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

	ISO/I	EC 27001:2013 附属書/	1		th-	イバー・フィミ	ジカル・セキュリティ対策フレームワーク
	管理策ID		要求事項	対策要件ID	対策要件		対策例
A.5 情報セキュリティのための 方針群	A.5.1 情報セキュリティのための 経営陣の方向性	A.5.1.1 情報セキュリティのための 方針群	情報セキュリティのための方針群は、これを定 義し、管理層が承認し、発行し、従業員及び関 連する外部関係者に通知しなければならない。	CPS.BE-2	・自組織の事業におけるミッション、目標、活動に関して優先順位を定め、セキュリティに関するポリシー・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	Advanced	 組織は、組織の業務、組織の資産、個人、他の組織等にもたらされるリスクを考慮して、自組織のミッション/業務プロセスを定義し、活動に関する優先限付けを確立する。 組織は、自組織のセキュリティボリシーにおいて規定されている自組織と関係する他組織のセキュリティに関する役割と責任について、関係する他組織に伝達する。
				CPS.GV-1	・セキュリティポリシーを策定し、自組織および関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする	Advanced	** 和願は、上は少刀前を欠えのセキュリフィ小リン―何かよりはいレベルととし、、例えは「此のよりなドモック側がの刀前および美趣中機を 塩定する。 a) アクセス制御および認証 b) 物理的セキュリティ対策 c) システムの開発および取扱い ・セキュリティボリシー前の策定に当たっては、自組織の a)事業戦略、b)関係する規制、法令および契約、c)セキュリティの脅威環境を十 がに考慮して、自組織の表別を十分に反映したものとなるよう策定を実施する。 ・組織は、自組織の a)事業戦略、b)関係する規制、法令および契約、c)セキュリティの脅威環境の変化に応じて、セキュリティ方針をレ ビュー、更新する。 [参考] より詳細なレベルの方針策定の際には、ISO/IEC 27002等の関連する標準を参照して方針が必要となる分野を把握したうえで、"中小 企業の情報セキュリティ対策ガイドライン ver.2.1"(IPA、2018年) 付銀3や"情報セキュリティボリシーサンブル改版(1.0版)"(INSA、2016年) 塩を金乗り信義セキュリティボリシー群の最も高いレベルに、セキュリティ基本方針を策定し、経営層の承認を得後、適切に適用す
		A.5.1.2	情報セキュリティのための方針群は、あらかじ			Basic	る。 ・組織は、自組織のセキュリティ方針を定期的(例えば、1年に1度)にレビュー、更新する。 「参考」セキュリティボリシーの策定に当たっては、「中小企業の情報セキュリティ対策ガイドライン」付録3における「情報セキュリティ基本方針」や、日本ネットワークセキュリティ協会(INSA)が公開する「情報セキュリティボリシーサンブル改版(1.0版)」における「01」情報セキュリティ基本方針」、「01、情報セキュリティ方針」等を参考とすることが可能である。 「PSRAペー学変形したパザーパー分析の結果に基づき、必要な場合、重要なパザードにつながりうるセキュリティに係るリスク源に対して通
			め定めた間隔で,又は重大な変化が発生した場合に,それが引き続き適切,妥当かつ有効であ			H.Advanced	切に対応する。 [参考] 特に安全制御系におけるセキュリティ面の統合については、近年国際標準化の場でも議論がなされており、IEC TR 63074, IEC TR 63069等を参照することが可能である。
			ることを確実にするためにレビューしなければならない。	CPS.RA-6	・リスクアセスメントに基づき、発生しうるセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する・loT機器およびloT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティおよび関連するセーフティのリスクに対して適宜対応する	Advanced Basic	・組織は、サネュリティリスタ対応のプロセスについての文章化した情報を安全に保管する。 ・組織は、サスタアセスメントの結果に応じて対応策を選定する際、実施する対応策および当該対応策を採用する理由を文書化することが望ましい。 ・組織は、対応策の適用等に関して、セキュリティリスク対応計画を策定し、リスク所有名の承認を得る。 ・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、リスク所有名の承認を得る。 ・組織は、セキュリティリスク対応計画をレビューし、当該計画が、自組職会体のリスクマネジメント戦略における優先順位に適合しているかどうかを確認する。 ・CPS.RA-4で抽出した、IoT機器を含む新しいシステムにおける必要なセキュリティ対策が実施されているかを受け入れ検査などで確認する。 ・組織は、IOT機器を含むシステムの導入時に、要求仕様や契約段階で定めたセキュリティ対策が実施されているかを受け入れ検査などで確認する。 ・組織は、次の事事を行うために、リスクアセズメントの結果を考慮して、対応策を選定する。 ・セキュリティメスタの受害について、リスク所を担ていて、リスクの管理について、リスタの管理について、リスタの管理について、リスクを持ちの必要が得る。
A.6 情報セキュリティのための 組織	A.6.1 内部組織	A.6.1.1 情報セキュリティの役割及 び責任	全ての情報セキュリティの責任を定め、割り当 てなければならない。			H.Advanced	・システムは、自組織が利用している外部情報サービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・システムは、利用を許可していない外部情報システムサービスを検知した場合、システム管理者へ通知するメカニズムを利用する。 ・組織は、外部プロバイダによるサービスを使用する際に必要な機能、ボート、プロトコル、および他のサービスを明確にする。 ・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。
				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	Advanced	a. 外部の情報システムから自組織の情報システムにアクセスすること b. 外部の情報システムを使用して自組織の管理下にある情報を処理または保存もしくは伝送すること ・外部のシステム上での自組織のボータブルストレーシの使用を制限する。 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
						Basic	る。 [参考] 特にクラウドサービス利用におけるユーザー側の役割と責任を、契約において規定する際のポイントについて、「クラウドセキュリ ティガイドライン 活用ガイドブック」(経済産業省、2013年) Appendix A 契約の具体的な内容例と解説 を参照することが可能である。
					・II ソーフ /向・レレ エノ ニ カ パラニバ ナ	Advanced	(本所が) ドンダン (株式産業場、603-47 内外回004 ステのシスキャラル 14 大学) (大学) (本学) (大学) (大学) (大学) (大学) (大学) (大学) (大学) (大
				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、関係者に伝達している	Basic	・組織は、サンドスのが場合に、分成の原的なじてもの力を対象的で使うしたのかしてユーラ るためりぬ手を含める。 ・関係する法規制等により、自組織のリソース(例:システム、データ)について特定の分類に従うことが要求されている場合、該当する分類を資産に適用する。 「参考]重要度の穿出方法には、「中小企業の情報セキュリティ対策ガイドライン」(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、「制御システムのセキュリティスク分析ガイド」(IPA, 2018年) P21に記載された事業被害の大きさにおける評価を用いる方法等がある。
						Advanced	 組織は、セキュリティインシデントにより損害が発生する場合に備えて、取引先等から指定されるセキュリティ対策の実装に加え、サイバー保険の利用等によるリスク移転を検討する。

ISO/IEC 27001:2013 附属書A			th.	イバー・フィシ	ガル・セキュリティ対策フレームワーク
管理策ID	要求事項	対策要件ID	対策要件		対策例
		CPS.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	Basic	・組織は、委託先あるいは委託元との契約において、業務においてセキュリティインシデントにより損害が発生した場合の自組織と取引先 の責任範囲(免責事項の明記、損害賠債額の契約金額等での上限設定等)を規定する。 ・組織は、契約において取引先に対応を求める/求められるセキュリティに関する要求事項の実効性を高めるため、要求事項への対応要否や 過不足、具体的な対応方法や費用負担、対応できない場合の代替措置について契約時あるいは契約期間の初めに合意することが望ましい。
				H.Advanced	・セキュリティに関わる研究会や会議等に出席したり、セキュリティの専門家による協会・団体との適切な連絡体制を維持することにより、セキュリティに関わる知識を最新のものとする。 ・主に自社が提供している製品・サービスにおいて、新たな能物性が含まれていないかを分析し、発見した場合、IPAに関連情報を届け出る。
		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	Advanced	・組織は、セキュリティ管理責任者を中心に、セキュリティが范围機を立ち上げ、組織内でセキュリティ対策を収ら体制を整える。 ・組織は、情報処理推進機構(PA)、JPCERT/CC、業界ISACのような組織や、取引関係のある機器ベンダー、ソフトウェアペンダーより、 結時熱感性情報、脅威情報等を収集し、自組織の資産目録と照らし合わせることで、対応要素を判断する。 「参考」セキュリティ対応組織の構想、構築、運用に当たっては、外部事業者からのサービスを利用するほかに、JPCERT/CCから公開されて いる「CSIRTマテリアル」、日本セキュリティオペレーション事業者協議のから公開されている「セキュリティ対応組織 (SOC/CSIRT) の 数料書 一機能、役割・人材スキル・成熟を、一等の実業や利用するほとが可能である。
				Basic	・租職は、セキュリティ管理責任者およびセキュリティ対策担当者を任命することで、租職内におけるセキュリティの役割と責任を明確化する。 は職は、利用中の機器ベンダーやソフトウェアベンダーが提供するセキュリティに関わる注意検起情報を確認し、自組織内の関係者に伝達する。
				H.Advanced	・組織は、セキュリティ専門の24時間365日モニタリングモニタリングにより収集した監査ログを、分析自動化ツール等を利用することで効率的に分析する。 ・組織は、従来のIT環境だけでなく、制御システムやIoT機器も含めて、セキュリティ状況のモニタリングの範囲とすることが望ましい。 ・組織は、従来のIT環境がはでなり、制御システムやIoT機器も含めて、セキュリティ状況のモニタリングやインシデントへの対応等のセキュリティ 関連集務を継続的に改善することが望ましい。 (参考)セキュリティ対策組織(SOC/CSIRT)を評価するためのメトリクスには、"セキュリティ対応組織成熟度セルフチェックシート"(ISOG-J. 2018年)や、SIM3(Security Incident Management Maturity Model)等がある。
			・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	Advanced	・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。 ・モニタリングするシステムの範囲をどこまでとするか ・どのような機器の口がを収集し、分析するが(CPSAE-3を参照) ・組織は、貴産情報、機器の構成情報、ネットワーク構成情報を経施的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、貴産情報、機器の構成情報、ネットワーク構成情報を経施的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、貴産情報、機器の構成情報、ネットワーク構成情報を経施的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、貴産情報、機器の構成情報、ネットワーク構成情報を経施的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、貴産情報、機器の構成情報、ネットワーク構成情報を経施的に収集・管理し、定期的に報告する。報告内容にはいい、対応を実施する。プロセスの内容については、CPSAP-1等を参照・ ・組織およびシステムのセキュリティ状態をセキュリティ管理責任者等の適切な変員に、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。 ・ログ分析の分析結果(対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等) ・モニタリングにおける今後の改善方針 ・参考1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)の教料書・機能・役割・人材スキル・成熟度 ~"(ISOG-J, 2018年)等を参照することが望ましい。
				Basic	・組織は、セキュリティ管理責任者/担当者を明確化し、社内・社外向けのセキュリティ関係の窓口とする。
		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	Basic	・組織は、リスクマネジメントに係る戦略やアセスメントの結果等から、セキュリティインシデントを検知するために収集することが望ましい口が開発を決定する。 い口が開発を決定する。 ・組織は、取引所(サービスプロバイダー)に対して、取得されるサービス利用者の活動、例外処理及びセキュリティインシデントを記録した 監査ログの存在を確認する。 ・組織は、サービスプロイイダーにより取得される監査ログが、サービスの利用者の活動、例外処理及びセキュリティインシデントを記録できており、適切ら方式で必要されていることを確認する。
職務の分離	相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離なければならない。	CPS.AC-5	・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	H.Advanced	 ・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・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。 ・システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入している。 ・システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。
				Advanced	・組織は、自組織のシステムにおいて職務分離(例:ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 ・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。
	関係当局との適切な連絡体制を維持しなければ ならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令 や、業界のガイドラインを考慮した社内ルールを策定 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	Basic	・自自国の事業活動において、セキュリティの文脈で関連するギベでの法令、規制及び契約上の要求事項、並びにこれらの要求事項を満た すための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。 ・要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文書化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全ての国における遵守を考慮する。 「参考」情報セキュリティ関連法令には例えば、不正競争防止法、電子署名認証法、e・文書法、個人情報保護法、不正アクセス禁止法等があ

	ISO/I	EC 27001:2013 附属書/	A		th-	イバー・フィシ	ジカル・セキュリティ対策フレームワーク
	管理策ID		要求事項	対策要件ID	対策要件		対策例
		A.6.1.4 専門組織との連絡	情報セキュリティに関する研究会又は会議,及び情報セキュリティの専門家による協会・団体 との適切な連絡体制を維持しなければならな		・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及	H.Advanced	・セキュリティに関わる研究会や会議等に出席したり、セキュリティの専門家による協会・団体との適切な連絡体制を維持することによ リ、セキュリティに関わる知識を最新のものとする。 ・主に自社が提供している製品・サービスにおいて、新たな脆弱性が含まれていないかを分析し、発見した場合、IPAに関連情報を届け出 る。
			U _a	CPS.RA-2	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	Advanced	・組織は、セキュリティ管理責任者を中心に、セキュリティ対応組織を立ち上げ、組織力でセキュリティ対策を収る体制を整える。 ・組織は、セキュリティを理性と機能(IPA)、IPCERI/CC、業界ISACのような組織や、取引関係のある機器ペンダー、ソフトウェアペンダーより、 随時施別性情報、脅威情報等を収集し、自組織の資産目録と照らし合わせることで、対応要高を判断する。 「参考]セキュリティ対応組織の構想、構築、運用に当たっては、外部事業者からのサービスを利用するほかに、JPCERI/CCから公開されて いる「CSIRTマテリアル」、日本セキュリティオペレーション事業者協議会から公開される「セキュリティ対応組織(SOC/CSIRT)の 数料書 〜機能・役割・人材スキル・成熟度・」等の文書を利用することが可能である。
				CPS.RA-3	・自組織の資産に対する脅威を特定し、文書化する	H.Advanced	 組織は、セキュリティに関わる研究会や会議等に出席したり、セキュリティの専門家による協会・団体との適切な連絡体制を維持することにより、セキュリティ脅威に関わる知識を最新のものとする。
				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	H.Advanced	・組織は、発生したセキュリティインシデントの形態、規模及び費用を定量化及び監視できるようにする自動的なメカニズムを備える。 ・組織は、セキュリティインシデント発生時において、マルウェアや双撃者が配置したプログラムやスクリプトが発見された場合、それらの 機能の解析を自能機のセキュリティ対応組織(SOC/CSIRT)にて実施する。 ・組織は、攻撃者のプロファイル(所属組織、組織の活動目的など)に関する仮設を構築する。 「卓利機数のシステムが連携する"System of Systems"が構築されている環境においては、セキュリティインシデントの影響評価により困難 なものになることが想定される。当該領域における先行的な試みである"Internet of Things(IoT)インシデントの影響評価に関する考察"(一般 社団法人日本クラウドセキュリティアライアンス、2016年)では、デバイスの特性、サービスの特性、デバイス数により影響度を評価する試 みがなされている。
						Advanced	・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティペンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、 共有することによって、当該セキュリティインシデントの全容を把握する。 ・セキュリティインシデント発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解 術を外部のセキュリティベンダー等に依頼する。
				CPS.AN-1	・セキュリティ事象の全容と、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	H.Advanced	・システムは、発生したセキュリティインシデントの形態、規模及び費用を定量化及び監視できるようにする自動的なメカニズムを備える。 ・組織は、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影響したプログラムやスクリプトが発見された場合、それらの 機能の解析を自組織のセキュリティ対応組織(SOC/CSIRT)にて実施する。 ・組織は、攻撃者のプロファイル(所属組織、組織の活動目的など)に関する仮説を構築する。 「参考地数のシステムが連携する「System of Systems"が構築されている環境においては、セキュリティインシデントの影響評価はより困難なものになることが想定される。当該領域における先行的な試みである"Internet of Things(IoT) インシデントの影響評価に関する考察"(一般社団法人日本クラウドセキュリティアライアンス、2016年)では、デバイスの特性、サービスの特性、デバイス数により影響度を評価する試みがなされている。
						Advanced	・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、 共有することによって、当該セキュリティインシデントの全容を把握する。 ・セキュリティインシデント発生時において、マルウェアや及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。
			プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティ に取り組まなければならない。	CPS.IP-3	・システムを管理するためのシステム開発ライフサイク ルを導入し、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	H.Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 ・セキュリティ機能に関する要求事項 ・セキュリティ機能に関する要求事項 ・セキュリティ保証に関する要求事項 ・セキュリティ保証に関する要求事項 ・セキュリティ関連のドキュメントに関する要求事項 ・セキュリティ関連のドキュメントの保護に関する要求事項 ・そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 ・受け入れ基準
						Advanced	・組織は、情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
	A.6.2 モバイル機器及びテレワー キング	A.6.2.1 モバイル機器の方針	モバイル機器を用いることによって生じるリス クを管理するために、方針及びその方針を支援 するセキュリティ対策を採用しなければならな い。	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する	Advanced	・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・組織は、自組織で利用する携帯機器から自組織のシステムの接続に関する承認ルール等を定める。
		A.6.2.2	テレワーキングの場所でアクセス、処理及び保			Advanced	・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・組織は、自組織で利用する携帯機器から自組織のシステムの接続に関する承認ルール等を定める。
		テレワーキング	存される情報を保護するために、方針及びその 方針を支援するセキュリティ対策を実施しなけ ればならない。	CPS.AC-3	・無線接続先(ユーザーやloT機器、サーバ等)を正しく認証する	Basic	・組織は、自組織(リバフ・ロット地域がプロール・アンスンとなるに関するようには、計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のに先立って、無線でシステムにアクセスする権限を与える。
A.7 人的資源のセキュリティ	A.7.1 雇用前	A.7.1.1 選考	全ての従業員候補者についての経歴などの確認 は、関連する法令、規制及び倫理に従って行わ なければならない。また、この確認は、事業上 の要求事項、アクセスされる情報の分類及び認 識されたリスクに応じて行わなければならな い。	CPS.AC-8	・IoT機器、サーバ等が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	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子 を無効にすることで、識別を管理する。 ・システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する 仕組みを構える。 ・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。
						H.Advanced	 組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。

	ISO	/IEC 27001:2013 附属書/	Α		th-	イバー・フィシ	ジカル・セキュリティ対策フレームワーク
	管理策ID		要求事項	対策要件ID	対策要件		対策例
				CPS.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	Advanced	 ・組織は、要員が自組織内で配置転換/異動になった場合に、要員の配置転換/異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、選用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。 ・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。
						Basic	・船間は、目他間ツンヘアルにかすのインセルをは切すの例に、乗員を審査する。 ・組間は、乗りの理論やに以下を集まする。 ・組間は、乗りの理論やに以下を集まする。 ・組員に関連する認証及びウレデンシャルを無効にする。 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
		A.7.1.2 雇用条件	従業員及び契約相手との雇用契約書には、情報 セキュリティに関する各自の責任及び組織の責			H.Advanced	 組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。
			任を記載しなければならない。		・人の異動に伴い生じる役割の変更に対応した対策にサ	Advanced	 ・組織は、要員が自組織内で配置転換/異動になった場合に、要員の配置転換/異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ・要員を指定する。
				CPS.IP-9	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	Basic	京開客加よう。 ・ 相関は、自見機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。 ・ 相関は、要員の退職時に以下を実施する。 ・ 相関は、要員の退職時に以下を支施する。 ・ 相関は、要員の退職時に以下を支施する。 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
	A.7.2	A.7.2.1	経営陣は、組織の確立された方針及び手順に			H.Advanced	・組織は、内部不正の兆候を認識・報告するためのセキュリティ意識向上トレーニングを、全要員に対して実施する。
	雇用期間中	経営陣の責任	従った情報セキュリティの適用を,全ての従業 員及び契約相手に要求しなければならない。	CPS.AT-1	・自組織の全ての要員に対して、セキュリティインシデントの発生と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	Advanced	 ・組職は、基本的なセキュリティ要議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役割別例:システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者)のプログラムを作成し、定期的に該当する要員に対して実施する。
					CALL CALLY STOWN SALE CALLY S	Basic	 組織は、自組機の利用するシステムに対する変更により必要になった場合や新規職員に対して基本的なセキュリティ意識向上トレーニングを実施する。
						H.Advanced	・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書者が必要な条件を定め、要員の再書金を実施する。・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。・組織は、要員の追職時で、情報セキュリティをトピックとした退職者面接を実施する。・組織は、要員が自組織内で起業を換く異動になった場合に、要員の促開転換/実動によりンステムや入退室管理等に関するアクセス権限
				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	Advanced	の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のパックアップ 要員を指定する。
			Gr 3.II - 3	員に対する審査)を含めている	Basic	・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。 ・組織は、要員の退職時に以下を実施する。 ・組織は、要員のと理論はに以下を実施する。 ・- ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
		A.7.2.2	組織の全ての従業員、及び関係する場合には契			H.Advanced	・組織は、内部不正の兆候を認識・報告するためのセキュリティ意識向上トレーニングを、全要員に対して実施する。
		情報セキュリティの意識向 上、教育及び訓練	情報セキュリティの意識向 約相手は、職務に関連する組織の方針及び手順	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	Advanced	 ・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。 ・組織は、情報セキュリティ要員の育成とレベル向上のための役割別例:システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者)のプログラムを作成し、定期的に該当する要員に対して実施する。
			従ってその更新を受けなければならない。		と責任を遂行するための適切な訓練、教育を実施する	Basic	 組織は、自組織の利用するシステムに対する変更により必要になった場合や新規職員に対して基本的なセキュリティ意識向上トレーニングを実施する。
	A.7.3	A.7.2.3 懲戒手続 A.7.3.1	情報セキュリティ違反を犯した従業員に対して 処置をとるための,正式かつ周知された懲戒手 続を備えなければならない。 雇用の終了又は変更の後もなお有効な情報セ	CPS IP-0	・人の異動に伴い生じる役割の変更に対応した対策にサ イパーセキュリティ(例:アクセス権限の無効化、従業	H.Advanced	 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。
	雇用の終了及び変更	雇用の終了又は変更に関す る責任		GI 3.II - 3	見に対する審査)を含めている	TI.Advanced	 ・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。
A.8 資産の管理	A.8.1 資産に対する責任	A.8.1.1 資産目録	情報及び情報処理施設に関連する資産を特定しなければならない。また、これらの資産の目録を、作成し、維持しなければならない。			H.Advanced	- 配職は、自組職のシステムを構成する資産(10T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、パージョン情報、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。 ・システムは、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、連用している。 [参考] 重要度の算出方法には、"中小企業の情報セキュリティ対策ガイドライン ver.2.1"(IPA、2018年)P.30~P.34に記載された情報の機密性、 完全性、同用性に関する評価を用いる方法や、"制御システムのセキュリティスク分析ガイド"(IPA、2018年)のP.21に記載された事業被害の大
				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	Advanced	きさにおける評価を用いる方法等がある - 資産の病成情報(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 - 品組は、システムコンポーネント上で利用可能な取り外し可能なメディア(例: USBメモリ)を一覧化し、使用を管理する。 - 組織は、ボータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 - 組織は、ボータブルストレージ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利用状況を適切に把握し、管理エリアの外部への持ち出し中のメディアの利用状況を適切に把握し、管理する。

ISO/I	EC 27001:2013 附属書	Α		th-	イバー・フィシ	ジカル・セキュリティ対策フレームワーク
管理策ID		要求事項	対策要件ID	対策要件		対策例
					Basic	・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。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 「参考」資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン」(IPA, 2018年)のP33を参照することが可能である。
	A.8.1.2 資産の管理責任 a)	目録の中で維持される資産は、管理されなければならない。 注a) 6.1.2及び 6.1.3 では、情報セキュリティのリスクを運用管理することについて、責任及び権限			H.Advanced	・組織は、自路機のシスケムを構成する質症(10機器等を含むパードウェア、ソフトウェア、情報)を一般に特定し、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、パージョン情報、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。 ・システムは、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。 歩考]重要度の弾出方法には、"中小企業の情報で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、"物理システムのセキュリティスク分析ガイド"(IPA、2018年)P30~P21に記載された博報の機密性、 まさによりな評価を用いる方法等がある。 ・資産の構成情報(例: 名称、パージョン情報、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
		をもつ人又は主体をリスク所有者としている。 情報セキュリティにおいて、多くの場合、資産 の管理責任を負う者は、リスク所有者でもあ る。	CPS.AM-1	・システムを構成するハードウェア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	Advanced	・資産の構成情報(例): 名称、パージョン情報、ライセンス情報、場所等)を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、システムコンボーネント上で利用可能な取り外し可能なメディア(例): USBメモリ)を一覧化し、使用を管理する。 ・組織は、ボータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの利用状況を適切に把握 し、管理する。
					Basic	・組織は、自組織の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、目録として一覧を支票化する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン」(IPA, 2018年)のP.33を参照することが可能である。
	A.8.1.3 資産利用の許容範囲	情報の利用の許容範囲、並びに情報及び情報処理無数と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施しなければならない。	CPS.AM-1	・システムを構成するハードウェア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	H.Advanced	・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)を一悪に特定し、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。 ・システムは、説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。 [参考] 重度反の輩出方法には、"中小企業の情報セキュリティ対策ガイドラインver2.1"(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スク分析ガイド"(IPA、2018年)のP21に記載された事業被害の大きにおける評価を用いる方法等がある ・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
					Advanced	る。 ・組織は、システムコンボーネント上で利用可能な取り外し可能なメディア(例: USBメモリ)を一覧化し、使用を管理する。 ・組織は、ボータブルストレージディイスに識別可能な所有者がいないとき、このようなディイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの利用状況を適切に把握し、管理する。
	A.8.1.4 資産の返却	全ての従業員及び外部の利用者は、雇用、契約 又は合意の終了時に、自らが所持する組織の資			H.Advanced	 組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。 ・組織は、要員の追組織内で起源転換、実動になった場合に、要員の配置を換/実動によりシステムや入送室管理等に関するアクセス権限
		産の全てを返却しなければならない。	CDC ID A	・人の異動に伴い生じる役割の変更に対応した対策にサ	Advanced	の変更を実施する。 ・要負が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ 要負を指定する。
				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	Basic	・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。 ・組織は、要員の過職時に以下を実施する。 ・自組織のシステムに対するアクセスを一定期間内に無効にする。 ・職員に関連する認定版グレデンシャルを無効にする。 ・セキュリティに関連するシステム関連の所有物をすべて回収する。 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
A.8.2 情報分類	A.8.2.1 情報の分類	情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに 慎重を要する度合いの観点から、分類しなけれ ばならない。	CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに 関する取決め等によって要求されるデータの保護の水準 を的確に把握し、それぞれの要求を踏まえたデータの区 分方法を整備し、ライフサイクル全体に渡って区分に応 じた適切なデータの保護を行う	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすた の組織の取組みを識別、支書化し、最新に保つ。 ・組織は、識別したルールの労気に従い、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実に従い、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: 割減販売法におけるカード情報 の非保持化)
	A.8.2.2 情報のラベル付け	情報のラベル付けに関する適切な一連の手順 は、組織が採用した情報分類体系に従って策定 し、実施しなければならない。			H.Advanced	 組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。
			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	Advanced	 組織は、システム、モノ等によって提供される機能とサービスをレビューし、削除の候補となる機能とサービスを特定する。 組織は、禁止されている機能、ボート、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 (ファイアウェール、ホストペースの侵入検知システム等)を活用する
					Basic	・使用するUSBメモリ等の周辺機器は、管理も様を作成し、保電場所を施能して管理する。 ・loT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メモリを用りる等の対策を行う。 ・使用しないUSBボート、シリアルポートは栓をするなど物理的に閉塞する。

	ISO/I	EC 27001:2013 附属書	4		th-	イバー・フィシ	プカル・セキュリティ対策フレームワーク	
	管理策ID		要求事項	対策要件ID	対策要件	対策例		
		A.8.2.3 資産の取扱い	資産の取扱いに関する手順は、組織が採用した 情報分類体系に従って策定し、実施しなければ ならない。	CPS.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	H.Advanced	〈High Advanced〉 ・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる 歳、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護するま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。 「参考」暗号技術検討合及び関連委員会(CRYPTREC)では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が 十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するものリストを「電子政府における調達のために参照すべき 暗号のリスト」(CRYPTREC暗号リスト)として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて 参照することが望ましい。	
						Advanced Basic	・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報(データ)を適切な強度の方式で暗号化して保管 する。CRYPTRCC銀号リスト電子政府推議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 な強度の方式で両者化して保管でる。 ・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報(データ)を適切な強度の方式で暗号化して保管	
				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	H.Advanced	する。 - ・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。	
	A.8.3	A.8.3.1	組織が採用した分類体系に従って, 取外し可能		・IoT機器、サーバ等の廃棄時には、内部に保存されてい	H.Advanced	・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。	
	媒体の取扱い	取外し可能な媒体の管理	な媒体の管理のための手順を実施しなければな	ODO ID C	るデータ及び、正規IoT機器、サーバ等を一意に識別する	Advanced	・組織は、自組織のIoT機器やサーバ等を廃棄するプロシージャを定め、そのプロシージャに従って内部に保存されている情報を削除又は読	
			らない。	CPS.IP-6	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	Basic	み取りできない状態し、適切に実施できたことを確認する。 - 相覷は、自相機のJoT機器やサーバ等をを廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態する。	
						H.Advanced	 ・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 	
				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	Advanced	・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。 ・組織は、システム、モン等によって提供される機能とサービスを レビューし、削除の候補となる機能とサービスを特定する。 ・組織は、禁止されている機能、ボート、プロトカル、サービスの使用を検加し防止するために、ネットワークスキャンツール、侵入検加 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	
		A.8.3.2	媒体が不要になった場合は、正式な手順を用い			Basic	・使用するUSBメモリ等の周辺機器は、管理台帳を作成し、保管場所を施錠して管理する。 10.17機器、サーバ等に接続するUSBメモリ等の外部返帰媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能な USBメモリを用いる等の対策を行う。 ・使用しないUSBボート、シリアルボートは栓をするなど物理的に閉塞する。 ・機能し、成果接換の10.17機器サール(等の)が最後定義し、その定義に従い必要な後	
		A.6.3.2 媒体の処分	無体が小安になった場合は、正式な子順を用いて、セキュリティを保って処分しなければならない。	CPS.IP-6	・loT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loT機器、サーバ等を一意に識別する	H.Advanced Advanced	HEIMINA、DIRACIONADIO INMENT A TO THIN INFO TO THE INFO THE	
			ar.	GI 3.II -0	データID(識別子)や重要情報(秘密鍵、電子証明書等)を削		み取りできない状態し、適切に実施できたことを確認する。	
					除又は読み取りできない状態にする	Basic	・組織は、自組織のIoT機器やサーバ等をを廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態する。	
		A.8.3.3 物理的媒体の輸送	情報を格納した媒体は、輸送の途中における、 認可されていないアクセス、不正使用又は破損 から保護しなければならない。			H.Advanced	・調達する機器に対して、契約におけるセキュリティ要求率項が満たせているかを、自組織あるいは第三者がテストする。 ・組織は、自組織のオペレーションにとって特に重要な機器について、再委託先以降の組織を含む関係するサプライチェーン全体に渡り、一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なブロシージャで製造されたものかを確認する。	
				CPS.SC-4	・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提供する製品・サービスが適合していることを確認する	Advanced	・組織は、契約において、例えば下記のように、取引先から調達する製品・サービスが具備すべきセキュリティ、要求事項を明確化する。 ・セキュリティに関わる特定の認定例:ISMS認証、ISASecure EDSA認証、ITセキュリティ評価及び認利度(ISEC))を有していること リスク分析の結果等から事かれた必要なセキュリティ要件を設計時からの実験(セキュリティ・デザイン)し、必能上でいること ・組織は、調達計画時に、製品またはサービス自体、あるいは当該製品・サービスの調達・供給にて使用される資産の保護に係るセキュリ ディ要件の費用を確保しておくことが望ましい。 ・下記を含む製品またはサービスの調達または供給を評価するためのセキュリティ測定ルールを策定し、運用および改善する。 ・測定対象の内容 ・指摘の報告方法、報告の規度 ・指摘の報告方法、報告の規度 ・組織は、搬送中の改ざん・漏えいを検知(又は抑止)する手段とともに納品されるIoT機器やソフトウェアが、不正操作されていないかを確認する。 ・物品:セキュリティ使、プロテクトシール等 ・微点:毎号化、電送データ全体のハッシュ信等	
A.9 アクセス制御	A.9.1 アクセス制御に対する業務 上の要求事項	A.9.1.1 アクセス制御方針	アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、 文書化し、 レビューしなければならない。			H.Advanced	・システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化および無効化について自動的に監査・ 報告する。	
				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 レ物証性組みな効 管理 確物 取当 医キオス	Advanced	・組織は、システムアカウントの利用状況をモニタリングする。・組織は、アカウントが不要になった場合や変更が必要となった場合には管理責任者に通知する。	

ISO/I	EC 27001:2013 附属書	1		y .	イバー・フィシ	ジカル・セキュリティ対策フレームワーク
管理策ID		要求事項	対策要件ID	対策要件		対策例
				この前に目前(*C プンバ)、 図・生、 V性部(*)、 □以(*)、 加、紅(*) ○	Basic	- 組織は、自組織のシステムのアカウントを管理する管理責任者を配置する。 - 組織は、自組織のミッションや業務機能を考慮して、必要なシステムアカウント種別(例: 一般ユーザ/ンステム管理者)を識別・選択する。 - 組織は、プロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 - 組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。
		利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを, 利用者に提供しなければならない。	CPS.AC-6	・特権を持つユーザーのシステムへのログインに対して、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	H.Advanced	・システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織のシステムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
					Advanced	・システムは、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要求する。
A.9.2 利用者アクセスの管理	A.9.2.1 利用者登録及び登録削除	アクセス権の割当てを可能にするために、利用 者の登録及び登録削除についての正式なプロセ スを実施しなければならない。		・承認されたモノとヒトおよびプロシージャの識別情報	H.Advanced	・組織は、自組織のシステムアカウントの管理について自動化されたメカニズムを導入し、運用している。 ・システムは、自組織のシステムの一時利用アカウントや緊急アカウント、用されていないアカウントについて、一定開間の経過後に自動的に無効にする。 ・システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化および無効化について自動的に監査・報告する。
			CPS.AC-1	と認証情報を発効、管理、確認、取消、監査する	Advanced	・組織は、システムアカウントの利用状況をモニタリングする。・組織は、アカウントが不要になった場合や変更が必要となった場合には管理責任者に通知する。
					Basic	・組織は、自組織のシステムのアカウントを管理する管理責任者を配置する。 ・組織は、組織のミッションや業務機能を考慮して、必要なシステムアカウント権別(例:一般ユーザ/システム管理者)を識別・選択する。 ・組織は、プロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。
			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	H.Advanced	・システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織のシステムについて、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、リアレイ攻撃に対する首性のある認定メカニズムを実施する。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
			01 3.40-0	用する	Advanced	・システムは、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要求する。
					Basic	・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。
			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 銃相手の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	Basic	 ・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 IoT機器での適信は、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。
	A.9.2.2 利用者アクセスの提供 (provisioning)	全ての種類の利用者について、全てのシステム 及びサービスへのアクセス権を割り当てる又は 無効化するために、利用者アクセスの提供につ いての正式なプロセスを実施しなければならな			H.Advanced	・組織は、自組織のシステムアカウントの管理について自動化されたメカニズムを導入し、運用している。 ・システムは、自組織のシステムの一時利用アカウントや緊急アカウント、用されていないアカウントについて、一定期間の経過後に自動的に無効にする。 ・システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化および無効化について自動的に監査・報告する。
		∪°	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	Advanced	・組織は、システムアカウントの利用状況をモニタリングする。・組織は、アカウントが不要になった場合や変更が必要となった場合には管理責任者に通知する。
				Carpine 17 TA C 2027 (m -ax -e-ax -e-ax -e-ax)	Basic	・組織は、自組織のシステムのアカウントを管理する管理責任者を配置する。 ・組織は、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別(例:一般ユーザ/システム管理者)を識別・選択する。 ・組織は、プロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。
	A.9.2.3 特権的アクセス権の管理	特権的アクセス権の割当て及び利用は、制限 し、管理しなければならない。	CPS.AC-5	・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	H.Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・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。 ・システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入している。 ・システムは、持特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権 ユーザによる特権的機能の実行を禁止する。
					Advanced	- 組織は、自組織のシステムにおいて職務の無例: ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 - 組織は、特定の職務権限に対して懸小権限の原則を採用する。 - 組織は、担当権によって割り当てられた職務を分離し、明文化する。
			CPS.AC-6	・特権を持つユーザーのシステムへのログインに対し て、二つ以上の認証機能を組み合わせた多要素認証を採	H.Advanced	- システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織のシステムについて、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、リアレイ攻撃に対する首性のある認証メカニズムを実施する。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。

ISO/	IEC 27001:2013 附属書	4		the state of the s	イバー・フィシ	プカル・セキュリティ対策フレームワーク
管理策ID		要求事項	対策要件ID	対策要件		対策例
				用する	Advanced	・システムは、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要求する。
	A.9.2.4 利用者の秘密認証情報の管理	秘密認証情報の割当ては、正式な管理プロセス によって管理しなければならない。	CPS.AC-1	・承認されたモノとヒトおよびプロシージャの識別情報 と認証情報を発効、管理、確認、取消、監査する	H.Advanced	・組織は、自組織のシステムアカウントの管理について自動化されたメカニズムを導入し、選用している。 ・システムは、自組織のシステムの一時利用アカウントや緊急アカウント、用されていないアカウントについて、一定期間の経過後に自動的 に無効にする。 ・システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化および無効化について自動的に監査・ 報告する。
					Advanced	・組織は、システムアカウントの利用状況をモニタリングする。 ・組織は、アカウントが不要にな-った場合や変更が必要となった場合には管理責任者に通知する。
	A.9.2.5 利用者アクセス権のレ ビュー	資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューしなければならない。	CPS.AC-1	・承認されたモノとヒトおよびプロシージャの識別情報 と認証情報を発効、管理、確認、取消、監査する	H.Advanced	・システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化および無効化について自動的に監査・ 観告する。
					Advanced	・組織は、システムアカウントの利用状況をモニタリングする。 ・組織は、アカウントが不要になった場合や変更が必要となった場合には管理責任者に通知する。 ・組織は、アカウントが不要になった場合や変更が必要となった場合には管理責任者に通知する。
	A.9.2.6 アクセス権の削除又は修正	全ての従業員及び外部の利用者の情報及び情報 処理施設に対するアクセス権は、雇用、契約又 は合意の終了時に削除しなければならず、ま た、変更に合わせて修正しなければならない。		・承認されたモノとヒトおよびプロシージャの識別情報	H.Advanced	・組織は、自組織のシステムアカウントの管理について自動化されたメカニズムを導入し、運用している。 ・システムは、自組織のシステムの一時利用アカウントや緊急アカウント、用されていないアカウントについて、一定期間の経過後に自動的に無効にする。 ・システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化および無効化について自動的に監査・報告する。
			CPS.AC-1	と認証情報を発効、管理、確認、取消、監査する	Advanced	・組織は、システムアカウントの利用状況をモニタリングする。・組織は、アカウントが不要にな-った場合や変更が必要となった場合には管理責任者に通知する。
					Basic	 ・組織は、自組織のシステムのアカウントを管理する管理責任者を配置する。 ・組織は、組織のミッションや業務機能を考慮して、必要なシステムアカウント権別(例:一般ユーザ/システム管理者)を識別・選択する。 ・組織は、プロシージャに役ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必要とする。
					H.Advanced	 ・組織は、自組織のloT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の施設に対する物理的な侵入について警報と監視装置(例)・監視カメラ)をモニタリングする。 ・組織は、自組織のの1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
			CPS.AC-2	・ IoT機器、サーバ等の設置エリアの施錠、入退室管理、 生体認証等の導入、監視カメラの設置、持ち物や体重検 査等の物理的セキュリティ対策を実施する	Advanced	態する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する来寄のアクセス記録を、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。
					Basic	・組織は、自組織のloT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設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。 ・組織は、自組織のloT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モニタリングする。
A.9.3 利用者の責任	A.9.3.1 秘密認証情報の利用	秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求しなければならない。			H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを 自動的に終了させる機能を実装する。
			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	Advanced	・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うメカニズムの強度を持った認証を 実施する。 ・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知 メッセージ等を表示する。 ・システムは、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、バ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。 ・バスワードに長低限必要な複雑をを確保するため、バスワードに来る要求事項を定め、運用する。 ・新しいバ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バスワードのみを保存・伝送する。 ・バスワード・ドロ有効期間を組織が変改する。 ・同じバ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。 ・強固なバスワードに下く定変更するのを条件に、ンステムへのログオン時に、一時的なバスワードを使用することを許可する。 ・システムは、自組織のシステムについて認証プロセス時に認定情報のフィードバックを見えないようにする。 ・システムは、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。
A.9.4 システム及びアプリケー ションのアクセス制御	A.9.4.1 情報へのアクセス制限	情報及びアプリケーションシステム機能へのア クセスは、アクセス制御方針に従って、制限し なければならない。	CPS.AC-5	・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	H.Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・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。 ・システムは、特権的機能の使用をチェックするため、システムが監査するメカニズと導入している。 ・システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権 ユーザによる特権的機能の実行を禁止する。

ISO/	IEC 27001:2013 附属書/	A	サイバー・フィジカル・セキュリティ対策フレームワーク				
管理策ID		要求事項	対策要件ID	対策要件		対策例	
					Advanced	・組織は、自組織のシステムにおいて職務分離(例:ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 ・組織は、担当者によって割り当てられた職務を分離し、明文化する。	
			CPS.AC-6	・特権を持つユーザーのシステムへのログインに対して、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	H.Advanced	・システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織のシステムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。	
					Advanced	・システムは、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要求する。	
	A.9.4.2 セキュリティに配慮したロ グオン手順	アクセス制御方針で求められている場合には、 システム及びアプリケーションへのアクセス は、セキュリティに配慮したログオン手順に	CPS.AC-4	・一定回数以上のログイン認証失敗によるロックアウト や、安全性が確保できるまで再ログインの間隔をあける	H.Advanced	・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。	
		よって制御しなければならない。		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	Advanced	・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一定期間再ログイン できない機能を実装する。	
	A.9.4.3 パスワード管理システム	パスワード管理システムは、対話式でなければ ならず、また、良質なパスワードを確実とする ものでなければならない。			H.Advanced	 システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 	
			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	Advanced	・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、ブ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。 ・システムは、ユーザが自組機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、ブ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。 ・システムは、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、バ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。 ・バ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。 ・新しいバ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。 ・細号によって保護されたバスワードのみを保守・伝送する。 ・バスワードの有効期間を組織が設定する。 ・同じバスワードを組織が変せる。 ・同じバスワードを組織が変ませたにシステムへのログオン時に、一時的なバスワードを使用することを許可する。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・システムは、自組織のシステムについて、ユーザによる認証後に一受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。	
	A.9.4.4 特権的なユーティリティブ ログラムの使用	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。	CPS.AC-5	・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	H.Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・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。 ・システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入している。 ・システムは、非特権コーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権 ユーザによる特権的機能の実行を禁止する。 ・組織は、自組織のシステムにおいて職務分離(例:ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、自組織のシステムにおいて職務分離(例:ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。	
					navancca	・組織は、担当者によって割り当てられた職務を分離し、明文化する。	
			CPS.AC-6	・特権を持つユーザーのシステムへのログインに対し 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	H.Advanced	・システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織のシステムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。	
					Advanced	・システムは、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要求する。	
	A.9.4.5 プログラムソースコードへ のアクセス制御	プログラムソースコードへのアクセスは、制限しなければならない。			H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを 自動的に終了させる機能を実装する。	

	ISO/II	EC 27001:2013 附属書/			th-	イバー・フィミ	ジカル・セキュリティ対策フレームワーク
	管理策ID		要求事項	対策要件ID	対策要件		対策例
				CPS.AC-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	Advanced	・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うメカニズムの強度を持った認証を 実施する。 ・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知 メッセージ等を表示する。 ・システムは、設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、バスワードによび基金を存り場合には、以下のことを満たすこととする。 ・バスワードに最低限必要な複雑さを確保するため、バスワードに求める要求事項を定め、運用する。 ・が、レバ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。 ・細句によって保護されたパスワードのみを存存・伝送する。 ・バ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。 ・週間がパスワードを組織が定数するかを条件に、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。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。
A.10 暗号	A.10.1 暗号による管理策	A.10.1.1 暗号による管理策の利用方 針	情報を保護するための暗号による管理策の利用 に関する方針は、策定し、実施しなければなら ない。	CPS.DS-2	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する	H.Advanced Advanced	・組織は、重要なデータを扱う通信路について、通信経路の暗号化を実装するか、あるいは、代替の物理面での対策によって保護する。 ・システムは、暗号メカニズムを導入し、通信経路を暗号化する。 「参考】通信経路の暗号化には、IP-VPNL, Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を開することが関生しい。
				CPS.DS-3	・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	H.Advanced Advanced	マーバーサモニ地で、ハルスを起とす。こことの選集といっ、 ・ンステムルの日報書は、少ないリアースでも可用性を損なわずに実装可能な暗号モジュールを導入し、重要度の高い機器からの遺伝データ を適切を強度で暗号化することが望ましい。 ・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、情報(データ) を暗号化して送受信する。
		A.10.1.2 鍵管理	暗号鍵の利用、保護及び有効期間(lifetime)に 関する方針を策定し、そのライフサイクル全体 にわたって実施しなければならない。			H.Advanced	・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。 ・秘密鍵及びプライベート鍵をセキュリティを保って管理することに加え、公開鍵の真正性についても考慮することが望ましい。この認証プロセスは、認証局によって通常発行される公開鍵証明書を用いて実施される。この認証局は、要求された信頼度を提供するために適切な管理策及び手順を備えている、認知された組織であることが望ましい。
				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。	Advanced	・組織は、秘密鍵が危殆化した際に選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。 ・ 級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) ・ 級密鍵が危殆化した。またはその恐れがあると判断するための基準 ・ 秘密鍵が危殆化した。またはその恐れがあると判断するとの基準 ・ 秘密鍵の危殆化の原因を調べること、及び、原因の解消を図ること ・ 当該鍵を利用するサービスの利用停止 ・ 新しい鍵ペアを生成し、新しい鍵に対する延明書を発行すること ・ 秘密鍵の危殆化についての情報の間示(通知先、通知の方法、公表の方針等) [参考] 鍵管理に関するより詳細な内容については、ISO/IEC 11770規格群や、NIST SP 800-57 Part 1 Rev 4等を参照することが望ましい。
				CPS.DS-7	・保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用したIoT機器、サーバ等を選定する	Basic H.Advanced	 組織は、全ての暗号鍵を、改変及び粉失から保護することが望ましい。 ・組織は、保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用した機器を調達する。 :組織は、情報システム内で使用されている暗号技術向けの暗号鍵を保管するにあたり耐タンパーデバイスを用いて管理する。
A.11 物理的及び環境的セキュリ ティ	A.11.1 セキュリティを保つべき領 域	A.11.1.1 物理的セキュリティ境界	取扱いに慎重を要する又は重要な情報及び情報 処理施設のある領域を保護するために、物理的 セキュリティ境界を定め、かつ、用いなければ ならない。	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、 生体認証等の導入、監視カメラの設置、持ち物や体重検	H.Advanced	- 組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 - 組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 - 組織は、自組織の施設に対する物理的な侵入について警報と監視装置(例: 監視カメラ)をモニタリングする。 - 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
					査等の物理的セキュリティ対策を実施する	Advanced	施する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリア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。
				CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的ア クセスの設定および記録、監視を実施する	H.Advanced Advanced Basic	・組織は、特に重要な資産を管理している範囲内での重要資産の位置や移動を認能し、モニタリングする。 ・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。 ・組織は、個人の物理的なアクセスを許可する前に、当該業員のアクセス権限を確認し、入退室管理分を保持する。 ・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを限持する。 ・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその光度が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア(執務室等)において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に接出し、対応できるようにする。 ・自組織のオレーションにとって重要技が高に生まえられる18世級、サーバ等のセンであるが、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。 ・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寄うなどして人手による代替的な対策を実施する。

ISO/IEC 27001:2013	対属書A		у -	イバー・フィシ	ジカル・セキュリティ対策フレームワーク
管理策ID	要求事項	対策要件ID	対策要件		対策例
A.11.1.2 物理的入退管理策	セキュリティを保つべき領域は、認可された者 だけにアクセスを許すことを確実にするため に、適切な入退管理策によって保護しなければ			H.Advanced	・組織は、自組織のJoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出功装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の施設に対する物理的な侵入について警報と監視装置(例:監視カメラ)をモニタリングする。 ・組織は、自組織の店舗と、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
	ならない。	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、 生体認証等の導入、監視カメラの設置、持ち物や体重検	Advanced	・船橋は、自船線の101機器、サーハ等が改置されているエリアに対する制理ドクセスをモニタリンクし、定期的に監査ログのレビューを実施する。 ・組織は、自組線の101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。
			査等の物理的セキュリティ対策を実施する	Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアを定め、必要に応じてアクセス制御を実施する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する来客について、付き添う等して来客の行動をモニタリングする。
			・IoT 機器、サーバ等のセキュリティ上重要なアップデー	H.Advanced	・組織は、自組織のIoT機械、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、 モニタリングを実施する。 ・組織は、自組織のIoT機械、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な 変更または不正な変更がないか確認する。 ・組織は、自組織のIoT機械、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認 した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アブリケーション)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1oT機能を導入する。
		CPS.MA-1	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	Advanced	・船線は、自船線の101機器、サーバ等のアップテ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、体認、又書化する。 ・組織は、自組線の101機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組線の101機器、サーバ等のアップデート等のメンテナンスを自組線の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に矢立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組線の101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デェックして、正しく機能しているかどうかを確認する。 ・組織は、自組線の101機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、自組線の101機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス製造がファナンスを成立している行う場合は、アナンスを受けるいるとの表示がよりませた。 ・組織は、メンテナンス製造がプロブロナスを確かし、認可されたメンテナンス製造は、オンデナンス製造がプロブロイを図え、 ・組織は、メンテナンス製造がプロブロイスを確かし、
				Basic	る。 ・組織は、必要なアクセス権限を持たない要員によるメンテナンス活動を監督するのに必要なアクセス権限と技術的能力を有する組織の要 費を指定する。
				H.Advanced	・組織は、特に重要な資産を管理している範囲内での重要資産の位置や移動を追跡し、モニタリングする。 ・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、入選室管理対策を実施する。 ・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入選室時のログを保持する。
		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	Advanced	・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆機が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア(執務室等)において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・自組織のオペレーションにとって重要度が高いと考えられる10T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、計タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。
				Basic	・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来 客に付き添うなどして人手による代替的な対策を実施する。
A.11.1.3 オフィス, 部屋及t ゼキュリティ	オフィス、部屋及び施設に対する物理的セキュ 施設の リティを設計し、適用しなければならない。			H.Advanced	・組織は、自組織のloT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の施設に対する物理的な侵入について警報と監視装置(例):監視カメラ)をモニタリングする。 ・組織は、自組織の店機器、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
		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	Advanced	施する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリア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。
			査等の物理的セキュリティ対策を実施する	Basic	 組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 組織は、自組織の施設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。 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モニタリングする。
				H.Advanced	・組織は、特に重要な資産を管理している範囲内での重要資産の位置や移動を追跡し、モニタリングする。

	ISO/IEC 27001:2013 附属書	4		y .	イバー・フィ	ジカル・セキュリティ対策フレームワーク
管理策ID		要求事項	対策要件ID	対策要件		対策例
			CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定および記録、監視を実施する	Advanced Basic	・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。 ・組織は、個人の物態的なアクセスを許可する前に、当該乗員のアクセス権股を確認し、入退室等のログを保持する。 ・組織は、個人の物態的なアクセスを許可する前に、当該乗員のアクセス権股を確認し、入退室等のログを保持する。 ・超視カメラ等による常勢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系統が顕在化した際に監査ログをレビューする。 ・自組織の提当者が来客に付き添って、来客の行動をモニタリグする。 ・組織は、10 機器、サーバ等が設置されている自組艦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。 ・組織は、10 機器、サーバ等が設置されている自組艦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。 ・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10 機器、サーバ等のもプであるが、遠隔地に存在している等の理由により、この物理的セキュリティ対策の実践が難しいと考えられる場合、耐タンバ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・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。 ・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、自組織の担当者が未
	A.11.1.4 外部及び環境の脅威からの 保護	自然災害,悪意のある攻撃又は事故に対する物理的な保護を設計し,適用しなければならない。	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、 生体認証等の導入、監視カメラの設置、持ち物や体重検 音等の物理的セキュリティ対策を実施する	H.Advanced	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JoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 - 組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 - 組織は、自組織の必及ドカする物理的な侵入について警報と監視装置(例): 監視カメラ)をモニタリングする。
			CPS.IP-5	・無停電電源装置、防火設備の確保、浸水からの保護 等、自組織のIoT機器、サーバ等の物理的な動作環境に関 するポリシーや規則を満たすよう物理的な対策を実施す	H.Advanced Advanced	 組織は、無停電電源装置等により自組織のIoT機器、サーバ等が設置されているエリア内の機器の安定な稼働を維持する。 ・組織は、独立した電源等により稼働する消火及び火災検知のための装置やシステムを導入し、維持する。 ・組織は、閉止弁や遮断弁を用意し、自組織のIoT機器、サーバ等が設置されているエリアを水漏れ等の被害から保護する。
	A.11.1.5 セキュリティを保つべき領	セキュリティを保つべき領域での作業に関する 手順を設計し、適用しなければならない。		3	Basic H.Advanced	・組織は、自組織のIT機器、サーバ等が設置されているエリアの温度と混度を定めた許容レベルに保つ仕組みを導入する。 ・組織は、自組織のIT機器、サーバ等が設置されているエリアの温度と湿度を定期的にモニタリングする。 ・組織は、自組織のIT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。
	域での作業		CPS.AC-2	・ loT機器、サーバ等の設置エリアの施錠、入退室管理、 生体認証等の導入、監視カメラの設置 持ち物や体重検 査等の物理的セキュリティ対策を実施する	Advanced	 ・組織は、自組織の施設に対する物理的な侵入について警報と監視装置(例:監視カメラ)をモニタリングする。 ・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 施する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する未容のアクセス記録を、一定期間保管するとともに定期的にレ ドラータを重する。
	A.11.1.6 受渡場所	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理しなければならない。また、可能な場合には、認可されていないアクセスを遅けるために、それらの場所を情報処理施設か	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	H.Advanced Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。
		ら離さなければならない。		査等の物理的セキュリティ対策を実施する	Basic	ビューを実施する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリア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 する。 ・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。 ・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モニタリングする。
A.11.2 装置	A.11.2.1 装置の設置及び保護	装置は、環境上の脅威及び災害からのリスク並 びに認可されていないアクセスの機会を低減す るように設置し、保護しなければならない。	CPS.IP-5	・無停電電源装置、防火設備の確保、浸水からの保護 等、自組織のIoT機器、サーバ等の物理的な動作環境に関 するポリシーや規則を満たすよう物理的な対策を実施す	H.Advanced Advanced	 組織は、無停電電源装置等により自組織のIoT機器、サーバ等が設置されているエリア内の機器の安定な稼働を維持する。 組織は、独立した電源等により稼働する消火及び火災検知のための装置やシステムを導入し、維持する。 組織は、閉止弁や遮断弁を用意し、自組織のIoT機器、サーバ等が設置されているエリアを水漏れ等の被害から保護する。
	A.11.2.2 サポートユーティリティ	装置は、サポートユーティリティの不具合による、停電、その他の故障から保護しなければならない。	CPS.BE-3	る ・ 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	Basic H.Advanced	- 代映徳信サービスの確立 - システ人の研究機構よど電力ケーブルの物理的保護 - 短期無停電電波展置の準備 - 特に、代普通信サービスの利用を検討する際、下記について考慮する - 通信サービス事業者との契約事項を検討する際、組織の可用性に関する要求事項(目標復旧時間を含む)を明確にする - 次遊信サービスとの間で単一障害点が共有される可能性を低減する
			CPS.DS-6	・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	Advanced	・要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・を予測する。 ・装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。 ・データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。 ・装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。 ・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用える。

ISO/IEC 27	7001:2013 附属書A		サイバー・フィジカル・セキュリティ対策フレームワーク					
管理策ID		要求事項	対策要件ID	対策要件		対策例		
				双、交換作業、グノトワエアの更新を行う	Basic	・要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 ・装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。 ・データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。 ・装置は、同用性及び完全性を経絡的に維持することを確実にするために、正しく保守する。		
		CPS	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	H.Advanced Advanced	・租職は、自租職の利用するシステムが設置されている施設に職員が常柱しない場合には、自動消火機能を導入する。 ・租職は、無停電電源援軍等により自租職の回収機、サーバ等が設置されているエリア内の機構の安定な稼働を維持する。 ・租職は、独立した電源等により移動する消火及が火災検知のための装置やシステムを導入し、維持する。 ・租職は、開生や遮断才を用意し、自租職の同び機能、サーバ等が設置されているエリアを水源れ等の被害から保護する。		
				\$	Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定めた許容レベルに保つ仕組みを導入する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定期的にモニタリングする。		
A.11.2 ケーフ ティ	ブル配線のセキュリ する通	マを伝送する又は情報サービスをサポート 性信ケーブル及び電源ケーブルの配線は、 妨害又は損傷から保護しなければならな		・IoT機器、サーバ等の設置エリアの施錠、入退室管理、 生体認証等の導入、監視カメラの設置、持ち物や体重検 査等の物理的セキュリティ対策を実施する	H.Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の施設に対する物理的な侵入について警報と監視装置(例:監視カメラ)をモニタリングする。		
	L'o			・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、対象を持続を持ていません。	Advanced	・要求されたンステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 ・炭製は、サポートユーティリティの不具合による、停電、その他の故障から保護する。 ・データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。 ・炭製は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。 ・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。		
				知、交換作業、ソフトウェアの更新を行う	Basic	・要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 ・装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。 ・データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。 ・装置は、可用性及び完全性を経過りに維持することを確実にするために、正しく保守する。		
A.11.2 装置の		t, 可用性及び完全性を継続的に維持する 確実にするために、正しく保守しなけれ ない。	CPS.DS-6	・IoT機器、通信機器、回線等に対し、定期的な品質管 PS.DS-6 理、予備機や無停電電源装置の確保、冗長化、故障の検 知、交換作業、ソフトウェアの更新を行う	Advanced	・要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 ・検査は、サポートユーティリティの不具合による、停電、その他の故障から保護する。 ・データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。 ・機額は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。 ・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。		
					Basic	 ・要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 ・装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。 ・データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。 		
				 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 	H.Advanced	・組織は、自組織のIOT機器、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、 モニタリングを実施する。 ・組織は、自組織のIOT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な 変更またに不定な実更がないか破認する。 ・組織は、自組織のIOT機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認 した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを 過去たい可襲を進入する。		
			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loT機器を導入 する	Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事情に承認するものともに、移動に先立って開連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正し、栄騰しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを経発を保管する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスと観音を発音する。 ・組織は、自然間のIoT機器、サーバ等のアップデート等のメンテナンスと観音を発音する。			
				6-60-66-01 T16-00 II	H.Advanced	・組織は、遠隔保守のための接続の確立と実施に関するポリシーとプロシージャを文書化し、その内容により実施する。		
		C		・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	Advanced Basic	・組織は、実施した遠隔保守の実施記録を保管する。 ・組織は、遠隔保守を実施する際には組織の定めるネットワークアクセスに求める認証を実施するとともに、遠隔保守が完了したらセッションとネットワーク接続を確実に終了する。		
A.11.2 資産の		情報又はソフトウェアは、事前の認可な 、構外に持ち出してはならない。		・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	H.Advanced	・組織は、遠居保守の実施に当たっては、実施計画を策定し、合意した上で実施し、実施結果を確認する。 ・組織は、自題側の1円機器、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、事前に来認するものとし、モニタリングを実施する。 ・組織は、自組織の10円機器、サーバ等のアップデート等を実施する要負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、不適切な変更またに不定を実更がないか確認する。 ・組織は、自組織の10円機器、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		

	ISO/	/IEC 27001:2013 附属書/	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					
	管理策ID		要求事項	対策要件ID	対策要件	対策例			
		A.11.2.6 構外にある装置及び資産の セキュリティ	構外にある資産に対しては、構外での作業に 伴った、構内での作業とは異なるリスクを考慮 に入れて、セキュリティを適用しなければなら ない。	CPS.MA-1	・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、アブリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する	Advanced	・組織は、自組織のloT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のloT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のloT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に充立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のloT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、影響を受けて可能性のあるすべてのセキュリティ対策を		
		A.11.2.7 装置のセキュリティを保っ た処分又は再利用	記憶媒体を内蔵した全ての装置は、処分又は再 利用する前に、全ての取扱いに慎重を要する データ及びライセンス供与されたソフトウェア を消去していること、又はセキュリティを保っ て上書きしていることを確実にするために、検	CPS.IP-6	loT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loT機器、サーバ等を一意に識別するデータD(識別子)や重要情報(秘密鍵、電子証明書等)を削除又は読み取りできない状態にする	H.Advanced Advanced Basic	・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接 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。 ・組織は、自組織のIoT機器やサーバ等を廃棄するブロシージャを定め、そのブロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。 ・組織は、自組織のIoT機器やサーバ等を廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態する。		
	A.11.2.8 利用者は、無人状態にある装置が適切な保護対 無人状態にある利用者装置 策を備えていることを確実にしなければならな い。		H.Advanced Advanced Basic	・組織は、自組織の10T機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の施設に対する物理的な役人について警報と監視装置例・監視カメラ)をモニタリングする。 ・組織は、自組織の10T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。 ・組織は、自組織の10T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。 ・組織は、自組織の10T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ング・セスリング・セスリング・セスリング・ロースに必要な許可証明書を発行する。 ・組織は、自組織の10T機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の10T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。					
		A.11.2.9 クリアデスク・クリアスク リーン方針	書類及び取外し可能な記憶媒体に対するクリア デスク方針、並びに情報処理設備に対するクリ アスクリーン方針を適用しなければならない。	対するクリ ならない。		H.Advanced Advanced	 - 組織は、自組織の10T機器、サーバ等が設置されているエリアに対する来率について、付き添う等して来客の行動をモニタリングする。 - 組織は、自組織のは関機、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 - 組織は、自組織のが起い対する物理的な侵入について警報と監視装置(例:監視カメラ)をモニタリングする。 - 組織は、自組織の応設に対する物理的な侵入について警報と監視装置(例:監視カメラ)をモニタリングする。 - 組織は、自組織の10T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。 - 組織は、自組織の10T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。 - 組織は、自組織の10T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延明書を発行 - 組織は、自組織の10T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延明書を発行 - 組織は、国籍側の10T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延明書を発行 		
A.12 運用のセキュリティ	A.12.1 運用の手順及び責任	A.12.1.1 操作手順書	操作手順は、文書化し、必要とする全ての利用 者に対して利用可能にしなければならない。		・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	Basic H.Advanced	する。 ・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。 ・組織は、自組織の10機器、サーバ等が設置されているエリアと対する来客について、付き添う等して来客の行動をモニタリングする。 ・経来の17環境において運用も大口なものと基本的な方針を共有しつへ、10T機器が設置されるサイトの性質等を十分に考慮したセキュリティポリシー群、運用手順を策定する。 [参考]例えば、産業用オードメーション及び制御システム(IACS)を対象としたセキュリティマネジメント規格であるIEC 62443-2-1では、IACS環境のための上位レベルのサイバーセキュリティポリシーの策定を求めている。特に産業分野におけるセキュリティボリシーおよび運用手順の策定にあたっては、"制御システムセキュリティ運用がイドライン"(日本電気制御機能工業会、2017年)等を参考とすることができ		
		A121 2	施設でした リニニュー中が研究とと 3 女女会会 至文が	CPS.GV-1		Advanced	を 地間は、上世の力計を支えるセキュリティボリシー科のより扱いレヘルとしく、例えば下近のようなトピッツ領別の力計を来走する。 a) アクセス制御および認証 b) 物理的セキュリティ対策 c) システムの開発および保守 d) 外部委託先管理 e) 情報分類および取扱い ・セキュリティボリシー群の東定に当たっては、自組織の a) 事業戦略、b)関係する規制、法令および契約、c)セキュリティの脅威環境を十分に考慮して、自組織の a)事業戦略、b)関係する規制、法令および契約、c)セキュリティの脅威環境を十分に考慮して、自組織の a)事業戦略、b)関係する規制、法令および契約、c)セキュリティの脅威環境を十分に考慮して、自組織の a)事業戦略、b)関係する規制、法令および契約、c)セキュリティの脅威環境を十分に考慮して、自組織し、自組織の a)事業、数略、b)関係する規制、法令および契約、c)セキュリティの脅威環境を十分に考慮して、セキュリティの脅威環境を十分に考慮して、セキュリティの脅威環境を十分に表して、セキュリティが関がより、たちなの事をとなる分野を把握したうえで、"中小企業の情報セキュリティボリシーサンブル改版(L10版)"UNSA、2016年)第五金集にすることがである。		
		A.12.1.2 変更管理	情報セキュリティに影響を与える,組織、業務 プロセス,情報処理設備及びシステムの変更 は,管理しなければならない。	CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び 設定変更管理プロセスを導入し、運用する	Advanced Advanced Basic	・組織は、構成管理の対象となる10T機器、サーバ等に対して変更を実施する前に、それらの変更をテスト・系統・文庫化する。 ・組織は、JoT機器、サーバ等の設定を一つの場所から管理・適用・検証するための自動化されたメカニズムを使用する。 ・組織は、JoT機器、サーバ等の設定を一つの場所が合管地・適用・検証するための自動化されたメカニズムを使用する。 ・組織は、持可された10T機器、サーバ等の変更に関して、実施できる要員(アクセス制限)を限定する。 ・組織は、計可された10T機器、サーバ等の変更に関して、実施できる要員(アクセス制限)を限定する。 ・組織は、計可された10T機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、計可された10T機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、JoT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。 ・組織は、JoT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 ・組織は、JoT機器の表別は、基础されている定を確認する ・組織は、JoT機器の表別は、基础されていると		

ISO/I	EC 27001:2013 附属書	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					
管理策ID		要求事項	対策要件ID	対策要件		対策例		
	A.12.1.3 容量・能力の管理	要求されたシステム性能を満たすことを確実に するために、資源の利用を監視・調整しなけれ ばならず、また、将来必要とする容量・能力を 予測しなければならない。	CPS.DS-5	・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	Advanced	・システムは、超極が定めたセキュリティ対策を実施することによって、組織が定めたタイプのサービス拒否攻撃、またはそうした情報の情報源への参照のサービス拒否攻撃による影響を最小限に加える。 ・システムは、予備の容量、帯域幅/その他の予備を管理して、大量の情報を送りつけるタイプのサービス拒否攻撃による影響を最小限に加える。 ・要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また。将来必要とする容量・能力を予測しなければならない。 ・組織は、 (a) 情報システムに対するサービス妨害攻撃の兆候を発見するための組織が定めた、モニタリングツールを使用する (b) 組織が定めた情報システムに対するサービス妨害攻撃の兆候を発見するための相機が定めた、モニタリングツールを使用する かどうかを判断する。		
			CPS.DS-6	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う	Advanced	・要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 ・ 装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。 ・ データを伝送する又は情報サービスをサポートする遺信ケーブル及び電源ケーブルの配線は、停受、妨害又は損傷から保護する。 ・ 装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。 ・ 組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。		
				A、人次(F本、 / / / 1 / 2 / 0 文前 č lj /	Basic	 要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。 データを伝送する又は情報サービスをサポートする過信ケーブル及び電源ケーブルの配検は、停気、妨害又は損傷から保護する。 装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。 		
	A.12.1.4 開発環境, 試験環境及び運 用環境の分離	開発環境, 試験環境及び運用環境は、運用環境 への認可されていないアクセス又は変更による リスクを低減するために、分離しなければならない。		・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	H.Advanced	・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。 ・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。		
				してネットワークの完全性を保護する	Advanced	 ・システムは、自組織のシステムの繋がるネットワークにおける外部境界及び内部境界について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、それ介して外部ネットワーク等に接続する。 		
					Basic	 組織は、システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、フローの制御を実施する。 		
A.12.2 マルウェアからの保護	A.12.2.1 マルウェアに対する管理策	マルウェアから保護するために、利用者に適切 に認識させることと併せて、検出、予防及び回 復のための管理策を実施しなければならない。	CPS.DS-9	・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	H.Advanced	・組織は、完全性検証時に不一数が発見された場合にシステム管理者に適知する。自動化されたツールを使用する。 ・組織は、設定の不正な変更や、システム権限の不正な昇格等の、セキュリティ関連の変更が不正に行われた場合の検知能力を、組織のインシデント対応能力に組み入れる。		
				る機能を有する機器を導入する	Advanced	・システムは、ソフトウェア・ファームウェアの完全性チェックを定期的に実施する。		
		C	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	H.Advanced	・loT機能あるいはそうした機能を含んだシステムが、通常開待される結果とは異なる展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。 ・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。 ・システムは、IDS/IPSによる悪質コードの検知ロジックを自動的に更新する。 ・エンドポイント(IoT機器、サーバ等)において、マルウェアに対する振舞い検知型の検出・修復ソフトウェアを導入することで、未知の脆弱性を実く攻撃コードの検知を実施する。 ・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、間かれ、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。		
			・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	Advanced	・システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・エンドポイント(IOT機能、サーバ等)において、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻 撃コードの検知を実施する。 米 特にIOT機能においては、マルウェア対策ソフトが利用可能なOSが使用されているとは関めないケースがある。組織は、調達時等に導入 する機器がマルウェア対策ソフトに対応できるものかを確認し、対応可能なものを選定することが望ましい。マルウェア対策ソフトに対応 する機器を調達することが困難な場合、ネットワーク上でマルウェアを検知する仕組みを導入・強化する等、代替的な対策を実施することが 望ましい。			

ISO/IEC	27001:2013 附属書		サイバー・フィジカル・セキュリティ対策フレームワーク					
管理策ID		要求事項	対策要件ID	対策要件		対策例		
	2.3.1 版のバックアップ	情報、ソフトウェア及びシステムイメージの バックアップは、合意されたバックアップ方針 に従って定期的に取得し、検査しなければなら ない。	CPS.BE-3	・自組織が事業を継続する上での自組織および関係する 他組織における依存関係と重要な機能を識別する	H.Advanced	・組織は、自らの事業を継続する上で、重要な依存関係にあるサプライヤーを規別する。 ・組織は、自らの事業を継続する上で、自組織が有する下記のサポートユーティリティの果たす機能および依存関係を識別する。 ・通信サービス ・悪力設備(能力ケーブル等を含む) ・上記で識別されたユーティリティの内、事業継続という観点から重要な役割を果たすものについて、下記のような対策を講ずることを検討する。 ・ 代野通信サービスの確立 ・ システムの電力設備および電力ケーブルの物理的保護 ・ 短期無序電池速波面の単備 ・ 特に、代替通信サービスの利用を検討する際、下記について考慮する ・ 通信サービスの利用を検討する際、下記について考慮する ・ 通信サービスを関係で乗業者との契約事項を検討する際、知識の可用性に関する要求事項(目標復旧時間を含む)を明確にする ・ 一次通信サービスをの間で単一階書点が共きれる可能性を抵索する		
					Advanced	- CPS.AM-6で規定した当該システムの可用性に対する要求水準に応じて、その容量・能力に関する要求事項を特定する。 - 要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。		
					H.Advanced	・組織は、パックアップ情報を定期的にテストして、媒体の信頼性と情報の完全性を確認する。		
			CPS.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	Advanced	組織は、自組織のシステムドキュメントのパックアップを定めたタイミングや頻度で実施する。組織は、保管拠点におけるパックアップ情報の機密性・完全性・可用性を保護する。		
				なンステムハックテックを実施し、テストしている	Basic	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。		
	.2.4.1 ベントログ取得	利用者の活動,例外処理,過失及び情報セキュリティ事象を記録したイベントログを取得し,保持し,定期的にレビューしなければならない。	, 白鉛線44門形でナス分割線トの430分	・白組織が関係する他組織との契約トの差務を里たして	H.Advanced	・組織は、取引先、第三者的な監査機関等の関係する他組織からのリアルタイムでのニーズに柔軟に応じるため、下記の特徴を有した証跡保管システムを利用する。 - 対象となる監査証跡の契約事項に対する遺格性を高速で検証することができる - 吸引先や委託を受けた監査機関等の許可を受けたエンティティのみがアクセスできる - 保管されているデータが、タイムスタンプや電子署名により証跡としての信頼性を有している		
			CPS.SC-7	・自組織が関係する他組織との契約上の義務を果たして いることを証明するための情報(データ)を収集、安全に 保管し、必要に応じて適当な範囲で開示できるようにす る	Advanced	・組織は、システムによって生成された監査記録のうち長期にわたって取得する監査記録を確実に取得できるよう、対策を実施する。 ・システムは、監査記録を次の脅威から保護するため、粒度の高いアクセス制御等を監査記録を保存するモノ、システムに適用することが望ましい。 ・記録されたメッセージ形式の変更 - ログファイルの変更又は削除 - ログファイル媒体の記録容量超過		
					Basic	・組織は、法規制等により要求される事項を満たす事ができるよう、適切な期間の監査記録を保持する。		
			CDC DT 1	・セキュリティインシデントを適切に検知するため、監	H.Advanced	・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、 (論理的・物理的を問わず) 管理される。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供 する。 ・システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用する10 T機器には、セキュリティに関わる監査ログの生成や成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 配性があるため。10 T機器から配査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム 側での対策による代替等、10 T機器のスペックを考慮した対応を行う必要がある。		
				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	Advanced	 システムは、監査ログおよび監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。 		
					Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を 行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要 に応じてシステム管理者等へ報告する。		
					H.Advanced	・組織は、セキュリティ専門の24時間365日モニタリングモニタリングにより収集した監査ログを、分析自動化ツール等を利用することで効率的に分析する。 ・組織は、従来のIT環境だけでなく、制御システムやIoT機器も含めて、セキュリティ状況のモニタリングやインシデントへの対応等のセキュリティ ・組織は、セキュリティ対応組織の成熟度を定期的に評価し、セキュリティ状況のモニタリングやインシデントへの対応等のセキュリティ 関連業務を経験的に改善することが望ましい。 [参考]セキュリティ対策組織(SOC/CSIRT)を評価するためのメトリクスには、"セキュリティ対応組織成熟度セルフチェックシート"(ISOG-J, 2018年)や、SIM3(Security Incident Management Maturity Model)等がある。		

ISO/IEC 27001:2013 附	《書A		th-	イバー・フィミ	ジカル・セキュリティ対策フレームワーク
管理策ID	要求事項	対策要件ID	対策要件		対策例
		CPS.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	Advanced	・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。 - モニタリングするシステムの範囲をどこまでとするか - どのような機器のログを収集し、分析するか (CPS.AE-3を参照) - 組織は、モニタリングにより収集した監査ログを定開的にレビューする。 - 組織は、モニタリングにより収集した監査ログを定開的にレビューする。 - 組織は、西海情機、機器の再情機、ネットワーク構成情報を建設的に収集・管理し、自組織のセキュリティ対応状況を評価する。 - 組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する。プロセスの内容については、CPS.RP-1等を参照。 - 組織およびシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には下記を含むことが望ましい。 - ログラ析の分析結果(対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等) - モニタリングにおける今後の改善方針 [参考]セキュリティ対策組織(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)の教料書 ~ 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。
				H.Advanced	・最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的なモニタリング に用いられている活動の修正の必要性を判断する。 ・組織は、自組織でIDS,IPS,SIEMと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。 ・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。
		CPS.AE-3	・セキュリティ事象の相関の分析、及び外部の脅威情報 と比較した分析を行う手順を実装することで、セキュリ ティインシデントを正確に特定する	Advanced	・*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 データベースに格勢したり、SIEMを利用したりして、効率的な分析を実現する必要がある。取得可能な場合はネットフローの情報も扱うこ とが望ましい。 - ファイアウォールなどのネットワーク装置からのログやネットフロー - IPS/IDSなどのセキュリティ装置からのログ - Web サーバなどのアクセスログ - ActiveDirectoryやDNSなどの各種システムからのログ - ユーザ利用端末に関するログ
				Basic	・ファイアウォールやエンドポイントセキュリティ製品等の通知を個別に確認することで、影響を及ぼすようなセキュリティインシデントを特定する。
		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	Basic	・組織は、リスクマネジメントに係る戦略やアセスメントの結果等から、セキュリティインシデントを検知するために収集することが望ましいログ情報を決定する。 ・組織は、取引先(サービスプロバイダー)に対して、取得されるサービス利用者の活動、例外処理及びセキュリティインシデントを記録した 監査ログの存在を確認する。 ・組織は、サービスプロバイグーにより取得される監査ログが、サービスの利用者の活動、例外処理及びセキュリティインシデントを記録で まており、適切な方式で保護されていることを確認する。
A.12.4.2 ログ情報の保護	ログ機能及びログ情報は、改ざん及び認可され ていないアクセスから保護しなければならな い。	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監 査記録/ログ記録の対象を決定、文書化し、そうした記 録を実施して、レビューする	H.Advanced	・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、 (論理的・物理的を問わず)管理される。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供 する。 ・システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用する101機器には、セキュリティに関わる監査ログの卓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、101機器のかの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム 側での対策による代替等、101機器のスペックを考慮した対応を行う必要がある。 ・システムは、監査ログおよび監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実後する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与す
A.12.4.3 実務管理者及び運用打 当者の作業ログ	システムの実務管理者及び運用担当者の作業 は、記録し、そのログを保護し、定期的にレ ビューしなければならない。		・セキュリティインシデントを適切に検知するため、監	H.Advanced	・システムは、医査レビュー・分析・レホートのそれぞれについて、一体的に扱う目動的なメカニスムを採用する。 ・組織が利用する101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、101機器からの監査ログの収象・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム
		CPS.PT-1	査記録・ク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	Advanced	側での対策による代替差、10円機器のスペッタを非慮した対応を行う必要がある。 ・システムは、監査ログおよび監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。

ISO/IE	C 27001:2013 附属書	A	サイバー・フィジカル・セキュリティ対策フレームワーク					
管理策ID		要求事項	対策要件ID	対策要件		対策例		
Ā	N.12.4.4	組織又はセキュリティ領域内の関連する全ての			Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの完候の有無を確認し、必に応じてシステム管理者等へ報告する。 ・タイムスタンが複数の企置の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券として		
	クロックの同期	情報処理システムのクロックは、単一の参照時 刻源と同期させなければならない。	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監 査記録/ログ記録の対象を決定、文書化し、そうした記 録を実施して、レビューする	H.Advanced	(論理的・物理的を問わず)管理される。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を指する。 ・システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用する10T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最終等が難しいものが含まれている 能性があるため、10T機器のから監査ログの収集・分析に当たっては、生活の用しているものとは別のログ管理システムの利用や、システ側での対策による代替等。10T機器のスペックを考慮した対応を行う必要がある。		
A.12.5	A.12.5.1	運用システムに関わるソフトウェアの導入を管			H.Advanced	・組織は、構成管理の対象となるloT機器、サーバ等に対して変更を実施する前に、それらの変更をテスト・承認・文書化する。		
	運用システムに関わるソフ トウェアの導入	理するための手順を実施しなければならない。	CPS.IP-1	・loT機器、サーバ等の初期設定手順(バスワード等)及び	Advanced	・組織は、loT機器、サーバ等の設定を一つの場所から管理・適用・検証するための自動化されたメカニズムを使用する。 ・組織は、MR成管理の対象となるloT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 可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたloT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。		
				設定変更管理プロセスを導入し、運用する	Basic	・組織は、計可されたIの機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、自即回の運用に適合でも無も制限され設定基準を定めた上で、導入されるIoT機器、サーバ等の切削設定手順及び設定内容を 増化するとともに、その文書に従って設定を実施する。 ・組織は、IoT機器を設置する前にデフォルトの初期設定値を確認する ・組織は、IoT機器を設置する前にデフォルトの初期設定値を確認する ・組織は、IoT機器を設定する前にデフォルトの初期設定値を確認する。		
			CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェア を制限する	H.Advanced	・ Namux、101gesの場入り15 作戦とれたいなノアウエアを強悪し、必然する ・ 組織は、自組織のシステム上を実行を計可するプリウェアの一覧(プラックリスト) 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。		
	A.12.6.1 利用中の情報システムの技術的ぜい弱性に関す 支術的ぜい弱性の管理		・自組織の資産の脆弱性を特定し、文書化する	H.Advanced	 ・組織は、自組織の管理するシステムにおける原知の脆弱性を認識するため、定期的に使入テストを実施する。 ・組織は、ツールを用いて脆弱性診断を行う場合、診断すべきシステムの脆弱性をすぐに更新できる脆弱性診断・アルを使用する。 ・組織は、脆弱性診断・に際して、診断者に特権アクセスの権利を一時的に許可する制度を整備することで、より徹底した脆弱性の洗い出し行う。 			
		CPS.RA-1		Advanced	・組織は、脆弱性診断を実施し、自組織の所有するシステムに存在する脆弱性を認識し、一覧化する。 ・組織は、自組織の所有するシステムの選用段階において、各種ソースから収集した脆弱性の内、自組織に関連することが想定されるも に対して、脆弱性検査ツール等を用いて、定期的に自組織のシステムにおける脆弱性を特定し、当該脆弱性の影響度とともに一覧に追加 る。 (参考)脱弾性情報の取得に限して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の の大きさを評価する指標として、CVSS(IPAによる解説: https://www.ipa.go.jp/security/vuln/CVSS.html)を参考とすることが可能である。			
		CPS.RA-4		・構成要素の管理におけるセキュリティルールが、実装 方法を含めて有効かを確認するため、定期的にリスクア セスメントを実施する ・IoT機器およびIoT機器を含んだシステムの企画・設計 の段階から、受容できない既知のセキュリティリスクの 有概を、セーフティに関するハザードの観点も踏まえて 確認する	H.Advanced	・ 組織は、モノの制制等を伴うような、フィジカル空間に影響を及ぼす可能性のある新たな機器やシステムを開発する場合には、従来のや他の事故事例を収集・分析し、セーフティに関わるハザードを特定する。 ・組織は、ハザードによって被害に至る状況を分析し、発生しやすさや被害の深刻度を明らかにすることで、生じるリスクを見積もる。 の際、セキュリティの問題に返因するハザードの有無を確認することが望ましい。 [参考]セーフティ設計におけるハザードの特定と分析については、「つながる世界のセーフティ&セキュリティ設計入門」(IPA、2015年) 42にて見体的な手法が記載されており、参照することが可能である。 ・組織は、ジオケム、またはアメカムが構造するが現状できな変化があった場合側がな脊板や影響性の特定を含む)、もしくはンステム・ ・組織は、ジオケム、またはアメカムが構造するが現状できな変化があった場合側がな脊板や影響性の特定を含む)、もしくはンステム・		
			CPS.RA-4		Advanced	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10世級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、高い可用性をられるモノ、システムを扱う場合は、設計以前の段階におけるセキュリティ対策の考慮が特に重要である。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものでることを確実にする。 「参考)ン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! 策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。		
			CPS.RA-5	・リスクを判断する際に、脅威、脆弱性、可能性、影響 を考慮する	Advanced	・組織は、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(銀行な脅威や脆弱性の特定を含む)、もしくはシステム キュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。その際、重要皮の高いシステムを優先的に 応する。 家CPS.RA-4と共通の実施内容		
					H.Advanced	・組織は、欠陥修正状況を管理するための自動化されたメカニズムを導入し、管理する。 ・組織は、修正内容の有効性と副次的な悪影響の可能性についてテストを行った上で欠陥の修正を実施し、当該修正を構成管理として管		
		CPS.IP-1	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	Advanced	する。 ・組織は、自組織のシステムに関する欠陥の特定・報告・修正を計画的に実施する。		
					Basic	[参考]特に、製造現場等に設置されるIoT機器には、可用性や機器自体の機能の関係で、タイムリーにパッチを適用すること、あるいはメ チの適用事態が困難な場合がある。その場合は、「制御システム利用者のための能弱性対応ガイド第2版」(IPA, 2016年)の P.23に記載さ いる通り、脅威への対策(機能の最小化、ネットワーク監視の強化等)を徹底し、セキュリティ被害の発生を回避することが望ましい。		
					H.Advanced	・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。		

	ISO/I	EC 27001:2013 附属書/	A	サイバー・フィジカル・セキュリティ対策フレームワーク					
	管理策ID		要求事項	対策要件ID	対策要件		対策例		
				CPS.CM-7	・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する	Advanced	・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ば す新たた酸弱性が確認され、報告された場合に実施する ・組織は、脆弱性矢キャンにツールを用いる。以下を満たす標準的な手法を使用することによって、脆弱性管理プロセスの一部を自動化で きることが求められる ・プラットフォーム、ソフトウェアの欠陥、および誤った設定を列挙する ・チェックリストとテスト手順をフォーマットする ・脱弱性による影響を評価する ・規織は、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開間中に修正する ・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]服勢性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報液を参照することが可能である。また、脆弱性の影響 の大きさを評価する指標として、CVSS(IPAによる解説:https://www.ipa.go.jp/security/vuln/CVSS.html)を参考とすることが可能である。 ・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実施する		
		A.12.6.2	利用者によるソフトウェアのインストールを管				・組織は、システムわよびアノリケーションの能物性のスキャンを走崩的に夫施する ・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(ボワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)		
			理する規則を確立し、実施しなければならな		・IoT機器、サーバ等の導入後に、追加するソフトウェア	H.Advanced	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。		
		ルの制限	い。	CPS.IP-2	・101機器、サーハ寺の導入後に、追加するアフトリエア を制限する	Advanced	・組織は、自組織のシステム上でのユーザによるソフトウェアのインストールについて管理するメカニズムを導入し、モニタリングを実施する。		
						Basic	・組織は、自組織のシステム上でのユーザによるソフトウェアのインストールに関するポリシーを確立し、ユーザに遵守させる。		
	A.12.7 情報システムの監査に対す る考慮事項	A.12.7.1 情報システムの監査に対す る管理策	運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意しなければならない。		・取引先等の関係する他組織が、契約上の義務を果たし	H.Advanced	・組織は、契約事項からの逸配および、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先およびその再委託先以降の組織に対して、契約にて規定した組織のセキュリティマネジメント、納入する製品・サービスに実装されるセキュリティ機能等に関する義務事項が履行されているかどうかを一覧化して確認できるメカニズムを利用する。 ・委託元による実地調査、外部監査等の手法により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。		
				CPS.SC-5	・ 取り、たみの関係する他組織が、乗約エの表がを来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	Advanced	 組織は、自組織が取引先との契約において要求事項として規定した内容に関連して、システム上での監査が可能かどうか、確認する。 ・上記で定義されているシステム上で監査可能なイベントのために、監査記録を生成する機能を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でレビュー・分析して、契約事項からの逸脱および、その系域の有益を確認する。 ・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。 		
				・セキュリティインシデントを適切に検知するため、監	H.Advanced	・システムは、監査レビュー・分析・レホートのそれぞれについて、一体的に扱う目動的なメカニスムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や原存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等。IoT機器のスペックを考慮した対応を行う必要がある。			
				CPS.PT-1	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	Advanced	・システムは、監査ログおよび監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。 ・ 地域、自組織のリスクマネジメントの戦略や、リスのアセスメントの結果等に基づき、監査対象を設定し、対象において護がいつ何を		
						Basic	行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンボーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ発生する。		
A.13 通信のセキュリティ	A.13.1 ネットワークセキュリティ 管理	A.13.1.1 ネットワーク管理策	システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御しなければならない。	・適宜ネットワークを分離する(例:開発・テスト環境と CPS.AC-7 実運用環境、loT機器を含む環境と組織内の他の環境)等	H.Advanced	・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分接続のじする。 ・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。			
					してネットワークの完全性を保護する	Advanced	・システムは、自組織のシステムの繋がるネットワークにおける外部境界及び内部境界について適信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、それ介して外部ネットワーク等に接続する。		
			組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、			H.Advanced	 組織は、外部情報ンステムサービスのプロバイダに対して、サービスの使用に必要な機能、ボート、プロトコル、および他のサービスを明確にするよう要求する。 組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。 		

ISO/IEC 27001:2013 附属書	A .	サイバー・フィジカル・セキュリティ対策フレームワーク					
管理策ID	要求事項	対策要件ID	対策要件		対策例		
*1971	でキュリティ機能、リーピスレベル及び管理上の要求事項を特定しなければならず、また、ネットワークサービス合意書にもこれらを盛り込まなければならない。	CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サー ビスプロバイダとの通信内容をモニタリングする	Advanced	・組織は、外部サービスプロバイダおよびシステム開発の委託先の要負に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要負が異動、または雇用が終了する場合に、自組織、通知することを要求する。 ・組織は、関連する業務情報、業務システム及父業務プロセスの重要性、並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダーおよびシステム開発の委託先による特あるら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機のシステムへのアクセスををモニタリングする。 ・組織は、外部サービスプロバイダーおよびシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。		
				Basic	 ・組織は、外部情報システムサービスのプロバイダおよびシステム開発の委託先に対して、自組機が対象となっている、あるいは当該プロバイダーが対象として該当するルールに従って、例えば下記に関連するようなセキュリティ要求事項を設定し、導入することを要求する。 ・(例えば、ISMS総証政権相当の)セキュリティ対策が十分に行われていること ・ 週用中のデータが適切に管理されること ・ サービス利用終了時にデータが適切に削除されること 		
A.13.1.3 ネットワークの分離	情報サービス、利用者及び情報システムは、 ネットワーク上で、グループごとに分離しなければならない。	CPS.AC-7	・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、loT機器を含む環境と組織内の他の環境)等 してネットワークの完全性を保護する	H.Advanced	・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分接続可とする。 ・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。 ・システムは、自組織のシステムの繋がるネットワークにおける外部場界及び内部境界について通信をモニタリングし、制御する。		
			o en y n y system e program	Advanced	・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、それ介して外部ネットワーク等に接続する。		
A.13.2 A.13.2.1 情報の転送 情報転送の方針及び手順				H.Advanced	 ・組織は、システム構成、遠信ネットワーク構成、データフローをリアルタイムでモニタリングし、管理するための自動化されたメカニズムを導入、管理している。 ・組織は、システムのベースライン構成のロールバックを可能にするために、旧パージョンのベースライン構成(例えば、ハードウェア・ソフトウェア・ファームウェア・構成ファイル・構成記録)を記録する。 		
		CPS.AM-4 ・企業内の通信ネットワーク構成図及び、データフ図を作成し、保管する	・企業内の通信ネットワーク構成図及び、データフロー	Advanced	 組織は、作成する図に、ネットワーク接続におけるインターフェース特性、セキュリティ要求事項、伝達されるデータの性質を記載する。 		
			and I MON Your / D	Basic	・組織は、企業内のシステム構成、通信ネットワーク構成、データフローを文書化し、保管する。 ・組織は、定期的、あるいは、システム構成、ネットワーク構成、データフローに変更が生じた場合、関連する文書をレビューし、必要に応じて更新する。 (参考)システム構成、ネットワーク構成、データフローの文書化を行う際の手順については、「制御システムのセキュリティリスク分析ガイド 第2版 [(PRA_2018年)の3.2、33を参照することが可能である。		
		CPS.AM-5	- 自組織の資産が接続している外部情報システムの一覧 を作成し、保管する	H.Advanced	・システムは、自組織が利用している外部情報サービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・システムは、利用を許可していない外部情報システムサービスを検知した場合、システム管理者へ通知するメカニズムを利用する。 ・組織は、外部プロバイダによるサービスを使用する際に必要な機能、ボート、プロトコル、および他のサービスを明確にする。		
				Advanced	・組織は、外部の情報システムを所有、運用する他の組織に対して、下記を許可するうえでの条件を設定する。 a、外部の情報システムから組組織の情報システムにアクセスすること b、外部の情報システムを使用して自組織の管理である情報を処理または保存もしくは伝送すること ・外部のシステム上での自組織のボータブルストレージの使用を制限する。		
		CDC 40 7	・適宜ネットワークを分離する(例:開発・テスト環境と	H.Advanced	・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分接続のとする。 ・機密性の高いデータを取り扱う自組機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.AC-1	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	Advanced	 システムは、自租機のシステムの繋がるネットワークにおける外部境界及び外部境界について通信をモニタリングし、制御する。 ・租機は、自租機のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、それ介して外部ネットワーク等に接続する。 		
				Basic	 組織は、システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、フローの制御を実施する。 		
			・IoT機器、サーバ等の間、サイバー空間で通信が行われ	H.Advanced	・組織は、重要なデータを扱う通信路について、通信経路の暗号化を実装するか、あるいは、代替の物理面での対策によって保護する。		
		CPS.DS-2	る際、通信経路を暗号化する	Advanced	・システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。		
		CPS.DS-3	・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	H.Advanced	・システム/IoT機器は、少ないリソースでも可用性を損なわずに実装可能な暗号モジュールを導入し、重要度の高い機器からの通信データ を適切な強度で暗号化することが望ましい。 ・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、情報(データ)		
				Advanced	を暗号化して送受信する。 ・・組織は、データス力に対する「ホワイトリスト」の概念を導入することで、インブットデータの出所を原知の信頼できるモノ、システム等と、そうしたインブットデータの許容できるフォーマットを指定する。		
		CPS.CM-4	・IoT機器、サーバ等において、送受信する情報(データ) の空心性セトバ吉正性た動作部に延歩する	H.Advanced			

	ISO/I	EC 27001:2013 附属書/		サイバー・フィジカル・セキュリティ対策フレームワーク				
	管理策ID		要求事項	対策要件ID	対策要件		対策例	
					77. 位注 17. 4. 0 突出 は 2. 80 (FB) (CR 80) 7. 0	Advanced	・システムは、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、当該IoT機器が自組線の業務において重要なものと認められる場合、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。	
		A.13.2.2 情報転送に関する合意	合意では、組織と外部関係者との間の業務情報 のセキュリティを保った転送について、取り扱 わなければならない。			H.Advanced	・組織は、システム構成、通信ネットワーク構成、データフローをリアルタイムでモニタリングし、管理するための自動化されたメカニズム を導入・管理している。 ・組織は、システムのベースライン構成のロールバックを可能にするために、旧パージョンのベースライン構成(例えば、ハードウェア・ソ フトウェア・ファームウェア・構成ファイル・構成記録)を記録する。	
				CPS.AM-4	・企業内の通信ネットワーク構成図及び、データフロー	Advanced	・組織は、作成する図に、ネットワーク接続におけるインターフェース特性、セキュリティ要求事項、伝達されるデータの性質を記載する。	
				図を作成し、保管する	Basic	・組織は、企業内のシステム構成、通信ネットワーク構成、データフローを文書化し、保管する。 ・組織は、定期的、あるいは、システム構成、ネットワーク構成、データフローに変更が生じた場合、関連する文書をレビューし、必要に応じて更新する。 (世考) システム構成、ネットワーク構成、データフローの文書化を行う際の手順については、「制御システムのセキュリティリスク分析ガイト第2版」(PA、2018年)の32、3.3を参照することが可能である。		
		A.13.2.3 電子的メッセージ通信	電子的メッセージ通信に含まれた情報は、適切に保護しなければならない。		・IoT機器、サーバ等の間、サイバー空間で通信が行われ	H.Advanced	・組織は、重要なデータを扱う適信路について、適信経路の暗号化を実装するか、あるいは、代替の物理面での対策によって保護する。	
				CPS.DS-2	る際、通信経路を暗号化する	Advanced	・システムは、暗号メカニズムを導入し、遺信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Jpsec-VPN、SSL-VPN等の方式が存在する。相機は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。	
				000000	・情報(データ)を送受信する際に、情報(データ)そのもの	H.Advanced	・システム/IoT機器は、少ないリソースでも可用性を損なわずに実装可能な暗号モジュールを導入し、重要度の高い機器からの通信データ を適切な強度で暗号化することが望ましい。	
				CPS.DS-3	を暗号化して送受信する	Advanced	・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、情報(データ) を解告化して详受信する	
			C	CPS.CM-4	4 ・loT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	H.Advanced	・ 地間域は、データ人力に対する「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原知の信頼できるモノ、システム等と、そうしたインプットデータの許容できるフォーマットを指定する。 ・ IoT機器、サーバ等は、他のIoT機器と通信する際、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把題を確実なものとする。 ・ システムは、通信セッションの真正性を保護する。	
						Advanced	・システムは、完全性検証ツールを使用して、10T機能、サーバ等からの適信データに対する不正な変更を検知する。 ・10T機能、サーバ等は、他の10機能を通信する際、当該10T機能が自組織の業務において重要なものと認められる場合、機器間の相互認証 が成功した後には100で適信を開始することで、データの出所の対策を要案なものとする。	
		A.13.2.4 秘密保持契約又は守秘養務 契約	情報保護に対する組織の要件を反映する秘密保 持契約又は守秘義務契約のための要求事項は、 特定し、定めに従ってレビューし、文書化しな ければならない。			H.Advanced	・組織は、システム・モブ・サービスのいずれかを提供する取引先との契約において、当該組織に対して、下記の実施を要求する。 - セキュリティアセスメント計画の作成 - テスト/評価の通切な影響での実施 - セキュリティアセスメント計画を実施したエピデンスの作成、セキュリティテスト/評価結果の提示 - 総当可能や下的機能デブロナスの主義	
				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	Advanced	・組織のミッション/業務ニーベに応じて、システム、モノ、またはサービスの調達契約に以下の要求事項、記述、および参考を記載する。 - セキュリティ対策に関する要求事項 - セキュリティ関連のドキュメントに関する要求事項 - セキュリティ関連のドキュメントに関する要求事項 - 秘密保持に関する条項 - インシデントが発生した際の報告先、報告内容、初動、調査、復旧等の各対応の実施主体、実施方法 - 自総職または認可された第三者によって監査され、定義されたセキュリティ要件への遵守を確認することを許可する条件 - 契約終了後の情報資産の扱い - 組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施し、委託内容の特性等により必要と認められる場合、 調達契約において、追加で対象を導入することを要求する。 - 法規制等を参照してセキュリティ要件を決定し、取引先へ遵守を要求する際、下記を事前に考慮することが望ましい。 - 自総職と取引条の間の法令の相違によって生しる潜在的な法的規則・200条に下記を事前に考慮することが望ましい。 - 自組織と取引条の間の法令の相違によって生しる潜在的な法的規則・200条に	
						Basic	組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施することを要求する。	
システムの取得、開発及び	A.14.1 青報システムのセキュリ ティ要求事項	A.14.1.1 情報セキュリティ要求事項 の分析及び仕様化	情報セキュリティに関連する要求事項は、新し い情報システム又は既存の情報システムの改善 に関する要求事項に含めなければならない。			H.Advanced	・調達する機器に対して、契約におけるセセキュリティ要求事項が満たせているかを、自相職あるいは第三者がテストする。 ・組織は、自組織のオペレーションにとって特に重要な機器について、再委託先以降の組織を含む関係するサプライチェーン全体に渡り、一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロシージャで製造されたものかを確認する。	

ISO/IEC 27001:2013 附属書	4	サイバー・フィジカル・セキュリティ対策フレームワーク					
管理策ID	要求事項	対策要件ID	対策要件		対策例		
		CPS.SC-4	・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提供する製品・サービスが適合していることを確認する	Advanced	・組織は、契約において、例えば下記のように、取引先から調達する製品・サービスが具備すべきセキュリティ要求事項を明確化する。 ・セキュリティに関わる特定の認証(例: ISMS認証、ISASecure EDSA認証、ITセキュリティ等価及び認証制度(ISECI)を有していること ・ベンダー自身により、セキュリティに関わる特定の認証の基準に適合する対策を実施していることが確認されていること ・リスク分析の結果等から導かれた必要なセキュリティ。要件を設計時からの実施(セキュリティ・バイ・デザイン)し、検査していること ・組織は、調達計画時に、製品またはサービス自体、あるいは当該製品・サービスの調達・供給にて使用される資産の保護に係るセキュリティ要件の費用を確保しておくことが望ましい。 ・下記を含む製品またはサービスの調達または供給を評価するためのセキュリティ測定ルールを策定し、運用および改善する。 ・測定対象の内容 ・措置が実施されない場合に遂行される措置 ・組織は、搬送中の改ざん・漏えいを検知(又は抑止)する手段とともに納品される10T機器やソフトウェアが、不正操作されていないかを確認する。 ・物品:セキュリティ便、プロテクトシール等 ・ 電送:暗号化、電送データ全体のハッシュ値等		
		CPS.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	H.Advanced Advanced Basic	・組織は、システムの測慮にあたり以下に示すような要求事項を明示的に提示する。 ・セキュリティ機能に関する要求事項 ・セキュリティ機能に関する要求事項 ・セキュリティ保証に関する要求事項 ・セキュリティ保証に関する要求事項 ・セキュリティ関連のドキュメントに関する要求事項 ・セキュリティ関連のドキュメントに関する要求事項 ・モャュリティ関連のドキュメントに関する要求事項 ・そのシステムの開発環境と、そのシステムを推動させる予定の環境についての記述 ・受け入れ基準 ・ 出機は、情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル企体を適じた情報セキュリティコスクマネジメントプロセスを実施する。 ・ 組織は、システムを構築するに当たり仕様素、設計、開発、導入、及び変更に、システムのセキュリティエンジニアリング原則を適用する。		
	公衆ネットワークを経由するアプリケーション サービスに含まれる情報は、不正行為、契約紛 争、並びに認可されていない開示及び変更から 保護しなければならない。	CPS.AC-7	・適宜ネットワークを分離する(例:開発・テスト環境と 実運用環境、IoT機器を含む環境と組織内の他の環境)等 してネットワークの完全性を保護する	H.Advanced Advanced	- 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、許可した遺信トラフィックの分接続可とする。 - 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。 - システムは、自組織のシステムの繋がるネットワークにおける外部境界及び内部境界について遺信をモニタリングし、制御する。 - 組織は、自組織のシステムの有効なセセュリティを促進する設計として境界を緩後置等を設置し、それ介して外部ネットワーク等に接続す		
		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際、通信経路を暗号化する	H.Advanced Advanced	る。 ・組織は、重要なデータを扱う通信路について、通信経路の暗号化を実装するか、あるいは、代替の物理面での対策によって保護する。 ・システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられ		
		CPS.DS-3	・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	H.Advanced Advanced	るコスト等を考慮しつつ、方式を選定することが望ましい。 ・システム/LOT機器は、少ないリソースでも可用性を損なわずに実装可能な暗号モジュールを導入し、重要度の高い機器からの通信データを適切な強度で暗号化することが望ましい。 ・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、情報(データ) を暗号化して送受信する。		
		CPS.DS-10	・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	H.Advanced Advanced	・組織は、、設定の不正な変更や、システム権限の不正な弊格等の、セキュリティ関連の変更が不正に行われた場合の検知能力を、組織の インシデント対応能力に組み入れる。 ・組織は、完全性検証ツールを使用して、IoT機器、サーバ等からの適信データに対する不正な変更を検知する。 ・システムは、保管データの完全性チェックを定開的に実施する。		
	アプリケーションサービスのトランザクション に含まれる情報は、次の事項を未然に防止する ために、保護しなければならない。 - 不完全な通信 - 誤った通信経路設定 - 認可されていないメッセージの変更	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	H.Advanced Advanced	・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、ネットワーク適信をデフォルトで拒否するものとし、許可した適信トラフィックのみ接続可とする。		
	- 認可されていない開示 - 認可されていないメッセージの複製又は再生	CPS.DS-10	・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	H.Advanced Advanced	シ・ ・ 相關は、、設定の不正な変更や、システム権限の不正な昇格等の、セキュリティ関連の変更が不正に行われた場合の検知能力を、組織の インシデント対応能力に組み入れる。 ・ 組閣は、完全性数ゴールを使用して、IoT機器、サーバ等からの遺信データに対する不正な変更を検知する。 ・ システムは、保管データの完全性チェックを定期的に実施する。		

ISO/IEC 2	27001:2013 附属書A			# -	イバー・フィシ	ジカル・セキュリティ対策フレームワーク
管理策ID		要求事項	対策要件ID	対策要件ID 対策要件		対策例
開発及びサポートプロセス セキ	4.2.1 キュリティに配慮した開 わための方針	ソフトウェア及びシステムの開発のための規則 は、組織内において確立し、開発に対して適用 しなければならない。	CPS.IP-3	・システムを管理するためのシステム開発ライフサイク ルを導入し、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	H.Advanced Advanced Basic	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 - セキュリティ機能に関する要求事項 - セキュリティ機能に関する要求事項 - セキュリティ保証に関する要求事項 - セキュリティ保証に関する要求事項 - セキュリティ関連のドキュメントに関する要求事項 - セキュリティ関連のドキュメントに関する要求事項 - セキュリティ関連のドキュメントの保護に関する要求事項 - そのシステムの開発環境と、そのシステムを推動させる予定の環境についての記述 - 受け入れ基準 - ・組織は、情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。 - 組織は、システムを構築するに当たり仕様書、設計、開発、導入、及び変更に、システムのセキュリティエンジニアリング原則を適用す
	ステムの変更管理手順	開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理しなければならない。	CPS.IP-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	H.Advanced Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 ・セキュリティ機能に関する要求事項 ・セキュリティ機能に関する要求事項 ・セキュリティ保証に関する要求事項 ・セキュリティ関連のドキュメントに関する要求事項 ・セキュリティ関連のドキュメントに関する要求事項 ・セキュリティ関連のドキュメントの保護に関する要求事項 ・そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 ・受け入れ基準 ・組織は、情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフ サイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
オペ フォ	ォーム変更後のアプリ ーションの技術的レ	オペレーティングブラットフォームを変更する ときは、組織の運用又はセキュリティに悪影響 がないことを確実にするために、重要なアブリ ケーションをレビューし、試験しなければなら ない。	CPS.IP-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	H.Advanced Advanced	・組織は、欠陥修正状況を管理するための自動化されたメカニズムを導入し、管理する。 ・組織は、欠陥修正状況を管理するための自動化されたメカニズムを導入し、管理する。 ・組織は、修正内容の有効性と副次的な悪影響の可能性についてテストを行った上で欠陥の修正を実施し、当該修正を構成管理として管理する。
パツ	ッケージソフトウェアの 更に対する制限	バッケージソフトウェアの変更は、抑止しなければならず、必要な変更だけに限らなければならない。また、全ての変更は、厳重に管理しなければならない。また、全ての変更は、厳重に管理しなければならない。	CPS.AM-1	・システムを構成するハードウェア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	Advanced	- 資産の構成情報(例:名称、バージョン情報、ライセンス情報、場所等)を含めて、目録を定期的にレビュー、更新することで維持・管理する。 - 組織は、システムコンボーネント上で利用可能な取り外し可能なメディア(例:USBメモリ)を一覧化し、使用を管理する。 - 組織は、ボータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を発止する。 - 組織は、標密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの利用状況を適切に把握し、管理する。
			CPS.MA-1	・IoT 機器、サーバ等のセキュリティ上重要なアップデー ト等を必要なタイミング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	H.Advanced	・組織は、自組織の10機器、サーバ等のアップアート等でメンア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、 セニタリングを実施する。 ・組織は、自組織の10T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 実更または不正な実更がないが確認する。 ・組織は、自組織の10T機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認 した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを 備えた10T機器を導入する。
					Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
セキ	キュリティに配慮したシ テム構築の原則	ゼキュリティに配慮したシステムを構築するための原則を確立し, 文書化し, 維持し, 全ての情報システムの実装に対して適用しなければならない。	CPS.IP-3	・システムを管理するためのシステム開発ライフサイク ルを導入し、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	H.Advanced	・組織は、ジステムの調達にあたり以下に示すような要求事項を明示的に提示する。 - セキュリティ機能に関する要求事項 - セキュリティ機能に関する要求事項 - セキュリティ機能に関する要求事項 - セキュリティ側連のドキュメントに関する要求事項 - セキュリティ関連のドキュメントに関する要求事項 - セキュリティ関連のドキュメントの保護に関する要求事項 - そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 - 受け入れ基準 - ・ 組織は、情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を適じた情報セキュリティリスクマネジメントプロセスを実施する。

ISO/IEC 27001:2013 附属書	Α		サイバー・フィジカル・セキュリティ対策フレームワーク					
管理策ID	管理策ID 要求事項		対策要件		対策例			
A.14.2.6 セキュリティに配慮した開 発環境	組織は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護しなければならない。	ため し, ・システムを管理するためのシステム開発ライフサイク 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 Advanced	H.Advanced	- 組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 - セキュリティ機能に関する要求事項 - セキュリティ機能に関する要求事項 - セキュリティ保証に関する要求事項 - セキュリティ保証のドキュメントに関する要求事項 - セキュリティ関連のドキュメントの保護に関する要求事項 - そのシステムの開連がドキュメントの保護に関する要求事項 - そのシステムの構造機能と、そのシステムを稼働させる予定の環境についての記述 - 受け入れ基準				
			Advanced Basic	 ・組織は、情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を過じた情報セキュリティリスクマネジメントプロセスを実施する。 ・組織は、システムを構築するに当たり仕様書、設計、開発、導入、及び変更に、システムのセキュリティエンジニアリング原則を適用す 				
A.14.2.7 外部委託による開発	組織は、外部委託したシステム開発活動を監督 し、監視しなければならない。				る。・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ボート、プロトコル、および他のサービスを明確にするよう要求する。・組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。			
		CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サー ビスプロバイダとの通信内容をモニタリングする	Advanced	・組織は、外部サービスプロバイダおよびシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が実動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報、業券システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を審理することが望ましい。 ・組織は、外部サービスプロバイダーおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダーおよびシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスををモニタリングする。 ・組織は、外部サービスプロバイダーおよびシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。			
				Basic	 ・組織は、外部情報システムサービスのプロバイダおよびシステム開発の委託先に対して、自組機が対象となっている、あるいは当該プロバイダーが対象として該当するルールに従って、例えば下記に関連するようなセキュリティ要求事項を設定し、導入することを要求する。 ・ (例えば、ISMS認定取得相当の)セキュリティ対策が十分に行われていること ・ 選用中のデータが適切に管理されること ・ サービス利用終了時にデータが適切に削除されること 			
A.14.2.8 システムセキュリティの試 験	セキュリティ機能(functionality)の試験は、 開発期間中に実施しなければならない。	CPS.DP-3	・監視業務として、セキュリティ事象を検知する機能が 意図したとおりに動作するかどうかを定期的にテスト	H.Advanced	・最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的なモニタリング に用いられている活動の修正の必要性を判断する。 ・システムに、原知で害のないテストケースを導入して、マルウェア検知メカニズムをテストする。 ・お開味は、侵入験打モニタリングに用いているメカニズムを定期的にテストする。テストの頻度は、組織が使用するツールの種類と、ツールの設置方法により変わる。			
		01 0.01 3	し、妥当性を検証する	Advanced	・組織は、自組織のシステムのモニタリング活動が、組織のリスクマネジメント戦略と、リスク対応のためのアクションの優先順位に適合 しているかどうかを定期的に確認するプロン・ジャを定め、運用する。 ・ネットワーク機能やエンドボイントからのセキュリティに係る情報の相関分析を行うのに合わせて、誤検出や検出漏れの割合を算出し。 定期的に検知メカニズムの妥当性を確認する。			
A.14.2.9 システムの受入れ試験	新しい情報システム,及びその改訂版・更新版 のために,受入れ試験のプログラム及び関連する基準を確立しなければならない。			H.Advanced	 調達する機器に対して、契約におけるセキュリティ要求事項が満たせているかを、自組織あるいは第三者がテストする。 組織は、自組織のオペレーションにとって特に重要な機器について、再委託先以降の組織を含む関係するサプライチェーン全体に渡り、一定水車以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロシージャで製造されたものかを確認する。 			
		CPS.SC-4	・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提供する製品・サービスが適合していることを確認する	Advanced	・組織は、契約において、例えば下記のように、取引先から調達する製品・サービスが具備すべきセキュリティ要求事項を明確化する。 ・セキュリティに関わる特定の設証(例:ISMS設証、ISASecure EDSA認証、ITセキュリティ評価及び認証制度(IISEO))を有していること ・リスク分析の結果等から導かれた必要なセキュリティ要件を設計時からの実験(セキュリティ・バイ・デザイン)し、検査していること ・組織は、調達計画時に、製品またはサービス自体、あるいは当該製品・サービスの調達・供給にて使用される資産の保護に係るセキュリティ要件の費用を確保しておくことが望ましい。 ・下記を含む製品またはサービスの調達または供給を評価するためのセキュリティ測定ルールを策定し、運用および改善する。 ・測定対象の内容 ・措置の報度方法、報告の頻度 ・措置が実施されない場合に遂行される措置 ・組織は、搬送中の改ざん・漏えいを検加(又は抑止)する手段とともに納品されるIoT機器やソフトウェアが、不正操作されていないかを確認する。 ・物品:セキュリティ便、プロテクトシール等 ・電送:暗号化、電送データ全体のハッシュ値等			
A.14.3 試験データ 試験データの保護	試験データは、注意深く選定し、保護し、管理 しなければならない。	CPS.SC-4	・外部の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提供する製品・サービスが適合していることを確認する	H.Advanced	・ 調達する機器に対して、契約におけるセキュリティ要求事項が満たせているかを、自組織あるいは第三者がテストする。 ・ 組織は、自組織のカペレーションにとって特に重要な機器について、再表託先以際の組織を含む関係するサブライチェーン全体に渡り、 一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロシージャで製造されたものかを確認する。			

	ISO/II	EC 27001:2013 附属書	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				
	管理策ID		要求事項	対策要件ID	対策要件		対策例	
					・取引先等の関係する他組織が、契約上の義務を果たし	H.Advanced	・組織は、契約事項からの逸配および、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれでついて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先さ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。	
				CPS.SC-5	なり、アストルマンス でいることを確認するために、監査、アスト結果、または他の形式の評価を使用して定期的に評価する	Advanced	・組織は、自組織が取引先との契約において要求事項として規定した内容に関連して、システム上での監査が可能かどうか、確認する。 ・上記で定義されているシステム上で監査可能なイベントのために、監査記録を生成する機能を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、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でレビュー・分析して、契約事項からの逸脱および、その充 彼の有無を経済する。 ・チェックリストを用いた取引先による内部監査により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。	
				CPS.IP-4	・構成要素(IoT機器、通信機器、回線等)に対し、定期的なシステムパックアップを実施し、テストしている	H.Advanced	・組織は、バックアップ情報を定期的にテストして、媒体の信頼性と情報の完全性を確認する。	
				CPS.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	H.Advanced	 最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的なモニタリング に用いられている活動の修正の必要性を判断する。 システムに、既知で害のないテストケースを導入して、マルウェア検知メカニズムをテストする。 ・組織は、侵入検知モニタリングに用いているメカニズムを定開的にテストする。テストの頻度は、組織が使用するツールの種類と、ツールの設置方法により変わる。 	
A.15 供給者関係	A.15.1 供給者関係における情報セ	A.15.1.1 供給者関係のための情報セ	組織の資産に対する供給者のアクセスに関連す るリスクを軽減するための情報セキュリティ要			Advanced	 組織は、セキュリティインシデントにより損害が発生する場合に備えて、取引先等から指定されるセキュリティ対策の実装に加え、サイバー保険の利用等によるリスク移転を検討する。 	
	共和省関係におり 3 情報で キュリティ		求事項について,供給者と合意し,文書化しな	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	Basic	・組織は、委託先あるいは委託元との契約において、業務においてセキュリティインシデントにより損害が発生した場合の自組織と取引先 の責任範囲(免責事項の明記、損害賠償額の契約金額等での上限設定等)を規定する。 ・組織は、契約において取引先に対応を求める/求められるセキュリティに関する要求事項の実効性を高めるため、要求事項への対応要否や 遠不足、具体的な対応方法や費用負担、対応できない場合の代替措置について契約時あるいは契約期間の初めに合意することが望ましい。	
			CPS.		・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	H.Advanced	・組織は、取引先(外部情報システムサービスのプロバイダ)に対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にする。	
						Advanced	・組織は、サプライチェーンに係るセキュリティ対策基準を参照して、ITT(Invitation To Tender)やRFP(Request For Proposal)などの入札 青翔を準備し、接在的な取引外に提供する。特に、入札書類には以下が含まれることが望ましい。 1) 調達する登風品またはサービスの仕様 2) 供給者が製品またはサービスの仕様 2) 供給者が製品またはサービスを供給している間に従うセキュリティ要件 3) 製品またはサービスの供給中に従うべきサービスレベルおよびその指標 4) セキュリティ要件に違反した場合に、委託元が繋する能性のもの場合を 5) 取引先の選定プロセス中に送信されるデータやシステムなどを保護するための秘密保持条項 ・組織は、取引先によるセキュリティ管理策の遵守状況を維持的にモニタリングするための、プロシージャを整備する。 ・取引先におりをセキュリティインラデントが自動能に影響した場合と備え、契約者につ外部事業者の責任分界点を明確にし、外部事業 者の責任部間において自組織に被害が発生した場合の損害賠償について記載する等の対応を行う。	
						Basic	・組織は、該当する法規制等を参照して、取引先(特に、自組織のデータを取り扱う可能性のある、またはデータを取り扱うための基盤を提供する可能性のあるものに対して適用するセキュリティ対策基準の策定に当たり、IPAによりISO/IEC 27001 附属書Aの管理策をベースに作成された「情報セキュリティベンチマーク」や、JASA(日本セキュリティ監査協会)「サプライチェーン情報セキュリティ管理基準」等を参考とすることが可能である。	
				・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・	H.Advanced	・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース(関係する他組織、とト、モノ、データ、システム等)と機能を特定し、優先層位付けずる。 ・取引先において、事業への悪影響を及ぼすセキュリティインシデントが発生した際の、自組織への影響の内容および、その起こりやすさ、規模を推定する。 ※関連する対策要件に、CPS.AM-6、CPS.BE-2等がある。		
				CPS.SC-2	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	Advanced	・組織は、自組織のミッション/業務プロセスに重要な影響を及ばしうるサプライチェーン上の取引先を特定し、当該組織が自組織のセキュ リティボリシーに規定されているセキュリティ上の役割と責任を果たせるかどうかを確認する。	
			・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	Basic	・組織は、長期に渡ってIoT機器が使用されることが想定される場合、長期間のサポートが期待できる取引先(機器ベンダ)を選定する。 ・組織は、機器のサポート終了時に機器を入れ替えることの要否についてシステムの導入前に取引先(機器ベンダ)に対して確認する。 ・組織は、取引先(サービスプロバイダー)の選定に当たり、JIS Q 2000のに基づくITSMS認証等を取得するか、あるいは自己適合確認により認証取得相当の対策の実装を確認しており、提供するITサービスのマネジメントを効率的、効果的に運営管理するサービスプロバイダーを選定することが望ましい。			
				CPS.MA-2	 ・自組織のIoT機器、サーバ等に対する適隔保守は、承認を得て、ログを記録し、不正アクセスを妨げる形で実施している 	H.Advanced		
			関連する全ての情報セキュリティ要求事項を確 立しなければならず、また、組織の情報に対し			H.Advanced	 ・組織は、取引先(外部情報システムサービスのプロバイダ)に対して、サービスの使用に必要な機能、ボート、プロトコル、および他のサービスを明確にする。 	

ISO/IEC 27001:2013 附属書	[‡] A	サイバー・フィジカル・セキュリティ対策フレームワーク				
管理策ID	要求事項	対策要件ID	対策要件		対策例	
キュリティの取扱い	て、アクセス、処理、保存若しくは通信を行う、又は組織の情報のための IT 基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意しなければならない。		・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	Advanced	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
				Basic	参の暫全部間において自日職に被称が条生した場合の期報賠償について記載する集の対抗を行う。 ・開職は、該当する法規制等を参照して、取引先代に、自租職のデータを収り扱う可能である。またはデータを取り扱うための基盤を提供する可能性のあるもの)に対して適用するセキュリティ対策基準を策定し、内容について合意する。 (参考) 取引先に対して適用するセキュリティ対策基準の策定に当たり、IPACよりISO/IEC 27001 附属権人の管理策をペースに作成された 「情報セキュリティペンチマーク」や、JASA(日本セキュリティ監査協会)「サプライチェーン情報セキュリティ管理基準」等を参考とする ことが可能である。	
			・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	H.Advanced	・組織は、あらかじめ優先して継栓・復旧すべき中原事業を特定しておき、当該事業を運用するにあたり機めて重要なリソース(関係する他 組織、とト、モノ、データ、システム等)と機能を特定し、優先順位付けする。 ・取引先において、事業への悪影響を及ぼすセキュリティインシデントが発生した際の、自組編への影響の内容および、その起こりやす さ、規模を推定する。 ※関連する対策要件に、CPS.AM-6、CPS.BE-2等がある。 ・組織は、自総のミッション/実券プロセスに重要な影響を及ぼしうるサプライチェーン上の取引先を特定し、当該組織が自組機のセキュ	
		CPS.SC-2	たして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	Advanced Basic	リティポリシーに規定されているセキュリティ上の役割と責任を果たせるかどうかを確認する。 ・組織は、長期に渡っている機能使用されることが想定される場合、長期間のサポートが期待できる取引先(機器ペンダ)を選定する。 ・組織は、機関のサポート終了時に機器を入れ替えることの要率についてシステムの乗り向に取引先(機器ペンダ)に対して確認する。 ・組織は、取引先(サービスプロバイダー)の選定に当たり、JIS Q 20000に基づくITSMS認証等を取得するか、あるいは自己適合確認により 認証収得自当の対策の実後を確認しており、提供するITサービスのマネジメントを効率的、効果的に運営管理するサービスプロバイダーを選定することが増生しい。	
				H.Advanced	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
		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	Advanced	る。 ・セキュリティ対策に関する要求事項 ・セキュリティ関連のドキュメントに関する要求事項 ・セキュリティ関連のドキュメントに関する要求事項 ・セキュリティ関連のドキュメントの保護に関する要求事項 ・秘密保持に関する表現 ・インシデントが発生した傷の報告先、報告内容、初動、調査、復旧等の各対応の実施主体、実施方法 ・自組織または認可された第二者によって監査され、定義されたセキュリティ要件への遵守を確認することを許可する条件 ・ 契約終了後の情報資産の扱い ・ 指摘は、取引先に対して、該当する法規制等に浮揚したセキュリティ要件への遵守を確認することを許可する条件 ・ 契約終了後の情報資産の扱い ・ 指摘は、取引先に対して、該当する法規制等に浮揚したセキュリティ要件への遵守を確認することを許可する条件 ・ 接続制等を参照してセキュリティ要件を決定し、取引先へ遵守を要求する。 ・ 法規制等を参照してセキュリティ要件を決定し、取引先へ遵守を要求する際、下記を事前に考慮することが望ましい。 ・ 自組織と取引先の間の法令の相違によって生じる潜在的法法的規制リスクの特定 ・ 取引性・ご報用された法律よりに関連しの指摘によって生じる潜在的法法的規制リスクの特定 ・ 取引性・ご報日よれた法律よりに関連しの指摘によって生じる潜在的法法的規制リスクの特定 ・ 取引性・ご報日まれた法律よりに関連して機能と、スターをリースの場合との	
				Basic	・組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施することを要求する。	
A.15.1.3 ICTサプライチェーン	供給者との合意には、情報通信技術 (ICT) サービス及び製品のサプライチェーンに関連す る情報セキュリティリスクに対処するための要			H.Advanced	・調達する機器に対して、契約におけるセキュリティ要求事務が満たせているわを、自組積あるいは第三者がラストする。 ・組積は、自組積のオペレーションにとって特に重要な機器について、再委託先以降の組積を含む関係するサプライチェーン全体に渡り、 一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロシージャで製造されたものかを確認する。	

ISO/II	EC 27001:2013 附属書	A .	サイバー・フィジカル・セキュリティ対策フレームワーク				
管理策ID		要求事項	対策要件ID	対策要件	対策例		
		※事項を含めなければならない。	CPS.SC-4	・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提供する製品・サービスが適合していることを確認する	Advanced	・組織は、契約において、例えば下記のように、取引先から調達する製品・サービスが具備すべきセキュリティ要求専項を明確化する。 ・セキュリティに関わる特定の認証(例:ISMS認証、ISASecure EDSA認証、ITセキュリティ評価及び認証制度(USEC))を有していること ・リスク分析の結果等から導かれた必要なセキュリティ要件を設計時からの実装(セキュリティ・バイ・デザイン)し、検査していること ・組織は、調達計画時に、製品またはサービス自体、あるいは当該製品・サービスの調達・供給にて使用される資産の保護に係るセキュリティ要件の費用を保住しておくことが望ましい。 ・下記を含む製品またはサービスの調達または供給を評価するためのセキュリティ測定ルールを策定し、運用および改善する。 ・測定対象の内容 ・措置が実施されない場合に遂行される措置 ・指摘は、搬送中の改さん・漏えいを検知(又は知止)する手段とともに納品されるIoT機器やソフトウェアが、不正操作されていないかを確認する。 ・物品:セキュリティ便、プロテクトシール等 ・電送:暗号化、電送データ全体のハッシュ値等	
A.15.2	A.15.2.1	組織は、供給者のサービス提供を定常的に監視			H.Advanced	・組織は、取引先(外部情報システムサービスのプロバイダ)に対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサー	
供給者のサービス提供の管理	供給者のサービス提供の監 視及びレビュー	し、レビューし、監査しなければならない。	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	Advanced	ビスを呼吸にする。 ・ 組織は、サプライチェーンに係るセキュリティ対策基準を参照して、ITT(Invitation To Tender)やRFP(Request For Proposal)などの入札 精類を推備し、潜在的な取引先に提供する。特に、入札書類には以下が含まれることが望ましい。 1) 調達する製品またはサービスの仕様 2) 供給者が製品またはサービスを供給している間に従うセキュリティ要件 3) 製品またはサービスを供給している間に従うセキュリティ要件 4) セキュリティ要件に違反した場合に、委託元が課す可能性のある罰則 5) 取引先の選定プロセス中に送信されるデータやシステムなどを保護するための秘密保持条項 ・ 組織は、取引先によるセキュリティ管理策の遵守状況を継続的にモニタリングするための、プロシージャを整備する。 ・ 取引先におけるセキュリティインシデントが自組職し影響した場合に備え、契約事に欠が部事業者との責任分界点を明確にし、外部事業者の責任範囲において自組職に被害が発生した場合の損害賠償について記載する等の対応を行う。	
		CPS.SC-5		・取引先等の関係する他組織が、契約上の義務を果たし CPS.SC-5 ていることを確認するために、監査、テスト結果、また は他の形式の評価を使用して定期的に評価する	H.Advanced	・組織は、契約事項からの逸脱および、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引免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最終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。	
			CPS.SC-5		Advanced	・組織は、自組織が取引先との契約において要求事項として規定した内容に関連して、システム上での監査が可能かどうか、確認する。 ・上記で定義されているシステム上で監査可能なイベントのために、監査記録を生成する機能を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開的にでレビュー・分析して、契約事項からの逸脱および、その充 彼の有無を確認する。 ・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。	
					H.Advanced	・組織は、遠隔保守のための接続の確立と実施に関するポリシーとプロシージャを文書化し、その内容により実施する。	
			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	Advanced	・組織は、実施した遠隔保守の実施記録を保管する。 ・組織は、遠隔保守を実施する際には組織の定めるネットワークアクセスに求める認証を実施するとともに、遠隔保守が完了したらセッ	
	A 15 0 0			している	Basic	ションとネットワーク接続を確実に終了する。 ・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。	
	A.15.2.2 供給者のサービス提供の変 更に対する管理	関連する業務情報、業務システム及び業務プロ セスの重要性、並びにリスクの再評価を考慮し て、供給者によるサービス提供の変更(現行の			H.Advanced	・組織は、外部階報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にするよう要求する。・組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。	
	情報セキュリティの方針群、手順及び管理策の 保守及び改善を含む。)を管理しなければなら ない。	CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サー ビスプロバイダとの通信内容をモニタリングする	Advanced	・組織は、外部サービスプロバイダおよびシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組職へ通知することを要求する。 ・組織は、関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を審审することが望ましい。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダーおよびシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組機のシステムへのアクセスをモニタリングする。 ・組織は、外部サービスプロバイダーおよびシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。		

ISO/IE	C 27001:2013 附属書A			th-	イバー・フィシ	ジカル・セキュリティ対策フレームワーク
管理策ID		要求事項	対策要件ID	対策要件		対策例
A.16 情報セキュリティインシデ ント管理 ントで管理及びその改善	A.16.1.1 責任及び手順	情報セキュリティインシデントに対する迅速, 効果的かつ順序だった対応を確実にするため に, 管理層の責任及び手順を確立しなければな らない。		セキュリティ運用マニュアルにおいて、取引先等の関係	H.Advanced	・組織は、サブ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、自組織とサブライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、インシデント対応実件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。 (参考)サブ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、システムコンボーネント、IT 製品、開発プロセスまたは開発
			CPS.RP-2	する他組織との連携について手順と役割分担を定め、選 用する	Advanced Basic	者、流過過程または金庫施設に対する侵害等がある。 ・組織は、セキュリティインシデントにより第1の処理拠点の可用性が低下した場合に利用する代替処理拠点を定める。 ・組織は、自組織の一次処理機能が利用できない場合と、自組織が定める目標復旧時間内に、代替処理拠点により所定のオペレーションを移転・再開して、重要なミッション/業務機能を遂行できるようにするようサービス契約で規定する。 ・組織は、同じ脅威に対する服勢さを減らすために、一次処理拠点から離れた代替処理拠点を指定する。 ・組織は、ジステムのユーザにセキュリティインシデントの対応と報告に関する助言と支援を提供する、組織のインシデント対応能力に不可欠な、インシデント対応支援リソース(ヘルプデスク、CSIRT等)を自組織に用意する。 ・対処の必要なセキュリティインシデントを発見した場合、透やかにIPA、JPCERT/CC等の関係機関に報告し、対応の支援、発生状況の把
	A.16.1.2	情報セキュリティ事象は,適切な管理者への連			Dasic	握、手口の分析、再発防止のための助言等を受ける。 ・組織は、委託先の要員により委託元が要求するセキュリティ要求事項が遵守されているかどうかを継続的にモニタリングし、通常とは異
		絡経路を通して、できるだけ速やかに報告しな			H.Advanced	なる行動があった場合、自組織の担当者に通知できるようにプロシージャを整備する。
7	告	ければならない。	CPS.SC-8	・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	Advanced	 サブライヤー関係のセキュリティ面について該当する要員を訓練し、機密情報の取り扱いが正しく理解されていることを特に確認する。 委託業務の遂行に当たり、委託元が要求するセキュリティ要求事項が遵守されていることを定期的に確認する。
				を行う	Basic	・委託業務に係るデータの内、機密データや知的制産のように、公開または変更すべきではないものへのアクセスおよびデータの開示または変更に関わる要負を特定し、評価する。 ・組織は、委託先との契約の終了後、遂やかに委託先の要員に対する自組織施設へのアクセス権限等の、一時的に許可していた権限を停止する。 ・組織は、ザブ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
			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	H.Advanced	で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、インシデント対応要件が満たされるよう、自組機のインシデント対応プロセスと、自組機の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。 [参考]サプライチェーンにおけるセキュリティインシデントには、たとえば、システムコンボーネント、IT 製品、開発プロセスまたは開発
					Advanced	書、洒湯総官または倉庫施院に対する侵害等がある。 ・組織は、セキュリティインシデントにより第二の地関島点の可用性が低下した場合に利用する代替処理拠点を定める。 ・組織は、自組織の一次処理機能が利用できない場合に、自組織が定める目標後旧時間内に、代替処理拠点により所定のオペレーションを移転・再開して、重要なミッション/業務機能を遂行できるようにするようサービス契約で規定する。 ・組織は、同じ脅威に対する能弱さを減らすために、一次処理拠点から離れた代替処理拠点を指定する。 ・組織は、同じ脅威に対する能弱さを減らすために、一次処理拠点が適性ん代替処理拠点を指定する。 ・組織は、システムのユーザにセキュリティインシデントの対応と報告に関する助言と支援を提供する、組織のインシデント対応能力に不可欠な、インシデント対応支援リソース(ヘルプデスク、CSIRT等)を自組織に用意さる。
					Basic	・対処の必要なセキュリティインシデントを発見した場合、速やかにIPA、JPCERT/CC等の関係機関に報告し、対応の支援、発生状況の把握、手口の分析、再発防止のための助言等を受ける。
	A.16.1.3 相綴の情報システム及びサービスを利用する従業員及び契約相手に、システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は、どのようなものでも記録し、報告するように要求しなければならない。 情報セキュリティ事象の評価及び決定 情報セキュリティインシデントに分類するか否かを決定しなければならない。			H.Advanced	・組織は、あらかじめ後先して無終・彼旧けべき中核事業を特定しておき、当該非業を選用するにあたり機构で重要なリソース(関係する他組織、ヒト、モノ、データ、システム等)と機能を特定し、優先順位付けする。 ※CPS.AM-6、CPS.BE-2に同様の対策例を記載・ 組織は、セキュリティインシデントの追踪と、インシデントに関係する脅威収集、後続性等の情報の収集および分析を支援する自動化されたメカニズムを使用して、セキュリティインシデントの分類(トリアージ)等に活用する。	
				・検知されたセキュリティインシデントの情報は、セ キュリティに関する影響度の大小や侵入経路等で分類 し、保管する	Advanced	ンジデントを分類する。 ・組織は、自組織に影響を及ばすセキュリティインシデントを追跡し、文書化する。 "SP 800-61 rex.1" では、セキュリティインシデントを文書化する際の記載の観点として、下記を例示している。 ・インシデントの規模 ・当該インシデントに対して自組織のとった行動の内容 ・ほかの関係者(システム所有者、システム管理者等)の連絡先情報 ・調査の際に収集した証拠の一覧 ・インシデントの処理担当者からのコメント ・次にとるときネラ・ツ
					Basic	・当該セキュリティインシデントのもたらす影響の大きさを考慮し、報告義務のあるインシデントを定める。 [参考]セキュリティインシデントの影響の大きさを測るための尺度を検討する場合、下記文書等を参照することができる。 ・"SP 800-61 rex1"(NIST, 2008年) 32.6 単年の優先報位付け ・"サイバー攻撃による重要インフラサービス障害等の運剣度評価基準"(NISC, 2018年)
t		セキュリティインシデントに分類するか否かを			H.Advanced	 組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース(関係する他組織、ヒト、モノ、データ、システム等)と機能を特定し、優先原位付けする。 ※CPSAM-6、CPS.BE-Zに同様の対策例を記載・組織は、セキュリティインシデントの追跡と、インシデントに関係する脅威収集・脆弱性等の情報の収集および分析を支援する自動化されたメカニズムを使用して、セキュリティインシデントの分類(トリアージ)等に活用する。
			CPS.AE-5	・セキュリティ事象の危険度の判定基準を定める	Advanced	 組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位、およびメトリクスを考慮してインシデントを分類する。

ISO/I	EC 27001:2013 附属書/	A		th-	イバー・フィシ	ジカル・セキュリティ対策フレームワーク	
管理策ID		要求事項	対策要件ID	対策要件	対策例		
					Basic	 - 当該セキュリティインシデントのもたらす影響の大きさを考慮し、報告義務のあるインシデントを定める。 [参考]セキュリティインシデントの影響の大きさを測るための尺度を検討する場合、下記文書等を参照することができる。 **SP 800-61 rev.1*(NIST, 2008年) 3.2.6 事件の優先帳位付け *サイバー攻撃による重要インフラサービス障害等の深刻度評価基準*(NISC, 2018年) 	
					H.Advanced	・組織は、あらかじめ優先して継続・復旧すべき中株事業を特定しておき、当該事業を運用するにあたり場かて重要なリソース(関係する他組織、ヒト、モノ、データ、システム等)と概能を特定し、優先原位付ける。 ※CPSAM-6、CPS.BE-2に同様の対策例を記載・組織は、セキュリティインシデントの追跡と、インシデントに関係する脅威収集・脆労性等の情報の収集および分析を支援する自動化されたメカニズムを使用して、セキュリティインシデントの分類(トリアーグ)等に活用する。	
			CPS.AN-3	・検知されたセキュリティインシデントの情報は、セ キュリティに関する影響度の大小や侵入経路等で分類 し、保管する	Advanced	 ・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位、およびメトリクスを考慮してインシデントを分類する。 ・組織は、自組織に影響を及ぼすセキュリティインシデントを追跡し、文書化する。 ・おおいた。 ・おいた。 ・・おいた。 ・・おいた。 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
					Basic	 - 当該性セュリティインシデントのもたらす影響の大きさを考慮し、報告義務のあるインシデントを定める。 [参考]セキュリティインシデントの影響の大きさを測るための尺度を検討する場合、下記文書等を参照することができる。 **SP 800-61 rev.1"(NIST, 2008年)、3.2.6 事件の優先順位付け *サイバー攻撃による重要インフラサービス障害等の深刻度評価基準"(NISC, 2018年) 	
	A.16.1.5 情報セキュリティインシデ ントへの対応	情報セキュリティインシデントは、文書化した デ 手順に従って対応しなければならない。			H.Advanced	・組織は、委託先の要員により委託元が要求するセキュリティ要求事項が遵守されているかどうかを継続的にモニタリングし、通常とは異なる行動があった場合、自組織の担当者に適知できるようにプロシージャを整備する。	
	2 1.402390		CPS.SC-8	・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	Advanced	 サプライヤー関係のセキュリティ面について該当する要員を訓練し、機密情報の取り扱いが正しく理解されていることを特に確認する。 委託業務の遂行に当たり、委託元が要求するセキュリティ要求事項が遵守されていることを定期的に確認する。 	
				2117	Basic	- 委託集務に係るデータの内、機密データや知的財産のように、公開または変更すべきではないものへのアクセスおよびデータの開示また は変更に関わる要員を特定し、評価する。 ・組織は、委託先との契約の終了後、速やかに委託先の要員に対する自組織施設へのアクセス権限等の、一時的に許可していた権限を停止 する。	
			CPS.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	H.Advanced	・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。	
				な対応を実施する	Advanced	・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ったことを検知した場合には、インシデントの把握・影響の拡大防止策を 実施する。 ・組織は、発生したインシデントに関して慣例責任者・関係部署・関係組織への連絡するとともに、証拠や記録等を保全する。	
					H.Advanced	・組織は、セキュリティ専門の24時間365日モニタリングモニタリングにより収集した監査ログを、分析自動化ツール等を利用することで効率的に分析する。 ・組織は、従来のIT環境だけでなく、制御ンステムやIoT機器も含めて、セキュリティ状況のモニタリングの範囲とすることが望ましい。 ・組織は、従来のIT環境だけでなく、制御ンステムやIoT機器も含めて、セキュリティ状況のモニタリングの範囲とすることが望ましい。 ・組織は、セキュリティ対応組織の成熟度を定期的に評価し、セキュリティ状況のモニタリングやインシデントへの対応等のセキュリティ関連業務を継続的に改善することが望ましい。 「参考]セキュリティ対策組織(SOC/CSIRT)を評価するためのメトリクスには、"セキュリティ対応組織成熟度セルフチェックシート"(ISOG-J, 2018年)や、SIM3(Security Incident Management Maturity Model)等がある。	
			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	Advanced	・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。 ・モニタリングするシステムの範囲をどこまでとするか ・どのような機器のログを収集し、分析するか(CPS AC-3を参照) ・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、資産情報、機器の構成情報、ネットワーク構成情報を経統的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、資産情報、機器の構成情報、ネットワーク構成情報を経統的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、資産情報、機能の構成情報、ネットワーク構成情報を経統的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、資産情報、機能の構成情報、ネットワーク構成情報を経験的に収集・管理し、定期的に報告する。報告内容にびい、対応を実施する。プロセスの和容については、CPS RP-1等を参照・ ・組織は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。報告内容にして記念合むことが望ましい。 ・ログ分析の分析結果(対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等) ・モニタリングにおける今後の改善方計 「参考]セキュリティ対策組織(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。	
					H.Advanced	・システムは、10T機器、サーバ等に異常(調動作等)が発生した場合に、緊急停止、管理者へのアラート通知等のフェールセーフのための対 応を実践する。 ・システムは、有効でないインブットデータを受け取った場合に、組織の目的とシステムの目的に沿って、予想できる形で、かつ記載どおり に動作する。	

ISO/I	EC 27001:2013 附属書A			th-	イバー・フィシ	プカル・セキュリティ対策フレームワーク
管理策ID		要求事項	対策要件ID	対策要件		対策例
				・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	Advanced	・組織は、セキュリティ運用マニュアルにおいてインシデントの検知および分析、封じ込め、低減、復旧を含む内容を規定する。 ・インシデントの報告を受けた者が、どのような判断で対応をするのか、あるいはより上位に報告するのか、の判断基準を明確にしておく ・すべてのインシデントの取り扱いに関する記録をとる ・外部組織等に対して、インシデント発生の事実と対応状況に関する報告をする必要があるかどうかを判断する
			CPS.RP-1	ロセスを定め、適用する ・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	Basic	・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選用プロセスを策定し、選用する。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。 - 緊急時の指揮命令と対応の優先順位の決定 - インシデントのの対応(インシデントレスポンス) - インシデントの影響と被害の分析 - 情報収集と自社に必要な情報の選別 - 社内関係者への連絡と周知 - 外部関係機関との連絡 (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"(IPCERT/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"(IPCERT/CC, 2015年)を参照することが可能である。
			CPS.MI-1	・セキュリティインシデントによる被害の拡大を最小限 に抑え、影響を低減する対応を行う	H.Advanced	・組織は、セキュリティインシデントの対応プロセスを支援する自動化されたメカニズムを使用する。 ・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。 「参考対対応段階におけるインシデントの影響低減、復旧段階において有用に機能すると考えられる情報の例として、"セキュリティ対応組織(SOC,CSIRT)強化に向けたサイバーセキュリティ構築共有の「FWHH」v1.0"(ISOG-J, 2017年)では、下記が挙げられる。 ・攻撃行為をセキュリティ製品や関連するシステムで遮断するための設定要件 ・攻撃を無効化する方法(バッチの適用、設定変更等) ・被害を受けたシステム復旧方法
					Basic	・組織(あるいはその構成員)は、あらかじめ定められたプロシージャに従って、セキュリティインシデントを低減するためのアクション(たとえば、システムのシャットダウン、有線/無線ネットワークからの切断、モデムケーブルの切断、特定の機能の無効化など)を実行する。 [参考]セキュリティインシデントの影響低減のための活動は、インシデントの性質(例えば、サービス担否攻撃、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別)により内容が異なる場合がある。より評細な影響を滅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」(PICERT/CC, 2015年)、"SP 800-61 rev.1"(NIST, 2008年)等を参照することが望ましい。
	A.16.1.6	情報セキュリティインシデントの分析及び解決			H.Advanced	・組織は、第三者によるセキュリティ評価を実施する。
	情報セキュリティインシデ ントからの学習			・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	Advanced	・組織は、セキュリティ評価を適切に、かつ、計画的に実施するため、以下に示す事項を含めたセキュリティ評価計画を策定した上で、セキュリティ評価を実施する。 ・セキュリティド語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 ・セキュリティ評価を実施する環境と実施体制 ・セキュリティ評価結果の取りまとめ方法とその活用方法
					Basic	・組織は、セキュリティ対策が正しく実装されているか及び運用されているかに加え、セキュリティ対策が期待された成果を上げているかに 関する定期的に評価(セキュリティ評価)を実施し、管理責任者へ報告する。 ・組織は、セキュリティ評価の結果に基づき、セキュリティ対策の改善を実施する。
					H.Advanced	・組閥は、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通切なパートナーと 適時双方向で共有をすることができる環境を整備する。
			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	Advanced	・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、パートナーに適時共有することができる環境を整備する。
					Basic	・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、適切なパートナーから入手できる環境を整備する。
			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	H.Advanced	・ハザードのエネルギー等を下げて事故が起きても影響を小さくするように設計する等、本質安全設計を適じて、影響度の高いハザードに対処することで、被害を極小化する。
			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	H.Advanced	・相關は、発生したセキュリティインシデントの形態、規模及び費用を定置化及び監視できるようにする自動的なメカニズムを備える。 ・相關は、発生もスリティインシデント発生等において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を自組機のセキュリティ対応相議(SOC/CSIRT)にて実施する。 ・相関は、攻撃者のプロファイル (所属阻服、組織の活動目的など) に関する仮設を構築する。 「参考 被数のシステムが連携する"System of Systems"が構築されている環境においては、セキュリティインシデントの影響評価はより困難なものになることが想定される。当該領域における条件的な試みである"Internet of Things(IoT) インシデントの影響評価に関する考察(一般社団法人日本クラウドセキュリティアライアンス、2016年)では、デバイスの特性、サービスの特性、デバイス数により影響度を評価する試みがなされている。

	ISO/I	EC 27001:2013 附属書/	4		#-	イバー・フィミ	ジカル・セキュリティ対策フレームワーク
	管理策ID		要求事項	対策要件ID	対策要件		対策例
						H.Advanced	 ・組織は、検知能力向上のため、様々な情報ソースをもとに、検知ルールの作成とチューニングを行う ・自服分析ルールの開発 ・IPS/IOSの独自シグネチャの開発 ・独自ブラックリストの開発 ・組織システムは、システムの通信やセキュリティアラートのパターンを分析し、典型的な通信パターンおよびセキュリティアラートを集的したプロファイルを作成、活用することで、誤検出の数や、検出漏れの数を減らすためのチューニングを行う。
				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	Advanced	・組織は、経営層等の組織内の然るべき要員に、定開的に組織およびシステムのセキュリティの状態を報告するプロシージャを整備し、選用する。組織は、報告の場を最新の脅威や残存するリスクに対する脅威を認識し、セキュリティを向上するための場とすることが望ましい。 ・例えば下記のような注意喚起情報の発応があった際等に、セキュリティに係らリスク増加の光候がある場合、信頼できる情報版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ンルを上げる。 米下記のリストは、"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-), 2017年)より引用している。 ・ 攻撃の特徴 攻撃の特徴 ン 攻撃形態、関連する通信の内容 ・ 大板心となる攻撃コード ・ 攻撃によって残る顕静 ・ 被害を受けた後の通信内容 ・ サーバやクライアントに残る日グ ・ サーバやクライアントに残る日グ ・ サーバやクライアントに残る日の特徴 ・ 各セキュリティ製品における検知名
				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	H.Advanced	・システムは、発生したセキュリティインシデントの形態、規模及び費用を定量化及び監視できるようにする自動的なメカニズムを備える。 ・組織は、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監置したプログラムやスクリプトが発見された場合、それらの 機能の解析を自組織のセキュリティ対応組織(SOC/CSIRT)にて実施する。 ・組織は、攻撃者のプロファイル(所属組織、担縁の活動目的など)に関する仮設を構築する。 ・組織は、攻撃者のプロファイル(所属組織、担縁の活動目的など)に関する仮設を構築する。 (参判複数のシステムが連携する"System of Systems"が構築されている環境においては、セキュリティインシデントの影響評価はより困難 なものになることが態定される。 並動機能に対ける条件的な起かである"Internet of Things(loT)インシデントの影響評価に関する事業"(一般 社団法人日本クラウドセキュリティアライアンス、2016年)では、デバイスの特性、サービスの特性、デバイス数により影響度を評価する試 みがなされている。
						H.Advanced	・システムが、発生したセキュリティインシデントの形態。規模及び費用を定量化及び監視できるようにする自動的なメカニズムを備えることが望ましい。
				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	Basic	・セキュリティインシデントの評価から得た脅威情報、脆弱性情報等は、再発する又は影響の大きいインシデントを特定するために利用する ことが望ましい。 ・セキュリティインシデントへの対応活動から学んだ教訓を事業継続計画又はコンティンジェンシープラン、教育/訓練に取り入れて、結果 として必要となる変更を実施する。NIST SP 800-61には、教訓を抽出する際の観点として下記が例として示されている。 - 正確に何がいつ起きたか。 - スタッフとマネジメント層がどの程度うまく事件に対処したか。文書化された手順に従ったか。それは適切だったか。 - すぐに必要になった情報は何か。 - 復旧を妨げたわもしれないステップや行動があったか。 - 次に同様の事件が起きた場合、スタッフやマネジメント層は、どのような違った行動をとるか。 - どのような是正推置があれば、将来にわたって同じ様な事件が起きるのを防げるか。 - 将来事件を検出、分析、軽減するために、どのようなツールやリソースが追加で必要となるか。
		A.16.1.7	組織は、証拠となり得る情報の特定、収集、取			H.Advanced	・システムが、重要なセキュリティインシデントに関する監査記録について処理するプロシージャを提供する。
		証拠の収集	得及び保存のための手順を定め、適用しなければならない。	CPS.AN-2	・セキュリティインシデント発生後に、デジタルフォレ ンジックを実施する	Advanced	・組織は、媒体、装置及び装置の状態(例えば、電源が入っているか、切れているか)に従って、証拠の特定、収集、取得及び保存のプロシージャを規定する ・組織は、重要なセキュリティインシデントについて、発生後に下記の証跡を保全することが望ましい。 ・説別情報(インシデントの発生場所/発生日時/対象となるモノのシリアル番号/ホスト名/MACアドレス/IPアドレス等) - 証跡を収集・処理したヒトの役職、名前、連絡先 - 証跡保全処理の日時(タイムゾーンを含む)
						Basic	・組織は、証拠となり得るデータを特定、収集、取得及び保存するためのプロシージャを定め、運用する。
A.17 事業継続マネジメントにお ける情報セキュリティの側 面	A.17.1 情報セキュリティ継続	A.17.1.1 情報セキュリティ継続の計 画	組織は、困難な状況 (adverse situation) (例 えば、危機又は災害) における、情報セキュリ ティ及び情報セキュリティマネジメントの継続 のための要求事項を決定しなければならない。	CPS.RP-3	・自然災害時における対応方針および対応手順を定めて いる事業継続計画又は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	Advanced	 組織は、災害等と比較して被害状況が見えづらく事業継続計画の発動タイミングが不明確、インシデントの原因究明の重要性が高い等の特徴を有するセキュリティインシデントに特化した事業継続計画又はコンティンジェンシーブランを策定し、運用する。 組織は、セキュリティインシデントに特化した事業継続計画又はコンティンジェンシーブランを策定する際、組織全体の事業継続に係る方針と合致するような内容とすることを確実にする。
				CPS.RP-4	・セキュリティ事象発生時に被害を受けた設備にて生産 される等して、何らかの品質上の欠落が生じていること が予想されるモノ(製品)に対して適切な対応を行う	Advanced	 組織は、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。 組織は、サプライチェーンに関与する外部関係者との間で、復旧活動およびインシデントの事後処理に関わる活動を調整する。その際、CPS AM・3C で記載し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。 ・自組織の業権を考集して、事業継続計画又はコンティンジェンシーブランの中に、インシデント身生後の生産したモノへの対応について
					ガ. L.W.G41vの 正人(祭印)に対して週刊な対心を行う	Basic	工能能するかを検討する。その際、事業継続計画又はコンティンジェンシープランは、必ずしもセキュリティインシデントを想定したものでない場合も許容されるものとする。

	ISO/II	EC 27001:2013 附属書	4		у -	イバー・フィシ	ジカル・セキュリティ対策フレームワーク
	管理策ID		要求事項	対策要件ID	対策要件		対策例
		A.17.1.2 情報セキュリティ継続の実 施	組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持しなければならない。	CPS.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係 する他組織との連携について手順と役割分担を定め、運	H.Advanced	 ・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、インシデント対応労力セスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。 (参考)サプライチェーンにおけるセキュリティインシデントには、たとえば、システムコンボーネント、IT 製品、開発プロセスまたは開発者、流過過程または倉庫施設に対する侵害等がある。
					用する	Advanced	・組織は、セキュリティインシデントにより第1の処理拠点の可用性が低下した場合に利用する代替処理拠点を定める。 ・組織は、自組織の一次処理機能が判用できない場合に、自組織が定める目標使旧時間内に、代替処理拠点により所定のオペレーションを移転・再開して、重要なミッション/業務機能を遂行できるようにするようアレビス契約で規定する。 ・組織は、同じ脅威に対する能勢を減らすために、一次処理拠点から離れた代替処理拠点を指定する。 ・組織は、システムのユーザにセキュリティインシデントの対応と報告に関する助言と支援を提供する、組織のインシデント対応能力に不可欠な、インシデント対応支援リソース(ヘルプデスク、CSIRT等)を自組織に用意する。
				CPS.CO-3	・復旧活動について内部および外部の利害関係者と役 員、そして経営陣に伝達する点を、事業継続計画又はコ	Advanced	・組織は、監督官庁、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。 ・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動およびインシデントの事後処理に関わる活動を調整する。ここで該当する活動の例として、生産システムにおけるセキュリティインシデント発生時に生産されたモノの回収等が挙げられる。
					ンティンジェンシープランの中に位置づける	Basic	・組織は、自組織に影響を及ばすようなセキュリティインシデント発生時における役割、責任、そうした役割と責任を割り当てられたヒトと連絡先情報を示す。 ・組織は、事業継続に関わる意思決定の責任が割り当てられたヒトに対して、意思決定をより適切なものとするため、セキュリティインシデントの概要や被害状況に関する説明を実施する。
		A.17.1.3 情報セキュリティ継続の検 証, レビュー及び評価	確立及び実施した情報セキュリティ継続のため の管理策が、困難な状況の下で妥当かつ有効で なことを確実にするために、組織は、定めら れた間隔でこれらの管理策を検証しなければな らない。	CPS.IM-2	・セキュリティインシデントへの対応から教訓を導き出 し、事業継続計画又はコンティンジェンシープランを継 続的に改善する	Basic	 ・組織は、セキュリティインシデントへの対応から、事業継続のためのプロシージャおよび関連する対策の機能が、事業継続のより上位の 方針と合致しているかを確認する。 ・セキュリティインシデントへの対応活動から学んだ教訓を事業継続計画又は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。
	A.17.2 冗長性	A.17.2.1 情報処理施設の可用性	情報処理施設は、可用性の要求事項を満たすの に十分な冗長性をもって、導入しなければなら ない。	CPS.DS-5	・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	Advanced	・システムは、組織が定めたセキュリティ対策を実施することによって、組織が定めたタイプのサービス拒否攻撃、またはそうした情報の情報派への参照のサービス拒否攻撃による影響を最小限に抑える。 ・システムは、予備の容量/帯域幅/その他の予備を管理して、大量の情報を送りつけるタイプのサービス拒否攻撃による影響を最小限に抑える。 ・要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測しなければならない。 ・組織は、 (3)情報システムに対するサービス妨害攻撃の完候を発見するための組織が定めた、モニタリングツールを使用する (5)組織が定め行情報システムリソースをモニタリングして、効果的なサービス妨害攻撃を阻止するための十分なリソースが確保されているかどうかを判断する。
						Basic	・システムは、組織が定めたセキュリティ対策を実施することによって、組織が定めたタイプのサービス拒否攻撃、またはそうした情報の情報源への参照のサービス拒否攻撃による影響から保護する。あるいはそうした影響を暴小隊に抑える。
				CPS.DS-6	・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、交換性業、ソフトウェアの更新を行う	Advanced	・要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、特未必要とする容量・能力を予測する。 ・
					AN AMIRAN 771 7+1-7-2-816117	Basic	・要求されたングアム性能を満たす。ことを集美にするために、資源の利用を高便・調整しなければならす。また、有来必要とする容重・能力 を予測する。 ・装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。 ・データを伝送する又は情報サービスをサポートする適信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。 ・装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。
A.18 順守	A.18.1 法的及び契約上の要求事項 の順守	A.18.1.1 適用法令及び契約上の要求 事項の特定	各情報システム及び組織について、全ての関連 する法令、規制及び契約上の要求事項、並びに これらの要求事項を満たすための組織の取組み を、明確に特定し、文書化し、また、最新に保 たなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令 や、業界のガイドラインを考慮した社内ルールを策定 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	Basic	・自組織の事業活動において、セキュリティの文脈で関連するすべての法令、規制及び契約上の要求事項、並びにこれらの要求事項を満た すための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。 ・要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文書化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全ての国における遵守を考慮する。 ・参考」情報セキュリティ関連法令には例えば、不正競争防止法、電子署名認証法、e・文書法、個人情報保護法、不正アクセス禁止法等がある。
				CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに 関する取決め等によって要求されるデータの保護の水準 を的確に把握し、それぞれの要求を踏まえたデータの区 分方法を整備し、ライフサイクル全体に渡って区分に応 じた適切なデータの保護を行う	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの受案事項に従い、送当するデータを扱うシステム、モノ等に対策を実施する。対策の実験が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例:割賦販売法におけるカード情報の非保持化)

	ISO/IEC 27001:2013 附属書A	1		# -	イバー・フィシ	プカル・セキュリティ対策フレームワーク
管理第	策ID	要求事項	対策要件ID	対策要件		対策例
			CPS.DP-2	・監視業務では、地域毎に適用される法令、適達や業界 標準等に準拠して、セキュリティ事象を検知する	Basic	 ・組織は、モニタリング業務に関係する法制度、業界標準、顧客との契約事項等が存在するか、存在するならばどのような制約があるかを認識する。 ・組織は、上記で認識したルールに準拠してモニタリングを実施し、セキュリティインシデントを検知する。 ・組織は、自組織のモニタリング活動がルールに準拠したものかどうかを定期的にレビューし、確認する。
	知的財産権	知的財産権及び権利関係のあるソフトウェア製品の利用に関連する,法令,規制及び契約上の要求事項の順守を確実にするための適切な手順を実施しなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令 や、業界のガイドラインを考慮した社内ルールを策定 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	Basic	・ 自脳腺の事業活動において、セキュリティの文脈で関連するすべての法令、規制及び契約上の要求事項、並びにこれらの要求事項を満た すための組織の取組みを、明確に特定し、文書化し、また、最新に保っ。 ・要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文書化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全ての国における遵守を考慮する。 「多考」情報セキュリティ関連法令には例えば、不正競争防止法、電子署名認証法、e・文書法、個人情報保護法、不正アクセス禁止法等がある。
			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	Basic	- 組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを識別、文書化し、最新に保つ。 - 組織は、議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: 割減販売法におけるカード情報の非保持代)
	記録の保護	記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改さん、認可されていないアクセス及び不正な流出から保護しなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令 や、業界のガイドラインを考慮した社内ルールを策定 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	Basic	・自路機の事業活動において、セキュリティの交換で関連するすべての法令、規制及び契約上の要求事項、並びにこれらの要求事項を満た すための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。 要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文章化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全での国における遵守を考慮する。 「参考」情報セキュリティ関連法令には例えば、不正競争防止法、電子署名認証法、e・文書法、個人情報保護法、不正アクセス禁止法等があ る。
			CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに 関する取決め等によって要求されるデータの保護の水準 を的確に把握し、それぞれの要求を踏まえたデータの区 分方法を整備し、ライフサイクル全体に渡って区分に応 じた適切なデータの保護を行う	Basic	・組織は、各システム及が組織について、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、競場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)
				・自組織が関係する他組織との契約上の義務を果たして	H.Advanced	・組織は、取引先、第三者的な監査機関等の関係する他組織からのリアルタイムでのニーズに柔軟に応じるため、下記の特徴を有した証跡保 管システムを利用する。 ・対象となる甚至証帥の契約事項に対する適格性を高速で検証することができる ・取引先や委託を受けた監査機関等の許可を受けたエンティティのみがアクセスできる ・保管されているデータが、タイムスタンプや電子署名により証跡としての信頼性を有している
			CPS.SC-7	いることを証明するための情報(データ)を収集、安全に 保管し、必要に応じて適当な範囲で開示できるようにす る	Advanced	・組織は、システムによって生成された監査記録のうち長期にわたって取得する監査記録を確実に取得できるよう、対策を実施する。 ・システムは、監査記録を次の脅威から保護するため、粒度の高いアクセス制御等を監査記録を保存するモノ、システムに適用することが望ましい。 ・記録されたメッセージ形式の変更 - ログファイルの変更又は削除 - ログファイル媒体の記録容量超過
					Basic	・組織は、法規制等により要求される事項を満たす事ができるよう、適切な期間の監査記録を保持する。
			00010	・構成要素(IoT機器、通信機器、回線等)に対し、定期的	H.Advanced	・組織は、バックアップ情報を定期的にテストして、媒体の信頼性と情報の完全性を確認する。
			CPS.IP-4	なシステムバックアップを実施し、テストしている	Advanced	・組織は、自組織のシステムドキュメントのバックアップを変めたタイミングや観度で実施する。 ・組織は、保管拠点におけるバックアップ情報の機密性・完全性・可用性を保護する。 ・自組織の事業活動において、セキュリティの支援で関連するすべての法令、限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。
	ブライバシー及び個人を特	ブライバシー及び PII の保護は、関連する法令 及び規制が適用される場合には、その要求に 従って確実にしなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令 や、業界のガイドラインを考慮した社内ルールを策定 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	Basic	・自信服の事業活動において、ゼキュリアイの人歌で関連するすべての法令、売助及び契約上の要求事項、並びにこれらの要求事項を満た すための組織の歌剧をも、明確に特定し、文書化し、また、豊新に保つ。 ・要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文書化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全での国における遵守を考慮する。 「参考」情報セキュリティ関連法令には例えば、不正競争防止法、電子署名認証法、e・文書法、個人情報保護法、不正アクセス禁止法等がある。
			CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに 関する取決め等によって要求されるデータの保護の水準 を的確に把握し、それぞれの要求を踏まえたデータの区 分方法を整備し、ライフサイクル全体に渡って区分に応 じた適切なデータの保護を行う	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを造別、文書化し、無緒に保つ。 ・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、鼓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)
		暗号化機能は、関連する全ての協定、法令及び 規制を順守して用いなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令 や、業界のガイドラインを考慮した社内ルールを策定 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	Basic	・自組織の事業活動において、セキュリティの文庫で関連するすべての法令、規制及び契約上の要求事項、並びにこれらの要求事項を満た すための組織の敗組みを、明確に特定し、文書化し、また、最新に保つ。 ・要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文書化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全ての国における遵守を考慮する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全ての国における遵守を考慮する。 参考]情報セキュリティ関連法令には例えば、不正競争防止法、電子署名認証法、e・文書法、個人情報保護法、不正アクセス禁止法等がある。

ISO/IEC 27001:2013 附属書	‡A		サイバー・フィジカル・セキュリティ対策フレームワーク				
管理策ID	管理策ID 要求事項			対策例			
		CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに 関する取決め等によって要求されるデータの保護の水準 を的確に把握し、それぞれの要求を踏まえたデータの区 分方法を整備し、ライフサイクル全体に渡って区分に応 した適切なデータの保護を行う	Basic	 組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取扱みを認め、実験には、銀統に保つ。 組織は、識別したルールの労疫に従い、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。対策の実験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: 割減販売法におけるカード情報の非保持化) 		
A.18.2 情報セキュリティのレ ピュー たレビュー	情報セキュリティ及びその実施の管理(例え 」ば、情報セキュリティのための管理目的、管理 策、方針、プロセス、手順)に対する組織の取 組みについて、あらかじめ定めた間隔で、又は 重大な変化が生じた場合に、独立したレビュー を実施しなければならない。	CPS.IP-7	・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視/測定/評価結果から教訓を導き出し、資産を保護するプロセスを改善している	H.Advanced Advanced Basic	・組織は、第三者によるセキュリティ評価を実施する。 ・組織は、セキュリティ評価を選択に、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を策定した上で、セキュリティ評価を実施する。 ・セキュリティ評価を実施する。 ・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表向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 ・組織は、セキュリティ対策が正しく実験されているか及び選用されているかに加え、セキュリティ対策が開待された成果を上げているかに 関する定期的に評価(セキュリティ評価)を実施し、管理責任者へ報告する。 ・組織は、セキュリティ評価(セキュリティ評価)を実施し、管理責任者へ報告する。		
A.18.2.2 情報セキュリティのためら 方針群及び標準の順守	管理者は、自分の責任の範囲内における情報処) 理及び手順が、適切な情報セキュリティのため の方針群、標準類、及び他の全てのセキュリ ティ要求事項を順守していることを定期的にレ ビューしなければならない。			H.Advanced	・組織は、モノの制御等を伴うような、フィジカル空間に影響を及ぼす可能性のある新たな機器やシステムを開発する場合には、従来の製品 や他の事故事例を収集・分析し、セーフティに関わるハザートを特定する。 ・組織は、ハギードによって非を正でる大弦を分析し、発生しやさな物害の深刻度を明らかにすることで、生じるリスクを目離れる。そ		
		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 ・ loT機器およびloT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	Advanced	・組織は、システム、またはシステムが整動する環境に大きな変化があった場合(新たな脊底が鹿倒性の特定を含む)、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、新たには「機整を利用したシステムを企画・設計する場合、既存の資産や新たに導入するシステムにおける守るべき資産を特定し、システムの利用用途や構成に応じて、セキュリティ対策をまとめる、特に、ライフサイクルの長いモノ、システムや、高い可用性を求められるモノ、システムを扱う場合は、設計以前の段階におけるセキュリティ対策の考慮が特に重要である。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 「参考)システムおよびモノにおけるセキュリティの要求仕様を検討するにあたり、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC、2015年)、「非確保要求クレード」(IPA、2018年)を参考してとか可能である。		
			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	Basic	・組織は、セキュリティリスクアセスメントのプロセスを定め、定期的(例えば、年に1回)に適用する。 ・セキュリティのリスク基準を確立し、維持する。 ・以下の方法によりセキュリティリスクを特定する。 1) 分析対象を明確化する 2) インシデント(周辺状況の変化を含む)並びにこれらの原因を特定する ・以下の方法により、セキュリティリスクを分析する。 1) 上記で特定されたリスクが実際に生じた場合に起こり得る結果について評価する 2) 上記で特定されたリスクの現実的な起こりやすまについて評価する 2) 上記で特定されたリスクの現実的な起こりやすまについて評価する ・リスク基準を参照し、リスクのレベルを決定し、優先順位付けする ・組織は、情報セキュリティリスクアセスメントのプロセスを文書化し、保管する。 [参考] セキュリティリスクアセスメントのプロセスを文書化し、保管する。 [参考] セキュリティリスクアセスメントの声法として、「資産ペース」の手法および「事業被害ペース」の手法があることが知られている。 資産ペースの手法でアセスメントを実施する場合は、「中小企業の情報セキュリティガイドライン」(IPA、2018年)や「制御システムのセキュリティリスク分析ガイド 第2版」(IPA、2018年)等を集まることができる。		
A.18.2.3 技術的順守のレビュー	情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューしなければならない。			H.Advanced	・組織は、モノの制御等を伴うような、フィジカル空間に影響を及ぼす可能性のある新たな機器やシステムを開発する場合には、従来の製品 や他の事故事例を収集・分析し、セーフティに関わるハザードを特定する。 ・組織は、ハザードによって被害に至る状況を分析し、発生しやするや被害の深刻度を明らかにすることで、生じるリスクを見積もる。その際、セキュリティの問題に起因するハザードの有無を確認することが望ましい。 [参考]セーフティ 放射におけるハザードの特定と分析については、「ながる世界のセーフティ&セキュリティ設計入門」(IPA, 2015年)の 4.2にて具体的な手法が記載されており、参照することが可能である。		
		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 ・ loT機器およびIoT機器を含んだシステムの企画・設計	Advanced	・組織は、システム、またはシステムが稼動する環境に大きな変化があった場合衝大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10世機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、システムの利用助途や機に広じて、セキュリティ対策をよりある。特に、ライフサイクルの長いモノ、システムや、高い可用性を求められるモノ、システムを扱う場合は、設計以前の段階におけるセキュリティ対策の考慮が特に重要である。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 「参考)システムおよびモノにおけるセキュリティの要求仕様を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 「参考)システムおよびモノにおけるセキュリティの要求仕様を検討するにあたり、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC、2015年)、「非機能要求グレード」(IPA、2018年)を参考にすることが可能である。		

ISO/IEC 27001:2013 附属書A	i e	サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID 要求事項		対策要件ID			対策例
			の段階から、受容できない収知のセキュリテイリスクの 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		・組織は、セキュリティリスクアセスメントのプロセスを定め、定期的(例えば、年に1回)に適用する。 ・セキュリティのリスク選手を確立し、維持する。 ・以下の方法によりセキュリティリスクを特定する。 1) 分析対象を明確化する 2) インシデント(周辺状況の変化を含む)並びにこれらの原因を特定する ・以下の方法により、セキュリティリスクを分析する。 1) 上記で特定されたリスクが実際に全じた場合に起こり得る結果について評価する 2) 上記で特定されたリスクの実実的に起じ、場合に起こり得る結果について評価する - リスク基準を参照し、リスクのレベルを決定し、優先順位付けする ・組織は、情報セキュリティリスクアセスメントのプロセスを支書化し、保管する。 [参考] セキュリティリスクアセスメントのプロセスを支書化し、保管する。 [参考] セキュリティリスクアセスメントを実施する場合は、「中小企業の情報セキュリティガイドライン」(IPA、2018年)や「制御システムのセキュリティンクが折ガイド 第2版 (IPA、2018年)等を、事業被害ペースの手法を実施する場合は、「影響システムのセキュリティリスク分析ガイド 第2版 (IPA、2018年)等を、事業被害ペースの手法を実施する場合は、「影響システムのセキュリティリスク分析ガイド 第2版。(IPA、2018年)等を参照することができる。