経済産業省

資料３

『第2層：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タスクフォースの検討の方向性

令和４年３月９日

経済産業省 商務情報政策局
サイバーセキュリティ課

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（CPSF）とその実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に向けた諸外国の検討状況

4. 本タスクフォースにおける検討事項
   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
   4. 今後の課題

分野別SWGにおけるサイバー・フィジカルセキュリティ対策フレームワーク（CPSF）の具体化とテーマ別TFにおける検討

- **7つの産業分野別サブワーキンググループ(SWG)**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 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**

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. 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）とその実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に向けた諸外国の検討状況

4. 本タスクフォースにおける検討事項
   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
   4. 今後の課題

米国上下水道分野における継続的なセキュリティ脅威

- 2021年10月、米国サイバーセキュリティ・インフラセキュリティ庁（CISA）、連邦捜査局（FBI）、環境保護庁（EPA）等は、共同でサイバーセキュリティ勧告を発表し、上下水道への継続的なサイバー脅威について詳述。
- 米国ではこの数年、上下水道施設を対象にしたサイバー攻撃が多数報告されており、地域社会に清潔な飲料水を提供し、効果的に廃水を管理する能力が脅かされているとされる。

上下水道への攻撃事例

2019年から2021年にかけて上下水道システム(WWS)への攻撃が多数発生している。

2021年3月

ネバダ州にてWWS施設のSCADA及びバックアップに対して未知のランサムウェアによる攻撃

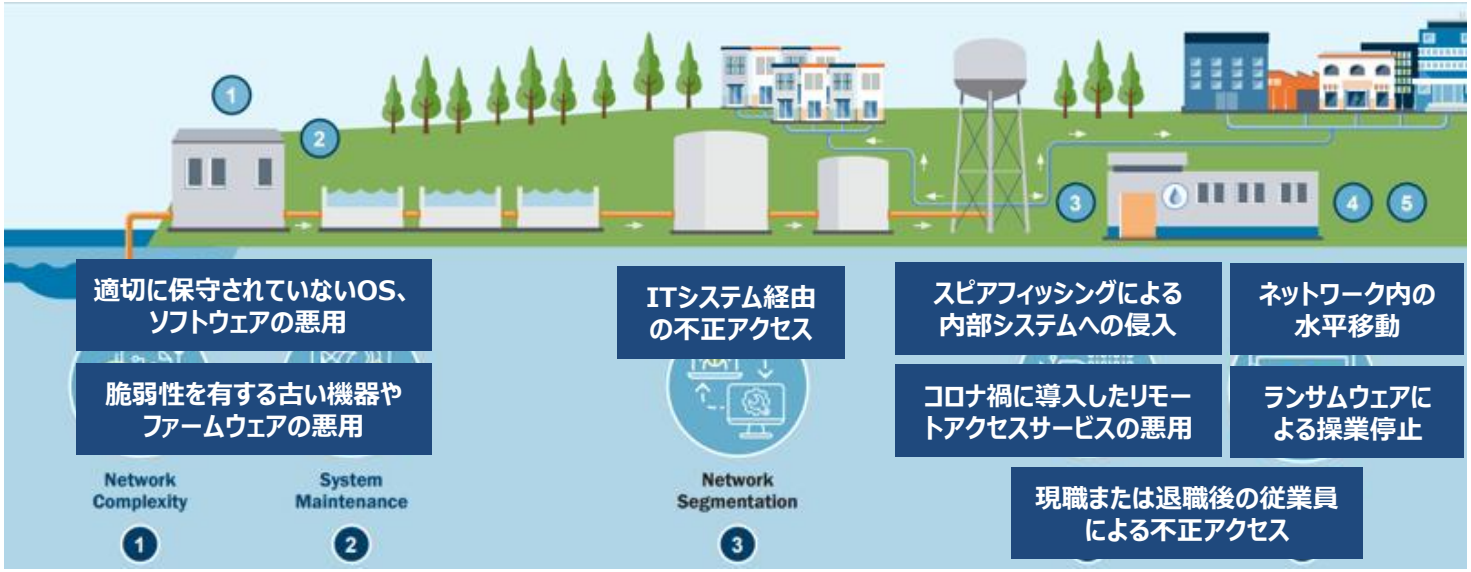
2021年7月

メイン州にてWWS施設のSCADAがランサムウェア ”ZuCaNo”に感染。復旧まで、手動のオペレーションを強制

2021年8月

カルフォルニア州のWWS施設にて3台のSCADAサーバがランサムウェア”Ghost”亜種に感染

共同勧告にて注意喚起がなされている脅威と推奨される対策



推奨される対策

システム監視による不審な活動の検知	リモートアクセスの保護	IT/OTネットワークのセグメント化	対応計画の策定及び訓練等の実施	独立した安全制御システムの設置

[出典] CISA “CYBER RISKS RESOURCES FOR THE WATER AND WASTEWATER SYSTEMS SECTOR”等 を参考に作成

組込み機器に対するランサムウェア攻撃

- 2022年1月、組込み機器向けのセキュリティプロバイダーRed Balloon Security社は、実際のネットワークで使用されている組込みシステムでランサムウェアを展開することが可能であるとの調査結果を発表。
- 同社は、Schneider Electric社製の保護リレーの脆弱性を悪用してランサムウェアのペイロードを展開することが可能で、このプロセスを「高度だが再現可能」と述べている。

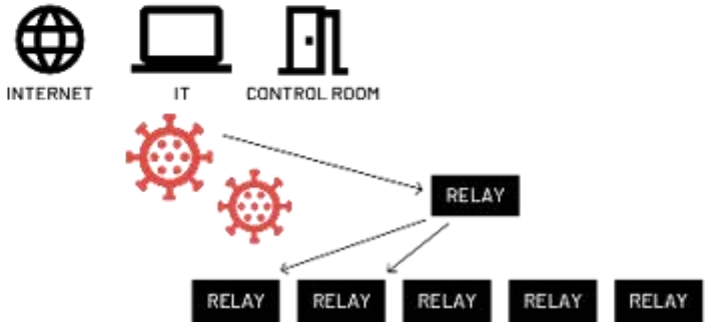
組込み機器に対してランサムウェアを展開する攻撃手法

- Red Balloon Security社は、以下の手法によりランサムウェアの感染等につながる Schneider Electric社製保護リレーの脆弱性を発見。
- 同社は、ミッションクリティカルな機器の完全性や可用性に関して、ランサムウェアが重要な脅威となる可能性を指摘。

物理的なアクセス

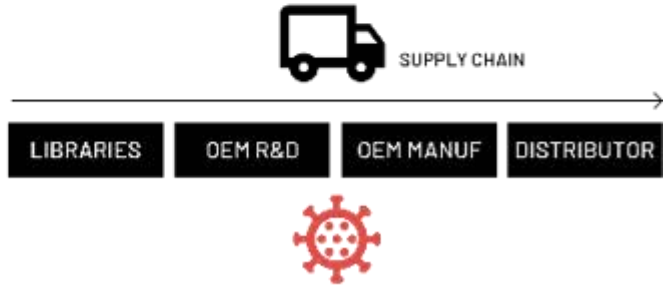
- 実施には、業界内での機器設置状況に関する特定の知識を要するが、現場での機器アクセスによって攻撃が実現し得る。

エンジニアリング・ワークステーション/SCADA経由の感染



- ITシステムを経由してOTシステムへと侵入する。オペレータのアカウントの侵害や、機器に接続する制御システムへの侵入から攻撃が始まる可能性がある。

サプライチェーン攻撃による感染



- ライブラリ、製造元の研究開発プロセス、製造プロセス、販売店で出荷を待つ間の機器操作など、様々な段階での侵害が含まれる。

[出典] Red Balloon Security “Ransomware installation on embedded devices is possible, because we’ve done it” を参考に作成

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（CPSF）とその実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に向けた諸外国の検討状況

4. 本タスクフォースにおける検討事項
   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
   4. 今後の課題

米国大統領令14028を受けたIoT製品のサイバーセキュリティ・ラベルの検討

- 2021年5月に公表された米国大統領令に基づき、NISTは消費者向けIoT製品のサイバーセキュリティ・ラベリングにおける推奨基準の最新版を公表。
- 2022年5月12日までに、NISTは、上記サイバーセキュリティラベリングに関する総括報告書を発行する予定。

Executive Order on Improving the Nation's Cybersecurity (2021/5/12公開)

Sec.4. ソフトウェアサプライチェーンセキュリティの強化
(s) IoT機器のセキュリティ機能とソフトウェアの開発方法について一般の人々を教育するためのパイロットプログラムを開始
(t) 本命令の日付から270日以内に、**消費者向けラベリングプログラムのためのIoTサイバーセキュリティ基準**を特定

大統領令(EO)を受けてNISTにて策定

Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products (2022/2/4公開)

- 消費者向けに提供されるIoT製品*を対象にしたラベリング制度を確立しようとする者(制度オーナー)が、実際にプログラムを開発する際に考慮すべき、以下のような検討事項と推奨事項を示している。

* IoT製品(IoT product)には、IoT機器だけではなく、当該機器を利用するために必要な製品コンポーネント(ネットワーク機器、モバイルアプリケーション等を含む)を含み得る。

推奨ベースライン製品基準 (2章)

- IoT製品及びその開発者に期待されるサイバーセキュリティ関連の成果を定義

✓ 資産の識別	✓ サイバーセキュリティ状態認識
✓ 製品の構成	✓ ドキュメンテーション
✓ データ保護	✓ 情報及び問合せの受付
✓ インターフェイスのアクセス制御	✓ 情報の発信
✓ ソフトウェアの更新	✓ 教育と意識向上

ラベリングに関する考慮事項 (3章)

- 推奨するIoTラベルのアプローチ、ラベルを消費者に提供する際の検討事項、消費者教育に関する検討事項等を提示

推奨アプローチ	バイナリーラベル(基準準拠を示す単一のラベル)に、URL等を記載し、追加情報を提供するレイヤーアプローチを推奨。
提示方法	消費者が購入前、購入時、購入後に確認できる必要があり、物理またはデジタルのフォーマットをサポートする。
消費者教育	消費者がアクセスできる内容に、ラベルの意図とスコープ、準拠基準、基準への適合宣言、消費者の責任等が含まれる。

適合性評価に関する考慮事項 (4章)

- IoT製品が製品基準に適合していることを証明するために活用できるIoT適合性評価活動には以下が含まれる。

自己適合宣言	製品提供者自身による基準への適合宣言
第三者による検査・試験	第三者機関によるIoT製品を対象にした試験または検査
第三者認証	総合的な審査に基づき第三者機関が付与する認証

IoT機器を対象にしたサイバーセキュリティガイダンス文書
（NIST IR 8259シリーズ/NIST SP 800-213シリーズ）

- 米国NISTは、IoT機器製造者向けに**NIST IR 8259として、IoT機器の製造者に推奨される6つのサイバーセキュリティに関連する活動を整理**(2020年5月公開)。
- 2021年11月、連邦政府機関向けのガイダンスとしてNIST SP 800-213シリーズを公表。

製造者向けガイダンス

NIST IR 8259 2020年5月公開
(Foundational Cybersecurity Activities for IoT Device Manufacturers)

IoT機器の製造者に推奨される**6つのサイバーセキュリティに関連する基本的な活動**を定義。

NIST IR 8259A 2020年5月公開
IoT Device Cybersecurity Capability Core Baseline

IoT機器が備えるべき**6つのコアサイバーセキュリティ機能**を定義。

NIST IR 8259B 2021年8月公開
IoT Non-Technical Supporting Capability Core Baseline

製造業者が製造するIoT機器をサポートするために導入を検討すべき、**4つの非技術的サポート機能**を定義。

NIST IR 8259C (Draft) 2020年12月ドラフト公開
Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline

8259A及び8259Bを拡張し、**カスタマイズされたプロファイルを作成するためのプロセス**を提供。

NIST IR 8259D (Draft) 2021年11月廃止
Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government

2021年11月に、NIST IR 8259D (Draft)が廃止され、NIST SP 800-213Aとして公表

連邦政府機関向けガイダンス

NIST SP 800-213 2021年11月公開
(IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements)

連邦政府機関向けに、**IoT機器を既存システムに統合する際の検討に資する推奨事項**を定義。

NIST SP 800-213A 2021年11月公開
IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog

連邦政府機関向けに詳細化された**IoT機器のサイバーセキュリティ機能と非技術的サポート機能**のカタログを提供。

NIST SP 800-213は、**NIST SP 800-53 Rev.5**をサポートするために必要となり得る技術的/非技術的な機能を特定するもの

NIST SP 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements

- 2021年11月、2021年2月12日まで意見募集を実施していたIoT機器を利用する米国連邦政府機関向けのガイダンスであるSP 800-213の最終版を公表。
- 本文書は、IoT機器を既存システムに統合する際のセキュリティ検討に資する推奨事項（IoT機器に適用されるサイバーセキュリティ要件の決定プロセスを含む）を記載。米国連邦政府機関が、既存の方針や手順（調達、セキュリティ、情報システム管理など）に沿ってIoT機器のセキュリティ要件を特定する際の出発点として機能する。

連邦政府機関が利用するIoT機器に適用されるサイバーセキュリティ要件の決定プロセス

IoT機器のユースケース及びIoT機器のサイバーセキュリティに関する特性の理解

- IoT機器のユースケース及びIoT機器の統合（利用）における利点の理解
- IoT機器で扱うデータに関する理解
  - ✓ 収集データに関する理解
  - ✓ 保存データに関する理解
  - ✓ 移転データに関する理解
- IoT機器の統合（利用）による他のシステム等に対する影響の理解
- IoT製造者における開発及びサポート内容の理解

IoT機器の統合がもたらす既存システムのリスクアセスメントに対する影響の理解

- IoT機器の統合（利用）がもたらす脅威源等の理解
- IoT機器の統合（利用）がもたらす脆弱性の理解
- IoT機器の統合（利用）が与える「起こりやすさ」への影響の理解
- IoT機器の統合（利用）が与える「被害の大きさ」への影響の理解

IoT機器に適用されるサイバーセキュリティ要件の特定

- SP 800-213Aを用いたサイバーセキュリティ要件の特定
- 以下の文書を用いたサイバーセキュリティ要件の特定
  - ✓ NISTIR 8259 A/B
  - ✓ NIST SP 800-53
  - ✓ NIST Cybersecurity Framework 等

欧州における消費者向けIoTに係るセキュリティ基準等の整備

- 2021年8月、欧州電気通信標準化機構（ETSI）は、消費者向けIoT機器のセキュリティ強化に向け、従前に策定したETSI EN 303 645に加え、その実装や評価を支援するETSI TS 103 701を公開した。
- 同規格は、ETSI TS 103 645及びETSI EN 303 645に対する適合性評価手法を規定するもの。

消費者IoT向けの要求事項

ETSI TS 103 645
Baseline Requirements

ETSI EN 303 645
Baseline Requirements

- 消費者向けIoT機器及び、当該機器と関連サービスとの関わりについて、セキュリティ及びデータ保護の規定を定める
- 関連サービス自体のセキュリティについては対象外とされる

※ ETSI TS 103 645及び ETSI EN 303 645は同様の規定を有する。

適合性評価の実施方法等

ETSI TS 103 701
Conformance Assessment of Baseline Requirements

- ETSI TS 103 645及びETSI EN 303 645に対する適合性評価手法を規定
- 上記規格の各規定に対するテストケースと評価基準を定義し、具体的な様式を提供することで、当該規格の必須/推奨規定、条件/補完事項への対応を支援

■ 適合性評価の実施手順

1. 評価対象*1の特定	2. 実装適合宣言*2作成	3. 実装追加情報*3作成
機器サプライヤは、様式に沿って評価対象を特定する。	機器サプライヤは、評価対象のセキュリティ機能に基づき、実装適合宣言を作成する。	実装しているセキュリティ機能ごとに、実装に関する詳細情報を追記する。
4. 実装適合宣言の検証	**5. 評価の実施**	**6. 総合評価**
テストラボは、機器サプライヤから提供された実装適合宣言を確認し、検証する。	テストラボはテスト計画を作成し、特定の方法に基づいてテスト群を実行する。	テストラボは、テスト群の結果に基づいて総合評価を行う。(例：合格/不合格/保留)

*1: 規格中では、Device Under Test (DUT) と表記される。
*2: 規格中では、Implementation Conformance Statement (ICS) と表記される。
*3: 規格中では、Implementation eXtra Information for Testing (IXIT) と表記される。

ENISA：Cybersecurity Certification - EUCC Scheme

- EUCC Candidate Schemeは、ICT製品を対象とするCommon Criteria（CC：ISO/IEC15408）と、関連する共通評価方法（ISO/IEC 18045）に基づく欧州サイバーセキュリティ認証フレームワークにおける最初の候補スキーム。欧州においてSOG-IS※1の下で運用されていた既存のCCのスキームの後継として機能させることが目的。**2021年5月、ドラフト版への意見募集を経て、用語の定義や他ステークホルダーとの協力について追記されたV.1.1.1が発行。**
- 本文書では、評価はCCに基づくものであること（3章）、保証レベルは「substantial」か「high」の2段階であること（4章）、自己適合性評価は認められないこと（5章）、認証証明書の有効期間は最長5年間であること（20章）等、**Cybersecurity Actにより候補スキームに必要とされる要件**（認証取得の際に実装すべき要求事項やその評価プロセス、認証制度の運用等に関する事項等）**を網羅的に規定**。

本文書の目次と、関連するCybersecurity Act 54条1項の項目 a – v の対応*

章	目次	*
1	主題とスコープ	a
2	本スキームの目的	b
3	評価標準	c
4	保証レベル	d
5	自己適合性評価	e
6	認証機関向けの具体的な要求事項	f
7	認証機関の通知と認可	f
8	具体的な評価基準及び評価手法	g
9	認証に必要な情報	h

章	目次	*
10	マークとラベル	i
11	コンプライアンスを監視するための規則	j
12	認証証明書の発行、維持、継続および更新の条件	k
13	違反に関する規則	l
14	脆弱性管理に関する規則	m
15	パッチ管理	m
16	認証機関による記録の保持	n
17	国家的または国際的なスキーム	o
18	認証証明書の内容とフォーマット	p

章	目次	*
19	情報の可用性	q
20	認証証明書の有効期間	r
21	認証証明書の開示ポリシー	s
22	第三国との相互認証	t
23	ピア評価	u
24	補足的なサイバーセキュリティ情報—第55条	v
25	スキームの追加要素	a
26	アドホックWGからの推奨事項	-
27	参考	-

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（CPSF）とその実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

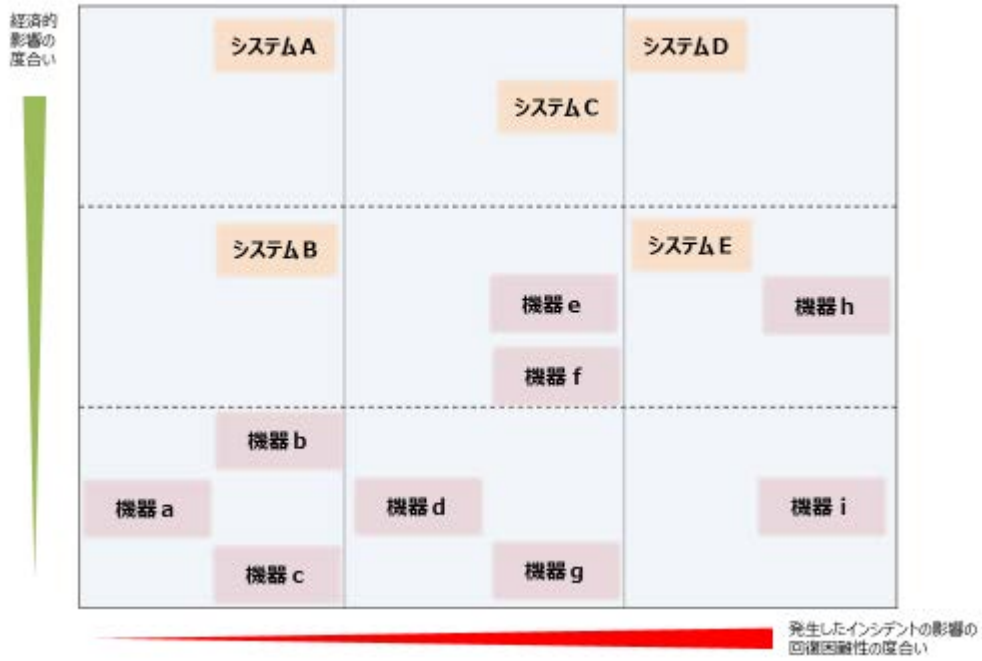
3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に向けた諸外国の検討状況

4. 本タスクフォースにおける検討
   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
   4. 今後の課題

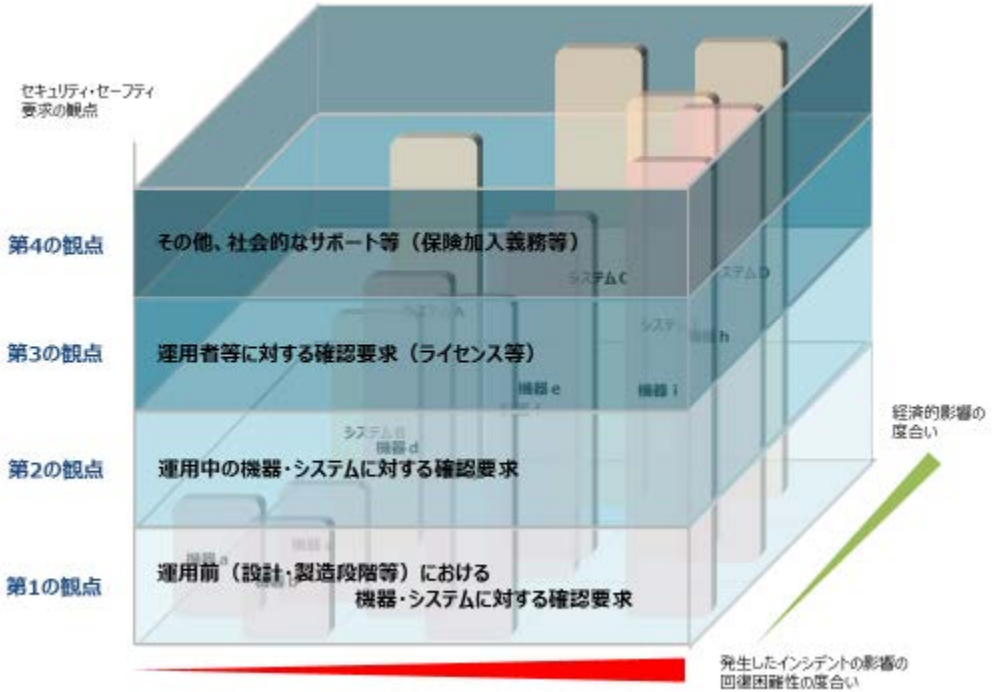
IoT-SSFの概要

- **用途や使用環境によって課題が異なるIoT機器・システムに対するセキュリティ対策を、複数のステークホルダー間で合意する**際に活用できる**「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」を2020年11月5日に公開。**
- 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



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



※　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。）

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. 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）とその実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に向けた諸外国の検討状況

4. 本タスクフォースにおける検討
   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. （IoT-SSF）の概要ユースケース集の構成
   3. 各ユースケースの概要
   4. 今後の課題

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

取扱うユースケースの一覧

- 幅広い読者にとって参考となるよう考慮した上で、取扱うユースケースを選定した。

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
2-3-1	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
2-3-2		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
2-3-3	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
2-3-4		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
2-3-5		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
2-3-6			**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**	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

IoT-SSFに基づくリスクマネジメントのプロセス

- 既存の国際標準（ISO 31000等）や本文書の上位の文書である「サイバー・フィジカル・セキュリティ対策フレームワーク」を踏まえて、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。

IoT-SSFに基づくリスクマネジメントのプロセス

- ユースケース集（2-2, 2-3）では、IoT-SSFにおける3つの軸の適用方法を示している。

ユースケース集

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：回復困難性の度合い

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：経済的影響の度合い

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

添付資料の概要（添付A）

- 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。

添付資料の概要（添付A）

- 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

添付資料の概要（添付B）

- 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 ● 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	CPS.BE-2 CPS.GV-1 CPS.GV-2
…		…	…	…

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（CPSF）とその実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に向けた諸外国の検討状況

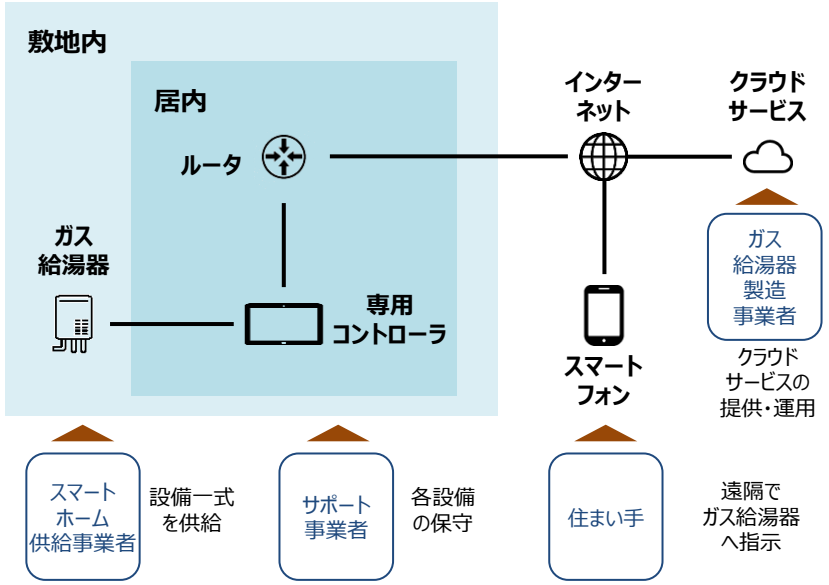
4. 本タスクフォースにおける検討
   1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要
   2. ユースケース集の構成
   3. 各ユースケースの概要
   4. 今後の課題

家庭用ガス給湯器の遠隔操作(2-3-1)

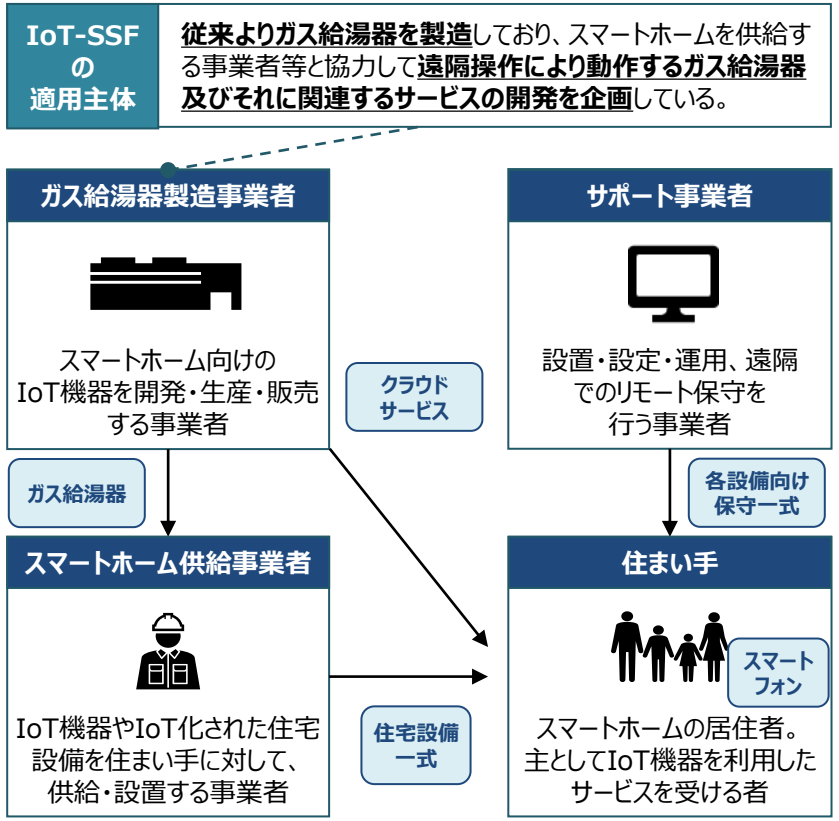
- スマートホーム向けIoT機器・サービスの事業者（ガス給湯器の製造元）がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- 住まい手が外出先よりスマートフォン用アプリを通じて、居内のガス給湯器を遠隔操作。

✓ 対象機器・システムの概要

- 住まい手が外出先よりスマートフォン用のアプリケーションを通じて、居内のガス給湯器を遠隔操作し、自動で浴槽のお湯張り等を実施するケースを想定する。
- 遠隔操作が許容される方式を用いた製品の利用を前提とする。



✓ 適用主体及び他のステークホルダーの情報



家庭用ガス給湯器の遠隔操作(2-3-1)

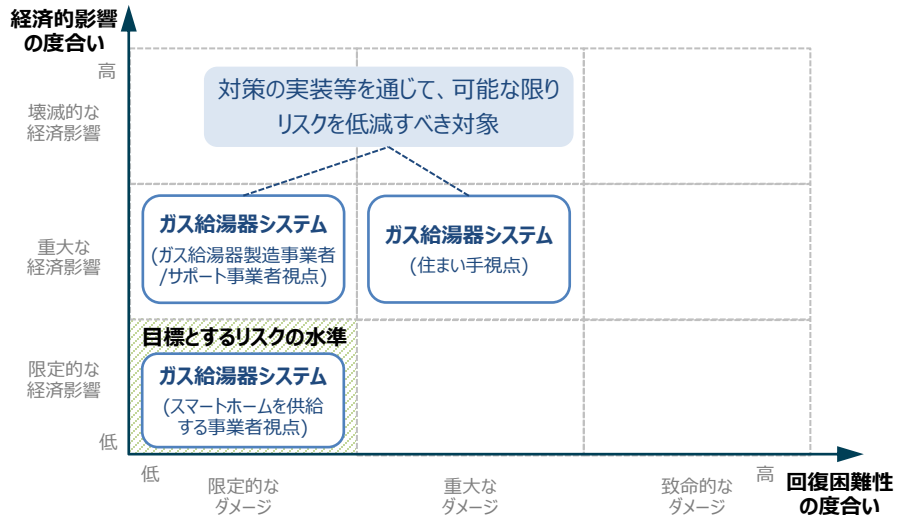
- 誤動作等により被り得るリスクが大きくなり得ると想定される「住まい手」は、一般にセキュリティに関する知見を十分に持たない場合が多いため、IoT-SSFの適用主体である「ガス給湯器製造事業者」は、これらを考慮してリスクの低減に努める必要がある。

✓ 対象機器・システムにおいて想定されるリスク(例)

分類	想定されるリスク（例）
ガス給湯器製造事業者にとってのリスク	• クラウドサービスから送信される指示データ等が改ざんされ、**ガス給湯器が誤動作し得る。**その結果、**製品回収が発生し得る。**また、製品・サービスの品質について利用者の間に**疑念が広がる可能性**がある。
サポート事業者にとってのリスク	• 自社環境が不正アクセスされ、配信前のアップデートを改ざんされることで、**ガス給湯器が誤動作し得る。**その結果、**サポート事業者の責任で製品回収が発生し得る。**また、サポートの品質について利用者の間に**疑念が広がる可能性**がある。
住まい手にとってのリスク	• クラウドサービスに不正アクセスされることで、自身の**個人情報が流出**する可能性がある。 • 専用コントローラに対するアップデートを改ざんされ配信先のコントローラがマルウェアに感染する、クラウドサービスから送信される指示データがネットワーク上で改ざんされる等により、**給湯器が誤動作し得る。**その結果、住まい手がやけど等を負うことで、**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	• 想定される**リスクは限定的**と考えられる。

✓ 想定されるリスク(例)のマッピング結果

- スマートホームを供給する事業者視点からみたガス給湯器システムの保有するリスクは、目標とする水準内に収まっている。
- しかし、住まい手、ガス給湯器製造事業者及びサポート事業者視点のガス給湯器システムの保有するリスクは、目標とする水準には収まっておらず、何らかの対処実施が望まれる。

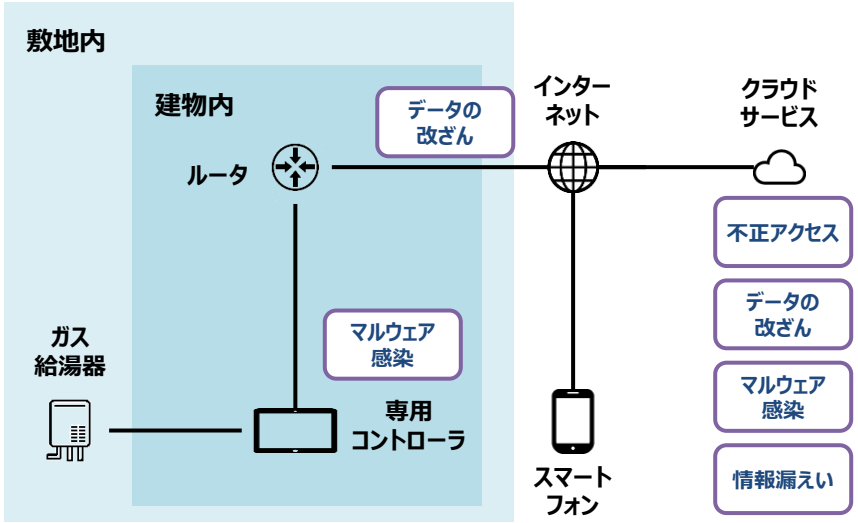


家庭用ガス給湯器の遠隔操作(2-3-1)

- 影響度が大きいリスクにつながり得る脅威の例：クラウドサービスに対する不正アクセス、専用コントローラのマルウェア感染及び、それらによるガス給湯器の誤動作等。
- 行うべきと考えられる対策の例：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[第1の観点]、IoT機器・システムに対するアップデートの適用[第2の観点]等。

✓ 影響度が大きいリスクにつながり得る脅威の例

- クラウドサービスに対する不正アクセス、情報漏えい、マルウェア感染に加えて、クラウドサービスからの通信情報に対するデータの改ざん、専用コントローラのマルウェア感染及び、それらによるガス給湯器の誤動作が、影響度が大きいリスクにつながり得る脅威の例と考えられる。



✓ 行うべきと考えられる対策の例

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(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

- **【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**
- **【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**
- **【第1の観点】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(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

- **【第2の観点】プログラムソースコード及び関連書類の保護**
- **【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**

住まい手にとってのリスクを低減するための対策(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

- **【第1の観点】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1の観点】セキュリティ設計と両立するセーフティ設計の仕様化**

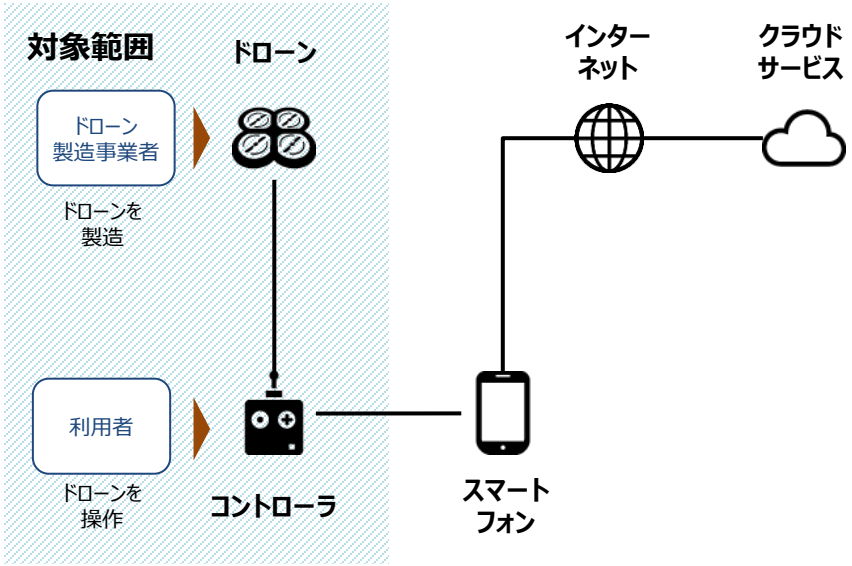
※セキュリティインシデントによっては、ガス給湯器製造事業者はガス供給事業者と連携して対応することが必要となる場合がある。

ドローンを活用した個人による写真撮影(2-3-2)

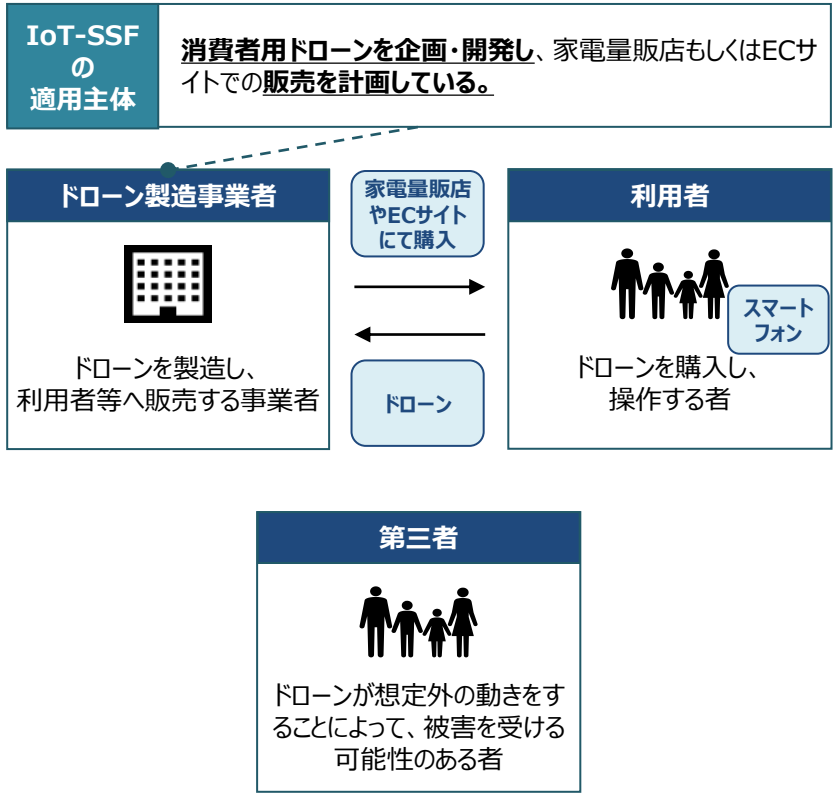
- ドローン製造事業者がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- 利用者はスマートフォンに接続されたコントローラにてドローンを操作し、ドローンに設置されたカメラで風景を撮影。

✓ 対象機器・システムの概要

- 利用者は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で風景を撮影するケースを想定する。
- 公共施設内の土地（屋外）にて許可を得た上で、各種法令で禁止されたエリアでは操作しないことについては、利用者が責任を持つと想定する。



✓ 適用主体及び他のステークホルダーの情報



ドローンを活用した個人による写真撮影(2-3-2)

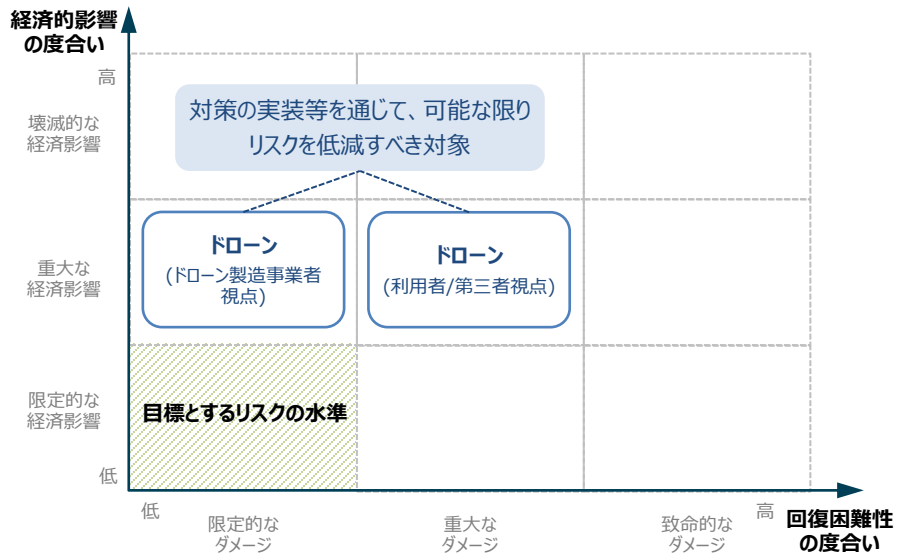
- セキュリティインシデントによってドローンの航行に影響が及んだ場合、周辺の第三者や住宅等の環境へ影響を及ぼし得ることから、 IoT-SSFの適用主体である「ドローン製造事業者」は、「利用者」に加えて「第三者」が被り得るリスクを考慮して対策を実装する必要がある。

✓ 対象機器・システムにおいて想定されるリスク(例)

分類	想定されるリスク（例）
ドローン製造事業者にとってのリスク	• **重大な脆弱性が発見される**ことによって、**大規模な製品回収**が生じ得る。
利用者にとってのリスク	• 内蔵された**カメラが不正アクセス**され、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**。 • ドローンの機体制御が乗っ取られ、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、生活にも支障をきたし得る。
第三者にとってのリスク	• 内蔵された**カメラが不正アクセス**され、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。** • ドローンの機体制御が乗っ取られ、ドローンが高高度から落下し、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。**

✓ 想定されるリスク(例)のマッピング結果

- ドローン製造事業者、利用者及び第三者視点のドローンの保有するリスクは、目標とする水準には収まっておらず、何らかの対処実施が望まれる。

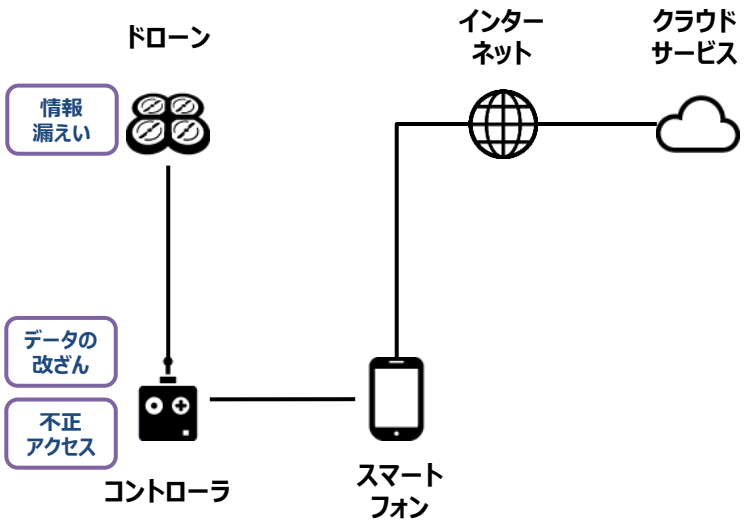


ドローンを活用した個人による写真撮影(2-3-2)

- 影響度が大きいリスクにつながり得る脅威の例：ドローンに設置されたカメラからの情報漏えい、コントローラから通信される制御データの改ざんや不正アクセス等。
- 行うべきと考えられる対策の例：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[第1の観点]、利用者へのリスクの周知等の情報発信 [第2の観点]等。

✓ 影響度が大きいリスクにつながり得る脅威の例

- ドローンに設置されたカメラからの情報漏えい、コントローラから通信される制御データの改ざんや不正アクセスが、影響度が大きいリスクにつながり得る脅威の例と考えられる。



✓ 行うべきと考えられる対策の例

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(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	• 【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 • 【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 • 【第1の観点】セキュリティ設計と両立するセーフティ設計の仕様化

利用者及び第三者にとってのリスクを低減するための対策(例)

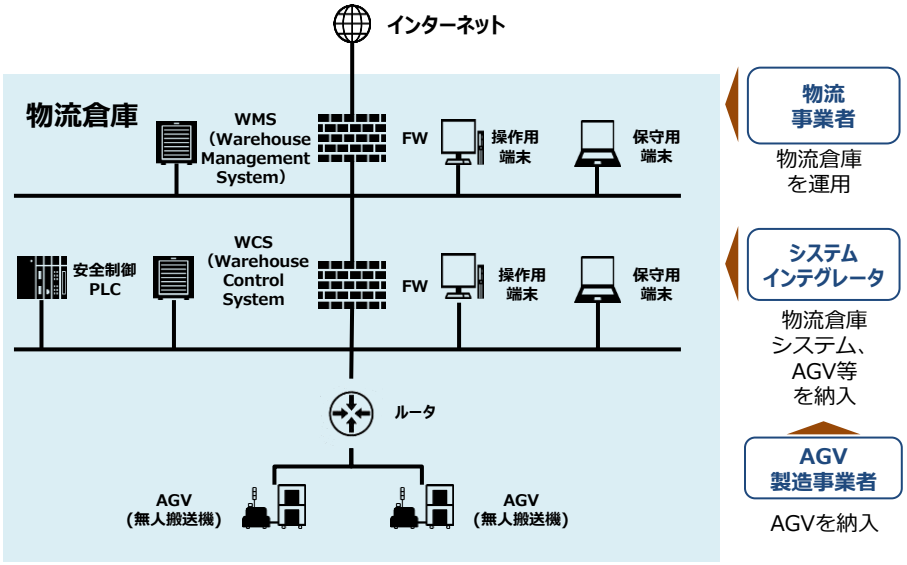
利用者への注意喚起の実施や推奨事項の明確化	• 【第2の観点】利用者へのリスクの周知等の情報発信 • 【第2の観点】IoT機器・システムの適正な使用 • 【第3の観点】IoT機器・システムの運用・管理を行う者への要求事項の特定
フェールセーフ等を含む安全対策の徹底	• 【第1の観点】セキュリティ設計と両立するセーフティ設計の仕様化

物流倉庫内のAGVによる自動ピッキング(2-3-3)

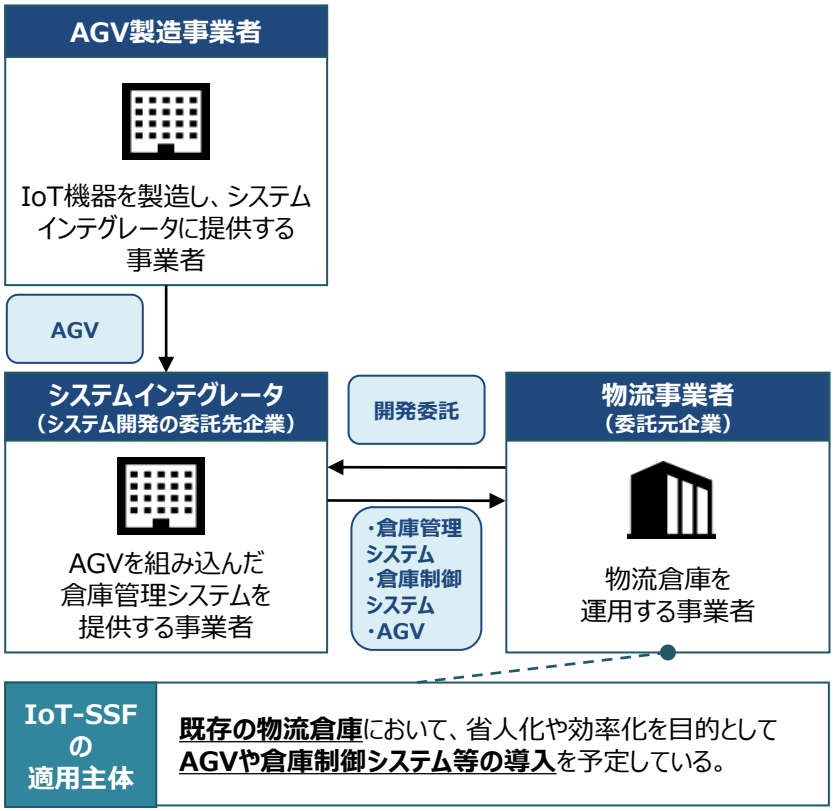
- 物流事業者がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- 当該事業者は、事業規模拡大に伴って既存の物流倉庫において、省人化や効率化を目的として新たにAGVや倉庫制御システム等の導入を予定。

✓ 対象機器・システムの概要

- 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。
- 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、作業員がピッキングを行う。



✓ 適用主体及び他のステークホルダーの情報



物流倉庫内のAGVによる自動ピッキング(2-3-3)

- 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し、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。

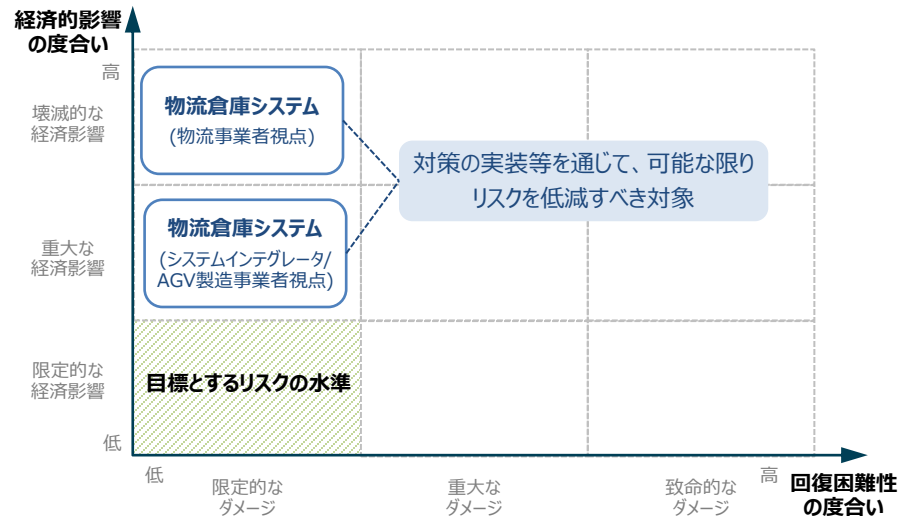
✓ 対象機器・システムにおいて想定されるリスク(例)

分類	想定されるリスク（例）
物流事業者にとってのリスク	• 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。その結果、**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	• **自社環境が不正アクセスされ、配信前のアップデートを改ざん**される。その結果、物流工場が停止し、**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**されることによって、**大規模な製品回収が生じ得る**。

※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。

✓ 想定されるリスク(例)のマッピング結果

- 物流事業者、システムインテグレータ及びAGV製造事業者視点の物流倉庫システムの保有するリスクは、目標とする水準には収まっておらず、何らかの対処実施が望まれる。

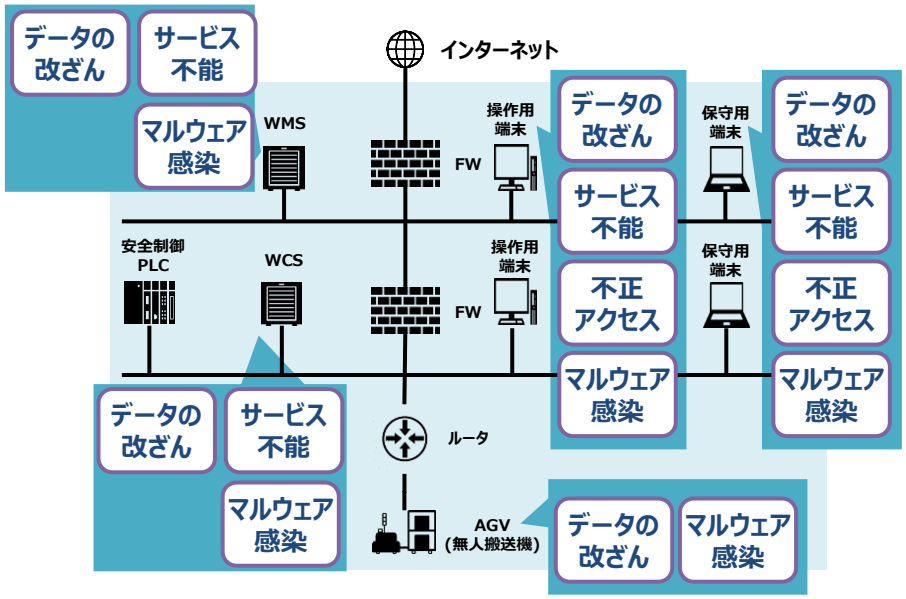


物流倉庫内のAGVによる自動ピッキング(2-3-3)

- 影響度が大きいリスクにつながり得る脅威の例： WMS、WCSに対する不正アクセス、サービス不能、マルウェア感染等。
- 行うべきと考えられる対策の例：様々なIoT機器を接続する際のセキュリティの確保 [第1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[第2の観点]等。

✓ 影響度が大きいリスクにつながり得る脅威の例

- WMS、WCSに対する不正アクセス、サービス不能、マルウェア感染に加えて、操作用端末及び保守用端末に対するデータの改ざん、サービス不能、不正アクセス、マルウェア感染が、影響度が大きいリスクにつながり得る脅威の例と考えられる。



✓ 行うべきと考えられる対策の例

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(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	• 【第1の観点】様々なIoT機器を接続する際のセキュリティの確保 • 【第1の観点】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	• 【第1の観点】IoT機器・システムの十分な可能性の確保 • 【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

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(例)

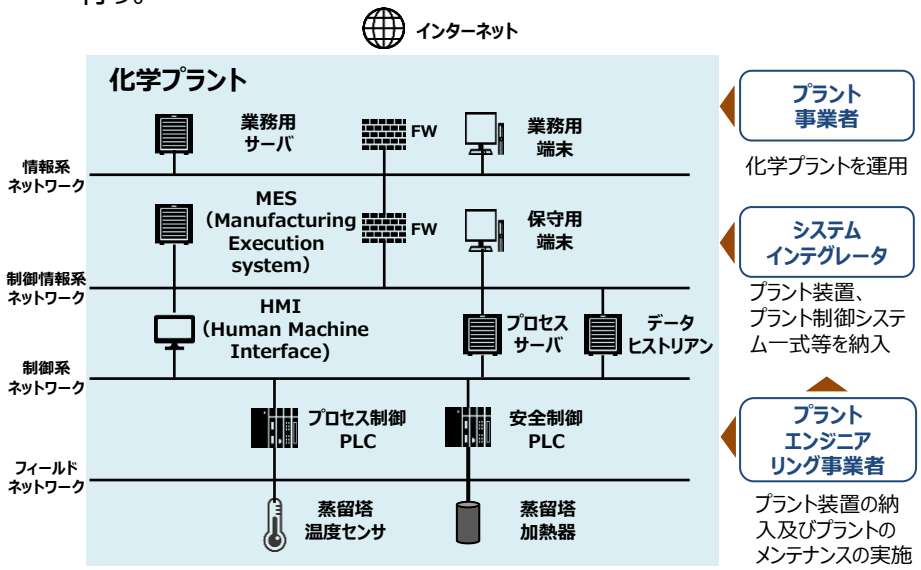
大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進	• 【第1の観点】運用前（設計・製造段階）における法令および契約上の要求事項の遵守 • 【第1の観点】セキュリティ設計と両立するセーフティ設計の仕様化
安全なアップデートプログラムの配信のための仕組みの構築	• 【第1の観点】IoT機器・システムに対するアップデートの適用

化学プラント施設内の蒸留工程の自動制御(2-3-4)

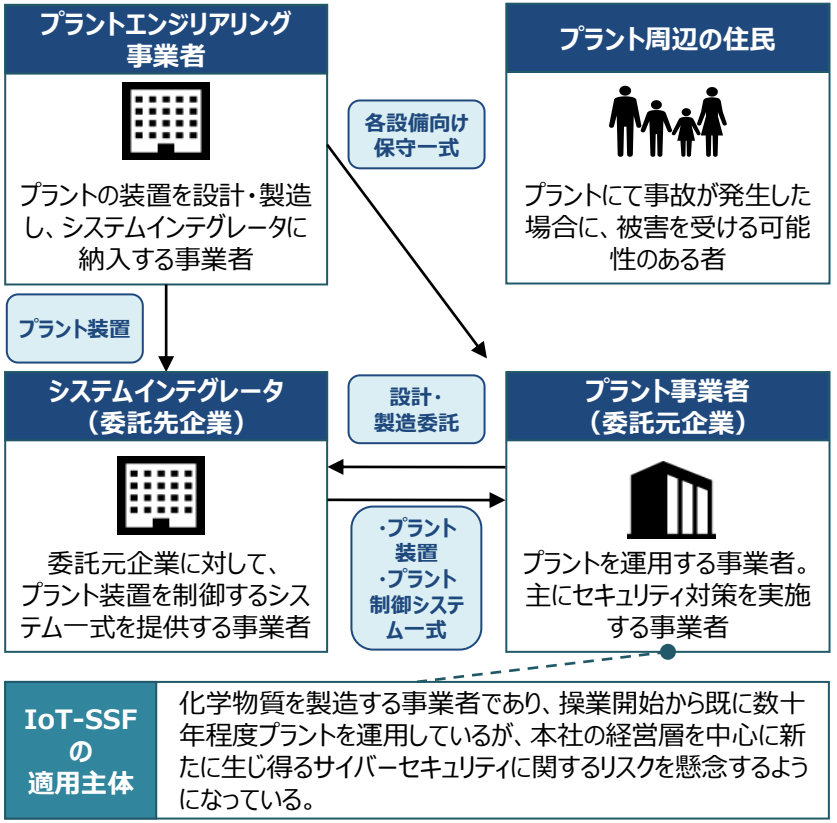
- プラント事業者がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- プラント事業者は、操業開始から既に数十年程度プラントを運用しており、既存のプラントシステムに対してリスクアセスメントを実施。

✓ 対象機器・システムの概要

- プラント事業者は、製造実行システム（MES）、HMI、プロセス制御PLC等からなるプラント制御システムを用いて、化学物質を製造するケースを想定する。
- 本社の経営層の指示により、プラント内のリスク管理部門が中心となって、対象機器・システムのセキュリティに関するリスクアセスメントを行う。



✓ 適用主体及び他のステークホルダーの情報



化学プラント施設内の蒸留工程の自動制御(2-3-4)

- 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。

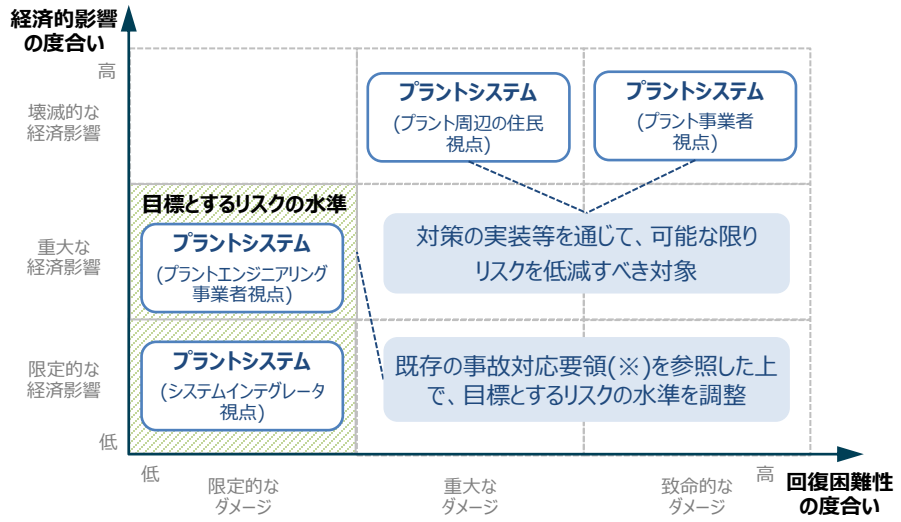
✓ 対象機器・システムにおいて想定されるリスク(例)

分類	想定されるリスク（例）
プラント事業者にとってのリスク	• MES等から、従業員や取引先担当者の**個人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感染に感染した上に、安全機能が適切に作動しないことで、**プラント設備が爆発し得る**。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**。（※）
プラント周辺の住民にとってのリスク	• プラント制御システムがマルウェア感染に感染した上に、安全機能が適切に作動しないことで、プラント設備が爆発し、**プラント周辺の住民に健康被害が生じる得る。**また、**生活にも大きな支障をきたし得る**。
プラントエンジニアリング事業者にとってのリスク	• **自社環境が不正アクセス**され、配信前のアップデートを改ざんされることで、蒸留塔等の設備が停止し得る。その結果、**契約上の責任が問われ得る。**
システムインテグレータにとってのリスク	• 想定される**リスクは限定的**と考えられる。

※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。

✓ 想定されるリスク(例)のマッピング結果

- プラントエンジニアリング事業者及びシステムインテグレータ視点のプラントシステムが保有するリスクは、目標とするリスクの水準に収まっている。
- プラント事業者、プラント周辺の住民視点のプラントシステムの保有するリスクは、目標とする水準には収まっておらず、何らかの対処実施が望まれる。



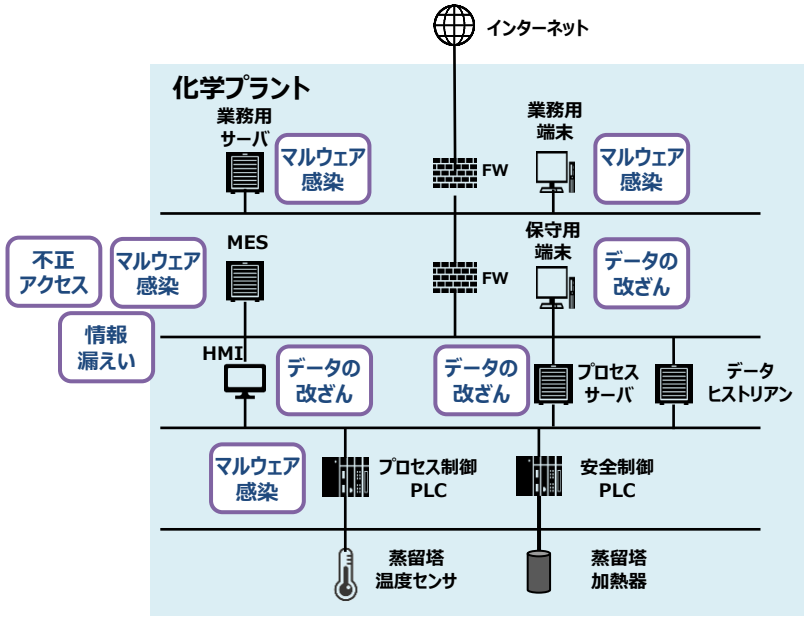
※本ユースケースでは、経済産業省「高圧ガス・石油コンビナート事故対応要領」を参照

化学プラント施設内の蒸留工程の自動制御(2-3-4)

- 影響度が大きいリスクにつながり得る脅威の例：MES、プロセス制御サーバに対するマルウェア感染、保守用端末、HMI、プロセスサーバに対するデータの改ざん等。
- 行うべきと考えられる対策の例：セキュリティ設計と両立するセーフティ設計の仕様化 [第1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[第2の観点]等。

✓ 影響度が大きいリスクにつながり得る脅威の例

- 業務用サーバ、業務用端末、MES、プロセス制御サーバに対するマルウェア感染に加えて、保守用端末、HMI、プロセスサーバに対するデータの改ざん、MESに対する情報漏えい、不正アクセスが影響度が大きいリスクにつながり得る脅威の例と考えられる。



✓ 行うべきと考えられる対策の例

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(例)

安全設備が事故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	• 【第1の観点】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	• 【第1の観点】様々なIoT機器を接続する際のセキュリティの確保 • 【第1の観点】適切なネットワークの分離 • 【第1の観点】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	• 【第1の観点】IoT機器・システムの十分な可用性の確保 • 【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 • 【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

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(例)

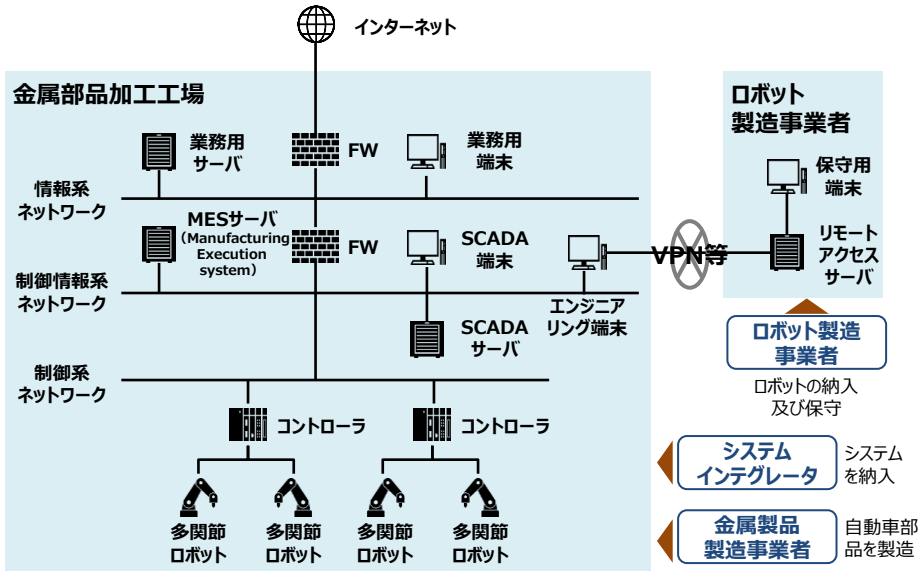
セキュリティに関するインシデントが発生したとしても周辺環境への影響を最小限に抑える仕組みの構築	• 【第1の観点】セキュリティ設計と両立するセーフティ設計の仕様化 • 【第2の観点】運用中における法令および契約上の要求事項の遵守

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(2-3-5)

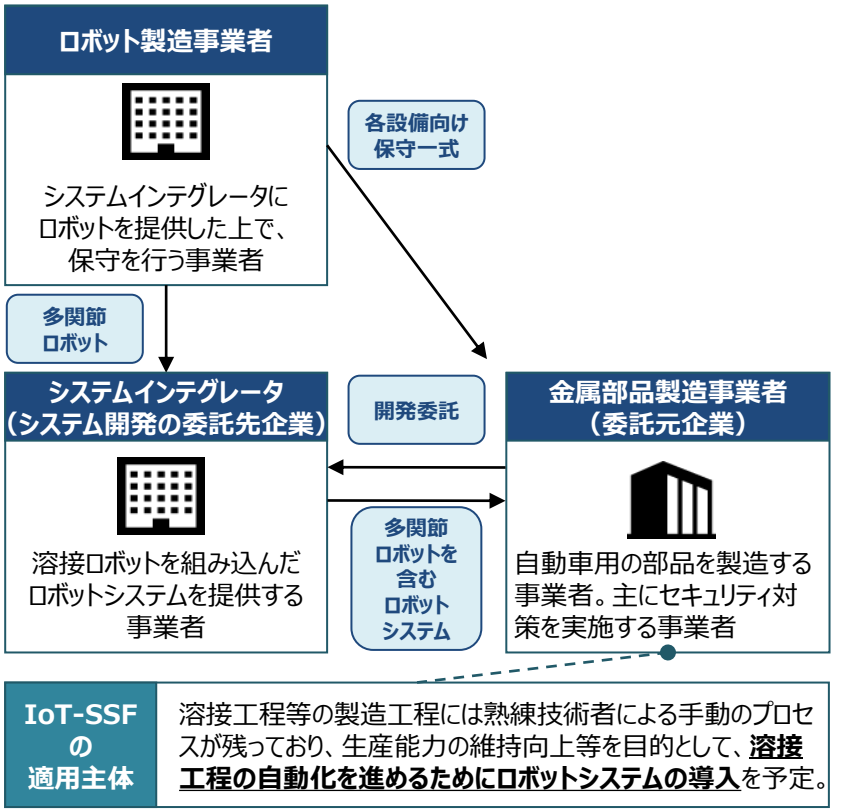
- 金属部品製造事業者がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- 輸送機器メーカ向けに事業を行う金属部品製造事業者は、品質の確保や生産能力の向上、人材不足の解決を目的として、複数の多関節ロボットを含むロボットシステムを導入。

✓ 対象機器・システムの概要

- 輸送機器メーカ向けに事業を行う金属部品製造事業者は、複数の多関節ロボットを含むロボットシステムを導入する。
- ロボットが稼働するエリアには、労働安全衛生を確保する観点から安全柵やレーザースキャナを設置し、作業員の不用意な立ち入りや不測の事故が発生することを防止する。



✓ 適用主体及び他のステークホルダーの情報



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(2-3-5)

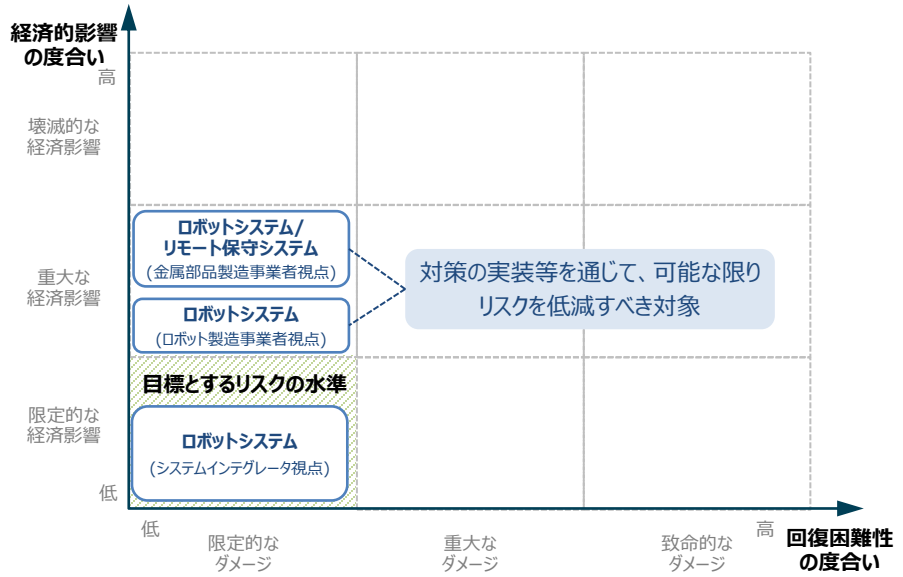
- 自社が管理するシステムだけでなく、リモート保守システムにおけるセキュリティインシデントによってもロボットシステムに影響が及び得るため、IoT-SSFの適用主体である「金属部品製造事業者」は、ロボットシステムに加えてリモート保守システムに対しても対策を具備させる必要がある。

✓ 対象機器・システムにおいて想定されるリスク(例)

分類	想定されるリスク（例）
金属部品製造事業者にとってのリスク	• MESサーバやSCADAサーバが**マルウェアに感染する**ことで、**生産活動が一時停止する**。
システムインテグレータにとってのリスク	• 想定される**リスクは限定的**と考えられる。
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し、製品回収が生じ得る。**

✓ 想定されるリスク(例)のマッピング結果

- 金属部品製造事業者視点のロボットシステム及びリモート保守システムの保有するリスク、ロボット製造事業者視点のロボットシステムの保有するリスクは、目標とする水準には収まっておらず、何らかの対処実施が望まれる。

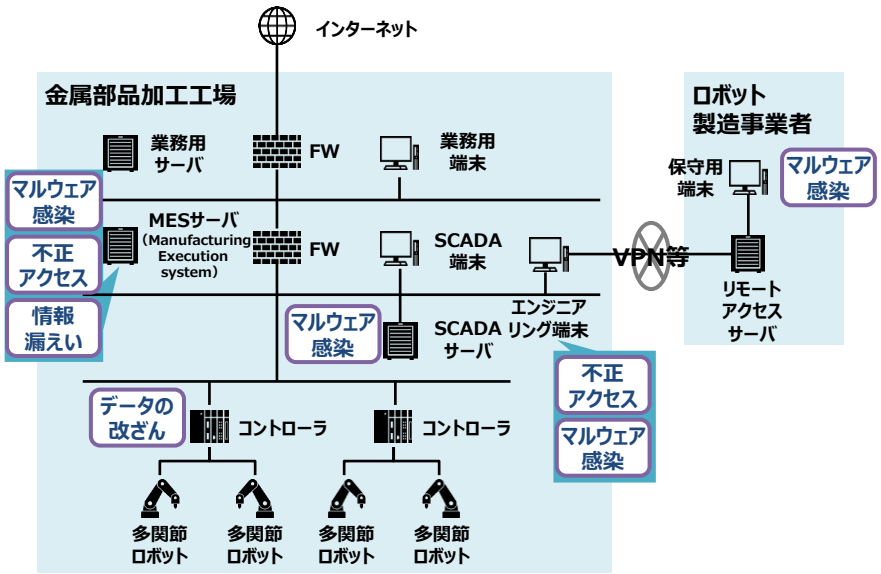


工場内のロボットによる部材加工作業（溶接工程）の自動化(2-3-5)

- 影響度が大きいリスクにつながり得る脅威の例：MESサーバに対する不正アクセス、情報漏えい、マルウェア感染及びSCADAサーバに対するマルウェア感染等。
- 行うべきと考えられる対策の例：適切な水準のアクセス制御の実装[第1の観点]、IoT機器・システムに対するアップデートの適用[第2の観点]等。

✓ 影響度が大きいリスクにつながり得る脅威の例

- MESサーバに対する不正アクセス、情報漏えい、マルウェア感染に加えて、SCADAサーバに対するマルウェア感染、エンジニアリング端末に対する不正アクセス、マルウェア感染等が、影響度が大きいリスクにつながり得る脅威の例と考えられる。



✓ 行うべきと考えられる対策の例

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(例)

ロボットの制御に関わる設備の保護	• 【第1の観点】適切な水準のアクセス制御の実装 • 【第1の観点】ソフトウェアのインストールの制限 • 【第1の観点】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	• 【第1の観点】適切な水準のアクセス制御の実装 • 【第1の観点】IoT 機器・システムの適正な運用・保守 • 【第1の観点】暗号化によるデータの保護 • 【第1の観点】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(例)

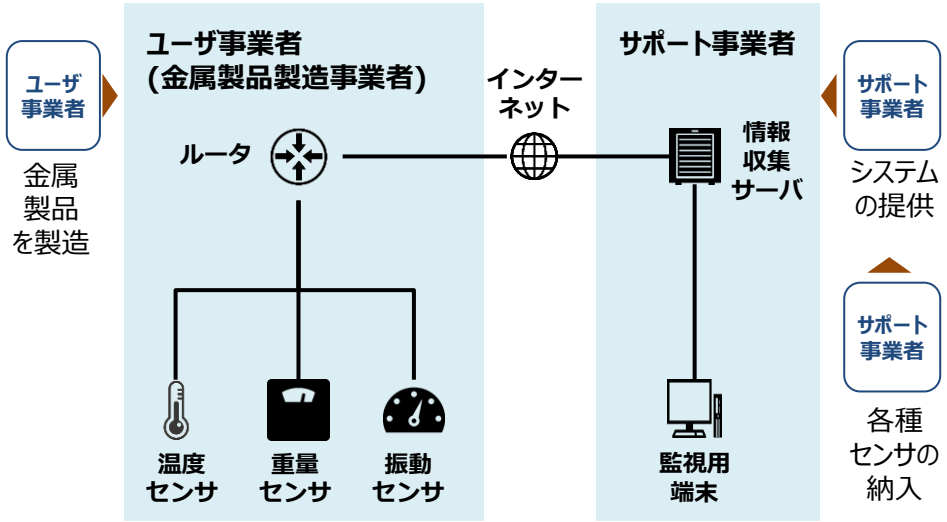
セキュアなロボット及び周辺機器の調達/提供	• 【第1の観点】企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
十分な期間のサポート契約締結	• 【第2の観点】IoT機器・システムに対するアップデートの適用

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(2-3-6)

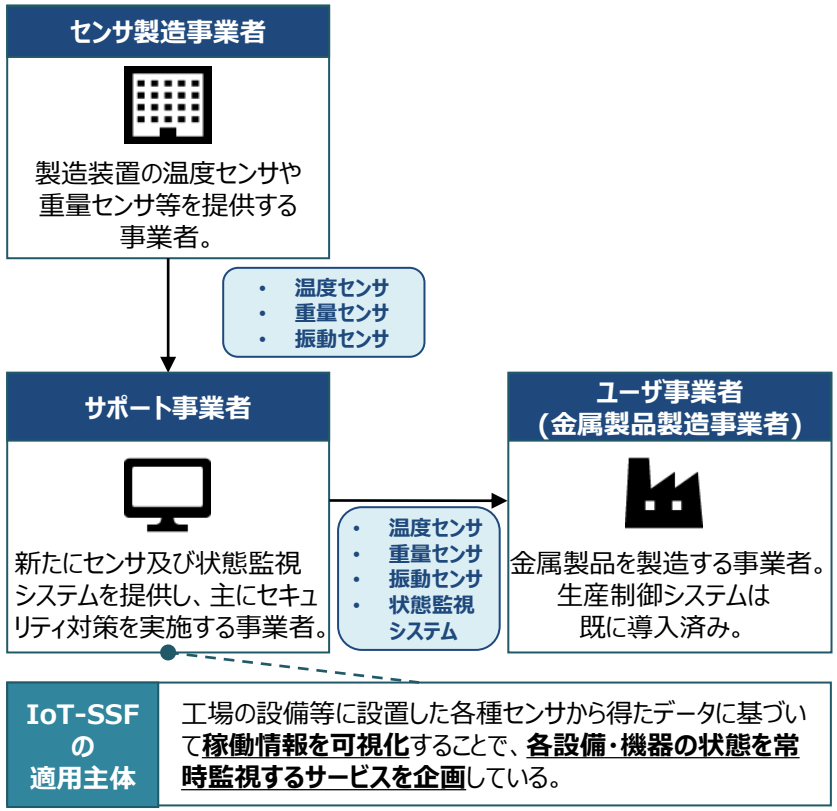
- サポート事業者がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- サポート事業者は工場の各設備に設置された各種IoT機器を通じて、稼働情報等を常時収集するとともに、収集した情報が適切な範囲に収まっているかを示すレポートを提供。

✓ 対象機器・システムの概要

- サポート事業者は、各設備に設置された各種IoT機器を通じて、稼働情報等を常時収集するとともに、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。



✓ 適用主体及び他のステークホルダーの情報



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(2-3-6)

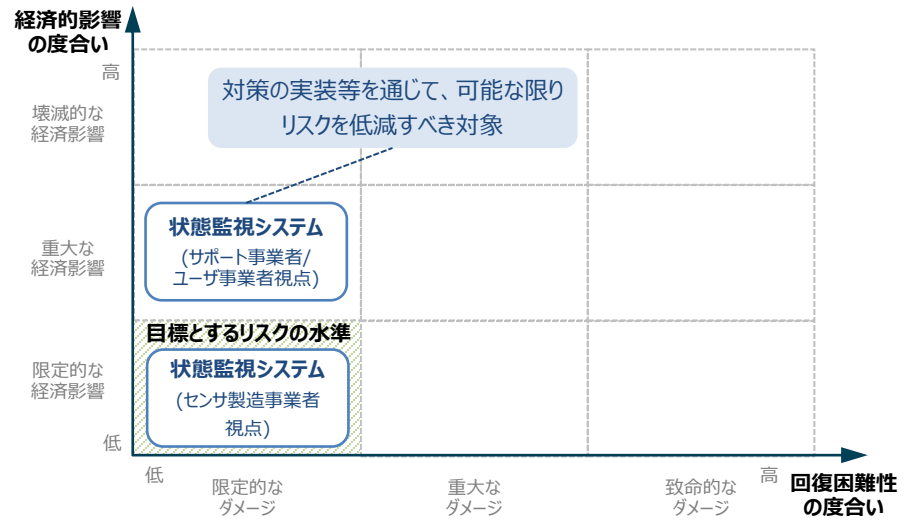
- IoT機器によって稼働情報を可視化しクラウド上でデータを管理する場合に、クラウドサーバから「ユーザ事業者」の営業秘密が外部へ流出する可能性が生じるため、IoT-SSFの適用主体である「サポート事業者」は、これらのリスクを踏まえて対策を実装することが望ましい。

✓ 対象機器・システムにおいて想定されるリスク(例)

分類	想定されるリスク（例）
サポート事業者にとってのリスク	• 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がマルウェアに感染することで、**情報収集サーバの一部機能が停止し得る**。
ユーザ事業者（金属製品製造事業者）にとってのリスク	• 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が不正アクセスされることで、**営業秘密が流出し得る。**
センサ製造事業者にとってのリスク	• 想定される**リスクは限定的**と考えられる。

✓ 想定されるリスク(例)のマッピング結果

- サポート事業者及びユーザ事業者視点の状態監視システムの保有するリスクは、目標とする水準には収まっておらず、何らかの対処実施が望まれる。

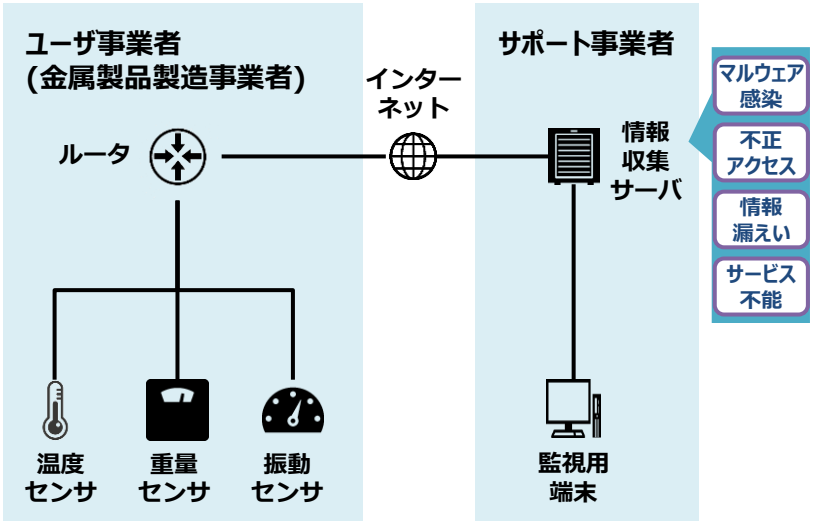


金属製造現場の温度センサ等による製造設備の状態監視(2-3-6)

- 影響度が大きいリスクにつながり得る脅威の例：情報収集サーバに対するマルウェア感染、不正アクセス、情報漏えい及びサービス不能等。
- 行うべきと考えられる対策の例：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[第1の観点] 等。

✓ 影響度が大きいリスクにつながり得る脅威の例

- 情報収集サーバに対するマルウェア感染、不正アクセス、情報漏えい及びサービス不能が、影響度が大きいリスクにつながり得る脅威の例と考えられる。



✓ 行うべきと考えられる対策の例

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(例)

稼働情報の漏えいを防ぐ仕組みの構築	• 【第1の観点】適切な水準のアクセス制御の実装 • 【第1の観点】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	• 【第1の観点】IoT機器・システムの十分な可用性の確保 • 【第1の観点】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対応を要請する対策(例)

稼働情報の漏えいを防ぐ仕組みの構築	• 【第1の観点】適切な水準のアクセス制御の実装 • 【第1の観点】暗号化によるデータの保護

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（CPSF）とその実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に向けた諸外国の検討状況

4. 本タスクフォースにおける検討
   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
   4. 今後の課題

今後の課題と対応の方向性（イメージ）

● IoT-SSF及びユースケースの普及啓発

➢ 経産省主催の研修会の開催、その他既存の枠組みの活用

例）地域における勉強会やコラボレーションプラットフォームやSC3等の枠組みを活用した周知　等

➢ 当TFに関係する企業・団体における活用

例）委員が所属する企業・団体における活用や所属する業界での横展開　等

➢ その他関係機関の巻き込み

例）２層に関わりの深い関係省庁や関係業界団体への提案　等

● 自立的な活用に向けた検討

➢ IoT-SSF、ユースケースを活用したビジネス化の促進

例）ソリューションベンダや保険会社等によるIoT-SSFを活用したリスクの見える化からソリューションの提供までを
パッケージとしたビジネスモデルの構築　等

➢ 支援機関への落とし込み

例）中小企業によるIoT機器・システム導入に係る相談に対するIoT-SSFの活用に向けた支援機関の体制整備　等

➢ IoT-SSF及びユースケースを使いこなせる人材の育成

例）各種教育プログラム・教材への落としこみによるIoT-SSFを使いこなせる人材の育成　等

➢ インセンティブの制度検討

例）IoT機器・システム導入に係る補助金等の支援制度における活用
（IoT-SSFに基づくユースケースの作成を加点要素や申請要件とする　等）