

添付D 海外の主要規格との対応関係

D.1 NIST Cybersecurity Framework 2.0のサブカテゴリと「サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1」との対応表

NIST Cyberseucurity Framework Ver 2.0			サイバー・フィジカル・セキュリティ対策フレームワーク Ver. 1.1	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
統治 (GV)	GV.OC-01	組織のミッションが理解され、サイバーセキュリティリスクマネジメントに情報を提供している。	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。
	GV.OC-02	社内外のステークホルダーが理解され、サイバーセキュリティリスクマネジメントに関する彼らのニーズと期待が理解され、考慮されている。	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。
	GV.OC-03	サイバーセキュリティに関する法的要求事項、規制上の要件、及び契約上の要求事項（プライバシー及び市民的自由の義務を含む）が理解され、管理されている。	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。
	GV.OC-04	外部ステークホルダーが組織に依存または期待する重要な目的、ケイパビリティ（能力）、及びサービスが理解され、伝達されている。	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。
	GV.OC-05	組織が依存する成果、ケイパビリティ（能力）、サービスを理解が理解され、伝達されている。	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。
	GV.RM-01	リスクマネジメントの目的が確立され、組織のステークホルダーによって合意されている。	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。
	GV.RM-02	リスク選好度及びリスク許容度が確立され、伝達され、維持されている。	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。
	GV.RM-03	サイバーセキュリティリスクマネジメントの活動及び成果が、事業体のリスクマネジメントプロセスに含まれている。	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。
	GV.RM-04	適切なリスク対応のオプションを表す戦略的方向性が確立され、伝達されている。	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。
	GV.RM-05	サプライヤ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関する組織全体にわたるコミュニケーション系統が確立されている。	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。
	GV.RM-06	サイバーセキュリティリスクの計算、文書化、分類、優先順位付けのための標準化された方法が確立され、伝達されている。	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。
	GV.RM-07	戦略的機会(すなわちプラスに働くリスク)が特徴付けられ、組織のサイバーセキュリティリスクに関する議論に含まれている。	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。
	GV.RR-01	組織のリーダーシップが、サイバーセキュリティリスクに対する責任と説明責任を負い、リスクを認識し、倫理的で、継続的に改善する文化を育んでいる。	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。
	GV.RR-02	サイバーセキュリティリスクマネジメントに関連する役割、責任、権限が確立され、伝達され、理解され、実施されている。	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。
	GV.RR-03	サイバーセキュリティリスク戦略、役割、責任、ポリシーに見合った適切なリソースが割り振られている。	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。
	GV.RR-04	サイバーセキュリティが人事プラクティスに含まれている。	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。
	GV.PO-01	サイバーセキュリティリスクマネジメントのポリシーが、組織の状況、サイバーセキュリティ戦略、優先順位に基づいて策定され、伝達され、実施されている。	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。
	GV.PO-02	サイバーセキュリティリスクマネジメントのポリシーが、要件、脅威、技術、組織のミッションの変化を反映するようレビューされ、更新され、伝達され、実施されている。	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。
	GV.OV-01	戦略と方向性に情報を与え調整するために、サイバーセキュリティリスクマネジメント戦略の成果がレビューされている。	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。
	GV.OV-02	組織の要件とリスクを確実にカバーするために、サイバーセキュリティリスクマネジメント戦略がレビューされ、調整されている。	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。
	GV.OV-03	組織のサイバーセキュリティリスクマネジメントの実績が、必要な調整のために評価され、レビューされている。	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。

NIST Cyberseucurity Framework Ver 2.0			サイバー・フィジカル・セキュリティ対策フレームワーク Ver. 1.1	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
	GV.SC-01	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のプログラム、戦略、目的、ポリシー、及びプロセスが確立され、組織のステークホルダーによって合意されている。	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。
	GV.SC-02	サプライヤ、顧客、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が確立され、伝達され、社内及び社外で調整されている。	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。
	GV.SC-03	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が、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されている。	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。
	GV.SC-04	サプライヤが把握され、重要度によって優先順位が付けられている。	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。
	GV.SC-05	サプライチェーンにおけるサイバーセキュリティリスクに対処するための要件が確立され、優先順位が付けられ、サプライヤやその他の関連する第三者との契約やその他の種類の合意に統合されている。	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。
	GV.SC-06	サプライヤまたはその他の第三者との正式な関係を結ぶ前に、リスクを低減するための計画と適正評価が実施されている。	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。
	GV.SC-07	サプライヤ、その製品及びサービス、並びにその他の第三者によってもたらされるリスクが理解され、記録され、優先順位が付けられ、アセスメントされ、対応され、その関係継続中に監視されている。	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。
			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。
			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。
			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。
			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シージャを策定し、運用する。
			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。
	GV.SC-08	関連するサプライヤ及びその他の第三者が、インシデントの計画、対応、及び復旧活動に含まれている。	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。
			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。
			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。
	GV.SC-09	サプライチェーンのセキュリティプラクティスが、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プログラムに統合され、その実行が、技術製品及びサービスのライフサイクルを通じて監視されている。	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。
			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。
	GV.SC-10	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計画に、パートナーシップまたはサービス合意の締結後に発生する活動に関する規定が含まれている。	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。
			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シージャを策定し、運用する。
			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。
			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シージャを策定し、運用する。

NIST Cyberseucurity Framework Ver 2.0			サイバー・フィジカル・セキュリティ対策フレームワーク Ver. 1.1	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
識別 (ID)	ID.AM-01	組織が管理するハードウェアのインベントリ（一覧）が維持されている。	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。
	ID.AM-02	組織が管理するソフトウェア、サービス、及びシステムのインベントリ（一覧）が維持されている。	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。
	ID.AM-03	組織が認可したネットワーク通信及び内部と外部のネットワークのデータフローの描写が維持されている。	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。
	ID.AM-04	サプライヤが提供するサービスのインベントリ（一覧）が維持されている。	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。
	ID.AM-05	資産は、分類、重要度、リソース、及びミッションへのインパクトに基づいて優先順位付けされている。	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。
	ID.AM-07	指定されたデータタイプのデータ及び対応するメタデータのインベントリ（一覧）が維持されている。	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。
	ID.AM-08	システム、ハードウェア、ソフトウェア、サービス、及びデータが、ライフサイクル全体を通じて管理されている。	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。
	ID.RA-01	資産の脆弱性が識別され、妥当性が確認され、記録されている。	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。
	ID.RA-02	サイバー脅威インテリジェンスが、情報共有フォーラムや情報源から入手されている。	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。
	ID.RA-03	組織に対する内部及び外部の脅威が識別され、記録されている。	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。
	ID.RA-04	脆弱性を悪用する脅威の潜在的インパクトと起こりやすさが識別され、記録されている。	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。
	ID.RA-05	脅威、脆弱性、起こりやすさ、及びインパクトが、内在するリスクを理解し、リスク対応の優先順位付けに情報を提供するために使用されている。	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。
	ID.RA-06	リスク対応が選択され、優先順位付けされ、計画され、追跡され、伝達されている。	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。
	ID.RA-07	変更及び例外が管理され、リスクのインパクトがアセスメントされ、記録され、追跡されている。	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。
	ID.RA-08	脆弱性開示情報を受領し、分析し、対応するプロセスが確立されている。	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。
	ID.RA-09	ハードウェア及びソフトウェアの真正性と完全性が、取得及び使用前にアセスメントされている。	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。
	ID.RA-10	取得前に重要なサプライヤがアセスメントされている。	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。
	ID.IM-01	改善点が評価から識別されている。	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。
	ID.IM-02	サプライヤ及び関連する第三者と協力して実施されるものを含め、セキュリティテスト及び演習から改善点が識別されている。	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。
			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。
	ID.IM-03	運用プロセス、手順、及び活動の実行から改善点が識別されている。	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。
	ID.IM-04	運用に影響を及ぼすインシデント対応計画及びその他のサイバーセキュリティ計画が策定され、伝達され、維持され、改善されている。	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。
			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。

NIST Cyberseucurity Framework Ver 2.0			サイバー・フィジカル・セキュリティ対策フレームワーク Ver. 1.1	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
防御 (PR)	PR.AA-01	認可されたユーザー、サービス、及びハードウェアの ID 及び認証情報が、組織によって管理されている。	CPS.PR.AA-01	・組織は、承認されたモノとヒト及びプロシーダの識別情報と認証情報を発効、管理、確認、取消、監査するプロシーダを確立し、実施する。
	PR.AA-02	相互作用の文脈に基づいてIDが証明され、認証情報に結びつけられている。	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。
	PR.AA-03	ユーザー、サービス、及びハードウェアが認証されている。	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。
	PR.AA-04	ID アサーションが保護され、伝達され、検証されている。	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。
	PR.AA-05	アクセス許可、資格の付与、及び認可がポリシーで定義され、管理され、実施され、レビューされ、最小特権と職務分離の原則が組み込まれている。	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。
			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。
	PR.AA-06	資産への物理的なアクセスが、リスクに応じて管理され、監視され、実施されている。	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。
	PR.AT-01	サイバーセキュリティリスクを念頭に置いて一般的な職務を遂行するための知識とスキルを有するよう、人員に意識向上とトレーニングが提供されている。	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。
	PR.AT-02	サイバーセキュリティリスクを念頭に置いて関連職務を遂行するための知識とスキルを有するよう、専門的な役割を担う個人に意識向上とトレーニングが提供されている。	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。
			CPS.PR.AT-02	・組織は、自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。
	PR.DS-01	保存されているデータの機密性、完全性、及び可用性が保護されている。	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。
	PR.DS-02	伝送中のデータの機密性、完全性、及び可用性が保護されている。	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。
	PR.DS-10	使用中のデータの機密性、完全性、及び可用性が保護されている。	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。
	PR.DS-11	データのバックアップが作成され、保護され、維持され、テストされている。	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。
	PR.PS-01	構成管理のプラクティスが確立され、適用されている	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。
	PR.PS-02	ソフトウェアはリスクに応じて保守され、交換され、削除されている。	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。
			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。
	PR.PS-03	ハードウェアはリスクに応じて保守され、交換され、削除されている。	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。
			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。
	PR.PS-04	ログ記録が生成され、継続的監視のために利用可能となっている。	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。
	PR.PS-05	認可されていないソフトウェアのインストール及び実行が防止されている。	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。
	PR.PS-06	セキュアなソフトウェア開発プラクティスが統合され、その実行がソフトウェア開発ライフサイクル全体を通じて監視されている。	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。
	PR.IR-01	ネットワーク及び環境が認可されていない論理アクセス及び使用から保護されている。	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。
	PR.IR-02	組織の技術資産が環境上の脅威から保護されている。	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。
	PR.IR-03	通常時及び困難な状況でのレジリエンス要件を達成するためのメカニズムが実装されている。	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。
	PR.IR-04	可用性を確実にするために十分なリソース容量が維持されている。	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。

NIST Cyberseucurity Framework Ver 2.0			サイバー・フィジカル・セキュリティ対策フレームワーク Ver. 1.1	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
検知 (DE)	DE.CM-01	潜在的な有害事象を発見するために、ネットワーク及びネットワークサービスが監視されている。	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。
	DE.CM-02	潜在的な有害事象を発見するために、物理的環境が監視されている。	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。
	DE.CM-03	潜在的な有害事象を発見するために、人員の活動及び技術の利用が監視されている。	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。
	DE.CM-06	潜在的な有害事象を発見するために、外部サービスプロバイダの活動及びサービスが監視されている。	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。
	DE.CM-09	潜在的な有害事象を発見するために、コンピューティングハードウェアとソフトウェア、ランタイム環境、及びそれらのデータが監視されている。	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。
	DE.AE-02	関連する活動をよりよく理解するために、潜在的な有害事象が分析されている。	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。
	DE.AE-03	情報は複数の情報源から相互に関連付けられている。	CPS.DE.AE-02	・組織は、セキュリティ事象の関連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。
	DE.AE-04	有害事象の推定されるインパクトと範囲が理解されている。	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。
	DE.AE-06	有害事象に関する情報が、認可されたスタッフ及びツールに提供されている。	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。
	DE.AE-07	サイバー脅威インテリジェンス及びその他の文脈的情報が分析に統合されている。	CPS.DE.AE-02	・組織は、セキュリティ事象の関連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。
	DE.AE-08	有害事象が、定義されたインシデント基準を満たす場合に、インシデントが宣言される。	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。
対応 (RS)	RS.MA-01	インシデントが宣言されると、関連する第三者と連携してインシデント対応計画が実行されている。	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。
	RS.MA-02	インシデント報告がトリアージされ、妥当性が確認されている。	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。
	RS.MA-03	インシデントが分類され、優先順位が付けられている。	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。
	RS.MA-04	インシデントは必要に応じてエスカレーションまたは昇格されている。	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。
	RS.MA-05	インシデントの復旧の開始基準が適用されている。	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。
	RS.AN-03	インシデント発生中に何が起こったのか、及びインシデントの根本原因を特定するための分析が実施されている。	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。
	RS.AN-06	調査中に実施されたアクションが記録され、記録の完全性と来歴が保持されている。	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。
	RS.AN-07	インシデントのデータ及びメタデータが収集され、その完全性と来歴が保持されている。	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。
	RS.AN-08	インシデントの規模が推定され、妥当性が確認されている。	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。
	RS.CO-02	社内外のステークホルダーにインシデントを通知する。	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。
	RS.CO-03	指定された社内外のステークホルダーと情報を共有する。	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。
	RS.MI-01	インシデントが封じ込められている。	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。
	RS.MI-02	インシデントが根絶されている。	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。

NIST Cyberseucurity Framework Ver 2.0			サイバー・フィジカル・セキュリティ対策フレームワーク Ver. 1.1	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
復旧 (RC)	RC.RP-01	インシデント対応計画の復旧に関する部分が、インシデント対応プロセスから取り組みが開始されると実行されている。	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。
	RC.RP-02	復旧活動が選択され、範囲が設定され、優先順位が付けられ、実施されている。	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。
	RC.RP-03	バックアップ及びその他の復旧資産の完全性が、復旧に使用する前に検証されている。	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。
	RC.RP-04	重要なミッション機能とサイバーセキュリティリスクマネジメントが、インシデント後の運用規範を確立するために考慮されている。	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。
	RC.RP-05	復旧した資産の完全性が検証され、システム及びサービスが復旧し、正常な運用状態が確認されている。	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。
	RC.RP-06	基準に基づいてインシデント復旧の終了が宣言され、インシデント関連の文書の作成が完成している。	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。
	RC.CO-03	復旧活動及び運用ケイパビリティ（能力）復旧の進捗状況が、指定された社内外のステークホルダーに伝達されている。	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。
	RC.CO-04	インシデント復旧に関する公開最新情報は、承認された方法及びメッセージングを使用して共有されている。	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。

D.2 NIST SP 800-171(Rev.3)の要求事項と「サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1」との対応表

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
アクセス制御	03.01.01	アカウント管理	a. 許可および禁止されるシステムアカウントのタイプを規定する。	・ AC-02 アカウント管理 ・ AC-02(03) アカウントの無効化 ・ AC-02(05) 非アクティブログアウト ・ AC-02(13) リスクの高い個人のアカウントの無効化	CPS.PR.AA-01	・ 組織は、承認されたモノとヒト及びプロシーダの識別情報と認証情報を発効、管理、確認、取消、監査するプロシーダを確立し、実施する。
			b. ポリシー、手順、前提条件、および基準に従って、システムアカウントを作成、有効化、変更、無効化、削除する。		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。
			c. 以下を規定する。 1. システムの認可されたユーザ 2. グループと役割のメンバーシップ 3. 各アカウントのアクセス認可（すなわち特権）		CPS.PR.AA-01	・ 組織は、承認されたモノとヒト及びプロシーダの識別情報と認証情報を発効、管理、確認、取消、監査するプロシーダを確立し、実施する。
			d. 以下に基づいてシステムへのアクセスを認可する。 1. 有効なアクセス認可 2. システムの使用目的		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。
			e. システムアカウントの使用を監視する。		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。
			f. 以下の場合に、システムアカウントを無効にする。 1. アカウントの有効期限が切れている。 2. アカウントが[設定：組織が定める期間]、非アクティブになっている。 3. アカウントがもはやユーザまたは個人に関連付けられていない。 4. アカウントが組織のポリシーに違反している。 5. 個人に関連する重大なリスクが発見されている。		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。
			g. 以下の場合に、アカウントマネージャーおよび指定された職員または役割に通知する。 1. [設定：組織が定める期間] アカウントが不要になったとき。 2. [設定：組織が定める期間] ユーザが退職または異動するとき。 3. [設定：組織が定める期間] システムの使用状況や個人の知る必要性（need-to-know）が変化したとき。		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。
			h. [設定：組織が定める期間] アクティブでないことが予想される場合、または [設定：組織が定める状況] になった場合、ユーザがシステムからログアウトすることを要求する。		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。
			CPS.PR.AA-01		・ 組織は、承認されたモノとヒト及びプロシーダの識別情報と認証情報を発効、管理、確認、取消、監査するプロシーダを確立し、実施する。	
			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。	
	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。				
	—	—				
	03.01.02	アクセス実施	適用されるアクセス制御ポリシーに従い、CUIおよびシステムリソースへの論理アクセスに対する承認された認可を実施する。	・ AC-03 アクセス実施 ・ AC-17 リモートアクセス	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。
					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。
	03.01.03	情報フローの実施	システム内および接続されたシステム間のCUIのフローを制御するために、承認された認可を実施する。	・ AC-04 情報フローの実施	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。

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.01.04	職務の分離	a. 分離が必要な個人の職務を特定する。	・ AC-05 職務の分離	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。
			b. 職務の分離をサポートするためのシステムアクセス認可を規定する。		—	—
	03.01.05	最小特権	a. ユーザ（またはユーザに代わって動作するプロセス）に対して、割り当てられた組織のタスクを達成するために必要な、認可されたシステムアクセスのみを許可する。	・ AC-06最小特権 ・ AC-06(01) セキュリティ機能へのアクセス認可 ・ AC-06(07) ユーザ特権のレビュー	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。
			b. [設定：組織が定めるセキュリティ機能] および [設定：組織が定めるセキュリティ関連情報] へのアクセスを認可する。		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。
			c. [設定：組織が定める頻度] で、ユーザの役割またはクラスに割り当てられた特権をレビューし、そのような特権の必要性の妥当性確認を行う。		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。
			d. 必要に応じて、特権を再割り当てまたは削除する。		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。
	03.01.06	最小特権 – 特権アカウント	a. システム上の特権アカウントを [設定：組織が定める職員または役割] に制限する。	・ AC-06(02) 非セキュリティ機能に関する非特権アクセス ・ AC-06(05) 特権アカウント	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。
			b. 特権アカウントを持つユーザ（または役割）が、非セキュリティ機能または非セキュリティ情報にアクセスするときは、非特権アカウントを使用することを要求する。		—	—
	03.01.07	最小特権 – 特権機能	a. 非特権ユーザが特権機能を実行できないように防止する。	・ AC-06(09) 特権機能使用のロギング ・ AC-06(10) 非特権ユーザによる特権機能の実行の禁止	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。
			b. 特権機能の実行をログに記録する。		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。
	03.01.08	ログオン試行の失敗	a. [設定：組織が定める期間] の間、[設定：組織が定める数] の連続無効ログオン試行回数の制限を実施する。	・ AC-07 ログオン試行の失敗	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け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。
			b. 失敗した試行の最大回数を超えた場合、自動的に [選択（1つ以上）：[設定：組織が定める期間] アカウントまたはノードをロックする；管理者が解除するまでアカウントまたはノードをロックする；次回のログオンプロンプトを遅延させる；システム管理者に通知する；その他の措置を取る]。		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け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。
	03.01.09	システム使用通知	システムへのアクセスを許可する前に、適用されるCUIルールに沿ったプライバシーおよびセキュリティに関する通知を含むシステム使用通知メッセージを表示する。	・ AC-08 システム使用の通知	—	—
	03.01.10	デバイスロック	a. [選択（1つ以上）：[設定：組織が定める期間] 非アクティブになった後、デバイスロックを開始する；システムを離れる前に、ユーザにデバイスロックを開始することを要求する] ことによって、システムへのアクセスを防止する。	・ AC-11デバイスロック ・ AC-11(01) パターン表示による隠蔽	—	—
			b. ユーザが確立された識別および認証手順を使用してアクセスを再確立するまで、デバイスロックを保持する。		—	—
			c. デバイスロックにより、これまでディスプレイに表示されていた情報を、一般に閲覧可能な画像で隠す。		—	—
	03.01.11	セッションの終了	[設定：組織が定める条件またはセッション切断を必要とするトリガーイベント] の後に、ユーザーセッションを自動的に終了する。	・ AC-12 セッションの終了	—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.01.12	リモートアクセス	a. 許容されるリモートアクセスのタイプごとに、使用制限、設定要件、接続要件を定める。	・ AC-17(03) 管理されたアクセス制御ポイント ・ AC-17(04) 特権コマンドおよびアクセス	—	—
			b. 接続を確立する前に、各タイプのリモートシステムアクセスを認可する。		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。
			c. 認可され管理されたアクセス制御ポイントを経由して、システムへのリモートアクセスをルーティングする。		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。
			d. 特権コマンドのリモート実行およびセキュリティ関連情報へのリモートアクセスを認可する。		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。
	03.01.13	撤回	03.13.08で扱われている。			
	03.01.14	撤回	03.01.12に組み込まれた。			
	03.01.15	撤回	03.01.12に組み込まれた。			
	03.01.16	ワイヤレスアクセス	a. システムへの各タイプのワイヤレスアクセスについて、使用制限、設定要件、接続要件を定める。	・ AC-18 ワイヤレスアクセス ・ AC-18(01) 認証および暗号化 ・ AC-18(03) ワイヤレスネットワークの無効化	—	—
			b. システムへのワイヤレスアクセスを確立する前に、各タイプのワイヤレスアクセスを認可する。		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。
			c. 使用が意図されていない場合は、発行および配備の前に、ワイヤレスネットワークケイパビリティを無効にする。		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。
			d. 認証と暗号化を使用して、システムへのワイヤレスアクセスを保護する。		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。
					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。
	03.01.17	撤回	03.01.16に組み込まれた。			
	03.01.18	モバイルデバイスのアクセス制御	a. モバイルデバイスの使用制限、設定要件、および接続要件を定める。	・ AC-19 モバイルデバイスのアクセス制御 ・ AC-19(05) デバイス全体またはコンテナ単位の暗号化	—	—
			b. モバイルデバイスのシステムへの接続を認可する。		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。
			c. モバイルデバイス上のCUIの機密性を保護するために、デバイス全体またはコンテナ単位の暗号化を導入する。		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。
	03.01.19	撤回	03.01.18に組み込まれた。			

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.01.20	外部システムの利用	a. 特別に認可された外部システム以外は、使用を禁止する。	・ AC-20外部システムの使用 ・ AC-20(01) 認可された使用に限定 ・ AC-20(02) ポータブルストレージデバイス 使用制限	—	—
			b. 認可された個人による外部システムの使用またはアクセスを許可する前に、外部システムで満たすべき〔設定：組織が定めるセキュリティ要件〕を設定する。		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。
			c. 認可された個人が外部システムを使用して組織のシステムにアクセスすること、またはCUIを処理、保存、伝送することを、以下の場合にのみ許可する。 1. 組織のシステムセキュリティ計画に規定されている外部システムのセキュリティ要件が満たされていることを検証していること、および 2. 外部システムをホストしている組織のエンティティとの、承認されたシステム接続または処理契約を保持していること。		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。
			d. 組織が管理するポータブルストレージデバイスの外部システムでの使用を、認可された個人に制限する。		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。
	03.01.21	撤回	03.01.20に組み込まれた。		—	—
	03.01.22	一般の人がアクセス可能なコンテンツ	a. 一般の人がアクセス可能な情報にCUIが含まれていないことを確実にするために、認可された個人をトレーニングする。	・ AC-22 公的にアクセス可能なコンテンツ	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。
b. 一般の人がアクセス可能なシステム上のコンテンツにCUIがないかレビューし、そのような情報が発見された場合は削除する。			—		—	
意識向上およびトレーニング	03.02.01	リテラシートレーニングおよび意識向上	a. 以下のタイミングで、システムユーザにセキュリティリテラシートレーニングを提供する。 1. 新規ユーザの初期トレーニングの一環として、およびその後は〔設定：組織が定める頻度〕で。 2. システムの変更により必要となった場合、または〔設定：組織が定めるイベント〕の後。 3. インサイダー脅威、ソーシャルエンジニアリング、ソーシャルマイニングの兆候が認識され報告された場合。	・ AT-02 リテラシートレーニングおよび意識向上 ・ AT-02(02) インサイダー脅威 ・ AT-02(03) ソーシャルエンジニアリングおよびマイニング	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。
			b. 〔設定：組織が定める頻度〕で、および〔設定：組織が定めるイベント〕の後に、セキュリティリテラシートレーニングの内容を更新する。		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。
	03.02.02	役割ベースのトレーニング	a. 以下のタイミングで、組織の職員に対して、役割ベースのセキュリティトレーニングを実施する。 1. システムまたはCUIへのアクセスを認可する前、割り当てられた職務を遂行する前、およびその後は〔設定：組織が定める頻度〕で。 2. システムの変更により必要となった場合、または〔設定：組織が定めるイベント〕の後。	・ AT-03 役割ベースのトレーニング	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。
b. 〔設定：組織が定める頻度〕および〔設定：組織が定めるイベント〕の後に、役割ベースのトレーニング内容を更新する。			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。	
	03.02.03	撤回	03.02.01に組み込まれた。			
監査および説明責任	03.03.01	イベントロギング	a. システム内のロギングのために選択される〔設定：組織が定めるイベントタイプ〕を規定する。	・ AU-02 イベントロギング	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。
			b. ロギングのために選択されたイベントタイプを〔設定：組織が定める頻度〕でレビューし、更新する。		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。

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.03.02	監査記録の内容	a. 監査記録には以下の内容を含める。 1. 発生したイベントのタイプ 2. イベントが発生した日時 3. イベントが発生した場所 4. イベントの発生源 5. イベントの結果 6. イベントに関連する個人、サブジェクト、オブジェクト、またはエンティティのアイデンティティ	・ AU-03 監査記録の内容 ・ AU-03(01) 追加の監査情報	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。
			b. 必要に応じて監査記録のための追加情報を提供する。		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。
	03.03.03	監査記録の生成	a. 03.03.01および03.03.02で指定された選択されたイベントタイプおよび監査記録内容の監査記録を生成する。	・ AU-11 監査記録の保持 ・ AU-12 監査記録の生成	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。
			b. 記録保持ポリシーと一致する期間、監査記録を保持する。		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。
	03.03.04	監査ログGINGプロセス障害時の対応	a. 監査ログGINGプロセスに障害が発生した場合は、[設定：組織が定める期間] 内に組織の職員または役割に警告する。	・ AU-05 監査ログGINGプロセス障害時の対応	—	—
			b. [設定：組織が定める追加の措置] を取る。		—	—
	03.03.05	監査記録のレビュー、分析、および報告	a. 不適切または異常な活動の兆候、および潜在的なインパクトについて、[設定：組織が定める頻度] でシステム監査記録をレビューし、分析する。	・ AU-06 監査記録のレビュー、分析、および報告 ・ AU-06(03) 監査記録リポジトリの関連付け	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。
					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。
			b. 調査結果を組織の職員または役割に報告する。		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。
			c. 組織全体の状況を認識するために、異なるリポジトリにわたって監査記録を分析し、相互に関連付ける。		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。
	03.03.06	監査記録の整理および報告書の作成	a. 監査記録のレビュー、分析、報告の要件、およびインシデントの事後調査をサポートする、監査記録の整理および報告書作成ケイパビリティを実装する。	・ AU-07 監査記録の整理および報告書の作成	—	—
					—	—
			b. 監査記録の元の内容と時間順序を維持する。		—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.03.07	タイムスタンプ	a. 内部システムクロックを使用して、監査記録のタイムスタンプを生成する。	・ AU-08 タイムスタンプ	—	—
			b. [設定：組織が定める時間測定の精度] を満たしており、協定世界時（UTC）を使用するか、UTC からの固定現地時間オフセットを有するか、またはタイムスタンプの一部として現地時間オフセットを含むタイムスタンプを監査記録のために記録する。		—	—
	03.03.08	監査情報の保護	a. 監査情報および監査ロギングツールを認可されていないアクセス、変更、削除から保護する。	・ AU-09 監査情報の保護 ・ AU-09(04) 一部の特権ユーザによるアクセス	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。
			b. 特権ユーザまたは役割の一部にのみ、監査ロギング機能の管理へのアクセスを認可する。		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。
	03.03.09	撤回	03.03.08に組み込まれた。			
構成管理	03.04.01	ベースライン構成	a. システムの現在のベースライン構成を作成し、構成管理の下で維持する。	・ CM-02 ベースライン構成	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。
			b. [設定：組織が定める頻度] で、およびシステムコンポーネントがインストールまたは変更された場合、システムのベースライン構成をレビューし、更新する。		—	—
	03.04.02	構成設定	a. 最も制限のきびしい運用要件と一致する状態を反映する、システムの [設定：組織が定める構成設定] を確立し、文書化し、実装する。	・ CM-06 構成設定	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。
			b. 確立された構成設定からの逸脱を特定し、文書化し、承認する。		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。
	03.04.03	構成変更管理	a. 構成管理されるシステムに対する変更のタイプを規定する。	・ CM-03 構成変更管理	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。
			b. システムに対して提案されている構成管理された変更をレビューし、セキュリティへのインパクトを明示的に考慮した上で、そのような変更を承認または不承認とする。		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。
			c. 承認された構成管理された変更をシステムに実装し、文書化する。		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。
			d. システムに対する構成管理された変更に関連する活動を監視し、レビューする。		—	—
	03.04.04	インパクト分析	a. システムに対する変更を実装する前に、潜在的なセキュリティインパクトを判断するために、変更を分析する。	・ CM-04 インパクト分析 ・ CM-04(02) 管理策の検証	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。
			b. システムのセキュリティ要件が、システム変更実装後も引き続き満たされていることを検証する。		—	—
	03.04.05	変更に対するアクセス制限	システムの変更に伴う物理的および論理的なアクセス制限を規定し、文書化し、承認し、実施する。	・ CM-05 変更に対するアクセス制限	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。
					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。

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.04.06	最小機能性	a. ミッションに必須なケイパビリティのみを提供するようにシステムを構成する。	・ CM-07 最小機能性 ・ CM-07(01) 定期的なレビュー	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。
			b. [設定：組織が定める機能、ポート、プロトコル、接続、およびサービス] の使用を禁止または制限する。		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。
			c. [設定：組織が定める頻度] でシステムをレビューし、不要または非セキュアな機能、ポート、プロトコル、接続、およびサービスを特定する。		—	—
			d. 不要または非セキュアな機能、ポート、プロトコル、接続、およびサービスを無効化または削除する。		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。
	03.04.07	撤回	03.04.06および03.04.08に組み込まれた。			
	03.04.08	認可されたソフトウェア – 例外による許可	a. システム上で実行が認可されるソフトウェアプログラムを識別する。	・ CM-07(05) 認可されたソフトウェア – 例外による許可	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。
			b. システム上で認可されたソフトウェアプログラムの実行について、すべて拒否・例外による許可のポリシーを実装する。		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。
			c. [設定：組織が定める頻度] で認可されたソフトウェアプログラムのリストをレビューし、更新する。		—	—
	03.04.09	撤回	03.01.05、03.01.06、03.01.07、03.04.08、03.12.03で扱われている。			
	03.04.10	システムコンポーネントのインベントリ	a. システムコンポーネントのインベントリを作成し、文書化する。	・ CM-08 システムコンポーネントのインベントリ ・ CM-08(01) インストール中および削除中の更新	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。
			b. [設定：組織が定める頻度] で、システムコンポーネントのインベントリをレビューし、更新する。		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。
			c. インストール、削除、システム更新の一環として、システムコンポーネントのインベントリを更新する。		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。
	03.04.11	情報の位置	a. CUIの位置、およびその情報が処理され保存されるシステムコンポーネントを識別し、文書化する。	・ CM-12 情報の位置	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。
			b. CUIが処理され保存されるシステムまたはシステムコンポーネントの位置の変更を文書化する。		—	—
	03.04.12	高リスクエリアのシステムおよびコンポーネントの構成	a. リスクの高い場所に出張する個人に対して、[設定：組織が定めるシステム構成] を持つシステムまたはシステムコンポーネントを支給する。	・ CM-02(07) 高リスク領域のシステムおよびコンポーネントの構成	—	—
			b. 個人が出張から戻ってきた時に [設定：組織が定めるセキュリティ要件] をシステムまたはシステムコンポーネントに適用する。		—	—
識別および認証	03.05.01	ユーザの識別および認証	a. システムユーザを一意に識別および認証し、その一意の識別情報を、それらのユーザに代わって動作するプロセスに関連付ける。	・ IA-02 識別および認証（組織のユーザ） ・ IA-11 再認証	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。
			b. [設定：再認証が必要な組織が定める状況または場面] の場合は、ユーザを再認証する。		—	—
	03.05.02	デバイスの識別および認証	システム接続を確立する前に、[設定：組織が定めるデバイスまたはデバイスのタイプ] を一意に識別および認証する。	・ IA-03 デバイスの識別および認証	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。

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.05.03	多要素認証	特権アカウントおよび非特権アカウントへのアクセスに多要素認証を導入する。	・ IA-02(01) 特権アカウントへの多要素認証 ・ IA-02(02) 非特権アカウントへの多要素認証	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。
	03.05.04	リブレイ攻撃耐性のある認証	特権アカウントおよび非特権アカウントへのアクセスについて、リブレイ攻撃耐性のある認証メカニズムを実装する。	・ IA-02(08) アカウントへのアクセス - リブレイ攻撃耐性	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。
	03.05.05	識別子管理	a. 個人、グループ、役割、サービス、またはデバイス識別子を割り当てるために、組織の職員または役割から認可を得る。	・ IA-04 識別子管理 ・ IA-04(04) ユーザステータスの識別	—	—
			b. 個人、グループ、役割、サービス、またはデバイスを識別する識別子を選択し、割り当てる。		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。
			c. [設定：組織が定める期間]、識別子の再利用を防止する。		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。
			d. [設定：組織が定める個人のステータスを識別する特性] で各個人を一意に識別することにより、個人の識別子を管理する。		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。
	03.05.06	撤回	SP 800-53 [8]と整合。			
	03.05.07	パスワード管理	a. 一般的に使用される、予想される、または危殆化したパスワードのリストを維持し、[設定：組織が定める頻度] で、および組織のパスワードが危殆化した疑いがある場合にリストを更新する。	・ IA-05(01) パスワードによる認証	—	—
			b. ユーザがパスワードを作成または更新する際に、そのパスワードが一般的に使用される、予想される、または危殆化したパスワードのリストにないことを確認する。		—	—
			c. パスワードの伝送は、暗号技術によって保護されたチャネルを介してのみ行う。		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。
			d. パスワードは暗号技術によって保護した形で保存する。		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。
			e. アカウント復旧後の最初の利用時に新しいパスワードを選択する。		—	—
			f. パスワードに対して、[設定：組織が定める構成および複雑さのルール] を強制する。		—	—
	03.05.08	撤回	SP 800-53 [8]と整合。			
	03.05.09	撤回	SP 800-53 [8]と整合。			
	03.05.10	撤回	03.05.07に組み込まれた。			
	03.05.11	認証フィードバック	認証プロセス時に認証情報のフィードバックを不明瞭にする。	・ IA-06 認証フィードバック	—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.05.12	オーセンティケータの管理	a. オーセンティケータの初回配布の一環として、オーセンティケータを受け取る個人、グループ、役割、サービス、またはデバイスのアイデンティティを検証する。	・ IA-05 オーセンティケータ管理	CPS.PR.AA-01	・ 組織は、承認されたモノとヒト及びプロセスの識別情報と認証情報を発効、管理、確認、取消、監査するプロセスを確立し、実施する。
			b. 組織が発行するオーセンティケータの初期オーセンティケータの内容を定める。		CPS.PR.AA-01	・ 組織は、承認されたモノとヒト及びプロセスの識別情報と認証情報を発効、管理、確認、取消、監査するプロセスを確立し、実施する。
			c. オーセンティケータの初回配布に関する管理手順、紛失、危殆化または破損したオーセンティケータに関する管理手順、およびオーセンティケータの失効に関する管理手順を定め、実装する。		CPS.PR.AA-01	・ 組織は、承認されたモノとヒト及びプロセスの識別情報と認証情報を発効、管理、確認、取消、監査するプロセスを確立し、実施する。
			d. 初回使用時にデフォルトのオーセンティケータを変更する。		CPS.PR.AA-01	・ 組織は、承認されたモノとヒト及びプロセスの識別情報と認証情報を発効、管理、確認、取消、監査するプロセスを確立し、実施する。
			e. [設定：組織が定める頻度] で、または [設定：組織が定めるイベント] が発生したとき、オーセンティケータを変更または更新する。		CPS.PR.AA-01	・ 組織は、承認されたモノとヒト及びプロセスの識別情報と認証情報を発効、管理、確認、取消、監査するプロセスを確立し、実施する。
			f. 認可されていない開示や変更からオーセンティケータの内容を保護する。		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。
インシデント対応	03.06.01	インシデント処理	インシデント対応計画に整合し、準備、検知および分析、封じ込め、根絶、復旧を含むインシデント処理ケイパビリティを実装する。	・ IR-04 インシデント対応	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。
					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。
	03.06.02	インシデントの監視、報告、対応支援	a. システムのセキュリティインシデントを追跡し、文書化する。	・ IR-05 インシデント監視 ・ IR-06 インシデント報告 ・ IR-07 インシデント対応支援	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。
			b. [設定：組織が定める期間] 内に、疑わしいインシデントを組織のインシデント対応ケイパビリティに報告する。		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。
			c. インシデント情報を [設定：組織が定める権限] に報告する。		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。
			d. システムユーザにインシデントの処理および報告に関する助言および支援を提供するために、インシデント対応サポートリソースを提供する。		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。
	03.06.03	インシデント対応テスト	[設定：組織が定める頻度] で、インシデント対応ケイパビリティの有効性をテストする。	・ IR-03 インシデント対応テスト	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。
					CPS.PR.AT-02	・ 組織は、自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。
	03.06.04	インシデント対応トレーニング	a. 割り当てられた役割および責任に一致するインシデント対応トレーニングを、以下のタイミングでシステムユーザに提供する。 1. インシデント対応の役割または責任を引き受けてから、またはシステムへのアクセス権を取得してから [設定：組織が定める期間] 内に。 2. システムの変更により必要となった場合。 3. その後は、[設定：組織が定める頻度]で。	・ IR-02 インシデント対応トレーニング	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。
			b. [設定：組織が定める頻度]、および [設定：組織が定めるイベント]の後に、インシデント対応トレーニングの内容をレビューし、更新する。		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。

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.06.05	インシデント対応計画	a. 以下のようなインシデント対応計画を策定する。 1. インシデント対応ケイパビリティを実装するためのロードマップを組織に提供する。 2. インシデント対応ケイパビリティの構造および組織を記述する。 3. インシデント対応ケイパビリティが組織全体にどのように適合するかについて、高レベルのアプローチを提供する。 4. 報告する必要のあるインシデントを規定する。 5. インシデント情報の共有に対処する。 6. 組織のエンティティ、職員、または役割に責任を指定する。	・ IR-08 インシデント対応計画	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。
			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。	
			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。	
			—		—	
			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。	
			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。	
メンテナ ス	03.07.01	撤回	NCOとして再分類された。			
	03.07.02	撤回	03.07.04および03.07.06に組み込まれた。			
	03.07.03	撤回	03.08.03に組み込まれた。			
	03.07.04	メンテナンスツール	a. システムメンテナンスツールの使用を承認、管理、監視する。	・ MA-03メンテナンスツール ・ MA-03(01) ツールの検査 ・ MA-03(02) 媒体の検査 ・ MA-03(03) 認可されていない移動の防止	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。
			b. 診断テストプログラムを含む媒体をシステムで使用する前に、悪意のあるコードについてチェックする。		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。
			c. メンテナンス装置上にCUIがないことを検証したり、装置をサニタイズまたは破壊したり、または装置を施設内に留めることにより、CUIを含むシステムメンテナンス装置の持ち出しを防止する。		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。
	03.07.05	非ローカルメンテナンス	a. 非ローカルメンテナンスおよび診断措置を承認し、監視する。	・ MA-04 非ローカルメンテナンス	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。
			b. 非ローカルメンテナンスおよび診断セッションの確立において、多要素認証およびリプレイ攻撃耐性を実装する。		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。
			c. 非ローカルメンテナンスが完了した際、セッションおよびネットワーク接続を切断する。		—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.07.06	メンテナンス作業員	a. メンテナンス作業員の認可プロセスを確立する。	・ MA-05 メンテナンス作業員	—	—
			b. 認可されたメンテナンス組織または作業員のリストを維持する。		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。
			c. システムのメンテナンスを行うエスコートされていない作業員が、必要なアクセス認可を持っていることを確認する。		—	—
			d. 必要なアクセス認可を持たない作業員のメンテナンス活動を監督するために、必要なアクセス認可および技術的力量を持つ組織の職員を指定する。		—	—
媒体保護	03.08.01	媒体保管	CUIを含むシステム媒体を物理的に管理し、セキュアに保管する。	・ MP-04 媒体保管	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。
					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。
	03.08.02	媒体へのアクセス	システム媒体上のCUIへのアクセスを認可された職員または役割に制限する。	・ MP-02 媒体へのアクセス	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。
					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。
	03.08.03	媒体のサニタイズ	CUIを含むシステム媒体は、廃棄する前、組織の管理外に持ち出す前、再利用のために持ち出す前にサニタイズする。	・ MP-06 媒体のサニタイズ	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。
	03.08.04	媒体へのマーキング	配布制限、取り扱いの警告、該当するCUIマーキングを示すために、CUIを含むシステム媒体にマークを付ける。	・ MP-03 媒体へのマーキング	CPS.PR.DS-01	・ 組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。
	03.08.05	媒体移送	a. 管理エリア外への移送中、CUIを含むシステム媒体を保護し、管理する。	・ MP-05 媒体移送 ・ SC-28 保管中の情報の保護	—	—
			b. 管理エリア外への移送中、CUIを含むシステム媒体の説明責任を維持する。		—	—
			c. CUIを含むシステム媒体の移送に関連する措置を文書化する。		—	—
	03.08.06	撤回	03.13.08で扱われている。			
	03.08.07	媒体の使用	a. [設定：組織が定めるシステム媒体のタイプ]の使用を制限または禁止する。	・ MP-07 媒体の使用	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。
			b. 識別可能なオーナーのいない取り外し可能なシステム媒体の使用を禁止する。		—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.08.08	撤回	03.08.07に組み込まれた。			
	03.08.09	システムバックアップー暗号化による保護	a. バックアップ情報の機密性を保護する。	・CP-09 システムバックアップ ・CP-09(08) 暗号化による保護	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。
			b. バックアップ保存場所におけるCUIの認可されていない開示を防止するため、暗号化のメカニズムを実装する。		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。
					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。
職員のセキュリティ	03.09.01	職員のスクリーニング	a. システムへのアクセスを認可する前に、個人をスクリーニングする。	・PS-03 職員のスクリーニング	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。
			b. [設定：再スクリーニングが必要な組織が定める条件] に従って、個人を再スクリーニングする。		—	—
	03.09.02	退職と異動	a. 個人の雇用が終了した場合、 1. [設定：組織が定める期間] 内にシステムアクセスを無効にする。 2. 個人に関連付けられたオーセンティケータおよびクレデンシャルを終了または取り消す。 3. セキュリティ関連のシステム資産を回収する。	・PS-04 職員の雇用終了 ・PS-05 職員の異動	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。
			b. 個人が組織内の他の職位に配置転換または異動する場合、 1. システムおよび施設に対する現行の論理的および物理的アクセス認可の継続的な運用上の必要性をレビューし、確認する。 2. 運用上の必要性の変化に応じて、アクセス認可を変更する。		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。
物理的保護	03.10.01	物理的アクセス認可			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。
					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。
			a. システムが存在する施設へのアクセスを許可された個人のリストを作成し、承認し、維持する。	・PE-02 物理的アクセス認可	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。
			b. 施設にアクセスするための認可クレデンシャルを発行する。		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。
			c. [設定：組織が定める頻度] で施設アクセスリストをレビューする。		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。
			d. アクセスが不要になった場合、施設アクセスリストから個人を削除する。		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。

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.10.02	物理的アクセスの監視	a. システムが存在する施設への物理的アクセスを監視し、物理的セキュリティインシデントを検知し対応する。	・ PE-06 物理的アクセスの監視	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。
			b. [設定：組織が定める頻度] で、および[設定：組織が定めるイベントまたはイベントの潜在的兆候]の発生時に物理的アクセスログをレビューする。		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。
					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。
	03.10.03	撤回	03.10.07に組み込まれた。			
	03.10.04	撤回	03.10.07に組み込まれた。			
	03.10.05	撤回	03.10.07に組み込まれた。			
	03.10.06	代替作業場所	a. 従業員が使用できる代替作業場所を決定する。	・ PE-17 代替作業サイト	—	—
			b. 代替作業場所において [設定：組織が定めるセキュリティ要件] を採用する。		—	—
	03.10.07	物理的アクセス制御	a. システムが存在する施設への出入口において、以下の方法により物理的アクセス認可を実施する。 1. 施設へのアクセスを許可する前に、個人の物理的アクセス認可を検証する。 2. 物理的なアクセス制御システム、デバイス、または警備員を使って出入りを管理する。	・ PE-03 物理的アクセス制御 ・ PE-05 出力デバイスのアクセス制御	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。
			b. 出入口の物理的アクセス監査ログを維持する。		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。
			c. 訪問者をエスコートし、訪問者の行動を管理する。		—	—
			d. 鍵、文字合せ錠、その他の物理的アクセスデバイスをセキュアに保護する。		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。
			e. 認可されていない個人がCUIにアクセスできないよう、出力デバイスへの物理的アクセスを管理する。		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。
	03.10.08	伝送のアクセス制御	組織の施設内のシステム配電線および送電線への物理的アクセスを制御する。	・ PE-04 伝送設備のアクセス制御	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。
リスクアセスメント	03.11.01	リスクアセスメント	a. CUIの処理、保存、伝送から生じる認可されていない開示のリスク（サプライチェーンリスクを含む）をアセスメントする。	・ RA-03 リスクアセスメント ・ RA-03(01) サプライチェーンのリスクアセスメント ・ SR-06 サプライヤのアセスメントおよびレビュー	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。
					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。
					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。
			b. [設定：組織が定める頻度] でリスクアセスメントを更新する。		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。

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.11.02	脆弱性の監視およびスキャン	a. [設定：組織が定める頻度] で、およびシステムに影響する新たな脆弱性が特定された場合に、システムの脆弱性を監視し、スキャンする。	・ RA-05 脆弱性の監視およびスキャン ・ RA-05(02) スキャンする脆弱性の更新	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。
			b. [設定：組織が定める応答時間] 内にシステムの脆弱性を修正する。		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。
			c. [設定：組織が定める頻度] で、および新たな脆弱性が特定および報告された場合に、スキャンするシステムの脆弱性を更新する。		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。
					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。
	03.11.03	撤回	03.11.02に組み込まれた。			
	03.11.04	リスク対応	セキュリティアセスメント、監視、および監査から得られた結果に対応する。	・ RA-07 リスク対応	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。
セキュリティアセスメントおよび監視	03.12.01	セキュリティアセスメント	システムおよびその運用環境のセキュリティ要件が満たされているかどうかを判断するために、[設定：組織が定める頻度] でセキュリティ要件をアセスメントする。	・ CA-02 管理策アセスメント	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。
					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。
	03.12.02	実施計画およびマイルストーン	a. 以下の目的のために、システムの実施計画およびマイルストーンを策定する。 1. セキュリティアセスメントで指摘された弱点や欠陥を是正するために計画した修正措置を文書化する。 2. 既知のシステム脆弱性を低減または排除する。	・ CA-05 実施計画およびマイルストーン	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。
					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。
			b. 以下からの結果に基づき、既存の実施計画およびマイルストーンを更新する。 1. セキュリティアセスメント 2. 監査またはレビュー 3. 常時監視活動		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。
		03.12.03	常時監視	継続的監視およびセキュリティアセスメントを含む、システムレベルの常時監視戦略を策定し、実施する。	・ CA-07 継続的監視	CPS.DE.CM-01
					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。
					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。
					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。
					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。
	03.12.04	撤回	03.15.02に組み込まれた。			

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.12.05	情報交換	a. [選択（1つ以上）：相互接続セキュリティ合意書；情報交換セキュリティ合意書；覚書または合意書；サービスレベル合意書；ユーザ合意書；非開示合意書；その他のタイプの合意書] を使用して、システムと他のシステム間のCUIの交換を承認し、管理する。	・ CA-03 情報交換	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。
			b. 交換合意書の一部として、各システムのインタフェース特性、セキュリティ要件、および責任を文書化する。		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。
			c. [設定：組織が定める頻度] で交換合意書をレビューし、更新する。		—	—
システムおよび通信の保護	03.13.01	境界保護	a. システムに対する外部管理インタフェースおよびシステム内の主要な内部管理インタフェースにおける通信を監視および制御する。	・ SC-07 境界保護	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。
					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。
					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。
			b. 内部ネットワークから物理的または論理的に分離された、一般の人がアクセス可能なシステムコンポーネント用のサブネットワークを実装する。		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。
			c. 組織のセキュリティアーキテクチャに従って配置された境界システム保護デバイスで構成される管理されたインタフェースを介してのみ、外部システムに接続する。		—	—
	03.13.02	撤回	NCOに再分類された。			
	03.13.03	撤回	03.01.01、03.01.02、03.01.03、03.01.04、03.01.05、03.01.06、03.01.07で扱われている。			
	03.13.04	共有システムリソース内の情報	共有システムリソースを介した認可されていない意図しない情報転送を防止する。	・ SC-04 共有システムリソース内の情報	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。
	03.13.05	撤回	03.13.01に組み込まれた。			
	03.13.06	ネットワーク通信 — デフォルトで拒否 — 例外による許可	デフォルトでネットワーク通信トラフィックを拒否し、例外によりネットワーク通信トラフィックを許可する。	・ SC-07(05) デフォルトで拒否 — 例外による許可	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。
	03.13.07	撤回	03.01.12、03.04.02、03.04.06で扱われている。			
	03.13.08	伝送中および保存中の機密性	伝送中および保存中のCUIの認可されていない開示を防止するため、暗号化のメカニズムを実装する。	・ AC-17(02) 暗号化を使用した機密性および完全性の保護 ・ SC-08 伝送の機密性および完全性 ・ SC-08(01) 暗号保護 ・ SC-28 保管中の情報の保護 ・ SC-28(01) 暗号保護	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。
					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。
	03.13.09	ネットワーク切断	セッションの終了時または [設定：組織が定める期間] の非アクティブ状態の後、通信セッションに関連するネットワーク接続を終了する。	・ SC-10 ネットワーク切断	—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.13.10	暗号鍵の確立および管理	[設定：鍵の生成、配布、保存、アクセス、破棄に関して組織が定める管理要件] に従って、システム内の暗号鍵を確立し、管理する。	・ SC-12 暗号鍵の確立および管理	CPS.PR.AA-01	・ 組織は、承認されたモノとヒト及びプロセスの識別情報と認証情報を発効、管理、確認、取消、監査するプロセスを確立し、実施する。
					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。
	03.13.11	暗号保護	CUIの機密性を保護するために、[設定：組織が定める暗号技術のタイプ] を実装する。	・ SC-13 暗号保護	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。
					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。
					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。
	03.13.12	共同コンピューティングデバイスおよびアプリケーション	a. [設定：リモート起動が許可される、組織が定める例外] を除き、共同コンピューティングデバイスおよびアプリケーションのリモート起動を禁止する。	・ SC-15 共同コンピューティングデバイスおよびアプリケーション	—	—
			b. デバイスに物理的に存在するユーザに、使用中であることを明示的に示す。		—	—
	03.13.13	モバイルコード	a. 許容されるモバイルコードとモバイルコード技術を規定する。	・ SC-18 モバイルコード	—	—
			b. モバイルコードの使用を認可、監視、管理する。		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。
	03.13.14	撤回	技術に固有。			
システムおよび情報の完全性	03.13.15	セッションの真正性	通信セッションの真正性を保護する。	・ SC-23 セッションの真正性	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。
	03.13.16	撤回	03.13.08に組み込まれた。			
	03.14.01	欠陥の修正	a. システムの欠陥を識別、報告、修正する。	・ SI-02 欠陥の修正	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。
					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。
					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。
			b. セキュリティ関連のソフトウェアおよびファームウェアの更新を、更新のリリースから [設定：組織が定める期間] 以内にインストールする。		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。
	03.14.02	悪意のあるコードからの保護	a. 悪意のあるコードを検知して根絶するために、システムの入口と出口に、悪意のあるコードからの保護メカニズムを実装する。	・ SI-03 悪意のあるコードからの保護	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。
			b. 構成管理ポリシーと手順に従って、新しいリリースが利用可能になった時点で悪意のあるコードからの保護メカニズムを更新する。		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。

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
			c. 悪意のあるコードからの保護メカニズムを以下のように構成する。 1. [設定：組織が定める頻度] でシステムのスキャンを実行し、ファイルがダウンロード、オープン、または実行される際に、エンドポイントまたはシステムの入口と出口で、外部ソースからのファイルのリアルタイムスキャンを実行する。 2. 悪意のあるコードの検知に応じて、悪意のあるコードをブロックしたり、検疫したり、その他の緩和措置を講じる。		—	—
	03.14.03	セキュリティアラート、勧告、および指令	a. 外部組織からシステムセキュリティアラート、勧告、指令を継続的に受け取る。	・ SI-05 セキュリティのアラート、勧告、および指令	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。
			b. 必要に応じて、内部システムのセキュリティアラート、勧告、指令を作成し、周知する。		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。
	03.14.04	撤回	03.14.02に組み込まれた。			
	03.14.05	撤回	03.14.02で扱われている。			
	03.14.06	システム監視	a. 以下を検知するためにシステムを監視する。 1. 攻撃および潜在的な攻撃の兆候 2. 認可されていない接続	・ SI-04 システム監視 ・ SI-04(04) インバウンドおよびアウトバウンド通信のトラフィック	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。
			b. 認可されていないシステムの使用を識別する。		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。
			c. インバウンドおよびアウトバウンドの通信トラフィックを監視し、異常または認可されていない活動や状況を検知する。		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。
	03.14.07	撤回	03.14.06に組み込まれた。			
	03.14.08	情報の管理および保持	システム内のCUIおよびシステムから出力されるCUIを、適用される法律、大統領令、指令、規則、ポリシー、基準、ガイドライン、および運用要件に従って管理し、保持する。	・ SI-12 情報管理および保持	—	—
					CPS.PR.DS-01	・ 組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。
計画	03.15.01	ポリシーおよび手順	a. CUIの保護のためのセキュリティ要件を満たすために必要なポリシーおよび手順を策定し、文書化し、組織の職員または役割に周知する。	・ AC-01 ポリシーおよび手順 ・ AT-01 ポリシーおよび手順 ・ AU-01 ポリシーおよび手順 ・ CA-01 ポリシーおよび手順 ・ CM-01 ポリシーおよび手順 ・ IA-01 ポリシーおよび手順 ・ IR-01 ポリシーおよび手順 ・ MA-01 ポリシーおよび手順 ・ MP-01 ポリシーおよび手順 ・ PE-01 ポリシーおよび手順 ・ PL-01 ポリシーおよび手順 ・ PS-01 ポリシーおよび手順 ・ RA-01 ポリシーおよび手順 ・ SA-01 ポリシーおよび手順 ・ SC-01 ポリシーおよび手順 ・ SI-01 ポリシーおよび手順 ・ SR-01 ポリシーおよび手順	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。
			b. [設定：組織が定める頻度] でポリシーおよび手順をレビューし、更新する。		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。

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.15.02	システムセキュリティ計画	a. 以下のようなシステムセキュリティ計画を策定する。 1. システムを構成するコンポーネントを規定する。 2. システムが処理、保存、伝送する情報タイプを識別する。 3. 組織にとって懸念される、システムに対する具体的な脅威を記述する。 4. システムの運用環境と、他のシステムまたはシステムコンポーネントへの依存関係または接続を記述する。 5. システムのセキュリティ要件の概要を示す。 6. セキュリティ要件を満たすために実施されている、または計画されている保全措置を記述する。 7. システムの役割と責任を果たす個人を識別する。 8. CUIの保護に必要なその他の関連情報を含む。	・ PL-02 システムセキュリティおよびプライバシー計画	—	—
			b. [設定：組織が定める頻度] で、システムセキュリティ計画をレビューし、更新する。		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。
			c. システムセキュリティ計画を認可されていない開示から保護する。		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。
	03.15.03	行動指針	a. システムの使用とCUIの保護に関する責任と期待される行動を記述したルールを確立する。	・ PL-04 行動指針	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。
			b. システムへのアクセスを必要とする個人にルールを提供する。		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。
			c. CUIおよびシステムへのアクセスを認可する前に、行動指針を読み、理解し、遵守することに同意することを示す文書化された確認書を個人から受け取る。		—	—
			d. [設定：組織が定める頻度] で、行動指針をレビューし、更新する。		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。
システムおよびサービスの取得	03.16.01	セキュリティエンジニアリングの原則	システムおよびシステムコンポーネントの開発または変更に、[設定：組織が定めるシステムセキュリティエンジニアリングの原則] を適用する。	・ SA-08 セキュリティおよびプライバシーエンジニアリングの原則	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。
	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. システムコンポーネントのサポートが開発元、ベンダー、または製造事業者から受けられなくなった場合は、システムコンポーネントを交換する。	・ SA-22 サポートされていないシステムコンポーネント	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。
			b. 交換不可能なサポートされていないコンポーネントについて、リスク軽減のためのオプション、またはサポート継続のための代替ソースを提供する。		—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-171から参照される NIST SP 800-53 (Rev.5 Release 5.1.1)	サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
ファミリ	管理策ID	分類	要求事項	管理策名称（中位ベースライン）	対策要件ID	対策要件
	03.16.03	外部システムサービス	a. CUIの処理、保存、または伝送に使用される外部システムサービスのプロバイダに対し、[設定：組織が定めるセキュリティ要件] に準拠することを要求する。	・ SA-09 外部システムサービス	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。
			b. 外部サービスプロバイダとの共有責任を含め、外部システムサービスに関するユーザの役割と責任を規定し、文書化する。		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。
			c. 外部サービスプロバイダによるセキュリティ要件への準拠を継続的に監視するためのプロセス、方法、手法を導入する。		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。
					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。
サプライチェーンの リスクマネジメント	03.17.01	サプライチェーンのリスクマネジメント計画	a. システム、システムコンポーネント、またはシステムサービスの研究開発、設計、製造、取得、引渡し、統合、運用、メンテナンス、および廃棄に関連するサプライチェーンのリスクを管理するための計画を策定する。	・ SR-02サプライチェーンのリスクマネジメント計画	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。
			b. [設定：組織が定める頻度] で、サプライチェーンのリスクマネジメント計画をレビューし、更新する。		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。
			c. サプライチェーンのリスクマネジメント計画を認可されていない開示から保護する。		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。
	03.17.02	取得戦略、ツール、方法	サプライチェーンリスクを識別、保護、軽減するための取得戦略、契約ツール、調達方法を策定し、実施する。	・ SR-05 獲得戦略、ツール、および方法	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。
	03.17.03	サプライチェーンの要件およびプロセス	a. サプライチェーン要素およびプロセスにおける弱点または欠陥を識別し、これに対処するためのプロセスを確立する。	・ SR-03 サプライチェーンの管理策およびプロセス	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。
			b. システム、システムコンポーネント、またはシステムサービスに対するサプライチェーンリスクから保護し、サプライチェーン関連のイベントによる被害や影響を抑制するために、[設定：組織が定めるセキュリティ要件] を実施する。		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シージャを策定し、運用する。
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。	

D.3 ISO/IEC 27001:2022 附属書Aの管理策群と「サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1」との対応表

ISO/IEC 27001:2022 附属書A			サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
管理策ID		管理策	対策要件ID	対策要件
5 組織的管理策	5.1 情報セキュリティのための方針群	情報セキュリティ方針及びトピック固有の方針は、これを定義し、管理層が承認し、発行し、関連する要員及び関連する利害関係者に伝達し、認識させ、あらかじめ定めた間隔で、及び重大な変化が発生した場合にレビューしなければならない。	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。
			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。
	5.2 情報セキュリティの役割及び責任	情報セキュリティの役割及び責任は、組織のニーズに従って定め、割り当てなければならない。	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。
			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。
			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。
			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。
	5.3 職務の分離	相反する職務及び相反する責任範囲は、分離しなければならない。	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。
	5.4 管理層の責任	管理層は、組織の確立された情報セキュリティ方針、トピック固有の方針及び手順に従った情報セキュリティの適用を、すべての要員に要求しなければならない。	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。
			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。
	5.5 関係当局との連絡	組織は、関係当局との連絡体制を確立し、維持しなければならない。	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。
	5.6 専門組織との連絡	組織は、情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との連絡体制を確立し、維持しなければならない。	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。
			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。
	5.7 脅威インテリジェンス	情報セキュリティの脅威に関連する情報を収集及び分析し、脅威インテリジェンスを構築しなければならない。	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。
			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。
	5.8 プロジェクトマネジメントにおける情報セキュリティ	情報セキュリティをプロジェクトマネジメントに組み入れなければならない。	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。

ISO/IEC 27001:2022 附属書A			サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
管理策ID		管理策	対策要件ID	対策要件
	5.9 情報およびその他の関連資産の目録	情報およびその他の関連資産の目録を、それぞれの管理責任者を含めて作成し、維持しなければならない。	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。
			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。
	5.10 情報およびその他の関連の許容される利用	情報およびその他の関連の許容される利用に関する規則及び取扱手順は、明確にし、文書化し、実施しなければならない。	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。
	5.11 資産の返却	要員及び必要に応じてその他の利害関係者は、雇用、契約又は合意の変更又は終了時に、自らが所持する組織の資産の全てを返却しなければならない。	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。
			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シージャを策定し、運用する。
	5.12 情報の分類	情報は、機密性、完全性、可用性及び関連する利害関係者の要求事項に基づく組織の情報セキュリティのニーズに従って分類しなければならない。	CPS.PR.DS-01	・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。
			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。
	5.13 情報のラベル付け	情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施することが望ましい。	CPS.PR.DS-01	・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。
	5.14 情報の転送	情報の転送の規則、手順又は合意を、組織内及び組織路と他の関係者との間の全ての種類の転送手段に関して備えなければならない。	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。
	5.15 アクセス制御	情報およびその他の関連資産への物理的及び論理的アクセスを制御するための規則を、事業場及び情報セキュリティの要求事項に基づいて確立し、実施しなければならない。	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。
	5.16 識別情報の管理	識別情報のライフサイクル全体を管理しなければならない。	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。
	5.17 認証情報	認証情報の割当及び管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理しなければならない。	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。
	5.18 アクセス権	情報およびその他の関連資産へのアクセス権は、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除しなければならない。	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。
	5.19 供給者関係における情報セキュリティ	供給者の製品又はサービスの利用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施しなければならない。	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。

ISO/IEC 27001:2022 附属書A		サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
管理策ID	管理策	対策要件ID	対策要件
5.20 供給者との合意における情報セキュリティの取扱い	供給者関係の種類に応じて、関連する情報セキュリティ要求事項を確立し、各供給者と合意しなければならない。	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。
5.21 ICTサプライチェーンにおける情報セキュリティの管理	ICT製品およびサービスのサプライチェーンに関する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施しなければならない。	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。
5.22 供給者のサービス提供の監視、レビュー及び変更管理	組織は、供給者の情報セキュリティの活動及びサービス提供を定常的に監視し、レビューし、評価し、変更を管理しなければならない。	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。
		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シージャを策定し、運用する。
		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。
5.23 クラウドサービスの利用における情報セキュリティ	クラウドサービスの調達、利用、管理及び利用終了のプロセスを、組織の情報セキュリティ要求事項に従って確立しなければならない。	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。
5.24 情報セキュリティインシデント管理の計画策定及び準備	組織は、情報セキュリティインシデント管理のプロセス、役割及び責任を定め、確立し、伝達することによって、情報セキュリティインシデント管理を計画し、準備しなければならない。	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。
		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。
5.25 情報セキュリティ事象の評価及び決定	組織は情報セキュリティ事象を評価し、それらを情報セキュリティインシデントに分類するか否かを決定しなければならない。	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。
		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。
		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。
5.26 情報セキュリティインシデントへの対応	情報セキュリティインシデントは、文書化した手順に従って対応しなければならない。	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。
5.27 情報セキュリティインシデントからの学習	情報セキュリティインシデントから得られた知識は、情報セキュリティ管理策を強化し、改善するために用いなければならない。	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。
		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。

ISO/IEC 27001:2022 附属書A			サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
管理策ID		管理策	対策要件ID	対策要件
	5.28 証拠の収集	組織は、情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための手順を確立し、実施しなければならない。	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。
			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。
	5.29 事業の中断・阻害時の情報セキュリティ	組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画しなければならない。	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。
	5.30 事業継続のためのICTの備え	事業継続の目的及びICT継続の要求事項に基づいて、ICTの備えを計画し、実施し、維持し、試験しなければならない。	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。
			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。
	5.31 法令、規制及び契約上の要求事項	情報セキュリティに関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組を特定し、文書化し、また、最新に保たなければならない。	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。
	5.32 知的財産権	組織は知的財産権を保護するための適切な手順を実施しなければならない。	—	—
	5.33 記録の保護	記録は、消失、破壊、改ざん、認可されていないアクセスおよび不正な流出から保護しなければならない。	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。
	5.34 プライバシー及びPIIの保護	組織は、適用される法令、規制及び契約上の要求事項に従って、プライバシー及びPIIの保護に関する要求事項を特定し、満たさなければならない。	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。
	5.35 情報セキュリティの独立したレビュー	人、プロセス及び技術を含む、情報セキュリティおよびその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施しなければならない。	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。
6 人的管理策	5.36 情報セキュリティのための方針群、規則及び標準の遵守	組織の情報セキュリティ方針、トピック固有の方針、規則及び標準を遵守していることを、定期的にレビューしなければならない。	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。
	5.37 操作手順書	情報処理設備の操作手順は、文書化し、必要とする要員に対して利用可能にしなければならない。	—	—
	6.1 選考	要因になる全ての候補者について経歴などの確認は、適用される法令、規制及び倫理を考慮に入れて、組織に加わる前に、及びその後継続的に行わなければならない。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行わなければならない。	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。
	6.2 雇用条件	雇用契約書には、情報セキュリティに関する要員及び組織の責任を記載しなければならない。	—	—

ISO/IEC 27001:2022 附属書A			サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
管理策ID		管理策	対策要件ID	対策要件
	6.3 情報セキュリティの意識向上、教育及び訓練	組織の要因及び関連する利害関係者は、職務に関連する組織の情報セキュリティ方針、トピック固有の方針および手順についての、適切な、情報セキュリティに関する意識向上プログラム、教育及び訓練を受けなければならない、また、定期的な更新を受けなければならない。	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。
			CPS.PR.AT-02	・組織は、自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。
	6.4 懲戒手続	情報セキュリティ方針違反を犯した要員及びその他の関連する利害関係者に対して処置を取るために、懲戒手続を正式に定め、伝達しなければならない。	—	—
	6.5 雇用の終了又は変更後の責任	雇用の終了又は変更の後もお有効な情報セキュリティに関する責任及び義務を定め、施行し、関連する要員及びその他の利害関係者に伝達しなければならない。	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。
	6.6 秘密保持契約又は守秘義務契約	情報保護に対する組織のニーズを反映する秘密保持契約又は守秘義務契約は、特定し、文書化し、定期的にレビューし、要員及びその他の関連する利害関係者が署名しなければならない。	—	—
	6.7 リモートワーク	組織の構外でアクセス、処理又は保存される情報を保護するために、要員が遠隔で作業をする場合のセキュリティ対策を実施しなければならない。	—	—
	6.8 情報セキュリティ事象の報告	組織は、要員が発見した又は疑いをもった情報セキュリティ事象を、適切な連絡経路を通して時期を失わずに報告するための仕組みを設けなければならない。	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。
			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。
7 物理的管理策	7.1 物理的セキュリティ境界	情報およびその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いなければならない。	—	—
	7.2 物理的入退	セキュリティを保つべき領域は、適切な入退管理策及びアクセス場所（受付など）によって保護しなければならない。	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。
	7.3 オフィス、部屋及び施設のセキュリティ	オフィス、部屋及び施設に対する物理的セキュリティを設計し、実装しなければならない。	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。
	7.4 物理的セキュリティの監視	施設は、認可していない物理的アクセスについて、継続的に監視しなければならない。	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。
	7.5 物理的及び環境的脅威からの保護	自然災害及びその他の意図的又は意図的でない、インフラストラクチャに対する物理的脅威などの物理的及び環境的脅威に対する保護を設計し、実装しなければならない。	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。
	7.6 セキュリティを保つべき領域での作業	セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実装しなければならない。	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。
	7.7 クリアデスク・クリアスクリーン	書類及び取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定め、適切に実施しなければならない。	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。

ISO/IEC 27001:2022 附属書A			サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
管理策ID		管理策	対策要件ID	対策要件
	7.8 装置の設置及び保護	装置は、セキュリティを保って設置し、保護しなければならない。	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。
			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。
	7.9 構外にある資産のセキュリティ	構外にある資産を保護しなければならない。	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。
	7.10 記憶媒体	記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理しなければならない。	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。
	7.11 サポートユーティリティ	情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保護しなければならない。	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。
	7.12 ケーブル配線のセキュリティ	電源ケーブル、データ伝送ケーブル又は情報サービスを支援するケーブルの配線は、傍受、妨害又は損傷から保護しなければならない。	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。
	7.13 装置の保守	装置は、情報の可用性、完全性及び機密性を維持することを確実にするために、正しく保守しなければならない。	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。
	7.14 装置のセキュリティを保った処分又は再利用	記憶媒体を内蔵した装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保てるよう上書きしていることを確実にするために、検証しなければならない。	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。
8 技術的管理策	8.1 利用者エンドポイント機器	利用者エンドポイント機器に保存されている情報、処理される情報、又は利用者エンドポイント機器を介してアクセス可能な情報を保護しなければならない。	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。
			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。
	8.2 特権的アクセス権	特権的アクセス権の割当て及び利用は、制限し、管理しなければならない。	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。
			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。
	8.3 情報へのアクセス制限	情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制限しなければならない。	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。
	8.4 ソースコードへのアクセス	ソースコード、開発ツール、及びソフトウェアライブラリへの読取り及び書き込みアクセスを適切に管理しなければならない。	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。

ISO/IEC 27001:2022 附属書A			サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
管理策ID		管理策	対策要件ID	対策要件
	8.5 セキュリティを保った認証	セキュリティを保った認証技術及び手順を、情報へのアクセス制限、及びアクセス制御に関するトピック固有の方針に基づいて備えなければならない。	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。
			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。
	8.6 容量・能力の管理	現在の及び予備される容量・能力の要求事項に合わせて、資源の利用を監視し調整しなければならない。	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。
	8.7 マルウェアに対する保護	マルウェアに対する保護を実施し、利用者の適切な認証によって支援しなければならない。	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。
			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。
			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。
			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。
	8.8 技術的ぜい弱性の管理	利用中の情報システムの技術的ぜい弱性に関する情報を獲得しなければならない。また、そのようなぜい弱性に組織がさらされている状況を評価し、適切な手段をとらなければならない。	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。
			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。
			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。
	8.9 構成管理	ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティ構成を含む構成を確立し、文書化し、実装し、監視し、レビューしなければならない。	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。
	8.10 情報の削除	情報システム、装置又はその他の記憶媒体に保存している情報は、必要でなくなった時点で削除しなければならない。	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。

ISO/IEC 27001:2022 附属書A		サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
管理策ID	管理策	対策要件ID	対策要件
8.11 データマスキング	データマスキングは、適用される法令等を考慮して、組織のアクセス制御に関するトピック固有の方針及びその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用しなければならない。	CPS.PR.DS-01	・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。
		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。
		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。
8.12 データ漏えい防止	データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存又は送信するシステム、ネットワーク及びその他の装置に適用しなければならない。	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。
		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。
		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。
8.13 情報のバックアップ	合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェア及びシステムのバックアップを維持し、定期的に検査しなければならない。	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。
		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。
		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。
8.14 情報処理施設・設備の冗長性	情報処理施設・設備は、可用性の要求事項を満たすのに十分な冗長性をもって、導入しなければならない。	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。
		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、十分なりソース（例：ヒト、モノ、システム）を確保する。
		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、十分なりソース（例：ヒト、モノ、システム）を確保する。
8.15 ログ取得	活動、例外処理、過失及びその他の関連する事象を記録したログを取得し、保存し、保護し、分析しなければならない。	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。
		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。
		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。
8.16 監視活動	情報セキュリティインシデントの可能性を評価するために、ネットワーク、システム及びアプリケーションについて異常な挙動がないか監視し、適切な処置を講じなければならない。	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。
		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。
		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。
		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。
8.17 クロックの同期	組織が使用する情報処理システムのクロックは、組織が採用した時刻源と同期させなければならない。	—	—
8.18 特徴的なユーティリティプログラムの使用	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。	—	—
8.19 運用システムへのソフトウェアの導入	運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施しなければならない。	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。
		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。

ISO/IEC 27001:2022 附属書A			サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.1	
管理策ID		管理策	対策要件ID	対策要件
	8.20 ネットワークセキュリティ	システム及びアプリケーション内の情報を保護するために、ネットワーク及びネットワーク装置のセキュリティを保ち、管理し、制御しなければならない。	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。
	8.21 ネットワークサービスのセキュリティ	ネットワークサービスのセキュリティ機能、サービスレベル及びサービスの要求事項を特定し、実装し、監視しなければならない。	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。
	8.22 ネットワークの分離	情報サービス、利用者及び情報システムは、組織のネットワーク上で、グループごとに分離しなければならない。	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。
	8.23 ウェブフィルタリング	悪意のあるコンテンツにさらされることを減らすために、外部ウェブサイトへのアクセスを管理しなければならない。	—	—
	8.24 暗号の利用	暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施しなければならない。	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。
			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。
			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。
	8.25 セキュリティに配慮した開発のライフサイクル	ソフトウェア及びシステムのセキュリティに配慮した開発のための規則を確立し、適用しなければならない。	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。
	8.26 アプリケーションセキュリティの要求事項	アプリケーションを開発又は取得する場合、情報セキュリティ要求事項を特定し、規定し、承認しなければならない。	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。
	8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則	セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの開発活動に対して適用しなければならない。	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。
	8.28 セキュリティに配慮したコーディング	セキュリティに配慮したコーディングの原則をソフトウェア開発に適用しなければならない。	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。
	8.29 開発及び受入れにおけるセキュリティテスト	セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施しなければならない。	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。
	8.30 外部委託による開発	組織は、外部委託したシステム開発に関する活動を指揮し、監視し、レビューしなければならない。	—	—
	8.31 開発環境、テスト環境及び本番環境の分離	開発環境、テスト環境及び本番環境は、分離してセキュリティを保つことが望ましい。	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。
	8.32 変更管理	情報処理設備及び情報処理システムの変更は、変更管理手順に従わなければならない。	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。
	8.33 テスト用情報	テスト用情報は、適切に選定し、保護し、管理しなければならない。	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。
	8.34 監査におけるテスト用の情報システムの保護	運用システムのアセスメントを伴う監査におけるテスト及びその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意しなければならない。	—	—