

添付C 対策要件に応じたセキュリティ対策例

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.OC-01	・組織は、自組織のミッションを理解し、サイバーセキュリティリスクマネジメントにおける判断に用いる。	L1_1_a_ORG L1_1_b_ORG L1_1_c_ORG	<High-Advanced><Advanced><Basic>共通 ・組織は、自組織のミッションを組織内部及び外部の要員に共有し、そのミッションの遂行を妨げ得るサイバーセキュリティリスクを特定、分析、評価及び対応するための判断材料とする。	0	-	○ (PM-11)	-	-	-
CPS.GV.OC-02	・組織は、サイバーセキュリティに関する法的要求事項や、規制上の要件、契約上の要求事項（プライバシー及び市民的自由の義務を含む）、及び業界のガイドライン等を理解した上で、それらを考慮した社内ルールを策定する。	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO L1_2_a_ORG L1_2_a_COM L1_2_a_SYS L1_2_a_PRO L1_2_a_DAT L3_4_a_ORG L3_4_b_ORG	<High-Advanced><Advanced><Basic>共通 ・組織は、その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。 ・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遵守を考慮する。 ・組織は、自組織の事業活動において、セキュリティの文脈で関連するすべての法令、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、文書化する。 ・組織は、モニタリング業務に自社に関係する法制度、業界標準、顧客との契約事項等が存在するか、存在するならばどのような制約があるかを認識した上で社内ルールを策定する。 ・組織は、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も定め、文書化する。 ・組織は、策定・見直した社内ルールを役員、従業員、派遣社員及び受入出向者へと周知する。 ・組織は、自社に関連する法令、規制、契約上の要求事項等の改定状況を確認し、年1回以上の頻度で社内ルールを点検する。 【参考】情報セキュリティ関連法令には、例えば、不正競争防止法、電子署名認証法、e-文書法、個人情報保護法、不正アクセス禁止法等がある。また、上記の法令等の遵守に際しては、関連各省庁から発出されているガイドライン文書等（例：不正競争防止法：「営業秘密管理指針」（経済産業省、2025年、3月）、「限定提供データに関する指針」（2024年、2月）、個人情報保護法：「個人情報の保護に関する法律についてのガイドライン(通則編)」（個人情報保護委員会、2026年、6月）、「個人情報の保護に関する法律についてのガイドライン(匿名加工情報編)」（個人情報保護委員会、2026年、4月)）を参照することが望ましい。	0	○ (03.15.03 行動指針 a)	○ (AC-01、AT-01、AU-01、CA-01、CM-01、CP-01、IA-01、IR-01、MA-01、MP-01、PE-01、PL-01、PM-01、PS-01、PT、RA-01、SA-01、SC-01、SI-01、SR-01)	-	-	
CPS.GV.OC-03	・組織は、自組織が事業を継続する上で、自組織及び関係する他組織における依存関係と重要な機能を特定し、共有する。	L1_3_b_ORG	<High-Advanced> ・組織は、自らの事業を継続する上で、自組織が有する下記のサポートユーティリティの果たす機能及び依存関係を特定する。 - 通信サービス - 電力設備（電力ケーブル等を含む） ・上記で識別されたユーティリティの内、事業継続という観点から重要な役割を果たすものについて、下記のような対策を講ずることを検討する。 - 代替通信サービスの確立 - 情報システム及び産業用制御システムの電力設備及び電力ケーブルの物理的保護 - 短期無停電電源装置の準備 ・特に、代替通信サービスの利用を検討する際、下記について考慮する - 通信サービス事業者との契約事項を検討する際、組織の可用性に関する要求事項（目標復旧時間を含む）を明確にする - 一次通信サービスとの間で単一障害点が共有される可能性を低減する	0	-	○ (下記に加えて、CP-02(08)、RA-09)	-	-	-
			<Advanced> ・組織は、自組織のミッション達成に不可欠な資産及び業務、並びにそれらの業務の喪失（又は部分的喪失）による潜在的影響を特定する。 ・組織の重要なケイバビリティ及びサービスにおいて、障害点となり得る外部依存関係を特定し、文書化するとともに、その情報を適切な要員と共有する。 ・組織は、システムの可用性に対する要求水準に応じて、その容量・能力に関する要求事項を特定する。 ・組織は、自組織が利用する情報システム及び産業用制御システムが、要求されたシステム性能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。	0	-		-	-	-
			<Basic> ・自組織の事業継続の観点から、組織のケイバビリティ及びサービスのうち重要なものを判定するための基準を確立する。 ・組織の外部リソース（例：設備、クラウドベースのホスティングプロバイダ）及びサプライヤーへの依存関係、及びそれらと組織の資産・業務機能との関連性を示したインベントリを作成する。	0	-	○ (CP-02、PM-08、PM-11、PM-30(01)、SA-09)	-	-	-
CPS.GV.RM-01	・組織は、リスクマネジメントの目的を定め、関係するステークホルダーとの間で合意する。	L1_1_a_PRO L1_1_b_PRO L1_1_c_PRO	<High-Advanced><Advanced>共通 ・組織は、年次のサイバーセキュリティ戦略策定時、及び重大な変化が発生した際に、短期的及び長期的なサイバーセキュリティリスクマネジメントの目的を更新する。 ・経営層がサイバーセキュリティの目的について合意し、その目的に基づいてリスク及び成果を測定・管理する。	0	-	○ (PM-09、RA-07、SR-02)	-	-	-
			<Basic> ・組織は、サイバーセキュリティリスクマネジメントの目的を具体化した、測定可能な目標（例：利用者教育の品質を管理する、産業用制御システムをリスクから適切に保護する）を設定する。	0	-		-	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.RM-02	・組織は、サイバーセキュリティリスクマネジメントを適切に行うために、サイバーセキュリティ戦略を策定する。	L1_1_a_PRO L1_1_b_PRO L1_1_c_PRO	<High-Advanced> ・組織は、サイバーセキュリティ戦略の策定時及び改定時に、重要度の高い取引先との間で、サイバーセキュリティ戦略に関するインタビューを実施することで、セキュリティ上のリスクや必要な対策に関する認識を合致させる。その際、下記事項を扱うことが望ましい。 - 自組織の事業内容及び事業の継続に関わる主なセキュリティリスク - 上記リスクが顕在化した際の、取引先における影響の内容とその規模 - 上記セキュリティリスクへの対応方針 - （リスクマネジメント戦略改定時の場合）内外の情勢の変化及び前回の版から変更すべきと考える主要なポイント	0	-	-	-	-	-
			<Advanced><Basic>共通 ・組織は、情報システム及び産業用制御システムの運用と使用により生じる組織の業務と資産、個人、他の組織等に対するリスクを管理するための、包括的なサイバーセキュリティ戦略を策定する。 ・組織は、サイバーセキュリティ戦略を組織全体にわたって一貫性が保たれるように実施する。 ・組織の経営層は、組織のサイバーセキュリティ戦略の内、セキュリティに関わるものについて、下記のような観点を定期的にレビューする。 - どの程度の攻撃に直面しているのか（検知しているのか） （アンチウイルス製品/IDSによる検出件数、最新の脅威動向等） - セキュリティ対策の状況は計画通りか （マルウェア対策、セキュリティパッチ適用等の実施すべきセキュリティ対策の適用率等） - 攻撃者（内部犯行を含む）の侵入を許したか、あるいはその可能性はあるか （セキュリティ監視活動を通じた外部からの侵入あるいは内部犯行が疑われるイベントの説明） - 直接情報システムや産業用制御システムとは関係しないセキュリティの状況はどのようなものか （退職者、PCやデバイスの紛失、盗難の発生状況等） ・組織は、経営層によるレビューの結果を文書化し、保管する。 ・組織は、サイバーセキュリティ戦略を定期的、あるいは組織的变化に対処するため必要な場合にレビューし、更新する。	0	-	-	-	-	-
CPS.GV.RM-03	・組織は、自組織におけるリスク選好度及びリスク許容度を定め、組織内に周知する。	L1_1_a_SYS L1_1_a_PRO L1_1_b_SYS L1_1_b_PRO L1_1_c_SYS L1_1_c_PRO	<High-Advanced> ・組織は、自組織におけるセキュリティインシデントにより望ましくない影響を受ける可能性がある重要な取引先に対して、自組織のリスク許容度に関する認識を共有する。	0	-	○ (PM-09)	-	-	-
			<Advanced> ・組織は、サプライチェーンに係るリスクの現状把握及びリスクアセスメントの結果を所与として、自組織におけるリスク選好度及びリスク許容度を決定し、組織内に周知する。 ・組織は、残存リスクを含む、把握しているリスクの状況を踏まえ、組織のリスク選好度及びリスク許容度を定期的に見直す。	0	-		-	○ (6.3.1.1、8.2.6.1)	-
			<Basic> ・組織は、リスクアセスメントの結果を所与として、自組織におけるリスク選好度及びリスク許容度を決定し、組織内に周知する。 ・組織は、残存しているリスクの受容について、リスク所有者の承認を得る。 ・組織は、リスク対応結果を文書化し、リスク許容度の基準及び許容したリスクの一覧を安全に保持する。	0	-		-		-
CPS.GV.RM-04	・組織は、サイバーセキュリティリスクマネジメントの活動及びその結果を、組織のリスクマネジメントプロセスに組み込み、当該プロセスの中でサイバーセキュリティリスクを管理する。	-	<High-Advanced><Advanced>共通 ・組織は、サイバーセキュリティリスクを、他の事業リスク（例：コンプライアンス、財務、業務、規制、レピュテーション、安全）と併せて集約し、管理する。	0	-	○ (下記に加えて、SA-24)	-	○ (6.2.1.1)	-
			<Basic> ・組織のリスクマネジメントの計画策定に、サイバーセキュリティリスクの管理者を関与させる。 ・組織のリスクマネジメントにおいて、サイバーセキュリティリスク（例：リスク許容度を超えるリスクの検知、リスク対応方針の変更を要する重大なリスク環境の変化、担当部署では判断できないリスク受容の判断）をエスカレーションするための基準を確立する。	0	-	○ (PM-03、PM-09、PM-30、RA-07、SR-02)	-		-
CPS.GV.RM-05	・組織は、リスク対応における選択肢及びその運用に係る方針を策定し、組織内に共有する。	L1_1_a_PRO L1_1_b_PRO L1_1_c_PRO	<High-Advanced><Advanced>共通 ・組織は、サイバー保険の加入可否を判断する。	0	-	○ (PM-09、PM-28、PM-30、SR-02)	-	○ (6.3.1.1)	-
			<Basic> ・組織は、データの様々な分類区分ごとに、サイバーセキュリティリスクの受容及び回避に関する基準を明確化する。 ・組織は、責任共有モデルが許容される条件（例：特定のサイバーセキュリティ機能のアウトソーシング、組織を代理する第三者による金融取引の実施、パブリッククラウドベースのサービスの利用）を文書化する。	0	-		-		-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみ適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.RM-06	・組織は、取引先及びその他の第三者によるリスクを含むサイバーセキュリティリスクについて、組織全体にわたるコミュニティ系統を明確にし、運用する。	L1_1_a_PEO L1_1_b_PEO	<High-Advanced><Advanced>共通 ・経営幹部、取締役、及び管理職に対し、組織のサイバーセキュリティ態勢を報告する頻度及び方法を定め、関係者間で合意する。 ・組織は、組織内の全部門（例：経営、業務、内部監査、法務、調達、物理セキュリティ、人事）が、サイバーセキュリティリスクについて相互にコミュニケーションを取る方法を明確化する。	0	○ (03.14.03 セキュリティアラート、勧告、および指令 a)	○ (PM-09、PM-30)	-	-	-
			<Basic> ・組織は、平時のセキュリティ推進活動に必要な役員(例えば、CISOを設置する会社の場合は、当該CISO)及びセキュリティ担当部署の連絡先リストを定める。 ・組織は、年1回以上の頻度で、平時のセキュリティ推進活動に必要な役員及びセキュリティ担当部署の連絡先リストについて点検する。	0	-		-	-	-
CPS.GV.RM-07	・組織は、サイバーセキュリティリスクの評価、文書化、分類及び優先順位付けに関する標準的な方法を整備し、組織内に共有する。	L1_1_a_PRO L1_1_b_PRO L1_1_c_PRO	<High-Advanced><Advanced><Basic>共通 ・組織は、サイバーセキュリティリスク分析に定量的アプローチを用いるための基準を確立し、リスクの起こりやすさ及び影響度の算出式を明確化する。 ・組織内のリスクマネジメントを実施する単位ごとに、リスクの優先順位付けを行うための基準を確立する。 ・サイバーセキュリティリスクの統合、集約、比較を行う際、統一されたリスク分類を活用する。 ・組織は、サイバーセキュリティリスクに関する情報（例：リスクの内容、影響度、対応、所有者）を文書化するためのテンプレート（例：リスク管理簿）を作成し、利用する。	0	-	○ (PM-09、PM-18、PM-28、PM-30、RA-03)	-	○ (6.3.1.1)	-
CPS.GV.RM-08	・組織は、戦略的機会（組織にとってプラスに働くリスク）を特定し、その特性を整理した上で、組織のサイバーセキュリティリスクに関する議論に含める。	L1_1_a_ORG L1_1_b_ORG L1_1_c_ORG	<High-Advanced><Advanced>共通 ・組織は、戦略的機会（プラスに働くリスク）を特定し、リスクに関する議論に含めるための手法等（例：SWOT分析）を定義し、伝達する。	0	-	○ (PM-09、PM-18、PM-28、PM-30、RA-03)	-	-	-
			<Basic> ・組織は、プラスに働くリスクとマイナスに働くリスクを併せて算定し、文書化し、優先順位付ける。	0	-		-	-	-
CPS.GV.RR-01	・組織の経営層は、サイバーセキュリティリスクに対する責任及び説明責任を負い、当該リスクを認識した上で、倫理的かつ継続的に改善する文化を醸成する。	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO	<High-Advanced><Advanced>共通 ・組織は、セキュリティリスクが経営に重大な影響を及ぼすことを前提として、その対応について、経営層が参加する情報セキュリティ委員会等の経営判断ができる体制を設置する。 ・組織は、サイバーセキュリティに関連する出来事が発生した際に、セキュリティ及び倫理に対する経営層の期待やメッセージを組織内に共有する。 ・組織のCISOに対し、サイバーセキュリティリスク戦略を維持し、少なくとも年次及び重大な出来事の発生後に、当該戦略をレビューし、更新するよう、経営層は指示する。	0	-	○ (PM-02、PM-19、PM-23、PM-24、PM-29)	○ (下記に加えて、A.5.4)	○ (6.2.3.1)	-
			<Basic> ・組織のサイバーセキュリティ戦略の策定、実施、及び評価における自らの役割と責任について、経営層（例：取締役）間で互いに合意する。	0	-		○ (A.5.2)		-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみ適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.RR-02	・組織は、自組織のサイバーセキュリティリスクマネジメントに関する役割、責任及び権限を定め、組織内へ周知する。	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO L1_3_a_ORG L1_3_c_PEO	<High-Advanced><Advanced>共通 ・組織は、脆弱性情報/脅威情報の収集から対応まで担当部署の役割・責任を定める。 ・組織は、サイバーセキュリティ、IT、業務、法務、人事、エンジニアリング等、サプライチェーンリスクマネジメントに関わる部門間の連携体制を、組織横断的に確立する。 ・サイバーセキュリティリスクマネジメントの責任を担う者が、業務を遂行するために必要な権限を有していることを確認するため、経営層によるレビューを定期的に実施する。 ・組織は、情報システムの運用に関わる部署と、産業用制御システムの運用に関わる部署間で、サイバーセキュリティリスクマネジメントに関する継続的な連携を確立し、維持する。 ・組織間のモノの流れ、データの流れ等を考慮して、自組織の関係するサプライチェーンの概要を、自組織の全体における役割がわかるように図示する。 ・組織は、上記の図示結果を関係する他組織（自組織からの発注先、自組織内の関係部門、自組織への発注元）と共有する。	0	-	○ (PM-02、PM-13、PM-19、PM-23、PM-24、PM-29)	○ (A.5.2)	○ (6.2.3.1)	-
			<Basic> ・組織は、セキュリティを統括する役員(例えば、CISOを設置する会社の場合は、当該CISO)及びセキュリティ担当部署の役割・責任を定める。 ・組織は、セキュリティインシデント発生時におけるセキュリティを統括する役員(例えば、CISOを設置する会社の場合は、当該CISO)及びセキュリティ担当部署の役割・責任を定める。 ・組織は、業務部門、リスク管理部門、及び内部監査部門の中で、サイバーセキュリティに関する責任を明確化する。 ・組織は、情報システム、産業用制御システムの双方において、自組織におけるセキュリティリスク対応の責任者を明確にする。 ・組織は、サイバーセキュリティリスクマネジメントに関する役割と責任を、セキュリティポリシーに文書化する。 ・組織は、サイバーセキュリティリスクマネジメントに関する役割と責任を、職務記述書に含める。 ・組織は、サイバーセキュリティサプライチェーンリスクマネジメント活動の実行責任者及び説明責任者と、関係するチーム及び個人への相談・情報共有の方法を文書化するため、責任分担表を作成する。 ・組織は、組織間のモノの流れ、データの流れ等を考慮して、自組織からの発注先、自組織、自組織への発注元という取引関係の概要を、自組織の役割がわかるように図示する。 ・上記の図示の結果を関係する他組織（自組織からの発注先、自組織内の関係部門、自組織への発注元）と共有する。 ・組織は、委託先あるいは委託元との契約において、業務においてセキュリティインシデントにより損害が発生した場合の自組織と取引先の責任範囲（免責事項の明記、損害賠償額の契約金額等での上限設定等）を規定する。 [参考] 特にクラウドサービスプロバイダーと自組織との役割と責任に関して、追加の情報を得るために、総務省「クラウドサービス提供における 情報セキュリティ対策ガイドライン（第3版）」の「1. 6. クラウドサービス事業者とクラウドサービス利用者の責任」を参照することが可能である。	0	○ (03.06.05 インシデント対応計画 a)			-	
CPS.GV.RR-03	・組織は、セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を設置し、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	L1_3_a_ORG	<High-Advanced> ・組織は、セキュリティ対応組織を立ち上げ、産業用制御システム、IoTシステム等も管轄に含めて、組織内で統合的にセキュリティ対策を取る体制を整える。 [参考] セキュリティ対応組織(SOC/CSIRT)を評価するためのメトリクスには、「セキュリティ対応組織サービスポートフォリオセルフチェックシート」(ISOG-J, 2024年)や、SIM3(Security Incident Management Maturity Model)等がある。	0	-	-	○ (A.5.2、A.5.24)	-	-
			<Advanced> ・組織は、サイバー攻撃及び脆弱性に関する公開情報又は非公開情報を活用する体制を整備する。 ・組織は、セキュリティ管理責任者を中心に、セキュリティ対応組織を立ち上げ、主に情報システムや事業における重要度の高いIoTシステムを管轄対象として、組織内でセキュリティ対策を取る体制を整える。 [参考] セキュリティ対応組織(SOC/CSIRT)の業務、望まれる規模等については、「セキュリティ対応組織（SOC/CSIRT）の教科書 ～X.1060フレームワークの活用～」(ISOG-J, 2025年, 10月)等を参照することが望ましい。	0	○ (下記に加えて、03.06.01 インシデント処理)	-		○ (6.2.3.1)	-
			<Basic> ・組織は、情報システム及び産業用制御システムの双方におけるセキュリティ管理責任者／担当者を明確化し、社内・社外向けのセキュリティ関係の窓口とする。	0	○ (03.06.02 インシデントの監視、報告、対応支援 d)	-	○ (A.5.2、A.5.24、A.6.8)	-	
CPS.GV.RR-04	・組織は、サイバーセキュリティ戦略、役割、責任及びポリシーに応じて、必要なリソースを確保する。	L1_3_a_ORG	<High-Advanced><Advanced><Basic>共通 ・組織は、情報システム及び産業用制御システムまたはシステムサービスを保護するのに必要なリソースを、リスク許容度及びリスク対応方針等を踏まえて決定・文書化のうえ割り当てる。 ・組織は、セキュリティの個々の予算項目を、組織の計画及び予算関連の資料に記載する。	0	-	○ (PM-03)	-	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.RR-05	・組織は、人の異動に伴い生じる役割の変更に対応した対策に、セキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO	<High-Advanced> ・組織は、機微な役割に就く新規採用者の入社手続き前にバックグラウンドチェックを実施するとともに、当該役割に就いている要員に対して、定期的にバックグラウンドチェックを繰り返す。 ・組織は、自組織の要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。 ・組織は、自組織の要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。	0	-	○ ○ (PM-13、PS-01、PS-07、PS-09)	○ (A.6.1、A.6.5)	○ (6.2.2.1)	-
			<Advanced> ・組織は、人事プロセス（例：人材スクリーニング、入社手続き、異動通知、退職手続き）に、サイバーセキュリティリスクマネジメントの観点を組み込む。 ・組織は、機密情報を扱う要員に対しては特に、採用から退職に至るまでのサイクル全体に渡り、セキュリティ上の責任に対処する。 ・組織は、採用、研修、及び人材維持に関する意思決定において、サイバーセキュリティの知識をプラスの要素として考慮する。 ・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、自組織の要員の退職時及び任期満了時に、機密情報及び情報機器を回収する。 - 回収物には、情報(印刷物及び記憶媒体)、パソコン、スマートデバイス及びアクセス権(ID及び鍵)を含める。 - 回収漏れが起こらない手順(例：回収物一覧のチェックシートの作成)を整備する。 ・組織は、年1回以上の頻度で、退職時及び任期満了時における機密情報及び情報機器の回収の状況について点検する。	0	○ (下記に加えて、03.01.01 アカウント管理 g、03.09.02 退職と異動 a)		○ (A.5.11、A.6.1、A.6.5)	-	
			<Basic> ・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。 ・組織は、雇用条件においてセキュリティに係る要員の責任について明記する。雇用終了後の情報漏えい等を抑止するため、この責任は、雇用終了後の妥当な期間に渡って持続するよう記載する。 ・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・組織は、要員の退職時に以下を実施する。 - 自組織のシステムに対するアクセスを一定期間内に無効にする。 - 職員に関連する認証及びクレデンシャルを無効にする。 - 退職する個人が管理していた組織の情報と情報システムに対するアクセスを保持する。	0	○ (03.01.01 アカウント管理 f、03.09.01 職員のスクリーニング a、03.09.02 退職と異動 b、03.10.01 物理的アクセス認可 d)		○ (A.6.1、A.6.5)	○ (6.2.2.1、11.2.2.1)	-
CPS.GV.PO-01	・組織は、自組織の状況、サイバーセキュリティ戦略、優先順位等に基づいてセキュリティポリシーを策定し、組織内及び自組織の取引に関係する者（必要に応じてサプライヤー、第三者プロバイダ等を含む）に伝達し、実施する。	L1_1_a_PEO L1_1_a_PRO L1_1_b_PEO L1_1_b_PRO L1_1_c_PEO L1_1_c_PRO	<High-Advanced> ・組織は、従来のIT環境において運用されているものと基本的な方針を共有しつつ、産業用制御システム等、IoT機器が設置されるサイトの性質等を十分に考慮したセキュリティポリシー群、運用手順を策定する。 [参考] 例えば、産業用制御システム(ICS)を対象としたセキュリティマネジメント規格であるIEC 62443-2-1では、ICS環境のための上位レベルのサイバーセキュリティポリシーの策定を求めている。特に、産業分野におけるセキュリティポリシー及び運用手順の策定にあたっては、「制御システムセキュリティ運用ガイドライン」（日本電気制御機器工業会, 2017年）等を参考とすることができる。	0	-	○ (03.15.01 ポリシーおよび手順 a、03.15.03 行動指針 b)	○ (A.5.1、A.5.10)	○ (6.2.1.1)	-
			<Advanced> ・組織は、組織の業務、組織の資産、個人、他の組織等にもたらされるリスクを考慮して、自組織のミッション／業務プロセスを定義し、活動に関する優先順位付けを確立する。 ・組織は、情報システムを対象としたセキュリティポリシー群の策定に当たり、自組織の事業戦略、関係する規制、法令及び契約、セキュリティの脅威環境を十分に考慮して、自組織の実情を十分に反映したものとなるよう策定を実施する。 ・組織は、上位の方針を支えるセキュリティポリシー群のより低いレベルとして、例えば、情報システムを対象とした下記のようなトピック個別の方針及び実施手順を策定する。 - アクセス制御及び認証 - 物理的セキュリティ対策 - システムの開発及び保守 - 外部委託先管理 - 情報分類及び取扱い ・組織は、産業用制御システム固有のポリシーと手順の策定にあたって、情報システム向けのセキュリティ管理策をそのまま適用出来ない点を考慮して、重要な運用機能、産業用制御システム固有のセキュリティ上の懸念、および代替管理策の優先順位を識別する。 ・組織は、入社時、毎年、及びセキュリティポリシーが更新された都度、自組織の要員からセキュリティポリシーを遵守することについての同意を得る。 [参考] より詳細なレベルの方針策定の際には、ISO/IEC 27002 等の関連する標準を参照して方針が必要となる分野を把握したうえで、「中小企業の情報セキュリティ対策ガイドライン 第4.0版」(IPA, 2026年) 付録5「情報セキュリティ関連規定（サンプル）」や、「情報セキュリティポリシーサンプル改版 (1.0版)」（JNSA, 2016年)等を参考にすることができる。	0	○ (AC-01、AT-01、AU-01、CA-01、CM-01、CP-01、IA-01、IR-01、MA-01、MP-01、PE-01、PL-01、PM-01、PS-01、PT-01、RA-01、SA-01、SC-01、SI-01、SR-01)		-	-	
			<Basic> ・組織は、自組織のセキュリティポリシー群の最も高いレベルに、セキュリティ基本方針を策定し、経営層の承認を得た後、適切な適用範囲（例：企業全体、事業部全体）で運用する。 ・組織は、自組織のセキュリティ基本方針を定期的(例えば、1年に1度)にレビュー、更新し、経営層の承認を得る。 ・組織は、あらかじめ優先して継続・復旧すべき中核事業及び重要と考えられる業務を特定しておき、事業継続の観点から重要なリソース(関係する他組織、ヒト、モノ、データ、システム等)と機能を特定し、優先順位付けする。 ・組織は、特に産業用制御システムに関して、自組織の事業活動の適切でない運用によりHSE(Health, Safety and Environment)への悪影響が発生するかも考慮してリソースの分類、優先順位付けを行う。 [参考] セキュリティポリシーの策定に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第4.0版」(IPA, 2026年) 付録5「情報セキュリティ関連規定（サンプル）」における"1. 組織的対策"の記載や、「情報セキュリティポリシーサンプル改版 (1.0版)」（JNSA, 2016年)における"01_情報セキュリティ基本方針"、"01_情報セキュリティ方針"等を参考とすることが可能である。	0	-		○ (A.5.1)	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.PO-02	・組織は、要件、脅威、技術及び自組織のミッションの変化を踏まえ、セキュリティポリシーを定期的にレビューし、必要に応じて更新する。	L1_1_a_PEO L1_1_a_PRO L1_1_b_PEO L1_1_b_PRO L1_1_c_PEO L1_1_c_PRO	<High-Advanced><Advanced><Basic>共通 ・組織は、法律や規制の変更、技術の変化（例：人工知能の導入）及び事業の変化（例：新規事業の取得、新規契約上の要求事項）等を踏まえ、年1回以上の頻度でセキュリティポリシーを更新する。	O	○ (03.15.01 ポリシーおよび手順 b、03.15.03 行動指針 d)	○ (AC-01、AT-01、AU-01、CA-01、CM-01、CP-01、IA-01、IR-01、MA-01、MP-01、PE-01、PL-01、PM-01、PS-01、PT-01、RA-01、SA-01、SC-01、SI-01、SR-01)	○ (A.5.1)	○ (6.3.4.1)	-
CPS.GV.OV-01	・組織は、サイバーセキュリティ戦略の成果をレビューし、当該結果及び内外の環境変化等を踏まえ、サイバーセキュリティ戦略並びに組織全体の戦略及び方向性を必要に応じて見直す。	-	<High-Advanced><Advanced><Basic>共通 ・組織は、サイバーセキュリティ戦略及びその結果が、経営層の意思決定や組織目標の達成にどの程度貢献しているかを測定する。 ・組織は、サイバーセキュリティ戦略が業務又はイノベーションの妨げとなっていないかを確認し、必要に応じて見直す。 ・組織は、監査結果等を踏まえ、既存のサイバーセキュリティ戦略が内部及び外部の要件へ準拠しているかを検証する。 ・組織は、サイバーセキュリティインシデントを踏まえ、サイバーセキュリティ戦略をレビューする。	O	-	○ (AC-01、AT-01、AU-01、CA-01、CM-01、CP-01、IA-01、IR-01、MA-01、MP-01、PE-01、PL-01、PM-01、PM-09、PM-18、PM-19、PM-30、PM-31、PS-01、PT-01、RA-01、RA-07、SA-01、SC-01、SI-01、SR-01、SR-06)	-	-	-
CPS.GV.OV-02	・組織は、自組織のサイバーセキュリティリスクマネジメントの実施状況をレビューし、必要に応じて見直す。	-	<High-Advanced> ・組織が直面しているリスクを特定するため、セキュリティ担当部署は、発生確率及び潜在的影響度を含む重要リスク指標（KRI）を定期的にレビューする。	O	-	○ (下記に加えて、SR-06)	○ (下記に加えて、A.5.35)	○ (6.3.4.1)	-
			<Advanced> ・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織及びシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には以下を含むことが望ましい。 - ログ分析の分析結果（対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等） - モニタリングにおける今後の改善方針 ・セキュリティ担当部署は、年1回以上、セキュリティを統括する役員(例えば、CISOを設置する会社の場合は、当該CISO)に対して、自組織のセキュリティ対策の点検結果を踏まえたセキュリティ対策の実態及び当該実態を踏まえて策定した今後の対策推進計画を報告し承認を得た上で、当該報告結果を社内部署と共有する。 ・セキュリティ担当部署からセキュリティを統括する役員（例：CISO）への対策推進計画の報告に際し、役員からの改善に向けた指示があった場合、セキュリティ担当部署は、当該指示内容の記録、計画への反映及び不備の是正を実施する。 ・組織は、第三者によるセキュリティ評価（セキュリティ監査等）を実施する。	O	-				
			<Basic> ・組織は、セキュリティ対応状況の評価を適切かつ計画的に実施するため、以下に示す事項を含めたセキュリティに係る自己点検の計画を策定した上で、自己点検を実施する。 - 点検の対象とするセキュリティ対策 - セキュリティ対策の有効性を図るために用いる点検手順 - 点検を実施する環境や実施体制 - 点検結果の取りまとめ方法とその活用方法	O	○ (03.12.01 セキュリティアセスメント、03.15.02 システムセキュリティ計画 b)	○ (PM-04、PM-06、RA-07)	○ (A.5.36)		-
CPS.GV.SC-01	・組織は、サプライチェーンに係るリスクマネジメントに関するプログラム、戦略、目的、ポリシー及びプロセスを明確にし、組織のステークホルダーと合意の上、運用する。	L1_1_a_ORG L1_1_a_PRO L1_1_b_ORG L1_1_b_PRO L1_1_c_ORG L1_1_c_PRO	<High-Advanced> (該当なし)	-	-	-	-	-	-
			<Advanced><Basic>共通 ・組織は、プログラムの実施及び改善計画（マイルストーン付き）、ポリシー、及び手順を含む、サイバーセキュリティサプライチェーンリスクマネジメントに関するプログラムを策定し、当該ポリシー及び手順を組織のステークホルダーと共有する。 ・組織のステークホルダーによって合意され、実行される戦略、目的、ポリシー、及び手順に基づき、サイバーセキュリティサプライチェーンリスクマネジメントに関するプログラムのプロセスを策定し、導入する。	O	○ (03.17.01 サプライチェーンのリスクマネジメント計画 a、03.17.02 取得戦略、ツール、方法)	○ (PM-30、SR-02、SR-03)	○ (A.5.19、A.5.21)	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.SC-02	・組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	L1_1_a_ORG L1_1_a_PRO L1_1_b_ORG L1_1_b_PRO L1_1_c_ORG L1_1_c_PRO L1_3_b_ORG L1_3_b_PRO L1_3_c_PRO	<High-Advanced><Advanced>共通 ・組織は、サイバーセキュリティリスクへの責任を関係者と分担するため、有事のみならず平時の対応も含め、サプライヤー、顧客、及び事業パートナーの役割と責任を策定し、これらを組織のポリシー及び該当する第三者との契約に組み込む。 ・組織は、契約において取引先に対応を求める／求められるセキュリティに関する要求事項の実効性を高めるため、要求事項への対応要否や過不足、具体的な対応方法や費用負担、対応できない場合の代替措置について契約時あるいは契約期間の初めに合意することが望ましい。 【参考】特にクラウドサービスプロバイダーと自組織との役割と責任に関して、追加の情報を得るために、総務省「クラウドサービス提供における 情報セキュリティ対策ガイドライン（第3版）」の「Ⅰ. 6. クラウドサービス事業者とクラウドサービス利用者の責任」を参照することが可能である。	O	○ (03.16.03 外部システムサービス b)	○ (SR-02、SR-03、SR-05)	○ (A.5.2)	○ (6.2.3.1)	-
			<Basic> ・組織は、委託先あるいは委託元との契約において、業務においてセキュリティインシデントにより損害が発生した場合の自組織と取引先の責任範囲（免責事項の明記、損害賠償額の契約金額等での上限設定等）を規定する。	O	-		-		-
CPS.GV.SC-03	・組織は、サイバーセキュリティサプライチェーンリスクマネジメントを、サイバーセキュリティ及び事業体のリスクマネジメント、リスクアセスメント、改善プロセスに統合する。	L1_1_a_ORG L1_1_a_PRO L1_1_b_ORG L1_1_b_PRO L1_1_c_ORG L1_1_c_PRO	<High-Advanced><Advanced>共通 ・組織は、サイバーセキュリティリスクマネジメント及び事業体のリスクマネジメントについて、重複している部分及び連携が必要な部分を明確化する。	O	-	○ (下記に加えて、SR-06)	-	-	-
			<Basic> ・組織は、サプライチェーンにおける重大なサイバーセキュリティリスクを経営層にエスカレーションし、事業体全体のリスクとして対応する。	O	○ (03.11.01 リスクアセスメント a、03.17.01 サプライチェーンのリスクマネジメント計画 b)	○ (AC-01、AT-01、AU-01、CA-01、CM-01、CP-01、IA-01、IR-01、MA-01、MP-01、PE-01、PL-01、PM-01、PM-09、PM-18、PM-19、PM-28、PM-30、PM-31、PS-01、PT-01、RA-01、RA-03、RA-07、SA-01、SA-04、SA-09SC-01、SI-01、SR-01、SR-02、SR-03、SR-05)	-	-	-
CPS.GV.SC-04	・組織は、自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをする。	L1_1_a_ORG L1_1_b_ORG L1_1_c_ORG L1_3_b_ORG	<High-Advanced> ・取引先において、事業への悪影響を及ぼすセキュリティインシデントが発生した際の自組織への影響の内容及び、その起こりやすさ、規模を組織は推定する。 ※ 関連する対策要件に、CPS.ID.AM-04、CPS.GV.PO-01等がある。	O	-	○ (下記に加えて、RA-09、SR-06)	-	-	-
			<Advanced> ・組織は、全てのサプライヤーを一覧として管理し、あらかじめ定めた重要度の判定基準に基づいて優先順位を付ける。 ・組織は、重要なサプライヤー、サービス、及び製品について、リスク状況の変化を監視し、変化に応じてサプライヤの重要度を再評価する。 ・組織は、重要度の高いサプライヤー（例：自組織のミッション／業務プロセスに重要な影響を及ぼしうる取引先）が、自組織のセキュリティポリシーに規定されているセキュリティ上の役割と責任を果たせるかどうかを確認する。	O	-		-	-	-
			<Basic> ・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付ける。 ・組織は、サプライヤーが取扱う又は保有するデータの機微性、自組織のシステムへのアクセス権限の度合い、提供される製品又はサービスが自組織のミッションに対して持つ重要性等を考慮要素として、サプライヤの重要度を判定する基準を策定する。 ・組織は、長年に渡ってIoT機器が使用されることが想定される場合、問い合わせ窓口やサポート体制等の適切な管理体制が整備されており、販売後のセキュリティサポート方針を明確にしている等、長期間のサポートが期待できる取引先（IoT機器ベンダ）を選定する。 ・組織は、IoT機器のサポート終了時に機器を入れ替えることの要否についてシステムの導入前に取引先（IoT機器ベンダ）に対して確認する。 ・組織は、下記の観点を確認することにより、ITサービスのマネジメントを効率的、効果的に運営管理するサービスプロバイダーを選定することが望ましい。 - JIS Q 20000 に基づく第三者認証（ITSMS認証）を取得している - 自己適合確認を通じて認証取得相当の対策の実装を確認している	O	-		-	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.SC-05	・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	L1_1_a_ORG L1_1_a_PRO L1_1_b_ORG L1_1_b_PRO L1_1_c_ORG L1_1_c_PRO L1_3_b_ORG L1_1_d_PRO L2_1_a_PRO L2_2_a_ORG L2_3_c_PRO L3_1_b_DAT L3_1_a_PRO L3_1_c_DAT	<High-Advanced> ・組織は、重要な製品について、構成要素の一覧（例：ソフトウェア部品表（SBOM）、ハードウェア部品表（HBOM））を最新の状態で提供し、維持するよう、契約によりサプライヤーに義務付ける。 ・組織は、再委託先以降の事業者へのデータ取扱い業務の委託を、直接の取引先に求める水準のセキュリティ対策が実装されていることが確認される場合に限って、許可する。	0	-	○ (下記に加えて、SR-06)	○ (A.5.20)	○ (6.2.6.1)	-
			<Advanced> ・組織は、サプライチェーンに係るセキュリティ対策基準を参照して、ITT(Invitation To Tender)やRFP(Request For Proposal)などの入札書類を準備し、潜在的な取引先に提供する。特に、入札書類には以下が含まれることが望ましい。 - 調達する製品またはサービスの仕様 - 供給者が製品またはサービスを提供している間に従うセキュリティ要件 - 製品またはサービスの供給中に従うべきサービスレベル及びその指標 - セキュリティ要件に違反した場合に、委託元が課す可能性のある罰則 - 取引先の選定プロセス中に送信されるデータやシステムなどを保護するための秘密保持条項 ・組織は、交換するデータの重要度、想定されるリスクを勘案して、具体的なセキュリティ対策要件を指定し、取引先に対して実装を求める。 ・組織は、第三者が遵守すべき全てのサイバーセキュリティ要件及びサプライチェーン要件、並びにこれらの要件への遵守状況を確認する方法を、契約のひな型に盛り込む。 ・組織は、自組織とサプライヤ及び再委託先となるサプライヤとの間における情報共有のルール及び手順を、契約に明記する。 ・組織は、取引関係のライフサイクルを通じて、サプライヤのセキュリティ実施状況が許容できる水準にあるかを監視するため、セキュリティ要件をサービスレベル合意書（SLA）に明記する。 ・組織は、製品の使用期間又はサービスの提供期間中、製品及びサービスのサイバーセキュリティに関する機能、仕様、及び脆弱性を開示するよう、契約によりサプライヤに義務付ける。 ・従業員を審査し、内部脅威に対する対策を講じるよう、契約によりサプライヤに義務付ける。	0	○ (下記に加えて、03.12.05 情報交換 b)		○ (6.2.2.1、6.2.6.1)	-	
			<Basic> ・組織は、自社の機密情報を共有する子会社又は取引先との間で、業務開始前に機密情報の取扱いについて、以下の事項を取り決める。 - 機密情報の定義 - 機密情報の利用制限、保管方法、複製可否及び第三者への提供可否 - 機密情報の返還又は廃棄 ・組織は、機密情報の取扱いについて、外部情報サービスの提供事業者と合意を取り交わす。 ・組織に代わってシステムを運用するサービス提供者に対する要件の中に、環境上の脅威からの保護及び適切な運用基盤の確保を含める。 ・組織は、直接の取引先に対して、データの管理に関わる業務の再委託を禁止する。	0	○ (03.01.20 外部システムの利用 b.c、03.12.05 情報交換 a、03.16.03 外部システムサービス a)	○ (SA-04、SA-09、SR-03、SR-05、SR-10)	○ (A.5.20、A.5.23)	-	-
CPS.GV.SC-06	・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	L1_1_a_ORG L1_1_b_ORG L1_1_c_ORG L1_1_d_PRO L2_3_c_ORG L2_3_c_PRO L3_3_b_ORG L3_3_c_ORG L3_1_b_ORG L3_1_b_PEO L3_3_d_ORG L3_1_c_ORG L3_1_c_PEO L3_3_a_ORG	<High-Advanced> ・組織は、システム・モノ・サービスのいずれかを提供する取引先との契約において、当該組織に対して、以下の実施を要求する。 - 契約にて指定されたセキュリティ対策を実施したエビデンスの作成、セキュリティテスト／評価結果の提示 - セキュリティテスト／評価時に特定された欠陥の修正計画の策定 - 欠陥の修正計画及び、その実施状況の提示 ・組織は、直接の委託先に対して要求しているセキュリティ対策に関する要求事項及びそれに付随する要求事項の内で必要な事項を、サプライチェーンに由来するリスクの大きさ等を勘案しつつ、再委託先以降の組織に対して（場合によっては再委託先以降の全サプライヤーに対して）も適用することが望ましい。 [参考] 委託契約に含め、実施を確認することが望ましい項目に関する追加の情報の取得のためには、「ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」（IPA, 2018年）の「3.2. IT サプライチェーン リスクマネジメント の全体像」等を参照することが可能である。	0	-	○ (下記に加えて、RA-09、SR-06)	○ (6.2.6.1)	○ (6.2.6.1)	-
			<Advanced> ・組織は、第三者の評判、及び提供される製品又はサービスの重要度に応じて、アセスメントの形式及び頻度を調整する。 ・組織は、事業要件及び該当するサイバーセキュリティ要件に基づき、サプライヤーのリスクアセスメントを実施する。 [参考] サプライヤーに課すサイバーセキュリティ要件として、例えば、サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）の要求事項・評価基準を活用すること等が考えられる。 ・組織は、契約候補のサプライヤーの技術対応力、サイバーセキュリティ対応力、及びリスクマネジメントの実施状況が、自社の要件に適合しているかを評価する。 ・組織は、法規制等を参照してセキュリティ要件を決定し、取引先へ遵守を要求する際、下記を事前に考慮することが望ましい。 - 自組織と取引先との法令の相違（例：業法の違い、国・地域の違い）により生じるコンプライアンス上のリスクの特定 - 取引先に適用される法律及び規制上の義務によるセキュリティの観点からの契約への悪影響 ・組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施し、委託内容の特性等により必要と認められる場合、調達契約において、追加で対策を導入することを要求する。 ・組織のミッション／業務ニーズに応じて、システム、モノ、またはサービスの調達契約に以下の要求事項、記述及び基準を記載する。 - セキュリティ対策に関する要求事項 - セキュリティ関連のドキュメントに関する要求事項 - セキュリティ関連のドキュメントの保護に関する要求事項 - 秘密保持に関する条項 - インシデントが発生した際の報告先、報告内容、初動、調査、復旧等の各対応の実施主体、実施方法 - 自組織または認可された第三者によって監査され、定義されたセキュリティ要件への遵守を確認することを許可する条件 - 契約終了後の情報資産の扱い	0	-				-
			<Basic> ・組織は、委託先の選定、評価のプロセスにおいて、取引先がセキュリティアクションを宣言していることを確認する。 ・組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施することを要求する。	0	-	○ (SA-04、SA-09、SR-03、SR-05)	-	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.SC-07	・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	L1_1_d_ORG L1_1_d_COM L1_1_d_PRO L2_1_a_COM L2_1_a_PRO L2_2_a_ORG L2_3_a_ORG L2_3_c_ORG L2_3_c_PRO L2_3_d_ORG L3_3_b_ORG L3_3_c_ORG L3_1_b_ORG L3_3_d_ORG L3_1_c_ORG L3_3_a_ORG	<High-Advanced> ・調達する機器に対して、契約におけるセキュリティ要求事項が満たされているかを、第三者がテストする。 ・組織は、自組織のオペレーションにとって特に重要な機器について、再委託先以降の組織を含む関係するサプライチェーン全体に渡り、一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロセスで製造されたものかを確認する。	O	-	○ (下記に加えて、RA-09、SR-06)	-	-	-
			<Advanced> ・組織は、調達計画時に、製品またはサービス自体、あるいは当該製品・サービスの調達・供給に使用される資産の保護に係るセキュリティ要件の費用を確保しておくことが望ましい。 ・組織は、第三者の評判、及び提供される製品又はサービスの重要度に応じて、アセスメントの形式及び頻度を調整する。 ・組織は、契約において、例えば下記のように、取引先から調達する製品・サービスが具備すべきセキュリティ要求事項を明確化する。 - セキュリティに関わる特定の認証（例：ISMS認証、ISASecure CSA認証、ITセキュリティ評価及び認証制度(IISEC)）を有していること - ベンダー自身により、セキュリティに関わる特定の認証の基準に適合する対策を実施していることが確認されていること - リスク分析の結果等から導かれた必要なセキュリティ要件を設計時からの実装（セキュリティ・バイ・デザイン）し、検査していること - 下記を含む製品またはサービスの調達または供給を評価するためのセキュリティ測定ルールを策定し、運用及び改善する。 - 測定対象の内容 - 措置の報告方法、報告の頻度 - 措置が実施されない場合に遂行される措置 ・組織は、搬送中の改ざん・漏えいを検知(又は抑止)する手段とともに納品されるIoT機器やソフトウェアが、不正操作されていないかを確認する。 - 物品：セキュリティ便、プロテクトシール等 - 電送：暗号化、電送データ全体のハッシュ値等 [参考] システム及びモノにおけるセキュリティの要求仕様を検討するにあたり、「IT 製品の調達におけるセキュリティ要件リスト 活用ガイドブック 第2.1版」(IPA, 2026年)、「セキュリティ要件適合評価及びラベリング制度 (JC-STAR) 」、「非機能要求グレード」(IPA, 2018年)等を参考にすることが可能である。	O	-		-	○ (6.2.6.1)	-
			<Basic> ・組織は、製品・サービスの提供について外部の関係者を選定する際、下記を確認する。 - セキュリティパッチの配布を含めた、製品・サービスのサポート期間が十分設けられていること - サポート期間終了後の対応が明確化されていること ・組織は、調達時に、自組織が所有するIoT機器が正規品であるかをラベルを確認する等して確かめる。 ・組織は、IoT機器やソフトウェアに含まれるIDや秘密鍵、電子証明書等を用いて調達した機器が正規品であることを確認する。	O	○ (03.17.03 サプライチェーンの要件およびプロセス b)	○ (SA-04、SA-09、SR-03)	-	-	-
CPS.GV.SC-08	・組織は、取引先等の関係する他組織が契約上の義務を果たしていることを確認するために、監査、テスト結果、又は他の形式の評価を使用して定期的に評価する。	L1_1_d_ORG L3_3_b_ORG L3_3_c_ORG L3_1_b_ORG L3_3_d_ORG L3_1_c_ORG L3_3_a_ORG	<High-Advanced> ・組織は、委託先の要員により委託先が要求するセキュリティ要求事項が遵守されているかどうかを継続的にモニタリングし、通常とは異なる行動があった場合、自組織の担当者に通知できるようにプロセスを整備する。 ・組織は、契約事項からの逸脱及び、その兆候に対する調査・対応のためのプロセスをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先及びその再委託先以降の組織に対して、契約にて規定した組織のセキュリティマネジメント、納入する製品・サービスに実装されるセキュリティ機能等に関する義務事項が履行されているかどうかを一覧化して確認できるメカニズムを利用する。 ・委託元による実地調査、外部監査等の手法により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。 ・重要な取引先及びその再委託先以降の組織は、関係する攻撃の予兆、情報流出の事実がないかを調査し、組織に対して結果を定期的に報告する。 ・組織は、自組織が取引先との契約において要求事項として規定した内容に関連して、システム上での監査が可能かどうか、確認する。 ・情報システムは、上記で定義されているシステム上で監査可能なイベントのために、監査記録を生成する機能を提供する。 ・組織は、手作業ないしは情報システムにより自動で生成された監査記録を定期的にレビュー・分析して、契約事項からの逸脱及び、その兆候の有無を確認する。	O/S	○ (下記に加えて、03.16.03 外部システムサービス c)	○ (下記に加えて、RA-09、SR-06)	○ (A.5.22)	-	-
			<Advanced> ・組織は、第三者の評判、及び提供される製品又はサービスの重要度に応じて、アセスメントの形式及び頻度を調整する。 ・組織は、以下に示す条件のいずれか若しくは複数に該当する子会社又は取引先を対象に、年1回以上の頻度で、以下の例を参考にセキュリティ対策状況を把握する。 [対策状況把握の対象とする子会社又は取引先の条件] - 自社の重要な機密情報を提供・共有する - 自社の事業継続にとって重要な位置づけを持つ - 当該取引先の環境から発注者の内部システムへのアクセスが可能 [対策状況の把握方法(例)] - 取引先に訪問し点検を実施する - セキュリティ対策チェックシートを作成して回答を受領する ・組織は、契約上のサイバーセキュリティ要件への遵守状況に関する第三者からの証跡（例：自己宣言書、保証書、認証書、その他成果物）を評価する。 ・組織は、重要なサプライヤーが取引関係のライフサイクルを通じてセキュリティ上の義務を果たしていることを確認するため、立入検査、監査、テスト、その他の評価手段等、多様な手法を用いて当該サプライヤーを監視する。 ・組織は、監査に関連する情報が必要な他の組織との間で、セキュリティ監査の整合性を保つことができるようにする。	O	○ (03.17.03 サプライチェーンの要件およびプロセス a)			-	-
			<Basic> ・各種認証・制度（ISMS認証、CSMS認証、Pマーク、SCS評価制度等）の取得証明書を確保することで、必要なセキュリティ対策が実施されていることの確認に代える。	O	-	○ (PM-31、RA-03、RA-05、RA-07、SA-04、SA-09、SR-02、SR-03、SR-05)		-	-

・第Ⅲ部にて記載した対策要件を実施する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実施する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.SC-09	・組織は、取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロセスを策定し、運用する。	L1_1_a_PRO L1_1_b_PRO L1_1_c_PRO	<High-Advanced> ・組織は、取引先の監査あるいはテストの不適合が発見された場合、下記を実施するプロセスを策定し、運用する。 1) 不適合から生じるセキュリティの影響を特定し評価する 2) 契約で定義されているセキュリティに関わる規定を再検討すべきかどうかを判断する 3) 調達された製品またはサービスの範囲内で許容可能なセキュリティレベルを取得するために、実施すべき是正措置を決定する。 4) 上記を取引先と同意する	0	-	○ (下記に加えて、RA-09、SR-06)	○ (A.5.22)	-	-
			<Advanced> ・組織は、取引先の監査あるいはテストの不適合が発見された場合、取引先に対して改善計画の策定を求め、計画の実施状況について必要に応じて確認するプロセスを策定し、運用する。	0	○ (03.17.03 サプライチェーンの要件およびプロセス a)			-	-
			<Basic> ・組織は、取引先の監査あるいは製品・サービスに対するテストで不適合が発見された場合、発生した不具合による自組織へのリスクを把握する。	0	-	○ (PM-31、RA-03、RA-05、RA-07、SA-04、SA-09、SR-02、SR-03、SR-05)		-	-
CPS.GV.SC-10	・組織は、技術製品及びサービスのライフサイクル全体を通じて、サプライチェーンに係るセキュリティ対策の実施状況を監視する。	L1_1_a_ORG L1_1_b_ORG L1_1_c_ORG	<High-Advanced><Advanced><Basic>共通 ・組織は、調達する技術製品及びサービスの重要度を踏まえて対象を定め、供給元及び合理的に把握可能な範囲において流通経路の記録を取得することを、ポリシー及び手順で定める。	0	○ (03.16.03 外部システムサービス c)	○ (PM-09、PM-19、PM-28、PM-30、PM-31、RA-03、RA-05、RA-07、SA-04、SA-06、SA-09、SR-02、SR-03、SR-05)	-	-	-
CPS.GV.SC-11	・組織は、取引先等との契約終了時に実施すべきプロセスを策定し、運用する。	L1_1_a_PRO L1_1_b_PRO L1_1_c_PRO	<High-Advanced><Advanced>共通 ・組織は、製品またはサービスの供給が取り消されるか、または自組織または他の取引先に返還されるかどうかを現在の取引先と決定する。 ・組織は、製品またはサービスの供給によって影響を受けるヒトに、その終了に関する情報を提供するためのコミュニケーションを行う。 ・組織は、終了計画に従い、製品またはサービス供給の終了を実行する。 ・組織は、サプライヤーとの取引終了に伴うデータ漏洩リスクを管理する。 ・組織は、サプライヤーによる自組織のリソースへのアクセス権限が不要になった時点で、その権限が速やかに無効化されていることを確認する。 ・組織は、自組織のデータが含まれる資産が、適切なタイミングかつ管理された安全な方法に則って返却又は廃棄されていることを確認する。 ・組織は、提供された製品またはサービスの終了の達成について、取引先と同意する。	0	-	○ (下記に加えて、SR-06)	○ (A.5.11)	-	-
			<Basic> ・組織は、サプライチェーンのセキュリティリスク及びレジリエンシーを考慮した、サプライヤーとの取引関係の解消又は移行に関する計画を策定し、実行する。 ・組織は、取引先等の関係する他組織との契約が終了する時期を常に把握する。	0	-	○ (PM-31、RA-03、RA-05、RA-07、SA-04、SA-09、SR-02、SR-03、SR-05)	-	-	-
CPS.GV.SC-12	・組織は、自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	-	<High-Advanced> ・組織は、取引先、第三者的な監査機関等の関係する他組織からのリアルタイムでのニーズに柔軟に応じるため、下記の特徴を有した証跡保管システムを利用する。 - 対象となる監査証跡の契約事項に対する適格性を高速で検証することができる - 取引先や委託を受けた監査機関等の許可を受けたエンティティのみがアクセスできる - 保管されているデータが、タイムスタンプや電子署名により証跡としての信頼性を有している	0	-	-	-	-	○ (SR 6.1)
			<Advanced> ・組織は、システムによって生成された監査記録のうち長期にわたって取得する監査記録を確実に取得できるよう、対策を実施する。 ・システムは、監査記録を次の脅威から保護するため、粒度の高いアクセス制御等を監査記録を保存するモノ、システムに適用することが望ましい。 - 記録されたメッセージ形式の変更 - ログファイルの変更又は削除 - ログファイル媒体の記録容量超過	O/S	-	-	-	-	
			<Basic> ・組織は、法規制等により要求される事項を満たす事ができるよう、適切な期間の監査記録を保持する。	0	-	-	-	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみ適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.AM-01	・組織は、システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	L1_1_a_COM L1_1_b_COM L1_1_c_COM L2_1_a_ORG L2_1_c_ORG	<High-Advanced> ・組織は、自組織の情報システム及び産業用制御システムを構成する資産（IoT機器等を含むハードウェア、ソフトウェア、情報）を一意に特定し、各々の資産に管理責任者を割り当てた上で、資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、定期的又はオペレータ等の求めに応じて、リアルタイムで状況を把握しながら目録を維持・管理する。 ・IoT機器には既存の資産管理システムと必ずしも接続できないものも存在することが想定されるため、組織が管理できる範囲で複数の資産管理システムを運用することも視野に入れて資産管理・構成管理を実施する。 ・情報システム及び産業用制御システムは、許可されていない資産を自動的に検出し、管理情報から外す・システムから切り離す等を実行するメカニズムを導入、運用している。	O/S	-	○ (AC-20、CM-08、PM-05、SA-05、SA-09)	○ (A.5.9)	○ (6.3.2.1、7.2.1.1)	○ (SR 7.8)
			<Advanced> ・組織は、スマートデバイスの製造元、OS及び台数を含む一覧を作成し、最新に維持する。 ・組織は、IoT機器及び産業用制御システムを構成する機器の製造元、OS及び台数を含む一覧を作成し、最新に維持する。 ・組織は、市販のパッケージソフト、オープンソースソフトウェア、独自開発アプリケーション、APIサービス、及びクラウドベースのアプリケーション・サービスを含む、全ての種類のソフトウェア及びサービスの一覧を作成し、最新に維持する。 ・組織は、会社支給のパソコンを対象に、社内で利用を許可するソフトウェアの一覧を作成し、最新に維持する。 ・組織は、年1回以上の頻度で、資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、作成した資産一覧を定期的にレビュー、更新することで維持・管理する。	O	○ (下記に加えて、03.04.10 システムコンポーネントのインベントリ b)			○ (7.2.1.1)	
			<Basic> ・組織は、自組織の情報システムや産業用制御システムを構成する資産（ハードウェア、ソフトウェア、情報）を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・資産は保有するものすべてを一覧化することが望ましいが、対象が膨大な場合、分析対象の統合（グループ化）と分析対象からの除外を通じて、対象とする資産を絞り込むことを検討する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づける。 ・組織は、情報システム及び産業用制御システムのネットワーク構成、資産、機器の設定情報、構成情報等のベースラインとなる情報を文書化し、内容が適切かどうかを定期的に確認する。 ・使用するUSBメモリ等の周辺機器は、管理台帳を作成し、保管場所を施錠して管理する。	O	○ (03.04.10 システムコンポーネントのインベントリ a)			○ (7.2.1.1、7.2.2.1、7.2.3.1)	
CPS.ID.AM-02	・組織は、組織内の通信ネットワーク構成図及びデータフロー図を作成し、適切に管理する。	L1_1_a_COM L1_1_b_COM L1_1_c_COM L1_3_b_ORG L1_3_c_ORG	<High-Advanced> ・組織は、情報システム及び産業用制御システムのシステム構成、通信ネットワーク構成及びデータフローをリアルタイムでモニタリングし、管理するための自動化されたメカニズムを導入・管理している。	O/S	-	○ (下記に加えて、AC-04、PL-08)	-	○ (下記に加えて、8.2.2.1、8.3.1.1)	○ (SR 7.6)
			<Advanced> ・組織は、自組織の有線及び無線ネットワーク内における通信及びデータフローのベースラインを整備し、最新に維持する。 ・組織は、自組織と第三者との間における通信及びデータフローのベースラインを整備し、最新に維持する。 ・組織は、自組織が利用するIaaS（Infrastructure as a Service）における通信及びデータフローのベースラインを整備し、最新に維持する。 ・組織は、認可されたシステム間で日常的に使用されるネットワークポート、プロトコル、及びサービスの一覧を整備し、最新に維持する。 ・組織は、関連する文書内の図に、ネットワーク接続におけるインターフェース特性、セキュリティ要求事項、伝達されるデータの性質を記載する。 【参考】システム構成、ネットワーク構成、データフローの文書化を行う際の手順については、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA、2026年）の3.2、3.3を参照することが可能である。	O/S	-				-
			<Basic> ・組織は、自組織のネットワークの所在地及び用途等を把握するための、仕組みを整備する。 ・組織は、自組織のネットワーク機器の製造元、モデル及び保守事業者等を把握するための、仕組みを整備する。	O	-			○ (7.2.1.1、7.2.2.1)	-
CPS.ID.AM-03	・組織は、自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	L1_1_a_COM L1_1_b_COM L1_1_c_COM L1_3_b_ORG L1_3_c_ORG	<High-Advanced> ・情報システムは、リアルタイムかつ自動的に自組織が利用している外部情報システムサービスを一元化し、利用しているサービスとともに利用者・機器等を管理する。 ・情報システムは、利用を許可していない外部情報システムサービスを検知した場合、システム管理者へ通知するメカニズムを利用する。	S	-	○ (AC-20、SA-09、SR-02)	-	-	-
			<Advanced> ・組織は、外部の情報システムを所有、運用する他の組織に対して、下記を許可するうえでの条件を設定する。 a. 外部の情報システムから自組織の情報システムにアクセスすること b. 外部の情報システムを使用して自組織の管理下にある情報を処理または保存もしくは伝送すること ・情報システムは、外部システム上に設置された自組織所有のストレージについて、許可された個人のみが使用できるよう制限する。 ・組織は、自組織が利用する外部サービスの一覧について年1回以上の頻度で点検し、必要に応じて一覧を更新するとともに、新しい外部サービスを利用する際にも更新を行う。	O/S	-			-	-
			<Basic> ・組織は、自組織が利用する全ての外部サービス（顧客・子会社・関係会社・取引先が管理・提供するシステム、及び第三者が提供するIaaS、PaaS、SaaS、API、その他外部ホスティングのアプリケーションサービスを含む）の一覧を作成し、各サービスにおけるユーザーとしての役割と責任を定義する。	O	-			-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.AM-04	・組織は、リソース（例：モノ、データ、システム）を機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	L3_4_a_ORG L3_4_a_DAT L3_4_b_DAT L3_1_b_DAT L3_1_a_ORG L3_1_c_DAT	<High-Advanced><Advanced>共通 ・組織は、情報システムや産業用制御システムにおけるリソース（データ及びデータを処理するモノ、システム等）を分類する際には、データを共有又は制限する業務上の要求及び法的要求事項を考慮する。 ・組織は、リソースの分類体系に、分類の規則と定期的に分類を見直すための基準を含める。 ・組織は、資産の優先順位を把握し、定期的又は組織に重大な変化が発生した際に更新する。	0	-	○ (下記に加えて、RA-09)	○ (A.5.12)	○ (10.2.1.1)	-
			<Basic> ・組織は、すべてのサーバ及びネットワーク機器について、システム管理者及び責任者を定める。 ・組織は、関係する法規制等により自組織のリソース（例：システム、データ）について特定の分類に従うことが要求されている場合、該当する分類を資産に適用する。 ・組織は、洗い出した情報システムや産業用制御システムにおける資産を、自組織にとっての重要度に応じて優先順位づけする。 ・組織は、特に産業用制御システムにおけるモノ、システム等の分類、優先付けに当たっては、自組織の事業活動の適切でない運用によりHSE(Health, Safety and Environment)への悪影響が発生するかを考慮して実施する。 [参考] 資産の重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第4.0版」（IPA, 2026年）の P44.45に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA, 2026年）の P91 に記載された事業被害の大きさにおける評価を用いる方法等がある。また、特に産業用制御システムにおける資産の重要度の判断基準については、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA, 2026年）4.2.2及び4.2.3を参照することができる。	0	-	○ (RA-02、RA-03)		-	-
CPS.ID.AM-05	・組織は、保有するデータ及びメタデータの一覧を作成し、適切に管理する。	L3_4_a_DAT L3_4_b_DAT L3_1_b_DAT L3_1_c_DAT	<High-Advanced><Advanced>共通 ・組織は、組織内に散在する整理されていないデータを継続的に探索・分析し、保護対象の種類のデータが新たに含まれていないかを把握する。 ・組織は、保護対象の種類のデータ一件ごとに、その取得元、データ管理責任者、及び保管場所を継続的に把握する。 ・組織は、年1回以上の頻度で、重要な機密情報並びに当該情報ごとの管理者名、部署名、保管場所、保管期限、開示先及び管理者の連絡先の内容について点検を行う。	0	○ (03.04.11 情報の位置 a)	○ (下記に加えて、CM-12)	○ (A.5.9)	○ (10.2.1.1)	-
			<Basic> ・組織は、組織として保護すべき特定の種類のデータ（例：個人情報、医療情報、金融口座番号、組織の知的財産、産業用制御システムに関するデータ）の一覧を作成し、最新に維持する。	0	-	○ (SI-12)		-	-
CPS.ID.AM-06	・組織は、システム、ハードウェア、ソフトウェア、サービス及びデータを、取得から廃棄に至るライフサイクル全体を通じて管理する。	L1_1_a_COM L1_1_b_COM L1_1_c_COM	<High-Advanced><Advanced><Basic>共通 ・組織は、システム、ハードウェア、ソフトウェア、サービス、及び製品のライフサイクル全体を通じて、サイバーセキュリティの観点を組み込む。 ・組織は、情報機器、OS及びソフトウェアについて、導入、設置、ネットワーク接続及びセキュリティパッチ適用のルールを含む管理ルールを定める。 ・組織は、年1回以上の頻度で、情報機器、OS及びSWの導入、設置、ネットワーク接続及びセキュリティパッチ適用のルールを含む管理ルールの遵守状況について点検する。	0	○ (03.04.08 認可されたソフトウェア 例外による許可 a、03.04.10 システムコンポーネントのインベントリ c、03.08.07 媒体の使用 a、03.16.02 サポートされていないシステムコンポーネント a)	○ (CM-09、MA-02、MA-06、PL-02、PM-22、PM-23、SA-03、SA-04、SA-08、SA-22、SI-12、SR-05、SR-12)	○ (A.7.10)	-	-
CPS.ID.AM-07	・組織は、自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。	L1_3_a_COM L1_3_b_COM	<High-Advanced> ・組織は、トレーサビリティが要求事項となっている場合には、組織はアウトプット（製品）について一意の識別を管理し、トレーサビリティを可能とするために必要な文書化した情報を保持する。 ・組織は、モノを一意に識別できるような方法を検討する際、異業種間でも適用するよう業種横断的な共通ナンバリングルール等に基づいていることが望ましい。 [参考] ISO9001:2015 - 8.5.2 識別及びトレーサビリティ	0	-	-	-	-	-
			<Advanced><Basic>共通 ・組織は、下記を例とする観点から、自組織が提供するモノを複数段階に優先順位付けする。 - モノの品質等に何かしらの問題が発見された際のサプライチェーンにおける影響範囲の広さ - モノの品質等に何かしらの問題が発見された際の自組織の事業に対する影響の大きさ ・組織は、自組織が生産したモノのサプライチェーン上の重要性に応じて、組織は、ナンバーを付与する等アウトプットを識別するために適切な特定方法（例：シリアルナンバーの付与）を定める。 ・組織は、製造及びサービスを提供する際の、組織が定める過程（例：製品の顧客納入時まで）において、当該製品・サービスにおいて法令、契約等で遵守が要求されている事項に関連して、アウトプットである製品・サービスの状態を識別する。	0	-	-	-	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみ適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.AM-08	・組織は、重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。	L1_3_a_COM L1_3_b_COM	<High-Advanced> ・組織は、生産活動に関する内部規則を整備するとともに、生産したモノの記録については、その重要性に応じて、後日監査を受ける可能性があることを踏まえ、取引先との間であらかじめ重要性について認識を共有し、適切な記録管理レベルを確保する。 ・作成され、管理される生産活動の記録は、生産日時やモノの分類（例：製品名）等で素早く検索できるよう構成されていることが望ましい。	0	-	-	-	-	-
			<Advanced><Basic>共通 ・組織は、生産したモノのサプライチェーン上の重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するための生産活動に内部規則を整備し、運用する。 ・組織は、上記の記録を作成、あるいは更新する際、以下の事項を考慮する。 - 適切な識別及び記述（例：タイトル、日付、作成者、参照番号）とすること - 適切な形式（例：言語、ソフトウェアの版、図表）及び媒体（例：紙、電子媒体）とすること - 適切性及び妥当性に関する、適切なレビュー及び承認を得ること	0	-	-	-	-	-
CPS.ID.RA-01	・組織は、自組織の資産の脆弱性を特定し、対応する資産と紐づけて管理する。	L1_1_a_SYS L1_1_b_SYS L1_1_c_SYS L2_1_a_ORG L2_1_c_ORG L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> ・組織は、自組織が管理する産業用制御システムの構成要素（IoT機器を含む）に対して、システムの運用に悪影響を及ぼさないよう、計画停止時等の予定されたタイミングに脆弱性診断を実施し、自組織の所有するシステムに存在する脆弱性を認識し、一覧化する。 ・組織は、ツールを用いて脆弱性診断を行う場合、診断すべきシステムに対する脆弱性データベースを更新できる脆弱性診断ツールを使用することが望ましい。 ・組織は、より徹底した脆弱性の洗い出しを行うために、脆弱性診断の実施者に自組織の管理するシステムにおける特権アクセスの権利を一時的に許可するメカニズムを整備する。 ・組織は、自組織の管理するシステムにおける最新の脆弱性を認識するため、定期的にペネトレーションテストを実施することが望ましい。	0	-	○ （下記に加えて、CA-08）	○ （A.8.8）	○ （6.3.2.1、12.2.9.1）	-
			<Advanced> ・組織は、自組織が管理する重要度の高い情報システムの構成要素（例えば、インターネットに公開されている機器を含む）に対して、脆弱性診断を実施し、自組織の所有するシステムに存在する脆弱性を認識し、一覧化する。 ・組織は、脆弱性管理ツールを用いて、パッチが適用されていないソフトウェア及び設定不備のあるソフトウェアを把握する。 ・組織は、ネットワーク及びシステムのアーキテクチャを評価し、サイバーセキュリティに影響を与える設計上及び実装上の弱点を特定する。 ・組織は、重要な機器が設置されている施設を評価し、物理的な脆弱性及びレジリエンス上の課題を明確化する。 ・組織は、自組織の所有する情報システムの運用段階において、各種資産から収集した脆弱性の内、自組織の事業運営等に関連することが想定されるものに対して、脆弱性検査ツール等を用いて、定期的に自組織のシステムにおける脆弱性を特定し、当該脆弱性の影響度とともに一覧に追加する。 【参考】脆弱性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の影響の大きさを評価する指標として、CVSS(IPAによる解説： https://www.ipa.go.jp/security/vuln/scap/cvssv3.html)を参考とすることが可能である。	0	-	○ （下記に加えて、SA-11、SA-15）		○ （8.2.2.1）	-
			<Basic> ・組織は、IPAやJPCERT-CCが公表する「重要なセキュリティ情報」等を活用して、自組織の情報システムにおける管理策上の脆弱性を把握する。	0	○ （03.14.01 欠陥の修正 a）	○ （CA-02、CA-07、RA-03、RA-05、SI-04、SI-05）		-	-
CPS.ID.RA-02	・組織は、組織内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	L1_1_a_SYS L2_1_a_ORG L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> ・組織は、セキュリティに関わる研究会や会議等に出席したり、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ことにより、情報システム、産業用制御システムの双方におけるセキュリティに関わる知識を最新のものとする。 ・組織は、セキュリティに関わる研究会や会議等に出席したり、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ことにより、セキュリティ脅威に関わる知識を最新のものとする。 ・組織は、信頼できる第三者や、サイバー脅威インテリジェンスの情報源から、自組織を狙う可能性のある攻撃者の種類及び彼らが使用する可能性の高い戦術・技術・手順（TTPs）を継続的に把握する。 ・組織は、先端技術がもたらす特有の脆弱性に関する情報を、サイバー脅威インテリジェンスの情報源から継続的に収集する。 ・検知又は対応の機能を持つサイバーセキュリティツールが、サイバー脅威インテリジェンスを自動的かつ安全に受け取れるよう設定する。 ・主に自社が提供している製品・サービスにおいて、新たな脆弱性が含まれていないかを分析し、発見した場合、IPAに関連情報を届け出る。	0	-	○ （下記に加えて、A.5.6）	○ （A.5.7）	○ （12.2.9.1）	-
			<Advanced> ・組織は、脆弱性情報/脅威情報を収集する情報源、ツール及び頻度を定める。 ・組織は、収集した脆弱性情報/脅威情報の対応要否の判断基準・対応手順を定める。 ・組織は、製品及びサービスにおける新たな脆弱性に関する情報を、サイバー脅威インテリジェンスの情報源から継続的に収集する。 ・組織は、契約で定められたルール及び手順に従って、自組織とサプライヤーの間で脆弱性情報を共有する。 【参考】セキュリティ対応組織の構想、構築、運用に当たっては、外部事業者からのサービスを利用するほかに、JPCERT/CCから公開されている「CSIRTマテリアル」、日本セキュリティオペレーション事業者協議会から公開されている「セキュリティ対応組織（SOC/CSIRT）の教科書 ～X.1060フレームワークの活用～」等の文書を利用することが可能である。	0	○ （下記に加えて、03.11.02 脆弱性の監視およびスキャン c）	○ （PM-15、PM-16、RA-05、SI-05）			-
			<Basic> ・組織は、IPAやJPCERT-CCが公表する「重要なセキュリティ情報」等に加え、利用中の機器ベンダーやソフトウェアベンダーが提供するセキュリティに関わる注意喚起情報を確認し、自組織内の関係者に伝達する。	0	○ （03.14.03 セキュリティアラート、勧告、および指令 a）				-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.RA-03	・組織は、自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	L1_1_a-SYS L1_1_b-SYS L1_1_c-SYS L2_1_a-COM L2_2_a-SYS	<High-Advanced> ・組織内に潜む攻撃者の痕跡を能動的に探すため、脅威ハンティングを実施する。 ・組織は、必要に応じて、専門家が提供するサービス等を活用し、一部の専門家しか知りえない情報を入力しそれをもとに、脅威を特定する。 ・組織は、産業用制御システムのようにモノの制御等を伴うような、フィジカル空間に影響を及ぼす可能性のある新たな機器やシステムを開発する場合には、従来の製品や他の事故事例を収集・分析し、セキュリティの観点も含めてセーフティに関わるハザードを特定する。 ・組織は、主に産業用制御システムにおいて、ハザードによって危害に至る状況を分析し、発生しやすさや被害の深刻度を明らかにすることで、生じるリスクを見積もる。その際、セキュリティの問題に起因するハザードの有無を確認することが望ましい。	0	-	○ (PM-12、PM-16、RA-03、SI-05)	-	○ (6.3.1.1、8.2.6.1)	-
			<Advanced> ・組織は、公開された新たな攻撃動向、マルウェア挙動情報や悪性IP アドレス/ドメイン情報などの情報（外部インテリジェンス）を収集する。 ・組織は、得られた脅威情報の信頼度、自組織に与える影響などを評価し、対応すべき脆弱性を取捨選択し、対応する脅威について文書化する。 ・組織は、新たにIoT機器を利用したシステムを企画・設計する場合、既存の資産や新たに導入するシステムにおける守るべき資産を特定し、システムの利用用途や構成に応じて、セキュリティ対策をまとめる。特に、ライフサイクルの長いモノ、システムや、高い可用性を求められるモノ、システムを扱う場合は、設計以前の段階におけるセキュリティ対策の考慮が特に重要である。	0	-		-	○ (6.3.1.1、8.2.6.1、12.2.9.1)	-
			<Basic> ・組織は、「中小企業の情報セキュリティ対策ガイドライン 第4.0版」(IPA, 2026年) 第2部4(1)「資産ベースのリスク分析」及び付録6「資産管理台帳」等の、セキュリティ脅威の洗い出しのベースラインとなる文書を活用して、自組織に関わるセキュリティ脅威及びその発生しやすさを把握する。	0	○ (03.11.01 リスクアセスメント a)		-	○ (6.3.1.1、8.2.6.1)	-
CPS.ID.RA-04	・組織は、構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施することにより、脆弱性を悪用する脅威の潜在的な影響と起こりやすさを識別する。	L1_1_a-SYS L1_1_b-SYS L1_1_c-SYS L2_1_a-ORG	<High-Advanced> ・組織は、新たな脅威や脆弱性に関する情報を入力した際のリスクアセスメント（例：影響範囲の評価）に自動化されたメカニズムを利用する。 ・組織は、産業用制御システム、またはそれが稼働する環境に大きな変化があった場合、もしくは産業用制御システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。	0	-	○ (下記に加えて、RA-09)	-	○ (6.3.1.1、8.2.6.1、12.2.9.1)	-
			<Advanced> ・組織は、情報システム、産業用制御システム、または当該システムが稼働する環境に大きな変化があった場合（新たな脅威や脆弱性の特定を含む）、もしくは当該システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。その際、重要度の高い情報システムを優先的に対応する。 ・組織は、複数のシステムが相互に連携する構造において、連鎖的な障害が発生した場合の潜在的な影響を明らかにする。	0	-		-		-
			<Basic> ・組織は、情報システム及び産業用制御システムに対するセキュリティリスクアセスメントのプロセスを定め、定期的（例えば、重要度の高い情報システムは年に1回）に適用する。 - セキュリティのリスク基準を確立し、維持する。 - 以下の方法によりセキュリティリスクを特定する。 1) 分析対象を明確化する 2) インシデント(周辺状況の変化を含む)並びにこれらの原因を特定する - 以下の方法により、セキュリティリスクを分析する。 1) 上記で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について評価する 2) 上記で特定されたリスクの現実的な起こりやすさについて評価する - リスク基準を参照し、リスクのレベルを決定し、優先順位付けする ・組織は、セキュリティリスクアセスメントのプロセスを文書化し、保管する。 ・組織は、システムにセキュリティインシデントが発生した際に想定される被害の大きさやセキュリティインシデントが発生する蓋然性（例：インターネットにつながっているか）、リスクアセスメント実施に係る工数等の観点を考慮し、システムを優先順位化してリスクアセスメントの頻度等を設定する。 ・組織は、データに対するリスクの理解を深め、適切なリスク対応を行えるよう、脅威モデルを作成する。	0	○ (03.11.01 リスクアセスメント a,b、03.12.01 セキュリティアセスメント)	○ (PM-09、PM-11、PM-16、RA-02、RA-03、RA-07)	-		-
CPS.ID.RA-05	・組織は、保護技術の有効性について、適切なパートナーとの間で情報を共有する。	L2_1_a-ORG	<High-Advanced> ・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、自動化されたメカニズムを通じて適切なパートナーと適時双方向で共有をすることができる環境を整備する。	0	-	-	○ (A.5.6)	-	-
			<Advanced> ・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、パートナーに適時共有することができる環境を整備する。	0	-	-		-	-
			<Basic> ・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、適切なパートナーから入手できる環境を整備する。 [参考] 適切なパートナーを選定するに当たり、「情報セキュリティサービス基準適合サービスリスト」に記載された事業者のサービスを利用することが考えられる。また、パートナーには、情報処理安全確保支援士やCISSP等のセキュリティに係る資格を有している要員を含めることが望ましい。	0	-	-		-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.RA-06	・組織は、リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化するとともに、その実施状況を把握し、関係者に共有する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	L1_1_a-SYS L1_1_b-SYS L1_1_c-SYS L2_1_a-ORG L2_1_a-COM L2_1_c-ORG L2_2_a-SYS	<High-Advanced> ・組織は、CPS.ID.RA-03で実施したハザード分析の結果に基づき、主に産業用制御システムに対して、必要な場合、重要なハザードにつながるセキュリティに係るリスク源に対して適切に対応する。 [参考] 特に安全制御系におけるセキュリティ面の統合については、IEC TS 63074:2023, IEC TR 63069:2019等を参照することが可能である。	0	-		-		-
			<Advanced> ・組織は、リスクアセスメントの結果に応じて対応策を選定する際、実施する対応策及び当該対応策を採用する理由を文書化することが望ましい。 ・組織は、対応策の適用等に関して、セキュリティリスク対応計画を策定し、リスク所有者の承認を得る。 ・組織は、セキュリティリスク対応計画をレビューし、当該計画が自組織全体のリスクマネジメント戦略における優先順位に適合しているかどうかを確認する。 ・組織は、策定したリスクへの対応策の影響を受ける関係者に対し、当該対応策を重要度の高いものから順に伝達する。 ・CPS.ID.RA-03で抽出した、IoT機器を含む新しいシステムにおける必要なセキュリティ対策について、然るべき外部事業者に要求仕様として伝達する。 ・組織は、IoT機器を含むシステムの導入時に、要求仕様や契約段階で定めたセキュリティ対策が実施されているかを受け入れ検査などで確認する。もし、不明な点があれば、外部事業者に確認する。 ・組織は、リスク対応の実施状況を、行動計画及びマイルストーン、リスク管理簿、リスク詳細レポート等を用いて継続的に把握する。 ・組織は、今後対応することを前提として受容しているリスクについて、定期的にレビューを行う。 ・組織は、セキュリティリスク対応のプロセスについての文書化した情報を安全に保管する。	0	○ (下記に加えて、03.12.02 実施計画およびマイルストーン a)		-		○ (6.3.1.1、8.2.6.1、12.2.9.1)
			<Basic> ・組織は、リスクアセスメントの結果を考慮して、対象とするリスクへの対応策を選定する。 ・組織は、本来のリスク低減対策が実施できない場合に備え、代替策を選定する。 ・組織は、セキュリティリスクの受容について、リスク所有者の承認を得る。	0	○ (03.11.04 リスク対応)		-		-
CPS.ID.RA-07	・組織は、自組織における重要な変更及びセキュリティ要件の例外について、それらがもたらすリスクの影響度をアセスメントし、その結果を記録し、管理する。	L1_1_a-SYS L1_1_b-SYS L1_1_c-SYS	<High-Advanced><Advanced><Basic>共通 ・組織は、提案された各変更について、実施する場合と実施しない場合のそれぞれで想定されるリスクを文書化するとともに、変更のロールバックに関する手引きを整備する。 ・組織は、申請された各例外に関連するリスク、及び当該リスクへの対応計画を文書化する。	0	○ (03.04.02 構成設定 b、03.04.03 構成変更管理 b、03.04.04 インパクト分析 a)	○ (CA-07、CM-03、CM-04)	-	○ (7.2.4.1、9.4.5.1)	-
CPS.ID.IM-01	・組織は、CPS.ID.IM-02以降に示す観点を含め、自組織における平時又は有事のサイバーセキュリティ管理態勢を継続的に改善する。	-	<High-Advanced> ・経営層による承認を受けたうえで、高いリスクを抱えるシステムに対してペネトレーションテストを実施し、セキュリティ態勢の改善機会を明確化する。 ・組織は、セキュリティ対応組織の成熟度を定期的に評価し、セキュリティ関連業務を継続的に改善することが望ましい。	0	-	○ (下記に加えて、CA-08、SA-17、SA-17(06))	-	-	-
			<Advanced> ・組織は、サイバーセキュリティ管理体制の改善に活かすため、セキュリティツール及びサービスを用いてセキュリティ対策の有効性を測る指標を収集し、分析する。 ・組織は、改善が必要な領域を特定するため、自組織のサイバーセキュリティ管理体制の有効性を評価する第三者評価又は独立監査に投資する。	0	-	○ (下記に加えて、IR-03、SA-11)	-	-	-
			<Basic> ・組織は、年1回以上の頻度で、セキュリティインシデント発生時の体制について点検を行い、必要に応じて改善を行う。	0	-	○ (AC-01、AT-01、AU-01、CA-01、CA-02、CA-05、CA-07、CM-01、CP-01、CP-02、CP-04、IA-01、IR-01、IR-04、IR-08、MA-01、MP-01、PE-01、PL-01、PL-02、PM-01、PM-04、PM-31、PS-01、PT-01、RA-01、RA-03、RA-05、RA-07、SA-01、SA-04、SA-08、SC-01、SI-01、SI-02、SI-04、SR-01、SR-05)	-	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.IM-02	・組織は、サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。	-	<High-Advanced><Advanced><Basic>共通 ・組織は、取引先のセキュリティに関わるパフォーマンスを継続的にモニタリングし、最新の脅威動向、規制動向等を踏まえ、サプライチェーンに係るセキュリティ対策基準及び、それに付随するプロシージャ等をレビューし、必要に応じて改定する。	O	○ (03.17.01 サプライチェーンのリスクマネジメント計画 b)	-	-	-	-
CPS.ID.IM-03	・組織は、自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を継続的に改善する。	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO L1_3_c_PEO L1_1_d_PEO	<High-Advanced><Advanced>共通 ・組織は、自組織の要員及び関係他組織の担当者等のセキュリティに対する理解をより確実にするため、教育、研修、訓練による効果を継続的に検証する。 ・組織は、年1回以上の頻度で、セキュリティの意識向上のための教育・研修の実施内容について点検を行い、必要に応じて改善する。	O	○ (下記に加えて、03.02.01 リテラシートレーニングおよび意識向上 b、03.02.02 役割ベースのトレーニング b)	○ (下記に加えて、CA-08、IR-03、SA-11)	-	○ (6.2.4.1)	-
			<Basic> ・組織は、年1回以上の頻度でセキュリティインシデント発生時の対応に関する教育・訓練の実施内容について点検を行い、必要に応じて改善する。	O	○ (03.06.04 インシデント対応トレーニング b)	○ (AC-01、AT-01、AU-01、CA-01、CA-02、CA-05、CA-07、CM-01、CP-01、CP-02、CP-04、IA-01、IR-01、IR-04、IR-08、MA-01、MP-01、PE-01、PL-01、PL-02、PM-01、PM-04、PM-31、PS-01、PT-01、RA-01、RA-03、RA-05、RA-07、SA-01、SA-04、SA-08、SC-01、SI-01、SI-02、SI-04、SR-01、SR-05)	-	-	-
CPS.ID.IM-04	・組織は、セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを継続的に改善する。	-	<High-Advanced><Advanced><Basic>共通 ・組織は、自組織あるいは第三者によるセキュリティ評価の結果から教訓を導き出し、資産を保護するプロセスを継続的に改善する。	O	○ (03.12.02 実施計画およびマイルストーン b)	-	○ (A.5.27)	○ (6.3.4.1)	-
CPS.ID.IM-05	・組織は、アラートやログ等の検知イベントの分析結果から教訓を導き出し、セキュリティ事象の検知プロセスを継続的に改善する。	L1_3_a_ORG L1_3_a_SYS	<High-Advanced> ・組織は、検知能力向上のため、様々な情報ソースをもとに、検知ルールの作成とチューニングを行う - 相関分析ルールの開発 - IPS/IDSの独自シグネチャの開発 - 独自ブラックリストの開発 ・組織／システムは、システムの通信やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、誤検出の数や、検出漏れのを減らすためのチューニングを行う。	O	-	-	-	-	-
			<Advanced> ・組織は、経営層等の組織内の然るべき要員に、定期的に組織及びシステムのセキュリティの状態を報告するプロセスを整備し、運用する。組織は、報告の場を最新の脅威や残存するリスクに対する脅威を認識し、セキュリティを向上するための場とすることが望ましい。 ・例えば、以下のような注意喚起情報の発信があった際等に、セキュリティに係るリスク増加の兆候がある場合、信頼できる情報源からの情報に基づいて、システムのモニタリング活動のレベルを上げる。 ※以下のリストは、「セキュリティ対応組織 (SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v2.0」(ISOG-J, 2019年)より引用している。 - 攻撃の特徴 ➢ 攻撃形態、関連する通信の内容 ➢ 核心となる攻撃コード - 攻撃によって残る痕跡 ➢ 被害を受けた後の通信内容 ➢ サーバやクライアントに残るログ ➢ サーバやクライアントに残るその他特徴 - 各セキュリティ製品における検知名	O	-	-	-	-	-
			<Basic> (該当なし)	-	-	-	-	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.ID.IM-06	・組織は、セキュリティインシデントへの対応から教訓を導き出し、インシデント対応計画を継続的に改善する。	L1_3_a_ORG L1_3_a_PEO L1_3_a_PRO L1_3_c_ORG	<High-Advanced> ・組織は、過去のセキュリティインシデントの種類、件数及び対応費用等を管理するメカニズムを導入し、対応の傾向や課題を把握できるようにする。	0	-	○ (CP-02、IR-08、PL-02、SR-02)	○ (A.5.27)	-	-
			<Advanced> ・組織は、インシデント対応後に重要なサプライヤーと共同で振り返りを実施する。 ・組織は、重要なサプライヤーと連携して実施した演習を踏まえ、今後のインシデント対応活動における改善点を明確化する。 ・組織は、インシデント対応計画について、毎年、又は改善が必要となった場合にレビューを行い、当該計画を更新する。	0	○ (03.06.05 インシデント対応計画 c)			-	-
			<Basic> ・セキュリティインシデントの評価から得た脅威情報、脆弱性情報等は、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ことが望ましい。 ・組織は、インシデント対応の評価結果（例：机上演習やシミュレーション、テスト、内部レビュー、独立監査）を踏まえ、今後のインシデント対応活動における改善点を明確化する。	0	-			-	-
CPS.ID.IM-07	・組織は、セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又は緊急時対応計画を継続的に改善する。	L1_3_a_PRO	<High-Advanced><Advanced><Basic>共通 ・組織は、セキュリティインシデントへの対応から、事業継続のためのプロシージャ及び関連する対策の機能が、事業継続のより上位の方針と合致しているかを確認する。 ・組織は、重要なサプライヤーと連携して実施した演習を踏まえ、事業継続計画又は緊急時対応計画における改善点を明確化する。 ・組織は、事業継続計画又は緊急時対応計画について、毎年、又は改善が必要となった場合にレビューを行い、当該計画を更新する。	0	-	-	-	○ (13.2.1.1)	-
CPS.PR.AA-01	・組織は、承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	L1_1_a_SYS L1_1_b_SYS L2_1_b_SYS L2_1_c_SYS L2_3_c_SYS L3_3_a_SYS	<High-Advanced> ・組織は、自組織の情報システム及び産業用制御システムにおけるアカウントの管理について、例えば以下のような自動化されたメカニズムを導入し、運用する。 - 管理対象となるシステムからアカウント情報を定期的に自動収集する - 特権アカウントのパスワードを自動で変更する ・産業用制御システムは、統合されたアカウント管理をサポートする。 ・情報システムは、自組織のシステムの一時的利用アカウントや緊急アカウント、利用されていないアカウントについて、一定期間の経過後又は申請時利用期限終了後に自動的に無効にする。 ・情報システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化及び無効化について自動的に監査・報告する。	O/S	-	○ (下記に加えて、IA-03)	○ (A.5.16、A.5.17)	-	○ (SR 1.1、SR 1.3、SR 1.5)
			<Advanced> ・組織は、各デバイスについて、変更不可能なハードウェア特性、又はデバイスに安全に配備された識別子のいずれかを、一意の識別子として選定する。 ・組織は、情報システム及び産業用制御システム上で使用されているデフォルトユーザ ID の利用を停止する。 ・既存の産業用制御システムのデフォルトのパスワードを変更するとともに、今後調達予定であるデバイスのデフォルトの認証情報を変更するためのポリシーを確立する。 ・共有ユーザアカウントに関しては、認証情報を知りえるユーザを一覧等で管理し、アカウントを利用する範囲を特定可能にする。 ・情報システムは、クレデンシャルを忘れてしまった際等にクレデンシャルを再設定する場合、悪意ある者によるクレデンシャルの不正な変更を防ぐため、当該アカウントが自身のものかどうかを確認するための安全な手順を適用する。 ・組織は、情報システム及び産業用制御システムにおいてパスワードが変更された場合、ユーザー（または管理責任者）に通知する。 ・組織は、情報システムにおけるシステムアカウントの利用状況をモニタリングする。 ・組織は、アカウントが不要になった場合や変更が必要となった場合には管理責任者に通知する。	O/S	○ (下記に加えて、03.05.12 オーセンティケータの管理 c,e)			○ (11.2.1.1、11.2.8.1)	○ (SR 1.1、SR 1.4、SR 1.5)
			<Basic> ・組織は、自組織の情報システム及び産業用制御システムのアカウントを管理する管理責任者を配置する。 ・組織は、認可されたハードウェアに識別子を記したラベルを貼る。 ・組織は、自社の役員、従業員、派遣社員及び受入出向者に対するユーザIDの付与・変更・削除は申請・承認制にする。 ・組織は、ユーザIDの共有について、以下のいずれかを適用する。 - ユーザIDを共有しない。 - やむを得ず共有IDが必要な場合(例えば、システムの仕様により、使用人数分のユーザIDを発行することができない場合)は、共有IDを利用したユーザを特定できるようにする。 ・組織は、ユーザIDが不要になった場合(例えば、ユーザが組織を退職した場合又はユーザIDが一定期間使用されなかった場合)、速やかにユーザIDを削除又は無効化する。 ・組織は、管理者IDの付与・変更・削除を申請・承認制にする。 ・組織は、管理者権限を付与する役員、従業員、派遣社員及び受入出向者を限定したうえで、管理者IDについて以下のいずれかを適用する。 - 管理者IDを共有しない。 - やむを得ず管理者IDの共有が必要な場合(例えば、システムの仕様により、使用人数分のIDを発行することができない場合)は、共有の管理者IDを利用したユーザを特定できるようにする。 ・組織内でどの役員、従業員、派遣社員及び受入出向者が管理者IDを持っているかを把握するための仕組みを整備する。 ・組織は、管理者IDが不要になった場合(例えば、管理者が組織を退職した場合及び管理者IDが一定期間使用されなかった場合)、速やかに管理者IDを削除又は無効化する。 ・組織は、自組織の情報システム及び産業用制御システムに対するクレデンシャル（例：パスワード、セキュリティキー）のポリシーを定め、システムが対応可能な場合は、当該ポリシーを満たすクレデンシャルでなければ設定できない機能を有効化する。技術的な制約により当該機能を利用できない場合は、アクセス経路の制限、監視の強化その他の代替策を講じる。 - クレデンシャルに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいクレデンシャルが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたクレデンシャルのみを保存・伝送する。 - 同じクレデンシャルを組織が定めた世代にわたって再利用するのを禁止する。 ・組織は、暗号証明書、ID トークン、暗号鍵（すなわち鍵管理）、及びその他の認証情報を発行、管理、及び失効する。 ・組織は、クレデンシャルを忘れてしまった際等に、強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なクレデンシャルを使用することを許可する。 ・組織は、パスワードの漏えい若しくは侵害が疑われる場合又は利用者に変更があった場合、当該パスワードを速やかに変更する。	O/S	○ (03.01.01 アカウント管理 a,b,c,f、03.05.05 識別子管理 b,c,d、03.05.12 オーセンティケータの管理 a,b,d、03.09.02 退職と異動 a、03.10.01 物理的アクセス認可 b、03.13.10 暗号鍵の確立および管理)	○ (AC-01、AC-02、AC-14、IA-01、IA-02、IA-04、IA-05、IA-06、IA-07、IA-11)	○ (10.2.6.1、11.2.1.1、11.2.2.1、11.2.8.1、11.2.11.1、11.2.12.1)	○ (SR 1.1、SR 1.3、SR 1.4、SR 1.5、SR 1.7、SR 1.8、SR 4.3)	

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.AA-02	・組織は、IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で、信頼性の高い方式（例：多要素認証）を用いて認証・認可する。	L1_1_a_SYS L1_1_b_SYS L1_1_c_SYS L2_1_b_SYS L2_1_c_SYS L2_3_c_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> ・情報システムにおいて、認証時に多要素認証を必須とする。 ・産業用制御システムにおいて、ベンダー／保守アカウント、リモートアクセス可能なユーザーおよびエンジニアリングワークステーション、リモートアクセス可能なHMI（利用可能な場合）など、リモートアクセス可能なすべてのアカウントおよびシステムで多要素認証を有効化する。多要素認証が利用できない場合は、リモートアクセスを削除し、追加のセグメント化手順を導入し、認証情報の管理を優先する。 ・機密性の高いデータを取り扱う自組織の情報システムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リブレイ攻撃に対する耐性のある認証メカニズムを実施する。 ・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザ及び機器による認証を暗号化とともに用いることによって保護する。 ・情報システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。	S	○ （下記に加えて、03.01.12 リモートアクセス d、03.01.16 ワイヤレスアクセス d、03.05.03 多要素認証、03.05.04 リブレイ攻撃耐性のある認証、03.07.05 非ローカルメンテナンス）		○ （下記に加えて、03.01.12 リモートアクセス d、03.01.16 ワイヤレスアクセス d、03.05.03 多要素認証、03.05.04 リブレイ攻撃耐性のある認証、03.07.05 非ローカルメンテナンス）	○ （8.4.2.1、8.4.3.1、11.2.8.1、11.2.9.1）	○ （SR 1.1、SR 2.6、SR 3.8）
			<Advanced> ・重要な機密情報を取り扱うシステムにおいて、重要な機密情報を取り扱うクラウドサービスへのアクセスに加えて、以下に示す場合は、常に多要素認証を使用する。 - インターネットを経由して社内環境へ接続する場合 - 管理者がインターネット経由でシステムにアクセスする場合 - ユーザがインターネット経由で重要な機密情報を取り扱うシステムにアクセスする場合 ・組織は、自組織で利用する携帯機器から自組織のシステムの接続に関する承認ルール等を定める。 ・組織は、対象システムにおける特権アカウントへの不正ログインのリスク等を勘案し、十分に信頼性の高い認証方式を実装できない場合、ネットワーク経由での特権アカウントへのログインを原則禁止する。 ・リスクに応じて、ユーザー、サービス、及びハードウェアを定期的に再認証する（例：ゼロトラストアーキテクチャの考え方を参考）。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、アクセスの認可を判断する際、アクセス権限の要求者及び対象リソースの属性（例：地理的位置、曜日や時間帯、要求者の端末のセキュリティ状態）を考慮する。	O/S	-			-	○ （SR 1.1、SR 1.2、SR 1.10）
			<Basic> ・すべてのユーザID及び管理者IDについて、システム及び情報機器へのアクセスを許可する前に、ユーザIDごとに設定されている認証情報(パスワード等)でユーザを認証する。 ・重要な機密情報を取り扱うクラウドサービスにおいて、ユーザ及び管理者がサービスにアクセスする場合は、多要素認証を使用する。 ・組織は、許可されていない無線接続を原則禁止とする。 ・組織は、無線によるシステムへのアクセスを、事前に権限を付与した端末・ユーザに限定する。	O/S	○ （03.05.01 ユーザの識別および認証 a、03.05.02 デバイスの識別および認証）	○ （AC-07、IA-02、IA-05、IA-07、IA-08、IA-11）		○ （11.2.8.1）	○ （SR 1.1、SR 2.2）

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.AA-03	・組織は、一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあげる機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ。	L1_1_a_SYS L1_1_b_SYS L1_1_c_SYS L2_1_b_SYS	<High-Advanced><Advanced>共通 ・産業用制御システムは、自組織のシステムに対してユーザが連続してログインを失敗できる上限を設定し、上限以上失敗した場合には一定期間再ログインできない機能を実装する。 ・情報システム及び産業用制御システムは、組織が定める時間を越えてシステムの無操作が持続する場合、手動又は自動でセッションロックを実施する。 ※ 産業用制御システムにおいて、緊急時対応においてオペレータの即時対応が求められるようなセッションを実施するケースが想定される場合、セッションロックを実施しないことが望ましい。	S	○ (下記に加えて、03.01.08 ログイン試行の失敗 b)	-	○ (A.8.5)	○ (11.2.3.1、11.2.15.1、11.2.18.1)	○ (SR 1.11、SR 2.5)
			<Basic> ・情報システムは、パソコンへのログイン及びスマートデバイスのロック解除にあたって、以下のいずれかを適用する。 - 試行回数を調整し、試行が失敗するたびに試行間隔が長くなるようにする。 - 試行が連続して10回以上失敗すると端末をロックする。 - 上記で示す要件のいずれも設定することができない場合、強度の高いパスワードを用いる等の代替策を用いること。	S	○ (03.01.08 ログイン試行の失敗 a)	-		-	-
CPS.PR.AA-04	・組織は、認証された主体に関する情報（IDアサーション）を保護し、送受信し、検証する。	L1_1_a_SYS L1_1_b_SYS	<High-Advanced><Advanced>共通 ・組織は、ID アサーションについて全ての場面で業界標準に準拠した方式を採用し、ID アサーションの生成（例：データモデル、メタデータ）、保護（例：デジタル署名、暗号化）、及び検証（例：署名検証）に関する全てのガイダンスに従う。 ・情報システムは、連携している外部システムとの間で認証情報及びユーザー情報を伝達するために用いられる ID アサーションを保護する。	O/S	-	-	-	-	-
			<Basic> ・情報システムは、シングルサインオン（SSO）システムで認証情報及びユーザー情報を伝達するために用いられる ID アサーションを保護する。	S	-		-	-	-
CPS.PR.AA-05	・組織は、アクセス権限の付与に関する規定をセキュリティポリシーに定義し、最小特権と職務分離の原則を組み込む。	L2_1_b_SYS L2_1_c_SYS	<High-Advanced> ・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・情報システムは、システム内（及び相互接続システム間）のデータフローを制御するために、ユーザに対して（管理者によって）承認されたアクセス権限を強制的に適用する。 ・情報システムは、非特権ユーザによるセキュリティ機能の無効化、回避、変更及びその他の特権機能の実行を禁止する。	O/S	○ (下記に加えて、03.01.05 最小特権 b、03.01.06 最小特権 – 特権アカウント a、03.01.07 最小特権 – 特権機能 a、03.03.08 監査情報の保護 b、	○ (下記に加えて、AC-10)	○ (A.5.15、A.8.2)	○ (11.3.2.1)	○ (SR 1.1)
			<Advanced> ・組織は、情報システム内（及び相互接続システム間）のデータフローを制御するために、ユーザのアクセス権限に応じて任意アクセス制御を実施する。 ・組織は、自組織の情報システム及び産業用制御システムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、担当者に割り当てた職務の分離結果を、明文化する。	O/S	○ (下記に加えて、03.01.05 最小特権 a、	○ (下記に加えて、AC-05、AC-06)	○ (A.5.3、A.5.15、A.8.2)	○ (11.2.4.1、11.3.2.1)	○ (SR 1.1、SR 2.1)
			<Basic> ・組織は、自組織の機密性の高い情報システムにおいて職務分離（例：ユーザ/システム管理者）を踏まえたアクセス制御を実施する。 ・人的リソース等の関係で、職務の分離が困難な場合、あらかじめ指定された役職者以外が特定の職務を実行する際に、他の要員が職務の遂行をモニタリングする等の代替策を講ずることが望ましい。 ・組織は、管理者IDの付与・変更・削除並びにサーバ及びネットワーク機器の設定内容の変更を行う権限を業務上必要な役員、従業員、派遣社員及び受入出向者に限定する。 ・組織は、業務で利用するシステム及びパソコンへのログイン時のユーザのアクセス権について、以下の内容の管理ルールを定める。 - アクセス権の発行・変更・削除は申請・承認制であること。 - 与えるアクセス権の範囲は必要な範囲に限定すること。 - アクセス権の棚卸について定めていること。 - 与えたアクセス権の申請書又は台帳を管理していること。 ・組織は、認可された担当者が安全確保に不可欠なアカウントへ緊急時にアクセスできる状態を確保する。	O/S	○ (03.01.01 アカウント管理 c、03.01.02 アクセス実施、03.01.04 職務の分離 a、03.04.05 変更に対するアクセス制限、03.08.02 媒体へのアクセス)	○ (AC-01、AC-02、AC-03、AC-17、AC-18、AC-19)		○ (11.2.4.1)	

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.AA-06	・組織は、アクセス権限の付与状況について、定期的に見直しを行い、不要又は過剰な権限を是正する。	L2_1_b_SYS L2_1_c_SYS	<High-Advanced><Advanced>共通 ・組織は、年1回以上の頻度で役員、従業員、派遣社員及び受入出向者に付与したアクセス権の棚卸を実施する。	O	○ (下記に加えて、03.01.05 最小特権 c、03.10.01 物理的アクセス認可 c)	○ (下記に加えて、AC-05、AC-06、AC-10)	○ (A.5.18、A.8.2)	○ (11.2.5.1)	-
			<Basic> ・組織は、ユーザIDに付与したアクセス権が不要になった場合(例えば、ユーザの業務上の役割が変わった場合)、当該権限を速やかに削除又は無効化する。	O	○ (03.01.01 アカウント管理 f、03.01.05 最小特権 d、03.09.02 退職と異動 b)	○ (AC-01、AC-02、AC-03、AC-17、AC-18、AC-19)		○ (11.2.2.1、11.2.4.1)	-
CPS.PR.AA-07	・組織は、IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	L1_1_a_SYS L1_1_c_SYS L2_3_b_PEO L2_3_b_SYS L2_3_d_SYS L3_1_a_SYS	<High-Advanced> ・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。	O/S	○ (下記に加えて、03.10.02 物理的アクセスの監視 a、03.10.07 物理的アクセス制御 e、03.10.08 伝送のアクセス制御)	○ (下記に加えて、PE-18)	○ (A.7.2、A.7.8)	○ (下記に加えて、13.2.2.1)	-
			<Advanced> ・組織は、サーバの設置エリア又はサーバを収納するラックを施錠するとともに、当該鍵等について、管理者を定めたうえで安全に管理する。 ・組織は、高いリスクを抱える資産を含む区域に対し、追加の物理的なセキュリティ対策を採用する。 ・組織は、パソコン、スマートデバイス、カメラ及び外部記憶媒体(個人所有機器の業務利用(BYOD)を含む。)を対象とした社内への持込みルールを定める。 ・組織は、年1回以上の頻度で、パソコン、スマートデバイス、カメラ及び外部記憶媒体（BYOD含む）における持込ルール内容及び遵守状況について点検する ・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。	O	○ (下記に加えて、03.10.07 物理的アクセス制御 d)	○ (下記に加えて、PE-04、PE-05)	○ (A.7.2、A.7.3)	○ (6.4.1.1)	-
			<Basic> ・組織は、自組織の施設においてセキュリティを保つべき物理的セキュリティ境界を定め、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応じてアクセス制御を実施する。 ・組織は、機密上の配慮が必要な場所及び部屋への入室について、以下の内容の管理ルールを定める。 - 与える入室許可の範囲は必要な範囲に限定すること。 - 入室権限の棚卸について定めていること。 - 与えた入室許可の申請書又は台帳を管理していること。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、物理的セキュリティ境界内における自組織または自組織外の一時的に認可された入場者に対して、認可された関係者の付き添い又は監視カメラ等により作業内容をモニタリングできるようにする。	O/S	○ (03.10.01 物理的アクセス認可 a、03.10.07 物理的アクセス制御 a)	(PE-02、PE-03、PE-06、PE-08)	○ (A.7.2、A.7.6)		-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみ適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.AT-01	・組織は、自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO L1_2_a_PEO L1_3_a_PEO L1_3_c_PEO L1_1_d_PEO L3_4_a_PEO L3_4_b_PEO	<High-Advanced> ・組織は、内部不正の兆候を認識・報告するためのセキュリティ意識向上トレーニングを、全要員に対して実施する。 ・組織は、調達した製品・サービスが、正規のサプライヤ以外から供給されていた、又は改ざんされていたことが判明した場合に備え、インシデント対応計画に基づく演習を実施する。	0	-	○ 			

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.DS-02	・組織は、保存しているデータの機密性、完全性、及び可用性を保護する。	L1_1_a_DAT L1_1_b_DAT L3_4_b_SYS L3_3_d_SYS L3_1_a_DAT L3_2_a_DAT	<High-Advanced> ・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・組織は、内部メモリのデータを暗号化して保管することのできるIoT機器を利用する。 ・組織は、暗号鍵の紛失に備え、鍵のバックアップ、復旧その他の方法により、暗号化された情報の可用性を維持する。 ・組織は、秘密鍵を安全に管理することに加え、公開鍵の真正性についても考慮することが望ましい。この認証プロセスは、認証局によって通常発行される公開鍵証明書を用いて実施される。この認証局は、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ている、認知された組織であることが望ましい。	O	-	○ (下記に加えて、SC-04、SC-28、SI-07)	○ (A.5.33、A.8.12、A.8.24)	○ (10.2.6.1)	○ (SR 4.1、SR 4.3)
			<Advanced> ・組織は、パソコン、スマートデバイス、カメラ、外部記憶媒体(個人所有機器の業務利用(BYOD)を含む。)及び印刷物(図面等の機密書類)に関する社外への持出しルールを定める。 ・組織は、年1回以上の頻度で、パソコン、スマートデバイス、カメラ及び外部記憶媒体(個人所有機器(BYOD)を含む。)における持込みルール及び持出しルール内容及び遵守状況について点検する。 ・組織は、重要な機密情報を暗号化するルールを定め、役員、従業員、派遣社員及び受入出向者を対象に周知する。 ・組織は、マルウェアによる被害を受けた場合に業務に支障をきたすデータはパソコン以外の社内ネットワーク(クラウドサービスを含む。)上の相対的に安全な区域にあるサーバに保管するようルールを定め、役員、従業員、派遣社員及び受入出向者を対象に周知する。 ・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、産業用制御システムが取り扱う重要度の高い情報（データ）を、パフォーマンスに許容できない影響が出ない範囲で適切な強度の方式で暗号化して保管する。 ・組織は、秘密鍵が危険化した際に遅滞なく適切な対処を行うため、必要に応じて下記のような事項について方針及び手順を定めることが望ましい。 - 秘密鍵の危険化に対応するための体制(関係者と役割、委託先との連携を含む) - 秘密鍵が危険化した、またはその恐れがあると判断するための基準 - 秘密鍵の危険化の原因を調べること及び原因の解消を図ること - 当該鍵を利用するサービスの利用停止 - 新しい鍵ペアを生成し、新しい鍵に対する証明書を発行すること - 秘密鍵の危険化についての情報の開示(通知先、通知の方法、公表の方針等) ・組織は、全ての暗号鍵を改変及び紛失から保護することが望ましい。	O/S	○ (下記に加えて、03.01.18 モバイルデバイスのアクセス制御 c、		○ (10.2.2.1、10.2.5.1、10.2.6.1)		
			<Basic> ・組織は、暗号化されていない機微情報を含むリムーバブルメディアを施錠されたオフィスやキャビネット等に保管し、物理的に保護する。	O	○ (03.05.07 パスワード管理 d、03.05.12 オーセンティケータの管理 f、03.06.05 インシデント対応計画 d、03.08.01 媒体保管、03.08.09 システムバックアップー暗号化による保護 a.b、03.13.08 伝送中および保存中の機密性、03.13.11 暗号保護、03.15.02 システムセキュリティ計画 c、03.17.01 サプライチェーンのリスクマネジメント計画 c)	○ (CA-07、CP-09、SC-07、SC-12、SC-13、SC-39、SI-03、SI-04)	○ (A.5.33、A.8.1、A.8.12、A.8.24)	-	-
CPS.PR.DS-03	・組織は、伝送中のデータの機密性、完全性、及び可用性を保護する。	L1_1_a_DAT L1_1_b_DAT L3_3_d_SYS L3_1_a_DAT L3_2_b_DAT L3_3_a_SYS	<High-Advanced> ・情報システムは、取扱うデータの重要度に限らず、組織外部への全ての通信を暗号化する。 ・組織は、産業用制御システムを構成する重要なデータを扱う通信路について、通信経路の暗号化を実装する又は代替の物理的な対策によって保護する。 ・システム/IoT機器は、少ないリソースでも可用性を損なわずに実装可能な暗号モジュールを導入し、リソースは制限されているが重要度の高い機器からの通信データを適切な強度で暗号化することが望ましい。 ・組織は、産業用制御システムにおいて、可能な場合、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。	O/S	○ (下記に加えて、03.13.08 伝送中および保存中の機密性)	○ (CA-03、SC-07、SC-12、SC-13、SI-03、SI-04、SC-04、SC-08、SI-07)	○ (A.8.12、A.8.24)	○ (下記に加えて、10.2.2.1)	○ (SR 3.1、SR 3.8、SR 4.1)
			<Advanced> ・組織は、取引先との情報共有及び情報送信に関して、以下をルールとして定め、役員、従業員、派遣社員及び受入出向者へ周知する。 - 社外とファイル共有する場合は、信頼できる相手とのみ共有すること。 - 社外へファイル転送をする場合は、送信履歴を残すこと。 ・データの分類に応じて、機微情報を含む送信メールその他の通信については、暗号化を自動的に行うか、又は送信を遮断する。 ・伝送中のデータの完全性を保護するため、デジタル署名、メッセージ認証コード等の適切な手段を利用する。 ・情報システムにおいて、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・情報システムは、電子メールにおける送信ドメイン認証技術をサポートして、送信者のなりすましやメールの改ざんを検知する。 [参考] 通信経路の保護には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。	O/S	○ (03.05.07 パスワード管理 c)		○ (A.5.14、A.8.12、A.8.24)	○ (10.2.7.1)	○ (SR 3.1、SR 3.8)
			<Basic> (該当なし)	-	-	-	-	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.DS-04	・組織は、使用中のデータの機密性、完全性、及び可用性を保護する。	L1_1_a_DAT L1_1_b_DAT L3_3_d_SYS L3_1_a_DAT L3_2_b_DAT	<High-Advanced><Advanced><Basic>共通 ・組織は、機密として保持すべきデータを不要となった時点で速やかに削除する（例：プロセッサやメモリ上のデータ）。 ・使用中のデータについて、同一のシステム上における他のユーザ及びプロセスからのアクセスを防止する。	O/S	○ (03.13.04 共有システムリソース内の情報)	○ (AC-02、AC-03、AC-04、AU-09、CA-03、CP-09、SA-08、SC-04、SC-07、SC-13、SC-24、SC-39、SI-03、SI-04、SI-07、SI-10、SI-16)	○ (A.8.1、A.8.12)	-	○ (SR 4.2)
CPS.PR.DS-05	・組織は、データの取得元、加工履歴等をライフサイクル全体に渡って維持・更新・管理する。	L1_1_b_DAT L3_2_a_DAT	<High-Advanced> ・組織は、自組織が管理するデータの処理を実施するサイバー空間におけるサプライチェーンの中に、自組織が委託先等に要求している水準の対策を実装していないエンティティが介在していないかを確認する。	O	-	-	-	-	-
			<Advanced> ・組織は、自組織が活用するデータの取得元及び、当該データを処理した組織、ヒト等を識別する。 ・組織は、他組織あるいは、自組織外の個人、IoT機器等から取得したデータの取得元を、当該データに紐づけて、取得から廃棄に至るまでのライフサイクル全体に渡り管理する。	O	-	-	-	-	-
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.PR.DS-06	・組織は、データ（例：構成要素の設定情報、業務データ等を含む）に対し、定期的なバックアップを実施し、バックアップデータの保護及び復旧のテストを行う。	L1_1_a_DAT L1_3_a_DAT L3_3_d_SYS L3_1_a_DAT	<High-Advanced> ・組織は、バックアップを定期的にテストして、媒体の信頼性と情報の完全性を確認する。	O	-	○ (下記に加えて、CP-06)	○ (A.8.13)	○ (13.3.3.1)	○ (SR 7.3)
			<Advanced> ・事業継続上重要なシステムについて、サイバー攻撃を念頭に、以下の対策を講じる。 - 目標復旧時点への復旧ができるように、取得したバックアップを保管する。 - 整備したリストア手順書どおりに、かつ、目標復旧時間内でバックアップの復元ができることを確認する。 ・重要データについては、システムの特性上実施可能な場合、準リアルタイムで継続的にバックアップを取得し、その他のデータについては定められたスケジュールに従い、頻繁にバックアップを取得する。 ・組織は、保管拠点におけるバックアップ情報の機密性・完全性・可用性を保護する。	O	○ (03.08.09 システムバックアップー 暗号化による保護)			○ (13.3.1.1、13.3.3.1、13.3.4.1、13.3.5.1)	
			<Basic> ・取得対象、取得頻度及び保管期間を定めて自社で取り扱うデータのバックアップを取得する。 ・組織は、バックアップ対象ごとにリストア手順書を整備する。 ・組織は、バックアップからの復旧が可能であることを、少なくとも年1回テストする。 ・事故や災害による影響を受けないよう、一部のバックアップはオフラインかつ別拠点において安全に保管する。	O	-	○ (CP-09)			

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.PS-01	・組織は、ハードウェア及びソフトウェアの真正性と完全性を、取得及び使用前に評価するとともに、稼働中もハードウェア及びソフトウェアの完全性を検証する。	L2_3_b_ORG L2_3_b_SYS L2_3_c_ORG L2_3_c_PRO	<High-Advanced> ・組織は、IC チップの純正品と不正品のサイドチャネル情報の違いからハードウェアの改ざん（ハードウェア・トロイの挿入）を検知する。 ・組織は、PUF（Physically unclonable function）の技術を活用して物理的に読取り可能なチップの固有IDを生成し、テストを通じてハードウェアの改ざん(ハードウェア・トロイの挿入)を検知する。 ・組織は、機器のシリアル番号やハッシュ値等を利用して、定期的にIoT機器及び搭載されているソフトウェアが正規品であることを確認するために、自動化されたメカニズムを含むツールを利用する。	O/S	-	○ (下記に加えて、SA-17)	○ (A.8.19)	-	○ (SR 3.4)
			<Advanced> ・署名を検証することにより、ソフトウェアの完全性を確認する。 ・調達した技術製品及びサービスの改ざんの有無及び真正性に関する確認状況を、定期的に経営層へ報告する。 ・産業用制御システムを保有する組織は、シリアル番号、チェックサム、デジタル証明書／署名、またはベンダーが提供するOTハードウェア、ソフトウェア、およびファームウェアの真正性を検証できるその他の識別機能を文書化し追跡する必要がある。 ・組織は、ハードウェアコンポーネントに対する不正な変更を検知するツール、複製しにくいラベルや、検証可能なシリアル番号等を用いて、完全性を確認できるようにする。 ・組織は、自組織のオペレーションにとって重要なハードウェアについて、設置エリアに対して監視カメラ等によるモニタリングを行うことで、ハードウェアに対する物理的な改ざんを検知できるようにする。 ・組織は、機器のシリアル番号やハッシュ値等を利用して、定期的にIoT機器及び搭載されているソフトウェアが正規品であることを確認する。	O/S	-	○ (下記に加えて、SA-10, SA-11、SA-15、SI-07、SA-06)	○ (A.8.7、A.8.19)	○ (9.4.1.1)	
			<Basic> ・組織は、調達時や資産の棚卸しを実施した際等に、自組織が所有するIoT機器が正規品であるかをラベルを確認する等して確かめる。	O	-	○ (SA-04、SA-05、SR-05、SR-10、SR-11)	-	-	-
CPS.PR.PS-02	・組織は、保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。	L1_1_d_COM L2_3_a_ORG L2_3_b_PEO L2_3_b_COM	<High-Advanced> ・組織は、保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用した機器を調達する。 ・組織は、情報システム及び産業用制御システム内で使用されている暗号技術向けの暗号鍵を保管するにあたり耐タンパーデバイスを用いて管理する。	O	-	-	-	-	○ (SR 1.9)
			<Advanced><Basic>共通 (該当なし)	-	-	-	-	-	-
CPS.PR.PS-03	・組織は、計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、適切なセキュリティ対策を実装した製品を利用する。	L1_2_a_COM L2_1_a_COM L2_1_a_PRO L2_2_a_ORG L2_1_a_PRO L2_3_a_ORG L2_3_d_ORG	<High-Advanced><Advanced>共通 ・ネットワーク接続性を持ち、フィジカル空間における動態をデジタル化しサイバー空間へ送信する機能を有する機器（センサ等）を導入する際、当該機器の機能における下記の観点を検討し、調達を実施することが望ましい。 - 完全性検証ツールを使用して、通信データに対する不正な変更を検知する機能を実装しているか - 他のIoT機器、サーバ等から識別可能なユニークIDを有するか、あるいは証明書を搭載しており、通信先との相互認証等を通じて真正性を主張できるか - 機器のリソースが、ある程度の規模のサービス拒否攻撃等を受けた際でも可用性を維持することが可能なレベルのものか [参考]インターネットとの通信が行えるIoT機器を調達する際は、IPAが運用する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」を参照することが可能である。	O	-	-	-	○ (13.2.2.1)	○ (SR1.2、SR 3.1)
			<Basic> ・組織は、物理的な攻撃に対して耐性を有しているIoT機器（センサ等）を調達する。	O	-	-	-		-
CPS.PR.PS-04	・組織は、ネットワークにつながることを踏まえた安全性を実装するIoT機器を導入する。	L2_1_a_COM L2_1_a_PRO L2_2_a_ORG	<High-Advanced> ・ハザードのエネルギ等を下げて事故が起きても影響を小さくするように設計する等、本質安全設計を通じて、影響度の高いハザードに対処することで、被害を極小化する。	O	-	-	-	-	-
			<Advanced> ・組織は、セーフティの側面を考慮したセキュリティリスクアセスメント(CPS.ID.RA-06)を実施し、対象システムにおける物理的な安全に関する対策の要否及びそのレベルを把握する。 ・本質安全設計を通じてハザードの縮減を図る。当該プロセスを通じて、影響度の高いハザードが残存した場合、例えば、下記のような代替的対策を講ずることが望ましい。 - 安全装置等の付加装置による安全確保 - ハザードを有する機器に要員が近づかないような空間設計の実施 ・産業用制御システムは、サイバー攻撃等により通常の操作が維持できない場合、あらかじめ決められた出力をするよう設定を行う。	O/S	-	-	-	○ (8.2.4.1、13.2.3.1)	○ (SR 3.6)
			<Basic> (該当なし)	-	-	-	-	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.PS-05	・組織は、セキュアなソフトウェア開発プラクティス（例：設計段階でのセキュリティレビュー、セキュアコーディング規約の適用、リリース前の脆弱性診断）をシステム開発ライフサイクルに統合し、その実施状況を確認する。	L3_4_b_SYS	<High-Advanced><Advanced>共通 ・自組織が開発したソフトウェアの全ての構成要素及びその開発環境（例：ソースコード、ビルド環境、依存ライブラリ、コンテナイメージ）について、改ざん及び不正アクセスから保護する。 ・自組織が開発したソフトウェアをレビュー、分析、又はテストし、設計、コーディング、及び初期設定における脆弱性を特定する。	O	-	○ (SA-10、SA-11、SA-15、SA-17)	○ (A.8.25、A.8.28、A.8.29)	○ (6.3.3.1)	-
			<Basic> ・組織は、システムを構築するに当たり仕様書、設計、開発、導入及び変更に、システムのセキュリティエンジニアリング原則を適用する。 [参考]システムの仕様策定、設計、開発、導入及び変更の各段階におけるセキュリティの確保に関する具体的な取組を検討するにあたっては、経済産業省が公開する「サイバーインフラ事業者に求められる役割等に関するガイドライン」を参照することが可能である。	O	○ (03.16.01 セキュリティエンジニアリングの原則)	○ (SA-03、SA-08)	○ (A.8.25、A.8.26、A.8.27)		-
CPS.PR.PS-06	・組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	L1_1_a_SYS L1_1_b_SYS L1_1_c_SYS L2_1_a_ORG L2_1_b_COM L2_1_b_PRO L2_1_c_ORG L2_3_c_SYS L3_3_d_SYS L3_1_a_SYS	<High-Advanced> ・情報システムは、実際の構成がベースライン構成に適合していない機器を検出した場合、組織が例外として許可したものを除き、当該機器の接続を遮断する等の是正措置を自動的に講じる。 ・組織は、ネットワーク構成、機器のソフトウェア構成等の情報を自動的に収集するメカニズムを利用し、常時最新の状況をモニタリングする。 ・情報システムは、機密性の高いデータを扱うネットワークに接続されたカメラ、マイク、ホワイトボード等の機器について、遠隔からの起動を禁止するとともに、利用中であることを利用者が認識できる仕組み（例：作動ランプの点灯）を備える。 ・組織は、IoT機器、サーバ等の設定を一つの場所から管理・適用・検証するための自動化されたメカニズムを使用する。 ・組織は、特に産業用制御システムにおけるセキュリティに係る変更管理手順を、既存のプロセス安全管理の手順に統合する。 ・組織は、情報システムのベースライン構成のロールバックを可能にするために、旧バージョンのベースライン構成（例えば、ハードウェア・ソフトウェア・ファームウェア・構成ファイル・構成記録）を記録する。	O/S	-	○ (下記に加えて、CM-03、CM-09)	○ (A.8.9、A.8.32)	○ (7.2.3.1)	○ (SR 7.6)
			<Advanced> ・重要なシステムを構成する情報機器について、設定情報を継続的に把握するための仕組みを整備する。 ・年1回以上の頻度で、重要システムを構成する情報機器の設定情報の内容を定期的に点検し、設定基準どおりに保たれているかを確認する。 ・パソコン、サーバ、及び複合機等のネットワークに接続する機器上で、不要サービス及びプロトコルを無効化する。 ・産業用制御システムにおいて、不正な機器の接続を防止するために、可能な場合は物理ポートを削除、無効化、またはその他の方法でセキュアにする手順を確立する。 ・産業用制御システムの運用に必要な特定の機能、プロトコル、およびサービスのみを許可することで、機能制限を実施する。 ・情報システム及び産業用制御システムのベースライン構成に変更が生じる場合、速やかにベースライン構成を更新し、常に最新の状況を把握できるようにする。 ・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等を文書化する。 ・組織は、構成管理の対象となるIoT機器、サーバ等に対して変更を実施する前に、テスト（動作検証）を実施する ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、セキュリティ上の変更によって情報システム及び産業用制御システムの可用性や安全性等に悪影響が及ばないことを確実にするため、運用及び変更管理のポリシー及び手順を定期的にレビューする。 ・組織は、システム、モノ等によって提供される機能とサービスをレビューし、削除の候補となる機能とサービスを特定する。 ・組織は、禁止されている機能、ポート、プロトコル、サービスの使用を検知し防止するために、ネットワークスキャンツール、侵入検知防止システム、エンドポイントプロテクション（ファイアウォール、ホストベースの侵入検知システム等）を活用する。	O	○ (下記に加えて、03.01.16 ワイヤレスアクセス c、03.04.01 ベースライン構成 a、03.04.03 構成変更管理 a.c、03.04.06 最小機能性 a,b,d、03.13.06 ネットワーク通信 ーデフォルトで拒否 ー例外による許可)			○ (6.3.2.1、7.2.3.1、7.2.4.1、8.2.8.1、8.3.1.1、9.2.1.1、9.2.2.1)	○ (SR 2.3、SR 5.3、SR 7.7)
			<Basic> ・組織は、外部記録媒体を使用する端末について、自動実行(auto-run)又は自動再生(auto-play)を無効化する。 ・組織は、サーバ及びネットワーク機器の設定変更を申請・承認制にする。 ・組織は、攻撃者に悪用される恐れのある、業務上不要なソフトウェア構成要素（例：OSのユーティリティ）をアンインストール・削除する。 ・組織は、自組織の運用に適合する最も制限された設定基準を定めた上で、導入されるIoT機器、サーバ等の初期設定手順及び設定内容を文書化するとともに、その文書に従って設定を実施する。 ・組織は、IoT機器を設置する前にデフォルトの初期設定値を確認し、予め定めたポリシーに準じていない場合に適切なものへと変更する。 ・組織は、使用しないUSBポート、シリアルポートは栓をするなど物理的に閉塞する。	O	○ (03.04.02 構成設定 a)	○ (CM-01、CM-02、CM-04、CM-05、CM-06、CM-07、CM-08、CM-10、CM-11)		○ (7.2.3.1、7.2.4.1、8.2.8.1、9.2.1.1、9.2.2.1)	○ (SR 7.7)

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.PS-07	・組織は、不正なソフトウェアのインストール及び実行を防止する。	L1_1_a-SYS L1_1_b-SYS	<High-Advanced> ・組織は、不正なソフトウェアが検知された場合に、対象ソフトウェアの起動を防止するツールを使用する。 ・組織は、ブラックリスト（禁止ソフトの一覧）も含めたリスト管理により、許可されていないソフトウェアのインストールを不可とする。 ・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・組織は、ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・産業用制御システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。	O/S	-	○ （下記に加えて、CM-07(02)、CM-07(05)）	○ （A.8.7、A.8.19）	-	○ （SR 3.2）
			<Advanced> ・組織は、自組織の情報システム及び産業用制御システム上でのユーザによるソフトウェアのインストールについて管理するメカニズムを導入し、管理する。 ・情報システム及び産業用制御システムは、システムの機能として実施可能な場合、起動を許可するソフトウェアを事前に登録するホワイトリスト方式により、登録されていないソフトウェアの起動を停止する。	O/S	○ （03.04.08 認可されたソフトウェア – 例外による許可 b）			○ （9.3.2.1）	
			<Basic> ・組織は、パソコン、サーバ及びスマートデバイスで利用を許可していないソフトウェアをすべて削除もしくは無効化するか、又は利用を許可するソフトウェア以外を自由にインストールできないようにする。 ・組織は、自組織の情報システム及び産業用制御システム上でのユーザによるソフトウェアのインストールに関するポリシーを確立し、ユーザに遵守させる。 ・IoT機器、サーバ等に接続するUSBメモリ等の外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能なUSBメモリを用いる等の対策を行う。 ・マルウェア対策ソフトウェアのパターンファイルを、ベンダーの推奨に従ってアップデートする。 ・情報システム及びそのソフトウェアを以下の状態に保つ。 - ライセンスが付与され、サポートされている。 - サポートが終了した場合に削除されるか、又はインターネットとの全てのトラフィックを遮断することで適用範囲から削除される。 - 可能であれば、自動アップデートが有効化されている。 ・産業用制御システムにおいて、パッチおよび更新を展開する際には、組織固有の追加要件を考慮する。 ・産業用制御システムにおいて、パッチ適用が不可能、あるいは可用性または安全性を著しく侵害する可能性がある資産については、代替管理策（セグメンテーション、監視など）を適用し、記録する。	O/S	-	○ （CM-07）		○ （9.2.1.1、9.3.1.1）	
CPS.PR.PS-08	・組織は、脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	L1_1_a-SYS L2_1_a_ORG L2_1_c-SYS L3_3_d-SYS L3_1_a-SYS L3_3_a-SYS	<High-Advanced> ・組織は、脆弱性修正状況を管理するための自動化されたメカニズムを導入し、管理する。	O	-	-	○ （A.8.8）	○ （9.4.3.1）	-
			<Advanced> ・組織は、定期的なパッチ適用及び緊急のパッチ適用を、脆弱性管理計画でそれぞれ定められた期限内に実施する。 ・組織は、パッチ適用中のIoT機器、サーバ等の動作により、他のソフトウェアアプリケーションやサービスの機能への影響が出るかどうかを調査やテストを通じて明らかにして、受容できるリスクを定める。 ・組織は、修正内容の有効性と副次的な悪影響の可能性についてテストを行った上で脆弱性の修正を実施し、当該修正を構成管理として管理する。	O	○ （下記に加えて、03.11.02 脆弱性の監視およびスキャン b）	-		○ （9.4.2.1、9.4.4.1、12.2.9.1）	-
			<Basic> ・組織は、様々な脆弱性を把握・評価し、リスク対応策の優先順位付け、テスト、及び実施を行うための脆弱性管理計画を策定するとともに、当該計画に沿って構成要素の脆弱性の修正を実施する。 ・脆弱性管理計画の策定にあたっては、脅威又は脆弱性の深刻さ、及び修正措置の適用に関わるリスク等を考慮する。	O	○ （03.12.02 実施計画およびマイルストーン a、03.14.01 欠陥の修正 a）	-		○ （12.2.9.1）	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみ適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.PS-09	・組織は、IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	L1_1_a_SYS L2_1_a_ORG L2_1_c_ORG L2_1_c_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> ・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な変更または不正な変更がないか確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。	0	-		-	○ (9.3.1.1)	-
			<Advanced> ・利用する情報システム及び産業用制御システムのOS、ソフトウェア及びハードウェア等について、以下のいずれかを適用する。 - 全てのOS、ソフトウェア、及びハードウェアについて、サポートのあるもの又は必要なセキュリティ機能を備えたものを利用する。 - やむを得ずサポート切れ又は必要なセキュリティ機能を備えていないものを利用する場合(例えば、代替システムを調達する必要があり、直ちに更改できない場合は、更改計画を策定した上で、更改するまでの間、脆弱性悪用のリスクを低減する対策を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画を策定し、計画に沿って実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。	0	-	○ (下記に加えて、MA-03、SA-10、SI-07)	-	○ (9.4.2.1、9.4.3.1、9.4.4.1、9.4.5.1)	-
			<Basic> ・利用している情報システムの機能又は設定に関して、検出された脆弱性の深刻度、当該脆弱性を悪用した攻撃が起こる蓋然性、アップデート適用対象となる機器等のインターネットへの露出状況を踏まえ、対応期限を設定の上アップデートを適用する。 ・やむを得ずアップデートが適用できない場合(例えば、動作検証に一定期間を要し、期限内にアップデートが完了しない場合)は、脆弱性管理計画に反映の上、アップデート適用までの間、以下のいずれかにより脆弱性悪用のリスクを低減する対策を実施する。 - 脆弱性悪用の対象となる機能を無効化する。 - ペンダーが推奨する回避策を実施する。 - 対象となる情報機器を適用範囲内のネットワークから分離する。 - 対象となる情報機器と適用範囲内のネットワークとの通信を監視し、当該脆弱性を悪用する不正な通信を遮断する機器又はソフトウェアを導入する。	0	○ (03.11.02 脆弱性の監視およびスキャン b、03.14.01 欠陥の修正 b、03.14.02 悪意のあるコードからの保護 b)	○ (CM-11、SI-02)	-	-	-
CPS.PR.PS-10	・組織は、自組織のIoT機器、サーバ等に対する保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	L1_1_a_SYS L2_1_a_ORG L2_1_c_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced><Advanced>共通 ・組織は、遠隔保守のための接続の確立と実施に関するポリシーとプロシージャを文書化し、その内容により実施する。 ・組織は、遠隔保守を実施する際には組織の定めるネットワークアクセスに求める認証を実施するとともに、遠隔保守が完了したらセッションとネットワーク接続を確実に終了する。	O/S	○ (03.07.05 非ローカルメンテナンス a)	-	○ (A.7.13)	-	-
			<Basic> ・組織は、遠隔保守の実施に当たっては、実施計画を策定し・合意した上で実施し、実施結果を確認する。 ・組織は、実施した遠隔保守の実施記録を保管する。 ・組織は、メンテナンス要員が付添いなしで情報システム及び産業用制御システムのメンテナンスを行う場合に、その要員が必要なアクセス権限を有することを確認する。 ・組織は、必要なアクセス権限を持たない要員によるメンテナンス活動を監督するのに必要なアクセス権限と技術的能力を有する組織の要員を指定する。	0	-	-		-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.PS-11	・組織は、セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、継続的にログを記録し、レビューする。	L1_1_a_SYS L1_3_a_SYS L2_1_b_ORG L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> ・ゼロトラストアーキテクチャで必要となるデータを記録するよう、ログ生成元の設定を行う。 ・組織は、セキュリティ専門の24時間365日監視により収集したログを、分析自動化ツール等を利用してことで効率的に分析する。 ・情報システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入する。 ・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からのログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。	O/S	○ (下記に加えて、03.01.07 最小特権 – 特権機能 b、03.03.02 監査記録の内容 b)		○ (A.8.15)	○ (8.2.9.1、12.2.1.1)	○ (SR 2.8、SR 2.11)
			<Advanced> ・情報システムについて、全てのオペレーティングシステム、アプリケーション及びサービス（クラウドサービスを含む）でログを生成するよう設定する。 ・生成したログを組織のログ基盤システム及びサービスと安全に共有するよう、ログ生成元の設定を行う。 ・ログが非標準または使用できない産業用制御システムについては、当該システムと他の資産間のネットワークトラフィックおよび通信を収集する。 ・情報システム及び産業用制御システムは、ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。 ・収集したログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。 ・組織は、サービスプロバイダーにより取得される監査ログが、サービスの利用者の活動、例外処理及びセキュリティインシデントを記録できており、適切な方式で保護されていることを確認する。	O/S	○ (下記に加えて、03.01.01 アカウント管理 e、03.03.03 監査記録の生成 a,b、03.03.05 監査記録のレビュー、分析、および報告 a,b)			○ (12.2.1.1、12.2.4.1)	○ (SR 2.8、SR 3.9)
			<Basic> ・組織は、リスクマネジメントに係る戦略やアセスメントの結果等から、セキュリティインシデントを検知するために収集することが望ましいログを決定する。 ・組織は、収集対象として定めたログが、対象システム上で誰がいつ何を行ったかを識別可能な形で取得できることを確認する。 ・組織は、産業用制御システムのパフォーマンスにログの取得作業が与える影響が許容範囲内であることを確認する。	O	○ (03.03.01 イベントロギング a,b、03.03.02 監査記録の内容 a)	○ (AU-02、AU-03、AU-06、AU-11、AU-12)		○ (12.2.1.1、12.2.4.1、12.2.5.2)	○ (SR 2.8、SR 2.12)
CPS.PR.PS-12	・組織は、IoT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする。	L2_3_b_DAT	<High-Advanced> ・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。	O	-	○ (SC-03)	○ (A.7.14、A.8.10)	-	○ (SR 4.2)
			<Advanced><Basic>共通 ・組織は、サーバ、IoT機器、産業用制御システム、会社支給のパソコン、スマートデバイス及び外部記憶媒体の廃棄時(リース終了時を含む。)に、データを復元できないよう抹消処理を行う（ディスクのフォーマットは、データを復旧される可能性があるため不十分）。なお、汎用的な抹消手法が適用できない機器については、物理破壊等、機器の特性に応じた方法で復元不能状態にする。 ・組織は、サーバ、IoT機器、産業用制御システム、会社支給のパソコン、スマートデバイス及び外部記憶媒体について、記憶領域を抹消処理した記録を保管する。 ・組織は、自組織のIoT機器やサーバ等を廃棄するプロシージャを定め、その当該プロシージャに従って廃棄を実施するとともに、適切に実施できたことを確認する。	O	○ (03.08.03 媒体のサニタイズ)	○ (CM-07、SA-10、SC-39)		-	

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみ適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.IR-01	・組織は、ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等して、認可されていないアクセス及び使用からネットワーク及び環境を保護する。	L1_1_c_SYS L3_a_SYS	<High-Advanced> ・組織は、各リソースに対するネットワーク経由のアクセスを必要最小限に制限するため、ゼロトラストアーキテクチャを導入する。 ・組織は、重要度の高い産業用制御システムのネットワークを、重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・情報システム及び産業用制御システムは、自組織のシステムを構成するネットワークの内部における境界について通信をモニタリングし、制御する。 ・機密性の高いデータを取り扱う自組織の情報システムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。 ・組織は、共有システム資源を介した、不正な予期せぬ情報の転送を防止する。 ・情報システム及び産業用制御システムは、許可されていないコンポーネントのネットワークアクセスが検知された場合に、そうしたコンポーネントによるネットワークアクセスを無効にする、それらのコンポーネントをネットワークから切り離す等の一次対処を実施し、システム管理者に通知する。	O/S	○ (下記に加えて、03.01.12 リモートアクセス c)			○ (8.2.1.1、8.2.7.1、13.2.2.1)	○ (SR 5.1、SR 5.2)
			<Advanced> ・情報システム及び産業用制御システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・情報システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする。 ・利用中のOSが対応していない場合を除いて、情報システムを構成するパソコン及びサーバにおいて、ソフトウェアファイアウォールを有効化する。 ・組織は、社外公開サーバ及び重要な機密情報を扱うサーバについて、それぞれ専用のネットワークセグメントに設置し、セグメント内外のアクセスを必要最小限に限定する。 ・情報システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・組織は、公開された新たな攻撃動向、マルウェア挙動情報や悪性IP アドレス／ドメイン情報などの情報（外部インテリジェンス）を収集し、必要に応じて危険性の高いIPアドレス等への通信を遮断する等の対応を実施する。 ・組織は、インターネットなどの外部ネットワークと社内ネットワークの中間に内部ネットワークへのアクセスを隔離されたネットワーク上のセグメント（DMZ: 非武装地帯）を構築する。 ・組織は、自組織外部に向けた大量のデータ通信を検知し、必要に応じてそのような通信の実施を制限する。	O/S	○ (下記に加えて、03.13.01 境界保護 b)	○ (下記に加えて、AC-04、SC-04)	○ (A.8.20、A.8.22)	○ (8.2.1.1、8.2.7.1、8.4.2.1、13.2.2.1)	○ (SR 1.13)
			<Basic> ・組織は、全てのファイアウォール(又はファイアウォール機能を持つネットワーク機器)について、データフロー制御ポリシーに基づき以下を実施する。 - インバウンド通信に関するファイアウォール・ルールを定める。 - 許可されていないインバウンド通信を遮断する。 - 不要になったファイアウォール・ルールを速やかに削除又は無効化する。 ・ファイアウォール・ルールの変更をインターネット経由で行う場合、多要素認証を適用するか、又は信頼できるIPアドレスにアクセスを制限する。 ・既知の悪意のあるドメインへのアクセスを遮断するため、承認済みのDNSサービスのみを利用するようプラットフォームを設定する。 ・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する。 ・組織は、産業用制御システムにおいて、適用可能な場合、制御システムのネットワークを情報システムとのネットワークから論理的あるいは物理的にセグメント化する。 【参考】他のネットワークと物理的に離れた環境においては物理的なセグメント化を実施する、他のネットワークと物理的に近接した環境では、対策のコスト等も考慮して論理的なセグメント化を実施する等の対応が可能である。	O/S	○ (03.01.03 情報フローの実施)	○ (AC-03、SC-05、SC-07)		○ (8.2.1.1、8.2.7.1、13.2.2.1)	○ (SR 5.1、SR 5.2)
CPS.PR.IR-02	・組織は、無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	L1_1_a_SYS L1_1_c_SYS L2_3_b_SYS L2_3_d_SYS L3_1_a_SYS	<High-Advanced> ・組織は、自組織の利用するシステムが設置されている施設に職員が常駐しない場合には、自動消火機能を導入する。	O	-	○ (下記に加えて、PE-18)	○ (A.7.5)	-	-
			<Advanced> ・組織は、無停電電源装置等により自組織のIoT機器、サーバ等が設置されているエリア内の機器の安定な稼働を維持する。 ・組織は、独立した電源等により稼働する消火及び火災検知のための装置やシステムを導入し、維持する。 ・組織は、閉止弁や遮断弁を用意し、自組織のIoT機器、サーバ等が設置されているエリアを水漏れ等の被害から保護する。	O	-	○ (下記に加えて、PE-09、PE-10、PE-11)	○ (A.7.5、A.7.8、A.7.11)	○ (13.2.2.1)	-
			<Basic> ・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定めた許容レベルに保つ仕組みを導入する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定期的にモニタリングする。 ・組織は、データを伝送する又は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を傍受、妨害又は損傷から保護する。	O	-	○ (CP-02、PE-12、PE-13、PE-14、PE-15)	○ (A.7.5、A.7.8、A.7.11、A.7.12)	-	-
CPS.PR.IR-03	・組織は、平時及び有事において、システム及びサービスの継続稼働に関する要件を達成するための仕組みを実装する。	L1_1_c_SYS L2_1_d_SYS L3_3_c_SYS	<High-Advanced><Advanced>共通 ・システム及びインフラにおいて、単一障害点が生じないよう設計する。 ・負荷分散を用いて、処理能力を向上させるとともに、システムの安定性を高める。	O	-	○ (CP、IR、SA-08、SC-24、SC-39)	○ (A.5.30、A.8.14)	○ (13.2.2.1)	○ (SR 7.1)
			<Basic> (該当なし)	-	-	-	-	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.PR.IR-04	・組織は、サイバー攻撃（例：ランサムウェア、サービス拒否攻撃等）を受けた場合でも、攻撃による影響を最小限に抑え、重要な機能を維持できるよう、十分なリソース（例：ヒト、モノ、システム）を確保する。	L1_1_c_SYS L2_1_d_SYS L3_3_c_SYS	<High-Advanced> ・制御機器やIoT機器において、ファームウェア等のロールバック機能が備わっていない場合、予備の制御機器やIoT機器を備えておくことが望ましい。 ・情報システム及び産業用制御システムは、組織が定めたセキュリティ対策を実施することによって、組織が定めたタイプのサービス拒否攻撃、またはそうした情報の情報源への参照のサービス拒否攻撃による影響から保護する、あるいはそうした影響を最小限に抑え、縮退運転を実施する機能を提供する。	O/S	-	○ (下記に加えて、CP-06、CP-07、CP-08)	○ (A.5.30、A.8.14)	○ (8.2.4.1、13.2.2.1)	○ (SR 7.1)
			<Advanced> ・組織は、冗長化されたストレージや電源等の高い可用性を有するコンポーネントを用いて、システムの安定性を高める。 ・組織は、将来のリソース需要の推定結果に応じて、リソースを拡張する。 ・情報システム及び産業用制御システムは、予備の容量／帯域幅／その他の予備リソース（ヒト／モノ／システム等）を管理して、大量の情報を送りつけるタイプのサービス拒否攻撃による影響を最小限に抑える。例えば、攻撃を受けているシステムが提供するサービスを、可用性の水準維持等の理由により停止できない場合、重要な機能を継続するため、以下のような対策をとる必要がある。 - 待機している予備システムへの自動的、あるいは、人手を介した移行 - ネットワークアクセスからの攻撃を受けたシステム構成要素の、自動的あるいは人手を介した隔離 ・組織は、 (a) 情報システムに対するサービス妨害攻撃の兆候を発見するための組織が定めた、モニタリングツールを使用する (b) 組織が定めた情報システム及び産業用制御システムのリソースをモニタリングして、効果的なサービス妨害攻撃を阻止するための十分なリソースが確保されているかどうかを判断する。	O/S	-		○ (A.5.30、A.8.6、A.8.14)	○ (13.2.2.1)	
			<Basic> ・組織は、情報システム及び産業用制御システムに要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならない、また、将来必要とする容量・能力を予測する。	O	-	○ (PM-03、PM-09)		○ (13.2.2.1)	-
CPS.DE.CM-01	・組織は、セキュリティ事象を適切に検知できるよう、ネットワーク及びネットワークサービスを監視する。	L1_1_a_SYS L1_1_b_SYS L2_1_b_ORG L2_3_b_SYS L2_3_c_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> ・組織／システムは、定期的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い（通信）を検知できるようにする。 ・情報システム及び産業用制御システムは、モバイルコードの使用を管理し、監視する。 ・情報システムは、音声や映像の伝送に利用されるプロトコル（例：VoIP）の使用を管理し、監視する。	O/S	-	○ (下記に加えて、CM-03)	○ (下記に加えて、A.8.21)	○ (6.3.2.1)	○ (SR 2.4)
			<Advanced> ・有害な事象を検知するため、DNS、BGP等のネットワークサービスを監視する。 ・有害な事象を検知するため、実際のネットワーク通信をベースラインと比較し、逸脱を検知する。 ・ネットワーク通信を監視し、ゼロトラストの観点からセキュリティ態勢の変化を特定する。 ・マルウェア、フィッシング、データ漏えい及び不正持ち出し、その他の有害な事象を検知するため、メール、ウェブ、ファイル共有、コラボレーションサービス等の一般的な攻撃経路を監視する。 ・組織は、産業用制御システムと情報システムとの境界において通信をモニタリングし、制御する。 ・組織は、特定の送信元、あるいは多数の送信元からの大量の通信がないかをシステムの外部境界及びシステム内の主要な内部境界にてモニタリングし、必要に応じて、特定IPアドレスからの通信を遮断するなど、適切な対応を実施する。	O/S	○ (下記に加えて、03.13.01 境界保護 a)			○ (6.3.2.1、13.2.2.1)	○ (SR 1.13、SR 5.2)
			<Basic> ・組織は、社内外ネットワークの境界又は端末において、インターネットから社内への通信及び社内から不正なサーバへの通信の双方について、不正アクセスをリアルタイム検知・遮断する仕組みを導入する。 ・不正アクセスをリアルタイム検知・遮断する機能を有したネットワーク機器又はネットワークサービスについて、異常時に以下の対応を行う仕組みを導入する。 - アラートが速やかに発報されること。 - インシデントの速報レポートが作成され、通知されること。 ・組織は、情報システムの外部境界（管理されたインターフェース）において、承認されていないモノ・システム等への通信や、適切でない内容を含む通信を検知するため、通信をモニタリングし、制御する。 ・組織は、自組織外部に向けた大量のデータ通信を検知し、必要に応じてそのような通信の実施を制限する。	O/S	○ (03.14.06 システム監視 c)	○ (AC-02、AU-12、CA-07、SC-05、SC-07、SI-04)	○ (A.8.16)	○ (6.3.2.1)	-
CPS.DE.CM-02	・組織は、セキュリティ事象を適切に検知できるよう、IoT機器、サーバ等のハードウェア及びソフトウェアの稼働状況、並びにネットワーク接続状況等を監視する。	L1_1_a_COM L1_1_a_SYS L1_1_b_COM L1_1_c_COM L2_3_b_ORG L2_3_b_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> ・組織は、情報システムだけでなく、産業用制御システムやIoT機器も含めて、セキュリティ状況のモニタリングの範囲とすることが望ましい。 ・組織は、システム内に許可されていないハードウェア、ソフトウェア、ファームウェアが存在する場合に、それを自動で検知するメカニズムを使用する。	O	-	○ (下記に加えて、AC-04、CM-03、SI-07)	○ (A.8.16)	○ (6.3.2.1、7.2.3.1、12.2.1.1、13.2.2.1)	-
			<Advanced> ・導入されたソフトウェアについて、定めた標準構成・設定ルールからの逸脱が生じていないかを継続的に監視し、逸脱を検知する。 ・ハードウェア及びソフトウェアに対する改ざんの兆候を監視する。 ・ストレージ、電源、処理能力等のリソース使用状況を監視する。 ・情報システムは、パッチ未適用、マルウェア感染及び認可されていないソフトウェア等の問題を検知し、アクセスを許可する前に当該端末を修復用の環境へ移す。	O/S	○ (システム監視 a)			○ (6.3.2.1)	-
			<Basic> ・組織は、運用時に実施すべき対策（IoTデバイスの不正利用や盗難、パッチの適用、ログのチェック等）、IoT機器の状況を定期的に確認する。	O	-	○ (AU-12、CA-07、CM-06、CM-10、CM-11、SI-04)		-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.DE.CM-03	・組織は、セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容を監視する。	L1_1_a_SYS L1_1_b_SYS L2_3_c_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced><Advanced>共通 ・組織は、外部サービスプロバイダー及びシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスををモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。	O/S	-	○ (CA-07、PS-07、SA-04、SA-09、SI-04)	○ (A.8.16)	-	-
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.DE.CM-04	・組織は、セキュリティ事象を適切に検知できるよう、組織内外の要員による構成要素（モノ／システム等）へのアクセスや操作等の活動を監視する。	L1_1_a_SYS L2_1_b_ORG L2_3_c_SYS L3_4_a_PRO L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> ・組織は、ユーザアカウント型のおとりを含むデセプション技術について、その利用(アクセス)の有無を継続的に監視する。 ・情報システム及び産業用制御システムは、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。	O/S	-	○ (AC-02、AU-12、CA-07、CM-10、CM-11)	○ (A.8.16)	○ (8.4.2.1)	○ (SR 1.13)
			<Advanced> ・重要な機密情報を扱うシステムは、付与したアクセス権の運用/利用状況を監視する仕組みを提供する。 ・組織は、内部不正を低減するため、行動分析ソフトウェアを用いて異常なユーザの挙動を検知する。 ・組織は、外部サービスプロバイダが組織のシステムに対して実施する、遠隔及び現地での管理及び保守活動を監視する。 ・組織は、システムのアクセスログを監視し、異常なアクセスパターン及びアクセスの失敗を特定する。認証サーバのログについては、月1回以上の頻度でモニタリングを実施し、不審な認証試行を検知する。	O/S	○ (03.01.01 アカウント管理 e、03.14.06 システム監視 b)			-	-
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.DE.CM-05	・組織は、IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	L1_1_a_SYS L2_3_b_PEO L2_3_b_SYS L2_3_d_SYS	<High-Advanced> ・組織は、特に重要な資産を管理している範囲内での重要資産の位置や移動を追跡し、監視する。	O	-	○ (CA-07、PE-03、PE-06)	○ (A.7.4)	-	-
			<Advanced> ・組織は、警報システム、カメラ及び警備員を活用して、物理的環境を監視する。 ・組織は、錠、掛け金、蝶番、警報装置等の物理的なアクセス制御について、改ざんの兆候を監視する。 ・組織は、入退場日時及び入場者氏名を含めて、サーバの設置エリアの入退場記録を取得し、少なくとも6ヶ月間保管する。 ・入退室管理システム（例：カードリーダー）のログを監視し、通常と異なるアクセスパターン及びアクセスの失敗を特定する。 ・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。 ・組織は、自組織の保護すべき資産に直接アクセス可能なエリア（執務室等）において、自組織の担当者が来客に付き添って、来客の行動を監視する。 ・組織は、自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.PR.PS-02)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。	O/S	○ (下記に加えて、03.10.02 物理的アクセスの監視 a,b)			○ (6.4.1.1)	-
			<Basic> ・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来客に付き添うなどして入手による代替的な対策を実施する。 ・施設内の、一般の人がアクセスできない指定エリアに対するアクセスを制御するための、入退室管理対策を実施する。 ・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入退室時のログを保持する。	O/S	○ (03.10.07 物理的アクセス制御 b)				-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.DE.CM-06	・組織は、自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	L1_1_a_SYS L2_1_a_ORG L2_1_c_ORG L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced> ・組織は、自組織が管理する産業用制御システムの構成要素（IoT機器を含む）に対して、計画停止時等に脆弱性診断を実施し、自組織の所有するシステムに存在する脆弱性を認識し、一覧化する。 ・組織は、ツールを用いて脆弱性診断を行う場合、診断すべきシステムの脆弱性データベースをすぐに更新できる脆弱性診断ツールを使用することが望ましい。 ・組織は、脆弱性スキャンにおける検査対象の脆弱性（スキャン定義）を、定期的に、あるいは新たな脆弱性が特定・報告された場合に更新する。 ・組織は、指定された脆弱性スキャン活動に関して、対象システムのコンポーネントに対する特権的アクセスの許可制度を実施する。	O	-	-	○ (A.8.8)	○ (6.3.2.1)	-
			<Advanced> ・組織は、インターネットとの境界に設置されているネットワーク機器のOS及びファームウェアについて、CVSS 基本値 7.0以上の脆弱性の有無を定期的に確認する ・組織は、情報システム及びアプリケーションの脆弱性のスキャンを定期的に、あるいは、それらのシステム／アプリケーションに影響を及ぼす新たな脆弱性が確認され、報告された場合に実施する。 ・組織は、脆弱性スキャンにツールを用いる。以下を満たす標準的な手法を使用することによって、脆弱性管理プロセスの一部を自動化する。 - ブラットフォーム、ソフトウェアの欠陥及び誤った設定を列挙する - チェックリストとテスト手順をフォーマットする - 脆弱性による影響を評価する ・組織は、脆弱性スキャン等で得た情報を組織内の他のシステムの管理者と共有し、他の情報システム内の同様の脆弱性を把握する。 [参考] 脆弱性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の影響の大きさを評価する指標として、CVSS(IPAによる解説： https://www.ipa.go.jp/security/vuln/scap/cvssv3.html)を参考とすることが可能である。	O/S	○ (下記に加えて、03.11.02 脆弱性の監視およびスキャン a)	-		-	-
			<Basic> ・組織は、情報システム及びアプリケーションの脆弱性のスキャンを定期的 to 実施する。	O	○ (03.14.01 欠陥の修正 a)	-		-	-
CPS.DE.CM-07	・組織は、サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	L1_1_a_SYS L1_1_b_SYS L1_1_b_DAT L2_2_a_COM L3_3_d_SYS L3_3_a_DAT	<High-Advanced> ・組織は、データ入力に対する「ホワイトリスト」の概念を導入することで、インプットデータの出所を既知の信頼できるモノ、システム等と、そうしたインプットデータの許容できるフォーマットを指定する。 ・情報システム及び産業用制御システムは、通信セッションの真正性を保護する。	O/S	○ (03.13.15 セッションの真正性)	-	-	○ (11.2.16.1)	-
			<Advanced> ・情報システムは、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、当該IoT機器が自組織の業務において重要なものと認められる場合、機器間の相互認証が成功した後はじめて通信を開始することで、データの出所の把握を確実なものとする。	S	-	-	-	-	○ (SR 1.2)
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.DE.CM-08	・組織は、指示された動作内容と実際の動作結果を比較して異常の検知や動作の停止を行うIoT機器を導入する。 ・組織は、サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	L1_1_a_SYS L1_3_a_SYS L2_2_a_COM L2_2_a_SYS L3_3_d_SYS L3_3_a_DAT	<High-Advanced> ・エンドポイント（特に、多様な機能を有するIoT機器、サーバ等）において、マルウェアに対する振舞い検知型の検出・修復ソフトウェアを導入することで、未知の脆弱性を突く攻撃コードの検知を実施する。 ・情報システムは、IDS/IPSによる悪質コードの検知ロジックを自動的に更新する。 ・IoT機器あるいはそうした機器を含んだシステムが、通常期待される結果とは異なる結果をもたらすような特定の攻撃（例：コマンドインジェクション）に備え、ソフトウェアプログラムまたはアプリケーションからの出力情報を検証して、期待される内容と一致しているかを確認する。	S	-	-	○ (A.8.7)	-	○ (SR 3.2)
			<Advanced> ・メールによるマルウェア感染を防止するため、メールゲートウェイ、メールサーバ等でマルウェアチェックを実施する。 ・外部から受け取ったファイルについて安全性を確認するため、マルウェア対策ソフトのリアルタイムスキャンを実行する、又は仮想環境上で安全性を確認する仕組みを整備する。 ・エンドポイント（IoT機器、サーバ等）において、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。 ・特に、機能が限定されているIoT機器において、ホワイトリスト型のマルウェア対策を実施することを考慮する。 ※ 特にIoT機器や制御機器においては、マルウェア対策ソフトが利用可能なOSが使用されているとは限らないケースがある。組織は、調達時等に導入する機器がマルウェア対策ソフトに対応できるものかを確認し、対応可能なものを選定することが望ましい。マルウェア対策ソフトに対応する機器を調達することが困難な場合、ネットワーク上でマルウェアを検知する仕組みを導入・強化する等、代替的な対策を実施することが望ましい。	S	-	-		○ (9.3.2.1)	
			<Basic> ・組織は、情報システム向けのネットワークに接続しているすべてのパソコン及びサーバにマルウェア対策ソフトウェアを導入し、機器ごとにマルウェア対策ソフトのスキャン範囲及び頻度を定め、スキャンを実行する。 ・情報システム及び産業用制御システムは、インプットとなるデータが指定されたフォーマットや内容に適合しているかどうかを確認することで、有効性を検証する。	O/S	○ (03.14.02 悪意のあるコードからの保護 a)	-		-	○ (SR 3.5)

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.DE.CM-09	・組織は、監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。	L1_1_a_SYS L1_3_a_SYS	<High-Advanced> ・システムに、既知で害のないテストケースを導入して、マルウェア検知メカニズムをテストする。 ・組織は、侵入検知モニタリングに用いているメカニズムを定期的にテストする。テストの頻度は、組織が使用するツールの種類と、ツールの設置方法等を考慮する。 ・組織は、最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的な監視活動の修正の必要性を判断する。	0	-	-	-	-	○ (SR 3.3、SR 6.2)
			<Advanced> ・組織は、自組織のシステムのモニタリング活動が、組織のリスクマネジメント戦略と、リスク対応のためのアクションの優先順位に適合しているかどうかを定期的に確認するプロシージャを定め、運用する。 ・組織は、ネットワーク機器やエンドポイントからのセキュリティに係る情報の相関分析を行うのに合わせて、誤検出や検出漏れの割合を算出し、定期的に検知メカニズムの妥当性を確認する。	0	-	-	-	-	○ (SR 6.2)
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.DE.AE-01	・組織は、潜在的なセキュリティ事象について分析を行い、当該事象の内容を把握する。	L1_1_a_SYS L3_3_d_SYS L3_1_a_SYS L3_3_a_SYS	<High-Advanced><Advanced>共通 ・組織は、既知の悪意ある活動及び不審な活動を検知するため、セキュリティ情報イベント管理（SIEM）等のツールを用いてログイベントを継続的に監視する。 ・組織は、自動化による監視が十分に行えない機器やシステムについて、ログイベントを定期的に手動で確認する。 ・サイバーセキュリティに関するソフトウェアを用いてアラートを生成し、セキュリティオペレーションセンター（SOC）、インシデント対応担当者及びインシデント対応ツールに提供する。 ・情報システムは、検知の仕組みにより、確認されたインシデントを自動的に報告する。 ・組織は、ログ分析ツールを用いて、分析結果に関するレポートを生成する。 ・組織は、インシデント対応担当者及びその他の認可された要員が、ログ分析結果に常時アクセスできるようにする。	O/S	○ (03.03.05 監査記録のレビュー、分析、および報告a)	○ (AU-06、CA-07、IR-04、SI-04、PM-15、PM-16)	○ (A.8.15)	○ (6.3.2.1、12.2.7.1)	○ (SR 6.2)
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.DE.AE-02	・組織は、セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。	L2_1_a_ORG	<High-Advanced> ・組織は、IDS,IPS,SIEMといったセキュリティ装置等のポリシーチューニング（適用シグネチャ管理）と維持管理を行う。 ・組織は、自組織でセンサー機器でのカスタムシグネチャを脅威情報から作成する。 ・組織は、可能な場合、自組織に悪影響を及ぼす可能性の高いセキュリティ事象を適切に検知するため、<Advanced>で提示している機器のログに加え、IoT機器等のエッジデバイスのログも収集し、分析することが望ましい。	0	-		-		-
			<Advanced> ・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。なお、相関分析の対象には、他組織とデータを連携する部分のログも含めることが望ましい。 - モニタリングするシステムの範囲をどこまでとするか - どのような機器のログを収集し、分析するか ・組織は、資産台帳の情報を担当者に安全に共有し、検知の仕組みや運用プロセスに組み込む。 ・組織は、最新の脅威インテリジェンスを担当者に安全に共有し、検知の仕組みや運用プロセスに組み込む。 ・組織は、最新の脅威インテリジェンスをログ分析ツールへと連携させることにより、検知精度を向上させるとともに、脅威主体、その手法及び侵害の痕跡を特定する。 ・組織は、自組織に悪影響を及ぼす可能性の高いセキュリティ事象を適切に検知するため、主に以下のような情報システムを構成する機器のログを監視し、リアルタイムに分析を行うことが望ましい。多種多様なログの取り扱いが必要になるため、ログを正規化し、同一のデータベースに格納したり、SIEMを利用したりして、効率的な分析を実現する必要がある。取得可能な場合はネットワーク下の情報も扱うことが望ましい。 - ファイアウォールなどのネットワーク装置からのログやネットワークフロー - IPS/IDSなどのセキュリティ装置からのログ - Web サーバなどのアクセスログ - ActiveDirectoryやDNSなどの各種システムからのログ - ユーザ利用端末に関するログ [参考] セキュリティ対応組織(SOC/CSIRT)が実施する各種業務の内容については、「セキュリティ対応組織（SOC/CSIRT）の教科書 ～X.1060フレームワークの活用機能・役割・人材スキル・成熟度～」(ISOG-J, 2025年, 10月)等を参照することが望ましい。	0	○ (03.03.05 監査記録のレビュー、分析、および報告c)		○ (AU-06、CA-07、IR-04、IR-05、IR-08、PM-16、RA-03、SI-04)		○ (A.5.7)
			<Basic> ・組織は、ファイアウォールやエンドポイントセキュリティ製品等の通知を個別に確認することで、自組織に悪影響を及ぼすようなセキュリティ事象を特定する。	0	-	-	-	-	

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.DE.AE-03	・組織は、関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。	L1_3_a_COM	<High-Advanced> ・組織は、発生したセキュリティ事象の形態、規模及び費用を定量化及び監視できるようにする自動的なメカニズムを備える。 ・組織は、セキュリティ事象発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を自組織のセキュリティ対応組織(SOC/CSIRT)にて実施する。 ・組織は、攻撃者のプロファイル（所属組織、組織の活動目的など）に関する仮説を構築する。	O/S	-	○ (PM-09、PM-11、PM-18、PM-28、PM-30)	-	-	-
			<Advanced> ・セキュリティ事象の影響の大きさ及び影響範囲を、担当者が自ら推定する。 ・組織は、SIEM等のツールを用いて、セキュリティ事象の影響の大きさ及び影響範囲を推定し、その推定結果を見直して、より正確にする。 ・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、共有することによって、当該セキュリティ事象の全容を把握する。 ・組織は、セキュリティ事象発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を外部のセキュリティベンダー等に依頼する。	O	-		-	-	-
			<Basic> (該当なし)		-	-		-	-
CPS.DE.AE-04	・組織は、セキュリティ事象がインシデントに該当するか否かの判定基準を定め、当該基準を満たす場合にインシデントの宣言を行う。	-	<High-Advanced> ・組織は、セキュリティ事象の追跡と、事象に関係する脅威収集・脆弱性等の情報の収集及び分析を支援する自動化されたメカニズムを使用して、セキュリティ事象の分類（トリアージ）等に活用する。	O	-	○ (IR-04、IR-08)	○ (A.5.25)	-	-
			<Advanced> ・組織は、自社におけるセキュリティインシデントのレベル及びレベルごとの対象範囲を定め、役員、従業員、派遣社員及び受入出向者に周知する。 ・組織は、認証サーバのログのモニタリングにより不審な認証試行を検知した場合、又は不正アクセスをリアルタイム検知・遮断する仕組みを有したネットワーク機器もしくはサービスからのアラートを受け取った場合は、あらかじめ定めたセキュリティインシデントのレベル及び対象範囲に基づき、どのレベルのインシデントに該当するかを分析し、判断する。	O	-			-	-
			<Basic> ・組織は、ネットワーク機器のログ及びアラートを分析し、セキュリティ担当部署の担当者又は管理者により不審な事象が発見された場合に、定めた判定基準を基に、当該事象それがセキュリティインシデントに該当するか否かを判断する。 ・組織は、セキュリティ事象がインシデントに該当するか否かを判断する際に、産業用制御システム固有の事象や異常を考慮に入れる。 ・組織は、当該セキュリティ事象のもたらす影響の大きさを考慮し、報告義務のあるインシデントを定める。 [参考] セキュリティ事象の影響の大きさを測るための尺度を検討する場合、SP 800-61 Rev.3 (NIST, 2025年)等を参照することが出来る。	O	-			-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみ適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.RS.MA-01	・組織は、セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	L1_3_a_PEO L1_3_a_PRO L1_3_b_PRO L1_3_c_PRO L2_1_a_PRO L2_1_b_PRO L2_1_c_SYS L2_1_d_SYS L2_2_a_PRO	<High-Advanced> ・組織は、設定の不正な変更や、システム権限の不正な昇格等の、セキュリティ関連の変更が不正に行われた場合の検知能力を、組織のインシデント対応能力に組み入れる。 ・組織は、特定の種類のアラートが発生した場合に、組織のチケット管理システムにおいてチケットを自動的に作成・割り当てる仕組みを整備し、その運用手順を定める。 ・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、サプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するテストを実施する。 [参考] サプライチェーンにおけるセキュリティインシデントには、例えば、システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害等がある。	O	-	○ (CP-01、CP-02、IR-01、IR-08、PL-02、SA-04、SA-09、SR-02、SR-03、SR-08)	○ (A.5.24)	○ (12.2.8.1)	-
			<Advanced> ・組織は、インシデント対応における組織及びサプライヤの役割と責任を明確にし、文書化する。 ・組織は、Basicで定めたセキュリティ運用プロセスに加えて、以下をプロセスに含める。 - インシデントの状況・対応内容・証拠等を追跡・記録する - 外部組織等に対して、インシデント発生の実事と対応状況に関する報告をする必要があるかどうかを判断する。 ・組織は、インシデント対応を追跡・管理するための仕組み（チケット管理システム等）を整備し、侵害の痕跡を検知した際に、手動で起票・担当割り当てを行う手順を定める。 ・組織は、インシデント対応要件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、自組織と外部サービスプロバイダーとの間で連携を要するインシデント対応プロセスをテストする。	O	-			○ (12.2.8.1)	-
			<Basic> ・組織は、定めたセキュリティインシデントへの対応手順を、インシデント対応計画として文書化し、自組織のステークホルダーに周知する。 ・産業用制御システムを保有する組織は、インシデント対応計画を策定する際、産業用制御システム固有の安全および封じ込めに関する事項を考慮する。 ・セキュリティインシデントの報告フォーマットを整備する。 ・組織は、セキュリティインシデントの発生時に利用するセキュリティ運用プロセスを策定し、運用する。当該プロセスは、発見報告・初動・調査対応・復旧・最終報告の一連の対応フェーズに沿って構成し、下記を例とする内容を含むことが望ましい。 - インシデントの報告を受けた者が、どのような対応をするのか、あるいはより上位に報告するのかの判断基準 - 緊急時の指揮命令と対応の優先順位の決定 - インシデントへの対応（インシデントレスポンス） - インシデントの影響と被害の分析 - 情報収集と自社に必要な情報の選別 - 社内関係者への連絡と周知 - 外部関係機関との連絡 ・システム（特に産業用制御システム）は、IoT機器、サーバ等に異常（誤動作等）が発生した場合に、緊急停止、管理者へのアラート通知等のフェールセーフのための対応を実施する。 [参考] セキュリティインシデント発生時の対応手順の検討において、「インシデントハンドリングマニュアル」(JPCERT/CC, 2021年)、SP 800-61 Rev.3 (NIST, 2025年)、「インシデント対応マニュアルの作成について」(JPCERT/CC, 2015年)を参照することが可能である。	O/S	○ (03.06.01 インシデント処理、03.06.05 インシデント対応計画 a)		○ (8.2.4.1、12.2.2.1、12.2.8.1)	○ (SR 3.7)	
CPS.RS.MA-02	・組織は、セキュリティインシデントとして報告された事象について、誤検知や重複報告でないことを確認し、インシデントとしての妥当性を確認する。	L1_3_a_PEO	<High-Advanced><Advanced>共通 ・組織は、インシデント報告を初期確認し、それがセキュリティ事象に該当し、インシデント対応が必要であるか否かを判断する。 ・組織は、進行中のすべてのセキュリティインシデントの状況を把握し、その妥当性を確認する。	O	○ (03.06.02 インシデントの監視、報告、対応支援 b)	○ (IR-04、IR-05、IR-06)	○ (A.5.25)	○ (12.2.8.1)	-
			<Basic> (該当なし)	-	-	-	-	-	

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.RS.MA-03	・組織は、検知されたセキュリティインシデントを、影響度の大小や侵入経路等に基づき分類し、優先順位を付ける。	L1_3_a_PEO	<High-Advanced> ・組織は、セキュリティ事象の追跡と、事象に関係する脅威収集・脆弱性等の情報の収集及び分析を支援する自動化されたメカニズムを使用して、セキュリティインシデントの分類（トリアージ）等に活用する。	0	-	○ (IR-04、IR-05、IR-06)	-	○ (12.2.8.1)	-
			<Advanced> ・組織は、セキュリティインシデントの種類（例：データ漏えい、ランサムウェア、DDoS、アカウント侵害）に基づき、セキュリティインシデントをさらにレビューし、分類する。 ・組織は、セキュリティインシデントの範囲、想定される影響、重大度、緊急性及び被害を受けた対象の復旧目標等に基づいて、対応の優先順位を決定する。 ・組織は、進行中のセキュリティインシデントに対し、迅速な復旧の必要性と、攻撃者の動向監視やより詳細な調査の必要性とのバランスを考慮して、セキュリティインシデント対応方針を選択する。	0	-		-		-
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.RS.MA-04	・組織は、セキュリティインシデントが宣言された場合、取引先等の関係する他組織と連携し、あらかじめ定めた対応手順に基づきインシデント対応を実行する。	L1_3_b_PEO L1_3_c_ORG	<High-Advanced> ・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。	0	-	○ (下記に加えて、SR-06)	-	○ (12.2.8.1)	-
			<Advanced> ・組織は、情報システム及び産業用制御システムのユーザに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、組織のインシデント対応能力に不可欠な、インシデント対応支援リソース（ヘルプデスク、CSIRT等）を自組織に用意する。 ・各インシデントごとに、対応の責任者を定める。 ・組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する。 ・組織は、外部のインシデント対応委託先に対して、対応支援を要請する。 ・組織は、セキュリティインシデントにより第1の処理拠点の可用性が低下した場合に利用する代替処理拠点を定める。 ・組織は、同じ脅威に対する脆弱さを減らすために、一次処理拠点から離れた代替処理拠点を指定する。 ・組織は、自組織の一次処理機能が利用できない場合に、自組織が定める目標復旧時間内に、代替処理拠点により所定のオペレーションを移転・再開して、重要なミッション／業務機能を遂行できるようにするようサービス契約で規定する。 ・インシデント対応を支援するため、必要に応じて事業継続計画や災害復旧計画等を追加で実行する。	0	-		○ (A.5.26)		-
			<Basic> ・組織は、セキュリティインシデントを発見した場合、速やかにIPA、JPCERT/CC等の関係機関に報告し、対応の支援、発生状況の把握、手口の分析、再発防止のための助言等を受ける。	0	-	○ (CP-01、IR-01、IR-06、IR-07、IR-08、PM-31、RA-03、RA-05、RA-07、SA-04、SA-09、SR-02、SR-03、SR-05、SR-08)	-		-
CPS.RS.MA-05	・組織は、セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ（製品）に対して適切な対応を行う。	L1_3_b_COM	<High-Advanced><Advanced>共通 ・組織は、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。 ・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動及びインシデントの事後処理に関わる活動を調整する。その際、CPS.ID.AM-07、CPS.ID.AM-08にて記載している方法により、対応の対象となるモノを特定していることが望ましい。 ・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動及びインシデントの事後処理に関わる活動を調整する。ここで該当する活動の例として、生産システムにおけるセキュリティインシデント発生時に生産されたモノの回収等が挙げられる。	0	-	-	-	○ (12.2.8.1)	-
			<Basic> ・組織は、自組織の業種等を考慮して、事業継続計画又は緊急時対応計画の中に、インシデント発生後の生産したモノへの対応について記載するかを検討する。その際、事業継続計画又は緊急時対応計画は、必ずしもセキュリティインシデントを想定したものでない場合も許容されるものとする。	0	-	-	-		-
CPS.RS.MA-06	・組織は、セキュリティインシデントの特性及び復旧活動が業務に与える影響を考慮し、あらかじめ定めた基準に基づき復旧の開始を判断する。	L1_3_a_PEO	<High-Advanced><Advanced>共通 ・組織は、インシデント復旧活動によって、業務に支障が生じる可能性を考慮する。 ・組織は、既知及び想定されるインシデントの特性に対してインシデント復旧基準を適用し、インシデント復旧プロセスを開始すべきかどうかを判断する。	0	-	○ (IR-04、IR-08)	-	○ (12.2.8.1)	-
			<Basic> (該当なし)	-	-	-	-	-	

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.RS.AN-01	・組織は、セキュリティインシデントに関するデータ及びメタデータ（インシデント対応において実施した措置の履歴等を含む）を収集し、それらの完全性を確保するとともに、取得元及び取得時点等が参照可能な状態で保管する。	L1_1_a_DAT L3_1_a_DAT L3_3_d_SYS	<High-Advanced><Advanced>共通 ・組織は、証拠保全及び証拠管理の連続性（チェーン・オブ・カストディ）に基づき、関連するすべてのセキュリティインシデントデータ及びメタデータ（例：データの取得元、取得日時）を収集・保管し、その完全性を確保する。	0	○ (03.06.02 インシデントの監視、報告、対応支援 a)	○ (AU-07、IR-04、IR-06)	○ (A.5.28)	-	-
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.RS.AN-02	・組織は、セキュリティインシデント発生後に、根本原因を特定するためのデジタルフォレンジックを実施する。その際、調査過程の記録を改ざんされない形で保管する。	L1_1_a_DAT L3_1_a_DAT L3_3_d_SYS	<High-Advanced> ・情報システムが、重要なセキュリティインシデントに関する監査記録について処理するプロシージャを提供する。	0	-	○ (下記に加えて、AU-07)	○ (A.5.28)	-	-
			<Advanced> ・組織は、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シージャを規定する。 ・組織は、重要なセキュリティインシデントについて、発生後に下記の証拠を保全することが望ましい。 - インシデントの識別情報（発生場所／発生日時／対象となるモノのシリアル番号／ホスト名／MACアドレス／IPアドレス等） - 証拠を収集・処理したヒトの役職、氏名、連絡先、及び処理日時（タイムゾーンを含む） - インシデント対応担当者及び対応業務を行う者の行動記録 ・組織は、インシデント中に発生した事象の時系列の流れを整理するとともに、各事象に関与した資産及びリソースを特定する。 ・組織は、インシデントに直接的又は間接的に関与した脆弱性、脅威及び攻撃主体を特定する。 ・組織は、インシデントを分析し、根本的なシステム上の原因を特定する。 ・組織は、侵害の痕跡や継続的な不正活動の証拠を確認するために、ツール等を用いてインシデントの影響を受けている可能性がある他の対象を確認する。 ・組織は、攻撃者の挙動に関する情報を追加で得るために、デセプション技術の情報を確認する。	0	-			○ (12.2.8.1)	-
			<Basic> ・組織は、証拠となり得るデータを特定、収集、取得及び保存するためのプロシージャを定め、運用する。	0	-	○ (IR-04、IR-06、SI-02)			-
CPS.RS.AN-03	・組織は、セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。	L1_3_a_COM	<High-Advanced> ・情報システムは、発生した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自動的なメカニズムを備える。 ・組織は、攻撃者のプロファイル（所属組織、組織の活動目的など）に関する仮説を構築する。	0	-	○ (IR-04、IR-08、RA-03、RA-07)	-	-	-
			<Advanced> ・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、共有することによって、当該セキュリティインシデントの全容を把握する。	0	-		-	-	-
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.RS.CO-01	・組織は、セキュリティインシデント発生後の、組織内部及び外部への情報公表に関するルールを策定し、運用する。	L1_3_a_PRO L1_3_a_PEO	<High-Advanced><Advanced>共通 ・自組織において内部不正が発生した場合には、人事部門に通知する。 ・組織は、契約で定められた要件や組織で定められた通知手順に従い、インシデントについて取引先及び顧客に通知する。 ・組織は、インシデント対応計画で定められた基準及び経営層の承認に基づき、関係当局及び所管省庁にインシデントを通知する。 ・組織は、すべての機微情報を削除したうえで、攻撃者のTTPに関する情報を情報共有分析センター（ISAC）へ自主的に共有する。	0	-	○ IR-04、IR-06、IR-07、SR-03、SR-08)	-	○ (12.2.8.1)	-
			<Basic> ・組織は、セキュリティインシデント発生時における社内外組織(関係当局及び所管省庁を含む。)の連絡先及び報告・情報共有ルートを定める。 ・組織は、下記の内容を含むセキュリティインシデント発生後の情報公表時のルールを策定し、運用する。 - 公表する内容 - 情報公表の実施時期 - 情報公表の実施者 - 情報公表までの実施プロセス ・組織は、年1回以上及び社内外で重大なセキュリティインシデントが発生した際に、インシデント事例及びその対応策を社内部署へ共有する。	0	○ (03.06.05 インシデント対応計画 a)		○ (A.5.5)		-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.RS.CO-02	・組織は、定めたルールに基づき、組織内部の上位意思決定者及び関係する外部組織に対し、必要に応じてエスカレーションを行う。	L1_3_a_PEO	<High-Advanced><Advanced>共通 ・重大なインシデントの状況について、経営層に定期的に報告する。 ・指定された社内外の関係者と連携し、インシデントのエスカレーション又は重要度の引き上げの調整を行う。	O	○ (03.06.02 インシデントの監視、報告、対応支援 c)	○ (IR-04、IR-05、IR-06、IR-07)	-	○ (12.2.8.1)	-
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.RS.MI-01	・組織は、セキュリティインシデントによる被害の拡大を最小限に抑え、原因の除去又は影響の低減を行う。	L1_3_a_PEO	<High-Advanced> ・組織は、セキュリティインシデントによる被害を最小化するため、有事においてシステム管理者の権限を利用できるユーザを必要に応じて最小化させる。 ・組織は、セキュリティインシデントによる被害を最小化するため、システム管理者であっても、サーバの重要なサービスや保護されたプロセスを必要に応じて停止できないようにする。 ・組織は、セキュリティインシデントの対応プロセスを支援する自動化されたメカニズムを使用する。 ・情報システムは、侵害された端末を、修復用のVLANへ自動的に移行させる。	O/S	-	○ (IR-04)	-	○ (12.2.8.1)	-
			<Advanced> ・サイバーセキュリティ技術（例：アンチウイルスソフト）や、他の技術（例：オペレーティングシステム、ネットワークインフラ機器）に組み込まれたサイバーセキュリティ機能が、自動的に封じ込め対応を実行する。 ・第三者（例：インターネットサービスプロバイダ、マネージドセキュリティサービス事業者）が、組織に代わって封じ込め対応を実行できるようにする ・サイバーセキュリティ技術や、他の技術（例：オペレーティングシステム、ネットワークインフラ機器）に組み込まれたサイバーセキュリティ機能が、自動的に排除の処置を実行する。 ・インシデント対応の担当者が、排除の処置を手動で選択し実行できるようにする。 ・第三者（例：マネージドセキュリティサービスプロバイダー）が、組織に代わって排除の処置を実行できるようにする。	O/S	-		-		-
			<Basic> ・組織（あるいはその構成員）は、あらかじめ定められたプロシージャに従って、セキュリティインシデントを低減するためのアクション（例えば、システムのシャットダウン、有線/無線ネットワークからの切断、モデムケーブルの切断、特定の機能の無効化など）を実行する。	O	-		-	○ (8.2.5.1、12.2.8.1)	-
CPS.RC.RP-01	・組織は、自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急時対応計画の中にセキュリティインシデントを位置づける。	L1_3_a_PRO	<High-Advanced><Advanced>共通 ・組織は、情報システム、産業用制御システム及び関係するプロセスの管理者を含めて、有事における事業継続のための体制を構築する。事業継続に支障をもたらす事象が発生した際には、この体制が、運用を再確立するためのシステムの優先順位を決定する。 ・組織は、災害等と比較して被害状況が見えづらく事業継続計画の発動タイミングが不明確、インシデントの原因究明の重要性が高い等の特徴を有するセキュリティインシデントに特化した事業継続計画又は緊急時対応計画を策定し、運用する。 ・組織は、セキュリティインシデントに特化した事業継続計画又は緊急時対応計画を策定する際、組織全体の事業継続に係る方針と合致するような内容とすることを確実にする。	O	-	-	○ (A.5.29)	○ (13.2.1.1)	-
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.RC.RP-02	・組織は、インシデント後の運用方針を定めるにあたり、重要な業務機能及びサイバーセキュリティリスクマネジメントの結果を踏まえる。	-	<High-Advanced><Advanced><Basic>共通 ・組織は、インシデント後の運用方針を定めるにあたり、あらかじめ優先して継続・復旧すべき中核事業及び当該事業の運用に極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を踏まえる。	O	-	○ (IR-01、IR-08、PM-08、PM-09、PM-11)	-	-	-
					-		-		
CPS.RC.RP-03	・組織は、復旧フェーズへの移行が判断された場合、あらかじめ定めた復旧計画に基づき復旧を実行する。	-	<High-Advanced><Advanced>共通 ・組織は、復旧の責任を負うすべての担当者に対し、復旧対応の実施に必要な承認や権限を理解させる。 ・組織は、インシデント対応プロセスの実行中又は実行後に、復旧対応を開始する。 ・組織は、インシデント対応計画で定められた基準および利用可能なリソースに基づいて、復旧対応を選択する。 ・組織は、組織のニーズや利用可能なリソースを再評価した結果に基づき、復旧対応を適宜見直す。	O	-	○ (CP-10、IR-04、IR-08)	-	-	-
			<Basic> (該当なし)	-	-	-	-	-	-

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。

・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。

・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。

・対策例の記載に当たっては、主要なセキュリティ文書等（本表「参照ガイドライン」という形に示している）を参照している。

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 付属書A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.RC.RP-04	・組織は、バックアップ及びその他の復旧資産の完全性を、使用前に検証する。	L1_3_a_DAT	<High-Advanced><Advanced>共通 ・組織は、復旧に用いる資産を使用する前に、侵害の痕跡やファイルの破損、その他の完全性について問題がないかを確認する。	0	-	○ (CP-02、CP-04、CP-09)	-	-	-
			<Basic> ・組織は、バックアップ及びその他の復旧資産を使用する前に、対象、取得日時、バージョン等の基本情報を確認し、当該復旧資産を使用することが適切であることを確認する。	-	-	-	-	-	-
CPS.RC.RP-05	・組織は、復旧した資産の完全性を検証するとともに、システム及びサービスを復旧し、正常な運用状態であることを確認する。	-	<High-Advanced><Advanced>共通 ・組織は、本番利用に移行する前に、復旧した資産について、侵害の痕跡がないことを確認するとともに、インシデントの根本原因が解消されていること、又は残存リスクを評価し、必要な封じ込め若しくは補完的対策が講じられていることを確認する。 ・組織は、業務への影響やシステム分類の記録（サービス提供目標を含む）に基づき、重要なサービスが適切な順序で復旧されていることを確認する。 ・組織は、復旧されたシステムの性能を監視し、復旧が適切であることを検証する。	0	-	○ (CP-10)	-	-	○ (SR 7.4)
			<Basic> ・組織は、復旧後、システムの起動及び業務上必要な基本機能が正常に動作することを確認した上で、運用を再開する。	-	-	-	-	-	-
CPS.RC.RP-06	・組織は、あらかじめ定めた基準に基づき、インシデント復旧の終了を宣言するとともに、インシデントに関する文書の作成を完了する。	-	<High-Advanced><Advanced>共通 ・組織は、インシデントの内容、実施した対応および復旧対応、並びに得られた教訓を記録した事後報告書を作成する。	0	-	○ (IR-04、IR-08)	-	-	-
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.RC.CO-01	・組織は、セキュリティインシデント発生後の、復旧に向けた情報交換に関するルールを策定し、運用する。	-	<High-Advanced><Advanced>共通 ・組織は、セキュリティインシデントの復旧状況について、組織とサプライヤー間で報告・共有するためのルール及び手順を定める。 ・組織は、インシデントからの復旧に向けて実施している対応内容と、再発防止のための対策について、組織内部及び組織外部へ説明を行う。	0	-	○ (CP-01、CP-02、SA-04、SA-09、SR-02、SR-03、SR-08、IR-01、IR-04)	-	-	-
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.RC.CO-02	・組織は、事業継続計画又は緊急時対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。	L1_3_a_PRO	<High-Advanced><Advanced><Basic>共通 ・組織は、マスコミや取引先に対する情報のやり取りの窓口を一本化し、対応方針が一貫したものとなるようにする。 ・組織は、セキュリティインシデントによる被害に関する重要な情報について、情報の機密性に配慮しつつ丁寧に説明する。	0	-	-	-	-	-
CPS.RC.CO-03	・組織は、復旧活動について内部及び外部のステークホルダーと役員、そして経営陣に伝達する点を、事業継続計画又は緊急時対応計画の中に位置づける。	L1_3_a_PRO	<High-Advanced><Advanced>共通 ・組織は、監督官庁、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。	0	-	○ (IR-04、IR-08、SR-08)	-	-	-
			<Basic> ・組織は、自組織に影響を及ぼすようなセキュリティインシデント発生時における役割、責任、そうした役割と責任を割り当てられたヒトと連絡先情報を示す。 ・組織は、事業継続に関わる意思決定の責任が割り当てられたヒトに対して、意思決定をより適切なものとするため、セキュリティインシデントの概要や被害状況に関する説明を実施する。	0	-		-	-	-