IoT セキュリティ・セーフティ・フレームワーク

適用手順書

内容

変更履歴

Version	変更年月	変更箇所	変更内容
1.0	2023 年 4 月	-	新規作成

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。

1. 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]
   分析対象となる範囲についてステークホルダーの合意を得たうえで、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、目標とするリスクの水準を整理する。
2. 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。
3. 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とおりである。作成手順については、各節にて説明する。

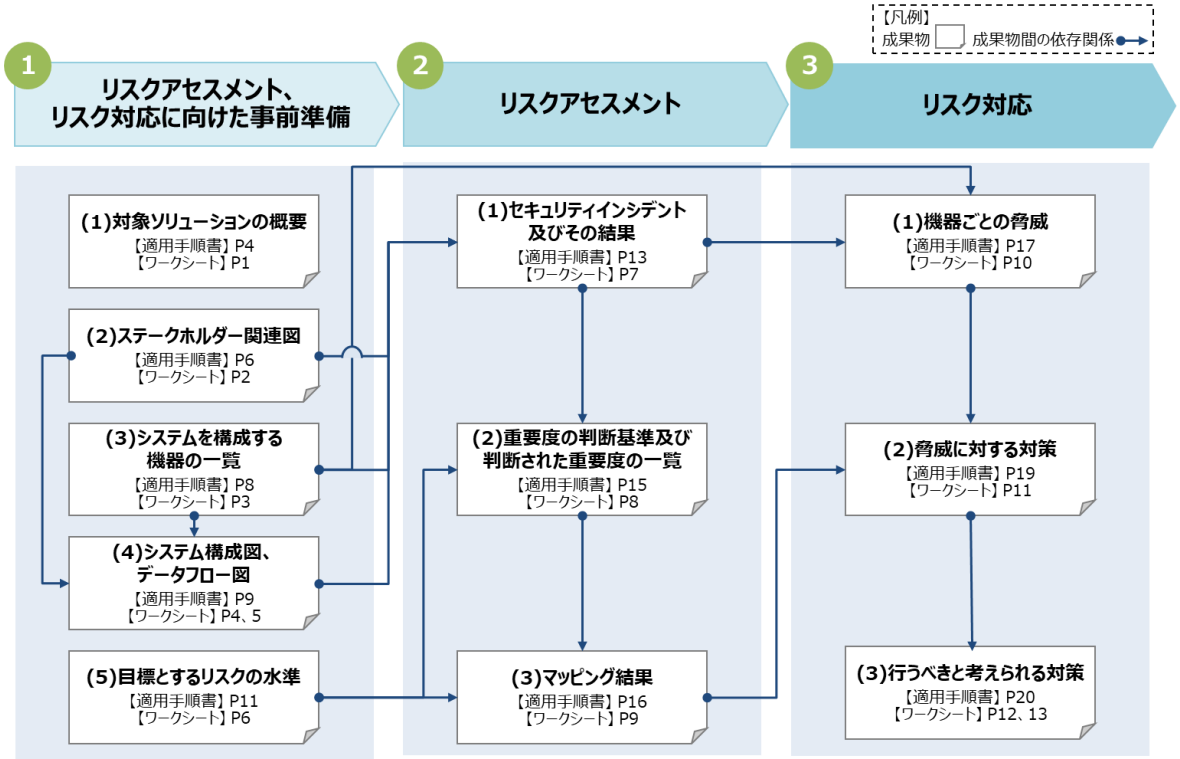

図 1 各ステップにおける成果物の一覧[1]

[1] 図内の矢印は成果物間の依存関係を示す。手順を進める途中で、成果物間で整合性が取れない場合や内容の過不足が明らかになった際には、適宜、以前の段階に戻って内容を修正する。

IoT-SSF を参照し、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」と呼ぶ。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当該事業者が「適用主体」になるが、複数の事業者が協力して IoT 関連サービスを提供・利用する場合は、それぞれの事業者が、それぞれの責任範囲において「適用主体」となる。

複数の事業者が共同で適用手順を推進する場合は、各事業者間で協議した上で、結果等のとりまとめ役を決定することが望ましい。より俯瞰的な立場で IoT 関連サービスを見渡すことが可能な事業者[2]が、とりまとめ役[3]となり、後述のステークホルダー関連図や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することにより、IoT 機器・システム全体の対策水準を向上させることができる。

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[4]等を参考にして、対象ソリューションの目的や、IoT サービス利用者[5]による IoT 機器・システムの利用方法を記述する。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 を適用させる範囲と適用の対象外とする範囲を明確化しなければならない。IoT-SSF の適用範囲は、IoT-SSF を適用する目的と整合させることが重要である。

対象の IoT 機器・システムと直接的なかかわりがない場合は 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外としてもよい。

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。

---

[2] 「俯瞰的な立場で IoT 関連サービスを見渡すことが可能なステークホルダー」とは、IoT 関連サービス全体に責任を有するステークホルダーを指す。(例:プラント事業者、スマートホームサービス提供事業者)

[3] スキルやリソースの都合上、適切な対応が難しいステークホルダーはとりまとめ役に適さない点に留意されたい。

[4] 「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。

[5] 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。

＜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・システムとその範囲を特定する。
2. 対象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。
3. (必要に応じて)使用する IoT 機器・システムに関する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、サブシステム等を記述する。
- 業界ごとに IoT 機器・システムの利用や運用等に影響を及ぼし得る規律(例:経済産業省「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」、厚生労働省「ボイラーの遠隔制御基準等について」)が設けられている場合は、これらの前提を明記しておく。

＜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とおりとされている。

  - 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 に対応した自動車等が該当する。

＜成果物＞

- 対象ソリューションの概要

- 「IoT 機器・システムを通じて提供されるサービスの開発者」であるプラント事業者が、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、化学物質を製造するケースを想定する。
- プラント事業者は、一般のビニール製品に広く使用される化学物質を製造する事業者であり、操業開始から既に数十年程度プラントを運用している。
- 本ケースケースでは、以下の工程のうち精製工程における蒸留工程を担う装置を扱う。
  1. 反応工程：原料や酸素等を反応させ化合物を生成する工程
  2. 洗浄工程：反応工程で生成された化合物を中和洗浄する工程
  3. 分解工程：中和洗浄された化合物を熱によって分解する工程
  4. 精製工程(蒸留工程を含む)：成分の沸点の差を利用して、分解工程までで生成された化合物を製品用に分離させる工程

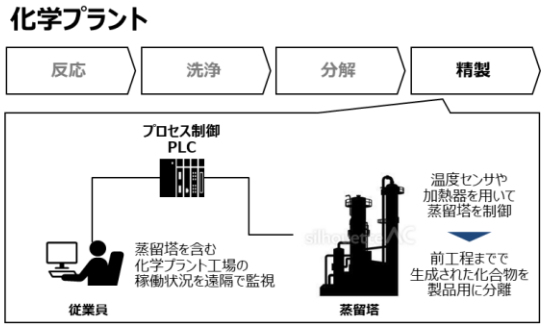

図 2 対象ソリューションの概要図(イメージ)

(2) ステークホルダー関連図

システム全体図や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。

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(例:IoT サービス開発者、IoT サービス提供者、IoT サービス利用者等)、対象サービスにおいてセキュリティ上の被害が生じた際に直接的または間接的に被害を受け得る主体をステークホルダーとして洗い出す。

ステークホルダーは、セキュリティ対策を実施する主体レベルで特定することが望ましい。

同じ企業内でセキュリティ対策を行う部署が異なる場合には、企画設計部門、運用部門のように部門を分けて記述することも検討する。

＜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、IoT 機器・システムにおける開発、運用、保守の過程でセキュリティの責任を負う主体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
  - 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[6]
    - 一般利用者

- 上記に示されていない主体であっても、対象とする IoT 機器・システムの近傍にいる等の理由でセキュリティインシデントによる被害を受け得る第三者は、ステークホルダー[7]に含めることを検討する。例えば、以下に示す主体が含まれ得る。
  - IoT 機器の使用環境周辺にいる第三者
  - IoT 機器・システムを扱う大規模設備(例:工場やプラント)におけるセキュリティインシデントの被害を受け得る近隣住民

＜成果物＞

- ステークホルダー関連図

[6] 企業利用者は、自社のビジネス(例:製品の生産活動、供給活動)の中に IoT 機器・システム、サービスを組み込んだ上で、利用している事業者が想定される。

[7] 「サイバー・フィジカル・セキュリティ対策フレームワーク」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ことから、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。

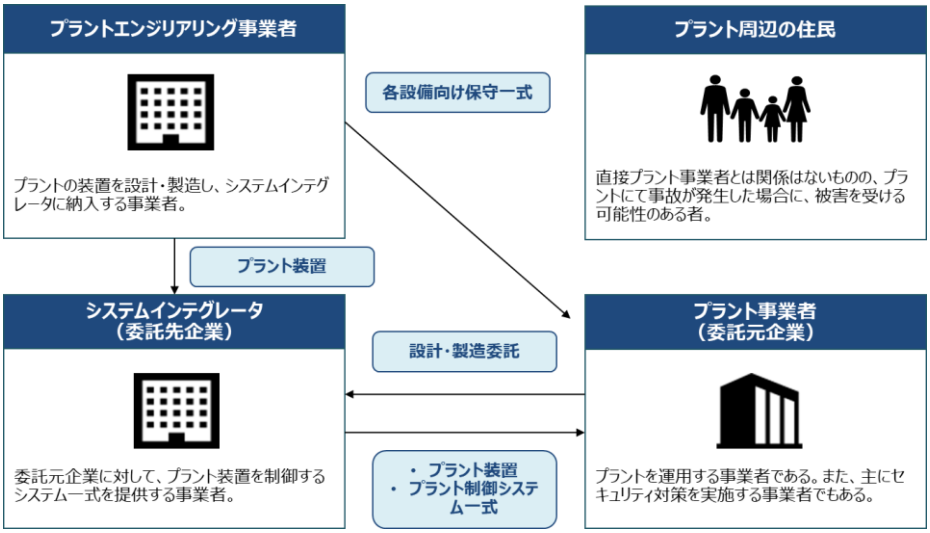

図 3 ステークホルダー関連図(イメージ)

(3) システムを構成する機器の一覧

既に整備、管理されている情報資産管理台帳[8]等を参考にした上で、対象ソリューションを構成する機器やシステムの一覧を作成する。

システムを構成する機器は、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を洗い出すことが望ましい。

分析対象を削減するためには、以下のように複数の機器を 1 つの機器にまとめることを検討する。

- 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。)
- 以下に該当する場合は複数の機器を 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。)
  - 接続先ネットワークが同一である機器・システム
  - 設置場所のセキュリティレベルが同一である機器・システム
  - 同一機能、類似機能を有する機器・システム

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で各図を作成することが望ましい。また、抜け漏れを防止するため、システムを構成する機器の記載粒度はステークホルダー間で調整し一致させることが必要となる。

＜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作成する。
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記述する。

8 「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。

- 適用主体のみでの対応が難しい場合は、システムインテグレータや機器メーカ等と適宜情報交換を行った上で、機器の一覧を作成することが望ましい。
- 制御システムを評価対象とする場合は、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よい。
- システムを構成する機器の記述内容には、例えば、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＞

- 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等を行うサーバ。 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、主な機能は以下のとおり。 - 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 ….
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。 ヒューマンマシンインターフェースはプラント事業所内に設置するものとする。
…	…

(4) システム構成図、データフロー図

ネットワーク構成図[9]及びシステム関係図[10]、機能情報関連図[11]、(2)で作成したステークホルダー関連図、(3)で作成したシステムを構成する機器の一覧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。

9 「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。

10 「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。

11 「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。

＜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
- ステークホルダー関連図(2-1(2)にて作成)
- システムを構成する機器の一覧(2-1(3)にて作成)

＜作成方法＞

1. エリア区分図を作成した上で、各システム・機器を配置する。
2. 各システム・機器のネットワーク接続状況を 1 に追記する。
3. システムを構成する機器に対する各ステークホルダーの関与方法(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)を 2 に追記する。
4. 1～3 で作成したシステム構成図にデータフローを追記する。

- 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。また、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には、資産が設置されているエリア(例:執務室、サーバルーム)を分けて記述する。
- データフロー図を作成する際には、機器・システムからどの機器・システムへデータが送られているかを記述する。複数の経路が考えられる場合や初期設定時や保守設定時等、通常と異なるデータの経路が考えられる場合には、パターン分けを行った上で各経路を記述する。

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

＜成果物＞

- システム構成図
- データフロー図

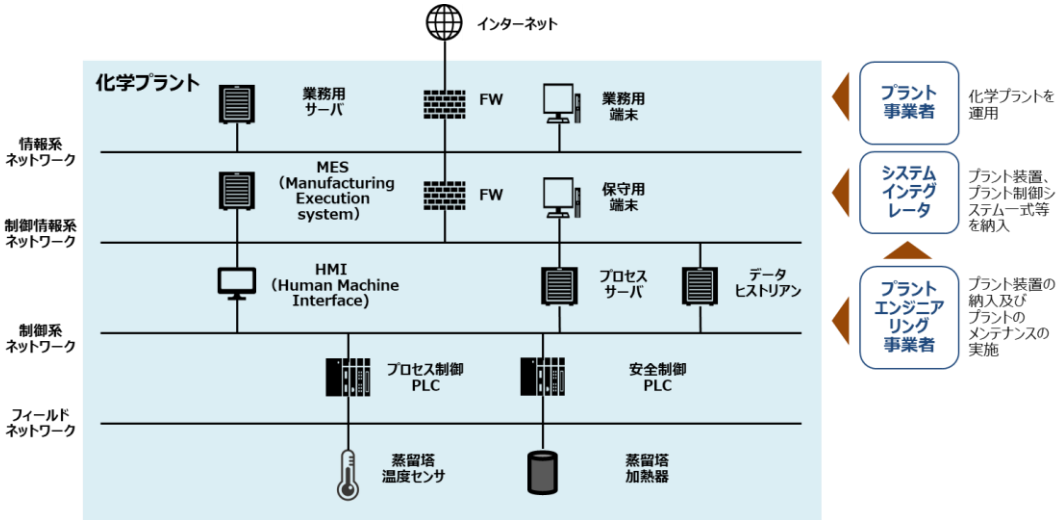

図 4 システム構成図(イメージ)

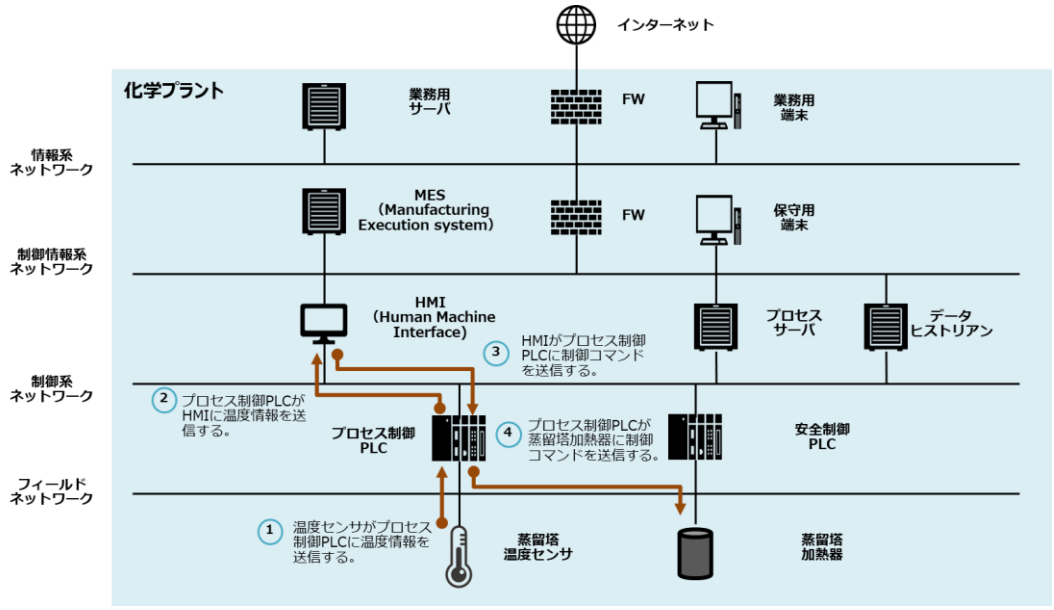

図 5 データフロー図(イメージ)

(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リスク水準として設定する。

「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」を参照しつつ、適用主体や各ステークホルダーにおける個別の事情等を勘案した上で、目標とするリスクの水準を設定することが望ましい。

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」にて判断された重要度とリスクの水準の間で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変更することも検討する。

＜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. 図 6 に示す判断基準を参考にして、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. 図 7 に示す判断基準を参考にして、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. 1、2 で定めたレベルから、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。

レベル	判断基準	（参考） IoT-SSFにおける 判断基準
致命的な ダメージ	• 資産が攻撃された場合、利用者または関係者の人命が失われるおそれがある。	• 人命が失われる
重大な ダメージ	• 資産が攻撃された場合、重症を負うおそれがある。 • 資産が攻撃された際の利用状況が適切でない場合(例：想定利用方法と異なる)、人命が失われるおそれがある。 • 重要度が高い個人情報が漏洩する。	• 重症を負う • 重要な個人情報の漏洩
限定的な ダメージ	• 資産が攻撃された場合、軽傷を負うおそれがある。 • 個人情報が漏洩する。	• 軽傷を負う • メールアドレスのみの漏洩

図 6 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

レベル	判断基準	（参考） IoT-SSFにおける 判断基準
壊滅的な 経済影響	• 影響の範囲が内部に限定されず、取引先やその他の関係者に及び、長期間影響が続くことが想定される。 • 影響を受ける機器・システムの機能を他の製品・サービスで補うことができない。 • 大規模な製品等の回収等が生じ得る。	• （破産） • 社会の大混乱
重大な 経済影響	• 影響の範囲が取引先やそれ以外の関係者に及び、長期間影響が及ぶものの、**他の製品等で影響の結果を補うことができる**。 • 影響の範囲が取引先やそれ以外の関係者に及び、影響の結果は他の製品・サービスで補えないものの、**影響は短期間で収束する。** • 影響が長時間に及び、影響の結果は他の製品・サービスで補えないものの、**影響の範囲が取引先やそれ以外の関係者に及ばない。**	• 大損害 • 社会の混乱
限定的な 経済影響	• 影響の範囲が取引先やそれ以外の関係者に及ぶものの、**影響は長時間に及ばず、影響の結果は他の製品・サービスで補うことができる**。 • 影響の結果は他の製品・サービスで補えないものの、**影響の範囲は取引先やそれ以外の関係者に及ばず、影響は長時間に及ばない。** • 影響が長時間に及ぶものの、**影響の範囲は取引先やそれ以外の関係者に及ばず、影響の結果は他の製品・サービスで補うことができる**。	• 損害、社会の悪影響

図 7 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

＜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、適用主体の判断に依存することに留意されたい。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。
- 組織内部における上位のセキュリティやセーフティに関する基本方針にて定められた内容と図 6 及び図 7 を比較した上で、目標とするリスクの水準を定めるが、各業界別のガイドラインや業法における規律を踏まえて、相対的に受容しがたいリスクを特定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。

- 目標とするリスクの水準を明確にする際には、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)の文献が参考となる。

＜成果物＞

- 目標とするリスクの水準

以下、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)を例にして、「目標とするリスクの水準」の設定を説明する。

この例では、社内の安全に関する方針でプラントの従業員の安全やプラント周辺の環境汚染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」は受容できず、「限定的なダメージ」とした。

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。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ステークホルダーに及ばなければ「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、「経済的影響の度合い」を「重大な経済影響」まで許容するとした。

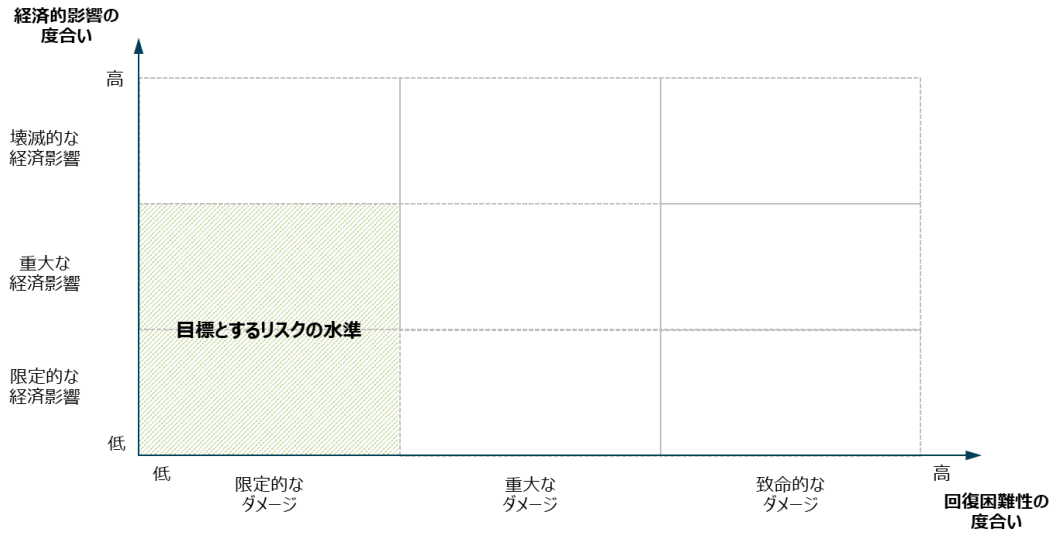

図 8 目標とするリスクの水準(イメージ)

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。

(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や報告書を参考としたり、脅威分析等の汎用的なセキュリティリスクアセスメント手法を活用したりすることで、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。

本項では、事業リスクの観点から評価対象の機器・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。

本項にて事業影響(例:事業の停止・劣化、自社に対する信頼の低下、人的被害)及びそれにつながり得るセキュリティインシデント等を特定した上で、後述の 2-3 リスク対応「(1)機器ごとの脅威の整理」にてかかるインシデントを引き起こし得る脅威を特定する点に留意されたい。例えば、従業員の個人情報や取引先担当者等の情報が流出するケースを想定した場合、2-3 リスク対応「(1)機器ごとの脅威の整理」では、かかる被害の原因となる業務用サーバや業務用端末、MES 等に対する不正アクセスや情報漏えいを記載することとなる。

＜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
- 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)
- ステークホルダー関連図(2-1(2)にて作成)
- システムを構成する機器の一覧(2-1(3)にて作成)
- システム構成図、データフロー図(2-1(4)にて作成)

＜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記述する。

＜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 27001:2013(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、以下に示す事業リスク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

- セキュリティインシデントによりもたらされ得る結果によって、企業の評判や評価、財務状況等が更なる影響を受ける可能性がある。そのため、例えば、上記に示す事業リスクに加えて、以下の観点からリスクを特定することも検討する。
  - 企業の評判や評価の低下に伴う企業イメージ・収益の悪化
  - 企業の評判や評価の低下に伴う事態収拾・信頼回復に係るコストの増大

- 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＞

- 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 9 セキュリティインシデント及びその結果(イメージ)[12]

(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

まず、「2-1. リスクアセスメント、リスク対応に向けた事前準備」における「(5)目標とするリスクの水準」や図 6、図 7 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. リスクアセスメント」における「(1)セキュリティインシデント及びその結果」で整理したセキュリティインシデント及びその結果の深刻度を勘案し、機器・システムの重要度(被害を受けた際の影響の大きさ)を一覧化する。

[12] 図 9 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 9 で示したもの以外についても起こり得ることに留意されたい。

機器・システムの重要度の判断基準を特定することによって、想定されるセキュリティインシデント及びその結果におけ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特定する。
2. 1 で特定された判断基準に基づいて機器・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)やかかる規格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が、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度を評価することに留意されたい。
- 重要度の判断基準は、「2-1.リスクアセスメント、リスク対応に向けた事前準備」における「(5)目標とするリスクの水準」で作成した目標とするリスクの水準と整合をとる必要がある。

＜成果物＞

- ステークホルダーごとに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。

図 10 判断された重要度の一覧(イメージ)

(3) リスクのマッピング結果

「2-2.リスクアセスメント」における「(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」で整理し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「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。

このマッピングによって、相対的にリスクが大きいとされる機器・システム(及びリスク)を把握し、リスク対応の方向性を検討することが可能となる。

＜収集しておくべき情報(例)＞

- 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)
- 判断された重要度の一覧(2-2(2)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」に機器・システムをマッピングする。

- 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器・システムをマッピングする。
- 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、その機器・システムごとにマッピングする。

＜成果物＞

- マッピング結果

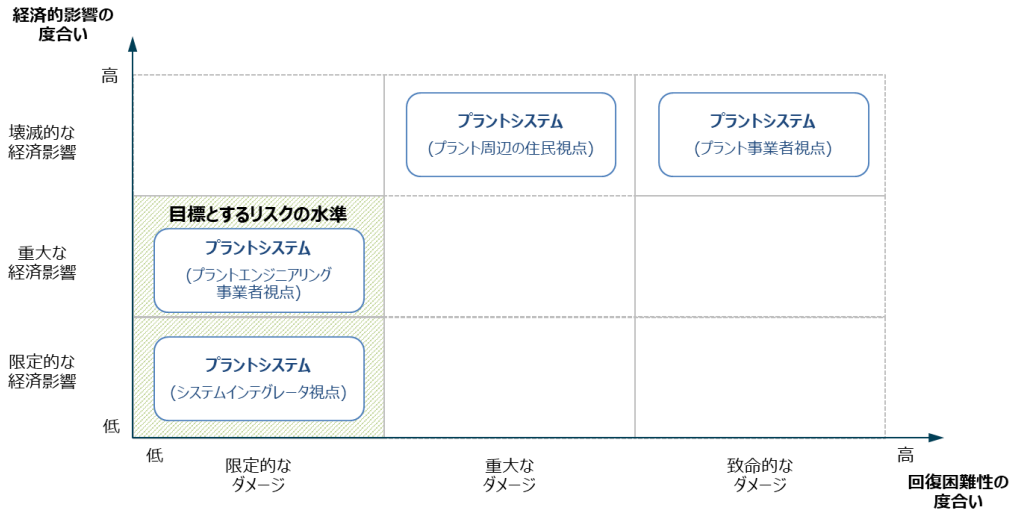

図 11 リスクのマッピング結果(イメージ)

2-3 リスク対応

本節では、以下の情報を整理する。

(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. リスクアセスメント、リスク対応に向けた事前準備」における「(3)システムを構成する機器の一覧」で作成したシステムを構成する機器の一覧や「2-2.リスクアセスメント」における「(1)セキュリティインシデント及びその結果」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. セキュリティインシデントが生じ得る機器ごとに想定される脅威を記述する。
3. セキュリティインシデント及びその結果を踏まえて、脅威ごとに生じ得るインシデントを記述する。

- 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・システム及びかかる機器・システムにて想定されるセキュリティインシデントに関連した脅威が明示されている。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.リスクアセスメント」における「(1)セキュリティインシデント及びその結果」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)を参照することもできる。

＜成果物＞

- 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。
	…	…
…	…	…

(2) 脅威に対する対策の洗い出し

「2-3.リスク対応」における「(1)機器ごとの脅威」で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。

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)
- マッピング結果(2-2(3)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)ごとに記述する。
   (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)ごとに記述する。
   (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)ごとに記述する。
   (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)ごとに記述する。

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、上記で記述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のみを記述する。

＜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」を参考とすることができる。
- 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＞

- 脅威に対する対策の一覧

表 3 脅威に対する対策の一覧(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)脅威に対する対策の洗い出し」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。

脅威に対する対策をすべて実装し、想定されるリスクを最小化することが理想であるが、対策の実施はコストを伴うので、現実的には全ての対策を実装することはできない。対策の絞り込みを行う際には、以下の＜作成方法＞に示す考え方を参考にしつつ対策の優先順位付けを行った上で、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各ステークホルダーが実施できる粒度で対策を整理することができるようになる。

なお、適用主体に関係する業界団体で公開されているガイドラインや基準がある場合には、かかるガイドラインや基準を参考にした上で対策の優先順位の決定に係る考え方を整理されたい。

＜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。
- 「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＞

- 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				

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)(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			●	

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”