添付D　海外の主要規格との対応関係

D．1　NIST Cybersecurity Framework 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」との対応表

NIST Cyberseucurity Framework v1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
特定（ID）	AM-1	自組織内の物理デバイスとシステムが、目録作成されている。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。
	AM-2	自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。		
	AM-3	組織内の通信とデータフロー図が、作成されている。	CPS.AM-4	・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。
	AM-4	外部情報システムが、カタログ作成されている。	CPS.AM-5	・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。
	AM-5	リソース（例：ハードウェア、デバイス、データ、時間、人員、ソフトウェア）が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。	CPS.AM-6	・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。
	AM-6	全労働力と利害にある第三者（例：サプライヤー、顧客、パートナー）に対してのサイバーセキュリティ上の役割と責任が、定められている。	CPS.AM-7	・自組織および関係する他組織のサイバーセキュリティ上の役割と責任を定める。
	BE-1	サプライチェーンにおける自組織の役割が、識別され、周知されている。	CPS.BE-1	・サプライチェーンにおいて、自組織が担う役割を特定し共有する。
	BE-2	重要インフラとその産業分野における自組織の位置付けが、識別され、周知されている。		
	BE-3	組織のミッション、目標、活動の優先順位が、定められ、周知されている。	CPS.BE-2	・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者(サプライヤー、第三者プロバイダ等を含む)に共有する。
	BE-4	重要サービスを提供する上での依存関係と重要な機能が、定められている。	CPS.BE-3	・自組織が事業を継続する上での自組織およ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する。
	BE-5	重要サービスの提供を支援するレジリエンスに関する要求事項が、すべてのオペレーション状況（例：脅迫・攻撃下、復旧時、通常時等）について定められている。	CPS.AT-1	・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.AT-2	・自組織におけるセキュリティインシデントに関係しうる、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。
			CPS.IP-5	・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。
			CPS.RP-1	・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.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。
			CPS.RP-3	・自然災害時における対応方針および対応手順を定めている事業継続計画又は緊急事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。
	GV-1	自組織のサイバーセキュリティポリシーが、定められ、周知されている。	CPS.GV-1	・セキュリティポリシーを策定し、自組織および関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。
	GV-2	サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。		
	GV-3	プライバシーや人権に関する義務を含む、サイバーセキュリティに関する法規制上の要求事項が、理解され、管理されている。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。
	GV-4	ガバナンスとリスクマネジメントプロセスがサイバーセキュリティリスクに対応している。	CPS.GV-4	・セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。
	RA-1	資産の脆弱性が識別され、文書化されている。	CPS.RA-1	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。
	RA-2	サイバー脅威に関する情報が、複数の情報共有フォーラムおよび複数のソースから入手されている。	CPS.RA-2	・セキュリティ対応組織(SOC/CSIRT)は、組織の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、対応および活用するプロセスを確立する。
	RA-3	内部および外部からの脅威が、識別され、文書化されている。	CPS.RA-3	・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。

NIST Cyberseucurity Framework v1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
	RA-4	ビジネスに対する潜在的な影響とその発生可能が、識別されている。	CPS.RA-4	・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。 ・IoT機器および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。
	RA-5	脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。	CPS.RA-5	・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。
	RA-6	リスク対応が、識別され、優先順位付けされている。	CPS.RA-6	・リスクアセスメントに基づき、発生しう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。 ・IoT機器および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および関連するセーフティのリスクに対して適宜対応する。
	RM-1	リスクマネジメントプロセスが、組織の利害関係者によって定められ、管理され、承認されている。	CPS.RM-1	・自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。
	RM-2	組織のリスク許容度が、決定され、明確に表現されている。	CPS.RM-2	・リスクアセスメント結果およびサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。
	RM-3	自組織によるリスク許容度の決定が、重要インフラにおける組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。		
	SC-1	サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別され、管理され、合意されている。	CPS.SC-1	・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、その内容について取引先と合意する。
	SC-2	情報システム、コンポーネント、サービスのサプライヤーと第三者であるパートナーが、識別され、優先順位付けられ、サイバーサプライチェーンのリスクアセスメントプロセスにより評価されている。	CPS.SC-2	・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、優先付けをし、評価する。
	SC-3	サプライヤーおよび第三者であるパートナーとの契約が、組織のサイバーセキュリティプログラムやサイバーサプライチェーンのリスクマネジメント計画の目的を達成するための適切な対策の実施に活用されている。	CPS.SC-3	・外部の組織との契約を行う場合、目的およ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のセキュリティマネジメントが適合していることを確認する。
	SC-4	サプライヤおよび第三者であるパートナーが、監査、テストの結果、またはその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている。	CPS.SC-6	・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、または他の形式の評価を使用して定期的に評価する。
	SC-5	対応・復旧計画の策定とテストが、サプライヤーおよび第三者プロバイダと共に行われている。	CPS.SC-9	・サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。
防御（PR）	AC-1	認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。	CPS.AC-1	・承認されたモノとヒトおよ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。
	AC-2	資産に対する物理アクセスが、管理され、保護されている。	CPS.AC-2	・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。
	AC-3	リモートアクセスが、管理されている。	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する。
			CPS.AC-4	・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。
	AC-4	アクセスの許可および認可が、最小権限の原則および役割の分離の原則を組み入れて、管理されている。	CPS.AC-5	・職務および責任範囲（例：ユーザー／システム管理者)を適切に分離する 。
			CPS.AC-6	・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。
	AC-5	ネットワークの完全性が、保護されている（例：ネットワークの分離、ネットワークのセグメント化）。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜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)等してネットワークの完全性を保護する。

NIST Cyberseucurity Framework v1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
	AC-6	IDは、ID利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで活用されている。	CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。
	AC-7	ユーザ、デバイス、その他の資産は、トランザクションのリスク（例：個人のセキュリティ及びプライバシーのリスク、その他組織上のリスク）の度合いに応じた認証（例えば、一要素、多要素）が行われている。	CPS.AC-6	・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。
			CPS.AC-9	・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）に見合う形で認証・認可する。
	AT-1	すべてのユーザは、情報が周知され、トレーニングが実施されている。	CPS.AT-1	・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。
	AT-2	権限を持つユーザが、自身の役割と責任を理解している。		
	AT-3	第三者である利害関係者（例：サプライヤー、顧客、パートナー）が、自身の役割と責任を理解している。	CPS.AT-2	・自組織におけるセキュリティインシデントに関係しうる、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。
	AT-4	上級役員（セキュリティ担当役員）が、自身の役割と責任を理解している。	CPS.AT-1	・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。
	AT-5	物理セキュリティおよびサイバーセキュリティの担当者が、自身の役割と責任を理解している。		
	DS-1	保存されているデータが、保護されている。	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。
	DS-2	伝送中のデータが、保護されている。	CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。
			CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。
	DS-3	資産は、撤去、譲渡、廃棄に至るまで、正式に管理されている。	CPS.IP-6	・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。
	DS-4	可用性を確保するのに十分な容量が、維持されている。	CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する。
			CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。
	DS-5	データ漏えいに対する防御対策が、実装されている。	CPS.DS-8	・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。
			CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。
	DS-6	完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されている。	CPS.DS-10	・IoT機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。
			CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する。
	DS-7	開発・テスト環境が、実稼働環境から分離されている。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜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)等してネットワークの完全性を保護する。
	DS-8	完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている。	CPS.DS-12	・ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。
	IP-1	情報技術／産業用制御システムのベースラインとなる構成は、セキュリティの原則（例：最低限の機能性の概念）を組み入れて、を定められ、維持されている。	CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。
			CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。
	IP-2	システムを管理するためのシステム開発ライフサイクルが、実装されている。	CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。
	IP-3	構成変更管理プロセスは、策定されている。	CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。
	IP-4	情報のバックアップが、実施され、維持され、テストされている。	CPS.IP-4	・構成要素（IoT機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする。
	IP-5	組織の資産の物理的な運用環境に関するポリシーと規制が、満たされている。	CPS.IP-5	・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。

NIST Cyberseucurity Framework v1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
	IP-6	データは、ポリシーに従って破壊されている。	CPS.IP-6	・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。
	IP-7	防御プロセスは、改善されている。	CPS.IP-7	・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改善する。
	IP-8	防御技術の有効性に関する情報が、共有されている。	CPS.IP-8	・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。
	IP-9	（インシデント対応及び事業継続）対応計画と（インシデントからの復旧及び災害復旧）復旧計画が、策定され、管理されている。	CPS.RP-1	・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.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。
	IP-10	対応計画と復旧計画が、テストされている。	CPS.AT-2	・自組織におけるセキュリティインシデントに関係しうる、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。
	IP-11	サイバーセキュリティには、人事に関わるプラクティス（例：アクセス権限の無効化、人員のスクリーニング）が含まれている。	CPS.IP-9	・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。
	IP-12	脆弱性管理計画が、作成され、実装されている。	CPS.IP-10	・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。
	MA-1	組織の資産の保守と修理は、承認・管理されたツールを用いて実施され、ログが記録されている。	CPS.MA-1	・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。 ・可能であれば、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。
	MA-2	組織の資産に対する遠隔保守は、承認を得て、ログが記録され、不正アクセスを防止した形式で実施されている。	CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、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。
	PT-1	監査記録／ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。	CPS.PT-1	・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、そうした記録を実施して、レビューする。
	PT-2	リムーバルメディアは、保護され、その使用がポリシーに従って制限されている。	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。
	PT-3	最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。		
	PT-4	通信（情報）ネットワークと制御ネットワークが、保護されている。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜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)等してネットワークの完全性を保護する。
	PT-5	メカニズム（例：フェイルセーフ、負荷分散、ホットスワップ）が、平時及び緊急時においてレジリエンスに関する要件を達成するために実装されている。	CPS.PT-3	・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。
検知（DE）	AE-1	ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが定められ、管理されている。	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。
	AE-2	検知したイベントは、攻撃の標的と手法を理解するために分析されている。	CPS.AE-2	・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)を立ち上げ、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。
	AE-3	イベントデータは、複数の情報源やセンサーから収集され、相互分析されている。	CPS.AE-3	・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。
	AE-4	イベントがもたらす影響が、判断されている。	CPS.AE-4	・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。
	AE-5	インシデント警告の閾値が、定められている。	CPS.AE-5	・セキュリティ事象の危険度の判定基準を定める。
	CM-1	ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。

NIST Cyberseucurity Framework v1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
	CM-2	物理環境は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	CPS.CM-2	・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および記録、監視を実施する。
	CM-3	人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）および他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。
	CM-4	悪質なコードは、検出されている。	CPS.CM-3	・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。 ・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。
			CPS.CM-4	・サイバー空間から受ける情報の完全性および真正性を動作前に確認する。
	CM-5	不正なモバイルコードは、検出されている。	CPS.CM-3	・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。 ・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。
			CPS.CM-4	・サイバー空間から受ける情報の完全性および真正性を動作前に確認する。
	CM-6	外部サービスプロバイダの活動は、潜在的なサイバーセキュリティイベントを検知できるようにモニタリングされている。	CPS.CM-5	・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モニタリングする。
	CM-7	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが、実施されている。	CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）および他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。
	CM-8	脆弱性スキャンが、実施されている。	CPS.CM-7	・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。
	DP-1	検知に関する役割と責任は、説明責任を果たせるように明確に定義されている。	CPS.DP-1	・セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知における自組織とサービスプロバイダが担う役割と負う責任を明確にする。
	DP-2	検知活動は必要なすべての要求事項を満たしている。	CPS.DP-2	・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する。
	DP-3	検知プロセスが、テストされている。	CPS.DP-3	・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。
	DP-4	イベント検知情報が、周知されている。	CPS.RP-1	・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。
	DP-5	検知プロセスが、継続的に改善されている。	CPS.DP-4	・セキュリティ事象の検知プロセスを継続的に改善する。
対応（RS）	RP-1	対応計画が、インシデントの発生中または発生後に実行されている。	CPS.RP-1	・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。
	CO-1	人員は、対応が必要になった時の自身の役割と行動の順序を認識している。	CPS.AT-2	・自組織におけるセキュリティインシデントに関係しうる、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。
	CO-2	インシデントが、定められた基準に沿って報告されている。	CPS.RP-1	・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。
	CO-3	対応計画に従って、情報が共有されている。		
	CO-4	利害関係者との間で調整が、対応計画に従って行われている。	CPS.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。
	CO-5	サイバーセキュリティに関する状況認識を広げるために、外部利害関係者との間で自発的な情報共有が行われている。		
	AN-1	検知システムからの通知は、調査されている。	CPS.AE-3	・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。
	AN-2	インシデントがもたらす影響は、把握されている。	CPS.AN-1	・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。
	AN-3	フォレンジックが、実施されている。	CPS.AN-2	・セキュリティインシデント発生後に、デジタルフォレンジックを実施する。

NIST Cyberseucurity Framework v1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
	AN-4	インシデントは、対応計画に従って分類されている。	CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。
	AN-5	プロセスは、内外のソース（例：内部テスト、セキュリティ情報、セキュリティ研究者）から報告された脆弱性情報を、自組織が受け取り、分析し、対応するために定められている。	CPS.RA-2	・セキュリティ対応組織(SOC/CSIRT)は、組織の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、対応および活用するプロセスを確立する。
	IM-1	対応計画は、学んだ教訓を取り入れられている。	CPS.IM-1	・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、セキュリティ運用プロセスを継続的に改善する。
	IM-2	対応戦略は、更新されている。		
	MI-1	インシデントは、封じ込められている。	CPS.MI-1	・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、影響を低減する対応を行う。
	MI-2	インシデントは、緩和されている。		
	MI-3	新たに特定された脆弱性は、許容できるリスクである場合にはその旨を文書化され、そうでない場合にはリスクが緩和されている。	CPS.RA-4	・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。 ・IoT機器および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.RA-6	・リスクアセスメントに基づき、発生しう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。 ・IoT機器および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および関連するセーフティのリスクに対して適宜対応する。
復旧（RC）	RP-1	復旧計画が、サイバーセキュリティインシデントの発生中または発生後に実施されている。	CPS.RP-3	・自然災害時における対応方針および対応手順を定めている事業継続計画又は緊急事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。
	IM-1	復旧計画は、学んだ教訓を取り入れている。	CPS.IM-2	・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事対応計画を継続的に改善する。
	IM-2	復旧戦略は、更新されている。		
	CO-1	広報活動が、管理されている。	CPS.CO-1	・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。
	CO-2	評判は、インシデント発生後に回復されている。	CPS.CO-2	・事業継続計画又は緊急事対応計画の中に、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。
	CO-3	復旧活動は、内外の利害関係者だけでなく役員と経営陣にも周知されている。	CPS.CO-3	・復旧活動について内部および外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急事対応計画の中に位置づける。

D．２　NIST SP 800-171 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」との対応表

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
アクセス制御	3.1.1	システムアクセスを許可された利用者、許可された利用者を代行して動作するプロセス、またはデバイス(その他のシステムを含めて)に制限する。	・AC-2 アカウント管理 ・AC-3 アクセス制御の実施 ・AC-17 リモートアクセス	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.1.2	システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。	・AC-2 アカウント管理 ・AC-3 アクセス制御の実施 ・AC-17 リモートアクセス	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.1.3	承認された権限付与に従ってCUI のフローを制御する。	・AC-4 情報フロー制御の実施	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜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)等してネットワークの完全性を保護する。	H.Advanced	・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システムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・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。 ・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。
						Basic	・組織は、情報システム及び産業用制御システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、適切に論理的あるいは物理的にネットワークを分離することで、フローの制御を実施する。 ・組織は、産業用制御システムにおいて、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。
				CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	H.Advanced	・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。 ・システムは、システム内（およ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。 ・組織/システムは、定常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およ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。
	3.1.4	共謀のない悪意のあるアクティビティのリスク低減のため、個人の職務を分離する。	・AC-5 職務の分離	CPS.AC-5	・職務および責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H.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御する。 ・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。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・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、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最少化させることができる。 ・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停止できないようにすることができる。
						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、特定の職務権限に対して最小権限の原則を採用する。 －一般のユーザアカウントの権限と、特権アカウントの権限を分離する （非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。） －自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
	3.1.5	具体的なセキュリティ機能と特権アカウントを含め、特権の最小化の原則を採用する。	・AC-6 特権の最小化 ・AC-6(1) 特権の最小化 セキュリティ機能へのアクセスを許可する ・AC-6(5) 特権の最小化 特権アカウント	CPS.AC-5	・職務および責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H.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御する。 ・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。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・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、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最少化させることができる。 ・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停止できないようにすることができる。
						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、特定の職務権限に対して最小権限の原則を採用する。 －一般のユーザアカウントの権限と、特権アカウントの権限を分離する （非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。） －自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
	3.1.6	非セキュリティ機能をアクセスするときは、非特権アカウントまたは役割を使用する。	・AC-6(2) 特権の最小化 非セキュリティ機能の非特権アクセス	CPS.AC-5	・職務および責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H.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御する。 ・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。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・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、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最少化させることができる。 ・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停止できないようにすることができる。
	3.1.7	非特権利用者による特権機能の実行とこのような機能の実行の監査を防止する。	・AC-6(9) 特権の最小化 特権機能の利用の監査 ・AC-6(10) 特権の最小化 特権機能の実行を非特権利用者に禁止する				
	3.1.8	ログイン試行失敗を制限する。	・AC-7 ログイン試行の失敗	CPS.AC-4	・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。	H.Advanced	・情報システム及び産業用制御システム(対応の即時性が求められる一部の例を除く)は、自組織のシステムに対してユーザが連続してログオ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管理者が解除しなければ再ログインできない機能を実装する。
						Advanced	・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対してユーザが連続してログオ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。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.1.9	適用可能なCUI 規則と整合性のあるプライバシーとセキュリティの通知を提供する。	・AC-8 システムの利用に関する通知	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.1.10	非アクティブな時間の経過後、データのアクセス及び閲覧を防止するため、パタンによる不可視化表示を用いてセションロックを使用する。	・AC-11 セションのロック ・AC-11(1) セションのロック パタンによる不可視化表示	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.1.11	定義された条件の後、利用者セションを(自動的に)終了する。	・AC-12 セションの終了	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
	3.1.12	リモートアクセスセションを監視し、制御する。	・AC-17(1) リモートアクセス 自動化された監視／管理	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する。	H.Advanced	・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。 ・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、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。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・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、ユーザおよ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、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の遠隔する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
				CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	Advanced	・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、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。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる。 ・組織は、個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・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、およ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。
						Basic	・組織は、情報システムの外部境界において通信をモニタリングし、制御する。
				CPS.CM-5	・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モニタリングする。	H.Advanced	・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にするよう要求する。 ・組織は、上記で明確化した事項が遵守されているかどうかをモニタリングする。
						Advanced	・組織は、外部サービスプロバイダおよびシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダーおよ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モニタリングする。 ・組織は、外部サービスプロバイダーおよ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。
	3.1.13	リモートアクセスセションの機密性を保護するために暗号メカニズムを採用する。	・AC-17(2) リモートアクセス 暗号化を用いた機密性／完全性の保護	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する。	H.Advanced	・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。 ・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、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。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・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、ユーザおよ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、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の遠隔する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、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。
	3.1.14	管理されたアクセス制御ポイントを介してリモートアクセスをルーティングする。	・AC-17(3) リモートアクセス 管理されたアクセス制御ポイント	CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	H.Advanced	・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。 ・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。
						Advanced	・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、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。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる。 ・組織は、個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・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、およ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。
	3.1.15	特権コマンドのリモート実行とセキュリティ関連情報へのリモートアクセスを許可する。	・AC-17(4) リモートアクセス 特権コマンド／アクセス	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する。	H.Advanced	・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。 ・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、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。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・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、ユーザおよ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、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の遠隔する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件		対策例
	3.1.16	無線のコネクションを許可する前に無線アクセスを許可する。	・AC-18 無線アクセスの制限	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する。	H.Advanced	・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。 ・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、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。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・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、ユーザおよ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、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の炎検を提供する。
						Advanced	・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・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。
						Basic	・組織は、許可しているリモートアクセスのタイプごとに使用制限・構成要件・実装ガイダンス等を定める。 ・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、自組織の情報システム及び産業用制御システムへのリモートアクセスの利用に関する承認ルール等を定める。 ・組織は、自組織のシステムへの無線によるアクセスを許可するのに先立って、無線でシステムにアクセスする権限を与える。
	3.1.17	認証と暗号化を用いて無線アクセスを保護する。	・AC-18(1) 無線アクセス 認証と暗号化	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する。	H.Advanced	・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。 ・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、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。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・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、ユーザおよ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、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の炎検を提供する。
	3.1.18	モバイルデバイスのコネクションを制御する。	・AC-19 携帯機器に対するアクセス制御	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する。	H.Advanced	・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。 ・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、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。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・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、ユーザおよ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、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の炎検を提供する。
						Advanced	・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・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。
				CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.1.19	モバイルデバイス及びモバイルコンピューティングプラットフォーム上のCUI を暗号化する。	・AC-19(5) 携帯機器に対するアクセス制御 デバイス全体／コンテナベースの暗号化	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H.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。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・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。
						Advanced	・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、情報(データ)を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト(電子政府推奨暗号リスト)に記載されたアルゴリズムが選択可能であれば、これを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。 ・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。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リ
	3.1.20	外部システムへのコネクション及び使用を検証し、制御／制限する。	・AC-20 外部情報システムの利用 ・AC-20(1) 外部情報システムの利用 許可された利用の制限	CPS.AM-5	・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。	H.Advanced	・システムは、自組織が利用している外部情報システムサービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・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。 ・組織は、外部プロバイダによる情報システムサービスを使用する際に必要な機能、ポート、プロトコル、および他のサービスを明確にする。
						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 ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。
	3.1.21	外部システム上での組織のポータブルストレージデバイスの使用を制限する。	・AC-20(2) 外部情報システムの利用 ポータブルストレージデバイス	CPS.AM-5	・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。	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 ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。
	3.1.22	公開アクセス可能なシステムにおいて掲載または処理されるCUI を制御する。	・AC-22 公的アクセス可能なコンテンツ	CPS.GV-3	・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。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法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識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)
意識向上と訓練	3.2.1	組織のシステムの責任者、システム管理者、及び利用者が、彼らのアクティビティに関連するセキュリティリスク及びそれらのシステムのセキュリティに関連する適用可能なポリシー、基準、及び手順について周知されていることを、保証する。	・AT-2 セキュリティの意識向上 ・AT-3 ロールベースのセキュリティトレーニング	CPS.AT-1	・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。	H.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。
						Advanced	・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。組織は、CPS.AT-1＜Basic＞の[参考]に記載されている一般的な事項を解説しているコンテンツに加えて、組織によって内容が異なる内容として、例えば、下記の事項を扱うことができる。 － 不審なメールを受信した際の対応手順(どこにどのような内容を連絡すればよいか) － モバイル端末利用の注意点(例：公衆無線LANに接続する際の注意点) － SNSを利用する際の注意点 ・組織は、情報セキュリティ要員の育成とレベル向上のための役割別(例：システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者)のプログラムを作成し、定期的に該当する要員に対して実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の記録を定期的にレビューする。
				CPS.AT-2	・自組織における セキュリティインシデントに関係しうる、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。	Advanced	・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うる関係組織に対して、担当する要員へ割り当てられた役割を遂行するための適切な訓練(例：実際のインシデント発生時を想定した、シミュレーション)、セキュリティ教育を実施を要求し、その実施状況を確認する。 ・組織は、自組織の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する教育・訓練の記録を定期的にレビューする。
						Basic	・組織は、自組織の要員へ割り当てられた役割を遂行するための適切な訓練(例：実際のインシデント発生時を想定した、シミュレーション)、セキュリティ教育を実施を要求し、その実施状況を確認する。 ・組織は、自組織の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する、セキュリティに係る教育・訓練の内容や結果等について記録し、管理する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.2.2	組織の要員が、その割り当てられた情報セキュリティ関連の職務と責任を遂行するために適切に訓練されていることを、保証する。	・AT-2 セキュリティの意識向上 ・AT-3 ロールベースのセキュリティトレーニング	CPS.AT-1	・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。	Advanced	・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。組織は、CPS.AT-1<Basic>の[参考]に記載されている一般的な事項を解説しているコンテンツに加えて、組織によって内容が異なる内容として、例えば、下記の事項を扱うことができる。 － 不審なメールを受信した際の対応手順(どこにどのような内容を連絡すればよいか) － モバイル端末利用の注意点(例:公衆無線LANに接続する際の注意点) － SNSを利用する際の注意点 ・組織は、情報セキュリティ要員の育成とレベル向上のための役割別(例:システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者)のプログラムを作成し、定期的に該当する要員に対して実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の記録を定期的にレビューする。
				CPS.AT-2	・自組織におけるセキュリティインシデントに関係しうる、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。	Advanced	・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うる関係組織に対して、担当する要員へ割り当てられた役割を遂行するための適切な訓練(例:実際のインシデント発生時を想定した、シミュレーション)、セキュリティ教育を実施を要求し、その実施状況を確認する。 ・組織は、自組織の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する教育・訓練の記録を定期的にレビューする。
	3.2.3	内部からの脅威の潜在指標の認識と報告についてのセキュリティ周知訓練を提供する。	・AT-2(2) セキュリティの意識向上 内部の脅威	CPS.AT-1	・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。	H.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。
監査と責任追跡性（説明責任）	3.3.1	非合法の、許可されない、または不適切なシステムアクティビティの監視、分析、調査、及び報告を可能とするために必要な範囲で、システム監査記録を作成、保護、及び維持する。	・AU-2 監査対象のイベント ・AU-3 監査記録の内容 ・AU-3(1) 監査記録の内容 追加の監査情報 ・AU-6 監査記録の監視、分析、及び報告 ・AU-12 監査の生成	CPS.SC-6	・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、または他の形式の評価を使用して定期的に評価する。	H.Advanced	・組織は、契約事項からの逸脱および、その兆候に対する調査・対応のためのプロシージャ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、特に重要な取引先およ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。 ・重要な取引先およ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。
						Advanced	・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。 ・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情報システムが提供する。 ・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。 ・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でレビュー・分析して、契約事項からの逸脱および、その兆候の有無を確認する。 ・チェックリストを用いた取引先による内部監査により、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。
				CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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)管理される。 ・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機器からの監査ログの収集・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。
						Advanced	・情報システム及び産業用制御システムは、監査ログおよ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、監査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。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査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、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
	3.3.2	個別のシステム利用者のアクションが、彼らのアクションについての説明責任を維持可能にするよう、それらの利用者に対して一意に追跡が可能であることを保証する。	・AU-2 監査対象のイベント ・AU-3 監査記録の内容 ・AU-3(1) 監査記録の内容 追加の監査情報 ・AU-6 監査記録の監視、分析、及び報告 ・AU-12 監査の生成	CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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)管理される。 ・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機器からの監査ログの収集・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。
						Advanced	・情報システム及び産業用制御システムは、監査ログおよ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、監査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。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査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、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
	3.3.3	監査された事象をレビューし、アップデートする。	・AU-2(3) 監査対象のイベント レビューとアップデート	CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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)管理される。 ・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機器からの監査ログの収集・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。
						Advanced	・情報システム及び産業用制御システムは、監査ログおよ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、監査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。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査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、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.3.4	監査プロセス失敗の事象においてアラート(警告) を発する。	・AU-5 監査処理エラーへの対応	CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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) 管理される。 ・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機器からの監査ログの収集・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。
						Advanced	・情報システム及び産業用制御システムは、監査ログおよ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、監査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。
	3.3.5	監査記録のレビュー、分析、及び調査のための報告プロセスを集めて相互の関係を比較し、不適切な、疑わしい、または異常なアクティビティの兆候に対応する。	・AU-6(3) 監査記録の監視、分析、及び報告 監査リポジトリとの相互の関連付け	CPS.SC-6	・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、または他の形式の評価を使用して定期的に評価する。	H.Advanced	・組織は、契約事項からの逸脱および、その兆候に対する調査・対応のためのプロシージャ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、特に重要な取引先およ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。 ・重要な取引先およ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。
				CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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) 管理される。 ・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機器からの監査ログの収集・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。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査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、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
	3.3.6	オンデマンド分析と報告をサポートするため、監査の簡素化と報告書生成を提供する。	・AU-7 監査量の低減と報告書の作成	CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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) 管理される。 ・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機器からの監査ログの収集・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。
	3.3.7	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。	・AU-8 タイムスタンプ ・AU-8(1) タイムスタンプ 権威ある時刻ソースとの同期	CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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) 管理される。 ・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機器からの監査ログの収集・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。
	3.3.8	監査情報と監査ツールを不正なアクセス、改変、及び削除から保護する。	・AU-9 監査情報の保護	CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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) 管理される。 ・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機器からの監査ログの収集・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。
						Advanced	・情報システム及び産業用制御システムは、監査ログおよ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、監査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。
	3.3.9	監査機能の管理を特権利用者の一部に制限する。	・AU-9(4) 監査情報の保護 特権利用者のサブセットによるアクセス	CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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) 管理される。 ・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機器からの監査ログの収集・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。
						Advanced	・情報システム及び産業用制御システムは、監査ログおよ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、監査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。
構成管理	3.4.1	個別のシステム開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、及び文書を含めて) のベースライン構成とインベントリを確立し、維持する。	・CM-2 ベースライン構成 ・CM-6 構成設定 ・CM-8 情報システムコンポーネントのインベントリ ・CM-8(1) 情報システムコンポーネントのインベントリ インストレーション／除去中のアップデート	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。	Advanced	・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、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、組織内で規定されたポータブルストレージデバイス(例：USBメモリ)のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						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する。 [参考] 資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第2.1版」(IPA, 2018年)のP.33を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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, 2018年)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。
				CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）および他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・情報システムは、信頼の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる。 ・個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・情報システム及び産業用制御システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
						Basic	・IoT機器、サーバ等を含む資産の型番やソフトウェアのバージョン、サポート期限等を管理する台帳を作成し、定期的に棚卸する。 ・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。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.4.2	組織のシステムで採用された情報技術製品のセキュリティ構成設定を確立し、強制（実施）する。	・CM-2 ベースライン構成 ・CM-6 構成設定 ・CM-8 情報システムコンポーネントのインベントリ ・CM-8(1) 情報システムコンポーネントのインベントリ インストレーション／除去中のアップデート	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。	H.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。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・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。 ※関連する対策要件に、CPS.CM-6がある。 [参考] 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2.1版」(IPA, 2018年)P.30～P.34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, 2018年)のP.21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
				CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。	Advanced	・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、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・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、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法(例：変更実施前に本人にしかわからないセキュリティコードを入力させる)を利用する。 ・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。
						Basic	・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、CPS.AC-1で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、IoT機器の導入前に、搭載されているソフトウェアを確認し、記録する。
	3.4.3	組織のシステムへの変更を追跡、レビュー、承認／非承認、及び監査する。	・CM-3 構成変更管理	CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。	Advanced	・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、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・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、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法(例：変更実施前に本人にしかわからないセキュリティコードを入力させる)を利用する。 ・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。
				CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）および他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる。 ・個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・情報システム及び産業用制御システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
	3.4.4	実装に先立ち、変更のセキュリティへの影響を分析する。	・CM-4 構成変更の監視	CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。	Advanced	・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、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・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、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法(例：変更実施前に本人にしかわからないセキュリティコードを入力させる)を利用する。 ・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。
	3.4.5	組織のシステムへの変更に関連する物理的及び論理的なアクセス制約事項を定義し、文書化し、承認し、強制（実施）する。	・CM-5 変更のためのアクセス制限				
	3.4.6	基本機能のみを提供するように組織のシステムを構成することによって、最小機能の原則を採用する。	・CM-7 機能の最小化	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	H.Advanced	・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。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・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、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
						Advanced	・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。 ・組織は、IoT機器やPC、サーバ以外の機器であっても、複合機等のネットワークにつながる機器に対しては、不要な機能やサービス等を停止する。
	3.4.7	非基本プログラム、機能、ポート、プロトコル、及びサービスの使用を制限、無効化、及び防止する。	・CM-7(1) 機能の最小化 定期的なレビュー ・CM-7(2) 機能の最小化 プログラム実行の防止	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	H.Advanced	・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。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・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、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
	3.4.8	許可されないソフトウェアの使用を防止するために例外による拒否（ブラックリスト）ポリシーを、または許可されたソフトウェアの実行を許可するような例外による許可（ホワイトリスト)ポリシーを適用する。	・CM-7(2) 機能の最小化 プログラム実行の防止 ・CM-7(5) 機能の最小化 許可されたソフトウェア／ホワイトリスト	CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	H.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実行を許可するソフトウェアの一覧(ホワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)を用いてソフトウェアの制限を実施する、あるいは、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。
				CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	H.Advanced	・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。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・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、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
	3.4.9	利用者がインストールしたソフトウェアを管理し、監視する。	・CM-11 利用者がインストールしたソフトウェア	CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	H.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実行を許可するソフトウェアの一覧(ホワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)を用いてソフトウェアの制限を実施する、あるいは、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。
						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。
識別と認証	3.5.1	システム利用者、利用者を代行して動作するプロセス、またはデバイスを識別する。	・IA-2 ユーザ識別及び認証 ・IA-5 認証コードの管理	CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・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。
	3.5.2	組織のシステムへのアクセスの許可に対する必要条件として、それらの利用者、プロセス、またはデバイスのアイデンティティを認証(または検証)する。	・IA-2 ユーザ識別及び認証 ・IA-5 認証コードの管理	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.5.3	多要素認証を、特権アカウントへのローカル及びネットワークアクセスのために、及び非特権アカウントへのネットワークアクセスのために、使用する。	・IA-2(1) ユーザ識別及び認証 特権アカウントへのネットワークアクセス ・IA-2(2) ユーザ識別及び認証 非特権アカウントへのネットワークアクセス ・IA-2(3) ユーザ識別及び認証 特権アカウントへのローカルアクセス	CPS.AC-6	・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	H.Advanced	・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多要素認証を実施する。 ・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、リプ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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・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。 ・情報システムは、自組織のシステムについて管理者アカウントの無効化等制限が実施できない場合には、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多要素認証を要求する。 ・情報システムにおけるデフォルトの管理者アカウントは、原則無効化する。 ・情報システムは、権限付与等の特権操作を実施する場合には、利用ユーザアカウントに対して必要最小限の特権操作権限を付与する。
	3.5.4	特権及び非特権アカウントへのネットワークアクセスのために、リプレイ耐性のある認証メカニズムを採用する。	・IA-2(8) ユーザ識別及び認証 特権アカウントへのネットワークアクセスーリプレイ耐性 ・IA-2(9) ユーザ識別及び認証 非特権アカウントへのネットワークアクセスーリプレイ耐性	CPS.AC-6	・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	H.Advanced	・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多要素認証を実施する。 ・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、リプ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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
	3.5.5	定義された期間について、識別コードの再利用を禁止する。	・IA-4 識別子の管理	CPS.AC-1	・承認されたモノとヒトおよ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。	Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・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。 ・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。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・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。 ・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。
						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、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別(例：一般ユーザ/システム管理者/共有ユーザ/一時的なユーザ)を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・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、その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実装する。ポリシーの内容の例としては、下記が挙げられる。 －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。 ・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、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。
				CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・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。
	3.5.6	定義された非アクティブな期間の後、識別子を無効化する。	・IA-4 識別子の管理	CPS.AC-1	・承認されたモノとヒトおよ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。	Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・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。 ・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。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・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。 ・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。
						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、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別(例：一般ユーザ/システム管理者/共有ユーザ/一時的なユーザ)を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・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、その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実装する。ポリシーの内容の例としては、下記が挙げられる。 －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。 ・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、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。
	3.5.7	新しいパスワードが作成されるとき、最小パスワード複雑性及び文字列の変更を強制(実施)する。	・IA-5(1) 認証コードの管理 パスワードベース認証	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.5.8	規定された生成回数の間、パスワードの再利用を禁止する。	・IA-5(1) 認証コードの管理 パスワードベース認証	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.5.9	永久パスワードへ直ちに変更するようなときのシステムログインのために一時的パスワードの使用を許可する。	・IA-5(1) 認証コードの管理 パスワードベース認証	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.5.10	暗号学的に保護されたパスワードのみを格納及び送信する。	・IA-5(1) 認証コードの管理 パスワードベース認証	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.5.11	認証情報のフィードバックを目に見えないようにする。	・IA-6 認証コードのフィードバック	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
インシデント対応	3.6.1	適切な準備、検知、分析、抑制（封じ込め）、リカバリ、及び利用者対応アクティビティを含めて、組織のシステムのための運用上のインシデントハンドリング能力を確立する。	・IR-2 インシデント対応のトレーニング ・IR-4 インシデントの対応 ・IR-5 インシデントの監視 ・IR-6 インシデントの報告 ・IR-7 インシデント対応の支援	CPS.SC-9	・サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	H.Advanced	・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、たとえば、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。
						Advanced	・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。
				CPS.AE-2	・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)を立ち上げ、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。	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（CPS.AE-3を参照） ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・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（プロセスの内容については、CPS.RP-1等を参照）。 ・組織およ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 [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 ～ 機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年)等を参照することが望ましい。
				CPS.AE-4	・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。	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、当該セキュリティ事象の全容を把握する。 ・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。
				CPS.RP-1	・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。	Basic	・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。当該プロセスには、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, 2015年)、SP 800-61 rev.1 (NIST, 2008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。
				CPS.CO-3	・復旧活動について内部および外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急事対応計画の中に位置づける。	Advanced	・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。 ・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、復旧活動およ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。
				CPS.AN-1	・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。	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。 ・セキュリティインシデント発生時において、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。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
				CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。	Advanced	・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位、およびメトリクスを考慮してインシデントを分類する。 ・組織は、自組織に影響を及ぼすセキュリティインシデントを追跡し、文書化する。 “SP 800-61 rev.1” では、セキュリティインシデントを文書化する際の記載の観点として、下記を例示している。 － インシデントの現在の状況 － インシデントの概要 － 当該インシデントに対して自組織のとった行動の内容 － ほかの関係者(システム所有者、システム管理者等)の連絡先情報 － 調査の際に収集した証拠の一覧 － インシデントの処理担当者からのコメント － 次にとるべきステップ
				CPS.MI-1	・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、影響を低減する対応を行う。	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(たとえば、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。 [参考]セキュリティインシデントの影響低減のための活動は、インシデントの性質(例えば、サービス拒否攻撃、マルウェア感染、不正アクセスのような脆弱性がある脅威の差異)により内容が異なる場合がある。より詳細な影響低減活動の情報については、「インシデントハンドリングマニュアル」(JPCERT/CC, 2015年)、SP 800-61 rev.1 (NIST, 2008年)等を参照することが望ましい。
	3.6.2	組織の内部及び外部の両方の、適切な担当官及び／または権威に対して、インシデントについての追跡、文書化、及び報告を行う。	・IR-2 インシデント対応のトレーニング ・IR-4 インシデントの対応 ・IR-5 インシデントの監視 ・IR-6 インシデントの報告 ・IR-7 インシデント対応の支援	CPS.RP-4	・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。	Advanced	・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、復旧活動およ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.AM-2, CPS.AM-3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。 ※ CPS.CO-3と関連
				CPS.CO-2	・事業継続計画又は緊急事対応計画の中に、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。	Basic	・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。 ・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。
				CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。	Advanced	・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位、およびメトリクスを考慮してインシデントを分類する。 ・組織は、自組織に影響を及ぼすセキュリティインシデントを追跡し、文書化する。 “SP 800-61 rev.1” では、セキュリティインシデントを文書化する際の記載の観点として、下記を例示している。 － インシデントの現在の状況 － インシデントの概要 － 当該インシデントに対して自組織のとった行動の内容 － ほかの関係者(システム所有者、システム管理者等)の連絡先情報 － 調査の際に収集した証拠の一覧 － インシデントの処理担当者からのコメント － 次にとるべきステップ
	3.6.3	組織のインシデント対応能力をテストする。	・IR-3 インシデント対応のテストと実習 ・IR-3(2) インシデント対応のテストと実習 関連する計画との調整	CPS.SC-9	・サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	H.Advanced	・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、たとえば、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。
						Advanced	・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。
				CPS.AT-1	・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。	H.Advanced	・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。組織は、CPS.AT-1＜Basic＞の[参考]に記載されている一般的な事項を解説しているコンテンツに加えて、組織によって内容が異なる内容として、例えば、下記の事項を扱うことができる。 － 不審なメールを受信した際の対応手順(どこにどのような内容を連絡すればよいか) － モバイル端末利用の注意点(例:公衆無線LANに接続する際の注意点) － SNSを利用する際の注意点 ・組織は、情報セキュリティ要員の育成とレベル向上のための役割別(例:システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者)のプログラムを作成し、定期的に該当する要員に対して実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の記録を定期的にレビューする。
						Advanced	・組織は、自組織の利用する情報システム及び産業用制御システムに対する変更により必要になった場合や新規職員に対して基本的なセキュリティ意識向上トレーニングを実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の内容や結果等について記録し、管理する。 [参考] 組織が従業員等に対してセキュリティ教育を実施する際、IPAが公開している「情報セキュリティ読本 教育用プレゼン資料」の内容を参照することが可能である。
メンテナンス	3.7.1	組織のシステムにおいてメンテナンスを実施する。	・MA-2 定期的な保守 ・MA-3 保守ツール ・MA-3(1) 保守ツール ツールを検査する ・MA-3(2) 保守ツール メディアを検査する	CPS.MA-1	・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。 ・可能であれば、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。	H.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。
						Advanced	・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、実施、確認、文書化する。 ・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を自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・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。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
	3.7.2	システムメンテナンスを実施するために使用されるツール、手法、メカニズム、及び要員における有効な管理策を提供する。	・MA-2 定期的な保守 ・MA-3 保守ツール ・MA-3(1) 保守ツール ツールを検査する ・MA-3(2) 保守ツール メディアを検査する	CPS.MA-1	・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。 ・可能であれば、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。	H.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。
						Advanced	・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、実施、確認、文書化する。 ・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を自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・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。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
	3.7.3	オフサイトのメンテナンスのために除去される装置は、あらゆるCUI についてサニタイズされることを保証する。	・MA-2 定期的な保守	CPS.IP-6	・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。	H.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。
						Advanced	・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、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。
						Basic	・組織は、自組織のIoT機器やサーバ等を廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.7.4	組織のシステム内でメディアが使用される前に、悪意のあるコードが入っていないか診断及びテストプログラムを用いてメディアをチェックする。	・MA-3(2) 保守ツール	CPS.MA-1	・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。 ・可能であれば、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。	H.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。
						Advanced	・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、実施、確認、文書化する。 ・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を自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・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。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
	3.7.5	外部のネットワークコネクションを介した非ローカルメンテナンスセッションを確立するため、複数要素の認証を要求し、非ローカルメンテナンスの完了時にこの	・MA-4 遠隔保守	CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、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	Advanced	・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。
						Basic	・組織は、遠隔保守の実施に当たっては、実施計画を策定・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。
	3.7.6	必要なアクセス許可なしにメンテナンス要員のメンテナンス活動を監督する。	・MA-5 保守要員	CPS.SC-5	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	H.Advanced	・組織は、委託先の要員により委託元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シージャを整備する。
						Advanced	・サプライヤー関係のセキュリティ面について該当する要員を訓練し、機密情報の取り扱いが正しく理解されていることを特に確認する。 ・委託業務の遂行に当たり、委託元が要求するセキュリティ要求事項が遵守されていることを定期的に確認する。
				CPS.MA-1	・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。 ・可能であれば、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。	Advanced	・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、実施、確認、文書化する。 ・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を自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・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。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
						Basic	・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。
メディア処理	3.8.1	紙及びディジタルの両方の、CUI を含む、システムメディアを保護する(即ち、物理的に制御及びセキュアに格納する)。	・MP-2 メディアへのアクセス ・MP-4 メディアの保管 ・MP-6 メディア上の記録の抹消とメディアの廃棄	CPS.AC-2	・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。	H.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。
						Advanced	・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。
						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、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、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。
				CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	H.Advanced	・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。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・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。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
						Advanced	・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。 ・組織は、IoT機器やPC、サーバ以外の機器であっても、複合機等のネットワークにつながる機器に対しては、不要な機能やサービス等を停止する。
						Basic	・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。 ・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。 ・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。
	3.8.2	システムメディア上のCUI へのアクセスを許可された利用者に制限する。	・MP-2 メディアへのアクセス ・MP-4 メディアの保管 ・MP-6 メディア上の記録の抹消とメディアの廃棄	CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・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。
				CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが利用されていないかを管理する。
	3.8.3	廃棄または再利用のために手放す前に、CUI を含むシステムメディアをサニタイズまたは破壊する。	・MP-2 メディアへのアクセス ・MP-4 メディアの保管 ・MP-6 メディア上の記録の抹消とメディアの廃棄	CPS.IP-6	・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。	H.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。
						Advanced	・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、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。
						Basic	・組織は、自組織のIoT機器やサーバ等を廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態する。
	3.8.4	CUI のマーク表示と配付制限が必要なメディアに対して表示を行う。	・MP-3 メディアへのラベル付け	CPS.AM-6	・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。	Advanced	・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(データおよ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。 ・当該資産の管理責任者は、データの分類に対して責任を負う。 ・組織は、リソースの分類体系に、分類の規則及びその分類を時間が経ってからレビューするための基準を含める。
						Basic	・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。 ・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、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遂行でない運用により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。 ・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、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。 [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2.1版」(IPA, 2018年)P.30～P.34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スコア分析ガイド 第2版」(IPA, 2018年)のP.21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, 2018年)4.2.2および4.2.3を参照することができる。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.8.5	CUI を含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの説明責任を維持する。	・MP-5 メディアの輸送	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。	Advanced	・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、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、組織内で規定されたポータブルストレージデバイス(例：USBメモリ)のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						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する。 [参考] 資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第2.1版」(IPA, 2018年)のP.33を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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, 2018年)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。
	3.8.6	代替の物理的予防手段による保護がない限り、持ち出し中はディジタルメディア上に格納されたCUI の機密性を保護するための暗号学的メカニズムを実装する。	・MP-5(4) メディアの輸送 暗号学的保護	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H.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。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・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。
	3.8.7	システムコンポーネント上の取り外し可能なメディアの使用を管理する。	・MP-7 メディアの利用	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。	Advanced	・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、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、組織内で規定されたポータブルストレージデバイス(例：USBメモリ)のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						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する。 [参考] 資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第2.1版」(IPA, 2018年)のP.33を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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, 2018年)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。
	3.8.8	ポータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。	・MP-7(1) メディアの利用 所有者以外の利用を禁止	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。	Advanced	・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、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、組織内で規定されたポータブルストレージデバイス(例：USBメモリ)のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						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する。 [参考] 資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第2.1版」(IPA, 2018年)のP.33を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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, 2018年)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。
	3.8.9	保存場所にあるバックアップCUI の機密性を保護する。	・CP-9 情報システムのバックアップ	CPS.IP-4	・構成要素（IoT機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする。	Advanced	・組織は、自組織のシステムドキュメントのバックアップを定めたタイミングや頻度で実施する。 ・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。
						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に含まれるユーザレベル・システムレベルの情報のバックアップを定めたタイミングや頻度で実施する。
人的セキュリティ	3.9.1	CUI を含む組織のシステムへのアクセスを許可する前に、個人を審査する。	・PS-3 要員に対する審査 ・PS-4 要員の解雇 ・PS-5 人事異動	CPS.IP-9	・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。	Advanced	・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。 ・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、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。 ・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。
						Basic	・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、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、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。 −セキュリティに関連するシステム関連の所有物をすべて回収する。 −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。
	3.9.2	離職または配置転換等の人事措置の間と後で、CUI 及びCUI を含む組織のシステムが保護されることを保証する。	・PS-3 要員に対する審査 ・PS-4 要員の解雇 ・PS-5 人事異動	CPS.IP-9	・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。	Advanced	・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。 ・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、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。 ・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。
						Basic	・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、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、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。 −セキュリティに関連するシステム関連の所有物をすべて回収する。 −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。
物理的保護	3.10.1	組織のシステム、装置、及びそれぞれの運用環境への物理的アクセスを許可された個人に制限する。	・PE-2 物理的アクセス権限 ・PE-5 表示メディアへのアクセス制御 ・PE-6 物理的アクセスの監視	CPS.AC-2	・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。	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、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メントの結果に応じてアクセス制御を実施する。 ・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。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.10.2	物理的設備を保護し、監視し、組織のシステムの基盤をサポートする。	・PE-2 物理的アクセス権限 ・PE-5 表示メディアへのアクセス制御 ・PE-6 物理的アクセスの監視	CPS.AC-2	・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。	Advanced	・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。
				CPS.CM-2	・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および記録、監視を実施する。	Advanced	・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。 ・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、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・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.DS-6)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。
						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人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。
	3.10.3	訪問者をエスコートし、訪問者の活動を監視する。	・PE-3 物理的アクセス制御	CPS.AC-2	・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。	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、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、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。
	3.10.4	物理的アクセスの監査ログを維持する。	・PE-3 物理的アクセス制御	CPS.AC-2	・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。	Advanced	・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。
				CPS.CM-2	・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および記録、監視を実施する。	Advanced	・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。 ・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、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・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.DS-6)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。
						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人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。
	3.10.5	物理的アクセスデバイスを制御し、管理する。	・PE-3 物理的アクセス制御	CPS.AC-2	・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。	Advanced	・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。
				CPS.CM-2	・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および記録、監視を実施する。	Advanced	・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。 ・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、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・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.DS-6)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。
						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人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。
	3.10.6	代替の作業サイト(例、テレワークのサイト)でのCUIに対する防護対策を強制(実施)する。	・PE-17 代替作業拠点	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する。	H.Advanced	・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。 ・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、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。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・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、ユーザおよ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、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
リスクアセスメント	3.11.1	組織のシステムの運用と関連するCUIの処理、ストレージ、または送信からの結果として組織運用(ミッション、職務、イメージ、または風評を含めて)、組織の資産、及び個人に対するリスクを定期的にアセスメントする。	・RA-3 リスクアセスメント	CPS.RA-4	・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。 ・IoT機器および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。	Advanced	・組織は、情報システム、または情報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)、もしくは情報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。 ・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。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 [参考]システムおよ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、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。
	3.11.2	定期的に、及び組織のシステムとアプリケーションに影響する新しい脆弱性が識別されるときに、それらのシステム及びアプリケーションの脆弱性についてスキャンする。	・RA-5 脆弱性のスキャン ・RA-5(5) 脆弱性のスキャン特権アクセス	CPS.CM-7	・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。	H.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、スキャンされたシステムの脆弱性を定期的に、あるいは新たな脆弱性が特定され、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。
						Advanced	・組織は、情報システムおよ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できることが求められる。 －プラットフォーム、ソフトウェアの欠陥、およ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、リスクアセスメントを通じて、特定された脆弱性を適切な期間中に修正する。 ・上記のプロセスから得た情報を組織内の他のシステムの管理者と共有することによって、他の情報システム内の同様の脆弱性を把握し、必要に応じて修正する。 [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/CVSS.html)を参考とすることが可能である。
						Basic	・組織は、情報システムおよびアプリケーションの脆弱性のスキャンを定期的に実施する

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク		
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例
	3.11.3	リスクのアセスメントに従い、脆弱性を修正する。	・RA-5 脆弱性のスキャン	CPS.RA-6	・リスクアセスメントに基づき、発生しう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。 ・IoT機器および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および関連するセーフティのリスクに対して適宜対応する。	Advanced ・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。 ・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、実施する対応策およ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。 ・CPS.RA-4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。
						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、セキュリティリスク対応の実施計画を策定する。 ・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。
				CPS.CM-7	・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。	Advanced ・組織は、情報システムおよ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できることが求められる。 －プラットフォーム、ソフトウェアの欠陥、およ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、リスクアセスメントを通じて、特定された脆弱性を適切な期間中に修正する。 ・上記のプロセスから得た情報を組織内の他のシステムの管理者と共有することによって、他の情報システム内の同様の脆弱性を把握し、必要に応じて修正する。 [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/CVSS.html)を参考とすることが可能である。
						Basic ・組織は、情報システムおよびアプリケーションの脆弱性のスキャンを定期的に実施する
セキュリティアセスメント	3.12.1	管理策がそれらのアプリケーションにおいて有効であるかどうかを決定するために、組織のシステムにおけるセキュリティ管理策を定期的にアセスメントする。	・CA-2 セキュリティア評価 ・CA-5 行動計画とマイルストン ・CA-7 継続的な監視 ・PL-2 システムセキュリティ計画	CPS.IP-7	・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改善する。	Advanced ・組織は、セキュリティ評価を適切に、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評価計画を策定した上で、セキュリティ評価を実施する。 －セキュリティ評価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評価手順 －セキュリティ評価を実施する環境や実施体制 －セキュリティ評価結果の取りまとめ方法とその活用方法
						Basic ・組織は、セキュリティ対策が正しく実装されているか及び運用されているかに加え、セキュリティ対策が期待された成果を上げているかに関する定期的に評価（セキュリティ評価）を実施し、管理責任者へ報告する。 ・組織は、セキュリティ評価の結果に基づき、セキュリティ対策の改善を実施する。
	3.12.2	欠陥を修正し、組織のシステムにおける脆弱性を軽減し、または取り除くために設計された行動計画を策定し、実施する。	・CA-2 セキュリティア評価 ・CA-5 行動計画とマイルストン ・CA-7 継続的な監視 ・PL-2 システムセキュリティ計画	CPS.RA-6	・リスクアセスメントに基づき、発生しう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。 ・IoT機器および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および関連するセーフティのリスクに対して適宜対応する。	Advanced ・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。 ・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、実施する対応策およ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。 ・CPS.RA-4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。
	3.12.3	管理策の継続的な有効性を保証するため、継続的にセキュリティ管理策を監視する。	・CA-2 セキュリティア評価 ・CA-5 行動計画とマイルストン ・CA-7 継続的な監視 ・PL-2 システムセキュリティ計画	CPS.RA-4	・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。 ・IoT機器および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。	H.Advanced ・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。 ・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。 [参考]セーフティ設計におけるハザードの特定と分析については、「つながる世界のセーフティ＆セキュリティ設計入門」(IPA, 2015年)の4.2にて具体的な手法が記載されており、参照することが可能である。
						Advanced ・組織は、情報システム、または情報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）、もしくは情報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。 ・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。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 [参考]システムおよ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、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。
						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ことが望ましい。 [参考] セキュリティリスクアセスメントの手法として、「資産ベース」の手法および「事業被害ベース」の手法があることが知られている。資産ベースの手法でリスクアセスメントを実施する場合は「中小企業の情報セキュリティガイドライン 第2.1版」(IPA, 2018年)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, 2018年) 等を、事業被害ベースの手法を実施する場合は「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, 2018年)等を参照することができる。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.12.4	システムの境界、システムの運用環境、セキュリティ要件の実装方法、及び他のシステムとの関係または他のシステムへのコネクションについて記述した、システムセキュリティ計画を策定、文書、及び定期的に更新する。	・CA-2 セキュリティア評価 ・CA-5 行動計画とマイルストン ・CA-7 継続的な監視 ・PL-2 システムセキュリティ計画	CPS.AM-5	・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。	H.Advanced	・システムは、自組織が利用している外部情報システムサービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・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。 ・組織は、外部プロバイダによる情報システムサービスを使用する際に必要な機能、ポート、プロトコル、および他のサービスを明確にする。
						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 ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。
				CPS.RA-6	・リスクアセスメントに基づき、発生しう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。 ・IoT機器および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および関連するセーフティのリスクに対して適宜対応する。	Advanced	・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。 ・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、実施する対応策およ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、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。 ・CPS.RA-4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。
システムと通信の保護	3.13.1	外部の境界及びシステムの鍵となる内部境界における通信（即ち、組織のシステムによって送信または受信される情報）を監視し、制御し、保護する。	・SC-7 境界保護 ・SA-8 セキュリティエンジニアリングの原則	CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	H.Advanced	・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。 ・組織/情報システムは、定常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およ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。 ・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。
						Advanced	・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/ドメインへの通信を遮断する等の対応を実施する。
				CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	H.Advanced	・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。 ・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。
						Advanced	・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、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。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる。 ・組織は、個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・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、およ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。
						Basic	・組織は、情報システムの外部境界において通信をモニタリングし、制御する。
	3.13.2	組織のシステム内の有効な情報セキュリティを促進するような、アーキテクチャ設計、ソフトウェア開発手法、及びシステムエンジニアリングの原則を採用する。	・SC-7 境界保護 ・SA-8 セキュリティエンジニアリングの原則	CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。	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。
	3.13.3	利用者機能をシステム管理機能と分離する。	・SC-2 アプリケーションの分離	CPS.AC-5	・職務および責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H.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、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。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・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、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最少化させることができる。 ・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停止できないようにすることができる。
						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、特定の職務権限に対して最小権限の原則を採用する。 －一般のユーザアカウントの権限と、特権アカウントの権限を分離する （非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。） －自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
	3.13.4	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。	・SC-4 残存情報	CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	H.Advanced	・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。 ・組織/情報システムは、定常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およ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。 ・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。
	3.13.5	内部ネットワークから物理的にまたは論理的に分離される、公開アクセス可能なシステムコンポーネント用には、サブネットワークを実装する。	・SC-7 境界保護	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜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)等してネットワークの完全性を保護する。	H.Advanced	・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システムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・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。 ・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。
						Basic	・組織は、情報システム及び産業用制御システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、適切に論理的あるいは物理的にネットワークを分離することで、フローの制御を実施する。 ・組織は、産業用制御システムにおいて、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。
				CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	H.Advanced	・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。 ・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。
						Advanced	・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、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。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる。 ・組織は、個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・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、およ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。
						Basic	・組織は、情報システムの外部境界において通信をモニタリングし、制御する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.13.6	デフォルトでネットワーク通信トラフィクを拒否し、また例外によってネットワーク通信トラフィクを許可する(即ち、すべて拒否、例外で許可)。	・SC-7(5) 境界保護 デフォルトで拒否／例外で許可	CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・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。
				CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	H.Advanced	・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。 ・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。
						Advanced	・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、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。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる。 ・組織は、個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・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、およ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。
	3.13.7	リモートデバイスが、組織のシステムとの非リモートコネクションの確立と同時に、外部ネットワークの資源への何らかの他のコネクションを介して通信することを防止する。	・SC-7(7) 境界保護 リモートデバイスのスピリットトンネルを禁止	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜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)等してネットワークの完全性を保護する。	H.Advanced	・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システムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・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。 ・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。
	3.13.8	代替の物理的予防手段による保護がない限り、持ち出し中にCUI の不正な暴露を防止するために暗号学的メカニズムを実装する。	・SC-8 伝送する情報の完全性 ・SC-8(1) 伝送する情報の完全性 暗号学的保護または代替の物理的保護	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H.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。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・組織は、内部メモリのデータを暗号化して保管することができるIoT機器を利用する。
						Advanced	・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、情報(データ)を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されたアルゴリズムが選択可能であれば、これを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。 ・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。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
	3.13.9	セション終了時または定義された非アクティブな時間の経過後に、通信セションに対応するネットワークコネクションを終了する。	・SC-10 ネットワークの切断	CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）および他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる。 ・個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・情報システム及び産業用制御システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
	3.13.10	組織のシステムで採用された暗号のための暗号鍵を確立し、管理する。	・SC-12 暗号鍵の確立と管理	CPS.DS-5	・送受信する情報データ、保管データする情報の暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。	Advanced	・組織は、秘密鍵が危殆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。 － 秘密鍵の危殆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) － 秘密鍵が危殆化した、またはその恐れがあると判断するための基準 － 秘密鍵の危殆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 － 秘密鍵の危殆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) [参考] 鍵管理に関するより詳細な内容については、ISO/IEC 11770規格群や、NIST SP 800-57 Part 1 Rev.4等を参照することが望ましい。
						Basic	・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。
	3.13.11	CUI の機密性を保護するために使用されるとき、FIPS 認証された暗号を採用する。	・SC-13 暗号化の利用	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H.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。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・組織は、内部メモリのデータを暗号化して保管することができるIoT機器を利用する。
						Advanced	・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、情報(データ)を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されたアルゴリズムが選択可能であれば、これを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。 ・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。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リ
	3.13.12	共同コンピューティングデバイスのリモートからの活性化を禁止し、使用中のデバイスの兆候をデバイスに存在する利用者に提供する。	・SC-15 共同コンピューティングデバイス	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する。	H.Advanced	・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。 ・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、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。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・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、ユーザおよ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、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の遠隔する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
	3.13.13	モバイルコードの使用を管理し監視する。	・SC-18 モバイルコード	CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	H.Advanced	・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。 ・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。
	3.13.14	VoIP 技術の使用を管理し、監視する。	・SC-19 ボイスオーバーインターネットプロトコル(VoIP)				
	3.13.15	通信セションの真正性を保護する。	・SC-23 セションの真正性	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する。	H.Advanced	・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。 ・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、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。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・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、ユーザおよ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、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の遠隔する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H.Advanced	・組織は、情報システム及び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。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、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。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.13.16	保存されたCUI の機密性を保護する。	・SC-28 保存情報の保護	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H.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。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・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。
						Advanced	・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、情報(データ)を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト(電子政府推奨暗号リスト)に記載されたアルゴリズムが選択可能であれば、これを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。 ・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。 [参考] 暗号技術検討会及び関連委員会(CRYPTREC)では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」(CRYPTREC暗号リスト)として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
システムと情報の完全性	3.14.1	タイムリーなやり方で情報及びシステムフローを識別し、報告し、訂正する。	・SI-2 欠陥の修正 ・SI-3 悪意のコード(不正プログラム) からの保護 ・SI-5 セキュリティ警報と勧告	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	H.Advanced	・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、システム内(およ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。 ・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。 ・組織/システムは、定常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およ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。
	3.14.2	組織のシステム内の適切な場所で、悪意のあるコードから保護を提供する。	・SI-2 欠陥の修正 ・SI-3 悪意のコード(不正プログラム) からの保護 ・SI-5 セキュリティ警報と勧告	CPS.CM-3	・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。 ・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。	H.Advanced	・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。 ・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。 ・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、自組織外から受信したファイルのリアルタイムスキャンを実行する。
						Advanced	・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。 ・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。
	3.14.3	システムセキュリティ警報及びアドバイザリを監視し、適切な対応アクションを取る。	・SI-2 欠陥の修正 ・SI-3 悪意のコード(不正プログラム) からの保護 ・SI-5 セキュリティ警報と勧告	CPS.IP-10	・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。	Advanced	・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欠陥の修正を実施し、当該修正を構成管理として管理する。
				CPS.CM-3	・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。 ・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。	H.Advanced	・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。 ・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。 ・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、自組織外から受信したファイルのリアルタイムスキャンを実行する。
						Advanced	・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。 ・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
	3.14.4	新しいリリースが利用可能となったとき、悪意のあるコードからの保護メカニズムをアップデートする。	・SI-3 悪意のコード(不正プログラム) からの保護	CPS.IP-8	・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。	H.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。
						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。
				CPS.AE-3	・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。	H.Advanced	・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、継続的なモニタリングに用いられている活動の修正の必要性を判断する。 ・組織は、自組織で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。
				CPS.CM-3	・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。 ・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。	H.Advanced	・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。 ・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。 ・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、自組織外から受信したファイルのリアルタイムスキャンを実行する。
	3.14.5	組織のシステムの定期的スキャン、及びファイルがダウンロードされ、開かれ、または実行されるような、外部情報源からのファイルのリアルタイムスキャンを実行する。	・SI-3 悪意のコード(不正プログラム) からの保護	CPS.CM-3	・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。 ・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。	H.Advanced	・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。 ・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。 ・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、自組織外から受信したファイルのリアルタイムスキャンを実行する。
				CPS.CM-4	・サイバー空間から受ける情報の完全性および真正性を動作前に確認する。	H.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。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、機器間の相互認証が成功した後に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。 ・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。
						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に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。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.14.6	内向き及び外向きの通信トラフィクを含めて、攻撃や潜在的な攻撃の兆候を検知するため、組織のシステムを監視する。	・SI-4 情報システムの監視ツールと監視技法 ・SI-4(4) 情報システムの監視ツールと監視技法 内向きと外向きの通信トラフィク	CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	H.Advanced	・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。 ・組織/情報システムは、定常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およ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。 ・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。
						Advanced	・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アドレスやドメインへの通信を遮断する等の対応を実施する。
				CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	H.Advanced	・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、システム内(およ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。 ・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。 ・組織/システムは、定常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およ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。
				CPS.AE-2	・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)を立ち上げ、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。	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（CPS.AE-3を参照） ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・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（プロセスの内容については、CPS.RP-1等を参照）。 ・組織およ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 [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 ～ 機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年)等を参照することが望ましい。
				CPS.CM-5	・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モニタリングする。	Advanced	・組織は、外部サービスプロバイダおよびシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダーおよ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およ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。
				CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）および他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる。 ・個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・情報システム及び産業用制御システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
				CPS.DP-4	・セキュリティ事象の検知プロセスを継続的に改善する。	Advanced	・組織は、経営層等の組織内の然るべき要員に、定期的に組織およびシステムのセキュリティの状態を報告するプロシージャを整備し、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」v1.0」(ISOG-J, 2017年)より引用している。 ・攻撃の特徴 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

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.14.7	組織のシステムの不正な使用を識別する。	・SI-4 情報システムの監視ツールと監視技法	CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	H.Advanced	・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。 ・組織/情報システムは、定常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およ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。 ・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。
						Advanced	・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アドレスやドメインへの通信を遮断する等の対応を実施する。
				CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	H.Advanced	・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、システム内(およ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。 ・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。 ・組織/システムは、定常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およ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。
				CPS.AE-2	・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)を立ち上げ、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。	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（CPS.AE-3を参照） ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・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（プロセスの内容については、CPS.RP-1等を参照）。 ・組織およ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 [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 ～ 機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年)等を参照することが望ましい。
				CPS.CM-5	・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モニタリングする。	Advanced	・組織は、外部サービスプロバイダおよびシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダーおよ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モニタリングする。 ・組織は、外部サービスプロバイダーおよ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。
				CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）および他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる。 ・個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・情報システム及び産業用制御システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
				CPS.DP-4	・セキュリティ事象の検知プロセスを継続的に改善する。	Advanced	・組織は、経営層等の組織内の然るべき委員に、定期的に組織およびシステムのセキュリティの状態を報告するプロシージャを整備し、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」v1.0」(ISOG-J, 2017年)より引用している。 ・攻撃の特徴 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

D．３　ISO/IEC 27001 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」との対応表

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
A.5 情報セキュリティのための方針群	A.5.1 情報セキュリティのための経営陣の方向性	A.5.1.1 情報セキュリティのための方針群	情報セキュリティのための方針群は，これを定義し，管理層が承認し，発行し，従業員及び関連する外部関係者に通知しなければならない。	CPS.BE-2	・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者(サプライヤー、第三者プロバイダ等を含む)に共有する。	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付けを確立する。 ・組織は、自組織のセキュリティポリシーにおいて規定されている自組織と関係する他組織のセキュリティに関する役割と責任について、関係する他組織に伝達する。
				CPS.GV-1	・セキュリティポリシーを策定し、自組織および関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。	Advanced	・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および実施手順を策定する。 a) アクセス制御および認証 b) 物理的セキュリティ対策 c) システムの開発および保守 d) 外部委託先管理 e) 情報分類および取扱い ・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っては、自組織の a)事業戦略、b)関係する規制、法令および契約、c)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、自組織の a)事業戦略、b)関係する規制、法令および契約、c)セキュリティの脅威環境 の 変化に応じて、セキュリティ方針をレビュー、更新する。 [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2.1版」(IPA, 2018年) 付録3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。
						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、更新する。 [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2.1版」(IPA, 2018年) 付録3<ツールB>における "組織的対策(基本方針)"における記載や、「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。
		A.5.1.2 情報セキュリティのための方針群のレビュー	情報セキュリティのための方針群は，あらかじめ定めた間隔で，又は重大な変化が発生した場合に，それが引き続き適切，妥当かつ有効であることを確実にするためにレビューしなければならない。	CPS.RA-6	・リスクアセスメントに基づき、発生しう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。 ・IoT機器および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および関連するセーフティのリスクに対して適宜対応する。	H.Advanced	・CPS.RA-4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りう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、近年国際標準化の場でも議論がなされており、IEC TR 63074, IEC TR 63069等を参照することが可能である。
						Advanced	・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。 ・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、実施する対応策およ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。 ・CPS.RA-4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。
						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、セキュリティリスク対応の実施計画を策定する。 ・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。
A.6 情報セキュリティのための組織	A.6.1 内部組織	A.6.1.1 情報セキュリティの役割及び責任	全ての情報セキュリティの責任を定め，割り当てなければならない。	CPS.AM-5	・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。	H.Advanced	・システムは、自組織が利用している外部情報システムサービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・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。 ・組織は、外部プロバイダによる情報システムサービスを使用する際に必要な機能、ポート、プロトコル、および他のサービスを明確にする。
						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 ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。
						Basic	・組織は、自組織が利用している外部情報システムサービスを一覧化し、それぞれの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。 [参考] 特にクラウドサービス利用におけるユーザー側の役割と責任を、契約において規定する際のポイントについて、「クラウドセキュリティガイドライン活用ガイドブック」(経済産業省, 2013年) Appendix A "契約の具体的な内容例と解説" を参照することが可能である。
				CPS.AM-6	・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。	Advanced	・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(データおよ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。 ・当該資産の管理責任者は，データの分類に対して責任を負う。 ・組織は、リソースの分類体系に，分類の規則及びその分類を時間が経ってからレビューするための基準を含める。
						Basic	・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。 ・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、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。 ・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、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。 [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2.1版」(IPA, 2018年)P.30～P.34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, 2018年)のP.21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, 2018年)4.2.2および4.2.3を参照することができる。
				CPS.AM-7	・自組織および関係する他組織のサイバーセキュリティ上の役割と責任を定める。	Advanced	・組織は、セキュリティインシデントにより損害が発生する場合に備えて、取引先等から指定されるセキュリティ対策の実装に加え、サイバー保険の利用等によるリスク移転を検討する。
						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。 ・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、「クラウドセキュリティガイドライン活用ガイドブック 2013年度版」(経済産業省, 2013年)の "4.4.クラウドサービスの契約" を参照することが可能である。
				CPS.DP-1	・セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知における自組織とサービスプロバイダが担う役割と負う責任を明確にする。	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情報を決定する。 ・組織は、取引先(サービスプロバイダー)に対して、取得されるサービス利用者の活動，例外処理及びセキュリティ事象を記録した監査ログの存在を確認する。 ・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事象を記録できており、適切な方式で保護されていることを確認する。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.6.1.2 職務の分離	相反する職務及び責任範囲は，組織の資産に対する，認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために，分離なければならない。	CPS.AC-5	・職務および責任範囲（例：ユーザー／システム管理者）を適切に分離する 。	H.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、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。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・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、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最少化させることができる。 ・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停止できないようにすることができる。
						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、特定の職務権限に対して最小権限の原則を採用する。 －一般のユーザアカウントの権限と、特権アカウントの権限を分離する （非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。） －自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
		A.6.1.3 関係当局との連絡	関係当局との適切な連絡体制を維持しなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	Basic	・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。 ・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。 ・管理者は，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。 [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 ,2019年)、「限定提供データに関する指針」(2019年 1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, 2019年)、「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, 2017年))を参照することが望ましい。
		A.6.1.4 専門組織との連絡	情報セキュリティに関する研究会又は会議，及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持しなければならない。	CPS.RA-2	・セキュリティ対応組織(SOC/CSIRT)は、組織の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、対応および活用するプロセスを確立する。	H.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。 ・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。 ・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。
						Advanced	・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。 ・組織は、情報処理推進機構(IPA)、JPCERT/CC、業界ISACのような組織や、取引関係のある機器ベンダー、ソフトウェアベンダーより、随時脆弱性情報、脅威情報等を収集し、自組織の資産目録と照らし合わせることで、対応要否を判断する。 [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 ～ 機能・役割・人材スキル・成熟度 ～」等の文書を利用することが可能である。
				CPS.RA-3	・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。	H.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、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、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手しそれをもとに、脅威を特定する。
				CPS.AE-4	・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。	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、当該セキュリティ事象の全容を把握する。 ・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。
				CPS.AN-1	・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。	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。 ・セキュリティインシデント発生時において、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。
		A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ	プロジェクトの種類にかかわらず，プロジェクトマネジメントにおいては，情報セキュリティに取り組まなければならない。	CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。	H.Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 －セキュリティ機能に関する要求事項 －セキュリティ強度に関する要求事項 －セキュリティ保証に関する要求事項 －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 －そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 －受け入れ基準
						Advanced	・組織は、情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通した情報セキュリティリスクマネジメントプロセスを実施する。
	A.6.2 モバイル機器及びテレワーキング	A.6.2.1 モバイル機器の方針	モバイル機器を用いることによって生じるリスクを管理するために，方針及びその方針を支援するセキュリティ対策を採用しなければならない。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。	H.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。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・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。 ※関連する対策要件に、CPS.CM-6がある。 [参考] 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2.1版」(IPA, 2018年)P.30～P.34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スク分析ガイド 第2版」(IPA, 2018年)のP.21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
						Advanced	・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、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、組織内で規定されたポータブルストレージデバイス(例：USBメモリ)のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						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する。 [参考] 資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第2.1版」(IPA, 2018年)のP.33を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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, 2018年)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。
				CPS.AM-5	・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。	H.Advanced	・システムは、自組織が利用している外部情報システムサービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・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。 ・組織は、外部プロバイダによる情報システムサービスを使用する際に必要な機能、ポート、プロトコル、および他のサービスを明確にする。
						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 ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する。	Advanced	・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・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。
				CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	H.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実行を許可するソフトウェアの一覧(ホワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)を用いてソフトウェアの制限を実施する、あるいは、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。
						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。
						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。
				CPS.CM-2	・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および記録、監視を実施する。	Advanced	・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。 ・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、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・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.DS-6)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。
						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人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。
				CPS.CM-3	・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。 ・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。	Advanced	・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。 ・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。
		A.6.2.2 テレワーキング	テレワーキングの場所でアクセス，処理及び保存される情報を保護するために，方針及びその方針を支援するセキュリティ対策を実施しなければならない。	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する。	Advanced	・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・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。
						Basic	・組織は、許可している(リモートアクセスのタイプごとに使用制限・構成要件・実装ガイダンス等を定める。 ・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、自組織の情報システム及び産業用制御システムへのリモートアクセスの利用に関する承認ルール等を定める。 ・組織は、自組織のシステムへの無線によるアクセスを許可するのに先立って、無線でシステムにアクセスする権限を与える。
				CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H.Advanced	・組織は、情報システム及び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。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、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。
				CPS.CM-3	・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。 ・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。	Advanced	・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。 ・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。
A.7 人的資源のセキュリティ	A.7.1 雇用前	A.7.1.1 選考	全ての従業員候補者についての経歴などの確認は，関連する法令，規制及び倫理に従って行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.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・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。
				CPS.IP-9	・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。	Advanced	・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。 ・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、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。 ・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。
						Basic	・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、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、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。 －セキュリティに関連するシステム関連の所有物をすべて回収する。 －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。
		A.7.1.2 雇用条件	従業員及び契約相手との雇用契約書には，情報セキュリティに関する各自の責任及び組織の責任を記載しなければならない。	CPS.IP-9	・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。	Advanced	・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。 ・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、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。 ・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。
						Basic	・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、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、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。 －セキュリティに関連するシステム関連の所有物をすべて回収する。 －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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
	A.7.2 雇用期間中	A.7.2.1 経営陣の責任	経営陣は，組織の確立された方針及び手順に従った情報セキュリティの適用を，全ての従業員及び契約相手に要求しなければならない。	CPS.AT-1	・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。	H.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。
						Advanced	・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。組織は、CPS.AT-1 <Basic>の[参考]に記載されている一般的な事項を解説しているコンテンツに加えて、組織によって内容が異なる内容として、例えば、下記の事項を扱うことができる。 － 不審なメールを受信した際の対応手順(どこにどのような内容を連絡すればよいか) － モバイル端末利用の注意点(例：公衆無線LANに接続する際の注意点) － SNSを利用する際の注意点 ・組織は、情報セキュリティ要員の育成とレベル向上のための役割別(例：システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者)のプログラムを作成し、定期的に該当する要員に対して実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の記録を定期的にレビューする。
						Basic	・組織は、自組織の利用する情報システム及び産業用制御システムに対する変更により必要になった場合や新規職員に対して基本的なセキュリティ意識向上トレーニングを実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の内容や結果等について記録し、管理する。 [参考] 組織が従業員等に対してセキュリティ教育を実施する際、IPAが公開している「情報セキュリティ読本 教育用プレゼン資料」の内容を参照することが可能である。
				CPS.IP-9	・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。	Advanced	・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。 ・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、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。 ・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。
						Basic	・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、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、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。 －セキュリティに関連するシステム関連の所有物をすべて回収する。 －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。
		A.7.2.2 情報セキュリティの意識向上，教育及び訓練	組織の全ての従業員，及び関係する場合には契約相手は，職務に関連する組織の方針及び手順についての，適切な，意識向上のための教育及び訓練を受けなければならず，また，定めに従ってその更新を受けなければならない。	CPS.AT-1	・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。	H.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。
						Advanced	・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。組織は、CPS.AT-1 <Basic>の[参考]に記載されている一般的な事項を解説しているコンテンツに加えて、組織によって内容が異なる内容として、例えば、下記の事項を扱うことができる。 － 不審なメールを受信した際の対応手順(どこにどのような内容を連絡すればよいか) － モバイル端末利用の注意点(例：公衆無線LANに接続する際の注意点) － SNSを利用する際の注意点 ・組織は、情報セキュリティ要員の育成とレベル向上のための役割別(例：システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者)のプログラムを作成し、定期的に該当する要員に対して実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の記録を定期的にレビューする。
						Basic	・組織は、自組織の利用する情報システム及び産業用制御システムに対する変更により必要になった場合や新規職員に対して基本的なセキュリティ意識向上トレーニングを実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の内容や結果等について記録し、管理する。 [参考] 組織が従業員等に対してセキュリティ教育を実施する際、IPAが公開している「情報セキュリティ読本 教育用プレゼン資料」の内容を参照することが可能である。
		A.7.2.3 懲戒手続	情報セキュリティ違反を犯した従業員に対して処置をとるための，正式かつ周知された懲戒手続を備えなければならない。	CPS.IP-9	・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。	Advanced	・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。 ・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、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。 ・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。
	A.7.3 雇用の終了及び変更	A.7.3.1 雇用の終了又は変更に関する責任	雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め，その従業員又は契約相手に伝達し，かつ，遂行させなければならない。	CPS.IP-9	・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。	Advanced	・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。 ・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、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。 ・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。
A.8 資産の管理	A.8.1 資産に対する責任	A.8.1.1 資産目録	情報及び情報処理施設に関連する資産を特定しなければならない。また，これらの資産の目録を，作成し，維持しなければならない。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。	H.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。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・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。 ※関連する対策要件に、CPS.CM-6がある。 [参考] 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2.1版」(IPA, 2018年)P.30～P.34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スク分析ガイド 第2版」(IPA, 2018年)のP.21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
						Advanced	・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、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、組織内で規定されたポータブルストレージデバイス(例：USBメモリ)のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						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する。 [参考] 資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第2.1版」(IPA, 2018年)のP.33を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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, 2018年)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.8.1.2 資産の管理責任 a)	目録の中で維持される資産は，管理されなければならない。 注a) 6.1.2及び 6.1.3 では，情報セキュリティのリスクを運用管理することについて，責任及び権限をもつ人又は主体をリスク所有者としている。情報セキュリティにおいて，多くの場合，資産の管理責任を負う者は，リスク所有者でもある。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。	H.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。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・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。 ※関連する対策要件に、CPS.CM-6がある。 [参考] 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2.1版」(IPA, 2018年)P.30～P.34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スク分析ガイド 第2版」(IPA, 2018年)のP.21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
						Advanced	・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、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、組織内で規定されたポータブルストレージデバイス(例：USBメモリ)のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						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する。 [参考] 資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第2.1版」(IPA, 2018年)のP.33を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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, 2018年)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。
		A.8.1.3 資産利用の許容範囲	情報の利用の許容範囲，並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施しなければならない。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。	H.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。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・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。 ※関連する対策要件に、CPS.CM-6がある。 [参考] 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2.1版」(IPA, 2018年)P.30～P.34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スク分析ガイド 第2版」(IPA, 2018年)のP.21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
						Advanced	・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、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、組織内で規定されたポータブルストレージデバイス(例：USBメモリ)のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
		A.8.1.4 資産の返却	全ての従業員及び外部の利用者は，雇用，契約又は合意の終了時に，自らが所持する組織の資産の全てを返却しなければならない。	CPS.IP-9	・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。	Advanced	・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。 ・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、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。 ・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。
						Basic	・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、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、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。 －セキュリティに関連するシステム関連の所有物をすべて回収する。 －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。
A.8.2 情報分類		A.8.2.1 情報の分類	情報は，法的要求事項，価値，重要性，及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から，分類しなければならない。	CPS.AM-6	・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。	Advanced	・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(データおよ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。 ・当該資産の管理責任者は、データの分類に対して責任を負う。 ・組織は、リソースの分類体系に、分類の規則及びその分類を時間が経ってからレビューするための基準を含める。
						Basic	・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。 ・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、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。 ・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、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。 [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2.1版」(IPA, 2018年)P.30～P.34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スク分析ガイド 第2版」(IPA, 2018年)のP.21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, 2018年)4.2.2および4.2.3を参照することができる。
				CPS.GV-3	・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。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法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識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)
		A.8.2.2 情報のラベル付け	情報のラベル付けに関する適切な一連の手順は，組織が採用した情報分類体系に従って策定し，実施しなければならない。	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	H.Advanced	・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。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・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。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
						Advanced	・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。 ・組織は、IoT機器やPC、サーバ以外の機器であっても、複合機等のネットワークにつながる機器に対しては、不要な機能やサービス等を停止する。
						Basic	・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。 ・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。 ・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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.8.2.3 資産の取扱い	資産の取扱いに関する手順は，組織が採用した情報分類体系に従って策定し，実施しなければならない。	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
				CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H.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。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・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。
						Advanced	・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、情報(データ)を適切な強度の方式で暗号化して保管する。 CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されたアルゴリズムが選択可能であれば、これを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。 ・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。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は，暗号機能を実装すべきシステム等を調達する場合，必要に応じて参照することが望ましい。
						Basic	・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、情報システムが取り扱う重要度の高い情報(データ)を適切な強度の方式で暗号化して保管する。
				CPS.IP-6	・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。	H.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。
	A.8.3 媒体の取扱い	A.8.3.1 取外し可能な媒体の管理	組織が採用した分類体系に従って，取外し可能な媒体の管理のための手順を実施しなければならない。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。	H.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。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・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。 ※関連する対策要件に、CPS.CM-6がある。 [参考] 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2.1版」(IPA, 2018年)P.30～P.34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ス分析ガイド 第2版」(IPA, 2018年)のP.21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
						Advanced	・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、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、組織内で規定されたポータブルストレージデバイス(例：USBメモリ)のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
				CPS.IP-6	・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。	H.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。
						Advanced	・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、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。
						Basic	・組織は、自組織のIoT機器やサーバ等を廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態する。
				CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	H.Advanced	・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。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・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。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
						Advanced	・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。 ・組織は、IoT機器やPC、サーバ以外の機器であっても、複合機等のネットワークにつながる機器に対しては、不要な機能やサービス等を停止する。
						Basic	・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。 ・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。 ・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。
		A.8.3.2 媒体の処分	媒体が不要になった場合は，正式な手順を用いて，セキュリティを保って処分しなければならない。	CPS.IP-6	・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。	H.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。
						Advanced	・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、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。
						Basic	・組織は、自組織のIoT機器やサーバ等を廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態する。
		A.8.3.3 物理的媒体の輸送	情報を格納した媒体は，輸送の途中における，認可されていないアクセス，不正使用又は破損から保護しなければならない。	CPS.SC-4	・外部の組織との契約を行う場合、目的およ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の提供する製品・サービスが適合していることを確認する。	H.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せているかを、自組織あるいは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、適切なプロシージャで製造されたものかを確認する。
						Advanced	・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 EDSA認証、ITセキュリティ評価及び認証制度(JISEC))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 ・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・供給にて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。 ・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、運用および改善する。 － 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

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
A.9 アクセス制御	A.9.1 アクセス制御に対する業務上の要求事項	A.9.1.1 アクセス制御方針	アクセス制御方針は，業務及び情報セキュリティの要求事項に基づいて確立し，文書化し，レビューしなければならない。	CPS.AC-1	・承認されたモノとヒトおよ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。	H.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および無効化について自動的に監査・報告する。
						Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・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。 ・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。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・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。 ・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。
						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、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別(例：一般ユーザ/システム管理者/共有ユーザ/一時的なユーザ)を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・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、その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実装する。ポリシーの内容の例としては、下記が挙げられる。 － 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。 ・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、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。
		A.9.1.2 ネットワーク及びネットワークサービスへのアクセス	利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを，利用者に提供しなければならない。	CPS.AC-6	・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	H.Advanced	・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多要素認証を実施する。 ・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、リプ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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・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。 ・情報システムは、自組織のシステムについて管理者アカウントの無効化等制限が実施できない場合には、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多要素認証を要求する。 ・情報システムにおけるデフォルトの管理者アカウントは、原則無効化する。 ・情報システムは、権限付与等の特権操作を実施する場合には、利用ユーザアカウントに対して必要最小限の特権操作権限を付与する。
	A.9.2 利用者アクセスの管理	A.9.2.1 利用者登録及び登録削除	アクセス権の割当てを可能にするために，利用者の登録及び登録削除についての正式なプロセスを実施しなければならない。	CPS.AC-1	・承認されたモノとヒトおよ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。	H.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および無効化について自動的に監査・報告する。
						Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・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。 ・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。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・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。 ・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。
						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、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別(例：一般ユーザ/システム管理者/共有ユーザ/一時的なユーザ)を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・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、その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実装する。ポリシーの内容の例としては、下記が挙げられる。 － 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。 ・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、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。
				CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.9.2.2 利用者アクセスの提供（provisioning）	全ての種類の利用者について，全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために，利用者アクセスの提供についての正式なプロセスを実施しなければならない。	CPS.AC-1	・承認されたモノとヒトおよ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。	H.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および無効化について自動的に監査・報告する。
						Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・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。 ・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。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・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。 ・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。
						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、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別(例：一般ユーザ/システム管理者/共有ユーザ/一時的なユーザ)を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・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、その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実装する。ポリシーの内容の例としては、下記が挙げられる。 － 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。 ・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、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。
		A.9.2.3 特権的アクセス権の管理	特権的アクセス権の割当て及び利用は，制限し，管理しなければならない。	CPS.AC-5	・職務および責任範囲（例：ユーザー／システム管理者）を適切に分離する 。	H.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、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。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・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、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最少化させることができる。 ・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停止できないようにすることができる。
						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、特定の職務権限に対して最小権限の原則を採用する。 － 一般のユーザアカウントの権限と、特権アカウントの権限を分離する （非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。） － 自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
				CPS.AC-6	・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	H.Advanced	・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多要素認証を実施する。 ・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、リプ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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・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。 ・情報システムは、自組織のシステムについて管理者アカウントの無効化等制限が実施できない場合には、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多要素認証を要求する。 ・情報システムにおけるデフォルトの管理者アカウントは、原則無効化する。 ・情報システムは、権限付与等の特権操作を実施する場合には、利用ユーザアカウントに対して必要最小限の特権操作権限を付与する。
		A.9.2.4 利用者の秘密認証情報の管理	秘密認証情報の割当ては，正式な管理プロセスによって管理しなければならない。	CPS.AC-1	・承認されたモノとヒトおよ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。	H.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および無効化について自動的に監査・報告する。
						Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・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。 ・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。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・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。 ・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。
		A.9.2.5 利用者アクセス権のレビュー	資産の管理責任者は，利用者のアクセス権を定められた間隔でレビューしなければならない。	CPS.AC-1	・承認されたモノとヒトおよ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。	H.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および無効化について自動的に監査・報告する。
						Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・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。 ・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。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・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。 ・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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.9.2.6 アクセス権の削除又は修正	全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は，雇用，契約又は合意の終了時に削除しなければならず，また，変更に合わせて修正しなければならない。	CPS.AC-1	・承認されたモノとヒトおよ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。	H.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および無効化について自動的に監査・報告する。
						Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・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。 ・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。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・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。 ・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。
						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、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別(例：一般ユーザ/システム管理者/共有ユーザ/一時的なユーザ)を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・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、その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実装する。ポリシーの内容の例としては、下記が挙げられる。 － 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。 ・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、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。
				CPS.AC-2	・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。	H.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。
						Advanced	・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おけ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。
						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、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、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。
	A.9.3 利用者の責任	A.9.3.1 秘密認証情報の利用	秘密認証情報の利用時に，組織の慣行に従うことを，利用者に要求しなければならない。	CPS.AC-4	・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。	H.Advanced	・情報システム及び産業用制御システム(対応の即時性が求められる一部の例を除く)は、自組織のシステムに対してユーザが連続してログオ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管理者が解除しなければ再ログインできない機能を実装する。
						Advanced	・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対してユーザが連続してログオ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。
				CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
				CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。	Basic	・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、CPS.AC-1で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、IoT機器の導入前に、搭載されているソフトウェアを確認し、記録する。
	A.9.4 システム及びアプリケーションのアクセス制御	A.9.4.1 情報へのアクセス制限	情報及びアプリケーションシステム機能へのアクセスは，アクセス制御方針に従って，制限しなければならない。	CPS.AC-5	・職務および責任範囲（例：ユーザー／システム管理者）を適切に分離する 。	H.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、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。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・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、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最少化させることができる。 ・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停止できないようにすることができる。
						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、特定の職務権限に対して最小権限の原則を採用する。 － 一般のユーザアカウントの権限と、特権アカウントの権限を分離する （非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。） － 自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
				CPS.AC-6	・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	H.Advanced	・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多要素認証を実施する。 ・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、リプ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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・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。 ・情報システムは、自組織のシステムについて管理者アカウントの無効化等制限が実施できない場合には、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多要素認証を要求する。 ・情報システムにおけるデフォルトの管理者アカウントは、原則無効化する。 ・情報システムは、権限付与等の特権操作を実施する場合には、利用ユーザアカウントに対して必要最小限の特権操作権限を付与する。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.9.4.2 セキュリティに配慮したログオン手順	アクセス制御方針で求められている場合には，システム及びアプリケーションへのアクセスは，セキュリティに配慮したログオン手順によって制御しなければならない。	CPS.AC-4	・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。	H.Advanced	・情報システム及び産業用制御システム(対応の即時性が求められる一部の例を除く)は、自組織のシステムに対してユーザが連続してログオ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管理者が解除しなければ再ログインできない機能を実装する。
						Advanced	・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対してユーザが連続してログオ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。
		A.9.4.3 パスワード管理システム	パスワード管理システムは，対話式でなければならず，また，良質なパスワードを確実とするものでなければならない。	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
		A.9.4.4 特権的なユーティリティプログラムの使用	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は，制限し，厳しく管理しなければならない。	CPS.AC-5	・職務および責任範囲（例：ユーザー／システム管理者）を適切に分離する 。	H.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、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。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・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、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最少化させることができる。 ・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停止できないようにすることができる。
						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、特定の職務権限に対して最小権限の原則を採用する。 －一般のユーザアカウントの権限と、特権アカウントの権限を分離する （非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。） －自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
				CPS.AC-6	・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	H.Advanced	・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多要素認証を実施する。 ・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、リプ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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・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。 ・情報システムは、自組織のシステムについて管理者アカウントの無効化等制限が実施できない場合には、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多要素認証を要求する。 ・情報システムにおけるデフォルトの管理者アカウントは、原則無効化する。 ・情報システムは、権限付与等の特権操作を実施する場合には、利用ユーザアカウントに対して必要最小限の特権操作権限を付与する。
		A.9.4.5 プログラムソースコードへのアクセス制御	プログラムソースコードへのアクセスは，制限しなければならない。	CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
A.10 暗号	A.10.1 暗号による管理策	A.10.1.1 暗号による管理策の利用方針	情報を保護するための暗号による管理策の利用に関する方針は，策定し，実施しなければならない。	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H.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。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・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。
						Advanced	・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、情報(データ)を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されたアルゴリズムが選択可能であれば、これを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。 ・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。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H.Advanced	・組織は、情報システム及び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。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、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。
				CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。	H.Advanced	・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。 ・情報システムは、重要度の高い・低いに限らず、組織外部へ送信するすべてのデータを適切な強度で暗号化する。
						Advanced	・組織は、機密性の高い情報を外部の組織等へ送信する際、情報を適切な強度の方式で暗号化する。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.10.1.2 鍵管理	暗号鍵の利用，保護及び有効期間（lifetime）に関する方針を策定し，そのライフサイクル全体にわたって実施しなければならない。	CPS.DS-5	・送受信する情報データ、保管データする情報の暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。	H.Advanced	・組織は、ユーザが暗号鍵を紛失した場合に、鍵の再発行等により情報の可用性を維持する。 ・秘密鍵及びプライベート鍵をセキュリティを保って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。
						Advanced	・組織は、秘密鍵が危殆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。 － 秘密鍵の危殆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) － 秘密鍵が危殆化した、またはその恐れがあると判断するための基準 － 秘密鍵の危殆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 － 秘密鍵の危殆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) [参考] 鍵管理に関するより詳細な内容については、ISO/IEC 11770規格群や、NIST SP 800-57 Part 1 Rev.4等を参照することが望ましい。
						Basic	・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。
				CPS.DS-8	・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。	H.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。
A.11 物理的及び環境的セキュリティ	A.11.1 セキュリティを保つべき領域	A.11.1.1 物理的セキュリティ境界	取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために，物理的セキュリティ境界を定め，かつ，用いなければならない。	CPS.AC-2	・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。	H.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。
						Advanced	・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。
				CPS.CM-2	・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および記録、監視を実施する。	H.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、モニタリングする。
						Advanced	・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。 ・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、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・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.DS-6)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。
						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人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。
		A.11.1.2 物理的入退管理策	セキュリティを保つべき領域は，認可された者だけにアクセスを許すことを確実にするために，適切な入退管理策によって保護しなければならない。	CPS.AC-2	・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。	H.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。
						Advanced	・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。
						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、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、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。
				CPS.CM-2	・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および記録、監視を実施する。	H.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、モニタリングする。
						Advanced	・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。 ・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、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・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.DS-6)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。
						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人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。
		A.11.1.3 オフィス，部屋及び施設のセキュリティ	オフィス，部屋及び施設に対する物理的セキュリティを設計し，適用しなければならない。	CPS.AC-2	・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。	H.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。
						Advanced	・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。
						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、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、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。
				CPS.CM-2	・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および記録、監視を実施する。	H.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、モニタリングする。
						Advanced	・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。 ・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、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・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.DS-6)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。
						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人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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.11.1.4 外部及び環境の脅威からの保護	自然災害，悪意のある攻撃又は事故に対する物理的な保護を設計し，適用しなければならない。	CPS.AC-2	・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。	H.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。
				CPS.IP-5	・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。	H.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。
						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。
						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。
		A.11.1.5 セキュリティを保つべき領域での作業	セキュリティを保つべき領域での作業に関する手順を設計し，適用しなければならない。	CPS.AC-2	・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。	H.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。
						Advanced	・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。
		A.11.1.6 受渡場所	荷物の受渡場所などの立寄り場所，及び認可されていない者が施設に立ち入ることもあるその他の場所は，管理しなければならない。また，可能な場合には，認可されていないアクセスを避けるために，それらの場所を情報処理施設から離さなければならない。	CPS.AC-2	・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。	H.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。
						Advanced	・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。
						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、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、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。
	A.11.2 装置	A.11.2.1 装置の設置及び保護	装置は，環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し，保護しなければならない。	CPS.IP-5	・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。	H.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。
						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。
						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。
		A.11.2.2 サポートユーティリティ	装置は，サポートユーティリティの不具合による，停電，その他の故障から保護しなければならない。	CPS.BE-3	・自組織が事業を継続する上での自組織およ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する。	H.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およ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およ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
				CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	Advanced	・装置は，サポートユーティリティの不具合による，停電，その他の故障から保護する。 ・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は，傍受，妨害又は損傷から保護する。 ・装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守する。 ・組織は，一次電源が失われた場合に，情報システムの長期間使用可能な代替電源への切り替えを支援する，短期無停電電源装置を用意する。
						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ず，また，将来必要とする容量・能力を予測する。 ・装置は，サポートユーティリティの不具合による，停電，その他の故障から保護する。 ・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は，傍受，妨害又は損傷から保護する。 ・装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守する。
				CPS.IP-5	・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。	H.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。
						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。
						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。
		A.11.2.3 ケーブル配線のセキュリティ	データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受，妨害又は損傷から保護しなければならない。	CPS.AC-2	・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。	H.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。
				CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	Advanced	・装置は，サポートユーティリティの不具合による，停電，その他の故障から保護する。 ・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は，傍受，妨害又は損傷から保護する。 ・装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守する。 ・組織は，一次電源が失われた場合に，情報システムの長期間使用可能な代替電源への切り替えを支援する，短期無停電電源装置を用意する。
						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ず，また，将来必要とする容量・能力を予測する。 ・装置は，サポートユーティリティの不具合による，停電，その他の故障から保護する。 ・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は，傍受，妨害又は損傷から保護する。 ・装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守する。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.11.2.4 装置の保守	装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守しなければならない。	CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	Advanced	・装置は，サポートユーティリティの不具合による，停電，その他の故障から保護する。 ・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は，傍受，妨害又は損傷から保護する。 ・装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守する。 ・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。
						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ず，また，将来必要とする容量・能力を予測する。 ・装置は，サポートユーティリティの不具合による，停電，その他の故障から保護する。 ・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は，傍受，妨害又は損傷から保護する。 ・装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守する。
				CPS.MA-1	・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。 ・可能であれば、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。	H.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。
						Advanced	・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、実施、確認、文書化する。 ・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を自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・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。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
				CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、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。	Advanced	・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。
						Basic	・組織は、遠隔保守の実施に当たっては、実施計画を策定・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。
		A.11.2.5 資産の移動	装置，情報又はソフトウェアは，事前の認可なしでは，構外に持ち出してはならない。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。	Advanced	・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、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア(例:USBメモリ)を一覧化し、使用を管理する。 ・組織は、組織内で規定されたポータブルストレージデバイス(例:USBメモリ)のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
				CPS.CM-2	・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および記録、監視を実施する。	H.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、モニタリングする。
		A.11.2.6 構外にある装置及び資産のセキュリティ	構外にある資産に対しては，構外での作業に伴った，構内での作業とは異なるリスクを考慮に入れて，セキュリティを適用しなければならない。	CPS.CM-2	・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および記録、監視を実施する。	Advanced	・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。 ・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、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・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.DS-6)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。
		A.11.2.7 装置のセキュリティを保った処分又は再利用	記憶媒体を内蔵した全ての装置は，処分又は再利用する前に，全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去しているこ又はセキュリティを保	CPS.IP-6	・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。	H.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。
						Advanced	・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、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。
						Basic	・組織は、自組織のIoT機器やサーバ等を廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態する。
		A.11.2.8 無人状態にある利用者装置	利用者は，無人状態にある装置が適切な保護対策を備えていることを確実にしなければならない。	CPS.AC-2	・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。	H.Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配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。
						Advanced	・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。
						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、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、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。
		A.11.2.9 クリアデスク・クリアスクリーン方針	書類及び取外し可能な記憶媒体に対するクリアデスク方針，並びに情報処理設備に対するクリアスクリーン方針を適用しなければならない。	CPS.AC-2	・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。	H.Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配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。
						Advanced	・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。
						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、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、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。
A.12 運用のセキュリティ	A.12.1 運用の手順及び責任	A.12.1.1 操作手順書	操作手順は，文書化し，必要とする全ての利用者に対して利用可能にしなければならない。	CPS.GV-1	・セキュリティポリシーを策定し、自組織および関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。	H.Advanced	・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およ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。
						Advanced	・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および実施手順を策定する。 a) アクセス制御および認証 b) 物理的セキュリティ対策 c) システムの開発および保守 d) 外部委託先管理 e) 情報分類および取扱い ・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っては、自組織の a)事業戦略、b)関係する規制、法令および契約、c)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、自組織の a)事業戦略、b)関係する規制、法令および契約、c)セキュリティの脅威環境 の 変化に応じて、セキュリティ方針をレビュー、更新する。 [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2.1版」(IPA, 2018年) 付録3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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.12.1.2 変更管理	情報セキュリティに影響を与える，組織，業務プロセス，情報処理設備及びシステムの変更は，管理しなければならない。	CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。	H.Advanced	・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、それらの変更をテスト・承認・文書化する。 ・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。
						Advanced	・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、実施手順等の文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・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、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法(例：変更実施前に本人にしかわからないセキュリティコードを入力させる)を利用する。 ・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。
						Basic	・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、CPS.AC-1で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、IoT機器の導入前に、搭載されているソフトウェアを確認し、記録する。
		A.12.1.3 容量・能力の管理	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ず，また，将来必要とする容量・能力を予測しなければならない。	CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する。	Advanced	・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 ・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ず，また，将来必要とする容量・能力を予測しなければならない。 ・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
				CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	Advanced	・装置は、サポートユーティリティの不具合による，停電，その他の故障から保護する。 ・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は，傍受，妨害又は損傷から保護する。 ・装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守する。 ・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。
						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ず，また，将来必要とする容量・能力を予測する。 ・装置は，サポートユーティリティの不具合による，停電，その他の故障から保護する。 ・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は，傍受，妨害又は損傷から保護する。 ・装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守する。
		A.12.1.4 開発環境，試験環境及び運用環境の分離	開発環境，試験環境及び運用環境への認可されていないアクセス又は変更によるリスクを低減するために，分離しなければならない。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜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)等してネットワークの完全性を保護する。	H.Advanced	・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システムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・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。 ・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。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界(産業用制御システムの場合は情報システムとの境界)について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。
						Basic	・組織は、情報システム及び産業用制御システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、適切に論理的あるいは物理的にネットワークを分離することで、フローの制御を実施する。 ・組織は、産業用制御システムにおいて、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。
	A.12.2 マルウェアからの保護	A.12.2.1 マルウェアに対する管理策	マルウェアから保護するために，利用者に適切に認識させることと併せて，検出，予防及び回復のための管理策を実施しなければならない。	CPS.DS-10	・IoT機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。	H.Advanced	・組織は、情報システムにおいて完全性検証時に不一致が発見された場合にシステム管理者に通知する、自動化されたツールを使用する。 ・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、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。
						Advanced	・情報システムは、ソフトウェア・ファームウェアの完全性チェックを定期的に実施する。 ・情報システム及び産業用制御システムは、起動を許可するソフトウェアを事前に登録しておくことで、登録されていないソフトウェアの起動を停止する。
				CPS.CM-3	・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。 ・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。	H.Advanced	・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。 ・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。 ・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、自組織外から受信したファイルのリアルタイムスキャンを実行する。
						Advanced	・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。 ・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。
	A.12.3 バックアップ	A.12.3.1 情報のバックアップ	情報，ソフトウェア及びシステムイメージのバックアップは，合意されたバックアップ方針に従って定期的に取得し，検査しなければならない。	CPS.BE-3	・自組織が事業を継続する上での自組織およ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する。	H.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およ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およ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
						Advanced	・CPS.AM-6で規定した当該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。 ・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。
				CPS.IP-4	・構成要素（IoT機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする。	H.Advanced	・組織は、バックアップ情報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。
						Advanced	・組織は、自組織のシステムドキュメントのバックアップを定めたタイミングや頻度で実施する。 ・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。
						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に含まれるユーザレベル・システムレベルの情報のバックアップを定めたタイミングや頻度で実施する。

ISO/IEC 27001:2013 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			
管理策ID		要求事項	対策要件ID	対策要件	対策例	
	A.12.4.1 イベントログ取得	利用者の活動，例外処理，過失及び情報セキュリティ事象を記録したイベントログを取得し，保持し，定期的にレビューしなければならない。	CPS.SC-8	・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。	H.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
					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
					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。
			CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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)管理される。 ・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機器からの監査ログの収集・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。
					Advanced	・情報システム及び産業用制御システムは、監査ログおよ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、監査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。
					Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査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、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
			CPS.AE-2	・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)を立ち上げ、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。	H.Advanced	・組織は、セキュリティ専門の24時間365日モニタリングモニタリングにより収集した監査ログを、分析自動化ツール等を利用することで効率的に分析する。 ・組織は、従来のIT環境だけでなく、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、セキュリティ対応組織の成熟度を定期的に評価し、セキュリティ状況のモニタリングやインシデントへの対応等の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。 [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成熟度セルフチェックシート」(ISOG-J, 2018年)や、SIM3(Security Incident Management Maturity Model)等がある。
					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（CPS.AE-3を参照） ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・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(プロセスの内容については、CPS.RP-1等を参照)。 ・組織およ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 [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 ～ 機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年)等を参照することが望ましい。
			CPS.AE-3	・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。	H.Advanced	・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、継続的なモニタリングに用いられている活動の修正の必要性を判断する。 ・組織は、自組織で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。
					Advanced	・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フロー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 ～ 機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年) 等を参照することが望ましい。
					Basic	・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。
			CPS.DP-1	・セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知における自組織とサービスプロバイダが担う役割と負う責任を明確にする。	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情報を決定する。 ・組織は、取引先(サービスプロバイダー)に対して、取得されるサービス利用者の活動，例外処理及びセキュリティ事象を記録した監査ログの存在を確認する。 ・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事象を記録できており、適切な方式で保護されていることを確認する。
	A.12.4.2 ログ情報の保護	ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護しなければならない。	CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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)管理される。 ・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機器からの監査ログの収集・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。
					Advanced	・情報システム及び産業用制御システムは、監査ログおよ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、監査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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.12.4.3 実務管理者及び運用担当者の作業ログ	システムの実務管理者及び運用担当者の作業は，記録し，そのログを保護し，定期的にレビューしなければならない。	CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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)管理される。 ・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機器からの監査ログの収集・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。
						Advanced	・情報システム及び産業用制御システムは、監査ログおよ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、監査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。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査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、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
		A.12.4.4 クロックの同期	組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは，単一の参照時刻源と同期させなければならない。	CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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)管理される。 ・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機器からの監査ログの収集・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。
	A.12.5 運用ソフトウェアの管理	A.12.5.1 運用システムに関わるソフトウェアの導入	運用システムに関わるソフトウェアの導入を管理するための手順を実施しなければならない。	CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。	H.Advanced	・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、それらの変更をテスト・承認・文書化する。 ・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。
						Advanced	・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、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・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、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法(例：変更実施前に本人にしかわからないセキュリティコードを入力させる)を利用する。 ・組織は、セキュリティと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。
						Basic	・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、CPS.AC-1で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、IoT機器の導入前に、搭載されているソフトウェアを確認し、記録する。
				CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	H.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実行を許可するソフトウェアの一覧(ホワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)を用いてソフトウェアの制限を実施する、あるいは、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。
	A.12.6 技術的ぜい弱性管理	A.12.6.1 技術的ぜい弱性の管理	利用中の情報システムの技術的ぜい弱性に関する情報は，時機を失せずに獲得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なければならない。さらに，それらと関連するリスクに対処するために，適切な手段をとらなければならない。	CPS.RA-1	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	H.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、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、定期的に侵入テストを実施することが望ましい。 ・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。
						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、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/CVSS.html)を参考とすることが可能である。
				CPS.RA-4	・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。 ・IoT機器および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。	H.Advanced	・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。 ・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。 [参考]セーフティ設計におけるハザードの特定と分析については、「つながる世界のセーフティ＆セキュリティ設計入門」(IPA, 2015年)の4.2にて具体的な手法が記載されており、参照することが可能である。
						Advanced	・組織は、情報システム、または情報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)、もしくは情報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。 ・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。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 [参考]システムおよ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、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。
				CPS.RA-5	・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。	Advanced	・組織は、情報システム、または情報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)、もしくは情報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及び産業用制御システムを優先的に対応する。 ※ CPS.RA-4と共通の実施内容
				CPS.IP-10	・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。	H.Advanced	・組織は、欠陥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。
						Advanced	・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欠陥の修正を実施し、当該修正を構成管理として管理する。
						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に関する欠陥の特定・報告・修正を計画的に実施する。計画を策定する際には、下記を考慮することが望ましい。 － 脅威または脆弱性の深刻さ － 修正措置の適用に関わるリスク [参考] 特に、製造現場等に設置されるIoT機器や制御機器(例：PLC、DCS)には、可用性や機器自体の機能の関係で、タイムリーにパッチを適用すること、あるいはパッチの適用事態が困難な場合がある。その場合は、「制御システム利用者のための脆弱性対応ガイド 第2版」(IPA, 2016年)の P.23に記載されている通り、脅威への対策(機能の最小化、ネットワーク監視の強化等)を徹底し、セキュリティ被害の発生を回避することが望ましい。 ※ PLC: Programmable Logic Controller, DCS: Distributed Control System

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.CM-7	・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。	H.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、スキャンされたシステムの脆弱性を定期的に、あるいは新たな脆弱性が特定され、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。
						Advanced	・組織は、情報システムおよ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できることが求められる。 － プラットフォーム、ソフトウェアの欠陥、およ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、リスクアセスメントを通じて、特定された脆弱性を適切な期間中に修正する。 ・上記のプロセスから得た情報を組織内の他のシステムの管理者と共有することによって、他の情報システム内の同様の脆弱性を把握し、必要に応じて修正する。 [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/CVSS.html)を参考とすることが可能である。
						Basic	・組織は、情報システムおよびアプリケーションの脆弱性のスキャンを定期的に実施する
		A.12.6.2 ソフトウェアのインストールの制限	利用者によるソフトウェアのインストールを管理する規則を確立し，実施しなければならない。	CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	H.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実行を許可するソフトウェアの一覧(ホワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)を用いてソフトウェアの制限を実施する、あるいは、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。
						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。
						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。
	A.12.7 情報システムの監査に対する考慮事項	A.12.7.1 情報システムの監査に対する管理策	運用システムの検証を伴う監査要求事項及び監査活動は，業務プロセスの中断を最小限に抑えるために，慎重に計画し，合意しなければならない。	CPS.SC-6	・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、または他の形式の評価を使用して定期的に評価する。	H.Advanced	・組織は、契約事項からの逸脱および、その兆候に対する調査・対応のためのプロシージャ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、特に重要な取引先およ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。 ・重要な取引先およ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。
						Advanced	・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。 ・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情報システムが提供する。 ・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。 ・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でレビュー・分析して、契約事項からの逸脱および、その兆候の有無を確認する。 ・チェックリストを用いた取引先による内部監査により、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。
				CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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)管理される。 ・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機器からの監査ログの収集・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。
						Advanced	・情報システム及び産業用制御システムは、監査ログおよ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、監査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。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査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、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
A.13 通信のセキュリティ	A.13.1 ネットワークセキュリティ管理	A.13.1.1 ネットワーク管理策	システム及びアプリケーション内の情報を保護するために，ネットワークを管理し，制御しなければならない。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜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)等してネットワークの完全性を保護する。	H.Advanced	・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システムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・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。 ・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。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界(産業用制御システムの場合は情報システムとの境界)について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。
				CPS.AC-9	・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）に見合う形で認証・認可する。	H.Advanced	・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。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、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)に見合うメカニズムの強度を持った認証を実施する。 ・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、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H.Advanced	・組織は、情報システム及び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。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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)管理される。 ・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機器からの監査ログの収集・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。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査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、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
		A.13.1.2 ネットワークサービスのセキュリティ	組織が自ら提供するか外部委託しているかを問わず，全てのネットワークサービスについて，セキュリティ機能，サービスレベル及び管理上の要求事項を特定しなければならず，また，ネットワークサービス合意書にもこれらを盛り込まなければならない。	CPS.SC-4	・外部の組織との契約を行う場合、目的およ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の提供する製品・サービスが適合していることを確認する。	H.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せているかを、自組織あるいは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、適切なプロシージャで製造されたものかを確認する。
						Advanced	・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 EDSA認証、ITセキュリティ評価及び認証制度(JISEC))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 ・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・供給にて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。 ・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、運用および改善する。 － 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
				CPS.CM-5	・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モニタリングする。	H.Advanced	・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にするよう要求する。 ・組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。
						Advanced	・組織は、外部サービスプロバイダおよびシステム開発の委託先の要員に対しての セキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダーおよ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およ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。
						Basic	・組織は、外部情報システムサービスのプロバイダおよびシステム開発の委託先に対して、自組織が対象となっている、あるいは当該プロバイダーが対象として該当するルールに従って、例えば下記に関連するようなセキュリティ要求事項を設定し、導入することを要求する。 － (例えば、ISMS認証取得相当の)セキュリティ対策が十分に行われていること － 運用中のデータが適切に管理されること － サービス利用終了時にデータが適切に削除されること
		A.13.1.3 ネットワークの分離	情報サービス，利用者及び情報システムは，ネットワーク上で，グループごとに分離しなければならない。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜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)等してネットワークの完全性を保護する。	H.Advanced	・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システムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・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。 ・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。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界(産業用制御システムの場合は情報システムとの境界)について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。
	A.13.2 情報の転送	A.13.2.1 情報転送の方針及び手順	あらゆる形式の通信設備を利用した情報転送を保護するために，正式な転送方針，手順及び管理策を備えなければならない。	CPS.AM-4	・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。	H.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。
						Advanced	・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。
						Basic	・組織は、自組織が管理する範囲(例：事業所単位で)における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、データフローを文書化し、保管する。 ・組織は、定期的、あるいは、システム構成、ネットワーク構成、データフローに変更が生じた場合、関連する文書をレビューし、必要に応じて更新する。 [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, 2018年)の3.2、3.3を参照することが可能である。
				CPS.AM-5	・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。	H.Advanced	・システムは、自組織が利用している外部情報システムサービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・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。 ・組織は、外部プロバイダによる情報システムサービスを使用する際に必要な機能、ポート、プロトコル、および他のサービスを明確にする。
						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 ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。
				CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜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)等してネットワークの完全性を保護する。	H.Advanced	・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システムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・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。 ・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。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界(産業用制御システムの場合は情報システムとの境界)について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。
						Basic	・組織は、情報システム及び産業用制御システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、適切に論理的あるいは物理的にネットワークを分離することで、フローの制御を実施する。 ・組織は、産業用制御システムにおいて、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。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H.Advanced	・組織は、情報システム及び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。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。	H.Advanced	・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。 ・情報システムは、重要度の高い・低いに限らず、組織外部へ送信するすべてのデータを適切な強度で暗号化する。
						Advanced	・組織は、機密性の高い情報を外部の組織等へ送信する際、情報を適切な強度の方式で暗号化する。
				CPS.CM-4	・サイバー空間から受ける情報の完全性および真正性を動作前に確認する。	H.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。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、機器間の相互認証が成功した後に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。 ・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。
						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に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。
		A.13.2.2 情報転送に関する合意	合意では，組織と外部関係者との間の業務情報のセキュリティを保った転送について，取り扱わなければならない。	CPS.AM-4	・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。	H.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。
						Advanced	・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。
						Basic	・組織は、自組織が管理する範囲(例：事業所単位で)における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、データフローを文書化し、保管する。 ・組織は、定期的、あるいは、システム構成、ネットワーク構成、データフローに変更が生じた場合、関連する文書をレビューし、必要に応じて更新する。 [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, 2018年)の3.2、3.3を参照することが可能である。
				CPS.DS-1	・組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取り決める。	Advanced	・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、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。
						Basic	・組織は、取引先が取り扱う可能性のあるデータに関して、秘密保持契約を締結することで、取り扱いを規定する。 ・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。 [参考]「中小企業の情報セキュリティ対策ガイドライン 第2.1版」(IPA, 2018年)で、委託契約時の機密保持契約条項のサンプルを提供している。
		A.13.2.3 電子的メッセージ通信	電子的メッセージ通信に含まれた情報は，適切に保護しなければならない。	CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H.Advanced	・組織は、情報システム及び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。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、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。
				CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。	H.Advanced	・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。 ・情報システムは、重要度の高い・低いに限らず、組織外部へ送信するすべてのデータを適切な強度で暗号化する。
						Advanced	・組織は、機密性の高い情報を外部の組織等へ送信する際、情報を適切な強度の方式で暗号化する。
				CPS.CM-4	・サイバー空間から受ける情報の完全性および真正性を動作前に確認する。	H.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。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、機器間の相互認証が成功した後に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。 ・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。
						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に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。
		A.13.2.4 秘密保持契約又は守秘義務契約	情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は，特定し，定めに従ってレビューし，文書化しなければならない。	CPS.SC-3	・外部の組織との契約を行う場合、目的およ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のセキュリティマネジメントが適合していることを確認する。	H.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およ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。
						Advanced	・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、および基準を記載する。 － 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 ・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。 ・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およ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
						Basic	・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。 ・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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
A.14 システムの取得，開発及び保守	A.14.1 情報システムのセキュリティ要求事項	A.14.1.1 情報セキュリティ要求事項の分析及び仕様化	情報セキュリティに関連する要求事項は，新しい情報システム又は既存の情報システムの改善に関する要求事項に含めなければならない。	CPS.SC-4	・外部の組織との契約を行う場合、目的およ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の提供する製品・サービスが適合していることを確認する。	H.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せているかを、自組織あるいは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、適切なプロシージャで製造されたものかを確認する。
						Advanced	・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 EDSA認証、ITセキュリティ評価及び認証制度(JISEC))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 ・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・供給にて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。 ・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、運用および改善する。 － 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、搬送中のなりすまし・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 － 電波：暗号化、電波データ全体のハッシュ値等
				CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。	H.Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 －セキュリティ機能に関する要求事項 －セキュリティ強度に関する要求事項 －セキュリティ保証に関する要求事項 －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 －そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 －受け入れ基準
						Advanced	・組織は、情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
						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。
		A.14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	公衆ネットワークを経由するアプリケーションサービスに含まれる情報は，不正行為，契約紛争，並びに認可されていない開示及び変更から保護しなければならない。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜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)等してネットワークの完全性を保護する。	H.Advanced	・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システムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・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。 ・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。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界(産業用制御システムの場合は情報システムとの境界)について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H.Advanced	・組織は、情報システム及び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。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、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。
				CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。	H.Advanced	・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。 ・情報システムは、重要度の高い・低いに限らず、組織外部へ送信するすべてのデータを適切な強度で暗号化する。
						Advanced	・組織は、機密性の高い情報を外部の組織等へ送信する際、情報を適切な強度の方式で暗号化する。
				CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する。	H.Advanced	・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。 ・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。
						Advanced	・組織は、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、保管データの完全性チェックを定期的に実施する。 ・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。
		A.14.1.3 アプリケーションサービスのトランザクションの保護	アプリケーションサービスのトランザクションに含まれる情報は，次の事項を未然に防止するために，保護しなければならない。 － 不完全な通信 － 誤った通信経路設定 － 認可されていないメッセージの変更 － 認可されていない開示 － 認可されていないメッセージの複製又は再生	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜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)等してネットワークの完全性を保護する。	H.Advanced	・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システムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・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。 ・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。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界(産業用制御システムの場合は情報システムとの境界)について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。
				CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・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。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H.Advanced	・組織は、情報システム及び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。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、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。
				CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する。	H.Advanced	・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。 ・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。
						Advanced	・組織は、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、保管データの完全性チェックを定期的に実施する。 ・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。
				CPS.CM-4	・サイバー空間から受ける情報の完全性および真正性を動作前に確認する。	H.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。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、機器間の相互認証が成功した後に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。 ・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。
						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に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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
	A.14.2 開発及びサポートプロセスにおけるセキュリティ	A.14.2.1 セキュリティに配慮した開発のための方針	ソフトウェア及びシステムの開発のための規則は，組織内において確立し，開発に対して適用しなければならない。	CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。	H.Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 −セキュリティ機能に関する要求事項 −セキュリティ強度に関する要求事項 −セキュリティ保証に関する要求事項 −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 −そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 −受け入れ基準
						Advanced	・組織は、情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
						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。
		A.14.2.2 システムの変更管理手順	開発のライフサイクルにおけるシステムの変更は，正式な変更管理手順を用いて管理しなければならない。	CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。	H.Advanced	・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、それらの変更をテスト・承認・文書化する。 ・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対けるセキュリティに係る変更管理手順を、既存のプロセス変全管理の手順に統合する。
						Advanced	・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、実施手順等の を文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・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、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法(例：変更実施前に本人にしかわからないセキュリティコードを入力させる)を利用する。 ・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。
				CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。	H.Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 −セキュリティ機能に関する要求事項 −セキュリティ強度に関する要求事項 −セキュリティ保証に関する要求事項 −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 −そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 −受け入れ基準
						Advanced	・組織は、情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
		A.14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	オペレーティングプラットフォームを変更するときは，組織の運用又はセキュリティに悪影響がないことを確実にするために，重要なアプリケーションをレビューし，試験しなければならない。	CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。	H.Advanced	・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、それらの変更をテスト・承認・文書化する。 ・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対けるセキュリティに係る変更管理手順を、既存のプロセス変全管理の手順に統合する。
						Advanced	・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、実施手順等の を文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・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、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法(例：変更実施前に本人にしかわからないセキュリティコードを入力させる)を利用する。 ・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。
				CPS.IP-10	・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。	H.Advanced	・組織は、欠陥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。
						Advanced	・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欠陥の修正を実施し、当該修正を構成管理として管理する。
		A.14.2.4 パッケージソフトウェアの変更に対する制限	パッケージソフトウェアの変更は，抑止しなければならず，必要な変更だけに限らなければならない。また，全ての変更は，厳重に管理しなければならない。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェアおよびその管理情報（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。	Advanced	・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、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、組織内で規定されたポータブルストレージデバイス(例：USBメモリ)のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
				CPS.MA-1	・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。 ・可能であれば、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。	H.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。
						Advanced	・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、実施、確認、文書化する。 ・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を自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・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。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
		A.14.2.5 セキュリティに配慮したシステム構築の原則	セキュリティに配慮したシステムを構築するための原則を確立し，文書化し，維持し，全ての情報システムの実装に対して適用しなければならない。	CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。	H.Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 −セキュリティ機能に関する要求事項 −セキュリティ強度に関する要求事項 −セキュリティ保証に関する要求事項 −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 −そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 −受け入れ基準
						Advanced	・組織は、情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
		A.14.2.6 セキュリティに配慮した開発環境	組織は，全てのシステム開発ライフサイクルを含む，システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し，適切に保護しなければならない。	CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。	H.Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 −セキュリティ機能に関する要求事項 −セキュリティ強度に関する要求事項 −セキュリティ保証に関する要求事項 −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 −そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 −受け入れ基準
						Advanced	・組織は、情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
						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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.14.2.7 外部委託による開発	組織は，外部委託したシステム開発活動を監督し，監視しなければならない。	CPS.SC-6	・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、または他の形式の評価を使用して定期的に評価する。	H.Advanced	・組織は、契約事項からの逸脱および、その兆候に対する調査・対応のためのプロシージャ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、特に重要な取引先およ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。 ・重要な取引先およ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。
						Advanced	・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。 ・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情報システムが提供する。 ・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。 ・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でレビュー・分析して、契約事項からの逸脱および、その兆候の有無を確認する。 ・チェックリストを用いた取引先による内部監査により、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。
				CPS.CM-5	・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モニタリングする。	H.Advanced	・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にするよう要求する。 ・組織は、上記で明確化した事項が遵守されているかどうかをモニタリングする。
						Advanced	・組織は、外部サービスプロバイダおよびシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダーおよ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モニタリングする。 ・組織は、外部サービスプロバイダーおよ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。
						Basic	・組織は、外部情報システムサービスのプロバイダおよびシステム開発の委託先に対して、自組織が対象となっている、あるいは当該プロバイダーが対象として該当するルールに従って、例えば下記に関連するようなセキュリティ要求事項を設定し、導入することを要求する。 －（例えば、ISMS認証取得相当の）セキュリティ対策が十分に行われていること －運用中のデータが適切に管理されること －サービス利用終了時にデータが適切に削除されること
		A.14.2.8 システムセキュリティの試験	セキュリティ機能（functionality）の試験は，開発期間中に実施しなければならない。	CPS.DP-3	・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。	H.Advanced	・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、継続的なモニタリングに用いられている活動の修正の必要性を判断する。 ・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、ツールの設置方法により変わる。
						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。 ・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。
		A.14.2.9 システムの受入れ試験	新しい情報システム，及びその改訂版・更新版のために，受入れ試験のプログラム及び関連する基準を確立しなければならない。	CPS.SC-4	・外部の組織との契約を行う場合、目的およ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の提供する製品・サービスが適合していることを確認する。	H.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せているかを、自組織あるいは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、適切なプロシージャで製造されたものかを確認する。
						Advanced	・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 EDSA認証、ITセキュリティ評価及び認証制度(JISEC))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 ・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・供給にて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。 ・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、運用および改善する。 －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 －電波：暗号化、電波データ全体のハッシュ値等
	A.14.3 試験データ	A.14.3.1 試験データの保護	試験データは，注意深く選定し，保護し，管理しなければならない。	CPS.SC-4	・外部の組織との契約を行う場合、目的およ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の提供する製品・サービスが適合していることを確認する。	H.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せているかを、自組織あるいは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、適切なプロシージャで製造されたものかを確認する。
				CPS.SC-6	・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、または他の形式の評価を使用して定期的に評価する。	H.Advanced	・組織は、契約事項からの逸脱および、その兆候に対する調査・対応のためのプロシージャ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、特に重要な取引先およ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。 ・重要な取引先およ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。
						Advanced	・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。 ・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情報システムが提供する。 ・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。 ・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でレビュー・分析して、契約事項からの逸脱および、その兆候の有無を確認する。 ・チェックリストを用いた取引先による内部監査により、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。
				CPS.IP-4	・構成要素（IoT機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする。	H.Advanced	・組織は、バックアップ情報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。
				CPS.PT-1	・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、そうした記録を実施して、レビューする。	H.Advanced	・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）管理される。 ・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機器からの監査ログの収集・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。
						Advanced	・情報システム及び産業用制御システムは、監査ログおよ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、監査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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
A.15 供給者関係	A.15.1 供給者関係における情報セキュリティ	A.15.1.1 供給者関係のための情報セキュリティの方針	組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化しなければならない。	CPS.AM-7	・自組織および関係する他組織のサイバーセキュリティ上の役割と責任を定める。	Advanced	・組織は、セキュリティインシデントにより損害が発生する場合に備えて、取引先等から指定されるセキュリティ対策の実装に加え、サイバー保険の利用等によるリスク移転を検討する。
						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。 ・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、「クラウドセキュリティガイドライン活用ガイドブック 2013年度版」(経済産業省, 2013年)の "4.4.クラウドサービスの契約" を参照することが可能である。
				CPS.SC-1	・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、その内容について取引先と合意する。	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。 1)調達する製品またはサービスの仕様 2)供給者が製品またはサービスを供給している間に従うセキュリティ要件 3)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およびその指標 4)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 5)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、取引先によるセキュリティ管理策の遵守状況を継続的にモニタリングするための、プロシージャを整備する。 ・取引先におけるセキュリティインシデントが自組織に影響した場合に備え、契約書にて外部事業者との責任分界点を明確にし、外部事業者の責任範囲において自組織に被害が発生した場合の損害賠償について記載する等の対応を行う。
						Basic	・組織は、該当する法規制等を参照して、取引先(特に、自組織のデータを取り扱う可能性のある、またはデータを取り扱うための基盤を提供する可能性のあるもの)に対して適用するセキュリティ対策基準を策定し、内容について合意する。 ・組織は、取引先(外部情報システムサービスのプロバイダ)に対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にする。 [参考] 取引先に対して適用するセキュリティ対策基準の策定に当たり、ISO/IEC 27001 附属書Aの管理策をベースに作成された「情報セキュリティベンチマーク」(IPA)や、「サプライチェーン情報セキュリティ管理基準」(日本セキュリティ監査協会)等を参考とすることが可能である。
				CPS.SC-2	・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、優先付けをし、評価する。	H.Advanced	・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、優先順位付けする。 ・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および、その起こりやすさ、規模を推定する。 ※ 関連する対策要件に、CPS.AM-6, CPS.BE-2等がある。
						Advanced	・組織は、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サプライチェーン上の取引先を特定し、当該組織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。
						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、優先順位付けする。 ・組織は、長期に渡って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
				CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、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。	Advanced	・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。
		A.15.1.2 供給者との合意におけるセキュリティの取扱い	関連する全ての情報セキュリティ要求事項を確立しなければならず，また，組織の情報に対して，アクセス，処理，保存若しくは通信を行う，又は組織の情報のための IT 基盤を提供する可能性のあるそれぞれの供給者と，この要求事項について合意しなければならない。	CPS.SC-1	・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、その内容について取引先と合意する。	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。 1)調達する製品またはサービスの仕様 2)供給者が製品またはサービスを供給している間に従うセキュリティ要件 3)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およびその指標 4)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 5)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、取引先によるセキュリティ管理策の遵守状況を継続的にモニタリングするための、プロシージャを整備する。 ・取引先におけるセキュリティインシデントが自組織に影響した場合に備え、契約書にて外部事業者との責任分界点を明確にし、外部事業者の責任範囲において自組織に被害が発生した場合の損害賠償について記載する等の対応を行う。
						Basic	・組織は、該当する法規制等を参照して、取引先(特に、自組織のデータを取り扱う可能性のある、またはデータを取り扱うための基盤を提供する可能性のあるもの)に対して適用するセキュリティ対策基準を策定し、内容について合意する。 ・組織は、取引先(外部情報システムサービスのプロバイダ)に対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にする。 [参考] 取引先に対して適用するセキュリティ対策基準の策定に当たり、ISO/IEC 27001 附属書Aの管理策をベースに作成された「情報セキュリティベンチマーク」(IPA)や、「サプライチェーン情報セキュリティ管理基準」(日本セキュリティ監査協会)等を参考とすることが可能である。
				CPS.SC-2	・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、優先付けをし、評価する。	H.Advanced	・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、優先順位付けする。 ・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および、その起こりやすさ、規模を推定する。 ※ 関連する対策要件に、CPS.AM-6, CPS.BE-2等がある。
						Advanced	・組織は、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サプライチェーン上の取引先を特定し、当該組織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。
						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、優先順位付けする。 ・組織は、長期に渡って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

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.SC-3	・外部の組織との契約を行う場合、目的およ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のセキュリティマネジメントが適合していることを確認する。	H.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およ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。
						Advanced	・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、および基準を記載する。 － 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 ・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。 ・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およ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
						Basic	・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。 ・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。
		A.15.1.3 ICTサプライチェーン	供給者との合意には，情報通信技術（ICT）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めなければならない。	CPS.SC-4	・外部の組織との契約を行う場合、目的およ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の提供する製品・サービスが適合していることを確認する。	H.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せているかを、自組織あるいは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、適切なプロシージャで製造されたものかを確認する。
						Advanced	・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 EDSA認証、ITセキュリティ評価及び認証制度(JISEC))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 ・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・供給にて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。 ・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、運用および改善する。 － 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
	A.15.2 供給者のサービス提供の管理	A.15.2.1 供給者のサービス提供の監視及びレビュー	組織は，供給者のサービス提供を定常的に監視し，レビューし，監査しなければならない。	CPS.SC-1	・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、その内容について取引先と合意する。	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。 1）調達する製品またはサービスの仕様 2）供給者が製品またはサービスを供給している間に従うセキュリティ要件 3）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およびその指標 4）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 5）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、取引先によるセキュリティ管理策の遵守状況を継続的にモニタリングするための、プロシージャを整備する。 ・取引先におけるセキュリティインシデントが自組織に影響した場合に備え、契約書にて外部事業者との責任分界点を明確にし、外部事業者の責任範囲において自組織に被害が発生した場合の損害賠償について記載する等の対応を行う。
				CPS.SC-6	・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、または他の形式の評価を使用して定期的に評価する。	H.Advanced	・組織は、契約事項からの逸脱および、その兆候に対する調査・対応のためのプロシージャ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、特に重要な取引先およ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。 ・重要な取引先およ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。
						Advanced	・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。 ・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情報システムが提供する。 ・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。 ・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でレビュー・分析して、契約事項からの逸脱および、その兆候の有無を確認する。 ・チェックリストを用いた取引先による内部監査により、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。
				CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、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。	Advanced	・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。
						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。
				CPS.CM-5	・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モニタリングする。	H.Advanced	・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にするよう要求する。 ・組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。
						Advanced	・組織は、外部サービスプロバイダおよびシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダーおよ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およ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。
						Basic	・組織は、外部情報システムサービスのプロバイダおよびシステム開発の委託先に対して、自組織が対象となっている、あるいは当該プロバイダーが対象として該当するルールに従って、例えば下記に関連するようなセキュリティ要求事項を設定し、導入することを要求する。 － (例えば、ISMS認証取得相当の)セキュリティ対策が十分に行われていること － 運用中のデータが適切に管理されること － サービス利用終了時にデータが適切に削除されること

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.15.2.2 供給者のサービス提供の変更に対する管理	関連する業務情報，業務システム及び業務プロセスの重要性，並びにリスクの再評価を考慮して，供給者によるサービス提供の変更（現行の情報セキュリティの方針群，手順及び管理策の保守及び改善を含む。）を管理しなければならない。	CPS.CM-5	・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モニタリングする。	H.Advanced	・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にするよう要求する。 ・組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。
						Advanced	・組織は、外部サービスプロバイダおよびシステム開発の委託先の要員に対しての セキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報，業務システム及び業務プロセスの重要性，並びにリスクの再評価を考慮して，外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダーおよ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モニタリングする。 ・組織は、外部サービスプロバイダーおよ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。
A.16 情報セキュリティインシデント管理	A.16.1 情報セキュリティインシデントの管理及びその改善	A.16.1.1 責任及び手順	情報セキュリティインシデントに対する迅速，効果的かつ順序だった対応を確実にするために，管理層の責任及び手順を確立しなければならない。	CPS.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	H.Advanced	・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、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、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。 [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、たとえば、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。
						Advanced	・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、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。 ・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、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。
						Basic	・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。
		A.16.1.2 情報セキュリティ事象の報告	情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけ速やかに報告しなければならない。	CPS.SC-5	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	H.Advanced	・組織は、委託先の要員により委託元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シージャを整備する。
						Advanced	・サプライヤー関係のセキュリティ面について該当する要員を訓練し、機密情報の取り扱いが正しく理解されていることを特に確認する。 ・委託業務の遂行に当たり、委託元が要求するセキュリティ要求事項が遵守されていることを定期的に確認する。
						Basic	・委託業務に係るデータの内、機密データや知的財産のように、公開または変更すべきではないものへのアクセスおよびデータの開示または変更に関わる要員を特定し、評価する。 ・組織は、委託先との契約の終了後、速やかに委託先の要員に対する自組織施設へのアクセス権限等の、一時的に許可していた権限を停止する。
				CPS.RP-1	・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。	Advanced	・組織は、セキュリティ運用マニュアルにおいてインシデントの検知および分析、封じ込め、低減、復旧を含む内容を規定する。 － すべてのインシデントの取り扱いに関する記録をとる － 外部組織等に対して、インシデント発生の事実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
						Basic	・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。当該プロセスには、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, 2015年)、SP 800-61 rev.1 (NIST, 2008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。
				CPS.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	H.Advanced	・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、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、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。 [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、たとえば、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。
						Advanced	・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、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。 ・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、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。
						Basic	・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。
		A.16.1.3 情報セキュリティ弱点の報告	組織の情報システム及びサービスを利用する従業員及び契約相手に，システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は，どのようなものでも記録し，報告するように要求しなければならない。	CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。	H.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およ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。
						Advanced	・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位、およびメトリクスを考慮してインシデントを分類する。 ・組織は、自組織に影響を及ぼすセキュリティインシデントを追跡し、文書化する。 "SP 800-61 rev.1" では、セキュリティインシデントを文書化する際の記載の観点として、下記を例示している。 － インシデントの現在の状況 － インシデントの概要 － 当該インシデントに対して自組織のとった行動の内容 － ほかの関係者(システム所有者、システム管理者等)の連絡先情報 － 調査の際に収集した証拠の一覧 － インシデントの処理担当者からのコメント － 次にとるべきステップ
						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、優先順位付けする。 ※ CPS.AM-6, CPS.BE-2に同様の対策例を記載 ・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]セキュリティインシデントの影響の大きさを測るための尺度を検討する場合、下記文書等を参照することができる。 ・SP 800-61 rev.1 (NIST, 2008年) 3.2.6 事件の優先順位付け ・「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準」(NISC, 2018年)

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.16.1.4 情報セキュリティ事象の評価及び決定	情報セキュリティ事象は，これを評価し，情報セキュリティインシデントに分類するか否かを決定しなければならない。	CPS.AE-5	・セキュリティ事象の危険度の判定基準を定める。	H.Advanced	・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、優先順位付けする。 ※ CPS.AM-6, CPS.BE-2に同様の対策例を記載 ・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およ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。
						Advanced	・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位、およびメトリクスを考慮してインシデントを分類する。
						Basic	・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、下記文書等を参照することができる。 ・SP 800-61 rev.1 (NIST, 2008年) 3.2.6 事件の優先順位付け ・「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準」(NISC, 2018年)
				CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。	H.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およ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。
						Advanced	・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位、およびメトリクスを考慮してインシデントを分類する。 ・組織は、自組織に影響を及ぼすセキュリティインシデントを追跡し、文書化する。 “SP 800-61 rev.1” では、セキュリティインシデントを文書化する際の記載の観点として、下記を例示している。 － インシデントの現在の状況 － インシデントの概要 － 当該インシデントに対して自組織のとった行動の内容 － ほかの関係者(システム所有者、システム管理者等)の連絡先情報 － 調査の際に収集した証拠の一覧 － インシデントの処理担当者からのコメント － 次にとるべきステップ
						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、優先順位付けする。 ※ CPS.AM-6, CPS.BE-2に同様の対策例を記載 ・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]セキュリティインシデントの影響の大きさを測るための尺度を検討する場合、下記文書等を参照することができる。 ・SP 800-61 rev.1 (NIST, 2008年) 3.2.6 事件の優先順位付け ・「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準」(NISC, 2018年)
		A.16.1.5 情報セキュリティインシデントへの対応	情報セキュリティインシデントは，文書化した手順に従って対応しなければならない。	CPS.SC-5	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	H.Advanced	・組織は、委託先の要員により委託元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シージャを整備する。
						Advanced	・サプライヤー関係のセキュリティ面について該当する要員を訓練し、機密情報の取り扱いが正しく理解されていることを特に確認する。
						Basic	・委託業務の遂行に当たり、委託元が要求するセキュリティ要求事項が遵守されていることを定期的に確認する。 ・委託業務に係るデータの内、機密データや知的財産のように、公開または変更すべきではないものへのアクセスおよびデータの開示または変更に関わる要員を特定し、評価する。 ・組織は、委託先との契約の終了後、速やかに委託先の要員に対する自組織施設へのアクセス権限等の、一時的に許可していた権限を停止する。
				CPS.AE-2	・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)を立ち上げ、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。	H.Advanced	・組織は、セキュリティ専門の24時間365日モニタリングモニタリングにより収集した監査ログを、分析自動化ツール等を利用することで効率的に分析する。 ・組織は、従来のIT環境だけでなく、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、セキュリティ対応組織の成熟度を定期的に評価し、セキュリティ状況のモニタリングやインシデントへの対応等の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。 [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成熟度セルフチェックシート」(ISOG-J, 2018年)や、SIM3(Security Incident Management Maturity Model)等がある。
						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 (CPS.AE-3を参照) ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・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(プロセスの内容については、CPS.RP-1等を参照)。 ・組織およ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 [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 ～ 機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年)等を参照することが望ましい。
				CPS.RP-1	・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。	H.Advanced	・情報システム及び産業用制御システムは、有効でないインプットデータを受け取った場合に、組織の目的とシステムの目的に沿って、予想できる形で、かつ記載どおりに動作する。
						Advanced	・組織は、セキュリティ運用マニュアルにおいてインシデントの検知および分析、封じ込め、低減、復旧を含む内容を規定する。 － すべてのインシデントの取り扱いに関する記録をとる － 外部組織等に対して、インシデント発生の事実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
						Basic	・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。当該プロセスには、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, 2015年)、SP 800-61 rev.1 (NIST, 2008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。
				CPS.MI-1	・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、影響を低減する対応を行う。	H.Advanced	・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。 ・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。 [参考]対応段階におけるインシデントの影響低減、復旧段階において有用に機能すると考えられる情報の例として、「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」 v1.0 」(ISOG-J, 2017年)では、下記が挙げられる。 ・攻撃行為をセキュリティ製品や関連するシステムで遮断するための設定要件 ・攻撃を無効化する方法(パッチの適用、設定変更等) ・被害を受けたシステム復旧方法
						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(たとえば、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。 [参考]セキュリティインシデントの影響低減のための活動は、インシデントの性質(例えば、サービス拒否攻撃、マルウェア感染、不正アクセスのような顕在化する脅威の差異)により内容が異なる場合がある。より詳細な影響低減活動の情報については、「インシデントハンドリングマニュアル」(JPCERT/CC, 2015年)、SP 800-61 rev.1 (NIST, 2008年)等を参照することが望ましい。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.16.1.6 情報セキュリティインシデントからの学習	情報セキュリティインシデントの分析及び解決から得られた知識は，インシデントが将来起こる可能性又はその影響を低減するために用いなければならない。	CPS.IP-7	・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改善する。	H.Advanced	・組織は、第三者によるセキュリティ評価を実施する。
						Advanced	・組織は、セキュリティ評価を適切に、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評価計画を策定した上で、セキュリティ評価を実施する。 －セキュリティ評価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評価手順 －セキュリティ評価を実施する環境や実施体制 －セキュリティ評価結果の取りまとめ方法とその活用方法
						Basic	・組織は、セキュリティ対策が正しく実装されているか及び運用されているかに加え、セキュリティ対策が期待された成果を上げているかに関する定期的に評価（セキュリティ評価）を実施し、管理責任者へ報告する。 ・組織は、セキュリティ評価の結果に基づき、セキュリティ対策の改善を実施する。
				CPS.IP-8	・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。	H.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。
						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。
						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。
				CPS.DP-4	・セキュリティ事象の検知プロセスを継続的に改善する。	H.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およ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、検出漏れの数を減らすためのチューニングを行う。
						Advanced	・組織は、経営層等の組織内の然るべき要員に、定期的に組織およびシステムのセキュリティの状態を報告するプロシージャを整備し、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」 v1.0」(ISOG-J, 2017年)より引用している。 ・攻撃の特徴 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
				CPS.IM-1	・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、セキュリティ運用プロセスを継続的に改善する。	H.Advanced	・情報システムが、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ことが望ましい。
						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。 ・セキュリティインシデントへの対応活動から学んだ教訓を事業継続計画又はコンティンジェンシープラン、教育／訓練に取り入れて、結果として必要となる変更を実施する。NIST SP 800-61には、教訓を抽出する際の観点として下記が例として示されている。 － 正確に何がいつ起きたか。 － スタッフとマネジメント層がどの程度うまく事件に対処したか。文書化された手順に従ったか。それは適切だったか。 － すぐに必要になった情報は何か。 － 復旧を妨げたかもしれないステップや行動があったか。 － 次に同様の事件が起きた場合、スタッフやマネジメント層は、どのような違った行動をとるか。 － どのような是正措置があれば，将来にわたって同じ様な事件が起きるのを防げるか。 － 将来事件を検出、分析、軽減するために、どのようなツールやリソースが追加で必要となるか。
		A.16.1.7 証拠の収集	組織は，証拠となり得る情報の特定，収集，取得及び保存のための手順を定め，適用しなければならない。	CPS.AN-2	・セキュリティインシデント発生後に、デジタルフォレンジックを実施する。	H.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。
						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、発生後に下記の証跡を保全することが望ましい。 － 識別情報(インシデントの発生場所/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) － 証跡を収集・処理したヒトの役職、名前、連絡先 － 証跡保全処理の日時(タイムゾーンを含む)
						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。
A.17 事業継続マネジメントにおける情報セキュリティの側面	A.17.1 情報セキュリティ継続	A.17.1.1 情報セキュリティ継続の計画	組織は，困難な状況（adverse situation）（例えば，危機又は災害）における，情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しなければならない。	CPS.RP-3	・自然災害時における対応方針および対応手順を定めている事業継続計画又は緊急事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。	Advanced	・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事対応計画を策定し、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事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。
				CPS.RP-4	・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。	Advanced	・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、復旧活動およ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.AM-2, CPS.AM-3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。 ※ CPS.CO-3と関連
						Basic	・自組織の業種等を考慮して、事業継続計画又は緊急事対応計画の中に、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事対応計画は、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。
		A.17.1.2 情報セキュリティ継続の実施	組織は，困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための，プロセス，手順及び管理策を確立し，文書化し，実施し，維持しなければならない。	CPS.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	H.Advanced	・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、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、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。 [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、たとえば、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。
						Advanced	・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、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。 ・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、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。
				CPS.CO-3	・復旧活動について内部および外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急事対応計画の中に位置づける。	Advanced	・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。 ・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、復旧活動およ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。
						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。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.17.1.3 情報セキュリティ継続の検証，レビュー及び評価	確立及び実施した情報セキュリティ継続のための管理策が，困難な状況の下で妥当かつ有効であることを確実にするために，組織は，定められた間隔でこれらの管理策を検証しなければならない。	CPS.IM-2	・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事対応計画を継続的に改善する。	Basic	・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およ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。 ・セキュリティインシデントへの対応活動から学んだ教訓を事業継続計画又は緊急事対応計画、教育／訓練に取り入れて、結果として必要となる変更を実施する。
	A.17.2 冗長性	A.17.2.1 情報処理施設の可用性	情報処理施設は，可用性の要求事項を満たすのに十分な冗長性をもって，導入しなければならない。	CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する。	Advanced	・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 ・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ず，また，将来必要とする容量・能力を予測しなければならない。 ・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
						Basic	・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。
				CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	Advanced	・装置は，サポートユーティリティの不具合による，停電，その他の故障から保護する。 ・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は，傍受，妨害又は損傷から保護する。 ・装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守する。 ・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。
						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ず，また，将来必要とする容量・能力を予測する。 ・装置は，サポートユーティリティの不具合による，停電，その他の故障から保護する。 ・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は，傍受，妨害又は損傷から保護する。 ・装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守する。
A.18 順守	A.18.1 法的及び契約上の要求事項の順守	A.18.1.1 適用法令及び契約上の要求事項の特定	各情報システム及び組織について，全ての関連する法令，規制及び契約上の要求事項，並びにこれらの要求事項を満たすための組織の取組みを，明確に特定し，文書化し，また，最新に保たなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	Basic	・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。 ・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。 ・管理者は，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。 [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 ,2019年)、「限定提供データに関する指針」(2019年 1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, 2019年)、「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, 2017年))を参照することが望ましい。
				CPS.GV-3	・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。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法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識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例:割賦販売法におけるカード情報の非保持化)
				CPS.DP-2	・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する。	Basic	・組織は、モニタリング業務に関係する法制度、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する。 ・組織は、上記で認識したルールに準拠してモニタリングを実施し、セキュリティ事象を検知する。 ・組織は、自組織のモニタリング活動がルールに準拠したものかどうかを定期的にレビューし、確認する。
		A.18.1.2 知的財産権	知的財産権及び権利関係のあるソフトウェア製品の利用に関連する，法令，規制及び契約上の要求事項の順守を確実にするための適切な手順を実施しなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	Basic	・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。 ・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。 ・管理者は，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。 [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 ,2019年)、「限定提供データに関する指針」(2019年 1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, 2019年)、「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, 2017年))を参照することが望ましい。
				CPS.GV-3	・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。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法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識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例:割賦販売法におけるカード情報の非保持化)
		A.18.1.3 記録の保護	記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊，改ざん，認可されていないアクセス及び不正な流出から保護しなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	Basic	・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。 ・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。 ・管理者は，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。 [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 ,2019年)、「限定提供データに関する指針」(2019年 1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, 2019年)、「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, 2017年))を参照することが望ましい。
				CPS.GV-3	・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。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法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識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例:割賦販売法におけるカード情報の非保持化)

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.SC-8	・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。	H.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
						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
						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。
				CPS.IP-4	・構成要素（IoT機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする。	H.Advanced	・組織は、バックアップ情報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。
						Advanced	・組織は、自組織のシステムドキュメントのバックアップを定めたタイミングや頻度で実施する。 ・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。
		A.18.1.4 プライバシー及び個人を特定できる情報（PII）の保護	プライバシー及び PII の保護は，関連する法令及び規制が適用される場合には，その要求に従って確実にしなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	Basic	・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。 ・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。 ・管理者は，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。 [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，2019年)、「限定提供データに関する指針」(2019年，1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，2019年)、「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，2017年))を参照することが望ましい。
				CPS.GV-3	・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。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法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識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)
		A.18.1.5 暗号化機能に対する規制	暗号化機能は，関連する全ての協定，法令及び規制を順守して用いなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	Basic	・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。 ・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。 ・管理者は，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。 [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，2019年)、「限定提供データに関する指針」(2019年，1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，2019年)、「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，2017年))を参照することが望ましい。
				CPS.GV-3	・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。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法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識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)
	A.18.2 情報セキュリティのレビュー	A.18.2.1 情報セキュリティの独立したレビュー	情報セキュリティ及びその実施の管理（例えば，情報セキュリティのための管理目的，管理策，方針，プロセス，手順）に対する組織の取組みについて，あらかじめ定めた間隔で，又は重大な変化が生じた場合に，独立したレビューを実施しなければならない。	CPS.IP-7	・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改善する。	H.Advanced	・組織は、第三者によるセキュリティ評価を実施する。
						Advanced	・組織は、セキュリティ評価を適切に、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評価計画を策定した上で、セキュリティ評価を実施する。 －セキュリティ評価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評価手順 －セキュリティ評価を実施する環境や実施体制 －セキュリティ評価結果の取りまとめ方法とその活用方法
						Basic	・組織は、セキュリティ対策が正しく実装されているか及び運用されているかに加え、セキュリティ対策が期待された成果を上げているかに関する定期的に評価(セキュリティ評価)を実施し、管理責任者へ報告する。 ・組織は、セキュリティ評価の結果に基づき、セキュリティ対策の改善を実施する。

ISO/IEC 27001:2013 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			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.18.2.2 情報セキュリティのための方針群及び標準の順守	管理者は，自分の責任の範囲内における情報処理及び手順が，適切な情報セキュリティのための方針群，標準類，及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューしなければならない。	CPS.RA-4	・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。 ・IoT機器および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。	H.Advanced	・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。 ・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。 [参考]セーフティ設計におけるハザードの特定と分析については、「つながる世界のセーフティ＆セキュリティ設計入門」(IPA, 2015年)の4.2にて具体的な手法が記載されており、参照することが可能である。
						Advanced	・組織は、情報システム、または情報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)、もしくは情報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。 ・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。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 [参考]システムおよ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、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。
						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ことが望ましい。 [参考] セキュリティリスクアセスメントの手法として、「資産ベース」の手法および「事業被害ベース」の手法があることが知られている。資産ベースの手法でリスクアセスメントを実施する場合は「中小企業の情報セキュリティガイドライン 第2.1版」(IPA, 2018年)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, 2018年) 等を、事業被害ベースの手法を実施する場合は「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, 2018年)等を参照することができる。
		A.18.2.3 技術的順守のレビュー	情報システムを，組織の情報セキュリティのための方針群及び標準の順守に関して，定めに従ってレビューしなければならない。	CPS.RA-4	・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。 ・IoT機器および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。	H.Advanced	・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。 ・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。 [参考]セーフティ設計におけるハザードの特定と分析については、「つながる世界のセーフティ＆セキュリティ設計入門」(IPA, 2015年)の4.2にて具体的な手法が記載されており、参照することが可能である。
						Advanced	・組織は、情報システム、または情報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)、もしくは情報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。 ・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。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 [参考]システムおよ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、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。
						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ことが望ましい。 [参考] セキュリティリスクアセスメントの手法として、「資産ベース」の手法および「事業被害ベース」の手法があることが知られている。資産ベースの手法でリスクアセスメントを実施する場合は「中小企業の情報セキュリティガイドライン 第2.1版」(IPA, 2018年)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, 2018年) 等を、事業被害ベースの手法を実施する場合は「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, 2018年)等を参照することができる。