サイバー・フィジカル・セキュリティ対策
フレームワーク

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

Version 1.0

経済産業省　商務情報政策局

サイバーセキュリティ課

平成 31 年 4 月 18 日

目次

エグゼクティブサマリー I
はじめに 1
1．「Society5.0」、「Connected Industries」が実現する社会 1
2．サイバー攻撃の脅威の増大 3
3．フレームワークを策定する目的と適用範囲 4
4．フレームワークの想定読者 5
5．フレームワークの全体構成 6
6．フレームワークに期待される効果と特徴 6
7．フレームワークの使い方 8
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 10
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 10
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（trustworthiness）の基点を設定するためのモデル －三層構造と６つの構成要素－ 11
2．1．三層構造アプローチの意義 14
2．2．６つの構成要素 16
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 19
4．フレームワークを活用した信頼性の確保の考え方 21
5．結び 23
第Ⅱ部　ポリシー：リスク源の洗い出しと対策要件の特定 25
1．三層構造モデルと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 25
1．1．分析対象の明確化(三層構造モデルへの落とし込み) 28
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 36
1．3．リスク分析の実施 41
1．4．リスク対応の実施 42
2．リスク源と対策要件の対応関係 48
第Ⅲ部　メソッド：セキュリティ対策要件と対策例集 50
1．対策要件及び対策例集を活用したリスク対応 50
2．対策例集の見方 51
3．対策要件 54
3．1．CPS.AM – 資産管理 56

３．２．CPS.BE – ビジネス環境 58
３．３．CPS.GV – ガバナンス 59
３．４．CPS.RA – リスク評価 61
３．５．CPS.RM – リスク管理戦略 63
３．６．CPS.SC – サプライチェーンリスク管理 64
３．７．CPS.AC – アイデンティティ管理、認証及びアクセス制御 68
３．８．CPS.AT – 意識向上及びトレーニング 72
３．９．CPS.DS – データセキュリティ 74
３．１０．CPS.IP – 情報を保護するためのプロセス及び手順 78
３．１１．CPS.MA – 保守 82
３．１２．CPS.PT – 保護技術 83
３．１３．CPS.AE – 異変とイベント 85
３．１４．CPS.CM – セキュリティの継続的なモニタリング 87
３．１５．CPS.DP – 検知プロセス 90
３．１６．CPS.RP – 対応計画 91
３．１７．CPS.CO – 伝達 93
３．１８．CPS.AN – 分析 94
３．１９．CPS.MI – 低減 95
３．２０．CPS.IM – 改善 96

添付 A　ユースケース
添付 B　リスク源と対策要件の対応関係
添付 C　対策要件に応じたセキュリティ対策例
添付 D　海外の主要規格との対応関係
添付 E　用語集

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、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、攻撃側が攻撃起点を得る機会が増え、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、ビジネス活動のレジリエンスまで考慮に入れた上で、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む必要がある。

○ 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（trustworthiness）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る必要があることから、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。

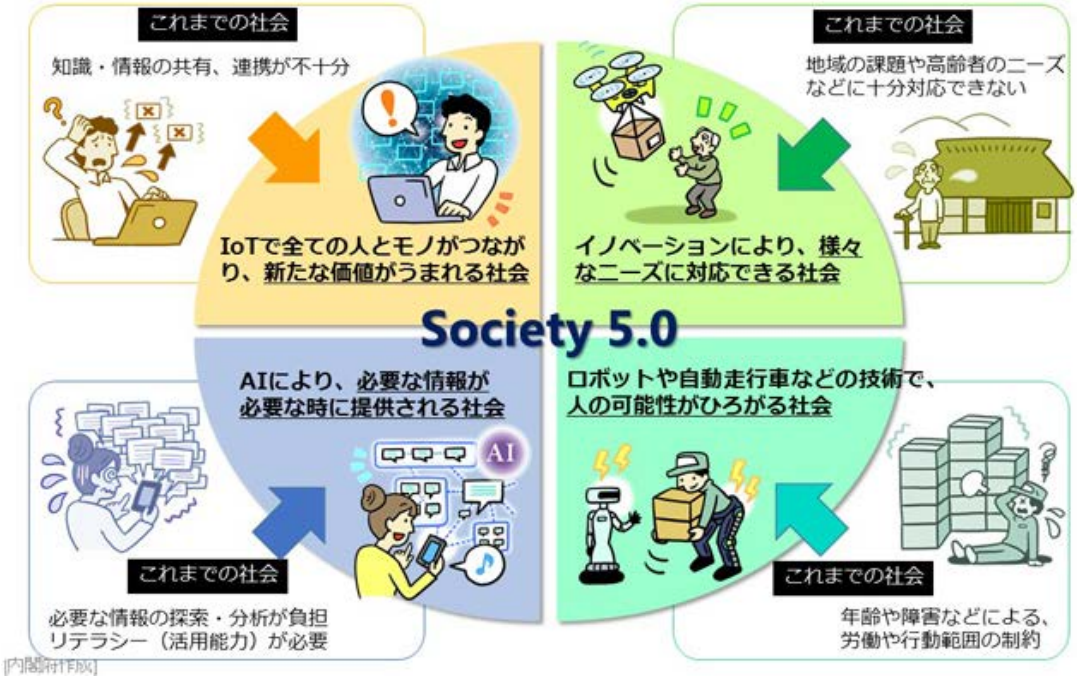


図 i-1 「Society 5.0」で実現する社会のイメージ[1]

[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）でも、新たな価値の創出に必要な知識や情報は十分に共有されない場合が多く、新たな価値の創出が困難であった。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。

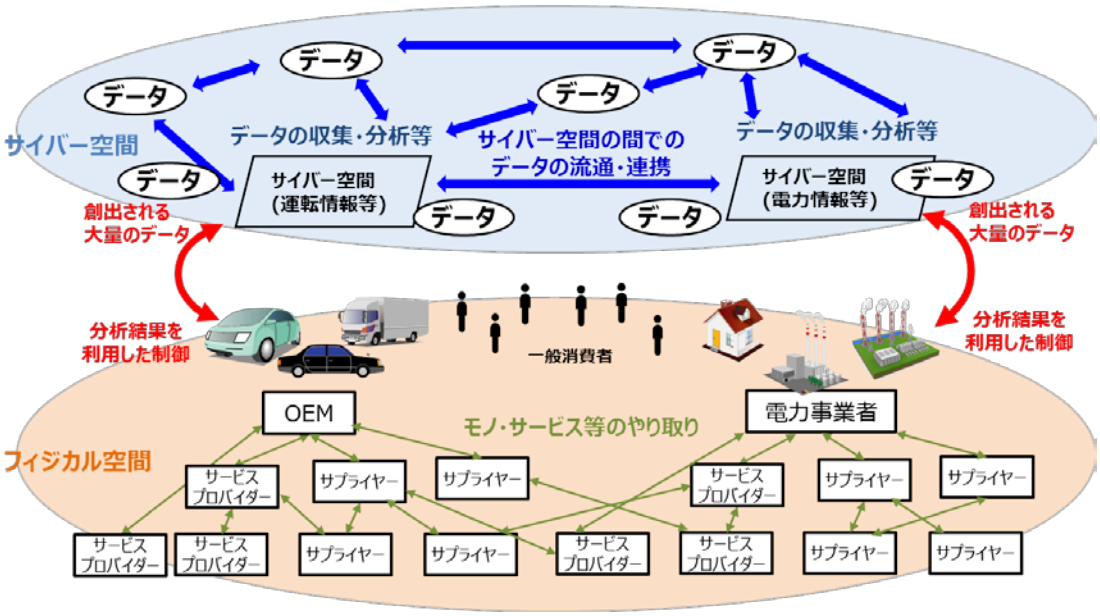


図 i-2 「Society5.0」社会におけるモノ・データ等のつながりのイメージ

■ 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る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内容自体も、開始時点で設定された“必要性”の変化に対応した変更や、より有用なデータが得られた場合にその要素を新たな活動の中に組み込み変化していく。

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、従来の上流から下流へとつながる定型的・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（以下、「バリュークリエイションプロセス」とする。）』と定義する。

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、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（trustworthiness）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の高度な融合に伴い発生する新たな処理が、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、情報のデジタル化機能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している。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）を行うことが追加され、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

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

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、それぞれの企業等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。

また、「ネットワーク化されず、インターネットにも接続されない」システムと認識していても、システムで使用していた独自仕様の電子機器や通信プロトコルが汎用化・標準化されることに伴い、機器間の連携がシームレスになり利便性向上につながる一方で、小さなインシデントの影響が容易にシステム全体へ波及する可能性が高まり、フィジカル空間を通じたサイバー攻撃を受けるなどの懸念も増大しているため、所有する電子機器及びシステムが本フレームワークの適用範囲に含まれ得るという認識に立ち、必要なセキュリティ対策を講じる必要がある。

読者は、本フレームワークを活用し、自らが所属する企業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重要である。

4．フレームワークの想定読者

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されることを想定しており、例えば、以下に示すような者を読者として想定している。

- CISO[3]（最高情報セキュリティ責任者）
- サプライチェーン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）
- バリュークリエイションプロセスに関わる企業・団体等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

[3] Chief Information Security Officer

- 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

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三部構成とした。

(1) 第Ⅰ部では、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。いわば、本フレームワークのコンセプトを説明する部である。

(2) 第Ⅱ部では、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。各企業・組織等が対策を講じるべき対策要件（ポリシー）を明らかにする部である。

(3) 第Ⅲ部では、第Ⅱ部で示した対策要件を対策の種類に応じて整理し、更に添付の形で、セキュリティの相対的な強度を踏まえて分類した対策例を提示する。各企業・組織等が実際に講じるべき具体的なメソッドを示す部となる。

このような三部構成を採用することで、必要な見直しを適時適切に行うことが可能となる。例えば、セキュリティ対策技術の進展により、より有効な対策事例を取り上げるべき際には第Ⅲ部を改訂することで対応し、また、サイバー空間とフィジカル空間の一体化が更に進展して新たなリスク源を捉える必要がある場合には、第Ⅱ部を改訂することで対応することが可能となる。

本フレームワークは、必要な見直しを迅速かつ柔軟に行うことも視野に入れた構成を採用しており、引き続き、状況の変化に応じて進化していくものであることを明確にしている。

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検討を進めた。

(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の実現に貢献する

- 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 などの国際標準や NIST Cybersecurity Framework など国外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。この対比表を活用することで、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、参照される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る必要がある。

したがって、各業界や各企業において、以下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企業等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企業等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得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) 企業等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対策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 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対策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、企業等の取組の助けになることを期待する。

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

⑶ 企業等、業界等における信頼のチェーンの構築への活用

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、一つ一つのバリュークリエイション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、信頼のチェーンの構築に活用することができる。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（第Ⅰ部 4.⑵で詳述）の作成
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）も上流から下流へとつながる従来の定型的・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いた。情報処理を委託する場合も、ISMSなどの認証を取得しているなどセキュリティ対策をしっかりと行っている企業かどうかを重要視していた。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ていたことになる。

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、従来はフィジカル空間に留まっていた環境情報（例：温度、湿度）や生体情報（例：体温、心拍数）といった様々な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に限らない。つまり、バリュークリエイション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、組織の信頼という観点だけではなく、他の観点から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、バリュークリエイション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。

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（trustworthiness）の基点を設定するためのモデル －三層構造と６つの構成要素－

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、フィジカル空間の情報が IoT によってデジタル化され、データとし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 によってフィジカル空間にフィードバックされることで新た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、対応方針を示すため、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－　企業間のつながり
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

また、この三層構造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対応していくためには、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方法では、その構成が動的に変化するバリュークリエイションプロセスで本質的に防御しなければならない対象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、動的な構成の変化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。それぞれの定義については 2.2 で詳述する。

－ソシキ
－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の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対策要件及び具体的な対策例を示すのが、本フレームワークの基本構成である。

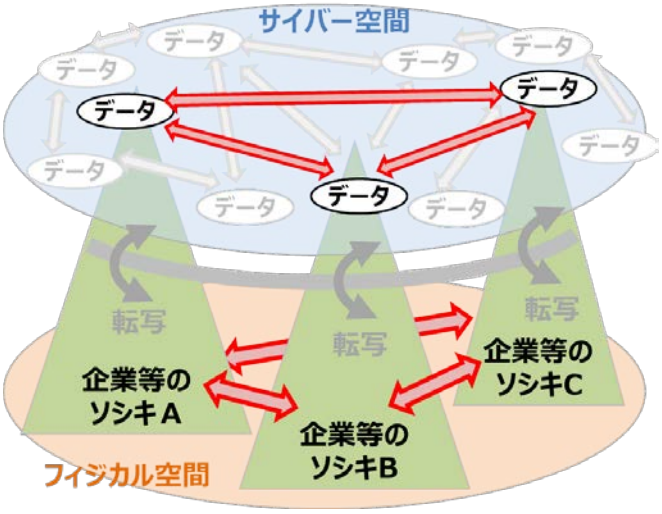
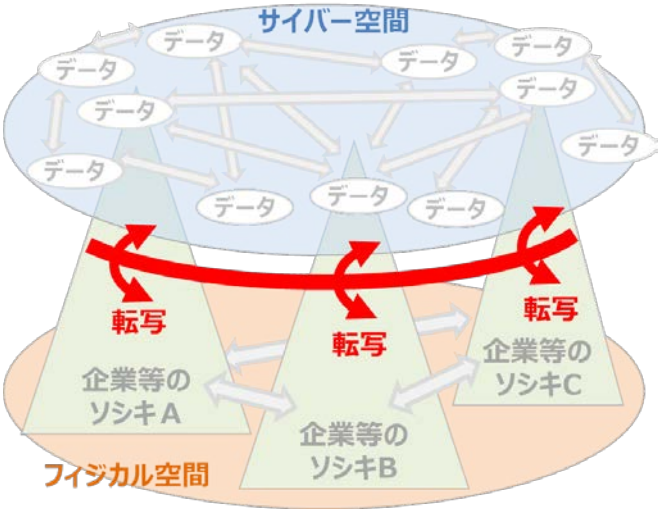
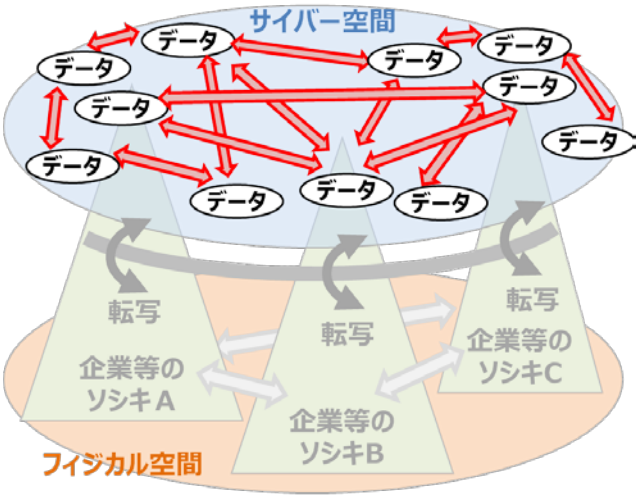
三層構造	概念図
企業間のつながり 【第1層】	
フィジカル空間とサイバー空間のつながり 【第 2 層】	
サイバー空間における つながり 【第 3 層】	

図 1.2-1 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、三層構造モデルを利用し信頼性を確保するためのアプローチである。各層でそれぞれ確保する信頼性について、以下で説明する。

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、温度、湿度や距離などの物理事象をデータに転写するセンサやデータを基に動作するアクチュエータなどから構成される、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/IEC 27036 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ー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・保管時における改ざんや流出のようなインシデントの発生は、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においては、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（三層構造モデル）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。

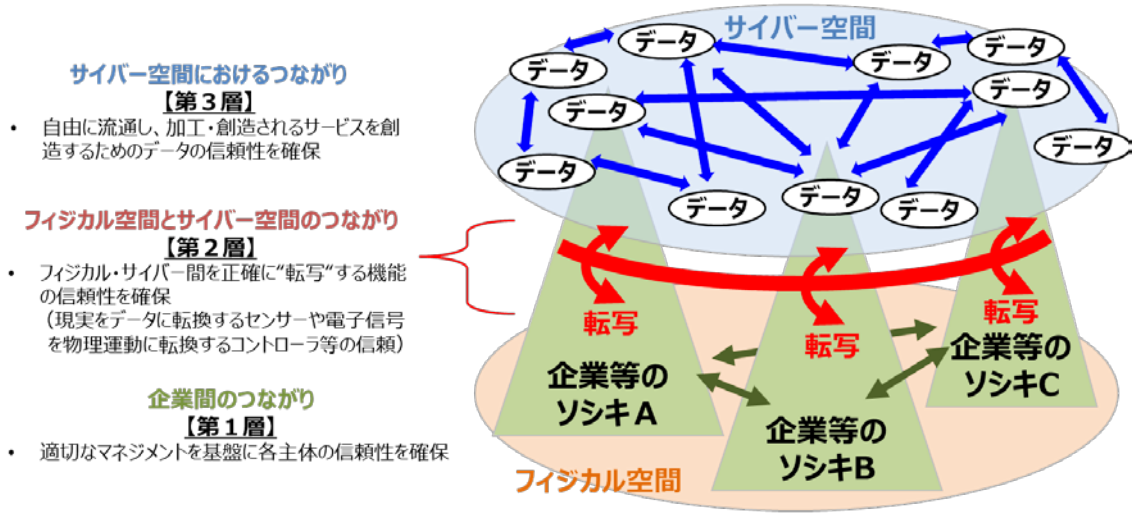


図 1.2-2 三層構造モデルと各層における信頼性

２．２．６つの構成要素

三層構造モデルを通じて、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、ビジネス資産を固定的に捉えることが難しく、一定の抽象化を行ったうえで構成要素を捉える必要がある。

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 1.2-1 に示す６つの構成要素を整理した。

表 1.2-1 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
ソシキ	バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	ソシキに属する人、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の一連の活動の手続き
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設定した。図 1.2-3 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）から付加価値を生み出す。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。それぞれの要素は、他の企業（組織）からの出力で生み出されるなど、６つの構成要素はそれぞれ複雑に関係していく。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、製造業のバリュークリエイションプロセスを例に、６つの構成要素と三層構造の関係を図 1.2-4 に示す。左側の企業「ソシキ」が、「モノ」を入力し、加工処理して「モノ」を出力する。左側の企業「ソシキ」から出力された「モノ」

は、右側の企業「ソシキ」が入力し、加工処理を加えて「モノ」を出力する。それぞれの企業「ソシキ」には、加工機械、センサ、アクチュエータ等の「モノ」、これらを制御するシステムや、他組織とデータを交換するシステム等の「システム」、システムを監視、制御する「ヒト」、各システムの活動手順を定める手順等の「プロシージャ」、システム間を流れる各種データ「データ」が存在する。

これらの構成要素は、各組織がマネジメントする構成要素であり、企業ごとに第 1 層の構成要素と捉える。一方で、第 1 層の構成要素の中で、サイバー空間とフィジカル空間の間を転写するセンサ、アクチュエータ、これらを制御するシステムや、それらに関連するプロシージャ、データは、第 2 層の構成要素としても捉える。2 つの組織間では、インターネット等を経由して各種のデータを交換しているが、これらに関連するシステム、プロシージャ、データ等は、サイバー空間におけるつながりである第 3 層の中で捉えられる。

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、「ソシキ」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、「ソシキ」を構成している要素である「ヒト」は「ソシキ」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。

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。

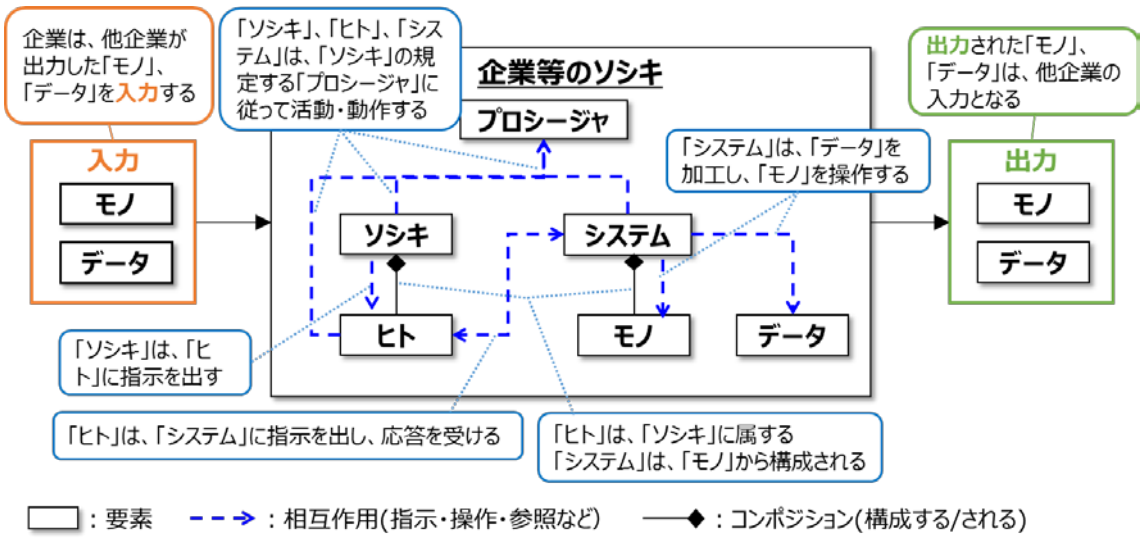


図 1.2-3　6 つの構成要素の関係

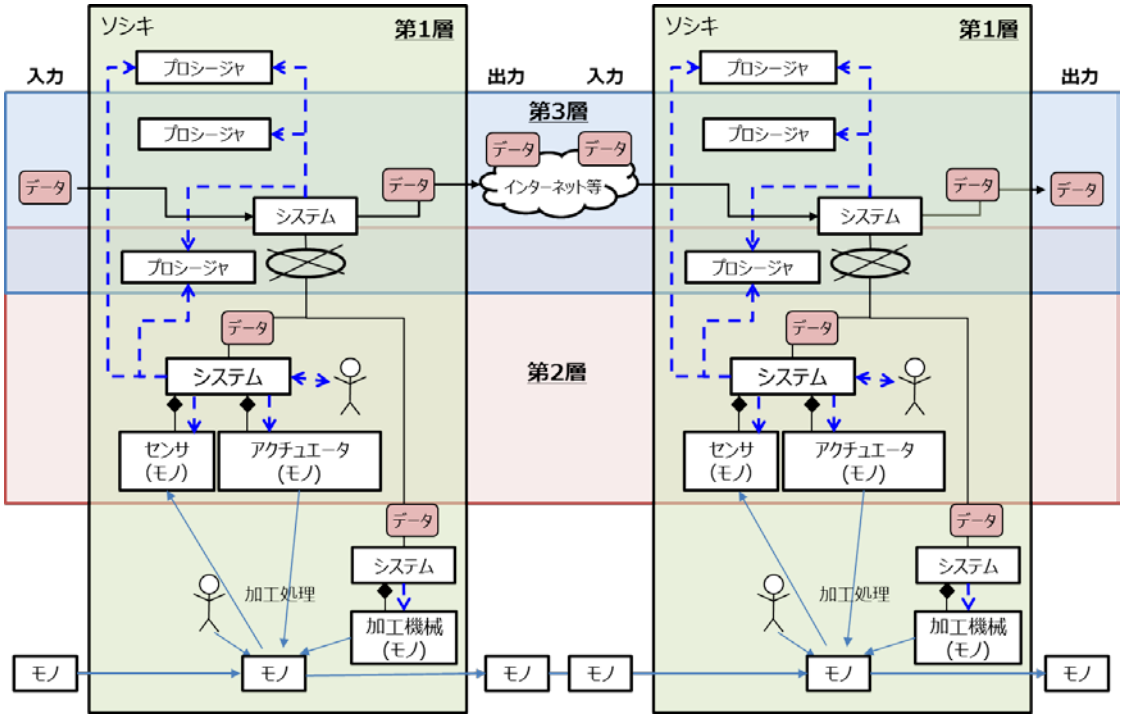


図 1.2-4 三層構造における 6 つの構成要素の関係

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

三層構造モデルと 6 つの構成要素に基づいて、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）を整理していくが、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の変化により、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。

三層構造モデルにおける第 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によるセキュリティ対策の取組（以下、「マルチステークホルダーアプローチ」とする。）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、図 1.3-1 に示すように、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。

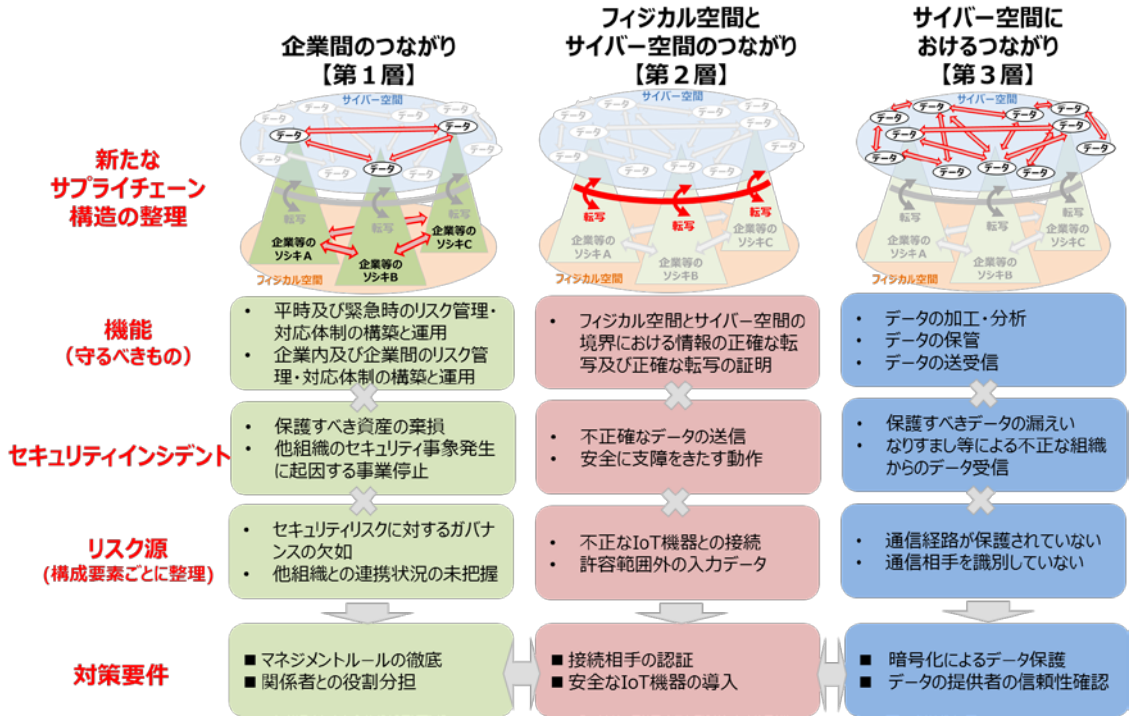


図 1.3-1 各層におけるセキュリティ対策の概要

４．フレームワークを活用した信頼性の確保の考え方

三層構造モデルに基づいて、各層の信頼性の基点となる構成要素のセキュリティを各主体がそれぞれ確保することによって、バリュークリエイションプロセス全体のセキュリティ確保が実現される。その実現には、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できること（信頼の創出）、それを確認した者以外の者による照会ができること （信頼の証明）に加えて、信頼の創出と証明を繰り返すことで連鎖的に構築される信頼関係のつながり（信頼のチェーン）の構築、維持が必要である（図 1.4-2 参照）。信頼の創出、信頼の証明、信頼のチェーンの構築と維持の実現に求められる事項の例を以下に示す。

(1) 信頼の創出

例）

- 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

例)

・ 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

例)

・ 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

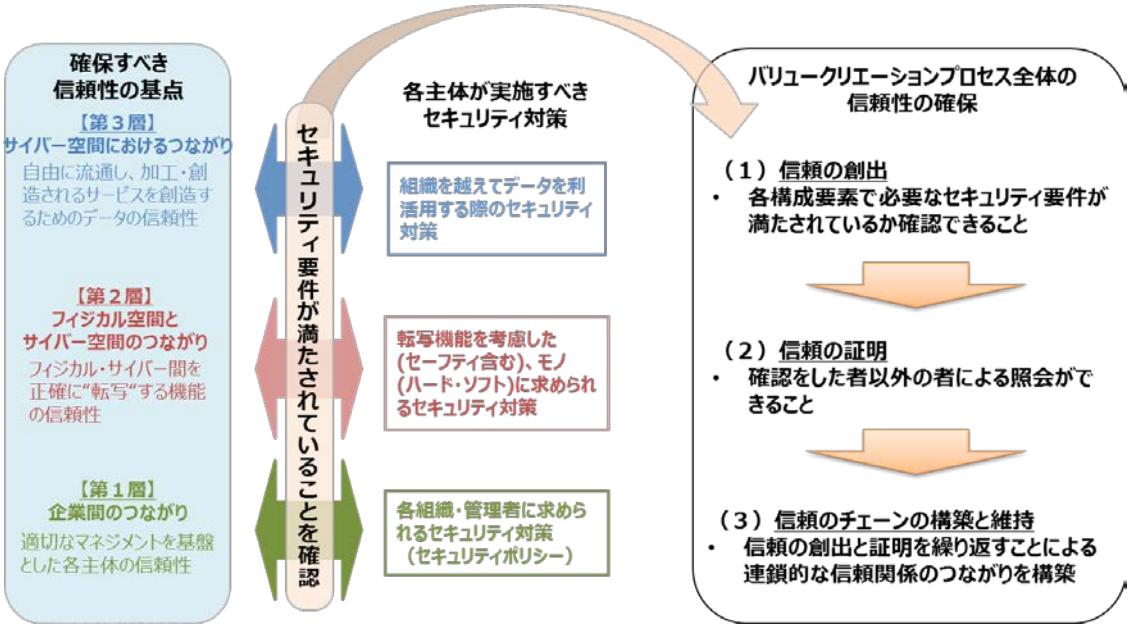


図 1.4-1 信頼性の基点と信頼性の確保の考え方

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、個々の構

成要素の信頼性の確認だけではなく、その関係性まで追跡して確認できる信頼のチェーンを構築してトレーサビリティも確保することで、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必要がある。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。

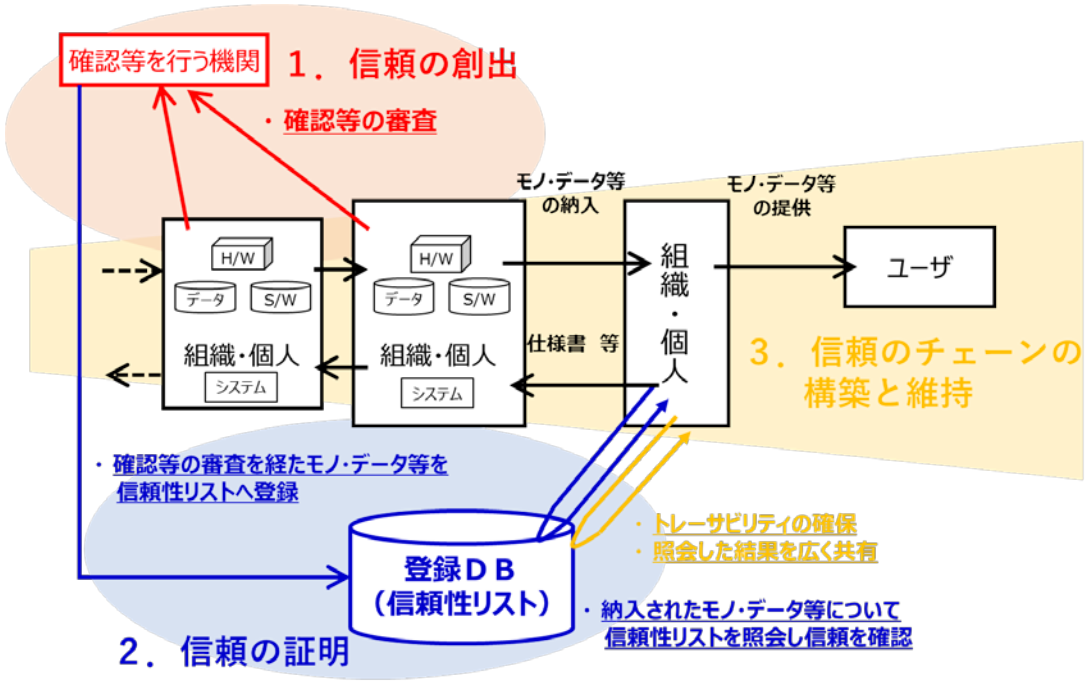


図 1.4-2 信頼の創出、信頼の証明、信頼のチェーンの構築と維持の関係のイメージ

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る必要がある。

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した三層構造モデルに基づいて、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. 三層構造モデルと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、適用範囲、状況、基準、リスクアセスメント、リスク対応への活用が可能である。

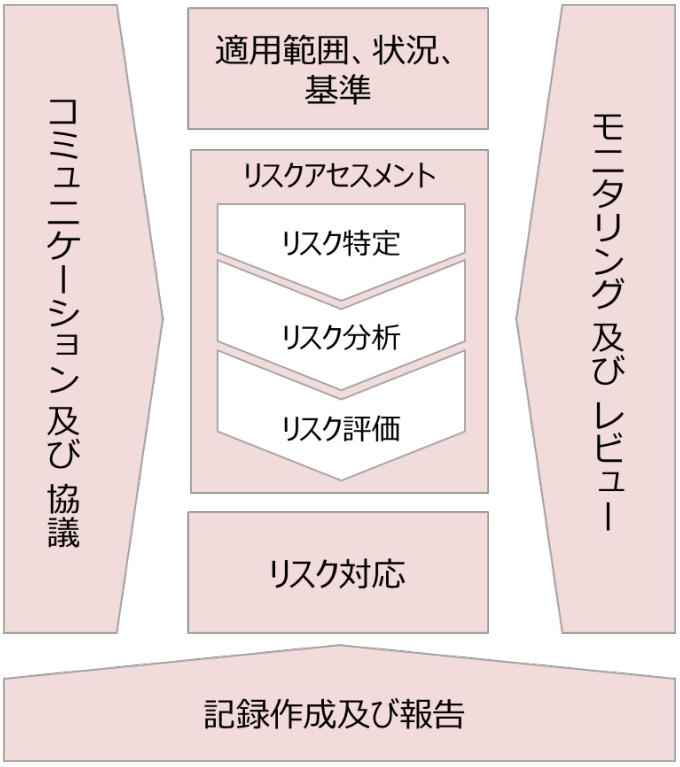


図 2.1-1 リスクマネジメントの一般的なプロセス [4]

セキュリティリスクマネジメントにおける具体的な適用範囲、状況、基準、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。

[4] JIS Q 31000:2019 リスクマネジメント−原則及び指針 を基に作成

■ 適用範囲、状況、基準

① 分析対象の明確化（１．１）

三層構造モデルに基づき、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。

■ リスクアセスメント［リスク特定/リスク分析/リスク評価］

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。

■ リスク対応

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。

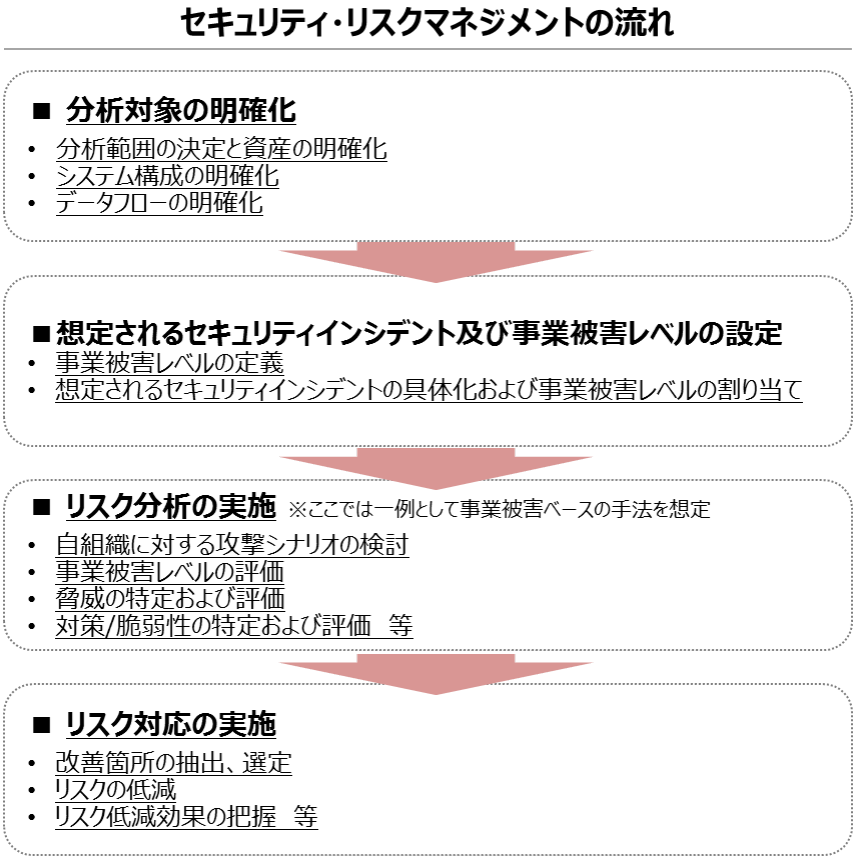


図 2.1-2 リスクマネジメントの流れ [5]

[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

なお、セキュリティリスクマネジメントを実施する際、図 2.1-3 に示すセキュリティリスクの概念を理解しておく必要がある。ここでリスクは「目的に対する不確かさの影響」として定義しており、セキュリティリスクとは目的に対するセキュリティに係る不確かさの影響を意味する。脅威や脆弱性のようなリスク源が原因となってセキュリティインシデントが発生し、セキュリティリスクは顕在化する。そのため、セキュリティリスクを適切かつ効率的に縮減するためには、回避すべきセキュリティインシデントや、その発生につながるリスク源（例：脅威、脆弱性）を適切に分析し、その結果に応じて適宜対応する必要がある。

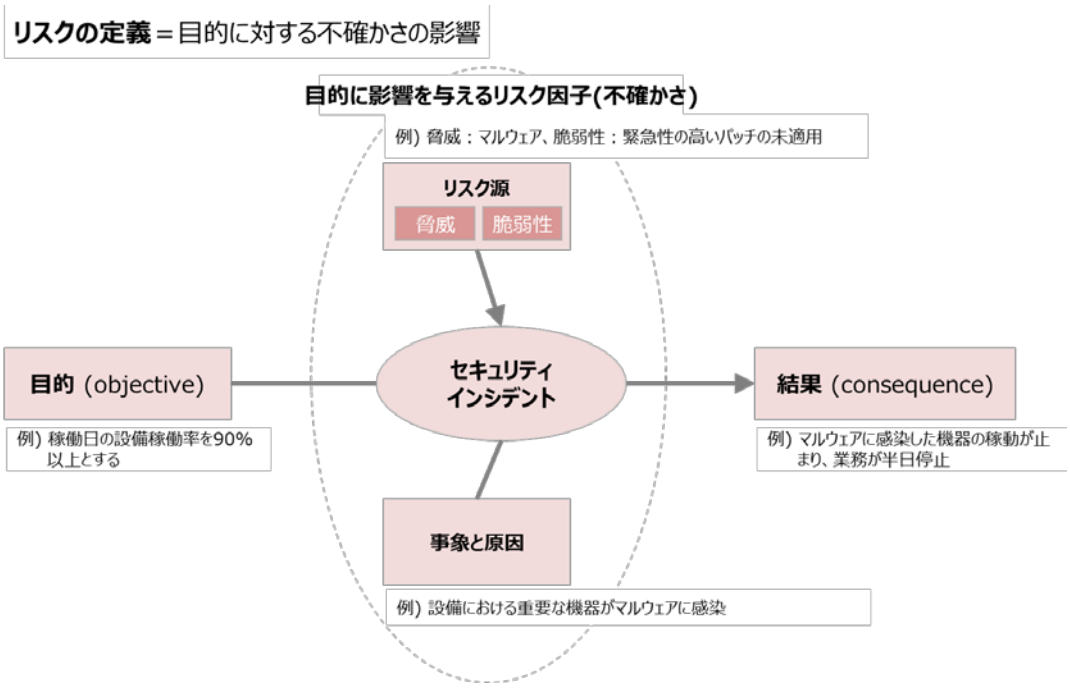


図 2.1-3 セキュリティリスクの概念 [6]

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、分析対象の明確化からリスク対応の実施に至る流れの中で以下に示す 4 つの観点を考慮すべきである。なお、これらの観点については、1.1.(2)「分析対象の明確化における留意点」で詳述する。

[6] 永宮直史氏編著「ISO/IEC27017　クラウドサービスのための情報セキュリティ管理策の実践の規範解説と活用ガイド」P.251 図 5.6 を参考にしつつ、本フレームワークの用語等に合うよう修正

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、各観点の捉え方も含め、セキュリティリスクマネジ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) 三層構造モデル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。「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）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、企業等が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 部にて提示した三層構造モデルに基づいて分析対象を明確にする方法を提供する。企業等は、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 [7]。

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 2.1-1 に示すような各層の特性及びその果たすべき機能・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分類を行う。

[7] 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及び３．３を参照することが望ましい。

企業等が管理するモノはすべて第１層に含まれる。その中で、第２層、第３層の機能を備えるモノについては、その層に含まれるモノとして分析する必要がある。また、第 2 層の機能と第 3 層の機能を併せ持つモノについては、両方の層での分析が必要で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る「場所」や、ヒトに対して特定のプロシージャを要求する「場所」も、リスクアセスメントにおいて留意する必要がある。

なお、クラウドサービスを利用する場合、サービスプロバイダからネットワークを介して提供されるリソースは第３層に位置するが、サービスの利用形態（例: SaaS/PaaS/IaaS[8]）に留意しつつ必要な範囲で第 1 層の機器としてもリスク分析を行う。

表 2.1-1 三層構造モデル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	分析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

[8] 記載している順に、Software as a Service、Platform as a Service、Infrastructure as a Service の略称を表している。

<table>
<tr><td colspan="4">第2層 － フィジカル空間とサイバー空間のつながり</td></tr>
<tr><td>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</td><td>・ フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、サイバー空間へ送る機能
・ サイバー空間から受け取ったデータに基づいて、一定のルールに基づいて、モノを制御したり、データを可視化したりする機能

【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</td><td>・ 転写機能に関わるソシキ・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</td><td>・ 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、コンピュータ（入力機器として）、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機能に関わる部品 等</td></tr>
<tr><td colspan="4">第3層 － サイバー空間におけるつながり</td></tr>
<tr><td>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。</td><td>・ 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</td><td>・ 特に、組織を越えてやりとりするデータを扱うソシキ・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</td><td>・ 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</td></tr>
</table>

例えば、コンピュータ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。

三層構造モデル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 2.1-4 に第１層の分析対象及びその具体的イメージを示す。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。

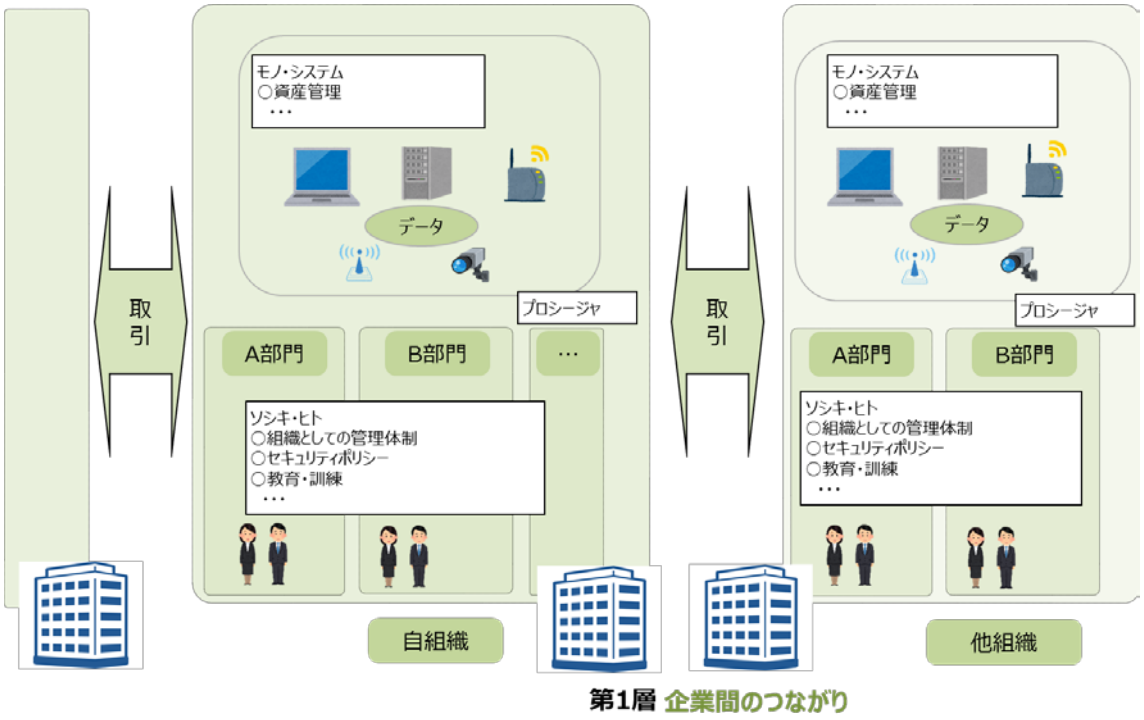


図 2.1-4　第１層の分析対象及び分析対象の具体的イメージ

次に、図 2.1-5 に第 2 層及び第 3 層の機能・役割及び分析対象の具体的イメージを示した上で、図 2.1-6 に第１層の分析対象と第 2 層、第 3 層の機能・役割とを関連付けたバリュークリエイションプロセスの分析対象の具体的イメージを示す。

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 2.1-5 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、添付 A に図 2.1-6 に示す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、企業等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必要がある。

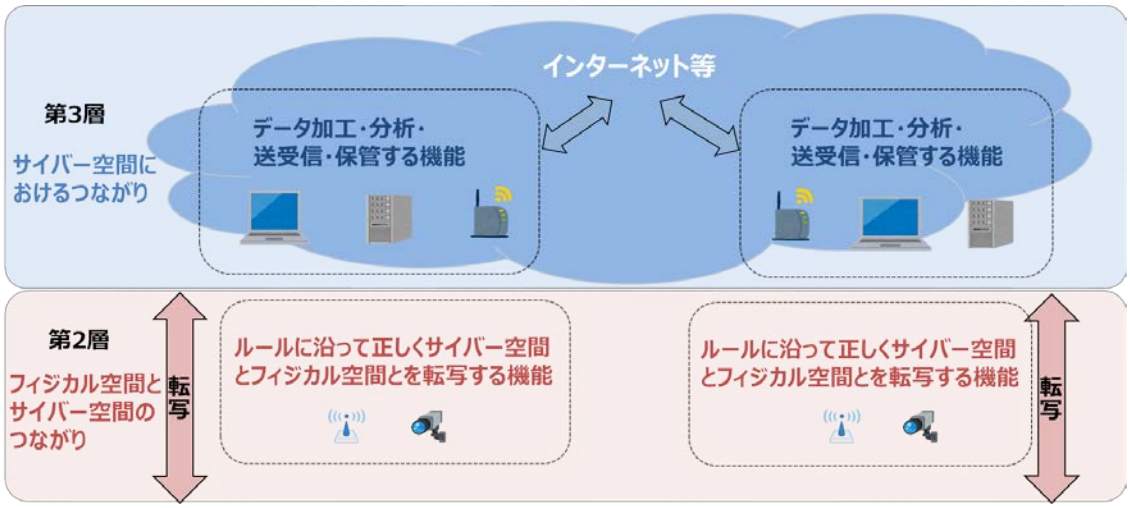


図 2.1-5 第 2 層及び第 3 層の機能・役割及び分析対象の具体的イメージ

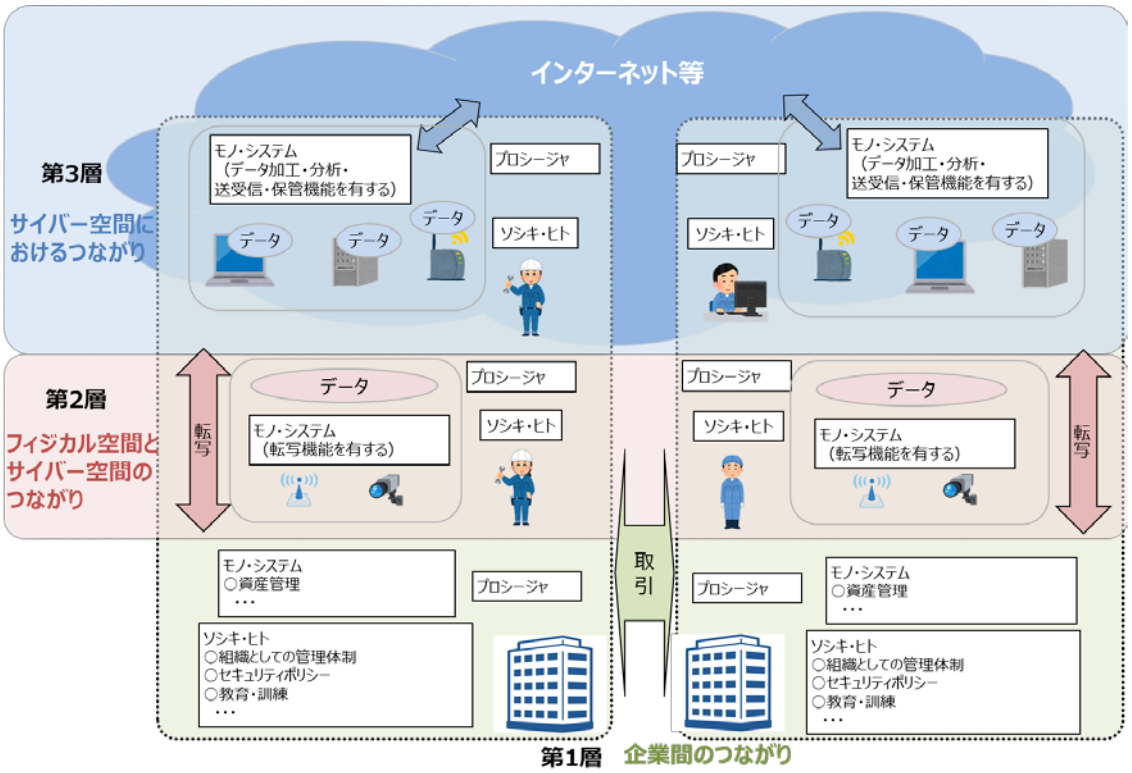


図 2.1-6 三層構造モデルと 6 つの構成要素を活用した分析対象の具体的イメージ

(2) 分析対象の明確化における留意点

三層構造モデル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の確保という目的を達成するために、以下の観点に留意しながら分析作業を進めることが重要である。

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

- 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、マルチステークホルダーアプローチが必要となる。
- 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「ソシキ」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重要である。

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

- サイバー空間とフィジカル空間が融合する境界では、フィジカル空間のデータを一定のルールに従って正しくサイバー空間のデータに転写できる必要がある。その際、例えば、センサの機能に対するサイバー攻撃の結果、フィジカル空間のデータが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、フィジカル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（例：センサ）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必要がある。
- 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、フィジカル空間のモノが制御され得る。その結果として、図 2.1-7 及び図 2.1-8 に示すように、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得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重要である。

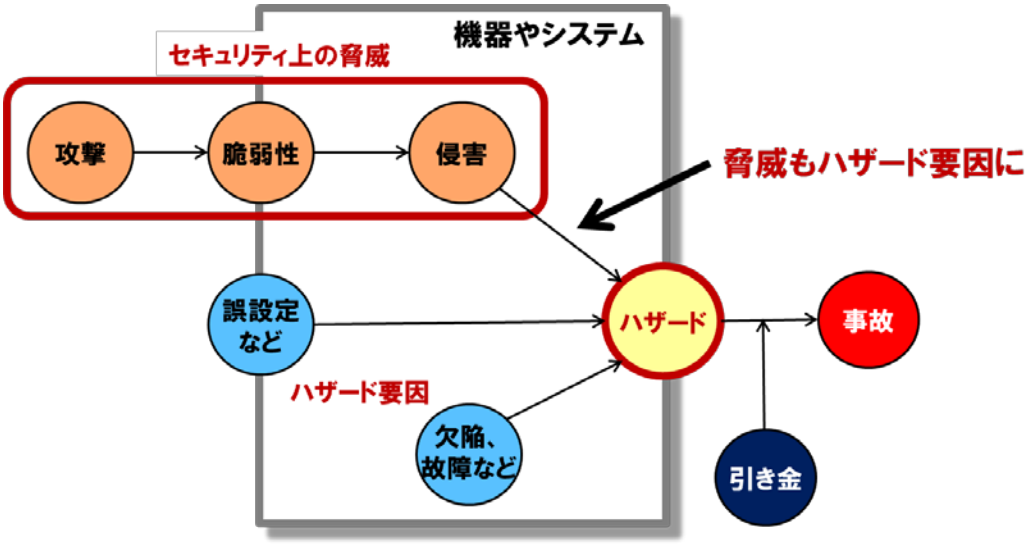


図 2.1-7 セキュリティ上の問題がセーフティに影響を与えるモデル [9]

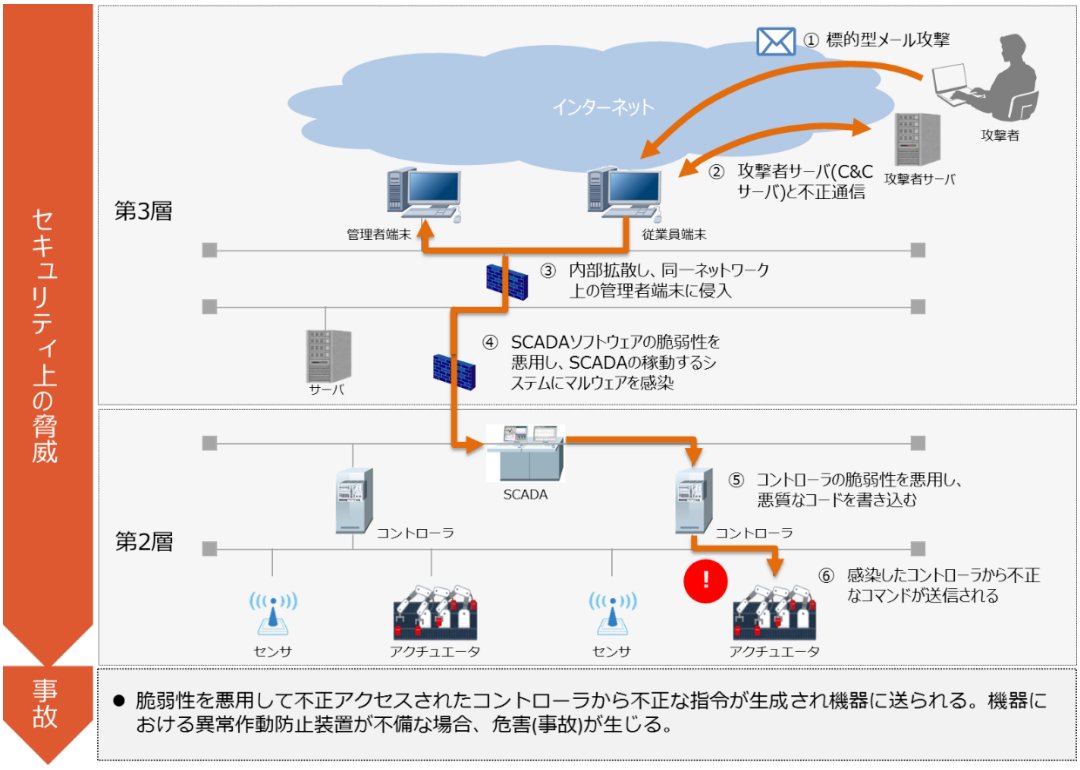


図 2.1-8 セキュリティ上の問題がセーフティに影響を与える事例

[9] 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

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（ソシキ、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（ソシキ、あるいはソシキに属さないヒト、モノ等）がわかるように可能な限り一覧化し、組織自らが定めた重要度等の基準に基づいて分類する必要がある。

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、上記①～③に記載の観点に留意し、信頼性の基点の確保を考慮した上で、信頼性の基点となる要素の明確化が重要である。

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得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、企業等は、各層の機能を脅かす上位レベルでの事象を検討し、その事象につながるセキュリティインシデントを抽出する必要がある。

表 2.1-1 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 2.1-2 に示す。企業等は、表 2.1-2 の「機能（守るべきもの）に対する悪影響のイメージ」を考慮した、セキュリティインシデントの抽出が重要である。

表 2.1-2 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、従業員の健康や安全、環境への悪影響等)
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、環境面、衛生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は、1.1.(2)で示した①～④の各観点を十分に考慮することも重要である。各観点への対応が不十分である場合、表 2.1-3 に例として示すようなセキュリティインシデントが発生し、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 2.1-3 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の例

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[10]
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, L2_3_d
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、各層の機能及び、機能に対する悪影響、1.1.(2). で示した①～④の各観点を踏まえ、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を表 2.1-4 にリストとして示す。

企業等においては、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、企業等の事情を加味して検討を具体化する必要がある。

表 2.1-4 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、ランサムウェアへの感染等により、自組織のデータを取り扱うシステムが停止する
	(d) 製品・サービスの提供チャネルでセキュリティインシデントが発生し、機器の破損等の意図しない品質劣化が生じる

[10] 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。

(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) セキュリティインシデント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(誤計測、モノの適切でない制御、制御機能、計測機能の停止等)	
	(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、計測機能の停止等)	
	(a)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、故障や正確でないデータ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、故障や正確でないデータの送信等が発生する
	(d) 計測機能に対する物理的な妨害により、正確でないデータ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)ソシキ/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

企業等は、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及び影響の大きさを割り当てる必要がある。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」や「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 及び 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、当該インシデントの発生を助長、あるいは発生したインシデントの被害を拡大させる可能性がある脅威及び、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及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 2.1-9 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企業等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、リスク源の評価は企業等の事情を加味して実施する必要がある。

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。例えば、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。

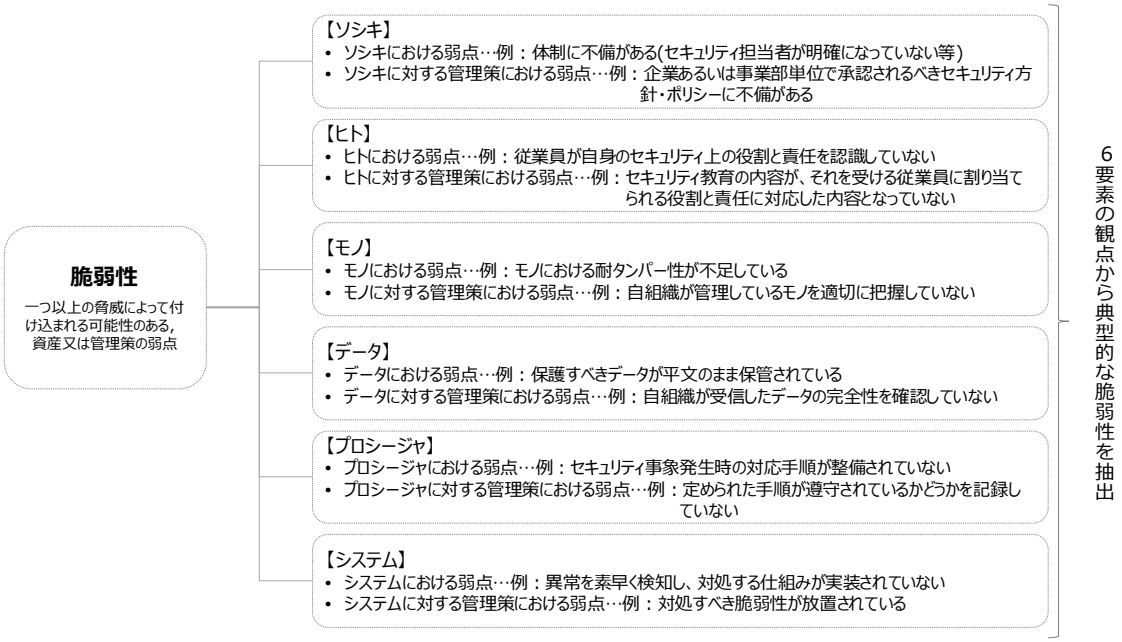


図 2.1-9 6 つの構成要素という観点による脆弱性の抽出

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[11]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。[12]

(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やリスクをとったとしても機会を追求するという場合に、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[13]。

上記の内、特に低減を選択する場合の対応として、各リスク源に対して、適当と考えられる対策要件を、各種のガイドライン等を参考にしながら導出し、添付 B に整理した。これを参照して、企業等に応じた対策要件を選択することが可能である。また、各々の対策要件に対して、特定の脆弱性との対応づけを行っているため、企業等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可能である。

対策要件の選定に際しても、先に提示した４つの観点を踏まえて検討を行うことが重要である。

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

・ 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

---

[11]「つながる世界のセーフティ&セキュリティ設計入門」（IPA, 2015 年）から引用。

[12] 記載しているリスク対応の類型は、JIS Q 31000:2019 において提示されるリスク対応の選択肢と下記のように対応している。
・ リスクの回避：「リスクを生じさせる活動を開始又は継続しないと決定することによってリスクを回避する。」、「リスク源を除去する。」を含む
・ リスクの低減：「起こりやすさを変える。」、「結果を変える。」を含む
・ リスクの移転：「(例えば，契約，保険購入によって)リスクを共有する。」を含む
・ リスクの保有：「ある機会を追求するために，リスクを取る又は増加させる。」、「情報に基づいた意思決定によって，リスクを保有する。」を含む

[13] リスクを回避、低減、移転するのでなく、保有する場合、当該リスクに関連する資産の管理者から承認を得る必要がある。

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 には、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 2.1-10 に示す 5 つのフェーズが記載されている。[14]

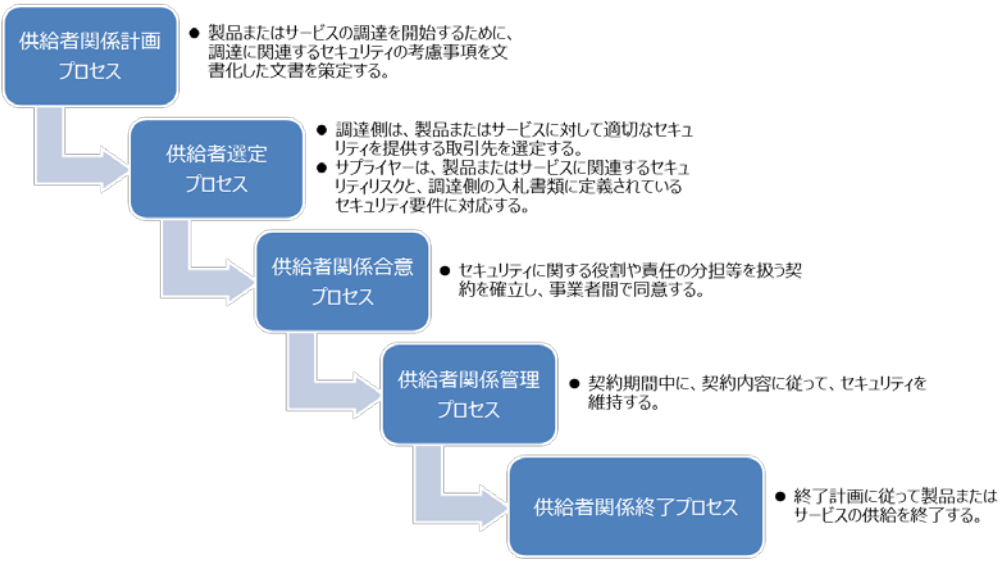


図 2.1-10　ISO/IEC 27036-2:2013 における個々のサプライヤーとの契約におけるライフサイクル

・ 特に、第Ⅲ部にて記載する対策カテゴリ 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。これらも参照し、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必要がある。

➢ 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（各対策要件の詳細については第Ⅲ部を参照されたい）。

[14] 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、対策要件及び対策例の記述に当たり、ISO/IEC 27036:2014 をそれぞれ参照している。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。

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-6, CPS.DS-11, 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、企画、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検討する必要がある。

  ➢ 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 2.1-11)。[15]

[15] 上記の IEC による規格以外では、IEC TR 63074 と同様に機械安全のセキュリティを扱っている ISO TR22100-4:2018(セキュリティ面のガイド及び考慮)も参照することが可能である。

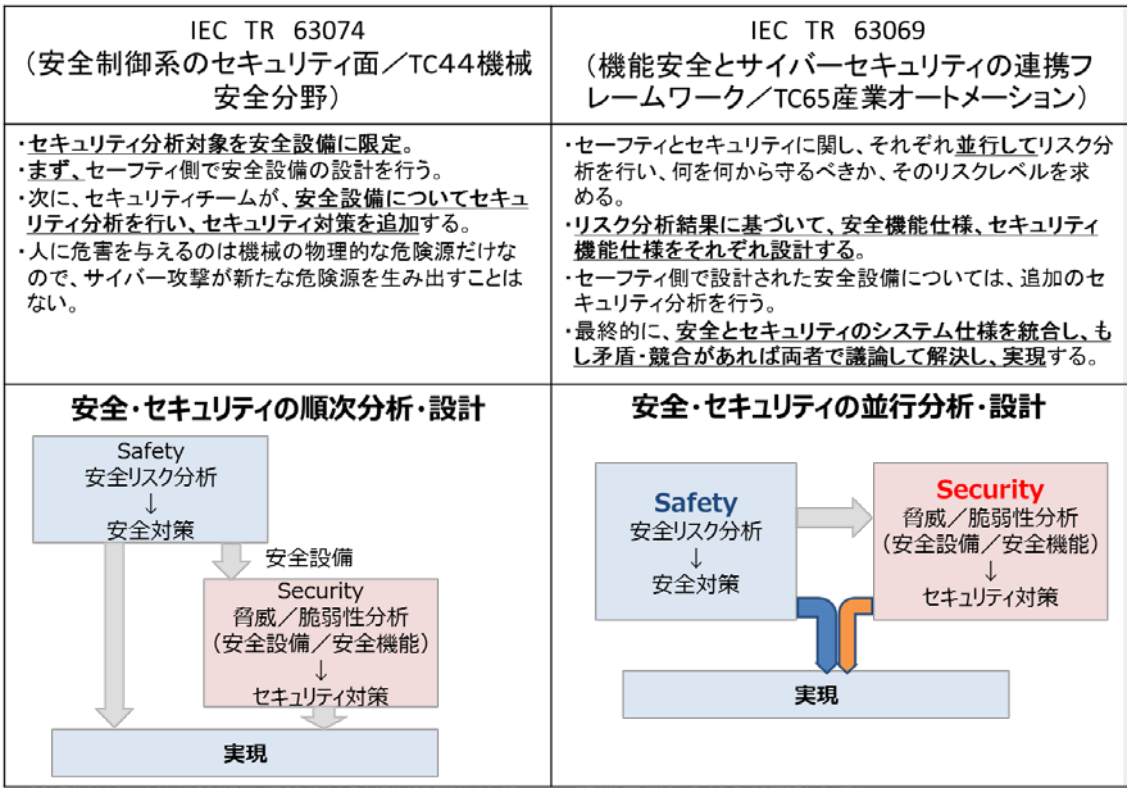


図 2.1-11 国際標準化活動におけるセーフティとセキュリティの統合に関する検討状況 [16]

- 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、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重要である [17]。
  - ➢ 関連する対策要件には、CPS.AC-2, CPS.DS-8, CPS.IP-5, CPS.IP-6, CPS.PT-2, CPS.CM-2 等がある。

[16] 「制御システム　セーフティ・セキュリティ要件検討ガイド」（IPA, 2018 年）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。
[17] 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。

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重要である。
- 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、適切に報告が必要な関係者へと周知しておく必要がある。
- 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重要である。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、再委託先以降の組織についても定めている要求事項が遵守され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-3, CPS.SC-4, CPS.SC-6, CPS.SC-8 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の維持・向上が重要である。
- 具体的には、企画、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重要である。
- 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ソフトウェアの設計、実装を含んだ製造、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点が指摘されている [18]。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-10, CPS.DS-12, CPS.DS-15, 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（ソシキ、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。

[18] 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-14, CPS.AE-1, CPS.CM-3, CPS.CM-4, CPS.CM-5 等がある。

表 2.1-5 リスクマネジメントのプロセス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-3, CPS.SC-4, CPS.SC-6, CPS.DS-10, CPS.DS-12, CPS.CM-4, CPS.CM-5

2. リスク源と対策要件の対応関係

添付 B では、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 2.2-1 に示す形式で一覧化している。

表 2.2-1 添付 B における記載の例(第 3 層)（抜粋）

機能	想定されるセキュリティインシデント	リスク源			対策要件	対策要件 ID
		脅威	脆弱性 ID	脆弱性		
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	サービス拒否攻撃により、関係する他組織における自組織のデータを取り扱うシステムが停止する	・システムを構成するサーバ等の電算機器、通信機器等に対するサービス拒否攻撃	L3.3_b_ORG	[ソシキ] ・データの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
					・外部の組織との契約を行う	CPS.SC-3

る機能		・妨害電波の発信			場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織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。	
	攻撃の有無に関わらず、データを取り扱うシステムが停止する	・品質や信頼性の低いシステムによるサービス提供	L3_3_c_SYS	[システム] ・IoT 機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース(例:ヒト、モト、システム)を確保する。	CPS.DS-6

「機能」は、1.1 の表 2.1-1 で整理した三層構造モデル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インシデントであり、1.1 の表 2-1.4 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。企業等は、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、実際に企業等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部及び添付 C では、対策要件、対策要件に対応したセキュリティ対策例及び他の国際規格等との関係性を示している。

第Ⅲ部及び添付 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ステップにおいて最も有用に機能すると考えられる。企業等は、以下に示す用途に本項の内容を活用することができる。

(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、企業等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及び、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とコスト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、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ことを目的にして、対策例を添付 C にまとめている。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を選択できるように、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。企業等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必要がある。

②に関しては、後述する 3.1 以降及び添付 C において、本フレームワークで整理している対策要件と、主要な国際規格等との対応関係を示している。特に、添付 C においては、対策例のレベル単位で、NIST SP800-171, NIST SP800-53 Rev.4, ISO/IEC 27001:2013 の対策項目との対比を整理している。また、添付 D

では、主要な国際規格等から見た、本フレームワークの対策要件との対応関係を表形式で整理している。これらを参照することで、対策要件の実装を通じた国際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を活用することが期待される。

(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

企業等は、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-6 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することが重要である。

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 3.2-1 に添付Cの記載事項を示す。

表 3.2-1 添付Cの記載事項

対策要件ID	対策要件	対策例	対策例を実行する主体	参照ガイドライン			
				NIST SP800-171	NIST SP800-53	ISO/IEC 27001	IEC 62443
		<High-Advanced>	O/S		O		O
		<Advanced>	O	O	O	O	
		<Basic>	O		O	O	

対策例のレベルは、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、対策例を導入・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。組織が、"High-Advanced"に分類される対策例を実装する際は、"Advanced"と"Basic"に分類されたセキュリティ対策例もカバーしておく必要がある。

組織においては、CPS.AM-5 や CPS.BE-2 で対応が求められている、事業、業務、システム等へ割り当てられた重要度を参照し、High-Advanced, Advanced, Basic の内、必要なレベルの対策の実装を進める必要がある。一例として、業務、システム等について、機密性、完全性、可用性の観点から、表 3.2-2 のように重要度を割り当てることが考えられる。組織は、評価値や評価基準等を自組織特有の条件も勘案しつつ具体化する必要がある。

表 3.2-2 情報資産の機密性・完全性・可用性に基づく重要度の例 [19]

評価値		評価基準
機密性	2	法律で安全管理(漏えい、滅失又はき損防止)が義務付けられている
		守秘義務の対象や限定提供データとして指定されている 漏えいすると取引先や顧客に大きな影響がある
		自社の営業秘密として管理すべき(不正競争防止法による保護を受けるため) 漏えいすると自社に深刻な影響がある
	1	漏えいすると業務に大きな影響がある
	0	漏えいしても業務にほとんど影響はない
完全性	2	法律で安全管理(漏えい、滅失又はき損防止)が義務付けられている
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある
	1	改ざんされると業務に大きな影響がある
	0	改ざんされても業務にほとんど影響はない
可用性	2	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある
	1	利用できなくなると事業に大きな影響がある
	0	利用できなくなっても事業にほとんど影響はない

なお、対策要件により、「<Advanced><Basic>共通」のように異なるレベルで同一の対策例を記載している場合がある。これは Advanced と Basic で同様の対策例を実施することを求めるものである。また、特に Basic にて「(該当なし)」と記載している要件は、対策例実施のためのリソースが厳しく制限されている場合や、対策の実施対象となるシステム、モノ等の重要度が高くない場合等において、当該要件の実装の優先度が必ずしも高くないことを示している。

また、「対策例を実装する主体」では、当該対策例を実装するに当たり、主体となる要素を 3 つに分類して提示している [20]。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は「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、企業等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

[19] 「中小企業の情報セキュリティ対策ガイドライン 第 3 版」(IPA, 2019 年)の P.45 表 10 を参考に記載している。なお、特に産業用制御システム等については、「評価値」あるいは「評価基準」において、情報システムで一般的に想定される影響に加えて、安全性(セーフティ)や環境、衛生という側面への影響についても考慮する必要がある。

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

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別に表 3.3.2～3.3.21 に示す。

(1) 対策要件のカテゴリ

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 Ver.1.1 のサブカテゴリに対応付ける形で表 3.3-1 に示すように 20 カテゴリを定めた。

表 3.3-1 対策要件のカテゴリと NIST Cybersecurity Framework との対応関係

カテゴリ名称	略称	NIST Cybersecurity Framework Ver.1.1 の対応カテゴリ
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)
情報を保護するためのプロセス及び手順	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)
異変とイベント	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)

カテゴリ名称	略称	NIST Cybersecurity Framework Ver.1.1 の対応カテゴリ
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 Ver.1.1 の参照文献やサイバーセキュリティ経営ガイドライン Ver 2.0 のチェックリストも参考に、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” (NIST Cybersecurity Framework Ver 1.1)
- Council on CyberSecurity（the Council） “The Critical Security Controls” (CIS CSC)
- 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”[21]
- NIST “Special Publication 800-53 Revision 4”（SP 800-53 Rev.4）
- “Common Criteria for Information Technology Security Evauation Version 3.1 Revision 5” (CC v3.1 Release 5)
- 経済産業省 “サイバーセキュリティ経営ガイドライン Ver 2.0”
- 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”

[21] クラウドサービスの利用にあたっては、「関連標準等」に言及されている ISO/IEC 27001:2013 Annex A の項番と対応した ISO/IEC 27017:2015 の項目も参照することが望ましい。

３．１．CPS.AM－資産管理

企業等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、それらが管理される場所等を特定し、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 3.3-2 CPS.AM カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	関連標準等
CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L2_1_a_ORG, L2_3_b_ORG, L2_3_b_SYS	NIST Cybersecurity Framework Ver.1.1 ID.AM-1, ID.AM-2 CIS CSC 1, 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.6.2.1, A.8.1.1, A.8.1.2, A.8.1.3, A.11.2.5 NIST SP 800-53 Rev. 4 CM-8, PM-5 CC v3.1 Release5 Part 2 FMT サイバーセキュリティ経営ガイドライン 指示 4 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、トレーサビリティ確保のための特定方法を定める。	L1_3_a_COM, L1_3_b_COM	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_3_a_COM, L1_3_b_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、適切に管理する。	L1_3_b_ORG, L1_3_c_ORG	NIST Cybersecurity Framework Ver.1.1 ID.AM-3 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4, 4.2.3.5 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 サイバーセキュリティ経営ガイドライン 指示 4

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、適切に管理する。	L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L1_3_b_ORG, L1_3_c_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.6.2.1, A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9 サイバーセキュリティ経営ガイドライン 指示 4 IoT セキュリティガイドライン 要点 3
CPS.AM-6	・リソース(例:モノ、、データ、システム)を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG, L3_1_a_ORG, L3_4_a_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, 4.3.4.4.3 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6 サイバーセキュリティ経営ガイドライン 指示 4 IoT セキュリティガイドライン 要点 3
CPS.AM-7	・自組織及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_b_ORG, L1_3_c_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 サイバーセキュリティ経営ガイドライン 指示 4., 指示 9 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 3.3-3 CPS.BE カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	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_b_ORG, L1_3_c_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 サイバーセキュリティ経営ガイドライン 指示 9 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、自組織の取引に関係する者(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 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 PM-11, SA-14 サイバーセキュリティ経営ガイドライン 指示 6, 指示 9
CPS.BE-3	・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。	L1_3_b_ORG, L1_3_c_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 サイバーセキュリティ経営ガイドライン 指示 9

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 3.3-4 CPS.GV カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	関連標準等
CPS.GV-1	・セキュリティポリシーを策定し、自組織及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, 4.3.2.2.1, 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 サイバーセキュリティ経営ガイドライン 指示 1, 指示 2, 指示 6 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する。	L1_2_a_ORG, L1_2_a_COM, L1_2_a_SYS, L1_2_a_PRO, L1_2_a_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 サイバーセキュリティ経営ガイドライン 指示 1
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	L1_1_a_SYS, L1_1_a_DAT, L1_1_b_SYS,	NIST Cybersecurity Framework Ver.1.1 ID.GV-3 CIS CSC 13 ISA 62443-2-1:2009 4.3.4.4.6, 4.4.3.7

	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。	L3_1_a_SYS, L3_1_a_DAT, L3_4_a_ORG, L3_4_a_PRO, L3_4_b_ORG, L3_4_b_PRO	ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4
CPS.GV-4	・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, 4.3.2.6.3 ISO/IEC 27001:2013 Clause 6 NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 CC v3.1 Release5 Part 2 FMT サイバーセキュリティ経営ガイドライン 指示 2, 指示 3 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

企業等は自組織の業務（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 3.3-5 CPS.RA カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	関連標準等
CPS.RA-1	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	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 CC v3.1 Release5 Part 1 サイバーセキュリティ経営ガイドライン 指示 4 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、対応及び活用するプロセスを確立する。	L1_1_a_SYS, L1_3_a_ORG, L2_1_a_ORG, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_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, A.12.6.1 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16 サイバーセキュリティ経営ガイドライン 指示 10 IoT セキュリティガイドライン 要点 18, 要点 21
CPS.RA-3	・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。	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 CC v3.1 Release5 Part 1 サイバーセキュリティ経営ガイドライン 指示 4

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 機器及び IoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_a_COM, L2_1_a_PRO, L2_2_a_ORG, L2_2_a_SYS	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, 4.2.3.11, 4.2.3.12 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 CC v3.1 Release5 Part 1 サイバーセキュリティ経営ガイドライン 指示 4 IoT セキュリティガイドライン 要件 4, 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, Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 CC v3.1 Release5 Part 1 サイバーセキュリティ経営ガイドライン 指示 4 IoT セキュリティガイドライン 要件 4, 要点 7
CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 ・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_a_COM, L2_1_a_PRO, L2_2_a_SYS	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 CC v3.1 Release5 Part 1 サイバーセキュリティ経営ガイドライン 指示 4 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 3.3-6 CPS.RM カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	関連標準等
CPS.RM-1	・自組織内における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し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスク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_b_ORG, L1_3_c_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 CC v3.1 Release5 Part 2 FMT サイバーセキュリティ経営ガイドライン 指示 4 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及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_ORG, L1_1_a_SYS, L1_1_b_ORG, 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 サイバーセキュリティ経営ガイドライン 指示 4

３．６．CPS.SC－サプライチェーンリスク管理

企業等の優先順位、制約、リスク許容値及び想定が、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。企業等は、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 3.3-7 CPS.SC カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	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、その内容について取引先と合意する。	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 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9 CC v3.1 Release5 Part 2 FMT サイバーセキュリティ経営ガイドライン 指示 9
CPS.SC-2	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG, L2_3_c_ORG, L3_1_b_ORG, L3_1_c_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_d_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, 4.2.3.13, 4.2.3.14 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9 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	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織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_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_1_d_ORG, L2_3_c_ORG, L3_1_b_ORG, L3_1_b_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 NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12,

		L3_1_c_ORG, L3_1_c_DAT, L3_3_d_ORG, L3_3_a_ORG,. L3_3_b_ORG, L3_3_c_ORG, L3_4_a_DAT, L3_4_b_DAT	PM-9 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	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_1_d_ORG, L1_1_d_COM, L2_1_a_COM, L2_1_a_PRO, L2_2_a_ORG, L2_3_a_ORG, L2_3_c_ORG, L2_3_c_PRO, L2_3_d_ORG, L3_1_b_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_c_ORG, L3_3_d_ORG	ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 ISO/IEC 27001:2013 A15.1.3 CC v3.1 Release5 Part 2 FIA, FDP サイバーセキュリティ経営ガイドライン 指示 9 IoT セキュリティガイドライン 要点 14
CPS.SC-5	・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	ISA 62443-2-1:2009 4.3.3.2.1 NIST SP 800-53 Rev.4 PS-7, SA-21
CPS.SC-6	・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,	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

		L2_3_c_PRO, L2_3_d_ORG, L3_1_a_DAT, L3_1_b_ORG, L3_1_b_DAT, L3_1_c_ORG, L3_1_c_DAT, L3_3_a_ORG,. L3_3_b_ORG, L3_3_c_ORG, L3_3_d_ORG, L3_4_a_DAT, L3_4_b_DAT	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-7	・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, L3_3_d_ORG	
CPS.SC-8	・自組織が、関係する他組織及び個人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。	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, L3_3_d_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-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、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	L1_3_b_PEO	NIST Cybersecurity Framework Ver.1.1 ID.SC-5 CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.4.3, 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.16.1.5, A.17.1.2, 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	NIST SP 800-53 Rev. 4 SA-22
CPS.SC-11	・サプライチェーンに係るセキュリティ対策基準及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

資産及びそれが管理される場所への論理的・物理的アクセスを、承認されたソシキ、ヒト、モノ、プロシージャに限定し、承認された活動及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 3.3-8 CPS.AC カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	関連標準等
CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM, L1_1_b_SYS, L1_1_c_COM, L2_3_c_SYS, L3_1_a_SYS, L3_3_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.6.2.1, 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 CC v3.1 Release5 Part 2 FAU, FIA, FMT サイバーセキュリティ経営ガイドライン 指示 5
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, L1_1_c_SYS, L2_3_b_PEO, L2_3_b_SYS, L2_3_c_SYS, L2_3_d_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 CC v3.1 Release5 Part 2 FIA, FMT, FDP サイバーセキュリティ経営ガイドライン 指示 5
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, CSC 15 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.6, SR 1.13, SR 2.6

			ISO/IEC 27001:2013 A.6.2.1, 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 CC v3.1 Release5 Part 2 FCS, FIA, FMT サイバーセキュリティ経営ガイドライン 指示 5 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 1.11, SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.9.4.2, 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 CC v3.1 Release5 Part 2 FIA サイバーセキュリティ経営ガイドライン 指示 5 IoT セキュリティガイドライン 要点 4
CPS.AC-5	・職務及び責任範囲(例:ユーザー/システム管理者)を適切に分離する。	L1_1_a_SYS, 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 CC v3.1 Release5 Part 2 FMT サイバーセキュリティ経営ガイドライン 指示 5 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、想定されるリスクも考慮して、信頼性の高い認証方式(例:	L1_1_a_SYS, 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, 14, 15, 16 COBIT 5 DSS05.04

	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。		ISA 62443-2-1:2009 4.3.3.7.3, 4.3.3.7.4 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 CC v3.1 Release5 Part 2 FMT, FIA サイバーセキュリティ経営ガイドライン 指示 5 IoT セキュリティガイドライン 要点 8
CPS.AC-7	・データフロー制御ポリシーを定め、それに従って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_DAT, L3_4_b_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 サイバーセキュリティ経営ガイドライン 指示 5
CPS.AC-8	・IoT 機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ(ヒト/モノ/システム等)との通信に限定する。	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 4.3.3.5.2, 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 CC v3.1 Release5 Part 2 FCO, FCS, FDP, FIA サイバーセキュリティ経営ガイドライン 指示 5 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 機器やユーザーによる構成要素(モノ/システム等)への論理的	L1_1_a_SYS, L1_1_b_SYS,	NIST Cybersecurity Framework Ver.1.1 PR.AC-7

	なアクセスを、取引のリスク(個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク)に見合う形で認証・認可する。	L2_1_b_SYS, L3_1_a_SYS, L3_4_b_SYS	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 CC v3.1 Release5 Part 2 FCS, FDP, FIA, FPR サイバーセキュリティ経営ガイドライン 指示 5 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

自組織の職員及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 3.3-9 CPS.AT カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	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、教育を実施し、その記録を管理する。	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO, L1_1_d_PEO, L1_2_a_PEO, L1_3_a_PEO, L1_3_a_DAT, L1_3_c_PEO, L3_4_a_PEO	NIST Cybersecurity Framework Ver.1.1 PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5 CIS CSC 17 ISA 62443-2-1:2009 4.3.2.4.1, 4.3.2.4.2, 4.3.2.4.6, 4.3.3.2.5, 4,3,4,5,2, 4.3.4.5.11 ISO/IEC 27001:2013 A.6.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.3.1 NIST SP 800-53 Rev. 4 AT-1, AT-2, AT-3, AT-4 サイバーセキュリティ経営ガイドライン 指示 3, 指示 5, 指示 8
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得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	L1_3_a_DAT, L1_3_b_PEO, L3_3_a_PEO	NIST Cybersecurity Framework Ver.1.1 PR.AT-3, PR.IP-10, RS.CO-1 CIS CSC 17 COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.1, 4.3.2.4.2, 4.3.2.4.3, 4.3.2.4.6, 4.3.4.5.11 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-4, PS-7, SA-9, SA-16 サイバーセキュリティ経営ガイドライン 指示 3, 指示 7, 指示 8
CPS.AT-3	・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO, L1_3_a_PEO, L1_3_b_PEO, L1_3_c_PEO,	CIS CSC 17 ISA 62443-2-1:2009 4.3.2.4.4, 4.3.2.4.5 ISO/IEC 27001:2013 A.7.2.2 NIST SP 800-53 Rev. 4 AT-1

		L3_3_a_PEO, L3_4_a_PEO, L3_4_b_PEO	

３．９．CPS.DS－データセキュリティ

情報を、その機密性、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 3.3-10 CPS.DS カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	関連標準等
CPS.DS-1	・組織間で保護すべき情報を交換する場合、当該情報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。	L3_1_a_PRO, L3_4_a_DAT, L3_4_b_DAT	ISO/IEC 27001:2013 A.13.1.2, A.13.2.1, A.13.2.2, A.13.2.3 NIST SP 800-53 Rev. 4 SC-1 サイバーセキュリティ経営ガイドライン 指示 5
CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	L1_1_a_DAT, L3_1_a_DAT, L3_3_d_SYS, L3_4_b_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-1 CIS CSC 13, 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, SR 4.3 ISO/IEC 27001:2013 A.8.2.3, A.10.1.1 NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28 CC v3.1 Release5 Part 2 FCA サイバーセキュリティ経営ガイドライン 指示 5
CPS.DS-3	・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_DAT, L3_2_b_DAT, L3_3_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-2 CIS CSC 13, 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, SR 4.3 ISO/IEC 27001:2013 A.6.2.2, 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 CC v3.1 Release5 Part 2 FCO, FCS サイバーセキュリティ経営ガイドライン 指示 5 IoT セキュリティガイドライン 要点 14
CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。	L1_1_a_DAT, L1_1_b_DAT, L3_1_a_DAT, L3_2_b_DAT, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-2 CIS CSC 13, 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, SR 4.3 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 CC v3.1 Release5 Part 2 FCS サイバーセキュリティ経営ガイドライン 指示 5 IoT セキュリティガイドライン 要点 14
CPS.DS-5	・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_DAT	CIS CSC 13 ISO/IEC 27001:2013 A.10.1.2 NIST SP 800-53 Rev. 4 SC-12 サイバーセキュリティ経営ガイドライン 指示 5
CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース(例:ヒト、モノ、システム)を確保する。	L1_1_c_SYS, L2_1_d_SYS, L3_3_c_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-4 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2, SR 7.1 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 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 CC v3.1 Release5 Part 2 FCO, FRU サイバーセキュリティ経営ガイドライン 指示 5
CPS.DS-7	・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。	L1_1_c_SYS, L2_1_d_SYS, L3_3_c_SYS	NIST Cybersecurity Framework Ver.1.1 PR.DS-4 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2, SR 7.5 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 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 CC v3.1 Release5 Part 2 FRU サイバーセキュリティ経営ガイドライン 指示 5
CPS.DS-8	・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 ISO/IEC 27001:2013 A.8.2.3, A.10.1.2, A.11.1.4, A.11.1.5, A.11.2.1 NIST SP 800-53 Rev. 4 PE-19 CC v3.1 Release5 Part 2 FCS, FPT

			サイバーセキュリティ経営ガイドライン 指示 5 IoT セキュリティガイドライン 要点 8
CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	L1_1_a_DAT, L2_3_c_SYS, L3_1_a_DAT	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.8.2.2, A.8.2.3, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, SC-7, SC-8, SC-13, SC-31, SI-4 CC v3.1 Release5 Part 2 FCS, FPT サイバーセキュリティ経営ガイドライン 指示 5 IoT セキュリティガイドライン 要点 8
CPS.DS-10	・IoT 機器、サーバ等にて稼動するソフトウェアの完全性を組織が定めるタイミングで検証し、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.14.2.4 NIST SP 800-53 Rev. 4 SC-16, SI-7 CC v3.1 Release5 Part 2 FCS, FPT サイバーセキュリティ経営ガイドライン 指示 5 IoT セキュリティガイドライン 要点 8
CPS.DS-11	・送受信・保管する情報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.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-16, SI-7 CC v3.1 Release5 Part 2 FCS, FPT サイバーセキュリティ経営ガイドライン 指示 5 IoT セキュリティガイドライン 要点 8
CPS.DS-12	・ハードウェアの完全性を検証するために完全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 CC v3.1 Release5 Part 2 FCS, FPT サイバーセキュリティ経営ガイドライン 指示 5 IoT セキュリティガイドライン 要点 8
CPS.DS-13	・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	CC v3.1 Release5 Part 2 FIA, FDP, FCS サイバーセキュリティ経営ガイドライン 指示 5
CPS.DS-14	・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, L3_4_b_PRO	ISO/IEC 27001:2013 A.18.1.3, A.18.1.4 CC v3.1 Release5 Part 2 FAU サイバーセキュリティ経営ガイドライン 指示 5 IoT セキュリティガイドライン 要点 13
CPS.DS-15	・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_COM, L2_1_a_PRO, L2_3_a_ORG, L2_3_d_ORG	ISO/IEC 27001:2013 A.15.1.3 NIST SP 800-53 Rev. 4 SA-12 サイバーセキュリティ経営ガイドライン 指示 5

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 3.3-11 CPS.IP カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	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。	L1_1_a_SYS, L1_1_b_SYS, L2_1_a_ORG, L2_1_b_COM, L2_1_b_PRO, L2_3_b_ORG, L3_1_a_SYS, L3_3_d_SYS	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, 4.3.4.3.5, 4.3.4.3.6 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, 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 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_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.IP-1 CIS CSC 9 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する。	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG, L2_1_d_SYS, L3_3_c_SYS	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 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、テストする。	L1_3_a_DAT, L2_1_d_SYS, L3_3_c_SYS	NIST Cybersecurity Framework Ver.1.1 ID.BE-5, 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 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, L1_1_c_SYS, L2_3_b_SYS, L2_3_d_SYS, L3_1_a_SYS	NIST Cybersecurity Framework Ver.1.1 ID.BE-5, 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 CC v3.1 Release5 Part 2 FPT, FRU サイバーセキュリティ経営ガイドライン 指示 8 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 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

			CC v3.1 Release5 Part 2 FCS, FIA, FDP, FMT, FPT サイバーセキュリティ経営ガイドライン 指示 5 IoT セキュリティガイドライン 要点 6
CPS.IP-7	・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L2_1_a_ORG	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 サイバーセキュリティ経営ガイドライン 指示 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_ORG	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 CC v3.1 Release5 Part 1 サイバーセキュリティ経営ガイドライン 指示 9 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, 4.3.3.2.4, 4.3.3.2.3, 4.3.3.2.6 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 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	・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	L1_1_a_SYS, L2_1_a_ORG, L3_1_a_SYS,	NIST Cybersecurity Framework Ver.1.1 PR.IP-12 CIS CSC 4, 18, 20 COBIT 5 BAI03.10, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.3.4.3.7

		L3_3_a_SYS, L3_3_d_SYS	ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 サイバーセキュリティ経営ガイドライン 指示 5 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 3.3-12 CPS.MA カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	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、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 ・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_ORG, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_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, A.14.2.4 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を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	L1_1_a_SYS, L2_1_a_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_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 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 3.3-13 CPS.PT カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	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。	L1_1_a_SYS, L2_1_b_ORG, L3_1_a_SYS, L3_3_a_SYS, 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, 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 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または論理的に閉塞することで、IoT 機器、サーバ等の機能を必要最小限とする。	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_b_COM, L2_3_b_SYS, L3_1_a_SYS, L3_3_d_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 1.6, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4 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 3.6, SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.16.1.6 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－異変とイベント

異変を検知し、事象がもたらす可能性のある影響を把握する。

表 3.3-14 CPS.AE カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	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情報の流れを特定し、管理するプロシージャを確立し、実施する。	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM, L1_1_c_COM, L1_3_b_ORG, L1_3_c_ORG, L2_1_b_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_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 CC v3.1 Release5 Part 2 FAU, FDP サイバーセキュリティ経営ガイドライン 指示 5
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_3_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 A6.1.1, A.12.4.1, A.16.1.5 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_1_b_SYS, L1_3_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 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する。	L1_3_b_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.6.1.4, A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4

			サイバーセキュリティ経営ガイドライン 指示 5 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_3_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 サイバーセキュリティ経営ガイドライン 指示 5

３．１４．CPS.CM – セキュリティの継続的なモニタリング

セキュリティ事象を検知し、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 3.3-15 CPS.CM カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	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・制御、アクセス監視・制御を実施する。	L1_1_a_SYS, L1_1_c_SYS, L1_3_a_SYS, L2_1_b_ORG, L2_3_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_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 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及び記録、監視を実施する。	L1_1_a_SYS, L1_1_c_SYS, L2_3_b_PEO, L2_3_b_SYS, L2_3_d_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, A.11.1.3, A.11.2.5, A.11.2.6 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20 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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	L1_1_b_SYS, 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, SR 3.5 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3, SI-8 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の完全性及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 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_a_SYS, L1_1_b_COM, L1_1_c_COM, L1_3_b_ORG, L1_3_c_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 DE.CM-6 COBIT 5 APO07.06, APO10.05 ISO/IEC 27001:2013 A.13.1.2, 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)及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM, L1_1_c_COM, L1_3_a_SYS, L1_3_b_ORG, L1_3_c_ORG, L2_1_a_ORG, L2_1_c_ORG, L2_1_c_SYS, L2_3_b_ORG, L2_3_b_SYS, L2_3_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 PR.AC-3, 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 ISO/IEC 27001:2013 A.12.4.1, 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, L2_1_c_SYS, L3_1_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

		L3_3_a_SYS, L3_3_d_SYS	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及び手順を維持し、テストする。

表 3.3-16 CPS.DP カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	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_3_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 サイバーセキュリティ経営ガイドライン 指示 5
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_a_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 サイバーセキュリティ経営ガイドライン 指示 1
CPS.DP-3	・監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。	L1_3_a_ORG	NIST Cybersecurity Framework Ver.1.1 DE.DP-3 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, A.14.3.1 CC v3.1 Release5 Part 2 FPT_TEE サイバーセキュリティ経営ガイドライン 指示 5 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_1_b_SYS, L1_3_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 サイバーセキュリティ経営ガイドライン 指示 5

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・復旧のプロセス及び手順を実施し、維持する。

表 3.3-17 CPS.RP カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	関連標準等
CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	L1_1_a_SYS, L1_3_a_PEO, L1_3_a_PRO, L2_1_a_PRO, L2_1_b_PRO, L2_1_c_PRO, L2_2_a_PRO, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	NIST Cybersecurity Framework Ver.1.1 ID.BE-5, 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 4.3.3.3.10, 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 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） サイバーセキュリティ経営ガイドライン 指示 5, 指示 7, 指示 8 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_b_PEO, L1_3_b_PRO, L1_3_c_PEO, L1_3_c_PRO	NIST Cybersecurity Framework Ver.1.1 ID.BE-5, 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, 4.3.4.5.2, 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 サイバーセキュリティ経営ガイドライン 指示 7, 指示 8
CPS.RP-3	・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急時対応計画の中にセキュリティインシデントを位置づける。	L1_3_a_PRO, L1_3_a_DAT	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 ISA 62443-2-1:2009 4.3.2.5.4, 4.3.3.3.10 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 サイバーセキュリティ経営ガイドライン 指示 8
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_b_COM	

３．１７．CPS.CO – 伝達

セキュリティインシデントがもたらす自組織、及び社会全体への影響を低減し、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 3.3-18 CPS.CO カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	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_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 RC.CO-1 CIS CSC 19 COBIT 5 EDM03.02 ISA 62443-2-1:2009 4.3.4.5.9 ISO/IEC 27001:2013 A.6.1.4, A.17.1.1, Clause 7.4 サイバーセキュリティ経営ガイドライン 指示 8 IoT セキュリティガイドライン 要点 18
CPS.CO-2	・事業継続計画又は緊急時対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。	L1_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 RC.CO-2 COBIT 5 MEA03.02 ISO/IEC 27001:2013 A.17.1.1, Clause 7.4 サイバーセキュリティ経営ガイドライン 指示 8
CPS.CO-3	・復旧活動について内部及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、事業継続計画又は緊急時対応計画の中に位置づける。	L1_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 RC.CO-3 CIS CSC 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.2.5.5, 4.3.4.5.9 ISO/IEC 27001:2013 A.17.1.1, Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4 サイバーセキュリティ経営ガイドライン 指示 8

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 3.3-19 CPS.AN カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	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、自組織及び関係する他組織を含む社会全体への影響を把握する。	L1_3_a_COM, L1_3_a_PRO	NIST Cybersecurity Framework Ver.1.1 RS.AN-2 CIS CSC 19 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 サイバーセキュリティ経営ガイドライン 指示 10
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_3_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_3_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、その影響を低減し、セキュリティインシデントを解決するための活動を実施する。

表 3.3-20 CPS.MI カテゴリの対策要件

対策要件 ID	対策要件	対応する 脆弱性 ID	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_3_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。

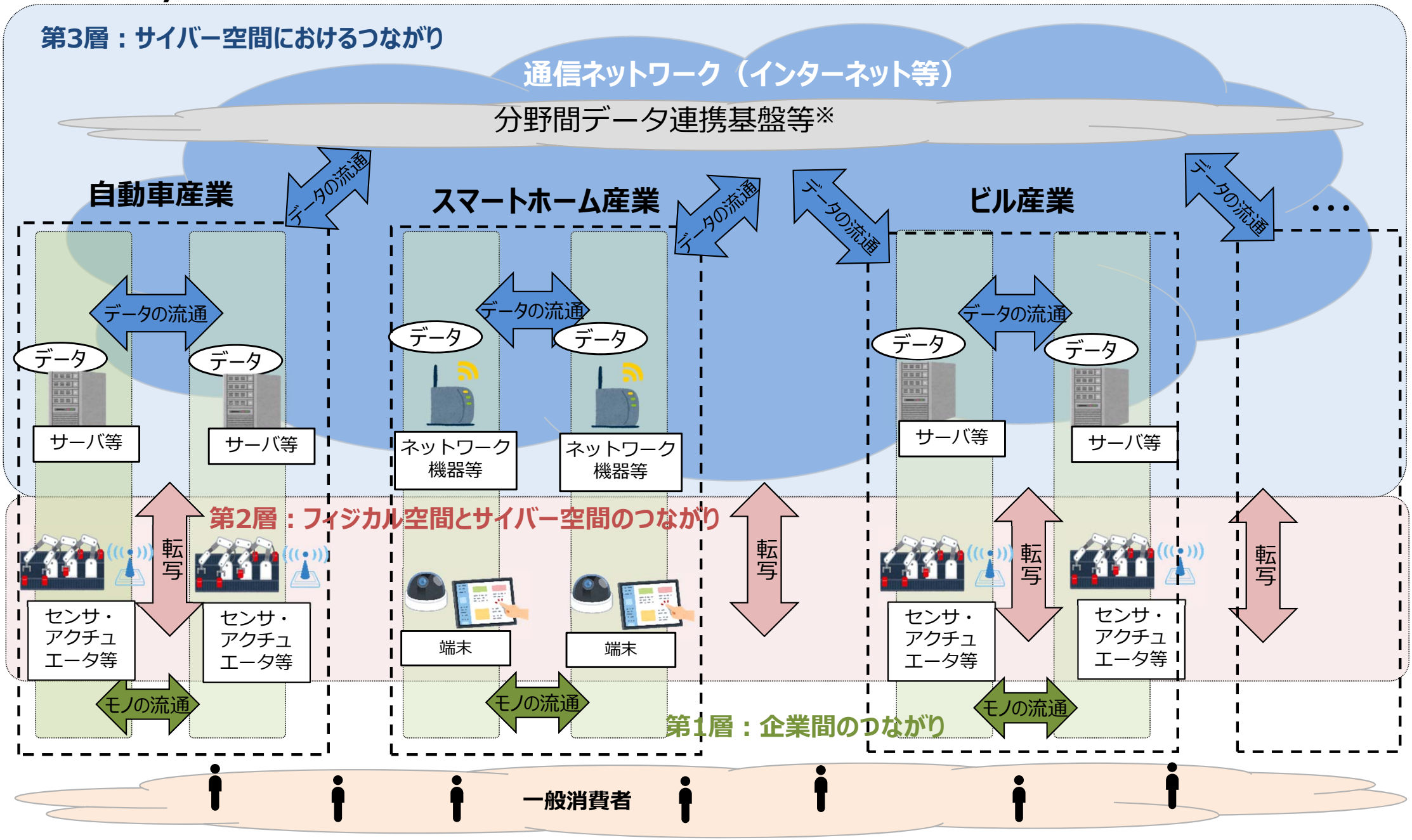
表 3.3-21 CPS.IM カテゴリの対策要件

対策要件 ID	対策要件	対応する脆弱性 ID	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_3_a_ORG	NIST Cybersecurity Framework Ver.1.1 RS.IM-1, RS.IM-2 CIS CSC 19 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 サイバーセキュリティ経営ガイドライン 指示 7 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、事業継続計画又は緊急時対応計画を継続的に改善する。	L1_3_a_ORG	NIST Cybersecurity Framework Ver.1.1 RC.IM-1, RC.IM-2 CIS CSC 19 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 サイバーセキュリティ経営ガイドライン 指示 8

添付Ａ．ユースケース
～分析対象の明確化の参考として～

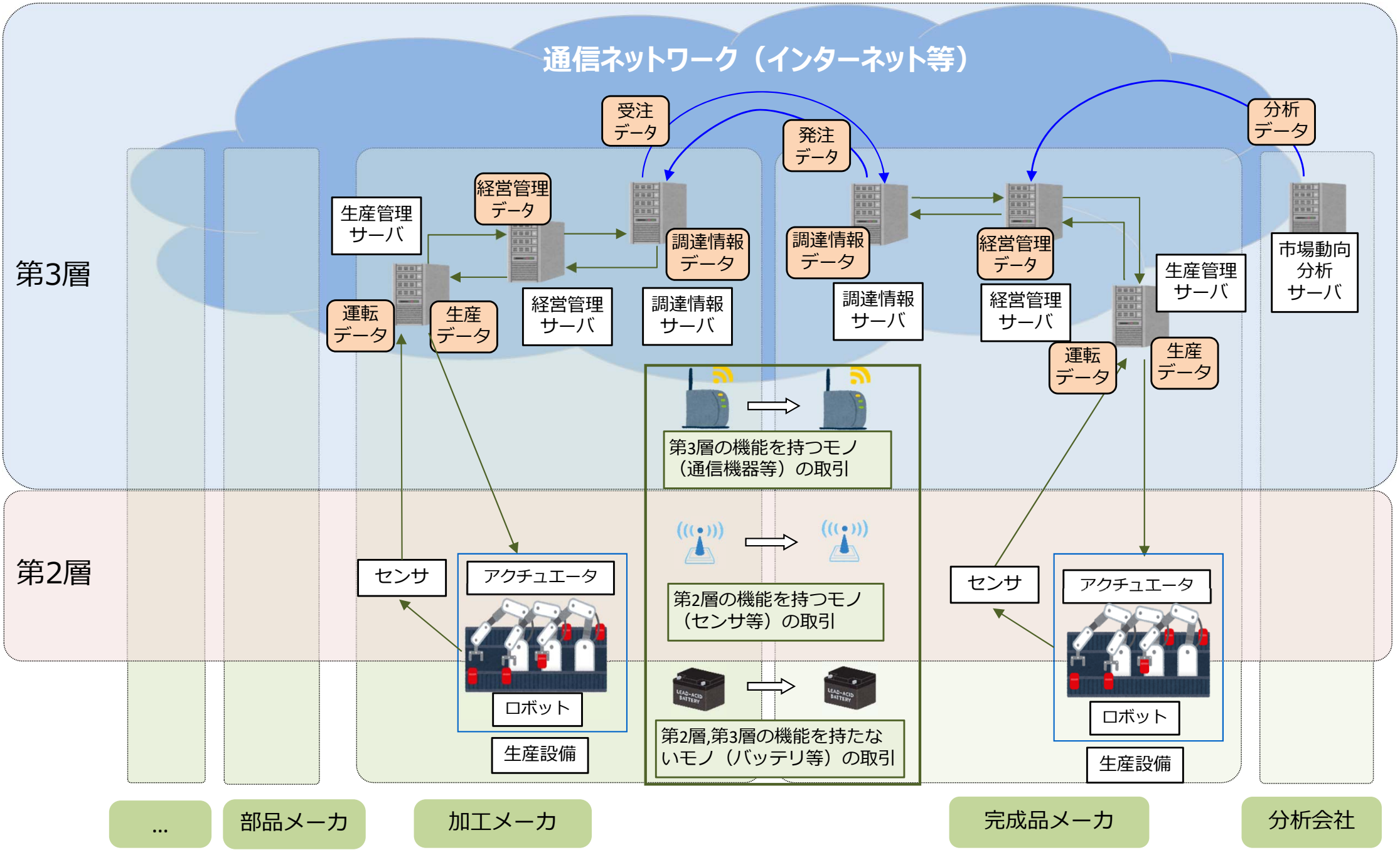
ユースケース①：「Society5.0」社会におけるモノ・データ等の繋がりの例

■「Society5.0」では、サイバー空間とフィジカル空間が高度に融合し、様々なモノやデータが企業間さらには産業間を跨いで流通。



※平成30年4月　内閣府説明資料「データ連携基盤の構築について」を参考に経済産業省が作成

ユースケース②：製造過程の例



製造過程の例のユースケース作成に当たっての整理について

１．本事例を作るに当たり想定したバリュークリエイションプロセス

■ 製造過程において、発注元企業が製品を発注し、発注先企業が発注データ(設計図など)を基に、製品を納める一連のプロセス。

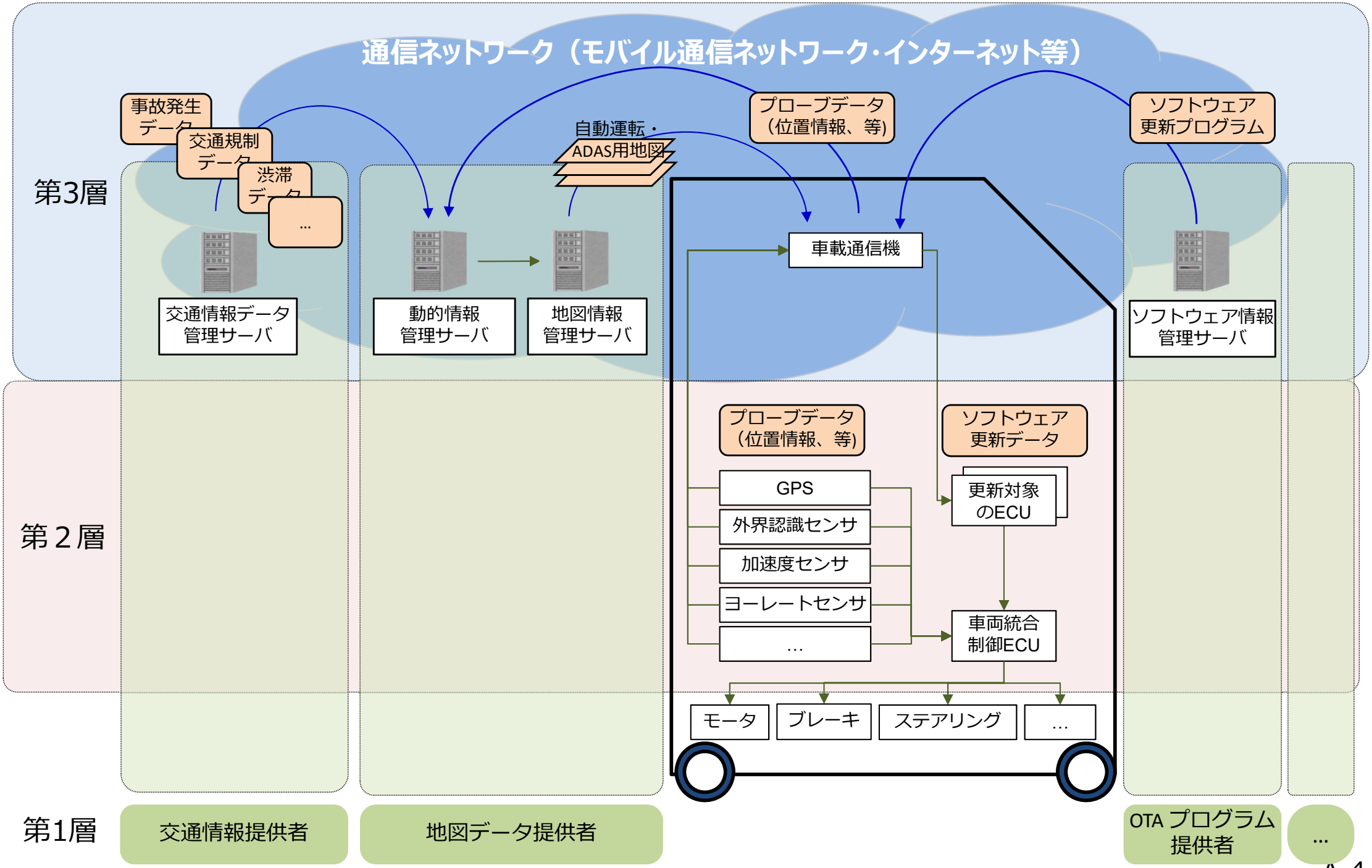
２．フレームワークの留意点を踏まえた本ユースケースの特徴

■ Society5.0への進展に伴い、製造装置にIoTが使われるようになるとともに、製造されるIoT製品も増加。
■ 市場動向分析データなど外部のデータの活用も増加。

３．資産等の各層への分類のイメージ

	分析対象の具体的イメージ
第１層	• 部品メーカ：加工メーカに部品を供給。 • 加工メーカ：部品メーカから部品の供給を受け、製品を加工。 • 完成品メーカ：加工メーカから製品の供給を受け、完成品を製造。 • 分析会社：市場動向などの分析データを完成品メーカに提供。　等
第２層	• センサ：生産設備の動作状況を監視し、その結果をデータに変換。 • アクチュエータ：生産管理データをもとに、生産設備を稼働。　等
第３層	• ネットワーク機器：データの組織外とのやりとり。 • データを取り扱うサーバ：データの保管・加工・分析等を実施。 • 取り扱うデータ – 調達情報データ：発注計画や取引会社間での取引などに関するデータ。 – 分析データ：市場動向などの分析データ。生産計画に利用。　等

ユースケース③：将来のコネクテッドカーの例



将来のコネクテッドカーの例のユースケース作成に当たっての整理について

１．本事例を作るに当たり想定したバリュークリエイションプロセス

■　車内外から得られるデータを活用し、ナビゲーション等のサービスや運転支援及び将来的には自動運転を行うプロセス。

２．フレームワークの留意点を踏まえた本ユースケースの特徴

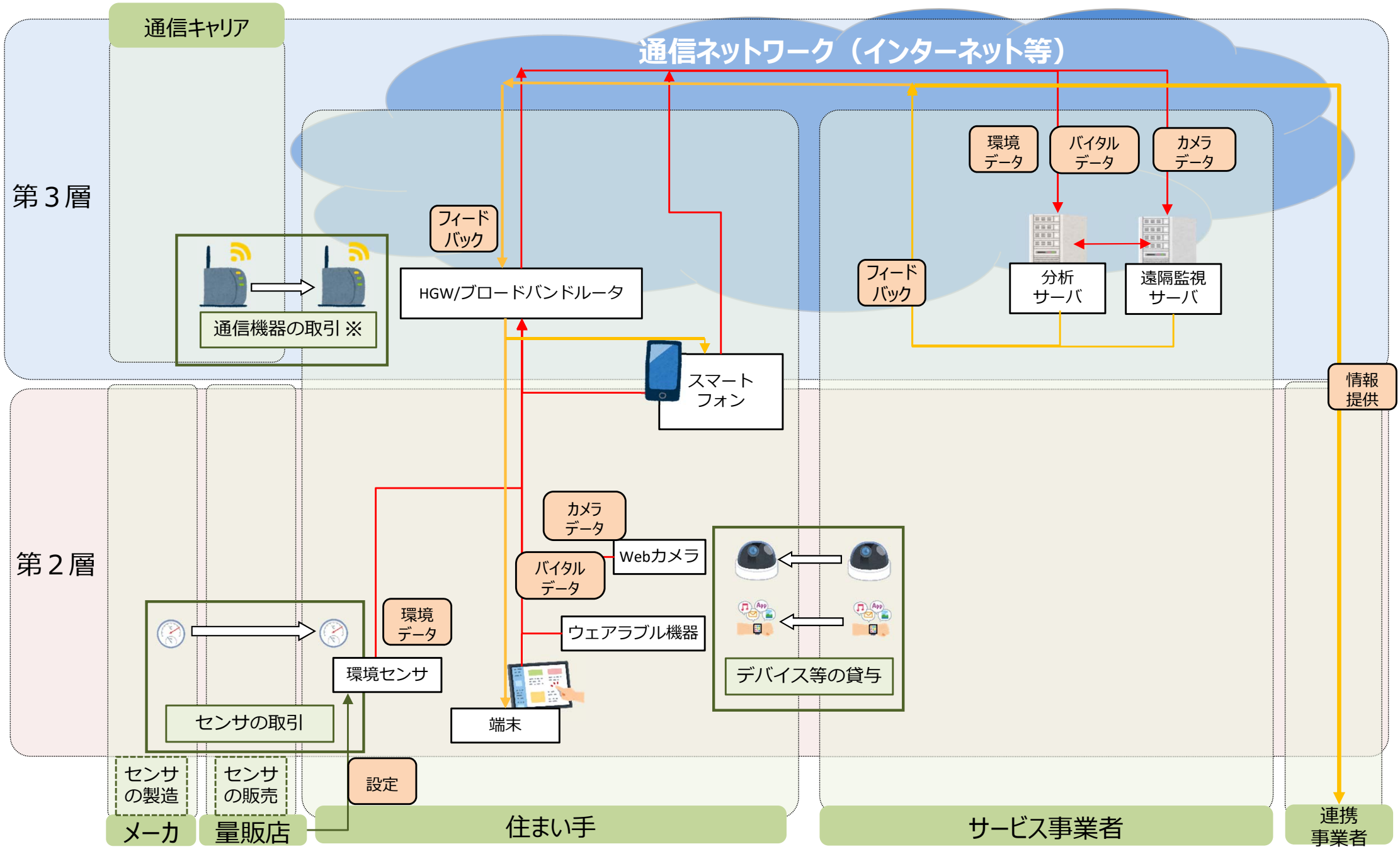
■　コネクテッド化(自動車のIoT化)の進展に伴い、車内外のデータのやり取りが発生し、フィジカル・サイバー空間並びにサイバー空間間のつながりが増加。

■　また、将来的な自動運転の実現には、外界認識センサ等による得られる周囲の情報に加え、地図情報や渋滞・交通規制情報など様々なデータのやり取りを必要とする可能性。

３．資産等の各層への分類のイメージ

	分析対象の具体的イメージ
第１層	• 交通情報提供者：交通規制・渋滞データなどを管理し、地図データ提供者等に提供。 • 地図データ提供者：プローブデータ（位置情報など）を分析し、自動車に提供。 • OTAプログラム提供者：ソフトウェアの更新プログラムを自動車に提供。 等
第２層	• 外界認識センサ：カメラ、レーダなどを周囲の障害物との距離などを測定。 • 加速度センサ：自動車の速度の変化を測定。 • 車両統合制御ECU：各種情報に基づきモータ、ブレーキ、ステアリングなどの各種アクチュエータを制御。 等
第３層	• 車載通信機：自動車内と外部との接続用の通信機器。 • データを取り扱う各種サーバ：データの保管・加工・分析等を実施。 • 取り扱うデータ －渋滞データ：個々の車両の位置情報などに基づく道路混雑データ。 －プローブデータ：自車位置・速度・経路、運転挙動情報、外界センシング情報等、自動車から収集可能な各種データ。 等

ユースケース④：スマートホームの例



スマートホームの例のユースケース作成に当たっての整理について

１．本事例を作るに当たり想定したバリュークリエイションプロセス

■ 日常生活において住まい手が購入した又はサービス事業者から貸与されたIoT機器などを通じて得られるデータを利活用し、住まい手のニーズに合ったサービスが提供されるプロセス。

２．フレームワークの留意点を踏まえた本ユースケースの特徴

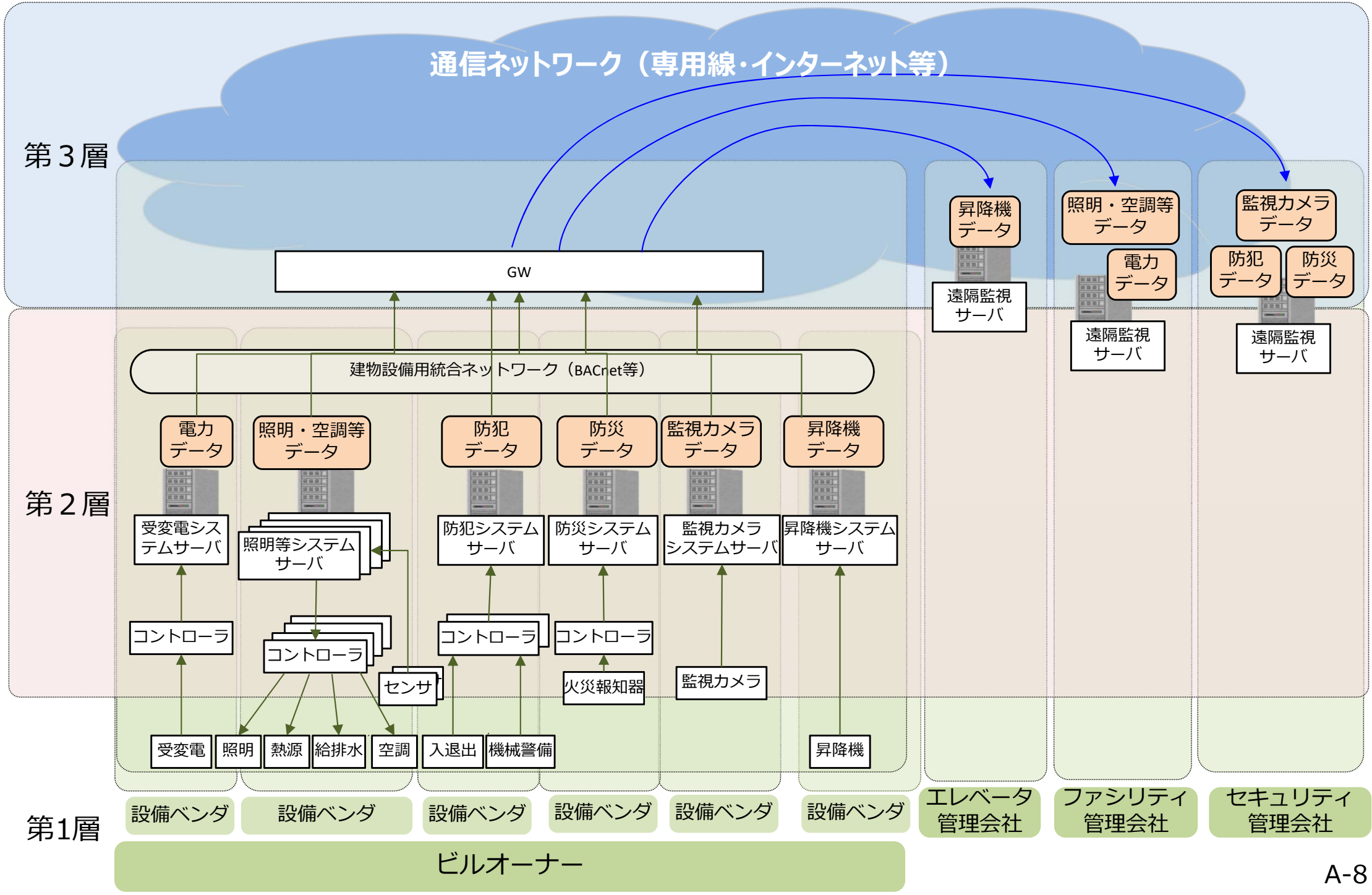
■ 家電や防犯カメラ、健康器具などがインターネットに繋がりIoT機器となっていく中で、日常生活に係るデータがネットワーク上でやりとりされるとともに、ネットワークを介してIoT機器の操作も可能となる等、サイバーとフィジカルの転写機能の信頼が重要。

■ IoT機器のメンテナンスや状態の管理について、明確な管理者が定まらないことが多い。

３．資産等の各層への分類のイメージ

	分析対象の具体的イメージ
第１層	• 住まい手：IoT機器を購入又は借受けて自宅に設置し、日常生活に係るデータを提供するとともに、それに基づくサービスを享受。 • サービス事業者：住まい手からデータを取得し、それに基づくサービスを実施。 • 通信キャリア：住まい手などに通信機器を貸与するなどして、インターネットやLTE網を提供。 • 連携事業者：サービス事業者から情報を受取り、サービスを提供。 • メーカ：インターネットに繋がるセンサなどを製造。 • 量販店：メーカが製造したセンサなどを販売、設定を実施。 等
第２層	• センサ、ウェアラブル機器、Webカメラ、ネットワーク家電：日常生活に関するデータを転写。 • 端末：データの閲覧、入力装置。 等
第３層	• HGW：データの家庭外とのやりとり。 • データを取り扱うサーバ：データの保管・加工・分析等を実施。 • 取り扱うデータ – 環境データ：温度、湿度などのデータ。 – バイタルデータ：心拍数、体温などのデータ。 等

ユースケース⑤：ビルの例



ビルの例のユースケース作成に当たっての整理について

1．本事例を作るに当たり想定したバリュークリエイションプロセス

■ ビルオーナーが、ファシリティ管理会社と契約等を行い、ビルから得られるデータを活用し、エネルギーマネジメントやビルの最適管理を行うプロセスや、遠隔地から監視・管理するプロセス。

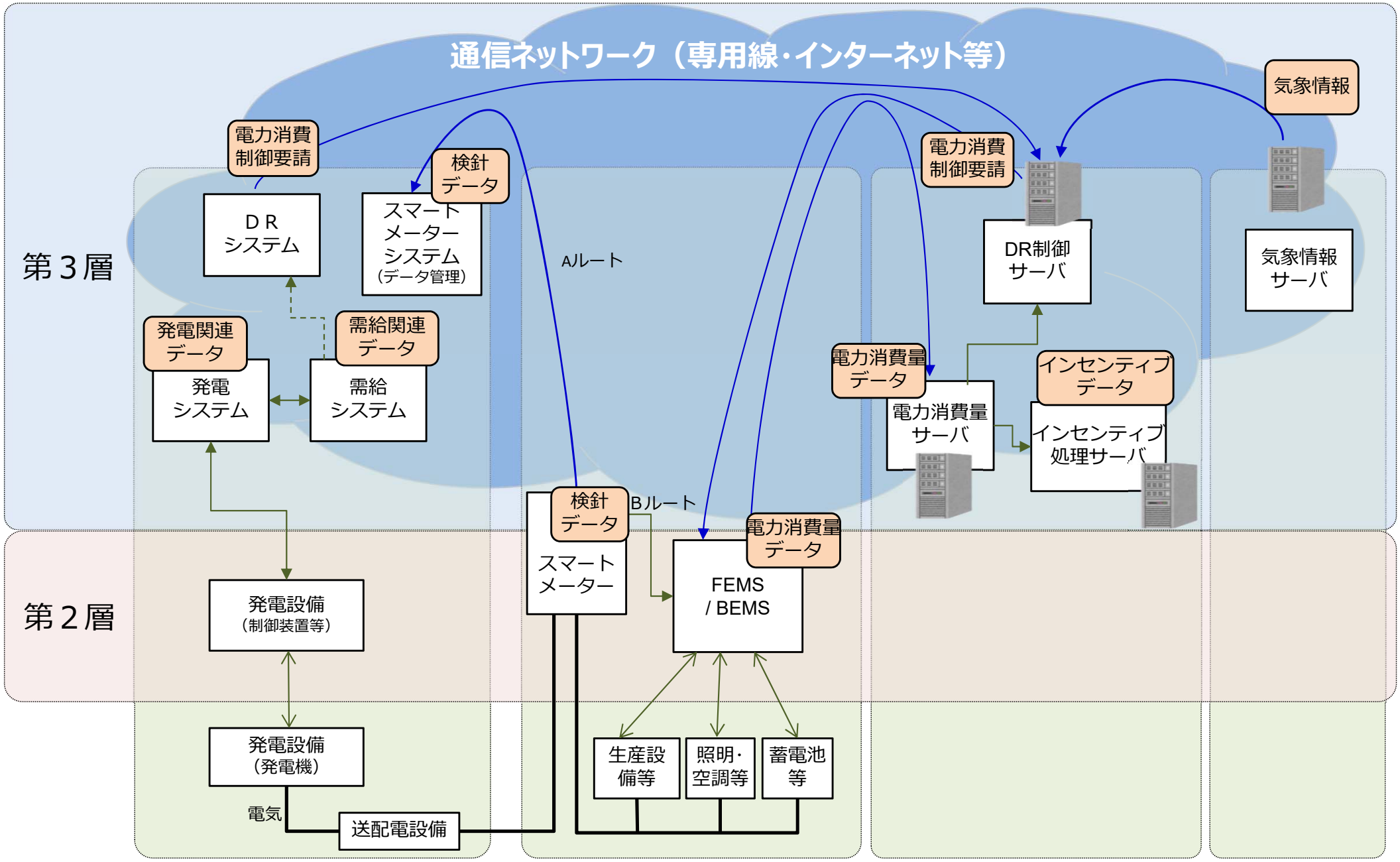
2．フレームワークの留意点を踏まえた本ユースケースの特徴

■ ビル内の数多くの制御系システムのIP化が進展。
■ ビル内の各々のシステムは、第3層の分析対象、かつ第2層の分析対象としての観点も重要視。
■ ビルの遠隔地からの監視・管理を実現するためには、電力データ、昇降機データなどさまざまなデータのやり取りが必要。
■ エレベータ監視会社、ファシリティ管理会社など、ステークホルダーが多い。

3．資産等の各層への分類のイメージ

	分析対象の具体的イメージ
第１層	• ビル：ビルシステムにより監視・管理。 • エレベータ管理会社：ビルに導入されているエレベータの運転状況などを遠隔から監視・管理。 • ファシリティ管理会社：ビルの電力使用量などを遠隔から監視・管理。 • セキュリティ管理会社：ビルを監視カメラなどにより遠隔から監視・管理。 等
第２層	• コントローラ：照明、熱源、空調などを制御。 • 監視カメラ：異常事態の発生の有無を監視。 • 統合ネットワーク（BACnet等）：データのビル内外とのやりとり。 • データを取り扱うサーバ：データの保管・加工・分析等を実施。 等
第３層	• データを取り扱うサーバ：データの保管・加工・分析等を実施。 • 取り扱うデータ －電力データ：ビルの様々な機器の電力使用量。ファシリティ管理会社が利用。 －防犯データ：入退室や機械警備などの情報を組み合わせたデータ。セキュリティ会社が利用。 等

ユースケース⑥：電力システムにおけるデマンド・レスポンスの例



EMS : Energy Management System　BEMS : Building EMS　FEMS : Factory EMS

電力システムにおけるデマンド・レスポンスの例のユースケース作成に当たっての整理について

1．本事例を作るに当たり想定したバリュークリエイションプロセス

■ 電力の需要逼迫時にインセンティブを与えることで需要を制御するデマンドレスポンスのプロセス。

2．フレームワークの留意点を踏まえた本ユースケースの特徴

■ スマートメータの利用などにより、電力供給に関するさまざまなデータのやり取りが増加。
■ 電力の自由化が進展する中で、電力供給に関わるステークホルダーが増大。

3．資産等の各層への分類のイメージ

	分析対象の具体的イメージ
第１層	• 電力会社：電力消費制御をアグリゲータに要請。 • 需要家（工場・ビル）：電力消費制御要請により、電力消費の制御を実施。 • アグリゲータ：電力会社から電力消費制御要請を受け、需要家（工場・ビル）に電力消費制御要請。 • 気象情報提供事業者：気象情報をアグリゲータに提供。 等
第２層	• スマートメータ：消費電力量を検針データに変換。 • FEMS/BEMS：工場やビルのエネルギーを管理。 等
第３層	• スマートメータ：検針データの送信。 • データを取り扱うサーバ：データの保管・加工・分析等を実施。 • 取り扱うデータ －気象情報：気温、湿度などの気象データ。電力需要予想に利用。 －電力消費制御要請：電力消費の制御量などのデータ。電力会社からアグリゲータ、アグリゲータから需要家への電力消費制御要請に利用。 等

添付B リスク源と対策要件の対応関係

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

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
1_1	組織として平時のリスク管理体制を構築し、適切に運用すること	自組織で管理している領域から保護すべきデータが漏洩する	・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・入力確認の不備を突いたインジェクション攻撃(例：SQLインジェクション、XSS) ・ネットワーク上の通信の盗聴 ・保護が必要なエリアに対する不正なヒトの物理的な侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・正規ユーザによる内部不正	L1_1_a_ORG	[ソシキ] ・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.AM-6
						・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、自組織の取引に関係する者（サプライヤー、第三者プロバイダ等を含む）に共有する。	CPS.BE-2
						・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、その内容について取引先と合意する。	CPS.SC-1
						・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・システムを管理するためのシステム開発ライフサイクルを導入する。	CPS.IP-3
				L1_1_a_PEO	[ヒト] ・自身が関わりうるセキュリティやセーフティに関するリスクに対して十分な認識を有していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
					[ヒト] ・ヒトに関わるセキュリティやセーフティに関係するリスクに対するガバナンスが十分でない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	CPS.SC-5
						・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	CPS.IP-9
				L1_1_a_COM	[モノ] ・モノのセキュリティ状況やネットワーク接続状況が適切に管理(例：資産の棚卸し、モニタリング)されていない	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-5
						・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
				L1_1_a_SYS	[システム] ・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	CPS.RA-1
						・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。	CPS.RA-3
						・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機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-4
						・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。	CPS.RA-5
						・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。	CPS.RA-6
						・リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。	CPS.RM-2
					[システム] ・自組織のシステムにおいて、対処すべき脆弱性が放置されている	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	CPS.IP-2
						・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.IP-10
						・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.MA-1
						・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2
						・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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
						・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.CM-7
					[システム] ・保護すべきデータが格納されたシステムにおいて、セキュアでない設定がなされている	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	CPS.PT-2
					[システム] 保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
						・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	CPS.AC-5
						・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	CPS.AC-6
						・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	CPS.AC-9
					[システム] ・IoT機器、サーバ等の設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.IP-5
						・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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	CPS.PT-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及び記録、監視を実施する。	CPS.CM-2
					[システム] ・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	CPS.PT-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・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・制御、アクセス監視・制御を実施する。	CPS.CM-1
						・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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.CM-3
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
				L1_1_a_DAT	[データ] ・自組織で管理しているデータの保護に係る区分が明確になっていない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
					[データ] ・定められた機密区分に沿った情報の保護が実装されていない	・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・情報を適切な強度の方式で暗号化して保管する。	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。	CPS.DS-3
						・情報を送受信する際に、情報そのものを暗号化して送受信する。	CPS.DS-4
						・送受信する情報データ、保管データする情報の暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。	CPS.DS-5
						・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	CPS.DS-9
				L1_1_a_PRO	[プロシージャ] ・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	・セキュリティポリシーを策定し、自組織及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。	CPS.GV-1
						・セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。	CPS.GV-4
						・自組織内における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し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。	CPS.RM-1
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-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。	CPS.SC-7
						・取引先等の関係する他組織との契約が終了する際（例：契約期間の満了、サポートの終了）に実施すべきプロシージャを策定し、運用する。	CPS.SC-10
						・サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。	CPS.SC-11
						・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	CPS.IP-7
		自組織で管理している領域において保護すべきデータが改ざんされる	・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・通信系路上でデータを改ざんする中間者攻撃等 ・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・正規ユーザによる内部不正 ・保護が必要なエリアに対する不正なヒトの物理的な侵入 ・保護が必要なデータを扱う媒体の物理的な破壊	L1_1_b_ORG	[ソシキ] ・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.AM-6
						・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、自組織の取引に関係する者（サプライヤー、第三者プロバイダ等を含む）に共有する。	CPS.BE-2
						・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、その内容について取引先と合意する。	CPS.SC-1
						・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・システムを管理するためのシステム開発ライフサイクルを導入する。	CPS.IP-3
				L1_1_b_PEO	[ヒト] ・自身が関わりうるセキュリティやセーフティに関係するリスクに対して十分な認識を有していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
					[ヒト] ・ヒトに関わるセキュリティやセーフティに関係するリスクに対するガバナンスが十分でない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	CPS.SC-5
						・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	CPS.IP-9
				L1_1_b_COM	[モノ] ・情報システムや産業用制御システムを構成しているモノのセキュリティ状況やネットワーク接続状況が適切に管理(例：資産の棚卸し、モニタリング)されていない	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-5
						・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
				L1_1_b_SYS	[システム] ・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	CPS.RA-1
						・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。	CPS.RA-3
						・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機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-4
						・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。	CPS.RA-5
						・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。	CPS.RA-6
						・リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。	CPS.RM-2
					[システム] ・保護すべきデータが格納されたシステムにおいて、セキュアでない設定がなされている	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	CPS.PT-2
					[システム] ・保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
						・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	CPS.AC-5
						・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	CPS.AC-6
						・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	CPS.AC-9

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
					[システム] ・早期にネットワーク上での異常(例：なりすまし、メッセージの改ざん)を素早く検知し、対処するような仕組みがシステムに実装されていない	・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。	CPS.AE-3
						・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.CM-3
						・セキュリティ事象の検知プロセスを継続的に改善する。	CPS.DP-4
				L1_1_b_PRO	[プロシージャ] ・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	・セキュリティポリシーを策定し、自組織及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。	CPS.GV-1
						・セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。	CPS.GV-4
						・自組織内における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し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。	CPS.RM-1
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-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。	CPS.SC-7
						・取引先等の関係する他組織との契約が終了する際（例：契約期間の満了、サポートの終了）に実施すべきプロシージャを策定し、運用する。	CPS.SC-10
						・サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。	CPS.SC-11
						・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	CPS.IP-7
				L1_1_b_DAT	[データ] ・通信路及び通信路上のデータが十分に保護されていない	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	CPS.DS-3
						・情報を送受信する際に、情報そのものを暗号化して送受信する。	CPS.DS-4
					[データ] ・取り扱うデータに改ざんを検知するメカニズムがない	・送受信・保管する情報に完全性チェックメカニズムを使用する。	CPS.DS-11
		サービス拒否攻撃、ランサムウェアへの感染等に より、自組織のデータを取り扱うシステムが停止する	・システムを構成するサーバ等の電算機器、通信機器等に対するサービス拒否攻撃 ・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・妨害電波の発信	L1_1_c_ORG	[ソシキ] ・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.AM-6
						・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、自組織の取引に関係する者（サプライヤー、第三者プロバイダ等を含む）に共有する。	CPS.BE-2
						・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、その内容について取引先と合意する。	CPS.SC-1
						・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・システムを管理するためのシステム開発ライフサイクルを導入する。	CPS.IP-3
				L1_1_c_PEO	[ヒト] ・自身が関わりうるセーフティやセキュリティに関わるリスクに対して十分な認識を有していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
					[ヒト] ・ヒトに関わるセーフティやセキュリティに関係するリスクに対するガバナンスが十分でない	・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
						・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	CPS.IP-9
				L1_1_c_COM	[モノ] ・情報システムや産業用制御システムを構成しているモノのセキュリティ状況やネットワーク接続状況が適切に管理（例：資産の棚卸し、モニタリング）されていない	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-5
						・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
				L1_1_c_SYS	[システム] ・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	CPS.RA-1
						・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。	CPS.RA-3
						・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。	CPS.RA-4
						・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。	CPS.RA-5
						・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。	CPS.RA-6
						・リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。	CPS.RM-2
					[システム] ・IoT、サーバ等に対する通信を適切に制御していない	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	CPS.PT-2
						・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	CPS.CM-1
					[システム] ・IoT、サーバ等に対する物理的な妨害（例：妨害電波）に対処できていない	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.IP-5
						・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.CM-2
					[システム] ・IoT機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する。	CPS.DS-6
						・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	CPS.DS-7

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
				L1_1_c_PRO	[プロシージャ] ・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	・セキュリティポリシーを策定し、自組織及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。	CPS.GV-1
						・セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。	CPS.GV-4
						・自組織内における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し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。	CPS.RM-1
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-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。	CPS.SC-7
						・取引先等の関係する他組織との契約が終了する際（例：契約期間の満了、サポートの終了）に実施すべきプロシージャを策定し、運用する。	CPS.SC-10
						・サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。	CPS.SC-11
						・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	CPS.IP-7
		法制度等で規定されている水準のセキュリティ対策を実装できない	All threats	L1_2_a_ORG	[ソシキ] ・遵守すべき法制度等を認識していないか、法制度に準拠した組織内のルールを策定・運用していない	・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する。	CPS.GV-2
						・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する。	CPS.DP-2
				L1_2_a_PEO	[ヒト] ・遵守すべき法制度等を認識していないか、法制度に準拠した組織内のルールを遵守していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
				L1_2_a_COM	[モノ] ・法制度等で一定の保護を義務付けられている種のモノが、要求される水準の保護を適用されていない	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	CPS.GV-2
				L1_2_a_SYS	[システム] ・法制度等で一定の保護を義務付けられている種のシステムが、要求される水準の保護を適用されていない	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	CPS.GV-2
				L1_2_a_PRO	[プロシージャ] ・組織内で規定されているプロシージャが関連する法規制等を遵守するような内容となっていない	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	CPS.GV-2
				L1_2_a_DAT	[データ] ・法制度等で一定の保護を義務付けられている種のデータが、要求される水準の保護を適用されていない	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	CPS.GV-2
1_2	組織としてセキュリティインシデント発生時においても適切に自組織の事業を継続すること	自組織のセキュリティインシデントにより自組織が適切に事業継続できない	All threats	L1_3_a_ORG	[ソシキ] ・セキュリティ事象を的確に検知するための体制が構築されていない	・セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	CPS.AE-2
						・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・セキュリティ事象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。	CPS.DP-1
						・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する。	CPS.DP-2
						・監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。	CPS.DP-3
						・セキュリティ事象の検知プロセスを継続的に改善する。	CPS.DP-4
					[ソシキ] ・セキュリティインシデントに的確に対応するための体制が構築されていない	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	CPS.AE-2
						・セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する。	CPS.IM-1
						・セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又は緊急事対応計画を継続的に改善する。	CPS.IM-2
				L1_3_a_PEO	[ヒト] ・セキュリティインシデント発生時に適切なアクションを取ることができない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
						・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
				L1_3_a_COM	[モノ] ・セキュリティインシデントにより被害を受けた自組織の事業の範囲(製品等)を特定することができない	・自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。	CPS.AM-2
						・重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。	CPS.AM-3
						・セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。	CPS.AN-1
				L1_3_a_SYS	[システム] ・セキュリティインシデントを適切に検知するための機器等が導入されていないか、あるいは正しく運用されていない	・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。	CPS.AE-3
						・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・制御、アクセス監視・制御を実施する。	CPS.CM-1
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
				L1_3_a_PRO	[プロシージャ] ・自組織におけるセキュリティインシデントへの対応手順が策定されていない	・セキュリティ事象の危険度の判定基準を定める。	CPS.AE-5
						・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-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、自組織及び関係する他組織を含む社会全体への影響を把握する。	CPS.AN-1
						・セキュリティインシデント発生後に、デジタルフォレンジックを実施する。	CPS.AN-2
						・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。	CPS.AN-3
						・セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う。	CPS.MI-1
					[プロシージャ] ・事業継続計画にセキュリティインシデントが位置づけられておらず、セキュリティインシデント発生時に自組織の事業継続に支障が生じる	・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。	CPS.RP-3
						・セキュリティインシデント発生後の情報公表時のルールを策定し、運用する。	CPS.CO-1
						・事業継続計画又は緊急事対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。	CPS.CO-2
						・復旧活動について内部及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、事業継続計画又は緊急事対応計画の中に位置づける。	CPS.CO-3

#	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	リスク源 脆弱性ID	リスク源 脆弱性	対策要件	対策要件ID
				L1_3_a_DAT	[データ] ・セキュリティインシデント発生時に事業を継続するために必要なデータが、適切に準備されていない、又は準備されてるが適切に機能しない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.AT-2
						・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、テストする。	CPS.IP-4
						・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。	CPS.RP-3
		自組織のセキュリティインシデントにより関係する他組織が適切に事業継続できない	All threats	L1_3_b_ORG	[ソシキ] ・自組織のモノ/システム/データのサイバー空間における他組織との連携状況を把握していない	・組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する。	CPS.AM-4
						・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-5
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
					[ソシキ] ・自組織と他組織(サプライヤー等)とのフィジカル空間における連携状況および責任分界を把握していない	・自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める。	CPS.AM-7
						・サプライチェーンにおいて、自組織が担う役割を特定し共有する。	CPS.BE-1
						・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。	CPS.BE-3
						・自組織内における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し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。	CPS.RM-1
				L1_3_b_PEO	[ヒト] ・他組織のヒトが自組織のセキュリティ事象発生時に適切なアクションを取ることができない	・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、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	CPS.SC-9
						・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.AT-2
						自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
						・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	CPS.RP-2
				L1_3_b_COM	[モノ] ・セキュリティ事象による被害を受けたモノ(製品)・サービスが生じる	・セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ（製品）に対して適切な対応を行う。	CPS.RP-4
					[モノ] ・自組織が提供する/されるモノ(製品)に関する記録(例:製造日/識別ナンバー/提供先)が保持されていない	・自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。	CPS.AM-2
						・重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。	CPS.AM-3
				L1_3_b_PRO	[プロシージャ] ・関係する他組織と連携したセキュリティ事象対応手順が策定されていない	・関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。	CPS.AE-4
						・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	CPS.RP-2
		関係する他組織のセキュリティインシデントにより自組織が適切に事業継続できない	All threats	L1_3_c_ORG	[ソシキ] ・自組織のモノ/システム/データのサイバー空間における他組織との連携状況を把握していない	・組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する。	CPS.AM-4
						・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-5
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
					[ソシキ] ・自組織と他組織(サプライヤー等)とのフィジカル空間における連携状況および責任分界を把握していない	・自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める。	CPS.AM-7
						・サプライチェーンにおいて、自組織が担う役割を特定し共有する。	CPS.BE-1
						・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。	CPS.BE-3
						・自組織内における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し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。	CPS.RM-1
				L1_3_c_PEO	[ヒト] ・自組織のヒトが他組織のセキュリティ事象発生時に適切なアクションを取ることができない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
						・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	CPS.RP-2
				L1_3_c_PRO	[プロシージャ] ・関係する他組織と連携したセキュリティ事象対応手順が策定されていない	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	CPS.RP-2
1_3	フィジカル空間での製品・サービスが、望まれる品質を備えて入荷又は出荷されること	製品・サービスの提供チャネルでセキュリティ事象が発生し、機器の破損等の意図しない品質劣化が生じる	・悪意を持った自組織内外のヒトによる不正改ざん ・正規の機器を模した偽造品の挿入	L1_1_d_ORG	[ソシキ] ・製品・サービスを調達する際、それが信頼できるものかを確認していない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
				L1_1_d_PEO	[ヒト] ・自組織の調達に関わる要員が、調達に係るセキュリティリスクを十分に認識していない。	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
				L1_1_d_COM	[モノ] ・調達する製品・サービスが十分な物理的保護を実施されていない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。	CPS.DS-8
				L1_1_d_PRO	[プロシージャ] ・製品・サービスの調達時に、調達品の適格性を確認するプロシージャが存在しない	・送受信・保管する情報に完全性チェックメカニズムを使用する。	CPS.DS-11
						・ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。	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。	CPS.DS-13

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

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
2_共通	下記機能の双方 ・フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、サイバー空間へ送る機能 ・サイバー空間から受け取ったデータに基づいて、一定のルールに基づいて、モノを制御したり、データを可視化したりする機能	脆弱性を悪用してIoT機器内部に不正アクセスされ、事前に想定されていない動作をする	・攻撃ツール等を利用したIoT機器におけるセキュリティ上の脆弱性を利用したマルウェア感染	L2_1_a_ORG	[ソシキ] ・情報システムや産業用制御システムに接続している自組織のIoT機器のセキュリティ対策状況(ソフトウェア構成情報、パッチ適用状況等)を把握できていない	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	CPS.IP-2
						・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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
					[ソシキ] ・利用しているIoT機器に関わる脆弱性情報、脅威情報を収集・分析し、適切に対応していない。	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・セキュリティインシデントへの対応、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する。	CPS.IP-7
						・保護技術の有効性について、適切なパートナーとの間で情報を共有する。	CPS.IP-8
						・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.IP-10
						・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 ・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。	CPS.MA-1
						・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。	CPS.MA-1
						・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2
				L2_1_a_COM	[モノ] ・利用しているIoT機器が十分なセキュリティ機能を実装していない	・IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-4
						・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.RA-6
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。	CPS.DS-15
				L2_1_a_PRO	[プロシージャ] ・調達時に、適切なレベルのセキュリティ機能が実装されているかを確認するプロシージャがない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。	CPS.DS-15
						・IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-4
						・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.RA-6
					[プロシージャ] ・IoT機器の誤動作を検知した後の対応手順が定義されていない	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
		正規のユーザーになりすましてIoT機器内部に不正アクセスされ、事前に想定されていない動作をする	・窃取したID等を利用した正規ホストへのなりすまし ・セキュリティが実装されていない脆弱なプロトコルを悪用した不正アクセス	L2_1_b_ORG	[ソシキ] ・ネットワークの適正利用を確認していない	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	CPS.PT-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・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・制御、アクセス監視・制御を実施する。	CPS.CM-1
				L2_1_b_COM	[モノ] ・セキュリティの観点において強度が十分でない設定(パスワード、ポート等)がなされている	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	CPS.PT-2
				L2_1_b_SYS	[システム] ・通信相手に対するアクセス制御が十分でない	・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ。	CPS.AC-4
						・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	CPS.AC-7
						・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	CPS.AC-8
						・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	CPS.AC-9
				L2_1_b_PRO	[プロシージャ] ・IoT機器のセキュリティ設定手順が定められていない	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
					[プロシージャ] ・IoT機器の誤動作を検知した後の対応手順が定義されていない	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
		遠隔からIoT機器を管理するシステムに不正アクセスされ、IoT機器に不正な入力をされ、事前に想定されていない動作をする。	・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・IoT機器を管理するシステムからIoT機器への不正なコマンド送信	L2_1_c_ORG	[ソシキ] ・IoT機器を管理するシステムのセキュリティ対策状況(ソフトウェア構成情報、パッチ適用状況等)を把握できていない	・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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
				L2_1_c_SYS	[システム] ・システム管理権限に対するアクセス制御が十分でない	・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	CPS.AC-5
						・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	CPS.AC-6
					[システム] ・システムにおいて対処すべき脆弱性が適切に対処されていない	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	CPS.IP-2
						・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.MA-1
						・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。	CPS.MA-1
						・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2
						・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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
						・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.CM-7
					[プロシージャ] ・IoT機器の誤動作を検知した後の対応手順が定義されていない	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1

#	機能	想定されるセキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
		サービス拒否攻撃等により、IoT機器や通信機器等の機能が停止する	・IoTシステムを構成するIoT機器、通信機器等に対するサービス拒否攻撃	L2_1_d_SYS	[システム] ・IoT機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する。	CPS.DS-6
						・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	CPS.DS-7
						・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、テストする。	CPS.IP-4
					[プロシージャ] ・IoT機器の停止を検知した後の対応手順が定義されていない	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
2_1	サイバー空間から受け取ったデータに基づいて、一定のルールに基づいて、モノを制御したり、データを可視化したりする機能	正常動作・異常動作に関わらず、安全に支障をきたすような動作をする	・不正なエンティティによるコマンドインジェクション攻撃 ・サイバー空間からの許容範囲外のインプットデータ ・マルウェアによる制御信号の改ざん	L2_2_a_ORG	[ソシキ] ・機器を調達する際、安全性を実装しているかを確認していない	・IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-4
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
						・ネットワークにつながることを踏まえた安全性を実装するIoT機器を導入する。	CPS.PT-3
				L2_2_a_COM	[モノ] ・インプットされたデータを検証する仕組みが無い	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行うIoT機器を導入する。 ・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.CM-3
				L2_2_a_SYS	[システム] ・稼動するシステムとして、安全計装が考慮されていない。	・IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-4
						・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.RA-6
				L2_2_a_PRO	[プロシージャ] ・安全に支障をきたしうる機器等の兆候を発見した際のプロシージャが定められていない	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
2_2	フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、サイバー空間へ送る機能	データがIoT機器・サイバー空間間の通信路上で改ざんされる	・通信系路上でデータを改ざんする中間者攻撃等	L2_3_a_ORG	[ソシキ] ・機器を調達する際、改ざん検知機能及び改ざん防止機能を実装しているかを確認していない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。	CPS.DS-15
		(監視が行き届かない場所に設置された機器の運用中、あるいは廃棄後の盗難等の後)改ざんされたIoT機器がネットワーク接続され、故障や正確でないデータの送信等が発生する	・盗難等により不正な改造を施されたIoT機器によるネットワーク接続 ・悪意を持った自組織内外のヒトによる不正改ざん ・センサーの測定値、閾値、設定の改ざん	L2_3_b_ORG	[ソシキ] ・自組織の情報システムや産業用制御システムに接続している機器の状態を把握できていない	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
				L2_3_b_PEO	[ヒト] ・自組織内外のヒトによるIoT機器に対する物理的な不正行為を防げない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	CPS.SC-5
						・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、監視力メラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.CM-2
				L2_3_b_COM	[モノ] ・利用している機器に耐タンパー性がなく、物理的な改ざんを防げない	・保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。	CPS.DS-8
				L2_3_b_SYS	[システム] ・定期的に接続機器の完全性を検証していない	・IoT機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。	CPS.DS-10
						・ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。	CPS.DS-12
					[システム] ・不正な機器がネットワークに接続されたことを適切に検知できない。	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
					[システム] ・IoT機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視力メラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.IP-5
						・IoT機器、サーバ等の本体に対して、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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	CPS.PT-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及び記録、監視を実施する。	CPS.CM-2
				L2_3_b_DAT	[データ] ・IoT機器の廃棄時に、データを削除（又は読み取りできない状態に）する手順がない	・IoT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする。	CPS.IP-6
		品質や信頼性の低いIoT機器がネットワーク接続され、故障や正確でないデータの送信、想定していない通信先へのデータ送信等が発生する	・品質や信頼性の低いIoT機器のネットワーク接続 ・正規の機器を模した偽造品の挿入	L2_3_c_ORG	[ソシキ] ・IoT機器を調達する際、調達製品が信頼できるものかを確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-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。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
					[ソシキ] ・運用時にIoT機器やソフトウェアが正規品である（改ざんされていない）ことを確認していない	・IoT機器やソフトウェアが正規品であることを定期的（起動時等）に確認する。	CPS.DS-13

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
				L2_3_c_SYS	[システム] ・不正な機器によるネットワーク接続（有線あるいは無線）を防止できない	・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、監視力メラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・無線接続先（ユーザーやIoT機器、サーバ等）を正しく認証する。	CPS.AC-3
						・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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
					[システム] ・組織外部への不正な通信を適切に検知し、遮断する等の対応ができない	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	CPS.DS-9
						・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・制御、アクセス監視・制御を実施する。	CPS.CM-1
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
					[システム] ・サイバー空間および正規の機器に接続する機器が正規のものかを確認する仕組みが実装されていない	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・IoT機器やソフトウェアが正規品であることを定期的（起動時等）に確認する。	CPS.DS-13
				L2_3_c_PRO	[プロシージャ] ・IoT機器を調達する際に、調達製品が信頼できるものかを確認するプロシージャがない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-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。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
		計測機能に対する物理的な不正行為により、正確でないデータの送信等が発生する	・悪意を持った自組織内外のヒトによる計測機能に対する不正行為	L2_3_d_ORG	[ソシキ] ・IoT機器を調達する際、調達製品が計測セキュリティを考慮しているものかを確認していない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。	CPS.DS-15
				L2_3_d_SYS	[システム] ・IoT機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	・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、監視力メラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.IP-5
						・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.CM-2

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

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
3_共通	下記すべてに関わる ・データを加工・分析する機能 ・データを保管する機能 ・データを送受信する機能	サービス拒否攻撃により、関係する他組織における自組織のデータを取り扱うシステムが停止する	・システムを構成するサーバ等の電算機器、通信機器等に対するサービス拒否攻撃 ・妨害電波の発信	L3_3_b_ORG	[ソシキ] ・データの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-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。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
		攻撃の有無に関わらず、データを取り扱うシステムが停止する	・品質や信頼性の低いシステムによるサービス提供	L3_3_c_ORG	[ソシキ] ・サービスサプライヤーに対して、組織、システム等の信頼性を契約前、契約後に確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-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。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
				L3_3_c_SYS	[システム] ・IoT機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する。	CPS.DS-6
						・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	CPS.DS-7
						・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、テストする。	CPS.IP-4
		サイバー空間におけるデータ保護を規定する法規制等への違反が発生する	・データ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・データ保管エリアに対する不正なエンティティの物理的な侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし	L3_4_a_ORG	[ソシキ] ・保護すべきデータの管理に関する組織内の責任が明確でない	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.AM-6
					[ソシキ] ・対応が必要なデータ保護に関する法規制等を十分に認識してない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
				L3_4_a_PEO	[ヒト] ・自組織の保護すべきデータのセキュリティ上の扱いについて、関係者が十分に認識していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
				L3_4_a_PRO	[プロシージャ] ・データの取り扱いについて、必要なプロシージャを規定していない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
					[プロシージャ] ・データの取り扱いについて、必要なプロシージャを満たしているかを確認していない	・データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する。	CPS.DS-14
				L3_4_a_DAT	[データ] ・複数の組織、システム等に個人情報等が分散して所在している	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
					[データ] 自組織で扱うデータが保護が必要な特定の種類のデータであることが識別されていない	・組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取り決める。	CPS.DS-1
		一部の関係者だけで共有する秘匿性の高いデータのセキュリティ要求が設定・対応されていない	・データ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・データ保管エリアに対する不正なエンティティの物理的な侵入 ・正規ユーザによる内部不正 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし	L3_4_b_ORG	[ソシキ] ・対応が必要なデータ保護に関する法規制等を十分に認識してない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
				L3_4_b_PEO	[ヒト] ・自組織の保護すべきデータのセキュリティ上の扱いについて、関係者が十分に認識していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
				L3_4_b_PRO	[プロシージャ] ・データの取り扱いについて、必要なプロシージャを規定していない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
					[プロシージャ] ・データの取り扱いについて、必要なプロシージャを満たしているかを確認していない	・データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する。	CPS.DS-14
				L3_4_b_SYS	[システム] ・データを扱うシステムにおいてデータの秘匿性に応じた設計がなされていない	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	CPS.AC-7
						・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	CPS.AC-9
						・情報を適切な強度の方式で暗号化して保管する。	CPS.DS-2
				L3_4_b_DAT	[データ] ・複数の組織、システム等に個人情報等が分散して所在している	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
					[データ] 自組織で扱うデータが保護が必要な特定の種類のデータであることが識別されていない	・組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取り決める。	CPS.DS-1
3_1	データを加工・分析する機能	関係する他組織で管理している(データ加工・分析)領域から自組織の保護すべきデータが漏洩する	・他組織の管理するデータ加工・分析システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・他組織の管理するデータ加工・分析エリアに対する不正なエンティティの物理的な侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・他組織のエンティティによる保護すべきデータの適切でない持出行為	L3_1_b_ORG	[ソシキ] ・データを加工・分析する組織、システム等の安全性・信頼性を契約前、契約後に確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-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。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
				L3_1_b_PEO	[ヒト] ・データの加工・分析を委託する組織における要員の信頼性を契約前、契約後に確認していない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	CPS.SC-5

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
				L3_1_b_DAT	[データ] ・セキュリティ水準が統一されていない複数の組織、システム等に自組織の保護すべき情報が分散して所在している	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
		データ加工・分析システムが誤動作することで、適切でない分析結果が出力される	・データ加工・分析システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・データ加工・分析システムに対する攻撃コードを含んだ許容範囲外のインプットデータ	L3_3_d_ORG	[ソシキ] ・データを加工・分析する組織、システム等の安全性・信頼性を契約前、契約後に確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-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。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
				L3_3_d_SYS	[システム] ・データを加工・分析するシステムにおいて、セキュアでない設定がなされている	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	CPS.PT-2
					[システム] ・データを加工・分析するシステムにおいて、対処すべき脆弱性が放置されている	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	CPS.IP-2
						・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.IP-10
						・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.MA-1
						・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2
						・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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
						・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.CM-7
					[システム] ・システム上でデータが十分に保護されていない	・情報を適切な強度の方式で暗号化して保管する。	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。	CPS.DS-3
						・情報を送受信する際に、情報そのものを暗号化して送受信する。	CPS.DS-4
					[システム] インプットとなるデータを十分に確認していない	・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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.CM-3
						・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	CPS.CM-4
					[システム] ・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	CPS.PT-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・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・制御、アクセス監視・制御を実施する。	CPS.CM-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
3_2	データを保管する機能	自組織で管理している(データ保管)領域から関係する他組織の保護すべきデータが漏洩する	・他組織の管理するデータ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・他組織の管理するデータ保管エリアに対する不正なエンティティの物理的侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・自組織における悪意あるエンティティによる保護すべきデータの持出し	L3_1_a_ORG	[ソシキ] ・保護すべきデータの管理に関する組織内の責任が明確でない	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.AM-6
				L3_1_a_SYS	[システム] ・関係する他組織の保護すべきデータを格納するシステムにおいて、セキュアでない設定がなされている	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	CPS.PT-2
					[システム] ・自組織のシステムにおいて、対処すべき脆弱性が放置されている	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	CPS.IP-2
						・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.IP-10
						・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.MA-1
						・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2
						・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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
						・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.CM-7
					[システム] 保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
						・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	CPS.AC-5
						・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	CPS.AC-6
						・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	CPS.AC-9
					[システム] ・IoT機器、サーバ等の設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.IP-5
						・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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	CPS.PT-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及び記録、監視を実施する。	CPS.CM-2
					[システム] ・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	CPS.PT-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・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・制御、アクセス監視・制御を実施する。	CPS.CM-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
				L3_1_a_PRO	[プロシージャ] ・他組織から管理を委託されるデータの機密区分および必要なセキュリティ対策について確認するプロシージャがない	・組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取り決める。	CPS.DS-1

#	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	リスク源 脆弱性ID	リスク源 脆弱性	対策要件	対策要件ID
				L3_1_a_DAT	[データ] ・他組織から管理を委託されているデータの保護に係る区分が明確になっていない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
					[データ] ・定められた機密区分に沿った情報の保護が実装されていない	・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	CPS.AC-7
						・情報を適切な強度の方式で暗号化して保管する。	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。	CPS.DS-3
						・情報を送受信する際に、情報そのものを暗号化して送受信する。	CPS.DS-4
						・送受信する情報データ、保管データする情報の暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。	CPS.DS-5
						・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	CPS.DS-9
		関係する他組織で管理している(データ保管)領域から自組織の保護すべきデータが漏洩する	・他組織の管理するデータ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・他組織の管理するデータ保管エリアに対する不正なエンティティの物理的侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・自組織における悪意あるエンティティによる保護すべきデータの持出し	L3_1_c_ORG	[ソシキ] ・データを保管する組織、システム等の安全性を契約前、契約後に確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-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。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
				L3_1_c_PEO	[ヒト] ・データの加工を委託する組織における要員の信頼性を契約前、契約後に確認していない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	CPS.SC-5
				L3_1_c_DAT	[データ] ・セキュリティ水準が統一されていない複数の組織、システム等に自組織の保護すべき情報が分散して所在している	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
		関係する他組織で保管中の自組織の保護すべきデータが改ざんされる	・窃取したID、パスワード等を利用した正規ユーザへのなりすまし	L3_2_a_DAT	[データ] ・保管中のデータに改ざんを検知するメカニズムがない	・送受信・保管する情報に完全性チェックメカニズムを使用する。	CPS.DS-11
3_3	データを送受信する機能	関係する他組織で使用中の自組織の保護すべきデータが改ざんされる	・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・通信系路上でデータを改ざんする中間者攻撃等	L3_2_b_DAT	[データ] ・通信路上でデータが十分に保護されていない	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	CPS.DS-3
						・情報を送受信する際に、情報そのものを暗号化して送受信する。	CPS.DS-4
					[データ] ・使用中のデータに改ざんを検知するメカニズムがない	・送受信・保管する情報に完全性チェックメカニズムを使用する。	CPS.DS-11
		(なりすまし等をした)ソシキ/ヒト/モノ等から不適切なデータを受信する	・不正な組織/ヒト/モノ/システムによる正規エンティティへのなりすまし ・改ざん等された正規なモノ/システムからの適切でないデータの受信	L3_3_a_ORG	[ソシキ] ・データ送信元となるデータの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-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。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
				L3_3_a_PEO	[ヒト] ・自組織の保護すべきデータのセキュリティ上の扱いについて、外部委託先の担当者が十分に認識していない	・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.AT-2
						自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
				L3_3_a_SYS	[システム] ・データを収集・分析等するシステムにおいて、対処すべき脆弱性が放置されている	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	CPS.IP-2
						・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.IP-10
						・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.MA-1
						・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。	CPS.MA-1
						・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2
						・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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
						・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.CM-7
					[システム] ・通信路が適切に保護されていない	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	CPS.DS-3
					[システム] ・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みが自組織のシステムに実装されていない	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	CPS.PT-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・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・制御、アクセス監視・制御を実施する。	CPS.CM-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
					[システム] ・サイバー空間との通信開始時に、通信相手を識別・認証していない	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・無線接続先（ユーザーやIoT機器、サーバ等）を正しく認証する。	CPS.AC-3
						・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ。	CPS.AC-4
						・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	CPS.AC-8
						・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	CPS.AC-9
				L3_3_a_DAT	[データ] ・通信相手のエンドポイントから送信されるデータをフィルタリングする仕組みが導入・運用されていない	・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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.CM-3
						・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	CPS.CM-4

添付C　対策要件に応じたセキュリティ対策例

・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。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 に分類されたセキュリティ対策例もカバーしておく必要がある。
・本項に記載している対策例のレベルは、既存の標準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）等により整理している。
・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。
・対策例の記載に当たっては、第Ⅲ部にて各要件に対して割り当てた「関連標準等」に記載の文書および該当項目の一部（本表「参照ガイドライン」という形に示している）を参照している。
・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L2_1_a_ORG, L2_3_b_ORG, L2_3_b_SYS	<High-Advanced> ・組織は、自組織の情報システム及び産業用制御システムを構成する資産（IoT機器等を含むハードウェア、ソフトウェア、情報）を一意に特定し、各々の資産に管理責任者を割り当てた上で、資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、定期的又はオペレータ等の求めに応じて、リアルタイムで状況を把握しながら目録を維持・管理する。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・情報システム及び産業用制御システムは、許可されていない資産を自動的に検出し、管理情報から外す・システムから切り離す等を実行するメカニズムを導入、運用している。 ※ 関連する対策要件に、CPS.CM-6がある。 [参考] 重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）のP.44～P.46 に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティスク分析ガイド 第2版」（IPA, 2018年）のP.21に記載された事業被害の大きさにおける評価を用いる方法等がある	O/S	○ (3.4.2)	○ (下記に加えて、 CM-8(1), CM-8(2), CM-8(3), CM-8(5))	○ (下記に加えて、 A.8.1.3)	-	-
			<Advanced> ・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。	O	○ (3.4.1, 3.8.5, 3.8.7, 3.8.8)	○ (CM-8, PM-5)		○ (4.2.3.4)	○ (SR 7.8)
			<Basic> ・組織は、自組織の情報システムや産業用制御システムを構成する資産（ハードウェア、ソフトウェア、情報）を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・資産は保有するものすべてを一覧化することが望ましいが、対象が膨大な場合、分析対象の統合（グループ化）と分析対象からの除外を通じて、対象とする資産を絞り込むことを検討する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録（情報資産管理台帳）の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年)のP47を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。	O			○ (A.8.1.1, A.8.1.2)		
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、トレーサビリティ確保のための特定方法を定める。	L1_3_a_COM, L1_3_b_COM	<High-Advanced> ・組織は、トレーサビリティが要求事項となっている場合には、組織はアウトプット（製品）について一意の識別を管理し、トレーサビリティを可能とするために必要な文書化した情報を保持する。 ・組織は、モノを一意に識別できるような方法を検討する際、異業種間でも通用するよう業種横断的な共通ナンバリングルール等に基づいていることが望ましい。 [参考] ISO9001:2015 - 8.5.2 識別及びトレーサビリティ	O	-	-	-	-	-
			<Advanced><Basic>共通 ・組織は、下記を例とする観点から、自組織が提供するモノを複数段階に優先順位付けする。 - モノの品質等に何かしらの問題が発見された際のサプライチェーンにおける影響範囲の広さ - モノの品質等に何かしらの問題が発見された際の自組織の事業に対する影響の大きさ ・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、組織は、ナンバーを付与する等アウトプットを識別するために適切な特定方法（例：シリアルナンバーの付与）を定める。 ・組織は、製造及びサービスを提供する際の、組織が定める過程（例：製品の顧客納入時まで）において、当該製品・サービスにおいて法令、契約等で遵守が要求されている事項に関連して、アウトプットである製品・サービスの状態を識別する。	O	-	-	-	-	-
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_3_a_COM, L1_3_b_COM	<High-Advanced> ・ 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。 ・作成され、管理される生産活動の記録は、生産日時やモノの分類（例：製品名）等で素早く検索できるよう構成されていることが望ましい。	O	-	-	-	-	-
			<Advanced><Basic>共通 ・生産したモノのサプライチェーン上の重要性に応じて、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し、運用する。 ・組織は、上記の記録を作成、あるいは更新する際、以下の事項を考慮 する。 - 適切な識別及び記述（例：タイトル，日付，作成者，参照番号）とすること - 適切な形式（例：言語，ソフトウェアの版，図表）及び媒体（例：紙，電子媒体）とすること - 適切性及び妥当性に関する、適切なレビュー及び承認を得ること	O	-	-	-	-	-

添付C

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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、適切に管理する。	L1_3_b_ORG, L1_3_c_ORG	<High-Advanced> ・組織は、情報システム及び産業用制御システムのシステム構成、通信ネットワーク構成及びデータフローをリアルタイムでモニタリングし、管理するための自動化されたメカニズムを導入・管理している。	O	-	○ (下記に加えて、CM-2(2), CM-2(3))	○ (A.13.2.1, A13.2.2)	-	-
			<Advanced> ・組織は、関連する文書内の図に、ネットワーク接続におけるインターフェース特性、セキュリティ要求事項、伝達されるデータの性質を記載する。	O	-	○ (下記に加えて、CA-9)		-	-
			<Basic> ・組織は、自組織が管理する範囲（例：事業所単位で）における情報システム及び産業用制御システムのシステム構成、通信ネットワーク構成、データフローを文書化し、保管する。 ・組織は、定期的、あるいは、システム構成、ネットワーク構成、データフローに変更が生じた場合、関連する文書をレビューし、必要に応じて更新する。 [参考] システム構成、ネットワーク構成、データフローの文書化を行う際の手順については、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA, 2018年）の3.2、3.3を参照することが可能である。	O	-	○ (CM-2, CM-2(1))		○ (4.2.3.4, 4.2.3.5)	-
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、適切に管理する。	L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L1_3_b_ORG, L1_3_c_ORG	<High-Advanced> ・システムは、自組織が利用している外部情報システムサービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・システムは、利用を許可していない外部情報システムサービスを検知した場合、システム管理者へ通知するメカニズムを利用する。 ・組織は、外部プロバイダによる情報システムサービスを使用する際に必要な機能、ポート、プロトコル及び他のサービスを明確にする。	O/S	○ (3.12.4)	○ (下記に加えて、SA-9(2))	○ (下記に加えて、A.13.1.2)	-	-
			<Advanced> ・組織は、外部の情報システムを所有、運用する他の組織に対して、下記を許可するうえでの条件を設定する。 a. 外部の情報システムから自組織の情報システムにアクセスすること b. 外部の情報システムを使用して自組織の管理下にある情報を処理または保存もしくは伝送すること ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。	O	○ (3.1.20, 3.1.21, 3.12.4)	○ (下記に加えて、AC-20)		-	-
			<Basic> ・組織は、自組織が利用している外部情報システムサービスを一覧化し、それぞれのサービスにおけるユーザーとしての役割と責任を定義する。 [参考] 特にクラウドサービス利用におけるユーザー側の役割と責任を、契約において規定する際のポイントについて、「クラウドセキュリティガイドライン活用ガイドブック」(経済産業省, 2013年) Appendix A "契約の具体的な内容例と解説" を参照することが可能である。	O	-	○ (SA-9)	○ (A.6.1.1)	-	-
CPS.AM-6	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG, L3_1_a_ORG, L3_4_a_ORG	<High-Advanced><Advanced>共通 ・組織は、情報システムや産業用制御システムにおけるリソース（データ及びデータを処理するモノ、システム等）を分類する際には、データを共有又は制限する業務上の要求及び法的要求事項を考慮する。 ・当該資産の管理責任者は、データの分類に対して責任を負う。 ・組織は、リソースの分類体系に分類の規則及びその分類を時間が経ってからレビューするための基準を含める。	O	-	○ (RA-2、SA-14)	○ (A.6.1.1)	-	-
			<Basic> ・組織は、洗い出した情報システムや産業用制御システムにおける資産を、自組織にとっての重要度に応じて優先順位づけする。 ・関係する法規制等により、自組織のリソース（例：システム、データ）について特定の分類に従うことが要求されている場合、該当する分類を資産に適用する。 ・組織は、特に産業用制御システムにおけるモノ、システム等の分類、優先付けに当たっては、自組織の事業活動の適切でない運用により HSE(Health, Safety and Environment)への悪影響が発生するかを考慮して実施する。 ・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、事業継続の観点から重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 [参考] 資産の重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）の P.44～46に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティスク分析ガイド 第2版」（IPA, 2018年）の P.21 に記載された事業被害の大きさにおける評価を用いる方法等がある。また、特に産業用制御システムにおける資産の重要度の判断基準については、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA, 2018年）4.2.2及び4.2.3を参照することができる。	O	-	○ (RA-2、SA-14)		○ (4.2.3.6, 4.3.4.4.3)	-
CPS.AM-7	・自組織及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_b_ORG, L1_3_c_ORG	<High-Advanced><Advanced>共通 ・組織は、セキュリティインシデントにより損害が発生する場合に備えて、取引先等から指定されるセキュリティ対策の実装に加え、サイバー保険の利用等によるリスク移転を検討する。	O	-	-	○ (A.6.1.1, A.15.1.1)	-	-
			<Basic> ・組織は、委託先あるいは委託元との契約において、業務においてセキュリティインシデントにより損害が発生した場合の自組織と取引先の責任範囲（免責事項の明記、損害賠償額の契約金額等での上限設定等）を規定する。 ・組織は、契約において取引先に対応を求める／求められるセキュリティに関する要求事項の実効性を高めるため、要求事項への対応要否や過不足、具体的な対応方法や費用負担、対応できない場合の代替措置について契約時あるいは契約期間の初めに合意することが望ましい。 [参考] 特にクラウドサービスプロバイダーと自組織との役割と責任に関して、追加の情報を得るために、「クラウドセキュリティガイドライン活用ガイドブック 2013年度版」（経済産業省, 2013年）の "4.4.クラウドサービスの契約" を参照することが可能である。	O	-	○ (SA-4)		○ (4.3.2.3.3)	-

添付C

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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_b_ORG, L1_3_c_ORG	<High-Advanced> ・自組織において、事業への悪影響を及ぼすセキュリティインシデントが発生した際の、直接的な取引先及びサプライチェーン全体への影響の内容及びその規模を推定する。	O	-	○ (CP-2, SA-14)	-	-	-
			<Advanced> ・組織間のモノの流れ、データの流れ等を考慮して、自組織の関係するサプライチェーンの概要を、自組織の全体における役割がわかるように図示する。 ・上記の結果を関係する他組織（自組織からの発注先、自組織内の関係部門、自組織への発注元）と共有する。	O	-	-	-	-	-
			<Basic> ・組織間のモノの流れ、データの流れ等を考慮して、自組織からの発注先、自組織、自組織への発注元という取引関係の概要を、自組織の役割がわかるように図示する。 ・上記の結果を関係する他組織（自組織からの発注先、自組織内の関係部門、自組織への発注元）と共有する。	O	-	-	-	-	-
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、自組織の取引に関係する者（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	<High-Advanced><Advanced>共通 ・組織は、組織の業務、組織の資産、個人、他の組織等にもたらされるリスクを考慮して、自組織のミッション／業務プロセスを定義し、活動に関する優先順付けを確立する。 ・組織は、自組織のセキュリティポリシーにおいて規定されている自組織と関係する他組織のセキュリティに関する役割と責任について、関係する他組織に伝達する。	O	-	○ (PM-11、SA-14)	○ (A.5.1.1)	○ (4.2.2.1, 4.2.3.6)	-
			<Basic> ・組織は、あらかじめ優先して継続・復旧すべき中核事業及び重要と考えられる業務を特定しておき、事業継続の観点から重要なリソース(関係する他組織、ヒト、モノ、データ、システム等)と機能を特定し、優先順位付けする。 ・組織は、特に産業用制御システムに関して、自組織の事業活動の適切でない運用によりHSE(Health, Safety and Environment)への悪影響が発生するかも考慮してリソースの分類、優先順位付けを行う。	O	-	-	-	-	-
CPS.BE-3	・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。	L1_3_b_ORG, L1_3_c_ORG	<High-Advanced> ・組織は、自らの事業を継続する上で、自組織が有する下記のサポートユーティリティの果たす機能及び依存関係を特定する。 - 通信サービス - 電力設備（電力ケーブル等を含む） ・上記で識別されたユーティリティの内、事業継続という観点から重要な役割を果たすものについて、下記のような対策を講ずることを検討する。 - 代替通信サービスの確立 - 情報システム及び産業用制御システムの電力設備及び電力ケーブルの物理的保護 - 短期無停電電源装置の準備 ・特に、代替通信サービスの利用を検討する際、下記について考慮する - 通信サービス事業者との契約事項を検討する際、組織の可用性に関する要求事項（目標復旧時間を含む）を明確にする - 一次通信サービスとの間で単一障害点が共有される可能性を低減する	O	-	○ (下記に加えて、CP-8, CP-8(1), CP-8(2), PE-9, PE-11)	○ (下記に加えて、A.11.2.2)	-	-
			<Advanced> ・CPS.AM-6で規定した当該システムの可用性に対する要求水準に応じて、その容量・能力に関する要求事項を特定する。 ・自組織が利用する情報システム及び産業用制御システムが、要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。	O	-	○ (SC-5(2))	○ (A.12.3.1)	-	-
			<Basic> ・組織は、自らの事業を継続する上で、重要な依存関係にあるサプライヤーを特定する。	O	-	-	-	-	-

添付C

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.GV-1	・セキュリティポリシーを策定し、自組織及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	<High-Advanced> ・従来のIT環境において運用されているものと基本的な方針を共有しつつ、産業用制御システム等、IoT機器が設置されるサイトの性質等を十分に考慮したセキュリティポリシー群、運用手順を策定する。 [参考] 例えば、産業用制御システム(ICS)を対象としたセキュリティマネジメント規格であるIEC 62443-2-1では、ICS環境のための上位レベルのサイバーセキュリティポリシーの策定を求めている。特に、産業分野におけるセキュリティポリシー及び運用手順の策定にあたっては、「制御システムセキュリティ運用ガイドライン」（日本電気制御機器工業会, 2017年）等を参考とすることができる。	O	-	○ (controls from all security control families)	○ (A.12.1.1)	○ (4.3.2.3.3, 4.3.2.2.1, 4.3.2.6)	-
			<Advanced> ・組織は、上位の方針を支えるセキュリティポリシー群のより低いレベルとして、例えば、情報システムを対象とした下記のようなトピック個別の方針及び実施手順を策定する。 a) アクセス制御及び認証 b) 物理的セキュリティ対策 c) システムの開発及び保守 d) 外部委託先管理 e) 情報分類及び取扱い ・情報システムを対象としたセキュリティポリシー群の策定に当たっては、自組織の a)事業戦略、b)関係する規制、法令及び契約、c)セキュリティの脅威環境 を十分に考慮して、自組織の実情を十分に反映したものとなるよう策定を実施する。 ・組織は、自組織の a)事業戦略、 b)関係する規制、法令及び契約、c)セキュリティの脅威環境 の変化に応じて、セキュリティ方針をレビュー、更新する。 [参考] より詳細なレベルの方針策定の際には、ISO/IEC 27002 等の関連する標準を参照して方針が必要となる分野を把握したうえで、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年) 付録5「情報セキュリティ関連規定（サンプル）」や、「情報セキュリティポリシーサンプル改版（1.0版）」(JNSA, 2016年)等を参考にすることができる。	O	-		○ (A.5.1.1, A12.1.1)		-
			<Basic> ・組織は、自組織のセキュリティポリシー群の最も高いレベルに、セキュリティ基本方針を策定し、経営層の承認を得た後、適切な適用範囲（例：企業全体、事業部全体）で運用する。 ・組織は、自組織のセキュリティ基本方針を定期的(例えば、1年に1度)にレビュー、更新する。 [参考] セキュリティポリシーの策定に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年) 付録5「情報セキュリティ関連規定（サンプル）」における "1．組織的対策"の記載や、「情報セキュリティポリシーサンプル改版（1.0版）」(JNSA, 2016年)における "01_情報セキュリティ基本方針"、"01_情報セキュリティ方針" 等を参考とすることが可能である。	O	-		○ (A.5.1.1)		-
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する。	L1_2_a_ORG, L1_2_a_COM, L1_2_a_SYS, L1_2_a_PRO, L1_2_a_DAT	<High-Advanced><Advanced><Basic>共通 ・自組織の事業活動において、セキュリティの文脈で関連するすべての法令、規制及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組みを明確に特定し、文書化する。 ・要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文書化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全ての国における遵守を考慮する。 [参考] 情報セキュリティ関連法令には、例えば、不正競争防止法、電子署名認証法、e-文書法、個人情報保護法、不正アクセス禁止法等がある。また、上記の法令等の遵守に際しては、関連各省庁から発出されているガイドライン文書等（例：不正競争防止法：「営業秘密管理指針」(経済産業省, 2019年)、「限定提供データに関する指針」(2019年, 1月)、個人情報保護法：「個人情報の保護に関する法律についてのガイドライン(通則編)」(個人情報保護委員会, 2019年)、「個人情報の保護に関する法律についてのガイドライン(匿名加工情報編)」(個人情報保護委員会, 2017年)）を参照することが望ましい。	O	-	○ (controls from all security control families)	○ (A.6.1.3, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5)	○ (4.4.3.7)	-
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_SYS, L1_1_a_DAT, L1_1_b_SYS, L3_1_a_SYS, L3_1_a_DAT, L3_4_a_ORG, L3_4_a_PRO, L3_4_b_ORG, L3_4_b_PRO	<High-Advanced><Advanced><Basic>共通 ・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)	O	○ (3.1.22)	○ (controls from all security control families)	○ (A.8.2.1, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5)	○ (4.3.4.4.6)	-
CPS.GV-4	・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	<High-Advanced><Advanced>共通 ・組織は、システムの運用と使用により生じる組織の業務と資産、個人、他の組織等に対するリスクを管理するための、短中期（例：1年~5年）のリスクマネジメント戦略を策定する。 ・組織は、短中期のリスクマネジメント戦略を定期的に、あるいは必要な場合にレビューし、更新する。	O	-	○ (下記に加えて、PM-3, PM-9)	○ (Clause 6)	○ (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)	-
			<Basic> ・組織は、情報システム及び産業用制御システムまたはシステムサービスのセキュリティ要求事項を決定するとともに、情報システム及び産業用制御システムまたはシステムサービスを保護するのに必要なリソースを決定・文書化のうえ割り当てる。 ・組織は、セキュリティの個々の予算項目を、組織の計画及び予算関連の資料に記載する。	O	-	○ (SA-2)		-	-

添付C

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.RA-1	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS	<High-Advanced> ・組織は、自組織が管理する産業用制御システムの構成要素（IoT機器を含む）に対して、システムの運用に悪影響を及ぼさないよう、計画停止時等の予定されたタイミングに脆弱性診断を実施し、自組織の所有するシステムに存在する脆弱性を認識し、一覧化する。 ・組織は、自組織の管理するシステムにおける最新の脆弱性を認識するため、定期的に侵入テストを実施することが望ましい。 ・組織は、ツールを用いて脆弱性診断を行う場合、診断すべきシステムに対する脆弱性データベースを更新できる脆弱性診断ツールを使用することが望ましい。 ・組織は、より徹底した脆弱性の洗い出しを行うために、脆弱性診断の実施者に自組織の管理するシステムにおける特権アクセスの権利を一時的に許可するメカニズムを整備する。	O	-	○ （下記に加えて、CA-8, RA-5(1), RA-5(5)）	○ (A.12.6.1)	○ （下記に加えて、4.2.3.7, 4.2.3.9）	-
			<Advanced> ・組織は、自組織が管理する重要度の高い情報システムの構成要素に対して、脆弱性診断を実施し、自組織の所有するシステムに存在する脆弱性を認識し、一覧化する。 ・組織は、自組織の所有する情報システムの運用段階において、各種資産から収集した脆弱性の内、自組織の事業運営等に関連することが想定されるものに対して、脆弱性検査ツール等を用いて、定期的に自組織のシステムにおける脆弱性を特定し、当該脆弱性の影響度とともに一覧に追加する。 [参考] 脆弱性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の影響の大きさを評価する指標として、CVSS(IPAによる解説：https://www.ipa.go.jp/security/vuln/CVSS.html)を参考とすることが可能である。	O	-	○ (RA-5, RA-5(2))		○ (4.2.3.12, 4.3.4.4.5)	-
			<Basic> ・組織は、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年) 付録7「リスク分析シート」における対策状況チェック等の、セキュリティ対策のベースラインとなる文書を活用して、自組織の情報システムにおける管理策上の脆弱性を把握する。	O	-	-	-	-	-
CPS.RA-2	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	L1_1_a_SYS, L1_3_a_ORG, L2_1_a_ORG, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> ・組織は、セキュリティ対応組織を立ち上げ、産業用制御システム、IoTシステム等も管轄に含めて、組織内で統合的にセキュリティ対策を取る体制を整える。 ・セキュリティに関わる研究会や会議等に出席したり、セキュリティの専門家による協会・団体との適切な連絡体制を維持することにより、情報システム、産業用制御システムの双方におけるセキュリティに関わる知識を最新のものとする。 ・主に自社が提供している製品・サービスにおいて、新たな脆弱性が含まれていないかを分析し、発見した場合、IPAに関連情報を届け出る。	O	-	○ （下記に加えて、PM-15）	○ （下記に加えて、A.6.1.4）	○ (4.3.2.3.2)	-
			<Advanced> ・組織は、セキュリティ管理責任者を中心に、セキュリティ対応組織を立ち上げ、主に情報システムや事業における重要度の高いIoTシステムを管轄対象として、組織内でセキュリティ対策を取る体制を整える。 ・組織は、情報処理推進機構（IPA）、JPCERT/CC、業界ISACのような組織や、取引関係のある機器ベンダー、ソフトウェアベンダーより、随時脆弱性情報、脅威情報等を収集し、自組織の資産目録と照らし合わせることで、対応要否を判断する。 [参考] セキュリティ対応組織の構想、構築、運用に当たっては、外部事業者からのサービスを利用するほかに、JPCERT/CCから公開されている「CSIRTマテリアル」、日本セキュリティオペレーション事業者協議会から公開されている「セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～」等の文書を利用することが可能である。	O	-	○ （下記に加えて、PM-16）		○ (4.2.3.9, 4.2.3.12)	-
			<Basic> ・組織は、情報システム及び産業用制御システムの双方を対象に、セキュリティ管理責任者及びセキュリティ対策担当者を任命することで、組織内におけるセキュリティの役割と責任を明確化する。 ・組織は、利用中の機器ベンダーやソフトウェアベンダーが提供するセキュリティに関わる注意喚起情報を確認し、自組織内の関係者に伝達する。	O	-	○ (SI-5)	○ (A.6.1.1)	○ (4.3.2.3.2)	-
CPS.RA-3	・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS	<High-Advanced> ・組織は、セキュリティに関わる研究会や会議等に出席したり、セキュリティの専門家による協会・団体との適切な連絡体制を維持することにより、セキュリティ脅威に関わる知識を最新のものとする。 ・組織は、必要に応じて、専門家が提供するサービス等を活用し、一部の専門家しか知りえない情報を入手しそれをもとに、脅威を特定する。	O	-	○ （下記に加えて、PM-15）	○ （下記に加えて、A.6.1.4）	-	-
			<Advanced> ・組織は、公開された新たな攻撃動向、マルウェア挙動情報や悪性IP アドレス/ドメイン情報などの情報（外部インテリジェンス）を収集する。 ・組織は、得られた脅威情報の信頼度、自組織に与える影響などを評価し、対応すべき脆弱性を取捨選択し、対応する脅威について文書化する。	O	-	○ (PM-16)	-	○ (4.2.3.9, 4.2.3.12)	-
			<Basic> ・組織は、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年) 付録7「リスク分析シート」における脅威の状況等の、セキュリティ脅威洗い出しのベースラインとなる文書を活用して、自組織に関わるセキュリティ脅威及びその発生しやすさを把握する。	O	-	-	○ (Clause 6.1.2)	-	-

添付C

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_a_COM, L2_1_a_PRO, L2_2_a_ORG, L2_2_a_SYS	<High-Advanced> ・組織は、産業用制御システムのようにモノの制御等を伴うような、フィジカル空間に影響を及ぼす可能性のある新たな機器やシステムを開発する場合には、従来の製品や他の事故事例を収集・分析し、セキュリティの観点も含めてセーフティに関わるハザードを特定する。 ・組織は、主に産業用制御システムにおいて、ハザードによって危害に至る状況を分析し、発生しやすさや被害の深刻度を明らかにすることで、生じるリスクを見積もる。その際、セキュリティの問題に起因するハザードの有無を確認することが望ましい。 ・組織は、産業用制御システム、またはそれが稼働する環境に大きな変化があった場合、もしくは産業用制御システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。 [参考] セーフティ設計におけるハザードの特定と分析については、「つながる世界のセーフティ＆セキュリティ設計入門」(IPA, 2015年)の4.2にて具体的な手法が記載されており、参照することが可能である。	O	-	-	○ (A.12.6.1, A.18.2.2, A.18.2.3)	-	-
			<Advanced> ・組織は、情報システム、または情報システムが稼働する環境に大きな変化があった場合（新たな脅威や脆弱性の特定を含む）、もしくは情報システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。 ・組織は、新たにIoT機器を利用したシステムを企画・設計する場合、既存の資産や新たに導入するシステムにおける守るべき資産を特定し、システムの利用用途や構成に応じて、セキュリティ対策をまとめる。特に、ライフサイクルの長いモノ、システムや、高い可用性を求められるモノ、システムを扱う場合は、設計以前の段階におけるセキュリティ対策の考慮が特に重要である。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 [参考] システム及びモノにおけるセキュリティの要求仕様を検討するにあたり、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。	O	○ (3.11.1)	○ (下記に加えて、SA-12(2))			-
			<Basic> ・組織は、情報システム及び産業用制御システムに対するセキュリティリスクアセスメントのプロセスを定め，定期的（例えば、重要度の高い情報システムは年に1回）に適用する。 - セキュリティのリスク基準を確立し，維持する。 - 以下の方法によりセキュリティリスクを特定する。 1) 分析対象を明確化する 2) インシデント(周辺状況の変化を含む)並びにこれらの原因を特定する - 以下の方法により、セキュリティリスクを分析する。 1) 上記で特定されたリスクが実際に生じた場合に起こり得る結果について評価する 2) 上記で特定されたリスクの現実的な起こりやすさについて評価する - リスク基準を参照し、リスクのレベルを決定し、優先順位付けする ・組織は，セキュリティリスクアセスメントのプロセスを文書化し、保管する。 ・組織は、システムにセキュリティインシデントが発生した際に想定される被害の大きさやセキュリティインシデントが発生する蓋然性（例：インターネットにつながっているか）、リスクアセスメント実施に係る工数等の観点を考慮し、システムを優先順位化してリスクアセスメントの頻度等を設定することが望ましい。 [参考] セキュリティリスクアセスメントの手法として、「資産ベース」の手法及び「事業被害ベース」の手法があることが知られている。資産ベースの手法でリスクアセスメントを実施する場合は「中小企業の情報セキュリティガイドライン 第3版」（IPA, 2019年）や「制御システムのセキュリティリスク分析ガイド 第2版」(IPA, 2018年) 等を、事業被害ベースの手法を実施する場合は「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)等を参照することができる。	O	-	○ (RA-3)	○ (Clause 6.1.2, A.18.2.2, A.18.2.3)	○ (4.2.3.9, 4.2.3.12)	-

添付C

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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	<High-Advanced> ・組織は、新たな脅威や脆弱性に関する情報を入手した際のリスクアセスメント（例：影響範囲の評価）に自動化されたメカニズムを利用する。 ・組織は、自組織にとって影響が大きく、他組織にとっても対応することが重要と考えられる脅威や脆弱性の情報について、サプライチェーンのステークホルダーへと安全に共有する。	O	-	-	-	-	-
			<Advanced> ・組織は、情報システム、または情報システムが稼働する環境に大きな変化があった場合(新たな脅威や脆弱性の特定を含む)、もしくは情報システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。その際、重要度の高い情報システム及び産業用制御システムを優先的に対応する。 ※ CPS.RA-4と共通の実施内容	O	-	○ (RA-3)	○ (A.12.6.1)	-	-
			<Basic> ・組織は、セキュリティリスクアセスメントのプロセスを定め，定期的(例えば、年に1回)に適用する。 - セキュリティのリスク基準を確立し，維持する。 - 以下の方法によりセキュリティリスクを特定する。 1) 分析対象を明確化する 2) インシデント(周辺状況の変化を含む)並びにこれらの原因を特定する - 以下の方法により、情報セキュリティリスクを分析する。 1) 上記で特定されたリスクが実際に生じた場合に起こり得る結果について評価する 2) 上記で特定されたリスクの現実的な起こりやすさについて評価する - リスク基準を参照し、リスクのレベルを決定し、優先順位付けする ・組織は，セキュリティリスクアセスメントのプロセスを文書化し、保管する。 ・組織は、システムにセキュリティインシデントが発生した際に想定される被害の大きさやセキュリティインシデントが発生する蓋然性(例：インターネットにつながっているか)、リスクアセスメント実施に係る工数等の観点を考慮し、システムを優先順位化してリスクアセスメントの頻度等を設定することが望ましい。 ※ CPS.RA-4と共通の実施内容 [参考] セキュリティリスクアセスメントの手法として、「資産ベース」の手法及び「事業被害ベース」の手法があることが知られている。資産ベースの手法でリスクアセスメントを実施する場合は「中小企業の情報セキュリティガイドライン 第3版」（IPA, 2019年）や「制御システムのセキュリティリスク分析ガイド 第2版」(IPA, 2018年) 等を、事業被害ベースの手法を実施する場合は「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)等を参照することができる。	O	-		○ (Clause 6.1.2)	-	-
CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_a_COM, L2_1_a_PRO, L2_2_a_SYS	<High-Advanced> ・CPS.RA-4で実施したハザード分析の結果に基づき、主に産業用制御システムに対して、必要な場合、重要なハザードにつながりうるセキュリティに係るリスク源に対して適切に対応する。 [参考] 特に安全制御系におけるセキュリティ面の統合については、近年国際標準化の場でも議論がなされており、IEC TR 63074, IEC TR 63069等を参照することが可能である。	O	-	-	○ (A.5.1.2)	-	-
			<Advanced> ・組織は、セキュリティリスク対応のプロセスについての文書化した情報を安全に保管する。 ・組織は、リスクアセスメントの結果に応じて対応策を選定する際、実施する対応策及び当該対応策を採用する理由を文書化することが望ましい。 ・組織は、対応策の適用等に関して、セキュリティリスク対応計画を策定し、リスク所有者の承認を得る。 ・組織は、セキュリティリスク対応計画をレビューし、当該計画が自組織全体のリスクマネジメント戦略における優先順位に適合しているかどうかを確認する。 ・CPS.RA-4で抽出した、IoT機器を含む新しいシステムにおける必要なセキュリティ対策について、然るべき外部事業者に要求仕様として伝達する。 ・組織は、IoT機器を含むシステムの導入時に、要求仕様や契約段階で定めたセキュリティ対策が実施されているかを受け入れ検査などで確認する。もし、不明な点があれば、外部事業者に確認する。	O	○ (3.12.4)	○ (PM-4)	○ (Clause 6.1.3, Clause 8.3, A.5.1.2)	-	-
			<Basic> ・組織は、リスクアセスメントの結果を考慮して、対象とするリスクへの対応策を選定する。 ・組織は、セキュリティリスク対応の実施計画を策定する。 ・セキュリティリスクの受容について、リスク所有者の承認を得る。	O	-	-		-	-

添付C

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.RM-1	・自組織内における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し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスク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_b_ORG, L1_3_c_ORG	<High-Advanced> ・組織は、リスクマネジメント戦略の策定時及び改定時に、重要度の高い取引先との間で、リスクマネジメント戦略に関するインタビューを実施することで、セキュリティ上のリスクや必要な対策に関する認識を合致させる。その際、下記事項を扱うことが望ましい。 - 自組織の事業内容及び事業の継続に関わる主なセキュリティリスク - 上記リスクが顕在化した際の、取引先における影響の内容とその規模 - 上記セキュリティリスクへの対応方針 - （リスクマネジメント戦略改定時の場合）内外の情勢の変化及び前回の版から変更すべきと考える主要なポイント	O	-	-	-		-
			<Advanced> ・組織は、情報システム及び産業用制御システムの運用と使用により生じる組織の業務と資産、個人、他の組織等に対するリスクを管理するための、包括的なリスクマネジメント戦略を策定する。 ・組織は、リスクマネジメント戦略を組織全体にわたって一貫性が保たれるように実施する。 ・組織は、リスクマネジメント戦略を定期的、あるいは組織的変化に対処するため必要な場合にレビューし、更新する。 ・組織の経営層は，組織の リスクマネジメント戦略の内、セキュリティに関わるものについて、下記のような観点を定期的にレビューする。 - どの程度の攻撃に直面しているのか（検知しているのか） （アンチウイルス製品/IDSによる検出件数、最新の脅威動向等） - セキュリティ対策の状況は計画通りか （マルウェア対策、セキュリティパッチ適用等の実施すべきセキュリティ対策の適用率等） - 攻撃者（内部犯行を含む）の侵入を許したか、あるいはその可能性はあるか （セキュリティ監視活動を通じた外部からの侵入あるいは内部犯行が疑われるイベントの説明） - 直接情報システムや産業用制御システムとは関係しないセキュリティの状況はどのようなものか （退職者、PCやデバイスの紛失、盗難の発生状況等） ・組織は，経営層によるレビューの結果を文書化し、保管する。 [参考] 組織の経営層に対してセキュリティに関して報告すべき事項について追加の情報を得る場合は、「CISOハンドブック Ver.1.1 β」(JNSA, 2018年)、「CISOダッシュボード ～サイバーセキュリティを経営に組み込むための考察～」(JNSA, 2018年)を参照することが可能である。	O	-	○ (PM-9)	○ (Clause 9.3)	○ (4.3.4.2)	-
			<Basic> ・組織は、情報システム、産業用制御システムの双方において、自組織におけるセキュリティリスク対応の責任者を明確にする。 ・組織は、自身の事業において自組織が担うセキュリティリスクの責任範囲を明確にする。	O	-	-	-	-	-
CPS.RM-2	・リスクアセスメント結果及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_ORG, L1_1_a_SYS, L1_1_b_ORG, L1_1_b_SYS, L1_1_c_SYS	<High-Advanced> ・CPS.BE-1 <High-Advanced> にて実施しているサプライチェーンに係るリスクの現状把握及び CPS.RA-4等で実施しているリスクアセスメントの結果を所与として、自組織におけるリスク許容度を決定する。 ・自組織におけるセキュリティインシデントにより望ましくない影響を受ける可能性がある重要な取引先に対して、自組織のリスク許容度に関する認識を共有する。	O	-	○ (下記に加えて、SA-14)	-	-	-
			<Advanced> ・CPS.BE-1 <Advanced> にて実施しているサプライチェーンの現状把握及び、CPS.RA-4等で実施しているリスクアセスメントの結果を所与として、自組織におけるリスク許容度を決定する。	O	-		○ (Clause 6.1.3, Clause 8.3)	○ (4.3.2.6.5)	-
			<Basic> ・組織は、CPS.RA-4等で実施しているリスクアセスメントの結果を所与として、自組織におけるリスク許容度を決定する。 ・組織は、残存しているリスクの受容について、リスク所有者の承認を得る。 ・組織は、リスク対応結果を文書化し、リスク許容度の基準及び許容したリスクの一覧を安全に保持する。	O	-	○ (PM-8)			-
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、その内容について取引先と合意する。	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG	<High-Advanced><Advanced>共通 ・組織は、サプライチェーンに係るセキュリティ対策基準を参照して、ITT(Invitation To Tender)やRFP(Request For Proposal)などの入札書類を準備し、潜在的な取引先に提供する。特に、入札書類には以下が含まれることが望ましい。 1）調達する製品またはサービスの仕様 2）供給者が製品またはサービスを供給している間に従うセキュリティ要件 3）製品またはサービスの供給中に従うべきサービスレベル及びその指標 4）セキュリティ要件に違反した場合に、委託元が課す可能性のある罰則 5）取引先の選定プロセス中に送信されるデータやシステムなどを保護するための秘密保持条項 ・組織は、取引先によるセキュリティ管理策の遵守状況を継続的にモニタリングするための、プロシージャを整備する。 ・取引先におけるセキュリティインシデントが自組織に影響した場合に備え、契約書にて外部事業者との責任分界点を明確にし、外部事業者の責任範囲において自組織に被害が発生した場合の損害賠償について記載する等の対応を行う。	O	-	○ (下記に加えて、SA-9(2))	○ (下記に加えて、A.15.2.1)	-	-
			<Basic> ・組織は、該当する法規制等を参照して、取引先（特に、自組織のデータを取り扱う可能性のある、またはデータを取り扱うための基盤を提供する可能性のあるもの）に対して適用するセキュリティ対策基準を策定し、内容について合意する。 ・組織は、取引先（外部情報システムサービスのプロバイダ）に対して、サービスの使用に必要な機能、ポート、プロトコル及び他のサービスを明確にする。 [参考] 取引先に対して適用するセキュリティ対策基準の策定に当たり、ISO/IEC 27001 附属書Aの管理策をベースに作成された「情報セキュリティベンチマーク」(IPA)や、「サプライチェーン情報セキュリティ管理基準」（日本セキュリティ監査協会）等を参考とすることが可能である。	O	-	○ (SA-9)	○ (A.15.1.1, A.15.1.2)	○ (4.3.4.4.1)	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.SC-2	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG, L2_3_c_ORG, L3_1_b_ORG, L3_1_c_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_d_ORG	<High-Advanced> ・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 ・取引先において、事業への悪影響を及ぼすセキュリティインシデントが発生した際の、自組織への影響の内容及び、その起こりやすさ、規模を推定する。 ※ 関連する対策要件に、CPS.AM-6, CPS.BE-2等がある。	O	-	○ (下記に加えて、SA-14)	○ (A.15.1.1, A.15.1.2)	○ （下記に加えて、4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.10）	-
			<Advanced> ・組織は、自組織のミッション/業務プロセスに重要な影響を及ぼしうるサプライチェーン上の取引先を特定し、当該組織が自組織のセキュリティポリシーに規定されているセキュリティ上の役割と責任を果たせるかどうかを確認する。	O	-			○ （4.2.3.1, 4.2.3.2, 4.2.3.4, 4.2.3.6, 4.2.3.12, 4.2.3.13, 4.2.3.14, 4.3.4.2）	-
			<Basic> ・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 ・組織は、長期に渡ってIoT機器が使用されることが想定される場合、問い合わせ窓口やサポート体制等の適切な管理体制が整備されており、販売後のセキュリティサポート方針を明確にしている等、長期間のサポートが期待できる取引先（IoT機器ベンダ）を選定する。 ・組織は、IoT機器のサポート終了時に機器を入れ替えることの要否についてシステムの導入前に取引先（IoT機器ベンダ）に対して確認する。 ・組織は、下記の観点を確認することにより、ITサービスのマネジメントを効率的、効果的に運営管理するサービスプロバイダーを選定することが望ましい。 - JIS Q 20000 に基づく第三者認証（ITSMS認証）を取得している - 自己適合確認を通じて認証取得相当の対策の実装を確認している	O	-	○ (SA-4)		-	-
CPS.SC-3	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織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_PRO, 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_1_c_ORG, L3_1_c_DAT, L3_3_d_ORG, L3_3_a_ORG,. L3_3_b_ORG, L3_3_c_ORG, L3_4_a_DAT, L3_4_b_DAT	<High-Advanced> ・組織は、システム・モノ・サービスのいずれかを提供する取引先との契約において、当該組織に対して、以下の実施を要求する。 - 契約にて指定されたセキュリティ対策を実施したエビデンスの作成、セキュリティテスト／評価結果の提示 - セキュリティテスト／評価時に特定された欠陥の修正計画の策定 - 欠陥の修正計画及び、その実施状況の提示 ・組織は、直接の委託先に対して要求しているセキュリティ対策に関する要求事項及びそれに付随する要求事項の内で必要な事項を、サプライチェーンに由来するリスクの大きさ等を勘案しつつ、再委託先以降の組織に対して（場合によっては再委託先以降の全サプライヤーに対して）も適用することが望ましい。 [参考] 委託契約に含め、実施を確認することが望ましい項目に関する追加の情報の取得のためには、「ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」(IPA, 2018年)の「3.2. IT サプライチェーン リスクマネジメント の全体像」等を参照することが可能である。	O	-	○ (下記に加えて、SA-11)	○ (A.13.2.4, A.15.1.2)	-	-
			<Advanced> ・組織のミッション／業務ニーズに応じて、システム、モノ、またはサービスの調達契約に以下の要求事項、記述及び基準を記載する。 - セキュリティ対策に関する要求事項 - セキュリティ関連のドキュメントに関する要求事項 - セキュリティ関連のドキュメントの保護に関する要求事項 - 秘密保持に関する条項 - インシデントが発生した際の報告先、報告内容、初動、調査、復旧等の各対応の実施主体、実施方法 - 自組織または認可された第三者によって監査され、定義されたセキュリティ要件への遵守を確認することを許可する条件 - 契約終了後の情報資産の扱い ・組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施し、委託内容の特性等により必要と認められる場合、調達契約において、追加で対策を導入することを要求する。 ・法規制等を参照してセキュリティ要件を決定し、取引先へ遵守を要求する際、下記を事前に考慮することが望ましい。 - 自組織と取引先との法令の相違（例：業法の違い、国・地域の違い）により生じるコンプライアンス上のリスクの特定 - 取引先に適用される法律及び規制上の義務によるセキュリティの観点からの契約への悪影響	O	-	○ (下記に加えて、SA-4)		○ （4.3.2.6.4, 4.3.2.6.7）	-
			<Basic> ・組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施することを要求する。 ・組織は、委託先の選定、評価のプロセスにおいて、取引先がセキュリティアクションを宣言していることを確認する。	O	-	○ (SA-9)			-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L1_1_d_ORG, L1_1_d_COM, L2_1_a_COM, L2_1_a_PRO, L2_2_a_ORG, L2_3_a_ORG, L2_3_c_ORG, L2_3_c_PRO, L2_3_d_ORG, L3_1_b_ORG, L3_3_a_ORG, L3_3_b_ORG, L3_3_c_ORG, L3_3_d_ORG	<High-Advanced> ・調達する機器に対して、契約におけるセキュリティ要求事項が満たせているかを、自組織あるいは第三者がテストする。 ・組織は、自組織のオペレーションにとって特に重要な機器について、再委託先以降の組織を含む関係するサプライチェーン全体に渡り、一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロシージャで製造されたものかを確認する。	O	-	-	○ (下記に加えて、A.14.3.1)	-	-
			<Advanced> ・組織は、契約において、例えば下記のように、取引先から調達する製品・サービスが具備すべきセキュリティ要求事項を明確化する。 - セキュリティに関わる特定の認証（例：ISMS認証、ISASecure EDSA認証、ITセキュリティ評価及び認証制度(JISEC)）を有していること - ベンダー自身により、セキュリティに関わる特定の認証の基準に適合する対策を実施していることが確認されていること - リスク分析の結果等から導かれた必要なセキュリティ要件を設計時からの実装（セキュリティ・バイ・デザイン）し、検査していること ・組織は、調達計画時に、製品またはサービス自体、あるいは当該製品・サービスの調達・供給にて使用される資産の保護に係るセキュリティ要件の費用を確保しておくことが望ましい。 ・下記を含む製品またはサービスの調達または供給を評価するためのセキュリティ測定ルールを策定し、運用及び改善する。 - 測定対象の内容 - 措置の報告方法、報告の頻度 - 措置が実施されない場合に遂行される措置 ・組織は、搬送中の改ざん・漏えいを検知(又は抑止)する手段とともに納品されるIoT機器やソフトウェアが、不正操作されていないかを確認する。 - 物品：セキュリティ便、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	O	-	-	○ (A.8.3.3, A.14.1.1, A.14.2.9, A.15.1.3)	-	-
			<Basic> ・組織は、調達時に、自組織が所有するIoT機器が正規品であるかをラベルを確認する等して確かめる。 ・組織は、IoT機器やソフトウエアに含まれるIDや秘密鍵、電子証明書等を用いて調達した機器が正規品であることを確認する。 ・組織は、製品・サービスの提供について外部の関係者を選定する際、下記を確認する。 - セキュリティパッチの配布を含めた、製品・サービスのサポート期間が十分設けられていること - サポート期間終了後の対応が明確化されていること	O	-	-	-	-	-
CPS.SC-5	・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	<High-Advanced> ・組織は、委託先の要員により委託元が要求するセキュリティ要求事項が遵守されているかどうかを継続的にモニタリングし、通常とは異なる行動があった場合、自組織の担当者に通知できるようにプロシージャを整備する。	O	-	○ (PS-7)	○ (A.16.1.2, A.16.1.5)	-	-
			<Advanced> ・サプライヤー関係のセキュリティ面について該当する要員を訓練し、機密情報の取り扱いが正しく理解されていることを特に確認する。 ・委託業務の遂行に当たり、委託元が要求するセキュリティ要求事項が遵守されていることを定期的に確認する。	O	-			-	-
			<Basic> ・委託業務に係るデータの内、機密データや知的財産のように、公開または変更すべきではないものへのアクセス及びデータの開示または変更に関わる要員を特定し、評価する。 ・組織は、委託先との契約の終了後、速やかに委託先の要員に対する自組織施設へのアクセス権限等の、一時的に許可していた権限を停止する。	O	-			-	-
CPS.SC-6	・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, L2_3_d_ORG, L3_1_a_DAT, L3_1_b_ORG, L3_1_b_DAT, L3_1_c_ORG, L3_1_c_DAT, L3_3_a_ORG,. L3_3_b_ORG, L3_3_c_ORG, L3_3_d_ORG, L3_4_a_DAT, L3_4_b_DAT	<High-Advanced> ・組織は、契約事項からの逸脱及び、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先及びその再委託先以降の組織に対して、契約にて規定した組織のセキュリティマネジメント、納入する製品・サービスに実装されるセキュリティ機能等に関する義務事項が履行されているかどうかを一覧化して確認できるメカニズムを利用する。 ・委託元による実地調査、外部監査等の手法により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。 ・重要な取引先及びその再委託先以降の組織は、関係する攻撃の予兆、情報流出の事実がないかを調査し、組織に対して結果を定期的に報告する。	O	○ (下記に加えて、3.3.5)	○ (下記に加えて、AU-6(1), AU-6(3))	○ (A.12.7.1, A.14.3.1, A.15.2.1)	-	-
			<Advanced> ・組織は、自組織が取引先との契約において要求事項として規定した内容に関連して、システム上での監査が可能かどうか、確認する。 ・上記で定義されているシステム上で監査可能なイベントのために、監査記録を生成する機能を情報システムが提供する。 ・組織は、監査に関連する情報が必要な他の組織との間で、セキュリティ監査の整合性を保つことができるようにする。 ・組織は、手作業ないしは情報システムにより自動で生成された監査記録を定期的にでレビュー・分析して、契約事項からの逸脱及び、その兆候の有無を確認する。 ・チェックリストを用いた取引先による内部監査により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。	O	○ (3.3.1)	○ (AU-2, AU-6, AU-12, SA-9)		○ (4.3.2.6.7, 4.3.4.3.1)	○ (SR 6.1)
			<Basic> ・各種認証・制度（ISMS認証、CSMS認証、Pマーク等）の取得証明書を確認することで、必要なセキュリティ対策実施確認の代替とする。	O	-	-	-	-	-
CPS.SC-7	・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, L3_3_d_ORG	<High-Advanced> ・組織は、取引先の監査あるいはテストの不適合が発見された場合、下記を実施するプロシージャを策定し、運用する。 1）不適合から生じるセキュリティの影響を特定し評価する 2）契約で定義されているセキュリティに関わる規定を再検討すべきかどうかを判断する 3）調達された製品またはサービスの範囲内で許容可能なセキュリティレベルを取得するために、実施すべき是正措置を決定する。 4）上記を取引先と同意する	O	-	-	-	-	-
			<Advanced> ・組織は、取引先の監査あるいはテストの不適合が発見された場合、取引先に対して改善計画の策定を求め、計画の実施状況について必要に応じて確認するプロシージャを策定し、運用する。	O	-	-	-	-	-
			<Basic> ・組織は、取引先の監査あるいは製品・サービスに対するテストで不適合が発見された場合、発生した不具合による自組織へのリスクを把握する。	O	-	-	-	-	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.SC-8	・自組織が関係する他組織及び個人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。	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	<High-Advanced> ・組織は、取引先、第三者的な監査機関等の関係する他組織からのリアルタイムでのニーズに柔軟に応じるため、下記の特徴を有した証跡保管システムを利用する。 - 対象となる監査証跡の契約事項に対する適格性を高速で検証することができる - 取引先や委託を受けた監査機関等の許可を受けたエンティティのみがアクセスできる - 保管されているデータが、タイムスタンプや電子署名により証跡としての信頼性を有している	O	-	-	○ (A.12.4.1, A.18.1.3)	-	-
			<Advanced> ・組織は、システムによって生成された監査記録のうち長期にわたって取得する監査記録を確実に取得できるよう、対策を実施する。 ・システムは、監査記録を次の脅威から保護するため、粒度の高いアクセス制御等を監査記録を保存するモノ、システムに適用することが望ましい。 - 記録されたメッセージ形式の変更 - ログファイルの変更又は削除 - ログファイル媒体の記録容量超過	O/S	-	○ (下記に加えて、AU-9, AU-11(1))		○ (4.3.2.6.7)	○ (SR 6.1)
			<Basic> ・組織は、法規制等により要求される事項を満たす事ができるよう、適切な期間の監査記録を保持する。	O	-	○ (AU-11)			-
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、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	L1_3_b_PEO	<High-Advanced> ・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、サプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するテストを実施する。 [参考] サプライチェーンにおけるセキュリティインシデントには、例えば、システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害等がある。	O	○ (3.6.1, 3.6.3)	○ (下記に加えて、IR-4, IR-4(10))	-	-	○ (下記に加えて、SR 3.3)
			<Advanced> ・組織は、インシデント対応要件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、自組織と外部サービスプロバイダーとの間で連携を要するインシデント対応プロセスをテストする。	O	○ (3.6.1, 3.6.3)	(CP-2, CP-2(7))	-	○ (4.3.2.5.7)	○ (SR 2.8, SR 6.1, SR 7.3, SR 7.4)
			<Basic> ・組織は、自組織で起こり得るセキュリティインシデント及び、生じうる被害を把握している。	O	-	-	-	-	-
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	<High-Advanced> ・組織は、製品またはサービスの供給に必要な自組織のリソースにアクセスしそれを処理するために相手方に付与された論理的及び物理的アクセス権が、契約終了後に適時に削除されることを保証する。	O	-	-	-	-	-
			<Advanced> ・組織は、製品またはサービスの供給が取り消されるか、または自組織または他の取引先に返還されるかどうかを現在の取引先と決定する。 ・組織は、製品またはサービスの供給によって影響を受けるヒトにその終了に関する情報を提供するためのコミュニケーションを行う。 ・組織は、終了計画に従い、製品またはサービス供給の終了を実行する。 ・組織は、提供された製品またはサービスの終了の達成について、取引先と同意する。	O	-	-	-	-	-
			<Basic> ・組織は、取引先等の関係する他組織との契約が終了する時期を常に把握している。	O	-	-	-	-	-
CPS.SC-11	・サプライチェーンに係るセキュリティ対策基準及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	<High-Advanced><Advanced><Basic>共通 ・取引先のセキュリティに関わるパフォーマンスを継続的にモニタリングし、最新の脅威動向、規制動向等を踏まえ、サプライチェーンに係るセキュリティ対策基準及び、それに付随するプロシージャをレビューし、必要に応じて改定する。	O	-	-	-	-	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM, L1_1_b_SYS, L1_1_c_COM, L2_3_c_SYS L3_1_a_SYS, L3_3_a_SYS	<High-Advanced> ・組織は、自組織の情報システム及び産業用制御システムにおけるアカウントの管理について、例えば以下のような自動化されたメカニズムを導入し、運用する。 - 管理対象となるシステムからアカウント情報を定期的に自動収集する - 特権アカウントのパスワードを自動で変更する ・産業用制御システムは、統合されたアカウント管理をサポートする。 ・情報システムは、自組織のシステムの一時利用アカウントや緊急アカウント、利用されていないアカウントについて、一定期間の経過後又は申請時利用期限終了後に自動的に無効にする。 ・情報システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化及び無効化について自動的に監査・報告する。	O/S	-	○ (下記に加えて、AC-2 (1), AC-2 (2), AC-2 (3), AC-2(4))	○ (下記に加えて、A.9.2.4, A.9.2.5)	-	-
			<Advanced> ・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・共有ユーザアカウントに関しては、認証情報を知りえるユーザを一覧等で管理し、アカウントを利用する範囲を特定可能にする。 ・組織は、情報システムにおけるシステムアカウントの利用状況をモニタリングする。 ・組織は、アカウントが不要にな-った場合や変更が必要となった場合には管理責任者に通知する。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・組織は、情報システム及び産業用制御システムにおいてパスワードが変更された場合、ユーザー（または管理責任者）に通知する。 ・情報システムは、クレデンシャルを忘れてしまった際等にクレデンシャルを再設定する場合、悪意ある者によるクレデンシャルの不正な変更を防ぐため、当該アカウントが自身のものかどうかを確認するための安全な手順を適用する。	O/S	-			-	-
			<Basic> ・組織は、自組織の情報システム及び産業用制御システムのアカウントを管理する管理責任者を配置する。 ・組織は、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別（例：一般ユーザ／システム管理者／共有ユーザ／一時的なユーザ）を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・組織は、自組織の情報システム及び産業用制御システムに対するクレデンシャル（例：パスワード、セキュリティキー）のポリシーを定め、そのポリシーを満たすクレデンシャルでなければ設定できない機能を実装する。ポリシーの内容の例としては、下記が挙げられる。 - クレデンシャルに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいクレデンシャルが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたクレデンシャルのみを保存・伝送する。 - 同じクレデンシャルを組織が定めた世代にわたって再利用するのを禁止する。 ・クレデンシャルを忘れてしまった際等に、強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なクレデンシャルを使用することを許可する。 ・組織は、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。	O	-	○ (AC-2)	○ (A.9.1.1, A.9.2.1, A.9.2.2, A.9.2.6)	○ (4.3.3.5.1)	○ (SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9)
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, L1_1_c_SYS, L2_3_b_PEO, L2_3_b_SYS, L2_3_c_SYS, L2_3_d_SYS, L3_1_a_SYS	<High-Advanced> ・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。	O	-	○ (下記に加えて、PE-4, PE-5, PE-6 (1))	○ (下記に加えて、A11.1.1.4, A11.2.3)	○ (4.3.3.3.2, 4.3.3.3.8)	-
			<Advanced> ・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。	O	○ (3.10.2, 3.10.4, 3.10.5)	○ (下記に加えて、PE-6, PE-8)	○ (下記に加えて、A.11.1.1, A.11.1.5)		-
			<Basic> ・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設においてセキュリティを保つべき物理的セキュリティ境界を定め、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に応じてアクセス制御を実施する。 ・組織は、物理的セキュリティ境界内における自組織または自組織外の一時的に認可された入場者に対して、認可された関係者の付き添い又は監視カメラ等により作業内容をモニタリングできるようにする。	O	○ (3.10.1, 3.10.3)	○ (PE-2, PE-3, PE-8)	○ (A.9.2.6, A.11.1.2, A.11.1.3, A.11.1.6, A.11.2.8, A.11.2.9)		-
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	<High-Advanced> ・情報システム及び産業用制御システムは、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・情報システム及び産業用制御システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・情報システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・情報システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザ及び機器による認証を暗号化とともに用いることによって保護する。 ・情報システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。	S	○ (下記に加えて、3.1.12, 3.1,13, 3.1.14, 3.1.15, 3.1.17, 3.1.19, 3.10.6, 3.13.12, 3.13.15)	○ (下記に加えて、AC-17(1), AC-17(2), AC-17(3), AC-17(4), AC-18(1), AC-19(5))	-	-	○ (下記に加えて、SR 1.13)
			<Advanced> ・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・組織は、自組織で利用する携帯機器から自組織のシステムの接続に関する承認ルール等を定める。	O	○ (下記に加えて、3.1.18)	○ (下記に加えて、AC-19)	○ (下記に加えて、A.6.2.1)	-	○ (SR 1.1, SR 1.2, SR 2.6)
			<Basic> ・組織は、許可しているリモートアクセスのタイプごとに使用制限・構成要件・実装ガイダンス等を定める。 ・組織は、許可されていない無線接続を原則禁止とする。 ・組織は、自組織の情報システム及び産業用制御システムへのリモートアクセスの利用に関する承認ルール等を定める。 ・組織は、自組織のシステムへの無線によるアクセスを許可するのに先立って、無線でシステムにアクセスする権限を与える。	O	○ (3.1.16)	○ (AC-17, AC-18)	○ (A.6.2.2)	-	

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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	<High-Advanced> ・情報システム及び産業用制御システム（対応の即時性が求められる一部の例を除く）は、自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定し、上限以上失敗した場合には管理者が解除しなければ再ログインできない機能を実装する。	S	○ (3.1.8)	○ (AC-7)	○ (A.9.4.2)	-	○ (SR 1.11)
			<Advanced> ・情報システム及び産業用制御システムは、自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定し、上限以上失敗した場合には一定期間再ログインできない機能を実装する。 ・情報システム及び産業用制御システムは、組織が定める時間を越えてシステムの無操作が持続する場合、手動又は自動でセッションロックを実施する。 ※ 産業用制御システムにおいて、緊急時対応においてオペレータの即時対応が求められるようなセッションを実施するケースが想定される場合、セッションロックを実施しないことが望ましい。	S				-	○ (SR 1.11, SR 1.13, SR 2.6)
			<Basic> (該当なし)	-	-	-	-	-	-
CPS.AC-5	・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	L1_1_a_SYS, L1_1_b_SYS, L2_1_c_SYS, L3_1_a_SYS	<High-Advanced> ・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・情報システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入する。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・組織は、セキュリティインシデントによる被害を最小化するため、有事においてシステム管理者の権限を利用できるユーザを最少化させることができる。 ・組織は、セキュリティインシデントによる被害を最小化するため、システム管理者であっても、サーバの重要なサービスや保護されたプロセスを停止できないようにすることができる。	O/S	○ (下記に加えて、3.1.6, 3.1.7)	○ (下記に加えて、AC-6(1), AC-6(2), AC-6(5), AC-6(9), AC-6(10))	○ (A.6.1.2, A.9.2.3, A.9.4.1, A.9.4.4)	-	-
			<Advanced> ・組織は、自組織の情報システム及び産業用制御システムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 - 一般のユーザアカウントの権限と、特権アカウントの権限を分離する (非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。) - 自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。	O	○ (3.1.4, 3.1.5, 3.13.3)	○ (AC-3, AC-5, AC-6, SC-2)		○ (4.3.3.2.7)	-
			<Basic> ・組織は、自組織の機密性の高い情報システムにおいて職務分離（例：ユーザ／システム管理者）を踏まえたアクセス制御を実施する。 ・人的リソース等の関係で、職務の分離が困難な場合、あらかじめ指定された役職者以外が特定の職務を実行する際に、他の要員が職務の遂行をモニタリングする等の代替策を講ずることが望ましい。	O	-	-	-	-	○ (SR 2.1)
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、想定されるリスクも考慮して、信頼性の高い認証方式（例：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_a_SYS, L1_1_b_SYS, L2_1_c_SYS, L3_1_a_SYS	<High-Advanced> ・情報システム及び産業用制御システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織の情報システムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。	S	○ (下記に加えて、3.5.4)	○ (下記に加えて、IA-2(2), IA-2(8), IA-2(9))	○ (下記に加えて、A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4)	-	○ (SR 2.1)
			<Advanced> ・組織は、対象システムにおける特権アカウントへの不正ログインのリスク等を勘案し、十分に信頼性の高い認証方式を実装できない場合、ネットワーク経由での特権アカウントへのログインを原則禁止する。 ・情報システムは、自組織のシステムについて管理者アカウントの無効化等制限が実施できない場合には、特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を要求する。 ・情報システムにおけるデフォルトの管理者アカウントは、原則無効化する。 ・情報システムは、権限付与等の特権操作を実施する場合には、利用ユーザアカウントに対して必要最小限の特権操作権限を付与する。	S	○ (下記に加えて、3.5.3)	○ (下記に加えて、IA-2(1), IA-2(3))		-	
			<Basic> ・組織は、自組織のシステムについて特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、一意に識別する認証を実施する。	O/S	○ (3.5.1)	○ (IA-2)	○ (A.9.2.1)	-	

添付C

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.AC-7	・データフロー制御ポリシーを定め、それに従って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_DAT, L3_4_b_SYS	<High-Advanced> ・情報システム及び産業用制御システムは、自組織のシステムを構成するネットワークの内部における境界について通信をモニタリングし、制御する。 ・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・機密性の高いデータを取り扱う自組織の情報システムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。	S	○ (下記に加えて、3.1.3, 3.13.6, 3.13.7)	○ (下記に加えて、SC-7(5), SC-7(7))	○ (下記に加えて、A.13.1.1, A.13.1.3, A.14.1.2, A.14.1.3)	-	-
			<Advanced> ・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界（産業用制御システムの場合は情報システムとの境界）について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。	O/S	-	○ (下記に加えて、SC-7)		○ (4.3.3.4.2, 4.3.3.4.3)	○ (SR 3.1, SR 3.8)
			<Basic> ・組織は、情報システム及び産業用制御システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、適切に論理的あるいは物理的にネットワークを分離することで、フローの制御を実施する。 ・組織は、産業用制御システムにおいて、制御システムのネットワークを情報システムとのネットワークから論理的あるいは物理的にセグメント化する。 [参考] 他のネットワークと物理的に離れた環境においては物理的なセグメント化を実施する、他のネットワークと物理的に近接した環境では、対策のコスト等も考慮して論理的なセグメント化を実施する等の対応が可能である。	O/S	○ (3.1.3)	○ (AC-4)	○ (A.12.1.4, A.13.2.1)	○ (4.3.3.4.1)	
CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	L2_1_b_SYS, L3_3_a_SYS	<High-Advanced><Advanced><Basic>共通 ・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・IoT機器での通信は、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。	O/S	○ (3.5.5, 3.5.6, 3.8.2)	○ (IA-4)	○ (A.7.1.1, A.9.2.1)	○ (4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.3)	○ (SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1)
CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	L1_1_a_SYS, L1_1_b_SYS, L2_1_b_SYS, L3_1_a_SYS, L3_4_b_SYS	<High-Advanced> ・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。	S	○ (下記に加えて、3.1.11)	○ (下記に加えて、IA-2, IA-5(2), AC-12)	○ (A.9.3.1, A.9.4.3, A.9.4.5)	○ (下記に加えて、4.3.3.6.3, 4.3.3.6.5, 4.3.3.6.7)	○ (下記に加え、SR 1.9)
			<Advanced> ・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。	O/S	○ (3.1.1, 3.1.2, 3.1.9, 3.1.10, 3.5.2, 3.5.7, 3.5.8, 3.5.9, 3.5.10, 3.5.11)	○ (IA-5, IA-5(1), IA-6, AC-8, AC-11, AC-11(1))		○ (4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.4, 4.3.3.6.6, 4.3.3.6.8, 4.3.3.6.9)	○ (SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.10)
			<Basic> ・組織は、自組織の情報システム及び産業用制御システムに対するクレデンシャル（例：パスワード、セキュリティキー）のポリシーを定め、そのポリシーを満たすクレデンシャルでなければ設定できない機能を実装する。ポリシーの内容の例としては、下記が挙げられる。 - クレデンシャルに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいクレデンシャルが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたクレデンシャルのみを保存・伝送する。 - 同じクレデンシャルを組織が定めた世代にわたって再利用するのを禁止する。 ・クレデンシャルを忘れてしまった際等に、強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なクレデンシャルを使用することを許可する。 ・情報システム及び産業用制御システムは、認証されたユーザに対して、実行可能なトランザクション及び機能を制限する。	O/S	-	-	-	-	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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、教育を実施し、その記録を管理する。	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO, L1_1_d_PEO, L1_2_a_PEO, L1_3_a_PEO, L1_3_a_DAT, L1_3_c_PEO, L3_4_a_PEO	<High-Advanced> ・組織は、内部不正の兆候を認識・報告するためのセキュリティ意識向上トレーニングを、全要員に対して実施する。	O	○ (下記に加えて、3.2.3)	○ (下記に加えて、AT-2(2))	○ (A.7.2.1, A.7.2.2)	-	-
			<Advanced> ・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。組織は、CPS.AT-1 <Basic> の[参考]に記載されている一般的な事項を解説しているコンテンツに加えて、組織によって内容が異なる内容として、例えば、下記の事項を扱うことができる。 - 不審なメールを受信した際の対応手順（どこにどのような内容を連絡すればよいか） - モバイル端末利用の注意点（例：公衆無線LANに接続する際の注意点） - SNSを利用する際の注意点 ・組織は、情報セキュリティ要員の育成とレベル向上のための役割別（例：システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者）のプログラムを作成し、定期的に該当する要員に対して実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の記録を定期的にレビューする。	O	○ (3.2.1)	○ (下記に加えて、AT-3)		○ (4.3.2.3.4, 4.3.2.4.1, 4.3.2.4.2, 4.3.2.4.6, 4.3.3.2.5, 4.3.4.5.4, 4.3.4.5.11)	-
			<Basic> ・組織は、自組織の利用する情報システム及び産業用制御システムに対する変更により必要になった場合や新規職員に対して基本的なセキュリティ意識向上トレーニングを実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の内容や結果等について記録し、管理する。 [参考] 組織が従業員等に対してセキュリティ教育を実施する際、IPAが公開している「情報セキュリティ読本 教育用プレゼン資料」の内容を参照することが可能である。	O	-	○ (AT-2)			-
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得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	L1_3_b_PEO, L1_3_a_DAT, L3_3_a_PEO	<High-Advanced> ・組織は、自組織の要員及びセキュリティインシデントに関係しうる関係組織に対して、担当する要員へ割り当てられた役割の遂行状況をモニタリングを実施する。	O		-	-	-	-
			<Advanced> ・組織は、自組織におけるセキュリティインシデントに関係しうる関係組織に対して、担当する要員へ割り当てられた役割を遂行するための適切な訓練（例：実際のインシデント発生時を想定した、シミュレーション）、セキュリティ教育を実施を要求し、その実施状況を確認する。 ・組織は、自組織のセキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対する教育・訓練の記録を定期的にレビューする。	O	○ (下記に加えて、3.2.2)	-	-	○ (下記に加えて、4.3.2.4.3, 4.3.4.5.11)	-
			<Basic> ・組織は、自組織の要員へ割り当てられた役割を遂行するための適切な訓練（例：実際のインシデント発生時を想定した、シミュレーション）、セキュリティ教育を実施を要求し、その実施状況を確認する。 ・組織は、自組織のセキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対する、セキュリティに係る教育・訓練の内容や結果等について記録し、管理する。	O	○ (3.2.1)	-	-	○ (4,3,2,4,1, 4.3.2.4.2, 4.3.2.4.6)	-
CPS.AT-3	自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO, L1_3_a_PEO, L1_3_b_PEO, L1_3_c_PEO, L3_3_a_PEO, L3_4_a_PEO	<High-Advanced><Advanced>共通 ・組織は、自組織の要員及び関係他組織の担当者等のセキュリティに対する理解をより確実にするため、教育、訓練による効果を継続的に検証する。 ・組織は、セキュリティに係る教育・訓練に関する記録のレビュー結果を参照し、新たな又は変化する脅威、脆弱性の情勢を踏まえて、教育、訓練の内容を改定する。	O	-	○ (AT-1)	○ (A.7.2.2)	○ (4.3.2.4.4, 4.3.2.4.5)	-
			<Basic> ・組織は、セキュリティに係る教育、訓練の実施後に、対象者の実施内容に対する理解を確認するため、アンケートや簡易のテスト等を実施し、結果を確認する。	O	-			-	-
CPS.DS-1	・組織間で保護すべき情報を交換する場合、当該情報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。	L3_1_a_PRO, L3_4_a_DAT, L3_4_b_DAT	<High-Advanced><Advanced>共通 ・組織は、交換するデータの重要度、想定されるリスクを勘案して、具体的なセキュリティ対策要件を指定し、取引先に対して実装を求める。 ・組織は、再委託先以降の事業者へのデータ取扱い業務の委託を、直接の取引先に求める水準のセキュリティ対策が実装されていることが確認される場合に限って、許可する。	O	-	-	-	-	-
			<Basic> ・組織は、取引先が取り扱う可能性のあるデータに関して、秘密保持契約を締結することで、取り扱いを規定する。 ・組織は、直接の取引先に対して、データの管理に関わる業務の再委託を禁止する。 [参考] 「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年)で、委託契約時の機密保持契約条項のサンプルを提供している。	O	-	-	-	-	-
CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	L1_1_a_DAT, L3_1_a_DAT, L3_3_d_SYS, L3_4_b_SYS	<High-Advanced> ・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・組織は、内部メモリのデータを暗号化して保管することのできるIoT機器を利用する。	O/S	○ (下記に加えて、3.8.6, 3.13.11, 3.13.8)	○ (下記に加えて、SC-12(1))	○ (A.8.2.3)	-	-
			<Advanced> ・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されたアルゴリズムが選択可能であれば、これを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。 ・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、産業用制御システムが取り扱う重要度の高い情報（データ）を、パフォーマンスに許容できない影響が出ない範囲で適切な強度の方式で暗号化して保管する。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。	O/S	○ (下記に加えて、3.13.16)	○ (下記に加えて、SC-28)		-	○ (SR 3.4, SR 4.1)
			<Basic> ・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報システムが取り扱う重要度の高い情報（データ）を適切な強度の方式で暗号化して保管する。	O/S	○ (3.13.10)	○ (SC-12)		-	

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.DS-3	・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_DAT, L3_2_b_DAT, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> ・組織は、情報システム及び産業用制御システムを構成する重要なデータを扱う通信路について、通信経路の暗号化を実装する又は代替の物理的な対策によって保護する。	O/S	○ (3.13.15)	○ (下記に加えて、SC-12(1))	○ (A.10.1.1,A.13.2.1, A.13.2.3, A.14.1.2)	-	○ (SR 3.1, SR 3.8, SR 4.1, SR 4.2, SR 4.3)
			<Advanced> ・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。	S	○ (3.13.15)	○(SC-8(1), SC-12)		-	
			<Basic> （該当なし）	-	-	-	-	-	-
CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。	L1_1_a_DAT, L1_1_b_DAT, L3_1_a_DAT, L3_2_b_DAT, L3_3_d_SYS	<High-Advanced> ・システム/IoT機器は、少ないリソースでも可用性を損なわずに実装可能な暗号モジュールを導入し、リソースは制限されているが重要度の高い機器からの通信データを適切な強度で暗号化することが望ましい。 ・情報システムは、重要度の高い・低いに限らず、組織外部へ送信するすべてのデータを適切な強度で暗号化する。	S	-	-	○ (A.10.1.1, A.13.2.1, A.13.2.3, A.14.1.2)	-	○ (SR 3.1, SR 3.8, SR 4.1, SR 4.2, SR 4.3)
			<Advanced> ・組織は、機密性の高い情報を外部の組織等へ送信する際、情報を適切な強度の方式で暗号化する。	O	-	○ (SC-8(1))		-	
			<Basic> （該当なし）	-	-	-	-	-	-
CPS.DS-5	・送受信する情報データ、保管データする情報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_DAT	<High-Advanced> ・組織は、ユーザが暗号鍵を紛失した場合に、鍵の再発行等により情報の可用性を維持する。 ・秘密鍵及びプライベート鍵をセキュリティを保って管理することに加え，公開鍵の真正性についても考慮することが望ましい。この認証プロセスは，認証局によって通常発行される公開鍵証明書を用いて実施される。この認証局は，要求された信頼度を提供するために適切な管理策及び手順を備えている，認知された組織であることが望ましい。	O/S	-	○ (下記に加えて、SC-12(1))	○ (A10.1.2)	-	-
			<Advanced>共通 ・組織は、秘密鍵が危殆化した際に遅滞なく適切な対処を行うため、必要に応じて下記のような事項について方針及び手順を定めることが望ましい。 - 秘密鍵の危殆化に対応するための体制(関係者と役割、委託先との連携を含む) - 秘密鍵が危殆化した、またはその恐れがあると判断するための基準 - 秘密鍵の危殆化の原因を調べること及び原因の解消を図ること - 当該鍵を利用するサービスの利用停止 - 新しい鍵ペアを生成し、新しい鍵に対する証明書を発行すること - 秘密鍵の危殆化についての情報の開示(通知先、通知の方法、公表の方針等) [参考] 鍵管理に関するより詳細な内容については、ISO/IEC 11770規格群や、NIST SP 800-57 Part 1 Rev.4等を参照することが望ましい。	O	○ (3.13.10)	○ (SC-12)		-	○ (SR 1.9, SR 4.3)
			<Basic> ・組織は、全ての暗号鍵を改変及び紛失から保護することが望ましい。	O				-	
CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する。	L1_1_c_SYS, L2_1_d_SYS, L3_3_c_SYS	<High-Advanced><Advanced>共通 ・情報システム及び産業用制御システムは、予備の容量／帯域幅／その他の予備リソース（ヒト／モノ／システム等）を管理して、大量の情報を送りつけるタイプのサービス拒否攻撃による影響を最小限に抑える。例えば、攻撃を受けているシステムが提供するサービスを、可用性の水準維持等の理由により停止できない場合、重要な機能を継続するため、以下のような対策をとる必要がある。 - 待機している予備システムへの自動的、あるいは、人手を介した移行 - ネットワークアクセスからの攻撃を受けたシステム構成要素の、自動的あるいは人手を介した隔離 ・要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整しなければならず，また，将来必要とする容量・能力を予測しなければならない。 ・組織は、 (a) 情報システムに対するサービス妨害攻撃の兆候を発見するための組織が定めた、モニタリングツールを使用する (b) 組織が定めた情報システム及び産業用制御システムのリソースをモニタリングして、効果的なサービス妨害攻撃を阻止するための十分なリソースが確保されているかどうかを判断する	S	-	○ （下記に加えて、SC-5(2)、SC-5(3)）	○ （下記に加えて、A.12.1.3）	-	○ （SR 5.2）
			<Basic> ・情報システム及び産業用制御システムは、組織が定めたセキュリティ対策を実施することによって、組織が定めたタイプのサービス拒否攻撃、またはそうした情報の情報源への参照のサービス拒否攻撃による影響から保護する、あるいはそうした影響を最小限に抑え、縮退運転を実施する機能を提供する。	S	-	○（SC-5）	○ （A.17.2.1）	-	
CPS.DS-7	・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。	L1_1_c_SYS, L2_1_d_SYS, L3_3_c_SYS	<High-Advanced><Advanced>共通 ・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。	O	-	○（PE-11）	○ （A.11.2.2、A.11.2.3、A.11.2.4、A.12.1.3, A.17.2.1）	-	○ （SR 5.2, SR 7.5）
			<Basic> ・組織は、情報システム及び産業用制御システムに要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 ・組織は、サポートユーティリティの不具合による停電、その他の故障から装置を保護する。 ・組織は、データを伝送する又はサービスをサポートする通信ケーブル及び電源ケーブルの配線を傍受、妨害又は損傷から保護する。 ・組織は、可用性及び完全性を継続的に維持することを確実にするために、装置を正しく保守する。	O	-	-		-	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.DS-8	・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	<High-Advanced> ・組織は、保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用した機器を調達する。 ・組織は、情報システム及び産業用制御システム内で使用されている暗号技術向けの暗号鍵を保管するにあたり耐タンパーデバイスを用いて管理する。	O	-	○（SC-12）	○（A.10.1.2）	-	○ （SR 5.2）
			<Advanced> （該当なし）	-	-	-	-	-	-
			<Basic> （該当なし）	-	-	-	-	-	-
CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	L1_1_a_DAT, L2_3_c_SYS, L3_1_a_DAT	<High-Advanced> ・産業用制御システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・組織/情報システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い（通信）を検知できるようにする。 ・共有システム資源を介した、不正な予期せぬ情報の転送を防止する。	S	○ (3.13.4)	○ （下記に加えて、SC-4）	○ (A.13.2.1)	-	-
			<Advanced> ・情報システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・組織は、公開された新たな攻撃動向、マルウェア挙動情報や悪性IP アドレス／ドメイン情報などの情報（外部インテリジェンス）を収集し、必要に応じて危険性の高いIPアドレスやドメインへの通信を遮断する等の対応を実施する。	O/S	○ (3.13.1)	○ (SC-7)		-	○ （SR 5.2）
			<Basic> ・組織は、自組織外部に向けた大量のデータ通信を検知し、必要に応じてそのような通信の実施を制限する。	O/S	-	-		-	-
CPS.DS-10	・IoT機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。	L2_3_b_SYS	<High-Advanced> ・組織は、情報システムにおいて完全性検証時に不一致が発見された場合にシステム管理者に通知する、自動化されたツールを使用する。 ・組織は、不正なソフトウェアが検知された場合に、対象ソフトウェアの起動を防止するツールを使用する。 ・組織は、設定の不正な変更や、システム権限の不正な昇格等の、セキュリティ関連の変更が不正に行われた場合の検知能力を、組織のインシデント対応能力に組み入れる。	O/S	-	○ （下記に加えて、SI-7(2), SI-7(7)）	○ (A.12.2.1)	-	-
			<Advanced> ・情報システムは、ソフトウェア・ファームウェアの完全性チェックを定期的に実施する。 ・情報システム及び産業用制御システムは、起動を許可するソフトウェアを事前に登録しておくことで、登録されていないソフトウェアの起動を停止する。	S	-	○ (SI-7, SI-7(1))		-	○ （SR 3.1, SR 3.3, SR 3.4, SR 3.8）
			<Basic> （該当なし）	-	-	-		-	-
CPS.DS-11	・送受信・保管する情報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	<High-Advanced> ・組織は、産業用制御システムにおいて、可能な場合、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・組織は、設定の不正な変更や、システム権限の不正な昇格等の、セキュリティ関連の変更が不正に行われた場合の検知能力を、組織のインシデント対応能力に組み入れる。	O	-	○ （下記に加えて、SI-7(7)）	○ (A.14.1.2, A.14.1.3)	-	-
			<Advanced> ・組織は、情報システムにおいて、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・情報システムは、保管データの完全性チェックを定期的に実施する。 ・情報システムは、電子メールにおける送信ドメイン認証技術をサポートして、送信者のなりすましやメールの改ざんを検知する。	O/S	-	○ (SI-7, SI-7(1))		-	○ （SR 3.1, SR 3.3, SR 3.4, SR 3.8）
			<Basic> （該当なし）	-	-	-	-	-	-
CPS.DS-12	・ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。	L1_1_d_PRO, L2_3_b_SYS	<High-Advanced> ・組織は、IC チップの純正品と不正品のサイドチャネル情報の違いからハードウェアの改ざん（ハードウェア・トロイの挿入）を検知する。 ・組織は、PUF（Physically unclonable function）の技術を活用して物理的に読取り可能なチップの固有IDを生成し、テストを通じてハードウェアの改ざん(ハードウェア・トロイの挿入)を検知する。	O	-	-	-	-	-
			<Advanced> ・組織は、ハードウェアコンポーネントに対する不正な変更を検知するツール、複製しにくいラベルや、検証可能なシリアル番号等を用いて、完全性を確認できるようにする。 ・組織は、自組織のオペレーションにとって重要なハードウェアについて、設置エリアに対して監視カメラ等によるモニタリングを行うことで、ハードウェアに対する物理的な改ざんを検知できるようにする。	O	-	○ (PE-6, SA-10(3))	-	○ (4.3.4.4.4)	-
			<Basic> （該当なし）	-	-	-	-	-	-
CPS.DS-13	・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	<High-Advanced> ・組織は、機器のシリアル番号やハッシュ値等を利用して、定期的にIoT機器及び搭載されているソフトウェアが正規品であること確認するために、自動化されたメカニズムを含むツールを利用する。	O	-	-	-	-	-
			<Advanced> ・組織は、機器のシリアル番号やハッシュ値等を利用して、定期的にIoT機器及び搭載されているソフトウェアが正規品であることを確認する。	O	-	-	-	-	-
			<Basic> ・組織は、調達時や資産の棚卸しを実施した際等に、自組織が所有するIoT機器が正規品であるかをラベルを確認する等して確かめる。	O	-	-	-	-	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.DS-14	・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, L3_4_b_PRO	<High-Advanced> ・組織は、自組織が管理するデータの処理を実施するサイバー空間におけるサプライチェーンの中に、自組織が委託先等に要求している水準の対策を実装していないエンティティが介在していないかを確認する。	O	-	-	-	-	-
			<Advanced> ・組織は、他組織あるいは、自組織外の個人、IoT機器等から取得したデータの取得元を、当該データに紐づけて、取得から廃棄に至るまでのライフサイクル全体に渡り管理する。 ・組織は、自組織が利活用するデータの取得元及び、当該データを処理した組織、ヒト等を識別する。	O	-	-	-	-	-
			<Basic> ・組織は、他組織あるいは、自組織外の個人から取得したデータの取得元を、当該データに紐づけて、取得から廃棄に至るまでのライフサイクル全体に渡り管理する。	O	-	-	-	-	-
CPS.DS-15	・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_COM, L2_1_a_PRO, L2_3_a_ORG, L2_3_d_ORG	<High-Advanced><Advanced>共通 ・ネットワーク接続性を持ち、フィジカル空間における動態をデジタル化しサイバー空間へ送信する機能を有する機器（センサ等）を導入する際、当該機器の機能における下記の観点を考慮し、調達を実施することが望ましい。 - 完全性検証ツールを使用して、通信データに対する不正な変更を検知する機能を実装しているか - 他のIoT機器、サーバ等から識別可能なユニークIDを有するか、あるいは証明書を搭載しており、通信先との相互認証等を通じて真正性を主張できるか - 機器のリソースが、ある程度の規模のサービス拒否攻撃等を受けた際でも可用性を維持することが可能なレベルのものか	O	-	○ (SC-5, SC-6, SI-7)	-	-	-
			<Basic> ・組織は、 物理的な攻撃に対して耐性を有しているIoT機器（センサ等）を調達する。	O	-	-	-	-	-
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。	L1_1_a_SYS, L1_1_b_SYS, L2_1_a_ORG, L2_1_b_COM, L2_1_b_PRO, L2_3_b_ORG, L3_1_a_SYS, L3_3_d_SYS	<High-Advanced> ・組織は、構成管理の対象となるIoT機器、サーバ等に対して変更を実施する前に、それらの変更をテスト・承認・文書化する。 ・組織は、IoT機器、サーバ等の設定を一つの場所から管理・適用・検証するための自動化されたメカニズムを使用する。 ・組織は、特に産業用制御システムにおけるセキュリティに係る変更管理手順を、既存のプロセス安全管理の手順に統合する。	O	-	○ (下記に加えて、CM-3(2))	○ (A.12.1.2, A.12.5.1)	-	○ (SR 7.6)
			<Advanced> ・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法（例：変更実施前に本人にしかわからないセキュリティコードを入力させる）を利用する。 ・組織は、セキュリティ上の変更によって情報システム及び産業用制御システムの可用性や安全性等に悪影響が及ばないことを確実にするため、運用及び変更管理のポリシー及び手順を定期的にレビューする。	O	○ (下記に加えて、3.4.3, 3.4.4, 3.4.5)	○ (下記に加えて、CM-3, CM-4, CM-5)		○ (4.3.4.3.2, 4.3.4.3.3)	
			<Basic> ・組織は、自組織の運用に適合する最も制限された設定基準を定めた上で、導入されるIoT機器、サーバ等の初期設定手順及び設定内容を文書化するとともに、その文書に従って設定を実施する。 ・組織は、IoT機器を設置する前にデフォルトの初期設定値を確認し、CPS.AC-1で定めたポリシーに準じていない場合に適切なものへと変更する。 ・組織は、IoT機器の導入前に、搭載されているソフトウェアを確認し、記録する。	O	○ (3.4.2)	○ (CM-6)		-	
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_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> ・組織は、自組織の情報システム及び産業用制御システム上で実行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）を用いてソフトウェアの制限を実施する、あるいは、許可されていないソフトウェアのインストールを不可とする。	O/S	○ (下記に加えて、3.4.8)	○ (下記に加えて、CM-7(4), CM7-(5))	○ (下記に加えて、A.12.5.1)	-	-
			<Advanced> ・組織は、自組織の情報システム及び産業用制御システム上でのユーザによるソフトウェアのインストールについて管理するメカニズムを導入し、管理する。	O/S	○ (3.4.9)	○ (CM-11)	○ (A.12.6.2)	○ (4.3.4.3.2, 4.3.4.3.3)	-
			<Basic> ・組織は、自組織の情報システム及び産業用制御システム上でのユーザによるソフトウェアのインストールに関するポリシーを確立し、ユーザに遵守させる。	O	-	-			○ (SR 7.6)
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する。	L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG, L2_1_d_SYS, L3_3_c_SYS	<High-Advanced> ・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 -セキュリティ機能に関する要求事項 -セキュリティ強度に関する要求事項 -セキュリティ保証に関する要求事項 -セキュリティ関連のドキュメントに関する要求事項 -セキュリティ関連のドキュメントの保護に関する要求事項 -そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 -受け入れ基準	O	-	○ (下記に加えて、SA-4)	○ (下記に加えて、A.6.1.5, A.14.2.2, A.14.2.5)	-	-
			<Advanced> ・組織は、 情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。	O	-	○ (下記に加えて、SA-3)		○ (4.3.4.3.3)	○ (SR 7.3, SR 7.4)
			<Basic> ・組織は、システムを構築するに当たり仕様書、設計、開発、導入及び変更に、システムのセキュリティエンジニアリング原則を適用する。	O	○ (3.13.2)	○ (SA-8)	○ (A.14.1.1, A.14.2.1, A.14.2.6)		

添付C

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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、テストする。	L1_3_a_DAT, L2_1_d_SYS, L3_3_c_SYS	<High-Advanced> ・組織は、バックアップ情報を定期的にテストして、媒体の信頼性と情報の完全性を確認する。	O	-	○ （下記に加えて、CP-9(1)）	○ （下記に加えて、A.14.3.1）	○ （4.3.4.3.9）	-
			<Advanced> ・組織は、自組織のシステムドキュメントのバックアップを定めたタイミングや頻度で実施する。 ・組織は、保管拠点におけるバックアップ情報の機密性・完全性・可用性を保護する。	O	○ （3.8.9）	○ （CP-9）	○ （下記に加えて、A.18.1.3）		-
			<Basic> ・組織は、自組織の情報システム及び産業用制御システムに含まれるユーザレベル・システムレベルの情報のバックアップを定めたタイミングや頻度で実施する。	O			○ （A.12.3.1）		-
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, L1_1_c_SYS, L2_3_b_SYS, L2_3_d_SYS, L3_1_a_SYS	<High-Advanced> ・組織は、自組織の利用するシステムが設置されている施設に職員が常駐しない場合には、自動消火機能を導入する。	O	-	○ （下記に加えて、PE-13, PE-15）	○ （A.11.1.4, A.11.2.1, A.11.2.2）	-	-
			<Advanced> ・組織は、無停電電源装置等により自組織のIoT機器、サーバ等が設置されているエリア内の機器の安定な稼働を維持する。 ・組織は、独立した電源等により稼働する消火及び火災検知のための装置やシステムを導入し、維持する。 ・組織は、閉止弁や遮断弁を用意し、自組織のIoT機器、サーバ等が設置されているエリアを水漏れ等の被害から保護する。	O				○ （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）	-
			<Basic> ・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定めた許容レベルに保つ仕組みを導入する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定期的にモニタリングする。	O	-	○ （PE-14）		-	-
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	<High-Advanced> ・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。	O	○ （3.8.3）	○ （MP-6）	○ （下記に加えて、A.8.2.3）	-	○ （SR 4.2）
			<Advanced> ・組織は、自組織のIoT機器やサーバ等を廃棄するプロシージャを定め、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。	O			○ （A.8.3.1, A.8.3.2, A.11.2.7）	-	
			<Basic> ・組織は、自組織のIoT機器やサーバ等を廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態にする。	O				-	
CPS.IP-7	・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	L1_1_a_PRO, L1_1_b_PRO, L1_1_c_PRO, L2_1_a_ORG	<High-Advanced> ・組織は、第三者によるセキュリティ評価を実施する。	O	-	○ （下記に加えて、CA-2(1)）	○ （A.16.1.6, A.18.2.1, Clause 9.1, Clause 9.2, Clause 10.1, Clause 10.2）	-	-
			<Advanced> ・組織は、セキュリティ評価を適切かつ計画的に実施するため、以下に示す事項を含めたセキュリティ評価計画を策定した上で、セキュリティ評価を実施する。 -セキュリティ評価の対象とするセキュリティ対策 -セキュリティ対策の有効性を図るために用いる評価手順 -セキュリティ評価を実施する環境や実施体制 -セキュリティ評価結果の取りまとめ方法とその活用方法	O	○ （3.12.1）	○ （CA-2）		○ （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）	-
			<Basic> ・組織は、セキュリティ対策が正しく実装されているか及び運用されているかに加え、セキュリティ対策が期待された成果を上げているかに関する定期的に評価（セキュリティ評価）を実施し、管理責任者へ報告する。 ・組織は、セキュリティ評価の結果に基づき、セキュリティ対策の改善を実施する。	O					-
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_ORG	<High-Advanced> ・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、自動化されたメカニズムを通じて適切なパートナーと適時双方向で共有をすることができる環境を整備する。	O	○ （3.14.4）	○ （AC-21）	○ （A.16.1.6）	-	-
			<Advanced> ・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、パートナーに適時共有することができる環境を整備する。	O				-	-
			<Basic> ・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、適切なパートナーから入手できる環境を整備する。 [参考] 適切なパートナーを選定するに当たり、「情報セキュリティサービス基準適合サービスリスト」に記載された事業者のサービスを利用することが考えられる。また、パートナーには、情報処理安全確保支援士やCISSP等のセキュリティに係る資格を有している要員を含めることが望ましい。	O	-	-		-	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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）を含める。	L1_1_a_PEO, L1_1_b_PEO, L1_1_c_PEO	<High-Advanced><Advanced>共通 ・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。 ・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。 ・組織は、機密情報を扱う要員に対しては特に、採用から退職に至るまでのサイクル全体に渡り、セキュリティ上の責任に対処する。	O	○ (3.9.1 3.9.2)	○ (下記に加えて、PS-5)	○ （下記に加えて、A.7.2.3, A.7.3.1)	○ （下記に加えて、4.3.3.2.3, 4,3,3,2,4)	-
			<Basic> ・組織は、雇用条件においてセキュリティに係る要員の責任について明記する。雇用終了後の情報漏えい等を抑止するため、この責任は、雇用終了後の妥当な期間に渡って持続するよう記載する。 ・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。 ・組織は、要員の退職時に以下を実施する。 -自組織のシステムに対するアクセスを一定期間内に無効にする。 -職員に関連する認証及びクレデンシャルを無効にする。 -セキュリティに関連するシステム関連の所有物をすべて回収する。 -退職する個人が管理していた組織の情報と情報システムに対するアクセスを保持する。	O		○ (PS-3, PS-4)	○ (A.7.1.1, A.7.1.2, A.7.2.1, A.8.1.4)	○ (4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.6, 4.3.4.4.2)	-
CPS.IP-10	・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	L1_1_a_SYS, L2_1_a_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> ・組織は、欠陥修正状況を管理するための自動化されたメカニズムを導入し、管理する。	O	-	○ (下記に加えて、SI-2(2))	○ （下記に加えて、A.14.2.3)	-	-
			<Advanced> ・パッチ適用中のIoT機器、サーバ等の動作により、他のソフトウェアアプリケーションやサービスの機能への影響が出るかどうかを調査やテストを通じて明らかにして、受容できるリスクを定める。 ・組織は、修正内容の有効性と副次的な悪影響の可能性についてテストを行った上で欠陥の修正を実施し、当該修正を構成管理として管理する。	O	○ (3.14.3)	○ (SI-2)		○ (4.3.4.3.7)	-
			<Basic> ・組織は、自組織の情報システム及び産業用制御システムに関する欠陥の特定・報告・修正を計画的に実施する。計画を策定する際には、下記を考慮することが望ましい。 - 脅威または脆弱性の深刻さ - 修正措置の適用に関わるリスク [参考] 特に、製造現場等に設置されるIoT機器や制御機器（例：PLC、DCS）には、可用性や機器自体の機能の関係で、タイムリーにパッチを適用すること、あるいはパッチの適用事態が困難な場合がある。その場合は、「制御システム利用者のための脆弱性対応ガイド 第2版」(IPA, 2016年)のP.23に記載されている通り、脅威への対策（機能の最小化、ネットワーク監視の強化等）を徹底し、セキュリティ被害の発生を回避することが望ましい。 ※ PLC: Programmable Logic Controller, DCS: Distributed Control System	O	-	-	○ (A.12.6.1)		-
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、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 ・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_ORG, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS L3_3_d_SYS	<High-Advanced> ・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な変更または不正な変更がないか確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。	O	○ (3.7.1, 3.7.2, 3.7.4)	○ (下記に加えて、MA-3, MA-3(1), MA-3(2))	○ （下記に加えて、A.11.2.4, A.11.2.5, A.11.2.6, A.14.2.4)	○ (4.3.3.3.7)	-
			<Advanced> ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。	O	○ (下記に加えて、3.7.1, 3.7.2, 3.7.4)	○ (下記に加えて、MA-2)			-
			<Basic> ・組織は、メンテナンス要員が付添いなしで情報システム及び産業用制御システムのメンテナンスを行う場合に、その要員が必要なアクセス権限を有することを確認する。 ・組織は、必要なアクセス権限を持たない要員によるメンテナンス活動を監督するのに必要なアクセス権限と技術的能力を有する組織の要員を指定する。	O	○ (3.7.6)	○ (MA-5)	○ (A.11.1.2)		-
CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	L1_1_a_SYS, L2_1_a_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced><Advanced>共通 ・組織は、遠隔保守のための接続の確立と実施に関するポリシーとプロシージャを文書化し、その内容により実施する。 ・組織は、遠隔保守を実施する際には組織の定めるネットワークアクセスに求める認証を実施するとともに、遠隔保守が完了したらセッションとネットワーク接続を確実に終了する。	O	○ (3.7.5)	○ (下記に加えて、MA-4(2))	○ （下記に加えて、A.15.1.1)	-	-
			<Basic> ・組織は、遠隔保守の実施に当たっては、実施計画を策定し・合意した上で実施し、実施結果を確認する。 ・組織は、実施した遠隔保守の実施記録を保管する。	O		○ (MA-4)	○ (A.11.2.4, A.15.2.1)	○ (4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7,	-

添付C

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	L1_1_a_SYS, L2_1_b_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> ・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。	O/S	○ （下記に加えて、3.3.7）	○ （下記に加えて、AU-6(1), AU-11(1)）	○ （下記に加えて、A.12.4.4）	○ （下記に加えて、4.4.2.4）	○ （下記に加えて、SR 2.10）
			<Advanced> ・情報システム及び産業用制御システムは、監査ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。	O/S	○ （下記に加えて、3.3.4, 3.3.8, 3.3.9）	○ （下記に加えて、AU-9(3), AU-9(4)）	○ （下記に加えて、A.12.4.2）	○ （4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.3.3.3.9, 4.3.3.5.8）	○ （SR 2.8, SR 2.9, SR 2.11, SR 2.12）
			<Basic> ・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。 ・組織は、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。	O/S	○ （3.3.1, 3.3.2, 3.3.3）	○ （AU-2, AU-3, AU-6, AU-11）	○ （A.12.4.1, A.12.4.3, A.12.7.1）		
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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	L1_1_a_SYS, L1_1_b_SYS, L1_1_c_SYS, L2_1_b_COM, L2_3_b_SYS, L3_1_a_SYS, L3_3_d_SYS	<High-Advanced> ・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。	O/S	○ （下記に加えて、3.4.7, 3.4.8）	○ （下記に加えて、CM-7(2), CM-7(4)）	○ （A.8.2.2, A.8.3.1）	-	-
			<Advanced> ・組織は、システム、モノ等によって提供される機能とサービスをレビューし、削除の候補となる機能とサービスを特定する。 ・組織は、禁止されている機能、ポート、プロトコル、サービスの使用を検知し防止するために、ネットワークスキャンツール、侵入検知防止システム、エンドポイントプロテクション（ファイアウォール、ホストベースの侵入検知システム等）を活用する。 ・組織は、IoT機器やPC、サーバ以外の機器であっても、複合機等のネットワークにつながる機器に対しては、不要な機能やサービス等を停止する。	O	○ （下記に加えて、3.4.6）	○ （下記に加えて、CM-7）		○ （4.3.3.5, 4.3.3.7）	-
			<Basic> ・使用するUSBメモリ等の周辺機器は、管理台帳を作成し、保管場所を施錠して管理する。 ・IoT機器、サーバ等に接続するUSBメモリ等の外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能なUSBメモリを用いる等の対策を行う。 ・使用しないUSBポート、シリアルポートは栓をするなど物理的に閉塞する。	O	○ （3.8.1, 3.8.4）	○ （MP-2, MP-3, MP-4）			○ （SR 2.3, SR 7.7）
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	<High-Advanced> ・ハザードのエネルギー等を下げて事故が起きても影響を小さくするように設計する等、本質安全設計を通じて、影響度の高いハザードに対処することで、被害を極小化する。	O	-	-	○ （A.16.1.6）	-	-
			<Advanced> ・セーフティの側面を考慮したセキュリティリスクアセスメント(CPS.RA-4)を実施し、対象システムにおける物理的な安全に関する対策の要否及びそのレベルを把握する。 ・本質安全設計を通じてハザードの縮減を図る。当該プロセスを通じて、影響度の高いハザードが残存した場合、例えば、下記のような代替的対策を講ずることが望ましい。 - 安全装置等の付加装置による安全確保 - ハザードを有する機器に要員が近づかないような空間設計の実施 ・産業用制御システムは、サイバー攻撃等により通常の操作が維持できない場合、あらかじめ決められた出力をする。	O/S	-	-	-	-	○ （SR 3.6, SR 7.1, SR 7.2）
			<Basic> （該当なし）	-	-	-	-	-	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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情報の流れを特定し、管理するプロシージャを確立し、実施する。	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM L1_1_c_COM L1_3_b_ORG, L1_3_c_ORG, L2_1_b_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> ・組織は、ネットワーク構成、機器のソフトウェア構成等の情報を自動的に収集するメカニズムを利用し、常時最新の状況をモニタリングする。 ・情報システムは、システム内（及び相互接続システム間）のデータフローを制御するために、ユーザに対して（管理者によって）承認されたアクセス権限を強制的に適用する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・組織／システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い（通信）を検知できるようにする。	O/S	○ (下記に加えて、3.1.3, 3.14.1, 3.14.6, 3.14.7)	○ (下記に加えて、AC-4, CM-2(2), SI-4, SI-4(13))	-	-	-
			<Advanced> ・構成管理の一環として、組織が情報システム及び産業用制御システムの最新のベースラインとなる構成を把握し、文書化する。 ・情報システム及び産業用制御システムのベースライン構成に変更が生じる場合、速やかにベースライン構成を更新し、常に最新の状況を把握できるようにする。 ・組織は、一方のシステムから他方のシステムへの接続に関して、一方のシステムが他方のシステムのセキュリティ対策状況が十分なものだと判断した上で、接続を許可する。 ・産業用制御システムは、産業用制御システム以外のネットワークに接続せず、制御システムのネットワークにサービスを提供する。 ・組織は、情報システム内（及び相互接続システム間）のデータフローを制御するために、ユーザのアクセス権限に応じて任意アクセス制御を実施する。	O/S	-	○ (下記に加えて、CA-3)	-	○ (4.4.3.3)	-
			<Basic> ・組織は、情報システム及び産業用制御システムのネットワーク構成、資産、機器の設定情報、構成情報等のベースラインとなる情報を文書化し、内容が適切かどうかを定期的に確認する。 ・組織は、産業用制御システムにおいて、制御システムのネットワークを情報システムとのネットワークから論理的あるいは物理的にセグメント化することで、情報の流れを管理する。 [参考] 他のネットワークと物理的に離れた環境においては物理的なセグメント化を実施する、他のネットワークと物理的に近接した環境では、対策のコスト等も考慮して論理的なセグメント化を実施する等の対応が可能である。	O	○ (3.4.1)	○ (CM-2)	-		-
CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対応組織(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_3_a_ORG	<High-Advanced> ・組織は、セキュリティ専門の24時間365日モニタリングモニタリングにより収集した監査ログを、分析自動化ツール等を利用することで効率的に分析する。 ・組織は、従来のIT環境だけでなく、制御システムやIoT機器も含めて、セキュリティ状況のモニタリングの範囲とすることが望ましい。 ・組織は、セキュリティ対応組織の成熟度を定期的に評価し、セキュリティ状況のモニタリングやインシデントへの対応等のセキュリティ関連業務を継続的に改善することが望ましい。 [参考] セキュリティ対応組織(SOC/CSIRT)を評価するためのメトリクスには、「セキュリティ対応組織成熟度セルフチェックシート」(ISOG-J, 2018年)や、SIM3(Security Incident Management Maturity Model)等がある。	O/S	-	○ (上記に加えて、SI-4(2), SI-4(5))	○ (下記に加えて、A.12.4.1, A.16.1.5)	-	-
			<Advanced> ・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。なお、相関分析の対象には、他組織とデータを連携する部分のログも含めることが望ましい。 - モニタリングするシステムの範囲をどこまでとするか - どのような機器のログを収集し、分析するか (CPS.AE-3を参照) ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する（プロセスの内容については、CPS.RP-1等を参照）。 ・組織及びシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には以下を含むことが望ましい。 - ログ分析の分析結果（対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等） - モニタリングにおける今後の改善方針 [参考] セキュリティ対応組織(SOC/CSIRT)の業務、望まれる規模等については、「セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年)等を参照することが望ましい。	O/S	○ (3.6.1, 3.12.2, 3.14.6, 3.14.7)	○ (CA-7, IR-4, SI-4)		○ (4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8)	○ (SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2)
			<Basic> ・組織は、情報システム及び産業用制御システムの双方におけるセキュリティ管理責任者／担当者を明確化し、社内・社外向けのセキュリティ関係の窓口とする。	O	-	-	○ (A.6.1.1)	-	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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_1_b_SYS, L1_3_a_SYS	<High-Advanced> ・最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的なモニタリングに用いられている活動の修正の必要性を判断する。 ・組織は、自組織でIDS,IPS,SIEMといったセキュリティ装置等のポリシーチューニング（適用シグネチャ管理）と維持管理を行う。 ・組織は、自組織でセンサー機器でのカスタムシグネチャを脅威情報から作成する。 ・組織は、可能な場合、自組織に悪影響を及ぼす可能性の高いセキュリティ事象を適切に検知するため、<Advanced>で提示している機器のログに加え、IoT機器等のエッジデバイスのログも収集し、分析することが望ましい。	O	○ (下記に加えて、3.14.4)	○ (下記に加え、CA-7(3))	○ (A.12.4.1)	-	-
			<Advanced> ・組織は、自組織に悪影響を及ぼす可能性の高いセキュリティ事象を適切に検知するため、主に以下のような情報システムを構成する機器のログを監視し、リアルタイムに分析を行うことが望ましい。 多種多様なログの取り扱いが必要になるため、ログを正規化し、同一のデータベースに格納したり、SIEMを利用したりして、効率的な分析を実現する必要がある。取得可能な場合はネットフローの情報も扱うことが望ましい。 - ファイアウォールなどのネットワーク装置からのログやネットフロー - IPS/IDSなどのセキュリティ装置からのログ - Web サーバなどのアクセスログ - ActiveDirectoryやDNSなどの各種システムからのログ - ユーザ利用端末に関するログ [参考] セキュリティ対応組織(SOC/CSIRT)が実施する各種業務の内容については、「セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年) 等を参照することが望ましい。	S	○ (3.12.3)	○ (CA-7)		-	○ (SR 6.1)
			<Basic> ・ファイアウォールやエンドポイントセキュリティ製品等の通知を個別に確認することで、自組織に悪影響を及ぼすようなセキュリティ事象を特定する。	O				-	-
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する。	L1_3_b_PRO	<High-Advanced> ・組織は、発生したセキュリティ事象の形態，規模及び費用を定量化及び監視できるようにする自動的なメカニズムを備える。 ・組織は、セキュリティ事象発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を自組織のセキュリティ対応組織(SOC/CSIRT)にて実施する。 ・組織は、攻撃者のプロファイル（所属組織、組織の活動目的など）に関する仮説を構築する。 [参考] 複数のシステムが連携する"System of Systems"が構築されている環境においては、セキュリティインシデントの影響評価はより困難なものになることが想定される。当該領域における先行的な試みである「Internet of Things(IoT)インシデントの影響評価に関する考察」(一般社団法人日本クラウドセキュリティアライアンス, 2016年)では、デバイスの特性、サービスの特性、デバイス数により影響度を評価する試みがなされている。	O/S	-	-	○ (下記に加えて、A.16.1.6)	-	-
			<Advanced> ・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、共有することによって、当該セキュリティ事象の全容を把握する。 ・セキュリティ事象発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を外部のセキュリティベンダー等に依頼する。	O	○ (3.6.1)	○ (IR-4, IR-4(8))	○ (A.6.1.4)	-	-
			<Basic> （該当なし）	-	-	-	-	-	-
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_3_a_PRO	<High-Advanced> ・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 ※ CPS.AM-6, CPS.BE-2に同様の対策例を記載 ・組織は、セキュリティ事象の追跡と、事象に関係する脅威収集・脆弱性等の情報の収集及び分析を支援する自動化されたメカニズムを使用して、セキュリティ事象の分類（トリアージ）等に活用する。	O	-	○ (下記に加え、CP-2(8), IR-5(1))	○ (A.16.1.4)	○ (4.2.3.10)	-
			<Advanced> ・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位及びメトリクスを考慮してインシデントを分類する。	O	-	○ (下記に加え、CP-2)		-	-
			<Basic> ・当該セキュリティ事象のもたらす影響の大きさを考慮し、報告義務のあるインシデントを定める。 [参考] セキュリティ事象の影響の大きさを測るための尺度を検討する場合、下記文書等を参照することができる。 ・SP 800-61 Rev.1 (NIST, 2008年) 3.2.6 事件の優先順位付け ・「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準」(NISC, 2018年)	O	-	○ (IR-8)		-	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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・制御、アクセス監視・制御を実施する。	L1_1_a_SYS, L1_1_c_SYS, L1_3_a_SYS, L2_1_b_ORG, L2_3_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> ・情報システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする。 ・情報システム及び産業用制御システムは、モバイルコードの使用を管理し、監視する。 ・情報システムは、音声や映像の伝送に利用されるプロトコル（例：VoIP）の使用を管理し、監視する。	S	○ （下記に加えて、3.13.13, 3.13.14）	○ （下記に加えて、SC-7(8)）	-	-	-
			<Advanced> ・組織は、産業用制御システムと情報システムとの境界において通信をモニタリングし、制御する。 ・組織は、インターネットなどの外部ネットワークと社内ネットワークの中間に内部ネットワークへのアクセスを隔離されたネットワーク上のセグメント（DMZ: 非武装地帯）を構築する。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）を必ず経由させる。 ・組織は、個々の管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・組織は、特定の送信元、あるいは多数の送信元からの大量の通信がないかをシステムの外部境界及びシステム内の主要な内部境界にてモニタリングし、必要に応じて、特定IPアドレスからの通信を遮断するなど、適切な対応を実施する。	O/S	○ （下記に加えて、3.13.6）	○ （下記に加えて、SC-7(4), SC-7(5)）	-	-	○ （SR 6.2）
			<Basic> ・組織は、情報システムの外部境界において通信をモニタリングし、制御する。	O	○ （3.13.1, 3.13.5）	○ （SC-7）	-	-	
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及び記録、監視を実施する。	L1_1_a_SYS, L1_1_c_SYS, L2_3_b_PEO, L2_3_b_SYS, L2_3_d_SYS, L3_1_a_SYS	<High-Advanced> ・組織は、特に重要な資産を管理している範囲内での重要資産の位置や移動を追跡し、モニタリングする。	O	-	○ （下記に加えて、PE-20）	-	-	-
			<Advanced> ・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア（執務室等）において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。	O	○ （3.10.4, 3.10.5）	○ （PE-3, PE-6）	○ [A.11.1.1, A.11.1.2, A.11.1.3]	-	-
			<Basic> ・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来客に付き添うなどして人手による代替的な対策を実施する。 ・施設内の、一般の人がアクセスできない指定エリアに対するアクセスを制御するための、入退室管理対策を実施する。 ・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入退室時のログを保持する。	O				-	-
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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	L1_1_b_SYS, L2_2_a_COM, L3_3_a_DAT, L3_3_d_SYS	<High-Advanced> ・IoT機器あるいはそうした機器を含んだシステムが、通常期待される結果とは異なる結果をもたらすような特定の攻撃（例：コマンドインジェクション）に備え、ソフトウェアプログラムまたはアプリケーションからの出力情報を検証して、期待される内容と一致しているかを確認する。 ・情報システムは、IDS/IPSによる悪質コードの検知ロジックを自動的に更新する。 ・エンドポイント（特に、多様な機能を有するIoT機器、サーバ等）において、マルウェアに対する振舞い検知型の検出・修復ソフトウェアを導入することで、未知の脆弱性を突く攻撃コードの検知を実施する。 ・情報システムは、自組織外から受信したファイルのリアルタイムスキャンを実行する。	S	○ （下記に加えて、3.14.4, 3.14.5）	○ （下記に加えて、SI-10, SI-15）	○ （A.12.2.1）	-	○ （SR 3.2）
			<Advanced> ・情報システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・エンドポイント（IoT機器、サーバ等）において、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。 ・特に、機能が限定されているIoT機器において、ホワイトリスト型のマルウェア対策を実施することを考慮する。 ※ 特にIoT機器や制御機器においては、マルウェア対策ソフトが利用可能なOSが使用されているとは限らないケースがある。組織は、調達時等に導入する機器がマルウェア対策ソフトに対応できるものかを確認し、対応可能なものを選定することが望ましい。マルウェア対策ソフトに対応する機器を調達することが困難な場合、ネットワーク上でマルウェアを検知する仕組みを導入・強化する等、代替的な対策を実施することが望ましい。	S	○ （3.14.2, 3.14.3）	○ （SI-3）		-	
			<Basic> ・情報システム及び産業用制御システムは、インプットとなるデータが指定されたフォーマットや内容に適合しているかどうかを確認することで、有効性を検証する。	S	-	-	-	-	○ （SR 3.5）

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.CM-4	・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	L3_3_a_DAT, L3_3_d_SYS	<High-Advanced> ・組織は、データ入力に対する「ホワイトリスト」の概念を導入することで、インプットデータの出所を既知の信頼できるモノ、システム等と、そうしたインプットデータの許容できるフォーマットを指定する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。 ・情報システム及び産業用制御システムは、通信セッションの真正性を保護する。	S	○ （下記に加えて、3.14.5）	○ （下記に加えて、SI-10(5)）	○ (A.13.2.1, A13.2.3)	-	○ （SR 3.2）
			<Advanced> ・情報システムは、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、当該IoT機器が自組織の業務において重要なものと認められる場合、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。	S	○ (3.14.5)	○ （下記に加えて、SI-7）		-	
			<Basic> （該当なし）	-	-	-	-	-	-
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_a_SYS, L1_1_b_COM L1_1_c_COM L1_3_b_ORG, L1_3_c_ORG, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> ・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル及び他のサービスを明確にするよう要求する。 ・組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。	O/S	-	○ （下記に加えて、SA-9(2)）	○ （下記に加えて、A.13.1.2, A.15.2.2）	-	-
			<Advanced> ・組織は、外部サービスプロバイダ及びシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報，業務システム及び業務プロセスの重要性並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスををモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。	O/S	○ (3.14.6, 3.14.7)	○ （下記に加えて、PS-7, SI-4）		-	-
			<Basic> ・組織は、外部情報システムサービスのプロバイダ及びシステム開発の委託先に対して、自組織が対象となっている、あるいは当該プロバイダーが対象として該当するルールに従って、例えば、下記に関連するようなセキュリティ要求事項を設定し、導入することを要求する。 - （例えば、ISMS認証取得相当の）セキュリティ対策が十分に行われていること - 運用中のデータが適切に管理されること - サービス利用終了時にデータが適切に削除されること	O	-	○ (SA-9)	○ (A.14.2.7)	-	-
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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	L1_1_a_COM, L1_1_a_SYS, L1_1_b_COM L1_1_c_COM L1_3_a_SYS, L1_3_b_ORG, L1_3_c_ORG, L2_1_a_ORG, L2_1_c_ORG, L2_1_c_SYS, L2_3_b_ORG, L2_3_b_SYS, L2_3_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> ・組織は、システム内に許可されてないハードウェア、ソフトウェア、ファームウェアが存在する場合に、それを自動で検知するメカニズムを使用する。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・情報システム及び産業用制御システムは、許可されていないコンポーネントのネットワークアクセスが検知された場合に、そうしたコンポーネントによるネットワークアクセスを無効にする、それらのコンポーネントをネットワークから切り離す等の一次対処を実施し、システム管理者に通知する。 ・組織は、情報システムのベースライン構成のロールバックを可能にするために、旧バージョンのベースライン構成（例えば、ハードウェア・ソフトウェア・ファームウェア・構成ファイル・構成記録）を記録する。 ・制御機器やIoT機器において、ファームウェア等のロールバック機能が備わっていない場合、予備の制御機器やIoT機器を備えておくことが望ましい。 ・IoT機器には、既存の資産管理システムと必ずしも接続できないものも存在することが想定されるため、組織が管理できる範囲で複数の資産管理システムを運用することも視野に入れて資産管理・構成管理を実施する。 ※ 関連する対策要件に、CPS.AM-1がある。	O/S	-	○ （下記に加えて、CM-8(3)）		-	-
			<Advanced> ・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）を必ず経由させる。 ・個々の管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・情報システム及び産業用制御システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。	O/S	○ （下記に加えて、3.4.1, 3.4.3, 3.13.9, 3.14.6, 3.14.7）	○ (下記に加えて、CM-3, CM-8(1), SC-7(4), SC-7(5), SI-4)		-	-
			<Basic> ・IoT機器、サーバ等を含む資産の型番やソフトウェアのバージョン、サポート期限等を管理する台帳を作成し、定期的に棚卸する。 ・組織は、運用時に実施すべき対策（IoTデバイスの不正利用や盗難、パッチの適用、ログのチェック等）、IoT機器の状況を定期的に確認する。	O	○ (3.4.1)	○ (CM-8)		-	-

添付C

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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, L2_1_c_SYS, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> ・組織は、自組織が管理する産業用制御システムの構成要素（IoT機器を含む）に対して、計画停止時等に脆弱性診断を実施し、自組織の所有するシステムに存在する脆弱性を認識し、一覧化する。 ・組織は、ツールを用いて脆弱性診断を行う場合、診断すべきシステムの脆弱性データベースをすぐに更新できる脆弱性診断ツールを使用することが望ましい。 ・組織は、スキャンされたシステムの脆弱性を定期的に、あるいは新たな脆弱性が特定され、報告された場合に更新する。 ・組織は、指定された脆弱性スキャン活動に関して、対象システムのコンポーネントに対する特権的アクセスの許可制度を実施する。	O	○ (下記に加えて、 3.11.2)	○ (下記に加えて、 RA-5(1), RA-5(2), RA-5(5))	○ (A.12.6.1)	○ (下記に加えて, 4.2.3.7)	-
			<Advanced> ・組織は、情報システム及びアプリケーションの脆弱性のスキャンを定期的に、あるいは、それらのシステム／アプリケーションに影響を及ぼす新たな脆弱性が確認され、報告された場合に実施する。 ・組織は、脆弱性スキャンにツールを用いる。以下を満たす標準的な手法を使用することによって、脆弱性管理プロセスの一部を自動化できることが求められる。 - プラットフォーム、ソフトウェアの欠陥及び誤った設定を列挙する - チェックリストとテスト手順をフォーマットする - 脆弱性による影響を評価する ・組織は、リスクアセスメントを通じて、特定された脆弱性を適切な期間中に修正する。 ・上記のプロセスから得た情報を組織内の他のシステムの管理者と共有することによって、他の情報システム内の同様の脆弱性を把握し、必要に応じて修正する。 [参考] 脆弱性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の影響の大きさを評価する指標として、CVSS(IPAによる解説：https://www.ipa.go.jp/security/vuln/CVSS.html)を参考とすることが可能である。	O	○ (3.11.2, 3.11.3)	○ (RA-5)			-
			<Basic> ・組織は、情報システム及びアプリケーションの脆弱性のスキャンを定期的に実施する。	O				○ (4.2.3.1)	-
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共・ピアプロパティが担う役割と各ラ	L1_3_a_ORG	<High-Advanced><Advanced><Basic>共通 ・組織は、リスクマネジメントに係る戦略やアセスメントの結果等から、セキュリティインシデントを検知するために収集することが望ましいログ情報を決定する。	O	○ (3.12.3)	○ (CA-7, PM-14)	○ (A.6.1.1, A.12.4.1)	○ (4.4.3.1)	-
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_a_ORG	<High-Advanced><Advanced><Basic>共通 ・組織は、モニタリング業務に関係する法制度、業界標準、顧客との契約事項等が存在するか、存在するならばどのような制約があるかを認識する。 ・組織は、上記で認識したルールに準拠してモニタリングを実施し、セキュリティ事象を検知する。 ・組織は、自組織のモニタリング活動がルールに準拠したものかどうかを定期的にレビューし、確認する。	O	○ (3.12.3)	○ (CA-7, PM-14)	○ (A.18.2.2)	○ (4.4.3.2)	-
CPS.DP-3	・監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。	L1_3_a_ORG	<High-Advanced> ・最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的なモニタリングに用いられている活動の修正の必要性を判断する。 ・システムに、既知で害のないテストケースを導入して、マルウェア検知メカニズムをテストする。 ・組織は、侵入検知モニタリングに用いているメカニズムを定期的にテストする。テストの頻度は、組織が使用するツールの種類と、ツールの設置方法により変わる。	O/S	-	○ (下記に加えて、 CA-7(3), SI-3(6), SI-4(9))	○ (下記に加えて、 A.14.3.1)	-	-
			<Advanced> ・組織は、自組織のシステムのモニタリング活動が、組織のリスクマネジメント戦略と、リスク対応のためのアクションの優先順位に適合しているかどうかを定期的に確認するプロシージャを定め、運用する。 ・ネットワーク機器やエンドポイントからのセキュリティに係る情報の相関分析を行うのに合わせて、誤検出や検出漏れの割合を算出し。定期的に検知メカニズムの妥当性を確認する。	O	-	○ (CA-7, PM-14)	○ (A.14.2.8)	○ (4.4.3.2)	○ (SR 3.3)
			<Basic> （該当なし）	-	-	-	-	-	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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_1_b_SYS, L1_3_a_ORG	<High-Advanced> ・組織は、検知能力向上のため、様々な情報ソースをもとに、検知ルールの作成とチューニングを行う - 相関分析ルールの開発 - IPS/IDSの独自シグネチャの開発 - 独自ブラックリストの開発 ・組織／システムは、システムの通信やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、誤検出の数や、検出漏れの数を減らすためのチューニングを行う。	O/S	-	○ （下記に加えて、SI-4(13)）	○ (A.16.1.6)	-	-
			<Advanced> ・組織は、経営層等の組織内の然るべき要員に、定期的に組織及びシステムのセキュリティの状態を報告するプロシージャを整備し、運用する。組織は、報告の場を最新の脅威や残存するリスクに対する脅威を認識し、セキュリティを向上するための場とすることが望ましい。 ・例えば、以下のような注意喚起情報の発信があった際等に、セキュリティに係るリスク増加の兆候がある場合、信頼できる情報源からの情報に基づいて、システムのモニタリング活動のレベルを上げる。　※以下のリストは、「セキュリティ対応組織 (SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0」(ISOG-J, 2017年)より引用している。 ・ 攻撃の特徴 攻撃の特徴 ➢ 攻撃形態、関連する通信の内容 ➢ 核心となる攻撃コード ・ 攻撃によって残る痕跡 ➢ 被害を受けた後の通信内容 ➢ サーバやクライアントに残るログ ➢ サーバやクライアントに残るその他特徴 ・ 各セキュリティ製品における検知名	O	○ (3.14.6, 3.14.7)	○ (CA-7, SI-4)		○ (4.4.3.4)	-
			<Basic> （該当なし）	-	-	-	-	-	-
CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	L1_1_a_SYS, L1_3_a_PEO, L1_3_a_PRO, L2_1_a_PRO, L2_1_b_PRO, L2_1_c_PRO, L2_2_a_PRO, L3_1_a_SYS, L3_3_a_SYS, L3_3_d_SYS	<High-Advanced> ・情報システム及び産業用制御システムは、有効でないインプットデータを受け取った場合に、組織の目的とシステムの目的に沿って、予想できる形で、かつ記載どおりに動作する。	S	-	（下記に加えて、SI-10(3), SI-17)	○ (A.16.1.5)	-	-
			<Advanced> ・組織は、セキュリティ運用マニュアルにおいてインシデントの検知及び分析、封じ込め、低減、復旧を含む内容を規定する。 - すべてのインシデントの取り扱いに関する記録をとる - 外部組織等に対して、インシデント発生の事実と対応状況に関する報告をする必要があるかどうかを判断する	O	-	○ （下記に加えて、IR-8）		○ (4.3.4.5.1)	-
			<Basic> ・組織は、セキュリティインシデントの発生時に利用するセキュリティ運用プロセスを策定し、運用する。当該プロセスには、下記を例とする内容を含むことが望ましい。 - インシデントの報告を受けた者が、どのような対応をするのか、あるいはより上位に報告するのかの判断基準 - 緊急時の指揮命令と対応の優先順位の決定 - インシデントへの対応（インシデントレスポンス） - インシデントの影響と被害の分析 - 情報収集と自社に必要な情報の選別 - 社内関係者への連絡と周知 - 外部関係機関との連絡 ・システム（特に産業用制御システム）は、IoT機器、サーバ等に異常（誤動作等）が発生した場合に、緊急停止、管理者へのアラート通知等のフェールセーフのための対応を実施する。 [参考] セキュリティインシデント発生時の対応手順の検討において、「インシデントハンドリングマニュアル」(JPCERT/CC, 2015年)、SP 800-61 Rev.1 (NIST, 2008年)、「インシデント対応マニュアルの作成について」(JPCERT/CC, 2015年)を参照することが可能である。	O/S	○ (3.6.1)	○ (IR-4)			-
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_b_PEO, L1_3_b_PRO, L1_3_c_PEO, L1_3_c_PRO	<High-Advanced> ・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、インシデント対応要件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。 [参考] サプライチェーンにおけるセキュリティインシデントには、たとえば、システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害等がある。	O	-	○ （下記に加えて、CP-2(7), IR-4(4), IR-4(10)）	○ （下記に加えて、A.17.1.2）	-	-
			<Advanced> ・組織は、セキュリティインシデントにより第1の処理拠点の可用性が低下した場合に利用する代替処理拠点を定める。 ・組織は、自組織の一次処理機能が利用できない場合に、自組織が定める目標復旧時間内に、代替処理拠点により所定のオペレーションを移転・再開して、重要なミッション／業務機能を遂行できるようにするようサービス契約で規定する。 ・組織は、同じ脅威に対する脆弱さを減らすために、一次処理拠点から離れた代替処理拠点を指定する。 ・組織は、情報システム及び産業用制御システムのユーザにセキュリティインシデントの対応と報告に関する助言と支援を提供する、組織のインシデント対応能力に不可欠な、インシデント対応支援リソース（ヘルプデスク、CSIRT等）を自組織に用意する。	O	-	○ （下記に加えて、CP-7, CP-7(1), CP-7(2), CP-7(3), IR-7)		○ (4.3.2.5.2, 4.3.2.5.3, 4.3.4.5.1, 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.5)	-
			<Basic> ・セキュリティインシデントを発見した場合、速やかにIPA、JPCERT/CC等の関係機関に報告し、対応の支援、発生状況の把握、手口の分析、再発防止のための助言等を受ける。	O	-	○ (IR-6)	○ (A.16.1.1, A.16.1.2)	-	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.RP-3	・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。	L1_3_a_PRO, L1_3_a_DAT	<High-Advanced><Advanced>共通 ・組織は、情報システム、産業用制御システム及び関係するプロセスの管理者を含めて、有事における事業継続のための体制を構築する。事業継続に支障をもたらす事象が発生した際には、この体制が、運用を再確立するためのシステムの優先順位を決定する。 ・組織は、災害等と比較して被害状況が見えづらく事業継続計画の発動タイミングが不明確、インシデントの原因究明の重要性が高い等の特徴を有するセキュリティインシデントに特化した事業継続計画又は緊急事対応計画を策定し、運用する。 ・組織は、セキュリティインシデントに特化した事業継続計画又は緊急事対応計画を策定する際、組織全体の事業継続に係る方針と合致するような内容とすることを確実にする。	O	-	○ (CP-2)	○ (A.17.1.1)	○ (4.3.2.5.4)	-
			<Basic> （該当なし）	-	-	-	-	-	-
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_b_COM	<High-Advanced><Advanced>共通 ・組織は、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。 ・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動及びインシデントの事後処理に関わる活動を調整する。その際、CPS.AM-2, CPS.AM-3にて記載している方法により、対応の対象となるモノを特定していることが望ましい。 ※ CPS.CO-3と関連	O	○ (3.6.2)	○ (下記に加えて、 IR-4, IR-4(10))	○ (A.17.1.1)	-	-
			<Basic> ・自組織の業種等を考慮して、事業継続計画又は緊急事対応計画の中に、インシデント発生後の生産したモノへの対応について記載するかを検討する。その際、事業継続計画又は緊急事対応計画は、必ずしもセキュリティインシデントを想定したものでない場合も許容されるものとする。	O	-	○ (CP-2)		-	-
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_3_a_PRO	<High-Advanced><Advanced><Basic>共通 ・組織は、下記の内容を含む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。 - 公表する内容 - 情報公表の実施時期 - 情報公表の実施者 - 情報公表までの実施プロセス	O	-	-	○ (Clause 7.4)	○ (4.3.4.5.9)	-
CPS.CO-2	・事業継続計画又は緊急事対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。	L1_3_a_PRO	<High-Advanced><Advanced><Basic>共通 ・マスコミや取引先に対する情報のやり取りの窓口を一本化し、対応方針が一貫したものとなるようにする。 ・セキュリティインシデントによる被害に関する重要な情報について、情報の機密性に配慮しつつ丁寧に説明する。	O	-	-	-	-	-
CPS.CO-3	・復旧活動について内部及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、事業継続計画又は緊急事対応計画の中に位置づける。	L1_3_a_PRO	<High-Advanced><Advanced>共通 ・組織は、監督官庁、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。 ・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動及びインシデントの事後処理に関わる活動を調整する。ここで該当する活動の例として、生産システムにおけるセキュリティインシデント発生時に生産されたモノの回収等が挙げられる。	O	○ (3.6.1)	○ (下記に加えて、 IR-4, IR-4(10))	○ (A.17.1.2)	-	-
			<Basic> ・組織は、自組織に影響を及ぼすようなセキュリティインシデント発生時における役割、責任、そうした役割と責任を割り当てられたヒトと連絡先情報を示す。 ・組織は、事業継続に関わる意思決定の責任が割り当てられたヒトに対して、意思決定をより適切なものとするため、セキュリティインシデントの概要や被害状況に関する説明を実施する。	O	-	○ (CP-2)		○ (4.3.2.5.5, 4.3.4.5.9)	-
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、自組織及び関係する他組織を含む社会全体への影響を把握する。	L1_3_a_COM, L1_3_a_PRO	<High-Advanced> ・情報システムは、発生したセキュリティインシデントの形態，規模及び費用を定量化及び監視できるようにする自動的なメカニズムを備える。 ・組織は、セキュリティインシデント発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を自組織のセキュリティ対応組織(SOC/CSIRT)にて実施する。 ・組織は、攻撃者のプロファイル（所属組織、組織の活動目的など）に関する仮説を構築する。 [参考] 複数のシステムが連携する"System of Systems"が構築されている環境においては、セキュリティインシデントの影響評価はより困難なものになることが想定される。当該領域における先行的な試みである「Internet of Things(IoT)-インシデントの影響評価に関する考察」(一般社団法人日本クラウドセキュリティアライアンス, 2016年)では、デバイスの特性、サービスの特性、デバイス数により影響度を評価する試みがなされている。	O/S	-	-	○ (下記に加えて、 A.16.1.6)	-	-
			<Advanced> ・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、共有することによって、当該セキュリティインシデントの全容を把握する。 ・セキュリティインシデント発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を外部のセキュリティベンダー等に依頼する。	O	○ (3.6.1)	○ (IR-4, IR-4(8))	○ (A.6.1.4)	○ (4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8)	-
			<Basic> （該当なし）	-	-	-	-	-	-

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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_3_a_PRO	<High-Advanced> ・情報システムが、重要なセキュリティインシデントに関する監査記録について処理するプロシージャを提供する。	S	○ (3.3.6)	○ (AU-7, AU-7(1))	○ (A.16.1.7)	-	○ (下記に加えて、SR 2.10)
			<Advanced> ・組織は、媒体、装置及び装置の状態（例えば、電源が入っているか、切れているか）に従って、証拠の特定、収集、取得及び保存のプロシージャを規定する。 ・組織は、重要なセキュリティインシデントについて、発生後に下記の証跡を保全することが望ましい。 - 識別情報（インシデントの発生場所／発生日時／対象となるモノのシリアル番号／ホスト名／MACアドレス／IPアドレス等） - 証跡を収集・処理したヒトの役職、名前、連絡先 - 証跡保全処理の日時（タイムゾーンを含む）	O				-	○ (SR 2.8, SR 2.9, SR 2.11, SR 2.12, SR 3.9, SR 6.1)
			<Basic> ・組織は，証拠となり得るデータを特定、収集、取得及び保存するためのプロシージャを定め、運用する。	O				-	-
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_3_a_PRO	<High-Advanced> ・組織は、セキュリティ事象の追跡と、事象に関係する脅威収集・脆弱性等の情報の収集及び分析を支援する自動化されたメカニズムを使用して、セキュリティインシデントの分類（トリアージ）等に活用する。	O	-	○ (下記に加えて、CP-2(8), IR-5(1))	○ (A.16.1.3, A.16.1.4)	-	-
			<Advanced> ・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位及びメトリクスを考慮してインシデントを分類する。 ・組織は、自組織に影響を及ぼすセキュリティインシデントを追跡し、文書化する。「SP 800-61 Rev.1」では、セキュリティインシデントを文書化する際の記載の観点として、下記を例示している。 - インシデントの現在の状況 - インシデントの概要 - 当該インシデントに対して自組織のとった行動の内容 - ほかの関係者(システム所有者、システム管理者等)の連絡先情報 - 調査の際に収集した証拠の一覧 - インシデントの処理担当者からのコメント - 次にとるべきステップ	O	○ (3.6.1)	○ (下記に加えて、CP-2, IR-5)		○ (4.3.4.5.6)	-
			<Basic> ・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 ※ CPS.AM-6, CPS.BE-2に同様の対策例を記載 ・当該セキュリティ事象のもたらす影響の大きさを考慮し、報告義務のあるインシデントを定める。 [参考] セキュリティインシデントの影響の大きさを測るための尺度を検討する場合、下記文書等を参照することができる。 ・SP 800-61 Rev.1 (NIST, 2008年) 3.2.6 事件の優先順位付け ・「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準」(NISC, 2018年)	O	-	○ (IR-8)			-
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_3_a_PRO	<High-Advanced> ・組織は、セキュリティインシデントの対応プロセスを支援する自動化されたメカニズムを使用する。 ・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。 [参考] 対応段階におけるインシデントの影響低減、復旧段階において有用に機能すると考えられる情報の例として、「セキュリティ対応組織(SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0 」(ISOG-J, 2017年)では、下記が挙げられる。 ・攻撃行為をセキュリティ製品や関連するシステムで遮断するための設定要件 ・攻撃を無効化する方法（パッチの適用、設定変更等） ・被害を受けたシステム復旧方法	O/S	-	○ (下記に加え、IR-4(1), IR-4(4))	○ (A.16.1.5)	-	-
			<Advanced><Basic>共通 ・組織（あるいはその構成員）は、あらかじめ定められたプロシージャに従って、セキュリティインシデントを低減するためのアクション（例えば、システムのシャットダウン、有線/無線ネットワークからの切断、モデムケーブルの切断、特定の機能の無効化など）を実行する。 [参考]セキュリティインシデントの影響低減のための活動は、インシデントの性質（例えば、サービス拒否攻撃、マルウェア感染、不正アクセスのような顕在化する脅威の差異）により内容が異なる場合がある。より詳細な影響低減活動の情報については、「インシデントハンドリングマニュアル」(JPCERT/CC, 2015年)、SP 800-61 Rev.1 (NIST, 2008年)等を参照することが望ましい。	O	○ (3.6.1)	○ (IR-4)		○ (4.3.4.5.6, 4.3.4.5.10)	○ (SR 5.1, SR 5.2, SR 5.4)

添付C

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
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_3_a_ORG	<High-Advanced> ・情報システムが、発生したセキュリティインシデントの形態，規模及び費用を定量化及び監視できるようにする自動的なメカニズムを備えることが望ましい。	S	-	-	○ (A.16.1.6)	–	–
			<Advanced><Basic>共通 ・セキュリティインシデントの評価から得た脅威情報、脆弱性情報等は、再発する又は影響の大きいインシデントを特定するために利用することが望ましい。 ・セキュリティインシデントへの対応活動から学んだ教訓を事業継続計画又は緊急事対応計画、教育／訓練に取り入れて、結果として必要となる変更を実施する。NIST SP 800-61には、教訓を抽出する際の観点として下記が例として示されている。 - 正確に何がいつ起きたか。 - スタッフとマネジメント層がどの程度うまく事件に対処したか。文書化された手順に従ったか。それは適切だったか。 - すぐに必要になった情報は何か。 - 復旧を妨げたかもしれないステップや行動があったか。 - 次に同様の事件が起きた場合、スタッフやマネジメント層は、どのような違った行動をとるか。 - どのような是正措置があれば、将来にわたって同じ様な事件が起きるのを防げるか。 - 将来事件を検出、分析、軽減するために、どのようなツールやリソースが追加で必要となるか。	O	○ (3.6.2)	○ (IR-4)		○ (4.3.4.5.10)	–
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、事業継続計画又は緊急事対応計画を継続的に改善する。	L1_3_a_ORG	<High-Advanced><Advanced><Basic>共通 ・組織は、セキュリティインシデントへの対応から、事業継続のためのプロシージャ及び関連する対策の機能が、事業継続のより上位の方針と合致しているかを確認する。 ・セキュリティインシデントへの対応活動から学んだ教訓を事業継続計画又は緊急事対応計画、教育／訓練に取り入れて、結果として必要となる変更を実施する。	O	○ (3.6.2)	○ (IR-4)	○ (A.17.1.3)	-	-

添付D　海外の主要規格との対応関係

D．1　NIST Cybersecurity Framework のサブカテゴリと「サイバー・フィジカル・セキュリティ対策フレームワーク」との対応表

NIST Cyberseucurity Framework Ver. 1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
特定（ID）	AM-1	自組織内の物理デバイスとシステムが、目録作成されている。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。
	AM-2	自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。		
	AM-3	組織内の通信とデータフロー図が、作成されている。	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、適切に管理する。
	AM-4	外部情報システムが、カタログ作成されている。	CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。
	AM-5	リソース（例：ハードウェア、デバイス、データ、時間、人員、ソフトウェア）が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。	CPS.AM-6	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。
	AM-6	全労働力と利害にある第三者（例：サプライヤー、顧客、パートナー）に対してのサイバーセキュリティ上の役割と責任が、定められている。	CPS.AM-7	・自組織及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。
	BE-1	サプライチェーンにおける自組織の役割が、識別され、周知されている。	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。
	BE-2	重要インフラとその産業分野における自組織の位置付けが、識別され、周知されている。		
	BE-3	組織のミッション、目標、活動の優先順位が、定められ、周知されている。	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、自組織の取引に関係する者（サプライヤー、第三者プロバイダ等を含む）に共有する。
	BE-4	重要サービスを提供する上での依存関係と重要な機能が、定められている。	CPS.BE-3	・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。
	BE-5	重要サービスの提供を支援するレジリエンスに関する要求事項が、すべてのオペレーション状況（例：脅迫・攻撃下、復旧時、通常時等）について定められている。	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、教育を実施し、その記録を管理する。
			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得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。
			CPS.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。
			CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。
			CPS.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。
			CPS.RP-3	・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。
	GV-1	自組織のサイバーセキュリティポリシーが、定められ、周知されている。	CPS.GV-1	・セキュリティポリシーを策定し、自組織及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。
	GV-2	サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。		
	GV-3	プライバシーや人権に関する義務を含む、サイバーセキュリティに関する法規制上の要求事項が、理解され、管理されている。	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する。
	GV-4	ガバナンスとリスクマネジメントプロセスがサイバーセキュリティリスクに対応している。	CPS.GV-4	・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。
	RA-1	資産の脆弱性が識別され、文書化されている。	CPS.RA-1	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。
	RA-2	サイバー脅威に関する情報が、複数の情報共有フォーラムおよび複数のソースから入手されている。	CPS.RA-2	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。
	RA-3	内部および外部からの脅威が、識別され、文書化されている。	CPS.RA-3	・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。

NIST Cyberseucurity Framework Ver. 1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
	RA-4	ビジネスに対する潜在的な影響とその発生可能が、識別されている。	CPS.RA-4	・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。
	RA-5	脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。	CPS.RA-5	・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。
	RA-6	リスク対応が、識別され、優先順位付けされている。	CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。
	RM-1	リスクマネジメントプロセスが、組織の利害関係者によって定められ、管理され、承認されている。	CPS.RM-1	・自組織内における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し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスク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。
	RM-2	組織のリスク許容度が、決定され、明確に表現されている。	CPS.RM-2	・リスクアセスメント結果及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。
	RM-3	自組織によるリスク許容度の決定が、重要インフラにおける組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。		
	SC-1	サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別され、管理され、合意されている。	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、その内容について取引先と合意する。
	SC-2	情報システム、コンポーネント、サービスのサプライヤーと第三者であるパートナーが、識別され、優先順位付けられ、サイバーサプライチェーンのリスクアセスメントプロセスにより評価されている。	CPS.SC-2	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。
	SC-3	サプライヤーおよび第三者であるパートナーとの契約が、組織のサイバーセキュリティプログラムやサイバーサプライチェーンのリスクマネジメント計画の目的を達成するための適切な対策の実施に活用されている。	CPS.SC-3	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織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。
	SC-4	サプライヤおよび第三者であるパートナーが、監査、テストの結果、またはその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている。	CPS.SC-6	・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。
	SC-5	対応・復旧計画の策定とテストが、サプライヤーおよび第三者プロバイダと共に行われている。	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、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。
防御（PR）	AC-1	認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。
	AC-2	資産に対する物理アクセスが、管理され、保護されている。	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。
	AC-3	リモートアクセスが、管理されている。	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。
			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。
	AC-4	アクセスの許可および認可が、最小権限の原則および役割の分離の原則を組み入れて、管理されている。	CPS.AC-5	・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。
			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、想定されるリスクも考慮して、信頼性の高い認証方式（例：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。
	AC-5	ネットワークの完全性が、保護されている（例：ネットワークの分離、ネットワークのセグメント化）。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って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。

NIST Cyberseucurity Framework Ver. 1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
	AC-6	IDは、ID利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで活用されている。	CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。
	AC-7	ユーザ、デバイス、その他の資産は、トランザクションのリスク（例：個人のセキュリティ及びプライバシーのリスク、その他組織上のリスク）の度合いに応じた認証（例えば、一要素、多要素）が行われている。	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、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。
			CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。
	AT-1	すべてのユーザは、情報が周知され、トレーニングが実施されている。	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、教育を実施し、その記録を管理する。
	AT-2	権限を持つユーザが、自身の役割と責任を理解している。		
	AT-3	第三者である利害関係者（例：サプライヤー、顧客、パートナー）が、自身の役割と責任を理解している。	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得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。
	AT-4	上級役員（セキュリティ担当役員）が、自身の役割と責任を理解している。	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、教育を実施し、その記録を管理する。
	AT-5	物理セキュリティおよびサイバーセキュリティの担当者が、自身の役割と責任を理解している。		
	DS-1	保存されているデータが、保護されている。	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。
	DS-2	伝送中のデータが、保護されている。	CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。
			CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。
	DS-3	資産は、撤去、譲渡、廃棄に至るまで、正式に管理されている。	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。
	DS-4	可用性を確保するのに十分な容量が、維持されている。	CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する。
			CPS.DS-7	・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。
	DS-5	データ漏えいに対する防御対策が、実装されている。	CPS.DS-8	・保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。
			CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。
	DS-6	完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されている。	CPS.DS-10	・IoT機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。
			CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する。
	DS-7	開発・テスト環境が、実稼働環境から分離されている。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って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。
	DS-8	完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている。	CPS.DS-12	・ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。
	IP-1	情報技術／産業用制御システムのベースラインとなる構成は、セキュリティの原則（例：最低限の機能性の概念）を組み入れて、を定められ、維持されている。	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。
			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。
	IP-2	システムを管理するためのシステム開発ライフサイクルが、実装されている。	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する。
	IP-3	構成変更管理プロセスは、策定されている。	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。
	IP-4	情報のバックアップが、実施され、維持され、テストされている。	CPS.IP-4	・構成要素（IoT機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする。
	IP-5	組織の資産の物理的な運用環境に関するポリシーと規制が、満たされている。	CPS.IP-5	・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。

NIST Cyberseucurity Framework Ver. 1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
	IP-6	データは、ポリシーに従って破壊されている。	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。
	IP-7	防御プロセスは、改善されている。	CPS.IP-7	・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。
	IP-8	防御技術の有効性に関する情報が、共有されている。	CPS.IP-8	・保護技術の有効性について、適切なパートナーとの間で情報を共有する。
	IP-9	（インシデント対応及び事業継続）対応計画と（インシデントからの復旧及び災害復旧）復旧計画が、策定され、管理されている。	CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。
			CPS.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。
	IP-10	対応計画と復旧計画が、テストされている。	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得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。
	IP-11	サイバーセキュリティには、人事に関わるプラクティス（例：アクセス権限の無効化、人員のスクリーニング）が含まれている。	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）を含める。
	IP-12	脆弱性管理計画が、作成され、実装されている。	CPS.IP-10	・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。
	MA-1	組織の資産の保守と修理は、承認・管理されたツールを用いて実施され、ログが記録されている。	CPS.MA-1	・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 ・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。
	MA-2	組織の資産に対する遠隔保守は、承認を得て、ログが記録され、不正アクセスを防止した形式で実施されている。	CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。
	PT-1	監査記録／ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。
	PT-2	リムーバルメディアは、保護され、その使用がポリシーに従って制限されている。	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。
	PT-3	最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。		
	PT-4	通信（情報）ネットワークと制御ネットワークが、保護されている。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って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。
	PT-5	メカニズム（例：フェイルセーフ、負荷分散、ホットスワップ）が、平時及び緊急時においてレジリエンスに関する要件を達成するために実装されている。	CPS.PT-3	・ネットワークにつながることを踏まえた安全性を実装するIoT機器を導入する。
検知（DE）	AE-1	ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが定められ、管理されている。	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情報の流れを特定し、管理するプロシージャを確立し、実施する。
	AE-2	検知したイベントは、攻撃の標的と手法を理解するために分析されている。	CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対応組織(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。
	AE-3	イベントデータは、複数の情報源やセンサーから収集され、相互分析されている。	CPS.AE-3	・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。
	AE-4	イベントがもたらす影響が、判断されている。	CPS.AE-4	・関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。
	AE-5	インシデント警告の閾値が、定められている。	CPS.AE-5	・セキュリティ事象の危険度の判定基準を定める。
	CM-1	ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	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・制御、アクセス監視・制御を実施する。

NIST Cyberseucurity Framework Ver. 1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
	CM-2	物理環境は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。
	CM-3	人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。
	CM-4	悪質なコードは、検出されている。	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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。
			CPS.CM-4	・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。
	CM-5	不正なモバイルコードは、検出されている。	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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。
			CPS.CM-4	・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。
	CM-6	外部サービスプロバイダの活動は、潜在的なサイバーセキュリティイベントを検知できるようにモニタリングされている。	CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。
	CM-7	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが、実施されている。	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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。
	CM-8	脆弱性スキャンが、実施されている。	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。
	DP-1	検知に関する役割と責任は、説明責任を果たせるように明確に定義されている。	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。
	DP-2	検知活動は必要なすべての要求事項を満たしている。	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。
	DP-3	検知プロセスが、テストされている。	CPS.DP-3	・監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。
	DP-4	イベント検知情報が、周知されている。	CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。
	DP-5	検知プロセスが、継続的に改善されている。	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。
対応（RS）	RP-1	対応計画が、インシデントの発生中または発生後に実行されている。	CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。
	CO-1	人員は、対応が必要になった時の自身の役割と行動の順序を認識している。	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得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。
	CO-2	インシデントが、定められた基準に沿って報告されている。	CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。
	CO-3	対応計画に従って、情報が共有されている。		
	CO-4	利害関係者との間で調整が、対応計画に従って行われている。	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。
	CO-5	サイバーセキュリティに関する状況認識を広げるために、外部利害関係者との間で自発的な情報共有が行われている。		
	AN-1	検知システムからの通知は、調査されている。	CPS.AE-3	・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。
	AN-2	インシデントがもたらす影響は、把握されている。	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、自組織及び関係する他組織を含む社会全体への影響を把握する。
	AN-3	フォレンジックが、実施されている。	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。

NIST Cyberseucurity Framework Ver. 1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
	AN-4	インシデントは、対応計画に従って分類されている。	CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。
	AN-5	プロセスは、内外のソース（例：内部テスト、セキュリティ情報、セキュリティ研究者）から報告された脆弱性情報を、自組織が受け取り、分析し、対応するために定められている。	CPS.RA-2	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。
	IM-1	対応計画は、学んだ教訓を取り入れられている。	CPS.IM-1	・セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する。
	IM-2	対応戦略は、更新されている。		
	MI-1	インシデントは、封じ込められている。	CPS.MI-1	・セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う。
	MI-2	インシデントは、緩和されている。		
	MI-3	新たに特定された脆弱性は、許容できるリスクである場合にはその旨を文書化され、そうでない場合にはリスクが緩和されている。	CPS.RA-4	・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。
			CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。
復旧（RC）	RP-1	復旧計画が、サイバーセキュリティインシデントの発生中または発生後に実施されている。	CPS.RP-3	・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。
	IM-1	復旧計画は、学んだ教訓を取り入れている。	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、事業継続計画又は緊急事対応計画を継続的に改善する。
	IM-2	復旧戦略は、更新されている。		
	CO-1	広報活動が、管理されている。	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。
	CO-2	評判は、インシデント発生後に回復されている。	CPS.CO-2	・事業継続計画又は緊急事対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。
	CO-3	復旧活動は、内外の利害関係者だけでなく役員と経営陣にも周知されている。	CPS.CO-3	・復旧活動について内部及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、事業継続計画又は緊急事対応計画の中に位置づける。

D. 2　NIST SP 800-171 の要求事項と「サイバー・フィジカル・セキュリティ対策フレームワーク」との対応表

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
アクセス制御	3.1.1	システムアクセスを許可された利用者、許可された利用者を代行して動作するプロセス、またはデバイス(その他のシステムを含めて)に制限する。	・AC-2 アカウント管理 ・AC-3 アクセス制御の実施 ・AC-17 リモートアクセス	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.1.2	システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。	・AC-2 アカウント管理 ・AC-3 アクセス制御の実施 ・AC-17 リモートアクセス	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.1.3	承認された権限付与に従ってCUI のフローを制御する。	・AC-4 情報フロー制御の実施	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムを構成するネットワークの内部における境界について通信をモニタリングし、制御する。 ・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・機密性の高いデータを取り扱う自組織の情報システムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。
						Basic	・組織は、情報システム及び産業用制御システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、適切に論理的あるいは物理的にネットワークを分離することで、フローの制御を実施する。 ・組織は、産業用制御システムにおいて、制御システムのネットワークを情報システムとのネットワークから論理的あるいは物理的にセグメント化する。 [参考] 他のネットワークと物理的に離れた環境においては物理的なセグメント化を実施する、他のネットワークと物理的に近接した環境では、対策のコスト等も考慮して論理的なセグメント化を実施する等の対応が可能である。
				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情報の流れを特定し、管理するプロシージャを確立し、実施する。	H-Advanced	・組織は、ネットワーク構成、機器のソフトウェア構成等の情報を自動的に収集するメカニズムを利用し、常時最新の状況をモニタリングする。 ・システムは、システム内（および相互接続システム間）のデータフローを制御するために、ユーザに対して（管理者によって）承認されたアクセス権限を強制的に適用する。 ・組織/システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターンおよびセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い(通信)を検知できるようにする。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.1.4	共謀のない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。	・AC-5 職務の分離	CPS.AC-5	・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H-Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・情報システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入する。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・組織は、セキュリティインシデントによる被害を最小化するため、有事においてシステム管理者の権限を利用できるユーザを最少化させることができる。 ・組織は、セキュリティインシデントによる被害を最小化するため、システム管理者であっても、サーバの重要なサービスや保護されたプロセスを停止できないようにすることができる。
						Advanced	・組織は、自組織の情報システム及び産業用制御システムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 - 一般のユーザアカウントの権限と、特権アカウントの権限を分離する （非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。） - 自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
	3.1.5	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。	・AC-6 特権の最小化 ・AC-6(1) 特権の最小化 セキュリティ機能へのアクセスを許可する ・AC-6(5) 特権の最小化 特権アカウント	CPS.AC-5	・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H-Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・情報システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入する。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・組織は、セキュリティインシデントによる被害を最小化するため、有事においてシステム管理者の権限を利用できるユーザを最少化させることができる。 ・組織は、セキュリティインシデントによる被害を最小化するため、システム管理者であっても、サーバの重要なサービスや保護されたプロセスを停止できないようにすることができる。
						Advanced	・組織は、自組織の情報システム及び産業用制御システムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 - 一般のユーザアカウントの権限と、特権アカウントの権限を分離する （非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。） - 自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
	3.1.6	非セキュリティ機能を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。	・AC-6(2) 特権の最小化 非セキュリティ機能の非特権アクセス	CPS.AC-5	・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H-Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・情報システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入する。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・組織は、セキュリティインシデントによる被害を最小化するため、有事においてシステム管理者の権限を利用できるユーザを最少化させることができる。 ・組織は、セキュリティインシデントによる被害を最小化するため、システム管理者であっても、サーバの重要なサービスや保護されたプロセスを停止できないようにすることができる。
	3.1.7	非特権利用者による特権機能の実行とこのような機能の実行の監査を防止する。	・AC-6(9) 特権の最小化 特権機能の利用の監査 ・AC-6(10) 特権の最小化 特権機能の実行を非特権利用者に禁止する	CPS.AC-5	・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H-Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・情報システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入する。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・組織は、セキュリティインシデントによる被害を最小化するため、有事においてシステム管理者の権限を利用できるユーザを最少化させることができる。 ・組織は、セキュリティインシデントによる被害を最小化するため、システム管理者であっても、サーバの重要なサービスや保護されたプロセスを停止できないようにすることができる。
	3.1.8	ログイン試行失敗を制限する。	・AC-7 ログイン試行の失敗	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。	H-Advanced	・情報システム及び産業用制御システム（対応の即時性が求められる一部の例を除く）は、自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定し、上限以上失敗した場合には管理者が解除しなければ再ログインできない機能を実装する。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定し、上限以上失敗した場合には一定期間再ログインできない機能を実装する。 ・情報システム及び産業用制御システムは、組織が定める時間を越えてシステムの無操作が持続する場合、手動又は自動でセッションロックを実施する。 ※ 産業用制御システムにおいて、緊急時対応においてオペレータの即時対応が求められるようなセッションを実施するケースが想定される場合、セッションロックを実施しないことが望ましい。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.1.9	適用可能なCUI 規則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。	・AC-8 システムの利用に関する通知	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.1.10	非アクティブな時間の経過後、データのアクセス及び閲覧を防止するため、パタンによる不可視化表示を用いてセションロックを使用する。	・AC-11 セションのロック ・AC-11(1) セションのロック パタンによる不可視化表示	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.1.11	定義された条件の後、利用者セションを(自動的に) 終了する。	・AC-12 セションの終了	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.1.12	リモートアクセスセションを監視し、制御する。	・AC-17(1) リモートアクセス 自動化された監視／管理	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。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・情報システム及び産業用制御システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・情報システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・情報システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザ及び機器による認証を暗号化とともに用いることによって保護する。 ・情報システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
				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・制御、アクセス監視・制御を実施する。	Advanced	・組織は、産業用制御システムと情報システムとの境界において通信をモニタリングし、制御する。 ・組織は、インターネットなどの外部ネットワークと社内ネットワークの中間に内部ネットワークへのアクセスを隔離されたネットワーク上のセグメント（DMZ: 非武装地帯）を構築する。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）を必ず経由させる。 ・組織は、個々の管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・組織は、特定の送信元、あるいは多数の送信元からの大量の通信がないかをシステムの外部境界及びシステム内の主要な内部境界にてモニタリングし、必要に応じて、特定IPアドレスからの通信を遮断するなど、適切な対応を実施する。
						Basic	・組織は、情報システムの外部境界において通信をモニタリングし、制御する。
				CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	H-Advanced	・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル及び他のサービスを明確にするよう要求する。 ・組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。
						Advanced	・組織は、外部サービスプロバイダ及びシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報，業務システム及び業務プロセスの重要性並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスををモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。
	3.1.13	リモートアクセスセションの機密性を保護するために暗号メカニズムを採用する。	・AC-17(2) リモートアクセス 暗号化を用いた機密性／完全性の保護	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。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・情報システム及び産業用制御システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・情報システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・情報システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザ及び機器による認証を暗号化とともに用いることによって保護する。 ・情報システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
				CPS.DS-3	・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。	Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.1.14	管理されたアクセス制御ポイントを介してリモートアクセスをルーティングする。	・AC-17(3) リモートアクセス 管理されたアクセス制御ポイント	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・制御、アクセス監視・制御を実施する。	H-Advanced	・情報システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする。 ・情報システム及び産業用制御システムは、モバイルコードの使用を管理し、監視する。 ・情報システムは、音声や映像の伝送に利用されるプロトコル（例：VoIP）の使用を管理し、監視する。
						Advanced	・組織は、産業用制御システムと情報システムとの境界において通信をモニタリングし、制御する。 ・組織は、インターネットなどの外部ネットワークと社内ネットワークの中間に内部ネットワークへのアクセスを隔離されたネットワーク上のセグメント（DMZ: 非武装地帯）を構築する。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）を必ず経由させる。 ・組織は、個々の管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・組織は、特定の送信元、あるいは多数の送信元からの大量の通信がないかをシステムの外部境界及びシステム内の主要な内部境界にてモニタリングし、必要に応じて、特定IPアドレスからの通信を遮断するなど、適切な対応を実施する。
	3.1.15	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。	・AC-17(4) リモートアクセス 特権コマンド／アクセス	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。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・情報システム及び産業用制御システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・情報システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・情報システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザ及び機器による認証を暗号化とともに用いることによって保護する。 ・情報システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
	3.1.16	無線のコネクションを許可する前に無線アクセスを許可する。	・AC-18 無線アクセスの制限	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。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・情報システム及び産業用制御システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・情報システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・情報システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザ及び機器による認証を暗号化とともに用いることによって保護する。 ・情報システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
						Advanced	・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・組織は、自組織で利用する携帯機器から自組織のシステムの接続に関する承認ルール等を定める。
						Basic	・組織は、許可しているリモートアクセスのタイプごとに使用制限・構成要件・実装ガイダンス等を定める。 ・組織は、許可されていない無線接続を原則禁止とする。 ・組織は、自組織の情報システム及び産業用制御システムへのリモートアクセスの利用に関する承認ルール等を定める。 ・組織は、自組織のシステムへの無線によるアクセスを許可するのに先立って、無線でシステムにアクセスする権限を与える。
	3.1.17	認証と暗号化を用いて無線アクセスを保護する。	・AC-18(1) 無線アクセス 認証と暗号化	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。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・情報システム及び産業用制御システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・情報システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・情報システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザ及び機器による認証を暗号化とともに用いることによって保護する。 ・情報システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.1.18	モバイルデバイスのコネクションを制御する。	・AC-19 携帯機器に対するアクセス制御	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。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・情報システム及び産業用制御システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・情報システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・情報システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザ及び機器による認証を暗号化とともに用いることによって保護する。 ・情報システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
						Advanced	・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・組織は、自組織で利用する携帯機器から自組織のシステムの接続に関する承認ルール等を定める。
				CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.1.19	モバイルデバイス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CUI を暗号化する。	・AC-19(5) 携帯機器に対するアクセス制御 デバイス全体／コンテナベースの暗号化	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H-Advanced	・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・組織は、内部メモリのデータを暗号化して保管することのできるIoT機器を利用する。
						Advanced	・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されたアルゴリズムが選択可能であれば、これを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。 ・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、産業用制御システムが取り扱う重要度の高い情報（データ）を、パフォーマンスに許容できない影響が出ない範囲で適切な強度の方式で暗号化して保管する。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
	3.1.20	外部システムへのコネクション及び使用を検証し、制御／制限する。	・AC-20 外部情報システムの利用 ・AC-20(1) 外部情報システムの利用 許可された利用の制限	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、適切に管理する。	H-Advanced	・システムは、自組織が利用している外部情報システムサービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・システムは、利用を許可していない外部情報システムサービスを検知した場合、システム管理者へ通知するメカニズムを利用する。 ・組織は、外部プロバイダによる情報システムサービスを使用する際に必要な機能、ポート、プロトコル及び他のサービスを明確にする。
						Advanced	・組織は、外部の情報システムを所有、運用する他の組織に対して、下記を許可するうえでの条件を設定する。 a. 外部の情報システムから自組織の情報システムにアクセスすること b. 外部の情報システムを使用して自組織の管理下にある情報を処理または保存もしくは伝送すること ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。
	3.1.21	外部システム上での組織のポータブルストレージデバイスの使用を制限する。	・AC-20(2) 外部情報システムの利用 ポータブルストレージデバイス	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、適切に管理する。	Advanced	・組織は、外部の情報システムを所有、運用する他の組織に対して、下記を許可するうえでの条件を設定する。 a. 外部の情報システムから自組織の情報システムにアクセスすること b. 外部の情報システムを使用して自組織の管理下にある情報を処理または保存もしくは伝送すること ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.1.22	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CUI を制御する。	・AC-22 公的アクセス可能なコンテンツ	CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)
意識向上と訓練	3.2.1	組織のシステムの責任者、システム管理者、及び利用者が、彼らのアクティビティに関連するセキュリティリスク及びそれらのシステムのセキュリティに関連する適用可能なポリシー、基準、及び手順について周知されていることを、保証する。	・AT-2 セキュリティの意識向上 ・AT-3 ロールベースのセキュリティトレーニング	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、教育を実施し、その記録を管理する。	H-Advanced	・組織は、内部不正の兆候を認識・報告するためのセキュリティ意識向上トレーニングを、全要員に対して実施する。
						Advanced	・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。組織は、CPS.AT-1＜Basic＞の[参考]に記載されている一般的な事項を解説しているコンテンツに加えて、組織によって内容が異なる内容として、例えば、下記の事項を扱うことができる。 - 不審なメールを受信した際の対応手順（どこにどのような内容を連絡すればよいか） - モバイル端末利用の注意点（例：公衆無線LANに接続する際の注意点） - SNSを利用する際の注意点 ・組織は、情報セキュリティ要員の育成とレベル向上のための役割別（例：システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者）のプログラムを作成し、定期的に該当する要員に対して実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の記録を定期的にレビューする。
				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得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	Advanced	・組織は、自組織におけるセキュリティインシデントに関係しうる関係組織に対して、担当する要員へ割り当てられた役割を遂行するための適切な訓練（例：実際のインシデント発生時を想定した、シミュレーション）、セキュリティ教育を実施を要求し、その実施状況を確認する。 ・組織は、自組織のセキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対する教育・訓練の記録を定期的にレビューする。
						Basic	・組織は、自組織の要員へ割り当てられた役割を遂行するための適切な訓練（例：実際のインシデント発生時を想定した、シミュレーション）、セキュリティ教育を実施を要求し、その実施状況を確認する。 ・組織は、自組織のセキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対する、セキュリティに係る教育・訓練の内容や結果等について記録し、管理する。
	3.2.2	組織の要員が、その割り当てられた情報セキュリティ関連の職務と責任を遂行するために適切に訓練されていることを、保証する。	・AT-2 セキュリティの意識向上 ・AT-3 ロールベースのセキュリティトレーニング	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、教育を実施し、その記録を管理する。	Advanced	・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。組織は、CPS.AT-1＜Basic＞の[参考]に記載されている一般的な事項を解説しているコンテンツに加えて、組織によって内容が異なる内容として、例えば、下記の事項を扱うことができる。 - 不審なメールを受信した際の対応手順（どこにどのような内容を連絡すればよいか） - モバイル端末利用の注意点（例：公衆無線LANに接続する際の注意点） - SNSを利用する際の注意点 ・組織は、情報セキュリティ要員の育成とレベル向上のための役割別（例：システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者）のプログラムを作成し、定期的に該当する要員に対して実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の記録を定期的にレビューする。
				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得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	Advanced	・組織は、自組織におけるセキュリティインシデントに関係しうる関係組織に対して、担当する要員へ割り当てられた役割を遂行するための適切な訓練（例：実際のインシデント発生時を想定した、シミュレーション）、セキュリティ教育を実施を要求し、その実施状況を確認する。 ・組織は、自組織のセキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対する教育・訓練の記録を定期的にレビューする。
	3.2.3	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提供する。	・AT-2(2) セキュリティの意識向上 内部の脅威	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、教育を実施し、その記録を管理する。	H-Advanced	・組織は、内部不正の兆候を認識・報告するためのセキュリティ意識向上トレーニングを、全要員に対して実施する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
監査と責任追跡性（説明責任）	3.3.1	非合法の、許可されない、または不適切なシステムアクティビティの監視、分析、調査、及び報告を可能とするために必要な範囲で、システム監査記録を作成、保護、及び維持する。	・AU-2 監査対象のイベント ・AU-3 監査記録の内容 ・AU-3(1) 監査記録の内容 追加の監査情報 ・AU-6 監査記録の監視、分析、及び報告 ・AU-12 監査の生成	CPS.SC-6	・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。	H-Advanced	・組織は、契約事項からの逸脱及び、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先及びその再委託先以降の組織に対して、契約にて規定した組織のセキュリティマネジメント、納入する製品・サービスに実装されるセキュリティ機能等に関する義務事項が履行されているかどうかを一覧化して確認できるメカニズムを利用する。 ・委託元による実地調査、外部監査等の手法により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。 ・重要な取引先及びその再委託先以降の組織は、関係する攻撃の予兆、情報流出の事実がないかを調査し、組織に対して結果を定期的に報告する。
						Advanced	・組織は、自組織が取引先との契約において要求事項として規定した内容に関連して、システム上での監査が可能かどうか、確認する。 ・上記で定義されているシステム上で監査可能なイベントのために、監査記録を生成する機能を情報システムが提供する。 ・組織は、監査に関連する情報が必要な他の組織との間で、セキュリティ監査の整合性を保つことができるようにする。 ・組織は、手作業ないしは情報システムにより自動で生成された監査記録を定期的にでレビュー・分析して、契約事項からの逸脱及び、その兆候の有無を確認する。 ・チェックリストを用いた取引先による内部監査により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。
				CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・情報システム及び産業用制御システムは、監査ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。 ・組織は、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
	3.3.2	個別のシステム利用者のアクションが、彼らのアクションについての説明責任を維持可能にするよう、それらの利用者に対して一意に追跡が可能であることを保証する。	・AU-2 監査対象のイベント ・AU-3 監査記録の内容 ・AU-3(1) 監査記録の内容 追加の監査情報 ・AU-6 監査記録の監視、分析、及び報告 ・AU-12 監査の生成	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・情報システム及び産業用制御システムは、監査ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。 ・組織は、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.3.3	監査された事象をレビューし、アップデートする。	・AU-2(3) 監査対象のイベント レビューとアップデート	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・情報システム及び産業用制御システムは、監査ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。 ・組織は、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
	3.3.4	監査プロセス失敗の事象においてアラート(警告) を発する。	・AU-5 監査処理エラーへの対応	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・情報システム及び産業用制御システムは、監査ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
	3.3.5	監査記録のレビュー、分析、及び調査のための報告プロセスを集めて相互の関係を比較し、不適切な、疑わしい、または異常なアクティビティの兆候に対応する。	・AU-6(3) 監査記録の監視、分析、及び報告 監査リポジトリとの相互の関連付け	CPS.SC-6	・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。	H-Advanced	・組織は、契約事項からの逸脱及び、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先及びその再委託先以降の組織に対して、契約にて規定した組織のセキュリティマネジメント、納入する製品・サービスに実装されるセキュリティ機能等に関する義務事項が履行されているかどうかを一覧化して確認できるメカニズムを利用する。 ・委託元による実地調査、外部監査等の手法により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。 ・重要な取引先及びその再委託先以降の組織は、関係する攻撃の予兆、情報流出の事実がないかを調査し、組織に対して結果を定期的に報告する。
				CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。 ・組織は、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.3.6	オンデマンド分析と報告をサポートするため、監査の簡素化と報告書生成を提供する。	・AU-7 監査量の低減と報告書の作成	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
	3.3.7	監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し同期するようなシステム機能を提供する。	・AU-8 タイムスタンプ ・AU-8(1) タイムスタンプ 権威ある時刻ソースとの同期	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
	3.3.8	監査情報と監査ツールを不正なアクセス、改変、及び削除から保護する。	・AU-9 監査情報の保護	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・情報システム及び産業用制御システムは、監査ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
	3.3.9	監査機能の管理を特権利用者の一部に制限する。	・AU-9(4) 監査情報の保護 特権利用者のサブセットによるアクセス	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・情報システム及び産業用制御システムは、監査ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
構成管理	3.4.1	個別のシステム開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、及び文書を含めて) のベースライン構成とインベントリを確立し、維持する。	・CM-2 ベースライン構成 ・CM-6 構成設定 ・CM-8 情報システムコンポーネントのインベントリ ・CM-8(1) 情報システムコンポーネントのインベントリ インストレーション／除去中のアップデート	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	Advanced	・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						Basic	・組織は、自組織の情報システムや産業用制御システムを構成する資産（ハードウェア、ソフトウェア、情報）を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・資産は保有するものすべてを一覧化することが望ましいが、対象が膨大な場合、分析対象の統合（グループ化）と分析対象からの除外を通じて、対象とする資産を絞り込むことを検討する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録（情報資産管理台帳）の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年) のP47を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。
				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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）を必ず経由させる。 ・個々の管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・情報システム及び産業用制御システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
						Basic	・IoT機器、サーバ等を含む資産の型番やソフトウェアのバージョン、サポート期限等を管理する台帳を作成し、定期的に棚卸する。 ・組織は、運用時に実施すべき対策（IoTデバイスの不正利用や盗難、パッチの適用、ログのチェック等）、IoT機器の状況を定期的に確認する。
	3.4.2	組織のシステムで採用された情報技術製品のセキュリティ構成設定を確立し、強制 (実施) する。	・CM-2 ベースライン構成 ・CM-6 構成設定 ・CM-8 情報システムコンポーネントのインベントリ ・CM-8(1) 情報システムコンポーネントのインベントリ インストレーション／除去中のアップデート	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システムを構成する資産（IoT機器等を含むハードウェア、ソフトウェア、情報）を一意に特定し、各々の資産に管理責任者を割り当てた上で、資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、定期的又はオペレータ等の求めに応じて、リアルタイムで状況を把握しながら目録を維持・管理する。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・情報システム及び産業用制御システムは、許可されていない資産を自動的に検出し、管理情報から外す・システムから切り離す等を実行するメカニズムを導入、運用している。 ※ 関連する対策要件に、CPS.CM-6がある。 [参考] 重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）のP.44～P.46 に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティスク分析ガイド 第2版」（IPA, 2018年）のP.21に記載された事業被害の大きさにおける評価を用いる方法等がある
				CPS.IP-1	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法（例：変更実施前に本人にしかわからないセキュリティコードを入力させる）を利用する。 ・組織は、セキュリティ上の変更によって情報システム及び産業用制御システムの可用性や安全性等に悪影響が及ばないことを確実にするため、運用及び変更管理のポリシー及び手順を定期的にレビューする。
						Basic	・組織は、自組織の運用に適合する最も制限された設定基準を定めた上で、導入されるIoT機器、サーバ等の初期設定手順及び設定内容を文書化するとともに、その文書に従って設定を実施する。 ・組織は、IoT機器を設置する前にデフォルトの初期設定値を確認し、CPS.AC-1で定めたポリシーに準じていない場合に適切なものへと変更する。 ・組織は、IoT機器の導入前に、搭載されているソフトウェアを確認し、記録する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.4.3	組織のシステムへの変更を追跡、レビュー、承認／非承認、及び監査する。	・CM-3 構成変更管理	CPS.IP-1	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法（例：変更実施前に本人にしかわからないセキュリティコードを入力させる）を利用する。 ・組織は、セキュリティ上の変更によって情報システム及び産業用制御システムの可用性や安全性等に悪影響が及ばないことを確実にするため、運用及び変更管理のポリシー及び手順を定期的にレビューする。
				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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）を必ず経由させる。 ・個々の管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・情報システム及び産業用制御システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
	3.4.4	実装に先立ち、変更のセキュリティへの影響を分析する。	・CM-4 構成変更の監視	CPS.IP-1	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法（例：変更実施前に本人にしかわからないセキュリティコードを入力させる）を利用する。 ・組織は、セキュリティ上の変更によって情報システム及び産業用制御システムの可用性や安全性等に悪影響が及ばないことを確実にするため、運用及び変更管理のポリシー及び手順を定期的にレビューする。
	3.4.5	組織のシステムへの変更に関連する物理的及び論理的なアクセス制約事項を定義し、文書化し、承認し、強制 (実施) する。	・CM-5 変更のためのアクセス制限	CPS.IP-1	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法（例：変更実施前に本人にしかわからないセキュリティコードを入力させる）を利用する。 ・組織は、セキュリティ上の変更によって情報システム及び産業用制御システムの可用性や安全性等に悪影響が及ばないことを確実にするため、運用及び変更管理のポリシー及び手順を定期的にレビューする。
	3.4.6	基本機能のみを提供するように組織のシステムを構成することによって、最小機能の原則を採用する。	・CM-7 機能の最小化	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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	H-Advanced	・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
						Advanced	・組織は、システム、モノ等によって提供される機能とサービスをレビューし、削除の候補となる機能とサービスを特定する。 ・組織は、禁止されている機能、ポート、プロトコル、サービスの使用を検知し防止するために、ネットワークスキャンツール、侵入検知防止システム、エンドポイントプロテクション（ファイアウォール、ホストベースの侵入検知システム等）を活用する。 ・組織は、IoT機器やPC、サーバ以外の機器であっても、複合機等のネットワークにつながる機器に対しては、不要な機能やサービス等を停止する。
	3.4.7	非基本プログラム、機能、ポート、プロトコル、及びサービスの使用を制限、無効化、及び防止する。	・CM-7(1) 機能の最小化 定期的なレビュー ・CM-7(2) 機能の最小化 プログラム実行の防止	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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	H-Advanced	・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
	3.4.8	許可されないソフトウェアの使用を防止するために例外による拒否 (ブラックリスト) ポリシーを、または許可されたソフトウェアの実行を許可するような例外による許可 (ホワイトリスト)ポリシーを適用する。	・CM-7(2) 機能の最小化 プログラム実行の防止 ・CM-7(5) 機能の最小化 許可されたソフトウェア／ホワイトリスト	CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システム上で実行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）を用いてソフトウェアの制限を実施する、あるいは、許可されていないソフトウェアのインストールを不可とする。
				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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	H-Advanced	・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.4.9	利用者がインストールしたソフトウェアを管理し、監視する。	・CM-11 利用者がインストールしたソフトウェア	CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システム上で実行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）を用いてソフトウェアの制限を実施する、あるいは、許可されていないソフトウェアのインストールを不可とする。
						Advanced	・組織は、自組織の情報システム及び産業用制御システム上でのユーザによるソフトウェアのインストールについて管理するメカニズムを導入し、管理する。
識別と認証	3.5.1	システム利用者、利用者を代行して動作するプロセス、またはデバイスを識別する。	・IA-2 ユーザ識別及び認証 ・IA-5 認証コードの管理	CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・IoT機器での通信は、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。
	3.5.2	組織のシステムへのアクセスの許可に対する必要条件として、それらの利用者、プロセス、またはデバイスのアイデンティティを認証(または検証)する。	・IA-2 ユーザ識別及び認証 ・IA-5 認証コードの管理	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.5.3	多要素認証を、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、使用する。	・IA-2(1) ユーザ識別及び認証 特権アカウントへのネットワークアクセス ・IA-2(2) ユーザ識別及び認証 非特権アカウントへのネットワークアクセス ・IA-2(3) ユーザ識別及び認証 特権アカウントへのローカルアクセス	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、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織の情報システムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、対象システムにおける特権アカウントへの不正ログインのリスク等を勘案し、十分に信頼性の高い認証方式を実装できない場合、ネットワーク経由での特権アカウントへのログインを原則禁止する。 ・情報システムは、自組織のシステムについて管理者アカウントの無効化等制限が実施できない場合には、特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を要求する。 ・情報システムにおけるデフォルトの管理者アカウントは、原則無効化する。 ・情報システムは、権限付与等の特権操作を実施する場合には、利用ユーザアカウントに対して必要最小限の特権操作権限を付与する。
	3.5.4	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、リプレイ耐性のある認証メカニズムを採用する。	・IA-2(8) ユーザ識別及び認証 特権アカウントへのネットワークアクセスーリプレイ耐性 ・IA-2(9) ユーザ識別及び認証 非特権アカウントへのネットワークアクセスーリプレイ耐性	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、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織の情報システムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.5.5	定義された期間について、識別コードの再利用を禁止する。	・IA-4 識別子の管理	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・共有ユーザアカウントに関しては、認証情報を知りえるユーザを一覧等で管理し、アカウントを利用する範囲を特定可能にする。 ・組織は、情報システムにおけるシステムアカウントの利用状況をモニタリングする。 ・組織は、アカウントが不要にな-った場合や変更が必要となった場合には管理責任者に通知する。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・組織は、情報システム及び産業用制御システムにおいてパスワードが変更された場合、ユーザー（または管理責任者）に通知する。 ・情報システムは、クレデンシャルを忘れてしまった際等にクレデンシャルを再設定する場合、悪意ある者によるクレデンシャルの不正な変更を防ぐため、当該アカウントが自身のものかどうかを確認するための安全な手順を適用する。
						Basic	・組織は、自組織の情報システム及び産業用制御システムのアカウントを管理する管理責任者を配置する。 ・組織は、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別（例：一般ユーザ／システム管理者／共有ユーザ／一時的なユーザ）を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・組織は、自組織の情報システム及び産業用制御システムに対するクレデンシャル（例：パスワード、セキュリティキー）のポリシーを定め、そのポリシーを満たすクレデンシャルでなければ設定できない機能を実装する。ポリシーの内容の例としては、下記が挙げられる。 - クレデンシャルに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいクレデンシャルが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたクレデンシャルのみを保存・伝送する。 - 同じクレデンシャルを組織が定めた世代にわたって再利用するのを禁止する。 ・クレデンシャルを忘れてしまった際等に、強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なクレデンシャルを使用することを許可する。 ・組織は、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。
				CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・IoT機器での通信は、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。
	3.5.6	定義された非アクティブな期間の後、識別子を無効化する。	・IA-4 識別子の管理	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・共有ユーザアカウントに関しては、認証情報を知りえるユーザを一覧等で管理し、アカウントを利用する範囲を特定可能にする。 ・組織は、情報システムにおけるシステムアカウントの利用状況をモニタリングする。 ・組織は、アカウントが不要にな-った場合や変更が必要となった場合には管理責任者に通知する。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・組織は、情報システム及び産業用制御システムにおいてパスワードが変更された場合、ユーザー（または管理責任者）に通知する。 ・情報システムは、クレデンシャルを忘れてしまった際等にクレデンシャルを再設定する場合、悪意ある者によるクレデンシャルの不正な変更を防ぐため、当該アカウントが自身のものかどうかを確認するための安全な手順を適用する。
						Basic	・組織は、自組織の情報システム及び産業用制御システムのアカウントを管理する管理責任者を配置する。 ・組織は、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別（例：一般ユーザ／システム管理者／共有ユーザ／一時的なユーザ）を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・組織は、自組織の情報システム及び産業用制御システムに対するクレデンシャル（例：パスワード、セキュリティキー）のポリシーを定め、そのポリシーを満たすクレデンシャルでなければ設定できない機能を実装する。ポリシーの内容の例としては、下記が挙げられる。 - クレデンシャルに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいクレデンシャルが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたクレデンシャルのみを保存・伝送する。 - 同じクレデンシャルを組織が定めた世代にわたって再利用するのを禁止する。 ・クレデンシャルを忘れてしまった際等に、強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なクレデンシャルを使用することを許可する。 ・組織は、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件		対策例
	3.5.7	新しいパスワードが作成されるとき、最小パスワード複雑性及び文字列の変更を強制(実施)する。	・IA-5(1) 認証コードの管理 パスワードベース認証	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.5.8	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。	・IA-5(1) 認証コードの管理 パスワードベース認証	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.5.9	永久パスワードへ直ちに変更するようなときのシステムログインのために一時的パスワードの使用を許可する。	・IA-5(1) 認証コードの管理 パスワードベース認証	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.5.10	暗号学的に保護されたパスワードのみを格納及び送信する。	・IA-5(1) 認証コードの管理 パスワードベース認証	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.5.11	認証情報のフィードバックを目に見えないようにする。	・IA-6 認証コードのフィードバック	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
インシデント対応				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、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	H-Advanced	・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、サプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するテストを実施する。 [参考] サプライチェーンにおけるセキュリティインシデントには、例えば、システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害等がある。
						Advanced	・組織は、インシデント対応要件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、自組織と外部サービスプロバイダーとの間で連携を要するインシデント対応プロセスをテストする。
				CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	Advanced	・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。なお、相関分析の対象には、他組織とデータを連携する部分のログも含めることが望ましい。 - モニタリングするシステムの範囲をどこまでとするか - どのような機器のログを収集し、分析するか (CPS.AE-3を参照) ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する（プロセスの内容については、CPS.RP-1等を参照）。 ・組織及びシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には以下を含むことが望ましい。 - ログ分析の分析結果（対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等） - モニタリングにおける今後の改善方針 [参考] セキュリティ対応組織(SOC/CSIRT)の業務、望まれる規模等については、「セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年)等を参照することが望ましい。
				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する。	Advanced	・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、共有することによって、当該セキュリティ事象の全容を把握する。 ・セキュリティ事象発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を外部のセキュリティベンダー等に依頼する。
	3.6.1	適切な準備、検知、分析、抑制 (封じ込め)、リカバリ、及び利用者対応アクティビティを含めて、組織のシステムのための運用上のインシデントハンドリング能力を確立する。	・IR-2 インシデント対応のトレーニング ・IR-4 インシデントの対応 ・IR-5 インシデントの監視 ・IR-6 インシデントの報告 ・IR-7 インシデント対応の支援	CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	Basic	・組織は、セキュリティインシデントの発生時に利用するセキュリティ運用プロセスを策定し、運用する。当該プロセスには、下記を例とする内容を含むことが望ましい。 - インシデントの報告を受けた者が、どのような対応をするのか、あるいはより上位に報告するのかの判断基準 - 緊急時の指揮命令と対応の優先順位の決定 - インシデントへの対応（インシデントレスポンス） - インシデントの影響と被害の分析 - 情報収集と自社に必要な情報の選別 - 社内関係者への連絡と周知 - 外部関係機関との連絡 ・システム（特に産業用制御システム）は、IoT機器、サーバ等に異常（誤動作等）が発生した場合に、緊急停止、管理者へのアラート通知等のフェールセーフのための対応を実施する。 [参考] セキュリティインシデント発生時の対応手順の検討において、「インシデントハンドリングマニュアル」(JPCERT/CC, 2015年)、SP 800-61 Rev.1 (NIST, 2008年)、「インシデント対応マニュアルの作成について」(JPCERT/CC, 2015年)を参照することが可能である。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件		対策例
				CPS.CO-3	・復旧活動について内部及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、事業継続計画又は緊急事対応計画の中に位置づける。	Advanced	・組織は、監督官庁、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。 ・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動及びインシデントの事後処理に関わる活動を調整する。ここで該当する活動の例として、生産システムにおけるセキュリティインシデント発生時に生産されたモノの回収等が挙げられる。
				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、自組織及び関係する他組織を含む社会全体への影響を把握する。	Advanced	・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、共有することによって、当該セキュリティインシデントの全容を把握する。 ・セキュリティインシデント発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を外部のセキュリティベンダー等に依頼する。
				CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。	Advanced	・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位及びメトリクスを考慮してインシデントを分類する。 ・組織は、自組織に影響を及ぼすセキュリティインシデントを追跡し、文書化する。「SP 800-61 Rev.1」では、セキュリティインシデントを文書化する際の記載の観点として、下記を例示している。 - インシデントの現在の状況 - インシデントの概要 - 当該インシデントに対して自組織のとった行動の内容 - ほかの関係者(システム所有者、システム管理者等)の連絡先情報 - 調査の際に収集した証拠の一覧 - インシデントの処理担当者からのコメント - 次にとるべきステップ
				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。	Basic	・組織（あるいはその構成員）は、あらかじめ定められたプロシージャに従って、セキュリティインシデントを低減するためのアクション（例えば、システムのシャットダウン、有線/無線ネットワークからの切断、モデムケーブルの切断、特定の機能の無効化など）を実行する。 [参考]セキュリティインシデントの影響低減のための活動は、インシデントの性質（例えば、サービス拒否攻撃、マルウェア感染、不正アクセスのような顕在化する脅威の差異）により内容が異なる場合がある。より詳細な影響低減活動の情報については、「インシデントハンドリングマニュアル」(JPCERT/CC, 2015年)、SP 800-61 Rev.1 (NIST, 2008年)等を参照することが望ましい。
	3.6.2	組織の内部及び外部の両方の、適切な担当官及び／または権威に対して、インシデントについての追跡、文書化、及び報告を行う。	・IR-2 インシデント対応のトレーニング ・IR-4 インシデントの対応 ・IR-5 インシデントの監視 ・IR-6 インシデントの報告 ・IR-7 インシデント対応の支援	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。	Advanced	・組織は、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。 ・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動及びインシデントの事後処理に関わる活動を調整する。その際、CPS.AM-2, CPS.AM-3にて記載している方法により、対応の対象となるモノを特定していることが望ましい。 ※ CPS.CO-3と関連
				CPS.CO-2	・事業継続計画又は緊急事対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。	Basic	・マスコミや取引先に対する情報のやり取りの窓口を一本化し、対応方針が一貫したものとなるようにする。 ・セキュリティインシデントによる被害に関する重要な情報について、情報の機密性に配慮しつつ丁寧に説明する。
				CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。	Advanced	・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位及びメトリクスを考慮してインシデントを分類する。 ・組織は、自組織に影響を及ぼすセキュリティインシデントを追跡し、文書化する。「SP 800-61 Rev.1」では、セキュリティインシデントを文書化する際の記載の観点として、下記を例示している。 - インシデントの現在の状況 - インシデントの概要 - 当該インシデントに対して自組織のとった行動の内容 - ほかの関係者(システム所有者、システム管理者等)の連絡先情報 - 調査の際に収集した証拠の一覧 - インシデントの処理担当者からのコメント - 次にとるべきステップ

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件		対策例
	3.6.3	組織のインシデント対応能力をテストする。	・IR-3 インシデント対応のテストと実習 ・IR-3(2) インシデント対応のテストと実習 関連する計画との調整	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、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	H-Advanced	・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、サプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するテストを実施する。 [参考] サプライチェーンにおけるセキュリティインシデントには、例えば、システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害等がある。
						Advanced	・組織は、インシデント対応要件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、自組織と外部サービスプロバイダーとの間で連携を要するインシデント対応プロセスをテストする。
				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、教育を実施し、その記録を管理する。	H-Advanced	・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。組織は、CPS.AT-1＜Basic＞の[参考]に記載されている一般的な事項を解説しているコンテンツに加えて、組織によって内容が異なる内容として、例えば、下記の事項を扱うことができる。 - 不審なメールを受信した際の対応手順（どこにどのような内容を連絡すればよいか） - モバイル端末利用の注意点（例：公衆無線LANに接続する際の注意点） - SNSを利用する際の注意点 ・組織は、情報セキュリティ要員の育成とレベル向上のための役割別（例：システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者）のプログラムを作成し、定期的に該当する要員に対して実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の記録を定期的にレビューする。
						Advanced	・組織は、自組織の利用する情報システム及び産業用制御システムに対する変更により必要になった場合や新規職員に対して基本的なセキュリティ意識向上トレーニングを実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の内容や結果等について記録し、管理する。 [参考] 組織が従業員等に対してセキュリティ教育を実施する際、IPAが公開している「情報セキュリティ読本 教育用プレゼン資料」の内容を参照することが可能である。
メンテナンス	3.7.1	組織のシステムにおいてメンテナンスを実施する。	・MA-2 定期的な保守 ・MA-3 保守ツール ・MA-3(1) 保守ツール ツールを検査する ・MA-3(2) 保守ツール メディアを検査する	CPS.MA-1	・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 ・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な変更または不正な変更がないか確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。
						Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
	3.7.2	システムメンテナンスを実施するために使用されるツール、手法、メカニズム、及び要員における有効な管理策を提供する。	・MA-2 定期的な保守 ・MA-3 保守ツール ・MA-3(1) 保守ツール ツールを検査する ・MA-3(2) 保守ツール メディアを検査する	CPS.MA-1	・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 ・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な変更または不正な変更がないか確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。
						Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.7.3	オフサイトのメンテナンスのために除去される装置は、あらゆるCUI についてサニタイズされることを保証する。	・MA-2 定期的な保守	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ID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする。	H-Advanced	・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。
						Advanced	・組織は、自組織のIoT機器やサーバ等を廃棄するプロシージャを定め、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。
						Basic	・組織は、自組織のIoT機器やサーバ等を廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態にする。
	3.7.4	組織のシステム内でメディアが使用される前に、悪意のあるコードが入っていないか診断及びテストプログラムを用いてメディアをチェックする。	・MA-3(2) 保守ツール	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、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 ・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な変更または不正な変更がないか確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。
						Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
	3.7.5	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。	・MA-4 遠隔保守	CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	Advanced	・組織は、遠隔保守のための接続の確立と実施に関するポリシーとプロシージャを文書化し、その内容により実施する。 ・組織は、遠隔保守を実施する際には組織の定めるネットワークアクセスに求める認証を実施するとともに、遠隔保守が完了したらセッションとネットワーク接続を確実に終了する。
						Basic	・組織は、遠隔保守の実施に当たっては、実施計画を策定し・合意した上で実施し、実施結果を確認する。 ・組織は、実施した遠隔保守の実施記録を保管する。
	3.7.6	必要なアクセス許可なしにメンテナンス要員のメンテナンス活動を監督する。	・MA-5 保守要員	CPS.SC-5	・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。	H-Advanced	・組織は、委託先の要員により委託元が要求するセキュリティ要求事項が遵守されているかどうかを継続的にモニタリングし、通常とは異なる行動があった場合、自組織の担当者に通知できるようにプロシージャを整備する。
						Advanced	・サプライヤー関係のセキュリティ面について該当する要員を訓練し、機密情報の取り扱いが正しく理解されていることを特に確認する。 ・委託業務の遂行に当たり、委託元が要求するセキュリティ要求事項が遵守されていることを定期的に確認する。
				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、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 ・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。	Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
						Basic	・組織は、メンテナンス要員が付添いなしで情報システム及び産業用制御システムのメンテナンスを行う場合に、その要員が必要なアクセス権限を有することを確認する。 ・組織は、必要なアクセス権限を持たない要員によるメンテナンス活動を監督するのに必要なアクセス権限と技術的能力を有する組織の要員を指定する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
メディア処理	3.8.1	紙及びディジタルの両方の、CUI を含む、システムメディアを保護する(即ち、物理的に制御及びセキュアに格納する)。	・MP-2 メディアへのアクセス ・MP-4 メディアの保管 ・MP-6 メディア上の記録の抹消とメディアの廃棄	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。	H-Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。
						Advanced	・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。
						Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設においてセキュリティを保つべき物理的セキュリティ境界を定め、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に応じてアクセス制御を実施する。 ・組織は、物理的セキュリティ境界内における自組織または自組織外の一時的に認可された入場者に対して、認可された関係者の付き添い又は監視カメラ等により作業内容をモニタリングできるようにする。
				CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	H-Advanced	・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
						Advanced	・組織は、システム、モノ等によって提供される機能とサービスをレビューし、削除の候補となる機能とサービスを特定する。 ・組織は、禁止されている機能、ポート、プロトコル、サービスの使用を検知し防止するために、ネットワークスキャンツール、侵入検知防止システム、エンドポイントプロテクション（ファイアウォール、ホストベースの侵入検知システム等）を活用する。 ・組織は、IoT機器やPC、サーバ以外の機器であっても、複合機等のネットワークにつながる機器に対しては、不要な機能やサービス等を停止する。
						Basic	・使用するUSBメモリ等の周辺機器は、管理台帳を作成し、保管場所を施錠して管理する。 ・IoT機器、サーバ等に接続するUSBメモリ等の外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能なUSBメモリを用いる等の対策を行う。 ・使用しないUSBポート、シリアルポートは栓をするなど物理的に閉塞する。
	3.8.2	システムメディア上のCUI へのアクセスを許可された利用者に制限する。	・MP-2 メディアへのアクセス ・MP-4 メディアの保管 ・MP-6 メディア上の記録の抹消とメディアの廃棄	CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する。
				CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
	3.8.3	廃棄または再利用のために手放す前に、CUI を含むシステムメディアをサニタイズまたは破壊する。	・MP-2 メディアへのアクセス ・MP-4 メディアの保管 ・MP-6 メディア上の記録の抹消とメディアの廃棄	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ID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする。	H-Advanced	・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。
						Advanced	・組織は、自組織のIoT機器やサーバ等を廃棄するプロシージャを定め、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。
						Basic	・組織は、自組織のIoT機器やサーバ等を廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態にする。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.8.4	CUI のマーク表示と配付制限が必要なメディアに対して表示を行う。	・MP-3 メディアへのラベル付け	CPS.AM-6	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	Advanced	・組織は、情報システムや産業用制御システムにおけるリソース（データ及びデータを処理するモノ、システム等）を分類する際には、データを共有又は制限する業務上の要求及び法的要求事項を考慮する。 ・当該資産の管理責任者は、データの分類に対して責任を負う。 ・組織は、リソースの分類体系に分類の規則及びその分類を時間が経ってからレビューするための基準を含める。
						Basic	・組織は、洗い出した情報システムや産業用制御システムにおける資産を、自組織にとっての重要度に応じて優先順位づけする。 ・関係する法規制等により、自組織のリソース（例：システム、データ）について特定の分類に従うことが要求されている場合、該当する分類を資産に適用する。 ・組織は、特に産業用制御システムにおけるモノ、システム等の分類、優先付けに当たっては、自組織の事業活動の適切でない運用によりHSE(Health, Safety and Environment)への悪影響が発生するかを考慮して実施する。 ・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、事業継続の観点から重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 [参考] 資産の重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）の P.44～46に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA, 2018年）の P.21 に記載された事業被害の大きさにおける評価を用いる方法等がある。また、特に産業用制御システムにおける資産の重要度の判断基準については、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA, 2018年）4.2.2及び4.2.3を参照することができる。
	3.8.5	CUI を含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの説明責任を維持する。	・MP-5 メディアの輸送	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	Advanced	・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						Basic	・組織は、自組織の情報システムや産業用制御システムを構成する資産（ハードウェア、ソフトウェア、情報）を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・資産は保有するものすべてを一覧化することが望ましいが、対象が膨大な場合、分析対象の統合（グループ化）と分析対象からの除外を通じて、対象とする資産を絞り込むことを検討する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録（情報資産管理台帳）の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年)のP47を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。
	3.8.6	代替の物理的予防手段による保護がない限り、持ち出し中はディジタルメディア上に格納されたCUI の機密性を保護するための暗号学的メカニズムを実装する。	・MP-5(4) メディアの輸送 暗号学的保護	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H-Advanced	・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・組織は、内部メモリのデータを暗号化して保管することのできるIoT機器を利用する。
	3.8.7	システムコンポーネント上の取り外し可能なメディアの使用を管理する。	・MP-7 メディアの利用	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	Advanced	・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						Basic	・組織は、自組織の情報システムや産業用制御システムを構成する資産（ハードウェア、ソフトウェア、情報）を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・資産は保有するものすべてを一覧化することが望ましいが、対象が膨大な場合、分析対象の統合（グループ化）と分析対象からの除外を通じて、対象とする資産を絞り込むことを検討する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録（情報資産管理台帳）の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年)のP47を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.8.8	ポータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。	・MP-7(1) メディアの利用 所有者以外の利用を禁止	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	Advanced	・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						Basic	・組織は、自組織の情報システムや産業用制御システムを構成する資産（ハードウェア、ソフトウェア、情報）を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・資産は保有するものすべてを一覧化することが望ましいが、対象が膨大な場合、分析対象の統合（グループ化）と分析対象からの除外を通じて、対象とする資産を絞り込むことを検討する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録（情報資産管理台帳）の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年)のP47を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。
	3.8.9	保存場所にあるバックアップCUI の機密性を保護する。	・CP-9 情報システムのバックアップ	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、テストする。	Advanced	・組織は、自組織のシステムドキュメントのバックアップを定めたタイミングや頻度で実施する。 ・組織は、保管拠点におけるバックアップ情報の機密性・完全性・可用性を保護する。
						Basic	・組織は、自組織の情報システム及び産業用制御システムに含まれるユーザレベル・システムレベルの情報のバックアップを定めたタイミングや頻度で実施する。
人的セキュリティ	3.9.1	CUI 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。	・PS-3 要員に対する審査 ・PS-4 要員の解雇 ・PS-5 人事異動	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）を含める。	Advanced	・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。 ・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。 ・組織は、機密情報を扱う要員に対しては特に、採用から退職に至るまでのサイクル全体に渡り、セキュリティ上の責任に対処する。
						Basic	・組織は、雇用条件においてセキュリティに係る要員の責任について明記する。雇用終了後の情報漏えい等を抑止するため、この責任は、雇用終了後の妥当な期間に渡って持続するよう記載する。 ・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。 ・組織は、要員の退職時に以下を実施する。 -自組織のシステムに対するアクセスを一定期間内に無効にする。 -職員に関連する認証及びクレデンシャルを無効にする。 -セキュリティに関連するシステム関連の所有物をすべて回収する。 -退職する個人が管理していた組織の情報と情報システムに対するアクセスを保持する。
	3.9.2	離職または配置転換等の人事措置の間と後で、CUI 及びCUI を含む組織のシステムが保護されることを保証する。	・PS-3 要員に対する審査 ・PS-4 要員の解雇 ・PS-5 人事異動	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）を含める。	Advanced	・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。 ・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。 ・組織は、機密情報を扱う要員に対しては特に、採用から退職に至るまでのサイクル全体に渡り、セキュリティ上の責任に対処する。
						Basic	・組織は、雇用条件においてセキュリティに係る要員の責任について明記する。雇用終了後の情報漏えい等を抑止するため、この責任は、雇用終了後の妥当な期間に渡って持続するよう記載する。 ・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。 ・組織は、要員の退職時に以下を実施する。 -自組織のシステムに対するアクセスを一定期間内に無効にする。 -職員に関連する認証及びクレデンシャルを無効にする。 -セキュリティに関連するシステム関連の所有物をすべて回収する。 -退職する個人が管理していた組織の情報と情報システムに対するアクセスを保持する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
物理的保護	3.10.1	組織のシステム、装置、及びそれぞれの運用環境への物理的アクセスを許可された個人に制限する。	・PE-2 物理的アクセス権限 ・PE-5 表示メディアへのアクセス制御 ・PE-6 物理的アクセスの監視	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。	Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設においてセキュリティを保つべき物理的セキュリティ境界を定め、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に応じてアクセス制御を実施する。 ・組織は、物理的セキュリティ境界内における自組織または自組織外の一時的に認可された入場者に対して、認可された関係者の付き添い又は監視カメラ等により作業内容をモニタリングできるようにする。
	3.10.2	物理的設備を保護し、監視し、組織のシステムの基盤をサポートする。	・PE-2 物理的アクセス権限 ・PE-5 表示メディアへのアクセス制御 ・PE-6 物理的アクセスの監視	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	Advanced	・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。
				CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	Advanced	・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア（執務室等）において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。
						Basic	・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来客に付き添うなどして人手による代替的な対策を実施する。 ・施設内の、一般の人がアクセスできない指定エリアに対するアクセスを制御するための、入退室管理対策を実施する。 ・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入退室時のログを保持する。
	3.10.3	訪問者をエスコートし、訪問者の活動を監視する。	・PE-3 物理的アクセス制御	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。	Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設においてセキュリティを保つべき物理的セキュリティ境界を定め、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に応じてアクセス制御を実施する。 ・組織は、物理的セキュリティ境界内における自組織または自組織外の一時的に認可された入場者に対して、認可された関係者の付き添い又は監視カメラ等により作業内容をモニタリングできるようにする。
	3.10.4	物理的アクセスの監査ログを維持する。	・PE-3 物理的アクセス制御	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	Advanced	・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。
				CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	Advanced	・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア（執務室等）において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。
						Basic	・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来客に付き添うなどして人手による代替的な対策を実施する。 ・施設内の、一般の人がアクセスできない指定エリアに対するアクセスを制御するための、入退室管理対策を実施する。 ・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入退室時のログを保持する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.10.5	物理的アクセスデバイスを制御し、管理する。	・PE-3 物理的アクセス制御	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	Advanced	・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。
				CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	Advanced	・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア（執務室等）において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。
						Basic	・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来客に付き添うなどして人手による代替的な対策を実施する。 ・施設内の、一般の人がアクセスできない指定エリアに対するアクセスを制御するための、入退室管理対策を実施する。 ・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入退室時のログを保持する。
	3.10.6	代替の作業サイト(例、テレワークのサイト)でのCUI に対する防護対策を強制(実施)する。	・PE-17 代替作業拠点	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。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・情報システム及び産業用制御システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・情報システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・情報システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザ及び機器による認証を暗号化とともに用いることによって保護する。 ・情報システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
リスクアセスメント	3.11.1	組織のシステムの運用と関連するCUI の処理、ストレージ、または送信からの結果として組織運用（ミッション、職務、イメージ、または風評を含めて）、組織の資産、及び個人に対するリスクを定期的にアセスメントする。	・RA-3 リスクアセスメント	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機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	Advanced	・組織は、情報システム、または情報システムが稼働する環境に大きな変化があった場合（新たな脅威や脆弱性の特定を含む）、もしくは情報システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。 ・組織は、新たにIoT機器を利用したシステムを企画・設計する場合、既存の資産や新たに導入するシステムにおける守るべき資産を特定し、システムの利用用途や構成に応じて、セキュリティ対策をまとめる。特に、ライフサイクルの長いモノ、システムや、高い可用性を求められるモノ、システムを扱う場合は、設計以前の段階におけるセキュリティ対策の考慮が特に重要である。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 [参考] システム及びモノにおけるセキュリティの要求仕様を検討するにあたり、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。
	3.11.2	定期的に、及び組織のシステムとアプリケーションに影響する新しい脆弱性が識別されるときに、それらのシステム及びアプリケーションの脆弱性についてスキャンする。	・RA-5 脆弱性のスキャン ・RA-5(5) 脆弱性のスキャン特権アクセス	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。	H-Advanced	・組織は、自組織が管理する産業用制御システムの構成要素（IoT機器を含む）に対して、計画停止時等に脆弱性診断を実施し、自組織の所有するシステムに存在する脆弱性を認識し、一覧化する。 ・組織は、ツールを用いて脆弱性診断を行う場合、診断すべきシステムの脆弱性データベースをすぐに更新できる脆弱性診断ツールを使用することが望ましい。 ・組織は、スキャンされたシステムの脆弱性を定期的に、あるいは新たな脆弱性が特定され、報告された場合に更新する。 ・組織は、指定された脆弱性スキャン活動に関して、対象システムのコンポーネントに対する特権的アクセスの許可制度を実施する。
						Advanced	・組織は、情報システム及びアプリケーションの脆弱性のスキャンを定期的に、あるいは、それらのシステム／アプリケーションに影響を及ぼす新たな脆弱性が確認され、報告された場合に実施する。 ・組織は、脆弱性スキャンにツールを用いる。以下を満たす標準的な手法を使用することによって、脆弱性管理プロセスの一部を自動化できることが求められる。 - プラットフォーム、ソフトウェアの欠陥及び誤った設定を列挙する - チェックリストとテスト手順をフォーマットする - 脆弱性による影響を評価する ・組織は、リスクアセスメントを通じて、特定された脆弱性を適切な期間中に修正する。 ・上記のプロセスから得た情報を組織内の他のシステムの管理者と共有することによって、他の情報システム内の同様の脆弱性を把握し、必要に応じて修正する。 [参考] 脆弱性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の影響の大きさを評価する指標として、CVSS(IPAによる解説：https://www.ipa.go.jp/security/vuln/CVSS.html)を参考とすることが可能である。
						Basic	・組織は、情報システム及びアプリケーションの脆弱性のスキャンを定期的に実施する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.11.3	リスクのアセスメントに従い、脆弱性を修正する。	・RA-5 脆弱性のスキャン	CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	Advanced	・組織は、セキュリティリスク対応のプロセスについての文書化した情報を安全に保管する。 ・組織は、リスクアセスメントの結果に応じて対応策を選定する際、実施する対応策及び当該対応策を採用する理由を文書化することが望ましい。 ・組織は、対応策の適用等に関して、セキュリティリスク対応計画を策定し、リスク所有者の承認を得る。 ・組織は、セキュリティリスク対応計画をレビューし、当該計画が自組織全体のリスクマネジメント戦略における優先順位に適合しているかどうかを確認する。 ・CPS.RA-4で抽出した、IoT機器を含む新しいシステムにおける必要なセキュリティ対策について、然るべき外部事業者に要求仕様として伝達する。 ・組織は、IoT機器を含むシステムの導入時に、要求仕様や契約段階で定めたセキュリティ対策が実施されているかを受け入れ検査などで確認する。もし、不明な点があれば、外部事業者に確認する。
						Basic	・組織は、リスクアセスメントの結果を考慮して、対象とするリスクへの対応策を選定する。 ・組織は、セキュリティリスク対応の実施計画を策定する。 ・セキュリティリスクの受容について、リスク所有者の承認を得る。
				CPS.CM-7	・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	Advanced	・組織は、情報システム及びアプリケーションの脆弱性のスキャンを定期的に、あるいは、それらのシステム／アプリケーションに影響を及ぼす新たな脆弱性が確認され、報告された場合に実施する。 ・組織は、脆弱性スキャンにツールを用いる。以下を満たす標準的な手法を使用することによって、脆弱性管理プロセスの一部を自動化できることが求められる。 - プラットフォーム、ソフトウェアの欠陥及び誤った設定を列挙する - チェックリストとテスト手順をフォーマットする - 脆弱性による影響を評価する ・組織は、リスクアセスメントを通じて、特定された脆弱性を適切な期間中に修正する。 ・上記のプロセスから得た情報を組織内の他のシステムの管理者と共有することによって、他の情報システム内の同様の脆弱性を把握し、必要に応じて修正する。 [参考] 脆弱性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の影響の大きさを評価する指標として、CVSS(IPAによる解説：https://www.ipa.go.jp/security/vuln/CVSS.html)を参考とすることが可能である。
						Basic	・組織は、情報システム及びアプリケーションの脆弱性のスキャンを定期的に実施する。
セキュリティアセスメント	3.12.1	管理策がそれらのアプリケーションにおいて有効であるかどうかを決定するために、組織のシステムにおけるセキュリティ管理策を定期的にアセスメントする。	・CA-2 セキュリティア評価 ・CA-5 行動計画とマイルストン ・CA-7 継続的な監視 ・PL-2 システムセキュリティ計画	CPS.IP-7	・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	Advanced	・組織は、セキュリティ評価を適切かつ計画的に実施するため、以下に示す事項を含めたセキュリティ評価計画を策定した上で、セキュリティ評価を実施する。 -セキュリティ評価の対象とするセキュリティ対策 -セキュリティ対策の有効性を図るために用いる評価手順 -セキュリティ評価を実施する環境や実施体制 -セキュリティ評価結果の取りまとめ方法とその活用方法
						Basic	・組織は、セキュリティ対策が正しく実装されているか及び運用されているかに加え、セキュリティ対策が期待された成果を上げているかに関する定期的に評価（セキュリティ評価）を実施し、管理責任者へ報告する。 ・組織は、セキュリティ評価の結果に基づき、セキュリティ対策の改善を実施する。
	3.12.2	欠陥を修正し、組織のシステムにおける脆弱性を軽減し、または取り除くために設計された行動計画を策定し、実施する。	・CA-2 セキュリティア評価 ・CA-5 行動計画とマイルストン ・CA-7 継続的な監視 ・PL-2 システムセキュリティ計画	CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	Advanced	・組織は、セキュリティリスク対応のプロセスについての文書化した情報を安全に保管する。 ・組織は、リスクアセスメントの結果に応じて対応策を選定する際、実施する対応策及び当該対応策を採用する理由を文書化することが望ましい。 ・組織は、対応策の適用等に関して、セキュリティリスク対応計画を策定し、リスク所有者の承認を得る。 ・組織は、セキュリティリスク対応計画をレビューし、当該計画が自組織全体のリスクマネジメント戦略における優先順位に適合しているかどうかを確認する。 ・CPS.RA-4で抽出した、IoT機器を含む新しいシステムにおける必要なセキュリティ対策について、然るべき外部事業者に要求仕様として伝達する。 ・組織は、IoT機器を含むシステムの導入時に、要求仕様や契約段階で定めたセキュリティ対策が実施されているかを受け入れ検査などで確認する。もし、不明な点があれば、外部事業者に確認する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.12.3	管理策の継続的な有効性を保証するため、継続的にセキュリティ管理策を監視する。	・CA-2 セキュリティア評価 ・CA-5 行動計画とマイルストン ・CA-7 継続的な監視 ・PL-2 システムセキュリティ計画	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機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	H-Advanced	・組織は、産業用制御システムのようにモノの制御等を伴うような、フィジカル空間に影響を及ぼす可能性のある新たな機器やシステムを開発する場合には、従来の製品や他の事故事例を収集・分析し、セキュリティの観点も含めてセーフティに関わるハザードを特定する。 ・組織は、主に産業用制御システムにおいて、ハザードによって危害に至る状況を分析し、発生しやすさや被害の深刻度を明らかにすることで、生じるリスクを見積もる。その際、セキュリティの問題に起因するハザードの有無を確認することが望ましい。 ・組織は、産業用制御システム、またはそれが稼働する環境に大きな変化があった場合、もしくは産業用制御システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。 [参考] セーフティ設計におけるハザードの特定と分析については、「つながる世界のセーフティ＆セキュリティ設計入門」(IPA, 2015年)の4.2にて具体的な手法が記載されており、参照することが可能である。
						Advanced	・組織は、情報システム、または情報システムが稼働する環境に大きな変化があった場合（新たな脅威や脆弱性の特定を含む）、もしくは情報システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。 ・組織は、新たにIoT機器を利用したシステムを企画・設計する場合、既存の資産や新たに導入するシステムにおける守るべき資産を特定し、システムの利用用途や構成に応じて、セキュリティ対策をまとめる。特に、ライフサイクルの長いモノ、システムや、高い可用性を求められるモノ、システムを扱う場合は、設計以前の段階におけるセキュリティ対策の考慮が特に重要である。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 [参考] システム及びモノにおけるセキュリティの要求仕様を検討するにあたり、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。
						Basic	・組織は、情報システム及び産業用制御システムに対するセキュリティリスクアセスメントのプロセスを定め，定期的（例えば、重要度の高い情報システムは年に1回）に適用する。 - セキュリティのリスク基準を確立し，維持する。 - 以下の方法によりセキュリティリスクを特定する。 1) 分析対象を明確化する 2) インシデント(周辺状況の変化を含む)並びにこれらの原因を特定する - 以下の方法により、セキュリティリスクを分析する。 1) 上記で特定されたリスクが実際に生じた場合に起こり得る結果について評価する 2) 上記で特定されたリスクの現実的な起こりやすさについて評価する - リスク基準を参照し、リスクのレベルを決定し、優先順位付けする ・組織は，セキュリティリスクアセスメントのプロセスを文書化し、保管する。 ・組織は、システムにセキュリティインシデントが発生した際に想定される被害の大きさやセキュリティインシデントが発生する蓋然性（例：インターネットにつながっているか）、リスクアセスメント実施に係る工数等の観点を考慮し、システムを優先順位化してリスクアセスメントの頻度等を設定することが望ましい。 [参考] セキュリティリスクアセスメントの手法として、「資産ベース」の手法及び「事業被害ベース」の手法があることが知られている。資産ベースの手法でリスクアセスメントを実施する場合は「中小企業の情報セキュリティガイドライン 第3版」（IPA, 2019年）や「制御システムのセキュリティリスク分析ガイド 第2版」(IPA, 2018年) 等を、事業被害ベースの手法を実施する場合は「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)等を参照することができる。
	3.12.4	システムの境界、システムの運用環境、セキュリティ要件の実装方法、及び他のシステムとの関係または他のシステムへのコネクションについて記述した、システムセキュリティ計画を策定、文書、及び定期的に更新する。	・CA-2 セキュリティア評価 ・CA-5 行動計画とマイルストン ・CA-7 継続的な監視 ・PL-2 システムセキュリティ計画	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、適切に管理する。	H-Advanced	・システムは、自組織が利用している外部情報システムサービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・システムは、利用を許可していない外部情報システムサービスを検知した場合、システム管理者へ通知するメカニズムを利用する。 ・組織は、外部プロバイダによる情報システムサービスを使用する際に必要な機能、ポート、プロトコル及び他のサービスを明確にする。
						Advanced	・組織は、外部の情報システムを所有、運用する他の組織に対して、下記を許可するうえでの条件を設定する。 a. 外部の情報システムから自組織の情報システムにアクセスすること b. 外部の情報システムを使用して自組織の管理下にある情報を処理または保存もしくは伝送すること ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。
				CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	Advanced	・組織は、セキュリティリスク対応のプロセスについての文書化した情報を安全に保管する。 ・組織は、リスクアセスメントの結果に応じて対応策を選定する際、実施する対応策及び当該対応策を採用する理由を文書化することが望ましい。 ・組織は、対応策の適用等に関して、セキュリティリスク対応計画を策定し、リスク所有者の承認を得る。 ・組織は、セキュリティリスク対応計画をレビューし、当該計画が自組織全体のリスクマネジメント戦略における優先順位に適合しているかどうかを確認する。 ・CPS.RA-4で抽出した、IoT機器を含む新しいシステムにおける必要なセキュリティ対策について、然るべき外部事業者に要求仕様として伝達する。 ・組織は、IoT機器を含むシステムの導入時に、要求仕様や契約段階で定めたセキュリティ対策が実施されているかを受け入れ検査などで確認する。もし、不明な点があれば、外部事業者に確認する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
システムと通信の保護	3.13.1	外部の境界及びシステムの鍵となる内部境界における通信 (即ち、組織のシステムによって送信または受信される情報) を監視し、制御し、保護する。	・SC-7 境界保護 ・SA-8 セキュリティエンジニアリングの原則	CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	H-Advanced	・産業用制御システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・組織/情報システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い（通信）を検知できるようにする。 ・共有システム資源を介した、不正な予期せぬ情報の転送を防止する。
						Advanced	・情報システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・組織は、公開された新たな攻撃動向、マルウェア挙動情報や悪性IP アドレス／ドメイン情報などの情報（外部インテリジェンス）を収集し、必要に応じて危険性の高いIPアドレスやドメインへの通信を遮断する等の対応を実施する。
				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・制御、アクセス監視・制御を実施する。	H-Advanced	・情報システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする。 ・情報システム及び産業用制御システムは、モバイルコードの使用を管理し、監視する。 ・情報システムは、音声や映像の伝送に利用されるプロトコル（例：VoIP）の使用を管理し、監視する。
						Advanced	・組織は、産業用制御システムと情報システムとの境界において通信をモニタリングし、制御する。 ・組織は、インターネットなどの外部ネットワークと社内ネットワークの中間に内部ネットワークへのアクセスを隔離されたネットワーク上のセグメント（DMZ: 非武装地帯）を構築する。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）を必ず経由させる。 ・組織は、個々の管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・組織は、特定の送信元、あるいは多数の送信元からの大量の通信がないかをシステムの外部境界及びシステム内の主要な内部境界にてモニタリングし、必要に応じて、特定IPアドレスからの通信を遮断するなど、適切な対応を実施する。
						Basic	・組織は、情報システムの外部境界において通信をモニタリングし、制御する。
	3.13.2	組織のシステム内の有効な情報セキュリティを促進するような、アーキテクチャ設計、ソフトウェア開発手法、及びシステムエンジニアリングの原則を採用する。	・SC-7 境界保護 ・SA-8 セキュリティエンジニアリングの原則	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する。	Basic	・組織は、システムを構築するに当たり仕様書、設計、開発、導入及び変更に、システムのセキュリティエンジニアリング原則を適用する。
	3.13.3	利用者機能をシステム管理機能と分離する。	・SC-2 アプリケーションの分離	CPS.AC-5	・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H-Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・情報システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入する。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・組織は、セキュリティインシデントによる被害を最小化するため、有事においてシステム管理者の権限を利用できるユーザを最少化させることができる。 ・組織は、セキュリティインシデントによる被害を最小化するため、システム管理者であっても、サーバの重要なサービスや保護されたプロセスを停止できないようにすることができる。
						Advanced	・組織は、自組織の情報システム及び産業用制御システムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 - 一般のユーザアカウントの権限と、特権アカウントの権限を分離する （非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。） - 自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
	3.13.4	共有システム資源を介した、不正な予期せぬ情報の転送を防止する。	・SC-4 残存情報	CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	H-Advanced	・産業用制御システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・組織/情報システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い（通信）を検知できるようにする。 ・共有システム資源を介した、不正な予期せぬ情報の転送を防止する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.13.5	内部ネットワークから物理的にまたは論理的に分離される、公開アクセス可能なシステムコンポーネント用には、サブネットワークを実装する。	・SC-7 境界保護	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムを構成するネットワークの内部における境界について通信をモニタリングし、制御する。 ・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・機密性の高いデータを取り扱う自組織の情報システムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。
						Basic	・組織は、情報システム及び産業用制御システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、適切に論理的あるいは物理的にネットワークを分離することで、フローの制御を実施する。 ・組織は、産業用制御システムにおいて、制御システムのネットワークを情報システムとのネットワークから論理的あるいは物理的にセグメント化する。 [参考] 他のネットワークと物理的に離れた環境においては物理的なセグメント化を実施する、他のネットワークと物理的に近接した環境では、対策のコスト等も考慮して論理的なセグメント化を実施する等の対応が可能である。
				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・制御、アクセス監視・制御を実施する。	H-Advanced	・情報システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする。 ・情報システム及び産業用制御システムは、モバイルコードの使用を管理し、監視する。 ・情報システムは、音声や映像の伝送に利用されるプロトコル（例：VoIP）の使用を管理し、監視する。
						Advanced	・組織は、産業用制御システムと情報システムとの境界において通信をモニタリングし、制御する。 ・組織は、インターネットなどの外部ネットワークと社内ネットワークの中間に内部ネットワークへのアクセスを隔離されたネットワーク上のセグメント（DMZ: 非武装地帯）を構築する。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）を必ず経由させる。 ・組織は、個々の管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・組織は、特定の送信元、あるいは多数の送信元からの大量の通信がないかをシステムの外部境界及びシステム内の主要な内部境界にてモニタリングし、必要に応じて、特定IPアドレスからの通信を遮断するなど、適切な対応を実施する。
						Basic	・組織は、情報システムの外部境界において通信をモニタリングし、制御する。
	3.13.6	デフォルトでネットワーク通信トラフィクを拒否し、また例外によってネットワーク通信トラフィクを許可する(即ち、すべて拒否、例外で許可)。	・SC-7(5) 境界保護 デフォルトで拒否／例外で許可	CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する。
				CPS.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・制御、アクセス監視・制御を実施する。	H-Advanced	・情報システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする。 ・情報システム及び産業用制御システムは、モバイルコードの使用を管理し、監視する。 ・情報システムは、音声や映像の伝送に利用されるプロトコル（例：VoIP）の使用を管理し、監視する。
						Advanced	・組織は、産業用制御システムと情報システムとの境界において通信をモニタリングし、制御する。 ・組織は、インターネットなどの外部ネットワークと社内ネットワークの中間に内部ネットワークへのアクセスを隔離されたネットワーク上のセグメント（DMZ: 非武装地帯）を構築する。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）を必ず経由させる。 ・組織は、個々の管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・組織は、特定の送信元、あるいは多数の送信元からの大量の通信がないかをシステムの外部境界及びシステム内の主要な内部境界にてモニタリングし、必要に応じて、特定IPアドレスからの通信を遮断するなど、適切な対応を実施する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.13.7	リモートデバイスが、組織のシステムとの非リモートコネクションの確立と同時に、外部ネットワークの資源への何らかの他のコネクションを介して通信することを防止する。	・SC-7(7) 境界保護 リモートデバイスのスピリットトンネルを禁止	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムを構成するネットワークの内部における境界について通信をモニタリングし、制御する。 ・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・機密性の高いデータを取り扱う自組織の情報システムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。
	3.13.8	代替の物理的予防手段による保護がない限り、持ち出し中にCUI の不正な暴露を防止するために暗号学的メカニズムを実装する。	・SC-8 伝送する情報の完全性 ・SC-8(1) 伝送する情報の完全性 暗号学的保護または代替の物理的保護	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H-Advanced	・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・組織は、内部メモリのデータを暗号化して保管することのできるIoT機器を利用する。
						Advanced	・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されたアルゴリズムが選択可能であれば、これを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。 ・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、産業用制御システムが取り扱う重要度の高い情報（データ）を、パフォーマンスに許容できない影響が出ない範囲で適切な強度の方式で暗号化して保管する。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
	3.13.9	セション終了時または定義された非アクティブな時間の経過後に、通信セションに対応するネッ トワークコネクションを終了する。	・SC-10 ネットワークの切断	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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）を必ず経由させる。 ・個々の管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・情報システム及び産業用制御システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
	3.13.10	組織のシステムで採用された暗号のための暗号鍵を確立し、管理する。	・SC-12 暗号鍵の確立と管理	CPS.DS-5	・送受信する情報データ、保管データする情報の暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。	Advanced	・組織は、秘密鍵が危殆化した際に遅滞なく適切な対処を行うため、必要に応じて下記のような事項について方針及び手順を定めることが望ましい。 - 秘密鍵の危殆化に対応するための体制(関係者と役割、委託先との連携を含む) - 秘密鍵が危殆化した、またはその恐れがあると判断するための基準 - 秘密鍵の危殆化の原因を調べること及び原因の解消を図ること - 当該鍵を利用するサービスの利用停止 - 新しい鍵ペアを生成し、新しい鍵に対する証明書を発行すること - 秘密鍵の危殆化についての情報の開示(通知先、通知の方法、公表の方針等) [参考] 鍵管理に関するより詳細な内容については、ISO/IEC 11770規格群や、NIST SP 800-57 Part 1 Rev.4等を参照することが望ましい。
						Basic	・組織は、全ての暗号鍵を改変及び紛失から保護することが望ましい。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.13.11	CUI の機密性を保護するために使用されるとき、FIPS 認証された暗号を採用する。	・SC-13 暗号化の利用	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H-Advanced	・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・組織は、内部メモリのデータを暗号化して保管することのできるIoT機器を利用する。
						Advanced	・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されたアルゴリズムが選択可能であれば、これを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。 ・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、産業用制御システムが取り扱う重要度の高い情報（データ）を、パフォーマンスに許容できない影響が出ない範囲で適切な強度の方式で暗号化して保管する。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
	3.13.12	共同コンピューティングデバイスのリモートからの活性化を禁止し、使用中のデバイスの兆候をデバイスに存在する利用者に提供する。	・SC-15 共同コンピューティングデバイス	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。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・情報システム及び産業用制御システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・情報システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・情報システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザ及び機器による認証を暗号化とともに用いることによって保護する。 ・情報システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
	3.13.13	モバイルコードの使用を管理し監視する。	・SC-18 モバイルコード	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・制御、アクセス監視・制御を実施する。	H-Advanced	・情報システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする。 ・情報システム及び産業用制御システムは、モバイルコードの使用を管理し、監視する。 ・情報システムは、音声や映像の伝送に利用されるプロトコル（例：VoIP）の使用を管理し、監視する。
	3.13.14	VoIP 技術の使用を管理し、監視する。	・SC-19 ボイスオーバーインターネットプロトコル (VoIP)	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・制御、アクセス監視・制御を実施する。	H-Advanced	・情報システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする。 ・情報システム及び産業用制御システムは、モバイルコードの使用を管理し、監視する。 ・情報システムは、音声や映像の伝送に利用されるプロトコル（例：VoIP）の使用を管理し、監視する。
	3.13.15	通信セションの真正性を保護する。	・SC-23 セションの真正性	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。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・情報システム及び産業用制御システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・情報システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・情報システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・情報システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザ及び機器による認証を暗号化とともに用いることによって保護する。 ・情報システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H-Advanced	・組織は、情報システム及び産業用制御システムを構成する重要なデータを扱う通信路について、通信経路の暗号化を実装する又は代替の物理的な対策によって保護する。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.13.16	保存されたCUI の機密性を保護する。	・SC-28 保存情報の保護	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H-Advanced	・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・組織は、内部メモリのデータを暗号化して保管することのできるIoT機器を利用する。
						Advanced	・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されたアルゴリズムが選択可能であれば、これを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。 ・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、産業用制御システムが取り扱う重要度の高い情報（データ）を、パフォーマンスに許容できない影響が出ない範囲で適切な強度の方式で暗号化して保管する。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
システムと情報の完全性	3.14.1	タイムリーなやり方で情報及びシステムフローを識別し、報告し、訂正する。	・SI-2 欠陥の修正 ・SI-3 悪意のコード(不正プログラム) からの保護 ・SI-5 セキュリティ警報と勧告	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情報の流れを特定し、管理するプロシージャを確立し、実施する。	H-Advanced	・組織は、ネットワーク構成、機器のソフトウェア構成等の情報を自動的に収集するメカニズムを利用し、常時最新の状況をモニタリングする。 ・情報システムは、システム内（及び相互接続システム間）のデータフローを制御するために、ユーザに対して（管理者によって）承認されたアクセス権限を強制的に適用する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・組織／システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い（通信）を検知できるようにする。
	3.14.2	組織のシステム内の適切な場所で、悪意のあるコードから保護を提供する。	・SI-2 欠陥の修正 ・SI-3 悪意のコード(不正プログラム) からの保護 ・SI-5 セキュリティ警報と勧告	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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	H-Advanced	・IoT機器あるいはそうした機器を含んだシステムが、通常期待される結果とは異なる結果をもたらすような特定の攻撃（例：コマンドインジェクション）に備え、ソフトウェアプログラムまたはアプリケーションからの出力情報を検証して、期待される内容と一致しているかを確認する。 ・情報システムは、IDS/IPSによる悪質コードの検知ロジックを自動的に更新する。 ・エンドポイント（特に、多様な機能を有するIoT機器、サーバ等）において、マルウェアに対する振舞い検知型の検出・修復ソフトウェアを導入することで、未知の脆弱性を突く攻撃コードの検知を実施する。 ・情報システムは、自組織外から受信したファイルのリアルタイムスキャンを実行する。
						Advanced	・情報システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・エンドポイント（IoT機器、サーバ等）において、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。 ・特に、機能が限定されているIoT機器において、ホワイトリスト型のマルウェア対策を実施することを考慮する。 ※ 特にIoT機器や制御機器においては、マルウェア対策ソフトが利用可能なOSが使用されているとは限らないケースがある。組織は、調達時等に導入する機器がマルウェア対策ソフトに対応できるものかを確認し、対応可能なものを選定することが望ましい。マルウェア対策ソフトに対応する機器を調達することが困難な場合、ネットワーク上でマルウェアを検知する仕組みを導入・強化する等、代替的な対策を実施することが望ましい。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.14.3	システムセキュリティ警報及びアドバイザリを監視し、適切な対応アクションを取る。	・SI-2 欠陥の修正 ・SI-3 悪意のコード(不正プログラム) からの保護 ・SI-5 セキュリティ警報と勧告	CPS.IP-10	・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	Advanced	・パッチ適用中のIoT機器、サーバ等の動作により、他のソフトウェアアプリケーションやサービスの機能への影響が出るかどうかを調査やテストを通じて明らかにして、受容できるリスクを定める。 ・組織は、修正内容の有効性と副次的な悪影響の可能性についてテストを行った上で欠陥の修正を実施し、当該修正を構成管理として管理する。
				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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	H-Advanced	・IoT機器あるいはそうした機器を含んだシステムが、通常期待される結果とは異なる結果をもたらすような特定の攻撃（例：コマンドインジェクション）に備え、ソフトウェアプログラムまたはアプリケーションからの出力情報を検証して、期待される内容と一致しているかを確認する。 ・情報システムは、IDS/IPSによる悪質コードの検知ロジックを自動的に更新する。 ・エンドポイント（特に、多様な機能を有するIoT機器、サーバ等）において、マルウェアに対する振舞い検知型の検出・修復ソフトウェアを導入することで、未知の脆弱性を突く攻撃コードの検知を実施する。 ・情報システムは、自組織外から受信したファイルのリアルタイムスキャンを実行する。
						Advanced	・情報システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・エンドポイント（IoT機器、サーバ等）において、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。 ・特に、機能が限定されているIoT機器において、ホワイトリスト型のマルウェア対策を実施することを考慮する。 ※ 特にIoT機器や制御機器においては、マルウェア対策ソフトが利用可能なOSが使用されているとは限らないケースがある。組織は、調達時等に導入する機器がマルウェア対策ソフトに対応できるものかを確認し、対応可能なものを選定することが望ましい。マルウェア対策ソフトに対応する機器を調達することが困難な場合、ネットワーク上でマルウェアを検知する仕組みを導入・強化する等、代替的な対策を実施することが望ましい。
	3.14.4	新しいリリースが利用可能となったとき、悪意のあるコードからの保護メカニズムをアップデートする。	・SI-3 悪意のコード(不正プログラム) からの保護	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。	H-Advanced	・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、自動化されたメカニズムを通じて適切なパートナーと適時双方向で共有をすることができる環境を整備する。
						Advanced	・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、パートナーに適時共有することができる環境を整備する。
				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。	H-Advanced	・最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的なモニタリングに用いられている活動の修正の必要性を判断する。 ・組織は、自組織でIDS,IPS,SIEMといったセキュリティ装置等のポリシーチューニング（適用シグネチャ管理）と維持管理を行う。 ・組織は、自組織でセンサー機器でのカスタムシグネチャを脅威情報から作成する。 ・組織は、可能な場合、自組織に悪影響を及ぼす可能性の高いセキュリティ事象を適切に検知するため、 <Advanced> で提示している機器のログに加え、IoT機器等のエッジデバイスのログも収集し、分析することが望ましい。
				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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	H-Advanced	・IoT機器あるいはそうした機器を含んだシステムが、通常期待される結果とは異なる結果をもたらすような特定の攻撃（例：コマンドインジェクション）に備え、ソフトウェアプログラムまたはアプリケーションからの出力情報を検証して、期待される内容と一致しているかを確認する。 ・情報システムは、IDS/IPSによる悪質コードの検知ロジックを自動的に更新する。 ・エンドポイント（特に、多様な機能を有するIoT機器、サーバ等）において、マルウェアに対する振舞い検知型の検出・修復ソフトウェアを導入することで、未知の脆弱性を突く攻撃コードの検知を実施する。 ・情報システムは、自組織外から受信したファイルのリアルタイムスキャンを実行する。
	3.14.5	組織のシステムの定期的スキャン、及びファイルがダウンロードされ、開かれ、または実行されるような、外部情報源からのファイルのリアルタイムスキャンを実行する。	・SI-3 悪意のコード(不正プログラム) からの保護	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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	H-Advanced	・IoT機器あるいはそうした機器を含んだシステムが、通常期待される結果とは異なる結果をもたらすような特定の攻撃（例：コマンドインジェクション）に備え、ソフトウェアプログラムまたはアプリケーションからの出力情報を検証して、期待される内容と一致しているかを確認する。 ・情報システムは、IDS/IPSによる悪質コードの検知ロジックを自動的に更新する。 ・エンドポイント（特に、多様な機能を有するIoT機器、サーバ等）において、マルウェアに対する振舞い検知型の検出・修復ソフトウェアを導入することで、未知の脆弱性を突く攻撃コードの検知を実施する。 ・情報システムは、自組織外から受信したファイルのリアルタイムスキャンを実行する。
				CPS.CM-4	・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	H-Advanced	・組織は、データ入力に対する「ホワイトリスト」の概念を導入することで、インプットデータの出所を既知の信頼できるモノ、システム等と、そうしたインプットデータの許容できるフォーマットを指定する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。 ・情報システム及び産業用制御システムは、通信セッションの真正性を保護する。
						Advanced	・情報システムは、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、当該IoT機器が自組織の業務において重要なものと認められる場合、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.14.6	内向き及び外向きの通信トラフィクを含めて、攻撃や潜在的な攻撃の兆候を検知するため、組織のシステムを監視する。	・SI-4 情報システムの監視ツールと監視技法 ・SI-4(4) 情報システムの監視ツールと監視技法 内向きと外向きの通信トラフィク	CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	H-Advanced	・産業用制御システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・組織/情報システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い（通信）を検知できるようにする。 ・共有システム資源を介した、不正な予期せぬ情報の転送を防止する。
						Advanced	・情報システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・組織は、公開された新たな攻撃動向、マルウェア挙動情報や悪性IP アドレス／ドメイン情報などの情報（外部インテリジェンス）を収集し、必要に応じて危険性の高いIPアドレスやドメインへの通信を遮断する等の対応を実施する。
				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情報の流れを特定し、管理するプロシージャを確立し、実施する。	H-Advanced	・組織は、ネットワーク構成、機器のソフトウェア構成等の情報を自動的に収集するメカニズムを利用し、常時最新の状況をモニタリングする。 ・情報システムは、システム内（及び相互接続システム間）のデータフローを制御するために、ユーザに対して（管理者によって）承認されたアクセス権限を強制的に適用する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・組織／システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い（通信）を検知できるようにする。
				CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	Advanced	・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。なお、相関分析の対象には、他組織とデータを連携する部分のログも含めることが望ましい。 - モニタリングするシステムの範囲をどこまでとするか - どのような機器のログを収集し、分析するか (CPS.AE-3を参照) ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する（プロセスの内容については、CPS.RP-1等を参照）。 ・組織及びシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には以下を含むことが望ましい。 - ログ分析の分析結果（対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等） - モニタリングにおける今後の改善方針 [参考] セキュリティ対応組織(SOC/CSIRT)の業務、望まれる規模等については、「セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年)等を参照することが望ましい。
				CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	Advanced	・組織は、外部サービスプロバイダ及びシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報，業務システム及び業務プロセスの重要性並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスををモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。
				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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）を必ず経由させる。 ・個々の管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・情報システム及び産業用制御システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件		対策例
				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。	Advanced	・組織は、経営層等の組織内の然るべき要員に、定期的に組織及びシステムのセキュリティの状態を報告するプロシージャを整備し、運用する。組織は、報告の場を最新の脅威や残存するリスクに対する脅威を認識し、セキュリティを向上するための場とすることが望ましい。 ・例えば、以下のような注意喚起情報の発信があった際等に、セキュリティに係るリスク増加の兆候がある場合、信頼できる情報源からの情報に基づいて、システムのモニタリング活動のレベルを上げる。　※以下のリストは、「セキュリティ対応組織（SOC,CSIRT）強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0」(ISOG-J, 2017年)より引用している。 ・ 攻撃の特徴 攻撃の特徴 ➢ 攻撃形態、関連する通信の内容 ➢ 核心となる攻撃コード ・ 攻撃によって残る痕跡 ➢ 被害を受けた後の通信内容 ➢ サーバやクライアントに残るログ ➢ サーバやクライアントに残るその他特徴 ・ 各セキュリティ製品における検知名
	3.14.7	組織のシステムの不正な使用を識別する。	・SI-4 情報システムの監視ツールと監視技法	CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	H-Advanced	・産業用制御システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・組織/情報システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い（通信）を検知できるようにする。 ・共有システム資源を介した、不正な予期せぬ情報の転送を防止する。
						Advanced	・情報システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・組織は、公開された新たな攻撃動向、マルウェア挙動情報や悪性IP アドレス／ドメイン情報などの情報（外部インテリジェンス）を収集し、必要に応じて危険性の高いIPアドレスやドメインへの通信を遮断する等の対応を実施する。
				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情報の流れを特定し、管理するプロシージャを確立し、実施する。	H-Advanced	・組織は、ネットワーク構成、機器のソフトウェア構成等の情報を自動的に収集するメカニズムを利用し、常時最新の状況をモニタリングする。 ・情報システムは、システム内（及び相互接続システム間）のデータフローを制御するために、ユーザに対して（管理者によって）承認されたアクセス権限を強制的に適用する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・組織／システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い（通信）を検知できるようにする。
				CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	Advanced	・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。なお、相関分析の対象には、他組織とデータを連携する部分のログも含めることが望ましい。 - モニタリングするシステムの範囲をどこまでとするか - どのような機器のログを収集し、分析するか (CPS.AE-3を参照) ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する（プロセスの内容については、CPS.RP-1等を参照）。 ・組織及びシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には以下を含むことが望ましい。 - ログ分析の分析結果（対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等） - モニタリングにおける今後の改善方針 [参考] セキュリティ対応組織(SOC/CSIRT)の業務、望まれる規模等については、「セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年)等を参照することが望ましい。
				CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	Advanced	・組織は、外部サービスプロバイダ及びシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報，業務システム及び業務プロセスの重要性並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスををモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
				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）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・情報システムは、個々の外部通信サービスに対して、管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）を必ず経由させる。 ・個々の管理されたインターフェース（ゲートウェイ、ルーター、ファイアウォール等）に対して、通信制御ポリシーを定める。 ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・情報システム及び産業用制御システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
				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。	Advanced	・組織は、経営層等の組織内の然るべき要員に、定期的に組織及びシステムのセキュリティの状態を報告するプロシージャを整備し、運用する。組織は、報告の場を最新の脅威や残存するリスクに対する脅威を認識し、セキュリティを向上するための場とすることが望ましい。 ・例えば、以下のような注意喚起情報の発信があった際等に、セキュリティに係るリスク増加の兆候がある場合、信頼できる情報源からの情報に基づいて、システムのモニタリング活動のレベルを上げる。　※以下のリストは、「セキュリティ対応組織 (SOC,CSIRT) 強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0」(ISOG-J, 2017年)より引用している。 ・ 攻撃の特徴 攻撃の特徴 ➢ 攻撃形態、関連する通信の内容 ➢ 核心となる攻撃コード ・ 攻撃によって残る痕跡 ➢ 被害を受けた後の通信内容 ➢ サーバやクライアントに残るログ ➢ サーバやクライアントに残るその他特徴 ・ 各セキュリティ製品における検知名

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

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
A.5 情報セキュリティのための方針群	A.5.1 情報セキュリティのための経営陣の方向性	A.5.1.1 情報セキュリティのための方針群	情報セキュリティのための方針群は，これを定義し，管理層が承認し，発行し，従業員及び関連する外部関係者に通知しなければならない。	CPS.BE-2	・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、自組織の取引に関係する者（サプライヤー、第三者プロバイダ等を含む）に共有する。	Advanced	・組織は、組織の業務、組織の資産、個人、他の組織等にもたらされるリスクを考慮して、自組織のミッション／業務プロセスを定義し、活動に関する優先順付けを確立する。 ・組織は、自組織のセキュリティポリシーにおいて規定されている自組織と関係する他組織のセキュリティに関する役割と責任について、関係する他組織に伝達する。
				CPS.GV-1	・セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。	Advanced	・組織は、上位の方針を支えるセキュリティポリシー群のより低いレベルとして、例えば、情報システムを対象とした下記のようなトピック個別の方針及び実施手順を策定する。 a) アクセス制御及び認証 b) 物理的セキュリティ対策 c) システムの開発及び保守 d) 外部委託先管理 e) 情報分類及び取扱い ・情報システムを対象としたセキュリティポリシー群の策定に当たっては、自組織の a)事業戦略、b)関係する規制、法令及び契約、c)セキュリティの脅威環境 を十分に考慮して、自組織の実情を十分に反映したものとなるよう策定を実施する。 ・組織は、自組織の a)事業戦略、 b)関係する規制、法令及び契約、c)セキュリティの脅威環境 の変化に応じて、セキュリティ方針をレビュー、更新する。 [参考] より詳細なレベルの方針策定の際には、ISO/IEC 27002 等の関連する標準を参照して方針が必要となる分野を把握したうえで、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年) 付録5「情報セキュリティ関連規定（サンプル）」や、「情報セキュリティポリシーサンプル改版（1.0版）」(JNSA, 2016年)等を参考にすることができる。
						Basic	・組織は、自組織のセキュリティポリシー群の最も高いレベルに、セキュリティ基本方針を策定し、経営層の承認を得た後、適切な適用範囲（例：企業全体、事業部全体）で運用する。 ・組織は、自組織のセキュリティ基本方針を定期的(例えば、1年に1度)にレビュー、更新する。 [参考] セキュリティポリシーの策定に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年) 付録5「情報セキュリティ関連規定（サンプル）」における "1．組織的対策"の記載や、「情報セキュリティポリシーサンプル改版（1.0版）」(JNSA, 2016年)における "01_情報セキュリティ基本方針"、"01_情報セキュリティ方針" 等を参考とすることが可能である。
		A.5.1.2 情報セキュリティのための方針群のレビュー	情報セキュリティのための方針群は，あらかじめ定めた間隔で，又は重大な変化が発生した場合に，それが引き続き適切，妥当かつ有効であることを確実にするためにレビューしなければならない。	CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	H-Advanced	・CPS.RA-4で実施したハザード分析の結果に基づき、主に産業用制御システムに対して、必要な場合、重要なハザードにつながりうるセキュリティに係るリスク源に対して適切に対応する。 [参考] 特に安全制御系におけるセキュリティ面の統合については、近年国際標準化の場でも議論がなされており、IEC TR 63074, IEC TR 63069等を参照することが可能である。
						Advanced	・組織は、セキュリティリスク対応のプロセスについての文書化した情報を安全に保管する。 ・組織は、リスクアセスメントの結果に応じて対応策を選定する際、実施する対応策及び当該対応策を採用する理由を文書化することが望ましい。 ・組織は、対応策の適用等に関して、セキュリティリスク対応計画を策定し、リスク所有者の承認を得る。 ・組織は、セキュリティリスク対応計画をレビューし、当該計画が自組織全体のリスクマネジメント戦略における優先順位に適合しているかどうかを確認する。 ・CPS.RA-4で抽出した、IoT機器を含む新しいシステムにおける必要なセキュリティ対策について、然るべき外部事業者に要求仕様として伝達する。 ・組織は、IoT機器を含むシステムの導入時に、要求仕様や契約段階で定めたセキュリティ対策が実施されているかを受け入れ検査などで確認する。もし、不明な点があれば、外部事業者に確認する。
						Basic	・組織は、リスクアセスメントの結果を考慮して、対象とするリスクへの対応策を選定する。 ・組織は、セキュリティリスク対応の実施計画を策定する。 ・セキュリティリスクの受容について、リスク所有者の承認を得る。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
A.6 情報セキュリティのための組織	A.6.1 内部組織	A.6.1.1 情報セキュリティの役割及び責任	全ての情報セキュリティの責任を定め，割り当てなければならない。	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、適切に管理する。	H-Advanced	・システムは、自組織が利用している外部情報システムサービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・システムは、利用を許可していない外部情報システムサービスを検知した場合、システム管理者へ通知するメカニズムを利用する。 ・組織は、外部プロバイダによる情報システムサービスを使用する際に必要な機能、ポート、プロトコル及び他のサービスを明確にする。
						Advanced	・組織は、外部の情報システムを所有、運用する他の組織に対して、下記を許可するうえでの条件を設定する。 a. 外部の情報システムから自組織の情報システムにアクセスすること b. 外部の情報システムを使用して自組織の管理下にある情報を処理または保存もしくは伝送すること ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。
						Basic	・組織は、自組織が利用している外部情報システムサービスを一覧化し、それぞれのサービスにおけるユーザーとしての役割と責任を定義する。 [参考] 特にクラウドサービス利用におけるユーザー側の役割と責任を、契約において規定する際のポイントについて、「クラウドセキュリティガイドライン活用ガイドブック」(経済産業省, 2013年) Appendix A "契約の具体的な内容例と解説" を参照することが可能である。
				CPS.AM-6	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	Advanced	・組織は、情報システムや産業用制御システムにおけるリソース（データ及びデータを処理するモノ、システム等）を分類する際には、データを共有又は制限する業務上の要求及び法的要求事項を考慮する。 ・当該資産の管理責任者は、データの分類に対して責任を負う。 ・組織は、リソースの分類体系に分類の規則及びその分類を時間が経ってからレビューするための基準を含める。
						Basic	・組織は、洗い出した情報システムや産業用制御システムにおける資産を、自組織にとっての重要度に応じて優先順位づけする。 ・関係する法規制等により、自組織のリソース（例：システム、データ）について特定の分類に従うことが要求されている場合、該当する分類を資産に適用する。 ・組織は、特に産業用制御システムにおけるモノ、システム等の分類、優先付けに当たっては、自組織の事業活動の適切でない運用によりHSE(Health, Safety and Environment)への悪影響が発生するかを考慮して実施する。 ・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、事業継続の観点から重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 [参考] 資産の重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）の P.44～46に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティスク分析ガイド 第2版」（IPA, 2018年）の P.21 に記載された事業被害の大きさにおける評価を用いる方法等がある。また、特に産業用制御システムにおける資産の重要度の判断基準については、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA, 2018年）4.2.2及び4.2.3を参照することができる。
				CPS.AM-7	・自組織及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。	Advanced	・組織は、セキュリティインシデントにより損害が発生する場合に備えて、取引先等から指定されるセキュリティ対策の実装に加え、サイバー保険の利用等によるリスク移転を検討する。
						Basic	・組織は、委託先あるいは委託元との契約において、業務においてセキュリティインシデントにより損害が発生した場合の自組織と取引先の責任範囲（免責事項の明記、損害賠償額の契約金額等での上限設定等）を規定する。 ・組織は、契約において取引先に対応を求める／求められるセキュリティに関する要求事項の実効性を高めるため、要求事項への対応要否や過不足、具体的な対応方法や費用負担、対応できない場合の代替措置について契約時あるいは契約期間の初めに合意することが望ましい。 [参考] 特にクラウドサービスプロバイダーと自組織との役割と責任に関して、追加の情報を得るために、「クラウドセキュリティガイドライン活用ガイドブック 2013年度版」（経済産業省, 2013年）の "4.4.クラウドサービスの契約" を参照することが可能である。
				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。	Basic	・組織は、リスクマネジメントに係る戦略やアセスメントの結果等から、セキュリティインシデントを検知するために収集することが望ましいログ情報を決定する。 ・組織は、取引先（サービスプロバイダ）に対して、取得されるサービス利用者の活動，例外処理及びセキュリティ事象を記録した監査ログの存在を確認する。 ・組織は，サービスプロバイダにより取得される監査ログが，サービスの利用者の活動，例外処理及びセキュリティ事象を記録できており、適切な方式で保護されていることを確認する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.6.1.2 職務の分離	相反する職務及び責任範囲は，組織の資産に対する，認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために，分離なければならない。	CPS.AC-5	・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H-Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・情報システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入する。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・組織は、セキュリティインシデントによる被害を最小化するため、有事においてシステム管理者の権限を利用できるユーザを最少化させることができる。 ・組織は、セキュリティインシデントによる被害を最小化するため、システム管理者であっても、サーバの重要なサービスや保護されたプロセスを停止できないようにすることができる。
						Advanced	・組織は、自組織の情報システム及び産業用制御システムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 - 一般のユーザアカウントの権限と、特権アカウントの権限を分離する （非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。） - 自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
		A.6.1.3 関係当局との連絡	関係当局との適切な連絡体制を維持しなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	Basic	・自組織の事業活動において、セキュリティの文脈で関連するすべての法令、規制及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組みを明確に特定し、文書化する。 ・要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文書化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全ての国における遵守を考慮する。 [参考] 情報セキュリティ関連法令には、例えば、不正競争防止法、電子署名認証法、e-文書法、個人情報保護法、不正アクセス禁止法等がある。また、上記の法令等の遵守に際しては、関連各省庁から発出されているガイドライン文書等（例：不正競争防止法：「営業秘密管理指針」(経済産業省, 2019年)、「限定提供データに関する指針」(2019年, 1月)、個人情報保護法：「個人情報の保護に関する法律についてのガイドライン(通則編)」(個人情報保護委員会, 2019年)、「個人情報の保護に関する法律についてのガイドライン(匿名加工情報編)」(個人情報保護委員会, 2017年)）を参照することが望ましい。
		A.6.1.4 専門組織との連絡	情報セキュリティに関する研究会又は会議，及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持しなければならない。	CPS.RA-2	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	H-Advanced	・組織は、セキュリティ対応組織を立ち上げ、産業用制御システム、IoTシステム等も管轄に含めて、組織内で統合的にセキュリティ対策を取る体制を整える。 ・セキュリティに関わる研究会や会議等に出席したり、セキュリティの専門家による協会・団体との適切な連絡体制を維持することにより、情報システム、産業用制御システムの双方におけるセキュリティに関わる知識を最新のものとする。 ・主に自社が提供している製品・サービスにおいて、新たな脆弱性が含まれていないかを分析し、発見した場合、IPAに関連情報を届け出る。
						Advanced	・組織は、セキュリティ管理責任者を中心に、セキュリティ対応組織を立ち上げ、主に情報システムや事業における重要度の高いIoTシステムを管轄対象として、組織内でセキュリティ対策を取る体制を整える。 ・組織は、情報処理推進機構（IPA）、JPCERT/CC、業界ISACのような組織や、取引関係のある機器ベンダー、ソフトウェアベンダーより、随時脆弱性情報、脅威情報等を収集し、自組織の資産目録と照らし合わせることで、対応要否を判断する。 [参考] セキュリティ対応組織の構想、構築、運用に当たっては、外部事業者からのサービスを利用するほかに、JPCERT/CCから公開されている「CSIRTマテリアル」、日本セキュリティオペレーション事業者協議会から公開されている「セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～」等の文書を利用することが可能である。
				CPS.RA-3	・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。	H-Advanced	・組織は、セキュリティに関わる研究会や会議等に出席したり、セキュリティの専門家による協会・団体との適切な連絡体制を維持することにより、セキュリティ脅威に関わる知識を最新のものとする。 ・組織は、必要に応じて、専門家が提供するサービス等を活用し、一部の専門家しか知りえない情報を入手しそれをもとに、脅威を特定する。
				CPS.AE-4	・関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。	Advanced	・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、共有することによって、当該セキュリティ事象の全容を把握する。 ・セキュリティ事象発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を外部のセキュリティベンダー等に依頼する。
				CPS.AN-1	・セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。	Advanced	・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、共有することによって、当該セキュリティインシデントの全容を把握する。 ・セキュリティインシデント発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を外部のセキュリティベンダー等に依頼する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ	プロジェクトの種類にかかわらず，プロジェクトマネジメントにおいては，情報セキュリティに取り組まなければならない。	CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。	H-Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 -セキュリティ機能に関する要求事項 -セキュリティ強度に関する要求事項 -セキュリティ保証に関する要求事項 -セキュリティ関連のドキュメントに関する要求事項 -セキュリティ関連のドキュメントの保護に関する要求事項 -そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 -受け入れ基準
						Advanced	・組織は、 情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
	A.6.2 モバイル機器及びテレワーキング	A.6.2.1 モバイル機器の方針	モバイル機器を用いることによって生じるリスクを管理するために，方針及びその方針を支援するセキュリティ対策を採用しなければならない。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システムを構成する資産（IoT機器等を含むハードウェア、ソフトウェア、情報）を一意に特定し、各々の資産に管理責任者を割り当てた上で、資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、定期的又はオペレータ等の求めに応じて、リアルタイムで状況を把握しながら目録を維持・管理する。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・情報システム及び産業用制御システムは、許可されていない資産を自動的に検出し、管理情報から外す・システムから切り離す等を実行するメカニズムを導入、運用している。 ※ 関連する対策要件に、CPS.CM-6がある。 [参考] 重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）のP.44～P.46 に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティスク分析ガイド 第2版」（IPA, 2018年）のP.21に記載された事業被害の大きさにおける評価を用いる方法等がある
						Advanced	・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						Basic	・組織は、自組織の情報システムや産業用制御システムを構成する資産（ハードウェア、ソフトウェア、情報）を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・資産は保有するものすべてを一覧化することが望ましいが、対象が膨大な場合、分析対象の統合（グループ化）と分析対象からの除外を通じて、対象とする資産を絞り込むことを検討する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録（情報資産管理台帳）の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年)のP47を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。
				CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	H-Advanced	・システムは、自組織が利用している外部情報システムサービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・システムは、利用を許可していない外部情報システムサービスを検知した場合、システム管理者へ通知するメカニズムを利用する。 ・組織は、外部プロバイダによる情報システムサービスを使用する際に必要な機能、ポート、プロトコル及び他のサービスを明確にする。
						Advanced	・組織は、外部の情報システムを所有、運用する他の組織に対して、下記を許可するうえでの条件を設定する。 a. 外部の情報システムから自組織の情報システムにアクセスすること b. 外部の情報システムを使用して自組織の管理下にある情報を処理または保存もしくは伝送すること ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。
				CPS.AC-3	・無線接続先（ユーザーやIoT機器、サーバ等）を正しく認証する。	Advanced	・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・組織は、自組織で利用する携帯機器から自組織のシステムの接続に関する承認ルール等を定める。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システム上で実行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）を用いてソフトウェアの制限を実施する、あるいは、許可されていないソフトウェアのインストールを不可とする。
						Advanced	・組織は、自組織の情報システム及び産業用制御システム上でのユーザによるソフトウェアのインストールについて管理するメカニズムを導入し、管理する。
						Basic	・組織は、自組織の情報システム及び産業用制御システム上でのユーザによるソフトウェアのインストールに関するポリシーを確立し、ユーザに遵守させる。
				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及び記録、監視を実施する。	Advanced	・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア（執務室等）において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。
						Basic	・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来客に付き添うなどして人手による代替的な対策を実施する。 ・施設内の、一般の人がアクセスできない指定エリアに対するアクセスを制御するための、入退室管理対策を実施する。 ・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入退室時のログを保持する。
				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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	Advanced	・情報システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・エンドポイント（IoT機器、サーバ等）において、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。 ・特に、機能が限定されているIoT機器において、ホワイトリスト型のマルウェア対策を実施することを考慮する。 ※ 特にIoT機器や制御機器においては、マルウェア対策ソフトが利用可能なOSが使用されているとは限らないケースがある。組織は、調達時等に導入する機器がマルウェア対策ソフトに対応できるものかを確認し、対応可能なものを選定することが望ましい。マルウェア対策ソフトに対応する機器を調達することが困難な場合、ネットワーク上でマルウェアを検知する仕組みを導入・強化する等、代替的な対策を実施することが望ましい。
		A.6.2.2 テレワーキング	テレワーキングの場所でアクセス，処理及び保存される情報を保護するために，方針及びその方針を支援するセキュリティ対策を実施しなければならない。	CPS.AC-3	・無線接続先（ユーザーやIoT機器、サーバ等）を正しく認証する。	Advanced	・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・組織は、自組織で利用する携帯機器から自組織のシステムの接続に関する承認ルール等を定める。
						Basic	・組織は、許可しているリモートアクセスのタイプごとに使用制限・構成要件・実装ガイダンス等を定める。 ・組織は、許可されていない無線接続を原則禁止とする。 ・組織は、自組織の情報システム及び産業用制御システムへのリモートアクセスの利用に関する承認ルール等を定める。 ・組織は、自組織のシステムへの無線によるアクセスを許可するのに先立って、無線でシステムにアクセスする権限を与える。
				CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H-Advanced	・組織は、情報システム及び産業用制御システムを構成する重要なデータを扱う通信路について、通信経路の暗号化を実装する又は代替の物理的な対策によって保護する。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	Advanced	・情報システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・エンドポイント（IoT機器、サーバ等）において、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。 ・特に、機能が限定されているIoT機器において、ホワイトリスト型のマルウェア対策を実施することを考慮する。 ※ 特にIoT機器や制御機器においては、マルウェア対策ソフトが利用可能なOSが使用されているとは限らないケースがある。組織は、調達時等に導入する機器がマルウェア対策ソフトに対応できるものかを確認し、対応可能なものを選定することが望ましい。マルウェア対策ソフトに対応する機器を調達することが困難な場合、ネットワーク上でマルウェアを検知する仕組みを導入・強化する等、代替的な対策を実施することが望ましい。
A.7 人的資源のセキュリティ	A.7.1 雇用前	A.7.1.1 選考	全ての従業員候補者についての経歴などの確認は，関連する法令，規制及び倫理に従って行わなければならない。また，この確認は，事業上の要求事項，アクセスされる情報の分類及び認識されたリスクに応じて行わなければならない。	CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する。
				CPS.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）を含める。	Advanced	・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。 ・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。 ・組織は、機密情報を扱う要員に対しては特に、採用から退職に至るまでのサイクル全体に渡り、セキュリティ上の責任に対処する。
						Basic	・組織は、雇用条件においてセキュリティに係る要員の責任について明記する。雇用終了後の情報漏えい等を抑止するため、この責任は、雇用終了後の妥当な期間に渡って持続するよう記載する。 ・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。 ・組織は、要員の退職時に以下を実施する。 -自組織のシステムに対するアクセスを一定期間内に無効にする。 -職員に関連する認証及びクレデンシャルを無効にする。 -セキュリティに関連するシステム関連の所有物をすべて回収する。 -退職する個人が管理していた組織の情報と情報システムに対するアクセスを保持する。
		A.7.1.2 雇用条件	従業員及び契約相手との雇用契約書には，情報セキュリティに関する各自の責任及び組織の責任を記載しなければならない。	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）を含める。	Advanced	・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。 ・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。 ・組織は、機密情報を扱う要員に対しては特に、採用から退職に至るまでのサイクル全体に渡り、セキュリティ上の責任に対処する。
						Basic	・組織は、雇用条件においてセキュリティに係る要員の責任について明記する。雇用終了後の情報漏えい等を抑止するため、この責任は、雇用終了後の妥当な期間に渡って持続するよう記載する。 ・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。 ・組織は、要員の退職時に以下を実施する。 -自組織のシステムに対するアクセスを一定期間内に無効にする。 -職員に関連する認証及びクレデンシャルを無効にする。 -セキュリティに関連するシステム関連の所有物をすべて回収する。 -退職する個人が管理していた組織の情報と情報システムに対するアクセスを保持する。

ISO/IEC 27001:2013 附属書A			サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID		要求事項	対策要件ID	対策要件	対策例	
A.7.2 雇用期間中	A.7.2.1 経営陣の責任	経営陣は，組織の確立された方針及び手順に従った情報セキュリティの適用を，全ての従業員及び契約相手に要求しなければならない。	CPS.AT-1	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	H-Advanced	・組織は、内部不正の兆候を認識・報告するためのセキュリティ意識向上トレーニングを、全要員に対して実施する。
					Advanced	・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。組織は、CPS.AT-1＜Basic＞の[参考]に記載されている一般的な事項を解説しているコンテンツに加えて、組織によって内容が異なる内容として、例えば、下記の事項を扱うことができる。 - 不審なメールを受信した際の対応手順（どこにどのような内容を連絡すればよいか） - モバイル端末利用の注意点（例：公衆無線LANに接続する際の注意点） - SNSを利用する際の注意点 ・組織は、情報セキュリティ要員の育成とレベル向上のための役割別（例：システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者）のプログラムを作成し、定期的に該当する要員に対して実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の記録を定期的にレビューする。
					Basic	・組織は、自組織の利用する情報システム及び産業用制御システムに対する変更により必要になった場合や新規職員に対して基本的なセキュリティ意識向上トレーニングを実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の内容や結果等について記録し、管理する。 [参考] 組織が従業員等に対してセキュリティ教育を実施する際、IPAが公開している「情報セキュリティ読本 教育用プレゼン資料」の内容を参照することが可能である。
			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）を含める。	Advanced	・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。 ・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。 ・組織は、機密情報を扱う要員に対しては特に、採用から退職に至るまでのサイクル全体に渡り、セキュリティ上の責任に対処する。
					Basic	・組織は、雇用条件においてセキュリティに係る要員の責任について明記する。雇用終了後の情報漏えい等を抑止するため、この責任は、雇用終了後の妥当な期間に渡って持続するよう記載する。 ・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。 ・組織は、要員の退職時に以下を実施する。 -自組織のシステムに対するアクセスを一定期間内に無効にする。 -職員に関連する認証及びクレデンシャルを無効にする。 -セキュリティに関連するシステム関連の所有物をすべて回収する。 -退職する個人が管理していた組織の情報と情報システムに対するアクセスを保持する。
	A.7.2.2 情報セキュリティの意識向上，教育及び訓練	組織の全ての従業員，及び関係する場合には契約相手は，職務に関連する組織の方針及び手順についての，適切な，意識向上のための教育及び訓練を受けなければならず，また，定めに従ってその更新を受けなければならない。	CPS.AT-1	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	H-Advanced	・組織は、内部不正の兆候を認識・報告するためのセキュリティ意識向上トレーニングを、全要員に対して実施する。
					Advanced	・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。組織は、CPS.AT-1＜Basic＞の[参考]に記載されている一般的な事項を解説しているコンテンツに加えて、組織によって内容が異なる内容として、例えば、下記の事項を扱うことができる。 - 不審なメールを受信した際の対応手順（どこにどのような内容を連絡すればよいか） - モバイル端末利用の注意点（例：公衆無線LANに接続する際の注意点） - SNSを利用する際の注意点 ・組織は、情報セキュリティ要員の育成とレベル向上のための役割別（例：システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者）のプログラムを作成し、定期的に該当する要員に対して実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の記録を定期的にレビューする。
					Basic	・組織は、自組織の利用する情報システム及び産業用制御システムに対する変更により必要になった場合や新規職員に対して基本的なセキュリティ意識向上トレーニングを実施する。 ・組織は、自組織の要員に対するセキュリティに係る教育・訓練の内容や結果等について記録し、管理する。 [参考] 組織が従業員等に対してセキュリティ教育を実施する際、IPAが公開している「情報セキュリティ読本 教育用プレゼン資料」の内容を参照することが可能である。
	A.7.2.3 懲戒手続	情報セキュリティ違反を犯した従業員に対して処置をとるための，正式かつ周知された懲戒手続を備えなければならない。	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）を含める。	Advanced	・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。 ・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。 ・組織は、機密情報を扱う要員に対しては特に、採用から退職に至るまでのサイクル全体に渡り、セキュリティ上の責任に対処する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
	A.7.3 雇用の終了及び変更	A.7.3.1 雇用の終了又は変更に関する責任	雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め，その従業員又は契約相手に伝達し，かつ，遂行させなければならない。	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）を含める。	Advanced	・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。 ・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。 ・組織は、機密情報を扱う要員に対しては特に、採用から退職に至るまでのサイクル全体に渡り、セキュリティ上の責任に対処する。
A.8 資産の管理	A.8.1 資産に対する責任	A.8.1.1 資産目録	情報及び情報処理施設に関連する資産を特定しなければならない。また，これらの資産の目録を，作成し，維持しなければならない。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システムを構成する資産（IoT機器等を含むハードウェア、ソフトウェア、情報）を一意に特定し、各々の資産に管理責任者を割り当てた上で、資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、定期的又はオペレータ等の求めに応じて、リアルタイムで状況を把握しながら目録を維持・管理する。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・情報システム及び産業用制御システムは、許可されていない資産を自動的に検出し、管理情報から外す・システムから切り離す等を実行するメカニズムを導入、運用している。 ※ 関連する対策要件に、CPS.CM-6がある。 [参考] 重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）のP.44～P.46 に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティスク分析ガイド 第2版」（IPA, 2018年）のP.21に記載された事業被害の大きさにおける評価を用いる方法等がある
						Advanced	・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						Basic	・組織は、自組織の情報システムや産業用制御システムを構成する資産（ハードウェア、ソフトウェア、情報）を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・資産は保有するものすべてを一覧化することが望ましいが、対象が膨大な場合、分析対象の統合（グループ化）と分析対象からの除外を通じて、対象とする資産を絞り込むことを検討する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録（情報資産管理台帳）の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年)のP47を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.8.1.2 資産の管理責任 a)	目録の中で維持される資産は，管理されなければならない。 注a) 6.1.2及び 6.1.3 では，情報セキュリティのリスクを運用管理することについて，責任及び権限をもつ人又は主体をリスク所有者としている。情報セキュリティにおいて，多くの場合，資産の管理責任を負う者は，リスク所有者でもある。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システムを構成する資産（IoT機器等を含むハードウェア、ソフトウェア、情報）を一意に特定し、各々の資産に管理責任者を割り当てた上で、資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、定期的又はオペレータ等の求めに応じて、リアルタイムで状況を把握しながら目録を維持・管理する。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・情報システム及び産業用制御システムは、許可されていない資産を自動的に検出し、管理情報から外す・システムから切り離す等を実行するメカニズムを導入、運用している。 ※ 関連する対策要件に、CPS.CM-6がある。 [参考] 重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）のP.44～P.46 に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティスク分析ガイド 第2版」（IPA, 2018年）のP.21に記載された事業被害の大きさにおける評価を用いる方法等がある
						Advanced	・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
						Basic	・組織は、自組織の情報システムや産業用制御システムを構成する資産（ハードウェア、ソフトウェア、情報）を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・資産は保有するものすべてを一覧化することが望ましいが、対象が膨大な場合、分析対象の統合（グループ化）と分析対象からの除外を通じて、対象とする資産を絞り込むことを検討する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録（情報資産管理台帳）の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年)のP47を参照することが可能である。また、対象の絞込みに関するより詳細な説明は、「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)における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。
		A.8.1.3 資産利用の許容範囲	情報の利用の許容範囲，並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施しなければならない。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システムを構成する資産（IoT機器等を含むハードウェア、ソフトウェア、情報）を一意に特定し、各々の資産に管理責任者を割り当てた上で、資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、定期的又はオペレータ等の求めに応じて、リアルタイムで状況を把握しながら目録を維持・管理する。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・情報システム及び産業用制御システムは、許可されていない資産を自動的に検出し、管理情報から外す・システムから切り離す等を実行するメカニズムを導入、運用している。 ※ 関連する対策要件に、CPS.CM-6がある。 [参考] 重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）のP.44～P.46 に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティスク分析ガイド 第2版」（IPA, 2018年）のP.21に記載された事業被害の大きさにおける評価を用いる方法等がある
						Advanced	・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
	A.8.1.4 資産の返却		全ての従業員及び外部の利用者は，雇用，契約又は合意の終了時に，自らが所持する組織の資産の全てを返却しなければならない。	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）を含める。	Advanced	・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。 ・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。 ・組織は、機密情報を扱う要員に対しては特に、採用から退職に至るまでのサイクル全体に渡り、セキュリティ上の責任に対処する。
						Basic	・組織は、雇用条件においてセキュリティに係る要員の責任について明記する。雇用終了後の情報漏えい等を抑止するため、この責任は、雇用終了後の妥当な期間に渡って持続するよう記載する。 ・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。 ・組織は、要員の退職時に以下を実施する。 -自組織のシステムに対するアクセスを一定期間内に無効にする。 -職員に関連する認証及びクレデンシャルを無効にする。 -セキュリティに関連するシステム関連の所有物をすべて回収する。 -退職する個人が管理していた組織の情報と情報システムに対するアクセスを保持する。
	A.8.2 情報分類	A.8.2.1 情報の分類	情報は，法的要求事項，価値，重要性，及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から，分類しなければならない。	CPS.AM-6	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	Advanced	・組織は、情報システムや産業用制御システムにおけるリソース（データ及びデータを処理するモノ、システム等）を分類する際には、データを共有又は制限する業務上の要求及び法的要求事項を考慮する。 ・当該資産の管理責任者は、データの分類に対して責任を負う。 ・組織は、リソースの分類体系に分類の規則及びその分類を時間が経ってからレビューするための基準を含める。
						Basic	・組織は、洗い出した情報システムや産業用制御システムにおける資産を、自組織にとっての重要度に応じて優先順位づけする。 ・関係する法規制等により、自組織のリソース（例：システム、データ）について特定の分類に従うことが要求されている場合、該当する分類を資産に適用する。 ・組織は、特に産業用制御システムにおけるモノ、システム等の分類、優先付けに当たっては、自組織の事業活動の適切でない運用によりHSE(Health, Safety and Environment)への悪影響が発生するかを考慮して実施する。 ・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、事業継続の観点から重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 [参考] 資産の重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）の P.44～46に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティスク分析ガイド 第2版」（IPA, 2018年）の P.21 に記載された事業被害の大きさにおける評価を用いる方法等がある。また、特に産業用制御システムにおける資産の重要度の判断基準については、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA, 2018年）4.2.2及び4.2.3を参照することができる。
				CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)
		A.8.2.2 情報のラベル付け	情報のラベル付けに関する適切な一連の手順は，組織が採用した情報分類体系に従って策定し，実施しなければならない。	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または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	H-Advanced	・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
						Advanced	・組織は、システム、モノ等によって提供される機能とサービスをレビューし、削除の候補となる機能とサービスを特定する。 ・組織は、禁止されている機能、ポート、プロトコル、サービスの使用を検知し防止するために、ネットワークスキャンツール、侵入検知防止システム、エンドポイントプロテクション（ファイアウォール、ホストベースの侵入検知システム等）を活用する。 ・組織は、IoT機器やPC、サーバ以外の機器であっても、複合機等のネットワークにつながる機器に対しては、不要な機能やサービス等を停止する。
						Basic	・使用するUSBメモリ等の周辺機器は、管理台帳を作成し、保管場所を施錠して管理する。 ・IoT機器、サーバ等に接続するUSBメモリ等の外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能なUSBメモリを用いる等の対策を行う。 ・使用しないUSBポート、シリアルポートは栓をするなど物理的に閉塞する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.8.2.3 資産の取扱い	資産の取扱いに関する手順は，組織が採用した情報分類体系に従って策定し，実施しなければならない。	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
				CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H-Advanced	・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・組織は、内部メモリのデータを暗号化して保管することのできるIoT機器を利用する。
						Advanced	・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されたアルゴリズムが選択可能であれば、これを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。 ・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、産業用制御システムが取り扱う重要度の高い情報（データ）を、パフォーマンスに許容できない影響が出ない範囲で適切な強度の方式で暗号化して保管する。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
						Basic	・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報システムが取り扱う重要度の高い情報（データ）を適切な強度の方式で暗号化して保管する。
				CPS.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ID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする。	H-Advanced	・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
	A.8.3 媒体の取扱い	A.8.3.1 取外し可能な媒体の管理	組織が採用した分類体系に従って，取外し可能な媒体の管理のための手順を実施しなければならない。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システムを構成する資産（IoT機器等を含むハードウェア、ソフトウェア、情報）を一意に特定し、各々の資産に管理責任者を割り当てた上で、資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、定期的又はオペレータ等の求めに応じて、リアルタイムで状況を把握しながら目録を維持・管理する。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・情報システム及び産業用制御システムは、許可されていない資産を自動的に検出し、管理情報から外す・システムから切り離す等を実行するメカニズムを導入、運用している。 ※ 関連する対策要件に、CPS.CM-6がある。 [参考] 重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）のP.44～P.46 に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティスク分析ガイド 第2版」（IPA, 2018年）のP.21に記載された事業被害の大きさにおける評価を用いる方法等がある
						Advanced	・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
				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ID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする。	H-Advanced	・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。
						Advanced	・組織は、自組織のIoT機器やサーバ等を廃棄するプロシージャを定め、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。
						Basic	・組織は、自組織のIoT機器やサーバ等を廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態にする。
				CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	H-Advanced	・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
						Advanced	・組織は、システム、モノ等によって提供される機能とサービスをレビューし、削除の候補となる機能とサービスを特定する。 ・組織は、禁止されている機能、ポート、プロトコル、サービスの使用を検知し防止するために、ネットワークスキャンツール、侵入検知防止システム、エンドポイントプロテクション（ファイアウォール、ホストベースの侵入検知システム等）を活用する。 ・組織は、IoT機器やPC、サーバ以外の機器であっても、複合機等のネットワークにつながる機器に対しては、不要な機能やサービス等を停止する。
						Basic	・使用するUSBメモリ等の周辺機器は、管理台帳を作成し、保管場所を施錠して管理する。 ・IoT機器、サーバ等に接続するUSBメモリ等の外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能なUSBメモリを用いる等の対策を行う。 ・使用しないUSBポート、シリアルポートは栓をするなど物理的に閉塞する。
		A.8.3.2 媒体の処分	媒体が不要になった場合は，正式な手順を用いて，セキュリティを保って処分しなければならない。	CPS.IP-6	・IoT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする。	H-Advanced	・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。
						Advanced	・組織は、自組織のIoT機器やサーバ等を廃棄するプロシージャを定め、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。
						Basic	・組織は、自組織のIoT機器やサーバ等を廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態にする。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.8.3.3 物理的媒体の輸送	情報を格納した媒体は，輸送の途中における，認可されていないアクセス，不正使用又は破損から保護しなければならない。	CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	H-Advanced	・調達する機器に対して、契約におけるセキュリティ要求事項が満たせているかを、自組織あるいは第三者がテストする。 ・組織は、自組織のオペレーションにとって特に重要な機器について、再委託先以降の組織を含む関係するサプライチェーン全体に渡り、一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロシージャで製造されたものかを確認する。
						Advanced	・組織は、契約において、例えば下記のように、取引先から調達する製品・サービスが具備すべきセキュリティ要求事項を明確化する。 - セキュリティに関わる特定の認証（例：ISMS認証、ISASecure EDSA認証、ITセキュリティ評価及び認証制度(JISEC)）を有していること - ベンダー自身により、セキュリティに関わる特定の認証の基準に適合する対策を実施していることが確認されていること - リスク分析の結果等から導かれた必要なセキュリティ要件を設計時からの実装（セキュリティ・バイ・デザイン）し、検査していること ・組織は、調達計画時に、製品またはサービス自体、あるいは当該製品・サービスの調達・供給にて使用される資産の保護に係るセキュリティ要件の費用を確保しておくことが望ましい。 ・下記を含む製品またはサービスの調達または供給を評価するためのセキュリティ測定ルールを策定し、運用及び改善する。 - 測定対象の内容 - 措置の報告方法、報告の頻度 - 措置が実施されない場合に遂行される措置 ・組織は、搬送中の改ざん・漏えいを検知(又は抑止)する手段とともに納品されるIoT機器やソフトウェアが、不正操作されていないかを確認する。 - 物品：セキュリティ便、プロテクトシール等 - 電送：暗号化、電送データ全体のハッシュ値等
A.9 アクセス制御	A.9.1 アクセス制御に対する業務上の要求事項	A.9.1.1 アクセス制御方針	アクセス制御方針は，業務及び情報セキュリティの要求事項に基づいて確立し，文書化し，レビューしなければならない。	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システムにおけるアカウントの管理について、例えば以下のような自動化されたメカニズムを導入し、運用する。 - 管理対象となるシステムからアカウント情報を定期的に自動収集する - 特権アカウントのパスワードを自動で変更する ・産業用制御システムは、統合されたアカウント管理をサポートする。 ・情報システムは、自組織のシステムの一時利用アカウントや緊急アカウント、利用されていないアカウントについて、一定期間の経過後又は申請時利用期限終了後に自動的に無効にする。 ・情報システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化及び無効化について自動的に監査・報告する。
						Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・共有ユーザアカウントに関しては、認証情報を知りえるユーザを一覧等で管理し、アカウントを利用する範囲を特定可能にする。 ・組織は、情報システムにおけるシステムアカウントの利用状況をモニタリングする。 ・組織は、アカウントが不要にな-った場合や変更が必要となった場合には管理責任者に通知する。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・組織は、情報システム及び産業用制御システムにおいてパスワードが変更された場合、ユーザー（または管理責任者）に通知する。 ・情報システムは、クレデンシャルを忘れてしまった際等にクレデンシャルを再設定する場合、悪意ある者によるクレデンシャルの不正な変更を防ぐため、当該アカウントが自身のものかどうかを確認するための安全な手順を適用する。
						Basic	・組織は、自組織の情報システム及び産業用制御システムのアカウントを管理する管理責任者を配置する。 ・組織は、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別（例：一般ユーザ／システム管理者／共有ユーザ／一時的なユーザ）を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・組織は、自組織の情報システム及び産業用制御システムに対するクレデンシャル（例：パスワード、セキュリティキー）のポリシーを定め、そのポリシーを満たすクレデンシャルでなければ設定できない機能を実装する。ポリシーの内容の例としては、下記が挙げられる。 - クレデンシャルに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいクレデンシャルが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたクレデンシャルのみを保存・伝送する。 - 同じクレデンシャルを組織が定めた世代にわたって再利用するのを禁止する。 ・クレデンシャルを忘れてしまった際等に、強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なクレデンシャルを使用することを許可する。 ・組織は、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.9.1.2 ネットワーク及びネットワークサービスへのアクセスだけを，利用者に提供しなければならない。	利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを，利用者に提供しなければならない。	CPS.AC-6	・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織の情報システムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、対象システムにおける特権アカウントへの不正ログインのリスク等を勘案し、十分に信頼性の高い認証方式を実装できない場合、ネットワーク経由での特権アカウントへのログインを原則禁止する。 ・情報システムは、自組織のシステムについて管理者アカウントの無効化等制限が実施できない場合には、特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を要求する。 ・情報システムにおけるデフォルトの管理者アカウントは、原則無効化する。 ・情報システムは、権限付与等の特権操作を実施する場合には、利用ユーザアカウントに対して必要最小限の特権操作権限を付与する。
	A.9.2 利用者アクセスの管理	A.9.2.1 利用者登録及び登録削除	アクセス権の割当てを可能にするために，利用者の登録及び登録削除についての正式なプロセスを実施しなければならない。	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システムにおけるアカウントの管理について、例えば以下のような自動化されたメカニズムを導入し、運用する。 - 管理対象となるシステムからアカウント情報を定期的に自動収集する - 特権アカウントのパスワードを自動で変更する ・産業用制御システムは、統合されたアカウント管理をサポートする。 ・情報システムは、自組織のシステムの一時利用アカウントや緊急アカウント、利用されていないアカウントについて、一定期間の経過後又は申請時利用期限終了後に自動的に無効にする。 ・情報システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化及び無効化について自動的に監査・報告する。
						Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・共有ユーザアカウントに関しては、認証情報を知りえるユーザを一覧等で管理し、アカウントを利用する範囲を特定可能にする。 ・組織は、情報システムにおけるシステムアカウントの利用状況をモニタリングする。 ・組織は、アカウントが不要にな-った場合や変更が必要となった場合には管理責任者に通知する。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・組織は、情報システム及び産業用制御システムにおいてパスワードが変更された場合、ユーザー（または管理責任者）に通知する。 ・情報システムは、クレデンシャルを忘れてしまった際等にクレデンシャルを再設定する場合、悪意ある者によるクレデンシャルの不正な変更を防ぐため、当該アカウントが自身のものかどうかを確認するための安全な手順を適用する。
						Basic	・組織は、自組織の情報システム及び産業用制御システムのアカウントを管理する管理責任者を配置する。 ・組織は、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別（例：一般ユーザ／システム管理者／共有ユーザ／一時的なユーザ）を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・組織は、自組織の情報システム及び産業用制御システムに対するクレデンシャル（例：パスワード、セキュリティキー）のポリシーを定め、そのポリシーを満たすクレデンシャルでなければ設定できない機能を実装する。ポリシーの内容の例としては、下記が挙げられる。 - クレデンシャルに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいクレデンシャルが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたクレデンシャルのみを保存・伝送する。 - 同じクレデンシャルを組織が定めた世代にわたって再利用するのを禁止する。 ・クレデンシャルを忘れてしまった際等に、強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なクレデンシャルを使用することを許可する。 ・組織は、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。
				CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・IoT機器での通信は、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。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.9.2.2 利用者アクセスの提供（provisioning）	全ての種類の利用者について，全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために，利用者アクセスの提供についての正式なプロセスを実施しなければならない。	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システムにおけるアカウントの管理について、例えば以下のような自動化されたメカニズムを導入し、運用する。 - 管理対象となるシステムからアカウント情報を定期的に自動収集する - 特権アカウントのパスワードを自動で変更する ・産業用制御システムは、統合されたアカウント管理をサポートする。 ・情報システムは、自組織のシステムの一時利用アカウントや緊急アカウント、利用されていないアカウントについて、一定期間の経過後又は申請時利用期限終了後に自動的に無効にする。 ・情報システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化及び無効化について自動的に監査・報告する。
						Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・共有ユーザアカウントに関しては、認証情報を知りえるユーザを一覧等で管理し、アカウントを利用する範囲を特定可能にする。 ・組織は、情報システムにおけるシステムアカウントの利用状況をモニタリングする。 ・組織は、アカウントが不要にな-った場合や変更が必要となった場合には管理責任者に通知する。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・組織は、情報システム及び産業用制御システムにおいてパスワードが変更された場合、ユーザー（または管理責任者）に通知する。 ・情報システムは、クレデンシャルを忘れてしまった際等にクレデンシャルを再設定する場合、悪意ある者によるクレデンシャルの不正な変更を防ぐため、当該アカウントが自身のものかどうかを確認するための安全な手順を適用する。
						Basic	・組織は、自組織の情報システム及び産業用制御システムのアカウントを管理する管理責任者を配置する。 ・組織は、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別（例：一般ユーザ／システム管理者／共有ユーザ／一時的なユーザ）を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・組織は、自組織の情報システム及び産業用制御システムに対するクレデンシャル（例：パスワード、セキュリティキー）のポリシーを定め、そのポリシーを満たすクレデンシャルでなければ設定できない機能を実装する。ポリシーの内容の例としては、下記が挙げられる。 - クレデンシャルに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいクレデンシャルが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたクレデンシャルのみを保存・伝送する。 - 同じクレデンシャルを組織が定めた世代にわたって再利用するのを禁止する。 ・クレデンシャルを忘れてしまった際等に、強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なクレデンシャルを使用することを許可する。 ・組織は、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。
		A.9.2.3 特権的アクセス権の管理	特権的アクセス権の割当て及び利用は，制限し，管理しなければならない。	CPS.AC-5	・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H-Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・情報システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入する。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・組織は、セキュリティインシデントによる被害を最小化するため、有事においてシステム管理者の権限を利用できるユーザを最少化させることができる。 ・組織は、セキュリティインシデントによる被害を最小化するため、システム管理者であっても、サーバの重要なサービスや保護されたプロセスを停止できないようにすることができる。
						Advanced	・組織は、自組織の情報システム及び産業用制御システムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 - 一般のユーザアカウントの権限と、特権アカウントの権限を分離する (非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。) - 自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				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、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織の情報システムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、対象システムにおける特権アカウントへの不正ログインのリスク等を勘案し、十分に信頼性の高い認証方式を実装できない場合、ネットワーク経由での特権アカウントへのログインを原則禁止する。 ・情報システムは、自組織のシステムについて管理者アカウントの無効化等制限が実施できない場合には、特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を要求する。 ・情報システムにおけるデフォルトの管理者アカウントは、原則無効化する。 ・情報システムは、権限付与等の特権操作を実施する場合には、利用ユーザアカウントに対して必要最小限の特権操作権限を付与する。
		A.9.2.4 利用者の秘密認証情報の管理	秘密認証情報の割当ては，正式な管理プロセスによって管理しなければならない。	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システムにおけるアカウントの管理について、例えば以下のような自動化されたメカニズムを導入し、運用する。 - 管理対象となるシステムからアカウント情報を定期的に自動収集する - 特権アカウントのパスワードを自動で変更する ・産業用制御システムは、統合されたアカウント管理をサポートする。 ・情報システムは、自組織のシステムの一時利用アカウントや緊急アカウント、利用されていないアカウントについて、一定期間の経過後又は申請時利用期限終了後に自動的に無効にする。 ・情報システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化及び無効化について自動的に監査・報告する。
						Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・共有ユーザアカウントに関しては、認証情報を知りえるユーザを一覧等で管理し、アカウントを利用する範囲を特定可能にする。 ・組織は、情報システムにおけるシステムアカウントの利用状況をモニタリングする。 ・組織は、アカウントが不要にな-った場合や変更が必要となった場合には管理責任者に通知する。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・組織は、情報システム及び産業用制御システムにおいてパスワードが変更された場合、ユーザー（または管理責任者）に通知する。 ・情報システムは、クレデンシャルを忘れてしまった際等にクレデンシャルを再設定する場合、悪意ある者によるクレデンシャルの不正な変更を防ぐため、当該アカウントが自身のものかどうかを確認するための安全な手順を適用する。
		A.9.2.5 利用者アクセス権のレビュー	資産の管理責任者は，利用者のアクセス権を定められた間隔でレビューしなければならない。	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システムにおけるアカウントの管理について、例えば以下のような自動化されたメカニズムを導入し、運用する。 - 管理対象となるシステムからアカウント情報を定期的に自動収集する - 特権アカウントのパスワードを自動で変更する ・産業用制御システムは、統合されたアカウント管理をサポートする。 ・情報システムは、自組織のシステムの一時利用アカウントや緊急アカウント、利用されていないアカウントについて、一定期間の経過後又は申請時利用期限終了後に自動的に無効にする。 ・情報システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化及び無効化について自動的に監査・報告する。
						Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・共有ユーザアカウントに関しては、認証情報を知りえるユーザを一覧等で管理し、アカウントを利用する範囲を特定可能にする。 ・組織は、情報システムにおけるシステムアカウントの利用状況をモニタリングする。 ・組織は、アカウントが不要にな-った場合や変更が必要となった場合には管理責任者に通知する。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・組織は、情報システム及び産業用制御システムにおいてパスワードが変更された場合、ユーザー（または管理責任者）に通知する。 ・情報システムは、クレデンシャルを忘れてしまった際等にクレデンシャルを再設定する場合、悪意ある者によるクレデンシャルの不正な変更を防ぐため、当該アカウントが自身のものかどうかを確認するための安全な手順を適用する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
	A.9.2.6 アクセス権の削除又は修正		全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は，雇用，契約又は合意の終了時に削除しなければならず，また，変更に合わせて修正しなければならない。	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システムにおけるアカウントの管理について、例えば以下のような自動化されたメカニズムを導入し、運用する。 - 管理対象となるシステムからアカウント情報を定期的に自動収集する - 特権アカウントのパスワードを自動で変更する ・産業用制御システムは、統合されたアカウント管理をサポートする。 ・情報システムは、自組織のシステムの一時利用アカウントや緊急アカウント、利用されていないアカウントについて、一定期間の経過後又は申請時利用期限終了後に自動的に無効にする。 ・情報システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化及び無効化について自動的に監査・報告する。
						Advanced	・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 ・共有ユーザアカウントに関しては、認証情報を知りえるユーザを一覧等で管理し、アカウントを利用する範囲を特定可能にする。 ・組織は、情報システムにおけるシステムアカウントの利用状況をモニタリングする。 ・組織は、アカウントが不要にな-った場合や変更が必要となった場合には管理責任者に通知する。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。 ・組織は、情報システム及び産業用制御システムにおいてパスワードが変更された場合、ユーザー（または管理責任者）に通知する。 ・情報システムは、クレデンシャルを忘れてしまった際等にクレデンシャルを再設定する場合、悪意ある者によるクレデンシャルの不正な変更を防ぐため、当該アカウントが自身のものかどうかを確認するための安全な手順を適用する。
						Basic	・組織は、自組織の情報システム及び産業用制御システムのアカウントを管理する管理責任者を配置する。 ・組織は、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別（例：一般ユーザ／システム管理者／共有ユーザ／一時的なユーザ）を識別・選択する。 ・組織は、事前に定められたプロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。 ・組織は、自組織の情報システム及び産業用制御システムに対するクレデンシャル（例：パスワード、セキュリティキー）のポリシーを定め、そのポリシーを満たすクレデンシャルでなければ設定できない機能を実装する。ポリシーの内容の例としては、下記が挙げられる。 - クレデンシャルに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいクレデンシャルが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたクレデンシャルのみを保存・伝送する。 - 同じクレデンシャルを組織が定めた世代にわたって再利用するのを禁止する。 ・クレデンシャルを忘れてしまった際等に、強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なクレデンシャルを使用することを許可する。 ・組織は、複数のユーザが単一のグループとして機能する場合を除き、情報システム及び産業用制御システムにおいてユーザ識別情報を、複数のシステムユーザで共有しない。
				CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。
						Advanced	・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。
						Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設においてセキュリティを保つべき物理的セキュリティ境界を定め、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に応じてアクセス制御を実施する。 ・組織は、物理的セキュリティ境界内における自組織または自組織外の一時的に認可された入場者に対して、認可された関係者の付き添い又は監視カメラ等により作業内容をモニタリングできるようにする。
	A.9.3 利用者の責任	A.9.3.1 秘密認証情報の利用	秘密認証情報の利用時に，組織の慣行に従うことを，利用者に要求しなければならない。	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。	H-Advanced	・情報システム及び産業用制御システム（対応の即時性が求められる一部の例を除く）は、自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定し、上限以上失敗した場合には管理者が解除しなければ再ログインできない機能を実装する。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定し、上限以上失敗した場合には一定期間再ログインできない機能を実装する。 ・情報システム及び産業用制御システムは、組織が定める時間を越えてシステムの無操作が持続する場合、手動又は自動でセッションロックを実施する。 ※ 産業用制御システムにおいて、緊急時対応においてオペレータの即時対応が求められるようなセッションを実施するケースが想定される場合、セッションロックを実施しないことが望ましい。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
				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。	Basic	・組織は、自組織の運用に適合する最も制限された設定基準を定めた上で、導入されるIoT機器、サーバ等の初期設定手順及び設定内容を文書化するとともに、その文書に従って設定を実施する。 ・組織は、IoT機器を設置する前にデフォルトの初期設定値を確認し、CPS.AC-1で定めたポリシーに準じていない場合に適切なものへと変更する。 ・組織は、IoT機器の導入前に、搭載されているソフトウェアを確認し、記録する。
	A.9.4 システム及びアプリケーションのアクセス制御	A.9.4.1 情報へのアクセス制限	情報及びアプリケーションシステム機能へのアクセスは，アクセス制御方針に従って，制限しなければならない。	CPS.AC-5	・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H-Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・情報システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入する。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・組織は、セキュリティインシデントによる被害を最小化するため、有事においてシステム管理者の権限を利用できるユーザを最少化させることができる。 ・組織は、セキュリティインシデントによる被害を最小化するため、システム管理者であっても、サーバの重要なサービスや保護されたプロセスを停止できないようにすることができる。
						Advanced	・組織は、自組織の情報システム及び産業用制御システムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 - 一般のユーザアカウントの権限と、特権アカウントの権限を分離する （非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。） - 自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
				CPS.AC-6	・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織の情報システムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、対象システムにおける特権アカウントへの不正ログインのリスク等を勘案し、十分に信頼性の高い認証方式を実装できない場合、ネットワーク経由での特権アカウントへのログインを原則禁止する。 ・情報システムは、自組織のシステムについて管理者アカウントの無効化等制限が実施できない場合には、特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を要求する。 ・情報システムにおけるデフォルトの管理者アカウントは、原則無効化する。 ・情報システムは、権限付与等の特権操作を実施する場合には、利用ユーザアカウントに対して必要最小限の特権操作権限を付与する。
		A.9.4.2 セキュリティに配慮したログオン手順	アクセス制御方針で求められている場合には，システム及びアプリケーションへのアクセスは，セキュリティに配慮したログオン手順によって制御しなければならない。	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。	H-Advanced	・情報システム及び産業用制御システム（対応の即時性が求められる一部の例を除く）は、自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定し、上限以上失敗した場合には管理者が解除しなければ再ログインできない機能を実装する。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定し、上限以上失敗した場合には一定期間再ログインできない機能を実装する。 ・情報システム及び産業用制御システムは、組織が定める時間を越えてシステムの無操作が持続する場合、手動又は自動でセッションロックを実施する。 ※ 産業用制御システムにおいて、緊急時対応においてオペレータの即時対応が求められるようなセッションを実施するケースが想定される場合、セッションロックを実施しないことが望ましい。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.9.4.3 パスワード管理システム	パスワード管理システムは，対話式でなければならず，また，良質なパスワードを確実とするものでなければならない。	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
		A.9.4.4 特権的なユーティリティプログラムの使用	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は，制限し，厳しく管理しなければならない。	CPS.AC-5	・職務及び責任範囲（例：ユーザー／システム管理者)を適切に分離する 。	H-Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・情報システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入する。 ・情報システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 ・組織は、セキュリティインシデントによる被害を最小化するため、有事においてシステム管理者の権限を利用できるユーザを最少化させることができる。 ・組織は、セキュリティインシデントによる被害を最小化するため、システム管理者であっても、サーバの重要なサービスや保護されたプロセスを停止できないようにすることができる。
						Advanced	・組織は、自組織の情報システム及び産業用制御システムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 - 一般のユーザアカウントの権限と、特権アカウントの権限を分離する (非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。) - 自らの担当外の職務に対する権限を最小とする ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
				CPS.AC-6	・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織の情報システムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、対象システムにおける特権アカウントへの不正ログインのリスク等を勘案し、十分に信頼性の高い認証方式を実装できない場合、ネットワーク経由での特権アカウントへのログインを原則禁止する。 ・情報システムは、自組織のシステムについて管理者アカウントの無効化等制限が実施できない場合には、特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を要求する。 ・情報システムにおけるデフォルトの管理者アカウントは、原則無効化する。 ・情報システムは、権限付与等の特権操作を実施する場合には、利用ユーザアカウントに対して必要最小限の特権操作権限を付与する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.9.4.5 プログラムソースコードへのアクセス制御	プログラムソースコードへのアクセスは，制限しなければならない。	CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
A.10 暗号	A.10.1 暗号による管理策	A.10.1.1 暗号による管理策の利用方針	情報を保護するための暗号による管理策の利用に関する方針は，策定し，実施しなければならない。	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	H-Advanced	・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 ・組織は、内部メモリのデータを暗号化して保管することのできるIoT機器を利用する。
						Advanced	・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されたアルゴリズムが選択可能であれば、これを選択し、情報（データ）を適切な強度の方式で暗号化して保管する。 ・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、産業用制御システムが取り扱う重要度の高い情報（データ）を、パフォーマンスに許容できない影響が出ない範囲で適切な強度の方式で暗号化して保管する。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H-Advanced	・組織は、情報システム及び産業用制御システムを構成する重要なデータを扱う通信路について、通信経路の暗号化を実装する又は代替の物理的な対策によって保護する。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。
				CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。	H-Advanced	・システム/IoT機器は、少ないリソースでも可用性を損なわずに実装可能な暗号モジュールを導入し、リソースは制限されているが重要度の高い機器からの通信データを適切な強度で暗号化することが望ましい。 ・情報システムは、重要度の高い・低いに限らず、組織外部へ送信するすべてのデータを適切な強度で暗号化する。
						Advanced	・組織は、機密性の高い情報を外部の組織等へ送信する際、情報を適切な強度の方式で暗号化する。
		A.10.1.2 鍵管理	暗号鍵の利用，保護及び有効期間（lifetime）に関する方針を策定し，そのライフサイクル全体にわたって実施しなければならない。	CPS.DS-5	・送受信する情報データ、保管データする情報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。	H-Advanced	・組織は、ユーザが暗号鍵を紛失した場合に、鍵の再発行等により情報の可用性を維持する。 ・秘密鍵及びプライベート鍵をセキュリティを保って管理することに加え，公開鍵の真正性についても考慮することが望ましい。この認証プロセスは，認証局によって通常発行される公開鍵証明書を用いて実施される。この認証局は，要求された信頼度を提供するために適切な管理策及び手順を備えている，認知された組織であることが望ましい。
						Advanced	・組織は、秘密鍵が危殆化した際に遅滞なく適切な対処を行うため、必要に応じて下記のような事項について方針及び手順を定めることが望ましい。 - 秘密鍵の危殆化に対応するための体制(関係者と役割、委託先との連携を含む) - 秘密鍵が危殆化した、またはその恐れがあると判断するための基準 - 秘密鍵の危殆化の原因を調べること及び原因の解消を図ること - 当該鍵を利用するサービスの利用停止 - 新しい鍵ペアを生成し、新しい鍵に対する証明書を発行すること - 秘密鍵の危殆化についての情報の開示(通知先、通知の方法、公表の方針等) [参考] 鍵管理に関するより詳細な内容については、ISO/IEC 11770規格群や、NIST SP 800-57 Part 1 Rev.4等を参照することが望ましい。
						Basic	・組織は、全ての暗号鍵を改変及び紛失から保護することが望ましい。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.DS-8	・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。	H-Advanced	・組織は、保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用した機器を調達する。 ・組織は、情報システム及び産業用制御システム内で使用されている暗号技術向けの暗号鍵を保管するにあたり耐タンパーデバイスを用いて管理する。
A.11 物理的及び環境的セキュリティ	A.11.1 セキュリティを保つべき領域	A.11.1.1 物理的セキュリティ境界	取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために，物理的セキュリティ境界を定め，かつ，用いなければならない。	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。
						Advanced	・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。
				CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	H-Advanced	・組織は、特に重要な資産を管理している範囲内での重要資産の位置や移動を追跡し、モニタリングする。
						Advanced	・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア（執務室等）において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。
						Basic	・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来客に付き添うなどして人手による代替的な対策を実施する。 ・施設内の、一般の人がアクセスできない指定エリアに対するアクセスを制御するための、入退室管理対策を実施する。 ・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入退室時のログを保持する。
		A.11.1.2 物理的入退管理策	セキュリティを保つべき領域は，認可された者だけにアクセスを許すことを確実にするために，適切な入退管理策によって保護しなければならない。	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。
						Advanced	・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。
						Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設においてセキュリティを保つべき物理的セキュリティ境界を定め、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に応じてアクセス制御を実施する。 ・組織は、物理的セキュリティ境界内における自組織または自組織外の一時的に認可された入場者に対して、認可された関係者の付き添い又は監視カメラ等により作業内容をモニタリングできるようにする。
				CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	H-Advanced	・組織は、特に重要な資産を管理している範囲内での重要資産の位置や移動を追跡し、モニタリングする。
						Advanced	・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア（執務室等）において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。
						Basic	・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来客に付き添うなどして人手による代替的な対策を実施する。 ・施設内の、一般の人がアクセスできない指定エリアに対するアクセスを制御するための、入退室管理対策を実施する。 ・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入退室時のログを保持する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件		対策例
		A.11.1.3 オフィス，部屋及び施設のセキュリティ	オフィス，部屋及び施設に対する物理的セキュリティを設計し，適用しなければならない。	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。
						Advanced	・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。
						Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設においてセキュリティを保つべき物理的セキュリティ境界を定め、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に応じてアクセス制御を実施する。 ・組織は、物理的セキュリティ境界内における自組織または自組織外の一時的に認可された入場者に対して、認可された関係者の付き添い又は監視カメラ等により作業内容をモニタリングできるようにする。
				CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	H-Advanced	・組織は、特に重要な資産を管理している範囲内での重要資産の位置や移動を追跡し、モニタリングする。
						Advanced	・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア（執務室等）において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。
						Basic	・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来客に付き添うなどして人手による代替的な対策を実施する。 ・施設内の、一般の人がアクセスできない指定エリアに対するアクセスを制御するための、入退室管理対策を実施する。 ・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入退室時のログを保持する。
		A.11.1.4 外部及び環境の脅威からの保護	自然災害，悪意のある攻撃又は事故に対する物理的な保護を設計し，適用しなければならない。	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。
				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。	H-Advanced	・組織は、自組織の利用するシステムが設置されている施設に職員が常駐しない場合には、自動消火機能を導入する。
						Advanced	・組織は、無停電電源装置等により自組織のIoT機器、サーバ等が設置されているエリア内の機器の安定な稼働を維持する。 ・組織は、独立した電源等により稼働する消火及び火災検知のための装置やシステムを導入し、維持する。 ・組織は、閉止弁や遮断弁を用意し、自組織のIoT機器、サーバ等が設置されているエリアを水漏れ等の被害から保護する。
						Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定めた許容レベルに保つ仕組みを導入する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定期的にモニタリングする。
		A.11.1.5 セキュリティを保つべき領域での作業	セキュリティを保つべき領域での作業に関する手順を設計し，適用しなければならない。	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。	H-Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。
						Advanced	・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。
		A.11.1.6 受渡場所	荷物の受渡場所などの立寄り場所，及び認可されていない者が施設に立ち入ることもあるその他の場所は，管理しなければならない。また，可能な場合には，認可されていないアクセスを避けるために，それらの場所を情報処理施設から離さなければならない。	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。
						Advanced	・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。
						Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設においてセキュリティを保つべき物理的セキュリティ境界を定め、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に応じてアクセス制御を実施する。 ・組織は、物理的セキュリティ境界内における自組織または自組織外の一時的に認可された入場者に対して、認可された関係者の付き添い又は監視カメラ等により作業内容をモニタリングできるようにする。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件		対策例
	A.11.2 装置	A.11.2.1 装置の設置及び保護	装置は，環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し，保護しなければならない。	CPS.IP-5	・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	H-Advanced	・組織は、自組織の利用するシステムが設置されている施設に職員が常駐しない場合には、自動消火機能を導入する。
						Advanced	・組織は、無停電電源装置等により自組織のIoT機器、サーバ等が設置されている エリア内の機器の安定な稼働を維持する。 ・組織は、独立した電源等により稼働する消火及び火災検知のための装置やシステムを導入し、維持する。 ・組織は、閉止弁や遮断弁を用意し、自組織のIoT機器、サーバ等が設置されているエリアを水漏れ等の被害から保護する。
						Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定めた許容レベルに保つ仕組みを導入する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定期的にモニタリングする。
		A.11.2.2 サポートユーティリティ	装置は，サポートユーティリティの不具合による，停電，その他の故障から保護しなければならない。	CPS.BE-3	・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。	H-Advanced	・組織は、自らの事業を継続する上で、自組織が有する下記のサポートユーティリティの果たす機能及び依存関係を特定する。 - 通信サービス - 電力設備（電力ケーブル等を含む） ・上記で識別されたユーティリティの内、事業継続という観点から重要な役割を果たすものについて、下記のような対策を講ずることを検討する。 - 代替通信サービスの確立 - 情報システム及び産業用制御システムの電力設備及び電力ケーブルの物理的保護 - 短期無停電電源装置の準備 ・特に、代替通信サービスの利用を検討する際、下記について考慮する - 通信サービス事業者との契約事項を検討する際、組織の可用性に関する要求事項（目標復旧時間を含む）を明確にする - 一次通信サービスとの間で単一障害点が共有される可能性を低減する
				CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	Advanced	・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。
						Basic	・組織は、情報システム及び産業用制御システムに要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 ・組織は、サポートユーティリティの不具合による停電、その他の故障から装置を保護する。 ・組織は、データを伝送する又はサービスをサポートする通信ケーブル及び電源ケーブルの配線を傍受、妨害又は損傷から保護する。 ・組織は、可用性及び完全性を継続的に維持することを確実にするために、装置を正しく保守する。
				CPS.IP-5	・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	H-Advanced	・組織は、自組織の利用するシステムが設置されている施設に職員が常駐しない場合には、自動消火機能を導入する。
						Advanced	・組織は、無停電電源装置等により自組織のIoT機器、サーバ等が設置されている エリア内の機器の安定な稼働を維持する。 ・組織は、独立した電源等により稼働する消火及び火災検知のための装置やシステムを導入し、維持する。 ・組織は、閉止弁や遮断弁を用意し、自組織のIoT機器、サーバ等が設置されているエリアを水漏れ等の被害から保護する。
						Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定めた許容レベルに保つ仕組みを導入する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定期的にモニタリングする。
		A.11.2.3 ケーブル配線のセキュリティ	データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受，妨害又は損傷から保護しなければならない。	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。
				CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	Advanced	・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。
						Basic	・組織は、情報システム及び産業用制御システムに要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 ・組織は、サポートユーティリティの不具合による停電、その他の故障から装置を保護する。 ・組織は、データを伝送する又はサービスをサポートする通信ケーブル及び電源ケーブルの配線を傍受、妨害又は損傷から保護する。 ・組織は、可用性及び完全性を継続的に維持することを確実にするために、装置を正しく保守する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.11.2.4 装置の保守	装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守しなければならない。	CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	Advanced	・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。
						Basic	・組織は、情報システム及び産業用制御システムに要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 ・組織は、サポートユーティリティの不具合による停電、その他の故障から装置を保護する。 ・組織は、データを伝送する又はサービスをサポートする通信ケーブル及び電源ケーブルの配線を傍受、妨害又は損傷から保護する。 ・組織は、可用性及び完全性を継続的に維持することを確実にするために、装置を正しく保守する。
				CPS.MA-1	・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 ・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な変更または不正な変更がないか確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。
						Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
				CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	Advanced	・組織は、遠隔保守のための接続の確立と実施に関するポリシーとプロシージャを文書化し、その内容により実施する。 ・組織は、遠隔保守を実施する際には組織の定めるネットワークアクセスに求める認証を実施するとともに、遠隔保守が完了したらセッションとネットワーク接続を確実に終了する。
						Basic	・組織は、遠隔保守の実施に当たっては、実施計画を策定し・合意した上で実施し、実施結果を確認する。 ・組織は、実施した遠隔保守の実施記録を保管する。
		A.11.2.5 資産の移動	装置，情報又はソフトウェアは，事前の認可なしでは，構外に持ち出してはならない。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	Advanced	・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
				CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	H-Advanced	・組織は、特に重要な資産を管理している範囲内での重要資産の位置や移動を追跡し、モニタリングする。
		A.11.2.6 構外にある装置及び資産のセキュリティ	構外にある資産に対しては，構外での作業に伴った，構内での作業とは異なるリスクを考慮に入れて，セキュリティを適用しなければならない。	CPS.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及び記録、監視を実施する。	Advanced	・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア（執務室等）において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.11.2.7 装置のセキュリティを保った処分又は再利用	記憶媒体を内蔵した全ての装置は，処分又は再利用する前に，全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること，又はセキュリティを保って上書きしていることを確実にするために，検証しなければなら	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ID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする。	H-Advanced	・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。
						Advanced	・組織は、自組織のIoT機器やサーバ等を廃棄するプロシージャを定め、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。
						Basic	・組織は、自組織のIoT機器やサーバ等を廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態にする。
		A.11.2.8 無人状態にある利用者装置	利用者は，無人状態にある装置が適切な保護対策を備えていることを確実にしなければならない。	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。
						Advanced	・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。
						Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設においてセキュリティを保つべき物理的セキュリティ境界を定め、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に応じてアクセス制御を実施する。 ・組織は、物理的セキュリティ境界内における自組織または自組織外の一時的に認可された入場者に対して、認可された関係者の付き添い又は監視カメラ等により作業内容をモニタリングできるようにする。
		A.11.2.9 クリアデスク・クリアスクリーン方針	書類及び取外し可能な記憶媒体に対するクリアデスク方針，並びに情報処理設備に対するクリアスクリーン方針を適用しなければならない。	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。	H-Advanced	・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。 ・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。 ・組織は、自組織の物理セキュリティ境界に対する物理的な侵入について警報と監視装置（例：監視カメラ）をモニタリングする。
						Advanced	・組織は、自組織の物理セキュリティ境界に対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織の物理セキュリティ境界内に対する入場者のアクセス記録を、一定期間保管し、定期的にレビューを実施する。
						Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設においてセキュリティを保つべき物理的セキュリティ境界を定め、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に応じてアクセス制御を実施する。 ・組織は、物理的セキュリティ境界内における自組織または自組織外の一時的に認可された入場者に対して、認可された関係者の付き添い又は監視カメラ等により作業内容をモニタリングできるようにする。
A.12 運用のセキュリティ	A.12.1 運用の手順及び責任	A.12.1.1 操作手順書	操作手順は，文書化し，必要とする全ての利用者に対して利用可能にしなければならない。	CPS.GV-1	・セキュリティポリシーを策定し、自組織及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。	H-Advanced	・従来のIT環境において運用されているものと基本的な方針を共有しつつ、産業用制御システム等、IoT機器が設置されるサイトの性質等を十分に考慮したセキュリティポリシー群、運用手順を策定する。 [参考] 例えば、産業用制御システム(ICS)を対象としたセキュリティマネジメント規格であるIEC 62443-2-1では、ICS環境のための上位レベルのサイバーセキュリティポリシーの策定を求めている。特に、産業分野におけるセキュリティポリシー及び運用手順の策定にあたっては、「制御システムセキュリティ運用ガイドライン」（日本電気制御機器工業会, 2017年）等を参考とすることができる。
						Advanced	・組織は、上位の方針を支えるセキュリティポリシー群のより低いレベルとして、例えば、情報システムを対象とした下記のようなトピック個別の方針及び実施手順を策定する。 a) アクセス制御及び認証 b) 物理的セキュリティ対策 c) システムの開発及び保守 d) 外部委託先管理 e) 情報分類及び取扱い ・情報システムを対象としたセキュリティポリシー群の策定に当たっては、自組織の a)事業戦略、b)関係する規制、法令及び契約、c)セキュリティの脅威環境 を十分に考慮して、自組織の実情を十分に反映したものとなるよう策定を実施する。 ・組織は、自組織の a)事業戦略、 b)関係する規制、法令及び契約、c)セキュリティの脅威環境 の変化に応じて、セキュリティ方針をレビュー、更新する。 [参考] より詳細なレベルの方針策定の際には、ISO/IEC 27002 等の関連する標準を参照して方針が必要となる分野を把握したうえで、「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年) 付録5「情報セキュリティ関連規定（サンプル）」や、「情報セキュリティポリシーサンプル改版（1.0版）」(JNSA, 2016年)等を参考にすることができる。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件		対策例
		A.12.1.2 変更管理	情報セキュリティに影響を与える，組織，業務プロセス，情報処理設備及びシステムの変更は，管理しなければならない。	CPS.IP-1	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	H-Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対して変更を実施する前に、それらの変更をテスト・承認・文書化する。 ・組織は、IoT機器、サーバ等の設定を一つの場所から管理・適用・検証するための自動化されたメカニズムを使用する。 ・組織は、特に産業用制御システムにおけるセキュリティに係る変更管理手順を、既存のプロセス安全管理の手順に統合する。
						Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法（例：変更実施前に本人にしかわからないセキュリティコードを入力させる）を利用する。 ・組織は、セキュリティ上の変更によって情報システム及び産業用制御システムの可用性や安全性等に悪影響が及ばないことを確実にするため、運用及び変更管理のポリシー及び手順を定期的にレビューする。
						Basic	・組織は、自組織の運用に適合する最も制限された設定基準を定めた上で、導入されるIoT機器、サーバ等の初期設定手順及び設定内容を文書化するとともに、その文書に従って設定を実施する。 ・組織は、IoT機器を設置する前にデフォルトの初期設定値を確認し、CPS.AC-1で定めたポリシーに準じていない場合に適切なものへと変更する。 ・組織は、IoT機器の導入前に、搭載されているソフトウェアを確認し、記録する。
		A.12.1.3 容量・能力の管理	要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整しなければならず，また，将来必要とする容量・能力を予測しなければならない。	CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する。	Advanced	・情報システム及び産業用制御システムは、予備の容量／帯域幅／その他の予備リソース（ヒト／モノ／システム等）を管理して、大量の情報を送りつけるタイプのサービス拒否攻撃による影響を最小限に抑える。例えば、攻撃を受けているシステムが提供するサービスを、可用性の水準維持等の理由により停止できない場合、重要な機能を継続するため、以下のような対策をとる必要がある。 - 待機している予備システムへの自動的、あるいは、人手を介した移行 - ネットワークアクセスからの攻撃を受けたシステム構成要素の、自動的あるいは人手を介した隔離 ・要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整しなければならず，また，将来必要とする容量・能力を予測しなければならない。 ・組織は、 (a) 情報システムに対するサービス妨害攻撃の兆候を発見するための組織が定めた、モニタリングツールを使用する (b) 組織が定めた情報システム及び産業用制御システムのリソースをモニタリングして、効果的なサービス妨害攻撃を阻止するための十分なリソースが確保されているかどうかを判断する
				CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	Advanced	・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。
						Basic	・組織は、情報システム及び産業用制御システムに要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 ・組織は、サポートユーティリティの不具合による停電、その他の故障から装置を保護する。 ・組織は、データを伝送する又はサービスをサポートする通信ケーブル及び電源ケーブルの配線を傍受、妨害又は損傷から保護する。 ・組織は、可用性及び完全性を継続的に維持することを確実にするために、装置を正しく保守する。
		A.12.1.4 開発環境，試験環境及び運用環境の分離	開発環境，試験環境及び運用環境は，運用環境への認可されていないアクセス又は変更によるリスクを低減するために，分離しなければならない。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムを構成するネットワークの内部における境界について通信をモニタリングし、制御する。 ・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・機密性の高いデータを取り扱う自組織の情報システムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界（産業用制御システムの場合は情報システムとの境界）について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。
						Basic	・組織は、情報システム及び産業用制御システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、適切に論理的あるいは物理的にネットワークを分離することで、フローの制御を実施する。 ・組織は、産業用制御システムにおいて、制御システムのネットワークを情報システムとのネットワークから論理的あるいは物理的にセグメント化する。 [参考] 他のネットワークと物理的に離れた環境においては物理的なセグメント化を実施する、他のネットワークと物理的に近接した環境では、対策のコスト等も考慮して論理的なセグメント化を実施する等の対応が可能である。

ISO/IEC 27001:2013 附属書A			サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID		要求事項	対策要件ID	対策要件	対策例	
A.12.2 マルウェアからの保護	A.12.2.1 マルウェアに対する管理策	マルウェアから保護するために，利用者に適切に認識させることと併せて，検出，予防及び回復のための管理策を実施しなければならない。	CPS.DS-10	・IoT機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。	H-Advanced	・組織は、情報システムにおいて完全性検証時に不一致が発見された場合にシステム管理者に通知する、自動化されたツールを使用する。 ・組織は、不正なソフトウェアが検知された場合に、対象ソフトウェアの起動を防止するツールを使用する。 ・組織は、設定の不正な変更や、システム権限の不正な昇格等の、セキュリティ関連の変更が不正に行われた場合の検知能力を、組織のインシデント対応能力に組み入れる。
					Advanced	・情報システムは、ソフトウェア・ファームウェアの完全性チェックを定期的に実施する。 ・情報システム及び産業用制御システムは、起動を許可するソフトウェアを事前に登録しておくことで、登録されていないソフトウェアの起動を停止する。
			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が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	H-Advanced	・IoT機器あるいはそうした機器を含んだシステムが、通常期待される結果とは異なる結果をもたらすような特定の攻撃（例：コマンドインジェクション）に備え、ソフトウェアプログラムまたはアプリケーションからの出力情報を検証して、期待される内容と一致しているかを確認する。 ・情報システムは、IDS/IPSによる悪質コードの検知ロジックを自動的に更新する。 ・エンドポイント（特に、多様な機能を有するIoT機器、サーバ等）において、マルウェアに対する振舞い検知型の検出・修復ソフトウェアを導入することで、未知の脆弱性を突く攻撃コードの検知を実施する。 ・情報システムは、自組織外から受信したファイルのリアルタイムスキャンを実行する。
					Advanced	・情報システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・エンドポイント（IoT機器、サーバ等）において、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。 ・特に、機能が限定されているIoT機器において、ホワイトリスト型のマルウェア対策を実施することを考慮する。 ※ 特にIoT機器や制御機器においては、マルウェア対策ソフトが利用可能なOSが使用されているとは限らないケースがある。組織は、調達時等に導入する機器がマルウェア対策ソフトに対応できるものかを確認し、対応可能なものを選定することが望ましい。マルウェア対策ソフトに対応する機器を調達することが困難な場合、ネットワーク上でマルウェアを検知する仕組みを導入・強化する等、代替的な対策を実施することが望ましい。
A.12.3 バックアップ	A.12.3.1 情報のバックアップ	情報，ソフトウェア及びシステムイメージのバックアップは，合意されたバックアップ方針に従って定期的に取得し，検査しなければならない。	CPS.BE-3	・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。	H-Advanced	・組織は、自らの事業を継続する上で、自組織が有する下記のサポートユーティリティの果たす機能及び依存関係を特定する。 - 通信サービス - 電力設備（電力ケーブル等を含む） ・上記で識別されたユーティリティの内、事業継続という観点から重要な役割を果たすものについて、下記のような対策を講ずることを検討する。 - 代替通信サービスの確立 - 情報システム及び産業用制御システムの電力設備及び電力ケーブルの物理的保護 - 短期無停電電源装置の準備 ・特に、代替通信サービスの利用を検討する際、下記について考慮する - 通信サービス事業者との契約事項を検討する際、組織の可用性に関する要求事項（目標復旧時間を含む）を明確にする - 一次通信サービスとの間で単一障害点が共有される可能性を低減する
					Advanced	・CPS.AM-6で規定した当該システムの可用性に対する要求水準に応じて、その容量・能力に関する要求事項を特定する。 ・自組織が利用する情報システム及び産業用制御システムが、要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。
			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、テストする。	H-Advanced	・組織は、バックアップ情報を定期的にテストして、媒体の信頼性と情報の完全性を確認する。
					Advanced	・組織は、自組織のシステムドキュメントのバックアップを定めたタイミングや頻度で実施する。 ・組織は、保管拠点におけるバックアップ情報の機密性・完全性・可用性を保護する。
					Basic	・組織は、自組織の情報システム及び産業用制御システムに含まれるユーザレベル・システムレベルの情報のバックアップを定めたタイミングや頻度で実施する。
A.12.4 ログ取得及び監視	A.12.4.1 イベントログ取得	利用者の活動，例外処理，過失及び情報セキュリティ事象を記録したイベントログを取得し，保持し，定期的にレビューしなければならない。	CPS.SC-8	・自組織が関係する他組織及び個人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。	H-Advanced	・組織は、取引先、第三者的な監査機関等の関係する他組織からのリアルタイムでのニーズに柔軟に応じるため、下記の特徴を有した証跡保管システムを利用する。 - 対象となる監査証跡の契約事項に対する適格性を高速で検証することができる - 取引先や委託を受けた監査機関等の許可を受けたエンティティのみがアクセスできる - 保管されているデータが、タイムスタンプや電子署名により証跡としての信頼性を有している
					Advanced	・組織は、システムによって生成された監査記録のうち長期にわたって取得する監査記録を確実に取得できるよう、対策を実施する。 ・システムは、監査記録を次の脅威から保護するため、粒度の高いアクセス制御等を監査記録を保存するモノ、システムに適用することが望ましい。 - 記録されたメッセージ形式の変更 - ログファイルの変更又は削除 - ログファイル媒体の記録容量超過
					Basic	・組織は、法規制等により要求される事項を満たす事ができるよう、適切な期間の監査記録を保持する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・情報システム及び産業用制御システムは、監査ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。 ・組織は、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
				CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対応組織(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。	H-Advanced	・組織は、セキュリティ専門の24時間365日モニタリングモニタリングにより収集した監査ログを、分析自動化ツール等を利用することで効率的に分析する。 ・組織は、従来のIT環境だけでなく、制御システムやIoT機器も含めて、セキュリティ状況のモニタリングの範囲とすることが望ましい。 ・組織は、セキュリティ対応組織の成熟度を定期的に評価し、セキュリティ状況のモニタリングやインシデントへの対応等のセキュリティ関連業務を継続的に改善することが望ましい。 [参考] セキュリティ対応組織(SOC/CSIRT)を評価するためのメトリクスには、「セキュリティ対応組織成熟度セルフチェックシート」(ISOG-J, 2018年)や、SIM3(Security Incident Management Maturity Model)等がある。
						Advanced	・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。なお、相関分析の対象には、他組織とデータを連携する部分のログも含めることが望ましい。 　- モニタリングするシステムの範囲をどこまでとするか 　- どのような機器のログを収集し、分析するか (CPS.AE-3を参照) ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する（プロセスの内容については、CPS.RP-1等を参照）。 ・組織及びシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には以下を含むことが望ましい。 　- ログ分析の分析結果（対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等） 　- モニタリングにおける今後の改善方針 [参考] セキュリティ対応組織(SOC/CSIRT)の業務、望まれる規模等については、「セキュリティ対応組織（SOC/CSIRT）の教科書 ～機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年)等を参照することが望ましい。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				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。	H-Advanced	・最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的なモニタリングに用いられている活動の修正の必要性を判断する。 ・組織は、自組織でIDS,IPS,SIEMといったセキュリティ装置等のポリシーチューニング（適用シグネチャ管理）と維持管理を行う。 ・組織は、自組織でセンサー機器でのカスタムシグネチャを脅威情報から作成する。 ・組織は、可能な場合、自組織に悪影響を及ぼす可能性の高いセキュリティ事象を適切に検知するため、<Advanced>で提示している機器のログに加え、IoT機器等のエッジデバイスのログも収集し、分析することが望ましい。
						Advanced	・組織は、自組織に悪影響を及ぼす可能性の高いセキュリティ事象を適切に検知するため、主に以下のような情報システムを構成する機器のログを監視し、リアルタイムに分析を行うことが望ましい。 多種多様なログの取り扱いが必要になるため、ログを正規化し、同一のデータベースに格納したり、SIEMを利用したりして、効率的な分析を実現する必要がある。取得可能な場合はネットフローの情報も扱うことが望ましい。 - ファイアウォールなどのネットワーク装置からのログやネットフロー - IPS/IDSなどのセキュリティ装置からのログ - Web サーバなどのアクセスログ - ActiveDirectoryやDNSなどの各種システムからのログ - ユーザ利用端末に関するログ [参考] セキュリティ対応組織(SOC/CSIRT)が実施する各種業務の内容については、「セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年) 等を参照することが望ましい。
						Basic	・ファイアウォールやエンドポイントセキュリティ製品等の通知を個別に確認することで、自組織に悪影響を及ぼすようなセキュリティ事象を特定する。
				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。	Basic	・組織は、リスクマネジメントに係る戦略やアセスメントの結果等から、セキュリティインシデントを検知するために収集することが望ましいログ情報を決定する。 ・組織は、取引先（サービスプロバイダ）に対して、取得されるサービス利用者の活動，例外処理及びセキュリティ事象を記録した監査ログの存在を確認する。 ・組織は，サービスプロバイダにより取得される監査ログが，サービスの利用者の活動，例外処理及びセキュリティ事象を記録できており、適切な方式で保護されていることを確認する。
		A.12.4.2 ログ情報の保護	ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護しなければならない。	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・情報システム及び産業用制御システムは、監査ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
	A.12.4.3 実務管理者及び運用担 当者の作業ログ		システムの実務管理者及び運用担当者の作業は，記録し，そのログを保護し，定期的にレビューしなければならない。	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・情報システム及び産業用制御システムは、監査ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。 ・組織は、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
		A.12.4.4 クロックの同期	組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは，単一の参照時刻源と同期させなければならない。	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
	A.12.5 運用ソフトウェアの 管理	A.12.5.1 運用システムに関わるソフトウェアの導入	運用システムに関わるソフトウェアの導入を管理するための手順を実施しなければならない。	CPS.IP-1	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	H-Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対して変更を実施する前に、それらの変更をテスト・承認・文書化する。 ・組織は、IoT機器、サーバ等の設定を一つの場所から管理・適用・検証するための自動化されたメカニズムを使用する。 ・組織は、特に産業用制御システムにおけるセキュリティに係る変更管理手順を、既存のプロセス安全管理の手順に統合する。
						Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法（例：変更実施前に本人にしかわからないセキュリティコードを入力させる）を利用する。 ・組織は、セキュリティ上の変更によって情報システム及び産業用制御システムの可用性や安全性等に悪影響が及ばないことを確実にするため、運用及び変更管理のポリシー及び手順を定期的にレビューする。
						Basic	・組織は、自組織の運用に適合する最も制限された設定基準を定めた上で、導入されるIoT機器、サーバ等の初期設定手順及び設定内容を文書化するとともに、その文書に従って設定を実施する。 ・組織は、IoT機器を設置する前にデフォルトの初期設定値を確認し、CPS.AC-1で定めたポリシーに準じていない場合に適切なものへと変更する。 ・組織は、IoT機器の導入前に、搭載されているソフトウェアを確認し、記録する。
				CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システム上で実行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）を用いてソフトウェアの制限を実施する、あるいは、許可されていないソフトウェアのインストールを不可とする。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
	A.12.6 技術的ぜい弱性管理	A.12.6.1 技術的ぜい弱性の管理	利用中の情報システムの技術的ぜい弱性に関する情報は，時機を失せずに獲得しなければならない。また，そのようなぜい弱性に組織がさらされている状況を評価しなければならない。さらに，それらと関連するリスクに対処するために，適切な手段をとらなければならない。	CPS.RA-1	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	H-Advanced	・組織は、自組織が管理する産業用制御システムの構成要素（IoT機器を含む）に対して、システムの運用に悪影響を及ぼさないよう、計画停止時等の予定されたタイミングに脆弱性診断を実施し、自組織の所有するシステムに存在する脆弱性を認識し、一覧化する。 ・組織は、自組織の管理するシステムにおける最新の脆弱性を認識するため、定期的に侵入テストを実施することが望ましい。 ・組織は、ツールを用いて脆弱性診断を行う場合、診断すべきシステムに対する脆弱性データベースを更新できる脆弱性診断ツールを使用することが望ましい。 ・組織は、より徹底した脆弱性の洗い出しを行うために、脆弱性診断の実施者に自組織の管理するシステムにおける特権アクセスの権利を一時的に許可するメカニズムを整備する。
						Advanced	・組織は、自組織が管理する重要度の高い情報システムの構成要素に対して、脆弱性診断を実施し、自組織の所有するシステムに存在する脆弱性を認識し、一覧化する。 ・組織は、自組織の所有する情報システムの運用段階において、各種資産から収集した脆弱性の内、自組織の事業運営等に関連することが想定されるものに対して、脆弱性検査ツール等を用いて、定期的に自組織のシステムにおける脆弱性を特定し、当該脆弱性の影響度とともに一覧に追加する。 [参考] 脆弱性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の影響の大きさを評価する指標として、CVSS(IPAによる解説：https://www.ipa.go.jp/security/vuln/CVSS.html)を参考とすることが可能である。
				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機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	H-Advanced	・組織は、産業用制御システムのようにモノの制御等を伴うような、フィジカル空間に影響を及ぼす可能性のある新たな機器やシステムを開発する場合には、従来の製品や他の事故事例を収集・分析し、セキュリティの観点も含めてセーフティに関わるハザードを特定する。 ・組織は、主に産業用制御システムにおいて、ハザードによって危害に至る状況を分析し、発生しやすさや被害の深刻度を明らかにすることで、生じるリスクを見積もる。その際、セキュリティの問題に起因するハザードの有無を確認することが望ましい。 ・組織は、産業用制御システム、またはそれが稼働する環境に大きな変化があった場合、もしくは産業用制御システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。 [参考] セーフティ設計におけるハザードの特定と分析については、「つながる世界のセーフティ＆セキュリティ設計入門」(IPA, 2015年)の4.2にて具体的な手法が記載されており、参照することが可能である。
						Advanced	・組織は、情報システム、または情報システムが稼働する環境に大きな変化があった場合（新たな脅威や脆弱性の特定を含む）、もしくは情報システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。 ・組織は、新たにIoT機器を利用したシステムを企画・設計する場合、既存の資産や新たに導入するシステムにおける守るべき資産を特定し、システムの利用用途や構成に応じて、セキュリティ対策をまとめる。特に、ライフサイクルの長いモノ、システムや、高い可用性を求められるモノ、システムを扱う場合は、設計以前の段階におけるセキュリティ対策の考慮が特に重要である。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 [参考] システム及びモノにおけるセキュリティの要求仕様を検討するにあたり、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。
				CPS.RA-5	・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。	Advanced	・組織は、情報システム、または情報システムが稼働する環境に大きな変化があった場合(新たな脅威や脆弱性の特定を含む)、もしくは情報システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。その際、重要度の高い情報システム及び産業用制御システムを優先的に対応する。 ※ CPS.RA-4と共通の実施内容
				CPS.IP-10	・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	H-Advanced	・組織は、欠陥修正状況を管理するための自動化されたメカニズムを導入し、管理する。
						Advanced	・パッチ適用中のIoT機器、サーバ等の動作により、他のソフトウェアアプリケーションやサービスの機能への影響が出るかどうかを調査やテストを通じて明らかにして、受容できるリスクを定める。 ・組織は、修正内容の有効性と副次的な悪影響の可能性についてテストを行った上で欠陥の修正を実施し、当該修正を構成管理として管理する。
						Basic	・組織は、自組織の情報システム及び産業用制御システムに関する欠陥の特定・報告・修正を計画的に実施する。計画を策定する際には、下記を考慮することが望ましい。 - 脅威または脆弱性の深刻さ - 修正措置の適用に関わるリスク [参考] 特に、製造現場等に設置されるIoT機器や制御機器（例：PLC、DCS）には、可用性や機器自体の機能の関係で、タイムリーにパッチを適用すること、あるいはパッチの適用事態が困難な場合がある。その場合は、「制御システム利用者のための脆弱性対応ガイド 第2版」(IPA, 2016年)の P.23に記載されている通り、脅威への対策（機能の最小化、ネットワーク監視の強化等）を徹底し、セキュリティ被害の発生を回避することが望ましい。 ※ PLC: Programmable Logic Controller, DCS: Distributed Control System

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				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。	H-Advanced	・組織は、自組織が管理する産業用制御システムの構成要素（IoT機器を含む）に対して、計画停止時等に脆弱性診断を実施し、自組織の所有するシステムに存在する脆弱性を認識し、一覧化する。 ・組織は、ツールを用いて脆弱性診断を行う場合、診断すべきシステムの脆弱性データベースをすぐに更新できる脆弱性診断ツールを使用することが望ましい。 ・組織は、スキャンされたシステムの脆弱性を定期的に、あるいは新たな脆弱性が特定され、報告された場合に更新する。 ・組織は、指定された脆弱性スキャン活動に関して、対象システムのコンポーネントに対する特権的アクセスの許可制度を実施する。
						Advanced	・組織は、情報システム及びアプリケーションの脆弱性のスキャンを定期的に、あるいは、それらのシステム／アプリケーションに影響を及ぼす新たな脆弱性が確認され、報告された場合に実施する。 ・組織は、脆弱性スキャンにツールを用いる。以下を満たす標準的な手法を使用することによって、脆弱性管理プロセスの一部を自動化できることが求められる。 - プラットフォーム、ソフトウェアの欠陥及び誤った設定を列挙する - チェックリストとテスト手順をフォーマットする - 脆弱性による影響を評価する ・組織は、リスクアセスメントを通じて、特定された脆弱性を適切な期間中に修正する。 ・上記のプロセスから得た情報を組織内の他のシステムの管理者と共有することによって、他の情報システム内の同様の脆弱性を把握し、必要に応じて修正する。 [参考] 脆弱性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の影響の大きさを評価する指標として、CVSS(IPAによる解説：https://www.ipa.go.jp/security/vuln/CVSS.html)を参考とすることが可能である。
						Basic	・組織は、情報システム及びアプリケーションの脆弱性のスキャンを定期的に実施する。
		A.12.6.2 ソフトウェアのインストールの制限	利用者によるソフトウェアのインストールを管理する規則を確立し，実施しなければならない。	CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する。	H-Advanced	・組織は、自組織の情報システム及び産業用制御システム上で実行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）を用いてソフトウェアの制限を実施する、あるいは、許可されていないソフトウェアのインストールを不可とする。
						Advanced	・組織は、自組織の情報システム及び産業用制御システム上でのユーザによるソフトウェアのインストールについて管理するメカニズムを導入し、管理する。
						Basic	・組織は、自組織の情報システム及び産業用制御システム上でのユーザによるソフトウェアのインストールに関するポリシーを確立し、ユーザに遵守させる。
	A.12.7 情報システムの監査に対する考慮事項	A.12.7.1 情報システムの監査に対する管理策	運用システムの検証を伴う監査要求事項及び監査活動は，業務プロセスの中断を最小限に抑えるために，慎重に計画し，合意しなければならない。	CPS.SC-6	・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。	H-Advanced	・組織は、契約事項からの逸脱及び、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先及びその再委託先以降の組織に対して、契約にて規定した組織のセキュリティマネジメント、納入する製品・サービスに実装されるセキュリティ機能等に関する義務事項が履行されているかどうかを一覧化して確認できるメカニズムを利用する。 ・委託元による実地調査、外部監査等の手法により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。 ・重要な取引先及びその再委託先以降の組織は、関係する攻撃の予兆、情報流出の事実がないかを調査し、組織に対して結果を定期的に報告する。
						Advanced	・組織は、自組織が取引先との契約において要求事項として規定した内容に関連して、システム上での監査が可能かどうか、確認する。 ・上記で定義されているシステム上で監査可能なイベントのために、監査記録を生成する機能を情報システムが提供する。 ・組織は、監査に関連する情報が必要な他の組織との間で、セキュリティ監査の整合性を保つことができるようにする。 ・組織は、手作業ないしは情報システムにより自動で生成された監査記録を定期的にでレビュー・分析して、契約事項からの逸脱及び、その兆候の有無を確認する。 ・チェックリストを用いた取引先による内部監査により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・情報システム及び産業用制御システムは、監査ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。 ・組織は、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
A.13 通信のセキュリティ	A.13.1 ネットワークセキュリティ管理	A.13.1.1 ネットワーク管理策	システム及びアプリケーション内の情報を保護するために，ネットワークを管理し，制御しなければならない。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムを構成するネットワークの内部における境界について通信をモニタリングし、制御する。 ・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・機密性の高いデータを取り扱う自組織の情報システムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界（産業用制御システムの場合は情報システムとの境界）について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。
				CPS.AC-9	・IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	H-Advanced	・情報システム及び産業用制御システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤(PKI)を利用した認証を要求する。 ※ 産業用制御システムにてPKIを使用した認証を実施する場合、発生する処理待ち時間がシステムのパフォーマンスを低下させないことをあらかじめ確認する。 ・情報システム及び産業用制御システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 [参考] 認証方式の強度及び適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に見合うメカニズムの強度を持った認証を実施する。 ・情報システムは、ユーザが自組織のシステムにログインする際に、取引のリスク（個人のセキュリティ、プライバシーのリスク等）に関する通知メッセージ等を表示する。 ・情報システム及び産業用制御システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・組織は、クレデンシャルの有効期限を設定し、有効期限を越えたパスワードが私用されていないかを管理する。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H-Advanced	・組織は、情報システム及び産業用制御システムを構成する重要なデータを扱う通信路について、通信経路の暗号化を実装する又は代替の物理的な対策によって保護する。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。 ・組織は、産業用制御システムのパフォーマンスに監査活動が与える影響が許容範囲内であることを確認する。
		A.13.1.2 ネットワークサービスのセキュリティ	組織が自ら提供するか外部委託しているかを問わず，全てのネットワークサービスについて，セキュリティ機能，サービスレベル及び管理上の要求事項を特定しなければならず，また，ネットワークサービス合意書にもこれらを盛り込まなければならない。	CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	H-Advanced	・調達する機器に対して、契約におけるセキュリティ要求事項が満たせているかを、自組織あるいは第三者がテストする。 ・組織は、自組織のオペレーションにとって特に重要な機器について、再委託先以降の組織を含む関係するサプライチェーン全体に渡り、一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロシージャで製造されたものかを確認する。
						Advanced	・組織は、契約において、例えば下記のように、取引先から調達する製品・サービスが具備すべきセキュリティ要求事項を明確化する。 - セキュリティに関わる特定の認証（例：ISMS認証、ISASecure EDSA認証、ITセキュリティ評価及び認証制度(JISEC)）を有していること - ベンダー自身により、セキュリティに関わる特定の認証の基準に適合する対策を実施していることが確認されていること - リスク分析の結果等から導かれた必要なセキュリティ要件を設計時からの実装（セキュリティ・バイ・デザイン）し、検査していること ・組織は、調達計画時に、製品またはサービス自体、あるいは当該製品・サービスの調達・供給にて使用される資産の保護に係るセキュリティ要件の費用を確保しておくことが望ましい。 ・下記を含む製品またはサービスの調達または供給を評価するためのセキュリティ測定ルールを策定し、運用及び改善する。 - 測定対象の内容 - 措置の報告方法、報告の頻度 - 措置が実施されない場合に遂行される措置 ・組織は、搬送中の改ざん・漏えいを検知(又は抑止)する手段とともに納品されるIoT機器やソフトウェアが、不正操作されていないかを確認する。 - 物品：セキュリティ便、プロテクトシール等 - 電送：暗号化、電送データ全体のハッシュ値等
				CPS.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。	H-Advanced	・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル及び他のサービスを明確にするよう要求する。 ・組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。
						Advanced	・組織は、外部サービスプロバイダ及びシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報，業務システム及び業務プロセスの重要性並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスををモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。
						Basic	・組織は、外部情報システムサービスのプロバイダ及びシステム開発の委託先に対して、自組織が対象となっている、あるいは当該プロバイダーが対象として該当するルールに従って、例えば、下記に関連するようなセキュリティ要求事項を設定し、導入することを要求する。 - （例えば、ISMS認証取得相当の）セキュリティ対策が十分に行われていること - 運用中のデータが適切に管理されること - サービス利用終了時にデータが適切に削除されること

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.13.1.3 ネットワークの分離	情報サービス，利用者及び情報システムは，ネットワーク上で，グループごとに分離しなければならない。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムを構成するネットワークの内部における境界について通信をモニタリングし、制御する。 ・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・機密性の高いデータを取り扱う自組織の情報システムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界（産業用制御システムの場合は情報システムとの境界）について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。
	A.13.2 情報の転送	A.13.2.1 情報転送の方針及び手順	あらゆる形式の通信設備を利用した情報転送を保護するために，正式な転送方針，手順及び管理策を備えなければならない。	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、適切に管理する。	H-Advanced	・組織は、情報システム及び産業用制御システムのシステム構成、通信ネットワーク構成及びデータフローをリアルタイムでモニタリングし、管理するための自動化されたメカニズムを導入・管理している。
						Advanced	・組織は、関連する文書内の図に、ネットワーク接続におけるインターフェース特性、セキュリティ要求事項、伝達されるデータの性質を記載する。
						Basic	・組織は、自組織が管理する範囲（例：事業所単位で）における情報システム及び産業用制御システムのシステム構成、通信ネットワーク構成、データフローを文書化し、保管する。 ・組織は、定期的、あるいは、システム構成、ネットワーク構成、データフローに変更が生じた場合、関連する文書をレビューし、必要に応じて更新する。 [参考] システム構成、ネットワーク構成、データフローの文書化を行う際の手順については、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA, 2018年）の3.2、3.3を参照することが可能である。
				CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	H-Advanced	・システムは、自組織が利用している外部情報システムサービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・システムは、利用を許可していない外部情報システムサービスを検知した場合、システム管理者へ通知するメカニズムを利用する。 ・組織は、外部プロバイダによる情報システムサービスを使用する際に必要な機能、ポート、プロトコル及び他のサービスを明確にする。
						Advanced	・組織は、外部の情報システムを所有、運用する他の組織に対して、下記を許可するうえでの条件を設定する。 a. 外部の情報システムから自組織の情報システムにアクセスすること b. 外部の情報システムを使用して自組織の管理下にある情報を処理または保存もしくは伝送すること ・外部のシステム上に接続された自組織が所有するストレージの許可された個人による使用を制限する。
				CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムを構成するネットワークの内部における境界について通信をモニタリングし、制御する。 ・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・機密性の高いデータを取り扱う自組織の情報システムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界（産業用制御システムの場合は情報システムとの境界）について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。
						Basic	・組織は、情報システム及び産業用制御システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、適切に論理的あるいは物理的にネットワークを分離することで、フローの制御を実施する。 ・組織は、産業用制御システムにおいて、制御システムのネットワークを情報システムとのネットワークから論理的あるいは物理的にセグメント化する。 [参考] 他のネットワークと物理的に離れた環境においては物理的なセグメント化を実施する、他のネットワークと物理的に近接した環境では、対策のコスト等も考慮して論理的なセグメント化を実施する等の対応が可能である。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H-Advanced	・組織は、情報システム及び産業用制御システムを構成する重要なデータを扱う通信路について、通信経路の暗号化を実装する又は代替の物理的な対策によって保護する。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。
				CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。	H-Advanced	・システム/IoT機器は、少ないリソースでも可用性を損なわずに実装可能な暗号モジュールを導入し、リソースは制限されているが重要度の高い機器からの通信データを適切な強度で暗号化することが望ましい。 ・情報システムは、重要度の高い・低いに限らず、組織外部へ送信するすべてのデータを適切な強度で暗号化する。
						Advanced	・組織は、機密性の高い情報を外部の組織等へ送信する際、情報を適切な強度の方式で暗号化する。
				CPS.CM-4	・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	H-Advanced	・組織は、データ入力に対する「ホワイトリスト」の概念を導入することで、インプットデータの出所を既知の信頼できるモノ、システム等と、そうしたインプットデータの許容できるフォーマットを指定する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。 ・情報システム及び産業用制御システムは、通信セッションの真正性を保護する。
						Advanced	・情報システムは、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、当該IoT機器が自組織の業務において重要なものと認められる場合、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。
		A.13.2.2 情報転送に関する合意	合意では，組織と外部関係者との間の業務情報のセキュリティを保った転送について，取り扱わなければならない。	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、適切に管理する。	H-Advanced	・組織は、情報システム及び産業用制御システムのシステム構成、通信ネットワーク構成及びデータフローをリアルタイムでモニタリングし、管理するための自動化されたメカニズムを導入・管理している。
						Advanced	・組織は、関連する文書内の図に、ネットワーク接続におけるインターフェース特性、セキュリティ要求事項、伝達されるデータの性質を記載する。
						Basic	・組織は、自組織が管理する範囲（例：事業所単位で）における情報システム及び産業用制御システムのシステム構成、通信ネットワーク構成、データフローを文書化し、保管する。 ・組織は、定期的、あるいは、システム構成、ネットワーク構成、データフローに変更が生じた場合、関連する文書をレビューし、必要に応じて更新する。 [参考] システム構成、ネットワーク構成、データフローの文書化を行う際の手順については、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA, 2018年）の3.2、3.3を参照することが可能である。
				CPS.DS-1	・組織間で保護すべき情報を交換する場合、当該情報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。	Advanced	・組織は、交換するデータの重要度、想定されるリスクを勘案して、具体的なセキュリティ対策要件を指定し、取引先に対して実装を求める。 ・組織は、再委託先以降の事業者へのデータ取扱い業務の委託を、直接の取引先に求める水準のセキュリティ対策が実装されていることが確認される場合に限って、許可する。
						Basic	・組織は、取引先が取り扱う可能性のあるデータに関して、秘密保持契約を締結することで、取り扱いを規定する。 ・組織は、直接の取引先に対して、データの管理に関わる業務の再委託を禁止する。 [参考] 「中小企業の情報セキュリティ対策ガイドライン 第3版」(IPA, 2019年)で、委託契約時の機密保持契約条項のサンプルを提供している。
		A.13.2.3 電子的メッセージ通信	電子的メッセージ通信に含まれた情報は，適切に保護しなければならない。	CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H-Advanced	・組織は、情報システム及び産業用制御システムを構成する重要なデータを扱う通信路について、通信経路の暗号化を実装する又は代替の物理的な対策によって保護する。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。
				CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。	H-Advanced	・システム/IoT機器は、少ないリソースでも可用性を損なわずに実装可能な暗号モジュールを導入し、リソースは制限されているが重要度の高い機器からの通信データを適切な強度で暗号化することが望ましい。 ・情報システムは、重要度の高い・低いに限らず、組織外部へ送信するすべてのデータを適切な強度で暗号化する。
						Advanced	・組織は、機密性の高い情報を外部の組織等へ送信する際、情報を適切な強度の方式で暗号化する。
				CPS.CM-4	・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	H-Advanced	・組織は、データ入力に対する「ホワイトリスト」の概念を導入することで、インプットデータの出所を既知の信頼できるモノ、システム等と、そうしたインプットデータの許容できるフォーマットを指定する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。 ・情報システム及び産業用制御システムは、通信セッションの真正性を保護する。
						Advanced	・情報システムは、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、当該IoT機器が自組織の業務において重要なものと認められる場合、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.13.2.4 秘密保持契約又は守秘義務契約	情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は，特定し，定めに従ってレビューし，文書化しなければならない。	CPS.SC-3	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織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。	H-Advanced	・組織は、システム・モノ・サービスのいずれかを提供する取引先との契約において、当該組織に対して、以下の実施を要求する。 - 契約にて指定されたセキュリティ対策を実施したエビデンスの作成、セキュリティテスト／評価結果の提示 - セキュリティテスト／評価時に特定された欠陥の修正計画の策定 - 欠陥の修正計画及び、その実施状況の提示 ・組織は、直接の委託先に対して要求しているセキュリティ対策に関する要求事項及びそれに付随する要求事項の内で必要な事項を、サプライチェーンに由来するリスクの大きさ等を勘案しつつ、再委託先以降の組織に対して（場合によっては再委託先以降の全サプライヤーに対して）も適用することが望ましい。 [参考] 委託契約に含め、実施を確認することが望ましい項目に関する追加の情報の取得のためには、「ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」(IPA, 2018年)の「3.2. IT サプライチェーン リスクマネジメント の全体像」等を参照することが可能である。
						Advanced	・組織のミッション／業務ニーズに応じて、システム、モノ、またはサービスの調達契約に以下の要求事項、記述及び基準を記載する。 - セキュリティ対策に関する要求事項 - セキュリティ関連のドキュメントに関する要求事項 - セキュリティ関連のドキュメントの保護に関する要求事項 - 秘密保持に関する条項 - インシデントが発生した際の報告先、報告内容、初動、調査、復旧等の各対応の実施主体、実施方法 - 自組織または認可された第三者によって監査され、定義されたセキュリティ要件への遵守を確認することを許可する条件 - 契約終了後の情報資産の扱い ・組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施し、委託内容の特性等により必要と認められる場合、調達契約において、追加で対策を導入することを要求する。 ・法規制等を参照してセキュリティ要件を決定し、取引先へ遵守を要求する際、下記を事前に考慮することが望ましい。 - 自組織と取引先との法令の相違（例：業法の違い、国・地域の違い）により生じるコンプライアンス上のリスクの特定 - 取引先に適用される法律及び規制上の義務によるセキュリティの観点からの契約への悪影響
						Basic	・組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施することを要求する。 ・組織は、委託先の選定、評価のプロセスにおいて、取引先がセキュリティアクションを宣言していることを確認する。
A.14 システムの取得，開発及び保守	A.14.1 情報システムのセキュリティ要求事項	A.14.1.1 情報セキュリティ要求事項の分析及び仕様化	情報セキュリティに関連する要求事項は，新しい情報システム又は既存の情報システムの改善に関する要求事項に含めなければならない。	CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	H-Advanced	・調達する機器に対して、契約におけるセキュリティ要求事項が満たせているかを、自組織あるいは第三者がテストする。 ・組織は、自組織のオペレーションにとって特に重要な機器について、再委託先以降の組織を含む関係するサプライチェーン全体に渡り、一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロシージャで製造されたものかを確認する。
						Advanced	・組織は、契約において、例えば下記のように、取引先から調達する製品・サービスが具備すべきセキュリティ要求事項を明確化する。 - セキュリティに関わる特定の認証（例：ISMS認証、ISASecure EDSA認証、ITセキュリティ評価及び認証制度(JISEC)）を有していること - ベンダー自身により、セキュリティに関わる特定の認証の基準に適合する対策を実施していることが確認されていること - リスク分析の結果等から導かれた必要なセキュリティ要件を設計時からの実装（セキュリティ・バイ・デザイン）し、検査していること ・組織は、調達計画時に、製品またはサービス自体、あるいは当該製品・サービスの調達・供給にて使用される資産の保護に係るセキュリティ要件の費用を確保しておくことが望ましい。 ・下記を含む製品またはサービスの調達または供給を評価するためのセキュリティ測定ルールを策定し、運用及び改善する。 - 測定対象の内容 - 措置の報告方法、報告の頻度 - 措置が実施されない場合に遂行される措置 ・組織は、搬送中の改ざん・漏えいを検知(又は抑止)する手段とともに納品されるIoT機器やソフトウェアが、不正操作されていないかを確認する。 - 物品：セキュリティ便、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

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				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する。	H-Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 -セキュリティ機能に関する要求事項 -セキュリティ強度に関する要求事項 -セキュリティ保証に関する要求事項 -セキュリティ関連のドキュメントに関する要求事項 -セキュリティ関連のドキュメントの保護に関する要求事項 -そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 -受け入れ基準
						Advanced	・組織は、 情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
						Basic	・組織は、システムを構築するに当たり仕様書、設計、開発、導入及び変更に、システムのセキュリティエンジニアリング原則を適用する。
		A.14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	公衆ネットワークを経由するアプリケーションサービスに含まれる情報は，不正行為，契約紛争，並びに認可されていない開示及び変更から保護しなければならない。	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムを構成するネットワークの内部における境界について通信をモニタリングし、制御する。 ・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・機密性の高いデータを取り扱う自組織の情報システムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界（産業用制御システムの場合は情報システムとの境界）について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H-Advanced	・組織は、情報システム及び産業用制御システムを構成する重要なデータを扱う通信路について、通信経路の暗号化を実装する又は代替の物理的な対策によって保護する。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。
				CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。	H-Advanced	・システム/IoT機器は、少ないリソースでも可用性を損なわずに実装可能な暗号モジュールを導入し、リソースは制限されているが重要度の高い機器からの通信データを適切な強度で暗号化することが望ましい。 ・情報システムは、重要度の高い・低いに限らず、組織外部へ送信するすべてのデータを適切な強度で暗号化する。
						Advanced	・組織は、機密性の高い情報を外部の組織等へ送信する際、情報を適切な強度の方式で暗号化する。
				CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する。	H-Advanced	・組織は、産業用制御システムにおいて、可能な場合、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・組織は、設定の不正な変更や、システム権限の不正な昇格等の、セキュリティ関連の変更が不正に行われた場合の検知能力を、組織のインシデント対応能力に組み入れる。
						Advanced	・組織は、情報システムにおいて、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・情報システムは、保管データの完全性チェックを定期的に実施する。 ・情報システムは、電子メールにおける送信ドメイン認証技術をサポートして、送信者のなりすましやメールの改ざんを検知する。
		A.14.1.3 アプリケーションサービスのトランザクションの保護	アプリケーションサービスのトランザクションに含まれる情報は，次の事項を未然に防止するために，保護しなければならない。 – 不完全な通信 – 誤った通信経路設定 – 認可されていないメッセージの変更 – 認可されていない開示 – 認可されていないメッセージの複製又は再生	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	H-Advanced	・情報システム及び産業用制御システムは、自組織のシステムを構成するネットワークの内部における境界について通信をモニタリングし、制御する。 ・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可能とするメカニズムを整備する。 ・組織は、重要度の高い産業用制御システムのネットワークを重要度の高くない制御システムのネットワークから物理的あるいは論理的に分離する。 ・機密性の高いデータを取り扱う自組織の情報システムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。
						Advanced	・情報システム及び産業用制御システムは、自組織のシステムの繋がるネットワークにおける外部境界（産業用制御システムの場合は情報システムとの境界）について通信をモニタリングし、制御する。 ・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、当該装置を介して外部ネットワーク等に接続する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・情報システム及び産業用制御システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する。
				CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	H-Advanced	・組織は、情報システム及び産業用制御システムを構成する重要なデータを扱う通信路について、通信経路の暗号化を実装する又は代替の物理的な対策によって保護する。
						Advanced	・情報システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。
				CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する。	H-Advanced	・組織は、産業用制御システムにおいて、可能な場合、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・組織は、設定の不正な変更や、システム権限の不正な昇格等の、セキュリティ関連の変更が不正に行われた場合の検知能力を、組織のインシデント対応能力に組み入れる。
						Advanced	・組織は、情報システムにおいて、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・情報システムは、保管データの完全性チェックを定期的に実施する。 ・情報システムは、電子メールにおける送信ドメイン認証技術をサポートして、送信者のなりすましやメールの改ざんを検知する。
				CPS.CM-4	・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	H-Advanced	・組織は、データ入力に対する「ホワイトリスト」の概念を導入することで、インプットデータの出所を既知の信頼できるモノ、システム等と、そうしたインプットデータの許容できるフォーマットを指定する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。 ・情報システム及び産業用制御システムは、通信セッションの真正性を保護する。
						Advanced	・情報システムは、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、当該IoT機器が自組織の業務において重要なものと認められる場合、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。
	A.14.2 開発及びサポートプロセスにおけるセキュリティ	A.14.2.1 セキュリティに配慮した開発のための方針	ソフトウェア及びシステムの開発のための規則は，組織内において確立し，開発に対して適用しなければならない。	CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。	H-Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 -セキュリティ機能に関する要求事項 -セキュリティ強度に関する要求事項 -セキュリティ保証に関する要求事項 -セキュリティ関連のドキュメントに関する要求事項 -セキュリティ関連のドキュメントの保護に関する要求事項 -そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 -受け入れ基準
						Advanced	・組織は、 情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
						Basic	・組織は、システムを構築するに当たり仕様書、設計、開発、導入及び変更に、システムのセキュリティエンジニアリング原則を適用する。
		A.14.2.2 システムの変更管理手順	開発のライフサイクルにおけるシステムの変更は，正式な変更管理手順を用いて管理しなければならない。	CPS.IP-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。	H-Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対して変更を実施する前に、それらの変更をテスト・承認・文書化する。 ・組織は、IoT機器、サーバ等の設定を一つの場所から管理・適用・検証するための自動化されたメカニズムを使用する。 ・組織は、特に産業用制御システムにおけるセキュリティに係る変更管理手順を、既存のプロセス安全管理の手順に統合する。
						Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法（例：変更実施前に本人にしかわからないセキュリティコードを入力させる）を利用する。 ・組織は、セキュリティ上の変更によって情報システム及び産業用制御システムの可用性や安全性等に悪影響が及ばないことを確実にするため、運用及び変更管理のポリシー及び手順を定期的にレビューする。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				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する。	H-Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 -セキュリティ機能に関する要求事項 -セキュリティ強度に関する要求事項 -セキュリティ保証に関する要求事項 -セキュリティ関連のドキュメントに関する要求事項 -セキュリティ関連のドキュメントの保護に関する要求事項 -そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 -受け入れ基準
						Advanced	・組織は、 情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
		A.14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	オペレーティングプラットフォームを変更するときは，組織の運用又はセキュリティに悪影響がないことを確実にするために，重要なアプリケーションをレビューし，試験しなければならない。	CPS.IP-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。	H-Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対して変更を実施する前に、それらの変更をテスト・承認・文書化する。 ・組織は、IoT機器、サーバ等の設定を一つの場所から管理・適用・検証するための自動化されたメカニズムを使用する。 ・組織は、特に産業用制御システムにおけるセキュリティに係る変更管理手順を、既存のプロセス安全管理の手順に統合する。
						Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 ・組織は、自身のアカウントや、IoT機器、サーバ等のパスワードを忘れてしまった場合、安全な回復方法（例：変更実施前に本人にしかわからないセキュリティコードを入力させる）を利用する。 ・組織は、セキュリティ上の変更によって情報システム及び産業用制御システムの可用性や安全性等に悪影響が及ばないことを確実にするため、運用及び変更管理のポリシー及び手順を定期的にレビューする。
				CPS.IP-10	・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	H-Advanced	・組織は、欠陥修正状況を管理するための自動化されたメカニズムを導入し、管理する。
						Advanced	・パッチ適用中のIoT機器、サーバ等の動作により、他のソフトウェアアプリケーションやサービスの機能への影響が出るかどうかを調査やテストを通じて明らかにして、受容できるリスクを定める。 ・組織は、修正内容の有効性と副次的な悪影響の可能性についてテストを行った上で欠陥の修正を実施し、当該修正を構成管理として管理する。
		A.14.2.4 パッケージソフトウェアの変更に対する制限	パッケージソフトウェアの変更は，抑止しなければならず，必要な変更だけに限らなければならない。また，全ての変更は，厳重に管理しなければならない。	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	Advanced	・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。
				CPS.MA-1	・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 ・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。	H-Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な変更または不正な変更がないか確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。
						Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.14.2.5 セキュリティに配慮したシステム構築の原則	セキュリティに配慮したシステムを構築するための原則を確立し，文書化し，維持し，全ての情報システムの実装に対して適用しなければならない。	CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。	H-Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 -セキュリティ機能に関する要求事項 -セキュリティ強度に関する要求事項 -セキュリティ保証に関する要求事項 -セキュリティ関連のドキュメントに関する要求事項 -セキュリティ関連のドキュメントの保護に関する要求事項 -そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 -受け入れ基準
						Advanced	・組織は、 情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
		A.14.2.6 セキュリティに配慮した開発環境	組織は，全てのシステム開発ライフサイクルを含む，システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し，適切に保護しなければならない。	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する。	H-Advanced	・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。 -セキュリティ機能に関する要求事項 -セキュリティ強度に関する要求事項 -セキュリティ保証に関する要求事項 -セキュリティ関連のドキュメントに関する要求事項 -セキュリティ関連のドキュメントの保護に関する要求事項 -そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述 -受け入れ基準
						Advanced	・組織は、 情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。
						Basic	・組織は、システムを構築するに当たり仕様書、設計、開発、導入及び変更に、システムのセキュリティエンジニアリング原則を適用する。
		A.14.2.7 外部委託による開発	組織は，外部委託したシステム開発活動を監督し，監視しなければならない。	CPS.SC-6	・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。	H-Advanced	・組織は、契約事項からの逸脱及び、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先及びその再委託先以降の組織に対して、契約にて規定した組織のセキュリティマネジメント、納入する製品・サービスに実装されるセキュリティ機能等に関する義務事項が履行されているかどうかを一覧化して確認できるメカニズムを利用する。 ・委託元による実地調査、外部監査等の手法により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。 ・重要な取引先及びその再委託先以降の組織は、関係する攻撃の予兆、情報流出の事実がないかを調査し、組織に対して結果を定期的に報告する。
						Advanced	・組織は、自組織が取引先との契約において要求事項として規定した内容に関連して、システム上での監査が可能かどうか、確認する。 ・上記で定義されているシステム上で監査可能なイベントのために、監査記録を生成する機能を情報システムが提供する。 ・組織は、監査に関連する情報が必要な他の組織との間で、セキュリティ監査の整合性を保つことができるようにする。 ・組織は、手作業ないしは情報システムにより自動で生成された監査記録を定期的にでレビュー・分析して、契約事項からの逸脱及び、その兆候の有無を確認する。 ・チェックリストを用いた取引先による内部監査により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				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。	H-Advanced	・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル及び他のサービスを明確にするよう要求する。 ・組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。
						Advanced	・組織は、外部サービスプロバイダ及びシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報，業務システム及び業務プロセスの重要性並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスををモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。
						Basic	・組織は、外部情報システムサービスのプロバイダ及びシステム開発の委託先に対して、自組織が対象となっている、あるいは当該プロバイダーが対象として該当するルールに従って、例えば、下記に関連するようなセキュリティ要求事項を設定し、導入することを要求する。 - （例えば、ISMS認証取得相当の）セキュリティ対策が十分に行われていること - 運用中のデータが適切に管理されること - サービス利用終了時にデータが適切に削除されること
		A.14.2.8 システムセキュリティの試験	セキュリティ機能（functionality）の試験は，開発期間中に実施しなければならない。	CPS.DP-3	・監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。	H-Advanced	・最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的なモニタリングに用いられている活動の修正の必要性を判断する。 ・システムに、既知で害のないテストケースを導入して、マルウェア検知メカニズムをテストする。 ・組織は、侵入検知モニタリングに用いているメカニズムを定期的にテストする。テストの頻度は、組織が使用するツールの種類と、ツールの設置方法により変わる。
						Advanced	・組織は、自組織のシステムのモニタリング活動が、組織のリスクマネジメント戦略と、リスク対応のためのアクションの優先順位に適合しているかどうかを定期的に確認するプロシージャを定め、運用する。 ・ネットワーク機器やエンドポイントからのセキュリティに係る情報の相関分析を行うのに合わせて、誤検出や検出漏れの割合を算出し。定期的に検知メカニズムの妥当性を確認する。
		A.14.2.9 システムの受入れ試験	新しい情報システム，及びその改訂版・更新版のために，受入れ試験のプログラム及び関連する基準を確立しなければならない。	CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	H-Advanced	・調達する機器に対して、契約におけるセキュリティ要求事項が満たせているかを、自組織あるいは第三者がテストする。 ・組織は、自組織のオペレーションにとって特に重要な機器について、再委託先以降の組織を含む関係するサプライチェーン全体に渡り、一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロシージャで製造されたものかを確認する。
						Advanced	・組織は、契約において、例えば下記のように、取引先から調達する製品・サービスが具備すべきセキュリティ要求事項を明確化する。 - セキュリティに関わる特定の認証（例：ISMS認証、ISASecure EDSA認証、ITセキュリティ評価及び認証制度(JISEC)）を有していること - ベンダー自身により、セキュリティに関わる特定の認証の基準に適合する対策を実施していることが確認されていること - リスク分析の結果等から導かれた必要なセキュリティ要件を設計時からの実装（セキュリティ・バイ・デザイン）し、検査していること ・組織は、調達計画時に、製品またはサービス自体、あるいは当該製品・サービスの調達・供給にて使用される資産の保護に係るセキュリティ要件の費用を確保しておくことが望ましい。 ・下記を含む製品またはサービスの調達または供給を評価するためのセキュリティ測定ルールを策定し、運用及び改善する。 - 測定対象の内容 - 措置の報告方法、報告の頻度 - 措置が実施されない場合に遂行される措置 ・組織は、搬送中の改ざん・漏えいを検知(又は抑止)する手段とともに納品されるIoT機器やソフトウェアが、不正操作されていないかを確認する。 - 物品：セキュリティ便、プロテクトシール等 - 電送：暗号化、電送データ全体のハッシュ値等
	A.14.3 試験データ	A.14.3.1 試験データの保護	試験データは，注意深く選定し，保護し，管理しなければならない。	CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	H-Advanced	・調達する機器に対して、契約におけるセキュリティ要求事項が満たせているかを、自組織あるいは第三者がテストする。 ・組織は、自組織のオペレーションにとって特に重要な機器について、再委託先以降の組織を含む関係するサプライチェーン全体に渡り、一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロシージャで製造されたものかを確認する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.SC-6	・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。	H-Advanced	・組織は、契約事項からの逸脱及び、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先及びその再委託先以降の組織に対して、契約にて規定した組織のセキュリティマネジメント、納入する製品・サービスに実装されるセキュリティ機能等に関する義務事項が履行されているかどうかを一覧化して確認できるメカニズムを利用する。 ・委託元による実地調査、外部監査等の手法により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。 ・重要な取引先及びその再委託先以降の組織は、関係する攻撃の予兆、情報流出の事実がないかを調査し、組織に対して結果を定期的に報告する。
						Advanced	・組織は、自組織が取引先との契約において要求事項として規定した内容に関連して、システム上での監査が可能かどうか、確認する。 ・上記で定義されているシステム上で監査可能なイベントのために、監査記録を生成する機能を情報システムが提供する。 ・組織は、監査に関連する情報が必要な他の組織との間で、セキュリティ監査の整合性を保つことができるようにする。 ・組織は、手作業ないしは情報システムにより自動で生成された監査記録を定期的にでレビュー・分析して、契約事項からの逸脱及び、その兆候の有無を確認する。 ・チェックリストを用いた取引先による内部監査により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。
				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、テストする。	H-Advanced	・組織は、バックアップ情報を定期的にテストして、媒体の信頼性と情報の完全性を確認する。
				CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	H-Advanced	・収集されたログは、セキュリティインシデントの検知に加え、セキュリティインシデントの原因を事後的に追跡することにも有効であるため、可能であれば、OS機能では残らない詳細ログ（OSコマンドレベル）も収集する。 ・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理する。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・情報システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・情報システム及び産業用制御システムは、監査ログ及び監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・情報システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
A.15 供給者関係	A.15.1 供給者関係における情報セキュリティ	A.15.1.1 供給者関係のための情報セキュリティの方針	組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化しなければならない。	CPS.AM-7	・自組織及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。	Advanced	・組織は、セキュリティインシデントにより損害が発生する場合に備えて、取引先等から指定されるセキュリティ対策の実装に加え、サイバー保険の利用等によるリスク移転を検討する。
						Basic	・組織は、委託先あるいは委託元との契約において、業務においてセキュリティインシデントにより損害が発生した場合の自組織と取引先の責任範囲（免責事項の明記、損害賠償額の契約金額等での上限設定等）を規定する。 ・組織は、契約において取引先に対応を求める／求められるセキュリティに関する要求事項の実効性を高めるため、要求事項への対応要否や過不足、具体的な対応方法や費用負担、対応できない場合の代替措置について契約時あるいは契約期間の初めに合意することが望ましい。 [参考] 特にクラウドサービスプロバイダーと自組織との役割と責任に関して、追加の情報を得るために、「クラウドセキュリティガイドライン活用ガイドブック 2013年度版」（経済産業省, 2013年）の "4.4.クラウドサービスの契約" を参照することが可能である。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				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、その内容について取引先と合意する。	Advanced	・組織は、サプライチェーンに係るセキュリティ対策基準を参照して、ITT(Invitation To Tender)やRFP(Request For Proposal)などの入札書類を準備し、潜在的な取引先に提供する。特に、入札書類には以下が含まれることが望ましい。 1）調達する製品またはサービスの仕様 2）供給者が製品またはサービスを供給している間に従うセキュリティ要件 3）製品またはサービスの供給中に従うべきサービスレベル及びその指標 4）セキュリティ要件に違反した場合に、委託元が課す可能性のある罰則 5）取引先の選定プロセス中に送信されるデータやシステムなどを保護するための秘密保持条項 ・組織は、取引先によるセキュリティ管理策の遵守状況を継続的にモニタリングするための、プロシージャを整備する。 ・取引先におけるセキュリティインシデントが自組織に影響した場合に備え、契約書にて外部事業者との責任分界点を明確にし、外部事業者の責任範囲において自組織に被害が発生した場合の損害賠償について記載する等の対応を行う。
						Basic	・組織は、該当する法規制等を参照して、取引先（特に、自組織のデータを取り扱う可能性のある、またはデータを取り扱うための基盤を提供する可能性のあるもの）に対して適用するセキュリティ対策基準を策定し、内容について合意する。 ・組織は、取引先（外部情報システムサービスのプロバイダ）に対して、サービスの使用に必要な機能、ポート、プロトコル及び他のサービスを明確にする。 [参考] 取引先に対して適用するセキュリティ対策基準の策定に当たり、ISO/IEC 27001 附属書Aの管理策をベースに作成された「情報セキュリティベンチマーク」(IPA)や、「サプライチェーン情報セキュリティ管理基準」（日本セキュリティ監査協会）等を参考とすることが可能である。
				CPS.SC-2	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	H-Advanced	・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 ・取引先において、事業への悪影響を及ぼすセキュリティインシデントが発生した際の、自組織への影響の内容及び、その起こりやすさ、規模を推定する。 ※ 関連する対策要件に、CPS.AM-6, CPS.BE-2等がある。
						Advanced	・組織は、自組織のミッション/業務プロセスに重要な影響を及ぼしうるサプライチェーン上の取引先を特定し、当該組織が自組織のセキュリティポリシーに規定されているセキュリティ上の役割と責任を果たせるかどうかを確認する。
						Basic	・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 ・組織は、長期に渡ってIoT機器が使用されることが想定される場合、問い合わせ窓口やサポート体制等の適切な管理体制が整備されており、販売後のセキュリティサポート方針を明確にしている等、長期間のサポートが期待できる取引先（IoT機器ベンダ）を選定する。 ・組織は、IoT機器のサポート終了時に機器を入れ替えることの要否についてシステムの導入前に取引先（IoT機器ベンダ）に対して確認する。 ・組織は、下記の観点を確認することにより、ITサービスのマネジメントを効率的、効果的に運営管理するサービスプロバイダーを選定することが望ましい。 - JIS Q 20000 に基づく第三者認証（ITSMS認証）を取得している - 自己適合確認を通じて認証取得相当の対策の実装を確認している
				CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	Advanced	・組織は、遠隔保守のための接続の確立と実施に関するポリシーとプロシージャを文書化し、その内容により実施する。 ・組織は、遠隔保守を実施する際には組織の定めるネットワークアクセスに求める認証を実施するとともに、遠隔保守が完了したらセッションとネットワーク接続を確実に終了する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.15.1.2 供給者との合意におけるセキュリティの取扱い	関連する全ての情報セキュリティ要求事項を確立しなければならず，また，組織の情報に対して，アクセス，処理，保存若しくは通信を行う，又は組織の情報のための IT 基盤を提供する可能性のあるそれぞれの供給者と，この要求事項について合意しなければならない。	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、その内容について取引先と合意する。	Advanced	・組織は、サプライチェーンに係るセキュリティ対策基準を参照して、ITT(Invitation To Tender)やRFP(Request For Proposal)などの入札書類を準備し、潜在的な取引先に提供する。特に、入札書類には以下が含まれることが望ましい。 1）調達する製品またはサービスの仕様 2）供給者が製品またはサービスを供給している間に従うセキュリティ要件 3）製品またはサービスの供給中に従うべきサービスレベル及びその指標 4）セキュリティ要件に違反した場合に、委託元が課す可能性のある罰則 5）取引先の選定プロセス中に送信されるデータやシステムなどを保護するための秘密保持条項 ・組織は、取引先によるセキュリティ管理策の遵守状況を継続的にモニタリングするための、プロシージャを整備する。 ・取引先におけるセキュリティインシデントが自組織に影響した場合に備え、契約書にて外部事業者との責任分界点を明確にし、外部事業者の責任範囲において自組織に被害が発生した場合の損害賠償について記載する等の対応を行う。
						Basic	・組織は、該当する法規制等を参照して、取引先（特に、自組織のデータを取り扱う可能性のある、またはデータを取り扱うための基盤を提供する可能性のあるもの）に対して適用するセキュリティ対策基準を策定し、内容について合意する。 ・組織は、取引先（外部情報システムサービスのプロバイダ）に対して、サービスの使用に必要な機能、ポート、プロトコル及び他のサービスを明確にする。 [参考] 取引先に対して適用するセキュリティ対策基準の策定に当たり、ISO/IEC 27001 附属書Aの管理策をベースに作成された「情報セキュリティベンチマーク」(IPA)や、「サプライチェーン情報セキュリティ管理基準」（日本セキュリティ監査協会）等を参考とすることが可能である。
				CPS.SC-2	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	H-Advanced	・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 ・取引先において、事業への悪影響を及ぼすセキュリティインシデントが発生した際の、自組織への影響の内容及び、その起こりやすさ、規模を推定する。 ※ 関連する対策要件に、CPS.AM-6, CPS.BE-2等がある。
						Advanced	・組織は、自組織のミッション/業務プロセスに重要な影響を及ぼしうるサプライチェーン上の取引先を特定し、当該組織が自組織のセキュリティポリシーに規定されているセキュリティ上の役割と責任を果たせるかどうかを確認する。
						Basic	・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 ・組織は、長期に渡ってIoT機器が使用されることが想定される場合、問い合わせ窓口やサポート体制等の適切な管理体制が整備されており、販売後のセキュリティサポート方針を明確にしている等、長期間のサポートが期待できる取引先（IoT機器ベンダ）を選定する。 ・組織は、IoT機器のサポート終了時に機器を入れ替えることの要否についてシステムの導入前に取引先（IoT機器ベンダ）に対して確認する。 ・組織は、下記の観点を確認することにより、ITサービスのマネジメントを効率的、効果的に運営管理するサービスプロバイダーを選定することが望ましい。 - JIS Q 20000 に基づく第三者認証（ITSMS認証）を取得している - 自己適合確認を通じて認証取得相当の対策の実装を確認している

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.SC-3	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織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。	H-Advanced	・組織は、システム・モノ・サービスのいずれかを提供する取引先との契約において、当該組織に対して、以下の実施を要求する。 - 契約にて指定されたセキュリティ対策を実施したエビデンスの作成、セキュリティテスト／評価結果の提示 - セキュリティテスト／評価時に特定された欠陥の修正計画の策定 - 欠陥の修正計画及び、その実施状況の提示 ・組織は、直接の委託先に対して要求しているセキュリティ対策に関する要求事項及びそれに付随する要求事項の内で必要な事項を、サプライチェーンに由来するリスクの大きさ等を勘案しつつ、再委託先以降の組織に対して（場合によっては再委託先以降の全サプライヤーに対して）も適用することが望ましい。 [参考] 委託契約に含め、実施を確認することが望ましい項目に関する追加の情報の取得のためには、「ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」(IPA, 2018年)の「3.2. IT サプライチェーン リスクマネジメント の全体像」等を参照することが可能である。
						Advanced	・組織のミッション／業務ニーズに応じて、システム、モノ、またはサービスの調達契約に以下の要求事項、記述及び基準を記載する。 - セキュリティ対策に関する要求事項 - セキュリティ関連のドキュメントに関する要求事項 - セキュリティ関連のドキュメントの保護に関する要求事項 - 秘密保持に関する条項 - インシデントが発生した際の報告先、報告内容、初動、調査、復旧等の各対応の実施主体、実施方法 - 自組織または認可された第三者によって監査され、定義されたセキュリティ要件への遵守を確認することを許可する条件 - 契約終了後の情報資産の扱い ・組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施し、委託内容の特性等により必要と認められる場合、調達契約において、追加で対策を導入することを要求する。 ・法規制等を参照してセキュリティ要件を決定し、取引先へ遵守を要求する際、下記を事前に考慮することが望ましい。 - 自組織と取引先との法令の相違（例：業法の違い、国・地域の違い）により生じるコンプライアンス上のリスクの特定 - 取引先に適用される法律及び規制上の義務によるセキュリティの観点からの契約への悪影響
						Basic	・組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施することを要求する。 ・組織は、委託先の選定、評価のプロセスにおいて、取引先がセキュリティアクションを宣言していることを確認する。
		A.15.1.3 ICTサプライチェーン	供給者との合意には，情報通信技術（ICT）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めなければならない。	CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	H-Advanced	・調達する機器に対して、契約におけるセキュリティ要求事項が満たせているかを、自組織あるいは第三者がテストする。 ・組織は、自組織のオペレーションにとって特に重要な機器について、再委託先以降の組織を含む関係するサプライチェーン全体に渡り、一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロシージャで製造されたものかを確認する。
						Advanced	・組織は、契約において、例えば下記のように、取引先から調達する製品・サービスが具備すべきセキュリティ要求事項を明確化する。 - セキュリティに関わる特定の認証（例：ISMS認証、ISASecure EDSA認証、ITセキュリティ評価及び認証制度(JISEC)）を有していること - ベンダー自身により、セキュリティに関わる特定の認証の基準に適合する対策を実施していることが確認されていること - リスク分析の結果等から導かれた必要なセキュリティ要件を設計時からの実装（セキュリティ・バイ・デザイン）し、検査していること ・組織は、調達計画時に、製品またはサービス自体、あるいは当該製品・サービスの調達・供給にて使用される資産の保護に係るセキュリティ要件の費用を確保しておくことが望ましい。 ・下記を含む製品またはサービスの調達または供給を評価するためのセキュリティ測定ルールを策定し、運用及び改善する。 - 測定対象の内容 - 措置の報告方法、報告の頻度 - 措置が実施されない場合に遂行される措置 ・組織は、搬送中の改ざん・漏えいを検知(又は抑止)する手段とともに納品されるIoT機器やソフトウェアが、不正操作されていないかを確認する。 - 物品：セキュリティ便、プロテクトシール等 - 電送：暗号化、電送データ全体のハッシュ値等
	A.15.2 供給者のサービス提供の管理	A.15.2.1 供給者のサービス提供の監視及びレビュー	組織は，供給者のサービス提供を定常的に監視し，レビューし，監査しなければならない。	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、その内容について取引先と合意する。	Advanced	・組織は、サプライチェーンに係るセキュリティ対策基準を参照して、ITT(Invitation To Tender)やRFP(Request For Proposal)などの入札書類を準備し、潜在的な取引先に提供する。特に、入札書類には以下が含まれることが望ましい。 1）調達する製品またはサービスの仕様 2）供給者が製品またはサービスを供給している間に従うセキュリティ要件 3）製品またはサービスの供給中に従うべきサービスレベル及びその指標 4）セキュリティ要件に違反した場合に、委託元が課す可能性のある罰則 5）取引先の選定プロセス中に送信されるデータやシステムなどを保護するための秘密保持条項 ・組織は、取引先によるセキュリティ管理策の遵守状況を継続的にモニタリングするための、プロシージャを整備する。 ・取引先におけるセキュリティインシデントが自組織に影響した場合に備え、契約書にて外部事業者との責任分界点を明確にし、外部事業者の責任範囲において自組織に被害が発生した場合の損害賠償について記載する等の対応を行う。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.SC-6	・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。	H-Advanced	・組織は、契約事項からの逸脱及び、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先及びその再委託先以降の組織に対して、契約にて規定した組織のセキュリティマネジメント、納入する製品・サービスに実装されるセキュリティ機能等に関する義務事項が履行されているかどうかを一覧化して確認できるメカニズムを利用する。 ・委託元による実地調査、外部監査等の手法により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。 ・重要な取引先及びその再委託先以降の組織は、関係する攻撃の予兆、情報流出の事実がないかを調査し、組織に対して結果を定期的に報告する。
						Advanced	・組織は、自組織が取引先との契約において要求事項として規定した内容に関連して、システム上での監査が可能かどうか、確認する。 ・上記で定義されているシステム上で監査可能なイベントのために、監査記録を生成する機能を情報システムが提供する。 ・組織は、監査に関連する情報が必要な他の組織との間で、セキュリティ監査の整合性を保つことができるようにする。 ・組織は、手作業ないしは情報システムにより自動で生成された監査記録を定期的にでレビュー・分析して、契約事項からの逸脱及び、その兆候の有無を確認する。 ・チェックリストを用いた取引先による内部監査により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。
				CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	Advanced	・組織は、遠隔保守のための接続の確立と実施に関するポリシーとプロシージャを文書化し、その内容により実施する。 ・組織は、遠隔保守を実施する際には組織の定めるネットワークアクセスに求める認証を実施するとともに、遠隔保守が完了したらセッションとネットワーク接続を確実に終了する。
						Basic	・組織は、遠隔保守の実施に当たっては、実施計画を策定し・合意した上で実施し、実施結果を確認する。 ・組織は、実施した遠隔保守の実施記録を保管する。
				CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	H-Advanced	・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル及び他のサービスを明確にするよう要求する。 ・組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。
						Advanced	・組織は、外部サービスプロバイダ及びシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報，業務システム及び業務プロセスの重要性並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスををモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。
						Basic	・組織は、外部情報システムサービスのプロバイダ及びシステム開発の委託先に対して、自組織が対象となっている、あるいは当該プロバイダーが対象として該当するルールに従って、例えば、下記に関連するようなセキュリティ要求事項を設定し、導入することを要求する。 - （例えば、ISMS認証取得相当の）セキュリティ対策が十分に行われていること - 運用中のデータが適切に管理されること - サービス利用終了時にデータが適切に削除されること
		A.15.2.2 供給者のサービス提供の変更に対する管理	関連する業務情報，業務システム及び業務プロセスの重要性，並びにリスクの再評価を考慮して，供給者によるサービス提供の変更（現行の情報セキュリティの方針群，手順及び管理策の保守及び改善を含む。）を管理しなければならない。	CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	H-Advanced	・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル及び他のサービスを明確にするよう要求する。 ・組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。
						Advanced	・組織は、外部サービスプロバイダ及びシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報，業務システム及び業務プロセスの重要性並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダ及びシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスををモニタリングする。 ・組織は、外部サービスプロバイダー及びシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
A.16 情報セキュリティインシデント管理	A.16.1 情報セキュリティインシデントの管理及びその改善	A.16.1.1 責任及び手順	情報セキュリティインシデントに対する迅速，効果的かつ順序だった対応を確実にするために，管理層の責任及び手順を確立しなければならない。	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。	H-Advanced	・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、インシデント対応要件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。 [参考] サプライチェーンにおけるセキュリティインシデントには、たとえば、システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害等がある。
						Advanced	・組織は、セキュリティインシデントにより第1の処理拠点の可用性が低下した場合に利用する代替処理拠点を定める。 ・組織は、自組織の一次処理機能が利用できない場合に、自組織が定める目標復旧時間内に、代替処理拠点により所定のオペレーションを移転・再開して、重要なミッション／業務機能を遂行できるようにするようサービス契約で規定する。 ・組織は、同じ脅威に対する脆弱さを減らすために、一次処理拠点から離れた代替処理拠点を指定する。 ・組織は、情報システム及び産業用制御システムのユーザにセキュリティインシデントの対応と報告に関する助言と支援を提供する、組織のインシデント対応能力に不可欠な、インシデント対応支援リソース（ヘルプデスク、CSIRT等）を自組織に用意する。
						Basic	・セキュリティインシデントを発見した場合、速やかにIPA、JPCERT/CC等の関係機関に報告し、対応の支援、発生状況の把握、手口の分析、再発防止のための助言等を受ける。
		A.16.1.2 情報セキュリティ事象の報告	情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけ速やかに報告しなければならない。	CPS.SC-5	・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。	H-Advanced	・組織は、委託先の要員により委託元が要求するセキュリティ要求事項が遵守されているかどうかを継続的にモニタリングし、通常とは異なる行動があった場合、自組織の担当者に通知できるようにプロシージャを整備する。
						Advanced	・サプライヤー関係のセキュリティ面について該当する要員を訓練し、機密情報の取り扱いが正しく理解されていることを特に確認する。 ・委託業務の遂行に当たり、委託元が要求するセキュリティ要求事項が遵守されていることを定期的に確認する。
						Basic	・委託業務に係るデータの内、機密データや知的財産のように、公開または変更すべきではないものへのアクセス及びデータの開示または変更に関わる要員を特定し、評価する。 ・組織は、委託先との契約の終了後、速やかに委託先の要員に対する自組織施設へのアクセス権限等の、一時的に許可していた権限を停止する。
				CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	Advanced	・組織は、セキュリティ運用マニュアルにおいてインシデントの検知及び分析、封じ込め、低減、復旧を含む内容を規定する。 - すべてのインシデントの取り扱いに関する記録をとる - 外部組織等に対して、インシデント発生の事実と対応状況に関する報告をする必要があるかどうかを判断する
						Basic	・組織は、セキュリティインシデントの発生時に利用するセキュリティ運用プロセスを策定し、運用する。当該プロセスには、下記を例とする内容を含むことが望ましい。 - インシデントの報告を受けた者が、どのような対応をするのか、あるいはより上位に報告するのかの判断基準 - 緊急時の指揮命令と対応の優先順位の決定 - インシデントへの対応（インシデントレスポンス） - インシデントの影響と被害の分析 - 情報収集と自社に必要な情報の選別 - 社内関係者への連絡と周知 - 外部関係機関との連絡 ・システム（特に産業用制御システム）は、IoT機器、サーバ等に異常（誤動作等）が発生した場合に、緊急停止、管理者へのアラート通知等のフェールセーフのための対応を実施する。 [参考] セキュリティインシデント発生時の対応手順の検討において、「インシデントハンドリングマニュアル」(JPCERT/CC, 2015年)、SP 800-61 Rev.1 (NIST, 2008年)、「インシデント対応マニュアルの作成について」(JPCERT/CC, 2015年)を参照することが可能である。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				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。	H-Advanced	・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、インシデント対応要件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。 [参考] サプライチェーンにおけるセキュリティインシデントには、たとえば、システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害等がある。
						Advanced	・組織は、セキュリティインシデントにより第1の処理拠点の可用性が低下した場合に利用する代替処理拠点を定める。 ・組織は、自組織の一次処理機能が利用できない場合に、自組織が定める目標復旧時間内に、代替処理拠点により所定のオペレーションを移転・再開して、重要なミッション／業務機能を遂行できるようにするようサービス契約で規定する。 ・組織は、同じ脅威に対する脆弱さを減らすために、一次処理拠点から離れた代替処理拠点を指定する。 ・組織は、情報システム及び産業用制御システムのユーザにセキュリティインシデントの対応と報告に関する助言と支援を提供する、組織のインシデント対応能力に不可欠な、インシデント対応支援リソース（ヘルプデスク、CSIRT等）を自組織に用意する。
						Basic	・セキュリティインシデントを発見した場合、速やかにIPA、JPCERT/CC等の関係機関に報告し、対応の支援、発生状況の把握、手口の分析、再発防止のための助言等を受ける。
		A.16.1.3 情報セキュリティ弱点の報告	組織の情報システム及びサービスを利用する従業員及び契約相手に，システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は，どのようなものでも記録し，報告するように要求しなければならない。	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。	H-Advanced	・組織は、セキュリティ事象の追跡と、事象に関係する脅威収集・脆弱性等の情報の収集及び分析を支援する自動化されたメカニズムを使用して、セキュリティインシデントの分類（トリアージ）等に活用する。
						Advanced	・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位及びメトリクスを考慮してインシデントを分類する。 ・組織は、自組織に影響を及ぼすセキュリティインシデントを追跡し、文書化する。「SP 800-61 Rev.1」では、セキュリティインシデントを文書化する際の記載の観点として、下記を例示している。 - インシデントの現在の状況 - インシデントの概要 - 当該インシデントに対して自組織のとった行動の内容 - ほかの関係者(システム所有者、システム管理者等)の連絡先情報 - 調査の際に収集した証拠の一覧 - インシデントの処理担当者からのコメント - 次にとるべきステップ
						Basic	・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 ※ CPS.AM-6, CPS.BE-2に同様の対策例を記載 ・当該セキュリティ事象のもたらす影響の大きさを考慮し、報告義務のあるインシデントを定める。 [参考] セキュリティインシデントの影響の大きさを測るための尺度を検討する場合、下記文書等を参照することができる。 ・SP 800-61 Rev.1 (NIST, 2008年) 3.2.6 事件の優先順位付け ・「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準」(NISC, 2018年)
		A.16.1.4 情報セキュリティ事象の評価及び決定	情報セキュリティ事象は，これを評価し，情報セキュリティインシデントに分類するか否かを決定しなければならない。	CPS.AE-5	・セキュリティ事象の危険度の判定基準を定める。	H-Advanced	・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 ※ CPS.AM-6, CPS.BE-2に同様の対策例を記載 ・組織は、セキュリティ事象の追跡と、事象に関係する脅威収集・脆弱性等の情報の収集及び分析を支援する自動化されたメカニズムを使用して、セキュリティ事象の分類（トリアージ）等に活用する。
						Advanced	・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位及びメトリクスを考慮してインシデントを分類する。
						Basic	・当該セキュリティ事象のもたらす影響の大きさを考慮し、報告義務のあるインシデントを定める。 [参考] セキュリティ事象の影響の大きさを測るための尺度を検討する場合、下記文書等を参照することができる。 ・SP 800-61 Rev.1 (NIST, 2008年) 3.2.6 事件の優先順位付け ・「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準」(NISC, 2018年)

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				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。	H-Advanced	・組織は、セキュリティ事象の追跡と、事象に関係する脅威収集・脆弱性等の情報の収集及び分析を支援する自動化されたメカニズムを使用して、セキュリティインシデントの分類（トリアージ）等に活用する。
						Advanced	・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位及びメトリクスを考慮してインシデントを分類する。 ・組織は、自組織に影響を及ぼすセキュリティインシデントを追跡し、文書化する。「SP 800-61 Rev.1」では、セキュリティインシデントを文書化する際の記載の観点として、下記を例示している。 - インシデントの現在の状況 - インシデントの概要 - 当該インシデントに対して自組織のとった行動の内容 - ほかの関係者(システム所有者、システム管理者等)の連絡先情報 - 調査の際に収集した証拠の一覧 - インシデントの処理担当者からのコメント - 次にとるべきステップ
						Basic	・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース（関係する他組織、ヒト、モノ、データ、システム等）と機能を特定し、優先順位付けする。 ※ CPS.AM-6, CPS.BE-2に同様の対策例を記載 ・当該セキュリティ事象のもたらす影響の大きさを考慮し、報告義務のあるインシデントを定める。 [参考] セキュリティインシデントの影響の大きさを測るための尺度を検討する場合、下記文書等を参照することができる。 ・SP 800-61 Rev.1 (NIST, 2008年) 3.2.6 事件の優先順位付け ・「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準」(NISC, 2018年)
		A.16.1.5 情報セキュリティインシデントへの対応	情報セキュリティインシデントは，文書化した手順に従って対応しなければならない。	CPS.SC-5	・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。	H-Advanced	・組織は、委託先の要員により委託元が要求するセキュリティ要求事項が遵守されているかどうかを継続的にモニタリングし、通常とは異なる行動があった場合、自組織の担当者に通知できるようにプロシージャを整備する。
						Advanced	・サプライヤー関係のセキュリティ面について該当する要員を訓練し、機密情報の取り扱いが正しく理解されていることを特に確認する。 ・委託業務の遂行に当たり、委託元が要求するセキュリティ要求事項が遵守されていることを定期的に確認する。
						Basic	・委託業務に係るデータの内、機密データや知的財産のように、公開または変更すべきではないものへのアクセス及びデータの開示または変更に関わる要員を特定し、評価する。 ・組織は、委託先との契約の終了後、速やかに委託先の要員に対する自組織施設へのアクセス権限等の、一時的に許可していた権限を停止する。
				CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、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。	H-Advanced	・組織は、セキュリティ専門の24時間365日モニタリングモニタリングにより収集した監査ログを、分析自動化ツール等を利用することで効率的に分析する。 ・組織は、従来のIT環境だけでなく、制御システムやIoT機器も含めて、セキュリティ状況のモニタリングの範囲とすることが望ましい。 ・組織は、セキュリティ対応組織の成熟度を定期的に評価し、セキュリティ状況のモニタリングやインシデントへの対応等のセキュリティ関連業務を継続的に改善することが望ましい。 [参考] セキュリティ対応組織(SOC/CSIRT)を評価するためのメトリクスには、「セキュリティ対応組織成熟度セルフチェックシート」(ISOG-J, 2018年)や、SIM3(Security Incident Management Maturity Model)等がある。
						Advanced	・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。なお、相関分析の対象には、他組織とデータを連携する部分のログも含めることが望ましい。 - モニタリングするシステムの範囲をどこまでとするか - どのような機器のログを収集し、分析するか (CPS.AE-3を参照) ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する（プロセスの内容については、CPS.RP-1等を参照）。 ・組織及びシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には以下を含むことが望ましい。 - ログ分析の分析結果（対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等） - モニタリングにおける今後の改善方針 [参考] セキュリティ対応組織(SOC/CSIRT)の業務、望まれる規模等については、「セキュリティ対応組織（SOC/CSIRT）の教科書 ～機能・役割・人材スキル・成熟度 ～」(ISOG-J, 2018年)等を参照することが望ましい。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	H-Advanced	・情報システム及び産業用制御システムは、有効でないインプットデータを受け取った場合に、組織の目的とシステムの目的に沿って、予想できる形で、かつ記載どおりに動作する。
						Advanced	・組織は、セキュリティ運用マニュアルにおいてインシデントの検知及び分析、封じ込め、低減、復旧を含む内容を規定する。 - すべてのインシデントの取り扱いに関する記録をとる - 外部組織等に対して、インシデント発生の事実と対応状況に関する報告をする必要があるかどうかを判断する
						Basic	・組織は、セキュリティインシデントの発生時に利用するセキュリティ運用プロセスを策定し、運用する。当該プロセスには、下記を例とする内容を含むことが望ましい。 - インシデントの報告を受けた者が、どのような対応をするのか、あるいはより上位に報告するのかの判断基準 - 緊急時の指揮命令と対応の優先順位の決定 - インシデントへの対応（インシデントレスポンス） - インシデントの影響と被害の分析 - 情報収集と自社に必要な情報の選別 - 社内関係者への連絡と周知 - 外部関係機関との連絡 ・システム（特に産業用制御システム）は、IoT機器、サーバ等に異常（誤動作等）が発生した場合に、緊急停止、管理者へのアラート通知等のフェールセーフのための対応を実施する。 [参考] セキュリティインシデント発生時の対応手順の検討において、「インシデントハンドリングマニュアル」(JPCERT/CC, 2015年)、SP 800-61 Rev.1 (NIST, 2008年)、「インシデント対応マニュアルの作成について」(JPCERT/CC, 2015年)を参照することが可能である。
				CPS.MI-1	・セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う。	H-Advanced	・組織は、セキュリティインシデントの対応プロセスを支援する自動化されたメカニズムを使用する。 ・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。 [参考] 対応段階におけるインシデントの影響低減、復旧段階において有用に機能すると考えられる情報の例として、「セキュリティ対応組織 (SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0 」(ISOG-J, 2017年)では、下記が挙げられる。 ・攻撃行為をセキュリティ製品や関連するシステムで遮断するための設定要件 ・攻撃を無効化する方法（パッチの適用、設定変更等） ・被害を受けたシステム復旧方法
						Basic	・組織（あるいはその構成員）は、あらかじめ定められたプロシージャに従って、セキュリティインシデントを低減するためのアクション（例えば、システムのシャットダウン、有線/無線ネットワークからの切断、モデムケーブルの切断、特定の機能の無効化など）を実行する。 [参考]セキュリティインシデントの影響低減のための活動は、インシデントの性質（例えば、サービス拒否攻撃、マルウェア感染、不正アクセスのような顕在化する脅威の差異）により内容が異なる場合がある。より詳細な影響低減活動の情報については、「インシデントハンドリングマニュアル」(JPCERT/CC, 2015年)、SP 800-61 Rev.1 (NIST, 2008年)等を参照することが望ましい。
		A.16.1.6 情報セキュリティインシデントからの学習	情報セキュリティインシデントの分析及び解決から得られた知識は，インシデントが将来起こる可能性又はその影響を低減するために用いなければならない。	CPS.IP-7	・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	H-Advanced	・組織は、第三者によるセキュリティ評価を実施する。
						Advanced	・組織は、セキュリティ評価を適切かつ計画的に実施するため、以下に示す事項を含めたセキュリティ評価計画を策定した上で、セキュリティ評価を実施する。 -セキュリティ評価の対象とするセキュリティ対策 -セキュリティ対策の有効性を図るために用いる評価手順 -セキュリティ評価を実施する環境や実施体制 -セキュリティ評価結果の取りまとめ方法とその活用方法
						Basic	・組織は、セキュリティ対策が正しく実装されているか及び運用されているかに加え、セキュリティ対策が期待された成果を上げているかに関する定期的に評価（セキュリティ評価）を実施し、管理責任者へ報告する。 ・組織は、セキュリティ評価の結果に基づき、セキュリティ対策の改善を実施する。
				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。	H-Advanced	・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、自動化されたメカニズムを通じて適切なパートナーと適時双方向で共有をすることができる環境を整備する。
						Advanced	・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、パートナーに適時共有することができる環境を整備する。
						Basic	・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、適切なパートナーから入手できる環境を整備する。 [参考] 適切なパートナーを選定するに当たり、「情報セキュリティサービス基準適合サービスリスト」に記載された事業者のサービスを利用することが考えられる。また、パートナーには、情報処理安全確保支援士やCISSP等のセキュリティに係る資格を有している要員を含めることが望ましい。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
				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。	H-Advanced	・組織は、検知能力向上のため、様々な情報ソースをもとに、検知ルールの作成とチューニングを行う - 相関分析ルールの開発 - IPS/IDSの独自シグネチャの開発 - 独自ブラックリストの開発 ・組織／システムは、システムの通信やセキュリティアラートのパターンを分析し、典型的な通信パターン及びセキュリティアラートを集約したプロファイルを作成、活用することで、誤検出の数や、検出漏れの数を減らすためのチューニングを行う。
						Advanced	・組織は、経営層等の組織内の然るべき要員に、定期的に組織及びシステムのセキュリティの状態を報告するプロシージャを整備し、運用する。組織は、報告の場を最新の脅威や残存するリスクに対する脅威を認識し、セキュリティを向上するための場とすることが望ましい。 ・例えば、以下のような注意喚起情報の発信があった際等に、セキュリティに係るリスク増加の兆候がある場合、信頼できる情報源からの情報に基づいて、システムのモニタリング活動のレベルを上げる。　※以下のリストは、「セキュリティ対応組織 (SOC,CSIRT) 強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0」(ISOG-J, 2017年)より引用している。 ・ 攻撃の特徴 攻撃の特徴 ➢ 攻撃形態、関連する通信の内容 ➢ 核心となる攻撃コード ・ 攻撃によって残る痕跡 ➢ 被害を受けた後の通信内容 ➢ サーバやクライアントに残るログ ➢ サーバやクライアントに残るその他特徴 ・ 各セキュリティ製品における検知名
				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。	H-Advanced	・情報システムが、発生したセキュリティインシデントの形態，規模及び費用を定量化及び監視できるようにする自動的なメカニズムを備えることが望ましい。
						Basic	・セキュリティインシデントの評価から得た脅威情報、脆弱性情報等は、再発する又は影響の大きいインシデントを特定するために利用することが望ましい。 ・セキュリティインシデントへの対応活動から学んだ教訓を事業継続計画又は緊急事対応計画、教育／訓練に取り入れて、結果として必要となる変更を実施する。NIST SP 800-61には、教訓を抽出する際の観点として下記が例として示されている。 - 正確に何がいつ起きたか。 - スタッフとマネジメント層がどの程度うまく事件に対処したか。文書化された手順に従ったか。それは適切だったか。 - すぐに必要になった情報は何か。 - 復旧を妨げたかもしれないステップや行動があったか。 - 次に同様の事件が起きた場合、スタッフやマネジメント層は、どのような違った行動をとるか。 - どのような是正措置があれば、将来にわたって同じ様な事件が起きるのを防げるか。 - 将来事件を検出、分析、軽減するために、どのようなツールやリソースが追加で必要となるか。
		A.16.1.7 証拠の収集	組織は，証拠となり得る情報の特定，収集，取得及び保存のための手順を定め，適用しなければならない。	CPS.AN-2	・セキュリティインシデント発生後に、デジタルフォレンジックを実施する。	H-Advanced	・情報システムが、重要なセキュリティインシデントに関する監査記録について処理するプロシージャを提供する。
						Advanced	・組織は、媒体、装置及び装置の状態（例えば、電源が入っているか、切れているか）に従って、証拠の特定、収集、取得及び保存のプロシージャを規定する。 ・組織は、重要なセキュリティインシデントについて、発生後に下記の証跡を保全することが望ましい。 - 識別情報（インシデントの発生場所／発生日時／対象となるモノのシリアル番号／ホスト名／MACアドレス／IPアドレス等） - 証跡を収集・処理したヒトの役職、名前、連絡先 - 証跡保全処理の日時（タイムゾーンを含む）
						Basic	・組織は，証拠となり得るデータを特定、収集、取得及び保存するためのプロシージャを定め、運用する。
A.17 事業継続マネジメントにおける情報セキュリティの側面	A.17.1 情報セキュリティ継続	A.17.1.1 情報セキュリティ継続の計画	組織は，困難な状況（adverse situation）（例えば，危機又は災害）における，情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しなければならない。	CPS.RP-3	・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。	Advanced	・組織は、情報システム、産業用制御システム及び関係するプロセスの管理者を含めて、有事における事業継続のための体制を構築する。事業継続に支障をもたらす事象が発生した際には、この体制が、運用を再確立するためのシステムの優先順位を決定する。 ・組織は、災害等と比較して被害状況が見えづらく事業継続計画の発動タイミングが不明確、インシデントの原因究明の重要性が高い等の特徴を有するセキュリティインシデントに特化した事業継続計画又は緊急事対応計画を策定し、運用する。 ・組織は、セキュリティインシデントに特化した事業継続計画又は緊急事対応計画を策定する際、組織全体の事業継続に係る方針と合致するような内容とすることを確実にする。
				CPS.RP-4	・セキュリティ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。	Advanced	・組織は、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。 ・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動及びインシデントの事後処理に関わる活動を調整する。その際、CPS.AM-2, CPS.AM-3にて記載している方法により、対応の対象となるモノを特定していることが望ましい。 ※ CPS.CO-3と関連
						Basic	・自組織の業種等を考慮して、事業継続計画又は緊急事対応計画の中に、インシデント発生後の生産したモノへの対応について記載するかを検討する。その際、事業継続計画又は緊急事対応計画は、必ずしもセキュリティインシデントを想定したものでない場合も許容されるものとする。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
	A.17.1.2 情報セキュリティ継続の実施		組織は，困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための，プロセス，手順及び管理策を確立し，文書化し，実施し，維持しなければならない。	CPS.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	H-Advanced	・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、インシデント対応要件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。 [参考] サプライチェーンにおけるセキュリティインシデントには、たとえば、システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害等がある。
						Advanced	・組織は、セキュリティインシデントにより第1の処理拠点の可用性が低下した場合に利用する代替処理拠点を定める。 ・組織は、自組織の一次処理機能が利用できない場合に、自組織が定める目標復旧時間内に、代替処理拠点により所定のオペレーションを移転・再開して、重要なミッション／業務機能を遂行できるようにするようサービス契約で規定する。 ・組織は、同じ脅威に対する脆弱さを減らすために、一次処理拠点から離れた代替処理拠点を指定する。 ・組織は、情報システム及び産業用制御システムのユーザにセキュリティインシデントの対応と報告に関する助言と支援を提供する、組織のインシデント対応能力に不可欠な、インシデント対応支援リソース（ヘルプデスク、CSIRT等）を自組織に用意する。
				CPS.CO-3	・復旧活動について内部及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、事業継続計画又は緊急事対応計画の中に位置づける。	Advanced	・組織は、監督官庁、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。 ・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動及びインシデントの事後処理に関わる活動を調整する。ここで該当する活動の例として、生産システムにおけるセキュリティインシデント発生時に生産されたモノの回収等が挙げられる。
						Basic	・組織は、自組織に影響を及ぼすようなセキュリティインシデント発生時における役割、責任、そうした役割と責任を割り当てられたヒトと連絡先情報を示す。 ・組織は、事業継続に関わる意思決定の責任が割り当てられたヒトに対して、意思決定をより適切なものとするため、セキュリティインシデントの概要や被害状況に関する説明を実施する。
		A.17.1.3 情報セキュリティ継続の検証，レビュー及び評価	確立及び実施した情報セキュリティ継続のための管理策が，困難な状況の下で妥当かつ有効であることを確実にするために，組織は，定められた間隔でこれらの管理策を検証しなければならない。	CPS.IM-2	・セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又は緊急事対応計画を継続的に改善する。	Basic	・組織は、セキュリティインシデントへの対応から、事業継続のためのプロシージャ及び関連する対策の機能が、事業継続のより上位の方針と合致しているかを確認する。 ・セキュリティインシデントへの対応活動から学んだ教訓を事業継続計画又は緊急事対応計画、教育／訓練に取り入れて、結果として必要となる変更を実施する。
	A.17.2 冗長性	A.17.2.1 情報処理施設の可用性	情報処理施設は，可用性の要求事項を満たすのに十分な冗長性をもって，導入しなければならない。	CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する。	Advanced	・情報システム及び産業用制御システムは、予備の容量／帯域幅／その他の予備リソース（ヒト／モノ／システム等）を管理して、大量の情報を送りつけるタイプのサービス拒否攻撃による影響を最小限に抑える。例えば、攻撃を受けているシステムが提供するサービスを、可用性の水準維持等の理由により停止できない場合、重要な機能を継続するため、以下のような対策をとる必要がある。 - 待機している予備システムへの自動的、あるいは、人手を介した移行 - ネットワークアクセスからの攻撃を受けたシステム構成要素の、自動的あるいは人手を介した隔離 ・要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整しなければならず，また，将来必要とする容量・能力を予測しなければならない。 ・組織は、 (a) 情報システムに対するサービス妨害攻撃の兆候を発見するための組織が定めた、モニタリングツールを使用する (b) 組織が定めた情報システム及び産業用制御システムのリソースをモニタリングして、効果的なサービス妨害攻撃を阻止するための十分なリソースが確保されているかどうかを判断する
						Basic	・情報システム及び産業用制御システムは、組織が定めたセキュリティ対策を実施することによって、組織が定めたタイプのサービス拒否攻撃、またはそうした情報の情報源への参照のサービス拒否攻撃による影響から保護する、あるいはそうした影響を最小限に抑え、縮退運転を実施する機能を提供する。
				CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	Advanced	・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。
						Basic	・組織は、情報システム及び産業用制御システムに要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測する。 ・組織は、サポートユーティリティの不具合による停電、その他の故障から装置を保護する。 ・組織は、データを伝送する又はサービスをサポートする通信ケーブル及び電源ケーブルの配線を傍受、妨害又は損傷から保護する。 ・組織は、可用性及び完全性を継続的に維持することを確実にするために、装置を正しく保守する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
A.18 順守	A.18.1 法的及び契約上の要求事項の順守	A.18.1.1 適用法令及び契約上の要求事項の特定	各情報システム及び組織について，全ての関連する法令，規制及び契約上の要求事項，並びにこれらの要求事項を満たすための組織の取組みを，明確に特定し，文書化し，また，最新に保たなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	Basic	・自組織の事業活動において、セキュリティの文脈で関連するすべての法令、規制及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組みを明確に特定し、文書化する。 ・要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文書化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全ての国における遵守を考慮する。 [参考] 情報セキュリティ関連法令には、例えば、不正競争防止法、電子署名認証法、e-文書法、個人情報保護法、不正アクセス禁止法等がある。また、上記の法令等の遵守に際しては、関連各省庁から発出されているガイドライン文書等（例：不正競争防止法：「営業秘密管理指針」(経済産業省, 2019年)、「限定提供データに関する指針」(2019年, 1月)、個人情報保護法：「個人情報の保護に関する法律についてのガイドライン(通則編)」(個人情報保護委員会, 2019年)、「個人情報の保護に関する法律についてのガイドライン(匿名加工情報編)」(個人情報保護委員会, 2017年)）を参照することが望ましい。
				CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)
				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。	Basic	・組織は、モニタリング業務に関係する法制度、業界標準、顧客との契約事項等が存在するか、存在するならばどのような制約があるかを認識する。 ・組織は、上記で認識したルールに準拠してモニタリングを実施し、セキュリティ事象を検知する。 ・組織は、自組織のモニタリング活動がルールに準拠したものかどうかを定期的にレビューし、確認する。
		A.18.1.2 知的財産権	知的財産権及び権利関係のあるソフトウェア製品の利用に関連する，法令，規制及び契約上の要求事項の順守を確実にするための適切な手順を実施しなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	Basic	・自組織の事業活動において、セキュリティの文脈で関連するすべての法令、規制及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組みを明確に特定し、文書化する。 ・要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文書化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全ての国における遵守を考慮する。 [参考] 情報セキュリティ関連法令には、例えば、不正競争防止法、電子署名認証法、e-文書法、個人情報保護法、不正アクセス禁止法等がある。また、上記の法令等の遵守に際しては、関連各省庁から発出されているガイドライン文書等（例：不正競争防止法：「営業秘密管理指針」(経済産業省, 2019年)、「限定提供データに関する指針」(2019年, 1月)、個人情報保護法：「個人情報の保護に関する法律についてのガイドライン(通則編)」(個人情報保護委員会, 2019年)、「個人情報の保護に関する法律についてのガイドライン(匿名加工情報編)」(個人情報保護委員会, 2017年)）を参照することが望ましい。
				CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.18.1.3 記録の保護	記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊，改ざん，認可されていないアクセス及び不正な流出から保護しなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	Basic	・自組織の事業活動において、セキュリティの文脈で関連するすべての法令、規制及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組みを明確に特定し、文書化する。 ・要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文書化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全ての国における遵守を考慮する。 [参考] 情報セキュリティ関連法令には、例えば、不正競争防止法、電子署名認証法、e-文書法、個人情報保護法、不正アクセス禁止法等がある。また、上記の法令等の遵守に際しては、関連各省庁から発出されているガイドライン文書等（例：不正競争防止法：「営業秘密管理指針」(経済産業省, 2019年)、「限定提供データに関する指針」(2019年, 1月)、個人情報保護法：「個人情報の保護に関する法律についてのガイドライン(通則編)」(個人情報保護委員会, 2019年)、「個人情報の保護に関する法律についてのガイドライン(匿名加工情報編)」(個人情報保護委員会, 2017年)）を参照することが望ましい。
				CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)
				CPS.SC-8	・自組織が関係する他組織及び個人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。	H-Advanced	・組織は、取引先、第三者的な監査機関等の関係する他組織からのリアルタイムでのニーズに柔軟に応じるため、下記の特徴を有した証跡保管システムを利用する。 - 対象となる監査証跡の契約事項に対する適格性を高速で検証することができる - 取引先や委託を受けた監査機関等の許可を受けたエンティティのみがアクセスできる - 保管されているデータが、タイムスタンプや電子署名により証跡としての信頼性を有している
						Advanced	・組織は、システムによって生成された監査記録のうち長期にわたって取得する監査記録を確実に取得できるよう、対策を実施する。 ・システムは、監査記録を次の脅威から保護するため、粒度の高いアクセス制御等を監査記録を保存するモノ、システムに適用することが望ましい。 - 記録されたメッセージ形式の変更 - ログファイルの変更又は削除 - ログファイル媒体の記録容量超過
						Basic	・組織は、法規制等により要求される事項を満たす事ができるよう、適切な期間の監査記録を保持する。
				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、テストする。	H-Advanced	・組織は、バックアップ情報を定期的にテストして、媒体の信頼性と情報の完全性を確認する。
						Advanced	・組織は、自組織のシステムドキュメントのバックアップを定めたタイミングや頻度で実施する。 ・組織は、保管拠点におけるバックアップ情報の機密性・完全性・可用性を保護する。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件		対策例
		A.18.1.4 プライバシー及び個人を特定できる情報（PII）の保護	プライバシー及び PII の保護は，関連する法令及び規制が適用される場合には，その要求に従って確実にしなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	Basic	・自組織の事業活動において、セキュリティの文脈で関連するすべての法令、規制及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組みを明確に特定し、文書化する。 ・要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文書化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全ての国における遵守を考慮する。 [参考] 情報セキュリティ関連法令には、例えば、不正競争防止法、電子署名認証法、e-文書法、個人情報保護法、不正アクセス禁止法等がある。また、上記の法令等の遵守に際しては、関連各省庁から発出されているガイドライン文書等（例：不正競争防止法：「営業秘密管理指針」(経済産業省, 2019年)、「限定提供データに関する指針」(2019年, 1月)、個人情報保護法：「個人情報の保護に関する法律についてのガイドライン(通則編)」(個人情報保護委員会, 2019年)、「個人情報の保護に関する法律についてのガイドライン(匿名加工情報編)」(個人情報保護委員会, 2017年)）を参照することが望ましい。
				CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)
		A.18.1.5 暗号化機能に対する規制	暗号化機能は，関連する全ての協定，法令及び規制を順守して用いなければならない。	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	Basic	・自組織の事業活動において、セキュリティの文脈で関連するすべての法令、規制及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組みを明確に特定し、文書化する。 ・要求事項を満たすための具体的な管理策及び具体的な責任についても定め、文書化する。 ・管理者は、その事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。 ・組織が他の国で事業を営む場合には、管理者は、関連する全ての国における遵守を考慮する。 [参考] 情報セキュリティ関連法令には、例えば、不正競争防止法、電子署名認証法、e-文書法、個人情報保護法、不正アクセス禁止法等がある。また、上記の法令等の遵守に際しては、関連各省庁から発出されているガイドライン文書等（例：不正競争防止法：「営業秘密管理指針」(経済産業省, 2019年)、「限定提供データに関する指針」(2019年, 1月)、個人情報保護法：「個人情報の保護に関する法律についてのガイドライン(通則編)」(個人情報保護委員会, 2019年)、「個人情報の保護に関する法律についてのガイドライン(匿名加工情報編)」(個人情報保護委員会, 2017年)）を参照することが望ましい。
				CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
	A.18.2 情報セキュリティのレビュー	A.18.2.1 情報セキュリティの独立したレビュー	情報セキュリティ及びその実施の管理（例えば，情報セキュリティのための管理目的，管理策，方針，プロセス，手順）に対する組織の取組みについて，あらかじめ定めた間隔で，又は重大な変化が生じた場合に，独立したレビューを実施しなければならない。	CPS.IP-7	・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	H-Advanced	・組織は、第三者によるセキュリティ評価を実施する。
						Advanced	・組織は、セキュリティ評価を適切かつ計画的に実施するため、以下に示す事項を含めたセキュリティ評価計画を策定した上で、セキュリティ評価を実施する。 -セキュリティ評価の対象とするセキュリティ対策 -セキュリティ対策の有効性を図るために用いる評価手順 -セキュリティ評価を実施する環境や実施体制 -セキュリティ評価結果の取りまとめ方法とその活用方法
						Basic	・組織は、セキュリティ対策が正しく実装されているか及び運用されているかに加え、セキュリティ対策が期待された成果を上げているかに関する定期的に評価（セキュリティ評価）を実施し、管理責任者へ報告する。 ・組織は、セキュリティ評価の結果に基づき、セキュリティ対策の改善を実施する。
		A.18.2.2 情報セキュリティのための方針群及び標準の順守	管理者は，自分の責任の範囲内における情報処理及び手順が，適切な情報セキュリティのための方針群，標準類，及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューしなければならない。	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機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	H-Advanced	・組織は、産業用制御システムのようにモノの制御等を伴うような、フィジカル空間に影響を及ぼす可能性のある新たな機器やシステムを開発する場合には、従来の製品や他の事故事例を収集・分析し、セキュリティの観点も含めてセーフティに関わるハザードを特定する。 ・組織は、主に産業用制御システムにおいて、ハザードによって危害に至る状況を分析し、発生しやすさや被害の深刻度を明らかにすることで、生じるリスクを見積もる。その際、セキュリティの問題に起因するハザードの有無を確認することが望ましい。 ・組織は、産業用制御システム、またはそれが稼働する環境に大きな変化があった場合、もしくは産業用制御システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。 [参考] セーフティ設計におけるハザードの特定と分析については、「つながる世界のセーフティ＆セキュリティ設計入門」(IPA, 2015年)の4.2にて具体的な手法が記載されており、参照することが可能である。
						Advanced	・組織は、情報システム、または情報システムが稼働する環境に大きな変化があった場合（新たな脅威や脆弱性の特定を含む）、もしくは情報システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。 ・組織は、新たにIoT機器を利用したシステムを企画・設計する場合、既存の資産や新たに導入するシステムにおける守るべき資産を特定し、システムの利用用途や構成に応じて、セキュリティ対策をまとめる。特に、ライフサイクルの長いモノ、システムや、高い可用性を求められるモノ、システムを扱う場合は、設計以前の段階におけるセキュリティ対策の考慮が特に重要である。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 [参考] システム及びモノにおけるセキュリティの要求仕様を検討するにあたり、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。
						Basic	・組織は、情報システム及び産業用制御システムに対するセキュリティリスクアセスメントのプロセスを定め，定期的（例えば、重要度の高い情報システムは年に1回）に適用する。 - セキュリティのリスク基準を確立し，維持する。 - 以下の方法によりセキュリティリスクを特定する。 1) 分析対象を明確化する 2) インシデント(周辺状況の変化を含む)並びにこれらの原因を特定する - 以下の方法により、セキュリティリスクを分析する。 1) 上記で特定されたリスクが実際に生じた場合に起こり得る結果について評価する 2) 上記で特定されたリスクの現実的な起こりやすさについて評価する - リスク基準を参照し、リスクのレベルを決定し、優先順位付けする ・組織は，セキュリティリスクアセスメントのプロセスを文書化し、保管する。 ・組織は、システムにセキュリティインシデントが発生した際に想定される被害の大きさやセキュリティインシデントが発生する蓋然性（例：インターネットにつながっているか）、リスクアセスメント実施に係る工数等の観点を考慮し、システムを優先順位化してリスクアセスメントの頻度等を設定することが望ましい。 [参考] セキュリティリスクアセスメントの手法として、「資産ベース」の手法及び「事業被害ベース」の手法があることが知られている。資産ベースの手法でリスクアセスメントを実施する場合は「中小企業の情報セキュリティガイドライン 第3版」（IPA, 2019年）や「制御システムのセキュリティリスク分析ガイド 第2版」(IPA, 2018年) 等を、事業被害ベースの手法を実施する場合は「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)等を参照することができる。

ISO/IEC 27001:2013 附属書A				サイバー・フィジカル・セキュリティ対策フレームワーク			
管理策ID			要求事項	対策要件ID	対策要件	対策例	
		A.18.2.3 技術的順守のレビュー	情報システムを，組織の情報セキュリティのための方針群及び標準の順守に関して，定めに従ってレビューしなければならない。	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機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	H-Advanced	・組織は、産業用制御システムのようにモノの制御等を伴うような、フィジカル空間に影響を及ぼす可能性のある新たな機器やシステムを開発する場合には、従来の製品や他の事故事例を収集・分析し、セキュリティの観点も含めてセーフティに関わるハザードを特定する。 ・組織は、主に産業用制御システムにおいて、ハザードによって危害に至る状況を分析し、発生しやすさや被害の深刻度を明らかにすることで、生じるリスクを見積もる。その際、セキュリティの問題に起因するハザードの有無を確認することが望ましい。 ・組織は、産業用制御システム、またはそれが稼働する環境に大きな変化があった場合、もしくは産業用制御システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。 [参考] セーフティ設計におけるハザードの特定と分析については、「つながる世界のセーフティ＆セキュリティ設計入門」(IPA, 2015年)の4.2にて具体的な手法が記載されており、参照することが可能である。
						Advanced	・組織は、情報システム、または情報システムが稼働する環境に大きな変化があった場合（新たな脅威や脆弱性の特定を含む）、もしくは情報システムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。 ・組織は、新たにIoT機器を利用したシステムを企画・設計する場合、既存の資産や新たに導入するシステムにおける守るべき資産を特定し、システムの利用用途や構成に応じて、セキュリティ対策をまとめる。特に、ライフサイクルの長いモノ、システムや、高い可用性を求められるモノ、システムを扱う場合は、設計以前の段階におけるセキュリティ対策の考慮が特に重要である。 ・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。 [参考] システム及びモノにおけるセキュリティの要求仕様を検討するにあたり、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。
						Basic	・組織は、情報システム及び産業用制御システムに対するセキュリティリスクアセスメントのプロセスを定め，定期的（例えば、重要度の高い情報システムは年に1回）に適用する。 - セキュリティのリスク基準を確立し，維持する。 - 以下の方法によりセキュリティリスクを特定する。 1) 分析対象を明確化する 2) インシデント(周辺状況の変化を含む)並びにこれらの原因を特定する - 以下の方法により、セキュリティリスクを分析する。 1) 上記で特定されたリスクが実際に生じた場合に起こり得る結果について評価する 2) 上記で特定されたリスクの現実的な起こりやすさについて評価する - リスク基準を参照し、リスクのレベルを決定し、優先順位付けする ・組織は，セキュリティリスクアセスメントのプロセスを文書化し、保管する。 ・組織は、システムにセキュリティインシデントが発生した際に想定される被害の大きさやセキュリティインシデントが発生する蓋然性（例：インターネットにつながっているか）、リスクアセスメント実施に係る工数等の観点を考慮し、システムを優先順位化してリスクアセスメントの頻度等を設定することが望ましい。 [参考] セキュリティリスクアセスメントの手法として、「資産ベース」の手法及び「事業被害ベース」の手法があることが知られている。資産ベースの手法でリスクアセスメントを実施する場合は「中小企業の情報セキュリティガイドライン 第3版」（IPA, 2019年）や「制御システムのセキュリティリスク分析ガイド 第2版」(IPA, 2018年) 等を、事業被害ベースの手法を実施する場合は「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)等を参照することができる。

添付Ｅ　用語集

（1）　CC（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）　CSIRT（Computer Security Incident Response Team）

コンピューターセキュリティに関連するインシデントへの対応を支援する目的で確立される機能 ; CIRT(Computer Incident Response Team)や、CIRC(Computer Incident Response Center, Computer Incident Response Capability)とも呼称されることがある。[NIST SP 800-61 Rev.2]

（3）　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 IEC 62443-2-1 に要求事項が定められている。

（4）　EDSA（Embedded Device Security Assurance）認証

IEC 62443-4-2 に基づいて、米国 ISCI（ISA Security Compliance Institute）が開発し、運営する、制御機器のセキュリティ保証に関する認証制度。ソフトウェア開発の各フェーズにおけるセキュリティ評価、セキュリティ機能の実装評価、通信の堅牢性テストという３つの観点から評価を実施する。

（5）　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。

（6）　IoT（Internet of Things）

フィジカル空間とサイバー空間からの情報を処理し、反応するサービスと相互接続されたエンティティ、ヒト、システムおよび情報資源のインフラストラクチャ。
[ISO/IEC 20924:2018 を本フレームワークの用語に合うよう一部改変]

（7）　IoT 機器

センシング、あるいはアクチュエーティングを通じてフィジカル空間と相互作用し、通信する IoT システムのエンティティ。
注記　IoT 機器とはセンサまたはアクチュエータを指す。

（8） 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。

（9） 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。

（10） 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 20000-1 に満たすべき要求事項が定められている。

（11） SOC（Security Operation Center）

セキュリティインシデントの検出、分析、対応、報告、防止を目的とした主にセキュリティアナリストから構成されるチーム。[RFC 2350, CNSS Instruction No. 4009]

（12） アクチュエータ

IoT の文脈においては、正当な入力に応答して物理的なエンティティの 1 つ以上の特性を変更する IoT 機器を指す。[ISO/IEC 20924:2018]

（13） エンティティ

物理的あるいは非物理的に、明確な存在を持つもの。[ISO/IEC 15459-3:2014]

（14） 可用性（Availability）

認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。[JIS Q 27000:2014]

（15） 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。[JIS Q 27000:2014]

（16） 完全性（Integrity）

正確さ及び完全さの特性。[JIS Q 27000:2014]

（17） 危害（harm）

人への傷害若しくは健康障害，又は財産及び環境への損害。[JIS Z 8051:2015]

（18） 機能安全

EUC（被制御機器）及び EUC 制御系の全体に関する安全のうち、E/E/PE（電気・電子・プログラマブル電子の）安全関連系及び他リスク軽減措置の正常な機能に依存する部分。[IEC 61508-4 Ed.2]

（19） 機密性（Confidentiality）

認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性。[JIS Q 27000:2014]

（20） 脅威

システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。[JIS Q 27000:2014]

（21） 公開鍵

エンティティが所有する非対称鍵ペアの鍵で、公開できるもの。

注記　非対称署名システムの場合、公開鍵は検証変換を定義する。非対称暗号化システムの場合、公開鍵は暗号化変換を定義する。“公知”の鍵は、全世界的に利用可能である必要はない。鍵は、既定のグループの全メンバーに利用可能であるだけでもよい。[JIS X 19790:2007]

（22） サービス

組織と顧客との間で必ず実行される，少なくとも一つの活動を伴う組織のアウトプット。[JIS Q 9000:2006]

（23） サービスプロバイダー

一般的に、公的機関や、その他の営利組織に対するネットワーク運用に関する基本的なサービスまたは付加価値サービスのプロバイダー。[NIST IR 4734]

（24） **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。

（25） **サイバー攻撃（Cyber attack）**

資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試み。[JIS Q 27000:2014]

（26） **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。

（27） **サプライチェーン**

複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達に始まり設計・開発・製造・加工・販売および購入者への配送に至る一連の流れ。[ISO 28001:2007、NIST SP 800-53 Rev.4]

（28） **サプライヤー**

製品またはサービスの供給のために買い手と合意した組織あるいは個人。[ISO/IEC 27036-1:2014]

（29） **産業用制御システム**

製造、製品の出荷、生産、および販売などの産業プロセスを制御するのに使用される情報システム。産業用制御システムには、地理的に分散している資産を管理するのに使用される監視制御データ収集システム（SCADA）、分散制御システム（DCS）、および前二者より小規模ながらローカルなプロセスをプログラマブル論理制御装置（PLC）の利用を通じて制御するシステムなどがある。[NIST SP 800-53 Rev.4]

（30） **識別子**

アイデンティティに関わる特定の文脈において、あるエンティティを他のエンティティと明確に区別する情報。[ISO/IEC 20924:2018]

（31） **冗長化**

機能単位が要求された機能を遂行するために十分な手段、又はデータが情報を表すのに十分な手段のほかに、別の手段を用意すること。[JIS X 0014:1999]

（32） **真正性（Authenticity）**

エンティティは、それが主張するとおりのものであるという特性。[JIS Q 27000:2014]

（33） **信頼（Trust）**

利用者又は他の利害関係者がもつ、製品又はシステムが意図したとおりに動作するという確信の度合い。[JIS X 25010:2013]

（34） **信頼性（Trustworthiness）**

信頼又は信用に値する特性。IoT の文脈では、IoT 実装のライフサイクル全体の中でセキュリティ、プライバシー、セーフティ、リライアビリティ及びレジリエンスを保証するための、信頼または信用に値する特性を指す。[ISO/IEC 20924:2018]

（35） **信頼性の基点（Basis of trustworthiness）**

信頼性を確保するための観点。

（36） **ステークホルダー**

意思決定若しくは活動に影響を与え、影響されることがある又は影響されると認知している、あらゆる人又は組織。[JIS Q 27000:2014]

（37） **脆弱性**

一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。[JIS Q 27000:2014]

（38） **脆弱性修正措置計画**

組織のシステムが直面する 1 つ以上の脅威または脆弱性を対象に、修正措置を実施するための計画。この計画には、通常、脅威や脆弱性を取り除くためのオプションと、修正措置を実施する優先順位が含まれる。[NIST SP 800-40 Ver.2.0]

（39） **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。

（40） **セーフティ（安全性）**

危害を引き起こすおそれがあると思われるハザードから守られている状態。[JIS Z 8501:2015]

(41) セキュリティインシデント

望まない単独若しくは一連のセキュリティ事象、又は予期しない単独若しくは一連のセキュリティ事象であって、事業運営を危うくする確率及びセキュリティを脅かす確率が高いもの。

(42) セキュリティ運用プロセス

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。

(43) 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。

(44) セキュリティ事象

セキュリティポリシーへの違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。

(45) セキュリティ対応組織

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。セキュリティ対応組織は、SOC, CSIRT といった組織や機能を包含する。[セキュリティ対応組織(SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0（日本セキュリティオペレーション事業者協議会(ISOG-J), 2017 年)、セキュリティ対応組織の教科書 v2.1（ISOG-J, 2018 年)、セキュリティ対応組織の教科書 ハンドブック v1.0 (ISOG-J, 2018 年)、セキュリティ対応組織の教科書 成熟度セルフチェックシート v2.2（ISOG-J, 2019 年）]

(46) 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（例：脅威分析、セキュリティアーキテクチャ、外部仕様分析、プライバシー影響評価)を組み込むこと。

(47) セキュリティポリシー

トップマネジメントによって正式に表明された組織のセキュリティに係る意図や方向付け及び、そのような意図や方向付けに基づいてセキュリティ対策を行うために組織が定めた規定。

（48） セキュリティリスク

セキュリティに関連した不具合が生じ、それによって自組織や取引先等の関係する他組織の目的、あるいは社会全体に何らかの影響が及ぶ可能性。

（49） 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。

（50） センサ

IoT の文脈では、1 つ以上の物理的なエンティティの 1 つ以上の特性を測定し、ネットワーク経由で送信可能なデジタルデータを出力する IoT 機器を指す。[ISO/IEC 20924:2018]

（51） 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。

（52） 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改ざん・読み出しの困難さを備えるデバイス。

（53） タイムスタンプ

共通の時刻基準に関して、ある時点を表す時変パラメータ。[ISO/IEC 18014-1:2008]

（54） 多要素認証（Multifactor authentication)

2 つ以上の異なる要素を使用する認証。要素には、以下をのものが含まれる：①被認証者が知っていること（例：パスワード・暗証番号）②被認証者が持っているもの（例：暗号認証デバイス・トークン）③被認証者であること（例：生体認証情報）。[NIST SP 800-53 Rev.4]

（55） 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。

（56） 認証（Authentication）

エンティティの主張する特性が正しいという保証の提供。[JIS Q 27000:2014]

(57) **ハザード**

危害の潜在的な源。[JIS Z 8051:2015]

(58) **ハッシュ関数**

任意のビット列（通常は上限が存在）を固定長のビット列に写像する関数であって、以下の 2 つの性質を満たすもの：

- 与えられた出力値について、出力値に対応する入力値を見つけることが計算上不可能であること
- 与えられた入力値について、同じ出力値に対応する 2 つ目の入力値を見つけることが計算上不可能であること [ISO/IEC 10118-1:2016]

(59) **ハッシュ値**

ハッシュ関数の出力であるビット列。 [ISO/IEC 27037:2012]

(60) **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。

(61) **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。

(62) **フィジカル空間**

現実の世界。サイバー空間と物質から構成される世界とを区別するための表現。

(63) **プロセス**

インプットをアウトプットに変換する、相互に関連する又は相互に作用する、論理的又は物理的な一連の活動。

(64) **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。

（65） **マルウェア（Malware）**

許可されていないプロセスの実施を試みることによって、情報システムの機密性・完全性・可用性に悪影響をもたらすソフトウェアまたはファームウェア。[NIST SP 800-53 Rev.4]

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。

（66） **マルチステークホルダー・プロセス**

3 者以上のステークホルダーが、対等な立場で参加・議論できる会議を通し、単体もしくは 2 者間では解決の難しい課題解決のために、合意形成などの意思疎通を図るプロセス。[内閣府]

（67） **目的**

達成する結果。[JIS Q 27000:2014]

（68） **リスク**

目的に対する不確かさの影響。[JIS Q 27000:2014]

（69） **リスク源**

それ自体又はほかとの組合せによって、リスクを生じさせる力を本来潜在的にもっている要素。[JIS Q 31000:2010]

（70） **リスクマネジメント**

リスクについて、組織を指揮統制するための調整された活動。[JIS Q 31000:2010]

（71） **レジリエンス**

システムが以下の状態を維持できること：①悪条件下にあっても、あるいは負荷が掛かった状態であっても、（顕著に低下した状態または無力化したような状態に陥ったとしても）稼働して、基礎的な運用能力を維持すること②ミッションニーズと平仄が合う時間内に、有効的に運用されている状態に復旧すること。[NIST SP 800-53 Rev.4]