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 (簡易版)

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

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。

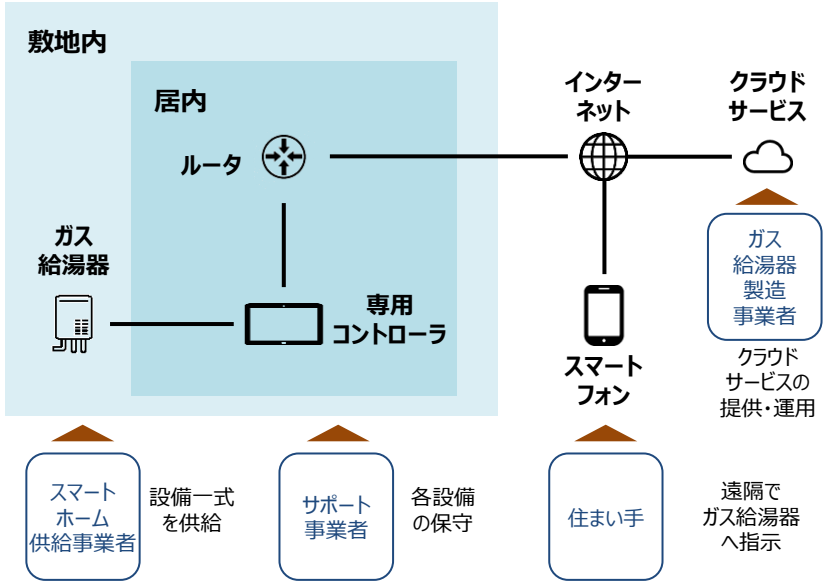
No	利用者の区分	利用環境	ユースケース	想定する適用主体	具体的な選定理由
2-3-1	個人又は家庭	家庭	**家庭用ガス給湯器の遠隔操作**	IoTサービス開発者、IoTサービス提供者(ガス給湯器製造事業者)	• 家庭用ガス給湯器は現状多くの住宅等に備えられており、その遠隔操作についても、今後利用の拡大が見込まれるため • インシデントが利用者の負傷につながりやすく、セーフティの側面がより重要となるケースであるため
2-3-2		公共空間	**ドローンを活用した個人による写真撮影**	IoTサービス開発者、IoTサービス提供者(ドローン機器事業者)	• ドローンは多種多様な活用方法が想定される機器であり、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

家庭用ガス給湯器の遠隔操作(2-3-1)

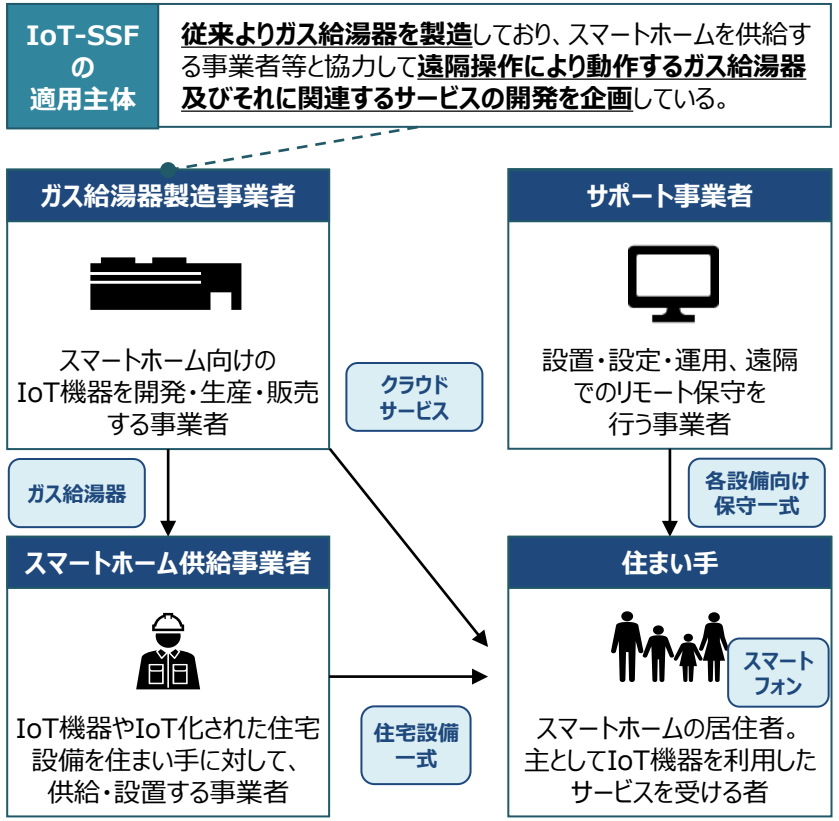
- スマートホーム向けIoT機器・サービスの事業者（ガス給湯器の製造元）がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- 住まい手が外出先よりスマートフォン用アプリを通じて、居内のガス給湯器を遠隔操作。

✓ 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。

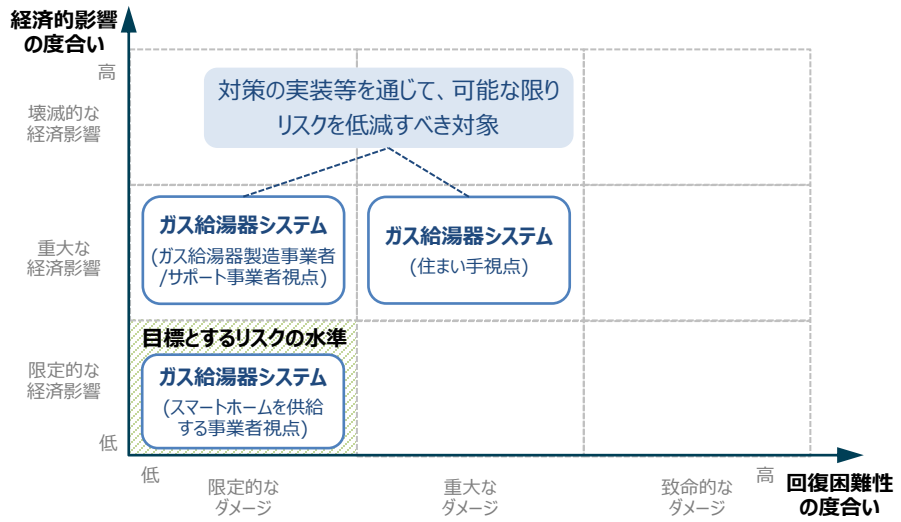
✓ 対象機器・システムにおいて想定されるリスク(例)

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	• 住まい手に対する注意喚起(例：利用方法の説明等)を怠ったために、過失が認められ得る。(※)

※その結果として、契約上の責任が問われ得る。

✓ 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。

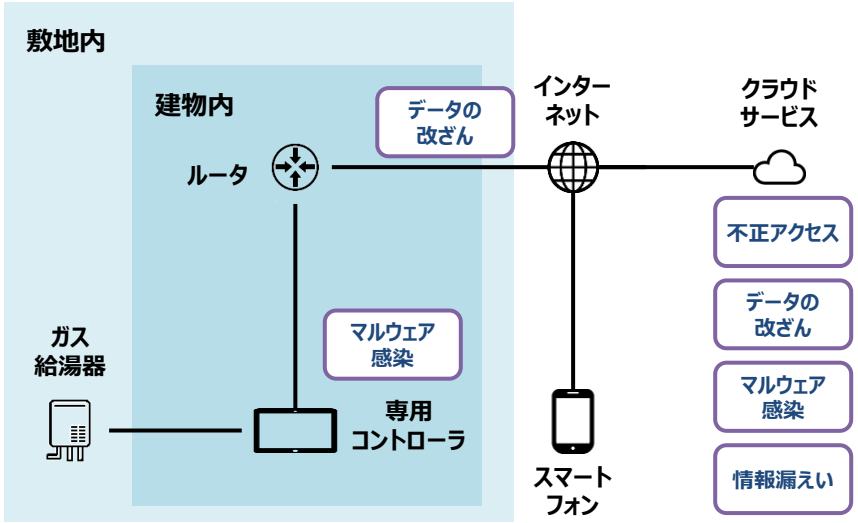


家庭用ガス給湯器の遠隔操作(2-3-1)

- 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・デザインの取組の推進	• 【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　等
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	• 【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 • 【第3の観点】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　等

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】IoT機器・システムに対するアップデートの適用　等

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

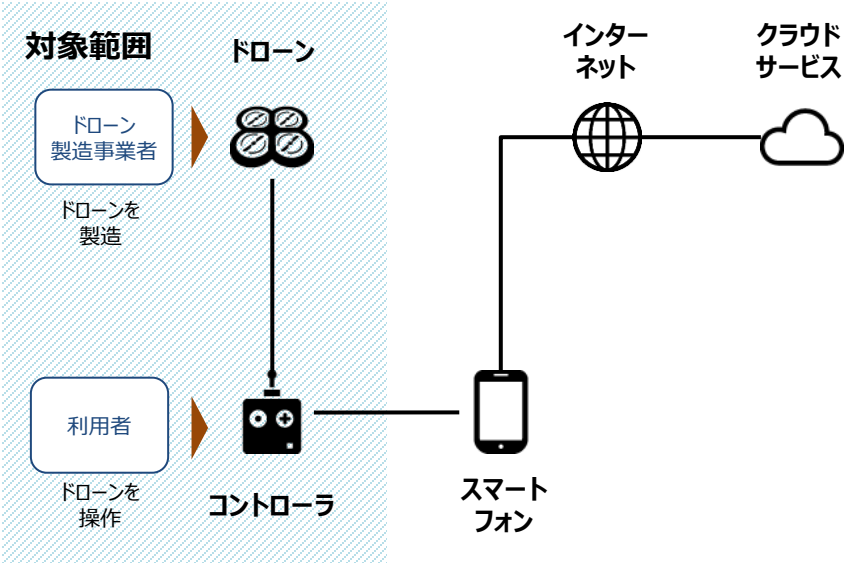
※セキュリティインシデントによっては、ガス給湯器製造事業者はガス供給事業者と連携して対応することが必要となる場合がある。

ドローンを活用した個人による写真撮影(2-3-2)

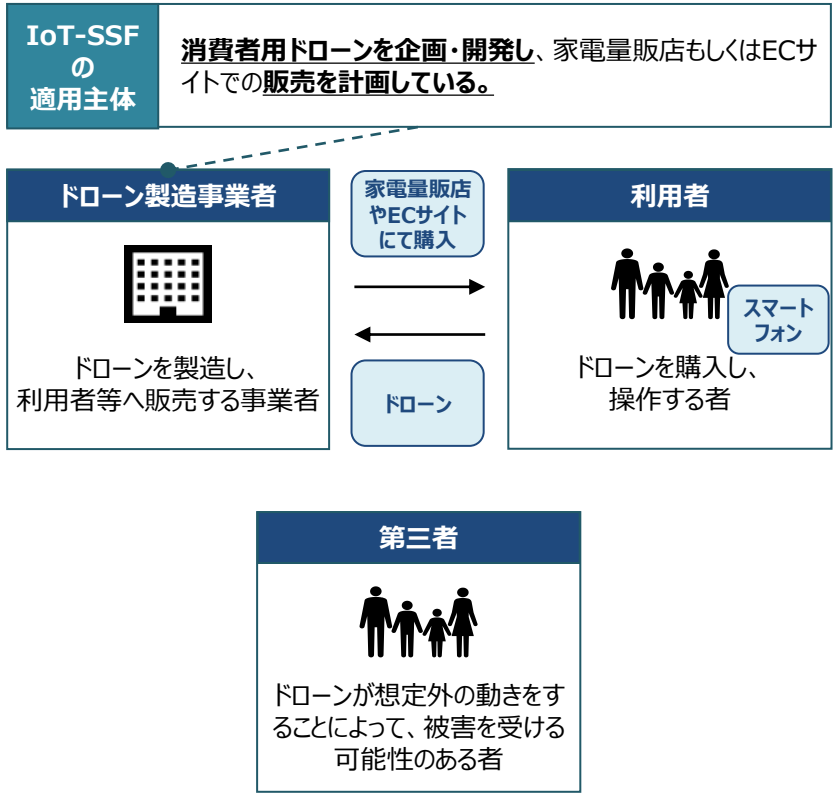
- ドローン製造事業者がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- 利用者はスマートフォンに接続されたコントローラにてドローンを操作し、ドローンに設置されたカメラで風景を撮影。

✓ 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)

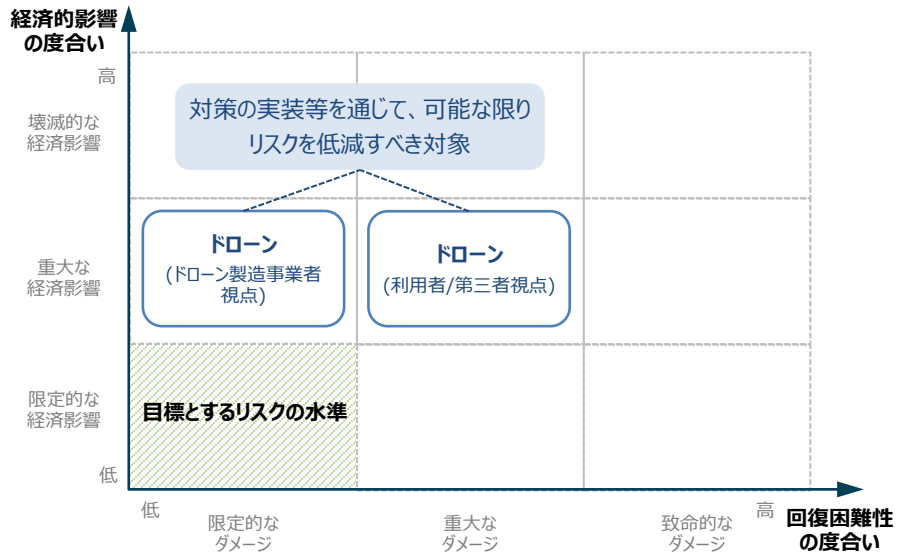
- セキュリティインシデントによってドローンの航行に影響が及んだ場合、周辺の第三者や住宅等の環境へ影響を及ぼし得ることから、 IoT-SSFの適用主体である「ドローン製造事業者」は、「利用者」に加えて「第三者」が被り得るリスクを考慮して対策を実装する必要がある。

✓ 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。

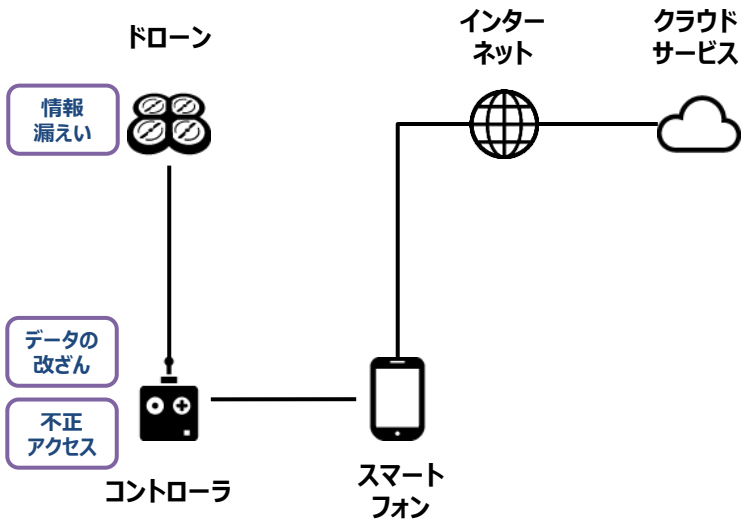


ドローンを活用した個人による写真撮影(2-3-2)

- 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・デザインの取組の推進	• 【第1の観点】運用前（設計・製造段階）における法令及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)

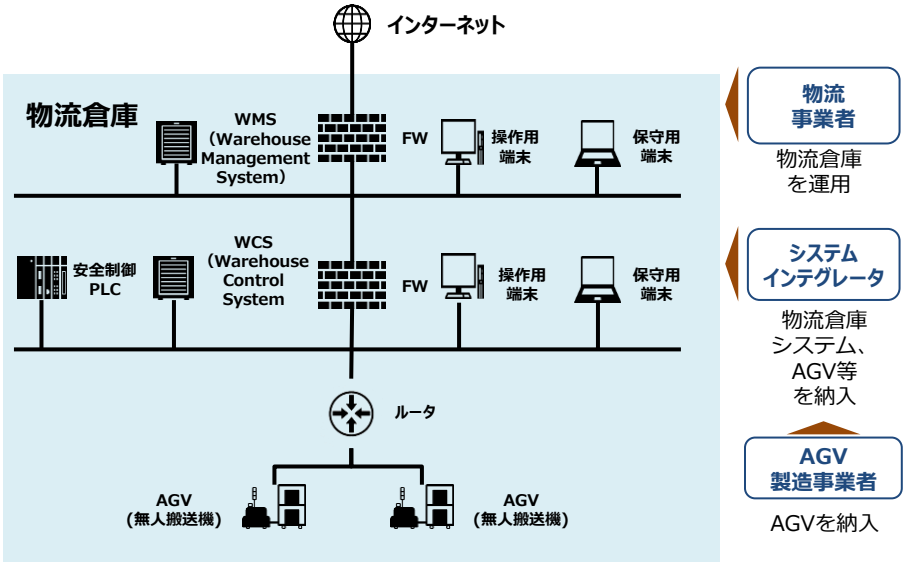
利用者への注意喚起の実施や推奨事項の明確化	• 【第2の観点】利用者へのリスクの周知等の情報発信 • 【第2の観点】IoT機器・システムの適正な使用 • 【第3の観点】IoT機器・システムの運用・管理を行う者への要求事項の特定
フェールセーフ等を含む安全対策の徹底	• 【第1の観点】セキュリティ設計と両立するセーフティ設計の仕様化

物流倉庫内のAGVによる自動ピッキング(2-3-3)

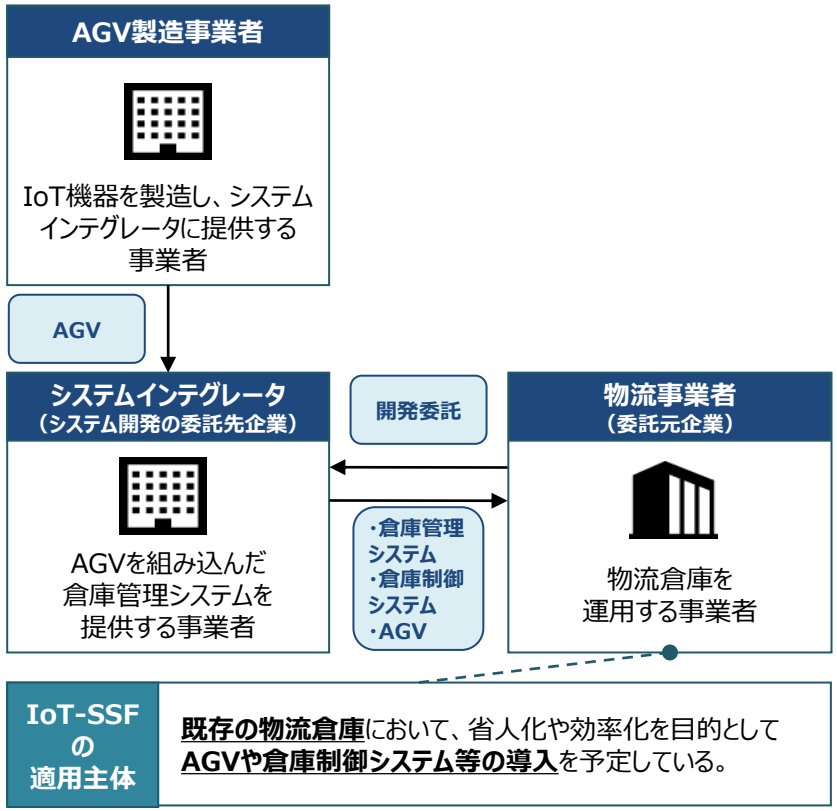
- 物流事業者がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- 当該事業者は、事業規模拡大に伴って既存の物流倉庫において、省人化や効率化を目的として新たにAGVや倉庫制御システム等の導入を予定。

✓ 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。

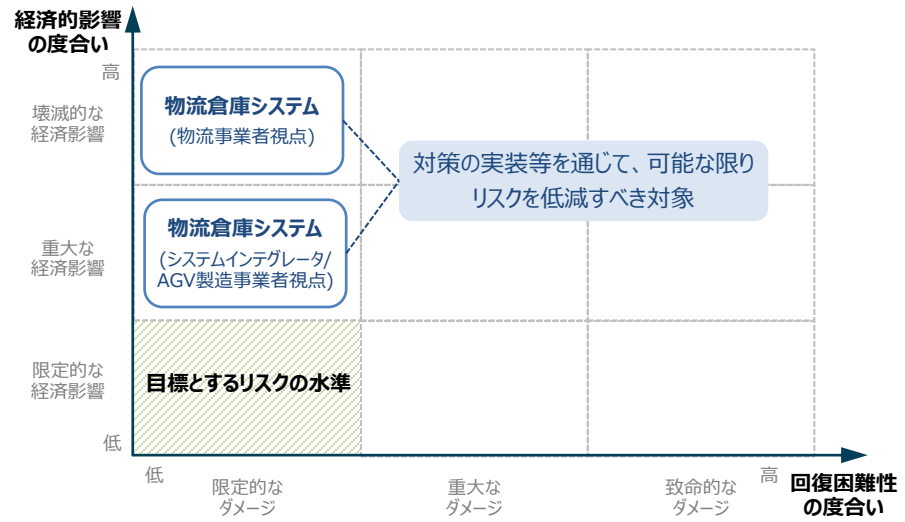
✓ 対象機器・システムにおいて想定されるリスク(例)

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。

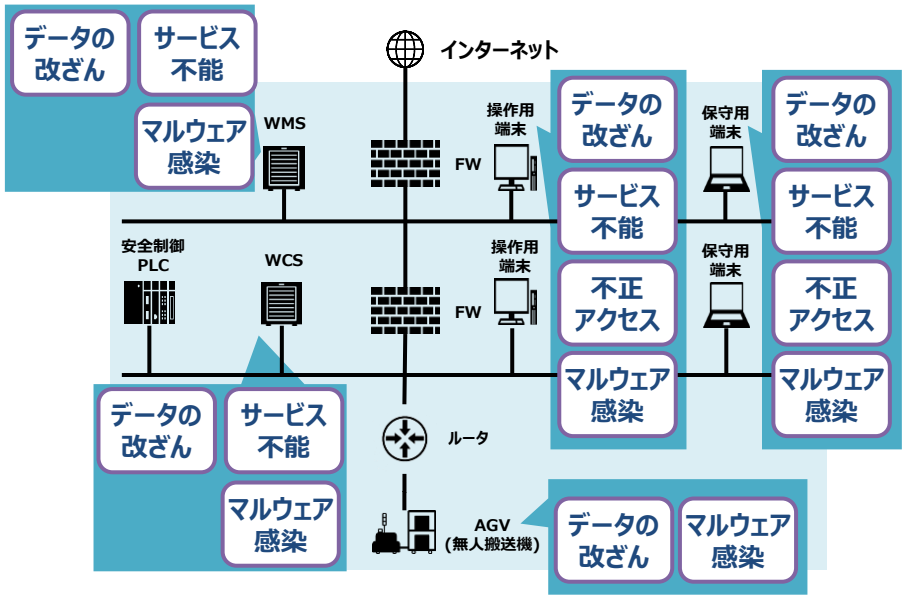


物流倉庫内のAGVによる自動ピッキング(2-3-3)

- 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)

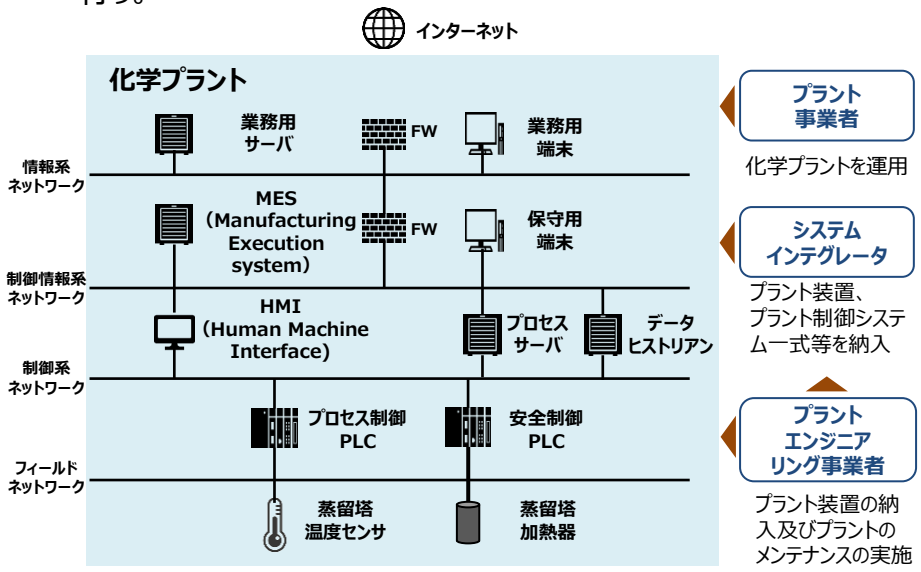
大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組の推進	• 【第1の観点】運用前（設計・製造段階）における法令及び契約上の要求事項の遵守 • 【第1の観点】セキュリティ設計と両立するセーフティ設計の仕様化
安全なアップデートプログラムの配信のための仕組みの構築	• 【第1の観点】IoT機器・システムに対するアップデートの適用

化学プラント施設内の蒸留工程の自動制御(2-3-4)

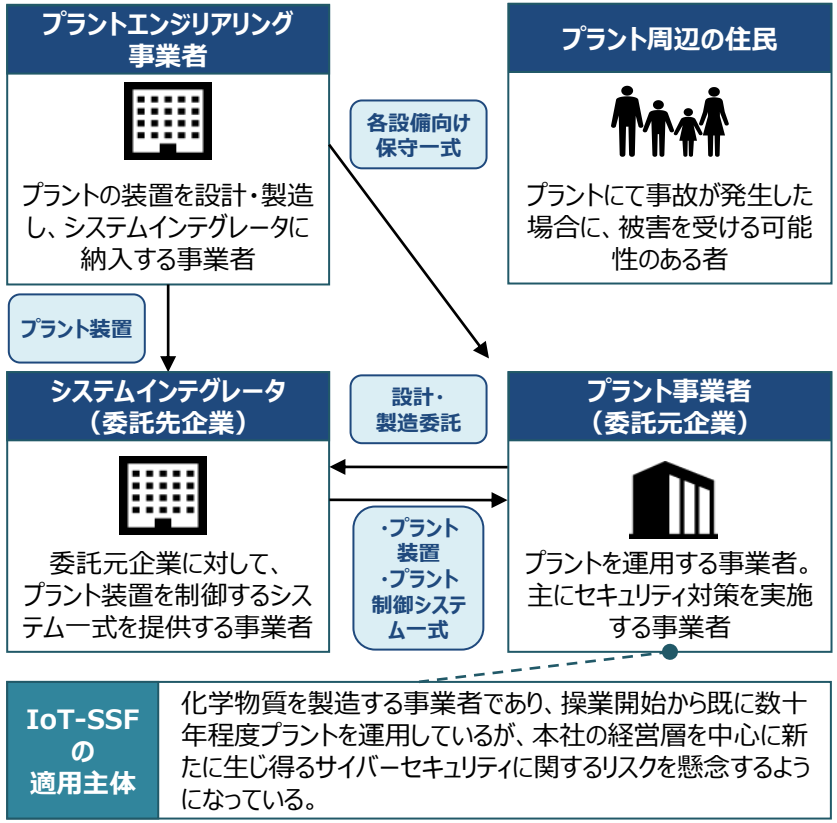
- プラント事業者がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- プラント事業者は、操業開始から既に数十年程度プラントを運用しており、既存のプラントシステムに対してリスクアセスメントを実施。

✓ 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。

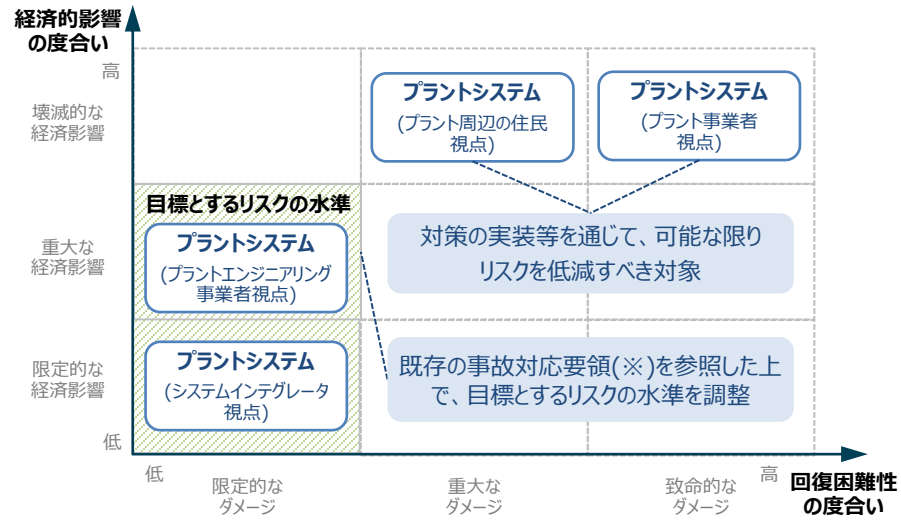
✓ 対象機器・システムにおいて想定されるリスク(例)

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**。（※1）
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。**（※2）
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)を怠ったために、過失が認められ得る。(※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、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。
※3その結果として、契約上の責任が問われ得る。

✓ 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。



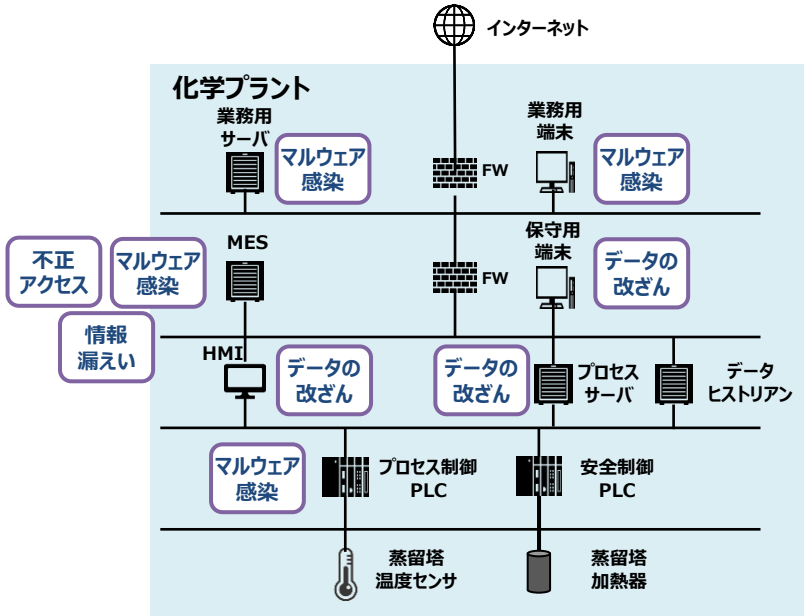
※本ユースケースでは、経済産業省「高圧ガス・石油コンビナート事故対応要領」を参照

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)

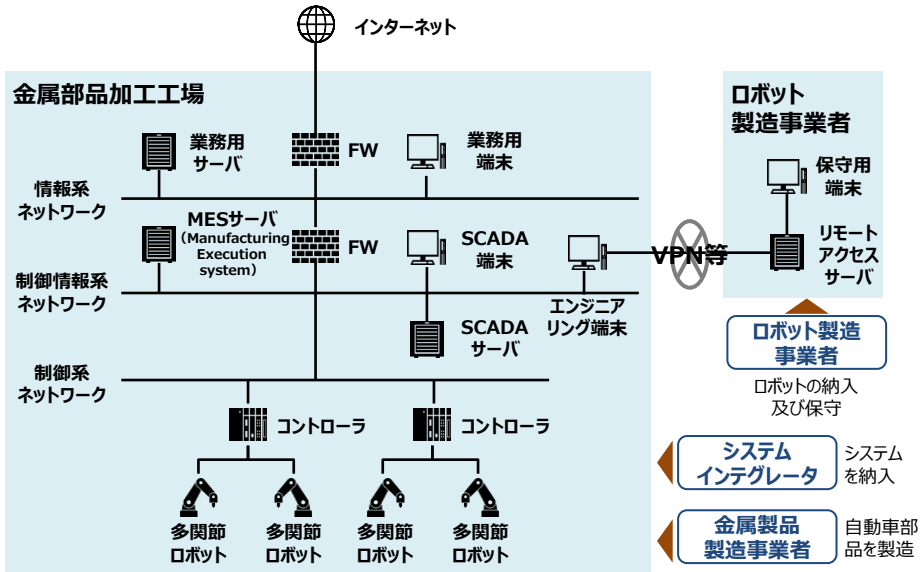
セキュリティに関するインシデントが発生したとしても周辺環境への影響を最小限に抑える仕組みの構築	• 【第1の観点】セキュリティ設計と両立するセーフティ設計の仕様化 • 【第2の観点】運用中における法令及び契約上の要求事項の遵守

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)

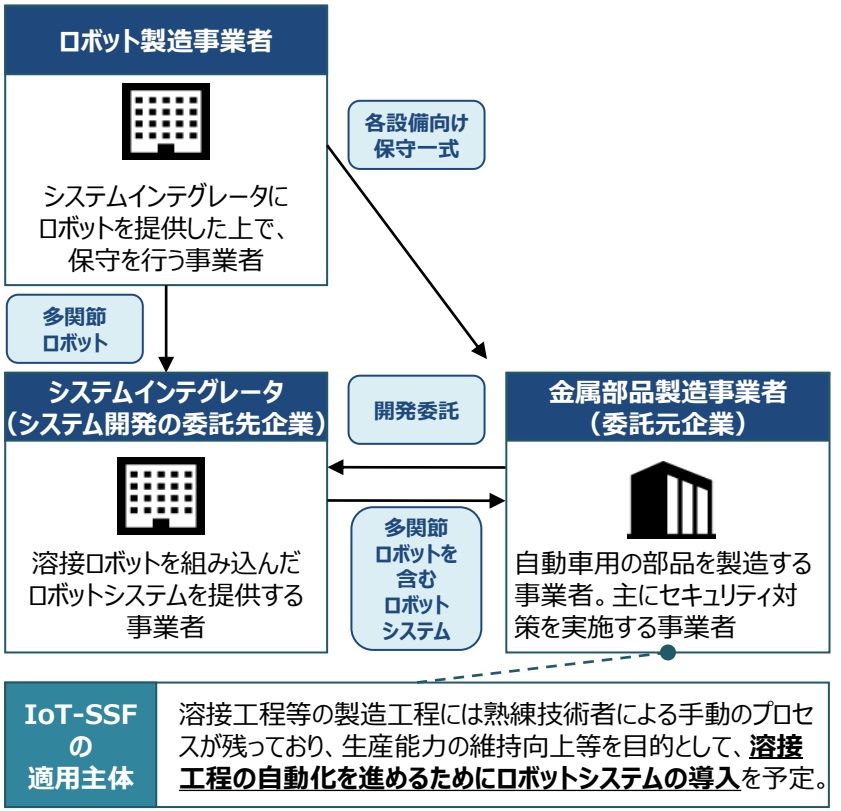
- 金属部品製造事業者がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- 輸送機器メーカ向けに事業を行う金属部品製造事業者は、品質の確保や生産能力の向上、人材不足の解決を目的として、複数の多関節ロボットを含むロボットシステムを導入。

✓ 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。

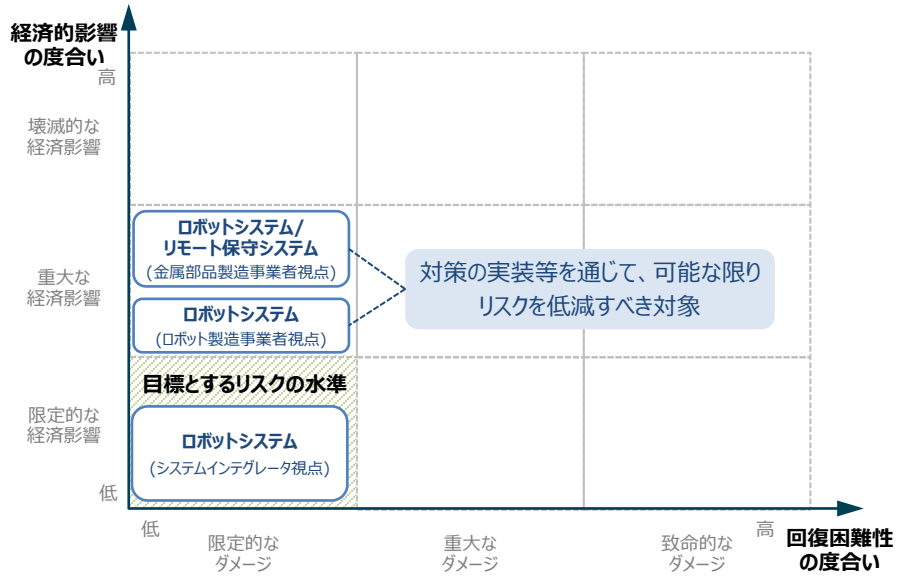
✓ 対象機器・システムにおいて想定されるリスク(例)

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	• 金属部品製造事業者に対する注意喚起(例：設定方法に関する説明等)を怠ったために、過失が認められ得る。(※)
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。**

※その結果として、契約上の責任が問われ得る。

✓ 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。

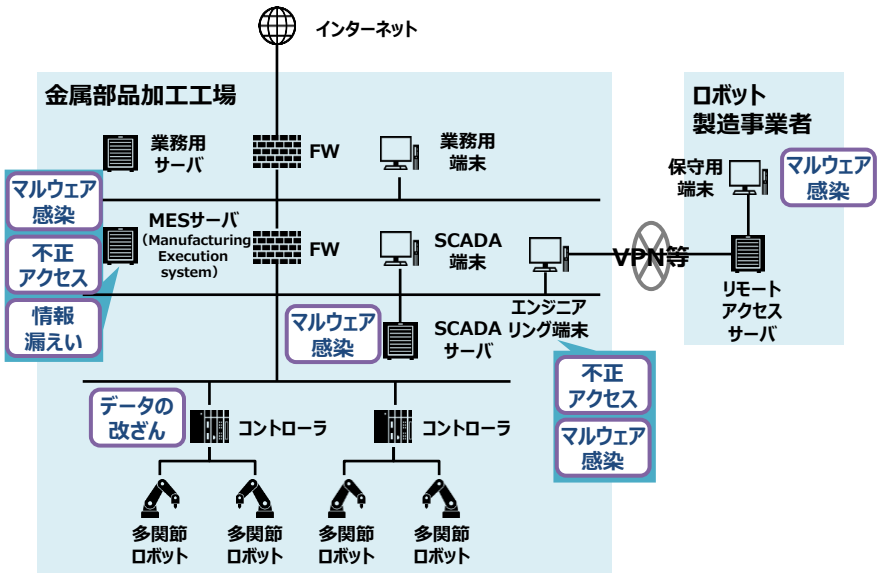


工場内のロボットによる部材加工作業（溶接工程）の自動化(2-3-5)

- 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)

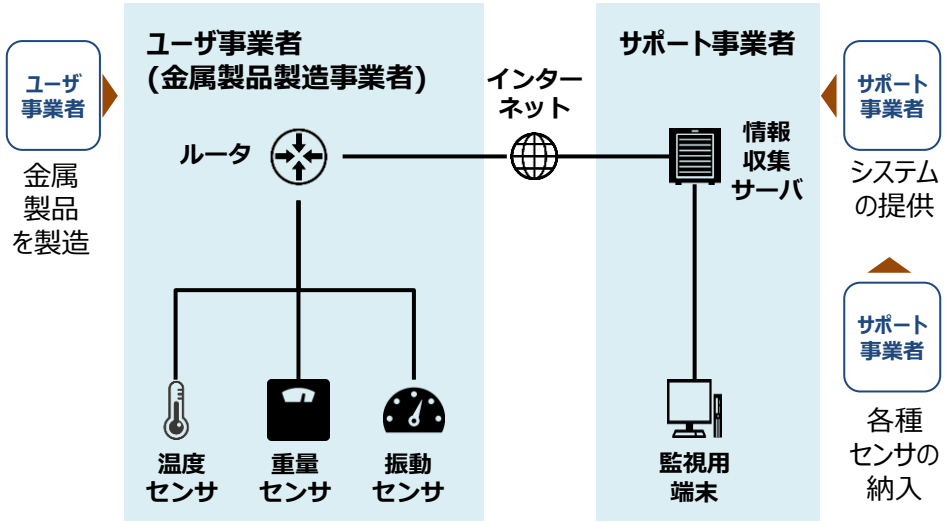
セキュアなロボット及び周辺機器の調達/提供	• 【第1の観点】企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
十分な期間のサポート契約締結	• 【第2の観点】IoT機器・システムに対するアップデートの適用

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)

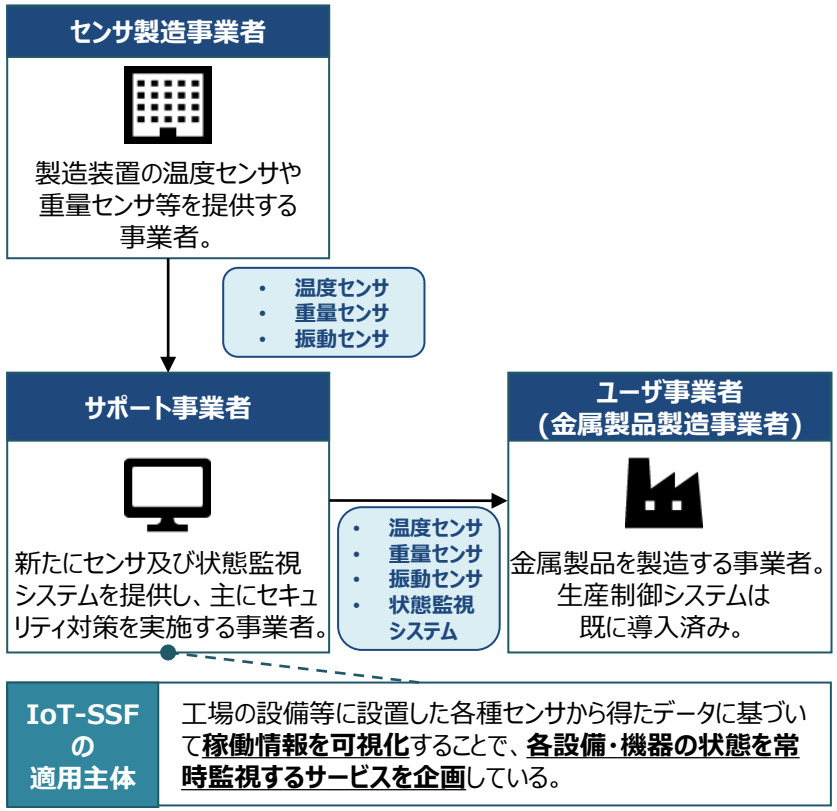
- サポート事業者がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- サポート事業者は工場の各設備に設置された各種IoT機器を通じて、稼働情報等を常時収集するとともに、収集した情報が適切な範囲に収まっているかを示すレポートを提供。

✓ 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。

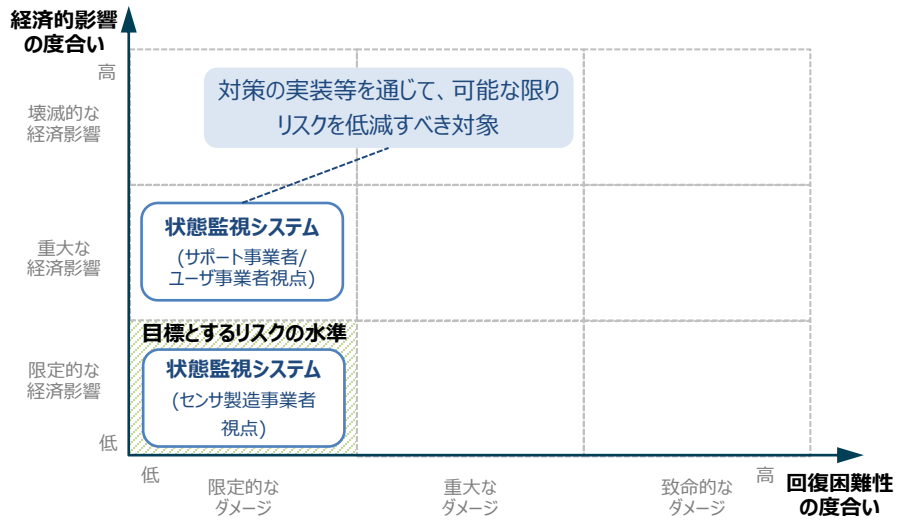
✓ 対象機器・システムにおいて想定されるリスク(例)

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	• インターネット又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	• インターネット又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	• サポート事業者に対する注意喚起(例：設定方法に関する説明等)を怠ったために、過失が認められ得る。(※)

※その結果として、契約上の責任が問われ得る。

✓ 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。

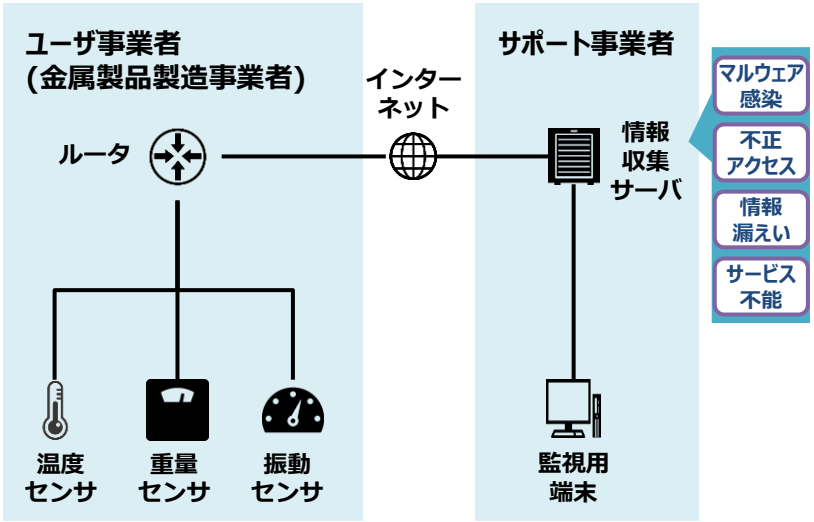


金属製造現場の温度センサ等による製造設備の状態監視(2-3-6)

- 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