

添付B リスク源と対策要件の対応関係

■第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件

#	機能	想定される セキュリティインシデント	リスク源		対策要件	対策要件ID			
			脅威	脆弱性ID					
1_1	組織として平時のリスク管理体制を構築し、適切に運用すること	自組織で管理している領域から保護すべきデータが漏洩する	・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・入力確認の不備を突いたインジェクション攻撃(例：SQLインジェクション、XSS) ・ネットワーク上の通信の盗聴 ・保護が必要なエリアに対する不正なヒトの物理的な侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・正規ユーザによる内部不正	L1_1_a_ORG	[ソシキ] ・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・組織は、自組織のミッションを理解し、サイバーセキュリティリスクマネジメントにおける判断に用いる。	CPS.GV.OC-01		
						・組織は、戦略的機会（組織にとってプラスに働くリスク）を特定し、その特性を整理した上で、組織のサイバーセキュリティリスクに関する議論に含める。	CPS.GV.RM-08		
						・組織は、サプライチェーンに係るリスクマネジメントに関するプログラム、戦略、目的、ポリシー及びプロセスを明確にし、組織のステークホルダーと合意の上、運用する。	CPS.GV.SC-01		
						・組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	CPS.GV.SC-02		
						・組織は、サイバーセキュリティサプライチェーンリスクマネジメントを、サイバーセキュリティ及び事業体のリスクマネジメント、リスクアセスメント、改善プロセスに統合する。	CPS.GV.SC-03		
						・組織は、自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをする。	CPS.GV.SC-04		
						・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05		
						・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06		
						・組織は、技術製品及びサービスのライフサイクル全体を通じて、サプライチェーンに係るセキュリティ対策の実施状況を監視する。	CPS.GV.SC-10		
						L1_1_a_PEO	[ヒト] ・自身に関わりうるセキュリティやセーフティに関するリスクに対して十分な認識を有していない	・組織は、自組織のサイバーセキュリティリスクマネジメントに関する役割、責任及び権限を定め、組織内へ周知する。	CPS.GV.RR-02
								・組織は、自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を継続的に改善する。	CPS.ID.IM-03
								・組織は、自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.PR.AT-01
			[ヒト] ・ヒトに関わるセキュリティやセーフティに関係するリスクに対するガバナンスが十分でない	・組織は、サイバーセキュリティに関する法的要求事項や、規制上の要件、契約上の要求事項（プライバシー及び市民的自由の義務を含む）、及び業界のガイドライン等を理解した上で、それらを考慮した社内ルールを策定する。	CPS.GV.OC-02				
				・組織は、取引先及びその他の第三者によるリスクを含むサイバーセキュリティリスクについて、組織全体にわたるコミュニティ系統を明確にし、運用する。	CPS.GV.RM-06				
				・組織の経営層は、サイバーセキュリティリスクに対する責任及び説明責任を負い、当該リスクを認識した上で、倫理的かつ継続的に改善する文化を醸成する。	CPS.GV.RR-01				
				・組織は、自組織のサイバーセキュリティリスクマネジメントに関する役割、責任及び権限を定め、組織内へ周知する。	CPS.GV.RR-02				
				・組織は、人の異動に伴い生じる役割の変更に対応した対策に、セキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	CPS.GV.RR-05				
				・組織は、自組織の状況、サイバーセキュリティ戦略、優先順位等に基づいてセキュリティポリシーを策定し、組織内及び自組織の取引に関係する者（必要に応じてサプライヤー、第三者プロバイダ等を含む）に伝達し、実施する。	CPS.GV.PO-01				
				・組織は、要件、脅威、技術及び自組織のミッションの変化を踏まえ、セキュリティポリシーを定期的にレビューし、必要に応じて更新する。	CPS.GV.PO-02				
				L1_1_a_COM	[モノ] ・モノのセキュリティ状況やネットワーク接続状況が適切に管理(例：資産の棚卸し、モニタリング)されていない	・組織は、システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.ID.AM-01		
			・組織は、組織内の通信ネットワーク構成図及びデータフロー図を作成し、適切に管理する。			CPS.ID.AM-02			
			・組織は、自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。			CPS.ID.AM-03			
			・組織は、システム、ハードウェア、ソフトウェア、サービス及びデータを、取得から廃棄に至るライフサイクル全体を通じて管理する。			CPS.ID.AM-06			
			・組織は、セキュリティ事象を適切に検知できるよう、IoT機器、サーバ等のハードウェア及びソフトウェアの稼働状況、並びにネットワーク接続状況等を監視する。			CPS.DE.CM-02			

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID	
			脅威	脆弱性ID	脆弱性			
				L1_1_a_SYS	[システム] ・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	・組織は、自組織におけるリスク選好度及びリスク許容度を定め、組織内に周知する。	CPS.GV.RM-03	
						・組織は、自組織の資産の脆弱性を特定し、対応する資産と紐づけて管理する。	CPS.ID.RA-01	
						・組織は、自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.ID.RA-03	
						・組織は、構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施することにより、脆弱性を悪用する脅威の潜在的な影響と起こりやすさを識別する。	CPS.ID.RA-04	
						・組織は、リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化するとともに、その実施状況を把握し、関係者に共有する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.ID.RA-06	
						・組織は、自組織における重要な変更及びセキュリティ要件の例外について、それらがもたらすリスクの影響度をアセスメントし、その結果を記録し、管理する。	CPS.ID.RA-07	
						[システム] ・自組織のシステムにおいて、対処すべき脆弱性が放置されている	・組織は、自組織の資産の脆弱性を特定し、対応する資産と紐づけて管理する。	CPS.ID.RA-01
							・組織は、組織内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.ID.RA-02
							・組織は、自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.DE.CM-06
							・組織は、脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.PR.PS-08
							・組織は、IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.PR.PS-09
							・組織は、自組織のIoT機器、サーバ等に対する保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.PR.PS-10
					[システム] ・保護すべきデータが格納されたシステムにおいて、セキュアでない設定がなされている	・組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.PR.PS-06	
						・組織は、不正なソフトウェアのインストール及び実行を防止する。	CPS.PR.PS-07	
					[システム] ・保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	・組織は、承認されたモノとヒト及びプロセスの識別情報と認証情報を発効、管理、確認、取消、監査するプロセスを確立し、実施する。	CPS.PR.AA-01	
						・組織は、IoT機器やユーザーによる構成要素（モノ/システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で、信頼性の高い方式（例：多要素認証）を用いて認証・認可する。	CPS.PR.AA-02	
						・組織は、一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ。	CPS.PR.AA-03	
						・組織は、認証された主体に関する情報（IDアサーション）を保護し、送受信し、検証する。	CPS.PR.AA-04	
					[システム] ・IoT機器、サーバ等の設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	・組織は、IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.PR.AA-07	
						・組織は、無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.PR.IR-02	
						・組織は、IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.DE.CM-05	

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
					[システム] ・早期にセキュリティ上の異常を素早く検知し、対処する ような仕組みがシステムに実装されていない	・組織は、セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、継続的にログを記録し、レビューする。	CPS.PR.PS-11
						・組織は、セキュリティ事象を適切に検知できるよう、ネットワーク及びネットワークサービスを監視する。	CPS.DE.CM-01
						・組織は、セキュリティ事象を適切に検知できるよう、IoT機器、サーバ等のハードウェア及びソフトウェアの稼働状況、並びにネットワーク接続状況等を監視する。	CPS.DE.CM-02
						・組織は、セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容を監視する。	CPS.DE.CM-03
						・組織は、セキュリティ事象を適切に検知できるよう、組織内外の要員による構成要素（モノ／システム等）へのアクセスや操作等の活動を監視する。	CPS.DE.CM-04
						・組織は、サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	CPS.DE.CM-07
						・組織は、指示された動作内容と実際の動作結果を比較して異常の検知や動作の停止を行うIoT機器を導入する。 ・組織は、サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.DE.CM-08
						・組織は、監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。	CPS.DE.CM-09
						・組織は、潜在的なセキュリティ事象について分析を行い、当該事象の内容を把握する。	CPS.DE.AE-01
				L1_1_a_DAT	[データ] ・自組織で管理しているデータの保護に係る区分が明確になっていない	・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.PR.DS-01
					[データ] ・定められた機密区分に沿った情報の保護が実装されていない	・組織は、保存しているデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-02
						・組織は、伝送中のデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-03
						・組織は、使用中のデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-04
						・組織は、データ（例：構成要素の設定情報、業務データ等を含む）に対し、定期的なバックアップを実施し、バックアップデータの保護及び復旧のテストを行う。	CPS.PR.DS-06
						・組織は、セキュリティインシデントに関するデータ及びメタデータ（インシデント対応において実施した措置の履歴等を含む）を収集し、それらの完全性を確保するとともに、取得元及び取得時点等が参照可能な状態で保管する。	CPS.RS.AN-01
						・組織は、セキュリティインシデント発生後に、根本原因を特定するためのデジタルフォレンジックを実施する。その際、調査過程の記録を改ざんされない形で保管する。	CPS.RS.AN-02
				L1_1_a_PRO	[プロシージャ] ・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	・組織は、リスクマネジメントの目的を定め、関係するステークホルダーとの間で合意する。	CPS.GV.RM-01
						・組織は、サイバーセキュリティリスクマネジメントを適切に行うために、サイバーセキュリティ戦略を策定する。	CPS.GV.RM-02
						・組織は、自組織におけるリスク選好度及びリスク許容度を定め、組織内に周知する。	CPS.GV.RM-03
						・組織は、リスク対応における選択肢及びその運用に係る方針を策定し、組織内に共有する。	CPS.GV.RM-05
						・組織は、サイバーセキュリティリスクの評価、文書化、分類及び優先順位付けに関する標準的な方法を整備し、組織内に共有する。	CPS.GV.RM-07
						・組織は、自組織の状況、サイバーセキュリティ戦略、優先順位等に基づいてセキュリティポリシーを策定し、組織内及び自組織の取引に関係する者（必要に応じてサプライヤー、第三者プロバイダ等を含む）に伝達し、実施する。	CPS.GV.PO-01
						・組織は、要件、脅威、技術及び自組織のミッションの変化を踏まえ、セキュリティポリシーを定期的にレビューし、必要に応じて更新する。	CPS.GV.PO-02
						・組織は、サプライチェーンに係るリスクマネジメントに関するプログラム、戦略、目的、ポリシー及びプロセスを明確にし、組織のステークホルダーと合意の上、運用する。	CPS.GV.SC-01
						・組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	CPS.GV.SC-02
						・組織は、サイバーセキュリティサプライチェーンリスクマネジメントを、サイバーセキュリティ及び事業体のリスクマネジメント、リスクアセスメント、改善プロセスに統合する。	CPS.GV.SC-03
						・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05
						・組織は、取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロセスを策定し、運用する。	CPS.GV.SC-09
						・組織は、取引先等との契約終了時に実施すべきプロセスを策定し、運用する。	CPS.GV.SC-11

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
		自組織で管理している領域において保護すべきデータが改ざんされる	・ 窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・ 通信系路上でデータを改ざんする中間者攻撃等 ・ システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・ 正規ユーザによる内部不正 ・ 保護が必要なエリアに対する不正なヒトの物理的な侵入 ・ 保護が必要なデータを扱う媒体の物理的な破壊	L1_1_b_ORG	[ソシキ] ・ 適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・ 組織は、自組織のミッションを理解し、サイバーセキュリティリスクマネジメントにおける判断に用いる。	CPS.GV.OC-01
						・ 組織は、戦略的機会（組織にとってプラスに働くリスク）を特定し、その特性を整理した上で、組織のサイバーセキュリティリスクに関する議論に含める。	CPS.GV.RM-08
						・ 組織は、サプライチェーンに係るリスクマネジメントに関するプログラム、戦略、目的、ポリシー及びプロセスを明確にし、組織のステークホルダーと合意の上、運用する。	CPS.GV.SC-01
						・ 組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	CPS.GV.SC-02
						・ 組織は、サイバーセキュリティサプライチェーンリスクマネジメントを、サイバーセキュリティ及び事業体のリスクマネジメント、リスクアセスメント、改善プロセスに統合する。	CPS.GV.SC-03
						・ 組織は、自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをする。	CPS.GV.SC-04
						・ 組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05
						・ 組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06
						・ 組織は、技術製品及びサービスのライフサイクル全体を通じて、サプライチェーンに係るセキュリティ対策の実施状況を監視する。	CPS.GV.SC-10
				L1_1_b_PEO	[ヒト] ・ 自身が関わりうるセキュリティやセーフティに関係するリスクに対して十分な認識を有していない	・ 組織は、自組織のサイバーセキュリティリスクマネジメントに関する役割、責任及び権限を定め、組織内へ周知する。	CPS.GV.RR-02
						・ 組織は、取引先及びその他の第三者によるリスクを含むサイバーセキュリティリスクについて、組織全体にわたるコミュニティ系統を明確にし、運用する。	CPS.GV.RM-06
						・ 組織は、自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を継続的に改善する。	CPS.ID.IM-03
						・ 組織は、自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.PR.AT-01
					[ヒト] ・ ヒトに関わるセキュリティやセーフティに関係するリスクに対するガバナンスが十分でない	・ 組織は、サイバーセキュリティに関する法的要求事項や、規制上の要件、契約上の要求事項（プライバシー及び市民的自由の義務を含む）、及び業界のガイドライン等を理解した上で、それらを考慮した社内ルールを策定する。	CPS.GV.OC-02
						・ 組織の経営層は、サイバーセキュリティリスクに対する責任及び説明責任を負い、当該リスクを認識した上で、倫理的かつ継続的に改善する文化を醸成する。	CPS.GV.RR-01
						・ 組織は、自組織のサイバーセキュリティリスクマネジメントに関する役割、責任及び権限を定め、組織内へ周知する。	CPS.GV.RR-02
						・ 組織は、人の異動に伴い生じる役割の変更に対応した対策に、セキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	CPS.GV.RR-05
						・ 組織は、自組織の状況、サイバーセキュリティ戦略、優先順位等に基づいてセキュリティポリシーを策定し、組織内及び自組織の取引に関係する者（必要に応じてサプライヤー、第三者プロバイダ等を含む）に伝達し、実施する。	CPS.GV.PO-01
						・ 組織は、要件、脅威、技術及び自組織のミッションの変化を踏まえ、セキュリティポリシーを定期的にレビューし、必要に応じて更新する。	CPS.GV.PO-02
				L1_1_b_COM	[モノ] ・ 情報システムや産業用制御システムを構成しているモノのセキュリティ状況やネットワーク接続状況が適切に管理(例：資産の棚卸し、モニタリング)されていない	・ 組織は、システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.ID.AM-01
						・ 組織は、組織内の通信ネットワーク構成図及びデータフロー図を作成し、適切に管理する。	CPS.ID.AM-02
						・ 組織は、自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.ID.AM-03
						・ 組織は、システム、ハードウェア、ソフトウェア、サービス及びデータを、取得から廃棄に至るライフサイクル全体を通じて管理する。	CPS.ID.AM-06
						・ 組織は、セキュリティ事象を適切に検知できるよう、IoT機器、サーバ等のハードウェア及びソフトウェアの稼働状況、並びにネットワーク接続状況等を監視する。	CPS.DE.CM-02
				L1_1_b_SYS	[システム] ・ 自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	・ 組織は、自組織におけるリスク選好度及びリスク許容度を定め、組織内に周知する。	CPS.GV.RM-03
						・ 組織は、自組織の資産の脆弱性を特定し、対応する資産と紐づけて管理する。	CPS.ID.RA-01
						・ 組織は、自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。 ・ IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.ID.RA-03
						・ 組織は、構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施することにより、脆弱性を悪用する脅威の潜在的な影響と起こりやすさを識別する。	CPS.ID.RA-04
						・ 組織は、リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化するとともに、その実施状況を把握し、関係者に共有する。 ・ IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.ID.RA-06
						・ 組織は、自組織における重要な変更及びセキュリティ要件の例外について、それらがもたらすリスクの影響度をアセスメントし、その結果を記録し、管理する。	CPS.ID.RA-07

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
					[システム] ・保護すべきデータが格納されたシステムにおいて、セキュアでない設定がなされている	・組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.PR.PS-06
						・組織は、不正なソフトウェアのインストール及び実行を防止する。	CPS.PR.PS-07
					[システム] ・保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	・組織は、承認されたモノとヒト及びプロセスの識別情報と認証情報を発効、管理、確認、取消、監査するプロセスを確立し、実施する。	CPS.PR.AA-01
						・組織は、IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で、信頼性の高い方式（例：多要素認証）を用いて認証・認可する。	CPS.PR.AA-02
						・組織は、一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ。	CPS.PR.AA-03
						・組織は、認証された主体に関する情報（IDアサーション）を保護し、送受信し、検証する。	CPS.PR.AA-04
					[システム] ・早期にネットワーク上での異常(例：なりすまし、メッセージの改ざん)を素早く検知し、対処するような仕組みがシステムに実装されていない	・組織は、セキュリティ事象を適切に検知できるよう、ネットワーク及びネットワークサービスを監視する。	CPS.DE.CM-01
						・組織は、セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容を監視する。	CPS.DE.CM-03
						・組織は、サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	CPS.DE.CM-07
				L1_1_b_PRO	[プロセス] ・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	・組織は、リスクマネジメントの目的を定め、関係するステークホルダーとの間で合意する。	CPS.GV.RM-01
						・組織は、サイバーセキュリティリスクマネジメントを適切に行うために、サイバーセキュリティ戦略を策定する。	CPS.GV.RM-02
						・組織は、自組織におけるリスク選好度及びリスク許容度を定め、組織内に周知する。	CPS.GV.RM-03
						・組織は、リスク対応における選択肢及びその運用に係る方針を策定し、組織内に共有する。	CPS.GV.RM-05
						・組織は、サイバーセキュリティリスクの評価、文書化、分類及び優先順位付けに関する標準的な方法を整備し、組織内に共有する。	CPS.GV.RM-07
						・組織は、自組織の状況、サイバーセキュリティ戦略、優先順位等に基づいてセキュリティポリシーを策定し、組織内及び自組織の取引に関係する者（必要に応じてサプライヤー、第三者プロバイダ等を含む）に伝達し、実施する。	CPS.GV.PO-01
						・組織は、要件、脅威、技術及び自組織のミッションの変化を踏まえ、セキュリティポリシーを定期的にレビューし、必要に応じて更新する。	CPS.GV.PO-02
						・組織は、サプライチェーンに係るリスクマネジメントに関するプログラム、戦略、目的、ポリシー及びプロセスを明確にし、組織のステークホルダーと合意の上、運用する。	CPS.GV.SC-01
						・組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	CPS.GV.SC-02
						・組織は、サイバーセキュリティサプライチェーンリスクマネジメントを、サイバーセキュリティ及び事業体のリスクマネジメント、リスクアセスメント、改善プロセスに統合する。	CPS.GV.SC-03
						・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05
						・組織は、取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロセスを策定し、運用する。	CPS.GV.SC-09
						・組織は、取引先等との契約終了時に実施すべきプロセスを策定し、運用する。	CPS.GV.SC-11
				L1_1_b_DAT	[データ] ・通信路及び通信路上のデータが十分に保護されていない	・組織は、伝送中のデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-03
					[データ] ・取り扱うデータに改ざんを検知するメカニズムがない	・組織は、保存しているデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-02
						・組織は、伝送中のデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-03
						・組織は、使用中のデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-04
						・組織は、データの取得元、加工履歴等をライフサイクル全体に渡って維持・更新・管理する。	CPS.PR.DS-05
						・組織は、サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	CPS.DE.CM-07

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
		サービス拒否攻撃、ランサムウェアへの感染等により、自組織のデータを取り扱うシステムが停止する	・システムを構成するサーバ等の電算機器、通信機器等に対するサービス拒否攻撃 ・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・妨害電波の発信	L1_1_c_ORG	[ソシキ] ・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・組織は、自組織のミッションを理解し、サイバーセキュリティリスクマネジメントにおける判断に用いる。	CPS.GV.OC-01
						・組織は、戦略的機会（組織にとってプラスに働くリスク）を特定し、その特性を整理した上で、組織のサイバーセキュリティリスクに関する議論に含める。	CPS.GV.RM-08
						・組織は、サプライチェーンに係るリスクマネジメントに関するプログラム、戦略、目的、ポリシー及びプロセスを明確にし、組織のステークホルダーと合意の上、運用する。	CPS.GV.SC-01
						・組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	CPS.GV.SC-02
						・組織は、サイバーセキュリティサプライチェーンリスクマネジメントを、サイバーセキュリティ及び事業体のリスクマネジメント、リスクアセスメント、改善プロセスに統合する。	CPS.GV.SC-03
						・組織は、自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをする。	CPS.GV.SC-04
						・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05
						・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06
						・組織は、技術製品及びサービスのライフサイクル全体を通じて、サプライチェーンに係るセキュリティ対策の実施状況を監視する。	CPS.GV.SC-10
			[ヒト] ・自身に関わりうるセーフティやセキュリティに関わるリスクに対して十分な認識を有していない	L1_1_c_PEO		・組織は、自組織のサイバーセキュリティリスクマネジメントに関する役割、責任及び権限を定め、組織内へ周知する。	CPS.GV.RR-02
						・組織は、自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を継続的に改善する。	CPS.ID.IM-03
						・組織は、自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.PR.AT-01
						[ヒト] ・ヒトに関わるセーフティやセキュリティに関係するリスクに対するガバナンスが十分でない	CPS.GV.OC-02
			[モノ] ・情報システムや産業用制御システムを構成しているモノのセキュリティ状況やネットワーク接続状況が適切に管理（例：資産の棚卸し、モニタリング）されていない	L1_1_c_COM		・組織は、システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.ID.AM-01
						・組織は、組織内の通信ネットワーク構成図及びデータフロー図を作成し、適切に管理する。	CPS.ID.AM-02
						・組織は、自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.ID.AM-03
						・組織は、システム、ハードウェア、ソフトウェア、サービス及びデータを、取得から廃棄に至るライフサイクル全体を通じて管理する。	CPS.ID.AM-06
						・組織は、セキュリティ事象を適切に検知できるよう、IoT機器、サーバ等のハードウェア及びソフトウェアの稼働状況、並びにネットワーク接続状況等を監視する。	CPS.DE.CM-02
			[システム] ・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	L1_1_c_SYS		・組織は、自組織におけるリスク選好度及びリスク許容度を定め、組織内に周知する。	CPS.GV.RM-03
						・組織は、自組織の資産の脆弱性を特定し、対応する資産と紐づけて管理する。	CPS.ID.RA-01
						・組織は、自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.ID.RA-03
						・組織は、構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施することにより、脆弱性を悪用する脅威の潜在的な影響と起こりやすさを識別する。	CPS.ID.RA-04
						・組織は、リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化するとともに、その実施状況を把握し、関係者に共有する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.ID.RA-06
						・組織は、自組織における重要な変更及びセキュリティ要件の例外について、それらをもたらすリスクの影響度をアセスメントし、その結果を記録し、管理する。	CPS.ID.RA-07

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID	
			脅威	脆弱性ID	脆弱性			
					[システム] ・IoT、サーバ等に対する通信を適切に制御していない	・組織は、IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で、信頼性の高い方式（例：多要素認証）を用いて認証・認可する。	CPS.PR.AA-02	
					・組織は、一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ。	CPS.PR.AA-03		
					・組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.PR.PS-06		
					・組織は、ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等して、認可されていないアクセス及び使用からネットワーク及び環境を保護する。	CPS.PR.IR-01		
					[システム] ・IoT、サーバ等に対する物理的な妨害（例：妨害電波）に対処できていない	・組織は、IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.PR.AA-07	
					・組織は、無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.PR.IR-02		
					[システム] ・IoT機器を含む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)が確保されていない	・組織は、平時及び有事において、システム及びサービスの継続稼働に関する要件を達成するための仕組みを実装する。	CPS.PR.IR-03	
					・組織は、サイバー攻撃（例：ランサムウェア、サービス拒否攻撃等）を受けた場合でも、攻撃による影響を最小限に抑え、重要な機能を維持できるよう、十分なリソース（例：ヒト、モノ、システム）を確保する。	CPS.PR.IR-04		
					L1_1_c-PRO	[プロシージャ] ・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	・組織は、リスクマネジメントの目的を定め、関係するステークホルダーとの間で合意する。	CPS.GV.RM-01
						・組織は、サイバーセキュリティリスクマネジメントを適切に行うために、サイバーセキュリティ戦略を策定する。	CPS.GV.RM-02	
						・組織は、自組織におけるリスク選好度及びリスク許容度を定め、組織内に周知する。	CPS.GV.RM-03	
						・組織は、リスク対応における選択肢及びその運用に係る方針を策定し、組織内に共有する。	CPS.GV.RM-05	
						・組織は、サイバーセキュリティリスクの評価、文書化、分類及び優先順位付けに関する標準的な方法を整備し、組織内に共有する。	CPS.GV.RM-07	
						・組織は、自組織の状況、サイバーセキュリティ戦略、優先順位等に基づいてセキュリティポリシーを策定し、組織内及び自組織の取引に関係する者（必要に応じてサプライヤー、第三者プロバイダ等を含む）に伝達し、実施する。	CPS.GV.PO-01	
						・組織は、要件、脅威、技術及び自組織のミッションの変化を踏まえ、セキュリティポリシーを定期的にレビューし、必要に応じて更新する。	CPS.GV.PO-02	
						・組織は、サプライチェーンに係るリスクマネジメントに関するプログラム、戦略、目的、ポリシー及びプロセスを明確にし、組織のステークホルダーと合意の上、運用する。	CPS.GV.SC-01	
						・組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	CPS.GV.SC-02	
						・組織は、サイバーセキュリティサプライチェーンリスクマネジメントを、サイバーセキュリティ及び事業体のリスクマネジメント、リスクアセスメント、改善プロセスに統合する。	CPS.GV.SC-03	
						・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05	
						・組織は、取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.GV.SC-09	
					・組織は、取引先等との契約終了時に実施すべきプロシージャを策定し、運用する。	CPS.GV.SC-11		
		法制度等で規定されている水準のセキュリティ対策を実装できない	All threats	L1_2_a-ORG	[ソシキ] ・遵守すべき法制度等を認識していないか、法制度に準拠した組織内のルールを策定・運用していない	・組織は、サイバーセキュリティに関する法的要求事項や、規制上の要件、契約上の要求事項（プライバシー及び市民的自由の義務を含む）、及び業界のガイドライン等を理解した上で、それらを考慮した社内ルールを策定する。	CPS.GV.OC-02	
				L1_2_a-PEO	[ヒト] ・遵守すべき法制度等を認識していないか、法制度に準拠した組織内のルールを遵守していない	・組織は、自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.PR.AT-01	
				L1_2_a-COM	[モノ] ・法制度等で一定の保護を義務付けられている種のモノが、要求される水準の保護を適用されていない	・組織は、サイバーセキュリティに関する法的要求事項や、規制上の要件、契約上の要求事項（プライバシー及び市民的自由の義務を含む）、及び業界のガイドライン等を理解した上で、それらを考慮した社内ルールを策定する。	CPS.GV.OC-02	
						・組織は、計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、適切なセキュリティ対策を実装した製品を利用する。	CPS.PR.PS-03	

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
				L1_2_a_SYS	[システム] ・法制度等で一定の保護を義務付けられている種のシステムが、要求される水準の保護を適用されていない	・組織は、サイバーセキュリティに関する法的要求事項や、規制上の要件、契約上の要求事項（プライバシー及び市民的自由の義務を含む）、及び業界のガイドライン等を理解した上で、それらを考慮した社内ルールを策定する。	CPS.GV.OC-02
				L1_2_a_PRO	[プロシージャ] ・組織内で規定されているプロシージャが関連する法規制等を遵守するような内容となっていない	・組織は、サイバーセキュリティに関する法的要求事項や、規制上の要件、契約上の要求事項（プライバシー及び市民的自由の義務を含む）、及び業界のガイドライン等を理解した上で、それらを考慮した社内ルールを策定する。	CPS.GV.OC-02
				L1_2_a_DAT	[データ] ・法制度等で一定の保護を義務付けられている種のデータが、要求される水準の保護を適用されていない	・組織は、サイバーセキュリティに関する法的要求事項や、規制上の要件、契約上の要求事項（プライバシー及び市民的自由の義務を含む）、及び業界のガイドライン等を理解した上で、それらを考慮した社内ルールを策定する。	CPS.GV.OC-02
						・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.PR.DS-01
1_2	組織としてセキュリティインシデント発生時においても適切に自組織の事業を継続すること	自組織のセキュリティインシデントにより自組織が適切に事業継続できない	All threats	L1_3_a_ORG	[ソシキ] ・セキュリティ事象を的確に検知するための体制が構築されていない	・組織は、自組織のサイバーセキュリティリスクマネジメントに関する役割、責任及び権限を定め、組織内へ周知する。	CPS.GV.RR-02
						・組織は、セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を設置し、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	CPS.GV.RR-03
						・組織は、サイバーセキュリティ戦略、役割、責任及びポリシーに応じて、必要なリソースを確保する。	CPS.GV.RR-04
						・組織は、アラートやログ等の検知イベントの分析結果から教訓を導き出し、セキュリティ事象の検知プロセスを継続的に改善する。	CPS.ID.IM-05
					[ソシキ] ・セキュリティインシデントに的確に対応するための体制が構築されていない	・組織は、自組織のサイバーセキュリティリスクマネジメントに関する役割、責任及び権限を定め、組織内へ周知する。	CPS.GV.RR-02
						・組織は、セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を設置し、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	CPS.GV.RR-03
						・組織は、サイバーセキュリティ戦略、役割、責任及びポリシーに応じて、必要なリソースを確保する。	CPS.GV.RR-04
						・組織は、セキュリティインシデントへの対応から教訓を導き出し、インシデント対応計画を継続的に改善する。	CPS.ID.IM-06
				L1_3_a_PEO	[ヒト] ・セキュリティインシデント発生時に適切なアクションを取ることができない	・組織は、セキュリティインシデントへの対応から教訓を導き出し、インシデント対応計画を継続的に改善する。	CPS.ID.IM-06
						・組織は、自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.PR.AT-01
						・組織は、自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.PR.AT-02
						・組織は、セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RS.MA-01
						・組織は、セキュリティインシデントとして報告された事象について、誤検知や重複報告でないことを確認し、インシデントとしての妥当性を確認する。	CPS.RS.MA-02
						・組織は、検知されたセキュリティインシデントを、影響度の大小や侵入経路等に基づき分類し、優先順位を付ける。	CPS.RS.MA-03
						・組織は、セキュリティインシデントの特性及び復旧活動が業務に与える影響を考慮し、あらかじめ定めた基準に基づき復旧の開始を判断する。	CPS.RS.MA-06
						・組織は、セキュリティインシデント発生後の、組織内部及び外部への情報公表に関するルールを策定し、運用する。	CPS.RS.CO-01
						・組織は、定めたルールに基づき、組織内部の上位意思決定者及び関係する外部組織に対し、必要に応じてエスカレーションを行う。	CPS.RS.CO-02
						・組織は、セキュリティインシデントによる被害の拡大を最小限に抑え、原因の除去又は影響の低減を行う。	CPS.RS.MI-01
				L1_3_a_COM	[モノ] ・セキュリティインシデントにより被害を受けた自組織の事業の範囲(製品等)を特定することができない	・組織は、自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。	CPS.ID.AM-07
						・組織は、重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。	CPS.ID.AM-08
						・組織は、関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。	CPS.DE.AE-03
						・組織は、セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。	CPS.RS.AN-03
				L1_3_a_SYS	[システム] ・セキュリティインシデントを適切に検知するための機器等が導入されていないか、あるいは正しく運用されていない	・組織は、アラートやログ等の検知イベントの分析結果から教訓を導き出し、セキュリティ事象の検知プロセスを継続的に改善する。	CPS.ID.IM-05
						・組織は、セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、継続的にログを記録し、レビューする。	CPS.PR.PS-11
						・組織は、指示された動作内容と実際の動作結果を比較して異常の検知や動作の停止を行うIoT機器を導入する。	CPS.DE.CM-08
						・組織は、サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	
						・組織は、監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。	CPS.DE.CM-09

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID		
			脅威	脆弱性ID	脆弱性				
				L1_3_a_PRO	【プロセス】 ・自組織におけるセキュリティインシデントへの対応手順が策定されていない	・組織は、セキュリティインシデントへの対応から教訓を導き出し、インシデント対応計画を継続的に改善する。	CPS.ID.IM-06		
					・組織は、セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RS.MA-01			
					・組織は、セキュリティインシデント発生後の、組織内部及び外部への情報公表に関するルールを策定し、運用する。	CPS.RS.CO-01			
				【プロセス】 ・事業継続計画にセキュリティインシデントが位置づけられておらず、セキュリティインシデント発生時に自組織の事業継続に支障が生じる	・組織は、セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又は緊急時対応計画を継続的に改善する。	CPS.ID.IM-07			
					・組織は、自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急時対応計画の中にセキュリティインシデントを位置づける。	CPS.RC.RP-01			
					・組織は、事業継続計画又は緊急時対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。	CPS.RC.CO-02			
					・組織は、復旧活動について内部及び外部のステークホルダーと役員、そして経営陣に伝達する点を、事業継続計画又は緊急時対応計画の中に位置づける。	CPS.RC.CO-03			
				L1_3_a_DAT	【データ】 ・セキュリティインシデント発生時に事業を継続するために必要なデータが、適切に準備されていない、又は準備されてるが適切に機能しない	・組織は、データ（例：構成要素の設定情報、業務データ等を含む）に対し、定期的なバックアップを実施し、バックアップデータの保護及び復旧のテストを行う。	CPS.PR.DS-06		
					・組織は、バックアップ及びその他の復旧資産の完全性を、使用前に検証する。	CPS.RC.RP-04			
		自組織のセキュリティインシデントにより関係する他組織が適切に事業継続できない	All threats	L1_3_b_ORG	【ソシキ】 ・自組織のモノ/システム/データのサイバー空間における他組織との連携状況を把握していない	・組織は、組織内の通信ネットワーク構成図及びデータフロー図を作成し、適切に管理する。	CPS.ID.AM-02		
						・組織は、自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.ID.AM-03		
					【ソシキ】 ・自組織と他組織(サプライヤー等)とのフィジカル空間における連携状況および責任分界を把握していない	・組織は、自組織が事業を継続する上で、自組織及び関係する他組織における依存関係と重要な機能を特定し、共有する。	CPS.GV.OC-03		
						・組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	CPS.GV.SC-02		
						・組織は、自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをする。	CPS.GV.SC-04		
						・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05		
				L1_3_b_PEO	【ヒト】 ・他組織のヒトが自組織のセキュリティ事象発生時に適切なアクションを取ることができない	・組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	CPS.GV.SC-02		
						・組織は、自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.PR.AT-02		
						・組織は、セキュリティインシデントが宣言された場合、取引先等の関係する他組織と連携し、あらかじめ定めた対応手順に基づきインシデント対応を実行する。	CPS.RS.MA-04		
				L1_3_b_COM	【モノ】 ・セキュリティ事象による被害を受けたモノ(製品)・サービスが生じる	・組織は、セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ（製品）に対して適切な対応を行う。	CPS.RS.MA-05		
						【モノ】 ・自組織が提供する/されるモノ(製品)に関する記録(例: 製造日/識別ナンバー/提供先)が保持されていない	・組織は、自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。	CPS.ID.AM-07	
					・組織は、重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。		CPS.ID.AM-08		
				L1_3_b_PRO	【プロセス】 ・関係する他組織と連携したセキュリティ事象対応手順が策定されていない	・組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	CPS.GV.SC-02		
						・組織は、セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RS.MA-01		
				関係する他組織のセキュリティインシデントにより自組織が適切に事業継続できない	All threats	L1_3_c_ORG	【ソシキ】 ・自組織のモノ/システム/データのサイバー空間における他組織との連携状況を把握していない	・組織は、組織内の通信ネットワーク構成図及びデータフロー図を作成し、適切に管理する。	CPS.ID.AM-02
								・組織は、自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.ID.AM-03
						【ソシキ】 ・自組織と他組織(サプライヤー等)とのフィジカル空間における連携状況および責任分界を把握していない	・組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	CPS.GV.SC-02	
							・組織は、セキュリティインシデントへの対応から教訓を導き出し、インシデント対応計画を継続的に改善する。	CPS.ID.IM-06	
		・組織は、自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.PR.AT-02						
		・組織は、セキュリティインシデントが宣言された場合、取引先等の関係する他組織と連携し、あらかじめ定めた対応手順に基づきインシデント対応を実行する。	CPS.RS.MA-04						

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID			
			脅威	脆弱性ID	脆弱性					
				L1_3_c_PEO	[ヒト] ・自組織のヒトが他組織のセキュリティ事象発生時に適切なアクションを取ることができない	・組織は、自組織のサイバーセキュリティリスクマネジメントに関する役割、責任及び権限を定め、組織内へ周知する。	CPS.GV.RR-02			
						・組織は、自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.PR.AT-01			
						・組織は、自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を継続的に改善する。	CPS.ID.IM-03			
						L1_3_c_PRO	[プロシージャ] ・関係する他組織と連携したセキュリティ事象対応手順が策定されていない	・組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	CPS.GV.SC-02	
							・組織は、セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RS.MA-01		
1_3	フィジカル空間での製品・サービスが、望まれる品質を備えて入荷又は出荷されること	製品・サービスの提供チャネルでセキュリティ事象が発生し、機器の破損等の意図しない品質劣化が生じる	・悪意を持った自組織内外のヒトによる不正改ざん ・正規の機器を模した偽造品の挿入	L1_1_d_ORG	[ソシキ] ・製品・サービスを調達する際、それが信頼できるものかを確認していない	・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07			
						・組織は、取引先等の関係する他組織が契約上の義務を果たしていることを確認するために、監査、テスト結果、又は他の形式の評価を使用して定期的に評価する。	CPS.GV.SC-08			
						L1_1_d_PEO	[ヒト] ・自組織の調達に関わる要員が、調達に係るセキュリティリスクを十分に認識していない。	・組織は、自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を継続的に改善する。	CPS.ID.IM-03	
							・組織は、自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.PR.AT-01		
							L1_1_d_COM	[モノ] ・調達する製品・サービスが十分な物理的保護を実施されていない	・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07
							・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する。	CPS.PR.PS-02		
							L1_1_d_PRO	[プロシージャ] ・製品・サービスの調達時に、調達品の適格性を確認するプロシージャが存在しない	・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05
									・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06
									・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07

■第2層における機能／想定されるセキュリティインシデント／リスク源／対策要件

#	機能	想定される セキュリティインシデント	リスク源		対策要件	対策要件ID	
			脅威	脆弱性			
2_共通	下記機能の双方 ・フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、サイバー空間へ送る機能 ・サイバー空間から受け取ったデータに基づいて、一定のルールに基づいて、モノを制御したり、データを可視化したりする機能	脆弱性を悪用してIoT機器内部に不正アクセスされ、事前に想定されていない動作をする	・攻撃ツール等を利用したIoT機器におけるセキュリティ上の脆弱性を利用したマルウェア感染	L2_1_a_ORG	[ソシキ] ・情報システムや産業用制御システムに接続している自組織のIoT機器のセキュリティ対策状況(ソフトウェア構成情報、パッチ適用状況等)を把握できていない	・組織は、システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.ID.AM-01
				・組織は、自組織の資産の脆弱性を特定し、対応する資産と紐づけて管理する。	CPS.ID.RA-01		
				・組織は、リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化するとともに、その実施状況を把握し、関係者に共有する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.ID.RA-06		
				・組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.PR.PS-06		
				・組織は、IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.PR.PS-09		
				・組織は、自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.DE.CM-06		
				L2_1_a_COM	[モノ] ・利用しているIoT機器に関わる脆弱性情報、脅威情報を収集・分析し、適切に対応していない。	・組織は、自組織の資産の脆弱性を特定し、対応する資産と紐づけて管理する。	CPS.ID.RA-01
				・組織は、組織内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.ID.RA-02		
				・組織は、構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施することにより、脆弱性を悪用する脅威の潜在的な影響と起こりやすさを識別する。	CPS.ID.RA-04		
				・組織は、保護技術の有効性について、適切なパートナーとの間で情報を共有する。	CPS.ID.RA-05		
				・組織は、リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化するとともに、その実施状況を把握し、関係者に共有する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.ID.RA-06		
				・組織は、脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.PR.PS-08		
				・組織は、IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.PR.PS-09		
				・組織は、自組織のIoT機器、サーバ等に対する保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.PR.PS-10		
				・組織は、自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.DE.CM-06		
				・組織は、セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。	CPS.DE.AE-02		
				L2_1_a_PRO	[プロセス] ・調達時に、適切なレベルのセキュリティ機能が実装されているかを確認するプロセスがない	・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07
				・組織は、自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.ID.RA-03		
				・組織は、リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化するとともに、その実施状況を把握し、関係者に共有する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.ID.RA-06		
				・組織は、計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、適切なセキュリティ対策を実装した製品を利用する。	CPS.PR.PS-03		
				・組織は、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。	CPS.PR.PS-04		
				L2_1_a_PRO	[プロセス] ・調達時に、適切なレベルのセキュリティ機能が実装されているかを確認するプロセスがない	・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05
				・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07		
				・組織は、計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、適切なセキュリティ対策を実装した製品を利用する。	CPS.PR.PS-03		
				・組織は、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。	CPS.PR.PS-04		

#	機能	想定される	リスク源			対策要件	対策要件ID			
		セキュリティインシデント	脅威	脆弱性ID	脆弱性					
		正規のユーザーになりすましてIoT機器内部に不正アクセスされ、事前に想定されていない動作をする	・ 窃取したID等を利用した正規ホストへのなりすまし ・ セキュリティが実装されていない脆弱なプロトコルを悪用した不正アクセス	L2_1_b_ORG	[プロシージャ] ・ IoT機器の誤動作を検知した後の対応手順が定義されていない	・ 組織は、セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RS.MA-01			
					[ソシキ] ・ ネットワークの適正利用を確認していない	・ 組織は、セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、継続的にログを記録し、レビューする。	CPS.PR.PS-11			
						・ 組織は、セキュリティ事象を適切に検知できるよう、ネットワーク及びネットワークサービスを監視する。	CPS.DE.CM-01			
						・ 組織は、セキュリティ事象を適切に検知できるよう、IoT機器、サーバ等のハードウェア及びソフトウェアの稼働状況、並びにネットワーク接続状況等を監視する。	CPS.DE.CM-02			
				L2_1_b_COM	[モノ] ・ セキュリティの観点において強度が十分でない設定（パスワード、ポート等）がなされている	・ 組織は、セキュリティ事象を適切に検知できるよう、組織内外の要員による構成要素（モノ／システム等）へのアクセスや操作等の活動を監視する。	CPS.DE.CM-04			
						・ 組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.PR.PS-06			
				L2_1_b_SYS	[システム] ・ 通信相手に対するアクセス制御が十分でない	・ 組織は、承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.PR.AA-01			
						・ 組織は、IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で、信頼性の高い方式（例：多要素認証）を用いて認証・認可する。	CPS.PR.AA-02			
						・ 組織は、一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあげる機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ。	CPS.PR.AA-03			
						・ 組織は、アクセス権限の付与に関する規定をセキュリティポリシーに定義し、最小特権と職務分離の原則を組み込む。	CPS.PR.AA-05			
						・ 組織は、アクセス権限の付与状況について、定期的に見直しを行い、不要又は過剰な権限を是正する。	CPS.PR.AA-06			
				L2_1_b_PRO	[プロシージャ] ・ IoT機器のセキュリティ設定手順が定められていない	・ 組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.PR.PS-06			
					[プロシージャ] ・ IoT機器の誤動作を検知した後の対応手順が定義されていない	・ 組織は、セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RS.MA-01			
	遠隔からIoT機器を管理するシステムに不正アクセスされ、IoT機器に不正な入力をされ、事前に想定されていない動作をする。	・ システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・ 窃取したID、パスワード等を利用した正規ユーザーへのなりすまし ・ IoT機器を管理するシステムからIoT機器への不正なコマンド送信	L2_1_c_ORG	[ソシキ] ・ IoT機器を管理するシステムのセキュリティ対策状況（ソフトウェア構成情報、パッチ適用状況等）を把握できていない	・ 組織は、システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.ID.AM-01				
					・ 組織は、自組織の資産の脆弱性を特定し、対応する資産と紐づけて管理する。	CPS.ID.RA-01				
					・ 組織は、リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化するとともに、その実施状況を把握し、関係者に共有する。 ・ IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.ID.RA-06				
					・ 組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.PR.PS-06				
					・ 組織は、IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.PR.PS-09				
					・ 組織は、自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.DE.CM-06				
					L2_1_c_SYS	[システム] ・ システム管理権限に対するアクセス制御が十分でない	・ 組織は、承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.PR.AA-01		
							・ 組織は、IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で、信頼性の高い方式（例：多要素認証）を用いて認証・認可する。	CPS.PR.AA-02		
							・ 組織は、アクセス権限の付与に関する規定をセキュリティポリシーに定義し、最小特権と職務分離の原則を組み込む。	CPS.PR.AA-05		
							・ 組織は、アクセス権限の付与状況について、定期的に見直しを行い、不要又は過剰な権限を是正する。	CPS.PR.AA-06		
							・ 組織は、脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.PR.PS-08		
									・ 組織は、IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.PR.PS-09
									・ 組織は、自組織のIoT機器、サーバ等に対する保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.PR.PS-10

#	機能	想定される	リスク源			対策要件	対策要件ID
		セキュリティインシデント	脅威	脆弱性ID	脆弱性		
					[プロシージャ] ・IoT機器の誤動作を検知した後の対応手順が定義されていない	・組織は、セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RS.MA-01
		サービス拒否攻撃等により、IoT機器や通信機器等の機能が停止する	・IoTシステムを構成するIoT機器、通信機器等に対するサービス拒否攻撃	L2_1_d_SYS	[システム] ・IoT機器を含む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)が確保されていない	・組織は、平時及び有事において、システム及びサービスの継続稼働に関する要件を達成するための仕組みを実装する。	CPS.PR.IR-03
						・組織は、サイバー攻撃（例：ランサムウェア、サービス拒否攻撃等）を受けた場合でも、攻撃による影響を最小限に抑え、重要な機能を維持できるよう、十分なリソース（例：ヒト、モノ、システム）を確保する。	CPS.PR.IR-04
					[プロシージャ] ・IoT機器の停止を検知した後の対応手順が定義されていない	・組織は、セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RS.MA-01
2_1	サイバー空間から受け取ったデータに基づいて、一定のルールに基づいて、モノを制御したり、データを可視化したりする機能	正常動作・異常動作に関わらず、安全に支障をきたすような動作をする	・不正なエンティティによるコマンドインジェクション攻撃 ・サイバー空間からの許容範囲外のインプットデータ ・マルウェアによる制御信号の改ざん	L2_2_a_ORG	[ソシキ] ・機器を調達する際、安全性を実装しているかを確認していない	・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05
						・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07
						・組織は、計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、適切なセキュリティ対策を実装した製品を利用する。	CPS.PR.PS-03
						・組織は、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。	CPS.PR.PS-04
				L2_2_a_COM	[モノ] ・インプットされたデータを検証する仕組みが無い	・組織は、サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	CPS.DE.CM-07
						・組織は、指示された動作内容と実際の動作結果を比較して異常の検知や動作の停止を行うIoT機器を導入する。 ・組織は、サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.DE.CM-08
				L2_2_a_SYS	[システム] ・稼動するシステムとして、安全計装が考慮されていない。	・組織は、自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.ID.RA-03
						・組織は、リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化するとともに、その実施状況を把握し、関係者に共有する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.ID.RA-06
						・組織は、指示された動作内容と実際の動作結果を比較して異常の検知や動作の停止を行うIoT機器を導入する。 ・組織は、サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.DE.CM-08
				L2_2_a_PRO	[プロシージャ] ・安全に支障をきたしうる機器等の兆候を発見した際のプロシージャが定められていない	・組織は、セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RS.MA-01
2_2	フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、サイバー空間へ送る機能	データがIoT機器・サイバー空間間の通信路上で改ざんされる	・通信系路上でデータを改ざんする中間者攻撃等	L2_3_a_ORG	[ソシキ] ・機器を調達する際、改ざん検知機能及び改ざん防止機能を実装しているかを確認していない	・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07
						・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する。	CPS.PR.PS-02
						・組織は、計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、適切なセキュリティ対策を実装した製品を利用する。	CPS.PR.PS-03
		(監視が行き届かない場所に設置された機器の運用中、あるいは廃棄後の盗難等の後)改ざんされたIoT機器がネットワーク接続され、故障や正確でないデータの送信等が発生する	・盗難等により不正な改造を施されたIoT機器によるネットワーク接続 ・悪意を持った自組織内外のヒトによる不正改ざん ・センサーの測定値、閾値、設定の改ざん	L2_3_b_ORG	[ソシキ] ・自組織の情報システムや産業用制御システムに接続している機器の状態を把握できていない	・組織は、ハードウェア及びソフトウェアの真正性と完全性を、取得及び使用前に評価するとともに、稼働中もハードウェア及びソフトウェアの完全性を検証する。	CPS.PR.PS-01
						・組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.PR.PS-06
						・組織は、セキュリティ事象を適切に検知できるよう、IoT機器、サーバ等のハードウェア及びソフトウェアの稼働状況、並びにネットワーク接続状況等を監視する。	CPS.DE.CM-02
				L2_3_b_PEO	[ヒト] ・自組織内外のヒトによるIoT機器に対する物理的な不正行為を防げない	・組織は、IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.PR.AA-07
						・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する。	CPS.PR.PS-02
						・組織は、IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.DE.CM-05
				L2_3_b_COM	[モノ] ・利用している機器に耐タンパー性がなく、物理的な改ざんを防げない	・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する。	CPS.PR.PS-02
				L2_3_b_SYS	[システム] ・定期的に接続機器の完全性を検証していない	・組織は、ハードウェア及びソフトウェアの真正性と完全性を、取得及び使用前に評価するとともに、稼働中もハードウェア及びソフトウェアの完全性を検証する。	CPS.PR.PS-01
					[システム] ・不正な機器がネットワークに接続されたことを適切に検知できない。	・組織は、セキュリティ事象を適切に検知できるよう、ネットワーク及びネットワークサービスを監視する。	CPS.DE.CM-01

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
						・組織は、セキュリティ事象を適切に検知できるよう、IoT機器、サーバ等のハードウェア及びソフトウェアの稼働状況、並びにネットワーク接続状況等を監視する。	CPS.DE.CM-02
					[システム] ・IoT機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	・組織は、IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.PR.AA-07
						・組織は、無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.PR.IR-02
						・組織は、IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.DE.CM-05
				L2_3_b_DAT	[データ] ・IoT機器の廃棄時に、データを削除（又は読み取りできない状態に）する手順がない	・組織は、IoT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するID（識別子）や重要情報（秘密鍵、電子証明書）を削除又は読み取りできない状態にする。	CPS.PR.PS-12
			品質や信頼性の低いIoT機器のネットワーク接続 ・正規の機器を模した偽造品の挿入	L2_3_c_ORG	[ノシキ] ・IoT機器を調達する際、調達製品が信頼できるものかを確認していない	・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06
						・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07
						・組織は、ハードウェア及びソフトウェアの真正性と完全性を、取得及び使用前に評価するとともに、稼働中もハードウェア及びソフトウェアの完全性を検証する。	CPS.PR.PS-01
				[ノシキ] ・運用時にIoT機器やソフトウェアが正規品である（改ざんされていない）ことを確認していない		・組織は、ハードウェア及びソフトウェアの真正性と完全性を、取得及び使用前に評価するとともに、稼働中もハードウェア及びソフトウェアの完全性を検証する。	CPS.PR.PS-01
				L2_3_c_SYS	[システム] ・不正な機器によるネットワーク接続（有線あるいは無線）を防止できない	・組織は、IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で、信頼性の高い方式（例：多要素認証）を用いて認証・認可する。	CPS.PR.AA-02
						・組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.PR.PS-06
					[システム] ・組織外部への不正な通信を適切に検知し、遮断する等の対応ができない	・組織は、セキュリティ事象を適切に検知できるよう、ネットワーク及びネットワークサービスを監視する。	CPS.DE.CM-01
						・組織は、セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容を監視する。	CPS.DE.CM-03
						・組織は、セキュリティ事象を適切に検知できるよう、組織内外の要員による構成要素（モノ／システム等）へのアクセスや操作等の活動を監視する。	CPS.DE.CM-04
					[システム] ・サイバー空間および正規の機器に接続する機器が正規のものかを確認する仕組みが実装されていない	・組織は、承認されたモノとヒト及びプロセスの識別情報と認証情報を発効、管理、確認、取消、監査するプロセスを確立し、実施する。	CPS.PR.AA-01
						・組織は、IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で、信頼性の高い方式（例：多要素認証）を用いて認証・認可する。	CPS.PR.AA-02
				L2_3_c_PRO	[プロセス] ・IoT機器を調達する際に、調達製品が信頼できるものかを確認するプロセスがない	・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05
						・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06
						・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07
						・組織は、ハードウェア及びソフトウェアの真正性と完全性を、取得及び使用前に評価するとともに、稼働中もハードウェア及びソフトウェアの完全性を検証する。	CPS.PR.PS-01
		計測機能に対する物理的な不正行為により、正確でないデータの送信等が発生する	・悪意を持った自組織内外のヒトによる計測機能に対する不正行為	L2_3_d_ORG	[ノシキ] ・IoT機器を調達する際、調達製品が計測セキュリティを考慮しているものかを確認していない	・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07
						・組織は、計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、適切なセキュリティ対策を実装した製品を利用する。	CPS.PR.PS-03
				L2_3_d_SYS	[システム] ・IoT機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	・組織は、IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.PR.AA-07
						・組織は、無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.PR.IR-02
						・組織は、IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.DE.CM-05

■第3層における機能／想定されるセキュリティインシデント／リスク源／対策要件

#	機能	想定される セキュリティインシデント	脅威	脆弱性ID	脆弱性	対策要件	対策要件ID			
3_共通	下記すべてに関わる ・データを加工・分析する機能 ・データを保管する機能 ・データを送受信する機能	サービス拒否攻撃により、関係する他組織における自組織のデータを取り扱うシステムが停止する	・システムを構成するサーバ等の電算機器、通信機器等に対するサービス拒否攻撃 ・妨害電波の発信	L3_3_b_ORG	[ソシキ] ・データの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない	・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06			
						・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07			
						・組織は、取引先等の関係する他組織が契約上の義務を果たしていることを確認するために、監査、テスト結果、又は他の形式の評価を使用して定期的に評価する。	CPS.GV.SC-08			
				L3_3_c_ORG	[ソシキ] ・サービスサプライヤーに対して、組織、システム等の信頼性を契約前、契約後に確認していない	・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06			
						・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07			
						・組織は、取引先等の関係する他組織が契約上の義務を果たしていることを確認するために、監査、テスト結果、又は他の形式の評価を使用して定期的に評価する。	CPS.GV.SC-08			
				L3_3_c_SYS	[システム] ・IoT機器を含む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)が確保されていない	・組織は、平時及び有事において、システム及びサービスの継続稼働に関する要件を達成するための仕組みを実装する。	CPS.PR.IR-03			
						・組織は、サイバー攻撃（例：ランサムウェア、サービス拒否攻撃等）を受けた場合でも、攻撃による影響を最小限に抑え、重要な機能を維持できるよう、十分なリソース（例：ヒト、モノ、システム）を確保する。	CPS.PR.IR-04			
	サイバー空間におけるデータ保護を規定する法規制等への違反が発生する	・データ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・データ保管エリアに対する不正なエンティティの物理的な侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし	・データ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・データ保管エリアに対する不正なエンティティの物理的な侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし	L3_4_a_ORG	[ソシキ] ・保護すべきデータの管理に関する組織内の責任が明確でない [ソシキ] ・対応が必要なデータ保護に関する法規制等を十分に認識していない	・組織は、リソース（例：モノ、データ、システム）を機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.ID.AM-04			
						・組織は、サイバーセキュリティに関する法的要求事項や、規制上の要件、契約上の要求事項（プライバシー及び市民的自由の義務を含む）、及び業界のガイドライン等を理解した上で、それらを考慮した社内ルールを策定する。	CPS.GV.OC-02			
						・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.PR.DS-01			
				L3_4_a_PEO	[ヒト] ・自組織の保護すべきデータのセキュリティ上の扱いについて、関係者が十分に認識していない	・組織は、自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.PR.AT-01			
						・組織は、自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.PR.AT-02			
				L3_4_a_PRO	[プロシージャ] ・データの取り扱いについて、必要なプロシージャを規定していない [プロシージャ] ・データの取り扱いについて、必要なプロシージャを満たしているかを確認していない	・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.PR.DS-01			
						・組織は、セキュリティ事象を適切に検知できるよう、組織内外の要員による構成要素（モノ/システム等）へのアクセスや操作等の活動を監視する。	CPS.DE.CM-04			
					L3_4_a_DAT	[データ] ・複数の組織、システム等に個人情報等が分散して所在している [データ] ・自組織で扱うデータが保護が必要な特定の種類のデータであることが識別されていない	・組織は、保有するデータ及びメタデータの一覧を作成し、適切に管理する。	CPS.ID.AM-05		
				・組織は、リソース（例：モノ、データ、システム）を機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。			CPS.ID.AM-04			
				・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。			CPS.PR.DS-01			
				一部の関係者だけで共有する秘密性の高いデータのセキュリティ要求が設定・対応されていない	・データ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・データ保管エリアに対する不正なエンティティの物理的な侵入 ・正規ユーザによる内部不正 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし	・データ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・データ保管エリアに対する不正なエンティティの物理的な侵入 ・正規ユーザによる内部不正 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし	L3_4_b_ORG	[ソシキ] ・対応が必要なデータ保護に関する法規制等を十分に認識していない	・組織は、サイバーセキュリティに関する法的要求事項や、規制上の要件、契約上の要求事項（プライバシー及び市民的自由の義務を含む）、及び業界のガイドライン等を理解した上で、それらを考慮した社内ルールを策定する。	CPS.GV.OC-02
									・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.PR.DS-01
									・組織は、自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.PR.AT-01
							L3_4_b_PEO	[ヒト] ・自組織の保護すべきデータのセキュリティ上の扱いについて、関係者が十分に認識していない	・組織は、自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.PR.AT-02
	L3_4_b_PRO	[プロシージャ] ・データの取り扱いについて、必要なプロシージャを規定していない [プロシージャ] ・データの取り扱いについて、必要なプロシージャを満たしているかを確認していない	・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。				CPS.PR.DS-01			
			・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。				CPS.PR.DS-01			
	L3_4_b_SYS	[システム] ・データを扱うシステムにおいてデータの秘密性に応じた設計がなされていない	・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。				CPS.PR.DS-01			
			・組織は、保存しているデータの機密性、完全性、及び可用性を保護する。				CPS.PR.DS-02			
			・組織は、セキュアなソフトウェア開発プラクティス（例：設計段階でのセキュリティレビュー、セキュアコーディング規約の適用、リリース前の脆弱性診断）をシステム開発ライフサイクルに統合し、その実施状況を確認する。	CPS.PR.PS-05						

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
				L3_4_b_DAT	[データ] ・複数の組織、システム等に個人情報等が分散して所在している	・組織は、保有するデータ及びメタデータの一覧を作成し、適切に管理する。	CPS.ID.AM-05
					[データ] 自組織で扱うデータが保護が必要な特定の種類のデータであることが識別されていない	・組織は、リソース（例：モノ、データ、システム）を機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.ID.AM-04
						・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.PR.DS-01
3_1	データを加工・分析する機能	関係する他組織で管理している(データ加工・分析)領域から自組織の保護すべきデータが漏洩する	・他組織の管理するデータ加工・分析システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・他組織の管理するデータ加工・分析エリアに対する不正なエンティティの物理的な侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・他組織のエンティティによる保護すべきデータの適切でない持出行為	L3_1_b_ORG	[ソシキ] ・データを加工・分析する組織、システム等の安全性・信頼性を契約前、契約後に確認していない	・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06
						・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07
						・組織は、取引先等の関係する他組織が契約上の義務を果たしていることを確認するために、監査、テスト結果、又は他の形式の評価を使用して定期的に評価する。	CPS.GV.SC-08
				L3_1_b_PEO	[ヒト] ・データの加工・分析を委託する組織における要員の信頼性を契約前、契約後に確認していない	・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06
						・組織は、取引先等の関係する他組織が契約上の義務を果たしていることを確認するために、監査、テスト結果、又は他の形式の評価を使用して定期的に評価する。	CPS.GV.SC-08
				L3_1_b_DAT	[データ] ・セキュリティ水準が統一されていない複数の組織、システム等に自組織の保護すべき情報が分散して所在している	・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05
						・組織は、リソース（例：モノ、データ、システム）を機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.ID.AM-04
						・組織は、保有するデータ及びメタデータの一覧を作成し、適切に管理する。	CPS.ID.AM-05
		データ加工・分析システムが誤動作することで、適切でない分析結果が出力される	・データ加工・分析システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・データ加工・分析システムに対する攻撃コードを含んだ許容範囲外のインプットデータ	L3_3_d_ORG	[ソシキ] ・データを加工・分析する組織、システム等の安全性・信頼性を契約前、契約後に確認していない	・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06
						・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07
						・組織は、取引先等の関係する他組織が契約上の義務を果たしていることを確認するために、監査、テスト結果、又は他の形式の評価を使用して定期的に評価する。	CPS.GV.SC-08
				L3_3_d_SYS	[システム] ・データを加工・分析するシステムにおいて、セキュアでない設定がなされている	・組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.PR.PS-06
						・組織は、自組織の資産の脆弱性を特定し、対応する資産と紐づけて管理する。	CPS.ID.RA-01
					[システム] ・データを加工・分析するシステムにおいて、対処すべき脆弱性が放置されている	・組織は、組織内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.ID.RA-02
						・組織は、脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.PR.PS-08
						・組織は、IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.PR.PS-09
						・組織は、自組織のIoT機器、サーバ等に対する保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.PR.PS-10
						・組織は、自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.DE.CM-06
				[システム] ・システム上でデータが十分に保護されていない		・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.PR.DS-01
						・組織は、保存しているデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-02
						・組織は、伝送中のデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-03
						・組織は、使用中のデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-04
						・組織は、データ（例：構成要素の設定情報、業務データ等を含む）に対し、定期的なバックアップを実施し、バックアップデータの保護及び復旧のテストを行う。	CPS.PR.DS-06
						・組織は、セキュリティインシデントに関するデータ及びメタデータ（インシデント対応において実施した措置の履歴等を含む）を収集し、それらの完全性を確保するとともに、取得元及び取得時点等が参照可能な状態で保管する。	CPS.RS.AN-01
						・組織は、セキュリティインシデント発生後に、根本原因を特定するためのデジタルフォレンジックを実施する。その際、調査過程の記録を改ざんされない形で保管する。	CPS.RS.AN-02

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
					[システム] ・インプットとなるデータを十分に確認していない	・組織は、サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	CPS.DE.CM-07
						・組織は、指示された動作内容と実際の動作結果を比較して異常の検知や動作の停止を行うIoT機器を導入する。 ・組織は、サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.DE.CM-08
						・組織は、セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、継続的にログを記録し、レビューする。	CPS.PR.PS-11
						・組織は、セキュリティ事象を適切に検知できるよう、ネットワーク及びネットワークサービスを監視する。	CPS.DE.CM-01
						・組織は、セキュリティ事象を適切に検知できるよう、IoT機器、サーバ等のハードウェア及びソフトウェアの稼働状況、並びにネットワーク接続状況等を監視する。	CPS.DE.CM-02
						・組織は、セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容を監視する。	CPS.DE.CM-03
						・組織は、セキュリティ事象を適切に検知できるよう、組織内外の要員による構成要素（モノ／システム等）へのアクセスや操作等の活動を監視する。	CPS.DE.CM-04
3_2	データを保管する機能	自組織で管理している(データ保管)領域から関係する他組織の保護すべきデータが漏洩する	・他組織の管理するデータ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・他組織の管理するデータ保管エリアに対する不正なエンティティの物理的侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・自組織における悪意あるエンティティによる保護すべきデータの持出し	L3_1_a_ORG	[ソシキ] ・保護すべきデータの管理に関する組織内の責任が明確でない	・組織は、リソース（例：モノ、データ、システム）を機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.ID.AM-04
				L3_1_a_SYS	[システム] ・関係する他組織の保護すべきデータを格納するシステムにおいて、セキュアでない設定がなされている	・組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.PR.PS-06
				L3_1_a_SYS	[システム] ・自組織のシステムにおいて、対処すべき脆弱性が放置されている	・組織は、自組織の資産の脆弱性を特定し、対応する資産と組づけて管理する。	CPS.ID.RA-01
						・組織は、組織内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.ID.RA-02
						・組織は、脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.PR.PS-08
						・組織は、IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.PR.PS-09
						・組織は、自組織のIoT機器、サーバ等に対する保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.PR.PS-10
						・組織は、自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.DE.CM-06
				L3_1_a_SYS	[システム] 保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	・組織は、承認されたモノとヒト及びプロセスの識別情報と認証情報を発効、管理、確認、取消、監査するプロセスを確立し、実施する。	CPS.PR.AA-01
						・組織は、IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で、信頼性の高い方式（例：多要素認証）を用いて認証・認可する。	CPS.PR.AA-02
				L3_1_a_SYS	[システム] ・IoT機器、サーバ等の設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	・組織は、IoT機器、サーバ等の設置エリアの施設、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.PR.AA-07
						・組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.PR.PS-06
						・組織は、無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.PR.IR-02
				L3_1_a_SYS	[システム] ・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない	・組織は、セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、継続的にログを記録し、レビューする。	CPS.PR.PS-11
						・組織は、セキュリティ事象を適切に検知できるよう、ネットワーク及びネットワークサービスを監視する。	CPS.DE.CM-01
						・組織は、セキュリティ事象を適切に検知できるよう、IoT機器、サーバ等のハードウェア及びソフトウェアの稼働状況、並びにネットワーク接続状況等を監視する。	CPS.DE.CM-02
						・組織は、セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容を監視する。	CPS.DE.CM-03
						・組織は、セキュリティ事象を適切に検知できるよう、組織内外の要員による構成要素（モノ／システム等）へのアクセスや操作等の活動を監視する。	CPS.DE.CM-04
						・組織は、潜在的なセキュリティ事象について分析を行い、当該事象の内容を把握する。	CPS.DE.AE-01
						・組織は、セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RS.MA-01
						・組織は、セキュリティインシデントによる被害の拡大を最小限に抑え、原因の除去又は影響の低減を行う。	CPS.RS.MI-01
				L3_1_a_PRO	[プロセス] ・他組織から管理を委託されるデータの機密区分および必要なセキュリティ対策について確認するプロセスがない	・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05
				L3_1_a_PRO		・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.PR.DS-01
						・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.PR.DS-01
				L3_1_a_DAT	[データ] ・他組織から管理を委託されているデータの保護に係る区分が明確になっていない	・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.PR.DS-01

#	機能	想定される	リスク源		対策要件				
		セキュリティインシデント	脅威	脆弱性ID	脆弱性	対策要件ID			
					[データ] ・定められた機密区分に沿った情報の保護が実装されていない	・組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.PR.DS-01		
					・組織は、保存しているデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-02			
					・組織は、伝送中のデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-03			
					・組織は、使用中のデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-04			
					・組織は、データ（例：構成要素の設定情報、業務データ等を含む）に対し、定期的なバックアップを実施し、バックアップデータの保護及び復旧のテストを行う。	CPS.PR.DS-06			
					・組織は、セキュリティインシデントに関するデータ及びメタデータ（インシデント対応において実施した措置の履歴等を含む）を収集し、それらの完全性を確保するとともに、取得元及び取得時点等が参照可能な状態で保管する。	CPS.RS.AN-01			
					・組織は、セキュリティインシデント発生後に、根本原因を特定するためのデジタルフォレンジックを実施する。その際、調査過程の記録を改ざんされない形で保管する。	CPS.RS.AN-02			
		関係する他組織で管理している(データ保管)領域から自組織の保護すべきデータが漏洩する	・他組織の管理するデータ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・他組織の管理するデータ保管エリアに対する不正なエンティティの物理的侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・自組織における悪意あるエンティティによる保護すべきデータの持出し	L3_1_c_ORG	[ソシキ] ・データを保管する組織、システム等の安全性を契約前、契約後に確認していない	・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06		
						・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07		
						・組織は、取引先等の関係する他組織が契約上の義務を果たしていることを確認するために、監査、テスト結果、又は他の形式の評価を使用して定期的に評価する。	CPS.GV.SC-08		
						L3_1_c_PEO	[ヒト] ・データの加工を委託する組織における要員の信頼性を契約前、契約後に確認していない	・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06
								・組織は、取引先等の関係する他組織が契約上の義務を果たしていることを確認するために、監査、テスト結果、又は他の形式の評価を使用して定期的に評価する。	CPS.GV.SC-08
						L3_1_c_DAT	[データ] ・セキュリティ水準が統一されていない複数の組織、システム等に自組織の保護すべき情報が分散して所在している	・組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.GV.SC-05
		・組織は、リソース（例：モノ、データ、システム）を機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.ID.AM-04						
						・組織は、保有するデータ及びメタデータの一覧を作成し、適切に管理する。	CPS.ID.AM-05		
						関係する他組織で保管中の自組織の保護すべきデータが改ざんされる	・窃取したID、パスワード等を利用した正規ユーザへのなりすまし	L3_2_a_DAT	[データ] ・保管中のデータに改ざんを検知するメカニズムがない
・組織は、データの取得元、加工履歴等をライフサイクル全体に渡って維持・更新・管理する。	CPS.PR.DS-05								
3_3	データを送受信する機能	関係する他組織で使用中の自組織の保護すべきデータが改ざんされる	・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・通信系路上でデータを改ざんする中間者攻撃等	L3_2_b_DAT	[データ] ・通信路上でデータが十分に保護されていない	・組織は、伝送中のデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-03		
					[データ] ・使用中のデータに改ざんを検知するメカニズムがない	・組織は、使用中のデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-04		
		(なりすまし等をした)ソシキ/ヒト/モノ等から不適切なデータを受信する	・不正な組織/ヒト/モノ/システムによる正規エンティティへのなりすまし ・改ざん等された正規なモノ/システムからの適切でないデータの受信	L3_3_a_ORG	[ソシキ] ・データ送信元となるデータの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない	・組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.GV.SC-06		
						・組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.GV.SC-07		
						・組織は、取引先等の関係する他組織が契約上の義務を果たしていることを確認するために、監査、テスト結果、又は他の形式の評価を使用して定期的に評価する。	CPS.GV.SC-08		
				L3_3_a_PEO	[ヒト] ・自組織の保護すべきデータのセキュリティ上の扱いについて、外部委託先の担当者が十分に認識していない	・組織は、自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.PR.AT-02		
						L3_3_a_SYS	[システム] ・データを収集・分析等するシステムにおいて、対処すべき脆弱性が放置されている	・組織は、自組織の資産の脆弱性を特定し、対応する資産と紐づけて管理する。	CPS.ID.RA-01
								・組織は、組織内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.ID.RA-02
		・組織は、脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.PR.PS-08						
		・組織は、IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.PR.PS-09						
		・組織は、自組織のIoT機器、サーバ等に対する保守を、適用先のモノ、システムオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.PR.PS-10						
		・組織は、自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.DE.CM-06						
						[システム] ・通信路が適切に保護されていない	・組織は、伝送中のデータの機密性、完全性、及び可用性を保護する。	CPS.PR.DS-03	
						・組織は、ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等して、認可されていないアクセス及び使用からネットワーク及び環境を保護する。	CPS.PR.IR-01		

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
					[システム] ・ 早期にセキュリティ上の異常を素早く検知し、対処する ような仕組みが自組織のシステムに実装されていない	・ 組織は、セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、継続的にログを記録し、レビューする。	CPS.PR.PS-11
						・ 組織は、セキュリティ事象を適切に検知できるよう、ネットワーク及びネットワークサービスを監視する。	CPS.DE.CM-01
						・ 組織は、セキュリティ事象を適切に検知できるよう、IoT機器、サーバ等のハードウェア及びソフトウェアの稼働状況、並びにネットワーク接続状況等を監視する。	CPS.DE.CM-02
						・ 組織は、セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容を監視する。	CPS.DE.CM-03
						・ 組織は、セキュリティ事象を適切に検知できるよう、組織内外の要員による構成要素（モノ／システム等）へのアクセスや操作等の活動を監視する。	CPS.DE.CM-04
						・ 組織は、潜在的なセキュリティ事象について分析を行い、当該事象の内容を把握する。	CPS.DE.AE-01
						・ 組織は、セキュリティインシデントによる被害の拡大を最小限に抑え、原因の除去又は影響の低減を行う。	CPS.RS.MI-01
				L3_3_a_DAT	[システム] ・ サイバー空間との通信開始時に、通信相手を識別・認証していない	・ 組織は、承認されたモノとヒト及びプロセスの識別情報と認証情報を発効、管理、確認、取消、監査するプロセスを確立し、実施する。	CPS.PR.AA-01
						・ 組織は、IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で、信頼性の高い方式（例：多要素認証）を用いて認証・認可する。	CPS.PR.AA-02
						・ 組織は、サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	CPS.DE.CM-07
					[データ] ・ 通信相手のエンドポイントから送信されるデータをフィルタリングする仕組みが導入・運用されていない	・ 組織は、指示された動作内容と実際の動作結果を比較して異常の検知や動作の停止を行うIoT機器を導入する。 ・ 組織は、サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.DE.CM-08