経済産業省

資料５

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 (概要版)

令和４年４月

経済産業省 商務情報政策局
サイバーセキュリティ課

1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

2. 本ユースケース集の構成

3. 各ユースケースの概要

1-1. IoT-SSFの概要

- 分野横断の共通課題を検討するために、3つの**タスクフォース（TF）を設置。**
- 『第2層』TF活動の成果として、IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）を公開（2020年11月5日）。

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）
Industry by Industryで検討
(分野ごとに検討するためのSWGを設置)

- **ビルSWG**
  - ガイドライン第1版の策定(2019.6)
- **電力SWG**
  - 小売電気事業者ガイドライン策定(2021.2)
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドライン1.0版を公表(2020.12)
- **スマートホームSWG**
  - ガイドライン1.0版を公表(2021.4)
- **宇宙産業SWG**
  - 2022年2月に第4回を開催
- **工場SWG**
  - 2022年2月に第2回を開催
- ・・・

分野横断SWG

『第3層』TF：『サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
データの信頼性確保に向け「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮）」案のパブリックコメント（2回目）を実施。

ソフトウェアTF：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース

検討事項：
OSSの管理手法に関するプラクティス集を策定、SBOM活用促進に向けた実証事業（PoC）を実施。

『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」を公開。

1-1. IoT-SSFの概要

- IoT-SSFは、IoTが社会に効果的に需要できるようIoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有するための「基本的共通基盤」を提供するものである。

IoT-SSFの基本情報

 **背景**	• サイバー空間とフィジカル空間をつなぐ機器・システムのセキュリティ・セーフティに関して、包括的に課題を捉える**統一的な手法が欠如**しているため、それぞれの分野/業界において別々の検討プロセスを経て、**独自のセキュリティ・セーフティ対策等が設定されることが懸念される**。 • それぞれの対応策に不整合が生じれば、**社会として新たな仕組みを受容・管理していくためのコストが増大する**おそれがある。
 **目的**	• **異なる分野/業界のプレーヤー**がサイバー空間とフィジカル空間をつなぐ機器・システム、つまり IoT 機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有するための**「基本的共通基盤」**を提供し、**IoTという新たな仕組みを社会として効果的に受容できる**ようにすることを目的とする。
 **想定読者**	• IoTを活用してサイバー空間とフィジカル空間をつなぐ新たな仕組み・サービスを実現しようとする者 • そのような新たな仕組み・サービスで活用されるIoT機器・システムの開発を行う者 • そのような新たな仕組み・サービスを適切に管理していく制度・環境を実現していこうとする者そのような新たな仕組み・サービスを受ける者

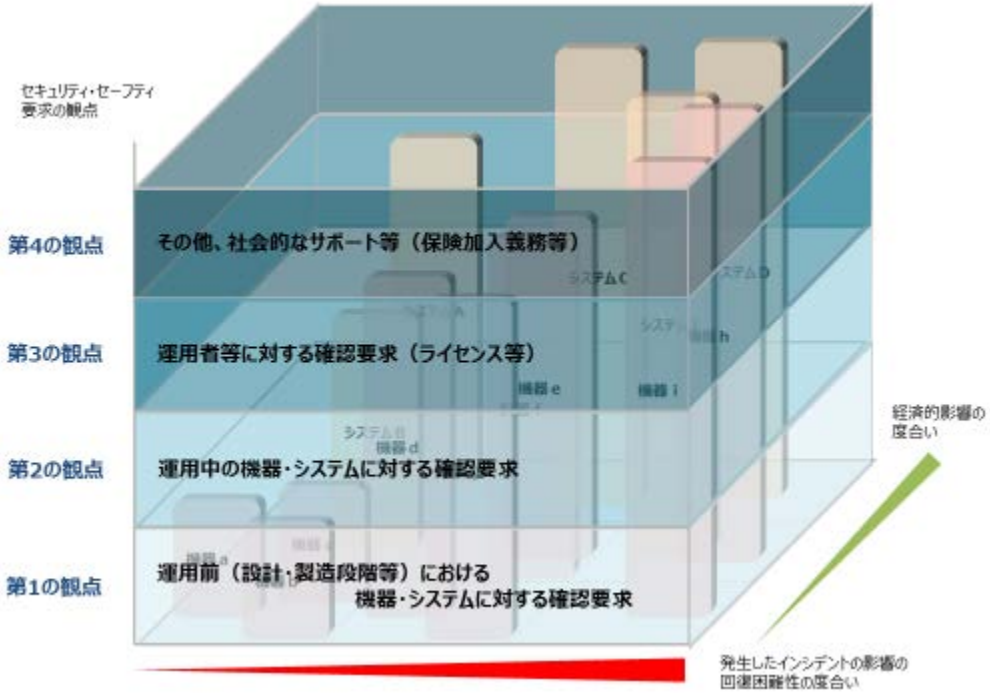
1-1. IoT-SSFの概要

- 本フレームワークで、IoT機器・システムをカテゴライズし、カテゴリごとに求められるセキュリティ・セーフティ要求の観点を把握・比較することにより、**それぞれに求める対策の観点・内容の整合性を確保できる**。

フィジカル・サイバー間をつなげる
機器・システムのカテゴライズのイメージ

※　同じ機器・システムでも使用形態などによってマッピング先が異なり得る。
例えば、機器ｇと機器ｈが同じ機器で異なる使用形態である場合などがあり得る。）

カテゴリに応じて求められる
セキュリティ・セーフティ要求の観点のイメージ



1-2. 策定時に指摘された課題

- 第4回までのTFやパブリックコメントにて寄せられたご意見を踏まえ、IoT-SSFをより活用しやすいものにすることを目的として、IoT-SSFのユースケースを作成する。

＜寄せられたご意見＞

- IoT-SSFがIoT機器・システムのセキュリティに係る様々な主体に適用可能な「基本的共通基盤」を提供していることを評価する。
- 一方で、 IoT-SSFには抽象度が高い部分も含まれているため、読者にとって理解が難しい部分がある可能性がある。
- IoT-SSFにて示されたリスクのマッピング手法やカテゴライズ手法に関する指針もしくはガイドラインの整備が必要ではないか。

＜本文での記載＞

- 今後、本フレームワークに基づいて、具体的な仕組み・サービスをユースケースとして整理していくことで、IoTが広く活用されるサイバー空間とフィジカル空間が高度に融合した社会におけるセキュリティ・セーフティ対策を適切に実施していく制度的対応の整備を進めていくための基礎的条件を整えて行く必要がある。

1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

2. ユースケース集の構成

3. 各ユースケースの概要

3-1.家庭用ガス給湯器の遠隔操作
3-2.ドローンを活用した個人による写真撮影
3-3.物流倉庫内のAGVによる自動ピッキング
3-4.化学プラント施設内の蒸留工程の自動制御
3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
3-6.金属製造現場の温度センサ等による製造設備の状態監視

2-1. ユースケース集の目次

- 2-1で、ユースケース選定の考え方及び具体的な選定基準を示す。2-2で各ユースケースに共通する事項を記載した上で、2-3で具体的な6種類のユースケースを示す。

- 添付Aと添付Bは、各ユースケース固有の事情に依存しない一般的に適用し得る内容
- 想定読者において具体的な対策を検討する際に適宜参照

2-1.「本文書の位置付けと構成」の概要

- 「IoTセキュリティ・セーフティ・フレームワーク」の概要、位置づけと構成、想定読者と利用用途を記載。

1-1 「IoTセキュリティ・セーフティ・フレームワーク」の概要

- IoTという新たな仕組みを社会として効果的に受容できるにすることを目的として、IoT機器・システムについて、リスクの捉え方とその対応に係る基本的な考え方を集約した3つの軸を活用し、機器・システムをカテゴライズするとともに、適切な対策の内容を整理して比較・検討することを提案。

1-2 本文書の位置づけと構成

- 本稿では、今後様々な分野/業界のプレーヤーが、IoT-SSFを「基本的共通基盤」として活用するために、既存のリスクマネジメントのプロセスも考慮しつつ、一連のIoT-SSFの適用の流れを複数のユースケースを用いて例示する。
- 本章を導入として、2章ではユースケース選定の考え方(2-1)、各ユースケースに共通する記載項目(2-2)、6件の具体的なユースケース(2-3)を記述する。

- 添付としては、本編でも参照されるセキュリティ、セーフティの確保に資する対策要件（添付A）、添付Aに示された対策要件ごとに実際に講じる対策の例（添付B）を整理している。これらは各ユースケース固有の事情に依存しない一般的に適用し得る内容を示しているため、想定読者において具体的な対策を検討する際に適宜参照されたい。

- 本稿における用語法は、「サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0」（以下、「CPSF」という。）及びIoT-SSFに準じることとする。各種用語定義については、それらを参照されたい。

1-3 想定読者と利用用途

主にIoT機器・システム及び関連サービスに係る様々な主体（事業者）により活用されることを想定する。

- IoT機器・システムを通じて提供されるサービスのユーザ （IoT利用者）
- IoT機器・システムを通じて提供されるサービスの開発者 （IoTサービス開発者）
- IoT機器・システムを通じて提供されるサービスの提供者 （IoTサービス提供者）
- IoT機器・システム及び関連サービスを適切に管理する制度・環境を検討する者

2-2.「対象となるユースケース」の概要

- ユースケース選定の考え方及び具体的な選定基準を示す。

選定にあたっての考え方	民間事業者がIoT-SSFを活用して各自で対策を検討でき、**幅広い読者にとってIoT-SSFが参考**となるよう、ユースケースを選定する

観点	選定基準
利用者の区分（誰が）	• 機器・システムの利用者の区分に偏りが生じず、ある程度の網羅性を確保できるようにユースケースを選定する。
利用環境（どこで）	• 機器・システムの利用環境に偏りが生じず、ある程度の網羅性を確保できるようにユースケースを選定する。
対象の機器・システム（何を）	• 利用が特定の事業者等に限定されない、汎用的な機器・システムを扱うユースケースを選定する。 • 現時点で普及している、もしくは、これから普及が見込まれる機器・システムに関するユースケースを選定する。
想定されるリスクと対策（どのように）	• 機器・システムに係る使用上のリスク及び当該リスクへの対処方法において、他のユースケースと比較して、特徴的な考慮事項があるようなユースケースを選定する。

2-2.「対象となるユースケース」の概要

- 選定基準を踏まえて６種類のユースケースを選定する。

No	利用者の区分	利用環境	ユースケース	想定する適用主体	具体的な選定理由
1	個人または家庭	家庭	**家庭用ガス給湯器の遠隔操作**	IoTサービス開発者、IoTサービス提供者(ガス給湯器製造事業者)	• 家庭用ガス給湯器は現状多くの住宅等に備えられており、その遠隔操作についても、今後利用の拡大が見込まれるため • インシデントが利用者の負傷につながりやすく、セーフティの側面がより重要となるケースであるため
2		公共空間	**ドローンを活用した個人による写真撮影**	IoTサービス開発者、IoTサービス提供者(ドローン機器事業者)	• ドローンは多種多様な活用方法が想定される機器であり、ビジネス用途を含めて、今後様々な業界で利用の拡大が見込まれるため • 利用者に限らず周囲のヒトやモノへ被害を及ぼす可能性があり、利用者のスキルや社会的な制度等が要求事項として含まれ得るため
3	事業者(主に産業)	物流現場	**物流倉庫内のAGVによる自動ピッキング**	IoT利用者(物流事業者)	• AGVは様々な利用シーンでの活用が想定される機器であり、物流業界や製造業界等において今後利用の拡大が見込まれるため • 機器・システムの停止等が、サプライチェーンにおける多くのステークホルダーに影響しやすいケースであるため
4		製造現場(原料製造)	**化学プラント施設内の蒸留工程の自動制御**	IoT利用者(プラント事業者)	• 自動制御システムは既に多くの現場で採用されており、特にPA（Process Automation）技術を活用する事業者にとって参考になると考えられるため • 自動制御システムの停止等、可用性の損失が課題になるケースであるため
5		製造現場(製品製造)	**工場内のロボットによる部材加工作業（溶接工程）の自動化**	IoT利用者(自動車部品製造事業者)	• 製造現場におけるロボットは引き続き利用の拡大が見込まれており、特にFA（Factory Automation）技術を活用する多くの事業者にとって参考になると考えられるため • 制御データの改ざんによる異常動作及びそれに伴う品質劣化等が課題になるケースであるため
6			**金属製造現場の温度センサ等による製造設備の状態監視**	IoTサービス開発者、IoTサービス提供者(サポート事業者)	• 温度センサ等による設備の状態監視は産業用途（例：原料製造、製品製造）における共通的な要素であり、多様な現場にて参考になると考えられるため • 状態監視は品質管理上、重要な要素であり、これらに関連するインシデントが事業者にとっての大規模な経済影響等につながりやすいため • 遠隔にて設備の状況を監視する点は、各種サービス業においても参考になると考えられるため

2-3.「ユースケースにおける記載事項」の概要

- 「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、「分析対象の明確化」、「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」、「リスク分析の実施」及び「リスク対応」のステップでリスクマネジメントを実施するとしている。
- 上記を踏まえ、以下のステップでリスクマネジメントを実施し、個別のユースケースを整理した。

1 リスクアセスメント、リスク対応に向けた事前準備

- 事前準備として必要となる以下の情報を整理する。
  - ✓ 対象ソリューションの概要
  - ✓ ステークホルダー関係図
  - ✓ 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
  - ✓ リスク基準

2 リスクアセスメント

- 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」の判断基準を考慮し、IoT機器システムをマッピングする。
  - ✓ 想定されるセキュリティインシデント等とその結果の特定
  - ✓ 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
  - ✓ マッピング結果の整理と評価の実施

3 リスク対応 (ステークホルダー別の対策要件一覧)

- リスク対応を行うステークホルダーが実際に講じる対策を以下の項目に沿って整理する。
  - ✓ システムを構成する機器ごとの脅威の整理
  - ✓ 脅威に対する対策の整理
  - ✓ 整理した対策に対する意思決定

※IoT利用者、IoTサービス開発者、IoTサービス提供者においては、現場の担当者だけではなく経営層と一体となって全社的にリスクに対応することが望ましい。

2-4.「添付A 対策要件」の概要

- 添付Aでは、IoT-SSFの第3軸「求められるセキュリティ・セーフティ要求」における4つの観点を参照しつつ、有効と考えられる対策要件を示す。

観点	実装先	対策要件
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
		運用前（設計・製造段階）におけるIoTセキュリティを目的とした体制の確保
		IoTセキュリティに関するステークホルダーの役割の明確化
		IoT機器・システムに係る要員のセキュリティ確保
	システム	運用前（設計・製造段階）における法令および契約上の要求事項の遵守
		企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		適切な水準のアクセス制御の実装
		ソフトウェアの完全性の検証
		ソフトウェアのインストールの制限
		様々なIoT機器に接続する際のセキュリティの確保
		暗号化によるデータの保護
		ライフサイクルを通じた暗号鍵の管理
第1の観点	システム	マルウェア対策の実施
		IoT機器・システムの十分な可用性の確保
		IoTに適したネットワークの利用
		適切なネットワークの分離
		IoT機器・システムの設置場所等に対する物理的アクセスの制御
		IoT機器システムの構成要素（機器、ネットワーク等）の物理的保護
		セキュリティ設計と両立するセーフティ設計の仕様化
		セキュアな開発環境と開発手法の適用
		IoT機器・システムにおけるセキュリティ機能の検証
		信頼できるIoT機器やサービスの選定
		IoT機器・システムの出荷時における安全な初期設定と構成
		IoT機器・システムにおける運用開始時の正しい設置、設定

※上記に加えて、CPSF「添付 C 対策要件に応じたセキュリティ対策例」を参照した上で、対策要件を検討することが望ましい。

2-4.「添付A 対策要件」の概要

- 添付Aでは、IoT-SSFの第3軸「求められるセキュリティ・セーフティ要求」における4つの観点を参照しつつ、有効と考えられる対策要件を示す。

観点	実装先	対策要件
第2の観点	ソシキ・ヒト	利用者へのリスクの周知等の情報発信
		運用中におけるIoTセキュリティを目的とした体制の確保
		過去の対応事例からの学習
		脆弱性対応に必要な手順等の整備と実践
	プロシージャ	インシデント対応手順の整備と実践
		事業継続計画の策定と実践
		IoT 機器・システムの適正な使用
		IoT 機器・システムの適正な運用・保守
	システム	運用中における法令および契約上の要求事項の遵守
第2の観点	システム	継続的な資産管理
		プログラムソースコード及び関連書類の保護
		IoT機器・システムのモニタリング及びログの取得、分析
		IoT機器・システムに対するアップデートの適用
		IoT機器・システムの安全な廃棄または再利用
第3の観点	ソシキ・ヒト	IoT機器・システムの運用・管理を行う者に対する要求事項の特定
		IoT機器・システムの運用・管理を行う者に対する要求事項の遵守の確認
第4の観点	ソシキ・ヒト	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

2-5.「添付B 対策例」の概要

- 添付Bでは、事業者が具体的なセキュリティ対策等を検討する際に参照できる情報として、添付Aに示された対策要件ごとに講じる対策の例を示す。

実際に講じる対策の例

観点	実装先	対策要件	対策例	対応するCPSFの対策要件ID
第1の観点	**ソシキ・ヒト**	**対象のIoT機器・システムにおけるセキュリティポリシーの策定**	● 自組織が提供または利用するIoT機器・システム、サービスのセキュリティに関する方針（ポリシー）を策定し、社内に周知するとともに、継続的に実現状況を把握し、定期的にレビューする。 - かかるポリシーとして、自組織の役割に応じて、IoT機器・システムの管理のポリシー、IoTサービス提供のポリシー、個人情報を含むデータ管理などのポリシー等が策定され得る。 - IoT機器・システム、サービスのセキュリティポリシーは以下の事項に関する記述を含むことが望ましい。 ➢ 対象となるIoT機器・システム、サービスの概要 ➢ IoT機器・システム、サービスに係る自組織の役割（例：IoTユーザ、IoTサービス提供者、IoTサービス開発者） ➢ IoT機器・システム、サービスに対するセキュリティ対策の目的 ➢ 組織内におけるIoT機器・システム、サービスのセキュリティに対する役割と責任	CPS.BE-2 CPS.GV-1 CPS.GV-2
			● 上記の全体的な方針に加え、特定のIoT機器・システム、サービスを対象としたより具体的なポリシー、対策基準等を策定する。かかる対策基準等のトピックとして、以下の事項に関する記述を含むことが望ましい。 - アクセス制御 - 情報分類及び取扱い - その他の対策領域	
…		…	…	…

1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

2. 本ユースケース集の構成

3. 各ユースケースの概要

3-1.家庭用ガス給湯器の遠隔操作

3-2.ドローンを活用した個人による写真撮影
3-3.物流倉庫内のAGVによる自動ピッキング
3-4.化学プラント施設内の蒸留工程の自動制御
3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
3-6.金属製造現場の温度センサ等による製造設備の状態監視

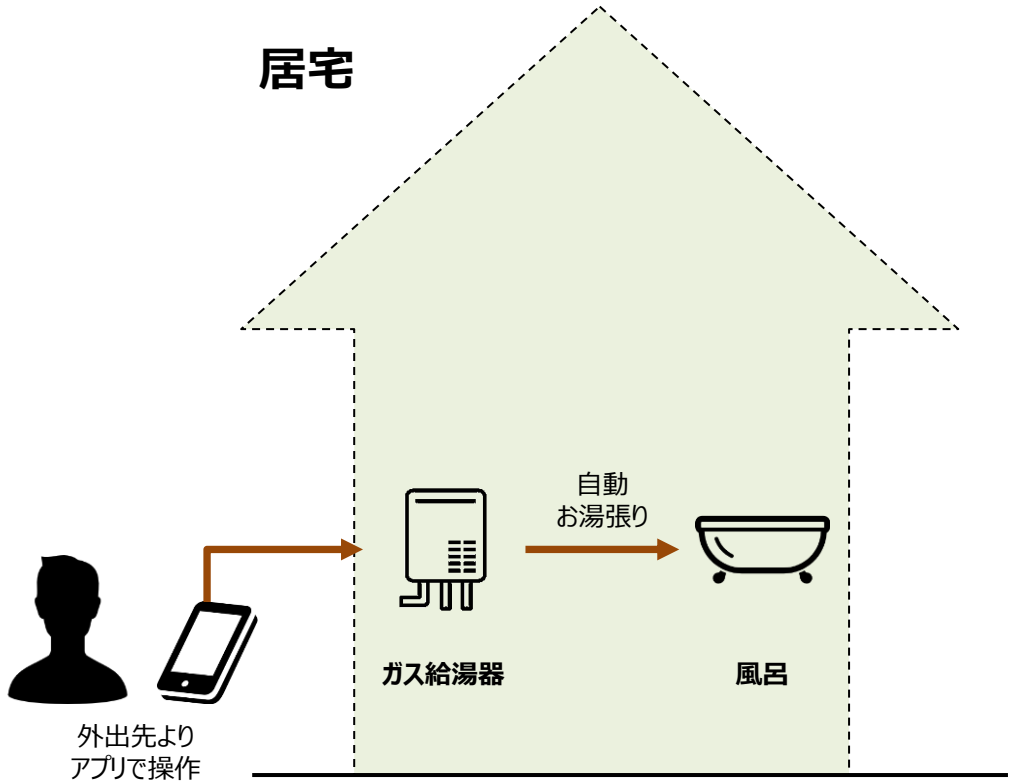
3-1.ガス給湯器の遠隔操作（ガス給湯器）

①リスクアセスメント、リスク対応に向けた事前準備->対象ソリューションの概要

- 本ユースケースの適用主体は、ガス給湯器の製造元であるスマートホーム向けのIoT機器を開発・生産・販売する事業者とする。
- 当該事業者は、既にスマートホームを供給する事業者等と協力して製造販売しているガス給湯器を活用して、新たにIoT機器サービスを企画しており、サイバーセキュリティに関するリスクを懸念している。

- 外出先よりスマートフォンの専用アプリケーションを活用して、自宅のお風呂のお湯張りを行う。
- なお、ガス給湯器は「自然給排気式・開放式」以外の機器を想定している。これは、「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）にて「自然給排気式・開放式」の遠隔操作が禁止されているため。（※）

※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」（令和2年7月）では、「自然吸排気式」及び「開放式」以外の機器において「リスク低減策を講じることにより遠隔操作に伴う危険源がないと評価されるもの等の基準に合致し、危険が生じるおそれがないものは、操作可能」とされている。

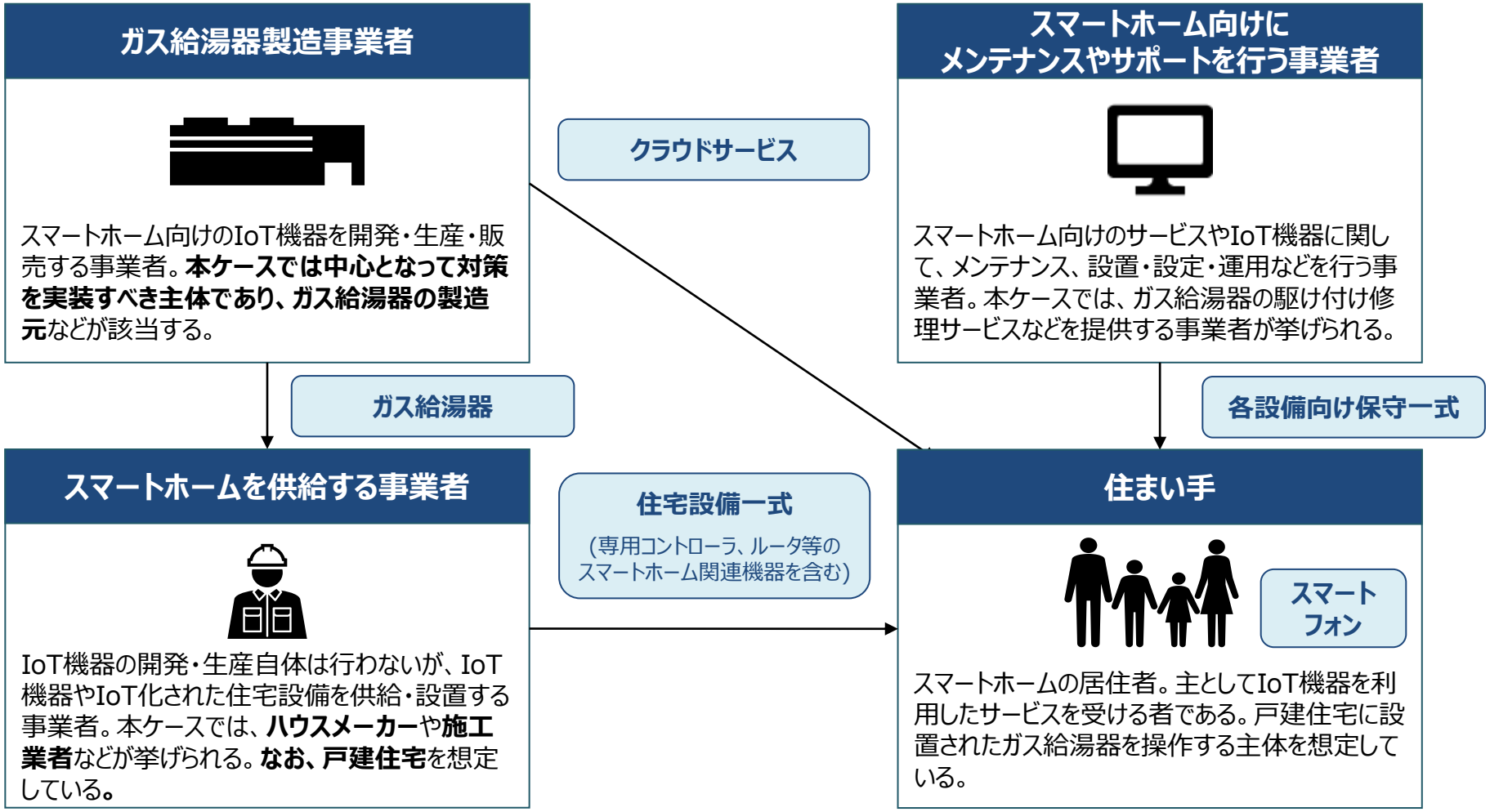


[参考] 経済産業省「令和２年度 産業保安等技術基準策定研究開発等事業 （電気用品等製品の IoT化等による安全確保の在り方に関する動向調査）」等

3-1.ガス給湯器の遠隔操作（ガス給湯器）

①リスクアセスメント、リスク対応に向けた事前準備->ステークホルダー関係図

- ステークホルダーは、「スマートホーム向けIoT機器の事業者」「スマートホームを供給する事業者」「スマートホーム向けにメンテナンスやサポートを行う事業者」「住まい手」の４者。



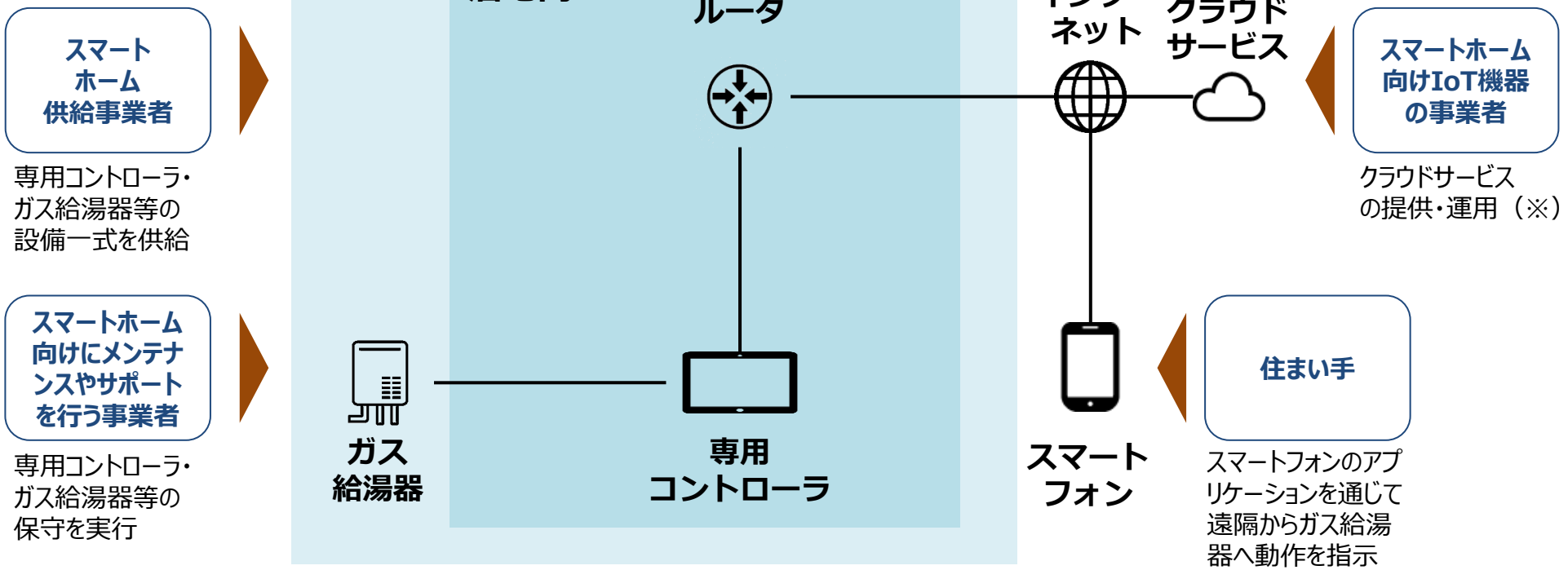
[参考] 経済産業省「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドラインスマートホームガイドライン」等

3-1.ガス給湯器の遠隔操作（ガス給湯器）

①リスクアセスメント、リスク対応に向けた事前準備->システム構成図

- システムを構成する機器は以下を想定。

システムを構成する機器の一覧
ガス給湯器
専用コントローラ
ルータ
スマートフォン（アプリ）
クラウドサービス



※実際の運用は他のITサービス事業者に委託する場合がある。

[参考] 経済産業省「令和２年度 産業保安等技術基準策定研究開発等事業 （電気用品等製品の IoT化等による安全確保の在り方に関する動向調査）」等

3-1.ガス給湯器の遠隔操作（ガス給湯器）
②リスクアセスメント->想定されるセキュリティインシデント等とその結果の特定

- ステークホルダーごとにリスクアセスメントを行うにあたり、対象機器・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及び想定される被害（例）を整理。

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)
スマートホーム向けIoT機器の事業者にとってのリスク	クラウドサービスから専用コントローラに送信される**データがネットワーク上で改ざん**されることによって、ガス給湯器が想定していない動作をする。	住まい手が異常に気づかずに入浴することによって、やけど等を負う。その結果、 **製品回収等が生じ得る。**また、**製品・サービスの品質について利用者の間に疑念が広がり得る。**
スマートホーム向けにメンテナンスやサポートを行う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、配信先の専用コントローラ等が**マルウェア感染**し、想定していない動作をする。	住まい手が異常に気づかずに入浴することによって、やけど等を負う。その結果、**製品回収が生じ得る**。また、**サポートの品質について利用者の間に疑念が広がり得る。**
住まい手にとってのリスク	改ざんされたアップデートプログラムの配信等により専用コントローラが**マルウェア感染**し、ガス給湯器が想定していない動きをする。	異常に気づかずに入浴することで、**やけど等を負う可能性がある。**
	悪意のある攻撃者やIoT機器・サービスの事業者が、クラウドサービスに対して**不正アクセス**する。	**個人情報が流出し得る。**
	クラウドサービスからから専用コントローラに送信される**データをネットワーク上で改ざん**されることによって、ガス給湯器が想定していない動作をする。	異常に気づかずに入浴することで、やけど等の重症を負う。その結果、**生活に支障をきたし得る。**
スマートホームを供給する事業者にとってのリスク	（スマートホームを供給する事業者のリスクは限定的であると想定されるため、ここでは詳細を記載しない。）	

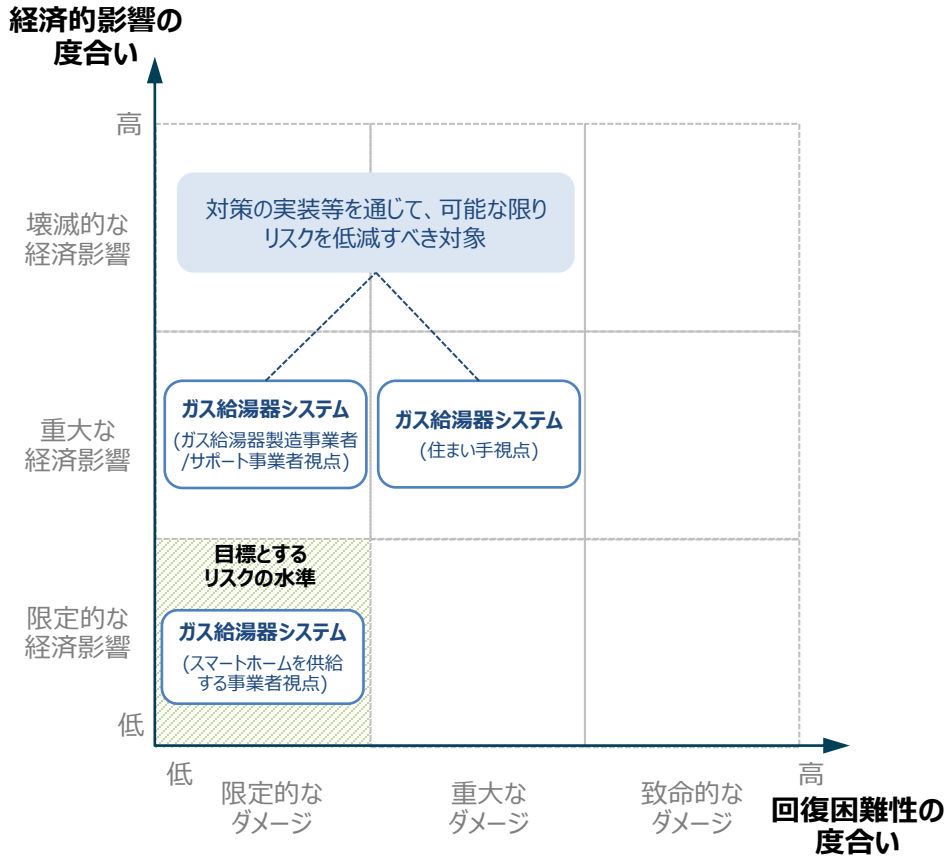
3-1.ガス給湯器の遠隔操作（ガス給湯器）
②リスクアセスメント->マッピング結果の整理と評価の実施

- 誤動作等により被るリスクが大きくなり得ると想定される「住まい手」は、一般にセキュリティに関する知見を十分に持たない場合が多いため、IoT-SSFの適用主体である「ガス給湯器製造事業者」は、これを考慮してリスクの低減に努める必要がある。

リスクの大きさ（※1）

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(※2)
スマートホーム向けIoT機器の事業者	• 従業員が重症を負う可能性は低い。	• 大規模な製品回収につながるおそれがある。
スマートホーム向けにメンテナンスやサポートを行う事業者	• 従業員が重症を負う可能性は低い。	• 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。
住まい手	• 個人情報が流出する可能性がある。 • やけど等の重症を負う可能性がある。	• 重症を負った場合、生活に支障をきたい得る。
スマートホームを供給する事業者	• 従業員が重症を負う可能性は低い。	• 大規模な製品回収が発生したとしても、大きな影響はない。

想定されるリスク(例)のマッピング結果

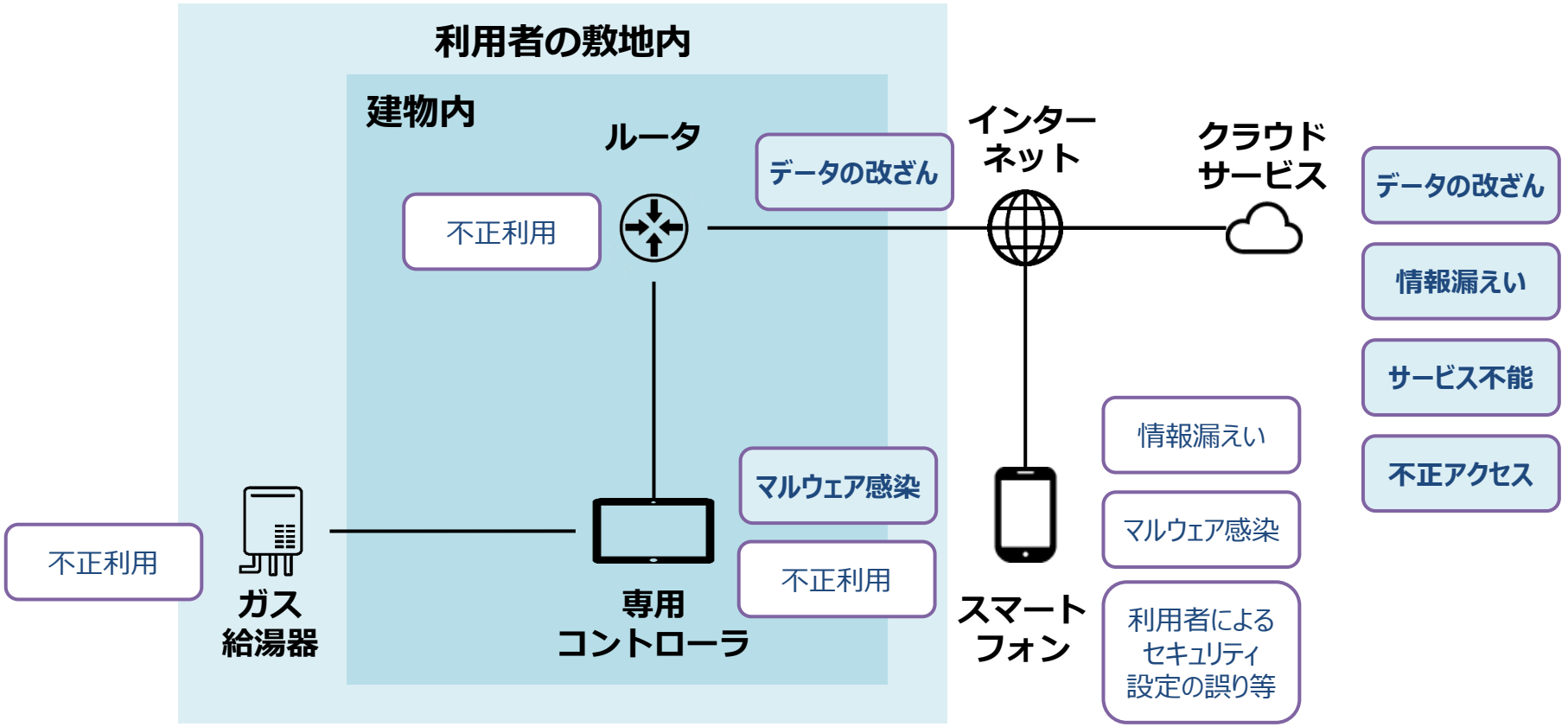


※1：「回復困難性の度合い」及び「経済的影響の度合い」では、主要な被害のみを記載していることに留意。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

3-1.ガス給湯器の遠隔操作（ガス給湯器）
③リスク対応->システムを構成する機器ごとの脅威の整理

- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

3-1.ガス給湯器の遠隔操作（ガス給湯器）
③リスク対応->脅威に対する対策の整理

- 適用主体であるIoT機器・サービスの事業（ガス給湯器等の製造元）は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討する。

住まい手にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
自社製品・サービスの利用者をけがや、やけどから守るための対策の徹底	• IoT機器・システムの出荷時における安全な初期設定と構成 • セキュリティ設計と両立するセーフティ設計の仕様化
ガス給湯器システムに対するリスクや安全な使用方法に関する情報提供の実施	• 利用者へのリスクの周知等の情報発信 • 運用手順や利用手順の文書化等の運用・管理を行う者への支援の実施

ガス給湯器製造事業者(自身)にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進	• 運用前（設計・製造段階）における法令および契約上の要求事項の遵守 • 企画・設計段階におけるセキュリティ要求事項の分析及び仕様化 • セキュリティ設計と両立するセーフティ設計の仕様化

サポート事業者にとってのリスクを低減するため対応を要請する対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
ガス給湯器に対する安全なアップデート等の脆弱性対応の実施	• プログラムソースコード及び関連書類の保護 • IoT機器・システムに対するアップデートの適用

※セキュリティインシデントによっては、ガス給湯器製造事業者はガス供給事業者と連携して対応することが必要となる場合がある

3-1.ガス給湯器の遠隔操作（ガス給湯器）
③リスク対応->脅威に対する対策の整理

- 想定される脅威を踏まえ、第3軸「求められるセキュリティ・セーフティ要求」における観点ごとにスマートホーム向けIoT機器・サービスの事業者にて実装が想定される対策要件を整理する。

スマートホーム向けIoT機器・サービスの事業者にて実装が想定される対策要件の例

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般[1]	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の明確化
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	運用前（設計・製造段階）における法令および契約上の要求事項の遵守
		全般	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		不正アクセス	適切な水準のアクセス制御の実施
		全般	IoT 機器・システムにおける運用開始時の正しい設置、設定
第 2 の観点	ソシキ・ヒト	全般	利用者へのリスクの周知等の情報発信
		全般	運用中における IoT セキュリティを目的とした体制の確保
		全般	過去の対応事例からの学習
	プロシージャ	全般	インシデント対応手順の整備と実践
		全般	運用手順や利用手順の文書化と提示
		全般	IoT 機器・システムの適正な使用
		全般	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令および契約上の要求事項の遵守
		不正アクセス マルウェア感染	継続的な資産管理の実施
		全般	プログラムソースコード及び関連書類の保護
		不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
		全般	IoT 機器・システムに対するアップデートの適用
第 3 の観点	ソシキ・ヒト	全般	IoT 機器・システムの運用・管理を行う者への要求事項の特定
		全般	IoT 機器・システムの運用・管理を行う者への要求事項の遵守の確認

3-1.ガス給湯器の遠隔操作（ガス給湯器）
③リスク対応->整理した対策に対する意思決定

- 影響度が大きいリスクに対処するための対策方針を踏まえて実装することとした対策例は、以下の通り。

観点	対策要件	実際に講じる対策の例
第1の観点	**運用前（設計・製造段階）における法令および契約上の要求事項の遵守**	• 本件に関連する法的、規制（例：製品安全関連法）又は契約上の義務の明確化及び、それらの違反を避けるための要求事項の遵守
	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化	• ガス給湯器システムの企画・設計時におけるリスクアセスメントの実施、セキュリティ要件の特定、要件の実装に係る費用の確保 • 必要なセキュリティ仕様が組み込まれているかを確認する設計レビューの実施
	セキュリティ設計と両立するセーフティ設計の仕様化	• ガス給湯器の近くにいる人や機器の周辺への危害を回避するための安全機能（本質安全設計、予防安全機能 等）の実装 • ガス給湯器等に実装された安全機能と外部との通信回線との分離
	IoT機器・システムの出荷時における安全な初期設定と構成	• ガス給湯器システムを構成する機器の不要なネットワークポート、その他USBやシリアルポートなどの物理的または論理的な閉塞 • 出荷時点で明らかに不要なIoT機器・システムが提供する機能、サービス、アプリケーション、アカウントの削除または無効化 • ルータを含む機器の初期パスワードの変更を促す機能の実装 • 暗号通信機能（例：TKIP、AES）を有した居内無線LANへの接続を促すガイダンスの提供

3-1.ガス給湯器の遠隔操作（ガス給湯器）
③リスク対応->整理した対策に対する意思決定

観点	対策要件	実際に講じる対策の例
第2の観点	**利用者へのリスクの周知等の情報発信**	• スマートフォン上のアプリケーションや企業ホームページ等を通じた、ガス給湯器システムに対するリスクやスマートホームを供給する事業者または住まい手で対応すべき点に関する情報提供の実施（例えば、サポート期間終了の予告及び通知、機器・システムの重大な脆弱性、ユーザー情報の漏えいや機器のマルウェア感染等のインシデントに関する情報発信等）
	運用手順や利用手順の文書化等の運用・管理を行う者への支援の実施	• 住まい手に対する、以下の内容を含むガス給湯器システムの運用手順や利用手順の作成及び提示 ✓ 初期設定の手順 ✓ 提供者が想定する安全な利用方法 ✓ 不適切な使用によって生じ得るセキュリティ関連のリスク ✓ 不具合を発見した際の連絡先 • 運用・管理を行う者へのガイドの作成及び提示
	プログラムソースコード及び関連書類の保護	• 確立した手順に従ってプログラムソースコードを厳重に管理する • （該当する文書が書面で保管される場合）施錠可能な文書保管庫での関連書類（設計書、仕様書、検証計画書、妥当性確認計画書）の保護
	脆弱性対応に必要な手順等の整備と実践	• 新たに検知されたクラウドサービス、スマートフォン上のアプリケーション及びガス給湯器に係る脅威や脆弱性の報告窓口の設置 • 以下を含む、脆弱性対応手順の策定 ✓ 報告された脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定 ✓ 開発委託先等への修正プログラム等開発の依頼 ✓ セキュリティパッチの提供
	IoT機器・システムに対するアップデートの適用	• セキュリティパッチを提供する前に、それらが有効であることや副作用がないかについて確認を実施 • 正規のウェブサイト等から適切な方法（例：通信経路の暗号化、機器間の相互認証）によるセキュリティパッチの提供

1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

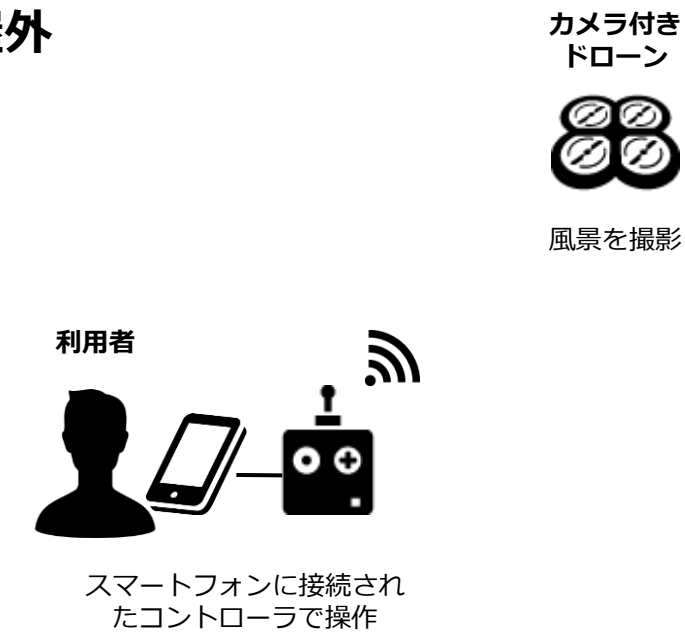
2. 本ユースケース集の構成

3. 各ユースケースの概要

3-2.ドローンを活用した個人による写真撮影（ドローン）
①リスクアセスメント、リスク対応に向けた事前準備->対象ソリューションの概要

- 本ユースケースの適用主体は、ドローン製造事業者とする。
- 新たに消費者用ドローンを企画・開発し、家電量販店もしくはECサイトでの販売を計画しているが、販売するドローンがセキュリティインシデント等によって利用者（消費者等）や周囲環境へ影響を与え得ることを懸念している。

- ドローン製造事業者は、利用者がスマートフォンに接続されたコントローラにてドローンを操作し、ドローンに設置されたカメラにて風景を撮影することを想定する。
- 利用者は公共施設内の土地（屋外）にて許可を得た上でドローンを操作するものとし、民法や自治体が定める条例に加えて小型無人機等飛行禁止法で禁止されたエリアでは操作しないものとドローン製造事業者は想定している。
- ドローンの重さは、199gを想定。飛行速度は、水平:10 m/s　上昇:3 m/s　下降:3 m/sを想定。

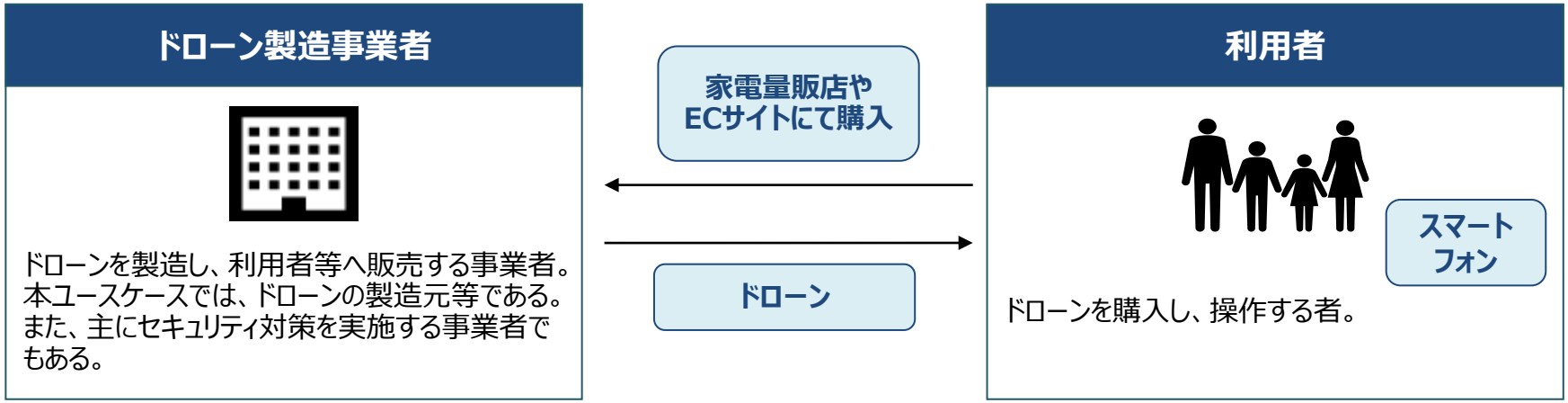


[参考] 経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」等

3-2.ドローンを活用した個人による写真撮影（ドローン）

①リスクアセスメント、リスク対応に向けた事前準備->ステークホルダー関係図

- ステークホルダーは、「ドローン製造事業者」「利用者」及び「ドローンの飛行箇所の周辺にいる第三者」の3者を想定する。

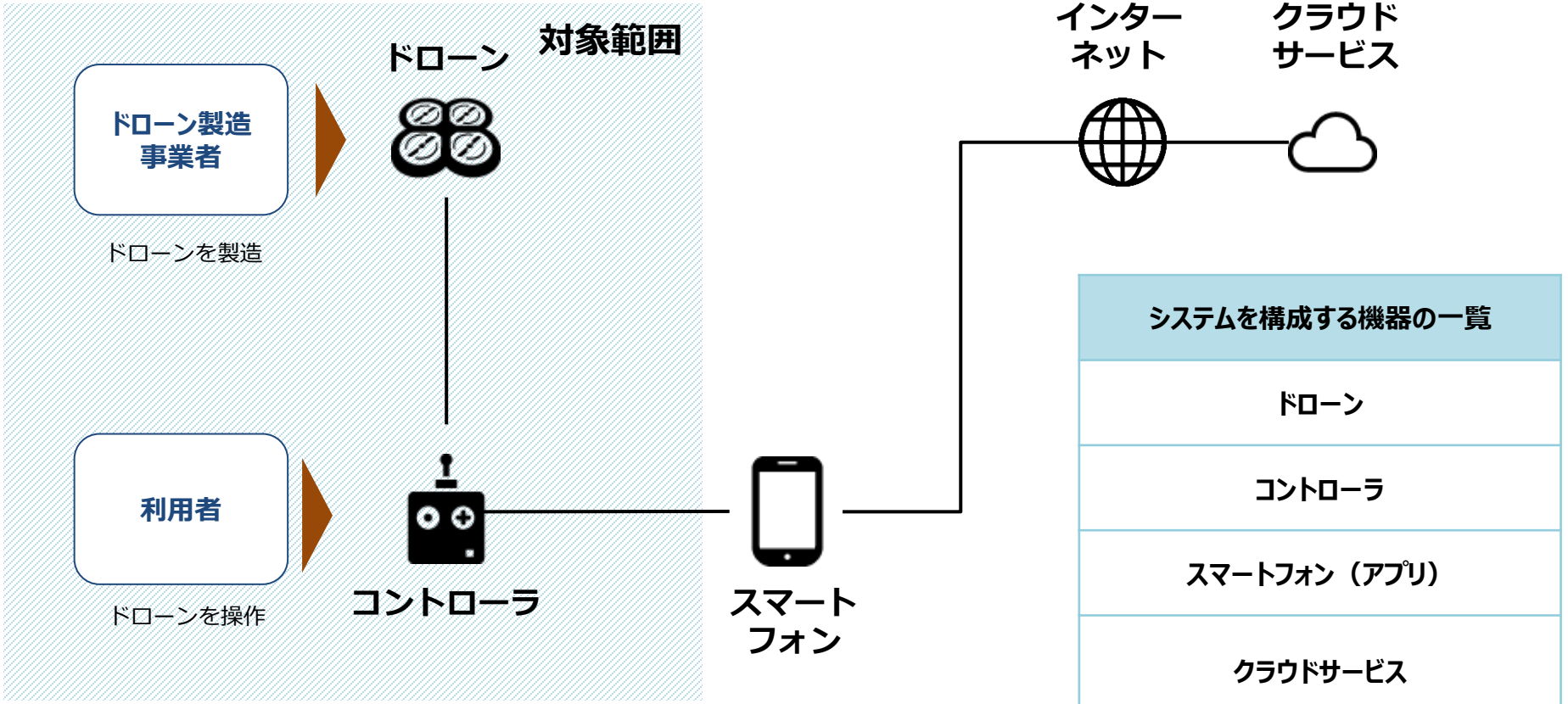


[参考]一般社団法人セキュアドローン協議会「ドローンセキュリティガイド-第2版-」等

3-2.ドローンを活用した個人による写真撮影（ドローン）

①リスクアセスメント、リスク対応に向けた事前準備->システム構成図

- システムを構成する機器は以下を想定。



システムを構成する機器の一覧
ドローン
コントローラ
スマートフォン（アプリ）
クラウドサービス

[参考] 経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」等

3-2.ドローンを活用した個人による写真撮影（ドローン）
②リスクアセスメント->想定されるセキュリティインシデント等とその結果の特定

- ステークホルダーごとにリスクアセスメントを行うにあたり、対象機器・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及び想定される被害（例）を整理。

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)
ドローン製造事業者にとってのリスク	ドローンに重大な脆弱性が発見される。	**大規模な製品回収等が生じ得る。**
利用者にとってのリスク	悪意のある攻撃者によって、**内蔵されたカメラが不正アクセスされる。**	利用者本人が映り込んだ画像や利用履歴等**の個人情報等が漏えいし得る。**
	悪意のある攻撃者によって、ドローンの**機体制御が乗っ取られる。**	ドローンが高高度から落下し、利用者が**けがをする可能性がある。**また、**けがを負うことによって生活に支障をきたし得る。**
ドローンの飛行箇所の周辺にいる第三者にとってのリスク	悪意のある攻撃者によって、**内蔵されたカメラが不正アクセスされる。**	ドローンの飛行箇所の周辺にいる第三者が映り込んだ画像や利用履歴等**の個人情報等が漏えいし得る。**
	悪意のある攻撃者によって、ドローンの**機体制御が乗っ取られる。**	ドローンが高高度から落下し、ドローンの飛行箇所の周辺にいる第三者が**けがをする可能性がある。**

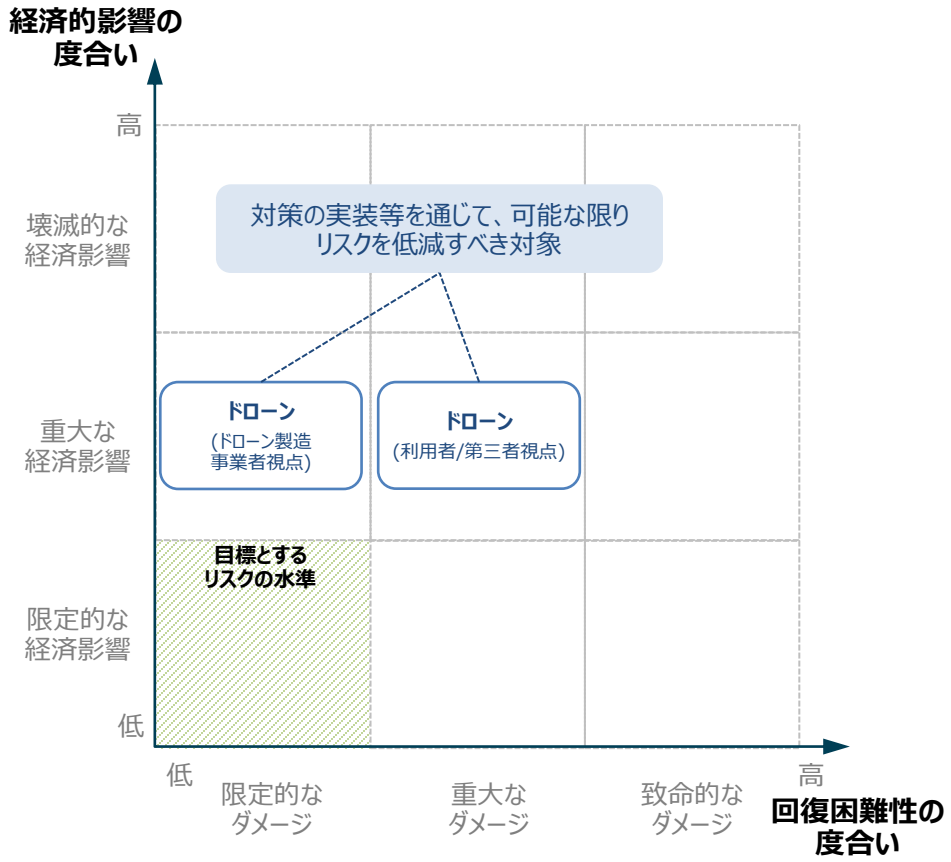
3-2.ドローンを活用した個人による写真撮影（ドローン）
②リスクアセスメント->マッピング結果の整理と評価の実施

- セキュリティインシデントによってドローンの航行に影響が及んだ場合、周辺の第三者や住宅等の環境へ影響を及ぼし得ることから、 IoT-SSFの適用主体である「ドローン製造事業者」は、「利用者」に加えて「第三者」が被り得るリスクを考慮して対策を実装する必要がある。

リスクの大きさ（※1）

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(※2)
ドローン製造事業者	• 従業員が重症を負う可能性は低い。	• 大規模な製品回収につながるおそれがある。
利用者	• 個人情報が流出する可能性がある。 • 利用者が重症を負う可能性がある。	• 重症を負った場合、生活に支障をきたす可能性がある。
ドローンの飛行箇所の周辺にいる第三者	• 個人情報が流出する可能性がある。 • 利用者が重症を負う可能性がある。	• 重症を負った場合、生活に支障をきたす可能性がある。

想定されるリスク(例)のマッピング結果



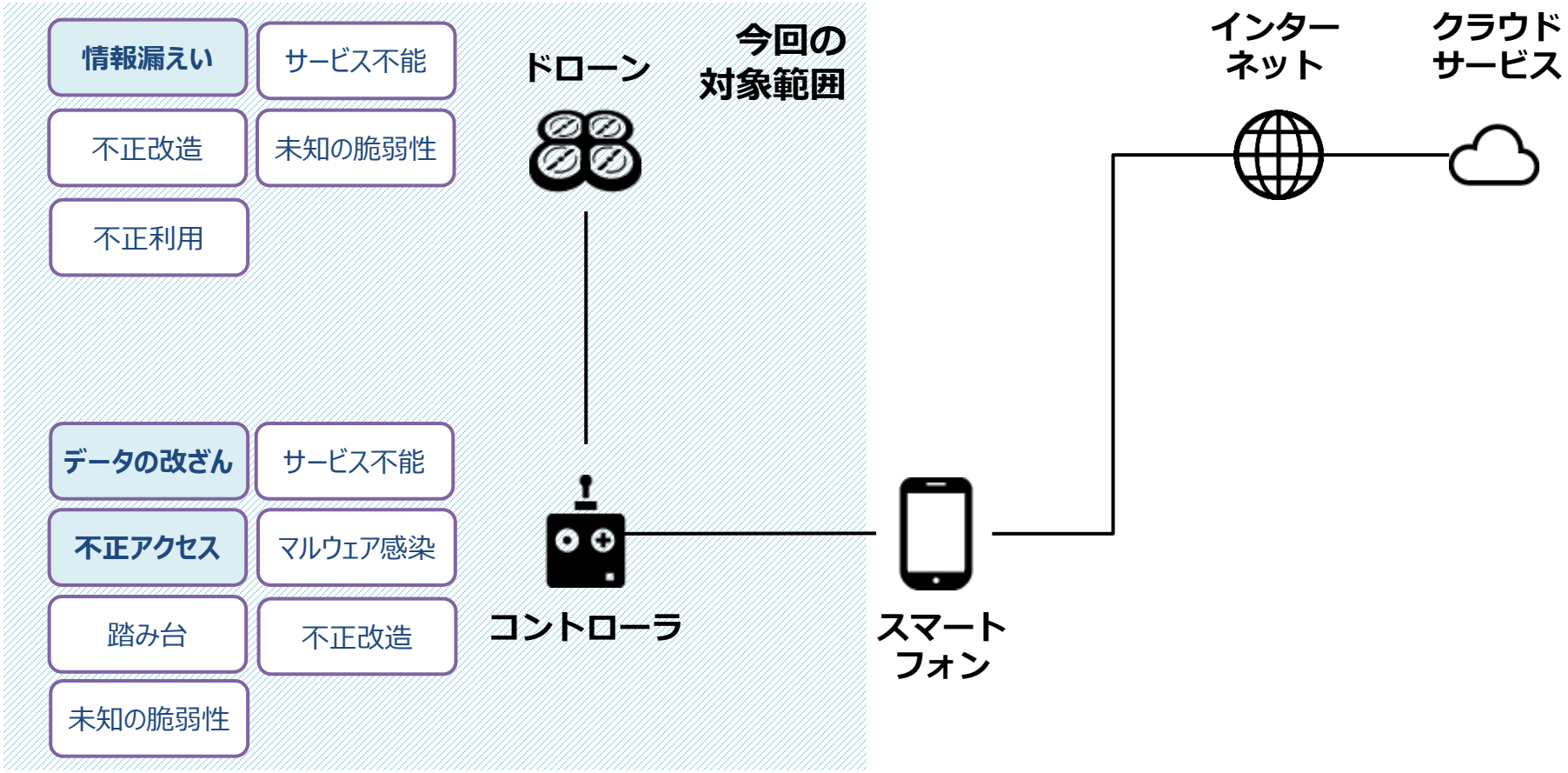
※1：「回復困難性の度合い」及び「経済的影響の度合い」では、主要な被害のみを記載していることに留意。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

3-2.ドローンを活用した個人による写真撮影（ドローン）

③リスク対応->システムを構成する機器ごとの脅威の整理

- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

3-2.ドローンを活用した個人による写真撮影（ドローン）
③リスク対応->脅威に対する対策の整理

- 適用主体であるドローン製造事業者は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討する。

ドローン製造事業者(自身)にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進	• 運用前（設計・製造段階）における法令および契約上の要求事項の遵守 • 企画・設計段階におけるセキュリティ要求事項の分析及び仕様化 • セキュリティ設計と両立するセーフティ設計の仕様化

利用者及びドローンの飛行箇所の周辺にいる第三者にとってのリスクを低減するため対応を要請する対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
利用者への注意喚起の実施や推奨事項の明確化	• プログラムソースコード及び関連書類の保護 • IoT機器・システムに対するアップデートの適用 • IoT機器・システムの運用・管理を行う者への要求事項の特定
フェールセーフ等を含む安全対策の徹底	• セキュリティ設計と両立するセーフティ設計の仕様化

3-2.ドローンを活用した個人による写真撮影（ドローン）
③リスク対応->脅威に対する対策の整理

- 想定される脅威を踏まえ、第3軸「求められるセキュリティ・セーフティ要求」における観点ごとに有効と考えられるドローン製造事業者にて実装が想定される対策要件を整理する。

ドローン製造事業者にて実装が想定される対策要件の例

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の決定
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	運用前（設計・製造段階）における法令および契約上の要求事項の遵守
		マルウェア感染	マルウェア対策の実施
		サービス不能	IoT 機器・システムの十分な可用性の確保
		データの改ざん 不正アクセス	IoT に適したネットワークの利用
		全般	セキュリティ設計と両立するセーフティ設計の仕様化
		全般	セキュアな開発環境と開発手法の適用
		全般	IoT 機器・システムにおけるセキュリティ機能の検証
		全般	IoT 機器・システムの出荷時における安全な初期設定と構成
第 2 の観点	ソシキ・ヒト	全般	利用者へのリスクの周知等の情報発信
		全般	サービス提供や管理のポリシーの提示・遵守
		全般	過去の対応事例からの学習
	プロシージャ	全般	脆弱性対応に必要な手順等の整備と実践
		全般	IoT 機器・システムの適正な使用
		全般	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令および契約上の要求事項の遵守
		全般	プログラムソースコード及び関連書類の保護
		全般	IoT 機器・システムに対するアップデートの適用
		全般	IoT 機器・システムの安全な廃棄または再利用
第 3 の観点	ソシキ・ヒト	全般	IoT 機器・システムの運用・管理を行う者への要求事項の特定
		全般	IoT 機器・システムの運用・管理を行う者への要求事項の遵守の確認

3-2.ドローンを活用した個人による写真撮影（ドローン）
③リスク対応->整理した対策に対する意思決定

- 影響度が大きいリスクに対処するための対策方針を踏まえて実装することとした対策例は、以下の通り。
- ドローン及びコントローラは常に通信を行いながら作動する。したがって、これらのどちらかの機器を優先すればよいということではなく、これらの機器一体で対策を行うことが望ましい。

観点	対策要件	実際に講じる対策の例
第1の観点	**運用前（設計・製造段階）における法令および契約上の要求事項の遵守**	• 情報セキュリティに関連する法的、規制（例：製品安全関連法）に対する違反を避けるための要求事項の遵守
	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化	• ドローン及び周辺機器を現に開発、運用する以前の企画・設計の段階における、想定されるリスクやその程度、具備すべきセキュリティ要求事項の特定
	セキュリティ設計と両立するセーフティ設計の仕様化	• 利用者やドローンの飛行箇所周辺にいる第三者への危害を回避するための安全機能（本質安全設計、予防安全機能等）の実装

3-2.ドローンを活用した個人による写真撮影（ドローン）
③リスク対応->整理した対策に対する意思決定

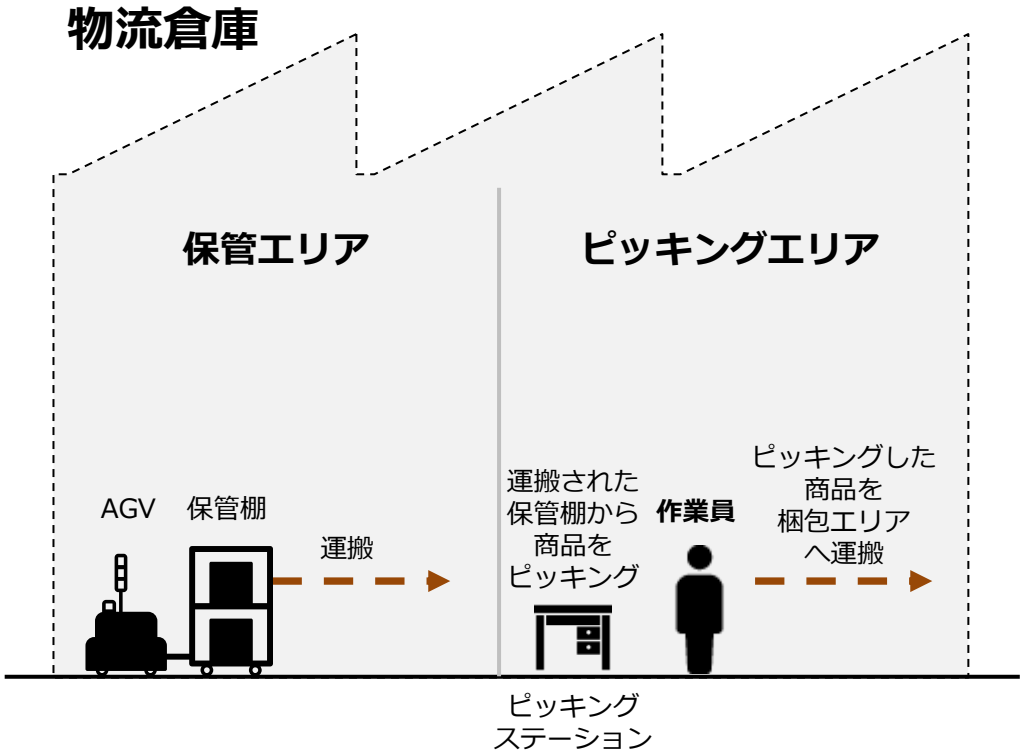
観点	対策要件	実際に講じる対策の例
第2の観点	**利用者へのリスクの周知等の情報発信**	• 企業ホームページ等を通じたサポート期間終了の予告及び通知、機器・システムの重大な脆弱性、ユーザ情報の漏えいや機器のマルウェア感染等のインシデントに関する情報発信等、ドローンに対するリスクや利用者で対応すべき点に関する情報提供の実施
	IoT機器・システムの適正な使用	• 利用者に対する、以下の内容を含むドローンの取り扱い説明書（利用手順や操作方法）の作成及び提示 ✓ 初期設定の手順 ✓ 提供者が想定する安全な利用方法 ✓ 不適切な使用によって生じ得るセキュリティ関連のリスク ✓ 不具合を発見した際の連絡先 ✓ ドローンの安全な廃棄方法
第3の観点	**IoT機器・システムの運用・管理を行う者への要求事項の特定**	• 以下の内容を含む、取り扱い説明書での利用者に能動的な行動を促すための推奨事項の明確化 ✓ 使用条件 ✓ 使用上のリスク・注意点 ✓ 異常通知があった場合に取るべき対応（手元操作の優先、近くにいる使用者による通信回線切り離し） ✓ ソフトウェアアップデート時の注意事項

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）

①リスクアセスメント、リスク対応に向けた事前準備->対象ソリューションの概要

- 本ユースケースのIoT-SSFの適用主体は、物流事業者とする。
- 当該事業者は、事業規模拡大に伴って既存の物流倉庫において、省人化や効率化を目的としてAGVや倉庫制御システム等の導入を予定しており、新たなシステムや機器の導入によって生じ得るサイバーセキュリティに関するリスクを懸念している。

- 工業用間接資材を扱う物流倉庫において、無人搬送車（AGV：Automatic Guided Vehicle）が自動ピッキングを行う。
- 具体的には、物流倉庫（入荷エリア、保管エリア、ピッキングエリア、梱包エリア、出荷エリア）内の保管エリアにて倉庫制御システムによって制御されたAGVが保管棚をピッキングエリアにいる作業員のもと（ピッキングステーション）まで移動させる。
- なお、保管棚からのピッキングする作業は作業員にて行うことを想定。

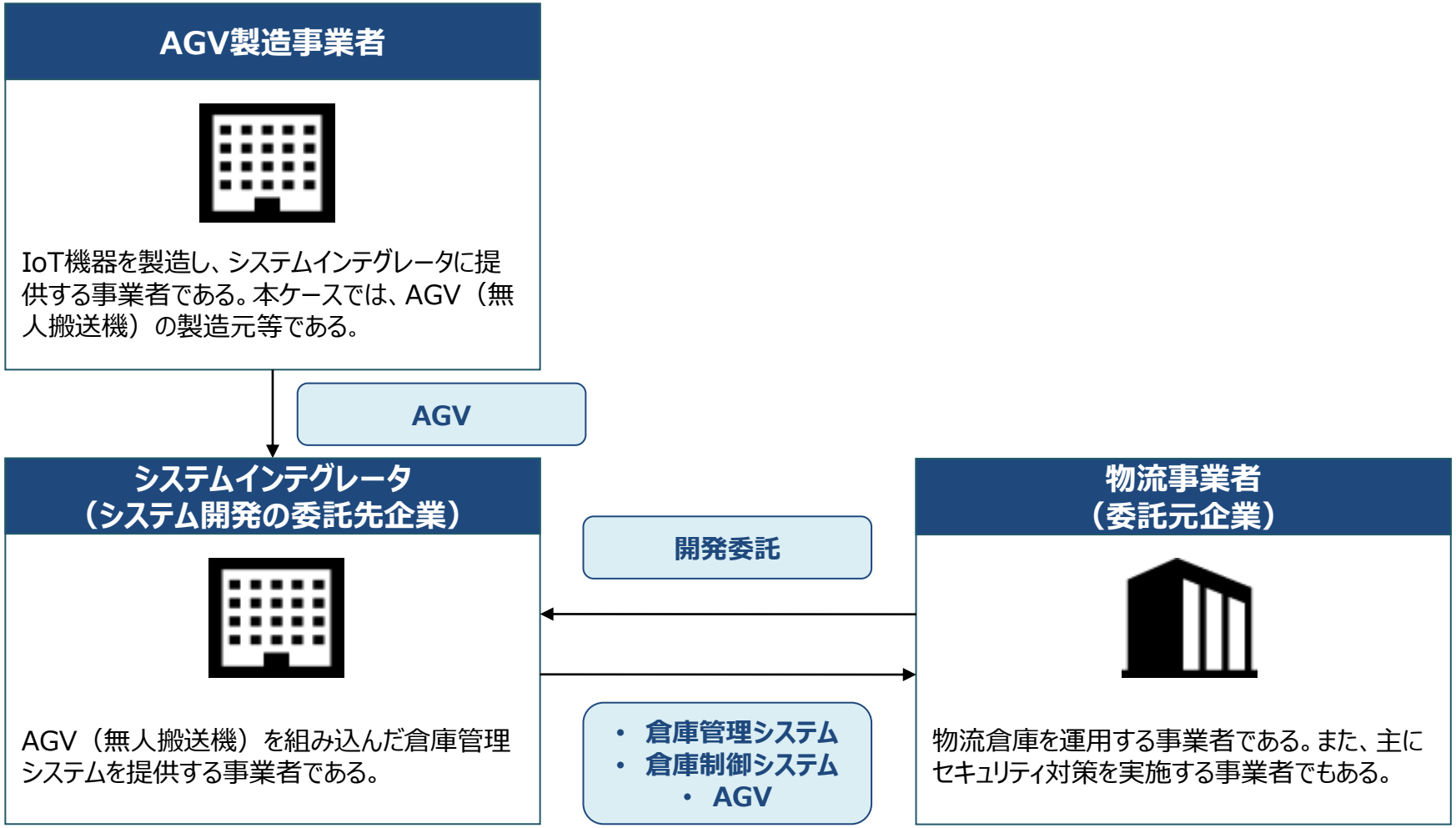


[参考] 国土交通省「物流分野における情報セキュリティ確保に係る安全ガイドライン」等

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）

①リスクアセスメント、リスク対応に向けた事前準備->ステークホルダー関係図

- ステークホルダーは、「物流事業者」「システムインテグレータ」「AGV製造事業者」の３者。

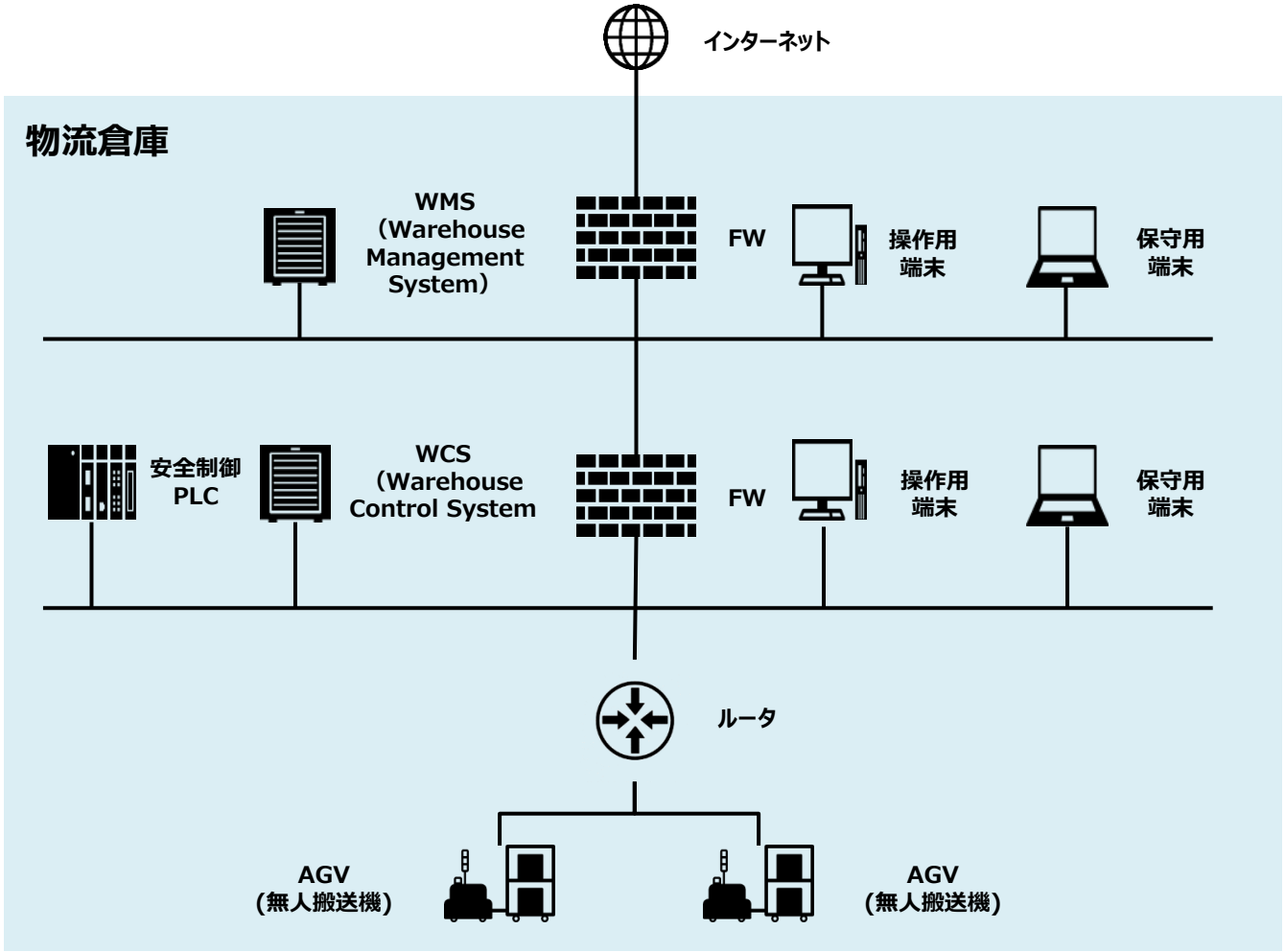


[参考] 国土交通省「物流分野における情報セキュリティ確保に係る安全ガイドライン」等

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）

①リスクアセスメント、リスク対応に向けた事前準備->システム構成図

- システムを構成する機器は以下を想定。



システムを構成する機器の一覧
倉庫管理システム
操作用端末
保守用端末
倉庫制御システム
安全制御PLC
AGV

[参考] 国土交通省「物流分野における情報セキュリティ確保に係る安全ガイドライン」等

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
②リスクアセスメント->想定されるセキュリティインシデント等とその結果の特定

- ステークホルダーごとにリスクアセスメントを行うにあたり、対象機器・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及び想定される被害（例）を整理。

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)
物流事業者にとってのリスク	悪意のある攻撃者により外部から倉庫管理システムが不正にアクセスされ、保存されている在庫情報が改ざんされる。	配送の停止や誤配送が生じ得る。（※） **配送の停止や誤配送**が生じることによって、担当地域で事業を行う搬送会社や工業資材の利用者等、物流事業者からサービスの提供を受ける**倉庫外部の事業者等へ影響が及ぶ**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	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、倉庫制御システムやAGV等が**マルウェアに感染**する。	AGVが想定していない動作をすることで、物流工場が停止することにより、**大規模な製品回収が生じ得る**。
AGV製造事業者にとってのリスク	AGVに重大な脆弱性が発見される。	**大規模な製品回収等が生じ得る。**

※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（配送遅延や誤配送への対応等）の事後的な対応が発生し得る。

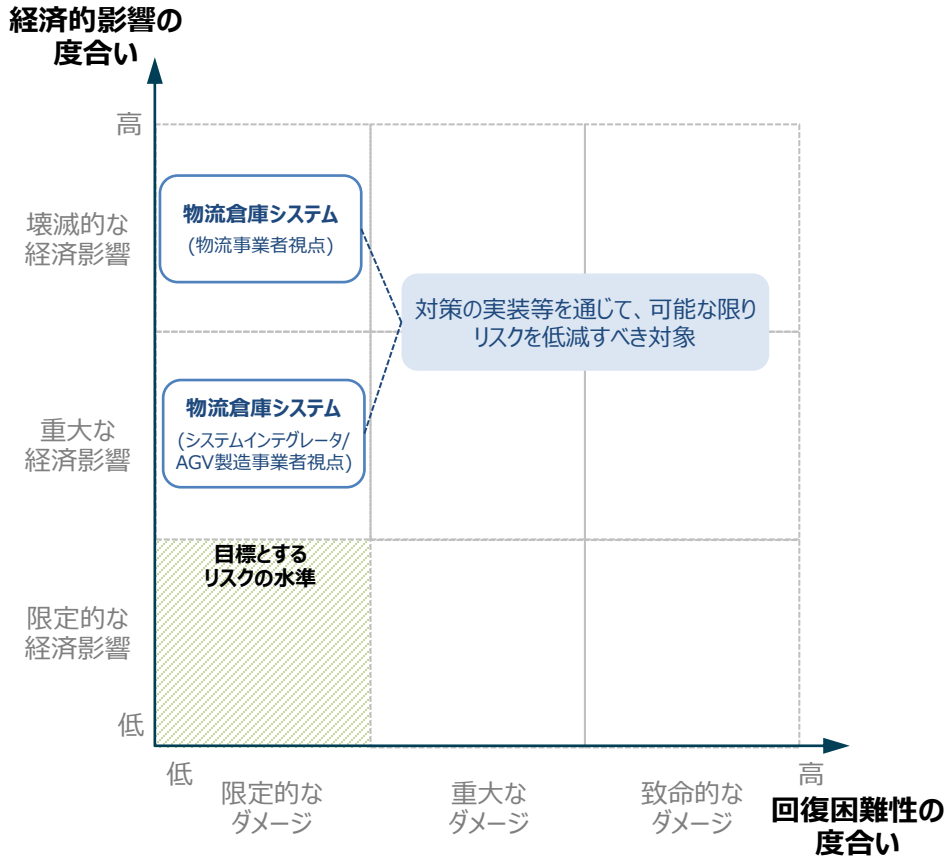
3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
②リスクアセスメント->マッピング結果の整理と評価の実施

- セキュリティインシデントによって「物流事業者」が保有する倉庫内の業務が停止することで、倉庫内のみならず取引先、サプライチェーン規模で影響が波及し、結果として生じる経済的影響が大きくなる可能性がある。

リスクの大きさ（※1）

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(※2)
物流事業者	• 従業員が重症を負う可能性は低い。	• 物流事業者からサービスの提供を受ける倉庫外部の事業者等へ影響が及ぶ可能性がある。 • 配送の停止や誤配送が生じる可能性がある。
システムインテグレータ	• 従業員が重症を負う可能性は低い。	• 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。
AGV製造事業者	• 従業員が重症を負う可能性は低い。	• 大規模な製品回収につながるおそれがある。

想定されるリスク(例)のマッピング結果



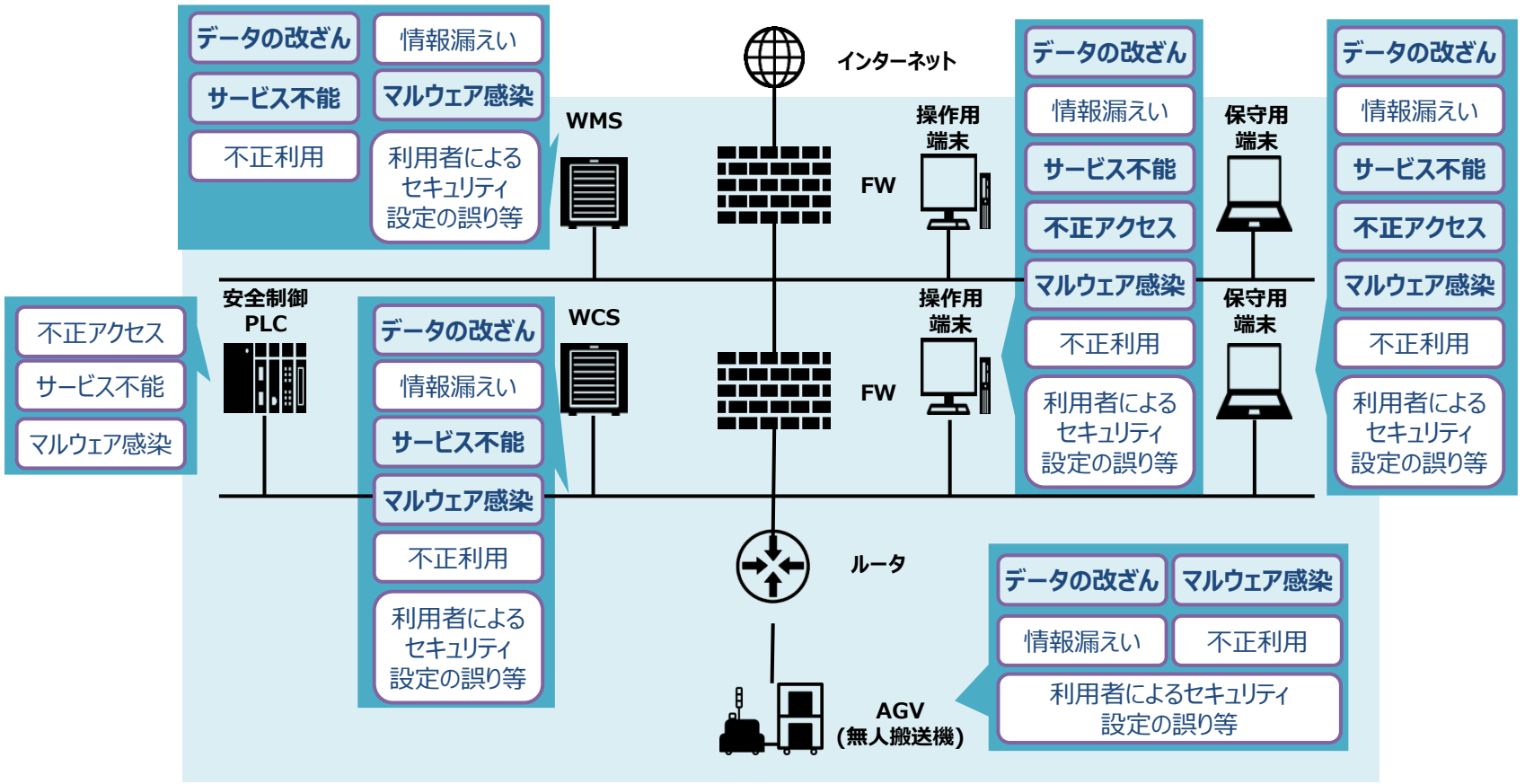
※1：「回復困難性の度合い」及び「経済的影響の度合い」では、主要な被害のみを記載していることに留意。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）

③リスク対応->システムを構成する機器ごとの脅威の整理

- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
③リスク対応->脅威に対する対策の整理

- 適用主体である物流事業者は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討する。

物流事業者(自身)にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
セキュリティインシデントが発生したとしても、それらの被害を最小限にするための仕組みの構築	• **様々なIoT機器を接続する際のセキュリティの確保** • **適切なネットワークの分離**
信頼性の高い物流倉庫の操業を可能にするための仕組みの構築	• **IoT機器・システムの十分な可能性の確保** • **IoT機器・システムのモニタリング及びログの取得、分析**

システムインテグレータにとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進	• **運用前（設計・製造段階）における法令および契約上の要求事項の遵守** • **セキュリティ設計と両立するセーフティ設計の仕様化**
安全なアップデートプログラムの配信のための仕組みの構築	• **IoT機器・システムに対するアップデートの適用**

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）

③リスク対応->脅威に対する対策の整理

- 被害の大きさだけでなく、その起こりやすさも踏まえ、システム全体としてのリスクを低減することを目的として対策の適用対象を検討する。

物流事業者にて実装が想定される対策要件の例想定される脅威（例）

第 3 軸	実装先	想定される脅威 （例）	対策要件
第 1 の観点	ソシキ・ヒト	全般	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の決定
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	運用前（設計・製造段階）における法令および契約上の要求事項の遵守
			置、設定
第 2 の観点	ソシキ・ヒト	全般	運用中における IoT セキュリティを目的とした体制の確保
		全般	過去の対応事例からの学習
		全般	サービス提供や管理のポリシーの提示・遵守
	プロシージャ	全般	脆弱性対応に必要な体制や手順等の整備と実践
		全般	インシデント対応手順の整備と実践
		全般	事業継続計画の策定と実践
		全般	IoT 機器・システムの用途・用法を守った使用
		不正利用 不正アクセス	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令および契約上の要求事項の遵守
		不正アクセス マルウェア感染	継続的な資産管理
		全般	プログラムソースコード及び関連書類の保護
		不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
		不正利用	IoT 機器・システムに対するアップデートの適用
		情報漏えい	IoT 機器・システムの安全な廃棄または再利用
		全般	IoT 機器・システムに対するアップデートの適用（セキュリティパッチの開発・配布等）

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）

③リスク対応->整理した対策に対する意思決定

- 近年、システム構成やその利用環境の変化、及び制御システムを狙った脅威の高度化等を背景に、セキュリティ対応の必要性が非常に高まってきていることから、制御システムに特有とされる性質等にも注意を払いながら、対策に関する意思決定を行う。

物流事業者において実際に講じる対策の例

観点	対策要件	実際に講じる対策の例
第1の観点	**運用前（設計・製造段階）における法令および契約上の要求事項の遵守**	• 情報セキュリティに関連する法的な規制又は契約上の義務に対する違反を避けるための要求事項の特定及び遵守。
第1の観点	**企画・設計段階におけるセキュリティ要求事項の分析及び仕様化**	• 本社の情報システム部門の担当者が中心となり、倉庫における業務担当者を巻き込み、倉庫制御システムの企画・設計時におけるリスクアセスメントの実施、セキュリティ要件の特定、要件の実装に係る費用の確保。 • 必要なセキュリティ仕様が組み込まれているかを確認する設計レビューの実施。 • 特定したセキュリティ要求事項を倉庫制御システムの委託仕様書への記載。
第2の観点	**IoT機器・システムのモニタリング及びログの取得、分析**	• 本社の情報システム部門の担当者による物流倉庫システムを構成する倉庫管理システムや倉庫制御システムを対象にした各種ログ（例：ユーザ認証、ネットワークトラフィック）の取得及び保護。 • 取得したログの定期的な分析及び異常の検知。

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）

③リスク対応->整理した対策に対する意思決定

- システムインテグレータに対応を依頼することとした対策例は以下の通り。

システムインテグレータにおいて実際に講じる対策の例（1/2）

観点	対策要件	実際に講じる対策の例
第1の観点	**様々なIoT機器に接続する際のセキュリティの確保**	• AGV制御PLC等を他のAGV機器等に接続する際のホワイトリストの適用。
	IoT機器・システムの十分な可用性の確保	• 倉庫外部からの通信を受信し得る倉庫管理システム等に対する(D)DoS 攻撃を想定し、一定レベルの負荷に耐える容量を確保。 • 倉庫管理システム、操作用端末、保守用端末、倉庫制御システム等において不審な通信（例：特定のIPアドレスからの大量のリクエスト）の検知及び遮断。 • アプリケーションのテスト段階における一定レベルの負荷試験の実施
	IoT機器・システムの十分な可用性の確保	• 倉庫外部からの通信を受信し得る倉庫管理システム等に対する(D)DoS 攻撃を想定し、一定レベルの負荷に耐える容量を確保。 • 倉庫管理システム、操作用端末、保守用端末、倉庫制御システム等において不審な通信（例：特定のIPアドレスからの大量のリクエスト）の検知及び遮断。 • アプリケーションのテスト段階における一定レベルの負荷試験の実施。

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
③リスク対応->整理した対策に対する意思決定

- システムインテグレータに対応を依頼することとした対策例は以下の通り。

システムインテグレータにおいて実際に講じる対策の例（2/2）

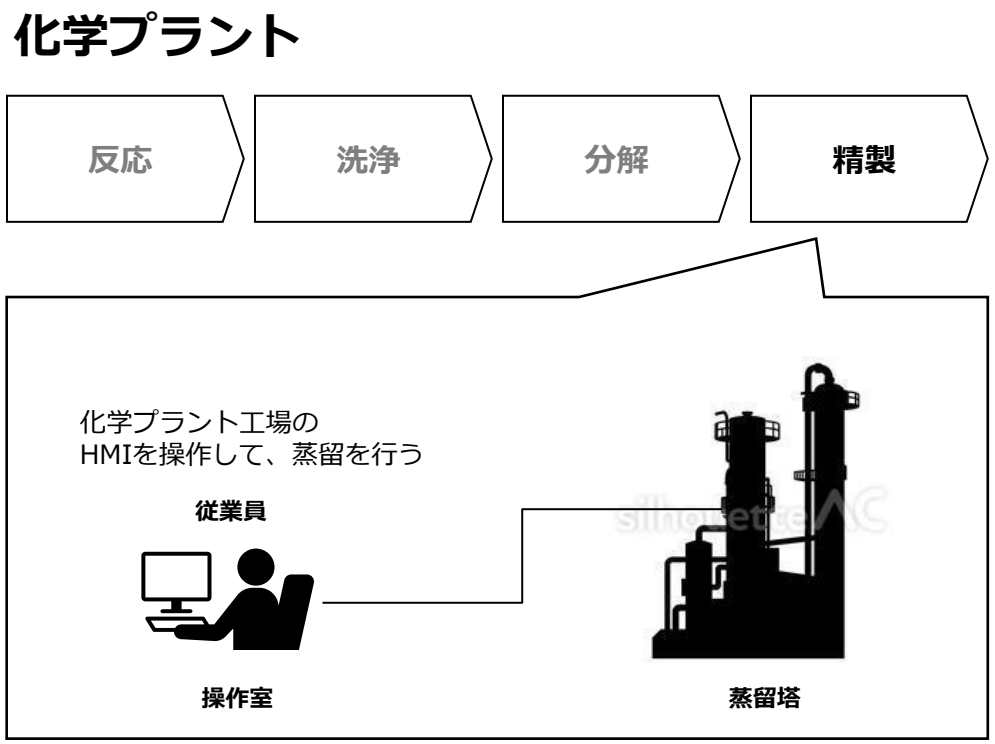
観点	対策要件	実際に講じる対策の例
第1の観点	**適切なネットワークの分離**	• リスクレベルに応じた情報ネットワーク、情報制御ネットワーク、制御ネットワーク等の複数のゾーンへのネットワークの分割。 • FW等でのAGVやAGV制御PLCが含まれているゾーンで送受信される全ての不要な通信の遮断。
	セキュリティ設計と両立するセーフティ設計の仕様化の指示	• 作業員や機器の周辺への危害を回避するための安全機能（本質安全設計、予防安全機能等）の実装。 • AGVに実装された安全機能と外部との通信回線との分離。
第2の観点	**IoT機器・システムに対するアップデートの適用（セキュリティパッチの開発・配布等）**	• 報告された脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定。 • IoT機器製造事業者や開発委託先等への修正プログラム等開発の依頼。 • 物流事業者へのセキュリティパッチの提供。

3-4.化学プラント施設内の蒸留工程の自動制御

①リスクアセスメント、リスク対応に向けた事前準備->対象ソリューションの概要

- 本ユースケースの適用主体は、プラント事業者とする。
- 当該事業者は、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が、本社の経営層を中心に新たに生じ得るサイバーセキュリティに関するリスクを懸念している。

- 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。

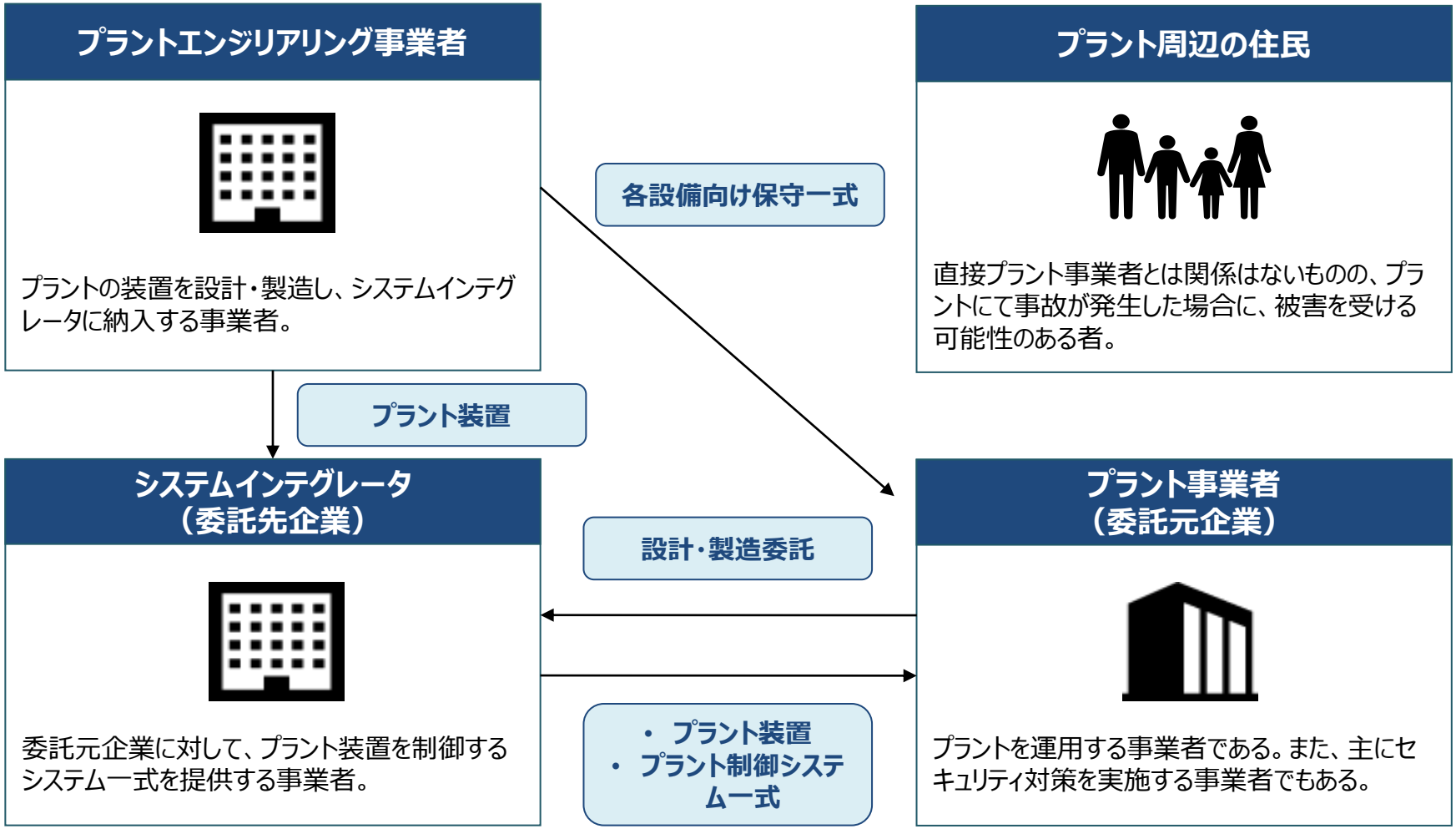


[参考] 経済産業省、国立研究開発法人新エネルギー・産業技術総合開発機構「IoTセキュリティ対応マニュアル産業保安版（第２版）」等

3-4.化学プラント施設内の蒸留工程の自動制御

①リスクアセスメント、リスク対応に向けた事前準備->ステークホルダー関係図

- ステークホルダーは、「プラント事業者」、「システムインテグレータ」、「プラントエンジニアリング事業者」及び「プラント周辺の住民」の４者。

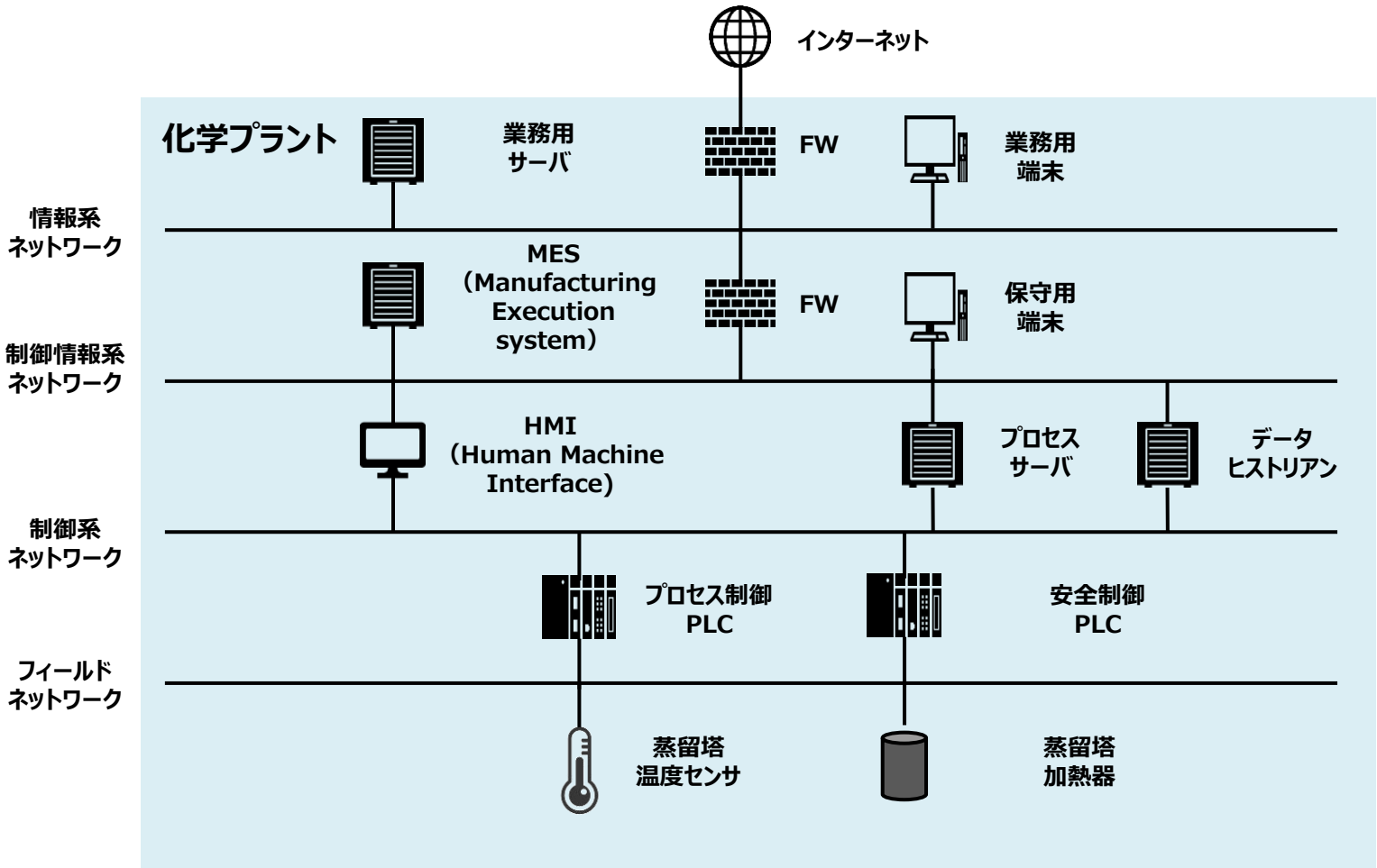


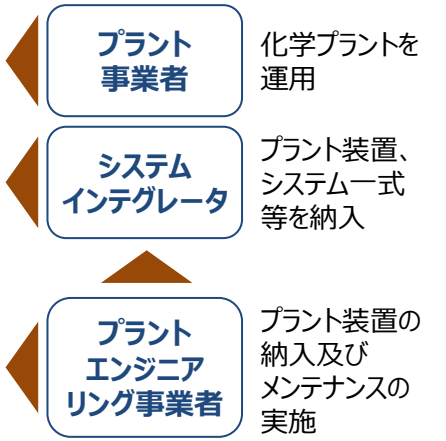
[参考] 経済産業省、国立研究開発法人新エネルギー・産業技術総合開発機構「IoTセキュリティ対応マニュアル産業保安版（第２版）」等

3-4.化学プラント施設内の蒸留工程の自動制御

①リスクアセスメント、リスク対応に向けた事前準備->システム構成図

- システムを構成する機器は以下を想定。





システムを構成する機器の一覧
MES(製造実行システム)
HMI(ヒューマンマシンインターフェース)
プロセスサーバ
データヒストリアン
業務用サーバ/業務用端末
安全制御PLC
プロセス制御PLC
蒸留塔温度センサ
蒸留塔加熱器

[参考] 経済産業省、国立研究開発法人新エネルギー・産業技術総合開発機構「IoTセキュリティ対応マニュアル産業保安版（第２版）」等

3-4.化学プラント施設内の蒸留工程の自動制御
②リスクアセスメント->想定されるセキュリティインシデント等とその結果の特定

- ステークホルダーごとにリスクアセスメントを行うにあたり、対象機器・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及び想定される被害（例）を整理。

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。**（※）
	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	（システムインテグレータのリスクは限定的であると想定されるため、ここでは詳細を記載しない。）	
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ことで、**契約上の責任を問われ得る。**

※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。

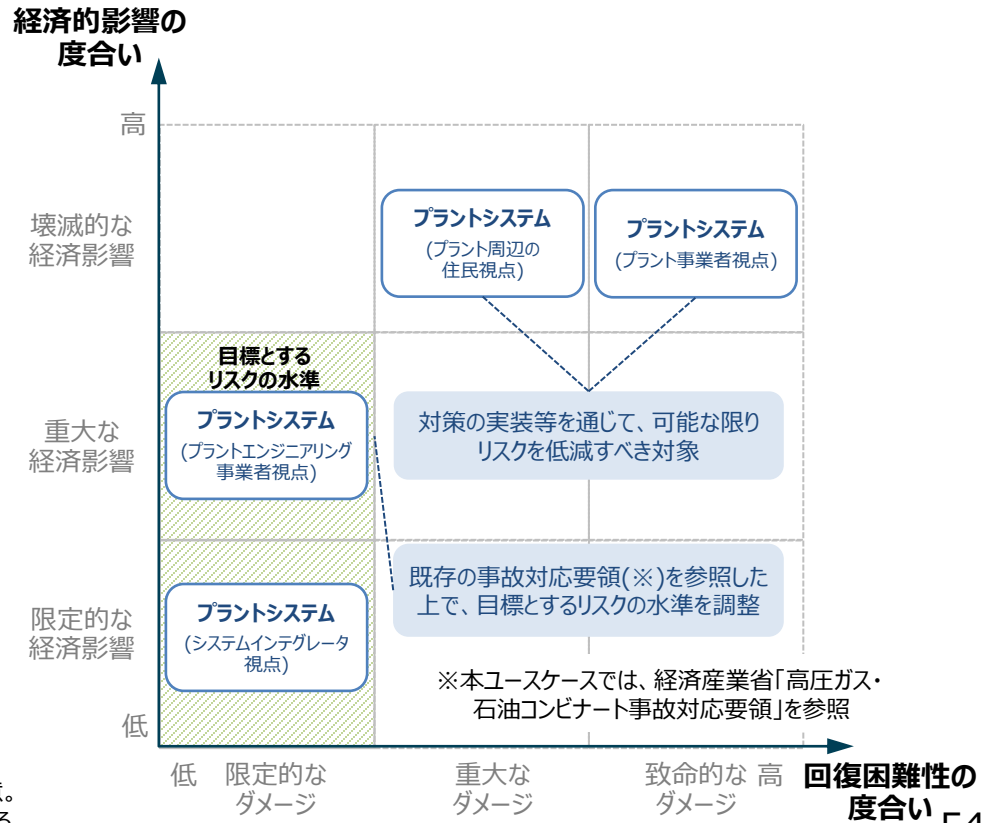
3-4.化学プラント施設内の蒸留工程の自動制御
②リスクアセスメント->マッピング結果の整理と評価の実施

- セキュリティインシデントが設備損傷や爆発等の安全上の事象に発展する場合、「プラント事業者」にとってのリスクは「回復困難性の度合い」及び「経済的影響の度合い」の双方が非常に大きくなる。また、それらの事故により自身だけではなく、「プラント周辺の住民」へも影響が及ぶ可能性がある。
- 監督官庁から公表されている事故対応要領等を参照した上で、目標とするリスクの水準を調整。

リスクの大きさ（※1）

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(※2)
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。	• プラント制御システムが既に稼働しており、大規模な製品回収は起こる可能性は低い。
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。

想定されるリスク(例)のマッピング結果



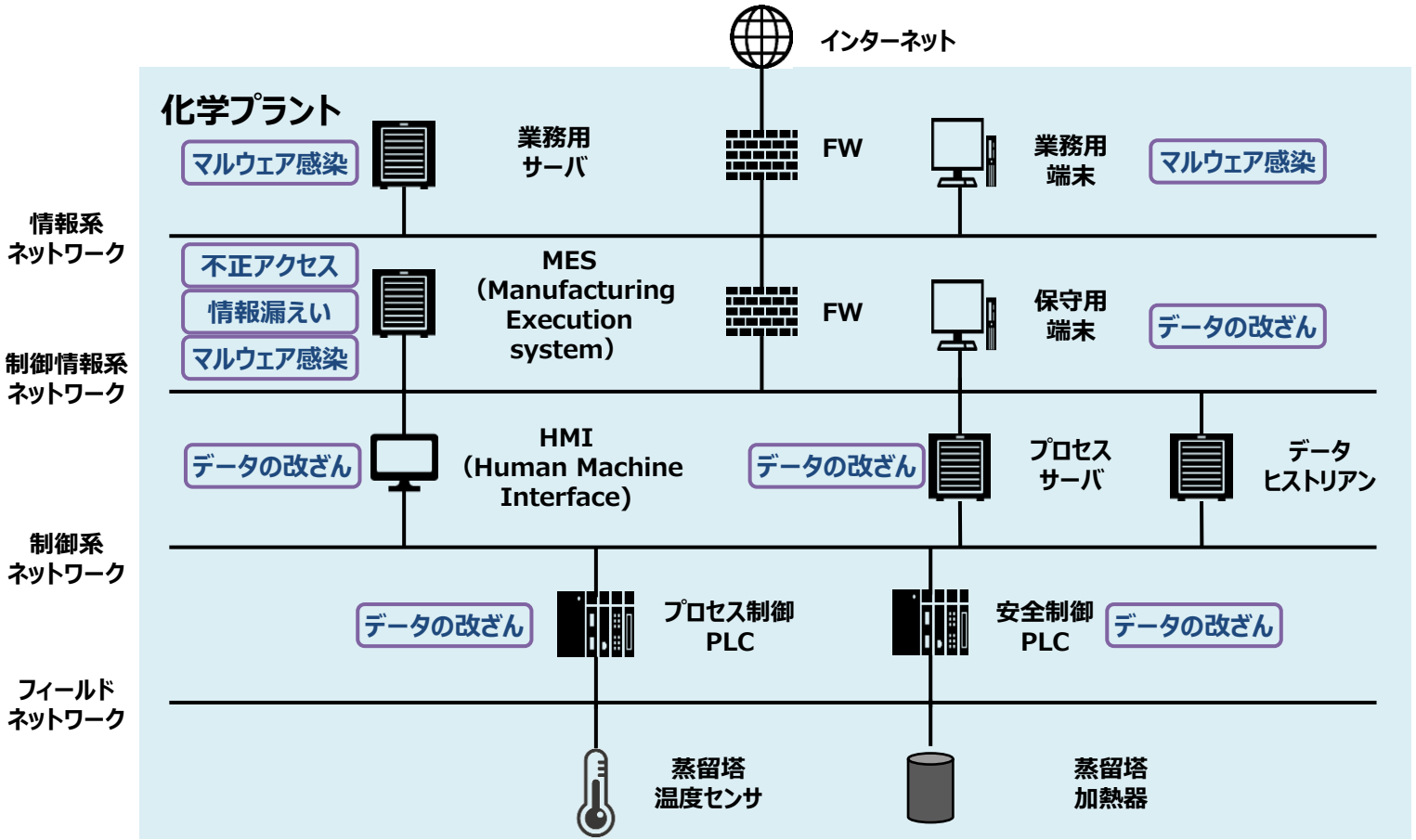
※1：「回復困難性の度合い」及び「経済的影響の度合い」では、主要な被害のみを記載していることに留意。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

3-4.化学プラント施設内の蒸留工程の自動制御

③リスク対応->システムを構成する機器ごとの脅威の整理

- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

3-4.化学プラント施設内の蒸留工程の自動制御
③リスク対応->脅威に対する対策の整理

- 適用主体であるプラント事業者は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討する。

プラント事業者（自身）にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
等の発生時に正しく作動することを確かなものとする対策	• セキュリティ設計と両立するセーフティ設計の仕様化
情報システム部門及び製造部門が一体となって対応を行うための体制の構築	• 運用前（設計・製造段階）におけるIoTセキュリティを目的とした体制の確保 • 運用中におけるIoTセキュリティを目的とした体制の確保
セキュリティインシデントが発生したとしても、それらの被害を最小限にするための仕組みの構築	• 様々なIoT機器を接続する際のセキュリティの確保 • 適切なネットワークの分離 • インシデント対応手順の整備と実践
信頼性の高いプラントの操業を可能にするための仕組みの構築	• IoT機器・システムの十分な可用性の確保 • IoT機器・システムのモニタリング及びログの取得、分析 • IoT機器・システムに対するアップデートの適用

プラント周辺の住民にとってのリスクを低減するため対応を要請する対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
セキュリティに関するインシデントが発生したととしても周辺環境への影響を最小限に抑える仕組みの構築	• セキュリティ設計と両立するセーフティ設計の仕様化 • 運用中における法令および契約上の要求事項の遵守

3-4.化学プラント施設内の蒸留工程の自動制御

③リスク対応->脅威に対する対策の整理

- 想定される脅威を踏まえ、第3軸「求められるセキュリティ・セーフティ要求」における観点ごとにプラント事業者にて実装が想定される対策要件を整理する。

プラント事業者にて実装が想定される対策要件の例

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の明確化
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	データの改ざん	ソフトウェアの完全性の検証
		情報漏えい	搭載するソフトウェアに対するインストール対策の実装
		マルウェア感染	マルウェア対策の実施
		全般	IoT 機器・システムの出荷時における安全な初期設定と構成
第 2 の観点	ソシキ・ヒト	全般	サービス提供や管理のポリシーの提示・遵守
		全般	運用中における IoT セキュリティを目的とした体制の確保
		全般	過去の対応事例からの学習
	プロシージャ	全般	脆弱性対応に必要な手順等の整備と実践
		不正利用 不正アクセス	IoT 機器・システムの適正な運用・保守
		全般	IoT 機器・システムの適正な使用
	システム	全般	運用中における法令および契約上の要求事項の遵守
		不正アクセス マルウェア感染	継続的な資産管理
		全般	プログラムソースコード及び関連書類の保護
		不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
		不正利用	IoT 機器・システムに対するアップデートの適用
		不正アクセス	IoT 機器・システムの安全な廃棄または再利用

3-4.化学プラント施設内の蒸留工程の自動制御

③リスク対応->整理した対策に対する意思決定

- 影響度が大きいリスクに対処するための対策方針を踏まえて実装することとした対策例は、以下の通り。

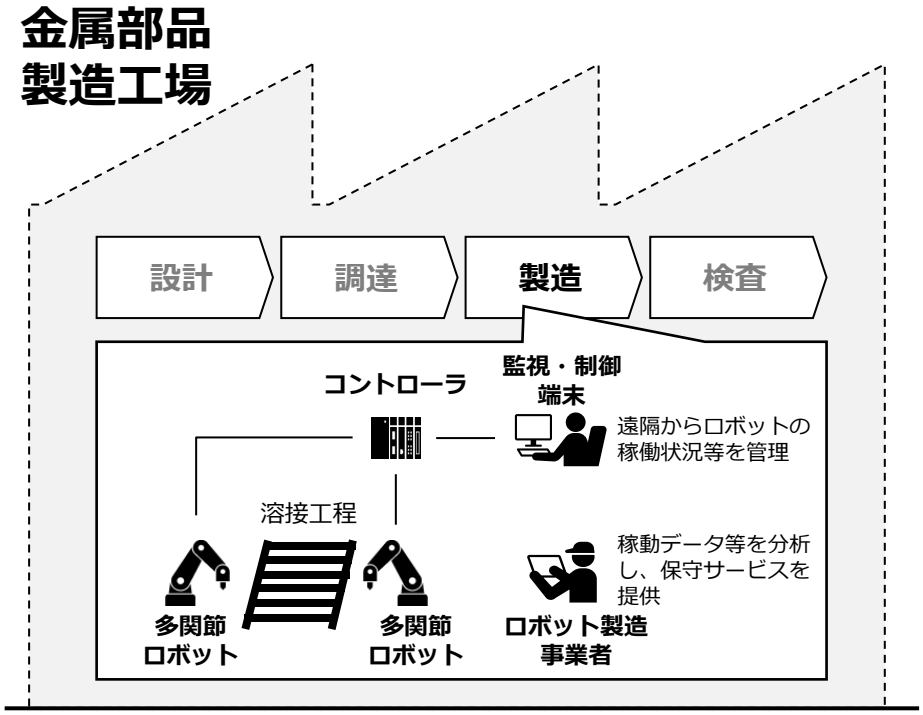
観点	対策要件	実際に講じる対策の例
第1の観点	**運用前（設計・製造段階）における法令および契約上の要求事項の遵守**	• 製造部門及び情報部門が一体となって対応できるようリスク対応組織を立上げ、組織内で統合的にセキュリティ対策を取る体制の構築。 • プラントにおけるセキュリティ管理責任者の任命。 • ※上記の管理責任者及び開発担当者の役割と責任は、プラントシステムのライフサイクルの各段階（例：開発、運用、保守）において明確化されていることが望ましい。
第2の観点	**運用中における法令および契約上の要求事項の遵守**	• 情報セキュリティに関連する法的な規制又は契約上の義務に対する違反を避けるための要求事項の特定及び遵守
	IoT機器・システムのモニタリング及びログの取得、分析	• プラントシステムを構成するMESやプロセス制御PLCを対象にした各種ログ（例：ユーザ認証、ネットワークトラフィック）の取得及び保護 • 取得したログの安全な入手 • 取得したログの定期的な分析及び異常の検知
	IoT機器・システムに対するアップデートの適用	• 脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定 • 開発委託先等への修正プログラム等開発の依頼 • 製造部門と調整を行った上で、提供を受けたセキュリティパッチの適用

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化

①リスクアセスメント、リスク対応に向けた事前準備->対象ソリューションの概要

- 本ユースケースの適用主体は、金属部品製造事業者とする。
- 当該事業者は、生産能力の維持向上等を目的として、溶接工程の自動化を進めるためにロボットシステムの導入を予定しているが、新たに生じ得るサイバーセキュリティに関するリスクを懸念している。

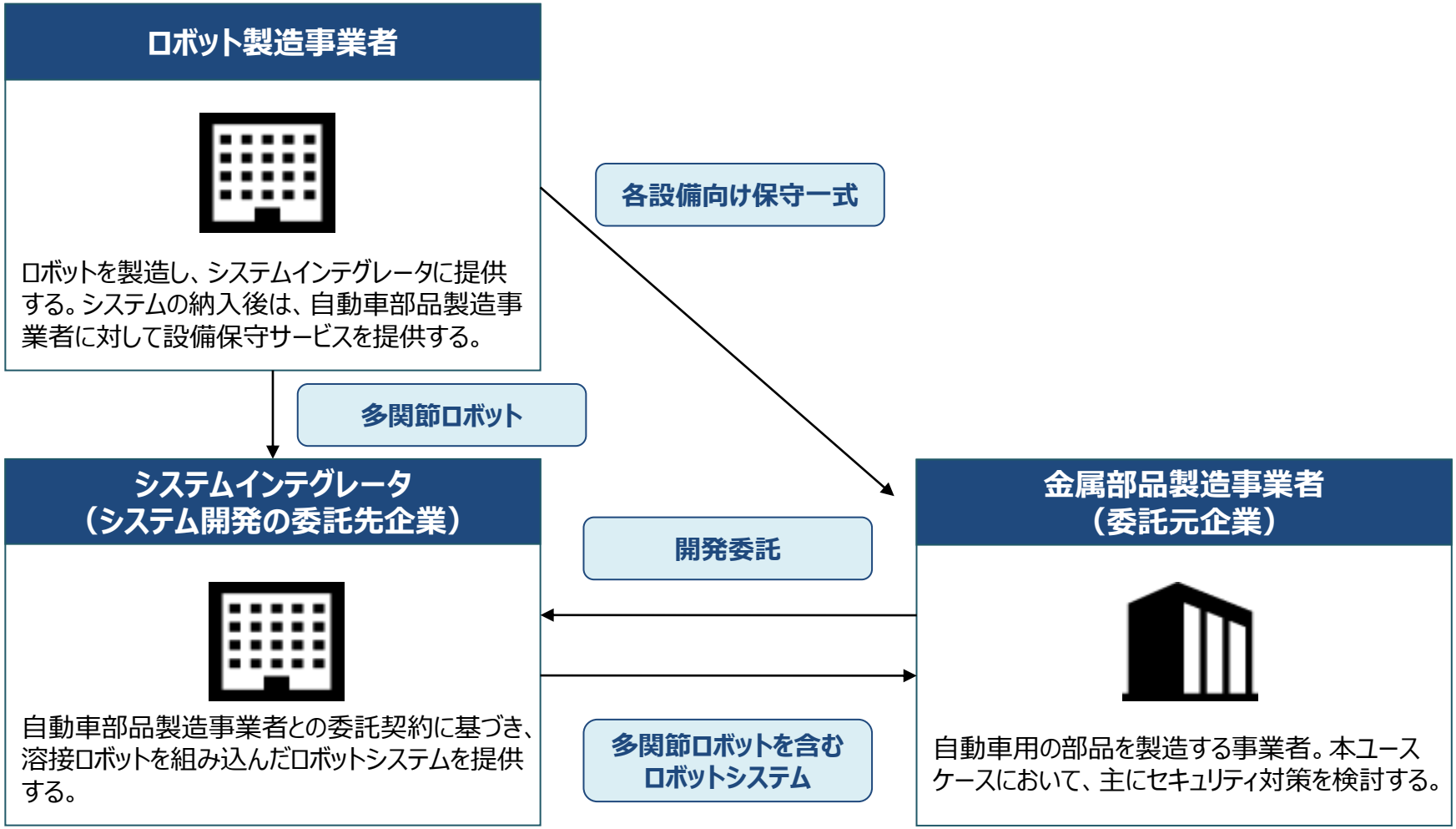
- 金属部品製造事業者の工場において、多関節ロボットを含むロボットシステムを導入し、従来の人手による溶接工程を自動化する。
- 加工対象となるのは、自動車用ボディフレーム等の比較的サイズの大きな部品であり、溶接時に歪を発生させないため左右同時溶接が要求される。
- ロボットが稼働するエリアには安全柵やレーザースキャナが設けられており、基本的に作業員は立ち入れない。
- ロボット製造事業者は、ロボットの稼動データを取得、分析し、効率的な保守サービスの提供に活用する。



[参考] 経済産業省、一般社団法人日本ロボット工業会「ロボット導入実証事業事例紹介ハンドブック2018」等

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
①リスクアセスメント、リスク対応に向けた事前準備->ステークホルダー関係図

- ステークホルダーは、「金属部品製造事業者」、「システムインテグレータ」及び「ロボット製造事業者」の３者。

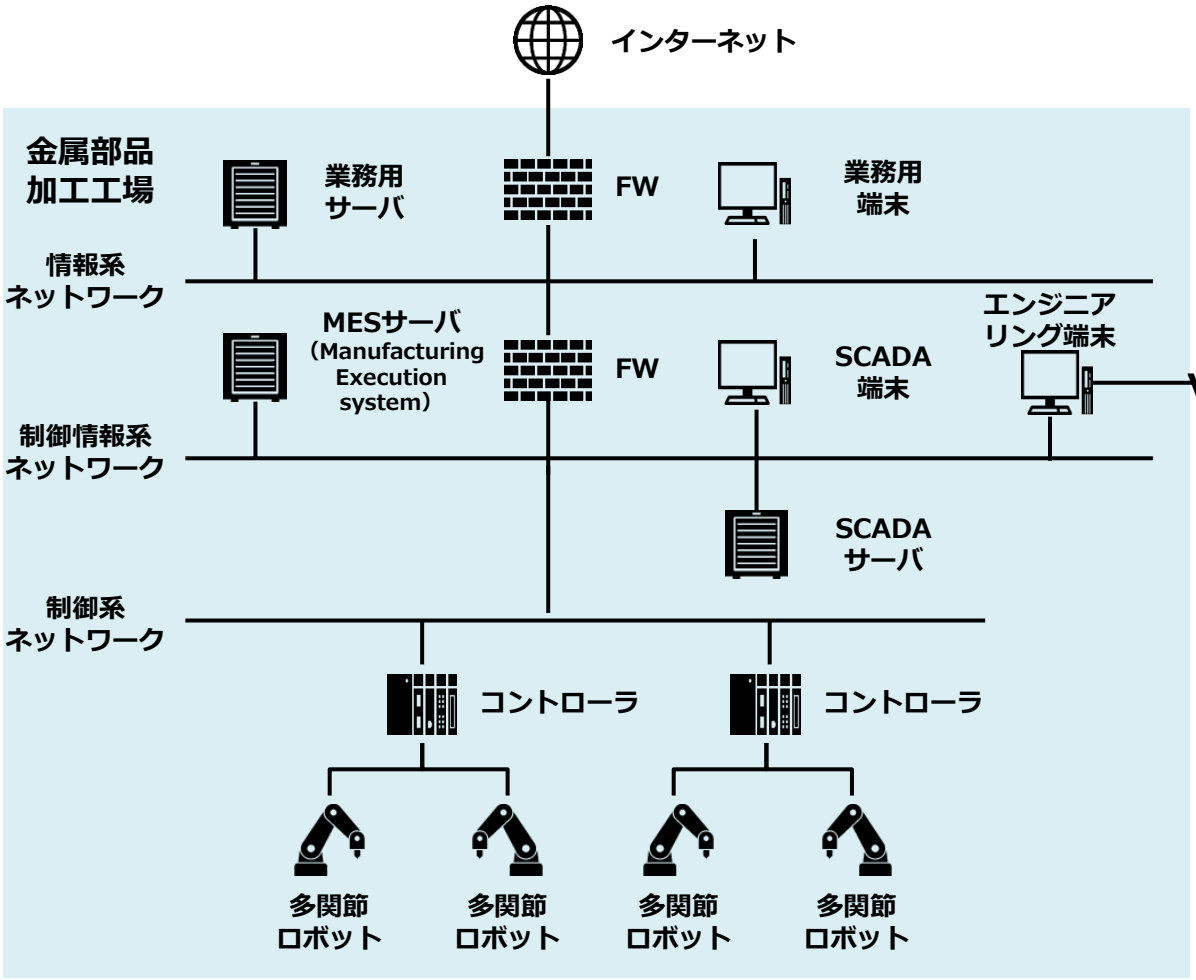


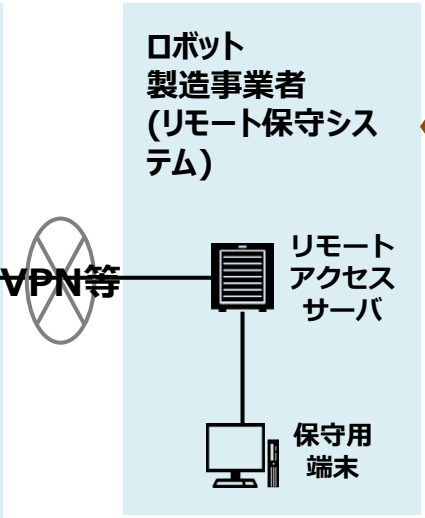
[参考] 経済産業省、一般社団法人日本ロボット工業会「ロボット導入実証事業事例紹介ハンドブック2018」等

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化

①リスクアセスメント、リスク対応に向けた事前準備->システム構成図

- システムを構成する機器は以下を想定。





ロボット製造事業者

ロボットの納入及び保守メンテナンスの実施

システムインテグレータ

ロボットシステムの提供

金属部品製造事業者

自動車用の部品を製造

システムを構成する機器の一覧
業務用サーバ/端末
ファイアウォール（FW）
MESサーバ
SCADAサーバ/端末
エンジニアリング端末
リモートアクセスサーバ/保守用端末（リモート保守システム）
コントローラ
多関節ロボット

[参考] 経済産業省　国立研究開発法人新エネルギー・産業技術総合開発機構「IoTセキュリティ対応マニュアル産業保安版（第２版）」等

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
②リスクアセスメント->想定されるセキュリティインシデント等とその結果の特定

- ステークホルダーごとにリスクアセスメントを行うにあたり、対象機器・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及び想定される被害（例）を整理。

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)
金属部品製造事業者にとってのリスク	外部に接続している情報系ネットワークを経由して、制御情報系ネットワークに設置された**MESサーバやSCADAサーバがマルウェアに感染する。**	**生産活動が一時的に停止**する。
	リモート保守サービスを受けるために外部ネットワークに接続している**エンジニアリング端末が不正アクセスされ、コントローラの制御プログラムを改ざんされる。**	仕様を満たさない**不良品が生産される。**
システムインテグレータにとってのリスク	（システムインテグレータのリスクは限定的であると想定されるため、ここでは詳細を記載しない。）	
ロボット製造事業者にとってのリスク	保守業務委託先のロボット製造事業者の従業員が、誤って不正なUSB等の外部記憶媒体をエンジニアリング端末に挿入することで、**同端末及び制御情報系ネットワーク内の他のサーバや端末がマルウェアに感染する。**	**製品回収が発生する。**

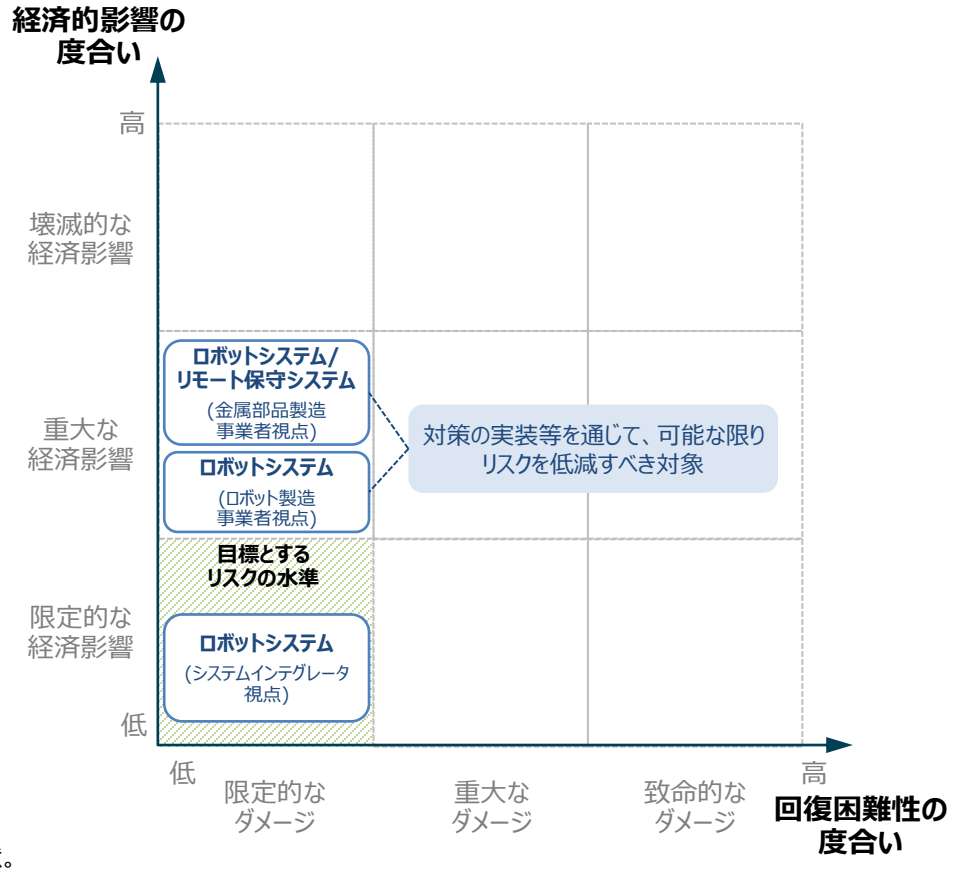
3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
②リスクアセスメント->マッピング結果の整理と評価の実施

- 自社が管理するシステムだけでなく、リモート保守システムにおけるセキュリティインシデントによってもロボットシステムに影響が及び得るため、IoT-SSFの適用主体である「金属部品製造事業者」は、ロボットシステムに加えてリモート保守システムに対しても対策を具備させる必要がある。

リスクの大きさ（※1）

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(※2)
金属部品製造事業者	• 保護柵があるため、従業員が重症を負う可能性は低い。	• 生産設備の停止や不良品の発生によって、経済的な損失を被る可能性がある。
システムインテグレータ	• 従業員が重症を負う可能性は低い。	• 責任は限定的である可能性がある。
ロボット製造事業者	• 従業員が重症を負う可能性は低い。	• 製品回収が発生するおそれがある。

想定されるリスク(例)のマッピング結果



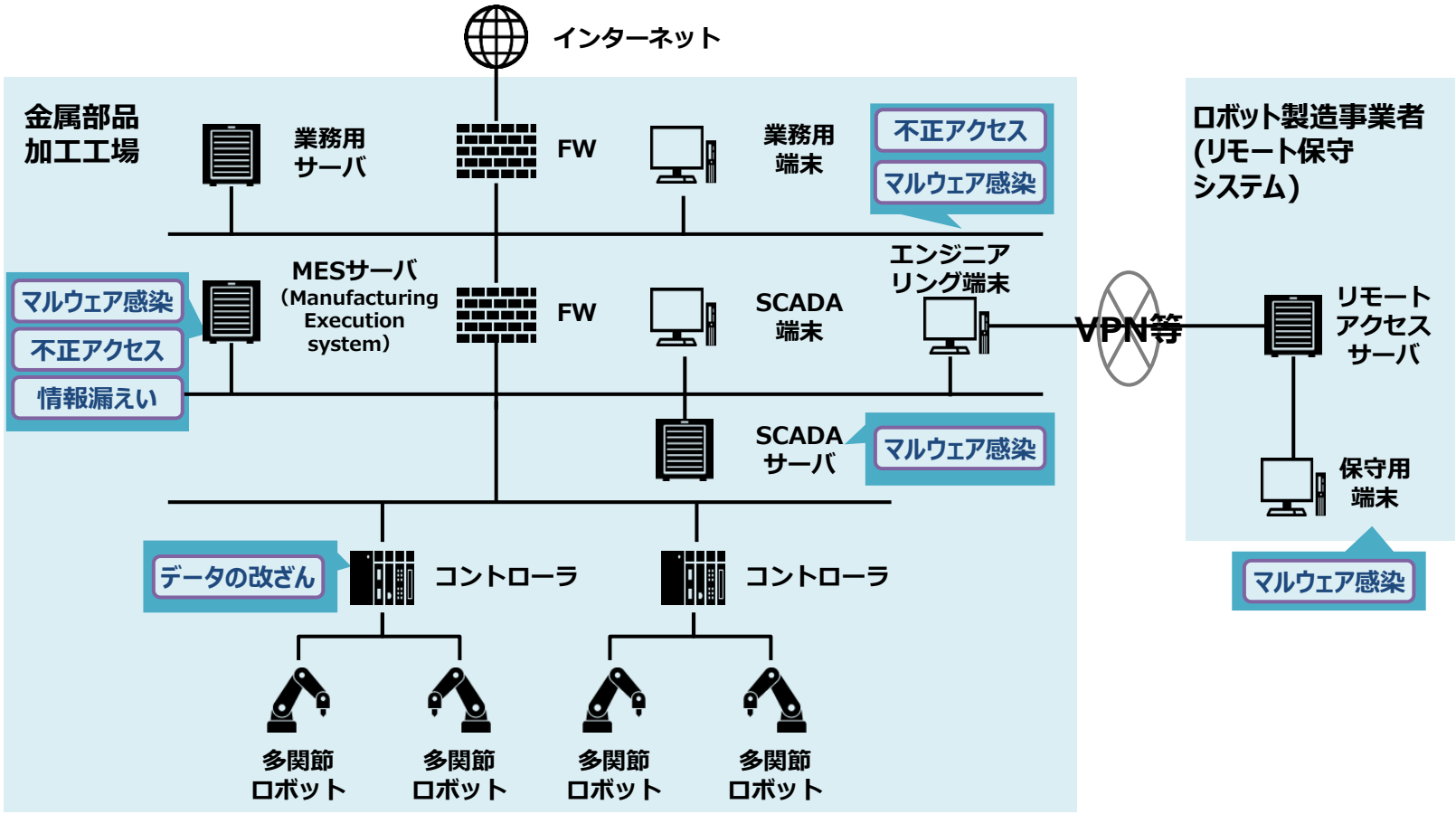
※1：「回復困難性の度合い」及び「経済的影響の度合い」では、主要な被害のみを記載していることに留意。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化

③リスク対応->システムを構成する機器ごとの脅威の整理

- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
③リスク対応->脅威に対する対策の整理

- 適用主体である金属部品製造事業者は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討する。

金属部品製造事業者（自身）にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
ロボットの制御に関わる設備の保護	• 適切な水準のアクセス制御の実装 • ソフトウェアのインストールの制限 • IoT機器・システムにおける運用開始時の正しい設置、設定
リモート保守システムからのアクセスの保護	• 適切な水準のアクセス制御の実装 • IoT 機器・システムの適正な運用・保守 • 暗号化によるデータの保護（通信経路の保護等） • ソフトウェアの完全性の検証

サポート事業者にとってのリスクを低減するため対応を要請する対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
セキュアなロボット及び周辺機器の調達/提供	• 企画・設計段階におけるセキュリティ要求事項の分析及び仕様化 • （ロボット製造事業者において適切に実施されていることが調達前に確認されるべき対策）
十分な期間のサポート契約締結	• IoT機器・システムに対するアップデートの適用

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
③リスク対応->脅威に対する対策の整理

- 想定される脅威を踏まえ、第3軸「求められるセキュリティ・セーフティ要求」における観点ごとに金属部品製造事業者にて実装が想定される対策要件を整理する。

金属部品製造事業者にて実装が想定される対策要件の例

第３軸	実装先	想定される脅威（例）	対策要件
第１の観点	ソシキ・ヒト	全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
			IoT セキュリティに関するステークホルダーの役割の明確化
			IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		なりすまし 不正アクセス	適切な水準のアクセス制御の実装
		マルウェア感染	ソフトウェアの完全性の検証
		マルウェア感染	ソフトウェアのインストールの制限
		なりすまし	暗号化によるデータの保護
		不正アクセス	適切なネットワークの分離
		不正利用	セキュリティ設計と両立するセーフティ設計の仕様化
		全般	セキュアな開発環境と開発手法の適用
		全般	IoT 機器・システムにおけるセキュリティ機能の検証
		全般	信頼できる IoT 機器やサービスの選定
		全般	IoT 機器・システムにおける運用開始時の正しい設置、設定
第２の観点	ソシキ・ヒト	全般	運用中における IoT セキュリティを目的とした体制の確保
			過去の対応事例からの学習
	プロシージャ	全般	脆弱性対応に必要な手順等の整備と実践
		全般	インシデント対応手順の整備と実践
		全般	事業継続計画の策定と実践
		全般	IoT 機器・システムの適正な使用
		全般	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令および契約上の要求事項の遵守
		全般	継続的な資産管理
		全般	IoT 機器・システムのモニタリング及びログの取得、分析
		マルウェア感染	IoT 機器・システムに対するアップデートの適用

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
③リスク対応->整理した対策に対する意思決定

- 影響度が大きいリスクに対処するための対策方針を踏まえて実装することとした対策例は、以下の通り。

金属部品製造事業者における実際に講じる対策要件の例

観点	対策要件	実際に講じる対策の例
第1の観点	**企画・設計段階におけるセキュリティ要求事項の分析及び仕様化**	• 本社情報システム部門のセキュリティ担当者と工場内のセキュリティ担当者が中心となり、ロボットシステムの企画・設計時においてリスクアセスメントを実施し、セキュリティ要件を特定、要件実装に係る費用を確保 • 特定したセキュリティ要求事項をロボットシステムの委託仕様書へ記載
第2の観点	**企画・設計段階におけるセキュリティ要求事項の分析及び仕様化**	• ロボット及び周辺機器に関して、ロボット製造事業者と十分な期間の保守契約を締結する。 • セキュリティアップデートを含むソフトウェアやファームウェアの更新を、以下のような措置を通じて不正アクセス等から保護したうえで実施 ✓ 自社の担当者または保守を担当するロボット製造事業者から提供されたことが確かなプログラムを適用 ✓ 更新をネットワーク経由で遠隔から行う場合、通信経路を適切な方式により暗号化 ✓ 更新実行前にあらかじめ動作検証等を実施

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化

③リスク対応->整理した対策に対する意思決定

- 影響度が大きいリスクに対処するための対策方針を踏まえて実装することとした対策例は、以下の通り。

システムインテグレータに対応を依頼すべき対策の例

観点	対策要件	実際に講じる対策の例
第1の観点	**適切な水準のアクセス制御の実装**	• 設備等の設置エリアに至るまでに物理セキュリティ対策が講じられているという前提のもと、SCADA端末/サーバやエンジニアリング端末等の操作を許可する前に、操作者に対するID、パスワードによる認証の要求 • エンジニアリング端末等からコントローラへの接続を行う際、端末ID及びパスワードによる認証 • 従業員及び関連会社の職員に対しては、各々の職務に応じて最小限の権限のみの付与
	ソフトウェアのインストールの制限	• エンジニアリング端末やSCADA等のロボットシステムを構成する機器において、起動を許可するソフトウェアやプロセスを定めたホワイトリストの作成、及びリストに掲載されていないもののインストールや起動の防止
	IoT機器・システムにおける運用開始時の正しい設置、設定	• ロボットシステムを構成する設備を設置、設定する際、機器の動作仕様を考慮しつつ、運用開始までに動作状況の確認

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
③リスク対応->整理した対策に対する意思決定

- 影響度が大きいリスクに対処するための対策方針を踏まえて実装することとした対策例は、以下の通り。

ロボット製造事業者に対応を依頼すべき対策の例

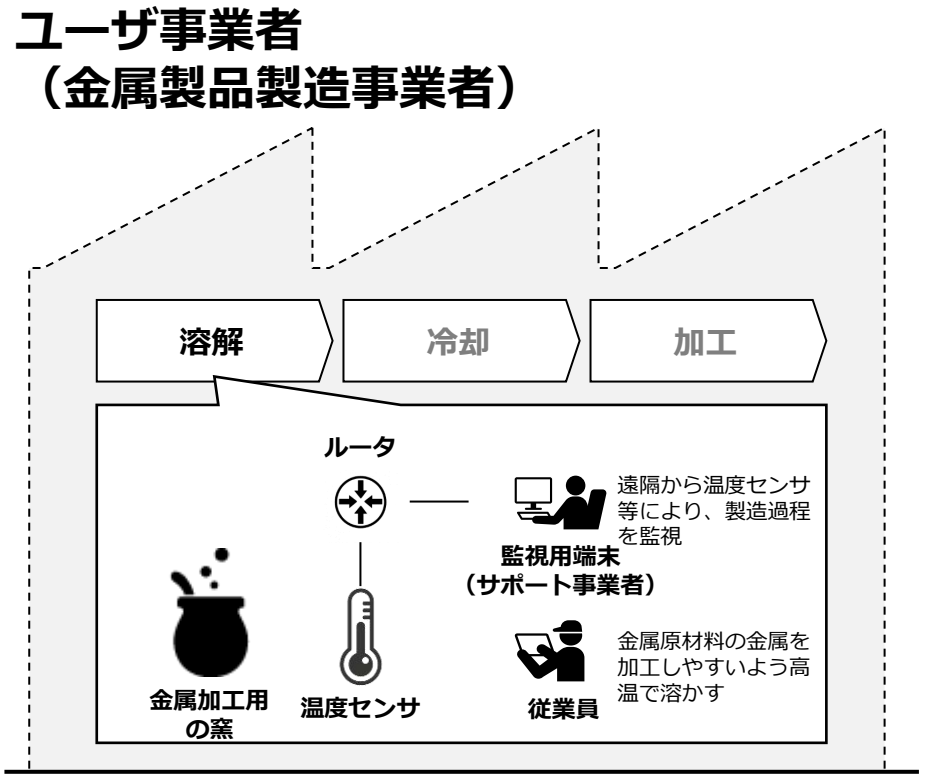
観点	対策要件	実際に講じる対策の例
第2の観点	**IoT機器・システムの適正な運用・保守**	• 設備等の設置エリアに至るまでに物理セキュリティ対策が講じられているという前提のもと、SCADA端末/サーバやエンジニアリング端末等の操作を許可する前に、操作者に対するID、パスワードによる認証の要求 • エンジニアリング端末等からコントローラへの接続を行う際、端末ID及びパスワードによる認証 • 従業員及び関連会社の職員に対しては、各々の職務に応じて最小限の権限のみの付与
	IoT機器・システムに対するアップデートの適用	• セキュリティアップデートを含むソフトウェアやファームウェアの更新を、以下のような措置を通じて不正アクセス等から保護したうえで実施 ✓ リモートアクセスを行う際、担当者に多要素認証の実施 ✓ 更新をネットワーク経由で遠隔から行う場合、通信経路を適切な方式による暗号化

3-6.金属製造現場の温度センサ等による製造設備の状態監視

①リスクアセスメント、リスク対応に向けた事前準備->対象ソリューションの概要

- 本ユースケースの適用主体は、ユーザ事業者にサービスを提供するサポート事業者とする。
- 当該事業者は工場の設備等に設置した各種センサから得たデータに基づいて稼働情報を可視化することで、各設備・機器の状態を常時監視するサービスを企画しており、サービス提供を見越して金属製品製造事業者をユーザ事業者と設定して、リスクアセスメント及びリスク対応を実施。

- サポート事業者は工場の各設備に設置された各種IoT機器を通じて、設備の稼働情報を常時収集する。
- サポート事業者は収集した情報が適切な範囲に収まっているかを示すレポートを提供するものとする。
- サポート事業者が各設備の保守業務も請け負うこととし、もし設備の異常を検知した場合には、ユーザ事業者（金属製品製造事業者）の管理者にメール等で通知するとともに、即座に現場に駆け付けることを想定。

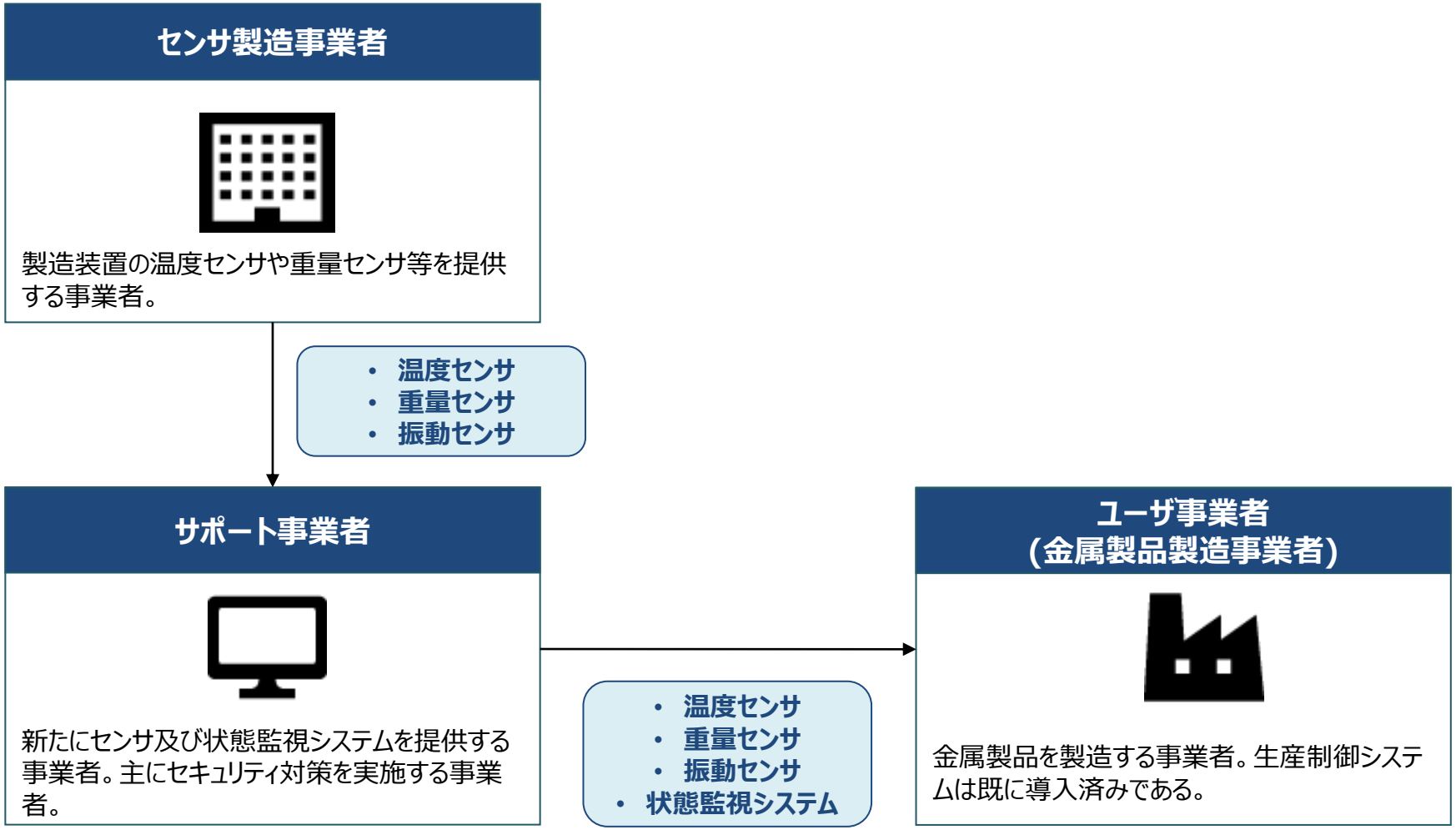


[参考] 経済産業省「中小ものづくり企業IoT等活用事例」等

3-6.金属製造現場の温度センサ等による製造設備の状態監視

①リスクアセスメント、リスク対応に向けた事前準備->ステークホルダー関係図

- ステークホルダーは、「サポート事業者」、「ユーザ事業者（金属製品製造事業者）」及び「センサ製造事業者」の３者。

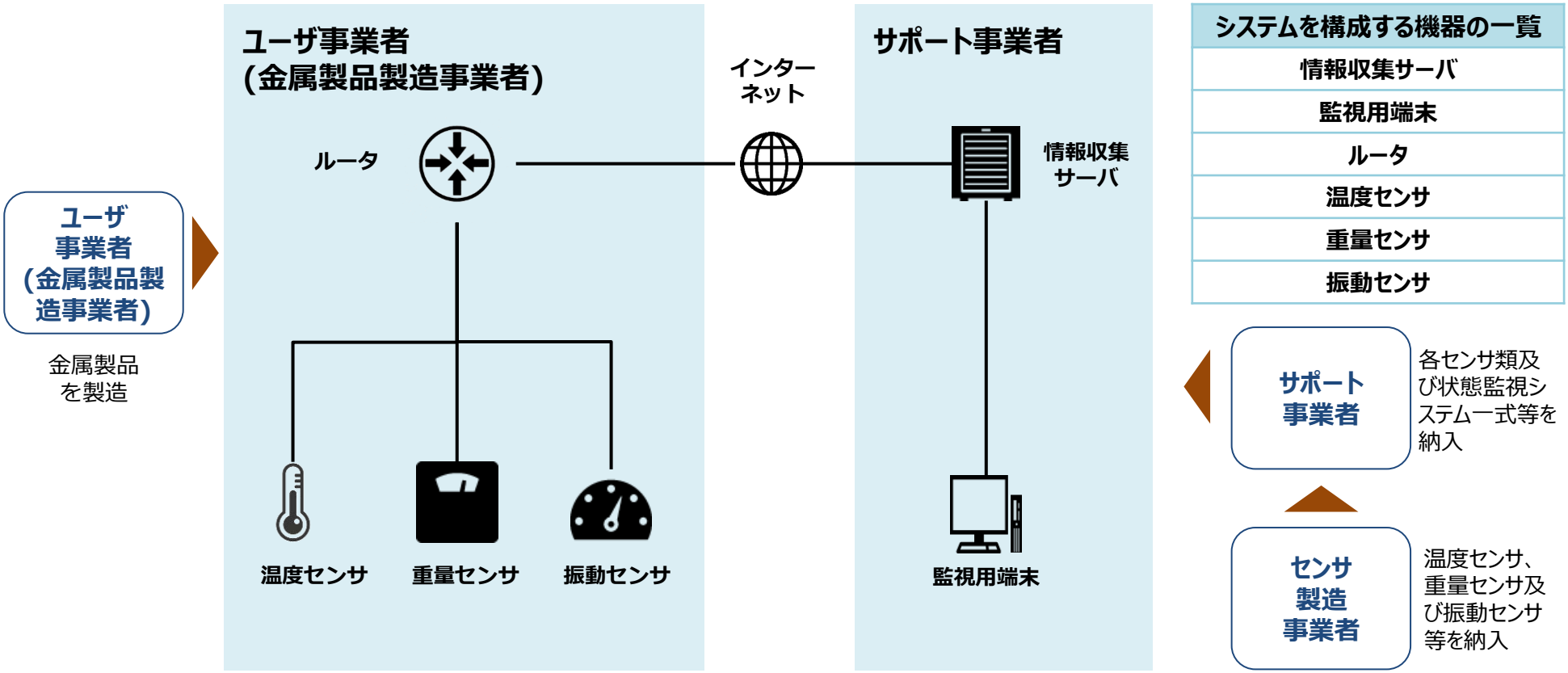


[参考] 経済産業省「中小ものづくり企業IoT等活用事例」等

3-6.金属製造現場の温度センサ等による製造設備の状態監視

①リスクアセスメント、リスク対応に向けた事前準備->システム構成図

- システムを構成する機器は以下を想定。



システムを構成する機器の一覧
情報収集サーバ
監視用端末
ルータ
温度センサ
重量センサ
振動センサ

[参考] 経済産業省「中小ものづくり企業IoT等活用事例」等

3-6.金属製造現場の温度センサ等による製造設備の状態監視
②リスクアセスメント->想定されるセキュリティインシデント等とその結果の特定

- ステークホルダーごとにリスクアセスメントを行うにあたり、対象機器・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及び想定される被害（例）を整理。

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)
サポート事業者にとってのリスク	悪意のある攻撃者が、インターネットまたはローカルネットワーク経由でサポート事業者が管理する情報収集サーバを**マルウェア（例：ランサムウェア）に感染させる。**	サーバの一部機能が停止することで、サポート事業者が**ユーザ事業者に対してサービスを提供できなくなるおそれがある。**
	悪意のある攻撃者またはサポート事業者の従業員が、インターネットまたはローカルネットワーク経由でサポート事業者が管理する**情報収集サーバにDoS攻撃**を行う。	サーバの一部機能が停止することで、**温度情報等を正確に表示することができなくなる。**
ユーザ事業者（金属製品製造事業者）にとってのリスク	悪意のある攻撃者またはサポート事業者の従業員が、インターネットまたはローカルネットワーク経由でサポート事業者が管理する**情報収集サーバに不正アクセス**する。	営業秘密として管理しているユーザ事業者（金属製品製造事業者）及び他の顧客における**設備の稼働情報等が流出することで、競争力が失われる。**
センサ製造事業者にとってのリスク	（センサ製造事業者のリスクは限定的であると想定されるため、ここでは詳細を記載しない。）	

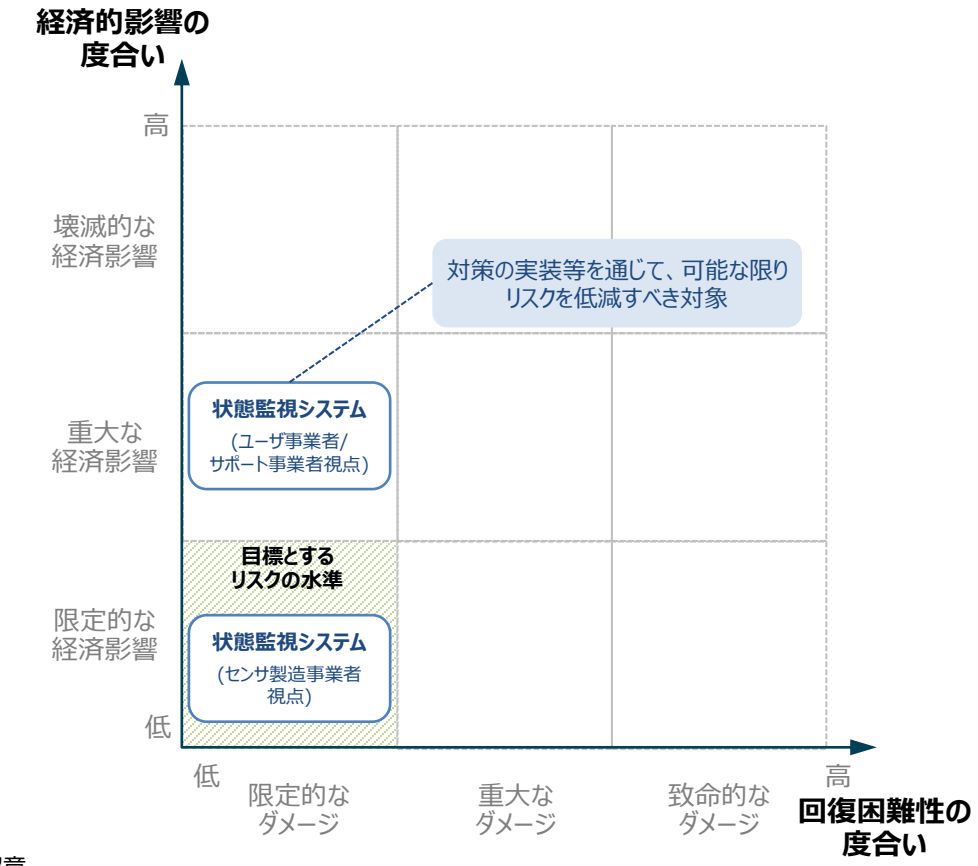
3-6.金属製造現場の温度センサ等による製造設備の状態監視
②リスクアセスメント->マッピング結果の整理と評価の実施

- IoT機器によって稼働情報を可視化しクラウド上でデータを管理する場合に、クラウドサーバから「ユーザ事業者」の営業秘密が外部へ流出する可能性が生じるため、IoT-SSFの適用主体である「サポート事業者」は、これらのリスクを踏まえて対策を実装することが望ましい。

リスクの大きさ（※1）

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(※2)
サポート事業者	• 従業員が重症を負う可能性は低い。	• ユーザ事業者に対してサービスを提供できなくなるおそれがある。
ユーザ事業者（金属製品製造事業者）	• 従業員が重症を負う可能性は低い。	• 営業秘密が流出することによって、競争力が失われるおそれがある。
センサ製造事業者	• 従業員が重症を負う可能性は低い。	• 責任は限定的である可能性がある。

想定されるリスク(例)のマッピング結果



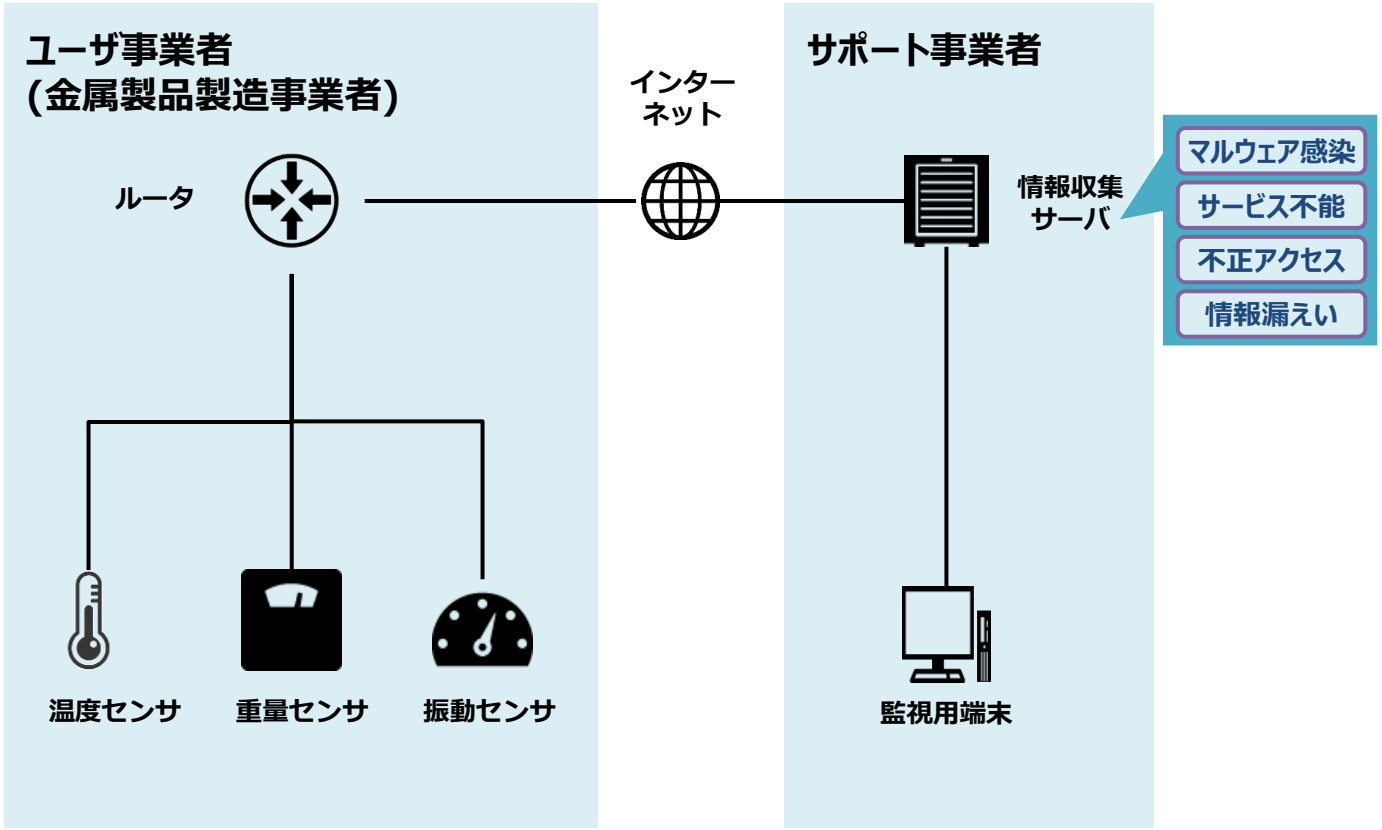
※1：「回復困難性の度合い」及び「経済的影響の度合い」では、主要な被害のみを記載していることに留意。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

3-6.金属製造現場の温度センサ等による製造設備の状態監視

③リスク対応->システムを構成する機器ごとの脅威の整理

- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

3-6.金属製造現場の温度センサ等による製造設備の状態監視
③リスク対応->脅威に対する対策の整理

- 適用主体であるサポート事業者は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討する。

サポート事業者（自身）にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
稼働情報の漏えいを防ぐ仕組みの構築	• 適切な水準のアクセス制御の実装 • 暗号化によるデータの保護
信頼性の高い状態監視システムを可能にするための仕組みの構築	• IoT機器・システムの十分な可用性の確保 • マルウェア対策の実施

ユーザ事業者（金属製品製造事業者）にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
稼働情報の漏えいを防ぐ仕組みの構築	• 適切な水準のアクセス制御の実装 • 暗号化によるデータの保護

3-6.金属製造現場の温度センサ等による製造設備の状態監視
③リスク対応->脅威に対する対策の整理

- 想定される脅威を踏まえ、第3軸「求められるセキュリティ・セーフティ要求」における観点ごとにサポート事業者にて実装が想定される対策要件を整理する。

サポート事業者にて実装が想定される対策要件の例

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の明確化
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	運用前（設計・製造段階）における法令および契約上の要求事項の遵守
		全般	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		不正アクセス	適切な水準のアクセス制御の実装
		データの改ざん	ソフトウェアの完全性の検証
		情報漏えい	ソフトウェアのインストールの制限
		全般	様々な IoT 機器に接続する際のセキュリティの確保
		データの改ざん	暗号化によるデータの保護
		マルウェア感染	
		全般	IoT 機器・システムにおける運用開始時の正しい設置、設定
第 2 の観点	ソシキ・ヒト	全般	利用者へのリスクの周知等の情報発信
		全般	運用中における IoT セキュリティを目的とした体制の確保
		全般	過去の対応事例からの学習
	プロシージャ	全般	脆弱性対応に必要な手順等の整備と実践
		全般	インシデント対応手順の整備と実践
		全般	IoT 機器・システムの適正な使用
		全般	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令および契約上の要求事項の遵守
		不正アクセス マルウェア感染	継続的な資産管理
		全般	プログラムソースコード及び関連書類の保護
		不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
		全般	IoT 機器・システムに対するアップデートの適用

3-6.金属製造現場の温度センサ等による製造設備の状態監視
③リスク対応->整理した対策に対する意思決定

- サポート事業者がシステムの設計、開発、運用等の段階で実装することとした対策要件の例を以下に示す。

観点	対策要件	実際に講じる対策の例
第1の観点	**適切な水準のアクセス制御の実装**	• あるユーザ事業者（金属製品製造事業者以外の事業者も含む）から収集した稼働情報を、他のユーザ事業者から情報収集サーバ上で閲覧できないように、ユーザ事業者ごとに適切なアクセス権限の設定 • 想定されるリスクの大きさを考慮した方式による、ユーザ事業者や自社の従業員、接続するIoT機器の認証 • 情報収集サーバのアプリケーションへの特権アクセスに対して、多要素認証を適用 • パスワード等の認証情報の安全管理（例：ハッシュ化のうえ保管）
	暗号化によるデータの保護	• 通信中のデータにおける完全性の検証 • 情報収集サーバ上に保管されている稼働情報等の暗号化
	マルウェア対策の実施	• 情報収集サーバ及び監視用端末におけるマルウェア対策ソフトウェアの導入 • 不正通信検知機能を有するルータ等の導入
	IoT機器・システムの十分な可用性の確保	• 情報収集サーバやルータに対する(D)DoS攻撃を想定し、一定レベルの負荷に耐える容量や負荷分散用機器を確保 • 情報収集サーバやルータにおいて不審な通信（例：特定のIPアドレスからの大量のリクエスト）を検知し、適宜遮断等する • アプリケーションのテスト段階における一定レベルの負荷試験の実施

付録　「具体的なユースケースにおける記載事項」の概要

- 「具体的なユースケース」の記載事項とIoT-SSFにおける3つの軸の対応は、以下の通り。

記載項目

リスクアセスメント、リスク対応に向けた事前準備

- 対象ソリューションの概要
- ステークホルダー関係図
- 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
- リスク基準

リスクアセスメント

- 想定されるセキュリティインシデント等とその結果の特定
- 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
- マッピング結果の整理と評価の実施

リスク対応（ステークホルダー別の対策例一覧）

- システムを構成する機器ごとの脅威の整理
- 脅威への対策の整理
- 整理した対策に対する意思決定

IoT-SSFにおける3つの軸

第1軸：経済的影響の度合い

インシデントの影響の回復の困難性からリスクを捉えるもの

第2軸：回復困難性の度合い

インシデントによる影響の回復の可能性・困難性という観点を除き、インシデントによる影響の大きさを金銭的価値に換算した場合の大きさ・度合いを基準としたもの

第3軸：求められるセキュリティ・セーフティ要求

フィジカル・サイバー間をつなぐ機器・システムのセキュリティ対策を包括的に整理するため、セキュリティ・セーフティを確保するための手法を4つの観点から整理したもの