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	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。		
	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。		
	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インシデントを位置づける
	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。		
	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	・関係者のサイバーセキュリティリスクマネジメントの実施状況について確認する。また、自組織の事業に関する自組織および関係者の責任範囲を明確化し、セキュリティ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	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。		

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
	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	・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、その内容について関係者と合意する
	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	・自組織の事業を継続するに当たり重要な関係者を特定、優先付けをし、評価する ・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 ・サービスやシステムの運用において、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
	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	・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
	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	・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	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-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、関係者間で対応プロセスの整備と訓練を行う
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	・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を管理し、保護している。	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	リモートアクセスを管理している。	CPS.AC-3 CPS.AC-4	・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 ・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	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	・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 ・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
	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	・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
	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	・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
	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	・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 ・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
	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	・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
	AT-2	権限を持つユーザが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：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	・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
	AT-4	上級役員が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
	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。		
	DS-1	保存されているデータを保護している。	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

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
	DS-2	伝送中のデータを保護している。	CPS.DS-2 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 ・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
	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、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 ・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に実施、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	・セキュリティ事象への対応、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 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
	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、レビューする
	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。		
	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	・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
	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、相互に関連付いている。	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 ・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-5	不正なモバイルコードを検出できる。		
	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 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
	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	・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 ・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	・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 ・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-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
	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	・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 ・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-3	対応計画に従って情報を共有している。		
	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。		
	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。		
	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。		

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
	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	・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 ・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	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	・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
	IM-1	学んだ教訓を復旧計画に取り入れている。	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、事業継続計画又はコンティンジェンシープランを継続的に改善する
	IM-2	復旧戦略を更新している。		
	CO-1	広報活動を管理している。	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	インシデント発生後に評判を回復している。	CPS.CO-2	・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
	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	・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