参考資料１

IoT セキュリティ・セーフティ・フレームワーク Version 1.0

適用実証報告書

目　次

1. 適用実証の実施概況

経済産業省では、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「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。) を 2020 年 11 月に公表した。また、2022 年 4 月には、IoT-SSF をより活用しやすいものにすることを目的として、「IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集」(以下、「ユースケース集」という。) を公表した。

ユースケース集の策定に向けた検討会の議論の中では、ユースケースやフィードバックの収集を目的として企業が実際に IoT-SSF を適用すべきとのご意見や IoT-SSF の第 3 軸「求められるセキュリティ・セーフティ要求の観点」の対策内容を更に具体化すべきという意見が提示された。

そこで本年度は、参考となる事例の蓄積を通じた利用促進や IoT-SSF の改善点の洗い出しを目的として、先進的な取組みを行う事業者より協力を得て、表 1 に示す 4 件の IoT-SSF の適用実証を実施した。各適用実証については、2 章で詳細を示す。

表 1 適用実証一覧

No	利用者の区分	業界	名称	参画事業者	対象システム/サービスの概要
1	個人又は家庭	スマートホーム	スマートホームサービス窓シャッター連携	住宅メーカ、シャッター製造販売事業者	住宅メーカが提供している住宅に居住の住まい手が、契約したサービスを通じて窓シャッターの遠隔操作を行う。
2			家庭用エアコン遠隔操作	エアコン製造事業者	エアコンの遠隔操作のために開発したシステム。住まい手が外出先より遠隔でエアコンを操作し、リビングを快適な温度に調整する。
3	事業者(主に産業)	製造	ボイラーの遠隔監視	日本電気制御機器工業会(オブザーバ:日本ボイラ協会)	ボイラーを設置している工場において、ボイラーのより安定的な稼働を目的として、ボイラーの制御装置等によりボイラーの遠隔監視を行うことを想定する。
4			設備保全業務支援サービス	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	受変電・電気設備をはじめとする設備に設置した各種センサ、エッジコントローラなどから得たデータに基づいて、運転情報、保全情報を可視化/分析することで、各設備・機器に最適なメンテナンスを提供するサービス。

また、上記適用実証の実施と並行して、参画いただいた各社から、以下のような IoT-SSF 改善のためのデータを収集し、今後の IoT-SSF 及び関連する検討活動へのインプットとすることとした。それらの内容については、3 章を参照されたい。

- 適用した際に感じたメリット/デメリット
- 適用して気付いた新たなリスク
- 適用の際の問題点/悩んだ点(他の文献とのハレーションを含む)
- IoT-SSF等の改訂に向けた要望等

2. 各適用実証事業の概要

2-1 スマートホームサービス窓シャッター連携

本ユースケースは、住宅メーカ、及びシャッター製造販売事業者が、住宅メーカが提供している住宅に居住する住まい手向けに提供しているスマートホームサービス及び、スマートホームサービスと連携する窓シャッターを対象に IoT-SSF に基づくリスクアセスメント及びリスク対応を行った結果をまとめたものである。

住宅メーカが提供するスマートホームサービスは、IoT 機器からのデータをクラウド上で蓄積し、在宅中、外出中に関わらずスマートフォンアプリから住まいの状態を確認、操作できるサービスである。今回の対象となる窓シャッターの遠隔操作を始めとして、玄関ドアの状態確認、不正開放を通知、温湿度センサで住環境を可視化し、熱中症のアラートを出す、家族の帰宅、外出の通知をお知らせ、機器操作履歴の確認などに対応する。

住宅メーカ及びシャッター製造販売事業者は、対象機器・システムに関するリスクアセスメントを行い、リスクに対してはステークホルダー間で対策内容を調整することで、可能な限り、リスクを低減する。住宅メーカ及びシャッター製造販売事業者は、一般社団法人重要生活機器連携セキュリティ協議会(以下、「CCDS」)が提供する IoT 機器を対象としたサーティフィケーションを取得している。住宅メーカは、サーティフィケーションのうち Lv.2(★★)を取得済み、シャッター製造販売事業者はLv.1(★)を取得済みであり、当該サーティフィケーションに係る対策は実装済みである。

住宅メーカ、シャッター製造販売事業者は、既存のソリューションを対象に 1 つのユースケースを作成したことで事前に調整を行う必要が生じた。責任分界点を改めて明確化した上で既存の認証制度と整合性を図りつつリスク対応を行った。

(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

住宅メーカにお住まいのお客様(住まい手)が、スマートフォンアプリを通じて窓シャッター(シャッター製造販売事業者製、住宅メーカが調達、施工)の遠隔操作を行うソリューションを対象とする。住まい手は、自身のスマートフォンから 24 時間 365 日窓シャッターを操作することが可能となる。

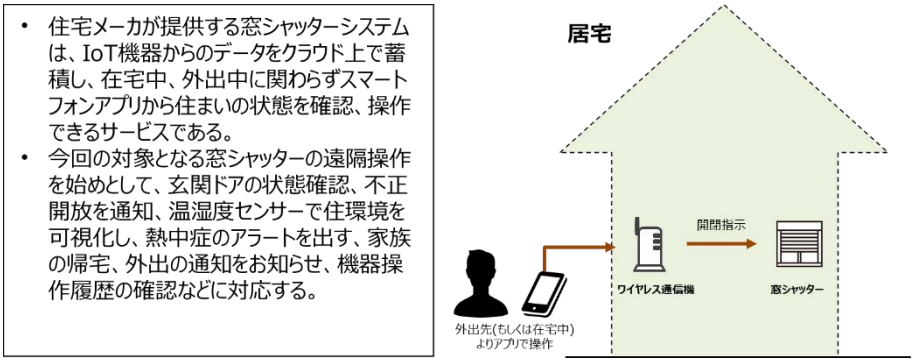


図 1 対象ソリューションのイメージ

② ステークホルダー関連図

本ユースケースにて示す取組に関与するステークホルダーは、以下に示すように住宅メーカやシャッター製造販売事業者、クラウドベンダ、インテグレータ、コンタクトセンタ、住まい手を想定している。契約関係や製品・サービスの提供関係を考慮したステークホルダー関連図は、以下に示すとおりである。

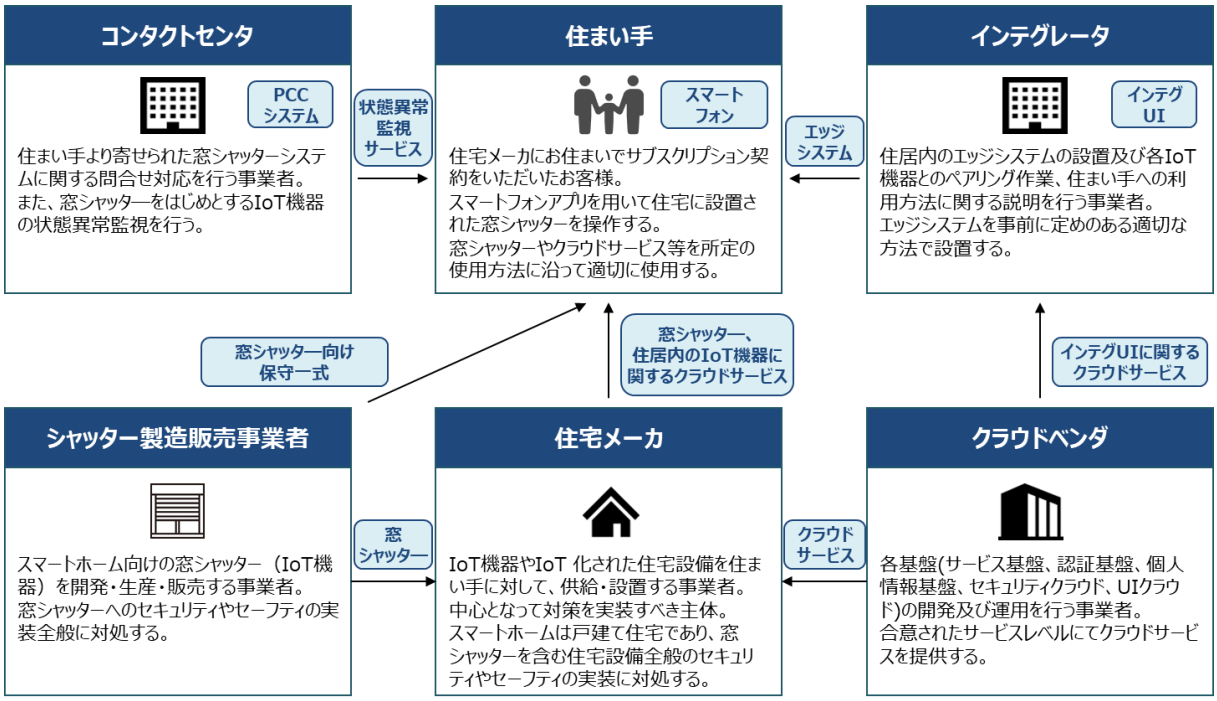


図 2 ステークホルダー関連図

＜IoT サービス開発者/IoT サービス提供者＞

● 住宅メーカ

住まい手に対して、IoT 機器や IoT 化された住宅設備を供給・設置する事業者であり、中心となって対策を実装すべき主体。対象とする建物は、戸建て住宅であり、窓シャッターを含む住宅設備全般のセキュリティやセーフティ対策の実装を行う。

● シャッター製造販売事業者

スマートホーム向けの窓シャッター(IoT 機器)を開発・生産・販売する事業者。窓シャッターへのセキュリティやセーフティ対策の実装を行う。

● クラウドベンダ

各基盤(サービス基盤、認証基盤、個人情報基盤、セキュリティクラウド、UI クラウド)の開発及び運用を行う事業者。合意されたサービスレベルにてクラウドサービスを提供する。

● インテグレータ

住居内のエッジシステム(居内の各機器との通信を行う機器)設置及び各 IoT 機器とのペアリング作業、住まい手への利用方法に関する説明を行う事業者。事前に定めのある適切な方法でエッジシステムを設置する。

● コンタクトセンタ

住まい手より寄せられたスマートホームサービスに関する問合せ対応を行う事業者。また、窓シャッターをはじめとする IoT 機器の状態異常監視を行う。

＜IoT サービス利用者＞

● 住まい手

スマートホームサービスを契約した住宅メーカに居住する住人。スマートフォンアプリを用いて住宅に設置された窓シャッターを操作する。窓シャッターやクラウドサービス等を所定の使用方法に沿って適切に使用する。

③ システムを構成する機器の一覧

本ユースケースの対象となる機器は以下の通りとする。

96

表 2 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
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エッジシステムに指示を出すシステム。 業務効率化を目的として外部のクラウドベンダが提供するデータセンターよりクラウドサービスを提供している。 CCDS☆2[1]に基づいて、セキュリティ設定を行う。
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窓シャッターの遠隔操作を行う。 スマートフォンは、住まい手が所有するものを使用する。
インテグ UI	スマートフォン上のアプリケーションから住居内の各機器の操作、クラウドサービスで各機器の状態を管理できるようなスマートホームサービスを利用するためのインテグレーションを行うためのシステム
PCC システム	住居内の各機器の死活監視、異常状態管理を行うシステム。遠隔からのファームウェアアップデートや再起動指示も担う。
ルータ	住居内に設置され、住居内のネットワーク及び住居外のネットワークを中継する通信機器。ルータは、住まい手が準備するものとし、住居内の他の機器にも接続することを想定する。 CCDS☆2 に基づいて、インテグレータが設定する
エッジシステム	住居内の各機器との通信(状態取得、制御、死活、異常)を行う機器。機器を設置する際には、インテグレータが CCDS☆2 に基づいてセキュリティ設定を行う。
ワイヤレス通信機 (無線親機)	エッジシステムから指示を受けることで、各窓シャッターへ開閉操作等が可能となる集中制御機器。機器内に特定の個人に関する情報は保管していない。 指示等の信号送受信に関して次の機能を有する。 ①ネットワークを通じてエッジシステムから窓シャッターの開閉指示を受ける。 ②上記①に応じ、対象窓シャッターへ開閉の指示信号を送信する[2] ③上記②で受けた窓シャッターの状態を、ネットワークを通じてエッジシステムへフィードバックする。
窓シャッター (無線子機)	ワイヤレス通信機やリモコンから指示を受けることで開閉操作などが可能となる窓シャッター。 機器内に特定の個人に関する情報は保管していない。 挟まれ防止機能として障害物感知時の反転動作などがある。防犯機能として、こじ開け防止制御などがある。 シャッター自体は軽量であり、駆動する動力も弱く、何かの原因でシャッターが上下した場合でも、挟まれて死亡するようなことには至らない。 指示等の信号送受信に関して次の機能を有する。 ①ワイヤレス通信機やリモコンからの開閉停の指示を受け開閉する。

[1] CCDS☆2:CCDS(重要生活機器連携セキュリティ協議会)サーティフィケーションプログラム レベル 2

[2] 送信信号は特定小電力の無線信号(独自プロトコル)

	②状態をワイヤレス通信機へフィードバックする。
リモコン	シャッター個々に付属され、窓シャッターへ開閉停の指示信号を送信する押しボタン式の無線リモコン。 機器内に特定の個人に関する情報は保管していない。 リモコンからの指示信号は、外部に接続するネットワークを経由しない。

④　システム構成図、データフロー図

本ユースケースで対象とするシステムは、住居内(敷地内)の機器及び住まい手が所有するスマートフォン、スマートホームサービスクラウド基盤、インテグレータのインテグ UI、コンタクトセンタの PCC システムから構成される。また、住居内(敷地内)の機器は、ルータやエッジシステム、ワイヤレス通信機、窓シャッター(リモコン附属)からなる。システム構成図は以下の通りとする。

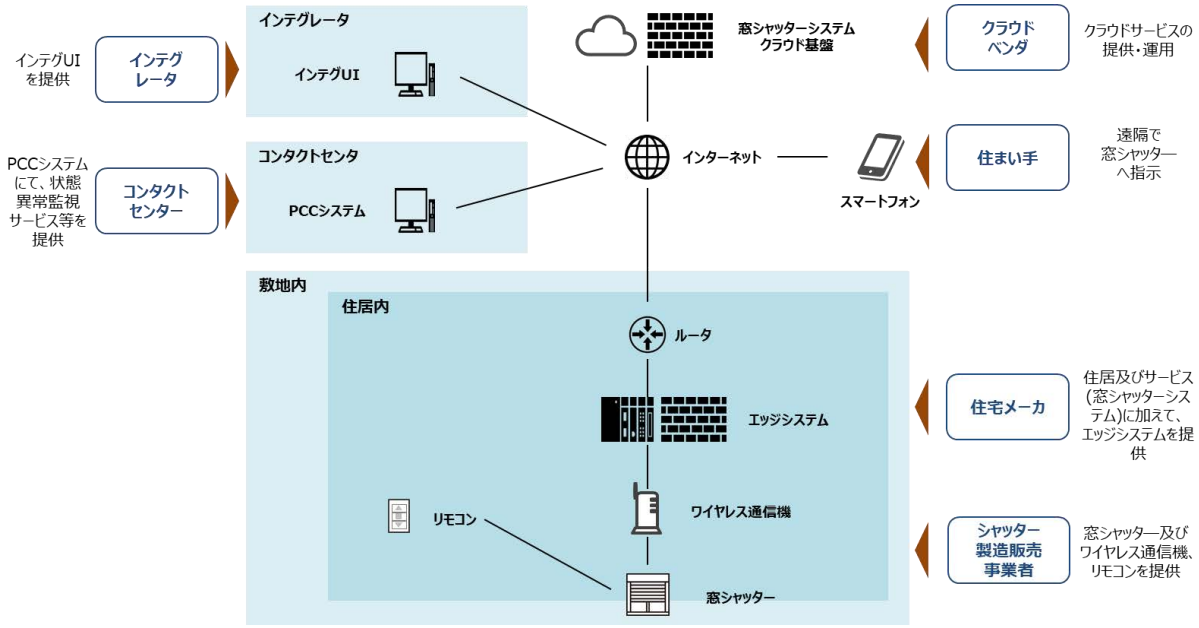


図 3 システム構成図

スマートフォンアプリから窓シャッター制御を行う場合のデータフローは以下の通りとする。本ユースケースでは以下の 2 パターンのデータフローを対象とする。

A) スマートフォンアプリから窓シャッター制御を行う場合のデータフロー

B) 窓シャッターから状態変化通知(異常、死活も同様)を行う場合のデータフロー

A) スマートフォンアプリから窓シャッター制御を行う場合のデータフロー

所有するスマートフォンを通じて窓シャッターを操作した上で、窓シャッターの動作完了後に住まい手が動作完了通知を受け取るまでのフローを対象とする。

＜機器制御通信＞

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. (～3)クラウドサービスからインターネットを通じて、ルータ経由でエッジシステムに指示を出す。
4. エッジシステムからワイヤレス通信機に指示を出す。
5. ワイヤレス通信機より窓シャッターに開閉指示を出す。

＜動作完了通知＞

6. 窓シャッターよりワイヤレス通信機に対して動作完了通知を送信する。
7. ワイヤレス通信機よりエッジシステムに対して動作完了通知を送信する。
8. (～9)エッジシステムからルータを通じてクラウドサービスに動作完了通知を送信する。
10. クラウドサービスより住まい手が所有するスマートフォンに対して動作完了通知を送信する。

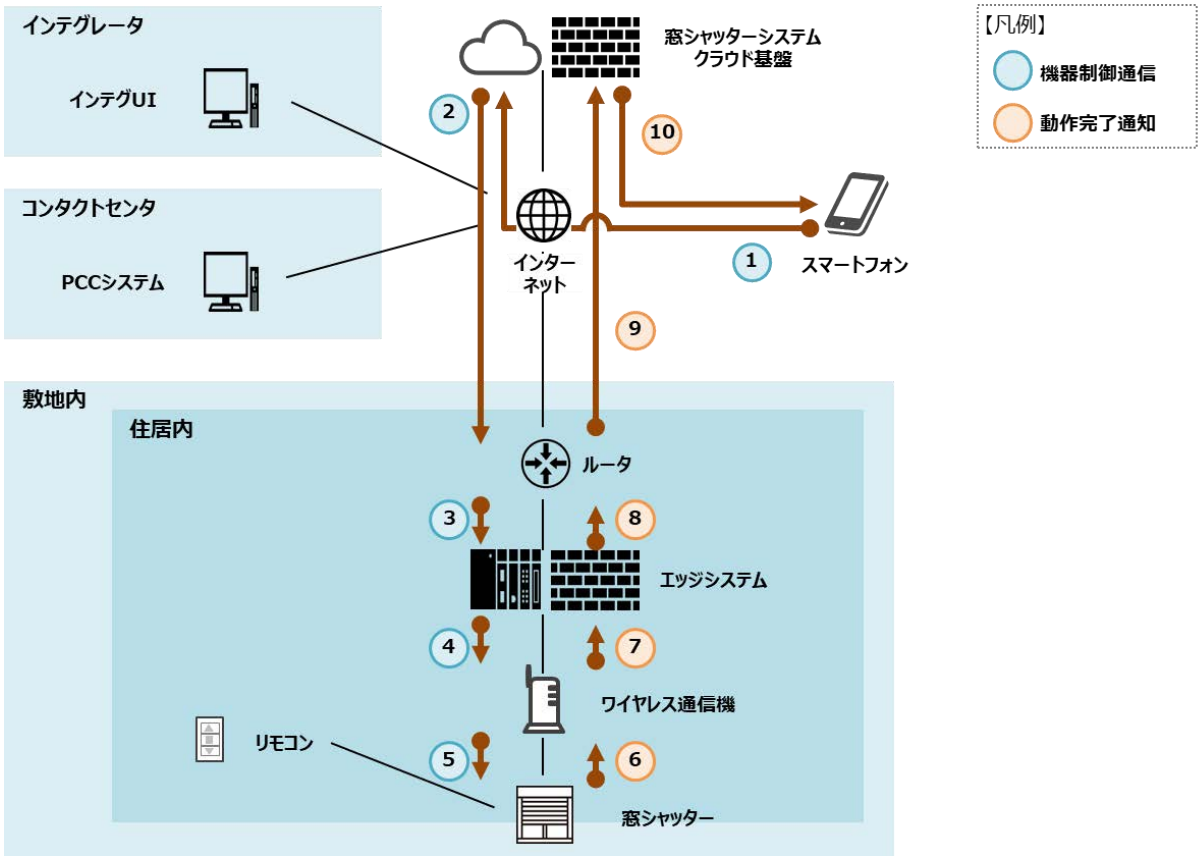


図 4 データフロー図(アプリからの窓シャッター制御を行う場合)

B) 窓シャッターから状態変化通知(異常、死活も同様)を行う場合のデータフロー

窓シャッターにて異常、死活を含めた状態変化が生じた場合、窓シャッターより住まい手が所有するスマートフォン及びコンタクトセンタの PCC システムへ状態変化通知が送信されるまでのフロー

を対象とする。

1. 窓シャッターよりワイヤレス通信機に対して状態変化通知を送信する。
2. ワイヤレス通信機よりエッジシステムに対して状態変化通知を送信する。
3. (～4)エッジシステムからルータを通じてクラウドサービスに状態変化通知を送信する。
5. クラウドサービスより住まい手が所有するスマートフォンに対して状態変化通知を送信する。
5. (同時に送信)クラウドサービスよりコンタクトセンタの PCC システムに対して状態変化通知を送信する。

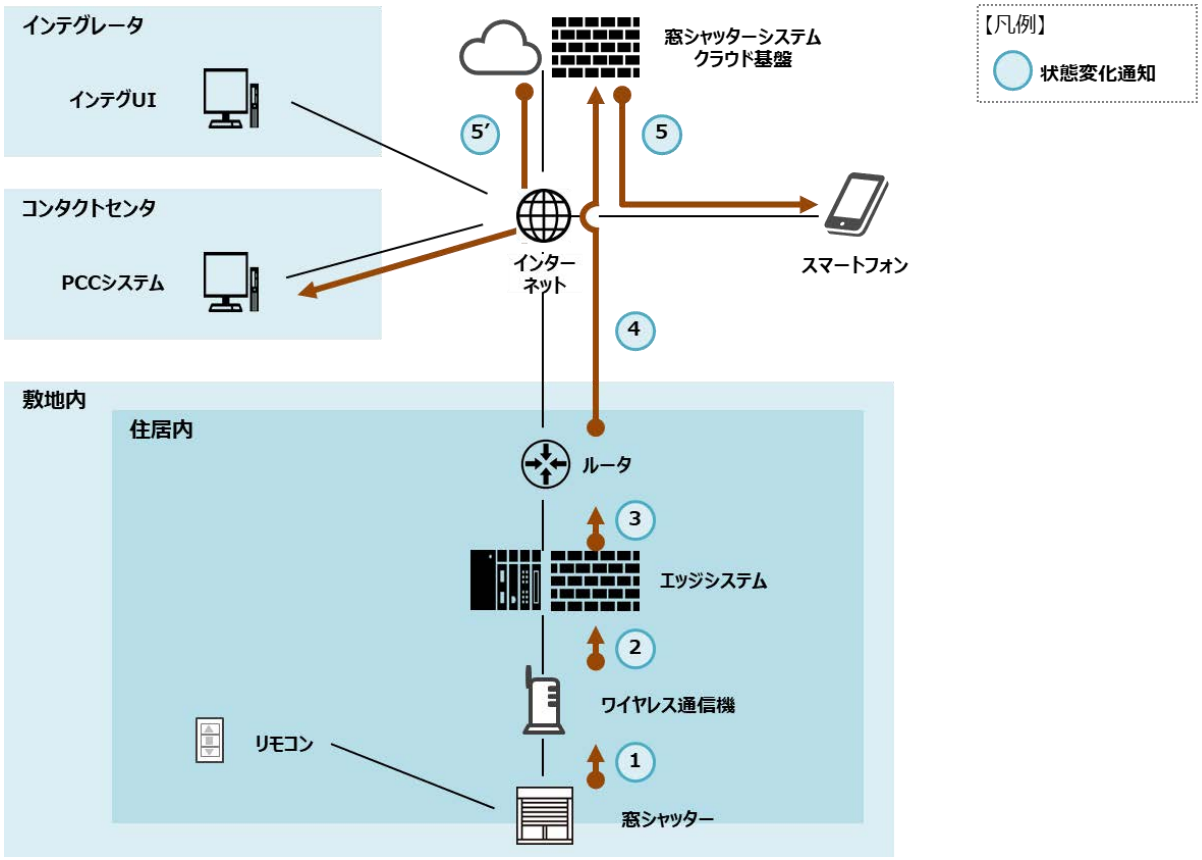


図 5 データフロー図(状態変化通知(異常、死活も同様)を行う場合)

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則り、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。

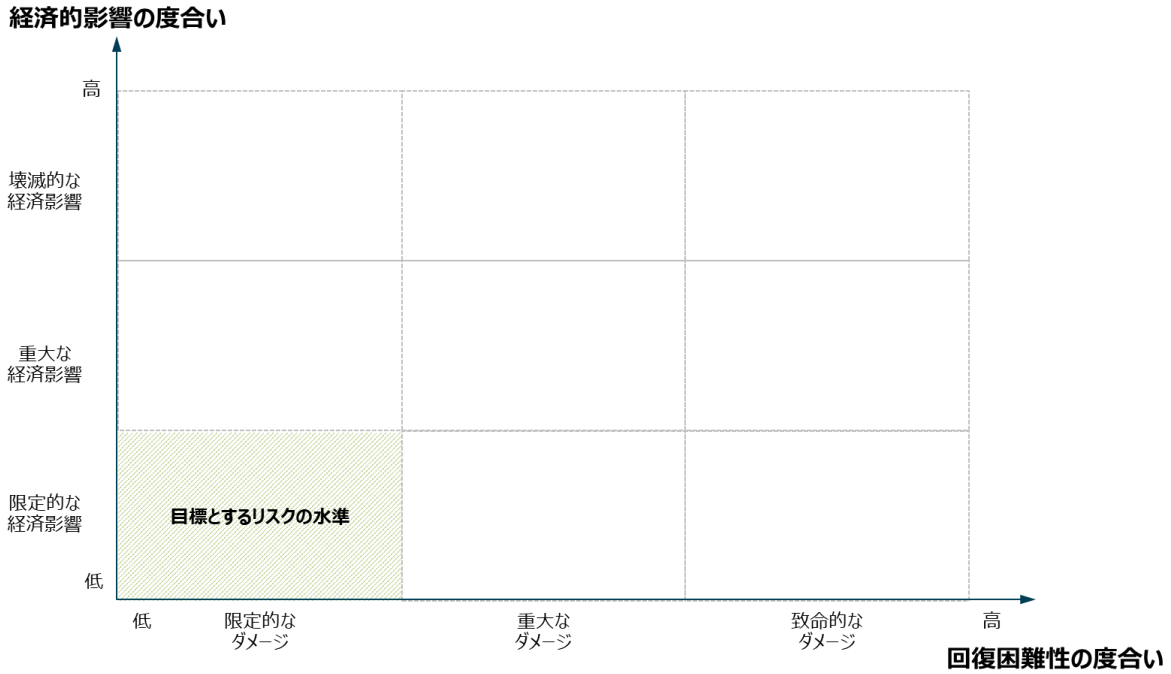


図 6 スマートホームサービスに連携した窓シャッターシステムにて目標とするリスクの水準

(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、窓シャッター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

窓シャッターシステムにおいて、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。窓シャッターシステムの提供又は利用に際して想定されるステークホルダーごとのセキュリティインシデント(例)は以下の通りである。

なお、図 4 に示した A)スマートフォンアプリから窓シャッター制御を行う場合のデータフロー(以下、「A のデータフロー」)及び図 5 に示した B)窓シャッターから状態変化通知(異常、死活も同様)を行う場合のデータフロー(以下、「B のデータフロー」)に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)は重複するものが多いことから、A のデータフロー及び B のデータフローにおいて想定され得るものを併せて以下に記載することとする。後述の「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」におけるリスクの値に直結する結果は下線太字にて記載する。

- 住まい手
- 住宅メーカ
- シャッター製造販売事業者

・　インテグレータ/コンタクトセンタ

- 住まい手
  - 住まい手にとっての想定され得るセキュリティインシデント及びその結果(影響)は多岐に渡ると想定される。住まい手にとってリスクの値が大きくなり得るのは、窓シャッターが想定していない動作をすることにより物の損傷や住まい手への危険が生じる場合や、それに伴って屋外やベランダ等への締め出しや、空き巣の侵入が発生した場合である。その結果を引き起こすセキュリティインシデントとしては、悪意のある攻撃者による制御データの改ざん等や、不正な機器のエッジシステムへの接続(不正接続)が挙げられる。悪意のある攻撃者によって、窓シャッターシステムのデータベースに保存された個人情報(スケジュール設定)が改ざんされ、特定の住宅にて窓シャッターの操作が不可能になる。
  - 窓シャッターの窓シャッターシステムのシステム運用者や、各基盤のシステム担当者によって、管理画面やファイルシステムから住まい手の個人情報が不正に参照される。また、システム運用担当者以外の要員によって、窓シャッターシステムのデータベースに保存された住まい手の個人情報が不正に参照される。その結果、住まい手の個人情報が流出する。
  - システム運用担当者以外の要員によって、窓シャッターシステムからログイン情報が取得され、住まい手のシャッターが不正に操作される。また、悪意のある攻撃者によって、窓シャッターシステムから各基盤への通信が傍受され、住まい手の窓シャッターが不正に操作されることや、各基盤の API を悪用して、任意のコードが実行される。その結果、窓シャッターが物・人をはさみ[3]、物の損傷や住まい手への危険が生じる。また、屋外やベランダ等への締め出しや空き巣の侵入が発生することにより、その結果として住まい手が負傷する可能性がある。
  - 悪意のある攻撃者によって、正常と偽って不正な機器がエッジシステムに接続される。その結果、窓シャッターが物・人をはさみ、物の損傷や住まい手への危険が生じる。また、屋外やベランダ等への締め出しや空き巣の侵入が発生することにより、場合によっては住まい手が負傷する可能性がある。加えて、住まい手の個人情報の流出も起こる可能性がある。
  - 悪意のある攻撃者によって、エッジシステムと窓シャッターの通信データが改ざんされる。また、クラウドサービスからエッジシステムやワイヤレス通信機に送信されるデータがネットワーク上で改ざんされることによって、窓シャッターが想定していない動作をする。**その結果、窓シャッターが物・人をはさみ、物の損傷や住まい手への危険が生じる。また、屋外やベランダ等への**

[3] 窓シャッターには独立した安全装置が備えられており、実際に物や人をはさむ可能性は少ないが、ここでは安全装置は考慮せずリスクアセスメントを行っている。リスク対応時にかかる装置を考慮した上で対策を検討するものとする。

締め出しや空き巣の侵入が発生することにより、場合によっては住まい手が負傷する可能性がある。

- 配信するエッジシステムやワイヤレス通信機のアップデートプログラムが改ざんされ、配信元偽装などの手法でインストールされることで、配信先のワイヤレス通信機がマルウェア感染し、想定していない動作をする。その結果、窓シャッターが物・人をはさみ、物の損傷や住まい手への危険が生じる。また、屋外やベランダ等への締め出しや空き巣の侵入が発生することにより、場合によっては住まい手が負傷する可能性がある。
- ワイヤレス通信機からエッジシステムやクラウドサービスに送信されるデータがネットワーク上で盗聴されることによって、窓シャッターの状態が悪意のある第三者に知られ得る。その結果、住居の窓シャッターの状態を悪意のある第三者が認識し得て、空き巣の侵入を許すことにより、住まい手が負傷する可能性がある。
- ルータへの攻撃などにより、ルータが不具合を起こし、クラウドサービスからエッジシステムへの通信が不通になる。その結果、宅外からの窓シャッター操作ができなくなり、窓シャッターの閉め忘れに伴う空き巣の侵入や飛来物(例:天候急変に伴う突風により生じる飛来物)による窓の破損が発生し得る。
- 引っ越し等に伴い住まい手が替わる際に、住まい手のスマートフォンやクラウドサービスの ID の登録が残っている。その結果、前の住まい手が宅外から操作可能な状態となる。
- 住まい手の独断でワイヤレス通信機を初期化せずに廃棄する。その結果、ワイヤレス通信機を自身のスマートフォンで操作可能に設定することにより、電波が届く範囲で悪意のある第三者が窓シャッターを操作でき得る。

- 住宅メーカ
  - クラウドサービスからエッジシステムやワイヤレス通信機に送信されるデータがネットワーク上で改ざんされることによって、窓シャッターが想定していない動作をする。また、配信するエッジシステムのアップデートプログラムが改ざんされ、配信元偽装などの手法でインストールされることで、配信先のワイヤレス通信機がマルウェア感染し、想定していない動作をする。その結果、窓シャッターが物・人をはさみ、物の損傷や住まい手への危険が生じる。また、屋外やベランダ等への締め出しや空き巣の侵入が発生することにより、場合によっては住まい手が負傷する可能性がある。**住まい手への影響が及ぶことによって、住宅メーカは原因調査・製品改修が生じ得る。また、製品・サービスの品質について住まい手の間に懸念が広がり、ブランド力の低下も起こり得る。**

- シャッター製造販売事業者

  - クラウドサービスからエッジシステムやワイヤレス通信機に送信されるデータがネットワーク上で改ざんされることによって、窓シャッターが想定していない動作をする。また、配信するワイヤレス通信機のアップデートプログラムが改ざんされ、配信元偽装等の手法でインストールされることで、配信先のワイヤレス通信機がマルウェア感染し、想定していない動作をする。その結果、窓シャッターが物・人をはさみ、物の損傷や住まい手への危険が生じる。また、屋外やベランダ等への締め出しや空き巣の侵入が発生することにより、場合によっては住まい手が負傷する可能性がある。**住まい手への影響が及ぶことによって、シャッター製造販売事業者は原因調査・製品改修が生じ得る。また、製品・サービスの品質について住まい手の間に懸念が広がり、ブランド力の低下も起こり得る。**
  - ワイヤレス通信機からエッジシステムやクラウドサービスに送信されるデータがネットワーク上で盗聴されることによって、窓シャッターの状態が悪意のある第三者に知られ得る。その結果、空き巣等が住居のシャッターの状態を認識し得て、住居へ侵入することにより、場合によっては住まい手が負傷する可能性がある。住まい手へ影響が及ぶことによって、シャッター製造販売事業者は原因調査・製品改修が生じ得る。また、製品・サービスの品質について住まい手の間に懸念が広がり、ブランド力の低下も起こり得る。

- インテグレータ/コンタクトセンタ

  - 住まい手に対して注意喚起(例：利用方法の説明など)が十分行われず、住まい手の人的ミスにてルータの誤設定や適切ではないルータの交換が生じる。その結果、窓シャッターがスマートフォンより操作できなくなることで、**サービスの品質について懸念が広がり得る。**

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。

- 住まい手
- 住宅メーカ/シャッター製造販売事業者
- インテグレータ/コンタクトセンタ

- 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

プライバシーの観点では、悪意のある攻撃者によって不正な機器が正常と偽ってエッジシステム

に接続されることで、個人情報が流出し得る。

セーフティの観点では、各機器を通じてクラウドサービスから窓シャッターに送信される制御データが改ざんされることによって、窓シャッターに人・物をはさみ、物の損傷や住まい手への危険が生じる。また、かかるデータの改ざんによって空き巣等による侵入を許し、場合によっては住まい手が負傷する可能性がある。

したがって、プライバシーの観点は個人情報が流出し得ること、セーフティの観点において状況によって住まい手が負傷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「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

「回復困難性の度合い」と同様に制御データの改ざんによって空き巣等が侵入した場合には、住まい手の生活に支障をきたし得る。また、その影響は一定期間続くと考えられる。

住まい手の生活に支障をきたした場合には他のサービスによって代替が難しい可能性がある。

したがって、空き巣等の侵入によって影響が一定期間続くこと、他のサービスによる代替が難しいことを考慮して、「経済的影響の度合い」は「重大な経済影響」と評価する。

- 住宅メーカ/シャッター製造販売事業者

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、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、窓シャッターが予期せぬ動作をしたとしても、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

直接的な経済影響の観点では、住まい手が負傷し、生活に支障をきたした場合、企業の信用、ブランド価値の低下や住まい手との契約解除に直結するおそれがある。

同様に間接的な経済影響の観点では、住まい手のけが等により大規模な製品回収につながるおそれがある。

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、インシデントが契約に影響し得ることやその影響が長期間に及び得ることから、「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。

- インテグレータ/コンタクトセンタ

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、今回対象としている範囲に限定すれば、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、窓シャッターが予期せぬ動作をしたとしても、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

住まい手に対する注意喚起(例：利用方法の説明など)が十分に行われず、住まい手の人的ミスによるルータの誤設定や適切ではないルータの交換が生じることよって、窓シャッターが動作せずサービスの品質について懸念が広がり得る。

一方で、上記に伴う影響は長時間に及ばず他の代替サービス(例:駆け付け対応)で補うことができるため、「経済的影響の度合い」は「限定的な経済影響」と評価する。

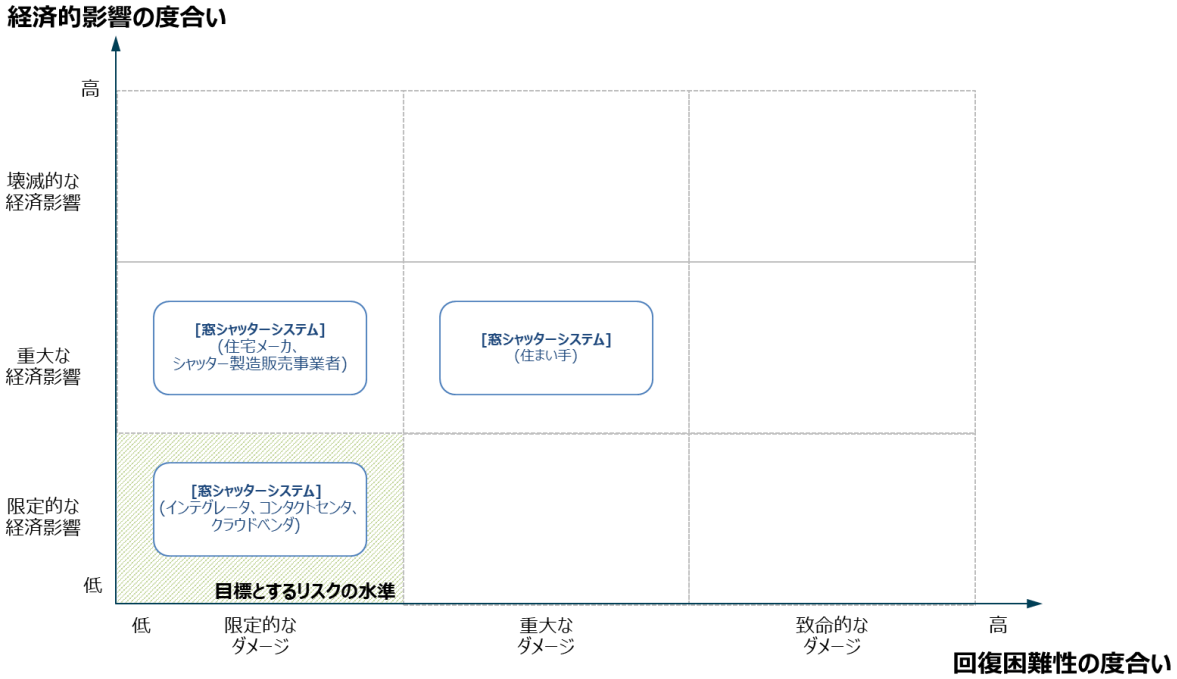
③ マッピング結果の整理と評価の実施

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。

これらを踏まえると、インテグレータやコンタクトセンタ、クラウドベンダ視点からみたスマートホームサービスの窓シャッターシステムで想定されるリスクは、目標とする水準に収まっているものの、住まい手や住宅メーカ、シャッター製造販売事業者視点からみたスマートホームサービスの窓シャッターシステムで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。

住まい手視点の「回復困難性の度合い」及び「経済的影響の度合い」を低減するためには、けが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取組みを推進することやフェールセーフ等を含む安全対策を徹底することが有効になると考えられる。また、機器・システムのセキュリティ上の欠陥を防ぐための取組みは住まい手に加えて、住宅メーカやシャッター製造販売事業

307 者視点の「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り得る。



308

309 図 7 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

310 ● 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

311 ➢ 住まい手のけが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取組
312 みの推進

313 ➢ フェールセーフ等を含む安全対策の徹底

314 ● 住宅メーカやシャッター製造販売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
315 方針

316 ➢ 住まい手のけが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取組
317 みの推進(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
318 を防ぐための取組みの推進)

319 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
320 によって、本ユースケース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した。

321

322

323

表 3 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	住まい手のけが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取組みの推進	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)における法令及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
		暗号化によるデータの保護
		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・システムの出荷時における安全な初期設定と構成
		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・システムの適正な運用・保守
		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・システムの運用・管理を行う者に対する要求事項の特定
	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
住宅メーカ及びシャッター製造販売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	住まい手のけが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取組みの推進(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取組みの推進)	運用前(設計・製造段階)における法令及び契約上の要求事項の遵守
		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

(3) リスク対応

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 4 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)
ワイヤレス通信機	データ改ざん	エッジシステム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。
	不正アクセス	外部からの悪意のある攻撃によって、ワイヤレス通信機がマルウェアに感染する。
エッジシステム	データ改ざん	クラウド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。
	不正アクセス	外部からの悪意のある攻撃によって、エッジシステムがマルウェアに感染する
	不正利用	エッジシステム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。
	引っ越し時の初期化の非実行	エッジシステムが前の住まい手(前の住まい手)によって不正に利用される
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、住宅メーカが想定する方法や内容でなされない。
クラウド	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等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。
	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。
	データ改ざん	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。

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以下の関連するステークホルダーにて実装が想定される対策要件を整理する。なお、住宅メーカ

は、インテグレータ、コンタクトセンタと協力を行い、セキュリティ対策を実装する。したがって、インテグレータ、コンタクトセンタで実施するセキュリティ対策は住宅メーカで実装するセキュリティ対策に含まれるものとする。

- 住宅メーカ
- シャッター製造販売事業者
- クラウドベンダ
- 住まい手

表 5 実装が想定される対策要件(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)における法令及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
		全般	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	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	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
		不正アクセス マルウェア感染	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
		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	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及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
		全般	IoT 機器・システムの安全な廃棄又は再利用
第 3 の観点	ソシキ・ヒト	全般	IoT 機器・システムの運用・管理を行う者に対する要求事項の特定
		全般	IoT 機器・システムの運用・管理を行う者に対する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

②で示した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。

上記(2)では、各ステークホルダー視点でスマートホームサービスの窓シャッターシステム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。

上記(2)で示したリスクアセスメントの結果を踏まえ、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。

- IoT 機器・システムにおけるセキュリティ機能の検証
- 運用前(設計・製造段階)における法令及び契約上の要求事項の遵守
- 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
- 暗号化によるデータの保護
- 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・システムの出荷時における安全な初期設定と構成

- 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・システムの適正な運用・保守
- 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・システムの運用・管理を行う者に対する要求事項の特定

上記を踏まえて、システムがもつリスクを受容可能なリスクの水準に収めることを目的として、住宅メーカ及びシャッター製造販売事業者が実装することとした対策要件の例を、それぞれ表 6 及び表 7 に示す。

なお、対策の抜け漏れが発生しないようシステム構成図を踏まえて、住宅内の機器における責任分界点を以下の通りとした。

- 住宅メーカはエッジシステムより上位の機器に責任を持つとした。ただし、ルータは住まい手が準備をするため対象には含めない。
- 窓シャッター販売製造事業者はエッジシステムより下位の機器に責任を持つとした。

また、住宅メーカ及びシャッター製造販売事業者では対応が難しい対策要件がいくつか見られた。かかる対策要件の実装はクラウドベンダや住まい手に依頼することとした。

- 住宅メーカにおける実際に講じる対策要件(例)

住宅メーカにおいて実際に講じることした対策要件(例)を整理する。

住宅メーカは冒頭でも述べた通り、CCDS が提供する IoT 機器を対象としたサーティフィケーション Lv.2(★★)を取得している。住宅メーカでは「添付 A 対策要件」[4]を参照し対策要件を整理した上で、各対策要件に対応する実際に講じる対策(例)として、認証取得時に準拠した「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」や「IoT 分野共通セキュリティ要件ガイドライン 2019 年版」(CCDS)にて示される合格要件を参照し整理を行った。なお、クラウドベンダへ対応を依頼すべき対策要件(例)についても住宅メーカよりクラウドベンダへ依頼を行うことから、住宅メーカと同様の手法で実際に講じる対策(例)を整理した。

[4] 経済産業省「IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集」

381

表 6 住宅メーカにおける実際に講じる対策要件(例)

No	第 3 軸	実装先	対策要件	実際に講じる対策(例)	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● サービスを対象とした・リスク分析・評価を行い、保護すべき資産と想定される脅威およびリスク値の評価を行う。 ● リスク分析・評価の過程で、個人情報などの重要なデータの取り扱いの有無、および生命・財産への影響の有無を検討して、サービスの認証レベルを定義する。 ● リスク分析・評価結果を踏まえて、必要なセキュリティ対策を策定する。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-1)>	○
2			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	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している。 ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● ISO/IEC27017:ISMS クラウドセキュリティ認証の取得あるいは、認証基準に準じた運用体制を保持する。 ● サービス提供において発生した想定外のリスクに対応するための CSIRT を組織し、インシデントの対応を行い、再発防止を行う。 ● 脆弱性の報告については、JPCERT/CC 等の組織と連携し、適切な対応を行う。	

				<CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4,R3-8)>	
3		システム	運用前(設計・製造段階)における法令及び契約上の要求事項の遵守	● スマートホームサービス利用時には、サービス契約を締結している利用者の認証を行い、転売時には利用者の認証情報の変更を行う。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-4)>	
4			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	● サービスを提供するシステム(サービス情報基盤、スマートホーム内の機器やスマートフォンアプリ)は、★★サービスの要求事項を満たした機器、システムによって構成する。 ● スマートホーム施工時には、宅内に設置される機器が、★★サービスの要求事項を満たした機種(品名・型番)であることを確認する。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-2)>	
5			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	● USB 接続端子(ポート)は、不用意な接続によるリスクの軽減策として、運用担当者以外が使用しにくい状態とするよう対策を行う。またサービス上、不要な USB 接続端子については、実装を行わない。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(SR2-H-5)>	
6			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	● USB 接続端子(ポート)は、不用意な接続によるリスクの軽減策として、運用担当者以外が使用しにくい状態とするよう対策を行う。またサービス上、不	

				要な USB 接続端子については、実装を行わない。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(SR2-H-5)>	
7			IoT 機器・システムにおけるセキュリティ機能の検証	● CCDS の認証マークを取得する。	
8			信頼できる IoT 機器やサービスの選定	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有する。 ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	
9			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	● システム運用上、必要な TCP/UDP ポートには、適切なアクセス制限や認証方法（機器毎にユニークな ID とパスワード、もしくは外部公開の恐れのない管理された ID とパスワード）で管理されていること ● Wi-Fi アライアンス推奨の最新の認証方式が装備されていること <CCDS「IoT 分野共通セキュリティ要件 ガイドライン 2019 年版」(共通要件 5,8)>	

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	● スマートホーム内の機器構成や設定については、利用者による変更を認めない範囲を明示し、該当する範囲については、利用者が無断で変更しないよう注意喚起を促す。 ● 利用者が想定外の用途で機器を使用しないよう、サービスの目的や提供機能について、周知する。 ● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有する 。 ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-6, R3-4)>	○
11	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	● スマートホーム内の機器構成や設定については、利用者による変更を認めない範囲を明示し、該当する範囲については、利用者が無断で変更しないよう注意喚起を促す。 ● 利用者が想定外の用途で機器を使用しないよう、サービスの目的や提供機能について、周知する。	

				<CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-4)>	
12			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	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること ISO/IEC27017:ISMS クラウドセキュリティ認証 サービス提供におけるインシデント対応 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4,R3-8)>	○
13		プロシージャ	インシデント対応手順の整備と実践	● サービス提供において発生した想定外のリスクに対応するための CSIRT を組織し、インシデントの対応を行い、再発防止対策を行う。 ● また、脆弱性の報告については、JPCERT/CC と連携し、適切な対応を行う。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-8)>	
14			事業継続計画の策定と実践	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュ	

				リティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	
15			IoT 機器・システムの適正な使用	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	
16			IoT 機器・システムの適正な運用・保守	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること ISO/IEC27017:ISMS クラウドセキュリティ認証	○

				<CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	
17		システム	運用中における法令及び契約上の要求事項の遵守	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している。 ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	
18			継続的な資産管理	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	
19			プログラムソースコード及び関連書類の保護	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している	

				● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	
20			IoT 機器・システムのモニタリング及びログの取得、分析	● サービスを提供するシステムは、インシデント対策として、ログ収集機能を有し、また収集したログデータの分析が可能な運用体制を有すること。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-5)>	○
21			IoT 機器・システムに対するアップデートの適用	● サービスを提供するシステム(サービス情報基盤、スマートホーム内の機器)は最新のソフトウェアへと定期的な更新を行うこと。 ● 上記において脆弱性が報告された場合には、速やかに更新用ソフトウェアの提供を行うこと ● サービス情報基盤やスマートホーム内の機器に対するソフトウェア更新の運用手順を明確化し、バージョン管理を行うこと。 1) 更新ソフトウェアをリリースする際の管理、運用手順 2) 更新ソフトウェアの更新内容と対応バージョンの履歴管理 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-7, R2-8)>	

22			IoT 機器・システムの安全な廃棄又は再利用	● 転売時には、スマートホーム内の構成機器に対して、下記の対応を行った上で、新しい利用者への引継ぎを行う。 1） 設定及び収集、蓄積した情報の初期化を行うこと。 2） 設置工事後、次の利用者がサービス運用を開始する際に、最新の状態へのソフトウェアアップデートを行うこと <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-9)>	
23	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[5]	● 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	○
24			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要求事項の確認 ● ソフトウェアアップデート時の注意事項の遵守の確認	

382 ● シャッター製造販売事業者にて実際に講じる対策要件(例)

383 シャッター製造販売事業者において実際に講じることした対策要件(例)を整理する。シャッター
384 製造販売事業者の目線ではスマートホームサービスの窓シャッターシステム全体のリスクを把握で
385 きているわけではない。したがって、システム構成図等を活用して認識を合わせた上で予め住宅メ
386 ーカとすり合わせを行い、実際に講じる対策要件(例)を整理した。

[5] 「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(CCDS)に対応する対策要件がなかったため、本適用実証内での検討結果を記載。

387 表 7 シャッター製造販売事業者における実際に講じる対策要件(例)

No	第 3 軸	実装先	対策要件	実際に講じる対策(例)	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	• 窓シャッターを含む自社が提供する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	• ワイヤレス通信機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	
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	• 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	○
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	• ワイヤレス通信機の企画・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	• 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	• ワイヤレス通信機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	• ワイヤレス通信機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	
10			様々な IoT 機器に接続する際のセキュリティの確保	• ワイヤレス通信機を他の IoT 機器等に接続する際のホワイトリストの適用	
11			暗号化によるデータの保護	• エッジシステム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	
13			IoT 機器・システムの十分な可用性の確保	• 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	
14			IoT に適したネットワークの利用	• (暗号化機能を有した Wi-Fi(例：WPA2-PSK(AES)等)に接続。)	
15			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 IoT 機器やエッジシステム、ワイヤレス通信機、ルータへの認可されていないアクセスを防ぐ目的で、施錠可能な住居内設置を原則とした物理的セキュリティ境界の確立。	
16			セキュリティ設計と両立するセーフティ設計の仕様化	• 窓シャッターへ安全機能の実装 • 窓シャッターに実装された安全機能と外部との通信回線との分離	○
17			セキュアな開発環境と開発手法の適用	• 設計書、プログラム、バイナリ等のバックアップ	

18			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)及びエッジシステム、ワイヤレス通信機に対するペネトレーションテストの実施	
19			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	• ワイヤレス通信機に接続する機器の不要なネットワークポート、その他 USB やシリアルポート等の物理的又は論理的な閉塞 • エッジシステム接続で明らかに不要な 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、アカウントの削除又は無効化	○
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	• 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、システムに対するリスクや住まい手で対応すべき点に関する情報提供の実施	
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 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)	

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。 • 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 • 脆弱性が明らかになった場合の、対応手順の整備。 • 脆弱性情報の収集及び評価の実施 • 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	• エッジシステムに適応したインシデント対応手順の整備 • 住宅メーカ、シャッター製造販売事業者とインテグレータ・コンタクトセンタの役割と責任の識別及び指定されたそれぞれによって実行されるアクションの定義・伝達	
25		システム	運用中における法令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	
26			継続的な資産管理	• エッジシステムに接続するワイヤレス通信機等に関する資産目録(機器上に実装されたソフトウェア及びファームウェア、工場出荷時の設定等を含む)の作成・維持	
27			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	

28			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 • 開発委託先等への修正プログラム等開発の依頼 • 住宅メーカを通じ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インテグレータへのセキュリティパッチの提供	
29			IoT 機器・システムの安全な廃棄又は再利用	• エッジシステムやワイヤレス通信機の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)。	
30	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	• 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住宅メーカ、インテグレータ・コンタクトセンタ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	
31			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住宅メーカ、インテグレータ・コンタクトセンタ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	

388 • クラウドベンダへ対応を依頼すべき対策要件(例)

389 クラウドベンダで対応が必要な対策について、住宅メーカはサービス提供時に対策を依頼するも
390 のとする。クラウドベンダは主に以下の対策要件を実施するものとする。

391 表 8 クラウドベンダへ対応を依頼すべき対策(例)

No	第 3 軸	実装先	対策要件	実際に講じる対策(例)	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	適切な水準のアクセス制御の実装	• サービス利用開始時に、IoT 機器間の認証情報あるいはアクセス制御が適切に初期設定されていることを確認する。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-3)>	
2			ソフトウェアの完全性の検証	• サービス情報基盤やスマートホーム内の機器に対するソフトウェア更新の運用手順を明確化し、バージョン管理を行うこと。 1) 更新ソフトウェアをリリースする際の管理、運用手順 2) 更新ソフトウェアの更新内容と対応バージョンの履歴管理 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-8)>	
3			ソフトウェアのインストールの制限	• サービス情報基盤やスマートホーム内の機器に対するソフトウェア更新の運用手順を明確化し、バージョン管理を行うこと。 1) 更新ソフトウェアをリリースする際の管理、運用手順 2) 更新ソフトウェアの更新内容と対応バージョンの履歴管理	

				<CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-8)>	
4			様々な IoT 機器に接続する際のセキュリティの確保	● システム運用上、必要な TCP/UDP ポートには、適切なアクセス制限や認証方法（機器毎にユニークな ID とパスワード、もしくは外部公開の恐れのない管理された ID とパスワード）で管理されていること。 <CCDS「IoT 分野共通セキュリティ要件 ガイドライン 2019 年版」(共通要件 8)>	○
5			暗号化によるデータの保護	● 認証に必要な情報が漏洩しないような仕組みを実装する。 ● スマートホームサービス情報基盤との通信や、ホームゲートウェイとの通信に対しては、通信経路の暗号化を行う。 ● 保護すべき資産に対する暗号化を行う。 ● 相互認証に必要な情報が漏洩しないような仕組みを実装すること。 ● USB 接続端子(ポート)は、不用意な接続によるリスクの軽減策として、運用担当者以外が使用しにくい状態とするよう対策を行うこと。またサービス上、不要な USB 接続端子については、実装を行わない。 ● 使用している OS、boot プログラム、アプリケーションに脆弱性が報告された場合には、テストを実施した上で、速やかに更新用ソフトウェアの提供を行う。 ● 接続機器との相互認証を行う仕組みを有すること。	

				<CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(SR2-SP-6, SR3-SP-9, 10, SR2-H-3,SR3-H-5, 6, SR2-D-3, SR2-D-5, SR3-D-2)>	
6			ライフサイクルを通じた暗号鍵の管理	● 通信経路暗号化やデータの暗号化に用いる鍵の管理を適切に行う。 ● 相互認証に必要な情報が漏洩しないような仕組みを実装する。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(SR3-SP-11, SR3-H-7, SR3-D-3)>	
7			IoT 機器・システムの十分な可用性の確保	● USB 接続端子(ポート)は不用意な接続によるリスクの低減策として、運用担当者以外が使用しにくい状態とするよう対策を行うこと。またサービス上、不要な USB 接続端子については、実装を行わないこと。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(SR3-D-4)>	
8			適切なネットワークの分離	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること ISO/IEC27017:ISMS クラウドセキュリティ認証	

				<CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	
9			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	● LAN 内接続機器との通信は、通信経路の暗号化を行う。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(SR2-H-5)>	
10			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	● LAN 内接続機器との通信は、通信経路の暗号化を行う。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(SR2-H-5)>	
11			セキュアな開発環境と開発手法の適用	● API における認証を実装し、認証情報の無効化と再発行が可能な認証方式を有すること。 ● API における認証については、報告されている脆弱性への対策を行うこと。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(SR2-SP-2)>	
12			IoT 機器・システムにおけるセキュリティ機能の検証	● CCDS のマークを取得する。	
13			信頼できる IoT 機器やサービスの選定	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。	

				ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	
14	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	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること ISO/IEC27017:ISMS クラウドセキュリティ認証 ● サービス提供におけるインシデント対応 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4, R3-8)>	○
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	● サービス提供において発生した想定外のリスクに対応するための CSIRT を組織し、インシデントの対応を行い、再発防止対策を行う。 ● また、脆弱性の報告については、JPCERT/CC と連携し、適切な対応を行う。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-8)>	
16			インシデント対応手順の整備と実践	● サービス提供において発生した想定外のリスクに対応するための CSIRT を組織し、インシデントの対応を行い、再発防止対策を行う。	

				● また、脆弱性の報告については、JPCERT/CC と連携し、適切な対応を行う。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-8)>	
17			事業継続計画の策定と実践	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している。 ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-8)>	
18			IoT 機器・システムの適正な使用	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している。 ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	

19			IoT 機器・システムの適正な運用・保守	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している。 ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	○
20		システム	運用中における法令及び契約上の要求事項の遵守	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している。 ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	
21			継続的な資産管理	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している。 ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セ	

				キュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	
22			プログラムソースコード及び関連書類の保護	● サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有している。 ● 第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行う。 ● 下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 ISO/IEC27017:ISMS クラウドセキュリティ認証 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-4)>	
23			IoT 機器・システムのモニタリング及びログの取得、分析	● サービスを提供するシステムは、インシデント対策として、ログ収集機能を有し、また収集したログデータの分析が可能な運用体制を有すること。 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R3-5)>	○
24			IoT 機器・システムに対するアップデートの適用	● サービスを提供するシステム(サービス情報基盤、スマートホーム内の機器)は最新のソフトウェアへと定期的な更新を行うこと。	

				● 上記において脆弱性が報告された場合には、速やかに更新用ソフトウェアの提供を行うこと。 ● サービス情報基盤やスマートホーム内の機器に対するソフトウェア更新の運用手順を明確化し、バージョン管理を行うこと。 1） 更新ソフトウェアをリリースする際の管理、運用手順 2） 更新ソフトウェアの更新内容と対応バージョンの履歴管理 <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-7,R2-8)>	
25			IoT 機器・システムの安全な廃棄又は再利用	● 転売時には、スマートホーム内の構成機器に対して、下記の対応を行った上で、新しい利用者への引継ぎを行う。 1） 設定及び収集、蓄積した情報の初期化を行うこと。 ● 設置工事後、次の利用者がサービス運用を開始する際に、最新の状態へのソフトウェアアップデートを行うこと <CCDS「製品分野別セキュリティガイドラインスマートホーム編_Ver.1.0」(R2-9)>	

392

393 • 住まい手へ対応を依頼すべき対策要件(例)

394 住まい手で対応が必要な対策について、住宅メーカはサービス提供時に対策を依頼するものと
395 する。住まい手は主に以下の対策要件を実装するものとする。

396 表 9 住まい手へ対応を依頼すべき対策(例)

No	第 3 軸	実装先	対策要件	実際に講じる対策(例)	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	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等のポリシーやセキュリティ対策に留意した上で、適切な窓シャッター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	運用中における法令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	
3		プロシージャ	IoT 機器・システムの安全な廃棄又は再利用	• エッジシステムやワイヤレス通信機の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)	

397 **2-2 家庭用エアコンの遠隔操作**

398 本ユースケースは、エアコン製造事業者が住まい手向けに提供しているエアコンを対象に IoT-
399 SSF に基づくリスクアセスメント及びリスク対応を行った結果をまとめたものである。

400 エアコン製造事業者が提供するエアコンは、住まい手のスマートフォンにインストールされた専用
401 のアプリケーションを利用し操作するものを想定する。エアコン専用のアプリケーションを通じて、住ま
402 い手は ON・OFF 操作や冷房、暖房、送風、除湿等の運転モードの切り替え、温度設定の変更
403 等を行うことができる。また、エアコン製造事業者はエアコンの稼働データや異常コードを収集する
404 ことで業務に活用している。

405 住まい手は家電量販店でエアコンを購入することとする。また、回線契約やインターネットサービ
406 スプロバイダ契約、ルータ購入等のインターネット環境も住まい手が準備するものとする。

407 エアコン製造事業者は、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
408 に対してはステークホルダーに対して対応を依頼することで、可能な限り、リスクを低減する。

(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、スマートフォンアプリを通じてエアコンの遠隔操作を行うエアコンシステムを対象とする。本ユースケースでは以下の 2 パターンの利用シーンを想定するものとする。

- 外出先から帰宅する際、住まい手がリビングのエアコンを遠隔操作し、部屋を冷やす。(温める)
- 就寝前に住まい手がリビングから寝室のエアコンを遠隔操作し、部屋を冷やす。(温める)

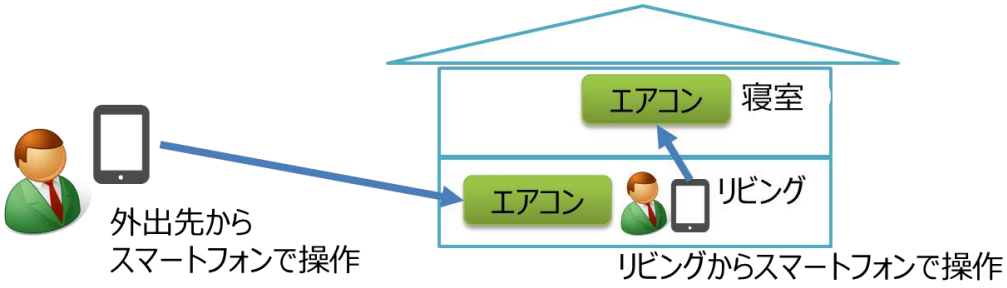


図 8 対象ソリューションのイメージ

② ステークホルダー関連図

本ユースケースにて示す取組に関与するステークホルダーは、以下に示すように「エアコン製造事業者」や「家電量販店」、「住まい手」を想定している。契約関係や製品・サービスの提供関係を考慮したステークホルダー関連図は、以下に示す通りである。

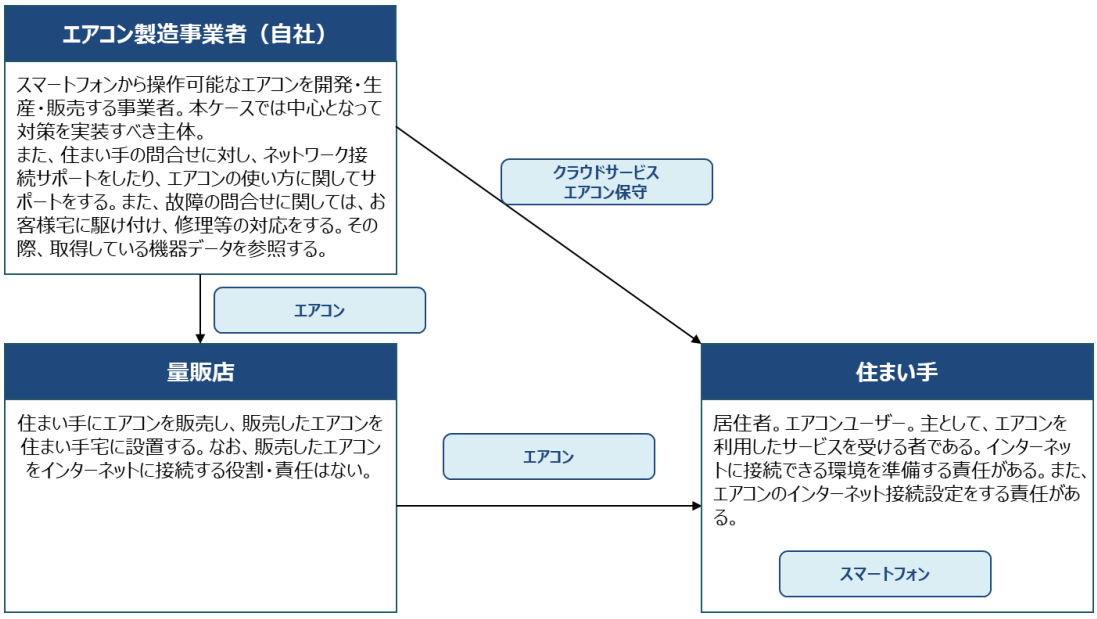


図 9 ステークホルダー関連図

＜IoT サービス開発者/IoT サービス提供者＞

● エアコン製造事業者

スマートフォンから操作可能なエアコンを開発・生産・販売する事業者。本ユースケースでは中心となって対策を実装すべき主体とする。また、住まい手の問合せに対し、ネットワーク接続のサポートや使用方法に関するサポートを行う。また、故障の問合せに関しては、住まい手宅に駆け付け、修理等の対応を行う。その際、取得している機器データを参照する。

＜IoT サービス利用者＞

● 住まい手

エアコンのユーザ。主として、エアコンを利用したサービスを受ける者である。インターネットに接続可能な環境を準備する責任を有する。また、エアコンのインターネット接続設定を行う責任も有する。

＜その他＞

● 家電量販店

住まい手にエアコンを販売し、販売したエアコンを住まい手宅に設置する。なお、販売したエアコンをインターネットに接続する役割・責任は有さない。

③ システムを構成する機器の一覧

本ユースケースの対象となる機器は以下の通りとする。

表 10 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
エアコン	クラウドサービス経由でスマートフォンから指示を受けて、部屋の空調を行うことが可能となる機器。 エアコンは、部屋を空調する室内に設置された室内機と、屋外の空気と熱交換する為に屋外に設置された室外機から構成される。 調整可能な温度は上限・下限の制限がある。 スマートフォンからの指示は、室内機内部の無線 LAN アダプタにて受け付ける。 エアコンの構成要素としては、例えば、以下があげられる。 ・センサ：室温センサ、室内熱交センサ、外気温度センサ、室外熱交センサ、吐出管温度センサ ・アクチュエータ：室内ファン、室外ファン、電動弁、圧縮機等 ・部品：室内熱交換器、室外熱交換器
無線 LAN ルータ	居宅内に設置され、居宅内のネットワーク及び居宅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、外出先やリビングからスマートフォン上のアプリケーションを操作してエアコンの遠隔操作を行う。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	エアコンから運転データやセンサデータを取得し、スマートフォンに渡す。また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エアコンに指示を出す。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

本ユースケースで対象とするシステムは、住まい手が所有するスマートフォンやクラウドサービス、無線 LAN ルータ、エアコンから構成される。システム構成図は以下の通りとする。

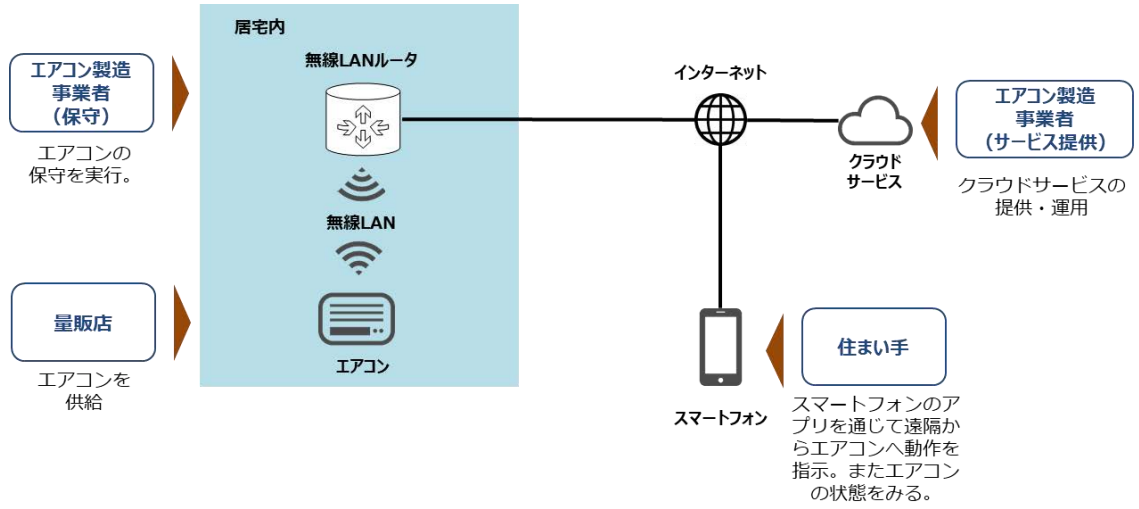


図 10 システム構成図

スマートフォンアプリからエアコンを操作する場合のデータフローは以下の通りとする。

1. 外出先より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。[6]
2. クラウドサービスからインターネットを通じて、無線 LAN ルータ経由でエアコンに指示を出す。

[6] スマートフォンの操作は、外出先からではなく居宅内から行うことも想定される。

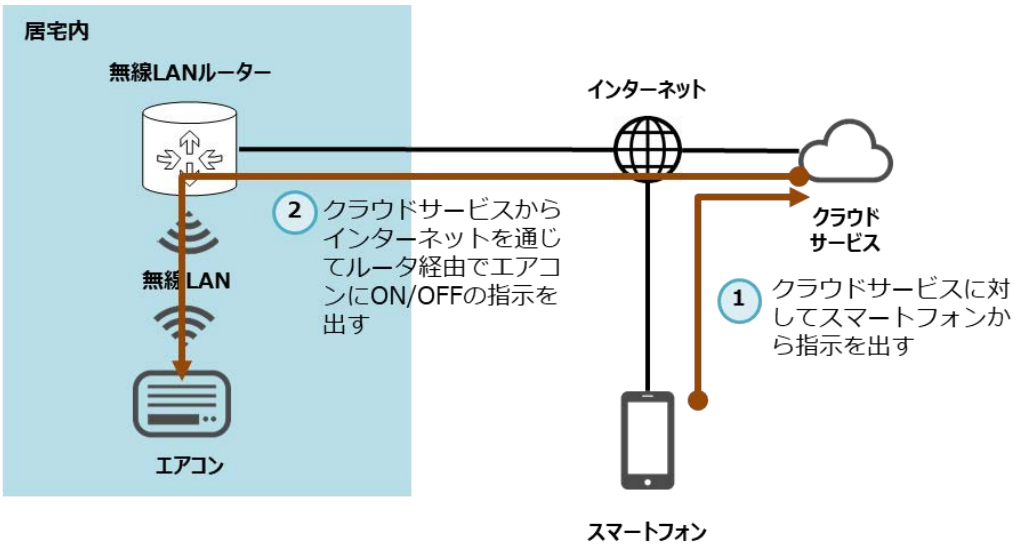


図 11 データフロー図

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」は、自社が定めるセキュリティや品質等に関する設計基準にのっとり、お客様に重大な事故が発生しないよう、被害を「限定的なダメージ」に抑えることを目指す。「経済的な影響の度合い」は、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。

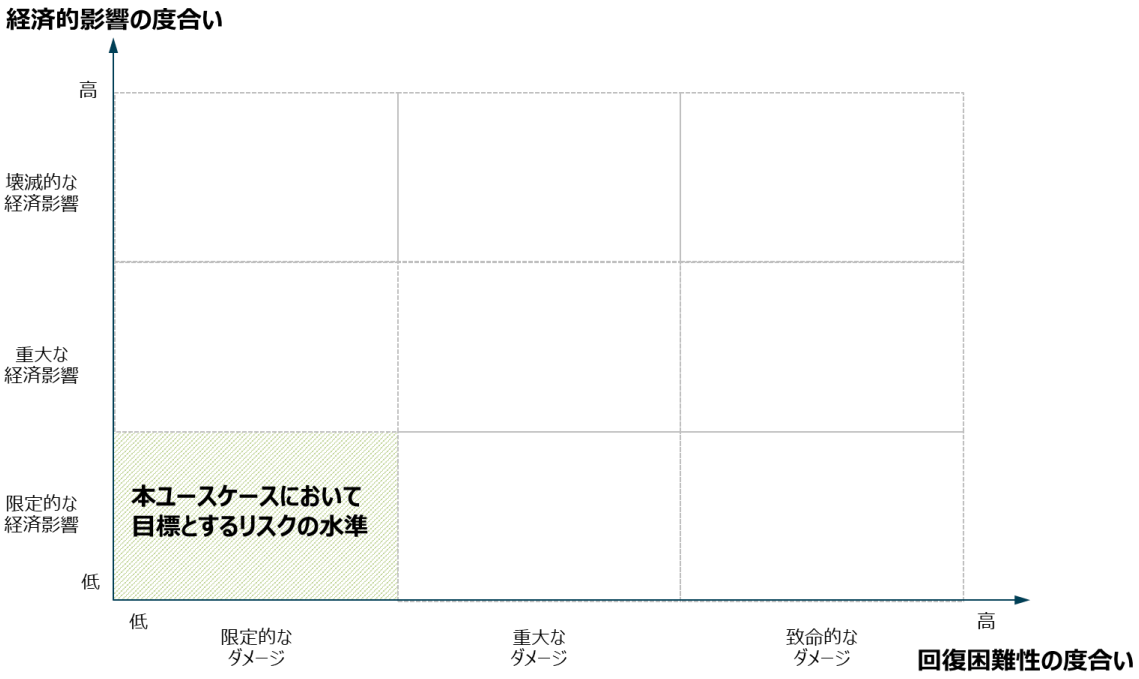


図 12 目標とするリスクの水準

(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、エアコン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

エアコンシステムにおいて、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。エアコンシステムの提供又は利用に際して想定されるステークホルダーごとのセキュリティインシデント(例)は以下の通りである。後述の「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」におけるリスクの値に直結する結果は下線太字にて記載する。なお、エアコン製造事業者内での役割や生じ得る被害が異なることから、エアコンの販売・保守を行う部門と IoT サービスを提供する IoT 事業・運用を行う部門を分けて記載するものとする。また、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)はないと考えられるため、家電量販店は除外するものとする。

- エアコン製造事業者(販売・保守部門)
- エアコン製造事業者(IoT 事業・運用部門)
- 住まい手

- エアコン製造事業者(販売・保守部門)
  - 悪意のある攻撃者によって、サーバ上のエアコンの稼働データが改ざんされ、あたかも顧客の機器が故障したかのように見える。その結果、サービスの保守を行う作業員による無駄な訪問が生じてしまい、**本来修理が必要な顧客に対してサービスの提供ができなくなり得る。**

- エアコン製造事業者(IoT 事業・運用部門)
  - 悪意のある攻撃者によってサーバへ不正アクセスされることにより、サーバに保存されている住まい手の個人情報が漏えいする。その結果、**ブランドイメージの低下**が起こり得る。また、住まい手の間で**保守サポートの品質について不安が広がり**得る。
  - また、悪意のある攻撃者によってサーバの管理者権限が奪われることによって、**エアコンシステムに係るサービスが停止し得る。**

- 住まい手
  - 悪意のある攻撃者によってアカウントが乗っ取られ、ユーザの意図しないコマンドがサーバに対して直接実行されることで、エアコンが予期せぬ動作をする。その結果、例えば**夏季の就寝中に部屋が暖められ、住まい手が熱失神、熱疲労に至る。**

- 悪意のある攻撃者によってサーバが不正アクセスされ、ユーザの意図しないコマンドが流れることで、エアコンが予期せぬ動作をする。その結果、例えば**冬季に部屋が冷やされることで住まい手が不快に感じ得る**。
- 悪意のある攻撃者によるクラウドサービスへの DDoS 攻撃によって、住まい手に対してサービスを提供できなくなる。また、DNS リバインディングにより、悪意のあるサーバに誘導される。その結果、**住まい手はスマートフォンからエアコンを遠隔操作できなくなり、不快な空間になり得る。**
- 悪意のある攻撃者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。その結果、住まい手はスマートフォンからエアコンを遠隔操作できなくなり、**不快な空間に**なり得る。
- クラウドサービス内の構成要素のソフトウェアが改ざんされる。その結果、住まい手はスマートフォンからエアコンを遠隔操作できなくなり、**不快な空間に**なり得る。
- 悪意のある攻撃者によってクラウドサービスのサーバが乗っ取られ、他サービスに攻撃を仕掛けられ得る。

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。

- エアコン製造事業者(販売・保守部門)
- エアコン製造事業者(IoT 事業・運用部門)
- 住まい手

- エアコン製造事業者(販売・保守部門)

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、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、エアコンが予期せぬ動作をしたとしても、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

サーバ上のエアコンの稼働データが改ざんされ、あたかも顧客の機器が故障したかのようにエアコン製造事業者(販売・保守部門)から見える場合には、現場の住まい手宅へ駆け付ける。ただし、エアコンが正常に動作している場合に無駄な費用となる可能性がある。

ただし、現場への駆け付け対応費用が大規模な製品回収費用と比較して小さくなることが想定されることから、「経済的影響の度合い」は「限定的な経済影響」と評価する。

- エアコン製造事業者(IoT 事業・運用部門)

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、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、エアコンが予期せぬ動作をしたとしても、従業員がけがを負う可能性は低いと想定される。一方で、ブランド価値の低下にはつながり得る。

プライバシーの観点では個人情報が流出する可能性が少なく、セーフティの観点で従業員がけがを負う可能性が少ないものの、ブランド価値の低下につながり得ることから、「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

経済影響の観点では、住まい手の個人情報の流出によって住まい手に対する賠償費用が生じ得るが、ここではその影響は限定的なものと想定した。したがって、「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

プライバシーの観点では、サーバ上の不正アクセスによって住まい手の個人情報等が流出し得る。

セーフティの観点では、悪意のある攻撃者によってアカウントの乗っ取りやサーバへの不正アクセスが生じることによって、意図しないコマンドが流れエアコンが予期せぬ動作をし得る。その結果、リビングや寝室が不快な環境になり、場合によってはお年寄りや子供等に健康被害(例:熱失神、熱疲労[7])が生じ得る。

[7] 被害の程度は、中央労働災害防止協会「製造業向け熱中症予防対策のためのリスクアセスメントマニュアル」を参考とした。(https://www.jisha.or.jp/research/pdf/201503_02_All_1.pdf)

548　プライバシーの観点では個人情報が流出し得ること、セーフティの観点では住まい手に健康被
549害が及び得ることから、「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。

550　B)　発生したインシデントの経済的影響の度合い
551　「回復困難性の度合い」と同様、エアコンが予期せぬ動作をして住まい手に健康被害が生じた
552場合、住まい手は診療を受ける必要が生じ生活に支障をきたし得る。また、場合によってはその
553影響が一定期間続く可能性がある。
554　したがって、インシデントによって一定期間住まい手の生活に支障をきたし得ることから、「経済
555的影響の度合い」のレベルは「重大な経済影響」と評価する。

556　③　マッピング結果の整理と評価の実施
557　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
558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
559度合い」からカテゴライズし、マッピングする。

560

561　図 13　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
562　リスク(例)のマッピング結果

563　「目標とするリスクの水準」の外側にある 2 つを「経済(的)影響の度合い」と「回復困難性の度
564合い」を軽減する観点から中心的に対策する。影響度が大きいリスクに対処するための対策方針
565を以下の通り整理した。

566　● エアコ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

567 ➢ エアコンの制御データの改ざんやサービスの停止等を防ぐことを目的としたセキュアな環
568 境の構築
569 ➢ 安全にエアコンを運用・管理するための仕組みの構築
570 ● 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
571 ➢ 安全にエアコンを運用・管理するための仕組みの構築

572 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
573 によって、本ユースケース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
574 ができる。

575 表 11 影響度が大きいリスクに対処するための対策方針及び
576 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
エアコン製造事業者	エアコンの制御データの改ざんやサービスの停止等を防ぐことを目的としたセキュアな環境の構築	セキュアな開発環境と開発手法の適用
	安全にエアコンを運用・管理するための仕組みの構築	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
住まい手	安全にエアコンを運用・管理するための仕組みの構築	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

577 (3) リスク対応
578 ① システムを構成する機器ごとの脅威の整理
579 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。本ユースケースで
580 は、サービスの提供に特に重要となるクラウドサービスを対象にして、脅威を洗い出した。

581 表 12 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)	被害を受けるステークホルダー
クラウドサービス	なりすまし	DNS リバインディングにより、悪意のあるサーバに誘導される。(なりすまされる)	住まい手
	データ改ざん	サーバ上の機器データや・機器への指示データが改ざんされる。	住まい手、エアコン製造事業者(販売・保守)
	情報漏えい	サーバ上の個人情報が漏えいする。	住まい手、エアコン製造事業者(販売・保守)

	サービス不能	DDoS 攻撃を受け、サービスを提供できなくなる。	エアコン製造事業者 (IoT 運用)、住まい手
	権限昇格	サーバシステムの管理者権限が奪われる。	エアコン製造事業者 (IoT 運用)、住まい手
	不正アクセス	クラウドサービスが認証・認可されていない悪意のある主体に、不正にアクセスされる。	エアコン製造事業者 (IoT 運用)、住まい手
	マルウェア感染	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。	エアコン製造事業者 (IoT 運用)、住まい手
	踏み台	サーバが乗っ取られ、他サービスに攻撃を仕掛ける。	国、国民等 エアコン製造事業者 (IoT 運用)
	不正改造	クラウドサービス内の構成要素のソフトウェアが改ざんされる。	エアコン製造事業者 (IoT 運用)、 住まい手

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エアコン製造事業者や家電量販店、住まい手にて実装が想定される対策要件を整理する。なお、想定される脅威ごとに対策要件(例)を整理した結果は以下の通りである。

表 13 実装が想定される対策要件(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	なりすまし、データの改ざん、情報漏えい、サービス不能、権限昇格、不正アクセス、マルウェア感染、踏み台、不正改造	IoT 機器・システムにおけるセキュリティポリシーの策定
	システム	データの改ざん、情報漏えい、権限昇格、不正アクセス、マルウェア感染、踏み台、不正改造	セキュアな開発環境と開発手法の適用
第 2 の観点	ソシキ・ヒト	不正アクセス	利用者へのリスクの周知等の情報発信
	プロシージャ	なりすまし、データの改ざん、情報漏えい、サービス不能、権限昇格、不正アクセス、マルウェア感染、踏み台、不正改造	脆弱性対応に必要な手順等の整備と実践
	システム	不正改造	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	権限昇格、不正アクセス	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

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。

- 適用する対策の内容(どのように対策を実施するか)

エアコン製造事業者及び住まい手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を実施する。

本ユースケースでは、エアコン事業者側でよりセキュアな環境を構築することとした。また、能動的な行動を促すことを目的として住まい手に対する要求事項を明確化した上、エアコン製造事業者はかかる要求事項を提示することによってリスクへ対処することとした。したがって、特に以下の対策は影響度が大きいリスクに対処するための対策要件に設定した。

- セキュアな開発環境と開発手法の適用
- IoT 機器・システムの運用・管理を行う者に対する要求事項の特定

上記を踏まえて、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、エアコン製造事業者が実施することとした対策の例を以下に示す。本ユースケースでは、ブランドイメージ低下への懸念から本来セキュリティに係る責任が少ない家電量販店に対して対策の実施を依頼した。また、機器・システムを運用・管理する住まい手に対しても対策の実施を依頼した。

第 1 の観点では、エアコンシステムの企画設計段階で住まい手及びエアコン製造事業者(IoT 事業・運用)で想定されるリスクを抑えることを目的として、実施することとした対策の例を整理した。

第 2 の観点では、エアコンシステムの運用中で住まい手及びエアコン製造事業者(IoT 事業・運用)で想定されるリスクを抑えることを目的として、実施することとした対策の例を整理した。

第 3 の観点では、エアコン製造事業者が住まい手及びエアコン製造事業者(IoT 事業・運用)で想定されるリスクを抑えることを目的として、IoT 機器・システムの運用・管理を行う者に対する要求を整理した。

表 14 エアコン製造事業者における実際に講じる対策要件(例)

No	第 3 軸	実装先	対策要件	実際に講じる対策(例)	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	• エアコンシステムを含む自社が提供する IoT 機器・システムは、自社で定めた各種	

				セキュリティ設計基準・規定に準じて設計・開発する。 ● 定められた期間ごとの各種セキュリティ設計基レビュー	
2		システム	セキュアな開発環境と開発手法の適用	● 開発環境やソースコードへのアクセスを制御する。 ● 使用している OSS や関連 OS および利用コンポーネントの脆弱性に関して管理を実施する。 ● 秘密鍵等、秘密にすべき情報は厳重に管理する。全社的に情報管理のルールを統一して実施する。	○
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	● 脆弱性情報の提供する情報窓口組織の構築。 ● 情報窓口組織は顧客である住まい手に対して脆弱性情報を適切に提供し、システムにおける適切な対処(バージョンアップ、軽減策の実施)を促す。 ✓ 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による通知 ✓ システムの脆弱性、ユーザ情報の漏えい、サポート期間終了の予告 ✓ 住まい手における対処方法(バージョンアップ、軽減策の方法)の通知 ● 情報窓口組織は、住まい手以外にも必要に応じて家電量販店などのサプライチェーンに対して脆弱性情報を提供する。 ● 情報窓口組織は、必要に応じて行政機関に対して脆弱性情報を報告する。	

4		プロシージャ	脆弱性対応に必要な手順等の整備と実践	• システムを構築するサーバや機器が内包する外部から調達した OSS などのようなソフトウェア・ライブラリについて、管理する仕組みを構築する。 • 上記のソフトウェア・ライブラリに関する脆弱性の情報をセキュリティベンダやセキュリティ関連機関(NVD,JPCERT)などからクラウドサービス等を使用して収集する。 • 対象の脆弱性情報がシステムに影響を及ぼすのか、また、影響の度合い、問題が発生する条件等について検討をおこない、修正要否を判断する。 • セキュリティパッチ等の適用を行い、システムへの影響について回帰テストによる検証を行いシステムのバージョンアップ・公開を行う。 • 脆弱性情報の情報窓口より、顧客に対して脆弱性情報を適切に提供し、システムにおける適切な対処(バージョンアップ、軽減策の実施)を促す。	
5		システム	IoT 機器・システムに対するアップデートの適用	• 顧客と双方向に脆弱性情報の授受する情報窓口組織の構築。 • 確認が取れたシステムのソフトウェアを公開し、システムのバージョンアップ・公開を行う。 • 脆弱性情報の情報窓口より、顧客に対して脆弱性情報を適切に提供し、顧客が所有するスマートフォン上のアプリケーション、エアコンの	

				通信機器に対して適切な対処(バージョンアップ、軽減策の実施)を促す。	
6	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	• 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要求事項を、取扱説明書や Web サイトで掲示する。 ✓ 無線 LAN のセキュリティリスクについて ✓ 無線 LAN のセキュリティ設定について ✓ 無線 LAN の SSID、KEY の管理について ✓ 無線 LAN の暗号方式について ✓ 遠隔から操作する際の安全上のリスクについて ✓ 遠隔から操作をする前、操作中に確認すべき内容について	○

612 • 家電量販店に対応を依頼すべき対策要件(例)

613 表 15 家電量販店に対応を依頼すべき対策(例)

No	第 3 軸	実装先	対策要件	実際に講じる対策(例)	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	利用者へのリスクの周知等の情報発信	• エアコン製造事業者より提供された脆弱性情報を確認した上で、適切な対処を行う。	

614 • 住まい手に対応を依頼すべき対策要件(例)

615 表 16 住まい手に対応を依頼すべき対策(例)

No	第 3 軸	実装先	対策要件	実際に講じる対策(例)	影響度が大きいリスクに対処するための対策要件
1	第 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	• 脆弱性情報の情報窓口より提供された脆弱性情報を踏まえて、所有するスマートフォン上のアプリケーション、	

				エアコンの通信機器に対して適切な対処(バージョンアップ、軽減策の実施)を行う。	
2	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	• 取扱説明書や Web サイトより以下の事項に関する要求事項を確認した上で、適切な対処を行う。 ✓ 無線 LAN のセキュリティリスクについて ✓ 無線 LAN のセキュリティ設定について ✓ 無線 LAN の SSID、KEY の管理について ✓ 無線 LAN の暗号方式について ✓ 遠隔から操作する際の安全上のリスクについて ✓ 遠隔から操作をする前、操作中に確認すべき内容について	○

2-3 ボイラーの遠隔監視

本ユースケースは、架空のアセットオーナ(以下、「事業者 X 」という。)における自社プラント(以下、「プラント」という。)のボイラーを対象に、IoT-SSF に基づくリスクアセスメント及びリスク対応を行った結果をまとめたものである。

既にボイラーを稼働させている事業者 X のプラントにおいてボイラーの制御装置等を交換した上で、かかる機器の遠隔監視を行う想定で新たに生じ得るリスクやそのリスクへの対応策について検討するものとする。遠隔監視の対象となるボイラーは、厚生労働省通達「ボイラーの遠隔制御基準等について」の別添 3「認定適合自動制御装置を備えたボイラーの点検及び運転に関する基準」[8]にて定められる認定適合自動制御装置を活用し、事業場外で常時監視を行うことを想定する。

本ユースケースでは、遠隔監視を行うことで新たに生じ得るリスクやそのリスクへの対応策に焦点を当てることとし、制御システムにおいて一般的に想定され得るリスクやその対応策のうち、ボイラー

[8] 厚生労働省通達「認定適合自動制御装置を備えたボイラーの点検及び運転に関する基準」(https://www.jaish.gr.jp/horei/hor1-44/hor1-44-6-1-4.html)

の遠隔操作とは必ずしもかかわりがないものについては取り扱わない可能性がある点にご留意されたい。

なお、本ユースケースの作成にあたり、日本電気制御機器工業会の支援とオブザーバとして参加された日本ボイラ協会より助言を得た。

(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

事業者Xは自社プラントにおいて石油化学製品を製造している事業者である。自社プラントの調達工程、製造工程、検査工程のうち、製造工程においてボイラーを用いて石油化学製品を製造する。

ボイラーは事業者 X の運用監視部門の従業員が監視することとする。事業者 X の従業員は遠隔監視の仕組みを導入することによって、ボイラーに 1 時間以内で駆け付けることのできるリモートオフィスよりボイラーの監視を行うことが可能となった。事業者 X の従業員はボイラーからコントローラを通じて送信される稼働情報(温度情報、圧力情報、流量情報等)を通じて、タブレットやスマートフォンにてボイラーの監視を行う。ただし、遠隔制御は実施できないものとする。[9]

なお、ボイラーの製造に関してはボイラーメーカが申請を行い都道府県労働局から許可を受ける必要がある。設置に関しては事業者 X が労働基準監督署に届け出る必要がある。また、ボイラーは「登録性能検査機関」による検査(1 回/年)や「登録適合性証明機関」による審査を受けているものとする。

- 事業者Xのプラントでは、既存のボイラーの制御装置等を交換した上で、かかる機器の遠隔監視を行う。
- 遠隔監視は、プラントの運用監視部門の従業員が行う。ただし、かかる従業員は遠隔監視を実施する一方で、遠隔制御は実施できないものとする。
- 遠隔監視の対象となるボイラーは、厚生労働省通達「ボイラーの遠隔制御基準等について」の別添3「認定適合自動制御装置を備えたボイラーの点検及び運転に関する基準」にて定められる認定適合自動制御装置を活用し、事業場外で常時監視を行うものとする。
- ボイラーは「登録性能検査機関」による審査(1回/年)や「登録適合性証明機関」による審査を受けているものとする。

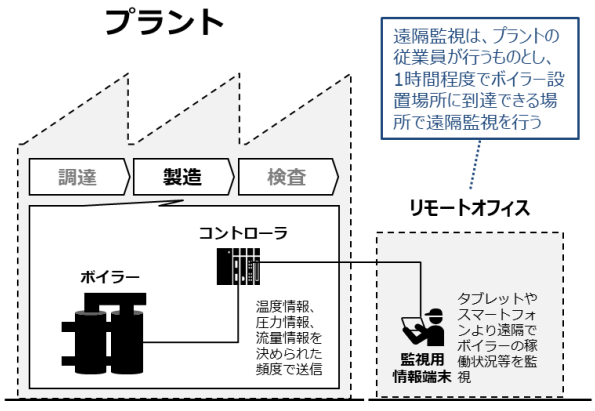


図 14 対象ソリューションのイメージ

[9] 悪意のある攻撃者が外部よりコントローラ(制御装置)にアクセスし、プログラムまたはパラメータ(空燃比制御等)を変更することは起こり得るとしている。

② ステークホルダー関連図

本ユースケースにて示す取組に関与するステークホルダー[10]は、以下に示す「事業者 X」や「ボイラーメーカ(アセットメーカ兼サービスプロバイダ)」(以下、「ボイラーメーカ」という。)、「ボイラー制御機器メーカ」、「ボイラー据付事業者」、「ボイラー整備事業者」を想定している。契約関係や製品・サービスの提供関係を考慮したステークホルダー関連図は、図 15 に示す通りである。

なお、ステークホルダーには含まれないものの「都道府県労働局」、「労働基準監督署」、「登録適合性証明機関」、「登録性能検査機関」の役割も整理した。

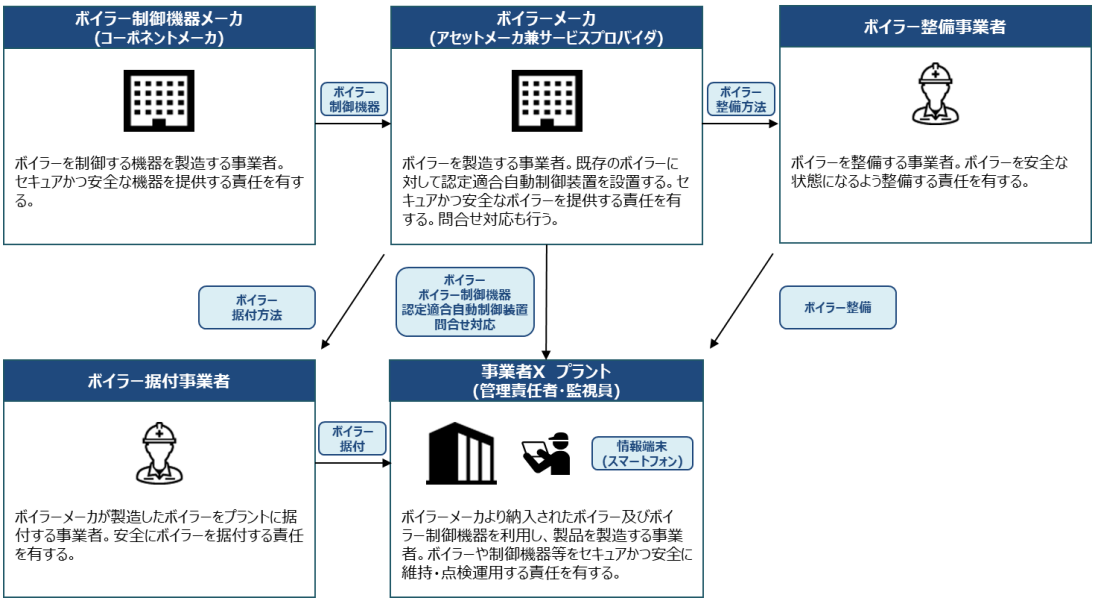


図 15 ステークホルダー関連図

＜IoT サービス利用者＞

- 事業者 X

ボイラーメーカより納入されたボイラー及びボイラー制御機器を利用し、製品を製造する事業者。ボイラーやボイラー制御機器等をセキュアかつ安全に維持・点検・運用する責任を有する。

＜IoT サービス開発者/IoT サービス提供者＞

- ボイラーメーカ

ボイラーを製造する事業者。既存のボイラーに対して認定適合自動制御装置を設置する。セキュアかつ安全なボイラーを提供する責任を有する。問合せ対応も行う。

[10] ボイラーの「発注」から「据付」「使用」「点検」「整備」段階で関連するステークホルダーを示す。

● ボイラー制御機器メーカ

ボイラーを制御する機器を製造する事業者。セキュアかつ安全な機器を提供する責任を有する。

● ボイラー据付事業者

ボイラーメーカが製造したボイラーをプラントに据付する事業者。安全にボイラーを据付する責任を有する。

● ボイラー整備事業者

ボイラーを整備する事業者。ボイラーを安全な状態になるよう整備する責任を有する。

＜関連行政当局/機関＞

● 都道府県労働局

ボイラーメーカの申請に対して、ボイラーの製造許可を行う。

● 労働基準監督署

事業者 X の申請に対して、ボイラーの設置許可を行う。

● 登録適合性証明機関

ボイラー及びボイラー制御機器が審査事業者の定める基準を満たしているかを審査する機関。なお、安全審査に加えてセキュリティに関する審査も実施する。

● 登録性能検査機関

ボイラーに対して年 1 回の性能検査を行う機関。

③ システムを構成する機器の一覧

本ユースケースの対象となる機器は以下の通りとする。

表 17 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
SCADA サーバ/端末	ボイラー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。 また、ボイラーより決められた間隔で温度情報や圧力情報、流量(燃料/空気)情報等を収集する。 SCADA とは、Supervisory Control And Data Acquisition の略称。
認定適合自動制御装置	ボイラーの運転の状態に係る異常があった場合に当該ボイラーを安全に停止させることができる機能その他の機能を有する自動制御装置であって、機能安全による機械等に係

	る安全確保に関する技術上の指針(平成 28 年厚生労働省告示第 353 号)に適合していると所轄労働基準監督署長が認定したもの。
コントローラ(制御装置)	プログラムで定められた順序や条件に従い、ボイラーの圧力、水位、燃焼量等を制御する装置。 作業場所近くに設置された制御盤に格納されており、作業員が操作できるように操作画面を備えている。
ボイラー	水管ボイラーを想定。ボイラー本体、バーナ、火災検出器、蒸気圧力調節器、圧力計、蒸気ドラム、蒸気弁、水位検出器、安全弁、水面計、水ドラム、ファン等を有している。各種安全装置を含む。
リモートアクセスサーバ[11]	クラウドサービスプロバイダ内に設置され、コントローラより送られてくる温度情報や圧力情報、流量(燃料/空気)情報等を収集するサーバ。
情報端末(PC/スマートフォン/タブレット等)	リモートアクセスサーバより送信されるボイラーの稼働情報を確認できる端末。 ここでは、PC やスマートフォン、タブレットを想定している。
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。

④　システム構成図、データフロー図

本ユースケースで対象とするシステムは、ボイラー(各種安全装置等を含む)や認定適合自動制御装置、コントローラ(制御装置)、SCADA サーバ/端末、エンジアリング端末(エンジニアリングツール)、リモートアクセスサーバ、情報端末(タブレット/スマートフォン)から構成される。[12]システム構成図は以下の通りとする。

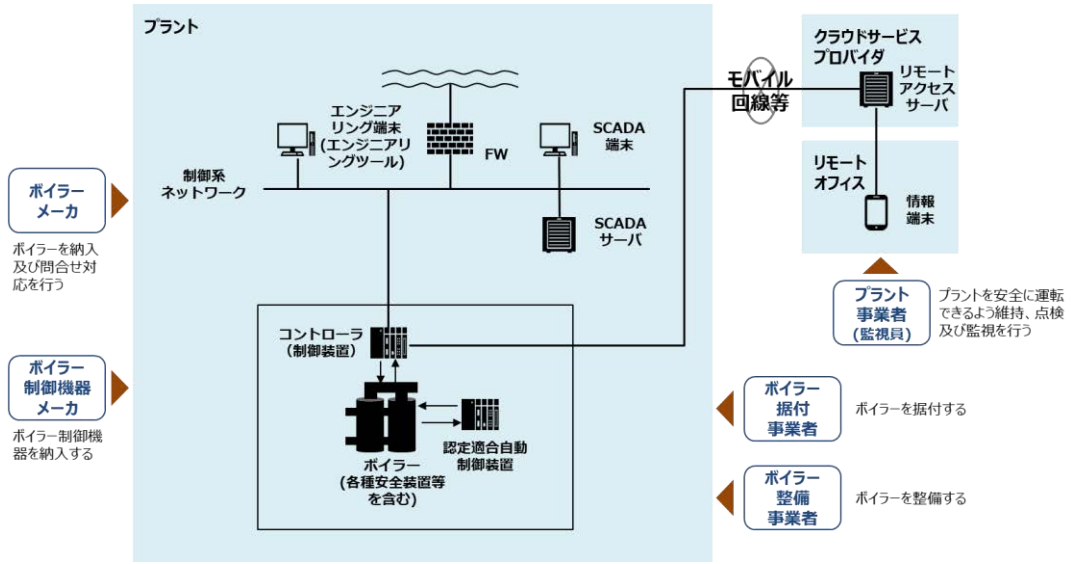


図 16 システム構成図

[11] 本ユースケースでは、一例としてクラウドを想定しているが、オンプレミスのシステムも考え得る。

[12] 本ユースケースでは情報系ネットワークの記載を省略している。

プラントでは、ボイラーの温度情報や圧力情報、流量(燃料等)情報等をコントローラ(制御装置)から SCADA サーバへ送信している。遠隔監視を行う際には、モバイル回線を利用して新たにかかる情報をコントローラ(制御装置)からリモートアクセスサーバへ送信することとした。

リモートアクセスサーバを通じてボイラーの遠隔監視を行う場合のデータフローは以下の通りとする。

1. 温度情報や圧力情報、流量(燃料/空気)情報等をコントローラからリモートアクセスサーバにモバイル回線等を利用して送信する。
2. 温度情報や圧力情報、流量(燃料/空気)情報等をリモートアクセスサーバから情報端末(スマートフォン等)に送信する。

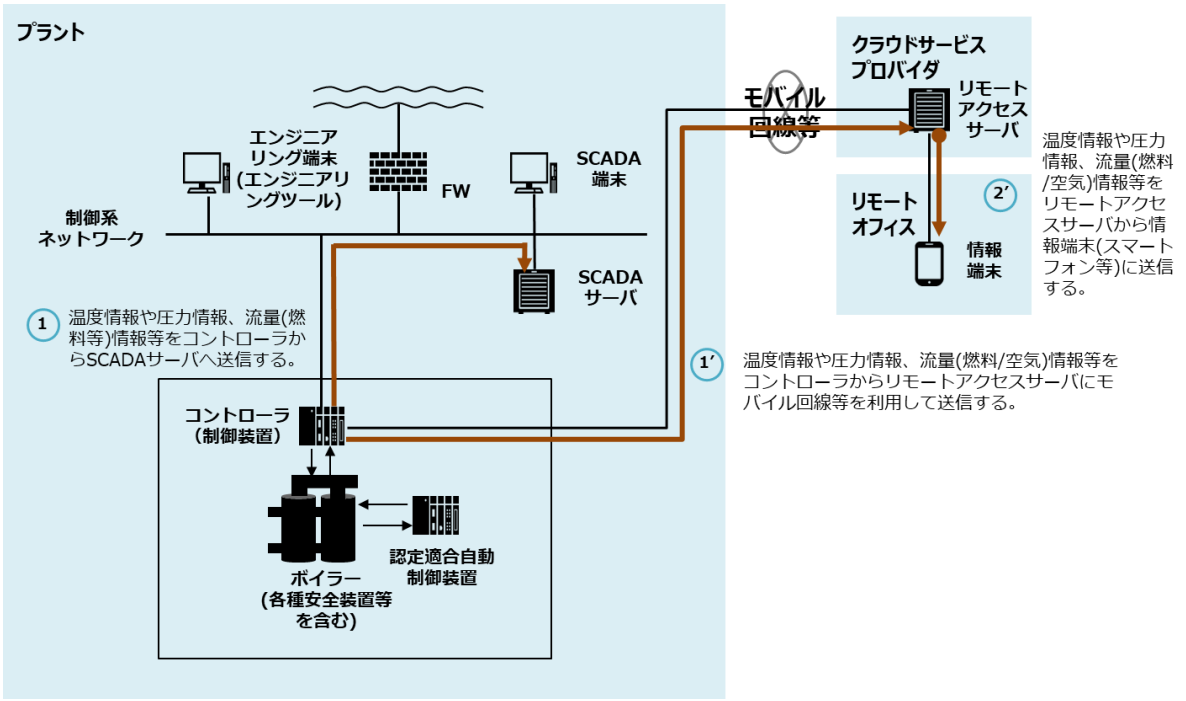


図 17 データフロー図

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、事業者 X が定めるプラントの安全に関する基本方針等に則り、従業員等において怪我または健康被害等の重大な事故等が生じないよう、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」についても、事故に伴うボイラーの破損や仮に工場の操業停止等が生じた場合であっても取引先等に対する納入の遅れ等が生じない、「限定的な経済影響」

に抑えることを目指すものとする。

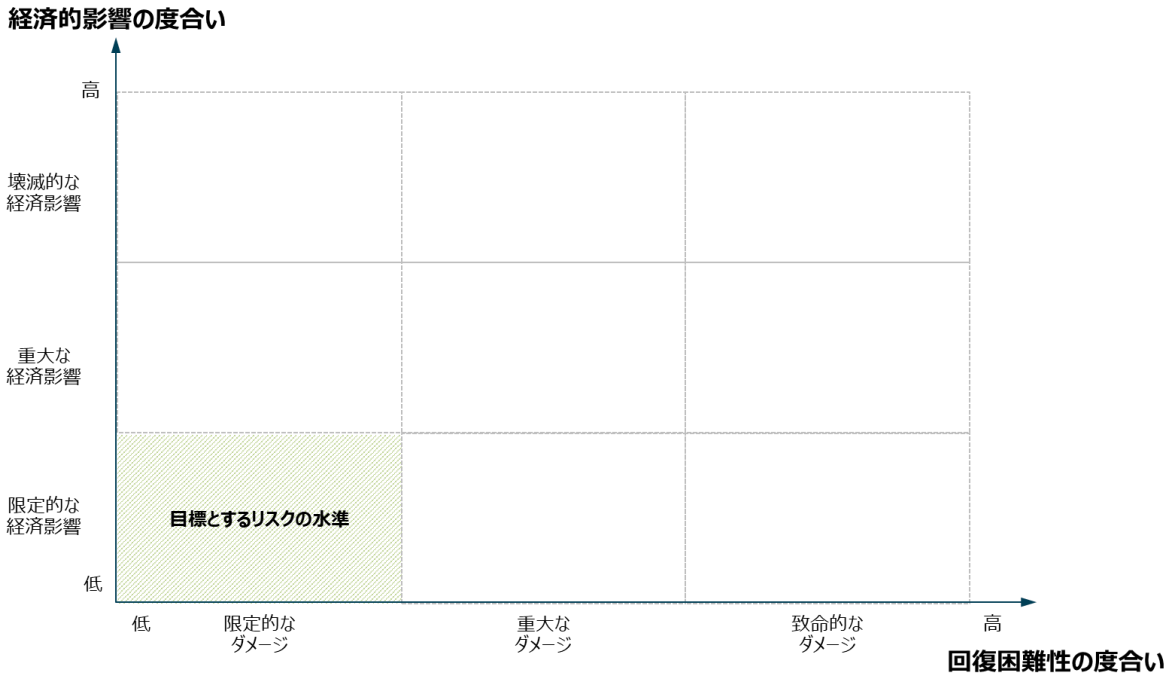


図 18 ボイラーシステムにて目標とするリスクの水準

(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、ボイラー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

ボイラーシステムにおいて、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。なお本ユースケースでは、遠隔監視の仕組みを新たに導入することによって生じるセキュリティインシデント等とその結果(影響)を特定するものとする。したがって、遠隔監視を新たに導入することによって生じるリスク以外のリスクは本ユースケースにおいて考慮していない点に留意いただきたい。

ボイラーシステムの提供又は利用に際して想定されるステークホルダーごとのセキュリティインシデント(例)は以下の通りである。データフロー後述の「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」におけるリスクの値に直結する結果は下線太字にて記載する。

- 事業者 X
- ボイラーメーカ
- ボイラー制御機器メーカ

- ボイラー据付事業者
- ボイラー整備事業者

- 事業者 X
  - 悪意のある攻撃者が、モバイル回線や情報系ネットワーク等を通じてコントローラ(制御装置)にアクセスし、プログラムまたはパラメータ(空燃比制御、蒸気圧力制御、給水制御等)を変更する。その結果、例えば、以下の 3 つの被害が生じ得る。
    - 空気量不足または排気不足によって不完全燃焼継続が生じることで未燃ガスが煙道に滞留し、煙道の爆発によって作業員が負傷し得る。また、CO 中毒によって作業員が負傷し得る。場合によってはかかる事故によって作業員が死亡し得る。
    - 化学プラントへ供給される蒸気圧力を目標とする値で制御できず、化学プラントのプロセスが異常終了することで、化学プラントが停止し得る。
    - ボイラー内の水位が低下し、ボイラー内水管などが異常過熱されることで、水管、炉壁などが損傷し、ボイラー水の漏洩や装置の破損が生じ得る。その結果、ボイラーの新規交換が必要となる。
  - 悪意のある攻撃者が、モバイル回線、情報系ネットワーク等を通じた論理的な不正アクセスや USB 等による物理的な不正アクセスによりエンジニアリング端末(エンジニアリングツール)をマルウェア感染させ、かかる端末が保存したプログラムまたはパラメータ(空燃比制御、蒸気圧力制御、給水制御等)を変更する。後日コントローラ(制御装置)がエンジニアリング端末(エンジニアリングツール)に接続されることで、コントローラ(制御装置)のプログラムまたはパラメータ(空燃比制御、蒸気圧力制御、給水制御等)が書き換えられる。その結果、例えば、以下の 3 つの被害が生じ得る。
    - 空気量不足または排気不足で不完全燃焼継続が生じることで、未燃ガスが煙道に滞留し煙道の爆発によって作業員が負傷し得る。また、CO 中毒によって作業員が負傷し得る。場合によってはかかる事故によって作業員が死亡し得る。
    - 化学プラントへ供給される蒸気圧力を目標とする値で制御できず、化学プラントのプロセスが異常終了することで、化学プラントが停止し得る 。
    - ボイラー内の水位が低下し、ボイラー内水管などが異常過熱されることで、水管、炉壁などが損傷し、ボイラー水の漏洩や装置の破損が生じ得る。その結果、ボイラーの新規交換が必要となる。
  - 悪意のある攻撃者が、モバイル回線を通じて自動制御装置に対して不正アクセスを行い、制御に関する情報を窃取する。その結果、ボイラーの監視情報が洩れ、プラントのノウハウが流

出し得る。

- 悪意のある攻撃者が、モバイル回線を通じて SCADA サーバ等に不正アクセスし、情報を漏えいさせる。その結果、プラントの管理責任者・作業員や取引先担当者の個人情報が流出し得る。

- ボイラーメーカ
  - コントローラ(制御装置)に対して脆弱性を含むアップデートを行うことにより、制御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。その結果、ボイラーの製品回収が生じ得る。
  - 事業者 X に対する注意喚起(例:遠隔監視に係る設定方法に関する説明等)を怠ることで、サービス提供における過失が認められ得る。また、契約上の責任が問われ得る。

- ボイラー制御機器メーカ
  - コントローラ(制御機器)、エンジニアリング端末(エンジニアリングツール)等に重大な脆弱性が発見される。その結果、大規模な製品回収等が生じ得る。

- ボイラー据付事業者
  - 適切な手順でボイラーを設置しなかったことにより、ボイラーが予期せぬ動作をする。その結果、サービス提供における過失が認められ得る。また、ステークホルダーを含む関係者に対する損害賠償が発生し得る。

- ボイラー整備事業者
  - 適切な手順でボイラーを整備しなかったことにより、ボイラーが予期せぬ動作をする。その結果、サービス提供における過失が認められ得る。また、ステークホルダーを含む関係者に対する損害賠償が発生し得る。

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。

- 事業者 X
- ボイラーメーカ
- ボイラー制御機器メーカ
- ボイラー据付事業者/ボイラー整備事業者

- 事業者 X

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、悪意のある攻撃者によって SCADA サーバ等へ不正アクセスされ、プラントの管理責任者・作業員や取引先担当者の個人情報が流出し得る。

セーフティの観点では、モバイル回線や情報系ネットワーク等を通じてコントローラ(制御装置)にアクセスされプログラムまたはパラメータ(空燃比制御、蒸気圧力制御、給水制御等)を変更されることによって、煙道の爆発や CO 中毒によって作業員にけがや健康被害が生じ得る。また、かかる事故の大きさや事故当時の作業員の立ち位置によっては作業員が死亡し得る。

したがって、プライバシーの観点は個人情報が流出し得ること、セーフティの観点において状況によって作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

「回復困難性の度合い」と同様にコントローラ(制御装置)のプログラムまたはパラメータ(空燃比制御、蒸気圧力制御、給水制御等)を変更されることによって、ボイラーへ供給される蒸気圧力を適切に制御できずボイラーが異常停止し、化学プラント内の一部工程が停止し得る。また、ボイラー内の水管が異常過熱されることで、ボイラー内の水の漏えいや装置の破損が生じ得る。場合によっては、ボイラーの新規交換が必要となる。

ボイラーが停止し化学プラントの工程が一部停止したとしても、他の機器・システムで代替されることによって取引先への影響を避けることが可能と考えた。

したがって、ボイラーの新規交換によって影響が一定期間続くものの、取引先への影響は小さいことを考慮して、「経済的影響の度合い」は「重大な経済影響」と評価する。

- ボイラーメーカ

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、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、ボイラーシステムが予期せぬ動作をしたとしても、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

直接的な経済影響の観点では、事業者 X の作業員が負傷しボイラーメーカの過失が認められる場合、企業の信用やブランド価値の低下に直結するおそれがある。

間接的な経済影響の観点でも同様に、ボイラーメーカの過失が認められる場合、大規模な製品回収につながるおそれがある。

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、インシデントが企業の信用やブランド価値に影響し得ることや大規模な製品回収にもつながり得ることから、「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。

- ボイラー制御機器メーカ

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、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、ボイラーシステムが予期せぬ動作をしたとしても、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

直接的な経済影響の観点では、事業者 X の作業員が負傷しボイラー制御機器メーカの過失が認められる場合、企業の信用やブランド価値の低下に直結するおそれがある。

間接的な経済影響の観点でも同様に、ボイラー制御機器メーカの過失が認められる場合、大規模な製品回収につながるおそれがある。

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、インシデントが企業の信用やブランド価値に影響し得ることや大規模な製品回収にもつながり得ることから、「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。

- ボイラー据付事業者/ボイラー整備事業者

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、ボイラーの据付時もしくは整備時を除いて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、ボイラーシステムが予期せぬ動作をしたとしても、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

適切な手順でボイラーの据付もしくは整備を行わなかったことで、ボイラーシステムに不具合が生じることによりサービスの提供に過失が認められ得る。その結果として、ステークホルダーを含む関係者に対する損害賠償の事後的な対応が発生し得る。

一方で、上記に伴う影響は限定的なものになると想定したため、「経済的影響の度合い」は「限定的な経済影響」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。

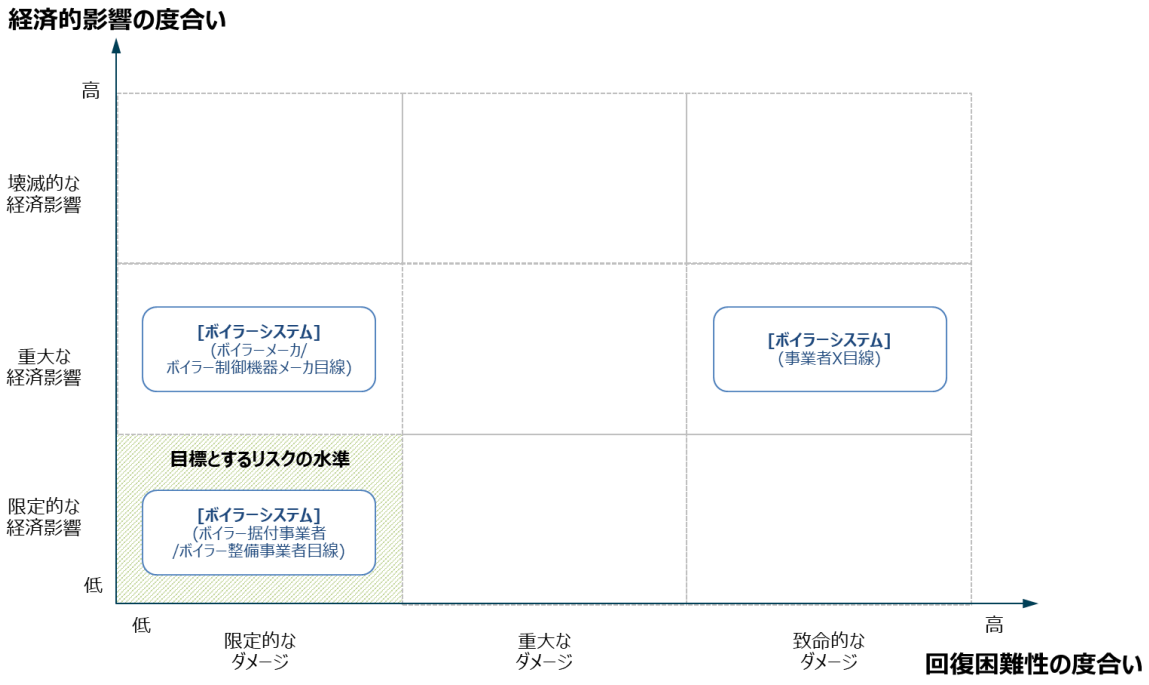


図 19 各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

「目標とするリスクの水準」の外側にある 2 つを「経済(的)影響の度合い」と「回復困難性の度合い」を軽減する観点から中心的に対策する。

- 事業者 X 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
  - セキュリティインシデントが発生したとしても、事業者 X の従業員への事故被害を最小限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、事業者 X の金銭的な被害を最小限にするための仕組みの構築

上記で示した対策方針を踏まえて、後述の「②脅威への対策」のうち行うべきと考えられる対策を明らかにした。

表 18 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
事業者 X 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	セキュリティインシデントが発生したとしても、事業者 X の従業員への事故被害を最小限にするための仕組みの構築	セキュリティ脆弱性のない(IT を使わない)安全装置の使用
		事故被害抑制マニュアルの作成
		セキュリティに関する知識・技能を有するボイラー取扱作業主任者による運用(リモートオフィス勤務時、日常現場点検時、定期自主検査時
		ボイラーの制御機器の機能の検査の実施
	セキュリティインシデントが発生したとしても、事業者 X の金銭的な被害を事後的に補填する仕組みの構築	工場操業のセキュリティ保険の利用(民間保険会社が提供するセキュリティ保険の利用)

(3) リスク対応

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 19 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)
コントローラ(制御装置)	不正アクセス	コントローラが不正アクセスされ、プログラムまたはパラメータ(空燃比制御/蒸気圧力制御/水位制御)が変更される。

	データの改ざん	コントローラの制御データが改ざんされ、プログラムまたはパラメータ(空燃比制御/蒸気圧力制御/水位制御)が変更される。
エンジニアリング端末(エンジニアリングツール)	不正アクセス	エンジニアリング端末が不正アクセスされ、エンジニアリング端末(エンジニアリングツール)が保存したプログラムまたはパラメータファイル(プログラムまたはパラメータ(空燃比制御/蒸気圧力制御/水位制御))を変更される。
	マルウェア感染	エンジニアリング端末がマルウェアに感染し、エンジニアリング端末(エンジニアリングツール)が保存したプログラムまたはパラメータファイル(プログラムまたはパラメータ(空燃比制御/蒸気圧力制御/水位制御)を変更される。
SCADA サーバ	不正アクセス	悪意のある攻撃者が、モバイル回線を通じて SCADA サーバ等に不正アクセスし、作業者や管理責任者等の情報を漏えいさせる。
	情報漏えい	SCADA サーバが不正アクセスされ、プラントにおける設備の稼働情報が流出する。
	マルウェア感染	悪意のある攻撃者が、モバイル回線を通じて SCADA サーバ等に不正アクセスし、SCADA サーバがマルウェアに感染することで、製造工程に関する設備が停止する。

881 ② 脅威への対策の整理

882 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
883 事業者 X、ボイラーメーカにて実装が想定される対策要件を整理する。

884 表 20 実装が想定される対策要件(例)

第 3 軸	実装先	想定される脅威(例)	対策要件
第 1 の観点	システム	不正アクセス、データの改ざん、 マルウェア感染	セキュリティ規格適合品の選択[13] (信頼できる IoT 機器やサービスの選定)
		不正アクセス、データの改ざん、 マルウェア感染	セキュリティ脆弱性のない(IT を使わない)安全装置の使用
		データの改ざん	遠隔監視を行う通信の保護
第 2 の観点	プロシージャ	全般	定期的なセキュリティリスクアセスメントの実施
		全般	遠隔操作の運用規則の作成
		全般	事故被害抑制マニュアルの作成
第 3 の観点	ソシキ・ヒト	全般	事業者を対象としたセキュリティ規格適合性評価の受審[14]

13 具体的な基準及び第三者評価機関等は現段階では未定とする。

14 具体的な基準及び第三者評価機関等は現段階では未定とする。

		全般	セキュリティに関する知識・技能を有するボイラー取扱作業主任者による運用[15](リモートオフィス勤務時、日常現場点検時、定期自主検査時)
	システム	全般	ボイラーの制御機器の機能の検査の実施
第４の観点	ソシキ・ヒト	全般	工場操業のセキュリティ保険の利用 (民間保険会社が提供するセキュリティ保険の利用)
		全般	サイバーセキュリティ対策サービスの利用[16]

③　整理した対策に対する意思決定

②で示した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。

上記(2)では、各ステークホルダー視点でボイラーシステム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する。

上記(2)で示したリスクアセスメントの結果を踏まえ、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。

- セキュリティインシデントが発生したとしても、事業者 X の従業員への事故被害を最小限にするための仕組みの構築
  - ✧ セキュリティ脆弱性のない(IT を使わない)安全装置の使用
  - ✧ 事故被害抑制マニュアルの作成
  - ✧ セキュリティに関する知識・技能を有するボイラー取扱作業主任者による運用(リモートオフィス勤務時、日常現場点検時、定期自主検査時
  - ✧ ボイラーの制御機器の機能の検査の実施
- セキュリティインシデントが発生したとしても、事業者 X の金銭的な被害を事後的に補填する仕組みの構築
  - ✧ 工場操業のセキュリティ保険の利用(民間保険会社が提供するセキュリティ保険の利用)

上記を踏まえて、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、事

[15] 「セキュリティに関する知識・技能を有するボイラー取扱作業主任者による運用」及び「ボイラーの制御機器の機能の検査の実施」は現時点では実施が困難な対策要件である。厚生労働省が別途定める労働安全規則及びボイラー則の改訂が必要になる。

[16] 「サイバーセキュリティお助け隊サービス制度」で認定を受けたサービスの利用を指す。サービスは多岐に渡るため、内容よっては第 1 の観点から第 3 の観点に入り得る。

904 業者 X 及びボイラーメーカが実装することとした対策要件の例を以下に示す。

905 表 21 事業者 X 及びボイラーメーカにおける実際に講じる対策要件(例)

No	第 3 軸	実装先	対策要件	実際に講じる対策(例)	対策の実施主体	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	セキュリティ規格適合品の選択(信頼できる IoT 機器やサービスの選定)	● ボイラーメーカあるいは第三者認証機関によるセキュリティ適合性評価結果をアセットオーナは確認した上で、例えば、以下の要求事項を満たしたボイラー及び関連機器・システムをボイラーメーカより調達する。 [要求事項の例] ✓ ボイラーシステムの各機器を論理的・物理的に一意に識別可能 ✓ ボイラーシステムのソフトウェア構成は許可された者のみが変更可能 ✓ 不正アクセス及び改ざんから保存・伝送するデータを保護可能 ✓ インターフェース(ローカル、ネットワーク)及びインターフェースで使用されるプロトコルやサービスに対するアクセスを許可された者のみに制限可能 ✓ 許可された者のみがソフトウェアを更新可能 ✓ セキュリティに関する状態を通知し、アクセスを許可された者のみがその情報へアクセス可能	ボイラーメーカ	
2			セキュリティ脆弱性のない(IT を	● 事業者 X は、安全装置でのセキュリティインシデントが結果的に及ぼし得るリス	ボイラーメーカ	○

			使わない)安全装置の使用	ク(例:安全装置の異常動作による操業の停止)を認識した上で、十分なセキュリティを実装している、あるいはセキュリティインシデントが生じえない安全機器を使用する等の方策を検討する。		
3			遠隔監視を行う通信の保護	• 遠隔監視を行うコントローラ(制御装置)とリモートアクセスサーバ間の通信を適切な強度で保護(IPsec-VPN の利用等)し、外部の不正アクセスを防ぐ。	ボイラーメーカ	
4	第 2 の観点	プロシージャ	定期的なセキュリティリスクアセスメント実施	• ボイラー及び関連機器・システムの運用中において、あらかじめ定めた間隔もしくは重大な変更が提案された場合に、事業者 X はかかる機器・システムに対するセキュリティリスクアセスメントを実施する。 • 事業者 X はセキュリティリスクアセスメントの結果を文書化し、一定期間保持する。	事業者 X	
5			遠隔操作の運用規則の作成	• アセットオーナは、「認定適合自動制御装置を備えたボイラーの点検及び運転に関する基準」(別添 3)を参照し、かかる基準の要求事項を満たすよう以下の要件を含む遠隔操作の運用規則を作成し、運用する。 <起動/停止> ✓ 装置(燃焼安全装置、自動圧力制御装置等)が正常であるかどうかを確認すること。	事業者 X	○

				✓ 系統(燃料系統、通風系統等)が正常であるかどうかを確認すること。 ✓ ボイラーの設置場所で起動を行うこと。 ✓ ボイラーの設置場所で定常停止を行うこと。 <点検> ✓ 起動後 1 時間以内、その後は 72 時間以内ごとに、ボイラー取扱作業主任者により、ボイラー設置場所でボイラーの状態が正常であるかどうかを点検すること。 ✓ 認定適合自動制御装置の認定を受けた者が定める方法及び頻度で認定適合自動制御装置を点検すること。 ✓ 煙道煙濃度を監視するために排煙濃度計を使用する場合は、保護ガラスの清掃を行う等により機能を維持すること。 <情報端末の管理> ✓ ボイラー取扱作業主任者は、ボイラー運転中に常時情報端末を携帯する、または情報端末を設置した場所に常駐すること。シフト制勤務とする場合は、交代の際に情報端末を確実に引き継ぐこと。 ✓ 情報端末を携帯する者は、電波が受信可能な場所に勤務し、1 時間ごとにボイラーの運		

				転状況を確認した上で、適切な頻度で情報端末の電池の充電状況を確認し、必要な充電を行うこと。 ※「点検」を行う際には、ボイラーに備え付けられた計器と情報端末が示す値が一致していることを確認すること。また、「情報端末の管理」を実施する際には、その状態が維持されていることを確認すること。		
6			事故被害抑制マニュアルの作成	● 既に事業者 X 側で整備している事故被害抑制マニュアルにセキュリティインシデント発生時の対応手順を追記する。以下の手順ごとに実施事項を整理する。 ➢ セキュリティインシデントの検知・受付連絡 ➢ トリアージ ➢ インシデント対応 ➢ 報告/情報公開等	事業者 X	
7	第 3 の観点	ソシキ・ヒト	事業者を対象としたセキュリティ規格適合性評価の受審	● アセットオーナは、適合性評価機関よりセキュリティマネジメントシステムに係る規格適合性評価を受ける。 ● 適合性評価結果を踏まえて、アセットオーナは認証機関よりセキュリティマネジメントシステムの認証を受ける。	事業者 X	
8			セキュリティに関する知識・技能を有するボイラー取扱作業主任者による運用(リモートオフィス勤	● 以下のサイバーセキュリティに関する知識・技能を有したボイラー取扱作業主任者を配置する。 ● IT ベンダやシステムインテグレータと連携をとりつつ、	事業者 X	○

			務時、日常現場点検時、定期自主検査時)	セキュリティインシデントに対応可能 ● マニュアル(※)に定められたセキュリティに関する役割を完遂可能 ※マニュアルに含まれる内容の例 ● 適切な資産管理(ボイラー、コントローラ、認定適合自動制御装置、情報端末等) ● セキュリティインシデントの拡大防止		
9			ボイラーの制御機器の機能の検査の実施	● アセットオーナはボイラーを対象とした性能検査(年1回)に加えて、認定適合自動制御装置を対象とした機能の検査も受けることとする。ただし、両検査は必ずしも同じ機関が実施する必要はない。 ● 検査結果によって、ボイラーメーカは産業用コンポーネント製品を対象とした認証(※)を取得する。 ※制御機器の機能の検査を、制御機器メーカ／ボイラー整備業者／登録性能検査機関／登録適合性証明機関のいずれかが併せて実施するか、それとも、別の事業者が実施するかついては、現段階では未定。機能の検査周期も未定。	事業者 X	○
10	第4の観点	ソシキ・ヒト	工場操業のセキュリティ保険の利用 (民間保険会社が提供するセキュリティ保険の利用)	● 事業者 X は、サイバー攻撃による工場停止に追い込まれた場合を想定して、以下を補償するセキュリティ保険に加入する。 ➢ 調査費用 ➢ 復旧費用	事業者 X/ボイラーメーカ	○

				➢ 工場停止に伴う逸失利益		
11			サイバーセキュリティ対策サービスの利用	● 事業者 X は、以下のサイバーセキュリティお助け隊サービスを利用する。 <サイバーセキュリティお助け隊サービスの例> ➢ セキュリティに関する相談対応 ➢ インシデント発生時の駆け付け支援 ➢ ネットワーク監視サービスの提供	事業者 X/ボイラーメーカ	

2-4 設備保全業務支援サービス

本ユースケースは、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、「設備保全サービス事業者」という。) が工場を持つユーザ事業者へ提供する設備保全業務支援サービスシステム等を対象にIoT-SSFに基づくリスクアセスメント及びリスク対応を行った結果をまとめたものである。

設備保全サービス事業者が提供する設備保全業務支援サービスシステムは、受変電・電気設備をはじめとする設備に設置した各種センサ、エッジコントローラなどから得たデータに基づいて、運転情報、保全情報を可視化、分析することで、各設備・機器に最適なメンテナンスを提供するものを想定する。

設備保全サービス事業者は、新たにサービスを提供するにあたって、サービスを受ける事業者をユーザ事業者として設定してリスクアセスメントを行い、リスクに対してはステークホルダー間で対策内容を調整することで、可能な限り、リスクを低減する。

(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

設備保全サービス事業者は、工場の各設備に設置された各種機器を通じて設備の稼働情報を常時収集する。計器がネットワークに接続していない場合、計器読取サービス事業者が提供する計器読取サービス(SaaSで提供)と連携して、かかる計器よりデータを取得する。計器読取サービス(SaaSで提供)では、IoTカメラで取得した画像データを値データへ変換し、設備保全業務支援サービスシステムへ送信する。

設備保全サービス事業者は、設備保全業務を支援するサービスと収集した設備情報に基づ

いてユーザ事業者へ通知を行うサービスを提供する。設備保全サービス事業者が各設備の保守業務も請け負うこととし、もし設備の異常を検知した場合には、ユーザ事業者の管理者にメール等で通知するとともに、即座に現場へ駆け付けることを想定する。

なお、各種センサ及びIoTカメラは工場内の制御ネットワークには接続していないものとする。

- 設備保全サービス事業者は工場の各設備に設置された各種機器を通じて、設備の稼働情報を常時収集する。
- ネットワークに接続していない計器についてはIoTカメラを使用した計器読取サービス(SaaS)と連携してデータを取得する。
- 設備保全サービス事業者は設備保全業務を支援するサービスと収集したデータに基づいた通知を行うサービスを提供する。
- 設備保全サービス事業者が各設備の保守業務も請け負うこととし、もし設備の異常を検知した場合には、ユーザ事業者の管理者にメール等で通知するとともに、即座に現場に駆け付けることを想定。

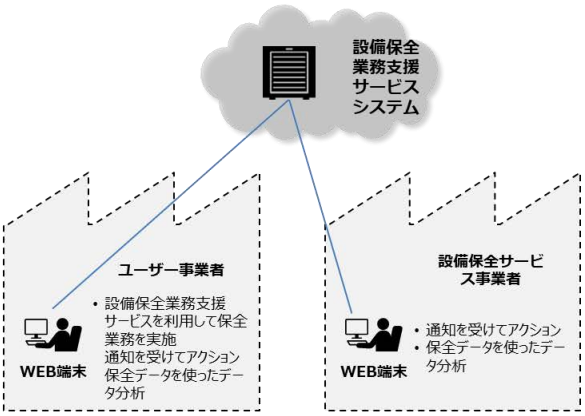


図 20 対象ソリューションのイメージ

② ステークホルダー関連図

本ユースケースにて示す取組に関与するステークホルダーは、以下に示すように「設備保全サービス事業者」や「計器読取サービス事業者」、「ユーザ事業者」を想定している。契約関係や製品・サービスの提供関係を考慮したステークホルダー関連図は、以下に示す通りである。

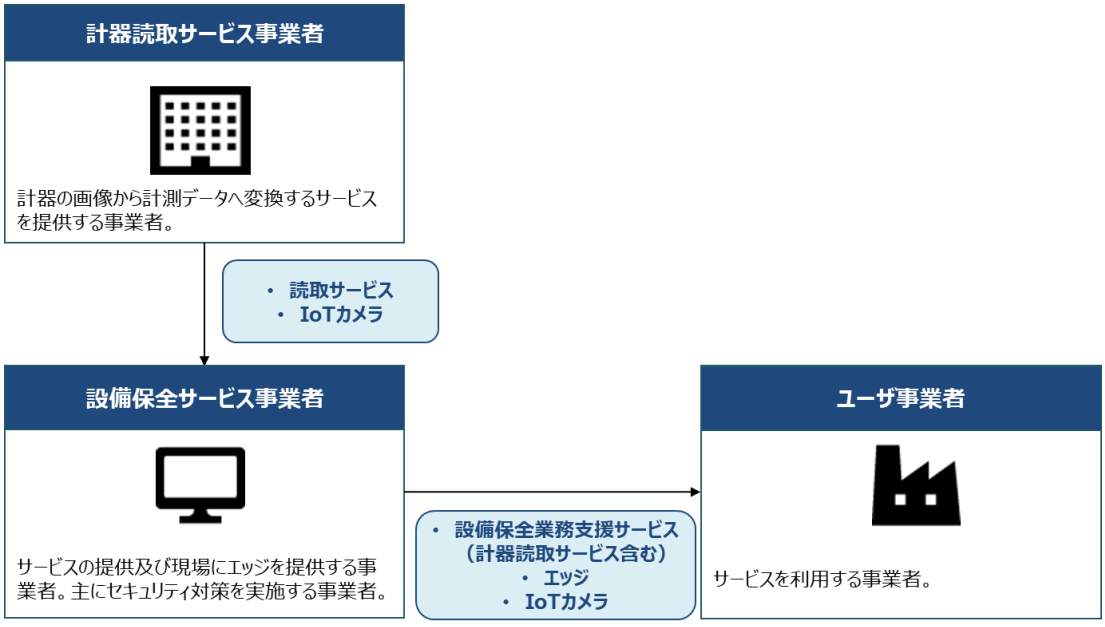


図 21 ステークホルダー関連図

＜IoT サービス開発者/IoT サービス提供者＞

● 設備保全サービス事業者

計器読取サービス事業者が提供する IoT カメラ及びサービスを活用しつつ、エッジ及びユーザ事業者が保有する設備への保守サービスの提供を行う事業者を想定する。本ユースケースでは、主にセキュリティ対策を実施する事業者とする。

● 計器読取サービス事業者

計器の画像から計測データへ変換するサービスを提供する事業者を想定する。設備保全サービス事業者を通じて、IoT カメラ及び画像読み取りサービスをユーザ事業者へ提供する。

＜IoT サービス利用者＞

● ユーザ事業者[17]

設備保全サービス事業者が提供するサービスを利用する事業者を想定する。なお、工場にて受変電・電気設備をはじめとする設備を保有する事業者を想定している。本ユースケースでは保守サービスを幅広い業界で活用いただくことを想定して、具体的な対象企業を定めずにリスクアセスメント及びリスク対応を行うこととした。

③ システムを構成する機器の一覧

本ユースケースの対象となる機器は以下の通りとする。なお、IoT カメラを除く各種センサや各計器、通信キャリアが提供する機器はリスクアセスメントの対象から除外している。

表 22 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
設備保全業務支援サービスシステム	ユーザ事業者の設備保全業務の支援サービスを提供する。 また、各種センサ・各種計器から収集したデータを基に事象発生通知やデータ分析支援を行う。
WEB 端末	ユーザ事業者が設備保全業務支援サービスを利用する端末。(WEB システム) 設備保全サービス事業者が顧客支援を行う端末。(WEB システム)
エッジ	各種センサからデータを収集し、インターネット経由で設備保全業務支援サービスシステムへ送信する機器。ユーザ事業者の工場内に設定されている。
IoT カメラ	各種計器の画像を撮り、インターネット経由で計器読取サービスへ画像データを送信するカメラ。画像データはユーザ事業者の従業員が取得するものとする。

[17] 本ユースケースでは、設備保全サービス事業者が提供する受変電・電気設備をユーザ事業者が利用するものとするが、他企業が提供する受変電・電気設備であってもサービスの提供は可能としている。

クラウドサービス (計器読取サービス)	各種計器の画像から値データへ変換し、設備保全業務支援サービスシステムへ送信するサービス。

④　システム構成図、データフロー図

本ユースケースで対象とするシステムは、計器読取サービス事業者が提供するクラウドサービスや設備保全サービス事業者が提供する設備保全業務支援サービスシステム、エッジ等から構成される。システム構成図は以下の通りとする。

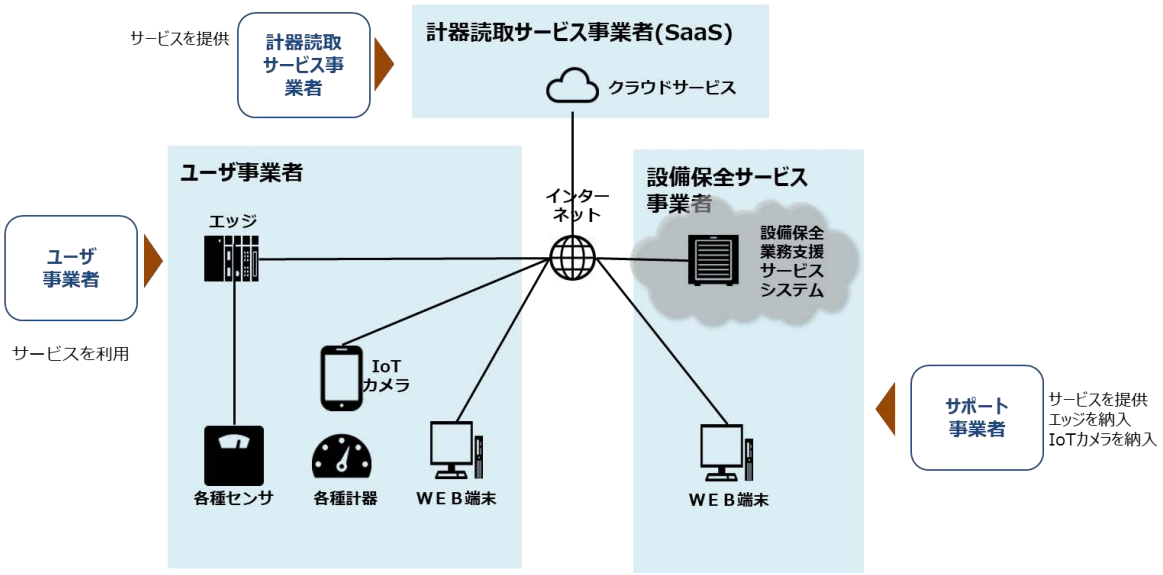


図 22 システム構成図

各種センサから設備稼働情報を収集した上で、WEB端末にて稼働情報を確認する際のデータフローは2パターンを想定している。データフローは以下の通りとする。

<パターン 1>

1. 各種センサよりエッジを通じて設備保全業務支援サービスシステムに稼働情報を送信する。
2. WEB 端末にて設備保全業務支援サービスシステムの稼働情報を確認及び分析する。

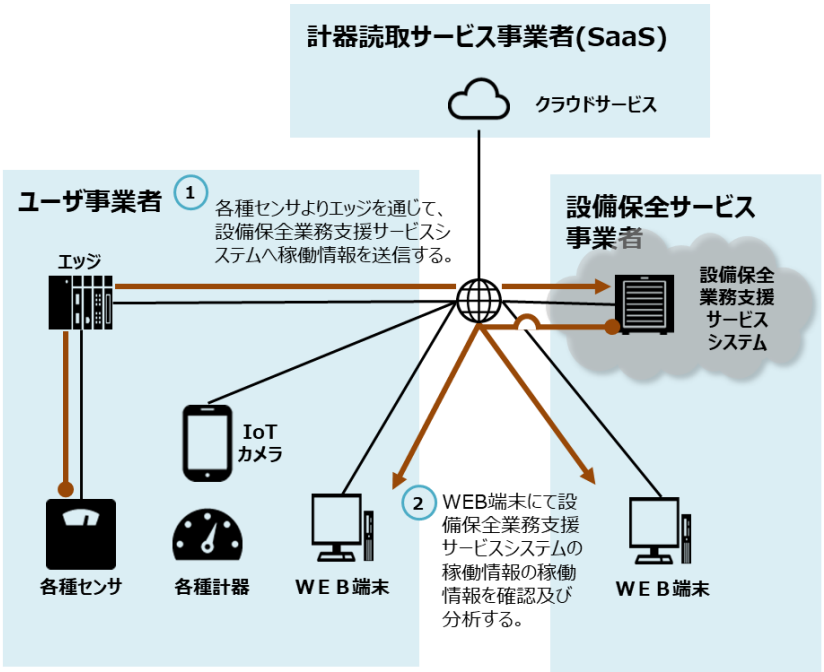


図 23 データフロー図(パターン 1)

<パターン 2>

1. IoT カメラより読取サービス事業者のクラウドサービスへ画像データを送信する。
2. 計器読取サービス事業者のクラウドサービスにて画像データを値データに変換した上で、設備保全業務支援サービスシステムに稼働情報を送信する。
3. WEB 端末にて設備保全業務支援サービスシステムの稼働情報を確認及び分析する。

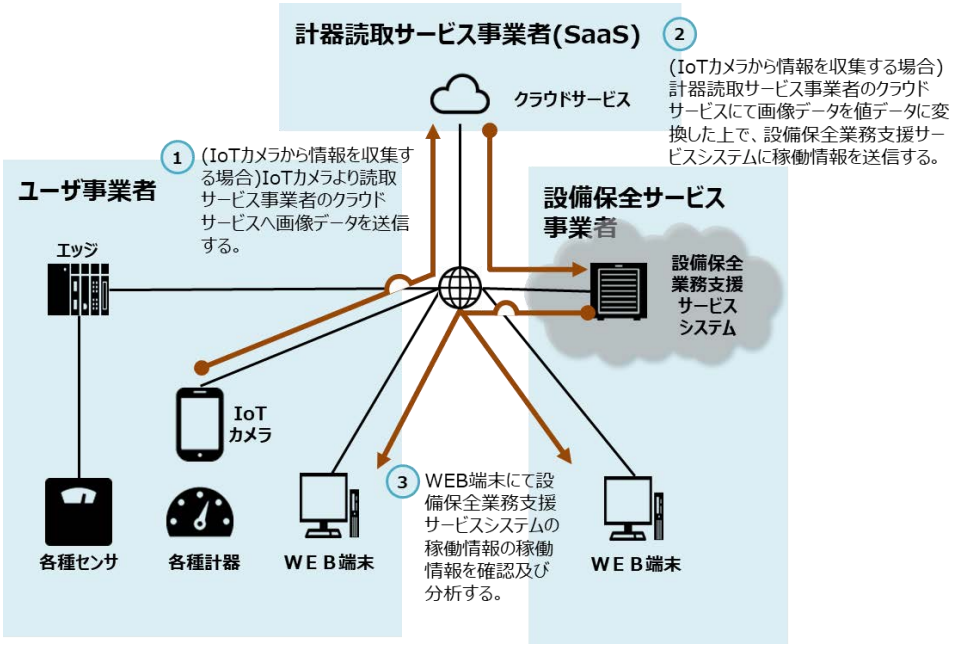


図 24 データフロー図(パターン 2)

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」は、設備保全サービス事業者において重大な事故が発生しないよう「限定的なダメージ」に抑えることを目指す。「経済的な影響の度合い」は、設備保全サービス事業者における工場の操業停止等が生じないよう「限定的な経済影響」に抑えることを目指す。

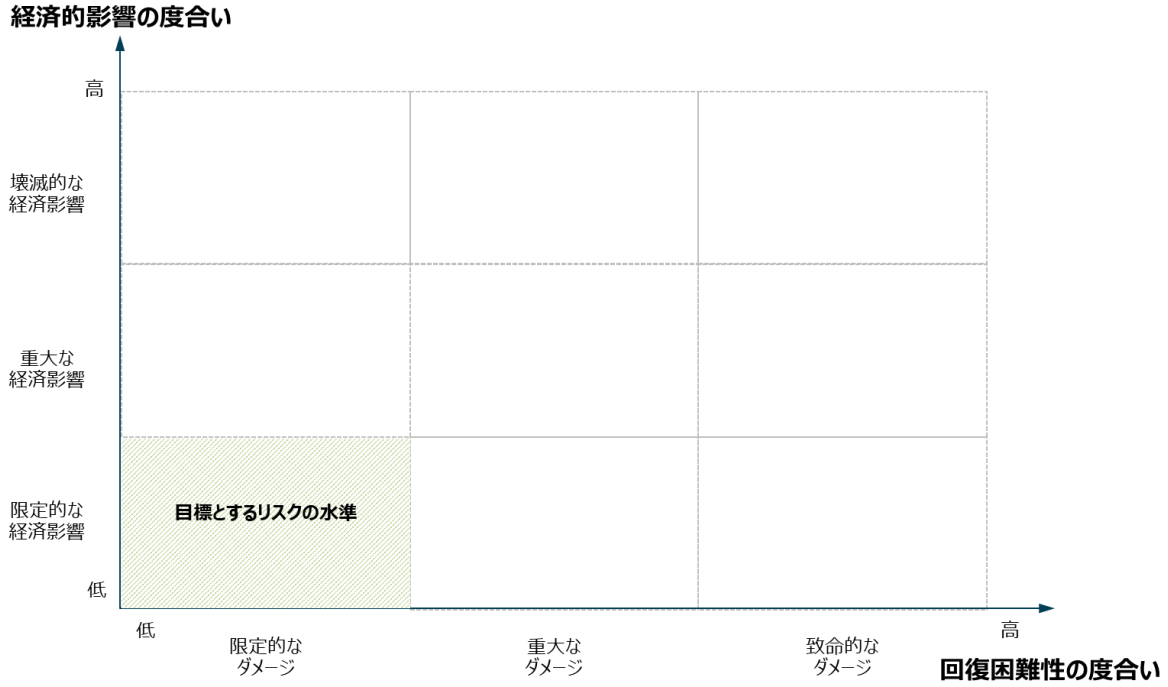


図 25 目標とするリスクの水準

(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、設備保全業務支援サービス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

設備保全業務支援サービスシステム及びクラウドサービス(計器読取サービス)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。設備保全業務支援サービスシステム及びクラウドサービス(計器読取サービス)の提供又は利用に際して想定されるステークホルダーごとのセキュリティインシデント(例)は以下の通りである。データフロー後述の「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」におけるリスクの値に直結する結果は下線太字にて記載する。

- 設備保全サービス事業者

- ユーザ事業者
- 計器読取サービス事業者

- 設備保全サービス事業者
  - 悪意のある攻撃者が、インターネット経由で設備保全サービス事業者が管理する設備保全業務支援サービスシステムをマルウェア(例:ランサムウェア)に感染させる。その結果、設備保全業務支援サービスの一部機能を停止せざるを得ないため、**設備保全サービス事業者がユーザ事業者に対してサービスを提供できなくなり得る**。また、設備稼働状況(生産状況)が漏えいすることで設備保全サービス事業者の信頼が低下し得る。

- ユーザ事業者
  - 悪意のある攻撃者または設備保全サービス事業者の従業員が、インターネット経由で設備保全サービス事業者が管理するサービスシステムに不正アクセスする。その結果、**設備稼働状況(生産状況)等のデータが流出することで、ユーザ事業者の競争力が失われ得る**。また、**設備保全業務支援サービスが利用できなくなることが想定され、設備稼働の低下につながり得る**。

- 計器読取サービス事業者
  - IoT カメラからクラウドサービス(計器読取サービス)に対する通信において、画像データが改ざんされる。その結果、**計器読取サービス提供における信頼を失い、契約を解除され得る**。また、過失が認められた場合、契約上の責任を問われ得る。

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」及び「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。

- 設備保全サービス事業者
- ユーザ事業者
- 計器読取サービス事業者

- 設備保全サービス事業者

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、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、設備保全業務支援サービスが予期せぬ動作をしたとしても、設備保全サービス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

直接的な経済影響の観点では、設備保全サービス事業者が管理する設備保全業務支援サービスシステムのマルウェア感染によって、サービスの一部機能が停止した場合、設備保全サービス事業者がユーザ事業者に対してサービスを提供できなくなり得る。また、顧客の設備稼働情報が流出することで企業の信用、ブランド価値の低下に直結し得る。

同様に、間接的な経済影響の観点では、顧客の設備稼働情報の流出によって設備保全サービス事業者に対する賠償費用が生じ得る。

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、インシデントが企業の信用低下、ブランド価値の低下につながり得ること、また、賠償費用が生じ得ることから、「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。

- ユーザ事業者

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、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、設備保全業務支援サービスが予期せぬ動作をしたとしても、ユーザ事業者の従業員がけがを負う可能性や設備機器が損害を受ける可能性は低いと想定される。

プライバシーの観点では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従業員がけがを負う可能性や設備機器が直接的に損害を受け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

直接的な経済影響の観点では、設備保全業務支援サービスシステムに対する不正アクセスによってサービス事業者が提供する保守サービスが利用できなくなることで、工場における設備稼働の低下につながり得る。また、設備稼働状況(生産状況)などのデータが流出することで、ユーザ事業者の競争力が失われ得る。

直接的な経済影響において、工場における設備稼働の低下やユーザ事業者の競争力が失わ

れ得ることから、「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。

- 計器読取サービス事業者

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、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、クラウドサービス(計器読取サービス)が予期せぬ動作をしたとしても、計器読取サービス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

直接的な経済影響の観点では、IoT カメラより計器読取サービス事業者が提供するクラウドサービス(計器読取サービス)へ送信される画像データが改ざんされることによって、サービス提供における信頼を失い、契約を解除されるおそれがある。また、サービス提供における過失が認められ得る。[18]

直接的な経済影響において、契約解除のおそれがあることから「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。

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。

[18] その結果として、契約上の責任を問われ得る。

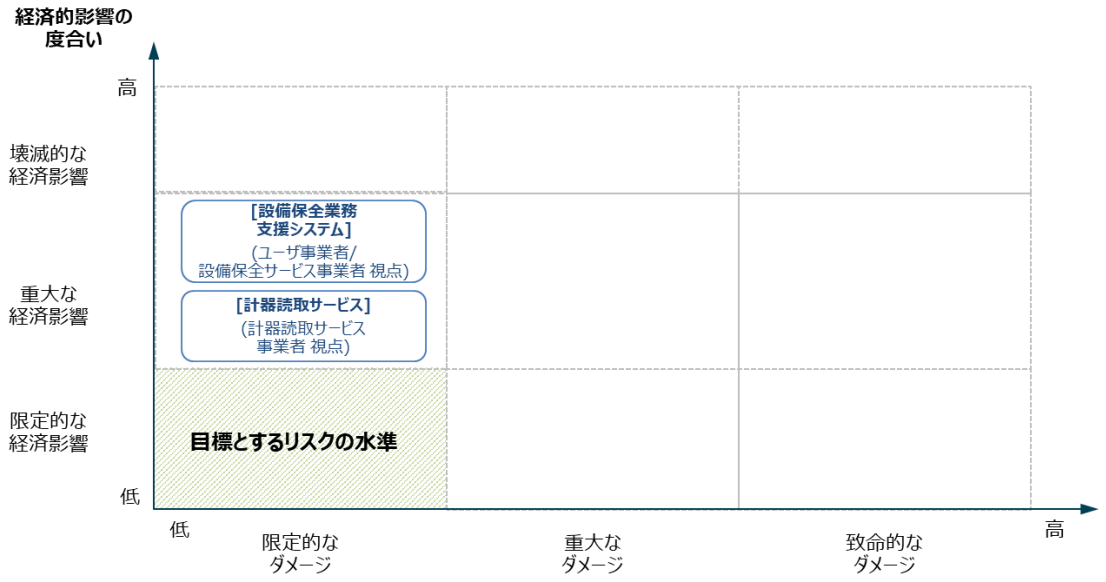


図 26 各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

「目標とするリスクの水準」の外側にあるシステムに対して「経済(的)影響の度合い」と「回復困難性の度合い」を軽減する観点から中心的に対策する。影響度が大きいリスクに対処するための対策方針を以下の通り整理した。

- ユーザ事業者及び設備保全サービス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」に影響を及ぼすサービス停止等を防ぐための対策
- 計器読取サービス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」に影響を及ぼすサービスへの信頼低下、契約解除等を防ぐための対策

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、本ユースケース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 23 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
ユーザ事業者及び設備保全サービス事業者	「経済的影響の度合い」に影響を及ぼすサービス停止等を防ぐための対策	適切な水準のアクセス制御の実装
		マルウェア対策の実施
		IoT 機器・システムに対するアップデートの適用
計器読取サービス事業者	「経済的影響の度合い」に影響を及ぼすサービスへの信頼低下、契約解除等を防ぐための対策	適切な水準のアクセス制御の実装
		マルウェア対策の実施
		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

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。なお、本ユースケースでは、サービスを提供する事業者の信頼低下や契約解除等の「経済的影響の度合い」に直接影響を及ぼし得る脅威[19]について検討することとした。

表 24 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)
設備保全業務支援サービスシステム	マルウェア感染	設備保全業務支援サービスシステムがマルウェア感染し一部機能が停止する。また、マルウェア感染によって一部または全部のサービスを停止させる必要が生じる。
	不正アクセス	設備保全業務支援サービスシステムが不正アクセスされ一部または全部のサービスを停止させられる。また、不正アクセスにより、顧客の設備稼働情報が組織外部へ流出する。
IoT カメラ	データの改ざん	IoT カメラが不正アクセスされ、画像データが改ざん・消去される。

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設備保全サービス事業者及び計器読取サービス事業者にて実装が想定される対策要件を整理する。

[19] マルウェア感染、不正アクセス、データの改ざんによってサービスの停止が、マルウェア感染や不正アクセスによってデータの漏えいが引き起こされ、結果的に「経済的影響の度合い」を大きくさせ得ると想定している。

表 25 設備保全サービス事業者及び計器読取サービス事業者にて実装が想定される対策要件(例)

第 3 軸	実装先	想定される脅威(例)	対策要件
第 1 の観点	システム	不正アクセス	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
		マルウェア感染	マルウェア対策の実施
		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
第 2 の観点	プロシージャ	マルウェア感染	脆弱性対応に必要な手順等の整備と実践
		不正アクセス、マルウェア感染	インシデント対応手順の整備と実践
	システム	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
		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。

- 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。設備保全業務支援サービスシステムに対するリスクにおいて、設備保全業務支援サービスシステムへのマルウェア感染や不正アクセスによって、設備保全サービス事業者のサービスの停止に直結し得る。また、その結果、ユーザ事業者の稼働率低下や稼働停止を招き得る。また、「設備保全業務支援サービス」の一部であるクラウドサービス(計器読取サービス)に関するデータの改ざんによってサービスへの信頼低下を招き得る。したがって、以下に示す対策によって「経済的影響の度合い」に影響を及ぼし得るリスクへ対処を行う。

- 適切な水準のアクセス制御の実装
- マルウェア対策の実施
- 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、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、設備保全サービス事業者が実装することとした対策の例を以下に示す。なお、一部対策については設備保全サービス事業者より計器読取サービス事業者へ対策を依頼することとした。

1121 第 1 の観点では、設備保全サービス事業者が企画段階において、当該事業者やユーザ事業
1122 者、計器読取サービス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
1123 理した。
1124 第 2 の観点では、運用段階において、当該事業者やユーザ事業者、計器読取サービス事業
1125 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。

1126 表 26 設備保全サービス事業者における実際に講じる対策要件(例)

No	第 3 軸	実装先	対策要件	実際に講じる対策(例)	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	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	● 企画・設計の段階で、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。	
2			適切な水準のアクセス制御の実装	● 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。<ユーザ(ヒト)の認証>	○
3			マルウェア対策の実施	● 「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対策を実施する。	
4			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	● システム構築セキュリティチェックリストを使って、下記のような初期設定や構成を、一定水準のセキュリティが確保できるものとする。 ✓ ネットワークポート ✓ ソフトウェアのバージョンとパッチ ✓ サービスの機能やデータへのアクセス制御	
5	第 2 の観点	プロシージャ	脆弱性対応に必要な手順等の整備と実践	● 会社推奨の脆弱性診断ツールを使って、自身が開発、提供している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の更新等の措置を講じる。	
6			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。 • インシデント対応手順には、以下のプロセスを含める。 ✓ 検知・受付連絡:「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: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。	
7		システム	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、対象のシステムの運用時において、サービス提供者は、利用者の活動、システムの挙動、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。	

8			IoT 機器・システムに対するアップデートの適用	● システムを構成するソフトウェアの更新は、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する。 ✓ 更新プログラムは、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たものを利用する。 ✓ 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)	

1127 • 計器読取サービス事業者に対応を依頼すべき対策要件(例)

1128 表 27 計器読取サービス事業者に対応を依頼すべき対策(例)

No	第 3 軸	実装先	対策要件	実際に講じる対策(例)	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	ソフトウェアの完全性の検証	● 計器読取サービス提供者は、データを利用する前に、ハッシュ等を利用し、データの真正性を確認する。	

1129 ## 3. 参画各社より頂戴した主なご意見

1130 適用実証では、2 章で紹介したユースケースの作成と並行して、適用に際して参画事業者が
1131 感じた所見や今後に向けた要望をヒアリングした。いただいた主なご意見について、以下で示す。

1132 ### ● 適用した際に感じたメリット、適用して気付いた新たなリスク

No	サマリ	実際に寄せられたご意見
1	サービスに係るステークホルダー間で共通認識を持ちつつ、リスク等を洗い出すことが可能。	● サービスを提供する際に IoT-SSF を適用することで、システム構成やステークホルダーを明らかにすることができ、関係者間で共通の認識を持ちつつ脅威を整理できる。[住宅メーカ/シャッター製造販売事業者] ● 製品安全分野における既存の規定や関連するステークホルダーと協力して、リスクアセスメントを実施した上で、対象とするシステムへの対策を検討することができる点にメリットを感じた。特に、製品安全の分野の技術

		者とセキュリティの分野の技術者で認識の差異が生じている点に対して認識をすり合わせることができた。[ボイラー制御機器メーカ等] ● 外部の SaaS 提供事象者のリスクも踏まえて、リスクアセスメントを実施することができた。[設備保全サービス事業者]
2	今までのリスクアセスメント手法で気付くことができなかったリスクに気付くことが可能。	● 「経済的影響の度合い」を考慮することによって、今までのリスク分析では考慮できていなかったブランド価値への影響(リスク)について考える機会を持てた。[住宅メーカ/シャッター製造販売事業者] ● 直接的なリスクではないが、既存のリスクアセスメントでは考慮していなかった販売店(コールセンター)の人員ひっ迫及び対応費用について考える機会を得た。[エアコン製造事業者] ● リスクアセスメントにおいて「誰にとってのリスクか」という観点で場合分けしている。今回のユースケースの「計器読取サービス事業者」にとってのリスクという観点は、通常の業務では考慮していないケースが多い。[設備保全サービス事業者] ● 遠隔監視の仕組みを導入することによって新たに生じるセキュリティリスク(例:通信に対するセキュリティリスク)に気付くことができた。[ボイラー制御機器メーカ等] ● システム構成をシンプルな構成図に見直す作業を通して、リスクが潜む箇所の顕在化に役立つケースがあると考えられる。[設備保全サービス事業者]

1133 ● **適用の際の問題点/悩んだ点(他の文献とのハレーションを含む)**

No	サマリ	実際に寄せられたご意見
1	システム構成図やデータフロー図を作成する際の記載粒度で悩んだ。	● ステークホルダー関連図の記載粒度やユースケースの適用範囲で悩んだ。作業の目的が明確であれば、記載粒度にも悩まずに済んだ可能性がある。記載目的が明確になると、記載粒度も自ずと明らかになる可能性がある[住宅メーカ/シャッター製造販売事業者] ● 感想に近いものになるが、リスクアセスメントを行う際にどこまで(例:整理する情報の粒度やセキュリティの強度、サービス範囲)実施すればよいかわからない。[住宅メーカ/シャッター製造販売事業者] ● データフロー図の番号のつけ方で悩んだ。大枠ではデータの流れなのかもしれないが、必ずしもシーケンシャルなデータフローとならないケースもあり得る。[設備保全サービス事業者] ● 脅威の洗い出しをどの程度まで実施(深堀)すべきかが判断できなかった。[住宅メーカ/シャッター製造販売事業者] ● 「リスクアセスメント」のワークシートは、ステークホルダーに記載するフォーマットになっている。想定するインシデントはステークホルダー毎に発生するわけではないので記入に悩むことがあった。[設備保全サービス事業者]
2	どこまでの粒度で情報を整理すれば IoT-SSF の適用したことになるのか判断できない。	● IoT-SSF をどこまで適用すればよいか不明瞭な部分があった。裏を返せばどこまでやれば、IoT-SSF を適用したことになるのかの線引きができない状況である。例えば、マルチステークホルダーで対策を実施する際や調

		達要件に IoT-SSF の適用を定めた場合に、ミスコミュニケーションが発生する可能性がある。[住宅メーカ/シャッター製造販売事業者]
3	IoT-SSF の適用に大きな工数が必要となる。	● IoT-SSF をソリューションに適用する際には、(実システムの機能仕様～セキュリティ専門的解析まで検討幅が広く、また、参照資料を見ながら対応するため、回答作成に)非常に大きな工数が必要となる[エアコン製造事業者] ● 様々な視点からセキュリティを考慮できる点はよいが、リスクアセスメントに係る工数が大きい。また、セキュリティを検討する際にどこに注力していくべきかがわからない(一企業では定められない)場合がある。[住宅メーカ/シャッター製造販売事業者] ● 脅威に対して添付 A から「対策要件」を選択する手順となっているが、添付 B の「実際に講じる対策の例」が頭に入っていないと選び難かった。今回の作業に当たっては、添付 A と添付 B の両方が記載された表を先に作成し、対策要件毎に「どの脅威に対する対策か」をマッピングし作成することになった。(結果的にワークシートの作成手順とは逆順のようになってしまった)当てはまる対策を選びにくかったため、脅威と対策がセットになっているとより選びやすい。[設備保全サービス事業者] ● 今回の IoT-SSF 適用対象では設備保全業務支援システムと計器読取支援サービスシステムを対象とした。今回は想定され得る脅威を絞ってリスクアセスメントを行ったが、実際には膨大になり得る。作業工数を減らすための仕組みがあるとよい。また、対象となる脅威を絞りこむための基準があるとよい。[設備保全サービス事業者]
4	類似事例がない場合、セキュリティの知識を持たない企業では IoT-SSF の適用が難しい。	● 同じ業界や近い業界における類似事例があればよいが、類似事例がない場合、セキュリティの知識を持たない企業では IoT-SSF の適用が難しい可能性がある。[住宅メーカ/シャッター製造販売事業者]
5	他のリスクアセスメントにて採用している考え方と一部異なる部分があり、判断に悩んだ。	● リスクの重要度を測る際、IEC62443 等の既存の文書では「起こりやすさ」を考慮する一方で、IoT-SSF では必ずしも考慮すべきとは記載していない。本ユースケースで起こりやすさを考慮すべきか悩んだ。[ボイラー制御機器メーカ等]

1134 ● **IoT-SSF等の改訂に向けた要望**

No	修正対象	内容	実際に寄せられたご意見
1	IoT-SSF	安全分野(けがの分野)との関係性の整理及びかかる記載の追加	● 安全分野(けがの分野)の視点を IoT-SSF を更に盛り込んだ上で、セキュリティ分野との関係性を整理できるとよい。[エアコン製造事業者]
2		第 3 軸に関する記載の追加	● 第 3 軸の第 3 の観点及び第 4 の観点について、具体的な内容が IoT-SSF やユースケース集に示されていなかったため、何を記載すればよいかわからなかった。[設備保全サービス事業者]

3	(適用実証時に使用した)IoT-SSF の適用手順書	適用主体やとりまとめを行う主体に関する説明の追加	● ユースケース集に記載された「適用主体」について、適用手順書においても説明があるとよい。[ボイラー制御機器メーカ等] ● マルチステークホルダーでサービスを展開する際に、誰が IoT-SSF をとりまとめるのかを明確にしていただきたい。[住宅メーカ/シャッター製造販売事業者] ● 複数社で責任分界点を明確にするためには、ステークホルダー関連図とシステム構成図、データフロー図を作成する際にステークホルダー間で共通認識を作る必要がある。(適用手順書にて強調すべき) [住宅メーカ/シャッター製造販売事業者] ● IoT-SSF を全社で適用することは非常に手間がかかり非現実的である。一方で、自社で完結するのであればよい。ルールが必要ではないか。（調達要件として提示することは可能。） ※全てのサービスに適用することは難しい。サービス要求レベルから求めるセキュリティのレベルが異なる。[住宅メーカ/シャッター製造販売事業者]
4		記載粒度の明確化	● 「リスクアセスメント、リスク対応に向けた事前準備」の(2)ステークホルダー関連図、(4)システム構成図、データフロー図を作成する際に、当該資料の作成目的が分からなかったため、記載粒度や記載方法で悩んだ。適用手順書に作成目的が明記されていればより作成がしやすくなると考えられる。[エアコン製造事業者] ● 適用手順書において、曖昧な用語(例:「整理する」とあるが、具体的なイメージが沸きにくい)があるため修正した方がよい。[エアコン製造事業者]
5		作業手順や各手順の関係性に関する補足説明の追加	● 「2.リスクアセスメント」の「(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」を整理する際には、「1.リスクアセスメント、リスク対応に向けた事前準備」の「(5) 目標とするリスクの水準」に整理結果を適宜フィードバックすることが望ましい。IoT-SSF では定量的な基準がないため、随時フィードバックを行いつつ、かかる水準や重要度の一覧を具体化することがよい。[エアコン製造事業者] ● 情報相関図のようなものがあるとよい。[エアコン製造事業者] ● 「機器毎に洗い出した脅威」毎に、「ヒト・ソシキ」と「システム」に対して、どういう対策要件があるかを洗い出すべき。脅威が「全般」に丸められており、具体

			的に１つ１つの脅威に対して何をやるかが不明確になってしまってしまう。[エアコン製造事業者]
6	その他	ワークシートの充実化	● スペースの都合上制約があるため、パワーポイント版のワークシートだけではなくエクセル版のワークシートがあるとよい。[エアコン製造事業者]

4. 適用実証を踏まえた改訂方針

(1) IoT-SSF の適用実証にて得られた問題・課題

「3.参画各社より頂戴した主なご意見」のうち、「適用の際の問題点/悩んだ点(他の文献とのハレーションを含む)」及び「IoT-SSF 等の改訂に向けた要望」より、IoT-SSF の適用実証にて得られた問題・課題を整理した。かかる問題・課題は大きく２つに分けた上で、以下に示す。

- 文書の改訂を要する問題・課題
- 文書の改訂は必要としないが、引き続き検討が必要な課題・問題

● 文書の改訂を要する問題・課題

No	修正対象	問題・課題
1	IoT-SSF	IoT-SSF において、安全分野(けがの分野)、セキュリティ分野との関係性が不明確。
2		第 3 軸の第 3 の観点及び第 4 の観点について、具体的な内容が IoT-SSF やユースケース集に示されていなかったため、何を記載すればよいかわからなかった。
3	IoT-SSF の適用手順書	「適用主体」の定義がわからない。
4		マルチステークホルダーで展開しているサービスを対象とした場合、誰がとりまとめるべきであるかわからない。
5		複数社で責任分界点を明確にするためには、ステークホルダー関連図とシステム構成図、データフロー図を作成する際にステークホルダー間で共通認識を作る必要がある。(適用手順書にて強調すべき)
6		リスクアセスメントを行う際の記載粒度(整理する情報の粒度やセキュリティの強度、サービス範囲)で悩んだ。
7		データフロー図は必ずしもシーケンシャルなデータフローとならないケースもあり得るため、表現方法で悩んだ。
8		リスクアセスメント「(2) 機器・システムの重要度の判断基準及び判断された重要度の一覧」を整理する際には、「事前準備」の「(5) 目標とするリスクの水準」と調整しながら作業を進める必要があった。
9		リスク対応「(2)脅威への対策の整理」について、各脅威に対して対策を洗い出すべきであるが、適用手順書では明確に記載されていない。
10		各ステップにおけるインプット及びアウトプット結果の関連性がわからない。
11	その他	パワーポイント版のワークシートはスペース上の制約があり、作業を円滑に進めにくい。

● **文書の改訂は必要としないが、引き続き検討が必要な課題・問題**

No	問題・課題
1	適用に大きな工数がかかる。(特に、ユースケースで扱う脅威の選定及び脅威への対策の選定に工数がかかった。)
2	類似事例がない場合、セキュリティの知識を持たない企業では IoT-SSF の適用が難しい。
3	どこまでの粒度で情報を整理すれば IoT-SSF の適用したことになるのか判断できない。
4	リスクの重要度を測る際一般的には「起こりやすさ」を考慮する一方で、IoT-SSF では考慮していない。

(2) IoT-SSF 等の改訂方針

「(1)IoT-SSF の適用実証にて得られた問題・課題」の「文書の改訂を要する問題・課題」から IoT-SSF 等の改訂方針を整理した。修正対象及び改訂方針を以下に示す。

● **修正対象及び改訂方針**

No	修正対象	改訂方針
1	IoT-SSF	「3.本フレームワークの基本構成」に、IoT-SSF で参照しているリスクマネジメントの国際規格 ISO 31000 とセーフティの基本概念を明確化した国際規格である ISO/IEC Guide 51 の関係性を追記する。
2		「3-3 求められるセキュリティ・セーフティ要求の整理」において、第 3 軸の第 3 の観点(例:全ての能力を 1 人が備えている必要はなく、事業部として能力を具備することが重要となる旨の追記)及び第 4 の観点(例:物理的被害を補償範囲に含んだ保険の利用やサイバーセキュリティお助け隊サービスの利用が考えられる旨の追記)に補足説明を行う。
3	IoT-SSF の適用手順書	「1.本手順書の概要」に適用主体の定義を追記する。また、ステップにおけるインプット及びアウトプット結果の関係性を追記する。
4		「2-1 リスクアセスメント、リスク対応に向けた事前準備」に、マルチステークホルダーで展開しているサービスを対象とした場合、とりまとめる主体について明記する。その際には関連するステークホルダーと共通認識を得ることが望ましい旨を追記する。また、更にデータフロー図の記載方法やシステム構成図やデータフロー図等の記載粒度を明確化した上で、適用手順書に追記する。
5		「2-2 リスクアセスメント」に、リスクアセスメント「(2) 機器・システムの重要度の判断基準及び判断された重要度の一覧」を整理する際には、「1.リスクアセスメント、リスク対応に向けた事前準備」の「(5) 目標とするリスクの水準」と調整しながら作業を進める必要がある旨を追記する。
6		「2-3 リスク対応」に、各脅威に対して対策の特定が必要である旨を追記する。
7	その他	パワーポイント版のワークシートに加えて、エクセル版のワークシートを準備する。