又は実務管理者が扱うシステム及びネットワークの構成ファイル d) セキュリティツールからのログ e) システム及びネットワークの活動に関するイベントログ f) 実行しているコードがそのシステムでの実行を認可されていること、及びそれが改ざんされていないことの確認 g) 資源の使用及びそれらの動作状況	手引に関連記載あり	–	（対応項なし）
			8b-8.16.3	組織は、正常な挙動の基準を確立し、この基準に照らして異常を監視する。基準を確立する場合、次の事項を考慮する。 a) 通常時及びピーク時のシステムの使用率 b) 各利用者又は利用者グループの通常のアクセス時間、アクセスの場所、アクセスの頻度	手引に関連記載あり	–	（対応項なし）
			8b-8.16.4	監視システムは、次のような異常な挙動を特定するために、確立した基準に照らして構成する。 a) プロセス又はアプリケーションの計画外の終了 b) 既知の悪意のあるIP アドレスはネットワークドメインから送信されるマルウェア又はトラフィックに典型的に伴う挙動 c) 既知の攻撃の特性 d) 異常なシステム動作 e) ボトルネック及び過負荷 f) システム又は情報への認可されていないアクセス又はその試み g) 業務アプリケーション、システム及びネットワークの認可されていないスキャン h) 保護された資源への成功及び失敗したアクセスの試み i) 想定される挙動に対して、利用者及びシステムの異常な挙動	手引に関連記載あり	–	（対応項なし）
8.16.2	リアルタイム又は定期的な間隔で監視を行う。	監視ツールによる継続的監視を使用し、次の実施を考慮する。 a) 監視は、組織のニーズ及び能力に応じて、リアルタイム又は定期的な間隔で行う。 b) 大量のデータを取り扱い、常に変化する脅威の状況に適応し、リアルタイムで通知することを可能にする。 c) 特定のシグネチャ及びデータ、又はネットワーク若しくはアプリケーションの動作パターンから記録できる監視ツールを利用する。 自動監視ソフトウェアは、あらかじめ定めたしきい値に基づいて警告を発するように構成する（例えば、管理コンソール、電子メールメッセージ又はインスタントメッセージングシステムを通して構成する）。 警告システムは、誤検出を最小限にするために、組織の基準に合わせて調整し、学習させる。	8b-8.16.5	監視ツールによる継続的監視を使用し、次の事項を考慮する。 a) 監視は、組織のニーズ及び能力に応じて、リアルタイム又は定期的な間隔で行う。 b) 大量のデータを取り扱い、常に変化する脅威の状況に適応し、リアルタイムで通知することを可能にする機能をもつ監視ツールを利用する。 c) 特定のシグネチャ及びデータ、又はネットワーク若しくはアプリケーションの動作パターンも記録できる監視ツールを利用する。	手引に関連記載あり	–	（対応項なし）
			8b-8.16.6	自動監視ソフトウェアは、あらかじめ定めたしきい値に基づいて警告を発するように構成する。	手引に関連記載あり	–	（対応項なし）
			8b-8.16.7	警告システムは、誤検出を最小限にするために、組織の基準に合わせて調整し、学習させる。	手引に関連記載あり	–	（対応項なし）
8.16.3	異常な挙動及び情報セキュリティインシデントの可能性のある事象は、組織が定める職員又は役割に伝達する。	要員は警告への対応に専念させることが望ましく、インシデントの可能性がある事象を正確に判定できるように適切に訓練を受けさせる。 警告通知を受信し、対応するための冗長性のあるシステム及びプロセスを備える。 監査、セキュリティ評価、ぜい弱性スキャン及び監視（5.25参照）を改善するために、異常な事象を関係者に伝達する。 情報セキュリティに対する有害な事象の影響を最小にするために、その存在を示す監視システムからの通知に時機を失せず対応する手順を確立する（5.26参照）。 将来の誤検出の数を減らすために監視ソフトウェアを調整するなど、誤検出を特定し、対処する手順も確立する。	8b-8.16.8	要員は警告への対応に専念させることが望ましく、インシデントの可能性がある事象を正確に判定できるように適切に訓練を受けさせる。	手引に関連記載あり	–	（対応項なし）
			8b-8.16.9	警告通知を受信し、対応するための冗長性のあるシステム及びプロセスを備える。	手引に関連記載あり	–	（対応項なし）
			8b-8.16.10	監査、セキュリティ評価、ぜい弱性スキャン及び監視を改善するために、異常な事象を関係者に伝達する。	手引に関連記載あり	–	（対応項なし）
			8b-8.16.11	情報セキュリティに対する有害な事象の影響を最小にするために、その存在を示す監視システムからの通知に時機を失せず対応する手順を確立する。	手引に関連記載あり	–	（対応項なし）
			8b-8.16.12	将来の誤検出の数を減らすために監視ソフトウェアを調整するなど、誤検出を特定し、対処する手順も確立する。	手引に関連記載あり	–	（対応項なし）
8.17	クロックの同期 統制目標：組織が使用する情報処理システムのクロックは、組織が採用した時刻源と同期させる。 目的：セキュリティ関連の事象及びその他の記録されたデータの関係付け及び分析を可能にし、情報セキュリティインシデントの調査を支援するため。		8.17	クロックの同期 管理策 組織が使用する情報処理システムのクロックは、組織が採用した時刻源と同期させる。 目的 セキュリティ関連の事象及びその他の記録されたデータの関係付け及び分析を可能にし、情報セキュリティインシデントの調査を支援するため。		12.4.4	クロックの同期 組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させる。
8.17.1	クロックは、組織が採用した時刻源と同期させる。	時刻の表現、信頼できる同期及び正確さに関する、外部及び内部の要求事項は、文書化し、実施する。この要求事項は、法令、規制、契約、標準及び内部監視のニーズに由来する可能性がある。 ビル管理システム、入退出システム、及び調査を支援するために使用できるその他のシステムを含む全てのシステムに対して、組織内で基準とする時刻源を考慮して定める。 国の原子時計又は全地球測位システム（GPS）から配信される時刻に基づくクロックを、ログ取得システムの基準クロック、すなわち、正確なタイムスタンプを確実にする一貫性のある信頼できる日付及び時刻源として使用する。 ネットワークで接続された全てのシステムを基準クロックと同期させるために、ネットワークタイムプロトコル（NTP）又は高精度タイムプロトコル（PTP）などのプロトコルを使用する。組織は、外部クロックの信頼性を改善し、変動を適切に管理するために、二つの外部時刻源を同時に使用することが可能である。 クラウドサービスの利用によりクロックの同期が困難となる場合、不一致から生じるリスクを軽減するために、各サービスのクロックを監視し、差を記録する。複数のクラウドサービスを使用する場合、又はクラウドサービス及びオンプレミスサービスの両方を使用する場合には、クロックの同期が困難なことがある。	8b-8.17.1	時刻の表現、信頼できる同期及び正確さに関する、外部及び内部の要求事項は、文書化し、実施する。	手引に関連記載あり	12.4.4.1	時刻の表示、同期及び正確さに関する外部及び内部の要求事項 は、文書化する。
			（8b-8.17.1参考）	この要求事項は、法令、規制、契約、標準及び内部監視のニーズに由来する可能性がある。	手引に関連記載あり	–	（対応項なし）
			8b-8.17.2	ビル管理システム、入退出システム、及び調査を支援するために使用できるその他のシステムを含む全てのシステムに対して、組織内で基準とする時刻源を考慮して定める。	手引に関連記載あり	12.4.4.2	組織内で用いるための基準となる時刻源を定める。
			8b-8.17.3	国の原子時計又は全地球測位システム（GPS）から配信される時刻に基づくクロックを、ログ取得システムの基準クロック、すなわち、正確なタイムスタンプを確実にする一貫性のある信頼できる日付及び時刻源として使用する。	手引に関連記載あり	12.4.4.3	基準となる時刻源を外部から取得するための組織の取組み及び内部のクロックを確実に同期させる方法を文書化し、実施する。
			8b-8.17.4	ネットワークで接続された全てのシステムを基準クロックと同期させるために、ネットワークタイムプロトコル（NTP）又は高精度タイムプロトコル（PTP）などのプロトコルを使用する。	手引に関連記載あり	–	（対応項なし）
			（8b-8.17.4参考）	組織は、外部クロックの信頼性を改善し、変動を適切に管理するために、二つの外部時刻源を同時に使用することが可能である。	手引に関連記載あり	–	（対応項なし）
			8b-8.17.5	クラウドサービスの利用によりクロックの同期が困難となる場合、不一致から生じるリスクを軽減するために、各サービスのクロックを監視し、差を記録する。	手引に関連記載あり	–	（対応項なし）
			（8b-8.17.5参考）	複数のクラウドサービスを使用する場合、又はクラウドサービス及びオンプレミスサービスの両方を使用する場合には、クロックの同期が困難なことがある。	手引に関連記載あり	–	（対応項なし）
8.17.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.18	特権的なユーティリティプログラムの使用 統制目標：システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。 目的：ユーティリティプログラムの使用が、システム及びアプリケーションについての情報セキュリティ管理策に害を与えないことを確実にするため。		8.18	特権的なユーティリティプログラムの使用 管理策 システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。 目的 ユーティリティプログラムの使用が、システム及びアプリケーションについての情報セキュリティ管理策に害を与えないことを確実にするため。		9.4.4	特権的なユーティリティプログラムの使用 システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。
8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用において必要な要求事項を定義し、対策を実施する。	クラウドサービス内で利用する全てのユーティリティプログラムのための要求事項を特定する。 システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 a) 可能な限り少人数の信頼できる認可された利用者だけに限定した、ユーティリティプログラムの使用制限（8.2参照） b) ユーティリティプログラムを使用する要員の一意の識別を含む、ユーティリティプログラムの識別、認証及び認可手順の使用 c) ユーティリティプログラムの認可レベルの明確化及び文書化 d) ユーティリティプログラムを臨時に用いる場合の認可 e) 権限の分離が必要な場合に、システム上のアプリケーションにアクセスする利用者に、ユーティリティプログラムの使用を不可とする f) 全ての不要なユーティリティプログラムの除去又は無効化 g) 少なくも、アプリケーションソフトウェアからのユーティリティプログラムの論理的分離。実施できる場合、ユーティリティプログラムのネットワーク通信をアプリケーショントラフィックから分離 h) ユーティリティプログラムの使用の制限（例えば、認可されたシステム変更のための期間での利用） i) ユーティリティプログラムの全ての使用に関するログ 通常の操作手順又はセキュリティ手順も回避することのできる全てのプログラムを、認可された要員に厳重に制限し、そのようなプログラムの利用を定期的にレビュー、監査する。	8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 a) 可能な限り少人数の信頼できる認可された利用者だけに限定した、ユーティリティプログラムの使用制限	手引に関連記載あり	9.4.4.3	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、可能な限り少人数の信頼できる認可された利用者だけに限定する。
			8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 b) ユーティリティプログラムを使用する要員の一意の識別を含む、ユーティリティプログラムの識別、認証及び認可手順の使用	手引に関連記載あり	9.4.4.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用のための識別、認証及び認可手順を整備し、使用する。
			8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 c) ユーティリティプログラムの認可レベルの明確化及び文書化	手引に関連記載あり	9.4.4.7	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの認可レベルを明確にし、文書化する。
			8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 d) ユーティリティプログラムを臨時に用いる場合の認可	手引に関連記載あり	9.4.4.4	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムを臨時に用いる場合の認可手順を整備する。
			8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 e) 権限の分離が必要な場合に、システム上のアプリケーションにアクセスする利用者に、ユーティリティプログラムの使用を不可とする	手引に関連記載あり	9.4.4.9	権限の分離が必要な場合には、システム上のアプリケーションへのアクセス権をもつ利用者に対して、システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用を禁止する。
			8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 f) 全ての不要なユーティリティプログラムの除去又は無効化	手引に関連記載あり	9.4.4.8	システム及びアプリケーションによる制御を無効にすることのできる不要なユーティリティプログラムは全て除去又は無効化する。
			8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 g) 少なくも、アプリケーションソフトウェアからのユーティリティプログラムの論理的分離。実施できる場合、ユーティリティプログラムのネットワーク通信をアプリケーショントラフィックから分離	手引に関連記載あり	9.4.4.2	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムは、アプリケーションソフトウェアから分離する。
			8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 h) ユーティリティプログラムの使用の制限	手引に関連記載あり	9.4.4.5	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用を制限する。（例えば、認可されたシステム変更のための期間での利用）
			8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 i) ユーティリティプログラムの全ての使用に関するログ	手引に関連記載あり	9.4.4.6	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの全ての使用に関するログを取得する。
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
8.19	運用システムへのソフトウェアの導入 統制目標：運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施する。 目的：運用システムの完全性の維持を確実にし、技術的せい弱性の悪用を防止するため。		8.19	運用システムへのソフトウェアの導入 管理策 運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施する。 目的 運用システムの完全性の維持を確実にし、技術的せい弱性の悪用を防止するため。		12.5	運用ソフトウェアの管理 管理目的：運用システムの完全性を確実にするため。
						12.5.1	運用システムに関わるソフトウェアの導入 運用システムに関わるソフトウェアの導入を管理するための手順を実施する。
						12.6.2	ソフトウェアのインストールの制限 利用者によるソフトウェアのインストールを管理する規則を確立し、実施する。
8.19.1	運用システムにおけるソフトウェアの導入及び変更をセキュリティを保って管理するための手順を策定し、対策を実施する。	特権の許可は最小限にするという原則を、運用システムへのソフトウェアの導入に適用する。 ソフトウェアのインストールの種類のうち、許可するもの（例えば、既存のソフトウェアの更新及びセキュリティパッチの適用）、及び禁止するもの（例えば、個人利用のためだけのソフトウェア、その由来から悪意のある可能性が不明又は疑わしいソフトウェア）を特定する。 特権は、利用者の役割に基づいて付与する。 組織は、利用者が導入できるソフトウェアの種類について、厳密な規則を定め、施行する。 運用システムにおけるソフトウェアの導入及び変更において、セキュリティを保つために、次の事項を考慮する。 a) 運用ソフトウェアの更新は、適切な管理層の認可に基づき、訓練された実務管理者だけが実施する（8.5参照）。 b) 運用システムには、承認された実行可能なコードだけを導入し、開発用コードとはコンパイラは一切導入しないことを確実にする。 c) ソフトウェアは、十分なテストに成功した後に導入し、更新する（8.29及び8.31参照）。 d) 対応する全てのプログラムソースライブラリを更新する。 e) 全ての運用ソフトウェアの管理を維持するために、システム文書の管理と同様に、構成管理システムを利用する。 f) 変更を実施する前に、ロールバック計画を定める。 g) 運用ソフトウェアの更新の全てについて、監査ログを維持する。 h) ソフトウェアの旧版は、緊急時対応の手段として、及び保管しているデータをそのソフトウェアで読みとるとは処理する必要がある期間、全ての必要な情報及びパラメータ、手順、設定の詳細並びにサポートソフトウェアとともに保管しておく。 新リースにアップグレードするとの決定には、その変更に対する事業上の要求及びそのリースのセキュリティ（例えば、新しい情報セキュリティ機能の導入、既存の版に影響を及ぼす情報セキュリティのせい弱性の数及び深刻度）を考慮に入れる。 情報セキュリティ上のせい弱性を除去するか、又は低減するために役立つ場合には、ソフトウェアパッチを適用する（8.8及び8.19参照）。 外部から供給されるソフトウェア及びパッケージ（例えば、外部サイトが提供しているモジュールを使用するソフトウェアプログラム）に依存するソフトウェアは、情報セキュリティのせい弱性をたらす可能性があるため、認可されていない変更を回避するために監視し、管理する。 運用システムで利用するソフトウェアの版を、ソフトウェア業者（供給者）がサポートする版に維持する。 組織は、サポートのないソフトウェアに依存することのリスクを考慮する。ソフトウェア業者は、徐々に古い版のソフトウェアのサポートを中止する。 運用システムで使用するオープンソースソフトウェアは、最新で適切なリリースの使用を維持する。時間の経過とともに、オープンソースコードが維持されなくなるにかかわらず、オープンソースソフトウェアポジトリで引き続き利用できる場合がある。組織は、運用システムで使用する場合、保守がなされないオープンソースソフトウェアに依存するリスクも考慮する。 供給者がソフトウェアの導入又は更新に関与する場合、物理的又は論理的アクセスは、必要なときに、適切な認可を得た場合にだけ許可することが望ましい。供給者の活動を監視する（5.22参照）。	8b-8.19.12	特権の許可は最小限にするという原則を、運用システムへのソフトウェアの導入に適用する。	手引に関連記載あり	12.6.2.2	特権の許可は最小限にするという原則を適用する。
					手引に関連記載あり	12.6.2.4	特権は、関連する利用者の役割を考慮したうえで付与する。
			8b-8.19.13	組織は、ソフトウェアのインストールの種類のうち、許可するもの、及び禁止するものを特定する。	手引に関連記載あり	12.6.2.3	組織は、ソフトウェアのインストールの種類のうち、許可するもの（例えば、既存のソフトウェアの更新及びセキュリティパッチの適用）、及び禁止するもの（例えば、個人利用のためのソフトウェア、潜在的な悪意のある有無が不明又はその疑いがあるソフトウェア）を特定する。
			8b-8.19.14	特権は、利用者の役割に基づいて付与する。	手引に関連記載あり	–	（対応項なし）
			8b-8.19.11	組織は、利用者が導入できるソフトウェアの種類について、厳密な規則を定め、施行する。	手引に関連記載あり	12.6.2.1	組織は、利用者がインストールしてもよいソフトウェアの種類について、厳密な方針を定め、施行する。
			8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 a) 運用ソフトウェアの更新は、適切な管理層の認可に基づき、訓練された実務管理者だけが実施する。	手引に関連記載あり	12.5.1.1	運用ソフトウェア、アプリケーション及びプログラムライブラリの更新は、適切な管理層の認可に基づき、訓練された実務管理者だけが実施する。
			8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 b) 運用システムには、承認された実行可能なコードだけを導入し、開発用コードとはコンパイラは一切導入しないことを確実にする。	手引に関連記載あり	12.5.1.2	運用システムは、実行可能なコードだけを保持し、開発用コード又はコンパイラは保持しない。
			8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 c) ソフトウェアは、十分なテストに成功した後に導入し、更新する。	手引に関連記載あり	12.5.1.3	アプリケーション及びオペレーティングシステムソフトウェアは、十分な試験に成功した後に導入する。
			8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 d) 対応する全てのプログラムソースライブラリを更新する。	手引に関連記載あり	12.5.1.6	アプリケーション及びオペレーティングシステムソフトウェアの試験は、対応するプログラムソースライブラリが更新済みであることを確実にする仕組みを整備する。
			8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 e) 全ての運用ソフトウェアの管理を維持するために、システム文書の管理と同様に、構成管理システムを利用する。	手引に関連記載あり	12.5.1.7	導入したソフトウェアの管理を維持するために、システムに関する文書化と同様に、構成管理システムを利用する。
			8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 f) 変更を実施する前に、ロールバック計画を定める。	手引に関連記載あり	12.5.1.8	変更を実施する前に、ロールバック計画を備える。
			8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 g) 運用ソフトウェアの更新の全てについて、監査ログを維持する。	手引に関連記載あり	12.5.1.9	運用プログラムライブラリの更新の全てについて、監査ログを維持する。
			8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 h) ソフトウェアの旧版は、緊急時対応の手段として、及び保管しているデータをそのソフトウェアで読みとるとは処理する必要がある期間、全ての必要な情報及びパラメータ、手順、設定の詳細並びにサポートソフトウェアとともに保管しておく。	手引に関連記載あり	12.5.1.10 12.5.1.11	緊急時対応の手段として、一つ前の版のアプリケーションソフトウェアを保持する。 ソフトウェアの旧版は、そのソフトウェアが扱った データが保存されている期間、必要とされる情報及びパラメータの全て、手順、設定の詳細並びにサポートソフトウェアとともに保管する。
			8b-8.19.2	新リースにアップグレードするとの決定には、その変更に対する事業上の要求及びそのリースのセキュリティを考慮に入れる。	手引に関連記載あり	12.5.1.14	新リースにアップグレードするとの決定には、その変更に対する事業上の要求及びそのリースのセキュリティ（例えば、新しい情報セキュリティ機能の導入、この版が必要になった情報セキュリティ問題の量及び質）を考慮して行う。
			8b-8.19.3	情報セキュリティ上のせい弱性を除去するか、又は低減するために役立つ場合には、ソフトウェアパッチを適用する。	手引に関連記載あり	12.5.1.15	情報セキュリティ上の弱点を除去するか、又は低減するために役立つ場合には、ソフトウェアパッチを適用する。
			8b-8.19.4	外部から供給されるソフトウェア及びパッケージに依存するソフトウェアは、情報セキュリティのせい弱性をたらす可能性があるため、認可されていない変更を回避するために監視し、管理する。	手引に関連記載あり	12.5.1.18	セキュリティ上の弱点を招く可能性のある認可されていない変更を回避するために、外部から供給されるソフトウェア及びモジュールは、監視し、管理する。
			8b-8.19.5	運用システムで利用するソフトウェアの版を、ソフトウェア業者（供給者）がサポートする版に維持する。	手引に関連記載あり	12.5.1.12	運用システムに利用される業者供給ソフトウェアは、供給者によってサポートされるレベルを維持する。
			8b-8.19.6	組織は、サポートのないソフトウェアに依存することのリスクを考慮する。	手引に関連記載あり	12.5.1.13	組織は、サポートのないソフトウェアに依存することのリスクを考慮して管理する。
			（8b-8.19.6参考）	ソフトウェア業者は、徐々に古い版のソフトウェアのサポートを中止する。	手引に関連記載あり	–	（対応項なし）
			8b-8.19.7	運用システムで使用するオープンソースソフトウェアは、最新で適切なリリースの使用を維持する。	手引に関連記載あり	–	（対応項なし）
			（8b-8.19.7参考）	時間の経過とともに、オープンソースコードが維持されなくなるにもかかわらず、オープンソースソフトウェアポジトリで引き続き利用できる場合がある。	手引に関連記載あり	–	（対応項なし）
			8b-8.19.8	組織は、運用システムで使用する場合、保守がなされないオープンソースソフトウェアに依存するリスクも考慮する。	手引に関連記載あり	–	（対応項なし）
			8b-8.19.9	供給者がソフトウェアの導入又は更新に関与する場合、物理的又は論理的アクセスは、必要なときに、適切な認可を得た場合にだけ許可する。	手引に関連記載あり	12.5.1.16	供給者による物理的又は論理的アクセスは、サポート目的で必要なときに、管理職の承認を得た場合にだけ許可する。
			8b-8.19.10	供給者の活動を監視する。	手引に関連記載あり	12.5.1.17	供給者による物理的又は論理的アクセスを許可している間は、供給者の活動を監視する。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.20	ネットワークセキュリティ 統制目標：システム及びアプリケーション内の情報を保護するために、ネットワーク及びネットワーク装置のセキュリティを保ち、管理し、制御する。 目的：ネットワーク及びそれを支援する情報処理設備において、情報をネットワークを通した侵害から保護するため。		8.20	ネットワークセキュリティ 管理策 システム及びアプリケーション内の情報を保護するために、ネットワーク及びネットワーク装置のセキュリティを保ち、管理し、制御する。 目的 ネットワーク及びそれを支援する情報処理設備において、情報をネットワークを通した侵害から保護するため。		13	通信のセキュリティ
						13.1	ネットワークセキュリティ管理 管理目的：ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。
						13.1.1	ネットワーク管理策 システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御する。
8.20.1	ネットワーク及びネットワーク装置のセキュリティを保つための対策を実施する。	ネットワークにおける情報のセキュリティを確実にし、接続したネットワークサービスを認可されていないアクセスから保護するために、管理策を実施する。 ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 a) ネットワークごとに、扱ってよい情報の種類及び分類レベル b) ネットワーク装置及び機器の管理に関する責任及び手順を確立する。 c) ネットワーク及び(装置・機器（例えば、ルーター、スイッチ）の構成ファイルを含む最新の文書を維持する。 d) 適切な場合には、ネットワークの運用責任は、ICTシステムの運用から分離する（5.3参照）。 e) 公衆ネットワーク、第三者ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及びアプリケーションを保護するために、管理策を確立する（5.22、8.24、5.14及び5.6参照。ネットワークサービスの可用性及びネットワークに接続したコンピュータの可用性を維持するためには、追加の管理策が要求される場合もある）。 f) 情報セキュリティに影響を及ぼす可能性のある行動、又は情報セキュリティに関係のある行動の記録及び検知ができるように、適切なログを取得し、監視する（8.16及び16.1参照）。 g) 組織に対するサービスを最適にするため、また、管理策を情報処理基盤全体に一貫して適用することを確実にするため、様々なネットワーク管理作業を綿密に調整する。 h) ネットワーク上のシステムを認証する。 i) ネットワークへのシステムの接続を制限し、フィルタリングする（例えば、ファイアウォールを使用する。）。 j) ネットワークへの装置及び機器の接続を検出し、制限し、認証する。 k) ネットワーク装置・機器の要塞化（hardening） l) ネットワーク管理の経路を他のネットワークトラフィックから分離する。 m) ネットワークが攻撃を受けた場合、重要なサブネットワークを一時的に分離する［例えば、ドローブッシ（跳ね橋）を用いて分離する。］。 n) ぜい弱なネットワークプロトコルを無効化する。 組織は、仮想化ネットワークの使用に、適切なセキュリティ管理策を適用することを確実にする。仮想化ネットワークには、ソフトウェア定義ネットワーク（SDN、SD-WAN）も含む。仮想化ネットワークは、物理的ネットワークとその通信の論理的分離を可能にすることから、セキュリティの観点で望ましい場合があり、特に分散型コンピューティングを用いて実装したシステム及びアプリケーションにおいてのことが該当する。	8c-8.20.1	ネットワークにおける情報のセキュリティを確実にし、接続したネットワークサービスを認可されていないアクセスから保護するために、管理策を実施する。	手引に関連記載あり	13.1.1.1	ネットワークにおける情報のセキュリティ、及び接続したネットワークサービスの認可されていないアクセスから保護を確実にするために、管理策を実施する。
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 a) ネットワークごとに、扱ってよい情報の種類及び分類レベル	手引に関連記載あり	–	（対応項なし）
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 b) ネットワーク装置及び機器の管理に関する責任及び手順を確立する。	手引に関連記載あり	13.1.1.2	ネットワーク設備の管理に関する責任及び手順を確立する。
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 c) ネットワーク図及び装置・機器の構成ファイルを含む最新の文書を維持する。	手引に関連記載あり	–	（対応項なし）
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 d) 適切な場合には、ネットワークの運用責任は、ICTシステムの運用から分離する。	手引に関連記載あり	13.1.1.3	ネットワークの運用責任は、コンピュータの運用から、分離する。
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 e) 公衆ネットワーク、第三者ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及びアプリケーションを保護するために、管理策を確立する。	手引に関連記載あり	13.1.1.4	公衆ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及びアプリケーションを保護するために、特別な管理策を確立する。
					手引に関連記載あり	13.1.1.5	ネットワークサービスの可用性及びネットワークを介して接続したコンピュータの可用性を維持するために、特別な管理策を確立する。
					手引に関連記載あり	14.1.1.11	公衆ネットワークを介してサービスを提供するアプケーション、又はトランザクションを実施するアプリケーションについては、14.1.2 及び14.1.3の管理策を考慮して決定する。
					手引に関連記載あり	14.1.2.6	公衆ネットワークを経由するアプリケーションサービスは、秘匿情報の保護に関する要求事項を定める。
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 f) 情報セキュリティに影響を及ぼす可能性のある行動、又は情報セキュリティに関係のある行動の記録及び検知ができるように、適切なログを取得し、監視する。	手引に関連記載あり	13.1.1.6	情報セキュリティに影響を及ぼす可能性のある行動、又は情報セキュリティに関連した行動を記録及び検知できるように、適切なログ取得及び監視を適用する。
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 g) 組織に対するサービスを最適にするため、また、管理策を情報処理基盤全体に一貫して適用することを確実にするために、様々なネットワーク管理作業を綿密に調整する。	手引に関連記載あり	13.1.1.7	組織に対するサービスを最適にするため、また、管理策を情報処理基盤全体に一貫して適用することを確実にするために、様々な管理作業を綿密に調整する。
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 h) ネットワーク上のシステムを認証する。	手引に関連記載あり	13.1.1.8	ネットワーク上のシステム（デバイスを含む）は接続前に認証する。
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 i) ネットワークへのシステムの接続を制限し、フィルタリングする。	手引に関連記載あり	13.1.1.9	ネットワークへのシステムの接続を制限する。
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 j) ネットワークへの装置及び機器の接続を検出し、制限し、認証する。	手引に関連記載あり	–	（対応項なし）
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 k) ネットワーク装置・機器の要塞化（hardening）	手引に関連記載あり	–	（対応項なし）
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 l) ネットワーク管理の経路を他のネットワークトラフィックから分離する。	手引に関連記載あり	–	（対応項なし）
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 m) ネットワークが攻撃を受けた場合、重要なサブネットワークを一時的に分離する。	手引に関連記載あり	–	（対応項なし）
			8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 n) ぜい弱なネットワークプロトコルを無効化する。	手引に関連記載あり	–	（対応項なし）
			8c-8.20.3	組織は、仮想化ネットワークの使用に、適切なセキュリティ管理策を適用することを確実にする。	手引に関連記載あり	–	（対応項なし）
			（8c-8.20.3参考1）	仮想化ネットワークには、ソフトウェア定義ネットワーク（SDN、SD-WAN）も含む。	手引に関連記載あり	–	（対応項なし）
			（8c-8.20.3参考2）	仮想化ネットワークは、物理的ネットワーク上での通信の論理的分離を可能にすることから、セキュリティの観点で望ましい場合があり、特に分散型コンピューティングを用いて実装したシステム及びアプリケーションにおいてのことが該当する。	手引に関連記載あり	–	（対応項なし）
8.20.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の出来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
8.21	ネットワークサービスのセキュリティ 統制目標：ネットワークサービスのセキュリティ機能、サービスレベル及びサービスの要求事項を特定し、実装し、監視する。 目的：ネットワークサービスの利用におけるセキュリティを確実にするため。		8.21	ネットワークサービスのセキュリティ 管理策 ネットワークサービスのセキュリティ機能、サービスレベル及びサービスの要求事項を特定し、実装し、監視する。 目的 ネットワークサービスの利用におけるセキュリティを確実にするため。		13.1.2	ネットワークサービスのセキュリティ 組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定し、また、ネットワークサービス合意書にもこれらを盛り込む。
8.21.1	ネットワークサービスの利用に関する規則を整備する。	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 a) アクセスが許可されているネットワーク及びネットワークサービス b) 様々なネットワークサービスにアクセスするための認証の要求事項 c) 誰にどのネットワーク及びネットワークサービスにアクセスすることを許すかを決定する認可手順 d) ネットワーク接続及びネットワークサービスへのアクセスを保護するためのネットワーク管理並びに技術的管理策及び手順 e) ネットワーク及びネットワークサービスにアクセスするために利用する手段［例えば、仮想プライベートネットワーク（VPN）又は無線ネットワークの利用］ f) アクセス時の利用者の時刻、場所及びその他の属性 g) ネットワークサービスの利用の監視	8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 a) アクセスが許可されているネットワーク及びネットワークサービス	手引に関連記載あり	9.1.2.2	ネットワーク及びネットワークサービスの利用に関する方針は、アクセスが許されるネットワーク及びネットワークサービスを対象にする。
			8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 b) 様々なネットワークサービスにアクセスするための認証の要求事項	手引に関連記載あり	9.1.2.6	ネットワーク及びネットワークサービスの利用に関する方針は、様々なネットワークサービスへのアクセスに対する利用者認証の要求事項を対象にする。
			8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 c) 誰にどのネットワーク及びネットワークサービスにアクセスすることを許すかを決定する認可手順	手引に関連記載あり	9.1.2.3	ネットワーク及びネットワークサービスの利用に関する方針は、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決めるための認可手順を対象にする。
			8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 d) ネットワーク接続及びネットワークサービスへのアクセスを保護するためのネットワーク管理並びに技術的管理策及び手順	手引に関連記載あり	9.1.2.4	ネットワーク及びネットワークサービスの利用に関する方針は、ネットワーク接続及びネットワークサービスへのアクセスを保護するための運用管理国からの管理策及び管理手順を対象にする。
			8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 e) ネットワーク及びネットワークサービスにアクセスするために利用する手段	手引に関連記載あり	9.1.2.5	ネットワーク及びネットワークサービスの利用に関する方針は、ネットワーク及びネットワークサービスへのアクセスに利用される手段（例えば、VPN、無線ネットワーク）を対象にする。
			8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 f) アクセス時の利用者の時刻、場所及びその他の属性	手引に関連記載あり	–	（対応項なし）
			8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 g) ネットワークサービスの利用の監視	手引に関連記載あり	9.1.2.7	ネットワーク及びネットワークサービスの利用に関する方針は、ネットワークサービスの利用の監視を対象にする。
8.21.2	ネットワークサービスに必要なセキュリティ対策を実装する。	ネットワークサービスには、接続、プライベートネットワークサービス及びネットワークセキュリティ管理ソリューション（例えば、ファイアウォール、侵入検知システム）が含まれる。これらのサービスは、単純で管理を行わない等級の提供から複雑な付加価値機能の提供まで、広い範囲に及ぶことがある。 それぞれのサービスに必要なセキュリティ対策（例えば、セキュリティ機能、サービスレベル及びサービスの要求事項）を、内部又は外部のネットワークサービス提供者が特定し、実装する。 組織は、ネットワークサービス提供者による、ネットワークサービスに必要なセキュリティ対策の実施を確実にする。	8c-8.21.1	それぞれのネットワークサービスに必要なセキュリティ対策を、内部又は外部のネットワークサービス提供者が特定し、実装する。	手引に関連記載あり	13.1.2.2	それぞれのサービスに必要なセキュリティについての取決め（例えば、セキュリティ特性、サービスレベル、管理上の要求事項）を特定し、組織は、ネットワークサービス提供者によるこれらの対策の実施を確実にする仕組みを整備する。
			8c-8.21.2	組織は、ネットワークサービス提供者による、ネットワークサービスに必要なセキュリティの対策の実施を確実にする。	手引に関連記載あり	–	（対応項なし）
8.21.3	ネットワークサービス提供者の能力を定常的に監視する。	合意したサービスをセキュリティを保って管理できる、ネットワークサービス提供者の能力を定め、定常的に監視する。	8c-8.21.3	合意したサービスをセキュリティを保って管理できる、ネットワークサービス提供者の能力を定め、定常的に監視する。	手引に関連記載あり	13.1.2.1	ネットワークサービスの提供者と合意したサービスをセキュリティを保って管理するために必要なネットワークサービス提供者の能力を定め、常に監視し、監査の権利についてネットワークサービス提供者と合意する。
8.21.4	監査の権利について組織とネットワークサービス提供者との間で合意する、又はネットワークサービス提供者が適切なセキュリティ対策を維持していることを実証するために、ネットワークサービス提供者が提示する第三者認証を利用する。	監査の権利について組織と提供者との間で合意する。 組織は、サービス提供者が適切なセキュリティ対策を維持していることを実証するために、サービス提供者が提示する第三者認証を考慮する。 ネットワークサービスの次のセキュリティ機能を考慮する。 a) ネットワークサービスのセキュリティに適用する技術（例えば、認証、暗号化、ネットワーク接続管理） b) セキュリティ規則及びネットワーク接続規則に従った、ネットワークサービスへのセキュリティを確保した接続のために要求される技術的パラメータ c) 利用者が性能、可用性及び機密性の要求事項に従ってキャッシングの利用を選択できる、キャッシング（例えば、コンテンツ配信ネットワークにおけるキャッシング）及びそのパラメータ d) 必要な場合、ネットワークサービス又はアプリケーションへのアクセスを制限するための、ネットワークサービス利用の手順	8c-8.21.4	監査の権利について組織と提供者との間で合意する。	手引に関連記載あり	–	（対応項なし）
			8c-8.21.5	組織は、サービス提供者が適切なセキュリティ対策を維持していることを実証するために、サービス提供者が提示する第三者認証を考慮する。	手引に関連記載あり	–	（対応項なし）
			8c-8.21.7	ネットワークサービスは次のセキュリティ機能を考慮する。 a) ネットワークサービスのセキュリティに適用する技術 b) セキュリティ規則及びネットワーク接続規則に従った、ネットワークサービスへのセキュリティを確保した接続のために要求される技術的パラメータ c) 利用者が性能、可用性及び機密性の要求事項に従ってキャッシングの利用を選択できる、キャッシング及びそのパラメータ d) 必要な場合、ネットワークサービス又はアプリケーションへのアクセスを制限するための、ネットワークサービス利用の手順	手引に関連記載あり	–	（対応項なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.22	ネットワークの分離 統制目標：情報サービス、利用者及び情報システムは、組織のネットワーク上で、グループごとに分離する。 目的：業務のニーズに基づいて、ネットワークをセキュリティ境界で分割し、それらの間のトラフィックを管理するため。		8.22	ネットワークの分離 管理策 情報サービス、利用者及び情報システムは、組織のネットワーク上で、グループごとに分離する。 目的 業務のニーズに基づいて、ネットワークをセキュリティ境界で分割し、それらの間のトラフィックを管理するため。		13.1.3	ネットワークの分離 情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離する。
8.22.1	ネットワーク領域の境界を定め、ネットワークを分離する。	組織は、大規模なネットワークを幾つかのネットワーク領域に分離し、公衆ネットワーク（すなわち、インターネット）から分離することによって、大規模なネットワークのセキュリティを管理する。 ネットワーク領域は、可能であれば組織の単位（例えば、人事、財務、マーケティング）又は特定の組合せ（例えば、複数の組織の単位に接続しているサーバ領域）に従い、信頼性、重要性及び取扱いに情報を要する度合い（例えば、公開されている領域、デスクトップ領域、サーバ領域、低リスクシステム及び高リスクシステム）に基づいて選択する。 ネットワークの分離は、可能であれば物理的に異なるネットワーク又は論理的に異なるネットワークを用いて行う。 それぞれのネットワーク領域の境界は、明確に定める。 ネットワーク領域間のアクセスを認める場合、アクセスは境界にゲートウェイ（例えば、ファイアウォール、フィルタリングルーター）を設けて制御する。 ネットワーク領域を分離する際の基準及びゲートウェイを通して認められるアクセスの基準は、それぞれの領域のセキュリティ要求事項のアセスメントに基づく。 それぞれのネットワーク領域のセキュリティ要求事項のアセスメントでは、次の事項を評価する。 a) アクセス制御に関するトピック固有の方針（5.15 参照）、アクセス要求事項、並びに処理する情報の価値及び分類に従っているか。 b) 適切なゲートウェイ技術を組み込むための費用対効果を考慮しているか。	8c-8.22.1	組織は、大規模なネットワークを幾つかのネットワーク領域に分離し、公衆ネットワーク（すなわち、インターネット）から分離することによって、大規模なネットワークのセキュリティを管理する。	手引に関連記載あり	13.1.3.1	大規模なネットワークのセキュリティを管理するために、必要に応じてネットワークを幾つかのネットワーク領域に分離（例えば、必要な単位でセグメントを分割）する。
			8c-8.22.2	ネットワーク領域は、可能であれば組織の単位又は特定の組合せに従い、信頼性、重要性及び取扱いに情報を要する度合いに基づいて選択する。	手引に関連記載あり	13.1.3.2	ネットワーク領域は、組織の単位（例えば、人的資源、財務、マーケティング）又は特定の組合せ（例えば、複数の組織の単位に接続しているサーバ領域）に従い、信頼性のレベル（例えば、公開されている領域、デスクトップ領域、サーバ領域）に基づいて選択する。
			8c-8.22.3	ネットワークの分離は、可能であれば物理的に異なるネットワーク又は論理的に異なるネットワークを用いて行う。	手引に関連記載あり	13.1.3.3	ネットワーク領域の分離は、物理的に異なるネットワークワ又は論理的に異なるネットワーク（例えば、仮想私設網）を用いることによって行う。
			8c-8.22.4	それぞれのネットワーク領域の境界は、明確に定める。	手引に関連記載あり	13.1.3.4	各ネットワーク領域の境界は、明確に定める。
			8c-8.22.5	ネットワーク領域間のアクセスを認める場合、アクセスは境界にゲートウェイを設けて制御する。	手引に関連記載あり	13.1.3.5	ネットワーク領域間のアクセスは、境界にゲートウェイ（例えば、ファイアウォール、WAF、プロキシ、リバースプロキシ、次世代ファイアウォール又はフィルタリングルータ）を設けて制御する。
			8c-8.22.6	ネットワーク領域を分離する際の基準及びゲートウェイを通して認められるアクセスの基準は、それぞれの領域のセキュリティ要求事項のアセスメントに基づく。	手引に関連記載あり	13.1.3.6	各ネットワーク領域のセキュリティ要求事項のアセスメントに基づき、ネットワークを領域に分離する際の基準及びゲートウェイを通して認められるアクセスの基準を定める。
			8c-8.22.7	それぞれのネットワーク領域のセキュリティ要求事項のアセスメントでは、次の事項を評価する。 a) アクセス制御に関するトピック固有の方針、アクセス要求事項、並びに処理する情報の価値及び分類に従っているか。 b) 適切なゲートウェイ技術を組み込むための費用対効果を考慮しているか。	手引に関連記載あり	13.1.3.7	各ネットワーク領域のセキュリティ要求事項のアセスメントは、アクセス制御方針、アクセス要求事項、並びに処理する情報の価値及び分類に従い、また、費用対効果を考慮して適切なゲートウェイ技術を組み込む。
8.22.2	無線ネットワークの分離の要件を定め、実装する。	無線ネットワークの分離のために、電波の届く範囲の調整を考慮する。無線ネットワークは、ネットワークの境界がテナントに定められていないため、特別な取扱いを要する。 取扱いに慎重を要する環境では、全ての無線アクセスは、外部接続として取り扱い、そのアクセスがネットワーク管理策（8.20参照）に従ってゲートウェイを通過して内部システムへのアクセスが許可されるまでは、内部ネットワークから分離するように配慮する。 要員が組織のトピック固有の方針に適合する管理されたエンドポイント機器だけを使用する場合、ゲスト用の無線アクセスネットワークを要員用の無線アクセスネットワークから分離する。 ゲスト用のWiFi は、要員によるゲストWiFi の利用を防ぐために、少なくとも要員用のWiFiと同じ制限をもつ。	8c-8.22.8	無線ネットワークの分離のために、電波の届く範囲の調整を考慮する。	手引に関連記載あり	13.1.3.8	ネットワークの境界が十分に定められていない無線ネットワークでは、ネットワーク領域の分離のための特別な取扱い定める。
			（8c-8.22.8参考）	無線ネットワークは、ネットワークの境界が十分に定められていないため、特別な取扱いを要する。	手引に関連記載あり	–	（対応項なし）
			8c-8.22.9	取扱いに慎重を要する環境では、全ての無線アクセスは、外部接続として取り扱い、そのアクセスがネットワーク管理策に従ってゲートウェイを通過して内部システムへのアクセスが許可されるまでは、内部ネットワークから分離するように配慮する。	手引に関連記載あり	13.1.3.9	取扱いに慎重を要する環境では、全ての無線アクセスは、外部接続として取り扱い、そのアクセスがネットワーク管理策の方針に従ってゲートウェイを通過して内部システムへのアクセスが許可されるまでは、内部ネットワークから分離する。
			8c-8.22.10	要員が組織のトピック固有の方針に適合する管理された利用者エンドポイント機器だけを使用する場合、ゲスト用の無線アクセスネットワークを要員用の無線アクセスネットワークから分離する。	手引に関連記載あり	–	（対応項なし）
			8c-8.22.11	ゲスト用のWiFiは、要員によるゲストWiFiの利用を防ぐために、少なくとも要員用のWiFiと同じ制限をもつ。	手引に関連記載あり	–	（対応項なし）
8.22.3	組織内ネットワークを複数セグメントに区切った上で、重要なシステムやサービスを専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。インターネットに接続する必要がある場合は、必要最小限のプロトコルやポートのみに限定する。	特になし。		（統一基準由来）	令和7年版にて追加（情報セキュリティ管理基準以外の由来）	–	（対応項なし）
8.22.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
8.22.5	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
8.22.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
8.23	ウェブフィルタリング 統制目標：悪意のあるコンテンツにさらされることを減らすために、外部ウェブサイトへのアクセスを管理する。 目的：システムがマルウェアによって危険にさらされることを防ぎ、認可されていないウェブ資源へのアクセスを防止するため。		8.23	ウェブフィルタリング 管理策 悪意のあるコンテンツにさらされることを減らすために、外部ウェブサイトへのアクセスを管理することが望ましい。 目的 システムがマルウェアによって危険にさらされることを防ぎ、認可されていないウェブ資源へのアクセスを防止するため。		–	（対応項なし）
8.23.1	外部ウェブサイトのアクセスに関する規則を整備し、外部ウェブサイトへのアクセスを制限し、維持する。	組織は、違法な情報があるウェブサイト、又はウイルス若しくはフィッシングの材料があることが知られているウェブサイトに組織の要員がアクセスするリスクを減らす。リスクを減らす手法として、関係するウェブサイトのIP アドレス又はドメインへのアクセスを阻止することがある。一部のブラウザ及びマルウェア対策技術は、アクセスすることが望ましくないウェブサイトへのアクセスを自動的に阻止、又は阻止するように構成することが可能である。 組織は、要員がアクセスすることが望ましい又は望ましくないウェブサイトの種類を特定する。 組織は次の種類のウェブサイトへのアクセスを選べことを考慮する。 a) 情報アップロード機能をもつウェブサイト。ただし、正当な業務上の理由のため許可されている場合を除く。 b) 悪意のある、又はその疑いのあるウェブサイト（例えば、マルウェア又はフィッシングコンテンツを配信しているウェブサイト） c) C&Cサーバ d) 脅威インテリジェンスで認識した悪意のあるウェブサイト（5.7 参照） e) 違法なコンテンツを供給しているウェブサイト ウェブフィルタリングに関する管理策を導入する前に、組織は、望ましくない又は不適切なウェブサイト及びウェブベースのアプリケーションに対する制限を含め、オンライン資源を安全かつ適切に使用するための規則を確立する。 オンライン資源を安全かつ適切に使用するための規則は最新の状態に保つ。	8c-8.23.1	組織は、違法な情報があるウェブサイト、又はウイルス若しくはフィッシングの材料があることが知られているウェブサイトに組織の要員がアクセスするリスクを減らす。	手引に関連記載あり	–	（対応項なし）
			（8c-8.23.1参考）	リスクを減らす手法として、関係するウェブサイトのIPアドレス又はドメインへのアクセスを阻止することがある。一部のブラウザ及びマルウェア対策技術は、アクセスすることが望ましくないウェブサイトへのアクセスを自動的に阻止、又は阻止するように構成することが可能である。	手引に関連記載あり	–	（対応項なし）
			8c-8.23.2	組織は、要員がアクセスすることが望ましい又は望ましくないウェブサイトの種類を特定する。	手引に関連記載あり	–	（対応項なし）
			8c-8.23.3	組織は次の種類のウェブサイトへのアクセスを選べことを考慮する。 a) 情報アップロード機能をもつウェブサイト。ただし、正当な業務上の理由のため許可されている場合を除く。 b) 悪意のある、又はその疑いのあるウェブサイト c) C&Cサーバ d) 脅威インテリジェンスで認識した悪意のあるウェブサイト e) 違法なコンテンツを供給しているウェブサイト	手引に関連記載あり	–	（対応項なし）
			8c-8.23.4	ウェブフィルタリングに関する管理策を導入する前に、組織は、望ましくない又は不適切なウェブサイト及びウェブベースのアプリケーションに対する制限を含め、オンライン資源を安全かつ適切に使用するための規則を確立する。	手引に関連記載あり	–	（対応項なし）
			8c-8.23.5	オンライン資源を安全かつ適切に使用するための規則は最新の状態に保つ。	手引に関連記載あり	–	（対応項なし）
			8c-8.23.6	ウェブへのアクセスを含む、オンライン資源のセキュリティを促進適切な使用について、要員を訓練する。	手引に関連記載あり	–	（対応項なし）
			8c-8.23.7	オンライン資源のセキュリティを促進適切な使用についての訓練には、組織の規則、セキュリティ上の懸念を報告するための連絡先、及び制限されたウェブ資源に正当な業務上の理由によってアクセスする必要がある場合の例外プロセスを含める。	手引に関連記載あり	–	（対応項なし）
			8c-8.23.8	ウェブサイトで、セキュリティが保たれないことを通知するブラウザアドバイザリを利用者が無効にしないことを確実にするように、要員を訓練する。	手引に関連記載あり	–	（対応項なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.24	暗号の利用 統制目標：暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施する。 目的：事業上及び情報セキュリティの要求事項に従い、暗号に関連する法令、規制及び契約上の要求事項を考慮して、情報の機密性、真正性又は完全性を保護するための暗号の適切かつ効果的な利用を確実にするため。		8.24	暗号の利用 管理策 暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施する。 目的 事業上及び情報セキュリティの要求事項に従い、暗号に関連する法令、規制及び契約上の要求事項を考慮して、情報の機密性、真正性又は完全性を保護するための暗号の適切かつ効果的な利用を確実にするため。		10	暗号
						10.1	暗号による管理策 管理目的：情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。
						10.1.1	暗号による管理策の利用方針 情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施する。
						10.1.2	鍵管理 暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全体にわたって実施する。
8.24.1	情報を保護する上での一般原則も含め、暗号化に関する方針を策定する。	暗号化を利用する場合、次の事項を考慮する。 a）情報を保護するとその一般原則も含め、組織で定義した暗号に関するトピック固有の方針、暗号技術の利用の便益を最大化し、リスクを最小化し、不適切又は誤った利用を回避するには、暗号の利用に関するトピック固有の方針が必要である。 b）要求された保護レベル及び情報の分類を特定し、その結果によって、要求される暗号アルゴリズムの種別、強度及び品質を確立する。 c）持ち運び可能な利用者エンドポイント機器又は記憶媒体に保持され、ネットワークを通じてその機器又は記憶媒体に伝送される情報を保護するための暗号の利用 d）鍵管理に対する取組。これには、暗号鍵の生成及び保護手法、並びに鍵が紛失した場合、危ない（恐）化した場合又は損傷した場合の暗号化された情報の復元手法を含む。 e）次の事項に関する役割及び責任 1）暗号を効果的に利用するための規則の実施 2）鍵生成を含めた鍵管理（8.24参照） f）採用する標準類、並びに組織での利用が承認又は要求されている暗号アルゴリズム、暗号強度、暗号ソリューション及び利用方法 g）暗号化した情報を用いることの、コンテンツ検査（例えば、マルウェアの検出又はコンテンツフィルタリング）に依存する管理策への影響 暗号を効果的に利用するための組織の規則を実施するときには、世界の様々な地域における暗号技術の利用、及び国境を越える暗号化された情報の流れに関する問題に適用される、規制及び国内の制約を考慮する（5.31参照）。 暗号サービスの外部供給者（例えば、認証局）とのサービスレベルに関する合意又は契約の内容は、賠償責任、サービスの信頼性及びサービス提供の応答時間を扱う（5.22参照）。	8c-8.24.1	暗号化を利用する場合、次の事項を考慮する。 a）情報を保護するとその一般原則も含め、組織で定義した暗号に関するトピック固有の方針、暗号技術の利用の便益を最大化し、リスクを最小化し、不適切又は誤った利用を回避するには、暗号の利用に関するトピック固有の方針が必要である。	手引に関連記載あり	10.1.1.1	暗号の利用に関する方針は、業務情報を保護する上での一般原則も含め、暗号による管理策の組織全体での使用に関する管理者の取組みを考慮して定める。
			8c-8.24.1	暗号化を利用する場合、次の事項を考慮する。 b）要求された保護レベル及び情報の分類を特定し、その結果によって、要求される暗号アルゴリズムの種別、強度及び品質を考慮して定める。	手引に関連記載あり	10.1.1.2	暗号の利用に関する方針は、リスクアセスメントに基づく、要求される暗号アルゴリズムの種別、強度及び品質を考慮に入れた、要求された保護レベルの識別を考慮して定める。
			8c-8.24.1	暗号化を利用する場合、次の事項を考慮する。 c）持ち運び可能な利用者エンドポイント機器又は記憶媒体に保持され、ネットワークを通じてその機器又は記憶媒体に伝送される情報を保護するための暗号の利用	手引に関連記載あり	10.1.1.3	暗号の利用に関する方針は、持ち運び可能な取り出し取外し可能な媒体装置又は通信によって伝送される情報を、保護するための暗号の利用を考慮して定める。
			8c-8.24.1	暗号化を利用する場合、次の事項を考慮する。 d）鍵管理に対する取組。これには、暗号鍵の生成及び保護手法、並びに鍵が紛失した場合、危ない（恐）化した場合又は損傷した場合の暗号化された情報の復元手法を含む。	手引に関連記載あり	10.1.1.4	暗号の利用に関する方針は、暗号鍵の保護手法、及び鍵が紛失、危険又は損傷した暗号の暗号化された情報の復元手法を含む、鍵管理に対する取組みを考慮して定める。
			8c-8.24.1	暗号化を利用する場合、次の事項を考慮する。 e）次の事項に関する役割及び責任 1）暗号を効果的に利用するための規則の実施 2）鍵生成を含めた鍵管理	手引に関連記載あり	10.1.1.5	暗号の利用に関する方針は、この方針の実施の責任や鍵生成を含めた鍵管理に対する責任など、役割及び責任を考慮して定める。
			8c-8.24.1	暗号化を利用する場合、次の事項を考慮する。 f）採用する標準類、並びに組織での利用が承認又は要求されている暗号アルゴリズム、暗号強度、暗号ソリューション及び利用方法	手引に関連記載あり	10.1.1.6	暗号の利用に関する方針は、組織全体にわたって効果的に実施するために採用する標準類（業務プロセス用いるソリューションの選択）を考慮して定める。
			8c-8.24.1	暗号化を利用する場合、次の事項を考慮する。 g）暗号化した情報を用いることの、コンテンツ検査に依存する管理策への影響	手引に関連記載あり	10.1.1.7	暗号の利用に関する方針は、暗号化した情報を用いることの、情報内容の検査（例えば、マルウェアの検出）に依存する管理策への影響を考慮して定める。
			8c-8.24.2	暗号を効果的に利用するための組織の規則を実施するときには、世界の様々な地域における暗号技術の利用、及び国境を越える暗号化された情報の流れに関する問題に適用される、規制及び国内の制約を考慮する。	手引に関連記載あり	10.1.1.8	暗号に関わる組織の方針を実施するときには、世界の様々な地域における暗号技術の利用、及び国境を越える暗号化された情報の流れに関する問題に適用される、規制及び国内の制約を含める。
			8c-8.24.3	暗号サービスの外部供給者とのサービスレベルに関する合意又は契約の内容は、賠償責任、サービスの信頼性及びサービス提供の応答時間を扱う。	手引に関連記載あり	10.1.2.19	暗号サービスの外部供給者（例えば、認証局）とのサービスレベルに関する合意又は契約の内容は、賠償責任、サービスの信頼性及びサービス提供のための応答時間に関する事項を含める。
8.24.2	鍵管理のための暗号鍵を生成、保管、保存、読出し、配布、利用停止、改変、紛失及び破壊するための、セキュリティを保ったプロセス及び手順を鍵し、実施する。	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 a）種々の暗号システム及び種々のアプリケーションのために鍵を生成する。 b）公開鍵証明書を発行し、入手する。 c）意図するエンティティに鍵を配布する。これには、受領時に、鍵をどのような方法で活性化するか（使える状態にするか）も含む。 d）鍵を保管する。これには、認可されている利用者がどのような方法で鍵にアクセスするかも含む。 e）鍵を変更又は更新する。これには、鍵をいつ、どのような方法で変更するかの規則も含む。 f）危たい（恐）化した鍵に対処する。 g）鍵を無効にする（例えば、鍵が危たい（恐）化した場合、又は利用者が組織を離脱した場合（後者の場合には、鍵は保存する。））。これには、鍵をどのような方法で取消し又は非活性化するかも含む。 h）紛失した鍵又は破損した鍵を回復する。 i）鍵をバックアップ又は保存する。 j）鍵を破壊する。 k）鍵管理に関連する活動を記録し、監査する。 l）鍵管理に関する組織の規則に従って鍵を一定期間だけ利用できるように、鍵の活性化及び非活性化の日付を設定する。 m）暗号鍵へのアクセスに関する法的要求（例えば、裁判での証拠として、暗号化された情報を平文で求められた場合）の取扱い 適切な鍵管理には、暗号鍵を生成、保管、保存、読出し、配布、利用停止及び破壊するための、セキュリティを保った プロセスが必要になる。 全ての暗号鍵は、改変及び紛失から保護する。 秘密鍵及びプライベート鍵は、認可されていない利用及び開示から保護する。 鍵の生成、保管及び保存のために用いる装置は、物理的に保護する。 暗号鍵の完全性に加え、多くの事例では、公開鍵の真正性も考慮する。	8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 a）種々の暗号システム及び種々のアプリケーションのために鍵を生成する。	手引に関連記載あり	10.1.2.5	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つた手法に基づき、種々の暗号システム及び種々のアプリケーションのための鍵を生成する。
			8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 b）公開鍵証明書を発行し、入手する。	手引に関連記載あり	10.1.2.6	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つた手法に基づき、公開鍵証明書を発行し、入手する。
			8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 c）意図するエンティティに鍵を配布する。これには、受領時に、鍵をどのような方法で活性化するか（使える状態にするか）も含む。	手引に関連記載あり	10.1.2.7	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つた手法に基づき、意図するエンティティに鍵を配布する。これには、受領時に、鍵をどのような方法で活性化するか（使える状態にするか）についても含める。
			8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 d）鍵を保管する。これには、認可されている利用者がどのような方法で鍵にアクセスするかも含む。	手引に関連記載あり	10.1.2.8	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つた手法に基づき、鍵を保管する。これには、認可されている利用者がどのような方法で鍵にアクセスするかも含める。
			8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 e）鍵を変更又は更新する。これには、鍵をいつ、どのような方法で変更するかの規則も含む。	手引に関連記載あり	10.1.2.9	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つた手法に基づき、鍵を変更又は更新する。これには、鍵をいつ、どのような方法で変更するかの規則も含める。
			8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 f）危たい（恐）化した鍵に対処する。	手引に関連記載あり	10.1.2.10	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つた手法に基づき、危険になった鍵に対処する。
			8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 g）鍵を無効にする。これには、鍵をどのような方法で取消し又は非活性化するかも含む。	手引に関連記載あり	10.1.2.11	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つた手法に基づき、鍵を無効にする（例えば、鍵が危険になった場合、利用者が組織を離脱した場合、後者の場合には、鍵は保存する。）。これには、鍵をどのような方法で取消し又は非活性化するかも含める。
			8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 h）紛失した鍵又は破損した鍵を回復する。	手引に関連記載あり	10.1.2.12	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つた手法に基づき、紛失した鍵又は破損した鍵を回復する。
			8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 i）鍵をバックアップ又は保存する。	手引に関連記載あり	10.1.2.13	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つた手法に基づき、鍵をバックアップ又は保存する。
			8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 j）鍵を破壊する。	手引に関連記載あり	10.1.2.14	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つた手法に基づき、鍵を破壊する。
			8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 k）鍵管理に関連する活動を記録し、監査する。	手引に関連記載あり	10.1.2.15	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つた手法に基づき、鍵管理に関連する活動を記録し、監査する。
			8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 l）鍵管理に関する組織の規則に従って鍵を一定期間だけ利用できるように、鍵の活性化及び非活性化の日付を設定する。	手引に関連記載あり	10.1.2.16	不適切な使用を起こりにくくするために、鍵の活性化及び非活性化の期日を定め、これによって、鍵管理の方針で定めた期間内でだけ鍵を使用できるようにする。
			8c-8.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つた手法に基づくことを考慮する。 m）暗号鍵へのアクセスに関する法的要求の取扱い	手引に関連記載あり	–	（対応項なし）
			（8c-8.24.4参考）	適切な鍵管理には、暗号鍵を生成、保管、保存、読出し、配布、利用停止及び破壊するための、セキュリティを保った プロセスが必要になる。	手引に関連記載あり	–	（対応項なし）
			8c-8.24.5	全ての暗号鍵は、改変及び紛失から保護する。	手引に関連記載あり	10.1.2.3	全ての暗号鍵は、改変及び紛失から保護する。
			8c-8.24.6	秘密鍵及びプライベート鍵は、認可されていない利用及び開示から保護する。	手引に関連記載あり	10.1.2.17	秘密鍵及びプライベート鍵は、認可されていない利用及び開示から保護するためセキュリティを保って管理し、公開鍵は、真正性を保つ。
			8c-8.24.7	鍵の生成、保管及び保存のために用いる装置は、物理的に保護する。	手引に関連記載あり	10.1.2.4	鍵の生成、保管及び保存のために用いられる装置は、物理的に保護する。
			8c-8.24.8	暗号鍵の完全性に加え、多くの事例では、公開鍵の真正性も考慮する。	手引に関連記載あり	10.1.2.17	秘密鍵及びプライベート鍵は、認可されていない利用及び開示から保護するためセキュリティを保って管理し、公開鍵は、真正性を保つ。
8.24.3	暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」に基づき、情報システムで使用する暗号及び電子署名のアルゴリズム及び鍵長並びにそれを利用した安全なプロトコルを定める。	特になし。	–	（統一基準由来）	令和7年版にて追加（情報セキュリティ管理基準以外の由来）	–	（対応項なし）
8.24.4	暗号化及び電子署名に使用するアルゴリズムは鍵長が危たい（恐）化した場合又はそれらを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を鍵備する。	特になし。	–	（統一基準由来）	令和7年版にて追加（情報セキュリティ管理基準以外の由来）	–	（対応項なし）
8.24.5	クラウドサービス利用者に、当該利用者の管理する情報の暗号化に用いる暗号鍵を管理する機能を提供し又は当該利用者が暗号鍵を管理する方法についての情報を提供する。	特になし。	–	（統一基準由来）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	10.1.2.20.PB	クラウドサービス事業者は、クラウドサービス利用者に、当該利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供する。
8.24.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
8.24.7	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
8.25	セキュリティに配慮した開発のライフサイクル 統制目標：ソフトウェア及びシステムのセキュリティに配慮した開発のための規則を確立し、適用する。 目的：情報セキュリティを、ソフトウェア及びシステムのセキュリティに配慮した開発ライフサイクルにおいて設計し、実装することを確実にするため。		8.25	セキュリティに配慮した開発のライフサイクル 管理策 ソフトウェア及びシステムのセキュリティに配慮した開発のための規則を確立し、適用する。 目的 情報セキュリティを、ソフトウェア及びシステムのセキュリティに配慮した開発ライフサイクルにおいて設計し、実装することを確実にするため。		14.2	開発及びサポートプロセスにおけるセキュリティ 管理目的：情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。
						14.2.1	セキュリティに配慮した開発のための方針 ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用する。
8.25.1	セキュリティに配慮したサービス、アーキテクチャ、ソフトウェア及びシステムを構築するための、開発ライフサイクルを設計する。	セキュリティに配慮したサービス、アーキテクチャ、ソフトウェア及びシステムを構築するには、セキュリティに配慮した開発方が要となる。セキュリティに配慮した開発を確立するために、次の側面を考慮する。 a）開発環境、テスト環境及び本番環境の分離（8.31参照） b）ソフトウェア開発のライフサイクルにおける、次に関するセキュリティに関する手引 1）ソフトウェア開発の方法論におけるセキュリティ（8.28及び8.27参照） 2）用いる各プログラム言語について定めた、セキュリティに配慮したコーディングに関する指針（8.28参照） c）仕様変更及び設計段階におけるセキュリティ要求事項（5.8参照） d）プロジェクトにおけるセキュリティの確認項目（5.8参照） e）回帰テスト、コードスキャン、侵入テストなどのシステム及びセキュリティのテスト（8.29参照） f）ソースコード及び構成ファイルのためのセキュリティが保たれたリポジトリ（8.4及び8.9参照） g）版の管理におけるセキュリティ（8.32参照） h）アプリケーションセキュリティに関し必要な知識及び訓練（8.28参照） i）ぜい弱性を防止し、発見し、修正するに当たっての開発者の能力（8.28参照） j）ライセンスに関する将来の問題を回避しつつ、費用対効果の高いソリューションを確実にするため、ライセンスの要求事項及び代替案（5.32参照） 開発を外部委託した場合、組織は、供給者がセキュリティに配慮した開発のための組織の規則を順守していることの保証を得る（8.30参照）。	（8d-8.25参考）	セキュリティに配慮したサービス、アーキテクチャ、ソフトウェア及びシステムを構築するには、セキュリティに配慮した開発方が要となる。	手引に関連記載あり	–	（対応項なし）
			8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 a）開発環境、テスト環境及び本番環境の分離	手引に関連記載あり	14.2.1.1	セキュリティに配慮した開発のための方針には、開発環境のセキュリティを含める。
			8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 b）ソフトウェア開発のライフサイクルにおける、次に関するセキュリティに関する手引 1）ソフトウェア開発の方法論におけるセキュリティ 2）用いる各プログラム言語について定めた、セキュリティに配慮したコーディングに関する指針	手引に関連記載あり	14.2.1.2	セキュリティに配慮した開発のための方針には、ソフトウェア開発のライフサイクルにおける、以下の2点の手引きを含める。 1）ソフトウェア開発の方法論におけるセキュリティ 2.用いる各プログラミング言語について定めた、セキュリティに配慮したコーディングに関する指針
			8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 c）仕様変更及び設計段階におけるセキュリティ要求事項	手引に関連記載あり	14.2.1.3	セキュリティに配慮した開発のための方針には、設計段階におけるセキュリティ要求事項を含める。
			8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 d）プロジェクトにおけるセキュリティの確認項目	手引に関連記載あり	14.2.1.4	セキュリティに配慮した開発のための方針には、プロジェクトの開発の節目ごとにおけるセキュリティの確認項目を含める。
			8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 e）回帰テスト、コードスキャン、侵入テストなどのシステム及びセキュリティのテスト	手引に関連記載あり	–	（対応項なし）
			8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 f）ソースコード及び構成ファイルのためのセキュリティが保たれたリポジトリ	手引に関連記載あり	14.2.1.5	セキュリティに配慮した開発のための方針には、セキュリティが保たれたリポジトリを含める。
			8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 g）版の管理におけるセキュリティ	手引に関連記載あり	14.2.1.6	セキュリティに配慮した開発のための方針には、版の管理におけるセキュリティを含める。
			8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 h）アプリケーションセキュリティに関し必要な知識及び訓練	手引に関連記載あり	14.2.1.7	セキュリティに配慮した開発のための方針には、アプリケーションのセキュリティに関して必要な知識を含める。
			8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 i）ぜい弱性を防止し、発見し、修正するに当たっての開発者の能力	手引に関連記載あり	14.2.1.8	セキュリティに配慮した開発のための方針には、ぜい弱性を回避、発見及び修正するに当たっての開発者の能力を含める。
			8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 j）ライセンスに関する将来の問題を回避しつつ、費用対効果の高いソリューションを確実にするため、ライセンスの要求事項及び代替案	手引に関連記載あり	–	（対応項なし）
			8d-8.25.2	開発を外部委託した場合、組織は、供給者がセキュリティに配慮した開発のための組織の規則を順守していることの保証を得る。	手引に関連記載あり	14.2.1.12	開発を外部委託した場合、組織は、その外部関係者がセキュリティに配慮した開発のための規則を順守していることの保証を得る。
8.25.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.26	アプリケーションセキュリティの要求事項 統制目標：アプリケーションを開発又は取得する場合、情報セキュリティ要求事項を特定し、規定し、承認する。 目的：アプリケーションを開発又は取得する場合、全ての情報セキュリティ要求事項を特定し、対応することを確実にするため。		8.26	アプリケーションセキュリティの要求事項 管理策 アプリケーションを開発又は取得する場合、情報セキュリティ要求事項を特定し、規定し、承認する。 目的 アプリケーションを開発又は取得する場合、全ての情報セキュリティ要求事項を特定し、対応することを確実にするため。		14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮 公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護する。
						14.1.3	アプリケーションサービスのトランザクションの保護 アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。 ・不完全な通信 ・誤った通信経路設定 ・認可されていないメッセージの変更 ・認可されていない開示 ・認可されていないメッセージの複製又は再生
8.26.1	アプリケーションを開発又は取得する際の、情報セキュリティ要求事項を定義する。	アプリケーションセキュリティの要求事項やリスクアセスメントを通じて特定し、規定する。 アプリケーションセキュリティの要求事項は、情報セキュリティの専門家の支援を受けて作成することを考慮する。アプリケーションセキュリティの要求事項は、アプリケーションの目的に応じて、幅広いトピックにわたることがある。 アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 a) エンティティの識別情報の信頼のレベル［例えば、認証を通じて（5.17、8.2及び8.5参照）］ b) アプリケーションで処理する情報の種類及び分類レベルの特定 c) アプリケーション内のデータ及び機能へのアクセス及びアクセスのレベルを分離するための要件 d) 悪意のある攻撃又は意図しない事象の中断・阻害に対するレジリエンス（例えば、バッファオーバーフローやSQL インジェクションからの保護） e) トランザクションが生成、処理、完結又は保管される法域における法令及び規制上の要求事項 f) 関与する全ての当事者のプライバシーの必要性 g) 秘密情報の保護に関する要求事項 h) 処理、転送及び保持するデータの保護 i) 関与する全ての当事者間の通信セキュリティを保って暗号化する必要性 j) 完全性の確認及び入力の妥当性確認を含む入力の管理策 k) 自動化した管理策（例えば、承認の回数制限又は二重承認の要求） l) 出力にアクセスできる人及びその認可を考慮した出力の管理策 m) 自由記述“欄の内容に関する制限、これは、機密データ（例えば、個人データ）を管理されずに保存することにつながり得るため。 n) トランザクションのログ取得及び監視、否認防止の要求事項など、業務プロセスに由来する要求事項 o) 他のセキュリティ管理策によって必要となる要求事項（例えば、ログ取得及び監視システム並びに情報漏えい検知システムとのインタフェース） p) エラーメッセージの取扱い 組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 a) 各当事者が提示する自らの識別情報について、それぞれが互いに要求し合う信頼のレベル b) 交換又は処理する情報の完全性に必要な信頼のレベル、及び完全性の欠如を特定するための仕組み（例えば、巡回冗長検査、ハッシュ化、ディジタル署名） c) 重要な取引文書の内容の承認、その発行、又はその文書への署名を誰が行えるかについての認可プロセス d) 重要な文書の機密性、完全性及び発送・受領の証明、並びに否認防止（例えば、入札手続、契約手続に関連する契約） e) トランザクションの機密性及び完全性（例えば、注文、納入先の宛名情報及び受領確認） f) トランザクションの機密性を維持する期間に関する要求事項 g) 保険及びその他の契約上の要求事項 電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。 a) 注文情報の機密性及び完全性を維持するための要求事項 b) 顧客から提供された支払い情報を検証するための、適切な検査の度合い c) トランザクション情報の紛失又は重複の防止 d) トランザクションの詳細を、公開している環境の外で保管すること（例えば、組織のイントラネット内に設置しているデータ保存環境とすること、及びインターネットから直接アクセス可能な電子記憶媒体上にそれらを保持して危険にさらさないこと） e) 信頼できる専門機関を利用（例えば、ディジタル署名又はディジタル証明書の発行・維持の目的で利用）する場合、エンド ツー エンドの証明書又は署名管理プロセスを通じたセキュリティの統合及び組込み これらの考慮事項の幾つかは、法的要求事項を考慮に入れながら、暗号（8.24参照）を適用することによって対応することが可能である（5.31～5.36を参照。特に、暗号に関連する法令については、5.31を参照。）。	8d-8.26.1	アプリケーションセキュリティの要求事項やリスクアセスメントを通じて特定し、規定する。	手引に関連記載あり	–	（対応現なし）
			8d-8.26.2	アプリケーションセキュリティの要求事項は、情報セキュリティの専門家の支援を受けて作成することを考慮する。	手引に関連記載あり	–	（対応現なし）
			(8d-8.26.2参考)	アプリケーションセキュリティの要求事項は、アプリケーションの目的に応じて、幅広いトピックにわたることがある。	手引に関連記載あり	–	（対応現なし）
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 a) エンティティの識別情報の信頼のレベル	手引に関連記載あり	–	（対応現なし）
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 b) アプリケーションで処理する情報の種類及び分類レベルの特定	手引に関連記載あり	–	（対応現なし）
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 c) アプリケーション内のデータ及び機能へのアクセス及びアクセスのレベルを分離することの必要性	手引に関連記載あり	–	（対応現なし）
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 d) 悪意のある攻撃又は意図しない事象の中断・阻害に対するレジリエンス	手引に関連記載あり	14.1.2.15	攻撃に対する対応力（resilience）の要求事項（関連するアプリケーションサーバを保護するための要求事項、及びリービスの提供に必要となるネットワーク相互接続の可用性を確実にするための要求事項を含む。）を定める。
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 e) トランザクションが生成、処理、完結又は保管される法域における法令及び規制上の要求事項	手引に関連記載あり	–	（対応現なし）
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 f) 関与する全ての当事者のプライバシーの必要性 g) 秘密情報の保護に関する要求事項	手引に関連記載あり	14.1.3.2	アプリケーションサービスのトランザクションでは、トランザクションの種々の面において、以下を確実にする仕組みを整備する。 1）全ての当事者の秘密認証情報は、有効であり、かつ、検証を経ている 2）トランザクションが秘密に保たれている 3）全ての当事者に関係するプライバシーを守っている
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 h) 処理、転送及び保持するデータの保護	手引に関連記載あり	–	（対応現なし）
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 i) 関与する全ての当事者間の通信セキュリティを保って暗号化する必要性	手引に関連記載あり	14.1.3.3	アプリケーションサービスのトランザクションでは、関わる全ての当事者間の通信経路を暗号化する。
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 j) 完全性の確認及び入力の妥当性確認を含む入力の管理策	手引に関連記載あり	–	（対応現なし）
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 k) 自動化した管理策	手引に関連記載あり	–	（対応現なし）
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 l) 出力にアクセスできる人及びその認可も考慮した出力の管理策	手引に関連記載あり	–	（対応現なし）
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 m) “自由記述”欄の内容に関する制限、これは、機密データを管理されずに保存することにつながり得るため。	手引に関連記載あり	–	（対応現なし）
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 n) トランザクションのログ取得及び監視、否認防止の要求事項など、業務プロセスに由来する要求事項	手引に関連記載あり	–	（対応現なし）
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 o) 他のセキュリティ管理策によって必要となる要求事項	手引に関連記載あり	–	（対応現なし）
			8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 p) エラーメッセージの取扱い	手引に関連記載あり	–	（対応現なし）
			8d-8.26.4	組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 a) 各当事者が提示する自らの識別情報について、それぞれが互いに要求し合う信頼のレベル	手引に関連記載あり	14.1.2.1	公衆ネットワークを経由するアプリケーションサービスは、各当事者が提示する自らの識別情報について、それぞれが互いに要求し合う信頼（例えば、認証）のレベルを定める。
			8d-8.26.4	組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 b) 交換又は処理する情報の完全性に必要な信頼のレベル、及び完全性の欠如を特定するための仕組み	手引に関連記載あり	–	（対応現なし）
			8d-8.26.4	組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 c) 重要な取引文書の内容の承認、その発行、又はその文書への署名を誰が行えるかについての認可プロセス	手引に関連記載あり	14.1.2.2	公衆ネットワークを経由するアプリケーションサービスは、重要な取引文書の内容の承認、その発行、及びその文書への署名を誰が行うかについての認可プロセスを明確にする。
			8d-8.26.4	組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 d) 重要な文書の機密性、完全性及び発送・受領の証明、並びに否認防止	手引に関連記載あり	14.1.2.4	公衆ネットワークを経由するアプリケーションサービスは、入札手続、契約手続などにおいて、重要な文書の機密性、完全性及び発送・受領の証明、並びに契約の当初的止に関する要求事項を決定し、それを達成する。
					手引に関連記載あり	14.1.2.5	公衆ネットワークを経由するアプリケーションサービスは、重要な文書の完全性についの、信頼のレベルを定める。
			8d-8.26.4	組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 e) トランザクションの機密性及び完全性	手引に関連記載あり	14.1.2.7	公衆ネットワークを経由するアプリケーションサービスは、注文のトランザクション、支払い情報、納入先の宛名情報及び受領確認の機密性及び完全性を維持する。
			8d-8.26.4	組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 f) トランザクションの機密性を維持する期間に関する要求事項	手引に関連記載あり	–	（対応現なし）
			8d-8.26.4	組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 g) 保険及びその他の契約上の要求事項	手引に関連記載あり	14.1.2.13	公衆ネットワークを経由するアプリケーションサービスは、保険の要件を決定する。
			8d-8.26.5	電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。 a) 注文情報の機密性及び完全性を維持するための要求事項	手引に関連記載あり	14.1.2.10	公衆ネットワークを経由するアプリケーションサービスは、注文情報の機密性及び完全性を維持するために要求される保護のレベルを定める。
			8d-8.26.5	電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。 b) 顧客から提供された支払い情報を検証するための、適切な検査の度合い	手引に関連記載あり	14.1.2.8	公衆ネットワークを経由するアプリケーションサービスは、顧客から提供された支払い情報を検証するため、適切な検査の度合いを定める。
			8d-8.26.5	電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。 c) トランザクション情報の紛失又は重複の防止	手引に関連記載あり	14.1.2.11	公衆ネットワークを経由するアプリケーションサービスは、トランザクション情報の紛失又は重複を防止する。
			8d-8.26.5	電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。 d) トランザクションの詳細を、公開している環境の外で保管すること	手引に関連記載あり	14.1.3.5	アプリケーションサービスのトランザクションでは、その詳細情報を、公開している環境の外（例えば、組織のイントラネット内に設置しているデータ保存環境）で保管すること、及びインターネットから直接アクセス可能な記憶媒体上にそれらを保持して危険にさらさないことを確実にする仕組みを整備する。
			8d-8.26.5	電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。 e) 信頼できる専門機関を利用する場合、エンド ツー エンドの証明書又は署名管理プロセスを通じたセキュリティの統合及び組込み	手引に関連記載あり	14.1.3.6	アプリケーションサービスのトランザクションでは、信頼できる専門機関を利用（例えば、ディジタル署名又はディジタル証明書の発行・維持の目的での利用）する場合、エンドツーエンドの証明書及びノ又は署名管理プロセスを通したセキュリティを統合し、組み込む。
			(8d-8.26参考)	これらの考慮事項の幾つかは、法的要求事項を考慮に入れながら、暗号を適用することによって対応することが可能である。	手引に関連記載あり	–	（対応現なし）
8.26.2	クラウドサービス利用者に、電子証明書を用いた署名等、提供するアプリケーションやコンテンツの改ざん等がなく真正なものであることを確認できる手段を提供する。	特になし。	–	（統一基準由来）	令和7年版にて追加（情報セキュリティ管理基準以外の由来）	–	（対応現なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.27	セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則 統制目標：セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの開発活動に対して適用する。 目的：情報システムを、開発のライフサイクルにおいてセキュリティに配慮して設計し、実装し、運用することを確実にするため。		8.27	セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則 管理策 セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの開発活動に対して適用する。 目的 情報システムを、開発のライフサイクルにおいてセキュリティに配慮して設計し、実装し、運用することを確実にするため。		14.2.5	セキュリティに配慮したシステム構築の原則 セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用する。
8.27.1	セキュリティに配慮したシステム構築の原則を整備する。	セキュリティに配慮したシステム構築の原則を確立し、文書化し、情報システム構築活動に適用する。 セキュリティは、全てのアーキテクチャ層（業務、データ、アプリケーション及び技術）において設計する。新技術は、セキュリティのリスクを分析し、その設計と既知の攻撃パターンに照らしてレビューする。セキュリティに配慮したシステム構築の原則は、利用者認証技術、セキュリティを保ったセッション管理及びデータの妥当性確認並びにサニタイジングに関する詳細管理策とする。 セキュリティに配慮したシステム構築の原則には、次の分析を含める。 a）特定した脅威から情報及びシステムを保護するために必要なあらゆるセキュリティ管理策 b）セキュリティ事象を防止し、検知し又はそれに対応するセキュリティ管理策の機能 c）特定の業務プロセスに必要な特定のセキュリティ管理策（例えば、取扱いに慎重を要する情報の暗号化、完全性の確認及び情報のディジタル著名） d）セキュリティ管理策をどこでどのように適用するか（例えば、セキュリティアーキテクチャ及び技術基盤と統合すること）。 e）個々のセキュリティ管理策（手動及び自動）を連携し、統合した管理策群を作るの方法 セキュリティに配慮したシステム構築の原則では、次の事項を考慮に入れる。 a）セキュリティアーキテクチャと統合する必要性 b）技術的なセキュリティ基盤（例えば、公開鍵基盤（PKI）、識別情報及びアクセスの管理（IAM）、データ漏えい防止、動的アクセス管理） c）選択した技術を開発し、サポートする組織の能力 d）セキュリティ要求事項を満たすための費用、時間及び複雑さ e）最新の優れた慣行	8d-8.27.1	セキュリティに配慮したシステム構築の原則を確立し、文書化し、情報システム構築活動に適用する。	手引に関連記載あり	14.2.5.1	セキュリティに配慮したシステム構築の原則に基づき、情報システムの構築手順を確立し、文書化し、組織の情報システム構築活動に適用する。
			8d-8.27.2	セキュリティは、全てのアーキテクチャ層（業務、データ、アプリケーション及び技術）において設計する。新技術は、セキュリティのリスクを分析し、その設計と既知の攻撃パターンに照らしてレビューする。	手引に関連記載あり	14.2.5.2	セキュリティは、情報セキュリティの必要性とアクセス性の必要性との均衡を保ちながら、全てのアーキテクチャ層（業務、データ、アプリケーション及び技術）において設計する。
					手引に関連記載あり	14.2.5.3	新技術は、セキュリティ上のリスクについて分析し、その設計と既知の攻撃パターンに照らしてレビューする。
			（8d-8.27参考）	セキュリティに配慮したシステム構築の原則は、利用者認証技術、セキュリティを保ったセッション管理及びデータの妥当性確認並びにサニタイジングに関する詳細管理策とする。	手引に関連記載あり	–	（対応項なし）
			8d-8.27.3	セキュリティに配慮したシステム構築の原則には、次の分析を含める。 a)特定した脅威から情報及びシステムを保護するために必要なあらゆるセキュリティ管理策 b)①セキュリティ事象を防止し、検知し又はそれに対応するセキュリティ管理策の機能 c)特定の業務プロセスに必要な特定のセキュリティ管理策 d)①セキュリティ管理策をどこでどのように適用するか、 e)①個々のセキュリティ管理策（手動及び自動）を連携し、統合した管理策群を作る方法	手引に関連記載あり	–	（対応項なし）
			8d-8.27.4	セキュリティに配慮したシステム構築の原則では、次の事項を考慮に入れる。 a) セキュリティアーキテクチャと統合する必要性 b) 技術的なセキュリティ基盤 c) 選択した技術を開発し、サポートする組織の能力 d) セキュリティ要求事項を満たすための費用、時間及び複雑さ e) 最新の優れた慣行	手引に関連記載あり	–	（対応項なし）
8.27.2	システム構築の原則に基づいた、システム構築を実施する。	セキュリティに配慮したシステム構築には、次の事項を含める。 a）設計によるセキュリティ（セキュリティバイデザイン）、多層防御、デフォルトでのセキュリティ、デフォルト拒否、故障時のセキュリティ、外部アプリケーションからの入力を信用しない、導入時のセキュリティ、適応の想定、最小特権、利便性及び管理性、最小機能などの、セキュリティアーキテクチャの原則の使用 b）情報セキュリティのもい弱性を特定し、セキュリティ管理策を規定することを確実にし、セキュリティ要求事項を満たす助けとなる、セキュリティ指向の設計レビュー c）要求事項を完全には満たしていない（例えば、安全に関する要求事項を優先するため）セキュリティ管理策の文書化及び正式な承認 d）システムの要塞化（hardening） 組織は、次のようなゼロトラスト（zero trust）の原則を考慮する。 a）組織の情報システムは既に侵害されていることを想定し、ネットワーク境界のセキュリティだけに依存しない。 b）情報システムへのアクセスにおいて決して信頼せず、常に検証する取組を採用する。 c）情報システムへの要求がエンドツーエンドで暗号化されることを確実にする。 d）情報システムへの各要求を、組織の内部からのものであっても、公開の外部ネットワークから来たかのように検証する（すなわち、組織の境界の内側又は外側のいずれであれ、自動的に信頼することはしない。）。 e）最小特権及び動的アクセス制御手法を使用する（5.15、5.18及び8.2参照）。これは、情報又はシステムへの要求の認証及び認可を、認証情報（5.17参照）、利用者識別情報（5.16参照）、エンドポイント機器に関するデータ、データ分類（5.12参照）などの、状況に関する情報に基づいて行うことを含む。 f）認証情報（5.17参照）及び利用者識別情報（5.16参照）、エンドポイント機器に関するデータ、並びにデータ分類（5.12参照）を含めた情報に基づいて、例えば、強力な認証［多要素認証（8.5参照）など］を実行することによって、情報システムへの要求を常に認証し、認可要求の妥当性を常に確認する。	8d-8.27.5	セキュリティに配慮したシステム構築には、次の事項を含める。 a) “設計によるセキュリティ（セキュリティバイデザイン）”、“多層防御”、“デフォルトでのセキュリティ”、“デフォルト拒否”、“故障時のセキュリティ”、“外部アプリケーションからの入力を信用しない”、“導入時のセキュリティ”、“適応の想定”、“最小特権”、“利便性及び管理性”、“最小機能”などの、セキュリティアーキテクチャの原則の使用 b) 情報セキュリティのもい弱性を特定し、セキュリティ管理策を規定することを確実にし、セキュリティ要求事項を満たす助けとなる、セキュリティ指向の設計レビュー c) 要求事項を完全には満たしていないセキュリティ管理策の文書化及び正式な承認 d) システムの要塞化（hardening）	手引に関連記載あり	–	（対応項なし）
			8d-8.27.6	組織は、次のような“ゼロトラスト（zero trust）”の原則を考慮する。 a) 組織の情報システムは既に侵害されていることを想定し、ネットワーク境界のセキュリティだけに依存しない。 b) 情報システムへのアクセスにおいて“決して信頼せず、常に検証する”取組を採用する。 c) 情報システムへの要求がエンド ツー エンドで暗号化されることを確実にする。 d) 情報システムへの各要求を、組織の内部からのものであっても、公開の外部ネットワークから来たかのように検証する（すなわち、組織の境界の内側又は外側のいずれであれ、自動的に信頼することはしない。）。 e) “最小特権”及び動的アクセス制御手法を使用する。これは、情報又はシステムへの要求の認証及び認可を、認証情報、利用者識別情報、利用者エンドポイント機器に関するデータ、並びにデータ分類などの、状況に関する情報に基づいて行うことを含む。 f) 認証情報及び利用者識別情報、利用者エンドポイント機器に関するデータ、並びにデータ分類を含めた情報に基づいて、例えば、強力な認証を実行することによって、情報システムへの要求を常に認証し、認可要求の妥当性を常に確認する。	手引に関連記載あり	–	（対応項なし）
8.27.3	システム構築の原則及び構築手順を定期的にレビューする。	確立したセキュリティに配慮したシステム構築の原則は、該当する場合には、組織と組織が外部委託した供給者との間の、契約及び同実力をもつその他の合意を通じて、外部委託した情報システムの開発にも適用する。 組織は、供給者のセキュリティに配慮したシステム構築のの行為が組織のニーズと一致することを確実にする。 セキュリティに配慮したシステム構築の原則及び確立した構築手順は、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするために、定期的にレビューする。 セキュリティに配慮したシステム構築の原則及び確立した構築手順が、新規の潜在的な脅威に対抗するという点で常に最新であること、及び適用される技術及びソリューションの進展に継続して適用可能であることを確実にするために、定期的にレビューする。	8d-8.27.7	確立したセキュリティに配慮したシステム構築の原則は、該当する場合には、組織と組織が外部委託した供給者との間の、契約及び同実力をもつその他の合意を通じて、外部委託した情報システムの開発にも適用する。	手引に関連記載あり	14.2.5.6	セキュリティに配慮したシステム構築の原則は、組織と組織が外部委託した供給者との間の、契約及び同実力をもつその他の合意を通じて、外部委託した情報システムにも適用する。
			8d-8.27.8	組織は、供給者のセキュリティに配慮したシステム構築の行為が組織のニーズと一致することを確実にする。	手引に関連記載あり	14.2.5.7	組織は、供給者の設計のセキュリティに関する原則が、自身の原則と同様に厳密なものであることを確認する。
			8d-8.27.9	セキュリティに配慮したシステム構築の原則及び確立した構築手順は、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするために、定期的にレビューする。	手引に関連記載あり	14.2.5.4	セキュリティに配慮したシステム構築の原則及び確立した構築手順は、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするために、定期的にレビューする。
			8d-8.27.10	セキュリティに配慮したシステム構築の原則及び確立した構築手順が、新規の潜在的な脅威に対抗するという点で常に最新であること、及び適用される技術及びソリューションの進展に継続して適用可能であることを確実にするために、定期的にレビューする。	手引に関連記載あり	14.2.5.5	セキュリティに配慮したシステム構築の原則及び手順が、新規の潜在的な脅威に対抗するという点で最新であり続けていること、及び適用される技術及びソリューションの進展に適用可能であり続けていることを確実にするために、定期的にレビューする。
8.28	セキュリティに配慮したコーディング 統制目標：セキュリティに配慮したコーディングの原則をソフトウェア開発に適用する。 目的：ソフトウェアをセキュリティに配慮した作成し、それによってソフトウェアの潜在的な情報セキュリティのもい弱性の数を減らすことを確実にするため。		8.28	セキュリティに配慮したコーディング 管理策 セキュリティに配慮したコーディングの原則をソフトウェア開発に適用することが望ましい。 目的 ソフトウェアをセキュリティに配慮して作成し、それによってソフトウェアの潜在的な情報セキュリティのもい弱性の数を減らすことを確実にするため。		–	（対応項なし）
8.28.1	セキュリティに配慮したコーディングの原則を策定する。	組織は、セキュリティに配慮したコーディングに関して優れたガバナンスを実現する、組織全体のプロセスを確立する。 最低限のセキュリティに配慮したベースラインを確立し、適用する。 セキュリティに配慮したコーディングのためのプロセス及び/ガバナンスを、第三者から入手したソフトウェア構成要素及び/オープンソースソフトウェアも対象とするように拡張する。 組織は、組織のセキュリティに配慮したコーディングの原則を下記に2)乃至4)の方向付ける。 a）現実世界の脅威、並びにソフトウェアのもい弱性に関する最新の動員及び/情報を監視する b）組織のセキュリティに配慮したコーディングの原則を継続的に改善する c）組織のセキュリティに配慮したコーディングの原則に従うための学習を要員に促す これは、急速に変化する脅威の状況に対抗するために、効果的なセキュリティに配慮したコーディング慣行の実施を確実にするのに役立ち得る。	8d-8.28.1	組織は、セキュリティに配慮したコーディングに関して優れたガバナンスを実現する、組織全体のプロセスを確立する。	手引に関連記載あり	–	（対応項なし）
			8d-8.28.2	最低限のセキュリティに配慮したコーディングのベースラインを確立し、適用する。	手引に関連記載あり	14.2.1.10	セキュリティに配慮したコーディングに関する標準類を確認し、その使用を義務付ける。
			8d-8.28.3	セキュリティに配慮したコーディングのためのプロセス及び/ガバナンスを、第三者から入手したソフトウェア構成要素及び/オープンソースソフトウェアも対象とするように拡張する。	手引に関連記載あり	–	（対応項なし）
			8d-8.28.4	組織は、組織のセキュリティに配慮したコーディングの原則を下記に2)乃至4)の方向付ける。 a) 現実世界の脅威、並びにソフトウェアのもい弱性に関する最新の動員及び/情報を監視する b) 組織のセキュリティに配慮したコーディングの原則を継続的に改善する c) 組織のセキュリティに配慮したコーディングの原則に従うための学習を要員に施す	手引に関連記載あり	–	（対応項なし）
			（8d-8.28.4参考）	これは、急速に変化する脅威の状況に対抗するために、効果的なセキュリティに配慮したコーディング慣行の実施を確実にするのに役立ち得る。	手引に関連記載あり	–	（対応項なし）
8.28.2	セキュリティに配慮したコーディングの原則を踏まえた計画又は前提条件を定める。	セキュリティに配慮したコーディングの原則を、新規の開発及び/再利用の両方で使用する。 セキュリティに配慮したコーディングの原則は、組織内の開発活動並びに組織が他者に提供する製品及び/サービスの両方に適用する。 コーディング前の計画及び/前提条件は、次の事項を含む。 a）組織内及び/外部委託のコード開発の両方に使用する、セキュリティに配慮したコーディングに関する組織固有の期待及び/並びに認められた原則 b）情報セキュリティのもい弱性につながる一般的及び/歴史的なコーディング慣行及び/欠陥 c）セキュリティに配慮したコードの作成を実施させるために、統合開発環境（IDE）などの開発ツールを構成する。 d）該当する場合には、開発ツール及び/実行環境の提供者が示す手引に従う。 e）更新された開発ツール（例えば、コンパイラ）の維持及び/使用 f）セキュリティに配慮したコードを作成する際の開発者の資格 g）脅威モデリングを含むセキュリティに配慮した設計及び/アーキテクチャ h）セキュリティに配慮したコーディング標準、及び/関係する場合はその使用を義務付けること i）開発のための管理された環境の使用	8d-8.28.6	セキュリティに配慮したコーディングの原則を、新規の開発及び/再利用の両方で使用する。	手引に関連記載あり	–	（対応項なし）
			8d-8.28.7	セキュリティに配慮したコーディングの原則は、組織内の開発活動並びに組織が他者に提供する製品及び/サービスの両方に適用する。	手引に関連記載あり	–	（対応項なし）
			8d-8.28.8	コーディング前の計画及び/前提条件は、次の事項を含む。 a) 組織内及び/外部委託のコード開発の両方に使用する、セキュリティに配慮したコーディングに関する組織固有の期待及び/並びに認められた原則 b) 情報セキュリティのもい弱性につながる一般的及び/歴史的なコーディング慣行及び/欠陥 c) セキュリティに配慮したコードの作成を実施させるために、統合開発環境（IDE）などの開発ツールを構成する。 d) 該当する場合には、開発ツール及び/実行環境の提供者が示す手引に従う。 e) 更新された開発ツールの維持及び/使用 f) セキュリティに配慮したコードを作成する際の開発者の資格 g) 脅威モデリングを含むセキュリティに配慮した設計及び/アーキテクチャ h) セキュリティに配慮したコーディング標準、及び/関係する場合はその使用を義務付けること i) 開発のための管理された環境の使用	手引に関連記載あり	–	（対応項なし）
8.28.3	セキュリティに配慮したコーディングを実施する。	コーディング中の考慮事項は、次の事項を含む。 a）使用するプログラム言語及び/手法に特有の、セキュリティに配慮したコーディング慣行 b）ペアプログラミング、リファクタリング、ピアレビュー、セキュリティイテレーション、テスト駆動開発など、セキュリティに配慮したプログラミング手法を使用する。 c）構造化プログラミング手法を使用する。 d）コードを文書化し、情報セキュリティのもい弱性の悪用を許す可能性のあるプログラミングの欠陥を除去する。 e）セキュリティに配慮しない設計手法の使用を禁止する［例えば、ハードコード（決め打ち）されたパスワード、承認されていないコードサンプル及び/認可されていないウェブサービスの使用］。 セキュリティに配慮して作成するソフトウェアのテストは開発中及び/開発後に実施する（8.29参照）。静的アプリケーションセキュリティテスト（SAST）プロセスで、ソフトウェアのセキュリティのもい弱性を特定することが可能である。	8d-8.28.9	コーディング中の考慮事項は、次の事項を含む。 a) 使用するプログラム言語及び/手法に特有の、セキュリティに配慮したコーディング慣行 b) ペアプログラミング、リファクタリング、ピアレビュー、セキュリティイテレーション、テスト駆動開発など、セキュリティに配慮したプログラミング手法を使用する。 c) 構造化プログラミング手法を使用する。 d) コードを文書化し、情報セキュリティのもい弱性の悪用を許す可能性のあるプログラミングの欠陥を除去する。 e) セキュリティに配慮しない設計手法の使用を禁止する。	手引に関連記載あり	–	（対応項なし）
			8d-8.28.10	セキュリティに配慮して作成するソフトウェアのテストは開発中及び/開発後に実施する。	手引に関連記載あり	–	（対応項なし）
			（8d-8.28.10参考）	静的アプリケーションセキュリティテスト（SAST）プロセスで、ソフトウェアのセキュリティのもい弱性を特定することが可能である。	手引に関連記載あり	–	（対応項なし）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.28.4	ソフトウェアの運用を開始する前に、攻撃対象領域（attack surface）及び最小特権の原則 を評価する。	ソフトウェアの運用を開始する前に、次の事項を評価する。 a) 攻撃対象領域（attack surface）及び最小特権の原則 b) 最も一般的なプログラミングエラーの分析を実行し、これらが低減されたことを文書化する。 コードの運用が開始された後、次のことを行う。 a) 更新はセキュリティに配慮してパッケージ化し、適用する。 b) 報告された情報セキュリティの弱い箇所に対処する（8.8参照）。 c) エラー及び攻撃の疑いのログを取得し、必要に応じてコードを調整するためにログを定期的にレビューする。 d) ソースコードを、認可されていないアクセス及び改ざんから保護する（例えば、アクセス制御、版管理などの機能を提供する構成管理ツールを使用する）。	8d-8.28.11	ソフトウェアの運用を開始する前に、次の事項を評価する。 a) 攻撃対象領域（attack surface）及び最小特権の原則 b) 最も一般的なプログラミングエラーの分析を実行し、これらが低減されたことを文書化する。	手引に関連記載あり	–	（対応項なし）
			8d-8.28.12	コードの運用が開始された後、次のことを行う。 a) 更新はセキュリティに配慮してパッケージ化し、適用する。 b) 報告された情報セキュリティの弱い箇所に対処する。 c) エラー及び攻撃の疑いのログを取得し、必要に応じてコードを調整するためにログを定期的にレビューする。 d) ソースコードを、認可されていないアクセス及び改ざんから保護する。	手引に関連記載あり	–	（対応項なし）
8.28.5	外部ツール及びライブラリを使用する場合のプロセスを整備する。	外部ツール及びライブラリを使用する場合、組織は次の事項を考慮する。 a) 外部ライブラリを管理し（例えば、使用するライブラリ及びそれらの版の目録を維持することによる）、リリースサイクルに合わせて規則正しく更新することを確実にする。 b) 十分に検査された構成要素、特に認証及び暗号化の構成要素の選択、認可及び再利用 c) 外部の構成要素の使用許諾、セキュリティ及び履歴 d) ソフトウェアが保守可能で、追跡することができ、実証された定評のある供給元に由来することを確実にする。 e) 開発資源及び成果物の十分に長期的な可用性 ソフトウェアパッケージを変更する必要がある場合、次のことを考慮する。 a) 組み込まれた管理策及び完全性プロセスが危険にさらされるリスク b) 業者の同意を得るかどうか。 c) 標準のプログラム更新として業者から必要な変更を得る可能性 d) 変更の結果として、将来、組織がソフトウェアの保守に責任を負うようになった場合の影響 e) 使用中の他のソフトウェアとの互換性	8d-8.28.13	外部ツール及びライブラリを使用する場合、組織は次の事項を考慮する。 a) 外部ライブラリを管理し、リリースサイクルに合わせて規則正しく更新することを確実にする。 b) 十分に検査された構成要素、特に認証及び暗号化の構成要素の選択、認可及び再利用 c) 外部の構成要素の使用許諾、セキュリティ及び履歴 d) ソフトウェアが保守可能で、追跡することができ、実証された定評のある供給元に由来することを確実にする。 e) 開発資源及び成果物の十分に長期的な可用性	手引に関連記載あり	–	（対応項なし）
			8d-8.28.14	ソフトウェアパッケージを変更する必要がある場合、次のことを考慮する。 a) 組み込まれた管理策及び完全性プロセスが危険にさらされるリスク	手引に関連記載あり	14.2.4.2	パッケージソフトウェアの変更が必要な場合は、組み込まれている機能及び処理の完全性が損なわれる リスクへの対応を行う。
			8d-8.28.14	ソフトウェアパッケージを変更する必要がある場合、次のことを考慮する。 b) 業者の同意を得るかどうか。	手引に関連記載あり	14.2.4.3	パッケージソフトウェアの変更が必要な場合は、業者の同意を取得する。
			8d-8.28.14	ソフトウェアパッケージを変更する必要がある場合、次のことを考慮する。 c) 標準のプログラム更新として業者から必要な変更を得る可能性	手引に関連記載あり	14.2.4.4	パッケージソフトウェアの変更が必要な場合は、標準のプログラム更新として、業者から必要とする変更が得られる可能性について確認を行う。
			8d-8.28.14	ソフトウェアパッケージを変更する必要がある場合、次のことを考慮する。 d) 変更の結果として、将来、組織がソフトウェアの保守に責任を負うようになった場合の影響	手引に関連記載あり	14.2.4.5	パッケージソフトウェアの変更が必要な場合は、変更の結果として、将来のソフトウェアの保守に対して、組織が責任を負うようになるかどうかの確認を行う。
			8d-8.28.14	ソフトウェアパッケージを変更する必要がある場合、次のことを考慮する。 e) 使用中の他のソフトウェアとの互換性	手引に関連記載あり	14.2.4.6	パッケージソフトウェアの変更が必要な場合は、用いている他のソフトウェアとの互換性について確認を行う。
8.29	開発及び受入れにおけるセキュリティテスト 統制目標：セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施する。 目的：アプリケーション又はコードを本番環境に導入するときに、情報セキュリティ要求事項が満たされているかどうかの妥当性確認をするため。		8.29	開発及び受入れにおけるセキュリティテスト 管理策 セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施する。 目的 アプリケーション又はコードを本番環境に導入するときに、情報セキュリティ要求事項が満たされているかどうかの妥当性確認をするため。		14.2.8	システムセキュリティの試験 セキュリティ機能（functionality）の試験は、開発期間中に実施する。
						14.2.9	システムの受入れ試験 新しい情報システム、及び その改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立する。
8.29.1	開発及び受入れにおけるセキュリティテスト計画を策定する。	セキュリティテスト計画には次の事項を含める。 a) 活動及びテストの詳細スケジュール b) 一連の条件の下での入力及び予想される出力 c) 結果を評価する基準 d) 必要な場合、更なる処置の決定	8d-8.29.7	セキュリティテスト計画には次の事項を含める。 a) 活動及びテストの詳細スケジュール b) 一連の条件の下での入力及び予想される出力 c) 結果を評価する基準 d) 必要な場合、更なる処置の決定	手引に関連記載あり	–	（対応項なし）
8.29.2	セキュリティテストを実施し、欠陥があれば修正をする。	新規の情報システム、アップグレード及び新しい版は、開発プロセスにおいて綿密に試験し、検証する。 セキュリティテストは、システム又は構成要素のテストに統合し、その一部とする。 セキュリティテストは、機能的又は非機能的に表現することができる一連の要求事項に照らして実施する。 セキュリティテストは、次の事項のテストを含む。 a) セキュリティ機能（例えば、利用者認証（8.5参照）、アクセス制限（8.3参照）及び暗号の利用（8.24参照）） b) セキュリティに配慮したコーディング（8.28参照） c) オペレーティングシステム、ファイアウォール及びその他のセキュリティ構成要素の構成を含む、セキュリティに配慮した構成（8.9、8.20及び8.22参照） セキュリティテスト計画は、一連の基準を使用して決定する。 セキュリティテストの程度は、システムの重要性、性質及び導入する変更の潜在的影響に見合ったものにする。 セキュリティに配慮したコーディングを対象としたセキュリティテストを実施する。 オペレーティングシステム、ファイアウォール及びその他のセキュリティ構成要素の構成を含む、セキュリティに配慮した構成を対象としたセキュリティテストを実施する。 組織は、セキュリティに関係する欠陥の修正を検証する。検証には、コード分析ツール又はぜい弱性スキャナなどの自動化ツールを利用することができる。 組織内で開発するソフトウェアについてのセキュリティテストは、次の順に行う。 a) 最初に開発チームが実施する。 b) 次に、システムが開発とは別に、かつ、期待した形でだけ動作することを確実にするために、独立した受入れテストを実施する（5.8参照）。 セキュリティのテストにおいて、次の事項を考慮する。 a) セキュリティの欠陥のテストに関連して、予期しない入力及び条件を含め、コードのレビュー活動を実施する。 b) セキュリティに配慮していない構成及びシステムのぜい弱性を特定するために、ぜい弱性スキャンを実施する。 c) セキュリティに配慮していないコード及び設計を特定するために、侵入テストを実施する。 外部委託した開発及び購入した構成要素については、取得プロセスに従う。 供給者との契約では、特定したセキュリティ要求事項に言及する（5.20 参照）。 外部から調達する製品及びサービスは、取得前に供給者との契約で特定したセキュリティ要求事項に基づく判定基準に照らして評価する。 セキュリティテストは、システムが組織の環境にぜい弱性をもたらさないこと及びテストが信頼できるものであることを確実にするために、対象の本番環境に可能な限り一致するテスト環境で実施する（8.31参照）。	8d-8.29.1	新規の情報システム、アップグレード及び新しい版は、開発プロセスにおいて綿密に試験し、検証する。	手引に関連記載あり	14.2.8.1	組織内でシステムを新規に開発、更新するプロセスにおいては、詳細な活動計画及び一定範囲の条件下での入出力試験の準備を含めた綿密な試験及び検証は、最初に開発チームが実施する。
			8d-8.29.2	セキュリティテストは、システム又は構成要素のテストに統合し、その一部とする。	手引に関連記載あり	14.2.9.2	受け入れた構成部品及び統合されたシステムに対して、試験を実施する。
			8d-8.29.3	セキュリティテストは、機能的又は非機能的に表現することができる一連の要求事項に照らして実施する。	手引に関連記載あり	14.2.8.2	システムが期待どおりに、かつ、期待した形でだけ動作することを確実にするために、組織内で開発するもの及び外部委託したものの両方について、開発チームから独立した受入れ試験を実施する。
			8d-8.29.4	セキュリティテストは、次の事項のテストを含む。 a) セキュリティ機能 b) セキュリティに配慮したコーディング c) オペレーティングシステム、ファイアウォール及びその他のセキュリティ構成要素の構成を含む、セキュリティに配慮した構成	手引に関連記載あり	14.2.9.1	システムの受入れ試験は、情報セキュリティ要求事項の試験及びセキュリティに配慮したシステム開発の慣行の順守を含める。
			8d-8.29.5	セキュリティテスト計画は、一連の判定基準を使用して決定する。	手引に関連記載あり	–	（対応項なし）
			8d-8.29.6	セキュリティテストの程度は、システムの重要性、性質及び導入する変更の潜在的影響に見合ったものにする。	手引に関連記載あり	14.2.8.3	試験は、そのシステムの重要性及び性質に見合った程度で実施する。
			8d-8.29.8	組織は、セキュリティに関係する欠陥の修正を検証する。	手引に関連記載あり	14.2.9.3	組織は、コード分析ツール又はぜい弱性スキャナのような自動化ツールを利用してセキュリティに関連する欠陥を修正した場合は、この修正を検証する。
			8d-8.29.9	組織内で開発するソフトウェアについてのセキュリティテストは、次の順に行う。 a) 最初に開発チームが実施する。 b) その次に、システムが開発とは別に、かつ、期待した形でだけ動作することを確実にするために、独立した受入れテストを実施する	手引に関連記載あり	–	（対応項なし）
			8d-8.29.10	セキュリティのテストにおいて、次の事項を考慮する。 a) セキュリティの欠陥のテストに関連して、予期しない入力及び条件を含め、コードのレビュー活動を実施する。 b) セキュリティに配慮していない構成及びシステムのぜい弱性を特定するために、ぜい弱性スキャンを実施する。 c) セキュリティに配慮していないコード及び設計を特定するために、侵入テストを実施する。	手引に関連記載あり	–	（対応項なし）
			8d-8.29.11	外部委託した開発、及び購入した構成要素については、取得プロセスに従う。	手引に関連記載あり	–	（対応項なし）
			8d-8.29.12	供給者との契約では、特定したセキュリティ要求事項に言及する。	手引に関連記載あり	–	（対応項なし）
			8d-8.29.13	外部から調達する製品及びサービスは、取得前に供給者との契約で特定したセキュリティ要求事項に基づく判定基準に照らして評価する。	手引に関連記載あり	–	（対応項なし）
			8d-8.29.14	セキュリティテストは、システムが組織の環境にぜい弱性をもたらさないこと及びテストが信頼できるものであることを確実にするために、対象の本番環境に可能な限り一致するテスト環境で実施する。	手引に関連記載あり	14.2.9.4	試験は、システムが組織の環境にぜい弱性をもたらさないこと及び試験が信頼できるものであることを確実にするために、現実に即した試験環境で実施する。
8.30	外部委託による開発 統制目標：組織は、外部委託したシステム開発に関する活動を指揮し、監視し、レビューする。 目的：組織が要求する情報セキュリティ対策が、外部委託したシステム開発で実施されることを確実にするため。		8.30	外部委託による開発 管理策 組織は、外部委託したシステム開発に関する活動を指揮し、監視し、レビューする。 目的 組織が要求する情報セキュリティ対策が、外部委託したシステム開発で実施されることを確実にするため。		14.2.7	外部委託による開発 組織は、外部委託したシステム開発活動を監督し、監視する。
8.30.1	外部委託したシステム開発に関して、要求する情報セキュリティ対策が実施されるための対策を実施する。	システム開発を外部委託する場合には、次の事項を行う。 a) 要求事項及び期待を伝達する。 b) 要求事項を満たし、期待に応えることを合意する。 c) 外部委託から提供された作業及び 成果物がこの期待を満たすかどうかを継続的に監視する。 d) 開発されたシステムをレビューする。 組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 a) 外部委託した内容に関する使用許諾の合意、コードの帰属及び知的財産権（5.32参照） b) セキュリティに配慮した設計、コーディング及びテストの実施についての契約上の要求事項（8.25～8.29参照） c) 外部の開発者が考慮すべき脅威モデルの提供 d) 成果物の質及び正確さに関する受入れテスト（8.29参照） e) 受け入れられる最低限のセキュリティ及びプライバシー機能を実現していることを示す証拠の提出（例えば、保証報告書） f) 引渡しに当たって、悪意のある内容（意図的なものも及び意図しないもの）の存在を防ぐために、十分なテストを実施していることを示す証拠の提出 g) 既知のぜい弱性が含まれないう、十分なテストを実施していることを示す証拠の提出 h) ソフトウェアソースコードの預託契約（例えば、供給者が事業を終了する場合） i) 開発のプロセス及び管理策を監査する、契約に基づく権利 j) 開発環境のセキュリティ要求事項（8.31参照） k) 適用される法令（例えば、個人データの保護に関する法令）の考慮	8d-8.30.1	システム開発を外部委託する場合には、次の事項を行う。 a) 要求事項及び期待を伝達する。 b) 要求事項を満たし、期待に応えることを合意する。 c) 外部委託から提供された作業及び成果物がこの期待を満たすかどうかを継続的に監視する。 d) 開発されたシステムをレビューする。	手引に関連記載あり	–	（対応項なし）
			8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 a) 外部委託した内容に関する使用許諾の合意、コードの帰属及び知的財産権	手引に関連記載あり	14.2.7.1	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、外部委託した内容に関連する使用許諾に関する取決め、コードの所有権及び知的財産権に関わる事項を契約に含める。
			8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 b) セキュリティに配慮した設計、コーディング及びテストの実施についての契約上の要求事項	手引に関連記載あり	14.2.7.2	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、セキュリティに配慮した設計、コーディング及び試験の実施についての要求事項を契約に含める。
			8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 c) 外部の開発者が考慮すべき脅威モデルの提供	手引に関連記載あり	14.2.7.3	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、外部の開発者への、承認済みの脅威モデルの提供を契約に含める。
			8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 d) 成果物の質及び正確さに関する受入れテスト	手引に関連記載あり	14.2.7.4	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、成果物の質及び正確さに関する受入れ試験を契約に含める。
			8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 e) 受け入れられる最低限のセキュリティ及びプライバシー機能を実現していることを示す証拠の提出	手引に関連記載あり	14.2.7.5	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、セキュリティ及びプライバシーについて、容認可能な最低限のレベルを定めるためにセキュリティしきい（閾）値を用いていることを示す証拠の提出を契約に含める。
			8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 f) 引渡しに当たって、悪意のある内容（意図的なものも及び意図しないもの）の存在を防ぐために、十分なテストを実施していることを示す証拠の提出	手引に関連記載あり	14.2.7.6	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、引渡しに当たって、悪意のある内容（意図的なものも及び意図しないもの）が含まれないよう、十分な試験が実施されていることを示す証拠の提出を契約に含める。
			8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 g) 既知のぜい弱性が含まれないよう、十分なテストを実施していることを示す証拠の提出	手引に関連記載あり	14.2.7.7	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、既知のぜい弱性が含まれないよう、十分な試験が実施されていることを示す証拠の提出を契約に含める。
			8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 h) ソフトウェアソースコードの預託契約	手引に関連記載あり	14.2.7.8	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、預託契約に関する取決め（例えば、ソースコードが利用できなくなった場合）を契約に含める。
			8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 i) 開発のプロセス及び管理策を監査する、契約に基づく権利	手引に関連記載あり	14.2.7.9	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、開発のプロセス及び管理策を監査するための契約上の権利を契約に含める。
			8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 j) 開発環境のセキュリティ要求事項	手引に関連記載あり	14.2.7.10	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、成果物の作成に用いたビル ド環境の有効な文書化を契約に含める。
			8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 k) 適用される法令の考慮	手引に関連記載あり	14.2.7.11	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、適用される法令の順守及び管理の効率の検証については、組織が責任を負うことを契約に含める。

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.31	開発環境、テスト環境及び本番環境の分離 統制目標：開発環境、テスト環境及び本番環境は、分離してセキュリティを保つ。 目的：開発活動及びテスト活動による危険から本番環境及びそのデータを保護するため。		8.31	開発環境、テスト環境及び本番環境の分離 管理策 開発環境、テスト環境及び本番環境は、分離してセキュリティを保つ。 目的 開発活動及びテスト活動による危険から本番環境及びそのデータを保護するため。		12.1.4	開発環境、試験環境及び運用環境の分離 開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離する。
						14.2.6	セキュリティに配慮した開発環境 組織は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護する。
8.31.1	本番環境、テスト環境及び開発環境の間の分離レベルを特定し、分離する。	本番環境における問題を防ぐために必要な、本番環境、テスト環境及び開発環境の間の分離レベルを特定し、それに従って分離する。 開発環境、テスト環境及び本番環境の分離を行う際には、特に、次の事項を考慮する。 a) 開発システムと本番システムとを適切に分離し、それらを異なる領域で（例えば、別々の仮想環境又は物理環境で）運用する。 b) 開発段階から本番段階へのソフトウェアの導入に関する規則及び認可を、明確に定め、文書化し、実施する。 c) 本番システム及びアプリケーションに対する変更は、本番システムに適用する前に、テスト環境又はステージング環境でテストする（8.29参照）。 d) 特定し、承認された状況を除いて、本番環境ではテストを行わない。 e) コンパイラ、エディタ、及びその他の開発ツール又はユーティリティプログラムは、必要がないときには、本番システムからアクセス可能としない。 f) 誤りのリスクを減らすために、メニューに適切な環境識別ラベルを表示する。 g) 取扱いに慎重を要する情報は、開発システム及びテストシステムに同等の管理策が備わっていない限り、その開発システム環境及びテストシステム環境にはコピーしない。	8d-8.31.1	本番環境における問題を防ぐために必要な、本番環境、テスト環境及び開発環境の間の分離レベルを特定し、それに従って分離する。	手引に関連記載あり	12.1.4.1	運用上の問題を防ぐために必要な、開発環境、試験環境及び運用環境の間の分離レベルを特定し、それに従って分離する。
			8d-8.31.2	開発環境、テスト環境及び本番環境の分離をする際には、特に、次の事項を考慮する。 a) 開発システムと本番システムとを適切に分離し、それらを異なる領域で運用する。	手引に関連記載あり	12.1.4.3	開発ソフトウェア及び運用ソフトウェアは、異なるシステム又はコンピュータ上で、及び異なる領域又はディレクトリで実行する。
			8d-8.31.2	開発環境、テスト環境及び本番環境の分離をする際には、特に、次の事項を考慮する。 b) 開発段階から本番段階へのソフトウェアの導入に関する規則及び認可を、明確に定め、文書化し、実施する。	手引に関連記載あり	12.1.4.2	ソフトウェアの開発から運用の段階への移行についての規則は、明確に定め、文書化する。
			8d-8.31.2	開発環境、テスト環境及び本番環境の分離をする際には、特に、次の事項を考慮する。 c) 本番システム及びアプリケーションに対する変更は、本番システムに適用する前に、テスト環境又はステージング環境でテストする。	手引に関連記載あり	12.1.4.4	運用システム及びアプリケーションに対する変更は、運用システムに適用する前に、試験環境又はステージング環境（運用環境に近い試験環境）で試験する。
			8d-8.31.2	開発環境、テスト環境及び本番環境の分離をする際には、特に、次の事項を考慮する。 d) 特定し、承認された状況を除いて、本番環境ではテストを行わない。	手引に関連記載あり	12.1.4.5	例外的な状況以外では、運用システムで試験を行わない。
			8d-8.31.2	開発環境、テスト環境及び本番環境の分離をする際には、特に、次の事項を考慮する。 e) コンパイラ、エディタ、及びその他の開発ツールはユーティリティプログラムは、必要がないときには、本番システムからアクセス可能としない。	手引に関連記載あり	12.1.4.6	コンパイラ、エディタ、及びその他の開発ツール又はシステムユーティティは、必要でない場合には、運用システムからアクセスできないようにする。
			8d-8.31.2	開発環境、テスト環境及び本番環境の分離をする際には、特に、次の事項を考慮する。 f) 誤りのリスクを減らすために、メニューに適切な環境識別ラベルを表示する。	手引に関連記載あり	12.1.4.7	利用者は、運用システム及び試験システムに対して、異なるユーザプロファイルを用いる。
					手引に関連記載あり	12.1.4.8	メニューには、誤操作によるリスクを低減するために、適切な識別メッセージを表示する。
			8d-8.31.2	開発環境、テスト環境及び本番環境の分離をする際には、特に、次の事項を考慮する。 g) 取扱いに慎重を要する情報は、開発システム及びテストシステムに同等の管理策が備わっていない限り、その開発システム環境及びテストシステム環境にはコピーしない。	手引に関連記載あり	12.1.4.9	取扱いに慎重を要するデータは、試験システムに同等の管理策が備わっていない限り、その試験システム環境には複写を禁止する。
8.31.2	開発環境及びテスト環境は必要な要件を定めて保護する。	全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。 a) 全ての開発、統合及びテストツール（ビルダ、インテグレータ、コンパイラ、構成システム及びライブラリ生成ら。）のパッチ適用及び更新 b) システム及びソフトウェアのセキュリティに配慮した構成 c) 環境へのアクセスの制御 d) 環境の変更及びそこに保存されているコードの監視 e) 環境の、セキュリティに配慮した監視 f) 環境のバックアップをとること	8d-8.31.3	全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。 a) 全ての開発、統合及びテストツール（ビルダ、インテグレータ、コンパイラ、構成システム及びライブラリ生成ら。）のパッチ適用及び更新	手引に関連記載あり	14.2.6.1	セキュリティに配慮した開発環境には、システムの開発及び統合に関連する要員、プロセス及び技術を含める。
			8d-8.31.3	全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。 b) システム及びソフトウェアのセキュリティに配慮した構成	手引に関連記載あり	–	（対応項なし）
			8d-8.31.3	全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。 c) 環境へのアクセスの制御	手引に関連記載あり	14.2.6.8	組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、開発環境へのアクセスの制御を実施する。
			8d-8.31.3	全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。 d) 環境の変更及びそこに保存されているコードの監視	手引に関連記載あり	14.2.6.9	組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、開発環境の変更及びそこに保管されたコードに対する変更を監視する。
			8d-8.31.3	全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。 e) 環境の、セキュリティに配慮した監視	手引に関連記載あり	–	（対応項なし）
			8d-8.31.3	全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。 f) 環境のバックアップをとること	手引に関連記載あり	14.2.6.10	組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、セキュリティに配慮した運用時でのバックアップを保管する。
8.31.3	一人の人間が、事前のレビュー及び承認なしに、開発環境及び本番環境の両方に変更を加えることができないようにする。	一人の人間が、事前のレビュー及び承認なしに、開発環境及び本番環境の両方に変更を加えることができないようにする。これは、例えばアクセス権の分離又は監視を伴う規則によって達成可能である。 通常と異なる状況では、認可されていない変更を検出し、対処するために、詳細なログ取得、リアルタイム監視などの追加の対策を実施する。	8d-8.31.4	一人の人間が、事前のレビュー及び承認なしに、開発環境及び本番環境の両方に変更を加えることができないようにする。	手引に関連記載あり	–	（対応項なし）
			（8d-8.31.4参考）	これは、例えばアクセス権の分離又は監視を伴う規則によって達成可能である。	手引に関連記載あり	–	（対応項なし）
			8d-8.31.5	通常と異なる状況では、認可されていない変更を検出し、対処するために、詳細なログ取得、リアルタイム監視などの追加の対策を実施する。	手引に関連記載あり	–	（対応項なし）
8.32	変更管理 統制目標：情報処理設備及び情報システムの変更は、変更管理手順に従う。 目的：変更を実行するときに情報セキュリティを維持するため。		8.32	変更管理 管理策 情報処理設備及び情報システムの変更は、変更管理手順に従う。 目的 変更を実行するときに情報セキュリティを維持するため。		12.1.2	変更管理 情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理する。
						14.2.2	システムの変更管理手順 開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理する。
						14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験する。
						14.2.4	パッケージソフトウェアの変更に対する制限 パッケージソフトウェアの変更は、抑止し、必要な変更だけに限る。また、全ての変更は、厳重に管理する。
8.32.1	情報処理設備及び情報システムの変更管理手順を整備し、対策を実施する。	新しいシステムの導入及び既存システムに対する重要な変更は、文書化、仕様化、テスト、品質管理及び管理された実装についての合意された規則及び正式な手続に従う。 変更管理手順には、次の事項を含む。 a) 全ての依存関係を考慮した、変更の潜在的影響に関する計画策定及び評価 b) 変更の認可 c) 関連する利害関係者への変更の伝達 d) 変更のテスト及びテストの受入れ（8.29参照） e) 導入計画を含む変更の実施 f) フォールバック手順（代替手順）を含む緊急時及び不測の事態の考慮 g) 上記の全てを含む変更の記録の維持 h) 運用文書類（5.37参照）及び利用者手順が、適切な状態であるように、必要に応じて変更することを確実にすること i) ICT継続計画並びに対応及び復旧手順（5.30 参照）が、適切な状態であるように、必要に応じて変更することを確実にすること 情報処理設備及び情報システムの全ての変更を良好に管理することを確実にするように、管理責任及び手順を設ける。 変更管理手順は、情報処理設備及び情報システムにおける情報の機密性、完全性及び可用性を確実にするために、設計の初期段階からその後の全ての保守作業までのシステム開発のライフサイクル全体にわたって文書化し、実装する。 実施可能な場合には、ICT基盤及びソフトウェアの変更管理手順を統合する。	8d-8.32.1	新しいシステムの導入及び既存システムに対する重要な変更は、文書化、仕様化、テスト、品質管理及び管理された実装についての合意された規則及び正式な手続に従う。	手引に関連記載あり	14.2.2.2	新しいシステムの導入及び既存システムに対する重要な変更は、文書化、仕様化、試験、品質管理及び管理された実装からなる正式な手続に従う。
					手引に関連記載あり	14.2.2.7	変更管理手順には、変更は、認可されている利用者によって提出されることを確実にすることを含める。
			8d-8.32.5	変更管理手順には、次の事項を含む。 a) 全ての依存関係を考慮した、変更の潜在的影響に関する計画策定及び評価	手引に関連記載あり	12.1.2.3	組織、業務プロセス、情報処理設備及びシステムの変更管理には、変更の潜在的な影響（情報セキュリティ上の影響を含む）のアセスメントを含める。
					手引に関連記載あり	14.2.2.3	新しいシステムの導入及び既存システムに対する重要な変更の際の手続には、リスクアセスメント、変更の影響分析及び必要なセキュリティ管理策の仕様化を含める。
					手引に関連記載あり	14.2.3.1	オペレーティングプラットフォームの変更によって、アプリケーションの機能及び処理の完全性が損なわれていないことを確実にするために、これらに関係する手続きをレビューする。
			8d-8.32.5	変更管理手順には、次の事項を含む。 b) 変更の認可	手引に関連記載あり	12.1.2.4	組織、業務プロセス、情報処理設備及びシステムの変更管理には、変更の申出を正式に承認する手順を含める。
					手引に関連記載あり	14.2.2.11	変更管理手順には、作業を開始する前に、提案の詳細について正式な承認を得ることを含める。
			8d-8.32.5	変更管理手順には、次の事項を含む。 c) 関連する利害関係者への変更の伝達	手引に関連記載あり	12.1.2.6	組織、業務プロセス、情報処理設備及びシステムの変更管理には、全ての関係者への変更に関する詳細事項の通知を含める。
					手引に関連記載あり	14.2.2.12	変更管理手順には、変更を実施する前に、認可されている利用者だその変更を受け入れることを確実にすることを含める。
					手引に関連記載あり	14.2.3.2	オペレーティングプラットフォームの変更の実施前に適切な試験及びレビューを行っても間に合うように、オペレーティングプラットフォームの変更を通知することを確実にする仕組みを整備する。
			8d-8.32.5	変更管理手順には、次の事項を含む。 d) 変更のテスト及びテストの受入れ	手引に関連記載あり	12.1.2.2	組織、業務プロセス、情報処理設備及びシステムの変更管理には、変更作業の計画策定及びテストの実施を含める。
					手引に関連記載あり	14.2.4.9	将来のソフトウェア更新において、パッケージソフトウェアの変更を再び適用できるように、全ての変更は、十分に試験し、文書化する。
			8d-8.32.5	変更管理手順には、次の事項を含む。 e) 導入計画を含む変更の実施	手引に関連記載あり	–	（対応項なし）
			8d-8.32.5	変更管理手順には、次の事項を含む。 f) フォールバック手順（代替手順）を含む緊急時及び不測の事態の考慮	手引に関連記載あり	12.1.2.7	組織、業務プロセス、情報処理設備及びシステムの変更管理には、うまくいかない変更及びこれに伴う予期できない事象を取り消し、これらから回復する手順及び責任を含む、代替手順を確立することを含める。
			8d-8.32.5	変更管理手順には、次の事項を含む。 g) 上記の全てを含む変更の記録の維持	手引に関連記載あり	12.1.2.10	組織、業務プロセス、情報処理設備及びシステムに対する変更がなされたときは、変更に関わる全ての関連情報を含んだ監査ログを保持する。
					手引に関連記載あり	14.2.2.6	変更管理手順には、合意された認可レベルの記録を維持することを含める。
					手引に関連記載あり	14.2.2.15	変更管理手順には、全ての変更要求の監査証跡を維持・管理することを含める。
			8d-8.32.5	変更管理手順には、次の事項を含む。 h) 運用文書類及び利用者手順が、適切な状態であるように、必要に応じて変更することを確実にすること	手引に関連記載あり	14.2.2.16	変更管理手順には、操作手順書などの運用文書類及び利用者手順が、適切な状態であるように、必要に応じて変更することを確実にすることを含める。
					手引に関連記載あり	14.2.2.13	変更管理手順には、システムに関する一式の文書が各変更の完了時点で更新されること、及び古い文書類は記録・保管されるか又は処分されることを確実にすることを含める。
					手引に関連記載あり	14.2.2.16	変更管理手順には、操作手順書などの運用文書類及び利用者手順が、適切な状態であるように、必要に応じて変更することを確実にすることを含める。
			8d-8.32.5	変更管理手順には、次の事項を含む。 i) ICT継続計画並びに対応及び復旧手順が、適切な状態であるように、必要に応じて変更することを確実にすること	手引に関連記載あり	12.1.2.8	組織、業務プロセス、情報処理設備及びシステムの変更管理には、インシデントの解決のために必要な変更を、迅速にかつ管理して実施できるようにするための、緊急時の変更プロセスの提供を含める。
					手引に関連記載あり	14.2.3.3	事業継続計画に対して、適切な変更がなされることを確実にする仕組みを整備する。
			8d-8.32.2	情報処理設備及び情報システムの全ての変更を良好に管理することを確実にするように、管理責任及び手順を設ける。	手引に関連記載あり	12.1.2.9	組織、業務プロセス、情報処理設備及びシステムに対するあり得る変更の十分な管理を確実にするために、正式な責任体制及び手順を備える。
					手引に関連記載あり	14.2.2.4	新しいシステムの導入及び既存システムに対する重要な変更の際の手続は、既存のセキュリティ及び管理手順が損なわれないこと、サポートプログラムによるシステムへのアクセスはその作業に必要な部分に限定されること、並びにいかなる変更に対しても正式な合意及び承認が得られていることを確実にする仕組みを整備する。
			8d-8.32.3	変更管理手順は、情報処理設備及び情報システムにおける情報の機密性、完全性及び可用性を確実にするために、設計の初期段階からその後の全ての保守作業までのシステム開発のライフサイクル全体にわたって文書化し、実装する。	手引に関連記載あり	12.1.2.1	組織、業務プロセス、情報処理設備及びシステムの変更管理には、情報処理設備及びシステムの構成品目の構成管理プロセス及び管理計画を策定、文書化し、実施し、重要な変更の特定及び記録を含める。
					手引に関連記載あり	14.2.2.1	初期設計段階からその後の全ての保守業務に至るまで、システム、アプリケーション及び製品の完全性を確実にするため、正式な変更管理手順を文書化し、実施する。
			8d-8.32.4	実施可能な場合には、ICT基盤及びソフトウェアの変更管理手順を統合する。	手引に関連記載あり	14.2.2.5	変更管理手順には、実施可能な範囲でアプリケーション及びその運用に関する変更管理手順を統合する。
8.32.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	(新)管理策基準	(参考)手引き	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(旧)管理策基準
8.33	テスト用情報 統制目標：テスト用情報は、適切に選定し、保護し、管理する。 目的：テストの適切な実施、及びテストに使用する運用情報の保護を確実にするため。		8.33	テスト用情報 管理策 テスト用情報は、適切に選定し、保護し、管理する。 目的 テストの適切な実施、及びテストに使用する運用情報の保護を確実にするため。		14.3	試験データ 管理目的：試験に用いるデータの保護を確実にするため。
						14.3.1	試験データの保護 試験データは、注意深く選定し、保護し、管理する。
8.33.1	テスト結果の信頼性及び関連する運用情報の機密性を確実にするように、テスト用情報を選択する。	テスト結果の信頼性及び関連する運用情報の機密性を確実にするように、テスト用情報を選択する。 取扱いに慎重を要する情報（PIIを含む。）を、開発環境及びテスト環境へ複製しない（8.31参照）。	8d-8.33.1	テスト結果の信頼性及び関連する運用情報の機密性を確実にするように、テスト用情報を選択する。	手引に関連記載あり	14.3.1.1	PII 又はその他の秘密情報を含んだ運用データは、試験目的に用いない。
			8d-8.33.2	取扱いに慎重を要する情報（PIIを含む。）を、開発環境及びテスト環境へ複製しない。	手引に関連記載あり	–	（対応項なし）
8.33.2	テスト用情報はセキュリティに配慮して保存し、使用する。	運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の事項を適用する。 a) 運用環境に適用するものと同じアクセス制御手順をテスト環境に適用する。 b) 運用情報の複製をテスト環境に置く場合は、その都度認可を受ける。 c) 運用情報の複製及び利用は、監査証跡とするためにログをとる。 d) テストに使用する場合、取扱いに慎重を要する情報は、削除又はマスキング（8.11参照）によって保護する。 e) テスト用情報の認可されていない使用を防止するために、テストの完了直後にテスト環境から運用情報を適切に削除（8.10参照）する。 テスト用情報は、セキュリティに配慮して保存し（結果を無効にする可能性がある改ざんも防止するため）、テスト目的でだけ使用する。	8d-8.33.3	運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の事項を適用する。 a) 運用環境に適用するものと同じアクセス制御手順をテスト環境に適用する。	手引に関連記載あり	14.3.1.3	運用データを試験目的で用いる場合は、運用アプリケーションシステムに適用されるアクセス制御手順を、試験アプリケーションシステムにも適用する。
			8d-8.33.3	運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の事項を適用する。 b) 運用情報の複製をテスト環境に置く場合は、その都度認可を受ける。	手引に関連記載あり	14.3.1.4	運用情報を試験環境にコピーする場合は、その都度認可を受ける。
			8d-8.33.3	運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の事項を適用する。 c) 運用情報の複製及び利用は、監査証跡とするためにログをとる。	手引に関連記載あり	14.3.1.6	運用データを試験目的で用いる場合は、運用情報の複製及び利用は、監査証跡とするためにログを取得する。
			8d-8.33.3	運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の事項を適用する。 d) テストに使用する場合、取扱いに慎重を要する情報は、削除又はマスキングによって保護する。	手引に関連記載あり	14.3.1.2	PII 又はその他の秘密情報を試験目的で用いる場合には、取扱いに慎重を要する詳細な記述及び内容の全てを、消去又は改変することによって保護する。
			8d-8.33.3	運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の事項を適用する。 e) テスト用情報の認可されていない使用を防止するために、テストの完了直後にテスト環境から運用情報を適切に削除する。	手引に関連記載あり	14.3.1.5	運用データを試験目的で用いる場合は、運用情報は、試験が完了した後直ちに試験環境から消去する。
			8d-8.33.4	テスト用情報は、セキュリティに配慮して保存し（結果を無効にする可能性がある改ざんも防止するため）、テスト目的でだけ使用する。	手引に関連記載あり	–	（対応項なし）
8.34	監査におけるテスト中の情報システムの保護 統制目標：運用システムのアセスメントを伴う監査におけるテスト及びその他の保証活動を計画し、テスト実施者と適切な管理職との間で合意する。 目的：監査及びその他の保証活動が運用システム及び業務プロセスに与える影響を最小限に抑えるため。		8.34	監査におけるテスト中の情報システムの保護 管理策 運用システムのアセスメントを伴う監査におけるテスト及びその他の保証活動を計画し、テスト実施者と適切な管理職との間で合意する。 目的 監査及びその他の保証活動が運用システム及び業務プロセスに与える影響を最小限に抑えるため。		12.7	情報システムの監査に対する考慮事項 管理目的：運用システムに対する監査活動の影響を最小限にするため。
						12.7.1	情報システムの監査に対する管理策 運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意する。
8.34.1	監査におけるテスト及びその他の保証活動を計画し、テスト実施者と適切な管理職との間で合意する。	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 a) システム及びデータへのアクセスに関する監査要求は、適切な管理職の同意を得る。 b) 技術監査におけるテストの範囲を、合意し、管理する。 c) 監査におけるテストは、ソフトウェア及びデータの読出し専用のアクセスに限定する。必要な情報を取得するために参照専用のアクセスを利用できない場合、監査人に代わって必要なアクセス権をもつ経験豊かな実務管理者がテストを実行する。 d) アクセスを許可する場合、許可する前にシステムへのアクセスに使用する装置・機器（例えば、ラップトップ又はタブレット）のセキュリティ要求事項（例えば、ウイルス対策及びパッチ適用）を確立し、検証する。 e) 読出し専用以外のアクセスは、システムファイルの隔離された複製に対して1日1回可い。それらの複製は、監査が完了した時点で削除するか、又は監査の文書化の要求によってそのようなファイルを保存する義務があるときは、適切に保護する。 f) 監査ツールの実行など、特別又は追加の処理に関する要求を特定し、合意する。 g) 監査におけるテストがシステムの可用性に影響する可能性がある場合、こうしたテストは営業時間外に実施する。 h) 監査及びテストを目的とする全てのアクセスを監視し、ログをとる。	8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 a) システム及びデータへのアクセスに関する監査要求は、適切な管理職の同意を得る。	手引に関連記載あり	12.7.1.1	システム及びデータへのアクセスに関する監査要求事項は、適切な管理職の同意を得る。
			8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 b) 技術監査におけるテストの範囲を、合意し、管理する。	手引に関連記載あり	12.7.1.2	技術監査における試験の範囲を、合意し、管理する。
			8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 c) 監査におけるテストは、ソフトウェア及びデータの読出し専用のアクセスに限定する。 必要な情報を取得するために参照専用のアクセスを利用できない場合、監査人に代わって必要なアクセス権をもつ経験豊かな実務管理者がテストを実行する。	手引に関連記載あり	12.7.1.3	監査における試験は、ソフトウェア及びデータの読出し専用のアクセスに限定する。
			8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 d) アクセスを許可する場合、許可する前にシステムへのアクセスに使用する装置・機器のセキュリティ要求事項を確立し、検証する。	手引に関連記載あり	–	（対応項なし）
			8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 e) 読出し専用以外のアクセスは、システムファイルの隔離された複製に対して1日1回許可しない。それらの複製は、監査が完了した時点で削除するか、又は監査の文書化の要求によってそのようなファイルを保存する義務があるときは、適切に保護する。	手引に関連記載あり	12.7.1.4	監査における試験では、読出し専用以外のアクセスは、システムファイルの隔離された複製に対して1日1回許可し、それらの複製は、監査が完了した時点で消去するか、又は監査の文書化の要求の下でそのようなファイルを保存する義務があるときは、適切に保護する。
			8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 f) 監査ツールの実行など、特別又は追加の処理に関する要求を特定し、合意する。	手引に関連記載あり	12.7.1.5	監査における試験を実施するための、特別又は追加の処理（異常が発見された場合の措置を含む。）に関する要求事項を特定し、合意する。
			8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 g) 監査におけるテストがシステムの可用性に影響する可能性がある場合、こうしたテストは営業時間外に実施する。	手引に関連記載あり	12.7.1.6	監査における試験がシステムの可用性に影響する可能性がある場合、こうした試験は営業時間外に実施する。
			8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 h) 監査及びテストを目的とする全てのアクセスを監視し、ログをとる。	手引に関連記載あり	12.7.1.7	監査における試験を実施する際には、参照用の証跡を残すために、全てのアクセスを監視し、ログをとる。
9.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
						（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.1.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.2.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.2.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.2.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
						（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.3.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.3.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.3.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.3.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.4.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.5	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.5.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.6.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
			–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.6.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.6.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.6.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.7	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.7.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
9.7.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	(旧)マネジメント基準	番号	(新) マネジメント基準
–	(対応項なし)	–	–
4.1	マネジメント基準	–	–
–	マネジメント基準は、JIS Q 27001:2014を基に、情報セキュリティについて組織を指揮統制するために調整された活動である情報セキュリティマネジメントを確立、導入、運用、監視、維持及び改善するための基準を定める。マネジメント基準は、原則としてすべて実施しなければならないものである。	–	–
4.2	記載内容について	–	–
–	「情報セキュリティ管理基準」の「マネジメント基準」に同じ。 クラウドサービスにおいては、クラウドサービス利用者の環境等を考慮して、クラウドサービス提供者の管理策等を検討し、実施する必要がある。そのため、クラウドサービス利用者及びクラウドサービス事業者間において、クラウドサービスにおける情報セキュリティリスクとその対応について、情報交換することが非常で重要である。 当該情報セキュリティリスクコミュニケーションについては、クラウドサービスにおいて特に考慮するべき事項として、4.9章に規定する。	–	–
4.3	凡例	–	–
–	4.4章以降は、以下の構成をとる。 4.4 情報セキュリティマネジメント確立 [27001-4] 4.4.1 組織の役割、責任及び権限 [27001-5.3 / 5.1] 4.4.1.1 トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。[27001-5.1b) / 5.1e) / 5.1f)] その際は、以下を行うこととする。 ・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する : [27001-X.X.X]は、JIS Q 27001:2014において関連する条項(X.X.X)を示す。	–	–
4.4	情報セキュリティマネジメントの確立 [27001-4.4]	–	–
–	情報セキュリティマネジメントを確立するために、その基盤となる適用範囲を決定し、方針を確立する。これらをもとに、情報セキュリティリスクアセスメントを実施し、その対応を計画し実施する。それにより、組織が有効な情報セキュリティマネジメントを実施するための基盤作りを行う。	–	–
4.4.1	組織の役割、責任及び権限 [27001-5.3 / 5.1]	4.4.1	組織の役割、責任及び権限 [27001-5.3 / 5.1]
4.4.1.1	トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。 [27001-5.1b) / 5.1e) / 5.1f)] ・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する。 ・情報セキュリティマネジメントがその意図した成果を達成することを確実にする。 ・情報セキュリティマネジメントの有効性に寄与するよう人々を指揮し、支援する。 また、トップマネジメントがリーダーシップ及びコミットメントを発揮していることを以下により確認する。 ・経営会議等の議事録に、トップマネジメントの情報セキュリティマネジメントに関する意思、判断、指示等が記録されていること。 ・情報セキュリティ方針、情報セキュリティ目的及びそれを達成する計画を策定する際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・達成すべきセキュリティの水準として、リスクレベルをトップマネジメントが決定していること。 ・リスクレベルに応じて選択したセキュリティ管理策を実施させる際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・内部監査において確認すべき事項に、トップマネジメントが要求する情報セキュリティ要求事項等が含まれていること。 ・内部監査報告書やそれらに基づく是正処置、マネジメントビュー議事録等に、トップマネジメントの意思、判断、指示等が含まれていること。	4.4.1.1	トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。 [27001-5.1b) / 5.1e) / 5.1f)] ・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する。 ・情報セキュリティマネジメントがその意図した成果を達成することを確実にする。 ・情報セキュリティマネジメントの有効性に寄与するよう人々を指揮し、支援する。 また、トップマネジメントがリーダーシップ及びコミットメントを発揮していることを以下により確認する。 ・経営会議等の議事録に、トップマネジメントの情報セキュリティマネジメントに関する意思、判断、指示等が記録されていること。 ・情報セキュリティ方針、情報セキュリティ目的及びそれを達成する計画を策定する際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・達成すべきセキュリティの水準として、リスクレベルをトップマネジメントが決定していること。 ・リスクレベルに応じて選択したセキュリティ管理策を実施させる際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・内部監査において確認すべき事項に、トップマネジメントが要求する情報セキュリティ要求事項等が含まれていること。 ・内部監査報告書やそれに基づく是正処置、マネジメントレビュー議事録等に、トップマネジメントの意思、判断、指示等が含まれていること。
4.4.1.2	トップマネジメントは、組織の役割について、以下の責任及び権限を割り当て、伝達する。[27001-5.3] ・情報セキュリティマネジメントを、本管理基準の要求事項として適合させる。 ・情報セキュリティマネジメントのパフォーマンス評価をトップマネジメントに報告する。 また、情報セキュリティマネジメントを本管理基準の要求事項に適合させるために、以下のような責任・権限を割り当てていることを確認する。 ・セキュリティ要求事項を盛り込んだ情報セキュリティ方針等の文書を策定する責任・権限 ・リスクアセスメントにおいて、リスクを運用管理する責任・権限を持つリスク所有者 ・セキュリティ要求事項を満たす管理策を教育、普及させる責任・権限 ・セキュリティ要求事項を満たしているか監査する責任・権限 ・各プロセスの結果及び効果をトップマネジメントに報告する責任・権限 ・各プロセスの結果及び効果を組織内に周知する責任・権限	4.4.1.2	トップマネジメントは、組織の役割について、以下の責任及び権限を割り当て、組織内に伝達する。[27001-5.3] ・情報セキュリティマネジメントを、本管理基準の要求事項として適合させる。 ・情報セキュリティマネジメントのパフォーマンス評価をトップマネジメントに報告する。 また、組織の情報セキュリティマネジメントを本管理基準の要求事項に適合させるために不可欠な責任・権限を明確にしたうえで、それぞれに適切な割り当てが行われていることを確認する。責任・権限の例を以下に示す。 ・セキュリティ要求事項を盛り込んだ情報セキュリティ方針等の文書を策定する責任・権限 ・リスクアセスメントにおいて、リスクを運用管理する責任・権限をもつリスク所有者 ・セキュリティ要求事項を満たす管理策を教育、普及させる責任・権限 ・セキュリティ要求事項を満たしているか監査する責任・権限 ・各プロセスの結果及び効果をトップマネジメントに報告する責任・権限 ・各プロセスの結果及び効果を組織内に周知する責任・権限
4.4.1.3	トップマネジメントは、管理層がその責任の領域においてリーダーシップを発揮できるよう、管理層の役割を支援する。[27001-5.1h)] 管理層が、その職掌範囲、組織等において、リーダーシップを発揮できるよう、トップマネジメントは、管理層に、必要な権限を委譲していることを確認する。	4.4.1.3	トップマネジメントは、その他の関連する管理層がその責任の領域においてリーダーシップを発揮できるよう、管理層の役割を支援する。[27001-5.1h)] ・その他の関連する管理層が、その職掌範囲、組織等において、リーダーシップを発揮できるよう、トップマネジメントは、管理層に、必要な権限を委譲していることを確認する。

番号	(旧)マネジメント基準	番号	(新) マネジメント基準
4.4.2	組織及びその状況の理解 [27001-4.1]	4.4.2	組織及びその状況の理解 [27001-4.1]
4.4.2.1	組織は、組織の目的に関連し、かつ、情報セキュリティマネジメントの意図した成果を達成する組織の能力に影響を与える、以下の課題を決定する。[27001-4.1] ・外部の課題 ・内部の課題 これらの課題の決定とは、組織の外部状況及び内部状況の確定のことをいう。外部状況及び内部状況には、以下のようなものが含まれる。 a) 外部状況 ・国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 ・組織の目的に影響を与える主要な原動力及び傾向 ・外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 b) 内部状況 ・統治、組織体制、役割及びアカウンタビリティ ・方針、目的及びこれらを達成するために策定された戦略 ・資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） ・情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） ・内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 ・組織文化 ・組織が採択した規格、指針及びモデル ・契約関係の形態及び範囲	4.4.2.1	組織は、組織の目的に関連し、かつ、情報セキュリティマネジメントの意図した成果を達成する組織の能力に影響を与える、以下の課題を決定する。[27001-4.1] ・外部の課題 ・内部の課題 これらの課題の決定とは、組織の外部状況及び内部状況の確定のことをいう。外部状況及び内部状況には、以下に例示するものが含まれ得る。 a) 外部状況 1) 国外、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 2) 組織の目的に影響を与える主要な原動力及び傾向 3) 外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 b) 内部状況 1) 統治、組織体制、役割及びアカウンタビリティ 2) 方針、目的及びこれらを達成するために策定された戦略 3) 資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） 4) 情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） 5) 内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 6) 組織文化 7) 組織が採択した規格、指針及びモデル 8) 契約関係の形態及び範囲
4.4.3	利害関係者のニーズ及び期待の理解 [27001-4.2]	4.4.3	利害関係者のニーズ及び期待の理解 [27001-4.2]
4.4.3.1	組織は、利害関係者のニーズ及び期待を理解するために、以下を決定する。[27001-4.2] ・情報セキュリティマネジメントに関連する利害関係者 ・利害関係者の、情報セキュリティに関連する要求事項 利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含めてもよいが、利害関係者には、以下のようなものが含まれる。 ・組織内で情報セキュリティマネジメントプロセスを推進する役割・権限を持つ人又は組織。例えば、以下のようなものをいう。 -情報セキュリティに関する方針等を策定する人又は組織(トップマネジメント等) -セキュリティ管理策を全組織に徹底させる人又は組織(総務部、情報システム部等) -情報セキュリティ監査を行う人又は組織(監査室等) -組織内の情報セキュリティ専門家 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・所属するセキュリティ団体、協会	4.4.3.1	組織は、利害関係者のニーズ及び期待を理解するために、以下を決定する。[27001-4.2] ・情報情報セキュリティマネジメントに関連する利害関係者 ・利害関係者に関連する要求事項 ・要求事項のうち、情報セキュリティマネジメントを通じて取り組むもの 利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含める場合もあるが、利害関係者には、以下に例示する人又は組織が含まれ得る。 ・組織内で情報セキュリティマネジメントプロセスを推進する役割・権限をもつ人又は組織。以下にその例を示す。 a) 情報セキュリティに関する方針等を策定する人又は組織(トップマネジメント等) b) セキュリティ管理策を全組織に徹底させる人又は組織(総務部、情報システム部等) c) 情報セキュリティ監査を行う人又は組織(監査室等) d) 組織内の情報セキュリティ専門家 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・所属するセキュリティ団体、協会
4.4.4	適用範囲の決定 [27001-4.3]	4.4.4	適用範囲の決定 [27001-4.3] 情報セキュリティマネジメントを確立、導入、運用、監視、レビュー、維持及び改善するために、まず適用範囲を明確にし、組織に合った情報セキュリティマネジメントを構築する基盤を整える。
–	情報セキュリティマネジメントを確立、導入、運用、監視、レビュー、維持及び改善するために、まず適用範囲を明確にし、組織に合った情報セキュリティマネジメントを構築する基盤を整える。		
4.4.4.1	組織は、情報セキュリティマネジメントの境界及び適用可能性を明確にし、適用範囲を決定する。[27001-4.3] a) 組織は以下の点を考慮して適用範囲及び境界を定義する。 ・自らの事業 ・体制 ・所在地 ・資産 ・技術の特徴 ・外部及び内部の課題 ・利害関係者の情報セキュリティに関連する要求事項 ・組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係 b) 情報セキュリティマネジメントの目的や目標は、組織の特徴によって異なる。 c) 情報セキュリティマネジメントに対する要求事項はそれぞれの組織の事業によって、外部状況、内部状況の双方があり、これらを考慮して適用範囲を定義する。 ・外部状況には、以下のようなものが含まれる。 – 国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 – 組織の目的に影響を与える主要な原動力及び傾向 – 外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 ・内部状況には、以下のようなものが含まれる。 – 統治、組織体制、役割及びアカウンタビリティ – 方針、目的及びこれらを達成するために策定された戦略 – 資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） – 情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） – 内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 – 組織文化 – 組織が採択した規格、指針及びモデル – 契約関係の形態及び範囲	4.4.4.1	組織は、情報セキュリティマネジメントの境界及び適用可能性を明確にし、適用範囲を決定する。[27001-4.3] ・組織は以下の点を考慮して適用範囲及び境界を定義する。 a) 自らの事業 b) 体制 c) 所在地 d) 資産 e) 技術の特徴 f) 外部及び内部の課題 g) 利害関係者の情報セキュリティに関連する要求事項 h) 組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係 ・情報セキュリティマネジメントの目的や目標は、組織の特徴によって異なる。 ・情報セキュリティマネジメントに対する要求事項はそれぞれの組織の事業によって、外部状況、内部状況の双方があり、これらを考慮して適用範囲を定義する。 a) 外部状況には、以下に例示するものが含まれ得る。 1) 国外、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 2) 組織の目的に影響を与える主要な原動力及び傾向 3) 外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 b) 内部状況には、以下に例示するものが含まれ得る。 1) 統治、組織体制、役割及びアカウンタビリティ 2) 方針、目的及びこれらを達成するために策定された戦略 3) 資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） 4) 情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） 5) 内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 6) 組織文化 7) 組織が採択した規格、指針及びモデル 8) 契約関係の形態及び範囲

番号	(旧)マネジメント基準	番号	(新) マネジメント基準
4.4.5	方針の確立 [27001-5.2 / 6.2 / 5.1]	4.4.5	方針の確立 [27001-5.2 / 6.2 / 5.1]
4.4.5.1	トップマネジメントは、以下を満たす組織の情報セキュリティ方針を確立する。[27001-5.2] ・組織の目的に対して適切であること。 ・情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組 ・情報セキュリティに関連して適用する要求事項を満たすことへのコミットメントを含むこと。 ・情報セキュリティマネジメントの継続的改善へのコミットメントを含むこと。 また、情報セキュリティ方針は情報セキュリティマネジメントにおける判断の基盤となる考え方を記載したものであり、組織の戦略に従って慎重に作成する。	4.4.5.1	トップマネジメントは、以下を満たす組織の情報セキュリティ方針を確立する。[27001-5.2] ・組織の目的に対して適切であること。 ・情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組 ・情報セキュリティに関連して適用する要求事項を満たすことへのコミットメントを含むこと。 ・情報セキュリティマネジメントの継続的改善へのコミットメントを含むこと。 また、情報セキュリティ方針は情報セキュリティマネジメントにおける判断の基盤となる考え方を記載したものであり、組織の戦略に従って慎重に作成する。
4.4.5.2	組織は、情報セキュリティ目的及びそれを達成するための計画を策定する。[27001-6.2] a) 情報セキュリティ目的は、以下を満たすこととする。 ・情報セキュリティ方針と整合していること。 ・（実行可能な場合）測定可能であること。 ・適用される情報セキュリティ要求事項、並びにリスクアセスメント及びリスク対応の結果を考慮に入れること。 b) 情報セキュリティ目的は、関係者に伝達し、必要に応じて更新するとともに、情報セキュリティ目的を達成するための計画においては、以下を決定する。 ・実施事項 ・必要な資源 ・責任者 ・達成期限 ・結果の評価方法	4.4.5.2	組織は、情報セキュリティ目的及びそれを達成するための計画を策定する。[27001-6.2] ・情報セキュリティ目的は、以下を満たすこととする。 a) 情報セキュリティ方針と整合していること。 b) （実行可能な場合）測定可能であること。 c) 適用される情報セキュリティ要求事項、並びにリスクアセスメント及びリスク対応の結果を考慮に入れること。 ・情報セキュリティ目的は、これを監視し、関係者に伝達し、必要に応じて更新し、文書化した情報として利用可能な状態にするとともに、情報セキュリティ目的を達成するための計画においては、以下を決定する。 a) 実施事項 b) 必要な資源 c) 責任者 d) 達成期限 e) 結果の評価方法
4.4.5.3	トップマネジメントは、以下によって、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。[27001-5.1a)] ・情報セキュリティ方針及び情報セキュリティ目的を確立すること。 ・情報セキュリティ方針及び情報セキュリティ目的は組織の戦略的な方向性と相矛盾しないこと。 また、情報セキュリティ方針は組織に伝えられるように文書化され、しかるべき方法で利害関係者が入手できるようにするとともに、トップマネジメントが情報セキュリティ方針にコミットした証拠を、以下のような記録をもって示す。 ・文書化された情報セキュリティ方針への署名 ・情報セキュリティ方針が議論された会議の議事録 これらはトップマネジメントの責任を明確にするために実施する。	4.4.5.3	トップマネジメントは、以下によって、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。[27001-5.1a)] ・情報セキュリティ方針及び情報セキュリティ目的を確立すること。 ・情報セキュリティ方針及び情報セキュリティ目的は組織の戦略的な方向性と相矛盾しないこと。 また、情報セキュリティ方針は組織に伝えられるように文書化され、しかるべき方法で利害関係者が入手できるようにするとともに、トップマネジメントが情報セキュリティ方針にコミットした証拠を記録として保管する。記録の例を以下に示す。 ・文書化された情報セキュリティ方針への署名 ・情報セキュリティ方針が議論された会議の議事録 これらはトップマネジメントの責任を明確にするために実施する。
4.4.6	リスク及び機会に対処する活動 [27001-6.1]	4.4.6	リスク及び機会に対処する活動 [27001-6.1]
4.4.6.1	リスク及び機会を決定する。[27001-6.1.1] a) 組織は、外部及び内部の課題、利害関係者の情報セキュリティに関連する要求事項を考慮し、以下のために対処する必要があるリスク及び機会を決定する。 ・情報セキュリティマネジメントが、組織が意図した成果を達成する。 ・望ましくない影響を防止又は低減する。 ・継続的改善を達成する。 当該決定の際、組織は、以下を計画する。 ・決定したリスク及び機会に対処する活動 ・リスク及び機会に対処する活動の情報セキュリティマネジメントプロセスへの統合及び実施方法 ・リスク及び機会に対処する活動の有効性の評価方法 b) リスク及び機会に対処する活動の記録として、具体的な対処計画（実施時期、実施内容、実施者、実施場所、実施に必要な資源などを規定した計画）を作成していることを確認するとともに、当該計画を作成する際、各対処計画が、情報セキュリティマネジメントプロセスの一部として実施されるよう、考慮するとともに、当該対処の有効性を評価する方法（実施状況や実施したことによる効果を評価する方法）を作成していることも確認する。	4.4.6.1	リスク及び機会を決定する。[27001-6.1.1] ・組織は、外部及び内部の課題、利害関係者の情報セキュリティに関連する要求事項を考慮し、以下のために対処する必要があるリスク及び機会を決定する。 a) 情報セキュリティマネジメントが、組織が意図した成果を達成する。 b) 望ましくない影響を防止又は低減する。 c) 継続的改善を達成する。 d) 当該決定の際、組織は、以下を計画する。 1) 決定したリスク及び機会に対処する活動 2) リスク及び機会に対処する活動の情報セキュリティマネジメントプロセスへの統合及び実施方法 3) リスク及び機会に対処する活動の有効性の評価方法 ・リスク及び機会に対処する活動の記録として、具体的な対処計画（実施時期、実施内容、実施者、実施場所、実施に必要な資源などを規定した計画）を作成していることを確認するとともに、当該計画を作成する際、各対処計画が、情報セキュリティマネジメントプロセスの一部として実施されるよう、考慮するとともに、当該対処の有効性を評価する方法（実施状況や実施したことによる効果を評価する方法）を作成していることも確認する。

番号	(旧)マネジメント基準	番号	(新) マネジメント基準
4.4.7	情報セキュリティリスクアセスメント [27001-6.1.2]	4.4.7	情報セキュリティリスクアセスメント [27001-6.1.2]
4.4.7.1	組織は、以下によって、情報セキュリティリスクアセスメントのプロセスを定め、適用する。[27001-6.1.2a) / 6.1.2b)] a) 以下を含む情報セキュリティのリスク基準を確立し、維持する。 ・リスク受容基準 ・情報セキュリティリスクアセスメントを実施するための基準 b) リスク受容基準に、以下を反映するよう、考慮する。 ・組織の価値観 ・目的 ・資源 c) リスク受容基準を策定する際には、以下の点を考慮する。 ・原因及び発生し得る結果の特質及び種類、並びにこれらの測定方法 ・発生頻度 ・発生頻度、結果を考える時間枠 ・リスクレベルの決定方法 ・利害関係者の見解 ・リスク基準は、法令及び規制の要求事項、並びに組織が合意するその他の要求事項によって、組織に課せられるもの又は策定されるものもあること。 d) 情報セキュリティアセスメントを繰り返し実施した際に、以下の結果を生み出すこと。 ・情報セキュリティリスクアセスメントの結果に、一貫性及び妥当性があること。 ・情報セキュリティリスクアセスメントの結果が比較可能であること。 なお、情報セキュリティマネジメントにおけるリスクアセスメント手法には、定番といえるものがなく、それぞれの組織に適合したものを選択している場合が多いことから、必要に応じてツールを利用するなどが必要になる。	4.4.7.1	組織は、以下によって、情報セキュリティリスクアセスメントのプロセスを定め、適用する。[27001-6.1.2a) / 6.1.2b)] ・以下を含む情報セキュリティのリスク基準を確立し、維持する。 a) リスク受容基準 b) 情報セキュリティリスクアセスメントを実施するための基準 ・リスク受容基準に、以下を反映するよう、考慮する。 a) 組織の価値観 b) 目的 c) 資源 ・リスク受容基準を策定する際には、以下の点を考慮する。 a) 原因及び発生し得る結果の特質及び種類、並びにこれらの測定方法 b) 発生頻度 c) 発生頻度、結果を考える時間枠 d) リスクレベルの決定方法 e) 利害関係者の見解 f) リスク基準は、法令及び規制の要求事項、並びに組織が合意するその他の要求事項によって、組織に課せられるもの又は策定されるものもあること。 ・情報セキュリティリスクアセスメントを繰り返し実施した際に、以下の結果を生み出すこと。 a) 情報セキュリティリスクアセスメントの結果に、一貫性及び妥当性があること。 b) 情報セキュリティリスクアセスメントの結果が比較可能であること。 なお、情報セキュリティマネジメントにおけるリスクアセスメント手法には、定番といえるものがなく、それぞれの組織に適合したものを選択している場合が多いことから、必要に応じてツールを利用することなどが必要になる。
4.4.7.2	組織は、以下によって、情報セキュリティリスクを特定する。[27001-6.1.2c)] a) 情報セキュリティリスクアセスメントのプロセスを適用し、情報の機密性、完全性及び可用性の喪失に伴うリスクを特定する。 b) リスクを特定する過程において、リスク所有者を特定する。 c) リスクを特定する際には、以下について考慮する。 ・リスク源 が組織の管理下にあるか否かに関わらず、リスク源又はリスクの原因が明らかでないリスクも特定の対象にすること。 ・波及効果及び累積効果を含めた、特定の結果の連鎖を注意深く検討すること。 ・何が起こり得るのかの特定に加えて、考えられる原因及びどのような結果が引き起こされることがあるのかを示すシナリオ ・全ての重大な原因及び結果 ・以下を特定すること。 －リスク源 －影響を受ける領域、事象 －原因及び起こり得る結果 この段階で特定されなかったリスクは、今後の分析の対象から外されてしまうため、ある機会を追及しなかったことに伴うリスクも含め、リスクの包括的な一覧を作成する。	4.4.7.2	組織は、以下によって、情報セキュリティリスクを特定する。[27001-6.1.2c)] ・情報セキュリティリスクアセスメントのプロセスを適用し、情報の機密性、完全性及び可用性の喪失に伴うリスクを特定する。 ・リスクを特定する過程において、リスク所有者を特定する。 ・リスクを特定する際には、以下について考慮する。 a) リスク源が組織の管理下にあるか否かに関わらず、リスク源又はリスクの原因が明らかでないリスクも特定の対象にすること。 b) 波及効果及び累積効果を含めた、特定の結果の連鎖を注意深く検討すること。 c) 何が起こり得るのかの特定に加えて、考えられる原因及びどのような結果が引き起こされることがあるのかを示すシナリオ d) 全ての重大な原因及び結果 e) 以下を特定すること。 1) リスク源 2) 影響を受ける領域、事象 3) 原因及び起こり得る結果 この段階で特定されなかったリスクは、今後の分析の対象から外されてしまうため、ある機会を追及しなかったことに伴うリスクも含め、リスクの包括的な一覧を作成する。
4.4.7.3	組織は、以下によって、情報セキュリティリスクを分析する。[27001-6.1.2d)] a) 以下の手順によりリスク分析を行う。 ・特定されたリスクが実際に生じた場合に起こり得る結果の分析を行う。 ・特定されたリスクの発生頻度の分析を行う。 ・リスクレベルを決定する。 ・特定した脅威やぜい弱性を基に、以下の点を考慮する。 －セキュリティインシデントが発生した場合の事業影響度 －セキュリティインシデントの発生頻度 －管理策が適用されている場合はその効果 b) リスク分析の際には、以下の点についても考慮する。 ・リスクの原因及びリスク源 ・リスクの好ましい結果及び好ましくない結果 ・リスクの発生頻度 ・リスクの結果及び発生頻度に影響を与える要素 なお、リスク分析は、状況に応じて、定性的、半定量的、定量的、又はそれらを組み合わせた手法で行うことが可能である。	4.4.7.3	組織は、以下によって、情報セキュリティリスクを分析する。[27001-6.1.2d)] ・以下の手順によりリスク分析を行う。 a) 特定されたリスクが実際に生じた場合に起こり得る結果の分析を行う。 b) 特定されたリスクの発生頻度の分析を行う。 c) リスクレベルを決定する。 d) 特定した脅威やぜい弱性を基に、以下の点を考慮する。 1) セキュリティインシデントが発生した場合の事業影響度 2) セキュリティインシデントの発生頻度 3) 管理策が適用されている場合はその効果 ・リスク分析の際には、以下の点についても考慮する。 a) リスクの原因及びリスク源 b) リスクの好ましい結果及び好ましくない結果 c) リスクの発生頻度 d) リスクの結果及び発生頻度に影響を与える要素 なお、リスク分析は、状況に応じて、定性的、半定量的、定量的、又はそれらを組み合わせた手法で行うことが可能である。
4.4.7.4	組織は、以下によって、情報セキュリティリスクを評価する。[27001-6.1.2e)] ・リスク分析の結果、決定されたリスクレベルとリスク基準との比較をする。 ・リスク対応のための優先順位付けを行う。 ・リスク評価の結果は今後の改善に利用するため保管する。 なお、リスク対応の優先順位を決定する際には、より広い範囲の状況を考慮し、他者が負うリスクの受容レベルについて考慮するとともに、法令、規制、その他の要求事項についても考慮する。	4.4.7.4	組織は、以下によって、情報セキュリティリスクを評価する。[27001-6.1.2e)] ・リスク分析の結果、決定されたリスクレベルとリスク基準との比較をする。 ・リスク対応のための優先順位付けを行う。 ・リスク評価の結果は今後の改善に利用するため保管する。 なお、リスク対応の優先順位を決定する際には、より広い範囲の状況を考慮し、他者が負うリスクの受容レベルについて考慮するとともに、法令、規制、その他の要求事項についても考慮する。

番号	(旧)マネジメント基準	番号	(新) マネジメント基準
4.4.8	情報セキュリティリスク対応 [27001-6.1.3]	4.4.8	情報セキュリティリスク対応 [27001-6.1.3]
4.4.8.1	組織は、情報セキュリティアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。[27001-6.1.3a)] 情報セキュリティリスク対応の選択肢には、以下が含まれる。 ・リスクを生じさせる活動を開始又は継続しないと決定することによるリスクの回避 ・ある機会を目的としたリスクの引受け又はリスクの負担 ・リスク源の除去 ・発生頻度の変更 ・結果の変更 ・（契約及びリスクファイナンス を含む）他者とのリスクの共有 ・情報に基づいた意思決定によるリスクの保有 さらに、リスク対応の評価や改善に役立てるため、どの選択肢を選んだ場合も、その理由を明確にし、記載する。	4.4.8.1	組織は、情報セキュリティリスクアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。[27001-6.1.3a)] ・情報セキュリティリスク対応の選択肢には、以下が含まれる。 a) リスクを生じさせる活動を開始又は継続しないと決定することによるリスクの回避 b) ある機会を目的としたリスクの引受け又はリスクの負担 c) リスク源の除去 d) 発生頻度の変更 e) 結果の変更 f) （契約及びリスクファイナンス を含む）他者とのリスクの共有 g) 情報に基づいた意思決定によるリスクの保有 さらに、リスク対応の評価や改善に役立てるため、どの選択肢を選んだ場合も、その理由を明確にし、記載する。
4.4.8.2	組織は、選定した情報セキュリティリスク対応の実施に必要な全ての管理策を決定する。[27001-6.1.3b)] リスク対応のための方針を決めた上で、管理策の目的（管理目的）及び管理策について検討する。以下を考慮しつつ、対応による効果と対応に必要な費用及び労力のバランスを取り、適切な情報セキュリティ対応の選択肢を選定する。 ・リスクの受容可能レベル ・関連する法令 ・規制や契約上の要求事項 ・その他の社会的責任 なお、具体的な管理策の選定においては、管理目的に対応した「管理策基準」から適切なものを選択するが、「管理策基準」はすべてを網羅しているわけではないので、組織の事業や業務などによってその他の管理策を追加してもよい。	4.4.8.2	組織は、選定した情報セキュリティリスク対応の実施に必要な全ての管理策を決定する。[27001-6.1.3b)] ・リスク対応のための方針を決めた上で、管理策の目的（管理目的）及び管理策について検討する。以下を考慮しつつ、対応による効果と対応に必要な費用及び労力のバランスを取り、適切な情報セキュリティ対応の選択肢を選定する。 a) リスクの受容可能レベル b) 関連する法令 c) 規制や契約上の要求事項 d) その他の社会的責任 なお、具体的な管理策の選定においては、管理目的に対応した「管理策基準」から適切なものを選択するが、「管理策基準」はすべてを網羅しているわけではないので、組織の事業や業務などによってその他の管理策を追加してもよい。
4.4.8.3	組織は、管理策が見落とされていないことを検証する。[27001-6.1.3c)] 必要な管理策の見落としがないか、管理策基準を参照するが、管理策基準に示す管理目的及び管理策以外の管理目的及び管理策が必要になった場合、他の管理目的及び管理策を追加することができる。	4.4.8.3	組織は、管理策が見落とされていないことを検証する。[27001-6.1.3c)] ・必要な管理策の見落としがないか、管理策基準を参照するが、管理策基準に示す管理目的及び管理策以外の管理目的及び管理策が必要になった場合、他の管理目的及び管理策を追加することができる。
4.4.8.4	組織は、情報セキュリティリスク対応計画を策定する。[27001-6.1.3e)] a)情報セキュリティリスク対応計画には、以下を含む。 ・期待される効果を含む、対応選択肢選定の理由 ・情報セキュリティリスク対応計画の承認者及び対応計画の実施責任者 ・対応内容 ・必要な資源 ・費用・労力、制約 ・後日の報告、監視に必要な要求事項 ・対応工程における節目ごとの目標 ・対応時期及び日程 b) 責任及び権限について 情報セキュリティマネジメントにおいては最終的な承認をトップマネジメントが行っていることがほとんどであり、責任がトップマネジメントに集中している。 一方で、情報セキュリティリスクアセスメント及びリスク対応については、責任及び権限を持つリスク所有者が、責任及び権限を持つ。 リスク所有者は、トップマネジメント、又はトップマネジメントから任命され、責任及び権限が委譲された者であることが多いことから、情報セキュリティマネジメントにおいて、トップマネジメント及びリスク所有者が、どのような責任を持つかについて明確にする。	4.4.8.4	組織は、情報セキュリティリスク対応計画を策定する。[27001-6.1.3e)] ・情報セキュリティリスク対応計画には、以下を含む。 a) 期待される効果を含む、対応選択肢選定の理由 b) 情報セキュリティリスク対応計画の承認者及び対応計画の実施責任者 c) 対応内容 d) 必要な資源 e) 費用・労力、制約 f) 後日の報告、監視に必要な要求事項 g) 対応工程における節目ごとの目標 h) 対応時期及び日程 ・情報セキュリティマネジメントにおいては最終的な承認をトップマネジメントが行っていることがほとんどであり、責任がトップマネジメントに集中している。一方で、情報セキュリティリスクアセスメント及びリスク対応については、責任及び権限をもつリスク所有者が、責任及び権限をもつ。リスク所有者は、トップマネジメント、又はトップマネジメントから任命され、責任及び権限が委譲された者であることが多いことから、情報セキュリティマネジメントにおいて、トップマネジメント及びリスク所有者が、どのような責任をもつかについて明確にする。
4.4.8.5	組織は、リスク所有者から、情報セキュリティリスク対応計画について承認を得、かつ、リスク所有者に、残留している情報セキュリティリスクを受け入れてもらう。[27001-6.1.3f)] すべてのリスクについて管理目的や管理策を選択した時点で、残留リスクについて明確にし、今後の対応計画を作成する。計画の作成においては以下の点について考慮する。 ・技術的に対応可能になる時期 ・コスト的に対応可能になる時期 残留リスクについては、定期的に見直しを行い、必要に応じて、対応の対象とするとともに、リスク対応後の残留リスクについては、リスク所有者のほか、経営陣やその他の利害関係者に認識させることを考慮する。 また、リスク所有者の責任を明確にするために、承認された会議の議事録を正しく保管する。	4.4.8.5	組織は、リスク所有者から、情報セキュリティリスク対応計画について承認を得、かつ、リスク所有者に、残留している情報セキュリティリスクを受け入れてもらう。[27001-6.1.3f)] ・すべてのリスクについて管理目的や管理策を選択した時点で、残留リスクについて明確にし、今後の対応計画を作成する。計画の作成においては以下の点について考慮する。 a) 技術的に対応可能になる時期 b) コスト的に対応可能になる時期 ・残留リスクについては、定期的に見直しを行い、必要に応じて、対応の対象とするとともに、リスク対応後の残留リスクについては、リスク所有者のほか、管理層やその他の利害関係者に認識させることを考慮する。また、リスク所有者の責任を明確にするために、承認された会議の議事録を正しく保管する。
4.5	情報セキュリティマネジメントの運用 [27001-8]	4.5	情報セキュリティマネジメントの運用 [27001-8]
4.5.1	資源管理 [27001-7.1 / 5.1]	4.5.1	資源管理 [27001-7.1 / 5.1]
4.5.1.1	組織は、情報セキュリティマネジメントの確立、実施、維持及び継続的改善に必要な資源を決定し、提供する。[27001-7.1] 管理目的を満たすためには、継続的に管理策を実施するとともに、人員の増加、システムの増加などの環境の変化に対応するために、適切な時期に適切に提供できるよう、経営資源を確保する。	4.5.1.1	組織は、情報セキュリティマネジメントの確立、実施、維持及び継続的改善に必要な資源を決定し、提供する。[27001-7.1] ・管理目的を満たすためには、継続的に管理策を実施するとともに、人員の増加、システムの増加などの環境の変化に対応するために、適切な時期に適切に提供できるよう、経営資源を確保する。
4.5.1.2	トップマネジメントは、情報セキュリティマネジメントに必要な資源が利用可能であることを確実にするため、以下のような資源を割り当てる。[27001-5.1c)] ・情報セキュリティマネジメントの各プロセスに必要な人又は組織 ・情報セキュリティマネジメントの各プロセスに必要な設備、装置、システム ・上記に必要な費用	4.5.1.2	トップマネジメントは、情報セキュリティマネジメントに必要な資源が利用可能であることを確実にするため、以下の資源を割り当てる。[27001-5.1c)] ・情報セキュリティマネジメントの各プロセスに必要な人又は組織 ・情報セキュリティマネジメントの各プロセスに必要な設備、装置、システム ・上記に必要な費用

番号	(旧)マネジメント基準	番号	（新）マネジメント基準
4.5.2	力量、認識 [27001-7.2 / 7.3 / 5.1]	4.5.2	力量、認識 [27001-7.2 / 7.3 / 5.1]
4.5.2.1	トップマネジメントは、有効な情報セキュリティマネジメント及びその要求事項への適合の重要性を伝達する。[27001-5.1d)] トップマネジメントは情報セキュリティマネジメントについて責任を負うが、実施においては組織全体の協力が必要であることを、情報セキュリティ方針と共に関係者に伝える。 また、組織が同じ規定に従って同じ判断ができるように、情報分類等の基準を策定するが、個人情報のように組織によって解釈が一部異なる情報の場合は、一般的な考え方に加え、自社の考え方を明確にした上で、関係者に伝える。	4.5.2.1	トップマネジメントは、有効な情報セキュリティマネジメント及びその要求事項への適合の重要性を伝達する。[27001-5.1d)] ・トップマネジメントは情報セキュリティマネジメントについて責任を負うが、実施においては組織全体の協力が必要であることを、情報セキュリティ方針と共に関係者に伝える。また、組織が同じ規定に従って同じ判断ができるように、情報分類等の基準を策定するが、個人情報のように組織によって解釈が一部異なる情報の場合は、一般的な考え方に加え、自社の考え方を明確にした上で、関係者に伝える。
4.5.2.2	組織は、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。[27001-7.2a)] 情報セキュリティマネジメントに関係する業務及び影響のある業務を特定し、役割を明確にした業務分掌を作成する。これらの業務分掌においては以下の点を明確にする。 ・役職名 ・業務内容 ・担当者の責任範囲 ・業務に必要な知識 ・業務に必要な資格 ・業務に必要な経験 知識や資格、経験などは環境や目的の変化によって変更される可能性があるため、最新の情報となるように随時見直しを行う。	4.5.2.2	組織は、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。[27001-7.2a)] ・情報セキュリティマネジメントに関係する業務及び影響のある業務を特定し、役割を明確にした業務分掌を作成する。これらの業務分掌においては以下の点を明確にする。 a) 役職名 b) 業務内容 c) 担当者の責任範囲 d) 業務に必要な知識 e) 業務に必要な資格 f) 業務に必要な経験 知識や資格、経験などは環境や目的の変化によって変更される可能性があるため、最新の情報となるように随時見直しを行う。
4.5.2.3	組織は、適切な教育、訓練又は経験に基づいて、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）が力量を備えられるようにする。[27001-7.2b)] 適用される処置には、例えば、現在雇用している人々に対する教育訓練の提供、指導の実施、配置転換の実施などがある（教育や訓練などが間に合わないと判断される場合には相応の力量を有した要員の雇用が、また、社内業務との関連が少ない業務においては外部委託などがある。）。	4.5.2.3	組織は、適切な教育、訓練又は経験に基づいて、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）が力量を備えられるようにする。[27001-7.2b)] ・適用される処置には、例えば、現在雇用している人々に対する教育訓練の提供、指導の実施、配置転換の実施などがある（教育や訓練などが間に合わないと判断される場合には相応の力量を有した要員の雇用が、また、社内業務との関連が少ない業務においては外部委託などがある。）。
4.5.2.4	組織は、必要な力量を身に着けるための処置をとり、とった処置の有効性を評価する。[27001-7.2c)] 必要な力量を身に着けるための処置としては、教育訓練が重要である。教育は「必要な知識を得させる」、訓練は「必要なスキル及び経験を得させる」ために実施する。教育の内容は一般的な脅威やぜい弱性などの知識だけではなく、業務上のリスクについてなど、組織の特徴を反映した内容を盛り込むなど、実効性のある内容となるようにする。 教育及び訓練を実施した結果、必要な力量が持てたかどうかを確認するために、以下を実施する。 ・知識の確認テスト ・スキルの実習テスト ・チェックリストなどによるベンチマーク 実施結果については記録し、要員選択の客観性を確保する。	4.5.2.4	組織は、必要な力量を身につけるための処置をとり、とった処置の有効性を評価する。[27001-7.2c)] ・必要な力量を身に着けるための処置としては、教育訓練が重要である。教育は「必要な知識を得させる」、訓練は「必要なスキル及び経験を得させる」ために実施する。教育の内容は一般的な脅威やぜい弱性などの知識だけではなく、業務上のリスクや、組織の特徴を反映した内容を盛り込むなど、実効性のある内容となるようにする。教育及び訓練を実施した結果、必要な力量が持てたかどうかを確認するための取組を実施する。取組の例を以下に示す。 a) 知識の確認テスト b) スキルの実習テスト c) チェックリストなどによるベンチマーク 実施結果については記録し、要員選択の客観性を確保する。
4.5.2.5	組織は、力量を常に把握し、その証拠として、適切な文書化した情報を組織が定めた期間保持する。[27001-7.2d)] 教育、訓練については以下を検討し、定期的に実施する。 ・教育・訓練基本計画 ・教育・訓練実施計画 ・確認テスト又は評価報告 教育や訓練の一部を免除する場合は、それがどの技能や経験、資格に当てはまるかを明確にし、それぞれの担当者について調査し、一覧にする。資格については有効期限などを明確にし、更新する。	4.5.2.5	組織は、力量を常に把握し、その証拠として、適切な文書化した情報を組織が定めた期間保持する。[27001-7.2d)] ・教育、訓練については以下の例示を参考に検討し、定期的に実施する。 a) 教育、訓練基本計画 b) 教育、訓練実施計画 c) 確認テスト又は評価報告 ・教育や訓練の一部を免除する場合は、それがどの技能や経験、資格に当てはまるかを明確にし、それぞれの担当者について調査し、一覧にする。資格については有効期限などを明確にし、更新する。
4.5.2.6	組織の管理下で働く人々は、情報セキュリティ方針を認識する。[27001-7.3a)] 情報セキュリティの活動について、組織が定めた目的と重要性について、情報セキュリティ方針の通達や教育の一環として周知徹底することによって、管理策がなぜ実施されているのかについての関係者の理解を深める。	4.5.2.6	組織の管理下で働く人々は、情報セキュリティ方針を認識する。[27001-7.3a)] ・情報セキュリティの活動について、組織が定めた目的と重要性について、情報セキュリティ方針の通達や教育の一環として周知徹底することによって、管理策がなぜ実施されているのかについて関係者の理解を深める。
4.5.2.7	組織の管理下で働く人々は、情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティマネジメントの有効性に対する自らの貢献を認識する。[27001-7.3b)] 以下の点について組織の管理下で働く人々に伝えることによって、各人の役割及び情報セキュリティマネジメントの有効性に対する自らの貢献を明確にする。 ・情報セキュリティマネジメントにおけるそれぞれの役割 ・役割を実行するための業務と手順（異常を検知した場合の報告手順も含む。） ・これらが記載された文書の所在	4.5.2.7	組織の管理下で働く人々は、情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティマネジメントの有効性に対する自らの貢献を認識する。[27001-7.3b)] ・以下の点について組織の管理下で働く人々に伝えることによって、各人の役割及び情報セキュリティマネジメントの有効性に対する自らの貢献を明確にする。 a) 情報セキュリティマネジメントにおけるそれぞれの役割 b) 役割を実行するための業務と手順（異常を検知した場合の報告手順も含む。） c) これらが記載された文書の所在
4.5.2.8	組織の管理下で働く人々は、情報セキュリティマネジメントの要求事項に適合しないことの意味を認識する。[27001-7.3c)]	4.5.2.8	組織の管理下で働く人々は、情報セキュリティマネジメントの要求事項に適合しないことの意味を認識する。[27001-7.3c)]

番号	(旧)マネジメント基準	番号	(新) マネジメント基準
4.5.3	コミュニケーション [27001-7.4]	4.5.3	コミュニケーション [27001-7.4]
4.5.3.1	組織は、情報セキュリティマネジメントに関連する内部及び外部のコミュニケーションを実施する必要性を決定する。[27001-7.4] a) 内部及び外部のコミュニケーションを実施する際は、以下を考慮することとする。 ・コミュニケーションの内容（何を伝達するか。） ・コミュニケーションの実施時期 ・コミュニケーションの対象者 ・コミュニケーションの実施者 ・コミュニケーションの実施プロセス b) 内部コミュニケーションでは、以下に示すような者と、適宜及び定期的なコミュニケーションを実施する。 ・トップマネジメント ・情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者 ・情報セキュリティマネジメントのパフォーマンスをトップマネジメント又は組織内に報告する権限者 ・組織内の従業員 c) 外部コミュニケーションでは、以下に示すような者と、必要に応じて、コミュニケーションを実施する。 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・所属するセキュリティ団体、協会	4.5.3.1	組織は、情報セキュリティマネジメントに関連する内部及び外部のコミュニケーションを実施する必要性を決定する。[27001-7.4] ・内部及び外部のコミュニケーションを実施する際は、以下を考慮することとする。 a) コミュニケーションの内容 b) コミュニケーションの実施時期 c) コミュニケーションの対象者 d) コミュニケーションの方法 ・内部コミュニケーションでは、以下の例示を参考に、組織の情報セキュリティマネジメントの実施に不可欠な者と、適宜及び定期的なコミュニケーションを実施する。 a) トップマネジメント b) 情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者 c) 情報セキュリティマネジメントのパフォーマンスをトップマネジメント又は組織内に報告する権限者 d) 組織内の従業員 ・外部コミュニケーションでは、以下の例示を参考に、組織の情報セキュリティマネジメントの実施に不可欠な者と、必要に応じて、コミュニケーションを実施する。 a) 取引先、パートナー、サプライチェーン上の関係者 b) 親会社、グループ会社 c) 当該組織のセキュリティを監督する省庁、政府機関 d) 所属するセキュリティ団体、協会
4.5.4	情報セキュリティマネジメントの運用の計画及び管理 [27001-8.1]	4.5.4	情報セキュリティマネジメントの運用の計画策定及び管理 [27001-8.1]
4.5.4.1	組織は、情報セキュリティ要求事項を満たすため、リスク及び機会に対処する活動を実施するために必要なプロセスを計画し、実施し、かつ管理する。[27001-8.1]	4.5.4.1	組織は、次に示す事項の実施によって情報セキュリティ要求事項を満たすため、リスク及び機会に対処する活動を実施するために必要なプロセスを計画し、実施し、かつ管理する。[27001-8.1] ・プロセスに関する基準の設定 ・その基準に従った、プロセスの管理の実施
4.5.4.2	組織は、情報セキュリティ目的を達成するための計画を実施する。[27001-8.1]		
4.5.4.3	組織は、計画通りに実施されたことを確信するために、文書化した情報を保持する。[27001-8.1] 文書化した情報に、以下の情報が集められているかどうかを確認する。 ・管理策の実施状況 ・管理策の有効性 ・管理策を取り巻く環境の変化 また、これらの情報を把握し判断する体制を構築する。	4.5.4.2	組織は、計画通りに実施されたことを確信するために、文書化した情報を利用可能な状態にする。[27001-8.1] ・文書化した情報に、以下の情報が集められているかどうかを確認する。 a) 管理策の実施状況 b) 管理策の有効性 c) 管理策を取り巻く環境の変化 また、これらの情報を把握し判断する体制を構築する。
4.5.4.4	組織は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置をとる。[27001-8.1]	4.5.4.3	組織は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置を講じる。[27001-8.1]
4.5.4.5	組織は、外部委託するプロセスを決定し、かつ、管理する。[27001-8.1]	–	（対応項なし）
4.5.5	情報セキュリティリスクアセスメントの実施 [27001-8.2 / 8.3]	4.5.5	情報セキュリティリスクアセスメントの実施 [27001-8.2 / 8.3]
4.5.5.1	組織は、以下のいずれかの場合において、情報セキュリティリスクアセスメントを実施する。[27001-8.2] ・あらかじめ定めた間隔 ・重大な変更が提案された場合 ・重大な変化が生じた場合	4.5.5.1	組織は、以下のいずれかの場合において、情報セキュリティリスクアセスメントを実施する。[27001-8.2] ・あらかじめ定めた間隔 ・重大な変更が提案された場合 ・重大な変化が生じた場合
4.5.5.2	組織は、情報セキュリティリスク対応計画を実施する。[27001-8.3] 情報セキュリティリスク対応計画の実施においては、明確にされた個々の責任について全うしていることを確認するための方策を講じる。	4.5.5.2	組織は、情報セキュリティリスク対応計画を実施する。[27001-8.3] ・情報セキュリティリスク対応計画の実施においては、明確にされた個々の責任について全うしていることを確認するための方策を講じる。
4.5.5.3	トップマネジメントは、情報セキュリティリスク対応計画のために十分な経営資源を提供する。 情報セキュリティリスク対応計画には相応の経営資源が必要になるところ、以下の点について考慮する。 ・管理策の導入及び運用にかかる費用、人員、作業工数、技術 ・セキュリティインシデント発生時の一時対応にかかる費用 ・その他のリスク対応にかかる費用 運用においては管理策の効果測定などを実施するために必要な経営資源について考察し、予算化する。	4.5.5.3	トップマネジメントは、情報セキュリティリスク対応計画のために十分な経営資源を提供する。 ・情報セキュリティリスク対応計画には相応の経営資源が必要になるところ、以下の点について考慮する。 a) 管理策の導入及び運用にかかる費用、人員、作業工数、技術 b) セキュリティインシデント発生時の一時対応にかかる費用 c) その他のリスク対応にかかる費用 運用においては管理策の効果測定などを実施するために必要な経営資源について考察し、予算化する。
4.6	情報セキュリティマネジメントの監視及びレビュー [27001-5.1 / 8.2 / 9 / 10.2]	4.6	情報セキュリティマネジメントの監視及びレビュー [27001-5.1 / 8.2 / 9 / 10.2]
4.6.1	有効性の継続的改善 [27001-10.2 / 8.2 / 9.2 / 9.3 / 5.1]	4.6.1	有効性の継続的改善 [27001-10.2 / 8.2 / 9.2 / 9.3 / 5.1]
4.6.1.1	組織は、以下を実施し、情報セキュリティマネジメントの適切性、妥当性及び有効性を継続的に改善する。[27001-10.2 / 8.2 / 9.2 / 9.3] ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・トップマネジメントによる定期的なマネジメントレビュー 継続的改善においては、これまで実施してきた管理策だけはなく、環境の変化に伴う新たな脅威やぜい弱性についても不適合を検出し処置する。	4.6.1.1	組織は、以下を実施し、情報セキュリティマネジメントの適切性、妥当性及び有効性を継続的に改善する。[27001-10.2 / 8.2 / 9.2 / 9.3] ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・トップマネジメントによる定期的なマネジメントレビュー 継続的改善においては、これまで実施してきた管理策だけはなく、環境の変化に伴う新たな脅威やぜい弱性についても不適合を検出し処置する。
4.6.1.2	トップマネジメントは、継続的改善を促進する。[27001-5.1g)] 4.6.1.1.を実施するための、役割、責任及び権限を割り当て、実施するよう関係者に伝達する。	4.6.1.2	トップマネジメントは、継続的改善を促進する。[27001-5.1g)] ・4.6.1.1.を実施するための、役割、責任及び権限を割り当て、実施するよう関係者に伝達する。

番号	(旧)マネジメント基準	番号	（新）マネジメント基準
4.6.2	パフォーマンス評価 [27001-9]	4.6.2	パフォーマンス評価 [27001-9]
4.6.2.1	組織は、情報セキュリティパフォーマンス及び情報セキュリティマネジメントの有効性を継続的に評価し、以下を決定する。[27001-9.1] ・必要とされる監視及び測定の対象（情報セキュリティプロセス及び管理策を含む。） ・妥当な結果を確実にするための、監視、測定、分析及び評価の方法（比較可能で再現可能な結果を生み出す方法とする。） ・監視及び測定の実施時期及び頻度 ・監視及び測定の実施者 ・監視及び測定の結果の、分析（因果関係、相関関係を含む）及び評価の時期及び頻度 ・監視及び測定の結果の、分析及び評価の実施者 ・分析及び評価の結果に応じた対応措置 ・分析及び評価の結果の報告頻度	4.6.2.1	組織は、以下を決定し、その結果の証拠として文書化した情報を利用可能な状態とするとともに、情報セキュリティパフォーマンス及び情報セキュリティマネジメントの有効性を継続的に評価する。[27001-9.1] ・必要とされる監視及び測定の対象（情報セキュリティプロセス及び管理策を含む。） ・妥当な結果を確実にするための、監視、測定、分析及び評価の方法（妥当と考えられる、比較可能で再現可能な結果を生み出す方法とする。） ・監視及び測定の実施時期及び頻度 ・監視及び測定の実施者 ・監視及び測定の結果の、分析（因果関係、相関関係を含む）及び評価の時期及び頻度 ・監視及び測定の結果の、分析及び評価の実施者 ・分析及び評価の結果に応じた対応措置 ・分析及び評価の結果の報告頻度
4.6.2.2	組織は、あらかじめ定めた間隔で内部監査を実施する。[27001-9.2a) / 9.2b)] a) 内部監査を実施する際は、以下を確認する。 ・以下に適合していること。 －情報セキュリティマネジメントに関して、組織自体が規定した要求事項 －本マネジメント基準の要求事項 ・情報セキュリティマネジメントが有効に実施され、維持されていること。 b) 内部監査は、管理策の有効性を総合的に確認するために定期的に実施し、計画及び結果について以下の文書で管理する。 ・内部監査基本計画 ・内部監査実施計画 ・内部監査報告書 基本計画書では対象範囲、目的、管理体制及び期間又は期日について、実施計画では実施時期や実施場所、実施担当者及びその割当て及び詳細な監査の手法についてあらかじめ決める。予定通り実施されたことを証明するためにも、実施報告書を作成する。 c) 適合性の監査においては、以下の項目を対象に含む。 ・関連する法令又は規制の要求事項 ・情報セキュリティリスクアセスメントなどによって特定された情報セキュリティ要　求事項 d) 情報セキュリティマネジメントが有効に実施され、維持されていることの監査においては、以下の項目を対象に含む。 ・管理策の有効性及び維持 ・管理策が期待通りに実施されていること。	4.6.2.2	組織は、あらかじめ定めた間隔で内部監査を実施する。[27001-9.2a) / 9.2b)] ・内部監査を実施する際は、以下を確認する。 a) 以下に適合していること。 1) 情報セキュリティマネジメントに関して、組織自体が規定した要求事項 2) 本マネジメント基準の要求事項 b) 情報セキュリティマネジメントが有効に実施され、維持されていること。 ・内部監査は、管理策の有効性を総合的に確認するために定期的に実施し、計画及び結果について以下の文書で管理する。 a) 内部監査基本計画 b) 内部監査実施計画 c) 内部監査報告書 基本計画書では対象範囲、目的、管理体制及び期間又は期日について、実施計画では実施時期や実施場所、実施担当者及びその割当て並びに詳細な監査の手法についてあらかじめ決める。予定通り実施されたことを証明するためにも、実施報告書を作成する。 ・適合性の監査においては、以下の項目を対象に含む。 a) 関連する法令又は規制の要求事項 b) 情報セキュリティリスクアセスメントなどによって特定された情報セキュリティ要求事項 ・情報セキュリティマネジメントが有効に実施され、維持されていることの監査においては、以下の項目を対象に含む。 a) 管理策の有効性及び維持 b) 管理策が期待通りに実施されていること。
4.6.2.3	組織は、頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持する。[27001-9.2c)] 監査プログラムでは、関連するプロセスの重要性及び前回までの監査の結果を考慮する。 監査は一度にすべての適用範囲について実施するだけではなく、範囲の一部のみを対象とする場合もあり、毎回の監査の目的を明確にし、適切な監査計画を実施することが重要であることから、監査プログラムの作成においては、以下の点を考慮する。 ・監査の目的と重点目標 ・対象となる監査プロセスの状況と重要性 ・対象となる領域の状況と重要性 ・前回までの監査結果	4.6.2.3	組織は、頻度、方法、責任及び計画策定に関する要求事項及び報告を含む、監査プログラムを計画、確立、実施及び維持する。[27001-9.2.2] ・ 内部監査プログラムを確立するとき、組織は、関連するプロセスの重要性及び前回までの監査の結果を考慮する。
4.6.2.4	組織は、監査基準及び監査範囲を明確にする。[27001-9.2d)] 監査プログラムでは全体的な監査の日程だけではなく、以下の内容について含める。 ・監査の基準（以下の内容も含む。） －目的、権限と責任 －独立性、客観性と職業倫理 －専門能力 －業務上の義務 －品質管理 －監査の実施方法 －監査報告書の形式 ・監査の範囲 ・監査の頻度又は時期 ・監査の方法（個別の情報セキュリティ監査基準を作成し、内部監査、外部組織による監査のいずれにおいても、品質の高い監査を実施できるように準備を整える。）	4.6.2.4	組織は、監査基準及び監査範囲を明確にする。[27001-9.2.2a)] ・監査プログラムでは全体的な監査の日程だけではなく、以下の内容について含める。 a) 監査の基準（以下の内容も含む。） 1) 目的、権限と責任 2) 独立性、客観性と職業倫理 3) 専門能力 4) 業務上の義務 5) 品質管理 6) 監査の実施方法 7) 監査報告書の形式 b) 監査の範囲 c) 監査の頻度又は時期 d) 監査の方法（個別の情報セキュリティ監査基準を作成し、内部監査、外部組織による監査のいずれにおいても、品質の高い監査を実施できるように準備を整える。）
4.6.2.5	組織は、監査プロセスの客観性及び公平性を確実にする監査員の選定及び監査の実施を行う。[27001-9.2e)] 監査人の選定においては監査基準に従い、以下の点を考慮する。 ・外観上の独立性 ・精神上の独立性 ・職業倫理と誠実性 なお、内部の監査員の場合は、自らが従事している業務については自身で監査しないように、他の担当者を割り当てる。	4.6.2.5	組織は、監査プロセスの客観性及び公平性を確実にする監査員の選定及び監査の実施を行う。[27001-9.2.2b)] ・監査人の選定においては監査基準に従い、以下の点を考慮する。 a) 外観上の独立性 b) 精神上の独立性 c) 職業倫理と誠実性 なお、内部の監査員の場合は、自らが従事している業務については自身で監査しないように、他の担当者を割り当てる。
4.6.2.6	組織は、監査の結果を関連する管理層に報告することを確実にする。[27001-9.2f)]	4.6.2.6	組織は、監査の結果を関連する管理層に報告することを確実にする。[27001-9.2.2c)]
4.6.2.7	組織は、監査プログラム及び監査結果の証拠として、文書化した情報を保持する。[27001-9.2g)] 監査手順に以下の内容を反映させるとともに、文書化し、お互いのコミュニケーションのために活用する。 ・監査の計画・実施に関する責任及び要求事項 ・結果報告・記録維持に関する責任と要求事項 要求事項については監査品質を確保するための必須条件であり、責任者と監査人が同じ目的をもって監査を実施する。	4.6.2.7	組織は、監査プログラムの実施及び監査結果の証拠として、文書化した情報を利用可能な状態にする。[27001-9.2.2] ・監査手順に以下の内容を反映させるとともに、文書化し、互いのコミュニケーションのために活用する。 a) 監査の計画・実施に関する責任及び要求事項 b) 結果報告・記録維持に関する責任及び要求事項 要求事項については監査品質を確保するための必須条件であり、責任者と監査人が同じ目的をもって監査を実施する。

番号	(旧)マネジメント基準	番号	(新) マネジメント基準
4.6.3	マネジメントレビュー [27001-9.3]	4.6.3	マネジメントレビュー [27001-9.3]
4.6.3.1	トップマネジメントは、あらかじめ定めた間隔で、マネジメントレビューする。[27001-9.3] あらかじめ定められた間隔でマネジメントレビューを実施するために、以下の点について考慮するとともに、文書化する。 ・マネジメントレビュー基本計画 ・マネジメントレビュー実施計画 ・マネジメントレビューのための実施報告 基本計画書では目的及び実施時期について、実施計画では詳細な監査の手法についてあらかじめ決める。	4.6.3.1	トップマネジメントは、あらかじめ定めた間隔で、マネジメントレビューする。[27001-9.3] ・あらかじめ定められた間隔でマネジメントレビューを実施するために、以下の点について考慮するとともに、文書化する。 a) マネジメントレビュー基本計画 b) マネジメントレビュー実施計画 c) マネジメントレビューのための実施報告 基本計画書では目的及び実施時期について、実施計画では詳細な監査の手法についてあらかじめ決める。
4.6.3.2	トップマネジメントは、マネジメントレビューにおいて、以下を考慮する。[27001-9.3] ・前回までのマネジメントレビューの結果とった処置の状況 ・情報セキュリティマネジメントに関連する外部及び内部の課題の変化 ・以下に示す内容を含めた、情報セキュリティパフォーマンスに関するフィードバック -不適合及び是正処置 -監視及び測定の結果 -監査結果 -情報セキュリティ目的の達成 ・利害関係者からのフィードバック ・情報セキュリティリスクアセスメントの結果及び情報セキュリティリスク対応計画の状況 ・継続的改善の機会 また、これらの情報を構成することが予想される活動及び事象を記録し、必要に応じて報告するとともに、緊急性が高いものについてはあらかじめ定義しておき、誰もが同じ判断をできるように基準を定める。	4.6.3.2	トップマネジメントは、マネジメントレビューにおいて、以下を考慮する。[27001-9.3.2] ・前回までのマネジメントレビューの結果講じた処置の状況 ・情報セキュリティマネジメントに関連する外部及び内部の課題の変化 ・情報セキュリティマネジメントに関連する利害関係者のニーズ及び期待の変化 ・以下に示す内容を含めた、情報セキュリティパフォーマンスに関するフィードバック a) 不適合及び是正処置 b) 監視及び測定の結果 c) 監査結果 d) 情報セキュリティ目的の達成 ・利害関係者からのフィードバック ・情報セキュリティリスクアセスメントの結果及び情報セキュリティリスク対応計画の状況 ・継続的改善の機会 また、これらの情報を構成することが予想される活動及び事象を記録し、必要に応じて報告するとともに、緊急性が高いものについてはあらかじめ定義しておき、誰もが同じ判断をできるように基準を定める。
4.6.3.3	マネジメントレビューからのアウトプットには、継続的改善の機会及び情報セキュリティマネジメントのあらゆる変更の必要性に関する決定を含める。[27001-9.3] マネジメントレビューの結果を改善策に反映するために、以下の活動を実施し、改善策を検討する。 ・情報セキュリティマネジメントの有効性の改善 ・情報セキュリティリスクアセスメント及び情報セキュリティリスク対応計画の更新 ・情報セキュリティマネジメントに影響を与える可能性のある内外の事象を考慮の上での手順及び管理策の修正 ・必要となる経営資源の特定 ・パフォーマンス測定方法の改善 なお、改善策の立案においては、情報セキュリティリスク対応の選択肢を選択した際の記録を参考にする。	4.6.3.3	マネジメントレビューの結果には、継続的改善の機会及び情報セキュリティマネジメントのあらゆる変更の必要性に関する決定を含める。[27001-9.3.3] ・マネジメントレビューの結果を改善策に反映するために、以下の活動を実施し、改善策を検討する。 a) 情報セキュリティマネジメントの有効性の改善 b) 情報セキュリティリスクアセスメント及び情報セキュリティリスク対応計画の更新 c) 情報セキュリティマネジメントに影響を与える可能性のある内外の事象を考慮の上での手順及び管理策の修正 d) 必要となる経営資源の特定 e) パフォーマンス測定方法の改善 なお、改善策の立案においては、情報セキュリティリスク対応の選択肢を選択した際の記録を参考にする。
4.6.3.4	組織は、マネジメントレビューの結果の証拠として文書化した情報を保持する。[27001-9.3] マネジメントレビューの結果は次回のマネジメントレビューに活用されるため、実施内容と結果が分かるように具体的に記録する。	4.6.3.4	組織は、マネジメントレビューの結果の証拠として文書化した情報を利用可能な状態にする。[27001-9.3] ・マネジメントレビューの結果は次回のマネジメントレビューに活用されるため、実施内容と結果が分かるように具体的に記録する。
4.7	情報セキュリティマネジメントの維持及び改善 [27001-10]	4.7	情報セキュリティマネジメントの維持及び改善 [27001-10]
4.7.1	是正処置 [27001-10.1]	4.7.1	是正処置 [27001-10.2]
4.7.1.1	組織は、不適合が発生した場合、不適合の是正のための処置を取る。[27001-10.1a)] a) 是正措置を取る際は、以下を実施する。 ・その不適合を管理し、是正するための処置 ・その不適合によって起こった結果への対処 ・是正処置を手順どおりに実施するために、以下について文書化する。 – 不適合の再発防止を確実にするために選択した処置の必要性の評価 – 必要な是正処置の決定 – 必要な是正処置の実施 – 実施した処置の記録 – 実施した是正処置のレビュー b) 不適合は以下の活動によって検出される。 ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・定期的なマネジメントレビュー ・不適合を手順どおりに検出するために、以下について文書化する。 – 情報セキュリティマネジメントに対する不適合の特定 – 情報セキュリティマネジメントに対する不適合の原因の決定 なお、単一の活動だけでは判断できない場合もあるので、複合的な結果の考察から不適合を検出する。	4.7.1.1	組織は、不適合が発生した場合、不適合の是正のための処置を取る。[27001-10.2] ・是正処置を取る際は、以下を実施する。 a) その不適合を管理し、是正するための処置 b) その不適合によって起こった結果への対処 c) 是正処置を手順どおりに実施するために、以下について文書化する。 1) 不適合の再発防止を確実にするために選択した処置の必要性の評価 2) 必要な是正処置の決定 3) 必要な是正処置の実施 4) 実施した処置の記録 5) 実施した是正処置のレビュー ・不適合は以下の活動によって検出される。 a) 定期的な情報セキュリティリスクアセスメント b) 定期的な情報セキュリティ内部監査 c) 定期的なマネジメントレビュー d) 不適合を手順どおりに検出するために、以下について文書化する。 1) 情報セキュリティマネジメントに対する不適合の特定 2) 情報セキュリティマネジメントに対する不適合の原因の決定 なお、単一の活動だけでは判断できない場合もあるので、複合的な結果の考察から不適合を検出する。
4.7.1.2	組織は、不適合が再発又は他のところで発生しないようにするため、その不適合の原因を除去するための処置をとる必要性を評価する。[27001-10.1b)] 必要性を評価する際は、以下を実施する。 ・その不適合のレビュー ・その不適合の原因の明確化 ・類似の不適合の有無、又はそれが発生する可能性の明確化	4.7.1.2	組織は、不適合が再発又は他のところで発生しないようにするため、その不適合の原因を除去するための処置を講じる必要性を評価する。[27001-10.2b)] ・必要性を評価する際は、以下を実施する。 a) その不適合のレビュー b) その不適合の原因の明確化 c) 類似の不適合の有無、又はそれが発生する可能性の明確化
4.7.1.3	組織は、必要な処置を実施する。[27001-10.1c)]	4.7.1.3	組織は、必要な処置を実施する。[27001-10.2c)]
4.7.1.4	組織は、とった全ての是正処置の有効性をレビューする。[27001-10.1d)]	4.7.1.4	組織は、講じた全ての是正処置の有効性をレビューする。[27001-10.2d)]
4.7.1.5	組織は、必要な場合には、情報セキュリティマネジメントの変更を行う。[27001-10.1e)]	4.7.1.5	組織は、必要な場合には、情報セキュリティマネジメントの変更を行う。[27001-10.2e)]
4.7.1.6	組織は、是正処置は、検出された不適合のもつ影響に応じたものとする。[27001-10.1]	4.7.1.6	組織は、是正処置は、検出された不適合のもつ影響に応じたものとする。[27001-10.2]
4.7.1.7	組織は、是正処置の証跡として、以下の文書化した情報を保持する。[27001-10.1f) / 10.1g)] ・不適合の性質及びとった処置 ・是正処置の結果	4.7.1.7	組織は、是正処置の証跡として、以下の文書化した情報を利用可能な状態にする。[27001-10.2f) / 10.2g)] ・不適合の性質及びそれに対して講じたあらゆる処置 ・是正処置の結果

番号	(旧)マネジメント基準	番号	(新) マネジメント基準
4.8	文書化した情報の管理 [27001-7.5]	4.8	文書化した情報の管理 [27001-7.5]
4.8.1	文書化の指針 [27001-7.5.1]	4.8.1	文書化の指針 [27001-7.5.1]
4.8.1.1	組織は、情報セキュリティマネジメントが必要とする以下の情報を文書化する。[27001-7.5.1] ・情報セキュリティ方針 ・情報セキュリティ目的 ・情報セキュリティリスクアセスメントのプロセス ・情報セキュリティリスク対応のプロセス ・情報セキュリティリスクアセスメントの結果 ・情報セキュリティリスク対応計画 ・パフォーマンス測定の結果 これらの内容についてはどの文書に記載されていてもかまわないが、その内容を知る必要がある担当者には必ず伝わるように構成するとともに、知る必要性のない者が閲覧できないことを確実にする。	4.8.1.1	組織は、情報セキュリティマネジメントが必要とする以下の情報を文書化する。[27001-7.5.1] ・情報セキュリティ方針 ・情報セキュリティ目的 ・情報セキュリティリスクアセスメントのプロセス ・情報セキュリティリスク対応のプロセス ・情報セキュリティリスクアセスメントの結果 ・情報セキュリティリスク対応計画 ・パフォーマンス測定の結果 これらの内容についてはどの文書に記載されていてもかまわないが、その内容を知る必要がある担当者には必ず伝わるように構成するとともに、知る必要性のない者が閲覧できないことを確実にする。
4.8.2	文書の作成・変更及び管理 [27001-7.5.2 / 7.5.3]	4.8.2	文書の作成・変更及び管理 [27001-7.5.2 / 7.5.3]
4.8.2.1	組織は、以下を行うことによって、文書化した情報を作成及び更新する。[27001-7.5.2] ・適切な識別情報の記述（例えば、表題、日付、作成者、参照番号） ・適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）の選択 ・適切性及び妥当性に関する、適切なレビュー及び承認 ・文書化した情報のライフサイクルの定義や、それに応じた処理ができるような手順の策定 ・文書を発行する前における、適正性のレビュー及び承認 ・必要に応じた、文書の更新及び再承認 ・廃止文書の誤使用の防止 ・廃止文書を何らかの目的で保持する場合における、廃止文書であることが分かる適切な識別情報の記述 ・法的及び規制の要求事項及び環境の変化に従い、定めた頻度での更新 また、これらのすべての活動が文書管理に反映されているか、またその活動が業務に大きな障害を与えていないかなどを考慮し、適切な文書管理手順を策定する。	4.8.2.1	組織は、以下を行うことによって、文書化した情報を作成及び更新する。[27001-7.5.2] ・適切な識別情報の記述（例えば、表題、日付、作成者、参照番号） ・適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）の選択 ・適切性及び妥当性に関する、適切なレビュー及び承認 ・文書化した情報のライフサイクルの定義や、それに応じた処理ができるような手順の策定 ・文書を発行する前における、適正性のレビュー及び承認 ・必要に応じた、文書の更新及び再承認 ・廃止文書の誤使用の防止 ・廃止文書を何らかの目的で保持する場合における、廃止文書であることが分かる適切な識別情報の記述 ・法的及び規制の要求事項及び環境の変化に従い、定めた頻度での更新 また、これらのすべての活動が文書管理に反映されているか、またその活動が業務に大きな障害を与えていないかなどを考慮し、適切な文書管理手順を策定する。
4.8.2.2	組織は、以下のことを確実にするために、情報セキュリティマネジメントで要求された文書化した情報を、管理する。[27001-7.5.3] ・文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態であること。 ・文書化した情報が十分に保護されていること（例えば、機密性の喪失、不適切な使用及び完全性の喪失からの保護）。 ・文書化した情報の配付、アクセス 、検索及び利用 ・文書化した情報の読みやすさが保たれることを含む、保管及び保存 ・文書化した情報の変更の管理（例えば、版の管理） ・文書化した情報の保持及び廃棄 また、情報セキュリティマネジメントの計画及び運用のために組織が必要と決定した文書は、外部から入手したものであっても、必要に応じて、特定し、管理する。	4.8.2.2	組織は、以下のことを確実にするために、情報セキュリティマネジメントで要求された、文書化した情報を管理する。[27001-7.5.3] ・文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態であること。 ・文書化した情報が十分に保護されていること（例えば、機密性の喪失、不適切な使用又は完全性の喪失からの保護）。 ・文書化した情報の配付、アクセス、検索及び利用 ・文書化した情報の読みやすさが保たれることを含む、保管及び保存 ・文書化した情報の変更の管理（例えば、版の管理） ・文書化した情報の保持及び廃棄 また、情報セキュリティマネジメントの計画策定及び運用のために組織が必要と決定した文書は、外部から入手したものであっても、必要に応じて、識別し、管理する。
4.9	情報セキュリティリスクコミュニケーション	4.9	情報セキュリティリスクコミュニケーション 利害関係者間の有効なコミュニケーションは、意思決定に大きな影響を与えることがある。情報セキュリティリスクコミュニケーションは、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間で情報セキュリティリスクに関する情報を交換、共有し、リスクを管理する方法に関する合意を得る。
–	利害関係者間の有効なコミュニケーションは、意思決定に大きな影響を与えることがある。情報セキュリティリスクコミュニケーションは、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間で情報セキュリティリスクに関する情報を交換、共有し、リスクを管理する方法に関する合意を得る。		
4.9.1	リスクコミュニケーションの計画	4.9.1	リスクコミュニケーションの計画
4.9.1.1	リスクコミュニケーション計画を策定する。 リスクコミュニケーション計画は、以下の２つに分けて策定し、文書化する。 ・通常運用のためのリスクコミュニケーション計画 ・緊急事態のためのリスクコミュニケーション計画 リスクコミュニケーション計画は、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間でどのようにコミュニケーションを図るかに留意し、以下の内容について含める。 ・適切な利害関係者の参画による、効果的な情報交換／共有 ・法令、規制及びガバナンスの要求事項の順守 ・コミュニケーション及び協議に関するフィードバック及び報告の提供 ・組織に対する信頼を醸成するためのコミュニケーションの活用 ・危機又は不測の事態発生時の利害関係者とのコミュニケーションの実施	4.9.1.1	リスクコミュニケーション計画を策定する。 ・リスクコミュニケーション計画は、以下の２つに分けて策定し、文書化する。 a) 通常運用のためのリスクコミュニケーション計画 b) 緊急事態のためのリスクコミュニケーション計画 リスクコミュニケーション計画は、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間でどのようにコミュニケーションを図るかに留意し、以下の内容について含める。 1) 適切な利害関係者の参画による、効果的な情報交換／共有 2) 法令、規制及びガバナンスの要求事項の順守 3) コミュニケーション及び協議に関するフィードバック及び報告の提供 4) 組織に対する信頼を醸成するためのコミュニケーションの活用 5) 危機又は不測の事態発生時の利害関係者とのコミュニケーションの実施
4.9.2	リスクコミュニケーションの実施	4.9.2	リスクコミュニケーションの実施
4.9.2.1	リスクコミュニケーションを実施する仕組みを確定する。 リスクに関する論議、その優先順位の決定及び適切なリスク対応、並びにリスク受容を行い、主要な意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の協調を得る仕組みを確定する。この仕組みでは次の事項を確実にする。 ・リスクマネジメントの枠組みの主要な構成要素、及びその後に行うあらゆる修正の適切な伝達 ・枠組み、その有効性及び成果に関する適切な内部報告 ・適切な階層及び時期に利用可能な、リスクマネジメントの適応から導出される関連情報の提供 ・内部の利害関係者との協議のためのプロセス 仕組みには、適切な場合には、多様な情報源からのリスク情報について、まとめ上げるプロセスが含まれ、また、リスク情報の影響の受けやすさを考慮する必要がある場合もある。なお、この仕組みを設ける場として、委員会がある。	4.9.2.1	リスクコミュニケーションを実施する仕組みを確定する。 ・リスクに関する論議、その優先順位の決定及び適切なリスク対応、並びにリスク受容を行い、主要な意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の協調を得る仕組みを確定する。この仕組みでは次の事項を確実にする。 a) リスクマネジメントの枠組みの主要な構成要素、及びその後に行うあらゆる修正の適切な伝達 b) 枠組み、その有効性及び成果に関する適切な内部報告 c) 適切な階層及び時期に利用可能な、リスクマネジメントの適応から導出される関連情報の提供 d) 内部の利害関係者との協議のためのプロセス 仕組みには、適切な場合には、多様な情報源からのリスク情報について、まとめ上げるプロセスが含まれ、また、リスク情報の影響の受けやすさを考慮する必要がある場合もある。なお、この仕組みを設ける場として、委員会がある。
4.9.2.2	リスクコミュニケーションを実施する。 リスクコミュニケーションは、次の点を達成するために、リスクマネジメントプロセスのすべての段階で継続的に実施する。 ・組織のリスクマネジメント結果の保証を提供する ・リスク情報を収集する ・リスクアセスメントの結果を共有しリスク対応計画を提示する ・意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の相互理解の欠如による情報セキュリティ違反の発生及び結果を回避又は低減する ・意思決定を支援する ・新しい情報セキュリティ知識を入手する ・他の組織と協調しすべてのインシデントの結果を低減するための対応計画を立案する ・意思決定者及び利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）にリスクについての責任を意識させる ・セキュリティ意識を改善する リスクコミュニケーションの実施においては、組織内の適切な広報又はコミュニケーション部門と協力し、リスクコミュニケーション関連の全タスクを調整して行う。	4.9.2.2	リスクコミュニケーションを実施する。 ・リスクコミュニケーションは、次の点を達成するために、リスクマネジメントプロセスのすべての段階で継続的に実施する。 a) 組織のリスクマネジメント結果の保証を提供する b) リスク情報を収集する c) リスクアセスメントの結果を共有しリスク対応計画を提示する d) 意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の相互理解の欠如による情報セキュリティ違反の発生及び結果を回避又は低減する e) 意思決定を支援する f) 新しい情報セキュリティ知識を入手する g) 他の組織と協調しすべてのインシデントの結果を低減するための対応計画を立案する h) 意思決定者及び利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）にリスクについての責任を意識させる i) セキュリティ意識を改善する リスクコミュニケーションの実施においては、組織内の適切な広報又はコミュニケーション部門と協力し、リスクコミュニケーション関連の全タスクを調整して行う。

番号	(旧)ガバナンス基準	番号	(新)ガバナンス基準
–	（JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策）	–	–
–	（JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策）	–	–
–	（JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策）	–	–
–	（対応項なし）	–	–
–	（JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策）	–	–
–	（JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策）	3.3.1 概要 情報セキュリティガバナンスは、評価、指示、モニタ及びコミュニケーションの各プロセスで構成される。次項以降において、各プロセスにおいて、ガバナンス主体及び各情報セキュリティマネジメントシステムの責任者が実行する内容を示す。	
–	（JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策）	–	–
–	（JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策）	3.3.2 評価	
–	（JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策）	–	（対応項なし）
–	（JIS Q 27014:2015 (ISO/IEC 27014:2013)を参照して作成した管理策）		
3.1.2.1	経営陣は、事業の取組みにおいて情報セキュリティ問題を考慮することを確実にする。 ・経営陣は、管理者に、情報セキュリティが事業目的を十分にサポートし、支えることを確実にさせる。	3.3.2.1	ガバナンス主体は、以下を実行する。 ・事業に取り組む際の関連するリスク及び機会の確実な考慮 ・情報セキュリティに関する報告に対応するための、情報セキュリティマネジメントシステムにおける目的と優先度の規定
3.1.2.2	経営陣は、情報セキュリティのパフォーマンス結果に対応し、必要な処置の優先順位を決めて開始する。		
3.1.2.3	経営陣は、管理者に、重大な影響のある新規情報セキュリティプロジェクトを経営陣に付託するようにさせる。		
–	（対応項なし）	3.3.2.2	各情報セキュリティマネジメントシステムの責任者は、以下を実行する。 ・組織体の目的を適切に支援し、維持するような情報セキュリティの確立 ・重大な影響を伴う新規の情報セキュリティプロジェクトを実施する際の、組織体のガバナンス主体への承認依頼
3.1.3 指示		3.3.3 指示	
–	指示は、経営陣が、実施する必要がある情報セキュリティの目的及び戦略についての指示を与えるガバナンスプロセスである。指示には、資源供給レベルの変更、資源の配分、活動の優先順位付け並びに、方針、適切なリスク受容及びリスクマネジメント計画の承認が含まれる。	–	（対応項なし）
	“指示”プロセスを実施するために、経営陣は次のことを行う。		
3.1.3.1	経営陣は、その組織のリスク選好を決定する。	3.3.3.1	ガバナンス主体は、以下を実行する。 ・組織体全体の戦略の方向性と目的の設定 ・その組織体のリスク選好の決定 ・情報セキュリティ戦略の承認
3.1.3.2	経営陣は、情報セキュリティの戦略及び方針を承認する。 (ア)経営陣は、管理者に、情報セキュリティの戦略及び方針を策定・実施させる。 (イ)経営陣は、管理者に、情報セキュリティの目的を事業目的に合わせて調整させる。		
3.1.3.3	経営陣は、適切な投資及び資源を配分する。		
3.1.3.4	経営陣は、管理者に、情報セキュリティに積極的な文化を推進させる。		
–	（対応項なし）	3.3.3.2	各情報セキュリティマネジメントシステムの責任者は、以下を実行する。 ・適切な投資及び資源の配分の実施 ・組織体の目的に合致するように情報セキュリティの目的を調整 ・情報セキュリティに関する役割と責任の割当 ・情報セキュリティポリシーの規定
3.1.4 モニタ		3.3.4 モニタ	
	モニタは、経営陣が戦略的目的の達成を評価することを可能にするガバナンスプロセスである。	–	（対応項なし）
	“モニタ”プロセスを実施するために、経営陣は次のことを行う。		
3.1.4.1	経営陣は、情報セキュリティマネジメント活動の有効性を評価する。 (ア)経営陣は、管理者に、事業の観点から適切なパフォーマンス指標を選択させる。 (イ)経営陣は、管理者に、経営陣が以前に特定した措置の実施及びそれらの組織への影響を含む、情報セキュリティのパフォーマンス成果についてのフィードバックを経営陣へ提供させる。	3.3.4.1	ガバナンス主体は、以下を実行する。 ・各情報セキュリティマネジメントシステムの活動の有効性に関する報告の受領 ・組織体の優先度の文脈での、前項で報告された内容の評価 ・各情報セキュリティマネジメントシステムの責任者への優先度の伝達
3.1.4.2	経営陣は、内部及び外部の要求事項への適合性を確実にする。		
3.1.4.3	経営陣は、変化する事業、法制度、規制の環境、及びそれらの情報リスクへの潜在的影響を考慮する。		
3.1.4.4	経営陣は、管理者に、情報リスク及び情報セキュリティに影響する新規開発案件について、経営陣に対し注意を喚起させる。		
–	（対応項なし）	3.3.4.2	各情報セキュリティマネジメントシステムの責任者は、以下を実行する。 ・情報セキュリティマネジメントシステム活動の有効性の評価 ・内部及び外部の要求事項への確実な適合の確保 ・組織体に関わる変化、法令及び規制の環境、並びに情報リスクへの潜在的影響の考慮 ・適切なパフォーマンス指標を選定し、組織的な観点から適切なタイミングで報告が実施されるよう要求を伝達 ・情報セキュリティの実績に関する結果のフィードバックを組織体の経営陣に提供 ・情報リスク及び情報セキュリティに影響する新規の開発についての、組織体の経営陣への注意喚起

番号	(旧)ガバナンス基準	番号	(新)ガバナンス基準
3.1.5　コミュニケーション		3.3.5 コミュニケーション	
	コミュニケーションは、経営陣及び利害関係者が、双方の特定のニーズに沿った情報セキュリティに関する情報を交換する双方向のガバナンスプロセスである。	–	（対応項なし）
	コミュニケーションの方法の一つは、情報セキュリティの活動及び課題を利害関係者に説明する情報セキュリティ報告書である。		
	“コミュニケーション”プロセスを実施するために、経営陣は次のことを行う。		
3.1.5.1	経営陣は、外部の利害関係者に、組織がその事業特性に見合った情報セキュリティのレベルを実践していることを報告する。	3.3.5.1	ガバナンス主体は、以下を実行する。 ・外部の利害関係者を対象とする、組織体がその活動及び優先度の実態に見合った情報セキュリティのレベルを実践していることの報告 ・規制上の義務、利害関係者の期待及び情報セキュリティに関する組織体の要求事項の特定及び優先度の決定 ・注意及び決定が必要な問題についての、各情報セキュリティマネジメントシステムの責任者への助言 ・関連する利害関係者に向けた、情報セキュリティの優先度決定を支援するために採用すべき詳細な対象に関する指導 ・情報セキュリティに積極的な文化の奨励 ・スタッフ及びその他の人々を対象とする、情報セキュリティマネジメントシステムの適用範囲での責任を果たすための訓練とコミュニケーション
3.1.5.2	経営陣は、管理者に、情報セキュリティ課題を特定した外部レビューの結果を通知し、是正処置を要請する。		
3.1.5.3	経営陣は、情報セキュリティに関する規制上の義務、利害関係者の期待及び事業ニーズを認識する。		
3.1.5.4	経営陣は、管理者に、注意が必要な問題、また、できれば決定が必要な問題について、経営陣へ助言させる。		
3.1.5.5	経営陣は、管理者に、関連する利害関係者に対し、経営陣の方向性及び決定を支援するためにとるべき詳細な行動を、経営陣の方向性及び決定に沿って説明させる。		
3.1.6 保証		–	（対応項なし）
–	保証は、経営陣が独立した客観的な監査、レビュー又は認証を委託するガバナンスプロセスである。これは、望ましいレベルの情報セキュリティを達成するためのガバナンス活動の実行及び運営の遂行に関連した目的及び処置を特定し、妥当性を検証する。		
–	“保証”プロセスを実施するために、経営陣は次のことを行う。		
3.1.6.1	経営陣は、要求している情報セキュリティ水準に対し、どのように説明責任を果たしているかについて、独立した客観的な意見を監査人等に求める。		
3.1.6.2	経営陣は、管理者に、経営陣が委託する監査、レビュー又は認証をサポートさせる。		

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
5	情報セキュリティのための方針群	5	組織的管理策	–	–	–	–
5.1	情報セキュリティのための経営陣の方向性 管理目的：情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制に従って提示するため。	5.1	情報セキュリティのための方針群 管理策 情報セキュリティ方針及びトピック固有の方針は、これを定義し、管理層が承認し、発行し、関連する要員及び関連する利害関係者に伝達し、認識させ、あらかじめ定めた間隔で、及び重大な変化が発生した場合にレビューする。 目的 事業、法令、規制及び契約上の要求事項に従って、情報セキュリティに対する管理層の指示及び支援の継続的な適合性、適切性、及び有効性を確実にするため。	–	5.1	情報セキュリティのための方針群 統制目標：情報セキュリティ方針及びトピック固有の方針は、これを定義し、管理層が承認し、発行し、関連する要員及び関連する利害関係者に伝達し、認識させ、あらかじめ定めた間隔で、及び重大な変化が発生した場合にレビューする。 目的：事業、法令、規制及び契約上の要求事項に従って、情報セキュリティに対する管理層の指示及び支援の継続的な適合性、適切性、及び有効性を確実にするため。	
5.1.1	情報セキュリティのための方針群のレビュー 情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知する。 (脚注) 管理層には、経営陣及び管理者が含まれる。ただし、実務管理者（administrator）は除かれる。						
5.1.1.1	組織は、経営陣によって承認され、組織の情報セキュリティ目的の管理に対する取組みを示すものとして、方針群の最も高いレベルに、一つの情報セキュリティ方針を定める。	5a-5.1.1	組織は、方針群の最も高いレベルに、一つの"情報セキュリティ方針"を定める。	手引に関連記載あり	5.1.1	情報セキュリティ方針を策定し、トップマネジメントが承認する。	組織は、方針群の最も高いレベルに、一つの情報セキュリティ方針を定める。この情報セキュリティ方針は、トップマネジメントが承認し、情報セキュリティの管理に対する組織の取組を示すものである。 情報セキュリティ方針は、次のものから得largeされる要求事項を考慮に入れる。 a) 事業上の戦略及び要求事項 b) 規制、法令及び契約 c) 現在の及び予想される情報セキュリティのリスク及び脅威 情報セキュリティ方針には、次の事項に関する記載を含める。 a) 情報セキュリティの定義 b) 情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組み c) 情報セキュリティに関する全ての活動の指針となる原則 d) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメント e) 情報セキュリティマネジメントシステムの継続的な改善へのコミットメント f) 情報セキュリティマネジメントに関する責任の、定められた役割への割当て g) 逸脱及び例外を取り扱う手順 方針群のより低いレベルでは、情報セキュリティ方針は、情報セキュリティ管理策の実施を率に責務が付されるために、必要に応じてトピック固有の方針によって支持する。トピック固有の方針は、一般に、組織内で対象とする特定のグループのニーズに対応するように、又は特定のセキュリティ領域を対象とするように構成される。 トピック固有の方針は、組織の情報セキュリティ方針に沿い、それを補完する。このようなトピックの例を次に示す。 a) アクセス制御 b) 物理的及び環境的セキュリティ c) 資産管理 d) 情報の転送 e) 利用者エンドポイント機器のセキュリティを保つた構成及び取扱い f) ネットワークセキュリティ g) 情報セキュリティインシデント管理 h) バックアップ i) 暗号及び鍵管理 j) 情報の分類及び取扱い k) 技術的ぜい弱性の管理 l) セキュリティに配慮した開発 トピック固有の方針の作成、レビュー及び承認に関する責任は、関連する要員に、権限及び技術的力量のレベルに基づいて割り当てる。 レビューには、次のための変化に応じた、組織の情報セキュリティ方針及びトピック固有の方針並びに情報セキュリティの管理に関する、改善の機会の評価を含める。 a) 組織の事業戦略 b) 組織の技術環境 c) 規制、法令及び契約 d) 情報セキュリティリスク e) 現在の及び予想される情報セキュリティの脅威の環境 f) 情報セキュリティ事象及びインシデントから学んだ教訓 情報セキュリティ方針及びトピック固有の方針のレビューでは、マネジメントレビュー及び監査の結果を考慮する。 一貫性を維持するため、一つの方針を変更する場合は、他の関連する方針のレビュー及び更新を検討する。
–	（対応項なし）	5a-5.1.3	情報セキュリティ方針には、次の事項に関する記載を含める。 a) 情報セキュリティの定義 b) 情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組み c) 情報セキュリティに関する全ての活動の指針となる原則	手引に関連記載あり			
–	（対応項なし）	5a-5.1.3	情報セキュリティ方針には、次の事項に関する記載を含める。 d) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメント e) 情報セキュリティマネジメントシステムの継続的な改善へのコミットメント	手引に関連記載あり			
5.1.1.6	情報セキュリティ方針には、情報セキュリティマネジメントに関する一般的な責任及び特定の責任の、定められた役割への割当てに関する記載を含める。	5a-5.1.3	情報セキュリティ方針には、次の事項に関する記載を含める。 f) 情報セキュリティマネジメントに関する責任の、定められた役割への割当て	手引に関連記載あり			
5.1.1.7	情報セキュリティ方針には、逸脱及び例外を取り扱う方法に関する記載を含める。	5a-5.1.3	情報セキュリティ方針には、次の事項に関する記載を含める。 g) 逸脱及び例外を取り扱う手順	手引に関連記載あり			
5.1.1.8	方針群のより低いレベルでは、情報セキュリティ方針は、トピックに応じて定める個別方針によって支持されるようにする。	5a-5.1.5	方針群のより低いレベルでは、情報セキュリティ方針は、情報セキュリティ管理策の実施を率に責務が付されるために、必要に応じてトピック固有の方針によって支持する。	手引に関連記載あり			
–	（対応項なし）	5a-5.1.5参考	トピック固有の方針は、一般に、組織内で対象とする特定のグループのニーズに対応するように、又は特定のセキュリティ領域を対象とするように構成される。	手引に関連記載あり			
–	（対応項なし）	5a-5.1.6	トピック固有の方針は、組織の情報セキュリティ方針に沿い、それを補完する。	手引に関連記載あり			
5.1.1.9	個別方針のトピックとして、アクセス制御を含める。	(5a-5.1.6参考)	このようなトピックの例を、次に示す。 a) アクセス制御	手引に関連記載あり			
5.1.1.10	個別方針のトピックとして、情報分類（及び取扱い）を含める。	(5a-5.1.6参考)	このようなトピックの例を、次に示す。 j) 情報の分類及び取扱い	手引に関連記載あり			
5.1.1.11	個別方針のトピックとして、物理的及び環境的セキュリティを含める。	(5a-5.1.6参考)	このようなトピックの例を、次に示す。 b) 物理的及び環境的セキュリティ	手引に関連記載あり			
5.1.1.12	個別方針のトピックとして、エンドユーザ関連のトピック（資産利用の許容範囲、クリアデスク・クリアスクリーン、情報転送、モバイル機器及びテレワーキング、ソフトウェアのインストール及び使用の制限）を含める。	(5a-5.1.6参考)	このようなトピックの例を、次に示す。 e) 利用者エンドポイント機器のセキュリティを保つた構成及び取扱い	手引に関連記載あり			
5.1.1.13	個別方針のトピックとして、バックアップを含める。	(5a-5.1.6参考)	このようなトピックの例を、次に示す。 h) バックアップ	手引に関連記載あり			
5.1.1.14	個別方針のトピックとして、情報の転送を含める。	(5a-5.1.6参考)	このようなトピックの例を、次に示す。 d) 情報の転送	手引に関連記載あり			
5.1.1.15	個別方針のトピックとして、マルウェアからの保護を含める。	–	（直接対応する詳細管理策無し）	特種な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
5.1.1.16	個別方針のトピックとして、技術的ぜい弱性の管理を含める。	(5a-5.1.6参考)	このようなトピックの例を、次に示す。 k) 技術的ぜい弱性の管理	手引に関連記載あり	5.1.1	【再】情報セキュリティ方針を策定し、トップマネジメントが承認する。	（5.1.1に対応する項を参照）
5.1.1.17	個別方針のトピックとして、暗号による管理策を含める。	(5a-5.1.6参考)	このようなトピックの例を、次に示す。 i) 暗号及び鍵管理	手引に関連記載あり			
5.1.1.18	個別方針のトピックとして、通信のセキュリティを含める。	(5a-5.1.6参考)	このようなトピックの例を、次に示す。 f) ネットワークセキュリティ	手引に関連記載あり			
–	（対応項なし）	(5a-5.1.6参考)	このようなトピックの例を、次に示す。 c) 資産管理 g) 情報セキュリティインシデント管理 l) セキュリティに配慮した開発	手引に関連記載あり			
5.1.1.19	個別方針のトピックとして、プライバシー及び個人を特定できる情報（以下"PII"という。）の保護を含める。	–	（直接対応する詳細管理策無し）	特種な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
5.1.1.20	個別方針のトピックとして、供給者関係を含める。	–	（直接対応する詳細管理策無し）	特種な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
5.1.1.21	トピック別の個別方針は、従業員及び関係する外部関係者によって適切で、アクセス可能かつ理解可能な形式で伝達する（例えば、情報セキュリティの意識向上、教育及び訓練のプログラムに従う。）。	5a-5.1.11	情報セキュリティ方針及びトピック固有の方針は、意図する読者によって適切で、アクセスでき、かつ、理解しやすい形で、関連する要員及び利害関係者に伝達する。	手引に関連記載あり	5.1.3	情報セキュリティ方針を、関連する要員及び利害関係者に伝達する。	情報セキュリティ方針は、関連する要員及び利害関係者にアクセスでき、かつ、理解しやすい形で、伝達する。 必要な場合には、方針の意味に、方針を理解したこと及びその順守に同意することの確認を求める。組織は、これらの方針文書について、組織のニーズを満たす形式及び名称を決定することが可能である。組織によって、情報セキュリティ方針及びトピック固有の方針を単一の文書にすることがある。組織は、トピック固有の方針に、標準、指令、方針、その他の名称を付けることがある。 情報セキュリティ方針を組織外に配布する場合には、秘密情報を不適切に開示しないように注意する。
–	（対応項なし）	5a-5.1.12	必要な場合には、方針の受領者に、方針を理解したこと及びその順守に同意することの確認を求める。	手引に関連記載あり			
–	（対応項なし）	(5a-5.1参考1)	組織は、これらの方針文書について、組織のニーズを満たす形式及び名称を決定することが可能である。	手引に関連記載あり			
–	（対応項なし）	(5a-5.1参考2)	組織によって、情報セキュリティ方針及びトピック固有の方針を単一の文書にすることがある。	手引に関連記載あり			
–	（対応項なし）	(5a-5.1参考3)	組織は、トピック固有の方針に、標準、指令、方針、その他の名称を付けることがある。	手引に関連記載あり			
–	（対応項なし）	5a-5.1.13	情報セキュリティ方針又はトピック固有の方針を組織外に配布する場合には、秘密情報を不適切に開示しないように注意する。	手引に関連記載あり			
5.1.1.22.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	5.1.4	クラウドサービスの提供及び利用に当たった、情報セキュリティ方針を策定する。	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
5.1.1.23.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）			
5.1.1.24.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）			
5.1.1.25.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）			
5.1.1.26.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）			
5.1.1.27.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）			
5.1.1.28.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）			
5.1.1.29.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）			
5.1.1.30.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）			
5.1.1.31.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）			
5.1.2	情報セキュリティのための方針群のレビュー 情報セキュリティのための方針群は、あらかじめ定めた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューする。	5.1	情報セキュリティのための方針群 管理策 情報セキュリティ方針及びトピック固有の方針は、これを定義し、管理層が承認し、発行し、関連する要員及び関連する利害関係者に伝達し、認識させ、あらかじめ定めた間隔で、及び重大な変化が発生した場合にレビューする。 目的 事業、法令、規制及び契約上の要求事項に従って、情報セキュリティに対する管理層の指示及び支援の継続的な適合性、適切性、及び有効性を確実にするため。		5.1	情報セキュリティのための方針群 統制目標：情報セキュリティ方針及びトピック固有の方針は、これを定義し、管理層が承認し、発行し、関連する要員及び関連する利害関係者に伝達し、認識させ、あらかじめ定めた間隔で、及び重大な変化が発生した場合にレビューする。 目的：事業、法令、規制及び契約上の要求事項に従って、情報セキュリティに対する管理層の指示及び支援の継続的な適合性、適切性、及び有効性を確実にするため。	
5.1.2.1	各々の情報セキュリティのための方針には、その方針の作成、レビュー及び評価についての管理責任を与えられた責任者を置く。	5a-5.1.7	トピック固有の方針の作成、レビュー及び承認に関する責任は、関連する要員に、権限及び技術的力量のレベルに基づいて割り当てる。	手引に関連記載あり	5.1.1	【再】情報セキュリティ方針を策定し、トップマネジメントが承認する。	（5.1.1に対応する項を参照）
5.1.2.2	情報セキュリティのための方針群のレビューには、組織環境、業務環境、法的状況又は技術環境の変化に応じた、組織の情報セキュリティのための方針群及び情報セキュリティの管理への取組みに関する、改善の機会の評価を含める。	5a-5.1.8	レビューには、次のための変化に応じた、組織の情報セキュリティ方針及びトピック固有の方針並びに情報セキュリティの管理に関する、改善の機会の評価を含める。 a) 組織の事業戦略 b) 組織の技術環境 c) 規制、法令及び契約 d) 情報セキュリティリスク e) 現在の及び予想される情報セキュリティの脅威の環境 f) 情報セキュリティ事象及びインシデントから学んだ教訓	手引に関連記載あり			
5.1.2.3	情報セキュリティのための方針群のレビューでは、マネジメントレビューの結果を考慮し、反映する。	5a-5.1.9	情報セキュリティ方針及びトピック固有の方針のレビューでは、マネジメントレビュー及び監査の結果を考慮する。	手引に関連記載あり			
–	（対応項なし）	5a-5.1.10	一貫性を維持するため、一つの方針を変更する場合は、他の関連する方針のレビュー及び更新を検討する。	手引に関連記載あり			
5.1.2.4	改訂された情報セキュリティのための方針は、管理層から承認を得る。	5a-5.1.4	情報セキュリティ方針のいかなる変更もトップマネジメントが承認する。	手引に関連記載あり	5.1.2	トップマネジメントは、情報セキュリティ方針をあらかじめ定めた間隔及び重大な変化が発生した場合に承認する。	情報セキュリティ方針のいかなる変更もトップマネジメントが承認する。

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
6.1 6.1.1	内部組織 管理目的：組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。 情報セキュリティの役割及び責任 全ての情報セキュリティの責任を定め、割り当てる。	5.2	情報セキュリティの役割及び責任 管理策 情報セキュリティの役割及び責任は、組織の ニーズに従って定め、割り当てる。 目的 組織内における情報セキュリティの実施、運用及び管理のために、定義され、承認され、理解される構造を確立するため。		5.2	情報セキュリティの役割及び責任 統制目標：情報セキュリティの役割及び責任は、組織のニーズに従って定め、割り当てる。 目的：組織内における情報セキュリティの実施、運用及び管理のために、定義され、承認され、理解されるための構造を確立するため。	
6.1.1.1	情報セキュリティの責任の割当ては、情報セキュリティのための方針に よって行う。	Sa-5.2.1	情報セキュリティの役割及び責任の割当ては、情報セキュリティ方針及び トピック固有の方針に従って行う。	干渉に関連記載あり	5.2.1	情報セキュリティ方針に従い、情報セキュリティの役割及び責任を定義し、割り当てる。	情報セキュリティの役割及び責任の割当ては、情報セキュリティ方針及びトピック固有の方針（5.1参照）に従って行う。 組織は、次の事項に関する責任を定義し、管理する。 a) 情報及びその他の関連資産の保護 b) 情報セキュリティプロセスの実施 c) 情報セキュリティのリスクマネジメント活動、特に残留リスクの受容（例えば、リスク所有者） d) 組織の情報及びその他の関連資産を使用するときの要員
6.1.1.2	個々の資産の保護に対する責任及び特定の情報セキュリティプロセスの実施に対する責任を定める。	Sa-5.2.2	組織は、次の事項に関する責任を定義し、管理する。 a) 情報及びその他の関連資産の保護 b) 特定の情報セキュリティプロセスの実施	干渉に関連記載あり			
6.1.1.3	情報セキュリティのリスクマネジメント活動に関する責任、特に残留リスクの受容に関する責任を定める。	Sa-5.2.2	組織は、次の事項に関する責任を定義し、管理する。 c) 情報セキュリティのリスクマネジメント活動、特に残留リスクの受容	干渉に関連記載あり			
–	（対応項なし）	Sa-5.2.2	組織は、次の事項に関する責任を定義し、管理する。 d) 組織の情報及びその他の関連資産を使用するときの要員	干渉に関連記載あり			
6.1.1.4	必要な場合には、この責任を、個別のサイト及び情報処理施設に対する、より詳細な手引で補完する。	Sa-5.2.3	必要な場合には、この責任を、個別のサイト及び情報処理施設に対する、より詳細な手引で補完する。	明確な対応関係なし	–	（対応項なし）	–
6.1.1.5	資産の保護及び特定の情報セキュリティプロセスの実行に関する局所的(local)な責任を定める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されて）	–	（対応項なし）	–
6.1.1.6	情報セキュリティの責任を割り当てられた個人は、情報セキュリティに関する職務を他者に委任してもよいが、責任は依然としてその個人にあり、委任した職務が しくれた正しく実施されていることを、その個人が確認する。	Sa-5.2.4	情報セキュリティの責任を割り当てられた個人は、情報セキュリティに関する職務を他者に委任してもよいが、アカウンタビリティは依然としてその個人にあり、委任した職務がしくれた正しく実施されていることを、その個人が確認する。	明確な対応関係なし	–	（対応項なし）	–
6.1.1.7	個人が責任をもつ領域を規定する。	Sa-5.2.5	個人が責任をもつ各セキュリティ領域を定義し、文書化し、伝達する。	干渉に関連記載あり	5.2.2	個人が責任をもつ各セキュリティ領域及び承認のレベルを定義し、情報セキュリティの役割をもつ個人に対してそれらを伝達する。	個人が責任をもつ各セキュリティ領域を定義し、文書化し、伝達する。 承認のレベルを定義し、文書化する。 特定の情報セキュリティの役割をもつ個人は、その役割に必要な知識及び技能においてカ量をもつ。 その役割に関連し、その役割の責任を果たす上での必要な最新の動向に追随し続けるように支援される。
6.1.1.8	個人が責任をもつ領域を規定するために、資産及び情報セキュリティプロセスの識別及び規定を実施する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されて）	–	（対応項なし）	–
6.1.1.9	個人が責任をもつ領域を規定するために、各資産又は情報セキュリティプロセスに対する責任主体の指定、及びその責任の詳細の文書化を実施する。	Sa-5.2.5	【再】個人が責任をもつ各セキュリティ領域を定義し、文書化し、伝達する。	干渉に関連記載あり	5.2.2	【再】個人が責任をもつ各セキュリティ領域及び承認のレベルを定義し、情報セキュリティの役割をもつ個人に対してそれらを伝達する。	（5.2.2に対応する項を参照）
6.1.1.10	個人が責任をもつ領域を規定するために、承認レベルの規定及び文書化を実施する。	Sa-5.2.6	承認のレベルを定義し、文書化する。	干渉に関連記載あり			
6.1.1.11	個人が責任をもつ領域を規定するために、情報セキュリティ分野における責任を果たせるよう、任命された個人が当該分野の力量をもつこと、及び最新の状況を把握するための場合が与えられるようにする。	Sa-5.2.7	特定の情報セキュリティの役割をもつ個人は、その役割に必要な知識及び技能においてカ量をもつ。	干渉に関連記載あり			
–	（対応項なし）	Sa-5.2.8	その役割に関連し、その役割の責任を果たす上での必要な最新の動向に追随し続けるように支援される。	干渉に関連記載あり			
6.1.1.12	個人が責任をもつ領域を規定するために、供給者関係における情報セキュリティの側面の調整及び管理に関する事項の特定及び文書化を実施する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されて）	–	（対応項なし）	–
6.1.1.13.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）	5.2.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
6.1.2	職務の分離 相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離する。	5.3	職務の分離 管理策 相反する職務及び相反する責任範囲は、分離する。 目的 情報セキュリティ管理策の不正、誤り及び違反のリスクを軽減するため。		5.3	職務の分離 統制目標：相反する職務及び相反する責任範囲は、分離する。 目的：情報セキュリティ管理策の不正、誤り及び違反のリスクを軽減するため。	
6.1.2.1	認可されていない状態又は検知されない状態で、一人で資産に対してアクセス、修正又は使用ができないように管理策を適用する。	Sa-5.3.1	組織は、この職務及び責任範囲を分離するか分離するかを決定する。	干渉に関連記載あり	5.3.1	この職務及び責任範囲を分離するか分離するか定義し、分離する。	職務及び責任範囲の分離は、相反する可能性がある職務を一人の個人が自ら実行することを防ぐために、相反する職務を異なる個人に分離することを目的としている。次の事項は、分離が必要になる可能性のある活動の例である。 a) 変更の提案、承認及び実行 b) アクセス権の要求、承認及び付与 c) コードの設計、実装及びレビュー d) ソフトウェアの開発及び本番システムの管理 e) アプリケーション の使用及び管理 f) アプリケーションの使用及びデータベースの管理 g) 情報セキュリティ管理策の設計、監査及び保証 h) 承認又は許可を受ける申請者と当該承認等を行う許可権限者 i) 監査を受ける者とその監査を実施する者 分離の管理策の設計においては、共謀のおそれを考慮する。小さな組織では、職務の分離を実現するのは難しい場合があるし、しかし、この原則は、実施可能な限り適用することが望ましい。 分離が困難である場合には、活動の監視、監査証跡、管理職による監督等の他の管理策を考慮する。 役割に基づくアクセス制御システムを使用する場合に、一人の個人に対して、相反する複数の役割を許可しないことを確実にするように意する。 多数の役割がある場合、組織は、相反する役割を特定し、その除去を容易にするために自動化ツールの使用を考慮する。 役割を除去又は再割当てする場合のアクセスの問題を最小限にするために、役割は慎重に定義し、付与する。
6.1.2.2	ある作業を始めることと、その作業を認可することを分離する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されて）	–	（対応項なし）	–
6.1.2.3	管理策は、共謀のおそれを考慮して設計する。	Sa-5.3.2	分離の管理策の設計においては、共謀のおそれを考慮する。	干渉に関連記載あり	5.3.1	【再】この職務及び責任範囲を分離するか分離するか定義し、分離する。	（5.3.1に対応する項を参照）
6.1.2.4	職務の分離が困難である場合には、他の管理策（例えば、活動の監視、監査証跡、管理職による監督）を実施する。	Sa-5.3.3	分離が困難である場合には、活動の監視、監査証跡、管理職による監督等の他の管理策を考慮する。	干渉に関連記載あり			
–	（対応項なし）	Sa-5.3.4	役割に基づくアクセス制御システムを使用する場合に、一人の個人に対して、相反する複数の役割を許可しないことを確実にするように意する。	干渉に関連記載あり			
–	（対応項なし）	Sa-5.3.5	多数の役割がある場合、組織は、相反する役割を特定し、その除去を容易にするために自動化ツールの使用を考慮する。	干渉に関連記載あり			
–	（対応項なし）	Sa-5.3.6	役割を除去又は再割当てする場合のアクセスの問題を最小限にするために、役割は慎重に定義し、付与する。	干渉に関連記載あり			
–	（対応項なし）	–	（統一基準由来）	令和7年版にて追加 （情報セキュリティ管理基準以外の由来）	5.3.2	情報セキュリティ対策の運用において、以下の役割を兼務させない。 ・承認又は許可を受ける申請者と当該承認等を行う許可権限者 ・監査を受ける者とその監査を実施する者	特になし。
6.1.3	関係当局との連絡 関係当局との適切な連絡体制を維持する。	5.5	関係当局との連絡 管理策 組織は、関係当局との連絡体制を確立し、維持する。 目的 組織と、関係する法務、規制及び監督当局との間で、情報セキュリティに関して適切な情報の流通が行われることを確実にするため。		5.5	関係当局との連絡 統制目標：組織は、関係当局との連絡体制を確立し、維持する。 目的：組織と、関係する法務、規制及び監督当局との間で、情報セキュリティに関して適切な情報の流通が行われることを確実にするため。	
6.1.3.1	組織は、いつ、誰が関係当局（例えば、法の執行機関、規制当局、監督官庁）に連絡するかの手順を備える。	Sa-5.5.1	組織は、いつ、誰が関係当局に連絡するか、及び特定した情報セキュリティインシデントをいかにして時機を失せずに報告するかを規定する。	干渉に関連記載あり	5.5.1	情報セキュリティに関して、適切な情報の流通が行われることを確実にするために、関係当局との連絡体制を確立し、維持する。	組織は、いつ、誰が関係当局（例えば、法執行機関、規制当局、監督官庁）に連絡するか、及び特定した情報セキュリティインシデントをいかにして時機を失せずに報告するかを規定する。 関係当局との連絡は、これらの関係当局の現在及び今後の期待（例えば、適用される情報セキュリティ規制）についての理解を促進するためにも用いる。
6.1.3.2	法が破られた疑われる場合に、特定した情報セキュリティインシデントをいかにして時機を失せずに報告するかの手順を備える。	Sa-5.5.1	【再】組織は、いつ、誰が関係当局に連絡するか、及び特定した情報セキュリティインシデントをいかにして時機を失せずに報告するかを規定する。	干渉に関連記載あり			
–	（対応項なし）	Sa-5.5.2	関係当局との連絡は、これらの関係当局の現在及び今後の期待についての理解を促進するためにも用いる。	干渉に関連記載あり			
6.1.3.3.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）	5.5.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
6.1.3.5	脅威すべき兆候がある場合には、関係当局からの情報に基づき監視活動の水準を上げる。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
6.1.4	専門組織との連絡 情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持する。	5.6	専門組織との連絡 管理策 組織は、情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との連絡体制を確立し、維持する。 目的 情報セキュリティに関して適切な情報流通が行われることを確実にするため。		5.6	専門組織との連絡 統制目標：組織は、情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との連絡体制を確立し、維持する。 目的：情報セキュリティに関して適切な情報流通が行われることを確実にするため。	
6.1.4.1	最適な慣行に関する認識を改善し、関係するセキュリティ情報を最新に保つ手段として、情報セキュリティに関する研究会又は会議へ参加する。	Sa-5.6.1	次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。 a) 最適な慣行に関する知識を改善し、関係するセキュリティ情報に追随する。	干渉に関連記載あり	5.6.1	情報セキュリティに関して、適切な情報の流通が行われることを確実にするために、専門組織との連絡体制を確立し、維持する。	次の事項を達成する手段として、専門組織（情報セキュリティに関する研究会又は会議及び情報セキュリティの専門家による協会・団体）との連絡体制を確立し、維持する。 a) 最適な慣行に関する知識を改善し、関係するセキュリティ情報に追随する。 b) 情報セキュリティ環境の理解が最新であることを確実にする。 c) 攻撃及びぜい弱性に関する早期警戒警報、勧告及びパッチを受理する。 d) 専門家から情報セキュリティの助言を得る。 e) 新しい技術、製品、サービス、脅威又はぜい弱性に関する情報を共有し、交換する。 f) 情報セキュリティインシデントを扱う場合の、適切な連絡窓口を提供する（5.24～5.28参照）。
6.1.4.2	情報セキュリティ環境の理解が最新かつ完全であることを確実にする手段として、情報セキュリティに関する研究会又は会議へ参加する。	Sa-5.6.1	次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。 b) 情報セキュリティ環境の理解が最新であることを確実にする。	干渉に関連記載あり			
6.1.4.3	攻撃及びぜい弱性に関連する早期警戒警報、勧告及びパッチを受理する手段として、情報セキュリティに関する研究会又は会議へ参加する。	Sa-5.6.1	次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。 c) 攻撃及びぜい弱性に関する早期警戒警報、勧告及びパッチを受理する。	干渉に関連記載あり			
6.1.4.4	専門家から情報セキュリティの助言を得る手段として、情報セキュリティに関する研究会又は会議へ参加する。	Sa-5.6.1	次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。 d) 専門家から情報セキュリティの助言を得る。	干渉に関連記載あり			
6.1.4.5	新しい技術、製品、脅威又はぜい弱性に関する情報を共用し、交換する手段として、情報セキュリティに関する研究会又は会議へ参加する。	Sa-5.6.1	次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。 e) 新しい技術、製品、サービス、脅威又はぜい弱性に関する情報を共有し、交換する。	干渉に関連記載あり			
6.1.4.6	情報セキュリティインシデントを扱う場合の、適切な連絡窓口を提供する手段として、情報セキュリティに関する研究会又は会議へ参加する。	Sa-5.6.1	次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。 f) 情報セキュリティインシデントを扱う場合の、適切な連絡窓口を提供する。	干渉に関連記載あり			
6.1.4.7	脅威すべき兆候がある場合には、情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体からの情報に基づき監視活動の水準を上げる。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–

番号	（旧）管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	（新）管理策基準	（参考）手引き
6.1.5	プロジェクトマネジメントにおける情報セキュリティ プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組む。	5.8	プロジェクトマネジメントにおける情報セキュリティ 管理策 情報セキュリティをプロジェクトマネジメントに組み入れる。 目的 プロジェクトのライフサイクル全体を通じて、プロジェクトマネジメントにおいて、プロジェクト及び成果物に関連する情報セキュリティリスクに効果的に対処することを確実にするため。		5.8	プロジェクトマネジメントにおける情報セキュリティ 統制目標：情報セキュリティをプロジェクトマネジメントに組み入れる。 目的：プロジェクトのライフサイクル全体を通じて、プロジェクトマネジメントにおいて、プロジェクト及び成果物に関連する情報セキュリティリスクに効果的に対処することを確実にするため。	
6.1.5.1	情報セキュリティリスクがプロジェクトの中で特定及び対処されることを確実にするために、情報セキュリティを組織のプロジェクトマネジメント手法に組み入れ、プロジェクトの特性にかかわらず、一般にあらゆるプロジェクト（例えば、中核事業プロセス、IT、施設管理、その他のサポートプロセスのためのプロジェクト）に適用されるようにする	5a-5.8.1	プロジェクトマネジメントの一部として情報セキュリティリスクに対処することを確実にするために、情報セキュリティをプロジェクトマネジメントに組み入れる。	手引に関連記載あり	5.8.1	情報セキュリティリスクへの対応をプロジェクトマネジメントに組み入れる。	プロジェクトマネジメントの一部として情報セキュリティリスクに対処することを確実にするために、情報セキュリティをプロジェクトマネジメントに組み入れる。これは、プロジェクトの複雑さ、規模、期間、分野又は適用領域にかかわらず、あらゆる種類のプロジェクトに適用可能である（例えば、中核事業プロセス、ICT、施設管理又はその他の支援プロセスのプロジェクト）。 プロジェクトマネジメントは、次の事項を要求する。 a）情報セキュリティリスクを、プロジェクトリスクの一部として、プロジェクトのライフサイクル全体を通じて、早い段階及び定期的にリスクアセスメント及びリスク対応を実施する。 b）情報セキュリティ要求事項（例えば、アプリケーションセキュリティの要求事項（8.26））、知的財産権を順守するための要求事項（5.32）など）には、プロジェクトの早い段階で対処する。 c）内部及び外部への伝達の側面のセキュリティなど、プロジェクトの実行に伴う情報セキュリティリスクを、プロジェクトのライフサイクル全体を通じて考慮し、処理する。 d）情報セキュリティリスク対応の選択状況をレビューし、対応の有効性を評価及び試験する。 情報セキュリティリスク対応の選択状況及び活動の適切性を、あらかじめ定めた段階において、適切な人物又はガバナンス機関がフォローアップする。 プロジェクトに関連する情報セキュリティの責任及び権限を定義し、規定された役割に割り当てる。
–	（対応項なし）	（5a-5.8.1参考）	これは、プロジェクトの複雑さ、規模、期間、分野又は適用領域にかかわらず、あらゆる種類のプロジェクトに適用可能である。	手引に関連記載あり			
6.1.5.2	プロジェクトマネジメント手法においては、情報セキュリティ目的をプロジェクトの目的に含める。	–	（直接対応する評価管理策無し）	明確な対応関係なし（情報セキュリティ管理策策定確保が打了）	–	（対応項なし）	–
6.1.5.3	プロジェクトマネジメント手法においては、必要な管理策を特定するため、プロジェクトの早い段階で情報セキュリティリスクアセスメントを実施する。	5a-5.8.2	用いるプロジェクトマネジメントでは、次の事項を要求する。 a）情報セキュリティリスクを、プロジェクトリスクの一部として、プロジェクトのライフサイクル全体を通じて、早い段階で及び定期的にリスクアセスメント及びリスク対応を実施する。 b）情報セキュリティ要求事項には、プロジェクトの早い段階で対処する。	手引に関連記載あり	5.8.1	【再】情報セキュリティリスクへの対応をプロジェクトマネジメントに組み入れる。	（5.8.1に対応する項を参照）
6.1.5.4	プロジェクトマネジメント手法においては、適用するプロジェクトマネジメントの方法論の全ての局面において、情報セキュリティを含める。	5a-5.8.2	用いるプロジェクトマネジメントでは、次の事項を要求する。 c）内部及び外部への伝達の側面のセキュリティなど、プロジェクトの実行に伴う情報セキュリティリスクを、プロジェクトのライフサイクル全体を通じて考慮し、処理する。	手引に関連記載あり			
6.1.5.5	全てのプロジェクトにおいて、情報セキュリティの組織への影響を明確にし、これを定期的にレビューする。	5a-5.8.2	用いるプロジェクトマネジメントでは、次の事項を要求する。 d）情報セキュリティリスク対応の選択状況をレビューし、対応の有効性を評価及び試験する。	手引に関連記載あり			
–	（対応項なし）	5a-5.8.3	情報セキュリティの考慮及び活動の適切性は、あらかじめ定めた段階において、適切な人物又はプロジェクト運営委員会などのガバナンス機関がフォローアップする。	手引に関連記載あり			
6.1.5.6	プロジェクトマネジメント手法で定められた役割を明確にするため、情報セキュリティに関する責任を定め、割り当てる。	5a-5.8.4	プロジェクトに関連する情報セキュリティの責任及び権限を定義し、規定された役割に割り当てる。	手引に関連記載あり			
6.2	モバイル機器及びテレワーキング 管理目的：モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。	8.1	利用者エンドポイント機器 管理策 利用者エンドポイント機器に保存されている情報、処理される情報、又は利用者エンドポイント機器をウェブアクセス可能な情報を保護する。 目的 利用者エンドポイント機器を使用することによってもたらされるリスクから情報を保護するため。		8.1	エンドポイント機器 統制目標：エンドポイント機器に保存されている情報、処理される情報、又はエンドポイント機器をウェブアクセス可能な情報を保護する。 目的：エンドポイント機器を使用することによってもたらされるリスクから情報を保護するため。	
6.2.1	モバイル機器を用いる場合、業務情報が危険にさらされないことを確実にするために、特別な注意を払う。						
6.2.1.1	モバイル機器を用いる場合、業務情報が危険にさらされないことを確実にするために、特別な注意を払う。	8a-8.1.6	利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧奨する。 b）利用者エンドポイント機器は、利用していない場合、物理的管理策及び論理的管理策を用いて、認可されていない利用から保護する。重要度の高い、取扱いに慎重を要する、又は影響の大きい業務情報が入っている機器を、無人の状態で放置しない。	手引に関連記載あり	8.1.2	エンドポイント機器を保護するための対策を実施する。	可能な限り、エンドポイント機器の管理策に関する推奨事項を、構成管理（8.9参照）又は自動化されたツールにより強制する。 エンドポイント機器を保護するためのセキュリティ要求事項及び手順、並びにそのセキュリティ対策を実施する際らの責任について、全ての利用者に認識させる。 エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧奨する。 a）エンドポイント機器を必要がなくなった、実行していたセッションからログオフ又、サービスを終了する。 b）エンドポイント機器は、利用していない場合、物理的管理策（例えば、キーロック又は時間ロック）及び論理的管理策（例えば、パスワードアクセス）を用いて、認可されていない利用から保護する。重要度の高い、取扱いに慎重を要する、又は影響の大きい業務情報が入っている機器を、無人の状態で放置しない。 c）公共の場所、オープンオフィス、集会所及びその他の保護されていない場所では、特別な注意を払ってエンドポイント機器を使用する（例えば、他人が背後から読むことが可能な場合に秘密情報を読むことは避ける、また、プライバシースクーンフィルタを使用する。）。 d）エンドポイント機器を盗難から物理的に保護する（例えば、自動車、他の輸送機関、ホテルの部屋、会議室、集会所において）。 個人所有の機器（BYODとしても知られる。）の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。 a）機器の個人使用と業務上の使用とを区別する。このような区別を可能とし、個人所有の機器に保存された業務データを保護するためのソフトウェアの使用も含む。 b）利用者が自らの義務（物理的保護、ソフトウェアの更新など）を受け入れた場合にだけ、業務情報にアクセスできるようにする。業務データについて権限を主張しないこと、及び機器の盗難若しくは紛失が含む場合又はサービス利用の認可が取り消された場合に組織の義務持ちデータを消去することへの合意を含む。こうした場合、利害機に関する法令を考慮することが望ましい。 c）個人所有の機器で開発された知的財産権に関する紛争を防止するためのトピック固有の手引及び手順 d）個人所有の機器へのアクセス（機械のセキュリティを検証する目的で、又は調査において）。これは法令で禁止されている場合がある。 e）要員又は外部組織の利用者が個人で所有するエンドポイント機器上のライアンドソフトウェアについて、ライセンスを受ける責任を組織が負うことになる可能性があるソフトウェアライセンス契約 禁止事項の例を以下に示す。 a）端末、OS、アプリケーション等の改造行為 b）安全性が確認できないアプリケーションのインストール及び利用 c）利用が禁止されている（ソフトウェア）のインストール及び利用（利用を禁止するソフトウェアを定める場合） d）許可されない通信回線サービスの利用（利用する回線を限定する場合） e）第三者への端末の貸与 f）利用者認証を用いないクラウドサービス等への機密情報のバックアップ g）機密性の高い情報の取扱い
6.2.1.2	モバイル機器の情報セキュリティ方針は、保護されていない環境におけるモバイル機器を用いた作業のリスクを考慮して定める。	8a-8.1.6	利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧奨する。 c）公共の場所、オープンオフィス、集会所及びその他の保護されていない場所では、特別な注意を払って利用者エンドポイント機器を使用する。	手引に関連記載あり			
–	（対応項なし）	8a-8.1.1	組織は、利用者エンドポイント機器のセキュリティを保つた構成及び取扱いに関するトピック固有の方針を確立する。	手引に関連記載あり	8.1.1	エンドポイント機器のセキュリティに関する方針、要求事項及び手順を整備する。	エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 a）エンドポイント機器が取扱い、処理、保存又は支援をすることが可能な情報の種類及び分類レベル b）エンドポイント機器の登録 c）物理的保護についての要求事項 d）ソフトウェアのインストールの制限（例えば、システムの実務管理者が適時で管理する。） e）エンドポイント機器のソフトウェア（ソフトウェアの脆を含む。）の要求事項及び更新の適用の要求事項（例えば、脆の自動更新） f）情報サービス、公衆ネットワーク、又はその他の構外ネットワークへの接続に関する規則（例えば、パーソナルファイアウォールの使用を求める。） g）アクセス制御 h）配信装置の暗号化 i）マルウェアからの保護 j）遠隔操作による機器の無効化、データの消去又はロック k）バックアップ l）ウェブサービス及びウェブアプリケーションの使用 m）エンユーザーの行動の分析（8.16参照） n）取外し可能な eMS装置を含む取外し可能な機器の使用、及び物理ポート（例えば、USB ポート）を無効化できる可能性 o）エンドポイント機器に分割機能がある場合は、その利用。これによって、組織の情報及びその他の関連資産がセキュリティを保つて分離することが可能である。 お含情報が特に慎重な取扱いを要する場合に、エンドポイント機器を用いてその情報にアクセスは可能とするが、その機器には保存はできないようにするかどうかを検討する。その場合、機器に追加の技術的保護手段が必要になる可能性がある。例えば、オフライン作業のためのファイルのダンロードの無効化、及びSDカードなどのローカルストレージの無効化を確実にすることがある。 組織は、エンドポイント機器のセキュリティのために次の事項に関する手順を確立する。 a）機器の無線接続の構成（例えば、ｗｉ-fiなどプロコルを無効化する。） b）関連するトピック固有の方針に従って適切な等域幅の無線又は有線接続を使用すること（例えば、バックアップ又はソフトウェア更新が必要であるため。） エンドポイント機器の監視又は紛失に備えて、法令、規則、契約（保険を含む。）及び組織のその他のセキュリティ要求事項を考慮して、そのための手順を確立する。
6.2.1.3	モバイル機器の情報セキュリティ方針には、モバイル機器の登録を含める。	8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 b）利用者エンドポイント機器の登録	手引に関連記載あり			
6.2.1.4	モバイル機器の情報セキュリティ方針には、物理的保護についての要求事項を含める。	8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 c）物理的保護についての要求事項	手引に関連記載あり			
6.2.1.5	モバイル機器の情報セキュリティ方針には、ソフトウェアのインストールの制限を含める。	8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 d）ソフトウェアのインストールの制限	手引に関連記載あり			
6.2.1.6	モバイル機器の情報セキュリティ方針には、モバイル機器のソフトウェアのバージョン及びパッチ適用に対する要求事項を含める。	8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 e）利用者エンドポイント機器のソフトウェア（ソフトウェアの脆を含む。）の要求事項及び更新の適用の要求事項	手引に関連記載あり			
6.2.1.7	モバイル機器の情報セキュリティ方針には、情報サービスへの接続の制限を含める。	8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 f）情報サービス、公衆ネットワーク、又はその他の構外ネットワークへの接続に関する規則	手引に関連記載あり			
6.2.1.8	モバイル機器の情報セキュリティ方針には、アクセス制御を含める。	8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 g）アクセス制御	手引に関連記載あり			
6.2.1.9	モバイル機器の情報セキュリティ方針には、暗号技術を含める。	8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 h）配信装置の暗号化	手引に関連記載あり			
6.2.1.10	モバイル機器の情報セキュリティ方針には、マルウェアからの保護を含める。	8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 i）マルウェアからの保護	手引に関連記載あり			
6.2.1.11	モバイル機器の情報セキュリティ方針には、遠隔操作による機器の無効化、データの消去又はロックを含める。	8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 j）遠隔操作による機器の無効化、データの消去又はロック	手引に関連記載あり			
6.2.1.12	モバイル機器の情報セキュリティ方針には、バックアップを含める。	8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 k）バックアップ	手引に関連記載あり			
6.2.1.13	モバイル機器の情報セキュリティ方針には、ウェブサービス及びウェブアプリケーションの使用を含める。	8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 l）ウェブサービス及びウェブアプリケーションの使用	手引に関連記載あり			
–	（対応項なし）	8a-8.1.2	利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。 a）利用者エンドポイント機器が取扱い、処理、保存又は支援をすることが可能な情報の種類及び分類レベル m）エンドユーザーの行動の分析 n）取外し可能なeMS装置を含む取外し可能な機器の使用、及び物理ポートを無効化できる可能性 o）利用者エンドポイント機器に分割機能がある場合は、その利用。これによって、組織の情報及びその他の関連資産がセキュリティを保つて分離することが可能である。	手引に関連記載あり			
–	（対応項なし）	8a-8.1.3	お含情報が特に慎重な取扱いを要する場合に、利用者エンドポイント機器を用いてその情報にアクセスは可能とするが、その機器には保存はできないようにするかどうかを検討する。	手引に関連記載あり			
–	（対応項なし）	（8a-8.1.3参考）	その場合、機器に追加の技術的保護手段が必要になる可能性がある。例えしては、オフライン作業のためのファイルのダンロードの無効化、及びSDカードなどのローカルストレージの無効化を確実にすることがある。	手引に関連記載あり			
–	（対応項なし）	8a-8.1.4	可能な限り、利用者エンドポイント機の管理策に関する豚策事項を、構成管理又は自動化されたツールによって強制する。	手引に関連記載あり			
–	（対応項なし）	8a-8.1.9	組織は、利用者エンドポイント機器のセキュリティのために次の事項に関する手順を確立する。 a）機器の無線接続の構成 b）関連するトピック固有の方針に従って適切な等域幅の無線又は有線接続を使用すること	手引に関連記載あり			
6.2.1.14	公共の場所、会議室、その他保護されていない場所でモバイル機器を用いるとは、注意を払う。	8a-8.1.6	【再】利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧奨する。 c）公共の場所、オープンオフィス、集会所及びその他の保護されていない場所では、特別な注意を払って利用者エンドポイント機器を使用する。	手引に関連記載あり			
6.2.1.15	モバイル機器に保管され、処理される情報について、認可されていないアクセスは並ぶいを防止するため、例えば、暗号技術の使用、秘密認証情報の使用の強制などの保護を実施する。	8a-8.1.6	【再】利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧奨する。 b）利用者エンドポイント機器は、利用していない場合、物理的管理策及び論理的管理策を用いて、認可されていない利用から保護する。重要度の高い、取扱いに慎重を要する、又は影響の大きい業務情報が入っている機器を、無人の状態で放置しない。	手引に関連記載あり			
6.2.1.16	モバイル機器は、盗難、特にごこか（例えば、自動車、他の輸送機関、ホテルの部屋、会議室、集会所）に置き忘れたための盗難から、物理的に保護する。	8a-8.1.6	利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧奨する。 d）利用者エンドポイント機器を盗難から物理的に保護する。	手引に関連記載あり			
6.2.1.17	モバイル機器の盗難又は紛失の場合の対策のために、法規則、保険及び組織の他のセキュリティ要求事項を考慮した特定の手順を確立する。	8a-8.1.7	利用者エンドポイント機器の盗難又は紛失に備えて、法令、規則、契約（保険を含む。）及び組織のその他のセキュリティ要求事項を考慮して、そのための手順を確立する。	手引に関連記載あり			
6.2.1.18	重要度の高い、取扱いに慎重を要する又は影響の大きい業務情報が入っているモバイル機器は、無人の状態で放置しない。	8a-8.1.6	【再】利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように勧奨する。 b）利用者エンドポイント機器は、利用していない場合、物理的管理策及び論理的管理策を用いて、認可されていない利用から保護する。重要度の高い、取扱いに慎重を要する、又は影響の大きい業務情報が入っている機器を、無人の状態で放置しない。	手引に関連記載あり			
6.2.1.19	重要度の高い、取扱いに慎重を要する又は影響の大きい業務情報が入っているモバイル機器は、可能な場合に、情報が暗号化技術を用いて保護されていることを確実にするために、特別な設定を用いる。	–	（直接対応する評価管理策無し）	明確な対応関係なし（情報セキュリティ管理策策定確保が打了）	–	（対応項なし）	–
6.2.1.20	作業形態に起因する追加のリスク及び実施すべき管理策についての徹底向上のために、モバイル機器を用いる要員に対する教育・訓練を計画・準備・実施する。	–	（直接対応する評価管理策無し）	明確な対応関係なし（情報セキュリティ管理策策定確保が打了）	–	（対応項なし）	–

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
6.2.1.21	モバイル機器の情報セキュリティ方針で、個人所有のモバイル機器の使用が許されている場合は、その方針及び関連するセキュリティ対策において、機器の私的な使用と業務上の使用とを区別する。（このような区別を可能とし、個人所有の機器に保存された業務データ保護するためのソフトウェアの使用も含む）	6a-8.1.8	個人所有の機器の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。 a) 機器が個人専用と業務上の使用とを区別する。このような区別を可能とし、個人所有の機器に保存された業務データを保護するためのソフトウェアの使用も含む。	手引に関連記載あり	8.1.2	【再】エンドポイント機器を保護するための対策を実施する。	（8.1.2に対応する項を参照）
6.2.1.22	モバイル機器の情報セキュリティ方針で、個人所有のモバイル機器の使用が許されている場合は、その方針及び関連するセキュリティ対策において、エンドユーザが悪意に利用者が若名した場合に応じ、業務情報にアクセスできるようにする（エンドユーザの悪意には、利用者の義務（物理的な保護、ソフトウェアの更新など）についての確認、業務データに対する所有権を主張しないこと、及び機器の盗難若しくは紛失があった場合又はサービス利用の認可が失われた場合に組織が遠隔操作でデータを消去することへの合意を含む。この方針では、プライバシーに関する点を考慮する。）。	6a-8.1.8	個人所有の機器の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。 b) 利用者が自らの義務（物理的な保護、ソフトウェアの更新など）を使い入れた場合には、業務情報にアクセスできるようにする。業務データに対する所有権を主張しないこと、及び機器の盗難若しくは紛失があった場合又はサービス利用の認可が失われた場合に組織が遠隔操作でデータを消去することへの合意を含む。こうした場合、円双護に関する点を考慮する。	手引に関連記載あり			
6.2.1.23	モバイル機器の情報セキュリティ方針で、個人所有のモバイル機器の使用が許されている場合は、その方針及び関連するセキュリティ対策において、モバイル機器に情報を保存させない機能の使用、又はモバイル機器に保存される情報を暗号化するための策を実施する。なお、可能な限りモバイル機器に情報を保存させない機能を使用する。	–	（統一基準由来）	明確な対応関係なし	–	（対応項なし）	–
6.2.2	テレワーキング テレワーキングの場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施する。	6.7	リモートワーク 管理策 組織の境外でアクセス、処理又は保存される情報を保護するために、要員が遠隔で作業をする場合のセキュリティ対策を実施する。 目的 要員が遠隔で作業をする場合の情報セキュリティを確実にするため。		6.7	リモートワーク 統制目標：組織の境外でアクセス、処理又は保存される情報を保護するために、要員が遠隔で作業をする場合のセキュリティ対策を実施する。 目的：要員が遠隔で作業をする場合の情報セキュリティを確実にするため。	
6.2.2.1	テレワーキング活動を許可する組織は、テレワーキング行う場合の条件及び制限を定めた方針を発行する。	6a-6.7.1	リモートワーク活動を許可する組織は、関連する条件及び制限を定めたリモートワーク に関するヒツ固有の方針を発行する。	手引に関連記載あり	6.7.1	リモートワーク活動を許可する組織は、関連する条件及び制限を定めたリモートワーク に関する方針を策定する。	リモートワークは、組織の境外から組織の要員が作業し、ハードエピ ではICT機器を通じて電子的に情報にアクセスするために行われる。リモートワーク環境は、テレワーキング、コワーキング等に有効に在宅勤務（telecommuting）、柔軟な作業場（flexible workplace）、仮想的な作業環境、及び遠隔保守と呼ばれる環境を含んでいる。 注記記載によって異なる、現場の法令及び規制のため、この手引の全ての振捉事項が適用できるとは限らない。リモートワーク活動を許可する組織は、関連する条件及び制限を定めたリモートワークに関するヒツ固有の方針を持する。 適用可能な場合には、リモートワークに関するヒツ固有の方針として、次の事項を考慮する。 a) 要員が配置されている活域を含め、リモートワークの場所及び周辺環境の物理的セキュリティを考慮に入れた、リモートワークの場所における既存の又は新たに提案する物理的セキュリティ b) 施設可能なファイリングキャビネット、場所間におけるセキュリティを保つべき移送、並びにリモートアクセス、クリアデスク、情報及びその他の関連資産の印刷及び廃棄、情報セキュリティ事象の報告及びインシデント管理、遠隔物理環境のための規則及びセキュリティの仕組み c) 期待される物理的なリモートワーク環境 d) 立を考慮した、通信のセキュリティに関する要求事項 1) 組織のシステムへのリモートアクセスの必要性 2) 通信回線からアクセスし、通信回線を通過する情報の取扱いに慎重を要する度合い 3) システム及びアプリケーションの取扱いに慎重を要する度合い e) 個人所有の機器での情報の処理及び保管を支援する、仮想デスクトップなどのリモートアクセスの使用 f) リモートワークの場所における、他者（例えば、家族、友人）による情報又は資源への認可されていないアクセスの脅威 g) 公共の場所における、他者による情報又は資源への認可されていないアクセスの脅威 h) 家庭のネットワーク及び公衆ネットワークの使用並びに無線ネットワークサービスの設定に関する要求事項又は制限 i) ファイアウォール及びマルウェア からの保護などのセキュリティ対策の使用 j) システムを遠隔で観視し、初期化するためのセキュリティに配慮した仕組み k) 組織のネットワークへのモートアクセスを許可する場合に、単一要素認証の仕組みのがい弱性を考慮に入れた、認証及びアクセス権限有効化のためのセキュリティに配慮した仕組み
6.2.2.2	テレワーキングを行う場合の条件及び制限は、適切に考えられ、かつ適法な場合には、建物及び周辺環境の物理的セキュリティを考慮に入れた、テレワーキングの場所の既存の物理的セキュリティの状況を考慮して定める。	6a-6.7.2	適用可能な場合には、リモートワークに関するヒツ固有の方針として、次の事項を考慮する。 a) 要員が配置されている活域を含め、リモートワークの場所及び周辺環境の物理的セキュリティを考慮に入れた、リモートワークの場所における既存の又は新たに提案する物理的セキュリティ	手引に関連記載あり			
6.2.2.3	テレワーキングを行う場合の条件及び制限は、適切に考えられ、かつ適法な場合には、提案された物理的なテレワーキングの環境を考慮して定める。	6a-6.7.2	適用可能な場合には、リモートワークに関するヒツ固有の方針として、次の事項を考慮する。 c) 期待される物理的なリモートワーク環境	手引に関連記載あり			
6.2.2.4	テレワーキングを行う場合の条件及び制限は、適切に考えられ、かつ適法な場合には、組織の内部システムへの遠隔アクセスの必要性、通信回線からアクセスし、通信回線を通過する情報の取扱い慎重度及び内部システムの取扱いに関する慎重度を考慮し、通信のセキュリティに関する要求事項を考慮して定める。	6a-6.7.2	適用可能な場合には、リモートワークに関するヒツ固有の方針として、次の事項を考慮する。 d) 立を考慮した、通信のセキュリティに関する要求事項 －組織のシステムへのリモートアクセスの必要性 －通信回線からアクセスし、通信回線を通過する情報の取扱いに慎重を要する度合い －システム及びアプリケーションの取扱いに慎重を要する度合い	手引に関連記載あり			
6.2.2.5	テレワーキングを行う場合の条件及び制限は、適切に考えられ、かつ適法な場合には、個人所有の装置で情報を処理及び保管できないように不正である仮想デスクトップなどを考慮して定める。	6a-6.7.2	適用可能な場合には、リモートワークに関するヒツ固有の方針として、次の事項を考慮する。 e) 個人所有の機器での情報の処理及び保管を支援する、仮想デスクトップなどのリモートアクセスの使用	手引に関連記載あり			
6.2.2.6	テレワーキングを行う場合の条件及び制限は、適切に考えられ、かつ適法な場合には、住環境を共有する者（例えば、家族、友人）による、情報又は資源への認可されていないアクセスの脅威を考慮して定める。	6a-6.7.2	適用可能な場合には、リモートワークに関するヒツ固有の方針として、次の事項を考慮する。 f) リモートワークの場所における、他者による情報又は資源への認可されていないアクセスの脅威	手引に関連記載あり			
6.2.2.7	テレワーキングを行う場合の条件及び制限は、適切に考えられ、かつ適法な場合には、家庭のネットワークの使用及び無線ネットワークサービスの設定に関する要求事項又は制限を考慮して定める。	6a-6.7.2	適用可能な場合には、リモートワークに関するヒツ固有の方針として、次の事項を考慮する。 h) 家庭のネットワーク及び公衆ネットワークの使用並びに無線ネットワークサービスの設定に関する要求事項又は制限	手引に関連記載あり			
–	（対応項なし）	6a-6.7.2	適用可能な場合には、リモートワークに関するヒツ固有の方針として、次の事項を考慮する。 i) 施設可能なファイリングキャビネット、場所間におけるセキュリティを保つべき移送、並びにリモートアクセス、クリアデスク、情報及びその他の関連資産の印刷及び廃棄、情報セキュリティ事象の報告に関する規則など、遠隔物理環境のための規則及びセキュリティの仕組み g) 公共の場所における、他者による情報又は資源への認可されていないアクセスの脅威 j) システムを遠隔で観視し、初期化するためのセキュリティに配慮した仕組み k) 組織のネットワークへのモートアクセスを許可する場合に、単一要素認証の仕組みのがい弱性を考慮に入れた、認証及びアクセス権限有効化のためのセキュリティに配慮した仕組み	手引に関連記載あり			
6.2.2.8	テレワーキングを行う場合の条件及び制限は、適切に考えられ、かつ適法な場合には、個人所有の装置の上で開発した知的財産の権利に関する論争を防ぐための方針及び手順を考慮して定める。	6a-8.1.8	【再】個人所有の機器の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。 c) 個人所有の機器で開発された知的財産権に関する紛争を防止するためのヒツ固有の方針及び手順	手引に関連記載あり	8.1.2	【再】エンドポイント機器を保護するための対策を実施する。	（8.1.2に対応する項を参照）
6.2.2.9	テレワーキングを行う場合の条件及び制限は、適切に考えられ、かつ適法な場合には、個人所有の装置へのアクセス（装置のセキュリティ保証のためのもの、又は調査期間中に行うもの）を考慮して定める。なお、このアクセスは、法令が厳している場合があ。	6a-8.1.8	【再】個人所有の機器の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。 d) 個人所有の機器へのアクセス（機械のセキュリティを検証する目的で、又は調査において）これは法令で禁止されている場合がある。	手引に関連記載あり			
6.2.2.10	テレワーキングを行う場合の条件及び制限は、適切に考えられ、かつ適法な場合には、従業員又は外部の利用者が個人的に所有するワークステーション上のライアンスソフトウェアの使用許可について、組織が責任をもつことにならない場合の、ソフトウェアの使用許可規則が考慮して定める。	6a-8.1.8	【再】個人所有の機器の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。 e) 要員又はお部組織の利用者が個人で所有する利用者エンドポイント機器上のライアンスソフトウェアについて、ライセンスを受ける責任を組織が負うことにならない場合があるソフトウェアライセンス契約	手引に関連記載あり			
6.2.2.11	テレワーキングを行う場合の条件及び制限は、適切に考えられ、かつ適法な場合には、マルウェアに対する保護及びファイアウォールの要件を考慮して定める。	6a-6.7.2	適用可能な場合には、リモートワークに関するヒツ固有の方針として、次の事項を考慮する。 i) ファイアウォール及びマルウェアからの保護などのセキュリティ対策の使用	手引に関連記載あり	6.7.1	【再】リモートワーク活動を許可する組織は、関連する条件及び制限を定めたリモートワークに関する方針を策定する。	（6.7.1に対応する項を参照）
6.2.2.12	テレワーキングを行う場合に考慮すべき物計及び取決めには、組織の管理下にない個人所有の装置の使用を許さない場合には、テレワーキング活動のための適切な装置及び保管用具の使用に関する事項を含める。	6a-6.7.3	リモートワークに関し、考慮すべき物計及び対策には、次の事項を含む。 a) 組織の管理下にない個人所有の機器の使用を許さない場合には、リモートワーク活動のための適切な機器及び保管用具の提供	手引に関連記載あり	6.7.2	リモートワーク活動に関するセキュリティ対策を実施する。	リモートワークに関し、考慮すべき物計及び対策には、次の事項を含む。 a) 組織の管理下にない個人所有の機器の使用を許さない場合には、リモートワーク活動のための適切な機器及び保管用具の提供 b) 許可した作業、保持することができる情報の分類、並びにプレートワークを行う者にアクセスを認可するため第ジステムなリサービスの定義
6.2.2.13	テレワーキングを行う場合に考慮すべき物計及び取決めには、許可した作業、作業時間、保持してもよい情報の分類、並びにテレワーキングを行う者にアクセスを認可するため第ジステムなリサービスの定義に関する事項を含める。	6a-6.7.3	リモートワークに関し、考慮すべき物計及び対策には、次の事項を含む。 b) 許可した作業、保持することができる情報の分類、並びにプレートワークを行う者にアクセスを認可するため第ジステムなリサービスの定義	手引に関連記載あり			c) 遠隔で作業する者及び支援を提供する者のための鋭線の提供。これは、遠隔で作業しつつセキュリティに配慮した方法で業務を行う方法を含む。 d) 機器画面のロック及び非アクティブ状態タイマー、機器の位置追跡の有効化、遠隔データ消去機能のインストールに関する要求事項など、セキュリティに配慮したプレートアクセス方法を含む。適切な遠隔機器の提供 e) 物理的セキュリティ f) 無装及び効照者による機器及び情報へのアクセスに関する規則及び手引 g) ハードウェア及びソフトウェアのサポート及び保守の提供 h) 保険の提供 i) バックアップ及び事業継続のための手順 j) 監査及びセキュリティの監視 k) リモートワークが終了したとき、権限及びアクセス権の失効並びに機器の返却 情報システムへリモートアクセスする場合、多要素認証を行う。
6.2.2.14	テレワーキングを行う場合に考慮すべき物計及び取決めには、安全な遠隔アクセス方法を含め、適切な遠隔装置の問題に関する事項を含める。	6a-6.7.3	リモートワークに関し、考慮すべき物計及び対策には、次の事項を含む。 d) 機器画面のロック及び非アクティブ状態タイマー、機器の位置追跡の有効化、遠隔データ消去機能のインストールに関する要求事項など、セキュリティに配慮したリモートアクセス方法を含む。適切な遠隔機器の提供	手引に関連記載あり			
6.2.2.15	テレワーキングを行う場合に考慮すべき物計及び取決めには、物理的セキュリティに関する事項を含める。	6a-6.7.3	リモートワークに関し、考慮すべき物計及び対策には、次の事項を含む。 e) 物理的セキュリティ	手引に関連記載あり			
6.2.2.16	テレワーキングを行う場合に考慮すべき物計及び取決めには装置及び情報へのアクセスに関する規則及び手引を含める。	6a-6.7.3	リモートワークに関し、考慮すべき物計及び対策には、次の事項を含む。 f) 無装及び効照者による機器及び情報へのアクセスに関する規則及び手引	手引に関連記載あり			
6.2.2.17	テレワーキングを行う場合に考慮すべき物計及び取決めには、ハードウェア及びソフトウェアのサポート及び保守の提供を含める。	6a-6.7.3	リモートワークに関し、考慮すべき物計及び対策には、次の事項を含む。 g) ハードウェア及びソフトウェアのサポート及び保守の提供	手引に関連記載あり			
6.2.2.18	テレワーキングを行う場合に考慮すべき物計及び取決めには、保険の問題を含める。	6a-6.7.3	リモートワークに関し、考慮すべき物計及び対策には、次の事項を含む。 h) 保険の提供	手引に関連記載あり			
6.2.2.19	テレワーキングを行う場合に考慮すべき物計及び取決めには、バックアップ及び事業継続のための手順を含める。	6a-6.7.3	リモートワークに関し、考慮すべき物計及び対策には、次の事項を含む。 i) バックアップ及び事業継続のための手順	手引に関連記載あり			
6.2.2.20	テレワーキングを行う場合に考慮すべき物計及び取決めには、監査及びセキュリティの監視に関する事項を含める。	6a-6.7.3	リモートワークに関し、考慮すべき物計及び対策には、次の事項を含む。 j) 監査及びセキュリティの監視	手引に関連記載あり			
6.2.2.21	テレワーキングを行う場合に考慮すべき物計及び取決めには、テレワーキング終了したとき、権限及びアクセス権の失効並びに装置の返却に関する事項を含める。	6a-6.7.3	リモートワークに関し、考慮すべき物計及び対策には、次の事項を含む。 k) リモートワーク が終了したとき、権限及びアクセス権の失効並びに機器の返却	手引に関連記載あり			
–	（対応項なし）	6a-6.7.3	リモートワークに関し、考慮すべき物計及び対策には、次の事項を含む。 c) 遠隔で作業する者及び支援を提供する者のための鋭線の提供。これは、遠隔で作業しつつセキュリティに配慮した方法で業務を行う方法を含む。	手引に関連記載あり			
6.3.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		9.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
6.3.1.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）						
6.3.1.1.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準で規定）	9.1.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
7	人的資源のセキュリティ	6.1	選考 管理策 要員になる全ての候補者についての経歴などの確認は、適用される法令、規制及び倫理を考慮に入れて、組織に加える前に、及びその後継続的に行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。 目的 全ての要員が、予定する役割に対して適格かつ適切であり、雇用中に適格かつ適切であり続けることを確実にするため。		6.1	選考 統制目標：要員になる全ての候補者についての経歴などの確認は、適用される法令、規制及び倫理を考慮に入れて、組織に加える前に、及びその後継続的に行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。 目的：全ての要員が、予定する役割に対して適格かつ適切であり、雇用中に適格かつ適切であり続けることを確実にするため。	
7.1	雇用前 管理目的：従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。						
7.1.1	雇用前 全ての従業員候補者について経歴などの確認は、関連する法令、規制及び倫理に従って行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。						
7.1.1.1	関連があるプライバシー、PIIの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、満足のいく職務状（例えば、業務についての）の入手についての確認を行う。	6a-6.1.4	要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許容される場合には、次の事項を含む。 a) 満足のいく職務状の入手の可否	手引に関連記載あり	6.1.2	全ての候補者に対する選考プロセスにおいて、PII保護及び雇用に関する法令を考慮に入れてC必要な確認を行う。	選考プロセスは、フルタイム、パートタイム及び臨時スタッフを含む全ての要員に対して実行する。 サービスの拡張を通じて提考された個人に対して契約する場合には、選考や要求事項を組織と供給者との間の合意に含める。 組織内である職位にだけはこれを検討している全ての候補者についての情報は、当該活域での適切な法令を考慮して収集し、扱う。 活域によっては、選考活動について、組織が候補者に事前に通知することが法的に必要な場合がある。 要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、次の事項を含む。 a) 満足のいく職務状（例えば、業務及び入物に関する振薦状）の入手の可否 b) 応募者の履歴書の確認（完全であるか及び正確であるかの確認） c) 提示された学術上及び職業上の資格の確認 d) 公的証明書（例えば、パスポート又は運転な当局が発行したその他の許可可能な文書）の確認 e) 候補者が重要な役割を担う場合には、信用情報又は犯罪記録のレビューなど、より詳細な確認
7.1.1.2	関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、応募者の履歴書の確認（完全であるか及び正確であるかの確認）を行う。	6a-6.1.4	要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許容される場合には、次の事項を含む。 b) 応募者の履歴書の確認（完全であるか及び正確であるかの確認）	手引に関連記載あり			
7.1.1.3	関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、提示された学術上及び職業上の資格の確認を行う。	6a-6.1.4	要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許容される場合には、次の事項を含む。 c) 提示された学術上及び職業上の資格の確認	手引に関連記載あり			
7.1.1.4	関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、公的証明書（パスポート又は同種の文書）の確認を行う。	6a-6.1.4	要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許容される場合には、次の事項を含む。 d) 公的証明書の確認	手引に関連記載あり			
7.1.1.5	関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、信用情報又は犯罪記録のレビューなど、より詳細な確認を行う。	6a-6.1.4	要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許容される場合には、次の事項を含む。 e) 候補者が重要な役割を担う場合には、信用情報又は犯罪記録のレビューなど、より詳細な確認	手引に関連記載あり			
7.1.1.6	情報セキュリティに関する特定の役割のために雇用する場合、組織は、候補者が、情報セキュリティに関するその役割を実にするために必要な力量を備えていることを確認する。	6a-6.1.5	情報セキュリティに関する特定の役割のために雇用する場合、組織は、次の事項を確認する。 a) 候補者が、情報セキュリティに関するその役割を実にするために必要な力量を備えている。	手引に関連記載あり	6.1.3	情報セキュリティに関する特定の役割のために雇用する場合、必要な確認を行う。	情報セキュリティに関する特定の役割のために雇用する場合、組織は、次の事項を確認する。 a) 候補者が、情報セキュリティに関するその役割を実にするために必要な力量を備えている。 b) 特に、その役割が組織にとって重要なものである場合は、候補者が、その役割を任せられる信頼できる人物である。 最初の発令で就く業務であるか、昇進して就く業務であるかにかかわず、情報処理施設にアクセスすることがその担当者にとって必要になる場合、特にそれらの設備が秘密情報（例えば、財務情報、個人情報又は医療情報）を扱っているときには、組織は、より詳細な確認も検討する。
7.1.1.7	情報セキュリティに関する特定の役割のために雇用する場合、組織は、特に、その役割が組織にとって重要なものである場合は、候補者が、その役割を任せられる信頼できる人物であることを確認する。	6a-6.1.5	情報セキュリティに関する特定の役割のために雇用する場合、組織は、次の事項を確認する。 b) 特に、その役割が組織にとって重要なものである場合は、候補者が、その役割を任せられる信頼できる人物である。	手引に関連記載あり			
7.1.1.8	最初の発令で就く業務であるか、昇進して就く業務であるかにかかわらず、情報処理施設にアクセスすることがその担当者にとって必要になる場合、特にそれらの設備が秘密情報（例えば、財務情報、個人情報又は医療情報）を扱っているときには、組織は、より詳細な確認も検討する。	6a-6.1.6	最初の発令で就く業務であるか、昇進して就く業務であるかにかかわらず、情報処理施設にアクセスすることがその担当者にとって必要になる場合、特にそれらの設備が秘密情報を扱っているときには、組織は、より詳細な確認も検討する。	手引に関連記載あり			
7.1.1.9	全般には、確認のためのレビューの基準及び制約を定める（例えば、誰が逆考するのか、また、この確認のためのレビューは、いつ、どのように、なぜ行うのか。）。	6a-6.1.7	逆考手順には、要員になる候補者の確認のためのレビューの基準及び制約を定める。	手引に関連記載あり	6.1.1	要員になる候補者の確認の基準及び制約を定める。	逆考手順には、要員になる候補者の確認のためのレビューの基準及び制約を定める（例えば、誰が逆考するのか、また、この確認のためのレビューは、いつ、どのように、なぜ行うのか。）。
7.1.1.10	逆考プロセスは、契約相手に対しても確実に実施する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で規定済み）	–	（対応項なし）	–
7.1.1.11	契約相手に対して逆考プロセスを実施する場合、組織と契約相手との間の合意では、逆考の実施に関する責任、及びその逆考が完了していると主張するための結果に疑念若しくは懸念が生じるに足り必要がある高知手順を定める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で規定済み）	–	（対応項なし）	–
7.1.1.12	組織内である職位にだけはこれを検討している全ての候補者についての情報は、当該活域での適切な法令に従って収集し、扱う。	6a-6.1.3	組織内である職位にだけはこれを検討している全ての候補者についての情報は、当該活域での適切な法令を考慮して収集し、扱う。	手引に関連記載あり	6.1.2	【再】全ての候補者に対する逆考プロセスにおいて、PII保護及び雇用に関する法令を考慮に入れてC必要な確認を行う。	（6.1.2に対応する項を参照）
7.1.1.13	適用される法令によっては、逆考活動について候補者へ、事前に通知する。	（6a-6.1.3参考）	活域によっては、逆考活動について、組織が候補者に事前に通知することが法的に必要な場合がある。	手引に関連記載あり			
–	（対応項なし）	6a-6.1.8	時機を失せずに要員になる候補者の確認を完了できない状況では、レビュー が終了するまで、例えば、次のような立場成のための管理策を実施する。 a) 実務研修の開始時期を遅らせる。 b) 企業高度の利用を遅らせる。 c) アクセス権を限定して実務研修を実施する。 d) 雇用を終了する。	手引に関連記載あり	6.1.4	時機を失せずに要員になる候補者の確認を完了できない状況では、確認が終了するまで、例えば、次のような立場成のための管理策を実施する。 a) 実務研修の開始時期を遅らせる。 b) 企業高度の利用を遅らせる。 c) アクセス権を限定して実務研修を実施する。 d) 雇用を終了する。 個人の役割の重要性に応じて、要員が適切であり続けることを確実にするための確認を定期的に繰り返す。
–	（対応項なし）	6a-6.1.9	個人の役割の重要性に応じて、要員が適切であり続けることを確実にするための確認を定期的に繰り返す。	手引に関連記載あり			
7.1.2	雇用条件 従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載する。	6.2	雇用条件 管理策 雇用契約書には、情報セキュリティに関する要員及び組織の責任を記載する。 目的 要員が、予定する役割における自らの情報セキュリティの責任を理解することを確実にするため。		6.2	雇用条件 統制目標：雇用契約書には、情報セキュリティに関する要員及び組織の責任を記載する。 目的：要員が、予定する役割における自らの情報セキュリティの責任を理解することを確実にするため。	
7.1.2.1	従業員又は契約相手の契約上の義務には、組織の情報セキュリティのための方針等を反映する。	6a-6.2.1	要員の契約上の義務は、組織の情報セキュリティ方針及びその他の関連するヒツ固有の方針を考慮に入れる。	手引に関連記載あり	6.2.1	情報セキュリティに関する役割及び責任を含む雇用条件を定める。	要員の契約上の義務は、組織の情報セキュリティ方針及びその他の関連する方針を考慮に入れる。 場合に応じて、次の事項を明確にし、民及する。 a) 秘密情報へのアクセスが与えられる全ての要員が情報及びその他の関連資産へのアクセスが与えられる前に

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
7.1.2.2	従業員又は契約相手の契約には、秘密情報への アクセスが与えられる全ての従業員及び契約相手による、情報処理施設へのアクセスが与えられる前の、秘密保持契約書又は守秘義務契約書への署名を含める。	6a-6.2.2	場合に応じて、次の事項について明確にし、合意する。 a) 秘密情報へのアクセスが与えられる全ての要員が情報及びその他の関連資産へのアクセス(与えられる)前に署名することが望ましい秘密保持契約書又は守秘義務契約書	予防に関連記載あり			署名することが望ましい秘密保持契約書又は守秘義務契約書（6.6参照） b) 法的な責任及び権利（例えば、著作権法、データ保護に関連して制定された法令（5.32及び5.34参照））に関するもの） c) 要員によって扱われる、情報の分類、組織の情報及びその他の関連資産の管理、並びに情報処理施設及び情報サービスの提供に関する責任（5.9及び5.13参照） d) 判断猶予者から受け取った情報の扱いに関する責任 e) 要員が組織の情報セキュリティ要求事項に従わない場合にとる処置（6.4参照） 情報セキュリティに関する役割及び責任は、雇用前のプロセスにおいて候補者に伝達する。
7.1.2.3	従業員又は契約相手の契約には、従業員及び契約相手の法的な責任及び権利（例えば、著作権法、データ保護に関連して制定された法律）を明確にする。	6a-6.2.2	場合に応じて、次の事項について明確にし、合意する。 b) 法的な責任及び権利	予防に関連記載あり			
7.1.2.4	従業員及び契約相手の契約には、従業員及び契約相手によって扱われる情報の分類に関する責任、並びに従業員及び契約相手によって扱われる組織の情報、情報に関連するその他の資産、情報処理施設及び情報サービスの管理に関する責任を明確にする。	6a-6.2.2	場合に応じて、次の事項について明確にし、合意する。 c) 要員によって扱われる、情報の分類、組織の情報及びその他の関連資産の管理、並びに情報処理施設及び情報サービスの管理に関する責任	予防に関連記載あり			
7.1.2.5	従業員及び契約相手の契約には、他社又は外部関係者から受け取った情報の扱いに関する従業員及び契約相手の責任を明確にする。	6a-6.2.2	場合に応じて、次の事項について明確にし、合意する。 d) 判断猶予者から受け取った情報の扱いに関する責任	予防に関連記載あり			
7.1.2.6	従業員及び契約相手の契約には、従業員及び契約相手が組織のセキュリティ要求事項に従わない場合にとる処置を含める。	6a-6.2.2	場合に応じて、次の事項について明確にし、合意する。 e) 要員が組織の情報セキュリティ要求事項に従わない場合にとる処置	予防に関連記載あり			
7.1.2.7	情報セキュリティに関する役割及び責任は、雇用前のプロセスにおいて候補者に伝達する。	6a-6.2.3	情報セキュリティに関する役割及び責任は、雇用前のプロセスにおいて候補者に伝達する。	予防に関連記載あり			
7.1.2.8	組織は、従業員及び契約相手が情報セキュリティに関する雇用条件に同意することを確実にする仕組みを整備する。	6a-6.2.4	組織は、要員が情報セキュリティに関する雇用条件に同意することを確実にする。	予防に関連記載あり	6.2.2	雇用契約書等を用いて、組織の要員と情報セキュリティに関する雇用条件の同意を得る。	組織は、要員が情報セキュリティに関する雇用条件に同意することを確実にする。 情報セキュリティに関する雇用条件は、情報システム及びサービスに関連する組織の資産に対する要員によるアクセスの特性及び範囲に応じて、適切なものとする。
7.1.2.9	雇用条件は、情報システム及びサービスと関連する組織の資産に対する、従業員及び契約相手によるアクセスの特性及び範囲に応じて、適切なものとする。	6a-6.2.5	情報セキュリティに関する雇用条件は、情報システム及びサービスに関連する組織の資産に対する要員によるアクセスの特性及び範囲に応じて、適切なものとする。	予防に関連記載あり			
7.1.2.10	雇用の終了後も、定められた期間は、その雇用条件に含まれている責任を維持させる。	6a-6.2.7	適切であれば、雇用の終了後も、定められた期間は、その雇用条件に含まれている責任を維持させる。	予防に関連記載あり	6.2.3	法令、規則、情報セキュリティ方針又は情報セキュリティに関連する方針が変更された場合は、情報セキュリティに関する雇用条件をレビューする。	法令、規則、情報セキュリティ方針又はトピック固有の方針が変更された場合は、情報セキュリティに関する雇用条件をレビューする。 適切であれば、雇用の終了後も、定められた期間は、その雇用条件に含まれている責任を維持させる（6.5参照）。
7.2.1	経営陣の責任 経営陣は、組織の確立された方針及び手順に従った情報セキュリティの適用を、全ての従業員及び契約相手に要求する。	5.4	管理陣の責任 管理策 管理陣は、組織の確立された情報セキュリティ方針、トピック固有の方針及び手順に従った情報セキュリティの適用を、全ての要員に要求する。 目的 管理陣が、情報セキュリティにおける自らの役割を理解し、全ての要員が自らの情報セキュリティの責任を認識し、果たすことを確実にすることを目的として行動することを確実にするため。		5.4	管理陣の責任 統制の目標：管理陣は、組織の確立された情報セキュリティ方針、トピック固有の方針及び手順に従った情報セキュリティの適用を、全ての要員に要求する。 目的：管理陣が、情報セキュリティにおける自らの役割を理解し、全ての要員が自らの情報セキュリティの責任を認識し、果たすことを確実にすることを目的として行動することを確実にするため。	
7.2.1.1	経営陣の責任には、従業員及び契約相手に、秘密情報又は情報システムへのアクセスが許可される前に、情報セキュリティの役割及び責任について、要点を絞り伝える仕組みを整備することを含める。	5a-5.4.2	管理陣の責任には、要員について、次の事項を確実にすることを含む。 a) 組織の情報及びその他の関連資産へのアクセスを許可する前に、情報セキュリティの役割及び責任について、要点を絞り伝える。	予防に関連記載あり	5.4.1	方針及び手順に従った情報セキュリティの適用を、全ての要員へ実施させることを、管理陣の責任として求める。	管理陣は、情報セキュリティ方針、トピック固有の方針、手順及び情報セキュリティ管理策に対する支援を実証するため、管理陣の責任には、要員について、次の事項を確実にすることを含む。 a) 組織の情報及びその他の関連資産へのアクセスを許可する前に、情報セキュリティの役割及び責任について、要点を絞り伝える。 b) 組織内で、情報セキュリティについて要員に期待する役割を示す指針を提供する。 c) 組織の情報セキュリティ方針及びトピック固有の方針に従うことを徹底する。 d) 組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する（6.3参照）。 e) 組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件、契約又は合意を順守させる。 f) 継続的な専門教育を通じて、情報セキュリティに関する適切な技能及び資格を保持し続ける。 g) 実行可能な場合、情報セキュリティ方針、トピック固有の方針又は情報セキュリティの認識についての手順への遵守を報告するための、匿名の報告経路を提供する（例えば、内部通報）。これによって、匿名の報告を可能にする。又は報告者のアイデンティティに関する知識をその報告を扱う必要のある人だけが知ることを確実にする等の工夫をすることも可能にする。 h) 組織のセキュリティ関連のプロセス及び管理策を実施するための、適切な資源及びプロジェクトを計画する時間を提供する。
7.2.1.2	経営陣の責任には、従業員及び契約相手に、組織内での役割において、情報セキュリティについて期待することをかてあの指針を提供する仕組みを整備することを含める。	5a-5.4.2	管理陣の責任には、要員について、次の事項を確実にすることを含む。 b) 組織内で、情報セキュリティについて要員に期待する役割を示す指針を提供する。	予防に関連記載あり			
7.2.1.3	経営陣の責任には、従業員及び契約相手に、組織の情報セキュリティのための方針に従うように動機付ける仕組みを整備することを含める。	5a-5.4.2	管理陣の責任には、要員について、次の事項を確実にすることを含む。 c) 組織の情報セキュリティ方針及びトピック固有の方針に従うことを徹底する。	予防に関連記載あり			
7.2.1.4	経営陣の責任には、従業員及び契約相手に、組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成させる仕組みを整備することを含める。	5a-5.4.2	管理陣の責任には、要員について、次の事項を確実にすることを含む。 d) 組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成させる。	予防に関連記載あり			
7.2.1.5	経営陣の責任には、従業員及び契約相手に、組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うように下るを仕組みを整備することを含める。	5a-5.4.2	管理陣の責任には、要員について、次の事項を確実にすることを含む。 e) 組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件、契約又は合意を順守させる。	予防に関連記載あり			
7.2.1.6	経営陣の責任には、従業員及び契約相手に、適切な技能及び資格を保持し、定期的に教育を受けさせる仕組みを整備することを含める。	5a-5.4.2	管理陣の責任には、要員について、次の事項を確実にすることを含む。 f) 継続的な専門教育を通じて、情報セキュリティに関する適切な技能及び資格を維持させる。	予防に関連記載あり			
7.2.1.7	経営陣の責任には、従業員及び契約相手に、情報セキュリティのための方針又は手順への違反を報告するための、匿名の報告経路を提供する（例えば、内部告発）仕組みを整備することを含める。	5a-5.4.2	管理陣の責任には、要員について、次の事項を確実にすることを含む。 g) 実行可能な場合、情報セキュリティ方針、トピック固有の方針又は情報セキュリティのための手順への違反を報告するための、匿名の報告経路を提供する。これによって、匿名の報告を可能にする。又は報告者のアイデンティティに関する知識をその報告を扱う必要のある人だけが知ることを確実にする等の工夫をすることも可能にする。	予防に関連記載あり			
–	（対応項なし）	5a-5.4.2	管理陣の責任には、要員について、次の事項を確実にすることを含む。 h) 組織のセキュリティ関連のプロセス及び管理策を実施するための、適切な資源及びプロジェクトを計画する時間を提供する。	予防に関連記載あり			
7.2.1.8	経営陣は、情報セキュリティのための方針、手順及び管理策に対する支持を実証し、手本となるように行動する。	5a-5.4.1	管理陣は、情報セキュリティ方針、トピック固有の方針、手順及び情報セキュリティ管理策に対する支援を実証する。	予防に関連記載あり			
7.2.2	情報セキュリティの意識向上、教育及び訓練 組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受ける。	6.3	情報セキュリティの意識向上、教育及び訓練 管理策 組織の要員及び関連する利害関係者は、職務に関連する組織の情報セキュリティ方針、トピック固有の方針及び手順についての、適切な、情報セキュリティに関する意識向上プログラム、教育及び訓練を受け、また、定期的な更新を受ける。 目的 要員及び関連する利害関係者が自らの情報セキュリティの責任を意識し、それを果たすことを確実にするため。		6.3	情報セキュリティの意識向上、教育及び訓練 統制の目標：組織の要員及び関連する利害関係者は、職務に関連する組織の情報セキュリティ方針、トピック固有の方針及び手順についての、適切な、情報セキュリティに関する意識向上プログラム、教育及び訓練を受け、また、定期的な更新を受ける。 目的：要員及び関連する利害関係者が自らの情報セキュリティの責任を意識し、それを果たすことを確実にするため。	
7.2.2.1	情報セキュリティの意識向上プログラムは、従業員、及び関係する場合は契約相手に対し、情報セキュリティに関する各自の責任及びその責任を果たす方法について、認識させることを狙いとする。	6a-6.3.5	情報セキュリティの意識向上プログラムは、要員に対し、情報セキュリティに関する各自の責任及びその責任を果たす方法について、認識させることを狙いとする。	予防に関連記載あり	6.3.1	内部及び外部の要員の役割を含めた、情報セキュリティの意識向上プログラムを計画し、定期的に実施する。	情報セキュリティ意識向上 教育及び訓練プログラムは、保護すべき組織の情報及び情報を保護するために実施されている情報セキュリティ管理策を考慮に入れて、組織の情報セキュリティ方針、情報セキュリティ関連に関連する方針及び手順に沿って確立する。 情報セキュリティの意識向上 教育及び訓練は、定期的に実施する。 可能な場合、開始時の意識向上 教育及び訓練は、新しい要員、及び情報セキュリティに関する要求事項が大幅に異なる前の又は役割に異動した者にも適用する。 知識が伝わったこと、並びに意識向上 教育及び訓練プログラムの有効性を確認するため、意識向上 教育及び訓練の活動終了時に、要員の理解の評価を行う。 情報セキュリティの意識向上プログラムは、要員に対し、情報セキュリティに関する各自の責任及びその責任を果たす方法について、認識させることを狙いとし、内部及び外部の要員（例えば、外部のコンサルタント、供給者の要員）を含む、組織における要員の役割を考慮に入れて、計画する。 意識向上プログラムの活動は、長期にわたり、ただすば定期的に実施する。これによって、活動が繰り返され、新しい要員も対象となる。 意識向上プログラムの活動では、情報セキュリティインシデントから学んだ教訓を生かす。 意識向上プログラムには、キャンペーン、パンフレット、ポスター、会報、ウェブサイト、説明会、ブリーフィング、eラーニングモジュール、電子メールなど、適切な物理的又は仮想的な手段を通じた多くの意識向上活動を含める。 情報セキュリティの意識向上には、例えば、次のような一般的な例題を含める。 a) 組織全体にわたる情報セキュリティに対する経営陣のコミットメント b) 情報セキュリティ及びトピック固有の方針、基準、法令、規則、契約及び企業を考慮に入れた、適用された情報セキュリティの規則及び義務に関する最適実及び順守のニーズ c) 自身が行動したこと及び行動しなかったことに対する個人のアカウンタビリティ、並びに組織及び利害関係者に属する情報のセキュリティを保ち、これを保護することに対する一般的な責任 d) 情報セキュリティに関する基本的な手順（例えば、情報セキュリティ事象の報告（6.8）及び基本的な管理策（例えば、パスワードのセキュリティ（5.17）） e) 情報セキュリティに関連する脆弱についての追加の情報及び助言（情報セキュリティの意識向上に関する追加の資料も含む）を得るための連絡先及び情報源 マルウェアに対する保護について、マルウェアに感染した電子メール、ファイル又はプログラムの受信、送信又はインストールを特定し、可能ならば阻止するりまについて、全ての利用者に意識向上又は訓練を提供する。（8.7.6） ウェブへのアクセスを含め、オンライン資源のセキュリティを保った適切な使用について、要員を訓練する。（8.23.2） オンライン資源のセキュリティを保った適切な使用についての訓練には、組織の規則、セキュリティの担当を報告するための連絡先、及び制限されたウェブ資源に正当な業務上の理由によってアクセスする必要がある場合の例外プロセスを含める。 ウェブサイトで、セキュリティが低下したりすることを通知するブラウザアドバイザリや無効にしないことを確実にするように、要員を訓練する。
7.2.2.2	情報セキュリティの意識向上プログラムは、保護すべき組織の情報及び情報を保護するために実施されている管理策を考慮に入れて、組織の情報セキュリティのための方針及び関連する手順に沿って確立する。	6a-6.3.1	情報セキュリティの意識向上、教育及び訓練プログラムは、保護すべき組織の情報及び情報を保護するために実施されている情報セキュリティ管理策を考慮に入れて、組織の情報セキュリティ方針、トピック固有の方針及び手順に沿って確立する。	予防に関連記載あり			
7.2.2.3	情報セキュリティの意識向上プログラムには、キャンペーン（例えば、情報セキュリティの日）、及びパンフレット又は会報の発行のような、複数の意識向上活動を含める。	6a-6.3.9	意識向上プログラムには、キャンペーン、パンフレット、ポスター、会報、ウェブサイト、説明会、ブリーフィング、eラーニングモジュール、電子メール など、適切な物理的又は仮想的な手段を通じた多くの意識向上活動を含める。	予防に関連記載あり			
7.2.2.4	情報セキュリティの意識向上プログラムは、組織における従業員の役割、及び関係する場合には契約相手の組織における組織の期待を考慮に入れて、計画する。	6a-6.3.6	意識向上プログラムは、内部及び外部の要員を含む、組織における要員の役割を考慮に入れて、計画する。	予防に関連記載あり			
7.2.2.5	情報セキュリティの意識向上プログラムの活動は、新しい従業員及び契約相手を対象にされるよう、長期にわたり、これは定期的に計画する。	6a-6.3.7	意識向上プログラムの活動は、長期にわたり、これは定期的に実施する。	予防に関連記載あり			
7.2.2.6	情報セキュリティの意識向上プログラムは、定期的に更新して組織の方針及び手順に沿って、情報セキュリティインシデントから学んだ教訓を生かす。	6a-6.3.8	意識向上プログラムの活動では、情報セキュリティインシデントから学んだ教訓を生かす。	予防に関連記載あり			
7.2.2.7	意識向上のための訓練は、（例えば、教室での訓練、通信教育、インターネットを利用した訓練、自己学習その他含め、多様な手段を用いて、）組織の情報セキュリティの意識向上プログラムで必要とされた場合に実施する。	6a-6.3.9	【再】意識向上プログラムには、キャンペーン、パンフレット、ポスター、会報、ウェブサイト、説明会、ブリーフィング、eラーニングモジュール、電子メールなど、適切な物理的又は仮想的な手段を通じた多くの意識向上活動を含める。	予防に関連記載あり			
7.2.2.8	情報セキュリティの教育及び訓練には、組織全体にわたる情報セキュリティに対する経営陣のコミットメントの提示を含める。	6a-6.3.10	情報セキュリティの意識向上には、例えば、次のような一般的な例題を含める。 a) 組織全体にわたる情報セキュリティに対する経営陣のコミットメント	予防に関連記載あり			
7.2.2.9	情報セキュリティの教育及び訓練には、方針、規則、法令、規則、契約及び企業で定められた、適用された情報セキュリティの規則及び義務を熟知し、これを順守する必要性を含める。	6a-6.3.10	情報セキュリティの意識向上には、例えば、次のような一般的な例題を含める。 b) 情報セキュリティ及びトピック固有の方針、基準、法令、規則、契約及び企業を考慮に入れた、適用された情報セキュリティの規則及び義務に関する最適実及び順守のニーズ	予防に関連記載あり			
7.2.2.10	情報セキュリティの教育及び訓練には、自身が行動したこと及び行動しなかったことに対する個人の責任、並びに組織及び外部関係者に属する情報のセキュリティを保つか、これを保護することに対する一般的な責任を含める。	6a-6.3.10	情報セキュリティの意識向上には、例えば、次のような一般的な例題を含める。 c) 自身が行動したこと及び行動しなかったことに対する個人のアカウンタビリティ、並びに組織及び利害関係者に属する情報のセキュリティを保ち、これを保護することに対する一般的な責任	予防に関連記載あり			
7.2.2.11	情報セキュリティの教育及び訓練には、情報セキュリティに関する基本的な手順（例えば、情報セキュリティインシデントの報告）及び基本的な管理策（例えば、パスワードのセキュリティ、マルウェアの制御、クリアデスク）を含める。	6a-6.3.10	情報セキュリティの意識向上には、例えば、次のような一般的な例題を含める。 d) 情報セキュリティに関する基本的な手順	予防に関連記載あり			
7.2.2.12	情報セキュリティの教育及び訓練には、情報セキュリティに関連する事項についての追加的な情報及び助言（情報セキュリティの教育及び訓練に関する追加の資料も含む）を得るための連絡先及び情報源を含める。	6a-6.3.10	情報セキュリティの意識向上には、例えば、次のような一般的な例題を含める。 e) 情報セキュリティに関連する脆弱についての追加の情報及び助言（情報セキュリティの意識向上に関する追加の資料も含む）を得るための連絡先及び情報源	予防に関連記載あり			
7.2.2.13	情報セキュリティの教育及び訓練は、定期的に実施するだけでなく、情報システムの変更に伴い必要に応じて実施する。	6a-6.3.2	情報セキュリティの意識向上、教育及び訓練は、定期的に実施する。	予防に関連記載あり			
7.2.2.14	最初の教育及び訓練は、新入社員だけでなく、情報セキュリティに関する要求事項が大幅に異なる新たな職位又は役割に異動した者にも適用し、その役割が始まる前に実施する。	6a-6.3.3	可能な場合、開始時の意識向上、教育及び訓練は、新しい要員、及び情報セキュリティに関する要求事項が大幅に異なる新たな職位又は役割に異動した者にも適用する。	予防に関連記載あり			
–	（対応項なし）	6a-6.3.4	知識が伝わったこと、並びに意識向上、教育及び訓練プログラムの有効性を確認するため、意識向上、教育及び訓練の活動終了時に、要員の理解の評価を行う。	予防に関連記載あり			
7.2.2.15	組織は、教育及び訓練を効果的に実施するためのプログラムを開発する。	–	（直接対応する評価管理策無し）	明確な対応関係なし（情報セキュリティ管理策基準で規承されず）	–	（対応項なし）	–
7.2.2.16	教育及び訓練を効果的に実施するためのプログラムは、保護する必要のある組織の情報及び情報を保護するために実施されている管理策を考慮に入れるプロセスを含める。	–	（直接対応する評価管理策無し）	明確な対応関係なし（情報セキュリティ管理策基準で規承されず）	–	（対応項なし）	–
7.2.2.17	教育及び訓練を効果的に実施するためのプログラムは、組織の情報セキュリティのための方針及び関連手順に沿って定める。	–	（直接対応する評価管理策無し）	明確な対応関係なし（情報セキュリティ管理策基準で規承されず）	–	（対応項なし）	–
–	（対応項なし）	6a-6.3.11	組織は、特定の技能及び専門知識を必要とする役割をセ技術チームに対して、適切な訓練計画を特定し、準備し、実施する。	予防に関連記載あり	6.3.2	特定の技能及び専門知識を必要とする役割をセ技術チームに対して、適切な訓練計画を策定し、定期的に実施する。	組織は、特定の技能及び専門知識を必要とする役割をセ技術チームに対して、適切な訓練計画を特定し、準備し、実施する。 技術チームは、装置・機器、システム、アプリケーション及びサービスに必要なセキュリティレベルを構成し、維持する技能をセる。 技術チームに不足している技能がある場合、組織は処置をとり、それを取得させる。 教育及び訓練プログラムは、様々な形式（例えば、講義又は自己学習、専門スクラブ又はコンサルタントによる助言（オンザジョブトレーニング）、スタッフ等異なる活動に従事させるローテーション、既に熟練している人材の採用及びコンサルタントの雇用）を検討する。教室、通信教育、ウェブ利用、自習式、及びその他異なる提供手段が利用可能である。 技術要員は、会報及び雑誌を購読する、又は技術的及び専門的な向上を目的とした会議及びイベントに参加することによって、自らの知識を最新の状態に保つ。
–	（対応項なし）	6a-6.3.12	技術チームは、装置・機器、システム、アプリケーション及びサービスに必要なセキュリティレベルを構成し、維持する技能をセる。	予防に関連記載あり			
–	（対応項なし）	6a-6.3.13	技術チームに不足している技能がある場合、組織は処置をとり、それを取得させる。	予防に関連記載あり			
7.2.2.18	教育及び訓練を効果的に実施するためのプログラムでは、講義又は自己学習のように、多様な教育及び訓練の形式（例えば、手順書確認訓練又はシナリオ非提示型訓練）を考慮して、定める。	6a-6.3.14	教育及び訓練プログラムは、様々な形式を検討する。	予防に関連記載あり			
–	（対応項なし）	（6a-6.3.14参考）	教室、通信教育、ウェブ利用、自習式、及びその他異なる提供手段が利用可能である。	予防に関連記載あり			
–	（対応項なし）	6a-6.3.15	技術要員は、会報及び雑誌を購読する、又は技術的及び専門的な向上を目的とした会議及びイベントに参加することによって、自らの知識を最新の状態に保つ。	予防に関連記載あり			
–	（対応項なし）	–	（統一基準由来）	令和7年度にて追加（情報セキュリティ管理策基準以外の由来）	6.3.3	情報セキュリティインシデントの対処手順が適切に機能することを訓練等により確認する。	訓練等には、実際に使用する機器を利用した「実機訓練」や、逐次の状況付与を受けて判断等を行う「ロールプレイング」、状況設定の上で予め作成を行う「シミュレーション」といった大掛かりなものの他、より簡易な「ウォークスルー」や「机上チェック」といった手法が存在する。緊急等の習熟度等に応じて、必要な訓練等を検討し実施することが考えられる。 S.24.1で規定された情報セキュリティインシデント管理プロセスに照らし確認する。
7.2.2.19.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理策基準以外の由来）	6.3.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
7.2.2.25	情報セキュリティの意識向上プログラム並びに教育及び訓練は、平時、非常時、不当時、緊急時、及びインシデント対応を考慮して定め、実施する。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–

番号	（旧）管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	（新）管理策基準	（参考）手引き
7.2.3	懲戒手続 情報セキュリティ違反を犯した従業員に対して処置をとるため、正式かつ周知された懲戒手続を備える。	6.4	懲戒手続 管理策 情報セキュリティ方針違反を犯した要員及びその他の関連する利害関係者に対して処置をとるために、懲戒手続を正式に定め、伝達する。 目的 要員及びその他の関連する利害関係者が情報セキュリティ方針違反の結果を理解すること、違反を防止すること、及び/それを犯した要員及びその他の関連する利害関係者を適切に扱うことを確実にするため。		6.4	懲戒手続 統制目標：情報セキュリティ方針違反を犯した要員及びその他の関連する利害関係者に対して処置をとるために、懲戒手続を正式に定め、伝達する。 目的：要員及びその他の関連する利害関係者が情報セキュリティ方針違反の結果を理解すること、違反を防止すること、及び/それを犯した要員及びその他の関連する利害関係者を適切に扱うことを確実にするため。	
7.2.3.1	懲戒手続は、情報セキュリティ違反が生じたことの事前の確認を待って開始する。	6a-6.4.1	懲戒手続は、情報セキュリティ違反が生じたことの事前の確認を待って開始する。	予防に関連記載あり	6.4.1	正式な懲戒手続として、違反の内容や性質に応じた段階別の対応を定め、関連する要員及びその他の利害関係者に伝達する。	正式な懲戒手続は、次のような要素を考慮した段階別の対応を定める。 a）違反の内容（誰が、何を、いつ、どのように）及び重大さ、並びにその結果 b）違反が意図的である（悪意がある）か、又は意図的でない（偶発的）か。 c）最初の違反か又は繰り返されたものか。 d）違反者は、適切に教育・訓練されていたかどうか。 懲戒手続は、情報セキュリティ方針違反が生じたことの事前の確認を待って開始する。証拠の収集については5.28参照。 懲戒手続の対応は、関連する法令、規制、契約及び事業上の要求事項、並びに必要に応じてその他の要素を考慮に入れる。 懲戒手続を、要員及びその他の関連する利害関係者が情報セキュリティ方針、トピック固有の方針、及び情報セキュリティの手順に違反することを防ぐための抑止力として使うことも望ましい。意図的な情報セキュリティ方針への違反には、直ちに処置をとることが求められる場合がある。
7.2.3.2	正式な懲戒手続には、情報セキュリティ違反を犯したという疑いがかけられた従業員に対する正確かつ公平な取扱いを含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応適切なし）	–
7.2.3.3	正式な懲戒手続は、違反の内容及び重大さ並びにその事象上の影響、最初の違反又は繰り返されたものか、適切に教育・訓練されていたかどうか、関連する法令、取引契約、その他の必要な要素を考慮した段階別の対応を定める。	6a-6.4.2	正式な懲戒手続は、次のような要素を考慮した段階別の対応を定める。 a）違反の内容（誰が、何を、いつ、どのように）及び重大さ、並びにその結果 b）違反が意図的である（悪意がある）か、又は意図的でない（偶発的）か。 c）最初の違反か又は繰り返されたものか。 d）違反者は、適切に教育・訓練されていたかどうか。	予防に関連記載あり	6.4.1	【再】正式な懲戒手続として、違反の内容や性質に応じた段階別の対応を定め、関連する要員及びその他の利害関係者に伝達する。	（6.4.1に対応する語を参照）
–	（対応適切なし）	6a-6.4.3	懲戒手続の対応は、関連する法令、規制、契約及び事業上の要求事項、並びに必要に応じてその他の要素を考慮に入れる。	予防に関連記載あり			
7.2.3.4	懲戒手続を、従業員が情報セキュリティ違反（従業員による組織の情報セキュリティのための方針群及び手順への違反並びに他のすべての情報セキュリティ違反）を犯すことを防ぐための抑止力として使う。	6a-6.4.4	懲戒手続を、要員及びその他の関連する利害関係者が情報セキュリティ方針、トピック固有の方針、及び情報セキュリティの手順に違反することを防ぐための抑止力として使う。	予防に関連記載あり			
–	（対応適切なし）	（6a-6.4.4参考）	意図的な情報セキュリティ方針への違反には、直ちに処置をとることが求められる場合がある。	予防に関連記載あり			
7.3	雇用の終了及び変更 管理目的：雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。	6.5	雇用の終了又は変更後の責任 管理策 雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、施行し、関連する要員及びその他の利害関係者に伝達する。 目的 雇用又は契約を変更又は終了する手続の一部として、組織の利益を保護するため。		6.5	雇用の終了又は変更後の責任 統制目標：雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、施行し、関連する要員及びその他の利害関係者に伝達する。 目的：雇用又は契約を変更又は終了する手続の一部として、組織の利益を保護するため。	
7.3.1	雇用の終了又は変更に関する責任 雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、その従業員又は契約相手に伝達し、かつ、遂行させる。						
7.3.1.1	雇用の終了に関する責任の伝達には、実施中の情報セキュリティ要求事項及び法的責任、並びに適切であれば、従業員又は契約相手の、雇用の終了以降の一定期間継続する、秘密保持契約及び雇用条件に規定された責任を含める。	6a-6.5.1	雇用の終了又は変更を管理する手続では、終了又は変更後にこの情報セキュリティの責任及び義務を引き続き有効とするかを定め、関連する要員及びその他の利害関係者に伝達する。	予防に関連記載あり	6.5.1	雇用終了又は変更時にこの情報セキュリティの責任及び義務を引き続き有効とするかを定め、関連する要員及びその他の利害関係者に伝達する。	雇用の終了又は変更を管理する手続では、終了又は変更後にこの情報セキュリティの責任及び義務を引き続き有効とすることが望ましいかを定める。 雇用の終了又は変更後の情報セキュリティの責任及び義務に、情報の秘密保持、知的財産及び取扱いたその他の知識、並びにその他の秘密保持契約に含まれる責任を含める（6.6参照）。
–	（対応適切なし）	6a-6.5.2	雇用の終了又は変更後の情報セキュリティの責任及び義務に、情報の秘密保持、知的財産及び取扱いたその他の知識、並びにその他の秘密保持契約に含まれる責任を含める。	予防に関連記載あり			
7.3.1.2	雇用の終了後も引き続き有効な責任及び義務は、従業員又は契約相手の雇用条件に含める。	6a-6.5.3	雇用又は契約の終了後も引き続き有効な責任及び義務は、その個人の雇用条件、契約又は合意に含める。	管理策に関連記載あり	6.5.2	雇用の終了又は変更後も引き続き有効な情報セキュリティの責任及び義務は、その個人（外部の要員を含む）の雇用条件、契約又は合意に含める。	雇用又は契約の終了後も引き続き有効な責任及び義務は、その個人の雇用条件（6.2参照）、契約又は合意に含める。個人の雇用の終了後、定められた期間継続するその他の契約又は合意も、情報セキュリティの責任を含む場合がある。 雇用の終了又は変更の手順は、供給者の変更、供給者との契約若しくは組織のその他の手順が生じる場合、又は組織内で仕事の変更がある場合に、外部の要員（すなわち、供給者）にも適用する。 責任又は雇用の変更は、現在の責任又は雇用の終了と新しい責任又は雇用の開始との組合せとして管理する。 職務を去る又は職務が変わる個人が、情報セキュリティの役割及び責任を特定し、別の個人に移す。 変更及び雇用の手順を要員、その他の利害関係者及び関連する連絡先担当者に（例えば、顧客及び供給者に）伝達するための手順を確立する。
–	（対応適切なし）	（6a-6.5.3参考）	個人の雇用の終了後、定められた期間継続するその他の契約又は合意も、情報セキュリティの責任を含む場合がある。	予防に関連記載あり			
7.3.1.3	責任又は雇用の変更は、現在の責任又は雇用の終了と新しい責任又は雇用の開始との組合せとして管理する。	6a-6.5.4	責任又は雇用の変更は、現在の責任又は雇用の終了と新しい責任又は雇用の開始との組合せとして管理する。	予防に関連記載あり			
–	（対応適切なし）	6a-6.5.5	職務を去る又は職務が変わる個人が、情報セキュリティの役割及び責任を特定し、別の個人に移す。	予防に関連記載あり			
–	（対応適切なし）	6a-6.5.6	変更及び雇用の手順を要員、その他の利害関係者及び関連する連絡先担当者に伝達するための手順を確立する。	予防に関連記載あり			
–	（対応適切なし）	6a-6.5.7	雇用の終了又は変更の手続は、供給者の要員、供給者との契約、又は組織との仕事の終了が生じる場合、又は組織内で仕事の変更がある場合に、外部の要員（すなわち、供給者）にも適用する。	予防に関連記載あり			
8.1	資産に対する責任 管理目的：組織の資産を特定し、適切な保護の責任を定めるため。	5.9	情報及びその他の関連資産の目録 管理策 情報及びその他の関連資産の目録を、それぞれの管理責任者を含めて作成し、維持する。 目的 組織の情報及びその他の関連資産を特定し、それらの情報セキュリティを維持し、適切な管理責任を割り当てるため。		5.9	情報及びその他の関連資産の目録 統制目標：情報及びその他の関連資産の目録を、それぞれの管理責任者を含めて作成し、維持する。 目的：組織の情報及びその他の関連資産を特定し、それらの情報セキュリティを維持し、適切な管理責任を割り当てるため。	
8.1.1	資産目録 情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持する。						
8.1.1.1	組織は、情報のライフサイクルに関連した資産を特定し、その重要度を文書化する。	Sb-5.9.1	組織は、情報及びその他の関連資産を特定し、情報セキュリティの観点からそれらの重要度を決定する。	予防に関連記載あり	5.9.1	情報及びその他の関連資産の目録を作成し、維持する。	文書は、必要に応じて専用の目録又は既存の目録として維持する。 情報及びその他の関連資産は、正確で、最新に保たれ、一貫性があり、他の目録と整合している、情報及びその他の関連資産の目録の正確性を確実にするための選択肢は次のものを含む。 a）資産目録に関与して、特定した情報及びその他の関連資産の定期的なレビューを実施する。 b）資産の設置、変更又は除去のプロセスにおいて目録の更新を自動的に適用する。 資産の場所を、必要に応じて目録に含める。 目録は、情報及びその他の関連資産の(単一の)リストである必要はない。目録は組織において関係する機能が維持することが望ましいことを考える、情報資産、ハードウェア、ソフトウェア、仮想マシン（VM）、施設、要員、力量、機能及び/又は類似の目録などの、動的な目録の集まりをどこが可能である。 資産度は、それに関係する情報の分類に従って分類する（5.12参照）。 情報及びその他の関連資産の目録の維持は、組織のニーズに適したレベルである。資産の性質上、情報のライフサイクルにおいて資産が特定のインスタンスが文書化できない場合がある。短期間だけ存続する資産の例として、ライフサイクル内にVMインスタンスがある。 情報及びその他の関連資産のそれぞれに対し、情報セキュリティの観点から重要度を決定する。 特定した情報及び資産の分類（5.12参照）を決定する。
8.1.1.2	情報のライフサイクルには、作成、処理、保管、送信、消去及び破棄を含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応適切なし）	–
8.1.1.3	文書は、専用の目録又は既存の目録として維持する。	Sb-5.9.2	文書は、必要に応じて専用の目録又は既存の目録として維持する。	予防に関連記載あり	5.9.1	【再】情報及びその他の関連資産の目録を作成し、維持する。	（5.9.1に対応する語を参照）
8.1.1.4	資産目録は、正確で、最新に保たれ、一貫性があり、他の目録と整合していることを確実にする仕組みを整備する。	Sb-5.9.3	情報及びその他の関連資産は、正確で、最新に保たれ、一貫性があり、他の目録と整合している。情報及びその他の関連資産の目録の正確性を確実にするための選択肢は次のものを含む。 a）資産目録に関与して、特定した情報及びその他の関連資産の定期的なレビューを実施する。 b）資産の設置、変更又は除去のプロセスにおいて目録の更新を自動的に適用する。	予防に関連記載あり			
–	（対応適切なし）	Sb-5.9.4	資産の場所を、必要に応じて目録に含める。	予防に関連記載あり			
–	（対応適切なし）	（Sb-5.9参考）	目録は、情報及びその他の関連資産の(単一の)リストである必要はない。目録は組織において関係する機能が維持することが望ましいことを考える、情報資産、ハードウェア、ソフトウェア、仮想マシン（VM）、施設、要員、力量、機能及び/又は類似の目録などの、動的な目録の集まりをどこが可能である。	予防に関連記載あり			
–	（対応適切なし）	Sb-5.9.5	各資産は、それに関係する情報の分類に従って分類する。	予防に関連記載あり			
–	（対応適切なし）	Sb-5.9.6	情報及びその他の関連資産の目録の粒度は、組織のニーズに適したレベルである。	予防に関連記載あり			
–	（対応適切なし）	（Sb-5.9.6参考）	資産の性質上、情報のライフサイクルにおいて資産の特定のインスタンスが文書化できない場合がある。短期間だけ存続する資産の例として、ライフサイクル内にVMインスタンスがある。	予防に関連記載あり			
8.1.1.5	特定された各資産について、管理責任者を割り当て、分類する。	Sb-5.9.7	特定した情報及びその他の関連資産について、各々の資産の管理責任を個人又はグループに割り当てて、それ上で分類を特定する。	予防に関連記載あり	5.9.2	情報及びその他の関連資産の責任を明確にし、管理責任を個人又はグループに割り当てる。	特定した情報及びその他の関連資産について、各々の資産の管理責任を個人又はグループに割り当て、それとで分類を特定する（5.12及び5.13参照）。 資産の管理責任を時機を失せずに割り当てることを確実にするための7プロセスを実施する。 資産を生成した時点、又は資産を組織に移転した時点で、管理責任を割り当てる。 現在の資産の管理責任者が職務を離れる又は変わる場合は、必要に応じて資産の管理責任を再割り当てする。 資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理するごとに責任を負う。 a）情報及びその他の関連資産の目録を作成する。 b）情報及びその他の関連資産を適切に分類し、保護する。 c）分類を定期的にレビューする。 d）データベース、ストレージ、ソフトウェアの構成要素、サブ構成要素など、採術資産の構成要素を一覧表示し、ひも（紐）付ける。 e）情報及びその他の関連資産の許容される利用に関する要求事項（5.10参照）を確立する。 f）アクセス制限が分類に対応し、有効であり、これを定期的にレビューする。 g）情報及びその他の関連資産は、削除又は破棄する場合、セキュリティに配慮した方法で処理し、目録から削除する。 h）資産の管理責任者が、資産に関連するリスクの特定及びマネジメントに関与する。 i）資産の管理責任者が、情報を管理する役割及び責任をもつ要員を支援する。
8.1.1.6.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の出典）	5.9.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
8.1.2	資産の管理責任 目録の中で維持される資産は、管理する。	5.9	情報及びその他の関連資産の目録 管理策 情報及びその他の関連資産の目録を、それぞれの管理責任者を含めて作成し、維持する。 目的 組織の情報及びその他の関連資産を特定し、それらの情報セキュリティを維持し、適切な管理責任を割り当てるため。		5.9	情報及びその他の関連資産の目録 統制目標：情報及びその他の関連資産の目録を、それぞれの管理責任者を含めて作成し、維持する。 目的：組織の情報及びその他の関連資産を特定し、それらの情報セキュリティを維持し、適切な管理責任を割り当てるため。	
8.1.2.1	資産の管理責任を時機を失せずに割り当てることを確実にするための7プロセスにおいて、資産が生成された時点、又は資産が組織に移転された時点で、適格な者（資産のライフサイクルの管理責任を与えられた個人及び組織）に管理責任を割り当てる。	Sb-5.9.8	資産の管理責任を時機を失せずに割り当てることを確実にするための7プロセスを実施する。	予防に関連記載あり	5.9.2	【再】情報及びその他の関連資産の責任を時機に、管理責任を個人又はグループに割り当てる。	（5.9.2に対応する語を参照）
8.1.2.1	【再】資産の管理責任を時機を失せずに割り当てることを確実にするための7プロセスにおいて、資産が生成された時点、又は資産が組織に移転された時点で、適格な者（資産のライフサイクルの管理責任を与えられた個人及び組織）に管理責任を割り当てる。	Sb-5.9.9	資産を生成した時点、又は資産を組織に移転した時点で、管理責任を割り当てる。	予防に関連記載あり			
–	（対応適切なし）	Sb-5.9.10	現在の資産の管理責任者が職務を離れる又は変わる場合は、必要に応じて資産の管理責任を再割り当てする。	予防に関連記載あり			
8.1.2.2	資産の管理責任者は、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。	Sb-5.9.11	資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。 b）資産の管理責任者が、資産に関連するリスクの特定及びマネジメントに関与する。 i）資産の管理責任者が、情報を管理する役割及び責任をもつ要員を支援する。	予防に関連記載あり			
8.1.2.3	資産の管理責任者は、資産の目録を作成し、維持する仕組みを整備する。	Sb-5.9.11	資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。 a）情報及びその他の関連資産の目録を作成する。	予防に関連記載あり			
8.1.2.4	資産の管理責任者は、資産を適切に分類及び保護する仕組みを整備する。	Sb-5.9.11	資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。 b）情報及びその他の関連資産を適切に分類し、保護する。	予防に関連記載あり			
8.1.2.5	資産の管理責任者は、適用されるアクセス制御方針を考慮に入れて、重要な資産に対するアクセスの制限及び分類を定め、定期的にレビューする。	Sb-5.9.11	資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。 c）分類を定期的にレビューする。 d）データベース、ストレージ、ソフトウェアの構成要素、サブ構成要素など、採術資産の構成要素を一覧表示し、ひも（紐）付ける。 e）情報及びその他の関連資産の許容される利用に関する要求事項を確立する。 f）アクセス制限が分類に対応し、有効であり、これを定期的にレビューする。	予防に関連記載あり			
8.1.2.6	資産の管理責任者は、資産を消去又は破壊する場合に、適切に取り扱う仕組みを整備する。	Sb-5.9.11	資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。 g）情報及びその他の関連資産は、削除又は破棄する場合、セキュリティに配慮した方法で処理し、目録から削除する。	予防に関連記載あり			
8.1.2.7.PB	クラウドサービス事業者は、クラウドサービス利用者に対し、当該利用者の資産（バックアップを含む）を管理するため、次のいずれかを提供する。 (a)当該利用者の管理する資産を、記録媒体に記録する（バックアップを含む）前に暗号化し、当該利用者が暗号鍵を管理し消去する機能 (b)当該利用者が、当該利用者の管理する資産を記録媒体に記録する（バックアップを含む）前に暗号化し、暗号鍵を管理し消去する機能を実装するために必要となる情報	–	（統一基準由来）	管理策に関連記載あり（情報セキュリティ管理基準以外の出典）	8.13.S	クラウドサービス利用者に対し、当該利用者の資産（バックアップを含む）を管理するため、次のいずれかを提供する。 a）当該利用者の管理する資産を、記録媒体に記録する（バックアップを含む）前に暗号化し、当該利用者が暗号鍵を管理し消去する機能 b）当該利用者が、当該利用者の管理する資産を記録媒体に記録する（バックアップを含む）前に暗号化し、暗号鍵を管理し消去する機能を実装するために必要となる情報	特になし。
8.1.3	資産利用の許容範囲 情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施する。	5.10	情報及びその他の関連資産の許容される利用 管理策 情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は、明確にし、文書化し、実施する。 目的 情報及びその他の関連資産を適切に保護し、利用し、取り扱うことを確実にするため。		5.10	情報及びその他の関連資産の許容される利用 統制目標：情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は、明確にし、文書化し、実施する。 目的：情報及びその他の関連資産を適切に保護し、利用し、取り扱うことを確実にするため。	
8.1.3.1	組織の資産を利用する又はアクセスする従業員及び外部の利用者に対し、組織における情報や情報処理施設に関連する資産あるいは資産に関するセキュリティ要求事項について、認識させる。	Sb-5.10.1	組織の情報及びその他の関連資産を利用する、又はそれらにアクセスする要員及び外部の利用者に対し、情報及びその他の関連資産を保護し、取り扱うための情報セキュリティ要求事項を認識させる。	予防に関連記載あり	5.10.1	情報及びその他の関連資産の許容される利用に関する方針を策定する。	組織の情報及びその他の関連資産を利用する、又はそれらにアクセスする要員及び外部の利用者に対し、情報及びその他の関連資産を保護し、取り扱うための情報セキュリティ要求事項を認識させる。 要員及び外部の利用者は、どのような情報処理施設・設備の利用に対しても、責任をもつ。 組織は、情報及びその他の関連資産の許容される利用に関するトピック固有の方針を確立し、情報及びその他の関連資産を利用する又は取り扱う全ての人にそれを伝達する。 許容される利用に関するトピック固有の方針では、個人に期待する情報及びその他の関連資産の利用方法について、明確に指示する。
8.1.3.2	従業員及び外部の利用者は、どのような情報処理資源の利用に対しても、また、利用者自身の責任の下で行うにいかなる利用に対しても、責任をもつ。	Sb-5.10.2	要員及び外部の利用者は、どのような情報処理施設・設備の利用に対しても、責任をもつ。	予防に関連記載あり			

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
–	（対応項なし）	Sb-S.10.3	組織は、情報及びその他の関連資産の許容される利用に関するトピック固有の方針を確立し、情報及びその他の関連資産を利用する又は取り扱う全ての人にそれを伝達する。	予防に関連記載あり			トピック固有の方針には、次の事項を記載する。 a) 情報セキュリティの観点から見た、個人に期待する好ましい行動 b) 情報及びその他の関連資産について許可する利用及び禁止する利用 c) 組織が実行している監視活動
–	（対応項なし）	Sb-S.10.4	許容される利用に関するトピック固有の方針では、個人に期待する情報及びその他の関連資産の利用方法に、明確に指示をする。	予防に関連記載あり			
–	（対応項なし）	Sb-S.10.5	トピック固有の方針には、次の事項を記載する。 a) 情報セキュリティの観点から見た、個人に期待する好ましい行動 b) 情報及びその他の関連資産について許可する利用及び禁止する利用 c) 組織が実行している監視活動	予防に関連記載あり			
8.1.4	資産の返却 全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。	S.11	資産の返却 管理策 要員及び必要に応じてその他の利害関係者は、雇用、契約又は合意の変更又は終了時に、自らが所持する組織の資産の全てを返却する。 目的 雇用、契約、又は合意を変更又は終了するプロセスの一環として、組織の資産を保護するため。		S.11	資産の返却 統制目標：要員及びより必要に応じてその他の利害関係者は、雇用、契約又は合意の変更又は終了時に、自らが所持する組織の資産の全てを返却する。 目的：雇用、契約、又は合意を変更又は終了するプロセスの一環として、組織の資産を保護するため。	
8.1.4.1	雇用の終了時の手続は、前もって支給された物理的及び電子的な資産（組織が管理責任をもつ又は組織に委託されたもの）の全ての返却を含める。	Sb-S.11.1	雇用の変更及び終了時のプロセスは、前もって支給された物理的及び電子的な資産（組織が所有するもの又は組織に預託されたもの）の全ての返却を含めて制定する。	予防に関連記載あり	S.11.1	要員及びその他の利害関係者における雇用の変更及び終了において、前もって支給された全ての物理的及び電子的な資産の返却プロセスを整備し、実施する。	雇用の変更及び終了時のプロセスは、前もって支給された物理的及び電子的な資産（組織が所有するもの又は組織に預託されたもの）の全ての返却を含めて制定する。 要員及びその他の利害関係者が継続中の作業に重要な知識を保有している場合には、その情報を文書化し、組織に引き継ぐ。 要員及びその他の利害関係者が組織の装置・機器を購入する場合、又は個人所有の機器を用いる場合には、予防に従って、全ての関連する情報を返却し、組織に返却し、装置・機器からセキュリティを保って削除することを確実にする。（7.14参照）。 雇用の終了の手続期間中及びそれ以降、組織は、予告を受けた要員が認可を得て関連情報（例えば、知的財産）を複製することを防止する。 組織は、返却する全ての情報及びその他の関連資産を明確に特定し、文書化する。これには、次のものが含まれ得る。 a) エンドポイント機器 b) 可搬型媒体装置 c) 専門機器 d) 情報システム、サイト及び物理的アーカイブ用の認証ハードウェア（例えば、機械式鍵、物理トークン及びスマートカード） e) 情報の物理的な複製
8.1.4.2	従業員及び外部の利用者が組織の設備を購入する場合、又は個人所有の設備を用いる場合には、予期に従って、全ての関連する情報を組織に返却し、設備からセキュリティを保って確実に消去する。	Sb-S.11.2	要員及びその他の利害関係者が組織の装置・機器を購入する場合、又は個人所有の機器を用いる場合には、予期に従って、全ての関連する情報を返却し、組織に返却し、装置・機器からセキュリティを保って削除することを確実にする。	予防に関連記載あり			
8.1.4.3	従業員及び外部の利用者が継続中の作業に重要な知識を保有している場合には、その情報を文書化し、組織に引き継ぐ。	Sb-S.11.3	要員及びその他の利害関係者が継続中の作業に重要な知識を保有している場合には、その情報を文書化し、組織に引き継ぐ。	予防に関連記載あり			
8.1.4.4	雇用の終了の予告期間中は、雇用が終了する従業員及び契約相手が認可を得て関連情報（例えば、知的財産）を複製、削除することのないよう、組織が管理する。	Sb-S.11.4	雇用の終了の予告期間中及びそれ以降、組織は、予告を受けた要員が認可を得て、関連情報を複製することを防止する。	予防に関連記載あり			
–	（対応項なし）	Sb-S.11.5	組織は、返却する全ての情報及びその他の関連資産を明確に特定し、文書化する。	予防に関連記載あり			
–	（対応項なし）	（Sb-S.11.5参考）	これには、次のものが含まれ得る。 a)固定型エンドポイント機器 b)可搬型媒体装置 c)専門機器 d)情報システム、サイト及び物理的アーカイブ用の認証ハードウェア e)情報の物理的な複製	予防に関連記載あり			
8.1.5.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		9.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
8.1.5.1.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.2.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
8.1.5.2.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.2.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
8.1.5.3.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.2.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
8.1.5.4.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	予防に関連記載あり（情報セキュリティ管理基準以外の由来）	9.2.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
8.2 8.2.1	情報分類 管理目的：組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。 情報の分類 情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類する。	S.12	情報の分類 管理策 組織は、情報の分類に関するトピック固有の方針を確立し、それを全ての関連する利害関係者に伝達する。 目的 組織における情報の重要度に従って、情報の保護のニーズを特定し、理解することを確実にするため。		S.12	情報の分類 統制目標：情報は、機密性、完全性、可用性及び関連する利害関係者の要求事項に基づく組織の情報セキュリティのニーズに従って分類する。 目的：組織における情報の重要度に従って、情報の保護のニーズを特定し、理解することを確実にするため。	
–	（対応項なし）	Sb-S.12.1	組織は、情報の分類に関するトピック固有の方針を確立し、それを全ての関連する利害関係者に伝達する。	予防に関連記載あり	S.12.1	情報の分類や分類体系に関する方針を策定し、分類する。	組織は、情報の分類に関するトピック固有の方針を確立し、それを全ての関連する利害関係者に伝達する。 組織は、分類体系において、機密性、完全性及び可用性の要求事項を考慮する。 情報の分類及び関連する保護管理策では、情報を共有又は制限するため、情報の完全性を保護するため、及び可用性を保証するための事業上のニーズ、並びに情報の機密性、完全性及び可用性に関する法的要求事項を考慮する。 情報には、分類体系において、機密性、完全性及び可用性の要求事項を考慮する。又は他の形で扱う際に、又は保護する情報の分類に応じて分類するニーズが可能である。 情報の管理責任者は、その情報の分類に対してカウンセリングを行う。 分類体系には、分類の周期及びその分類を後にレビューするための基準を含める。 分類の結果は、ライフサイクルを通じた情報の価値、取扱いに慎重を要する度合い、及び重要度の変化に従って更新する。 分類体系は、アクセス制御に関するトピック固有の方針（5.1参照）と整合していて、組織のそれぞれの事業上のニーズに対応できる。 分類は、情報の侵害が組織に与える影響のレベルによって決定することが可能である。分類体系で定義されたそれぞれのレベルには、分類体系の適用において意味をなす名称を付ける。 分類体系は、全員が情報及び関連する資産の分類の適用を同じ方法で分類できるよう、組織全体にわたって一貫し、組織の文脈に含まれている。これによって、全員が保護に関する要求事項について共通した理解をもち、適切な保護を適用できるようになる。 情報共有を含む他の組織との合意は、他の組織から共有された情報の分類を特定し、分類レベルを解釈するための手順を含む。組織内で使用する分類体系は、レベルの名称が異なっている場合でも、他の組織で使用する体系と異なる可能性がある。さらに、組織間で移動する情報は、分類体系が同じであっても、各組織の状況に依存して分類が異なる場合がある。異なる体系間の対応は、情報について同等の取扱い及び保護方法を探すことによって決定することが可能である。
8.2.1.1	情報の分類及び関連する保護管理策には、情報を共有又は制限する業務上の要求、及び法的要求事項を含める。	Sb-S.12.3	情報の分類及び関連する保護管理策では、情報を共有又は制限するため、情報の完全性を保護するため、及び可用性を保証するための事業上のニーズ、並びに情報の機密性、完全性及び可用性に関する法的要求事項を考慮する。	予防に関連記載あり			
8.2.1.2	情報資産の管理責任者は、その情報の分類に対して責任を負う。	Sb-S.12.4	情報の管理責任者は、その情報の分類に対してアカウンタビリティを負う。	予防に関連記載あり			
8.2.1.3	情報の分類体系には、分類の周期及びその分類を時間が経つてからレビューするための基準を含める。	Sb-S.12.5	分類体系には、分類の周期及びその分類を後にレビューするための基準を含める。	予防に関連記載あり			
8.2.1.4	情報の分類体系における保護レベルは、対象とする情報についての機密性、完全性、可用性及びその他の特性を分析することによって評価する。	Sb-S.12.2	組織は、分類体系において、機密性、完全性及び可用性の要求事項を考慮する。	予防に関連記載あり			
8.2.1.5	情報の分類体系は、アクセス制御方針と整合させる。	Sb-S.12.7	分類体系は、アクセス制御に関するトピック固有の方針と整合していて、組織のそれぞれの事業上のニーズに対応できる。	予防に関連記載あり			
8.2.1.6	情報の分類体系におけるそれぞれの保護レベルには、分類体系の適用において意味をなすような名称を付ける。	Sb-S.12.8	分類は、情報の侵害が組織に与える影響のレベルによって決定することが可能である。分類体系で定義されたそれぞれのレベルには、分類体系の適用において意味をもつ名称を付ける。	予防に関連記載あり			
8.2.1.7	情報の分類体系は、組織全体にわたって一貫せず、全員が情報及び関連する資産を同じ方法で分類し、保護に関する要求事項について共通した理解をもち、適切な保護を適用できるようにする。	（Sb-S.12.9参考）	これによって、全員が保護に関する要求事項について共通した理解をもち、適切な保護を適用できるようにな。	予防に関連記載あり			
8.2.1.8	情報の分類は、組織の万物ネに当ホ、組織全体にわたって一貫した論理的なものとする。	Sb-S.12.9	分類体系は、全員が情報及び関当するその他の関連資産を同じ方法で分類できるよう、組織全体にわたって一貫し、組織の手順に含まれている。	予防に関連記載あり			
–	（対応項なし）	Sb-S.12.10	情報共有を含む他の組織との合意は、他の組織から共有された情報の分類を特定し、分類レベルを解釈するための手順を含む。	予防に関連記載あり			
8.2.1.9	情報の分類の結果は、組織にとっての取扱いに慎重を要する度合い及び重要性（例えば、機密性、完全性、可用性）に応じた資産の価値を含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で規定外だ）	–	（対応項なし）	–
8.2.1.10	情報の分類の結果は、ライフサイクルを通じた、情報の価値、取扱いに慎重を要する度合い及び重要性の変化に応じて、更新する。	Sb-S.12.6	分類の結果は、ライフサイクルを通じた情報の価値、取扱いに慎重を要する度合い、及び重要度の変化に従って分類の更新を行う。	予防に関連記載あり	S.12.2	分類の結果は、ライフサイクルを通じた情報の価値、取扱いに慎重を要する度合い、及び重要度の変化に従って分類の決定者や責任者に確認し、定期的に見直し更新する。	特になし。
8.2.2	情報のラベル付け 情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施する。	S.13	情報のラベル付け 管理策 情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施する。 目的 情報の分類の伝達を容易にし、情報の処理及び管理の自動化を支援するため。		S.13	情報のラベル付け 統制目標：情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施する。 目的：情報の分類の伝達を容易にし、情報の処理及び管理の自動化を支援するため。	
8.2.2.1	情報のラベル付けに関する手順は、物理的形式及び電子的形式の情報及び関連する資産に適用できるようにする。	Sb-S.13.1	情報のラベル付けに関する手順は、あらゆる形式の情報及びその他の関連資産に適用できるものである。	予防に関連記載あり	S.13.1	情報の分類体系を反映し上情報のラベル付けに関する手順を整備し、ラベル付けを実施する。	情報のラベル付けに関する手順は、あらゆる形式の情報及びその他の関連資産に適用できるものである。ラベル付けは、5.12で確立した分類体系を反映している。 ラベルは、容易に認識できる。 情報のラベル付けに関する手順では、記憶媒体の種類に応じて、情報がどのようにアクセスされ少又は資産がどのように取り扱われるかを考慮して、ラベルを添付する場所及びその添付方法に関する手引を示す。手順では、次の事項を定めることが可能である。 a) ラベル付けを省略する場合（例えば、作業負荷を減らすため、秘密でない情報のラベル付け） b) 電子的取り扱いが物理的手段、又はその他の形式で活供又は保存される情報のラベル付けの方法 c) ラベル付けが不可能な場合（例えば、技術的制約のため）の取扱いの方法 ラベル付け手法の例は次のものを含む。 a) 物理的ラベル b) ヘッダ及びフッタ c) メタデータ d) 透かし e) ゴムスタンプ ディジタル情報は、特に機密性に関して、情報を特定し、管理し、制御するために、メタデータを活用する。メタデータは、付加した分類ラベルに基づいて、複数のシステムが連携し、決定を下すことを容易にする。 手順には、組織の情報モデル及びICTアーキテクチャに沿って、情報にメタデータをどのように付けるか、どのラベルを使用するか、及びデータをどのように取り扱うことが望ましいかを記載する。 システムが情報をその情報セキュリティ特性に応じて処理するとき、関係する追加のメタデータをシステムで付加する。 要員及びその他の利害関係者に、ラベル付けに関する手順を認識させる。情報に正しくラベルを付け、それに応じて取り扱うことを確実にするために、全ての要員に必要な訓練を提供する。
–	（対応項なし）	Sb-S.13.2	情報のラベル付けは、S.12で確立した分類体系を反映している。	予防に関連記載あり			
8.2.2.3	情報のラベルは、容易に認識できるようにする。	Sb-S.13.3	情報のラベルは、容易に認識できる。	予防に関連記載あり			
8.2.2.4	情報のラベル付けに関する手順では、媒体の種類に応じて、情報がどのようにアクセスされるか又は資産がどのように取り扱われるかを考慮して、ラベルを添付する場所及びその添付方法に関する手引 を示す。	Sb-S.13.4	情報のラベル付けに関する手順では、記憶媒体の種類に応じて、情報がどのようにアクセスされるか又は資産がどのように取り扱われるかを考慮して、ラベルを添付する場所及びその添付方法に関する手引を示す。	予防に関連記載あり			
–	（対応項なし）	（Sb-S.13参考1）	手順では、次の事項を定めることも可能である。 a) ラベル付けを省略する場合 b) 電子的取り扱いが物理的手段、又はその他の形式で活供又は保存される情報のラベル付けの方法 c) ラベル付けが不可能な場合の取扱いの方法	予防に関連記載あり			
–	（対応項なし）	（Sb-S.13参考2）	ラベル付け手法の例は次のものを含む。 a) 物理的ラベル b) ヘッダ及びフッタ c) メタデータ d) 透かし e) ゴムスタンプ	予防に関連記載あり			
–	（対応項なし）	Sb-S.13.5	ディジタル情報は、特に機密性に関して、情報を特定し、管理し、制御するために、メタデータを活用する。	予防に関連記載あり			
–	（対応項なし）	Sb-S.13.6	メタデータは、情報の効率的かつ正確な検索を可能にする。	予防に関連記載あり			
–	（対応項なし）	Sb-S.13.7	メタデータは、付加した分類ラベルに基づいて、複数のシステムが連携し、決定を下すことを容易にする。	予防に関連記載あり			
–	（対応項なし）	Sb-S.13.8	手順には、組織の情報モデル及びICTアーキテクチャに沿って、情報にメタデータをどのように付けるか、どのラベルを使用するか、及びデータをどのように取り扱うことが望ましいかを記載する。	予防に関連記載あり			
–	（対応項なし）	Sb-S.13.9	システムが情報をその情報セキュリティ特性に応じて処理するとき、関係する追加のメタデータをシステムで付加する。	予防に関連記載あり			
8.2.2.5	従業員及び契約相手に、情報のラベル付けに関する手順を認識させる。	Sb-S.13.10	要員及びその他の利害関係者に、ラベル付けに関する手順を認識させる。	予防に関連記載あり			
–	（対応項なし）	Sb-S.13.11	情報に正しくラベルを付け、それに応じて取り扱うことを確実にするために、全ての要員に必要な訓練を提供する。	予防に関連記載あり			
8.2.2.6	取扱いに慎重を要する又は重要と分類され情報を含むシステム出力には、適切な分類ラベルを付ける。	Sb-S.13.12	取扱いに慎重を要する又は重要と分類され情報を含むシステム出力には、適切な分類ラベルを付ける。	予防に関連記載あり			
8.2.7.7.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	S.13.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
8.2.3	資産の取扱い 資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施する。	5.10	情報及びその他の関連資産の許容される利用 管理策 情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は、明確にし、文書化し、実施する。 目的 情報及びその他の関連資産を適切に保護し、利用し、取り扱うことを確実にするため。		5.10	情報及びその他の関連資産の許容される利用 統制目標：情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は、明確にし、文書化し、実施する。 目的：情報及びその他の関連資産を適切に保護し、利用し、取り扱うことを確実にするため。	
8.2.3.1	情報を分類に従って取り扱い、処理し、保管し、伝達するための手順を作成する。	Sb-S.10.6	許容される利用の手順は、情報の分類及び特定したリスクに従って、情報のライフサイクル全体にわたって立案する。	干引に関連記載あり	5.10.2	情報及びその他の関連資産の許容される利用に関する規則及び取扱手順を整備し、実施する。	許容される利用の手順は、情報の分類（5.12参照）及び特定したリスクに従って、情報のライフサイクル全体にわたって立案する。 許容される利用の手順の立案においては、次の項目を考慮する。 a) 分類のレベルに応じた保護の要求事項に対応するアクセス制限（5.12参照） b) 情報及びその他の関連資産の認可された利用者についての、記録の維持 c) 情報の一時的又は恒久的な複製についての、情報の原本の保護と整合性のあるレベルでの保護 d) 情報に関連する資産の、製造業者の仕様に従った保管（7.8参照） e) 記憶媒体（電子的又は物理的な）の全ての複製についての、認可された受領者の注意をひくような明確な表示（7.10参照） f) 情報及びその他の関連資産の破棄、並びにサポートされている削除方法の認可（8.10参照）
8.2.3.2	情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、各レベルの分類に応じた保護の要求事項に対応するアクセス制限に関する手順を含める。	Sb-S.10.7	許容される利用の手順の立案においては、次の項目を考慮する。 a) 分類のレベルに応じた保護の要求事項に対応するアクセス制限	干引に関連記載あり			
8.2.3.3	情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、資産の認可された受領者についての、正式な記録を維持するための手順を含める。	Sb-S.10.7	許容される利用の手順の立案においては、次の項目を考慮する。 b) 情報及びその他の関連資産の認可された利用者についての、記録の維持	干引に関連記載あり			
8.2.3.4	情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、情報の一時的又は恒久的な複製について、情報の原本と同等のレベルで保護するための手順を含める。	Sb-S.10.7	許容される利用の手順の立案においては、次の項目を考慮する。 c) 情報の一時的又は恒久的な複製についての、情報の原本の保護と整合性のあるレベルでの保護	干引に関連記載あり			
8.2.3.5	情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、IT 資産について、製造業者の仕様に従って保管するための手順を含める。	Sb-S.10.7	許容される利用の手順の立案においては、次の項目を考慮する。 d) 情報に関連する資産の、製造業者の仕様に従った保管	干引に関連記載あり			
8.2.3.6	情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、媒体の全ての複製について、認可された受領者の注意をひくよう明確な印を付けるための手順を含める。	Sb-S.10.7	許容される利用の手順の立案においては、次の項目を考慮する。 e) 記憶媒体（電子的又は物理的な）の全ての複製についての、認可された受領者の注意をひくような明確な表示	干引に関連記載あり			
8.2.3.7	他組織との情報共有を含む合意には、その情報の分類を特定し、他組織からの又は他組織への分類ラベル及びアクセス制限の解釈を伝達するための手順（並びにその解釈を支援する手順）を含める。	Sb-S.12.10	情報共有を含む他の組織との合意は、他の組織から共有された情報の分類を特定し、分類レベルを解釈するための手順を含む。	干引に関連記載あり	5.12.1	【再】情報の分類や分類体系に関する方針を策定し、分類する。	（5.12.1に対応する項を参照）
8.3	媒体の取扱い 管理目的：媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。	7.10	記憶媒体 管理策 記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理する。 目的 記憶媒体上の情報に対して認可された開示、変更、移動又は破壊だけがなされることを確実にするため。		7.10	記憶媒体 統制目標：記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理する。 目的：記憶媒体上の情報に対して認可された開示、変更、移動又は破壊だけがなされることを確実にするため。	
8.3.1	取外し可能な媒体の管理 組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施する。						
8.3.1.1	取外し可能な媒体の管理のために、再利用可能な媒体を組織から移動する場合に、その内容が以後不要であるならば、これを復元不能とする。	7b-7.10.1	取外し可能な記憶媒体の管理において、次の事項を考慮する。 a) 取外し可能な記憶媒体の管理に関するトピック固有の方針を確立し、取外し可能な記憶媒体を使用する又は取り扱う全ての人にトピック固有の方針を伝達する。	干引に関連記載あり	7.10.1	取外し可能な記憶媒体の管理に関する方針を策定し、管理する。	取外し可能な記憶媒体の管理において、次の事項を考慮する。 a) 取外し可能な記憶媒体の管理に関するトピック固有の方針を確立し、取外し可能な記憶媒体を使用する又は取り扱う全ての人にトピック固有の方針を伝達すること。 b) 必要かつ実施可能な場合には、組織から記憶媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持すること。 c) 全ての記憶媒体は、情報の分類に従って安全でセキュリティが保たれた環境に保管し、製造業者の仕様に従って、環境の脅威（熱、水分、湿度、電磁、経年劣化など）から保護すること。 d) 情報の機密性又は完全性が重要な考慮事項である場合は、取外し可能な記憶媒体上の情報を保護するために、暗号技術を用いること。 e) 保管した情報が正必要な間に記憶媒体が劣化するリスクを軽減するため、読み出せなくなる前に情報を新しい記憶媒体に移し替えること。 f) 複数の価値ある情報は、一斉に損失するリスクを減らすために、複数の複製を別の記憶媒体に保管すること。 g) 情報を失う危険性を小さくするために、取外し可能な記憶媒体の登録を検討すること。 h) 取外し可能な記憶媒体のポート（例えば、セキュアデジタル（SD）カードコネクタ又はユニバーサルシリアルバス（USB）ポート）は、組織にその利用について理由があるときにだけ有効とすること。 i) 取外し可能な記憶媒体を用いる必要がある場合、そのような記憶媒体への情報の転送を監視すること。 j) 情報は、物理的な輸送中、例えば、郵便サービス又は宅配便で記憶媒体を送る場合に、認可されていないアクセス、不正使用又は破損に関して守り切れる可能性がある。 媒体は組の交差を含んでいる、物理的記憶媒体を輸送する場合には、5.14のセキュリティ対策を適用する。
8.3.1.2	取外し可能な媒体の管理のために、必要かつ実際的な場合には、組織から移動する媒体について、認可を要求する。	7b-7.10.1	取外し可能な記憶媒体の管理において、次の事項を考慮する。 b) 必要かつ実施可能な場合には、組織から記憶媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する。	干引に関連記載あり			
8.3.1.3	取外し可能な媒体の管理のために、組織から移動する媒体について、監査証跡の維持のために記録を保管する。	7b-7.10.1	【再】取外し可能な記憶媒体の管理において、次の事項を考慮する。 b) 必要かつ実施可能な場合には、組織から記憶媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する。	干引に関連記載あり			
8.3.1.4	取外し可能な媒体の管理のために、全ての媒体は、製造業者の仕様に従って、安全でセキュリティが保たれた環境に保管する。	7b-7.10.1	取外し可能な記憶媒体の管理において、次の事項を考慮する。 c) 全ての記憶媒体は、情報の分類に従って安全でセキュリティが保たれた環境に保管し、製造業者の仕様に従って、環境の脅威（熱、水分、湿度、電磁、経年劣化など）から保護する。	干引に関連記載あり			
8.3.1.5	取外し可能な媒体の管理において、データの機密性又は完全性が重要な考慮事項である場合は、取外し可能な媒体上のデータを保護するために、暗号技術を用いる。	7b-7.10.1	取外し可能な記憶媒体の管理において、次の事項を考慮する。 d) 情報の機密性又は完全性が重要な考慮事項である場合は、取外し可能な記憶媒体上の情報を保護するために、暗号技術を用いる。	干引に関連記載あり			
8.3.1.6	取外し可能な媒体の管理において、保管されたデータが正必要な間に媒体が劣化するリスクを軽減するため、読み出せなくなる前にデータを新しい媒体に移動する。	7b-7.10.1	取外し可能な記憶媒体の管理において、次の事項を考慮する。 e) 保管した情報が正必要な間に記憶媒体が劣化するリスクを軽減するため、読み出せなくなる前に情報を新しい記憶媒体に移し替えること。	干引に関連記載あり			
8.3.1.7	取外し可能な媒体の管理において、価値の高いデータは、一斉に損失又は消失するリスクを上げ低減するために、複数の複製を別の媒体に保管する。	7b-7.10.1	取外し可能な記憶媒体の管理において、次の事項を考慮する。 f) 価値の高い情報は、一斉に損失又は消失するリスクを上げ低減するために、複数の複製を別の記憶媒体に保管すること。	干引に関連記載あり			
8.3.1.8	取外し可能な媒体の管理において、データ消失の危険性を小さくするために、取外し可能な媒体の登録を含める。	7b-7.10.1	取外し可能な記憶媒体の管理において、次の事項を考慮する。 g) 情報を失う危険性を小さくするために、取外し可能な記憶媒体の登録を検討する。	干引に関連記載あり			
8.3.1.9	取外し可能な媒体の管理のために、取外し可能な媒体がドライブ上の利用のための業務上の理由がある者にだけ有効とする。	7b-7.10.1	取外し可能な記憶媒体の管理において、次の事項を考慮する。 h) 取外し可能な記憶媒体のポートは、組織にその利用について理由がある者にだけ有効とする。	干引に関連記載あり			
8.3.1.10	取外し可能な媒体の管理のために、取外し可能な媒体を用いる必要がある場合、媒体への情報の転送を監視する。	7b-7.10.1	取外し可能な記憶媒体の管理において、次の事項を考慮する。 i) 取外し可能な記憶媒体を用いる必要がある場合、そのような記憶媒体への情報の転送を監視する。	干引に関連記載あり			
–	（対応項なし）	7b-7.10.1	取外し可能な記憶媒体の管理において、次の事項を考慮する。 j) 情報は、物理的な輸送中、例えば、郵便サービス又は宅配便で記憶媒体を送る場合に、認可されていないアクセス、不正使用又は破損に関して守り切れる可能性がある。	干引に関連記載あり			
8.3.1.11	取外し可能な媒体の管理のための手順及び認可のレベルは、文書化する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策案で継承ガイド）	–	（対応項なし）	–
8.3.2	媒体の処分 媒体が不要になった場合は、正式な手順を用いて、セキュリティを保って処分する。	7.10	記憶媒体 管理策 記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理する。 目的 記憶媒体上の情報に対して認可された開示、変更、移動又は破壊だけがなされることを確実にするため。		7.10	記憶媒体 統制目標：記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理する。 目的：記憶媒体上の情報に対して認可された開示、変更、移動又は破壊だけがなされることを確実にするため。	
8.3.2.1	認可されていない者に秘密情報が置かれリスクを最小化するために、媒体のセキュリティを保った処分のための正式な手順を確立する。	7b-7.10.2	認可されていない者に秘密情報が置かれリスクを最小化するために、記憶媒体のセキュリティを保った再利用又は処分の手順を確立する。	干引に関連記載あり	7.10.2	記憶媒体のセキュリティを保った再利用又は処分の手順を整備し、セキュリティ対策を実施する。	認可されていない者に秘密情報が置かれリスクを最小化するために、記憶媒体のセキュリティを保った再利用又は処分の手順を確立する。 秘密情報を格納した記憶媒体の、セキュリティを保った再利用又は処分の手順は、その情報の取扱いや分類に応じたものとする。
8.3.2.2	秘密情報を格納した媒体の、セキュリティを保った処分の手順は、その情報の取扱いに慎重を要する度合いに応じたものとする。	7b-7.10.3	秘密情報を格納した記憶媒体の、セキュリティを保った再利用又は処分の手順は、その情報の取扱いに慎重を要する度合いに応じたものとする。	干引に関連記載あり			記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 a) 秘密情報を含む記憶媒体を組織内で再利用できる必要がある場合には、セキュリティを保ってデータを消去するか、又は再利用できる前に記憶媒体をフォーマットする（8.10参照）。 b) 秘密情報を含む記憶媒体は、必要でなくなったときはセキュリティを保って処分する（例えば、内容を破壊、細断又はセキュリティを保って消去することによって）。 c) セキュリティを保った処分を必要とする可能性のある品目を特定する手順をもつ。 d) 多くの業者が、記憶媒体の収集及び処分のサービスを提供している。十分な管理策及び経験をもつ適切な外部の供給者を選定することに、注意を払う。 e) 監査証跡を維持するために、取扱いに慎重を要する品目の処分を記録しておく。 f) 処分のために記憶媒体を集める場合、集積することによる影響に配慮する。取扱いに慎重を要する情報ではない情報でも、その量が集まると、取扱いに慎重を要する情報に変わる場合がある。 取扱いに慎重を要するデータを含んだ装置・機器が損傷した場合には、リスクアセスメントを実施し、修理又は廃棄に出すよりも物理的に破壊する方が望ましい作品作を決定する（7.14参照）。
8.3.2.3	秘密情報を格納した媒体は、セキュリティを保って、保管し、処分する（例えば、焼却、シュレッダーの利用、組織内の他のアプリケーションでの媒体の再利用のためのデータ消去）。	7b-7.10.4	記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 b) 秘密情報を含む記憶媒体は、必要でなくなったときはセキュリティを保って処分する。	干引に関連記載あり			
8.3.2.4	セキュリティを保った処分を必要とする品目を特定するための手順を定める。	7b-7.10.4	記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 c) セキュリティを保った処分を必要とする可能性のある品目を特定する手順をもつ。	干引に関連記載あり			
8.3.2.5	取扱いに慎重を要する媒体類を選び出すことが困難な場合には、セキュリティを保って全ての媒体を処分する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策案で継承ガイド）	–	（対応項なし）	–
8.3.2.6	媒体の収集及び処分のサービスを提供する外部事業者は、十分な管理策及び経験を持つ適切な契約相手を選択する。	7b-7.10.4	記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 d) 多くの業者が、記憶媒体の収集及び処分のサービスを提供している。十分な管理策及び経験をもつ適切な外部の供給者を選定することに、注意を払う。	干引に関連記載あり	7.10.2	【再】記憶媒体のセキュリティを保った再利用又は処分の手順を整備し、セキュリティ対策を実施する。	（7.10.2に対応する項を参照）
8.3.2.7	監査証跡を維持するために、取扱いに慎重を要する品目の処分を記録する。	7b-7.10.4	記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 e) 監査証跡を維持するために、取扱いに慎重を要する品目の処分を記録しておく。	干引に関連記載あり			
8.3.2.8	処分のために情報を含む媒体を集める場合、それらの情報が集積されることによる影響に配慮し、手順に含める。	7b-7.10.4	記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。 f) 処分のために記憶媒体を集める場合、集積することによる影響に配慮する。取扱いに慎重を要する情報ではない情報でも、その量が集まると、取扱いに慎重を要する情報に変わる場合がある。	干引に関連記載あり			
8.3.3	物理的媒体の輸送 情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護する。	7.10	記憶媒体 管理策 記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理する。 目的 記憶媒体上の情報に対して認可された開示、変更、移動又は破壊だけがなされることを確実にするため。		7.1	記憶媒体 統制目標：記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理する。 目的：記憶媒体上の情報に対して認可された開示、変更、移動又は破壊だけがなされることを確実にするため。	
8.3.3.1	輸送される情報を格納した媒体を保護するために、信頼できる輸送機関又は運送業者を用いる。	Sb-S.14.6	物理的記憶媒体（紙を含む。）を輸送する場合、期間、手順及び合意には、次の事項も含める。 a) 管理責任を割り当てること。認可された信頼できる運送業者のリスト	干引に関連記載あり	S.14.4	物理的記憶媒体の輸送について、規則又は手順を整備する。	物理的記憶媒体（紙を含む。）を輸送する場合、期間、手順及び合意には、次の事項も含める。 a) 輸送、受取、及び受領を管理し、通知する責任 b) 伝票の正しい送付先及び送付を確実にすること c) 輸送中に発生する可能性が高い物理的損傷から、製造業者の仕様に従って内容物を保護すること（例えば、雨対よ、熱、湿気又は電磁界への露出など。記録媒体の再生を妨げる可能性のある環境要因からの保護、こん（梱）包及び法付のため最小限の技術標準の使用（例えば、不透明な封筒の使用））。 d) 管理責任を割り当てること。認可された信頼できる運送業者のリスト e) 運送業者を確認する頻度 f) 輸送するお標媒体内の情報の分類レベルに応じて、開封を明らかにする又は開封を防止する管理策（例えば、バッグ、コンテナ）の使用 g) 運送業者の識別情報を検証する手順 h) 情報の分類に応じた、輸送又は運送業者のサービスを提供する第三者の承認された一覧 i) 記憶媒体の内容及び適用した保護方法を特定するためのCIアを保持し、認可された受領者の以入、輸送の責任窓口への発送時刻、及び宛先での受領時刻を記録すること ☆書については5.20.1供給者との☆書にて、「物理的輸送又は運搬的な情☆に情報を保護するための情報の転送の管理策」が存在することから、本管理策においては「規則、手順」を対象とする。
8.3.3.2	輸送される情報を格納した媒体を保護するために、認可された運送業者の一覧について、管理者の☆書を得る。	Sb-S.14.6	【再】物理的記憶媒体（紙を含む。）を輸送する場合、期間、手順及び合意には、次の事項も含める。 d) 管理責任を割り当てること。認可された信頼できる運送業者のリスト	干引に関連記載あり			
8.3.3.3	輸送される情報を格納した媒体を保護するために、運送業者を確認する手順を導入する。	Sb-S.14.6	物理的記憶媒体（紙を含む。）を輸送する場合、期間、手順及び合意には、次の事項も含める。 e) 運送業者を確認する頻度	干引に関連記載あり			
8.3.3.4	輸送される情報を格納した媒体を保護するために、輸送途中に生じるかもしれない物理的損傷から内容物を保護（例えば、媒体の復旧効果を低減させる場合のある、熱、湿気又は電磁界への露出など）するために、製造業者の仕様にも従う。	Sb-S.14.6	物理的記憶媒体（紙を含む。）を輸送する場合、期間、手順及び合意には、次の事項も含める。 c) 輸送中に発生する可能性が高い物理的損傷から、製造業者の仕様に従って内容物を保護すること（例）包、例えば、熱、湿気又は電磁界への露出など。記録媒体の再生を妨げる可能性のある環境要因からの保護、こん（梱）包及び法付のための最小限の技術標準の使用。	干引に関連記載あり			
8.3.3.5	輸送される情報を格納した媒体を保護するために、媒体の内容、適用された保護、並びに輸送の責任窓口への受領時刻及び目的地での受取の時刻の記録を特定するログを保持する。	Sb-S.14.6	物理的記憶媒体（紙を含む。）を輸送する場合、期間、手順及び合意には、次の事項も含める。 i) 記憶媒体の内容及び適用した保護方法を特定するためのCIアを保持し、認可された受領者の以入、輸送の責任窓口への発送時刻、及び宛先での受領時刻を記録すること	干引に関連記載あり			

番号	（旧）管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	（新）管理策基準	（参考）手引き
9.1	アクセス制御に対する業務上の要求事項 管理目的：情報及び情報処理施設へのアクセスを制限するため。	5.15	アクセス制御 管理策 情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を、事業上及び情報セキュリティの要求事項に基づいて確立し、実施する。 目的 情報及びその他の関連資産への認可されたアクセスを行わせ、認可されていないアクセスを防ぐことを確実にするため。		5.15	アクセス制御 統制目標：情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を、事業上及び情報セキュリティの要求事項に基づいて確立し、実施する。 目的：情報及びその他の関連資産への認可されたアクセスを行わせ、認可されていないアクセスを防ぐことを確実にするため。	
9.1.1	アクセス制御方針 アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューする。						
9.1.1.1	資産の管理責任者は、資産に対する利用者のそれぞれの役割に対して、適切なアクセス制御規則、アクセス権及び制御を、アクセスに伴う情報セキュリティリスクを反映した制御の詳細さ及び厳密さで決定し、利用者の認証を要求しないシステム及びサービスは認証を要求しない根拠と共に文書化する。	Sc-5.15.1	情報及びその他の関連資産の管理責任者は、アクセス制御に関連する情報セキュリティ及び事業上の要求事項を決定する。	于当に関連記載あり	5.15.1	アクセス制御に関連する情報セキュリティ及び事業上の要求事項を踏まえたアクセス制御に関する方針及び規則を策定し、実施する。	情報及びその他の関連資産の管理責任者は、アクセス制御に関連する情報セキュリティ及び事業上の要求事項を決定する。 情報セキュリティ及び事業上の要求事項を考慮したアクセス制御に関する方針を定め、関連する全ての利害関係者に伝達する。 アクセス制御に関する方針では以下を含める a）どのエンティティが、情報及びその他の関連資産ごとの種類のアクセスを必要とするかの決定 b）アプリケーションセキュリティ（8.26参照） c）物理的アクセス、これは適切な物理的入退管理策（7.2、7.3及び7.4参照）による支援する必要がある。 d）情報の配布及び認可（例えば、知る必要性の原則）、並びに情報のセキュリティ水準及び情報の分類（5.10、5.12及び5.13参照） e）特権的アクセスの制限（8.2参照） f）職務の分離（5.3参照） g）データ又はサービスへのアクセスの制限に関連する法令、規制及び契約上の義務（5.31、5.32、5.33、5.34及び5.35参照） h）アクセス制御機能の分離（例えば、アクセス要求、アクセス認可、アクセス管理） i）アクセス要求の正式な認可（5.16及び5.18参照） j）アクセス権の管理（5.18参照） k）ログ取得（8.15参照） アクセス制御規則は、関連するエンティティに対して、適切なアクセス権及び制限を定義し、対応付けすることによって実施する（5.16参照）。エンティティは、人間の利用者だけでなく、技術的又は論理的なアイテム（例えば、機械、装置・機器又はサービス）の場合もある。アクセス制御の管理を簡潔にするために、役割をエンティティのグループに割り当てることが可能である。 アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。 a）アクセス権と情報分類との整合性 b）アクセス権と物理的境界のセキュリティのニーズ及び要求事項との整合性 c）エンティティに、使用が認められているネットワーク及びネットワークサービスを含む、情報及びその他の関連資産へのアクセスだけを提供するために、分散環境で利用可能な全ての種類の接続を考慮すること d）動的アクセス制御に関連する要素又は要因をどのように反映できるかを検討すること
9.1.1.2	アクセス制御は、論理的アクセス制御と物理的アクセス制御の両面を考慮して決定する。	Sc-5.15.5	アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。 b）アクセス権と物理的境界のセキュリティのニーズ及び要求事項との整合性	于当に関連記載あり			
9.1.1.3	利用者及びクラウドサービス事業者には、アクセス制御によって達成する業務上の要求事項を明確に規定した提供する。	Sc-5.15.2	情報セキュリティ及び事業上の要求事項を考慮したアクセス制御に関するトピック固有の方針を定め、関連する全ての利害関係者に伝達する。	于当に関連記載あり			
9.1.1.4	アクセス制御方針に、業務用アプリケーションのセキュリティ要求事項を反映する。	Sc-5.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 b）アプリケーションセキュリティ	于当に関連記載あり			
9.1.1.5	アクセス制御方針には、情報の伝達及び認可に対する方針（例えば、知る必要性の原則、情報のセキュリティ水準、情報の分類）を含める。	Sc-5.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 d）情報の配布及び認可、並びに情報のセキュリティ水準及び情報の分類	于当に関連記載あり			
9.1.1.6	アクセス制御方針は、システム及びネットワークにおける、アクセス権と情報分類の方針との整合性を考慮して定める。	Sc-5.15.5	アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。 a）アクセス権と情報分類との整合性	于当に関連記載あり			
9.1.1.7	アクセス制御方針には、データ又はサービスへのアクセスの制限に関連する法令及び契約上の義務を反映する。	Sc-5.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 g）データ又はサービスへのアクセスの制限に関連する法令、規制及び契約上の義務	于当に関連記載あり			
9.1.1.8	アクセス制御方針に、利用可能な全ての種類の接続を認識する分散ネットワーク環境におけるアクセス権の管理を含める。	Sc-5.15.5	アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。 c）エンティティに、使用が認められているネットワーク及びネットワークサービスを含む、情報及びその他の関連資産へのアクセスだけを提供するために、分散環境で利用可能な全ての種類の接続を考慮すること	于当に関連記載あり			
9.1.1.9	アクセス制御方針に、アクセス制御における役割の分離（例えば、アクセス要求、アクセス認可、アクセス管理）の方針を含める。	Sc-5.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 h）アクセス制御機能の分離	于当に関連記載あり			
9.1.1.10	アクセス制御方針に、アクセス要求の正式な認可に対する要求事項を含める。	Sc-5.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 i）アクセス要求の正式な認可	于当に関連記載あり			
9.1.1.11	アクセス制御方針に、アクセス権の定期的なレビューに対する要求事項を含める。	Sc-5.18.2	物理的及び論理的なアクセス権の定期的なレビューでは、次の事項を考慮する。 a）同じ組織内での何らかの変更後又は退職後の利用者のアクセス権 b）特権的アクセス権の認可	于当に関連記載あり	5.18.2	物理的及び論理的なアクセス権の定期的なレビューでは、次の事項を考慮する。 a）同じ組織内での何らかの変更後（例えば、異動、昇進、降格）又は退職後の利用者のアクセス権（6.1～6.5参照） b）特権的アクセス権の認可 情報及びその他の関連資産への利用者のアクセス権は、雇用の変更又は終了の前に、次に示すリスク因子の評価に基づいて、レビュー、調整又は削除する。 a）雇用の終了又は変更が、利用者の側によるものか又は経営側によるものかどうか、及び雇用の終了の理由 b）利用者の現時点の責任 c）現在アクセス可能な資産の価値	
9.1.1.12	アクセス制御方針に、アクセス権の削除の方針を含める。	Sc-5.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 j）アクセス権の管理	于当に関連記載あり	5.15.1	【再】アクセス制御に関連する情報セキュリティ及び事業上の要求事項を踏まえたアクセス制御に関する方針及び規則を策定し、実施する。	（5.15.1に対応する項を参照）
9.1.1.13	アクセス制御方針に、利用者の識別情報及び秘密認証情報の利用及び管理に関する、全ての重要な事象の記録の保管を含める。	Sc-5.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 k）ログ取得	于当に関連記載あり			
9.1.1.14	アクセス制御方針に、特権的アクセスを認められた役割を含める。	Sc-5.15.3	情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。 e）特権的アクセスの制限	于当に関連記載あり			
9.1.1.15	アクセス制御方針に、利用者の認証を要求しないシステム及びサービスを定め、識別することを含める。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
9.1.1.16	アクセス制御方針に、ゼロトラストアーキテクチャ（動的なアクセス制御）に関する要求事項を含める。	Sc-5.15.5	アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。 d）動的アクセス制御に関連する要素又は要因をどのように反映できるかを検討すること	于当に関連記載あり	5.15.1	【再】アクセス制御に関連する情報セキュリティ及び事業上の要求事項を踏まえたアクセス制御に関する方針及び規則を策定し、実施する。	（5.15.1に対応する項を参照）
9.1.2	ネットワーク及びネットワークサービスへのアクセス 利用者ことを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供する。	5.15	アクセス制御 管理策 情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を、事業上及び情報セキュリティの要求事項に基づいて確立し、実施する。 目的 情報及びその他の関連資産への認可されたアクセスを行わせ、認可されていないアクセスを防ぐことを確実にするため。		5.15	アクセス制御 統制目標：情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を、事業上及び情報セキュリティの要求事項に基づいて確立し、実施する。 目的：情報及びその他の関連資産への認可されたアクセスを行わせ、認可されていないアクセスを防ぐことを確実にするため。	
		8.21	管理策 ネットワークサービスのセキュリティ機能、サービスレベル及びサービスの要求事項を特定し、実装し、監視する。 目的 ネットワークサービスの利用における安全性を確実にするため。		8.21	ネットワークサービスのセキュリティ 統制目標：ネットワークサービスのセキュリティ機能、サービスレベル及びサービスの要求事項を特定し、実装し、監視する。 目的：ネットワークサービスの利用における安全性を確実にするため。	
9.1.2.1	ネットワーク及びネットワークサービスの利用に関し、方針を設定する。	Sc-5.15.2	【再】情報セキュリティ及び事業上の要求事項を考慮したアクセス制御に関するトピック固有の方針をまとめ、関連する全ての利害関係者に伝達する。	于当に関連記載あり	5.15.1	【再】アクセス制御に関連する情報セキュリティ及び事業上の要求事項を踏まえたアクセス制御に関する方針及び規則を策定し、実施する。	（5.15.1に対応する項を参照）
9.1.2.2	ネットワーク及びネットワークサービスの利用に関する方針は、アクセスが許されるネットワーク及びネットワークサービスを対象にする。	8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 a）アクセスが許可されているネットワーク及びネットワークサービス	于当に関連記載あり	8.21.1	ネットワークサービスの利用に関する規則を整備する。	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 a）アクセスが許可されているネットワーク及びネットワークサービス b）様々なネットワークサービスにアクセスするための認証の要求事項 c）誰にどのネットワーク及びネットワークサービスにアクセスすることを許すかを決定する認可手順 d）ネットワーク接続及びネットワークサービスのアクセスを保護するためのネットワーク管理並びに技術的管理策及び手順 e）ネットワーク及びネットワークサービスにアクセスするために利用する手段（例えば、仮想プライベートネットワーク（VPN）又は無線ネットワークの利用） f）アクセス時の利用者の特長、場所及びその他の属性 g）ネットワークサービスの利用の監視
9.1.2.3	ネットワーク及びネットワークサービスの利用に関する方針は、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決めるための認可手順を対象にする。	8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 c）誰にどのネットワーク及びネットワークサービスにアクセスすることを許すかを決定する認可手順	于当に関連記載あり			
9.1.2.4	ネットワーク及びネットワークサービスの利用に関する方針は、ネットワーク接続及びネットワークサービスへのアクセスを保護するための運用管理策から管理策及び管理手順を対象にする。	8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 d）ネットワーク接続及びネットワークサービスのアクセスを保護するためのネットワーク管理並びに技術的管理策及び手順	于当に関連記載あり			
9.1.2.5	ネットワーク及びネットワークサービスの利用に関する方針は、ネットワーク及びネットワークサービスへのアクセスに利用される手段（例えば、VPN、無線ネットワーク）を対象にする。	8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 e）ネットワーク及びネットワークサービスにアクセスするために利用する手段	于当に関連記載あり			
9.1.2.6	ネットワーク及びネットワークサービスの利用に関する方針は、様々なネットワークサービスへのアクセスに対する利用者認証の要求事項を対象にする。	8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 b）様々なネットワークサービスにアクセスするための認証の要求事項	于当に関連記載あり			
9.1.2.7	ネットワーク及びネットワークサービスの利用に関する方針は、ネットワークサービスの利用の監視を対象にする。	8c-8.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 g）ネットワークサービスの利用の監視	于当に関連記載あり			
9.1.2.8	ネットワークサービスの利用に関する方針は、組織のアクセス制御方針と整合させる。	Sc-5.15.5	【再】アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。 c）エンティティに、使用が認められているネットワーク及びネットワークサービスを含む、情報及びその他の関連資産へのアクセスだけを提供するために、分散環境で利用可能な全ての種類の接続を考慮すること	于当に関連記載あり	5.15.1	【再】アクセス制御に関連する情報セキュリティ及び事業上の要求事項を踏まえたアクセス制御に関する方針及び規則を策定し、実施する。	（5.15.1に対応する項を参照）
9.2	利用者アクセスの管理 管理目的：システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。	5.16	識別情報の管理 管理策 識別情報のライフサイクル全体を管理する。 目的 組織の情報及びその他の関連資産にアクセスする個人及びシステムを一意に特定できるようにし、アクセス権を適切に割り当てることができるようにするため。		5.16	識別情報の管理 統制目標：識別情報のライフサイクル全体を管理する。 目的：組織の情報及びその他の関連資産にアクセスする個人及びシステムを一意に特定できるようにし、アクセス権を適切に割り当てることができるようにするため。	
9.2.1	利用者登録及び登録削除 アクセス権の割当てを可能にするために、利用者の登録及び登録削除について正式なプロセスを実施する。						
9.2.1.1	利用者IDを管理するプロセスに、利用者と利用者自身の行動とを対応付けること、及び利用者がその行動に責任をもつことを可能にする。一般な利用者ID の利用を含める。	Sc-5.16.1	識別情報の管理におけるプロセスは、次の事項を確実にする。 a）個人に割り当てられる識別情報の場合、特定の識別情報を使って実行した処理に関してその個人にアカウンタビリティを負わせることができるよう、一つの識別情報は一人の個人に対応付ける（紐）付ける。	于当に関連記載あり	5.16.1	識別情報のライフサイクル全体を管理するプロセスを整備し、管理する。	識別情報の管理における方法では、次の事項を確実にする。 a）個人に割り当てられる識別情報の場合、特定の識別情報を使って実行した処理に関してその個人にアカウンタビリティを負わせることができるよう、一つの識別情報は一人の個人に対応付ける（紐）付ける。 b）複数の人に割り当てられる識別情報（例えば、共有の識別情報）は、業務上又は運用上の理由で必要であり、そのための承認及び文書化をする場合にだけ許可する。 c）人間以外のエンティティに割り当てられる識別情報は、適切に権限を分離した承認及び独立した継続的な監視の対象とする。 d）識別情報が不要になった場合（例えば、関連するエンティティが所掌されたに戻しは使用されなくなった場合、又は識別情報にひも（紐）付けされた人が組織を去った戻しには役割を変えた場合）、識別情報を時機を失せずに無効化又は削除する。 e）特定の領域では、一つだけの識別情報を一つのエンティティに対応付ける【すなわち、同じ環境下で一つのエンティティに複数の識別情報を対応付けるこ（複数識別情報）は避ける。】。 f）利用者識別情報及び認証情報の使用及び管理に関する全ての重要な事象の記録を保持する。 組織は、利用者識別情報に関連する情報の変更を他の扱う支援プロセスをもう。このプロセスは、個人に関連する保護する文書の再検証を含む場合がある。
9.2.1.2	利用者IDを管理するプロセスに、共有ID の利用は、業務上又は運用上の理由での要な場合に万が許可し、承認し、記録することを含める。	Sc-5.16.1	識別情報の管理におけるプロセスは、次の事項を確実にする。 b）複数の人に割り当てられる識別情報の場合、業務上又は運用上の理由で必要であり、そのための承認及び文書化をする場合にだけ許可する。	于当に関連記載あり			
–	（対応項なし）	Sc-5.16.1	識別情報の管理におけるプロセスは、次の事項を確実にする。 c）人間以外のエンティティに割り当てられる識別情報は、適切に権限を分離した承認及び独立した継続的な監視の対象とする。	于当に関連記載あり			
9.2.1.3	利用者IDを管理するプロセスに、組織を離れた利用者の利用者ID、即座の無効化又は削除を含める。	Sc-5.16.1	識別情報の管理におけるプロセスは、次の事項を確実にする。 d）識別情報が不要になった場合、識別情報を時機を失せずに無効化又は削除する。	于当に関連記載あり			
–	（対応項なし）	Sc-5.16.1	識別情報の管理における方法では、次の事項を確実にする。 e）特定の領域では、一つだけの識別情報を一つのエンティティに対応付ける。	于当に関連記載あり			
–	（対応項なし）	Sc-5.16.1	識別情報の管理における方法では、次の事項を確実にする。 f）利用者識別情報及び認証情報の使用及び管理に関する全ての重要な事象の記録を保持する。	于当に関連記載あり			
9.2.1.4	利用者IDを管理するプロセスに、必要のない利用者ID の定期的な特定、及び削除又は無効化することを含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.2.1.5	利用者IDを管理するプロセスに、別の利用者に重複する利用者ID を発行しないことを確実にするよう定める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
–	（対応項なし）	Sc-5.16.2	組織は、利用者識別情報に関連する情報の変更を他の扱う支援プロセスをもう。	于当に関連記載あり	5.16.1	【再】識別情報のライフサイクル全体を管理するプロセスを整備し、管理する。	（5.16.1に対応する項を参照）
–	（対応項なし）	（Sc-5.16.2参考）	このプロセスは、個人に関連する保護する文書の再検証を含む場合がある。	于当に関連記載あり			
–	（対応項なし）	Sc-5.16.3	第三者が提供し又は発行した識別情報を使用する場合、組織は、必要な信頼レベルが第三者の識別情報にあり、関連するリスクを知り、十分に対応する。	于当に関連記載あり	5.16.2	第三者が提供又は発行した識別情報を使用する場合、第三者の識別情報及び必要な信頼レベルにあること及び関連するリスクを特定し、対応する。	第三者が提供し又は発行した識別情報（例えば、ソーシャルメディアのログインなど）を使用する場合、組織は、必要な信頼レベルが第三者の識別情報にあり、関連するリスクを知り、十分に対応する。このプロセスは、第三者に関連する管理策（5.19参照）、及び認証情報に関連する管理策（5.17参照）を含む場合がある。
–	（対応項なし）	（Sc-5.16.3参考）	このプロセスは、第三者に関連する管理策、及び認証情報に関連する管理策を含む場合がある。	于当に関連記載あり			
9.2.1.6.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	于当に関連記載あり（情報セキュリティ管理基準以外の由来）	5.16.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
9.2.2	利用者アクセスの提供 全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者アクセスの提供についての正式なプロセスを実施する。	5.18	アクセス権 管理策 情報及びその他の関連資産へのアクセス権は、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除する。 目的 情報及びその他の関連資産へのアクセスを、事業上の要求事項に従って定義し、認可することを確実にするため。		5.18	アクセス権 統制目標：情報及びその他の関連資産へのアクセス権は、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除する。 目的：情報及びその他の関連資産へのアクセスを、事業上の要求事項に従って定義し、認可することを確実にするため。	
9.2.2.1	利用者ID に対するアクセス権の割当て及び無効化のプロセに、情報システム又はサービスの利用について、その情報システム又はサービスの管理責任者から認可を得ていることの点検を含める。（アクセス権について、管理職から別の承認を受けることが適切な場合もある。）	Sc-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセには、次の事項を含む。 a) 情報及びその他の関連資産の利用について、その情報及びその他の関連資産の管理責任者からの認可の取得	予引に関連記載あり	5.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て及び無効化のプロセスを整備し、アクセス権の割り当て、変更及び削除する。	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセには、次の事項を含む。 a) 情報及びその他の関連資産の利用について、その情報及びその他の関連資産の管理責任者からの認可の取得（5.9参照）。アクセス権について、管理職による承認を受けることが適切な場合がある。 b) 事業上の要求事項及び組織のアクセス制御に関するトピック固有の方針並びに規則の考慮 c) アクセス権の承認及び実施の役割の分離、並びに相反する役割の分離を含む、職務の分離の考慮 d) ある者が情報及びその他の関連資産にアクセスする必要がなくなった場合にアクセス権を削除する。特に、組織を去った利用者のアクセス権を時機を失せずに削除する。 e) 特に臨時要員、又は要員が必要とする一時的なアクセスについて、限られた期間の一時的アクセス権を与え、期限の経た後の消すことの考慮 f) 許可したアクセスのレベル、アクセス制御に関するトピック固有の方針に適していること（5.15参照）、及び職務の分離（5.3参照）などのその他の情報セキュリティ要求事項と整合していることの検証 g) 認可手順が問題なく完了した後にだけ、アクセスを有効にする（例えば、サービス提供者がアクセス権を有効にする） h) 情報及びその他の関連資産にアクセスするために利用者識別子（ID、論理的又は物理的）に与えられたアクセス権の、一元的な記録の維持 i) 役割又は職務を変更した利用者のアクセス権の変更 j) 物理的及び論理的アクセス権の削除又は調整 k) 利用者の論理的及び物理的アクセス権の変更の記録の維持
9.2.2.2	（対応項なし）	Sc-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセには、次の事項を含む。 a) 臨時要員、又は要員が必要とする一時的なアクセスについて、限られた期間の一時的アクセス権を与え、期限の経た後の消すことの考慮	予引に関連記載あり			
9.2.2.3	利用者ID に対するアクセス権の割当て及び無効化のプロセに、許可したアクセスのレベルが、職務の分離などその他の要求事項と整合していることの検証を含める。	Sc-S.18.1	【再】エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセには、次の事項を含む。 c) アクセス権の承認及び実施の役割の分離、並びに相反する役割の分離を含む、職務の分離の考慮 f) 許可したアクセスのレベル、アクセス制御に関するトピック固有の方針に適していること、及び職務の分離などその他の情報セキュリティ要求事項と整合していることの検証	予引に関連記載あり			
–	（対応項なし）	Sc-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセには、次の事項を含む。 e) 臨時要員、又は要員が必要とする一時的なアクセスについて、限られた期間の一時的アクセス権を与え、期限の経た後の消すことの考慮	予引に関連記載あり			
9.2.2.4	利用者ID に対するアクセス権の割当て及び無効化のプロセに、認可手順が完了するまで、（例えば、クラウドサービス事業者が）アクセス権を有効にしないことが確実になるよう定める。	Sc-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセには、次の事項を含む。 g) 認可手順が問題なく完了した後にだけ、アクセスを有効にする	予引に関連記載あり			
9.2.2.5	利用者ID に対するアクセス権の割当て及び無効化のプロセに、情報システム又はサービスにアクセスするために利用者ID に与えられたアクセス権の、一元的な記録の維持を含める。	Sc-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセには、次の事項を含む。 h) 情報及びその他の関連資産にアクセスするために利用者識別子（ID、論理的又は物理的）に与えられたアクセス権の、一元的な記録の維持 k) 利用者の論理的及び物理的アクセス権の変更の記録の維持	予引に関連記載あり			
9.2.2.6	利用者ID に対するアクセス権の割当て及び無効化のプロセに、役割又は職務を変更した利用者のアクセス権の変更、及び組織を離れた利用者のアクセス権の即座の削除又は停止することを含める。	Sc-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセには、次の事項を含む。 d) ある者が情報及びその他の関連資産にアクセスする必要がなくなった場合にアクセス権を削除する。特に、組織を去った利用者のアクセス権を時機を失せずに削除する。 i) 役割又は職務を変更した利用者のアクセス権の変更	予引に関連記載あり			
–	（対応項なし）	Sc-S.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセには、次の事項を含む。 j) 物理的及び論理的アクセス権の削除又は調整	予引に関連記載あり			
9.2.2.7	利用者ID に対するアクセス権の割当て及び無効化のプロセに、情報システム又はサービスの管理責任者による、アクセス権の定期的なレビューを含める。	Sc-S.18.2	【再】物理的及び論理的なアクセス権の定期的なレビューでは、次の事項を考慮する。 a) 同じ組織内での同らかの変更後又は退職後の利用者のアクセス権 b) 特権的アクセス権の認可	予引に関連記載あり	5.18.2	【再】物理的及び論理的なアクセス権の定期的なレビューを実施する。	（5.18.2に対応する項を参照）
–	（対応項なし）	Sc-S.18.3	情報及びその他の関連資産への利用者のアクセス権は、雇用の変更又は終了の前に、次に示すリスク因子の評価に基づいて、レビュー、調整又は削除する。 a) 雇用の終了又は変更が、利用者の側によるものか又は経営側によるものだか、及び雇用の終了の理由 b) 利用者の現時点の責任 c) 保有アクセス可能な資産の価値	予引に関連記載あり			
9.2.2.8.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の出来）	5.18.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
9.2.3	特権的アクセス権の管理 特権的アクセス権の割当て及び利用は、制限し、管理する。	8.2	特権的アクセス権 管理策 特権的アクセス権の割当て及び利用は、制限し、管理する。 目的 認可された利用者、ソフトウェア構成要素及びサービス已に特権的アクセス権が与えられることを確実にするため。		8.2	特権的アクセス権 統制目標：特権的アクセス権の割当て及び利用は、制限し、管理する。 目的：認可された利用者、ソフトウェア構成要素及びサービス已に特権的アクセス権が与えられることを確実にするため。	
9.2.3.1	特権的アクセス権の割当ては、関連するアクセス制御方針に従って、正式な認可プロセスによって管理する。	8a-8.2.1	特権的アクセス権の割当ては、アクセス制御に関するトピック固有の方針に従って、認可プロセスによって管理する。	予引に関連記載あり	8.2.1	特権的アクセス権の割当て及び利用を制限し、管理する。	特権的アクセス権の割当ては、アクセス制御に関するトピック固有の方針（5.15参照）に従って、認可プロセスによって管理する。 この管理策の実施については、次の事項を考慮する。 a) 各々のシステムはなプロセス（例えば、オペレーティングシステム、データベース管理システム、アプリケーション）の特権的アクセス権を必要とする利用者を特定する。 b) 特権的アクセス権を、アクセス制御に関するトピック固有の方針（5.15参照）に沿って、必要に応じて、かつ、事後ごと、利用者に割り当てる（すなわち、特権的アクセスを必要とする活動を実行するために必要な力量をもつ個人に対して行う、かつその個人の職務上の役割のための最小限の要求に基づいて）。 c) 特権の認可プロセス（すなわち、誰が特権的アクセス権を承認することが可能かを決定するか、又は特権的アクセス権は認可プロセスが完了するまで許可しない）及び割り当て主全ての特権の記録を維持する。 d) 特権的アクセス権の終了に関する要求事項を定め、実施する。 e) 利用者が、自らが特権的アクセス権をもっていること、及び設らかへ特権的アクセスモードにないるかを認識することを確実にするための対策を講じる。考えられる対策には、特別の利用者識別情報、利用者インタフェース設定、又は特別の装置の使用が含まれる。 f) 特権的アクセス権における認証の要求事項は、通常のアクセス権における要求事項よりも要求が厳なる場合がある。特権的アクセス権を用いて作業を行う前に、両認証又は認証の強とが必要になる場合がある。 g) 定期的に、また組織に何か変更があった後に、特権的アクセス権を用いて作業する利用者をレビュー、特権的アクセス権を用いた作業に関して、その利用者の職務、役割、責任及び力量のさで今と適確であるかどうかを検証する（5.18参照）。 h) 汎用の実務管理者ID（root又は）の使用を避けるため、システムの構成管理機能に応じて、具体的な規則を確立する。そのような汎ID の認証情報を管理し、保護する（5.17参照）。 i) 特権的アクセス権を永続的に許可するのではく、承認された変更又は活動（例えば、保守活動又は一部の重要な変更）を実施するのに必要な時間枠だけ一時的な特権的アクセス許可する。これは、ぱんぱブレークグラス手順（break glass procedure）と呼ばれ、しばしば特権的アクセス管理策において取動化されている。 j) 監査の目的で、システムへの全ての特権的アクセスのログを記録する。 k) 特権的アクセス権をセ識別情報を複数の人で共有又は連携することはせず、特定の特権的アクセス権の割当て許可された個別の識別情報を各人に割り当てる。特権的アクセス権の管理を簡素化するために、識別情報をグループ化することが可能である（例えば、業務管理者グループ化と変えることによって）。 l) 特権的アクセス権をセ識別情報は、管理作業を実行するために使用し、日常の一般的な職務（すなわち、電子メールの閲覧、ウェブへのアクセス）には使用しない（利用者はこれらの活動のために別の通常のネットワーク識別情報をもつ）。
9.2.3.2	特権の割当ての正式な認可プロセスは、各々のシステム又はプロセス（例えば、オペレーティングシステム、データベース管理システム、及びアプリケーション）に関連した特権的アクセス権、及び特権的アクセス権を割り当てる必要がある利用者を特定する。	8a-8.2.2	この管理策の実施については、次の事項を考慮する。 a) 各々のシステム又はプロセスの特権的アクセス権を必要とする利用者を特定する。	予引に関連記載あり			
9.2.3.3	特権の割当ての正式な認可プロセスは、特権的アクセス権を、アクセス制御方針に沿って、使用の必要性ごとに、かつ、事後ごと、利用者に割り当てる。すなわち、利用者の職務上の役割のための最小限の要求事項に基づいて割り当てる。	8a-8.2.2	この管理策の実施については、次の事項を考慮する。 b) 特権的アクセス権を、アクセス制御に関するトピック固有の方針に沿って、必要に応じて、かつ、事後ごと、利用者に割り当てる（すなわち、特権的アクセスを必要とする活動を実行するために必要な力量をもつ個人に対して行う、かつその個人の職務上の役割のための最小限の要求に基づいて）。	予引に関連記載あり			
9.2.3.4	特権の割当ての正式な認可プロセスは、割り当て主全ての特権の認可プロセス及び記録を維持する。	8a-8.2.2	この管理策の実施については、次の事項を考慮する。 c) 特権の認可プロセス（すなわち、誰が特権的アクセス権を承認することが可能かを決定するか、又は特権的アクセス権は認可プロセスが完了するまで許可しない）及び割り当て主全ての特権の記録を維持する。	予引に関連記載あり			
9.2.3.5	特権の割当ての正式な認可プロセスは、特権的アクセス権は、認可プロセスが完了するまで許可しない	8a-8.2.2	【再】この管理策の実施については、次の事項を考慮する。 c) 特権の認可プロセス（すなわち、誰が特権的アクセス権を承認することが可能かを決定するか、又は特権的アクセス権は認可プロセスが完了するまで許可しない）及び割り当て主全ての特権の記録を維持する。	予引に関連記載あり			
9.2.3.6	特権の割当ての正式な認可プロセスは、特権的アクセス権の終了に関する要求事項を定める。	8a-8.2.2	この管理策の実施については、次の事項を考慮する。 d) 特権的アクセス権の終了に関する要求事項を定め、実施する。	予引に関連記載あり			
9.2.3.7	特権の割当ての正式な認可プロセスは、特権的アクセス権は、通常業務に用いている利用者ID とは別の利用者ID に割り当てる。特権を与えられたID からは、通常業務を行わない。	8a-8.2.2	この管理策の実施については、次の事項を考慮する。 f) 特権的アクセス権をセ識別情報は、管理作業を実行するために已に使用し、日常の一般的な職務（すなわち、電子メールの閲覧、ウェブへのアクセス）には使用しない（利用者はこれらの活動のために別の通常のネットワーク識別情報をもつ）。	予引に関連記載あり			
9.2.3.8	特権の割当ての正式な認可プロセスは、特権的アクセス権を与えられた利用者のカ量が不の職務に見合っていることを検証するために、その力量を定期的にレビューする。	8a-8.2.2	この管理策の実施については、次の事項を考慮する。 g) 定期的に、また組織に何か変更があった後に、特権的アクセス権を用いて作業する利用者をレビュー、特権的アクセス権を用いた作業に関して、その利用者の職務、役割、責任及び力量のさで今と適確であるかどうかを検証する。	予引に関連記載あり			
9.2.3.9	特権の割当ての正式な認可プロセスは、汎用の実務管理者ID の認可されていない使用を避けるため、システムの構成管理機能に応じて、具体的な手順を確立及び維持する。	8a-8.2.2	この管理策の実施については、次の事項を考慮する。 h) 汎用の実務管理者ID の使用を避けるため、システムの構成管理機能に応じて、具体的な規則を確立する。そのような ID の認証情報を管理し、保護する。	予引に関連記載あり			
9.2.3.10	特権の割当ての正式な認可プロセスは、汎用の実務管理者ID に関して、共有する場合に秘密認証情報の機密性を維持する。（例えば、頻繁にパスワードを変更する、特権を与えられた利用者が頻繁する又は職務を変更する場合はできるだけ*ヤパスワードを変更する。特権を与えられた利用者の間で適切な方法でパスワードを伝達する）	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準と組承点だ）	–	（対応項なし）	–
9.2.3.11.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の出来）	8.2.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
9.2.4	利用者の秘密認証情報の管理 秘密認証情報の割当ては、正式な管理プロセスによって管理する。	5.17	認証情報 管理策 認証情報の割当ては管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理する。 目的 適切なエンティティ認証を確実にし、認証プロセスの失敗を防ぐため。		5.17	認証情報 統制目標：認証情報の割当ては管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理する。 目的：適切なエンティティ認証を確実にし、認証プロセスの失敗を防ぐため。	
9.2.4.1	秘密認証情報の割当ての正式な管理プロセスでは、個人の秘密認証情報を秘密に保つ旨の文書への署名を、利用者に要求する。この署名文書は、雇用契約の条件に含める場合がある。	Sc-S.17.2	認証情報にアクセスする立はそれを使用する者に、次の事項を確実に行うよう助言する。 a) パスワードなどの秘密認証情報は機密を保つ、個人の秘密認証情報を他人と共有しない、複数の利用者に、又は個人でないエンティティにひも（紐）付けられている識別情報に対して使用する秘密認証情報は、認可された人だけは共有する。 b) 影響を受けた又は侵害された認証情報は、侵害の知らが又はその他の兆候があれば、直ちに変更する。 c) パスワードを認証情報として使用する場合、例えば、次のような最適な個行の推奨事項に従った強力なパスワードを選択する。 1) パスワードは、当人に関する情報から、他の者が容易に推測できる又は得られる事項に基づかない。 2) パスワードは辞書の単語又はそれらの組合せに基づかない。 3) 覚えやすいパスフレーズを使用し、英数字及び特殊文字を含めるようにする。 4) パスワードに最小限必要とする長さを定める。 d) 異なるサービス及びシステム間で同じパスワードを使用しない。 e) a)～d)の規則に従う義務が、雇用条件にも含まれている（6.2参照）。	予引に関連記載あり	5.17.2	認証情報にアクセスする立はそれを使用する者に、機密性を保つために必要な事項を伝達する。	認証情報にアクセスする立はそれを使用する者に、次の事項を確実に行うよう助言する。 a) パスワードなどの秘密認証情報は機密を保つ、個人の秘密認証情報を他人と共有しない、複数の利用者に、又は個人でないエンティティにひも（紐）付けられている識別情報に対して使用する秘密認証情報は、認可された人だけは共有する。 b) 影響を受けた又は侵害された認証情報は、侵害の知らが又はその他の兆候があれば、直ちに変更する。 c) パスワードを認証情報として使用する場合、例えば、次のような最適な個行の推奨事項に従った強力なパスワードを選択する。 1) パスワードは、当人に関する情報（例えば、名前、電話番号、誕生日）から、他の者が容易に推測できる又は得られる事項に基づかない。 2) パスワードは辞書の単語又はそれらの組合せに基づかない。 3) 覚えやすいパスフレーズを使用し、英数字及び特殊文字を含めるようにする。 4) パスワードに最小限必要とする長さを定める。 d) 異なるサービス及びシステム間で同じパスワードを使用しない。 e) a)～d)の規則に従う義務が、雇用条件にも含まれている（6.2参照）。
9.2.4.2	秘密認証情報の割当ての正式な管理プロセスでは、グループの（すなわち、共用の）秘密認証情報はグループのメンバだけの秘密に保つ旨の文書への署名を、利用者に要求する。この署名文書は、雇用契約の条件に含める場合がある。			予引に関連記載あり			
9.2.4.3	秘密認証情報の割当ての正式な管理プロセスでは、利用者に各自の秘密認証情報を保持することを求める場合、最初に、セキュリティが弱ただ仮の秘密認証情報を発行し、最初の使用時にこれを変更させる。	Sc-S.17.1	認証情報の割当ておび管理のプロセには、次の事項を確実にする。 a) 他の秘密認証情報として登録プロセスに自動的に生成される個人パスワードは個人識別番号（PIN）は、推測不可能であり、各人に対して一意で、かつ、利用者は最初の使用後にそれを変更することが要求される。	予引に関連記載あり	5.17.1	認証情報の割当ておび管理のプロセスを整備し、管理する。	認証情報の割当ておび管理のプロセには、次の事項を確実にする。 a) 他の秘密認証情報として登録プロセスに自動的に生成される個人パスワードは個人識別番号（PIN）は、推測不可能であり、各人に対して一意で、かつ、利用者は最初の使用後にそれを変更することが要求される。 b) 新規、更新又は他の認証情報を発行する前に、利用者の本人確認の手順を確立する。 c) 他の認証情報を含む認証情報は、セキュリティを保つた方法（例えば、使用できる保護された経路を通じて）で利用者に届し、保護されていない（平文の）電子メールのメッセージをこの目的で利用することは避ける。 d) 利用者は、認証情報の受領を知らせる。 e) 事業があらかじめ定めた又は提供した初期設定の認証情報は、システム又はソフトウェアのインストール直後に変更する。 f) 認証情報の割当ておび管理に関する重要な事象の記録を保持し、記録に機密性を付与する方法は、承認を受ける【例えば、承認された パスワード管理ツール（password vault tool）を使用】。
9.2.4.4	秘密認証情報の割当ての正式な管理プロセスでは、新規、更新又は他の秘密認証情報を発行する前に、利用者の本人確認の手順を確立する。	Sc-S.17.1	認証情報の割当ておび管理のプロセには、次の事項を確実にする。 b) 新規、更新又は他の認証情報を発行する前に、利用者の本人確認の手順を確立する。	予引に関連記載あり			
9.2.4.5	秘密認証情報の割当ての正式な管理プロセでは、他の秘密認証情報は、セキュリティを保つた方法で利用者に渡す。外部関係者を通して渡すことは保護されていない（暗号化していない）電子メールのメッセージを利用することは避ける。	Sc-S.17.1	認証情報の割当ておび管理のプロセには、次の事項を確実にする。 c) 他の認証情報を含む認証情報は、セキュリティを保つた方法で利用者に渡し、保護されていない（平文の）電子メールのメッセージこの目的で利用することは避ける。	予引に関連記載あり			
9.2.4.6	秘密認証情報の割当ての正式な管理プロセでは、他の秘密認証情報は、一人一人に対して一意とし、推測されないものとする。	Sc-S.17.1	【再】認証情報の割当ておび管理のプロセには、次の事項を確実にする。 a) 他の秘密認証情報として登録プロセスに自動的に生成される個人パスワードは個人識別番号（PIN）は、推測不可能であり、各人に対して一意で、かつ、利用者は最初の使用後にそれを変更することが要求される。	予引に関連記載あり			
9.2.4.7	秘密認証情報の割当ての正式な管理プロセでは、利用者は、秘密認証情報の受領を知らせる。	Sc-S.17.1	認証情報の割当ておび管理のプロセには、次の事項を確実にする。 d) 利用者は、認証情報の受領を知らせる。	予引に関連記載あり			
9.2.4.8	秘密認証情報の割当ての正式な管理プロセでは、事業があらかじめ設定した秘密認証情報は、システム又はソフトウェアのインストール直後に変更する。	Sc-S.17.1	認証情報の割当ておび管理のプロセには、次の事項を確実にする。 e) 事業があらかじめ定めた又は提供した初期設定の認証情報は、システムまはソフトウェアのインストール直後に変更する。	予引に関連記載あり			
–	（対応項なし）	Sc-S.17.1	認証情報の割当ておび管理のプロセには、次の事項を確実にする。 f) 認証情報の割当ておび管理に関する重要な事象の記録を保持し、記録に機密性を付与する方法は、承認を受ける。	予引に関連記載あり			
9.2.4.9.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の出来）	5.17.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
9.2.5	利用者アクセス権のレビュー 資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューする。	5.18	アクセス権 管理策 情報及びその他の関連資産へのアクセス権は、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除する。 目的 情報及びその他の関連資産へのアクセスを、事業上の要求事項に従って定義し、認可することを確実にするため。		5.18	アクセス権 統制目標：情報及びその他の関連資産へのアクセス権は、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除する。 目的：情報及びその他の関連資産へのアクセスを、事業上の要求事項に従って定義し、認可することを確実にするため。	
9.2.5.1	利用者のアクセス権は、定められた間隔で見直す。	Sc-5.18.2	【再】物理的及び論理的なアクセス権の定期的なレビューでは、次の事項を考慮する。 a) 同じ組織内での何らかの変更後又は退職後の利用者のアクセス権	子引に関連記載あり	5.18.2	【再】物理的及び論理的なアクセス権の定期的なレビューを実施する。	（5.18.2に対応する項を参照）
9.2.5.2	利用者のアクセス権は、何らかの変更（例えば、昇進、降格、雇用の終了）があった後に見直す。	Sc-5.18.2	【再】物理的及び論理的なアクセス権の定期的なレビューでは、次の事項を考慮する。 a) 同じ組織内での何らかの変更後又は退職後の利用者のアクセス権	子引に関連記載あり			
9.2.5.3	利用者のアクセス権は、利用者の役割が同一組織内で変更された場合、そのアクセス権についてレビュー、新当てもし直す。	Sc-5.18.2	【再】物理的及び論理的なアクセス権の定期的なレビューでは、次の事項を考慮する。 a) 同じ組織内での何らかの変更後又は退職後の利用者のアクセス権	子引に関連記載あり			
9.2.5.4	特権的アクセス権の認可は、利用者のアクセス権より頻繁な間隔でレビューする。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.2.5.5	特権の割当て定められた間隔で点検して、認可されていない特権が取得されていないことを確認する。	8a-8.2.2	【再】この管理策の実施については、次の事項を考慮する。 g) 定期的に、また組織に何か変更があった後に、特権的アクセス権を用いて作業する利用者をレビューし、特権的アクセス権を用いた作業に関して、その利用者が職務、役割、責任及び力量の点でやる適性であるかどうかを検証する。	子引に関連記載あり	8.2.1	【再】特権的アクセス権の割当て及び利用を制限し、管理する。	（8.2.1に対応する項を参照）
9.2.5.6	特権アカウントを変更する際は、定期的なレビューのために変更ログをとる。			子引に関連記載あり			
9.2.6	アクセス権の削除又は修正 全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正する。	5.18	アクセス権 管理策 情報及びその他の関連資産へのアクセス権は、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除する。 目的 情報及びその他の関連資産へのアクセスを、事業上の要求事項に従って定義し、認可することを確実にするため。		5.18	アクセス権 統制目標：情報及びその他の関連資産へのアクセス権は、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除する。 目的：情報及びその他の関連資産へのアクセスを、事業上の要求事項に従って定義し、認可することを確実にするため。	
9.2.6.1	雇用の終了時に、アクセス権を削除する必要があるかどうかを決定し、情報並びに情報処理施設及びサービスに関連する資産に対する個人のアクセス権を削除又は一時停止を行う。	Sc-5.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスは、次の事項を含む。 d) ある者が情報及びその他の関連資産にアクセスする必要がなくなった場合にアクセス権を削除する。特に、組織を去った利用者のアクセス権を時機を失せずに削除する。	子引に関連記載あり	5.18.1	【再】エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て及び無効化のプロセスを監視し、アクセス権の割り当て、変更及び削除する。	（5.18.1に対応する項を参照）
9.2.6.2	雇用を変更した場合、新規の業務において承認されていない全てのアクセス権を削除する。	Sc-5.18.3	情報及びその他の関連資産への利用者のアクセス権は、雇用の変更又は終了の前に、次に示すリスク因子の評価に基づいて、レビュー、調整又は削除する。 a) 雇用の終了又は変更が、利用者の側によるものか又は経営側によるものかどうか、及び雇用の終了の理由 b) 利用者の現時点の責任 c) 現在アクセス可能な資産の価値	子引に関連記載あり	5.18.2	【再】物理的及び論理的なアクセス権の定期的なレビューを実施する。	（5.18.2に対応する項を参照）
9.2.6.3	削除又は修正が望ましいアクセス権には、物理的な及び論理的なアクセスに関するものを含める。	Sc-5.18.1	エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスは、次の事項を含む。 j) 物理的及び論理的アクセス権の削除又は調整	子引に関連記載あり	5.18.1	【再】エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て及び無効化のプロセスを監視し、アクセス権の割り当て、変更及び削除する。	（5.18.1に対応する項を参照）
9.2.6.4	従業員及び契約相手のアクセス権を特定するあゆる文書に、アクセス権の削除又は修正を反映する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.2.6.5	訴わていく従業員 又は外部の利用者が引き続き有効な利用者ID のパスワードを知っている場合、雇用・契約・合意の終了又は変更に当たって、これらのパスワードを変更する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.2.6.6	情報及び情報処理施設に関連する資産へのアクセス権は、雇用の終了又は変更の前に、雇用の終了又は変更が、従業員等以外の部の利用者の側によるものか又は経営側によるものかどうか、及び雇用の終了の理由、従業員、外部の利用者、又は他の利用者の現時点の責任、現在アクセス可能な資産の価値のリスク因子の評価に応じて、縮小又は削除する。	Sc-5.18.3	【再】情報及びその他の関連資産への利用者のアクセス権は、雇用の変更又は終了の前に、次に示すリスク因子の評価に基づいて、レビュー、調整又は削除する。 a) 雇用の終了又は変更が、利用者の側によるものか又は経営側によるものかどうか、及び雇用の終了の理由 b) 利用者の現時点の責任 c) 現在アクセス可能な資産の価値	子引に関連記載あり	5.18.2	【再】物理的及び論理的なアクセス権の定期的なレビューを実施する。	（5.18.2に対応する項を参照）
9.3	利用者の責任 管理目的：利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。	5.17	認証情報 管理策 認証情報の割当て及び管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理する。 目的 適切なエンティティ認証を確実にし、認証プロセスの失敗を防ぐため。		5.17	認証情報 統制目標：認証情報の割当て及び管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理する。 目的：適切なエンティティ認証を確実にし、認証プロセスの失敗を防ぐため。	
9.3.1	秘密認証情報の利用 秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求する。						
9.3.1.1	全ての利用者に、秘密認証情報を秘密にしており、関係当局の者を含む他者に秘密認証情報が漏えいしないよう助言する。	Sc-5.17.2	認証情報にアクセスする又はそれを使用する者に、次の事項を確実に行うよう助言する。 a) パスワードなどの秘密認証情報は機密を保つ。個人の秘密認証情報を他人と共有しない。職務の利用者に、又は個人でないエンティティにつも（組）付けられている識別情報に対して使用する秘密認証情報は、認可された人だけ共有する。	子引に関連記載あり	5.17.2	【再】認証情報にアクセス又は使用する者に、機密性を保つために必要な事項を伝達する。	（5.17.2に対応する項を参照）
9.3.1.2	全ての利用者に、秘密認証情報を、例えば、紙、ソフトウェアのファイル、携帯用の機器に、記録して保管しないように助言する。ただし、記録がセキュリティを確保して保管され、その保管方法が承認されている場合には、この限りではない。（例えば、パスワード保管システム：password vault）	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.3.1.3	全ての利用者に、秘密認証情報に対する危険の兆候が見られる場合には、その秘密認証情報を変更するよう助言する。	Sc-5.17.2	認証情報にアクセスする又はそれを使用する者に、次の事項を確実に行うよう助言する。 b) 影響を受けた又は侵害された認証情報は、侵害の知らせ又はその他の兆候があれば、直ちに変更する。	子引に関連記載あり	5.17.2	【再】認証情報にアクセス又は使用する者に、機密性を保つために必要な事項を伝達する。	（5.17.2に対応する項を参照）
9.3.1.4	全ての利用者に、秘密認証情報としてパスワードを用いる場合は、十分な最短文字数をもつ「良い品質のパスワードを設定するよう助言する（「良い品質のパスワードとは、次の条件を満たすものとする。1) 覚えやすい。2) 当人の関連情報（例えば、名前、電話番号、誕生日）から、他の者が容易に推測できる又は調べられる事項に基づかない。3) 辞書攻撃にでも、容易でない（すなわち、辞書に含まれる語から成り立っていない。）。4) 同一文字を連ねただけ、数字だけ、又はアルファベットだけの文字列ではない。5) 他のパスワードを再利用する場合、最初のログオン時点で変更する。）。	Sc-5.17.2	認証情報にアクセスする又はそれを使用する者に、次の事項を確実に行うよう助言する。 c) パスワードや認証情報として使用する場合、例えば、次のような厳選な個行の推奨事項に従って強力なパスワードを選択する。 1) パスワードは、当人に関する情報から、他の者が容易に推測できる又は調べられる事項に基づかない。 2) パスワードは辞書の単語又はそれらの組合せに基づかない。 3) 覚えやすいパスフレーズを使用。英数字及び特殊文字を含めるように。 4) パスワードに適う限り長くする長さを定める。	子引に関連記載あり			
9.3.1.5	全ての利用者に、個人用の秘密認証情報を共有しないよう助言する。	Sc-5.17.2	【再】認証情報にアクセスする又はそれを使用する者に、次の事項を確実に行うよう助言する。 a) パスワードなどの秘密認証情報は機密を保つ。個人の秘密認証情報を他人と共有しない。職務の利用者に、又は個人でないエンティティにつも（組）付けられている識別情報に対して使用する秘密認証情報は、認可された人だけ共有する。	子引に関連記載あり			
9.3.1.6	全ての利用者に、自動ログオン手順において、秘密認証情報としてパスワードを用い、かつ、そのパスワードを保管する場合、パスワードの適切な保護を確実にするよう助言する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.3.1.7	全ての利用者に、業務目的のものと業務目的でないものに、同じ秘密認証情報を用いないよう助言する。	Sc-5.17.2	認証情報にアクセスする又はそれを使用する者に、次の事項を確実に行うよう助言する。 d) 異なるサービス及びシステム間で同じパスワードを使用しない。	子引に関連記載あり	5.17.2	【再】認証情報にアクセス又は使用する者に、機密性を保つために必要な事項を伝達する。	（5.17.2に対応する項を参照）

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
9.4 9.4.1	システム及びアプリケーションのアクセス制御 管理目的：システム及びアプリケーションへ、認可されていないアクセスを防止するため。 情報へのアクセス制限 情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制御する。	8.3	情報へのアクセス制限 管理策 情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制御する。 目的 情報及びその他の関連資産への認可されたアクセスだけを確実にし、認可されていないアクセスを防止するため。		8.3	情報へのアクセス制限 統制目標：情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関するポリシー固有の方針に従って、制御する。 目的：情報及びその他の関連資産への認可されたアクセスだけを確実にし、認可されていないアクセスを防止するため。	
9.4.1.1	アクセスへの制限は、個々の業務用アプリケーションの要求事項に基づき、定められたアクセス制御方針に従う。	8a-8.3.1	情報及びその他の関連資産へのアクセスは、確立されたトピック固有の方針に従って制御する。	手引に関連記載あり	8.3.1	情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関する方針に従って、制御する。	アクセス制限の要求事項を満たすために、次の事項を考慮する。 a）未知の利用者識別情報又は匿名の者による、取扱いに慎重を要する情報へのアクセスを許可しない。公開アクセス又は匿名アクセスは、取扱いに慎重を要する情報を含まない保管場所に対し許可する。 b）システム、アプリケーション及びサービスにもう情報へのアクセスを制御するための構成の仕組みを提供する。 c）利用者がアクセスできるデータを制御する。 d）どの識別情報又は識別情報のグループがどのアクセス権（読出し、書込み、削除、実行など）をもつかを制御する。 e）取扱いに慎重を要するアプリケーション、アプリケーションデータ又はシステムを隔離するための、物理的又は論理的なアクセス制御を提供する。 次の場合には、初期にとって高い価値をもつ取扱いに慎重を要する情報を保護するための動的アクセス管理手法及びプロセスの採用を検討する。 a）誰がどの期間、どのように情報にアクセスできるかを細かく制御する必要がある。 b）情報を組織外の人々と共有し、誰がそれにアクセスできるかを制御する。 c）情報の使用法及び配布ポリシを用いて動的に管理する。 d）認可されていない変更、複製及び配布（印刷を含む。）から情報を保護する。 e）情報の使用を監視する。 f）将来、調査が必要になった場合に備えて、情報の変更を記録する。 動的アクセス管理手法は、次の事項を含め、情報をそのライフサイクル（すなわち、作成、処理、保存、送信及び処分）を通じて保護する。 a）次の事項を考慮して、個別の事例に基づき動的アクセス管理に関する規則を確立する。 1）識別情報、装置・機器、場所又はアプリケーションに基づいてアクセス許可を与える。 2）動的アクセス管理手法を用いてその情報を保護する必要があるかを決定するために分類体系を活用する。 b）運用、監視及び報告のプロセスを確立し、技術基盤を支援する。
9.4.1.2	アクセス制限の要求事項を満たすために、アプリケーションシステム機能は不可欠な機能のみを提供し、その機能へのアクセスを制御するためのメニューを提供する。	8a-8.3.2	アクセス制限の要求事項を満たすために、次の事項を考慮する。 b）システム、アプリケーション及びサービスにもう情報へのアクセスを制御するための構成の仕組みを提供する。	手引に関連記載あり			
9.4.1.3	アクセス制限の要求事項を満たすために、利用者がアクセスできる機能、ポート、プロトコル、サービス、データを制御する。	8a-8.3.2	アクセス制限の要求事項を満たすために、次の事項を考慮する。 c）利用者がアクセスできるデータを制御する。	手引に関連記載あり			
9.4.1.4	アクセス制限の要求事項を満たすために、利用者のアクセス権（例えば、読出し、書込み、削除、実行）を制御する。	8a-8.3.2	アクセス制限の要求事項を満たすために、次の事項を考慮する。 d）どの識別情報又は識別情報のグループがどのアクセス権をもつかを制御する。	手引に関連記載あり			
–	（対応項なし）	8a-8.3.2	アクセス制限の要求事項を満たすために、次の事項を考慮する。 a）未知の利用者識別情報又は匿名の者による、取扱いに慎重を要する情報へのアクセスを許可しない。公開アクセスは匿名アクセスは、取扱いに慎重を要する情報を含まない保管場所に対し許可する。	手引に関連記載あり			
9.4.1.5	アクセス制限の要求事項を満たすために、他のアプリケーションのアクセス権を制御する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.4.1.6	アクセス制限の要求事項を満たすために、出力に含まれる情報を制限する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.4.1.7	アクセス制限の要求事項を満たすために、取扱いに慎重を要するアプリケーション、アプリケーションデータ又はシステムを隔離するための、物理的又は論理的なアクセス制御を提供する。	8a-8.3.2	アクセス制限の要求事項を満たすために、次の事項を考慮する。 a）取扱いに慎重を要するアプリケーション、アプリケーションデータ又はシステムを隔離するための、物理的又は論理的なアクセス制御を提供する。	手引に関連記載あり	8.3.1	[再]情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関する方針に従って、制御する。	（8.3.1に対応する項を参照）
–	（対応項なし）	8a-8.3.3	次の場合には、初期にとって高い価値をもつ取扱いに慎重を要する情報を保護するための動的アクセス管理手法及びプロセスの採用を検討する。 a）誰がどの期間、どのように情報にアクセスできるかを細かく制御する必要がある。 b）情報を組織外の人々と共有し、誰がそれにアクセスできるかを制御する。 c）情報の使用法及び配布ポリシを用いて動的に管理する。 d）認可されていない変更、複製及び配布（印刷を含む。）から情報を保護する。 e）情報の使用を監視する。 f）将来、調査が必要になった場合に備えて、情報の変更を記録する。	手引に関連記載あり			
–	（対応項なし）	8a-8.3.4	動的アクセス管理手法は、次の事項を含め、情報をそのライフサイクル（すなわち、作成、処理、保存、送信及び処分）を通じて保護する。 a）次の事項を考慮して、個別の事例に基づき動的アクセス管理に関する規則を確立する。 1）識別情報、装置・機器、場所又はアプリケーションに基づいてアクセス許可を与える。 2）動的アクセス管理手法を用いてその情報を保護する必要があるかを決定するために分類体系を活用する。 b）運用、監視及び報告のプロセスを確立し、技術基盤を支援する。	手引に関連記載あり			
–	（対応項なし）	8a-8.3.5	動的アクセス管理システムは、次の方法によって情報を保護する。 a）情報にアクセスする際に、認証、適切な資格情報又は証明書を要求する。 b）アクセスを、例えば、規定された時間帯に制限する。 c）情報を保護するために暗号化を利用する。 d）情報の印刷許可を定義する。 e）誰が情報にアクセスし、その情報がどのように使用されたかを記録する。 f）情報の悪用のおそれが検知された場合に警報を上げる。	手引に関連記載あり			
9.4.1.8.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の出典）	8.3.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
9.4.2	セキュリティに配慮したログオン手順 アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御する。	8.5	セキュリティを保った認証 管理策 セキュリティを保った認証技術及び手順を、情報へのアクセス制限、及びアクセス制御に関するトピック固有の方針に基づいて備える。 目的 システム、アプリケーション及びサービスへのアクセスを許可するときに、利用者又はエンティティをセキュリティを保って認証することを確実にするため。		8.5	セキュリティを保った認証 統制目標：セキュリティを保った認証技術及び手順を、情報へのアクセス制限、及びアクセス制御に関するトピック固有の方針に基づいて備える。 目的：システム、アプリケーション及びサービスへのアクセスを許可するときに、利用者又はエンティティをセキュリティを保って認証することを確実にするため。	
9.4.2.1	利用者が提示する識別情報を検証するために、適切な認証技術を選択する。	8a-8.5.1	利用者、ソフトウェア、メッセージ、及びその他のエンティティが提示する識別情報を検証するために、適切な認証技術を選択する。	手引に関連記載あり	8.5.1	セキュリティを保った認証技術及び手順は、情報へのアクセス制限、及びアクセス制御に関する方針に基づいて、実施する。	利用者、ソフトウェア、メッセージ、及びその他のエンティティが提示する識別情報を検証するために、適切な認証技術を選択する。 認証の強度は、アクセスする情報の分類に適したものを選択する。 強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、ディジタル証明書、スマートカード、トークン、生体認証などの認証方法を用いる。 重要な情報システムへアクセスするために、認証情報に追加の認証要素を加える（多要素認証とも呼ばれる。）。知識、所持物、生体情報など、複数の認証要素を組み合わせて使用することで、認可されていないアクセスの可能性を減らすことが可能である。特定の状況下においては、多要素認証と他の手法を組み合わせて、あらかじめ定義したルールのパターンに基づく追加の要素も条件として要求することが可能である。このルールのパターンには、通常と異なる場所からのアクセス、通常と異なる頻度・機器からのアクセス、通常と異なる時間でのアクセスなどがある。 生体認証情報は、機密性が損なわれた場合は無効化する。 使用の条件（例えば、湿気又は加齢）によっては、生体認証が利用できないことに備えるため、生体認証は少なくとも一つの代替の認証手法を与える。 ログオンの手順及び技術は、次の事項を考慮して実装する。 a）認可されていない利用者にその要なする助ける提供することを避けるために、取扱いに慎重を要するシステム又はアプリケーションの情報を、ログオン手順が正常に終了するまで表示しない。 b）システム、アプリケーション、又はサービスへのアクセスは、認可されている利用者に限定するでない一般的な警告を表示する。 c）ログオン手順中に、認可されていない利用者の助けになるようなメッセージを表示しない（例えば、エラー状態が発生しても、システムからは、データベースの部分が正しい少又は間違っているかを示すことは望ましくない）。 d）ログオン情報の妥当性確認は、全てのスカテータが完了した時点で行行う。 e）利用者名及び/パスワードに関する組当の攻撃でログオンしようとする試みから保護する（例えば、コンピュータ人間と区別する完全に自動化された公開チューリングテスト（CAPTCHA）を使用する。あらかじめ定義した回数の誤行失敗の後にパスワード/セットを要求する。又は最大と定めた回数のエラーの後に利用者をブロックする。）。 f）失敗した試み及び成功した試みのログをとる。 g）ログオン制御への違反又は違反が試みられた可能性を検知した場合には、セキュリティ事象として取り上げる（例えば、誤ったパスワードの試行が特定の回数に達したときに利用者及び組織のシステム実務管理者に警告を送信する。）。 h）ログオンが成功裏に終了した時点で、次の情報を別の手段で表示又は送信する。 1）前回成功裏にログオンできた日時 2）前回のログオン以降、失敗したログオンの試みがある場合には、その詳細 i）入力したパスワードを平文で表示しない。場合によっては、利用者のログオンを容易にするため、この機能を無効化する必要がある可能性がある（例えば、アカウンビリティのために、又はエラーの経過記載によって利用者がブロックされないようにするために）。 j）ネットワークニファプログラムで構捉されることを避けるため、ネットワークを介してパスワードを平文で通信しない。 k）リスクの高い場所（例えば、組織のセキュリティ管理外にある公共の場所又は外部の区域、利用者エンドポイント機器）では、特に、使用せずにあらかじめ定めた時間が経過したセッションを終了する。 l）リスクの高いリアプリケーションのセキュリティを高め、認可されていないアクセスの危険性を低減するために、接続の継続時間を制御する。
9.4.2.2.B	強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、暗号による手段、スマートカード、トークン、生体認証などの認証方法を用いる。	8a-8.5.3	強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、ディジタル証明書、スマートカード、トークン、生体認証などの認証方法を用いる。	手引に関連記載あり			
9.4.2.3	システム又はアプリケーションへログオンするための手順は、認可されていないアクセスの機会を最小限に抑えるように設計する。	8a-8.5.7	システム又はアプリケーションにログオンする手順は、認可されていないアクセスのリスクを最小限に抑えるように設計する。	手引に関連記載あり			
9.4.2.4	ログオン手順では、認可されていない利用者に無用な助けを与えないために、システム又はアプリケーションについての情報の開示は、最小限にする。	8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 a）認可されていない利用者にその要なする助けを提供することを避けるために、取扱いに慎重を要するシステム又はアプリケーションの情報を、ログオン手順が正常に終了するまで表示しない。	手引に関連記載あり			
9.4.2.5	システム又はアプリケーションの識別子を、ログオン手順が正常に終了するまで表示しない。	8a-8.5.8	【再】ログオンの手順及び技術は、次の事項を考慮して実装する。 a）認可されていない利用者にその要なする助けを提供することを避けるために、取扱いに慎重を要するシステム又はアプリケーションの情報を、ログオン手順が正常に終了するまで表示しない。	手引に関連記載あり			
9.4.2.6	ログオン手順では、「コンピュータへのアクセスは、認可されている利用者に限定する」という警告を表示する。	8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 b）「システム、アプリケーション、又はサービスへのアクセスは、認可されている利用者に限定するでない一般的な警告を表示する。	手引に関連記載あり			
9.4.2.7	ログオン手順中に、認可されていない利用者の助けとなるようなメッセージを表示しない。	8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 c）ログオン手順中に、認可されていない利用者の助けとなるようなメッセージを表示しない。	手引に関連記載あり			
9.4.2.8	ログオン手順では、ログオン情報の妥当性検証は、全ての入力データが完了した時点で行行う。（誤り条件が発生しても、システムからは、データベースの部分が正しい少又は間違っているかを開示しない。	8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 d）ログオン情報の妥当性確認は、全ての入力データが完了した時点で行行う。	手引に関連記載あり			
9.4.2.9	総当たり攻撃でログオンしようとする試みから保護する。	8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 e）利用者名及び/パスワードに関する総当たり攻撃でログオンしようとする試みから保護する。	手引に関連記載あり			
9.4.2.10	ログオン手順では、失敗した試み及び成功した試みのログをとる。	8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 f）失敗した試み及び成功した試みのログをとる。	手引に関連記載あり			
9.4.2.11	ログオン制御への違反又は違反が試みられた可能性が検知された場合には、セキュリティ事象として取り上げる。	8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 g）ログオン制御への違反又は違反が試みられた可能性を検知した場合には、セキュリティ事象として取り上げる。	手引に関連記載あり			
9.4.2.12	ログオンが成功裏に終了した時点で、①前回成功裏にログオンできた日時、②前回のログオン以降、失敗したログオンの試みがある場合は、その詳細を表示する。	8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 h）ログオンが成功裏に終了した時点で、次の情報を別の手段で表示又は送信する。 1）前回成功裏にログオンできた日時 2）前回のログオン以降、失敗したログオンの試みがある場合は、その詳細	手引に関連記載あり			
9.4.2.13	ログオン手順では、入力したパスワードは表示しない。	8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 i）入力したパスワードを平文で表示しない。場合によっては、利用者のログオンを容易にするため、この機能を無効化する必要がある可能性がある。	手引に関連記載あり			
9.4.2.14	ログオン手順では、ネットワークを介してパスワードを平文で通信しない。	8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 j）ネットワークニファプログラムで構捉されることを避けるため、ネットワークを介してパスワードを平文で通信しない。	手引に関連記載あり			
9.4.2.15	ログオン手順では、リスクの高い場所（例えば、組織のセキュリティ管理外にある公共の場所又は外部の区域、モバイル機器）では特に、あらかじめ定めた条件に合致したセッションは終了する。	8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 k）リスクの高い場所では、特に、使用せずにあらかじめ定めた時間が経過したセッションを終了する。	手引に関連記載あり			
9.4.2.16	ログオン手順では、リスクの高いリアプリケーションのセキュリティを高めるために、接続時間を制限し、認可されていないリアセスの危険性を低減する。	8a-8.5.8	ログオンの手順及び技術は、次の事項を考慮して実装する。 l）リスクの高いリアプリケーションのセキュリティを高め、認可されていないリアセスの危険性を低減するために、接続の継続時間を制御する。	手引に関連記載あり			
9.4.3	パスワード管理システム パスワード管理システムは、対話式とすること。また、良質なパスワードを確実にするものとする。	5.17	認証情報 管理策 認証情報の割当て及び管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理する。 目的 適切なエンティティ認証を確実にし、認証プロセスの失敗を防ぐため。		5.17	認証情報 統制目標：認証情報の割当て及び管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理する。 目的：適切なエンティティ認証を確実にし、認証プロセスの失敗を防ぐため。	
9.4.3.1	パスワードの管理システムでは、責任追跡性を維持するために、それぞれの利用者ID及びパスワードを使用させるようにする。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.4.3.2	パスワードの管理システムは、利用者に自分のパスワードの選択及び変更を許可し、また、入力誤りを考慮した確認手順を組み入れる。	Sc-5.17.3	パスワード認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 a）利用者が自分のパスワードを選択及び変更できるようにし、入力エラーに対処するための確認手順を含める。	手引に関連記載あり	5.17.3	パスワード認証を使用する場合は、機密性を保つために必要な機能を備えたものを利用する。	パスワード認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 a）利用者が自分のパスワードを選択及び変更できるようにし、入力エラーに対処するための確認手順を含める。 b）優良な慣行の推奨事項［5.17.2c)参照］に従って強固なパスワードを使用させる。 c）パスワードは、最初のログイン時に利用者に変更させる。 d）必要に応じて、例えば、セキュリティインシデントの後に、又は有効な識別情報（例えば、共有識別情報）のパスワードを知っている利用者の雇用の終了若しくは変更の時に、パスワードを変更させる。 e）以前のパスワードの再利用を防止する。 f）一般的に使われるパスワード、盗むパスワードなどが侵されたときにシステムで侵害された利用者名及びパスワードの組合せの使用を防止する。 g）パスワードは、入力時に、画面上に表示しない。 h）パスワードは、保護した形態で保存し、伝達する。 パスワードの暗号化及び/ハッシュ化は、パスワードに関する承認された暗号技術に従って実行する（8.24参照）。
9.4.3.3	パスワードの管理システムは、質の良いパスワードを選択させるようにする。例えば、強固なパスワードに必要な桁数や複雑さをもつパスワードとする。	Sc-5.17.3	パスワード認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 b）優良な慣行の推奨事項に従って強固なパスワードを使用させる。	手引に関連記載あり			
9.4.3.4	パスワードの管理システムでは、パスワードは、最初のログオン時に利用者に変更させるようにする。	Sc-5.17.3	パスワード認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 c）パスワードは、最初のログイン時に利用者に変更させる。	手引に関連記載あり			
9.4.3.5	パスワードの管理システムでは、パスワードは、定期的又は必要に応じて変更させるようにする。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.4.3.6	パスワードの管理システムでは、以前に用いられたパスワードの記録を維持し、再使用を防止する。	Sc-5.17.3	パスワード認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 e）以前のパスワードの再利用を防止する。	手引に関連記載あり	5.17.3	【再】パスワード認証を使用する場合は、機密性を保つために必要な機能を備えたものを利用する。	（5.17.3c.対応する項を参照）
9.4.3.7	パスワードの管理システムでは、パスワードは、入力時に、画面上に表示しないようにする。	Sc-5.17.3	パスワード認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 g）パスワードは、入力時に、画面上に表示しない。	手引に関連記載あり			
9.4.3.8	パスワードの管理システムでは、パスワードのファイルは、アプリケーションシステムのデータとは別に保存する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.4.3.9	パスワードの管理システムでは、パスワードは、保護した形態で保存し、伝達する。	Sc-5.17.3	パスワード認証情報として使用する場合、パスワード管理システムは、次の事項を行う。 h）パスワードは、保護した形態で保存し、伝達する。	手引に関連記載あり	5.17.3	【再】パスワード認証を使用する場合は、機密性を保つために必要な機能を備えたものを利用する。	（5.17.3c.対応する項を参照）
9.4.4	特権的なユーティリティプログラムの使用 システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。	8.18	特権的なユーティリティプログラムの使用 管理策 システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。 目的 ユーティリティプログラムの使用が、システム及びアプリケーションについての情報セキュリティ管理策に悪を与えないことを確実にするため。		8.18	特権的なユーティリティプログラムの使用 統制目標：システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。 目的：ユーティリティプログラムの使用が、システム及びアプリケーションについての情報セキュリティ管理策に悪を与えないことを確実にするため。	
9.4.4.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用のための識別、認証及び認可手順を整備し、使用する。	8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用において、ユーティリティプログラムを使用する要員の一意の識別を含む、ユーティリティプログラムの識別、認証及び認可手順の使用	手引に関連記載あり	8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用において必要な要求事項を定義し、対策を実施する。	クラウドサービス内で利用する全てのユーティリティプログラムのための要求事項を特定する。 システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用において、次の事項を考慮する。 a）可能な限り少人数の信頼できる認可された利用者だけに限定した、ユーティリティプログラムの使用制限（8.2参照）

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
9.4.4.2	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムは、アプリケーションソフトウェアから分離する。	8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 g) 少なくとも、アプリケーションソフトウェアからのユーティリティプログラムの論理的分離、実施できる場合、ユーティリティプログラムのネットワーク通信をアプリケーショントラフィックから分離	手引に関連記載あり			b) ユーティリティプログラムを使用する要員の一意の識別を含む、ユーティリティプログラムの識別、認証及び認可手順の使用 c) ユーティリティプログラムの認可レベルの明確化及び文書化 d) ユーティリティプログラムを臨時に用いる場合の認可 e) 権限の分離が必要な場合に、システム上のアプリケーションにアクセスする利用者に、ユーティリティプログラムの使用を不可とする f) 全ての不要なユーティリティプログラムの除去又は無効化 g) 少なくとも、アプリケーションソフトウェアからのユーティリティプログラムの論理的分離、実施できる場合、ユーティリティプログラムのネットワーク通信をアプリケーショントラフィックから分離 h) ユーティリティプログラムの使用の制限（例えば、認可されたシステム変更のための期間での利用） i) ユーティリティプログラムの全ての使用に関するログ 通常の操作手順又はセキュリティ手順を回避することのできる全てのプログラムを、認可された要員に厳重に制限し、そのようなプログラムの利用を定期的にレビュー、監査する。
9.4.4.3	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、可能な限り少人数の信頼できる認可された利用者だけに限定する。	8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 a) 可能な限り少人数の信頼できる認可された利用者だけに限定した、ユーティリティプログラムの使用制限	手引に関連記載あり			
9.4.4.4	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムを臨時に用いる場合の認可手順を整備する。	8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 d) ユーティリティプログラムを臨時に用いる場合の認可	手引に関連記載あり			
9.4.4.5	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用を制限する。（例えば、認可されたシステム変更のための期間での利用）	8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 h) ユーティリティプログラムの使用の制限	手引に関連記載あり			
9.4.4.6	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの全ての使用に関するログを取得する。	8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 i) ユーティリティプログラムの全ての使用に関するログ	手引に関連記載あり			
9.4.4.7	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの認可レベルを明確にし、文書化する。	8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 c) ユーティリティプログラムの認可レベルの明確化及び文書化	手引に関連記載あり			
9.4.4.8	システム及びアプリケーションによる制御を無効にすることのできる不要なユーティリティプログラムは全て除去又は無効化する。	8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 f) 全ての不要なユーティリティプログラムの除去又は無効化	手引に関連記載あり			
9.4.4.9	権限の分離が必要な場合には、システム上のアプリケーションへのアクセス権をもつ利用者に対して、システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用を禁止する。	8b-8.18.1	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用においては、次の事項を考慮する。 e) 権限の分離が必要な場合に、システム上のアプリケーションにアクセスする利用者に、ユーティリティプログラムの使用を不可とする	手引に関連記載あり			
9.4.4.10.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）			
9.4.4.11.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）			
9.4.5	プログラムソースコードへのアクセス制御 プログラムソースコードへのアクセスは、制御する。	8.4	ソースコードへのアクセス 管理策 ソースコード、開発ツール、及びソフトウェアライブラリへの読取り及び書込みアクセスを適切に管理する。 目的 認可されていない機能が入り込むことを防止し、意図しない又は悪意のある変更を回避し、価値の高い知的財産の機密性を維持するため。		8.4	ソースコードへのアクセス 統制目標：ソースコード、開発ツール、及びソフトウェアライブラリへの読取り及び書込みアクセスを適切に管理する。 目的：認可されていない機能が入り込むことを防止し、意図しない又は悪意のある変更を回避し、価値の高い知的財産の機密性を維持するため。	
9.4.5.1	プログラムソースコード及び関連書類（例えば、設計書、仕様書、検証計画書、妥当性確認計画書）へのアクセスは、認可されていない機能が入り込むことを防止し、意図しない変更を回避し、価値の高い知的財産の機密性を維持するために、厳重に管理する。	8a-8.4.1	ソースコード、関連書類及び開発ツールへのアクセスは、厳重に管理する。	手引に関連記載あり	8.4.2	ソースコード関連書類及び開発ツールへの読取り及び書込みのアクセスを管理する。	ソースコード、関連書類（例えば、設計書、仕様書、検証計画書、妥当性確認計画書）及び開発ツール（例えば、コンパイラ、ビルダ、統合ツール、テストプラットフォーム及びテスト環境）へのアクセスは、厳重に管理する。 ソースコードについては、できればソースコード管理システムにおいて、コードを集中保管して管理することによってこれを達成することが可能である。 ソースコードへの読取りアクセス及び書込みアクセスは、必要に応じて要員の役割に基づいて制限する。例えば、ソースコードへの読取りアクセスは組織内で広く提供することはできるが、ソースコードへの書込みアクセスは、特権をもつ要員又は指定された管理責任者だけに認める。 ソースコードへの読取りアクセスは、特権をもつ要員又は指定された管理責任者だけに認める。 コード部品を組織内の複数の開発者が使用する場合には、一元化した一つのリポジトリへの読取りアクセスを提供する。 オープンソースコード又は第三者のコード部品の一元化した外部コードリポジトリへの書込みアクセスは制限する。
–	（対応項なし）	（8a-8.4.1参考）	ソースコードについては、できればソースコード管理システムにおいて、コードを集中保管して管理することによってこれを達成することが可能である。	手引に関連記載あり			
–	（対応項なし）	8a-8.4.2	ソースコードへの読取りアクセス及び書込みアクセスは、必要に応じて要員の役割に基づいて制限する。	手引に関連記載あり			
–	（対応項なし）	（8a-8.4.2参考）	例えば、ソースコードへの読取りアクセスは組織内で広く提供することはできるが、ソースコードへの書込みアクセスは、特権をもつ要員又は指定された管理責任者だけに認める。	手引に関連記載あり			
–	（対応項なし）	8a-8.4.3	コード部品を組織内の複数の開発者が使用する場合には、一元化したコードリポジトリへの読取りアクセスを提供する。	手引に関連記載あり			
–	（対応項なし）	8a-8.4.4	オープンソースコード又は第三者のコード部品の一元化した外部コードリポジトリへの書込みアクセスは制限する。	手引に関連記載あり			
9.4.5.2	可能な限り、プログラムソースライブラリは、運用システムの中に保持しない。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.4.5.3	プログラムソースコード及びプログラムソースライブラリは、確立した手順に従って管理する。	8a-8.4.5	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 a) プログラムソースコード及びプログラムソースライブラリへのアクセスは、確立した手順に従って管理する。	手引に関連記載あり	8.4.1	プログラムソースコード及びプログラムソースライブラリへの読取り及び書込みのアクセスを管理する。	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 a) プログラムソースコード及びプログラムソースライブラリへのアクセスは、確立した手順に従って管理する。 b) ソースコードへの読取り及び書込みアクセスの許可は、業務上のニーズに基づき、変更又は悪用のリスクに対処するために管理し、かつ、確立された手順に従って行う。 c) ソースコード及び関連情報の更新、並びにソースコードへのアクセスの許可は、変更管理手順（8.32参照）に従って行い、かつ、適切な認可を得た後に行う。 d) 開発者にソースコードリポジトリへの直接アクセスは許可せず、ソースコードに関する読取り及び認可を管理する開発ツールを通じて許可する。 e) プログラムリストは、セキュリティが保たれた環境で保持する。その環境では、読取り及び書込みアクセスを適切に管理し、割り当てる。 f) ソースコードへの全てのアクセス及び全ての変更について、監査ログを維持する。 プログラムソースコードの公開を意図している場合には、その完全性に保証を与える追加の管理策（例えば、ディジタル署名）の使用を考慮する。
9.4.5.4	サポート要員による、プログラムソースライブラリへの無制限のアクセスを許さない。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
9.4.5.5	プログラムソースライブラリ及び関連情報の更新、並びにプログラマへのプログラムソースの発行は、適切な認可を得た後に已だけ実施する。	8a-8.4.5	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 d) 開発者にソースコードリポジトリへの直接アクセスは許可せず、ソースコードに関する読取り及び認可を管理する開発ツールを通じて許可する。	手引に関連記載あり	8.4.1	[再]プログラムソースコード及びプログラムソースライブラリへの読取り及び書込みのアクセスを管理する。	（8.4.1に対応する項を参照）
9.4.5.6	プログラムリストは、セキュリティが保たれた環境で保持する。	8a-8.4.5	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 e) プログラムリストは、セキュリティが保たれた環境で保持する。その環境では、読取り及び書込みアクセスを適切に管理し、割り当てる。	手引に関連記載あり			
9.4.5.7	プログラムソースライブラリへの全てのアクセスについて、監査ログを維持する。	8a-8.4.5	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 f) ソースコードへの全てのアクセス及び全ての変更について、監査ログを維持する。	手引に関連記載あり			
9.4.5.8	プログラムソースライブラリの保守及び複製は、厳しい変更管理手順に従う。	8a-8.4.5	コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。 c) ソースコード及び関連情報の更新、並びにソースコードへのアクセスの許可は、変更管理手順に従って行い、かつ、適切な認可を得た後に已だけ実施する。	手引に関連記載あり			
9.4.5.9	プログラムソースコードの公開を意図している場合には、その完全性を保証するために役立つ追加的な管理策（例えば、ディジタル署名）を実施する。	8a-8.4.6	プログラムソースコードの公開を意図している場合には、その完全性に保証を与える追加の管理策の使用を考慮する。	手引に関連記載あり			
9.5.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		9.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
9.5.1.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）						
9.5.1.1.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.3.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
9.5.1.2.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.3.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
9.5.1.3.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.3.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
9.5.1.4.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.3.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
9.5.2.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		9.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
9.5.2.1.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	予引に関連記載あり（情報セキュリティ管理基準以外の由来）	9.4.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
10	暗号	8.24	暗号の利用 管理策 暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施する。 目的 事業上及び情報セキュリティの要求事項に従い、暗号に関連する法令、規制及び契約上の要求事項を考慮して、情報の機密性、真正性又は完全性を保護するための暗号の適切かつ効果的な利用を確実にするため。		8.24	暗号の利用 統制目標：暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施する。 目的：事業上及び情報セキュリティの要求事項に従い、暗号に関連する法令、規制及び契約上の要求事項を考慮して、情報の機密性、真正性又は完全性を保護するための暗号の適切かつ効果的な利用を確実にするため。	
10.1	暗号による管理策 管理目的：情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。						
10.1.1	暗号による管理策の利用方針 情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施する。						
10.1.1.1	暗号の利用に関する方針は、業務情報を保護するとその一般原則も含め、暗号による管理策の組織全体での使用に関する管理の取組みを考慮して定める。	8c-B.24.1	暗号化を利用する場合、次の事項を考慮する。 a）情報を保護するとその一般原則も含め、組織で定義した暗号に関するトピック固有の方針。暗号技術の利用の便益を最大化し、リスクを最小化し、不適切又は誤った利用を回避するには、暗号の利用に関するトピック固有の方針が必要である。	予引に関連記載あり	8.24.1	情報を保護するとその一般原則も含め、暗号化に関する方針を策定する。	暗号化を利用する場合、次の事項を考慮する。 a）情報を保護するとその一般原則も含め、組織で定義した暗号に関するトピック固有の方針、暗号技術の利用の便益を最大化し、リスクを最小化し、不適切又は誤った利用を回避するには、暗号の利用に関するトピック固有の方針が必要である。 b）要求された保護レベル及び情報の分類を特定し、その結果によって、要求される暗号アルゴリズムの種別、強度及び品質を確立する。 c）持ち運び可能な利用者エンドポイント機器又は記憶媒体に保持され、ネットワークを通じてその機器又は記憶媒体に伝送される情報を保護するための暗号の利用 d）鍵管理に対する助成。これには、暗号鍵の生成及び保護手法、並びに鍵が紛失した場合、危たい（恕）化した場合又は損傷した場合の暗号化された情報の復元手法を含む。 e）次の事項に関する役割及び責任 1）暗号を効果的に利用するための規則の実施 2）鍵生成を含めた鍵管理（8.24参照） f）採用する標準類、並びに組織での利用が承認又は要求されている暗号アルゴリズム。暗号強度、暗号ソリューション及び利用方法 g）暗号化した情報を用いるための、コンテンツ検査（例えば、マルウェアの検出又はコンテンツフィルタリング）に依存する管理策への影響 暗号を効果的に利用するための組織の規則を実施するとおには、世界の様々な地域における暗号技術の利用、及び国境を越える暗号化された情報の流れに関する問題に適用される、規制及び国内の制約を考慮する（5.31参照）。 暗号サービスの外部供給者（例えば、認証局）とのサービスレベルに関する合意又は契約の内容は、賠償責任、サービスの信頼性及びサービス提供の応答時間を扱う（5.22参照）。
10.1.1.2	暗号の利用に関する方針は、リスクアセスメントに基づく、要求される暗号アルゴリズムの種別、強度及び品質を考慮に入れた、要求された保護レベルの識別を考慮して定める。	8c-B.24.1	暗号化を利用する場合、次の事項を考慮する。 b）要求された保護レベル及び情報の分類を特定し、その結果によって、要求される暗号アルゴリズムの種別、強度及び品質を確立する。	予引に関連記載あり			
10.1.1.3	暗号の利用に関する方針は、持ち運び可能な取扱い可能な媒体装置又は通信によって伝送される情報を、保護するための暗号の利用を考慮して定める。	8c-B.24.1	暗号化を利用する場合、次の事項を考慮する。 c）持ち運び可能な利用者エンドポイント機器又は記憶媒体に保持され、ネットワークを通じてその機器又は記憶媒体に伝送される情報を保護するための暗号の利用	予引に関連記載あり			
10.1.1.4	暗号の利用に関する方針は、暗号鍵の保護手法、及び鍵が紛失、危殆又は損傷した場合の暗号化された情報の復元手法を含め、鍵管理に対する助成方々を考慮して定める。	8c-B.24.1	暗号化を利用する場合、次の事項を考慮する。 d）鍵管理に対する助成。これには、暗号鍵の生成及び保護手法、並びに鍵が紛失した場合、危たい（恕）化した場合又は損傷した場合の暗号化された情報の復元手法を含む。	予引に関連記載あり			
10.1.1.5	暗号の利用に関する方針は、この方針の実施の責任や鍵生成を含めた鍵管理に対する責任など、役割及び責任を考慮して定める。	8c-B.24.1	暗号化を利用する場合、次の事項を考慮する。 e）次の事項に関する役割及び責任 1）暗号を効果的に利用するための規則の実施 2）鍵生成を含めた鍵管理	予引に関連記載あり			
10.1.1.6	暗号の利用に関する方針は、組織全体にわたって効果的に実施するために採用する標準類（業務プロセスに用いるソリューションの選択）を考慮して定める。	8c-B.24.1	暗号化を利用する場合、次の事項を考慮する。 f）採用する標準類、並びに組織での利用が承認又は要求されている暗号アルゴリズム。暗号強度、暗号ソリューション及び利用方法	予引に関連記載あり			
10.1.1.7	暗号の利用に関する方針は、暗号化した情報を用いることの、情報内容の検査（例えば、マルウェアの検出）に依存する管理策への影響を考慮して定める。	8c-B.24.1	暗号化を利用する場合、次の事項を考慮する。 g）暗号化した情報を用いるための、コンテンツ検査に依存する管理策への影響	予引に関連記載あり			
10.1.1.8	暗号に関する組織の方針を実施するとおには、世界の様々な地域における暗号技術の利用、及び国境を越える暗号化された情報の流れに関する問題に適用される、規制及び国内の制約を含める。	8c-B.24.2	暗号を効果的に利用するための組織の規則を実施するとおには、世界の様々な地域における暗号技術の利用、及び国境を越える暗号化された情報の流れに関する問題に適用される、規制及び国内の制約を考慮する。	予引に関連記載あり			
–	（対応項なし）	8c-B.24.3	暗号サービスの外部供給者とのサービスレベルに関する合意又は契約の内容は、賠償責任、サービスの信頼性及びサービス提供の応答時間を扱う。	予引に関連記載あり			
–	（対応項なし）	–	（統一基準由来）	令和7年版にて追加（情報セキュリティ管理基準以外の由来）	8.24.3	暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」に基づき、情報システムで使用する暗号及び電子署名のアルゴリズム及び鍵長並びにそれを利用した安全なプロトコルを定める。	特になし。
–	（対応項なし）	–	（統一基準由来）	令和7年版にて追加（情報セキュリティ管理基準以外の由来）	8.24.4	暗号化及び電子署名に使用するアルゴリズム又は鍵長が危たい（恕）化した場合又はそれらを利用した安全なプロトコルに脆弱性が曝露された場合を想定した緊急対応手順を整備する。	特になし。
10.1.1.9.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	8.24.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
10.1.1.10.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	8.24.7	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
10.1.2	鍵管理 暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全体にわたって実施する。	8.24	暗号の利用 管理策 暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施する。 目的 事業上及び情報セキュリティの要求事項に従い、暗号に関連する法令、規制及び契約上の要求事項を考慮して、情報の機密性、真正性又は完全性を保護するための暗号の適切かつ効果的な利用を確実にするため。		8.24	暗号の利用 統制目標：暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施する。 目的：事業上及び情報セキュリティの要求事項に従い、暗号に関連する法令、規制及び契約上の要求事項を考慮して、情報の機密性、真正性又は完全性を保護するための暗号の適切かつ効果的な利用を確実にするため。	
10.1.2.1	方針には、暗号鍵の生成、保管、保存、読出し、配布、使用停止及び破棄を含むライフサイクル全体にわたって必要となる、セキュリティを保つためのプロセスにおいて、暗号鍵を管理するための要求事項を含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承ガイド）	–	（対応項なし）	–
10.1.2.2	組織が同行に従って、暗号アルゴリズム、鍵の長さ及び使用法を確定する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承ガイド）	–	（対応項なし）	–
–	（対応項なし）	8c-B.24.1	暗号化を利用する場合、次の事項を考慮する。 a）情報を保護するとその一般原則も含め、組織で定義した暗号に関するトピック固有の方針。暗号技術の利用の便益を最大化し、リスクを最小化し、不適切又は誤った利用を回避するには、暗号の利用に関するトピック固有の方針が必要である。 b）要求された保護レベル及び情報の分類を特定し、その結果によって、要求される暗号アルゴリズムの種別、強度及び品質を確立する。 c）持ち運び可能な利用者エンドポイント機器又は記憶媒体に保持され、ネットワークを通じてその機器又は記憶媒体に伝送される情報を保護するための暗号の利用 d）鍵管理に対する助成。これには、暗号鍵の生成及び保護手法、並びに鍵が紛失した場合、危たい（恕）化した場合又は損傷した場合の暗号化された情報の復元手法を含む。 e）次の事項に関する役割及び責任 1）暗号を効果的に利用するための規則の実施 2）鍵生成を含めた鍵管理 f）採用する標準類、並びに組織での利用が承認又は要求されている暗号アルゴリズム。暗号強度、暗号ソリューション及び利用方法 g）暗号化した情報を用いるための、コンテンツ検査に依存する管理策への影響	予引に関連記載あり	8.24.2	鍵管理のための暗号鍵を生成、保管、保存、読出し、配布、利用停止、破棄するため及び改変、紛失から保護するために、セキュリティを保つためプロセス及び手順を整備し、実施する。	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 a）種々の暗号システム及び種々のアプリケーションのために鍵を生成する。 b）公開鍵証明書を発行し、入手する。 c）意図するエンティティに鍵を配布する。これには、受領時に、鍵をどのような方法で活性化するか（使える状態にする）も含む。 d）鍵を保管する。これには、即可されている利用者がどのような方法で鍵にアクセスするかも含む。 e）鍵を変更又は更新する。これには、鍵もいつ、どのような方法で変更するかの規則も含む。 f）危たい（恕）化した鍵に対処する。 g）鍵を無効にする（例えば、鍵が危たい（恕）化した場合、又は利用者が組織を離脱した場合（後者の場合には、鍵は保存する。））。これには、鍵をどのような方法で取消し又は非活性化するかも含む。 h）紛失した鍵又は破損した鍵を回復する。 i）鍵をバックアップ又は保存する。 j）鍵を破壊する。 k）鍵管理に関連する活動を記録し、監査する。 l）鍵管理に関する組織の規則に従って鍵を一定期間だけ利用できるように、鍵の活性化及び非活性化の日付を設定する。 m）暗号鍵へのアクセスに関する法的要求（例えば、裁判での経脱として、暗号化された情報を平文で求められた場合）の取扱い。 適切な鍵管理には、暗号鍵を生成、保管、保存、読出し、配布、利用停止及び破棄するため、セキュリティを保つプロセスが必要となる。 全ての暗号鍵は、改変及び紛失から保護する。 秘密鍵及びプライベート鍵は、即可されていない利用及び開示から保護する。 鍵の生成、保管及び保存のために用いる装置は、物理的に保護する。 暗号鍵の完全性に加え、多の事例では、公開鍵の真正性も考慮する。
10.1.2.3	全ての暗号鍵は、改変及び紛失から保護する。	8c-B.24.5	全ての暗号鍵は、改変及び紛失から保護する。	予引に関連記載あり			
10.1.2.4	鍵の生成、保管及び保存のために用いられる装置は、物理的に保護する。	8c-B.24.7	鍵の生成、保管及び保存のために用いる装置は、物理的に保護する。	予引に関連記載あり			
10.1.2.5	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つ手法に基づき、種々の暗号システム及び種々のアプリケーションのための鍵を生成する。	8c-B.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 a）種々の暗号システム及び種々のアプリケーションのために鍵を生成する。	予引に関連記載あり			
10.1.2.6	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つ手法に基づき、公開鍵証明書を発行し、入手する。	8c-B.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 b）公開鍵証明書を発行し、入手する。	予引に関連記載あり			
10.1.2.7	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つ手法に基づき、意図するエンティティに鍵を配布する。これには、受領時に、鍵をどのような方法で活性化するか（使える状態にする）についても含める。	8c-B.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 c）意図するエンティティに鍵を配布する。これには、受領時に、鍵をどのような方法で活性化するか（使える状態にする）も含む。	予引に関連記載あり			
10.1.2.8	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つ手法に基づき、鍵を保管する。これには、即可されている利用者がどのような方法で鍵にアクセスするかも含める。	8c-B.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 d）鍵を保管する。これには、即可されている利用者がどのような方法で鍵にアクセスするかも含む。	予引に関連記載あり			
10.1.2.9	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つ手法に基づき、鍵を変更又は更新する。これには、鍵もいつ、どのような方法で変更するかの規則も含める。	8c-B.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 e）鍵を変更又は更新する。これには、鍵もいつ、どのような方法で変更するかの規則も含む。	予引に関連記載あり			
10.1.2.10	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つ手法に基づき、危殆になった鍵に対処する。	8c-B.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 f）危たい（恕）化した鍵に対処する。	予引に関連記載あり			
10.1.2.11	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つ手法に基づき、鍵を無効にする（例えば、鍵が危殆になった場合、利用者が組織を離脱した場合、後者の場合には、鍵は保存する。）。これには、鍵をどのような方法で取消し又は非活性化するかも含める。	8c-B.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 g）鍵を無効にする。これには、鍵をどのような方法で取消し又は非活性化するかも含む。	予引に関連記載あり			
10.1.2.12	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つ手法に基づき、紛失した鍵又は破損した鍵を回復する。	8c-B.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 h）紛失した鍵又は破損した鍵を回復する。	予引に関連記載あり			
10.1.2.13	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つ手法に基づき、鍵をバックアップ又は保存する。	8c-B.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 i）鍵をバックアップ又は保存する。	予引に関連記載あり			
10.1.2.14	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つ手法に基づき、鍵を破壊する。	8c-B.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 j）鍵を破壊する。	予引に関連記載あり			
10.1.2.15	鍵管理システムは、一連の合意された標準類、手順及びセキュリティを保つ手法に基づき、鍵管理に関連する活動を記録し、監査する。	8c-B.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 k）鍵管理に関連する活動を記録し、監査する。	予引に関連記載あり			
10.1.2.16	不適切な使用を起こりにくくするために、鍵の活性化及び非活性化の期日を定め、これによって、鍵管理の方針で定めた期間内でだけ鍵を使用できるようにする。	8c-B.24.4	鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリティを保つ手法に基づくことを考慮する。 l）鍵管理に関する組織の規則に従って鍵を一定期間だけ利用できるように、鍵の活性化及び非活性化の日付を設定する。	予引に関連記載あり			
10.1.2.17	秘密鍵及びプライベート鍵は、即可されていない利用及び開示から保護するためセキュリティを保つ管理し、公開鍵は、真正性を保つ。	8c-B.24.8	暗号鍵の完全性に加え、多の事例では、公開鍵の真正性も考慮する。	予引に関連記載あり			
10.1.2.18	公開鍵証明書を発行する認証局は、要求された信頼度を提供するために適切な管理策及び手順を備え、認知された組織であることを確認する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承ガイド）	–	（対応項なし）	–
10.1.2.19	暗号サービスの外部供給者（例えば、認証局）とのサービスレベルに関する合意又は契約の内容は、賠償責任、サービスの信頼性及びサービス提供のため応答時間に関する事項を含める。	8c-B.24.3	暗号サービスの外部供給者とのサービスレベルに関する合意又は契約の内容は、賠償責任、サービスの信頼性及びサービス提供の応答時間を扱う。	予引に関連記載あり	8.24.1	【再】情報を保護するとその一般原則も含め、暗号化に関する方針を策定する。	（8.24.1に対応する項を参照）
10.1.2.20.PB	クラウドサービス事業者は、クラウドサービス利用者に、当該利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供する。	–	（統一基準由来）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	8.24.5	クラウドサービス利用者に、当該利用者の管理する情報の暗号化に用いる暗号鍵を管理する機能を提供し、又は当該利用者が暗号鍵を管理する方法についての情報を提供する。	特になし。

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
11	物理的及び環境的セキュリティ	7	物理的管理策		7.1	物理的セキュリティ境界 統制目標：情報及びその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。 目的：組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷及び干渉を防ぐため。	
11.1	セキュリティを保つべき領域 管理目的：組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。	7.1	物理的セキュリティ境界 管理策 情報及びその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。 目的 組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷及び干渉を防ぐため。				
11.1.1	物理的セキュリティ境界 取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。						
11.1.1.1	情報及び情報処理施設のある領域を保護するために、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に基づいて、それぞれの物理的セキュリティ境界の位置及び強度を定める。	7a-7.1.1	物理的セキュリティ境界について、次の事項を、必要な場合には、考慮し、実施する。 a) 境界内に設置している資産の情報セキュリティ要求事項に従って、セキュリティ境界並びにそれぞれの境界の位置及び強度を定める。	手引に関連記載あり	7.1.1	情報及びその他の関連資産のある領域に関する物理的セキュリティ境界を定め、保護する。	物理的セキュリティ境界について、次の事項を、必要な場合には、考慮し、実施する。 a) 境界内に設置している資産の情報セキュリティ要求事項に従って、セキュリティ境界並びにそれぞれの境界の位置及び強度を定める。 b) 情報処理設備を収容した建物又は数地内物理的に適正な境界をもつ（すなわち、境界には開放がなく、又は容易に侵入できる箇所がない。）。数地内の壁構、壁、天井及び床は、堅固な構造物にし、外部に接する全ての扉を、開閉制御の仕組み（例えば、かんぬき、警報装置、窓）によって、認可されていないアクセスから適切に保護する。要員が不在のときには、扉及び窓を施錠し、窓（特に一階の窓）については外部からの保護を考慮する。施錠口の位置も考慮する。 c) セキュリティ境界上にある全ての防火扉は、適切な標準が要求するレベルの抵抗力を確立するために、壁と併せて、警報、監視及び試験を行う。防火扉は、不具合が発生しても安全側に作動するように運用する。
11.1.1.2	情報及び情報処理施設のある領域を保護するために、情報処理施設を収容した建物又は敷地の境界は、物理的に適えてる（すなわち、境界には開放がなく、又は容易に侵入できる箇所がない）。具体的には、以下の4点を行う。 1.敷地内の壁構、壁及び床は、堅固な構造物にする。 2.外部に接する全ての扉を、開閉制御の仕組み（例えば、かんぬき、警報装置、窓）によって、認可されていないアクセスから適切に保護する。 3.要員が不在のときには、扉及び窓を施錠する。 4.窓（特に一階の窓）については外部から保護する。	7a-7.1.1	物理的セキュリティ境界について、次の事項を、必要な場合には、考慮し、実施する。 b) 情報処理設備を収容した建物又は敷地内物理的に適正な境界をもつ（すなわち、境界には開放がなく、又は容易に侵入できる箇所がない）。敷地内の壁構、壁、天井及び床は、堅固な構造物にし、外部に接する全ての扉を、開閉制御の仕組みによって、認可されていないアクセスから適切に保護する。要員が不在のときには、扉及び窓を施錠し、窓（特に一階の窓）については外部からの保護を考慮する。施錠口の位置も考慮する。	手引に関連記載あり			
11.1.1.3	情報及び情報処理施設のある領域を保護するために、敷地又は建物への物理的アクセスを管理する。具体的には、以下の3点を行う。 1.有人の受付又はその他の手段を備える。 2.敷地又は建物へのアクセスは、認可された要員だけに制限する。 3.認可された要員の一覧を作成し維持する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
11.1.1.4	情報及び情報処理施設のある領域を保護するために、認可されていない物理的アクセス及び周囲への悪影響を防止するために、物理的な障壁を設置する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
11.1.1.5	情報及び情報処理施設のある領域を保護するために、以下の2点を行う。 1.セキュリティ境界上にある全ての防火扉は、該当する地域標準、国内標準及び国際標準が要求するレベルの抵抗力を確立するために、壁と併せて、警報機能を備え、監視し、試験する 2.防火扉は、その地域の消防規則に従って、不具合が発生しても安全側に作動するように運用する	7a-7.1.1	物理的セキュリティ境界について、次の事項を、必要な場合には、考慮し、実施する。 c) セキュリティ境界上にある全ての防火扉は、適切な標準が要求するレベルの抵抗力を確立するために、壁と併せて、警報、監視及び試験を行う。防火扉は、不具合が発生しても安全側に作動するように運用する。	手引に関連記載あり	7.1.1	【再】情報及びその他の関連資産のある領域に関する物理的セキュリティ境界を定め、保護する。	（7.1.1に対応する項を参照）
11.1.1.6	情報及び情報処理施設のある領域を保護するために、以下の4点を行う。 1.全ての非常口扉と扉及びアクセス可能な窓を保護するために、侵入者を検知する適切なシステムを、地域標準、国内標準又は国際標準に沿って導入する 2.定期に従って試験を実施する 3.無人の領域では、常に警報装置を作動させる 4.セキュリティと重要な他の領域（例えば、コンピュータ室、通信機器室）にも、常に警報装置を作動させる	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
11.1.1.7	情報及び情報処理施設のある領域を保護するために、組織が自ら管理する情報処理施設と、外部関係者が管理する施設から物理的に分離する。	7a-7.2.2	可能な場合には、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す。	手引に関連記載あり	7.2.1	セキュリティを保つべき領域の物理的入退に関するセキュリティ対策を実施する。	荷物の受渡場所などアクセス場所（受付など）、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。 可能な場合には、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す。 物理的入退の管理策の実施については、次の事項を考慮する。 a) 敷地及び建物へのアクセスは、認可された要員だけに制限する。物理的領域へのアクセス権の管理プロセスに、認可の提供、定期的なレビュー、要員及び外注先各点（5.1参照）。 b) 全てのアクセスについて、物理的な記録又は電子形式の監査証跡を、セキュリティを保って維持及び監視し、全ての記録（5.13参照）及び敷地へに慎重を要する認証情報を保護する。 c) 情報を処理する又は保管する領域へのアクセスを管理するための プセス及び技術的な仕組みを備える。実装する。認証の仕組みには、アクセスカード、生体認証、又はアクセスカード及び秘密の個人識別番号のような二要素認証の仕組みの使用を含む。慎重を要するその他の手段を設定する。 d) 要員が監視している受付エリア、又は敷地周辺には建物への物理的なアクセスを管理するための手段を設定する。 e) 入退の際に要員及び利害関係者の持ち物を検査し、確認する。 注記：持ち物の検査が可能か否かに関して、地域の法令及び規制が存在する可能性がある。 f) すべての要員及び利害関係者に、何らかの形式の、目に見える証明書の着用を要求する。関係者が許可されていない訪問者及び目に見える証明書を着用していない者を見かけた場合には、直ちにセキュリティ要員に知らせる。常勤の従業員、供給者及び訪問者を識別しやすくするために、容積に区別できるバッジの使用を検討する。 g) セキュリティを保つべき領域又は情報処理施設への、供給者の要員によるアクセスは、限定的かつ必要なときに付与する。このアクセスは、認可を必要とし、監視する。 h) 複数の組織の資産を保持する建物の場合、物理的なアクセスのセキュリティには特別な注意を払う。 i) 物理的なインシデントの起こりやすさが高くなった場合に強化できるように物理的セキュリティ対策を設計する。 j) 非常口などの他の入退場所を、認可されていないアクセスから保護する。 k) 物理的な鍵又は認証情報の管理を確実にし、記録落又は每年の鍵監査、及び物理的な鍵又は認証情報へのアクセスの管理を確実にするための鍵管理プロセスを設定する。（認証情報の詳細については5.17参照）。
11.1.2	物理的入退管理策 セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護する。	7.2	物理的入退 管理策 セキュリティを保つべき領域は、適切な入退管理策及びアクセス場所（受付など）によって保護する。 目的 組織の情報及びその他の関連資産に、認可された物理的アクセスだけがなされることを確実にするため。		7.2	物理的入退 統制目標：セキュリティを保つべき領域は、適切な入退管理策及びアクセス場所（受付など）によって保護する。 目的：組織の情報及びその他の関連資産に、認可された物理的アクセスだけがなされることを確実にするため。	
11.1.2.1	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、訪問者の入退の日付及び時刻を記録し、定期的かつイベント発生又はイベントの兆候がある場合に、レビューする。	7a-7.2.4	物理的入退の訪問者に関する管理策では、次の事項を考慮する。 d) 明示的に例外が許可されない限り、全ての訪問者を監視する。	手引に関連記載あり	7.2.2	物理的入退の訪問者に関するセキュリティ対策を実施する。	物理的入退の訪問者に関する管理策では、次の事項を考慮する。 a) 適切な手段によって訪問者のアイデンティティを認証する。 b) 訪問者の出入りの日時を記録する。 c) 特定の認可された目的で、かつ、領域のセキュリティ要求事項及び緊急時の手順に関する指示の下で訪、訪問者にアクセスを許可する。 d) 明示的に例外が許可されない限り、全ての訪問者を監視する。 荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 a) 建物外部からの受渡場所へのアクセスは、特定の認可された要員に制限する。 b) 受渡場所は、配達要員が建物の他の場所に認可されていないアクセスをすることなく荷積み及び荷降ろしであるように設計する。 c) 受渡場所の外扉開は、制限領域への扉が開いているときにはセキュリティを保つ。 d) 入荷物は、受渡場所から移動する前に、爆発物、化学物質又はその他の危険物がないか検査する。 e) 入荷物は、事業所へ持ち込む(また資産の管理手順（5.9及び7.10参照）に従って登録する。 f) 可能な場合には、入荷と出荷とは、物理的に分離した場所で扱う。 g) 入荷物は、輸送中に関連された盗難が起いやを検査する。開封の盗難が見つかった場合には、直ちにセキュリティ要員に報告する。
11.1.2.2	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、アクセスが事前に承認された場合を除いて、全ての訪問者を監督する。	7a-7.2.4	物理的入退の訪問者に関する管理策では、次の事項を考慮する。 b) 訪問者の出入りの日時を記録する。	手引に関連記載あり			
11.1.2.3	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、訪問者には、特定され、認可された目的のためのアクセスだけを許可し、その領域のセキュリティ要求事項及び緊急時の手順についての指示を与える。	7a-7.2.4	物理的入退の訪問者に関する管理策では、次の事項を考慮する。 c) 特定の認可された目的で、かつ、領域のセキュリティ要求事項及び緊急時の手順に関する指示の下でだけ、訪問者にアクセスを許可する。	手引に関連記載あり			
11.1.2.4	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、適切な手段によって、訪問者の識別情報を認証する。	7a-7.2.4	物理的入退の訪問者に関する管理策では、次の事項を考慮する。 a) 適切な手段によって訪問者のアイデンティティを認証する。	手引に関連記載あり			
–	（対応項なし）	7a-7.2.1	荷物の受渡場所などのアクセス場所（受付など）、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。	手引に関連記載あり	7.2.1	【再】セキュリティを保つべき領域の物理的入退に関するセキュリティ対策を実施する。	（7.2.1に対応する項を参照）
–	（対応項なし）	7a-7.2.2	可能な場合には、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す。	手引に関連記載あり			
11.1.2.5	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、適切なアクセス制御（例えば、アクセスカード及び秘密の個人識別番号のような二要素認証の仕組みの使用）を実施する。	7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 c) 情報を処理する又は保管する領域へのアクセスを管理するためのプロセス及び技術的な仕組みを備える。実装する。認証の仕組みには、アクセスカード、生体認証、又はアクセスカード及び秘密の個人識別番号のような二要素認証の仕組みの使用を含む。慎重を要するその他の手段を設定する。 d) 要員が監視している受付エリア、又は敷地周辺には建物への物理的なアクセスを管理するための手段を設定する。	手引に関連記載あり			
11.1.2.6	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、秘密情報を処理又は保管する領域へのアクセスを、認可された者だけに制限する。	7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 a) 敷地及び建物へのアクセスは、認可された要員だけに制限する。物理的領域へのアクセス権の管理プロセスに、認可の提供、定期的なレビュー、要員及び失効を含める。	手引に関連記載あり			
11.1.2.7	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、全てのアクセスについて、物理的な記録日誌又は電子形式の監査証跡を、セキュリティを保って維持及び監視する。	7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 b) 全てのアクセスについて、物理的な記録落又は電子形式の監査証跡を、セキュリティを保って維持及び監視し、全ての記録及び敷地へに慎重を要する認証情報を保護する。	手引に関連記載あり			
11.1.2.8	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、全ての従業員、契約相手及び外部関係者に、何らかの形式の、目に見える証明書の着用を要求する。	7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 f) 全ての要員及び利害関係者に、何らかの形式の、目に見える証明書の着用を要求する。関係者が許可されていない訪問者及び目に見える証明書を着用していない者を見かけた場合には、直ちにセキュリティ要員に知らせる。常勤の従業員、供給者及び訪問者を識別しやすくするために、容積に区別できるバッジの使用を検討する。	手引に関連記載あり			
11.1.2.9	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、関係者が付与されていない訪問者及び目に見える証明書を着用していない者を見かけた場合には、直ちにセキュリティ要員に知らせる。	7a-7.2.3	【再】物理的入退の管理策の実施については、次の事項を考慮する。 f) 全ての要員及び利害関係者に、何らかの形式の、目に見える証明書の着用を要求する。関係者が許可されていない訪問者及び目に見える証明書を着用していない者を見かけた場合には、直ちにセキュリティ要員に知らせる。常勤の従業員、供給者及び訪問者を識別しやすくするために、容積に区別できるバッジの使用を検討する。	手引に関連記載あり			
11.1.2.10	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、セキュリティを保つべき領域又は秘密情報処理施設への、外部のサポートサービス要員によるアクセスは、限定的かつ必要なときに只け許可する。	7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 g) セキュリティを保つべき領域又は情報処理施設への、供給者の要員によるアクセスは、限定的かつ必要なときに只け許可する。このアクセスは、認可を必要とし、監視する。	手引に関連記載あり			
11.1.2.11	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、セキュリティを保つべき領域又は秘密情報処理施設への、全てのアクセスは認可を必要とし、監視する。	7a-7.2.3	【再】物理的入退の管理策の実施については、次の事項を考慮する。 g) セキュリティを保つべき領域又は情報処理施設への、供給者の要員によるアクセスは、限定的かつ必要なときに只け許可する。このアクセスは、認可を必要とし、監視する。	手引に関連記載あり			
11.1.2.12	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、セキュリティを保つべき領域へのアクセス権は、定期的にレビュー、更新し、必要なときには無効にする。	7a-7.2.3	【再】物理的入退の管理策の実施については、次の事項を考慮する。 a) 敷地及び建物へのアクセスは、認可された要員だけに制限する。物理的領域へのアクセス権の管理プロセスに、認可の提供、定期的なレビュー、要員及び失効を含める。	手引に関連記載あり			
–	（対応項なし）	7a-7.2.3	物理的入退の管理策の実施については、次の事項を考慮する。 d) 要員が監視している受付エリア、又は敷地周辺には建物への物理的なアクセスを管理するための手段を設定する。 e) 入退の際に要員及び利害関係者の持ち物を検査し、確認する。 h) 複数の組織の資産を保持する建物の場合、物理的なアクセスのセキュリティには特別な注意を払う。 i) 物理的なインシデントの起こりやすさが高くなった場合に強化できるように物理的セキュリティ対策を設計する。 j) 非常口などの他の入退場所を、認可されていないアクセスから保護する。 k) 物理的な鍵又は認証情報の管理を確実にし、記録落又は每年の鍵監査、及び物理的な鍵又は認証情報へのアクセスの管理を確実にするための鍵管理プロセスを設定する。	手引に関連記載あり			
11.1.2.13	セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、訪問者の入退の日付及び時刻の記録のレビュー結果に応じて、インシデント対応チームが連携する。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
11.1.3	オフィス、部屋及び施設のセキュリティ オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する。	7.3	オフィス、部屋及び施設のセキュリティ 管理策 オフィス、部屋及び施設に対する物理的セキュリティを設計し、実装する。 目的 オフィス、部屋及び施設内の組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷、及び干渉を防ぐため。		7.3	オフィス、部屋及び施設のセキュリティ 統制目標：オフィス、部屋及び施設に対する物理的セキュリティを設計し、実装する。 目的：オフィス、部屋及び施設内の組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷、及び干渉を防ぐため。	
11.1.3.1	オフィス、部屋及び施設のセキュリティを保つために、主要な施設は、一般の人のアクセスが通られる場所に設置する。	7a-7.3.1	オフィス、部屋及び施設のセキュリティを保つために、次の事項を考慮する。 a) 重要な施設は、一般の人のアクセスが通られる場所に設置する。	手引に関連記載あり	7.3.1	オフィス、部屋及び施設に関するセキュリティ対策を実施する。	オフィス、部屋及び施設のセキュリティを保つために、次の事項を考慮する。 a) 重要な施設は、一般の人のアクセスが通られる場所に設置する。 b) 適用可能な場合、建物を目立たず、その目的を示す表示は最小限とし、情報処理活動の存在を示すものは、建物の内外を問わず、一切表示しないことを確実にする。 c) 施設は、秘密の情報又は活動が外部から見えたり聞こえたりしないように構成する。該当する場合、電磁遮蔽も考慮する。 d) 秘密情報処理施設の場所を示す案内板、内線電話帳及びオンラインでアクセス可能な地図は、認可されていない者に容易に利用可能とならないようにする。
11.1.3.2	オフィス、部屋及び施設のセキュリティを保つために、建物を目立たず、その目的を示す表示は最小限とし、情報処理活動の存在を示すものは、建物の内外を問わず、一切表示しないことを設計する。	7a-7.3.1	オフィス、部屋及び施設のセキュリティを保つために、次の事項を考慮する。 b) 適用可能な場合、建物を目立たず、その目的を示す表示は最小限とし、情報処理活動の存在を示すものは、建物の内外を問わず、一切表示しないことを確実にする。	手引に関連記載あり			
11.1.3.3	オフィス、部屋及び施設のセキュリティを保つために、施設は、秘密の情報又は活動が外部から見えたり聞こえたりしないように構成する。（該当する場合、電磁遮蔽も含める）	7a-7.3.1	オフィス、部屋及び施設のセキュリティを保つために、次の事項を考慮する。 c) 施設は、秘密の情報又は活動が外部から見えたり聞こえたりしないように構成する。該当する場合、電磁遮蔽も考慮する。	手引に関連記載あり			
11.1.3.4	オフィス、部屋及び施設のセキュリティを保つために、秘密情報処理施設の場所を示す案内板及び内線電話帳は、認可されていない者が容易にアクセスできないようにする。	7a-7.3.1	オフィス、部屋及び施設のセキュリティを保つために、次の事項を考慮する。 d) 秘密情報処理施設の場所を示す案内板、内線電話帳及びオンラインでアクセス可能な地図は、認可されていない者に容易に利用可能とならないようにする。	手引に関連記載あり			

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
11.1.4	外部及び環境の脅威からの保護 自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用する。	7.5	物理的及び環境的脅威からの保護 管理策 自然災害及びその他の意図的又は意図的でない、インフラストラクチャに対する物理的脅威などの物理的及び環境的脅威に対する保護を設計し、実装する。 目的：物理的及び環境的脅威に起因する事象の結果を防止又は低減するため。 目的 物理的及び環境的脅威に起因する事象の結果を防止又は低減するため。		7.5	物理的及び環境的脅威からの保護 統制目標：自然災害及びその他の意図的又は意図的でない、インフラストラクチャに対する物理的脅威などの物理的及び環境的脅威に対する保護を設計し、実装する。 目的：物理的及び環境的脅威に起因する事象の結果を防止又は低減するため。	
11.1.4.1	火災、洪水、地震、爆発、暴力行為、及びその他の自然災害又は人的災害からの損傷を回避する方法について、専門家の助言を得る。	7a-7.5.3	火災、洪水、地震、爆発、暴力行為、有毒廃棄物、環境排出物、その他の自然災害又は人的災害などの物理的及び環境的脅威から生じるリスクを管理する方法について、専門家の助言を得る。	主刊に関連記載あり	7.5.1	物理的及び環境的脅威に対する保護を設計し、セキュリティ対策を実施する。	物理的及び環境的脅威が与たらす潜在的な結果を特定するためのリスクアセスメントは、物理的な場所で重要な運用を開始する前に、及び定期的に実施する。 必要な物理的及び環境的脅威からの保護策を実施し、また、物理的及び環境的脅威の変化を監視する。 火災、洪水、地震、爆発、暴力行為、有毒廃棄物、環境排出物、その他の自然災害又は人的災害などの物理的及び環境的脅威から生じるリスクを管理する方法について、専門家の助言を得る。 物理的施設の場所及び建造物では、次のことを考慮に入れる。 a）適切な標高、水域、構造断層線など、現地の地形 b）政治不安、犯罪活動又はテロ攻撃を誘発する可能性が高い場所など、都市の機威 リスクアセスメントの結果に基づいて、関連する物理的及び環境的脅威を特定し、次の状況のような例において適切な管理策の配置を考慮する。 a）火災：記憶媒体及び関連する情報処理システムの火災による損傷を防ぐために、火災を早期に検知できるシステムを設置する。消火は、周囲の環境に対して最も適切な物質を使用して実施する（例えば、閉鎖空間におけるガス）。 b）洪水：記憶媒体又は情報処理システムを床の頭端の床の下に、洪水を早期に検知できるシステムを設置する。消火が発生した場合にポンプ又は同等の手段を下に利用できるようにする。 c）電気サージ：サーバおよびクライアントの前方の情報システムを電気サージは同様の事象から保護し、そのような事象の結果を最小化することができるシステムを採用する。 d）爆発物及び武器：危険にく慣重を要する情報処理施設にある要員、車両又は商品に対して、爆発物又は武器がないかランダムな検査を実施する。
–	（対応項なし）	7a-7.5.1	物理的及び環境的脅威が与たらす潜在的な結果を特定するためのリスクアセスメントは、物理的な場所で重要な運用を開始する前に、及び定期的に実施する。	主刊に関連記載あり			
–	（対応項なし）	7a-7.5.2	必要な物理的及び環境的脅威からの保護策を実施し、また、物理的及び環境的脅威の変化を監視する。	主刊に関連記載あり			
–	（対応項なし）	7a-7.5.4	物理的施設の場所及び建造物では、次のことを考慮に入れる。 a）適切な標高、水域、構造断層線など、現地の地形 b）政治不安、犯罪活動又はテロ攻撃を誘発する可能性が高い場所など、都市の機威	主刊に関連記載あり			
–	（対応項なし）	7a-7.5.5	リスクアセスメントの結果に基づいて、関連する物理的及び環境的脅威を特定し、次の状況のような例において適切な管理策の配置を考慮する。 a）火災：記憶媒体及び関連する情報処理システムの火災による損傷を防ぐために、火災を早期に検知できるシステムを設置する。消火は、周囲の環境に対して最も適切な物質を使用して実施する。 b）洪水：記憶媒体又は情報処理システムを床の頭端の床の下に、洪水を早期に検知できるシステムを設置する。消火が発生した場合にポンプ又は同等の手段を下に利用できるようにする。 c）電気サージ：サーバおよびクライアントの前方の情報システムを電気サージは同様の事象から保護し、そのような事象の結果を最小化することができるシステムを採用する。 d）爆発物及び武器：危険にく慣重を要する情報処理施設にある要員、車両又は商品に対して、爆発物又は武器がないかランダムな検査を実施する。	主刊に関連記載あり			
11.1.5	セキュリティを保つべき領域での作業 セキュリティを保つべき領域での作業に関する手順を設計し、適用する。	7.6	セキュリティを保つべき領域での作業 管理策 セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実施する。 目的 セキュリティを保つべき領域にある情報及びその他の関連資産を、この領域で作業する要員による損傷及び妨可されていない干渉から保護するため。		7.6	セキュリティを保つべき領域での作業 統制目標：セキュリティを保つべき領域にある情報及びその他の関連資産を、この領域で作業する要員による損傷及び妨可されていない干渉から保護するため	
11.1.5.1	セキュリティを保つべき領域での作業に関する手順の設計においては、セキュリティを保つべき領域の存在又はその領域内での活動は、業務上知る必要のある要員にのみ知らせることを含める。	7a-7.6.2	セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 a）要員には、セキュリティを保つべき領域の存在又はその領域内での活動を、知る必要性の原則に基づく範囲でだけ認識させる。	主刊に関連記載あり	7.6.1	セキュリティを保つべき領域での作業に関するセキュリティ対策を実施する。	セキュリティを保つべき領域での作業のセキュリティ対策は、全ての要員に適用し、セキュリティを保つべき領域で行われる全ての活動を対象とする。 セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 a）要員には、セキュリティを保つべき領域の存在又はその領域内での活動を、知る必要性の原則に基づく範囲でだけ認識させる。 b）安全面の理由のため又び悪意のある活動の機会を低減するための調査から、セキュリティを保つべき領域での監視されていない作業は、認可する。 c）セキュリティを保つべき領域が無人のとき、物理的に施錠し、定期的に検査する。 d）撮像、映像、音声又はその他の記録装置（例えば、エンドポイント機器に付いたカメラ）は、可されたものも含め許可しない。 e）セキュリティを保つべき領域でのエンドポイント機器の携行及び使用を適切に管理する。 f）見やすいように又はアクセスできるように緊急手順を掲示する。
11.1.5.2	セキュリティを保つべき領域での作業に関する手順の設計に、安全面の理由のため及び悪意のある活動の機会を低減するための調査から、セキュリティを保つべき領域での監視されていない作業は、認可すること を含める。	7a-7.6.2	セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 b）安全面の理由のため及び悪意のある活動の機会を低減するための調査から、セキュリティを保つべき領域での監視されていない作業は、認可する。	主刊に関連記載あり			
11.1.5.3	セキュリティを保つべき領域での作業に関する手順の設計に、セキュリティを保つべき領域が無人のとき は、物理的に施錠し、定期的に点検すること を含める。	7a-7.6.2	セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 c）セキュリティを保つべき領域が無人のとき は、物理的に施錠し、定期的に検査する。	主刊に関連記載あり			
11.1.5.4	セキュリティを保つべき領域での作業に関する手順の設計に、撮像、映像、音声又はその他の記録装置（例えば、携帯端末に付いたカメラ）は、認可されたものも含め許可しないこと を含める。	7a-7.6.2	セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 d）撮像、映像、音声又はその他の記録装置は、認可されたものも含め許可しない。	主刊に関連記載あり			
11.1.5.5	セキュリティを保つべき領域での作業に関する取決めには、その領域で作業する従業員及び外部の利用者に対する管理策を含める。	7a-7.6.2	セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。 a）セキュリティを保つべき領域での利用者エンドポイント機器の携行及び使用を適切に管理する。	主刊に関連記載あり			
11.1.5.6	セキュリティを保つべき領域での作業に関する取決めは、セキュリティを保つべき領域で行われる全ての活動に適用する。	7a-7.6.1	セキュリティを保つべき領域での作業のセキュリティ対策は、全ての要員に適用し、セキュリティを保つべき領域で行われる全ての活動を対象とする。	主刊に関連記載あり			
11.1.6	受渡場所 荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。また、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す。	7.2	物理的入退 管理策 セキュリティを保つべき領域は、適切な入退管理策及びアクセス場所（受付など）によって保護する。 目的 組織の情報及びその他の関連資産に、認可された物理的アクセス以けがなされることを確実にするため。		7.2	物理的入退 統制目標：セキュリティを保つべき領域は、適切な入退管理策及びアクセス場所（受付など）によって保護する。 目的：組織の情報及びその他の関連資産に、認可された物理的アクセス以けがなされることを確実にするため。	
11.1.6.1	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、建物外部からの受渡場所への アクセスは、識別及び認可された要員に制限する。	7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 a）建物外部からの受渡場所への アクセスは、特定の認可された要員に制限する。	主刊に関連記載あり	7.2.2	【再】物理的入退の記録に関するセキュリティ対策を実施する。	（7.2.2に対応する項を参照）
11.1.6.2	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、受渡場所は、配達業員が建物の他の場所にアクセスすることなく荷積み及び荷降ろしできるように設計する。	7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 b）受渡場所は、配達業員が建物の他の場所に認可されていないアクセスをすることなく荷積み及び荷降ろしできるように設計する。	主刊に関連記載あり			
11.1.6.3	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、受渡場所の外部扉は、内部の扉が開いているときにはセキュリティを保つ。	7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 c）受渡場所の外部扉は、制限領域への扉が開いているときにはセキュリティを保つ。	主刊に関連記載あり			
11.1.6.4	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷物は、受渡場所から移動する前に、爆発物、化学物質又はその他の危険物がないか を検査する。	7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 d）入荷物は、受渡場所から移動する前に、爆発物、化学物質又はその他の危険物がないか を検査する。	主刊に関連記載あり			
11.1.6.5	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷物は、事業所へ持ち込むときに資産の管理手順に従って登録する。	7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 e）入荷物は、事業所へ持ち込むときに資産の管理手順に従って登録する。	主刊に関連記載あり			
11.1.6.6	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷と出荷は、物理的に分離した場所で扱う。	7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 f）可能な場合には、入荷と出荷は、物理的に分離した場所で扱う。	主刊に関連記載あり			
11.1.6.7	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷物は、輸送中に関財された脆弱性がないかを検査する。開封の脆弱が見つかった場合には、直ちにセキュリティ要員に報告する。	7a-7.2.5	荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。 g）入荷物は、輸送中に関財された脆弱性がないかを検査する。開封の脆弱が見つかった場合には、直ちにセキュリティ要員に報告する。	主刊に関連記載あり			
11.2 11.2.1	装置 管理目的：資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。 装置の設置及び保護 装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、保護する。	7.8	装置の設置及び保護 管理策 装置は、セキュリティを保つて設置し、保護する。 目的 物理的及び環境的脅威、並びに認可されていないアクセス及び損傷により リスクを低減するため。		7.8	装置の設置及び保護 統制目標：装置は、セキュリティを保つて設置し、保護する。 目的：物理的及び環境的脅威、並びに認可されていないアクセス及び損傷により リスクを低減するため。	
11.2.1.1	装置を保護するために、装置は、作業領域への不必要なアクセスが最小限になるよう設置する。	7b-7.8.1	装置を保護するために、次の事項を考慮する。 a）装置は、作業領域への不必要なアクセスを最小限とし、認可されていないアクセスを回避するように設置する。	主刊に関連記載あり	7.8.1	装置を保護するためのセキュリティ対策を実施する。	装置を保護するために、次の事項を考慮する。 a）装置は、作業領域への不必要なアクセスを最小限とし、認可されていないアクセスを回避するように設置する。 b）取扱いに慎重を要するデータを扱う情報処理設備は、設備の使用中に認可されていない者が情報をのぞき見るリスクを低減するように、その位置を慎重に定める。 c）潜在的な物理的及び環境的脅威（例えば、盗難、火災、爆発、ばい（煤）煙、水（又は給水の不具合）、しんあい（塵埃）、振動、化学的汚染、電力供給の妨害、通信妨害、電磁波放射、破壊）のリスクを最小限に抑えるための管理策を採用する。 d）情報処理施設・設備の周辺での飲食及び喫煙に関する指針を確立する。 e）情報処理施設・設備の運用に悪影響を与える可能性がある環境条件（例えば、温度、湿度）を監視する。 f）全ての建物に、落雷からの保護を適用する。全ての電力及び通信の引込線に避雷器を装着する。 g）作業現場などの環境にある装置には、特別な保護方法（例えば、キーボードカバー）の使用を考慮する。 h）電磁波の放射による情報漏えいのリスクを最小限にするため、秘密情報を処理する装置を保護する。 i）組織が管理する情報処理施設・設備を、組織が管理していない情報処理施設・設備から物理的に分離装置には、情報処理施設・設備の採掘構成要素、無停電電源装置（UPS）及びバッテリ、発電機、交流発電機及びコンバータ、物理的侵入検知システム及び層報装置、煙探知器、消火器、空調並びに非飛機が含まれる。
11.2.1.2	装置を保護するために、取扱いに慎重を要するデータを扱う情報処理施設は、施設の使用中に認可されていない者が情報をのぞき見るリスクを低減するよう、その位置を慎重に定める。	7b-7.8.1	装置を保護するために、次の事項を考慮する。 b）取扱いに慎重を要するデータを扱う情報処理施設は、設備の使用中に認可されていない者が情報をのぞき見るリスクを低減するために、その位置を慎重に定める。	主刊に関連記載あり			
11.2.1.3	装置を保護するために、認可されていないアクセス（通風機作による起動を含む）を回避するよう、装置設備のセキュリティを保つ。	7b-7.8.1	【再】装置を保護するために、次の事項を考慮する。 a）装置は、作業領域への不必要なアクセスを最小限とし、認可されていないアクセスを回避するように設置する。	主刊に関連記載あり			
11.2.1.4	装置を保護するために、特別な保護を必要とする装置は、それ以外の装置を分離するか、若しくは装置間に障壁を設ける。	7b-7.8.1	装置を保護するために、次の事項を考慮する。 i）組織が管理する情報処理施設・設備を、組織が管理していない情報処理施設・設備から物理的に分離する。	主刊に関連記載あり			
11.2.1.5	装置を保護するために、潜在的な物理的及び環境的脅威（例えば、盗難、火災、爆発、ばい（煤）煙、水（又は給水の不具合）、しんあい（塵埃）、振動、化学的汚染、電力供給の妨害、通信妨害、電磁波放射、破壊）のリスクを最小限に抑えるよう管理策を採用する。	7b-7.8.1	装置を保護するために、次の事項を考慮する。 c）潜在的な物理的及び環境的脅威のリスクを最小限に抑えるための管理策を採用する。	主刊に関連記載あり			
11.2.1.6	装置を保護するために、情報処理施設の周辺での飲食及び喫煙に関する指針を確立する。	7b-7.8.1	装置を保護するために、次の事項を考慮する。 d）情報処理施設・設備の周辺での飲食及び喫煙に関する指針を確立する。	主刊に関連記載あり			
11.2.1.7	装置を保護するために、情報処理施設の運用に悪影響を与えることがある環境条件（例えば、温度、湿度）を監視する。	7b-7.8.1	装置を保護するために、次の事項を考慮する。 e）情報処理施設・設備の運用に悪影響を与える可能性がある環境条件を監視する。	主刊に関連記載あり			
11.2.1.8	装置を保護するために、全ての建物に、落雷からの保護を適用する。全ての電力及び通信の引込線に避雷器を装着する。	7b-7.8.1	装置を保護するために、次の事項を考慮する。 f）全ての建物に、落雷からの保護を適用する。全ての電力及び通信の引込線に避雷器を装着する。	主刊に関連記載あり			
11.2.1.9	装置を保護するために、作業現場などの環境にある装置には、特別な保護方法（例えば、キーボードカバー）を使用する。	7b-7.8.1	装置を保護するために、次の事項を考慮する。 g）作業現場などの環境にある装置には、特別な保護方法の使用を考慮する。	主刊に関連記載あり			
11.2.1.10	装置を保護するために、秘密情報を処理する装置は、電磁波の放射による情報漏えいのリスクを最小限にする。	7b-7.8.1	装置を保護するために、次の事項を考慮する。 h）電磁波の放射による情報漏えいのリスクを最小限にするため、秘密情報を処理する装置を保護する。	主刊に関連記載あり			
11.2.2	サポートユーティリティ 装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。	7.11	サポートユーティリティ 管理策 情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保護する。 目的 サポートユーティリティの故障及び中断・阻害による情報及びその他の関連資産の消失、損傷若しくは侵害、又は組織の運用の中断を防止するため。		7.11	サポートユーティリティ 統制目標：情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保護する。 目的：サポートユーティリティの故障及び中断・阻害による情報及びその他の関連資産の消失、損傷若しくは侵害、又は組織の運用の中断を防止するため。	
11.2.2.1	サポートユーティリティ（例えば、電気、通信サービス、給水、ガス、下水、換気、空調）は、装置の製造業者の仕様及び地域の法的要求事項に適合しているものを採用する。	7b-7.11.1	組織は、情報処理施設・設備をサポートするユーティリティに依存している。そのため、組織は次の事項を行う。 a）ユーティリティを支援する装置を、関連する製造業者の仕様に従って構成し、操作し、保守すること を確実にする。	主刊に関連記載あり	7.11.1	情報処理施設・設備をサポートするユーティリティを保護するためのセキュリティ対策を実施する。	組織は、情報処理施設・設備をサポートするユーティリティ（例えば、電気、通信サービス、給水、ガス、下水、換気、空調）に依存している。そのため、組織は次の事項を行う。 a）ユーティリティを支援する装置を、関連する製造業者の仕様に従って構成し、操作し、保守すること を確実にする。 b）ユーティリティが事業の成長及び他のサポートユーティリティとの相互作用に対応する能力を、定期的に評価すること を確実にする。 c）ユーティリティを支援する装置が適切に機能すること を確実にするために、定期的に検査し、試験すること を確実にする。 d）必要であれば、ユーティリティの不具合を検知するための警報装置を取り付ける。 e）必要であれば、物理的な経路が異なる複数の供給元をユーティリティに備えること を確実にする。 f）ユーティリティを支援する装置がネットワークに接続されている場合、情報処理施設・設備から分離したネットワークとにあること を確実にする。 g）ユーティリティを支援する装置を、必要な場合だけ、かつ、セキュリティを保つた方法でだけインターネットに接続すること を確実にする。 緊急連絡先の詳細を記録し、停止した場合に要員が利用できるようにする。 サポートユーティリティのための非常用の照明及び通信手段を備える。 非常口又は設備室の近くに、電源、給水、ガス又はその他のユーティリティを遮断するための緊急スイッチ及び緊急バルブを設置する。
11.2.2.2	サポートユーティリティは、事業の成長及び他のサポートユーティリティとの相互作用に対応する能力を、定期的に評価する。	7b-7.11.1	組織は、情報処理施設・設備をサポートするユーティリティに依存している。そのため、組織は次の事項を行う。 b）ユーティリティが事業の成長及び他のサポートユーティリティとの相互作用に対応する能力を、定期的に評価すること を確実にする。	主刊に関連記載あり			
11.2.2.3	サポートユーティリティは、適切に機能すること を確実にするために、定期的に検査及び試験する。	7b-7.11.1	組織は、情報処理施設・設備をサポートするユーティリティに依存している。そのため、組織は次の事項を行う。 c）ユーティリティを支援する装置が適切に機能すること を確実にするために、定期的に検査し、試験すること を確実にする。	主刊に関連記載あり			
11.2.2.4	サポートユーティリティは、必要であれば、不具合を検知するための警報装置を取り付ける。	7b-7.11.1	組織は、情報処理施設・設備をサポートするユーティリティに依存している。そのため、組織は次の事項を行う。 d）必要であれば、ユーティリティの不具合を検知するための警報装置を取り付ける。	主刊に関連記載あり			
11.2.2.5	サポートユーティリティは、必要であれば、物理的な経路が異なる複数の供給元を確保する。	7b-7.11.1	組織は、情報処理施設・設備をサポートするユーティリティに依存している。そのため、組織は次の事項を行う。 e）必要であれば、物理的な経路が異なる複数の供給元をユーティリティに備えること を確実にする。	主刊に関連記載あり			
–	（対応項なし）	7b-7.11.1	組織は、情報処理施設・設備をサポートするユーティリティに依存している。そのため、組織は次の事項を行う。 f）ユーティリティを支援する装置がネットワークに接続されている場合、情報処理施設・設備から分離したネットワークとにあること を確実にする。 g）ユーティリティを支援する装置を、必要な場合だけ、かつ、セキュリティを保つた方法でだけインターネットに接続すること を確実にする。	主刊に関連記載あり			
11.2.2.6	非常用の照明及び通信手段を備える。	7b-7.11.2	サポートユーティリティのための非常用の照明及び通信手段を備える。	主刊に関連記載あり			
11.2.2.7	非常口又は設備室の近くに、電源、給水、ガス又はその他のユーティリティを遮断するための緊急スイッチ及び緊急バルブを設置する。	7b-7.11.3	非常口又は設備室の近くに、電源、給水、ガス又はその他のユーティリティを遮断するための緊急スイッチ及び緊急バルブを設置する。	主刊に関連記載あり			

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
11.2.3	ケーブル配線のセキュリティ データ牧伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。	7.12	ケーブル配線のセキュリティ 管理策 電源ケーブル、データ伝送ケーブル又は情報サービスを支援するケーブルの配線は、傍受、妨害又は損傷から保護する。 目的 電源ケーブル及び通信ケーブルの配線に関連した、情報及びその他の関連資産の消失、損傷、盗難又は侵害、並びに組織の運用の中断を防止するため。		7.12	ケーブル配線のセキュリティ 統制目標：電源ケーブル、データ伝送ケーブル又は情報サービスを支援するケーブルの配線は、傍受、妨害又は損傷から保護する。 目的：電源ケーブル及び通信ケーブルの配線に関連した、情報及びその他の関連資産の消失、損傷、盗難又は侵害、並びに組織の運用の中断を防止するため。	
11.2.3.1	情報処理施設に接続する電源ケーブル及び通信回線は、地下に埋設するか、又はこれに代わる十分な保護手段を施す。	7b-7.12.1	ケーブル配線のセキュリティのために、次の事項を考慮する。 a) 情報処理施設・設備に接続する電源ケーブル及び通信回線は、可能な場合には、地下に埋設するか、又はケーブル保護装置、電柱など、これに代わる十分な保護手段を施す。ケーブルが地下にある場合は、偶発的な損傷を保護する（例えば、外装電線管又はケーブルの存在を示す表示を利用し、）。 b) 干渉を防止するために、電源ケーブルは、通信ケーブルから隔離する。 c) 取扱いに慎重を要するシステム又は重要なシステムのために、次の追加の管理策の採用を検討する。 1) 外装電線管の導入、点検箇所・終端箇所の施錠可能な部屋又は箱への設置及び警報装置の設置 2) ケーブルを保護するための電磁遮蔽の利用 3) ケーブルに取り付けられた認可されていない装置・機器を検知するための定期的な技術的探査及び物理的検査 4) 配線盤、端子盤及びケーブル室への管理されたアクセス 5) 光ファイバーケーブルの使用	予引に関連記載あり	7.12.1	ケーブル配線のセキュリティを維持・保護するためのセキュリティ対策を実施する。	ケーブル配線のセキュリティのために、次の事項を考慮する。 a) 情報処理施設・設備に接続する電源ケーブル及び通信回線は、可能な場合には、地下に埋設するか、又はケーブル保護装置、電柱など、これに代わる十分な保護手段を施す。ケーブルが地下にある場合は、偶発的な損傷を保護する（例えば、外装電線管又はケーブルの存在を示す表示を利用し、）。 b) 干渉を防止するために、電源ケーブルは、通信ケーブルから隔離する。 c) 取扱いに慎重を要するシステム又は重要なシステムのために、次の追加の管理策の採用を検討する。 1) 外装電線管の導入、点検箇所・終端箇所の施錠可能な部屋又は箱への設置及び警報装置の設置 2) ケーブルを保護するための電磁遮蔽の利用 3) ケーブルに取り付けられた認可されていない装置・機器を検知するための定期的な技術的探査及び物理的検査 4) 配線盤、端子盤及びケーブル室への管理されたアクセス（例えば、物理鍵又はPINを用いる。） 5) 光ファイバーケーブルの使用 d) ケーブル配線の物理的識別及び検査を可能にするために、ケーブルの各端に始点及び終点に関する十分な詳細情報をラベル付けする。 ケーブルに関するインシデント又は不具合から生じるリスクを管理する方法について、専門家の助言を求める。
11.2.3.2	ケーブル間の干渉を防止するために、電源ケーブルは、通信ケーブルから隔離する。	7b-7.12.1	ケーブル配線のセキュリティのために、次の事項を考慮する。 b) 干渉を防止するために、電源ケーブルは、通信ケーブルから隔離する。	予引に関連記載あり			
11.2.3.3	取扱いに慎重を要するシステム又は重要なシステムのために、以下の4点を行う。 1.外装電線管を導入し、点検箇所・終端箇所の施錠可能な部屋又は箱へ設置する。 2.ケーブルを保護するための電磁遮蔽を利用する。 3.ケーブルに取り付けられた認可されていない装置の技術的探査及び物理的検査を実施する。 4.配線盤、端子盤及びケーブル室への管理されたアクセスを実施する。	7b-7.12.1	ケーブル配線のセキュリティのために、次の事項を考慮する。 c) 取扱いに慎重を要するシステム又は重要なシステムのために、次の追加の管理策の採用を検討する。 1) 外装電線管の導入、点検箇所・終端箇所の施錠可能な部屋又は箱への設置及び警報装置の設置 2) ケーブルを保護するための電磁遮蔽の利用 3) ケーブルに取り付けられた認可されていない装置・機器を検知するための定期的な技術的探査及び物理的検査 4) 配線盤、端子盤及びケーブル室への管理されたアクセス 5) 光ファイバーケーブルの使用	予引に関連記載あり			
11.2.4	装置の保守 装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。	7.13	装置の保守 管理策 装置は、情報の可用性、完全性及び機密性を維持することを確実にするために、正しく保守する。 目的 不十分な保守による、情報及びその他の関連資産の消失、損傷、盗難又は侵害、並びに組織の運用の中断を防止するため。		7.13	装置の保守 統制目標：装置は、情報の可用性、完全性及び機密性を維持することを確実にするために、正しく保守する。 目的：不十分な保守による、情報及びその他の関連資産の消失、損傷、盗難又は侵害、並びに組織の運用の中断を防止するため。	
11.2.4.1	可用性及び完全性を継続的に維持することを確実にするために、装置は、供給者の推奨する間隔及び仕様に従って保守する。	7b-7.13.1	装置の保守のために、次の事項を考慮する。 a) 装置は、供給者の推奨するサービスの頻度及び仕様に従って保守する。	予引に関連記載あり	7.13.1	装置を保守するためのセキュリティ対策を実施する。	装置の保守のために、次の事項を考慮する。 a) 装置は、供給者の推奨するサービスの頻度及び仕様に従って保守する。 b) 組織の保守プログラムを実施し、監視する。 c) 認可された保守要員だけが、装置の修理及び保守を実施する。 d) 故障と見られるの及び実際の故障の全て、並びに予防及び是正のための保守の全てについての記録を保持する。 e) 装置の保守を計画する場合には、この保守を、要員が構内で行うのか、又は組織の外で行うのかを考慮して、適切な管理策を実施する。保守要員に適切な秘密保持契約を結ばせる。 f) 構内で保守を実施する場合は保守要員を監督する。 g) 遠隔保守のためのアクセスを認可し、管理する。 h) 情報を保有している装置を保守のために構外へ持ち出す場合は、構外にある資産のセキュリティ（7.9参照）の対策を適用する。 i) 保険において課された全ての保守要求事項を順守する。 j) 保守の後、装置を作動させる前に、その装置が改ざんされていないこと及び適切に機能することを確実にするために検査する。 k) 装置を処分するごとに決定した場合、装置のセキュリティを保つ処分又は再利用（7.14参照）の対策を適用する。
11.2.4.2	可用性及び完全性を継続的に維持することを確実にするために、認可された保守要員の一覧を維持し、その保守要員だけが、装置の修理及び手入れを実施する。	7b-7.13.1	装置の保守のために、次の事項を考慮する。 c) 認可された保守要員だけが、装置の修理及び保守を実施する。	予引に関連記載あり			
11.2.4.3	可用性及び完全性を継続的に維持することを確実にするために、故障と見られるの及び実際の故障の全て、並びに予防及び是正のための保守の全てについての記録を保持し、レビューする。	7b-7.13.1	装置の保守のために、次の事項を考慮する。 d) 故障と見られるの及び実際の故障の全て、並びに予防及び是正のための保守の全てについての記録を保持する。	予引に関連記載あり			
11.2.4.4	可用性及び完全性を継続的に維持することを確実にするために、装置の保守を計画する場合には、この保守を、要員が構内で行うのか、又は組織の外で行うのかを考慮して、適切な管理策を実施する。その装置から秘密情報を消去するか、又は保守要員が十分に信頼できる者であり、必要なアクセス権を有することを確かめる。	7b-7.13.1	装置の保守のために、次の事項を考慮する。 e) 装置の保守を計画する場合には、この保守を、要員が構内で行うのか、又は組織の外で行うのかを考慮して、適切な管理策を実施する。保守要員に適切な秘密保持契約を結ばせる。	予引に関連記載あり			
11.2.4.5	可用性及び完全性を継続的に維持することを確実にするために、保険約款で定められた、保守に関する全ての要求事項を順守する。	7b-7.13.1	【再】装置の保守のために、次の事項を考慮する。 e) 装置の保守を計画する場合には、この保守を、要員が構内で行うのか、又は組織の外で行うのかを考慮して、適切な管理策を実施する。保守要員に適切な秘密保持契約を結ばせる。	予引に関連記載あり			
11.2.4.6	可用性及び完全性を継続的に維持することを確実にするために、保守の後、装置を作動させる前に、その装置が改ざんされていないこと及び不具合を起こさないことを確実にするために検査する。	7b-7.13.1	装置の保守のために、次の事項を考慮する。 j) 保守の後、装置を作動させる前に、その装置が改ざんされていないこと及び適切に機能することを確実にするために検査する。	予引に関連記載あり			
11.2.4.7	可用性及び完全性を継続的に維持することを確実にするために、遠隔保守は認可を必要とし、監視する。	7b-7.13.1	装置の保守のために、次の事項を考慮する。 g) 遠隔保守のためのアクセスを認可し、管理する。	予引に関連記載あり			
–	（対応項なし）	7b-7.13.1	装置の保守のために、次の事項を考慮する。 b) 組織の保守プログラムを実施し、監視する。 f) 構内で保守を実施する場合は保守要員を監督する。 h) 情報を保有している装置を保守のために構外へ持ち出す場合は、構外にある資産のセキュリティの対策を適用する。 i) 保険において課された全ての保守要求事項を順守する。 k) 装置を処分するごとに決定した場合、装置のセキュリティを保つ処分又は再利用の対策を適用する。	予引に関連記載あり			
11.2.4.8	可用性及び完全性を継続的に維持することを確実にするために、遠隔保守用のツールの要求仕様及び認可を監視する。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
11.2.4.9	可用性及び完全性を継続的に維持することを確実にするために、遠隔保守用のセッションを確立する際には、認証を行う。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
11.2.4.10	可用性及び完全性を継続的に維持することを確実にするために、遠隔保守は記録し、記録を保持する。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
11.2.4.11	可用性及び完全性を継続的に維持することを確実にするために、遠隔保守の終了後、それに用いたセッション及びネットワークの接続を切る。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
11.2.5	資産の移動 装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さない。	7.9	構外にある資産のセキュリティ 管理策 構外にある資産を保護する。 目的 構外にある装置・機器の紛失、損傷、盗難又は侵害、及び組織の業務の中断を防止するため。		7.9	構外にある資産のセキュリティ 統制目標：構外にある資産を保護する。 目的：構外にある装置・機器の紛失、損傷、盗難又は侵害、及び組織の業務の中断を防止するため。	
11.2.5.1	資産を構外に持ち出すことを許す権限を与え従業員及び外部の利用者を特定し、承認する。	7b-7.9.2	組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。 d) 必要かつ実施可能な場合には、組織の構内から装置・機器及び媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する	予引に関連記載あり	7.9.1	構外にある装置・機器を保護するためのセキュリティ対策を実施する。	組織が所有する装置・機器、及び個人が所有し組織のために用いる機器【私物機器の業務利用（BYOD）】を含む、情報を保管又は処理する、組織の構外で使用する装置・機器（例えば、モバイル機器）は全て配慮する必要がある。構外にある装置・機器の使用は、管理者によって認可がある。 組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。 a) 構外に持ち出した装置・機器及び記憶媒体は、公共の場所で、かつ、セキュリティが保たれない場所に無人状態で放置しない。 b) 装置・機器の保護（例えば、強力な電磁場、水、熱、湿度、ほこり（塩）にかちてごに対する保護）に関する製造業者の指示を常に守る。 c) 構外にある装置・機器を、複数の個人又は利害関係者の間で移動する場合には、その装置・機器の受渡記録を明記した記録（少なくとも、その装置・機器に対して責任を負う者の氏名及び組織を含むもの）を維持する。両者ともに移動する必要のない情報は、移動前にセキュリティを保つ措置を講じる。 d) 必要かつ実施可能な場合には、組織の構内から装置・機器及び媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する（5.14参照）。 e) 公共ご通信網において機器（例えば、モバイル又はラップトップ）上の情報を見ること、及びのそ目見に関連するリスクに対して保護する。 f) 機器の位置追跡及び遠隔データ消去機能を実装する。 組織の構外に装置【アンテナ、複合自動預け払い機（ATM）など】を恒久的に設置するど、損傷、盗難又は傍受のリスクが高くなる可能性がある。これらのリスクは、場所によってかなり異なる可能性がある。装置を恒久的に設置する構外のそれぞれの場所に応じた最も適切な対策の決定には、リスクを考慮する。 装置を組織の構外に恒久的に設置する場合、次の事項を考慮する。 a) 物理的セキュリティの監視（7.4参照） b) 物理的及び環境的脅威からの保護（7.5参照） c) 物理的アクセス制御及び不正防止（tamper proofing）の管理策 d) 論理的アクセス制御
11.2.5.2	資産の特出し期限を設定し、また、返却がそのとおりであった か検証する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承され て）	–	（対応項なし）	–
11.2.5.3	資産が構外に持ち出されていることを記録し、また、返却時に記録する。	7b-7.9.2	組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。 d) 必要かつ実施可能な場合には、組織の構内から装置・機器及び媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する	予引に関連記載あり	7.9.1	【再】構外にある装置・機器を保護するためのセキュリティ対策を実施する。	（7.9.1に対応する項を参照）
11.2.5.4	資産を戻り又は利用する者について、その識別情報、役割及び所属を文書化し、構外へ持ち出した装置、情報又はソフトウェアとともに返却させる。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承され て）	–	（対応項なし）	–
11.2.6	構外にある装置及び資産のセキュリティ 構外にある資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用する。	7.9	構外にある資産のセキュリティ 管理策 構外にある資産を保護する。 目的 構外にある装置・機器の紛失、損傷、盗難又は侵害、及び組織の業務の中断を防止するため。		7.9	構外にある資産のセキュリティ 統制目標：構外にある資産を保護する。 目的：構外にある装置・機器の紛失、損傷、盗難又は侵害、及び組織の業務の中断を防止するため。	
11.2.6.1	情報を保管及び処理する装置（組織が所有する装置、及び個人が所有し組織のために用いる装置）を組織の構外で用いる場合は、管理者の認可を得る。	7b-7.9.1	構外にある装置・機器の使用は、管理者によって認可される。	予引に関連記載あり	7.9.1	【再】構外にある装置・機器を保護するためのセキュリティ対策を実施する。	（7.9.1に対応する項を参照）
11.2.6.2	構外に持ち出した装置及び媒体は、公共の場所に無人状態で放置しない。	7b-7.9.2	組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。 a) 構外に持ち出した装置・機器及び記憶媒体は、公共の場所で、かつ、セキュリティが保たれない場所に無人状態で放置しない。	予引に関連記載あり			
11.2.6.3	構外にある装置の保護のために、装置の保護（例えば、強力な電磁場にかちてごに対する保護）に関する製造業者の指示を常に守る。	7b-7.9.2	組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。 b) 装置・機器の保護に関する製造業者の指示を常に守る。	予引に関連記載あり			
11.2.6.4	構外にある装置の保護のために、在宅勤務、テレワーキング及び一時的サイトのような構外の場所についての管理策を、リスクアセスメントに基づいて決定し、状況に応じた管理策（例えば、施錠可能な文書保管庫、クリアデスク方針、コンピュータのアクセス制御、セキュリティを保ったオンライン通信）を適切に適用する。	7b-7.9.3	装置を恒久的に設置する構外のそれぞれの場所に応じた最も適切な対策の決定には、リスクを考慮する。	予引に関連記載あり			
11.2.6.5	構外にある装置の保護のために、構外にある装置を、複数の個人又は外部関係者の間で移動する場合には、その装置の受渡記録を明記した記録（少なくとも、その装置に対して責任を負う者の氏名及び組織を含むもの）を維持する。	7b-7.9.2	組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。 c) 構外にある装置・機器を、複数の個人又は外部関係者の間で移動する場合には、その装置・機器の受渡記録を明記した記録（少なくとも、その装置・機器に対して責任を負う者の氏名及び組織を含むもの）を維持する。両者ともに移動する必要のない情報は、移動前にセキュリティを保つ措置を講じる。	予引に関連記載あり			
11.2.6.6	リスク（例えば、損傷、盗難、傍受）は、場所によってかなり異なる場合があるため、それぞれの場所に応じた最も適切な管理策は、リスクを考慮して決定する。	7b-7.9.3	【再】装置を恒久的に設置する構外のそれぞれの場所に応じた最も適切な対策の決定には、リスクを考慮する。	予引に関連記載あり			
–	（対応項なし）	7b-7.9.4	装置を組織の構外に恒久的に設置する場合、次の事項を考慮する。 a) 物理的セキュリティの監視 b) 物理的及び環境的脅威からの保護 c) 物理的アクセス制御及び不正防止（tamper proofing）の管理策 d) 論理的アクセス制御	予引に関連記載あり			

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
11.2.7	装置のセキュリティを保った処分又は再利用 記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに機密を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証する。	7.14	装置のセキュリティを保った処分又は再利用 管理策 記憶媒体を内蔵した装置は、処分又は再利用する前に、全ての取扱いに機密を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保てるよう上書きしていることを確実にするために、検証する。 目的 処分又は再利用する装置からの情報漏えいを防止するため。		7.14	装置のセキュリティを保った処分又は再利用 統制目標：記憶媒体を内蔵した装置は、処分又は再利用する前に、全ての取扱いに機密を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保てるよう上書きしていることを確実にするために、検証する。 目的：処分又は再利用する装置からの情報漏えいを防止するため。	
11.2.7.1	装置は、処分又は再利用する前に、記憶媒体が内蔵されているか否かを確かめるために検証する。	7b-7.14.1	装置は、処分又は再利用する前に、記憶媒体が内蔵されているか否かを確かめるために検証する。	手引に関連記載あり	7.14.1	装置の処分又は再利用する前に、セキュリティを保つための対策を実施する。	装置は、処分又は再利用する前に、記憶媒体が内蔵されているか否かを確かめるために検証する。 秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊、又はその情報を破壊、消去若しくは上書きする。 秘密情報又は著作権のある情報の消去又は上書きには、標準的な削除機能を利用するよりも、元の情報を媒体から取り出せなくする技術を利用する。記憶媒体のセキュリティを保つ処分に関する詳細な手引については7.10を、情報の削除に関する手引については8.10を参照。 組織を特定する、又は情報の分類、管理責任者、システム若しくはネットワークの区別を示すラベル及び表示は、再販又は装置内部への寄付を含む処分を行う前に除去する。 （上記の他、一部 JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
11.2.7.2	秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊すること、又はその情報を破壊、消去若しくは上書きする。	7b-7.14.2	秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊、又はその情報を破壊、消去若しくは上書きする。	手引に関連記載あり			
11.2.7.3	秘密情報又は著作権のある情報を格納した記憶媒体の消去又は上書きには、標準的な消去又は初期化の機能を利用するよりも、元の情報を媒体から取り出せなくする技術を利用する。	7b-7.14.3	秘密情報又は著作権のある情報の消去又は上書きには、標準的な削除機能を利用するよりも、元の情報を媒体から取り出せなくする技術を利用する。	手引に関連記載あり			
11.2.7.4.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり （情報セキュリティ管理基準以外の由来）			
–	（対応項なし）	（7b-7.14.3参考）	秘密情報又は著作権のある情報の消去又は上書きには、標準的な削除機能を利用するよりも、	手引に関連記載あり			
–	（対応項なし）	7b-7.14.4	組織を特定する、又は情報の分類、管理責任者、システム若しくはネットワークの区別を示すラベル及び表示は、再販又は装置内部への寄付を含む処分を行う前に除去する。	手引に関連記載あり			
–	（対応項なし）	7b-7.14.5	組織は、施設のリース終了時又は施設外への移転時に、アクセス制御、監視装置などのセキュリティ管理策の除去を検討する。	手引に関連記載あり	7.14.2	施設のリース終了時又は施設外への移転時に関するセキュリティ対策を実施する。	組織は、施設のリース終了時又は施設外への移転時に、アクセス制御、監視装置などのセキュリティ管理策の除去を検討する。これは、次のような要因に依存する。 a）施設を元の状態に戻すリース合意 b）次のテナントに対して、取扱いに機密を要する情報を含むシステムが残されるリスクの最小化（例えば、利用者アセットのリスト、映像又は画像ファイル） c）移転元の施設で管理策を再利用できること
–	（対応項なし）	（7b-7.14.5参考）	これは、次のような要因に依存する。 a）施設を元の状態に戻すリース合意 b）次のテナントに対して、取扱いに機密を要する情報を含むシステムが残されるリスクの最小化 c）移転元の施設で管理策を再利用できること	手引に関連記載あり			
11.2.8	無人状態にある利用者装置 利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にする仕組みを整備する。	8.1	利用者エンドポイント機器 管理策 利用者エンドポイント機器に保存されている情報、処理される情報、又は利用者エンドポイント機器を介してアクセス可能な情報を保護する。 目的 利用者エンドポイント機器を使用することによってもたらされるリスクから情報を保護するため。		8.1	エンドポイント機器 統制目標：エンドポイント機器に保存されている情報、処理される情報、又はエンドポイント機器を介してアクセス可能な情報を保護する。 目的：エンドポイント機器を使用することによってもたらされるリスクから情報を保護するため。	
11.2.8.1	無人状態にある装置の保護を実施する責任と同様に、その装置を保護するためのセキュリティ要求事項及び手順についても、全ての利用者に認識させる。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
11.2.8.2	利用者に、実行して止処理が終わった時点で、接続を切るよう助言する。（ただし、例えば、パスワードによって保護された スクリーンセーバなどの適切なロック機能によって保護されている場合は、その限りではない）	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
–	（対応項なし）	8a-8.1.5	利用者エンドポイント機器を保護するためのセキュリティ要求事項及び手順、並びにそのセキュリティ対策を実施する責任の責任について、全ての利用者に認識させる。	手引に関連記載あり	8.1.2	【再】エンドポイント機器を保護するための対策を実施する。	（8.1.2に対応する項を参照）
11.2.8.3	利用者に、必要がなくなった、アプリケーション又はネットワークサービスからログオフするよう助言する。	8a-8.1.6	【再】利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するよう助言する。 a）利用者エンドポイント機器を利用する必要がなくなったら、実行していたセッションからログオフ、サービスを終了する。	手引に関連記載あり			
11.2.8.4	利用者に、コンピュータ又はモバイル機器は、利用していない場合、キーロック又は同等の管理策（例えば、パスワードアクセス）によって、認可されていない利用から保護するよう助言する。	8a-8.1.6	【再】利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するよう助言する。 b）利用者エンドポイント機器は、利用していない場合、物理的管理策及び論理的管理策を用いて、認可されていない利用から保護する。重要度の高い、脅威に関連する要する、又は影響の大きい業務情報が入っている機器を、無人の状態で放置しない。	手引に関連記載あり			
–	（対応項なし）	8a-8.1.7	利用者エンドポイント機器の盗難又は紛失に備えて、送付、現期、契約（保険を含む。）及び組織のその他のセキュリティ要求事項を考慮して、そのための手順を確立する。	手引に関連記載あり			
11.2.9	クリアデスク・クリアスクリーン方針 書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用する。 （脚注）クリアデスクとは、机上に書類を放置しないことをいう。また、クリアスクリーンとは、情報をスクリーンに残しておき続けないことをいう。	7.7	クリアデスク・クリアスクリーン 管理策 書類及び取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定め、適切に実施させる。 目的 通常の勤務時間内及び時間外の、机、スクリーン及びその他のアクセス可能な場所にある情報への認可されていないリスクを、情報の消失及び損傷のリスクを低減するため。		7.7	クリアデスク・クリアスクリーン 統制目標：書類及び取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定め、適切に実施させる。 目的：通常の勤務時間内及び時間外の、机、スクリーン及びその他のアクセス可能な場所にある情報への認可されていないリスクを、情報の消失及び損傷のリスクを低減するため。	
11.2.9.1	クリアデスク・クリアスクリーン方針において、組織の、情報分類、法的及び契約上の要求事項、並びにそれらに対応するリスクのリスク受容の側面を含める。	7a-7.7.1	組織は、クリアデスク・クリアスクリーンに関するトピック固有の方針を確立し、全ての関連する利害関係者へ伝達する。	手引に関連記載あり	7.7.1	書類及び取外し可能な記憶媒体に対するクリアデスク及び情報処理施設に対するクリアスクリーンに関する方針を実施する。	組織は、クリアデスク・クリアスクリーンに関するトピック固有の方針を確立し、全ての関連する利害関係者へ伝達する。
11.2.9.2	取扱いに機密を要する業務情報又は重要な業務情報（例えば、紙又は電子記憶媒体上の業務情報）は、必要のない場合、特にオフィスに誰もいないときには、施錠して（理想的には金庫、書庫又はセキュリティを備えた他の形態の収納用具に）保管する。	7a-7.7.2	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 a）取扱いに機密を要する業務情報又は重要な業務情報は、必要のない場合、特にオフィスに誰もいないときには、施錠して（理想的には金庫、書庫又はセキュリティを備えた他の形態の収納用具に）保管しておく。	手引に関連記載あり	7.7.2	書類及び取外し可能な記憶媒体に対するクリアデスク及び情報処理施設に対するクリアスクリーンに関するセキュリティ対策を実施する。	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 a）取扱いに機密を要する業務情報又は重要な業務情報（例えば、紙又は電子記憶媒体上の業務情報）は、必要のない場合、特にオフィスに誰もいないときには、施錠して（理想的には金庫、書庫又はセキュリティを備えた他の形態の収納用具に）保管しておく。 b）使用していないときには施錠用机には、施錠又はその他のセキュリティ手段によってエンドポイント機器を保護する。 c）エンドポイント機器は、離席時には、ログオフ状態にしておか、又は利用者認証機能で管理されたスクリーン及びキーボードのロック機能によって保護しておく。全てのコンピュータ及びシステムは、タイムアウト又は自動ログアウト機能をもう構成とする。 d）印刷を実行した人に、プリンタは複合機からの出力をすぐに収集させる。印刷を実行した人だけが、プリンタの傍に立ったときだけ、印刷物を得ることができる認証機能をもつプリンタを利用する。 e）取扱いに機密を要する情報を含む文書及び取外し可能な記憶媒体をセキュリティを保って保管し、不要になった場合はセキュリティを保った処分の仕組みを使用してそれらを廃棄する。 f）画面上のポップアップの設定に関する規則及び手引を確立し、伝達する（例えば、プレゼンテーション、画面共有の際、又は公共の場所においては、可能であれば開いい電子メール及びメッセージングのポップアップを抑止する。）。 g）不要になった場合には、ホワイトボード上及びその他の種類の掲示上の取扱いに機密を要する情報又は重要な情報を消去する。 初備は、初備の資産（例えば、引渋出し又は収納用具の後に落ちた文書など）を後に残さないことを確実にするために、適出する前に最後の点検を行うことを含む。施設から退去する際の適切な手順をもつ。
11.2.9.3	コンピュータ及び端末は、離席時には、ログオフ状態にしておか、又はパスワード、トークン若しくは類似の利用者認証機能で管理されたスクリーン及びキーボードのロック機能によって保護する。	7a-7.7.2	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 b）使用していないときには離席時には、施錠又はその他のセキュリティ手段によって利用者エンドポイント機器を保護する。	手引に関連記載あり			
11.2.9.4	コンピュータ及び端末は、利用しないときは、施錠、パスワード又は他の管理策によって保護する。	7a-7.7.2	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 c）利用者エンドポイント機器は、離席時には、ログオフ状態にしておか、又は利用者認証機能で管理されたスクリーン及びキーボードのロック機能によって保護しておく。全てのコンピュータ及びシステムは、タイムアウト又は自動ログアウト機能をもう構成とする。	手引に関連記載あり			
11.2.9.5	次ー機及びその他の再生技術（例えば、スキャナ、ディジタルカメラ）の認可されていない利用は、防止する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
11.2.9.6	取扱いに機密を要する情報又は構成担い情報を含む媒体は、プリンタから直ちに取り出す。	7a-7.7.2	クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。 d）印刷を実行した人に、プリンタは複合機からの出力をすぐに収集させる。印刷を実行した人だけが、プリンタの傍に立ったときだけ、印刷物を得ることができる認証機能をもつプリンタを利用する。	手引に関連記載あり	7.7.2	【再】書類及び取外し可能な記憶媒体に対するクリアデスク及び情報処理施設に対するクリアスクリーンに関するセキュリティ対策を実施する。	（7.7.2に対応する項を参照）
12	運用のセキュリティ	5.37	操作手順書 管理策 情報処理設備の操作手順は、文書化し、必要とする要員に対して利用可能にする。 目的 情報処理設備の正確で、かつ、セキュリティに配慮した操作を確実にするため。		5.37	操作手順書 統制目標：情報処理設備の操作手順は、文書化し、必要とする要員に対して利用可能にする。 目的：情報処理設備の正確で、かつ、セキュリティに配慮した操作を確実にするため。	
12.1	運用の手順及び責任 管理目的：情報処理設備の正確かつセキュリティを保った運用を確実にするため。						
12.1.1	操作手順書 操作手順は、文書化し、必要とする全ての利用者に対して利用可能にする。						
12.1.1.1	情報処理設備及び通信設備に関連する操作（例えば、コンピュータの起動・停止の手順、インストール、設定、バックアップ、装置の保守、媒体の取扱い、コンピュータ室及びメールの取扱いの管理・安全）の手順書を、利用者の特権の有無を考慮して、作成する。	5g-5.37.2	次の場合には、情報セキュリティに関連する組織の操作活動の手順書を作成する。 a）多くの人が同じ活動を行う必要がある場合 b）まれにしか行われない活動で、次に実行する此に手順を忘れている可能性が高い場合 c）新たな活動で、正しく実行しないリスクが生じる場合 d）新しい要員に活動を引き継ぐ前	手引に関連記載あり	5.37.1	情報処理設備における操作手順書を作成する。	例えば、次の場合に、情報セキュリティに関連する組織の操作活動の手順書を作成する。 a）多くの人が同じ活動を行う必要がある場合 b）まれにしか行われない活動で、次に実行する此に手順を忘れている可能性が高い場合 c）新たな活動で、正しく実行しないリスクが生じる場合 d）新しい要員に活動を引き継ぐ前 情報処理設備の操作手順には、次の事項を明記する。 a）責任者 b）システムのセキュリティに配慮した導入及び構成 c）情報の処理及び取扱い（自動化されたもの及び手動によるものを含む。） d）バックアップ（8.3参照）及びレジリエンス e）スケジュールに関する要求事項。これには、他のシステムとの依存関係を含む。 f）作業中に発生し得る、誤りの又はその他の例外状況の処理についての指示（例えば、ユーティリティプログラムの利用の制限（8.18参照）） g）操作上又は技術上の予期の問題が発生した場合の、外部のサポート用連絡先を含む、サポート用及びエスカレーション用の連絡先 h）記憶媒体の取扱いに関する指示（7.10及び7.14参照） i）システムが故障した場合の再起動及び回復の手順 j）監査証跡及びシステムログ情報（8.15及び8.17参照）並びにビデオ監視システム（7.4参照）の管理 k）容量・能力、パフォーマンス及びセキュリティ(2)の監視手順 l）保守手順
–	（対応項なし）	5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 a）責任者	手引に関連記載あり			
12.1.1.2	情報処理設備及び通信設備に関連する操作手順には、システムの運用前認可、導入及び構成（ベースライン構成を含む）、セキュリティ機能、管理機能の設定及び使用に関する既知のぜい弱性を含む、操作上の指示を明記する。	5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 b）システムのセキュリティに配慮した導入及び構成	手引に関連記載あり			
12.1.1.3	情報処理設備及び通信設備に関連する操作手順には、情報の処理及び取扱い（自動化されたもの及び手動によるものを含む）を含む、操作上の指示を明記する。	5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 c）情報の処理及び取扱い（自動化されたもの及び手動によるものを含む。）	手引に関連記載あり			
12.1.1.4	情報処理設備及び通信設備に関連する操作手順には、バックアップを含む、操作上の指示を明記する。	5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 d）バックアップ及びレジリエンス	手引に関連記載あり			
12.1.1.5	情報処理設備及び通信設備に関連する操作手順には、スケジュール作成に関する要求事項（他のシステムとの相互 依存性、最も早い作業の開始時刻及び最も遅い作業の完了時刻など）を含む、操作上の指示を明記する。	5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 e）スケジュールに関する要求事項。これには、他のシステムとの依存関係を含む。	手引に関連記載あり			
12.1.1.6	情報処理設備及び通信設備に関連する操作手順には、作業中に発生し得る、誤りの又はその他の例外状況の処理についての指示（システムユーティティの利用の制限）を含む、操作上の指示を明記する。	5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 f）作業中に発生し得る、誤りの又はその他の例外状況の処理についての指示	手引に関連記載あり			
12.1.1.7	情報処理設備及び通信設備に関連する操作手順には、必要な文書が入手できない場合及び操作上又は技術上の予期の問題が発生した場合の、外部のサポート用連絡先を含む、サポート用及び段階的取扱い（escalation）用の連絡先を含む、操作上の指示を明記する。	5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 g）操作上又は技術上の予期の問題が発生した場合の、外部のサポート用連絡先を含む、サポート用及びエスカレーション用の連絡先	手引に関連記載あり			
12.1.1.8	情報処理設備及び通信設備に関連する操作手順には、特別な出力及び媒体の取扱いに関する指示（特殊な用紙の使用、秘密情報の出力の管理（失敗した作業出力のセキュリティを保つ処 分手順を含む））を含む、操作上の指示を明記する。	5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 h）記憶媒体の取扱いに関する指示	手引に関連記載あり			
12.1.1.9	情報処理設備及び通信設備に関連する操作手順には、システムが故障した場合の再起動及び回復の手順を含む、操作上の指示を明記する。	5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 i）システムが故障した場合の再起動及び回復の手順	手引に関連記載あり			
12.1.1.10	情報処理設備及び通信設備に関連する操作手順には、監査証跡及びシステムの情報の管理を含む、操作上の指示を明記する。	5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 j）監査証跡及びシステムの情報並びにビデオ監視システムの管理	手引に関連記載あり			
12.1.1.11	情報処理設備及び通信設備に関連する操作手順には、監視手順を含む、操作上の指示を明記する。	5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 k）容量・能力、パフォーマンス及びセキュリティ(2)の監視手順	手引に関連記載あり			
–	（対応項なし）	5g-5.37.2	情報処理設備の操作手順には、次の事項を明記する。 l）保守手順	手引に関連記載あり			
12.1.1.12	システムの管理活動のための操作手順及び文書化手順は、正式な文書として取り扱い、その手順書の変更は、管理層が認可する。	5g-5.37.4	情報処理設備の操作手順書の変更は認可のもと行う。	手引に関連記載あり	5.37.2	情報処理設備の操作手順書の変更は認可のもと実施する。	情報処理設備の操作手順書の変更は必要に応じてレビュー、更新する。 情報処理設備の操作手順書の変更は認可のもと行う。 技術的に可能であれば、情報システムは、同一の手順、ツール及びユーティティを用いて、首尾一貫した管理を行う。
12.1.1.13	情報システムは、技術的に可能な場合には、同一の手順、ツール及びユーティティを用いて、首尾一貫した管理を行う。	5g-5.37.5	技術的に可能であれば、情報システムは、同一の手順、ツール及びユーティティを用いて、首尾一貫した管理を行う。	手引に関連記載あり			

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
12.1.2	変更管理 情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理する。	8.32	変更管理 管理策 情報処理設備及び情報システムの変更は、変更管理手順に従う。 目的 変更を実行するときに情報セキュリティを維持するため。		8.32	変更管理 統制目標：情報処理設備及び情報システムの変更は、変更管理手順に従う。 目的：変更を実行するときに情報セキュリティを維持するため。	
12.1.2.1	組織、業務プロセス、情報処理設備及びシステムの変更管理には、情報処理設備及びシステムの構成品目の構成管理プロセス及び管理計画を策定、文書化し、実施し、重要な変更の特定及び記録を含める。	8d-8.32.3	変更管理手順は、情報処理設備及び情報システムにおける情報の機密性、完全性及び可用性を確実にするために、設計の初期段階からその後の全ての保守作業までのシステム開発のライフサイクル全体にわたって実施し、実装する。	手引に関連記載あり	8.32.1	情報処理設備及び情報システムの変更管理手順を整備し、対策を実施する。	新しいシステムの導入及び既存システムに対する重要な変更は、文書化、仕様化、テスト、品質管理及び管理された実装についての合意および規則及び正式な手続に従う。 変更管理手順には、次の事項を含む。 a）全ての依存関係を考慮した、変更の潜在的影響に関する計画策定及び評価 b）変更の認可 c）関連する利害関係者への変更の伝達 d）変更のテスト及びテストの受入れ（8.29参照） e）導入計画を含む変更の実施 f）フォールバック手順（代替手順）を含む緊急時及び不測の事態の考慮 g）上記の全てを含む変更の記録の維持 h）適用文書類（5.37参照）及び利害者手順が、適切な状態であるように、必要に応じて変更することを確実にすること i）ICT継続計画並びに対応及び復旧手順（5.30 参照）が、適切な状態であるように、必要に応じて変更することを確実にすること 情報処理設備及び情報システムの全ての変更を良好に管理することを確実にするように、管理責任及び手順を設ける。 変更管理手順は、情報処理設備及び情報システムにおける情報の機密性、完全性及び可用性を確実にするために、設計の初期段階からその後の全ての保守作業までのシステム開発のライフサイクル全体にわたって文書化し、実装する。 実施可能な場合には、ICT基盤及びソフトウェアの変更管理手順を統合する。
12.1.2.5	組織、業務プロセス、情報処理設備及びシステムの変更管理には、情報セキュリティ要求事項が満たされていることの検証を含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし。（情報セキュリティ管理基準で組承されず）	–	（対応項なし）	–
12.1.2.6	組織、業務プロセス、情報処理設備及びシステムの変更管理には、全ての関係者への変更に関する詳細事項の通知を含める。	8d-8.32.5	変更管理手順には、次の事項を含む。 c）関連する利害関係者への変更の伝達	手引に関連記載あり	8.32.1	【再】情報処理設備及び情報システムの変更管理手順を整備し、対策を実施する。	（8.32.1に対応する項を参照）
12.1.2.7	組織、業務プロセス、情報処理設備及びシステムの変更管理には、うまくいかない変更及びこれに伴う予期できない事象を取り扱い、これらの回復する手順及び責任を含む、代替手順を確立することを含める。	8d-8.32.5	変更管理手順には、次の事項を含む。 f）フォールバック手順（代替手順）を含む緊急時及び不測の事態の考慮	手引に関連記載あり			
12.1.2.8	組織、業務プロセス、情報処理設備及びシステムの変更管理には、インシデントの解決のために必要な変更を、迅速にかつ管理して実施できるように定めの、緊急時の変更プロセスの受け入れを含める。	8d-8.32.5	変更管理手順には、次の事項を含む。 i）ICT継続計画並びに対応及び復旧手順が、適切な状態であるように、必要に応じて変更することを確実にすること	手引に関連記載あり			
12.1.2.9	組織、業務プロセス、情報処理設備及びシステムに対するあらゆる変更の十分な管理を確実にするために、正式な責任体制及び手順を設ける。	8d-8.32.2	情報処理設備及び情報システムの全ての変更を良好に管理することを確実にするように、管理責任及び手順を設ける。	手引に関連記載あり			
12.1.2.10	組織、業務プロセス、情報処理設備及びシステムに対する変更がなされたときには、変更に関わる全ての関連情報を含んだ監査ログを保持する。	8d-8.32.5	変更管理手順には、次の事項を含む。 g）上記の全てを含む変更の記録の維持	手引に関連記載あり			
12.1.2.11.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	8.32.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.1.2.13	情報処理設備及びシステムの変更管理には、運用上の要求事項に適合する最も制限された設定項目を含める。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
12.1.2.14	情報処理設備及びシステムの変更管理には、完全性検証ツールによるソフトウェア及びファームウェアに対する不正な変更の検知を含める。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
12.1.3	容量・能力の管理 要求された主要なシステム資源の使用を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。	8.6	容量・能力の管理 管理策 現在の及び予測される容量・能力の要求事項に合わせて、資源の利用を監視し調整する。 目的 情報処理施設、人的資源、オフィス及びその他の施設で必要とされる容量・能力の確保を確実にするため。		8.6	容量・能力の管理 統制目標：現在の及び予測される容量・能力の要求事項に合わせて、資源の利用を監視し調整する。 目的：情報処理施設、人的資源、オフィス及びその他の施設で必要とされる容量・能力の確保を確実にするため。	
12.1.3.1	事業における変化の重要度を考慮に入れて、その容量・能力に関する要求事項を特定する。	8a-8.6.1	事業におけるシステム及びプロセスの重要度を考慮に入れて、情報処理施設、人的資源、オフィス及びその他の施設の容量・能力に関する要求事項を特定する。	手引に関連記載あり	8.6.1	情報処理施設、人的資源、オフィス及びその他の施設の容量・能力に関する要求事項を定義する。	事業におけるシステム及びプロセスの重要度を考慮に入れて、情報処理施設、人的資源、オフィス及びその他の施設の容量・能力に関する要求事項を特定する。 業務上必須のシステムについては、容量・能力の管理計画を文書化することを検討する。
12.1.3.2	システムの可用性及び効率性を確実にするため、また、改善のために、システム調整及び監視を適用する。	8a-8.6.2	システムの可用性及び効率性の確保を確実にするため、また、必要な場合には、改善のために、システムの調整及び監視を適用する。	手引に関連記載あり			
–	（対応項なし）	8a-8.6.3	組織は、最大性能の要求事項を満たすのに十分なシステム容量・能力が利用できることを確認するために、システム及びサービスの負荷テストを実施する。	手引に関連記載あり	8.6.2	資源の利用を監視する。	システムの可用性及び効率性の確保を確実にするため、また、必要な場合には、改善のために、システムの調整及び監視を適用する。 適切な時点で問題を知らせるために、検知のための管理策を備える。 資源不足による情報セキュリティインシデントを防ぐため、資源の容量を監視する。 組織は、最大性能の要求事項を満たすのに十分なシステム容量・能力が利用できることを確認するために、システム及びサービスの負荷テストを実施する。
12.1.3.3	適切な時点で問題を知らせるために、検知のための管理策を備える。	8a-8.6.4	適切な時点で問題を知らせるために、検知のための管理策を備える。	手引に関連記載あり			
12.1.3.4	将来必要とされる容量・能力の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理の能力についての現在の傾向及び予測される傾向を含める。	8a-8.6.5	将来必要とされる容量・能力の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理の能力についての現在の傾向及び予測される傾向を考慮する。	手引に関連記載あり	8.6.3	容量・能力に脆弱があると予測される場合は、容量・能力の増強又は需要の低減を実施する。	将来必要とされる容量・能力の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理の能力についての現在の傾向及び予測される傾向を考慮する。 入手に長い期間又は高額な費用がかかる資源については、特別な注意を払うため、管理者、及びサービス又は製品の管理責任者は、主要なシステム資源の使用を監視する。 システムセキュリティ又はサービスに脅威をもたらす可能性がある、潜在的な資源の制限及び主要な要員への依存度合いを特定し、回避するために、管理者は、容量・能力に関する脆弱を問い、また、適切な処置を立案する。 十分な容量・能力の提供は、容量・能力の増強又は需要の低減によって達成することが可能である。 容量・能力を増強するには、次の事項を考慮する。 a）新しい要員を雇用する。 b）新しい施設又は場所を取得する。 c）より強力な処理システム、メモリ及びストレージを取得する。 d）容量・能力の課題に直接に応えるという特性があるクラウドコンピューティングを利用する。クラウドコンピューティングは、特定のアプケーション及びサービスで利用できる資源を要求に応じて迅速に拡張し、削減することを可能とする。弾力性及びスケーラビリティをもっている。 組織の資源に関する需要を減らすために、次の事項を考慮する。 a）古いデータの削除（ディスクスペース） b）保持期間を満了したハードコピー記録の処分（個スペースを空ける。） c）アプケーション、システム、データベーススは環境の廃止 d）バッチのスケジュリングスケジュールの最適化 e）アプリケーションコード及びデータベースへの問合せの最適化 f）重要でない場合、大量の単域をお要とするサービスに対する単域割当ての拡張又は制限
12.1.3.5	管理者は、特別な注意を払う必要のある主要なシステム資源（入手時間がかかるか又は費用がかかる資源）の使用を監視する。	8a-8.6.6	入手に長い期間又は高額な費用がかかる資源については、特別な注意を払うため、管理者、及びサービス又は製品の管理責任者は、主要なシステム資源の使用を監視する。	手引に関連記載あり			
12.1.3.6	管理者は、使用の傾向、特に業務用アプケーション又は情報システムの管理ツールに関連した傾向を特定する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし。（情報セキュリティ管理基準で組承されず）	–	（対応項なし）	–
12.1.3.7	システムセキュリティ又はサービスに脅威をもたらすおそれのある、潜在的なあい（隘）路（bottlenecks）及び主要な要員への依存度合いを特定し、回避するために、管理者は、上記の監視及び傾向を特定した情報を利用して、適切な処置を立案する。	8a-8.6.7	システムセキュリティ又はサービスに脅威をもたらす可能性のある、潜在的な資源の制限及び主要な要員への依存度合いを特定し、回避するために、管理者は、容量・能力に関する情報を用い、また、適切な処置を立案する。	手引に関連記載あり	8.6.3	【再】容量・能力に脆弱があると予測される場合は、容量・能力の増強又は需要の低減を実施する。	（8.6.3に対応する項を参照）
–	（対応項なし）	8a-8.6.8	容量・能力を増強するには、次の事項を考慮する。 a）新しい要員を雇用する。 b）新しい施設又は場所を取得する。 c）より強力な処理システム、メモリ及びストレージを取得する。 d）容量・能力の課題に直接に応えるという特性があるクラウドコンピューティングを利用する。クラウドコンピューティングは、特定のアプケーション及びサービスで利用できる資源を要求に応じて迅速に拡張し、削減することを可能とする。弾力性及びスケーラビリティをもっている。	手引に関連記載あり			
–	（対応項なし）	8a-8.6.9	組織の資源に関する需要を減らすために、次の事項を考慮する。 a）古いデータの削除（ディスクスペース） b）保持期間を満了したハードコピー記録の処分（個スペースを空ける。） c）アプケーション、システム、データベーススは環境の廃止 d）バッチのスケジュリングスケジュールの最適化 e）アプリケーションコード及びデータベースへの問合せの最適化 f）重要でない場合、大量の単域をお要とするサービスに対する単域割当ての拡張又は制限	手引に関連記載あり			
12.1.3.8	業務上必須のシステムについては、容量・能力の管理計画を文書化することを検討する。	8a-8.6.10	業務上必須のシステムについては、容量・能力の管理計画を文書化することを検討する。	手引に関連記載あり			
12.1.3.9.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり（情報セキュリティ管理基準以外の由来）	8.6.2	資源の利用を監視する。	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.1.4	開発環境、試験環境及び運用環境の分離 開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更による(リスクを低減するために、分離する。	8.31	開発環境、テスト環境及び本番環境の分離 管理策 開発環境、テスト環境及び本番環境は、分離してセキュリティを保つ。 目的 開発活動及びテスト活動による危険から本番環境及びそのデータを保護するため。		8.31	開発環境、テスト環境及び本番環境の分離 統制目標：開発環境、テスト環境及び本番環境は、分離してセキュリティを保つ。 目的：開発活動及びテスト活動による危険から本番環境及びそのデータを保護するため。	
12.1.4.1	運用上の問題を防ぐために必要な、開発環境、試験環境及び運用環境の間の分離レベルを特定し、それに従って分離する。	8d-8.31.1	本番環境における問題を防ぐために必要な、本番環境、テスト環境及び開発環境の間の分離レベルを特定し、それに従って分離する。	手引に関連記載あり	8.31.1	本番環境、テスト環境及び開発環境の間の分離レベルを特定し、分離する。	本番環境における問題を防ぐために必要な、本番環境、テスト環境及び開発環境の間の分離レベルを特定し、それに従って分離する。 開発環境、テスト環境及び本番環境の分離を実施には、特に、次の事項を考慮する。 a）開発システムと本番システムとを適切に分離し、それらを異なる領域で（例えば、別々の仮想環境又は物理環境で）運用する。 b）開発段階から本番段階へのソフトウェアの導入に関する規則及び認可を、明確に定め、文書化し、実施する。 c）本番システム及びアプケーションに対する変更は、本番システムに適用する前に、テスト環境又はステージング環境でテストする（8.29参照）。 d）特定し、承認された状況を除いて、本番環境ではテストを行わない。 e）コンパイラ、エディタ、及びその他の開発ツール又はユーティティプログラムは、必要がないときには、本番システムからアクセス可能としない。 f）誤りのリスクを減らすために、メニューに適切な環境識別ラベルを表示する。 g）取扱いに際重を要する情報は、開発システム及びテストシステムに同等の管理策が備わっていない限り、その開発システム環境及びテストシステム環境にはコピーしない。
12.1.4.2	ソフトウェアの開発から運用の段階への移行についての規則は、明確に定め、文書化する。	8d-8.31.2	開発環境、テスト環境及び本番環境の分離するを目には、特に、次の事項を考慮する。 b）開発段階から本番段階へのソフトウェアの導入に関する規則及び認可を、明確に定め、文書化し、実施する。	手引に関連記載あり			
12.1.4.3	開発ソフトウェア及び運用ソフトウェアは、異なるシステム又はコンピュータ上で、及び異なる領域又はディレクトリで実行する。	8d-8.31.2	開発環境、テスト環境及び本番環境の分離するを目には、特に、次の事項を考慮する。 a）開発システムと本番システムとを適切に分離し、それらを異なる領域で運用する。	手引に関連記載あり			
12.1.4.4	運用システム及びアプケーションに対する変更は、運用システムに適用する前に、試験環境又はステージング環境（運用環境に近い試験環境）で試験する。	8d-8.31.2	開発環境、テスト環境及び本番環境の分離するを目には、特に、次の事項を考慮する。 c）本番システム及びアプケーションに対する変更は、本番システムに適用する前に、テスト環境又はステージング環境でテストする。	手引に関連記載あり			
12.1.4.5	例外的な状況以外では、運用システムで試験を行わない。	8d-8.31.2	開発環境、テスト環境及び本番環境の分離するを目には、特に、次の事項を考慮する。 d）特定し、承認された状況を除いて、本番環境ではテストを行わない。	手引に関連記載あり			
12.1.4.6	コンパイラ、エディタ、及びその他の開発ツール又はシステムユーティティは、必要でない場合には、運用システムからアクセスできないようにする。	8d-8.31.2	開発環境、テスト環境及び本番環境の分離するを目には、特に、次の事項を考慮する。 e）コンパイラ、エディタ、及びその他の開発ツール又はユーティティプログラムは、必要がないときには、本番システムからアクセス可能としない。	手引に関連記載あり			
12.1.4.7	利用者は、運用システム及び試験システムに対して、異なるユーザプロファイルを用いる。	8d-8.31.2	開発環境、テスト環境及び本番環境の分離するを目には、特に、次の事項を考慮する。 f）誤りのリスクを減らすために、メニューに適切な環境識別ラベルを表示する。	手引に関連記載あり			
12.1.4.8	メニューには、誤操作による(リスクを低減するために、適切な識別メッセージを表示する。	8d-8.31.2	【再】開発環境、テスト環境及び本番環境の分離するを目には、特に、次の事項を考慮する。 f）誤りのリスクを減らすために、メニューに適切な環境識別ラベルを表示する。	手引に関連記載あり			
12.1.4.9	取扱いに慎重を要するデータは、試験システムに同等の管理策が備わっていない限り、その試験システム環境には複写を許止する。	8d-8.31.2	開発環境、テスト環境及び本番環境の分離するを目には、特に、次の事項を考慮する。 g）取扱いに慎重を要する情報は、開発システム及びテストシステムに同等の管理策が備わっていない限り、その開発システム環境及びテストシステム環境にはコピーしない。	手引に関連記載あり			
12.1.5.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		9.5	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.1.5.1.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.5.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）

番号	（旧）管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	（新）管理策基準	（参考）手引き
12.2	マルウェアからの保護 管理目的：情報及び情報処理施設がマルウェアから保護されることを確実にするため。	8.7	マルウェアに対する保護 管理策 マルウェアに対する保護を実施し、利用者の適切な認識によって支援する。 目的 情報及びその他の関連資産をマルウェアに対して保護することを確実にするため。		8.7	マルウェアに対する保護 統制目標：マルウェアに対する保護を実施し、利用者の適切な認識によって支援する。 目的：情報及びその他の関連資産をマルウェアに対して保護することを確実にするため。	
12.2.1	マルウェアに対する管理策 マルウェアから保護するために、利用者に適切に認識させるとと併せて、検出、予防及び回復のための管理策を実施する。						
12.2.1.1	マルウェアに対する検出・修復ソフトウェア、情報セキュリティに対する認識、及びシステムへの適切なアクセス・変更管理、及び外部からの不正通信の監視・分析に基づく悪意等の対応についての管理策により、マルウェアから保護する。	8b-8.7.1	マルウェアに対する保護には、マルウェアの検出・修復ソフトウェア、情報セキュリティに対する認識、及びシステムへの適切なアクセス・変更管理についての管理策に基づく、通常、マルウェアの検出・修復ソフトウェアを単独で使用するだけは十分ではない。	千代に関連記載あり	8.7.1	情報及びその他の関連資産をマルウェアから保護する。	マルウェアに対する保護には、マルウェアの検出・修復ソフトウェア、情報セキュリティに対する認識、及びシステムへの適切なアクセス・変更管理についての管理策に基づく、通常、マルウェアの検出・修復ソフトウェアを単独で使用するだけは十分ではない。 マルウェアに対する保護については、次の手引きを考慮する。 a）認可されていないソフトウェアの使用を防止又は検出するための規則及び管理策の実施（例えば、アプリケーションの許可リスト（すなわち、許可されたアプリケーションを示すリストの使用）（8.19及び8.32参照） b）悪意のあるウェブサイトであり知られている又は疑われるウェブサイトの使用を、防止又は検出するための管理策の実施（例えば、ブロックリスト） c）マルウェアに付け込まれる可能性のあるぜい弱性を減らす（例えば、技術的ぜい弱性管理によって（8.8及び9参照））。 d）システム、特に重要な業務プロセスを支えるシステムのソフトウェア及びデータについて、定期的な自動化された安当性確認の実施。承認されていないファイル又は認可されていない変更の存在を調査する。 e）外部ネットワークから若しくは外部ネットワーク提供で、又は他の媒体を通じてファイル及びソフトウェアを入手するごとにおけるリスクに対する保護対策を確立する。 f）コンピュータ及び電子型情報媒体をスキャンするための、マルウェアの検出・修復ソフトウェアの導入及び定期的な更新、次の事項を含む定期的なスキャンを実施する。 1）ネットワーク経由又は何らかの形式の電子型情報媒体を通じて入手した全てのデータに対する、マルウェア検出のための悪意のスキャン 2）電子メールスパイングストメッセージングの添付ファイル及びダウンロードしたファイルに対する、マルウェア検出のための悪意のスキャン 3）ウェブページに対するアクセスの際のマルウェア検出のためのスキャン g）リスクアセスメントの結果に基づき、かつ、次の事項を考慮して、マルウェアの検出・修復ツールの配置及び構成を決定する。 1）特に効果的である場合には、多層防御の原則。例えば、これはネットワークゲートウェイ（電子メール、ファイル転送、ウェブなどの様々なアプリケーション・プロトコルにおける）、並びに利用者エンドポイント機器及びサーバにおいて、マルウェアの検出につながる可能性がある。 2）攻撃者がマルウェアを送り込むための回避技術（例えば、暗号化されたファイルの使用）、又はマルウェアの送信における暗号化プロトコルの使用 h）マルウェアに対する通常の管理策を5（注）に関する可能性がある、保守及び緊急時の手順中におけるマルウェアの入り込みの防止に注意をおう。 i）例外承認機能、文書化した正当性の提示、及びレビューの日付を含む、マルウェアに対する一部又は全ての対策の一時的又は恒久的な無効化を認可する プロセスを実施する。これは、マルウェアに対する保護によって通常の運用が中断・阻害される場合に必要になる可能性がある。 j）マルウェアの攻撃や回復するための適切な管理策統計書の策定、これには、必要な全てのデータ及びソフトウェアのバックアップ（オンラインとオフラインの両方のバックアップを含む。）並びに回復の封筆を含める（8.13参照） k）環境的な影響が生じる可能性のある環境の隔離 l）システムとてマルウェアに対する保護を扱う手順及び責任の定義。これには、手順の使用、報告及びマルウェア攻撃からの回復に関する説明を含む。 m）マルウェアに感染した電子メール、ファイル又はプログラムの受信、送信又はインストールを特定し、可能ならば軽減する方法について、全ての利用者に意識向上又は訓練（6.3参照）を提供する（n)及びo)で収集された情報を、意識向上及び訓練を最新状態に保つことを確実にするために使用することが可能である。） n）定常的に新種のマルウェアに関する情報を収集するための手順の実施（例えば、メーリングリストへの登録又はウェブサイトの閲覧） o）提供者提供のマルウェアに関する情報が適格で正評のある情報源（例えば、信頼できるインターネットサイト、マルウェア検出ソフトウェアの供給者）から来ており、正確かつ役立つことを検証する。	
12.2.1.2	認可されていないソフトウェアの使用を禁止する正式な方針を確立し、定期的に見直しを行う。	8b-8.7.2	マルウェアに対する保護については、次の手引きを考慮する。 a）認可されていないソフトウェアの使用を防止又は検出するための規則及び管理策の実施	千代に関連記載あり			
12.2.1.3	認可されていないソフトウェアの使用を防止又は検出するための管理策を実施（例えば、アプリケーションのホワイトリスト化）する。	8b-8.7.2	【再】マルウェアに対する保護については、次の手引きを考慮する。 a）認可されていないソフトウェアの使用を防止又は検出するための規則及び管理策の実施	千代に関連記載あり			
12.2.1.4	悪意のあるウェブサイトであるか知られている又は疑われるウェブサイトの使用を、防止又は検出するための管理策を実施（例えば、ブラックリスト）する。	8b-8.7.2	マルウェアに対する保護については、次の手引きを考慮する。 b）悪意のあるウェブサイトであるか知られている又は疑われるウェブサイトの使用を、防止又は検出するための管理策の実施	千代に関連記載あり			
12.2.1.5	外部ネットワークから若しくは外部ネットワーク経由で、又は他の媒体を通じてファイル及びソフトウェアを入手するごとにおけるリスクに対する保護対策を確立する。	8b-8.7.2	マルウェアに対する保護については、次の手引きを考慮する。 e）外部ネットワークから若しくは外部ネットワーク経由で、又は他の媒体を通じてファイル及びソフトウェアを入手するごとにおけるリスクに対する保護対策を確立する。	千代に関連記載あり			
12.2.1.6	マルウェアに付け込まれる可能性のあるぜい弱性を、技術的ぜい弱性管理などを通じて低減させる。	8b-8.7.2	マルウェアに対する保護については、次の手引きを考慮する。 c）マルウェアに付け込まれる可能性のあるぜい弱性を調査する。	千代に関連記載あり			
12.2.1.7	重要な業務プロセスを支えるシステムのソフトウェア及びデータの、定めに従った レビューを実施する。未承認のファイル又は認可されていない変更が見つかった場合には、正式に調査する。	8b-8.7.2	マルウェアに対する保護については、次の手引きを考慮する。 d）システム、特に重要な業務プロセスを支えるシステムのソフトウェア及びデータについて、定常的な自動化された安当性確認の実施。承認されていないファイル又は認可されていない変更の存在を調査する。	千代に関連記載あり			
12.2.1.8	予防又は定常作業として、コンピュータ及び媒体を走査（scan）するために、マルウェアの検出・修復ソフトウェアの導入及び定めに従った更新として、以下のことを行う。 1．ネットワーク経由又は何らかの形式の記憶媒体を通じて入手した全てのファイルに対する、マルウェア検出のための使用前の走査。 2.電子メールの添付ファイル及びダウンロードしたファイルに対する、マルウェア検出のための使用前の走査。この走査は、様々な場所（例えば、電子メールサーバ、デスクトップコンピュータ、組織のネットワークの入口）で実施する。 3.ウェブページに対するマルウェア検出のための走査。	8b-8.7.2	マルウェアに対する保護については、次の手引きを考慮する。 f）コンピュータ及び電子型情報媒体をスキャンするための、マルウェアの検出・修復ソフトウェアの導入及び定期的な更新、次の事項を含む定期的なスキャンを実施する。 1）ネットワーク経由又は何らかの形式の電子型情報媒体を通じて入手した全てのデータに対する、マルウェア検出のための悪意のスキャン 2）電子メールスパイングストメッセージングの添付ファイル及びダウンロードしたファイルに対する、マルウェア検出のための使用前のスキャン 3）ウェブページに対するアクセスの際のマルウェア検出のためのスキャン	千代に関連記載あり			
12.2.1.9	システムにおけるマルウェアからの保護、保護策の利用方法に関する訓練、マルウェアの攻撃の報告及びマルウェアの攻撃からの回復に関する手順及び責任を明確にする。	8b-8.7.2	マルウェアに対する保護については、次の手引きを考慮する。 l）システムとてマルウェアに対する保護を扱う手順及び責任の定義。これには、手順の使用、報告及びマルウェア攻撃からの回復に関する説明を含む。	千代に関連記載あり			
12.2.1.10	マルウェアの攻撃から回復するための適切な事業継続計画を策定する。	8b-8.7.2	マルウェアに対する保護については、次の手引きを考慮する。 j）マルウェアの攻撃や回復するための適切な事業継続計画の策定、これには、必要な全てのデータ及びソフトウェアのバックアップ（オンラインとオフラインの両方のバックアップを含む。）並びに回復の封筆を含める。	千代に関連記載あり			
12.2.1.11	マルウェアの攻撃から回復するための適切な事業継続計画には、必要な全てのデータ及びソフトウェアの、バックアップ及び回復の手順を含める。	8b-8.7.2	【再】マルウェアに対する保護については、次の手引きを考慮する。 j）マルウェアの攻撃や回復するための適切な事業継続計画の策定、これには、必要な全てのデータ及びソフトウェアのバックアップ（オンラインとオフラインの両方のバックアップを含む。）並びに回復の封筆を含める。	千代に関連記載あり			
12.2.1.12	新に情報を収集するための手順を実施（例えば、新種のマルウェアに関する情報を提供するメーリングリストへの登録又はウェブサイトの閲覧）する。	8b-8.7.2	マルウェアに対する保護については、次の手引きを考慮する。 n）定常的に新種のマルウェアに関する情報を収集するための手順の実施	千代に関連記載あり			
12.2.1.13	マルウェアに関する情報を確認し、誤誘情報が正確かつ役立つことを確実にするための以下の2つの手順を実施する。 1.管理者は、疑なないずれと真のマルウェアとを識別するために、適切な情報源（例えば、定評のある刊行物、信頼できるインターネットサイト、マルウェアの対策ソフトウェア供給者）の利用を確実にするに社組みを整備する。 2.管理者は、マルウェアではなく、いたずらの問題及びそれらを受け取ったときの対応について、全ての利用者に認識させる仕組みを整備する。	8b-8.7.2	マルウェアに対する保護については、次の手引きを考慮する。 o）提供者提供のマルウェアに関する情報が適格で正評のある情報源（例えば、信頼できるインターネットサイト、マルウェア検出ソフトウェアの供給者）から来ており、正確かつ役立つことを検証する。	千代に関連記載あり			
12.2.1.14	環境的な影響が及ぶ可能性のある環境を隔離する。	8b-8.7.2	マルウェアに対する保護については、次の手引きを考慮する。 k）環境的な影響が生じる可能性のある環境の隔離	千代に関連記載あり			
12.2.1.15	マルウェアに対する検出精度向上や感染リスクの低減の手段（例えば、機械学習方式又はサンドボックス型の不正対策プログラム等）を実施する。	–	（統一基準由来）	明確な対応関係なし	–	（対応項なし）	–
12.3	バックアップ 管理目的：データの消失から保護するため。	8.13	情報のバックアップ 管理策 合意された バックアップに関するトピック固有の方針に従って、情報、ソフトウェア及びシステムのバックアップを維持し、定期的に検査する。 目的 データ又はシステムの損失からの回復を可能にするため。		8.13	情報のバックアップ 統制目標：合意された バックアップに関するトピック固有の方針に従って、情報、ソフトウェア及びシステムのバックアップを維持し、定期的に検査する。 目的：データ又はシステムの損失からの回復を可能にするため。	
12.3.1	情報のバックアップ 情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査する。						
12.3.1.1	バックアップ方針を確立し、情報、ソフトウェア及びシステムイメージのバックアップに関する組織の要求事項を定める。	8b-8.13.1	組織のデータ保持及び情報セキュリティの要求事項に対応するために、バックアップに関するトピック固有の方針を確立する。	千代に関連記載あり	8.13.1	組織のデータ保持及び情報セキュリティの要求事項に対応するために、バックアップに関する方針を策定する。	組織のデータ保持及び情報セキュリティの要求事項に対応するために、バックアップに関するトピック固有の方針を確立する。 インシデント又は記憶媒体の故障若しくは損失の後に、全ての重要な情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備える。 重要なシステム及びサービスに関するバックアップ対策は、災害に際してシステム全体を復旧させるために必要になる、システム情報、アプリケーション及びデータの全てを対象とする。 組織がクラウドサービスを利用する場合、クラウドサービス環境にある組織の情報、アプリケーション及びシステムのバックアップ情報を作成する。 組織は、クラウドサービスの一部として提供される情報バックアップサービスを利用する場合、バックアップの要求事項が満たされるかどうか、また、どのように満たされるかを特定する。 重要な業務情報の保持期間は、職業の保存に関するあらゆる要求事項を考慮に入れて、決定する。 組織は、情報の保持期間が終了したら、バックアップに使用している記憶媒体にある情報の削除（8.10参照）、また、活性及び残存を考慮する。
12.3.1.2	バックアップ方針では、保管及び保護に関する要求事項を定める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で規承されず）	–	（対応項なし）	–
12.3.1.3	災害又は媒体故障の発生の後に、全ての重要な情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備える。	8b-8.13.2	インシデント又は記憶媒体の故障若しくは損失の後に、全ての重要な情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備える。	千代に関連記載あり	8.13.1	【再】組織のデータ保持及び情報セキュリティの要求事項に対応するために、バックアップに関する方針を策定する。	（8.13.1に対応する項を参照）
–	（対応項なし）	8b-8.13.3	バックアップに関するトピック固有の方針に対応するため、組織は、情報、ソフトウェア及びシステム並びにバックアップする方法について計画を作成し、実装する。	千代に関連記載あり	8.13.2	バックアップ計画を策定し、実装する。	バックアップに関するトピック固有の方針に対応するため、組織は、情報、ソフトウェア及びシステム並びにバックアップする方法について計画を作成し、実装する。 バックアップ計画を策定するとき、次の事項を考慮に入れる。 a）バックアップ情報の正確かつ完全な記録及び文書化した データ復旧手順を作成する。 b）バックアップの範囲（例えば、フルバックアップ、差分バックアップ）及びバックアップの頻度は、組織の事業上の要求事項、関連する情報のセキュリティ要求事項、及び止めの情報の組織の継続的な運用に対する重要度を考慮して決定する。 c）バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた安全でセキュリティを保った場所に保管する。 d）バックアップ情報に対して、主事業所に適用されている標準と整合した、適切なレベルの物理的及び環境的保護（箇条7及び8.1参照）を実施する。 e）バックアップに用いる媒体は、必要になった場合の緊急利用について信頼できることを確実にするために、定期的に試験する。バックアップデータで復旧する機能のテストは、バックアップ又はデータ復旧プロセスに失敗して、データに修復不能な損傷又は損失が生じることがないよう、テストシステム上で行い、原本の記憶媒体に上書きしない。 f）特定しだリスクに応じて、暗号化によってバックアップ情報を保護する（例えば、機密性が重要な状況において）。 g）バックアップを作成する前に、不注意によるデータ損失の検出を確実にするよう工夫する。
12.3.1.4	バックアップ情報の正確かつ完全な記録及び文書化したデータ復旧手順を作成する。	8b-8.13.4	バックアップ計画を策定するとき、次の事項を考慮に入れる。 a）バックアップ情報の正確かつ完全な記録及び文書化したデータ復旧手順を作成する。	千代に関連記載あり			
12.3.1.5	バックアップの範囲（例えば、フルバックアップ、差分バックアップ）、及びバックアップの頻度は、組織の業務上の要求事項、関連する情報のセキュリティ要求事項、及びその情報の組織の事業継続に対しての重要度を考慮して決定する。	8b-8.13.4	バックアップ計画を策定するとき、次の事項を考慮に入れる。 b）バックアップの範囲、及びバックアップの頻度は、組織の事業上の要求事項、関係するその情報のセキュリティ要求事項、及びその情報の組織の継続的な運用に対する重要度を考慮して決定する。	千代に関連記載あり			
12.3.1.6	バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた場所に保管する。	8b-8.13.4	バックアップ計画を策定するとき、次の事項を考慮に入れる。 c）バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた安全でセキュリティを保った場所に保管する。	千代に関連記載あり			
12.3.1.7	バックアップ情報に対して、主事業所に適用されている標準と整合した、適切なレベルの物理的及び環境的保護を実施する。	8b-8.13.4	バックアップ計画を策定するとき、次の事項を考慮に入れる。 d）バックアップ情報に対して、主事業所に適用されている標準と整合した、適切なレベルの物理的及び環境的保護を実施する。	千代に関連記載あり			
12.3.1.8	バックアップに用いる媒体は、必要になった場合の緊急利用について信頼できることを確実にするために、定めに従って試験する。	8b-8.13.4	バックアップ計画を策定するとき、次の事項を考慮に入れる。 e）バックアップに用いる媒体は、必要になった場合の緊急利用について信頼できることを確実にするために、定期的に試験する。バックアップデータで復旧する機能のテストは、バックアップ又はデータ復旧プロセスに失敗して、データに修復不能な損傷又は損失が生じることがないよう、テストシステム上で行い、原本の記憶媒体に上書きしない。	千代に関連記載あり			
12.3.1.9	バックアップに用いる媒体の試験は、データ復旧手順の試験と併せて行い、必要なデータ復旧時間に照らし合わせて確認する。	8b-8.13.4	【再】バックアップ計画を策定するとき、次の事項を考慮に入れる。 e）バックアップに用いる媒体は、必要になった場合の緊急利用について信頼できることを確実にするために、定期的に試験する。バックアップデータで復旧する機能のテストは、バックアップ又はデータ復旧プロセスに失敗して、データに修復不能な損傷又は損失が生じることがないよう、テストシステム上で行い、原本の記憶媒体に上書きしない。	千代に関連記載あり			
12.3.1.10	バックアップデータを復旧させる能力の試験は、バックアップ手順又はデータ復旧プロセスに失敗し、データに修復不能な損傷又は損失が発生した場合に備えて、原本の媒体に上書きするのではなく、専用の試験媒体を用いて行う。	8b-8.13.4	【再】バックアップ計画を策定するとき、次の事項を考慮に入れる。 e）バックアップに用いる媒体は、必要になった場合の緊急利用について信頼できることを確実にするために、定期的に試験する。バックアップデータで復旧する機能のテストは、バックアップ又はデータ復旧プロセスに失敗して、データに修復不能な損傷又は損失が生じることがないよう、テストシステム上で行い、原本の記憶媒体に上書きしない。	千代に関連記載あり			
12.3.1.11	機密性が重要な場合には、暗号化によってバックアップ情報を保護する。	8b-8.13.4	バックアップ計画を策定するとき、次の事項を考慮に入れる。 f）特定しだリスクに応じて、暗号化によってバックアップ情報を保護する。	千代に関連記載あり			
12.3.1.12	運用手順では、バックアップ方針に従って、バックアップの完全性を確保するために、その実行を監視し、計画されたバックアップの失敗に対処する。	8b-8.13.5	バックアップの運用手順では、バックアップに関するトピック固有の方針に従って、バックアップの完全性を確保するために、その実行を監視し、計画したバックアップの失敗に対処する。	千代に関連記載あり	8.13.3	バックアップの実行を監視し、失敗した場合は適切に対処する。	バックアップの運用手順では、バックアップに関するトピック固有の方針に従って、バックアップの完全性を確保するために、その実行を監視し、計画したバックアップの失敗に対処する。
12.3.1.13	個々のシステム及びサービスに関するバックアップの取決めは、事業継続計画の要求事項を満たすことを確実にするために、定めに従って試験する。	8b-8.13.6	個々のシステム及びサービスに関するバックアップ対策は、インシデント対応及び事業継続計画の日的を満たすことを確実にするために、定期的に試験する。	千代に関連記載あり	8.13.4	個々のシステム及びサービスに関するバックアップ対策は、インシデント対応及び事業継続計画の日的を満たすことを確実にするために、定期的に試験する。 定期的な試験は、これを復旧手順のテストと組み合わせて、事業継続計画において必要とされる復旧時間に照らして確認する。	個々のシステム及びサービスに関するバックアップ対策は、インシデント対応及び事業継続計画の日的を満たすことを確実にするために、定期的に試験する（5.30参照）。
–	（対応項なし）	8b-8.13.7	定期的な試験は、これを復旧手順のテストと組み合わせて、事業継続計画において必要とされる復旧時間に照らして確認する。	千代に関連記載あり			
12.3.1.14	重要なシステム及びサービスに関するバックアップの取決めは、災害に際してシステム全体を復旧させるために必要となる、システム情報、アプケーション及びデータの全てを対象とする。	8b-8.13.8	重要なシステム及びサービスに関するバックアップ対策は、災害に際してシステム全体を復旧させるために必要となる、システム情報、アプリケーション及びデータの全てを対象とする。	千代に関連記載あり	8.13.1	【再】組織のデータ保持及び情報セキュリティの要求事項に対応するために、バックアップに関する方針を策定する。	（8.13.1に対応する項を参照）
–	（対応項なし）	8b-8.13.9	組織がクラウドサービスを利用する場合、クラウドサービス環境にある組織の情報、アプリケーション及びシステムのバックアップ情報を作成する。	千代に関連記載あり			
–	（対応項なし）	8b-8.13.10	組織は、クラウドサービスの一部として提供されるバックアップサービスを利用する場合、バックアップの要求事項が満たされるかどうか、また、どのように満たされるかを特定する。	千代に関連記載あり			
12.3.1.15	永久保存する機密情に関するあらゆる要求事項を考慮に入れて、不可欠な業務情報の保留期間を決定する。	8b-8.13.11	重要な業務情報の保持期間は、職業の保存に関するあらゆる要求事項を考慮に入れて、決定する。	千代に関連記載あり			
–	（対応項なし）	8b-8.13.12	組織は、情報の保持期間が終了したら、バックアップに使用している記憶媒体にある情報の削除、また、活性及び残存を考慮する。	千代に関連記載あり			
12.3.1.16.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）	8.13.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.3.1.17.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	千代に関連記載あり （情報セキュリティ管理基準以外の由来）			
12.3.1.18.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	千代に関連記載あり （情報セキュリティ管理基準以外の由来）			
12.3.1.19.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	千代に関連記載あり （情報セキュリティ管理基準以外の由来）			
12.3.1.20.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	千代に関連記載あり （情報セキュリティ管理基準以外の由来）			
12.3.1.21.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	千代に関連記載あり （情報セキュリティ管理基準以外の由来）			
12.3.1.22.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	千代に関連記載あり （情報セキュリティ管理基準以外の由来）			
12.3.1.23.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	千代に関連記載あり （情報セキュリティ管理基準以外の由来）			
12.3.1.24.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）	8.13.7	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.4	ログ取得及び監視 管理目的：イベントを記録し、証拠を作成するため。	8.15	ログ取得 管理策 活動、例外処理、過失及びその他の関連する事象を記録したログを取得し、保存し、保護し、分析する。 目的 事象を記録し、証拠を生成し、ログ情報の完全性を確実にし、認可されていないアクセスを防止し、情報セキュリティインシデントにつながる可能性のある情報セキュリティ事象を特定し、調査を支援するため。		8.15	ログ取得 統制目標：活動、例外処理、過失及びその他の関連する事象を記録したログを取得し、保存し、保護し、分析する。 目的：事象を記録し、証拠を生成し、ログ情報の完全性を確実にし、認可されていないアクセスを防止し、情報セキュリティインシデントにつながる可能性のある情報セキュリティ事象を特定し、調査を支援するため。	
12.4.1	イベントログ取得 利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。						

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
–	（対応項なし）	8b-8.15.1	組織は、ログを作成する目的、どのデータを収集し、ログに記録するか、及びログデータを保護し、取り扱うためのログ特有の要求事項を決定する。	于引に関連記載あり	8.15.1	ログ特有の要求事項を定義し、ログ取得に関する方針を策定し、取得する。	組織は、ログを作成する目的、どのデータを収集し、ログに記録するか、及びログデータを保護し、取り扱うためのログ特有の要求事項を決定する。 ログ特有の要求事項は、ログ取得に関するトピック固有の方針に文書化する。 活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。 a) 利用者ID b) システムの動作 c) 関係する事象の日時及び内容（例えば、ログオン、ログオフ） d) 装置・機器の識別情報、システムの識別子及び所在地 e) ネットワークアドレス及びプロトコル 次の事項について、ログ取得を検討する。 a) システムへのアクセスの、成功及び失敗した試み b) データ及び他の資源へのアクセスの、成功及び失敗した試み c) システム構成の変更 d) 特権の利用 e) ユーティリティプログラム及びアプリケーションの利用 f) アクセスされたファイル、及び重要なデータファイルの削除を含むアクセスの種類 g) アクセス制御システムが発した警報 h) セキュリティシステム（例えば、ウイルス対策システム、侵入検知システム）の起動及び停止 i) 識別情報の作成、変更又は削除 j) アプリケーションにおいて利用者が実行したトランザクション。このアプリケーションは、第三者が提供又は実行するサービスでは製品の場合がある。 インシデントの分析、普段及び調査のためにシステム間のログを関係付けられるように、全てのシステムが同期した時刻源（8.17参照）をもつことが重要である。
12.4.1.1	イベントログには、利用者IDを含める。	8b-8.15.3	活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。 a) 利用者ID	于引に関連記載あり			
12.4.1.2	イベントログには、システムの動作を含める。	8b-8.15.3	活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。 b) システムの動作	于引に関連記載あり			
12.4.1.3	イベントログには、主要なイベントの日時及び内容（例えば、ログオン、ログオフ）を含める。	8b-8.15.3	活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。 c) 関係する事象の日時及び内容	于引に関連記載あり			
12.4.1.4	イベントログには、装置のID 又は所在地（可能な場合）、及びシステムの識別子を含める。	8b-8.15.3	活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。 d) 装置・機器の識別情報、システムの識別子及び所在地	于引に関連記載あり			
12.4.1.5	イベントログには、システムへのアクセスの、成功及び失敗した試みの記録を含める。	8b-8.15.4	次の事象について、ログ取得を考慮する。 a) システムへのアクセスの、成功及び失敗した試み	于引に関連記載あり			
12.4.1.6	イベントログには、データ及び他の資源へのアクセスの、成功及び失敗した試みの記録を含める。	8b-8.15.4	次の事象について、ログ取得を考慮する。 b) データ及び他の資源へのアクセスの、成功及び失敗した試み	于引に関連記載あり			
12.4.1.7	イベントログには、システム構成の変更を含める。	8b-8.15.4	次の事象について、ログ取得を考慮する。 c) システム構成の変更	于引に関連記載あり			
12.4.1.8	イベントログには、特権の利用を含める。	8b-8.15.4	次の事象について、ログ取得を考慮する。 d) 特権の利用	于引に関連記載あり			
12.4.1.9	イベントログには、システムユーティティ及びアプリケーションの利用を含める。	8b-8.15.4	次の事象について、ログ取得を考慮する。 e) ユーティティプログラム及びアプリケーションの利用	于引に関連記載あり			
12.4.1.10	イベントログには、アクセスされたファイル及びアクセスの種類を含める。	8b-8.15.4	次の事象について、ログ取得を考慮する。 f) アクセスされたファイル、及び重要なデータファイルの削除を含むアクセスの種類	于引に関連記載あり			
12.4.1.11	イベントログには、ネットワークアドレス及びプロトコルを含める。	8b-8.15.3	活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。 e) ネットワークアドレス及びプロトコル	于引に関連記載あり			
12.4.1.12	イベントログには、アクセス制御システムが発した警報を含める。	8b-8.15.4	次の事象について、ログ取得を考慮する。 g) アクセス制御システムが発した警報	于引に関連記載あり			
12.4.1.13	イベントログには、保護システム（例えば、ウィルス対策システム、侵入検知システム）の作動及び停止を含める。	8b-8.15.4	次の事象について、ログ取得を考慮する。 h) セキュリティシステムの起動及び停止	于引に関連記載あり			
12.4.1.14	イベントログには、アプリケーションにおいて利用者が実行したトランザクションの記録を含める。	8b-8.15.4	次の事象について、ログ取得を考慮する。 j) アプリケーションにおいて利用者が実行したトランザクション	于引に関連記載あり			
–	（対応項なし）	（8b-8.15.4参考）	インシデントの分析、普及及び調査のためにシステム間のログを関係付けられるように、全てのシステムが同期した時刻源をもつことが重要である。	于引に関連記載あり			
12.4.1.15.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理策重立外由来）	8.15.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.4.1.17	イベントログには、必要に応じて設置した監視装置が取得した重要なトランザクションの記録を含める。	–	（SP800-53由来）	特理な対応関係なし	–	（対応項なし）	–
12.4.1.18	利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、悪意のある第三者等からの不正侵入、不正操作等の有無について定期的に点検又は分析を実施する。	8b-8.15.11	ログ分析は、侵害の可能性がある通常とは異なる活動又は異常な挙動を特定する活動となるように、情報セキュリティ事象の分析及び解釈を含む。	于引に関連記載あり	8.15.3	ログ分析を実施する。	ログ分析は、侵害の可能性がある通常とは異なる活動又は異常な挙動を特定する活動となるように、情報セキュリティ事象の分析及び解釈を含む。 事象の分析は、次の事項を考慮して実施する。 a) 分析を実施する専門家に必要な技能 b) ログ分析の手順の決定 c) 各セキュリティ関連事象の必要な属性 d) 設定台帳例（例えば、セキュリティ情報及びイベント管理（SIEM）又はファイアウォールの規則、並びに侵入検知システム（IDS）又はマルウェアのシグネチャ）の使用を通じて特定される例外事象 e) 異常な活動及び挙動と比較する［利用者及びエンティティの挙動分析（UEBA）］、既知の挙動パターン及び標準ネットワークトラフィック f) 傾向分析又はパターン分析の結果（例えば、データ分析、ビッグデータ技術及び特定の目的のある分析ツールを使用した結果） g) 利用可能な脅威インテリジェンス ログ分析は、次の事項を含む、異常な挙動を特定し、分析する活動となる監視活動によって支援する。 a) 保護された資源（例えば、ドメインネームシステム（DNS）サーバ、ウェブページ及び共有ファイル）への成功及び失敗したアクセスの試みをレビューする。 b) ボットネットのコマンド アンド コントロール サーバ（以下、C&Cサーバと言う。）への接続のような、悪意のあるサーバへのアウトバウンドネットワーク接続を特定するために、DNSログを確認する。 c) システム及びネットワークから異常な活動に関するサービス提供者からの使用状況報告（例えば、インボイス又はサービス報告）を調べる（例えば、活動のパターンをレビューする）。 d) より正確な検知及びインシデント分析を確実にするために、入口、出口などの物理的監視のイベントログを含める。 e) 効率的で非常に正確な分析を行えるよう、ログを相互に関係付ける。 情報セキュリティインシデントの使い、及び実際の情報セキュリティインシデント特定し（例えば、マルウェア感染又はファイアウォールに対する探査）、更なる調査を行う（例えば、情報セキュリティインシデント管理プロセスの一部として調査を行う。5.25参照）。
12.4.2	ログ情報の保護 ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護する。	8.15	ログ取得 管理策ロ 活動、例外処理、過失及びその他の関連する事象を記録したログを取得し、保存し、保護し、分析する。 目的ロ 事象を記録し、証拠を生成し、ログ情報の完全性を確実にし、認可されていないアクセスを防止し、情報セキュリティインシデントにつながる可能性のある情報セキュリティ事象を特定し、調査を支援するため。		8.15	ログ取得 統制目標：活動、例外処理、過失及びその他の関連する事象を記録したログを取得し、保存し、保護し、分析する。 目的：事象を記録し、証拠を生成し、ログ情報の完全性を確実にし、認可されていないアクセスを防止し、情報セキュリティインシデントにつながる可能性のある情報セキュリティ事象を特定し、調査を支援するため。	
12.4.2.1	記録されたメッセージ形式の変更から保護する。	8b-8.15.7	管理策は、次の事項を含む、ログ情報の認可されていない変更及びログ取得機能の運用上の問題から保護することを目指す。 a) 記録された メッセージ形式の変更	于引に関連記載あり	8.15.2	ログ情報の完全性を確実にするための対策を実施する。	特権的アクセス権をもつ利用者を含め、利用者は自らの活動のログを削除又は停止する権限をもたない。 特権をもつ与えられた利用者に関するアカウンティビティを維持するために、ログを保護及びレビューする。利用者は、その活動の管理下で、情報処理施設・設備に関するログを改変する可能性がある。 管理策は、次の事項を含む、ログ情報の認可されていない変更及びログ取得機能の運用上の問題から保護することを目指す。 a) 記録された メッセージ形式の変更 b) ログファイルの編集又は削除 c) ログファイルを保持している記憶媒体の記録容量を超過した場合のイベント記録の不具合又は過去のイベント記録への上書き ログは保護することと、その手法として、次の使用を考慮する。 a) 標準技術によるハッシュ化 b) 追加専用及び読取り専用ファイルへの記録 c) 公開透明性ファイル（第三者が確認できるようにすることで運用における透明性を確保することを目的として公開されるファイル）への記録 ログは、データ保持に関する要求事項、又は証拠の収集及び保持（5.28参照）のための要求事項によって、保存が求められる場合がある。 組織がエラーのデバッグ又はトラブルシューティングを支援するために、システム又はアプリケーションのログを業者に送信する必要がある場合、利用者名、インターネットプロトコル、IPアドレス、ホスト名、組織名などの情報について、業者に送信する前に、可能な場合はデータマスキング手法（8.11参照）を使用して、ログの非識別化を行う。 イベントログは、取扱いに慎重を要するデータ及び PII を含む可能性があるため、適切なプライバシー保護対策を講じる（5.34参照）。 組織が定める監査ログの保存要件に対応するために、監査ログオンのストレージ容量を割り当てる。
12.4.2.2	認可されていないログファイルの編集又は削除から保護する。	8b-8.15.7	管理策は、次の事項を含む、ログ情報の認可されていない変更及びログ取得機能の運用上の問題から保護することを目指す。 b) ログファイルの編集又は削除	于引に関連記載あり			
12.4.2.3	イベント記録の不具合又は過去のイベント記録への上書きを引き起こす、ログファイル媒体の記録容量超過の問題から記録を保護するため、イベント記録の生成中止などの手順を定める。	8b-8.15.7	管理策は、次の事項を含む、ログ情報の認可されていない変更及びログ取得機能の運用上の問題から保護することを目指す。 c) ログファイルを保持している記憶媒体の記録容量を超過した場合のイベント記録の不具合又は過去のイベント記録への上書き	于引に関連記載あり			
–	（対応項なし）	8b-8.15.8	ログは保護することと、その手法として、次の使用を考慮する。 a) 標準技術によるハッシュ化 b) 追加専用及び読取り専用ファイルへの記録 c) 公開透明性ファイルへの記録	于引に関連記載あり			
–	（対応項なし）	（8b-8.15.8参考）	ログは、データ保持に関する要求事項、又は証拠の収集及び保持のための要求事項によって、保存が求められる場合がある。	于引に関連記載あり			
–	（対応項なし）	8b-8.15.9	組織がエラーのデバッグ又はトラブルシューティングを支援するために、システム又はアプリケーションのログを業者に送信する必要がある場合、利用者名、インターネットプロトコル、IPアドレス、ホスト名、組織名などの情報について、業者に送信する前に、可能な場合はデータマスキング手法を使用してログの非識別化を行う。	于引に関連記載あり			
–	（対応項なし）	8b-8.15.10	イベントログは、取扱いに慎重を要するデータ及び PII を含む可能性があるため、適切なプライバシー保護対策を講じる。	于引に関連記載あり			

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
12.4.3	実務管理者及び運用担当者の作業ログ システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビュー する。	8.15	ログ取得 管理策C 活動、例外処理、過失及びその他の関連する事象を記録し、ログを取得し、保存し、保護し、分析する。 目的C 事象を記録し、証拠を生成し、ログ情報の完全性を確実にし、認可されていないアクセスを防止し、情報セキュリティインシデントにつながる可能性のある情報セキュリティ事象を特定し、調査を支援するため。		8.15	ログ取得 統制目標：活動、例外処理、過失及びその他の関連する事象を記録し、ログを取得し、保存し、保護し、分析する。 目的：事象を記録し、証拠を生成し、ログ情報の完全性を確実にし、認可されていないアクセスを防止し、情報セキュリティインシデントにつながる可能性のある情報セキュリティ事象を特定し、調査を支援するため。	
12.4.3.1	特権を与えられた利用者（システムの実務管理者及び運用担当者）に関する責任追跡性を維持するために、その作業を記録する。	8b-8.15.5	特権的アクセス権をもつ利用者を含め、利用者は自らの活動のログを削除又は停止する権限をもたない。	予引に関連記載あり	8.15.2	【再】ログ情報の完全性を確実にするための対策を実施する。	（8.15.2に対応する項を参照）
12.4.3.2	特権を与えられた利用者（システムの実務管理者及び運用担当者）に関する責任追跡性を維持するために、その利用者の作業のログを保護する。	8b-8.15.6	特権を与えられた利用者に関するアカウンタビリティを維持するために、ログを保護及びレビューする。	予引に関連記載あり			
12.4.3.3	特権を与えられた利用者（システムの実務管理者及び運用担当者）に関する責任追跡性を維持するために、その作業のログを定期的にレビューする。	8b-8.15.6	【再】特権を与えられた利用者に関するアカウンタビリティを維持するために、ログを保護及びレビューする。	予引に関連記載あり			
–	（対応項なし）	（8b-8.15.6参考）	利用者は、その直接の管理下で、情報処理施設・設備に関するログを改変する可能性がある。	予引に関連記載あり			
–	（対応項なし）	8b-8.15.11	ログ分析は、侵害の可能性がある通常とは異なる活動又は異常な挙動を特定する活動となるように、情報セキュリティ事象の分析及び解析を含む。	予引に関連記載あり	8.15.3	【再】ログ分析を実施する。	（8.15.3に対応する項を参照）
–	（対応項なし）	8b-8.15.12	事象の分析は、次の事項を考慮して実施する。 a) 分析を実施する専門家に必要な技能 b) ログ分析の手順の決定 c) 各セキュリティ関連事象の必要な属性 d) 規定の期間の使用を通じて特定された外れ事象 e) 異常な活動及び挙動と比較する利用者及びエンティティの挙動分析（UEBA），既知の挙動パターン及び標準ネットワークトラフィック f) 傾向分析又はパターン分析の結果 g) 利用可能な脅威インテリジェンス	予引に関連記載あり			
–	（対応項なし）	8b-8.15.13	ログ分析は，次の事項を含む，異常な挙動を特定し，分析する助けとなる監視活動によって支援する。 a) 保護された資源への成功及び失敗したアクセスの試みをレビューする。 b) ボットネットのコマンド アンド コントロールサーバ（以下，C&Cサーバという。）への接続のような，悪意のあるサーバへのアウトバウンドネットワーク接続を特定するために，DNSログを確認する。 c) システム及びネットワーク内の異常な活動に関するサービス提供者からの使用状況報告を調べる。 d) より正確な検知及びインシデント分析を確実にするために，入口，出口などの物理的監視のイベントログを調べる。 e) 効率的で非常に正確な分析を行えるように，ログを相互に関係付ける。	予引に関連記載あり			
–	（対応項なし）	8b-8.15.14	情報セキュリティインシデントの疑い，及び実際の情報セキュリティインシデントを特定し、更なる調査を行う。	予引に関連記載あり			
12.4.4	クロックの同期 組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させる。	8.17	クロックの同期 管理策 組織が使用する情報処理システムのクロックは、組織が採用した時刻源と同期させる。 目的 セキュリティ関連の事象及びその他の記録されたデータの関係付け及び分析を可能にし、情報セキュリティインシデントの調査を支援するため。		8.17	クロックの同期 統制目標：組織が使用する情報処理システムのクロックは、組織が採用した時刻源と同期させる。 目的：セキュリティ関連の事象及びその他の記録されたデータの関係付け及び分析を可能にし、情報セキュリティインシデントの調査を支援するため。	
12.4.4.1	時刻の表示、同期及び正確さに関する外部及び内部の要求事項 は、文書化する。	8b-8.17.1	時刻の表現、信頼できる同期及び正確さに関する、外部及び内部の要求事項は、文書化し、実施する。	予引に関連記載あり	8.17.1	クロックは、組織が採用した時刻源と同期させる。	時刻の表現、信頼できる同期及び正確さに関する、外部及び内部の要求事項は、文書化し、実施する。この要求事項は、法令、規則、契約、標準及び内部監査のニーズに由来する可能性がある。 ビル管理システム、入退出システム、及び調査を支援するために使用できるその他のシステムを含む全てのシステムに対して、組織内で基準とする時刻源を考慮して定める。 国の原子時計又は全地球測位システム（GPS）から配信される時刻に基づくクロックを、ログ取得システムの基準クロック、すなわち、正確なタイムスタンプを確実にする一貫性のある依頼できる日付及び時刻源として使用する。 ネットワークで接続された全てのシステムを基準クロックと同期させるために、ネットワークタイムプロトコル（NTP）又は高精度タイムプロトコル（PTP）などのプロトコルを使用する。組織は、外部クロックの依頼性を改善し、変動を適切に管理するために、二つの外部時刻源を同時に使用することが可能である。 クラウドサービスの利用によりクロックの同期が困難となる場合、不一致から生じるリスクを軽減するために、各サービスのログを監視し、差を記録する。複数のクラウドサービスを使用する場合、又はクラウドサービス及びオンプレミスサービスの両方を使用する場合には、クロックの同期が困難なことがある。
–	（対応項なし）	（8b-8.17.1参考）	この要求事項は、法令、規則、契約、標準及び内部監査のニーズに由来する可能性がある。	予引に関連記載あり			
12.4.4.2	組織内で用いるための基準となる時刻源を定める。	8b-8.17.2	ビル管理システム、入退出システム、及び調査を支援するために使用できるその他のシステムを含む全てのシステムに対して、組織内で基準とする時刻源を考慮して定める。	予引に関連記載あり			
12.4.4.3	基準となる時刻源を外部から取得するための組織の取組み及び内部のログを確実に同期させる方法を文書化し、実施する。	8b-8.17.3	国の原子時計又は全地球測位システム（GPS）から配信される時刻に基づくクロックを、ログ取得システムの基準クロック、すなわち、正確なタイムスタンプを確実にする一貫性のある依頼できる日付及び時刻源として使用する。	予引に関連記載あり			
–	（対応項なし）	8b-8.17.4	ネットワークで接続された全てのシステムを基準クロックと同期させるために、ネットワークタイムプロトコル（NTP）又は高精度タイムプロトコル（PTP）などのプロトコルを使用する。	予引に関連記載あり			
–	（対応項なし）	（8b-8.17.4参考）	組織は、外部クロックの依頼性を改善し、変動を適切に管理するために、二つの外部時刻源を同時に使用することが可能である。	予引に関連記載あり			
–	（対応項なし）	8b-8.17.5	クラウドサービスの利用によりクロックの同期が困難となる場合、不一致から生じるリスクを軽減するために、各サービスのログを監視し、差を記録する。	予引に関連記載あり			
–	（対応項なし）	（8b-8.17.5参考）	複数のクラウドサービスを使用する場合、又はクラウドサービス及びオンプレミスサービスの両方を使用する場合には、クロックの同期が困難なことがある。	予引に関連記載あり			
12.4.4.4.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	8.17.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.4.5.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		9.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.4.5.1.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.6.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.4.5.2.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.6.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.4.5.3.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.6.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.4.5.4.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.6.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.4.5.5.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	予引に関連記載あり（情報セキュリティ管理基準以外の由来）	9.6.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.5	運用ソフトウェアの管理 管理目的：運用システムの完全性を確実にするため。	8.19	運用システムへのソフトウェアの導入 管理策 運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施する。 目的 運用システムの完全性の維持を確実にし、技術的ぜい弱性の悪用を防止するため。		8.19	運用システムへのソフトウェアの導入 統制目標：運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施する。 目的：運用システムの完全性の維持を確実にし、技術的ぜい弱性の悪用を防止するため。	
12.5.1	運用システムに関わるソフトウェアの導入 運用システムに関わるソフトウェアの導入を管理するための手順を実施する。						

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
12.5.1.1	運用ソフトウェア、アプケーション及びプログラムライブラリの更新は、適切な管理策の認可に基づき、訓練された実務管理者だけが実施する。	8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 a) 運用ソフトウェアの更新は、適切な管理策の認可に基づき、訓練された実務管理者だけが実施する。	子引に関連記載あり	8.19.1	運用システムにおけるソフトウェアの導入及び変更をセキュリティを保って管理するための手順を策定し、対策を実施する。	特権の許可は最小限にするという原則を、運用システムへのソフトウェアの導入に適用する。 ソフトウェアのインストールの種類のうち、許可するもの（例えば、既存のソフトウェアの更新及びセキュリティパッチの適用）、及び禁止するもの（例えば、個人利用のために出力のソフトウェア、その由来が入手者の合理的な信用性が不明なソフトは疑わしいソフトウェア）を特定する。 特権は、利用者の役割に基づいて付与する。 組織は、利用者が導入できるソフトウェアの種類について、厳密な規則を定め、施行する。 運用システムにおけるソフトウェアの導入及び変更において、セキュリティを保つために、次の事項を考慮する。 a) 運用ソフトウェアの更新は、適切な管理策の認可に基づき、訓練された実務管理者だけが実施する（8.5参照）。 b) 運用システムには、承認された実行可能なコードだけを導入し、開発用コードやコンパイラは一切導入しないことを確実にする。 c) ソフトウェアは、十分なテストに成功した後に導入し、更新する（8.29及び8.31参照）。 d) 対応する全てのプログラムソースライブラリを更新する。 e) 全ての運用ソフトウェアの管理を維持するために、システム文書の管理と同様に、構成管理システムを利用する。 f) 変更を実装する前に、ロールバック計画を定める。 g) 運用ソフトウェアの更新の全てについて、監査ログを維持する。 h) ソフトウェアの旧版は、緊急時対応の手段として、及び保管しているデータをそのソフトウェアで読みみ込む又は処理する必要がある間は、全ての必要な情報及びパラメータ、手順、設定の詳細並びにサポートソフトウェアとともに保管しておく。 新リリースにアップグレードするとの決定には、その変更に対する事業上の要求及びそのリリースのセキュリティ（例えば、新しい情報セキュリティ機能の導入、この版が必要になった情報セキュリティ問題の量及び質）を考慮して行う。 情報セキュリティ上の弱点を除去するか、又は低減するために役立つ場合には、ソフトウェアパッチを適用する。 外部から供給されるソフトウェア及びパッケージ（例えば、外部サイトが提供しているモジュールを使用するソフトウェアプログラム）に依存するソフトウェアは、情報セキュリティのため弱性をもたらす可能性があるため、認可されていない変更を認識するために監視し、管理する。 運用システムで利用するソフトウェアの版を、ソフトウェア業者（供給者）がサポートする版に維持する。 組織は、サポートのないソフトウェアに依存することのリスクを考慮する。ソフトウェア業者は、使やこさい版のソフトウェアのサポートや止する。 運用システムで使用するオープンソースソフトウェアは、最新で適切なリリースの使用を維持する。時間の経過とともに、オープンソースコードが開発されなくなるかもしれないため、オープンソースウェアがポジリリで引き続き利用できる場合が多い。組織は、運用システムで使用する場合、保守がなされないオープンソースソフトウェアに依存するリスクも考慮する。 供給者がソフトウェアの導入又は更新に関与する場合、物理的又は論理的アクセスは、必要なときに、適切な認可を得た場合にだけ許可することが望ましい。供給者の活動を監視する（5.22参照）。
12.5.1.2	運用システムは、実行可能なコードだけを保持し、開発用コード又はコンパイラは保持しない。	8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 b) 運用システムには、承認された実行可能なコードだけを導入し、開発用コードやコンパイラは一切導入しないことを確実にする。	子引に関連記載あり			
12.5.1.3	アプケーション及びオペレーティングシステムソフトウェアは、十分な試験に成功した後に導入する。	8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 c) ソフトウェアは、十分なテストに成功した後に導入し、更新する。	子引に関連記載あり			
12.5.1.4	アプケーション及びオペレーティングシステムソフトウェアの試験は、使用性、セキュリティ、他システムへの影響及びユーザプレンドリ性の試験を含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策で総承おけて）	–	（対応項なし）	–
12.5.1.5	アプケーション及びオペレーティングシステムソフトウェアの試験は、運用システムとは別のシステムで実行する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策で総承おけて）	–	（対応項なし）	–
12.5.1.6	アプケーション及びオペレーティングシステムソフトウェアの試験は、対応するプログラムソースライブラリが更新済みであるこさを確実にする仕組みを整備する。	8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 d) 対応する全てのプログラムソースライブラリを更新する。	子引に関連記載あり	8.19.1	【再】運用システムにおけるソフトウェアの導入及び変更をセキュリティを保って管理するための手順を策定し、対策を実施する。	(8.19.1C対応する項を参照)
12.5.1.7	導入したソフトウェアの管理を維持するために、システムに関する文書化と同様に、構成管理システムを利用する。	8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 e) 全ての運用ソフトウェアの管理を維持するために、システム文書の管理と同様に、構成管理システムを利用する。	子引に関連記載あり			
12.5.1.8	変更を実施する前に、ロールバック計画を備える。	8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 f) 変更を実装する前に、ロールバック計画を定める。	子引に関連記載あり			
12.5.1.9	運用プログラムライブラリの更新の全てについて、監査ログを維持する。	8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 g) 運用ソフトウェアの更新の全てについて、監査ログを維持する。	子引に関連記載あり			
12.5.1.10	緊急時対応の手段として、一つ前の版のアプケーションソフトウェアを保持する。	8b-8.19.1	運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 h) ソフトウェアの旧版は、緊急時対応の手段として、及び保管しているデータをそのソフトウェアで読みみ込む又は処理する必要がある間は、全ての必要な情報及びパラメータ、手順、設定の詳細並びにサポートソフトウェアとともに保管しておく。	子引に関連記載あり			
12.5.1.11	ソフトウェアの旧版は、そのソフトウェアが扱ったデータが保存されている間は、必要とされる情報及びパラメータの全て、手順、設定の詳細並びにサポートソフトウェアとともに保管する。	8b-8.19.1	【再】運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。 h) ソフトウェアの旧版は、緊急時対応の手段として、及び保管しているデータをそのソフトウェアで読みみ込む又は処理する必要がある間は、全ての必要な情報及びパラメータ、手順、設定の詳細並びにサポートソフトウェアとともに保管しておく。	子引に関連記載あり			
12.5.1.12	運用システムに利用される業者供給ソフトウェアは、供給者によってサポートされ乱ベルを維持する。	8b-8.19.5	運用システムで利用するソフトウェアの版を、ソフトウェア業者（供給者）がサポートする版に維持する。	子引に関連記載あり			
12.5.1.13	組織は、サポートのないソフトウェアに依存することのリスクを考慮して管理する。	8b-8.19.6	組織は、サポートのないソフトウェアに依存することのリスクを考慮する。	子引に関連記載あり			
12.5.1.14	新リリースにアップグレードするとの決定には、その変更に対する事業上の要求及びそのリリースのセキュリティ（例えば、新しい情報セキュリティ機能の導入、この版が必要になった情報セキュリティ問題の量及び質）を考慮して行う。	8b-8.19.2	新リリースにアップグレードするとの決定には、その変更に対する事業上の要求及びそのリリースのセキュリティを考慮に入れる。	子引に関連記載あり			
12.5.1.15	情報セキュリティ上の弱点を除去するか、又は低減するために役立つ場合には、ソフトウェアパッチを適用する。	8b-8.19.3	情報セキュリティ上の弱性を除去するか、又は低減するために役立つ場合には、ソフトウェアパッチを適用する。	子引に関連記載あり			
12.5.1.16	供給者による物理的又は論理的アクセスは、サポート目的で必要なおに、管理策の承認を得た場合に限り、必ごだけ許可する。	8b-8.19.9	供給者がソフトウェアの導入又は更新に関与する場合、物理的又は論理的アクセスは、必要なときに、適切な認可を得た場合にだけ許可する。	子引に関連記載あり			
12.5.1.17	供給者による物理的又は論理的アクセスを許可している間は、供給者の活動を監視する。	8b-8.19.10	供給者の活動を監視する。	子引に関連記載あり			
12.5.1.18	セキュリティ上の弱点を含む可能性のある認可されていない変更を認識するために、外部から供給されるソフトウェア及びモジュールは、監視し、管理する。	8b-8.19.4	外部から供給されるソフトウェア及びパッケージに依存するソフトウェアは、情報セキュリティのため弱性をもたらす可能性があるため、認可されていない変更を認識するために監視し、管理する。	子引に関連記載あり			
12.6	技術的ぜい弱性管理 管理目的：技術的ぜい弱性の悪用を防止するため。	8.8	技術的ぜい弱性の管理 管理策 利用中の情報システムの技術的ぜい弱性に関する情報を獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価し、適切な手段をとる。 目的 技術的ぜい弱性の悪用を防止するため。		8.8	技術的ぜい弱性の管理 統制目標：利用中の情報システムの技術的ぜい弱性に関する情報を獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価し、適切な手段をとる。 目的：技術的ぜい弱性の悪用を防止するため。	
12.6.1	技術的ぜい弱性の管理 利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得する。また、そのような弱性に組織がさらされている状況を評価する。さらに、それら関連するリスクに対処するために、適切な手段をとる。						
12.6.1.1	技術的ぜい弱性（ソフトウェアの欠陥、誤った設定を含む。）の管理をサポートするために必要となる具体的な役割には、ソフトウェア業者、脆弱号、配置状況（例えば、どのソフトウェアがどのシステム上で導入されている か。）、及びそのソフトウェアに責任のある組織内の担当者を含める。	8b-8.8.1	組織は、効果的な技術的ぜい弱性管理の前提条件として、正確な資産の目録をもつ。	子引に関連記載あり	8.8.1	技術的ぜい弱性を特定し、評価する。	組織は、効果的な技術的ぜい弱性管理の前提条件として、正確な資産の目録（5.9～5.14参照）をもつ。資産の目録には、ソフトウェア業者、ソフトウェア名、版番号、配置状況（例えば、どのソフトウェアがどのシステム上に導入されているか。）、及びそのソフトウェアに責任のある組織内の担当者を含める。 技術的ぜい弱性を特定するために、組織は次の事項を考慮する。 a) 技術的ぜい弱性の管理に関連する役割及び責任を定める。確立する。技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性に関わるリスクアセスメント、更新、資産移動の追跡、及び要求される全ての調整責務が含まれる。 b) ソフトウェア及びその他の技術（組織の資産目録リスト）に基づく、5.9 参照）に関して、関連する技術的ぜい弱性を特定し、また、ぜい弱性を継続して認識するために用いる情報源を特定する。情報源のリストは、この目録を変更したとき、又は他の新しい若しくは有益な情報源を発見したときに更新する。 c) 情報システム（その構成要素を含む。）の利益者に、適当かつ合的に、要求事項を含め、ぜい弱性の報告、指数、及び関係を確実にすることを要求する（5.20参照）。 d) ぜい弱性を特定し、ぜい弱性のパッチ適用が成功したかどうかを検証するために、使用している技術に適したぜい弱性スキャンツールを使用する。 e) ぜい弱性の特定を支援するため、力量があり認可された者が、計画され、文書化された、再現可能な侵入テスト又はぜい弱性アセスメントを実施する。この活動はシステムのセキュリティを危うくする可能性があるため、注意を払う。 f) 第三者のライブラリ及びソースコードの使用について、ぜい弱性を追跡する。これはセキュアにに配備とコーディングに含める（8.28参照）。 特定した技術的ぜい弱性を評価するために、次の手引を考慮する。 a) どのような対応及び修復活動が必要かを決定するために、報告書を分析及び検証する。 b) 潜在的な技術的ぜい弱性を特定したとき は、それに伴うリスク及び関しるべき処置を特定する。 この処置は、ぜい弱性のあるシステムの要素又は他の脆弱性の適用を含む可能性がある。 組織は、次の事項のための手順及び能力を開発する。 a) 自らの製品及びサービス並びにこれらで使用している外部の構成要素について、ぜい弱性の存在を検知する。 b) 内部又は外部の供給元からぜい弱性報告を受け取る。 組織は、調査者及び他の人的問題を報告するように、ぜい弱性の開示に関するヒドック窓有の方針の一部として公開連絡先を示す。 組織は、ぜい弱性の報告手順、オンライン報告書式を確立し、適切な商概インテリジェンス又は情報共有の場を利用する。 組織は、ぜい弱性を適切に修復するために、組織における技術ぜい弱性の特定を支援する動機付けとして、脆弱を提供するバグ報奨金プログムの採用を検討する。 組織が力量のある業界団体又は他の利害関係者と情報を共有する。
–	（対応項なし）	8b-8.8.2	資産の目録には、ソフトウェア業者、ソフトウェア名、版番号、配置状況、及びそのソフトウェアに責任のある組織内の担当者を含める。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.4	組織は、次の事項のための手順及び能力を開発する。 a) 自らの製品及びサービス並びにこれらで使用している外部の構成要素について、ぜい弱性の存在を検知する。 b) 内部又は外部の供給元からぜい弱性報告を受け取る。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.5	組織は、調査者及び他の人的問題を報告するように、ぜい弱性の開示に関するヒドック窓有の方針の一部として公開連絡先を示す。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.6	組織は、ぜい弱性の報告手順、オンライン報告書式を確立し、適切な商概インテリジェンス又は情報共有の場を利用する。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.7	組織は、ぜい弱性を適切に修復するために、組織における ぜい弱性の特定を支援する動機付けとして、脆弱を提供するバグ報奨金プログムの採用を検討する。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.8	組織が力量のある業界団体又は他の利害関係者と情報を共有する。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.9	特定した技術的ぜい弱性を評価するために、次の手引を考慮する。 a) どのような対応及び修復活動が必要かを決定するために、報告書を分析及び検証する。 b) 潜在的な技術的ぜい弱性を特定したとき は、それに伴うリスク及び関しるべき処置を特定する。	子引に関連記載あり			
–	（対応項なし）	（8b-8.8.9参考）	この処置は、ぜい弱性のあるシステムの要素又は他の管理策の適用を含む可能性がある。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.10	認可された全てのソフトウェアに、最新の承認済みパッチ及びアプケーション更新を適用することを確実にするために、ソフトウェア更新管理プロセスを実装する。	子引に関連記載あり	8.8.2	情報システムに関連するぜい弱性への対策を実施する。	必要に応じて、独立した評価機関がソフトウェアの変更を試験し、妥当性を確認する。 認可された全てのソフトウェア、最新の承認済みパッチ及びアプケーション更新を適用することを確実にするために、ソフトウェア更新管理プロセスを実装する。 変更が必要な場合は、元のソフトウェアを保持し、指定された複製に変更を適用する。 全ての変更は、必要に応じて将来のソフトウェアアップグレードに再適用できるように、完全に試験し、文書化する。 技術的ぜい弱性に対処するために、次の手引を考慮する。 a) 潜在的な技術的ぜい弱性の特定に対応して、適切に、かつ、時機を失せずに処置を講じる。関係する可能性のある技術的ぜい弱性の通知に対応するためのタイムライン を定義する。 b) 技術的ぜい弱性への対処の緊急性に応じて、変更管理に関する管理策（8.32参照）又は情報セキュリティインシデント対応手順（5.26参照）に従って、処置を実行する。 c) 正当な理由（組織の内部又は外部の可能性がある）から変更ロけを使用する。 d) 更新を適用する前に、それが有効であること及び耐えられない副作用をもたらさないことを確実にするために、更新を試験し、評価する【すなわち、更新が利用可能な場合、更新の適用に伴うリスクを評価する（ぜい弱性が引き起こすリスク vs. 更新を適用することのリスクとを比較する。】。）。 e) リスクの高いシステムには最初に対処する。 f) 修復（一般にはソフトウェアの更新又はパッチ）を開発する。 g) 修復又は低減策が効果的であるかどうかを確認するために試験する。 h) 修復の真正性を検証する仕組みを提供する。 i) 利用可能な更新がない場合、又は更新を適用できない場合は、次のような他の管理策を検討する。 1) ソフトウェア業者又はその他の関連供給元に問題すること(追加策を適用する。 2) そのぜい弱性に関係するサービスは機能を停止する。 3) ネットワーク境界におけるアセス制御（例えば、ファイヤウォール）を調整又は追加する（8.20～8.22参照）。 4) ぜい弱なシステム、装置・機器又はアプケーションを、適切なトフィックウィル ウ（とに侵想パケと呼ばれる。）を挿入して攻撃から保護する。 5) 実際の攻撃を検知するために、監視を強化する。 6) そのぜい弱性に対する認識を高める。 脆弱点ソフトウェアについて、その業者がソフトウェアのセキュリティ更新に関する情報を定常的にリリース、更新を自動的に適用する機能を提供している場合、組織は、自動更新を使用するかどうかを決定する。 監査ログは、技術的ぜい弱性管理で行われる全てのステップについて保持する。 技術的ぜい弱性の管理プロセスは、その有効性及び改善性を確実にするために、定常的に監視し、評価する。 技術的ぜい弱性に対する有効な管理プロセスは、インシデント管理活動と整合させる。これは、ぜい弱性に関するデータをインシデント対応部署に伝達し、インシデントが発生した場合に実施する技術的手順を提供するためである。 組織が第三者のクラウドサービスプロバイダが提供するクラウドサービスを利用する場合、クラウドサービスプロバイダの資源の技術的ぜい弱性管理は、クラウドサービスプロバイダがその実施を確実に行うことを確認する。 クラウドサービスの利用に関する合意には、次を含める。 a) 技術的ぜい弱性管理に対するクラウドサービスプロバイダの責任 b) 技術的ぜい弱性に関するクラウドサービスプロバイダがその対応を指示するプロセス（5.23参照） 一部のクラウドサービスの場合には、クラウドサービスプロバイダはクラウドサービスカスタマにそれぞれの責任が存在する。例えば、クラウドサービスカスタマは、クラウドサービスにおいて使用する自身の資産のぜい弱性管理に責任がある。
–	（対応項なし）	8b-8.8.11	変更が必要な場合は、元のソフトウェアを保持し、指定された複製に変更を適用する。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.12	全ての変更は、必要に応じて将来のソフトウェアアップグレードに再適用できるように、完全に試験し、文書化する。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.13	必要に応じて、独立した評価機関がソフトウェアの変更を試験し、妥当性を確認する。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 f) 修復（一般にはソフトウェアの更新又はパッチ）を開発する。 g) 修復又は低減策が効果的であるかどうかを確認するために試験する。 h) 修復の真正性を検証する仕組みを提供する。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.15	脆弱点ソフトウェアについて、その業者がソフトウェアのセキュリティ更新に関する情報を定常的にリリース、更新を自動的に適用する機能を提供している場合、組織は、自動更新を使用するかどうかを決定する。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.19	組織が第三者のクラウドサービスプロバイダが提供するクラウドサービスを利用する場合、クラウドサービスプロバイダの資源の技術的ぜい弱性管理は、クラウドサービスプロバイダがその実施を確実に行うことを確認する。	子引に関連記載あり			
–	（対応項なし）	8b-8.8.20	クラウドサービスの利用に関する合意には、次を含める。 a) 技術的ぜい弱性管理に対するクラウドサービスプロバイダの責任 b) 技術的ぜい弱性に関するクラウドサービスプロバイダの対応を指示する	子引に関連記載あり			
–	（対応項なし）	（8b-8.8.20参考）	一部のクラウドサービスの場合には、クラウドサービスプロバイダはクラウドサービスカスタマにそれぞれの責任が存在する。例えば、クラウドサービスカスマは、クラウドサービスにおいて使用する自身の資産のぜい弱性管理に責任がある。	子引に関連記載あり			
12.6.1.2	報告していた技術的ぜい弱性を特定したとおは、適切かつ時機を失しない処置をとる。	8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 a) 潜在的な技術的ぜい弱性の特定に対応して、適切に、かつ、時機を失せずに処置を講じる。関係する可能性のある技術的ぜい弱性の通知に対応するためのタイムライン を定義する。	子引に関連記載あり			

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
12.6.1.3	技術的ぜい弱性の管理に関連する役割及び責任を定める。	8b-8.8.3	技術的ぜい弱性を特定するため、組織は次の事項を考慮する。 a) 技術的ぜい弱性の管理に関連する役割及び責任を定め、確立する。技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性に関わるリスクアセスメント、更新、資産移動の追跡、及び要求された全ての調整責務が含まれる。	手引に関連記載あり	8.8.1	【再】技術的ぜい弱性を特定し、評価する。	（8.8.1に対応する項を参照）
12.6.1.4	技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性に関わるリスクアセスメント、パッチの適用、資産移動の追跡、及び要求される全ての調整責務を含める。	8b-8.8.3	【再】技術的ぜい弱性を特定するために、組織は次の事項を考慮する。 a) 技術的ぜい弱性の管理に関連する役割及び責任を定め、確立する。技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性に関わるリスクアセスメント、更新、資産移動の追跡、及び要求された全ての調整責務が含まれる。	手引に関連記載あり			
12.6.1.5	技術的ぜい弱性を特定し、また、それらぜい弱性を継続して把握するために用いる情報資源（ぜい弱性検査ツールなど）を、リソフィルア及びその他の技術に関して（関連する技術的ぜい弱性を特定します。また、ぜい弱性を継続して把握するために用いる情報源を特定する。情報源のリストは、この項目を変更したとき、又は他の新しい若しくは有益な情報源を発見したときに更新する。	8b-8.8.3	技術的ぜい弱性を特定するために、組織は次の事項を考慮する。 b) リソフィルア及びその他の技術に関して、関連する技術的ぜい弱性を特定します。また、ぜい弱性を継続して把握するために用いる情報源を特定する。情報源のリストは、この項目を変更したとき、又は他の新しい若しくは有益な情報源を発見したときに更新する。	手引に関連記載あり			
12.6.1.6	技術的ぜい弱性の情報資源は、資産目録を変更したとき、又は他の新しい若しくは有益な資源を発見したときに更新を行う。	8b-8.8.3	【再】技術的ぜい弱性を特定するために、組織は次の事項を考慮する。 b) リソフィルア及びその他の技術に関して、関連する技術的ぜい弱性を特定します。また、ぜい弱性を継続して把握するために用いる情報源を特定する。情報源のリストは、この項目を変更したとき、又は他の新しい若しくは有益な情報源を発見したときに更新する。	手引に関連記載あり			
12.6.1.7	潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める。	8b-8.8.14	【再】技術的ぜい弱性に対処するために、次の手引を考慮する。 a) 潜在的な技術的ぜい弱性の特定に対応して、適切に、かつ、時機を失せずに処置を講じる。関係する可能性のある技術的ぜい弱性の通知に対応するためのタイムラインを定義する。	手引に関連記載あり	8.8.2	【再】情報システムに関連するぜい弱性への対策を実施する。	（8.8.2に対応する項を参照）
12.6.1.8	潜在的な技術的ぜい弱性が特定されたとき、組織は、それと関連するリスクおよびとるべき処置（例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用）を特定する。	8b-8.8.9	特定した技術的ぜい弱性を評価するために、次の手引を考慮する。 b) 潜在的な技術的ぜい弱性を特定したときは、それに伴うリスクおよびとるべき処置を特定する。	手引に関連記載あり	8.8.1	【再】技術的ぜい弱性を特定し、評価する。	（8.8.1に対応する項を参照）
12.6.1.9	技術的ぜい弱性の低い の緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に 従って、とるべき処置を実行する。	8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 b) 技術的ぜい弱性への対処の緊急性に応じて、変更管理に関する管理策又は情報セキュリティインシデント対応手順に従って、処置を実行する。	手引に関連記載あり	8.8.2	【再】情報システムに関連するぜい弱性への対策を実施する。	（8.8.2に対応する項を参照）
12.6.1.10	正当な供給元からパッチを入手できる場合は、そのパッチを適用することに関連したリスクを評価する（ぜい弱性が引き起こすリスク、パッチの適用によるリスクとを比較する。）。	8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 c) 正当な供給元（組織の内部又は外部の可能性がある）からの更新だけを使用する。	手引に関連記載あり			
12.6.1.11	パッチの適用前に、それらが有効であること及びそれらが他とうまくいない副作用をもたらさないことを確実にするために、テスト を試験及び評価するとともに、利用可能なパッチがない場合は、以下の4点を実施する。 1.そのぜい弱性に関係するサービスまたは機能を停止する。 2.ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する。 3.実際の攻撃を検知するために、監視を強化する。 4.ぜい弱性に対する認識を高める。	8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 d) 更新を適用する前に、それが有効であること及び他とうまくいかない副作用をもたらさないことを確実にするために、更新を試験し、評価する。	手引に関連記載あり			
12.6.1.12	修正パッチの適用、その他実施した全ての手順について監査ログを保持する。	8b-8.8.16	監査ログは、技術的ぜい弱性管理で行われる全てのステップについて保持する。	手引に関連記載あり			
12.6.1.13	技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する。	8b-8.8.17	技術的ぜい弱性の管理プロセスは、その有効性及び効率性を確実にするために、定常的に監視し、評価する。	手引に関連記載あり			
12.6.1.14	技術的ぜい弱性は、リスクの高いシステムには最初に対処する。	8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 e) リスクの高いシステムには最初に対処する。	手引に関連記載あり			
12.6.1.15	技術的ぜい弱性に対する有効な管理プロセスは、ぜい弱性に関するデータをインシデント対応部署に伝達し、インシデントが発生した場合に実施する技術的手順を準備するために、インシデント管理活動と整合させ、組織全体にわたってぜい弱性に対処する。	8b-8.8.18	技術的ぜい弱性に対する有効な管理プロセスは、インシデント管理活動と整合させる。	手引に関連記載あり			
12.6.1.16	ぜい弱性が特定されていながら適切な対応策がない場合には、その状況に対処するための手順を定める。	8b-8.8.14	技術的ぜい弱性に対処するために、次の手引を考慮する。 f) 利用可能な更新がない場合、又は更新を適用できない場合は、次のような他の管理策を検討する。 1) ソフトウェア業者又はその他の関連供給元が提案する回避策を適用する。 2) その ぜい弱性に関係するサービスは機能を停止する。 3) ネットワーク境界におけるアクセス制御を調整又は追加する。 4) ぜい弱なシステム、装置・機器又はアプリケーションを、適切なトラフィックフィルタ（とおに仮想パッチ呼ばれる。）を導入して攻撃から保護する。 5) 実際の攻撃を検知するために、監視を強化する。 6) その ぜい弱性に対する認識を高める。	手引に関連記載あり			
12.6.1.17	ぜい弱性が特定されていながら適切な対応策がない場合には、組織は、既知のぜい弱性に関する リスクを評価し、適切な検知及び是正処置を定める。	–	（最接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で最未点打）	–	（対応項なし）	–
12.6.1.18.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	8.8.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
12.6.2	ソフトウェアのインストールの制限 利用者による ソフトウェアのインストールを管理する規則を確立し、実施する。	8.19	運用システムへのソフトウェアの導入 管理策 運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施する。 目的 運用システムの完全性の維持を確実にし、技術的ぜい弱性の悪用を防止するため。		8.19	運用システムへのソフトウェアの導入 統制目標：運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施する。 目的：運用システムの完全性の維持を確実にし、技術的ぜい弱性の悪用を防止するため。	
12.6.2.1	組織は、利用者がインストールしてもよいソフトウェアの種類について、厳密な方針を定め、施行する。	8b-8.19.11	組織は、利用者が導入できるソフトウェアの種類について、厳密な規則を定め、施行する。	手引に関連記載あり	8.19.1	【再】運用システムにおけるソフトウェアの導入及び変更をセキュリティを保って管理するための手順を策定し、対策を実施する。	（8.19.1に対応する項を参照）
12.6.2.2	特権の許可は最小限にするという原則を適用する。	8b-8.19.12	特権の許可は最小限にするという原則を、運用システムへのソフトウェアの導入に適用する。	手引に関連記載あり			
12.6.2.3	組織は、ソフトウェアのインストールの種類のうち、許可するもの（例えば、既存のソフトウェアの更新及びセキュリティパッチの適用）、及び禁止するもの（例えば、個人利用のためのソフトウェア、潜在的な悪意の有無が不明又はその疑いがあるソフトウェア）を特定する。	8b-8.19.13	組織は、ソフトウェアのインストールの種類のうち、許可するもの、及び禁止するものを特定する。	手引に関連記載あり			
12.6.2.4	特権は、関連する利用者の役割を考慮に入 れて付与する。	8b-8.19.12	【再】特権の許可は最小限にするという原則を、運用システムへのソフトウェアの導入に適用する。	手引に関連記載あり			
–	（対応項なし）	8b-8.19.14	特権は、利用者の役割に基づいて付与する。	手引に関連記載あり			
12.7	情報システムの監査に対する考慮事項 管理目的：運用システムに対する監査活動の影響を最小限にするため。	8.34	監査におけるテスト中の情報システムの保護 管理策 運用システムのアセスメントを伴う監査におけるテスト及びその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意する。 目的：監査及びその他の保証活動が運用システム及び業務プロセスに与える影響を最小限に抑えるため。		8.34	監査におけるテスト中の情報システムの保護 統制目標：運用システムのアセスメントを伴う監査におけるテスト及びその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意する。 目的：監査及びその他の保証活動が運用システム及び業務プロセスに与える影響を最小限に抑えるため。	
12.7.1	情報システムの監査に対する管理策 運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意する。						
12.7.1.1	システム及びデータへのアクセスに関する監査要求事項は、適切な管理層の同意を得る。	8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 a) システム及びデータへのアクセスに関する監査要求は、適切な管理層の同意を得る。	手引に関連記載あり	8.34.1	監査におけるテスト及びその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意する。	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 a) システム及びデータへのアクセスに関する監査要求は、適切な管理層の同意を得る。 b) 技術監査におけるテストの範囲を、合意し、管理する。 c) 監査におけるテストは、ソフトウェア及びデータの読出し専用のアクセスに限定する。必要な情報を取得するために参照専用のアクセスを利用できない場合、監査 人に代わって必要なアクセス権をもつ経験豊かな実務管理者がテストを実行する。 d) アクセスを許可する場合、許可する前にシステムへのアクセスに使用する装置・機器（例えば、ラップトップ又はプレット）のセキュリティ要求事項（例えば、ウイルス対策及びパッチ適用）を確立し、検証する。 e) 読出し専用以外のアクセスは、システムファイルの隔離された複製に対して行う。それらの複製は、監査が完了した時点で削除するか、又は監査の文書化の要求によってそのようなファイルを保存する義務があるときは、適切に保護する。 f) 監査ツールの実行など、特別又は追加の処理に関する要求を特定し、合意する。 g) 監査におけるテストがシステムの可用性に影響する可能性がある場合、こうしたテストは営業時間外に実施する。 h) 監査及びテストを含めた全てのアクセスを監視し、ログをとる。
12.7.1.2	技術監査における試験の範囲を、合意し、管理する。	8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 b) 技術監査におけるテストの範囲を、合意し、管理する。	手引に関連記載あり			
12.7.1.3	監査における試験は、ソフトウェア及びデータの読出し専用のアクセスに限定する。	8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 c) 監査におけるテストは、ソフトウェア及びデータの読出し専用のアクセスに限定する。必要な情報を取得するために参照専用のアクセスを利用できない場合、監査 人に代わって必要なアクセス権をもつ経験豊かな実務管理者がテストを実行する。	手引に関連記載あり			
12.7.1.4	監査における試験では、読出し専用以外のアクセスは、システムファイルの隔離された複製に対して行う。それらの複製は、監査が完了した時点で消去するか、又は監査の文書化の要求の下でそのようなファイルを保存する義務があるときは、適切に保護する。	8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 a) 読出し専用以外のアクセスは、システムファイルの隔離された複製に対して行う。それらの複製は、監査が完了した時点で削除するか、又は監査の文書化の要求によってそのようなファイルを保存する義務があるときは、適切に保護する。	手引に関連記載あり			
12.7.1.5	監査における試験を実施するための、特別又は追加の処理（異常が発見された場合の措置を含む。）に関する要求事項を特定し、合意する。	8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 f) 監査ツールの実行など、特別又は追加の処理に関する要求を特定し、合意する。	手引に関連記載あり			
12.7.1.6	監査における試験がシステムの可用性に影響する可能性がある場合、こうした試験は営業時間外に実施する。	8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 g) 監査におけるテストがシステムの可用性に影響する可能性がある場合、こうしたテストは営業時間外に実施する。	手引に関連記載あり			
12.7.1.7	監査における試験を実施する際には、参照用の経路を残すために、全てのアクセスを監視し、ログをとる。	8d-8.34.1	監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。 h) 監査及びテストを含めた全てのアクセスを監視し、ログをとる。	手引に関連記載あり			
12.7.1.8	監査における試験が失敗した際には、情報システムが警告を表示する。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
12.7.1.9	監査における試験が失敗した際には、内部の要員又は組織へ伝達する。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
13	通信のセキュリティ	8.20	ネットワークセキュリティ 管理策 システム及びアプリケーション内の情報を保護するために、ネットワーク及びネットワーク装置のセキュリティを保ち、管理し、制御する。 目的 ネットワーク及びそれを支援する情報処理設備において、情報をネットワークを通じた侵害から保護するため。		8.20	ネットワークセキュリティ 統制目標：システム及びアプリケーション内の情報を保護するために、ネットワーク及びネットワーク装置のセキュリティを保ち、管理し、制御する。 目的：ネットワーク及びそれを支援する情報処理設備において、情報をネットワークを通じた侵害から保護するため。	
13.1	ネットワークセキュリティ管理 管理目的：ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。						
13.1.1	ネットワーク管理策 システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御する。						
13.1.1.1	ネットワークにおける情報のセキュリティ、及び接続したネットワークサービスの認可されていないアクセスから の保護を確実にするために、管理策を実施する。	8c-8.20.1	ネットワークにおける情報のセキュリティを確実に、接続したネットワークサービスを認可されていないアクセスから保護するために、管理策を実施する。	手引に関連記載あり	8.20.1	ネットワーク及びネットワーク装置のセキュリティを保つための対策を実施する。	ネットワークにおける情報のセキュリティを確実に、接続したネットワークサービスを認可されていないアクセスから保護するために、管理策を実施する。 ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 a) ネットワークごと に、扱てよい情報の種類及び分類レベル b) ネットワーク装置及び機器の管理に関する責任及び手順を確立する。 c) ネットワーク接続及び装置・機器（例えば、ルーター、スイッチ）の構成ファイルを含む最新の文書を維持する。 d) 適切な場合には、ネットワークの運用責任は、ICTシステムの運用から分離する（5.3参照）。 e) 公衆ネットワーク、第三者ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及びアプリケーションを保護するために、管理策を実施する（5.22、8.24、5.14及び6.6参照）。ネットワークサービスの可用性及びネットワークに接続した コピュータの可用性を維持するために、追加の管理策が要求される場合がある）。 f) 情報セキュリティに影響を及ぼすり能性のある行動、又は情報セキュリティに関係のある行動の記録及び検知ができるように、適切なログを取得し、監視する（8.16及び8.15参照）。 g) 組織に対するサービスを最適にするため、また、管理策を情報処理施設全体に一貫して適用することを確実にするために、様々なネットワーク管理作業を緊密に調整する。 h) ネットワークとのシステム接続を制限し、フィルタリングする（例えば、ファイアウォールを使用する。）。 i) ネットワークへの装置及び機器の接続を検出し、制限し、認証する。 k) ネットワーク装置・機器の変更化（hardening） l) ネットワーク管理の経路を他のネットワークトラフック から分離する。 m) ネットワーク攻撃を受けた場合、重要なデプネットワークを一時的に分離する（例えば、FローブックシDS（誤な検）を用いて分離する。）。 n) ぜい弱なネットワークプロトコルを無効化する。 組織は、仮想化ネットワークの使用に、適切なセキュリティ管理策を適用することを確実にする。仮想化ネットワークには、ソフトウェア定義ネットワーク（SDN、SD-WAN）も含む。仮想化ネットワークは、物理的ネットワークとその通信の論理的分離を可能にすることから、セキュリティの観点で望ましい場合があり、特に分散型コンピューティングを用いて実装したシステム及びアプリケーションにおいてこのことが該当する。
13.1.1.2	ネットワーク設備の管理に関する責任及び手順を確立する。	8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 b) ネットワーク装置及び機器の管理に関する責任及び手順を確立する。	手引に関連記載あり			
13.1.1.3	ネットワークの運用責任は、コンピュータの運用から、分離する。	8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 d) 適切な場合には、ネットワークの運用責任は、ICTシステムの運用から分離する。	手引に関連記載あり			
13.1.1.4	公衆ネットワークまたは無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及びアプリケーションを保護するために、特別な管理策を確立する。	8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 e) 公衆ネットワーク、第三者ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及びアプリケーションを保護するために、管理策を確立する。	手引に関連記載あり			
13.1.1.5	ネットワークサービスの可用性及びネットワークを介して接続したコンピュータの可用性を維持するために、特別な管理策を確立する。	8c-8.20.2	【再】ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 e) 公衆ネットワーク、第三者ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及びアプリケーションを保護するために、管理策を確立する。	手引に関連記載あり			
13.1.1.6	情報セキュリティに影響を及ぼすり可能性のあるり動、又は情報セキュリティに関係した行動を記録及び検知できるように、適切なログ取得及び監視を実施する。	8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 f) 情報セキュリティに影響を及ぼすり可能性のあるり動、又は情報セキュリティに関係のある行動の記録及び検知ができるように、適切なログを取得し、監視する。	手引に関連記載あり			
13.1.1.7	組織に対するサービスを最適にするため、また、管理策を情報処理施設全体に一貫して適用することを確実にするために、様々な管理作業を緊密に調整する。	8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 g) 組織に対するサービスを最適にするため、また、管理策を情報処理施設全体に一貫して適用することを確実にするために、様々なネットワーク管理作業を緊密に調整する。	手引に関連記載あり			
13.1.1.8	ネットワーク上のシステム（デバイスを含む）は接続前に認証する。	8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 h) ネットワーク上のシステムを認証する。	手引に関連記載あり			
13.1.1.9	ネットワークへのシステムの接続を制限する。	8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 i) ネットワークへのシステムの接続を制限し、フィルタリングする。	手引に関連記載あり			
–	（対応項なし）	8c-8.20.2	ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 a) ネットワークごと に、扱てよい情報の種類及び分類レベル c) ネットワーク接続及び装置・機器の構成ファイルを含む最新の文書を維持する。	手引に関連記載あり			
–	（対応項なし）	8c-8.20.3	組織は、仮想化ネットワークの使用に、適切なセキュリティ管理策を適用することを確実にする。	手引に関連記載あり			
–	（対応項なし）	（8c-8.20.3参考1）	仮想化ネットワークには、ソフトウェア定義ネットワーク（SDN、SD-WAN）も含む。	手引に関連記載あり			
–	（対応項なし）	（8c-8.20.3参考2）	仮想化ネットワークは、物理的ネットワーク上での通信の論理的分離を可能にすることから、セキュリティの観点で望ましい場合があり、特に分散型コンピューティングを用いて実装したシステム及びアプリケーションにおいてこのことが該当する。	手引に関連記載あり			
13.1.1.10	情報システムの周辺装置から情報システムへの内部ネットワーク接続を認可するため、要求事項、転送される情報の性質及び手順を定め、文書化する。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
13.1.1.11.P	クラウドサービス事業者は、当該事業者が提供するサービスにおけるIPv6への対応状況について、クラウドサービス利用者に情報を提供する。	–	（統一基準由来）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	8.20.2	クラウドサービス事業者が提供するサービスにおけるIPv6への対応状況について、クラウドサービス利用者に情報を提供する。	特になし。
13.1.2	ネットワークサービスのセキュリティ 組織が自ら提供する か外部委託して いるかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定し、また、ネットワークサービスの合意書にこれらを盛り込む。	8.21	ネットワークサービスのセキュリティ 管理策 ネットワークサービスのセキュリティ機能、サービスレベル及びサービスの要求事項を特定し、実装し、監視する。 目的 ネットワークサービスの利用におけるセキュリティを確実にするため。		8.21	ネットワークサービスのセキュリティ 統制目標：ネットワークサービスのセキュリティ機能、サービスレベル及びサービスの要求事項を特定し、実装し、監視する。 目的：ネットワークサービスの利用におけるセキュリティを確実にするため。	
13.1.2.1	ネットワークサービスの提供者と合意したサービスをセキュリティを保って管理するために必要なネットワークサービス提供者の能力を定め、常に監視し、監査の権利について ネットワークサービス提供者と合意する。	8c-8.21.3	合意したサービスをセキュリティを保って管理できる、ネットワークサービス提供者の能力を定め、定常的に監視する。	手引に関連記載あり	8.21.3	ネットワークサービス提供者の能力を定常的に監視する。	合意したサービスをセキュリティを保って管理できる、ネットワークサービス提供者の能力を定め、定常的に監視する。

番号	（旧）管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	（新）管理策基準	（参考）索引語
13.1.2.2	それぞれのサービスに必要なセキュリティについて（例えば、セキュリティ特性、サービスレベル、管理上の要求事項）を特定し、組織は、ネットワークサービス提供者によるこれらの対策の実施を確実にする仕組みを整備する。	8c-B.21.1	それぞれのネットワークサービスに必要なセキュリティ対策を、内部又は外部のネットワークサービス提供者が特定し、実装する。	子刊に関連記載あり	8.21.2	ネットワークサービスに必要なセキュリティ対策を実装する。	ネットワークサービスは、接続、プライベートネットワークサービス及びネットワークセキュリティ管理ソリューション（例えば、ファイアウォール、侵入検知システム）が含まれる。これらのサービスは、単純で管理を伴わない簡単の提供から複雑な分別処理機能の提供まで、広い範囲に及ぶこと がある。 それぞれのサービスに必要なセキュリティ対策（例えば、セキュリティ機能、サービスレベル及びサービスの要求事項）を、内部又は外部のネットワークサービス提供者が特定し、実装する。 組織は、ネットワークサービス提供者による、ネットワークサービスに必要なセキュリティ対策の実施を確実にする。
–	（対応項なし）	8c-B.21.2	組織は、ネットワークサービス提供者による、ネットワークサービスに必要なセキュリティの対策の実施を確実にする。	子刊に関連記載あり			
–	（対応項なし）	8c-B.21.6	ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。 a）アクセスが許可されているネットワーク及びネットワークサービス b）様々なネットワークサービスにアクセスするための認証の要求事項 c）誰にどのネットワーク及びネットワークサービスにアクセスすることを許すかを決定する認可手順 d）ネットワーク接続及びネットワークサービスへのアクセスを保護するためのネットワーク管理策に採用が管理策及び手順 e）ネットワーク及びネットワークサービスにアクセスするために利用する手段 f）アクセス時の利用者の時刻、場所及び他の属性 g）ネットワークサービスの利用の監視	子刊に関連記載あり	8.21.1	【再】ネットワークサービスの利用に関する規則を整備する。	（8.21.1に対応する項を参照）
–	（対応項なし）	8c-B.21.4	監査の権利について組織と提供者との間で合意する。	子刊に関連記載あり	8.21.4	監査の権利について組織とネットワークサービス提供者との間で合意する。又はネットワークサービス提供者が適切なセキュリティ対策を維持していることを実証するために、ネットワークサービス提供者が提示する第三者証拠を利用する。	監査の権利について組織と提供者との間で合意する。 組織は、サービス提供者が適切なセキュリティ対策を維持していることを実証するために、サービス提供者が提示する第三者証拠を考慮する。 ネットワークサービスの次のセキュリティ機能を考慮する。 a）ネットワークサービスのセキュリティに適用する技術（例えば、認証、暗号化、ネットワーク接続管理） b）セキュリティ規則及びネットワーク接続規則に従った、ネットワークサービスへのセキュリティを確保した接続のために要求される技術的パラメータ c）利用者が性能、可用性及び機密性の要求事項に従ってキャッシングの利用を選択できる、キャッシング（例えば、コンテンツ配信ネットワークにおけるキャッシング）及びそのパラメータ d）必要な場合、ネットワークサービスはアプリケーションへのアクセスを制限するための、ネットワークサービス利用の手順
–	（対応項なし）	8c-B.21.5	組織は、サービス提供者が適切なセキュリティ対策を維持していることを実証するために、サービス提供者が提示する第三者証拠を考慮する。	子刊に関連記載あり			
–	（対応項なし）	8c-B.21.7	ネットワークサービスは次のセキュリティ機能を考慮する。 a）ネットワークサービスのセキュリティに適用する技術 b）セキュリティ規則及びネットワーク接続規則に従った、ネットワークサービスへのセキュリティを確保した接続のために要求される技術的パラメータ c）利用者が性能、可用性及び機密性の要求事項に従ってキャッシングの利用を選択できる、キャッシング及びそのパラメータ d）必要な場合、ネットワークサービスはアプリケーションへのアクセスを制限するための、ネットワークサービス利用の手順	子刊に関連記載あり			
13.1.3	ネットワークの分離 情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離する。	8.22	ネットワークの分離 管理策 情報サービス、利用者及び情報システムは、組織のネットワーク上で、グループごとに分離する。 目的 業務のニーズに基づいて、ネットワークセキュリティ境界で分割し、それらの間のトラフィックを管理するため。		8.22	ネットワークの分離 統制目標：情報サービス、利用者及び情報システムは、組織のネットワーク上で、グループごとに分離する。 目的：業務のニーズに基づいて、ネットワークセキュリティ境界で分割し、それらの間のトラフィックを管理するため。	
13.1.3.1	大規模なネットワークのセキュリティを管理するために、必要に応じてネットワークを異つかのネットワーク領域に分離（例えば、必要な単位でセグメントを分割）する。	8c-B.22.1	組織は、大規模なネットワークを異つかのネットワーク領域に分離し、公衆ネットワーク（すなわち、インターネット）から分離することによって、大規模なネットワークのセキュリティを管理する。	子刊に関連記載あり	8.22.1	ネットワーク領域の境界を定め、ネットワークを分離する。	組織は、大規模なネットワークを異つかのネットワーク領域に分離し、公衆ネットワーク（すなわち、インターネット）から分離することによって、大規模なネットワークのセキュリティを管理する。 ネットワーク領域は、可能であれば組織の単位（例えば、人事、財務、マーケティング）又は特定の組合せ（例えば、複数の組織の単位に接続しているサーバ領域）に従い、情報性のレベル（例えば、公開されている領域、デスクトップ領域、サーバ領域）に基づいて選択する。 ネットワークの分離は、可能であれば物理的に異なるネットワーク又は論理的に異なるネットワークを用いて行う。 それぞれのネットワーク領域の境界は、明確に定める。 ネットワーク領域間のアクセス制御の場合、アクセスは境界にゲートウェイ（例えば、ファイアウォール、フィルタリングルーター）を設けて制御する。 ネットワーク領域を分離する際の基準及びゲートウェイを通して認められるアクセスの基準は、それぞれの領域のセキュリティ要求事項のアセスメントに基づく。 それぞれのネットワーク領域のセキュリティ要求事項のアセスメントでは、次の事項を評価する。 a）アクセス制御に関するトピック固有の方針（5.15 参照）、アクセス要求事項、並びに処理する情報の価値及び分類に従っている。 b）適切なゲートウェイ技術を組み込むための費用対効果を考慮している。
13.1.3.2	ネットワーク領域は、組織の単位（例えば、人的資源、財務、マーケティング）又は特定の組合せ（例えば、複数の組織の単位に接続しているサーバ領域）に従い、情報性のレベル（例えば、公開されている領域、デスクトップ領域、サーバ領域）に基づいて選択する。	8c-B.22.2	ネットワーク領域は、可能であれば組織の単位又は特定の組合せに従い、情報性、重要性及び取扱いに価値を要する度合に基づいて選択する。	子刊に関連記載あり	8.22.2	ネットワーク領域の境界を定め、ネットワークを分離する。	
13.1.3.3	ネットワーク領域の分離は、物理的に異なるネットワークは論理的に異なるネットワーク（例えば、仮想私設網）を用いることによって行う。	8c-B.22.3	ネットワークの分離は、可能であれば物理的に異なるネットワークは論理的に異なるネットワークを用いて行う。	子刊に関連記載あり			
13.1.3.4	各ネットワーク領域の境界は、明確に定める。	8c-B.22.4	それぞれのネットワーク領域の境界は、明確に定める。	子刊に関連記載あり			
13.1.3.5	ネットワーク領域間のアクセスは、境界にゲートウェイ（例えば、ファイアウォール、WAF、プロキシ、リバースプロキシ、又はセファイアウォール又はフィルタリングルータ）を設けて制御する。	8c-B.22.5	ネットワーク領域間のアクセスを認める場合、アクセスは境界にゲートウェイを設けて制御する。	子刊に関連記載あり			
13.1.3.6	各ネットワーク領域のセキュリティ要求事項のアセスメントに基づき、ネットワーク領域に分離する際の基準及びゲートウェイを通して認められるアクセスの基準を定める。	8c-B.22.6	ネットワーク領域を分離する際の基準及びゲートウェイを通して認められるアクセスの基準は、それぞれの領域のセキュリティ要求事項のアセスメントに基づく。	子刊に関連記載あり			
13.1.3.7	各ネットワーク領域のセキュリティ要求事項のアセスメントは、アクセス制御方針、アクセス要求事項、並びに処理する情報の価値及び分類に従い、また、費用対効果を考慮して適切なゲートウェイ技術を組み込む。	8c-B.22.7	それぞれのネットワーク領域のセキュリティ要求事項のアセスメントでは、次の事項を評価する。 a）アクセス制御に関するトピック固有の方針、アクセス要求事項、並びに処理する情報の価値及び分類に従っている。 b）適切なゲートウェイ技術を組み込むための費用対効果を考慮している。	子刊に関連記載あり			
13.1.3.8	ネットワークの境界が十分に定められていない無線ネットワークは、ネットワーク領域の分離のための特別な取扱いを定める。	8c-B.22.8	無線ネットワークの分離のために、電波の届く範囲の調整を考慮する。	子刊に関連記載あり	8.22.2	無線ネットワークの分離の要件を定め、実装する。	無線ネットワークの分離のために、電波の届く範囲の調整を考慮する。無線ネットワークは、ネットワークの境界が十分に定められていないため、特別な取扱いを要する。 取扱いに価値を要する環境では、全ての無線アクセスは、外部接続として取り扱い、そのアクセスがネットワーク管理策（8.20参照）に従ってゲートウェイを通過して内部システムへのアクセスが許可されるまでは、内部ネットワークから分離するように配置する。 要員が組織のトピック固有の方針に適合する管理されたエンドポイント機器以外を使用する場合、ゲスト用の無線アクセスネットワークを要員用の無線アクセスネットワークから分離する。 ゲスト用のWiFi は、要員によるゲストWiFi の利用を防ぐために、少なくとも要員用のWiFiと同し制限をもつ。
–	（対応項なし）	（8c-B.22.8参考）	無線ネットワークは、ネットワークの境界が十分に定められていないため、特別な取扱いを要する。	子刊に関連記載あり			
13.1.3.9	無線いに価値を要する環境では、全ての無線アクセスは、外部接続として取り扱い、そのアクセスがネットワーク管理策の方針に従ってゲートウェイを通過して内部システムへのアクセスが許可されるまでは、内部ネットワークから分離する。	8c-B.22.9	無線いに価値を要する環境では、全ての無線アクセスは、外部接続として取り扱い、そのアクセスがネットワーク管理策に従ってゲートウェイを通過して内部システムへのアクセスが許可されるまでは、内部ネットワークから分離するよう配置する。	子刊に関連記載あり			
–	（対応項なし）	8c-B.22.10	要員が組織のトピック固有の方針に適合する管理された利用者エンドポイント機器以外を使用する場合、ゲスト用の無線アクセスネットワークを要員用の無線アクセスネットワークから分離する。	子刊に関連記載あり			
–	（対応項なし）	8c-B.22.11	ゲスト用のWiFiは、要員によるゲストWiFiの利用を防ぐために、少なくとも要員用のWiFiと同し制限をもつ。	子刊に関連記載あり			
–	（対応項なし）	–	（統一基準由来）	令和7年度にて追加（情報セキュリティ管理基準以外の由来）	8.22.3	組織内ネットワークを複数セグメントに区切った上で、重要なシステムやサービスを専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。インターネットに接続する必要がある場合は、必要最小限のプロトコルやポートのみに限定する。	特になし。
13.1.3.10.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	8.22.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
13.1.3.11.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	8.22.5	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
13.1.3.12.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	8.22.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
13.1.4.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		9.7	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
13.1.4.1.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.7.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
13.1.4.2.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	9.7.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
13.2	情報の転送 管理目的：組織の内部及び外部に転送した情報のセキュリティを維持するため。	5.14	情報の転送 管理策 情報の転送の規則、手順又は合意を、組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備える。 目的 組織内及び外部の利害関係者との間で転送される情報のセキュリティを維持するため。		5.14	情報の転送 統制目標：情報の転送の規則、手順又は合意を、組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備える。 目的：組織内及び外部の利害関係者との間で転送される情報のセキュリティを維持するため。	
13.2.1	情報の転送 あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備える。						
13.2.1.1	情報転送のために通信設備を利用するときに従う手順及び管理策には、転送する情報を、盗聴、複製、改ざん、誤った経路での通信及び破壊から保護するために設計された手順を反映する。	5b-S.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 a）転送する情報を、盗聴、認可されていないアクセス、複製、改ざん、誤った経路での通信、破壊及びサービス拒否から保護するために設計された管理策。これは、情報の分類に合った それぞれのレベルのアクセス制御、及び暗号技術の利用など取扱いに価値を要する情報を保護するために必要な管理策を含む。	子刊に関連記載あり	5.14.2	全ての種類の情報の転送について、規則又は手順を整備する。	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 a）転送する情報を、盗聴、認可されていないアクセス、複製、改ざん、誤った経路での通信、破壊及びサービス拒否から保護するために設計された管理策。これは、情報の分類に合った それぞれのレベルのアクセス制御、及び暗号技術（8.24参照）などの取扱いに価値を要する情報を保護するために必要な管理策を含む。 b）転送中の情報の完全性及び否認防止を維持することを含む、追跡可能性及び否認防止を確実にするための管理策 c）該当する場合には、情報の管理責任者、リスク所有者、セキュリティ担当者及び情報管理者など、転送に関連する適切な連絡先の特定 d）物理的な記憶媒体の紛失又はデータの消失などの情報セキュリティインシデントが発生した場合の責任及び期間義務 e）取扱いに価値を要する又は重要な情報に対する、合意したラベル付けシステム（ラベルの意味を直ちに理解できること、及び情報を適切に保護することを確実にするための）の使用（5.13参照） f）転送サービスの信頼性及び可用性 g）情報転送手段の許容される利用に関するビジ固有の方針又は指針（5.10参照） h）メッセージを含む全ての業務記録の保持及び破棄の指針 注記 業務記録の保持及び破棄に関しては、地域の法令及び規制が存在する場合がある。 i）情報の転送に関連するその他の関連する法令、規則及び契約上の要求事項（5.31、5.32、5.33、5.34参照）の考慮（例えば、電子署名の要求事項） 合意については5.20.1供給者との合意にて、「物理的輸送又は論理的送信中に情報を保護するための情報の転送の管理策」が存在することから、本管理策においては「規則、手順」を対象とする。
13.2.1.2	情報転送のために通信設備を利用するときに従う手順及び管理策には、電子的メッセージ通信を通じて伝送される可能性のあるマルウェアを検出し、これから保護するための手順を反映する。	5b-S.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 a）電子通信の利用を通じて伝送される可能性のあるマルウェアの検知及び伝送に対する保護	子刊に関連記載あり	5.14.3	電子通信手段の使用について、規則又は手順を整備する。	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 a）電子通信の利用を通じて伝送される可能性のあるマルウェアの検知及び伝送に対する保護（8.7参照） b）添付して通信する、取扱いに価値を要する電子情報の保護 c）通信において変質及びメッセージを誤った宛先又は誤り伝送することの防止 d）誰でも使える外部サービス（例えば、インスタントメッセージ、ソーシャルネットワーク、ファイル共有又はクラウドストレージ）を利用する際の、事前承認の取得 e）公開されている アクセス可能なネットワークを通じて情報を転送するより強固な認証レベル f）電子通信手段に関連する制限（例えば、外部のメールアドレスへの電子メールの自動転送の防止） g）シャトルメッセージサービス（SMS）又はインスタントメッセージで重要な情報を送信しないように要員及びその他の利害関係者に助言する。これは、これらが公共の場所で（したがって、認可されていない人に）読まれたり、又は適切に保護されていない装置・機器に保存されたりする可能性があるためである。 h）ファクシミリ又はそのサービスの利用に伴う、次の問題に関わる要員及びその他の利害関係者への助言 1）組み込まれている記憶装置から受信文を取り出す、認可されていないアクセス 2）特定の番号にメッセージを送る故意又は偶然のプログラミング 合意については5.20.1供給者との合意にて、「物理的輸送又は論理的送信中に情報を保護するための情報の転送の管理策」が存在することから、本管理策においては「規則、手順」を対象とする。
13.2.1.3	情報転送のために通信設備を利用するときに従う手順及び管理策には、添付形式として通信される、取扱いに価値を要する電子情報の保護に関する手順を反映する。	5b-S.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 b）添付して通信する、取扱いに価値を要する電子情報の保護	子刊に関連記載あり			
13.2.1.4	情報転送のために通信設備を利用するときに従う手順及び管理策には、通信設備の許容できる利用（物理的な脆い者含む。）について規定した方針又は指針を反映する。	5b-S.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 g）情報転送手段の許容される利用に関するビジ固有の方針又は指針	子刊に関連記載あり	5.14.2	【再】全ての種類の情報の転送について、規則又は手順を整備する。	（5.14.2に対応する項を参照）
13.2.1.5	情報転送のために通信設備を利用するときに従う手順及び管理策には、要員、外部関係者及びその他の利用者の、組織を危うくするような行為（例えば、名誉き（毀）損、嫌がらせ、成りまし、チェーンメールの転送、架空購入）をしないことの責任を含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で最求めず）	–	（対応項なし）	–
13.2.1.6	情報転送のために通信設備を利用するときに従う手順及び管理策には、暗号技術の利用（例えば、情報の機密性、完全性及び責任性を保護するための暗号の利用）を含める。	5b-S.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 a）転送する情報を、盗聴、認可されていないアクセス、複製、改ざん、誤った経路での通信、破壊及びサービス拒否から保護するために設計された管理策。これは、情報の分類に合った それぞれのレベルのアクセス制御、及び暗号技術の利用など取扱いに価値を要する情報を保護するために必要な管理策を含む。	子刊に関連記載あり	5.14.2	【再】全ての種類の情報の転送について、規則又は手順を整備する。	（5.14.2に対応する項を参照）
13.2.1.7	情報転送のために通信設備を利用するときに従う手順及び管理策には、関連する国及び地域の法令及び規制に従った、全ての業務通信文（メッセージを含む）の保持及び処分に関する指針を反映する。	5b-S.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 i）情報の転送に関連するその他の関連する法令、規則及び契約上の要求事項の考慮	子刊に関連記載あり			
13.2.1.8	情報転送のために通信設備を利用するときに従う手順及び管理策には、通信設備の利用（例えば、外部のメールアドレスへの電子メールの自動転送）に関する管理策及び制限を反映する。	5b-S.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 f）電子通信手段に関連する制限	子刊に関連記載あり	5.14.3	【再】電子通信手段の使用について、規則又は手順を整備する。	（5.14.3に対応する項を参照）
13.2.1.9	情報転送のために通信設備を利用するときに従う手順及び管理策には、秘密情報を漏えいしないように適切な予防策を講じることの、要員への助言を含める。	5b-S.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 g）シャトルメッセージサービス（SMS）又はインスタントメッセージで重要な情報を送信しないように要員及びその他の利害関係者に助言する。これは、これらが公共の場所で（したがって、認可されていない人に）読まれたり、又は適切に保護されていない装置・機器に保存されたりする可能性があるためである。	子刊に関連記載あり			
13.2.1.10	情報転送のために通信設備を利用するときに従う手順及び管理策には、留守番電話に残したメッセージの、認可されていない者による再生、共有システムに保管、又は誤ダイアルによる間違った先へ保管されることを防止するため、秘密情報を含んだメッセージを留守番電話に残さないことを含める。	5b-S.14.7	情報の口頭での伝達を保護するために、要員及びその他の利害関係者に対して、次の事項を行うことが望ましいことを周整させる。 b）秘密情報を含んだメッセージを留守番電話又は音声メッセージに残さない、留守番電話又は音声メッセージに残したメッセージは、認可されていない者が再生する可能性、共有システムに保管されるり可能性、又は誤ダイアルの結果、間違って保管される可能性があるから である。	子刊に関連記載あり	5.14.1	転送中の情報を保護するための方針を策定する。	組織は、情報の転送に関するビジ固有の方針を確立し、それを間違える全ての関係者に伝達する。 転送中の情報を保護するための規則、手順及び合意は、関連する情報の分類を反映する。 組織と第三者との間で情報を転送する場合、転送中の全ての形式の情報を保護するために、転送の合意（受領者の認証を含む。）を備える。（5.14参照）、情報の転送は、電子的転送、物理的記憶媒体の輸送及び口頭での伝達によって行われる場合がある。 情報の口頭での伝達を保護するために、要員及びその他の利害関係者に対して、次の事項を行うことが望ましいことを留意させる。 a）公共の場所又は安全でない通信チャネルを通じた口頭での秘密会話は、認可されていない者に聞かれる可能性があるので行わない。 b）秘密情報を含んだメッセージを留守番電話又は音声メッセージに残さない、留守番電話又は音声メッセージに残したメッセージは、認可されていない者が再生する可能性、共有システムに保管される可能性又は誤ダイアル結果、間違って保管される可能性があるからである。 c）取扱いに価値を要する会話においては、始めに注意事項を説明し、出席者に、これから伝える情報の分類レベル及び取扱いの要求事項を知らせる。

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
13.2.1.11	情報転送のために通信設備を利用するときに従う手順及び管理策には、ファクシミリ又はそのサービスの利用に伴う問題（ファクシミリの受信文の取出し装置への認可されていないアクセス、特定の番号にメッセージを送る放棄又は誤操作のプログラミング、誤ダイヤル、又は意図って記憶した番号を問いることによる、誤った番号への文書及びメッセージの送付）について妥当に意識させることを含める。	Sb-S.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 h) ファクシミリ又はそのサービスの利用に伴う、次の問題に関わる妥当及びその他の利害関係者への影響： 1) 組み込まれている記憶装置から受信文を取り出す、認可されていないアクセス 2) 特定の番号にメッセージを送る放棄又は偶然のプログラミング	子引に関連記載あり	S.14.3	【再】電子通信手段の使用について、規則又は手順を整備する。	（S.14.3に対応する項を参照）
13.2.1.12	公共の場所、部外にセキュリティが確保されていない通信経路、出入り が自由なオフィス及び会議室では、秘密の会話はしないようがんことを要質に意識させる。	Sb-S.14.7	情報の口頭での伝達を保護するために、要員及びその他の利害関係者に対して、次の事項を行うことが望ましいことを規意させる。 a) 公共の場所又は安全でない通信チネルを通じた口頭での秘密会話は、認可されていない者に聞かれる可能性があるので行ってはいない。 c) 会話を聞く際は、適切なレベルで声を適用する。 d) 適切な部屋の管理策が実施されることを確実にする（例えば、防音、ドアを閉める。）。 e) 取扱いに意義を要する会話においては、始めに注意事項を説明し、出席者に、これから伝える情報の分類レベル及び取扱いの要求事項を知らせる。	子引に関連記載あり	S.14.1	【再】転送中の情報を保護するための方針を策定する。	（S.14.1に対応する項を参照）
13.2.1.13	情報転送サービスは、関連するいかなる法的要求事項についても順守する。	Sb-S.14.4	【再】全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 i) 情報の転送に関連するその他の関連する法令、規制及び契約上の要求事項の考慮	子引に関連記載あり	S.14.2	【再】全ての種類の情報の転送について、規則又は手順を整備する。	（S.14.2に対応する項を参照）
13.2.1.14	共有システム(リソース を介して情報が不正又は誤って転送されないように適切な予防策を講じることを含める。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
13.2.2	情報転送に関する合意 合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱う。	S.14	情報の転送 管理策 情報の転送の規則、手順又は合意を、組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備える。 目的 組織内及び外部の利害関係者との間で転送される情報のセキュリティを維持するため。		S.14	情報の転送 統制目標：情報の転送の規則、手順又は合意を、組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備える。 目的：組織内及び外部の利害関係者との間で転送される情報のセキュリティを維持するため。	
13.2.2.1	情報転送に関する合意に、送信、発送及び受領についての管理及び通知を行う責任を含める。	Sb-S.14.3	組織と第三者との間で情報を転送する場合、転送中の全ての形式の情報を保護するために、転送の合意（受領書の認証を含む。）を確立し、維持する。	子引に関連記載あり	S.14.1	【再】転送中の情報を保護するための方針を策定する。	（S.14.1に対応する項を参照）
13.2.2.2	情報転送に関する合意に、追跡可能性及び否認防止を確実にするための手順を含める。	Sb-S.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 b) 転送中の情報の受渡及び譲を維持することを含む、追跡可能性及び否認防止を確実にするための管理策	子引に関連記載あり	S.14.2	【再】全ての種類の情報の転送について、規則又は手順を整備する。	（S.14.2に対応する項を参照）
13.2.2.3	情報転送に関する合意に、こん（梱）包及び送信に関する必要最小限の技術標準を含める。	Sb-S.14.6	【再】物理的記憶媒体（紙を含む。）を転送する場合、規則、手順及び合意には、次の事項も含める。 c) 転送中に発生する可能性が思い物理的損傷から、製造業者の仕様に従って内容物を保護するこん（梱）包、例えば、熱、湿気又は電磁界への露出など、記録媒体の再生を妨げる可能性のある環境要因からの保護。こん（梱）包及び送付のための最小限の技術標準の使用。	子引に関連記載あり	S.14.4	【再】物理的記憶媒体の転送について、規則又は手順を整備する。	（S.14.4に対応する項を参照）
13.2.2.4	情報転送に関する合意に、預託条項を含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
13.2.2.5	情報転送に関する合意に、運送業者を確認する規準を含める。	Sb-S.14.6	【再】物理的記憶媒体（紙を含む。）を転送する場合、規則、手順及び合意には、次の事項も含める。 e) 運送業者を確認する規準	子引に関連記載あり	S.14.4	【再】物理的記憶媒体の転送について、規則又は手順を整備する。	（S.14.2に対応する項を参照）
13.2.2.6	情報転送に関する合意に、情報セキュリティインシデントが発生した場合（例えば、データの紛失）の責任及び賠償義務を含める。	Sb-S.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 d) 物理的記憶媒体の紛失又はデータの消失などの情報セキュリティインシデントが発生した場合の責任及び賠償義務	子引に関連記載あり	S.14.2	【再】全ての種類の情報の転送について、規則又は手順を整備する。	（S.14.2に対応する項を参照）
13.2.2.7	情報転送に関する合意に、取扱いに慎重を要する又は重要な情報に対する、合意されたラベル付けシステム（ラベルの意味を直ちに理解すること、及び情報を適切に保護することを確実にするため）の使用を含める。	Sb-S.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 a) 取扱いに慎重を要する又は重要な情報に対する、合意したラベル付けシステム（ラベルの意味を直ちに理解できること、及び情報を適切に保護することを確実にするもの）の使用	子引に関連記載あり			
13.2.2.8	情報転送に関する合意に、情報及びソフトウェアの記録及び読出しに関する技術標準を含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
13.2.2.9	情報転送に関する合意に、取扱いに慎重を要するもの（例えば、暗号鍵）を保護するために必要とされる、特別な管理策を含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
13.2.2.10	情報転送に関する合意に、転送中の情報についての、管理状況の維持を含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
13.2.2.11	情報転送に関する合意に、認証できるアクセス制御のレベルを含める。	Sb-S.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 a) 転送する情報を、盗聴、認可されていないアクセス、複製、誤った経路での通信、破壊及びサービス拒否から保護するために設計された管理策。これは、情報の分類に合ったそれぞれのレベルのアクセス制御、及び暗号技術の利用など取扱いに慎重を要する情報を保護するために必要な管理策を含む。	子引に関連記載あり	S.14.2	【再】全ての種類の情報の転送について、規則又は手順を整備する。	（S.14.2に対応する項を参照）
13.2.2.12	情報転送に関する合意においては、転送中の情報及び物理的媒体を保護するための方針、手順及び標準間を確立及び維持し、参照する。	Sb-S.14.1	組織は、情報の転送に関するトピック固有の方針を確立し、それを関連する全ての関係者に伝達する。	子引に関連記載あり	S.14.1	【再】転送中の情報を保護するための方針を策定する。	（S.14.1に対応する項を参照）
–	（対応項なし）	Sb-S.14.2	転送中の情報を保護するための規則、手順及び合意は、関連する情報の分類を反映する。	子引に関連記載あり	S.14.1	【再】転送中の情報を保護するための方針を策定する。	（S.14.1に対応する項を参照）
13.2.2.13	情報交換に関する、いかなる合意における情報セキュリティの事項も、関連する業務情報の取扱いに慎重を要する度合いを反映する。	Sb-S.14.4	【再】全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 a) 転送する情報を、盗聴、認可されていないアクセス、複製、改ざん、誤った経路での通信、破壊及びサービス拒否から保護するために設計された管理策。これは、情報の分類に合ったそれぞれのレベルのアクセス制御、及び暗号技術の利用など取扱いに慎重を要する情報を保護するために必要な管理策を含む。	子引に関連記載あり	S.14.2	【再】全ての種類の情報の転送について、規則又は手順を整備する。	（S.14.2に対応する項を参照）
13.2.3	電子的メッセージ通信 電子的メッセージ通信に含まれた情報は、適切に保護する。	S.14	情報の転送 管理策 情報の転送の規則、手順又は合意を、組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備える。 目的 組織内及び外部の利害関係者との間で転送される情報のセキュリティを維持するため。		S.14	情報の転送 管理策 情報の転送の規則、手順又は合意を、組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備えることが望ましい。 目的 組織内及び外部の利害関係者との間で転送される情報のセキュリティを維持するため。	
13.2.3.1	電子的メッセージ通信のための情報セキュリティでは、組織が採用している分類体系に従った、認可されていないアクセス、改ざん又はサービス妨害からのメッセージを保護する。	Sb-S.14.4	【再】全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 a) 転送する情報を、盗聴、認可されていないアクセス、複製、改ざん、誤った経路での通信、破壊及びサービス拒否から保護するために設計された管理策。これは、情報の分類に合ったそれぞれのレベルのアクセス制御、及び暗号技術の利用など取扱いに慎重を要する情報を保護するために必要な管理策を含む。	子引に関連記載あり	S.14.2	【再】全ての種類の情報の転送について、規則又は手順を整備する。	（S.14.2に対応する項を参照）
13.2.3.2	電子的メッセージ通信のための情報セキュリティでは、正しい送付先及びメッセージ送信を確実にするた組みを整備する。	Sb-S.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 c) 通信において文書及びメッセージを誤った宛先又は番号に送信することの防止	子引に関連記載あり	S.14.3	【再】電子通信手段の使用について、規則又は手順を整備する。	（S.14.3に対応する項を参照）
13.2.3.3	電子的メッセージ通信のための情報セキュリティでは、サービスの依頼性及び可用性を確保する。	Sb-S.14.4	全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 f) 転送サービスの依頼性及び可用性	子引に関連記載あり	S.14.2	【再】全ての種類の情報の転送について、規則又は手順を整備する。	（S.14.2に対応する項を参照）
13.2.3.4	電子的メッセージ通信のための情報セキュリティでは、法的考慮（例えば、電子署名のための要求事項）を含める。	Sb-S.14.4	【再】全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。 i) 情報の転送に関連するその他の関連する法令、規制及び契約上の要求事項の考慮	子引に関連記載あり	S.14.2	【再】全ての種類の情報の転送について、規則又は手順を整備する。	（S.14.2に対応する項を参照）
13.2.3.5	電子的メッセージ通信のための情報セキュリティでは、誰でも使える外部サービス（例えば、インスタントメッセージ、ソーシャルネットワーク、ファイル共有）を利用する際の、事前承認を取得する。	Sb-S.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 d) 誰でも使える外部サービスを利用する際の、事前承認の取得	子引に関連記載あり	S.14.3	【再】電子通信手段の使用について、規則又は手順を整備する。	（S.14.3に対応する項を参照）
13.2.3.6	電子的メッセージ通信のための情報セキュリティでは、公開されているネットワークからのアクセスを制御する。より強固な認証レベルを決定する。	Sb-S.14.5	情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。 e) 公開されているアクセス可能なネットワークを通じて情報を転送するとき、より強固な認証レベル	子引に関連記載あり			
13.2.3.7.β	クラウドサービス事業者は、電子メールによる電子的メッセージ通信において、クラウドサービス利用者がSPF、DKIMのいずれか又は両方による送信ドメイン認証技術の対策及び、DMARCによる送信側の対策を実施できるための機能又は利用者が設定するための情報を提供する。	–	（統一基準由来）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	S.14.5	電子メールサービスをクラウドサービス利用者に対して提供する場合、電子メールによる電子的メッセージ通信において、クラウドサービス利用者がSPF、DKIMのいずれか又は両方による送信ドメイン認証技術の対策及び、DMARCによる送信側の対策を実施できるための機能又は利用者が設定するための情報を提供する。	クラウドサービス事業者は、電子メールによる電子的メッセージ通信において、クラウドサービス利用者がSPF、DKIMのいずれか又は両方による送信ドメイン認証技術の対策及びDMARCによる送信側の対策を実施できるための機能又は利用者が設定するための情報を提供する。 a) SPF（sender policy Framework） b) DKIM（DomainKyes Identified Mail） c) DMARC（Domain-based Message Authentication Reporting and Conformance）

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
13.2.4	秘密保持契約又は守秘義務契約 情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ったレビュー、文書化する。	6.6	秘密保持契約又は守秘義務契約 管理策 情報保護に対する組織のニーズを反映する秘密保持契約又は守秘義務契約は、特定し、文書化し、定期的にレビューし、要員及びその他の関連する利害関係者が署名する。 目的： 要員又は外部の関係者がアクセスできる情報の秘密保持のため。		6.6	秘密保持契約又は守秘義務契約 統制目標：情報保護に対する組織のニーズを反映する秘密保持契約又は守秘義務契約は、特定し、文書化し、定期的にレビューし、要員及びその他の関連する利害関係者が署名する。 目的：要員又は外部の関係者がアクセスできる情報の秘密保持のため。	
13.2.4.1	秘密保持契約又は守秘義務契約には、法的に強制できる表現を用いて、秘密情報を保護するための要求事項を取り上げる。	6a-6.6.1	秘密保持契約又は守秘義務契約には、法的に強制できる表現を用いて、秘密情報を保護するための要求事項を取り上げる。	千代に関連記載あり	6.6.1	秘密保持契約又は守秘義務契約には、秘密情報を保護するための要求事項を含める。	秘密保持契約又は守秘義務契約には、法的に強制できる表現を用いて、秘密情報を保護するための要求事項を取り上げる。 組織の情報セキュリティ要求事項に基づいて、契約の条件は、取り扱われる情報の種類、その分類レベル、その使用及び当事者に許可されるアクセスを考慮して決定する。 秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 a）保護する情報の定義（例えば、秘密情報） b）秘密を無期限にては情報が一般公開されるまで保持する必要がある場合も含めた、契約の有効期間 c）契約終了時に要求する処置 d）認可されていない情報開示を避けるための、署名者の責任及び行為 e）情報、企業秘密及び知的財産の帰属、並びにこれらと秘密情報の保護との関係 f）秘密情報の許可された利用範囲、及び情報を利用する署名者の権利 g）悪意に取扱いに関連を要する状況における、秘密情報に関わる行為の監査及び監視の権利 h）認可されていない開示または秘密情報漏えいの、通知及び報告のプロセス i）契約終了時における情報の返却又は破棄に関する条件 j）契約の不履行が発生した場合に講じるべき処置 組織は、適用される法域における秘密保持契約又は守秘義務契約の順守を考慮に入れる。
13.2.4.2	秘密保持契約又は守秘義務契約は、外部関係者又は組織の従業員に適用する。	6a-6.6.2	秘密保持契約又は守秘義務契約は、利害関係者及び組織の要員との間で締結される。	管理策に関連記載あり	6.6.2	秘密保持契約又は守秘義務契約は、供給者を含む利害関係者及び組織の要員との間で締結する。	秘密保持契約又は守秘義務契約は、利害関係者及び組織の要員との間で締結される。
13.2.4.3	秘密保持契約又は守秘義務契約の当事者の種類、並びに当事者に許可される秘密情報のアクセス及び取扱いを考慮して、契約の要素を追定又は追加する。	6a-6.6.3	組織の情報セキュリティ要求事項に基づいて、契約の条件は、取り扱われる情報の種類、その分類レベル、その使用及び当事者に許可されるアクセスを考慮して決定する。	千代に関連記載あり	6.6.1	【再】秘密保持契約又は守秘義務契約には、秘密情報を保護するための要求事項を含める。	(6.6.1に対応する項を参照)
13.2.4.4	秘密保持契約又は守秘義務契約には、保護される情報の定義（例えば、秘密情報）を含める。	6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 a）保護する情報の定義	千代に関連記載あり			
13.2.4.5	秘密保持契約又は守秘義務契約には、秘密を無期限に保持する場合も含めた、契約の有効期間を含める。	6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 b）秘密を無期限にては情報が一般公開されるまで保持する必要がある場合も含めた、契約の有効期間	千代に関連記載あり			
13.2.4.6	秘密保持契約又は守秘義務契約には、契約終了時に要求する処置を含める。	6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 c）契約終了時に要求する処置	千代に関連記載あり			
13.2.4.7	秘密保持契約又は守秘義務契約には、認可されていない情報開示を避けるための、署名者の責任及び行為を含める。	6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 d）認可されていない情報開示を避けるための、署名者の責任及び行為	千代に関連記載あり			
13.2.4.8	秘密保持契約又は守秘義務契約には、情報、企業秘密及び知的財産の所有権、並びにこれらの秘密情報の保護との関連を含める。	6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 e）情報、企業秘密及び知的財産の帰属、並びにこれらと秘密情報の保護との関係	千代に関連記載あり			
13.2.4.9	秘密保持契約又は守秘義務契約には、秘密情報の許可された利用範囲、及び情報を利用する署名者の権利を含める。	6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 f）秘密情報の許可された利用範囲、及び情報を利用する署名者の権利	千代に関連記載あり			
13.2.4.10	秘密保持契約又は守秘義務契約には、秘密情報に関する行為の監査及び監視の権利を含める。	6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 g）悪意に取扱いに関連を要する状況における、秘密情報に関わる行為の監査及び監視の権利	千代に関連記載あり			
13.2.4.11	秘密保持契約又は守秘義務契約には、認可されていない開示又は秘密情報漏えいの、通知及び報告のプロセスを含める。	6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 h）認可されていない開示または秘密情報漏えいの、通知及び報告のプロセス	千代に関連記載あり			
13.2.4.12	秘密保持契約又は守秘義務契約には、契約終了時における情報の返却又は破棄に関する条件を含める。	6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 i）契約終了時における情報の返却又は破棄に関する条件	千代に関連記載あり			
13.2.4.13	秘密保持契約又は守秘義務契約には、契約違反が発生した場合にとるべき処置を含める。	6a-6.6.4	秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。 j）契約の不履行が発生した場合に講じるべき処置	千代に関連記載あり			
13.2.4.14	組織の情報セキュリティ要求事項に応じて、秘密保持契約又は守秘義務契約に必要な要素を含める。	6a-6.6.3	【再】組織の情報セキュリティ要求事項に基づいて、契約の条件は、取り扱われる情報の種類、その分類レベル、その使用及び当事者に許可されるアクセスを考慮して決定する。	千代に関連記載あり			
13.2.4.15	秘密保持契約又は守秘義務契約は、その法域において適用される法令及び規制の全てに従う。	6a-6.6.5	組織は、適用される法域における秘密保持契約又は守秘義務契約の順守を考慮に入れる。	千代に関連記載あり			
13.2.4.16	秘密保持契約又は守秘義務契約に関する要求事項は、定期的に及びこれら要求に影響する変化が発生した場合に、レビューする。	6a-6.6.6	秘密保持契約又は守秘義務契約に関する要求事項は、定期的に及びこれら要求に影響する変化が発生した場合に、レビューする。	管理策に関連記載あり	6.6.3	秘密保持契約又は守秘義務契約に関する要求事項は、定期的に及びこれら要求に影響する変化が発生した場合に、レビューする。	秘密保持契約又は守秘義務契約に関する要求事項は、定期的に及びこれら要求に影響する変化が発生した場合に、レビューする。
14.1.1	情報セキュリティ要求事項の分析及び仕様化 情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含める。	5.8	プロジェクトマネジメントにおける情報セキュリティ 管理策 情報セキュリティをプロジェクトマネジメントに組み入れる。 目的 プロジェクトのライフサイクル全体を通じて、プロジェクトマネジメントにおいて、プロジェクト及び成果物に関連する情報セキュリティリスクに効果的に対処することを確実にするため。		5.8	プロジェクトマネジメントにおける情報セキュリティ 統制目標：情報セキュリティをプロジェクトマネジメントに組み入れる。 目的：プロジェクトのライフサイクル全体を通じて、プロジェクトマネジメントにおいて、プロジェクト及び成果物に関連する情報セキュリティリスクに効果的に対処することを確実にするため。	
14.1.1.1	情報セキュリティ要求事項は、方針及び規則に由来する順守の要求事項、脅威のモデリング、インシデントのレビュー、又はぜい弱性の解押の使用のような、様々な方法を用いて特定する。	Sa-5.8.5	プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項は、情報セキュリティ方針、トピック固有の方針及び規則から順守すべき要求事項を導出することを含む、様々な方法を用いて決定する。	千代に関連記載あり	5.8.2	プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項を定義する。	プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項は、情報セキュリティ方針、トピック固有の方針及び規則から順守すべき要求事項を導出することを含む、決定する。 プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項は、脅威のモデリング、インシデントのレビュー、ぜい弱性の使用、緊急時対応計画策定などの活動から導き出すことができ、それによって、情報システムのアーキテクチャ及び設計を適用環境における脅威の脅威から保護することを確実にする。 情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 a）どのような情報が関係するか（情報の決定）、それに対応する情報セキュリティのニーズは何か（分類、5.12参照）。及び適切なセキュリティの欠如から生じる可能性のある事業への潜在的な悪影響 b）特に機密性、完全性及び可用性の観点から、関係する情報及びその他の関連資産に必要な保護のニーズ c）認証の要求事項を導き出すための、エンティティが提示する識別情報に求める保護又は保証のレベル d）顧客及びその他の潜在的な業務上の利用者のほか、関係するプロジェクトメンバ、潜在的な運用スタッフ、外部供給者などの特権をもつ、又は技術をもつ利用者に対する、アクセスの提供及び認可のプロセス e）利用者に対する、各自の義務及び責任の通知 f）トランザクションのログ取得及び監視、並びに否認防止の要求事項のような、業務プロセスに由来する要求事項 g）他の情報セキュリティ管理策によって必要になる要求事項 h）組織の活動に適用される法令、規則及び契約上の条件の順守 i）第三者からの委又は契約における関連セキュリティ義務を含む、組織の情報セキュリティ方針及びトピック固有の方針を満たすまでの必要な、第三者に求める保護又は保証のレベル
14.1.1.2	情報セキュリティ要求事項の特定作業の結果は、文書化し、全ての利害関係者によってレビューし、更新する。	Sa-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 d）顧客及びその他の潜在的な業務上の利用者のほか、関係するプロジェクトメンバ、潜在的な運用スタッフ、外部供給者などの特権をもつ、又は技術をもつ利用者に対する、アクセスの提供及び認可のプロセス	千代に関連記載あり			
14.1.1.3	情報セキュリティ要求事項及び情報セキュリティ管理策には、関連する情報の業務上の価値、及びセキュリティが不十分だった場合に業務に及ぼす可能性のある悪影響を反映する。	Sa-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 a）どのような情報が関係するか（情報の決定）、それに対応する情報セキュリティのニーズは何か、及び適切なセキュリティの欠如から生じる可能性のある事業への潜在的な悪影響	千代に関連記載あり			
14.1.1.4	情報セキュリティ要求事項及び関連するプロセスの特定及び管理は、情報システムプロジェクトにその初期段階で統合する。	Sa-5.8.2	問いもプロジェクトマネジメントでは、次の事項を要求する。 b）情報セキュリティ要求事項に基づいて、プロジェクトの早い段階で対処する。	千代に関連記載あり	5.8.1	【再】情報セキュリティリスクへの対応をプロジェクトマネジメントに組み入れる。	(5.8.1に対応する項を参照)
14.1.1.5	情報セキュリティ要求事項においては、利用者認証の要求事項を導き出すために、利用者が提示する識別情報に対して求める信頼のレベルを定める。	Sa-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 c）認証の要求事項を導き出すための、エンティティが提示する識別情報に求める信頼又は保証のレベル	千代に関連記載あり	5.8.2	【再】プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項を定義する。	(5.8.2に対応する項を参照)
14.1.1.6	情報セキュリティ要求事項においては、業務上の利用者のほか、特権を与えられた利用者及び技術をもつ利用者に対する、アクセスの提供及び認可のプロセスを定める。	Sa-5.8.7	【再】情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 d）顧客及びその他の潜在的な業務上の利用者のほか、関係するプロジェクトメンバ、潜在的な運用スタッフ、外部供給者などの特権をもつ、又は技術をもつ利用者に対する、アクセスの提供及び認可のプロセス	千代に関連記載あり			
14.1.1.7	情報セキュリティ要求事項においては、利用者及び運用担当者に対する、各自の義務及び責任の通知を明確にする。	Sa-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 e）利用者に対する、各自の義務及び責任の通知	千代に関連記載あり			
14.1.1.8	情報セキュリティ要求事項においては、関連する資産の保護の要求、特に、可用性、機密性及び完全性に関する保護の要求を明確にする。	Sa-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 b）特に機密性、完全性及び可用性の観点から、関係する情報及びその他の関連資産に必要な保護のニーズ	千代に関連記載あり			
14.1.1.9	情報セキュリティ要求事項においては、トランザクションのログ取得及び監視、並びに否認防止の要求事項のような、業務プロセスに由来する要求事項を定める。	Sa-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 f）トランザクションのログ取得及び監視、並びに否認防止の要求事項のような、業務プロセスに由来する要求事項	千代に関連記載あり			
14.1.1.10	情報セキュリティ要求事項においては、他のセキュリティ管理策によって義務が与えられる要求事項を定める（例えば、ログ取得及び監視のインタフェース、情報漏えい検知システム）。	Sa-5.8.7	情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。 g）他の情報セキュリティ管理策によって必要になる要求事項	千代に関連記載あり			
14.1.1.11	公衆ネットワークを介してサービスを提供するアプリケーション、又はトランザクションを実施するアプリケーションについては、14.1.2 及び14.1.3の管理策を考慮して決定する。	8c-8.20.2	【再】ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 e）公衆ネットワーク、第三者ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及びアプリケーションを保護するために、管理策を確立する。	千代に関連記載あり	8.20.1	【再】ネットワーク及びネットワーク装置のセキュリティを保つための対策を実施する。	(8.20.1に対応する項を参照)
14.1.1.12	製品を入手する際には、正式な試験及び調達プロセスに従う。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策等で総体的に）	–	（対応項なし）	–
14.1.1.13	製品の供給者との契約は、明確にされたセキュリティ要求事項を規定する。	Sd-5.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 a）ICT製品の供給者に、自らの製品が実装するセキュリティ機能及びそのセキュリティに配慮した適用に必要な機能を説明する情報を提供するよう要求する。	千代に関連記載あり	5.21.1	ICT製品及びサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセス及び手順を整備し、実施する。	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 a）ICT製品及びサービスの提供に適用する情報セキュリティ要求事項を定める。 b）供給者が組織に提供するICTサービスの一部を下請負契約に出す場合には、そのサプライチェーン全体に組織のセキュリティ要求事項を伝達するようICTサービスの供給者に要求する。 c）ICT製品に関して、その製品に他の供給者又は他のエンティティ（例えば、下請負ソフトウェア開発者、ハードウェア構成要素供給者）が導入又は依頼した構成要素が含まれる場合には、そのサプライチェーン全体に渡りセキュリティ要件を伝達するようICT製品の供給者に要求する。 d）ICT製品の供給者に、製品で使用しているソフトウェア構成要素を記載した情報を提供するよう要求する。 e）ICT製品の供給者に、自らの製品が実装するセキュリティ機能及びそのセキュリティに配慮した適用に必要な機能を説明する情報を提供するよう要求する。 f）提供されたICT製品及びサービスが指定のセキュリティ要求事項を順守していることを確認するため、監視プロセス及び順守状況を監視方法を実施する。このような供給者レビュー方法の例に、侵入テスト、及び供給者の情報セキュリティ運用に関する第三者立証の検証又は受け入れ確認がある。 g）製品又はサービスの機能を維持するために重要な構成要素を特定し、文書化するプロセスを実施する。重要な構成要素に対しては、組織の外で行われる場合に必要とされる活動、問題及び潜在的フォローアップの処分が求められる（例：供給者が製品又はサービスの構成要素を他の供給者に外部委託する場合。）。 h）重要な構成要素及びその供給元が、サプライチェーン全体を通じて追跡可能であるという保証を得る。 i）提供されたICT製品が期待どおりに機能し、予期しない又は好ましくない特性をたさないという保証を得る。 j）供給者からの構成要素が偽正のものであり、それが偽りで変更されていないことを確実にするための プロセスを実施する。対策の例に、改ざん防止ような、暗号ハッシュ検証又はポリシら署名がある。仕様外の動作を監視することが、改ざんは自由度を見つけるや新たな不可能性がある。改ざんの防止及び検知は、設計、開発、統合、運用及び保守を含むシステム開発ライフサイクルの段階の活動で実施する。 k）ICT製品が、例えば、正式な認証又は共通基準承認アレンジメント（Common Criteria Recognition Arrangement）などの評価保証を通じて、必要なセキュリティレベルを満たしていることの検証を得る。 l）サプライチェーンについての情報、並びに組織と供給者との間で主じる可能性のある問題及び妥協について の情報を共有するための規則を定める。 m）ICT構成要素のライフサイクル及び廃棄時の管理、並びにこれに関連するセキュリティリスクを管理するための具体的な プロセス実施すること。このようには、その構成要素が入手できなくなる（供給者が事業を変えるなる、又は供給者がこれらの構成要素の一部又は全部を製造しなくなる）ようなリスクを管理することを含める。代替供給者の特定、並びにソフトウェア及び力量を代替供給者に移転するプロセスを含める。

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
14.1.1.14	提案された製品のセキュリティの機能性が指定された要求を満たさない場合は、発生するリスク及び関連する管理策を、製品を購入する前又は変更前に再考する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応情なし）	–
14.1.1.15	当該システムにおいて情報するソフトウェア及びサービスと整合する製品のセキュリティ機能に関して、入手可能な手引を用いて、これを評価し、実施する。	8b-8.9.3	ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保つ構成のための標準テンプレートを次のように定義する。 a) 公開され、入手できる手引を使用する。	手引に関連記載あり	8.9.1	ハードウェア、ソフトウェア、サービス及びネットワークに関して、定義した構成を維持する元セスの整備及びツールを定義し、実装する。	組織は、ハードウェア、ソフトウェア、サービス（例えば、クラウドサービス）及びネットワークに関して、新しく導入したシステム及び運用システムの存続期間にわたって、定義した構成（セキュリティ機能を含む。）を維持するためのプロセス及びツールを定義し、実装する。 全ての構成変更を他の管理者とこを検索してするために、段階、責任及び手順を定める。 ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保つ構成のための標準テンプレートを次のように定義する。 a) 公開され、入手できる手引（例えば、業界及び独立したセキュリティ組織による認定のテンプレート）を使用する。 b) 十分なセキュリティレベルを決定するために、必要な保護レベルを考慮する。 c) 組織の情報セキュリティ方針、リスク評価の方針、標準及びその他のセキュリティ要求事項を支援する。 d) 組織内状況において、セキュリティ構成の実現可能性及び適用可能性を考慮する。 ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保つ構成の標準テンプレートは、定期的にレビューするこに加えて、新しい脅威又は新し技術に対処するが必要がある場合、又は組織のリアクレ対しハウハウを導入と場合に更新する。 ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保つ構成の標準テンプレートの確定に当たって、次の事項を考慮する。 a) 特権的又は業務管理者レベルのアクセス権をも１織装置機能と設を最小限にする。 b) 予め変化、使用されていない又はセキュリティが脆弱たいない機能情報を無効化する。 c) 予め変化機能及びサービスを無効化又は制限する。 d) 強力なユーティリティプログラム及びホストパラメータ設定へのアクセスを制限する。 e) ログを初期設定。 f) 初期パスワードなどの業者による初期設定情報を導入の直後に変更し、その他の重要なセキュリティ関連パラメータの初期状態もセレーする。 g) 既支の使用中断時間の後に、コンピューティング装置・機器から自動的にログオフするタイムアウト機能を作動させる。 h) 使用目的の要求事項が明示されていることを特証する（5.32参照）。 ハードウェア、ソフトウェア、サービス及びネットワークについて決定した構成を記録、全ての構成変更のログを維持する。これらの記録はセキュリティを保つ保管する。これは、構成サーバーによる構成やテンプレートなど使うなり方法で運用することが可能である。構成の変更は、変更管理プロセスに従う（8.32参照）。構成記録には、次の事項を含み得る。 a) 承認の最新の管理責任者又は連絡先情報 b) 構成の最終変更日 c) 構成テンプレートの版 d) その他の承認された構成との関係
14.1.1.16	製品を受け入れる基準は、特定したセキュリティ要求事項を満たすことの確証を与える機能の観点で定める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応情なし）	–
14.1.1.17	製品は、入手する前に製品を受け入れる基準に照らして評価する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応情なし）	–
14.1.1.18	機能の追加によって、許容できない追加のリスクを意の込まないことを確実にするために、レビューする。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応情なし）	–
14.1.1.19.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）	5.8.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
14.1.1.20.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）	5.8.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	特になし。
14.1.1.23	情報システムの誤りメッセージは、悪意ある者にとって役立つ情報の開示にならないようにする。	–	（SP800-53由来）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）			
14.1.1.24	情報システムの誤りメッセージは、特定の利用者にのみ開示する。	–	（SP800-53由来）	明確な対応関係なし	–	（対応情なし）	–
14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮 公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護する。	8.26	アプリケーションセキュリティの要求事項 管理策 アプリケーションを開発又は取得する場合、情報セキュリティ要求事項を特定し、規定し、承認する。 目的 アプリケーションを開発又は取得する場合、全ての情報セキュリティ要求事項を特定し、対応することを確実にするため。		8.26	アプリケーションセキュリティの要求事項 統制目標：アプリケーションを開発又は取得する場合、情報セキュリティ要求事項を特定し、規定し、承認する。 目的：アプリケーションを開発又は取得する場合、全ての情報セキュリティ要求事項を特定し、対応することを確実にするため。	
14.1.2.1	公衆ネットワークを経由するアプリケーションサービスは、各当事者が提示する自らの識別情報について、それぞれが互いに要求し合う技術（例えば、認証）のレベルを定める。	8d-8.26.4	組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 a) 各当事者が提示する自らの識別情報について、それぞれが互いに要求し合う技術のレベル	手引に関連記載あり	8.26.1	アプリケーションを開発又は取得する際の、情報セキュリティ要求事項を定義する。	アプリケーションセキュリティの要求事項はリスクアセスメントを通じて特定し、規定する。 アプリケーションセキュリティの要求事項は、情報セキュリティの専門家の支援を受けて作成することを考慮する。アプリケーションセキュリティの要求事項は、アプリケーションの目的に応じて、幅広いトピックにわたることがある。 アプリケーションセキュリティの要求事項には、具当するを場合には、次の事項を含める。 a) エンティその識別情報の保護のレベル（例えば、認証を通じて（5.17、8.2及び8.5参照）） b) アプリケーションや処理する情報の機能及びその他レベルの特定 c) アプリケーション内のデータ及び機能へのアクセス及びアクセスのレベルを分離することの必要性 d) 悪意のある攻撃又は意図しない事象の中断・阻害に対するレジリエンス（例えば、バックオーバーフロー又はSQL インジェクションの保護） e) トランザクションが生成、処理、完結又は保管される法域における法令及び規制上の要求事項 f) 関与する全ての当事者のプライバシーの必要性 g) 秘密情報の保護に関する要求事項 h) 処理、転送及び保持するデータの保護 i) 関与する全ての当事者間の通信をセキュリティを保って暗号化する必要性 j) 完全性の確認及び入力の妥当性確認を含む入力の管理策 k) 例外的な処理策（例えば、承認の自動解除又は二重承認の要求） l) 出力にアクセスできる人及びその認可も考慮した出力の管理策 m) 自由記述"欄の内容に関する制限、これは、機密データ（例えば、個人データ）を管理されずに保存することにつながり得るため。 n) トランザクションのログ取得及び監視、活動防止の要求事項及び、業務プロセスに由来する要求事項 o) 他のセキュリティ管理策によって必要となる要求事項（例えば、DLP取得及び監視システム並びに情報漏えい検知システムのインタフェース）
14.1.2.2	公衆ネットワークを経由するアプリケーションサービスは、重要な取引文書の内容の承認、その発行、及びその文書への署名を上限が行うかについての認可プロセスを明確にする。	8d-8.26.4	組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 c) 重要な取引文書の内容の承認、その発行、又はその文書への署名を上限が行えるかについての認可プロセス	手引に関連記載あり			組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 a) 各当事者が提示する自らの識別情報について、それぞれが互いに要求し合う技術のレベル b) 交換又は処理する情報の完全性に必要な保護のレベル、及び完全性の欠如を特定するための仕組み（例えば、追加の高機密、ハッシュ化、デジタル署名） c) 重要な取引文書の内容の承認、その発行、又はその文書への署名を上限が行えるかについての認可プロセス d) 重要な文書の機密性、完全性及び発送・受領の証明、並びに否認防止（例えば、入札手続、契約手続に関連する契約） e) トランザクションの機密性及び完全性（例えば、注文、納入先の宛名情報及び受領確認） f) トランザクションの機密性を維持する期間に関する要求事項 g) 保険及びその他の契約上の要求事項 電子注文及び支払を伴うアプリケーションの場合、次の事項を考慮する。 a) 注文情報の機密性及び完全性を維持するための要求事項 b) 顧客から提供された支払い情報を検証するため、適切な検証の度合い c) トランザクション情報が転送又は重複の防止 d) トランザクションの詳細を、公開している環境の外で保管すること（例えば、組織のイントラネット内に設置しているデータ保存環境）すること、及びインターネットから直接アクセス可能な電子記憶媒体上にそれを保持して危険にさらさないこと） e) 信頼できる専門機関を利用（例えば、ディジタル署名及びディジタル証明書の発行・維持の目的で利用）する場合、エンドトゥ エンドの証明書及び署名管理プロセスを通したセキュリティの統合及び組込み これらの考慮事項の幾つかは、法的要求事項を満たすにとがら、暗号（8.24参照）を適用することによって対応することが可能である（5.31～5.36を参照。特に、暗号に関連する法令については、5.31を参照。）。
14.1.2.3	公衆ネットワークを経由するアプリケーションサービスは、サービスの提供又は利用が認可されていることを適時業務ヒトラに通知しいることを確実にする仕組みを整備する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応情なし）	–
14.1.2.4	公衆ネットワークを経由するアプリケーションサービスは、入札手続、契約手続などにおいて、重要な文書の機密性、完全性及び発送・受領の証明、並びに契約の否認防止に関する要求事項を決定し、それを達成する。	8d-8.26.4	組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 d) 重要な文書の機密性、完全性及び発送・受領の証明、並びに否認防止	手引に関連記載あり	8.26.1	【再】アプリケーションを開発又は取得する際の、情報セキュリティ要求事項を定義する。	（8.26.1に対応する項を参照）
14.1.2.5	公衆ネットワークを経由するアプリケーションサービスは、重要な文書の完全性についての、供頼のレベルを定める。	8d-8.26.4	【再】組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 d) 重要な文書の機密性、完全性及び発送・受領の証明、並びに否認防止	手引に関連記載あり			
14.1.2.6	公衆ネットワークを経由するアプリケーションサービスは、秘密情報の保護に関する要求事項を定める。	8c-8.20.2	【再】ネットワークセキュリティの管理策では、特に、次の事項を考慮する。 a) 公衆ネットワーク、第三者ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及びアプリケーションを保護するために、管理策を確立する。	手引に関連記載あり			
14.1.2.7	公衆ネットワークを経由するアプリケーションサービスは、注文のトランザクション、支払い情報、納入先の宛名情報及び受領確認の機密性及び完全性を維持する。	8d-8.26.4	組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 e) トランザクションの機密性及び完全性	手引に関連記載あり			
14.1.2.8	公衆ネットワークを経由するアプリケーションサービスは、顧客から提供された支払い情報を検証するための、適切な検査の度合いを定める。	8d-8.26.5	電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。 b) 顧客から提供された支払い情報を検証するため、適切な検査の度合い	手引に関連記載あり			
14.1.2.9	公衆ネットワークを経由するアプリケーションサービスは、不正行為を防ぐため、最も適切な支払いの決済形式を選択する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応情なし）	–
14.1.2.10	公衆ネットワークを経由するアプリケーションサービスは、注文情報の機密性及び完全性を維持するために要求される保護のレベルを定める。	8d-8.26.5	電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。 a) 注文情報の機密性及び完全性を維持するための要求事項	手引に関連記載あり	8.26.1	【再】アプリケーションを開発又は取得する際の、情報セキュリティ要求事項を定義する。	（8.26.1に対応する項を参照）
14.1.2.11	公衆ネットワークを経由するアプリケーションサービスは、トランザクション情報の紛失又は重複を防止する。	8d-8.26.5	電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。 c) トランザクション情報の紛失の防止	手引に関連記載あり	8.26.1	【再】アプリケーションを開発又は取得する際の、情報セキュリティ要求事項を定義する。	（8.26.1に対応する項を参照）
14.1.2.12	公衆ネットワークを経由するアプリケーションサービスは、不正なトランザクションに関する賠償義務を明確にする。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応情なし）	–
14.1.2.13	公衆ネットワークを経由するアプリケーションサービスは、保険の要件を決定する。	8d-8.26.4	組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。 g) 保険及びその他の契約上の要求事項	手引に関連記載あり	8.26.1	【再】アプリケーションを開発又は取得する際の、情報セキュリティ要求事項を定義する。	（8.26.1に対応する項を参照）
14.1.2.14	アプリケーションサービスに関する当事者間の紛決めは、権限の詳細も含め、合意したサービス条件を商当事者に義務付ける合意書によって責付ける。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応情なし）	–
14.1.2.15	攻撃に対する対応力（resilience）の要求事項（関連するアプリケーションサーバを保護するための要求事項及びサービスの提供に必要となるネットワーク経立接続の可用性を確実にするための要求事項を含む。）を定める。	8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 d) 悪意のある攻撃又は意図しない事象の中断・阻害に対するレジリエンス	手引に関連記載あり	8.26.1	【再】アプリケーションを開発又は取得する際の、情報セキュリティ要求事項を定義する。	（8.26.1に対応する項を参照）
–	（対応情なし）	–	（統一基準由来）	令和7年度にて追加 （情報セキュリティ管理基準以外の由来）	8.26.2	クラウドサービス利用者に、電子証明書を用いた署名等、提供するアプリケーションやコンテンツの改ざん等がない真正なものであることを確認できる手段を提供する。	特になし。
14.1.3	アプリケーションサービスのトランザクションの保護 アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。 ・不完全な通信 ・誤った通信経路設定 ・認可されていないメッセージの変更 ・認可されていない開示 ・認可されていないメッセージの複製又は再生	8.26	アプリケーションセキュリティの要求事項 管理策 アプリケーションを開発又は取得する場合、情報セキュリティ要求事項を特定し、規定し、承認する。 目的 アプリケーションを開発又は取得する場合、全ての情報セキュリティ要求事項を特定し、対応することを確実にするため。		8.26	アプリケーションセキュリティの要求事項 統制目標：アプリケーションを開発又は取得する場合、情報セキュリティ要求事項を特定し、規定し、承認する。 目的：アプリケーションを開発又は取得する場合、全ての情報セキュリティ要求事項を特定し、対応することを確実にするため。	
14.1.3.1	アプリケーションサービスのトランザクションでは、トランザクションに関わる各当事者による電子署名を利用する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応情なし）	–
14.1.3.2	アプリケーションサービスのトランザクションでは、トランザクションの張々の面において、以下を確実にする仕組みを整備する。 1）全ての当事者の秘密認証情報は、有効であり、かつ、検証を経ている 2）トランザクションが秘密に保たれている 3）全ての当事者に関係するプライバシーを守っている	8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 f) 関与する全ての当事者のプライバシーの必要性 g) 秘密情報の保護に関する要求事項	手引に関連記載あり	8.26.1	【再】アプリケーションを開発又は取得する際の、情報セキュリティ要求事項を定義する。	（8.26.1に対応する項を参照）
14.1.3.3	アプリケーションサービスのトランザクションでは、関わる全ての当事者間の通信経路を暗号化する。	8d-8.26.3	アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。 i) 関与する全ての当事者間の通信をセキュリティを保って暗号化する必要性	手引に関連記載あり			
14.1.3.4	アプリケーションサービスのトランザクションでは、関わる全ての当事者間で使われる通信プロトコルのセキュリティを維持する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準で継承されず）	–	（対応情なし）	–
14.1.3.5	アプリケーションサービスのトランザクションでは、その詳細情報を、公開している環境の外（例えば、組織のイントラネット内に設置しているデータ保存環境）で保管すること、及びインターネットから直接アクセス可能な記憶媒体上にそれらを保持して危険にさらさないことを確実にする仕組みを整備する。	8d-8.26.5	電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。 d) トランザクションの詳細を、公開している環境の外で保管すること	手引に関連記載あり	8.26.1	【再】アプリケーションを開発又は取得する際の、情報セキュリティ要求事項を定義する。	（8.26.1に対応する項を参照）
14.1.3.6	アプリケーションサービスのトランザクションでは、信頼できる専門機関を利用（例えば、ディジタル署名及びディジタル証明書の発行・維持の目的での利用）する場合、エンドツーエンドの証明書及び／又は署名管理プロセスを通したセキュリティを統合し、組み込む。	8d-8.26.5	電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。 e) 信頼できる専門機関を利用する場合、エンドツー エンドの証明書及び署名管理プロセスを通したセキュリティの統合及び組込み	手引に関連記載あり			

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
14.2	開発及びサポートプロセスにおけるセキュリティ 管理目的：情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。	8.25	セキュリティに配慮した開発のライフサイクル 管理策 ソフトウェア及びシステムのセキュリティに配慮した開発のための規則を確立し、適用する。 目的 情報セキュリティを、ソフトウェア及びシステムのセキュリティに配慮した開発ライフサイクルにおいて設計し、実装することを確実にするため。		8.25	セキュリティに配慮した開発のライフサイクル 統制目標：ソフトウェア及びシステムのセキュリティに配慮した開発のための規則を確立し、適用する。 目的：情報セキュリティを、ソフトウェア及びシステムのセキュリティに配慮した開発ライフサイクルにおいて設計し、実装することを確実にするため。	
14.2.1	セキュリティに配慮した開発のための方針 ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用する。						
14.2.1.1	セキュリティに配慮した開発のための方針には、開発環境のセキュリティを含める。	8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 a）開発環境、テスト環境及び本番環境の分離	手引に関連記載あり	8.25.1	セキュリティに配慮したサービス、アーキテクチャ、ソフトウェア及びシステムを構築するための開発ライフサイクルを設計する。	セキュリティに配慮したサービス、アーキテクチャ、ソフトウェア及びシステムを構築するには、セキュリティに配慮した開発が必要となる。セキュリティに配慮した開発を達成するために、次の側面を考慮する。 a）開発環境、テスト環境及び本番環境の分離（8.31参照） b）ソフトウェア開発のライフサイクルにおける、次に関わるセキュリティに関する手引 1）ソフトウェア開発の方法論におけるセキュリティ（8.26及び8.27参照） 2）用いる各プログラム言語について定めた、セキュリティに配慮したコーディングに関する指針（8.28参照） c）仕様策定及び設計段階におけるセキュリティ要求事項（5.8参照） d）プロジェクトにおけるセキュリティの確認項目（5.8参照） e）開発テスト、コードスキャン、侵入テストなどのシステム及びセキュリティのテスト（8.29参照） f）ソースコード及び構成ファイルのためのセキュリティが保たれたリポジトリ（8.4及び8.9参照） g）担当管理におけるセキュリティ（8.32参照） h）アプリケーションセキュリティに関して必要な知識及び訓練（8.28参照） i）ぜい弱性を防止し、発見し、修正するに当たっての開発者の能力（8.28参照） j）トレンセンに関する将来の問題を回避しつつ、費用対効果の高いソリューションを確実にするための、ライセンスの要求事項及び代替案（5.32参照） 開発を外部委託した場合、組織は、供給者がセキュリティに配慮した開発のための組織の規則を順守していることの証拠を得る（8.30参照）。
14.2.1.2	セキュリティに配慮した開発のための方針には、ソフトウェア開発のライフサイクルにおける、以下の2点の手引きを含める。 1.ソフトウェア開発の方法論におけるセキュリティ 2.用いる各プログラミング言語について定めた、セキュリティに配慮したコーディングに関する指針	8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 b）ソフトウェア開発のライフサイクルにおける、次に関わるセキュリティに関する手引 1）ソフトウェア開発の方法論におけるセキュリティ 2）用いる各プログラム言語について定めた、セキュリティに配慮したコーディングに関する指針	手引に関連記載あり			
14.2.1.3	セキュリティに配慮した開発のための方針には、設計段階におけるセキュリティ要求事項を含める。	8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 c）仕様策定及び設計段階におけるセキュリティ要求事項	手引に関連記載あり			
14.2.1.4	セキュリティに配慮した開発のための方針には、プロジェクトの開発の節目ごとにおけるセキュリティの確認項目を含める。	8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 d）プロジェクトにおけるセキュリティの確認項目	手引に関連記載あり			
14.2.1.5	セキュリティに配慮した開発のための方針には、セキュリティが保たれたリポジトリを含める。	8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 f）ソースコード及び構成ファイルのためのセキュリティが保たれたリポジトリ	手引に関連記載あり			
14.2.1.6	セキュリティに配慮した開発のための方針には、版の管理におけるセキュリティを含める。	8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 g）版の管理におけるセキュリティ	手引に関連記載あり			
14.2.1.7	セキュリティに配慮した開発のための方針には、アプリケーションのセキュリティに関して必要な知識を含める。	8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 h）アプリケーションセキュリティに関して必要な知識及び訓練	手引に関連記載あり			
14.2.1.8	セキュリティに配慮した開発のための方針には、ぜい弱性を認識、発見及び修正するに当たっての開発者の能力を含める。	8d-8.25.1	セキュリティに配慮した開発を達成するために、次の側面を考慮する。 i）ぜい弱性を防止し、発見し、修正するに当たっての開発者の能力	手引に関連記載あり			
14.2.1.9	開発に適用される標準類が知られていない可能性がある場合、又は現行の最適な慣行に整合していなかった場合に、新規開発する場合及び/又は再利用する場合の両方に、セキュアプログラミング技術を用いる。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
14.2.1.10	セキュリティに配慮したコーディングに関する標準類を確認し、その使用を義務付ける。	8d-8.28.2	最低限のセキュリティに配慮したコーディングのベースラインを確立し、適用する。	手引に関連記載あり	8.28.1	セキュリティに配慮したコーディングの原則を策定する。	組織は、セキュリティに配慮したコーディングに関して優れたガバナンスを実現する。組織全体のプロセスを確立する。 最低限のセキュリティに配慮したベースラインを確立し、適用する。 セキュリティに配慮したコーディングのためのプロセス及びガバナンスを、第三者から入手したソフトウェア構成要素及びオープンソースソフトウェアも対象とするように拡張する。 組織は、組織のセキュリティに配慮したコーディングの原則を下記により方向付ける。 a）現実世界の脅威、並びにソフトウェアのぜい弱性に関する最新の動き及び情報を監視する b）組織のセキュリティに配慮したコーディングの原則を継続的に改善する c）組織のセキュリティに配慮したコーディングの原則に従うための学習を要員に促す これは、急速に変化する脅威の状況に対処するため、効果的なセキュリティに配慮したコーディング慣行の実施を確実にするのに役立ち得る。
14.2.1.11	開発者は、開発に適用する標準類の使用及び試験について訓練を受け、コードレビューによって標準類の使用を検証する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
14.2.1.12	開発を外部委託した場合、組織は、その外部開発者がセキュリティに配慮した開発のための規則を順守していることの保証を得る。	8d-8.25.2	開発を外部委託した場合、組織は、供給者がセキュリティに配慮した開発のための組織の規則を順守していることの保証を得る。	手引に関連記載あり	8.25.1	【再】セキュリティに配慮したサービス、アーキテクチャ、ソフトウェア及びシステムを構築するための、開発ライフサイクルを設計する。	（8.25.1に対応する項を参照）
14.2.1.13.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準で継承されず）	8.25.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
14.2.2	システムの変更管理手順 開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理する。	8.32	変更管理 管理策 情報処理設備及び情報システムの変更は、変更管理手順に従う。 目的 変更を実行するときに情報セキュリティを維持するため。		8.32	変更管理 統制目標：情報処理設備及び情報システムの変更は、変更管理手順に従う。 目的：変更を実行するときに情報セキュリティを維持するため。	
14.2.2.1	初期設計段階からその後の全ての保守業務に至るまで、システム、アプリケーション及び製品の完全性を確実にするため、正式な変更管理手順を文書化し、実施する。	8d-8.32.3	【再】変更管理手順は、情報処理設備及び情報システムにおける情報の機密性、完全性及び可用性を確実にするために、設計の初期段階からその後の全ての保守作業までのシステム開発のライフサイクル全体にわたって文書化し、実装する。	手引に関連記載あり	8.32.1	【再】情報処理設備及び情報システムの変更管理手順を整備し、対策を実施する。	（8.32.1に対応する項を参照）
14.2.2.2	新しいシステムの導入及び既存システムに対する重要な変更は、文書化、仕様化、試験、品質管理及び管理された実装からなる正式な手続に従う。	8d-8.32.1	【再】新しいシステムの導入及び既存システムに対する重要な変更は、文書化、仕様化、テスト、品質管理及び管理された実装についての合意された規則及び正式な手続に従う。	手引に関連記載あり			
14.2.2.3	新しいシステムの導入及び既存システムに対する重要な変更の際の手続には、リスクアセスメント、変更の影響分析及び必要なセキュリティ管理策の仕様化を含める。	8d-8.32.5	【再】変更管理手順には、次の事項を含む。 a）全ての依存関係を考慮した、変更の潜在的影響に関する計画策定及び評価	手引に関連記載あり			
14.2.2.4	新しいシステムの導入及び既存システムに対する重要な変更の際の手順は、既存のセキュリティ及び管理手順が損なわないこと、サポートプログラムとシステムへのアクセス又はその作業に必要な部分に限定されること、並びにいかなる変更に対しても正式な合意及び承認が得られていることを確実にするため仕組みを整備する。	8d-8.32.2	情報処理設備及び情報システムの全ての変更を良好に管理することを確実にするように、管理責任及び手順を設ける。	手引に関連記載あり			
14.2.2.5	変更管理手順には、実施可能な範囲でアプリケーション及びその運用に関する変更管理手順も統合する。	8d-8.32.4	【再】実施可能な場合には、ICT基盤及びソフトウェアの変更管理手順を統合する。	手引に関連記載あり			
14.2.2.6	変更管理手順には、合意された認可レベルの記録を維持することを含める。	8d-8.32.5	変更管理手順には、次の事項を含む。 g）上記の全てを含む変更の記録の維持	手引に関連記載あり			
14.2.2.7	変更管理手順には、変更は、認可されている利用者によって提出されることを確実にすることを含める。	8d-8.32.1	【再】新しいシステムの導入及び既存システムに対する重要な変更は、文書化、仕様化、テスト、品質管理及び管理された実装についての合意された規則及び正式な手続に従う。	手引に関連記載あり			
14.2.2.8	変更管理手順には、変更によって管理策及び完全性に関する手順が損なわれないことを確実にするために、管理策及び手順をレビューすることを含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
14.2.2.9	変更管理手順には、修正を必要とする全てのソフトウェア、情報、データベース及びハードウェアを特定することを含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
14.2.2.10	変更管理手順には、セキュリティとの既知の弱点を最少化するために、セキュリティ特に重要とされるコードを特定し、これを点検することを含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
14.2.2.11	変更管理手順には、作業を開始する前に、提案の詳細について正式な承認を得ることを含める。	8d-8.32.5	変更管理手順には、次の事項を含む。 b）変更の認可	手引に関連記載あり	8.32.1	【再】情報処理設備及び情報システムの変更管理手順を整備し、対策を実施する。	（8.32.1に対応する項を参照）
14.2.2.12	変更管理手順には、変更を実施する前に、認可されている利用者がその変更を受け入れることを確実にすることを含める。	8d-8.32.5	変更管理手順には、次の事項を含む。 c）関連する利害関係者への変更の伝達	手引に関連記載あり			
14.2.2.13	変更管理手順には、システムに関する一式の文書が各変更の完了時点で更新されること、及び古い文書は記録・保管されるか又は処分されることを確実にすることを含める。	8d-8.32.5	変更管理手順には、次の事項を含む。 h）運用文書類及び利用者手順が、適切な状態であるように、必要に応じて変更することを確実にすること	手引に関連記載あり			
14.2.2.14	変更管理手順には、全てのソフトウェアの更新について、版数の管理を維持することを含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
14.2.2.15	変更管理手順には、全ての変更要求の監査証跡を維持・管理することを含める。	8d-8.32.5	【再】変更管理手順には、次の事項を含む。 g）上記の全てを含む変更の記録の維持	手引に関連記載あり	8.32.1	【再】情報処理設備及び情報システムの変更管理手順を整備し、対策を実施する。	（8.32.1に対応する項を参照）
14.2.2.16	変更管理手順には、操作手順書などの適用文書類及び利用者手順が、適切な状態であるように、必要に応じて変更することを確実にすることを含める。	8d-8.32.5	変更管理手順には、次の事項を含む。 h）運用文書類及び利用者手順が、適切な状態であるように、必要に応じて変更することを確実にすること	手引に関連記載あり			
14.2.2.17	変更管理手順には、変更の実施は最も適切な時期に行い、関係する業務処理を妨げないことを確実にすることを含める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験する。	8.32	変更管理 管理策 情報処理設備及び情報システムの変更は、変更管理手順に従う。 目的 変更を実行するときに情報セキュリティを維持するため。		8.32	変更管理 統制目標：情報処理設備及び情報システムの変更は、変更管理手順に従う。 目的：変更を実行するときに情報セキュリティを維持するため。	
14.2.3.1	オペレーティングプラットフォームの変更によって、アプリケーションの機能及び処理の完全性が損なわれていないことを確実にするために、これに関係する手続きをレビューする。	8d-8.32.5	【再】変更管理手順には、次の事項を含む。 a）全ての依存関係を考慮した、変更の潜在的影響に関する計画策定及び評価	手引に関連記載あり	8.32.1	【再】情報処理設備及び情報システムの変更管理手順を整備し、対策を実施する。	（8.32.1に対応する項を参照）
14.2.3.2	オペレーティングプラットフォームの変更の実施前に適切な試験及びレビューを行っても際に合うように、オペレーティングプラットフォームの変更を通知することを確実にする仕組みを整備する。	8d-8.32.5	【再】変更管理手順には、次の事項を含む。 c）関連する利害関係者への変更の伝達	手引に関連記載あり			
14.2.3.3	事業継続計画に対して、適切な変更がなされることを確実にする仕組みを整備する。	8d-8.32.5	【再】変更管理手順には、次の事項を含む。 i）ICT継続計画並びに対応及び復旧手順が、適切な状態であるように、必要に応じて変更することを確実にすること	手引に関連記載あり			
14.2.4	パッケージソフトウェアの変更に対する制限 パッケージソフトウェアの変更は、抑止し、必要な変更だけに限る。また、全ての変更は、厳重に管理する。	8.32	変更管理 管理策 情報処理設備及び情報システムの変更は、変更管理手順に従う。 目的 変更を実行するときに情報セキュリティを維持するため。		8.32	変更管理 統制目標：情報処理設備及び情報システムの変更は、変更管理手順に従う。 目的：変更を実行するときに情報セキュリティを維持するため。	
14.2.4.1	可能な限り、そして実行可能な場合には、業者が供給するパッケージソフトウェアは、変更しないで用いる。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
14.2.4.2	パッケージソフトウェアの変更が必要な場合は、組み込まれている機能及び処理の完全性が損なわれるリスクへの対応を行う。	8d-8.28.13	ソフトウェアパッケージを変更するか要がある場合、次のことを考慮する。 a）組み込まれた管理策及び完全性プロセスが危険にさらされるリスク	手引に関連記載あり	8.28.5	外部ツール及びライブラリを使用する場合のプロセスを監督する。	外部ツール及びライブラリを使用する場合、組織は次の事項を考慮する。 a）外部ライブラリを管理し（例えば、使用するライブラリ及びそれらの版の目録を維持することによる）、リリースサイクルごとおよび規則正しく更新することを確実にする。 b）十分に検査された構成要素、特に認証及び暗号化の構成要素の選択、認可及び再利用 c）外部の構成要素の使用許可、セキュリティ及び脆弱 d）ソフトウェアが保守可能で、追跡することが、実証された定評のある供給元に由来することを確実にする。 e）開発資源及び成果物の十分に長期的な可用性 ソフトウェアパッケージを変更するか要がある場合、次のことを考慮する。 a）組み込まれた管理策及び完全性プロセスが危険にさらされるリスク b）業者の同意を得るかどうか。 c）標準のプログラム更新として業者から必要な変更を得る可能性 d）変更の結果として、将来、組織がソフトウェアの保守に責任を負うようになった場合の影響 e）使用中の他のソフトウェアとの互換性
14.2.4.3	パッケージソフトウェアの変更が必要な場合は、変更の頻度について、将来のソフトウェアの保守に対して、組織が責任を負うようになるかどうかの確認を行う。	8d-8.28.13	ソフトウェアパッケージを変更するか要がある場合、次のことを考慮する。 b）業者の同意を得るかどうか。	手引に関連記載あり			
14.2.4.4	パッケージソフトウェアの変更が必要な場合は、標準のなプログラム更新として、業者から必要とする変更が得られる可能性について確認を行う。	8d-8.28.13	ソフトウェアパッケージを変更するか要がある場合、次のことを考慮する。 c）標準のプログラム更新として業者から必要な変更を得る可能性	手引に関連記載あり			
14.2.4.5	パッケージソフトウェアの変更が必要な場合は、変更の結果として、将来のソフトウェアの保守に対して、組織が責任を負うようになるかどうかの確認を行う。	8d-8.28.13	ソフトウェアパッケージを変更するか要がある場合、次のことを考慮する。 d）変更の結果として、将来、組織がソフトウェアの保守に責任を負うようになった場合の影響	手引に関連記載あり			
14.2.4.6	パッケージソフトウェアの変更が必要な場合は、用いている他のソフトウェアとの互換性について確認を行う。	8d-8.28.13	ソフトウェアパッケージを変更するか要がある場合、次のことを考慮する。 e）使用中の他のソフトウェアとの互換性	手引に関連記載あり			
14.2.4.7	パッケージソフトウェアの変更が必要な場合、原本のソフトウェアは保管し、指定された箇所に対して変更を適用する。	8d-8.8.11	変更が必要な場合は、元のソフトウェアを保持し、指定された箇所に変更を適用する。	手引に関連記載あり	8.8.2	【再】情報システムに関連するぜい弱性への対策を実施する。	（8.8.2に対応する項を参照）
14.2.4.8	全ての認可されたソフトウェアに対して最新の承認したパッチ及びアプリケーションの更新を導入していることを確実にするために、ソフトウェアの更新管理手順を実施する。	8d-8.8.10	認可された全てのソフトウェアに、最新の承認済みパッチ及びアプリケーション更新を適用することを確実にするために、ソフトウェア更新管理プロセスを実装する。	手引に関連記載あり			
14.2.4.9	将来のソフトウェア更新において、パッケージソフトウェアの変更を再び適用できるように、全ての変更は、十分に制御し、文書化する。	8d-8.8.12	全ての変更は、必要に応じて将来のソフトウェアアップグレードに再適用できるように、完全に試験し、文書化する。	手引に関連記載あり			
14.2.4.9	【再】将来のソフトウェア更新において、パッケージソフトウェアの変更を再び適用できるように、全ての変更は、十分に制御し、文書化する。	8d-8.32.5	変更管理手順には、次の事項を含む。 d）変更のテスト及びテストの受入れ g）上記の全てを含む変更の記録の維持	手引に関連記載あり	8.32.1	【再】情報処理設備及び情報システムの変更管理手順を整備し、対策を実施する。	（8.32.1に対応する項を参照）
14.2.4.10	パッケージソフトウェアの変更が必要な場合には、変更は、独立した評価機関による試験を受け、正当性を証明する。	8d-8.8.13	必要に応じて、独立した評価機関がソフトウェアの変更を試験し、妥当性を確認する。	手引に関連記載あり	8.8.2	【再】情報システムに関連するぜい弱性への対策を実施する。	（8.8.2に対応する項を参照）

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
14.2.5	セキュリティに配慮したシステム構築の原則 セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用する。	8.27	セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則 管理策 セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの開発活動に対して適用する。 目的 情報システムを、開発のライフサイクルにおいてセキュリティに配慮して設計し、実装し、運用することを確実にするため。		8.27	セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則 統制目標：セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの開発活動に対して適用する。 目的：情報システムを、開発のライフサイクルにおいてセキュリティに配慮して設計し、実装し、運用することを確実にするため。	
14.2.5.1	セキュリティに配慮したシステム構築の原則に基づき、情報システムの構築手順を確立し、文書化し、組織の情報システム構築活動に適用する。	8d-8.27.1	セキュリティに配慮したシステム構築の原則を確立し、文書化し、情報システム構築活動に適用する。	手引に関連記載あり	8.27.1	セキュリティに配慮したシステム構築の原則を整備する。	セキュリティに配慮したシステム構築の原則を確立し、文書化し、情報システム構築活動に適用する。 セキュリティは、全てのアーキテクチャ（業務、データ、アプリケーション及び技術）において設計する。新技術は、セキュリティのリスクを分析し、その設計を既知の攻撃パターンに照らしてレビューする。セキュリティに配慮したシステム構築の原則は、利用者認証技術、セキュリティを保ったセッション管理及びデータの妥当性確認及びサニタイジング に関する詳細管理策となる。 セキュリティに配慮したシステム構築の原則には、次の分析を含める。 a）特定した脅威から情報及びシステムを保護するために必要なありゆるセキュリティ管理策 b）セキュリティ要件を明示した、検知、又はそれに対応するセキュリティ管理策の機能 c）特定の業務プロセスにとって必要な特定のセキュリティ管理策（例えば、税務にく関連を要する情報の暗号化、完全性の確認及び情報のディジタル署名） d）セキュリティ管理策をどこでどのように適用するか（例えば、セキュリティアーキテクチャ及び技術基盤に統合することによって）。 e）個々のセキュリティ管理策（手動及び自動）を連携し、統合した管理策群を作る方法
14.2.5.2	セキュリティは、情報セキュリティの必要性とアクセス性の必要性との均衡を保ちながら、全てのアーキテクチャ層（業務、データ、アプリケーション及び技術）において設計する。	8d-8.27.2	セキュリティは、全てのアーキテクチャ層（業務、データ、アプリケーション及び技術）において設計する。新技術は、セキュリティのリスクを分析し、その設計を既知の攻撃パターンに照らしてレビューする。	手引に関連記載あり			
14.2.5.3	新技術は、セキュリティとのリスクについて分析し、その設計を既知の攻撃パターンに照らしてレビューする。	8d-8.27.2	【再】セキュリティは、全てのアーキテクチャ層（業務、データ、アプリケーション及び技術）において設計する。新技術は、セキュリティのリスクを分析し、その設計を既知の攻撃パターンに照らしてレビューする。	手引に関連記載あり			
–	（対応項なし）	8d-8.27.3	セキュリティに配慮したシステム構築の原則には、次の分析を含める。 a)脅威した脅威から情報及びシステムを保護するために必要なありゆるセキュリティ管理策 b)セキュリティ要件を明示した、検知、又はそれに対応するセキュリティ管理策の機能 c)特定の業務プロセスにとって必要な特定のセキュリティ管理策 d)セキュリティ管理策をどこでどのように適用するか。 e)個々のセキュリティ管理策（手動及び自動）を連携し、統合した管理策群を作る方法	手引に関連記載あり			
–	（対応項なし）	8d-8.27.4	セキュリティに配慮したシステム構築の原則では、次の事項を考慮に入れる。 a) セキュリティアーキテクチャに統合する必要性 b) 技術的なセキュリティ基盤 c) 選択した技術を開発し、サポートする組織の能力 d) セキュリティ要求事項を満たすための費用、時間及び複雑さ e) 最新の優れた慣行	手引に関連記載あり			
–	（対応項なし）	8d-8.27.5	セキュリティに配慮したシステム構築には、次の事項を含める。 a）「設計によるセキュリティ（セキュリティバイデザイン）」、"多層防御"、"デフォルトでのセキュリティ"、デフォルト拒否"、"故障時のセキュリティ"、"外部アプリケーションからの入力を信用しない"、"導入時のセキュリティ"、"適応の歴史"、"最小特権"、"利便性及び冗長性"、"最小機能"などの、セキュリティアーキテクチャの原則の使用 b）情報セキュリティのいろいろな特性に、セキュリティ管理策を規定することを確実にし、セキュリティ要求事項を満たす取り組みとなる、セキュリティ側向の設計レビュー c）要求事項を完全には満たしていない（例えば、安全に関する要求事項を優先するため）セキュリティ管理策の文書化及び正式な承認 d）システムの要塞化（hardening）	手引に関連記載あり	8.27.2	システム構築の原則に基づいた、システム構築を実施する。	セキュリティに配慮したシステム構築には、次の事項を含める。 a）設計による セキュリティ（セキュリティバイデザイン）、多層防御、デフォルトでのセキュリティ、デフォルト拒否、故障時のセキュリティ、外部アプリケーションからの入力を信用しない、導入時のセキュリティ、適応の歴史、最小特権、利便性及び冗長性、最小機能などの、セキュリティアーキテクチャの原則の使用 b）情報セキュリティのいろいろな特性に、セキュリティ管理策を規定することを確実にし、セキュリティ要求事項を満たす取り組みとなる、セキュリティ側向の設計レビュー c）要求事項を完全には満たしていない（例えば、安全に関する要求事項を優先するため）セキュリティ管理策の文書化及び正式な承認 d）システムの要塞化（hardening） 組織は、次のようなゼロトラスト（zero trust）の原則を考慮する。
–	（対応項なし）	8d-8.27.6	組織は、次のような"ゼロトラスト（zero trust）"の原則を考慮する。 a）組織の情報システムは既に保護されていることを想定し、ネットワーク境界のセキュリティだけに依存しない。 b）情報システムへのアクセスにおいて"決して信頼せず、常に検証する"態度を採用する。 c）情報システムへの要求ゼロトラ エンドで暗号化されることを確実にする。 d）情報システムへの各要求を、組織の内部からのものであっても、公開の外部ネットワークから来たかのように検証する（すなわち、組織の境界の内側又は外側のいずれであれ、自動的に信頼することはしない）。 e）"最小特権"及び動的アクセス制御手法を使用する。これは、情報又はシステムの要求の認証及び認可を、認証情報、利用者識別情報、利用者エンドポイント機器に関するデータ、データ分類などの、状況に関する信頼に基づいて行うことを含む。 f）認証情報及び利用者識別情報、利用者エンドポイント機器に関するデータ、並びにデータ分類を含めた信頼に基づいて、例えば、強力な認証を実行することによって、情報システムの要求を常に認証し、認可要求の妥当性を常に確認する。	手引に関連記載あり			
14.2.5.4	セキュリティに配慮したシステム構築の原則及び確立した構築手順は、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするために、定期的にレビューする。	8d-8.27.9	セキュリティに配慮したシステム構築の原則及び確立した構築手順は、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするために、定期的にレビューする。	手引に関連記載あり	8.27.3	システム構築の原則及び構築手順を定期的にレビューする。	確立したセキュリティに配慮したシステム構築の原則は、該当する場合には、組織と組織が外部委託した供給者との間の、契約及び利害カを持つその他の企業を通じて、外部委託した情報システムの開発にも適用する。 組織は、供給者のセキュリティに配慮したシステム構築の原則及び確立した構築手順が、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするために、定期的にレビューする。 セキュリティに配慮したシステム構築の原則及び確立した構築手順が、新規の潜在的な脅威に対応するないろいろで常に最新であること、及び適用される技術及びソリューションの進展に継続して適用可能であることを確実にするために、定期的にレビューする。
14.2.5.5	セキュリティに配慮したシステム構築の原則及び手順が、新規の潜在的な脅威に対抗するいろいろで最新であり続けていること、及び適用される技術及びソリューションの進展に適用可能であり続けていることを確実にするために、定期的にレビューする。	8d-8.27.10	セキュリティに配慮したシステム構築の原則及び確立した構築手順が、新規の潜在的な脅威に対抗するないろいろで常に最新であること、及び適用される技術及びソリューションの進展に継続して適用可能であることを確実にするために、定期的にレビューする。	手引に関連記載あり			
14.2.5.6	セキュリティに配慮したシステム構築の原則は、組織と組織が外部委託した供給者との間の、契約及び利害カを持つその他の企業を通じて、外部委託した情報システムにも適用する。	8d-8.27.7	確立したセキュリティに配慮したシステム構築の原則は、該当する場合には、組織と組織が外部委託した供給者との間の、契約及び利害カを持つその他の企業を通じて、外部委託した情報システムの開発にも適用する。	手引に関連記載あり			
14.2.5.7	組織は、供給者の設計のセキュリティに関する原則が、自身の原則と同様に厳密なものであることを確認する。	8d-8.27.8	組織は、供給者のセキュリティに配慮したシステム構築の行為が組織のニーズと一致することを確実にする。	手引に関連記載あり			
14.2.5.8	セキュリティに配慮したシステムを構築するための原則に基づき、通信セッションの真正性を維持する。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
14.2.5.9	セキュリティに配慮したシステムを構築するための原則に基づき、システムへの入力情報の有効性を確かめる。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
14.2.6	セキュリティに配慮した開発環境 組織は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護する。	8.31	開発環境、テスト環境及び本番環境の分離 管理策 開発環境、テスト環境及び本番環境は、分離してセキュリティを保つ。 目的 開発活動及びテスト活動による危険から本番環境及びそのデータを保護するため。		8.31	開発環境、テスト環境及び本番環境の分離 統制目標：開発環境、テスト環境及び本番環境は、分離してセキュリティを保つ。 目的：開発活動及びテスト活動による危険から本番環境及びそのデータを保護するため。	
14.2.6.1	セキュリティに配慮した開発環境には、システムの開発及び統合に関連する資産、プロセス及び技術を含める。	8d-8.31.3	全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。 a）全ての開発、統合及びテストツール（ビルド、インテグレータ、コンパイラ、構成システム及びライブラリを含む。）のパッチ適用及び更新	手引に関連記載あり	8.31.2	開発環境及びテスト環境は必要な要件を定めて保護する。	全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。 a）全ての開発、統合及びテストツール（ビルダ、インテグレータ、コンパイラ、構成システム及びライブラリを含む。）のパッチ適用及び更新 b）システム及びソフトウェアのセキュリティに配慮した構成 c）環境へのアクセスの制御 d）環境の変更及びそこに保存されているコードの監視 e）環境の、セキュリティに配慮した監視 f）環境のバックアップをとること
14.2.6.2	組織は、個々のシステム開発業務に伴うリスクを評価し、システムごとに処理、保管及び伝送されるデータの取扱いに関連する変化へも考慮して、セキュリティに配慮した開発環境を確立する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策まで継承されず）	–	（対応項なし）	–
14.2.6.3	組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、適用される外部及び内部の要求事項（例えば、規制又は方針によるもの）を定める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策まで継承されず）	–	（対応項なし）	–
14.2.6.4	組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、組織によって既に実施されており、システム開発を支えるようなセキュリティ管理策を定める。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策まで継承されず）	–	（対応項なし）	–
14.2.6.5	組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、その環境で作業する要員の信頼性を考慮して要員を決定する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策まで継承されず）	–	（対応項なし）	–
14.2.6.6	組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、システム開発に関連した外部委託の程度を考慮して委託先を決定する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策まで継承されず）	–	（対応項なし）	–
14.2.6.7	組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、異なる開発環境の分離の必要性を考慮して環境を構築する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策まで継承されず）	–	（対応項なし）	–
14.2.6.8	組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、開発環境へのアクセスの制御を実施する。	8d-8.31.3	全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。 c）環境へのアクセスの制御	手引に関連記載あり	8.31.2	【再】開発環境及びテスト環境は必要な要件を定めて保護する。	（8.31.2に対応する項を参照）
14.2.6.9	組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、開発環境の変更及びそこに保存されているコードに対する変更を監視する。	8d-8.31.3	全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。 d）環境の変更及びそこに保存されているコードの監視	手引に関連記載あり			
14.2.6.10	組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、セキュリティに配慮した適用可能でのバックアップを保管する。	8d-8.31.3	全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。 f）環境のバックアップをとること	手引に関連記載あり			
14.2.6.11	組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、開発環境から、及び開発環境への、データの移動を管理する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策まで継承されず）	–	（対応項なし）	–
14.2.6.12	特定の開発環境の保護レベルを決定した後、組織は、セキュリティに配慮した開発手順の中の該当する プロセス を定義し、必要とするgeneral の要員にこれらを提供する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理策まで継承されず）	–	（対応項なし）	–
–	（対応項なし）	8d-8.31.4	一人の人間が、事前のレビュー及び承認なしに、開発環境及び本番環境の両方に変更を加えることができないようにする。	手引に関連記載あり	8.31.3	一人の人間が、事前のレビュー及び承認なしに、開発環境及び本番環境の両方に変更を加えることができないようにする。	一人の人間が、事前のレビュー及び承認なしに、開発環境及び本番環境の両方に変更を加えることができないようにする。これは、例えばアクセス権の分離又は監視を伴う規則によって達成可能である。 通常と異なる状況では、即可されていない変更を検出し、対処するために、詳細なログ取得、リアルタイム監視などの追加の対策を実施する。
–	（対応項なし）	（8d-8.31.4参考）	これは、例えばアクセス権の分離又は監視を伴う規則によって達成可能である。	手引に関連記載あり			
–	（対応項なし）	8d-8.31.5	通常と異なる状況では、即可されていない変更を検出し、対処するために、詳細なログ取得、リアルタイム監視などの追加の対策を実施する。	手引に関連記載あり			
14.2.7	外部委託による開発 組織は、外部委託したシステム開発活動を監督し、監視する。	8.30	外部委託による開発 管理策 組織は、外部委託したシステム開発に関する活動を指揮し、監視し、レビューする。 目的 組織が要求する情報セキュリティ対策が、外部委託したシステム開発で実施されることを確実にするため。		8.30	外部委託による開発 統制目標：組織は、外部委託したシステム開発に関する活動を指揮し、監視し、レビューする。 目的：組織が要求する情報セキュリティ対策が、外部委託したシステム開発で実施されることを確実にするため。	
–	（対応項なし）	8d-8.30.1	システム開発を外部委託する場合には、次の事項を行う。 a）要求事項及び期待を伝達する。 b）要求事項を満たし、期待に応えることを合意する。 c）外部委託が提供された作業及び成果物がこの期待を満たすかどうかを継続的に監視する。 d）開発されたシステムをレビューする。	手引に関連記載あり	8.30.1	外部委託したシステム開発に関して、要求する情報セキュリティ対策が実施されるための対策を実施する。	システム開発を外部委託する場合には、次の事項を行う。 a）要求事項及び期待を伝達する。 b）要求事項を満たし、期待に応えることを合意する。 c）外部委託が提供された作業及び 成果物がこの期待を満たすかどうかを継続的に監視する。 d）開発されたシステムをレビューする。 組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 a）外部委託した内容に関する使用許諾の合意、コードの帰属及び知的財産権（8.32参照） b）セキュアに配慮した設計、コーディング及びテストの実施についての契約上の要求事項（8.25～8.29参照） c）外部の開発者が考慮すべき脅威モデルの提供 d）成果物の受入れ工程にて脆弱な部分へテスト（8.29参照） e）受け入れられる最低限のセキュリティ及びプライバシー機能を実現していることを示す証拠の提出（例えば、契約報告書） f）可能に当たって、悪意のある内容（意図的なものか及び意図しないものの）の存在を防ぐために、十分なテストを実施していることを示す証拠の提出 g）既知のかい弱性が含まれないよう、十分なテストを実施していることを示す証拠の提出 h）ソフトウェアソースコードの開発契約（例えば、供給者が作業を終了する場合） i）開発のプロセス及び管理策を監査する、契約に基づく権利 j）開発環境のセキュリティ要求事項（8.31参照） k）適用される法令（例えば、個人データの保護に関する法令）の考慮
14.2.7.1	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、外部委託した内容に関連する使用許諾に関する取決め、コードの所有権及び知的財産権に関わる事項を契約に含める。	8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 a）外部委託した内容に関する使用許諾の合意、コードの帰属及び知的財産権	手引に関連記載あり			
14.2.7.2	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、セキュリティに配慮した設計、コーディング及び試験の実施についての要求事項を契約に含める。	8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 b）セキュリティに配慮した設計、コーディング及びテストの実施についての契約上の要求事項	手引に関連記載あり			
14.2.7.3	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、外部の開発者への、承認済みの脅威モデルの提供を契約に含める。	8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 c）外部の開発者が考慮すべき脅威モデルの提供	手引に関連記載あり			
14.2.7.4	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、成果物の受入れ工程にて脆弱な部分を受け入れ試験を契約に含める。	8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 d）成果物の受入れ工程にて脆弱な部分へテスト	手引に関連記載あり			
14.2.7.5	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、セキュリティ及びプライバシーについて、容認可能な最低限のレベルを定めるために セキュリティに well （関）値を用いることを示す証拠の提出を契約に含める。	8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 e）受け入れられる最低限のセキュリティ及びプライバシー機能を実現していることを示す証拠の提出	手引に関連記載あり			
14.2.7.6	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、引用に当たって、悪意のある内容（意図的なものか及び意図しないものの）が含まれないよう、十分な試験が実施されていることを示す証拠の提出を契約に含める。	8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 f）引用に当たって、悪意のある内容（意図的なものか及び意図しないものの）の存在を防ぐために、十分なテストを実施していることを示す証拠の提出	手引に関連記載あり			
14.2.7.7	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、既知のかい弱性が含まれないよう、十分な試験が実施されていることを示す証拠の提出を契約に含める。	8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 g）既知のかい弱性が含まれないよう、十分なテストを実施していることを示す証拠の提出	手引に関連記載あり			
14.2.7.8	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、脆弱契約に関する取決め（例えば、リースコード が利用できなくなった場合）を契約に含める。	8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 h）ソフトウェアソースコードの預託契約	手引に関連記載あり			
14.2.7.9	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、開発のプロセス及び管理策を監督するための権利を契約に含める。	8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 i）開発のプロセス及び管理策を監督する、契約に基づく権利	手引に関連記載あり			
14.2.7.10	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、成果物の作成に用いられる開発環境の再効な又は最化を契約に含める。	8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 j）開発環境のセキュリティ要求事項	手引に関連記載あり			
14.2.7.11	システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、適用される法令の順守及び管理の効果の検証については、組織が責任を負うことを契約に含める。	8d-8.30.2	組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。 k）適用される法令の考慮	手引に関連記載あり			
14.2.8	システムセキュリティの試験 セキュリティ機能（functionality）の試験は、開発期間中に実施する。	8.29	開発及び受入れにおけるセキュリティテスト 管理策 セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施する。 目的 アプリケーション又はコードを本番環境に導入するに、情報セキュリティ要求事項が満たされているかどうかの受け入れ機能を定めるため。		8.29	開発及び受入れにおけるセキュリティテスト 統制目標：セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施する。 目的：アプリケーション又はコードを本番環境に導入するに、情報セキュリティ要求事項が満たされているかどうかの受け入れ機能を定めるため。	

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
14.2.8.1	組織内でシステムを新規に開発、更新するプロセスにおいては、詳細な活動計画及び一定範囲の条件下での入出力試験の準備を含め組織的な試験及び検証は、最初に開発チームが実施する。	8d-8.29.1	新規の情報システム、アップグレード及び新しい版は、開発プロセスにおいて組織的に試験し、検証する。	予引に関連記載あり	8.29.2	セキュリティテストを実施し、欠陥があれば修正をする。	新規の情報システム、アップグレード及び新しい版は、開発プロセスにおいて組織的に試験し、検証する。 セキュリティテストは、システム又は構成要素のテストに絞込む、その一部とする。 セキュリティテストは、機能的又は非機能的に表現することができる一連の要求事項に照らして実施する。 セキュリティテストは、次の事項のテストを含む。 a) セキュリティ機能（例えば、利用者認証（8.5参照）、アクセス制限（8.3参照）及び暗号の利用（8.24参照）） b) セキュリティに配慮したコーディング（8.28参照） c) オペレーティングシステム、ファイアウォール及びその他のセキュリティ構成要素の構成を含む、セキュリティに配慮した構成（8.9、8.20及び8.22参照） セキュリティテスト計画は、一連の基準を使用して決定する。 セキュリティの程度は、システムの重要性、性質及び導入する変更の潜在的影響に見合ったものにする。 セキュリティに配慮したコーディングを対象としたセキュリティテストを実施する。 オペレーティングシステム、ファイアウォール及びその他のセキュリティ構成要素の構成を含む、セキュリティに配慮した構成を対象としたセキュリティテストを実施する。 組織は、セキュリティに関係する欠陥の修正を検証する。検証には、コード分析ツールなどの脆弱性スキャナなどの自動化ツールを利用することができる。 組織内で開発するソフトウェアについてのセキュリティテストは、次の順に行う。 a) 最初に開発チームが実施する。 b) 次に、システムが期待どおりに、かつ、期待した形で行う動作することを確実にするために、独立した受入れテストを実施する（5.8参照）。 セキュリティのテストにおいて、次の事項を考慮する。 a) セキュリティの欠陥のテストに関連して、予期しない入力又は条件を含め、コードのレビュー活動を実施する。 b) セキュリティに配慮していない構成及びシステムの甘い弱性を特定するために、甘い弱性スキャンを実施する。 c) セキュリティに配慮していないコード及び設計を特定するために、侵入テストを実施する。 外部委託した開発及び購入した構成要素については、取得プロセスに従う。 供給者との契約では、特定したセキュリティ要求事項に言及する（5.20 参照）。 外部から調達する製品及びサービスは、取得前に供給者との契約で特定したセキュリティ要求事項に基づ判定基準に照らして評価する。 セキュリティテストは、システムが組織の環境にてい弱性をもたらさないこと及びテストが脅威であるものであることを確実にするために、対象の本番環境に可能な限り一致するテスト環境で実施する（8.31参照）。
–	（対応項なし）	8d-8.29.5	セキュリティテスト計画は、一連の判定基準を使用して決定する。	予引に関連記載あり			
14.2.8.3	試験は、そのシステムの重要性及び性質に見合った程度で実施する。	8d-8.29.6	セキュリティテストの程度は、システムの重要性、性質及び導入する変更の潜在的影響に見合ったものにする。	予引に関連記載あり			
–	（対応項なし）	8d-8.29.7	セキュリティテスト計画には次の事項を含める。 a) 活動及びテストの詳細スケジュール b) 一連の条件の下での入力及び予想される出力 c) 結果を評価する基準 d) 必要な場合、更なる処置の決定	予引に関連記載あり	8.29.1	開発及び受入れにおけるセキュリティテスト計画を策定する。	セキュリティテスト計画には次の事項を含める。 a) 活動及びテストの詳細スケジュール b) 一連の条件の下での入力及び予想される出力 c) 結果を評価する基準 d) 必要な場合、更なる処置の決定
14.2.9	システムの受入れ試験 新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立する。	8.29	開発及び受入れにおけるセキュリティテスト 管理策 セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施する。 目的 アプリケーション又はコードを本番環境に導入するに、情報セキュリティ要求事項が満たされているかどうかの受け入れ可能性確認をするため。		8.29	開発及び受入れにおけるセキュリティテスト 統制目標：セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施する。 目的：アプリケーション又はコードを本番環境に導入するに、情報セキュリティ要求事項が満たされているかどうかの受け入れ可能性確認をするため。	
14.2.9.1	システムの受入れ試験は、情報セキュリティ要求事項の試験及びセキュリティに配慮したシステム開発の側行の観守を含める。	8d-8.29.4	セキュリティテストは、次の事項のテストを含む。 a) セキュリティ機能 b) セキュリティに配慮したコーディング c) オペレーティングシステム、ファイアウォール及びその他のセキュリティ構成要素の構成を含む、セキュリティに配慮した構成	予引に関連記載あり	8.29.2	[再]セキュリティテストを実施し、欠陥があれば修正をする。	（8.29.2に対応する項を参照）
14.2.9.2	受け入れた構成部品及び統合されたシステムに対して、試験を実施する。	8d-8.29.2	セキュリティテストは、システム又は構成要素のテストに絞込む、その一部とする。	予引に関連記載あり			
14.2.9.3	組織は、コード分析ツール又はぜい弱性スキャナのような自動化ツールを利用してセキュリティに関連する欠陥を検出した場合は、この修正を検証する。	8d-8.29.8	組織は、セキュリティに関係する欠陥の修正を検証する。	予引に関連記載あり			
–	（対応項なし）	8d-8.29.9	組織内で開発するソフトウェアについてのセキュリティテストは、次の順に行う。 a) 最初に開発チームが実施する。 b) その次に、システムが期待どおりに、かつ、期待した形で行う動作することを確実にするために、独立した受入れテストを実施する	予引に関連記載あり			
–	（対応項なし）	8d-8.29.10	セキュリティのテストにおいて、次の事項を考慮する。 a) セキュリティの欠陥のテストに関連して、予期しない入力又は条件を含め、コードのレビュー活動を実施する。 b) セキュリティに配慮していない構成及びシステムの甘い弱性を特定するために、甘い弱性スキャンを実施する。 c) セキュリティに配慮していないコード及び設計を特定するために、侵入テストを実施する。	予引に関連記載あり			
–	（対応項なし）	8d-8.29.11	外部委託した開発、及び購入した構成要素については、取得プロセスに従う。	予引に関連記載あり			
–	（対応項なし）	8d-8.29.12	供給者との契約では、特定したセキュリティ要求事項に言及する。	予引に関連記載あり			
–	（対応項なし）	8d-8.29.13	外部から調達する製品及びサービスは、取得前に供給者との契約で特定したセキュリティ要求事項に基づく判定基準に照らして評価する。	予引に関連記載あり			
14.2.9.4	試験は、システムが脆弱の環境にてい弱性をもたらさないこと及びが脆弱であるものであることを確実にするために、現実に即した試験環境で実施する。	8d-8.29.14	セキュリティテストは、システムが脆弱の環境にてい弱性をもたらさないこと及びテストが脆弱であるものであることを確実にするために、対象の本番環境に可能な限り一致するテスト環境で実施する。	予引に関連記載あり			
14.3	試験データ 管理目的：試験に用いるデータの保護を確実にするため。	8.33	テスト用情報 管理策 テスト用情報は、適切に選定し、保護し、管理する。 目的 テストの適切な実施、及びテストに使用する運用情報の保護を確実にするため。		8.33	テスト用情報 統制目標：テスト用情報は、適切に選定し、保護し、管理する。 目的：テストの適切な実施、及びテストに使用する運用情報の保護を確実にするため。	
14.3.1	試験データの保護 試験データは、注意深く選定し、保護し、管理する。						
14.3.1.1	PII 又はその他の秘密情報を含んだ運用データ、試験目的に用いない。	8d-8.33.1	テスト結果の機密性及び関連する運用情報の機密性を確実にするよう、テスト用情報を選択する。	予引に関連記載あり	8.33.1	テスト結果の機密性及び関連する運用情報の機密性を確実にするよう、テスト用情報を選択する。 取扱いに慎重を要する情報（PII等含む。）を、開発環境及びテスト環境へ複製しない（8.31参照）。	
14.3.1.2	PII 又はその他の秘密情報を試験目的で用いる場合には、取扱いに慎重を要する詳細な記述及び内容の全てを、消去又は改変することによって保護する。	8d-8.33.3	運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の事項を適用する。 d) テストに使用する場合、取扱いに慎重を要する情報は、削除又はスキンク化によって保護する。	予引に関連記載あり	8.33.2	テスト用情報はセキュリティに配慮して保存し、使用する。	運用情報の複製をテスト目的で用いる場合には、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の管理策を適用する。 a) 運用環境に適用するのと同じアクセス制御手順をテスト環境に適用する。 b) 運用情報の複製をテスト環境に置く場合は、その都度認可を受ける。 c) 運用情報の複製及び利用は、監査証跡とするためにログをとる。 d) テストに使用する場合、取扱いに慎重を要する情報は、削除又はスキンク（8.11参照）によって保護する。 e) テスト用情報の認可されていない使用を防止するために、テストの完了直後にテスト環境から運用情報を速やかに削除（8.10参照）する。 テスト用情報は、セキュリティに配慮して保存し（脆薬を無効にする可能性がある改ざんを防止するため）、テスト目的でだけ使用する。
14.3.1.3	運用データを試験目的で用いる場合は、運用アプリケーションシステムに適用されるアクセス制御手順を、試験アプリケーションシステムにも適用する。	8d-8.33.3	運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の管理策を適用する。 a) 運用環境に適用するのと同じアクセス制御手順をテスト環境に適用する。	予引に関連記載あり			
14.3.1.4	運用情報を試験環境に二次一する場合は、その都度認可を受ける。	8d-8.33.3	運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の管理策を適用する。 b) 運用情報の複製をテスト環境に置く場合は、その都度認可を受ける。	予引に関連記載あり			
14.3.1.5	運用データを試験目的で用いる場合は、運用情報は、試験が完了した後直ちに試験環境から消去する。	8d-8.33.3	運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の管理策を適用する。 e) テスト用情報の認可されていない使用を防止するために、テストの完了直後にテスト環境から運用情報を速やに削除する。	予引に関連記載あり			
14.3.1.6	運用データを試験目的で用いる場合には、運用情報の複製及び利用は、監査証跡とするためにログを取得する。	8d-8.33.3	運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の管理策を適用する。 c) 運用情報の複製及び利用は、監査証跡とするためにログをとる。	予引に関連記載あり			
15	供給者関係	5.19	供給者関係における情報セキュリティ 管理策 供給者の製品又はサービスの利用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施する。 目的 供給者関係において合意したレベルの情報セキュリティを維持するため。		5.19	供給者関係における情報セキュリティ 統制目標：供給者の製品又はサービスの利用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施する。 目的：供給者関係において合意したレベルの情報セキュリティを維持するため。	
15.1	供給者関係における情報セキュリティ 管理目的：供給者がアクセスできる組織の資産の保護を確実にするため。						
15.1.1	供給者関係のための情報セキュリティの方針 組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化する。						
15.1.1.1	組織は、供給者による組織の情報へのアクセスに具体的に対処するため、方針において情報セキュリティ管理策を特定し、義務付ける。	5d-5.19.1	組織は、供給者関係に関するトピック固有の方針を確立し、関連する全ての利害関係者に伝達する。	管理策に関連記載あり	5.19.1	供給者の製品又はサービスの利用に関連する方針を策定し、関連する全ての利害関係者に伝達する。	特になし。
15.1.1.2	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、組織が、自らの情報へのアクセスを許可する供給者の種類（例えば、IT サービス、物流サービス、金融サービス、IT 基盤の構成要素などの供給者）の特定及び文書化を含める。	5d-5.19.2	組織は、供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するためのプロセス及び手順を特定し、実施する。	予引に関連記載あり	5.19.2	供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するためのプロセス及び手順を整備し、実施する。	組織は、供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するために、次を行う。 供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するための方法及び手順は、組織の調達ライフサイクル・プロセスから供給者の利用に当たり適用する。 供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するための方法及び手順は、組織の調達ライフサイクル・プロセスから供給者の利用に当たり適用する。 a) 供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するための方法及び手順は、組織が実施する、自らの供給者の種類（例えば、ICT サービス、物流、公金事業、金融サービス、ICT 基盤の構成要素）の特定及び文書化。 b) 情報、製品及びサービスの取扱いに慎重を要する程度を与える可能性のある供給者の種類（例えば、セクター（ら、物流、公金事業、金融サービス、ICT 基盤の構成要素）の特定及び文書化。 c) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 d) 供給者の情報へのアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化する。 e) 組織が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 f) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 g) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 h) 供給者の情報へのアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化する。 i) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 j) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 k) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 l) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 m) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 n) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 o) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 p) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 q) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 r) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 s) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 t) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 u) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 v) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 w) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 x) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 y) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 z) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 aa) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ab) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ac) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ad) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ae) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 af) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ag) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ah) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ai) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 aj) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ak) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 al) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 am) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 an) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ao) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ap) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 aq) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ar) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 as) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 at) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 au) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 av) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 aw) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ax) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ay) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 az) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ba) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bb) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bc) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bd) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 be) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bf) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bg) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bh) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bi) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bj) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bk) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bl) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bm) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bn) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bo) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bp) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bq) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 br) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bs) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bt) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bu) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bv) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bw) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bx) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 by) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 bz) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ca) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cb) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cc) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cd) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ce) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cf) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cg) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ch) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ci) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cj) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ck) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cl) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cm) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cn) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 co) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cp) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cq) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cr) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cs) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ct) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cu) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cv) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cw) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cx) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cy) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 cz) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 da) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 db) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dc) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dd) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 de) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 df) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dg) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dh) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 di) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dj) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dk) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dl) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dm) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dn) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 do) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dp) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dq) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dr) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ds) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dt) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 du) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dv) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dw) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dx) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dy) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 dz) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ea) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 eb) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ec) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ed) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ee) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ef) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 eg) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 eh) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ei) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ej) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ek) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 el) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 em) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 en) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 eo) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ep) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 eq) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 er) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 es) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 et) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 eu) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ev) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ew) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ex) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ey) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 ez) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 fa) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択するための方法の確立及び適用。 fb) 供給者が提供する製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
15.1.1.5	組織が実施する、部(仁)組織が供給者に対して実施を要求するプロセス及び手順には、情報の種類及びアクセスの種類ごとの最低限の情報セキュリティ要求事項で、組織の事業上のニーズ及び要求事項並びに組織のリスクアプローチに基づく供給者との個々の合意の締結となるのを含める。	(Sd-S.20.1参考)	特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。 h) 供給者のCOTI基盤に関する情報セキュリティ要求事項。特に、組織の事業上のニーズ及び(リスク)基準に基づき、個々の供給者との合意の締結となる。情報の種類及びアクセスの種類それぞれについての最小限の情報セキュリティ要求事項	手引に関連記載あり	S.20.1	供給者関係の種類に応じて、関連する情報セキュリティ要求事項を定義し、供給者と合意する。	関連する情報セキュリティ要求事項を満たすために、供給者との合意を確立し、実施することが望ましい。供給者との合意には、次の事項を含めることが望ましい。 特定された情報セキュリティ要求事項に関連付ける。合意には、次の事項を含めることを考慮することが可能である。 a) 説明、及び(アクセスの)許諾の記載。及び提供のルール(アクセスのルールの記載 b) 組織から供給者に対する開示の要件（5.10、5.12及び5.13参照） c) 供給者の情報及び供給者の活動を含むリスクの対応付け d) 法令、規制及び契約上の要求事項（データ保護、個人識別可能情報（PII）の取扱い、知的財産権の譲渡権に関する要求事項含む。）、並びにこれらの要求事項を満たすことを確実にするための方法についての記載 e) 契約の各事項に対する、合意した一連の管理策（アセスに関連、パフォーマンスのレビュー、監視、報告(又は)監査含む）、の実施の義務、及び供給者に対する義務の割当 f) 情報及びその他の関連資産の許容される利用に関する規則。必要な場合、許容されない利用についての規則も含める。 g) 供給者の要求による組織の情報及びその他の関連資産の使用を認可する権限及びその認可を解除する場合の手順又は条件 h) 供給者の(又は)組織に対する、合意した一連の管理策（アセスに関連、パフォーマンスのレビュー、監視、報告(又は)監査含む）、の実施の義務、及び供給者に対する義務の割当 i) 情報及びその他の関連資産の取扱いに使用が許されるもの j) 供給者のCOTI基盤の情報セキュリティ要求事項について、特に、組織の事業上のニーズ及び(リスク)基準に基づき、個々の供給者との合意の締結となる。情報の種類及びアクセスの種類それぞれについての最小限の情報セキュリティ要求事項 k) 供給者の要求による組織の情報及びその他の関連資産の使用を認可する権限及びその認可を解除する場合の手順又は条件（例えば、供給者の(又は)組織に対する、合意した一連の管理策（アセスに関連、パフォーマンスのレビュー、監視、報告(又は)監査含む）、の実施の義務、及び供給者に対する義務の割当 l) 情報及びその他の関連資産の取扱いに使用が許されるもの m) 供給者のCOTI基盤の情報セキュリティ要求事項について、特に、組織の事業上のニーズ及び(リスク)基準に基づき、個々の供給者との合意の締結となる。情報の種類及びアクセスの種類それぞれについての最小限の情報セキュリティ要求事項 n) 情報セキュリティに関する連絡先担当者との、関連する連絡先 o) 特定の手順(又は)情報セキュリティ要求事項について、合意した一連の管理策（例えば、インシデントの対応手順、認可手順） p) 下請負者組織の使用に関する合意(又)、実施する必要がある(又)管理策のあり、下請負者(又)に関する(又)特定の義務、及び(又)特定の(又)それらの(又)下請負者(又)の(又)それらの(又)(又)(又)

番号	（旧）管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	（新）管理策基準	（参考）手引き
I5.1.2.18.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	5.20.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
I5.1.3	ICTサプライチェーン 供給者との合意には、情報通信技術（以下「ICT」という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含める。	S.21	ICTサプライチェーンにおける情報セキュリティの管理 管理策 ICT製品及びサービスのサプライチェーンに関連する情報セキュリティリスクを管理するための方法及び手順を定め、実施する。 目的 供給者関係において合意したレベルの情報セキュリティを維持するため。		S.21	ICTサプライチェーンにおける情報セキュリティの管理 統制目標：ICT製品及びサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施する。 目的：供給者関係において合意したレベルの情報セキュリティを維持するため。	
I5.1.3.1	供給者との合意には、供給者関係に関する一般的な情報セキュリティ要求事項のほかに、ICT 製品又はサービスの取得に適用する情報セキュリティ要求事項を定めることを含める。	Sd-S.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 a) ICT 製品及びサービスの取得に適用する情報セキュリティ要求事項を定める。	手引に関連記載あり	S.21.1	【再】ICT製品及びサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセス及び手順を整備し、実施する。	（S.21.1に対応する項を参照）
I5.1.3.2	供給者との合意には、ICT サービスに関して、供給者が組織に提供するICT サービスの一部を下請負契約にお て場合には、そのサプライチェーン全体に組織のセキュリティ要求事項を伝達するよう供給者に要求することを含める。	Sd-S.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 b) 供給者が組織に提供するICTサービスの一部を下請負契約に出す場合には、そのサプライチェーン全体に組織のセキュリティ要求事項を伝達するようにICTサービスの供給者に要求する。	手引に関連記載あり			
I5.1.3.3	供給者との合意には、ICT 製品に関して、その製品に他の供給者から購入した構成部品が含まれる場合には、そのサプライチェーン全体に適切なセキュリティ慣行を伝達するよう供給者に要求することを含める。	Sd-S.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 c) ICT 製品に関して、その製品に他の供給者又は他のエンティティから購入した構成要素が含まれる場合には、そのサプライチェーン全体に適切なセキュリティ慣行を伝達するようにICT製品の供給者に要求する。	手引に関連記載あり			
I5.1.3.4	供給者との合意には、提供された ICT 製品及びサービスが規定のセキュリティ要求事項を順守していることを確認するための、監視プロセス及び許容可能な監視方法を実施することを含める。	Sd-S.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 f) 提供されたICT製品及びサービスが規定のセキュリティ要求事項を順守していることを確認するため、監視プロセス及び許容可能な監視方法を実施する。このような供給者レビュー方法の例に侵入テスト、及び供給者の情報セキュリティ運用に関する独立者立証の検証又は妥当性確認がある。	手引に関連記載あり			
I5.1.3.5	特に、直接の供給者が製品又はサービスの構成要素を他の供給者に外部委託する場合（製品又はサービスの機能を維持するために重要な構成要素に対しては、組織の外で作られる場合に注意及び精査の強化が求められるため）、供給者との合意には、重要な構成要素を特定するためのプロセスを実施することを含める。	Sd-S.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 g) 製品又はサービスの機能を維持するために重要な構成要素を特定し、文書化するプロセスを実施する。重要な構成要素に対しては、組織の外で作られる場合に必要とされる注意、精査及び更なるフォローアップの強化が求められる（特に、供給者が製品又はサービスの構成要素を他の供給者に外部委託する場合。）。	手引に関連記載あり			
I5.1.3.6	供給者との合意には、重要な構成要素及びその供給元が、サプライチェーン全体を通じて追跡可能であるという保証を得ることを含める。	Sd-S.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 h) 重要な構成要素及びその供給元が、サプライチェーン全体を通じて追跡可能であるという保証を得る。	手引に関連記載あり			
I5.1.3.7	供給者との合意には、提供される ICT 製品が期待どおりに機能し、予期しない又は好ましくない特性をもたらないという保証を得ることを含める。	Sd-S.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 i) 提供される ICT 製品が期待どおりに機能し、予期しない又は好ましくない特性をもたらないという保証を得る。	手引に関連記載あり			
I5.1.3.8	供給者との合意には、サプライチェーンについての情報、並びに組織と供給者との間で生じる可能性のある問題及び妥協についての情報を共有するための規則を定めることを含める。	Sd-S.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 j) サプライチェーンについての情報、並びに組織と供給者との間で生じる可能性のある問題及び妥協についての情報を共有するための規則を定める。	手引に関連記載あり			
I5.1.3.9	供給者との合意には、ICT 構成要素のライフサイクル及び陳腐化の管理、並びにこれに関連するセキュリティリスクを管理するための具体的なプロセスを実施することを含める。このプロセスには、その構成要素が入手できなくなる（供給者が事業を営まなくなる、又は技術進歩によって供給者がその構成要素を提供しなくなる）というリスクを管理することも含める。	Sd-S.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 m) ICT 構成要素のライフサイクル及び陳腐化の管理、並びにこれに関連するセキュリティリスクを管理するための具体的なプロセスを実施する。このプロセスには、その構成要素が入手できなくなる（供給者が事業を営まなくなる、又は技術進歩によって供給者がその構成要素を提供しなくなる）というリスクを管理することも含まれる。代替供給者の特定、並びにソフトウェア及び力量を代替供給者に移転するプロセスを検討する。	手引に関連記載あり			
–	（対応項なし）	Sd-S.21.1	供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。 d) ICT 製品の供給者に、製品で使用しているソフトウェア構成要素を記載した情報を提供するよう要求する。 e) ICT 製品の供給者に、自らの製品が実装するセキュリティ機能及びそのセキュリティに配慮した運用に必要な構成を説明する情報を提供するよう要求する。 i) 供給者からの構成要素が真正のものであり、その仕様から変更されていないことを確実にするためのプロセスを実施する。対策の例に、改ざん防止テープ、暗号パッシ機能又はデジタル署名がある。仕様外の動作を監視することが、改ざん又は偽造を見つける可能性がある。改ざんの防止及び検知は、設計、開発、統合、運用及び保守を含むシステム開発ライフサイクルの複数の段階で実施する。 k) ICT製品が、例えば、正式な認証又は共通基準承認アレンジメント（Common Criteria Recognition Arrangement）などの評価体系を通じて、必要なセキュリティレベルを達成していることの保証を得る。	手引に関連記載あり			
I5.1.3.10.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	S.21.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
I5.1.3.11.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	S.21.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
I5.2 I5.2.1	供給者のサービス提供の管理 管理目的：供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。 供給者のサービス提供の監視及びレビュー 組織は、供給者のサービス提供を定期的に監視し、レビュー、監査する。	S.22	供給者のサービス提供の監視、レビュー及び変更管理 管理策 組織は、供給者の情報セキュリティの活動及びサービス提供を定期的に監視し、レビュー、評価し、変更を管理する。 目的 供給者との合意に沿って、合意したレベルの情報セキュリティ及びサービス提供を維持するため。		S.22	供給者のサービス提供の監視、レビュー及び変更管理 統制目標：組織は、供給者の情報セキュリティの活動及びサービス提供を定期的に監視し、レビュー、評価し、変更を管理する。 目的：供給者との合意に沿って、合意したレベルの情報セキュリティ及びサービス提供を維持するため。	
I5.2.1.1	供給者のサービスを監視及びレビューすることによって、その合意における情報セキュリティの条件の順守、並びに情報セキュリティのインシデント及び問題の適切な管理を確実にする仕組みを整備する。	Sd-S.22.1	供給者のサービスを監視し、レビューし、変更管理することによって、次の点を確実にする。 a) 合意における情報セキュリティの条件の順守	手引に関連記載あり	S.22.1	供給者の情報セキュリティの活動及びサービス提供を監視し、レビューし、変更を管理する。	供給者のサービスを監視し、レビューし、変更管理することによって、次の点を確実にする。 a) 合意における情報セキュリティの条件の順守 b) 情報セキュリティインシデント及び問題の適切な管理 c) 供給者のサービスの変更又は事業状況の変化がサービス提供に影響を与えないこと 供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理する方法とする点も含む。
I5.2.1.1	【再】供給者のサービスを監視及びレビューすることによって、その合意における情報セキュリティの条件の順守、並びに情報セキュリティのインシデント及び問題の適切な管理を確実にする仕組みを整備する。	Sd-S.22.1	供給者のサービスを監視し、レビューし、変更管理することによって、次の点を確実にする。 b) 情報セキュリティのインシデント及び問題の適切な管理	手引に関連記載あり			
–	（対応項なし）	Sd-S.22.1	供給者のサービスを監視し、レビューし、変更管理することによって、次の点を確実にする。 c) 供給者のサービスの変更又は事業状況の変化がサービス提供に影響を与えないこと	手引に関連記載あり			
I5.2.1.2	供給者のサービスの監視及びレビューは、合意の順守を検証するために、サービスのパフォーマンスレベルを監視するこを含める。	Sd-S.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 a) 合意の順守を検証するために、サービスのパフォーマンスレベルを監視する。	手引に関連記載あり			a) 合意における情報セキュリティの条件の順守 b) 情報セキュリティインシデント及び問題の適切な管理 c) 供給者のサービスの変更又は事業状況の変化がサービス提供に影響を与えないこと 供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理する方法とする点も含む。 a) 合意の順守を検証するために、サービスのパフォーマンスレベルを監視する。 b) 次の事項を含む供給者によるサービスの変更を監視する。 1) 現在提供されているサービスの強化 2) 新しいアプリケーション及びシステムの開発 3) 組織の諸方針及び諸手順の、変更又は更新 4) 情報セキュリティインシデントの解決及び情報セキュリティの改善のため、新たな又は変更した管理策 c) 次の事項を含む供給者サービスの変更を監視する。 1) ネットワークの変更及び強化 2) 新技術の利用 3) 新製品又は新しい版若しくはリリースの採用 4) 新たな開発ツール及び開発環境 5) サービス設備の物理的設置場所の変更 6) 下請負供給者の変更 7) 他の供給者への下請負契約 d) 供給者の作成したサービスの報告をレビュー、合意で求めている定期的な進捗会議を設定する。 e) 独立した監査人の報告書が入手できれば、これのレビュー併せて供給者及び下請負供給者の監査を実施し、特定された問題の追跡調査を行う。 f) 合意書並びに全ての例掲の個別及び手順書の要求に従い、情報セキュリティインテントの情報を提供し、その情報をレビューする。 g) 供給者の監査証跡、情報セキュリティ事象の記録、運用上の問題の記録、故障記録、障害履歴及び提供サービスに関連する事象の中断・阻害の記録をレビューする。 h) 特定された情報セキュリティ事象又はインシデントに対応し、管理する。 i) 情報セキュリティの忙・弱性を特定し、管理する。 j) 供給者とその供給者と介護の供給者関係における情報セキュリティの側面をレビューする。 k) 供給者が、十分なサービス提供能力を維持すること、及び重大なサービスの不具合又は災害の場においても合意したサービス継続レベルが維持されることを確実にするように設計された実行可能な計画を維持することを確実にする（S.29、S.30、S.35、S.36及びI5.14参照）。 l) 供給者が、順守をレビュー、合意の要求事項を実施する責任を割り当てることを確実にする。 m) 供給者が適切な情報セキュリティレベルを維持していることを定期的に評価する。
I5.2.1.3	供給者のサービスの監視及びレビューは、供給者の作成したサービスの報告をレビュー、合意で求めている定期的な進捗会議を設定することを含める。	Sd-S.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 d) 供給者の作成したサービスの報告をレビュー、合意で求めている定期的な進捗会議を設定する。	手引に関連記載あり			
I5.2.1.4	供給者のサービスの監視及びレビューは、独立した監査人の報告書が入手できれば、供給者の作成したサービスの報告のレビューと併せて供給者の監査を実施し、特定された問題の追跡調査を行うことを含める。	Sd-S.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 e) 独立した監査人の報告書が入手できれば、これのレビュー併せて供給者及び下請負供給者の監査を実施し、特定された問題の追跡調査を行う。	手引に関連記載あり			
I5.2.1.5	供給者のサービスの監視及びレビューは、合意書並びに全ての例掲の個別及び手順書の要求に従い、情報セキュリティインテントの情報を提供し、その情報をレビューすることを含める。	Sd-S.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 f) 合意書並びに全ての例掲の個別及び手順書の要求に従い、情報セキュリティインテントの情報を提供し、その情報をレビューする。	手引に関連記載あり			
I5.2.1.6	供給者のサービスの監視及びレビューは、供給者の監査証跡、情報セキュリティ事象の記録、運用上の問題の記録、故障記録、障害履歴及び提供サービスに関連する中断記録をレビューすることを含める。	Sd-S.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 g) 供給者の監査証跡、情報セキュリティ事象の記録、運用上の問題の記録、故障記録、障害履歴及び提供サービスに関連する事象の中断・阻害の記録をレビューする。	手引に関連記載あり			
I5.2.1.7	供給者のサービスの監視及びレビューは、特定された問題の解決及び管理を実施することを含める。	Sd-S.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 h) 特定された情報セキュリティ事象又はインシデントに対応し、管理する。	手引に関連記載あり			
I5.2.1.8	供給者のサービスの監視及びレビューは、供給者との供給者との間の供給者関係における情報セキュリティの側面をレビューすることを含める。	Sd-S.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 i) 供給者との供給者との間の供給者関係における情報セキュリティの側面をレビューする。	手引に関連記載あり			
I5.2.1.9	供給者のサービスの監視及びレビューは、重大なサービスの不具合又は災害の後においても、合意したサービス継続レベルが維持されることを確実にするように設計された実行可能な計画とともに、供給者が十分なサービス提供能力を維持することを確実にすることを含める。	Sd-S.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 k) 供給者が、十分なサービス提供能力を維持すること、及び重大なサービスの不具合又は災害の後においても合意したサービス継続レベルが維持されることを確実にするように設計された実行可能な計画を維持する。	手引に関連記載あり			
I5.2.1.10	供給者関係を管理する責任は、指定された個人又はサービス管理チームに割り当てる。	Sd-S.22.3	供給者関係を管理する責任は、指定された個人又はチームに割り当てる。	管理策に関連記載あり	S.22.2	供給者関係を管理及び監視する責任は、指定された個人又はチームに割り当て、監視するために十分な技術力及び人的資源を確保する。	供給者関係を管理する責任は、指定された個人又はチームに割り当てる。 合意書における要求事項、特に情報セキュリティに関する要求事項を満たしているかどうかを監視するために、十分な技術力及び人的資源を確保しておく。 サービスの提供において不完全な点があった場合は、適切な処置をとる。
I5.2.1.11	組織は、供給者が、順守状況のレビュー及び合意書における要求事項の実施について責任を割り当てる。	Sd-S.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 l) 供給者が、順守をレビューし、合意の要求事項を実施する責任を割り当てる。	手引に関連記載あり	S.22.1	【再】供給者の情報セキュリティの活動及びサービス提供を監視し、レビューし、変更を管理する。	（S.22.1に対応する項を参照）
I5.2.1.12	組織は、合意書における要求事項、特に情報セキュリティに関する要求事項を満たしているかどうかを監視するために、十分な技術力及び人的資源を確保する。	Sd-S.22.4	合意書における要求事項、特に情報セキュリティに関する要求事項を満たしているかどうかを監視するために、十分な技術力及び人的資源を確保しておく。	管理策に関連記載あり	S.22.2	【再】供給者関係を管理及び監視する責任は、指定された個人又はチームに割り当て、監視するために十分な技術力及び人的資源を確保する。	（S.22.2に対応する項を参照）
I5.2.1.13	組織は、サービスの提供において不完全な点があった場合に適切な処置をとる。	Sd-S.22.5	サービスの提供において不完全な点があった場合は、適切な処置をとる。	手引に関連記載あり			
I5.2.1.14	組織は、供給者がプロセス、処理又は管理する、脆弱に情報を保するICは重要な情報・情報処理設備に対して、全てのセキュリティの側面についての十分かつ包括的な管理及び可視性を維持する。	–	（追加対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で規承されず）	–	（対応項なし）	–
I5.2.1.15	組織は、報告プロセスを規定することで、セキュリティに関連した活動（例えば、変更管理、ぜい弱性識別、情報セキュリティインシデントの報告及び対応）の可視性を維持する。	Sd-S.22.1	【再】供給者のサービスを監視し、レビューし、変更管理することによって、次の点を確実にする。 b) 情報セキュリティのインシデント及び問題の適切な管理	手引に関連記載あり	S.22.1	【再】供給者の情報セキュリティの活動及びサービス提供を監視し、レビューし、変更を管理する。	（S.22.1に対応する項を参照）

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
15.2.2	供給者のサービス提供の変更に対する管理 関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む）を管理する。	5.22	供給者のサービス提供の監視、レビュー及び変更 管理策 組織は、供給者の情報セキュリティの活動及びサービス提供を定常的に監視し、レビュー、評価し、変更を管理する。 目的 供給者との合意に沿って、合意したレベルの情報セキュリティ及びサービス提供を維持するため。		5.22	供給者のサービス提供の監視、レビュー及び変更管理 統制目標：組織は、供給者の情報セキュリティの活動及びサービス提供を定常的に監視し、レビュー、評価し、変更を管理する。 目的：供給者との合意に沿って、合意したレベルの情報セキュリティ及びサービス提供を維持するため。	
15.2.2.1	供給者のサービス提供の変更に対する管理は、供給者との合意に対する変更を考慮して実施する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし （情報セキュリティ管理基準と組み合わ	–	（対応項なし）	–
15.2.2.2	供給者のサービス提供の変更に対する管理は、以下の4点を実施するために組織が行う変更を考慮して実施する。 1.現在提供されているサービスの強化 2.新しいアプリケーション及びシステムの開発 3.組織の諸方針及び諸手順の、変更又は更新 4.情報セキュリティインシデントの解決及びセキュリティの改善のため、新たな又は変更した管理策	Sd-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 b）次の事項を含め供給者による変更を監視する。 1）現在提供されているサービスの強化 2）新しいアプリケーション及びシステムの開発 3）組織の諸方針及び諸手順の、変更又は更新 4）情報セキュリティインシデントの解決及び情報セキュリティの改善のため、新たな又は変更した管理策	手引に関連記載あり	5.22.1	【再】供給者の情報セキュリティの活動及びサービス提供を監視、レビュー、変更を管理する。	（5.22.1に対応する項を参照）
15.2.2.3	供給者のサービス提供の変更に対する管理は、以下の7点を実施するための供給者サービスにおける変更を考慮して実施する。 1.ネットワークに対する変更及び強化 2.新技術の利用 3.新製品又は新しい版・リリースの採用 4.新たな開発ツール及び開発環境 5.サービス設備の物理的設置場所の変更 6.供給者の変更 7.他の供給者への下請負契約	Sd-5.22.2	供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。 c）次の事項を含め供給者サービスの変更を監視する。 1）ネットワークの変更及び強化 2）新技術の利用 3）新製品又は新しい版若しくはリリースの採用 4）新たな開発ツール及び開発環境 5）サービス設備の物理的設置場所の変更 6）下請負供給者の変更 7）他の供給者への下請負契約	手引に関連記載あり			
16	情報セキュリティインシデント管理	5.24	情報セキュリティインシデント管理の計画策定及び準備 管理策 組織は、情報セキュリティインシデント管理のプロセス、役割及び責任を定め、確立し、伝達することによって、情報セキュリティインシデント管理を計画し、準備する。 目的 情報セキュリティ事象に関する伝達を含め、情報セキュリティインシデントへの迅速で、効果的で、一貫性が有り、かつ、秩序のある対応を確実にするため。		5.24	情報セキュリティインシデント管理の計画策定及び準備 統制目標：組織は、情報セキュリティインシデント管理のプロセス、役割及び責任を定め、確立し、伝達することによって、情報セキュリティインシデント管理を計画し、準備する。 目的：情報セキュリティ事象に関する伝達を含め、情報セキュリティインシデントへの迅速で、効果的で、一貫性が有り、かつ、秩序のある対応を確実にするため。	
16.1	情報セキュリティインシデントの管理及びその改善 管理目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含め、情報セキュリティインシデントの管理のため の、一貫性のある効果的な取組みを確実にするため。						
16.1.1	責任及び手順 情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理策の責任及び手順を確立する。						
16.1.1.1	情報セキュリティインシデント管理に関する管理策の責任及び手順について、組織において、以下の7点の手順が策定され、十分に伝達されることを確実にするために、管理策の責任を確立する。 1.インシデント対応の計画及び準備のための手順 2.情報セキュリティ事象及び情報セキュリティインシデントを監視、検知、分析及び報告するための手順 3.インシデント管理活動のログを取得するための手順 4.法的証拠を提出するための手順 5.情報セキュリティ事象の評価及び決定のための手順、並びに情報セキュリティ弱点の評価のための手順 6.対応手順（段階的取扱い、インデントからの回復の管理、並びに内部及び外部の要員 又は組織への連絡、報告、指示の伝達のための手順を含む。） 7.内部及び外部の要員 又は組織への指示に関する対応手順には、定めた時間内での指示の履行又は指示の発行元への不履行の程度の通知を含む。	Se-5.24.7	経営陣は、次の活動のためにそれぞれのシナリオ及び手順が作成され、実施されていることを考慮して、情報セキュリティインシデント管理計画の作成を確実にする。 a）何が情報セキュリティインシデントに該当するかに関する基準に従った情報セキュリティ事象の評価 b）情報セキュリティ事象及び情報セキュリティインシデントの監視、検知、分類、分析及び報告 c）インシデントの種類及び カテゴリに従った、対応及びエスカレーション、危機管理の発動及び継続計画の発動の可能性、インシデントからの管理された回復、並びに内部及び外部の利害関係者への伝達を含む、情報セキュリティインシデントの終結までの管理 d）関係当局、外部の利益団体及び会議、供給者、顧客など、内部及び外部の利害関係者との調整 e）インシデント管理活動のログ取得 f）証拠の取扱い g）根本原因分析又は事後分析手順 h）学んだ教訓及びインシデント管理手順又は一般的な情報セキュリティ管理策についての必要な改善の特定	手引に関連記載あり	5.24.1	情報セキュリティインシデント管理プロセスを整備する。	組織は、適切な情報セキュリティインシデント管理プロセスを確立する。 情報セキュリティインシデント管理プロセスを確立するに際には、次の事項を考慮する。 a）連絡先を含む、情報セキュリティ事象を報告するための共通の方法を確立する（6.8参照）。 b）監視、文書化、検知、トリアージ、優先順位付け、分析、伝達及び判断関係者の調整を含む、組織が情報セキュリティインシデントを管理する機能を備えるためのインシデント管理プロセスを確立する。 c）情報セキュリティインシデントを評価し、それに対応し、そこから学習する機能を組織が備えるためのインシデント対応プロセスを確立する。 d）組織内で、情報セキュリティインシデントに関連する事項と、力量のある要員だけが取り扱えるようにする。要員には、文書化した手順及び定期的な訓練を提供する。 e）インシデントに対応する要員に必要な訓練、認証及び継続的な専門能力開発を特定するプロセスを確立する。
–	（対応項なし）	Se-5.24.6	これらの目的及び優先順位を満たすようにインシデント管理手順を実施する。	手引に関連記載あり			
–	（対応項なし）	Se-5.24.2	インシデント管理手順を実行するための役割及び責任を決定し、関連する内部及び外部の利害関係者に効果的に伝達する。	手引に関連記載あり	5.24.2	情報セキュリティインシデント管理手順を実行するための役割及び責任を決定し、関連する内部及び外部の利害関係者に伝達する。	情報セキュリティインシデント管理手順を実行するための役割及び責任を決定し、関連する内部及び外部の利害関係者に伝達する。 クラウドサービス利用者と情報セキュリティインシデント管理の責任の割当て及び手順を定める。
–	（対応項なし）	Se-5.24.1	組織は、適切な情報セキュリティインシデント管理プロセスを確立する。	管理策に関連記載あり	5.24.1	【再】情報セキュリティインシデント管理プロセスを整備する。	（5.24.1に対応する項を参照）
16.1.1.2	情報セキュリティインシデント管理に関する管理策の責任及び手順について、確立する手順においては、以下の4点を確実にする。 1.組織内の情報セキュリティに関連する事項は、力量のある要員が取り扱う。 2.セキュリティインシデントの対応と報告に関する助言と支援を提供する。 3.セキュリティインシデントを検知及び報告する場合の連絡先を定める。 4.情報セキュリティインシデントに関連した事項を取り扱う関係当局、外部の利益団体又は会議との適切な連絡（顧客、動画、指示を含む。）を保つ。	Se-5.24.3	情報セキュリティインシデント管理プロセスを確立する際には、次の事項を考慮する。 a）連絡先を含む、情報セキュリティ事象を報告するための共通の方法を確立する。 b）監視、文書化、検知、トリアージ、優先順位付け、分析、伝達及び判断関係者の調整を含む、組織が情報セキュリティインシデントを管理する機能を備えるためのインシデント管理プロセスを確立する。 c）情報セキュリティインシデントを評価し、それに対応し、そこから学習する機能を組織が備えるためのインシデント対応プロセスを確立する。 d）組織内で、情報セキュリティインシデントに関連する事項と、力量のある要員だけが取り扱えるようにする。そうした要員には、文書化した手順及び定期的な訓練を提供する。 e）インシデントに対応する要員に必要な訓練、認証及び継続的な専門能力開発を特定するプロセスを確立する。	手引に関連記載あり			
16.1.1.3	情報セキュリティインシデント管理に関する管理策の責任及び手順について、報告手順においては、以下の4点を含める。 1.情報セキュリティ事象が発生した場合に、報告が事前に取り、報告する者が必要な全ての処置を忘れないよう手助けするための情報セキュリティ事象の報告書式の作成 2.情報セキュリティ事象が発生した場合に取るべき手順、例えば、詳細全て（不順守又は違反の形態、生じた誤動作、画面上の表示など）の記録を含むこと、並びに連絡先に報告し、協調した処置だけをとる 3.セキュリティ違反を犯した従業員を処罰するために確立された正式な懲戒手続への言及 4.情報セキュリティ事象の報告者に、その件の処理が終結した後で結果を知らせることを確実にするための適切なフィードバックの手続	Se-5.24.8	情報セキュリティ事象及び情報セキュリティインシデントの報告手順には、次の事項を含める。 a）情報セキュリティ事象が発生した場合ごとの処置 b）情報セキュリティインシデントを報告する際に要員が必要な全ての活動を実行できることを支援するための連絡先 c）情報セキュリティ事象の報告者に、その件が終結され、終結した後で、可能な限り結果を知らせることを確実にするための適切なフィードバックの手続 d）インシデント報告書の作成	手引に関連記載あり	5.24.4	情報セキュリティインシデントの報告手順を整備する。	情報セキュリティ事象及び情報セキュリティインシデントの報告手順には、次の事項を含める。 a）情報セキュリティ事象が発生した場合ごとの処置（例えば、生じた誤動作、画面上の表示など関連する詳細全てを含めに記録し、直ちに連絡先に報告し、協調した処置だけをとる。） b）情報セキュリティインシデントを報告する際に要員が必要な全ての活動を実行できることを支援するためのインシデント書式の使用 c）情報セキュリティ事象の報告者に、その件が終結され、終結した後で、可能な限り結果を知らせることを確実にするための適切なフィードバックの手続 d）インシデント報告書の作成 インシデント管理手順を実施する際は、関連する利害関係者へ定められた時間内にインシデント報告する外部の要求事項（例えば、規制当局への侵害通知の要求事項）も考慮する。
–	（対応項なし）	Se-5.24.9	インシデント管理手順を実施する際は、関連する利害関係者へ定められた時間内にインシデント報告する外部の要求事項を考慮する。	手引に関連記載あり			
16.1.1.4	情報セキュリティインシデント管理の目的について、経営陣の同意を得る。	Se-5.24.4	情報セキュリティインシデント管理の目的について、経営陣が同意している。	手引に関連記載あり	5.24.3	情報セキュリティ管理手順を整備する。	情報セキュリティインシデント管理の目的について、経営陣が同意している。 情報セキュリティインシデント管理について責任ある人々が、現在的な結果及び重大度に基づく解決の時間枠を含め、組織が決めた情報セキュリティインシデントの取扱いの優先順位を理解していることを確実にする。 これらの目的及び優先順位を満たすSCインシデント管理手順を実施する。 経営陣は、次の活動のためにそれぞれのシナリオ及び手順が作成され、実施されていることを考慮して、情報セキュリティインシデント管理計画の作成を確実にする。 a）何が情報セキュリティインシデントに該当するかに関する基準に従った情報セキュリティ事象の評価 b）情報セキュリティ事象及び情報セキュリティインシデントの監視（8.15及び8.16参照）、検知（8.16参照）、分類（5.25参照）、分析及び報告（6.8参照）（人間又は自動の手段によって） c）インシデントの種類及び カテゴリに従った、対応及びエスカレーション（5.26参照）、危機管理の発動及び継続計画の発動の可能性、インシデントからの管理された回復、並びに内部及び外部の利害関係者への伝達を含む、情報セキュリティインシデントの終結までの管理 d）関係当局、外部の利益団体及び会議、供給者、顧客など、内部及び外部の利害関係者との調整（5.5及び5.6参照） e）インシデント管理活動のログ取得 f）証拠の取扱い（5.28参照） g）根本原因分析又は事後分析手順 h）学んだ教訓及びインシデント管理手順又は一般的な情報セキュリティ管理策についての必要な改善の特定
16.1.1.5	情報セキュリティインシデント管理について責任ある人々に対し、組織が決めた情報セキュリティインシデントの取扱いの優先順位を確実に理解させる。	Se-5.24.5	情報セキュリティインシデント管理について責任ある人々が、潜在的な結果及び重大度に基づく解決の時間枠を含め、組織が決めた情報セキュリティインシデントの取扱いの優先順位を理解していることを確実にする。	手引に関連記載あり			
–	（対応項なし）	–	（統一基準由来）	令和7年度にて追加 （情報セキュリティ管理基準以外の由来）	5.24.5	組織は、CSIRT（Computer Security Incident Response Team）を整備し、その役割を明確化する。	CSIRTに属する職員等として専門的な知識又は適性を有する と認められる者を選任する。 その为組織内における情報セキュリティインシデントに対処するための責任者としてCSIRT責任者を置く。また、CSIRTの为業務統括及び外部との連携等を行う職員等及び役割を定める。 以下を例とする役割を 定める。 a）CSIRTは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行う。 b）CSIRTは、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、関係への通報・連絡等を行う。 c）CSIRTは、情報セキュリティインシデントに関する封じ込め、対応及びエスカレーション（5.26参照）、危機管理の発動及び継続計画の発動の可能性、インシデントからの管理された回復、並びに内部及び外部の利害関係者への伝達を含む、情報セキュリティインシデントの終結までの管理 d）CSIRTは、同様の情報セキュリティインシデント が別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システム の管理する情報システムセキュリティ責任 者へ検証を指示する。 e）CSIRTは、情報セキュリティインシデントに関する封じ込めの 段階を記録する。
16.1.1.6.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	手引に関連記載あり （情報セキュリティ管理基準以外の由来）	5.24.2	情報セキュリティインシデント管理手順を実行するための役割及び責任を決定し、関連する内部及び外部の利害関係者に伝達する。	情報セキュリティインシデント管理手順を実行するための役割及び責任を決定し、関連する内部及び外部の利害関係者に伝達する。 クラウドサービス利用者と情報セキュリティインシデント管理の責任の割当て及び手順を定める。
16.1.1.7.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）	5.24.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
16.1.1.8.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）			
16.1.1.9.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）			
16.1.1.10.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）			
16.1.1.11.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）			
16.1.1.12.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり （情報セキュリティ管理基準以外の由来）			
16.1.1.14	情報セキュリティインシデント管理を確実にするために、インシデント対応能力を定期的に確認し、インシデント対応の有効性を判断し、結果を文書化する。	–	（SP800-53由来）	明確な対応関係なし	–	（対応項なし）	–
16.1.1.15.P	クラウドサービス事業者は、クラウドサービス利用者が情報セキュリティインシデントに備え、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備するための情報を、当該利用者に提供する。	–	（統一基準由来）	明確な対応関係なし	–	（対応項なし）	–

番号	（旧）管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	（新）管理策基準	（参考）手引き
16.1.2	情報セキュリティ事象の報告 情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告する。	6.8	情報セキュリティ事象の報告 管理策 組織は、要員が発見した又は疑いをもった情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設ける。 目的 要員が特定する可能性がある情報セキュリティ事象を、時機を失せず、一貫性をもって効果的に報告することを支援するため。		6.8	情報セキュリティ事象の報告 統制目標：組織は、要員が発見した又は疑いをもった情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設ける。 目的：要員が特定する可能性がある情報セキュリティ事象を、時機を失せず、一貫性をもって効果的に報告することを支援するため。	
16.1.2.1	全ての従業員及び契約相手に、情報セキュリティ事象をできるだけ速やかに報告する責任のあることを認識させておく。	6a-6.8.1	情報セキュリティインシデントの影響を防止又は最小化するために、全ての要員及び利害者に、情報セキュリティ事象をできるだけ速やかに報告する責任のあることを認識させておく。	予兆に関連記載あり	6.8.1	全ての利害者に、情報セキュリティ事象をできるだけ速やかに報告する責任のあること、情報セキュリティ事象の報告手順及び情報セキュリティ事象を報告する連絡先を伝達する。	情報セキュリティインシデントの影響を防止又は最小化するために、全ての利害者に、情報セキュリティ事象をできるだけ速やかに報告する責任のあることを認識させておく。 全ての利害者に、情報セキュリティ事象の報告手順及び情報セキュリティ事象を報告する連絡先を認識させる。 報告の仕組みは、できるだけ簡単で使いやすく、いつでも利用できるものとする。 情報セキュリティ事象には、インシデント、違反及びけん信性を含める。 情報セキュリティ事象の報告を検討する状況には、次を含める。 a) 効果のない情報セキュリティ管理策 b) 情報の機密性、完全性又は可用性に関する期待に対する違反 c) ヒューマンエラー d) 情報セキュリティ方針、トピック固有の方針又は適用される標準の不順守 e) 物理的セキュリティ対策に対する違反 f) 変更管理プロセスを経ないシステム変更 g) ソフトウェア若しくはハードウェアの誤動作又はその他の異常なシステム挙動 h) アクセス違反 i) けん信性 j) マルウェア感染の疑い
16.1.2.2	全ての従業員及び契約相手に、情報セキュリティ事象の報告手順及び情報セキュリティ事象を報告する連絡先を認識させる。	6a-6.8.2	全ての要員及び利用者に、情報セキュリティ事象の報告手順及び情報セキュリティ事象を報告する連絡先を認識させる。	予兆に関連記載あり			
–	（対応漏なし）	6a-6.8.3	報告の仕組みは、できるだけ簡単で使いやすく、いつでも利用できるものとする。	予兆に関連記載あり			
–	（対応漏なし）	6a-6.8.4	情報セキュリティ事象には、インシデント、違反及びけん信性を含める。	予兆に関連記載あり			
16.1.2.3	情報セキュリティ事象の報告には、効果のないセキュリティ管理策を含める。	6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 a) 効果のない情報セキュリティ管理策	予兆に関連記載あり			
16.1.2.4	情報セキュリティ事象の報告には、情報の完全性、機密性又は可用性に関する期待に対する違反を含める。	6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 b) 情報の機密性、完全性又は可用性に関する期待に対する違反	予兆に関連記載あり			
16.1.2.5	情報セキュリティ事象の報告には、人による誤りを含める。	6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 c) ヒューマンエラー	予兆に関連記載あり			
16.1.2.6	情報セキュリティ事象の報告には、個別方針又は曖昧の不順守を含める。	6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 d) 情報セキュリティ方針、トピック固有の方針又は適用される標準の不順守	予兆に関連記載あり			
16.1.2.7	情報セキュリティ事象の報告には、物理的セキュリティの取決めに対する違反を含める。	6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 e) 物理的セキュリティ対策に対する違反	予兆に関連記載あり			
16.1.2.8	情報セキュリティ事象の報告には、管理されていないシステム変更を含める。	6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 f) 変更管理プロセスを経ないシステム変更	予兆に関連記載あり			
16.1.2.9	情報セキュリティ事象の報告には、ソフトウェア又はハードウェアの誤動作を含める。	6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 g) ソフトウェア若しくはハードウェアの誤動作又はその他の異常なシステム挙動	予兆に関連記載あり			
16.1.2.10	情報セキュリティ事象の報告には、アクセス違反を含める。	6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 h) アクセス違反	予兆に関連記載あり			
–	（対応漏なし）	6a-6.8.5	情報セキュリティ事象の報告を検討する状況には、次を含める。 i) けん信性 j) マルウェア感染の疑い	予兆に関連記載あり			
–	（対応漏なし）	6a-6.8.6	要員及び利用者に、疑いをもった情報セキュリティのけん信性の立証を試みないように要求する。	予兆に関連記載あり	6.8.2	全ての利害者に、疑いをもった情報セキュリティのけん信性の立証や検査を試みないように要求する。	全ての利害者に、疑いをもった情報セキュリティのけん信性の立証を試みないように要求する。けん信性を検査することは、システムの不正使用の立て見られる可能性があり、情報システム又はサービスに損傷を与える可能性がある。最終的に、検査した個人に法的責任が発生する可能性がある。
–	（対応漏なし）	（6a-6.8.6参考）	けん信性を検査することは、システムの不正使用の立てと見られる可能性があり、情報システム又はサービスに損傷を与える可能性がある。それはディジタル証拠を破損又は不明瞭にする可能性がある。最終的に、検査した個人に法的責任が発生する可能性がある。	予兆に関連記載あり			
16.1.2.11.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の出典）	6.8.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
16.1.2.12.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の出典）	6.8.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
16.1.2.13.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の出典）	6.8.5	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
16.1.3	情報セキュリティ弱点の報告 組織の情報システム及びサービスを利用する従業員及び契約相手に、システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は、どのようなものでも記録し、報告するように要求する。	6.8	情報セキュリティ事象の報告 管理策 組織は、要員が発見した又は疑いをもった情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設ける。 目的 要員が特定する可能性がある情報セキュリティ事象を、時機を失せず、一貫性をもって効果的に報告することを支援するため。		6.8	情報セキュリティ事象の報告 統制目標：組織は、要員が発見した又は疑いをもった情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設ける。 目的：要員が特定する可能性がある情報セキュリティ事象を、時機を失せず、一貫性をもって効果的に報告することを支援するため。	
16.1.3.1	全ての従業員及び契約相手は、情報セキュリティインシデントを防止するため、情報セキュリティ弱点をできるだけ速やかに連絡先に報告する。	6a-6.8.1	情報セキュリティインシデントの影響を防止又は最小化するために、全ての要員及び利害者に、情報セキュリティ事象をできるだけ速やかに報告する責任のあることを認識させておく。	予兆に関連記載あり	6.8.1	【再】全ての利害者に、情報セキュリティ事象をできるだけ速やかに報告する責任のあること、情報セキュリティ事象の報告手順及び情報セキュリティ事象を報告する連絡先を伝達する。	（6.8.1に対応する箇を参照）
16.1.3.2	情報セキュリティ弱点の報告の仕組みは、できるだけ簡単で使いやすく、いつでも利用できるようにする。	6a-6.8.3	報告の仕組みは、できるだけ簡単で使いやすく、いつでも利用できるものとする。	予兆に関連記載あり			
16.1.4	情報セキュリティ事象の評価及び決定 情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定する。	S.25	情報セキュリティ事象の評価及び決定 管理策 組織は情報セキュリティ事象を評価し、それらを情報セキュリティインシデントに分類するか否かを決定する。 目的 情報セキュリティ事象の効果的な分類及び優先順位付けを確実にするため。		S.25	情報セキュリティ事象の評価及び決定 統制目標：組織は情報セキュリティ事象を評価し、それらを情報セキュリティインシデントに分類するか否かを決定する。 目的：情報セキュリティ事象の効果的な分類及び優先順位付けを確実にするため。	
16.1.4.1	連絡先の者は、合意された情報セキュリティ事象-情報セキュリティインシデントの分類基準を用いて各情報セキュリティ事象を評価し、その事象を情報セキュリティインシデントに分類するか否かを決定する。	Se-S.25.1	インシデントの結果及び優先順位を特定するために、情報セキュリティインシデントの分類及び優先順位付けの体系について合意する。	予兆に関連記載あり	S.25.1	情報セキュリティインシデント対応を目的とする情報セキュリティ事象の分類及び優先順位付けの体系を定義する。	インシデントの結果及び優先順位を特定するために、情報セキュリティインシデントの分類及び優先順位付けの体系について合意する。 体系には、事象を情報セキュリティインシデントに分類する基準を含める。
16.1.4.2	評価及び決定の結果は、以後の参照及び検証のために詳細に記録する。	Se-S.25.5	評価及び決定の結果は、以後の参照及び検証のために詳細に記録しておく。	予兆に関連記載あり	S.25.2	情報セキュリティインシデントの分類及び優先順位付けの体系に基づき、情報セキュリティ事象を評価し、評価及び決定の結果を記録する。	連絡の窓口は、合意した体系を使用して、各情報セキュリティ事象を評価する。 情報セキュリティインシデントの調整及び対応に責任を負う要員は、評価を実行し、情報セキュリティ事象に関する決定をする。 評価及び決定の結果は、以後の参照及び検証のために詳細に記録しておく。
16.1.5	情報セキュリティインシデントへの対応 情報セキュリティインシデントは、文書化した手順に従って対応する。	S.26	情報セキュリティインシデントへの対応 管理策 情報セキュリティインシデントは、文書化した手順に従って対応する。 目的 情報セキュリティインシデントへの効率的かつ効果的な対応を確実にするため。		S.26	情報セキュリティインシデントへの対応 統制目標：情報セキュリティインシデントは、文書化した手順に従って対応する。 目的：情報セキュリティインシデントへの効率的かつ効果的な対応を確実にするため。	
–	（対応漏なし）	Se-S.26.1	組織は、情報セキュリティインシデント対応に関する手順を確立し、それを全ての関連する利害関係者に伝達する。	予兆に関連記載あり	S.26.1	情報セキュリティインシデントを、文書化した手順に従って対応する。	組織は、情報セキュリティインシデント対応に関する手順を確立し、それを全ての関連する利害関係者に伝達する。 情報セキュリティインシデントには、必要な力量をもつ指定されたチームが対応する（5.24参照）。 情報セキュリティインシデントへの対応には、次の事項を含める。 a) インシデントの結果が拡がる可能性がある場合には、インシデントの影響を受けるシステムを含める。 b) 情報セキュリティインシデントの発生後、できるだけ速やかに証拠（5.28参照）を収集する。 c) 必要に応じて、危機管理活動及び場合によっては事業継続計画の発動を含むエスカレーションを行う（5.29及び5.30参照）。 d) 後で行う分析のために、関連する全ての対応活動を適正に記録することを確実にする。 e) 知るべき責任の原則に従って全ての関連する内部及び外部の利害関係者に対し、情報セキュリティインシデントの存在又は関連するその詳細を伝達する。 f) 対応の有効性を改善し、他の組織への影響を最小限にする助けとするために、関係当局、外部の利益団体及び会議、供給者、顧客などの内部及び外部の関係者と調整する。 g) インシデントへの対処が望ひな演人正後、正式にそれを終了し、記録する。 h) 必要に応じて、情報セキュリティのオレンジック分析を実施する（5.28参照）。 i) 根本原因を特定するために、インシデント後の分析を実施する。それが定められた手順に従って文書化され、伝達されることを確実にする（5.27参照）。 j) インシデントを引き起こし、インシデントの一因となり、又はインシデントの防止に失敗した管理策に関連するもの含む、情報セキュリティのけん信性及び弱点を特定し、管理する。 情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、組織の情報セキュリティ責任者に報告する。
16.1.5.1	情報セキュリティインシデントには、指定された連絡先、及び組織又は外部関係者の他の関係する要員が対応する。	Se-S.26.2	情報セキュリティインシデントには、必要な力量をもつ指定されたチームが対応する。	予兆に関連記載あり			
–	（対応漏なし）	Se-S.26.3	情報セキュリティインシデントへの対応には、次の事項を含める。 a) インシデントの結果が拡がる可能性がある場合には、インシデントの影響を受けるシステムを含める。	予兆に関連記載あり			
16.1.5.2	対応策には、情報セキュリティインシデントの発生後、できるだけ速やかに証拠を収集することを含める。	Se-S.26.3	情報セキュリティインシデントへの対応には、次の事項を含める。 b) 情報セキュリティインシデントの発生後、できるだけ速やかに証拠を収集する。	予兆に関連記載あり			
16.1.5.4	対応策には、必要に応じて、段階的取扱い（escalation）を行うことを含める。	Se-S.26.3	情報セキュリティインシデントへの対応には、次の事項を含める。 c) 必要に応じて、危機管理活動及び場合によっては事業継続計画の発動を含むエスカレーションを行う。	予兆に関連記載あり			
16.1.5.5	対応策には、後で行う分析のために、関連する全ての対応活動を適正に記録することを確実にすることを含める。	Se-S.26.3	情報セキュリティインシデントへの対応には、次の事項を含める。 d) 後で行う分析のために、関連する全ての対応活動を適正に記録することを確実にする。	予兆に関連記載あり			
16.1.5.6	対応策には、知るべき責任を認められている内部・外部の他の要員又は組織に対し、情報セキュリティインシデントの存在又は関連するその詳細を伝達することを含める。	Se-S.26.3	情報セキュリティインシデントへの対応には、次の事項を含める。 e) 知るべき責任の原則に従って全ての関連する内部及び外部の利害関係者に対し、情報セキュリティインシデントの存在又は関連するその詳細を伝達する。	予兆に関連記載あり			
16.1.5.7	対応策には、インシデントの原因又はインシデントの一因であると判明した情報セキュリティ弱点に対処することを含める。	Se-S.26.3	情報セキュリティインシデントへの対応には、次の事項を含める。 j) インシデントを引き起こし、インシデントの一因となり、又はインシデントの防止に失敗した管理策に関連するものを含む、情報セキュリティのけん信性及び弱点を特定し、管理する。	予兆に関連記載あり			
16.1.5.8	対応策には、インシデントへの対応が望ひな演人正後、正式にそれを終了し、記録することを含める。	Se-S.26.3	情報セキュリティインシデントへの対応には、次の事項を含める。 g) インシデントへの対処が望ひな演人正後、正式にそれを終了し、記録する。	予兆に関連記載あり			
16.1.5.9	インシデントの根本原因を特定するために、インシデント後の分析を実施する。	Se-S.26.3	情報セキュリティインシデントへの対応には、次の事項を含める。 i) 根本原因を特定するために、インシデント後の分析を実施する。それが定められた手順に従って文書化され、伝達されることを確実にする。	予兆に関連記載あり			
–	（対応漏なし）	Se-S.26.3	情報セキュリティインシデントへの対応には、次の事項を含める。 f) 対応の有効性を改善し、他の組織への影響を最小限にする助けとするために、関係当局、外部の利益団体及び会議、供給者、顧客などの内部及び外部の関係者と調整する。 h) 必要に応じて、情報セキュリティのオレンジック分析を実施する。	予兆に関連記載あり			
16.1.6	情報セキュリティインシデントからの学習 情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いる。	S.27	情報セキュリティインシデントからの学習 管理策 情報セキュリティインシデントから得られた知識は、情報セキュリティ管理策を強化し、改善するために用いる。 目的 将来のインシデントの起こりやすさ又は影響を減らすため。		S.27	情報セキュリティインシデントからの学習 統制目標：情報セキュリティインシデントから得られた知識は、情報セキュリティ管理策を強化し、改善するために用いる。 目的：将来のインシデントの起こりやすさ又は影響を減らすため。	
16.1.6.1	情報セキュリティインシデントの形態、規模及び費用を定量化及び監視できるようにする仕組みを備える。	Se-S.27.1	組織は情報セキュリティインシデントの形態、規模及び費用を定量化し、監視するための手順を確立する。	予兆に関連記載あり	S.27.1	情報セキュリティインシデントから得た情報を、情報セキュリティ管理策の強化及び改善に使用する。	組織は情報セキュリティインシデントの形態、規模及び費用を定量化し、監視するための手順を確立する。 情報セキュリティインシデントの評価から得た情報は、次の目的で使用する。 a) インシデントのシナリオ及び手順を含むインシデント管理計画を強化する（5.24参照）。 b) 情報セキュリティのケアセスメントを更新し、将来の同様のインシデントの起こりやすさ又は影響を減らすために必要な追加の管理策を決定し、実施するために、再発する又は重大なインシデント及びそれらの原因を特定する。これを可能にする仕組みには、インシデントの形態、規模及び費用に関する情報の収集、定量化及び監視を含む。 c) 発生し得るインシデントの事例、こうしたインシデントの対応方法の事例、及び以後これらを回避するための方法の事例を示すことによって、利用者の意識向上及び訓練（6.3参照）を強化する。
16.1.6.2	情報セキュリティインシデントの評価から得た情報は、再発する又は影響の大きいインシデントを特定するために利用する。	Se-S.27.2	情報セキュリティインシデントの評価から得た情報は、次の目的で使用する。 a) インシデントのシナリオ及び手順を含むインシデント管理計画を強化する。 b) 組織の情報セキュリティリスクアセスメントを更新し、将来の同様のインシデントの起こりやすさ又は影響を減らすために必要な追加の管理策を決定し、実施するために、再発する又は重大なインシデント及びそれらの原因を特定する。これを可能にする仕組みには、インシデントの形態、規模及び費用に関する情報の収集、定量化及び監視を含む。 c) 発生し得るインシデントの事例、こうしたインシデントの対応方法の事例、及び以後これらを回避するための方法の事例を示すことによって、利用者の意識向上及び訓練を強化する。	予兆に関連記載あり			

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
16.1.7	証拠の収集 組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用する。	5.28	証拠の収集 管理策 組織は、情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための手順を確立し、実施する。 目的： 徴候処置及び法的処置の目的で、情報セキュリティインシデントに関連する証拠の一貫した効果的な管理を確実にするため。		5.28	証拠の収集 統制目標：組織は、情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための手順を確立し、実施する。 目的：徴候処置及び法的処置の目的で、情報セキュリティインシデントに関連する証拠の一貫した効果的な管理を確実にするため。	
16.1.7.1	徴候処置及び法的処置のために証拠を取り扱う場合は、内部の手順を定め、それに従う。	5e-5.28.1	徴候処置及び法的処置のために情報セキュリティ事象に関連する証拠を取り扱う場合は、内部の手順を定めてそれに従う。	予引に関連記載あり	5.28.1	徴候処置及び法的処置のために情報セキュリティ事象に関連する証拠を取り扱う場合の手順を整備する。	徴候処置及び法的処置のために情報セキュリティ事象に関連して取り扱われる証拠は、関連する法域において受容される可能性を最大にするために、異なる幾つかの法域の要求事項を考慮する。 情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための証拠の管理に関する手順では、各種の記憶媒体、装置・機器及び装置・機器の状態（すなわち、電源が入っている/ない、切れている/ない）に従って、証拠の特定、収集、取得及び保存の指示を規定する。
16.1.7.2	徴候処置及び法的処置のために証拠を取り扱う手順では、各種の媒体、装置及び装置の状態（例えば、電源が入っている/ない、切れている/ない）に従って、証拠の特定、収集、取得及び保存のプロセスを規定する。	5e-5.28.3	情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための証拠の管理に関する手順では、各種の記憶媒体、装置・機器及び装置・機器の状態（すなわち、電源が入っている/ない、切れている/ない）に従って、証拠の特定、収集、取得及び保存の指示を規定する。	予引に関連記載あり			
16.1.7.3	徴候処置及び法的処置のために証拠を取り扱う手順では、管理状況の一連の履歴を取得するプロセスを規定する。	–	（追按対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
16.1.7.4	徴候処置及び法的処置のために証拠を取り扱う手順では、証拠の保全を行うプロセスを規定する。	5e-5.28.4	証拠は原則として、適切な国内法廷又は別の徴候会議において受容される方法で収集し、次の事項を示す。 a) 記録は完全で、いかなる方法でも改ざんされていない。 b) 電子証拠の複製は原本と同一であることが保定される。 c) 証拠の収集元である情報システムは、証拠を記録した時点で正しい機能していた。	予引に関連記載あり	5.28.2	情報セキュリティ事象に関連する証拠を収集、取得及び保存する。	証拠は原則として、適切な国内法廷又は別の徴候会議において受容される方法で収集し、次の事項を示す。 a）記録は完全で、いかなる方法でも改ざんされていない。 b）電子証拠の複製は原本と同一であることが保定される。 c）証拠の収集元である情報システムは、証拠を記録した時点で正しく機能していた。 保存した証拠の価値を強化するために、入手可能であれば、要員及びツールの適格性を示す証明書又はその他適切な手段を追求する。 ディジタル証拠の初動の枠又は法域を越える場合、組織は必要とされる情報をディジタル証拠として収集することが法的に認められていることを確認する。
16.1.7.5	徴候処置及び法的処置のために証拠を取り扱う手順では、要員の安全を確保するプロセスを規定する。	–	（追按対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
16.1.7.6	徴候処置及び法的処置のために証拠を取り扱う手順では、関与する要員の役割及び責任を定める。	–	（追按対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
16.1.7.7	徴候処置及び法的処置のために証拠を取り扱う手順では、要員の力量を定める。	–	（追按対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
16.1.7.8	徴候処置及び法的処置のために証拠を取り扱う手順では、文書化することを定める。	–	（追按対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
16.1.7.9	徴候処置及び法的処置のために証拠を取り扱う手順では、集点説明を行うことを定める。	–	（追按対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
16.1.7.10	保存された証拠の価値を強化するために、要員及びツールの適格性を示す証明書又はその他適切な手段を追求する。	5e-5.28.5	保存した証拠の価値を強化するために、入手可能であれば、要員及びツールの適格性を示す証明書又はその他適切な手段を追求する。	予引に関連記載あり	5.28.2	【再】情報セキュリティ事象に関連する証拠を収集、取得及び保存する。	（5.28.2に対応する項を参照）
16.1.7.11	徴候処置及び法的処置に必要な法的証拠が、組織の枠又は法域を越える場合、組織は必要とされる情報をディジタル証拠として収集することが法的に認められていることを確認する。	5e-5.28.6	ディジタル証拠が初動の枠又は法域を越える場合、組織は必要とされる情報をディジタル証拠として収集することが法的に認められていることを確認する。	予引に関連記載あり			
16.1.7.12	徴候処置及び法的処置に関連する幾つかの法域にまたがる証拠の利用の可能性を最大にするために、それらの異なる法域の要求事項を確認する。	5e-5.28.2	【再】法的処置のために情報セキュリティ事象に関連して取り扱われる証拠は、関連する法域において受容されるよう最大限の注意を払う。	予引に関連記載あり	5.28.1	【再】徴候処置及び法的処置のために情報セキュリティ事象に関連する証拠を取り扱う場合の手順を整備する。	（5.28.1に対応する項を参照）
16.1.7.13.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	5.28.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
17	事業継続マネジメントにおける情報セキュリティの側面	5.29	事業の中断・阻害時の情報セキュリティ 管理策 組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画する。 目的： 事業の中断・阻害時に情報及びその他の関連資産を保護するため。		5.29	事業の中断・阻害時の情報セキュリティ 統制目標：組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画する。 目的：事業の中断・阻害時に情報及びその他の関連資産を保護するため。	
17.1	情報セキュリティ継続 管理目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。						
17.1.1	情報セキュリティの継続の計画 組織は、困難な状況（adverse situation）（例えば、危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定する。						
17.1.1.1	組織は、情報セキュリティの継続が事業継続マネジメント（以下「BCM」という。）プロセス又は災害復旧管理（以下「DRM」という。）プロセスに織り込まれているか否かを判断する。	SF-5.29.2	情報セキュリティ要求事項は、事業継続マネジメントプロセスに含める。	予引に関連記載あり	5.29.1	事業の中断・阻害時に情報セキュリティ管理策を適応させるための要求事項を定義する。	組織は、事業の中断・阻害時に情報セキュリティ管理策を適応させるための自らの要求事項を決定する。 情報セキュリティ要求事項は、事業継続マネジメントプロセスに含める。
17.1.1.2	組織は、事業継続及び災害復旧に関する計画を立てる場合に、情報セキュリティ要求事項を定める。	SF-5.29.1	組織は、事業の中断・阻害時に情報セキュリティ管理策を適応させるための自らの要求事項を決定する。	予引に関連記載あり			
17.1.1.3	事業継続及び災害復旧に関する正式な計画が策定されていない場合に、通常の業務状況とは異なる困難な状況においても、情報セキュリティ要求事項は変わらず存続するよう定める。	–	（追按対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
17.1.1.4	事業継続及び災害復旧に関する正式な計画が策定されていない場合において、情報セキュリティ要求事項が変わらず存続すると定められない場合には、情報セキュリティの側面について事業影響度分析を実施し、通常の業務状況とは異なる困難な状況に適用できる情報セキュリティ要求事項を定める。	–	（追按対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
17.1.2	情報セキュリティ継続の実施 組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持する。	S.29	事業の中断・阻害時の情報セキュリティ 管理策 組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画する。 目的： 事業の中断・阻害時に情報及びその他の関連資産を保護するため。		S.29	事業の中断・阻害時の情報セキュリティ 統制目標：組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画する。 目的：事業の中断・阻害時に情報及びその他の関連資産を保護するため。	
17.1.2.1	組織は、必要な権限、経験及び力量を備えた要員を問い中断・阻害を引き起こす事象に備え、これを軽減し、これに対処するための十分な管理構造を確実に設ける。	5e-5.26.2	【再】情報セキュリティインシデントには、必要な力量をもつ指定されたチームが対応する。	予引に関連記載あり	5.26.1	【再】情報セキュリティインシデントを、文書化した手順に従って対応する。	（5.26.1に対応する項を参照）
17.1.2.2	組織は、インシデント管理し、情報セキュリティを維持するための責任、権限及び力量を備えたインシデント対応要員を確実に任命する。	5e-5.26.2	【再】情報セキュリティインシデントには、必要な力量をもつ指定されたチームが対応する。	予引に関連記載あり			
17.1.2.3	組織は、経営陣が参加し情報セキュリティ継続の枠内に基づいて、組織が中断・阻害を引き起こす事象を管理し、その情報セキュリティを既定のレベルに維持する場合の方法を計画及び手順に詳細に記して、計画、対応及び回復の文書化した手順を確実に策定し、これらを承認する。	SF-5.29.3	中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するために、計画を策定し、実施し、試験し、レビューし、評価する。	予引に関連記載あり	5.29.2	中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するために、計画を策定する。	中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するために、計画を策定し、実施し、試験し、レビューし、評価する。 情報のセキュリティは、必要なレベル及び必要な時間内に復旧する。 組織は次の事項を実施し、維持する。 a）事業継続計画及びIT継続計画における情報セキュリティ管理策、支援システム及びツール b）事業の中断・阻害時に既存の情報セキュリティ管理策を維持するためのプロセス c）事業の中断・阻害時に維持できない情報セキュリティ管理策を補う管理策
–	（対応項なし）	SF-5.29.4	情報のセキュリティは、必要なレベル及び必要な時間内に復旧する。	予引に関連記載あり			
17.1.2.4	組織は、情報セキュリティ継続に関する要求事項に従って、事業継続又は災害復旧のためのプロセス及び手順、並びにこれらを支援するシステム及びツールにおける情報セキュリティ管理策を確立し、文書化し、実施し、維持する。	SF-5.29.5	組織は次の事項を実施し、維持する。 a）事業継続計画及びICT継続計画における情報セキュリティ管理策、支援システム及びツール	予引に関連記載あり			
17.1.2.5	組織は、情報セキュリティ継続に関する要求事項に従って、困難な状況において既存の情報セキュリティ管理策を維持するための、プロセス及び手順の変更並びにそれらの実施の変更を確立し、文書化し、実施し、維持する。	SF-5.29.5	組織は次の事項を実施し、維持する。 b）事業の中断・阻害時に既存の情報セキュリティ管理策を維持するためのプロセス	予引に関連記載あり			
17.1.2.6	組織は、情報セキュリティ継続に関する要求事項に従って、困難な状況において維持することが不可能な情報セキュリティ管理策を補うための管理策を確立し、文書化し、実施し、維持する。	SF-5.29.5	組織は次の事項を実施し、維持する。 c）事業の中断・阻害時に維持できない情報セキュリティ管理策を補う管理策	予引に関連記載あり			
17.1.3	情報セキュリティ継続の検証、レビュー及び評価 確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、組織は、定められた間隔でこれらの管理策を検証する。	S.29	事業の中断・阻害時の情報セキュリティ 管理策 組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画する。 目的： 事業の中断・阻害時に情報及びその他の関連資産を保護するため。		S.29	事業の中断・阻害時の情報セキュリティ 統制目標：組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画する。 目的：事業の中断・阻害時に情報及びその他の関連資産を保護するため。	
17.1.3.1	運用に関するもの、組織に関するものを問わず、組織、採用、手順及びプロセスの変更が、情報セキュリティ継続に関する要求事項の変更につながる場合、変更後の要求事項に照らして、情報セキュリティのための プロセス、手順及び管理策の継続性をレビューする。	SF-5.29.3	【再】中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するために、計画を策定し、実施し、試験し、レビューし、評価する。	予引に関連記載あり	5.29.3	中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するための計画を試験する。	特になし。
17.1.3.2	組織は、情報セキュリティ継続のためのプロセス、手順及び管理策の機能が情報セキュリティ継続の目的と整合していることを確実にするために、これらの機能を実行し、試験する。	SF-5.29.3	【再】中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するために、計画を策定し、実施し、試験し、レビューし、評価する。	予引に関連記載あり			
17.1.3.3	組織は、情報セキュリティ継続のためのプロセス、手順及び管理策を機能させる知識及びルーチンを実行及び試験し、そのパフォーマンスの情報セキュリティ継続の目的に整合していることを確実にするために組み立てる。	–	（追按対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
17.1.3.4	組織は、情報システム、情報セキュリティのプロセス、手順及び管理策、又はBCM-DRM のプロセス及びソリューションが変更された場合には、情報セキュリティ継続のための手段の妥当性及び有効性をレビューする。	–	（追按対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
17.2	冗長性 管理目的：情報処理施設の可用性を確実にするため。	8.14	情報処理施設・設備の冗長性 管理策 情報処理施設・設備は、可用性の要求事項を満たすに十分な冗長性をもって、導入する。 目的 情報処理施設・設備の継続的な運用を確実にするため。		8.14	情報処理施設・設備の冗長性 統制目標：情報処理施設・設備は、可用性の要求事項を満たすに十分な冗長性をもって、導入する。 目的：情報処理施設・設備の継続的な運用を確実にするため。	
17.2.1	情報処理施設の可用性 情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。						
17.2.1.1	組織は、情報システムの可用性に関する業務上の要求事項を特定する。	8b-8.14.1	組織は、業務上のサービス及び情報システムの可用性に関する要求事項を特定する。	予引に関連記載あり	8.14.1	業務上のサービス及び情報システムの可用性に関する要求事項を定義し、この要求事項を満たすために、適切な冗長性をもってシステムアーキテクチャを設計し、実装する。	組織は、業務上のサービス及び情報システムの可用性に関する要求事項を特定する。 組織は、この要求事項を満たすために、適切な冗長性をもってシステムアーキテクチャを設計し、実装する。冗長性は、情報処理施設・設備の一部又は全体を二重化させる（手順の構成要素をもつか、又は二つの全ての要素をもつ。）ことによって導入することが可能である。 冗長な構成要素及び処理施設・設備を作動させる手順では、冗長な構成要素及び処理活動を常に作動させておくか、又は緊急の場合に自動若しくは手動で作動させるかを定める。 冗長な構成要素及び情報処理施設・設備は、主たる構成要素及び情報処理施設・設備と同じセキュリティレベルをもつことを確実にする。 情報処理施設・設備の故障を組織に警告し、計画した手順を実行できるようにし、情報処理施設・設備を修理又は交換している間も、継続して可用性の維持を可能とするため組み合わせる。 組織は、冗長システムを実装する場合、次の事項を考慮する。 a）インターネットサービス提供者など、ネットワーク及び重要な情報処理施設・設備の供給者、二重以上と契約する。 b）冗長性のあるネットワークを使用する。 c）冗長構成をとったシステムをもつ地理的に離れた二つのデータセンターを使用する。 d）物理的に冗長性のある電力供給装置又は電源を使用する。 e）ソフトウェア構成要素の複数の並列インスタンスを、同じデータセンター内又は異なるデータセンターのインスタンス間で自動負荷分散によって使用する。 f）システムにおいて二重化した構成要素（例えば、CPU、ハードディスク、メモリ）をもつ、又はネットワークにおいて二重化した構成要素（例えば、ファイアウォール、ルーター、スイッチ）をもつ。
–	（対応項なし）	8b-8.14.3	組織は、冗長な構成要素及び情報処理施設・設備を作動させる手順を計画し、実装する。	予引に関連記載あり			
–	（対応項なし）	（8b-8.14.3参考）	冗長性は、情報処理施設・設備の一部又は全体を二重化させることによって導入することが可能である。	予引に関連記載あり			
–	（対応項なし）	8b-8.14.4	冗長な構成要素及び情報処理施設・設備を作動させる手順では、冗長な構成要素及び処理活動を常に作動させておか、又は緊急の場合に自動若しくは手動で作動させるかを定める。	予引に関連記載あり			
–	（対応項なし）	8b-8.14.5	冗長な構成要素及び情報処理施設・設備は、主たる構成要素及び情報処理施設・設備と同じセキュリティレベルをもつことを確実にする。	予引に関連記載あり			
–	（対応項なし）	8b-8.14.6	情報処理施設・設備の故障を組織に警告し、計画した手順を実行できるようにし、情報処理施設・設備を修理又は交換している間も、継続して可用性の維持を可能とするため組み合わせる。	予引に関連記載あり			
–	（対応項なし）	8b-8.14.7	組織は、冗長システムを実装する場合、次の事項を考慮する。 a）インターネットサービス提供者など、ネットワーク及び重要な情報処理施設・設備の供給者、二重以上と契約する。 b）冗長性のあるネットワークを使用する。 c）冗長構成をとったシステムをもつ地理的に離れた二つのデータセンターを使用する。 d）物理的に冗長性のある電力供給装置又は電源を使用する。 e）ソフトウェア構成要素の複数の並列インスタンスを、同じデータセンター内又は異なるデータセンターのインスタンス間で自動負荷分散によって使用する。 f）システムにおいて二重化した構成要素をもつ、又はネットワークにおいて二重化した構成要素をもう。	予引に関連記載あり			
17.2.1.3	組織は、一つの構成要素から別の構成要素への切替え（failover）による冗長の場合、それが機能したときに動作することを確実にするために、冗長な情報システムを試験する。	8b-8.14.8	実施できる場合、であれば本書モードにおいて、一つの構成要素から別の構成要素への切替え（failover）が機能したときに動作することを確実にするために、冗長な情報システムを試験する。	予引に関連記載あり	8.14.2	一つの構成要素から別の構成要素への切替え（failover）が機能したときに動作することを試験する。	実施できる場合、であれば本書モードにおいて、一つの構成要素から別の構成要素への切替え（failover）が機能したときに動作することを確実にするために、冗長な情報システムを試験する。

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
18	順守	S.31	法令、規制及び契約上の要求事項 管理策 情報セキュリティに関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組を特定し、文書化し、また、最新に保つ。 目的 情報セキュリティに関連する法令、規制及び契約上の要求事項の順守を確実にするため。		S.31	法令、規制及び契約上の要求事項 統制目標：情報セキュリティに関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組を特定し、文書化し、また、最新に保つ。 目的：情報セキュリティに関連する法令、規制及び契約上の要求事項の順守を確実にするため。	
18.1 法的及び契約上の要求事項の順守 管理目的：情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。							
18.1.1 適用法令及び契約上の要求事項の特定 各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。							
18.1.1.1	各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項を満たすための具体的な管理策及び具体的な責任について定め、文書化する。	Sg-S.31.1	法令、規制又は契約上の要求事項を含む外部の要求事項は、次の場合に考慮に入れる。 a) 情報セキュリティの方針获取り下げの制定 b) 情報セキュリティ管理策の設計、実施又は変更 c) 内部のニーズ又は供給者との合意のために情報セキュリティ要求事項を設定するプロセスの一部として、情報及びその他の関連資産の分類 d) 情報セキュリティリスクアセスメントの実施、及び情報セキュリティリスク対応活動の決定 e) 情報セキュリティに関連する役割及び責任に従ったプロセスの決定 f) 組織、並びに供給を受ける製品及びサービスの範囲に関係する、供給者の契約上の要求事項の特定	予℃に関連記載あり	S.31.1	組織の情報セキュリティに関連する全ての法令及び規制を特定し、自らの事業の概観に対する要求事項を特定し、維持する。	法令、規制又は契約上の要求事項を含む外部の要求事項は、次の場合に考慮に入れる。 a) 情報セキュリティの方針获取り下げの制定 b) 情報セキュリティ管理策の設計、実施又は変更 c) 内部のニーズ又は供給者との合意のために情報セキュリティ要求事項を設定するプロセスの一部として、情報及びその他の関連資産の分類 d) 情報セキュリティリスクアセスメントの実施、及び情報セキュリティリスク対応活動の決定 e) 情報セキュリティに関連する役割及び責任に従ったプロセスの決定 f) 組織、並びに供給を受ける製品及びサービスの範囲に関係する、供給者の契約上の要求事項の特定 組織は、次の事項を行う。 a) 自らの事業の概観に対する要求事項を認識するために、組織の情報セキュリティに関連する全ての法令及び規制を特定する。 b) 組織が次のとおりである場合に、関連する全ての国における順守を考慮する。 1) 他国で事業を行っている。 2) 法令及び規制が組織に影響を与える可能性がある、他国の製品及びサービスを利用している。 3) 法令及び規制が組織に影響を与える可能性がある、法域との境界を越えて情報の移転を行う。 c) 変更に追随し、新しい法令を特定するために、特定した法令及び規制を定期的にレビューする。 d) これらの要求事項を満たすためのプロセス及び個々の責任を定義し、文書化する。D110 情報セキュリティに関する契約上の要求事項には、次のものに記載されている要求事項を含む。 a) 顧客との契約 b) 供給者との契約（S.20参照） c) 保険契約
18.1.1.2	管理者は、事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。	Sg-S.31.2	組織は、次の事項を行う。 a) 自らの事業の概観に対する要求事項を認識するために、組織の情報セキュリティに関連する全ての法令及び規制を特定する。	予℃に関連記載あり			
18.1.1.3	組織が他の国で事業を営む場合には、管理者は、関連する全ての国における法令、規制及び契約上の要求事項を順守する。	Sg-S.31.2	組織は、次の事項を行う。 b) 組織が次のとおりである場合に、関連する全ての国における順守を考慮する。 – 他国で事業を行っている。 – 法令及び規制が組織に影響を与える可能性がある、他国の製品及びサービスを利用している。 – 法令及び規制が組織に影響を与える可能性がある、法域との境界を越えて情報の移転を行う。	予℃に関連記載あり			
–	（対応項なし）	Sg-S.31.2	組織は、次の事項を行う。 c) 変更に追随し、新しい法令を特定するために、特定した法令及び規制を定期的にレビューする。	予℃に関連記載あり			
18.1.1.4.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	S.31.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
18.1.1.5.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	予℃に関連記載あり（情報セキュリティ管理基準以外の由来）	S.31.5	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
18.1.1.6.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）			
18.1.1.7.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	S.31.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
18.1.2 知的財産権 知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施する。		S.32	知的財産権 管理策 組織は知的財産権を保護するための適切な手順を実施する。 目的 知的財産権及び権利関係のある製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするため。		S.32	知的財産権 統制目標：組織は知的財産権を保護するための適切な手順を実施する。 目的：知的財産権及び権利関係のある製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするため。	
–	（対応項なし）	Sg-S.32.1	知的財産との得るための保護するために、次の事項を考慮する。 a) 知的財産権の保護に関するトピック箇有の方針を定め、伝達する。	予℃に関連記載あり	S.32.1	知的財産権及び権利関係のある製品の利用に関連する、法令、規制、契約上の要求事項の順守に関する方針とプロセスを策定する。	知的財産との得るための保護するために、次の事項を考慮する。 a) 知的財産権の保護に関するトピック箇有の方針を定め、伝達する。 b) ソフトウェア製品及び情報製品のコンプライアンスにのっとった利用を定めた、知的財産権の順守の手順を実行する。
18.1.2.1	ソフトウェア製品及び情報製品の合法利用を明確に定めた知的財産権順守方針を公表する。	Sg-S.32.1	知的財産との得るための保護するために、次の事項を考慮する。 b) ソフトウェア製品及び情報製品のコンプライアンスにのっとった利用を定めた、知的財産権の順守の手順を実行する。	予℃に関連記載あり			c) 著作権を侵害しないことを確実にするために、ソフトウェアは、知名度の高い、かつ、定評のある供給元だけを通して取得する。 d) 適切な資産登録簿を維持管理し、知的財産権の保護が求められている全ての資産を特定する。 e) 使用許諾条件に従っていることの証明及び証拠、手引などを維持・管理する。 f) 使用許諾で許可された最大利用者数又は資源数（例えば、中央処理装置（CPU）］を超過しないことを確実にする。 g) 認可されていないソフトウェア及び使用許諾されている製品だけが導入されていることを確実にするためのレビューを行う。 h) 適切な使用許諾条件を維持・管理するための手順を定める。 i) ソフトウェアの処分又は他人への譲渡についての手順を定める。 j) 公衆ネットワークなど外部供給元から入手するソフトウェア及び情報の使用条件を順守する。 k) 著作権法又は適用される使用許諾が認めている場合を除いて、商用記録（ビデオ、録音）を複製、他形式に変換、又は抜粋しない。 l) 著作権法又は適用される使用許諾が認めている場合を除いて、規格（例えば、ISO/IEC規格）、書籍、記事、報告書又はその他文書の全部又は一部を複写しない。
18.1.2.2	著作権を侵害しないことを確実にするために、ソフトウェアは、知名度の高い、かつ、定評のある供給元だけを通して取得する。	Sg-S.32.1	知的財産との得るための保護するために、次の事項を考慮する。 c) 著作権を侵害しないことを確実にするために、ソフトウェアは、知名度の高い、かつ、定評のある供給元だけを通して取得する。	予℃に関連記載あり			
18.1.2.3	知的財産権を保護するための方針に対する認識を持続させ、それらの方針に違反した要員に対して懲戒処置をとる意思を通知する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で組承された）	–	（対応項なし）	–
18.1.2.4	適切な資産登録簿を維持・管理し、知的財産権の保護が求められている全ての資産を特定する。	Sg-S.32.1	知的財産との得るための保護するために、次の事項を考慮する。 d) 適切な資産登録簿を維持管理し、知的財産権の保護が求められている全ての資産を特定する。	予℃に関連記載あり	S.32.1	【再】知的財産権及び権利関係のある製品の利用に関連する、法令、規則、契約上の要求事項の順守に関する方針とプロセスを策定する。	（S.32.1に対応する項目を参照）
18.1.2.5	使用許諾を得ているこの証明及び証拠、マスディスク、手引などを維持・管理する。	Sg-S.32.1	知的財産との得るための保護するために、次の事項を考慮する。 e) 使用許諾を得ているこの証明及び証拠、手引などを維持・管理する。	予℃に関連記載あり			
18.1.2.6	使用許諾で許可された最大利用者数を超過しないことを確実にするための管理策を実施する。	Sg-S.32.1	知的財産との得るための保護するために、次の事項を考慮する。 f) 使用許諾で許可された最大利用者数又は資源数を超過しないことを確実にする。	管理策に関連記載あり	S.32.2	知的財産権及び権利関係のある製品の利用において、使用許諾で許可された最大利用者数又は資源数を超過しないことを確実にする。	特になし。
18.1.2.7	認可されていないソフトウェア及び使用許諾されている製品だけが導入されていることのレビューを行う。	Sg-S.32.1	知的財産との得るための保護するために、次の事項を考慮する。 g) 認可されていないソフトウェア及び使用許諾されている製品だけが導入されていることを確実にするためのレビューを行う。	予℃に関連記載あり	S.32.1	知的財産権及び権利関係のある製品の利用に関連する、法令、規則、契約上の要求事項の順守に関する方針とプロセスを策定する。	知的財産との得るための保護するために、次の事項を考慮する。 a) 知的財産権の保護に関するトピック箇有の方針を定め、伝達する。 b) ソフトウェア製品及び情報製品のコンプライアンスにのっとった利用を定めた、知的財産権の順守の手順を実行する。 c) 著作権を侵害しないことを確実にするために、ソフトウェアは、知名度の高い、かつ、定評のある供給元だけを通して取得する。 d) 適切な資産登録簿を維持管理し、知的財産権の保護が求められている全ての資産を特定する。 e) 使用許諾を得ているこの証明及び証拠、手引などを維持・管理する。 f) 使用許諾で許可された最大利用者数又は資源数（例えば、中央処理装置（CPU）］を超過しないことを確実にする。 g) 認可されていないソフトウェア及び使用許諾されている製品だけが導入されていることを確実にするためのレビューを行う。 h) 適切な使用許諾条件を維持・管理するための手順を定める。 i) ソフトウェアの処分又は他人への譲渡についての手順を定める。 j) 公衆ネットワークなど外部供給元から入手するソフトウェア及び情報の使用条件を順守する。 k) 著作権法又は適用される使用許諾が認めている場合を除いて、商用記録（ビデオ、録音）を複製、他形式に変換、又は抜粋しない。 l) 著作権法又は適用される使用許諾が認めている場合を除いて、規格（例えば、ISO/IEC規格）、書籍、記事、報告書又はその他文書の全部又は一部を複写しない。
18.1.2.8	適切な使用許諾条件を維持・管理するための手順を定める。	Sg-S.32.1	知的財産との得るための保護するために、次の事項を考慮する。 h) 適切な使用許諾条件を維持・管理するための手順を定める。	予℃に関連記載あり			
18.1.2.9	ソフトウェアの処分又は他人への譲渡についての手順を定める。	Sg-S.32.1	知的財産との得るための保護するために、次の事項を考慮する。 i) ソフトウェアの処分又は他人への譲渡についての手順を定める。	予℃に関連記載あり			
18.1.2.10	公衆ネットワークから入手するソフトウェア及び情報の使用条件に従う。	Sg-S.32.1	知的財産との得るための保護するために、次の事項を考慮する。 j) 公衆ネットワークなど外部供給元から入手するソフトウェア及び情報の使用条件を順守する。	予℃に関連記載あり			
18.1.2.11	著作権法が認めている場合を除いて、商用記録（フィルム、録音）を複製、他形式に変換、又は抜粋しない。	Sg-S.32.1	知的財産との得るための保護するために、次の事項を考慮する。 k) 著作権法又は適用される使用許諾が認めている場合を除いて、商用記録（ビデオ、録音）を複製、他形式に変換、又は抜粋しない。	予℃に関連記載あり			
18.1.2.12	著作権法が認めている場合を除いて、書籍、記事、報告書又はその他文書の全部又は一部を複写しない。	Sg-S.32.1	知的財産との得るための保護するために、次の事項を考慮する。 l) 著作権法又は適用される使用許諾が認めている場合を除いて、規格、書籍、記事、報告書又はその他文書の全部又は一部を複写しない。	予℃に関連記載あり			
18.1.2.13.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	Sg-S.32.1	【再】知的財産との得るための保護するために、次の事項を考慮する。 b) ソフトウェア製品及び情報製品のコンプライアンスにのっとった利用を定めた、知的財産権の順守の手順を実行する。	予℃に関連記載あり			
18.1.3 記録の保護 記録は、法令、規則、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。		S.33	記録の保護 管理策 記録は、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護するべきである。 目的 記録の保護及び可用性に関連する、法令、規則及び契約上の要求事項の順守、並びにコミュニティ又は社会の期待に応えることを確実にするため。		S.33	記録の保護 統制目標：記録は、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。 目的：記録の保護及び可用性に関連する、法令、規則及び契約上の要求事項の順守、並びにコミュニティ又は社会の期待に応えることを確実にするため。	
18.1.3.1	具体的な組織の記録の保護について決定する場合は、組織の分類体系に基づき、その情報に適用されている分類を考慮して決定する。	Sg-S.33.4	具体的な組織の記録の保護について決定する場合は、組織の分類体系に基づき、その情報に適用されている情報セキュリティ分類を考慮する。	予℃に関連記載あり	S.33.1	記録を保護するための方針を策定する。	組織は、自らの事業の状況及び自らの管理の要求事項が時間の経過とともに変化するため、記録の真正性、信頼性、完全性及び使用可能性を保護するための段階を踏む。 a) 記録の改変の防止を含む、記録の保存、受渡記録の整備、及び記録の紛失に関する指針を発行する。この指針は、記録管理及びその他の記録の要求事項に関する組織のヒック箇有の方針に沿っている。 b) 記録及びそれらの記録の保持することが望ましい期間を明確にした保持計画を作成する。 具体的な組織の記録の保護について決定する場合は、組織の分類体系に基づき、その情報に適用されている情報セキュリティ分類を考慮する。 記録類は、記録の種類（例えば、会計記録、事業のトランザクション記録、人事記録、法規記録）によって、また、それぞれの種類を扱い詳細に、保持期間、及び許容される物理的又は電子的な記憶媒体の種類によって分類する。
18.1.3.2	記録類は、記録の種類（例えば、会計記録、データベース記録、トランザクション記録、監査ログ、運用手順）によって、また、更にそれぞれの種類での保持期間及び許容される記憶媒体の種類（例えば、紙、マイクロフィッシュ、磁気媒体、光媒体）の詳細によって分類する。	Sg-S.33.5	記録類は、記録の種類によって、また、それぞれの種類を更に詳細に、保持期間、及び許容される物理的又は電子的な記憶媒体の種類によって分類する。	予℃に関連記載あり			
18.1.3.3	保存した記録の暗号化又はディジタル署名に用いた暗号鍵及び暗号プログラムは、その記録類を保存している期間中に記録の復号が可能なように、保管する。	Sg-S.33.8	記録を保存している期間中、記録の復号を可能にするために、暗号化したアーカイブ又はディジタル署名に用いた暗号鍵及び暗号プログラムも保持する。	予℃に関連記載あり	S.33.3	記録を保護するための対策を実施する。	適にすべき要求に応じて、許容される時間枠内及び書式で、要求された記録を型の出すことができるよう、データ保存システムを選択する。 電子記憶媒体を選択する場合は、将来の技術変化によって読出しができなくなることを防ぐため、保持期間を通じて記録にアクセスできること（記憶媒体及び書式の読取の可能性）を確実にする手順を確立する。 記録を保持している期間中、記録の復号を可能にするために、暗号化したアーカイブ又はディジタル署名に用いた暗号鍵及び暗号プログラムも保持する（8.24参照）。 記録媒体の保存及び取扱いの手順は、記憶媒体の製造業者が示す推奨の仕様に従って実施する。 記録の保存に用いる媒体が劣化する可能性を考慮する。
18.1.3.4	記録の保存に用いる媒体が劣化する可能性を考慮して記録の保存及び取扱いの手順を定める。	Sg-S.33.10	記録の保存に用いる媒体が劣化する可能性を考慮する。	予℃に関連記載あり			
18.1.3.5	記録の保存及び取扱いの手順は、媒体の製造業者の推奨の仕様に従って実施する。	Sg-S.33.9	記録媒体の保存及び取扱いの手順は、記憶媒体の製造業者が示す推奨の仕様に従って実施する。	予℃に関連記載あり			
18.1.3.6	電子的記憶媒体を選択する場合は、将来の技術変化によって読出しができなくなることを防ぐため、保持期間を通じてデータにアクセスできること（媒体及び書式の読取の可能性）を確実にする手順を確立する。	Sg-S.33.7	電子記憶媒体を選択する場合は、将来の技術変化によって読出しができなくなることを防ぐため、保持期間を通じて記録にアクセスできること（記憶媒体及び書式の読取の可能性）を確実にする手順を確立する。	予℃に関連記載あり			
18.1.3.7	適にすべき要求に応じて、許容される時間枠内及び書式で、要求された記録を型の出すことができるよう、データ保存システムを選択する。	Sg-S.33.6	適にすべき要求に応じて、許容される時間枠内及び書式で、要求された記録を型の出すことができるよう、データ保存システムを選択する。	予℃に関連記載あり			
18.1.3.8	データ保存及びデータ処理システムは、記録を確実に特定し、国又は地域の法令又は規制が適用される場合に定められている記録の保持期間を確実に特定する。	Sg-S.33.2	記録を保存し、取り扱うシステムは、国又は地域の法令又は規則、及び該当する場合には、コミュニティ又は社会の期待も考慮に入れて、記録及びその保存期間の特定を確実にする。	予℃に関連記載あり	S.33.2	記録を保存するシステムは、国、地域の法令、規則、該当する場合には、コミュニティ又は社会の期待も考慮に入れて、記録及びその保存期間を特定する。	記録を保存し、取り扱うシステムは、国又は地域の法令又は規則、及び該当する場合には、コミュニティ又は社会の期待も考慮に入れて、記録及びその保存期間の特定を確実にする。 記録の保存期間が終了した後、組織にとって必要ない場合には、そのシステムは、記録を適切に廃棄できるようにする。
18.1.3.9	保持期間が終了した後、組織にとって必要ない場合には、データ保存及びデータ処理システムは、記録を適切に廃棄できるようにする。	Sg-S.33.3	記録の保持期間が終了した後、組織にとって必要ない場合には、そのシステムは、記録を適切に廃棄できるようにする。	予℃に関連記載あり			
18.1.3.10	記録保護の目的を考慮して、組織内では、記録及び情報の保持、保存、取扱い及び処分に関する指針を発行する。	Sg-S.33.1	組織は、自らの事業の状況及び自らの管理の要求事項が時間の経過とともに変化するため、記録の真正性、信頼性、完全性及び使用可能性を保護するための段階を踏む。 a) 記録の改変の防止を含む、記録の保存、受渡記録の整備、及び記録の紛失に関する指針を発行する。これらの指針は、記録管理及びその他の記録の要求事項に関する組織のヒック箇有の方針に沿っている。	予℃に関連記載あり	S.33.1	【再】記録を保護するための方針を策定する。	（S.33.1に対応する項目を参照）
18.1.3.11	記録保護の目的を考慮して、組織内では、記録及びそれらの記録の保持期間を明確にした保持計画を作成する。	Sg-S.33.1	組織は、自らの事業の状況及び自らの管理の要求事項が時間の経過とともに変化するため、記録の真正性、信頼性、完全性及び使用可能性を保護するための段階を踏む。 b) 記録及びそれらの記録の保持することが望ましい期間を明確にした保持計画を作成する。	予℃に関連記載あり			
18.1.3.12	記録保護の目的を考慮して、組織内では、主要な情報の出典一覧を維持・管理する。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で組承された）	–	（対応項なし）	–
18.1.3.13.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	S.33.4	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
18.1.4	プライバシー及び個人を特定できる情報（PII）の保護 プライバシー及び個人識別情報（PII）の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実に行う。	5.34	プライバシー及びPIIの保護 管理策 組織は、適用される法令、規制及び契約上の要求事項に従って、プライバシー及びPIIの保護に関する要求事項を特定し、満たす。 目的 PIIの保護の情報セキュリティの側面に関連する法令、規制及び契約上の要求事項の順守を確実にするため。		5.34	プライバシー及びPIIの保護 統制目標：組織は、適用される法令、規制及び契約上の要求事項に従って、プライバシー及びPIIの保護に関する要求事項を特定し、満たす。 目的：PIIの保護の情報セキュリティの側面に関連する法令、規制及び契約上の要求事項の順守を確実にするため。	
18.1.4.1	プライバシー及びPII の保護に関する組織の方針を確立して実施する。	5g-5.34.1	組織は、プライバシー及びPII の保護に関するトピック固有の方針を確立し、全ての関連する利害関係者に伝達する。	予防に関連記載あり	5.34.1	適用される法令、規制及び契約上の要求事項に従って、プライバシー及びPIIの保護に関する要求事項を特定し、対策を実施する。	組織は、プライバシー及びPIIの保護に関するトピック固有の方針を確立し、全ての関連する利害関係者に伝達する。 組織は、プライバシー及びPIIの保護のための手順を策定し、実施する。 組織は、プライバシー及びPIIの保護のために策定した手順を、PIIの処理に関わる全ての利害関係者に伝達する。 PIIを保護するための適切な技術的及び組織的対策を実施する。
18.1.4.2	プライバシー及びPII の保護に関する組織の方針は、PIIの処理に関与する全ての者に伝達する。	5g-5.34.2	組織は、プライバシー及びPII の保護のための手順を策定し、実施する。	予防に関連記載あり			
18.1.4.3	プライバシー及びPII の保護に関する組織の方針の順守、並びに人々のプライバシーの保護及びPII の保護に関する全ての法令及び規制の順守のために、適切な管理構造及び管理策を確立する。	5g-5.34.4	組織は、プライバシー及びPII の保護のために策定した手順の順守、並びにプライバシー及びPII の保護に関する全ての法令及び規制の順守のために、適切な役割、責任及び管理策を整備する。	予防に関連記載あり	5.34.2	プライバシー及びPII の保護に関する全ての法令及び規制の順守のための役割及び責任を割り当てる。	組織は、プライバシー及びPII の保護のために策定した手順の順守、並びにプライバシー及びPII の保護に関する全ての法令及び規制の順守のために、適切な役割、責任及び管理策を整備する。 プライバシー及びPII の保護に関する責任者は、審査、サービス提供者及びその他の利害関係者に対して、それぞれの責任及び従って行うことが望ましい特定の手順について、手引を提供する。多くの場合、例えば、プライバシー担当役員のような一人の責任者を任命することによって最も達成される。 PIIの取扱いについての責任は、関連する法令及び規制を考慮に入れて処置する。
18.1.4.4	プライバシー及びPII の保護の責任者（例えば、プライバシー担当役員）は、管理者、利用者及びサービス提供者に対して、それぞれの責任及び従うことが望ましい特定の手順について、手引を提供する。	5g-5.34.5	プライバシー及びPII の保護に関する責任者は、審査、サービス提供者及びその他の利害関係者に対して、それぞれの責任及び従うことが望ましい特定の手順について、手引を提供する。	予防に関連記載あり			
18.1.4.5	PII の取扱い、及びプライバシーの原則の処置を確実にすることについての責任は、関連する法令及び規制に従って処置する。	5g-5.34.6	PIIの取扱いについての責任は、関連する法令及び規制を考慮に入れて処置する。	予防に関連記載あり			
18.1.4.6	PII を保護するための適切な技術的及び組織的対策を実施する。	5g-5.34.7	PIIを保護するための適切な技術的及び組織的対策を実施する。	予防に関連記載あり			
18.1.5	暗号化機能に対する規制 暗号化機能は、関連する全ての協定、法令及び規制を順守して用いる。	5.31	法令、規制及び契約上の要求事項 管理策 情報セキュリティに関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組を特定し、文書化し、また、最新に保つ。 目的 情報セキュリティに関連する法令、規制及び契約上の要求事項の順守を確実にするため。		5.31	法令、規制及び契約上の要求事項 統制目標：情報セキュリティに関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組を特定し、文書化し、また、最新に保つ。 目的：情報セキュリティに関連する法令、規制及び契約上の要求事項の順守を確実にするため。	
18.1.5.1	関連する協定、法令及び規制を順守するため、暗号機能を実行するためのコンピュータのハードウェア及びソフトウェアの、輸入又は輸出に関する規制を順守する。	5g-5.31.3	暗号化は、次の項目に関連する合意、法令及び規制の順守を考慮に入れる。 a) 暗号機能を実行するためのコンピュータのハードウェア及びソフトウェアの、輸入又は輸出に関する規制	予防に関連記載あり	5.31.2	暗号化に関連する合意、法令及び規制における要求事項への順守を確実にするための手順を整備する。	暗号化は、次の項目に関連する合意、法令及び規制の順守を考慮に入れる。 a) 暗号機能を実行するためのコンピュータのハードウェア及びソフトウェアの、輸入又は輸出に関する規制 b) 暗号機能を追加するように設計されているコンピュータのハードウェア及びソフトウェアの、輸入又は輸出に関する規制 c) 暗号利用に関する規制 d) 暗号化された情報への、国の当局による強制的又は任意的アクセス方法 e) ディジタル署名、eシール及びディジタル証明書の有効性 暗号化は、多くの場合、国外の法的要求事項をも つ分野である。関連する法令及び規制の順守を確実にするために、特に暗号化された情報又は暗号化ツールを法域の境界を越えて転送する場合、法的な助言を求めることが推奨される。
18.1.5.2	関連する協定、法令及び規制を順守するため、暗号機能を追加するように設計されているコンピュータのハードウェア及びソフトウェアの、輸入又は輸出に関する規制を順守する。	5g-5.31.3	暗号化は、次の項目に関連する合意、法令及び規制の順守を考慮に入れる。 b) 暗号機能を追加するように設計されているコンピュータのハードウェア及びソフトウェアの、輸入又は輸出に関する規制	予防に関連記載あり			
18.1.5.3	関連する協定、法令及び規制を順守するため、暗号利用に関する規制を順守する。	5g-5.31.3	暗号化は、次の項目に関連する合意、法令及び規制の順守を考慮に入れる。 c) 暗号利用に関する規制	予防に関連記載あり			
18.1.5.4	関連する協定、法令及び規制を順守するため、内容の機密性を守るためにハードウェア又はソフトウェアによって暗号化された情報への、国の当局による強制的又は任意的アクセス方法を定める。	5g-5.31.3	暗号化は、次の項目に関連する合意、法令及び規制の順守を考慮に入れる。 d) 暗号化された情報への、国の当局による強制的又は任意的アクセス方法	予防に関連記載あり			
18.1.5.5	関連する法令及び規制の順守を確実にするために、法的な助言を求める。	(5g-5.31.3参考2)	関連する法令及び規制の順守を確実にするために、特に暗号化された情報又は暗号化ツールを法域の境界を越えて転送する場合、法的な助言を求めることが推奨される。	予防に関連記載あり			
18.1.5.6	暗号化された情報又は暗号制御機能を、法域を越えて持ち出す前に、法的な助言を受ける。	(5g-5.31.3参考2)	【再】関連する法令及び規制の順守を確実にするために、特に暗号化された情報又は暗号化ツールを法域の境界を越えて転送する場合、法的な助言を求めることが推奨される。	予防に関連記載あり			
–	（対応項なし）	5g-5.31.4	情報セキュリティに関する契約上の要求事項には、次のものに起因されている要求事項を含む。 a) 顧客との契約 b) 供給者との契約 c) 保険契約	予防に関連記載あり	5.31.1	【再】組織の情報セキュリティに関連する全ての法令及び規制を特定し、自らの事業の種類に対する要求事項を特定し、維持する。	(5.31.1に対応する項を参照)
18.1.5.7.PB	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	5.31.7	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
18.2	情報セキュリティのレビュー 管理目的：組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。	5.35	情報セキュリティの独立したレビュー 管理策 人、プロセス及び技術を含む、情報セキュリティ及びその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。 目的 組織における情報セキュリティ管理の取組の、継続的な適切性、十分性及び有効性を確実にするため。		5.35	情報セキュリティの独立したレビュー 統制目標：人、プロセス及び技術を含む、情報セキュリティ及びその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。 目的：組織における情報セキュリティ管理の取組の、継続的な適切性、十分性及び有効性を確実にするため。	
18.2.1	情報セキュリティの独立したレビュー 情報セキュリティ及びその実施の管理（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）に対する組織の取組について、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。						
18.2.1.1	経営陣は、情報セキュリティをマネジメントする組織の取組みが、引き続き適切、妥当及び有効であることを確実にするために、独立したレビューを実施し、実施させる。	5g-5.35.1	組織は、情報セキュリティの独立したレビューを実施するための プロセスをも つ。	予防に関連記載あり	5.35.1	情報セキュリティの定期的な独立したレビュー計画に、実施する。	組織は、情報セキュリティの独立したレビューを実施するための プロセスをも つ。 管理策は、情報セキュリティの定期的な独立したレビュー計画に、実施する。 情報セキュリティの独立したレビューは、情報セキュリティ方針、トピック固有の方針、及びその他の管理策を含む、情報セキュリティの取組の改善の機会及び変更の必要性の評価を含む。 情報セキュリティの定期的な独立したレビューに加えて、組織は次の場合にも、独立したレビューの実施を検討する。 a) 組織に影響する法令及び規制が変わる。 b) 重大なインシデントが生じる。 c) 組織が新しい事業を開始する、又は現在の事業を変更する。 d) 組織が新しい製品若しくはサービスの利用を開始する、又は現在の製品若しくはサービスの利用を変更する。 e) 組織が情報セキュリティの管理策及び手順を大幅に変更する。
–	（対応項なし）	5g-5.35.2	管理職は、情報セキュリティの定期的な独立したレビューを計画し、実施する。	予防に関連記載あり			
18.2.1.2	独立したレビューは、改善の機会のアセスメントを含める。	5g-5.35.3	情報セキュリティの独立したレビューは、情報セキュリティ方針、トピック固有の方針、及びその他の管理策を含む、情報セキュリティの取組の改善の機会及び変更の必要性の評価を含む。	予防に関連記載あり			
18.2.1.3	独立したレビューは、方針及び管理目的を含む セキュリティの取組みの変更について、その必要性の評価を含める。	5g-5.35.3	【再】情報セキュリティの独立したレビューは、情報セキュリティ方針、トピック固有の方針、及びその他の管理策を含む、情報セキュリティの取組の改善の機会及び変更の必要性の評価を含む。	予防に関連記載あり			
–	（対応項なし）	5g-5.35.10	情報セキュリティの定期的な独立したレビューに加えて、組織は次の場合にも、独立したレビューの実施を検討する。 a) 組織に影響する法令及び規制が変わる。 b) 重大なインシデントが生じる。 c) 組織が新しい事業を開始する、又は現在の事業を変更する。 d) 組織が新しい製品若しくはサービスの利用を開始する、又は現在の製品若しくはサービスの利用を変更する。 e) 組織が情報セキュリティの管理策及び手順を大幅に変更する。	予防に関連記載あり			
18.2.1.4	独立したレビューは、レビュー対象の領域から独立した個人・組織（例えば、内部監査の担当部署、独立した管理者、このようなレビューを専門に行う外部関係者）が実施する。	5g-5.35.4	情報セキュリティの独立したレビューは、レビューの対象となる領域から独立した個人・組織が実施する。	予防に関連記載あり	5.35.2	情報セキュリティの独立したレビューを実施する個人・組織は、レビューの対象となる領域から独立した個人・組織（例えば、内部監査の担当部署、独立した管理者、このようなレビューを専門に行う外部関係者）が実施する。 情報セキュリティの独立したレビューを実施する個人・組織は、適切な力量をもつ。 情報セキュリティの独立したレビューを実施する個人は、評価を行うこと で独立性をもつことを確実にするため、権限をもつ系統に属さない。	情報セキュリティの独立したレビューは、レビューの対象となる領域から独立した個人・組織（例えば、内部監査の担当部署、独立した管理者、このようなレビューを専門に行う外部関係者）が実施する。
18.2.1.5	独立したレビューは、適切な技能及び経験をもつ個人・組織が実施する。	5g-5.35.5	情報セキュリティの独立したレビューを実施する個人・組織は、適切な力量をもつ。	予防に関連記載あり			
18.2.1.6	独立したレビューの結果は、記録し、レビューを実施した経営陣に報告する。	5g-5.35.7	情報セキュリティの独立したレビューの結果は、レビューを実施した管理職、及び、適切な場合には、トップマネジメントに報告する。	予防に関連記載あり	5.35.3	独立したレビューの結果は、レビューを実施した管理職及び適切な場合には、トップマネジメントに報告する。 情報セキュリティの独立したレビューの記録は、維持する。	情報セキュリティの独立したレビューの結果は、レビューを実施した管理職、及び、適切な場合には、トップマネジメントに報告する。 情報セキュリティの独立したレビューの記録は、維持する。
18.2.1.7	独立したレビューの結果の記録は、維持する。	5g-5.35.8	情報セキュリティの独立したレビューの記録は、維持する。	予防に関連記載あり			
18.2.1.8	独立したレビューにおいて、情報セキュリティマネジメントに対する組織の取組及び実施が十分でない（例えば、文書化した目的及び要求事項が、情報セキュリティのための方針に記載された情報セキュリティに関する方向付けを満たしていない、又はこれと適合していない）ことが明確になった場合には、経営陣は是正処置の検討を指示する。	5g-5.35.9	情報セキュリティの独立したレビューにおいて、情報セキュリティマネジメントに対する組織の取組及び実施が十分でない場合には管理職は是正処置を指示する。	予防に関連記載あり	5.35.4	独立したレビューにおいて、情報セキュリティマネジメントに対する組織の取組及び実施が十分でない場合には管理職は是正処置を指示する。	情報セキュリティの独立したレビューにおいて、情報セキュリティマネジメントに対する組織の取組及び実施が十分でない【例えば、文書化した目的及び要求事項が、情報セキュリティ方針及びトピック固有の方針（5.1参照）に記載された情報セキュリティに関する方向付けを満たしていない、又はこれを順守していない。】ことが明確になった場合には、管理職は是正処置を実施する。
18.2.1.9.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	5.35.5	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
18.2.1.10.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	5.35.6	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
18.2.1.11.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	5.35.7	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
18.2.1.12.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	5.35.8	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
18.2.1.13.P	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	–	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	管理策に関連記載あり（情報セキュリティ管理基準以外の由来）	5.35.9	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した手引き）
18.2.2	情報セキュリティのための方針群及び標準の順守 管理者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューする。	5.36	情報セキュリティのための方針群、規則及び標準の順守 管理策 組織の情報セキュリティ方針、トピック固有の方針、規則及び標準を順守していることを定期的にレビューする。 目的 情報セキュリティを、組織の情報セキュリティ方針、トピック固有の方針、規則及び標準に従って実施し、運用することを確実にするため。		5.36	情報セキュリティのための方針群、規則及び標準の順守 統制目標：組織の情報セキュリティ方針、トピック固有の方針、規則及び標準を順守していることを定期的にレビューする。 目的：情報セキュリティを、組織の情報セキュリティ方針、トピック固有の方針、規則及び標準に従って実施し、運用することを確実にするため。	
18.2.2.1	管理者は、方針、標準類及びその他適用される規則で定められた情報セキュリティ要求事項が満たされていることをレビューするための方法を特定する。	5g-5.36.1	管理者及びサービス、製品又は情報の管理責任者は、情報セキュリティ方針、トピック固有の方針、規則、標準及びその他適用される規則で定められた情報セキュリティ要求事項が満たされていることをレビューする方法を特定する。	予防に関連記載あり	5.36.1	管理者及びサービス、製品又は情報の管理責任者による、情報セキュリティ要求事項が満たされていることをレビューする方法を定める。	管理者及びサービス、製品又は情報の管理責任者は、情報セキュリティ方針、トピック固有の方針、規則、標準及びその他適用される規則で定められた情報セキュリティ要求事項が満たされていることをレビューする方法を特定する。 定めに従って効率的にレビューを行うため、自動的な測定ツール及び報告ツールの使用を考慮する。
18.2.2.2	管理者は定めに従って効率的にレビューを行うため、自動的な測定ツール及び報告ツールを使用する。	5g-5.36.2	定めに従って効率的に情報セキュリティのレビューを行うため、自動的な測定ツール及び報告ツールの使用を考慮する。	予防に関連記載あり			
18.2.2.3	管理者による レビューの結果、何らかの不順守を検出した場合、管理者は、不順守の原因を特定する。	5g-5.36.3	情報セキュリティのレビューの結果、何らかの不順守を検出した場合、管理者は、次の事項を行う。 a) 不順守の原因を特定する。	予防に関連記載あり	5.36.3	レビューの結果、不順守を検出した場合、是正処置を実施する。	情報セキュリティのレビューの結果、何らかの不順守を検出した場合、管理者は、次の事項を行う。 a) 不順守の原因を特定する。 b) 順守を達成するための是正処置の必要性を評価する。 c) 適切な是正処置を実施する。 d) 是正処置の有効性を検証し、不備又は弱点を特定するために、講じた是正処置をレビューする。 情報セキュリティ要求事項の不順守に対する是正処置は、リスクに対して適切に、時機を失すること なく実施する。 次に不定している情報セキュリティのレビューまで に完了しない場合、そのレビュー時に少なくとも進捗状況を取り上げる。
18.2.2.4	管理者による レビューの結果、何らかの不順守を検出した場合、管理者は、順守を達成するための処置の必要性を評価する。	5g-5.36.3	情報セキュリティのレビューの結果、何らかの不順守を検出した場合、管理者は、次の事項を行う。 b) 順守を達成するための是正処置の必要性を評価する。	予防に関連記載あり			
18.2.2.5	管理者による レビューの結果、何らかの不順守を検出した場合、管理者は、適切な是正処置を実施する。	5g-5.36.3	情報セキュリティのレビューの結果、何らかの不順守を検出した場合、管理者は、次の事項を行う。 c) 適切な是正処置を実施する。	予防に関連記載あり			
18.2.2.6	管理者による レビューの結果、何らかの是正処置を実施した場合、管理者は、是正処置の有効性を検証し、不備又は弱点を特定するために、とった是正処置をレビューする。	5g-5.36.3	情報セキュリティのレビューの結果、何らかの不順守を検出した場合、管理者は、次の事項を行う。 d) 是正処置の有効性を検証し、不備又は弱点を特定するために、講じた是正処置をレビューする。	予防に関連記載あり			
18.2.2.7	管理者が実施したレビュー及び是正処置の結果を記録する。また、その記録を維持・管理する。	5g-5.36.4	管理者及びサービス、製品又は情報の管理責任者が実施した情報セキュリティのレビュー及び是正処置の結果を記録し、また、その記録を維持管理する。	予防に関連記載あり	5.36.2	管理者及びサービス、製品又は情報の管理責任者が実施したレビュー及び是正処置の結果を記録し、また、その記録を維持管理する。 管理者の責任範囲に対して、情報セキュリティの独立したレビュー（5.35参照）が実施されるとき は、管理者は、独立したレビュー実施者に対して、その結果を報告する。	管理者及びサービス、製品又は情報の管理責任者が実施したレビュー及び是正処置の結果を記録し、また、その記録を維持管理する。 管理者の責任範囲に対して、情報セキュリティの独立したレビュー（5.35参照）が実施されるとき は、管理者は、独立したレビュー実施者に対して、その結果を報告する。
18.2.2.8	管理者の責任範囲に対して、独立したレビューが実施されるとき は、管理者は、独立したレビュー実施者に対して、レビュー及び是正処置の結果を報告する。	5g-5.36.5	管理者の責任範囲に対して、情報セキュリティの独立したレビューが実施されるとき は、管理者は、独立したレビュー実施者に対して、その結果を報告する。	予防に関連記載あり			
18.2.3	技術的順守のレビュー 情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューする。	8.8	技術的ぜい弱性の管理 管理策 利用中の情報システムの技術的ぜい弱性に関する情報を獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価し、適切な手段をとる。 目的 技術的ぜい弱性の悪用を防止するため。		8.8	技術的ぜい弱性の管理 統制目標：利用中の情報システムの技術的ぜい弱性に関する情報を獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価し、適切な手段をとる。 目的：技術的ぜい弱性の悪用を防止するため。	
18.2.3.1	技術的順守は、技術専門家が後に解釈するための技術レポートを生成する自動ツールを活用してレビューする。	5g-5.36.2	【再】定めに従って効率的に情報セキュリティのレビューを行うため、自動的な測定ツール及び報告ツールの使用を考慮する。	予防に関連記載あり	5.36.1	【再】管理者及びサービス、製品又は情報の管理責任者による、情報セキュリティ要求事項が満たされていることをレビューする方法を定める。	(5.36.1に対応する項を参照)
18.2.3.2	技術的順守は、自動ツールの活用に代わるものとして、経験をもつシステムエンジニアが手動で（必要な場合には、適切なソフトウェアツールの助けを得て）レビューする。	–	（直接対応する詳細管理策無し）	明確な対応関係なし（情報セキュリティ管理基準で継承されず）	–	（対応項なし）	–
18.2.3.3	侵入テスト又はぜい弱性アセスメントを用いる場合、このような作業は、システムのセキュリティを危うくするおそれがないように注意する。	8b-8.8.3	【再】技術的ぜい弱性を特定するために、組織は次の事項を考慮する。 a) ぜい弱性の特定を支援するために、力量が必要かどうかを判断する。	予防に関連記載あり	8.8.1	【再】技術的ぜい弱性を特定し、評価する。	(8.8.1に対応する項を参照)
18.2.3.4	侵入テスト又はぜい弱性アセスメントは、計画し、文書化し、また、繰り返し実施するだけでなく、新たな ぜい弱性が導入された、顕著なされた場合にも実施する。			予防に関連記載あり			
18.2.3.5	いかなる技術的順守のレビューも、力量があり、認可されている者によって、又はその者の監督の下で行う、実施する。			予防に関連記載あり			
–	（対応項なし）	–	機能インテリジェンス 管理策 情報セキュリティの機能に関連する情報を収集及び分析し、機能インテリジェンスを構築することが望ましい。 目的 適切なリスク低減処置を講じることが可能となるように、組織の機能環境についての認識をもつため。		5.7	機能インテリジェンス 統制目標：情報セキュリティの機能に関連する情報を収集及び分析し、機能インテリジェンスを構築する。 目的：適切なリスク低減処置を講じることが可能となるように、組織の機能環境についての認識をもつため。	
–	（対応項なし）	5a-5.7.1	既存の又は新たな機能に関する情報を、次の目的で収集し、分析する。 a) 機能が組織に危害を及ぼすことを防止するために、十分な情報に基づく改善を支援する。 b) 機能の影響を減らす。	予防に関連記載あり	5.7.1	既存の又は新たな機能に関する情報を収集及び分析するための目的を定める。	既存の又は新たな機能に関する情報を、次の目的で収集し、分析する。 a) 機能が組織に危害を及ぼすことを防止するために、十分な情報に基づく改善を支援する。 b) 機能の影響を減らす。 機能インテリジェンスは2面に分けることができ、これらの全てを考慮する。

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
–	（対応項なし）	Sa-5.7.2	脅威インテリジェンスを構成する次の3種全てを考慮する。 a）戦略的脅威インテリジェンス：脅威の動向に関する大局的な情報の交換 b）戦術的脅威インテリジェンス：攻撃者が使う手法、ツール及び技術に関する情報の交換 c）運用上の脅威インテリジェンス：技術的特徴を含む特定の攻撃に関する詳細	予防に関連記載あり			a）戦略的脅威インテリジェンス：変化する脅威の状況に関する高レベルの情報の交換（例えば、攻撃者の種類又は攻撃の種類） b）戦術的脅威インテリジェンス：攻撃者が使う手法、ツール及び技術に関する情報の交換 c）運用上の脅威インテリジェンス：技術的特徴を含む特定の攻撃に関する詳細 脅威インテリジェンスの構築に必要な情報を提供するために必要かつ適切な情報源を特定し、呼吸し、選択する。
–	（対応項なし）	Sa-5.7.3	脅威インテリジェンスは、次の事項を満たす。 a）課題に応える（すなわち、組織の保護に関係する。）。 b）十分な情報を含む（すなわち、脅威の状況に関する正確かつ詳細な理解を組織に提供する。）。 c）状況認識を与えるような状況情報を含む（すなわち、事象の発生時間、場所、以前の経験及び同種の組織における傾向によって、情報に状況を加える。）。 d）対応可能である（すなわち、組織が情報に基づいて迅速かつ効果的に対応可能である。）。	予防に関連記載あり	S.7.2	目的を達成するために必要なインテリジェンス要件を定める。	脅威インテリジェンスは、次の事項を満たす。 a）課題に応える（すなわち、組織の保護に関係する。）。 b）十分な情報を含む（すなわち、脅威の状況に関する正確かつ詳細な理解を組織に提供する。）。 c）状況認識を与えるような状況情報を含む（すなわち、事象の発生時間、場所、以前の経験及び同種の組織における傾向によって、情報に状況を加える。）。 d）対応可能である（すなわち、組織が情報に基づいて迅速かつ効果的に対応可能である。）。
–	（対応項なし）	Sa-5.7.4	脅威インテリジェンス活動は、次の事項を含む。 a）脅威インテリジェンスの構築の目的を確立する。 b）脅威インテリジェンスの構築に必要な情報を提供するために必要かつ適切な内部及び外部の情報源を特定し、呼吸し、選択する。 c）内部及び外部のいずれにおよび、精選した情報源から情報を収集する。 d）収集した情報を、分析に備えて処理する。 e）情報を、それが組織にどのように関係し、意味をもつかを理解するために分析する。 f）関係する個人に分析した結果を理解可能な形式で伝達した。	予防に関連記載あり	S.7.3	脅威インテリジェンス活動を実施する。	脅威インテリジェンス活動は、次の事項を含む。 a）脅威インテリジェンスの構築の目的を確立する。 b）脅威インテリジェンスの構築に必要な情報を提供するために必要かつ適切な内部及び外部の情報源を特定し、呼吸し、選択する。 c）内部及び外部のいずれにおよび、精選した情報源から情報を収集する。 d）収集した情報を、分析に備えて処理する（例えば、情報を変換、形式化、又は集約けることによる）。 e）情報を、それが組織にどのように関係し、意味をもつかを理解するために分析する。 f）関係する個人に分析した結果を理解可能な形式で伝達した。共有する。 次の観点で分析し、組織が必要とする適切かつ低減処理を講じるために使用する。 a）脅威インテリジェンスの情報源から収集した情報を組織の情報セキュリティリスクマネジメントプロセスに反映する必要性があるか否か。 b）ファイアウォール、侵入検知システム、マルウェア対策ソリューションなどの技術的な予防及び検知の管理策への追加の考慮事項とすべきか否か。 c）情報セキュリティリスクのプロセス及び手法への考慮事項とすべきか否か。 組織は、脅威インテリジェンス全体を改善するために、脅威インテリジェンスを他の組織と相互に共有する。
–	（対応項なし）	Sa-5.7.5	脅威インテリジェンスを分析し、次のために使用する。 a）脅威インテリジェンスの情報源から収集した情報を組織の情報セキュリティリスクマネジメントプロセスに良めるプロセスを実施することによって、 b）ファイアウォール、侵入検知システム、マルウェア対策ソリューションなどの技術的な予防及び検知の管理策への追加の入力として、 c）情報セキュリティリスクのプロセス及び手法への入力として。	予防に関連記載あり			
–	（対応項なし）	Sa-5.7.6	組織は、脅威インテリジェンス全体を改善するために、脅威インテリジェンスを他の組織と相互に共有する。	予防に関連記載あり			
–	（対応項なし）	S.23	クラウドサービスの利用における情報セキュリティ 管理策 クラウドサービスの調達、利用、管理及び利用終了のプロセスを、組織の情報セキュリティ要求事項に従って確立することが望ましい。 目的 クラウドサービスの利用における情報セキュリティを規定し、管理するため。		S.23	クラウドサービスの利用における情報セキュリティ 統制目標：クラウドサービスの調達、利用、管理及び利用終了のプロセスを、組織の情報セキュリティ要求事項に従って確立する。 目的：クラウドサービスの利用における情報セキュリティを規定し、管理するため。	
–	（対応項なし）	Sd-5.23.1	組織はクラウドサービスの利用に関するトピック固有の方針を確立し、全ての関連する利害関係者に伝達する。	予防に関連記載あり	S.23.1	ビアクラウドサービスの調達・利用・管理及び利用終了に関する方針を策定する。	組織はクラウドサービスの利用に関するトピック固有の方針を確立し、全ての関連する利害関係者に伝達する。 組織は、クラウドサービスの利用に伴う情報セキュリティリスクを管理する方法を定め、伝達する。これは、外部関係者が提供するサービス、組織が管理する方法の既存の取組の拡張又はその一部である可能性がある（5.21及び5.22参照）。
–	（対応項なし）	Sd-5.23.2	組織は、クラウドサービスの利用に伴う情報セキュリティリスクを管理する方法を定め、伝達する。	予防に関連記載あり			
–	（対応項なし）	Sd-5.23.3	組織は次の事項を定義する。 a）クラウドサービスの利用に伴う全ての関係する情報セキュリティ要求事項 b）クラウドサービスの選定基準及びクラウドサービスを利用の範囲 c）クラウドサービスの利用及び管理に関する役割及び責任 d）どの情報セキュリティ管理策をクラウドサービスプロバイダが管理し、どの情報セキュリティ管理策をクラウドサービスカスタマとしての組織が管理するか。 e）クラウドサービスプロバイダが提供する情報セキュリティ機能を取得し、利用する方法 f）クラウドサービスプロバイダが実施する情報セキュリティ管理策に関して提供を得る方法 g）組織が複数のクラウドサービス、特に異なるクラウドサービスプロバイダのクラウドサービスを利用する場合に、管理策、インタフェース及びサービスの変更を管理する方法 h）クラウドサービスの利用に関連して発生する情報セキュリティインシデントを取り扱うための手順 i）情報セキュリティリスクを管理するため、クラウドサービスの継続的な利用性を監視し、レビューし、評価する組織の取組 j）クラウドサービスの出口戦略を含め、クラウドサービスの利用を変更又は停止する方法	予防に関連記載あり	S.23.2	ビアクラウドサービスの利用に伴う情報セキュリティ要求事項を定義する。	組織は次の事項を定義する。 a）クラウドサービスの利用に伴う全ての関係する情報セキュリティ要求事項 b）クラウドサービスの選定基準及びクラウドサービスを利用の範囲 c）クラウドサービスの利用及び管理に関する役割及び責任 d）どの情報セキュリティ管理策をクラウドサービスプロバイダが管理し、どの情報セキュリティ管理策をクラウドサービスカスマとしての組織が管理するか。 e）クラウドサービスプロバイダが提供する情報セキュリティ機能を取得し、利用する方法 f）クラウドサービスプロバイダが実施する情報セキュリティ管理策に関して提供を得る方法 g）組織が複数のクラウドサービス、特に異なるクラウドサービスプロバイダのクラウドサービスを利用する場合に、管理策、インタフェース及びサービスの変更を管理する方法 h）クラウドサービスの利用に関連して発生する情報セキュリティインシデントを取り扱うための手順 i）情報セキュリティリスクを管理するため、クラウドサービスの継続的な利用性を監視し、レビューし、評価する組織の取組 j）クラウドサービスの出口戦略を含め、クラウドサービスの利用を変更又は停止する方法 取り扱う情報の格付及び取扱制限並びにクラウドサービス提供者との情報セキュリティに関する役割及び責任の範囲を踏まえて、クラウドサービスに求める情報セキュリティ対策を含むセキュリティ要件を定めること。 クラウドサービスの利用は、クラウドサービスプロバイダ、クラウドサービスカスタマである組織との間の、情報セキュリティに関する責任の共有及び分担、並びに共同作業を伴う可能性がある。クラウドサービスプロバイダ、クラウドサービスカスタマである組織との両方の責任を適切に定義し、実践することが不可欠である。
–	（対応項なし）	Sd-5.23.4	クラウドサービスの合意は、場合性、完全性、可用性及び情報の取扱いについての組織の要求事項、並びに、適切なクラウドサービスレベル目標及びクラウドサービスの定性的目標に言及する。	予防に関連記載あり	S.23.3	定義された、ビアクラウドサービスの利用に伴う情報セキュリティ要求事項を踏まえ、合意をする。	クラウドサービスの合意は、多くの場合、事前に定義されており、交渉の余地はないことを踏まえ、全てのクラウドサービスについて、組織は、クラウドサービスプロバイダのクラウドサービスの合意をレビューする。 クラウドサービスの合意は、機密性、完全性、可用性及び情報の取扱いについての組織の要求事項、並びに、適切なクラウドサービスレベル目標及びクラウドサービスの定性的目標に言及する。 組織は、クラウドサービスの利用に関連するリスクを特定するために、関連するリスクアセスメントを実施する。 クラウドサービスの利用に関連する残留リスクは、組織の適切な管理層が明確に特定し、受容する。 クラウドサービスプロバイダ、クラウドサービスカスマである組織との間の合意は、組織のデータ及びサービスの可用性を保護するために次の規定を含む。 a）アーキテクチャ及びインフラストラクチャに関する業界で認められた標準に基づくソリューションを提供する。 b）組織の要求事項を満たすためにクラウドサービスのアクセス制御を管理する。 c）マルウェア監視及び脅威ソリューションを実装する。 d）組織の取扱いに懸念を要する情報を、承認されている場所（例えば、特定の国又は地域）、又は特定の法域内若しくは特定の裁判権の下で処理し、保存する。 e）クラウドサービス環境で情報セキュリティインシデントが発生した場合に専用の支援を提供する。 f）クラウドサービスが、更に外部の供給者へ下請負契約がいている場合に、組織の情報セキュリティ要求事項が満たされることを確実にする（又はクラウドサービスの下請負を禁止する。）。 g）異なる法域にわたるデジタル経営に関する法令及び規則を考慮して、デジタル経営を収集する際に組織を支援する。 h）組織がクラウドサービスの利用を終了したいとき、適切な期間にわたって、適切な支援及びサービスを提供する。 i）クラウドサービスカスタマである組織が利用するクラウドサービスプロバイダが提供する機能に基づいて、該当する場合に、データ及び構成情報の安全なバックアップを提供し、セキュリティを保った方法でバックアップを管理する。 j）サービスの提供又はサービスの終了時に組織が要求する場合、クラウドサービスカスマである組織が所有する構成ファイル、ソースコード、データなどの情報を提出し、返却する。
–	（対応項なし）	Sd-5.23.5	組織は、クラウドサービスの利用に関連するリスクを特定するために、関連するリスクアセスメントを実施する。	予防に関連記載あり			
–	（対応項なし）	Sd-5.23.6	クラウドサービスの利用に関連する残留リスクは、組織の適切な管理層が明確に特定し、受容する。	予防に関連記載あり			
–	（対応項なし）	Sd-5.23.7	クラウドサービスプロバイダ、クラウドサービスカスマである組織との間の合意は、組織のデータ及びサービスの可用性を保護するために次の規定を含む。 a）アーキテクチャ及びインフラストラクチャに関する業界で認められた標準に基づくソリューションを提供する。 b）組織の要求事項を満たすためにクラウドサービスのアクセス制御を管理する。 c）マルウェア監視及び脅威ソリューションを実装する。 d）組織の取扱いに懸念を要する情報を、承認されている場所（例えば、特定の国又は地域）、又は特定の法域内若しくは特定の裁判権の下で処理し、保存する。 e）クラウドサービス環境で情報セキュリティインシデントが発生した場合に専用の支援を提供する。 f）クラウドサービスが、更に外部の供給者へ下請負契約がいている場合に、組織の情報セキュリティ要求事項が満たされることを確実にする（又はクラウドサービスの下請負を禁止する。）。 g）異なる法域にわたるデジタル経営に関する法令及び規則を考慮して、デジタル経営を収集する際に組織を支援する。 h）組織がクラウドサービスの利用を終了したいとき、適切な期間にわたって、適切な支援及びサービスを提供する。 i）クラウドサービスカスタマが利用するクラウドサービスプロバイダが提供する機能に基づいて、該当する場合に、データ及び構成情報の安全なバックアップを提供し、セキュリティを保った方法でバックアップを管理する。 j）サービスの提供又はサービスの終了時に組織が要求する場合、クラウドサービスカスマである組織が所有する構成ファイル、ソースコード、データなどの情報を提出し、返却する。 クラウドサービスを利用する組織は、クラウドサービスプロバイダ（又は）製造元連絡を維持する。こうした連絡によって、クラウドサービスプロバイダ（又はクラウドサービスカスマである組織との両方が各サービスの特性を監視し、合意に含まれるコントロールの不履行を最小化する組みを良め、クラウドサービスの利用について情報セキュリティに関する情報の相互交換が 可能になる。	クラウドサービスカスマである組織は、組織へのサービス提供方法に対して、実現的に顧客に影響を与える変更を行う前にクラウドサービスプロバイダ（又はクラウドサービスプロバイダ）が事前に通知することを合意において要求することが望ましいかどうかを、次の事項を良めて考慮する。 a）クラウドサービスの提供に影響するか又はそれを変更するような技術インフラストラクチャの変更 b）新しい地理的又は法的区域での情報の処理又は保存 c）ビアクラウドサービスプロバイダ（又はその他の下請負業者の利用（既存の業者の変更又は新しい業者の利用を含む。）
–	（対応項なし）	Sd-5.23.9	クラウドサービスを利用する組織は、クラウドサービスプロバイダ（又）製造元連絡を維持する。	予防に関連記載あり			
–	（対応項なし）	Sd-5.23.8	クラウドサービスカスマである組織は、組織へのサービス提供方法に対して、実現的に顧客に影響を与える変更を行う前にクラウドサービスプロバイダ（又）事前に通知することを合意において要求することが望ましいかどうかを、次の事項を良めて考慮する。 a）クラウドサービスの提供に影響するか又はそれを変更するような技術インフラストラクチャの変更 b）新しい地理的又は法的区域での情報の処理又は保存 c）ビアクラウドサービスプロバイダ（又はその他の下請負業者の利用（既存の業者の変更又は新しい業者の利用を含む。）	予防に関連記載あり	S.23.4	ビアクラウドサービスプロバイダから自組織へのサービス提供方法に対して、実現的にクラウドサービス利用者に影響を与える変更を行う前にビアクラウドサービスプロバイダ（又）事前に通知することを合意において要求することを検討し、記録に残す。	クラウドサービスカスマである組織は、組織へのサービス提供方法に対して、実現的に顧客に影響を与える変更を行う前にクラウドサービスプロバイダ（又）事前に通知することを合意において要求することが望ましいかどうかを、次の事項を良めて考慮する。 a）クラウドサービスの提供に影響するか又はそれを変更するような技術インフラストラクチャの変更（例えば、再配置、再構成、又はハードウェア若しくはソフトウェアの変更） b）新しい地理的又は法的区域での情報の処理又は保存 c）ビアクラウドサービスプロバイダ又はその他の下請負業者の利用（既存の業者の変更又は新しい業者の利用を含む。）
–	（対応項なし）	S.30	事業継続のための次の備え 管理策 事業継続の目的及びICT継続の要求事項に基づいて、ICTの備えを計画し、実施し、維持し、試験することが望ましい。 目的 事業の中断・阻害時に組織の情報及びその他の関連資産の可用性を確実にするため。		S.30	事業継続のためのICTの備え 統制目標：事業継続の目的及びICT継続の要求事項に基づいて、ICTの備えを計画し、実施し、維持し、試験する。 目的：事業の中断・阻害時に組織の情報及びその他の関連資産の可用性を確実にするため。	
–	（対応項なし）	SF-5.30.1	ICT継続の要求事項を、事業影響度分析（BIA）の結果をもとに規定する場合、そのBIA及びセスでは、影響の種類及び評価基準を用いて、製品及びサービスを提供する事業活動の中断・阻害から生じる影響を経時的に評価する。	予防に関連記載あり	S.30.1	事業継続の目的及びICT継続の要求事項に基づいて、ICTの備えを計画する。	事業継続に関するICTの備えは、事業の中断・阻害時にも組織の目的が継続して満たされることを確実にするため、事業継続マネジメント及び情報セキュリティマネジメントの重要な構成要素である。 ICT継続の要求事項を、事業影響度分析（BIA）の結果をもとに規定する場合、その BIA プロセスは、影響の種類及び評価基準を用いて、製品及びサービスを提供する事業活動の中断・阻害から生じる影響を経時的に評価する。 事業の中断・阻害の結果として生じる影響の大きさ及び期間を用いて優先する活動を特定し、これに目標復旧時間（RTO）を設定した後、BIAでは、優先する活動の支援にどの資源が必要かを決定する。 優先する事業活動を支援する資源にもRTOを定め、これらの資源に の一部としてICTサービスを良める。 ICTサービスに係るBIAを記憶して、事業の中断・阻害時の活動を支援するため、必要な、ICTシステムのパフォーマンス、容量・能力の要求事項、及び情報の目標復旧時点（RPO）を定めることが可能である。 ICTサービスに関するBIA及びリスクアセスメントの結果に基づいて、組織は、事業の中断・阻害の前、中断・阻害の加工中断・阻害の後の適切な手順を考慮したICT継続戦略を特定し、選択する。 組織は、次の事項を確実にする。 a）事業の中断・阻害に備え、それを緩和し、それに対応するために、必要な資源、権限及び力量をもつ要員が支援する適切な組織構造を備えている。 b）組織がICTサービスの中断・阻害を管理する方法を評価した、対応及び復旧手順を含むICT継続計画について、経営陣による承認を得る。 c）ICT継続計画は、次のICT継続に関する情報を含む。 1）BIAで特定した事業継続の要求事項及び目的を満たすためのパフォーマンス及び容量・能力の仕様 2）優先するICTサービスそれぞれのRTO及びそれらの構成要素を復旧する手順 3）情報として定義された優先するICT資源のRPO及び情報を復旧する手順 組織がICTサービスの中断・阻害を管理する方法を評価した、対応及び復旧手順を含むICT継続計画について、経営陣による承認を得る。
–	（対応項なし）	SF-5.30.2	事業の中断・阻害の結果として生じる影響の大きさ及び期間を用いて優先する活動を特定し、これに目標復旧時間（RTO）を設定した後、BIAでは、優先する活動の支援にどの資源が必要かを決定する。	予防に関連記載あり			
–	（対応項なし）	SF-5.30.3	優先する事業活動を支援する資源にもRTOを定め、これらの資源の一部としてICTサービスを良める。	予防に関連記載あり			
–	（対応項なし）	SF-5.30.4	ICTサービスに関するBIA及びリスクアセスメントの結果に基づいて、組織は、事業の中断・阻害の前、中断・阻害の加工中断・阻害の後の適切な手順を考慮したICT継続戦略を特定し、選択する。	予防に関連記載あり			
–	（対応項なし）	SF-5.30.5	ICTサービスに必要な可用性レベルを満たし、重要なプロセスの中断 又は失敗後に求められる時間内に回復するために、この戦略に基づいて計画を作成し、実装し、試験する。	予防に関連記載あり			
–	（対応項なし）	SF-5.30.6	組織は、次の事項を確実にする。 a）事業の中断・阻害に備え、それを緩和し、それに対応するために、必要な資源、権限及び力量をもつ要員が支援する適切な組織構造を備えている。 b）組織がICTサービスの中断・阻害を管理する方法を評価した、対応及び復旧手順を含むICT継続計画について、次を実施する。 1）演習及びテストを通じた定期的な計画 2）経営陣による承認 c）ICT継続計画は、次のICT継続に関する情報を含む。 1）BIAで特定した事業継続の要求事項及び目的を満たすためのパフォーマンス及び容量・能力の仕様 2）優先するICTサービスそれぞれのRTO及びそれらの構成要素を復旧する手順 3）情報として定義された優先するICT資源のRPO及び情報を復旧する手順	予防に関連記載あり			
–	（対応項なし）	SF-5.30.5	ICTサービスに必要な可用性レベルを満たし、重要なプロセスの中断 又は失敗後に求められる時間内に回復するために、この戦略に基づいて計画を作成し、実装し、試験する。	予防に関連記載あり	S.30.2	事業継続の目的及びICT継続の要求事項に基づいて、ICTの備えの試験をする。	（5.30.2に対応する項を参照）
–	（対応項なし）	（SF-5.30.5参考）	事業継続戦略は、一つ以上のソリューションから成る可能性がある。	予防に関連記載あり			

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
–	(対応項なし)	7.4	物理的セキュリティの監視 管理策 施設は、認可していない物理的アクセスについて継続的に監視すること。 目的 認可されていない物理的アクセスを検知し、抑止するため。		7.4	物理的セキュリティの監視 統制目標：施設は、認可していない物理的アクセスについて継続的に監視する。 目的：認可されていない物理的アクセスを検知し、抑止するため。	
–	(対応項なし)	7a-7.4.1	物理的な施設は、監視システムによって監視する。	予引に関連記載あり	7.4.1	認可されていないアクセス又は疑わしい行動を検知するため、監視システム（監視カメラ、検知器、警報器など）によりその建物を監視する。	物理的な施設は、監視システムによって監視する。これには、内部で又は監視サービス提供者が管理する、警備員、侵入者警報、監視カメラなどのビデオ監視システム、及び物理的セキュリティ情報管理ソフトウェアを含む場合がある。 重要なシステムを収容している建物へのアクセスは、認可されていないアクセスは疑わしい行動を検知するために、次の手段によって継続的に監視する。 a）組織の施設の内部及び外部の境重を要する領域へのアクセスを日視し、記録するために、監視カメラなどのビデオ監視システムを設置する。 b）関連する適用される標準に従って、侵入者警報を起動する次のような接触、音又は動きの検知器を設置し、それらを定期的に試験する。 1）パニック警報装置として使用するために、接触が発生又は遮断される可能性のある場所（窓及びドア並びに物体のドなど）に、接触が発生又は遮断されたときに警報を起動する接触検知器 2）物体が異野を通過したときに警報を起動する、赤外線技術に基づく動きの検知器 3）ガラスが割れる際に動感に反応し、それを使用して警報を発し、セキュリティ要員に警告することができるセンサー c）全ての外部扉及びアクセス可能な窓を対象として、これらの警報を使用する。無人の領域は常に警報器を稼働させる。その他の領域も対象とする。
–	(対応項なし)	7a-7.4.9	監視及び記録の仕組みは、特に要員の監視及び記録された映像の保持期間に関して、データ保護及びPII保護の法令を含む当地域の法規制を考慮して使用する。	予引に関連記載あり			
–	(対応項なし)	7a-7.4.3	監視システムの設計は機密性を維持する。	予引に関連記載あり	7.4.2	監視システムの設計及び動画などの監視情報の機密性を維持する。	監視システムの設計は機密性を維持する。これは、誤えいすると、検知されずに侵入することが容易になるためである。 監視システムは、動画などの監視情報が、認可されていない人によってアクセスされることを抑止するため、又はシステムが適用から無効にされることを抑止するために、認可されていないアクセスから保護する。 管轄システムの制御部は建物付きの領域に配置する。 安全管理の場合は、管理を設定した人が簡単に出られるような場所に配置する。 制御盤及び検知器は不正防止（tamperproof）の仕組みをもつ。 システムは、應答したとおりの動いていることを確実にするため定期的に試験する（システムの構成要素がバッテリ駆動の場合は特に試験が重要である）。
–	(対応項なし)	7a-7.4.4	監視システムは、動画などの監視情報が、認可されていない人によってアクセスされることを防止するため、又はシステムが適用から無効にされることを防止するために、認可されていないアクセスから保護する。	予引に関連記載あり			
–	(対応項なし)	7a-7.4.5	管轄システムの制御部は管轄付きの領域に配置する。	予引に関連記載あり			
–	(対応項なし)	7a-7.4.6	安全管轄の場合は、管轄を設定した人が簡単に出られるような場所に配置する。	予引に関連記載あり			
–	(対応項なし)	7a-7.4.7	制御盤及び検知器は不正防止（tamperproof）の仕組みをもつ。	予引に関連記載あり			
–	(対応項なし)	7a-7.4.8	システムは、應答したとおり作動していることを確実にするため定期的に試験する。	予引に関連記載あり			
–	(対応項なし)	8.9	構成管理 管理策 ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティ構成を含む構成を確立し、文書化し、実装し、監視し、レビューすることが望ましい。 目的 ハードウェア、ソフトウェア、サービス及びネットワーク、必要とされるセキュリティ設定で正しく機能し、認可されていない変更又は誤った変更によって構成が変えられないことを確実にするため。		8.9	構成管理 統制目標：ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティ構成を含む構成を確立し、文書化し、実装し、監視し、レビューする。 目的：ハードウェア、ソフトウェア、サービス及びネットワーク、必要とされるセキュリティ設定で正しく機能し、認可されていない変更又は誤った変更によって構成が変えられないことを確実にするため。	
–	(対応項なし)	8b-8.9.1	組織は、ハードウェア、ソフトウェア、サービス及びネットワークに関して、新しく導入したシステム及び適用システムの存続期間にわたって、定義した構成（セキュリティ構成を含む。）を維持するためのプロセス及びツールを定義し、実装する。	予引に関連記載あり	8.9.1	【再】ハードウェア、ソフトウェア、サービス及びネットワークに関して、定義した構成を維持するプロセスの整備及びツールを定義し、実装する。	(8.9.1に対応する箇条参照)
–	(対応項なし)	8b-8.9.2	全ての構成変更を良好に管理することを確実にするために、役割、責任及び手順を定める。	予引に関連記載あり			
–	(対応項なし)	8b-8.9.3	ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保った構成のための標準テンプレートを次のように定義する。 a）公開され、入手できる手引を使用する。 b）十分なセキュリティレベルを決定するために、必要な保護のレベルを考慮する。 c）組織の情報セキュリティ方針、トピック固有の方針、標準及びその他のセキュリティ要求事項を支援する。 d）組織の状況において、セキュリティ構成の実現可能性及び適用可能性を考慮する。	予引に関連記載あり			
–	(対応項なし)	8b-8.9.4	ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保った構成の標準テンプレートは、定期的にレビューするごとに加えて、新しい脅威又は弱い弱性に対処する必要がある場合、又は新規のソフトウェア若しくはハードウェアを導入した場合に更新する。	予引に関連記載あり			
–	(対応項なし)	8b-8.9.5	ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保った構成の標準テンプレートの策定に当たって、次の事項を考慮する。 a）特権的又は業務管理者レベルのアクセス権をもつ識別情報の数を最小限にする。 b）不必要な、使用されていない又はセキュリティが保たれていない識別情報を無効化する。 c）不必要な機能及びサービスを無効化又は制限する。 d）強力なユーティティプログラム及びホストパラメータ設定へのアクセスを制限する。 e）クロックを同期させる。 f）初期パスワードなどの業者による初期設定情報を導入の直後に変更し、その他の重要なセキュリティ関連パラメータの初期状態をレビューする。 g）既定の使用中断時間の後に、コンピューティング装置・機器から自動的にログオフするタイムアウト機能を作動させる。 h）使用許可の要求事項が満たされていることを検証する。	予引に関連記載あり			
–	(対応項なし)	8b-8.9.6	ハードウェア、ソフトウェア、サービス及びネットワークについて決定した構成を記録し、全ての構成変更のログを維持する。これらの記録はセキュリティを保って保管する。	予引に関連記載あり			
–	(対応項なし)	(8b-8.9.6参考1)	これは、構成データベース又は構成テンプレートなど様々な方法で達成することが可能である。	予引に関連記載あり			
–	(対応項なし)	(8b-8.9.6参考2)	構成の変更は、変更管理プロセスに従う。	予引に関連記載あり			
–	(対応項なし)	(8b-8.9.6参考3)	構成記録には、次の事項を含み得る。 a）資産の最新の管理責任者又は連絡先情報 b）構成の最終変更日 c）構成テンプレートの版 d）その他の資産の構成との関係	予引に関連記載あり			
–	(対応項なし)	8b-8.9.7	構成は、包括的なシステム管理ツール群を用いて監視する。	予引に関連記載あり	8.9.2	構成を監視し、定期的にレビューする。	構成は、包括的なシステム管理ツール群（例えば、保守ユーティティ、適用サポート、エンタープライズ管理ツール、バックアップ及び復元ソフトウェア）を用いて監視する。 構成設定を検証し、パスワードの強度を評価し、また、実施する活動を評価するために、定期的にレビューする。
–	(対応項なし)	8b-8.9.8	構成設定を検証し、パスワードの強度を評価し、また、実施する活動を評価するために、定期的にレビューする。	予引に関連記載あり			
–	(対応項なし)	8b-8.9.9	実際の構成を、定義した目標テンプレートと比較することが可能である。逸脱には、定義した目標構成を自動適用して、又は逸脱を手動で分析し、是正処置を講じて対処する。	予引に関連記載あり	8.9.3	定期的なレビューの結果、逸脱を検知した場合には是正処置を実施する。	実際の構成を、定義した目標テンプレートと比較することが可能である。逸脱には、定義した目標構成を自動適用して、又は逸脱を手動で分析し、是正処置を講じて対処する。
–	(対応項なし)	8.10	情報の削除 管理策 情報システム、装置又はその他の記憶媒体に保存している情報は、必要でなくなった時点で削除することが望ましい。 目的 敗因に慣重を要する情報の不用意な漏えいを防止し、情報の削除に関する法令、規則及び契約上の要求事項を順守するため。		8.10	情報の削除 統制目標：情報システム、装置又はその他の記憶媒体に保存している情報は、必要でなくなった時点で削除する。 目的：敗因に慣重を要する情報の不用意な漏えいを防止し、情報の削除に関する法令、規則及び契約上の要求事項を順守するため。	
–	(対応項なし)	8b-8.10.1	敗因に慣重を要する情報は、望ましくない開示のリスクを減らすために、必要な期間より長く保持しない。	予引に関連記載あり	8.10.1	情報システム、装置又はその他の記憶媒体に保存している情報は、時期を失せずに削除する。	敗因に慣重を要する情報は、望ましくない開示のリスクを減らすために、必要な期間より長く保持しない。 システム、アプリケーション及びサービスに関する情報を削除する場合は、次の事項を考慮する。 a）業務の要求事項に従い、また、関連する法令及び規則を考慮して、削除手法（例えば、電子的な上書き又は暗号化消去）を選択する。 b）削除の結果を証拠として記録する（情報の削除の正式記録は、生じ得る情報漏えい事象の原因を分析するに役立つ。）。 c）情報の削除を行うサービス提供者を利用する場合、サービス提供者から情報の削除の証拠を得る。 第三者が組織にわたっても情報を保存する場合、組織は、情報の削除に関する要求事項を第三者との合意に含め、サービスの実施中及び終了時に実行させることを検討する。 組織のデータ保持に関するトピック固有の方針に従い、また、関連する法令及び規則を考慮して、敗因に慣重を要する情報は、必要がなくなったとき、次の方法で削除する。 a）必要でなくなったとき、情報をセキュリティを保って破棄するようにシステムを構成する（例えば、データ保持に関するトピック固有の方針に従って定義した期間の後に、又は対象のアクセス要求に応じて）。 b）古い版、複製及び一時ファイルは、それらがどこあっても削除する。 c）情報を他システムに削除し、専門家が使う敗旧ツール又はオンラインツールを使用して情報が復旧できないことを確実にする助力とするために、広く認められた、セキュリティを保った削除ソフトウェアを使用する。 d）広く認められ、認定された、セキュリティを保った廃棄サービス提供者を利用する。 e）処分する記憶媒体の種類に適した処分の仕組みを使用する。
–	(対応項なし)	8b-8.10.2	システム、アプリケーション及びサービスに関する情報を削除する場合は、次の事項を考慮する。 a）業務の要求事項に従い、また、関連する法令及び規則を考慮して、削除手法を選択する。 b）削除の結果を証拠として記録する。 c）情報の削除を行うサービス提供者を利用する場合、サービス提供者から情報の削除の証拠を得る。	予引に関連記載あり			
–	(対応項なし)	8b-8.10.3	第三者が組織にわたっても情報を保存する場合、組織は、情報の削除に関する要求事項を第三者との合意に含め、サービスの実施中及び終了時に実行させることを検討する。	予引に関連記載あり			
–	(対応項なし)	8b-8.10.4	組織のデータ保持に関するトピック固有の方針に従い、また、関連する法令及び規則を考慮して、敗因に慣重を要する情報は、必要がなくなったとき、次の方法で削除する。 a）必要でなくなったとき、情報をセキュリティを保って破棄するようにシステムを構成する。 b）古い版、複製及び一時ファイルは、それらがどこあっても削除する。 c）情報を他システムに削除し、専門家が使う敗旧ツール又はオンラインツールを使用して情報が復旧できないことを確実にする助力とするために、広く認められた、セキュリティを保った削除ソフトウェアを使用する。 d）広く認められ、認定された、セキュリティを保った廃棄サービス提供者を利用する。 e）処分する記憶媒体の種類に適した処分の仕組みを使用する。	予引に関連記載あり			
–	(対応項なし)	8b-8.10.5	クラウドサービスを利用する場合、組織はクラウドサービスプロバイダが提供する削除手法が許容できるかどうかを検証し、許容できるならばそれを利用し、又はクラウドサービスプロバイダに情報の削除を要請する。	予引に関連記載あり			
–	(対応項なし)	8b-8.10.6	削除プロセスは、利用可能かつ適用可能な場合には、トピック固有の方針に従って自動化する。	予引に関連記載あり			
–	(対応項なし)	8b-8.10.7	装置・機器を業者に送送するとき、敗因に慣重を要する情報が意図せず漏えいすることを防止するために、装置・機器を組織の施設から出す前に、補助記憶媒体及びメモリを含む除くことによって、敗因に慣重を要する情報を保護する。	予引に関連記載あり			
–	(対応項なし)	8b-8.10.8	組織はその装置・機器で取り扱う情報の分類に従って適切な手法を選択する。	予引に関連記載あり			
–	(対応項なし)	8b-8.10.9	記憶装置を物理的に破壊し、同時にそこに含む情報を消去するために、7b-7.14にある対策を適用する。	予引に関連記載あり			

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
–	（対応項なし）	8.11	データマスキング 管理策 データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有のポリシ及びその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用することが望ましい。 目的 PIIを含む、取扱いに慎重を要するデータの開示を制限し、法令、規制及び契約上の要求事項を順守するため。		8.11	データマスキング 統制の趣旨：データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有のポリシ及びその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用する。 目的：PIIを含む、取扱いに慎重を要するデータの開示を制限し、法令、規制及び契約上の要求事項を順守するため。	
–	（対応項なし）	8b-8.11.1	取扱いに慎重を要するデータの保護が必要である場合、組織は仮名化、匿名化などを含むデータマスキングの手法を利用してそのデータ処理でこと を検討する。	予防に関連記載あり	8.11.1	適用される法令や事業上の要求事項に従い、データマスキングの要件及び手法を特定する。	取扱いに慎重を要するデータ（例えば、PII）の保護が必要である場合、組織はデータマスキング、仮名化、匿名化などを含むデータマスキングの手法（データマスキング手法という。）を利用してそのデータ処理でこと を検討する。 仮名化又は匿名化の手法では、次のことが可能である。 a）PIIのデータ置する。 b）PII主体の真のアイデンティティ又はその他の取扱いに慎重を要する情報を偽装する。 c）PII又はPII主体のアイデンティティの間のひも（紐）付け又は他の取扱いに慎重を要する情報との間のひも（紐）付けを切る。 仮名化又は匿名化の手法を利用する場合、データが十分に仮名化又は匿名化されていることを検証する。 データの匿名化では、取扱いに慎重を要する情報の全ての要素に対して有効とするように考慮する。データの匿名化が適切に考慮されていない場合、あふ人物が識別できるデータが匿名化されていても、間接的に識別を可能とする別のデータが存在して、その人物が識別できる場合がある。 データマスキング手法には、仮名化、匿名化のほか、次を含む手法も考慮する。 a）データを暗号化する。 b）文字をスキル化又は消去する。 c）数及び日付を変える。 d）取扱いに慎重を要するデータの一つ特定の値を別の値に置き換える。 e）値をそのハッシュ値に置き換える。
–	（対応項なし）	8b-8.11.2	仮名化又は匿名化の手法を利用する場合、データが十分に仮名化又は匿名化されていることを検証する。	予防に関連記載あり			
–	（対応項なし）	8b-8.11.3	データの匿名化では、取扱いに慎重を要する情報の全ての要素に対して有効とするように考慮する。	予防に関連記載あり			
–	（対応項なし）	8b-8.11.4	データマスキング手法には、仮名化、匿名化のほか、次を含む手法を考慮する。 a）データを暗号化する。 b）文字をスキル化又は消去する。 c）数及び日付を変える。 d）取扱いに慎重を要するデータの一つ特定の値を別の値に置き換える。 e）値をそのハッシュ値に置き換える。	予防に関連記載あり			
–	（対応項なし）	8b-8.11.5	データマスキング手法を実装する場合、次の事項を考慮する。 a）利用者に必要最小限のデータだけを示すように問合せ（クエリ）及びマスクを設計する。 b）データセットの一部の記録に関して、利用者に一部のデータ見せないことが望ましい場合、データを難読化する仕組みを設計し、実装する。 c）データを難読化する場合、データを難読化していないかどうかを利用者が知ることができないことを、PII主体が要求できるようにする。 d）法令又は規制上の要求事項。	予防に関連記載あり	8.11.2	特定したデータマスキング手法を実装する。	データマスキング手法を実装する場合、次の事項を考慮する。 a）利用者に必要最小限のデータだけを示すように問合せ（クエリ）及びマスクを設計する。 b）データセットの一部の記録に関して、利用者に一部のデータ見せないことが望ましい場合、データを難読化する仕組みを設計し、実装する。（例えば、緊急の場合であっても、患者内容らの記録の全てを病院スタッフが見ることができることが望ましい場合、病院スタッフには部分的に難読化したデータを提示し、そのデータが適切な治療に有用な情報を含む場合は、特定の役割をもつスタッフだけがアクセスできるようにする。）。 c）データを難読化する場合、データを難読化していないかどうかを利用者が知ることができないことを、PII主体が要求できるようにする（難読化の解読化、これは医療機関で利用され、例えば、血液検査の結果などを取扱いに慎重を要する情報が難読化されていることを、患者が要員に知らされていない場合などである。）。 d）法令又は規制上の要求事項（例えば、処理中又は保管中に、支払いカードの情報をマスキングすることを要求する。）。
–	（対応項なし）	8b-8.11.6	データマスキング、仮名化又は匿名化を利用する場合、次の事項を考慮する。 a）処理するデータの使用法に応じた、データマスキング、仮名化又は匿名化の強度のレベル b）処理するデータへのアクセス制御 c）処理するデータの使用法に関する合意又は制限 d）PII主体を識別するために、処理するデータを他の情報と照合することの禁止 e）処理するデータの提供及び受領の追跡	予防に関連記載あり			データマスキング、仮名化又は匿名化を利用する場合、次の事項を考慮する。 a）処理するデータの使用法に応じた、データマスキング、仮名化又は匿名化の強度のレベル b）処理するデータへのアクセス制御 c）処理するデータの使用法に関する合意又は制限 d）PII主体を識別するために、処理するデータを他の情報と照合することの禁止 e）処理するデータの提供及び受領の追跡
–	（対応項なし）	8.12	データ漏えい防止 管理策 データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存又は送信するシステム、ネットワーク及びその他の装置に適用すること が望ましい。 目的 個人又はシステムによる情報の認可されていない開示及び抽出を検出し、防止するため。		8.12	データ漏えい防止 統制の趣旨：データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存又は送信するシステム、ネットワーク及びその他の装置に適用する。 目的：個人又はシステムによる情報の認可されていない開示及び抽出を検出し、防止するため。	
–	（対応項なし）	8b-8.12.1	組織は、データ漏えいのリスクを減らすために、次の事項を考慮する。 a）漏えいから保護する情報の特定及び分類 b）データ漏えいの経路・手段の監視 c）情報の漏えい を防止するための処置	予防に関連記載あり	8.12.1	データ漏えいのリスクへの対策を実施する。	組織は、データ漏えいのリスクを減らすために、次の事項を考慮する。 a）漏えいから保護する情報（例えば、個人情報、機微設定モデル及び製品設計）の特定及び分類 b）データ漏えいの経路・手段の監視（例えば、電子メール、ファイル転送、モバイル機器及び可搬記憶装置） c）情報の漏えい を防止するための処置（例えば、取扱いに慎重を要する情報を含むメールの検疫）
–	（対応項なし）	8b-8.12.2	データ漏えい防止ツールを、次の目的で使用する。 a）認可されていない開示のリスクがある取扱いに慎重を要する情報を特定し、監視する。 b）取扱いに慎重を要する情報の開示を検出する。 c）取扱いに慎重を要する情報を組みいする利用者の行為又はネットワーク送信を阻止する。	予防に関連記載あり			データ漏えい防止ツールを、次の目的で使用する。 a）認可されていない開示のリスクがある取扱いに慎重を要する情報を特定し、監視する（例えば、利用者のシステム上の管理されていない情報）。 b）取扱いに慎重を要する情報の開示を検出する（例えば、信頼できない第三者のクラウドサービスに情報がアップロードされた場合、又は電子メールで送信された場合にこれらを検出する。）。 c）取扱いに慎重を要する情報を組みいする利用者の行為又はネットワーク送信を阻止する（例えば、データベースエントリのスプレッドシートへのコピーを防止する。）。
–	（対応項なし）	8b-8.12.3	組織は、組織の外部のサービス、装置・機器及び記憶媒体にデータをコピーして貼り付ける、又はアップロードする利用者の権限を制限するか要がみかのつかを判断する。	予防に関連記載あり			組織は、組織の外部のサービス、装置・機器及び記憶媒体にデータをコピーして貼り付ける、又はアップロードする利用者の権限を制限するか要がみかのつかを判断する。 組織の管理外にデータをコピーして貼り付ける、又はアップロードする利用者の権限を制限する場合、データ漏えい防止ツール又は既存のツールの組合せなどの技術を導入する。 データの取り出し件必要な場合、利用者による取り出し件可じ。利用者に自らの行動にアカウンタビリティをもたせる設置を、データの管理責任者にならえる。 画面のスクリーンショット又は写真を撮ることには、利用条件、損賠及び監査によって対応する。 データをバックアップする場合、暗号化、アクセス制御及びバックアップを保持する記憶媒体の物理的保護などの対策を使用して、取扱いに慎重を要する情報の保護を確実にする。 データ漏えい防止は、ちょう（直）報改動の対象となる可能性がある、又はコミュニケーションで重要な可能性がある（例えば、人、財務、商取引、科学又はその他に関する）秘密情報を取引者が情報収集活動によって取得することに対する保護も考慮する。 データ漏えい防止活動は、独立の活動又は取引者の情報収集活動への対応のいずれかとして、取引者の決定を混乱させる方策（真正の情報を偽の情報に置き換えることによる、リバースエンジニアリング又は攻撃者を引き付けるハニーポットの使用があるる）を講じる。
–	（対応項なし）	8b-8.12.4	組織の管理外にデータをコピーして貼り付ける、又はアップロードする利用者の権限を制限する場合、データ漏えい防止ツール又は既存のツールの組合せなどの技術を導入する。	予防に関連記載あり			
–	（対応項なし）	8b-8.12.5	データの取り出しが必要な場合、利用者による取り出し件可じ。利用者に自らの行動にアカウンタビリティをもたせる設置を、データの管理責任者にならえる。	予防に関連記載あり			
–	（対応項なし）	8b-8.12.6	画面のスクリーンショット又は写真を撮ることには、利用条件、損賠及び監査によって対応する。	予防に関連記載あり			
–	（対応項なし）	8b-8.12.7	データをバックアップする場合、暗号化、アクセス制御及びバックアップを保持する記憶媒体の物理的保護などの対策を使用して、取扱いに慎重を要する情報の保護を確実にする。	予防に関連記載あり			
–	（対応項なし）	8b-8.12.8	データ漏えい防止は、ちょう報改動の対象となる可能性がある、又はコミュニティにとって重要な可能性がある秘密情報を取引者が情報収集活動によって取得することに対する保護も考慮する。	予防に関連記載あり			
–	（対応項なし）	8b-8.12.9	データ漏えい防止活動は、独立の活動又は取引者の情報収集活動への対応のいずれかとして、取引者の決定を混乱させる方策を講じる。	予防に関連記載あり			
–	（対応項なし）	8.16	監視活動 管理策 情報セキュリティインシデントの可能性を評価するために、ネットワーク、システム及びアプリケーションについて異常な挙動がないか監視し、適切な処置を講じる。 目的 異常な挙動及び情報セキュリティインシデントの可能性を検出するため。		8.16	監視活動 統制の趣旨：情報セキュリティインシデントの可能性を評価するために、ネットワーク、システム及びアプリケーションについて異常な挙動がないか監視し、適切な処置を講じる。 目的：異常な挙動及び情報セキュリティインシデントの可能性を検出するため。	
–	（対応項なし）	8b-8.16.1	監視のために、次の事項を行う。 a）監視の範囲及びレベルは、業務及び情報セキュリティの要求事項に従い、関連する法令及び規制を考慮して決定する。 b）監視を記録する。 c）監視記録は、定めた保持期間にわたって維持する。	予防に関連記載あり	8.16.1	監視の範囲及びレベルを定義する。	監視のために、次の事項を行う。 a）監視の範囲及びレベルは、業務及び情報セキュリティの要求事項に従い、関連する法令及び規制を考慮して決定する。 b）監視を記録する。 c）監視記録は、定めた保持期間にわたって維持する。
–	（対応項なし）	8b-8.16.2	監視システムに含めるものとして、次の事項を考慮する。 a）アウトバウンド及びインバウンドの、ネットワーク、システム及びアプリケーションのトラフィック b）システム、サーバ、ネットワーク装置、監視システム、重要なアプリケーションなどへのアクセス c）重要なシステム及び業務管理者が設ったシステム及びネットワークの構成ファイル d）セキュリティツールからのログ e）システム及びネットワークの活動に関するイベントログ f）実行しているコードがそのシステムでの実行を認可されていること、及びそれが改ざんされていないことの確認 g）資源（例えば、CPU、ハードディスク、メモリ、無線機）の使用及びそれらの動作状況	予防に関連記載あり			監視システムに含めるものとして、次の事項を考慮する。 a）アウトバウンド及びインバウンドの、ネットワーク、システム及びアプリケーションのトラフィック b）システム、サーバ、ネットワーク装置、監視システム、重要なアプリケーションなどへのアクセス c）重要なシステム及び業務管理者が設ったシステム及びネットワークの構成ファイル d）セキュリティツールからのログ（例えば、ウイルス対策、IDS、不正侵入防止システム（IPS）、ウェブフィルタ、ファイアウォール、データ漏えい防止（DLP）） e）システム及びネットワークの活動に関するイベントログ f）実行しているコードがそのシステムでの実行を認可されていること、及びそれが改ざん（例えば、望ましくないコードを追加する再コンパイルによる改ざん）されていないことの確認 g）資源（例えば、CPU、ハードディスク、メモリ、無線機）の使用及びそれらの動作状況
–	（対応項なし）	8b-8.16.3	組織は、正常な挙動の基準を確立し、この基準に照らして異常を監視する。基準を確立する場合、次の事項を考慮する。 a）通常時及びピーク時のシステムの使用率 b）各利用者又は利用者グループの通常のアクセス時間、アクセスの場所、アクセスの頻度	予防に関連記載あり			組織は、正常な挙動の基準を確立し、この基準に照らして異常を監視する。基準を確立する場合、次の事項を考慮する。 a）通常時及びピーク時のシステムの使用率 b）各利用者又は利用者グループの通常のアクセス時間、アクセスの場所、アクセスの頻度
–	（対応項なし）	8b-8.16.4	監視システムは、次のような異常な挙動を特定するために、確立した基準に照らして構成する。 a）プロセス又はアプリケーション計画外の終了 b）既知の悪意のあるIP アドレス又はネットワークドメインから送信されるマルウェアなどトラフィックに典型的に伴う挙動 c）既知の攻撃の特性 d）異常なシステム動作 e）ボトルネック及び過負荷 f）システム又は情報への認可されていないアクセス又はその試み g）業務アプリケーション、システム及びネットワークの認可されていないスキャン h）保護された資源への成功及び失敗したアクセスの試み i）想定される挙動に対して、利用者及びシステムの異常な挙動	予防に関連記載あり			監視システムは、次のような異常な挙動を特定するために、確立した基準に照らして構成する。 a）プロセス又はアプリケーション計画外の終了 b）既知の悪意のあるIP アドレス又はネットワークドメイン（例えば、ボットネットのC&C サーバに関係するものから送信されるマルウェアなどトラフィックに典型的に伴う挙動 c）既知の攻撃の特性（例えば、サービス妨害及びパフォーマーフロー） d）異常なシステム動作（例えば、キーストロークロガー、プロセスインジェクション、及び標準プロトコルの使用における悪用） e）ボトルネック及び過負荷（例えば、ネットワークの持ち行列、遅延レベル及びネットワーク上の通信の乱れ） f）システム又は情報への認可されていないアクセス又はその試み g）業務アプリケーション、システム及びネットワークの認可されていないスキャン h）保護された資源（例えば、DNS サーバ、ウェブポータル及びファイルシステム）への成功及び失敗したアクセスの試み i）想定される挙動に対して、利用者及びシステムの異常な挙動
–	（対応項なし）	8b-8.16.5	監視ツールによる継続的監視を使用し、次の事項を考慮する。 a）監視は、組織のニーズ及び能力に応じて、リアルタイム又は定期的な間隔で行う。 b）大量のデータ処の扱い、常に変化する脅威の状況に適応し、リアルタイムで適知することを可能にする機能をもつ監視ツールを利用する。 c）特定のシグネチャ及びデータ、又はネットワーク乱いはアプリケーションの動作パターンを認識できる監視ツールを利用する。	予防に関連記載あり	8.16.2	リアルタイム又は定期的な間隔で監視を行う。	監視ツールによる継続的監視を使用し、次の事項を考慮する。 a）監視は、組織のニーズ及び能力に応じて、リアルタイム又は定期的な間隔で行う。 b）大量のデータ処の扱い、常に変化する脅威の状況に適応し、リアルタイムで適知することを可能にする。 c）特定のシグネチャ及びデータ、又はネットワーク乱いはアプリケーションの動作パターンを認識できる監視ツールを利用する。 自動監視ソフトウェアは、あらかじめ定めたしきい値に基づいて警告を発するように構成する（例えば、管理コンソール、電子メールやセージ又はインスタントかセージングシステムを通じて構成する）。 警告システムは、誤検出を最小限にするために、組織の基準に合わせて調整し、学習させる。
–	（対応項なし）	8b-8.16.6	自動監視ソフトウェアは、あらかじめ定めたしきい値に基づいて警告を発するように構成する。	予防に関連記載あり			
–	（対応項なし）	8b-8.16.7	警告システムは、誤検出を最小限にするために、組織の基準に合わせて調整し、学習させる。	予防に関連記載あり			
–	（対応項なし）	8b-8.16.8	要員は警告への対応に専念させることが望ましく、インシデントの可能性がある事象を正確に判定できるように適切な訓練を受けさせる。	予防に関連記載あり	8.16.3	異常な挙動及び情報セキュリティインシデントの可能性のある事象は、組織が定める職員又は役割に伝達する。	要員は警告への対応に専念させることが望ましく、インシデントの可能性がある事象を正確に判定できるように適切な訓練を受けさせる。 警告通知を受領し、対応するための工長性のあるシステム及びプロセスを備える。
–	（対応項なし）	8b-8.16.9	警告通知を受領し、対応するための工長性のあるシステム及びプロセスを備える。	予防に関連記載あり			監査、セキュリティ評価、ぜい弱性スキャン及び監視（5.25参照）を改善するために、異常な事象を関係者に伝達する。
–	（対応項なし）	8b-8.16.10	監査、セキュリティ評価、ぜい弱性スキャン及び監視を改善するために、異常な事象を関係者に伝達する。	予防に関連記載あり			情報セキュリティに対する有害な事象の影響を最小にするために、その存在を示す監視システムからの通知に時機を失せずに対応する手順を確立する（5.26参照）。 将来の誤検出の数を減らすために監視ソフトウェアを調整するなど、誤検出を特定し、対処する手順も確立する。
–	（対応項なし）	8b-8.16.11	情報セキュリティに対する有害な事象の影響を最小にするために、その存在を示す監視システムからの通知に時機を失せず対応する手順を確立する。	予防に関連記載あり			
–	（対応項なし）	8b-8.16.12	将来の誤検出の数を減らすために監視ソフトウェアを調整するなど、誤検出を特定し、対処する手順も確立する。	予防に関連記載あり			

番号	(旧)管理策基準	番号	情報セキュリティ管理基準（令和７年版）	備考	番号	(新)管理策基準	(参考)手引き
–	（対応項なし）	8.23	ウェブフィルタリング 管理策 悪意のあるコンテンツにさらされることを減らするために、外部ウェブサイトへのアクセスを管理することが望ましい。 目的 システムがマルウェアによって危険にさらされることを防ぎ、認可されていないウェブ資源へのアクセスを防止するため。		8.23	ウェブフィルタリング 統制目標：悪意のあるコンテンツにさらされることを減らするために、外部ウェブサイトへのアクセスを管理する。 目的：システムがマルウェアによって危険にさらされることを防ぎ、認可されていないウェブ資源へのアクセスを防止するため。	
–	（対応項なし）	8c-8.23.1	組織は、違法な情報があるウェブサイト、又はウイルス若しくはフィッシングの材料があることが知られているウェブサイトに組織の要員がアクセスするリスクを減らす。	干渉に関連記載あり	8.23.1	外部ウェブサイトのアクセスに関する規則を整備し、外部ウェブサイトへのアクセスを制限し、維持する。	組織は、違法な情報があるウェブサイト、又はウイルス若しくはフィッシングの材料があることが知られているウェブサイトに組織の要員がアクセスするリスクを減らす。リスクを減らす手法として、関係するウェブサイトのIP アドレスなどはドメインへのアクセスを阻止することがある。一部のブラウザ及びマルウェア対策技術は、アクセスすることが望ましくないウェブサイトへのアクセスを自動的に阻止、又は阻止するように構成することが可能である。 組織は、要員がアクセスすることが望ましい又は望ましくないウェブサイトの機能を特定する。 組織は次の種類のウェブサイトへのアクセスを審べこを考慮する。 a) 情報アップロード機能をもつウェブサイト。ただし、正当な業務上の理由のため許可されている場合を除く。 b) 悪意のある、又はその疑いのあるウェブサイト（例えば、マルウェアズはフィッシングコンテンツを配布しているウェブサイト） c) C&Cサーバ d) 飛威インテリジェンスで認識した悪意のあるウェブサイト（5.7 参照） e) 違法なコンテンツを供給しているウェブサイト ウェブフィルタリングに関する管理策を導入する前に、組織は、望ましくない又は不適切なウェブサイト及びウェブベースのアプリケーションに対する制限を含め、オンライン資源を安全かつ適切に使用するための規則を確立する。 オンライン資源を安全かつ適切に使用するための規則は最新の状態に保つ。
–	（対応項なし）	8c-8.23.2	組織は、要員がアクセスすることが望ましい又は望ましくないウェブサイトの種類を特定する。	干渉に関連記載あり			
–	（対応項なし）	8c-8.23.3	組織は次の種類のウェブサイトへのアクセスを審べこを考慮する。 a) 情報アップロード機能をもつウェブサイト。ただし、正当な業務上の理由のため許可されている場合を除く。 b) 悪意のある、又はその疑いのあるウェブサイト c) C&Cサーバ d) 飛威インテリジェンスで認識した悪意のあるウェブサイト e) 違法なコンテンツを供給しているウェブサイト	干渉に関連記載あり			
–	（対応項なし）	8c-8.23.4	ウェブフィルタリングに関する管理策を導入する前に、組織は、望ましくない又は不適切なウェブサイト及びウェブベースのアプリケーションに対する制限を含め、オンライン資源を安全かつ適切に使用するための規則を確立する。	干渉に関連記載あり			
–	（対応項なし）	8c-8.23.5	オンライン資源を安全かつ適切に使用するための規則は最新の状態に保つ。	干渉に関連記載あり			
–	（対応項なし）	8c-8.23.6	ウェブへのアクセスを含む、オンライン資源のセキュリティを保つ適切な使用について、要員を訓練する。	干渉に関連記載あり			
–	（対応項なし）	8c-8.23.7	オンライン資源のセキュリティを保つ適切な使用についての訓練には、組織の規則、セキュリティ上の懸念を報告するための連絡先、及び制限されたウェブ資源に正当な業務上の理由によってアクセスする必要がある場合の例外プロセスを含める。	干渉に関連記載あり			
–	（対応項なし）	8c-8.23.8	ウェブサイトで、セキュリティが保たれないことを通知するブラウザアドバイザリを利用者が無効にしないことを確実にするように、要員を訓練する。	干渉に関連記載あり			
–	（対応項なし）	8.28	セキュアに配慮したコーディング 管理策 セキュアに配慮したコーディングの原則をソフトウェア開発に適用することが望ましい。 目的 ソフトウェアをセキュアに配慮して作成し、それによってソフトウェアの潜在的な情報セキュリティのぜい弱性の数を減らすことを確実にするため。		8.28	セキュアに配慮したコーディング 統制目標：セキュアに配慮したコーディングの原則をソフトウェア開発に適用する。 目的：ソフトウェアをセキュアに配慮して作成し、それによってソフトウェアの潜在的な情報セキュリティのぜい弱性の数を減らすことを確実にするため。	
–	（対応項なし）	8d-8.28.1	組織は、セキュリティに配慮したコーディングに関して優れたガバナンスを実現する。組織全体のプロセスを確立する。	干渉に関連記載あり	8.28.1	セキュリティに配慮したコーディングの原則を策定する。	（8.28.1C対応する項を参照）
–	（対応項なし）	8d-8.28.2	最低限のセキュリティに配慮したコーディングのベースラインを確立し、適用する。	干渉に関連記載あり			
–	（対応項なし）	8d-8.28.3	セキュリティに配慮したコーディングのための プロセス及びガバナンスを、第三者から入手したソフトウェア構成要素及びオープンソースソフトウェアを対象とするように拡張する。	干渉に関連記載あり			
–	（対応項なし）	8d-8.28.4	組織は、組織のセキュリティに配慮したコーディングの原則を下記により方向付ける。 a) 現実世界の脅威、並びにソフトウェアのぜい弱性に関する最新の動 及び情報を監視する b) 組織のセキュリティに配慮したコーディングの原則を継続的に改善する c) 組織のセキュリティに配慮したコーディングの原則に従うための学習を要員に施す	干渉に関連記載あり			
–	（対応項なし）	（8d-8.28.4参考）	これは、急速に変化する脅威の状況に対抗するために、効果的なセキュリティに配慮したコーディング慣行の実施を確実にするのに役立ち得る。	干渉に関連記載あり			
–	（対応項なし）	8d-8.28.6	セキュリティに配慮したコーディングの原則を、新規の開発及び再利用の両方で使用する。	干渉に関連記載あり	8.28.2	セキュリティに配慮したコーディングの原則を踏まえた計画及び前提条件を定める。	セキュリティに配慮したコーディングの原則を、新規の開発及び再利用の両方で使用する。 セキュリティに配慮したコーディングの原則は、組織内の開発活動並びに組織が他者に提供する製品及びサービスの両方に適用する。 コーディング前の計画及び前提条件は、次の事項を含む。 a) 組織内及び外部委託のコード開発の両方に使用する、セキュリティに配慮したコーディングに関する組織固有の期待及び広く認められた原則 b) 情報セキュリティのぜい弱性につながる一般的及び歴史的なコーディング慣行及び欠陥 c) セキュリティに配慮したコードの作成を実施させるために、統合開発環境（IDE）などの開発ツールを構成する。 d) 該当する場合には、開発ツール及び実行環境の提供者が示す手引に従う。 e) 要素された開発ツールの種類及び使用 f) セキュリティに配慮したコードを作成する際の開発者の資格 g) 飛威モデリングを含むセキュリティに配慮した設計及びアーキテクチャ h) セキュリティに配慮したコーディング標準、及び開発する場合はその使用を義務付けること i) 開発のための管理された環境の使用
–	（対応項なし）	8d-8.28.7	セキュリティに配慮したコーディングの原則は、組織内の開発活動並びに組織が他者に提供する製品及びサービスの両方に適用する。	干渉に関連記載あり			
–	（対応項なし）	8d-8.28.8	コーディング前の計画及び前提条件は、次の事項を含む。 a) 組織内及び外部委託のコード開発の両方に使用する、セキュリティに配慮したコーディングに関する組織固有の期待及び広く認められた原則 b) 情報セキュリティのぜい弱性につながる一般的及び歴史的なコーディング慣行及び欠陥 c) セキュリティに配慮したコードの作成を実施させるために、統合開発環境（IDE）などの開発ツールを構成する。 d) 該当する場合には、開発ツール及び実行環境の提供者が示す手引に従う。 e) 要素された開発ツールの種類及び使用 f) セキュリティに配慮したコードを作成する際の開発者の資格 g) 飛威モデリングを含むセキュリティに配慮した設計及びアーキテクチャ h) セキュリティに配慮したコーディング標準、及び開発する場合はその使用を義務付けること i) 開発のための管理された環境の使用	干渉に関連記載あり			
–	（対応項なし）	8d-8.28.9	コーディング中の考慮事項は、次の事項を含む。 a) 使用するプログラム言語及び手法に特有の、セキュリティに配慮したコーディング慣行 b) ペアプログラミング、リファクタリング、ピアレビュー、セキュリティイテレーション、テスト駆動開発など、セキュリティに配慮したプログラミング手法を使用する。 c) 構造化プログラミング手法を使用する。 d) コード生文書化し、情報セキュリティのぜい弱性の悪用を許す可能性のあるプログラミングの欠陥を除去する。 e) セキュリティに配慮しない設計手法の使用を禁止する。	干渉に関連記載あり	8.28.3	セキュリティに配慮したコーディングを実施する。	コーディング中の考慮事項は、次の事項を含む。 a) 使用するプログラム言語及び手法に特有の、セキュリティに配慮したコーディング慣行 b) ペアプログラミング、リファクタリング、ピアレビュー、セキュリティイテレーション、テスト駆動開発など、セキュリティに配慮したプログラミング手法を使用する。 c) 構造化プログラミング手法を使用する。 d) コード生文書化し、情報セキュリティのぜい弱性の悪用を許す可能性のあるプログラミングの欠陥を除去する。 e) セキュリティに配慮しない設計手法の使用を禁止する（例えば、ハードコード（決め打ち）されたパスワード、承認されていないロードサンプル及び認可されていないウェブサービスの使用）。 セキュリティに配慮して作成するソフトウェアのテストは開発中及び開発後に実施する（8.29参照）。静的アプリケーションセキュリティテスト（SAST）プロセスで、ソフトウェアのセキュリティのぜい弱性を特定することが可能である。
–	（対応項なし）	8d-8.28.10	セキュリティに配慮して作成するソフトウェアのテストは開発中及び開発後に実施する。	干渉に関連記載あり			
–	（対応項なし）	（8d-8.28.10参考）	静的アプリケーションセキュリティテスト（SAST）プロセスで、ソフトウェアのセキュリティのぜい弱性を特定することが可能である。	干渉に関連記載あり			
–	（対応項なし）	8d-8.28.11	ソフトウェアの運用を開始する前に、次の事項を評価する。 a) 攻撃対象領域（attack surface）及び最小特権の原則 b) 最も一般的なプログラミングエラーの分析を実行し、これらが低減されたことを文書化する。	干渉に関連記載あり	8.28.4	ソフトウェアの運用を開始する前に、攻撃対象領域（attack surface）及び最小特権の原則 を評価する。	ソフトウェアの運用を開始する前に、次の事項を評価する。 a) 攻撃対象領域（attack surface）及び最小特権の原則 b) 最も一般的なプログラミングエラーの分析を実行し、これらが低減されたことを文書化する。 コードの運用が開始された後、次のことを行う。 a) 要素はセキュリティに配慮してパケージ化し、適用する。 b) 報告された情報セキュリティのぜい弱性に対処する（8.8参照）。 c) エラー及び攻撃の疑いのログを取得し、必要に応じてコードを調整するためにログを定期的にレビューする。 d) ソースコードを、認可されていないアクセス及び改ざんから保護する。
–	（対応項なし）	8d-8.28.12	コードの運用が開始された後、次のことを行う。 a) 要素はセキュリティに配慮してパケージ化し、適用する。 b) 報告された情報セキュリティのぜい弱性に対処する。 c) エラー及び攻撃の疑いのログを取得し、必要に応じてコードを調整するためにログを定期的にレビューする。 d) ソースコードを、認可されていないアクセス及び改ざんから保護する。	干渉に関連記載あり			
–	（対応項なし）	8d-8.28.13	外部ツール及びライブラリを使用する場合、組織は次の事項を考慮する。 a) 外部ライブラリを管理し、リリースサイクルに合わせて規則正しく更新することを確実にする。 b) 十分に検査された構成要素、特に認証及び暗号化の構成要素の選択、認可及び再利用 c) 外部の構成要素の使用許可、セキュリティ及び整理 d) ソフトウェアが保守可能で、追跡することができ、実証された定評のある供給元に由来することを確実にする。 e) 開発資産及び成果物の十分に長期的な可用性	干渉に関連記載あり	8.28.5	【再】外部ツール及びライブラリを使用する場合のプロセスを整備する。	（8.28.5C対応する項を参照）
14.2.4.2	パッケージソフトウェアの変更が必要な場合は、組み込まれている機能及び処理の完全性が損なわれるリスクへの対応を行う。	8d-8.28.14	パッケージソフトウェアの変更が必要な場合は、組み込まれている機能及び処理の完全性が損なわれるリスクへの対応を行う。	干渉に関連記載あり			
14.2.4.3	パッケージソフトウェアの変更が必要な場合は、業者の同意を取得する。	8d-8.28.14	パッケージソフトウェアの変更が必要な場合は、業者の同意を取得する。	干渉に関連記載あり			
14.2.4.4	パッケージソフトウェアの変更が必要な場合は、標準のプログラム更新として、業者から必要とする変更が得られる可能性について確認を行う。	8d-8.28.14	パッケージソフトウェアの変更が必要な場合は、標準のプログラム更新として、業者から必要とする変更が得られる可能性について確認を行う。	干渉に関連記載あり			
14.2.4.5	パッケージソフトウェアの変更が必要な場合は、変更の結果として、将来のソフトウェアの保守に対して、組織が責任を負うようになるかどうかの確認を行う。	8d-8.28.14	パッケージソフトウェアの変更が必要な場合は、変更の結果として、将来のソフトウェアの保守に対して、組織が責任を負うようになるかどうかの確認を行う。	干渉に関連記載あり			
14.2.4.6	パッケージソフトウェアの変更が必要な場合は、用いている他のソフトウェアとの互換性について確認を行う。	8d-8.28.14	パッケージソフトウェアの変更が必要な場合は、用いている他のソフトウェアとの互換性について確認を行う。	干渉に関連記載あり			