資料４

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(仮題)

目次

1. 本文書の位置づけと構成

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 セキュリティ・セーフティ・フレームワーク」（以下、「IoT-SSF」という。）は、サイバー空間とフィジカル空間をつなぐ新たな仕組みによってもたらされる新たなリスクに着目し、リスク形態及びそうしたリスクに対応するセキュリティ・セーフティ対策の類型化の手法を提示するものである。

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にすることを目的として、IoT-SSF では 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している。

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ものである。

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。本稿にて詳述するユースケースは、以下に示す通りである。

- 家庭用ガス給湯器の遠隔操作 (2-3-1)
- ドローンを活用した個人による写真撮影 (2-3-2)
- 物流倉庫内の AGV[1]による自動ピッキング (2-3-3)
- 化学プラント施設内の蒸留工程の自動制御 (2-3-4)
- 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)

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] AGV（Automatic Guided Vehicle）は、人間が運転操作を行わなくとも自動で走行可能な搬送車である。

1-3　想定読者と利用用途

・　本稿の具体的な想定読者と利用用途は以下に示す通りである。なお、想定読者のうち、本稿は主に 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・システム及び関連サービスの利用を計画したり、現に利用しているものの状況をレビューしたりする際に、セキュリティやそれと関連するセーフティの観点で自身が考慮すべき事項や、IoT サービス提供事業者等に対応を依頼する事項を整理する参考として本稿を参照することができる。

・　**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）**

自社製品として IoT 機器・システムまたは関連サービスを企画・設計する際、あるいはそのような機器・システムの設計や開発に係る委託を他社から受けた際に、対象機器・システムの運用開始より以前にセキュリティやそれと関連するセーフティの観点で考慮すべき事項や、IoT 利用者や関連事業者（例：業務委託先）等に対応を依頼する事項を整理する参考として本稿を参照することができる。

・　**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・システムまたは関連サービス[2]を、新たに IoT 利用者に提供する際、あるいは既に提供しているものをレビューし、品質等の改善を図ろうとする際に、対象機器・システムの運用中または運用終了時にセキュリティやそれと関連するセーフティの観点で考慮すべき事項や、IoT 利用者や関連事業者（例：業務委託先）等に対応を依頼する事項を整理する参考として本稿を参照することができる。

・　**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**

IoT 機器・システムに関連するセキュリティ及びそれと関連するセーフティの観点から、今後より具体的な制度・環境を検討しようとする際の参考として本書を参照することができる。

[2] ここで、IoT サービス提供者に係る「IoT 機器・システムまたは関連サービス」には、利用者に提供されるサービスのみならず、それに付随して発生し得る役務（例：機器・システムの保守業務）の提供等が含まれ得る。

2. 「IoT セキュリティ・セーフティ・フレームワーク」実践に係るユースケース集

2-1 対象となるユースケース

IoT-SSF にて既に述べられているように、第 2 層におけるセキュリティ対策には、様々な IoT 機器・システムに共通する課題への対応だけでなく、利用者の区分や利用環境の多様性も十分に踏まえた対応が必要となる。全体としての網羅性を意識しつつ、想定読者が IoT 機器・システム（関連するサービスを含む）を提供または利用する際に、ユースケースがセキュリティ確保を目指した取組みの助けとなるよう、選定にあたっては以下の観点を考慮した。

- **IoT 機器・システムの利用者の区分**
  IoT 機器・システムの利用者の区分を、「個人または家庭」と、「事業者（主に産業）」に分類し、双方からユースケースを選定する。

- **利用環境の多様性**
  IoT 機器・システムが現に利用される環境には非常に多様なものが想定され得るが、本稿では、消費者用途として消費者現場（家庭、公共空間）、産業用途として製造現場と物流現場を取扱う。また、製造現場としては、網羅性を確保する観点から、原料製造（プラント）、製品製造（工場）という 2 つの業態からユースケースを選定する。

- **IoT 機器・システムの汎用性及び普及率の高さ**
  より幅広い読者にとって参考となるよう、選定する IoT 機器・システムは、利用や提供が特定の事業者等に限定されない汎用的なものであり、広く普及もしくはこれから普及が見込まれるものが望ましい。したがって、以下の 2 点を考慮してユースケースを選定する。
  - 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
  - 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

- **想定されるリスクと対策の多様性**
  各 IoT 機器・システムは上記の通り、利用者や利用環境が異なるため、使用上のリスクもそれぞれ異なる。加えて、想定されるリスクの差異は、優先的に講じるべき対策の差異にもつながる。読者にとって具体的な検討に参考となるよう IoT 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。

上記に示したユースケース選定の考え方を踏まえ、本稿では以下 6 件のユースケースを取扱う。

なお、IoT-SSF を参照した上で IoT 機器・システム及び関連サービスにおけるリスクマネジメントを実行する主体を IoT-SSF の「適用主体」と定めた上で、ユースケースごとにこれらを定めるものとする。

表 1 本稿で取扱うユースケースの一覧

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	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	・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	・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	・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）	工場における部材加工作業（溶接工程）の自動化	IoT 利用者	・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	・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、これらに関連するセキュリティ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

2-2 ユースケースにおける記載事項

前述したように、IoT-SSF は、IoT 機器・システムを対象に、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 つの軸を提示するものである。以下に示すリスクマネジメントの一般的なプロセスと関連付けて言うならば、提案されている 3 軸のうち、「第 1 軸：発生したインシデントの影響の回復困難性の度合い」（以下、「回復困難性の度合い」という。）と「第 2 軸：発生したインシデントの経済的影響の度合い」（以下、「経済的影響の度合い」という。）は「リスクアセスメント」において IoT 機器・システムに潜むリスクの整理に用いられるものであり、第 3 軸「求められるセキュリティ・セーフティ要求の観点」（以下、「求められるセキュリティ・セーフティ要求」という。）は「リスク対応」の方策をカテゴライズしたものと捉えることができる。

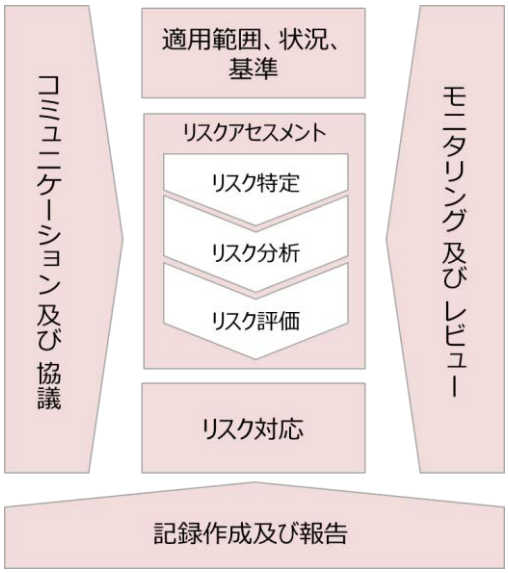


図 1 リスクマネジメントの一般的なプロセス[3]

CPSF では、上記プロセスを参照しつつ、国内外の関連文献の記載内容も加味して、「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」のステップでセキュリティリスクマネジメントの流れを整理している。

これらを踏まえ、本稿では、前述した 6 つの具体的なケースを対象に、以下のステップからなる一連のリスクマネジメントプロセスを取扱う[4]。

- リスクアセスメント、リスク対応に向けた事前準備[5]（2-2-1）
- リスクアセスメント（2-2-2）
- リスク対応（2-2-3）

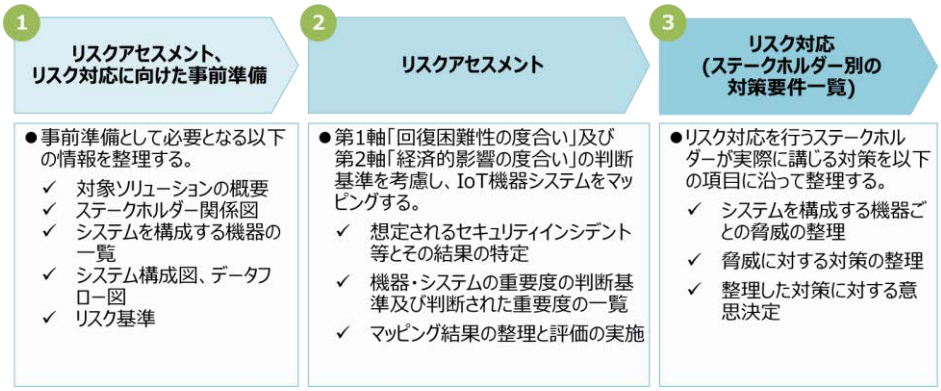


図 2 本稿におけるリスクマネジメントのステップ

[3] JIS Q 31000:2019 リスクマネジメント―原則及び指針を基に作成

[4] 「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」における事業被害レベル（セキュリティインシデントによりもたらされ得る被害の程度。）は、本稿では「第 1 軸：発生したインシデントの影響の回復困難性の度合い」と「第 2 軸：発生したインシデントの経済的影響の度合い」により評価される。

[5] JIS Q 31000:2019 における「適用範囲、状況、基準」に相当する内容を想定する。

また、想定読者に示した 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。具体的には、現場の担当者においてリスクマネジメントを行った場合、経営層に実施結果を共有した上で、必要に応じて内容を更新することが考えられる。

2-2-1 リスクアセスメント、リスク対応に向けた事前準備

IoT 機器・システムを対象にリスクアセスメント及びリスク対応を行う場合には、まず対象となる IoT 機器・システムの置かれている状況の整理ができていなければ、詳細で信頼性のあるリスクアセスメント及びリスク対応を行うことができない。したがって、事前準備として必要となる情報を整理するために、以下の内容を明確にする必要がある。

(1) 対象となる機器・システムの概要と目的

リスクアセスメント及びリスク対応の実施にあたり、対象となる IoT 機器・システム及び関連サービスの概要を特定する。その際、どのような目的で(why)、誰が(who)、何を(what)、いつ(when)、どこで(where)、どのように(how)利用するのかという点等を明確にすることが望ましい。

(2) ステークホルダー関連図

対象機器・システムの提供または利用における自身の役割と責任を特定する。IoT 機器・システムの提供または利用には、複数のステークホルダーが関与することが多いため、対象の機器・システムにおけるセキュリティ上のリスクを特定し対応する場合、自身に加えて、サプライヤや顧客のセキュリティ対策実装に係る役割や責任を考慮することが重要である。IoT 機器・システムの提供または利用に関連して、典型的には以下の役割が特定され得る。

- IoT サービス提供者:IoT 機器・システム及び関連するサービスの運用や管理に係る者
- IoT サービス開発者:IoT 機器・システム及び関連するサービスの設計や開発に係る者(システムインテグレータや IoT 機器の製造者、部品サプライヤを含む)
- IoT 利用者:IoT 機器・システム及び関連するサービスのエンドユーザ

(3) システムを構成する機器の一覧

リスク分析実施範囲内に存在する機器、及び分析に必要となるシステムを構成する機器の一覧を作成する。かかる一覧には、IoT の典型的な構成要素として、IoT 機器(センサ、アクチュエータ)、ネットワーク、ネットワーク機器(ルータ、IoT ゲートウェイ等)、サーバ等が含まれ得る。

(4) システム構成図、データフロー図

対象となる機器・システムの構成図やデータフロー図を特定する。論理構成を示すネットワーク構成図等を作成した後、分析用のシステム構成図及びデータフロー図を整理する。また、その際、各機器とそれらの操作や保守に係る組織やヒトとの関係性が明確化されていることが望ましい。本稿で示すユースケースでは、データフローのうち抜粋したデータフローを示す。

(5) リスク基準

機器・システムに関連する自身の目的に対して、受容できるリスク、または相対的に受容しがたいリ

スクの大きさ及び種類をリスク基準として特定する。リスク基準を検討する際、一般的には、セキュリティインシデントにより生じ得る被害の大きさや、セキュリティインシデントの起こりやすさ、対象となる資産の重要度等が考慮され得る。

本稿では、2-2-2 にて述べるように、セキュリティインシデントにより生じ得る被害の大きさという観点に着目し、かかる基準を、「目標とするリスクの水準」として、「回復困難性の度合い」と「経済的影響の度合い」に関連付けて整理する。特定されるリスク基準は、適用主体となる組織内部の上位のセキュリティやセーフティ等に関する基本方針や目標と整合したものとなっていることが望ましい。2-2-2 におけるアセスメントの結果をリスク基準と比較し、分析することを通じて、リスク対応を重点的に行う機器・システム等を特定したり、リスク対応の方針や内容等を検討したりすることが可能となる。

2-2-2 リスクアセスメント

(1) 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

2-2-1 で明確化した適用範囲において、想定され得るセキュリティインシデント等とその結果（影響）を特定する。2-3 では想定され得るセキュリティインシデントの例を示すが、機器・システム及びそれに関連するステークホルダーに対して重大な影響を及ぼし得るものについては、漏れ等がないよう取り組むことが望ましい。生じ得る具体的なインシデントや影響は、対象となる IoT 機器・システムの種類や利用環境、適用主体の役割等により様々なものが考えられるが、参考までに、IoT 機器・システムの提供または利用に際して典型的に想定されるセキュリティインシデントやその結果には以下が挙げられる。

＜想定されるセキュリティインシデント（例）＞

- センサ機能の異常（誤計測、計測機能の停止等）
- アクチュエータ機能の異常（誤動作、稼働停止等）
- ネットワーク機器（ルータ、ゲートウェイ等）の異常（誤動作、設定の不正変更、稼働停止等）
- ネットワーク上における通信データの漏えい、改ざん、ネットワーク機能の停止
- 各種サービスを提供するサーバ等にて保管、活用されるデータの漏えい、改ざん、サービスの停止

＜セキュリティインシデント等により生じ得る結果（例）＞

- 事業の停止、劣化（例：機器・システム及び関連する業務の停止、製造物・供給物の品質低下等）
- 自社に対する信頼の低下 （例：顧客情報の漏えいに伴うサービスへの信頼の低下）
- 人的被害 （例：機器・システムの停止や誤動作等による人的損傷、健康被害の発生）
- システム破壊 （例：機器・システムの停止や誤動作等による周辺設備の損傷、環境への悪影響）
- 法令順守抵触事象の発生 （例：各業法、またはデータ保護法等に定められた報告事案等の発生）

(2) 機器・システムの重要度の判断基準及び判断された重要度の一覧

(1)にて特定されたセキュリティインシデント等とその結果を考慮し、想定される被害（リスク）の程度に応じて重要度を割り当てる。

IoT-SSF は、適用主体が「回復困難性の度合い」及び「経済的影響の度合い」を 2 つの軸として設定した上で、フィジカル・サイバー間をつなぐ機器・システムを、(1)にて特定される当該機器・システムに潜むリスク（インシデント及びその結果）に基づいてカテゴライズし、マッピングすると記述している。

以下では、上記の 2 つの軸に基づきリスクの大きさを評価する際の判断基準や留意すべき点等につ

いて、IoT-SSF を参照しつつ考え方を示す。

IoT-SSF では、「インシデント発生によって影響を受ける事象ごとに整理を行うことは、フィジカル・サイバー間をつなげる機器・システムのセキュリティ対策を検討する上で、その考え方を逆に複雑なものにしてしまう」とされていることから、本稿では、（リスクアセスメント等でしばしば行われるような）想定されるリスクごとの整理を行うのではなく、かかるリスクが想定される「機器・システム」という単位で整理を行うこととする。

また、本来、リスクの大きさを評価する際の判断基準は、適用主体やその他の関係者における個別の事情等を勘案して作成されるものだが、IoT-SSF にて示された共通の尺度に基づいて複数のユースケースを評価するという本稿の性質上、評価が取扱うユースケース間で相対的なものとなっている点に留意されたい。

なお、同一のインシデントを想定するとしても、それにより受ける影響の内容やその程度は主体や役割により異なり得るが、IoT-SSF を「基本的共通基盤」として活用しようとする際には、対象の機器・システムが提供主体のみならず、利用者やその他の関係者にとって十分に信頼できるものとなるよう取組みを行うべきである。よって、適用主体は、自身のみならず、関係し得る各主体（例：適用主体が IoT サービス提供者の場合、IoT 利用者、IoT サービス開発者、その他の関係者）が機器・システムの利用または提供を通じて被り得るリスクを十分に明確化したうえで、その程度に関する評価（マッピング）を行い、後の対策の検討等に活用することが望ましい。

① 第 1 軸：発生したインシデントの影響の回復困難性の度合い

IoT-SSF では、人命/身体にかかわるセーフティ側面の影響に加え、個人のプライバシー/名誉に関する影響も第 1 軸「回復困難性の度合い」にて考慮すべきとしている。

人命/身体にかかわる影響の観点では、資産が攻撃された場合に、利用者または関係者の人命が失われるおそれがある場合は「致命的なダメージ」、重症を負うおそれがある場合には「重大なダメージ」、軽傷を負うおそれがある場合は「限定的なダメージ」と判断できる。資産が悪意のある者により攻撃された場合や、機器・システムを製造する事業者が当初想定していなかった方法で機器・システムが利用される場合に、機器・システムの種類や利用環境等によっては利用者または関係者の人命が失われる可能性も想定される。なお、人命が失われるおそれがある場合であっても、そのような状態に至る条件等が成立する可能性が高くない場合（例：機器の利用状況が製造者側の想定と著しく異なっている）は、「重大なダメージ」と位置付けることも考えられる。

個人のプライバシー/名誉に関する影響の観点では、個人情報等が流出した際に軽度なプライバシーの侵害が認められる場合は「限定的なダメージ」とした上で、重要度の高い個人情報等が漏えいした際に重大なプライバシーの侵害が認められる場合は「重大なダメージ」とする。より具体的に、プライバシーの侵害等に関連して、想定されるリスクの深刻度を判断するにあたっては、既に公開されている文献[6]を参考にされたい。

以下に、上記の議論を踏まえて特定した第 1 軸「回復困難性の度合い」の判断基準を示す。

[6] 特定非営利法人 日本ネットワークセキュリティ協会(JNSA)「情報セキュリティインシデントに関する調査報告書 別紙」（第 1 版）では、漏洩個人情報の価値を EP 図（Economic-Privacy Map）にマッピングしている。

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

図 3 発生したインシデントの影響の回復困難性の度合いの判断基準

② 第 2 軸：発生したインシデントの経済的影響の度合い

IoT-SSF によると、第 2 軸「経済的影響の度合い」は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であるとしている。ここでは、例えば、IoT 機器・システムの停止等により事業者に生じる逸失利益や、個人の生活や社会への影響等（例：サプライチェーンにおける遅延、ライフラインの停止等）が評価の対象となり得る。

金銭的価値に係る評価の尺度は個別の分野や企業の規模によって異なるものである。例えば、企業や事業部門の規模や財務状況等によって、インシデントにより発生する 1,000 万円程度の経済的影響が、「限定的な経済影響」となる場合も、「壊滅的な経済影響」となる場合もあり得る。そのため、具体的な金銭的価値に換算された経済的影響の評価基準は各々の企業や事業部門等において検討されることが望ましい。本稿では、リスクが大きいにも関わらずリスクが過少評価される可能性を低減するため、レベルごとに具体的な金額を示さず、各レベルを判断するための考え方を示している。定量的な金銭的価値へ換算方法については、既存の文献[7]などを参考にされたい。

「経済的影響の度合い」を評価する際、「直接的な経済影響」及び「間接的な経済影響」に分けて検討を行うことができる[8]。「直接的な経済影響」とは、インシデントによりもたらされる逸失利益、復旧に要したコスト、営業継続費用、喪失情報資産額、機会損失額等、直接的に生じる被害の金額をいう。また、「間接的な経済影響」とは、製品回収等の間接的に生じる被害の金額をいう。

[7] 既存の文献として、特定非営利法人 日本ネットワークセキュリティ協会(JNSA)「インシデント損害額調査レポート 2021 年版」(2021 年 9 月)、一般社団法人 日本サイバーセキュリティ・イノベーション委員会(JCIC)「取締役会で議論するためのサイバーリスクの数値化モデル」(2018 年 9 月)等が挙げられる。

[8] 特定非営利法人 日本ネットワークセキュリティ協会(JNSA)「セキュリティ被害調査 WG の定量化アプローチ」を参考とした。ただし、当該文書の「潜在化被害」はここでは考慮しないものとする。

また、「直接的な経済影響」を評価する際には、「内外への直接影響」、「直接影響の継続時間」及び「代替可能性」に分けて評価を行うこととしている[9]。単に影響の規模が大きなものだけでなく、影響が長期間継続するものや、影響のリカバリーが困難なものに対して、「直接的な経済影響」が大きいと評価され得る点に留意する必要がある。

「内外への直接影響」では、直接的な影響が及ぶ範囲として当事者内部と、当事者外部（顧客、取引先等）の双方を考慮する必要がある。また、影響範囲が当事者内部に限定される場合においても、その被害影響が当事者にとって重要な位置づけかを考慮する。

「直接影響の継続時間」では、経済的影響を及ぼす事象が長時間に渡って継続するかを考慮する。

「代替可能性」では、経済的影響を代替的な手段（例：DR サイト[10]への切り替え）により軽減できるかを考慮する。

「間接的な経済影響」では、間接被害の規模として、大規模な製品等の回収が想定されるかを考慮する。

これらの基準を踏まえ、本稿における第 2 軸「経済的影響の度合い」の判断基準を以下に示す。

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

図 4 発生したインシデントの経済的影響の度合いの判断基準

(3) マッピング結果の整理と評価の実施

(2)①及び②にて特定された対象機器・システムにおけるリスクの概要（シナリオ）及びその水準（重要度）を、2-2-1 にて確立した自身のリスク基準と比較し、2-2-3 におけるリスク対応の方向性を検討する。

リスク基準との比較の結果、対象の機器・システムが、特定のセキュリティインシデントを通じて受容しがたい水準のリスクをもたらし得ると判断できる場合、適用主体は当該機器・システム等への対処を念頭に置きつつ、適切なリスク対応の手段を選定することが望ましい。その際、対象の機器・システムに

[9] 直接的な経済影響は内閣サイバーセキュリティセンター(NISC)「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準（初版）」の「サービスの持続可能性への影響」を参考としている。なお、「サービスの持続可能性への影響」はサービス障害の範囲、時間の程度、サービスの代替性の有無から評価するとしている。

[10] DR サイトとは、災害などで主要な IT システム拠点での業務の続行が不可能になった際に、緊急の代替拠点として使用する施設や設備を指す。

おいて想定される相対的に影響の大きなセキュリティインシデントとその実現シナリオを特定[11]し、それが顕在化した場合の影響の度合いを低減することに加え、起こりやすさの低減についても考慮することが適切であることに留意されたい。

典型的なリスク対応の手段には、以下が含まれる。

- インシデントの影響の回復困難性の度合い、または経済的影響の度合いを低減するもの
- インシデントの起こりやすさを低減するもの
- リスクを生じさせる活動を開始、または継続しないと決定することによってリスクを回避するもの
- 例えば、契約、保険購入等の手段により、リスクを共有するもの
- リスクを保有するもの

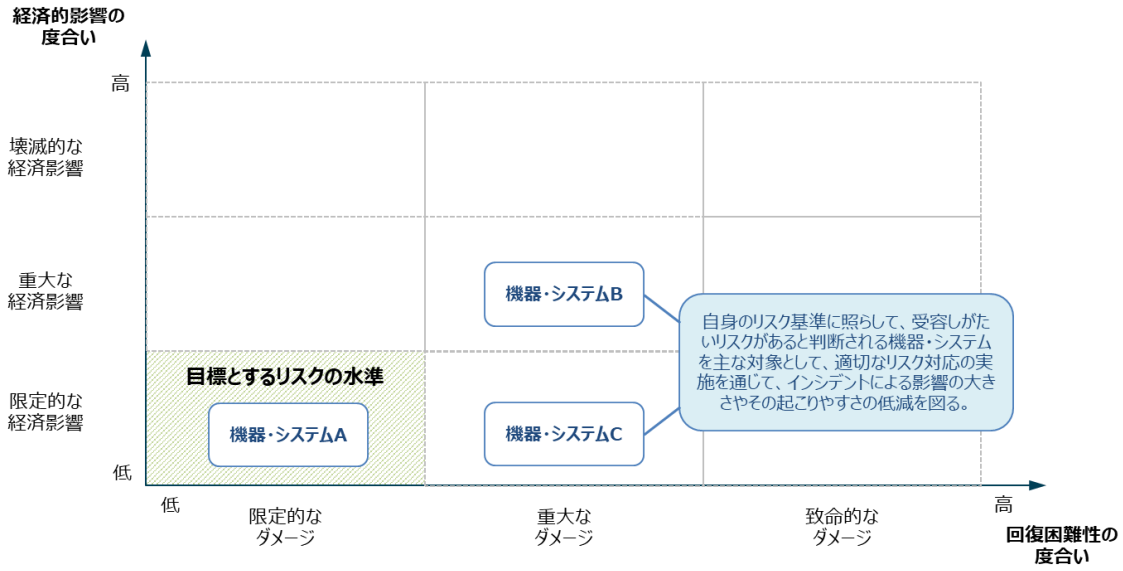


図 5 マッピング結果の整理と評価の実施における考え方

リスク対応手段の選定を含め、適用主体が具体的にリスク対応に係る方針を検討するにあたり、想定される様々な対策を優先順位づけ、リスク対応計画等に反映することが有効である。その際、優先順位が高いと評価され得る対策の特徴として、例えば以下が挙げられる。

- 生じ得る影響の度合いが相対的に大きいと評価される機器・システムを対象にした対策
- インシデント等により被り得る影響の度合いが相対的に大きいと評価される主体（例：IoT 利用者）を保護するための対策
- 効率的に（低コストで）相対的に大きなリスクを低減等することができると見込まれる対策
- 対象となる機器・システムにおいて法律等により適用が義務とされているもの

[11] 攻撃シナリオの検討方法等について、本稿では、2-2-3 (1)に示す脅威の整理に留め、詳細なプロセスには言及しない。読者においては、必要に応じて、「制御システムのセキュリティリスク分析ガイド 第2版」の「6. リスク分析の実施（2）～事業被害ベースのリスク分析～」等を参照されたい。

2-2-3 リスク対応（ステークホルダー別の対策例一覧）

リスク対応を行うステークホルダーが、実施すべき対策を整理する。対策を整理するにあたり、以下の手順にて行う。本稿では、システムを構成する機器を網羅的に分析することで対策を強化することが可能な資産ベースのリスク分析手法を参考にしている[12]。

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

(1) システムを構成する機器ごとの脅威の整理

「リスクアセスメント、リスク対応に向けた事前準備」にて整理したシステムを構成する機器に対する脅威を整理する。本稿では、特に、相対的に影響の度合いが大きいと評価された機器・システム及びそこで想定されるセキュリティインシデントに関連した脅威を中心に検討するものとする。

以下に示すように、2-2-2 にて評価されるリスクを引き起こし得る要因は、対象となる機器・システムの故障や性能限界、故意に基づかない人為的ミス、故意による内外からの攻撃等、様々なものが想定され得るが、本稿では情報の機密性、完全性、可用性に影響を及ぼすような「セキュリティ上の脅威」を取扱うこととし、セキュリティ上の脅威とは直接的に関係しない要因（例：機器・システムの欠陥や故障、性能限界）は検討の対象外とする。対象外とした要因への対処等については、機能安全や SOTIF (Safety Of The Intended Functionality)等に関する既存のガイドライン等を参照されたい。

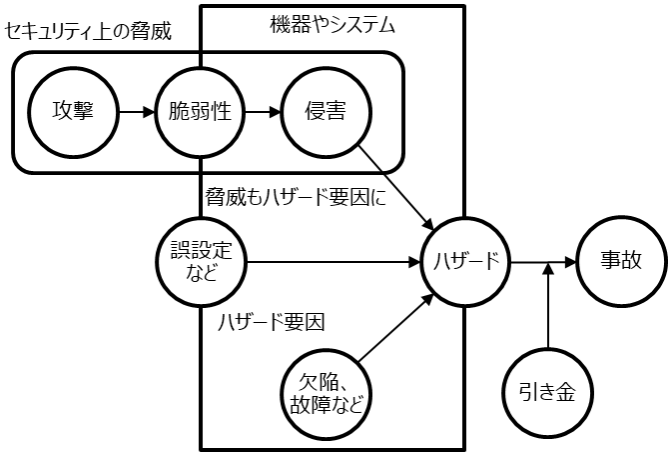


図 6 セキュリティ上の問題がセーフティに影響を与えるモデル[13]

セキュリティ上の脅威の整理にあたっては、例えば脅威分析手法として広く用いられる STRIDE モデル[14]が参考となる。

[12] 本稿にて示すリスク対応方法は、資産ベースのリスク分析手法を参考にしているが、シナリオベースのリスク分析手法を制限するものではない。
[13] IoT 推進コンソーシアム、総務省、経済産業省「IoT セキュリティガイドライン ver.1.0」（2016 年 7 月）
[14] STRIDE モデルは Microsoft 社が脅威分析手法として提唱したものであり、脅威分析にあたり国内外で広く参照されている。

表 2 STRIDE モデルにおける脅威

脅威	内容
なりすまし	コンピュータに対し、他の利用者や機器を装うこと。
データの改ざん・消去	権限なしでデータを改ざんまたは削除し、データの完全性を失わせること。
否認	利用者が、あるアクションを行ったことを否認し、相手はこのアクションを証明する方法がないこと。
情報漏えい	アクセス権限を持たない個人に情報が公開されること。
サービス不能	正規のユーザがサーバやサービス等にアクセスできないこと。 ※DDoS 攻撃やジャミングによるサービス妨害など。
権限の昇格	権限のない利用者がアクセス権限を得ること。

上記モデルは IT システムの脅威を抽出する目的で提唱されたものであり、必要に応じて STRIDE モデル以外の手法[15]を組み合わせた上で、脅威抽出の網羅性を向上させることが望ましい。なお、上記モデルにて示した脅威に加え、IoT 機器・システムに対する脅威として、例えば以下のような脅威が挙げられる。

表 3 IoT 機器・システムに関する脅威（例）

脅威	内容
不正アクセス	アクセス権限を持たない者にアクセスされること。
マルウェア感染	他の機器への汚染源になる。ランサムウェアなどにより業務妨害を受けること。
踏み台	他の機器へ不正アクセス等を行う際の中継地点として使用されること。
不正改造	不正（違法）なハードウェア、ソフトウェアの改造により、内部データを抜き取り、脆弱性の要因を組み込まれること。
未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性のこと。
不正利用	アクセス権限を持つ者が不正に意図しない用途等でアクセスすること。
利用者によるセキュリティ設定の誤り等	機器が利用者等により十分なセキュリティ設定等がなされずに使われること。

これらの脅威は様々な原因によって生じるものであり、実際に対策要件を整理する際には、より具体的に原因を特定することが望ましい。本稿では、上記に示す脅威の洗い出しにとどめているが、より詳細な分析を行う際には既存の文献[16]等を参照して脅威の洗い出しを実施することが望ましい。

[15] 一般社団法人 重要生活機器連携セキュリティ協議会(CCDS)「IoT 機器に対するリスク分析のガイド」の「CCDS-STRIDE モデルによる脅威の分類」や経済産業省 商務情報政策局 サイバーセキュリティ課「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 別冊 1 脅威分析及びセキュリティ検証の詳細解説書」を一部参照。

[16] 既存の文献として、独立行政法人 情報処理推進機構(IPA)「制御システムのセキュリティリスク分析ガイド第2版」(2020 年 3 月)及び経済産業省「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 別冊 1 脅威分析及びセキュリティ検証の詳細解説書」(2021 年 4 月)等が挙げられる。

(2) 脅威への対策の整理

上記で整理した脅威のうち具体的な対処が必要なものに対して、IoT-SSF における「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[17]を参照しつつ、リスク対応に有効と考えられる対策を整理する。また、対策の整理にあたっては、4 つの観点のほか、以下の事項を考慮しつつ具体化を図る。

・ 対策の実施主体

一般に IoT 機器・システムの開発、運用等にあたっては、役割の異なる複数の主体が関係することが想定される。その際、適用主体は、他の事業者等に対して必要な対策の実施を依頼等することにより、当該主体間で責任分界が不明確になり、結果としてセキュリティ対策の抜け漏れが発生したり、全体の対策水準が十分でなくなったりする事態を防ぐ必要がある。かかる観点から、2-3 における各ユースケースでは、参考として、「リスクアセスメント、リスク対応に向けた事前準備」の「ステークホルダー関連図」にて整理したステークホルダーを参照し、適用主体が実施すべき対策のほか、対象機器・システムの提供または利用に責任を有する他の事業者または個人に対応を依頼する対策例を示す。

IoT 利用者(発注側)及び IoT サービス開発者、IoT サービス提供者(受注側)の役割分担を検討するにあたり、以下に参考として、IoT 利用者等が企画・設計の段階からセキュリティ仕様等の策定に積極的に関与し得る場合を想定した、IoT 機器・システムの調達プロセスにおける対策実施の役割分担(例)を示す。

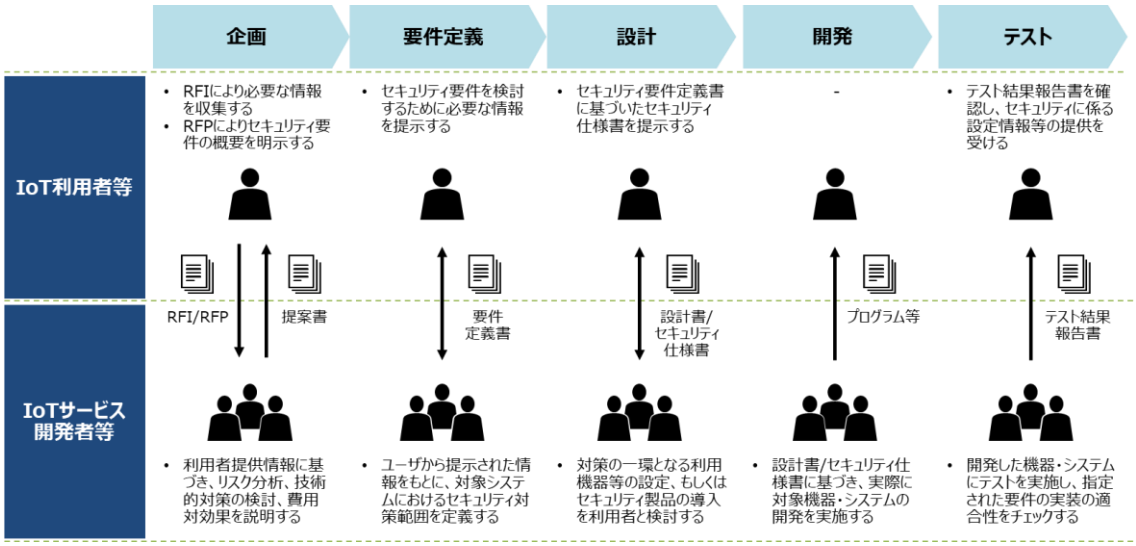


図 7 IoT 機器・システムの調達プロセスにおける対策実施の役割分担(例)[18]

ここで IoT-SSF の適用主体を IoT 利用者等とすると、自身が将来的に利用する IoT 機器・システムの

[17] 第 3 軸「求められるセキュリティ・セーフティ要求」では、第 1 の観点「運用前(設計・製造段階等)におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求」、第 2 の観点「運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求」、第 3 の観点「機器・システムの運用・管理を行う者の能力に関する確認要求」、第 4 の観点「その他、社会的なサポート等の仕組みの要求」という 4 つの観点に分けてセキュリティ・セーフティを確保するための手法を整理している。

[18] 内閣サイバーセキュリティセンター(NISC)「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」、セキュリティ検討プロジェクトチーム「セキュリティ仕様策定プロセス」等を参照し作成。

企画からテスト、あるいは運用に至るまでのライフサイクルを通じて、設計、開発等の実務を担う IoT サービス開発者等との間で文書を通じたコミュニケーションを行い、最終的な成果物である機器・システムのセキュリティを確保する。また、これらのプロセスにおいては、契約等の適切な合意に基づいて責任が割り振られ、それが適切に実施される必要がある。

IoT 利用者（消費者等）がセキュリティについて十分な知見を有さない場合や、商習慣上このようなプロセスを実施することが困難な場合には、システムインテグレータや IoT 機器製造者等の IoT サービス開発者側が利用者の潜在的なニーズ等を調査してセキュリティ仕様の策定を行う等、上記の例とは異なった対応が必要になる点に留意する必要がある。

・ 対策の実装先

IoT 機器・システムの適切な保護にあたっては、第 3 軸における 4 つの観点の各々に関して、通信の暗号化やユーザ認証の実施等の機器やシステムに対する技術的な対策だけではなく、セキュリティ対応組織の設置や関連するポリシーや手順の策定等のソシキ・ヒトに対する非技術的な対策も含めて検討を行う必要がある。本稿では、参考として、「ソシキ・ヒト」、「プロシージャ」または「システム」という対策の実装先ごとに想定される要件や対策の例を示す。

・ セーフティ[19]確保に向けた対策の考慮

IoT 機器・システムには、外界に何か物理的な力を与えるアクチュエータが備えられている場合があることを踏まえると、セキュリティ対策とセーフティに関連する対策を両立することも求められる。本稿では機器・システムが IoT 化することによって新たに考慮すべきセーフティの対策も示す。ただし、IoT 化とは必ずしも関連しないと考えられ、従来から必要とされているセーフティに関する対策については、既存の各文献を参照されたい。

本稿においては、国内外で策定された複数の文献を参照し、IoT 機器・システムに関する対策要件を添付 A、実際に講じる対策の例を添付 B に示した。

例えば、第 1 の観点では、「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」等、第 2 の観点では「IoT 機器・システムの出荷時における安全な設定と構成」等、第 3 の観点では「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」等、第 4 の観点[20]では「賠償等の対処を実施することが容易ではないケース等における社会的なセーフティネットの構築」等が整理された。

ただし、添付 A、添付 B に示す対策要件はあくまで例示にすぎないことに留意されたい。必要に応じて、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。また、添付 A に示す対策要件のうち、どの主体がどの対策要件を実装するかはユースケースに依存することから、本節では記載せず、各ユースケースの記述において記載する。

(3) 整理した対策に対する意思決定

(2)で対策を整理した後で、それらの対策をすべて実装し、想定されるリスクを最小化することが一見

[19] 本稿では、工場、社会インフラの観点での安全性を「セーフティ」と記載する。
[20] 本稿では、第 4 の観点（その他、社会的なサポート等の仕組みの要求）に関する対策を、専ら規制当局や業界団体等による措置に限定して捉えることとする。

理想的なようにも思われるが、IoT-SSF でも触れられているように、対策の実施はコストに直結するものであることから、全ての対策を実装することは現実的ではない。また、運用上重要な要件（例：小型化）を実現しようとする際に一部の対策の実装がそれと矛盾する可能性もある。

各事業者において実際に適用する対策を特定する際には、各ステークホルダーにとって許容可能な範囲までリスクを低減することを前提に、それを可能な限り効率的に（低コストで）かつ、各事業者の負荷を軽減させる形で実装することが目的となる。IoT-SSF でも記載した通り、リスクはインシデントによる影響の度合いと、インシデントの起こりやすさを用いて捉えることとなることから、対策等を検討する際にはインシデント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ような対策を検討する必要がある。様々な考え方が適用され得るが、例えば以下のように、リスクがより高いとされる機器や脅威への対策を中心に検討する方法がある。

- 対策の適用対象（どの機器を中心に検討するか）
- 適用する対策の内容（どのように対策を実施するか）

① 対策の適用対象（どの機器を中心に検討するか）

ある機器に係るリスクの大きさを評価しようとする際、例えば、当該機器に影響を及ぼす事象が実際に生じた場合に結果として生じ得る被害の大きさや、当該機器に悪影響を及ぼし得る事象の起こりやすさのそれぞれに着目することができる。

被害の大きさを評価する際、機密性の観点が特に重視される一般的な情報システムとは異なり、IoT 機器・システムではしばしば完全性や可用性が優先される[21]ことから、IoT 機器・システムに関する対策を実装する際には、特に完全性及び可用性の観点で大きなリスク（例：人身事故、設備の損傷、プロセスの停止）が想定される機器への対策を実装することが適切な場合がある。

完全性・可用性の観点で大きなリスクが想定される資産は、物理空間に直接作用する末端の機器及びその制御に関わる機器・システムである場合が多く、一つのシステムに多数の機器が利用される、機器の演算能力が十分でない等の理由で、個々の機器すべてに高いセキュリティ対策を実装することが困難である場合がある。そこで、起こりやすさを低減する観点では、外部からの攻撃への対策は、外部からの脅威にさらされやすい（インターネットに直接接続されている、または外部ネットワーク、その他のインターフェースからの侵入が比較的容易な領域に位置する）機器に関して対策を実施することで、効率的にリスクを低減させるアプローチも考えられる。その場合、末端の機器における外部からの攻撃への対策が不在になることから、末端の機器においてはフェールセーフの対策を実装することで、被害の大きさを低減させてリスクを小さくとどめることが可能になると考えられる。

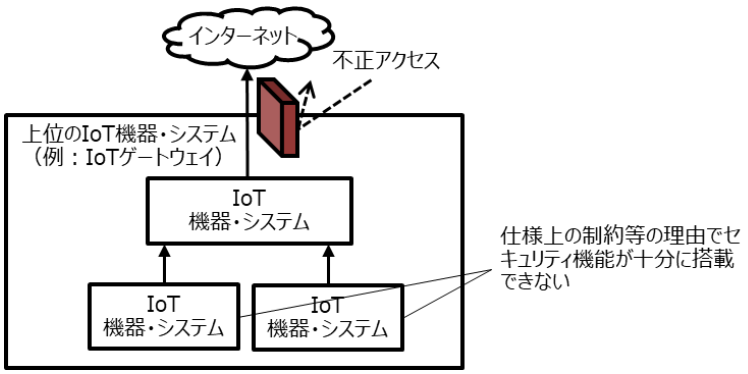
② 適用する対策の内容（どのように対策を実施するか）

実施する対策を評価する際、より効率的・効果的にリスクを低減できるものがあれば評価は必然的に高くなる。こうした評価は、例えば当該対策によって見込まれる効果の大きさ（結果として低減されるリスクの大きさ）や、対策に係るコスト等が勘案されるべきである。例えば、同一の機器に対策を行う場合に、

[21] IoT 機器・システムにて収集するデータは非常に粒度が細かく、攻撃者にとっても個別の IoT 機器・システムから情報を窃取することはかかる手間に対して割に合わないとされている。特に産業用 IoT 機器では、機密性よりも完全性や可用性が重視される傾向があるとされるが、一方で、消費者用 IoT では、機密性がより重視される場合もある。

411 コストや労力が同等であればより低減できるリスクの大きいものを採用することが望ましい。
412 　一方で、リスク低減効果の高い対策であっても、対象となる機器の種類によっては、仕様上の制約等
413 の理由でセキュリティ機能が十分に搭載できない場合がある。こうした機器に対して単体での対策を行
414 うことが現実的、効率的でない場合、よりリソースが十分である「上位の IoT 機器・システム」（例：IoT
415 ゲートウェイ）がシステム単位で対策を担うことも想定される。そのような対策の例としては、以下が挙げ
416 られる。

417 ・ 末端の IoT 機器等にてマルウェア検出ソフト等の実装が困難な場合、IoT ゲートウェイ等にてマル
418 ウェア検査を実施する。
419 ・ 末端の IoT 機器等による外部への通信を IoT ゲートウェイ等において監視し、必要に応じて不審な
420 ものを検出する。
421 ・ 末端の IoT 機器等にて通信の暗号化に対応することが困難な場合、IoT ゲートウェイ等に係る機能
422 を実装することで、インターネットを経由する通信を保護しつつ、エンドポイント機器側の処理を効
423 率化する。



424
425 図 8 上位の IoT・機器システムでセキュリティ対策を実装するイメージ[22]

[22] IoT 推進コンソーシアム、総務省、経済産業省「IoT セキュリティガイドライン Ver1.0」（2016 年 7 月）P30 を参照し、修正。

2-3　具体的なユースケース

2-3-1 家庭用ガス給湯器の遠隔操作

「IoT 機器・システムを通じて提供されるサービスの開発者」である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を記載する。

ガス給湯器の製造元はスマートホームを供給する事業者等と協力して新たに遠隔操作を可能とするガス給湯器及びそれに関連するサービスの開発を企画しており、機器のネットワーク接続等に伴い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。

特に、IoT 機器の利用者（消費者等）がセキュリティについて十分な知見を有さない主体と考えられるため、ガス給湯器の製造元やスマートホームを供給する事業者（ハウスメーカー等）の供給側が中心となって、対象機器・システムに関するリスクアセスメントを行い、残存するリスクに対しては利用者に対応を依頼することで、可能な限り、リスクを低減することを目的とする。

(1)　リスクアセスメント、リスク対応に向けた事前準備

①　対象ソリューションの概要

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、居宅内のガス給湯器[23]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。

なお、ガス製品には遠隔操作が禁止されるものも存在するが、本稿では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。各事業者等において、本稿を参照し、具体的な取組みを進めようとする際には、改めて既存の法律や文献[24]を参照されたい。

- 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。(※1)

※1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、危険が生ずるおそれがないものは、操作可能」とされている。

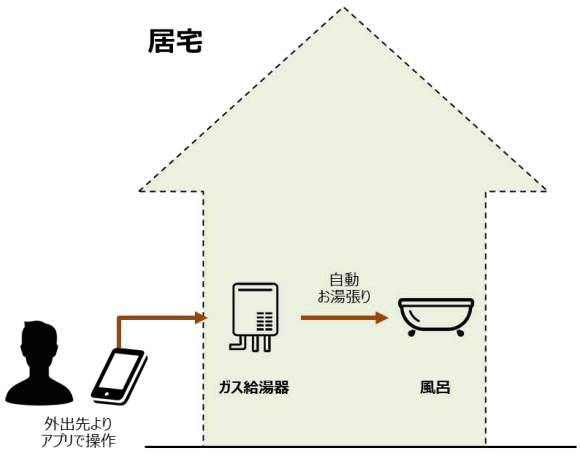


図 9 対象ソリューションの概要

[23] 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」（2020 年 7 月）では、「自然吸排気式」及び「開放式」以外のガス給湯器において「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、危険が生ずるおそれがないものは、操作可能」とされている。したがって、本稿では「自然吸排気棄式・開放式」以外のガス給湯器を想定する。

[24] 既存の文献として、経済産業省「電気用品、ガス用品等製品の IoT 化等による安全確保の在り方に関するガイドライン」（2021 年 4 月）等が挙げられる。

② ステークホルダー関連図

本稿にて示す取組みに関与するステークホルダーとして、以下に示すように、「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」、「住まい手」及び「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」を想定している。

本稿では、既に完成している住宅ではなく、新築の住宅に対して IoT 機器・システムを含む設備一式を納入する事例を想定する。具体的には、「スマートホーム向け IoT 機器の事業者」が製造したガス給湯器は、「スマートホームを供給する事業者」を通じて「住まい手」に納入される。また、「スマートホームを供給する事業者」が提供する専用コントローラは、ガス給湯器以外の IoT 機器・システムにも接続することは想定していない。一般にスマートホームとして戸建住宅もしくは集合住宅が扱われ得るが、本稿では戸建住宅を想定している。

＜IoT サービス開発者/IoT サービス提供者＞

- スマートホーム向け IoT 機器・サービスの事業者

スマートホーム向けの IoT 機器を開発・生産・販売する事業者であり、本稿で想定するガス給湯器の遠隔操作を実現するサービスの提供にあたり、中心となって IoT 機器・システムに関して対策を実装すべき主体である。本稿ではガス給湯器の製造元を想定している。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を本事業者とは分けて記載しているが、しばしば同一の事業者が担い得る。

- スマートホームを供給する事業者

IoT 機器の開発・生産自体は行わないが、IoT 機器や IoT 化された住宅設備を住まい手に対して供給・設置する事業者である。本稿ではハウスメーカーや施工業者等を想定している。

- 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

スマートホーム向けのサービスや IoT 機器・システムに関して、メンテナンスはじめ、設置・設定・運用などを行う事業者である。本稿では、遠隔保守サービスなどを提供する事業者等を想定し、脆弱性対応や機能のアップデートに関する更新プログラムの配信等を行う。また、関連法令に基づいて、ガス給湯器を含めた給排気設備などの法定点検調査を行うものとする。

＜IoT 利用者＞

- 住まい手

スマートホームの居住者であり、主として IoT 機器を利用したサービスを受ける。本稿では、戸建住宅に設置されたガス給湯器を遠隔操作する主体となる。

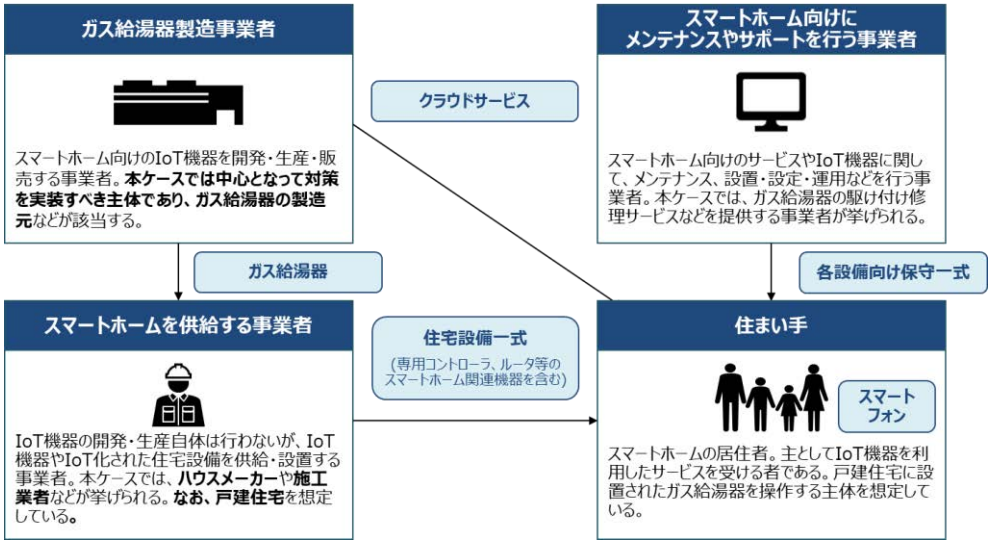


図 10 ステークホルダー関連図

③ システムを構成する機器の一覧

本稿の対象となる機器は以下の通りとする。

表 4 システムを構成する機器の一覧

システムを構成する機器	内容
ガス給湯器	専用コントローラから指示を受けることで、自動湯沸かし等が可能となる機器。 ガス給湯器内に特定の個人に関する情報を保管しないことを想定する。 ガス給湯器は台所等の給湯にも使われ得るが、主な用途を風呂の自動湯沸かしと設定し、居宅外に設置するものとする。 ガス給湯器内の構成要素としては、例えば以下が挙げられる。 ● センサ：水量センサ、水位センサ、CO センサ等 ● アクチュエータ：燃焼ファン、給湯熱交換器等
専用コントローラ	スマートフォンから指示を受け、居宅内のガス給湯器に指示を出す機器。 専用コントローラは、住まい手が簡単に設定変更できる位置に設置するものとする。
ルータ	居宅内に設置され、居宅内のネットワークおよび居外のネットワークを中継する通信機器。 ルータは、居宅内の他の機器にも接続することを目的として住まい手が簡単に設定変更できる位置に設置するものとする。
スマートフォン	専用のアプリケーションをインストールしたスマートフォン。 住まい手は、外出先からスマートフォン上のアプリケーションを操作してガス給湯器の遠隔操作を行う。 スマートフォンは、住まい手が所有するものを使用することとする。
クラウドサービス	スマートフォンから指示を受け、インターネット回線を通じて専用コントローラに指示を出すシステム。 クラウドサービスは、業務効率化を目的として外部の IT サービス事業者が提供するデータセンターから提供するものとする。

④　システム構成図、データフロー図

システム構成図は以下の通りとする。

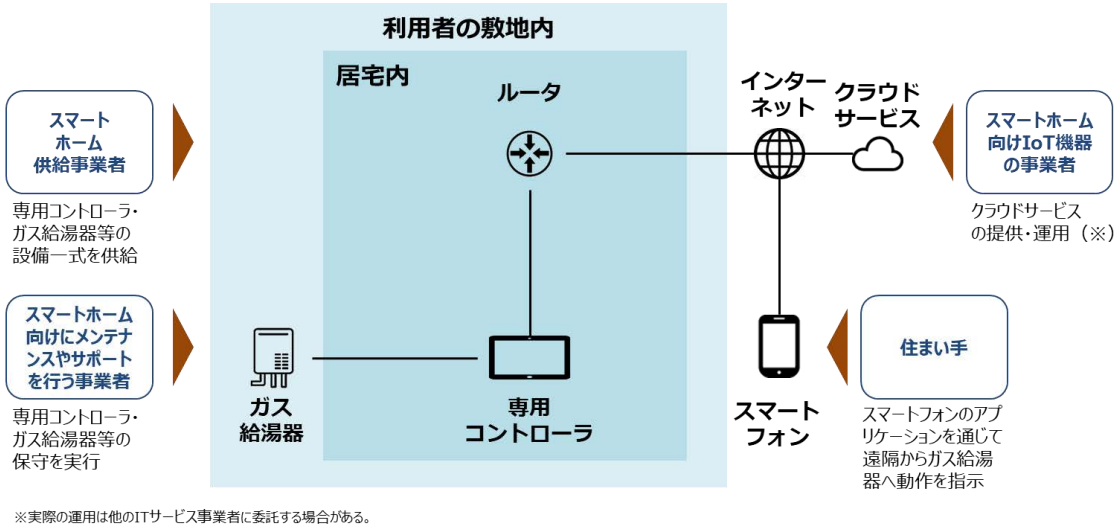


図　11　システム構成図

住まい手が外出先よりスマートフォン専用のアプリケーションを通じて、居宅内のガス給湯器を遠隔操作し、自動お湯張りを実施する場合のデータフローは以下の通りとする。

1. 住まい手が所有するスマートフォンからクラウドサービスに対して、操作指示を出す。
2. クラウドサービスからインターネットを通じて、ルータ経由で専用コントローラに指示を出す。
3. 専用コントローラから居宅内のネットワークを通じてガス給湯器に ON/OFF の指示を出す。

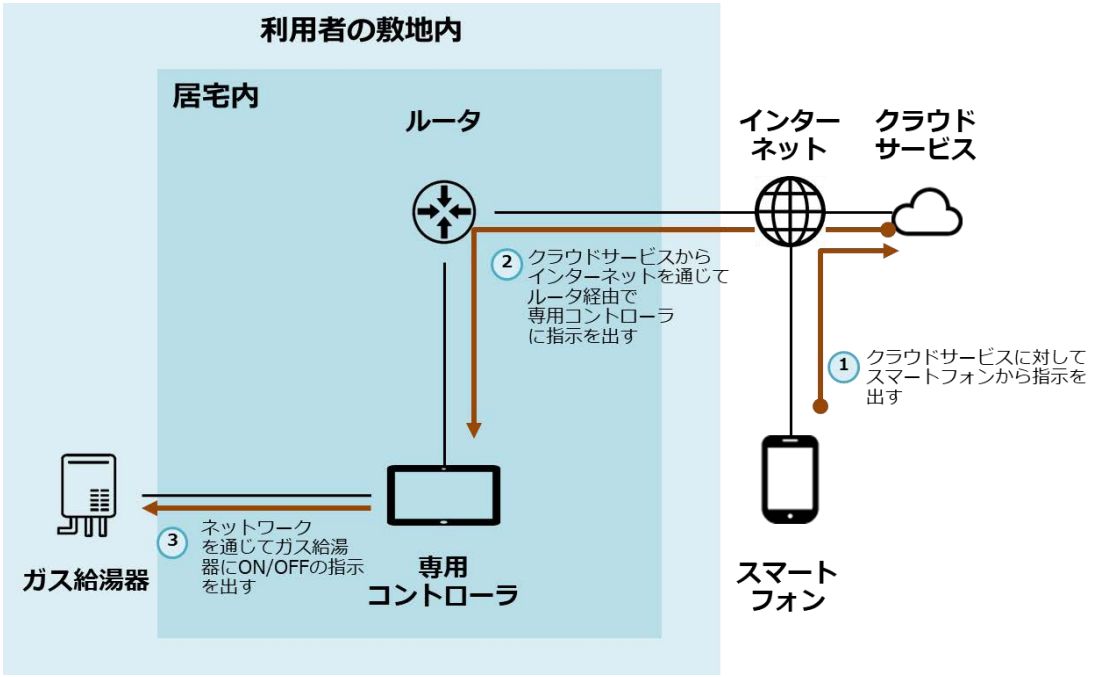


図　12　データフロー図（一部を抜粋）

⑤　リスク基準

「回復困難性の度合い」及び「経済的影響の度合い」に関連付けて整理する。

「回復困難性の度合い」に関しては、自社が定めるセキュリティやセーフティ等に関する基本方針に乗っ取り、住まい手による製品の利用において重大な事故等がないよう、セキュリティ、セーフティの対策を通じて、可能な限り生じ得る被害の度合いを「限定的なダメージ」に抑えることを目指す。

また、「経済的影響の度合い」は、自社の事業規模を考慮し、大規模な製品回収等が生じない、「限定的な経済影響」に抑えることを目指すものとする。

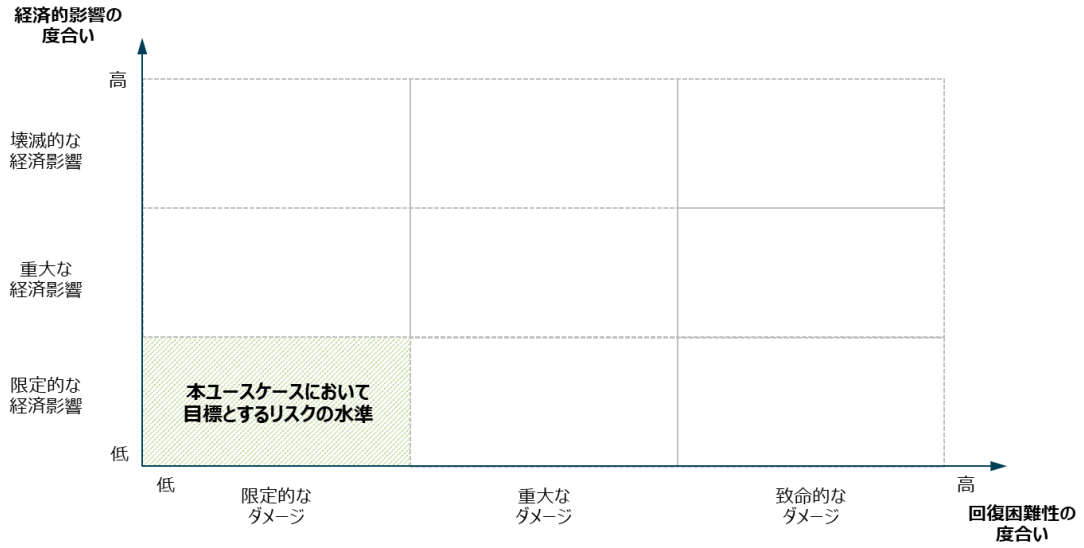


図 13 ガス給湯器システムにて目標とするリスクの水準

(2)　リスクアセスメント

「回復困難性の度合い」及び「経済的影響の度合い」から、ガス給湯器システムのリスクアセスメントを行う。

①　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

ガス給湯器システムにおいて、想定され得るセキュリティインシデント等とその結果（影響）を特定する。ガス給湯器システムの提供または利用に際して想定されるセキュリティインシデント（例）は以下の通り。

- 悪意のある攻撃者がクラウドサービスに対して不正アクセスすることによって、クラウドサーバから利用者の個人情報が流出する。
- 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改ざんされ、ガス給湯器が想定されていない動きをする。その結果、住まい手がけがをしたり、住まい手の財産が侵害されたりする。
- 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た上で、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から、専用コントローラに対してネットワークを通じて不正なアップデートの配信やローカル環境で不正なアップデートが実行され、ガス給湯器が想定しない動きをする。その結果、温度の上昇に気付かずに入浴することによって、住まい手がやけど等のけがをする。
- リモートで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より、ガス給湯器内の情報

処理に関わっているコンポートネント（例：ネットワークインターフェース、MCU）が不正に改造される。
その結果、フェールセーフの機能が働かなくなり、住まい手のけがを抑止できない。

② ステークホルダーごとの観点を踏まえたリスクアセスメント

以下に示すステークホルダーごとに「回復困難性の度合い」「経済的影響の度合い」の観点からリスクアセスメントを行う。

- スマートホーム向け IoT 機器・サービスの事業者
- スマートホームを供給する事業者
- 住まい手
- 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

- 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）

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点及びセーフティの観点から判断した上で、「回復困難性の度合い」の大きさを評価する。

プライバシーの観点では、クラウドサービスもしくはスマートフォンにインストールされたアプリケーションから住まい手のアカウント情報やサービスの利用状況等が流出する可能性があると想定される。セーフティの観点では、ガス給湯器が予期せぬ動作をしたとしても、スマートホーム向け IoT 機器・サービスの事業者の従業員がけがを負う可能性は低いと想定される。

プライバシーの観点では住まい手の個人情報（アカウント情報やサービスの利用状況等）が流出する可能性があるものの、必ずしも重要な個人情報ではないこと、またセーフティの観点でも影響は限定的と想定されることから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

「経済的影響の度合い」は、直接的な経済影響及び間接的な経済影響から評価する。

直接的な経済影響は「内外への直接影響」、「直接影響の継続時間」及び「代替可能性」の観点から評価する。

「内外への直接影響（内部）」の観点では、各家庭に設置されたガス給湯器が停止したとしても、その製造元が運用する製造拠点やその他の活動等の直接的な停止にはつながりにくく、スマートホーム向け IoT 機器・サービスの事業者による経済活動の中断等は生じ難いと想定される。「内外への直接影響（外部）」の観点では、ガス給湯器の停止に加えて、クラウドサービスから送信される指示データ等の改ざんにより、ガス給湯器が誤作動を引き起こすことによって、スマートホーム供給事業者との取引に影響（例：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ことによる当該事業者製のガス給湯器の買い控え等）が及び得ると想定される。

「直接影響の継続時間」の観点では、ガス給湯器の故障等の不具合が認められたとしても、大規模なリコールに直結しないと判断される場合、製造等の事業の停止にはつながらないと想定される。

「代替可能性」の観点では、本ユースケースにて想定するインシデントが発生したとしても、事業活動のバックアップが必要になるような経済活動（例：自社工場の停止）等にはつながらないため考慮しない。

間接的な経済影響の観点では、ガス給湯器の修理に対する問い合わせ対応や交換対応に一定のコ

ストを要する可能性があり、また、場合によっては大規模な製品回収が発生する可能性があるものと想定される。

直接的な経済影響では、工場の直接的な停止にはつながらないと判断されたとしても、間接的な経済影響の観点で製品回収が発生する可能性があることから、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

- スマートホームを供給する事業者

A) 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、今回対象としている範囲に限定すれば、スマートホームを供給する事業者の責任で、住まい手のアカウント情報やサービスの利用状況等が流出する可能性は少ないと想定される。

セーフティの観点では、ガス給湯器が予期せぬ動作をしたとしても、スマートホームを供給する事業者の従業員がけがを負う可能性は低いと想定される。

プライバシーの観点では住まい手の個人情報が流出する可能性が少ないこと、セーフティの観点ではスマートホームを供給する事業者がけがを負う可能性が少ないことから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B) 発生したインシデントの経済的影響の度合い

「内外への直接影響」の観点では、ガス給湯器が停止したとしても、スマートホームを供給する事業者による経済活動の中断等は生じ難いと想定される。したがって、「直接影響の継続時間」の観点や「代替可能性」の観点でも、スマートホームを供給する事業者には影響が及びにくいと想定される。

同様に、間接的な経済影響の観点では、インシデントによるガス給湯器の大量回収が発生したとしてもスマートホームを供給する事業者が追う責任は限定的であると想定される。

直接的な経済影響及び間接的な経済影響の観点において、「経済的影響の度合い」が大きくなりにくいと想定されることから、「経済的影響の度合い」のレベルは「限定的な経済影響」と評価する。

- 住まい手

A) 発生したインシデントの影響の回復困難性の度合い

自身のプライバシーという観点では、クラウドサービスもしくはスマートフォンにインストールされたアプリケーションから住まい手のアカウント情報やサービスの利用状況等が流出する可能性があると想定される。

セーフティの観点では、セキュリティインシデントに伴って組込まれたセンサやアクチュエータが正常に作動せずガス給湯器が予期せぬ動作をした際に、機器近くにいる利用者がやけど等などの軽傷、あるいはその場の状況によっては重症を負う可能性があると想定される。

プライバシーの観点では住まい手自身の個人情報が流出する可能性があること、セーフティの観点では状況によっては利用者が重症を負う可能性があることから、「回復困難性の度合い」のレベルは「重大なダメージ」と評価する。

B) 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、ガス給湯器や関連する設備の稼働が停止した場合、住ま

い手が重症を負う等することによって、自身の生活に支障をきたす可能性があると想定される。

「内外への直接影響（外部）」の観点では、ガス給湯器が停止することによって、利用環境（居宅）外部へ影響は及びにくいものと想定される。

「直接影響の継続時間」の観点では、ガス給湯器の故障等の不具合が認められた場合、修理や交換に一定の時間を要する可能性があると想定される。

「代替可能性」の観点では、停止期間中、給湯が不可能になるものの、外部のサービスを利用することで機能を代替できる場合が一般的であると想定される。ただし、重症を負った場合には外部のサービスを利用することも難しくなる可能性がある。

間接的な経済影響の観点では、適正なガス給湯器の利用を行っている場合には、利用者が被る金銭的な負担等は発生しないと想定される。

間接的な経済影響では大きな影響はないものの、直接的な経済影響では、「直接影響の継続時間」の観点から生活に支障をきたす可能性があり、場合によっては代替的な手段でも代用不可と想定されることから、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

- 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

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、保守用端末に住まい手のアカウント情報やサービスの利用状況等が保存されていないとすると、これらのデータが流出する可能性は低いと想定される。

セーフティの観点では、ネットワークを通じて専用コントローラへ配信された不正なアップデートプログラムによって、ガス給湯器が予期せぬ動作をした際に、機器近くにいる利用者がやけど等などの軽傷、あるいはその場の状況によっては重症を負う可能性があると想定される。

プライバシーの観点では住まい手の個人情報が流出する可能性は低いものの、セーフティの観点では状況によっては利用者が重症を負う可能性があることから、「回復困難性の度合い」のレベルは「重大なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、配信前のアップデートが改ざんされた上でその不正なアップデートが流されることによって、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よる経済活動の中断等は生じる可能性があると想定される。

「内外への直接影響（外部）」の観点では、不正なアップデートプログラムによってアップデートプログラムを適用した多くのガス給湯器の利用者にも影響が及ぶことに加え、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と想定される。

「直接影響の継続時間」の観点では、ガス給湯器の故障等の不具合が認められる可能性があり、修理や交換に一定の時間を要する可能性があると想定される。

「代替可能性」の観点では、保守用端末に関するサービスの停止を余儀なくされる上に、他のサービスで代替できる可能性は低いと想定される。

間接的な経済影響の観点では、不正なアップデートが流されることによって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の責任のもとで、大規模な製品回収が生じ得ると想定される。

直接的な経済影響及び間接的な経済影響の観点も含め、「経済的影響の度合い」が大きくなりにくい

と想定されることから、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

③　マッピング結果の整理と評価の実施

上記を踏まえ、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて、ステークホルダーごとに第 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」からカテゴライズし、マッピングする。

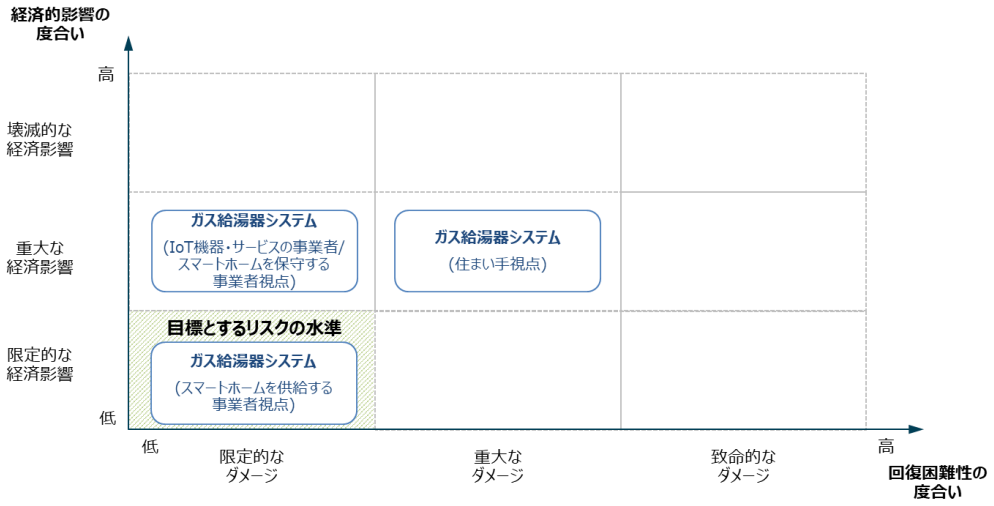


図 14 各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

住まい手視点からみたガス給湯器システムの「回復困難性の度合い」及び「経済的影響の度合い」は比較的大きくなると想定される。住まい手がガス給湯器システムのインシデントにより、やけど等の直接的な被害を受ける可能性があること、また、ガス給湯器システムのインシデントが住まい手の生活（例：けがやけど等によって風呂に入れない、毎日の通院を余儀なくされる等）に影響を及ぼしやすいためである。

IoT 機器・サービスの事業者や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視点からみたガス給湯器システムの「回復困難性の度合い」は限定的であるものの、「経済的影響の度合い」は重大になると想定される。ガス給湯器システムの運用段階におけるインシデントが、当該事業者における従業員のけがや個人情報流出等には直結することは想定しがたいものの、製品に何らかの重大な欠陥や不正な機能が発見され、大規模な製品回収等につながった場合に、多額の対応費用が計上され得るためである。

一方で、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「回復困難性の度合い」及び「経済的影響の度合い」は目標とする水準内に収まると想定される。ガス給湯器システムのインシデントが、スマートホームを供給する事業者が保有するデータの情報流出や従業員のけがにはつながらず、スマートホームへの製造工程や販売工程等の経済活動に影響を与えるとは考えにくいため、「回復困難性の度合い」及び「経済的影響の度合い」にも大きな影響を与えないからであると考えられる。

これらを踏まえると、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は、目標とする水準内に収まっているものの、住まい手、IoT 機器・サービスの事業者及びスマートホームを供給する事業者視点のガス給湯器システムは、目標とする水準には収まっていない。

651 したがって、適用主体である IoT 機器・サービスの事業者（ガス給湯器等の製造元）は、これらのガス
652 給湯器システムがもつリスクを、可能な限り目標とする水準に収めることを目的として、例えば、以下の
653 ように影響度が大きいリスクに対処するための対策方針を明確にすることで、以降の行うべきと考えら
654 れる対策[25]等の検討を行うことができると考えられる。

655 ● 住まい手にとって影響度が大きいリスクに対処するための対策方針
656 ➢ 自社製品の利用者をけがややけどから守る安全対策の徹底
657 ➢ 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
658 ➢ 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、
659 セキュリティ・バイ・デザインの取組みの推進

660 ● 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影響度が大きいリスクに対
661 処するための対策方針
662 ➢ 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

663 上記で示した対策方針を添付 A に示す対策要件と比較した上で、対応関係を整理することによって、
664 本稿で整理した対策要件のうち、行うべきと考えられる対策を明らかにすることができる。

665 表 5 影響度が大きいリスクに対処するための対策方針及び添付 A に記載された対策要件との関係性

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
住まい手	自社製品の利用者をけがややけどから守る安全対策の徹底	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
IoT 機器・サービスの事業者	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
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	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

666

667 (3) リスク対応（ステークホルダー別の対策例一覧）

668 ① システムを構成する機器ごとの脅威の整理

669 システムを構成する機器・システムごとに想定される脅威（例）は以下の通り。

670 表 6 想定される脅威（例）

システムを構成する機器	想定される脅威（例）	生じ得るインシデント（例）
ガス給湯器	不正利用	悪意のある住まい手により、ガス給湯器が意図しない用途等で利用される。
	不正改造	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より、ガス給湯器内の情報処理に関わっているコンポートネント（例：ネットワークインターフェース、MCU）を不正に改造される。
専用コントローラ	マルウェア感染	外部からの悪意のある攻撃によって、専用コントローラがマルウェアに感染する。
	不正利用	専用コントローラが正規の住まい手によって不正に意図しない用途等で利用される。

ルータ	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、ルータに不正アクセスされる。
	不正利用	ルータが正規の住まい手によって不正な設定等で利用される。
スマートフォン	情報漏えい	スマートフォンのアプリケーションから個人情報等が漏えいする。
	マルウェア感染	外部からの悪意のある攻撃によって、スマートフォンのアプリケーションがマルウェアに感染する。
	利用者によるセキュリティ設定の誤り等	住まい手によるスマートフォンアプリケーションのセキュリティ設定が、スマートホーム向け IoT 機器・サービスの事業者が想定する方法や内容ででなされない。
	データの改ざん	スマートフォンから発信される指示情報等がネットワーク上で改ざんされる。
クラウドサービス	情報漏えい	クラウドサービスに保存された利用者の個人情報が漏えいする。
	サービス不能	クラウドサービスが Wi-Fi ルータやネットワークカメラなどを起点とした大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	クラウドサービスが認可されていない主体により不正にアクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、クラウドサービス内の構成要素がマルウェアに感染する。

.

② 脅威への対策の整理

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。

表 7 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[26]	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
		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
		不正アクセス	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 情報漏えい	暗号化によるデータの保護
		データの改ざん 情報漏えい	ライフサイクルに応じた暗号鍵の管理
		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
		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
		不正アクセス マルウェア感染	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
		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

[26] 「全般」は特定の脅威でなく、様々な脅威に対して共通に有効な対策であることを示す。

		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　整理した対策に対する意思決定

対策等を検討する際には、インシデントによる影響の度合いだけでなく、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ような対策を検討する。

- 対策の適用対象（どの機器を中心に検討するか）

想定しているインシデントが発生した際に想定される被害の大きさ及び起こりやすさ等を考慮して、資産であるガス給湯器、専用コントローラ、ルータ、スマートフォン・アプリ、クラウドサービス等から、特に対策を検討すべき資産を検討する。

被害の大きさという観点では、本稿で想定する環境に所在する「住まい手」以外のヒトや、居宅内に設置されているガス給湯器システム以外の機器・システムにも影響すると思われる以下の資産を中心として対策を検討すべきである。

- クラウドサービス、スマートフォン・アプリ
  特定の利用者だけでなく、同様のアプリケーションを利用する者全体に対して影響が波及し得る。
- ルータ
  建物内のネットワークに接続するガス給湯器システム以外の機器・システムにも被害を拡大させるおそれがある。一般的に消費者側で対策の必要性を認識していない場合があるため、利用者への周知啓発を行うことも有効であると考えられる。

また、「起こりやすさ」の観点では、外部からのネットワーク経由での攻撃に対して十分に対処する必要があるため、インターネットに直接接続されている資産（例：ルータやクラウドサービス等）を中心として対策を検討することが望ましい。

- 適用する対策の内容（どのように対策を実施するか）

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より、より効率的・効果的にリスクを低減できるものを中心として対策を検討する。具体的には、深刻とされているリスクに対してセキュリティ上、基本的かつ確実に効果が期待できる対策や、一つの対策で複数の脅威に対処できるものを実施することが望ましい。

上記(2)リスクアセスメントでは、各ステークホルダー視点でガス給湯器のリスクを評価した上で、表 5 にて影響度が大きいリスクに対処するための対策方針や行うべきと考えられる対策要件を整理した。また、既存の文書[27]では、例えば、専用コントローラやガス給湯器等の IoT 機器を対象とする初期設定パスワードの変更、脆弱性に関する情報の公開、セキュリティアップデートに関する対策は、特に大きな効果が短期間で得られるとされている。

したがって、上記(2)で示したリスクアセスメントの結果や既存の文書を踏まえ、本ユースケースでは、

[27] 英国デジタル・文化・メディア・スポーツ省 ”Code of Practice for consumer IoT security” （2018 年 10 月）参照

以下の対策要件を行うべきと考えられる対策に設定した。
なお、ここで行うべきと考えられる対策以外のものであっても、事業者のリスクに対する認識やセキュリティ対策に割けるリソース、IoT 機器の利用環境等によっては積極的に実装を検討すべき項目となる場合がある。したがって、以下に記載されていない対策についても何ら実装を妨げるものではない。
　また、ステークホルダー関連図には記載されていないものの、セキュリティインシデントによっては、スマートホーム向け IoT 機器・サービスの事業者はガス供給事業者と連携した対応が求められ得ることにご留意いただきたい。

- 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
- 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
- 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
- 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

　上記を踏まえて、ガス給湯器システムがもつリスクが受容可能なリスクの水準に収めることを目的として、IoT 機器・サービスの事業者が実装することとした対策要件の例を以下に示す。
　第 1 の観点では、スマートホーム向け IoT 機器の事業者がガス給湯器の遠隔操作に関する新たなサービスの企画段階において、主に当該事業者や住まい手視点のガス給湯器システムのリスクを抑えることを目的として実装することとした対策要件を整理した。
　第 2 の観点では、スマートホーム向け IoT 機器の事業者が企画したガス給湯器の遠隔操作に関するサービスの運用中において、主に当該事業者、スマートホーム向けにメンテナンス及びサポートを行う事業者視点のガス給湯器システムのリスクを抑えることを目的として実装することとした対策要件を整理した。
　第 3 の観点では、スマートホーム向け IoT 機器の事業者が当該事業者及びスマートホーム向けにメンテナンス及びサポートを行う事業者視点のガス給湯器システムのリスクを抑えることを目的として、スマートホーム向けにメンテナンス及びサポートを行う事業者に対する要求事項の特定等の対策要件を整理した。
　第 4 の観点には、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネットの構築等）が該当するため、本ユースケースにてこれらに該当する対策要件は実装しないこととした。

736 表 8 スマートホーム向け IoT 機器の事業者における実際に講じる対策要件の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● ガス給湯器システムを含む自社が提供する IoT 機器・システムを対象としたセキュリティポリシー（情報セキュリティ関連規定を含む）の策定及び適切な承認権限を有する者の承認 ● 定められた期間ごとの当該ポリシーのレビュー	
2			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	● ガス給湯器システムを対象としたセキュリティ管理責任者及びセキュリティ対策担当者の任命 ※ 上記の管理責任者及び開発担当者は、ガス給湯器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。	
3			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・システムのセキュリティ対策の設計・開発・運用等における関係各社の責任範囲の決定 ● 運用中に発生したセキュリティインシデントにより損害が発生した場合の責任範囲（役割分担や損害賠償）の決定	
4			IoT 機器・システムに係る要員のセキュリティ確保	● 委託する業務に関わる者に対するセキュリティ上の要求事項の規定（退職後も含む） ● 自社内の要員に対する適切な訓練及びセキュリティ教育の実施	
5		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	● 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）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遵守	○ （「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」に有効と考えられる対策）
6			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	○ （「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」に有効と考えられる対策）
7			適切な水準のアクセス制御の実装	● 想定されるリスクの大きさを考慮した方式による、ユーザや IoT 機器の認証 ● クラウド上のアプリケーションへの特権アクセスに対して、多要素認証等の強度の高い認証方式の適用認証済みのユーザまたはアプリケーション等に対する最小権限の原則の適用[28] ● 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、通信経路上での保護）	
8			ソフトウェアの完全性の検証	● ガス給湯器システムのソフトウェアに関する完全性の検証機能の実装	
9			ソフトウェアのインストールの制限	● ガス給湯器システムにインストール可能なソフトウェアの種類に関する厳密な方針の策定及び実装	

[28] JPCERT/CC によると、最小特権の原則とは場面に応じて必要最小限の権限だけを与えるようにする原則であり、この原則を守ることで、実際にインシデントが発生した場合の被害を最小限に抑えることができるとされている。

10			様々なIoT機器に接続する際のセキュリティの確保	● ガス給湯器等を他のIoT機器等に接続する際のホワイトリストの適用 ● 識別情報を登録している機器（ガス給湯器等）によるクラウドサービスへの接続に限り許可	
11			暗号化によるデータの保護	● ルータ等による適切な強度の方式による通信経路（住居宅内及び住居外）の暗号化 ● クラウドサービス上に保管されている利用者データ等の暗号化 ※ ガス給湯器等に対して暗号化等のデータ保護措置を十分に講じることが難しい場合、当該機器に機微なデータが保管しない等の代替的な措置をとる。	
12			ライフサイクルを通じた暗号鍵の管理	● 暗号鍵の利用、保護及び有効期間に関するポリシーの策定及び遵守	
13			マルウェア対策の実施	● クラウドサービスにおけるマルウェア対策ソフトウェアの導入 ● ルータにおけるマルウェア対策ソフトウェアの導入	
14			IoT 機器・システムの十分な可用性の確保	● ガス給湯器システムを構成するクラウドサービス等に対する(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 ● クラウドサービス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	
15			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[29]等）の実装 ● ガス給湯器に実装された安全機能と外部との通信回線との分離	○ （「自社製品の利用者をけがややけどから守る安全対策の徹底」及び「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」に有効と考えられる対策）
16			セキュアな開発環境と開発手法の適用	● セキュアコーディング手法の適用 ● 委託先を含む開発人員向けのセキュリティ対策、開発環境やコードへのアクセスの制御、開発環境と運用環境の分離等、安全な開発環境に必要な対応の実施 ● 設計書、プログラム、バイナリ等のバックアップ	
17			IoT機器・システムにおけるセキュリティ機能の検証	● コード分析ツール又は脆弱性スキャナのような自動化ツール等を活用したセキュリティ機能に関する検証の実施 ● クラウドサービス（アプリケーション部分）及びガス給湯器に対するペネトレーションテストの実施	
18			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	○ （「自社製品の利用者をけがややけどから守る安全対策の徹底」に有効と考えられる対策）

[29] 「予防安全機能」の概要については、経済産業省「電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドライン」の「5．予防安全機能について」を参照

				● ルータ等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）を有した居宅内無線 LAN への接続を促すガイダンスの提供	
19	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	● 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、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	○ （「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」に有効と考えられる対策）
20			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	● セキュリティ管理責任者及びセキュリティ対策担当者が異動した場合の後任の選任	
21			過去対応事例からの学習	● 発生したセキュリティインシデントの分析や解決から得られた知見の将来的なインシデント抑制への活用（他社の IoT 機器・システムにおけるセキュリティインシデントを含む）	
22		プロシージャ	インシデント対応手順の整備	● ガス給湯器システムその他の自社が提供する IoT サービスに適応したインシデント対応手順の整備 ● 各要員の役割と責任の識別及び指定された個人によって実行されるアクションの定義・伝達 ● 事業継続上重要な機能を有する外部サービスプロバイダに対する自組織のインシデント対応手順の伝達および内容調整 ● インシデント対応手順の定期的な訓練（自組織と外部プロバイダとの間で連携を要する部分も含む） ● ※ セキュリティの観点に加え、セーフティの観点を考慮する。	
23			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	○ （「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」に有効と考えられる対策）
24		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	● 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）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遵守	
25			継続的な資産管理の実施	● クラウドサービスに接続するガス給湯器等に関する資産目録（機器上に実装されたソフトウェアおよびファームウェア、工場出荷時の設定等を含む）の作成・維持	
26			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管理する ● 施錠可能な文書保管庫での及び関連書類（設計書、仕様書、検証計画書、妥当性確認計画書）の保護の管理	○ （「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」に有効と考えられる対策）

27			IoT 機器・システムのモニタリング及びログの取得、分析	● ガス給湯器システムを構成するクラウドサービスやスマートフォン上のアプリケーション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	
28			IoT 機器・システムに対するアップデートの適用	● 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 ● 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 ● 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へのセキュリティパッチの提供	○ （「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」に有効と考えられる対策）
29	第 3 の観点	ソシキ・ヒト	IoT 機器・システムの運用・管理を行う者への要求事項の特定	● 以下の内容を含む、住まい手に能動的な行動を促すための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への要求事項の明確化 - 使用条件 - 使用上のリスク・注意点 - 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	
30			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	● 明確化した住まい手に能動的な行動を促すための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への要求事項の遵守の確認 ● ソフトウェアアップデート時の注意事項の遵守の確認	

737 ● スマートホームを供給する事業者に対応を依頼すべき対策要件の例

738 表 9 スマートホームを供給する事業者に対応を依頼すべき対策の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	IoT 機器・システムにおける運用開始時の正しい設置、設定	● IoT 機器の事業者から提供されたガイドに従った設置、設定 ● IoT 機器の事業者の想定する仕様に適合したネットワーク環境の整備	

739 ● 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対応を依頼すべき対策要件の例

740 表 10 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対応を依頼すべき対策の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 2 の観点	ソシキ・ヒト	IoT 機器・システムの適正な使用	● ガス給湯器システムを対象としたサービス提供や管理のポリシー提示及び遵守 ● セキュリティパッチの適用手順の提示	

2		プロシージャ	IoT 機器・システムの適正な運用・保守	● スマートホーム向け IoT 機器の事業者が提示するガイドに従った保守、管理	

741 ● 住まい手に対応を依頼すべき対策要件の例

742 表 11 住まい手に対応を依頼すべき対策の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	信頼できる IoT 機器やサービスの選定	● 個人情報を含む様々なデータ管理などのポリシーやセキュリティ対策に留意した上で、適切なガス給湯器及びクラウドサービスの選択。	
2	第 2 の観点	プロシージャ	IoT 機器・システムの用途・用法を守った使用	● 仕様書や手順書を把握し、想定された用途・方法でのガス給湯器の使用。	
3		システム	法的及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）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遵守。	

743

2-3-2 ドローンを活用した個人による写真撮影

「IoT 機器・システムを通じて提供されるサービスの開発者」である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を記載する。

本事業者は、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の周辺環境への影響等を考慮した上で、実際にドローンを製造・販売する前に対象機器・システムに関するリスクアセスメントを行い、適切なリスク対応策を特定することで、可能な限り、リスクを低減することを IoT-SSF 適用の目的とする。

(1) リスクアセスメント、リスク対応に向けた事前準備

① 対象ソリューションの概要

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で風景を撮影することを想定している。なお、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こと、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ことについては利用者が責任を持つものと想定している。

また、ドローンの重さが 200g以下であることから、飛行高度が 150m 以上[30]となることがあるものとする。

- 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。

図 15 対象ソリューションの概要

[30] 本稿執筆段階の 2022 年 1 月現在では、200g 未満のドローンは航空法の対象とならないとされている。

② ステークホルダー関連図

本稿にて関与する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」を想定する。

- ドローン製造事業者

ドローンを製造し、家電量販店や EC サイト等のチャネルにて利用者等へ販売する事業者である。また、本ユースケースにおいて、主にセキュリティ対策を実施する事業者である。

- 利用者

ドローンを購入し、操作する者である。なお、本ユースケースではドローン操作に関する特別な技能を有していないものとする。

- ドローンの飛行箇所の周辺にいる第三者

利用者やドローン製造事業者とは直接関係はないものの、ドローンが想定外の動きをすることによって、被害を受ける可能性のある者。

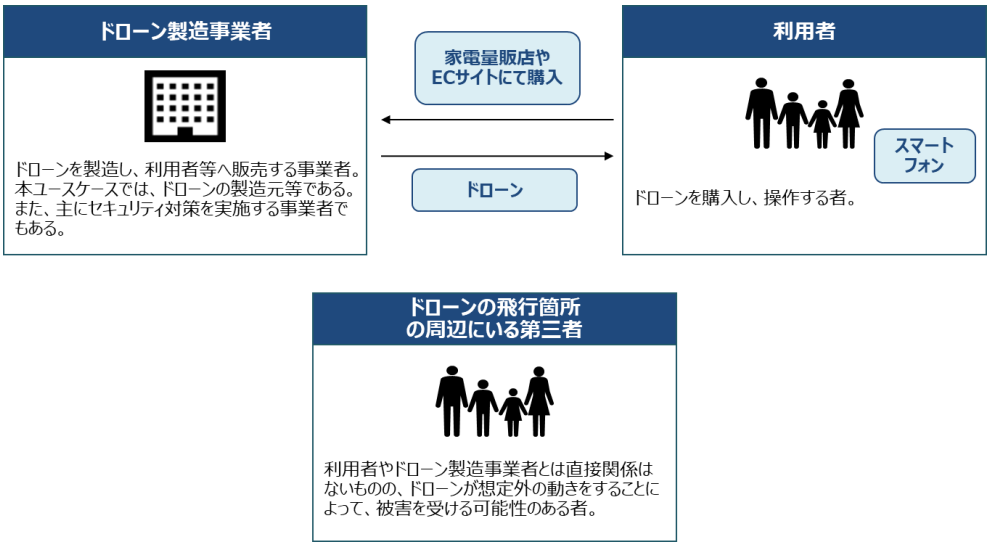


図 16 ステークホルダー関連図

③ システムを構成する機器の一覧

本稿の対象となる機器は以下の通りである。

表 12 システムを構成する機器の一覧

システムを構成する機器	内容
ドローン	カメラが内蔵されたドローン。 画像データは SD カードに保存を行い、利用者自らがスマートフォンへ画像データを転送する。 ドローン製造事業者はドローンの主な用途を個人の風景撮影と設定するものの、他の用途での利用を排除していない。 ドローンの重さは、199g、飛行速度は水平:10 m/s、上昇:3 m/s、下降:3 m/s を想定。 なお、ドローンの構成要素としては、例えば以下が挙げられる。 ● センサ:GPS、ジャイロ(角速度)センサ、加速度センサ、気圧センサ ● アクチュエータ:プロペラ

コントローラ	ドローンの飛行を操縦する機器。 ドローン製造事業者がドローンと併せて販売・製造を行うことを想定。 このコントローラには、製造者側で利用者を認証する仕組みを実装するものとする。
スマートフォン	ドローンが撮影した画像データを転送・確認するためのスマートフォン。 なお、本ユースケースではリスクマネジメントの直接の対象とはしない。
クラウドサービス	スマートフォンから転送された画像データを保存するサービス。 ドローン製造事業者等が提供するサービスではなく、一般に提供されている写真ストレージサービスを想定する。したがって、本ユースケースではリスクマネジメントの直接の対象とはしない。

④ システム構成図、データフロー図

ドローン製造事業者側で想定しているシステム構成図は以下の通りとする。

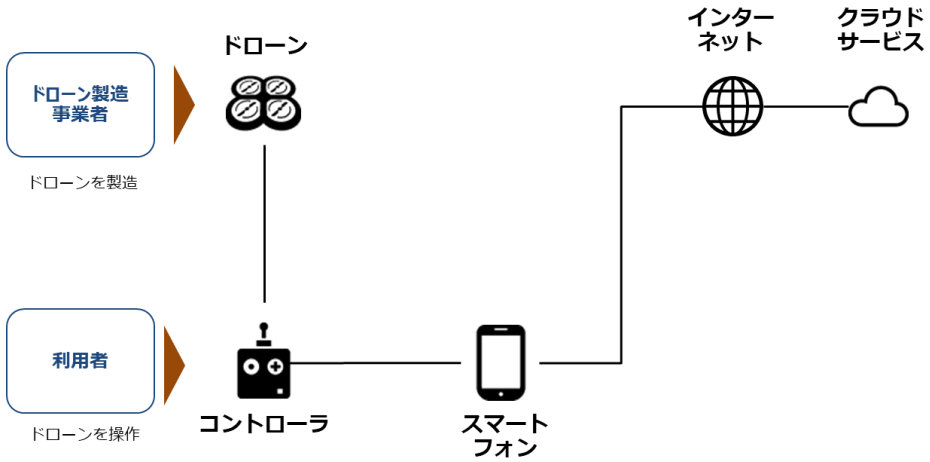


図 17 システム構成図

例えば、公共施設内の土地で許可を取得した上で、利用者がドローンに設置されたカメラにて風景を撮影する場合のデータフローは以下の通りとする。

1. コントローラからドローンに制御データを送信
2. ドローンからコントローラ経由にてスマートフォンに画像データを送信
3. スマートフォンからクラウドサービスに画像データを送信

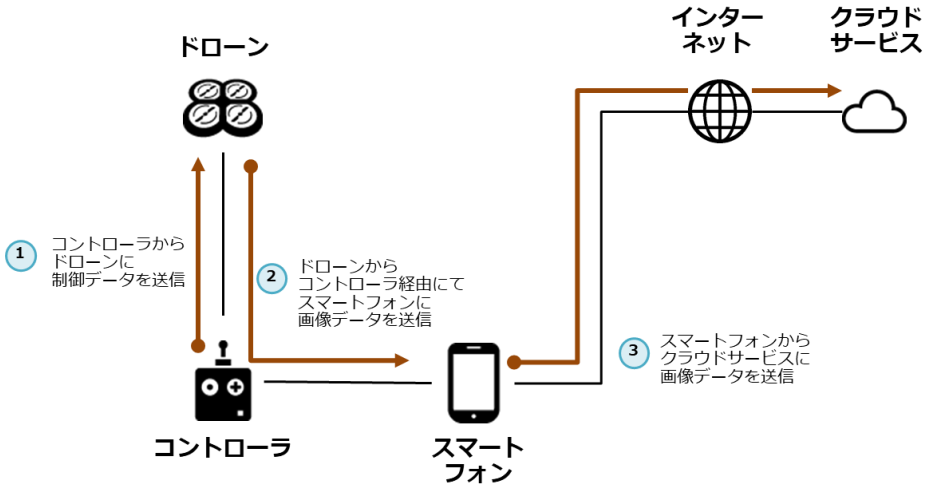


図 18 データフロー図（一部を抜粋）

⑤ リスク基準

「回復困難性の度合い」は、自社が定めるセキュリティやセーフティ等に関する基本方針にのっとり、利用者による製品の利用において重大な事故（例：高高度からのドローンの落下、ドローンの落下に伴う周囲の環境への損害）等がないよう、セキュリティ、セーフティの対策を通じて可能な限り生じ得る被害の度合いを「限定的なダメージ」に抑えることを目指す。

「経済的影響の度合い」は、自社の事業規模を考慮し、大規模な製品回収等が生じないよう、可能な限り「限定的な経済影響」に抑えるものとする。

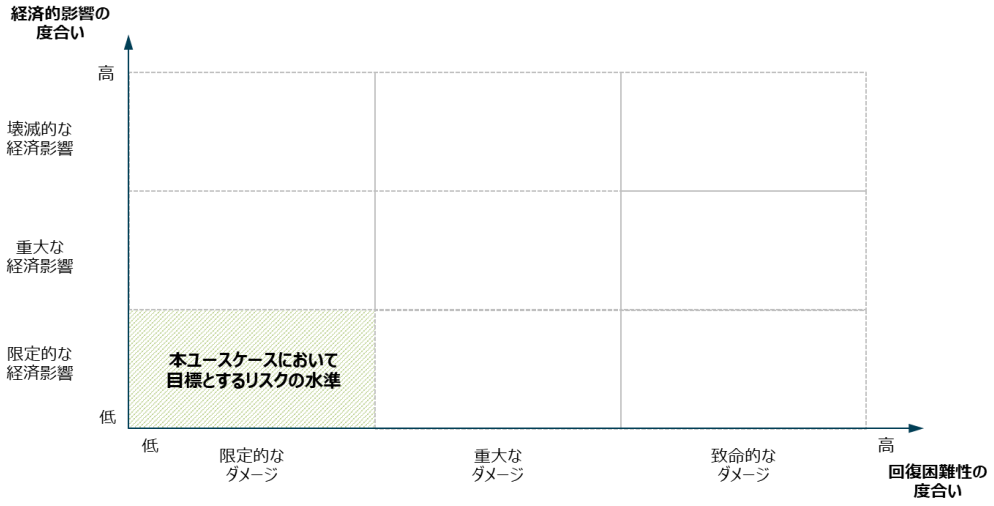


図 19 ドローンにて目標とするリスクの水準

(2) リスクアセスメント

「回復困難性の度合い」及び「経済的影響の度合い」から、ドローンのリスクアセスメントを行う。

① 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

ドローンにおいて、想定され得るセキュリティインシデント等とその結果（影響）を特定する。ドローンの提供または利用に際して想定されるセキュリティインシデント（例）は以下の通り。

- 悪意のある攻撃者により操縦をするための制御権限が奪われ、ドローンが高高度から墜落する。その結果、ドローンが利用者やドローンの飛行箇所の周辺にいる第三者に当たることによって、これらが重症を負う。
- 悪意のある攻撃者によりドローンに内蔵されたカメラが不正アクセスされる。その結果、撮影したデータが外部へ漏えいする。

② ステークホルダーごとの観点を踏まえたリスクアセスメント

以下に示すステークホルダーごとに「回復困難性の度合い」「経済的影響の度合い」の観点からリスクアセスメントを行う。

- ドローン製造事業者
- 利用者

- ドローンの飛行箇所の周辺にいる第三者

- ドローン製造事業者

A) 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、ドローンが撮影した画像データが流出したとしても、ドローン製造事業者の従業員の情報は含まれておらず、ドローン製造事業者への直接の影響はないと想定される。また、セーフティの観点において、ドローンが攻撃者による機体制御の乗っ取り等により落下した場合においても、ドローン製造事業者への直接の影響はないと想定される。

したがって、プライバシーの観点においてもセーフティの観点においても、ドローン製造事業者の従業員等には直接的な影響はないため、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B) 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、機体制御の乗っ取り等の運用時におけるセキュリティインシデントが発生したとしても、その製造元が運用する製造拠点やその他の活動等の直接的な停止等にはつながりにくく、ドローン製造事業者による経済活動の中断等は生じ難いと想定される。一方で「内外への直接影響（外部）」の観点では、運用時におけるセキュリティインシデントが発生することによって、一部の消費者によるドローンの買い控え等が生じると想定される。

「直接影響の継続時間」の観点において、ドローンの故障等が発生した後であっても、同様の製品は比較的流通していると考えられ、大きな影響はないと想定される。

「代替可能性」の観点において、本ユースケースにて想定するインシデントが発生したとしても、事業活動のバックアップが必要になるような経済活動（例：自社工場の停止）等にはつながらないため考慮しない。

ただし、間接的な経済影響の観点において、ドローンに重大な脆弱性が発見された場合、大規模な製品回収につながる可能性があると想定される。

したがって、直接的な経済影響は限定的であると想定されるものの間接的な経済影響は重大であると想定されるため、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

- 利用者

A) 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、内蔵されたカメラから利用者本人が映り込んだ画像や利用履歴等が流出することから、個人情報等が漏えいする可能性があると想定される。また、セーフティの観点において、撮影高度がある程度高くなることが想定されることからドローンが落下した場合において、利用者が重症を負う可能性があると想定される。

したがって、プライバシーの観点では個人情報等が流出する可能性があり、セーフティの観点では生じ得る損害が利用者の重症となる可能性があると考えられることから、「回復困難性の度合い」のレベルは「重大なダメージ」と評価する。

B) 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では悪意のある攻撃者により操縦をするための制御権限が奪わ

れた場合、ドローンが高高度から落下する可能性がある。その結果、利用者が重症を負うことで生活に支障をきたし得る。また、ドローンによる撮影もできなくなる可能性がある。「内外への直接影響（外部）」の観点においては、ドローンの高高度からの落下により利用者の住居等を傷つける可能性がある。

「直接影響の継続時間」の観点において、ドローンの故障等が発生した場合、製造元に問い合わせた上で、修理手続き等をとらないといけないため、即座に復旧されることは難しいと想定される。

「代替可能性」の観点において、、高高度での撮影を目的としてドローンを購入しているため、同様の製品を新たに購入しない限り、ドローンの代替は難しいと想定される。

間接的な経済影響の観点において、ドローン製造事業者による製品回収が発生したとしても、利用者に対する影響は発生しない。

したがって、直接的な経済影響及び間接的な経済影響を双方踏まえると、利用者への住居や生活に影響を与える可能性があることから、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

- ドローンの飛行箇所の周辺にいる第三者

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、利用者が人通りのあるエリアで撮影を行う可能性があり、内蔵されたカメラから、場合によっては第三者の機微な個人情報等が漏えいする可能性があると想定される。また、セーフティの観点において、撮影高度がある程度高くなることが想定されることからドローンが落下した場合において、第三者が重症を負う可能性があると想定される。

したがって、プライバシーの観点では場合によっては機微な個人情報等が流出する可能性があり、セーフティの観点では生じ得る損害が利用者の重症となる可能性があると考えられることから、「回復困難性の度合い」のレベルは「重大なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

「内外への直接影響」の観点では、攻撃者による機体制御の乗っ取られたドローンによって、第三者が重症を負うことによって、生活に支障をきたす可能性がある。

「直接影響の継続時間」や「代替可能性」の観点において、ドローンの故障等が発生したとしても、第三者に対する大きな影響は発生しない。

間接的な経済影響の観点において、ドローン製造事業者による製品回収が発生したとしても、第三者に対する影響は発生しない。

したがって、直接的な経済影響及び間接的な経済影響を双方踏まえると、第三者が重症を負うことによって生活に影響を及ぼし得ることから、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

③ マッピング結果の整理と評価の実施

上記を踏まえ、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて、ステークホルダーごとに第 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」からカテゴライズし、マッピングする。

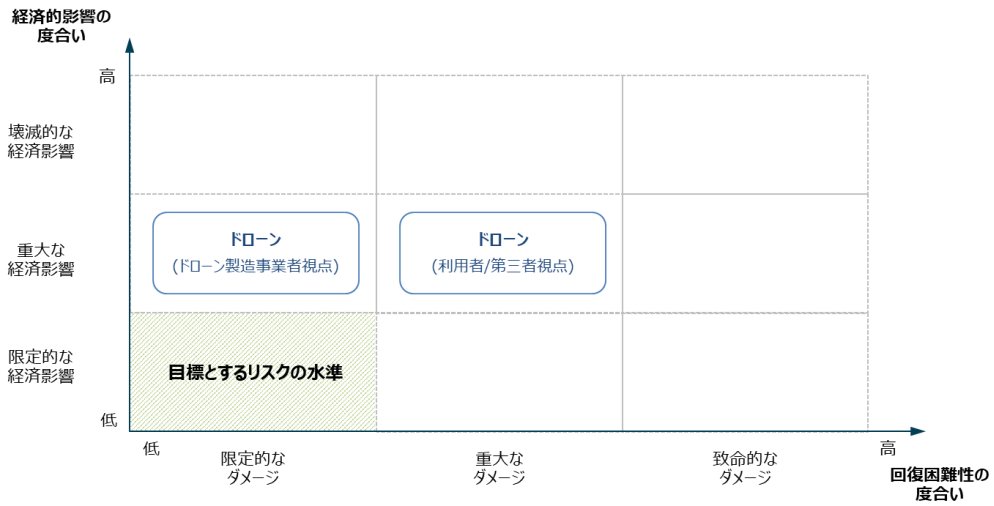


図 20 各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

ドローン製造事業者視点からみたドローンの「回復困難性の度合い」は小さくなるものの、「経済的影響の度合い」は比較的大きくなる。これは、当該事業者における従業員のけがや個人情報流出等には直結しないものの、製品に何らかの重大な欠陥や不正な機能が発見され、大規模な製品回収等につながった場合に、多額の対応費用が計上され得るためである。

利用者やドローンの飛行箇所の周辺にいる第三者視点からみたドローンの「回復困難性の度合い」及び「経済的影響の度合い」は重大になる。これは、ドローンが「回復困難性の度合い」に与える影響が利用者や第三者を問わず直接危害を加える可能性があることに加えて、その影響が周辺の環境に対して及ぶことが想定され、「経済的影響の度合い」が併せて大きくなるためである。

これらを踏まえると、ドローン製造事業者及び利用者視点のドローンは、目標とするリスクの水準には収まっていない。

したがって、適用主体であるドローン製造事業者は、これらのドローンの利用において想定されるリスクを目標とするリスクの水準に可能な限り収めることを目的として、例えば、以下のように影響度が大きいリスクに対処するための対策方針を明確にすることで、以降の行うべきと考えられる対策等の検討を行うことができると考えられる。

- ドローン製造事業者にとって影響度が大きいリスクに対処するための対策方針
  - 「経済的影響の度合い」の観点

    ドローン製造事業者にとっては、重大な脆弱性やその他の欠陥が発見されることによって大規模な製品回収が発生することが大きなリスクであり、以下のように、製品の企画、設計の段階からこうしたリスクに対して意識的に取り組むことが有効である。
    - ✧ 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

- 利用者にとっての影響度が大きいリスクに対処するための対策方針
  - 「回復困難性の度合い」の観点

    利用者にとっては、自身が映り込んだ画像データが意図せずして流出することや、操作する

ドローンが落下した際に重症を負うことが主要なリスクである。これらのリスクに対応するため以下の対策が有効であると考えられる。

- ✧ 利用者への注記喚起の実施
- ✧ フェールセーフ等を含む安全対策の徹底

- ➢ 「経済的影響の度合い」の観点

利用者自身がドローンの落下等によりけがを負うことによって普段の生活に支障が生じたり、近隣の家屋や住民に危害が加わることで金銭的な補償等が発生し得たりすることがリスクである。これらのリスクに対応するため以下の対策が有効であると考えられる。

- ✧ 利用者への注記喚起の実施
- ✧ フェールセーフ等を含む安全対策の徹底

● ドローンの飛行箇所の周辺にいる第三者にとって影響度が大きいリスクに対処するための対策方針

- ➢ 「回復困難性の度合い」の観点

ドローンの飛行箇所の周辺にいる第三者にとっては、意図せずして自身が映り込んだ画像データが流出することや、ドローンが落下してきた際に自身に直撃することによってけがを負うことがリスクである。これらのリスクに対応するため以下の対策が有効であると考えられる。

- ✧ 利用者への注記喚起の実施
- ✧ フェールセーフ等を含む安全対策の徹底

- ➢ 「経済的影響の度合い」の観点

ドローンの飛行箇所の周辺にいる第三者にとっては、落下したドローンが直撃した結果負うけがで普段の生活に支障が生じることや、落下したドローンが自身の所有する建物等に直撃し、これらが破損することがリスクとして想定される。これらのリスクに対応するため以下の対策が有効であると考えられる。

- ✧ フェールセーフ等を含む安全対策の徹底

上記で示した対策方針を添付 A に示す対策要件と比較した上で、対応関係を整理することによって、本稿で整理した対策要件のうち、行うべきと考えられる対策を明らかにすることができる。

表 13 影響度が大きいリスクに対処するための対策方針及び添付 A に記載された対策要件との関係性

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
ドローン製造事業者	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	利用者への注意喚起の実施や推奨事項の明確化	利用者へのリスクの周知等の情報発信

		IoT 機器・システムの適正な使用
		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
ドローンの飛行箇所の周辺にいる第三者	利用者への注意喚起の実施や推奨事項の明確化	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
		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) リスク対応（ステークホルダー別の対策例一覧）

① システムを構成する機器ごとの脅威の整理

システムを構成する機器ごとに整理した脅威は以下の通り。

表 14 想定される脅威（例）

システムを構成する機器	想定される脅威（例）	生じ得るインシデント(例)
ドローン	情報漏えい	ドローンに設置されたカメラ内部に保存された画像データ等が漏えいする。
	サービス不能	ドローンが大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正改造	ドローンに対する不正（違法）なハードウェア、ソフトウェアの改造により、内部データを抜き取り、脆弱性の要因を組み込まれる。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	不正利用	攻撃者によりドローンが乗っ取られ、取り扱い説明書に記載された用途以外で利用される。
コントローラ	データの改ざん・消去	コントローラの制御情報等が改ざんされる
	サービス不能	コントローラが大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	コントローラが攻撃者により不正なアクセスを受ける。
	マルウェア感染	コントローラが外部からの攻撃によりマルウェアに感染する。
	踏み台	コントローラが乗っ取られ踏み台になる。
	不正改造	コントローラに対する不正（違法）なハードウェア、ソフトウェアの改造により、内部データを抜き取り、脆弱性の要因を組み込まれる。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。

② 脅威への対策の整理

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。

表 15 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　整理した対策に対する意思決定

対策等を検討する際には、インシデントによる影響の度合いだけでなく、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ような対策を検討する。

- 対策の適用対象（どの機器を中心に検討するか）

想定しているインシデントが発生した際に想定される被害の大きさ及び起こりやすさ等を考慮して、システムを構成する機器であるドローン、コントローラから、特に対策を検討すべき機器を検討すべきであるが、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。なお、前述の通り、スマートフォン、クラウドサービスは本ユースケースで想定するステークホルダー以外の事業者が提供する機器・サービスであることから、リスク対応の対象外とする。

- 適用する対策の内容（どのように対策を実施するか）

本ユースケースの特徴は、2―3―1 と同様にドローンの利用者が IT に関する知見を有していない可能性があることに加え、公共空間でドローンが飛行することによって、ドローンが第三者に対して被害を及ぼす可能性があるということである。

ドローン製造事業者は、利用者や飛行箇所の周囲にいる第三者がけが等をしないよう利用者に対して、ガイドにてセキュリティに関する設定方法及び利用方法等について十分な説明や注意喚起を行うことが望ましい。

したがって、本ユースケースでは、以下の対策要件を行うべきと考えられる対策に設定した。

- 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
- 利用者へのリスクの周知等の情報発信
- IoT 機器・システムの適正な使用
- 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

上記を踏まえて、ドローンがもつリスクを目標とする水準に収めることを目的として、IoT 機器・サービ

スの事業者が実装することとした対策要件の例を以下に示す。

第 1 の観点では、ドローン製造事業者がドローンに関する新たなサービスの企画段階において、ドローン製造事業者、利用者や飛行箇所の周囲にいる第三者視点のドローンのリスクを抑えることを目的として実装することとした対策要件を整理した。

第 2 の観点では、ドローンの販売後において、ドローン製造事業者、利用者や飛行箇所の周囲にいる第三者視点のドローンのリスクを抑えることを目的として実装することとした対策要件を整理した。

第 3 の観点では、ドローン製造事業者が利用者や飛行箇所の周囲にいる第三者視点のドローンのリスクを抑えることを目的として、利用者に対する要求事項の特定等の対策要件を整理した。

第 4 の観点は、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネットの構築等）が該当するため、本ユースケースにてこれらに該当する対策要件は実装しないこととした。

表 16 ドローン製造事業者における実際に講じる対策要件の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● ドローン及び周辺機器を対象としたセキュリティポリシー（情報セキュリティ関連規定を含む）の策定及び適切な承認権限を有する者の承認。 ● 定められた期間ごとの当該ポリシーのレビュー。	
2			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	● 設計部門または製造部門におけるセキュリティ管理責任者及びセキュリティ担当者の任命。 ● 情報セキュリティ部門において自社製品のセキュリティを担当する要員の明確化。 ※ 上記の管理責任者及び開発担当者は、ドローンのライフサイクルの各段階（例：開発、運用）において明確化されていることが望ましい。	
3			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	● ドローン及び周辺機器の運用段階等における利用者との責任分界の決定。	
4			IoT 機器・システムに係る要員のセキュリティ確保	● 設計部門または製造部門の人員に対して製品のセキュリティ確保に関する適切な訓練及びセキュリティ教育を実施。	
5		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	● 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。	○ （「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」に有効と考えられる対策）
6			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。	○ （「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」に有効と考えられる対策）
7			IoT 機器・システムの十分な可用性の確保	● ネットワークが停止しても、ドローンが動作を継続してローカルで動作し続ける仕組みの構築。	

8			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。	○ （「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」及び「フェールセーフ等を含む安全対策の徹底」に有効と考えられる対策）
9			セキュアな開発環境と開発手法の適用	● セキュアコーディング手法の適用。 ● 委託先を含む開発人員向けのセキュリティ対策、開発環境やコードへのアクセスの制御、開発環境と運用環境の分離等、安全な開発環境に必要な対応の実施。 ● 設計書、プログラム、バイナリ等のバックアップ。	
10			IoT 機器・システムにおけるセキュリティ機能の検証	● ドローン及び周辺機器に対するペネトレーションテストの実施。	
11			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	● 機体の初期パスワードの変更を促す機能の実装。	
12	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	● 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。	○ （「利用者への注意喚起の実施や推奨事項の明確化」に有効と考えられる対策）
13			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	● 保守部門におけるセキュリティ管理責任者及びセキュリティ担当者の任命。 ● 情報セキュリティ部門において自社製品のセキュリティを担当する要員の明確化。	
14			過去の対応事例からの学習	● 発生したセキュリティインシデントの分析や解決から得られた知見の将来的なインシデント抑制への活用。（他社の IoT 機器・システムにおけるセキュリティインシデントを含む）	
15		プロシージャ	脆弱性対応に必要な手順等の整備と実践	● 脆弱性に関する問題を報告するための連絡窓口の設置。 ● 入手した脆弱性情報に対する対処手順の策定。	
16			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	○ （「利用者への注意喚起の実施や推奨事項の明確化」に有効と考えられる対策）
17		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	● 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）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遵守。	
18			プログラムソースコード及び関連書類の保護	● 最小限の人員によるプログラムソースコード及び関連書類（例えば、設計書、仕様書、検証計画書、妥当性確認計画書）へのアクセスの限定。 ● アクセスログのレビューの定期的な実施。	

19			IoT 機器・システムに対するアップデートの適用	● 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。 ● 開発部門等への修正プログラム等開発の依頼。 ● ホームページを通じたセキュリティパッチの提供。	
20	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。	○ （「利用者への注意喚起の実施や推奨事項の明確化」に有効と考えられる対策）

986 ● 利用者に対応を依頼すべき対策要件の例

987 ドローン製造事業者が全ての対策を行うことは現実的に難しいため、安全なドローンの稼働を目的と
988 して、利用者に対して主に以下の対策要件を実装するよう依頼する。

989 表 17 利用者に対応を依頼すべき対策の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	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	● 機体の初期パスワードの変更。	
2	第 2 の観点	プロシージャ	IoT 機器・システムの適正な運用・保守	● 利用者に対して提示した取り扱い説明書に従った管理。	
3		システム	IoT 機器・システムに対するアップデートの適用	● 適切な方法でのホームページを通じて提供されたセキュリティパッチの適用。	
4			IoT 機器・システムの安全な廃棄または再利用	● ドローンを廃棄するに当たって、ドローン内部やカメラに保存されている情報の削除。	

990

2-3-3 物流倉庫内の AGV による自動ピッキング

本項では、「IoT 機器・システムを通じて提供されるサービスの開発者」である物流事業者が 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を記載する。

物流事業者は、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。なお、既に在庫管理等を支援する倉庫管理システムは導入済である。

本ユースケースでは、IoT 機器の利用者（物流事業者）が対象機器・システムの稼働前にリスクアセスメント及びリスク対応を行い、それでもなお残存するリスクに対しては運用時にも脆弱性対応等を依頼することで、可能な限りリスクを低減させることを目的とする。

(1) リスクアセスメント、リスク対応に向けた事前準備

① 対象ソリューションの概要

ある物流事業者が運用する工業用間接資材を扱う物流倉庫において、庫内の資材搬送業務の効率化のため、無人搬送車（以下、「AGV」という。）が自動ピッキングを行うケースを想定する。

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。作業員は保管棚から対象となる製品をピッキングする作業を行う。

なお、作業員が作業行うピッキングエリアと AGV の稼働する保管エリアは保護柵等で区切られており、かつ、AGV が低速で進むことを前提としている。

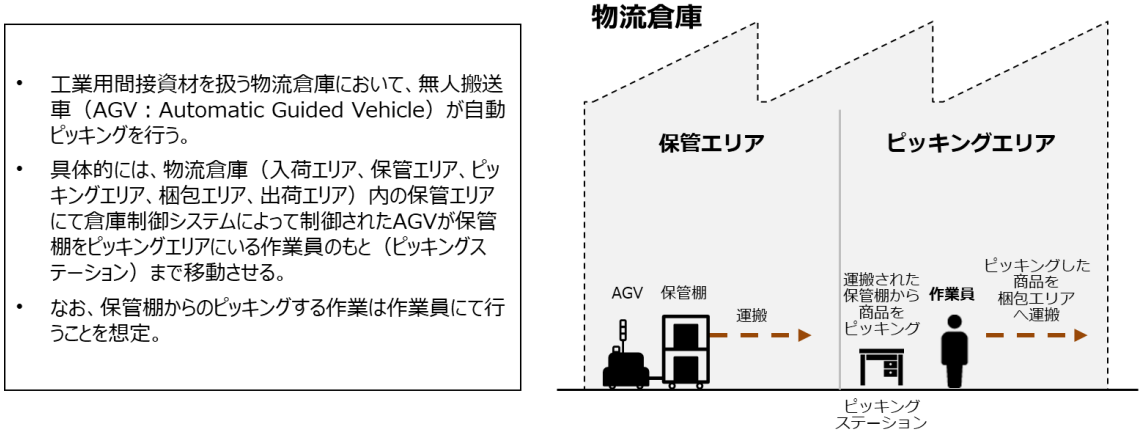


図 21 対象ソリューションの概要

② ステークホルダー関連図

本稿にて関与するステークホルダーは、「物流事業者（委託元企業）」「システムインテグレータ（システム開発の委託先企業）」、「AGV 製造事業者」を想定している。

- 物流事業者（委託元企業）

物流倉庫を運用する事業者であり、本サービスにおいて、中心となって IoT 機器・システムに関して対

策要件を実装する主体である。本事業者の主な顧客となる製造事業者等は工場並びに生産設備システムを所有しており、物流機能の一部を本事業者に委託していると想定する。なお、当該物流倉庫の稼働は 24 時間、年中無休を想定している。

- システムインテグレータ（システム開発の委託先企業）

物流事業者からの委託を受け、AGV を組み込んだ倉庫管理システム及び倉庫制御システムを開発する事業者。物流事業者が定めた仕様に従ってシステム全体の設計、供給、製造などを行い、倉庫管理システム及び倉庫制御システムを物流事業者に納入する。。なお、物流事業者とは保守契約を結ぶことを想定しており、倉庫管理システム及び倉庫制御システムのアップデートを配信する。また、AGV の調達及び保守については、システム開発及び保守の一環として物流事業者から受注しており、AGV 製造事業者と契約して実施することを想定している。

- AGV 製造事業者

AGV を製造し、関連する保守サービスを含めてシステムインテグレータに提供する事業者を想定している。AGV のアップデートをシステムインテグレータ経由にて配信することを想定している。

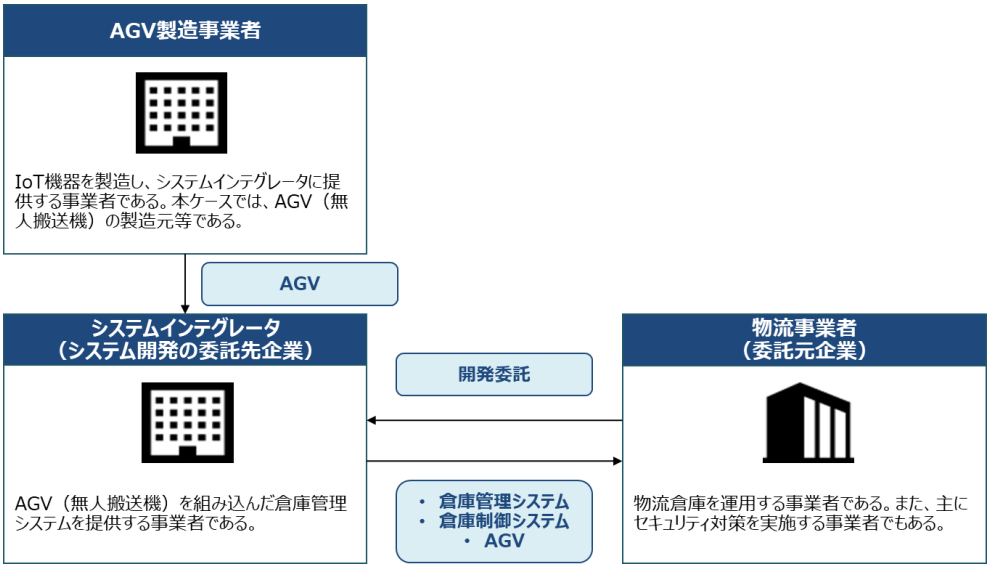


図 22 ステークホルダー関連図

③ システムを構成する機器の一覧

本稿の対象となる機器は以下の通りとする。

なお、以下の機器を包括したシステムを物流倉庫システムと表現するものとする。

表 18 システムを構成する機器の一覧

システムを構成する機器	内容
倉庫管理システム （WMS：Warehouse Management System）	在庫管理、在庫引き当て、出荷指示等を行うシステム。 倉庫管理システムは、オンプレミスにて物流倉庫内にサーバを設置するものとする。 なお、倉庫管理システムは、例えば以下の機能を有するものとする。 ● 入庫管理機能 ● 出庫管理機能 ● 在庫管理機能

	● 棚卸管理機能
操作用端末	倉庫管理システムや倉庫制御システムを操作する端末。 操作用端末はスタンドアロンにて物流倉庫内に設置するものとする。
保守用端末	倉庫管理システムや制御システムの保守を行う端末。 保守用端末はスタンドアロンにて物流倉庫内に設置するものとする。
倉庫制御システム (WCS:Warehouse Control System)	AGV を対象として、工程別指示や制御指示等を行うシステム。 倉庫制御システムは、オンプレミスにて物流倉庫内にサーバを設置するものとする。 なお、倉庫制御システムは、例えば以下の機能を有するものとする。 ● AGV 等の設備の管理機能 ● AGV 等の設備の制御機能
安全制御 PLC (PLC:Programmable Logic Controller)	停電等の有事の際に、作業員による安全確保の処理がなされるまでは勝手に稼働しないような「安全な仕組み」を提供する PLC。 安全制御 PLC は、倉庫内に設置するものとする。
AGV	自動で保管棚を搬送する IoT 機器。 AGV は、倉庫内の保管エリアのみで稼働するものし、倉庫内で常時稼働するものとする。 最大積載量 500 kg、前進移動速度 60m/分(500kg 負荷時)を想定。 日本工業規格 JIS　D 6802「無人搬送車システム−安全通則」に準拠していることを想定。

④　システム構成図、データフロー図

システム構成図は以下の通りとする。

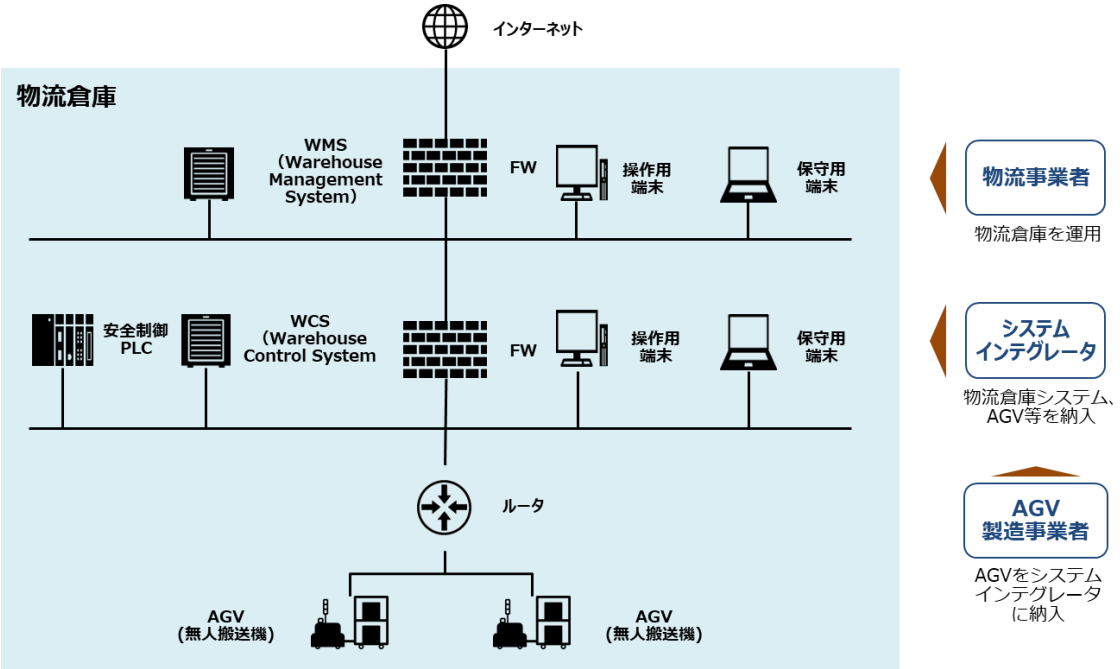


図 23 システム構成図

物流事業者の倉庫管理システムが工場外部の受発注システムから売上データを受領して、対象の商品をピッキングする場合のデータフローは以下の通りとする。

1. 外部の受発注システムから倉庫管理システム(WMS)が売上データを受領
2. 倉庫管理システム(WMS)から倉庫制御システム(WCS)に出荷指示を送信
3. 倉庫制御システム(WCS)から AGV に搬送指示を送信

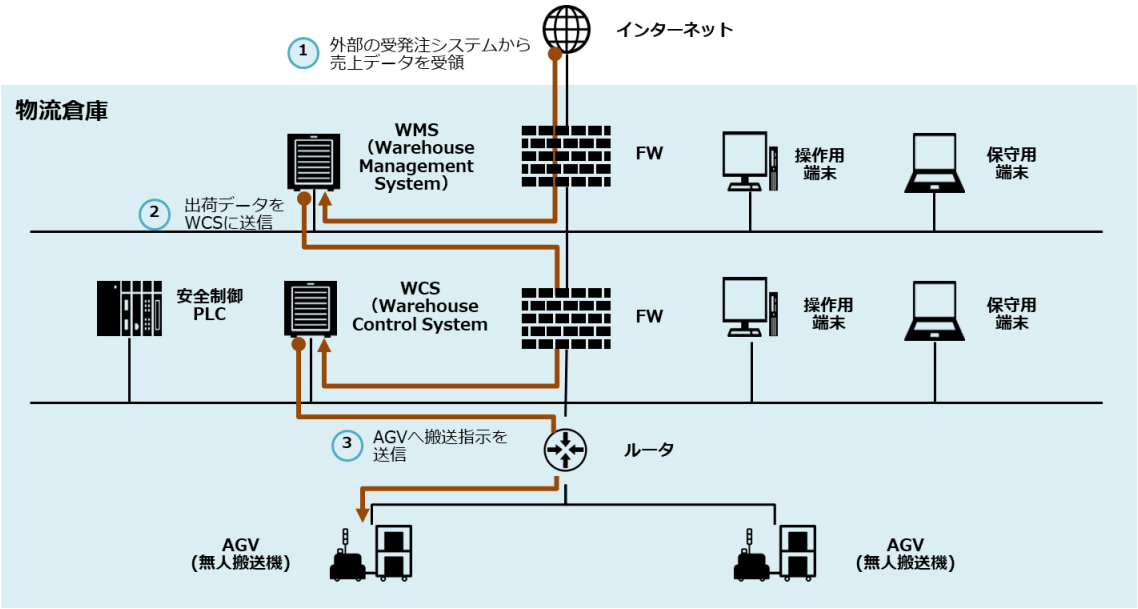


図 24 データフロー図（一部を抜粋）

⑤ リスク基準

「回復困難性の度合い」は、自社が定めるセキュリティやセーフティ等に関する基本方針にのっとり、物流倉庫内の作業員に重大な事故等が発生しないよう、セキュリティ、セーフティの対策を通じて生じ得る被害の度合いを「限定的なダメージ」に抑えることを目指す。

また、「経済的影響の度合い」は、大規模な誤配送が生じないよう「限定的な経済影響」に抑えるものとする。

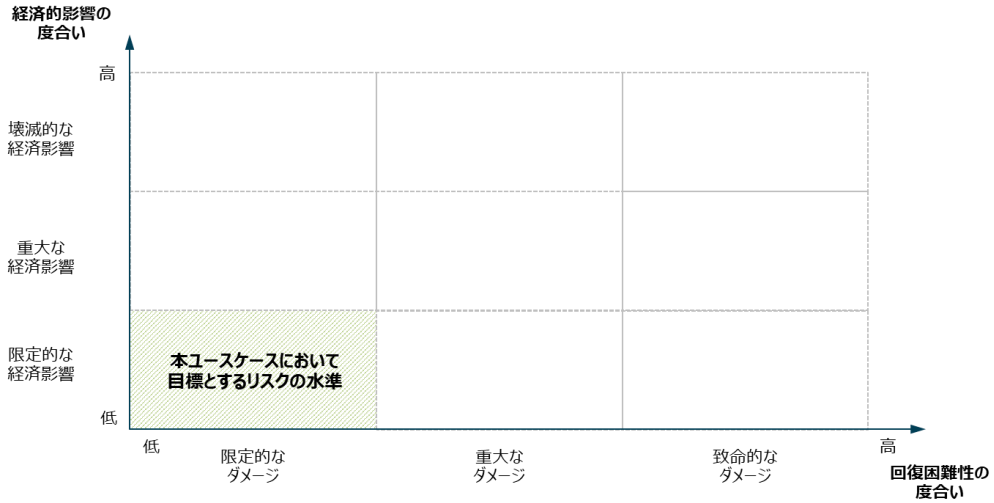


図 25 物流倉庫システムにて目標とするリスクの水準

(2) リスクアセスメント

「回復困難性の度合い」及び「経済的影響の度合い」から、物流倉庫システムのリスクアセスメントを行う。

① 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

倉庫管理システム、倉庫制御システム及び AGV 等において、想定され得るセキュリティインシデント等とその結果（影響）を特定する。倉庫管理システム、倉庫制御システム、AGV 等の利用に際して想定されるセキュリティインシデント（例）は以下の通り。

- 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アクセスされる。その結果、顧客情報が流出する。
- 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アクセスされる。その結果、保存されている在庫情報が改ざんされ、配送の停止や誤配送が生じる。
- 不正な外部記憶媒体（USB メモリ等）を挿入された保守用端末を通じて倉庫制御システムがマルウェアに感染する。その結果、AGV が停止することで、庫内の資材搬送業務が停止する。
- システムインテグレータから、ネットワークを通じた不適切な内容を含むアップデートの配信、もしくはローカル環境での不適切な内容を含むアップデートの実行がなされる。その結果、倉庫管理システム、倉庫制御システム及び AGV 等が想定しない動きをすることで庫内の資材搬送業務が停止する。

② ステークホルダーごとの観点を踏まえたリスクアセスメント

以下に示すステークホルダーごとに「回復困難性の度合い」「経済的影響の度合い」の観点からリスクアセスメントを行う。

- 物流事業者
- システムインテグレータ
- AGV 製造事業者

- 物流事業者

A) 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、AGV 等から稼働情報が漏えいする可能性があるものの、物流事業者の従業員の個人情報等が漏えいする可能性は低いと想定される。セーフティの観点においては、作業員が作業するエリアと AGV が稼働するエリアが保護柵で分けられており、かつ、AGV が低速で進むことを前提としているため、ピッキングステーションで商品を集荷する作業員が AGV の誤作動により、重症を負う可能性は低く軽傷で済む可能性が高い。

したがって、プライバシーの観点では個人情報等が流出する可能性があること、セーフティの観点では軽傷を負う可能性があることから、「回復困難性の度合い」のレベルは「限定的なダメージ」とする。

B) 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、倉庫制御システムがマルウェアに感染し AGV が停止する

ことによって倉庫内の経済活動（庫内の資材搬送業務）の中断や資材の誤配送等が生じる可能性がある。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。加えて、「内外への直接影響（外部）」の観点において、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の影響が及ぶ可能性がある。本件倉庫が多数の在庫を抱えていることを踏まえると、大規模なシステムの障害等が生じた際には、稼働している全 AGV の停止やそれに伴う AGV の修理・交換が必要となった場合、自社のみならず多数の取引先の事業活動に大きな影響を及ぼすことが想定される。

「直接影響の継続時間」の観点においては、障害等が発生した後、AGV の修理や交換に一定の時間を要する可能性があり、業務の停止や効率低下等の影響がすぐには解消されないものと想定される。

「代替可能性」の観点において、AGV が停止した際には集荷を人力で行う必要が生じ、大規模な物流機能を維持するための高い出荷能力を保てない可能性が高いと想定される。

また、間接的な経済影響の観点において、AGV の修理や交換に一定のコストを要する可能性がある。

したがって、直接的な経済影響及び間接的な経済影響を双方踏まえると、広範囲に影響が及ぶ可能性があり、サプライチェーン全体の経済活動も停止する可能性があることから、全体の経済影響は非常に大きくなると想定されるため、「経済的影響の度合い」のレベルは「壊滅的な経済影響」とする。

- システムインテグレータ

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、倉庫管理システム、倉庫制御システム、AGV 等からシステムインテグレータの従業員の個人情報等が漏えいする可能性はなく、また、セーフティの観点においても AGV 等に関する事故がシステムインテグレータに及ぼす可能性はないと考えらえる。

したがって、プライバシーの観点では個人情報等が流出する可能性が低いこと、セーフティの観点でもけがを負う可能性が低いことから、「回復困難性の度合い」のレベルは「限定的なダメージ」とする。

B） 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、不正なアップデートを倉庫管理システム、倉庫制御システム、AGV 等に配信した場合、物流事業者のシステムに対する影響範囲を確認する必要があるため、システムインテグレータの経済活動等の直接的な停止につながると想定される。また、「内外への直接影響（外部）」の観点では、倉庫管理システム等を提供している他の物流事業者への影響を確認する必要が生じるため、少なからず影響が生じると想定される。

「直接影響の継続時間」の観点において、不正なアップデートを倉庫管理システム、倉庫制御システム、AGV 等に配信した場合、物流倉庫の現場は混乱をきたしすぐに復旧するとは考えにくい。

「代替可能性」の観点において、不正なアップデートを倉庫管理システム、倉庫制御システム、AGV 等に配信した場合、代わりとなる仕組みを即座に用意することはできない。

間接的な経済影響の観点において、倉庫制御システム等に重大な脆弱性が発見され、システムインテグレータの責任において工場が停止した場合、製品回収が生じる可能性があると想定される。

したがって、直接的な経済影響は重大であり、間接的な経済影響も重大であると想定されるため、「経済的影響の度合い」のレベルは「重大な経済影響」とする。

- AGV 製造事業者

A)　発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、AGV 等から AGV 製造事業者の従業員の個人情報等が漏えいする可能性はなく、また、セーフティの観点においても AGV 等に関する事故がシステムインテグレータに及ぼす可能性はないと考えらえる。

したがって、プライバシーの観点では個人情報等が流出する可能性が低いこと、セーフティの観点でもけがを負う可能性が低いことから、「回復困難性の度合い」のレベルは「限定的なダメージ」とする。

B)　発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、AGV のサイバーセキュリティに関する故障等により、AGV 製造事業者の経済活動等の直接的な停止につながるとは想定しにくい。また、「内外への直接影響（外部）」の観点では、AGV のサイバーセキュリティに関する故障等により他の企業による買い控えが生じる可能性があると想定される。

「直接影響の継続時間」の観点において、AGV のサイバーセキュリティに関する故障等により、物流倉庫の現場は混乱をきたしすぐに復旧するとは考えにくい。

「代替可能性」の観点において、AGV のサイバーセキュリティに関する故障等が生じた場合、代わりとなる仕組みを即座に用意することはできない。

ただし、間接的な経済影響の観点において、AGV に重大な脆弱性が発見され、AGV 製造事業者の責任において工場が停止した場合、製品回収が生じる可能性があると想定される。

したがって、直接的な経済影響は重大であり、間接的な経済影響も重大であると想定されるため、「経済的影響の度合い」のレベルは「重大な経済影響」とする。

③　マッピング結果の整理と評価の実施

上記を踏まえ、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて、ステークホルダーごとに第 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」からカテゴライズし、マッピングする。

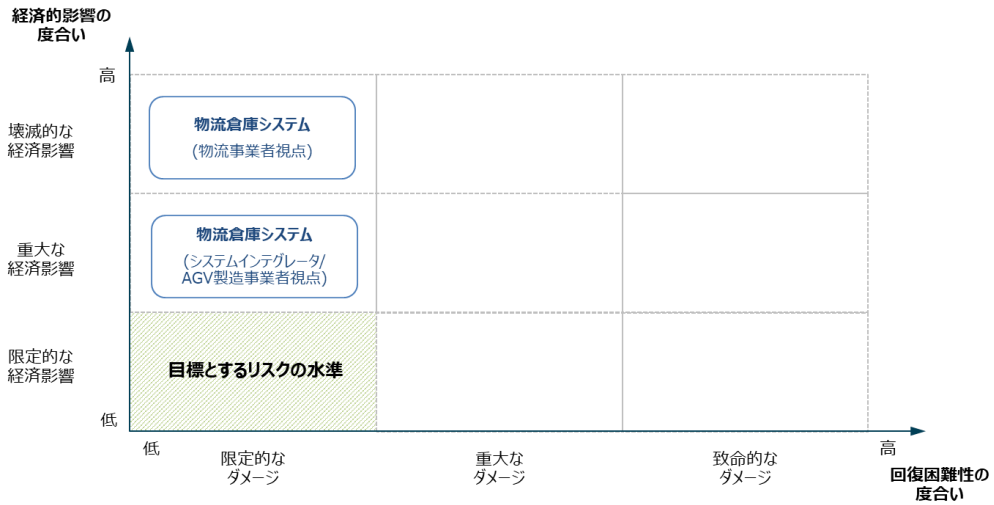


図 26　各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

物流事業者視点からみた物流倉庫システムの「回復困難性の度合い」は低くなるものの、「経済的影響の度合い」は、大きくなる。これは、当該事業者における従業員のけがや個人情報流出等には直結することは想定しがたいものの、物流倉庫システムに何らかの重大な欠陥や不正な機能が発見され、物流倉庫システムの停止につながった場合に、工場が停止し損害を被るためである。

システムインテグレータ、AGV 製造事業者視点からみた対象の機器・システムの「回復困難性の度合い」は物流事業者視点の物流倉庫システムと同様に低くなる。一方で、物流事業者視点の物流倉庫システム程の被害ではないものの、「経済的影響の度合い」は重大になると想定される。これは、各々の経済活動は停止しないものの、製品回収が生じる可能性があるためである。

これらを踏まえると、物流事業者、システムインテグレータ及び AGV 製造事業者視点の対象の機器・システムにおいて想定されるリスクは、目標とするリスクの水準には収まっていないため、適用主体である物流事業者は、これらの対象の機器・システムがもつリスクを目標とするリスクの水準に収めることを目指して対策を行う。

例えば、以下のように影響度が大きいリスクに対処するための対策方針を明確にすることで、以降の行うべきと考えられる対策等の検討を行うことができると考えられる。

- 物流事業者にとって影響度が大きいリスクに対処するための対策方針
  - 経済的影響の度合いの観点

    物流事業者にとっては、自身が運用する倉庫の長時間の稼働停止及び、それに伴う取引先を含む広範囲にわたるサプライチェーンの途絶等が重要なリスクとなるが、これらのリスクに対応するため以下の対策が有効であると考えられる。
    - ✧ 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
    - ✧ 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

- システムインテグレータにとって影響度が大きいリスクに対処するための対策方針
  - 経済的影響の度合いの観点

    システムインテグレータにとっては、開発や保守を担当する倉庫管理システムや倉庫制御システムにおいて、自身の過失（アップデート等を実行する保守端末の管理不備）により契約違反が生じ得ることがリスクである。これらのリスクに対応するため、物流事業者から以下の対策の実施をシステムインテグレータに依頼することが望ましい。
    - ✧ 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

上記で示した対策例を添付 A に示す対策要件と比較した上で、対応関係を整理することによって、本稿で整理した対策要件のうち、行うべきと考えられる対策を明らかにすることができる。

表 19 影響度が大きいリスクに対処するための対策方針及び添付 A に記載された対策要件との関係性

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
物流事業者	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	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) リスク対応（ステークホルダー別の対策例一覧）

① システムを構成する機器ごとの脅威の整理

システムを構成する機器ごとに整理した脅威は以下の通り。

表 20 想定される脅威（例）

システムを構成する機器	想定される脅威（例）	生じ得るインシデント（例）
倉庫管理システム (WMS：Warehouse Management System)	データの改ざん	倉庫管理システムに保存された情報（例：入庫管理情報、在庫管理情報、出荷管理情報、棚卸管理情報等）が改ざんされる。
	情報漏えい	倉庫管理システムに保存された情報（例：入庫管理情報、在庫管理情報、出荷管理情報、棚卸管理情報等）が漏えいする。
	サービス不能	倉庫管理システムが外部からの大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、倉庫管理システムに不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、倉庫管理システムがマルウェアに感染する。
	不正利用	倉庫管理システムが正規の物流事業者の事業員によって不正に意図しない用途等で利用される。
	利用者によるセキュリティ設定の誤り等	物流事業者の従業員による倉庫管理システムのセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
操作用端末	データの改ざん	操作用端末に保存された情報が改ざんされる。
	情報漏えい	操作用端末に保存された情報が漏えいする。
	サービス不能	操作用端末が外部からの大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、操作用端末に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、操作用端末がマルウェアに感染する。
	不正利用	操作用端末が正規の物流事業者の事業員によって不正に意図しない用途等で利用される。
	利用者によるセキュリティ設定の誤り等	物流事業者の従業員による操作用端末のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
保守用端末	データの改ざん	保守用端末に保存された情報が改ざんされる。
	情報漏えい	保守用端末に保存された情報が漏えいする。
	サービス不能	保守用端末が外部からの大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、保守用端末に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、保守用端末がマルウェアに感染する。
	不正利用	保守用端末が正規の物流事業者の事業員によって不正に意図しない用途等で利用される。
	利用者によるセキュリティ設定の誤り等	物流事業者の従業員による保守用端末のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。

倉庫制御システム (WCS：Warehouse Control System)	データの改ざん	倉庫制御システムに保存された情報（例：AGV 等の設備の管理情報、AGV 等の設備の制御情報等）が改ざんされる。
	情報漏えい	倉庫制御システムに保存された情報（例：例：AGV 等の設備の管理情報、AGV 等の設備の制御情報等）が漏えいする。
	サービス不能	倉庫制御システムが外部からの大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、倉庫制御システムに不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、倉庫制御システムがマルウェアに感染する。
	不正利用	倉庫制御システムが正規の物流事業者の事業員によって不正に意図しない用途等で利用される。
	利用者によるセキュリティ設定の誤り等	物流事業者の従業員による倉庫制御システムのセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
安全制御 PLC	サービス不能	安全制御 PLC が外部からの大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、安全制御 PLC に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、安全制御 PLC がマルウェアに感染する。
ルータ	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、ルータに不正アクセスされる。
	不正利用	ルータが正規の住まい手によって不正な設定等で利用される。
AGV	データの改ざん	AGV に保存された情報（例： AGV 等の設備の制御情報等）が改ざんされる。
	情報漏えい	AGV に保存された情報（例： AGV 等の設備の制御情報等が漏えいする。
	マルウェア感染	外部からの悪意のある攻撃によって、AGV がマルウェアに感染する。
	不正利用	AGV が正規の物流事業者の事業員によって不正に意図しない用途等で利用される。
	利用者によるセキュリティ設定の誤り等	物流事業者の従業員による AGV のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。

② 脅威への対策の整理

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物流事業者にて実装が想定される対策要件を整理する。

表 21 物流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
		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
		全般	適切な水準のアクセス制御の実装の要求
		全般	ソフトウェアの完全性の検証
		全般	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
		全般	暗号化によるデータの保護
		全般	ライフサイクルを通じた暗号鍵の管理
		マルウェア感染	マルウェア対策の実施
		全般	IoT 機器・システムの十分な可用性の確保
		全般	適切なネットワークの分離
		全般	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
		データの改ざん 不正アクセス	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
		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の指示
		全般	セキュアな開発環境と開発手法の適用の指示
		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	システムインテグレータに対する 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
		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　整理した対策に対する意思決定

対策等を検討する際にはインシデント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ような対策を検討する。従来、工場や物流拠点等において稼働する制御システムは、ベンダーごとに固有の仕様を多く含み、外部ネットワークや共用システムとは接続されていない等の認識の下で、セキュリティの脅威は殆ど問題視されてこなかった。しかし、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[31]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。

- 対策の適用対象（どの機器を中心に検討するか）

想定しているインシデントが現に発生した際に生じる被害の大きさ及びその起こりやすさ等を考慮して、本稿における倉庫管理システム、操作用端末、保守用端末、倉庫制御システム及び AGV 等の資産から、特に重点的に対策を検討すべき資産を検討する。

被害の大きさの観点では、情報系ネットワークと制御システムネットワークを分離した上で、本稿で想定する物流倉庫の稼働に直接影響を与えると思われる以下のシステム及びその機器を中心として対策を検討すべきである。

- 倉庫管理システム、操作用端末、保守用端末
  倉庫制御システムに対して出庫指示ができなくなる結果、倉庫全体に混乱をもたらし、庫内物流機能がストップする上に、倉庫外部の経済活動にも影響を及ぼす可能性がある。
- 倉庫制御システム、安全制御 PLC、AGV
  人手による出庫ができるため、完全停止までは至らないものの、AGV 等を活用した自動運搬ができなくなった場青ため、大規模な遅延が生じる。

また、起こりやすさの観点では、外部からのネットワーク経由での攻撃に対して十分に対処する必要

[31] 独立行政法人 情報処理推進機構(IPA)「制御システムのセキュリティリスク分析ガイド第2版」(2020年 3 月)参照。

があるため、倉庫外部のネットワークに直接接続されている機器（例：倉庫管理システム、操作用端末及び保守用端末等）を中心として重点的に対策を検討しつつ、その他の資産も含めて多層的に対策要件を実装することが望ましい。

- 適用する対策の内容（どのように対策を実施するか）

②にて検討した物流事業者にて実装が想定される対策要件の例より、より効率的・効果的にリスクを低減できるものを中心として対策を検討する。例えば、制御システムのセキュリティにおいては、情報の機密性よりも可用性や完全性が重視される傾向があり、運用上の制約等も相まって、AGV や AGV を制御する PLC にエンドポイントセキュリティソフトを導入する等の IT 環境では一般的なセキュリティ対策を実施することが難しいケースがある。その場合には、以下の対策要件を実装した上で、より上位のシステムで守る構成とすることにより、効率的・効果的にリスクを低減することが望ましい。

- 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
- 様々な IoT 機器を接続する際のセキュリティの確保
- IoT 機器・システムの十分な可能性の確保
- 適切なネットワークの分離
- セキュリティ設計と両立するセーフティ設計の仕様化
- 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

上記を踏まえて、AGV がもつリスクを目標とする水準に収めることを目的として、物流事業者が実装することとした対策要件の例を以下に示す。

第 1 の観点では、物流事業者が企画段階において、物流事業者、システムインテグレータ及び AGV 製造事業者のリスクを抑えることを目的として実装することとした対策要件を整理した。

第 2 の観点では、物流事業者の運用段階において、物流事業者、システムインテグレータ及び AGV 製造事業者のリスクを抑えることを目的として実装することとした対策要件を整理した。

第 3 の観点については、本ユースケースが対象とする業務やシステムでは法令等による運用担当者への専門資格保有の要求、あるいはそれに相当する業界または社内の人事等に関する慣行は必ずしも認められないと考えることから、システムの仕様について知見を有するシステムインテグレータとの平時または有事の際における協力を念頭に置きつつも、これらに該当する対策要件は必ずしも実装しないこととした。

第 4 の観点には、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネットの構築等）が該当するため、本ユースケースにてこれらに該当する対策要件は実装しないこととした。

なお、第 1 の観点及び第 2 の観点における対策要件のうち、物流事業者単体では対応が難しい対策要件がいくつか見られた。これらの対策要件の実装やその他の技術的支援はシステムインテグレータに依頼することとした。

1252

表 22 物流事業者において実際に講じる対策の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● 対象となっている物流倉庫におけるセキュリティポリシー（例：情報システムを対象としたセキュリティ規定、制御システムを対象としたセキュリティ規定）の策定及び、事業部長等の適切な承認権限を有する者の承認。 ● 定められた期間ごとの当該ポリシーのレビュー。	
2			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	● 各倉庫におけるセキュリティ管理責任者の任命。 ● 本社の情報システム部門における自社倉庫のセキュリティを担当する要員の明確化。 ※ 上記の管理責任者及び開発担当者は、ドローンのライフサイクルの各段階（例：開発、運用）において明確化されていることが望ましい。	
3			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	● 倉庫制御システム及び関連機器(AGV)のセキュリティ対策の設計・開発・運用等における関係各社の責任範囲の決定。 ● 運用中に発生したセキュリティインシデントにより損害が発生した場合の責任範囲（役割分担や損害賠償）の決定	
4			IoT 機器・システムに係る要員のセキュリティ確保	● 自社の要員及び委託する業務（システムインテグレータに対する倉庫制御システムの開発）に関わる者に対するセキュリティ上の要求事項の規定。（退職後または契約後も含む） ● 自社内の要員（倉庫にて業務に従事する要員）に対する適切な訓練及びセキュリティ教育の実施。	
5		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	● 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。	○ （「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」に有効と考えられる対策）
6			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。	○ （「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」に有効と考えられる対策）
7			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	● 外部の物理的な脅威から保護されるべき AGV や AGV 制御 PLC、その他の資産への認可されていないアクセスを防ぐ目的で、入退管理（例：職員証や入館ゲート等）を通じた物理的セキュリティ境界の確立。	
8	第 2 の観点	ソシキ・ヒト	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	● 各倉庫におけるセキュリティ管理責任者の任命。	

				● 本社の情報システム部門における自社倉庫のセキュリティを担当する要員の明確化。 ※ 上記の管理責任者及び開発担当者は、ドローンのライフサイクルの各段階（例：開発、運用）において明確化されていることが望ましい。	
9			過去の対応事例からの学習	● 発生したセキュリティインシデントの分析や解決から得られた知見の将来的なインシデント抑制への活用。（同業他社の IoT 機器・システムにおけるセキュリティインシデントを含む）	
10			サービス提供や管理のポリシーの提示・遵守	● 倉庫制御システムを対象としたセキュリティポリシーの遵守。	
11		プロシージャ	脆弱性対応に必要な体制や手順等の整備と実践	● 本社の情報システム部門における脆弱性情報の収集及び評価の実施。 ● 倉庫制御システムまたは倉庫管理システムに関連した脆弱性が明らかになった場合、これらの脆弱性に対応するための手順の整備。 ● 倉庫制御システムを構成するソフトウェアの脆弱性が明らかになった場合の、対応手順の整備。	
12			インシデント対応手順の整備と実践	● 物流事業者が自身で運用する物流倉庫システムに適応したインシデント対応手順の整備。 ● 各要員の役割と責任の識別及び指定された個人によって実行されるアクションの定義・伝達。 ● システムインテグレータ等に対する自組織のインシデント対応手順の伝達および内容調整。 ● インシデント対応手順の定期的な訓練。（自組織とシステムインテグレータ等との間で連携を要する部分も含む） ※セキュリティの観点に加え、セーフティの観点を考慮する。	
13			事業継続計画の策定と実践	● 危機的な事象が発生した場合に達成すべき事業上の必要性に基づいた復旧目標を規定し、物流倉庫の運用業務に対する事業継続計画の作成。 ● 事業継続計画を支援するバックアップ及び復元の手順の作成。 ※事業継続計画はサイバーセキュリティを主たる脅威として想定したものとなっていることが望ましい。	
14			IoT 機器・システムの適正な使用	● 想定された用途・方法での倉庫管理システム、倉庫制御システム及び AGV 等の使用。	
15			IoT 機器・システムの適正な運用・保守	● システムインテグレータ及び AGV 製造事業者が提示するガイドに従った保守、管理。	
16		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	● 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。	
17			継続的な資産管理	● 物流倉庫システムを構成する資産目録（機器上に実装されたソフトウェアおよびファームウェア、工場出荷時の設定等を含む）の作成・維持 ※物流倉庫システムが長期の運用となることを想定する。	

18			プログラムソースコード及び関連書類の保護	● 物流倉庫システムに係るプログラムソースコード及び関連書類(例:設計文書)への論理アクセスを最小限にした上で、多要素認証の実施	
19			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。	○ (「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」に有効と考えられる対策)
20			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 ● システムインテグレータ等への修正プログラム等開発の依頼 ● パッチの適用前に動作検証を実施。 ● 提供を受けたセキュリティパッチの適用 ※システムインテグレータ等と相談した上で、パッチを適用することが望ましい。	
21			IoT 機器・システムの安全な廃棄または再利用	● 物流倉庫システムを構成する機器(例:AGV や AGV 制御 PLC 等)内部に保存されている情報の削除。(読み取り不可処理を含む)	

1253

1254 ● 委託仕様書に基づきシステムインテグレータが実装する対策の例

1255 物流倉庫システムの開発及び保守を委託しているシステムインテグレータへの委託仕様書等に基づ
1256 いて、システムインテグレータは主に以下の対策要件を実装するものとする。

1257 表 23 委託仕様書等に基づきシステムインテグレータが実装する対策の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	適切な水準のアクセス制御の実装の要求	● 物流倉庫システムにおけるアカウントの管理について、例えば以下のような自動化されたメカニズムの導入・運用。 ● 倉庫管理システム及び倉庫制御システムからアカウント情報の定期的な自動収集	
2			ソフトウェアの完全性の検証	● 倉庫管理システム、倉庫制御システム、操作用端末、保守用端末のソフトウェアに関する完全性の検証機能の実装。	
3			ソフトウェアのインストールの制限	● 倉庫制御システムを構成する機器(例:AGV、AGV 制御 PLC)にインストール可能なソフトウェアをあらかじめ特定した上で、構成を維持できる機能の実装。 ● ※構成を変更する場合は、システムインテグレータ等と相談した上で、ソフトウェアのインストール等を実施することが望ましい。	
4			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。	○ (「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」に有効と考えられる対策)

5			暗号化によるデータの保護	● 適切な強度の方式（IPsec-VPN、SSL-VPN 等）による倉庫外（自社の他拠点）からの通信の保護。 ● 倉庫管理システム、倉庫制御システムに保管されている利用者情報、配送先情報、対象商品情報、システム稼働情報等の暗号化。	
6			ライフサイクルを通じた暗号鍵の管理	● 暗号鍵の利用，保護及び有効期間に関するポリシーの策定及び遵守。	
7			マルウェア対策の実施	● 倉庫管理システム、操作用端末、保守用端末におけるマルウェア対策ソフトウェアの導入。 ● 外部の保存媒体（例：USB メモリ）との接続の制限。	
8			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。	○ （「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」に有効と考えられる対策）
9			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」に有効と考えられる対策）
10			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	● AGV や倉庫管理システム等が設置されている自組織の業務上重要な施設への物理アクセスに対する監視カメラ等によるモニタリング。	
11			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。	○ （「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」に有効と考えられる対策）
12			セキュアな開発環境と開発手法の適用の指示	● 物流倉庫システム開発時のセキュアコーディング手法の適用。 ● 委託先を含む開発人員向けのセキュリティ対策、開発環境やコードへのアクセスの制御、開発環境と運用環境の分離等、安全な開発環境に必要な対応の実施。 ● 設計書、プログラム、バイナリ等のバックアップ。	
13			IoT 機器・システムにおけるセキュリティ機能の検証	● 倉庫管理システムリリース前の倉庫管理システム、操作用端末、保守用端末、倉庫制御システム等に対するペネトレーションテストの実施。	
14			システムインテグレータに対するIoT 機器・システムにおける運用開始時の正しい設置、設定	● 倉庫管理システム、倉庫制御システム、AGV 制御 PLC、操作用端末及保守端末の適切な設置・設定。 ● AGV 製造事業者から提供されたガイドに従った AVG 等の設置及び設定。 ● IoT 機器製造事業者が想定する仕様に適合したネットワーク環境の整備。	

15	第 2 の観点	システム	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。	○ （「安全なアップデートプログラムの配信」に有効と考えられる対策）

1258

2-3-4 化学プラント施設内の蒸留工程の自動制御

「IoT 機器・システムを通じて提供されるサービスの開発者」であるプラント事業者が 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を記載する。

プラント事業者は、一般のビニール製品に広く使用される化学物質を製造する事業者であり、操業開始から既に数十年程度プラントを運用している。当該事業者が製造する化学物質は、装置外部へ流出した場合に人体や環境に悪影響を及ぼす可能性のあるものであり、従来から従業員や立地地域等の安全(セーフティ)や環境の保護に関わる対応を重点的に実施してきたが、昨今世界的にプラント施設等におけるセキュリティインシデントやそれに伴う操業の停止等が多く報告されているため、本社の経営層を中心に機器のオープン化やネットワーク接続等に伴い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するようになっている。

本ユースケースでは、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等を行い、対処が必要なリスクに対しては、自身に加えてシステムインテグレータやプラント事業者向けにメンテナンスやサポートを行う事業者に対応を依頼することで、可能な限りリスクを低減することを目的とする。

(1) リスクアセスメント、リスク対応に向けた事前準備

① 対象ソリューションの概要

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。

本ユースケースでは、主に以下の工程からなる化学プラントを扱うが、その中でも特に 4.の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。

1. 反応工程:原料や酸素等を反応させ化合物を生成する工程
2. 洗浄工程:反応工程で生成された化合物を中和洗浄する工程
3. 分解工程:中和洗浄された化合物を熱によって分解する工程
4. 精製工程(蒸留工程を含む):成分の沸点の差を利用して、分解工程までで生成された化合物を製品用に分離させる工程

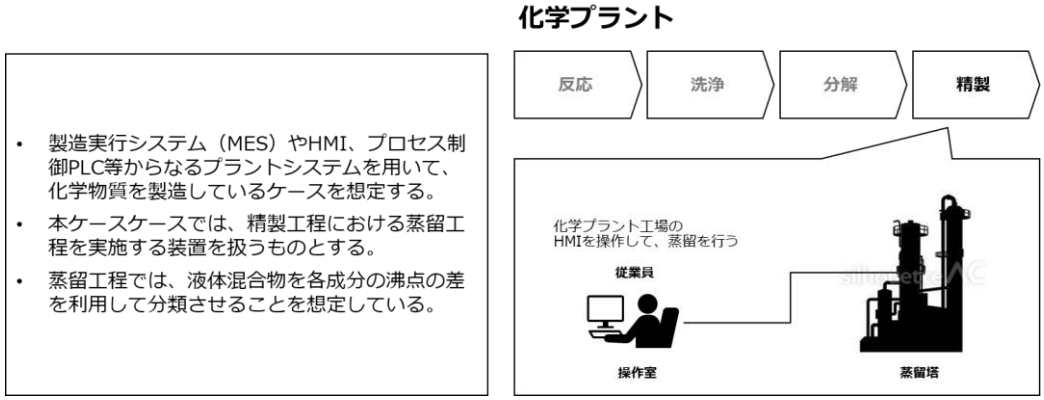


図 27 対象ソリューションの概要

② ステークホルダー関連図

対象の機器・システムの設計や構築、運用に関与するステークホルダーとして、「プラント事業者（委託元企業）」、「システムイングレータ（委託先企業）」「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」を想定している。

- プラント事業者（委託元企業）

プラントを制御するシステムの開発をシステムインテグレータに対して委託した上で、本プラントを運用・管理する事業者であり、セキュリティ対策等の実施に対して主に責任を有する事業者である。本ユースケースで対象とするプラントは、操業開始から数十年が経過しており、設備の一部に老朽化等が見られるものとする。また、プラント事業者において今回リスクアセスメント等の対象となっている事業所におけるセキュリティ対策等の状況は以下の通り。

- リスク管理部門は存在するものの、プラント制御システムを所掌するセキュリティ責任者や担当者は必ずしも明確になっていない。セキュリティポリシーは存在するものの、情報システムのセキュリティに重点が置かれたものになっている。
- 情報システムにおけるセキュリティを念頭に置いた教育は実施されているものの、制御システムにおけるセキュリティを主に扱った教育は実施されていない。
- 情報資産管理台帳（サーバ、クライアント端末、ネットワーク機器、設備等を対象とする）は既に作成済みであり、特に制御システムについては資産の移動や追加の度に担当者が手動でメンテナンスしている。
- 外部ネットワークとプラント内部ネットワークとの境界及び、情報系ネットワークと制御情報系ネットワークとの境界にファイアウォールを導入しているものの、外部の監視サービス等は特に利用していない。
- 自然災害を想定した事業継続計画や、情報漏えいを想定したセキュリティインシデント対応手順は整備済み。

なお、本プラントは農林水産業が盛んな沿岸地域に立地しており、爆発事故が発生した場合には、人体に有害な物質が外部へ流出することで、プラント周辺の住民だけではなく、住民が営む農林水産業にも影響が生じ得るものとする。

- システムイングレータ（委託先企業）

プラント事業者から委託を受けプラントを制御するシステムを開発した上で、委託元企業に対して、プラント装置を制御するプラントシステム一式を提供する事業者である。

- プラントエンジニアリング事業者

プラントの装置を設計・製造し、システムインテグレータに納入する事業者である。また、プラントシステム（例：MES、HMI 等）のアップデートの配信等プラントの装置の保守・管理を行うことも想定している。

- プラント周辺の住民

直接プラント事業者とは関係はないものの、プラントにて事故が発生した場合に、被害を受ける可能

性のある者。

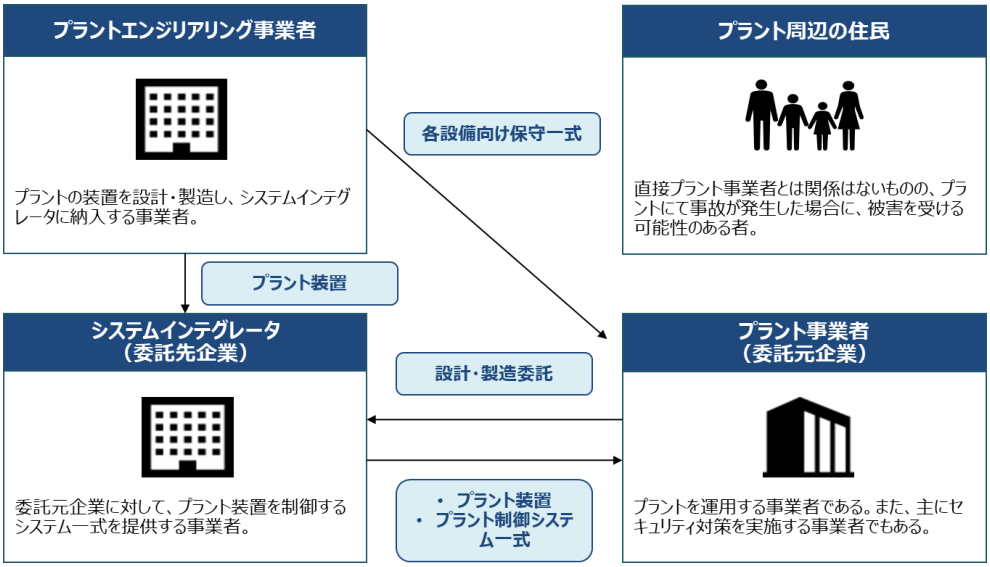


図 28 ステークホルダー関連図

③ システムを構成する機器の一覧

本稿の対象となる機器は以下の通りとする。

表 24 システムを構成する機器の一覧

システムを構成する機器	内容
製造実行システム （MES：Manufacturing Execution System）	製造工程の把握や管理、作業者への指示や支援などを行うサーバ。 MES は、プラント事業者所内にサーバを設置するものとする。 なお、主な機能は以下の通り。 - 作業のスケジュール管理機能 - 作業手配・製造指示機能 - 作業者管理機能 - データ収集機能 - プロセス管理機能 - 製品の追跡と製品体系管理機能 - 実績管理機能 - 生産資源の配分と監視機能 - 仕様・文書管理機能 - 設備の保守・保全管理機能 - 製品品質管理機能
ヒューマンマシンインターフェース （HMI：Human Machine Interface）	人間の操作と機械の動作をスムーズに結合するために使用されるハードウェアとソフトウェア。 具体的には、タッチパネル式の表示器やパネルコンピュータを指す。
プロセスサーバ	プロセス制御 PLC から収集するデータを扱うサーバ。
データヒストリアン	長期間のプロセス値や管理パラメータを保存し、分析を行うためのサーバ。 プロセス制御 PLC からのデータを収集するプロセスサーバより静的なデータ（ヒストリデータ）を扱う。
業務用サーバ/業務用端末	非制御系の情報を保存、利用するサーバ及び端末。 例えば、ファイルサーバやメールサーバ及びそれらを利用する端末を指す。
保守用端末	プラントシステムの保守を行う端末。 保守用端末はスタンドアロンにてプラント内に設置するものとする。
安全制御 PLC （PLC：Programmable Logic Controller）	停電等の有事の際に、作業員による安全確保の処理がなされるまでは勝手に稼働しないような「安全な仕組み」を提供する PLC。 安全制御 PLC は、プラント内に設置するものとする。

プロセス制御 PLC（PLC：Programmable Logic Controller）	センサからの測定値が設定値に一致する様に、偏差から調節方式に応じて算出した操作量を調節するPLC。
蒸留塔温度センサ	蒸留塔の中の温度を計測するセンサ。
蒸留塔加熱器	蒸留塔の中の温度を上昇させるための蒸気を作成する加熱器。

④　システム構成図、データフロー図

システム構成図は以下の通りとする。各種センサ、アクチュエータ類や、PLC、プロセスサーバ等から構成されるプラント制御システムは、セキュリティのレベルやネットワークの種類等に応じてあらかじめ複数の階層（制御情報系ネットワーク、制御系ネットワーク等）に分離されており、インターネット等の外部ネットワークと接続する情報系ネットワークとは最小限の通信しか行わないよう設計、運用されていることを想定する。

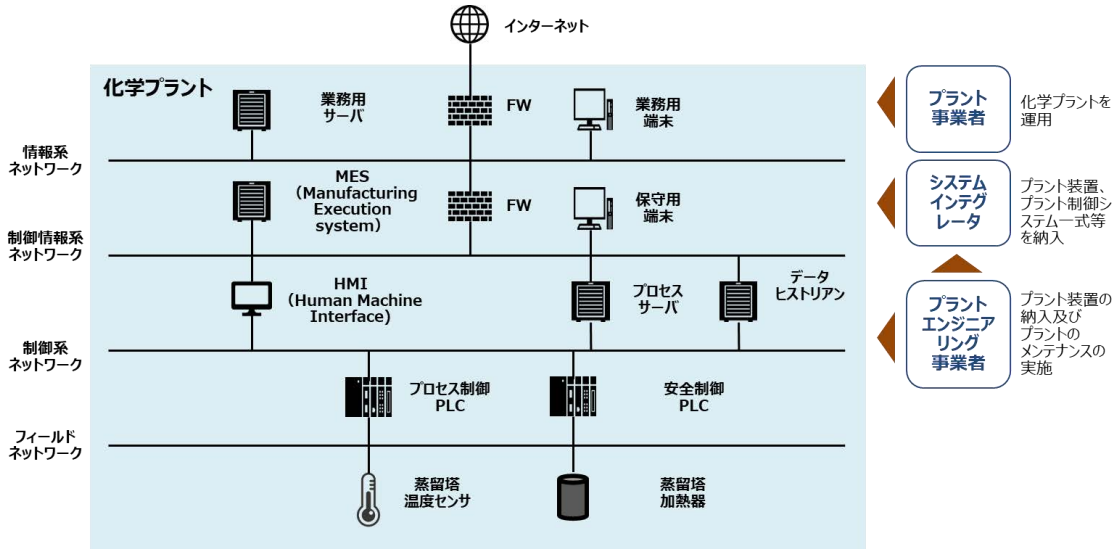


図 29 システム構成図

プラント事業者の従業員が HMI を操作して、蒸留塔内の温度を操作する場合のデータフローは以下の通りとする。

1. 温度センサがプロセス制御 PLC に温度情報を送信する。
2. プロセス制御 PLC が HMI に温度情報を送信する。
3. 従業員が HMI を操作することで、HMI がプロセス制御 PLC に制御コマンドを送信する。
4. プロセス制御 PLC が蒸留塔加熱器に制御コマンドを送信する。

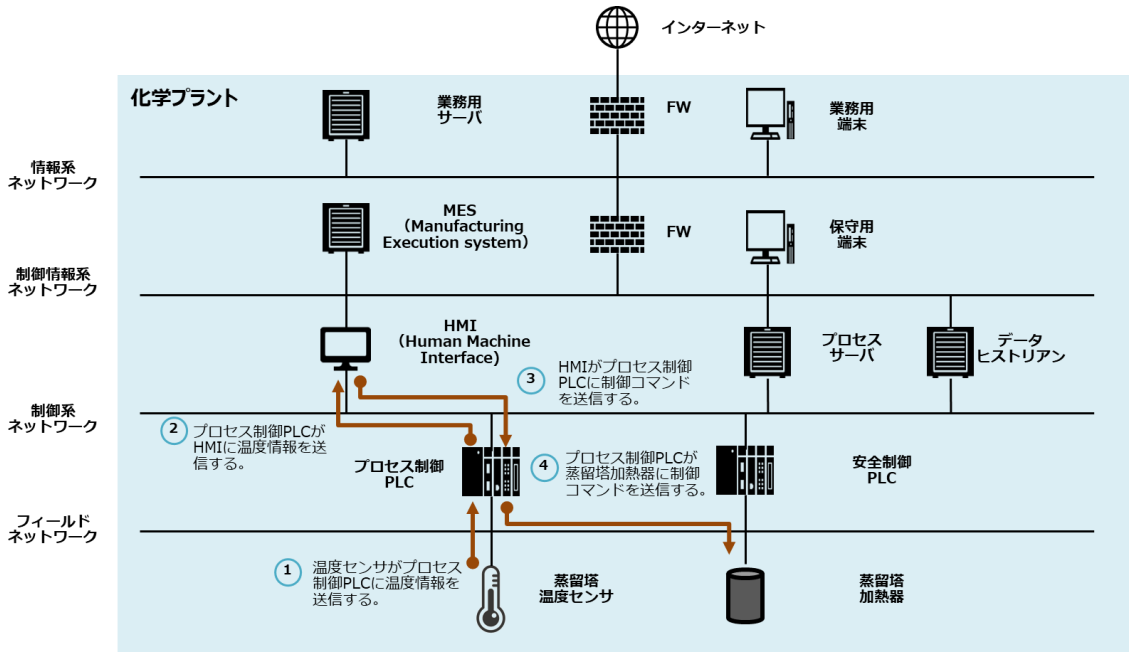


図 30 データフロー図（一部を抜粋）

⑤ リスク基準

化学プラントは、機能が停止、低下又は利用不可能な状態に陥った場合に、国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じる「重要インフラ」の 1 つに位置づけられており[32]、事業者内外を含めた社会という単位で見て、「回復困難性の度合い」及び「経済的影響の度合い」が相対的に大きくなりやすいことが想定される。かかる環境においては、他の業種等と同様に、「回復困難性の度合い」を「限定的なダメージ」なレベルまで、「経済的影響の度合い」を「限定的な経済影響」まで下げることが理想的ではあるが、それが現実的には難しいケースも想定される。ここでは、仮にプラント設備等に係る事故が発生した場合であっても、「高圧ガス・石油コンビナート事故対応要領」における C1 級[33]以上の事故にて想定される被害への発展を可能な限り防ぐことを念頭に置き、対策を講じることとした。

「回復困難性の度合い」に関しては、仮に内外に非常に大規模な影響を及ぼし得るような脅威が顕在化したとしても、C1 級に相当する事故につながらず、安全に業務やサービスの提供を保証できるよう「重大なダメージ」とならないようにすることを目指す。

また、「経済的影響の度合い」に関しては、工場の停止等が社会の大混乱（例：広範囲にわたるサプライチェーンの停止等）を引き起こす可能性があるため、持続的に業務やサービスの提供を保証できるよう「壊滅的な経済影響」とならないようにすることを目指す。

[32] 内閣サイバーセキュリティセンター(NISC)「活動内容」参照。

[33] ① 人的被害（負傷者1名以上5名以下かつ重傷者1名以下）があった事故、② 爆発、火災又は破裂・破損等が発生した事故、③ 毒性ガスが漏えいした事故）を生じた事故、④ ①から③までのほか、反応暴走に起因する事故又は多量漏えいが発生した事故のいずれかに該当するものを指す。

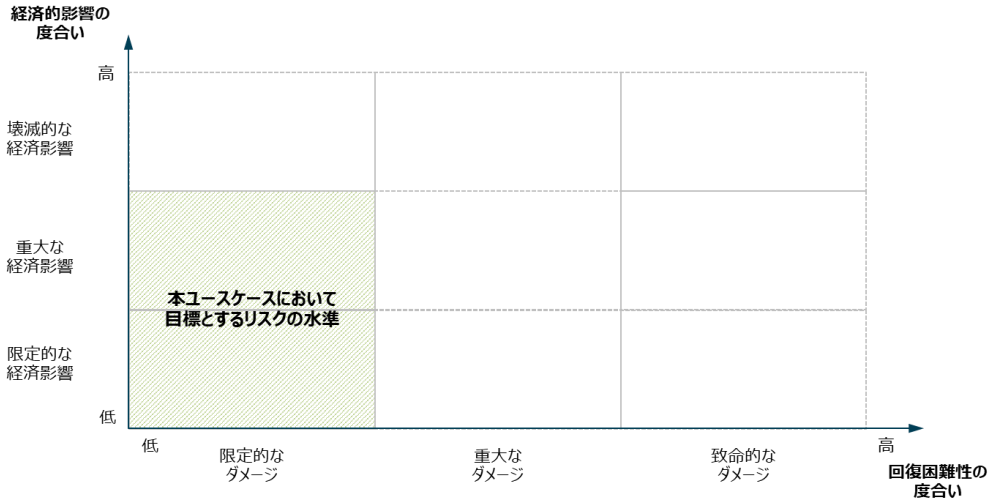


図 31 プラントシステムにて目標とするリスクの水準

(2) リスクアセスメント

「回復困難性の度合い」及び「経済的影響の度合い」から、プラント制御システムのリスクアセスメントを行う。

① 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

プラント制御システムにおいて、想定されるセキュリティインシデント等とその結果(影響)を特定する。当該システムの提供または利用に際して想定されるセキュリティインシデント(例)は以下の通り。

- 生産計画を作成する情報システムや生産活動を実際に制御する制御設備等が外部ネットワークを通じてランサムウェアに感染することにより、プラントの操業が一時的に停止する。フェールセーフの機能が失われた場合、一部の化学反応が進み蒸留塔内部の温度が急速に上昇することによって、蒸留塔での爆発事故等が発生する。
- 不正な USB 等の外部記憶媒体を挿入された保守用端末を通じて、プラント制御システム内の設備がマルウェアに感染し、予期しない動作をする。その結果、蒸留塔内の正確な温度を把握することができなくなる。
- プラントエンジニアリング事業者が、ローカル環境にて MES やプロセス制御 PLC 等に対して不適切な内容を含む不正なアップデートを実行することで、これらの機器が想定しない動作を行う。その結果、プラント設備の稼働が停止する。

② ステークホルダーごとの観点を踏まえたリスクアセスメント

以下に示すステークホルダーごとに「回復困難性の度合い」「経済的影響の度合い」の観点からリスクアセスメントを行う。

- プラント事業者
- プラント周辺の住民
- 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

- プラント事業者

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、業務用サーバや業務用端末に加えて、MES 等からプラント事業者におけ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。セーフティの観点では、セキュリティに関するインシデントによりプラント制御システムが停止し、かつ安全設備等が十分に作動しなかった場合に、一部の化学反応が進み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、作業員が重症を負うか死亡する可能性がある。

プライバシーの観点では重要な個人情報が流出する可能性があることに加えて、セーフティの観点では、セキュリティインシデントにより、最悪の場合、従業員が死亡する可能性があることから、「回復困難性の度合い」のレベルは「致命的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、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今回評価対象となる蒸留工程で制御設備（蒸留塔）が爆発し得る。また、爆発等の事故が発生した場合、その他の工程も停止する可能性が高く、プラント全体の生産活動が中断すると想定される。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。「内外への直接影響（外部）」の観点では、サプライチェーンの川上に位置するプラントが停止することによって、川下の企業の経済活動にも大きな影響を与える可能性がある。

「直接影響の継続時間」の観点では、操業停止等の事象が発生した場合に稼働開始まで時間を要するとともに、環境汚染が発生した場合には長時間悪影響を及ぼし続けることとなると想定される。

「代替可能性」の観点では、本ユースケースにて想定するインシデントが発生し工場が停止した場合、即座に生産を他のプラント等に移転することは現実的ではなく、設備が再度稼働しなければ製品を精製することはできないと想定される。

間接的な経済影響の観点では、爆発事故等が発生した場合、プラント設備の修理に一定のコストを要する可能性があると想定される。

直接的な経済影響の観点において、爆発事故や工場停止に伴い大きな経済影響が生じる可能性があることから、「経済的影響の度合い」のレベルは「壊滅的な経済影響」と評価する。

- プラント周辺の住民

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、プラントにてセキュリティインシデントが発生したとしてもプラント周辺の住民の個人情報等が流出する可能性は低いと想定される。セーフティの観点において、セキュリティに関するインシデントにより、上述の通りプラントシステムが停止し爆発事故が発生した場合、有害物質が流出し周辺の環境を汚染することによって、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と想定される。

プライバシーの観点では個人情報等が流出する可能性が少ないものの、セーフティの観点では周辺の住民等に重大な健康被害が生じる可能性があると考えられることから、「回復困難性の度合い」のレベルは「重大なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

「内外への直接影響」の観点では、セキュリティに関するインシデントにより前述の通りプラントシステムが停止し爆発事故が発生した場合、有害物質が周辺の環境を汚染することによって、農業や水産業に重大な影響を与える可能性がある。

「直接影響の継続時間」の観点において、有害物質が周辺の環境を汚染した場合、その影響は数年から数十年間の長期間にわたって続く可能性があると想定される。

「代替可能性」の観点において、農業や水産業に影響を与えた場合、代替は難しいと想定される。

また、間接的な経済影響の観点において、製品回収等の影響はないと想定される。

したがって、間接的な経済影響は大きくないものの、セキュリティに関するインシデントによりプラント制御システムが停止し爆発事故が発生した場合、直接的な経済影響が大きくなると想定されるため、「経済的影響の度合い」のレベルは「壊滅的な経済影響」と評価する。

- システムインテグレータ

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、システムインテグレータの従業員の個人情報等が流出する可能性は少ないと想定される。

セーフティの観点では、システムインテグレータの従業員がプラントの製造現場に常駐していない限りは、けがを負う可能性は低いと想定される。

プライバシーの観点ではシステムインテグレータの従業員の個人情報が流出する可能性が少ないこと、セーフティの観点ではシステムインテグレータの従業員がけがを負う可能性が少ないことから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

「内外への直接影響」の観点では、セキュリティインシデントに伴いプラント制御システムが停止したとしても、システムインテグレータによる経済活動の中断等は生じ難いと想定される。したがって、「直接影響の継続時間」の観点や「代替可能性」の観点でも、システムインテグレータには影響が及びにくいと想定される。

間接的な経済影響の観点では、プラント制御システムが既に稼働していることもあり、システムインテグレータの責任に基づく大規模な製品回収（例：MES やプロセス制御 PLC 等）は起こりにくいと考えられるため、影響は限定的であると想定される。

直接的な経済影響及び間接的な経済影響の観点において、「経済的影響の度合い」が大きくなりにくいと想定されることから、「経済的影響の度合い」のレベルは「限定的な経済影響」と評価する。

- プラントエンジニアリング事業者

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、システムインテグレータと同様、プラントエンジニアリング事業者の従業員の個人情報等が流出する可能性は低いと想定される。

セーフティの観点では、プラントエンジニアリング事業者の従業員がプラント工場の現場に常駐していない限りは、けがを負う可能性は低いと想定される。

プライバシーの観点ではプラントエンジニアリング事業者の個人情報が流出する可能性が低いこと、セーフティの観点ではプラントエンジニアリング事業者の従業員がけがを負う可能性が低いことから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B)　発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、ローカル環境にて不正なアップデートを MES やプロセス制御 PLC 等に実行した場合、システムに対する影響範囲を確認する必要があるため、プラント事業者向けにメンテナンスやサポートを行う事業者の経済活動等の直接的な停止につながると想定される。また、「内外への直接影響（外部）」の観点では、プラントシステムの保守等を提供している他のプラント事業者への影響を確認する必要が生じるため、少なからず影響が生じると想定される。

「直接影響の継続時間」の観点において、不正なアップデートをプラントシステム等に配信した場合、物流倉庫の現場は混乱し、すぐに復旧するとは考えにくい。

「代替可能性」の観点において、不正なアップデートを MES プロセス制御 PLC 等に配信した場合、代わりとなる仕組みを即座に用意することは難しいと想定される。

間接的な経済影響の観点では、プラントエンジニアリング事業者の不作為により保守用端末がマルウェアに感染したり、制御設備に不正なアップデート等が行われたりする場合にプラント事業者より契約上の責任を問われる可能性があると考えられるため、影響は重大であると想定される。

したがって、直接的な経済影響は重大であり、間接的な経済影響も重大であると想定されるため、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

③　マッピング結果の整理と評価の実施

上記を踏まえ、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて、ステークホルダーごとに第 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」からカテゴライズし、マッピングする。

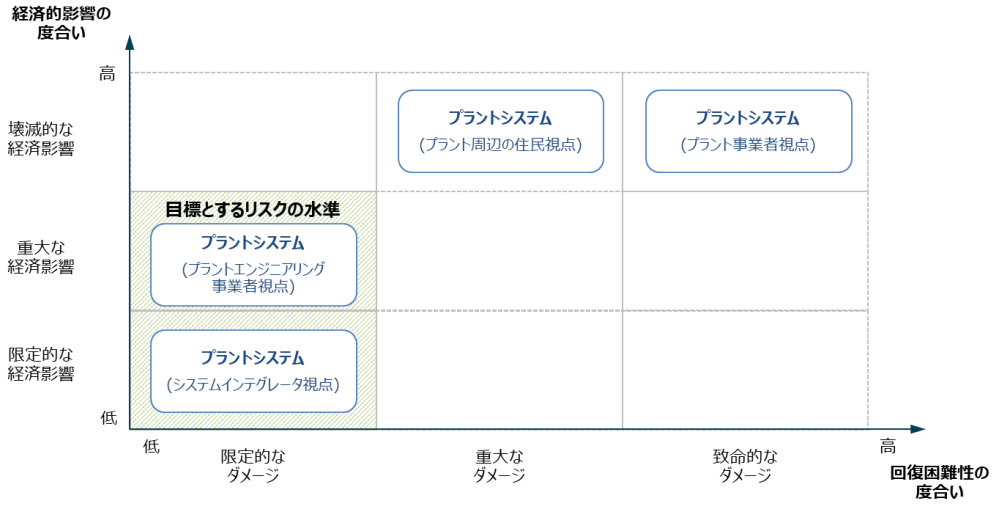


図 32 各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

プラント事業者視点からみたプラントシステムの「回復困難性の度合い」及び「経済的影響の度合い」はどちらも非常に大きくなると想定される。また、プラント周辺の住民視点からみた「経済的影響の度合

い」も非常に大きくなると想定される。これは、プラントシステムにおけるセキュリティインシデントが非常に重大な事故につながり得ること、そしてその事故がサプライチェーンや周辺の環境に大きな影響を与え得るためである。

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視点の「回復困難性の度合い」は限定的となるものの、プラントエンジニアリング事業者視点の「経済的影響の度合い」はシステムインテグレータより比較的大きくなる。これは、プラントエンジニアリング事業者がアップデートの配信等を含む保守作業を担当しているためであり、ローカル環境で不正なアップデートを実行した場合に契約上の責任を問われ得るためである。

これらを踏まえると、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視点のプラントシステム視点からみたプラントシステムで想定されるリスクは、目標とする水準内に収まっているものの、プラント事業者及びプラント周辺の住民視点のプラントシステムに想定されるリスクは、目標とする水準には収まっていない。

プラント事業者やプラント周辺の住民の視点から回復困難性の度合いを低減するためには、あらかじめ実装している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ことに加え、ネットワーク分離等を通じて被害拡大の抑制を図ったり、セキュリティインシデント対応の体制や手順等の整備を行ったりすることが有効と考えられる。これらの対策は、経済的影響の度合いを低減するためにも、有効なものとなる。

したがって、適用主体であるプラント事業者は、これらのプラントシステムがもつリスクを、可能な限り目標とする水準に収めることを目的として、例えば、以下のように影響度が大きいリスクに対処するための対策方針を明確にすることで、以降の行うべきと考えられる対策等の検討を行うことができると考えられる。

- プラント事業者にとって影響度が大きいリスクに対処するための対策方針
  - 回復困難性の度合いの観点

    プラント事業者にとっては、セキュリティに関するインシデントによって、重大な事故が発生し従業員が死亡することが主要なリスクである。これらのリスクに対応するため以下の対策が有効であると考えられる。
    - ✧ 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
    - ✧ 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

  - 経済的影響の度合いの観点

    プラント事業者にとっては、自身が運用するプラントの長時間の稼働停止及び、それに伴う取引先を含む広範囲にわたるサプライチェーンの途絶等が重要なリスクとなるが、これらのリスクに対応するため以下の対策が有効であると考えられる。
    - ✧ 情報システム部門及び製造部門が一体となってセキュリティインシデント対応を行うための体制の構築
    - ✧ 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

- プラント周辺の住民にとって影響度が大きいリスクに対処するための対策方針
  - 回復困難性の度合いの観点

    プラント周辺の住民にとっては、重大な事故が発生し有害物質が流出することによって、周辺の住民に健康被害が生じることが主要なリスクである。これらのリスクに対応するため以下の対策が有効であると考えられる。
    - ✧ 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[34]

  - 経済的影響の度合いの観点

    プラント周辺の住民にとっては、重大な事故によって環境汚染が発生した場合に地域の農林水産業への悪影響が重要なリスクとなるが、これらのリスクに対応するため以下の対策が有効であると考えられる。なお、回復困難性の度合いにおける対策例が経済的影響の度合いの観点においても有効であると考えられる。
    - ✧ 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

上記で示した対策例を添付 A に示す対策要件と比較した上で、対応関係を整理することによって、本稿で整理した対策要件のうち、行うべきと考えられる対策を明らかにすることができる。

表 25 影響度が大きいリスクに対処するための対策方針及び添付 A に記載された対策要件との関係性

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
プラント事業者	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	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	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	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

[34] 本稿ではセキュリティ分野に関する法令等を扱うものとする。それ以外の分野（例：安全分野）においては既存の安全基準やガイドラインに従って、対策を行うことが望ましい。

1535 (3) リスク対応に係る事項（ステークホルダー別の対策例一覧）

1536 ① システムを構成する機器ごとの脅威の整理

1537 システムを構成する機器・システムごとに想定される脅威（例）は以下の通り。

1538 表 26 想定される脅威（例）

システムを構成する機器	想定される脅威（例）	生じ得るインシデント（例）
製造実行システム（MES：Manufacturing Execution System）	データの改ざん	製造実行システムに保存された稼働情報等が改ざんされる。
	情報漏えい	製造実行システムに保存された稼働情報等が外部に漏えいする。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、製造実行システムに不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、製造実行システムがマルウェアに感染する。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員による製造実行システムのセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
ヒューマンマシンインターフェース（HMI：Human Machine Interface）	データの改ざん	ヒューマンマシンインターフェースから出された指示情報等が改ざんされる。
	情報漏えい	ヒューマンマシンインターフェースから出された指示情報等が外部に漏えいする。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、ヒューマンマシンインターフェースに不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、ヒューマンマシンインターフェースがマルウェアに感染する。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員によるヒューマンマシンインターフェースのセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
プロセスサーバ	データの改ざん	プロセスサーバに保存された稼働情報等が改ざんされる。
	情報漏えい	プロセスサーバに保存された稼働情報等が外部に漏えいする。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、プロセスサーバに不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、プロセスサーバがマルウェアに感染する。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員によるプロセスサーバのセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
データヒストリアン	データの改ざん	データヒストリアンに保存された稼働情報等が改ざんされる。
	情報漏えい	データヒストリアンに保存された稼働情報が外部に漏えいする。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、データヒストリアンに不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、データヒストリアンがマルウェアに感染する。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員によるデータヒストリアンのセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
業務用サーバ/業務用端末	データの改ざん	業務用サーバ/業務用端末に保存されたデータが改ざんされる。
	情報漏えい	業務用サーバ/業務用端末に保存された稼働情報が外部に漏えいする。
	権限の昇格	権限のない従業員が不正にアクセス権限を取得する。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、業務用サーバ/業務用端末に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、業務用サーバ/業務用端末がマルウェアに感染する。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員による業務用サーバ/業務用端末のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
保守用端末	データの改ざん	保守用端末に保存されたデータが改ざんされる。
	情報漏えい	保守用端末に保存された稼働情報が外部に漏えいする。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、保守用端末に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、保守用端末がマルウェアに感染する。

	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員による保守用端末のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
安全制御 PLC	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、安全制御 PLC に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、安全制御 PLC がマルウェアに感染する。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員による安全制御 PLC のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
プロセス制御 PLC	データの改ざん	プロセス制御 PLC から発信される制御情報が改ざんされる。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、プロセス制御 PLC に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、プロセス制御 PLC がマルウェアに感染する。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員によるプロセス制御 PLC のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
蒸留塔加熱器	データの改ざん	加熱器に対する制御情報が改ざんされる。
	情報漏えい	加熱器に対する制御情報が漏えいする。
蒸留塔内温度センサ	データの改ざん	センサから発信される温度情報が改ざんされる
	情報漏えい	センサから発信される温度情報が外部に漏えいする。

② 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。

表 27 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 整理した対策に対する意思決定

対策等を検討する際には、インシデントによる影響の度合いだけでなく、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ような対策を検討する。

- 対策の適用対象（どの機器を中心に検討するか）

計画的な停止期間を除いて持続的な稼働が要求され、システム停止が大きな経済的損失に繋がり得る本プラントシステムでは、「可用性」が非常に重視される。セキュリティ対策の実装（例：IDS/IPS の導入、機器に対する更新プログラムの適用）は、そうしたニーズとは相反して、システムの持続的かつ安定した運用に対して往々にしてネガティブな影響を及ぼし得るために、製造部門とリスク管理部門で利害が対立する可能性がある。例えば、リスク管理部門で IDS/IPS の導入を検討している際、ネットワークの「可用性」が損なわれる可能性があるため製造部門が導入に反対する可能性がある。その際には、どちらか一方が意見を押し付けることなく、製造部門とリスク管理部門が対話をしつつ検討することが望ましい。

- 適用する対策の内容（どのように対策を実施するか）

対策一覧より、より効率的・効果的にリスクを低減できるものを中心として対策を検討する。2-3-3 のユースケースと同様にプラントシステムにおいても、情報の機密性よりも可用性や完全性が重視される傾向があり、運用上の制約等も相まって、プロセス制御 PLC 等にエンドポイントセキュリティソフトを導入する等の IT 環境では一般的なセキュリティ対策を実施することが難しいケースがある。その場合には、より上位のシステムで守る構成とすることにより、効率的・効果的にリスクを低減することが望ましい。

なお、本ユースケースでは新たにシステムを導入するのではなく、既存の対象としてリスクアセスメントを行った。以下の対策を優先して実装することとした。

- 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
- 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

上記を踏まえて、プラントシステムがもつリスクを目標とする水準まで収めることを目的として、プラント事業者が実装することとした対策要件の例を以下に示す。

第 1 の観点では、プラント事業者が、プラント事業者やプラント周辺の住民のリスクを抑えることを目的として既存の組織体制やシステムを踏まえて、新たに実装することとした対策要件を整理した。

第 2 の観点では、プラントシステムの運用段階において、物流事業者、プラント周辺の住民のリスクを抑えることを目的として実装することとした対策要件を整理した。

第 3 の観点では、本ユースケースにてこれらに該当する対策要件は実装しないこととした。

第 4 の観点には、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネットの構築等）が該当するため、本ユースケースにてこれらに該当する対策要件は実装しないこととした。

表 28 プラント事業者における実際に講じる対策要件の例

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

				● 定められた期間ごとの当該ポリシーのレビュー	
2			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	● 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。	○ （「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」に有効と思われる対策）
3			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	● プラント施設のセキュリティ対策の設計・開発・運用等における関係各社の責任範囲の明確化。	
4			IoT機器・システムに係る要員のセキュリティ確保	● 自社内の要員（プラントにて業務に従事する要員）に対する適切な訓練及びセキュリティ教育の徹底。	
5		システム	システムインテグレータに対する搭載するソフトウェアの改ざん検知機能の実装の要求の指示	● システムインテグレータに以下の内容を指示 - MES やプロセス制御 PLC 等のソフトウェアに関する完全性の検証機能の実装	
6			システムインテグレータに対する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の指示	● システムインテグレータに以下の内容を指示 - ホワイトリストの作成等を通じて、認可されていないソフトウェアの使用の防止または検出。	
7			システムインテグレータに対するマルウェア対策の実施の指示	● システムインテグレータに以下の内容を指示 - 各ネットワークを監視する制御システム向けの機器（例：IDS/IPS）の導入	
8			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	● システムインテグレータに以下の内容を指示 - プラントエンジニアリング事業者から提供されたガイドに従ったセンサ等の設置及び設定 - プラントエンジニアリング事業者が想定する仕様に適合したネットワーク環境の整備	
9	第2の観点	ソシキ・ヒト	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	● 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維持	
10			過去の対応事例からの学習	● 発生したセキュリティインシデントの分析や解決から得られた知見の将来的なインシデント抑制への活用（同業他社の IoT 機器・システムにおけるセキュリティインシデントを含む）	
11		プロシージャ	脆弱性対応に必要な手順等の整備と実践	● 脆弱性が明らかになった場合、これらの脆弱性に対応するための体制の整備 ※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事業者向けにメンテナンスやサポートを行う事業者と連携しつつ社内体制を整備する ● プラントシステムを構成するソフトウェアの脆弱性が明らかになった場合の、対応手順の整備	
12			IoT 機器・システムの適正な運用・保守	● システムインテグレータ及びプラントエンジニアリング事業者が提示するガイドに従った保守、管理	
13			IoT 機器・システムの適正な使用	● 想定された用途・方法でのプラントシステムの使用	

14		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	● 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	○ (「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」に有効と思われる対策)
15			継続的な資産管理	● プラントシステムを構成する資産目録(機器上に実装されたソフトウェアおよびファームウェア、工場出荷時の設定等を含む)の作成・維持	
16			プログラムソースコード及び関連書類の保護	● プラントシステムに係るプログラムソースコード及び関連書類(例:設計文書)への論理アクセスを最小限にした上で、多要素認証の実施	
17			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	○ (「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」に有効と思われる対策)
18			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	○ (「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」に有効と思われる対策)
19			IoT 機器・システムの安全な廃棄または再利用	● プラントシステムを構成する機器(例:プロセス制御 PLC や温度センサー等)内部に保存されている情報の削除(読み取り不可処理を含む)	

1577 ● システムインテグレータに対応を依頼すべき対策要件の例

1578 プラント事業者にて対応が難しいシステムに関する対策は、システムインテグレータに依頼する。シス
1579 テムインテグレータは、プラント事業者によるリスクアセスメントによって追加で必要となった以下の対策
1580 要件を実装するものとする。

1581 表 29 システムインテグレータに対応を依頼すべき対策の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	搭載するソフトウェアの改ざん検知機能の実装の要求	● MES やプロセス制御 PLC 等のソフトウェアに関する完全性の検証機能の実装。	
2			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	● ホワイトリストの作成等を通じて、認可されていないソフトウェアの使用の防止または検出	
3			マルウェア対策の実施	● 各ネットワークを監視する制御システム向けの機器(例:IDS)の導入	

1582 ● プラント事業者向けにメンテナンスやサポートを行う事業者に対応を依頼すべき対策要件の例

1583 プラント事業者にて対応が難しい対策は、プラント事業者向けにメンテナンスやサポートを行う事業者
1584 に依頼する。プラント事業者向けにメンテナンスやサポートを行う事業者は、プラント事業者に対してシ
1585 ステムの保守を行っているため、主に以下の対策要件を実装するものとする。

1586 表 30 プラント事業者向けにメンテナンスやサポートを行う事業者に対応を依頼すべき対策の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 2 の観点	システム	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）の指示	● 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 ● プラントエンジニアリング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 ● プラント事業者へのセキュリティパッチの提供	

1587

2-3-5 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

輸送機器等の金属部品を設計、加工し、輸送機器メーカ等に提供する製造事業者（以下、金属部品製造事業者）が主たる適用主体となり、自社工場内に新たに導入する部品加工設備を対象にリスクマネジメントを行うユースケースを以下に記載する。

本事業者は、国内に複数の製造拠点を有し、従前より輸送機器メーカ等を主な顧客として、設計や溶接、プレス等の加工を行った上で輸送機器メーカ等に納入しており、顧客からの注文増等の状況に応じて、設計工程における 3D-CAD/CAM の導入や検査工程における各種検査機器の導入等の生産性向上に向けた投資を進めてきた。一方、溶接工程等の製造工程には熟練技術者による手動のプロセスが残り、本事業者としても品質確保や生産能力の維持・向上、技術者の高齢化による人材不足の面で課題があると認識してきたところ、この度、溶接工程の自動化を進めるためにロボットシステムを導入することとなった。

本ユースケースは、実際にロボットシステム及び他の制御システムとの接続部分を導入し、運用する前に、工場内の設備の企画や管理等を担当する生産技術部及び、本社情報システム部門にて、リスク管理を担当する複数の従業員が中心となって対象システム（ロボットシステム及び関連する制御システム）に対するリスクアセスメントを行い、適切なリスク対応策を特定することで、可能な限り、受容しがたいリスクを低減することを目指すものとする。

(1) リスクアセスメント、リスク対応に向けた事前準備

① 対象ソリューションの概要

上述の通り、主に輸送機器メーカ向けに事業を行う金属部品製造事業者が、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し、溶接工程の自動化を図っている。溶接加工の対象となるのは、顧客からの要請に基づいて様々な製品種別がある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に溶接を行うことが要求される。

従来は少なくとも 2 名の熟練技術者が溶接工程に関わっていたが、システムの導入後は同工程に直接関わる作業要員は不要となり、ロボットの稼働状況等は遠隔から管理される。稼動状況に関するデータは製造元のロボット製造事業者にも提供され、効率的な保守サービスの提供に活用される。

なお、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、作業員が不用意に立ち入り、不測の事故が発生することを防止している。

- 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。

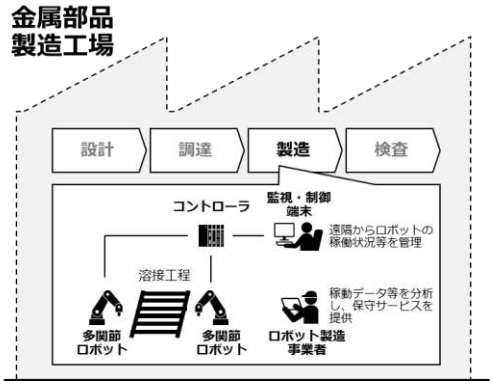


図 33 対象ソリューションの概要

② ステークホルダー関連図

本稿にて関与するステークホルダーとして、「金属部品製造事業者（委託元企業）」「システムインテグレータ（システム開発の委託先企業）」及び「ロボット製造事業者」を想定している。

- 金属部品製造事業者（委託元企業）

輸送機器用の金属部品を製造する事業者であり、自社工場の溶接工程において新たに多関節ロボットを含むロボットシステムの構築（既存システム（SCADA 等）との接続部分も含む）及び、ロボット及び周辺機器のリモート保守サービスの利用を進めようとしている。本ユースエースにおいて、主にセキュリティ対策を検討する主体である。なお、今回リスクアセスメント等の対象となっている同事業者の工場におけるセキュリティ対策等の現状は以下の通り。

- 当該工場は製造機能（工場）だけでなく、本社機能も有している。本社機能として、CIO（最高情報責任者）及び情報システム部門は存在するものの、その所掌範囲は、情報系ネットワークに所在する OA 系システムへの対応に留まっている。工場内の生産設備を所掌する生産技術部ではセキュリティ責任者や担当者が必ずしも明確になっておらず、ロボットシステムを含む制御システムのセキュリティに対する現場の関心は低い。
- 一方で、従業員や設備の安全（セーフティ）確保は重視されており、安全衛生の観点から組織的に労働災害ゼロを目指した活動等が実施されている。
- 情報資産管理台帳やネットワーク構成図は作成されているが、変更があるたびに更新されているわけではなく、内容の一部に現実との相違が存在しており、また、そのことが認識されていない。
- 工場内のネットワークと外部ネットワークや情報系ネットワークとの通信はファイアウォールを通じて必要なものだけに制御されており、その点が現場のセキュリティに対する自信の根拠となっている。ただし、工場内のファイアウォール等のログや設定を定期的に確認するプロセスは整備されていない。
- 工場内には、ID カードを付与された同社または関係先の従業員のみが入場できるようになっており、監視カメラ等も稼働していることから、外部からの工場内部への物理的な侵入は困難である。
- 自然災害を想定した事業継続計画や、情報漏えいを想定したインシデント対応手順は整備済み。

- システムインテグレータ（システム開発の委託先企業）

金属部品製造事業者との委託契約に基づき、多関節ロボットを組み込んだロボットシステム一式を提供する。

- ロボット製造事業者

多関節ロボットやそれに対応したコントローラ等を製造し、システムインテグレータに提供する。システムの納入後は、金属部品製造事業者に対して、稼働データ等の収集・分析を通じて効率的な運用・保守等（リモートでの状態監視、適宜オンサイトでの保守）を行うサービスを提供する。

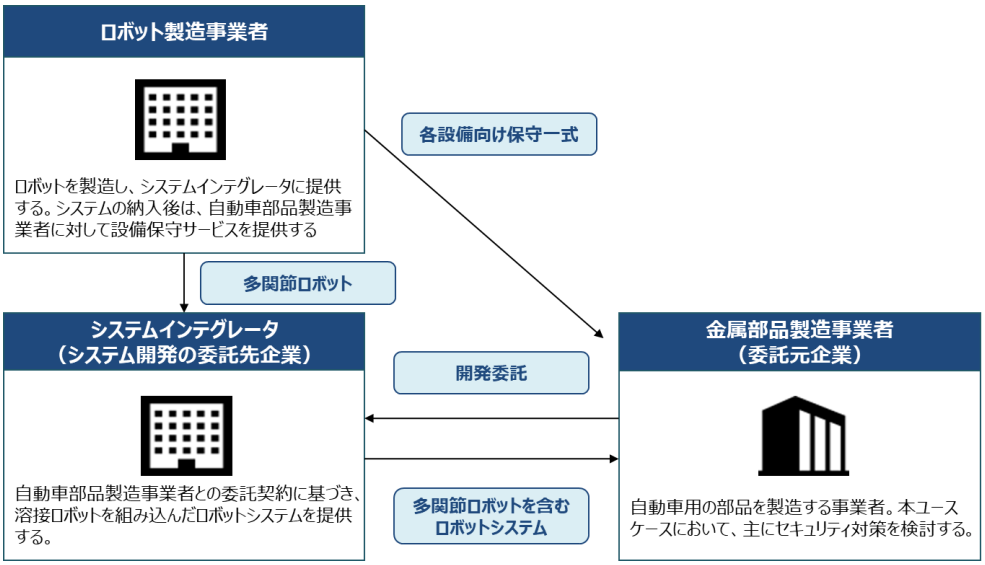


図 34 ステークホルダー関連図

③ システムを構成する機器の一覧

本稿の対象となる機器は以下の通りとする。

表 31 システムを構成する機器の一覧

システムを構成する機器	内容
業務用サーバ/端末	非制御系の情報を保存、利用するサーバ及び端末。例えば、ファイルサーバやメールサーバ及びそれらを利用するサーバ及び端末を指す。
ファイアウォール（FW）	外部ネットワークと工場内のネットワーク、工場内の情報系ネットワークと制御情報ネットワークとの間の通信を論理的に制御するネットワーク機器。
MES サーバ	製造工程の把握や管理、作業者への指示や支援などを行うサーバ。 物理サーバは、工場内のサーバ室に設置するものとする。
SCADA サーバ/端末	ロボットシステムを含む工場内で稼動するシステムの監視及びプロセス制御(制御コマンドの発行等)を行うサーバ及び端末。 SCADA とは、Supervisory Control And Data Acquisition の略称。
エンジニアリング端末	コントローラのプログラム開発及びプログラムの変更等を行うための端末。エンジニアリング用の専用ソフトウェアをインストールしている。
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）	ロボット及び周辺機器の OS やソフトウェアの更新プログラムを開発し、リモートから配信するサーバ及び端末。
コントローラ	プログラムで定められた順序や条件に従い、多関節ロボット及び周辺機器の位置、速度などの動きを制御する装置。 作業場所近くに設置された制御盤に格納されており、作業員が状態を視認、操作できるように操作画面を備えている。
多関節ロボット	アームに 3 つ以上の関節（ジョイント）を持つロボットであり、本ユースケースにおいては金属材料に対する溶接作業を行う。ロボットの可動に必要なビジョンセンサ等の周辺機器も含むこととする。

④ システム構成図、データフロー図

システム構成図は以下の通りとする。本ユースケースでは、金属部品加工工場にて稼働する「ロボットシステム」と、ロボット製造事業者が自社に構築した「リモート保守システム」の2つのシステムを考慮するものとする。ロボットシステムとは、コントローラ及び多関節ロボットを指した上で、他のシステムとの接続部分を含めてリスクアセスメントの対象とする。

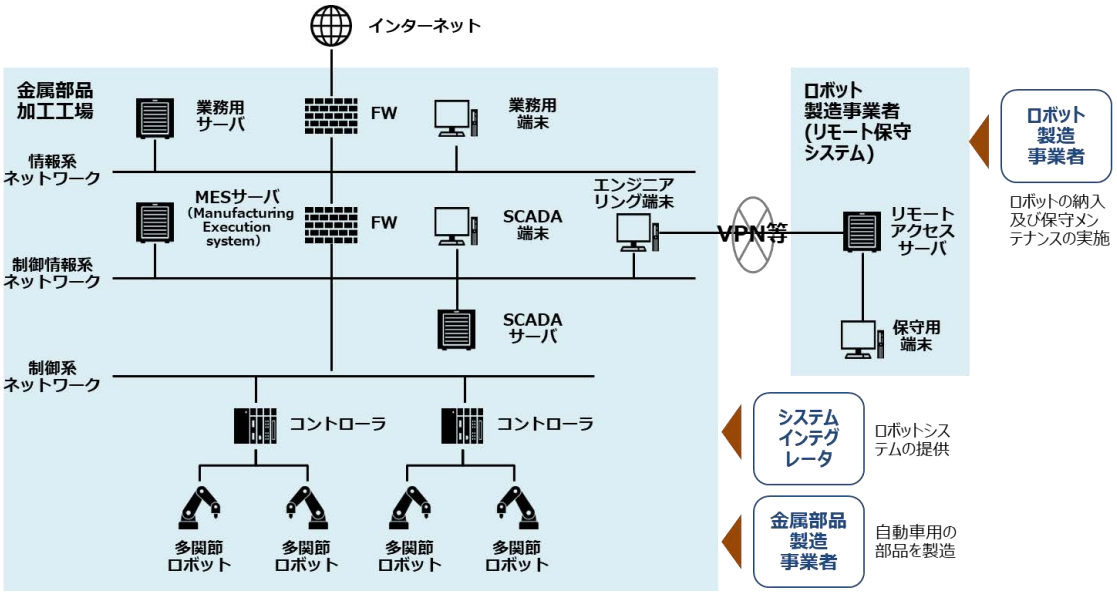


図 35 システム構成図

金属部品製造事業者が、顧客事業者からの発注を受け、設計等の前工程を終えた後に溶接工程を実施する際のデータフロー（一部を抜粋）は以下の通りである。

1. エンジニアリング端末にて制御プログラムを作成し、コントローラにインストールする。
2. ビジョンセンサ等のセンサ類から制御に必要な数値情報を取得し、コントローラに送信する。
3. コントローラが多関節ロボットに制御コマンドを送信する。
4. 多関節ロボットの稼働実績に関するデータが SCADA サーバや MES サーバに送信される。

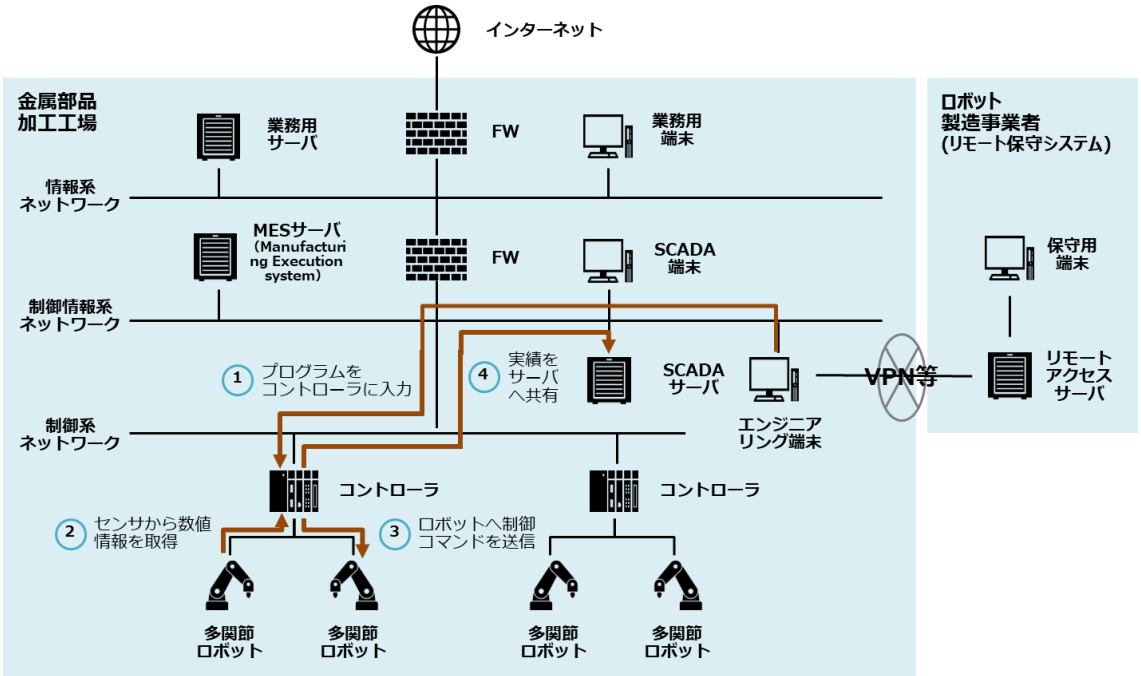


図 36 データフロー図（一部を抜粋）

⑤　リスク基準

適用主体の金属部品製造事業者においては、かねてより SQCD の観点から、それぞれセーフティ（Safety）、品質（Quality）、コスト（Cost）、納期（Delivery）の順に優先順位づけを行い、現場の改善活動等を行ってきた。今回の評価に際しても、それらの優先順位づけと矛盾がないようにリスクに関する意思決定を行う必要があることから、既に社内で策定されている基準を参照することとした。

「回復困難性の度合い」に関連して、社内ではセーフティは他の項目（品質、コスト、納期）よりも優先すべきものとみなされており、安全衛生の観点から組織的に労働災害ゼロを目指した活動等を実施していることから、本ユースケースにおいてもセキュリティ、セーフティの対策を通じて生じ得る被害の度合いを「限定的なダメージ」に抑えることを目指す。

また、同社は、コストや納期を重視しつつも、顧客事業者から見た自社製品の品質を競合他社との主な差別化要因と考えている。よって、設備の停止等による納期遅延やコスト超過以上に、不良品の出荷やそれによる返品、それらにかかる対応コスト等はできる限り避けなければならないと意識されている。上記を踏まえ、本ユースケースでは、「経済的影響の度合い」についても、「回復困難性の度合い」と同様に、「限定的な経済影響」に抑えることを目指すものとする。

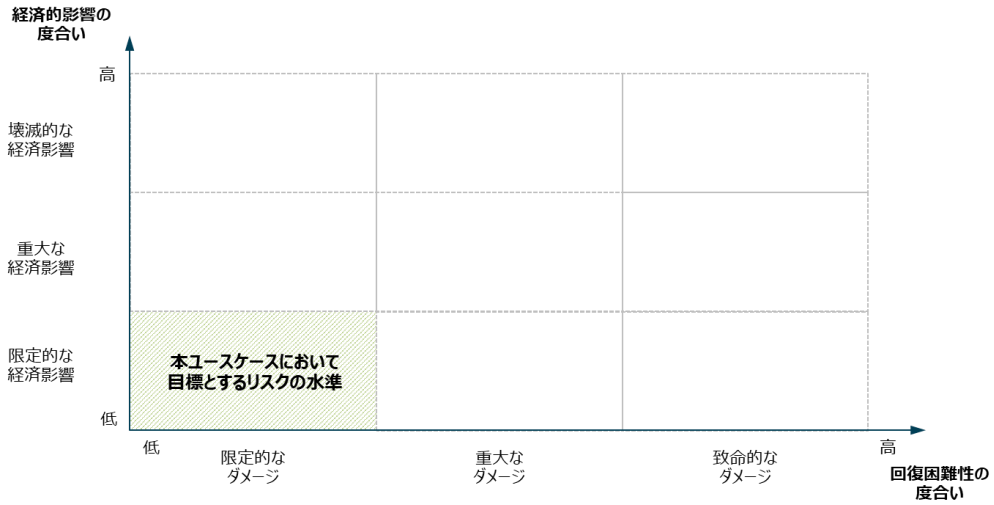


図 37 ロボットシステム及び関連する制御システムにて目標とするリスクの水準

(2)　リスクアセスメント

回復困難性の度合い」及び「経済的影響の度合い」から、プラント制御システムのリスクアセスメントを行う。

①　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

対象のロボットシステムにおいて、想定され得るセキュリティインシデント等とその結果（影響）を特定する。対象システムの利用に際して想定されるインシデント（例）は以下の通り。

・　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。その結果、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。その結果、本来の仕様を満たさない

不良品が生産される。

・ 金属部品製造事業者または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してしまい、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。

② ステークホルダーごとの観点を踏まえたリスクアセスメント

以下に示すステークホルダーそれぞれの立場を考慮し、適用主体である金属部品製造事業者から見て、「ロボットシステム」と「リモート保守システム」に対して、「回復困難性の度合い」「経済的影響の度合い」の観点でリスクアセスメントを行う。

＜ロボットシステムに関連する主なステークホルダー＞

- 金属部品製造事業者
- システムインテグレータ
- ロボット製造事業者

＜リモート保守システム[35]に関連する主なステークホルダー＞

- 金属部品製造事業者

＜ロボットシステム＞

- 金属部品製造事業者

A） 発生したインシデントの影響の回復困難性の度合い

プライバシー及びセーフティの観点を踏まえ、総合的な「回復困難性の度合い」の大きさを評価する。

先に述べたとおり、物理的な不正アクセス等（例：USB 等の外部記憶媒体の接続によるマルウェア感染）により、従業員情報やその他ビジネスに関する情報が外部に漏えいする可能性が指摘されている。ただし、ロボットシステムを構成する制御情報系ネットワークや制御系ネットワークでは、工場の稼働状況や設備に関する情報等の機微なデータを取扱うものの、プライバシーに影響をもたらすような個人情報にあたるデータはほとんど扱われていない。

セーフティの観点では、制御プログラムの改ざん等により生じるロボットの誤動作や停止等が周囲の従業員に影響を及ぼすことが懸念され得るが、稼働するロボットにはあらかじめ安全機能が実装されており、さらに、金属部品製造事業者側では安全衛生確保の観点からロボットの動作環境に安全柵を設け、レーザースキャナにより不適切な侵入を検知できることから、仮にロボットに誤作動が認められた場合であっても従業員等を巻き込んだ事故となる可能性は非常に低いと考えられる。

プライバシーの観点では、従業員の個人情報（氏名、社員番号、所属部署等）が流出する可能性は少なく、セーフティの観点でもロボットの誤動作等は懸念されるものの各種の安全対策により従業員の安全に及ぶ影響は限定的と想定されることから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

[35] 適用主体外部の事業者が管理するシステムをアセスメントにて考慮する場合、当該システムにおけるインシデントが及ぼし得る適用主体への影響を主に考慮することとする。

「経済的影響の度合い」を、直接的な経済影響及び間接的な経済影響に分けて評価する。

そのうち、直接的な経済影響は「内外への直接影響」、「直接影響の継続時間」及び「代替可能性」の観点を考慮して総合的に評価する。

「内外への直接影響（内部）」について、金属部品製造事業者にとっての金銭的な被害につながるものとしては生産設備の停止や不良品の発生、営業秘密の漏えい等が挙げられるが、いずれも事業者の本業に影響し得る重要なリスクである。前述したように、品質確保は事業者において特に重視する観点であり、後の検査工程にて発生した不良品を検出したとしても、一定の業績悪化は避けられないと考えられる。さらに、「内外への直接影響（外部）」としては、顧客となる輸送機器メーカにおいても完成車の納品遅延等の影響が及ぶ可能性があり、影響は内部に留まらない。

また、インシデントの初期対応や原因究明等に係る時間を考慮すれば、インシデント発生後速やかに通常の運用に戻るとは考え難く、「直接影響の継続時間」も無視できないものとなることが想定される。

「代替可能性の観点」では、対象のプロセスは元々人手で行われていたものであり、有事の際には従来の運用に戻すことで、生産能力が低くなるものの、工場の運用は可能であると想定される。

一方で、間接的な経済影響の観点としては、生産停止や不良品の出荷等に伴う顧客との関係悪化（例：取引の縮小）等が懸念される。

よって、セキュリティインシデントの影響が最悪の場合、自社内での損益悪化に留まらず顧客の事業にも影響を及ぼし得る点を考慮し、「経済的影響の度合い」のレベルを「重大な経済影響」と評価する。

- システムインテグレータ

A） 発生したインシデントの影響の回復困難性の度合い

システムインテグレータは本ユースケースにおいて、金属部品製造事業者に対してロボットシステム一式を納品することを役割としており、運用中のロボットシステムにおいてセキュリティインシデントが発生したとしても、必ずしも同社従業員の個人情報が漏えいしたり、機器の誤動作等によりけがを負ったりすることは想定されない。そのため、「回復困難性の度合い」のレベルを「限定的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

システムインテグレータが対象システムの運用において大きな役割を有さないことを念頭に置けば、運用時に発生するセキュリティインシデントが同社に与える「直接影響」、「直接影響の継続時間」は、限定的なものになると想定される。

間接的な経済影響としても、同社が設計、開発したロボットシステムにおいてセキュリティに係る仕様の不遵守がないことを前提とすれば、仮に金属部品製造事業者による運用においてインシデントが発生したとしても責任は限定的であると想定される。

よって、「経済的影響の度合い」のレベルを「限定的な経済影響」と評価する。

- ロボット製造事業者

A） 発生したインシデントの影響の回復困難性の度合い

ロボット製造事業者は、本ユースケースにおいて、多関節ロボット及び周辺機器の製造及び保守を行うが、運用中のロボットシステムにおいてセキュリティインシデントが発生した場合であっても、必ずしも同社従業員の個人情報が漏えいしたり、機器の誤動作等により従業員がけがを負ったりすることは想

定されない。そのため、「回復困難性の度合い」のレベルを「限定的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

ロボット製造事業者にとって、経済的な影響の観点から大きな問題となり得るのは、提供しているロボットまたはコントローラ等の周辺機器に何らかの重大な（セキュリティ上の）欠陥が存在しており、製品回収等に発展する場合と考えられる。この点については事例等も多いわけではなく、特にサイバーセキュリティを念頭に置いた場合にどこまでが製造者側の責任かという範囲を特定することが困難な側面もあるが、「内外への直接影響」としては、大規模な製品回収が発生するリスクの顕在化も否定できない。そのような背景から、必ずしも判断が容易ではない部分は残るが、将来的な問題の顕在化に備え、「経済的影響の度合い」のレベルを「重大な経済影響」と評価する。

＜リモート保守システム＞

- 金属部品製造事業者

A） 発生したインシデントの影響の回復困難性の度合い

ロボットシステムを運用する金属部品製造事業者にとって、外部ネットワークとは論理的に分離した形で構築している制御情報系ネットワーク、制御系ネットワークに対して外部からのアクセスを許可することには、一定の不正アクセスやマルウェア感染等のリスクが伴う。

しかしながら、既に「ロボットシステム」に関する評価で述べたように、仮にかかるセキュリティ上の脅威が顕在化した場合であっても、一定の前提（ロボット稼働範囲における安全柵の設置等）を置けば、プライバシーの観点とセーフティの観点のそれぞれについて、「回復困難性の度合い」のレベルを「限定的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

事前の対策が十分ではなかった結果として、ロボット製造事業者が管理するリモート保守システム、及び当該システムと金属部品製造事業者の内部ネットワークの境界が攻撃の侵入口として機能してしまう場合は、外部から保護すべき制御情報系ネットワーク、制御系ネットワークへ不正アクセスされるおそれがあり、ロボットシステムと同じく、セキュリティインシデントの発生により、自社に留まらず顧客の事業にも影響を及ぼし得る。そのため、適用主体である金属部品製造事業者以外の事業者が管理するシステムではあるが、「経済的影響の度合い」のレベルを「重大な経済影響」と評価する。

③ マッピング結果の整理と評価の実施

上記を踏まえ、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて、ステークホルダーごとに第 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」からカテゴライズし、マッピングする。

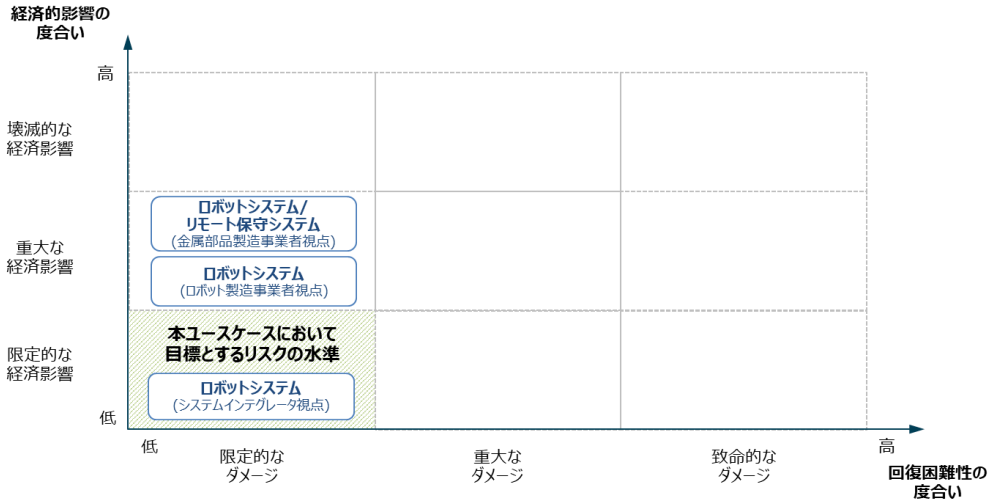


図 38 各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

上記で検討した各システム/ステークホルダーごとに想定される被害の程度と(1)⑤において規定したリスク基準を比較すると、金属部品製造事業者から見たロボットシステム及びリモート保守システムの「経済的影響の度合い」、ロボット製造事業者から見たロボットシステムの「経済的影響の度合い」は目標とするリスクの水準に収まっていない。

金属部品製造事業者にとっては、品質、コスト、納期に対する悪影響(例:不良品の増加、製造にかかるコストの増大、納品の遅延)を及ぼし得る脅威が特に優先的に対処すべきものであり、中でも品質の観点を重視している。一方でロボット製造事業者にとっては、提供しているロボットまたはコントローラ等の周辺機器における重大な(セキュリティ上の)欠陥及びそれに起因する製品回収等が重大なリスクと考えられる。適用主体の金属部品製造事業者にとっても利用機器のセキュリティ上の欠陥は避けるべきものであることから、金属部品製造事業者からの要請、またはロボット製造事業者の自主的な取組み等に基づき、何らかの対処(セキュリティ基準の遵守確認等)を講じることが望ましい。

以上を踏まえると、適用主体である金属部品製造事業者は、対象のシステムにて想定されるリスクを可能な限り目標とする水準に収めるために、例えば、以下のように影響度が大きいリスクに対処するための対策方針を明確にすることで、以降の行うべきと考えられる対策等の検討を行うことができると考えられる。

- 金属部品製造事業者にとって影響度が大きいリスクに対処するための対策方針
  - 経済的影響の度合いの観点

    運用時におけるロボット及びその制御に必要な設備(制御プログラムを含む)の信頼性をより確かなものとして、製品の品質、次いでロボット等の製造設備の可用性に影響を及ぼすような脅威を低減する対策が有効であると考えられる。
    - ロボットの制御に関わる設備(例:コントローラ、エンジニアリング端末、SCADA)の保護
    - リモート保守システムからのアクセスの保護

- ロボット製造事業者にとって影響度が大きいリスクに対処するための対策方針
  - 経済的影響の度合いの観点

運用時におけるサポートに加え、ロボットや周辺機器の設計、開発の段階からセキュリティを十分に考慮し、あらかじめ脅威に対処しておくことで、長期にわたり利用されることが想定される機器においても一定のセキュリティを確保し、ロボット製造事業者とユーザ事業者（金属部品製造事業者を含む）のリスク低減に資することができる。

- ✧ セキュアなロボット及び周辺機器（コントローラ等）の調達/提供
- ✧ 十分な期間のサポート契約締結

上記で示した対策例を添付 A に示す対策要件と比較した上で、対応関係を整理することによって、本稿で整理した対策要件のうち、行うべきと考えられる対策を明らかにすることができる。

表 32 影響度が大きいリスクに対処するための対策方針及び添付 A に記載された対策要件との関係性

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
金属部品製造事業者にとっての「経済的影響の度合い」を低減するための対策	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
ロボット製造事業者に由来する「経済的影響の度合い」を低減するための対策	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) リスク対応(ステークホルダー別の対策例一覧)

① システムを構成する機器ごとの脅威の整理

システムを構成する機器・システムごとに想定される脅威（例）は以下の通り。業務用サーバ/端末における一部の脅威を除き、これらの多くは制御プログラムの書き換えやコマンドの不正発行、マルウェア感染による操業の停止等につながり得る影響の大きいものとなっている。

表 33 想定される脅威（例）

システムを構成する機器	想定される脅威（例）	生じ得るインシデント(例)
業務用サーバ/端末	データの改ざん・消去	標的型メール攻撃等を通じて外部からの不正侵入を受け、業務用サーバ/端末に格納されているデータが改ざんまたは消去される。
	情報漏えい	標的型メール攻撃等を通じて外部からの不正侵入を受け、業務用サーバ/端末に格納されているデータが漏えいする。
	踏み台	マルウェアに感染した業務用サーバ/端末を踏み台にして、顧客のシステムに不正アクセスを試みたり、工場内ネットワークの調査等に悪用されたりする。
MES サーバ	なりすまし	MES サーバの管理者になりすまされ、生産計画、生産実績等の重要データに不正アクセスされる。
	マルウェア感染	MES サーバが情報系ネットワークを経由して受信したランサムウェアに感染し、製造ラインに対する指示が滞る。
SCADA サーバ/端末	不正アクセス	SCADA 製品の脆弱性を悪用し、同サーバへ不正ログインしたうえで、不正な制御プログラムを作成し、実行させる。
	マルウェア感染	SCADA サーバ/端末がマルウェアに感染し、製造現場の情報を遠隔から正確に把握することができなくなる。

エンジニアリング端末	不正アクセス	アクセス制御の実装が不十分であるために、エンジニアリング端末が外部からの不正アクセスを受け、制御情報系ネットワーク/制御ネットワークの調査等に悪用される。
	マルウェア感染	エンジニアリング端末に不正な USB メモリが挿入され、端末がマルウェアに感染し、外部からの不正操作を受ける。
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）	不正アクセス	リモートアクセスサーバ/保守用端末に外部から不正アクセスされ、保守サービス利用者向けの更新プログラムに不正なプログラムを混入される。
	不正改造	リモートアクセスサーバ/保守用端末に外部から不正アクセスされ、ロボットシステムの構成や稼働状況等の保守サービス利用者のデータが漏えいする。
コントローラ	情報漏えい	機器外からのアクセスに対して認証が設定されていない、またはエンジニアリング端末がマルウェアに感染している等の原因で、コントローラに外部化から不正にアクセスされ、プログラムや動作設定データ等が漏えいする。
	不正利用	エンジニアリング端末や制御盤の操作画面が不正操作され、コントローラが処理する制御プログラムや設定が変更される。
多関節ロボット	不正利用	制御プログラムの改ざんや不正な制御コマンドの発行等を通じて、多関節ロボットが予期せぬ動作を行い、周辺設備への危害や、製品の品質低下等が発生する。

② 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。

表 34 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 情報漏えい	暗号化によるデータの保護
		なりすまし 情報漏えい	ライフサイクルを通じた暗号鍵の管理
		マルウェア感染	マルウェア対策の実施
		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 整理した対策に対する意思決定

対策等を検討する際には、インシデントによる影響の度合いだけでなく、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ような対策を検討する。

- 対策の適用対象（どの機器を中心に検討するか）

金属部品製造事業者にとって、自社製品の品質や工場の事業継続こそが守るべき価値であり、それらに対して強い影響を及ぼし得る機器には十分な保護が必要と考えられる。

セキュリティの観点では、製品の品質低下（不良品の増加等）は、制御プログラムや設定の改ざん、制御コマンドの改ざん、不正発行等によりロボットが適切でない制御を実行することで生じ得る。かかるインシデントに関係し得る金属部品製造事業者の資産として以下が挙げられる。

- コントローラ：プログラムや設定の改ざんを通じて、適切でない制御を実行させる可能性がある。
- エンジニアリング端末：コントローラに不正なプログラムや設定を入力される可能性がある。
- SCADA 端末/サーバ：管理者権限を奪われた場合等に制御コマンドの不正発行が実行される可能性がある。
- FW：通信制御の設定を誤ったり、改ざんされたりすることによって、避けるべきセキュリティインシデントをまねく脆弱性を拡大させ得る。

また、適用主体外部のシステムではあるが、「リモート保守システム」及び工場内システムとの間のネットワークについてもエンジニアリング端末等につながるものとして一定のセキュリティ対策を要求することが有効と考えられる。

これらの機器では上記以外の機器と比較して相対的にセキュリティ対策の意義が大きい一方で、製造現場の運用に対してネガティブな影響を及ぼし得るために、工場内部の部門から対策強化に異論が生じる可能性がある。その際には、生産技術部等においてセキュリティ対策に責任を持つ者が、各部門と継続的にコミュニケーションをとりつつ、対策の範囲や内容について意見をくみ取り、合意を得ていくことが望ましい。

- 適用する対策の内容（どのように対策を実施するか）

（1）②にて述べた適用主体における対策の現状を踏まえると、セキュリティに責任のある従業員が不明確な状況では今後の対策推進もままならないと考えられることから、まずは第 1 の観点として、組織内部で「セキュリティを目的とした体制の確保」を進め、ロボットシステムを含む工場内のシステムに係る責任者及び担当者とそれらが負う責任を明確にすることが望ましい。

今回はロボットシステムを溶接工程に新たに導入することから、以降の段階におけるセキュリティ投資のコストを効率化することも目指し、上記で定めた責任者等が中心となり、「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」を行い、「適切な水準のアクセス制御の実装」や「ソフトウェアのインストールの制限」等の基本的なセキュリティ要求事項を明確化し、システムインテグレータへの発注の際に提示できるようにしておくことが望ましい。システムの運用段階で新たにセキュリティ対策を追加することには困難も想定されることから、設計、開発段階でこれらの要求事項が明確にされていることが重要である。

かかる対策は、前述したように、コントローラ、エンジニアリング端末、SCADA 端末/サーバの機能を、プログラムの改ざんや不正アクセス等の脅威から保護するものとすべきである。一方で、セキュリティ対策の実装が本来求められる稼動に悪影響を及ぼすことを避けることが求められるため、実際の実施内

容はそれらのバランスをとった内容となっていることが望ましい。

ロボットシステムの運用中は第 2 の観点のうち、基礎的な対策として「継続的な資産管理」を行うとともに、必要に応じて「IoT 機器・システムに対するアップデートの適用」がなされるべきである。この点については、ロボット及び周辺機器の保守業務を担うロボット製造事業者の支援を受けつつ、セキュリティ責任者/担当者が製造部門と十分に調整のうえ実施することが望まれる。その際、ロボット製造事業者が管理するリモート保守システムにおいて、不正アクセス対策等の一定のセキュリティ対策の実装を求めることも想定される。

第 3 の観点については、本ユースケースに登場する業務及びシステムの安全な運用において特別な資格等が必要なケースは必ずしも想定されないと考えられることから、これらに該当する対策要件は実装しないこととした。

さらに、第 4 の観点としても、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネットの構築等）が該当するため、本ユースケースにてこれらに該当する対策要件は実装しないこととした。

表 35 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

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● ロボットシステムを含む工場システムにおけるセキュリティポリシーを策定し、従業員や他の関係者への周知を実施 ● 策定したセキュリティポリシーについて、関係者にて少なくとも1年に1度レビューを実施	
2			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	● ロボットシステムを含む工場内のシステムの企画・設計、開発段階におけるセキュリティに係る責任者及び担当者、それらの責任の明確化 ● 本社情報システム部門との連携の確立、役割分担の明確化	
3			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	● 対象ロボットシステムのセキュリティ対策実施に係るステークホルダー（例：自社の他に、システムインテグレータ、ロボット製造事業者）を特定し、設計・開発における責任範囲を明確化	
4		システム	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	○ （「セキュアなロボット及び周辺機器の調達/提供」に有効と考えられる対策）
5 6	第 2 の観点	ソシキ・ヒト	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	● ロボットシステムを含む工場内のシステムの運用段階におけるセキュリティに係る責任者及び担当者、それらの責任の明確化 ● 本社情報システム部門との連携の確立、役割分担の明確化	
7		プロシージャ	事業継続計画の策定と実践	● 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既存の事業継続計画をレビューし、ロボットシステム等の工場システ	

				ムの故障や停止による影響等が十分に考慮されているかを確認する。	
9			IoT 機器・システムの適正な使用	● ロボット製造事業者またはシステムインテグレータから提供される機器・システムの運用手順に沿って、機器・システムを設定し、利用	
10		システム	継続的な資産管理	● 工場内のネットワークに接続している機器（サーバ、端末、ネットワーク機器、その他の設備）の管理台帳を作成し、適時に反映を実施 ● 必ずしも常時工場内のネットワークにつながっているわけではないモバイル機器（例：タブレット端末、スマートフォン、ハンディ端末）や可搬媒体（例：USB メモリ、DVD/CD）の持ち込み、持ち出し、利用状況等の厳重な管理を実施	
11			プログラムソースコード及び関連書類の保護	● ロボットシステムに関するプログラムソースコード及び関連書類（例：設計書、仕様書）へのアクセスや変更履歴（例：作成日時、変更日時、変更点）について、開発要員によるアクセスを最小限にする、アクセスログを取得する等の方法で、厳重な管理を実施	
12			IoT 機器・システムのモニタリング及びログの取得、分析	● ロボットシステムを構成する以下の機器等からログを収集しておき、定期的に、あるいは異常検知時に分析を実施 – 工場システム内2か所に設置した FW の通信ログ – SCADA 端末/サーバ、エンジニアリング端末、MES サーバへの操作ログやアクセスログ（保守用のリモートアクセスを含む）	
13			IoT 機器・システムに対するアップデートの適用	● 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	○ （「十分な期間のサポート契約締結」に有効と考えられる対策）

1897 ● 委託仕様書に基づきシステムインテグレータが実装する対策の例

1898 ロボットシステムの開発業務を行うシステムインテグレータへの委託仕様書等に基づいて、システムイ
1899 ンテグレータは主に以下の対策要件を実装するものとする。

1900 表 36 システムインテグレータに対応を依頼すべき対策の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件

1	第 1 の観点	システム	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	○ (「ロボットの制御に関わる設備の保護」に有効と考えられる対策)
2			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	○ (「ロボットの制御に関わる設備の保護」に有効と考えられる対策)
3			マルウェア対策の実施	● ロボットシステムを構成する機器において、USB メモリ等の外部記憶媒体を接続する際、登録されたもののみを利用できるようにしたうえで、事前にセキュリティスキャンの実施 ● 制御情報系ネットワークにおいて侵入検知システム(IDS/IPS)を導入し、ロボットシステムを構成する機器の脆弱性を突いた攻撃の検知・遮断 ● ロボットシステムを構成する機器において重大な脆弱性が発見された際に、サポート切れや運用上の問題でパッチ適用が困難な場合、仮想パッチとして機能させることを目的とした IDS/IPS の設定	
5			適切なネットワークの分離	● ロボットシステムを構成する機器は、既に運用されている制御情報系ネットワーク及び制御系ネットワーク内で稼動するように開発し、当該ネットワーク内外での通信を必要最小限にするよう FW 等の設定	
6			セキュリティ設計と両立するセーフティ設計の仕様化	● ロボットシステムにおいて、不正操作、誤操作、誤動作、異常発生時に設備、装置、システム、機器等を安全な方向に導くフェールセーフの仕組みの導入 ● 無関係な従業員等が無断で立ち入れないようにすることを目的として、ロボットが稼働するエリアの周辺に安全柵の設置	
7			セキュアな開発環境と開発手法の適用	● ロボットシステムの開発環境を、本番環境を含む他の環境と分離し、当該環境に対するアクセスの制限 ● 開発環境の変更及び、保管されたコードに対する変更の継続的な監視	
8			IoT 機器・システムにおけるセキュリティ機能の検証	● 開発したロボットシステムに対して、ペネトレーションテストを実施し、侵入に使用できる攻撃手法や脆弱性の特定及び、対処	
			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	● 運用前の段階で利用しないと考えられる、ロボットシステムを構成する機器のネットワークポート、USB やシリアルポートの物理的または論理的な閉塞 ● ロボットシステムを構成する機器において運用前の段階で不要と考えられるアプリケーション、機能がある場合、運用開始までの削除、無効化、停止	

10			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	○ (「ロボットの制御に関わる設備の保護」に有効と考えられる対策)

- ロボット製造事業者に対応を依頼すべき対策要件の例

ロボット及び周辺機器の保守業務を行うロボット製造事業者に対して、保守業務に係る契約書の条項等に基づいて、例えば以下の対策要件の実装を求めるものとする。

表 37 ロボット製造事業者に対応を依頼すべき対策の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	暗号化によるデータの保護	● 遠隔からの監視や保守に用いる通信経路を適切な方式(例:IPsec)により暗号化	
2			ライフサイクルを通じた暗号鍵の管理	● 利用開始後、一定の期間を経過した暗号鍵や一定の回数使用した暗号鍵の更新を実施 ● 暗号鍵の危殆化が発覚した場合、漏えいした暗号鍵の不正利用を防止するため、速やかに暗号鍵の更新を実施	
3	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	● ロボット及び周辺機器の運用手順において、提供機器の正しい利用方法や保守契約の期間や内容、利用者側で実施すべき事項等を発信 ● 上記製品に何らかの重大な脆弱性が発見された場合に、推奨策とともに金属部品製造事業者へ注意喚起を実施	
4		プロシージャ	IoT 機器・システムの適正な運用・保守	● 提供するロボット及び周辺機器の運用手順(取扱方法等を含む)を文書化し、金属部品製造事業者に提供 ● ロボット及び周辺機器に係る保守の実施手順を明確にするか、あるいは金属部品製造事業者から受領し、当該手順に沿って保守業務を実行	○ (「リモート保守システムからのアクセスの保護」に有効と考えられる対策)
5		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	● 保守契約にて規定された業務の実施方法やその他の要求事項(セキュリティ規定を含む)を認識し、確実な遵守	
6			プログラムソースコード及び関連書類の保護	● ロボットシステムに関するプログラムソースコード及び関連書類(例:設計書、仕様書)へのアクセスや変更履歴(例:作成日時、変更日時、変更点)について、開発要員によるアクセスを最小限にする、アクセスログを取得する等の方法で、厳重な管理を実施	
7			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	○ (「リモート保守システムからのアクセスの保護」に有効と考えられる対策)

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

(1) リスクアセスメント、リスク対応に向けた事前準備

本項では、IoT 機器・システムを通じて提供されるサービスの開発者または提供者である製造事業者向けにメンテナンスやサポートを行う事業者（以下、「サポート事業者」という。）が IoT-SSF の主たる適用主体となってリスクアセスメント等を行うユースケースを記載する。

サポート事業者は、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いる。サービスの提供を受ける事業者（以下、「ユーザ事業者」という。）は、当該サービスの導入によって、既存設備の設備管理業務の一部を外部に委託することが可能となるとともに、安定的に高品質の製品を製造することが可能となる。

サポート事業者は、今後のシステム構築、サービスの提供開始及び将来のサービス展開を見据え、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おり、この度、ユーザ事業者を設定し、リスクアセスメント及びリスク対応を実施することとした。

本ユースケースでは、サポート事業者がサービスの提供開始前に行ったリスクアセスメント及びリスク対応の結果、残存するリスクに対しては、ユーザ事業者に脆弱性対応等を依頼することで、可能な限り、受容しがたいリスクを低減させることとする。

① 対象ソリューションの概要

本ユースケースでは、サポート事業者のソリューションに加え、ユーザ事業者の対象業務も明示した。本ユースケースでは、具体的なユーザ事業者を金属製品製造事業者とした。

- サポート事業者

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するものとする。また、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、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している。

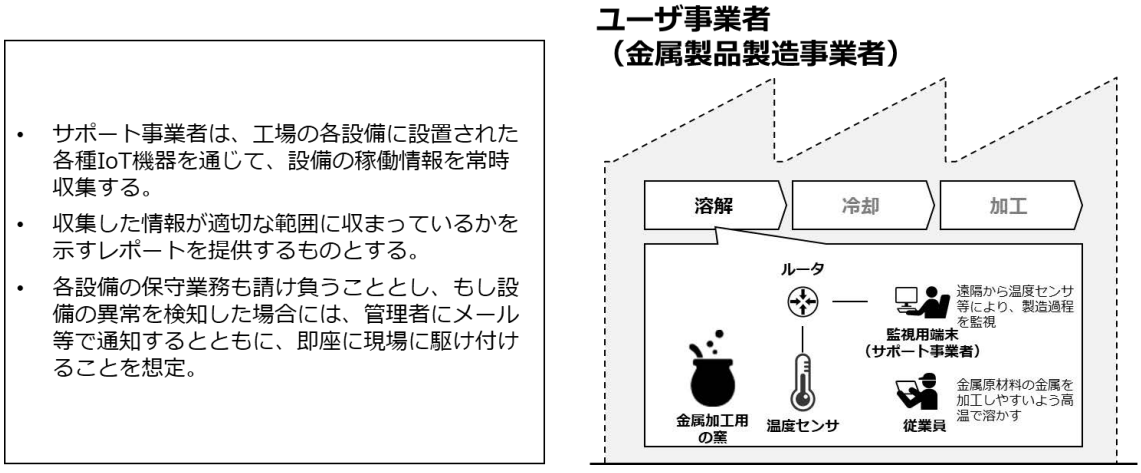


図 39 対象ソリューションの概要

- ユーザ事業者（金属製品製造事業者）

ユーザ事業者（金属製品製造事業者）の工場内で対象とする業務内容を整理する。

ユーザ事業者（金属製品製造事業者）の工場では以下の 3 つの作業を行っており、本ユースケースでは、既にサポート事業者の関連会社が設備を導入している 1 の溶解作業で使用する窯に各種センサを設置する。これらの窯は非防爆エリアに配置されており、フェールセーフの機能が備わっているものとする。

1. 溶解作業：原材料の金属を加工しやすいよう高温で溶かす作業
2. 加工作業：溶かした金属を型に流し込み加工する作業
3. 冷却作業：型に流し込んだ金属を冷却する作業

今回、新たに導入する温度センサ、重量センサ及び振動センサによって、温度情報や重量情報を含む設備の稼働情報が可視化されることを想定している。

なお、ユーザ事業者では、既に導入している生産制御システム等とサポート事業者が提供する各種センサや情報収集サーバからなる状態監視システムとは接続しない前提とする。

② ステークホルダー関連図

本稿にて関与するステークホルダーは、「サポート事業者」、「センサ製造事業者」及び「ユーザ事業者（金属製品製造事業者）」を想定する。

- サポート事業者

既存の工場の設備に対して、新たに温度センサ、重量センサ及び振動センサ等を導入し、設備の状況をリアルタイムで監視するサービスを提供する事業者である。また、設備の運用保守を行い、故障などの際には現場に駆け付けることを想定している。セキュリティ対策等の実施に対して主に責任を有する事業者である。

- センサ製造事業者

製造設備の温度センサ、重量センサ及び振動センサ等をサポート事業者に提供する事業者である。

- ユーザ事業者(金属製品製造事業者)

サポート事業者が設定したサービスの提供を想定する事業者であり、既に稼働している工場で金属製品を製造する事業者を想定する。

また、ユーザ事業者（金属製品製造事業者）では既に以下の対策は既に実施済みである。

- 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

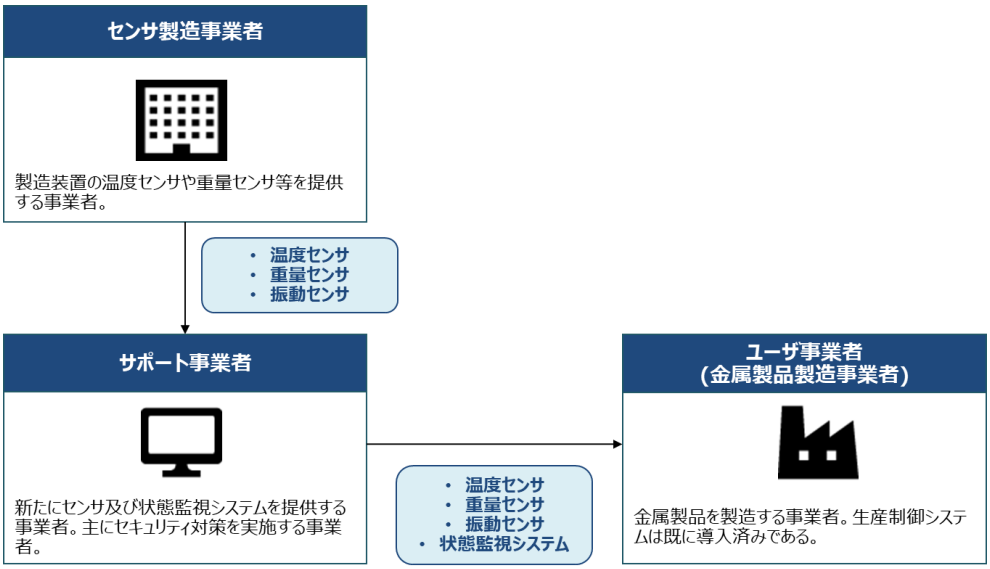


図 40 ステークホルダー関連図

③ システムを構成する機器の一覧

本稿の対象となる機器は以下の通りとする。

表 38 システムを構成する機器の一覧

システムを構成する機器	内容
情報収集サーバ	温度データ、重量データ、振動データ等を収集するサーバ。 異常が発生した場合には、監視用端末にアラートを出す。 状態監視システムとは、情報収集サーバ及び各種センサを含めたシステムを指す。 情報収集サーバは、サポート事業者内に設置されるものとする。
監視用端末	情報収集サーバのデータを監視し、異常が発生していないかを監視する端末。 監視用端末は、サポート事業者内に設置されるものとする。
ルータ	工場内に設置され、工場内のネットワークおよび工場外のネットワークを中継する通信機器。 ルータは、工場内の各センサやカメラの情報を取得できる位置に設置するものとする。
温度センサ	金属加工用の窯の温度を計測するセンサ。 窯の内部に設置されているものとする。サポート事業者よりリースにて提供される。
重量センサ	金属加工用の窯の重量を計測するセンサ。 窯の外部に設置されているものとする。 サポート事業者よりリースにて提供される。
振動センサ	金属加工用の窯の振動を計測するセンサ。 窯の外部に設置されているものとする。 サポート事業者よりリースにて提供される。

④ システム構成図、データフロー図

システム構成図は以下の通りとする。状態監視システムは既存の生産制御システムのネットワークとは分かれており、これらのシステム間で通信がなされないことを想定する。

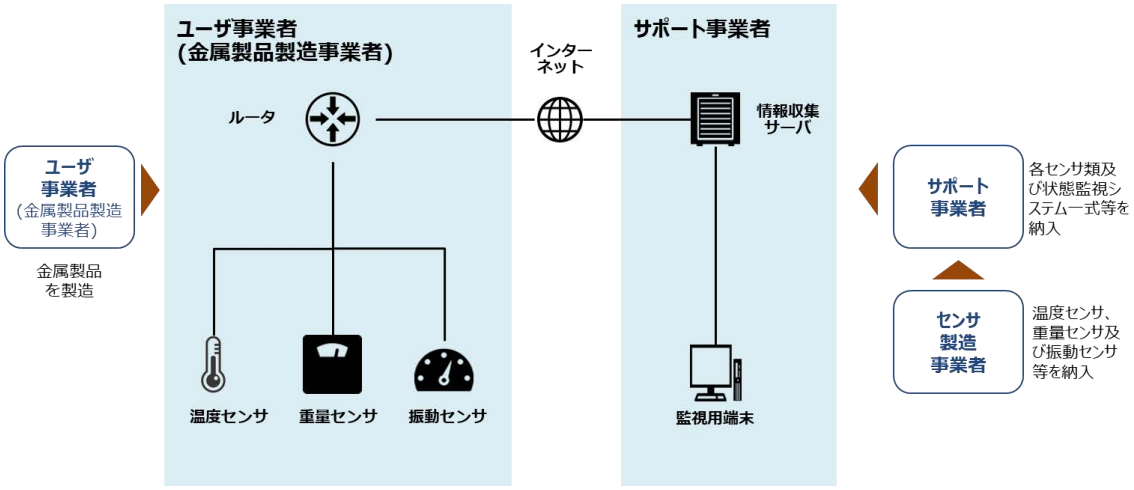


図 41 システム構成図

サポート事業者の従業員が窯の状態を遠隔監視する場合のデータフローは以下の通りとする。

1. 各センサ等がルータを通じて取得した情報を情報収集サーバに送信する。
2. 情報収集サーバの情報を監視用端末が確認する。

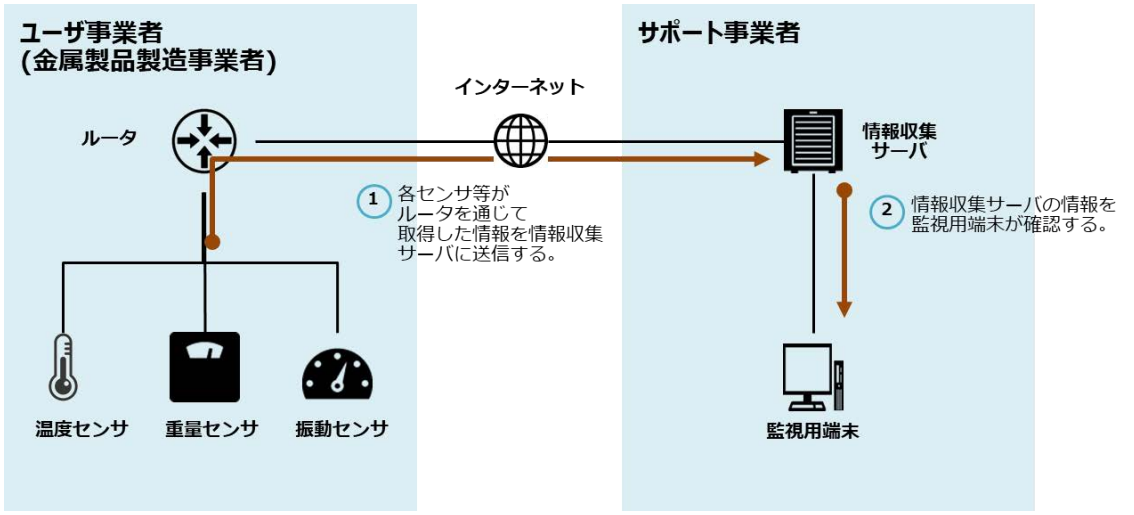


図 42 データフロー図(一部を抜粋)

⑤ リスク基準

「回復困難性の度合い」において、自社が定めるセキュリティ及びセーフティに関する基本方針にのっとるとともに、個人情報等の漏えい等がないよう、セキュリティ対策を通じて生じ得る被害の度合いを「限定的なダメージ」に抑えることを目指す。

「経済的影響の度合い」において、稼働情報を可視化し継続的にサービスを提供することが重要視される。したがって、サービスの停止が生じないようセキュリティ対策を通じて「限定的な経済影響」に抑えることを目指す。

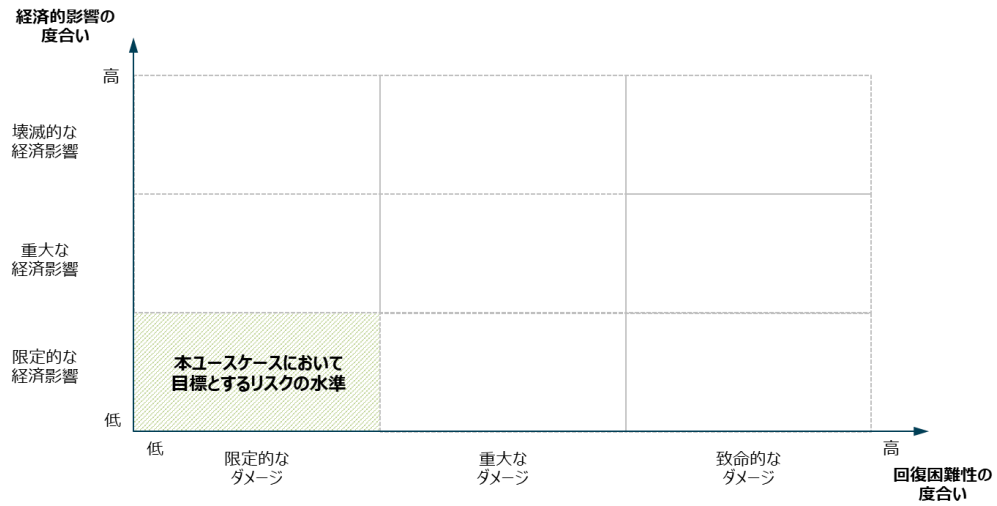


図 43 状態監視システムにて目標とするリスクの水準

(2) リスクアセスメント

「回復困難性の度合い」及び「経済的影響の度合い」から、状態監視システムのリスクアセスメントを行う。

① 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

状態監視システムにおいて、想定され得るセキュリティインシデント等とその結果(影響)を特定する。当該システムの提供または利用に際して想定されるセキュリティインシデント(例)は以下の通り。

- 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ことによって、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。
- 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)に感染させることによって、サーバの一部機能を停止させる。悪意のある攻撃者より脅迫を受けることで、サポート事業者が金銭的な被害を受ける。
- 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 攻撃を仕掛けることによって、サーバの一部機能を停止させることで、温度情報等を正確に表示することができなくなる。

ステークホルダーごとの観点を踏まえたリスクアセスメント

以下に示すステークホルダーごとに「回復困難性の度合い」「経済的影響の度合い」の観点からリスクアセスメントを行う。

- サポート事業者
- センサ製造事業者
- ユーザ事業者(金属製品製造事業者)

- サポート事業者

A) 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、情報収集サーバに従業員の個人情報等が保存されていないとすれば、仮に何らかの情報流出があったとしても、プライバシーに係る影響は限定的である。

セーフティの観点では、インターネット経由で情報収集サーバがマルウェア（例：ランサムウェア）に感染したり、DoS 攻撃を受けたりすることでセンサの情報を適切に処理できなくなった場合に、サポート事業者の従業員は現場へ駆け付けることを想定している。ただし、各設備にはフェールセーフ等の機能が具備されていたり、予め温度センサ等が正確な情報を取得できていないことを従業員が理解できていたりするため、けがを負う可能性は低いと想定される。

プライバシーの観点ではサポート事業者の従業員の個人情報が流出する可能性は低く、セーフティの観点においても従業員がけがをする可能性が低いことから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B) 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、インターネット経由で情報収集サーバがマルウェア（例：ランサムウェア）に感染した場合に悪意のある攻撃者による脅迫により金銭的な被害を受ける可能性や、DoS 攻撃を受けることでセンサの情報を適切に処理できなくなった場合にユーザ事業者（金属製品製造事業者）を含むサービスを利用する事業者全体に対してサービスを提供できなくなる可能性がある。また、「内外への直接影響（外部）」の観点では、情報収集サーバにおけるマルウェア感染によって、他の事業者に対してサービスを提供できなくなる可能性があり、影響が広範囲にわたって及ぶと想定される。

また、インシデントの初期対応や原因究明等にかかる時間を考慮すれば、インシデント検知後速やかに通常の運用に戻るとは考え難く、「直接影響の継続時間」も無視できないものとなることが想定される。

「代替可能性」の観点において、情報収集サーバがマルウェアに感染したり、DoS 攻撃を受けたりした場合、代わりとなる仕組みを即座に用意することはできず、影響が一定期間継続するため、代替となるサービスを提供することはできないと想定される。

間接的な経済影響の観点において、情報収集サーバや各種センサの修理や交換に一定のコストを要する可能性があると想定される。

したがって、直接的な経済影響は重大であり、間接的な経済影響も重大であると想定されるため、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

- センサ製造事業者

A) 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、従業員の個人情報等が流出する可能性は少ないと想定される。

セーフティの観点では、従業員が金属製品製造工場の現場に常駐していない限りは、けがを負う可能性は低いと想定される。

プライバシーの観点ではセンサ製造事業者の個人情報が流出する可能性が少ないこと、セーフティの観点ではセンサ製造事業者及び監視カメラ製造事業者の従業員がけがを負う可能性が少ないことから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B)　発生したインシデントの経済的影響の度合い

センサ製造事業者が状態監視システムの運用において大きな役割を有さないことを念頭に置けば、運用時に発生するセキュリティインシデントが同社に与える「直接影響」、「直接影響の継続時間」は、限定的なものになると想定される。

間接的な経済影響としても、センサ製造事業者が設計、開発した各種センサ等において契約上大きな問題がない場合、仮にサポート事業者による運用においてセキュリティインシデントが発生したとしても責任は限定的であると想定される。

よって、「経済的影響の度合い」のレベルを「限定的な経済影響」と評価する。

- ユーザ事業者（金属製品製造事業者）

A)　発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、情報収集サーバに設備の稼働情報は保存されているものの、ユーザ事業者（金属製品製造事業者）の従業員の個人情報等が保存されていないため、セキュリティインシデントによって個人情報が流出する可能性は低いと想定される。

セーフティの観点では、情報収集サーバ等がマルウェア感染し正確な数値を表示できなくなった場合、生産制御システムとは接続されておらず、これらのシステムもフェールセーフ等の機能が具備されていると想定すると、従業員がけがを負う可能性は低いと想定される。

プライバシーの観点ではユーザ事業者（金属製品製造事業者）の個人情報が流出する可能性が低く、セーフティの観点においては従業員がけがを負う可能性は低いことから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B)　発生したインシデントの経済的影響の度合い

「内外への直接影響(内部)」の観点では、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によって、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）における設備の稼働情報等が流出し、ユーザ事業者（金属製品製造事業者）の金属製造に係るノウハウが外部へ流出する。競争力の源泉となっていたノウハウが流出することで、ユーザ事業者（金属製品製造事業者）の競争力が失われ事業上の損害が生じる可能性がある。「内外への直接影響（外部）」の観点では、設備の稼働情報が流出したとしてもユーザ事業者外部への影響は限定的であると想定される。

「直接影響の継続時間」の観点では、状態監視システムが停止した場合においても、生産制御システムとは接続しておらず工場内で運用されている監視の仕組みが正常に稼働しているならば、工場の稼働停止にはつながらないと想定される。

「代替可能性」の観点では、上記の通り、状態監視システムがセキュリティインシデントに伴って停止したとしても、上述した理由により、製造プロセスに必ずしも異常は生じないと想定される。

間接的な経済影響の観点では、マルウェア（例：ランサムウェア）に感染したり、DoS 攻撃を受けたりすることにより、情報収集サーバがセンサの情報を適切に処理できなくなったとしても、ユーザ事業者（金属製品製造事業者）の工場内での運用によって、金属製品の品質や製造設備の劣化等は防げると想定されるため、ここでは設備の稼働停止等による間接影響を考慮しない。

直接的な経済影響の観点から、「経済的影響の度合い」が比較的大きくなると想定されることから、

「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

② マッピング結果の整理と評価の実施

上記を踏まえ、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて、ステークホルダーごとに第 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」からカテゴライズし、マッピングする。

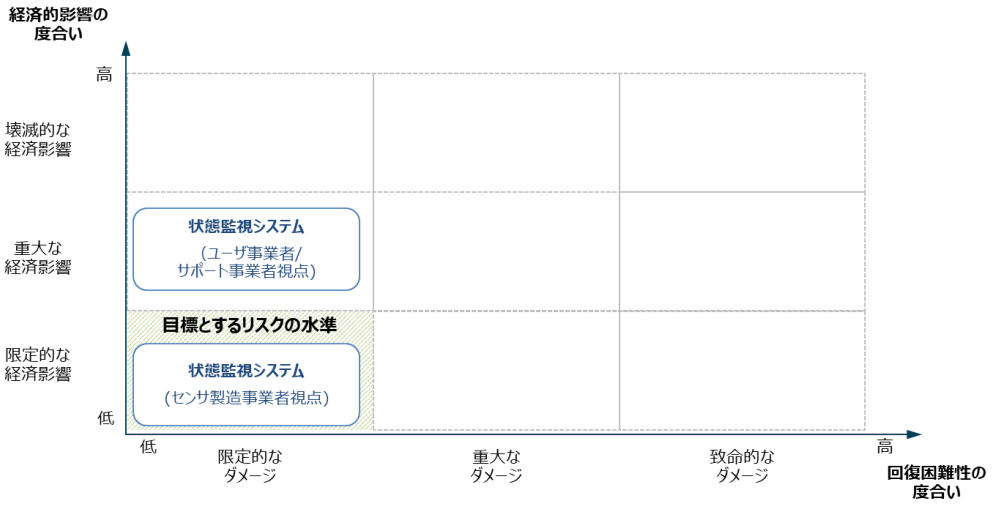


図 44 各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

マッピング結果を踏まえると、センサ製造事業者視点の状態監視システムが保有するリスクは目標とする水準内に収まっているものの、サポート事業者やユーザ事業者（金属製品製造事業者）視点の情報監視システムが保有するリスクは目標とする水準内に収まっていない。

以下では、まずサポート事業者やユーザ事業者（金属製品製造事業者）において目標とするリスク水準に収まっていない原因を整理した上で、リスクを低減するための対策を検討するものとする。

サポート事業者及びユーザ事業者（金属製品製造事業者）視点からみた状態監視システムの「回復困難性の度合い」は小さいものの、「経済的影響の度合い」は比較的大きくなる。

サポート事業者及びユーザ事業者（金属製品製造事業者）の「経済的影響の度合い」が比較的大きくなるのは、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）の設備の稼働情報が外部に流出した場合である。これらを引き起こすと考えられる脅威は、例えば以下の通りである。

- 情報収集サーバに保存しているデータに対して不正アクセスされる

上記を踏まえて、IoT-SSF の適用主体であるサポート事業者は、これらの状態監視システムがもつリスクを、可能な限り目標とする水準に収めることを目的として、例えば、以下のように影響度が大きいリスクに対処するための対策方針を明確にすることで、以降の行うべきと考えられる対策等の検討を行うことができると考えられる。

- サポート事業者にとってのリスクを低減するための対策方針
  - 経済的影響の度合いの観点

サポート事業者にとっては、情報収集サーバに保存された稼働情報の漏えいやマルウェア感染（例：ランサムウェア）が重要なリスクとなるが、これらのリスクに対応するため以下の対策が有効であると考えられる。

- ✧ 稼働情報の漏えいを防ぐ仕組みの構築
- ✧ 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

- 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方針
  - ➢ 経済的影響の度合いの観点

ユーザ事業者（金属製品製造事業者）にとっては、情報収集サーバに保存された稼働情報が漏えいし、事業上の損失を負うことが重要なリスクとなるが、これらのリスクに対応するため以下の対策が有効であると考えられる。

- ✧ 稼働情報の漏えいを防ぐ仕組みの構築

上記で示した対策例を添付 A に示す対策要件と比較した上で、対応関係を整理することによって、本稿で整理した対策要件のうち、行うべきと考えられる対策を明らかにすることができる。

表 39 影響度が大きいリスクに対処するための対策方針及び添付 A に記載された対策要件との関係性

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
サポート事業者	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
		暗号化によるデータの保護
ユーザ事業者（金属製品製造事業者）	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) リスク対応に係る事項（ステークホルダー別の対策例一覧）

① システムを構成する機器ごとの脅威の整理

システムを構成する機器・システムごとに想定される脅威（例）は以下の通り。

表 40 想定される脅威（例）

システムを構成する機器	想定される脅威（例）	生じ得るインシデント（例）
情報収集サーバ	情報漏えい	情報収集サーバから製品製造事業者の工場における設備の稼働情報が流出する。
	サービス不能	情報収集サーバが(D)DoS 攻撃を受けて、サポート事業者やユーザ事業者（金属製品製造事業者）がサーバやサービス等にアクセスできなくなる。
	不正アクセス	インターネット経由で情報収集サーバに保存されたデータに対して、不正アクセスされる。
	マルウェア感染	情報収集サーバがマルウェア感染する。
監視用端末	マルウェア感染	監視用端末がマルウェア感染する。
ルータ	不正アクセス	既知の脆弱性等を悪用することでルータに不正アクセスされる。
温度センサ	データの改ざん	温度センサから発信される通信中に温度情報が改ざんされる
	情報漏えい	温度センサから発信される温度情報が外部に漏えいする。
重量センサ	データの改ざん	重量センサから発信される通信中に重量情報が改ざんされる
	情報漏えい	重量センサから発信される温度情報が外部に漏えいする。
振動センサ	データの改ざん	振動センサから発信される通信中に振動情報が改ざんされる
	情報漏えい	振動センサから発信される温度情報が外部に漏えいする。

② 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。

表 41 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 情報漏えい	暗号化によるデータの保護
		データの改ざん 情報漏えい	ライフサイクルを通じた暗号鍵の管理
		マルウェア感染	マルウェア対策の実施
		全般	IoT 機器・システムの十分な可用性の確保
		全般	IoT に適したネットワークの利用
		全般	適切なネットワークの分離
		全般	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
		全般	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
		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
		不正アクセス マルウェア感染	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
		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 整理した対策に対する意思決定

対策等を検討する際にはインシデント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ような対策を検討する。

- 対策の適用対象（どの機器を中心に検討するか）

想定しているインシデントが発生した際に想定される被害の大きさ及び起こりやすさ等を考慮して、情報収集サーバ、監視用端末、ルータ、各種センサ等から、特に対策を検討すべき資産を検討する。

被害の大きさという観点では、個々のセンサ等では個別の稼働情報のみが保管、送信されている状

2136 況に留まっていることを考慮すれば、各種センサ等からのデータを集約し、より多くの価値あるデータを
2137 取扱っていると考えられる以下の資産を中心として対策を検討すべきである。

2138 ➢ 情報収集サーバ
2139 自社の事業継続及び、サービスの提供を想定しているユーザ事業者（金属製品製造事業者）だ
2140 けでなく、同様のサービスを利用する事業者全体に対して影響が波及し得る。

2141 また、「起こりやすさ」の観点では、外部からのネットワーク経由での攻撃に対して対処する必要があ
2142 るため、インターネットに直接接続されている資産（例：情報収集サーバやルータ等）を中心として対策を
2143 検討することが望ましい。

2144 • 適用する対策の内容（どのように対策を実施するか）
2145 ②にて検討した事業者にて実装が想定される対策要件の例より、より効率的・効果的にリスクを低減
2146 できるものを中心として対策を検討する。例えば、ユーザ事業者（金属製品製造事業者）の工場に設置
2147 される各種センサは、非常に数が多いうえに簡単な構成であり、各種センサにエンドポイントセキュリテ
2148 ィソフトを導入する等の IT 環境では一般的なセキュリティ対策を実施することが難しいケースがある。一
2149 方で、上述したように、情報収集サーバには各種データが集約され、攻撃者にとってもより魅力的な標
2150 的としてとらえられる可能性が高い。その場合には、サーバ側で以下の対策要件を実装した上で、より
2151 上位のシステムで守る構成とすることにより、システム全体として効率的・効果的にリスクを低減するこ
2152 とが望ましい。

2153 ➢ 適切な水準のアクセス制御の実装
2154 ➢ 暗号化によるデータの保護
2155 ➢ マルウェア対策の実装
2156 ➢ IoT 機器・システムの十分な可用性の確保

2157 上記を踏まえて、状態監視システムがもつリスクを目標とする水準に収めることを目的として、サポー
2158 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。
2159 第 1 の観点では、サポート事業者が企画段階において、当該事業者やユーザ事業者（金属製品製造
2160 事業者）のリスクを抑えることを目的として実装することとした対策要件を整理した。
2161 第 2 の観点では、サポート事業者の運用段階において、当該事業者やユーザ事業者（金属製品製造
2162 事業者）のリスクを抑えることを目的実装することとした対策要件を整理した。
2163 第 3 の観点については、本ユースケースが対象とする業務やシステムでは法令等による運用担当者
2164 への専門資格保有の要求、あるいはそれに相当する業界または社内の人事等に関する慣行は必ずし
2165 も認められないことから、これらに該当する対策要件は実装しないこととした。
2166 第 4 の観点には、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネッ
2167 トの構築等）が該当するため、本ユースケースにてこれらに該当する対策要件は実装しないこととした。
2168 なお、第 1 の観点及び第 2 の観点における対策要件のうち、サポート事業者単体では対応が難しい
2169 対策要件がいくつか見られた。これらの対策要件の実装はユーザ事業者（金属製品製造事業者）に依
2170 頼することとした。

2171

表 42 サポート事業者において実際に講じる対策の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● 自社が提供するサービスを対象としたセキュリティポリシー（情報セキュリティ関連規定を含む）の策定及び適切な承認権限を有する者の承認 ● 定められた期間ごとの当該ポリシーのレビュー	
2			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	● 状態監視システムのセキュリティ管理責任者及びセキュリティ対策担当者の任命 ※ 上記の管理責任者及び開発担当者は、状態監視システムのライフサイクルの各段階（例：設計、開発）において明確化されていることが望ましい。	
3			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	● 状態監視システムのセキュリティ対策の設計・開発・運用等における関係各社の責任範囲の決定 ● 運用中に発生したセキュリティインシデントにより損害が発生した場合の責任範囲（役割分担や損害賠償）の決定	
4			IoT 機器・システムに係る要員のセキュリティ確保	● 自社内の要員に対する適切な訓練及びセキュリティ教育の実施	
5		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	● 状態監視システムや監視用端末にて扱う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、知的財産法）又は各製造事業者にサービスを提供する場合に契約上の義務に対する違反を避けるための要求事項の遵守 ● 関係省庁から公表されているガイドライン（例：経済産業省「AI・データの利用に関する契約ガイドライン」、「営業秘密管理指針」等）の参照	
6			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	● 状態監視システムの企画・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	
7			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）	○ （「稼働情報の漏えいを防ぐ仕組みの構築」及び「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」に有効と考えられる対策）
8			ソフトウェアの完全性の検証	● 情報収集サーバや監視用端末のソフトウェアや格納されたデータにおける完全性の検証機能の実装	
9			ソフトウェアのインストールの制限	● 情報収集サーバや監視用端末の構成についてベースラインを作成し、必要な変更がなければ当該構成を継続的に維持	

10			様々なIoT機器に接続する際のセキュリティの確保	● あらかじめ識別情報（例：MACアドレス）を登録している機器（各種センサ等）による情報収集サーバへの接続に限り許可	
11			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	○ （「稼働情報の漏えいを防ぐ仕組みの構築」及び「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」に有効と考えられる対策）
12			ライフサイクルを通じた暗号鍵の管理	● 暗号鍵の利用、保護及び有効期間に関するポリシーの策定及び遵守	
13			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	○ （「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」に有効と考えられる対策）
14			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	○ （「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」に有効と考えられる対策）
15			IoT に適したネットワークの利用	● ユーザ事業者（金属製品製造事業者）内の設備に設置された各種センサを、暗号化機能を有したWi-Fi（例：WPA2-PSK（AES）等）に接続 ● ユーザ事業者（金属製品製造事業者）における既存の帯域を圧迫しない通信方法の選択（例：既存の制御システムとは別のネットワークを整備する）	
16			セキュアな開発環境と開発手法の適用	● セキュアコーディング手法の適用 ● 委託先を含む開発人員向けのセキュリティ対策、開発環境やコードへのアクセスの制御、開発環境と運用環境の分離等、安全な開発環境に必要な対応の実施 ● 設計書、プログラム、バイナリ等のバックアップ	
17			IoT 機器・システムにおけるセキュリティ機能の検証	● コード分析ツール又は脆弱性スキャナのような自動化ツール等を活用したセキュリティ機能に関する検証の実施 ● 情報収集サーバや監視用端末に対するペネトレーションテストの実施	
18			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	● 情報収集サーバや監視用端末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	
19			IoT 機器・システムにおける運用開始時の正しい設置、設定	● IoT 機器の事業者から提供されたガイドに従った設置、設定	
20	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	● 営業担当者、保守担当者、企業ホームページ等を通じた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の実施	
21			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	● セキュリティ管理責任者及びセキュリティ対策担当者が異動した場合の後任の選任	
22			過去の対応事例からの学習	● 発生したセキュリティインシデントの分析や解決から得られた知見の将来的	

				なインシデント抑制への活用（他社の類似サービスにおけるセキュリティインシデントを含む）	
23		プロシージャ	脆弱性対応に必要な手順等の整備と実践	● 脆弱性情報の収集及び評価の実施。 ● 状態監視システムに関連した脆弱性が明らかになった場合、これらの脆弱性に対応するための手順の整備。	
24			インシデント対応手順の整備と実践	● 状態監視システムに適応したインシデント対応手順の整備。 ● サポート事業者とユーザ事業者（金属製品製造事業者）の役割と責任の識別及び指定された個人によって実行されるアクションの定義・伝達 ● インシデント対応手順の定期的な訓練。	
25			IoT 機器・システムの適正な運用・保守	● 状態監視システムの適切な運用手順の整備 ● 運用手順に従った保守、管理	
26			IoT 機器・システムの適正な使用	● 状態監視システムを対象としたサービス提供や管理のポリシー提示及び遵守 ● 状態監視システムを対象としたセキュリティパッチの適用手順の提示	
27		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	● 状態監視システムや監視用端末にて扱う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、知的財産法）又は各製造事業者にサービスを提供する場合に契約上の義務に対する違反を避けるための要求事項の遵守 ● 関係省庁から公表されているガイドライン（例：経済産業省「AI・データの利用に関する契約ガイドライン」、「営業秘密管理指針」等）が更新された場合、更新されたガイドラインへの対応	
28			継続的な資産管理	● 各種センサを含む状態監視システムの資産目録（機器上に実装されたソフトウェアおよびファームウェア、工場出荷時の設定等を含む）の作成・維持	
29			プログラムソースコード及び関連書類の保護	● 状態監視システムに係るプログラムソースコード及び関連書類（例：設計文書）への論理アクセスを最小限にした上で、閲覧、編集等に際して多要素認証を実施	
30			IoT 機器・システムのモニタリング及びログの取得、分析	● 状態監視システムを構成する情報収取サーバや監視用端末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。 ● ルータを対象とした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。	
31			IoT 機器・システムに対するアップデートの適用	● 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 ※新たに検知された情報収集サーバ上のアプリケーション及び各種センサに係る脅威や脆弱性の報告窓口は既に設置されているものとする。	

- ユーザ事業者（金属製品製造事業者）が実装する対策の例

ユーザ事業者（金属製品製造事業者）で対応が必要な対策について、サポート事業者はサービス提供時に対策を依頼するものとする。ユーザ事業者（金属製品製造事業者）は主に以下の対策要件を実装

2176 するものとする。

2177 ただし、ユーザ事業者（金属製品製造事業者）では、「IoT 機器・システムの設置場所等に対する物理
2178 的アクセスの制御」及び「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」の対策を
2179 既に実施済みである想定だが、ここでは改めて対策の例を記載する。

2180 表 43 ユーザ事業者（金属製品製造事業者）が実装する対策の例

No	第 3 軸	実装先	対策要件	実際に講じる対策の例	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	適切なネットワークの分離	● 新たに導入するセンサを含むネットワークと既存の生産制御システムを含むネットワークの分離	
2			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	● 外部の物理的な脅威から保護されるべき各種センサやルータへの認可されていないアクセスを防ぐ目的で、入退管理（例：職員証や入館ゲート等）を通じた物理的セキュリティ境界の確立。	
3			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	● 業務上重要な施設への物理アクセスに対する監視カメラ等によるモニタリング。	
4			IoT 機器・システムにおける運用開始時の正しい設置、設定	● IoT 機器の事業者の想定する仕様に適合したネットワーク環境の整備	

2181

添付 A 対策要件

「IoT セキュリティ・セーフティ・フレームワーク」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以下に整理する。

対策要件の実装先は、「ソシキ・ヒト」、「プロシージャ」及び「システム」に分けられる。

「ソシキ・ヒト」には、「バリュークリエーションプロセスに参加する組織・団体・組織」や「その組織に属する人及び価値創造過程に直接参加する人」のセキュリティ向上を目的とした非技術的な対策要件（例：セキュリティ対応組織の設置や関連するポリシーの策定等）が該当する。

「プロシージャ」には、セキュリティ能力の向上を目的として、「目的を達成するための一連の活動の手続き」を定めた非技術的な対策要件（例：脆弱性対応に必要な手順等の整備と実践等）が該当する。

「システム」には、「目的を実現するためにモノで構成される仕組み・インフラ」のセキュリティ能力の向上を目的とした技術的な対策要件が該当する。

「システム」に該当する対策要件は、IoT 機器・システムにて一般的に想定されるライフサイクルの段階の順で示す。

例えば、第 1 の観点は以下の段階の順で示す。

- 企画・設計（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）
- 開発（例：適切な水準のアクセス制御の実装）
- 試験（例：IoT 機器・システムにおけるセキュリティ機能の検証）
- 設置（例：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 の観点は、以下の段階の順で示す。

- 運用（例：継続的な資産管理の実施）
- 廃棄（例：IoT 機器・システムの安全な廃棄または再利用）

表 A-1 対策要件の例

第 3 軸	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
		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
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
	プロシージャ	脆弱性対応に必要な手順等の整備と実践
		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
		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

2204

添付 B 実際に講じる対策の例

本添付資料では、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[36]。具体的な対策の内容は、業種や事業者に固有の条件等により様々に異なることが想定されるが、以下の内容は、そうした個別の検討を行う際の共通的な基礎のひとつになることを意図するものである。

なお、読者においては、以下の記載事項が何ら事業者にとっての義務的な事項を含んだものではなく、単に IoT 機器・システムにおいてセキュリティ対策等を実装する際の参考情報を示すものとなっている点に留意されたい。

第 3 軸における観点	実装先[37]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
第 1 の観点	ORG	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[38]。 - 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
		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	● 自組織の IoT 機器・システム、サービスの提供または利用に係るセキュリティポリシーに沿って、対象機器・システムのセキュリティに対する役割と責任の割り当てを行い、その内容を文書化した上で関係者に周知する。 ● 割り当てる役割と責任には、以下が含まれていることが望ましい。 - 意思決定等を行う経営層（CISO 等）及びその補佐 - 機器・システムの企画・設計段階におけるセキュリティ仕様の検討	CPS.AE-2 CPS.RM-1

[36] 第 4 の観点には、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネットの構築等）が該当するが、IoT 機器・システムを開発、提供あるいは利用する事業者が講じるべき対策とは性質が異なる内容のため、本添付資料での記載は割愛している。

[37] 添付 B では、実装先として添付 A に示したもののうち、「ソシキ・ヒト」を「ORG」、「システム」を「SYS」、「プロシージャ」を「PRO」と表記する。

[38] 産業サイバーセキュリティ研究会ワーキンググループ 1（制度・技術・標準化）スマートホームサブワーキンググループ「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 Version 1.0」添付E-5

			- 機器・システムの開発段階におけるセキュリティ対策の実装と運用 - IoT 機器・システムに係る調達先及び委託先の管理 - 機器・システムの企画や設計、開発を担当する者を対象にした意識向上、教育・訓練プログラム - 開発環境等における脆弱性やインシデントへの対応 ※ より具体的な実施内容等については、経済産業省「サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き 第1.1版」等を参照されたい。	
		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・システムのライフサイクルの全体にわたり、IoT 機器・システムの提供または利用に係る自身の役割を考慮しつつ、関係する IoT 利用者、IoT サービス開発者、IoT サービス提供者の責任を特定することが望ましい。 - IoT サービス開発者は、適宜 IoT 利用者と連携し、例えば以下の要件に対応した開発、実装における役割を果たすことが望ましい。 ➢ 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 - IoT サービス提供者は、IoT 機器・システム及び関連サービスの運用、保守において、IoT 利用者との分担も念頭に置きつつ、例えば以下の要件に対応した役割を担うことが望ましい。 ➢ 脆弱性対応に必要な手順等の整備と実践 ➢ サービスと IoT 機器・システムのガイドに従った保守、管理 ➢ IoT 機器・システムのモニタリング及びログの取得、分析 - IoT 利用者は、IoT 機器・システム及び関連サービスの利用において、例えば以下の要件に対応した役割を担うことが望ましい。 ➢ IoT 機器・システムにおける運用開始時の正しい設置、設定 ➢ IoT 機器・システムの用途・用法を守った使用 ➢ IoT 機器・システムの安全な廃棄または再利用 ● 機器・システムの運用中に発生したインシデントにより損害が発生した場合の責任範囲や対応を契約関連文書等において明確にしておくことが望ましい。 - 契約内容に違反した場合の措置 - インシデントが発生した場合の対応 - 新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応 - 契約終了後の情報資産の扱い（返却、消去、廃棄等）	CPS.AM-7 CPS.BE-1 CPS.BE-3 CPS.SC-2 CPS.SC-10 CPS.DP-1
		IoT 機器・システムに係る要員のセキュリティ確保	● IoT 機器・システムの提供または利用に係る自組織の要員及び委託先の従業員等が、雇用前、雇用期間中、雇用終了後にわたってセキュリティに関する役割を認識し、実行できるよう、例えば以下に示す対策を実施することが望ましい。 - 雇用前の対策 ➢ 対象者が、セキュリティに関する役割と責任を果たすために必要な能力を備えているかどうかの確認 ➢ 秘密保持契約書または守秘義務契約書への署名 - 雇用期間中の対策 ➢ 対象者へのセキュリティ上の役割と責任に関する要点の伝達 ➢ チェックリストの確認やログのレビュー等を通じた、対象者によるセキュリティ上の要求遵守の定期的な確認 - 雇用終了後の対策 ➢ 雇用の終了以降も一定期間継続する秘密保持契約等の適用 ● IoT 機器・システムの提供または利用に係る自組織の要員及び委託先の従業員等は、職務に対応した適切な教育や訓練を受け、自身のセキュリティに係る役割と責任について十分な認識を有していることが望ましい。教育の内容は当事者の役割等により変わり得るが、組込まれ得る事項として、例えば以下がある。 - インシデントを通じて組織や個人が被り得る影響とその一般的な動向 - 組織内のセキュリティ関連規則、手順等の内容	CPS.SC-5 CPS.SC-9 CPS.AT-1 CPS.AT-2 CPS.AT-3 CPS.IP-9

			- セキュリティに関する手順(例:インシデントの報告)や管理策(例:パスワード等の設定、ソフトウェアの更新、開発環境のセキュリティ確保)の実施方法	
	SYS	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	● IoT 機器・システムの提供または利用に係る組織は、新たに機器・システムを開発する場合、あるいは既に開発されている機器・システムにおいて関連する法令等が変更された場合に、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みをレビューし、最新に保つことが望ましい。 ● 関連する法令、規制及び契約上の要求事項を特定する際には、対象機器・システムに限定せず、全社的に日頃より自組織が受ける法的な規制やガイドラインを明確化し、各システムが規制対象となる場合の法令等と遵守事項、罰則などを文書化しておく。 ● 特に個人情報保護法は 3 年毎の見直しに連携し、業界向けのガイドラインの改定もあるため留意する。また、GDPR を始めとする他国の規制について、関連があれば文書化しておく。	CPS.GV-2
		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	● IoT 機器・システムを現に開発、運用する以前の企画・設計の段階で、当該機器・システムに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を特定すること(いわゆる、「セキュリティ・バイ・デザイン」)が望ましい。 ● セキュリティ・バイ・デザインを具体的に実践する過程では、以下の活動を実施することが望ましい。 - 適用範囲の決定:セキュリティ対策の対象となる IoT 機器・システム及び関連する組織、ヒトの活動を特定する。 - リスクアセスメント:対象の IoT 機器・システムによる目的の達成を妨げ得るリスクを網羅性も意識しつつ特定し、その影響の大きさや起こりやすさ等を考慮して、対応策を検討するうえでの優先順位づけを行う。 - リスク対応策の具体化:上記にて特定され、評価されたリスクに対処するための方策を選定し、具備すべき要求事項として仕様化する。セキュリティ要求事項には様々なものが選定され得るが、例えば以下が挙げられる。 ➢ 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 ➢ マルウェア対策の実施 ※ より具体的な実施内容、プロセス等については、IPA「制御システムのセキュリティリスク分析ガイド 第 2 版」や ISO 31000:2018 等を参照されたい。	CPS.RA-3 CPS.RA-5 CPS.RA-6 CPS.IP-3
		適切な水準のアクセス制御の実装	● 想定されるリスクの大きさに応じて、単一または複数の要素を組み合わせた適切な手法により IoT 機器や関連するシステムにアクセスするユーザ、機器の識別及び認証を行う。適用可能な要素とその具体例は以下の通り。 ＜ユーザ(ヒト)の認証＞ - 知識:パスワード - 所有物:IC カード等のハードウェア - 生体情報:指紋、顔、指静脈等 ＜IoT 機器の認証＞ - MAC アドレス等の機器に割り振られる識別情報 - ハードウェア機構により保護された電子証明書等 ● 以下の対策等を通じて、上記の要素による認証に必要な情報を安全に保つ。 - パスワードは、文字数や文字種等の観点で十分な複雑性を持たせ、ハッシュ化等したうえで適切に保護する。 - IC カード等の認証用の所有物は、紛失、盗難等から厳重に保護する。 ● 機器内外に保存されている IoT 機器の識別、認証情報は、論理的または物理的な不正アクセスから適切に保護する。	CPS.AC-1 CPS.AC-3 CPS.AC-4 CPS.AC-5 CPS.AC-6 CPS.AC-9

		ソフトウェアの完全性の検証	● IoT 利用者または IoT サービス提供者は、ソフトウェアを実行する前に、当該ソフトウェアの完全性を確認することが望ましい。 ● ソフトウェアの完全性を検証する際、確認すべきものとして以下がある。 – 信頼の基点とセキュアブートメカニズム – ソフトウェアの出所（当該ソフトウェアがベンダーによって署名された信頼できるソースのものか） – ソフトウェアの入手経路のセキュリティ（例：暗号化された接続を介してダウンロードされているか） – ソフトウェアの署名またはチェックサム	CPS.DS-10 CPS.DS-13 CPS.CM-4
		ソフトウェアのインストールの制限	● 不要なソフトウェアや既知の脆弱性を持つソフトウェアは、バックドアの設置や脆弱性の悪用等を通じて攻撃者に利用される可能性があることから、IoT 利用者または IoT サービス提供者は、組織内でソフトウェアのインストールを管理するための規則を確立し、実施することが望ましい。 ● 具体的な管理策には以下のようなものがある。 – ホワイトリストの作成等を通じて、認可されていないソフトウェアの使用を防止または検出する。 – ブラックリストの作成等を通じて、悪意のあるソフトウェアであると知られている、または疑われるソフトウェアの使用を防止または検出する。 – 上記のリストは、ベンダーから提供されるか、またはベンダーとの協議で定義され、定期的に、またはシステムの変更を実施する際に見直す。 – 特定の特権を許可された利用者によりソフトウェアのインストールが可能となることがあるため、特権の付与を最小限にする。	CPS.IP-2
		様々な IoT 機器に接続する際のセキュリティの確保	● IoT 機器、ネットワーク、サーバ等から構成されるシステムは、様々な IoT 機器との接続を適切に管理し、意図したセキュリティ水準を維持すべきである。 ● 設計、開発の段階で予定している IoT 機器またはサーバ等との接続に関しては、接続する IoT 機器に関する情報（例：製造者、モデル、製造年、準拠規格）を明確化し、提供する機能や情報の範囲を特定したうえで、運用前に動作確認を行う。 ● 設計、開発段階で必ずしも想定していなかった機器との接続を行う場合、製造者等が事前に十分な検証を実施できないことも想定されるが、このような状況に備えて、システムに以下のような機能を実装することが検討され得る。 - ホワイトリストを使用して他の IoT 機器との接続を制御する。 - 機器との接続交渉時、接続先機器に関する情報（例：製造者、モデル、製造年、準拠規格）を取得し、接続可否の判断や、提供する機能、情報の範囲の調整を行う。	CPS.AC-8
		暗号化によるデータの保護	● 技術的に可能な場合、IoT 機器やサーバ等の記憶媒体に保管されるデータ及び、ネットワークを通じて転送されるデータの機密性や完全性を、暗号技術を適切に利用しつつ保護する。 ● サーバ上の保管データに対して、データの保管形態や重要度に応じてファイルの暗号化やデータベースの暗号化を行う。 ● ネットワークを通じて転送されるデータに対して、技術的に可能な場合、機密性だけでなく完全性や真正性も含めた保護を行うため、TLS や IPsec 等のプロトコルを利用する。 ● 利用する暗号技術については、信頼できる機関が発行する文書等（例：CRYPTREC 暗号リスト(電子政府推奨暗号リスト)）を参照し、安全でない方式を無効にする。	CPS.DS-2 CPS.DS-3 CPS.DS-4 CPS.DS-11 CPS.CM-4

			● 機能や性能が限られた IoT 機器では、暗号等のセキュリティ対策を適用できない場合があるため、機器内に機微なデータを保管しない、ゲートウェイ等のネットワーク機器にてセキュリティ機能を補完する等の措置を実施する。	
		ライフサイクルを通じた暗号鍵の管理	● 暗号によりデータを保護する期間の全体にわたって、利用する暗号鍵を安全に管理する。その際、以下の事項に関して検討を行うことが望ましい。 - 暗号鍵管理システムの設計原理と運用ポリシー - 暗号アルゴリズム運用のための暗号鍵管理オペレーション対策 - 暗号アルゴリズムの選択 - 暗号アルゴリズム運用に必要な鍵情報の管理 - 暗号鍵管理デバイスのセキュリティ対策 - 暗号鍵管理システムのオペレーション対策 ※ 各事項における具体的な実施内容等については、IPA「暗号鍵管理システム設計指針（基本編）Ver. 1」等を参照されたい。	CPS.DS-5
		マルウェア対策の実施	● IoT 機器・システムをマルウェアから保護するため、「IoT 機器・システムに対するアップデートの適用」や「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」等の実施に加え、端末及びネットワーク上にて多層的に以下の対策を実施することが望ましい。 - 外部ネットワークまたは可搬媒体経由でファイル及びソフトウェアを取得する際にマルウェア検出を実施する。 ➢ 端末にマルウェア対策ソフトウェア（パターンファイル、振舞い検知等の方式による）を導入し、外部から取得した全てのファイルに対して使用前の検査を行う。 ➢ ネットワーク上にセキュリティ機器（例：IDS/IPS、ウェブアプリケーション・ファイアウォール）を導入し、セキュアでない外部サイトとの通信や不審な通信を検知し、適宜遮断等の対応を実施する。 - マルウェアの検知に利用するソフトウェア等のバージョンを、信頼できる出所を利用して、常に最新の状態に維持、更新する。 - パソコンやサーバ等の端末の状況および通信内容などを監視し、異常、あるいは不審な挙動を検知した際に管理者に通知する。 - マルウェア等の脅威について最新の情報を収集する手段やプロセス（例：ISAC への参画、脅威インテリジェンスに係るサービスの利用）を整備する ● 機器の種類によっては、計算能力が低い、OS が実装されていない等の理由で十分なマルウェア対策を実装できない場合がある。そのような場合、かかる機器が接続する「上位の IoT 機器・システム」（例：IoT ゲートウェイ、ルータ）にて通信ファイル等に対するマルウェア検査を実施することが望ましい。	CPS.DS-10 CPS.CM-3
		IoT 機器・システムの十分な可用性の確保	● IoT サービス開発者または IoT 利用者は、対象機器・システムの可用性に関する業務上の要求事項を特定し、機器・システムを設計、開発する。また、機器・システムの運用時においても、リソースの利用を監視・調整し、将来必要とする容量・能力を予測することが望ましい。 ● 対象において高い可用性の保証が求められる場合、通常稼働するものとは別に構成要素を複数用意しておき、異常が発生した際であってもシステム全体の停止を回避できるよう、システムを冗長化する。その場合、冗長化した構成要素への切替えを意図したとおりに行うため、あらかじめ試験を行っておくことが望ましい。 ● 機器の故障、自然災害等によるデータの消失に備えるため、IoT サービス提供者または IoT 利用者は、データ、ソフトウェア及びシステムイメージのバックアップを定期的に取得し、検査することが望ましい。 ● 他の機器・システム等との関係で高い可用性や信頼性が必要とされる場合、ネットワークの停止や停電が発生した場合でもローカルで動作を継続し、停電等から回復した場合にはスムーズに復旧する	CPS.DS-6 CPS.DS-7 CPS.IP-4 CPS.IP-5

			回復性(レジリエンス)を機器やサービスに組み込むことが望ましい。	
		IoT に適したネットワークの利用	● IoT 機器間または IoT 機器とサーバの間の通信で利用するネットワークの方式(例:Wi-Fi、Bluetooth、LPWA、5G 等の移動通信)を、セキュリティ機能、通信速度等のパフォーマンス、以下に示すその他の観点を踏まえて決定する。 - 通信元の IoT 機器と通信先の物理的な距離 - IoT 機器の可動性の有無 - ネットワークの帯域幅 - 同時接続可能な機器の数 - 消費電力量	-
		適切なネットワークの分離	● IoT 機器・システムを構成するネットワークに関して、必要に応じて、共通のセキュリティレベルを持つセグメントを構築し、他のセグメントと論理的または物理的に分離する。本番環境と開発環境、インターネット経由でアクセス可能な社内ネットワークと生産拠点の制御ネットワークの分離等がかかる例に該当し得る。生産拠点等の情報システム及び制御システムのネットワークについて、下記のように階層化を行う場合がある。 – 情報系ネットワーク 企業内で構築された LAN で、外部ネットワーク(インターネット等)との接続点に存在する。 – 制御情報系ネットワーク 情報系ネットワークまたは DMZ 上のサーバ等との間で、制御目的に使用するためのステータス情報やデータを転送する。 – 制御系ネットワーク 制御ネットワーク及びフィールドネットワーク上の機器(コントローラ)との間で、制御目的に使用するためのステータス情報やデータを即時転送するためのネットワークであり、制御に特化した高い応答性を持つ。 – フィールドネットワーク 制御ネットワークのコントローラ等の接続機器とフィールドに存在する機器の間の通信に用いられる。 ● 上記環境では、基本的に同一セグメント内でのみ通信を行い、セグメント間の通信を行う場合はファイアウォールやゲートウェイ等のネットワーク機器により制御する。 ● 可能であれば、安全計装用のネットワークを他のネットワークから分離する。	CPS.AC-7 CPS.AC-8 CPS.DS-9 CPS.CM-1
		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・システムが設置される領域(例:事業所、サーバ室)を保護するために, 物理的セキュリティ境界を定めることが望ましい。 ● 定められた物理的セキュリティ境界の内部に認可されていない者がアクセスできないよう、適切な入退管理(例:IC カードによる認証)を行う。その際、機微なデータや重要なプロセスを取扱う資産が所在する場所については、組織内または関係する取引先等であってもアクセスできる要員を最小限にする。 ● 物理的セキュリティ境界内部に対するあらゆる物理的なアクセスの記録を保管しておき、定期的にレビューする。	CPS.AC-2 CPS.CM-2
		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	● 自然災害(例:火災、洪水、地震)や他の物理的な脅威(例:盗難、破壊、改造)に起因する障害に対処するため、IoT 機器・システム及びそれが設置される施設等は適切に保護(例:耐震性や火災への耐性の確保)されていることが望ましい。 ● 電磁波の放射等による情報漏えい(サイドチャネル攻撃)のリスクを最小限にするため、機微なデータを処理する機器を保護する。	CPS.DS-8

			● IoT 機器・システムが外部からの物理的な脅威に晒されやすい場所（例：公共空間等の拠点外で管理者のいない場所）に所在し得る場合、以下を考慮することが望ましい。 - 耐タンパ化等により、末端の IoT 機器（センサ、アクチュエータ）を物理的な盗難、破壊、改造から保護する。そのような保護が限られる場合、機器・システムの利用者は物理的な脅威によるリスクが残存することを認識し、運用中に必要に応じて当該機器・システムが正しい状態で稼動しているかを確認することが望ましい。 - 暗号鍵等の機微なデータを取扱う機器内のコンポーネントを不正な開示や改ざんから保護する。	
		セキュリティ設計と両立するセーフティ設計の仕様化	● IoT 機器・システムの開発者は、セキュリティインシデントが結果的に機器・システムのセーフティ側面に及ぼし得るリスク（例：制御データの改ざんによる誤動作の発生、マルウェア感染による機器・システムの安全機能の停止）を認識し、それらに適切に対処する方策を検討する。有効となり得る方策として、例えば以下が挙げられる。 - 異常検知時にフェールセーフを実現する安全機能を実装する。 - 安全機能の動作に影響を与える可能性のある IoT システムに対する脅威を考慮し、当該安全機能を通信機能と分離する 等 ● IoT サービス開発者は、実装しようとするセキュリティ管理策が IoT システムとその安全機能の動作に与える影響も考慮して、実際に履行する管理策の検討を行う。	CPS.RA-4 CPS.PT-3
		セキュアな開発環境と開発手法の適用	● IoT 機器・システムの開発に係るヒトやプロセス、設備（開発環境）をより安全なものとするため、以下の点を考慮することが望ましい。 - 開発環境で業務に従事する人員（外部委託を含む）のセキュリティに係る能力 - 上記人員に対する開発環境へのアクセス制御 - 本番環境や別の開発環境との分離、環境間でのデータ移動の管理 - 開発環境の変更及び、保管されたコードに対する変更の監視 ● 機器・システムの開発に際して、フリーソフトウェア/オープンソースソフトウェア（FOSS）や関連 OS および利用コンポーネントの脆弱性管理を実施する。FOSS について、開発環境を狙った不正コードを含むコンポーネントも報告されており、適切な管理を通じて開発環境の汚染を抑制することが望ましい。 ● 以下に示すようなセキュアなソフトウェア開発の手順や手法を、IoT 機器・システムの開発に適用する。 - 安全なソフトウェア開発のためのライフサイクル - 言語別のセキュアコーディングに関する指針	CPS.AC-7 CPS.IP-3
		IoT 機器・システムにおけるセキュリティ機能の検証	● IoT 機器・システムの開発者、または利用者は、当該機器・システムを現に利用し始める前に、セキュリティ機能を含む要求事項が設計した通りに実装され、正しく機能することを検証する必要がある。検証の実施に際しては、信頼できる外部事業者による検証サービスを利用することも想定される。 ● 機器・システムの開発者、利用者及び（適切な場合）外部の検証サービス事業者は、検証実施に際して以下を実施することが望ましい。 - 準備：必要な情報の整理や検証目的、スコープの明確化を行う。 - 計画：検証に係る体制や環境を構築し、検証項目やその手法を具体化する。検証の手法には、静的手法（例：設計文書レビュー、ソースコード解析、バイナリ解析）と動的手法（例：ネットワークスキャン、既知脆弱性の診断、ファジング）等が存在するが、検証の目的や費用、検証実施者のスキル等を考慮して適切なものを選択することが望ましい。 - 検証の実施：計画段階で特定された項目について、合意された手法により検証を行う。	CPS.IP-3 CPS.DP-3

			- 分析：検証結果に基づき、特定・検出された脆弱性や脅威がある場合、想定される影響や対応策の案を分析する。 - 報告：分析・整理された検証結果に基づき、検証報告書を作成する。 ※ IoT 機器をはじめとするネットワークに常時接続する機器、及び関連サービス（ただし、IoT 機器等が接続するサーバやシステム全体の検証は除く）のセキュリティ検証において、検証依頼者と検証サービス事業者が行うべき事項等を詳細化する場合は、別途、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」等を参照されたい。	
		信頼できる IoT 機器やサービスの選定	● IoT の利用者、または他の事業者から機器・システムのコンポーネントを調達してサービス等の開発・提供を行う事業者は、自身が取得する機器・システム及びコンポーネントのセキュリティに関する要求事項や、以下に例示するようなその他の要求事項を定めることが望ましい。 - 機器・システムに係るサポートの実施及び、それを受けられる期間 - 開発者や供給者が機器・システム等の仕様変更を行う際の事前の通知 - セキュリティ等に係る問題を検知した際の問合せ先 ● かかる要求事項を検討する際、既存のガイドライン等を参照して対象の特性を踏まえつつ、セキュリティ要求事項を具体化することが望ましい。 ＜業種横断的な参照ガイドラインの例＞ - ISO/IEC 27001:2013 - ISO/IEC 27017:2015 [対象：クラウドサービス] - NISTIR 8259 シリーズ [対象：個々の IoT 機器] - IoT セキュリティガイドライン Ver.1.0 [対象：IoT システム] ● 利用者自身で適切な IoT 機器・システム及び関連サービスの選定が困難な場合、販売店や Web サイト等で公開されている資料の活用、IoT 機器やサービスの選定が可能な事業者への相談等の対応を実施することが望ましい。	CPS.SC-1 CPS.SC-3 CPS.SC-4 CPS.DS-15
		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 機器やサービスの運用前（設計・製造段階）の初期設定や構成を、一定水準のセキュリティが確保できるものとする。その際に考慮すべき IoT 機器やサービスの設定や構成、想定される対策例として以下のようなものがある。なお、一定水準のセキュリティとは、機器・システムごとに異なる。一方で、ポリシーで一定水準が定義される場合、当該ポリシーを参照するものとする。 - ネットワークポート、その他 USB やシリアルポート：運用前の段階で利用しないと考えられるものを、物理的または論理的に閉塞する。 - ソフトウェアのバージョンとパッチ：IoT 機器・システムに運用前の段階で不要と考えられるアプリケーション、機能がある場合、利用者への提供までに削除、無効化、停止する。 - サービスの機能やデータへのアクセス制御：IoT 機器・システムが利用者にパスワードを要求する場合、初期段階も含めて製品のライフライクル全体をとおしてセキュリティ強度を高く維持できるようにする。 ● 特に IoT 機器は、初期段階に弱いパスワードが設定される場合が多く、初期段階でパスワード強度を上げるメカニズムが必要である。そのような措置として、例えば、機器ごとに固有の推測されにくいパスワードを用意する、または機器ごとに初期パスワードが同一である場合に初回の利用時等に一定の複雑さを持つパスワードを変更しない限り利用できないようにする等が考えらえる。	CPS.IP-1 CPS.PT-2
		IoT 機器・システムにおける運用開始時の正しい設置、設定	● IoT サービス開発者は、IoT 機器やシステムを構成するその他の設備を設置、設定する際、機器の動作仕様を考慮しつつ、想定されるセキュリティインシデントや危害を回避や軽減するために提示された	CPS.IP-1

			ガイドやポリシーに従って業務を行い、運用開始までに動作状況を確認することが望ましい。 ● IoT 機器を公共空間や事業者の敷地外、住戸外等の外部のヒトが接触可能な場所に設置する場合、IoT サービス開発者/提供者は、不正な改造や不正なソフトウェアのインストール、ネットワークの不正利用防止についてあらかじめ留意しておくことが望ましい。	
第 2 の観点	ORG	利用者へのリスクの周知等の情報発信	● IoT 機器・システムの運用段階において、セキュリティ対策の一部を IoT 利用者が実施する必要があることから、IoT サービス開発者(IoT 機器製造者を含む)または IoT サービス提供者は、以下のようなサイバーセキュリティ関連情報について、想定されるリスクとともに利用者に発信することが望ましい。 － 提供する IoT 機器・システムの正しい利用方法(例:設定や構成の変更方法) － サポート対象の IoT 機器・システム及びその構成要素 － ソフトウェア更新の有無 － 利用者側で実施が必要な保守作業 － 脆弱性及び緩和措置に関する注意喚起 － サポートまたはサービス提供の終了時期 － 利用者向け窓口の連絡先 ● 対策の内容の機密性等にも配慮しつつ、IoT サービス開発者(IoT 機器製造者を含む)または IoT サービス提供者が、例えば以下の発信を通じて、機器・システムにおけるセキュリティ対策の水準を対外的に広報することも、利用者からの信頼を確保する上で有用と考えらえる。 － 取得している第三者認証等 － 適用している規格や対策の概要 － 情報セキュリティ報告書における取組み内容の紹介	－
		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	● 自組織の IoT 機器・システム、サービスの提供または利用に係るセキュリティポリシーに沿って、対象機器・システムのセキュリティに対する役割と責任の割り当てを行い、その内容を文書化した上で関係者に周知する。 ● 割り当てる役割と責任には、以下が含まれていることが望ましい。 - 意思決定等を行う経営層(CISO 等)及びその補佐 - 機器・システムの運用段階における対策の実装と運用 - IoT 機器・システムの運用に係るサービスの委託先の管理 - 機器・システムの運用担当者や利用者向けの意識向上、教育・訓練プログラム - 機器・システムの運用時における脆弱性やインシデントへの対応 ※ より具体的な実施内容等については、経済産業省「サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き 第1.1版」等を参照されたい。	CPS.RM-1 CPS.AE-2
		過去の対応事例からの学習	● IoT 利用者または IoT サービス提供者は、自身が管理する IoT 機器・システムまたは関連するその他の機器・システムにおいて発生したセキュリティインシデントから得られた知見を、今後の対策強化に活用することが望ましい。 ● 取得できる知見の情報源として、例えば以下が挙げられる。 － 自社で発生したインシデントへの対応結果及び、対応後の原因分析 － 信頼できる外部機関(例:セキュリティベンダ、情報共有基盤(ISAC/ISAO)、政府機関、学会等)からの情報発信や注意喚起 ● 機密性の側面に留意する必要はあるが、実際に発生したセキュリティインシデントを、それに対する対応や事前に取るべきだった対策等を含め、利用者向けの教育のコンテンツとして用いることができる。	CPS.IP-7 CPS.IM-1 CPS.IM-2

			● 取得した知見に基づき、機器・システムの管理者は、必要に応じて以下をレビューすることが望ましい。 – リスクアセスメントの結果(例：想定されるセキュリティインシデント等とその結果、機器・システムに潜むリスクの程度、脅威の整理結果への変更) – リスク対応の内容 – インシデントや脆弱性への対応体制や手順等	
	PRO	脆弱性対応に必要な手順等の整備と実践	● IoT サービス開発者または IoT サービス提供者は、自身が開発、提供している機器・システムに係る脆弱性の情報を収集、分析、必要に応じて関係者に周知し、最終的にソフトウェアやファームウェアの更新等の措置を講じる必要がある。 ● 脆弱性対応の手順には、以下の対処が含まれていることが望ましい。 – 脆弱性情報の収集： 製品開発者が提供する情報や、セキュリティベンダやセキュリティ関連機関(IPA、JPCERT/CC、ISAC 等)がホームページやメール等で提供するアドバイザリ等を利用して情報収集を行う。また、自社製品に関する脆弱性情報に関する連絡を受けるため、対外的な窓口を設置することが望ましい。 – セキュリティ上の問題の有無に関する調査： 入手した脆弱性情報について、自社システム上の脆弱性の有無や問題が発生する条件等を調査する。 – 影響と対策の方向性の検討： 問題箇所が及ぼす影響を特定し、修正方法や回避方法を検討する。 – 対策作業計画の策定 対策作業を進める手順や期間等について計画を策定する。費用、人員等を勘案しつつ、機器・システムの利用部門(例：製造部門)とも十分にコミュニケーションをとったうえで、代替機でのテスト、対策実施に伴うサービスの停止と再開等を計画する。 – 対策の実施 作業計画に基づき対策を実施する。具体的な方法等については、「IoT 機器・システムに対するアップデートの適用」も参照されたい。	CPS.RA-2 CPS.IP-10 CPS.CM-7 CPS.RP-2
		インシデント対応手順の整備と実践	● セキュリティインシデントに対する迅速，効果的かつ順序だった対応を確実にするため、管理層の責任及び手順を確立することが望ましい。 ● 組織は、自身の役割や対応の対象となるシステムの種別等を考慮して、例えば以下に挙げるようなインシデント対応組織を確立することが望ましい。 – IT システム：CSIRT(Computer Security Incident Response Team) – 製造現場：FSIRT(Factory Security Incident Response Team) – 製品・サービス：PSIRT(Product Security Incident Response Team) ● インシデント対応手順には、以下のプロセスを含めることが望ましい。 – 検知・受付連絡： 「IoT 機器・システムのモニタリング及びログの取得、分析」に示す組織内部の活動や、外部からの通報受付を通じて、インシデントの発生を検知する。 – トリアージ： 得られた情報に基づいて、事実関係を確認し、その情報を得たインシデント対応組織が対応すべきインシデントか否かを判断する。 – インシデント対応： インシデントにより生じた被害の特定、原因の分析を行ったうえで、被害の拡散を防止し、被害箇所の原因の根絶、修復を行い、復旧をする。 – 報告/情報公開	CPS.AE-4 CPS.AE-5 CPS.RP-1 CPS.RP-2 CPS.CO-1 CPS.AN-1 CPS.AN-2 CPS.AN-3 CPS.MI-1

			必要に応じて、組織内部への情報展開の他、メディアや一般に向けたプレスリリースや監督官庁への報告を行なう。 ※ より具体的な実施内容等については、JPCERT/CC「インシデントハンドリングマニュアル」等を参照されたい。	
		事業継続計画の策定と実践	● IoT 利用者または IoT サービス提供者は、対象の IoT 機器・システムを含む自身が管理するシステム群の継続を、自社の事業継続計画（BCP）や事業継続管理（BCM）プログラムに組み込むことが望ましい。 ● 策定する BCP には、以下の事項を含めることが望ましい。 － 対象業務及びシステム群を対象とした BCP の実施・運用体制 － 想定する危機的事象 － 被害状況の想定 － 業務及びシステムの復旧優先度、目標復旧時間 － システム構成要素ごとの対策目標 ● BCP/BCM において規定している事業継続上の要求事項を満たすため、例えば以下に示す対策要件のレビューや追加的な実装を行うことが望ましい。 － IoT 機器・システムのモニタリング及びログの取得、分析 － インシデント対応手順の整備と実践 － IoT 機器・システムの十分な可用性の確保 ● BCP/BCM においては、危機的事象として、自然災害のみならず、サイバー攻撃を考慮し、以下に示すような特性を十分に踏まえることが望ましい。 － 災害等とは異なり、標的を定めて攻撃が行われることが多い － 被害状況を把握しづらく、早期発見には障壁がある － 対処後も再度攻撃を受ける可能性があるため、原因究明が必要	CPS.AE-4 CPS.AE-5 CPS.RP-3 CPS.CO-2 CPS.CO-3
		IoT 機器・システムの適正な使用	● IoT サービス開発者または IoT サービス提供者は、IoT 利用者に対して、機器・システム及び関連するサービスの適正な使用に関するガイダンスを提供することが望ましい。 ● IoT 利用者は、IoT サービス開発者/提供者から提示されるガイダンスに従い、機器・システムを設定し、利用する。 ● 利用者に提示されるガイダンスの内容には以下が含まれ得る。 － 設置方法 － 安全な使用環境（例：ネットワーク設定、構成）、使用方法 － IoT 機器が収集する情報 － セキュリティアップデートの適用方法 － 適格なパスワードの基準 － サポート期間 ● 上記に加え、IoT 利用者には機器・システムの使用に伴い発生し得る、例えば以下のようなセキュリティインシデントや危害も通知されることが望ましい。 － IoT 機器のマルウェア感染 － 個人情報の漏洩 － 企業情報の漏洩 － IoT 機器の踏み台化	CPS.IP-1 CPS.PT-2
		IoT 機器・システムの適正な運用・保守	● IoT サービス開発者または IoT サービス提供者は、提供する機器・システムの運用手順を文書化し、利用者に対して示すことが望ましい。また、IoT 利用者及び IoT サービス提供者は、提示された運用手順に沿って、機器・システムの操作や保守を行う必要がある。 ● 提示する機器・システムの運用・保守に関する手順には、例えば以下の事項に関する説明を示すことが望ましい。 － 機器の（再）起動または停止の手順 － バックアップの取得及び管理 － 外部媒体（例：USB メモリ）の取扱い － アップデートの適用	CPS.IP-1

			− 障害等が発生した際にサポートを受けるための連絡先 − 機器・システムのパフォーマンスや問題事象等の監視 ● 機器・システムを外部の事業者に委託等する場合、IoT 利用者及び IoT サービス提供者は、作成した運用・保守に関する手順書を委託先に示し、契約期間中も手順の遵守を定期的に確認することが望ましい。	
	SYS	運用中における法令および契約上の要求事項の遵守	● IoT 機器・システムの提供または利用に係る組織は、新たに機器・システムを開発する場合、あるいは既に開発されている機器・システムにおいて関連する法令等が変更された場合に、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みをレビューし、最新に保つことが望ましい。 ● 関連する法令、規制及び契約上の要求事項を特定する際には、対象機器・システムに限定せず、全社的に日頃より自組織が受ける法的な規制やガイドラインを明確化し、各システムが規制対象となる場合の法令等と遵守事項、罰則などを文書化しておく。 ● 特に個人情報保護法は 3 年毎の見直しに連携し、業界向けのガイドラインの改定もあるため留意する。また、GDPR を始めとする他国の規制について、関連があれば文書化しておく。	CPS.GV-2 CPS.DP-2
		継続的な資産管理の実施	● IoT 機器・システムの運用を担当する IoT サービス提供者または IoT 利用者は、管理対象の IoT 機器・システムの資産目録（インベントリ）を作成し、継続的に管理する。 ● 資産目録では、各資産に管理責任者や重要度等を割り当て、手動または自動的な方法により、正確かつ最新の内容となるように管理する。 ● 管理対象となる資産及び管理すべき情報(例)には以下が含まれる。 − ハードウェア 機器種別、名称、ネットワークアドレス、管理者、性能情報、OS 情報 − ソフトウェア及びファームウェア 名称、バージョン、ライセンス情報、アップデートの適用状況 − 取扱われるデータ 名称、種別（例：個人情報、営業秘密）、重要度、管理者、保管媒体、　利用目的	CPS.AM-1 CPS.AM-6 CPS.RA-1 CPS.CM-6
		プログラムソースコード及び関連書類の保護	● 想定していない機能の組込みや意図しない変更を回避するため、IoT サービス開発者または IoT サービス提供者は、対象となる IoT 機器・システムに関連したプログラムソースコード及び関連書類（例：設計書、仕様書、検証計画書、妥当性確認計画書）へのアクセスや変更履歴（例：作成日時、変更日時、変更点）を厳重に管理する。 ● プログラムソースコードはデータベース（リポジトリ）に格納し、以下に示すような管理を適切に行いつつ、複数の開発者間で閲覧及び編集を行えるようにする。 − プログラムソースコードを運用システムの中に保持しない。 − 委託先等も含めた開発要員によるリポジトリへのアクセスを最小限にする。 − リポジトリ及び格納されているプログラムソースコードへの全てのアクセスのログを取得し、保持する。 − プログラムソースコードの保守及び複製を行う際は、あらかじめ定められた管理手順に従う。 − プログラムソースコードの公開を意図している場合、その完全性を保証するために追加の管理策（例：デジタル署名）を考慮することが望ましい。	CPS.AC-1 CPS.AC-4 CPS.AC-5 CPS.AC-6 CPS.AC-9
		IoT 機器・システムのモニタリング及びログの取得、分析	● 機器・システムの故障、不審な動作等を早期に検知し、対処するため、対象の IoT 機器・システムの運用時において、IoT 利用者または IoT サービス提供者は、利用者の活動、機器・システムの挙動、	CPS.DS-9 CPS.PT-1 CPS.AE-3

			セキュリティに係る事象を記録したログを取得し、安全に保持し、定期的にレビューすることが望ましい。 ● 取得及びレビューの対象となり得るもの、現に取得やレビュー等を行おうとする際の注意事項等として、例えば以下が挙げられる。 ＜対象となる機器・システムの例＞ － 末端の IoT 機器（センサ及びアクチュエーター） － 制御システムを構成する機器等（例：PLC、DCS、SCADA） － ネットワーク機器（例：IoT ゲートウェイ、ルータ、ファイアウォール） － サーバ（クラウドとオンプレミスの双方を含む） － 業務用端末 ＜対象となり得るログ等の例＞ － 機器・システムに対するアクセス（例：ユーザ認証の成功及び失敗） － 機器・システムの操作履歴、特に正常でないとみなされ得る動作（例：事前に想定されていない外部サーバ等との通信、不正なプログラムのインストール） － センサまたはアクチュエータの通常の範囲を超えた値 － 対象システムの構成変更 － 対象システム内または外部ネットワークとの間のネットワークトラフィック － IoT 機器またはシステムを構成するその他の機器の停止 － プロセッサとメモリの使用状況 － IoT 機器の物理的な位置 － 温度や湿度等の機器が位置する環境の状況 ＜注意事項等＞ － ログの取得や保管、通信等にかかるリソースを考慮すると、あらゆる機器からあらゆる種類のログを取得し、レビューすることは現実的ではないため、対象となる機器やログの種類に優先順位をつける必要がある。例えば、ログの取得や保管、異常の報告ができない IoT 機器が含まれる場合、システムを構成するサーバやネットワーク機器でモニタリングやログの取得を行う必要がある。 － 取得し、レビューするログの正確性を担保するため、IoT システム内で時計を同期させることが望ましい。 － 論理的または物理的なアクセス制御、バックアップの取得、改ざん検知、暗号化等を通じて、機器・システムのログ機能及びログを、改ざん及び不正なアクセスから保護することが望ましい。	CPS.CM-1 CPS.CM-2 CPS.CM-5
		IoT 機器・システムに対するアップデートの適用	● IoT 機器・システムを構成するソフトウェアやファームウェアの更新は、以下の機能の実装等を通じて、不正アクセス等の脅威に対して安全に実施される必要がある。 － 更新プログラムは、IoT 機器・サービスの開発者の正規のウェブサイト等、信頼できるソースから提供されるべきである。 － 更新プログラムを受信する機器は、更新を開始する前に、当該プログラム及び発信者の完全性及び真正性を検証する必要がある（例：デジタル署名、署名証明書、署名証明書チェーンの検証）。 － 更新が無線ネットワーク経由で遠隔から行われる場合、通信経路は適切な方式により暗号化されるべきである。 － 更新に利用される暗号鍵は、完全性と真正性を保護するために安全に管理されるべきである。 － 更新を実行することにより機器・システムの既存の運用が悪影響を受けないよう、更新の実行前にあらかじめ動作検証等を行うことが望ましい。 ● 更新を実行したことにより IoT 機器・システムのセキュリティレベルが低下する事態を防ぐため、遠隔からの更新処理は、完全に成功するか、失敗したとしても以下に示すようにロールバック可能な状態となっている必要がある。 － 更新の失敗に備え、ソフトウェアやファームウェアをロールバックする仕組みを実装することが望ましい。	CPS.MA-1 CPS.MA-2

			– 平時の運用において、不正なダウングレードやロールバックがなされないよう、それらを防止する仕組みを実装することが望ましい。	
		IoT 機器・システムの安全な廃棄または再利用	● IoT 機器やIoTシステムを構成するその他の機器を廃棄したり、中古品として売買したりする際、保管されているデータの重要度や各種法の実行可能性等を加味しつつ、以下に挙げる方法等に基づき、機微情報やライセンスされたソフトウェア等の消去、あるいはデータの上書きを行うことが望ましい。 – データ抹消ソフトウェア(データに異なるランダムなデータを複数回上書きしてデータを抹消するソフトウェア)によりファイルを抹消する – ハードディスクを消磁装置に入れてディスク内のデータを抹消する – 媒体を物理的に破壊する – データが暗号化された状態で保管されている場合に、暗号鍵を消去することで、元データへと複合できないようにする – 機器を工場出荷時の状態に初期化する ※ データ保管媒体の安全な廃棄方法に関するより詳細な情報については、米国国立標準技術研究所(NIST)「SP 800-88 rev.1 媒体のデータ抹消処理(サニタイズ)に関するガイドライン」(IPA 翻訳)等を参照されたい。	CPS.IP-6
第 3 の観点	ORG	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 利用者または IoT サービス提供者は、現に機器・システムの運用・管理を行う自社または委託先等の担当者が、安全で信頼できる運用を実現しようとするにあたり有すべき適格性(知識や技能等)に関する要求事項を特定し、担当者を割り当てる際に十分考慮することが望ましい。 ● かかる適格性に関する要求事項には、業種や業務によって様々なものが含まれ得るが、担当する業務の執行に係る知識や経験、それらと関連する限りにおいてパーソナリティ側面等が考慮され得る。 ● 業種や業務によっては、業法や関連する資格制度等により能力が規定され、資格の取得等が(事実上)義務化されている場合がある。	CPS.SC-5
		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	● IoT 利用者または IoT サービス提供者は、IoT 機器・システムの運用・管理を担当する者(候補者を含む)が特定された要求事項を満たしているかどうかを、業務の実施前または実施中の適切なタイミングで、例えば以下の手段により確認することが望ましい。 – 推薦状(例えば、業務や人物に関するもの) – 該当者の履歴書(記載が正確であるかの確認を含む) – 業務に係る資格等の(公的な)証明書 – 信用情報や犯罪履歴等の入手 ● 上記の確認は、プライバシー保護及び雇用に関する法令の全てを考慮に入れた適切な方法で行われなければならない。	CPS.SC-5

2213