

## 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 Cybersecurity 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 (仮訳)	対策ID	対策要件
特定 (ID)	AM-1	企業内の物理デバイスとシステムの一覧を作成している。	CPS.AM-1	・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する
	AM-2	企業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の一覧を作成している。	CPS.AM-1	
	AM-3	企業内の通信とデータの流れの図を作成している。	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、保管する
	AM-4	外部情報システムの一覧を作成している。	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、保管する
	AM-5	リソース (例: ハードウェア、デバイス、データ、ソフトウェア) を分類、重要度、ビジネス上の価値に基づいて優先順位付けしている。	CPS.AM-6	・リソース (例: ヒト、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、関係者に伝達する
	AM-6	すべての従業員と第三者である利害関係者 (例: 供給業者、顧客、パートナー) に治して、サイバーセキュリティ上の役割と責任を定めている。	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こえる企業の役割を特定し、伝達している。	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こえる企業の位置付けを特定し、伝達している。	CPS.BE-1	
	BE-3	企業のミッション、目標、活動に関して優先順位を定め、伝達している。	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、関係者(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を把握している。	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識別する
	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を定めている。	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コンティンジェンシープランの中にセキュリティ事象を位置づける
	GV-1	自組織の情報セキュリティポリシーを定めている。	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	情報セキュリティ上の役割と責任について、内部と外部パートナーとで調整・連携している。	CPS.GV-1	
	GV-3	プライバシーや市民の自由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を理解し、管理している。	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し、法令や業界のガイドラインの更新に合わせて継続的かつ速やかにルールを見直す
	GV-4	ガバナンスとリスク管理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	・サイバー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	資産の脆弱性を特定し、文書化している。	CPS.RA-1	・自組織の資産の脆弱性を特定し、文書化する
	RA-2	情報共有フォーラム/ソースより、脅威と脆弱性に関する情報を入手している。	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	内外からの脅威を特定し、文書化している。	CPS.RA-3	・自組織の資産に対する脅威を特定し、文書化する
	RA-4	ビジネスに対する潜在的な影響と、その可能性を特定している。	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	リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮している。	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	リスクに対する対応を定め、優先順位付けしている。	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	リスク管理プロセスが自組織の利害関係者によって確立、管理され、承認されている。	CPS.RM-1	・自組織だけでなく、関係者と共同でセキュリティリスクの管理プロセスを確立、承認し、運用する	
RM-2	自組織のリスク許容度を決定し、明確にしている。	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	企業によるリスク許容度の決定が、重要インフラにおける自組織の役割と、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。	CPS.RM-2		
SC-1	サイバーサプライチェーンのリスク管理プロセスは、組織のステークホルダーによって特定され、確立され、評価され、管理され、合意される。	CPS.SC-1	・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、その内容について関係者と合意する	

NIST Cybersecurity 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 (仮訳)	対策ID	対策要件
	SC-2	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を使用して、情報システム、コンポーネント及びサービスのサプライヤ及び第三者パートナーを特定、優先順位付け、評価する。	CPS.SC-2	<ul style="list-style-type: none"> <li>・ 自組織の事業を継続するに当たり重要なサプライヤーを特定、優先付けをし、評価する</li> <li>・ 機器調達時に、適切なマネジメントシステムが構築・運用され、問い合わせ窓口やサポート体制等が確立されたIoT機器のサプライヤーを選定する</li> <li>・ サービスやシステムの運用において、ITSMS認証等を取得しており、サービスマネジメントを効率的、効果的に運営管理するサービスサプライヤーを選定する</li> </ul>
	SC-3	サプライヤーと第三者パートナーは、情報セキュリティプログラムまたはサイバーサプライチェーンリスクマネジメント計画の目的に合うように設計された適切な措置を実施する契約が要求される。	CPS.SC-3	<ul style="list-style-type: none"> <li>・ 外部の関係者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</li> </ul>
	SC-4	サプライヤとサードパーティのパートナーは、契約上の義務を履行しているかを定期的に評価する。監査のレビュー、検査結果の要約、またはサプライヤ/プロバイダの同等の評価が行われる。	CPS.SC-5	<ul style="list-style-type: none"> <li>・ 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</li> </ul>
	SC-5	応答と復旧の計画とテストは、サプライヤと第三者プロバイダとの間で実施する。	CPS.SC-8	<ul style="list-style-type: none"> <li>・ 応答および復旧の計画とテストは、サプライヤと第三者プロバイダとの間で行われる</li> </ul>
	防御 (PR)	AC-1	承認されたデバイスとユーザの識別情報と認証情報を管理している。	CPS.AC-1
AC-2		資産に対する物理アクセスを管理し、保護している。	CPS.AC-2	<ul style="list-style-type: none"> <li>・ 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</li> </ul>
AC-3		リモートアクセスを管理している。	CPS.AC-3 CPS.AC-4	<ul style="list-style-type: none"> <li>・ 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</li> <li>・ 一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあげる機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ</li> </ul>
AC-4		最小権原及び職務の分離の原則を取り入れて、アクセス権限を管理している。	CPS.AC-5 CPS.AC-6	<ul style="list-style-type: none"> <li>・ ユーザーが利用する機能と、システム管理者が利用する機能を分離する</li> <li>・ 特権を持つユーザーのシステムへのログインに対して、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</li> </ul>
AC-5		適宜、ネットワークの分離を行って、ネットワークの完全性を保護している。	CPS.AC-7	<ul style="list-style-type: none"> <li>・ 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</li> </ul>
AC-6		識別情報は証明され認証情報と結合し、相互に主張されている。	CPS.AC-8	<ul style="list-style-type: none"> <li>・ IoT機器、サーバ等がサイバー空間で得られた分析結果を受信する際、及びIoT機器、サーバ等が生成した情報(データ)をサイバー空間へ送信する際、双方がそれぞれ接続相手のID(識別子)を利用して、接続相手を識別し、認証する</li> <li>・ 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</li> </ul>
AC-7		取り扱いのリスク (例えば、個人のセキュリティ及びプライバシーのリスク及びその他の組織上のリスク)に見合うように、ユーザ、デバイス及びその他の資産が認証されている (例えば、単一認証、多要素認証)	CPS.AC-6 CPS.AC-9	<ul style="list-style-type: none"> <li>・ 特権を持つユーザーのシステムへのログインに対して、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</li> <li>・ IoT機器やユーザーを、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)に見合う形で認証する</li> </ul>
AT-1		全てのユーザに情報を周知し、トレーニングを実施している。	CPS.AT-1	<ul style="list-style-type: none"> <li>・ 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、教育を実施する</li> </ul>
AT-2		権限を持つユーザが役割と責任を理解している。	CPS.AT-1	
AT-3		第三者である利害関係者 (例：供給業者、顧客、パートナー) が役割と責任を理解している。	CPS.AT-2	<ul style="list-style-type: none"> <li>・ 自組織におけるセキュリティインシデントに関係する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する</li> </ul>
AT-4		上級役員が役割と責任を理解している。	CPS.AT-1	<ul style="list-style-type: none"> <li>・ 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、教育を実施する</li> </ul>
AT-5		物理セキュリティ及び情報セキュリティの担当者が役割と責任を理解している。	CPS.AT-1	
DS-1		保存されているデータを保護している。	CPS.DS-1	<ul style="list-style-type: none"> <li>・ 情報(データ)を適切な強度の方式で暗号化して保管する</li> </ul>
DS-2		伝送中のデータを保護している。	CPS.DS-2 CPS.DS-3	<ul style="list-style-type: none"> <li>・ 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</li> <li>・ 情報(データ)を送受信する際に、情報(データ)そのものを暗号化して送受信する</li> </ul>

NIST Cybersecurity 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 (仮訳)	対策ID	対策要件
	DS-3	資産について撤去、譲渡、廃棄プロセスを正式に管理している。	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データ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を保持している。	CPS.DS-5 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、サービス活動を停止しないよう、モノ、システムに十分なリソース(処理能力、通信帯域、ストレージ容量)を確保する ・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保護対策を実施している。	CPS.DS-7 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 ・自組織の保護すべきデータが不適切なエンティティに渡ったことを検知した場合、ファイル閲覧停止等の適切な対応を実施する
	DS-6	ソフトウェア、ファームウェア及び情報の完全性の検証に、完全性チェックメカニズムを使用している。	CPS.DS-9 CPS.DS-10	・IoT機器、サーバ等の起動時に、起動するソフトウェアの完全性を検証し、不正なソフトウェアの起動を防止する ・送受信・保管する情報(データ)に完全性チェックメカニズムを使用する
	DS-7	開発・テスト環境を実稼働環境から分離している。	CPS.AC-7	・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	ハードウェアの完全性を検証するために整合性チェックメカニズムが使用されている。	CPS.DS-11	・ハードウェアの完全性を検証するために整合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設定を定め、維持している。	CPS.IP-1 CPS.IP-2	・IoT機器を設置する前にデフォルトの初期設定値を確認する ・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
	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を導入している。	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し、定めた各段階におけるセキュリティに関わる要求事項を明確化する
	IP-3	設定変更管理プロセスを導入している。	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を定期的を実施、保持し、テストしている。	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、テストしている
	IP-5	自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を満たしている。	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
	IP-6	ポリシーに従ってデータを破壊している。	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データ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	保護プロセスを継続的に改善している。	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している
	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している。	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	対応計画(インシデント対応及び事業継続)と復旧計画(インシデントからの復旧及び災害復旧)を実施し、管理している。	CPS.RP-1 CPS.RP-2	・対応が必要なセキュリティインシデント発生時の対応の内容や優先順位、対策範囲を明確にするため、セキュリティ運用プロセスを定め、運用する ・不適切なセキュリティインシデント(例：アクセス元/先が不正なエンティティである、送受信情報が許容範囲外である)を検知した後のIoT機器、サーバ等による振る舞いをあらかじめ定義し、実装する ・セキュリティ運用マニュアルにおいて、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をテストしている。	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する
	IP-11	人事に関わる対策にサイバーセキュリティ(例：アクセス権限の無効化、従業員に対する審査)を含めている。	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サイバーセキュリティ(例：アクセス権限の無効化、従業員に対する審査)を含めている
	IP-12	脆弱性管理計画を作成し、実施している。	CPS.IP-10	・脆弱性管理計画を作成し、計画に沿って構成要素の脆弱性を修正する

NIST Cybersecurity 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 (仮訳)	対策ID	対策要件
	MA-1	自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、タイムリーに実施しログを記録している。	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で適切に実施する方法を検討し、適用する ・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	自組織の資産に対する遠隔保守は、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は、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している
	PT-1	ポリシーに従って監査記録/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、レビューしている。	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、レビューしている
	PT-2	ポリシーに従って取り外し可能な外部記録媒体を保護し、そうした媒体の使用を制限している。	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に閉塞する
	PT-3	最小機能の原則を取り入れて、システムと資産に対するアクセスを制御している。	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に閉塞する
	PT-4	通信ネットワークと制御ネットワークを保護している。	CPS.AC-7	・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	正常及び不利な状況で回復力の要件を達成するためのメカニズム(フェイルセーフ、負荷分散、ホットスワップなど)が実装されている。	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、ユーザとシステム間の予測されるデータの流れを特定し、管理している。	CPS.AE-1
AE-2		攻撃の標的と手法を理解するために、検知したイベントを分析している。	CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対策組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティインシデントを検知・分析・対応する体制を整える
AE-3		イベントデータを複数の情報源やセンサーから収集し、相互に関連付けている。	CPS.AE-3	・セキュリティインシデントの相関の分析、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を特定している。	CPS.AE-4	・関係する他組織への影響を含めてセキュリティインシデントがもたらす影響を特定している
AE-5		インシデント警告の閾値を定めている。	CPS.AE-5	・セキュリティインシデントの危険度の判定基準を定める
CM-1		発生する可能性のあるサイバーセキュリティイベントを検知できるよう、ネットワークをモニタリングしている。	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・アクセス監視を実施する
CM-2		発生する可能性のあるサイバーセキュリティイベントを検知できるよう、物理環境をモニタリングしている。	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		発生する可能性のあるサイバーセキュリティイベントを検知できるよう、個人の活動をモニタリングしている。	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)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する
CM-4		悪質なコードを検出できる。	CPS.CM-3 CPS.CM-4	・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(データ)が許容範囲内であることを動作前に検証する
CM-5		不正なモバイルコードを検出できる。	CPS.CM-3 CPS.CM-4	・IoT機器、サーバ等において、送受信する情報(データ)の完全性および真正性を動作前に確認する
CM-6		発生する可能性のあるサイバーセキュリティイベントを検知できるよう、外部サービスプロバイダの活動をモニタリングしている。	CPS.CM-5	・発生する可能性のあるセキュリティインシデントを検知できるよう、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		権限のない従業員、接続、デバイス、ソフトウェアのモニタリングを実施している。	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)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する
CM-8		脆弱性スキャンを実施している。	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		説明責任を果たせるよう、検知に関する役割と責任を明確に定義している。	CPS.DP-1	・セキュリティインシデントの説明責任を果たせるよう、セキュリティインシデント検知における自組織とサービスプロバイダーが担う役割と負う責任を明確にする

NIST Cybersecurity 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 (仮訳)	対策ID	対策要件
	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、セキュリティインシデントを検知する
	DP-3	検知プロセスをテストしている。	CPS.DP-3	・監視業務として、セキュリティインシデント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	イベント検知情報を適切な関係者に伝達している。	CPS.RP-1	・対応が必要なセキュリティインシデント発生時の対応の内容や優先順位、対策範囲を明確にするため、セキュリティ運用プロセスを定め、運用する ・不適切なセキュリティインシデント(例：アクセス元/先が不正なエンティティである、送受信情報が許容範囲外である)を検知した後のIoT機器、サーバ等による振る舞いをあらかじめ定義し、実装する
	DP-5	検知プロセスを継続的に改善している。	CPS.DP-4	・セキュリティインシデントの検知プロセスを継続的に改善する
	対応 (RS)	RP-1	イベントの発生中または発生後に対応計画を実施している。	CPS.RP-1
CO-1		対応が必要になった時の自身の役割と行動の順番を従業員は認識している。	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する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する
CO-2		定められた基準に沿って、イベントを報告している。	CPS.RP-1	・対応が必要なセキュリティインシデント発生時の対応の内容や優先順位、対策範囲を明確にするため、セキュリティ運用プロセスを定め、運用する
CO-3		対応計画に従って情報を共有している。	CPS.RP-1	・不適切なセキュリティインシデント(例：アクセス元/先が不正なエンティティである、送受信情報が許容範囲外である)を検知した後のIoT機器、サーバ等による振る舞いをあらかじめ定義し、実装する
CO-4		対応計画に従って、利害関係者との間で調整を行っている。	CPS.RP-2	・セキュリティ運用マニュアルにおいて、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深めるために、外部利害関係者との間で任意の情報共有を行っている。	CPS.RP-2	
AN-1		検知システムからの通知を調査している。	CPS.AE-3	・セキュリティインシデントの関連の分析、及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する
AN-2		インシデントがもたらす影響を把握している。	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、組織全体への影響を把握する
AN-3		フォレンジックを実施している。	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
AN-4		対応計画に従ってインシデントを分離している。	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		組織に開示された脆弱性情報を社内外の情報源(例えば、内部テスト、セキュリティ速報、セキュリティ研究者)から受け取り、分析し、対応するためのプロセスが確立されている。	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
IM-1		学んだ教訓を対応計画に取り入れている。	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		対応戦略を更新している。	CPS.IM-1	
MI-1		インシデントを封じ込めている。	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		インシデントを提言している。	CPS.MI-1	

NIST Cybersecurity 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 (仮訳)	対策ID	対策要件
復旧 (RC)	MI-3	新たに特定された脆弱性に関して、許容できるリスクである場合にはその旨を文書化し、そうでない場合には低減している。	CPS.RA-4 CPS.RA-6	<ul style="list-style-type: none"> <li>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、定期的にはリスクアセスメントを実施する</li> <li>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</li> <li>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</li> <li>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</li> </ul>
	RP-1	イベントの発生中または発生後に復旧計画を実施している。	CPS.RP-3	<ul style="list-style-type: none"> <li>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コンティンジェンシープランの中にセキュリティインシデントを位置づける</li> </ul>
	IM-1	学んだ教訓を復旧計画に取り入れている。	CPS.IM-2	<ul style="list-style-type: none"> <li>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、事業継続計画又はコンティンジェンシープランを継続的に改善する</li> </ul>
	IM-2	復旧戦略を更新している。	CPS.IM-2	
	CO-1	広報活動を管理している。	CPS.CO-1	<ul style="list-style-type: none"> <li>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</li> </ul>
	CO-2	インシデント発生後に評判を回復している。	CPS.CO-2	<ul style="list-style-type: none"> <li>事業継続計画又はコンティンジェンシープランの中に、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</li> </ul>
	CO-3	復旧活動について内外の利害関係者及び役員、経営陣に伝達している。	CPS.CO-3	<ul style="list-style-type: none"> <li>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、事業継続計画又はコンティンジェンシープランの中に位置づける</li> </ul>

## 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			サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリー	管理策ID	要求事項	対策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。	CPS.AC-9	・IoT機器やユーザーを、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)に見合う形で認証する	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>組織は、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。</li> <li>組織は、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。</li> <li>組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 <ul style="list-style-type: none"> <li>-パスワード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、従わせる。</li> <li>-新しいパスワード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。</li> <li>-暗号によって保護されたパスワードのみを保存・伝送する。</li> <li>-パスワードの有効期間を組織が設定する。</li> <li>-同じパスワード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。</li> </ul> </li> <li>組織は、永続的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、一時的なパスワードを使用することを許可する。</li> <li>組織は、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。</li> <li>組織は、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。</li> </ul>
	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。	CPS.AC-9	・IoT機器やユーザーを、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)に見合う形で認証する	Middle	<ul style="list-style-type: none"> <li>組織は、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とする。</li> <li>組織は、機密性の高いデータを取り扱う自組織の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。</li> <li>組織は、情報伝達が許可される範囲やシステム間における情報伝達が許可される範囲を定めた情報フロー制御ポリシーを定め、情報フローの制御を実施する。</li> <li>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。</li> <li>組織は、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。</li> <li>組織は、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。</li> </ul>
	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。	CPS.AC-7	・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	High	<ul style="list-style-type: none"> <li>組織は、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とする。</li> <li>組織は、機密性の高いデータを取り扱う自組織の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。</li> <li>組織は、情報伝達が許可される範囲やシステム間における情報伝達が許可される範囲を定めた情報フロー制御ポリシーを定め、情報フローの制御を実施する。</li> <li>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。</li> <li>組織は、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。</li> <li>組織は、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。</li> </ul>
			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データの流れを特定し、管理するポリシーを確立し、実施する	High	
	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。	CPS.AC-5	・ユーザーが利用する機能と、システム管理者が利用する機能を分離する	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>組織は、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。</li> <li>組織は、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。</li> <li>組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 <ul style="list-style-type: none"> <li>-パスワード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、従わせる。</li> <li>-新しいパスワード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。</li> <li>-暗号によって保護されたパスワードのみを保存・伝送する。</li> <li>-パスワードの有効期間を組織が設定する。</li> <li>-同じパスワード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。</li> </ul> </li> <li>組織は、永続的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、一時的なパスワードを使用することを許可する。</li> <li>組織は、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。</li> <li>組織は、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。</li> </ul>
	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。	CPS.AC-5	・ユーザーが利用する機能と、システム管理者が利用する機能を分離する	Middle	<ul style="list-style-type: none"> <li>組織は、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とする。</li> <li>組織は、機密性の高いデータを取り扱う自組織の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。</li> <li>組織は、情報伝達が許可される範囲やシステム間における情報伝達が許可される範囲を定めた情報フロー制御ポリシーを定め、情報フローの制御を実施する。</li> <li>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。</li> <li>組織は、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。</li> <li>組織は、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。</li> </ul>
	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。	CPS.AC-5	・ユーザーが利用する機能と、システム管理者が利用する機能を分離する	High	<ul style="list-style-type: none"> <li>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。</li> <li>組織は、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。</li> <li>組織は、特権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している。</li> <li>組織は、非特権ユーザによって変更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機能の実行を禁止する。</li> </ul>
	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。	CPS.AC-5	・ユーザーが利用する機能と、システム管理者が利用する機能を分離する	High	<ul style="list-style-type: none"> <li>組織は、非特権ユーザによって変更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機能の実行を禁止する。</li> </ul>
				・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	High	<ul style="list-style-type: none"> <li>組織は、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。</li> </ul>

NIST SP 800-171		サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例
	3.1.8	ログイン試行失敗を制限する。	CPS.AC-4	・不正ログインを防ぐ 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	Middle ・組織は、自組織のシステムに対してユーザが連続してログインを失敗できる上限を設定し、上限以上失敗した場合には一定期間再ログインできない機能を実装する。
	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。	CPS.AC-9	・IoT機器やユーザーを、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)に見合う形で認証する	Middle ・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。 ・組織は、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。
	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、ボタンによる不可視化表示を用いてセッションロックを使用する。	CPS.AC-9	・IoT機器やユーザーを、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)に見合う形で認証する	Middle ・組織は、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。 ・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 -パスワード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、従わせる。 -新しいパスワード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。
	3.1.11	定義された条件の後、利用者セッションを(自動的に)終了する。	CPS.AC-9	・IoT機器やユーザーを、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)に見合う形で認証する	High ・組織は、自組織のシステムについて、個人の身元の確認のためのクレデンシャル等を用いた認証をする。 ・組織は、自組織のシステムについて、公開鍵基盤による認証を行う。 ・組織は、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。
	3.1.12	リモートアクセスセッションを監視し、制御する。	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	High ・組織は、自組織のシステムに関するリモートアクセスについて、自動監視または自動制御を実施する。 ・組織は、リモートアクセスセッションの機密性を完全性ととも保護するため、自組織が利用するシステムに暗号メカニズムを導入・管理する。
	3.1.13	リモートアクセスセッ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。	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	High ・組織は、必要がある場合には自組織が利用するシステムにおけるすべてのリモートアクセスが制御ポイントの管理を実施する。 ・組織は、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。 ・組織は、組織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。
	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。	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	High ・組織は、自組織の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。 ・組織は、情報の機密性を情報の完全性ととも保護するために、機器全体の暗号化等を実施する。
	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。	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	High ・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。
	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。	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	Low ・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、自組織の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。 ・組織は、自組織のシステムに関するリモートアクセスについて、自動監視または自動制御を実施する。
	3.1.17	認証と暗号化を用いて無線アクセスを保護する。	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	High ・組織は、リモートアクセスセッションの機密性を完全性ととも保護するため、自組織が利用するシステムに暗号メカニズムを導入・管理する。 ・組織は、必要がある場合には自組織が利用するシステムにおけるすべてのリモートアクセスが制御ポイントの管理を実施する。 ・組織は、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。 ・組織は、組織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。 ・組織は、自組織の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。 ・組織は、情報の機密性を情報の完全性ととも保護するために、機器全体の暗号化等を実施する。
	3.1.18	モバイルデバイスのコネクションを制御する。	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	Middle ・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との接続に関する承認ルール等を定める。
	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。	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	High ・組織は、自組織のシステムに関するリモートアクセスについて、自動監視または自動制御を実施する。 ・組織は、リモートアクセスセッションの機密性を完全性ととも保護するため、自組織が利用するシステムに暗号メカニズムを導入・管理する。 ・組織は、必要がある場合には自組織が利用するシステムにおけるすべてのリモートアクセスが制御ポイントの管理を実施する。 ・組織は、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。 ・組織は、組織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。 ・組織は、自組織の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。 ・組織は、情報の機密性を情報の完全性ととも保護するために、機器全体の暗号化等を実施する。 ・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。
	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。	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、保管する	Middle ・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

NIST SP 800-171			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	対策ID	対策要件	対策例
	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。	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、保管する	Middle 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は伝送すること ・外部のシステム上での自組織のポータブルストレージの使用を制限する。
	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。	CPS.GV-3	・各種法令や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	共通 ・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。	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発生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、教育を実施する	Middle ・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、情報セキュリティ要員の育成とレベル向上のため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。
	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。	CPS.AT-2	・自組織の構成員および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する	Low ・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、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。
	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。	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発生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、教育を実施する	Middle ・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、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。
					High ・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。	CPS.SC-5	・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	Middle ・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、手作業ないしはシステムにより自動で生成された監査記録を定期的にレビュー・分析して、契約事項からの逸脱および、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、レビューしている	Low ・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。
	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。	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、レビューしている	Low ・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さう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。
	3.3.3	監査された事象をレビューし、アップデートする。	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、レビューしている	Low ・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。
	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。	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、レビューしている	Middle ・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、情報システムが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、組織が監査ログの管理権限を付与する。 ・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。	CPS.SC-5	・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	High ・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・対応のためのプロセスをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先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。
				High ・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セスをシステムが提供する。	

NIST SP 800-171		サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例
	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。	CPS.AN-2	・セキュリティ事象発生後に、デジタルフォレンジックを実施する	<p>Middle</p> <ul style="list-style-type: none"> <li>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</li> <li>組織は、重要なセキュリティインシデントについて、発生後に下記の証拠を保全することが望ましい。 <ul style="list-style-type: none"> <li>- 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)</li> <li>- 証拠を収集・処理したヒトの役職、名前、連絡先</li> <li>- 証拠保全処理の日時(タイムゾーンを含む)</li> </ul> </li> </ul> <p>Low</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
	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。	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、レビューしている	<p>High</p> <ul style="list-style-type: none"> <li>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拠として、(論理的・物理的を問わず)管理される。</li> <li>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。</li> <li>組織は、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。</li> <li>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。</li> </ul>
	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。	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、レビューしている	<p>Middle</p> <ul style="list-style-type: none"> <li>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、情報システムが暗号メカニズムを実装する。</li> <li>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、組織が監査ログの管理権限を付与する。</li> <li>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。</li> </ul>
	3.3.9	監査機能の管理を特権利用者の一部に制限する。	CPS.PT-1	・危険性の高いセキュリティ事象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、レビューしている	<p>Middle</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
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。	CPS.AM-1	・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する	<p>Middle</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>ポータブルストレージデバイスに識別可能な所有者がないとき、このようなデバイスの使用を禁止する。</li> <li>GUI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。</li> </ul>
			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データの流れを特定し、管理するプロシージャを確立し、実施する	<p>Low</p> <ul style="list-style-type: none"> <li>組織は、システムのネットワーク構成、資産、機器の設定情報、構成情報等のベースラインとなる情報を文書化し、内容が適切かどうかを定期的に確認する。</li> </ul>
			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)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する	<p>Middle</p> <ul style="list-style-type: none"> <li>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。</li> <li>組織は、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</li> <li>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</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
			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)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する	<p>Low</p> <ul style="list-style-type: none"> <li>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。</li> <li>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、バッチの適用、ログのチェック等)、IoT機器の状況を定期的に確認する。</li> </ul>
	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。	CPS.AM-1	・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する	<p>High</p> <ul style="list-style-type: none"> <li>組織は、自組織の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、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。</li> <li>組織は、認可されていない資産を自動的に検出するメカニズムを導入、運用している。</li> </ul> <p>[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 ver.2.1」(IPA, 2018年)P30~P34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分析ガイド」(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</p>
			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	<p>Low</p> <ul style="list-style-type: none"> <li>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。</li> <li>IoT機器を設置する前にデフォルトの初期設定値を確認する</li> <li>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</li> </ul>

NIST SP 800-171			サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例	
	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。	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	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
			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)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>組織は、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</li> <li>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</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
	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。	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	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
	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。	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	Middle	<ul style="list-style-type: none"> <li>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。</li> </ul>
	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。	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に閉塞する	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>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</li> </ul>
	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。	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に閉塞する	High	<ul style="list-style-type: none"> <li>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。</li> <li>「ブラックリスト」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。</li> <li>ブラックリストの一覧を定期的にレビューし、更新する。</li> <li>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。</li> </ul>
	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。	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	High	<ul style="list-style-type: none"> <li>組織は、自組織の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とともに、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。</li> </ul>
			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に閉塞する	High	<ul style="list-style-type: none"> <li>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。</li> <li>「ブラックリスト」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。</li> <li>ブラックリストの一覧を定期的にレビューし、更新する。</li> <li>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。</li> </ul>
	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。	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	Middle	<ul style="list-style-type: none"> <li>組織は、自組織のシステム上でのユーザー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、モニタリングを実施する。</li> </ul>
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。	CPS.AC-6	・特権を持つユーザーのシステムへのログインに対して、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	Low	<ul style="list-style-type: none"> <li>組織は、自組織の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、一意に識別する認証を実施する。</li> </ul>
			CPS.AC-9	・IoT機器やユーザーを、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)に見合う形で認証する	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>組織は、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。</li> <li>組織は、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。</li> <li>組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 <ul style="list-style-type: none"> <li>パスワード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、従わせる。</li> <li>新しいパスワード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。</li> <li>暗号によって保護されたパスワードのみを保存・伝送する。</li> <li>パスワードの有効期間を組織が設定する。</li> <li>同じパスワード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。</li> <li>永続的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、一時的なパスワードを使用することを許可する。</li> </ul> </li> <li>組織は、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。</li> <li>組織は、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。</li> </ul>
	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。	CPS.AC-9	・IoT機器やユーザーを、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)に見合う形で認証する	Middle	<ul style="list-style-type: none"> <li>組織は、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。</li> </ul>
	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。	CPS.AC-6	・特権を持つユーザーのシステムへのログインに対して、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	Middle	<ul style="list-style-type: none"> <li>組織は、自組織のシステムについて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。</li> </ul>

NIST SP 800-171			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	対策ID	対策要件	対策例
	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。	CPS.AC-6	・特権を持つユーザーのシステムへのログインに対して、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	High ・組織は、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。 ・組織は、自組織の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。
	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。	CPS.AC-8	・IoT機器、サーバ等がサイバー空間で得られた分析結果を受信する際、及びIoT機器、サーバ等が生成した情報(データを)サイバー空間へ送信する際、双方がそれぞれ接続相手のID(識別子)を利用して、接続相手を識別し、認証する ・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する	共通 ・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、識別子を管理する。 ・組織は、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斉に識別し、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。	CPS.AC-8	・IoT機器、サーバ等がサイバー空間で得られた分析結果を受信する際、及びIoT機器、サーバ等が生成した情報(データを)サイバー空間へ送信する際、双方がそれぞれ接続相手のID(識別子)を利用して、接続相手を識別し、認証する ・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する	共通
	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。	CPS.AC-9	・IoT機器やユーザーを、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)に見合う形で認証する	Middle ・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。
	3.5.8	規定された生成回数間、パスワードの再利用を禁止する。	CPS.AC-9	・IoT機器やユーザーを、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)に見合う形で認証する	Middle ・組織は、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。 ・組織は、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。 ・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 -パスワード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、従わせる。 -新しいパスワード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パスワードのみを保存・伝送する。 -パスワードの有効期間を組織が設定する。 -同じパスワード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。 -永続的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、一時的なパスワードを使用することを許可する。
	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。	CPS.AC-9	・IoT機器やユーザーを、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)に見合う形で認証する	Middle ・組織は、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。
	3.5.10	暗号的に保護されたパスワードのみを格納及び送信する。	CPS.AC-9	・IoT機器やユーザーを、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)に見合う形で認証する	Middle
	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。	CPS.AC-9	・IoT機器やユーザーを、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)に見合う形で認証する	Middle
インシデント対応			CPS.SC-8	・応答および復旧の計画とテストは、サプライヤと第三者プロバイダの間で行われる	High ・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關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關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。 Middle ・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。

NIST SP 800-171		サイバー・フィジカル・セキュリティ対策フレームワーク				
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例	
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。	CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対策組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティインシデントを検知・分析・対応する体制を整える	Middle	<ul style="list-style-type: none"> <li>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。 <ul style="list-style-type: none"> <li>- モニタリングするシステムの範囲をどこまでとするか</li> <li>- 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)</li> </ul> </li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。報告内容には下記を含むことが望ましい。 <ul style="list-style-type: none"> <li>- 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）</li> <li>- モニタリングにおける今後の改善方針</li> </ul> </li> </ul> <p>[参考]セキュリティ対策組織(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。</p>
			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している	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
			CPS.RP-1	<ul style="list-style-type: none"> <li>・対応が必要なセキュリティインシデント発生時の対応の内容や優先順位、対策範囲を明確にするため、セキュリティ運用プロセスを定め、運用する</li> <li>・不適切なセキュリティインシデント(例：アクセス元/先が不正なエンティティである、送受信情報が許容範囲外である)を検知した後のIoT機器、サーバ等による振る舞いをあらかじめ定義し、実装する</li> </ul>	Low	<ul style="list-style-type: none"> <li>組織は、対処が必要と判断された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。 <ul style="list-style-type: none"> <li>- 緊急時の指揮命令と対応の優先順位の決定</li> <li>- インシデントへの対応（インシデントレスポンス）</li> <li>- インシデントの影響と被害の分析</li> <li>- 情報収集と自社に必要な情報の選別</li> <li>- 社内関係者への連絡と周知</li> <li>- 外部関係機関との連絡</li> </ul> </li> </ul> <p>[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。</p>
			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、事業継続計画又はコンテンツエンジニアリングプランの中に位置づける	High Middle	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
			CPS.AN-1	・セキュリティ事象の全容と、推測される攻撃者の意図から、組織全体への影響を把握する	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
			CPS.AN-3	・検知されたセキュリティ事象の情報は、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	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> <p>"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。</p> <ul style="list-style-type: none"> <li>- インシデントの現在の状況</li> <li>- インシデントの概要</li> <li>- 当該インシデントに対して自組織の行った行動の内容</li> <li>- 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</li> <li>- 調査の際に収集した証拠の一覧</li> <li>- インシデントの処理担当者からのコメント</li> <li>- 次にとるべきステップ</li> </ul>
			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	Middle Low	<ul style="list-style-type: none"> <li>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。</li> </ul> <p>[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。</p>
			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陥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	High Middle	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>

NIST SP 800-171			サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例	
	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。	CPS.IM-1	・セキュリティ事象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	Middle Low	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。 <ul style="list-style-type: none"> <li>- 正確に何がいつ起きたか。</li> <li>- 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。</li> <li>- すぐに必要になった情報は何か。</li> <li>- 復旧を妨げたかもしれないステップや行動があったか。</li> <li>- 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。</li> <li>- 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。</li> <li>- 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が必要となるか。</li> </ul> </li> </ul>
			CPS.IM-2	・セキュリティ事象への対応から教訓を導き出し、事業継続計画又はコンティンジェンシープランを継続的に改善する	共通	<ul style="list-style-type: none"> <li>・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セス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。</li> <li>・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。</li> </ul>
	3.6.3	組織のインシデント対応能力をテストする。	CPS.SC-8	・応答および復旧の計画とテストは、サプライヤと第三者プロバイダとの間で行われる	High  Middle	<ul style="list-style-type: none"> <li>・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セスを整備する。</li> <li>・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。</li> </ul> <p>[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。</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・組織は、自組織と外部サービスプロバイダ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。</li> </ul>
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。	CPS.MA-1	<ul style="list-style-type: none"> <li>・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で適切に実施する方法を検討し、適用する</li> <li>・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</li> </ul>	High	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>
					Middle	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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行う場合には、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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>
				<ul style="list-style-type: none"> <li>・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で適切に実施する方法を検討し、適</li> </ul>	High	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>

NIST SP 800-171			サイバー・フィジカル・セキュリティ対策フレームワーク		
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例
	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。	CPS.MA-1	<ul style="list-style-type: none"> <li>使用する</li> <li>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</li> </ul>	<p>High</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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行う場合には、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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul> <p>Middle</p> <ul style="list-style-type: none"> <li>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行う場合には、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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
	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についてサンタイズされることを保証する。	CPS.IP-6	<ul style="list-style-type: none"> <li>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データ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</li> </ul>	<p>High</p> <ul style="list-style-type: none"> <li>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。</li> </ul> <p>Middle</p> <ul style="list-style-type: none"> <li>組織は、自組織のIoT機器やサーバ等を廃棄するプロセスを定め、そのプロセス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にし、適切に実施できたことを確認する。</li> </ul> <p>Low</p> <ul style="list-style-type: none"> <li>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にする。</li> </ul>
	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。	CPS.MA-1	<ul style="list-style-type: none"> <li>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が必要なタイミングで適切に実施する方法を検討し、適用する</li> <li>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</li> </ul>	<p>High</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul> <p>Middle</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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行う場合には、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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
	3.7.5	外部のネットワークコネク션을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ようなセッションを終了する	CPS.MA-2	<ul style="list-style-type: none"> <li>自組織のIoT機器、サーバ等に対する遠隔保守は、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している</li> </ul>	<p>Middle</p> <ul style="list-style-type: none"> <li>組織は、実施した遠隔保守の実施記録を保管する。</li> </ul> <p>Low</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
	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。	CPS.MA-1	<ul style="list-style-type: none"> <li>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が必要なタイミングで適切に実施する方法を検討し、適用する</li> <li>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</li> </ul>	<p>Low</p> <ul style="list-style-type: none"> <li>組織は、メンテナンス要員が付属しないシステムで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。</li> <li>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。</li> </ul>
メディア処理	3.8.1	紙及びデジタルの両方の、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)。	CPS.PT-2	<ul style="list-style-type: none"> <li>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に閉塞する</li> </ul>	<p>Low</p> <ul style="list-style-type: none"> <li>使用するUSBメモリ等の周辺機器は、管理台帳を作成し、保管場所を施設して管理する。</li> <li>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。</li> <li>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。</li> </ul>
	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。	CPS.AC-8	<ul style="list-style-type: none"> <li>IoT機器、サーバ等がサイバー空間で得られた分析結果を受信する際、及びIoT機器、サーバ等が生成した情報(データを)サイバー空間へ送信する際、双方がそれぞれ接続相手のID(識別子)を利用して、接続相手を識別し、認証する</li> <li>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</li> </ul>	<p>共通</p> <ul style="list-style-type: none"> <li>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、識別子を管理する。</li> <li>組織は、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。</li> <li>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。</li> </ul>

NIST SP 800-171		サイバー・フィジカル・セキュリティ対策フレームワーク				
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例	
人的セ キュリ	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ンタイズまたは破壊する。	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データ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	High Middle Low	<ul style="list-style-type: none"> <li>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。</li> <li>組織は、自組織のIoT機器やサーバ等を廃棄するプロセスを定め、そのプロセス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に、適切に実施できたことを確認する。</li> <li>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にする。</li> </ul>
	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。	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に閉塞する	Low	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
	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。	CPS.AM-1	・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する	Middle Low	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>ポータブルストレージデバイスに識別可能な所有者がないとき、このようなデバイスの使用を禁止する。</li> <li>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。</li> <li>組織は、自組織の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。</li> <li>組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づける。</li> <li>IoT機器に初期設定されていたID・パスワードは導入時に変更する。</li> <li>IoT機器の設定画面の認証を有効・無効に設定できる場合は、必ず有効にする。</li> <li>組織は、資産目録を定期的にレビューし、更新する。</li> </ul>
	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。	CPS.DS-1	・情報(データ)を適切な強度の方式で暗号化して保管する	High	<ul style="list-style-type: none"> <li>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。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。</li> <li>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、識別コード及び本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。【政府機関の情報セキュリティ対策のための統一基準(抜粋)平成19年6月14日 情報セキュリティ政策会議決定】</li> <li>組織は、情報システム内で使用されている暗号技術向けの暗号鍵を生成・配布・保管・アクセス・破壊するにあたり組織が定めた要求事項に従って作成・管理する。</li> <li>組織は、ユーザが暗号鍵を紛失した場合に、情報の可用性を維持する。</li> <li>情報システムは、保存されている情報の機密性と完全性を保護する。</li> <li>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。</li> </ul>
	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。	CPS.AM-1	・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する	Middle Low	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>ポータブルストレージデバイスに識別可能な所有者がないとき、このようなデバイスの使用を禁止する。</li> <li>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。</li> <li>組織は、自組織の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。</li> <li>組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づける。</li> <li>IoT機器に初期設定されていたID・パスワードは導入時に変更する。</li> <li>IoT機器の設定画面の認証を有効・無効に設定できる場合は、必ず有効にする。</li> <li>組織は、資産目録を定期的にレビューし、更新する。</li> </ul>
	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ないとき、このようなデバイスの使用を禁止する。	CPS.AM-1	・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する	Middle Low	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>ポータブルストレージデバイスに識別可能な所有者がないとき、このようなデバイスの使用を禁止する。</li> <li>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。</li> <li>組織は、自組織の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。</li> <li>組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づける。</li> <li>IoT機器に初期設定されていたID・パスワードは導入時に変更する。</li> <li>IoT機器の設定画面の認証を有効・無効に設定できる場合は、必ず有効にする。</li> <li>組織は、資産目録を定期的にレビューし、更新する。</li> </ul>
	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。	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、テストしている	Middle Low	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>組織は、自組織の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。</li> </ul>
					High	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>

NIST SP 800-171			サイバー・フィジカル・セキュリティ対策フレームワーク		
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例
サイバー 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。	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サイバーセキュリティ（例：アクセス権限の無効化、従業員に対する審査）を含めている	Low <ul style="list-style-type: none"> <li>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。</li> <li>組織は、要員の退職時に以下を実施する。 <ul style="list-style-type: none"> <li>-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。</li> <li>-職員に関連する認証及びクレデンシャルを無効にする。</li> <li>-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。</li> <li>-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。</li> </ul> </li> </ul>
	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。	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サイバーセキュリティ（例：アクセス権限の無効化、従業員に対する審査）を含めている	High <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> Middle <ul style="list-style-type: none"> <li>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室管理等に関するアクセス権限の変更を実施する。</li> </ul> Low <ul style="list-style-type: none"> <li>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。</li> <li>組織は、要員の退職時に以下を実施する。 <ul style="list-style-type: none"> <li>-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。</li> <li>-職員に関連する認証及びクレデンシャルを無効にする。</li> <li>-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。</li> <li>-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。</li> </ul> </li> </ul>
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。	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	Low <ul style="list-style-type: none"> <li>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。</li> <li>組織は、自組織の施設内の一般の人がアクセスできるエリアを定め、必要に応じてアクセス制御を実施する。</li> <li>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来客について、付き添う等して来客の行動を監視する。</li> </ul>
	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。	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	Middle <ul style="list-style-type: none"> <li>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。</li> <li>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来客のアクセス記録を、一定期間保管するとともに定期的にレビューを実施する。</li> </ul>
	3.10.3	訪問者をエスコートし、訪問者の活動を監視する。	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	Low <ul style="list-style-type: none"> <li>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。</li> <li>組織は、自組織の施設内の一般の人がアクセスできるエリアを定め、必要に応じてアクセス制御を実施する。</li> <li>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来客について、付き添う等して来客の行動を監視する。</li> </ul>
	3.10.4	物理的アクセスの監査ログを維持する。	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	Middle <ul style="list-style-type: none"> <li>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来客のアクセス記録を、一定期間保管するとともに定期的にレビューを実施する。</li> </ul>
					Middle <ul style="list-style-type: none"> <li>施設内の、一般の人がアクセスできる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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
	3.10.5	物理的アクセスデバイスを制御し、管理する。	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	Middle <ul style="list-style-type: none"> <li>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。</li> <li>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来客のアクセス記録を、一定期間保管するとともに定期的にレビューを実施する。</li> </ul>
Middle <ul style="list-style-type: none"> <li>施設内の、一般の人がアクセスできる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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>					
3.10.4	物理的アクセスの監査ログを維持する。	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	Middle <ul style="list-style-type: none"> <li>施設内の、一般の人がアクセスできる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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>	
				Low <ul style="list-style-type: none"> <li>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。</li> </ul>	

NIST SP 800-171			サイバー・フィジカル・セキュリティ対策フレームワーク		
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例
	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。	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	Low ・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。 ・組織は、自組織のシステムに関するリモートアクセスについて、自動監視または自動制御を実施する。 ・組織は、リモートアクセスセッションの機密性を完全性ととも保護するため、自組織が利用するシステムに暗号メカニズムを導入・管理する。
					High ・組織は、必要がある場合には自組織が利用するシステムにおけるすべてのリモートアクセスが制御ポイントの管理を実施する。 ・組織は、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。 ・組織は、組織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。 ・組織は、自組織の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。 ・組織は、情報の機密性を情報の完全性ととも保護するために、機器全体の暗号化等を実施する。 ・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あセスメントする。	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	Middle ・組織は、システム、または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。 【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。	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	High ・組織は、スキャンすべきシステムの脆弱性をすぐに更新できる脆弱性スキャンツールを使用する。 ・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。
					Middle ・組織は、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( <a href="https://jvn.jp/">https://jvn.jp/</a> )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： <a href="https://www.ipa.go.jp/security/vuln/CVSS.html">https://www.ipa.go.jp/security/vuln/CVSS.html</a> )を参考とすることが可能である。
					Low ・組織は、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実施する
3.11.3	リスクのアセスメントに従い、脆弱性を修正する。	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	Middle ・組織は、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( <a href="https://jvn.jp/">https://jvn.jp/</a> )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： <a href="https://www.ipa.go.jp/security/vuln/CVSS.html">https://www.ipa.go.jp/security/vuln/CVSS.html</a> )を参考とすることが可能である。	
Low ・組織は、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あセスメントする。	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している	Middle ・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、セキュリティ表裏k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

NIST SP 800-171			サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例	
3.12	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。	CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対策組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティインシデントを検知・分析・対応する体制を整える	Low	<ul style="list-style-type: none"> <li>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な評価(セキュリティ評価)を実施し、管理責任者へ報告する。</li> <li>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。</li> </ul>
					Middle	<ul style="list-style-type: none"> <li>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。 <ul style="list-style-type: none"> <li>- モニタリングするシステムの範囲をどこまでとするか</li> <li>- 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)</li> </ul> </li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。報告内容には下記を含むことが望ましい。 <ul style="list-style-type: none"> <li>- 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)</li> <li>- モニタリングにおける今後の改善方針</li> </ul> </li> </ul> <p>[参考]セキュリティ対策組織(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。</p>
	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。	CPS.AE-3	・セキュリティインシデントの相関の分析、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	Middle	<ul style="list-style-type: none"> <li>「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)では、主に下記のような機器のログを監視し、リアルタイムに分析を行うよう記載されている。多種多様なログの取り扱いが必要になるため、ログを正規化し、同一のデータベースに格納したり、SIEMを利用したりして、効率的な分析を実現する必要がある。取得可能な場合はネットワークフローの情報も扱うことが望ましい。</li> <li>- ファイアウォールなどのネットワーク装置からのログやネットワークフロー</li> <li>- IPS/IDSなどのセキュリティ装置からのログ</li> <li>- Web サーバなどのアクセスログ</li> <li>- ActiveDirectoryやDNSなどの各種システムからのログ</li> <li>- ユーザ利用端末に関するログ</li> </ul>
					共通	<ul style="list-style-type: none"> <li>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。</li> <li>組織は、取引先(サービスプロバイダ)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インシデントを記録した監査ログの存在を確認する。</li> <li>組織は、サービスプロバイダにより取得される監査ログが、サービスの利用者の活動、例外処理及びセキュリティインシデントを記録できており、適切な方式で保護されていることを確認する。</li> </ul>
					共通	<ul style="list-style-type: none"> <li>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。</li> <li>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、セキュリティインシデントを検知する。</li> <li>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であるかを定期的にレビューし、確認する。</li> </ul>
	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。	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、保管する	High	<ul style="list-style-type: none"> <li>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、リアルタイムで一覧を管理している。</li> <li>組織は、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。</li> <li>組織は、外部プロバイダによる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。</li> </ul>
					Middle	<ul style="list-style-type: none"> <li>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。 <ol style="list-style-type: none"> <li>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</li> <li>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</li> </ol> </li> <li>外部のシステム上での自組織のポータルストレージの使用を制限する。</li> </ul>
	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。	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	Middle	<ul style="list-style-type: none"> <li>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保管する。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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送する。</li> <li>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、外部事業者を確認する。</li> </ul>
					Low	<ul style="list-style-type: none"> <li>組織は、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おいて通信をモニタリングし、制御する。</li> </ul>
	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。	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・アクセス監視を実施する	Low	<ul style="list-style-type: none"> <li>組織は、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おいて通信をモニタリングし、制御する。</li> </ul>

NIST SP 800-171		サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例
	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。	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 導入し、定めた各段階におけるセキュリティに関する要求 事項を明確化する	Low ・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、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。	CPS.AC-5	・ユーザーが利用する機能と、システム管理者が利用する 機能を分離する	Middle ・組織は、自組織のシステムについて、ユーザの利用する機能と、システムの管理面で利用する機能を分離する。 ・組織は、自組織のシステムにおいて職務分離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。 ・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。	CPS.DS-8	・自組織の保護すべきデータが不適切なエンティティに 渡ったことを検知した場合、ファイル閲覧停止等の適切な 対応を実施する	High ・組織は、自組織の保護すべきデータが不適切なエンティティに渡らないように、自動化されたメカニズムを利用して検知を実施する。 ・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。	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・アクセス監視を実施する	Low ・組織は、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おいて通信をモニタリングし、制御する。
	3.13.6	デフォルトでネットワーク通信トラフィックを拒否し、また 例外によってネットワーク通信トラフィックを許可する(即 ち、すべて拒否、例外で許可)。	CPS.AC-7	・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	High ・組織は、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とする。 ・組織は、機密性の高いデータを取り扱う自組織の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。
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・アクセス監視を実施する	Middle ・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。 ・組織は、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	
	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。	CPS.AC-7	・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	High ・組織は、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とする。 ・組織は、機密性の高いデータを取り扱う自組織の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。	CPS.DS-1	・情報(データ)を適切な強度の方式で暗号化して保管する	High ・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。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、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。 【政府機関の情報セキュリティ対策のための統一基準(抜粋) 平成19年6月14日 情報セキュリティ政策会議決定】 ・組織は、情報システム内で使用されている暗号技術向けの暗号鍵を鍵を生成・配布・保管・アクセス・破壊するに当たり組織が定めた 要求事項に従って作成・管理する。 ・組織は、ユーザが暗号鍵を紛失した場合に、情報の可用性を維持する。 ・情報システムは、保存されている情報の機密性と完全性を保護する。 ・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。
	3.13.9	セッ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、通信セッ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。	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 よび他の組織、ヒト、モノ、システムとのデータの送受信 状況について、継続的に把握する	Middle ・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。 ・組織は、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。 ・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。 ・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.DS-1	・情報(データ)を適切な強度の方式で暗号化して保管する	Low ・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。 ・組織は、情報システム内で使用されている暗号技術向けの暗号鍵を鍵を生成・配布・保管・アクセス・破壊するに当たり組織が定めた 要求事項に従って作成・管理する。

NIST SP 800-171			サイバー・フィジカル・セキュリティ対策フレームワーク		
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例
システム と通信の 保護	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。	CPS.DS-4	・送受信データ、保管データ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。	<p>Middle</p> <ul style="list-style-type: none"> <li>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。</li> <li>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)</li> <li>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</li> <li>秘密鍵の危殆化の原因を調べることで、及び、原因の解消を図ること</li> <li>当該鍵を利用するサービスの利用停止</li> <li>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</li> <li>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)</li> </ul> <p>[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 Rev4等を参照することが望ましい。</p> <p>Low</p> <ul style="list-style-type: none"> <li>組織は、全ての暗号鍵を、変更及び紛失から保護することが望ましい。</li> </ul>
	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。	CPS.DS-1	・情報(データ)を適切な強度の方式で暗号化して保管する	<p>High</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。【政府機関の情報セキュリティ対策のための統一基準(抜粋) 平成19年6月14日 情報セキュリティ政策会議決定】</li> <li>組織は、情報システム内で使用されている暗号技術向けの暗号鍵を鍵を生成・配布・保管・アクセス・破壊するにあたり組織が定めた要求事項に従って作成・管理する。</li> <li>組織は、ユーザが暗号鍵を紛失した場合に、情報の可用性を維持する。</li> <li>情報システムは、保存されている情報の機密性と完全性を保護する。</li> <li>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。</li> </ul>
	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。	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	<p>High</p> <ul style="list-style-type: none"> <li>組織は、自組織のシステムに関するリモートアクセスについて、自動監視または自動制御を実施する。</li> <li>組織は、リモートアクセスセッションの機密性を完全性ととも保護するため、自組織が利用するシステムに暗号メカニズムを導入・管理する。</li> <li>組織は、必要がある場合には自組織が利用するシステムにおけるすべてのリモートアクセスが制御ポイントの管理を実施する。</li> <li>組織は、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。</li> <li>組織は、組織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。</li> <li>組織は、自組織の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。</li> <li>組織は、情報の機密性を情報の完全性ととも保護するために、機器全体の暗号化等を実施する。</li> <li>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。</li> </ul>
	3.13.13	モバイルコードの使用を管理し監視する。	CPS.CM-1	・組織内のネットワークと広域ネットワークの接続において、ネットワーク監視・アクセス監視を実施する	<p>High</p> <ul style="list-style-type: none"> <li>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</li> </ul>
	3.13.14	VoIP技術の使用を管理し、監視する。	CPS.CM-1	・組織内のネットワークと広域ネットワークの接続において、ネットワーク監視・アクセス監視を実施する	<p>High</p> <ul style="list-style-type: none"> <li>組織は、モバイルコードの使用を管理し、監視する。</li> <li>組織は、VoIPの使用を管理し、監視する。</li> </ul>
	3.13.15	通信セッションの真正性を保護する。	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	<p>High</p> <ul style="list-style-type: none"> <li>組織は、自組織のシステムに関するリモートアクセスについて、自動監視または自動制御を実施する。</li> <li>組織は、リモートアクセスセッションの機密性を完全性ととも保護するため、自組織が利用するシステムに暗号メカニズムを導入・管理する。</li> <li>組織は、必要がある場合には自組織が利用するシステムにおけるすべてのリモートアクセスが制御ポイントの管理を実施する。</li> <li>組織は、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。</li> <li>組織は、組織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。</li> <li>組織は、自組織の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。</li> <li>組織は、情報の機密性を情報の完全性ととも保護するために、機器全体の暗号化等を実施する。</li> <li>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。</li> </ul> <p>High</p> <ul style="list-style-type: none"> <li>情報システムは、情報の伝送中に、不正な情報の開示を防ぎ、情報に対する変更を検出するために、暗号メカニズムを導入し、通信経路を暗号化する。ただし、代替の物理面での対策によって保護されている場合を除く。</li> <li>情報システムは、システムの組織が定めたセキュリティ機能(少なくとも情報システムの認証および再認証を含む)とユーザとの間に信頼できる通信経路を確立する。</li> <li>組織は、情報システム内で使用されている暗号技術向けの暗号鍵を鍵を生成・配布・保管・アクセス・破壊するにあたり組織が定めた要求事項に従って作成・管理する。</li> <li>組織は、ユーザが暗号鍵を紛失した場合に、情報の可用性を維持する。</li> </ul>
				CPS.DS-2	・IoT機器、サーバ等の間、サイバー空間で通信が行われる

NIST SP 800-171			サイバー・フィジカル・セキュリティ対策フレームワーク		
ファミリー	管理策ID	要求事項	対策ID	対策要件	対策例
				際、通信経路を暗号化する	Middle <ul style="list-style-type: none"> <li>情報システムは、情報の伝送中に、不正な情報の開示を防ぎ、情報に対する変更を検出するために、暗号メカニズムを導入し、通信経路を暗号化する。ただし、代替の物理面での対策によって保護されている場合を除く。</li> <li>組織は、情報システム内で使用されている暗号技術向けの暗号鍵を生成・配布・保管・アクセス・破壊するにあたり組織が定めた要求事項に従って作成・管理する。</li> </ul>
					Low <ul style="list-style-type: none"> <li>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。</li> <li>組織は、情報システム内で使用されている暗号技術向けの暗号鍵を生成・配布・保管・アクセス・破壊するにあたり組織が定めた要求事項に従って作成・管理する。</li> </ul>
	3.13.16	保存されたCUIの機密性を保護する。	CPS.DS-1	・情報(データ)を適切な強度の方式で暗号化して保管する	Middle <ul style="list-style-type: none"> <li>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。</li> <li>組織は、情報システム内で使用されている暗号技術向けの暗号鍵を生成・配布・保管・アクセス・破壊するにあたり組織が定めた要求事項に従って作成・管理する。</li> <li>情報システムは、保存されている情報の機密性と完全性を保護する。</li> </ul>
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。	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データの流れを特定し、管理するプロセスを確立し、実施する	High <ul style="list-style-type: none"> <li>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。</li> <li>組織は、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。</li> <li>組織は、定期的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン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。</li> </ul>
	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。	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(データ)が許容範囲内であることを動作前に検証する	Middle <ul style="list-style-type: none"> <li>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。</li> </ul>
	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。	CPS.IP-10	・脆弱性管理計画を作成し、計画に沿って構成要素の脆弱性を修正する	Middle <ul style="list-style-type: none"> <li>組織は、修正内容の有効性及び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。</li> </ul>
			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(データ)が許容範囲内であることを動作前に検証する	Middle <ul style="list-style-type: none"> <li>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。</li> </ul>
	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。	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	High <ul style="list-style-type: none"> <li>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。</li> </ul>
			CPS.AE-3	・セキュリティインシデントの相関の分析、及び外部の脅威情報と比較した分析を行う手順を実施することで、セキュリティインシデントを正確に特定する	Middle <ul style="list-style-type: none"> <li>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をすることができる環境を整備する。</li> </ul>
			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(データ)が許容範囲内であることを動作前に検証する	High <ul style="list-style-type: none"> <li>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。</li> <li>組織は、自組織でIDS,IPS,SIEMと言ったセンサー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。</li> <li>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。</li> </ul>
	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。	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(データ)が許容範囲内であることを動作前に検証する	High <ul style="list-style-type: none"> <li>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。</li> <li>システムは、インプットとなるデータが指定されたフォーマットや内容に適合しているかどうかを確認することで、有効性をチェックする。</li> <li>システムは、IDS/IPSによる悪質コードの検知ログを自動的に更新する。</li> <li>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。</li> </ul>
			CPS.CM-4	IoT機器、サーバ等において、送受信する情報(データ)の完全性および真正性を動作前に確認する	High <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>システムは、通信セッションの真正性を保護する。</li> </ul>

NIST SP 800-171		サイバー・フィジカル・セキュリティ対策フレームワーク				
ファミリー	管理策ID	要求事項	対策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ックを含めて、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。	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データの流れを特定し、管理するプロセスを確立し、実施する	High	<ul style="list-style-type: none"> <li>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。</li> <li>組織は、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。</li> <li>組織は、定期的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン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。</li> </ul>
			CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対策組織(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	Middle	<ul style="list-style-type: none"> <li>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。 <ul style="list-style-type: none"> <li>- モニタリングするシステムの範囲をどこまでとするか</li> <li>- 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)</li> </ul> </li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。報告内容には下記を含むことが望ましい。 <ul style="list-style-type: none"> <li>- 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)</li> <li>- モニタリングにおける今後の改善方針</li> </ul> </li> </ul> <p>[参考]セキュリティ対策組織(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。</p>
			CPS.CM-5	・発生する可能性のあるセキュリティ事象を検知できるよう、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	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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によるサービス提供の変更を管理することが望ましい。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
			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)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>組織は、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</li> <li>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</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
			CPS.DP-4	・セキュリティインシデントの検知プロセスを継続的に改善する	Middle	<ul style="list-style-type: none"> <li>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セスを整備し、運用する。組織は、報告の場を最新の脅威や残存するリスクに対する脅威を認識し、セキュリティを向上するための場とすることが望ましい。</li> <li>例えば下記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。 ※下記のリストは、「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「5WIH」 v1.0」(ISOG-J, 2017年)より引用している。 <ul style="list-style-type: none"> <li>・ 攻撃の特徴 攻撃の特徴 <ul style="list-style-type: none"> <li>➢ 攻撃形態、関連する通信の内容</li> <li>➢ 核心となる攻撃コード</li> </ul> </li> <li>・ 攻撃によって残る痕跡 <ul style="list-style-type: none"> <li>➢ 被害を受けた後の通信内容</li> <li>➢ サーバやクライアントに残るログ</li> <li>➢ サーバやクライアントに残るその他特徴</li> </ul> </li> </ul> </li> <li>・ 各セキュリティ製品における検知名</li> </ul>

NIST SP 800-171		サイバー・フィジカル・セキュリティ対策フレームワーク				
ファミリー	管理策ID	要求事項	対策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。	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データの流れを特定し、管理するプロセスを確立し、実施する	High	<ul style="list-style-type: none"> <li>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。</li> <li>組織は、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。</li> <li>組織は、定期的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン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。</li> </ul>
			CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対策組織(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	Middle	<ul style="list-style-type: none"> <li>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。 <ul style="list-style-type: none"> <li>- モニタリングするシステムの範囲をどこまでとするか</li> <li>- 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)</li> </ul> </li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。報告内容には下記を含むことが望ましい。 <ul style="list-style-type: none"> <li>- 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）</li> <li>- モニタリングにおける今後の改善方針</li> </ul> </li> </ul> <p>[参考]セキュリティ対策組織(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。</p>
			CPS.CM-5	・発生する可能性のあるセキュリティ事象を検知できるよう、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	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>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は、自組織へ通知することを要求する。</li> <li>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によるサービス提供の変更を管理することが望ましい。</li> <li>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。</li> <li>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作偽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。</li> <li>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。</li> </ul>
			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)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する	Middle	<ul style="list-style-type: none"> <li>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。</li> <li>組織は、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</li> <li>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</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
			CPS.DP-4	・セキュリティインシデントの検知プロセスを継続的に改善する	Middle	<ul style="list-style-type: none"> <li>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セスを整備し、運用する。組織は、報告の場を最新の脅威や残存するリスクに対する脅威を認識し、セキュリティを向上するための場とすることが望ましい。</li> <li>例えば下記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。 ※下記のリストは、「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。 <ul style="list-style-type: none"> <li>・ 攻撃の特徴 攻撃の特徴 <ul style="list-style-type: none"> <li>➢ 攻撃形態、関連する通信の内容</li> <li>➢ 核心となる攻撃コード</li> </ul> </li> <li>・ 攻撃によって残る痕跡 <ul style="list-style-type: none"> <li>➢ 被害を受けた後の通信内容</li> <li>➢ サーバやクライアントに残るログ</li> <li>➢ サーバやクライアントに残るその他特徴</li> </ul> </li> </ul> </li> <li>各セキュリティ製品における検知名</li> </ul>