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#	脆弱性		
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 ・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	L1_1_a_ORG	[組織] ・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	あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、関係者(サプライヤー、第三者プロバイダ等を含む)に共有する	CPS.BE-2
						リソース（例：ヒト、モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、関係者に伝達する	CPS.AM-6
						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	CPS.SC-1
						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	CPS.SC-2
						システムを管理するためのシステム開発ライフサイクルを導入し、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	CPS.IP-3
				L1_1_a_PEO	[ヒト] ・自身が関わりうるセキュリティリスクに対して十分な認識を有していない	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	CPS.AT-1
					[ヒト] ・ヒトに関わるセキュリティリスクに対するガバナンスが十分でない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する	CPS.SC-8
						人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含めている	CPS.IP-9
				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されていない	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	CPS.AM-1
						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	CPS.AM-5
						承認されたモノとヒトおよびプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する	CPS.AC-1
						ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理している	CPS.AE-1
						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	CPS.CM-5
						機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
				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	自組織の資産の脆弱性を特定し、文書化する	CPS.RA-1
						自組織の資産に対する脅威を特定し、文書化する	CPS.RA-3
						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	CPS.RA-5
						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	CPS.RA-6
						リスクアセスメント結果およびサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する	CPS.RM-2
						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	CPS.RA-4
					[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	セキュリティ対策組織(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	CPS.RA-2
						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	CPS.IP-10
						機器等の構成管理では、設定情報およびネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
						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	CPS.IP-2
						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.CM-7
						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	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	CPS.MA-2
						自組織のIoT機器、サーバ等に対する遠隔保守は、承認を得て、ログを記録し、不正アクセスを防げる形で実施している	CPS.DS-2
					[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	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	CPS.AC-1
						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	CPS.AC-9
						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.GV-3
						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	CPS.AC-5
						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	CPS.AC-6
					[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	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.AC-2
						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.IP-5
						重要度の高いIoT機器、サーバ等が設置されたエリアに対する物理的アクセスの記録や監視を行う	CPS.CM-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	CPS.PT-2
					[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	ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理している	CPS.AE-1
						組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する	CPS.CM-1
						危険性の高いセキュリティ事象を適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューしている	CPS.PT-1
						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	CPS.CM-5
						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	CPS.RP-1
				L1_1_a_DAT	[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	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.GV-3
						サプライヤおよび第三者パートナーが、契約上の義務を果たしているかどうかを確認するために、監査、テスト結果、または他の形式の評価を利用して定期的に評価する	CPS.SC-5
						情報(データ)を適切な強度の方式で暗号化して保管する	CPS.DS-1
						IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する	CPS.DS-2
						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	CPS.DS-3
						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	CPS.DS-4

#	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#	脆弱性		
						自組織の保護すべきデータが不適切なエンティティに渡ったことを検知した場合、ファイル閲覧停止等の適切な対応を実施する	CPS.DS-8
				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	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、情報の共有方法等に関する方針を明確にする	CPS.GV-1
						サイバーセキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う	CPS.GV-4
						関係者のサイバーセキュリティリスクマネジメントの実施状況について確認する。また、自組織の事業に関する自組織および関係者の責任範囲を明確化し、セキュリティマネジメントの実施状況を確認するプロセスを確立し、実施する。	CPS.RM-1
						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	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.SC-4
						取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する	CPS.SC-5
						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.SC-6
						取引先等の関係する他組織との契約が終了する際(例：契約期間の満了、サポートの終了)に実施すべきプロシージャを策定し、運用する	CPS.SC-10
						サプライチェーンに係るセキュリティ対策基準および関係するプロシージャ等を継続的に改善する	CPS.SC-11
						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	CPS.IP-7
		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	L1_1_b_ORG	[組織] ・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	あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、関係者(サプライヤー、第三者プロバイダ等を含む)に共有する	CPS.BE-2
						リソース（例：ヒト、モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、関係者に伝達する	CPS.AM-6
						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	CPS.SC-1
						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	CPS.SC-2
						システムを管理するためのシステム開発ライフサイクルを導入し、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	CPS.IP-3
				L1_1_b_PEO	[ヒト] ・自身が関わりうるセキュリティリスクに対して十分な認識を有していない	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	CPS.AT-1
					[ヒト] ・ヒトに関わるセキュリティリスクに対するガバナンスが十分でない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する	CPS.SC-8
						人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含めている	CPS.IP-9
				L1_1_b_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されていない	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	CPS.AM-1
						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	CPS.AM-5
						承認されたモノとヒトおよびプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する	CPS.AC-1
						ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理している	CPS.AE-1
						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	CPS.CM-5
						機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
				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	自組織の資産の脆弱性を特定し、文書化する	CPS.RA-1
						自組織の資産に対する脅威を特定し、文書化する	CPS.RA-3
						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	CPS.RA-5
						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	CPS.RA-6
						リスクアセスメント結果およびサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する	CPS.RM-2
						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	CPS.RA-4
					[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	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	CPS.AC-1
						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	CPS.AC-9
						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.GV-3
						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	CPS.AC-5
						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	CPS.AC-6
				L1_1_b_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	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、情報の共有方法等に関する方針を明確にする	CPS.GV-1
						サイバーセキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う	CPS.GV-4
						関係者のサイバーセキュリティリスクマネジメントの実施状況について確認する。また、自組織の事業に関する自組織および関係者の責任範囲を明確化し、セキュリティマネジメントの実施状況を確認するプロセスを確立し、実施する。	CPS.RM-1
						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	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.SC-4
						取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する	CPS.SC-5
						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.SC-6
						取引先等の関係する他組織との契約が終了する際に実施すべきプロシージャを策定し、運用する	CPS.SC-10
						サプライチェーンに係るセキュリティ対策基準および関係するプロシージャ等を継続的に改善する	CPS.SC-11
						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	CPS.IP-7
				L1_1_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	IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する	CPS.DS-2
						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	CPS.DS-3
					[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	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	CPS.DS-10

#	機能	想定される セキュリティインシデント	リスク源 脅威	脆弱性#	脆弱性	対策要件	対策要件ID
		サービス拒否攻撃により、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DoS攻撃	L1_1_c_ORG	[組織] ・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	あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、関係者(サプライヤー、第三者プロバイダ等を含む)に共有する	CPS.BE-2
						リソース（例：ヒト、モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、関係者に伝達する	CPS.AM-6
						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	CPS.SC-1
						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	CPS.SC-2
						システムを管理するためのシステム開発ライフサイクルを導入し、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	CPS.IP-3
				L1_1_c_PEO	[ヒト] ・自身が関わりうるセキュリティリスクに対して十分な認識を有していない	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	CPS.AT-1
					[ヒト] ・ヒトに関わるセキュリティリスクに対するガバナンスが十分でない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する	CPS.SC-8
						人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含めている	CPS.IP-9
				L1_1_c_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されていない	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	CPS.AM-1
						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	CPS.AM-5
						承認されたモノとヒトおよびプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する	CPS.AC-1
						ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理している	CPS.AE-1
						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	CPS.CM-5
						機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
				L1_1_c_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	自組織の資産の脆弱性を特定し、文書化する	CPS.RA-1
						自組織の資産に対する脅威を特定し、文書化する	CPS.RA-3
						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	CPS.RA-5
						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	CPS.RA-6
						リスクアセスメント結果およびサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する	CPS.RM-2
						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	CPS.RA-4
					[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	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	CPS.PT-2
						組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する	CPS.CM-1
					[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	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	CPS.DS-5
						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	CPS.DS-6
				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	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、情報の共有方法等に関する方針を明確にする	CPS.GV-1
						サイバーセキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う	CPS.GV-4
						関係者のサイバーセキュリティリスクマネジメントの実施状況について確認する。また、自組織の事業に関する自組織および関係者の責任範囲を明確化し、セキュリティマネジメントの実施状況を確認するプロセスを確立し、実施する。	CPS.RM-1
						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	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.SC-4
						取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する	CPS.SC-5
						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.SC-6
						取引先等の関係する他組織との契約が終了する際に実施すべきプロシージャを策定し、運用する	CPS.SC-10
						サプライチェーンに係るセキュリティ対策基準および関係するプロシージャ等を継続的に改善する	CPS.SC-11
						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	CPS.IP-7
		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	[組織] ・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	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	CPS.GV-2
						監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティインシデントを検知する	CPS.DP-2
				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	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	CPS.AT-1
				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	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	CPS.GV-2
				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	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	CPS.GV-2
				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	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	CPS.GV-2
				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	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	CPS.GV-2
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	[組織] ・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	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	CPS.AE-2
						セキュリティ対策組織(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	CPS.RA-2
						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.DP-3
						監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する	CPS.DP-2
						セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知における自組織とサービスプロバイダーが担う役割と負う責任を明確にする	CPS.DP-1
						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.DP-4

#	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#	脆弱性		
					[組織] ・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	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	CPS.AE-2
						セキュリティ対策組織(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	CPS.RA-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、セキュリティ運用プロセスを継続的に改善する	CPS.IM-1
						セキュリティインシデントへの対応から教訓を導き出し、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	CPS.IM-2
				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	セキュリティインシデント発生時の対応の内容や優先順位、対策範囲を明確にするため、セキュリティ運用プロセスを定め、運用する	CPS.RP-1
						自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施する	CPS.AT-1
				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	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、特定方法を定める	CPS.AM-2
						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.AM-3
						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	CPS.AN-1
				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	組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する	CPS.CM-1
						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、セキュリティ事象を正確に特定する	CPS.AE-3
				L1_3_a_PRO	[プロシージャ] ・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	セキュリティインシデント発生時の対応の内容や優先順位、対策範囲を明確にするため、セキュリティ運用プロセスを定め、運用する	CPS.RP-1
						セキュリティ事象の危険度の判定基準を定める	CPS.AE-5
						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	CPS.AN-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	CPS.MI-1
						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	CPS.AN-2
						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	CPS.AN-3
					[プロシージャ] ・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	自然災害時における対応方針および対応手順を定めている事業継続計画又はコンティンジェンシープランの中にセキュリティインシデントを位置づける	CPS.RP-3
						セキュリティインシデント発生後の情報公表時のルールを策定し、運用する	CPS.CO-1
						事業継続計画又はコンティンジェンシープランの中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける	CPS.CO-2
						復旧活動について内部および外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又はコンティンジェンシープランの中に位置づける	CPS.CO-3
		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	[組織] ・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	組織内の通信ネットワーク構成図及び、データフロー図を作成し、保管する	CPS.AM-4
						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	CPS.AM-5
						ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理するプロシージャを確立し、実施する	CPS.AE-1
						機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
						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	CPS.CM-5
					[組織] ・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	サプライチェーンにおいて、自組織が担う役割を特定し共有する	CPS.BE-1
						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	CPS.BE-3
						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	CPS.AM-7
						自組織だけでなく、関係者と共同でセキュリティリスクの管理プロセスを確立、承認し、運用する	CPS.RM-1
				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	セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する	CPS.RP-2
						自組織におけるセキュリティインシデントに関係しうる関係組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練(トレーニング)、セキュリティ教育を実施する	CPS.AT-2
						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	CPS.SC-9
				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	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、回収等の適切な対応を行う	CPS.RP-4
					[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	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、特定方法を定める	CPS.AM-2
						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の生産活動の記録に関する内部規則を整備し、運用する	CPS.AM-3
				L1_3_b_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	セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する	CPS.RP-2
						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	CPS.AE-4
		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	[組織] ・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	組織内の通信ネットワーク構成図及び、データフロー図を作成し、保管する	CPS.AM-4
						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	CPS.AM-5
						ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理するプロシージャを確立し、実施する	CPS.AE-1
						機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
						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	CPS.CM-5
					[組織] ・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	サプライチェーンにおいて、自組織が担う役割を特定し共有する	CPS.BE-1
						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	CPS.BE-3
						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	CPS.AM-7
						自組織だけでなく、関係者と共同でセキュリティリスクの管理プロセスを確立、承認し、運用する	CPS.RM-1
				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	セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する	CPS.RP-2

#	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#	脆弱性		
						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	CPS.AT-1
				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	セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する	CPS.RP-2
1_3	フィジカル空間現実世界での製品・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、危機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	[組織] ・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	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	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.SC-4
						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.SC-6
						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	CPS.SC-7
				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。	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、教育を実施する	CPS.AT-1
				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	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	CPS.SC-4
						保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する	CPS.DS-7
				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	IoT機器、サーバ等の起動時に、起動するソフトウェアの完全性を検証し、不正なソフトウェアの起動を防止する	CPS.DS-10
						ハードウェアの完全性を検証するために整合性チェックメカニズムを使用する	CPS.DS-11
						IoT機器やソフトウェアが正規品であることを定期的(起動時等)に確認する	CPS.DS-12

■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#	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、3層へ送る機能 ・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ように表示したりする機能	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	[組織] ・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	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	CPS.AM-1
						IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する	CPS.IP-1
						機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
						IoT機器の導入後に、追加するソフトウェアを制限する	CPS.IP-2
					[組織] ・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。	セキュリティ対策組織(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	CPS.RA-2
						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	CPS.IP-7
						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.IP-8
						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	CPS.IP-10
						IoT 機器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	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	CPS.MA-1
						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	CPS.MA-2
				L2_1_a_COM	[モノ] ・利用している機器が十分なセキュリティ機能を実装していない	IoT機器およびIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する	CPS.RA-4
						IoT機器およびIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティおよび関連するセーフティのリスクに対して適宜対応する	CPS.RA-6
						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	CPS.SC-4
						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、計測セキュリティの観点が考慮された製品を利用する	CPS.DS-16
				L2_1_a_PRO	[プロシージャ] ・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シージャがない	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	CPS.SC-4
						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、計測セキュリティの観点が考慮された製品を利用する	CPS.DS-16
						IoT機器およびIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を安全性の観点も踏まえて確認する	CPS.RA-4
						IoT機器およびIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティリスクに対して適宜対応する	CPS.RA-6
	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	[組織] ・ネットワークの適正利用を定期的に確認していない	危険性の高いセキュリティ事象を適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューしている	CPS.PT-1
						ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理している	CPS.AE-1
						組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する	CPS.CM-1
				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	IoT機器、サーバ等の設定変更管理プロセスを導入し、運用する	CPS.IP-1
						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	CPS.PT-2
				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	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	CPS.AC-9
						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.AC-4
						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	CPS.AC-7
						IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する	CPS.AC-8
				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	IoT機器の初期設定手順(パスワード等)及び設定値の更新方法を定義する	CPS.IP-1
	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へのなりすまし		L2_1_c_ORG	[組織] ・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	機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
				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	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	CPS.AC-5
						特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、二つ以上の認証機能を組み合わせた多要素認証を採用する	CPS.AC-6
					[システム] ・システムにおいて対処すべき脆弱性が適切に対処されていない	セキュリティ対策組織(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	CPS.RA-2
						機器等の構成管理では、設定情報およびネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
						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	CPS.IP-2
						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.CM-7
						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	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	CPS.MA-1
						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	CPS.MA-2
		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DoS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	・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	CPS.DS-5
						・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	CPS.DS-6
						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	CPS.IP-4
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ように表示したりする機能	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	L2_2_a_ORG	[組織] ・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	IoT機器およびIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を安全性の観点も踏まえて確認する	CPS.RA-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	CPS.SC-4
						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.SC-6
						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	CPS.SC-7
						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.PT-3

#	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#	脆弱性		
				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	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.CM-3
				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	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	CPS.RP-1
						セキュリティインシデント発生時の対応の内容や優先順位、対策範囲を明確にするため、セキュリティ運用マニュアルを定め、運用する	CPS.RP-1
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、3層へ送る機能	(MAC等の改ざん検知機能に対応していない機器から生成された)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	[組織] ・機器を調達する際、改ざん検知の機能を実装しているかを確認していない	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	CPS.SC-4
						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、計測セキュリティの観点が考慮された製品を利用する	CPS.DS-16
		(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、故障や正確でない情報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	L2_3_b_ORG	[組織] ・機器の状態を把握できていない	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	CPS.AM-1
						IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する	CPS.IP-1
						機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
				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	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する	CPS.SC-8
						・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.AC-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	CPS.CM-2
				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	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	CPS.DS-7
				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	IoT機器、サーバ等の起動時に、起動するソフトウェアの完全性を検証し、不正なソフトウェアの起動を防止する	CPS.DS-9
						ハードウェアの完全性を検証するために整合性チェックメカニズムが使用されている	CPS.DS-11
					[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	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.AC-2
						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.IP-5
						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	CPS.CM-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	CPS.PT-2
				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	IoT機器、サーバ等の撤去・譲渡・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	CPS.IP-6
		品質や信頼性の低いIoT機器がネットワーク接続され、故障や正確でない情報の送信等が発生する	・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	[組織] ・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	機器調達時に、適切なマネジメントシステムが構築・運用され、問い合わせ窓口やサポート体制等が確立されたIoT機器のサプライヤーを選定する	CPS.SC-2
						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を策定する	CPS.SC-3
						外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する	CPS.SC-4
						取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する	CPS.SC-5
						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.SC-6
						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	CPS.SC-7
					[組織] ・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	IoT機器やソフトウェアが正規品であることを定期的(起動時等)に確認する	CPS.DS-13
				L2_3_c_SYS	[システム] ・不正な機器によるネットワーク接続を防止できない	無線接続先(ユーザーやIoT機器)を正しく認証する	CPS.AC-3
					[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	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	CPS.AC-1
						IoT機器やソフトウェアが正規品であることを定期的(起動時等)に確認する	CPS.DS-13
				L2_3_c_PRO	[プロシージャ] ・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シージャがない	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	CPS.SC-4
						取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する	CPS.SC-5
						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.SC-6
						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	CPS.SC-7

■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	リスク源			対策要件	対策要件ID
			脅威	脆弱性#	脆弱性		
3_共通	下記すべてに関わる ・データをセキュアに加工・分析する機能 ・データをセキュアに保管する機能 ・データをセキュアに送受信する機能	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DoS攻撃	L3_3_b_ORG	[組織] ・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	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	CPS.SC-2
						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を策定する	CPS.SC-3
						外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する	CPS.SC-4
						サプライヤおよび第三者パートナーが、契約上の義務を果たしているかどうかを確認するために、監査、テスト結果、または他の形式の評価を利用して定期的に評価する	CPS.SC-5
						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.SC-6
						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	CPS.SC-7
		攻撃の有無に関わらず、データを取り扱うシステムが停止する	・品質や信頼性の低いシステムによるサービス提供	L3_3_c_ORG	[組織] ・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	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	CPS.SC-2
						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を策定する	CPS.SC-3
						外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する	CPS.SC-4
						サプライヤおよび第三者パートナーが、契約上の義務を果たしているかどうかを確認するために、監査、テスト結果、または他の形式の評価を利用して定期的に評価する	CPS.SC-5
						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.SC-6
						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	CPS.SC-7
				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	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	CPS.DS-5
						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	CPS.DS-6
						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	CPS.IP-4
		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	L3_4_a_ORG	[組織] ・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ない	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.GV-3
				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	自組織の全ての要員に対して、セキュリティインシデント発生を抑止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	CPS.AT-1
				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	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.GV-3
					[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	データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する	CPS.DS-13
				L3_4_a_DAT	[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	組織間で保護すべきデータを交換する場合、当該データの保護に係るセキュリティ要件について、事前に組織間で取り決める	CPS.DS-15
					[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	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	CPS.SC-3
						サプライヤおよび第三者パートナーが、契約上の義務を果たしているかどうかを確認するために、監査、テスト結果、または他の形式の評価を利用して定期的に評価する	CPS.SC-5
		一部の関係者だけで共有する秘匿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 ・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	[組織] ・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ない	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.GV-3
				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	自組織の全ての要員に対して、セキュリティインシデント発生を抑止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	CPS.AT-1
				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	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.GV-3
					[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	データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する	CPS.DS-13
				L3_4_b_DAT	[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	組織間で保護すべきデータを交換する場合、当該データの保護に係るセキュリティ要件について、事前に組織間で取り決める	CPS.DS-15
					[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	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	CPS.SC-3
						サプライヤおよび第三者パートナーが、契約上の義務を果たしているかどうかを確認するために、監査、テスト結果、または他の形式の評価を利用して定期的に評価する	CPS.SC-5
3_1	データをセキュアに加工・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	[組織] ・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	サービスやシステムの運用において、ITSMS認証等を取得しており、サービスマネジメントを効率的、効果的に運営管理するサービスサプライヤーを選定する	CPS.SC-2
						第三者機関によるセキュリティ評価を経て安全性を確認された製品・サービスを提供しているサプライヤーを選定する	CPS.SC-2
						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を策定する	CPS.SC-3
						外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する	CPS.SC-4
						サプライヤおよび第三者パートナーが、契約上の義務を果たしているかどうかを確認するために、監査、テスト結果、または他の形式の評価を利用して定期的に評価する	CPS.SC-5
						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.SC-6
						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	CPS.SC-7
				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	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する	CPS.SC-8
				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	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を策定する	CPS.SC-3
						サプライヤおよび第三者パートナーが、契約上の義務を果たしているかどうかを確認するために、監査、テスト結果、または他の形式の評価を利用して定期的に評価する	CPS.SC-5

#	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#	脆弱性		
		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	[組織] ・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	サービスやシステムの運用において、ITSMS認証等を取得しており、サービスマネジメントを効率的、効果的に運営管理するサービスサプライヤーを選定する	CPS.SC-2
						第三者機関によるセキュリティ評価を経て安全性を確認された製品・サービスを提供しているサプライヤーを選定する	CPS.SC-2
						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を策定する	CPS.SC-3
						外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する	CPS.SC-4
						サプライヤおよび第三者パートナーが、契約上の義務を果たしているかどうかを確認するために、監査、テスト結果、または他の形式の評価を利用して定期的に評価する	CPS.SC-5
						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.SC-6
						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	CPS.SC-7
				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、対処すべき脆弱性が放置されている	セキュリティ対策組織(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	CPS.RA-2
						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	CPS.IP-10
						機器等の構成管理では、設定情報およびネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
						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	CPS.IP-2
						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.CM-7
						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	CPS.MA-1
						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	CPS.MA-2
					[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	情報(データ)を適切な強度の方式で暗号化して保管する	CPS.DS-1
						IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する	CPS.DS-2
						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	CPS.DS-3
					[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	IoT機器、サーバ等において、送受信する情報(データ)の完全性および真正性を動作前に確認する	CPS.CM-4
						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	CPS.CM-3
					[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	ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理している	CPS.AE-1
						組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する	CPS.CM-1
						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	CPS.CM-5
						セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューしている	CPS.PT-1
						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	CPS.RP-1
3_2	データをセキュアに保管する機能	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_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	セキュリティ対策組織(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	CPS.RA-2
						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	CPS.IP-10
						機器等の構成管理では、設定情報およびネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
						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	CPS.IP-2
						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.CM-7
						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	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	CPS.MA-2
					[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	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	CPS.AC-1
						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	CPS.AC-9
						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.GV-3
						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	CPS.AC-5
						特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、二つ以上の認証機能を組み合わせた多要素認証を採用する	CPS.AC-6
					[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	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.AC-2
						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.IP-5
						重要度の高いIoT機器、サーバ等が設置されたエリアに対する物理的アクセスの記録や監視を行う	CPS.CM-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	CPS.PT-2
					[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	ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理している	CPS.AE-1
						組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する	CPS.CM-1
						危険性の高いセキュリティ事象を適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューしている	CPS.PT-1
						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	CPS.CM-5
						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	CPS.RP-1
				L3_1_a_PRO	[プロシージャ] ・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シージャがない	組織間で保護すべきデータを交換する場合、当該データの保護に係るセキュリティ要件について、事前に組織間で取り決める	CPS.DS-15
				L3_1_a_DAT	[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	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.GV-3
						サプライヤおよび第三者パートナーが、契約上の義務を果たしているかどうかを確認するために、監査、テスト結果、または他の形式の評価を利用して定期的に評価する	CPS.SC-5
						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	CPS.AC-7
						情報(データ)を適切な強度の方式で暗号化して保管する	CPS.DS-1
						IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する	CPS.DS-2
						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	CPS.DS-3
						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	CPS.DS-4
						自組織の保護すべきデータが不適切なエンティティに渡ったことを検知した場合、ファイル閲覧停止等の適切な対応を実施する	CPS.DS-8

#	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#	脆弱性		
		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	[組織] ・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	サービスやシステムの運用において、ITSMS認証等を取得しており、サービスマネジメントを効率的、効果的に運営管理するサービスサプライヤーを選定する	CPS.SC-2
						第三者機関によるセキュリティ評価を経て安全性を確認された製品・サービスを提供しているサプライヤーを選定する	CPS.SC-2
						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を策定する	CPS.SC-3
						サプライヤおよび第三者パートナーが、契約上の義務を果たしているかどうかを確認するために、監査、テスト結果、または他の形式の評価を利用して定期的に評価する	CPS.SC-5
						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.SC-6
						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	CPS.SC-7
				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	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する	CPS.SC-8
				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	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を策定する	CPS.SC-3
						サプライヤおよび第三者パートナーが、契約上の義務を果たしているかどうかを確認するために、監査、テスト結果、または他の形式の評価を利用して定期的に評価する	CPS.SC-5
		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	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	CPS.DS-10
3_3	データをセキュアに送受信する機能	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] ・使用中のデータに改ざんを検知するメカニズムがない	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	CPS.DS-10
					[データ] ・通信路上でデータが十分に保護されていない	IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する	CPS.DS-2
						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	CPS.DS-3
		(なりすまし等をした)組織/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/システムによる適切でないデータの送受信	L3_3_a_ORG	[組織] ・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	サービスやシステムの運用において、ITSMS認証等を取得しており、サービスマネジメントを効率的、効果的に運営管理するサービスサプライヤーを選定する	CPS.SC-2
						第三者機関によるセキュリティ評価を経て安全性を確認された製品・サービスを提供しているサプライヤーを選定する	CPS.SC-2
						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を策定する	CPS.SC-3
						外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する	CPS.SC-4
						サプライヤおよび第三者パートナーが、契約上の義務を果たしているかどうかを確認するために、監査、テスト結果、または他の形式の評価を利用して定期的に評価する	CPS.SC-5
						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.SC-6
						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	CPS.SC-7
				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	自組織におけるセキュリティインシデントに関係しうる関係組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練(トレーニング)、セキュリティ教育を実施する	CPS.AT-2
				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	セキュリティ対策組織(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	CPS.RA-2
						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	CPS.IP-10
						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	CPS.MA-1
						機器等の構成管理では、設定情報およびネットワーク接続状況(ネットワーク接続の有無、アクセス先等)およびデータの送受信状況について、継続的に把握する	CPS.CM-6
						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.CM-7
						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	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	CPS.MA-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	CPS.IP-2
					[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	ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理している	CPS.AE-1
						組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する	CPS.CM-1
						セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューしている	CPS.PT-1
						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	CPS.CM-5
						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	CPS.RP-1
				L3_3_a_SYS	[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	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	CPS.AC-1
						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	CPS.AC-8
						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.AC-4
						無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する	CPS.AC-3
				L3_3_a_DAT	[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	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	CPS.CM-3
						IoT機器、サーバ等において、送受信する情報(データ)の完全性および真正性を動作前に確認する	CPS.CM-4