未定稿　資料６

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）

Society5.0 における新たなサプライチェーン
（バリュークリエイションプロセス）の信頼性の確保に向けて

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

エグゼクティブサマリー

○ 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」の実現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」における産業社会では、データなど様々なつながりが生まれる「Connected Industries」という形で企業間・産業間のネットワーク化が進展して、従来とは異なる、これまで取引を行うことがなかった主体を新たに巻き込んだ、より柔軟で動的なサプライチェーンを構成することが可能となり、サイバー空間とフィジカル空間が相互に作用しあう中で、両空間を跨いで構成される新たな形のサプライチェーンが新たな付加価値を生み出していくことになる。

○ 一方で、ネットワーク化によってサイバー空間とフィジカル空間の両空間を跨いで動的に構成される新たな形のサプライチェーンの拡大は、攻撃側にとっては、ネットワーク化されたサプライチェーン上に攻撃起点が広く拡散していくことになり、防御側が守るべき範囲が急激に拡大することを意味する。

○ また、サイバー空間とフィジカル空間が相互に作用しあうことは、サイバー攻撃がフィジカル空間に及ぼす影響も増大していくことを意味し、サイバー攻撃による被害は甚大なものになっていく可能性がある。

○ このように、サイバー空間とフィジカル空間が融合することで新たな価値を生み出していく「Society5.0」における産業社会では、一方で、サイバー攻撃の起点が拡大するとともに、サイバー攻撃による被害がフィジカル空間に及ぼす影響も増大し、これまでとは異なる新たなリスクを伴うことになる。本フレームワークは、新たな産業社会におけるこうした環境において、付加価値を創造する活動が直面する新たなリスクに対応していくための指針を示すものである。

○ 高度にネットワーク化され、動的に構成されるサプライチェーンに様々な主体が参加する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、それぞれの企

業がセキュリティ・バイ・デザイン等の観点を踏まえて、企画・設計段階から製品やサービスのサイバーセキュリティ対策を実施することに加え、関連企業、取引先等を含めた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マルチステークホルダーによるアプローチや、データ流通における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」における新たな形のサプライチェーンにおいて全産業にほぼ共通して求められるセキュリティ対策をわかりやすく示すために、サイバー空間とフィジカル空間が高度に融合した産業社会を 3 つの切り口(「企業間のつながり」、「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」)から捉え、サプライチェーンの信頼性を確保する観点から、それぞれの切り口において守るべきもの、直面するリスク源、対応の方針等を整理している。

○ 一方、それぞれの産業分野においては、産業構造や商慣行などの観点から、業界や企業により、守るべきもの、許容できるリスク等が異なっている実態があり、セキュリティ対策は、こうした各産業分野の持つ特徴も踏まえたものであることが必要であることから、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。

○ 最後に、ＡＩ技術の更なる進展等によりサイバー空間とフィジカル空間の一体化が進むことで、新たな脅威の出現が考えられる。本フレームワークも新たな脅威に対応するために適切に見直しを図っていく。

はじめに

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って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。

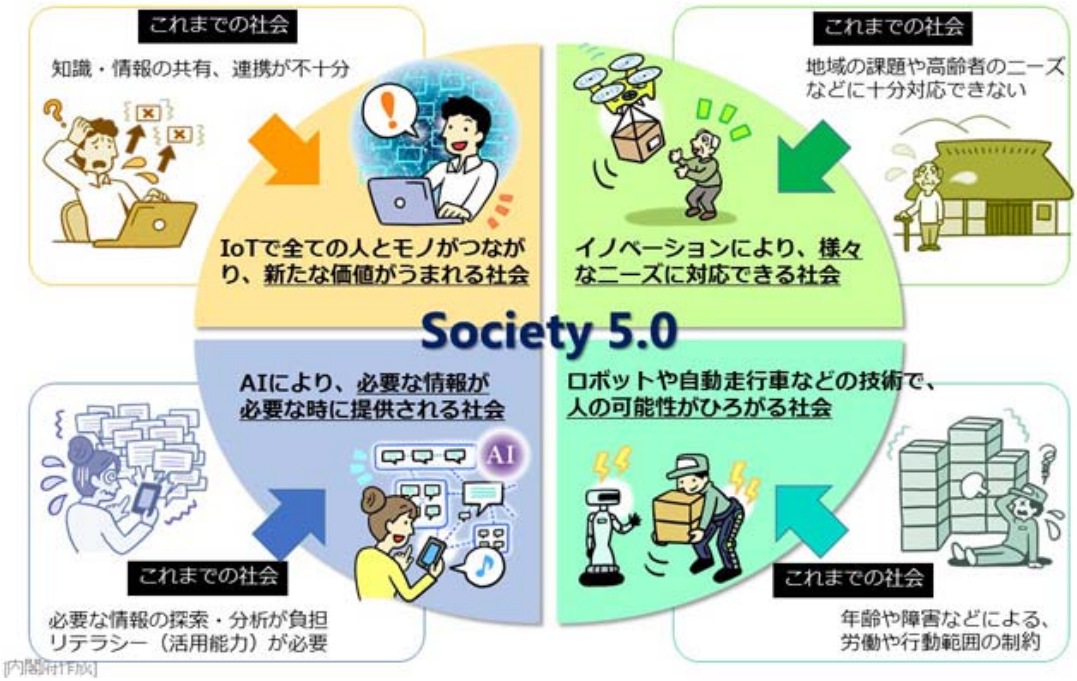


図1 「Society 5.0」で実現する社会のイメージ[1]

[1] 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」

「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。

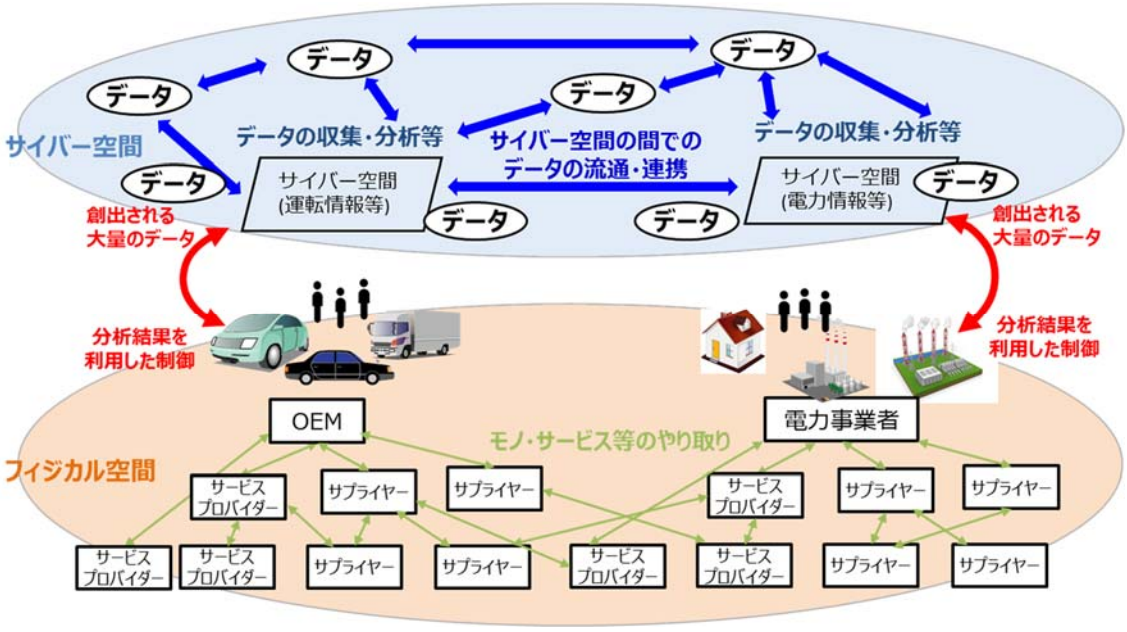


図 2 「Society5.0」社会におけるモノ・データ等のつながりのイメージ

■ サプライチェーンの構造変化

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、サイバー空間とフィジカル空間が高度に融合する中で、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供されることになる。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、需要者が付加価値の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、より有用なデータが得られれば、その要素を取り入れて新たな活動を組み込んでいく。

このように、サプライチェーンはサイバー空間とフィジカル空間の両空間を跨いで、様々なモノやデータが動的につながって構成される付加価値の創造活動へと変化していくことになる。このように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」型のサプライチェーンとして捉え、既存のシステムやプロシージャなどについても、改めて捉え直すことが必要となる。本フレームワークでは、このような「Society5.0」型のサプライチェーンをこれまでの定型的・直線的な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）』と定義することとする。

２．サイバー攻撃の脅威の増大

サイバー空間とフィジカル空間が高度に融合する「Society5.0」における産業社会では、サイバー空間が急激に拡大する中でサイバー攻撃の起点が拡大するとともに、サイバー空間とフィジカル空間が相互に作用しあうことでサイバー攻撃がフィジカル空間に及ぼす影響も増大する。このため、サイバー空間とフィジカル空間の両空間を跨いで複雑につながる新たなサプライチェーンであるバリュークリエイションプロセスに対する脅威は、定型的・直線的なサプライチェーンが直面していたものと比べ、これまでとは異なる複雑なものであり、脅威によって発生した被害が影響する範囲も広くなっていく。

環境が大きく変わることでまず認識しなければならないことは、サイバー攻撃の起点が拡大することである。つまり、価値創造過程（バリュークリエイションプロセス）は、その全過程を通じてサイバー攻撃の脅威に晒される可能性がある。よって、バリュークリエイションプロセスに関わる全要素についてセキュリティの確保のための対応を検討し、部分的ではなく全体的な対応を通じてバリュークリエイションプロセスの信頼性を確保することが必要である。

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など、サイバー空間とフィジカル空間が高度に融合することで発生する新たなプロセスがサイバー攻撃の新たな対象として顕在化してくることを認識する必要があり、データの転換処理の信頼性の確保や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となっていく。

大量のデータの流通・連携	→	・データの性質に応じた適切な管理の重要性が増大
フィジカル空間とサイバー空間の融合	→	・サイバー空間からの攻撃がフィジカル空間まで到達 ・フィジカル空間から侵入してサイバー空間へ攻撃を仕掛けるケースも想定 ・フィジカル空間とサイバー空間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	→	・サイバー攻撃による影響範囲が拡大

なお、サプライチェーンに対する脅威は、既に現実の問題となって発生するようになっている。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。

こうした状況を受け、海外においても、IoT や産業用制御システム（ICS）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[2]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）を 2018 年 4 月に改訂した。この中で、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．フレームワークを策定する目的と適用範囲

「Society5.0」、「Connected Industries」の実現へ向けた歩みの中で、産業構造、社会環境は大きく変化していく。こうした変化に伴う形で、サイバー攻撃の脅威も増大し、これまでとは異なる脅威も発生する。まさに今こそ、そうした脅威の増大、新たな脅威の出現に対する準備を開始することが必要である。

こうした問題意識の下、今般、『サイバー・フィジカル・セキュリティ対策フレームワーク』を策定し、新たな産業社会において付加価値を創造する活動が直面するリスクを適切に捉えるためのモデルを構築し、リスク源を明らかにしつつ、求められるセキュリティ対策の全体像を整理するとともに、産業界が自らのセキュリティ対策に活用できる対策例をまとめることとした。

本フレームワークは新たな産業社会の全体像をとらえており、本フレームワークにおけるリスク源の洗い出しやセキュリティ対策の適用範囲は、新たな産業社会におけるバリュークリエイションプロセス全てである。

リスク源の洗い出しやセキュリティ対策の具体的な内容としては、①従来型サプライチェーンにおいても適用可能なものに加えて、②新たな産業社会に変化したからこそ新たに対応が必要なものを整理しており、それぞれの組織の状況に応じてセキュリティ対策を選定することが可能である。

読者は、本フレームワークを活用し、自らが所属する組織等の実態に合わせて、必要となるセキュリティ対策を実施することが望ましい。

４．フレームワークの想定読者

- CISO（Chief Information Security Officer、最高情報セキュリティ責任者）
- サプライチェーンのマネジメントに関わる戦略・企画部門の担当者（主に第Ⅰ部）
- 企業（組織）のセキュリティ担当者
- 情報関連機器、制御系機器の開発・品質保証、システム設計・構築・検証担当者
- データマネジメントの担当者
- 各産業分野におけるセキュリティ対策のガイドライン等を策定する業界団体等の担当者

[2] National Institute of Standards and Technology（米国国立標技術研究所）

５．フレームワークの全体構成

本フレームワークは、バリュークリエイションプロセスにおけるサイバーセキュリティの観点からリスク源を的確に捉え、それに対応していく指針としての役割を担っていくべく、全体を以下のように構成することとした。

（1） 第Ⅰ部（コンセプト）では、バリュークリエイションプロセスにおけるサイバーセキュリティの観点からリスク源を整理するためのモデル(三層構造アプローチと6つの構成要素)と基本的なリスク認識、それに対するアプローチを、信頼性の確保という形で整理する。

（2） 第Ⅱ部（ポリシー）では、第Ⅰ部で示したモデルを活用して、リスク源を整理するとともに、こうしたリスク源に対応する対策要件を提示する。

（3） 第Ⅲ部（メソッド）では、第Ⅱ部で示した対策要件を対策の種類に応じて整理し、更に、付録の形で、セキュリティの強度を踏まえて分類した対策例を示す。

６．フレームワークに期待される効果と特徴

本フレームワークの策定に当たっては、活用することで期待される効果と特徴を以下のように設定して取組を進めた。

(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

- セキュリティ対策の実行によるバリュークリエイションプロセスの信頼性の確保
- 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

- 産業社会として目指すべきセキュリティ対策の概念の整理（第Ⅰ部）に加え、各事業者が実際にセキュリティ対策を実施する上で方針を確認し、対策を実装できる内容（第Ⅱ部及び第Ⅲ部）にする。

② セキュリティ対策の必要性と適切な水準の対策例を示すことでコストの関係を把握できるようにする

- バリュークリエイションプロセス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、想定されるリスク源と必要な対策の関係を明確にするとともに、できるだけコストがイメージできるような内容にする。
- リスク源からセキュリティ対策を導き出し(リスクベースの考え方を踏まえる)、事業者が適切なセキュリティ対策を選択することでセキュリティレベルを保ったままでコストを圧縮する工夫ができるようにする。

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把握し、ISO/IEC 27001 を始めとする国際標準や NIST Cybersecurity Framework など米欧などの主要な規格との整合性を確保し、こうした規格を踏まえた各国の認証制度との相互承認を進めていくことができる内容にする。
- 本フレームワークでは、国外の規格との関係を整理した対比表も用意している。これにより、日本国内におけるサイバーセキュリティの取組が、そのまま国外においても一定水準を満たしていることを示すことができるとともに、国外における取組が、日本国内においても一定水準を満たしていることを示すことができるようになっている。

7．フレームワークの使い方

本フレームワークは、「Society 5.0」という新たな産業社会において、付加価値の創造活動に取り組む主体が、その活動に必要なセキュリティ対策を講じようとする際に、参照してもらうことを目的としているものである。

一方、それぞれの産業分野においては、産業構造や商慣行などの観点から、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実態があり、セキュリティ対策は、こうした各産業分野の持つ特徴も踏まえたものであることが必要である。

したがって、各業界や各企業において、下記の内容を参考に本フレームワークを活用することを期待している。

(1) リスク源の洗い出し【第Ⅱ部、添付 A、添付 B】

本フレームワークで示す三層構造モデルを参考にして、信頼性の基点を基礎として各組織において取り組んでいる付加価値の創造活動におけるモデルを組み立てることができる。第Ⅱ部ではそのために必要な三層構造モデルの各層において注意すべき特性、機能、具体的な機器のイメージを示すとともに、添付 A において、各業界における代表的なユースケースを示している。

また、同じく第Ⅱ部及び添付 B で整理している想定されるセキュリティインシデントと脅威、6 つの構成要素に落とし込んだ脆弱性を参考にして各組織のリスク源を明らかにすることができる。

これらにより、これまでのリスクアセスメントの観点と比較して、以下の点について新たなリスク源の洗い出しを行うことができることを期待する。

① 各組織を取り巻くマルチステークホルダーの関係性の把握
② サイバー空間とフィジカル空間の融合により発生しうる新たなセキュリティインシデントの把握（安全性の考慮 等）
③ 組織を跨るデータの流通の仕方の把握
④ 各層における信頼性の基点の把握

（2） 各組織におけるセキュリティポリシーの策定及び対策の実装【第Ⅲ部、添付 C】

第Ⅲ部及び添付 C において示されたセキュリティ要件及び対策例を参考にして、自組織におけるセキュリティポリシーの策定及びセキュリティ対策の実装に取り組むことができる。第Ⅲ部には、NIST の Cybersecurity Framework の考え方も踏まえて整理したセキュリティ対策要件を示している。また、添付 C ではそれぞれのセキュリティ要件を満たすためのセキュリティ対策例を示している。

これらにより特に以下の点について、各組織の取組の助けになることを期待している。

① 各組織におけるコストを考慮した対策の実施
② 国際標準等との比較

（3） 各組織、業界等における信頼のチェーンの構築

本フレームワークに基づき、リスクを洗い出し、セキュリティ対策を実施することを通じて、一つ一つの付加価値創造プロセスにおける信頼性を確保することができる。こうした取組をつなげていくことにより、信頼のチェーンを構築することができる。具体的には、以下のような取組に繋がっていくことを期待する。

① 信頼性リストの策定
② 組織、機器等の認証

第Ⅰ部　コンセプト：サイバー空間とフィジカル空間が高度に融合した産業社会における産業分野のサイバーセキュリティの在り方

1．サイバー空間とフィジカル空間が高度に融合した産業社会における「Society5.0」型サプライチェーン“価値創造過程（バリュークリエイションプロセス）”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」型の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ことを目指す。

従来のサプライチェーンでは、セキュリティ対応をしっかりと行った主体間で行われる定型的・直線的な取引であれば、そのプロセス全体のセキュリティが確保される、つまり、参加主体の組織ガバナンス、マネジメントがセキュリティの確保された信頼できるものであれば、サプライチェーンの信頼性も確保されるという考え方に基づいてセキュリティ対策を講じることが基本となっていた。したがって、セキュリティを確保するための基点は、組織のマネジメントの信頼性に基礎が置かれることになる。

しかし、サイバー空間とフィジカル空間が高度に融合した産業社会における新たな形の付加価値の創造活動であるバリュークリエイションプロセスでは、従来のサプライチェーンの場合のように、組織のマネジメントの信頼性にのみ基点を置くことでバリュークリエイションプロセスの信頼性を確保することは困難となる。

例えば、サイバー空間とフィジカル空間が高度に融合した産業社会では、IoT の進展によって、従来はフィジカル分野に留まっていた情報がデジタル化され、データとしてサイバー空間に大量に移転され、バリュークリエイションプロセスにおいて、サイバー空間のこうした様々なデータを柔軟に取り込んでいくことで新たな付加価値が生み出されていく。このプロセスに関係しているのは、従来のサプライチェーンのように、マネジメントの信頼性を確認した主体だけではない。つまり、プロセス全体の信頼性を確保するためには、参加主体のマネジメントの信頼性を確保するアプローチでは限界があるということである。

バリュークリエイションプロセスにおけるセキュリティ対応を進め、信頼性を確保するためには、組織の信頼という信頼点だけではなく、他の観点からの信頼性を確認する

基点を追加設定し、それに対応することで、プロセス全体の信頼性を確保するアプローチが必要となる。

本フレームワークの第Ⅰ部では、バリュークリエイションプロセスの信頼性を確保するために必要な信頼性の基点を明確にするためのモデルを提示し、その上で、リスク源に直面する産業社会の構成要素を明確にすることで、各構成要素が各リスク源に対応する方針を整理するためのコンセプトを明らかにする。

２．価値創造過程（バリュークリエイションプロセス）のセキュリティを確保するための信頼性の基点を設定するためのモデルー三層構造アプローチと６つの構成要素ー

バリュークリエイションプロセスのセキュリティ確保に当たっては、従来のサプライチェーンで想定されているマネジメントの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、新たな付加価値を創造するための一連の新たな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源を的確に洗い出し、対処方針を示すため、バリュークリエイションプロセスが発生する産業社会を、本フレームワークでは以下のように3つの「層」で整理して捉える。

第 1 層ー　企業間のつながり
第 2 層ー　フィジカル空間とサイバー空間のつながり
第 3 層ー　サイバー空間におけるつながり

また、このモデルからリスク源を抽出し、オペレーションレベルでこうしたリスク源への対応を実施していくためには、リスク源となる脆弱性を持つ要素を明確にする必要がある。一方で、バリュークリエイションプロセスは動的に柔軟に構成されるものであるため、ビジネス資産を固定的に把握してリスク源に対応していくのでは、それぞれのバリュークリエイションプロセスで防御しなければならない本質を見逃す恐れがある。そのため、バリュークリエイションプロセスに関与する構成要素を分解してある程度抽象化し、動的に構成が変化することにも対応してリスク源に対応できるようにし構成要素ごとにセキュリティ対策の指針を示すことが必要である。

本フレームワークでは、これらの構成要素を以下の6つに整理する。

－組織
－ヒト
－モノ
－データ
－プロシージャ
－システム

このように、3つの層でバリュークリエイションプロセスにおけるリスク源を洗い出し、6つの構成要素について各リスク源に対するセキュリティ対策の方針と具体的な対策事例を示すのが、本フレームワークの基本構成である。

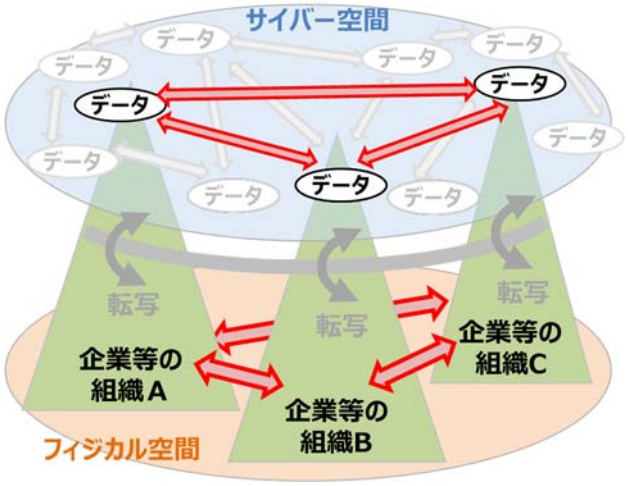
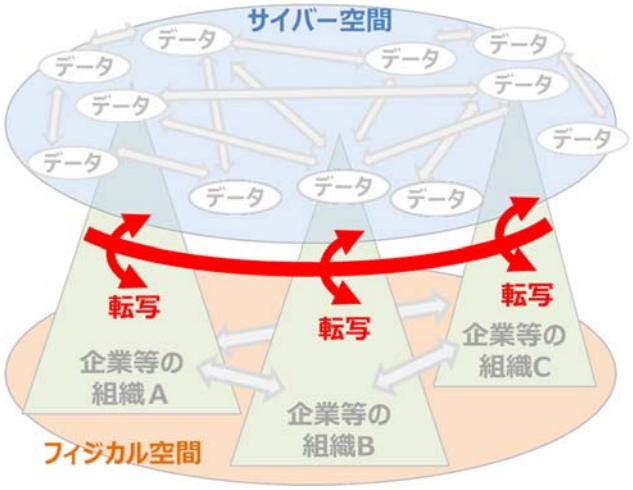
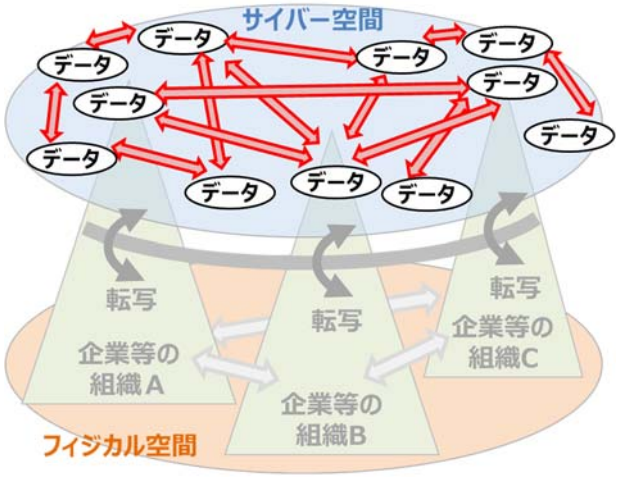
三層構造	概念図
企業間のつながり 【第1層】	
フィジカル空間とサイバー空間のつながり 【第 2 層】	
サイバー空間におけるつながり 【第 3 層】	

図 3 バリュークリエイションプロセスが展開する産業社会の三層構造

２．１．三層構造アプローチの意義

既に述べた通り、サイバー空間とフィジカル空間が高度に融合した産業社会では、企業(組織)のマネジメントの信頼性にのみ基点を置くことでバリュークリエイションプロセスのセキュリティを確保することは困難である。バリュークリエイションプロセスにおけるセキュリティの課題に対応し、信頼性を確保するためには、企業(組織)のマネジメントの信頼性だけではなく、他の観点からの信頼性を確保するための基点を追加設定し、それを確保することで、プロセス全体の信頼性を確保するアプローチが必要であり、ここで示している三層構造アプローチは、信頼性の基点を的確に設定するためのモデルである。

第 1 層－　企業（組織）間のつながり

第 1 層では、企業(組織)のマネジメントの信頼性が確保されることが求められる。

この考え方は、サプライチェーンのセキュリティを実現するためにこれまでも採用されてきた考え方であり、企業（組織）のマネジメントの信頼性を確認し、信頼性が確保された企業（組織）の間で構成されるサプライチェーンはセキュリティが確保されるという考え方が基礎にある。

ISO/IEC 27001 を基礎にした ISMS などの認証制度は、企業のマネジメントの信頼性を確認することが中心となっており、信頼性の確認された企業（組織）間のつながりをサプライチェーンのセキュリティ確保につなげる仕組みも整備されてきている。これまで、ISMS の取得は、企業全体、或いは事業所単位、事業部単位で行われてきているが、ポイントは、セキュリティポリシーが共有され、それが実行されている単位でマネジメントの確認・認証が行われているということである。つまり、第 1 層は、セキュリティポリシーの共有・実行を一体として行う組織のマネジメントに基礎を置いて捉え、サプライチェーンの信頼性の確保を図ることになる。

しかしながら、サイバー空間とフィジカル空間が一体化した産業社会におけるバリュークリエイションプロセスの信頼性を確保するという観点では、企業（組織）のマネジメントの信頼性を確認するだけでは、そのプロセス全体の信頼性を確保することは難しい。そのため、以下の第 2 層、そして第 3 層において、企業（組織）のマネジメントとは異なる信頼性の基点を設定し、その信頼性を確認することが必要になる。

第 2 層－　フィジカル空間とサイバー空間のつながり

サイバー空間とフィジカル空間が高度に融合した産業社会では、フィジカル空間における様々な情報が取り込まれ、デジタル化されてサイバー空間に送り出されるとともに、サイバー空間で加工・編集されたデータをフィジカル空間に展開することで新たな付加価値を生み出すことが様々な局面で実現される。あらゆるものがネットワークにつながることをイメージする IoT は、サイバー空間とフィジカル空間の相互作用が発生す

る境界があらゆる産業活動や社会生活に広がることに一つの本質がある。

一方、様々な局面で発生するサイバー空間とフィジカル空間の相互作用が信頼できるものでなければ、サイバー空間とフィジカル空間の一体性は産業社会に不確かさをもたらすことになってしまう。バリュークリエイションプロセスは、サイバー空間とフィジカル空間の境界線を越えて展開されるが、サイバー空間とフィジカル空間の相互作用、つまり、両空間の境界において行われる情報の変換は高い正確性を求められ、いわば、転写・翻訳というべき正確性が確保されなければ、バリュークリエイションプロセスの信頼性が確保されることはない。

第 2 層は、サイバー空間とフィジカル空間の境界において、要求される情報の正確性に応じて適切な正確さで情報が変換されること、つまり転写機能（正確な翻訳という意味も含む）の正確性が信頼性の基点となる。

実際のサイバー空間とフィジカル空間の境界は、センサ、アクチュエータ、コントローラといった要素[3]から構成される、いわゆる IoT のシステムによって成立することになるが、この境界におけるサイバー空間とフィジカル空間の間を転写する機能は、企業（組織）のマネジメントの信頼性を確認するだけでセキュリティが確保されるものではない。

転写という機能の信頼性を確保するためには、その機能を構成するモノの信頼性や構築・保守の信頼性が確保される必要があり、単体組織のマネジメントだけではなく、ISO/IEC27036 に基づいてライフサイクル全体まで視野に入れて、モノ、そしてシステムそのものの信頼性の確認などがなされて初めてこの層における信頼性が確保されることになる。また、既存のシステムが新たにサイバー空間とフィジカル空間の境界に組み込まれていくことになることを認識し、改めてセキュリティについて評価し、転写という機能の信頼性を確保するための措置を行う必要があることに留意しなければならない。

第 3 層－　サイバー空間におけるつながり

デジタル化の進展によってデータが産業社会において爆発的に増大する中、様々なデータの交換や編集などによってサイバー空間の中で新たな付加価値を生み出す活動も日常的なものとなってきている。

フィジカル空間からサイバー空間に転写されたデータは第 2 層の転写機能の信頼性を確保することによってデータ自体の信頼性が確保されるが、サイバー空間では様々なデータが生成・編集・加工され、自由に流通し、かつ、こうした過程はマネジメントの信頼性が確認された企業（組織）によってのみ扱われるわけではないことに留意しなければならない。データには、様々な主体が関与することになるが、そのデータがサイバ

[3] センサ、アクチュエータ、コントローラ等の装置は、定義上、必ずしもインターネットに接続して運用されるとは限らないものであるが、本フレームワークにおいてこれらの装置に言及する際は、特にインターネットに接続する IoT 機器として運用されるケースを想定して記載することとする。

一空間で付加価値を創出する基礎である。

目的どおりの価値を生み出すためにバリュークリエイションプロセスの信頼性を確保するためには、サイバー空間においては、バリュークリエイションプロセスに関わるデータそのものの信頼性を確保することが必要となる。 したがって、第 3 層においては、信頼性の基点はデータそのものとなり、データ流通・保管時における改竄やデータの流出のようなことの発生は、バリュークリエイションプロセスの信頼性を失わせることになる。したがって、第 3 層では、データの流通・管理や適切な編集・加工を行うためのセキュリティ対策などが求められることになる。

このように、サイバー空間とフィジカル空間が一体化した産業社会における付加価値創造活動おいては、3 つの層からのセキュリティの取組が必要であり、これをバリュークリエイションプロセスにおける「層」として捉えて信頼性の基点とすること（三層構造アプローチ）により、リスク源を明らかにし、対策の方向を示すことが可能となる。

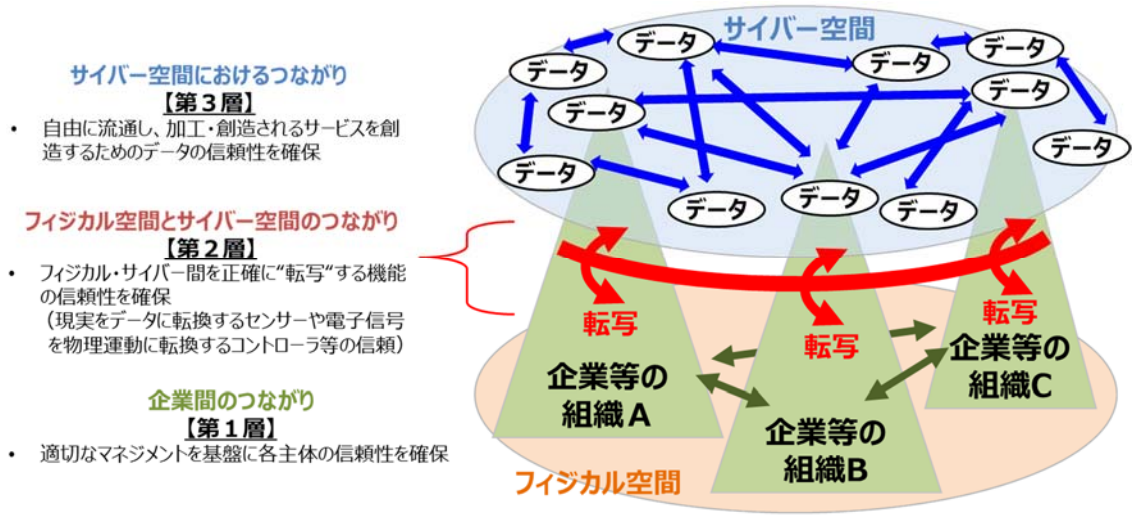


図 4 三層構造アプローチと各層における信頼性

２．２．６つの構成要素

三層構造アプローチを通じて、バリュークリエイションプロセスを構成する要素に影響を与える脅威を明らかにし、リスク源として洗い出していくことが必要である。セキュリティ対策の方針を定め、具体的な対策に取り組むためには、バリュークリエイションプロセスを構成する要素を整理することが必要となる。この際、バリュークリエイションプロセスは、動的に柔軟に構成されることから、資産を固定的に捉えることが難しく、構成要素について一定の抽象化を行って捉える必要がある。

本フレームワークでは、バリュークリエイションプロセスを構成する要素を分解し、セキュリティ対策を講じる上で最適な最小単位として、表1に示す6つの構成要素を整理した。

表１　バリュークリエイションプロセスに関わる６つの構成要素

構成要素	定義
組織	バリュークリエイションプロセスに参加する企業・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 操作する機器を含む
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一連の活動を定めたもの
システム	目的を実現するためにモノで構成される仕組み・インフラ

６つの構成要素は、品質マネジメントの技法である 4M(Man, Machine, Material, Method)を参考に，企業(組織)におけるバリュークリエイションプロセスを入出力や企業(組織)を構成する要素を抽象化して表現した。図6に示すように，企業(組織)は他の企業(組織)からの入力（原料等のモノ，情報等）を用いて，出力（製品・サービス，廃棄物等）を他者に対して提供する。また，企業(組織)は入力と出力の他に，バリュークリエイションプロセスを実施する上で必要な「ヒト」、IT/OT システムなどの「システム」，物理装置などの「モノ」や，従うべき「プロシージャ」(規格・計画など)から構成される。また、企業(組織)の各構成要素は、他の企業(組織)の出力から導かれる。例えば、「システム」は、コンピューターメーカーやシステムインテグレータなどの他の企業のバリュークリエイションプロセスの出力でありえる。また、本フレームワークで示した三層構造を踏まえると、図7のとおり表現できる。

これらの6つの構成要素はそれぞれ排他的な関係にあるのではない。例えば、企業は、「ヒト」、「システム」、「プロシージャ」などの他の構成要素によって形成されることになるが、「組織」はバリュークリエイションプロセスにおいて独自の構成要素としての意味を持ち、「組織」を構成している要素である「ヒト」は「組織」に内包されるだけではなく、バリュークリエイションプロセスに直接関与するものでもある。

PC やサーバは、アプリケーションプログラムや OS を含めて、大規模な「システム」を構成する一部としての「システム」として扱うのが適当な場合もあるが、出力として「モノ」として扱うのが適当な場合もある。また、ソフトウェアは、「システム」にとっては、一連の活動を定めた「プロシージャ」であるが、出力としては、「データ」や「モノ」として扱う方が適切な場合もある。

バリュークリエイションプロセスにおける6つの構成要素のリスク源に対してセキュリティ対策を講じることで、バリュークリエイションプロセスの信頼性が確保され、最終的に生み出されるハードウェアやソフトウェア、サービスの信頼性が確保されることになる。

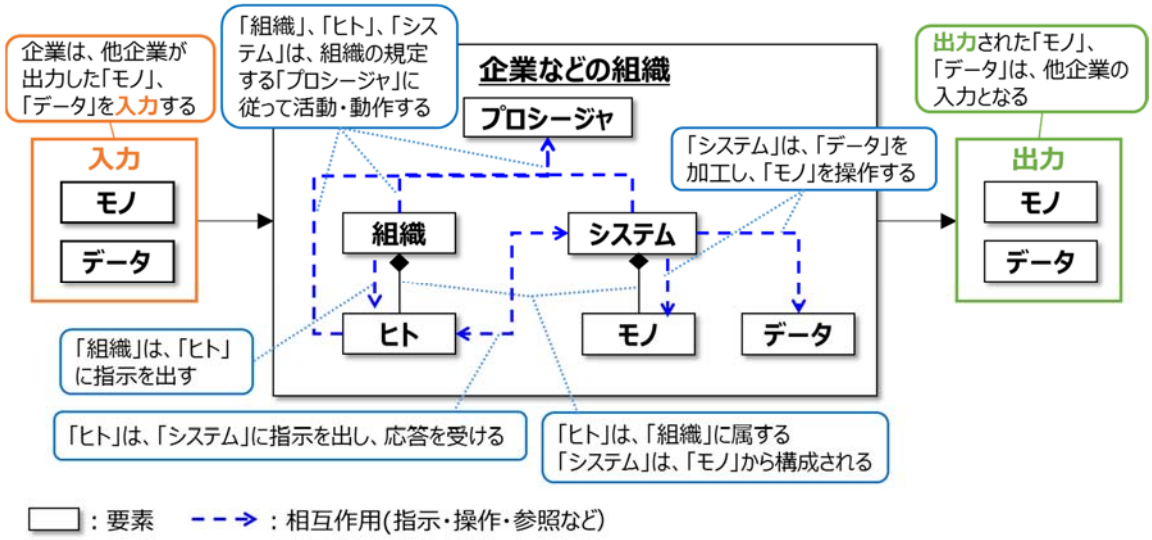


図 5　6 つの構成要素の関係

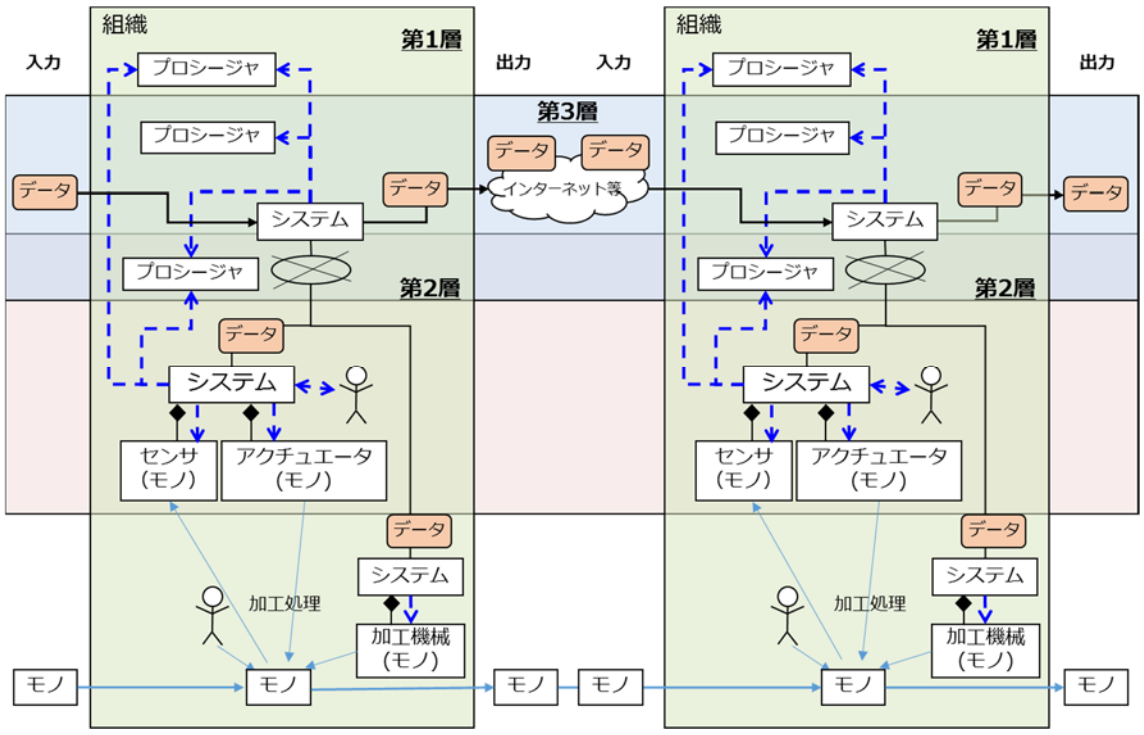


図 6 三層構造における 6 つの構成要素の関係

３．価値創造過程（バリュークリエイションプロセス）におけるリスク源とそれに対応する方針の整理

三層構造アプローチと6つの構成要素によって、第Ⅱ部においてバリュークリエイションプロセスのリスク源と対応方針（ポリシー）を整理していく。特に第Ⅰ部では、サイバー空間とフィジカル空間が高度に融合した産業社会へと変化していることによって、バリュークリエイションプロセスが従来のサプライチェーンとは異なるリスク源に直面することになることを整理しておきたい。

三層構造アプローチにおける第 1 層は企業（組織）のマネジメントに信頼性の基点が設定され、セキュリティ対策は各企業（組織）のマネジメントを中心に実施される。しかし、既に述べたように、サイバー空間とフィジカル空間を跨いで展開するバリュークリエイションプロセスのセキュリティ対策では、第 2 層と第 3 層におけるセキュリティ対策を講じることが必要になる。

第２層では、サイバー空間とフィジカル空間の境界における正確な転写機能を確保することがセキュリティ対策の要点となるが、このような転写機能の信頼性を確保するためには、バリュークリエイションプロセスに直接関与している企業（ここでは仮にA社とする）に加え、直接関与していないもののA社の転写機能を担うシステムの構成品の供給や構築に関わる企業の協力が不可欠となる。

つまり、あるバリュークリエイションプロセスに直接関与していない企業も、適切なセキュリティ対策を実施するためには不可欠な存在としてセキュリティ対策に参加することが求められることになり、マルチステークホルダーアプローチによる取組が必要となる。

例えば、あるバリュークリエイションプロセスに間接的に関与する企業が、直接的に関与する企業に対してセキュリティが確保された製品やサービスを提供することで、最終的に第 2 層の信頼性の基点である転写機能の信頼性が確保されることになる。

また、第 3 層では、バリュークリエイションプロセスに参加する企業は、サイバー空間における様々なデータを活用することになるが、そのデータが適切に扱われ、信頼性が確保されていることがバリュークリエイションプロセスのセキュリティ確保の前提となる。

ここでも、バリュークリエイションプロセスに直接関与していないものの、データの流通や取扱いにおいて間接的に関与する主体がセキュリティの確保のために一定の役割を果たすことが求められていくこととなり、マルチステークホルダーアプローチによるセキュリティ対策の取組が必要になる。

そのため、例えば、ある特定の区分に分類されるデータについては、当該データを扱う者の間で同じセキュリティ対策を講じることが必要となるなど、第 1 層、第 2 層とは異なる観点からのセキュリティ対策を実施することが、データの信頼性に基点を設定する第 3 層における具体的なセキュリティ対策となる。

このように、リスク源はそれぞれの層で捉え方が異なり、対応方針もまた各層で異なることになる。

こうした理解を踏まえて、本フレームワーク全体で、各層で守るべきものとリスク源を整理し、どのような方針に基づいてどのような対策を講じるかを整理する。

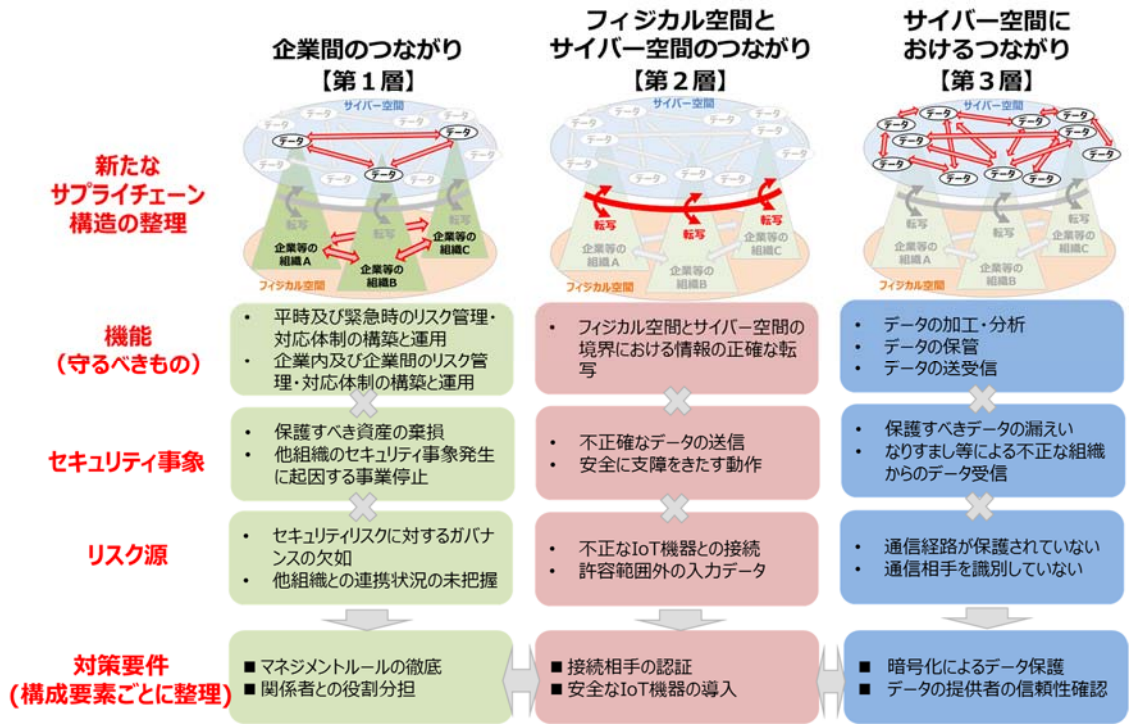


図７ 各層におけるセキュリティ対策の概要

４．フレームワークにおける信頼性の確保の考え方

バリュークリエイションプロセスのセキュリティ確保のためには、三層構造アプローチに従い、各層において信頼性の基点のセキュリティを確保することになる。そのためには、各構成要素について必要なセキュリティ要件が満たされていることを確認し(信頼の創出)、確認した主体以外の者による照会ができるようにし(信頼の証明)、それを繰り返し行い、広く共有して信頼のチェーンを構築、維持することで、バリュークリエイションプロセス全体のセキュリティを実現することになる(図8参照)。

(1) 信頼の創出

Ex.

- セキュリティ要件を満たすモノ・データ等の生成
- 上記生成物の記録の保存
- 対象のモノ・データ等がセキュリティ要件を満たした形で生成されたことの自己確認

・ 対象のモノ・データ等がセキュリティ要件を満たした形で生成されたことの第三者による認証

(2) 信頼の証明

Ex.

・ 対象のモノ・データ等がセキュリティ要件を満たした形で生成されたものであることを生成主体以外の者も照会できるリスト(信頼性リスト)の作成と管理(統合管理型台帳か、分散台帳(ブロックチェーンの活用等)かを問わず)

・ 信頼性リストを照会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

Ex.

・ 信頼の創出と証明を繰り返すことによる信頼のチェーンの構築(信頼性リスト間でお互いの信頼性が確認され、それによってトレーサビリティを確保すること等)

・ 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

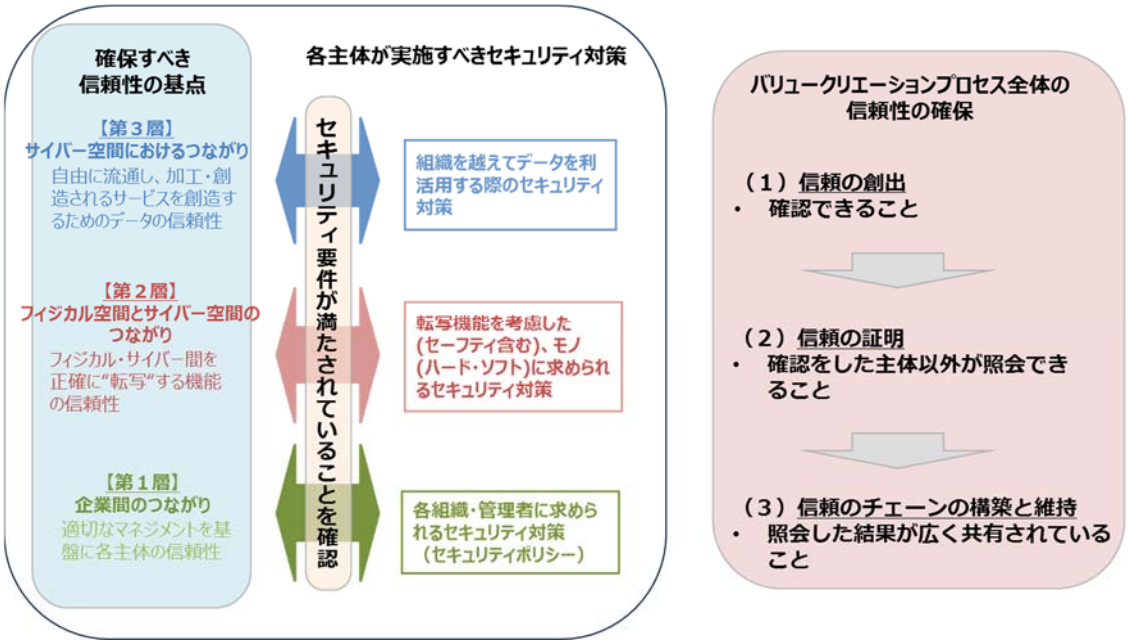


図 8 信頼性の基点と信頼性の確保の考え方

バリュークリエイションプロセスは、動的・柔軟に構成されるため、個々の信頼性を確認することで対応するだけではなく、信頼のチェーンを構築することで、バリュークリエイションプロセス全体で信頼性を確保するような、多層的な形でセキュリティを確保するアプローチが求められることになる。

一方、こうした体制を構築するためには、技術的・制度的に整備しなければならない課題は依然として多く、引き続き、官民が連携して必要な取組を進めていくことが必要である。技術・制度等の整備に伴い、本フレームワークの第Ⅱ部以降については、必要な見直しを適宜行っていく。

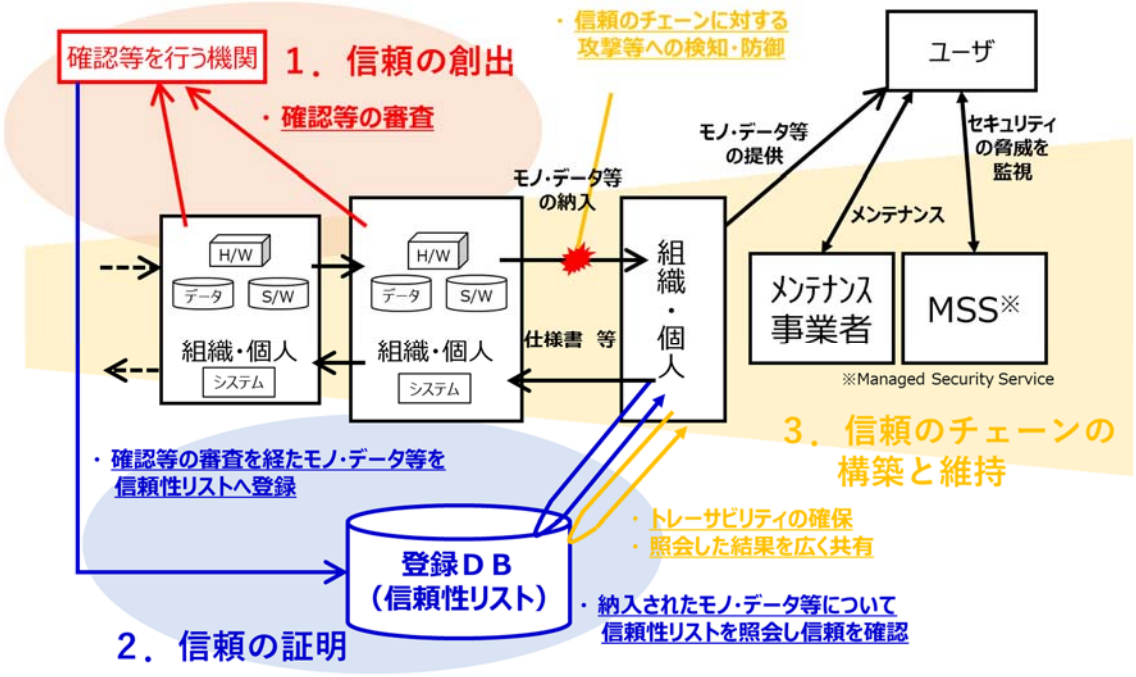


図 9 信頼の創出、信頼の証明、信頼のチェーンの構築と維持の関係のイメージ

５．結び

本フレームワークは、サイバー空間とフィジカル空間が高度に融合した新たな産業社会となる「Society5.0」におけるバリュークリエイションプロセスの全産業に共通的なセキュリティ対策を示している。一方、それぞれの産業分野においては、産業構造や商慣行などの観点から、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実態があり、セキュリティ対策は、こうした各産業分野の持つ特徴も踏まえたものであることが必要である。

したがって、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。

第Ⅱ部　ポリシー：リスク源の洗い出しと対策要件の特定

第Ⅱ部では、本フレームワークが示す「Society5.0」においてより重要となる信頼性の基点を整理するための三層構造アプローチに基づいて、新たな産業社会におけるバリュークリエイションプロセスのリスク源を整理し、対策要件を提示する。

１．三層構造アプローチと６つの構成要素を活用したリスクマネジメントの進め方

バリュークリエイションプロセスに関与する主体は、JIS Q 31000:2010 や JIS Q 27001:2014 等のリスクマネジメントにおける標準的なプロセスを活用して、本フレームワークを活用することができる。第Ⅱ部で提示する内容は、リスクマネジメントプロセスの中でも、特に、組織の状況の確定、リスクアセスメント、リスク対応において活用することが可能である。

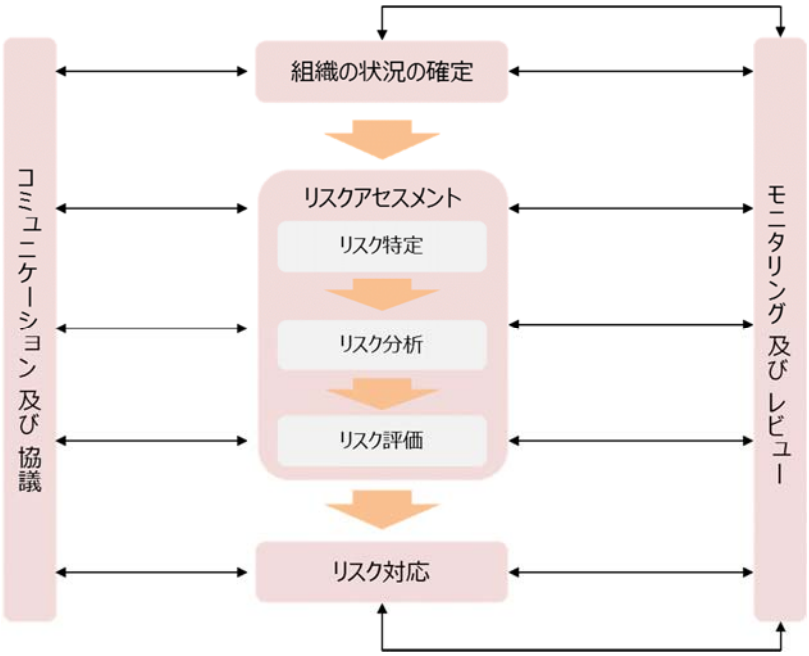


図 10 リスクマネジメントの一般的なプロセス[4]

セキュリティリスクマネジメントにおける具体的な組織の状況の確定、リスクアセスメント及びリスク対応は以下のステップで実施していく。

① 分析対象の明確化（1．1）

[4] JIS Q 31000:2010 リスクマネジメント−原則及び指針 を基に作成

三層構造アプローチに基づき、分析対象となるバリュークリエイションプロセスを明確化し、各層における構成要素を把握する。

② 想定されるセキュリティインシデント及び事業被害レベルの設定（1．2）

自組織の事業に対して、各層の機能が脅かされることになると想定されるセキュリティインシデント及び、そのセキュリティインシデントの結果、事業に影響がどの程度及ぶかについて、事業被害レベルとして設定する。

③ リスク分析の実施（1．3）

②で定義したセキュリティインシデントについて、想定される攻撃シナリオを検討し、リスクを脅威と脆弱性の観点から分析する。

④ リスク対応の実施（1．4）

リスク分析の結果を受けて、リスク対応を実施する。

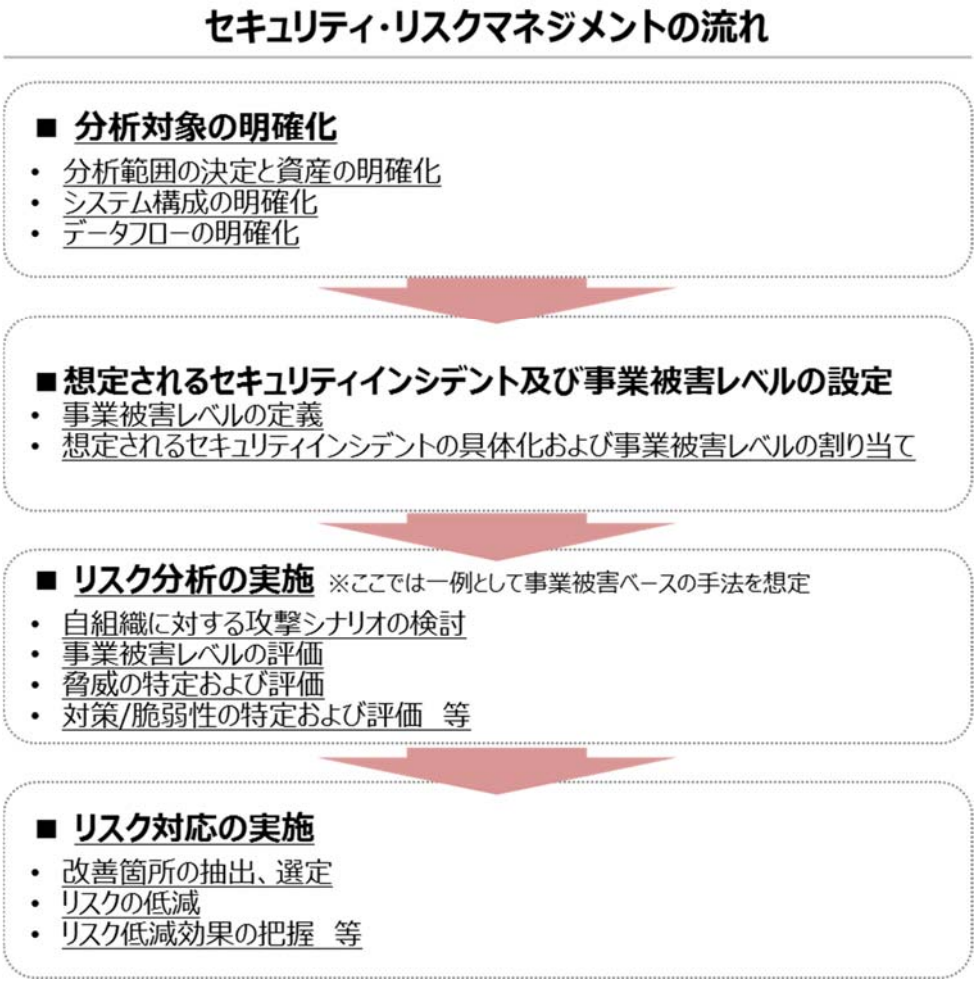


図 11 リスクマネジメントの流れ[5]

[5] IPA「制御システムのセキュリティリスク分析ガイド 第 2 版」を参考にしつつ、本フレームワークのコンセプトを活かすように修正

特に、本フレームワークが対象とする「Society5.0」におけるセキュリティリスクを適切に評価し、効果的な対応を実施するためには以下の 4 点を、分析対象の明確化からリスク対応の実施に至るまでの流れの中で考慮するべきである。

① バリュークリエイションプロセスに関わるステークホルダーとの関係
② IoT 機器を介したサイバー空間とフィジカル空間の融合
③ 組織を跨るデータの流通
④ 各層における信頼性の基点の確保

以降、①～④という観点の捉え方も含め、リスクアセスメントの実施について、順に説明する。

１．１．分析対象の明確化（三層構造モデルへの落とし込み）

リスクアセスメントにおける分析対象の明確化について、(1) 実施プロセス、(2) 実施上の留意点の順に以下で記述する。

(1) 三層構造アプローチに基づいた分析対象の明確化プロセス

リスクアセスメントを実施するに当たり、まずは分析対象を明確化する必要がある。IPA『制御システムのセキュリティリスク分析ガイド 第 2 版』では、分析対象の明確化として、以下の三つを実施するよう記載されている。

- 分析範囲の決定と資産の明確化
- システム構成の明確化
- データフローの明確化

分析範囲及び資産の明確化は、組織の枠を超えてサイバー空間とフィジカル空間が高度に融合した産業社会においては、より困難となることが予想される。上記の達成のためには、自組織の関わるバリュークリエイションプロセスにおけるステークホルダーを整理し、サイバー空間、フィジカル空間の双方におけるモノやデータの動きの把握が重要になる。本フレームワークでは、第Ⅰ部第2節にて提示した三層構造アプローチに基づいて分析対象を明確にする方法を提供する。組織は、本節における方法を活用して分析範囲を決定し資産を明確化した後で、従前に定めた範囲内におけるシステムの構成やデータフローを明確化することで、リスクアセスメントを実施する対象に

対する理解を詳細化することができる[6]。

リスクアセスメントのための分析対象の明確化を行うにあたっては、まず、表2に示すような各層の特性及び機能・役割を理解する必要がある。これらの機能・役割に照らして、分析対象のシステムが果たす機能に着目し、三層構造に基づいて分析範囲及び資産の整理を行う。

管理対象となるモノはすべて第1層に含まれるものの、その中でも、第2層、第3層の機能を備えるモノについては、第２層及び／または第3層に関わるモノとして整理を行う。その際、分析対象のシステムによっては、第2層の機能と第3層の機能を併せ持つモノもあることに留意する。その際、機能を踏まえてモノやシステムが設置され、ヒトに対して特定のプロシージャを求めることになる”場所”という捉え方もリスクアセスメントにおいて注意することが適当である。

表２　三層構造アプローチにおける各層の特性、機能・役割、分析対象及び具体的イメージ

特性	機能・役割	分析対象	対象の具体的イメージ
第１層 － 企業間のつながり			
個々の組織の適切なガバナンス・マネジメントによって信頼を維持 個々の組織が適切な業務連携によって信頼を維持する	・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 ・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 ・フィジカル空間での製品・サービスが、望まれる品質を備えて入荷又は出荷されること **【セキュリティ要件】** **組織単位のセキュリティポリシーを定めて維持すること** **【信頼性の基点】** **組織・マネジメント**	・組織等で管理されるヒト・モノ・データ・プロシージャ・システム ・上記の要素が管理される場所 ・組織内でのデータの流通	・社員、従業員 ・企業のIT資産 ・企業のセキュリティポリシー ・企業間の契約
第2層 － フィジカル空間とサイバー空間のつながり			
IoT 機器を介して、フィジカル空間とサイバー空間のつながりが拡大 ネットワークにつながるライフサイクルの長い機器が増加する （遠隔地などにあり）管理が行き届きにくいネットワークにつながる機	・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、第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、	・転写する機能に関わる組織・ヒト ・ルールに沿って正しくサイバー空間とフィジカル空間を転写する機能を	・アクチュエータ、センサ、コントローラ、医療機器、ECU、3D プリンタ、監視カメラ、パソコン（入力機器と

6 システム構成の明確化、データフローの明確化を実施するに当たり、「制御システムのセキュリティリスク分析ガイド 第２版」(IPA, 2018 年)の３．２および３．３を参照することが望ましい。

	器が増加する ネットワークにつながる機器が様々な場所（重要インフラから家庭まで）に分離する サイバー空間からのインプットに基づいて、フィジカル空間において作業を実行する機器が増加する	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 **【セキュリティ要件】** **サイバー空間とフィジカル空間との間の転写におけるセキュリティを確保すること** **【信頼性の基点】** **ルールに沿って正しくサイバー空間とフィジカル空間とを転写する機能・トラスト**	備えるモノ・システム ・ 転写に関するデータ ・ 転写するプロシージャ	して）、スマートメータ（検針機器として） ・ これらの機器等を構成する転写する機能に関わる部品　等
第3層 － サイバー空間におけるつながり				
	サイバー空間にて自組織のデータだけでなく、組織を超えて多様かつ大量なデータを収集・蓄積・加工・分析 組織や業界をまたいで様々なエンドポイントからデータが収集される ストリーミングデータや機密データ等を含む、様々なデータが収集される 複数のデータソースから取得したデータが統合的な分析のために加工される 公開データ及び機密データ等を含む自社の蓄積データが、組織や業界をまたいで様々なエンドポイントからアクセスされる可能性がある データの加工・分析において、AI等を活用して高度かつ高速なデータ処理がなされる サイバー空間におけるデータのサプライチェーンの構成は、動的に変化する。	・ データを送受信する機能 ・ データを加工・分析する機能 ・ データを保管する機能 **【セキュリティ要件】** **サイバー空間におけるデータの送受信等におけるセキュリティを確保すること** **【信頼性の基点】データ**	・ 組織を越えてやりとりするデータを扱う組織・ヒト ・ データを送受信、加工、分析、保管するモノ・システム ・ 組織を越えて流通するデータ ・ 組織を越えてデータを扱う際の共通のルール・プロシージャ	・ サーバ、ルータ、スマートメータ（検針データの送信機器として） ・ これらのシステム等を構成するハードウェア及びソフトウェア（OS、ミドルウェア、アプリケーション　等） ・ オープンデータ ・ 限定提供データ ・ データ管理ポリシー　等

例えば、パソコンやスマートメータは、第2層と第3層の機能を併せ持つモノと考えられるが、分析対象のシステムにおける機器の役割などを考慮した上で第2層であるのか、第3層であるのか、いずれの層にも含まれるモノであるのかを検討する。

三層構造アプローチに基づいて明確化された、分析範囲及び資産は文書化し、構成に変更があった場合にすぐに対応できるようにすることが望ましい。

以上の整理を抽象化したモデルとして、図 12 に第1層の分析範囲及び資産の関係を示す。第1層では、バリュークリエイションプロセスとは関係なく、セキュリティポリシーの共有・実行を一体として行う組織のマネジメントに基礎を置いて整理した。

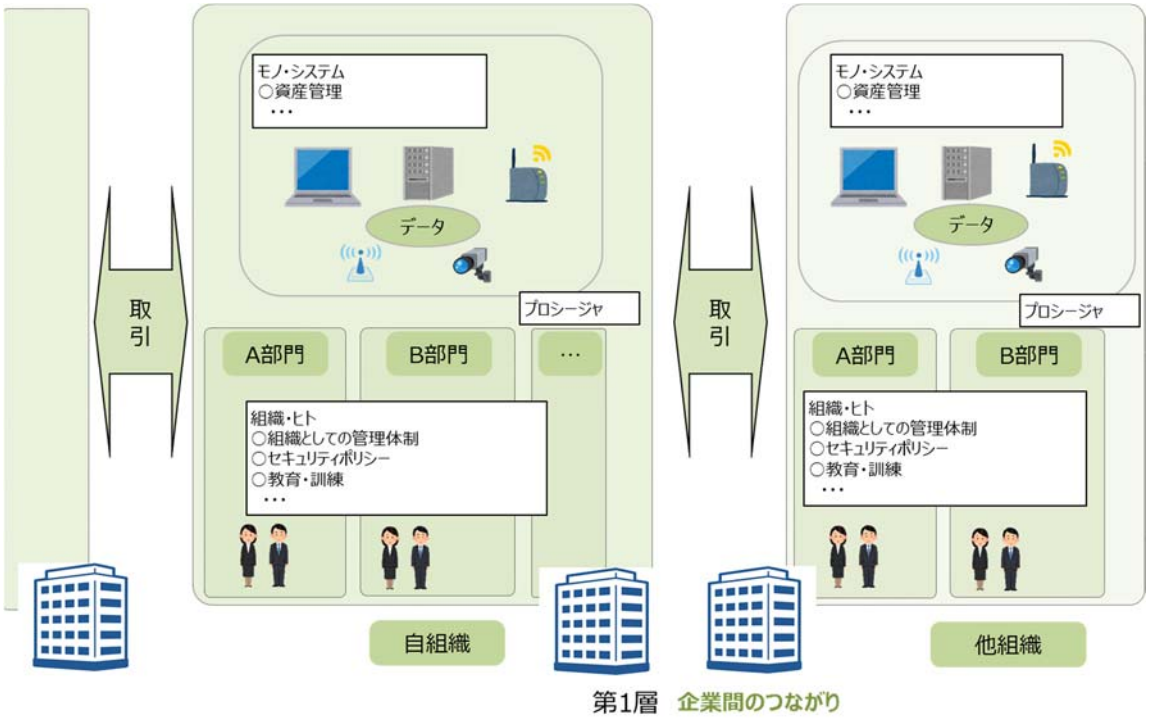


図 12　第 1 層の分析範囲及び資産に関する抽象モデル

次に、図 13 として第2層及び第3層の機能を示した上で、図 14 として第 1 層の構成要素について第 2 層、第 3 層の機能との関連付けを行ったバリュークリエイションプロセスのイメージを示す。

組織の資産は第 1 層に位置づけられるが、バリュークリエイションプロセスが発達してきたときには、組織のセキュリティポリシーだけを考慮すればよいのではなく、図 13 にあるように第 2 層の転写の機能、第 3 層のデータ流通等の機能に着目して、そのセキュリティを確保できなければ、信頼性は確保できない。

第 1 層で整理した構成要素について、この第 2 層、第 3 層の機能との関連付けを行うと、一つの組織の中で第 2 層に関わる構成要素、第 3 層に関わる構成要素を明確化することができる。この整理を行うことで、それぞれの構成要素について、第 1 層、第 2 層、第 3 層それぞれの信頼性の基点をどのように置くべきか、セキュリティ対策は何を行えばいいか明確化することができる。

参考として、付録 A に図 14 のモデルを代表的な産業分野に適用した場合のユース

ケース例を用意したので、各実施主体において実際に分析対象の明確化を行う際に必要に応じて参照されたい。

なお、より詳細なシステム構成及びデータフローの明確化については、各業界、各組織でその分析対象が様々に異なると想定されるため、各実施主体が明確化することが望ましい。

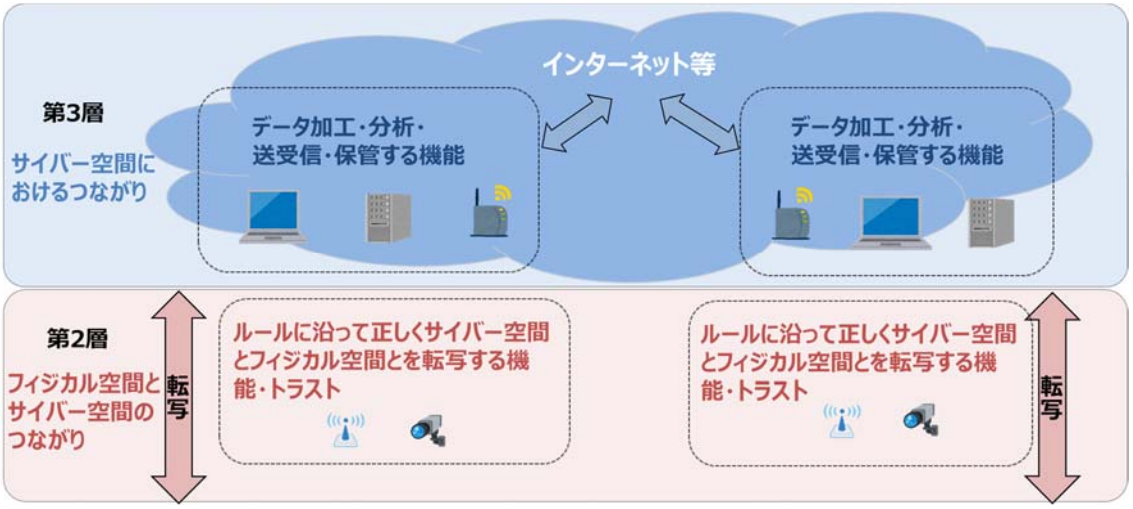


図 13　第２層及び第３層の分析範囲及び資産に関する抽象モデル

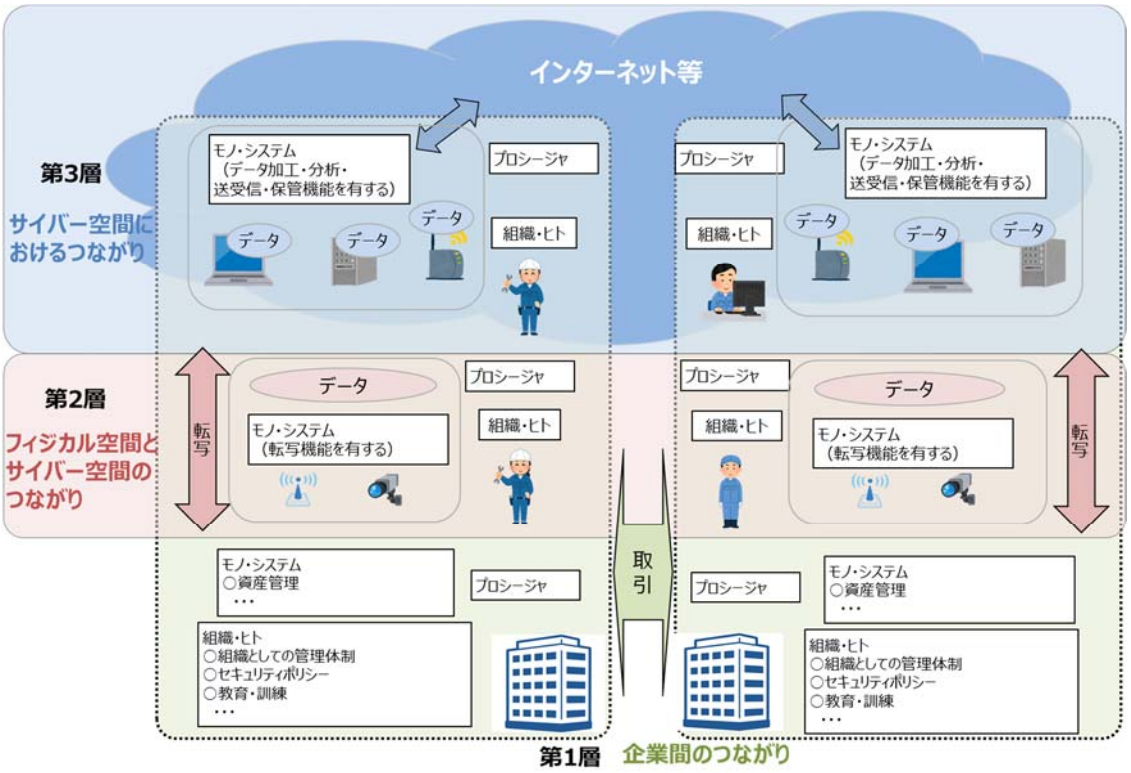


図 14 分析範囲及び資産に関する抽象モデル

(2) 分析対象の明確化における留意点

三層構造アプローチに基づいて分析対象を明確化する際、リスクマネジメント実施主体は、バリュークリエイションプロセス全体のセキュリティを確保する観点から、以下のポイントに留意しながら作業を進めることが望ましい。

① バリュークリエイションプロセスに関わるステークホルダーとの関係

- 第 I 部で説明しているように、第 2 層や第 3 層では、バリュークリエイションプロセスに直接関与していない企業も、適切なセキュリティ対策を実施するためには不可欠な存在としてセキュリティ対策への参加が求められることになり、マルチステークホルダーアプローチによる取組が必要となる。
- このため、三層構造モデルを用いて、バリュークリエイションプロセスに関わるステークホルダーを洗い出し、その役割、自組織の事業における重要度を明確にする必要がある。
  - ➢ 三層構造のそれぞれにおいて、自組織のアクションに関連する「組織」を洗い出す。その際、自組織の提供する製品・サービスの部品等を提供するサプライヤーだけでなく、IoT 機器ベンダーや第 3 層でデータを保管、加工・分析するサービスプロバイダ等も含めて洗い出す必要がある。ま

た、重要な取引先については、業務の再委託先等も含めて把握しておくことが望ましい。

② IoT 機器を介したサイバー空間とフィジカル空間の融合

- サイバー空間とフィジカル空間が融合する境界では、物理空間の情報を一定のルールに従って正しくサイバー空間の情報に転写できる必要がある。その際、例えば、センサの機能が攻撃され、正しく転写できずに誤ったデータがサイバー空間へ提供されると、収集された解析対象となるデータ及び、そのようなデータを利活用して実施されるオペレーションに対する信頼が失われることになる。
- このため、物理空間の動態を計測し、サイバー空間へデータとして伝送する機能を果たす機器を適切に識別し、自組織のオペレーションにおける重要度等に応じて分類しておくことが望ましい。
- サイバー空間とフィジカル空間が融合する境界では、上述の例とは逆に、サイバー空間におけるデータの解析結果に基づき、モノを制御することが起きる。その結果として、図 15 が示すように、セキュリティ上の脅威が、機器の誤動作により従業員への物理的な危害、機器の損壊等の安全上の問題につながる可能性が生じる。
- そのため、リスク分析対象の明確化にあたっては、安全に関するリスク分析の結果を用いて、上記のような安全上の問題に繋がりうる事象を引き起こす可能性のある箇所、該当する機器を明確化し、リスク分析等を実施する際に参照できるようにすることが望ましい。

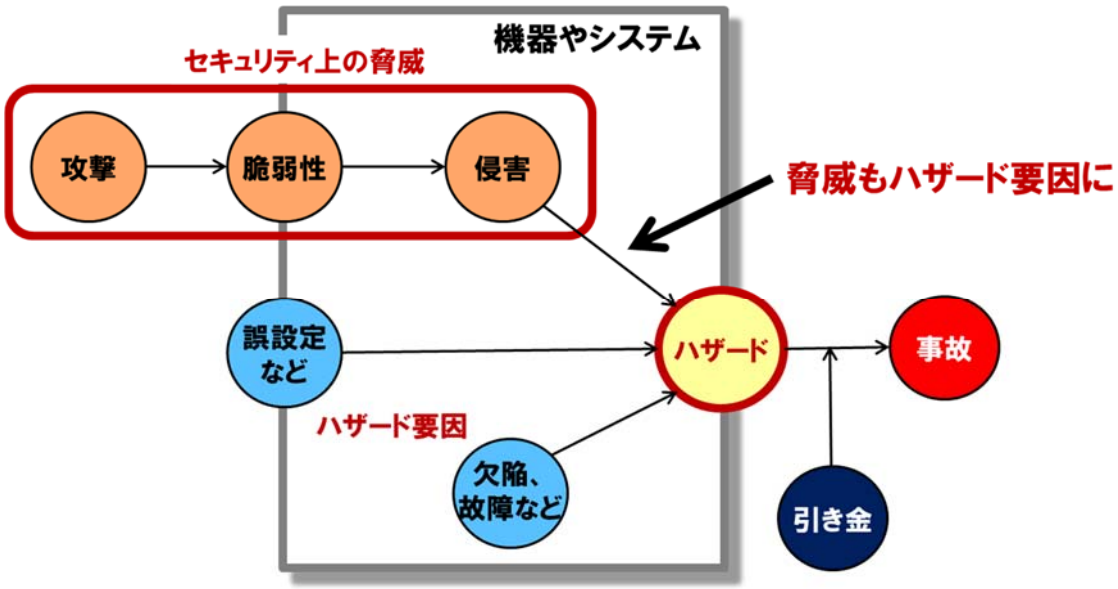


図 15 セキュリティ上の問題がセーフティに影響を与えるモデル[7]

③ 組織を跨るデータの流通

- 組織を跨いだデータ等のやり取りが活発化すると、事前に想定されていない構成要素(組織、ヒト、モノ等)から適切でないデータが自組織に提供される可能性が高くなると想定される。
- また、組織を超えて、限られた範囲内で第三者にデータを提供する若しくは提供を受ける機会が増加することも想定される。
- そのため、自組織で利活用すると想定されるデータを、データの取得元である構成要素(組織、あるいは組織に属さないヒト、モノ等)がわかるように可能な限り一覧化し、自組織のアクションにおける重要度等の基準に基づいて分類することが望ましい。

④ 各層における信頼性の基点の確保

- 第 I 部の「三層構造アプローチの意義」でも述べたように、「Society5.0」では、従来から考慮されてきた組織のマネジメントの信頼性という観点に加え、第 2 層における IoT 機器を介した転写機能の正確性、第 3 層におけるバリュークリエイションプロセスに関わるデータそのものの信頼性という複数の観点を踏まえた対策を講ずることが、目的どおりの価値を生み出すために重要になる。
- このため、分析対象の明確化に当たっては、信頼性の基点の確保を考慮して、信頼性の基点となる要素について明確化しておくことが望ましい。上記の実施においては、本節の①～③で記載した施策が有効である。

１．２．想定されるセキュリティインシデント及び事業被害レベルの設定

明確化された分析対象の事業活動に対し、重大な影響を及ぼしうるセキュリティインシデントを整理し、それによる事業への影響を整理する。まず、考慮すべきセキュリティインシデントを設定するに当たり、組織は、各層の機能を脅かす上位レベルでの事象を検討し、そのような事象につながるようなセキュリティインシデントを抽出することが望ましい。

表2で提示した各層の機能に対応して、それを脅かす上位レベルでの事象(機能に対して想定される悪影響)を表 3 に記載している。組織は、表 3 の「機能(守るべきもの)に対する悪影響」のそれぞれを考慮し、セキュリティインシデントを抽出することが望ましい。

---

[7] IoT 推進コンソーシアム，総務省，経済産業省『IoT セキュリティガイドライン ver.1.0』より引用

表３ 各層の機能に対する悪影響のイメージ

階層	各層の機能(守るべきもの)	機能(守るべきもの)に対する悪影響のイメージ
第１層	• 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 • 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 • フィジカル空間での製品・サービスが、望まれる品質を備えて入荷又は出荷されること	• **法制度等への不準拠** • **セキュリティインシデントの発生**：情報資産の棄損(漏洩/改ざん/破壊/利用停止) • **セキュリティインシデントによる影響の拡大**：被害拡大による事業影響(稼動停止、誤ったアウトプット等)
第２層	• 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、第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	• **機器の機能停止**：IoT 機器の稼動が停止すること • **信頼性の低い稼動**：IoT 機器が意図した稼動をしないこと ✓ 安全面に問題のある稼動 ✓ 誤計測
第３層	• 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	• **データ保護に係る法制度等への不準拠** • **セキュアでない稼動**：データ処理側でのセキュリティインシデントによる情報資産の棄損(漏洩/改ざん/破壊/利用停止) • **信頼性の低い稼動** ：データ関連サービスが意図した稼動をしないこと(誤動作、停止等)

また、セキュリティインシデントの洗い出しに際して1．で記載した①～④のそれぞれの観点を十分に考慮する必要がある。①～④への対応が不十分なものとなる場合、下記に例として示すような事象が発生し、自組織及び関係する他組織の事業運営に重大な影響が及ぶ可能性が高まる。

表４ リスク源の洗い出しにおいて考慮すべき観点を看過した場合のリスク

考慮すべき観点	観点を考慮しないことで発生し得るセキュリティインシデント	【添付 B】において関連するセキュリティインシデント[8]

[8] 例えば、セキュリティインシデント L1_3_b は、後述する、第１層において想定されるセキュリティインシデント(3)(b)の記載内容を指している。

バリュークリエイションプロセスに関わるステークホルダーとの関係	バリュークリエイションプロセスのあるポイントにおけるセキュリティインシデント発生時に、事業継続が適切になされない	L1_3_b, L1_3_c
IoT 機器を介したサイバー空間とフィジカル空間の融合	サイバー空間とフィジカル空間との接点(IoT 機器)において、安全性に影響を及ぼす事象が発生する	L2_1_a, L2_1_b, L2_1_c, L2_2_a
	IoT 機器を起点としたサイバー空間への攻撃が発生する	L2_3_b, L2_3_c
組織を跨るデータの流通	自組織の保護すべきデータが、情報処理業務等の外部委託先にて適切に管理されない	L3_1_a, L3_1_b, L3_1_c, L3_2_a, L3_2_b, L3_4_b

本フレームワークでは、各層の機能および、機能に対する悪影響、①～④の観点を踏まえ、三層構造の各層で発生を回避すべき一般的なセキュリティインシデントのリストを表5に示す。

各組織においては、考慮すべきインシデントに漏れが発生しないよう、添付 B を参照して想定インシデントを洗い出し、各組織の事情を加味して検討を具体化することが望ましい。

表５　想定されるセキュリティインシデント

第 1 層において想定されるセキュリティインシデント	
(1) 平時のリスクマネジメントプロセスに支障があり、セキュリティインシデント(情報資産の漏洩/改ざん/破壊/利用停止)が発生する	
	(a) 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
	(b) 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
	(c) 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
	(d) 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
(2) セキュリティに係る法制度等の規定内容を遵守できない	
	(a) 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
(3) セキュリティ事象による被害が拡大し、自組織及び関係する他組織が適切に事業継続できない	
	(a) 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
	(b) 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

	(c) 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

第 2 層において想定されるセキュリティインシデント	
(1) セキュリティに係る攻撃を受けた IoT 機器の意図しない動作	
	(a) 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
	(b) 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
	(c) 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
	(d) 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
(2) IoT 機器の動作(正常動作・異常動作を問わない)による安全面に問題のある事象の発生(機器の破損、従業員への物理的危害、業務への悪影響等)	
	(a) 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
(3) IoT 機器によるサイバー空間へのフィジカル空間の状況の適切でない転写(誤計測)	
	(a) (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・サイバー空間の通信路上で改ざんされる
	(b) (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
	(c) 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

第 3 層において想定されるセキュリティインシデント	
(1) サイバー空間にて取り扱われる保護すべきデータが漏洩する	
	(a) 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
	(b) 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
	(c) 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
(2) サイバー空間にて取り扱われる保護すべきデータが改ざんされる	
	(a) 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
	(b) 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

(3) サイバー空間にて取り扱われる保護すべきデータ及びデータを収集/加工/蓄積/分析するシステムが意図しない動作(停止等)をする	
	(a) (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
	(b) 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
	(c) 攻撃の有無にかかわらず、データを取り扱うシステムが停止する
	(d) 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
(4) サイバー空間上のデータの取扱いに係る法規制や一部の関係者のみで共有するデータについて求められるセキュリティ水準を満たせない。	
	(a) サイバー空間におけるデータ保護を規定する法規則等への違反が発生する
	(b) 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

組織は、想定されるセキュリティインシデントを具体化した後に、当該インシデントによってもたらされる事業への影響および影響の大きさを割り当てることが望ましい。特に、事業への影響度を示す事業被害レベルの定義を検討する際は、「制御システムのセキュリティリスク分析ガイド 第 2 版」(IPA, 2018 年)の 4.3 事業被害と事業被害レベル、「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準(初版)」(NISC, 2018 年)等を参照することが可能である。

抽出した個々のセキュリティインシデント及びその結果に、それぞれ影響度に関するスコアを割り当てることで、適切に優先順位付けされたリスク対応が可能になると考えられる。

1．3．リスク分析の実施

1．1、1．2にて実施した内容を踏まえ、抽出したセキュリティインシデントにつながるような攻撃シナリオの検討、事業被害レベル、リスク源(脅威/脆弱性)の評価等を実施する。添付 B では、抽出したセキュリティインシデントに対して、当該事象の発生を助長、あるいは発生した事象の被害を拡大させる可能性がある脅威および、典型的な脆弱性を抽出しており、実際のリスク分析を実施する際にも、検討するリスク源の抽出および過不足のチェック等に活用可能である。

脆弱性の抽出に当たっては、図 16 に示すように、6 つの構成要素の観点から、より網羅的に典型的な脆弱性を抽出することを試みている。ただし、システム構成やデータフロー、該当する資産の内訳等は各組織において様々に異なることが予想されるため、具体的な攻撃シナリオの検討、事業被害レベル、リスク源の評価は各組織の事情を加味して実施することが望ましい。

リスク源の評価やセキュリティ対策を選定する際には、同一の具体的なモノが、異な

るバリュークリエイションプロセスにおいては、異なる6つの構成要素に対応する可能性があることに留意することが重要である。第Ⅰ部で説明したように、PC やサーバは、「システム」だけでなく、「モノ」として評価するのが適当な場合もある。また、ソフトウェアは、「プロシージャ」、「データ」、「モノ」のそれぞれで評価することが適切な場合もある。

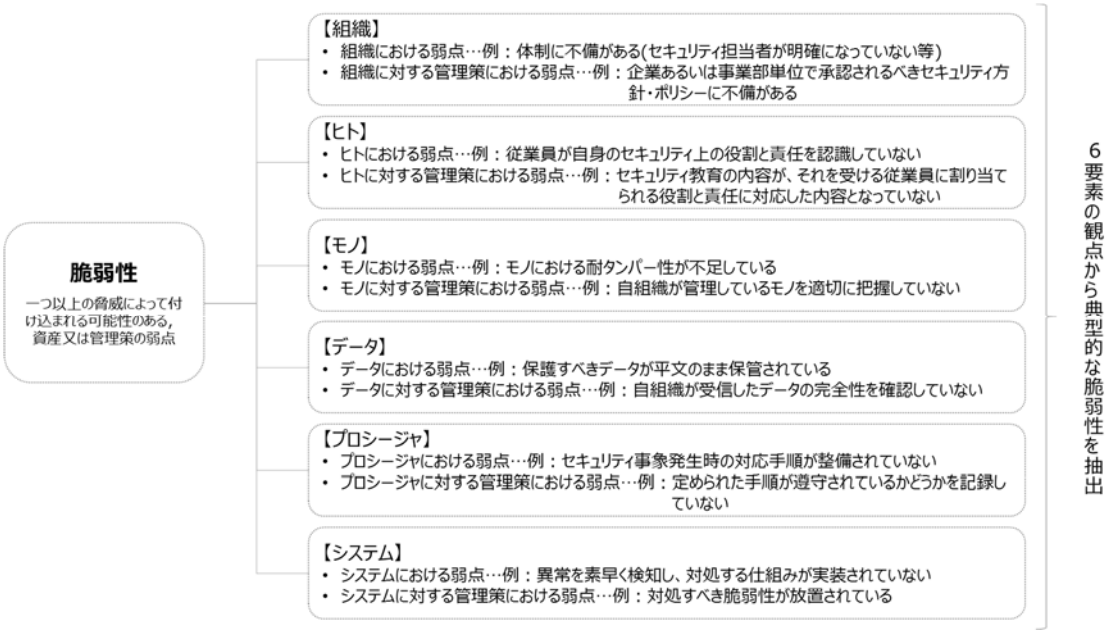


図 16 6 つの構成要素という観点による脆弱性の抽出

1．4．リスク対応の実施

1．3で実施したリスク分析により抽出されたリスクに対して、回避、低減、移転、保有[9]の内、いずれの対応をとるかを、発生時の被害の大きさ等に基づいて検討する。

(1) リスクの回避：リスクのある機能を削除したり全く別の方法に変更したりすることにより、リスクが発生する可能性を取り去る。
(2) リスクの低減：リスクに対して対策を講じることにより、発生しやすさや被害の深刻度を低減する。
(3) リスクの移転：保険加入や、リスクのある部分を他社製品・システムに置き換えることにより、リスクを他社などに移す。
(4) リスクの保有：リスクが小さい場合、特にリスクを低減するための対策を行わず、許容範囲内として受容する。

9 IPA「つながる世界のセーフティ&セキュリティ設計入門」から引用。

上記の内、特に低減を選択する場合の対応として、リスクの内容（脅威と脆弱性）に応じた対策要件を添付 B のとおり整理した。これを参照して、組織それぞれにあった対策要件を選択することが可能である。添付 B では、各々の対策要件に対して、特定の脆弱性との対応が図られているため、各組織が実施したリスク分析の結果と比較しつつ利用することが望ましい。

特に、本フレームワークにて、先に提示した 4 つのポイントについて、下記を例とした対策を実施することが望ましい。

① バリュークリエイションプロセスに関わるステークホルダーとの関係

- 1．1において明確化したステークホルダーとの関係性を基礎として、継続的に自組織を取り巻くステークホルダーの関係性に関する全体像を把握し続け、組織間でサイバーセキュリティ上の役割と責任を明確化しておくことが重要である。また、取引先や実施内容に変更等があった場合は、1．1で検討した内容を速やかに更新することが望ましい。
- ISO/IEC 27036-2:2014 は、個々のサプライヤーとの関係におけるライフサイクルとして、図17に示すような 5 つのフェーズがあると記載している。[10]

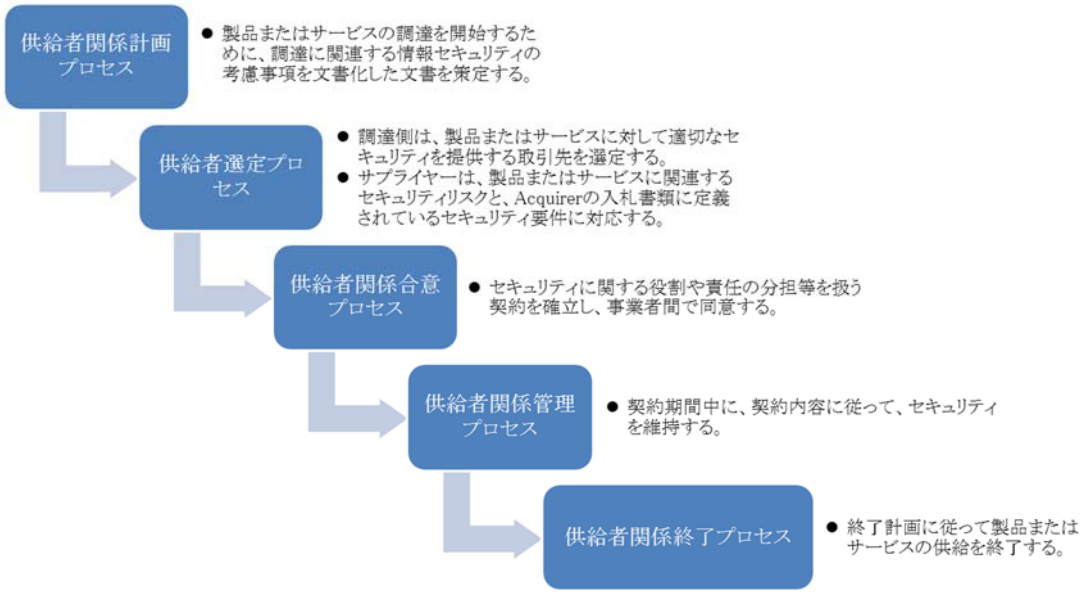


図 17 ISO/IEC 27036-2:2013 における個々のサプライヤーとの契約におけるライフサイクル

---

[10] 本ポイントに関連して、サプライチェーンにおけるセキュリティ対策に関して記述した標準として、ISO/IEC 27036:2014 や NIST SP 800-161 が策定されている。本フレームワークの策定に当たり、リスク源抽出において NIST SP 800-161 を、対策要件および対策例の記述に当たり、ISO/IEC 27036:2014 を参照している。本ポイントに関して、より高度な対策を実装する必要があると考えられる場合は、NIST SP 800-161 における管理策群を参照することが可能である。

・ 特に、第三部にて記載する対策カテゴリーCPS.SC(サプライチェーンリスクマネジメント)において、上記のライフサイクルを考慮した対策要件を設けている。左記の対策カテゴリー等を参照し、各組織においてライフサイクルを通じたステークホルダーとの関係性のマネジメントを検討することが望ましい。
  ➢ 関連する対策要件には、CPS.AM-5, CPS.AM-7, CPS.BE-2, CPS.BE-3, CPS.SC-1, CPS.SC-2 等がある。

② IoT 機器を介したサイバー空間とフィジカル空間の融合

・ センサ等から実際とは異なる計測データがサイバー空間へ提供される、あるいは計測データのサイバー空間への提供が停止してしまうと、収集された解析対象となるデータ及び、そのようなデータを利活用して実施されるオペレーションに対する信頼が損なわれる可能性がある。
・ そのような事態を避けるため、センサ等の機能に対する攻撃を考慮してセキュリティ対策を講ずる必要がある。具体的には、サービス拒否攻撃等を受けた場合でも動作を停止しづらい機器の利用、データの完全性チェックメカニズムを利用できる機器の利用、計測データの真正性を保証する機能を有した機器の利用等が考えられる。
  ➢ 関連する対策要件には、CPS.DS-4, CPS.DS-9, CPS.DS-15, CPS.CM-4 等がある。

・ 1．1でも述べた通り、サイバー空間からのデータ入力を受けてフィジカル空間でモノを制御したりする場合、セキュリティ上の問題が物理的な危害等の安全性に関する問題につながる可能性がある。フィジカル空間とサイバー空間の界面におけるセキュリティと安全の両立のためには、設計、調達の段階から安全性に係るハザードとそのリスク源を分析し、その結果から、セキュリティが影響を与える側面を特定するという一連のプロシージャを構築し、分析結果に応じて、設計・調達から運用・保守・廃棄の段階まで含めて、適切に対応することが重要である。
・ その際、安全性の確保を大前提として、その実現方策については、機能安全の観点からの対策やサイバーセキュリティ対策を組み合わせて対応することが必要である。こうした対応には、セーフティの観点からの検討と、セキュリティの観点からの検討の双方が求められるため、それぞれの検討の担当者同士がよく対話しながら対応を進めていくことが必要である。
  ➢ 関連する対策要件には、CPS.RA-4, CPS.RA-6, CPS.PT-3, CPS.CM-3 等がある。

➢ 安全制御系におけるセキュリティ面の統合については、近年国際標準化の場でも議論がなされており、IEC TR 63074, IEC TR 63069 等を参照することが可能である(参考図 18)。

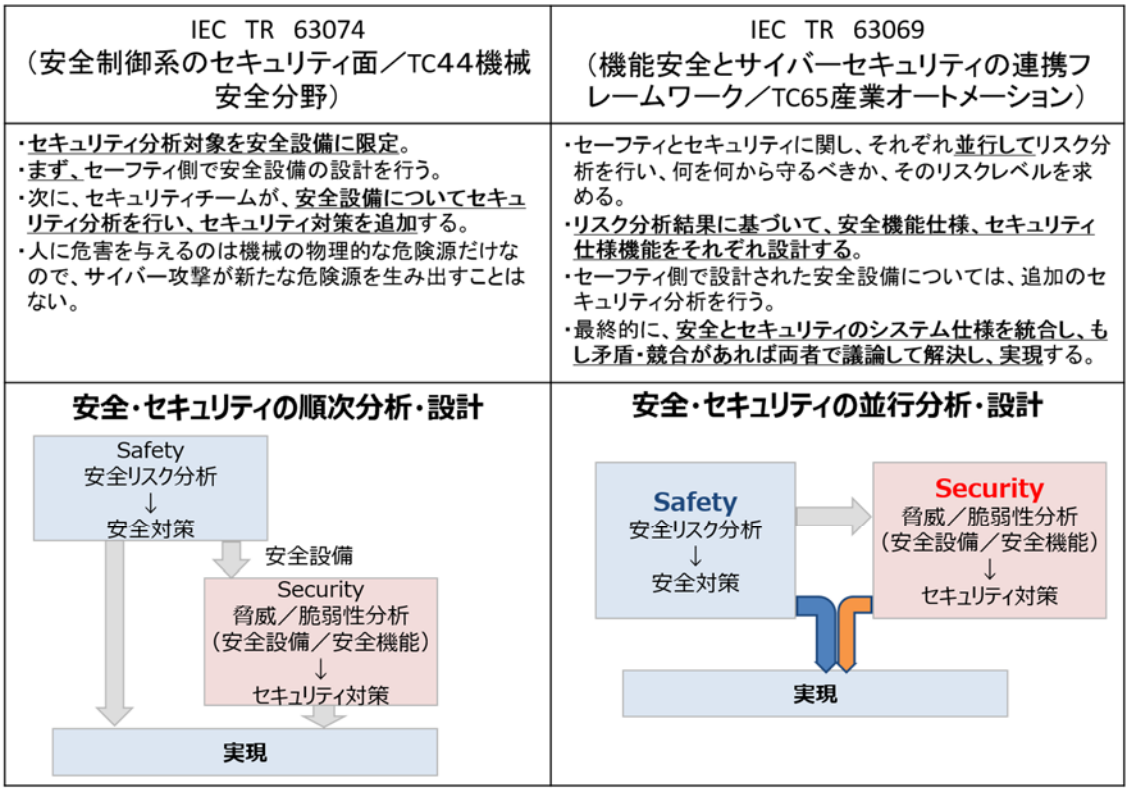


図 18 国際標準化活動におけるセーフティとセキュリティの統合に関する検討状況[11]

- サイバー空間とフィジカル空間とをつなぐ境界に位置する IoT 機器を介して、論理的な脅威だけでなく、フィジカル空間における物理的な脅威がサイバー空間に影響を与えることも想定される。
- そのため、自組織で利用する IoT 機器の重要度に応じて、物理的なセキュリティ対策を講ずる必要がある。例えば、重要な IoT 機器を設置する区域と、それ以外の区域を区分し、境界でアクセス制御を実施する、当該エリアを監視カメラ等で常時モニタリングし不正行為を検知する等の多層的な対策を行うことが考えられる。一方で、IoT 機器には、個人が持ち歩いたり、家庭や公共空間等に設置されたりするような、組織による管理が行き届きにくいものも存在する。この場合、

11 IPA「制御システム　セーフティ・セキュリティ要件検討ガイド」及び神余浩夫氏「機能安全と制御セキュリティの標準化動向」, 情報処理, Vol.58, No.11, Nov.2017 などを基に作成

上記で記載したアクセス制御やモニタリングが困難となるケースもあるため、盗難、紛失のリスクも考慮して対策を実施することが望ましい[12]。

- 関連する対策要件には、CPS.AC-2, CPS.DS-6, CPS.IP-5, CPS.IP-6, CPS.PT-2, CPS.CM-2 等がある。

③ 組織を跨るデータの流通

- 自組織の保護すべきデータが取引先により加工・分析、あるいは保管される、または、他組織の保護すべきデータを自組織が取扱うケースでは、交換するデータの重要性に関する区分、当該データに対する適切なレベルのデータの保護の確保に必要な、データの区分に応じたセキュリティ対策について事前に当該取引先との間で合意しておき、定期的に監査等の手法を用いて遵守を確認することが望ましい。
- その際、組織間で交換されるデータの性質、取引先あるいは自組織が提供するサービスの内容等を勘案してリスクを分析し、セキュリティ要求事項を具体化することが望ましい。
- また、事前に十分な対策を実施したとしても、保護すべきデータに対するセキュリティインシデントを検知した場合に適切に取引先へと状況の説明ができるよう、対応手順を事前に策定し、適切に関係者へと周知しておくことが望ましい。
- 他組織で処理されたデータを自組織が受入れる場合、正しい送信元からデータが送信されているか、データに攻撃コードが含まれていないか等を常時モニタリングしておき、異常を検知した場合に即座に対応できるようにしておくことが望ましい。
  - 関連する対策要件には、CPS.SC-3, CPS.SC-4, CPS.SC-6, CPS.CM-1, CPS.CM-3, CPS.CM-4, CPS.DP-1, CPS.RP-2, CPS.CO-1 等がある。

④ 各層における信頼性の基点の確保

- 第 1 層においては、①において特定されているステークホルダーとの関係性の全体像に基づいて、各々の組織(ステークホルダー)との信頼関係を維持するに当たり必要なサイバーセキュリティに関係する要求事項を契約にて明確化し、定期的に遵守を確認することが重要である。
- その際、確認を受ける側は、あらかじめ、遵守を証明するための情報(データ)を収集しておき、求めに応じて開示できるようにしておくことが望ましい。特に、自組織の事業継続上重要な取引先については、直接の委託先のみならず、再委

[12] 対策を検討する場合、IoT 推進コンソーシアム，総務省，経済産業省『IoT セキュリティガイドライン ver.1.0』の要点 6 を参照することが望ましい。

託先以降の組織についても定めている要求事項を遵守しているかどうかを確認することで、信頼のチェーンを構築することが望ましい。

- 関連する対策要件には、CPS.SC-2, CPS.SC-3, CPS.SC-4, CPS.SC-5 等がある。

・ 第 2 層においては、IoT 機器による転写機能の正確性を確保することが求められる。そのためには、設計、調達フェーズから運用、廃棄フェーズに至るまでの、ライフサイクルを通じた対策を講ずることで当該 IoT 機器におけるセキュリティ上の健全性を維持・向上することが重要である。

・ 具体的には、設計、調達時におけるセキュリティ・バイ・デザインの実施、テストによるセキュリティ機能の検証、運用時における脆弱性マネジメント、機器・ソフトウェアの完全性検証等の対策を実施することが望ましい。

・ また、自組織の事業継続において特に重要な IoT 機器については、転写機能を保証するためのセキュリティ等に係る要求事項を契約の際に明確化しておき、委託先、あるいは再委託先以降の組織により実行される製造、輸送等の一連のプロセスにおいて要求事項が正確に遵守されているかどうかを、確認できるようにしておくことが望ましい。

・ 一方、IoT 機器におけるセキュリティ対策を考える上で、従来の IT システムに対する対策とは異なるポイントを考慮する必要がある可能性がある点が指摘されている[13]。調達においてはセキュリティ・バイ・デザインの原則に基づき、十分なセキュリティ機能を要求することを前提とするが、そのような機能を実装する機器の調達が困難な場合、システム側において代替的な対策を検討する必要が生じる。添付 C では、CPS.IP-10、CPS.CM-3、CPS.CM-6 等、複数の対策要件について IoT 機器に対する対策を検討する上で考慮すべきポイントを記載している。IoT 機器における対策を検討する際には、当該項目を参照することが望ましい。

- 関連する対策要件には、CPS.RA-4, CPS.RA-6, CPS.DS-8, CPS.DS-10, CPS.DS-12, CPS.CM-6, CPS.CM-7 等がある。

・ 第 3 層においては、サイバー空間のデータ及び、その加工・分析・保管という諸機能の信頼性を確保することが求められる。

・ そのためには、第 1 層、第 2 層で述べた観点に加え、利活用するデータそのものが信頼できるかを確認することが重要となる。具体的には、データが改ざんされたものでないか、攻撃コード等を含む許容範囲外のものでないか、不正な構成要素(組織、ヒト、モノ等)から生成・送信されたものでないか等の観点があると考えられる。

---

13 例えば、Draft NISTIR 8228 では、機器のセキュリティ、データのセキュリティ、プライバシーという 3 つの観点から IoT におけるセキュリティ保護を実現するにあたり、資産管理、脆弱性管理、アクセス管理、インシデント検知、データフロー管理等の対策で従来の IT 機器とは異なる IoT 機器特有の性質を踏まえる必要があるとしている。

・ また、自組織の事業継続において特に重要なデータについては、当該データの作成・加工元である組織のマネジメントの信頼性を確認し、自組織に発信される利活用データの適格性(改ざんの有無、攻撃コードの有無等)をモニタリングすることに加え、データの加工・分析等の業務が、適切なレベルのセキュリティを実装したモノ及びシステムで、適切なプロシージャによって実行されているかを確認できるようにしておくことが望ましい。

➢ 関連する対策要件には、CPS.DS-9, CPS.DS-13, CPS.AE-1, CPS.CM-3, CPS.CM-4, CPS.CM-5 等がある。

表６ リスク源の洗い出しにおいて考慮すべき観点に対応した対策要件の一例

リスク源を洗い出す観点	関係する対策要件の一例
バリュークリエイションプロセスに関わるステークホルダーとの関係	CPS.AM-5, CPS.AM-7, CPS.BE-2, CPS.BE-3, CPS.SC-1, CPS.SC-2, CPS.DS-13, CPS.CM-4
IoT 機器を介したサイバー空間とフィジカル空間の融合	CPS.RA-4, CPS.RA-6, CPS.PT-3, CPS.CM-3
組織を跨るデータの流通	CPS.SC-3, CPS.SC-4, CPS.SC-6, CPS.CM-1, CPS.CM-3, CPS.CM-4, CPS.DP-1, CPS.RP-2, CPS.CO-1
各層における信頼性の基点の確保	CPS.RA-4, CPS.RA-6, CPS.SC-2, CPS.SC-3, CPS.SC-4, CPS.DS-8, CPS.DS-10, CPS.CM-4, CPS.CM-5

２．添付Ｂの見方

添付 B では、下記表5に示す通り、各層における機能、想定されるセキュリティインシデント、リスク源(脅威、脆弱性)、対策要件を表形式で一覧化している。

表７ 添付 B における記載の例(第 3 層)

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#
		脅威	脆弱性#	脆弱性		
下記すべてに関わる ・データを加工・分析する機能 ・データを保管する機能 ・データを送受信する機能	サービス拒否攻撃により、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_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、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-4

「機能」は、１．１の表2で整理した三層構造アプローチにおける各層の機能を表している。「想定されるセキュリティインシデント」は、左記に記載した各層の機能を侵害

する可能性のある、主にセキュリティに起因した事象であり、1．1の表5で整理したものである。当該セキュリティインシデントは、「リスク源」に記載されている「脅威」や「脆弱性」を原因として引き起こされ得る。組織は、深刻な影響を及ぼす可能性のある「リスク源」に対して、リスク対応を実施する必要があるが、その際に対応策となる見込みの高い要件を、「対策要件」として記載している。脆弱性及び対策要件には、固有の識別子（ID）を付与しており、第Ⅲ部及びより詳細な対策例等を記載した添付Cにおいても当該識別子による参照が可能である。

以上の記載は簡易的ではあるが、リスクアセスメントの形式を模したものとなっており、実際に各組織においてリスクマネジメントを実施する際にも参照しやすいように記載している。

第Ⅲ部　メソッド：セキュリティ対策要件と対策例集

１．対策要件及び対策例集を活用したリスク対応

第Ⅱ部におけるリスク源と対策要件の抽出を受けて、第Ⅲ部および添付 C では、抽出した対策要件に対応したセキュリティ対策例、対策要件および対策例と他の国際規格等との関係性を示す。

第Ⅲ部および添付 C は、リスクマネジメントプロセスにおけるリスク対応のフェーズにおいて最も有用に機能すると考えられる。組織は、下記の用途に本項の内容を活用することができる。以下で、(1)(2)のそれぞれについて本項の利用方法を記述する。

(1) 自組織のセキュリティマネジメント強化

第Ⅱ部1．4にも記載したとおり、組織はリスクアセスメントの結果に応じて、第Ⅲ部に記載された対策要件および、添付 C に記載されたセキュリティ対策例を実装し、リスクマネジメントプロセスを適切に実施することで、自組織のセキュリティマネジメントを改善することが可能である。その際、「はじめに　7．フレームワークの使い方」でも記載したとおり、以下の 2 点にて各組織のセキュリティ対策の助けになることが期待される。

① 各組織において実装する対策の水準を考慮した対策の実施
② 国際標準等との比較

①に関しては、添付 C にて、各組織で実装すべきセキュリティ対策のレベル選択の一助とするため、国内外の様々なガイドライン等を参照した上で、参照した文書による分類をベースに、対象とするスコープ(例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か)、対策を導入・運用する際の相対的コスト等の観点を考慮して、セキュリティ対策例を High　Advanced、Advanced、Basic の三段階のレベルに分けて示している。

なお、添付Cで整理した対策例集は、あくまで対策の一例を示すものであり、他の実装を何ら否定するものではない。各組織のセキュリティ対策の実施担当者は、適用対象となる組織やシステムの重要度やリスクアセスメントの結果等に応じて、対策例集も参考に適切なセキュリティ対策を検討することが望ましい。

②に関しては、第Ⅲ部、添付 C 及び添付Dにおいて、主要な国際規格等との対応関係を記載している。これにより、対策要件の実装を通じた特定の規格等への準拠や参照先の規格等の要求事項と組み合わせたセキュリティ対策の高度化等に本フレームワークが活用されることを期待する。

(2) サプライチェーン上の取引先に対するセキュリティのガバナンス強化

組織は、自組織のセキュリティマネジメント強化だけでなく、自身の関係するサプライチェーン上の取引先に対して、本フレームワークの特定の対策要件への準拠を求める等の手段により、取引先へのセキュリティガバナンスを強化することが可能である。

その際に取引先に対して実施する一連のプロセスを記載した対策要件として、CPS.SC-2、CPS.SC-3、CPS.SC-4、CPS.SC-5 等がある。上記を効果的に実施することにより、委託元は委託先に対して、第Ⅱ部1．4でも言及した契約のライフサイクルを通じたガバナンスの強化を図ることができる。

委託先への要求事項は、委託する業務の内容や、自組織の事業における当該委託先の重要度等により変化することが見込まれるため、第Ⅱ部を参考に、(取引先の行為に起因する)対処すべきリスク・リスク源を抽出した上で決定されることが望ましい。

また、委託元と委託先という二者関係にガバナンスの範囲をとどめるのでなく、特に重要な委託先については、再委託先以降にまで仕様・要求事項の遵守を確認することで、サプライチェーン全体におけるセキュリティリスクマネジメントを確立・維持することも可能であると考えられる。その際は、当該事業者において、求められるセキュリティ対策のレベルを適切に把握し、妥当性があると考えられるレベルの対策の実装を求めることが望ましい。

２．対策例集の見方

添付Ｃでは、対策要件、対策要件を実装する際のレベル別の対策例、対策例と主要な国際規格等との対応関係を表形式で一覧化している。表８に添付Ｃの記載事項を示す。

表８ 添付Ｃの記載例

対策要件ID	対策要件	対策例	対策例を実行する主体	NIST SP800-171	NIST SP800-53	ISO/IEC 27001 附属書 A
		<H.Advanced>			○	
		<Advanced>		○	○	○
		<Basic>			○	○

対策のレベルは、既存の国際規格等におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により、High Advanced, Advanced, Basic の順に整理している。High Advanced の対策例を

実装する場合は、High Advanced だけでなく、Advanced 及び Basic に記載の内容も包含するように対策を実装する必要がある。

また、「対策例を実装する主体」において、当該対策例を実装するに当たり、主体となる要素を、3 つに分類して提示する[14]。一般的に技術的な手法を通じてシステムにより実装される対策は、”S”を、一般的に組織（例：非技術的な手法を通じてヒト)により実装される対策は、”O”を、実装主体がシステム及び組織の両方であり得る場合、”O/S”をそれぞれ記載している。

対策例集に記載の対策例は、あくまで対策要件に対応するための対策の一例を参考として示しているに過ぎず、対策例集に記載のない対策により当該対策要件を充足することも可能である。したがって、本対策例集は、各組織におけるコストを考慮した対策の実施や、国際標準等との比較のため、活用されることが望ましい。

３．対策要件

本フレームワークにて示す対策要件をカテゴリー別に表10～29に示す。

(1) 対策要件のカテゴリー

本フレームワークにて示す対策要件を記述する上で、国際ハーモナイゼーションの観点から、NIST Cybersecurity Framework ver1.1 のサブカテゴリーに対応付ける形で表9に示すように20カテゴリーを定めた。

表 9 対策要件のカテゴリーと NIST Cybersecurity Framework との対応関係

カテゴリー名称	略称	NIST Cybersecurity Framework v1.1 の対応カテゴリー
資産管理	CPS.AM	ID.AM (Asset Management)
ビジネス環境	CPS.BE	ID.BE (Business Environment)
ガバナンス	CPS.GV	ID.GV (Governance)
リスク評価	CPS.RA	ID.RA (Risk Assessment)
リスク管理戦略	CPS.RM	ID.RM (Risk Management Strategy)
サプライチェーンリスク管理	CPS.SC	ID.SC (Supply Chain Risk Management)
アイデンティティ管理、認証及びアクセス制御	CPS.AC	PR.AC (Identity Management and Access Control)
意識向上及びトレーニング	CPS.AT	PR.AT (Awareness and Training)
データセキュリティ	CPS.DS	PR.DS (Data Security)

[14] 表記法は、NIST SP 800-53 Rev. 5 (DRAFT) APPENDIX D に従っている。

カテゴリー名称	略称	NIST Cybersecurity Framework v1.1 の対応カテゴリー
情報を保護するためのプロセスおよび手順	CPS.IP	PR.IP (Information Protection Processes and Procedures)
保守	CPS.MA	PR.MA (Maintenance)
保護技術	CPS.PT	PR.PT (Protective Technology)
異常とイベント	CPS.AE	DE.AE (Anomalies and Events)
セキュリティの継続的なモニタリング	CPS.CM	DE.CM (Security Continuous Monitoring)
検知プロセス	CPS.DP	DE.DP (Detection Processes)
対応計画	CPS.RP	RS.RP (Response Planning) RC.RP (Recovery Planning)
伝達	CPS.CO	RS.CO (Communications) RC.CO (Communications)
分析	CPS.AN	RS.AN (Analysis)
低減	CPS.MI	RS.MI (Mitigation)
改善	CPS.IM	RS.IM (Improvements) RC.IM (Improvements)

(2) 国内外主要規格との対応

NIST Cybersecurity Framework ver1.1 の参照文献も参考に、各対策要件に対応する国内外主要規格を「関連標準等」として整理した。整理の対象とした規格は以下のとおりである。

- NIST “Framework for Improving Critical Infrastructure Cybersecurity Version 1.1”
- Council on CyberSecurity(the Council) “The Critical Security Controls”
- ISACA “Control Objectives for Information- related Technology 5” (COBIT 5)
- ISA 62443-2-1:2010 “Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program”
- ISA 62443-3-3:2013 “Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels”
- ISO/IEC 27001:2013 “Information technology -- Security techniques -- Information security management systems - Requirements”
- NIST “Special Publication 800-53 Revison 4”(SP 800-53 Rev.4)

・ ISO/IEC 15408-2:2010 “Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components”
・ IoT 推進コンソーシアム，総務省，経済産業省 “IoT セキュリティガイドライン”

３．１．CPS.AM – 資産管理

組織が事業目的を達成することを可能にするデータ、ヒト、モノ、システム、施設等を特定し、自組織のリスク戦略とその目的における重要性に応じた管理をする。

表 10 CPS.AM カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.AM-1	・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する	L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L2_1_a_ORG, L2_3_b_ORG	NIST Cybersecurity Framework Ver.1.1 ID.AM-1, ID.AM-2 CCSCIS CSC 1, CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FMT IoT セキュリティガイドライン 要点 3, 要点 15
CPS.AM-2	・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	L1_2_a_COM	ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FIA
CPS.AM-3	・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	L1_2_a_COM, L1_3_a_COM	
CPS.AM-4	・組織内の通信ネットワーク構成図及び、データフロー図を作成し、保管する	L1_3_a_ORG, L1_3_b_ORG	NIST Cybersecurity Framework Ver.1.1 ID.AM-3 CIS CSC 112 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8

CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、保管する	L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L1_3_a_ORG, L1_3_b_ORG	NIST Cybersecurity Framework Ver.1.1 ID.AM-4 CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9 IoT セキュリティガイドライン 要点 3
CPS.AM-6	・リソース(例:ヒト、モノ、データ、システム)を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、関係者に伝達する	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG	NIST Cybersecurity Framework Ver.1.1 ID.AM-5 CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6 IoT セキュリティガイドライン 要点 3
CPS.AM-7	・自組織および関係する他組織のサイバーセキュリティ上の役割と責任を定める	L1_3_a_ORG, L1_3_b_ORG	NIST Cybersecurity Framework Ver.1.1 ID.AM-6 CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 IoT セキュリティガイドライン 要点 18, 要点 19, 要点 20

3．2．CPS.BE – ビジネス環境

自組織のミッション、目標、利害関係者、活動を理解し、優先順位付けを行う。この情報はサイバーセキュリティ上の役割、責任、リスク管理上の意思決定を伝達するために使用される。

表 11 CPS.BE カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.BE-1	・サプライチェーンにおいて、自組織が担う役割を特定し共有する	L1_3_a_ORG, L1_3_b_ORG	NIST Cybersecurity Framework Ver.1.1 ID.BE-1, ID.BE-2

			COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12 IoT セキュリティガイドライン 要点 20
CPS.BE-2	・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、関係者(サプライヤー、第三者プロバイダ等を含む)に共有する	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG	NIST Cybersecurity Framework Ver.1.1 ID.BE-3 COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
CPS.BE-3	・自組織が事業を継続する上での自組織および関係する他組織における依存関係と重要な機能を識別する	L1_3_a_ORG, L1_3_b_ORG	NIST Cybersecurity Framework Ver.1.1 ID.BE-4 COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

３．３．CPS.GV – ガバナンス

自組織に対する規制、法律、リスクと、自組織の環境、運用上の要求事項を管理しモニタリングするためのポリシー、手順、プロセスを理解し、サイバーセキュリティリスクの管理者に伝達する。

表 12 CPS.GV カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.GV-1	・セキュリティポリシーを策定し、自組織および関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO	NIST Cybersecurity Framework Ver.1.1 ID.GV-1, ID.GV-2 CIS CSC 19 COBIT 5 APO01.02, APO01.03, APO10.03, APO13.01, APO13.1202, DSS05.04, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6, 4.3.2.3.3 ISO/IEC 27001:2013 A.5.1.1, A.6.1.1, A.7.2.1, A.15.1.1

			NIST SP 800-53 Rev. 4 -1 controls from all security control families IoT セキュリティガイドライン 要点 1, 要点 18, 要点 19
CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定し、法令や業界のガイドラインの更新に合わせて継続的かつ速やかにルールを見直す	L1_3_c_ORG, L1_3_c_COM, L1_3_c_SYS, L1_3_c_PRO, L1_3_c_DAT	NIST Cybersecurity Framework Ver.1.1 ID.GV-3 CIS CSC 19 COBIT 5 BAI02.01, MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 NIST SP 800-53 Rev. 4 -1 controls from all security control families ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FPR, FDP
CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う	L1_1_a_DAT, L1_1_b_SYS, L3_1_a_SYS, L3_1_a_DAT, L3_4_a_ORG, L3_4_a_PRO	
CPS.GV-4	・サイバーセキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO	NIST Cybersecurity Framework Ver.1.1 ID.GV-4 COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 ISO/IEC 27001:2013 Clause 6 NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FMT IoT セキュリティガイドライン 要点 2

3．4．CPS.RA – リスク評価

組織は自組織の業務（ミッション、機能、イメージ、評判を含む）、資産、個人に対するサイバーセキュリティリスクを把握する。

表 13 CPS.RA カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.RA-1	・自組織の資産の脆弱性を特定し、文書化する	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS	NIST Cybersecurity Framework Ver.1.1 ID.RA-1 CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 ISO/IEC 15408-1 (CC v3.1 Release5 Part 1) IoT セキュリティガイドライン 要点 21
CPS.RA-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	L1_2_a_ORG, L2_1_a_ORG, L2_1_c_SYS, L3_1_a_SYS, L3_3_d_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 ID.RA-2, RS.AN-5 CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16 IoT セキュリティガイドライン 要点 18, 要点 21
CPS.RA-3	・自組織の資産に対する脅威を特定し、文書化する	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS	NIST Cybersecurity Framework Ver.1.1 ID.RA-3 CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16 ISO/IEC 15408-1 (CC v3.1 Release5 Part 1)
CPS.RA-4	・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する ・IoT 機器および IoT 機器を含んだ	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_a_ORG L2_1_a_PRO	NIST Cybersecurity Framework Ver.1.1 ID.RA-4, RS.MI-3 CIS CSC 4 COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12

	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	L2_2_a_ORG	ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM-9, PM-11 ISO/IEC 15408-1 (CC v3.1 Release5 Part 1) IoT セキュリティガイドライン 要点 10, 要点 12
CPS.RA-5	・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS	NIST Cybersecurity Framework Ver.1.1 ID.RA-5 CIS CSC 4 COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 ISO/IEC 15408-1 (CC v3.1 Release5 Part 1)
CPS.RA-6	・リスクアセスメントに基づき、発生しうるセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する ・IoT 機器および IoT 機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティおよび関連するセーフティのリスクに対して適宜対応する	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_a_ORG, L2_1_a_PRO	NIST Cybersecurity Framework Ver.1.1 ID.RA-6, RS.MI-3 CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Clause 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9 ISO/IEC 15408-1 (CC v3.1 Release5 Part 1) IoT セキュリティガイドライン 要点 10, 要点 12

３．５．CPS.RM – リスク管理戦略

自組織の優先順位、制約、リスク許容度、想定を定め、運用リスクの判断に利用する。

表 14 CPS.RM カテゴリーの対策要件

対策要 ID	対策要件	対応する脆弱性	関連標準等
CPS.RM-1	・関係者のサイバーセキュリティリスクマネジメントの実施状況について確認する。また、自組織の事業に関する自組織および関係者の責任範囲を明確化し、セキュリティマネジメントの実施状況を確認するプロセスを確立し、実施する。	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_3_a_ORG, L1_3_b_ORG	NIST Cybersecurity Framework Ver.1.1 ID.RM-1 CIS CSC 4 COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3

			NIST SP 800-53 Rev. 4 PM-9 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FMT IoT セキュリティガイドライン 要点 12
CPS.RM-2	・リスクアセスメント結果およびサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS	NIST Cybersecurity Framework Ver.1.1 ID.RM-2, ID.RM-3 COBIT 5 APO12.02, APO12.06 ISA 62443-2-1:2009 4.3.2.6.5 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11

3．6．CPS.SC – サプライチェーンリスク管理

組織の優先順位、制約、リスク許容値、および想定が、サプライチェーンリスク管理に関連するリスクの決定を支援するために確立され、利用される。組織は、サプライチェーンのリスクを特定、評価、管理するプロセスを確立し、実施する。

表 15 CPS.SC カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.SC-1	・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について関係者と合意する	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG	NIST Cybersecurity Framework Ver.1.1 ID.SC-1 CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FMT
CPS.SC-2	・自組織の事業を継続するに当たり重要な関係者を特定、優先付けをし、評価する ・機器調達時に、適切なマネジメントシステムが構築・運用され、問い合わせ窓口やサポート体制等が確	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG, L2_1_a_COM, L2_1_a_PRO, L2_1_a_DAT, L2_3_a_ORG,	NIST Cybersecurity Framework Ver.1.1 ID.SC-2 COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12,

	立されたIoT機器のサプライヤーを選定する ・サービスやシステムの運用において、サービスマネジメントを効率的、効果的に運営管理するサービスサプライヤーを選定する	L2_3_c_ORG, L3_1_b_ORG, L3_3_d_ORG, L3_1_c_ORG, L3_3_a_ORG, L3_3_b_ORG	4.2.3.13, 4.2.3.14ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9 ISO/IEC 15408-1 (CC v3.1 Release5 Part 1) IoT セキュリティガイドライン 要点 14
CPS.SC-3	・外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	L1_1_a_ORG, L1_1_a_PRO, L1_1_a_DAT, L1_1_b_PRO, L1_1_c_PRO, L1_1_d_ORG, L2_3_c_ORG, L3_1_b_ORG, L3_1_b_DAT, L3_3_d_ORG, L3_1_c_ORG, L3_1_c_DAT, L3_3_a_ORG,. L3_3_b_ORG, L3_3_c_ORG, L3_4_a_DAT	NIST Cybersecurity Framework Ver.1.1 ID.SC-3 COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCS, FDP, FIA, FMT IoT セキュリティガイドライン 要点 5, 要点 11
CPS.SC-4	・外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する	L1_1_a_ORG, L1_1_a_DAT, L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_1_d_ORG, L1_1_d_COM, L2_1_a_ORG, L2_1_a_COM, L2_1_a_PRO, L2_2_a_ORG, L2_3_a_ORG, L2_3_c_ORG, L2_3_c_PRO,	ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FIA, FDP IoT セキュリティガイドライン 要点 14

		L3_1_b_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_c_ORG, L3_3_d_ORG	
CPS.SC-5	・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する	L1_1_a_DAT, L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L2_3_c_ORG, L2_3_c_PRO, L1_1_a_ORG, L1_1_a_DAT, L3_1_a_DAT, L3_1_b_ORG, L3_1_b_DAT, L3_3_d_ORG, L3_1_c_ORG, L3_1_c_DAT, L3_3_a_ORG,. L3_3_b_ORG, L3_3_c_ORG, L3_4_a_DAT	NIST Cybersecurity Framework Ver.1.1 ID.SC-4 COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISA 62443-2-1:2009 4.3.2.6.7 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
CPS.SC-6	・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。	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_1_d_ORG, L2_2_a_ORG, L2_3_c_ORG, L2_3_c_PRO, L3_1_b_ORG, L3_1_c_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_c_ORG	

CPS.SC-7	・自組織が関係する他組織との契約上の義務を果たしていることを証明するための情報(データ)を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする	LL1_1_d_ORG, 2_2_a_ORG, L2_3_c_ORG, L2_3_c_PRO, L3_1_b_ORG, L3_1_c_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_b_ORG, L3_3_c_ORG	COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISA 62443-2-1:2009 4.3.2.6.7 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
CPS.SC-8	・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	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO, L2_3_b_PEO, L3_1_b_PEO, L3_1_c_PEO	NIST SP 800-53 Rev.4 PS-7
CPS.SC-9	・サプライチェーンにおけるインシデント対応活動を確実にするために、関係者間で対応プロセスの整備と訓練を行う	L1_3_a_PEO	NIST Cybersecurity Framework Ver.1.1 ID.SC-5 CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
CPS.SC-10	・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。	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO	
CPS.SC-11	・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。	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO	

3．7．CPS.AC – アイデンティティ管理、認証及びアクセス制御

資産および関連施設への論理的・物理的アクセスを、承認された組織、ヒト、

モノ、プロシージャに限定し、承認された活動およびトランザクションに対する不正アクセスのリスクの大きさに合うよう管理する。

表 16 CPS.AC カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.AC-1	・承認されたモノとヒトおよびプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する	L1_1_b_SYS, L2_3_c_SYS L3_3_a_SYS L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-1 CIS CSC 1, 5, 15, 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA Family-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FAU, FIA, FMT
CPS.AC-2	・IoT 機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する	L1_1_a_SYS, L2_3_b_PEO, L2_3_b_SYS, L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-2 COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 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.11.2.3 1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FIA, FMT, FDP
CPS.AC-3	・無線接続先(ユーザーや IoT 機器、サーバ等)を正しく認証する	L2_3_c_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-3 CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.21, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1

			NIST SP 800-53 Rev. 4 AC--1, AC-17, AC-19, AC-20, SC-15 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCS, FIA, FMT IoT セキュリティガイドライン 要点 8, 要点 11, 要点 14, 要点 16__
CPS.AC-4	・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける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	L2_1_b_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-3 CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.21, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC--1, AC-17, AC-19, AC-20, SC-15 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FIA IoT セキュリティガイドライン 要点 4
CPS.AC-5	・ユーザーが利用する機能と、システム管理者が利用する機能を分離する	L1_1_b_SYS, L2_1_c_SYS, L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-4 CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FMT IoT セキュリティガイドライン 要点 4
CPS.AC-6	・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	L1_1_b_SYS, L2_1_c_SYS, L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-4, PR.AC-7 CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5

			NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FMT, FIA IoT セキュリティガイドライン 要点 8
CPS.AC-7	・適宜ネットワークを分離する(例:開発・テスト環境と実運用環境、IoT 機器を含む環境と組織内の他の環境)等してネットワークの完全性を保護する	L2_1_b_SYS, L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-5, PR.DS-7, PR.PT-4 CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
CPS.AC-8	・IoT 機器、サーバ等がサイバー空間で得られた分析結果を受信する際、及び IoT 機器、サーバ等が生成した情報(データ)をサイバー空間へ送信する際、双方がそれぞれ接続相手の ID(識別子)を利用して、接続相手を識別し、認証する ・IoT 機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する	L2_1_b_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-6 CIS CSC, 16 COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCO, FCS, FDP, FIA IoT セキュリティガイドライン 要点 11, 要点 14, 要点 16
CPS.AC-9	・IoT 機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する	L1_1_b_SYS, L2_1_b_SYS L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-7 CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9

			ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCS, FDP, FIA, FPR IoT セキュリティガイドライン 要点 8, 要点 14, 要点 16

３．８．CPS.AT – 意識向上及びトレーニング

自組織の職員およびパートナーに対して、関連するポリシー、手順、契約に基づいた、サイバーセキュリティに関連する義務と責任を果たすために、サイバーセキュリティ意識向上教育と、訓練を実施する。

表 17 CPS.AT カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.AT-1	・自組織の全ての要員に対して、セキュリティインシデントの発生と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	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO, L1_1_d_PEO, L1_2_a_PEO, L1_3_b_PEO, L3_4_a_PEO	NIST Cybersecurity Framework Ver.1.1 PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5
CPS.AT-2	・自組織におけるセキュリティインシデントに関係しうる関係組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施する	L1_3_c_PEO, L3_3_a_PEO	NIST Cybersecurity Framework Ver.1.1 PR.AT-3, PR.IP-10, RS.CO-1 CIS CSC 917 COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16

３．９．CPS.DS – データセキュリティ

データと記録をデータの機密性、完全性、可用性を保護するために定められた自組織のリスク戦略に従って管理する。

表 18 CPS.DS カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.DS-1	・情報(データ)を適切な強度の方式で暗号化して保管する	L1_1_a_DAT, L1_1_a_SYS, L3_1_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-1 CIS CSC 1713, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCA
CPS.DS-2	・IoT 機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する	L1_1_a_SYS, L1_1_b_DAT, L3_1_a_SYS, L3_2_b_DAT, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-2 CIS CSC 1713, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 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 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCO, FCS IoT セキュリティガイドライン 要点 14
CPS.DS-3	・情報(データ)を送受信する際に、情報(データ)そのものを暗号化して送受信する	L1_1_a_SYS, L1_1_b_DAT, L3_1_a_SYS, L3_2_b_DAT, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-2 CIS CSC 1713, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 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 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCS IoT セキュリティガイドライン 要点 14

CPS.DS-4	・送受信データ、保管データの暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。	L1_1_a_DAT, L3_1_a_SYS	ISO/IEC 27001:2013 A.10.1.2 NIST SP 800-53 Rev. 4 SC-12
CPS.DS-5	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、サービス活動を停止しないよう、モノ、システムに十分なリソース(処理能力、通信帯域、ストレージ容量)を確保する	L2_1_d_SYS, L1_1_c_SYS, L3_3_c_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-4 CIS CSC 13 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2 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.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCO, FRU
CPS.DS-6	・IoT 機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う	L2_1_d_SYS, L1_1_c_SYS, L3_3_c_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-4 CIS CSC 13 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2 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.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FRU
CPS.DS-7	・保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する	L1_1_d_COM L2_3_b_COM	NIST Cybersecurity Framework Ver.1.1 PR.DS-5 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2

			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.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCS, FPT IoT セキュリティガイドライン 要点 8
CPS.DS-8	・自組織の保護すべきデータが不適切なエンティティに渡ったことを検知した場合、ファイル閲覧停止等の適切な対応を実施する	L1_1_a_DAT, L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-5 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2 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.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCS, FPT IoT セキュリティガイドライン 要点 8
CPS.DS-9	・IoT 機器、サーバ等の起動時に、起動するソフトウェアの完全性を検証し、不正なソフトウェアの起動を防止する	L2_3_b_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-6 CIS CSC 2, 3 COBIT 5 APO01.06, BAI06.01, DSS06.02 ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 NIST SP 800-53 Rev. 4 SC-16, SI-7 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCS, FPT

			IoT セキュリティガイドライン 要点 8
CPS.DS-10	・送受信・保管する情報(データ)に完全性チェックメカニズムを使用する	L1_1_b_DAT, L1_1_d_PRO, L3_2_a_DAT, L3_2_b_DAT	NIST Cybersecurity Framework Ver.1.1 PR.DS-6 CIS CSC 2, 3 COBIT 5 APO01.06, BAI06.01, DSS06.02 ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 NIST SP 800-53 Rev. 4 SC-16, SI-7 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCS, FPT IoT セキュリティガイドライン 要点 8
CPS.DS-11	・ハードウェアの完全性を検証するために整合性チェックメカニズムを使用する	L1_1_d_PRO, L2_3_b_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-8 COBIT 5 BAI03.05 ISA 62443-2-1:2009 4.3.4.4.4 ISO/IEC 27001:2013 A.11.2.4 NIST SP 800-53 Rev. 4 SA-10, SI-7 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCS, FPT IoT セキュリティガイドライン 要点 8
CPS.DS-12	・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	L1_1_d_PRO, L2_3_c_ORG, L2_3_c_SYS	ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FIA, FDP, FCS
CPS.DS-13	・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	L3_4_a_PRO	ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FAU IoT セキュリティガイドライン 要点 13
CPS.DS-14	・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	L2_1_a_ORG, L2_1_a_COM, L2_1_a_PRO L2_3_a_ORG	
CPS.DS-15	・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	L1_1_a_DAT, L1_1_a_ORG, L3_1_a_SYS, L3_4_a_DAT	

３．１０．CPS.IP – 情報を保護するためのプロセス及び手順

（目的、範囲、役割、責任、経営コミットメント、組織間の調整を扱う）セキュリティポリシー、プロセス、手順を維持し、システムと資産の保護の管理に使用する。

表 19 CPS. IP カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.IP-1	・IoT 機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する	L2_1_a_ORG, L2_1_a_DAT, L2_1_b_PRO, L2_3_b_ORG	NIST Cybersecurity Framework Ver.1.1 PR.IP-1, PR.IP-3 CIS CSC 3, 9, 11 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05, BAI01.06, BAI06.01 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FMT, FDP, FIA IoT セキュリティガイドライン 要点 4, 要点 15
CPS.IP-2	・IoT 機器、サーバ等の導入後に、追加するソフトウェアを制限する	L1_1_a_SYS, L2_1_a_ORG, L2_1_c_SYS, L3_3_d_SYS, L3_1_a_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.IP-1 CIS CSC 3, 9, 11 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05, BAI01.06, BAI06.01 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入し、定めた各段階におけるセキュリティに関わる要求事項を明確化する	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG	NIST Cybersecurity Framework Ver.1.1 PR.IP-2 CIS CSC 18 COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03 ISA 62443-2-1:2009 4.3.4.3.3 ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1,

			A.14.2.5 NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8SI-12, SI-13, SI-14, SI-16, SI-17 ISO/IEC 15408-1/3 (CC v3.1 Release5 Part 1/3)
CPS.IP-4	・構成要素(IoT 機器、通信機器、回線等)に対し、定期的なシステムバックアップを実施し、テストしている	L1_1_a_SYS, L2_1_d_SYS, L3_3_c_SYS	NIST Cybersecurity Framework Ver.1.1 PR.IP-4 CIS CSC 10 COBIT 5 APO13.01, DSS01.01, DSS04.07 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FRU, FPT_TEE, FPT_TST
CPS.IP-5	・無停電電源装置、防火設備の確保、浸水からの保護等、自組織の IoT 機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する	L1_1_a_SYS, L2_3_b_SYS,	NIST Cybersecurity Framework Ver.1.1 PR.IP-5 COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FPT, FRU IoT セキュリティガイドライン 要点 6
CPS.IP-6	・IoT 機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規 IoT 機器、サーバ等を一意に識別するデータ ID(識別子)や重要情報(秘密鍵、電子証明書等)を削除又は読み取りできない状態にする	L2_3_b_DAT	NIST Cybersecurity Framework Ver.1.1 PR.DS-3, PR.IP-6 COBIT 5 BAI09.03, DSS05.06 ISA 62443-2-1:2009 4.3.4.4.4 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 NIST SP 800-53 Rev. 4 MP-6 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCS, FIA, FDP, FMT, FPT

			IoT セキュリティガイドライン 要点 6
CPS.IP-7	・セキュリティ事象への対応、内部及び外部からの攻撃に関する監視/測定/評価結果から教訓を導き出し、資産を保護するプロセスを改善している	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L2_1_a_COM	NIST Cybersecurity Framework Ver.1.1 PR.IP-7 COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
CPS.IP-8	・保護技術の有効性について、適切なパートナーとの間で情報を共有する	L2_1_a_COM	NIST Cybersecurity Framework Ver.1.1 PR.IP-8 COBIT 5 BAI08.04, DSS03.04 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4 ISO/IEC 15408-1 (CC v3.1 Release5 Part 1) IoT セキュリティガイドライン 要点 18
CPS.IP-9	・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項(例:アクセス権限の無効化、従業員に対する審査)を含めている	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO,	NIST Cybersecurity Framework Ver.1.1 PR.IP-11 CIS CSC 5, 16 COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FMT, FIA IoT セキュリティガイドライン 要点 4
CPS.IP-10	・脆弱性管理計画を作成し、計画に沿って構成要素の脆弱性を修正する	L1_1_a_SYS, L2_1_a_COM, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.IP-12 CIS CSC 4, 18, 20 COBIT 5 BAI03.10, DSS05.01, DSS05.02 ISO/IEC 27001:2013 A.12.6.1, A.1814.2.3, A.16.1.3, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 IoT セキュリティガイドライン 要点 17, 要点 21

３．１１．CPS.MA – 保守

産業用制御システムと情報システムの構成要素の保守と修理をポリシーと手順に従って実施する。

表 20 CPS.MA カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.MA-1	・IoT 機器、サーバ等のセキュリティ上重要なアップデート等を必要なタイミングで適切に実施する方法を検討し、適用する ・可能であれば、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えた IoT 機器を導入する	L1_1_a_SYS, L2_1_a_COM, L2_1_c_SYS, L3_3_d_SYS, L3_1_a_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.MA-1 COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.7 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6 IoT セキュリティガイドライン 要点 17
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	L1_1_a_SYS, L2_1_a_COM, L2_1_c_SYS, L3_3_d_SYS, L3_1_a_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.MA-2 CIS CSC 3, 5 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.43.3.6.8 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 4 MA-4 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FAU IoT セキュリティガイドライン 要点 17

３．１２．CPS.PT – 保護技術

関連するポリシー、手順、契約に基づいて、システムと資産のセキュリティとレジリエンス、セーフティを確保するための、技術的なソリューションを管理する。

表 21 CPS.PT カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記	L1_1_a_SYS, L2_1_b_ORG, L3_3_d_SYS,	NIST Cybersecurity Framework Ver.1.1 PR.PT-1 CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04,

	録の対象を決定、文書化し、そうした記録を実施して、レビューする	L3_1_a_SYS, L3_3_a_SYS	DSS05.07, MEA02.01 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FAU IoT セキュリティガイドライン 要点 9, 要点 13
CPS.PT-2	・IoT 機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的に閉塞する	L1_1_a_SYS, L1_1_c_SYS, L2_1_b_COM, L2_3_b_SYS, L3_1_a_SYS,	NIST Cybersecurity Framework Ver.1.1 PR.PT-2, PR.PT-3 CIS CSC 3, 8, 11, 13, 14 COBIT 5 DSS05.02, DSS05.05, DSS05.06, DSS06.06 ISA 62443-3-3:2013 SR 2.3 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.1.2, A.11.2.9 NIST SP 800-53 Rev. 4 AC-3, CM-7, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
CPS.PT-3	・ネットワークにつながることを踏まえた安全性を実装する IoT 機器を導入する	L2_2_a_ORG	NIST Cybersecurity Framework Ver.1.1 PR.PT-5 COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 ISA 62443-2-1:2009 4.3.2.5.2 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.17.1.2, A.17.2.1

			NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6 IoT セキュリティガイドライン 要点 10

３．１３．CPS.AE – 異常とイベント

異常な活動を検知し、事象がもたらす可能性のある影響を把握する。

表 22 CPS.AE カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理するプロシージャを確立し、実施する	L1_1_a_COM, L1_1_b_COM L1_1_c_COM L1_1_a_SYS, L1_3_a_ORG, L1_3_b_ORG, L2_1_b_ORG, L3_3_d_SYS, L3_1_a_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 DE.AE-1 CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01ISA 62443-2-1:2009 4.4.3.3 ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FAU, FDP
CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対策組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える	L1_2_a_ORG	NIST Cybersecurity Framework Ver.1.1 DE.AE-2 CIS CSC 3, 6, 13, 15 COBIT 5 DSS05.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.16.112.4.1, A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
CPS.AE-3	・セキュリティ事象の相関の分析、及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する	L1_2_a_SYS	NIST Cybersecurity Framework Ver.1.1 DE.AE-3, RS.AN-1 CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 COBIT 5 BAI08.02 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.16.1.7

			NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
CPS.AE-4	・関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定している	L1_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 DE.AE-4 CIS CSC 4, 6 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4 IoT セキュリティガイドライン 要点 5
CPS.AE-5	・セキュリティ事象の危険度の判定基準を定める	L1_2_a_PRO	NIST Cybersecurity Framework Ver.1.1 DE.AE-5 CIS CSC 6, 19 COBIT 5 APO12.06, DSS03.01 ISA 62443-2-1:2009 4.2.3.10 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8

３．１４．CPS.CM – セキュリティの継続的なモニタリング

セキュリティ事業を検知し、保護対策の有効性を検証するために、システムと資産をモニタリングする。

表 23 CPS.CM カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する	L1_1_a_SYS, L1_1_c_SYS, L1_2_a_SYS, L2_1_b_ORG, L3_3_d_SYS, L3_1_a_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 DE.CM-1 CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05, DSS05.07 ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FAU, FDP IoT セキュリティガイドライン 要点 8, 要点 13
CPS.CM-2	・IoT 機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定および記録、監視を実施する	L1_1_a_SYS, L2_3_b_SYS L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 DE.CM-2 COBIT 5 DSS01.04, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20

			ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FAU, FDP IoT セキュリティガイドライン 要点 8
CPS.CM-3	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行うIoT 機器を導入する ・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	L2_2_a_COM, L3_3_a_DAT, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 DE.CM-4, DE.CM-5 CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.12.6.2 NIST SP 800-53 Rev. 4 SI-3, SI-8 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FAU_SAA.2 IoT セキュリティガイドライン 要点 9
CPS.CM-4	・サイバー空間から受ける情報(データ)の完全性および真正性を動作前に確認する	L3_3_a_DAT, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 DE.CM-4, DE.CM-5 CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.12.6.2 NIST SP 800-53 Rev. 4 SI-3, SI-8 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FCS
CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする	L1_1_a_COM, L1_1_b_COM L1_1_c_COM L1_1_a_SYS, L1_3_a_ORG, L1_3_b_ORG, L3_3_d_SYS, L3_1_a_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 DE.CM-6 COBIT 5 APO07.06, APO10.05 ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4 IoT セキュリティガイドライン 要点 8, 要点 9, 要点 13
CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)および他の組織、ヒト、モ	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM L1_1_c_COM	NIST Cybersecurity Framework Ver.1.1 DE.CM-3, DE.CM-7 CIS CSC 1, 2, 3, 5, 7, 9, 12, 13, 14, 15, 16 COBIT 5 DSS05.02, DSS05.05, DSS05.07

	ノ、システムとのデータの送受信状況について、継続的に把握する	L1_3_a_ORG, L1_3_b_ORG, L2_1_a_ORG, L2_3_b_ORG, L2_1_c_ORG, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS	ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, PE-3, PE-6, PE-20, SI-4 IoT セキュリティガイドライン 要点 13
CPS.CM-7	・自組織の管理している IoT 機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する	L1_1_a_SYS, L3_3_d_SYS, L3_1_a_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 DE.CM-8 CIS CSC 4, 20 COBIT 5 BAI03.10, DSS05.01 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5 IoT セキュリティガイドライン 要点 8, 要点 21

３．１５．CPS.DP – 検知プロセス

異常なセキュリティ事象を正確に検知するための検知プロセスおよび手順を維持し、テストする。

表 24 CPS.DP カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.DP-1	・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が担う役割と負う責任を明確にする	L1_2_a_ORG	NIST Cybersecurity Framework Ver.1.1 DE.DP-1 CIS CSC 19 COBIT 5 APO01.02, DSS05.01, DSS06.03 ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
CPS.DP-2	・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する	L1_2_a_ORG, L1_3_c_ORG	NIST Cybersecurity Framework Ver.1.1 DE.DP-2 COBIT 5 DSS06.01, MEA03.03, MEA03.04 ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, PM-14SA-18, SI-4, PM-14
CPS.DP-3	監視業務として、セキュリティ事象を検知する機能が意図したとおり	L1_2_a_ORG	NIST Cybersecurity Framework Ver.1.1 DE.DP-3

	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		COBIT 5 APO13.02, DSS05.02 ISA 62443-2-1:2009 4.4.3.2 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.14.2.8 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FPT_TEE IoT セキュリティガイドライン 要点 9
CPS.DP-4	・セキュリティ事象の検知プロセスを継続的に改善する	L1_2_a_ORG	NIST Cybersecurity Framework Ver.1.1 DE.DP-5 COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

３．１６．CPS.RP－対応計画

検知したセキュリティインシデントに対応し、適切に自組織の事業を継続しつつ、影響を受ける資産やシステムを復元できるよう、対応・復旧のプロセスおよび手順を実施し、維持する。

表 25 CPS.RP カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.RP-1	・セキュリティインシデント発生時の対応の内容や優先順位、対策範囲を明確にするため、セキュリティ運用プロセスを定め、運用する ・セキュリティインシデント(例：アクセス元/先が不正なエンティティである、送受信情報が許容範囲外である)を検知した後の IoT 機器、サーバ等による振る舞いをあらかじめ定義し、実装する	L1_1_a_SYS, L1_2_a_PEO, L2_2_a_PRO, L3_3_d_SYS, L3_1_a_SYS, L3_3_a_SYS	NIST Cybersecurity Framework Ver.1.1 PR.IP-9, DE.DP-4, RS.RP-1, RS.CO-2, RS.CO-3 CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8 ISO/IEC 15408-2 (CC v3.1 Release5 Part 2) FTA (左記の「あらかじめ定義し、実装する」に対して) IoT セキュリティガイドライン 要点 5
CPS.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する	L1_3_a_PEO, L1_3_a_PRO, L1_3_b_PEO, L1_3_b_PRO	NIST Cybersecurity Framework Ver.1.1 PR.IP-9, RS.CO-4, RS.CO-5 CIS CSC 19 COBIT 5 APO12.06, DSS03.04, DSS04.03 ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1, 4.3.4.5.5

			ISO/IEC 27001:2013 Clause 7.4, A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-4, IR-7, IR-8, IR-9, PE-17
CPS.RP-3	・自然災害時における対応方針および対応手順を定めている事業継続計画又はコンティンジェンシープランの中にセキュリティインシデントを位置づける	L1_2_a_PRO	NIST Cybersecurity Framework Ver.1.1 ID.BE-5, RC.RP-1 CIS CSC 10 COBIT 5 APO12.06, BAI03.02, DSS02.05, DSS03.04, DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.16.1.5, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, CP-10, IR-4, IR-8, SA-13, SA-14
CPS.RP-4	・セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ(製品)に対して適切な対応を行う	L1_3_a_COM	

３．１７．CPS.CO – 伝達

例えば法執行機関のような組織からの支援を得られるよう、内外の利害関係者(例えば、取引先、JPCERT/CC、他組織の CSIRT、ベンダー)との間で対応・復旧活動を調整する。

表 26 CPS.CO カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.CO-1	・セキュリティインシデント発生後の情報公表時のルールを策定し、運用する	L1_2_a_PRO	NIST Cybersecurity Framework Ver.1.1 RC.CO-1 COBIT 5 EDM03.02 ISO/IEC 27001:2013 A.6.1.4, Clause 7.4 IoT セキュリティガイドライン 要点 18
CPS.CO-2	・事業継続計画又はコンティンジェンシープランの中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける	L1_2_a_PRO	NIST Cybersecurity Framework Ver.1.1 RC.CO-2 COBIT 5 MEA03.02 ISO/IEC 27001:2013 Clause 7.4

CPS.CO-3	・復旧活動について内部および外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又はコンティンジェンシープランの中に位置づける	L1_2_a_PRO	NIST Cybersecurity Framework Ver.1.1 RC.CO-3 COBIT 5 APO12.06 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4

３．１８．CPS.AN – 分析

効率的な対応を確実にし、復旧活動を支援するために、分析を実施する。

表 27 CPS.AN カテゴリーの対策要件

対策要件 ID	対策要件	対応する脆弱性	関連標準等
CPS.AN-1	・セキュリティインシデントの全容と、推測される攻撃者の意図から、組織全体への影響を把握する	L1_2_a_PRO	NIST Cybersecurity Framework Ver.1.1 RS.AN-2 COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4
CPS.AN-2	・セキュリティインシデント発生後に、デジタルフォレンジックを実施する	L1_2_a_PRO	NIST Cybersecurity Framework Ver.1.1 RS.AN-3 COBIT 5 APO12.06, DSS03.02, DSS05.07 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4
CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する	L1_2_a_PRO	NIST Cybersecurity Framework Ver.1.1 RS.AN-4 CIS CSC 19 COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8

３．１９．CPS.MI – 低減

セキュリティ事象の拡大を防ぎ、その影響を緩和し、セキュリティインシデントを解消するための活動を実施する。

表 28 CPS.MI カテゴリーの対策要件

対策要件ID	対策要件	対応する脆弱性	関連標準等
CPS.MI-1	・セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う	L1_2_a_PRO	NIST Cybersecurity Framework Ver.1.1 RS.MI-1, RS.MI-2 CIS CSC 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4 IoT セキュリティガイドライン 要点 9

３．２０．CPS.IM – 改善

現在と過去の意思決定／対応活動から学んだ教訓を取り入れることで、自組織の対応・復旧活動を改善する。

表 29 CPS.IM カテゴリーの対策要件

対策要件ID	対策要件	対応する脆弱性	関連標準等
CPS.IM-1	・セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する	L1_2_a_ORG	NIST Cybersecurity Framework Ver.1.1 RS.IM-1, RS.IM-2 COBIT 5 BAI01.13, DSS04.08 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 IoT セキュリティガイドライン 要点 7
CPS.IM-2	・セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又はコンティンジェンシープランを継続的に改善する	L1_2_a_ORG	NIST Cybersecurity Framework Ver.1.1 RC.IM-1, RC.IM-2 COBIT 5 APO12.06, BAI05.07, DSS04.08 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8