参考資料２

IoT セキュリティ・セーフティ・フレームワーク

適用手順書

目 次

12 変更履歴

Version	変更年月日	変更箇所	変更内容
1.0	2022/6/2	-	新規作成

13

1. 本手順書の概要

本手順書では、IoT セキュリティ・セーフティ・フレームワーク（以下、「IoT-SSF」という。）の適用方法を以下のステップごとに説明する。

- リスクアセスメント、リスク対応に向けた事前準備 [2-1 にて詳述]
  IoT 機器・システムの概要及びシステムを構成する機器の一覧、システム構成図、データフロー図等を整理する。
- リスクアセスメント [2-2 にて詳述]
  適用範囲において、想定されるリスクやその原因を特定し、想定される被害の大きさを「第１軸：発生したインシデントの影響の回復困難性の度合い」（以下、「回復困難性の度合い」という。）や「第 2 軸：発生したインシデントの経済的影響の度合い」（以下、「経済的影響の度合い」という。）に沿って整理する。
- リスク対応 [2-3 にて詳述]
  リスク対応を行うステークホルダーが実施すべき対策を「第３軸：求められるセキュリティ・セーフティ要求の観点」（以下、「セキュリティ・セーフティ要求」という。）ごとに整理する。

各ステップで作成する成果物は以下の通り。作成手順については、各節の冒頭にて説明する。

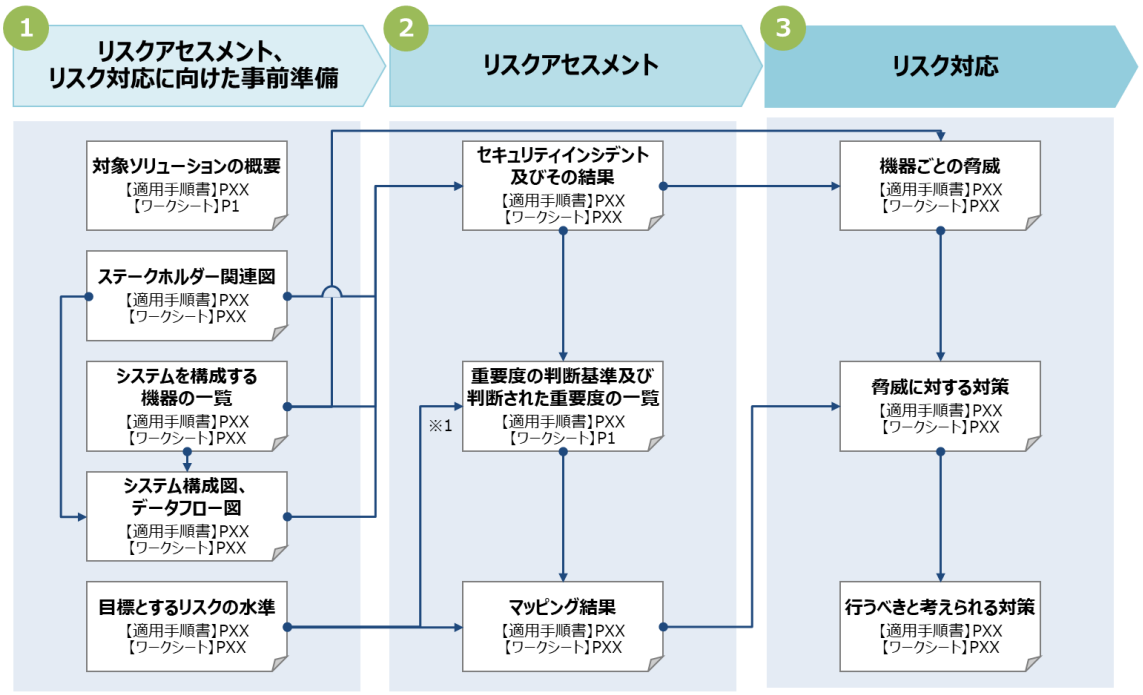

図 1 各ステップにおけるアウトプットの一覧

ここで、IoT-SSF を参照した上で IoT 機器・システム及び関連サービスにおけるリスクマネジメントを実行する主体を IoT-SSF の「適用主体」と定める。単一の事業者のみでサービス提供・利用が完結する場合は「適用主体」が当該事業者のみとなると考えられるが、複数のステークホルダーが協力して IoT 関連サービスを

提供・利用する場合、ステークホルダーが調整を行いつつ IoT-SSF を適用することが望ましい。その際には、俯瞰的な立場で IoT 関連サービスを見渡せるステークホルダーが主たる適用主体となり、他の事業者の成果を含めたとりまとめ役になると効率的に IoT-SSF を適用することが可能となる場合がある。主たる適用主体は、後述のステークホルダー関連図やシステム構成図、データフロー図等を活用して、他の事業者等に対して必要な対策の実施を依頼等することにより、当該主体間で責任分界が不明確になり、結果としてセキュリティ対策の抜け漏れが発生したり、全体の対策水準が低下する事態を防ぐ必要がある。

2. 適用手順

2-1 リスクアセスメント、リスク対応に向けた事前準備

本節では、後段のリスクアセスメントやリスク対応を実施するための基礎となる以下の情報を整理する。

(1) 対象ソリューションの概要
(2) ステークホルダー関連図
(3) システムを構成する機器の一覧
(4) システム構成図、データフロー図
(5) 目標とするリスクの水準

(1) 対象ソリューションの概要

IoT-SSFを適用するIoT機器・システムを特定し、対象ソリューションの概要を記述する。具体的には、IoT-SSF を適用する IoT 機器・システムに関する提案書やシステム全体図[1]等を参考にして、対象とするソリューションの目的や、IoT サービス利用者[2]がどのように利用するかを記述する。また、必要に応じて対象とするソリューションの IoT 機器・システムに関する前提条件を記述する。

対象ソリューションの概要を記述する際には、IoT-SSF を適用させる範囲を明確化しなければならない。IoT-SSF の適用範囲は、主たる適用主体が IoT-SSF を適用する目的と整合させることが重要である。かかる目的に整合させる形で、IoT 機器・システムを構成する要素を適用範囲とすることが望ましいが、OA 系の処理を行うための機器及びネットワークについては対象の IoT システムと直接的なかかわりがない場合は対象外としてよい。なお、IoT 機器・システムを構成する要素は以下の TIPS に示す内容が参考となる。

＜収集しておくべき情報（例）＞

- 対象機器・システムに関する提案書
- システム全体図

＜作成方法＞

1. IoT-SSF を適用する IoT 機器・システムを特定する。
2. 1.で特定されたソリューションの目的、利用シーンや提供形態を記述する。

---

[1]「システム全体図」の例：情報処理推進機構（IPA）「超上流から攻める IT 化の事例集：システム化の方向性と計画」「システム全体図」参照。

[2] ISO/IEC 30141:2018 において定義されている IoT サービス開発者を指す。具体的には、企業利用者及び一般利用者を指す。

3. （必要に応じて）使用する IoT 機器・システムの前提条件を記述する。

- ２．では、目的、受益者、提供する価値、運用時間、提供場所、提供形態、提供方法、利用する IoT 機器、サブシステムなどを記述する。
- 業界ごとに IoT 機器の利用や運用等に影響を及ぼし得る規律が設けられている場合がある。そのような場合は、これらの前提[3]を明記しておく。

＜TIPS＞

- 対象とする IoT 機器・システムの範囲を明確化する際には、情報処理推進機構（IPA）「IoT 開発におけるセキュリティ設計の手引き」（2.本書における IoT の定義）が参考となる。当該文書では IoT 機器の構成要素は以下の通りとされている。適用の範囲を明確にするにあたっては、これらの要素が含まれるよう検討を行うことが想定される。

  - サービス提供サーバ・クラウド
    ネットワークに接続され、IoT に対応するサービスを提供するサーバやクラウドサービスを指す。
  - 中継機器
    IoT 機器・システムをネットワークに接続する中継機器を指す。例えば、ファイアウォール、ゲートウェイ、ルータ等が該当する。
  - システム
    中継機器経由でネットワークに接続される、複数の機器で構成されたシステムを指す。例えば、制御システム、病院内の医療ネットワークシステムが該当する。
  - 機器
    ネットワークに接続される機器を指す。例えば、情報家電やヘルスケア機器が該当する。
  - 直接相互通信する機器
    中継機器を通してネットワークに接続するだけでなく、機器自身が他の機器と直接通信する機能をもつ機器を指す。機器同士の通信機能を有するポータブルゲーム機や、車々間通信 Car2X に対応した自動車などが該当する。

＜成果物のイメージ＞

- 対象ソリューションの概要

[3] 例えば、「液化石油ガス器具等の技術上の基準等に関する省令の運用について」（令和２年７月）では、「自然給排気式・開放式」の遠隔操作が禁止」されている。

- 製造実行システム（MES）やHMI、プロセス制御PLC等からなるプラントシステムを用いて、化学物質を製造しているケースを想定する。
- 本ケースケースでは、精製工程における蒸留工程を実施する装置を扱うものとする。
- 蒸留工程では、液体混合物を各成分の沸点の差を利用して分類させることを想定している。

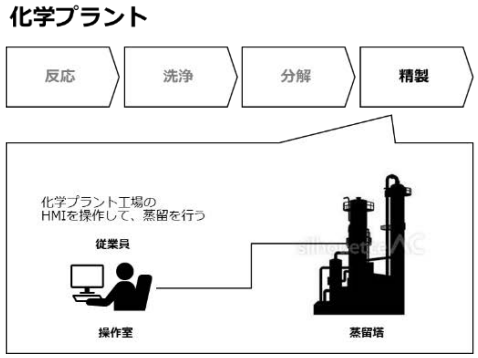

図 2 対象ソリューションの概要図（イメージ）

(2) ステークホルダー関連図

対象ソリューションの概要やシステム全体図、対象ソリューションに関する各種仕様書・契約書等を参考にして、対象ソリューションのステークホルダーを洗い出し、各ステークホルダーの役割と責任を整理したステークホルダー関連図を作成する。

前述の通り、対象ソリューションの提供・利用が複数の事業者等から構成される場合、主たる適用主体は他の事業者等に対して必要な対策の実施を依頼等することにより、セキュリティ対策の抜け漏れや全体の対策水準の低下を防ぐことが有効である。ステークホルダー関連図では、対象となる IoT 関連サービスにおいてセキュリティ上の責任を有する主体[4]（例：サービス利用者、サービス提供者、当該サービスを構成する機器・システムを提供する機器製造者、システムインテグレータ等）を洗い出すこととする。また、同じ企業であっても、セキュリティ対策を行う部署が異なる場合にはかかる部署（例：企画設計部門、運用部門）を分けて記載することも考えられる。後述の 2-3.リスク対応「(3)行うべきと考えられる対策」にてステークホルダー間で実施する対策を分担することから、実施する主体レベルでステークホルダーを特定することが望ましい。

＜収集しておくべき情報（例）＞

- システム全体図
- 対象ソリューションに関する各種仕様書・契約書（例：IoT 機器・システムの提供方法、管理方法、利用許諾等に関する条文）

＜作成方法＞

1. 対象ソリューションの提供又は利用に関連するステークホルダーを洗い出す。
2. 各ステークホルダーの役割や責任を整理する。
3. 各ステークホルダー間の関係性（例：契約関係や提供機器、サービス）を整理する。

- ステークホルダーを洗い出す際には、対象の IoT 機器・システムを開発、運用、保守等する過程でセキュリティ対策上の責任を負う者やセキュリティインシデントを通じて直接もしくは間接的に被害を受け得る

[4] インシデント発生時に機器が稼働する場所の近傍にいる等の理由で被害を受け得る主体を含む場合がある点に留意いただきたい。

主体を抽出する。

- 洗い出したステークホルダーの役割を明確にした上で、適用主体自身の役割や責任を明確にする。

＜TIPS＞

- セキュリティ対策上の責任を負い得る主体の抽出には、ISO/IEC 30141:2018 にて示されている以下の分類を参考にすることができる。
  - IoT サービス開発者
    - 機器メーカ
    - システムインテグレータ提供者
  - IoT サービス提供者
    - クラウドサービス事業者
    - メンテナンス事業者
  - IoT サービス利用者
    - 企業利用者[5]
    - 一般利用者
- ただし、上記にない主体であっても、インシデント発生時に機器が稼働する場所の近傍にいる等の理由で被害を受け得る可能性があるので、IoT 機器・システムにおけるセキュリティインシデントによって被害を受け得る第三者をステークホルダー[6]に含めることも検討する。例えば、以下の様な主体が含まれ得る。
  - ドローンの飛行箇所の周辺にいる第三者
  - プラント周辺の住民

＜成果物のイメージ＞

- ステークホルダー関連図

[5] 企業利用者については、IoT 機器・システム、サービスを自社の生産活動やサービス供給等ビジネスの中に組み込んでこれらの管理を行いつつ、利用している事業者が想定されている。

[6]「サイバー・フィジカル・セキュリティ対策フレームワーク」（以下、「CPSF」という。）ではステークホルダーを「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。」と定義している。セキュリティインシデントの被害を受け得る人又は組織を「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。」と理解することができる。したがって、ユースケース集では IoT 機器・システムにおけるセキュリティインシデントによって被害を受け得る第三者をステークホルダーに含めている。

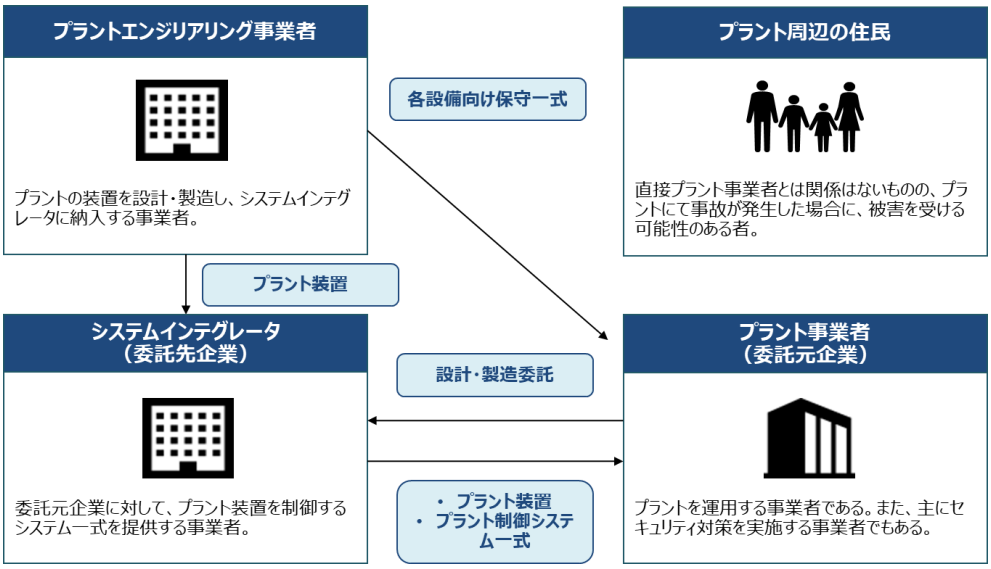

図 3 ステークホルダー関連図（イメージ）

(3) システムを構成する機器の一覧

既に適用主体の内部で整備、管理されている情報資産管理台帳[7]等を参考にした上で、リスク分析の対象となっているシステムを構成する機器やサービスの一覧を作成する。

システムを構成する機器は後述の 2-2.リスクアセスメント「(1 セキュリティインシデント及びその結果)」や 2-3 リスク対応「(3)機器ごとの脅威」を洗い出す際に活用することから、対象となる IoT 関連サービスの範囲内で脅威が生じ得る機器は洗い出すことが望ましい。一方で、分析対象が多数あると工数が膨大になることから、資産の絞りこみが必要となる。資産の絞り込みを行う際には例えば以下を行うことが可能である。

- 同じネットワークに直列に接続されているネットワーク機器を 1 つにまとめる。(例:直列に接続されているルータと FW を「ネットワーク機器(FW)」とする。)
- 接続先ネットワークが同一である情報系資産・制御系資産や設置場所のセキュリティレベルが同一である情報系資産・制御系資産、同一機能、類似機能を有する情報系資産・制御系資産を 1 つの資産と見なす。(例:エンジニアリング端末 1、エンジニアリング端末 2、エンジニアリング端末 3 を「エンジアリング端末」とする。)

なお、システム構成図やデータフロー図を作成する際には、本項で整理した記載粒度に沿って各図を作成することが望ましい。また、抜け漏れ等を防止する目的でシステムを構成する機器の記載レベルはステークホルダー間で調整し一致させることが必要である。

＜収集しておくべき情報（例）＞

- 情報資産管理台帳

＜作成方法＞

1. システムを構成する機器の一覧を整理する。

[7]「情報資産管理台帳」の例：情報処理推進機構（IPA）「中小企業の情報セキュリティ対策ガイドライン」参照。

2. システムを構成する機器ごとに、保有する機能や役割を整理する。

- 適用主体のみで資産の一覧を整理することが難しい場合には、構築ベンダ/機器製造事業者等と適宜情報交換を行うことが望ましい。
- 制御システムを評価対象とする場合には、情報系のネットワークに接続している OA 系の処理を行うための機器及びネットワークは対象外としても良い。
- 機器の一覧は、基本的には機器ひとつひとつを識別できるよう整備されることを想定するが、管理が煩雑となることを避けるために、同種の機器群（例：温度センサ）をまとめてひとつの対象として管理することも可能である。
- システムを構成する機器の記述内容には、以下の情報を含める。
  - 機器・システムの持つ機能
  - 設置場所
  - （IoT 機器の場合）スペック（大きさ・重量・走行スピード等）
  - （汎用的でない機器の場合）特記事項

＜成果物のイメージ＞

- システムを構成する機器の一覧

表 1 システムを構成する機器の一覧

システムを構成する機器	内容
製造実行システム（MES：Manufacturing Execution System）	製造工程の把握や管理、作業者への指示や支援などを行うサーバ。 MES は、プラント事業者所内にサーバを設置するものとする。 なお、主な機能は以下の通り。 - 作業のスケジュール管理機能 - 作業手配・製造指示機能 - 作業者管理機能 - データ収集機能 - プロセス管理機能 - 製品の追跡と製品体系管理機能 - 実績管理機能 - 生産資源の配分と監視機能 - 仕様・文書管理機能 - 設備の保守・保全管理機能 - 製品品質管理機能
ヒューマンマシンインターフェース（HMI：Human Machine Interface）	人間の操作と機械の動作をスムーズに結合するために使用されるハードウェアとソフトウェア。 具体的には、タッチパネル式の表示器やパネルコンピュータを指す。
プロセスサーバ	プロセス制御 PLC から収集するデータを扱うサーバ。
データヒストリアン	長期間のプロセス値や管理パラメータを保存し、分析を行うためのサーバ。 プロセス制御 PLC からのデータを収集するプロセスサーバより静的なデータ（ヒストリデータ）を扱う。
…	…

(4) システム構成図、データフロー図

ネットワーク構成図[8]及びシステム関係図[9]、(2)で作成したステークホルダー関連図等を参考にした上で、対象となる機器・システムの構成図、データフロー図を作成する。

システムを構成する機器の一覧をもとにシステムの構成図、データフロー図を整理することによって、発生し得るセキュリティインシデントやその結果に関する分析が実施しやすくなる。特に、異常な制御コマンドやプロセスデータが制御システムの稼働に容易に直接影響を与えるため、データフローの視点は重要となる。

＜収集しておくべき情報（例）＞

- ネットワーク構成図
- システム関係図
- 機能情報関連図[10]
- ステークホルダー関連図（2-1（2）にて作成）

＜作成方法＞

1. エリア区分図と資産の配置を整理する。
2. 各資産のネットワーク接続状況を記述する。
3. ネットワーク接続状況を基にシステム構成図を作成する。
4. システムを構成する機器に対して、各ステークホルダーがどのように関与（例：サービスの開発、サービス提供（運用を含む）、サービスの使用）しているかを整理する。
5. システム構成図にデータフローを記入する。

- システム構成図を作成する際には、物理的な境界となる資産の配置とネットワーク的な境界となるルータやファイアウォールを軸とした配置を明確にする。
- システムの構成図については、エリアごとに物理的なセキュリティのレベルが異なる場合では、資産の設置されているエリア（例：執務室、サーバルーム）を分けて記載する。
- データフローについては、機器・システムからどの機器・システムへとデータが送られているかを記載する。複数の経路が考えられる場合には、経路も明記する。
- 初期設定時や保守設定時など、通常と異なるデータの経路やデータが一時的に保存される場合がある。必要に応じてこのような場合を考慮する。

対象となるIoT関連サービスの内容やシステム構成によっては、複数の機器から1つのサーバへデータを集約させる場合がある。かかる場合にはデータフローは必ずしも連続したものにはならない。その場合には、各機器からサーバに送信されるデータを同じ番号(例えば、全てのデータを1とする)で表現することとする。ただし、視認性

---

[8]「ネットワーク構成図」の例：情報処理推進機構（IPA）「超上流から攻めるIT化の事例集：システム化の方向性と計画」参照。

[9]「システム関係図」の例：情報処理推進機構（IPA）「超上流から攻めるIT化の事例集：システム化の方向性と計画」参照。

[10]「機能情報関連図」の例：情報処理推進機構（IPA）「超上流から攻めるIT化の事例集：システム化の方向性と計画」参照。

の問題が生じる場合には各機器からサーバに送信されるデータごとにパターン分けを行って、データフローを記載することが望ましい。

＜成果物のイメージ＞

- システム構成図

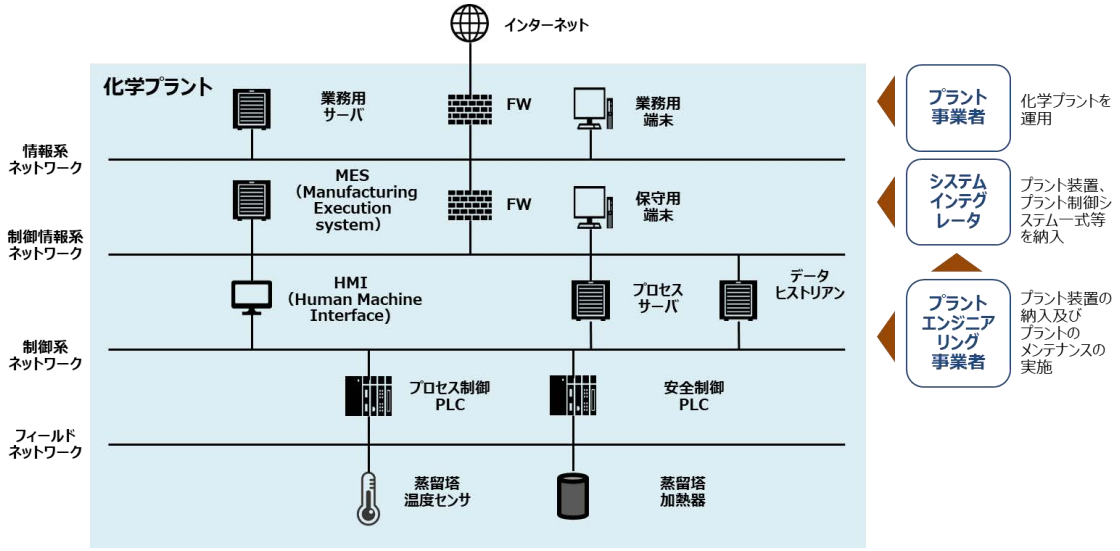

図 4 システム構成図（イメージ）

- データフロー図

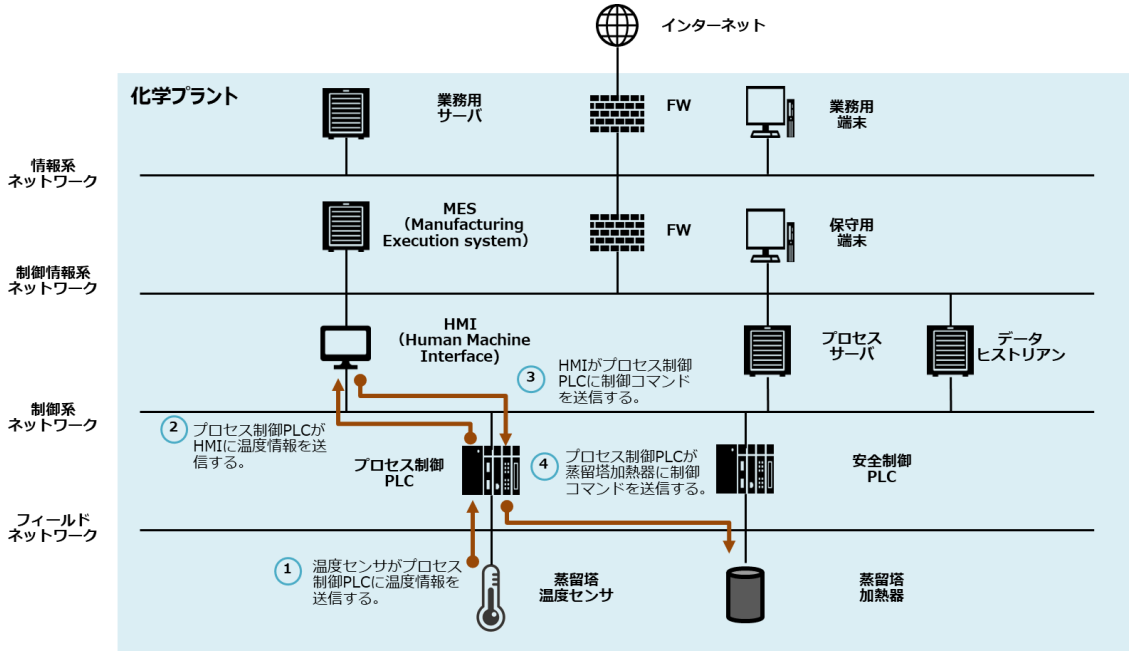

図 5 データフロー図（イメージ）

(5) 目標とするリスクの水準

組織内部における上位のセキュリティやセーフティ等に関する基本方針等を参考にした上で、対象ソリューションの目的に対して、受容できるリスクの大きさ及び種類を「目標とするリスクの水準」として特定する。

目標とするリスクの水準は、本来、適用主体やその他の関係者における個別の事情等を勘案して作成されるものである。「IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集」（以下、「ユースケース集」という。）に記載されている「発生したインシデントの影響の回復困難性の度合いの判断基準」や「発生したインシデントの経済的影響の度合いの判断基準」もひとつの材料として参照しつつ、適用主体において個別に目標とするリスクの水準を設定することが望ましい。

なお、本項にて目標とするリスクの水準を設定したとしても、後述の 2-2.リスクアセスメント「(2) 機器・システムの重要度の判断基準及び判断された重要度の一覧」における重要度と調整が発生する可能性がある。その際には、判断された重要度を考慮しつつ目標とするリスクの水準を調整することも考え得る。

＜収集しておくべき情報（例）＞

- 適用主体内部のリスクマネジメントに関する基本方針

＜作成方法＞

1. 受容可能な第 1 軸「回復困難性の度合い」のレベルを定める。
2. 受容可能な第 2 軸「経済的影響の度合い」のレベルを定める。
3. 回復困難性の度合いのレベル及び経済的影響の度合いから、受容できるリスク又は相対的に受容しがたいリスクの大きさを特定する。

＜TIPS＞

- 目標とするリスクの水準は業界や業種によって異なるため、意思決定者の判断に依存することに留意されたい。したがって、業界や業種によっては目標とするリスクの水準が一部大きくなる（例えば、第 2 軸「経済的影響の度合い」が重大な経済影響となる）こともあり得る。
- また、相対的に受容しがたいリスクを算出することで目標とするリスクの水準を明確することができる可能性がある。例えば、各業界別のガイドラインや業法における規律がこれらの目標とするリスクの水準の特定に参考となる場合がある目標とするリスクの水準を明確にする場合には、例えば、情報処理推進機構（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」（4.3 事業被害と事業被害レベル）や内閣サイバーセキュリティセンター（NISC）「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）」（深刻度評価の概要）等の既存の文献が参考となる。
- 例えば、目標とするリスクの水準の目安として以下が考えられる。
  - 回復困難性の度合い
    重傷者の有無、個人情報漏洩の有無
  - 経済的影響の度合い
    サービスの維持の可否、監督官庁への報告の要否

＜成果物のイメージ＞

- 目標とするリスクの水準

以下、目標とするリスク水準をユースケース集「2-3-4 化学プラント施設内の蒸留工程の自動制御」（⑤リスク基準）で示した「目標とするリスクの水準」を例にして説明する。

当該ケースでは、どこまでのリスクを許容することができるかを踏まえて「目標とするリスクの水準」を設定した。

社内の安全に関する方針では、プラントの従業員の安全やプラント周辺の環境保護に対してより高い優先

度で対処する規定を設けていると仮定した。

「回復困難性の度合い」に関しては、資産が攻撃された際に従業員が重症を負うとしている「重大なダメージ」は受容できないとした。

また、インシデントの影響の範囲が内部に限定されず、取引先やそれ以外の関係者にも長期間影響が続いた上で、それらの機能を他のサービスで補うことができない場合、「経済的影響の度合い」は「壊滅的な経済影響」となるとされている。これらのインシデントが発生した場合には、当該部門の売上（経済活動）や取引先等から得ている信頼関係に大きな影響を与えるため、「壊滅的な経済影響」は許容できないとした。

一方で、プラントにおける事故は重大な事故に発展しやすいため、「経済的影響の度合い」が大きくなりやすく、セキュリティインシデントに伴う機器設備の停止等が生じた場合に「限定的な経済影響」に抑えることは現実的に難しい場合も想定される。仮にインシデントが発生したとしても、影響が取引先やそれ以外の関係者に及ばなければ「重大な経済影響」と位置付けられることから、これらを念頭に置いて、「重大な経済影響」までは「経済的影響の度合い」を許容するとした。

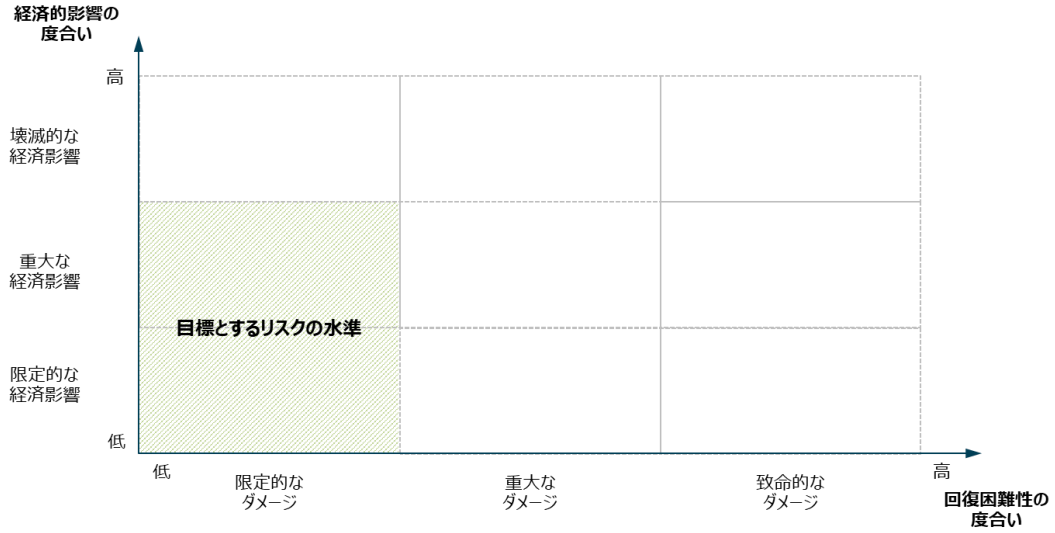

図 6 目標とするリスクの水準（イメージ）

2-2 リスクアセスメント

本節では、以下の情報を整理するものとする。

(1) セキュリティインシデント及びその結果

(2) 機器・システムの重要度の判断基準及び判断された重要度の一覧

(3) リスクのマッピング結果

(1) セキュリティインシデント及びその結果

過去に発生したセキュリティインシデントに関するメディア報道、報告書や今後発生する可能性があると想定されているセキュリティインシデントに関する文書等を参考として、適用対象となっている機器・システムにおいて想定されるセキュリティインシデントとそのセキュリティインシデント等によって生じ得る結果を整理する。

＜収集しておくべき情報（例）＞

- 社内やグループ会社、業界内において過去に発生したセキュリティインシデントに関するメディア報道や

社内外の文書等

- 業界内や対象機器・システムにおいて発生する可能性があると想定されているセキュリティインシデントに関する文書（研究報告等を含む）

＜作成方法＞

1. 評価対象の機器・システムで生じ得るセキュリティインシデントとその結果を特定する。
   (ア) 機密性、完全性、可用性の各観点を考慮し、生じ得るセキュリティインシデントとその結果（事業被害）を特定する。
   (イ) 特定したセキュリティインシデントや事業被害が、最終的に対象機器・システム内のどの機器で生じ得るかを特定する。
   (ウ) 重大な影響を及ぼし得るセキュリティインシデントが成立するシナリオ（どのような主体が、どのような侵入経路で、どのような攻撃を行うか）を検討する。
2. セキュリティインシデントにより起こり得る結果及びその影響の度合いをステークホルダーごとに特定する。

＜TIPS＞

- 想定されるセキュリティインシデントを抽出する際には、ISO/IEC 27001:2014（6.1.2 情報セキュリティリスクアセスメント）で示された考え方を参考にすることができる。
- セキュリティインシデントによりもたらされ得る結果を特定する際には、以下の観点を参考とすることができる。
  - 事業の停止、劣化
  - 自社に対する信頼の低下
  - 人的被害
  - システム破壊
  - 法令順守抵触事象の発生
- また、情報処理推進機構（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」（4.3 事業被害と事業被害レベル）を参考にすることができる。

＜成果物のイメージ＞

- セキュリティインシデント及びその結果

分類	想定されるセキュリティインシデント	想定される被害(例)
プラント事業者にとってのリスク	悪意のある攻撃者が、業務用サーバや業務用端末に加えて、MES等に**不正アクセス**し、**情報を漏えい**させる。	従業員の個人情報や取引先担当者等の情報が流出する可能性がある。
	プラント制御システムが**マルウェアに感染**（例：ランサムウェア）し、かつ安全設備等が十分に作動しない。	一部の化学反応が進むことで、蒸留塔内部の温度が上昇し、**蒸留塔等が爆発し得る。**その結果、プラント工場が停止するとともに、**従業員が重症を負うか死亡する可能性がある。**（※1）
	プラント制御システムが**マルウェアに感染**（例：ランサムウェア）し、蒸留工程に関する設備が停止する。	その他の工程も停止することにより、**工場全体の稼働が停止する**とともに、川下の企業の経済活動にも大きな影響を与える。
プラント周辺の住民	プラント制御システムが**マルウェアに感染**（例：ランサムウェア）し、かつ安全設備等が十分に作動しない。	一部の化学反応が進むことで、蒸留塔内部の温度が上昇し、蒸留塔等が爆発することにより、環境汚染が生じた場合には、**住民等の健康や安全に多大な影響**が生じる可能性がある。また、**住民の生活にも大きな支障をきたす**可能性がある。
システムインテグレータにとってのリスク	プラント事業者に対する注意喚起(例：設定方法に関する説明等)を怠る。	サービス提供における過失が認められ得る。（※2）
プラントエンジニアリング事業者にとってのリスク	開発するアップデートプログラムが改ざんされ、そのまま配信されることで、MESやプロセス制御PLC等が**マルウェアに感染**する。	MESやプロセス制御PLCが想定していない動作をして、**蒸留塔等の設備が停止する。**（※3）

※1:その結果として、各事象のステークホルダーを含む関係者に対する損害賠償（住民被害や環境汚染の対応等）の事後的な対応が発生し得る。
※2:その結果として、契約上の責任が問われ得る。
※3:その結果として、各事象のステークホルダーを含む関係者に対する損害賠償（システムインテグレータへの補償等）の事後的な対応が発生し得る。

図 7 セキュリティインシデント及びその結果（イメージ）[11]

(2) 機器・システムの重要度の判断基準及び判断された重要度の一覧

2-1(5)で整理した目標とするリスクの水準を参考として、機器・システムにおける重要度の判断基準を明らかにする。その上で、2-2(1)で整理したセキュリティインシデント及びその結果を踏まえて、機器・システムにおける重要度を一覧化する。

機器・システムの重要度の判断基準及び判断された重要度の一覧を整理することによって、想定されるセキュリティインシデント及びその結果より特定される機器・システムで想定されるリスクの大きさを算出することが可能となる。

＜収集しておくべき情報（例）＞

- 目標とするリスクの水準（2-1（5）にて作成）
- 想定されるセキュリティインシデント等とその結果（2-2（1）にて作成）

＜作成方法＞

1. 第 1 軸「回復困難性の度合い」及び第 2 軸「経済的影響の度合い」ごとに機器・システムにおける重要度の判断基準を明確化する。
2. 1. で明確化された基準基づいて判断された機器・システムの重要度をステークホルダーごとに一覧化する。

- 既存の規格（例：ISO/IEC 27001）やそれらに基づくリスクアセスメントでは、想定される個々のリスクや脅威を単位としてリスクレベルを評価する一方で、IoT-SSF では想定されるセキュリティインシデントを踏まえて機器・システムという単位で重要度を評価することが求められている点に留意されたい。
- 機器・システムで生じ得るセキュリティインシデントの影響の内容や大きさは、被害を受けるステークホルダーごとに異なることが想定される。IoT-SSF では、評価対象の機器・システムを取り巻くエコシステム全体でセキュリティ等を確保する観点から、ステークホルダー関連図で整理したステークホルダーごとに重要

[11] 図 7 に示したセキュリティインシデント及びその結果は一部である。したがって、図 7 で示したもの以外についても起こりえることに留意いただきたい。

326 度を評価することにも留意されたい。
327 ● 重要度の判断基準は、2-1（5）で作成された目標とするリスクの水準と整合をとる必要がある。

328 ＜成果物（例）＞
329 ● 判断された重要度の一覧

ステークホルダー	回復困難性の度合い	経済的影響の度合い
プラント事業者	• 爆発事故によって、従業員が死亡する可能性がある。	• 大規模な製品回収につながるおそれがある。
プラント周辺の住民	• プラント周辺の住民が重症を負う可能性がある。	• 農林水産業への打撃により、住民の生活にも大きな支障をきたすおそれがある。
システムインテグレータ	• 従業員がけがをする可能性は低い。	• サービス提供における過失が認められ得る。
プラントエンジニアリング事業者	• 従業員がけがをする可能性は低い。	• 開発するアップデートプログラムが改ざんされ、大規模な製品回収につながる可能性がある。

330
331 図 8 判断された重要度の一覧（イメージ）

332 (3) リスクのマッピング結果
333 2-2(2)で整理した判断された重要度の一覧を参考にして、第 1 軸「回復困難性の度合い」及び第 2 軸
334 「経済的影響の度合い」に対象機器・システムをマッピングする。
335 第 1 軸「回復困難性の度合い」及び第 2 軸「経済的影響の度合い」に機器・システムをマッピングすることに
336 よって、相対的にリスクが大きいとされている機器・システム（及びリスク）を把握することが可能となり、リスク対
337 応の方向性を検討するための基礎情報を得ることが可能となる。

338 ＜収集しておくべき情報（例）＞
339 ● 想定されるセキュリティインシデント等とその結果（2-2（1）にて作成）
340 ● 判断された重要度の一覧（2-2（2）にて作成）

341 ＜作成方法＞
342 1. 第１軸「回復困難性の度合い」及び第２軸「経済的影響の度合い」に機器・システムをマッピングする。

343 ● 同じ機器・システムであってもステークホルダーによって重要度は異なるため、ステークホルダーごとに機
344 器・システムをマッピングする。
345 ● 機器・システムによって、生じ得るインシデントやその結果及びリスクの大きさが異なる場合には、その機
346 器・システムごとにマッピングする。

347
348

＜成果物（例）＞

- マッピング結果

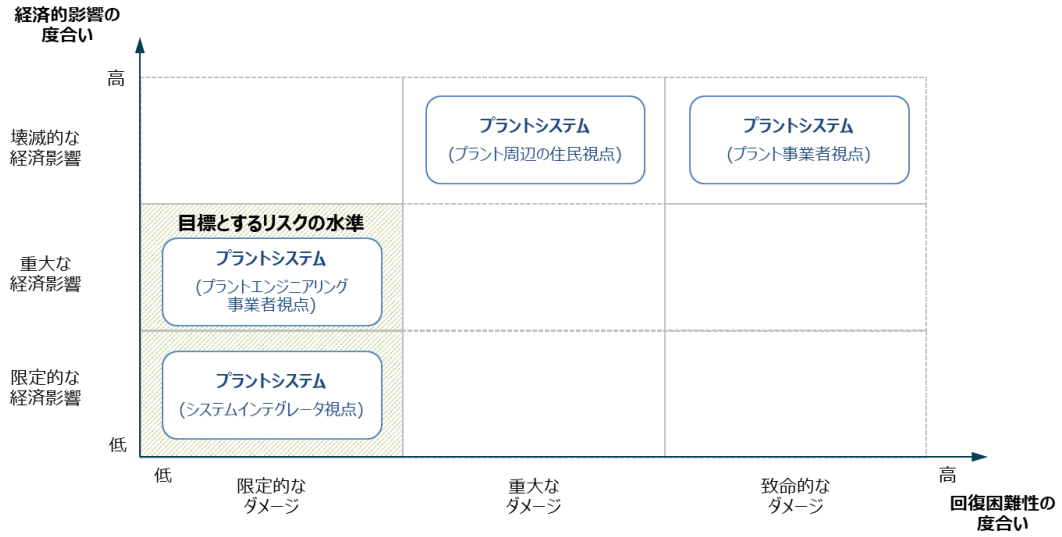

図 9 マッピング結果（イメージ）

2-3 リスク対応

本節では、以下の情報を整理するものとする。

(1) 機器ごとの脅威

(2) 脅威に対する対策

(3) 行うべきと考えられる対策

(1) 機器ごとの脅威

2-1（3）にて作成したシステムを構成する機器の一覧や 2-2（1）で作成したセキュリティインシデント及びその結果より、対象の機器・システムを構成する機器ごとの脅威を特定する。

機器ごとの脅威を特定することによって、脅威に対応した対策を整理することが可能となる。

＜収集しておくべき情報（例）＞

- システムを構成する機器の一覧（2-1（3）にて作成）
- セキュリティインシデント及びその結果（2-2（1）にて作成）

＜作成方法＞

1. セキュリティインシデント及びその結果より、セキュリティインシデントが生じ得る機器の一覧を作成する。
2. 1. で作成した一覧から、対象の機器・システムを構成する機器ごとに想定される脅威を整理する。
3. セキュリティインシデント及びその結果より、想定される脅威ごとに生じ得るインシデントとその影響の度合いを評価する。

- ユースケース集では、相対的に影響の度合いが大きいと評価された機器・システム及びそこで想定されるセキュリティインシデントに関連した脅威を中心に検討している。しかし、実際に脅威を洗い出す際には、その前段としてある程度網羅的に脅威を洗い出しておくことが望ましい。

- セキュリティインシデントが生じ得る機器の一覧を作成する際に過不足が生じた場合、2-2（1）に戻り、セキュリティインシデント及びその結果を再整理することが望ましい。

＜TIPS＞

- 想定される脅威を洗い出す際には、ユースケース集における「(1) システムを構成する機器ごとの脅威の整理」で示した脅威を参考とすることができる。
  - STRIDE モデルにおける脅威
    - なりすまし
    - データの改ざん・消去
    - 否認
    - 情報漏えい
    - サービス不能
    - 権限の昇格
  - IoT 機器・システムにおいて追加的に想定される脅威（例）
    - 不正アクセス
    - マルウェア感染
    - 踏み台
    - 不正改造
    - 未知の脆弱性
    - 不正利用
    - 利用者によるセキュリティ設定等の誤り等
- また、情報処理推進機構（IPA）「制御システムの制御システムのセキュリティリスク分析ガイド 第 2 版」（5.3.1. 想定される脅威（攻撃手法）一覧の確認）を参照することができる。

＜成果物のイメージ＞

- 機器ごとの脅威

表 2 想定される脅威（イメージ）

システムを構成する機器	想定される脅威	生じ得るインシデント
製造実行システム（MES：Manufacturing Execution System）	データの改ざん	製造実行システムに保存された稼働情報等が改ざんされる。
	情報漏えい	製造実行システムに保存された稼働情報等が外部に漏えいする。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、製造実行システムに不正アクセスされる。
	…	…
…	…	…

(2) 脅威に対する対策の洗い出し

2-3（1）にて作成した機器ごとの脅威を参考にして、第 3 軸「セキュリティ・セーフティ要求」における 4 つの観点ごとに脅威に対する対策を整理する。対策を整理する際には、想定される脅威ごとに個別に対策を洗い出す。なお、ユースケース集では脅威を「全般」と表記している箇所が散見されるが、これは想定される脅威ごとに洗い出した対策をまとめたものである。したがって、ここで示す「全般」は対策ごとにまとめられた複数の脅威を

示す点にご留意いただきたい。

また、適用主体が実施すべき対策のほか、ステークホルダー関連図に含まれる他の事業者又は個人に対応を依頼する対策も整理する。脅威に対する対策を整理することによって、各ステークホルダーが実装する（可能性）がある対策を網羅的に整理することができる。

＜収集しておくべき情報（例）＞

- 機器ごとの脅威（2-3（1）にて作成）
- ステークホルダー関連図（2-1（2）にて作成）

＜作成方法＞

1. 第 3 軸「セキュリティ・セーフティ要求」における 4 つの観点ごとに、脅威に対して必要と考えられる対策を整理する。
   (ア) 第 1 の観点における対策を対策要件の実装先（ソシキ・ヒト及びシステム）ごとに整理する。
   (イ) 第 2 の観点における対策を対策要件の実装先（ソシキ・ヒト及びプロシージャ、システム）ごとに整理する。
   (ウ) 第 3 の観点における対策を対策要件の実装先（ソシキ・ヒト及びシステム）ごとに整理する。
   (エ) 第 4 の観点における対策を対策要件の実装先（ソシキ・ヒト及びシステム）ごとに整理する。

ただし、既存の機器・システムを対象にリスクアセスメント、リスク対応を行う場合には、上記で整理した対策の一部を既に実装している可能性がある。その場合には、以下の作業が必要となる。

2. 上記で整理した対策と既に実装している対策を照らし合わせた上で、新たに実装すべき部分を明確化する。

＜TIPS＞

- 対策要件を整理する際には、CPSF」における「添付 C 対策要件に応じたセキュリティ対策例」やユースケース集における「添付 A 対策要件」等を参考とすることができる。
- 特に第 4 の観点では、「賠償等の対処を実施することが容易ではないケース等における社会的なセーフティネットの構築」を広く検討することが望ましい。

＜成果物（例）＞

- 脅威に対する対策

表 3 脅威に対する対策（イメージ）

第 3 軸	実装先	想定される脅威	対策要件
第 1 の観点	ソシキ・ヒト	データの改ざん	IoT 機器・システムにおけるセキュリティポリシーの策定
		…	…
第 2 の観点			
第 3 の観点			
第 4 の観点			

(3) 行うべきと考えられる対策の整理

2-3（2）で作成した脅威に対する対策を参考にして、優先的に行うべきと考えられる対策を整理する。

行うべきと考えらえる対策を整理することで、コストや効率性等を考慮して実際にアクションができる粒度で対策を整理することができるようになる。

＜収集しておくべき情報（例）＞

- 脅威に対する対策（2-3（2）にて作成）

＜作成方法＞

1. 脅威に対する対策より、適用主体にて行うべきと考えられる対策要件を抽出する。
2. 1 で抽出した対策要件ごとに実際に講じる対策を整理する。
3. 脅威に対する対策より、各ステークホルダーにて行うべきと考えられる対策要件（他のステークホルダーにて実装を依頼する対策要件）を整理する。
4. 3.で抽出した対策要件ごとに実際に講じる対策を整理する。
5. 4 で整理した対策の実装を各ステークホルダーに依頼する。

- 実際に講じる対策を抽出する際には、目標とするリスクの水準に収まっていない機器・システムを対象としたものの優先度を上げることを考慮する。
- また、「対策の適用対象」、「適用する対策の内容」の観点から、以下のような観点を考慮して対策等の優先順位付けを行うことも有効である。
  - 対策の適用対象

    当該機器に影響を及ぼす事象が実際に生じた場合に、結果として生じ得る被害の大きさや、当該機器に悪影響を及ぼし得る事象の起こりやすさを考慮する。
  - 適用する対策の内容

    対策に係る費用対効果の大きさや対策に係る実施可否を考慮する。

＜TIPS＞

- 実際に講じる対策を整理する際には、CPSF における「添付 C 対策要件に応じたセキュリティ対策例」やユースケース集における「添付 B 実際に講じる対策の例」を参考とすることができる。

＜成果物（例）＞

- 適用主体にて行うべきと考えられる対策
- 他のステークホルダーにて行うべきと考えられる対策（他のステークホルダーにて実装を依頼する対策）

表 4 適用主体にて行うべきと考えらえる対策（イメージ）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● 対象となっているプラント施設におけるセキュリティポリシー（例：情報セキュリティ関連規定を含む）の見直し及び、事業部長等の適切な承認権限を有する者の承認 ● 定められた期間ごとの当該ポリシーのレビュー	

			…	…	…
	第 2 の観点				
	第 3 の観点				
	第 4 の観点				

460

461 表 5 他のステークホルダーにて行うべきと考えられる対策（他のステークホルダーにて実装を依頼する対策）

462 （イメージ）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	搭載するソフトウェアの改ざん検知機能の実装の要求	● MES やプロセス制御 PLC 等のソフトウェアに関する完全性の検証機能の実装。	
	第 2 の観点			●	
	第 3 の観点			●	
	第 4 の観点			●	

463

3. 参考

- 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」
- 経済産業省「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」
- 経済産業省「IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集」
- 情報処理推進機構（IPA）「IoT 開発におけるセキュリティ設計の手引き」
- 情報処理推進機構（IPA）「超上流から攻める IT 化の事例集：システム化の方向性と計画」
- 情報処理推進機構（IPA）「超上流から攻める IT 化の事例集：要件定義」
- 情報処理推進機構（IPA）「中小企業の情報セキュリティ対策ガイドライン」
- 情報処理推進機構（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」
- 内閣サイバーセキュリティセンター（NISC）「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）」
- ISO/IEC 27001:2014
- ISO/IEC 30141:2018
- Microsoft” Microsoft Threat Modeling Tool の脅威”