番号	統制目標	番号	詳細管理策
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。		
3.3.2	評価		
		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
		3.3.2.2	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
3.3.3	指示		
		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
		3.3.3.2	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
3.3.4	モニタ		
		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
		3.3.4.2	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
3.3.5	コミュニケーション		
		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

番号	統制目標	番号	詳細管理策
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。
		4.4.1.2	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、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。
4.4.2	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
4.4.3	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

番号	統制目標	番号	詳細管理策
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
4.4.5	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。
		4.4.5.2	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]		
		4.4.6.1	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	統制目標	番号	詳細管理策
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。
		4.4.7.2	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)] ・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。

番号	統制目標	番号	詳細管理策
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。
		4.4.8.2	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。
		4.4.8.4	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。 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。
4.5.1	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。
		4.5.1.2	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	統制目標	番号	詳細管理策
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。
		4.5.2.2	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。）。
		4.5.2.4	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)] ・必要な力量を身につ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
		4.5.2.8	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)]
4.5.3	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

番号	統制目標	番号	詳細管理策
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、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、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]
4.5.5	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
		4.5.5.2	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。
4.6.1	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。
		4.6.1.2	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	統制目標	番号	詳細管理策
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
		4.6.2.2	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。[27001-9.2.2a)] ・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。[27001-9.2.2b)] ・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。[27001-9.2.2c)]
		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	統制目標	番号	詳細管理策
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。
		4.6.3.2	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。

番号	統制目標	番号	詳細管理策
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。[27001-10.2] ・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。[27001-10.2c)]
		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。[27001-10.2e)]
		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。[27001-10.2]
		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
4.8.1	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。
4.8.2	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。
		4.8.2.2	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。

番号	統制目標	番号	詳細管理策
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
4.9.2	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。
		4.9.2.2	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	統制目標	番号	詳細管理策
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	情報セキュリティ方針を策定し、トップマネジメントが承認する。
		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。
		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。
		5.1.4	クラウドサービスの提供及び利用に言及した、情報セキュリティ方針を策定する。
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。		
		5.2.1	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。
		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。
		5.2.3	（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、誤り及び回避のリスクを軽減するため。		
		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。
		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
5.4	管理層の責任 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。		
		5.4.1	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。
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。		
		5.5.1	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。
		5.5.2	（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。		
		5.6.1	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。
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、組織の脅威環境についての認識をもつため。		
		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。
		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。
		5.7.3	脅威インテリジェンス活動を実施する。
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 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。		
		5.8.1	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。
		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。
		5.8.3	（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）

番号	統制目標	番号	詳細管理策
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。		
		5.9.1	情報及びその他の関連資産の目録を作成し、維持する。
		5.9.2	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。
		5.9.3	（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。		
		5.10.1	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。
		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。
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。		
		5.11.1	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。
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。		
		5.12.1	情報の分類や分類体系に関する方針を策定し、分類する。
		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。
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。		
		5.13.1	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。
		5.13.2	（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。		
		5.14.1	転送中の情報を保護するための方針を策定する。
		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。
		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。
		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。
		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。
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。		
		5.15.1	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。
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。		
		5.16.1	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。
		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。
		5.16.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	統制目標	番号	詳細管理策
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。		
		5.17.1	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。
		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。
		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。
		5.17.4	（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。		
		5.18.1	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。
		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。
		5.18.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
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。		
		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。
		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。
		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。
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。		
		5.20.1	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。
		5.20.2	供給者との合意の登録簿を作成し、維持する。
		5.20.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
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。		
		5.21.1	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。
		5.21.2	（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）
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、レビューし、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。		
		5.22.1	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。
		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。
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。		
		5.23.1	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。
		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。
		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。
		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。

番号	統制目標	番号	詳細管理策
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。		
		5.24.1	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。
		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。
		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。
		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。
		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。
		5.24.6	（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。		
		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。
		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。
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。		
		5.26.1	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。
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。		
		5.27.1	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。
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。		
		5.28.1	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。
		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。
		5.28.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
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。		
		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。
		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。
		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。
5.30	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。		
		5.30.1	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。
		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。
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。		
		5.31.1	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。
		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。
		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。
		5.31.4	（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）
		5.31.6	（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）

番号	統制目標	番号	詳細管理策
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。		
		5.32.1	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。
		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。
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。		
		5.33.1	記録を保護するための方針を策定する。
		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。
		5.33.3	記録を保護するための対策を実施する。
		5.33.4	（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。		
		5.34.1	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。
		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。
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。		
		5.35.1	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。
		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、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。
		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層及び適切な場合には、トップマネジメントに報告する。
		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層は是正処置を指示する。
		5.35.5	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
		5.35.6	（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）
		5.35.8	（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）
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。		
		5.36.1	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。
		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。
		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。
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。		
		5.37.1	情報処理設備における操作手順書を作成する。
		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。
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、組織に加わる前に、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。		
		6.1.1	要員になる候補者の確認の基準及び制約を定める。
		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。
		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。
		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。

番号	統制目標	番号	詳細管理策
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。		
		6.2.1	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。
		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。
		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。
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。		
		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。
		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。
		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。
		6.3.4	（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。		
		6.4.1	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。
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。		
		6.5.1	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。
		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。
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、定常的にレビューし、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。		
		6.6.1	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。
		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。
		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。
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。		
		6.7.1	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。
		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。
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。		
		6.8.1	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。
		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ぜい弱性の立証や検査を試みないように要求する。
		6.8.3	（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）
		6.8.5	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
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。		
		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。
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。		
		7.2.1	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。
		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。

番号	統制目標	番号	詳細管理策
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。		
		7.3.1	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。
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。		
		7.4.1	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。
		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。
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。		
		7.5.1	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。
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		
		7.6.1	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。
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。		
		7.7.1	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。
		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。
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。		
		7.8.1	装置を保護するためのセキュリティ対策を実施する。
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。		
		7.9.1	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。
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。		
		7.10.1	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。
		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。
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。		
		7.11.1	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。
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。		
		7.12.1	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。
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。		
		7.13.1	装置を保守するためのセキュリティ対策を実施する。

番号	統制目標	番号	詳細管理策
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。		
		7.14.1	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。
		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。
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。		
		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。
		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。
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。		
		8.2.1	特権的アクセス権の割当て及び利用を制限し、管理する。
		8.2.2	（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。		
		8.3.1	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、制限する。
		8.3.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
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。		
		8.4.1	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。
		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。
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。		
		8.5.1	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。
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。		
		8.6.1	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。
		8.6.2	資源の利用を監視する。
		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。
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。		
		8.7.1	情報及びその他の関連資産をマルウェアから保護する。
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。		
		8.8.1	技術的ぜい弱性を特定し、評価する。
		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。
		8.8.3	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
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。		
		8.9.1	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。
		8.9.2	構成を監視し、定期的にレビューする。
		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。

番号	統制目標	番号	詳細管理策
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。		
		8.10.1	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。
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。		
		8.11.1	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。
		8.11.2	特定したデータマスキング手法を実装する。
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。		
		8.12.1	データ漏えいのリスクへの対策を実施する。
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。		
		8.13.1	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。
		8.13.2	バックアップ計画を策定し、実装する。
		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。
		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。
		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
		8.13.6	（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）
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。		
		8.14.1	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。
		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。
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。		
		8.15.1	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。
		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。
		8.15.3	ログ分析を実施する。
		8.15.4	（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。		
		8.16.1	監視の範囲及びレベルを定義する。
		8.16.2	リアルタイム又は定期的な間隔で監視を行う。
		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。
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。		
		8.17.1	クロックは、組織が採用した時刻源と同期させる。
		8.17.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
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。		
		8.18.1	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。

番号	統制目標	番号	詳細管理策
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、技術的ぜい弱性の悪用を防止するため。		
		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。
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。		
		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。
		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。
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。		
		8.21.1	ネットワークサービスの利用に関する規則を整備する。
		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。
		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。
		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。
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。		
		8.22.1	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。
		8.22.2	無線ネットワークの分離の要件を定め、実装する。
		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。
		8.22.4	（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）
		8.22.6	（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。		
		8.23.1	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。
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。		
		8.24.1	情報を保護する上での一般原則も含む、暗号化に関する方針を策定する。
		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、破壊するため及び改変、紛失から保護するために、セキュリティを保ったプロセス及び手順を整備し、実施する。
		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らを利用した安全なプロトコルを定める。
		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（殆）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整備する。
		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。
		8.24.6	（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）
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。		
		8.25.1	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。
		8.25.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）

番号	統制目標	番号	詳細管理策
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。		
		8.26.1	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。
		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。
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。		
		8.27.1	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。
		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。
		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。
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。		
		8.28.1	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。
		8.28.2	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。
		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。
		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。
		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。
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。		
		8.29.1	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。
		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。
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。		
		8.30.1	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。
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。		
		8.31.1	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。
		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。
		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。
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。		
		8.32.1	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。
		8.32.2	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）
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。		
		8.33.1	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。
		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。
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。		
		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。

番号	統制目標	番号	詳細管理策
9.1	（JIS Q 27017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策）		
		9.1.1	（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）		
		9.2.1	（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）
		9.2.3	（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）		
		9.3.1	（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）
		9.3.3	（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）
9.4	（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）
9.5	（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）
9.6	（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）
		9.6.2	（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）
		9.6.4	（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）		
		9.7.1	（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）