サイバー・フィジカル・セキュリティ対策
フレームワーク（案）

経済産業省　商務情報政策局

サイバーセキュリティ課

目次

サイバー・フィジカル・セキュリティ対策フレームワークの策定にあたって

○ 我が国では、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society5.0」の実現を提唱している。さらに、「Society5.0」へ向けて様々なデータの「つながり」から新たな付加価値を創出していく「Connected Industries」という概念を提唱し、その実現に向けた取組を推進している。

○ 「Society5.0」では、サイバー空間とフィジカル空間が密接に関わることにより、サイバー攻撃がフィジカル空間へ及ぼす影響が大きくなる。また、「Connected Industries」を始めとするネットワーク化の進展は、従来とは異なる、より柔軟で動的なサプライチェーンの構成を可能とし、新たな付加価値を生み出す機会を増大させることになるが、サイバーセキュリティの観点でみれば、防御側の視点では、守るべき範囲が増大する一方で、攻撃者の視点で考えると、攻撃の起点が増えることになる。セキュリティが弱いポイントを一か所見つけるだけで侵入することが可能というサイバー攻撃の特徴を踏まえれば、今まで以上に侵入が容易になりつつあると言える。

○ このような状況においては、一企業が取り組むセキュリティ対策だけでサイバーセキュリティを確保していくことには限界がある。このため、各企業が各製品・サービス等において、セキュリティバイデザインの観点を踏まえて、企画・設計段階からサイバーセキュリティ対策を考慮することに加え、関連企業、取引先等サプライチェーン全体として、ビジネス活動のレジリエンスまで考慮に入れてセキュリティ対策に取り組むことや、個々の主体が厳格に管理することが難しいデータの流通のセキュリティも含めて、サイバーセキュリティ確保に取り組んでいく必要がある。

○ 本フレームワークでは、「Society5.0」における全産業に共通的なセキュリティ対策を 3 つの切り口(「企業間のつながり(従来型サプライチェーン)」、「フィジカル空間とサイバー空間のつながり」、「サイバー空間におけるつながり」)で整理し、それぞれの切り口における守るべきもの、セキュリティリスク、具体的な対策を示している。

○ 本フレームワークは、「Society5.0」における全産業に共通的なセキュリティ対策を示しているが、それぞれの業界や企業により、守るべき重要な資産、人的・

資金的リソース、又は許容できるリスク等が異なることから、本フレームワークを活用して、それぞれの実態に則した脅威・リスクシナリオの想定、リスクアセスメント、具体的な対策の実装などに活用していただきたい。

1．はじめに~サイバーセキュリティを巡る状況の変化

1．1．「Society5.0」、「Connected Industries」が実現する社会

ネットワーク化やIoT（Internet of Things）の利活用が進む中、世界では、ドイツの「インダストリー4.0」等、ものづくり分野でITを最大限に活用し、第4次産業革命とも言うべき変化を先導していく取組が、官民協力の下で打ち出され始めている。我が国においても、平成28年1月22日に閣議決定された「第5期科学技術基本計画」において、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society5.0」を提唱している。さらに、「Society5.0」へ向けて、様々なつながりによる新たな付加価値を創出する「Connected Industries」の実現に向けた新たな産業構造の構築が求められている。

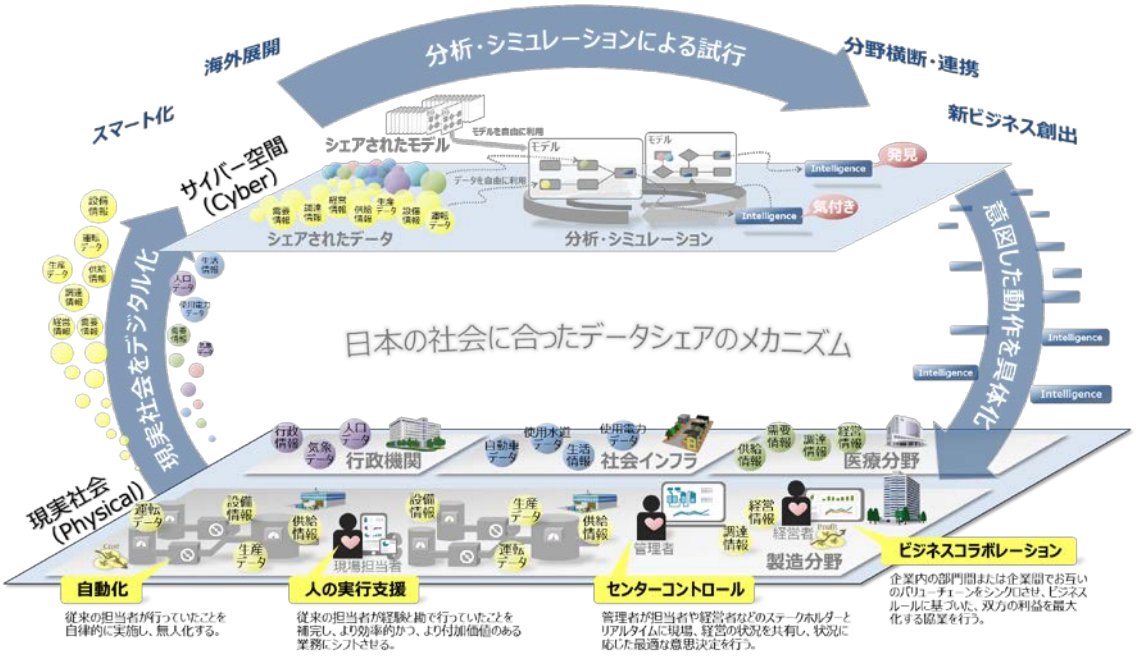


図1 サイバー空間とフィジカル空間のイメージ[1]

[1] 経済産業省「平成27年度我が国経済社会の情報化・サービス化に係る基盤整備(水道事業におけるCPS(サイバーフィジカルシステム)実装のための調査研究)」報告書を基に作成

「Society 5.0」は、狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）に続く、新たな社会を指すものである。

これまでの情報社会（Society 4.0）では、必要な知識や情報が共有されず、新たな価値の創出が困難であったり、また、膨大な情報の中から必要な情報を見つけ、分析する作業に困難や負担が生じるなどの問題があった。

「Society 5.0」で実現する社会は、IoT で全ての人とモノがつながり、様々な知識や情報が共有され、新たな価値が生まれる社会である。また、人工知能（AI）により、多くの情報を分析するなどの面倒な作業から解放される社会である。さらに、「Society 5.0」では、これまでの経済や組織のシステムが優先される社会ではなく、AI やロボットなどがこれまで人間が行っていた作業を支援し、必要なモノやサービスを、必要な人に、必要な時に、必要なだけ提供する人間中心の社会となる。

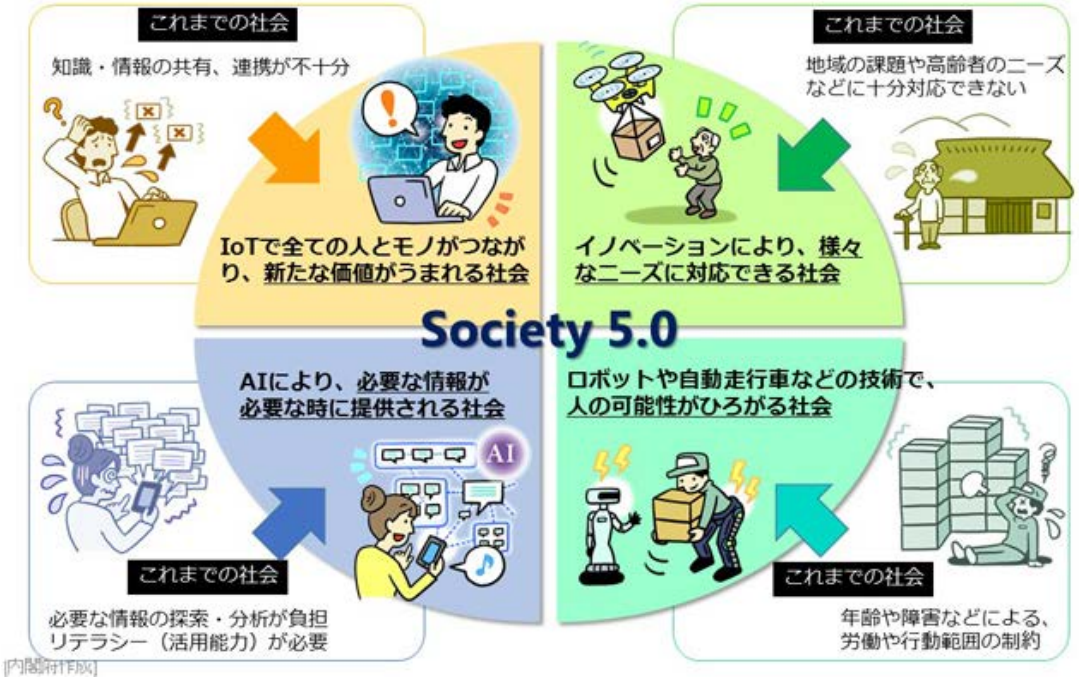


図 2 「Society 5.0」で実現する社会のイメージ[2]

こうした「Society 5.0」においては、企業を中心に付加価値を創造するための一連の活動であるサプライチェーンも、その姿を変えることになる。これまでのサプライチェーンは、始めに厳密な企画・設計を行い、それを踏まえて必要な部品やサービスを調達し、組み立て・加工を行い、最終的な製品・サービスを提供するという、一連の活動の順番が固定的・安定的な形で展開される、定型的・直線的な構成をとっていた。しかし、「Society5.0」では、必要な人に対して、必要な時に、必要なモノやサービスが提

[2] 内閣府「Society 5.0「科学技術イノベーションが拓く新たな社会」説明資料」

供されることになり、付加価値を創造するための一連の活動の起点は、これまでのように供給者が企画・設計するという固定的なものではなく、需要者が付加価値創造活動の起点となっていくことも増大していく。また、付加価値を創造するための一連の活動の開始時点で設定された“必要性”の内容が変化したことに対応して活動内容が途中で変更されたり、より有効な情報が得られれば、その要素を取り入れて新たな活動を組み込んでいくような、多様なつながりによる付加価値創造活動へと変化していくことになる。こうした変化したサプライチェーンは、従来の定型的・直線的なサプライチェーンと対比し、「Society5.0」型サプライチェーンとして捉える必要がある。

１．２．サイバー攻撃の脅威の増大

IoT と AI によって実現される「Society5.0」の社会（人間中心の社会）では、サイバー攻撃の起点が増大するとともに、複雑につながるサプライチェーンを通じてサイバーリスクの範囲が拡大していく。さらに、サイバー空間とフィジカル空間が高度に融合するため、サイバー攻撃がフィジカル空間まで到達する危険が急激に増大することになる。また、IoT から得られる情報のデジタル化のための転換処理や、大量に創出されたデータの受け渡しがサイバーにおける新たな攻撃点として顕在化してくることになる中、大量のデータの正確性・流通・連携を支えるセキュリティ対策も重要な課題である。

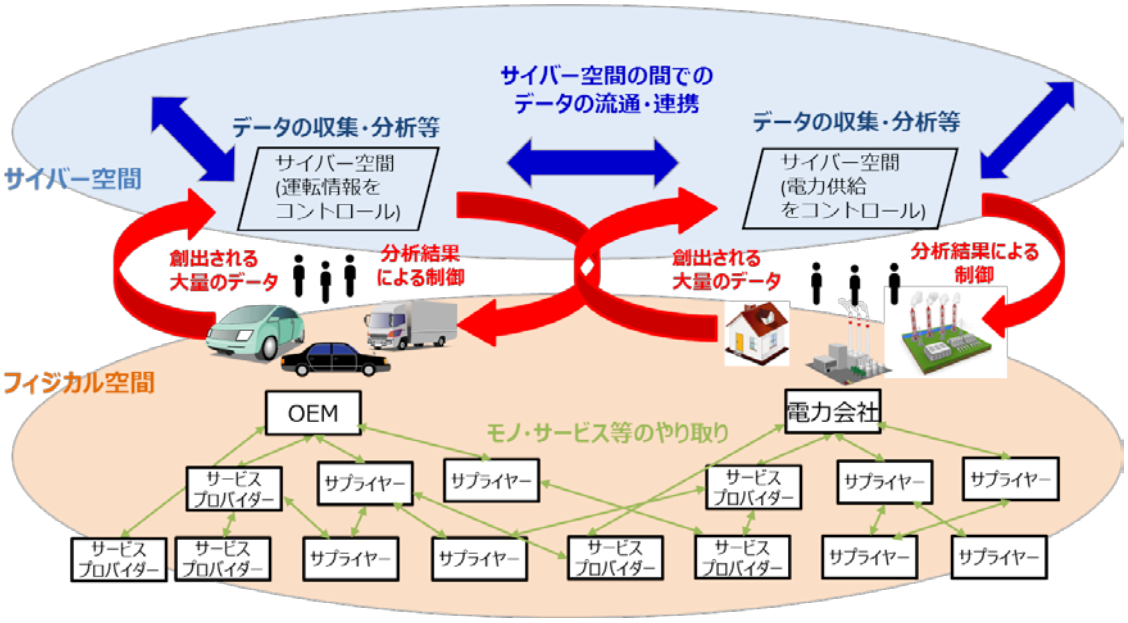


図 3 「Society5.0」社会におけるモノ・データ等のつながりのイメージ

大量のデータの流通・連携	→	データ管理の重要性が増大
フィジカルとサイバーの融合	→	フィジカル空間までサイバー攻撃が到達 フィジカルから侵入しサイバー空間への攻撃も想定 フィジカルとサイバーの間における情報の転換作業への介入
複雑につながるサプライチェーン	→	影響範囲が拡大

実際に、欧州のグループ会社の機器がランサムウェア（身代金要求型ウイルス）に感染し、それがサプライチェーン経由で国内企業へ侵入して感染を広げたことで、一部業務が停止した事例も報告されている。

さらに、海外においても、IoT や ICS（産業用制御システム）防衛のためにはサプラ

イチェーンマネジメントでアプローチする必要性が広く認識されるようになっている。米国では、NIST[3]が 2014 年 2 月に策定した特に重要インフラに対するサイバーセキュリティ対策の全体像を示したフレームワーク（Cybersecurity Framework）の改訂ドラフト版が 2017 年 1 月と 12 月に公開された。ここでは、サプライチェーンのリスク管理（Supply Chain Risk Management）が事前の対策(特定)として追加され、サプライチェーン全体で対策を実施することや、必要に応じて監査を行うことを要求している。

[3] National Institute of Standards and Technology（アメリカ国立標準技術研究所）

2．サイバー・フィジカル・セキュリティ対策フレームワークの考え方

2．1．フレームワークを策定する目的

「Society5.0」、「Connected Industries」の実現へ向けて、産業構造、社会の変化に伴うサイバー攻撃の脅威の増大に対応していかなければならず、まさに今こそ、そのための準備を開始することが必要である。このため、産業に求められるセキュリティ対策の全体像を整理し、産業界が活用できる『サイバー・フィジカル・セキュリティ対策フレームワーク』を策定することとした。

フレームワークを活用することで期待される効果と特徴は以下のとおりである。

(1) 各事業者がフレームワークを活用することで期待される効果

- 「Society5.0」、「Connected Industries」の実現に求められるセキュリティの確保
- 製品・サービスのセキュリティ品質を差別化要因（価値）にまで高めることによる競争力の強化

(2) フレームワークの特徴

① **各事業者が実施するセキュリティ対策のオペレーションレベルで活用できる**

- 社会として目指すべき概念だけではなく、各事業者が実際にセキュリティ対策を実施するうえで活用できる内容にする。

② **セキュリティ対策の必要性とコストの関係を把握できる**

- サプライチェーン全体を構成する中小企業を含めた事業者が、実際に対策を行えるよう、想定されるリスクと必要な対策のコストのバランスをイメージできるような内容にする。
- セキュリティレベルを保ったままでコストを圧縮できるような内容にする。
- リスクシナリオベースの考え方も考慮した内容にする。

③ **グローバルハーモナイゼーションを実現する**

- グローバルサプライチェーンの中で、日本における製品・サービスのセキュリティ対策が海外からも認められるよう、諸外国の動きをよく取り入れ、ISMS や NIST Cybersecurity Framework など米欧などの主要な認証制度との整合性を確保し、相互承認を進めていくことができる内容にする。

２．２．フレームワークの構造
～「Society5.0」型サプライチェーン“価値創造過程”への対応

あらゆるものがつながる IoT、データがインテリジェンスを生み出す AI などによって実現される「Society5.0」（人間中心の社会）、「Connected Industries」では、製品/サービスを生み出す工程（サプライチェーン）も従来の定型的・直線的なものとは異なる、多様なつながりによる非定型の形態を取ることになる。

本フレームワークでは、このような「Society5.0」型サプライチェーンをこれまでのサプライチェーンとは区別して認識するため、価値創造過程（バリュークリエイションプロセス）と定義し、「Society5.0」、「Connected Industries」によって拡張したサプライチェーンの概念に求められるセキュリティへの対応指針を示す。

本フレームワークは、価値創造のための活動が営まれる産業社会を、下記の三層構造と 6 つの構成要素で捉え、包括的にセキュリティポイントを整理し、それらに対応するための指針となるものである。

◆三層構造

価値創造過程（バリュークリエイションプロセス）は、従来のサプライチェーンにおける信頼できる企業間のつながりによって付加価値が創造される領域を越えて、IoT によってフィジカル空間における情報がデジタル化されてサイバー空間に取り込まれ、そうしたデータがサイバー空間で自由に流通することで、多様なデータが新たなデータを生み出して付加価値を創出することや、新たに創出されたデータが IoT を通じてフィジカル空間における物理的な製品やサービスを創出するという、新たな付加価値のための一連の活動を視野に入れる必要がある。

こうした、従来のサプライチェーンの活動範囲から拡張された付加価値を創造する活動のセキュリティ上のリスクを的確に洗い出し、対処方針を示すため、価値創造過程（バリュークリエイションプロセス）が発生する領域を、以下のように三層構造に整理して捉える。

第 1 層－　企業間のつながり（従来型サプライチェーン）
第 2 層－　フィジカル空間とサイバー空間のつながり
第 3 層－　サイバー空間におけるつながり

◆6 つの構成要素

フレームワークがオペレーションレベルで活用されるためには、価値創造過程に関与する構成要素を明確化し、構成要素ごとにどのようなセキュリティ対策を行うべきかについて、指針を示すことが求められる。

そのため、価値創造過程において、付加価値の創造に関与するものとして、以下を構成要素として定義する。

－組織、ヒト、モノ、データ、プロシージャ、システム

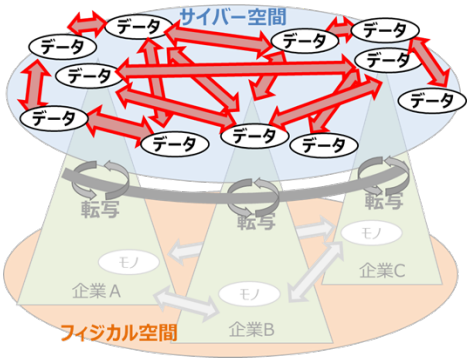
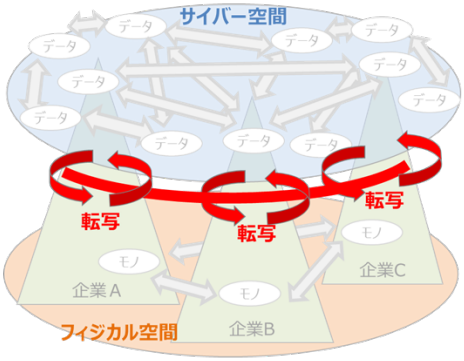
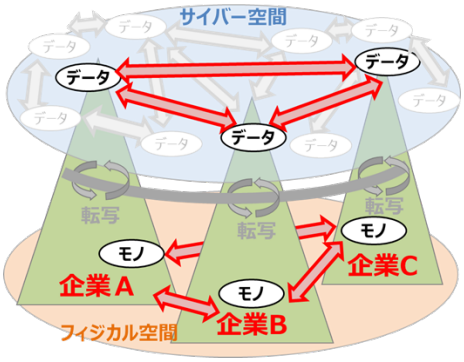
三層構造	概念図
サイバー空間におけるつながり 【第３層】	
フィジカル空間とサイバー空間の つながり 【第２層】	
企業間のつながり （従来型サプライチェーン） 【第１層】	

図 4 価値創造過程が展開する産業社会の三層構造

■三層構造アプローチの意義

3 つの層には、価値創造過程において確保されなければならない機能・役割が存在する。

例えば、各層において以下で示すようなことが確保されていなければ、価値創造過程は成立をしないことになる。

- 第1層では生産された製品等－信頼できる企業が信頼できる生産活動によって仕様どおりの製品やサービスを供給しているか否か
- 第2層ではセンサーで読み込まれたデータ等－フィジカル空間における情報を、センサーなどの IoT 機器が正確にデジタル化し、サイバー空間に“転写”しているか否か
- 第3層ではデータ分析で得られたデータ等－収集する過程で改ざんされていないデータを適切な方法で加工した、信頼できるデータを活用できるか否か

本フレームワークでは、各層で創造される価値の持つ特徴を踏まえた対応の方針を示す。

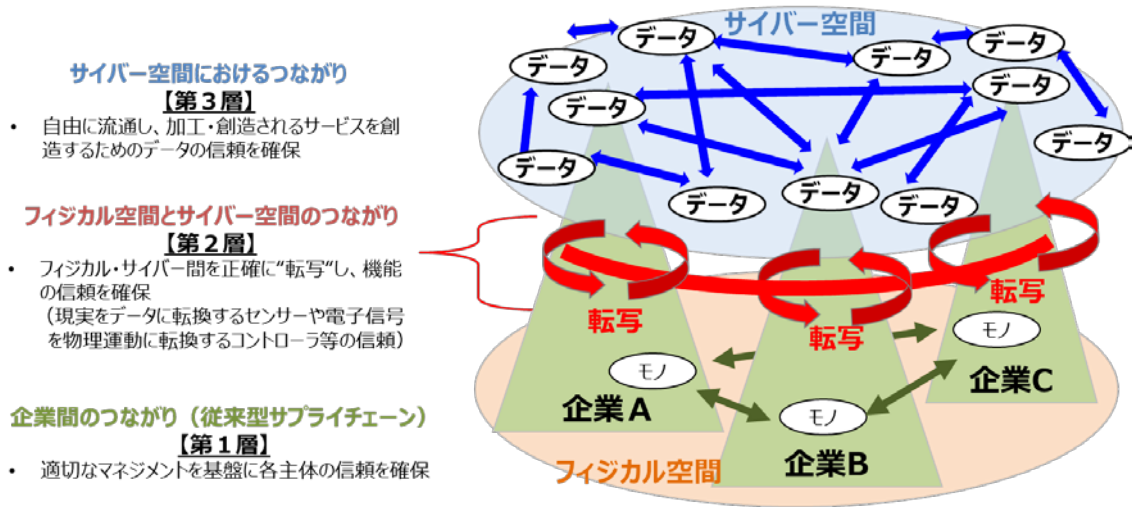


図 5 三層構造アプローチの意義

表 1 価値創造過程に関わる 6 つの要素

構成要素	定義
組織	価値創造過程（特に、従来型サプライチェーン）に参加する企業・団体
ヒト	組織に属する人、及び価値創造過程に直接参加する人
モノ	ハードウェア、ソフトウェア、及びそれらの部品
データ	フィジカル空間にて収集された情報、及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	定義された目的を達成するために要求される定型化された一連の活動
システム	サービスを実現するためにモノで構成される仕組み・インフラ

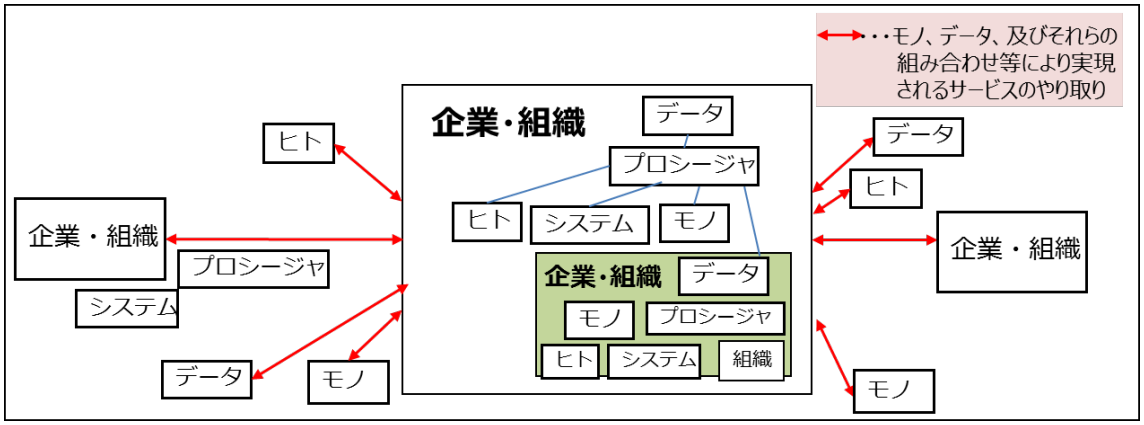


図 6 構成要素の関係

２．３．フレームワークの構成

２．２．で整理した構造を踏まえて、三層構造の各層におけるサイバー・フィジカル・セキュリティ対策について以下の図のとおり整理する。

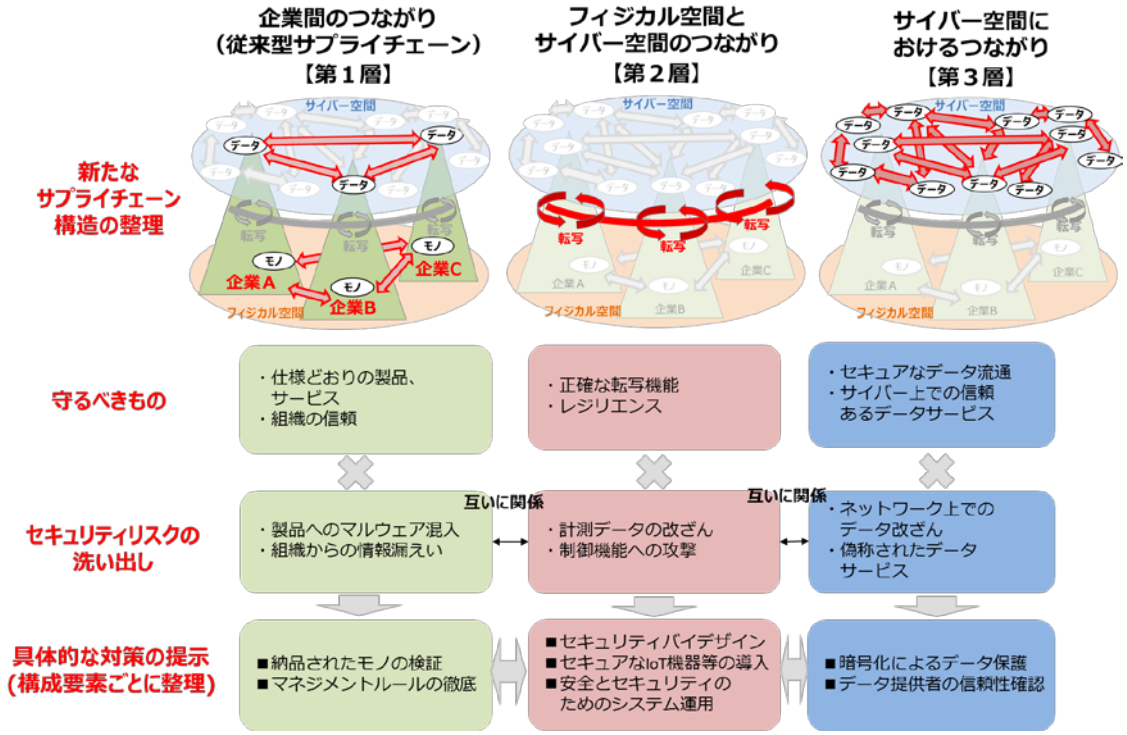


図７ 各層におけるセキュリティ対策の概要

本フレームワークは、「Society5.0」における全産業に共通的なセキュリティ対策を示しているが、それぞれの業界や企業により、守るべき重要な資産、人的・資金的リソース、又は許容できるリスク等が異なっている。

よって、各業界や各企業において、本フレームワークに記載の内容を参考に実態に則したセキュリティ対策の項目を列挙したプロファイルの作成に活用していただきたい。

また、現在のプロファイルと目標となるプロファイルを比較することで、それらの隔たりを明らかにし、セキュリティリスクの低減に活用していただきたい。

３．必要なサイバー・フィジカル・セキュリティ対策

３．１．【第１層】企業間のつながり（従来型サプライチェーン）に係るセキュリティ対策

L1.001 セキュリティポリシーの策定、体制の整備

■リスク要因

組織内で統一的なセキュリティ対策がとれず、効率的な対策ができない。

セキュリティインシデント発生時の実施すべき内容、対応の優先度がわからず、対応着手が遅れる。

■リスク影響

- セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する

■対策の概要

- セキュリティポリシーの策定と運用
- セキュリティ管理責任者の任命とセキュリティ対策組織立ち上げ

■対策ポイント

自組織の事業におけるミッション、目標、活動に関して優先順位を確立し、共有した上で、セキュリティポリシーを策定し、役割、責任、情報の共有方法等を明確にする。セキュリティ管理責任者を任命し、セキュリティ対策組織を立ち上げ、セキュリティインシデントへの適切な対処方法(優先順位、範囲等)を判断する体制を整える。これにより、セキュリティインシデント発生の対応の遅れによるセキュリティ被害の拡大を防ぐ。

- セキュリティポリシーを策定し、組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする
- 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を立ち上げ、組織内でセキュリティ対策を取る体制を整える
- セキュリティ対策組織は、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)から脆弱性情報を収集、分析し、対応するプロセスを確立する

本対策には、セキュリティマネジメントシステムの構築・運用が有効である。

- 情報セキュリティマネジメントシステム(ISMS)
- サイバーセキュリティマネジメントシステム(CSMS)

■構成要素毎の対策例

○組織

- 自組織の事業におけるミッション、目標、活動に関して優先順位を定め、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。
- セキュリティポリシーを策定し、組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。
  - 関係者の役割と責任、情報の共有方法やコンプライアンスを示す。

- 関係者に対し、自組織が担う役割を特定し、共有する。
- 自組織が提供する機能に応じて、その稼働状況等を関係者に提供する。
- 関係者、特に特権を持つユーザーに対して、セキュリティ上の役割と責任を正しく理解させる。

・ セキュリティ管理責任者を任命し、セキュリティ対策組織を立ち上げ、組織内でセキュリティ対策を取る体制を整える。
- セキュリティ対策組織は、内部及び外部から脆弱性情報を継続的に収集・分析し、監視対象とするセキュリティインシデントへの適切な対処方法(優先順位、範囲等)を判断する。
- 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)から脆弱性情報を収集、分析し、対応するプロセスを確立する。
- セキュリティ上の役割と責任について、関係者とあらかじめ調整し、連携する体制を整える。
- 関係者、特に特権を持つユーザーに対して、セキュリティ上の役割と責任を正しく理解させる。
- セキュリティインシデントに関する情報を公開する際、技術的な要件を理解している担当者を広報として割り当てる。

○ヒト

・ 関係者は、役割と責任を十分に理解する。
- 特に特権を持つ関係者は、セキュリティ上の役割と責任を正しく理解する。

・ セキュリティ対策組織は、セキュリティアラート、アドバイザリーを活用してセキュリティインシデントを監視する。

○モノ

(なし)

○データ

(なし)

○プロシージャ

・ セキュリティインシデントに関する情報公開は、確定事実のみを公表する。

○システム

(なし)

L1.002 セキュリティリスク管理

■リスク要因

セキュリティ対策の内容や優先順位、範囲がわからない。

■リスク影響

・ セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する

■対策の概要

・ リスクアセスメント(発生しうるセキュリティリスクの特定・分析・評価)の実施
・ セキュリティルールの策定(情報公表時のルールを含む)

■対策ポイント

組織内に存在するセキュリティリスクの特定や分析、評価を行い、そのセキュリティリスクに対するセキュリティバイデザインの考え方を含めたセキュリティ対策の内容、優先順位、対策範囲の特定等をあらかじめ行うことで、重大なセキュリティインシデントの発生やセキュリティ被害の拡大を防ぐ。また、セキュリティルールを策定することで、セキュリティ対策の推進を図る。

・ リスクアセスメント(セキュリティリスクの特定・分析・評価)を実施する
・ リスクアセスメントに基づき、発生しうるセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理し、セキュリティルールを策定する
・ セキュリティルールの優先順位を組織で決定し、セキュリティ管理責任者が承認する

本対策には、セキュリティマネジメントシステムの構築・運用が有効である。

・ 情報セキュリティマネジメントシステム(ISMS)
・ サイバーセキュリティマネジメントシステム(CSMS)

■構成要素毎の対策例

○組織

・ リスクアセスメント(発生しうるセキュリティリスクの特定・分析・評価)を実施する。
  - セキュリティ上の脅威、脆弱性、可能性、影響を考慮して、リスクアセスメントを実施し、文書化する。
  - 適切なセルフアセスメントができる体制を整備する。また、必要に応じて第三者機関に依頼する。
  - 内部及び外部からの攻撃や自然災害からの脅威を想定して、セキュリティリスクを特定する。
  - リスクシナリオベースなど多様な方法を用いて、セキュリティリスクの特定に漏れがないようにする。
  - サプライチェーンを含めてセキュリティリスクを分析する。
  - 関係者の役割に応じたセキュリティリスク許容度に応じて、セキュリティリスクを分析・評価する。
  - 自組織におけるリスク許容度の決定を、サプライチェーンにおける自組織の役割と、その分野に特化したリスク分析の結果に基づいて実施する。
  - 組織内に存在するセキュリティリスクの情報を関係者と共有する。
  - リスクアセスメントは、実際のビジネスを想定して実施する。
・ リスクアセスメントに基づき、セキュリティリスクに対する対策の内容、優先順位、対応範囲を整理し、セキュリティルールを定める。
  - 取り扱う情報(データ)の分類と取扱基準を定める。
  - 個人情報保護やプライバシー保護に関する国際的な基本原則「OECD 8 原則」に則り、プライバシー情報に関する取扱ルールを文書化し運用する。

- 地域毎に適用される法令、通達や業界標準等を理解し、セキュリティルールを定める。
- 構成要素への物理的なアクセスは、特権を持つユーザーに制限する。
- 構成要素への物理的なアクセスは、記録を残す。
- 構成要素から取得すべき監査ログを定義する。
- 重要施設への入館は、責任のある者が帯同し、部外者の行動を監視する。
- 現場環境で災害が発生した場合の被害内容を想定し、機能別の復元方法を定める。
- 代替の作業拠点(例:テレワークサイト)からのアクセスは、アクセス制限を課す。
- システムの境界、運用環境、セキュリティ要件の実装方法、及び他システムへのコネクション方法について文書化する。
- 開発・テスト環境を実稼働環境から分離する。
- 機器等の操作手順を文書化し、必要とする全てのユーザーに対して利用可能にしなければならない。
- 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める。
- 機器の廃棄手順を定める。
- モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用する。
- 無線接続に関する制約条件、環境設定等を定める。
- 情報を保護するための暗号による管理策の利用に関する方針を策定、実施する。
- セキュリティインシデント情報を公開する場合、非公開情報が含まれていないことを確認する。
- セキュリティリスクの内容により、リスク転嫁としてサイバー保険活用する。

・ サプライチェーンに係るセキュリティルールは、責任範囲を明確化したうえで、関係者によって、策定、管理、合意される。
・ セキュリティルールの優先順位を組織で決定し、セキュリティ管理責任者が承認する。

〇ヒト
・ 人の異動に伴い生じる役割の変更に対応した対策にサイバーセキュリティ(例:アクセス権限の無効化、従業員に対する審査)を含めている。
・ 情報セキュリティ違反を犯した従業員に対して処置をとるための、正式かつ周知された懲戒手続を備える。

〇モノ
・ セキュリティバイデザインを踏まえ構成要素に関する機能の設計、開発、実装、修正において、セキュリティを考慮したシステム開発ライフサイクルを導入する。

〇データ
(なし)

〇プロシージャ
・ 機器等の操作手順を文書化し、必要とする全てのユーザーに対して利用可能にしなければならない。

〇システム
・ セキュリティバイデザインを踏まえ構成要素に関する機能の設計、開発、実装、修正において、セキュリティを考慮したシステム開発ライフサイクルを導入する。
・ 開発・テスト環境を実稼働環境から分離する。

L1.003 セキュリティインシデントへの対応の明確化

■リスク要因

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、範囲がわからない。

■リスク影響

・ セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する

■対策の概要

・ セキュリティ運用マニュアルの作成

■対策ポイント

セキュリティ運用マニュアルを定め、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ことで、セキュリティインシデントへの対応を速め、セキュリティ被害の拡大を防ぐ。

・ 検知したセキュリティインシデントに即座に対応できるよう、あらかじめ対応手順をセキュリティ運用マニュアルで明確に文書化し、運用する

・ 組織のセキュリティ運用マニュアルの目的に合致する関係者を選定する

・ セキュリティに関する状況認識を深めるため、セキュリティ管理責任者は関係者との間で、セキュリティインシデントに関する情報共有を行う

・ セキュリティインシデントへの対応について、作業の目的、インシデントの判定基準、復旧の優先順位、作業順序、及び担当責任を理解し、作業を実施する

本対策には、セキュリティマネジメントシステムの構築・運用が有効である。

・ 情報セキュリティマネジメントシステム(ISMS)

・ サイバーセキュリティマネジメントシステム(CSMS)

■構成要素毎の対策例

○組織

・ 検知したセキュリティインシデントに即座に対応できるよう、あらかじめ対応手順をセキュリティ運用マニュアルで明確に文書化し、運用する。
  - セキュリティインシデント対応について、作業の目的、インシデントの判定基準、復旧の優先順位、作業順序、及び担当責任をセキュリティ運用マニュアルに示す。
  - 組織内部の関係者、執行役員、経営層、及び幹部層に対して随時状況を報告し、情報を共有する手順を示す。
  - 検知されたセキュリティインシデント等、適切な情報量で、適切な関係者に対して報告する手順を示す。
  - 関係者との間で連携して対応する手順を示す。
・ 組織のセキュリティ運用マニュアルの目的に合致する関係者を選定する。
・ セキュリティに関する状況認識を深めるため、セキュリティ管理責任者は関係者との間で、セキュリティインシデントに関する情報共有を行う。

○ヒト

・ セキュリティインシデント対応について、作業の目的、インシデントの判定基準、復旧の優先順位、作業順序、及び担当責任を理解し、作業を実施する。

○モノ

（なし）

○データ

（なし）

○プロシージャ

・　インシデントの判定基準を定める。

○システム

（なし）

L1.004 サプライヤーとの保守契約

■リスク要因

セキュリティ対策の内容や優先順位、範囲がわからない。

■リスク影響

・ セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する

■対策の概要

・ サービスやシステム、機器のサプライヤーとの保守契約手続き

■対策ポイント

問い合わせ窓口やサポート体制等が確立されたサービスやシステム、機器のサプライヤーを選定する。また、サプライヤーからの定期的な修正プログラムの入手、故障発生時の交換作業を迅速に行い、セキュリティレベル低下、業務運用効率の低下等を防ぐ。

- サプライチェーンに係るセキュリティルールは、関係者によって、責任範囲を明確化したうえで、策定、管理、合意される
- セキュリティ運用マニュアルの目的に合致するサプライヤーを選定する
- 特権を持つユーザーに対して、セキュリティ上の役割と責任を正しく理解させる
- 外部システムの利用において、外部システムを運営している組織とサービス契約を締結し、利用範囲を制限する
- 利用している外部情報システムの一覧を作成する。

本対策には、セキュリティマネジメントシステムの構築・運用が有効である。

- 情報セキュリティマネジメントシステム(ISMS)
- サイバーセキュリティマネジメントシステム(CSMS)

■構成要素毎の対策例

○組織

- サプライチェーンに係るセキュリティルールは、関係者によって、責任範囲を明確化したうえで、策定、管理、合意される。
  - 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。
  - 関係者、特に特権を持つユーザーに対して、セキュリティ上の役割と責任を正しく理解させる。
  - 組織内に存在するセキュリティリスクの情報を関係者と共有し、セキュリティインシデントに連携して対応する。
- セキュリティ運用マニュアルの目的に合致するサプライヤーを選定する。
  - サプライヤーに対し、契約上の義務を履行しているかどうかを定期的に評価する。
  - 潜在的なセキュリティインシデントを検知するため、サプライヤーの行動を監視する。
  - サプライヤーが使用する保守ツールを確認し、承認する。
  - 利用している外部情報システムの一覧を作成する。
- 検知されたセキュリティインシデント情報は、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。

○ヒト

- 特権を持つユーザーに対して、セキュリティ上の役割と責任を正しく理解させる。
- 外部システムへの接続を許可されたユーザーに対しては、アクセスの制限を行う。

○モノ

- (なし)

○データ

(なし)

○プロシージャ

- 外部システムの利用において、外部システムを運営している組織とサービス契約を締結し、利用範囲を制限する。
    - サービス契約では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱う。

○システム

- セキュリティバイデザインを踏まえ構成要素に関する機能の設計、開発、実装、修正において、セキュリティを考慮したシステム開発ライフサイクルを導入する。
- システムの境界、運用環境、セキュリティ要件の実装方法、及び他システムへのコネクションについて文書化する。
- 利用している外部情報システムの一覧を作成する。

L1.005 セキュリティ対策の PDCA 実施等

■リスク要因

新たに発生したセキュリティインシデントに対応できない。

■リスク影響

- セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する
- セキュリティ対策のための要員確保、要員の専門知識、再発防止の準備が不十分になり、セキュリティインシデントが再発する

■対策の概要

- セキュリティリスクに対する PDCA の実施
- モノ、システム等に関する最新の脆弱性情報の継続的な収集

■対策ポイント

セキュリティリスクに対する PDCA を実施し、セキュリティマネジメントシステムを改善し続けることで、新たなセキュリティインシデントにも迅速に対応することが可能となる。

- セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視/測定/評価結果から教訓を導き出し、構成要素を保護するプロセスを継続的に改善する体制を整える
- 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
- 最新の脆弱性情報を常時入手し、セキュリティルール及びセキュリティ運用マニュアルへフィードバックする
- 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
- セキュリティインシデントの検知プロセスを継続的に改善する

本対策には、セキュリティマネジメントシステムの構築・運用が有効である。

- 情報セキュリティマネジメントシステム(ISMS)
- サイバーセキュリティマネジメントシステム(CSMS)

■構成要素毎の対策例

○組織

- 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
- 必要に応じてセキュリティポリシーを見直す。
- セキュリティインシデントへの対応により得られた教訓や、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、構成要素を保護するプロセスを継続的に改善する体制を整える。
- 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。
    - 適切なセルフアセスメントができる体制を整備する。また、必要に応じて第三者機関に依頼する。
    - 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。
    - 新たに特定された脆弱性に関して、許容できるリスクの場合、その旨を文書化し、許容できない場合には

対策を通じてリスクを低減する。
    - 判明した問題点の修正や、脆弱性の軽減等に関して、セキュリティ運用マニュアルに反映する手順を整備する。
    - 復旧手順から得られた教訓をもとに、復旧に関する訓練、テストを行い、セキュリティ運用マニュアルを更新する。
- セキュリティインシデントの検知プロセスを継続的に改善する。
    - 構成要素の脆弱性に関する最新の公開情報を常時確認、収集し、関連する問題に対処する体制を整える。
    - 監視業務として、セキュリティインシデントを検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。
    - 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。
    - 潜在的なセキュリティインシデントを検知するため、サプライヤーの行動を監視する。
- 組織の全ての要員及び、関係者へのセキュリティインシデント発生時の対応訓練を継続的に実施し、対応能力を定期的にテストする。
- 内部からの脅威の潜在指標の認識と報告についてのセキュリティ周知訓練を実施する。

〇ヒト

(なし)

〇モノ

(なし)

〇データ

(なし)

〇プロシージャ

(なし)

〇システム

(なし)

L1.006 定期的な教育・訓練

■リスク要因

組織内で統一的なセキュリティ対策がとれない。

■リスク影響

・ セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する

■対策の概要

・ 定期的なセキュリティ対策教育の実施
・ 定期的なセキュリティインシデント対応訓練の実施

■対策ポイント

セキュリティ対策を考慮した運用やセキュリティインシデント発生時の対応について、組織内の全ての要員へ教育を行うことにより周知徹底し、定期的な見直しを行う。これにより、セキュリティインシデント発生時の対応の遅れ、セキュリティ被害の拡大を防ぐ。

・ 組織の全ての要員に対して、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(トレーニング)、セキュリティ教育を実施し、セキュリティポリシー、セキュリティルール、セキュリティ対応マニュアルについて周知する

本対策には、セキュリティマネジメントシステムの構築・運用が有効である。

・ 情報セキュリティマネジメントシステム(ISMS)
・ サイバーセキュリティマネジメントシステム(CSMS)

■構成要素毎の対策例

○組織

・ 組織の全ての要員(システム責任者、システム管理者、及び利用者等)に対して、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、セキュリティ教育を実施し、セキュリティポリシー、セキュリティルール、セキュリティ対応マニュアルについて周知する。
  - セキュリティインシデントへの適切な準備、検知、分析、抑制（封じ込め)、リカバリ、及び顧客への対応を含めて対応能力を確立する。
  - 内部不正についての報告制度を整備し、組織の要員に対する意識向上教育を実施する。
    (内部不正の例:過度な労働への不満による業務外情報へのアクセス、組織内運用ルールの違反等)
  - 関係者も交え、セキュリティインシデントへの対応能力を定期的にテストする。
  - 内部からの脅威の潜在指標の認識と報告についてのセキュリティ周知訓練を実施する。

○ヒト

・ 組織の全ての要員は、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、セキュリティ教育を受講し、セキュリティポリシー、セキュリティルール、セキュリティ対応マニュアルについて理解する。
  - セキュリティインシデントへの対応能力のテストを定期的に受ける。

○モノ

(なし)

○データ

(なし)

○プロシージャ

（なし）

○システム

（なし）

L1.007 モノ、システム等の資産管理

■リスク要因

サイバー空間と接続する機器等の資産管理の対応不足。

■リスク影響

・ セキュリティ対策漏れを引き起こす機器等が存在し、外部からの不正アクセス、マルウェア感染源になる

■対策の概要

・ 機器等の棚卸しや資産管理
・ 機器等の適切な資産運用

■対策ポイント

機器等資産の構成管理及び変更管理を確実に実施することで、現場において無断で導入された機器等、資産管理されていない機器を踏み台としたセキュリティインシデントの発生を抑制する。

・ 機器等の構成管理及び変更管理を実施する
・ 機器等の構成管理では、設定情報を継続的に管理することとし、システムを構成するハードウェア及びソフトウェアの管理情報を文書化し、保存する
・ 機器等やユーザーに関する ID(識別子)や重要情報(秘密鍵、電子証明書等)に対し、管理方法を明確にしたうえで管理する
・ ハードウェア及びソフトウェアのリソース割り当ての優先付けは、種別、重要性、ビジネス的価値に基づいて行う

本対策には、セキュリティマネジメントシステムの構築・運用が有効である。

・ 情報セキュリティマネジメントシステム(ISMS)
・ サイバーセキュリティマネジメントシステム(CSMS)

■構成要素毎の対策例

○組織

・ 情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則を、明確化し、文書化し、実施する。
・ 機器等の資産の構成管理及び変更管理を実施する。
  - 施設に出入りする全ての構成要素について、取り外し、移送、廃棄の手順を文書化する。
  - 企業内の通信ネットワーク構成図及び、データフロー図を作成し、保存する。
  - 変更(廃棄、追加、交換等)が発生した場合、直ちに構成管理情報を更新し、変更記録を作成し、保管する。保管する期間は、用途に合わせて定める。
  - 過去の変更の追跡、変更に関する監査、レビュー、及びセキュリティへの影響を考慮した上で変更の承認手続きを行う。

○ヒト

・ ユーザーは、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)に見合う形で認証される。

○モノ

- 機器等の構成管理では、設定情報を継続的に管理することとし、システムを構成するハードウェア及びソフトウェアの管理情報を文書化し、保存する。
  (ハードウェアの管理情報:ハードウェア構成情報、機器名、シリアル番号、所有者、設置場所等)
  (ソフトウェアの管理情報:ライセンス情報、バージョン番号、OS 情報等)
  - 重要情報を格納し配付期限を設定した外部メディアに対しては、取扱いに関する警告表示、配付制限等のラベリングを行う。
  - 所有者が特定できないポータブルストレージデバイスの利用は禁止する。
- 機器等は、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)に見合う形で認証される。

○データ

- 機器等やユーザーに関する ID(識別子)や重要情報(秘密鍵、電子証明書等)に対し、ライフサイクル全体にわたって、管理方法(重要情報の利用、保護及び有効期間等)を明確にした上で管理する。

○プロシージャ

(なし)

○システム

- ハードウェア及びソフトウェアのリソース割り当ての優先付けは、種別、重要性、ビジネス的価値に基づいて行う。
- 機器等やユーザーを一意に識別できる ID(識別子)を採番する。
- 企業内の通信ネットワーク構成図及び、データフロー図を作成し、保存する。

L1.008 セキュリティインシデントの適切な検知・分析機能、手順の実装

■リスク要因

セキュリティインシデントを正確に特定できない。

■リスク影響

- セキュリティインシデントの発見の遅れにより、セキュリティ被害が拡大する

■対策の概要

- 不正通信などのインシデントの検知体制の整備
- アラート通知後の相関の分析
- 外部の脅威情報と比較したセキュリティインシデント検知内容の分析

■対策ポイント

セキュリティインシデントの相関の分析、及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントの発生を正確に特定する。

分析の対象とするセキュリティインシデントは、サイバー空間に接続される複数の機器から情報収集し、統合的に判断することで精度を高める。さらに、組織内外から入手する情報をもとに脆弱性や脅威を速やかに発見し、適切な対策を検討する。

- 発生したセキュリティインシデントについて、セキュリティ管理責任者及び適切な関係者に報告する
- 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
- セキュリティインシデント発生前の構成情報をもとに、復旧計画を実行する
- 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

本対策には、セキュリティマネジメントシステムの構築・運用が有効である。

- 情報セキュリティマネジメントシステム(ISMS)
- サイバーセキュリティマネジメントシステム(CSMS)

■構成要素毎の対策例

○組織

- 発生したセキュリティインシデントについて、セキュリティ管理責任者及び適切な関係者に報告する。
- 発生したセキュリティインシデントの分析において、組織内外から脅威情報を入手し、攻撃の標的と攻撃手法を特定する。
- 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思から、組織全体への影響を把握する。
- セキュリティインシデント発生前の構成情報をもとに、復旧計画を実行する。
- セキュリティ被害の拡大を最小限に抑え、影響を低減する対応を行う。
- 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。

○ヒト

- 発生したセキュリティインシデントについて、セキュリティ管理者及び適切な関係者に報告する。

○モノ

（なし）

○データ

（なし）

○プロシージャ

（なし）

○システム

・ 監視機能を使用して、構成要素の各データソースからのデータや、ネットワークパケット等を収集し統合して、総合的に判断することで、検知したセキュリティインシデントの分析精度を高める。

L1.009 事業継続計画又はコンティンジェンシープランへの反映

■リスク要因

セキュリティインシデント発生時における事業継続判断が適切に行えない。

■リスク影響

・ セキュリティインシデント発生時において、その影響と事業継続の可否について適切な判断を行うことができず、組織の社会機能や組織に対する社会的評価を喪失する

■対策の概要

・ 事業継続計画又はコンティンジェンシープランにセキュリティインシデント発生時の対応を位置づける

■対策ポイント

自然災害時における対応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、インシデントが発生した場合の影響の最小化と事業継続のための措置についてあらかじめ計画的に定めサイバーレジリエンスを高める。

・ セキュリティインシデント発生前の構成情報を基にした事業継続計画又はコンティンジェンシープランを定める

・ セキュリティ被害の拡大を最小限に抑え、影響を低減する対応を行う

・ 発生したセキュリティインシデントの対応により得られた教訓を復旧計画に反映し、継続的に更新する

■構成要素毎の対策例

○組織

・ セキュリティインシデント発生前の構成情報を基にした事業継続計画又はコンティンジェンシープランを定める。
・ セキュリティインシデント発生前の構成情報を基にした復旧計画を実行する。
・ セキュリティ被害の拡大を最小限に抑え、影響を低減する対応を行う。
・ セキュリティインシデントの発生後、組織の社会的機能と組織に対する社会的評価の回復に取り組む。

○ヒト

(なし)

○モノ

(なし)

○データ

(なし)

○プロシージャ

・ 発生したセキュリティインシデントの対応により得られた教訓を復旧計画に反映し、継続的に更新する。

○システム

(なし)

L1.010 各種法令への対応

■リスク要因

組織内で各種法令が守られない。

■リスク影響

・ 組織内でコンプライアンス違反が発生する

■対策の概要

・ 法令や業界のガイドラインを考慮したセキュリティ対策の立案

■対策ポイント

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。これにより、他の事業者との間でデータを共有した場合においても、業務上の公正な競争秩序を維持することができる。

・ プライバシーや人権に対する義務を含む、セキュリティに関する法令等の規制や要求事項を理解し、セキュリティルールに文書化し、運用管理する

本対策には、セキュリティマネジメントシステムの構築・運用が有効である。

・ 情報セキュリティマネジメントシステム(ISMS)

・ サイバーセキュリティマネジメントシステム(CSMS)

■構成要素毎の対策例

○組織

・ プライバシーや人権に対する義務を含む、セキュリティに関する法令等の規制や要求事項を理解し、セキュリティルールに文書化し、運用管理する。
  - 地域毎に適用される法律、法令、通達や業界標準等に変更が加えられた際に、速やかにセキュリティルールの変更を行う。
  - 監視業務では、地域毎に適用される法律、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。
  - 知的財産権及び権利関係のあるソフトウェア製品の利用に関連する法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施する。
  - 暗号化機能は，関連する全ての協定，法令及び規制を順守して用いる。

○ヒト

(なし)

○モノ

(なし)

○データ

(なし)

○プロシージャ

(なし)

○システム

(なし)

L1.011 生産したモノの記録の管理

■リスク要因

サプライチェーン上で発生したと考えられる問題の発生時点の把握ができない。

■リスク影響

・ 価値(モノ)を創造するプロセスにおける問題発生時点が特定できないことから、サプライチェーンにおける問題対処の方法が決まらず、生産活動の適正化に長時間を要することになる

■対策の概要

・ 生産したモノに関し、後日、監査によって確認できるように、生産したモノの特定方法を定めるとともに、生産記録を作成し、一定期間保管する

■対策ポイント

生産したモノのサプライチェーン上の重要性に応じて、ナンバーを付与する等特定方法を定めるとともに、その重要性に応じて、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に内部規則を整備する。

・ 生産活動に関する内部規則を整備するとともに、生産したモノの記録については、その重要性に応じて、後日監査を受ける可能性があることを踏まえ、取引先との間であらかじめ重要性について認識を共有し、適切な記録管理レベルを確保する

■構成要素毎の対策例

○組織

・ 生産記録に関する内部規則を整備する。

○ヒト

(なし)

○モノ

・ 生産記録に関する内部規則に基づき、記録を作成し、記録を保管する。

○データ

(なし)

○プロシージャ

(なし)

○システム

(なし)

L1.012 プライバシー保護

■リスク要因

現場の機器及びサイバー空間を通じて、ユーザーのプライバシーに関する情報(データ)が本人の同意なしに収集・活用される。

■リスク影響

- 収集されたデータの取扱いにおいて、ユーザーのプライバシーに関する情報(データ)が本人の同意なしにシステムに収集され、プライバシー侵害の問題を引き起こす

■対策の概要

- プライバシー保護の法令に準拠したプライバシー情報の取扱ルールの作成
- 定期的なプライバシー情報の所在確認の実施

■対策ポイント

個人情報保護やプライバシー保護に関する国際的な基本原則「OECD 8 原則」に則り、プライバシー情報の取扱ルールを文書化し運用する。

これにより、組織の運用におけるプライバシー侵害を防ぐ。

- 構成要素(ヒト、モノ、プロシージャ、システム)に対し、プライバシー情報の取扱ルールを明確にし、アクセスを制限する

■構成要素毎の対策例

○組織

- 個人情報保護やプライバシー保護に関する国際的な基本原則「OECD 8 原則」に則り、プライバシー情報に関する取扱ルールを文書化し、運用する。
- 構成要素(ヒト、モノ、プロシージャ、システム)に対し、プライバシー情報の取扱ルールを明確にし、アクセスを制限する。

○ヒト

- プライバシー情報へのアクセスを制限する。

○モノ

- プライバシー情報へのアクセスを制限する。

○データ

(なし)

○プロシージャ

- プライバシー情報へのアクセスを制限する。

○システム

- プライバシー情報へのアクセスを制限する。

L1.013 セキュリティインシデントの適切な情報共有

■リスク要因

セキュリティ対策の内容や優先順位、範囲がわからない。

■リスク影響

・ セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する

■対策の概要

・ セキュリティインシデントの適切な情報共有

■対策ポイント

セキュリティ運用マニュアルを定め、セキュリティインシデント発生時に JPCERT/CC などに適切な情報共有を行う。また、日ごろから JPCERT/CC などから最新のセキュリティインシデント情報を入手しセキュリティ対策に活用する。

・ 組織のセキュリティ運用マニュアルに情報共有手順を明確に文書化し、運用する

・ 最新のセキュリティインシデント情報を入手しセキュリティ対策に活用する

本対策には、セキュリティマネジメントシステムの構築・運用が有効である。

・ 情報セキュリティマネジメントシステム(ISMS)

・ サイバーセキュリティマネジメントシステム(CSMS)

■構成要素毎の対策例

○組織

・ セキュリティインシデント発生時に即座に JPCERT/CC などに適切な情報共有を行えるよう、あらかじめ対応手順をセキュリティ運用マニュアルで明確に文書化し、運用する。
  - 検知されたセキュリティインシデント等、適切な情報量で、適切な関係者に対して報告する手順を示す。
  - 関係者との間で連携して対応する手順を示す。
・ 最新のセキュリティインシデント情報を入手しセキュリティ対策に活用する。

○ヒト

・ セキュリティインシデントの適切な情報共有の重要性について理解し、確実な対応を実施する。

○モノ

(なし)

○データ

(なし)

○プロシージャ

(なし)

○システム

(なし)

３．２.【第２層】フィジカル空間とサイバー空間のつながりに係るセキュリティ対策

L2.001 セキュリティ対策が施されたIoT機器の導入

■リスク要因

IoT機器のアクセス制御等のセキュリティ対策が不十分で、不正アクセスされる。

■リスク影響

・ IoT機器が不正に操作されることで、誤動作が発生する

■対策の概要

・ 第三者機関による評価を取得したIoT機器（例：EDSA認証(IEC 62443-4-2)）や自己適合確認により安全性を確認されたIoT機器の選択

■対策ポイント

第三者機関による評価を取得したIoT機器を導入することで、外部からの不正アクセスによるIoT機器の誤動作等を防ぐ。

・ 受容できない既知のセキュリティリスクの有無を企画・設計の段階から確認する。

・ 受容できない既知のセキュリティリスクに対して企画・設計段階から対策を講じる。

・ IoT 機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する

■構成要素毎の対策例

○組織

・ IoT機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。
  - 新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立する。
  - 試験データは、注意深く選定し、保護し、管理する。

○ヒト

・ 受容できない既知のセキュリティリスクの有無を企画・設計の段階から確認する。

○モノ

・ 受容できない既知のセキュリティリスクの有無を企画・設計の段階から確認する。

・ 第三者機関による評価を取得したIoT機器（例：EDSA認証(IEC 62443-4-2)）や自己適合確認により安全性を確認されたIoT機器を選択する。
  - 企画・設計段階において実施する要件定義や設計仕様を第三者機関がセキュリティの観点から評価する。

○データ

（なし）

○プロシージャ

（なし）

○システム

・ IoT 機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。

L2.002 IoT 機器におけるセキュリティバイデザインの実践

■リスク要因

セキュリティ対策を考慮していない IoT 機器を利用する。

■リスク影響

・ IoT 機器における脆弱性に対し、対策に時間がかかり費用が増加する

■対策の概要

・ 企画・設計の段階からセキュリティリスクを考慮して実装された IoT 機器の選択

■対策ポイント

企画・設計の段階からセキュリティリスクを考慮して実装された IoT 機器を導入することで、開発時における手戻りが少なくなり、また、運用フェーズでの IoT 機器へのセキュリティ対策費用の増加を防ぐ。

- 受容できない既知のセキュリティリスクの有無を企画・設計の段階から確認する
- 受容できない既知のセキュリティリスクに対して企画・設計段階から対策を講じる
- IoT 機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する

■構成要素毎の対策例

○組織

・ IoT 機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。

○ヒト

・ 受容できない既知のセキュリティリスクの有無を企画・設計の段階から確認する。

○モノ

・ 受容できない既知のセキュリティリスクに対して企画・設計段階から対策を講じる。

○データ

（なし）

○プロシージャ

（なし）

○システム

・ IoT 機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。

L2.003 機能安全を考慮した IoT 機器の導入

■リスク要因

機能安全を実装しない IoT 機器を利用する。

■リスク影響

・ IoT 機器の動作により作業員に危害が及ぶ、又は IoT 機器の破損が発生する

■対策の概要

・ 機能安全を考慮した IoT 機器の導入

■対策ポイント

機能安全を考慮した IoT 機器を利用することで、正常動作・異常動作に関わらず、IoT 機器の動作による作業員への危害、IoT 機器の破損を防ぐ。

- 受容できない既知のセキュリティリスクの有無を企画・設計の段階から確認する。
- 受容できない既知のセキュリティリスクに対して企画・設計段階から対策を講じる。
- ネットワークにつながることを踏まえた機能安全を実装する IoT 機器を導入する
- IoT 機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する

■構成要素毎の対策例

○組織

・ IoT 機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。

○ヒト

・ 受容できない既知のセキュリティリスクの有無を企画・設計の段階から確認する。

○モノ

・ 受容できない既知のセキュリティリスクに対して企画・設計段階から対策を講じる。
・ ネットワークにつながることを踏まえた機能安全を実装する IoT 機器を導入する。

○データ

(なし)

○プロシージャ

(なし)

○システム

・ IoT 機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。

L2.004 IoT 機器における正規品の導入

■リスク要因

不正な IoT 機器やソフトウェアが混入する。

■リスク影響

- 模倣品等品質や信頼性が低い IoT 機器(IoT 機器に導入されているソフトウェア含む)を利用することで、不正な情報(データ)の混入、故障頻度の上昇を引き起こす

■対策の概要

- IoT 機器のサプライヤーにより、正規であることが認証された IoT 機器の導入
- ソフトウェアのサプライヤーにより、正規であることが認証されたソフトウェアの導入

■対策ポイント

正規の IoT 機器であることを検証できる IoT 機器を利用することで、模倣品等の品質や信頼性が低い IoT 機器の利用による、不正な情報(データ)の混入や誤動作の発生、故障頻度の上昇に伴う業務運用効率の低下等を防ぐ。同様に、正規のソフトウェアであることを検証できるソフトウェアを利用することで、模倣品等の品質や信頼性が低いソフトウェアの利用によるマルウェア感染や、不正確な情報(データ)の混入に伴う業務運用効率の低下等を防ぐ。

- IoT 機器やソフトウェアには、一意であることを示すための ID(識別子)や重要情報(秘密鍵、電子証明書等)が含まれる
- 正規品であることを確認するために、IoT 機器やソフトウェアのサプライヤーを識別し、認証する(完全性の検証等)
- 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

■構成要素毎の対策例

○組織

- IoT 機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。
- IoT 機器やソフトウェアのサプライヤーを特定し、そのサプライヤーから正規品を導入する。
- 正規品であることを確認するために、IoT 機器やソフトウェアのサプライヤーを識別し、認証する。

○ヒト

(なし)

○モノ

- IoT 機器やソフトウェアには、一意であることを示すための ID(識別子)や重要情報(秘密鍵、電子証明書等)が含まれる。
- 電子証明書は、有効期限を定める。
- IoT 機器やソフトウェアは、搬送中の改ざん・漏えいを検知(又は抑止)する手段とともに納品される。
  - 物品:セキュリティ便、プロテクトシール等
  - 電送:暗号化、電送データ全体のハッシュ値等

○データ

(なし)

○プロシージャ

- 正規品であることを確認するために、IoT 機器やソフトウェアのサプライヤーを識別し、認証する。
- IoT 機器やソフトウェア 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。

○システム

- IoT 機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。
- IoT 機器やソフトウェアのサプライヤーを特定し、そのサプライヤーから正規品を導入する。
- IoT 機器やソフトウェアを一意に識別できる ID(識別子)を採番する。

L2.005 IoT 機器への適切なセキュリティ設定

■リスク要因

IoT 機器が不正に操作される。

■リスク影響

・ IoT 機器に対する不正アクセスにより、誤動作が発生する

■対策の概要

・ IoT 機器の初期設定手順(パスワード等)を定義する
・ 不要なサービスの停止等、IoT 機器の利用環境に適した設定値を適用する

■対策ポイント

IoT 機器に対し、強固なパスワードの設定、機器やサービスの間で使い回しのないパスワードへの定期的な変更等利用環境に適した設定値の使用を行うことで、IoT 機器への不正ログインによる設定変更や、IoT 機器の誤動作等を防ぐ。

・ 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

・ IoT 機器を設置する前に、デフォルトの初期設定値を確認する

■構成要素毎の対策例

○組織
・ 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し、セキュリティルールに定める。
  - 新しくパスワードを設定する際、パスワードに最低限の複雑性(文字種、文字数等)を強制する。
  - 規定された生成回数の間、パスワードの再利用を禁止する。
  - システムログイン時に恒久パスワードを即時的に変更し、一時的なパスワードを使用することを許可する。

○ヒト
・ セキュリティルールに従って IoT 機器を設定する。

○モノ
・ 基本機能のみを提供するように IoT 機器を設定することによって、最小機能の原則を採用する。

○データ
(なし)

○プロシージャ
・ IoT 機器を設置する前に、デフォルトの初期設定値を確認する。

○システム
(なし)

L2.006 IoT 機器へのアクセス制限

■リスク要因

IoT 機器が不正に操作される。

■リスク影響

・ IoT 機器に対する不正アクセスにより、誤動作が発生する

■対策の概要

・ アクセス元に対する識別、認証、認可の実施
・ 通信におけるセッションの開始、終了条件の明確化

■対策ポイント

IoT 機器へのアクセスに対し、アクセス元を識別・認証して適切なアクセス制御を行うことで、IoT 機器に対する不正ログインを防止する。さらに、通信におけるセッションを開始する際の確認事項、及び終了(遮断)する条件を明確にすることで、IoT 機器の設定変更や誤動作を防ぐ。

・ 通信におけるセッションの開始、終了条件をあらかじめ定義する
・ IoT 機器やユーザーは、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)に見合う形で認証される

■構成要素毎の対策例

○組織
・ 通信におけるセッションの開始、終了条件をあらかじめ定義する。
・ IoT 機器やユーザーは、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)に見合う形で認証される。

○ヒト
・ 必要に応じて、ユーザー認証に対応する。

○モノ
・ IoT 機器認証に対応する。
・ システムリソースやサービスへのアクセスを許可する前に、アクセス元(ユーザー、サイバー空間、IoT 機器)を識別し、認証する。
・ 許可していないアクセス元からのアクセスは拒絶する。

○データ
(なし)

○プロシージャ
・ システムリソースやサービスへのアクセスを許可する前に、アクセス元を識別し、認証する。
・ アクセス元の認証失敗に対する振る舞い(中止、警報等)をあらかじめ定義する。
  - 装置の停止／動作継続等
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する
・ IoT 機器やユーザーは、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)に見合う形で認証される。

○システム
・ あらかじめ定義された条件に従って、通信におけるセッションを開始、終了する。
  - 一定時間内にデータの授受がない等、あらかじめ定義した条件を満たせないときは、通信におけるセッ

ションを終了する。

- セッションを終了する直前の管理画面をロックする等の方法で、セッション関連情報を隠ぺいする。

・共同作業用コンピューティング装置(ネットワーク接続されたホワイトボード、カメラ、マイク等)に対しては、リモートからのアクティベーションを禁止し、装置のユーザーに対して使用中の装置を表示する。[4]

[4] ビデオ会議をアクティベートするために他者を呼び出したり、接続したりする参加者に信頼を置くような、ビデオ会議専用システムは、除外される。

L2.007 IoT 機器への不正ログイン対策

■リスク要因

IoT 機器が不正に操作される。

■リスク影響

・ 不正なユーザーによるシステム等へのアクセスにより、IoT 機器の設定変更や、IoT 機器にある情報(データ)が抜き取られ解析されることで、誤動作が発生する

■対策の概要

・ ログイン認証失敗等への適切な対応

■対策ポイント

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で、IoT 機器に対する不正ログインを防止し、IoT 機器の設定変更や、IoT 機器の誤動作を防ぐ。

・ 一定回数以上、ログイン認証に失敗した場合の振る舞いをあらかじめ定義する

・ 連続してログイン認証に失敗した場合の振る舞いをあらかじめ定義する

■構成要素毎の対策例

○組織

・ 一定回数以上、ログイン認証に失敗した場合の振る舞いをあらかじめ定義する。
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する
・ 連続してログイン認証に失敗した場合の振る舞いをあらかじめ定義する。
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する

○ヒト

・ ユーザーに、システム等を管理するために必要な権限を与える。
  - ユーザーが行った管理業務を書面で記録する。
  - 権限を持たないユーザーが管理業務にあたる場合の対処を定める。
    (例:管理監督者が帯同し、監視する等)

○モノ

・ 連続してログイン認証に失敗した場合の振る舞いをあらかじめ定義する。
  - 装置の停止／動作継続等
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する

○データ

(なし)

○プロシージャ

・ 一定回数以上、ログイン認証に失敗した場合の振る舞いをあらかじめ定義する。
  - 装置の停止／動作継続等
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する

○データ

(なし)

○システム

(なし)

L2.008 IoT 機器への物理的なセキュリティ対策

■リスク要因

IoT 機器が不正に操作される。

■リスク影響

・ IoT 機器に対する物理的な不正アクセスにより、マルウェア感染被害が発生し、誤動作が発生する

■対策の概要

・ 監視カメラ等による物理的なアクセスの記録・監視
・ 施錠・入退室管理等による物理的なアクセスの制限

■対策ポイント

IoT 機器やその設置エリアに対し、物理的なセキュリティ対策を行う。これにより、IoT 機器に対する不正アクセスを防止し、マルウェア感染等を防ぐ。

・ IoT 機器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対策を実施する

・ IoT 機器本体に対して、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

■構成要素毎の対策例

○組織
・ 要員の役割に応じて出入りできる場所を明確にする。
・ 重要な IoT 機器に対して盗難防止策(例:施錠)を講じる。

○ヒト
・ 要員の役割に応じて出入りできる場所を制限する。

○モノ
・ 基本機能のみを提供するように IoT 機器を設定することによって、最小機能の原則を採用する。

○データ
(なし)

○プロシージャ
・ セキュリティ運用マニュアルに従って、監視カメラ設置、部外者の入室時における責任者の帯同等、物理的アクセスの記録や監視を行う。
・ セキュリティを保つべき領域での作業に関する手順を設計し、適用する。

○システム
・ IoT 機器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対策を実施する。
・ 重要な IoT 機器に対して盗難防止策(例:施錠)を講じる。

L2.009 IoT 機器の可用性維持

■リスク要因

IoT 機器に故障や不具合が生じる。

■リスク影響

・ 現場の IoT 機器や通信機器、回線の機能が停止し、業務の運用に悪影響を及ぼす

■対策の概要

・ サービス不能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、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
・ 定期的なバックアップや品質管理、冗長化、予備を確保する

■対策ポイント

サービス不能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、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。さらに、定期的なバックアップや品質管理、冗長化、予備の確保を行うことで可用性を維持する。これにより、現場の IoT 機器、通信機器、回線で不具合が生じた場合においても迅速な原因の特定、サービスの復旧等により、セキュリティ被害の拡大を防ぐことができる。

・ 問い合わせ窓口やサポート体制等が確立された IoT 機器及びサービスのサプライヤーを選定する

・ 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、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

・ サービス不能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、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)を確保して可用性を実現する

■構成要素毎の対策例

○組織
・ 問い合わせ窓口やサポート体制等が確立された IoT 機器及びサービスのサプライヤーを選定する。
・ システムに関する機能の設計、開発、実装、修正において、セキュリティを考慮したシステム開発ライフサイクルを導入する。

○ヒト
(なし)

○モノ
(なし)

○データ
(なし)

○プロシージャ
(なし)

○システム
・ システムに関する機能の設計、開発、実装、修正において、セキュリティを考慮したシステム開発ライフサイクル

を導入する。

- 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、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。
- サービス不能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、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)を確保して可用性を実現する。
- サービス不能攻撃等のサイバー攻撃を受けた場合には、あらかじめ定義した状態で動作を継続する。
(例:通常運転中、異常発生中、回復作業中等)

L2.010 IoT 機器の適切な廃棄

■リスク要因

不適切な手順で IoT 機器を廃棄する。

■リスク影響

・ 廃棄された IoT 機器を悪用され、不正 IoT 機器が作成される

■対策の概要

・ 適切な手順で IoT 機器を廃棄する

■対策ポイント

IoT 機器の廃棄時には、内部に保存されている情報(データ)及び、正規 IoT 機器を一意に識別する ID(識別子)や重要情報(秘密鍵、電子証明書等)を削除(又は読み取りできない状態に)する。これにより、不正 IoT 機器の生成を防ぐ。

・ IoT 機器の廃棄時には、情報(データ)を削除(又は読み取りできない状態に)する手順を定め、セキュリティルールに定義する

・ 視覚、触覚で識別できる表示のみならず、記憶領域及び耐タンパーデバイスを再生不能な手段(焼却、溶解、粉砕等)を用いて読み取りができない状態にする

・ 製造元が指定する廃棄手段を加味した廃棄手順を含む管理手順を作成する

■構成要素毎の対策例

○組織

・ IoT 機器の廃棄時には、情報(データ)を削除(又は読み取りできない状態に)する手順を定め、セキュリティルールに定義する。
  - 内部に保存されている情報(データ)及び正規 IoT 機器を一意に識別する ID(識別子)や重要情報(秘密鍵、電子証明書等)を対象とする。
  - 視覚、触覚で識別できる表示のみならず、記憶領域及び耐タンパーデバイスを再生不能な手段(焼却、溶解、粉砕等)を用いて読み取りができない状態にする。
・ 製造元が指定する廃棄手段を加味した廃棄手順を含む管理手順を作成する。

○ヒト

・ セキュリティルールに基づく廃棄手順を順守する。
・ IoT 機器の中の重要情報を消去してから、保守作業を開始する。
・ 保存期限が経過したバックアップデータを消去する。
・ IoT 機器の管理・廃棄に係る作業履歴を残す。

○モノ

(なし)

○データ

(なし)

○プロシージャ

・ IoT 機器の管理・廃棄に係る作業履歴を確認する。
・ IoT 機器の中の重要情報を消去してから、保守作業を開始する。
・ バックアップデータの保存期限と期限経過後の扱い(消去等)を定める。

○システム

（なし）

L2.011 IoT 機器における不正なソフトウェアへの対策

■リスク要因

IoT 機器が不正に操作される。

■リスク影響

・ IoT 機器の起動時に動作するマルウェア等により、誤動作が発生する

■対策の概要

・ ソフトウェアの適切な起動順序確認機能を実装した IoT 機器の導入
・ 不正なソフトウェアの起動防止機能を実装した IoT 機器の導入

■対策ポイント

IoT 機器の起動時に、起動するソフトウェアの完全性を確認したり、不正なソフトウェアの起動を防止したりすることで、マルウェア感染等による IoT 機器の誤動作等の被害を防ぐ。

なお、ソフトウェアの起動の記録は遠隔からも確認できる必要がある。

・ ソフトウェアの完全性検証の結果を記録する

・ ソフトウェアの完全性検証の結果を遠隔地から参照できる

■構成要素毎の対策例

○組織
・ ソフトウェアのサプライヤーを特定し、そのサプライヤーから正規品を導入する。
・ 正規品であることを確認するために、ソフトウェアのサプライヤーを識別し、認証する。
・ ソフトウェアの機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。

○ヒト
（なし）

○モノ
・ 完全性を検証できたソフトウェアのみ起動する。
・ ソフトウェアの完全性検証の結果を記録する。
・ ソフトウェアの完全性検証の結果にチェックサムを付与する。
・ ソフトウェアの完全性検証の結果を遠隔地から参照できる。

○データ
・ ソフトウェア及び設定データの完全性を検証するチェックサムを付与する。

○プロシージャ
（なし）

○システム
・ ソフトウェアの機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。

L2.012 IoT 機器のマルウェアへの感染防止

■リスク要因

IoT 機器が不正に操作される。

■リスク影響

・ IoT 機器に対する不正アクセスにより、マルウェア感染被害が発生し、誤動作が発生する

■対策の概要

・ IoT 機器に対するウイルスチェックの実施

■対策ポイント

現場の IoT 機器において、定期的(起動時等)に、ウイルスチェックを行うことで、マルウェア感染被害を防ぐ。

・ セキュリティパッチ適用、ソフトウェア追加等の更新時に、ウイルス感染の有無をチェックする

・ 定期的(起動時等)に、ウイルス感染の有無をチェックする

・ ホワイトリスト以外の通信を遮断するなど IoT 機器間の通信を管理する。

■構成要素毎の対策例

○組織

・ セキュリティパッチ適用、ソフトウェア追加等の更新時に、ウイルス感染の有無をチェックする。
・ 定期的(起動時等)に、ウイルス感染の有無をチェックする。
・ ホワイトリスト以外の通信を遮断するなど IoT 機器間の通信を管理する。

○ヒト

(なし)

○モノ

・ ホワイトリスト以外の通信を遮断するなど IoT 機器間の通信を管理する。

○データ

(なし)

○プロシージャ

・ セキュリティパッチ適用、ソフトウェア追加等の更新時に、ウイルス感染の有無をチェックする。
・ 定期的(起動時等)に、ウイルス感染の有無をチェックする。
・ ウイルス感染の有無のチェックの結果を確認する。

○システム

・ ウイルス対策ソフトウェアを導入する。

L2.013 IoT 機器の継続的な脆弱性対策

■リスク要因

IoT 機器が不正に操作される。

■リスク影響

・ IoT 機器の脆弱性が悪用され、マルウェア感染被害が発生し、誤動作が発生する

■対策の概要

・ IoT 機器のセキュリティパッチの定期的な更新

■対策ポイント

脆弱性が残存した IoT 機器が稼働し続けることで、外部からの不正ログインや不正操作を引き起こしやすくなる。

IoT 機器に対し定期的な脆弱性対策を行うことで、セキュリティインシデントの発生やセキュリティ被害の拡大を防ぐ。

・ 定期的にセキュリティパッチを入手し、必要に応じて IoT 機器に適用する

・ IoT 機器のセキュリティパッチ更新履歴を確認する

■構成要素毎の対策例

○組織

・ 構成要素の脆弱性に関する公開情報を定期的及び必要に応じて確認、収集し、関連する問題に対処する体制を整える。

○ヒト

（なし）

○モノ

・ セキュリティパッチ適用、ソフトウェア更新、設定変更が可能な IoT 機器を導入する。

○データ

（なし）

○プロシージャ

・ 定期的にセキュリティパッチを入手し、必要に応じて IoT 機器に適用する。

・ IoT 機器のセキュリティパッチ更新履歴を確認する。

○システム

（なし）

L2.014 IoT 機器のリモートアップデート

■リスク要因

IoT 機器の脆弱性が発見された場合への対応(セキュリティパッチの適用等)に時間がかかる。

■リスク影響

・ セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する

■対策の概要

・ IoT 機器に対して、迅速な脆弱性対策の実施

■対策ポイント

IoT 機器に対して、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実装する。これにより、脆弱性が残存した IoT 機器が稼働し続けることなく、迅速な脆弱性対策を実施する。

・ リモートアップデートは、遠隔地との相互認証に成功した場合に操作を開始する

・ ソフトウェアの更新作業は、盗聴・改ざんに十分に配慮する

■構成要素毎の対策例

○組織

・ 構成要素の脆弱性に関する公開情報を定期的、及び必要に応じて確認、収集し、関連する問題に対処する体制を整える。

○ヒト

(なし)

○モノ

・ 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。
  - ソフトウェアの更新作業を中断した場合も再開又はやり直しが可能である。

○データ

・ ソフトウェアの更新作業は、データの暗号化やメッセージ認証コード(MAC)の付与等、盗聴・改ざんに十分に配慮する。

○プロシージャ

・ リモートアップデートは、遠隔地との相互認証に成功した場合に更新作業を開始する。

○システム

・ 外部のネットワークコネクションを介した非ローカルメンテナンスセションを確立するため、複数要素の認証を要求し、非ローカルメンテナンスの完了時にこのようなセションを終了する。

L2.015 IoT 機器に導入するソフトウェアの管理

■リスク要因

IoT 機器に、不正なソフトウェアが搭載される。

■リスク影響

- IoT 機器に搭載された不正なソフトウェアにより、マルウェア感染被害が発生し、誤動作が発生する

■対策の概要

- IoT 機器の導入前に、搭載されているソフトウェアを確認する
- IoT 機器の導入後に、追加するソフトウェアを制限する

■対策ポイント

特別な権限を必要とする等、ソフトウェアのインストールを制限する機能を実装した IoT 機器を導入することで、意図しないソフトウェアの動作による誤動作、マルウェア感染等による IoT 機器での不正な情報(データ)の生成を防ぐ。

- IoT 機器に追加/削除/更新を許可するソフトウェアの一覧(ホワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)を用いて、利用するソフトウェアを制限する
- ユーザーの役割に合わせて、ソフトウェアの使用と追加/削除/更新を制限する
- セキュリティルールに従って、ソフトウェアの追加/削除/更新を監視し、その作業履歴や監査ログを残し、定期的にレビューする

■構成要素毎の対策例

○組織

- IoT 機器で利用するソフトウェアを規定する。

○ヒト

- ユーザーの役割に合わせて、ソフトウェアの使用と追加/削除/更新を制限する。

○モノ

- ソフトウェア更新や設定変更が可能な IoT 機器を導入する。

○データ

(なし)

○プロシージャ

- セキュリティルールに従って、ソフトウェアの追加/削除/更新を監視し、その作業履歴や監査ログを残し、定期的にレビューする。。

○システム

- IoT 機器に追加/削除/更新を許可するソフトウェアの一覧(ホワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)を用いて、利用するソフトウェアを制限する。

L2.016 IoT 機器の機能の分離

■リスク要因

IoT 機器を管理するシステムの機能が不正に操作される。

■リスク影響

・ システムの管理機能に対する不正アクセスにより、設定が変更され、マルウェア感染被害が発生し、誤動作が発生する

■対策の概要

・ 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

■対策ポイント

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。これにより、システムの管理機能への不正アクセスを防止し、設定変更に伴うマルウェア感染等を防ぐ。

・ 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

■構成要素毎の対策例

○組織

・ 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。

○ヒト

・ 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。

○モノ

・ 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。

○データ

（なし）

○プロシージャ

・ 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。

○システム

（なし）

L2.017 IoT 機器におけるネットワークの分離

■リスク要因

IoT 機器を管理するシステムが不正に操作される。

■リスク影響

・ システムに対する不正アクセスにより、マルウェア感染被害が発生し、誤動作が発生する

■対策の概要

・ ネットワークの物理的又は論理的な分離

■対策ポイント

組織内のネットワークを物理的又は論理的に分離する。また、セキュリティに関する状態を示すデータ(暗号化の有無、IoT 機器のセキュリティ対策状況等)は、専用のチャネルにて取り扱う。これにより、不正アクセスや、ネットワークの負荷がネットワーク全体に影響を及ぼすことを防ぎ、インシデント発生時に問題ある IoT 機器を遮断する。

■構成要素毎の対策例

○組織

・ IoT 機器で構成する組織内のネットワークを、他のネットワークと物理的又は論理的な手法で分離する。
・ セキュリティ関連情報(監査ログ、稼働状況、IoT 機器の構成情報等)を送受信する専用チャネルを用意する。

○ヒト

(なし)

○モノ

(なし)

○データ

(なし)

○プロシージャ

(なし)

○システム

・ システムは所定のネットワーク(通信相手)にのみ接続する。
・ IoT 機器で構成する組織内のネットワークを、他のネットワークと物理的又は論理的な手法で分離する。
・ セキュリティ関連情報(監査ログ、稼働状況、IoT 機器の構成情報等)を送受信する専用チャネルを用意する。

L2.018 IoT 機器への広域ネットワークからの不正侵入対策

■リスク要因

IoT 機器が不正に操作される。

■リスク影響

・ IoT 機器に対する不正アクセスにより、マルウェア感染被害が発生し、誤動作が発生する

■対策の概要

・ ネットワーク監視によるサイバー攻撃検知
・ ファイアウォール、IDS(不正侵入検知システム)、IPS(不正侵入防止システム)の導入
・ 接続元の MAC アドレス、IoT 機器の設置場所、アクセス時間・頻度等の情報をもとにした不正接続の有無の確認

■対策ポイント

IoT 機器を管理する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、ファイアウォールや IDS、IPS 等を設置し、ネットワーク監視・アクセス監視を実施する。これにより、広域ネットワークからの不正アクセスを検知し、マルウェア感染やサイバー攻撃を受けることを防ぐ。

・ システムの仕様(プロトコル、接続先等)に合わせて、監視する事象と条件を定義する
・ セキュリティ関連情報(監査ログ、稼働状況、IoT 機器の構成情報等)を送受信する専用チャネルを用意する
・ IoT 機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する

■構成要素毎の対策例

○組織
・ IoT 機器で構成する組織内のネットワークを、他のネットワークと物理的、又は論理的な手法で分離する。
・ セキュリティ関連情報(監査ログ、稼働状況、IoT 機器の構成情報等)を送受信する専用チャネルを用意する。

○ヒト
(なし)

○モノ
(なし)

○データ
(なし)

○プロシージャ
・ 異常な通信を発見した際の振る舞いをあらかじめ定める。
  - 装置の停止／動作継続、データの無効化／再送等
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する
・ IoT 機器を管理する組織内のネットワークを広域ネットワークから分離する。

○システム
・ IoT 機器を管理する組織内のネットワークを広域ネットワークから分離する。
・ IoT 機器を管理する組織内のネットワークと広域ネットワークの接点にて通信を監視する。

- IoT 機器間での通信は、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。
- システムの仕様(プロトコル、接続先等)に合わせて、監視する事象と条件を定義する。
- セキュリティ関連情報(監査ログ、稼働状況、IoT 機器の構成情報等)を送受信する専用チャネルを用意する。

L2.019 IoT 機器における不正な無線接続への対応

■リスク要因

IoT 機器が不正に操作される。

■リスク影響

・ IoT 機器に対する不正アクセスにより、マルウェア感染被害が発生し、誤動作が発生する

■対策の概要

・ Bluetooth 等による無線接続の制限
・ 無線 LAN アクセスポイントの認証強化

■対策ポイント

IoT 機器に対し、不必要な無線接続機能(Bluetooth や無線 LAN 等)の無効化や、不特定の無線接続の制限を行う。また、接続先の認証やデータの暗号化等の適切な設定を行う。これにより、IoT 機器に対する不正アクセスを防止し、マルウェア感染、誤動作の発生等を防ぐ。

・ 無線 LAN を利用する場合は、環境設定(ESSID 、MAC アドレスフィルタリング、強固な暗号化方式(WPA2 等))を行う。
・ 無線接続先(ユーザーや IoT 機器)を正しく認証する

■構成要素毎の対策例

○組織
・ 無線接続に関する制約条件、環境設定等をあらかじめセキュリティルールに定義する。

○ヒト
・ セキュリティルールに従って無線通信を利用する。

○モノ
・ 不必要な無線接続機能(Bluetooth や無線 LAN 等)を無効化する。
・ 不特定の無線接続先(Bluetooth や無線 LAN 等)を制限する。
・ 無線通信の通信経路及び通信データそのものを暗号化する。
・ 無線接続先(ユーザーや IoT 機器)を正しく認証する。

○データ
(なし)

○プロシージャ
・ 無線接続先(ユーザーや IoT 機器)を認証した後、通信を開始する。

○システム
・ アクセスポイントでの無線通信相手の認証機能を利用する。

L2.020 IoT 機器の集中管理

■リスク要因

IoT 機器の稼働状況の把握や、セキュリティインシデントの検知に時間がかかる。

■リスク影響

・ セキュリティインシデントへの対応が遅れ、セキュリティ被害が拡大する

■対策の概要

・ IoT 機器の稼働情報等を集中管理する仕組みの導入

■対策ポイント

IoT 機器の稼働状況、監査ログ、IoT 機器の設定、ソフトウェアの構成等を遠隔地から集中管理する。これにより、稼働状況の把握やセキュリティインシデントの検知を迅速に実施する。

・ 遠隔地からの集中管理で、異常を検知した場合の振る舞いをあらかじめ定める

・ 遠隔地からの集中管理は、相互認証に成功した場合に開始する

■構成要素毎の対策例

○組織

・ IoT 機器の稼働状況、監査ログ、IoT 機器の設定、ソフトウェアの構成等を遠隔地から集中管理する。
・ 遠隔地からの集中管理で、異常を検知した場合の振る舞いをあらかじめ定める。
  - 装置の停止／動作継続、データの無効化／再送等
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する
・ IoT 機器を管理する組織内のネットワークを広域ネットワークから分離する

○ヒト

(なし)

○モノ

・ 稼働状況、監査ログ、IoT 機器の設定、ソフトウェアの構成等を遠隔地から集中管理する仕組みを備えた IoT 機器を導入する。

○データ

・ IoT 機器の情報(データ)は、セキュリティルールに従って取り扱う。
  - ユーザー認証及び IoT 機器認証に利用する鍵情報等の重要情報は暗号化して受け渡し、保存する。
  - 監査ログ等の記録は、完全性を検証するためのチェックサムを付与する。

○プロシージャ

・ 遠隔地からの集中管理は、相互認証に成功した場合に開始する。

○システム

・ ユーザーを一意に識別できる ID(識別子)を採番する。
・ IoT 機器を一意に識別できる ID(識別子)を採番する。

L2.021 IoT 機器の不正動作の検知

■リスク要因

IoT 機器が不正に動作する。

■リスク影響

・ IoT 機器が故障等により不正に動作し、作業員に危害が及ぶ、又は IoT 機器の破損が発生する

■対策の概要

・ IoT 機器が、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

■対策ポイント

指示された動作内容と、IoT 機器の動作結果を比較し、不正と判断できる動作を IoT 機器が検知する機能安全の仕組みを実装することで、IoT 機器の誤動作による現場人員の怪我、IoT 機器の破損を防ぐ。

・ 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

・ 許容範囲外等、異常と判断した場合の振る舞いをあらかじめ定義する

■構成要素毎の対策例

○組織

・ セキュリティルールで定められた、情報(データ)の取扱基準に従って送受信する。
・ 異常(許容範囲外、期待値と一致しない等)と判断した場合の振る舞いをあらかじめ定義する。
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する

○ヒト

(なし)

○モノ

・ サイバー空間から受けた、動作指示が許容範囲内であることを動作前に検証する。
・ サイバー空間から受けた、動作指示による動作の期待値と、実際の動作結果を比較検証する。

○データ

(なし)

○プロシージャ

・ 異常(許容範囲外、期待値と一致しない等)と判断した場合の振る舞いをあらかじめ定義する。
  - 装置の停止／動作継続、データの無効化／再送等
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する
・ あらかじめ定義した状態で IoT 機器の動作を継続する。
  - 例:通常運転中、異常発生中、回復作業中等

○システム

(なし)

３．３.【第 3 層】サイバー空間におけるつながりに係るセキュリティ対策

L3.001 信頼できるサービスサプライヤーの選定

■リスク要因

システムの停止が頻発する、又は復旧時間の長期化が生じる。

■リスク影響

・ システムが停止することで、情報(データ)の収集・分析・IoT 機器、サーバ等へのフィードバックができず、業務の運用に悪影響を及ぼす

■対策の概要

・ 第三者機関による評価(ITSMS 認証等)を取得したサービスサプライヤーの選択

■対策ポイント

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ぶ。これにより、サービス停止時間の長期化、サービス停止の再発等による、業務運用効率の低下を防ぐ。

・ 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

・ 企画・設計段階において実施する要件定義・設計の結果を第三者機関がセキュリティの観点から評価する

・ セキュリティインシデントの説明責任を果たせるよう、セキュリティインシデント検知におけるサプライヤーが担う役割と負う責任を明確にする

■構成要素毎の対策例

○組織

・ 第三者機関によるセキュリティ評価等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。
(例: ITSMS 認証(ISO/IEC 20000))
・ 企画・設計段階において実施する要件定義・設計の結果を第三者機関がセキュリティの観点から評価する。
・ セキュリティインシデントの説明責任を果たせるよう、セキュリティインシデント検知におけるサプライヤーが担う役割と負う責任を明確にする。

○ヒト

(なし)

○モノ

(なし)

○データ

(なし)

○プロシージャ

(なし)

○システム

（なし）

L3.002 耐タンパーデバイスを利用したIoT機器、サーバ等の導入

■リスク要因

IoT機器、サーバ等が盗難にあい、情報(データ)が不正閲覧される。

■リスク影響

・ IoT機器、サーバ等が盗難され内部に残存していた情報(データ)を解析されることで、情報(データ)が漏えいする

■対策の概要

・ 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

■対策ポイント

耐タンパーデバイスを利用したIoT機器、サーバ等を利用することで、IoT機器、サーバ等の盗難・不正閲覧による情報(データ)の漏えいを防ぐ。

■構成要素毎の対策例

○組織

・ 取り扱う情報(データ)の分類と取扱基準を、セキュリティルールに定める

○ヒト

(なし)

○モノ

・ 重要情報(秘密鍵、電子証明書等)の保存は、耐タンパーデバイスを利用したIoT機器、サーバ等を利用する。

○データ

・ 耐タンパーデバイスを利用したIoT機器、サーバ等に保存するデータは暗号化する。

○プロシージャ

(なし)

○システム

(なし)

L3.003 サイバー空間への不正ログイン対策

■リスク要因

サイバー空間にある情報(データ)が不正アクセスされる。

■リスク影響

・ 不正なユーザーによるシステムへのアクセスにより、情報(データ)が抜き取られ解析されることで、情報(データ)が漏えいする

■対策の概要

・ パスワード、生体認証、電子証明書等、二つの認証機能を組み合わせた二要素認証機能の実装

■対策ポイント

特権を持つユーザーのシステムへのログインに対して、二つの認証機能を組み合わせた二要素認証を採用する。

これにより、不正なユーザーによるシステムの情報(データ)の不正閲覧による漏えいを防ぐ。

・ 特権を持つユーザー等の認証に、二要素認証を採用する

・ 二要素認証の1つは、ユーザーの存在を確認する認証方式を採用する

・ 二要素認証の1つは、耐タンパーデバイスを用いた認証を採用する

■構成要素毎の対策例

○組織

・ ユーザーに、システムを管理するために必要な権限を与える。
・ 関係者、特に特権を持つユーザーに対して、セキュリティ上の役割と責任を正しく理解させる。
・ 認証に用いる情報の初期設定手順(パスワード等)及び設定値の更新方法を定義し、セキュリティルールに定める。
  - 新しくパスワードを設定する際、パスワードに最低限の複雑性(文字種、文字数等)を強制する。
  - 規定された生成回数の間、パスワードの再利用を禁止する。
  - システムログイン時に恒久パスワードを即時的に変更し、一時的なパスワードを使用することを許可する。

○ヒト

・ ユーザーに、システムを管理するために必要な権限を与える。
  - 特権を持つユーザーが行った管理業務を書面で記録する。
  - 権限を持たないユーザーが管理業務にあたる場合の対処を定める
    (例:管理監督者が帯同し、監視する等)
・ 特権を持つユーザー等の認証に、適切な強度を有した認証方式を採用する。
  - 二要素認証を、特権アカウントへのローカル及びネットワークアクセスのために、及び非特権アカウントへのネットワークアクセスのために、採用する。
  - 特権及び非特権アカウントへのネットワークアクセスのために、リプレイ攻撃に耐性のある認証メカニズムを採用する。

○モノ

(なし)

○データ

（なし）

○プロシージャ

（なし）

○システム

- 二要素認証の1つは、ユーザーの存在を確認する認証方式を採用する。
  (例：パスワード照合、生体(指紋等)照合等)
- 二要素認証の1つは、耐タンパーデバイスを用いた認証を採用する。
  (例：非接触カード等)
- 外部のネットワークコネクションを介した非ローカルメンテナンスセションを確立するため、複数要素の認証を要求し、非ローカルメンテナンスの完了時にこのようなセションを終了する。
- 特権ユーザーと一般ユーザーのアクセス権限は分離して管理を行う。

L3.004 サイバー空間における接続相手の識別

■リスク要因

サイバー空間における IoT 機器、サーバ等への処理結果の送信において、IoT 機器、サーバ等が誤った接続元から通信データを受信する。

■リスク影響

- 本来とは異なるサイバー空間からの情報(データ)を受け取ることで、業務の運用に悪影響を及ぼす
- IoT 機器、サーバ等の設定を誤り、本来とは異なるサイバー空間に収集データを送信することで情報(データ)が漏えいする

■対策の概要

- 接続相手の一意の識別

■対策ポイント

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、接続相手を識別する。これにより、不正な接続相手との接続を防ぎ、不正確な情報(データ)の混入に伴う業務運用効率の低下や、情報(データ)が漏えいすることを防ぐ。

- ユーザー、IoT 機器、サーバ等は自分自身の ID(識別子)を持つ
- 適切な通信相手の ID(識別子)を持つ
- データ送信前に通信相手(ユーザーや IoT 機器、サーバ等)を識別する
- 不適切な通信相手であることが判明した場合の振る舞いをあらかじめ定義する

■構成要素毎の対策例

○組織

- 不適切な通信相手であることが判明した場合の振る舞いをあらかじめ定義する。
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する
- IoT 機器、サーバ等を管理する組織内のネットワークを広域ネットワークから分離する。

○ヒト

- ユーザーは自分自身の ID(識別子)を持つ。

○モノ

- IoT 機器、サーバ等は自分自身の ID(識別子)を持つ。
- IoT 機器、サーバ等は適切な通信相手の ID(識別子)を持つ。

○データ

(なし)

○プロシージャ

- データ送信前に通信相手(ユーザーや IoT 機器、サーバ等)を識別する。
- 不適切な通信相手であることが判明した場合の振る舞いをあらかじめ定義する。
  - 装置の停止／動作継続、データの無効化／再送等
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する

・ IoT 機器、サーバ等を管理する組織内のネットワークを広域ネットワークから分離する。

〇システム

・ ユーザーを一意に識別できる ID(識別子)を採番する。
・ IoT 機器、サーバ等を一意に識別できる ID(識別子)を採番する。

L3.005 サイバー空間における接続相手の認証

■リスク要因

サイバー空間における IoT 機器、サーバ等への処理結果の送信において、IoT 機器、サーバ等が誤った接続元から通信データを受信する。

■リスク影響

- 本来とは異なるサイバー空間からの情報(データ)を受け取ることで、業務の運用に悪影響を及ぼす
- IoT 機器、サーバ等の設定を誤り、本来とは異なるサイバー空間に収集データを送信することで情報(データ)が漏えいする

■対策の概要

- 相互認証による接続相手の認証

■対策ポイント

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、双方の電子証明書等を利用した相互認証により、接続相手を認証する。これにより、現場の IoT 機器、サーバ等が相手を認証することによって、なりすましによる不正アクセスを防ぎ、不正確な情報(データ)の混入に伴う業務運用効率の低下や、情報(データ)が漏えいすることを防ぐ。

- データ送信前に、相互に認証する
- 認証に失敗した場合の振る舞いをあらかじめ定義する

■構成要素毎の対策例

○組織

- 認証失敗に対する振る舞いをあらかじめ定義する。
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する

○ヒト

- 必要に応じて、ユーザー認証に対応する。

○モノ

- データ送信前に、相互に認証する。

○データ

(なし)

○プロシージャ

- 必要に応じて、ユーザーを認証する。
- データ送信前に、相互に認証する。
  - 相互認証は、通信相手の識別に成功した後に行う
  - 認証失敗に対する振る舞いをあらかじめ定義する
  - 装置の停止／動作継続等
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する

○システム

- 必要に応じて、ユーザー認証に対応する。

・ データ送信前に、相互に認証する。

L3.006 IoT 機器、サーバ等のデータへの物理的な不正アクセス対策

■リスク要因

IoT 機器、サーバ等が不正に操作される。

■リスク影響

・ IoT 機器、サーバ等に対する物理的な不正アクセスにより、情報(データ)が漏えいする

■対策の概要

・ 監視カメラ等による物理的なアクセスの記録・監視
・ 施錠・入退室管理等による物理的なアクセスの制限

■対策ポイント

IoT 機器、サーバ等や設置エリアに対し、物理的なセキュリティ対策を行う。これにより、IoT 機器、サーバ等に対する不正アクセスを防止し、情報(データ)の漏えいを防ぐ。

・ 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対策を実施する

・ IoT 機器、サーバ等本体に対して、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

■構成要素毎の対策例

○組織
・ 要員の役割に応じて出入りできる場所を明確にする。
・ 重要な IoT 機器、サーバ等に対して盗難防止策(例:施錠)を講じる。

○ヒト
・ 要員の役割に応じて出入りできる場所を制限する。

○モノ
(なし)

○データ
(なし)

○プロシージャ
・ セキュリティ運用マニュアルに従って、監視カメラ設置、部外者の入室時における責任者の帯同等、物理的アクセスの記録や監視を行う。
・ セキュリティを保つべき領域での作業に関する手順を設計し、適用する。

○システム
・ 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対策を実施する。
・ 重要な IoT 機器、サーバ等に対して盗難防止策(例:施錠)を講じる。

L3.007 サイバー空間における不正な送受信情報(データ)の検知

■リスク要因

不正な情報(データ)が送受信される。

■リスク影響

- マルウェア感染やサイバー攻撃を受けることで、情報(データ)が不正に送受信される
- 本来とは異なるサイバー空間からの情報(データ)を受け取ることで、業務の運用に悪影響を及ぼす

■対策の概要

- 送受信する情報(データ)に対し、許容範囲内であることを動作前に検証する

■対策ポイント

サイバー空間におけるシステムや IoT 機器、サーバ等間で送受信する情報(データ)に対し、許容範囲内であることを動作前に検証し、業務の運用に悪影響を及ぼすことを防ぐ。

- 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
- 許容範囲外等、異常と判断した場合の振る舞いをあらかじめ定義する

■構成要素毎の対策例

○組織

- セキュリティルールで定められた、情報(データ)の取扱基準に従って送受信する。
- 異常(許容範囲外、期待値と一致しない等)と判断した場合の振る舞いをあらかじめ定義する。
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する

○ヒト

- IoT 機器、サーバ等の振る舞いを監視し、異常発生時にはセキュリティルールやセキュリティ対応マニュアルに沿って作業する。
  - モバイルコードの使用を管理、監視し、不正なモバイルコードを検知する。

○モノ

- サイバー空間から受ける情報(データ)が許容範囲内(過去のデータを分析した結果から得る)であることを動作前に検証する。
- 機能安全を実装した IoT 機器、サーバ等を利用する。

○データ

(なし)

○プロシージャ

- 異常(許容範囲外、期待値と一致しない等)と判断した場合の振る舞いをあらかじめ定義する。
  - 装置の停止／動作継続、データの無効化／再送等
  - 影響を受ける範囲のシステム管理者又はセキュリティ管理者へ警告・報告する
  - IoT 機器、サーバ等を管理する組織内のネットワークを広域ネットワークから分離する
- あらかじめ定義した状態で IoT 機器、サーバ等の動作を継続する。
  - 例:通常運転中、異常発生中、回復作業中等

○システム

- IoT 機器、サーバ等の振る舞いを監視する。
  - モバイルコードの使用を管理、監視し、不正なモバイルコードを検知する。

- VoIP 技術の使用を管理し、監視する。

L3.008 サイバー空間の可用性維持

■リスク要因

サイバー空間のサーバや通信機器、回線等に故障や不具合が生じる。

■リスク影響

- サイバー空間のサーバや通信機器、回線等の機能が停止し、業務の運用に悪影響を及ぼす

■対策の概要

- サービス不能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、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
- 定期的なバックアップや品質管理、冗長化、予備を確保する

■対策ポイント

サービス不能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、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。さらに、定期的なバックアップや品質管理、冗長化、予備の確保を行うことで可用性を維持する。これにより、サイバー空間のサーバ、通信機器、回線で不具合が生じた場合においても迅速な原因の特定、サービスの復旧等により、セキュリティ被害の拡大を防ぐ。

- 問い合わせ窓口やサポート体制等が確立されたサイバー空間、IoT 機器、サーバ等及びサービスのサプライヤーを選定する
- 構成要素(サーバ、通信機器、回線等)に対し、定期的なシステムバックアップ、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
- サービス不能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、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)を確保して可用性を実現する

■構成要素毎の対策例

○組織

- 問い合わせ窓口やサポート体制等が確立されたサイバー空間、IoT 機器、サーバ等及びサービスのサプライヤーを選定する。
- システムに関する機能の設計、開発、実装、修正において、セキュリティを考慮したシステム開発ライフサイクルを導入する。

○ヒト

(なし)

○モノ

(なし)

○データ

(なし)

○プロシージャ

(なし)

○システム

- システムに関する機能の設計、開発、実装、修正において、セキュリティを考慮したシステム開発ライフサイクルを導入する。

- 構成要素(サーバ、通信機器、回線等)に対し、定期的なシステムバックアップ、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。
- サービス不能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、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)を確保して可用性を実現する。
- あらかじめ定義した状態で IoT 機器、サーバ等の動作を継続する。
(例:通常運転中、異常発生中、回復作業中等)

L3.009 IoT 機器、サーバ等の適切な廃棄

■リスク要因

不適切な手順で IoT 機器、サーバ等を廃棄する。

■リスク影響

・ 廃棄された IoT 機器、サーバ等を悪用され、内部に残存する情報(データ)が漏えいする

■対策の概要

・ 適切な手順で IoT 機器、サーバ等を廃棄する

■対策ポイント

IoT 機器、サーバ等の廃棄時には、内部に保存されている情報(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。これにより、IoT 機器、サーバ等の内部に残存する情報(データ)の漏えいを防ぐ。

・ 視覚、触覚で識別できる表示のみならず、記憶領域及び耐タンパーデバイスを再生不能な手段(焼却、溶解、粉砕等)を用いて読み取りができない状態にする

・ 製造元が指定する廃棄手段を加味した廃棄手順を含む管理手順を作成する

■構成要素毎の対策例

○組織

・ IoT 機器、サーバ等の廃棄時には、情報(データ)を削除(又は読み取りできない状態に)する手順を定め、セキュリティルールに定義する。
  - 内部に保存されている情報(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、電子証明書等)を対象とする
  - 視覚、触覚で識別できる表示のみならず、記憶領域及び耐タンパーデバイスを再生不能な手段(焼却、溶解、粉砕等)を用いて読み取りができない状態にする
・ 製造元が指定する廃棄手段を加味した廃棄手順を含む管理手順を作成する。

○ヒト

・ セキュリティルールに基づく廃棄手順を順守する。
・ IoT 機器、サーバ等の中の重要情報を消去してから、保守作業を開始する。
・ 保存期限が経過したバックアップデータを消去する。
・ IoT 機器、サーバ等の管理・廃棄に係る作業履歴を残す。

○モノ

(なし)

○データ

(なし)

○プロシージャ

・ IoT 機器、サーバ等の管理・廃棄に係る作業履歴を確認する。
・ IoT 機器、サーバ等の中の重要情報を消去してから、保守作業を開始する
・ バックアップデータの保存期限と期限経過後の扱い(消去等)を定める。

○システム

(なし)

L3.010 IoT 機器、サーバ等の継続的な脆弱性対策

■リスク要因

IoT 機器、サーバ等が不正に操作される。

■リスク影響

・ IoT 機器、サーバ等の脆弱性が悪用され、情報(データ)が漏えいする

■対策の概要

・ IoT 機器、サーバ等のセキュリティパッチの定期的な更新

■対策ポイント

脆弱性が残存した IoT 機器、サーバ等が稼働し続けることで、外部からの不正ログインや不正操作を引き起こしやすくなる。

IoT 機器、サーバ等に対し定期的な脆弱性対策を行うことで、セキュリティインシデントの発生やセキュリティ被害の拡大を防ぐ。

・ 定期的にセキュリティパッチを入手し、必要に応じて IoT 機器、サーバ等に適用する

・ IoT 機器、サーバ等のセキュリティパッチ更新履歴を確認する

■構成要素毎の対策例

○組織

・ 構成要素の脆弱性に関する公開情報を定期的及び必要に応じて確認、収集し、関連する問題に対処する体制を整える。

○ヒト

(なし)

○モノ

・ セキュリティパッチ適用後も、ソフトウェア更新や設定変更が可能な IoT 機器、サーバ等を導入する。

○データ

(なし)

○プロシージャ

・ 定期的にセキュリティパッチを入手し、必要に応じて IoT 機器、サーバ等に適用する。

・ IoT 機器、サーバ等のセキュリティパッチ更新履歴を確認する。

○システム

(なし)

L3.011 サイバー空間の保管データの暗号化

■リスク要因

サイバー空間にある情報(データ)が不正アクセスされる。

■リスク影響

・ 情報(データ)が抜き取られ解析されることで、保管していた情報(データ)が漏えいする

■対策の概要

・ 保管データの機密性確保

■対策ポイント

情報(データ)を暗号化して保管する。これにより、不正アクセスによる情報(データ)漏えいを防ぐ。

・ 取り扱う情報(データ)の分類と取扱基準を、セキュリティルールに定める

・ ポータブルストレージデバイスや外部メディアに、データ又はバックアップデータ(チェックサム含む)を移す際は、保存時とは異なる鍵にて暗号化する

■構成要素毎の対策例

○組織

・ 情報(データ)の分類と取扱基準を、セキュリティルールに定める。
  - データの保存(バックアップ)、持ち出し(ポータブルストレージデバイスや外部メディアの利用)に関して規定する
・ 情報(データ)は、セキュリティルールに従って取り扱う。
・ 情報(データ)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。

○ヒト

(なし)

○モノ

(なし)

○データ

・ 情報(データ)は、セキュリティルールに従って取り扱う。
  - ユーザー認証及び IoT 機器、サーバ等認証に利用する鍵情報等の重要情報は暗号化して受け渡し、保存する
  - 監査ログ等の記録は、完全性を検証するためのチェックサムを付与する
  - バックアップを取る場合は、元データ及びバックアップデータのそれぞれを暗号化する

○プロシージャ

・ ポータブルストレージデバイスや外部メディアに、データ、又はバックアップデータ(チェックサム含む)を移す際は、保存時とは異なる鍵にて暗号化する。

○システム

(なし)

L3.012 IoT 機器、サーバ等に導入するソフトウェアの管理

■リスク要因

IoT 機器、サーバ等に、不正なソフトウェアが搭載される。

■リスク影響

・ IoT 機器、サーバ等に搭載された不正なソフトウェアにより、情報(データ)が漏えいする

■対策の概要

・ IoT 機器、サーバ等の導入前に、搭載されているソフトウェアを確認する
・ IoT 機器、サーバ等の導入後に、追加するソフトウェアを制限する

■対策ポイント

特別な権限を必要とする等、ソフトウェアのインストールを制限する機能を実装した IoT 機器、サーバ等を導入することで、意図しないソフトウェアの動作による誤動作、マルウェア感染等による情報(データ)の漏えい、IoT 機器、サーバ等での不正な情報(データ)の生成を防ぐ。

- IoT機器、サーバ等に追加/削除/更新を許可するソフトウェアの一覧(ホワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)を用いて、利用するソフトウェアを制限する
- ユーザーの役割に合わせて、ソフトウェアの使用と追加/削除/更新を制限する
- セキュリティルールに従って、ソフトウェアの追加/削除/更新を監視し、その作業履歴や監査ログを残し、定期的にレビューする

■構成要素毎の対策例

○組織
・ IoT 機器、サーバ等で利用するソフトウェアを規定する。

○ヒト
・ ユーザーの役割に合わせて、ソフトウェアの使用と追加/削除/更新を制限する。

○モノ
・ ソフトウェア更新や設定変更が可能な IoT 機器、サーバ等を導入する。

○データ
(なし)

○プロシージャ
・ セキュリティルールに従って、ソフトウェアの追加/削除/更新を監視し、その作業履歴や監査ログを残し、定期的にレビューする。。

○システム
・ IoT 機器、サーバ等に追加/削除/更新を許可するソフトウェアの一覧(ホワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)を用いて、利用するソフトウェアを制限する。

L3.013 サイバー空間における機能の分離

■リスク要因

IoT 機器、サーバ等を管理するシステムの機能が不正に操作される。

■リスク影響

・ システムの管理機能に対する不正アクセスにより、情報(データ)が漏えいする

■対策の概要

・ 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

■対策ポイント

システムにおいて、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。これにより、システムの管理機能への不正アクセスを防止し、情報(データ)の漏えいや、設定変更に伴うマルウェア感染等を防ぐ。

・ ユーザーの役割に応じて利用を許可する機能を分ける

■構成要素毎の対策例

○組織

・ 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。
・ ユーザーの役割に応じて利用を許可する機能を分ける。

○ヒト

・ 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。

○モノ

・ 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。

○データ

(なし)

○プロシージャ

・ ユーザーの役割に応じて利用を許可する機能を分ける。

○システム

(なし)

L3.014 ネットワークの分離

■リスク要因

IoT 機器、サーバ等を管理するシステムが不正に操作される。

■リスク影響

・ システムに対する不正アクセスにより、情報(データ)が漏えいする

■対策の概要

・ ネットワークの物理的又は論理的な分離

■対策ポイント

組織内のネットワークを物理的又は論理的に分離する。また、セキュリティに関する状態を示すデータ(暗号化の有無、IoT 機器、サーバ等のセキュリティ対策状況等)は、専用のチャネルにて取り扱う。これにより、不正アクセスや、ネットワークの負荷がネットワーク全体に影響を及ぼすことを防ぎ、インシデント発生時に問題ある IoT 機器を遮断する。

- IoT 機器、サーバ等で構成する組織内のネットワークを、他のネットワークと物理的、又は論理的な手法で分離する
- セキュリティ関連情報(監査ログ、稼働状況、IoT 機器、サーバ等の構成情報等)を送受信する専用チャネルを用意する

■構成要素毎の対策例

○組織

・ IoT 機器、サーバ等で構成する組織内のネットワークを、他のネットワークと物理的、又は論理的な手法で分離する。
・ セキュリティ関連情報(監査ログ、稼働状況、IoT 機器、サーバ等の構成情報等)を送受信する専用チャネルを用意する。

○ヒト

(なし)

○モノ

(なし)

○データ

(なし)

○プロシージャ

(なし)

○システム

・ システムは所定のネットワーク(通信相手)にのみ接続する。
・ IoT 機器、サーバ等で構成する組織内のネットワークを、他のネットワークと物理的、又は論理的な手法で分離する。
・ セキュリティ関連情報(監査ログ、稼働状況、IoT 機器、サーバ等の構成情報等)を送受信する専用チャネルを用意する。

L3.015 サイバー空間における不正アクセスの検知

■リスク要因

サイバー空間にある情報(データ)が不正閲覧される。

■リスク影響

・ システムや IoT 機器、サーバ等への不正なアクセスにより、構成要素にある情報(データ)が抜き取られ解析されることで、保管していた情報(データ)が漏えいする

■対策の概要

・ システムや IoT 機器、サーバ等へのアクセスに対する監査ログの実装

■対策ポイント

システムや IoT 機器、サーバ等へのアクセスに対して、監査ログを記録し、定期的にレビューする。これにより、動作状況確認において異常を検知し、情報(データ)の不正閲覧や漏えいを防ぐ。

・ 監査ログには管理のためのアクセス、起動と停止、識別又は認証の失敗等の情報を含める

・ 監査ログを利用して動作状況を確認した際、異常を検知した場合の振る舞いをあらかじめ定める

■構成要素毎の対策例

○組織

・ IoT 機器、サーバ、システム等へのアクセスに対して、監査ログを記録し、定期的にレビューする。

○ヒト

(なし)

○モノ

(なし)

○データ

・ 監査ログには以下の情報を含める。
  a. 管理のためのアクセス
  b. 起動と停止
  c. 識別、又は認証の失敗
  d. セキュアな通信経路上での完全性検証の失敗
  e. ソフトウェアの更新
  f. 各種診断結果(アンチウイルス、ネットワーク診断等)

○プロシージャ

・ 監査ログを利用して動作状況を確認した際、異常を検知した場合の振る舞いをあらかじめ定める。
  - 装置の停止／動作継続、データの無効化／再送等
  - 影響を受ける範囲のシステム管理者、又はセキュリティ管理者へ警告・報告する
  - IoT 機器、サーバ等を管理する組織内のネットワークを広域ネットワークから分離する

  【動作確認の観点】
  a. 監査ログ内の予期しない記録の有無
  b. 測定データの傾向(異常な数値の有無)
  c. 操作指示と測定データとの相関関係の妥当性
  d. ソフトウェアコンポーネントのバージョンの妥当性
  e. OS 及びアプリケーションの設定ファイルの妥当性(不正に改ざんの有無)
  f. ソフトウェアが正常に動作している(不正なソフトウェアが動作していない)
  g. 起動時の監査ログに不正な点がない。

○システム

- セキュリティインシデントを検知するため、ネットワークを監視する。
- 監査ログを暗号化して保存する。
- 監査ログは、完全性を検証するためのチェックサムを付与する。
- 監査記録を含む、組織又はセキュリティ領域内の関連する全ての情報システムについて、タイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し同期するようなシステム機能を提供する。
- オンデマンド分析と報告をサポートするため、監査情報の集約及び、報告書生成機能を提供する。

L3.016 IoT 機器、サーバ等への広域ネットワークからの不正侵入対策

■リスク要因

IoT 機器、サーバ等が不正に操作される。

■リスク影響

- IoT 機器、サーバ等に対する不正アクセスにより、情報(データ)が漏えいする
- マルウェア感染やサイバー攻撃を受けることで、情報(データ)が漏えいする

■対策の概要

- ネットワーク監視によるサイバー攻撃検知
- ファイアウォール、IDS(不正侵入検知システム)、IPS(不正侵入防止システム)の導入
- 接続元の MAC アドレス、IoT 機器、サーバ等の設置場所、アクセス時間・頻度等の情報をもとにした不正接続の有無の確認

■対策ポイント

IoT 機器、サーバ等を管理する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、ファイアウォールや IDS、IPS 等を設置し、ネットワーク監視・アクセス監視を実施する。これにより、広域ネットワークからの不正アクセスを検知し、マルウェア感染やサイバー攻撃を受けることを防ぐ。

- IoT 機器、サーバ等を管理する組織内のネットワークを広域ネットワークから分離する
- IoT 機器、サーバ等を管理する組織内のネットワークと広域ネットワークの接点にて通信を監視する
- IoT 機器、サーバ等の間での通信は、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

■構成要素毎の対策例

○組織

- IoT 機器、サーバ等で構成する組織内のネットワークを、他のネットワークと物理的、又は論理的な手法で分離する。
- セキュリティ関連情報(監査ログ、稼働状況、IoT 機器、サーバ等の構成情報等)を送受信する専用チャネルを用意する。

○ヒト

(なし)

○モノ

(なし)

○データ

(なし)

○プロシージャ

- 異常な通信を発見した際の振る舞いをあらかじめ定める。
  - 装置の停止／動作継続、データの無効化／再送等
  - 影響を受ける範囲のシステム管理者、又はセキュリティ管理者へ警告・報告する
- IoT 機器、サーバ等を管理する組織内のネットワークを広域ネットワークから分離する。

○システム

- システムは所定のネットワーク(通信相手)にのみ接続する。
- IoT 機器、サーバ等を管理する組織内のネットワークを広域ネットワークから分離する。
- IoT 機器、サーバ等を管理する組織内のネットワークと広域ネットワークの接点にて通信を監視する。
- IoT 機器、サーバ等の間での通信は、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。
- システムの仕様(プロトコル、接続先等)に合わせて、監視する事象と条件を定義する。
- セキュリティ関連情報(監査ログ、稼働状況、IoT 機器、サーバ等の構成情報等)を送受信する専用チャネルを用意する。

L3.017 IoT 機器、サーバ等の間における通信の保護

■リスク要因

IoT 機器、サーバ等間で送受信する情報(データ)が盗聴される。

■リスク影響

・ IoT 機器、サーバ等間の通信経路上で情報(データ)が漏えいする

■対策の概要

・ 通信経路の暗号化を利用して情報(データ)を送信する

■対策ポイント

IoT 機器、サーバ等の間で通信が行われる際、暗号化通信(TLS、DTLS、IPsec 等) の機能を利用し通信経路上の情報(データ)を暗号化する。さらに、電子署名やメッセージ認証コード(MAC)、チェックサム、タイムスタンプ等を付与し、改ざんを防ぐ。

・ 送信する情報(データ)に ID(識別子)を割り当てる

・ 送信する情報(データ)及び ID(識別子)にメッセージ認証コード(MAC)を付与する

■構成要素毎の対策例

○組織

・ セキュリティルールで定められた、情報(データ)の取扱基準に従って送受信する。
・ 異常を検知した場合の振る舞いをあらかじめ定める。
  - 影響を受ける範囲のシステム管理者、又はセキュリティ管理者へ警告・報告する

○ヒト

(なし)

○モノ

・ 暗号化通信(TLS、DTLS、IPsec 等)に対応する通信機器を利用する。
・ 情報(データ)そのものを暗号化する IoT 機器、サーバ等を利用する。
・ 電子署名やメッセージ認証コード(MAC)、チェックサム、タイムスタンプ等の付与に対応する IoT 機器、サーバ等を利用する。

○データ

・ 情報(データ)そのものを暗号化する。
・ 送信する情報(データ)に ID(識別子)を割り当てる。

○プロシージャ

・ 認証失敗や ID(識別子)に異常を検知した場合の振る舞いをあらかじめ定義する。
  - 装置の停止／動作継続、データの無効化／再送等
  - 影響を受ける範囲のシステム管理者、又はセキュリティ管理者へ警告・報告する
  - IoT 機器、サーバ等を管理する組織内のネットワークを広域ネットワークから分離する

○システム

・ 暗号化通信を利用する。
・ 情報(データ)そのものを暗号化する。
・ セッション内で一意に特定できる識別子を持つメッセージ認証コード(MAC)を導入する。

L3.018 サイバー空間における暗号化通信

■リスク要因

サイバー空間において送受信する情報(データ)が盗聴される。

■リスク影響

・ 通信経路上で情報(データ)が漏えいする

■対策の概要

・ 通信経路の暗号化を利用して情報(データ)を送受信する

■対策ポイント

情報(データ)を送受信する際に、暗号化通信を利用して通信経路を暗号化することで、情報(データ)の盗聴による漏えいを防ぐ。

・ 暗号化通信(TLS、DTLS、IPsec 等)に対応する通信機器を利用する

・ 通信相手を認証した後に、通信経路を暗号化する

■構成要素毎の対策例

○組織

・ セキュリティルールで定められた、情報(データ)の取扱基準に従って送受信する。
・ 異常を検知した場合の振る舞いをあらかじめ定める。
  - 影響を受ける範囲のシステム管理者、又はセキュリティ管理者へ警告・報告する。
・ 情報(データ)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。

○ヒト

(なし)

○モノ

・ 暗号化通信(TLS、DTLS、IPsec 等)に対応する通信機器を利用する。

○データ

(なし)

○プロシージャ

・ 通信相手を認証した後に、通信経路を暗号化する。
・ セッション内で一意に特定できる識別子を持つメッセージ認証コード(MAC)を導入する。
・ 受信データの完全性検証に失敗した場合、暗号通信(セッション)に利用した鍵を消去する。

○システム

・ 暗号化通信を利用する。

L3.019 サイバー空間における送受信情報(データ)の暗号化

■リスク要因

サイバー空間において送受信する情報(データ)が盗聴される。

■リスク影響

・ 通信経路上で情報(データ)が漏えいする

■対策の概要

・ 情報(データ)そのものを暗号化して送受信する

■対策ポイント

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ことで、情報(データ)の盗聴による漏えいを防ぐ。

- セキュリティルールで定められた、情報(データ)の取扱基準に従って送受信する
- 情報(データ)そのものを暗号化する IoT 機器、サーバ等を利用する
- 暗号／復号における異常に対する振る舞いをあらかじめ定義する

■構成要素毎の対策例

○組織

・ セキュリティルールで定められた、情報(データ)の取扱基準に従って送受信する。
・ 異常を検知した場合の振る舞いをあらかじめ定める。
  - 影響を受ける範囲のシステム管理者、又はセキュリティ管理者へ警告・報告する
・ 情報(データ)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。

○ヒト

(なし)

○モノ

・ 情報(データ)そのものを暗号化する IoT 機器、サーバ等を利用する。

○データ

・ 情報(データ)そのものを暗号化する。

○プロシージャ

・ 暗号／復号における異常に対する振る舞いをあらかじめ定義する。
  - 装置の停止／動作継続、データの無効化／再送等
  - 影響を受ける範囲のシステム管理者、又はセキュリティ管理者へ警告・報告する
・ IoT 機器、サーバ等を管理する組織内のネットワークを広域ネットワークから分離する。

○システム

・ 情報(データ)そのものを暗号化する。

L3.020 サイバー空間における送受信情報(データ)の改ざん対策、トレーサビリティ

■リスク要因

通信経路上で情報(データ)が改ざんされる。

■リスク影響

・ 送受信する情報(データ)が改ざんされる

■対策の概要

・ 送受信する情報(データ)に電子署名やメッセージ認証コード(MAC)やチェックサム、タイムスタンプ等を付与し、改ざんを検知する

■対策ポイント

情報(データ)を送受信する際に、情報(データ)に電子署名やメッセージ認証コード(MAC)やチェックサム、タイムスタンプ等を付与することで、改ざんを防ぎ、データのトレーサビリティを確保する。

・ セキュリティルールで定められた、情報(データ)の取扱基準に従って送受信する

・ 送受信する情報(データ)に電子署名やメッセージ認証コード(MAC)やチェックサム、タイムスタンプ等を付与する

・ 暗号／復号における異常に対する振る舞いをあらかじめ定義する

■構成要素毎の対策例

○組織

・ セキュリティルールで定められた、情報(データ)の取扱基準に従って送受信する。
  - 異常を検知した場合の振る舞いをあらかじめ定める。
  - 影響を受ける範囲のシステム管理者、又はセキュリティ管理者へ警告・報告する
・ 情報(データ)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。

○ヒト

(なし)

○モノ

・ 電子署名やメッセージ認証コード(MAC)やチェックサム、タイムスタンプ等を付与に対応する IoT 機器、サーバ等を利用する。

○データ

・ 送受信する情報(データ)に電子署名やメッセージ認証コード(MAC)やチェックサム、タイムスタンプ等を付与する。

○プロシージャ

・ 暗号／復号における異常に対する振る舞いをあらかじめ定義する。装置の停止／動作継続、データの無効化／再送等。
  - 影響を受ける範囲のシステム管理者、又はセキュリティ管理者へ警告・報告する
・ IoT 機器、サーバ等を管理する組織内のネットワークを広域ネットワークから分離する。

○システム

・ 送受信する情報(データ)に電子署名やメッセージ認証コード(MAC)やチェックサム、タイムスタンプ等を付与する。

L3.021 不正な無線接続への対応

■リスク要因

IoT 機器、サーバ等が不正に操作される。

■リスク影響

・ IoT 機器、サーバ等に対する不正アクセスにより、情報(データ)が漏えいする

■対策の概要

・ Bluetooth 等による無線接続の制限
・ 無線 LAN アクセスポイントの認証強化

■対策ポイント

IoT 機器、サーバ等に対し、不必要な無線接続機能(Bluetooth や無線 LAN 等)の無効化や、不特定の無線接続の制限を行う。また、接続先の認証やデータの暗号化等の適切な設定を行う。これにより、IoT 機器、サーバ等に対する不正アクセスを防止し、情報(データ)の漏えいやマルウェア感染等を防ぐ。

・ 無線 LAN を利用する場合は、環境設定(ESSID 、MAC アドレスフィルタリング、強固な暗号化方式(WPA2 等))を行う

・ 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

■構成要素毎の対策例

○組織
・ 無線接続に関する制約条件、環境設定等をあらかじめセキュリティルールに定義する。

○ヒト
・ セキュリティルールに従って無線通信を利用する。

○モノ
・ 不必要な無線接続機能(Bluetooth や無線 LAN 等)を無効化する。
・ 不特定の無線接続先(Bluetooth や無線 LAN 等)を制限する。
・ 無線通信の通信経路及び通信データそのものを暗号化する。
・ 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。

○データ
(なし)

○プロシージャ
・ 無線接続先(ユーザーや IoT 機器、サーバ等)を認証した後、通信を開始する。

○システム
・ アクセスポイントでの無線通信相手の認証機能を利用する。

L3.022 適切な区分を踏まえたデータの管理

■リスク要因

各種法令や取決め等によって要求されるデータ(個人情報、営業秘密、CUI[5]等)の保護の水準を適切に確保できなくなる。

■リスク影響

- 各種法令や取決め等によっては、要求されるデータの保護の水準が異なることになるが、データを区分して管理しないことにより、要求を満たしていない不十分な保護によって漏えい等が起きた場合の賠償責任の重大化や、逆に過剰な保護による管理コストの増大等が発生する

■対策の概要

- 各種法令や取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、区分毎に適切なデータの保護を行う

■対策ポイント

各種法令や取決め等では、データの保護を必要とする背景を基にそれぞれ要求するデータの保護の水準が異なることになる。データを保持しようとする組織又はヒトは、法令の制定背景や関係者間で定めた取決めの理由を的確に把握し、それらを踏まえてデータを区分し、要求されるデータの保護の水準を満たすように管理する。

■構成要素毎の対策例

○組織

- データ区分及び区分されたデータの管理方法に関する規則を定める。
  - システムメディア上の各種法令や取決め等により一定水準の保護が要求される情報 へのアクセスを許可された利用者に制限する。
  - 各種法令や取決め等により一定水準の保護が要求される情報 を含む組織のシステムへのアクセスを許可する前に、個人を審査する。
  - 適用可能な各種法令や取決め等と整合性のあるプライバシーとセキュリティの通知を提供する。
  - 各種法令や取決め等により一定水準の保護が要求される情報 の機密性を保護するために使用されるとき、安全性が十分に確保されていると評価された暗号技術を採用する。
  - 離職または配置転換等の人事措置の間と後で、各種法令や取決め等により一定水準の保護が要求される情報及びそのような情報 を含む組織のシステムが保護されることを保証する。
  - IoT 機器、サーバ等の中の各種法令や取決め等により一定水準の保護が要求される情報を消去してから、保守作業を開始する。
  - IoT 機器、サーバ等の廃棄時に、各種法令や取決め等により一定水準の保護が要求される情報を削除(又は読み取りできない状態に)する手順を定め、セキュリティルールに定義する。
  - 各種法令や取決め等により一定水準の保護が要求される情報を格納し配付期限を設定した外部メディアに対しては、取扱いに関する警告表示、配付制限等のラベリングを行う。
  - 所有者が特定できないポータブルストレージデバイスの利用は禁止する。
- 構成要素の資産管理では、種別、重要性、ビジネス的価値に基づき、装置(ハードウェア、ソフトウェア)のリソース割り当ての優先付けを行う。

○ヒト

- データ区分の必要を理解し、データ区分に応じて求められる保護の水準を満たす管理を実施する。
- IoT 機器、サーバ等の中の各種法令や取決め等により一定水準の保護が要求される情報を消去してから、保

[5] Controlled Unclassified Information の略。管理すべき重要情報ではあるが、米国連邦政府が秘・極秘・機密等のように特別な取扱を定めてはいない情報を指す。

守作業を開始する。

○モノ

（なし）

○データ

・ モバイル端末及び、モバイルコンピューティングプラットフォーム上の各種法令や取決め等により一定水準の保護が要求される情報を暗号化して受け渡し、保存する。

○プロシージャ

（なし）

○システム

・ 各種法令や取決め等により一定水準の保護が要求される情報の機密性を保護するために使用されるとき、安全性が十分に確保されていると評価された暗号技術を採用する。
・ 公開アクセス可能なシステムにおいて掲載または処理される各種法令や取決め等により一定水準の保護が要求される情報を制御する。

L3.023 適切な区分を踏まえた権限の管理

■リスク要因

サイバー空間にある情報(データ)が不正アクセスされる。

■リスク影響

・ 不正なユーザーによるシステムへのアクセスにより、情報(データ)が抜き取られ解析されることで、情報(データ)が漏えいする。

■対策の概要

・ データへのアクセスを、正しく権限を付与されたユーザーや、ユーザーを代行して動作するプロセスに制限するだけでなく、ユーザーに実行が許可されるトランザクション（処理）と機能の種類についても制限する。
・ データへのアクセスを、正しく権限を付与された IoT 機器、サーバ等や、これらの機器を代行して動作するプロセスに制限するだけでなく、これらの機器に実行が許可されるトランザクション（処理）と機能の種類についても制限する。

■対策ポイント

サイバー空間にある資産へのアクセス要求に対して、適切な強度の認証を行うだけでなく、ユーザーあるいは IoT 機器、サーバ等の役割に合わせて、データ等に対する権限(追加/削除/更新)を最小限に制限する必要がある。

・ 最小権限および職務の分離の原則を取り入れて、アクセス権限を管理している。

■構成要素毎の対策例

○組織

・ 情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則を、明確化し、文書化し、実施する。
・ ユーザーあるいは IoT 機器、サーバ等の役割に合わせて、ソフトウェア、データ等の使用と追加/削除/更新を制限し、割り当てたアクセス権限を定期的にレビューする。
  - 監査機能の管理を特権利用者の一部に制限する。
  - 特権コマンドのリモート実行とセキュリティ関連情報へのリモートアクセスを許可する。
・ 具体的なセキュリティ機能と特権アカウントを含め、特権の最小化の原則を採用する。

○ヒト

・ 悪意のあるアクティビティのリスク低減のため、個人の職務を分離する。
・ 非セキュリティ機能にアクセスするときは、非特権アカウントまたは役割を使用する。

○モノ

(なし)

○データ

(なし)

○プロシージャ

(なし)

○システム

・ ユーザーあるいは IoT 機器、サーバ等の役割に合わせて、ソフトウェア、データ等の使用と追加/削除/更新を制限する。

4．信頼の確保に向けて

4．1．フレームワークにおける信頼の確保の考え方

サイバーフィジカルシステムのセキュリティを確保するため、それぞれの構成要素についてのセキュリティの確保(信頼の創出)とその確認(信頼の証明)を繰り返し行い、信頼のチェーンを構築、維持することで、価値創造過程全体のセキュリティを実現する。

1. **信頼の創出**
   - セキュリティ要件を満たすモノ・データ等の生成
   - 対象のモノ・データ等が要件を満たした形で生成されたことの確認
2. **信頼の証明**
   - 対象のモノ・データ等が正常に生成されたものであることを確認できるリスト(トラストリスト)の作成と管理
   - トラストリストを参照することで対象のモノ・データ等が信頼できるものであることの確認
3. **信頼のチェーンの構築と維持**
   - 信頼の創出と証明を繰り返すことで信頼のチェーンの構築(トレーサビリティの確保)
   - 信頼のチェーンに対する外部からの攻撃等の検知・防御
   - 攻撃に対するレジリエンスの強化

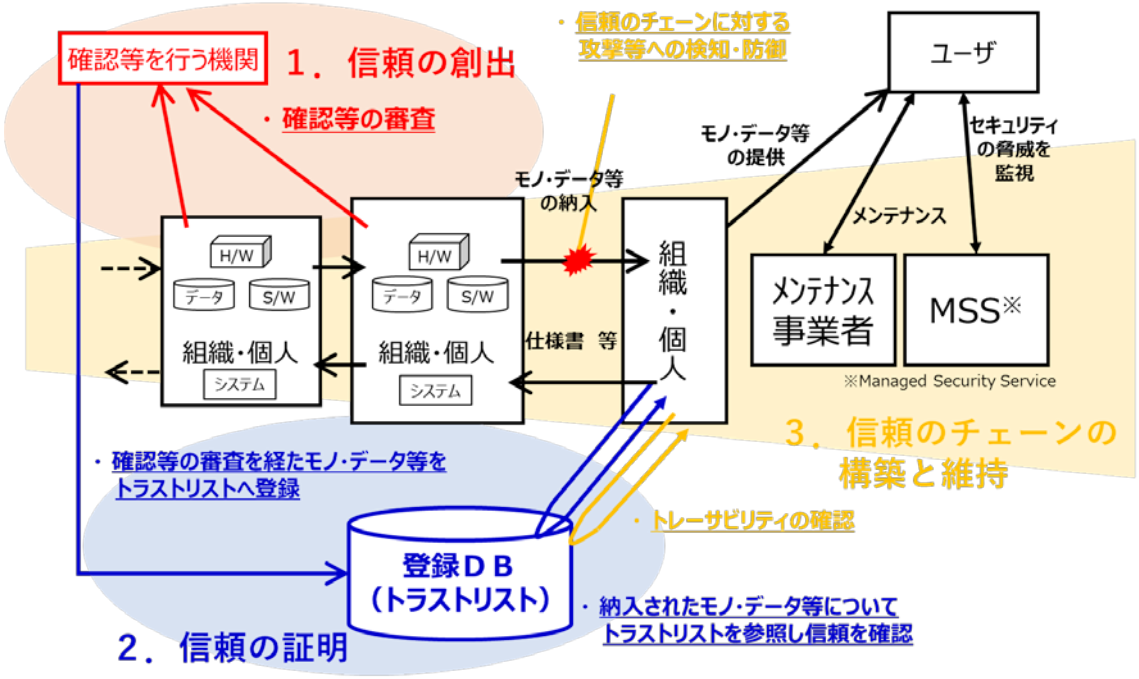


図 8 信頼の創出、信頼の証明、信頼のチェーンの構築と維持の関係のイメージ

付録 A　参考文献リスト

- Framework for Cyber-Physical Systems [Release 1.0]（NIST Cyber Physical Systems Public Working Group）

  （CPS の包括的な分析を可能にするためのフレームワーク。）

  https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf

- Framework for Improving Critical Infrastructure Cybersecurity [Version 1.1 Draft 2]（NIST）

  （重要インフラに係る企業向けに実施すべきセキュリティ対策を「特定」、「防御」、「検知」、「対応」、「復旧」の 5 つの機能に分類し、さらにそれらの機能を 22 のカテゴリーで提示した米国のガイドライン。重要インフラ以外の企業でも活用可能。）

  https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf

- The Industrial Internet of Things Volume G1: Reference Architecture [Version 1.8]（IIC）

  （Industrial Internet of Things（IIoT）システムを共通のフレームワークと概念に基づき、独自のシステムを設計するためのリファレンスアーキテクチャ。）

  http://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf

- Industrial Internet of Things Volume G4: Security Framework（IIC）

  （専門家のビジョン、経験、セキュリティのベストプラクティスからなる、詳細な業界横断的のセキュリティフレームワーク。）

  http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

- IEC 62443（IEC）

  （汎用制御システムのセキュリティ要件を定めた国際標準規格であり、制御システムのセキュリティマネジメントを定めた規格、制御システムが準拠すべきセキュリティ規格、制御システムを構成するコンポーネントが準拠すべきセキュリティ規格など、複数の規格群より構成される。）

- ISO/IEC 27002:2013（ISO/IEC）

  （情報マネジメントシステムの仕様を定めた国際標準規格であり、情報セキュリティ管理のベストプラクティスを提供。）

- IoT セキュリティガイドライン [ver 1.0]（経済産業省／総務省）

  （IoT 特有の性質と IoT でのセキュリティ対策の必要性を踏まえて、IoT 機器やシステム、サービスについて、セキュリティ・バイ・デザインを基本原則としつつ、セキュリティ確保等の観点から求められる基本的な取組を明確化するためのガイドライン。）

  http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html

- ITSMS 適合性評価制度（JIPDEC）

  （国際的に整合性のとれた IT サービスマネジメントに対する第三者適合性評価制度。）

  https://isms.jp/isms.html

- Draft NISTIR 8200（NIST）

  （「NISTIR 8074」をもとに、11 のサイバーセキュリティコア領域について説明し、関連する標準の例を示すとともに、IoT の一般的なアプリケーションと IoT の 5 つのアプリケーションのそれぞれの分野について、IoT サイバーセキュリティの目的、リスク、及び脅威を分析した報告書。）

  https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf

- NIST SP800-53 [Rev.4]（NIST）

  （連邦政府機関が実施すべきセキュリティ対策を提示した米国のガイドライン。米国連邦政府向けのクラウドサービスを提供する際に、本ガイドラインへの準拠が要求される場合がある。）

  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

- NIST SP800-161（NIST）

  （ICT サプライチェーンリスクの管理を支援するための、リスク管理プロセスの特定、評価、選択、実施、及び組織全体の統制の緩和に関する指針。）

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

- NIST SP800-171 [Rev.1]（NIST）

  （連邦政府機関以外の組織及び情報システムに対する CUI[6]を保護する上で実施すべきセキュリティ対策を提示した米国のガイドライン。米国連邦政府関係の業務を受託する際に、本ガイドラインへの準拠が要求される場合がある。）

  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

- Secure cross-company communication（Plattform Industrie 4.0）

  （Industrie 4.0 の環境で特に会社間のバリューネットワークのニーズを扱う、安全な通信のための基本的な要件、セキュリティの課題、各種アプローチについての共通の立場を策定した報告書。）

  https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/secure-cross-company-communication.html

- Secure Identities（Plattform Industrie 4.0）

  （Industrie 4.0 環境での安全なアイデンティティのためのセキュリティの課題、要件、及びアプローチの概要を提供するための報告書。）

  https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/secure-identities.html

- Security in RAMI4.0（Plattform Industrie 4.0）

  （インダストリー4.0 のリファレンスアーキテクチャモデルである RAMI4.0（Reference Architecture Model Industrie 4.0）の様々なセキュリティ面の明確な概要を紹介。）

[6] Controlled Unclassified Information の略。管理すべき重要情報ではあるが、連邦政府が秘・極秘・機密等のように特別な取扱を定めてはいない情報を指す。

http://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/security-rami40-en.pdf;jsessionid=FF86A6CB8A08538B1325F55506938D36?__blob=publicationFile&v=7

- Structure of the Administration Shell（Plattform Industrie 4.0）

  （「管理シェル」の構造に関して、ZVEI「モデルと標準」SG における技術的な議論をまとめた報告書。）

  https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/structure-of-the-administration-shell.html

- Umsetzungsstrategie Industrie 4.0(インダストリー4.0 実現戦略)（Plattform Industrie 4.0）

  （インダストリー4.0 の研究ロードマップや構成する要素の構造と機能、安全性に対する要求等をまとめた調査報告書。）

  https://www.jetro.go.jp/ext_images/_Reports/01/c982b4b54247ac1b/20150076.pdf

- サイバーセキュリティ経営ガイドライン [Ver.2.0]（経済産業省／IPA）

  （サイバーセキュリティ経営ガイドラインの 3 原則、重要 10 項目を具体的に実施するための考え方。）

  http://www.meti.go.jp/policy/netsecurity/mng_guide.html

- サイバーセキュリティ戦略（NISC）

  （サイバーセキュリティ基本法を踏まえ、「自由、公正かつ安全なサイバー空間」を創出・発展させ、「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」に寄与することを目的とした方針。）

  http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf

- サイバーセキュリティマネジメントシステム（CSMS）適合性評価制度（JIPDEC）

  （産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムにおける国際標準規格 IEC62443-2 に基づいて第三者認証を行う制度。）

  https://isms.jp/csms.html

- 情報セキュリティ早期警戒パートナーシップガイドライン [2017 年版]（IPA）

  （脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルス等による被害発生を抑制するために、関係者に推奨する行為をとりまとめたガイドライン。）

  https://www.ipa.go.jp/security/ciadr/partnership_guide.html

- 情報セキュリティマネジメントシステム（ISMS）適合性評価制度（JIPDEC）

  （情報セキュリティマネジメントシステムにおける国際標準規格 ISO/IEC27001 に基づいて第三者認証を行う制度。）

  https://isms.jp/isms.html

- セキュリティ評価基準 [CC バージョン 3.1 リリース 5]（IPA）

  （情報技術セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するためのセキュリティ評価基準。）

  https://www.ipa.go.jp/security/jisec/cc/index.html

○ つながる世界の開発指針 [第 2 版]（IPA）

（IoT 製品があらゆるモノとつながることを想定し、IoT 製品の開発者が開発時に考慮すべきリスクや対策を指針として明確化した開発指針。）

https://www.ipa.go.jp/sec/reports/20160324.html

○ JVN（IPA、JPCERT/CC）

（日本で使用されているソフトウェア等の脆弱性関連情報とその対策情報を提供する、脆弱性対策情報ポータルサイト。）

https://jvn.jp/

○ CSIRT 構築マテリアル（JPCERT/CC）

（組織的なインシデント対応を行うための CSIRT を構築する上で、「構想フェーズ」、「構築フェーズ」、「運用フェーズ」のそれぞれの段階で考慮すべきポイントを解説したガイドライン。）

https://www.jpcert.or.jp/csirt_material/

○ 事業継続ガイドライン [平成 25 年 8 月改訂]（内閣府）

（事業継続計画の策定・改善にあたって、事業継続の必要性を明示し、実施が必要な事項、望ましい事項等を提示したガイドライン。）

http://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline03.pdf

○ SECURITY ACTION セキュリティ対策自己宣言 （IPA）

（中小企業がセキュリティ対策に取り組むことを自己宣言する制度。）

https://www.ipa.go.jp/security/security-action/

○ サイバー情報共有イニシアティブ（J-CSIP） （IPA）

（重要インフラで利用される機器の製造業者、電力業界、ガス業界、化学業界、石油業界、資源開発業界、自動車業界、クレジット業界において情報共有と早期対応を行うための活動。）

https://www.ipa.go.jp/security/J-CSIP/

なお、包括的な形ではないものの、IEC61508 などの関連規格も参照している。

付録 B　主な国際規格との比較

本フレームワークの作成にあたり、様々な規格やガイドラインなどを参照した。
ここに、本フレームワークと以下の規格との対応関係を示す。

- ISO/IEC 27001:2013
- NIST:「Framework for Improving Critical Infrastructure Cybersecurity Version 1.0」（CSF V1.0）
- NIST:「Framework for Improving Critical Infrastructure Cybersecurity Version 1.1」（CSF V1.1）
- NIST:「Special Publication 800-171」(SP 800-171)

対策番号	フレームワーク/規格名	Subcategory ID
L1.001	ISO/IEC 27001:2013	A.5.1.1, A.7.2.2, A.15.1.3, A.15.2.1, A.15.2.2, A.12.6.1, A.18.2.3, A.16.1.3
	CSF V1.0	DE.CM-1, ID.AM-6, ID.BE-1, ID.BE-2, ID.BE-3, ID.GV-1, ID.GV-2, ID.RA-1, PR.AT-3, RC.CO-1
	CSF V1.1	ID.AM-6, ID.BE-2
	SP800-171	3.11.2, 3.12.2, 3.14.3, 3.14.6
L1.002	ISO/IEC 27001:2013	A.6.1.5, A.6.2.1, A.6.2.2, A.7.1.1, A.7.2.3, A.7.3.1, A.8.1.4, A.8.2.1, A.9.2.6, A.10.1.1, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.2, A.11.2.3, A.12.1.1, A.12.1.3, A.12.1.4, A.12.6.1, A.13.1.1, A.13.2.1, A.14.1.1, A.14.2.1,

		A.14.2.5, A.14.2.6, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.16.1.6, A.18.2.3
	CSF V1.0	DE.CM-3, DE.CM-7, ID.AM-5, ID.BE-4, ID.GV-4, ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, ID.RM-2, ID.RM-3, PR.AC-2, PR.AC-3, PR.DS-7, PR.IP-2, PR.IP-11,
	CSF V1.1	ID.GV-4, ID.RA-3, ID.RA-4, ID.RA-6, ID.RM-2, ID.RM-3, ID.SC-1
	SP800-171	3.10.1, 3.10.4, 3.11.1, 3.12.4, 3.13.2, 3.13.7, 3.10.6
L1.003	ISO/IEC 27001:2013	A.6.1.1, A.6.1.3, A.16.1.1, A.16.1.2
	CSF V1.0	DE.AE-5, DE.DP-1, DE.DP-4, RC.CO-3, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.CO-5
	SP800-171	3.6.1, 3.6.2
L1.004	ISO/IEC 27001:2013	A.6.1.5, A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6, A.13.1.2, A.13.2.2, A.14.1.1, A.14.2.1, A.14.2.5, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.16.1.4, A.16.1.7

	CSF V1.0	DE.CM-6, ID.AM-4, PR.IP-2, PR.MA-1, RS.AN-3, RS.AN-4
	CSF V1.1	ID.SC-1, ID.SC-3, ID.SC-4
	SP800-171	3.1.20, 3.7.2, 3.13.2, 3.13.7
L1.005	ISO/IEC 27001:2013	A.5.1.2, A.6.1.4, A.7.2.2, A.12.6.1, A.14.2.7, A.14.2.8, A.15.2.1, A.16.1.1, A.16.1.3, A.16.1.4, A.16.1.6, A.17.1.3, A.18.1.4, A.18.2.2
	CSF V1.0	DE.AE-2, DE.CM-1, DE.CM-6, DE.CM-8, DE.DP-2, DE.DP-3, DE.DP-5, ID.GV-4, ID.RA-2, ID.RM-1, PR.IP-7, PR.IP-10, PR.IP-12, RC.IM-1, RC.IM-2, RS.IM-1, RS.IM-2, RS.MI-3
	CSF V1.1	ID.GV-4, ID.RA-2, ID.RM-1, ID.SC-5
	SP800-171	3.2.3, 3.10.3, 3.11.1, 3.11.3, 3.12.1, 3.12.3, 3.14.3, 3.14.6
L1.006	ISO/IEC 27001:2013	A.6.1.1, A.7.2.2, A.16.1.5, A.17.1.3
	CSF V1.0	PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5, PR.IP-10, RS.MI-1
	CSF V1.1	ID.SC-5

	SP800-171	3.2.1, 3.2.2, 3.6.1, 3.6.3
L1.007	ISO/IEC 27001:2013	A.8.1.1, A.8.1.2, A.8.1.3, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.10.1.2, A.11.2.7, A.11.2.9, A.12.1.2, A.12.5.1, A.12.6.1, A.12.6.2, A.13.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.18.2.3
	CSF V1.0	DE.AE-1, ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-5, ID.RA-1, PR.AC-1, PR.DS-3, PR.IP-3, PR.PT-2
	SP800-171	3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5, 3.5.2, 3.8.1, 3.8.5, 3.8.7, 3.8.8
L1.008	ISO/IEC 27001:2013	A.12.2.1, A.12.4.1, A.12.4.3, A.16.1.5, A.16.1.6
	CSF V1.0	DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-7, ID.RA-3, RS.AN-1, RS.AN-2, RS.CO-4, RS.MI-1, RS.MI-2, RS.RP-1
	CSF V1.1	ID.RA-3
	SP800-171	3.3.5
L1.009	ISO/IEC 27001:2013	A.11.1.4, A.16.1.1, A.16.1.5, A.16.1.6, A.17.1.1, A.17.1.2, A.17.2.1

	CSF V1.0	ID.BE-5, ID.RA-4, PR.IP-9, RC.CO-2, RC.IM-1, RC.IM-2, RC.RP-1, RS.IM-1, RS.IM-2
	CSF V1.1	ID.BE-5, ID.RA-4
L1.010	ISO/IEC 27001:2013	A.18.1.1, A.18.1.2, A.18.1.5
	CSF V1.0	ID.GV-3
L1.011	ISO/IEC 27001:2013	A.18.1.3
L1.012	ISO/IEC 27001:2013	A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
	CSF V1.0	PR.DS-1, PR.DS-5
L1.013	ISO/IEC 27001:2013	A.6.1.4, A.16.1.2
	CSF V1.0	ID.RA-2、RS.CO-5
L2.001	ISO/IEC 27001:2013	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.14.2.6, A.14.2.9, A.14.3.1
	CSF V1.0	PR.IP-2
	SP800-171	3.13.2
L2.002	ISO/IEC 27001:2013	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.14.2.6
	CSF V1.0	PR.IP-2

	SP800-171	3.13.2
L2.003	ISO/IEC 27001:2013	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.14.2.6
	CSF V1.0	PR.IP-2
	SP800-171	3.13.2
L2.004	ISO/IEC 27001:2013	A.6.1.5, A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.14.1.1, A.14.2.1, A.14.2.5, A.14.2.6
	CSF V1.0	PR.AC-1, PR.IP-2
	SP800-171	3.5.1
L2.005	ISO/IEC 27001:2013	A.9.1.2, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
	CSF V1.0	PR.IP-1, PR.PT-3
	SP800-171	3.4.6, 3.5.7, 3.5.8, 3.5.9
L2.006	ISO/IEC 27001:2013	A.9.2.2, A.11.2.8
	SP800-171	3.1.1, 3.1.10, 3.1.11, 3.5.2, 3.13.9, 3.13.12, 3.14.1, 3.14.7
L2.007	CSF V1.0	DE.CM-3, DE.CM-7
	SP800-171	3.1.8, 3.7.6
L2.008	ISO/IEC 27001:2013	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.8

	CSF V1.0	DE.CM-2, DE.CM-3, PR.AC-2, PR.IP-5, PR.PT-3
	SP800-171	3.10.2, 3.10.3, 3.10.5
L2.009	ISO/IEC 27001:2013	A.6.1.5, A.11.1.4, A.14.1.1, A.14.2.1, A.14.2.5, A.14.2.6, A.15.2.1, A.15.2.2, A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1, A.18.1.3
	CSF V1.0	PR.DS-4, PR.IP-2, PR.IP-4
	CSF V1.1	ID.BE-5, ID.SC-2
L2.010	ISO/IEC 27001:2013	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
	CSF V1.0	PR.IP-6
	SP800-171	3.7.3
L2.011	ISO/IEC 27001:2013	A.6.1.5, A.12.2.1, A.12.5.1, A.14.1.1, A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.5, A.14.2.6
	CSF V1.0	PR.DS-6, PR.IP-2
L2.012	ISO/IEC 27001:2013	A.12.2.1
	SP800-171	3.7.4, 3.14.5
L2.013	ISO/IEC 27001:2013	A.6.1.4
	CSF V1.0	ID.RA-2
L2.014	ISO/IEC 27001:2013	A.6.1.4, A.11.2.4, A.12.6.1, A.15.1.1, A.15.2.1, A.16.1.3

	CSF V1.0	DE.CM-8, ID.RA-2, PR.MA-2
	CSF V1.1	ID.RA-2
	SP800-171	3.7.5, 3.13.15
L2.015	CSF V1.0	DE.CM-7, PR.PT-1
	SP800-171	3.1.2, 3.3.1, 3.4.8, 3.4.9
L2.016	SP800-171	3.13.3
L2.017	ISO/IEC 27001:2013	A.12.4.2, A.13.1.1, A.13.1.3, A.13.2.1
	CSF V1.0	PR.AC-5, PR.PT-4
L2.018	ISO/IEC 27001:2013	A.12.4.2, A.13.1.1, A.13.1.3, A.13.2.1
	CSF V1.0	DE.CM-1, DE.CM-7, PR.AC-5, PR.PT-4
	SP800-171	3.1.12, 3.14.1, 3.14.2, 3.14.3, 3.14.6
L2.019	ISO/IEC 27001:2013	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
	CSF V1.0	PR.DS-2
	SP800-171	3.1.14, 3.1.16, 3.1.17, 3.1.18
L2.020	ISO/IEC 27001:2013	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.12.1.2, A.12.2.1, A.12.4.2, A.12.5.1, A.12.6.2, A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3, A.14.2.2, A.14.2.3, A.14.2.4

	CSF V1.0	PR.AC-1, PR.AC-5, PR.DS-6, PR.IP-1, PR.PT-4
	SP800-171	3.1.12, 3.3.2, 3.3.8, 3.5.1, 3.5.10, 3.5.11, 3.5.5, 3.5.5, 3.8.1, 3.8.6, 3.13.10, 3.13.8, 3.14.1
L2.021	ISO/IEC 27001:2013	A.16.1.2, A16.1.5
	SP800-171	3.10.6, 3.13.4, 3.14.1
L3.001	ISO/IEC 27001:2013	A.6.1.1, A.15.2.1, A.15.2.2
	CSF V1.0	DE.DP-1
	CSF V1.1	ID.SC-2
L3.002	ISO/IEC 27001:2013	A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
	CSF V1.0	PR.DS-1, PR.DS-5
	SP800-171	3.8.1
L3.003	ISO/IEC 27001:2013	A.9.1.2, A.9.2.2
	SP800-171	3.1.7, 3.5.3, 3.5.4, 3.7.6
L3.004	ISO/IEC 27001:2013	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.13.1.1, A.13.1.3, A.13.2.1, A.13.1.1, A.13.2.1
	CSF V1.0	PR.AC-1, PR.AC-5, PR.PT-4

	SP800-171	3.1.12, 3.3.2, 3.14.1
L3.005	ISO/IEC 27001:2013	A.9.1.2, A.9.2.2, A16.1.2
	SP800-171	3.13.15, 3.14.1
L3.006	ISO/IEC 27001:2013	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.2, A.11.2.3
	CSF V1.0	DE.CM-2, DE.CM-3, PR.AC-2, PR.IP-5
	SP800-171	3.4.7, 3.10.2, 3.10.3, 3.10.5
L3.007	ISO/IEC 27001:2013	A.12.2.1, A.12.5.1, A.13.1.1, A.13.1.3, A.13.2.1
	CSF V1.0	DE.CM-4, DE.CM-5, PR.AC-5, PR.PT-4
	SP800-171	3.1.3, 3.5.6, 3.13.4, 3.13.13
L3.008	ISO/IEC 27001:2013	A.6.1.5, A.11.1.4, A.12.3.1, A.14.1.1, A.14.2.1, A.14.2.5, A.14.2.6, A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1, A.18.1.3
	CSF V1.0	PR.IP-2, PR.IP-4
	CSF V1.1	ID.BE-5
	SP800-171	3.13.14
L3.009	ISO/IEC 27001:2013	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
	CSF V1.0	PR.IP-6
L3.010	ISO/IEC 27001:2013	A.6.1.4, A.12.6.1, A.16.1.3

	CSF V1.0	DE.CM-8, ID.RA-2
	CSF V1.1	ID.RA-2
	SP800-171	3.14.4
L3.011	ISO/IEC 27001:2013	A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.12.4.2, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3, A.16.1.6
	CSF V1.0	PR.DS-1, PR.DS-5, PR.IP-8
	SP800-171	3.1.21, 3.8.6, 3.8.9, 3.10.4, 3.13.8, 3.13.10, 3.13.16
L3.012	CSF V1.0	PR.PT-1
	SP800-171	3.1.2, 3.3.1, 3.4.7, 3.4.8, 3.4.9
L3.014	ISO/IEC 27001:2013	A.13.1.1, A.13.1.3, A.13.2.1
	CSF V1.0	PR.AC-5, PR.PT-4
	SP800-171	3.13.5
L3.015	ISO/IEC 27001:2013	A.11.1.2, A.11.2.4, A.11.2.5, A.12.4.4, A.13.1.1, A.13.1.3, A.13.2.1, A.15.1.1, A.15.2.1
	CSF V1.0	DE.CM-1, PR.AC-5, PR.MA-1, PR.MA-2, PR.PT-1, PR.PT-4

	SP800-171	3.3.1, 3.3.3, 3.3.4, 3.3.6, 3.3.7
L3.016	ISO/IEC 27001:2013	A.13.1.1, A.13.1.3, A.13.2.1
	CSF V1.0	DE.CM-1, DE.CM-7, PR.AC-5, PR.AC-5, PR.PT-4
	SP800-171	3.13.1, 3.13.6, 3.14.1, 3.14.2
L3.017	ISO/IEC 27001:2013	A.8.2.3, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
	CSF V1.0	PR.AC-5, PR.DS-2, PR.PT-4
	SP800-171	3.1.3, 3.1.13, 3.5.1, 3.5.5, 3.13.4, 3.13.15
L3.018	ISO/IEC 27001:2013	A.16.1.6
	CSF V1.0	PR.IP-8
	SP800-171	3.1.3, 3.1.13, 3.13.4
L3.019	ISO/IEC 27001:2013	A.13.1.1, A.13.1.3, A.13.2.1, A.16.1.6
	CSF V1.0	PR.AC-5, PR.PT-4
	SP800-171	3.5.10, 3.5.11, 3.13.4, 3.14.1
L3.020	ISO/IEC 27001:2013	A.16.1.6
	CSF V1.0	PR.IP-8
	SP800-171	3.13.15, 3.14.1, 3.13.4
L3.021	SP800-171	3.5.10, 3.5.11

L3.022	ISO/IEC 27001:2013	A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
	CSF V1.0	ID.GV-3, PR.DS-1, PR.DS-5
	SP800-171	3.1.9, 3.1.19, 3.1.22, 3.8.2, 3.8.3, 3.8.4, 3.8.5, 3.9.1, 3.9.2, 3.13.11
L3.023	ISO/IEC 27001:2013	A.6.1.2, A.8.1.3, A.9.1.2, A.9.2.3, A.9.2.5, A.9.4.1, A.9.4.4
	CSF V1.0	PR.AC-4
	SP800-171	3.1.4, 3.1.5, 3.1.6, 3.1.15, 3.3.9

付録 C　用語集

(1) Common Criteria

セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための仕組み。国際規格 ISO/IEC 15408 に規定されている。

(2) CSMS(Cyber Security Management System)

産業用オートメーション及び制御システムを対象としたサイバーセキュリティのマネジメントシステム。国際規格 IEC62443-2-1 に要求事項が定められている。

(3) EDSA(Embedded Device Security Assurance)認証

制御機器のセキュリティ保証に関する認証制度。国際規格 IEC62443-4-2 に要求事項が定められている。

(4) IDS(Intrusion Detection System)

サーバやネットワークの外部との通信を監視し、攻撃や侵入の試み等不正なアクセスを検知して管理者にメール等で通報するシステム。

(5) IoT 機器

インターネットに接続して動作する機器。フィジカル空間とサイバー空間とをつなぐ。

(6) IPS(Intrusion Prevention System)

サーバやネットワークの外部との通信を監視し、侵入の試み等不正なアクセスを検知して攻撃を未然に防ぐシステム。

(7) ISMS(Information Security Management System)

組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用するための仕組み。国際規格 ISO/IEC 27001 に要求事項が定められている。

(8) ITSMS(IT Service Management System)

IT サービス提供者が、提供する IT サービスを PDCA サイクルに基づいて管理することで、品質の維持管理及び改善を行っていくための仕組み。国際規格 ISO/IEC 20000 に満たすべき要求事項が定められている。

(9) OECD8 原則

OECD(経済協力開発機構)の理事会で採択された「プライバシー保護と個人データの国際流通についての勧告」に記述されている 8 つの原則。

(10) PDCA

Plan - Do - Check - Act の略。

品質改善や環境マネジメントでよく知られた手法であり、次のステップを繰り返しながら、継続的に業務を改善していく手法の1つのこと。

1.Plan:問題を整理し、目標を立て、その目標を達成するための計画を立てる。

2.Do:目標と計画をもとに、実際の業務を行う。

3.Check:実施した業務が計画とおり行われて、当初の目標を達成しているかを確認し、評価する。

4.Act:評価結果をもとに、業務の改善を行う。

(11) 可用性(availability)

コンピュータシステムに関する指標の1つ。情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態であること。

(12) 監査

組織内においてサイバーセキュリティ対策が適切に実施されているかどうかを判定するために、監査証拠を収集し、それを客観的に評価するための、体系的で、独立し、文書化したプロセスのこと。監査は、内部監査(第一者)又は外部監査(第二者・第三者)のいずれでも、又は複合監査(複数の分野の組合せ)でもあり得る。

(13) 完全性(integrity)

コンピュータシステムに関する指標の1つ。情報が破壊、改ざん又は消去されていない状態であること。

(14) 機能安全

安全機能や安全対策により、リスクを軽減し許容できるレベルの安全を維持すること。

(15) 機密性(confidentiality)

コンピュータシステムに関する指標の1つ。情報が漏れないように、アクセスを認められたユーザーだけがこれにアクセスできる状態であること。

（16） 公開鍵

暗号化と復号に異なる鍵を用いる公開鍵暗号方式で使用される一対の鍵の組のうち、一般に公開される側の鍵。

（17） サイバー空間

コンピュータシステムやネットワークの中に広がる仮想空間。デジタル化されたデータを活用して価値を生み出す。

（18） サイバー攻撃

コンピュータシステムやネットワークに、悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うこと。

（19） サイバーセキュリティ

電子データの漏えい・改ざん等や、期待されていたITシステムや制御システム等の機能が果たされないといった不具合が生じないようにすること。

（20） サイバーフィジカルシステム(CPS：Cyber Physical System)

現実社会に新たな価値を生み出すデータシェアのメカニズムのこと。現実社会をサイバー空間に写し取り、モデル化されたノウハウや経験・知識を活用し、誰でも自由に情報(データ)を組み合わせることで、新たな気付きや発見を得ることができる。

（21） サプライヤー

自社の業務に必要な機器や資材、部品、原材料、サービス等を提供する供給元のこと。

（22） 識別子

様々な対象から特定の 1 つを識別するのに用いられる名前や符号、数字等のこと。

（23） 冗長化

コンピュータやシステムに何らかの障害が発生した場合に備え、予備装置を配置すること。

（24） 脆弱性

システムや IoT 機器等が有する、攻撃者に悪用されてセキュリティインシデントに発展する可能性がある弱点。

（25） 生体認証

指紋や静脈、眼球の虹彩、声紋等の身体的特徴によって本人確認を行う認証方式のこ

と。

（26） セキュリティインシデント

サイバーセキュリティ分野において、セキュリティリスクが発現・現実化した事象のこと。

（27） セキュリティ管理責任者

組織のセキュリティマネジメントシステムの運用及び管理に係る最終責任者。

（28） セキュリティバイデザイン

機器やシステムの企画・設計段階からセキュリティ確保するための方策を組み込むこと。

（29） セキュリティポリシー

自組織や、関係者における役割と責任、情報の共有方法等を明確に定めたもの。

（30） セキュリティリスク

セキュリティリスクとは、セキュリティに関連して不具合が生じ、それによって企業の経営に何らかの影響が及ぶ可能性のこと。

（31） セキュリティルール

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し、対応の範囲や優先順位を定めたもの。

（32） セキュリティ運用マニュアル

検知したセキュリティインシデントに即座に対応できるよう、あらかじめ対応手順を明確に文書化したもの。

（33） セキュリティ対策組織

組織の内部及び外部の情報源から脆弱性情報を継続的に収集・分析し、監視対象とするセキュリティインシデントへの適切な対処方法(優先順位、範囲等)を判断する体制のこと。

（34） 相互認証

認証方式の１つで、双方の当事者が互いに相手の正当性を認証する方式。

（35） 耐タンパーデバイス

内部構造や記憶しているデータ等の解析の困難さを備えるデバイス。

（36） **タイムスタンプ**

電子データに属性として付与される時刻情報。そのデータの作成や最終更新、最終アクセス等の日時を記録するに利用される。

（37） **チェックサム**

誤り検出符号の 1 つで、データ列を整数値の列とみなして和を求め、これをある定数で割った余り(余剰)を検査用データとするもの。

（38） **電子証明書**

認証局(CA)が発行する、デジタル署名解析用の公開鍵が真正であることを証明するデータ。

（39） **二要素認証**

異なる二種類の情報を組み合わせた認証方式のこと。本人が知っている情報、本人が持っている情報、本人の身体的特徴のうち二つを組み合わせる。一要素による認証方式に比べて安全性が高い。

（40） **認証**

正当性を検証する作業。

（41） **ハッシュ値**

元になるデータから一定の計算手順により求められた、規則性のない固定長の値。

（42） **秘密鍵**

暗号化と復号に異なる鍵を用いる公開鍵暗号方式で使用される一対の鍵の組のうち、他者に対して公開しない鍵。

（43） **ファイアウォール**

あるコンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システム等のこと。

（44） **プロトコル**

複数の主体が滞りなく信号やデータ、情報を相互に伝送できるよう、あらかじめ決められた約束事や手順の集合のこと。

（45） マルウェア

セキュリティ上の被害を及ぼすウイルス、スパイウエア、ボット等の悪意を持ったプログラムを指す総称。これらのプログラムは、使用者や管理者の意図に反して(あるいは気づかぬうちに)コンピュータに入り込み悪意ある行為を行う。

（46） メッセージ認証

ネットワークを通じて伝送されたデータに改ざんがないことを確認すること。メッセージ認証のために伝送データに添付される短いデータのことをメッセージ認証コード(MAC：Message Authentication Code)あるいはメッセージ認証符号という。

（47） リスク

国際規格(ISO/IEC 27000)では、「諸目的に対する不確かさの影響」と定義されている。