経済産業省

資料３

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

令和5年2月17日

経済産業省 商務情報政策局
サイバーセキュリティ課

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

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

4. 本タスクフォースに係る検討の状況

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

- **7つの産業分野別サブワーキンググループ(SWG)**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 分野横断の共通課題を検討するために、3つの**タスクフォース（TF）を設置**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
(分野ごとに検討するためのSWGを設置)

- **ビルSWG**
  - ガイドライン(空調sys)の策定(2022.10)
- **電力SWG**
  - 小売電気事業者ガイドライン策定(2021.2)
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドライン1.0版を公表(2020.12)
- **スマートホームSWG**
  - ガイドライン1.0版を公表(2021.4)
- **宇宙産業SWG**
  - ガイドライン1.0を公開(2022.7)
- **工場SWG**
  - ガイドライン1.0を公開(2022.11)
- ・・・

分野横断SWG

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

検討事項：
「協調的なデータ利活用に向けたデータマネジメント・フレームワーク～データによる価値創造の信頼性確保に向けた新たなアプローチ」を公開。

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

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

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

検討事項：
「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」及び「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」を公開。

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

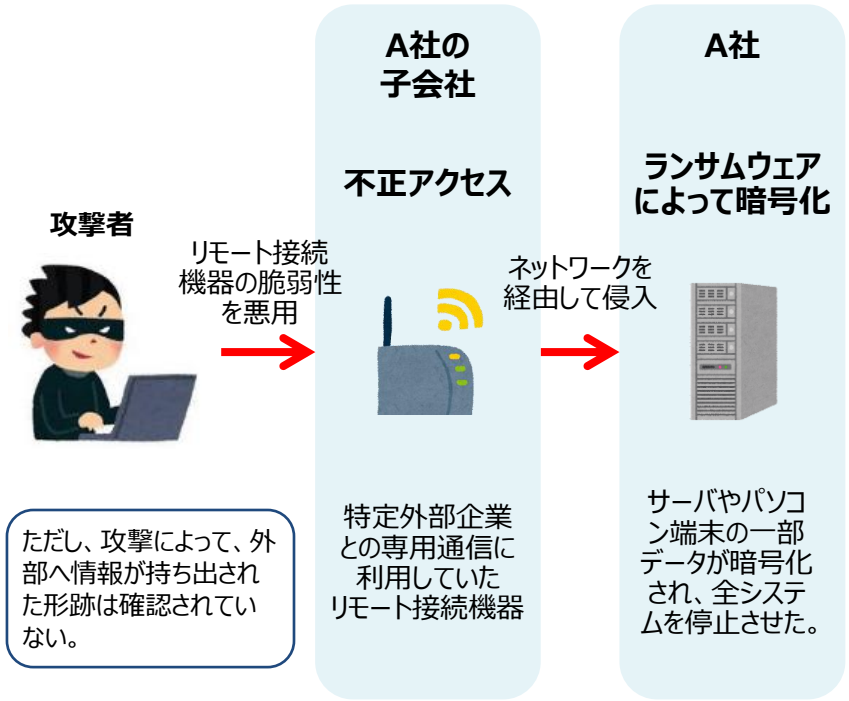
3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に向けた諸外国の検討状況

4. 本タスクフォースに係る検討の状況

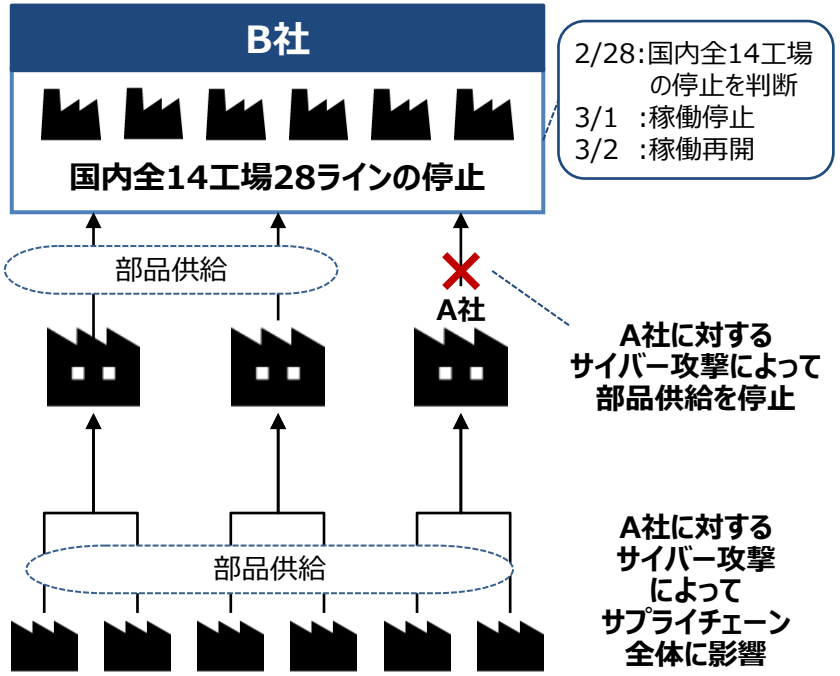
自動車部品メーカーに対するランサムウェア攻撃事案

- 2022年2月、B社に自動車部品を納入しているA社は、子会社のネットワークを経由して不正アクセスを受けたことで、サーバやパソコン端末の一部データがランサムウェアによって暗号化され、被害拡大防止のために全システムを停止させた。
- A社へのサイバー攻撃によって、 2022年3月にB社は国内全14工場28ラインの停止を判断。

子会社を通じた不正アクセスの概要



サプライチェーン全体への波及

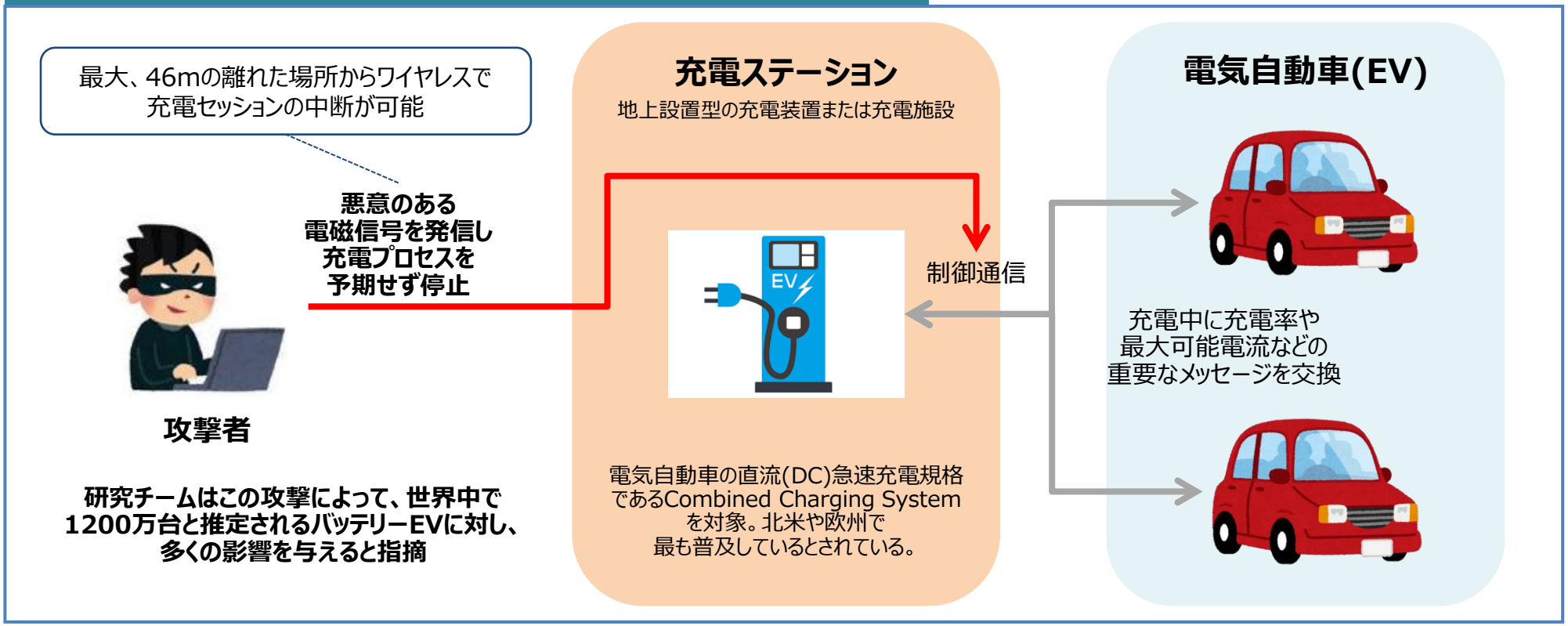


[参考] 各公開情報を基に作成

電気自動車の充電ステーションに対する攻撃

- 英国のオックスフォード大学等の研究チームは、電気自動車(EV)向けの充電ステーションに対する新しい攻撃手法を発表した。
- その攻撃は、車両と充電ステーションの間に行われる制御通信に干渉し、最大、46mの離れた場所からワイヤレスで充電セッションの中断が行えるものとされている。

攻撃者が充電ステーションの制御通信に攻撃するイメージ



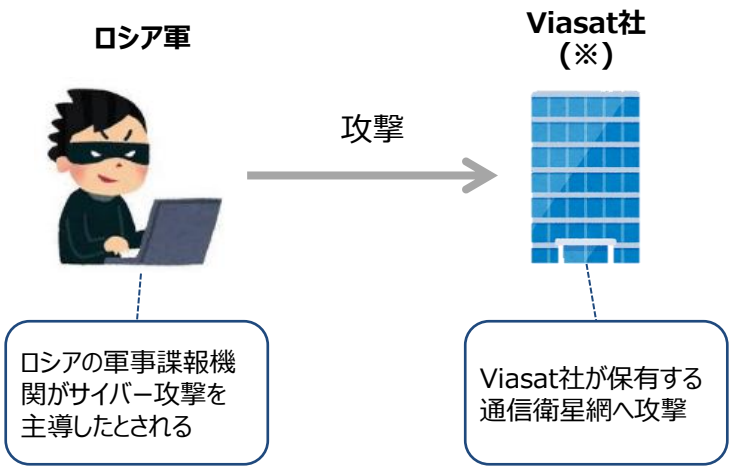
[参考] 各公開情報を基に作成

ウクライナ侵攻に伴う衛星通信等に対する攻撃

- 2022年4月、ロシアからとみられるサイバー攻撃によって、ウクライナおよび欧州で展開する衛星通信サービスが妨害されたとの報道がなされた。
- 影響を受けた機器はウクライナだけで数千台、その他ヨーロッパ地域を含めると数万台規模にわたるとされ、衛星通信が遮断されたことによって、発電施設を含む重要施設の稼働状況の監視に支障が出たとされている。

ロシアからのサイバー攻撃の疑惑

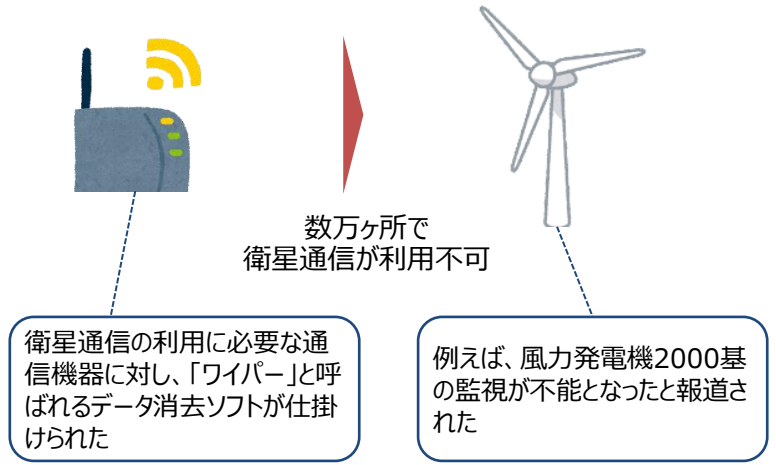
- ロシアの軍事諜報機関がサイバー攻撃を主導し、ロシア軍がウクライナおよび欧州で展開する衛星通信サービスを妨害したとされている。



※:高速衛星ブロードバンドサービスと、軍事および商業市場に対してネットワークシステムを提供する米国の通信会社

重要施設の稼働監視に影響

- 発電施設などの社会インフラや一般家庭など広い範囲で通信が断たれ、重要施設(例:風力発電所)の稼働状況の監視に支障が出たとされている。



[参考] 各公開情報を基に作成

ネットワークカメラに対する攻撃事例

- 中国のメーカー・Hikvisionが製造するネットワークカメラにおいて発見されたコマンドインジェクションの脆弱性(CVE-2021-36260)を悪用して、機器の認証情報(例:ID、パスワード)が漏えいした。
- 2022年7月、セキュリティ企業CYFIRMAは漏えいした認証情報がロシアのフォーラムで公表されていることを報告した。既に修正パッチは公開(2021年9月)されている一方で、修正パッチを未適用であり攻撃を受ける可能性があるカメラは全世界で8万台以上とされた。

ネットワークカメラへの攻撃イメージ

- 複数のネットワークカメラに対して、攻撃者はコマンドインジェクションの脆弱性を悪用し、**ネットワークカメラの認証情報(例:ID、パスワード)を不正に取得した**。

- **窃取されたHikvision製カメラの認証情報(例:ID、パスワード)がロシアのフォーラムで確認された。**
- 100カ国にわたる2300の組織で使用されている8万台以上のカメラがいまだに修正パッチを適用しておらず、脆弱性を突かれる可能性があることが明らかとなった。

[参考] 各公開情報を基に作成

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

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

4. 本タスクフォースに係る検討の状況

【欧州】NIS指令の改正

- 2023年1月、欧州においてNIS指令(指令(EU)2022/2555)(**NIS2**)が発効し、既存のNIS指令(指令(EU)2016/1148)に置き換えられた。加盟国は、指令の発効から21ヶ月以内に国内法に条項を組み込む必要が生じた。
- NIS2は、既存の指令から適用業種が大きく拡大しており、事業者に課すセキュリティ要件や罰則等においても規定が強化されている。

変更項目	現行NIS(2016年制定)の規定	主な改正事項
適用範囲	● **基幹サービス運営者** ①エネルギー(電力、石油、ガス)、②輸送、③銀行、④金融市場インフラ、⑤医療、⑥上水道、⑦デジタルインフラ ● **デジタルサービス提供者** ①オンラインマーケット、②オンライン検索エンジン、③クラウドコンピューティングサービス	● 基幹サービス運営者・デジタルサービス提供者という分類を、重大エンティティ(essential entity)と重要エンティティ(important entity)に変更。 ● 重大エンティティは、基幹サービス運営者７分野に**「下水道」、「行政」、「宇宙」の３分野を追加**した10分野。 ● 重要エンティティには、デジタルサービス提供者以外に、「郵便・配送」、「廃棄物処理」、「化学品」、「食品」、**「製造(医療機器、コンピューター及び電気電子製品、電気設備、機械設備、自動車、その他の輸送機器)」が追加。**
適用範囲の事業者に関連する規律	● 適用範囲の事業者が適切かつ均衡の取れた技術的及び組織的措置を講じる。 ● サービスの継続性に重大な影響を及ぼすインシデントの、管轄官庁又はCSIRTへの届出。	● 重点的な対策（サイバーセキュリティテスト、暗号化の利用等）をリストアップし、**セキュリティ要件を強化。** ● **ICTサプライチェーンにおけるセキュリティへの対応を明記。** ● インシデント報告に関して、**プロセス、内容、およびタイムラインに関するより正確な規定を設定。**
罰則	● 罰則を設けることのみ規定。	● **罰則の程度を指定**（1000万ユーロまたは全世界の年間売上高の2%を上限とする罰金）。

EUサイバーレジリエンス法(草案)の公開

- 9月16日、欧州委員会はデジタル要素を含む製品を対象としたサイバーセキュリティ規則を定めるEUサイバーレジリエンス法(草案)を提出した。2023年後半の発効、2025年後半適用を目指す。
- 対象機器のセキュリティ必須要求や製造業者への義務、かかる規定に関する罰則等が定められた。

対象機器

- 機器またはネットワークへの直接的または間接的な論理的または物理的なデータ接続を含む**デジタル要素を備えた製品が対象**となる。(2条)
- ただし、医療機器規則、体外診断用医療機器規則、民間航空機規則、自動車の型式承認規則の対象製品や国家安全保障に関するデジタル製品や軍事目的・機密情報処理目的のものは適用除外とする。(2条)　また、SaaSのようなソフトウェアサービスや研究開発目的のOSS等は対象外とする。(前文9、10)

セキュリティ必須要求及び製造業者が満たすべき要求

[各要件は次頁に記載]

- 本法適用対象の機器は、附属書Ⅰの第1節に規定される**セキュリティ必須要求**を満たしていることが求められる。(第5条、第10条、附属書Ⅰ)

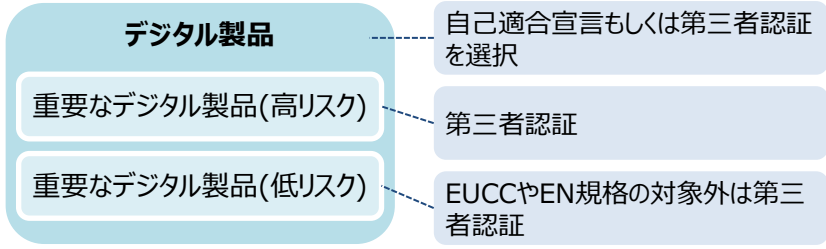
  ＜セキュリティ必須要求の例＞
  リスクに基づいて適切な**サイバーセキュリティを確保するよう設計・開発・生産されている**こと/**リスクベースアセスメントに基づいて**適切な状態になっていること 等
- 製造業者が実施するプロセスは、附属書Ⅰの第2節に規定される**脆弱性処理要求**を満たしていることが求められる。(第5条、第10条、附属書Ⅰ)

  ＜脆弱性処理要求の例＞
  製品に含まれる脆弱性とコンポーネントを特定し、文書化すること。そのために、一般的に使用される機械読み取り可能な形式により**SBOMの作成を行うこと/セキュリティパッチや更新プログラムが遅滞なく無料で配布され、ユーザーへの助言メッセージも添付**すること

製造業者の義務/報告義務

[義務の内容は次々頁に記載]

- 使用環境等のリスクレベルごとに**適合性評価が求められる**(図参照)。重要なデジタル製品は附属書Ⅲ(高リスクの例:公開鍵インフラ、低リスクの例:パスワードマネージャー)にて規定される。(10条)
- 積極的に悪用された脆弱性を発見した場合やインシデントを認識してから**24時間以内にENISAへ通知**することが求められた。また、是正措置についても**遅滞ないユーザへの通知**が必要となる。(11条)



罰則

セキュリティ必須要求等や10条、11条に規定された義務を遵守しない場合、罰金として最高1,500万ユーロまたは前年度の年間総売上の2.5%の高い方を適用する。

[出典] European Commission" Cyber Resilience Act"

参考　セキュリティ必須要求及び製造業者が満たすべき要求

セキュリティ必須要求(附属書Ⅰの第1節)

1. リスクに基づいて適切なサイバーセキュリティを確保するよう設計・開発・生産されていること。
2. 悪用可能な脆弱性が含まれないこと。
3. リスクベースアセスメントに基づいて、以下を満たすこと。
   a. 製品を元の状態にリセット可能である等、安全な構成となっていること。
   b. 適切な制御メカニズムにより不正アクセスからの保護が確保されていること。
   c. 最先端の暗号化などにより個人データ・その他のデータの機密性を保護すること。
   d. データやプログラムなどの完全性を許可されていない操作から保護し、破損についても報告すること。
   e. 必要なデータに限定して処理を行うこと。(データの最小化)
   f. DoS攻撃からの回復・緩和などの重要な可用性の機能を保護すること。
   g. 他の機器やネットワークからのサービスの可用性について自身への悪影響を最小化すること。
   h. 外部インターフェース等の攻撃対象領域を制限して設計・開発・製造されていること。
   i. インシデントの影響を軽減するように設計・開発・製造されていること。
   j. アクセス、データ修正、サービス、機能などの内部活動を記録・監視し、セキュリティ情報を提供すること。
   k. 自動更新やユーザへのアップデート通知などによりセキュリティアップデートによる脆弱性対応を確実に行えること。

脆弱性処理要求(附属書Ⅰの第2節)

1. 製品に含まれる脆弱性とコンポーネントを特定し、文書化すること。そのために、一般的に使用される機械読み取り可能な形式によりSBOM作成(少なくとも最上位レベルの依存関係含む)を行うこと。
2. セキュリティアップデートの提供など、遅滞なく脆弱性に対処・緩和すること。
3. 効果的かつ定期的なテストとレビューを行うこと。
4. 脆弱性情報の公開及び修正を行うこと。
5. 脆弱性開示ポリシーを導入し、実施すること。
6. 製品やサードパーティコンポーネントの潜在的な脆弱性に関する情報共有を行い、連絡先を提供すること。
7. 悪用可能な脆弱性が適時に修正・緩和されるように安全にアップデートを配布するメカニズムを提供すること。
8. セキュリティパッチや更新プログラムが遅滞なく無料で配布され、ユーザーへの助言メッセージも添付すること。

[出典] European Commission" Cyber Resilience Act"

参考　製造業者の義務/報告義務

製造業者の義務(10条)

1. デジタル製品を市場に出す際、**附属書Iの１「セキュリティ必須要求」**を遵守して設計・開発・製造されていることを確認する。
2. サイバーセキュリティ上の**リスクアセスメントを実施**し、その結果を設計・開発・製造・配送・メンテナンスの際の考慮に入れる。
3. デジタル製品を市場に出する際、上記のリスクアセスメントの結果を技術文書に含める。
4. 第三者から提供された部品を使用する際には、その部品により製品のセキュリティリスクを高めないことを保証する。
5. リスクに比例した方法でデジタル製品に関するサイバーセキュリティ側面を体系的に文書化する。
6. 上市後5年間または製品寿命のうち短い期間の間、**脆弱性に効果的に対処**する。製造業者は脆弱性開示ポリシー等、適切なポリシーや手続きを有する。
7. 上市前に製造業者は**技術文書を作成**する。対応する適合性評価手続きを行い、適合性が実証された場合は**CEマーキングを貼付**する。
8. **上市後10年間**、**技術文書と(該当する場合は)EU適合性証明書**を市場監視当局が自由に使えるように**保管**する。
9. 一連の製造の中で、適合性を維持するための手順が整備されていることを確認する。
10. 附属書IIに規定される情報が製品に付属されていることを確認する。
11. EU適合性証明書を提供するか、その情報を記載したURLを提供する。
12. **上市後5年間**または製品寿命のうち短い期間の間、附属書Iの1節**「セキュリティ必須要求」を遵守しない場合、直ちに必要な是正措置を講じ、製品の撤回またはリコール**を行う。
13. **市場監視当局からの要求**に応じて製品の**適合性を証明する情報・文書を提出**する。
14. 操業を停止し義務を遵守できなくなる場合、操業停止前に市場監視当局やユーザに通知する。
15. **欧州委員会は実施法の中で、SBOMの形式と要素を指定することができる。**

製造業者の報告義務(11条)

1. デジタル製品の中に**積極的に悪用された脆弱性を発見してから24時間以内にENISAに通知**する。通知には、その脆弱性の情報、講じられた是正措置・緩和措置を含む。(ENISAは正当なサイバーセキュリティリスク等の事由が無い限り、NIS2指令に基づいて遅滞なく脆弱性開示目的で指定されているCSIRTに転送し、市場監視当局にも通知する。)
2. 製品のセキュリティに影響を与える**インシデントを認識してから24時間以内にENISAに通知する**。インシデント通知には、インシデントの深刻度・影響、国境を越える影響があるか等を含む。(ENISAは、正当なサイバーセキュリティリスク等の事由が無い限り、NIS2指令に基づいて指定されたコンタクト先に通知を転送し、市場監視当局にも通知する。
3. 運用レベルでの大規模なインシデントや危機管理に関する場合、ENISAはその情報をNIS2指令に基づいて設立されたEU CyCLONe(欧州サイバー危機連絡組織ネットワーク)に提出する。
4. 製造業者は、**必要に応じてインシデントの影響を緩和するための是正措置について遅滞なくユーザに通知する**。
5. 欧州委員会は、通知された情報の種類、形式、手順を更に指定することができる。
6. ENISAはNIS2指令の協力グループに対して、サイバーセキュリティに関する最新の傾向を技術レポートとして2年に1度提出する。
7. 製造業者が製品に統合されているOSSコンポーネントの脆弱性を特定した場合、その脆弱性をコンポーネントを維持する個人/団体に報告する。

[出典] European Commission" Cyber Resilience Act"

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

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

4. 本タスクフォースに係る検討の状況

昨年度の振り返り

第6回第2層TF頂戴した今後の取組に関する主なご意見

- 第6回第2層TFでは、IoT-SSFに関する取組及び今後のIoTセキュリティ対策全般に係る取組に関するご意見を頂戴した。

IoT-SSFに関する取組へのご意見	**IoT-SSF等の普及啓発**	◆ 各団体が作成した**ユースケースが蓄積することで、様々な分野でIoT-SSFの活用が可能となる**と考えられる。 ◆ **第3軸の第3の観点及び第4の観点をより具体化**できるとよい。 ◆ IoT-SSFのようなまとめ方をしている文書は国際的に見ても類を見ない。IoT-SSFの様な文書の作成が、将来的な課題の提起、提案へつながるとよい。
	自立的な活用に向けた検討	◆ ユースケースを普及させるための**民間事業者に対するインセンティブ**があるとよい。 ◆ 事業者に対して、**IoT-SSFに取り組む必要性を意識させることができる**とよい。例えば、IoT-SSFをガイドラインに位置付けることが考えられる。 ◆ IoT-SSFを適用する際、評価に主観的な差が生まれる可能性があるため、**ガイドラインのためのガイドライン**があるとよい。
上記以外のIoTセキュリティに全体に関する取組へのご意見		◆ WG2やWG3と連携しつつ、**講じるべきセーフティネットの具体化(例:保険制度の構築)に向けた検討を行う**ことができればよい。 ◆ IoTに限らず**セキュリティ対策の実施に際しては、どの程度まで実施するかを検討することが重要**である。実施範囲を示さない限り、ユーザはセキュリティ対策の重要性を理解していても対策を講じることができない可能性がある。 ◆ 今後ますます高度なサイバーシステムが社会や企業に導入されていく中で、複雑で高度なシステムを導入する際のセキュリティは簡単に実装できない可能性がある。したがって、例えば、**IoTセキュリティ対策を行うために必要な素養、要件を整理する必要がある**のではないか。

今年度の取組状況

- 昨年度に整理した今後の課題を踏まえて、今年度の取組内容を整理した。

昨年度に整理した今後の課題

IoT-SSF及びユースケースの普及啓発

- 経産省主催の研修会の開催、その他既存の枠組みの活用
- 当TFに関係する企業・団体における活用
- その他関係機関の巻き込み

自立的な活用に向けた検討

- IoT-SSF、ユースケースを活用したビジネス化の促進
- 支援機関への落とし込み
- IoT-SSF及びユースケースを使いこなせる人材の育成
- インセンティブの制度検討

今年度の取組

1. IoT-SSFの適用実証
2. IoT-SSF第3軸(第3の観点及び第4の観点)の具体化
3. IoT-SSFの有効性検証
4. CPSF等の利活用状況に関するアンケート調査
5. 各種セミナー等でのIoT-SSFの紹介

①～④の結果に鑑みて、今後検討する可能性がある

①IoT-SSFの適用実証

- 今後の更なる適用拡大に際して参考となる事例を蓄積するとともに、適用を通じてIoT-SSFの改善点を洗い出すことを目的として、IoT-SSFの適用実証を行った。

適用実証の概要

- 参画事業者に対象システム/サービスを選定いただき、事務局も支援しつつIoT-SSFを適用し、今後の改善等に向けた課題の整理を行う。

1 対象システム/サービスの選定 → 2 IoT-SSFの適用 → 3 課題等の整理

- 4件の適用実証を実施。別途、医療機器業界でIoT-SSFを適用する際の事前検討を実施。

No	利用者の区分	業界	名称	参画事業者
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
2			家庭用エアコン操作	エアコン製造事業者
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)
4			設備保全業務支援サービス	設備保全サービス事業者
参考		医療	医療機器(例：心電計、生体情報モニタ)	日本光電

想定する成果物

① ユースケース

- 対象システム/サービス
- 取扱うデータの種類とデータフロー
- 想定されるリスクと対応策

② IoT-SSF改善のためのデータ

- 適用作業に要した期間・工数(人月)
- 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改訂に向けた要望
- 効果的と考えられるIoT-SSFの活用場面等

IoT-SSF適用実証の実施概要 ユースケース一覧表

- 参考となる事例の蓄積によるIoT-SSFの活用促進、IoT-SSFの改善点の洗い出しを目的として、参画事業者からの協力をいただきつつ、適用実証を実施。

#	利用者の区分	業界	名称	参画事業者	対象システム/ソリューション
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、サブスクリプション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	エアコン製造事業者が提供している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架空の事業場において、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。
4			設備保全業務支援サービス	設備保全サービス事業者	受変電・電気設備等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。
参考		医療	医療機器(例：心電計、生体情報モニタ)	日本光電	心電計、生体情報モニタ等の医療機器を対象とする。かかる医療機器の開発おけるIoT-SSFの適用可能性を検討するとともに、適用にあたって生じ得る課題を洗い出す。

「ユースケースにおける記載事項」の概要

- CPSFでは、「分析対象の明確化」、「想定されるセキュリティインシデント及び事業被害レベルの設定」、「リスク分析の実施」及び「リスク対応」のステップでリスクマネジメントを実施するとしている。
- 上記を踏まえ、以下のステップでリスクマネジメントを実施し、個別のユースケースを整理した。

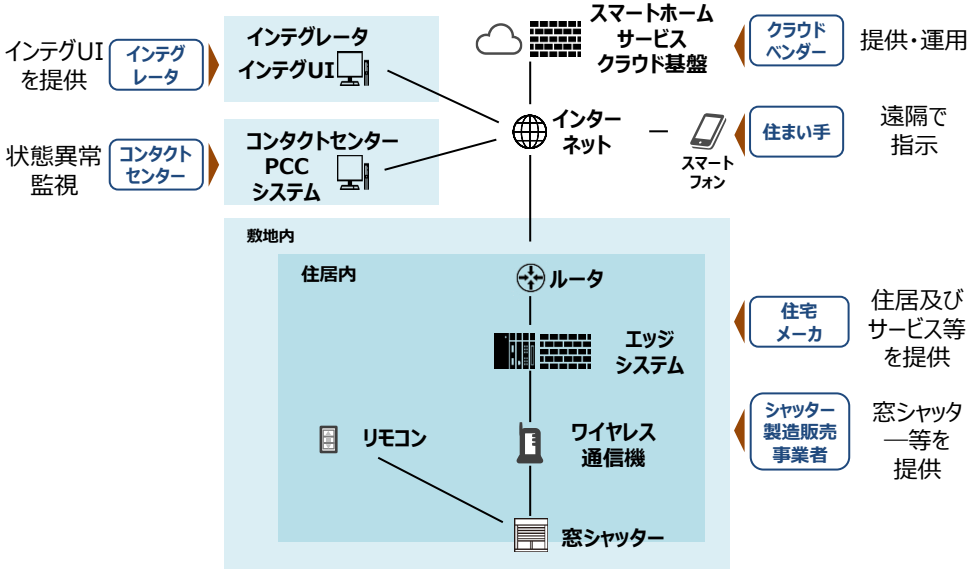
1 リスクアセスメント、リスク対応に向けた事前準備	2 リスクアセスメント	3 リスク対応
●事前準備として必要となる以下の情報を整理する。 ✓ 対象ソリューションの概要 ✓ ステークホルダー関係図 ✓ システムを構成する機器の一覧 ✓ システム構成図、データフロー図 ✓ リスク基準	●第1軸「回復困難性の度合い」及び第2軸「経済的影響の度合い」の判断基準を考慮し、IoT機器・システムをマッピングする。 ✓ 想定されるセキュリティインシデント等とその結果の特定 ✓ 機器・システムの重要度の判断基準及び判断された重要度の一覧 ✓ マッピング結果の整理と評価の実施	●リスク対応を行うステークホルダーが実際に講じる対策を以下の項目に沿って整理する。 ✓ システムを構成する機器ごとの脅威の整理 ✓ 脅威に対する対策の整理 ✓ 整理した対策に対する意思決定

1. スマートホームサービス窓シャッター連携

- 住宅メーカが提供している住宅の住まい手向けに提供しているスマートホームサービスや連携する窓シャッターが対象。

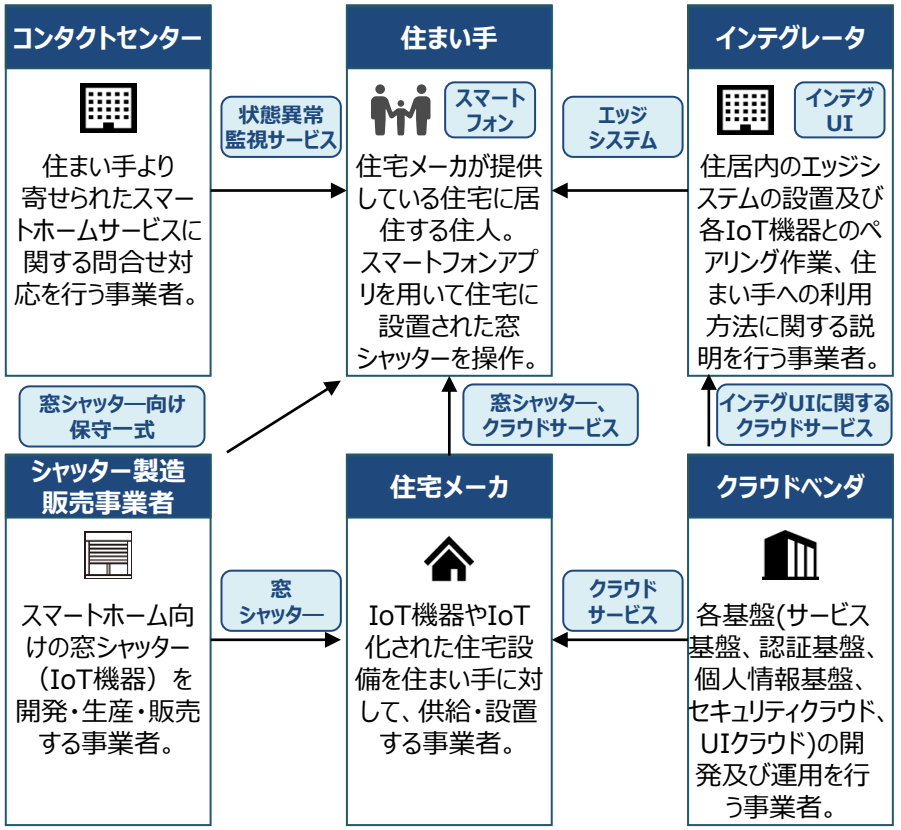
✓ 対象機器・システムの概要

- 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。



※シャッター自体は軽量で、駆動する動力も弱い

✓ 適用主体及び他のステークホルダーの情報



1. スマートホームサービス窓シャッター連携

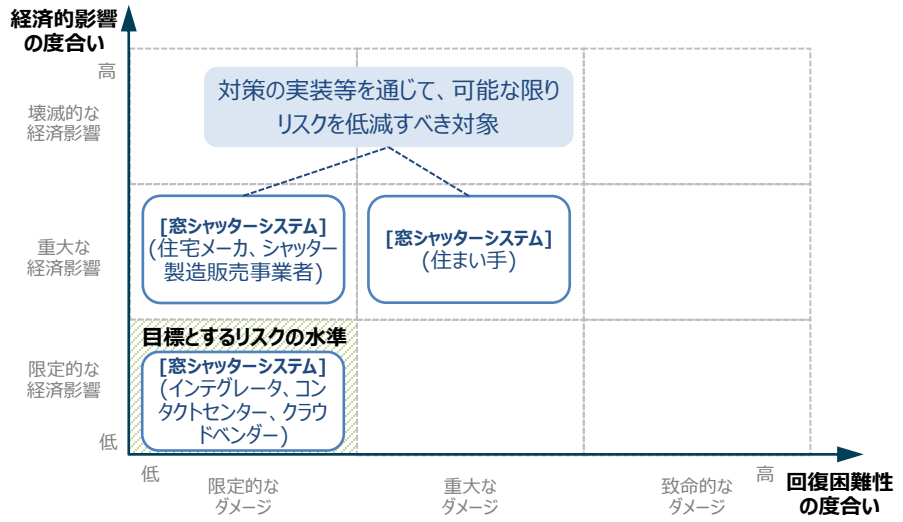
- 窓シャッターの誤動作等により、「住まい手」にとって「空き巣の侵入」や「けが」につながり得る機器・システムについて、リスクの低減に努める必要。

✓ 対象機器・システムにおいて想定されるリスク(例)

分類	想定されるリスク（例）
住まい手	• ネットワーク上で制御データが改ざんされることによって、シャッターが物・人をはさみ、**物の損傷や住まい手が負傷する可能性がある。** • 制御データがネットワーク上で盗聴されることによって、住居の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。**
住宅メーカ	• セキュリティインシデントが住まい手への影響が及ぶことによって、住宅メーカーは**原因調査・製品改修**が生じ得る。 • **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、ブランドカの低下**も起こり得る。
シャッター製造販売事業者	• セキュリティインシデントが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。 • **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、ブランドカの低下**も起こり得る。
インテグレータ、コンタクトセンター、クラウドベンダ	• サービスの品質や信用について懸念が広がるおそれがある。

✓ 想定されるリスク(例)のマッピング結果

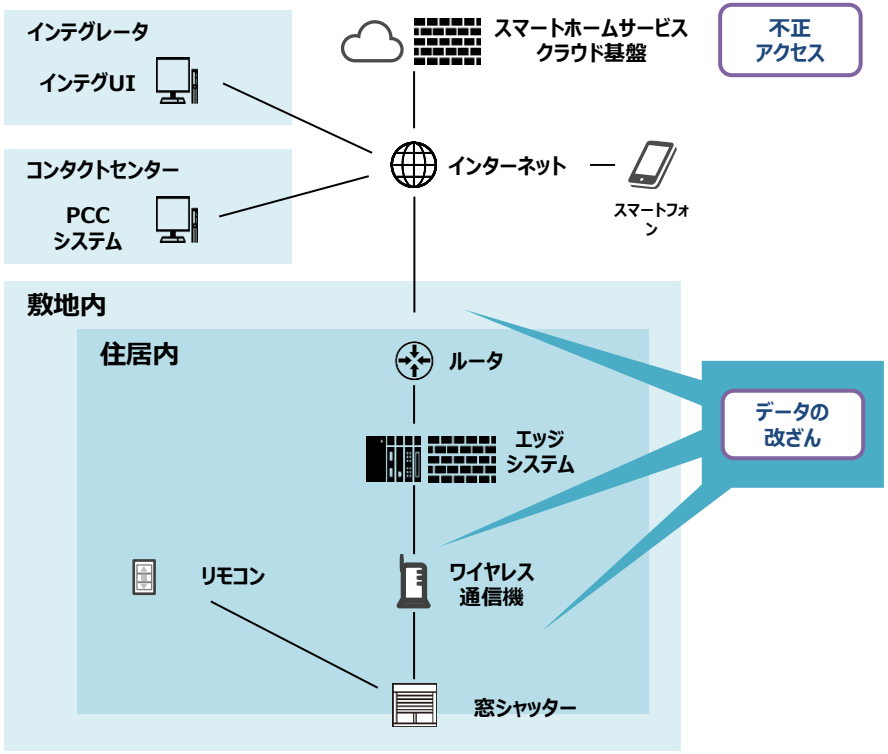
- インテグレータ、コンタクトセンター、クラウドベンダー視点からみたスマートホームサービスの窓シャッターシステムの保有するリスクは、目標とする水準内に収まっている。
- しかし、住まい手及び住宅メーカ、シャッター製造販売事業者視点のスマートホームサービスの窓シャッターシステムの保有するリスクは、目標とする水準には収まっておらず、何らかの対処実施が望まれる。



1. スマートホームサービス窓シャッター連携

✓ 影響度が大きいリスクにつながり得る脅威の例

- クラウドサービスに対する不正アクセスに加えて、クラウドサービスからエッジシステムへの制御データの改ざんやエッジシステム等から窓シャッターへの制御データの改ざんが、影響度が大きいリスクにつながり得る脅威の例と考えられる。



✓ 行うべきと考えられる対策の例

住まい手にとってのリスクを低減するため住宅メーカもしくはシャッター製造販売事業者、クラウドベンダが実施する対策(例)

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	• **【第1の観点】IoT機器・システムにおけるセキュリティポリシーの策定** [住宅メーカ] • **【第2の観点】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** [住宅メーカ/クラウドベンダ] • **【第2の観点】IoT機器・システムの適正な運用・保守** [住宅メーカ/クラウドベンダ] • **【第3の観点】IoT機器・システムの運用・管理を行う者(インテグレータ)に対する要求事項の遵守の確認** [住宅メーカ]
フェールセーフ等を含む安全対策の徹底	• **【第1の観点】セキュリティ設計と両立するセーフティ設計の仕様化** [シャッター製造販売事業者]

住宅メーカ、シャッター製造販売事業者にとってのリスクを低減するためシャッター製造事業者が実施する対策(例)

大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための取組みの推進	• **【第1の観点】運用前(設計・製造段階)における法令及び契約上の要求事項の遵守** [シャッター製造販売事業者] • **【第1の観点】IoT機器・システムの出荷時における安全な初期設定と構成** [シャッター製造販売事業者] • **【第1の観点】セキュリティ設計と両立するセーフティ設計の仕様化**(例:窓シャッタへ安全機能の実装)[シャッター製造販売事業者]

1. スマートホームサービス窓シャッター連携

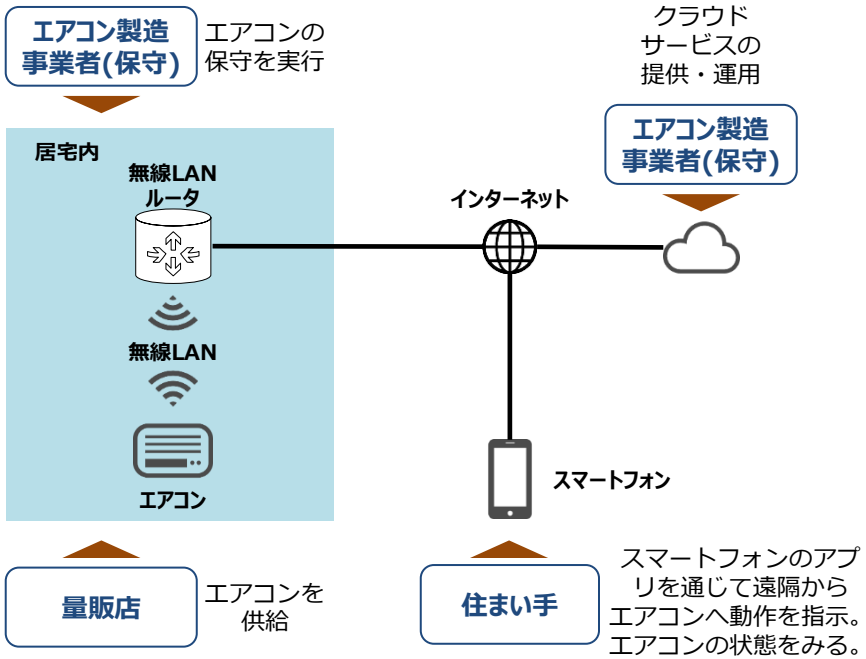
分類	主なご意見
適用した際に感じたメリット/デメリット	• サービスを提供する際にIoT-SSFを適用することで、システム構成やステークホルダーを明らかにすることができ、**関係者間で共通の認識を持ちつつ脅威を整理できる可能性がある**と感じた。 • 同じ業界や近い業界における類似事例があればよいが、類似事例がない場合、セキュリティの知識を持たない企業ではIoT-SSFの適用が難しい可能性がある。今回の様な取組み等を通じて事例を集めていくことが重要である。
適用して気付いた新たなリスク	• 「経済的影響の度合い」を考慮することによって、**今までのリスク分析では考慮できていなかったブランド価値への影響について考える機会を持てた**。**事業者としての経済的なリスクを明文化した点にIoT-SSFを作成した成果がある**と考えられる。
適用の際の問題点/悩んだ点	• 「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。 • **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**。例えば、CCDSの認証を取得する際に実施したレベルで、詳細にリスクアセスメントを行うと非常に時間をかかると想定される。 • セキュリティ対策を既に実施している企業における脅威の洗い出しをどのように記載すべきかも明記いただけるとよい。
IoT-SSF改訂に向けた要望	• **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。**例えば、サービスを提供する一社が複数の機器メーカ部分も含めて適用することは非常に手間がかかり非現実的である。適用に係る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。） • 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ため、工数を減らすための仕組みがあるとよい。
効果的と考えられるIoT-SSFの活用場面	• 受発注の際に、IoT-SSFを利用することは有効であると考えられる。ただし、各社ごとに記載粒度が異なる可能性があるため、統一の基準が必要となる。
作業工数	**合計　18人日** (以下、内訳) • 事前準備 **合計2.0人日**（住宅メーカ:0.7人日/シャッター製造販売事業者:1.3人日) • リスクアセスメント **合計7.8人日** (住宅メーカ:5.9人日/シャッター製造販売事業者:1.9人日) • リスク対応 **合計8.2人日**　(住宅メーカ:6.1人日/シャッター製造販売事業者:2.1人日)

2. 家庭用エアコン遠隔操作

● 本ユースケースは、エアコン製造事業者が提供しているエアコンを対象に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。既存のソリューションに対して網羅的に脅威を洗い出した上でリスク対応を行った。

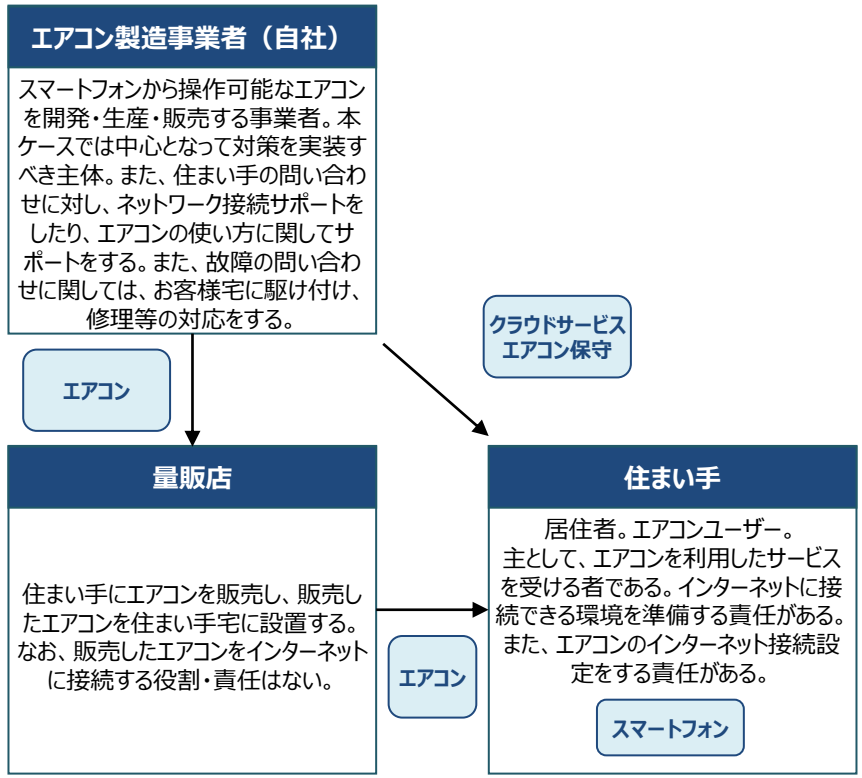
✓ 対象機器・システムの概要

- エアコン製造事業者が提供するエアコンを利用し、例えば住まい手は以下を行うことができる。
  - ✓ 帰宅時に遠隔でエアコンを操作し、リビングを快適な生活空間にする。
  - ✓ 就寝前にリビングから寝室のエアコンを遠隔操作することで、快適な睡眠空間をつくる。



※エアコンの調整可能な温度は上限・下限の制限がある

✓ 適用主体及び他のステークホルダーの情報



2. 家庭用エアコン遠隔操作

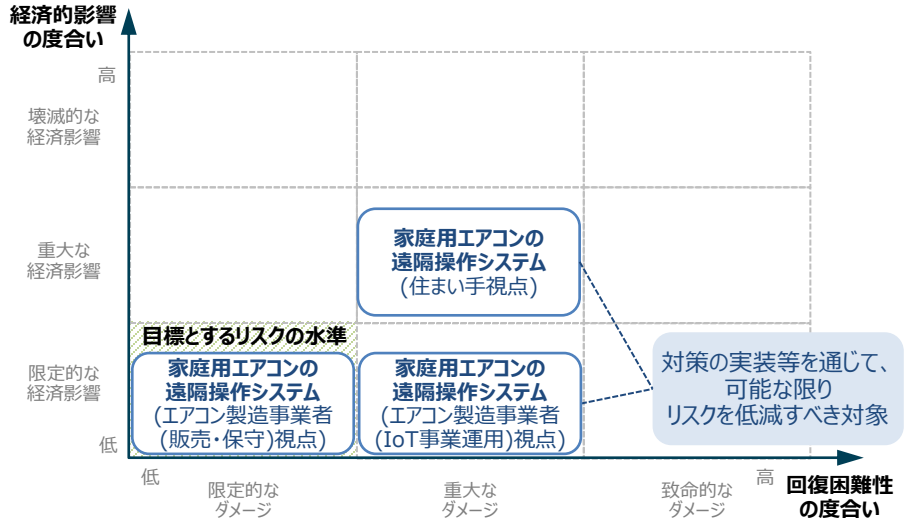
- エアコンの誤動作等により被り得る被害が大きくなり得ると想定される「住まい手」に対して、けが(例:熱失神、熱疲労)につながり得る機器・システムのセキュリティ上の欠陥等を減らすよう考慮して、リスクの低減に努める必要がある。

✓ 対象機器・システムにおいて想定されるリスク(例)

分類	想定されるリスク（例）
住まい手	• アカウントが乗っ取られ、ユーザーが意図しないコマンドがサーバに対して直接（悪意のあるユーザーから）実行され、機器が期待しない動作をする。その結果、**例えば夏季の就寝中に部屋が暖房で暖められ、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。
エアコン製造事業者(販売・保守)	• サーバ上の機器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、サービスマンが誤報により、**無駄な訪問をしていまい、本来修理が必要な顧客に対して提供できなくなる**。
エアコン製造事業者(IoT事業・運用)	• サーバ上の住まい手の個人情報が、漏洩する。その結果、**ブランドイメージが落ちる。サポートの品質について利用者に不安が広がる。** • 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。**

✓ 想定されるリスク(例)のマッピング結果

- エアコン製造事業者(販売・保守)視点からみた家庭用エアコンの遠隔操作システムの保有するリスクは、目標とする水準内に収まっている。
- しかし、住まい手及びエアコン製造事業者(IoT事業運用) 視点の家庭用エアコンの遠隔操作システムの保有するリスクは、目標とする水準には収まっておらず、何らかの対処実施が望まれる。

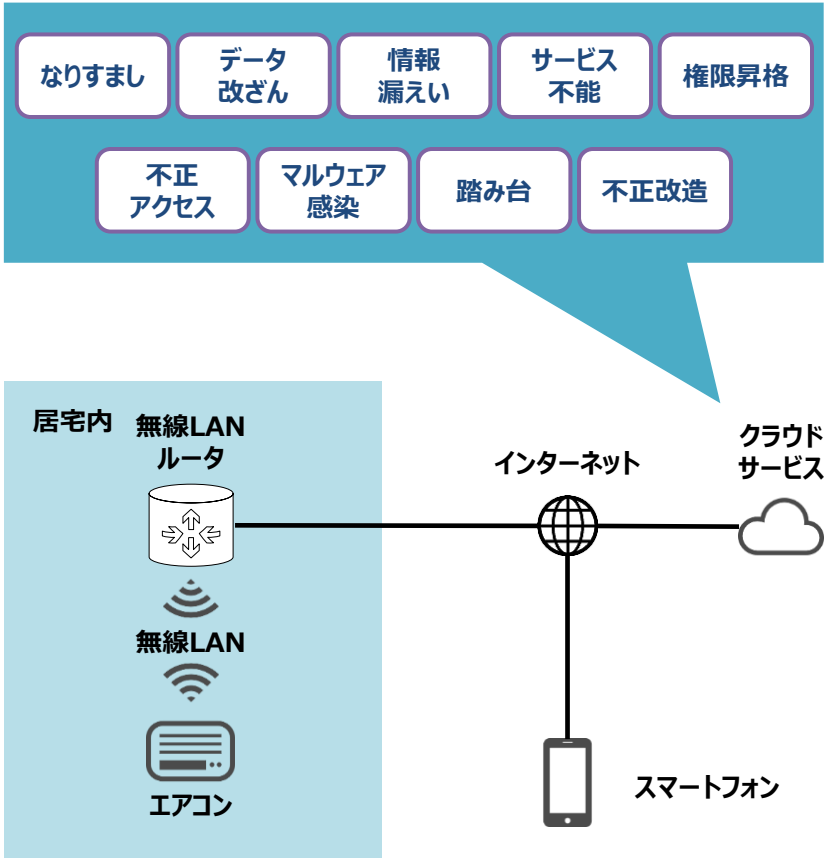


参考資料：製造業向け熱中症予防対策のためのリスクアセスメントマニュアル https://www.jisha.or.jp/research/pdf/201503_02_All_1.pdf

2. 家庭用エアコン遠隔操作

✓ 影響度が大きいリスクにつながり得る脅威の例

- 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。



✓ 行うべきと考えられる対策の例

エアコン製造事業者にとってのリスクを低減するため
エアコン製造事業者が実施する対策(例)

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	• **【第1の観点】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	• **【第1の観点】セキュリティ設計と両立するセーフティ設計の仕様化** • **【第3の観点】IoT機器・システムの運用・管理を行う者に対する要求事項の特定**

住まい手にとってのリスクを低減するため
エアコン製造事業者が家電量販店に対応を依頼する対策(例)

安全にエアコンを運用・管理するための仕組みの構築	• **【第1の観点】利用者へのリスクの周知等の情報発信**

住まい手にとってのリスクを低減するため
エアコン製造事業者が住まい手に対応を依頼する対策(例)

安全にエアコンを運用・管理するための仕組みの構築	• **【第3の観点】IoT機器・システムの運用・管理を行う者に対する要求事項の特定**

2. 家庭用エアコン遠隔操作

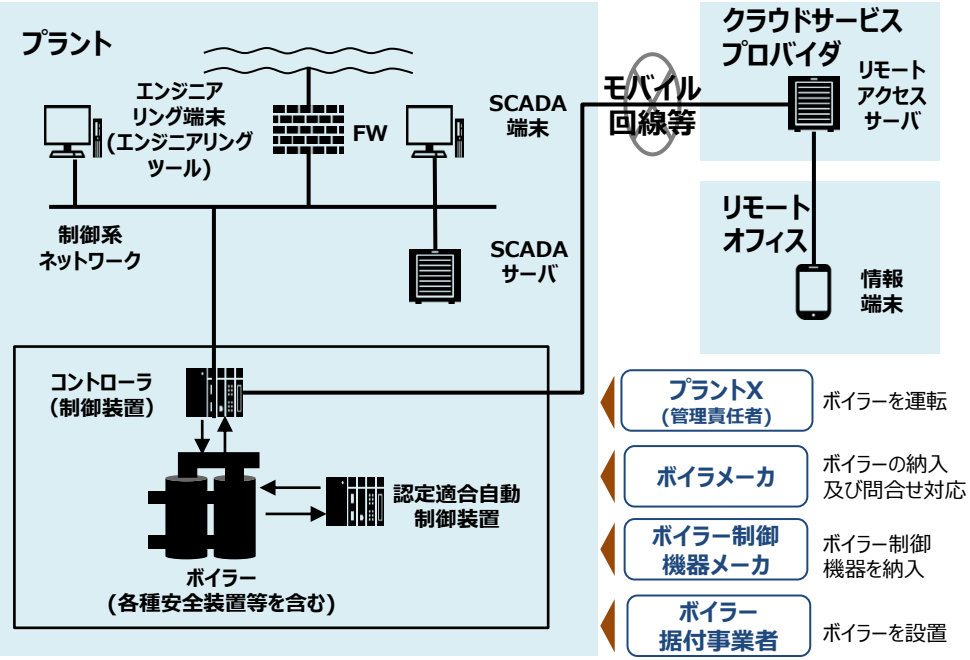
分類	主なご意見
適用した際に感じたメリット/デメリット	• 直接的なリスクではないが、既存のリスクアセスメントでは考慮していなかった販売店(コールセンター)の人員ひっ迫及びやエアコン製造事業者内での対応費用について考える機会を得た。
適用して気付いた新たなリスク	• 今まで考慮してこなかった量販店において想定されるリスクも考慮することができた。
適用の際の問題点/悩んだ点	• 「2.リスクアセスメント」の「(2) 機器・システムの重要度の判断基準及び判断された重要度の一覧」を整理する際には、「1.リスクアセスメント、リスク対応に向けた事前準備」の「(5) 目標とするリスクの水準」に整理結果を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。 • また第1軸「回復困難性の度合い」の概念は既存のリスクアセスメントの考え方とは異なるため、理解に時間を要する場合がある。例えば、通常は「影響の大きさ」と「起こりやすさ」の2軸からリスクアセスメントを実施する。「影響の大きさ」は「経済的影響の度合い」の大きさとして考えることができる一方で、「回復困難性の度合い」は馴染みがない。（定量的な尺度を組織、人にあわせて定義がないため、定性的な判断となってしまった。） • **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。**
IoT-SSF改訂に向けた要望	• **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。** • 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。また、情報相関図のようなものがあるとよい（各手順によって作成されるアウトプットが、次以降のどの手順で使用されるものかといった手順全体のデータフロー図が欲しい）。 • 「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。(1つ1つ実施できる手順にすべき) • 各工程を別々に作っていくのではなく全体のどの工程を実施しているのかが見えるような視認性のあるワークシートがよい。 • 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。
効果的と考えられるIoT-SSFの活用場面	• **直接的な回答にはなっていないかもしれないが、(メーカーとしては製品安全に対する経験は豊富であり、)双方の少し結びつきが弱いため、サイバーセキュリティと製品安全との関係性をより具体化できれば、活用が進むと考えられる。**
作業工数	**合計　3.2人日** (以下、内訳) • 事前準備 **合計1.2人日** • リスクアセスメント　**合計1.2人日** • リスク対応 **合計0.8人日**

3. ボイラーの遠隔監視

- 架空の事業者Xが自社プラントにおいて、ボイラーの遠隔監視の仕組みを導入することを想定する。新たに生じ得るサイバーセキュリティに関するリスクに対して、IoT-SSFを用いてリスクアセスメントを行い、セキュリティ対策を検討する。

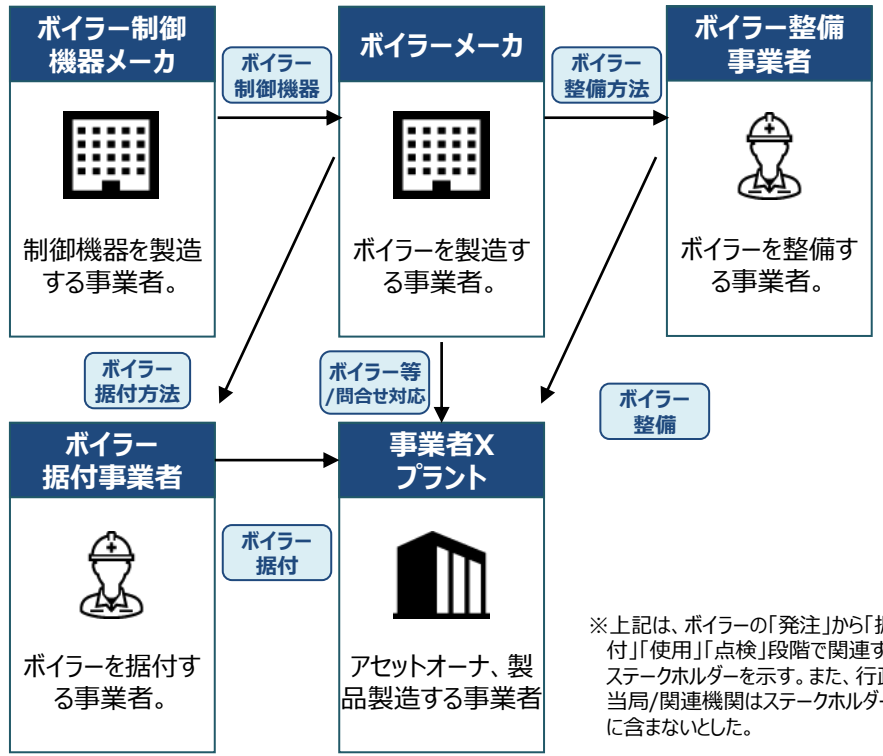
✓ 対象機器・システムの概要

- ボイラーは水管ボイラーを想定。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コントローラ(制御装置)を通じて、ボイラーの制御を行う。



※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

✓ 適用主体及び他のステークホルダーの情報



※上記は、ボイラーの「発注」から「据付」「使用」「点検」段階で関連するステークホルダーを示す。また、行政当局/関連機関はステークホルダーに含まないとした。

3. ボイラーの遠隔監視

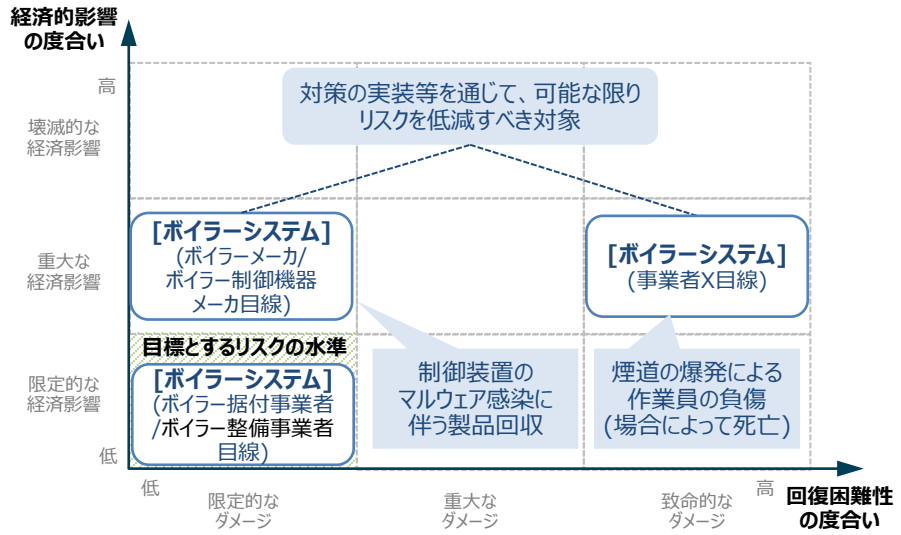
- 例えば、コントローラ(制御装置)にアクセスし、プログラムまたはパラメータ(空燃比制御等)が変更されることで、被害が大きくなり得ると想定される。「アセットオーナ」の作業員のけがにつながり得るリスクの低減に努める必要がある。

✓ 対象機器・システムにおいて想定されるリスク(例)

分類	想定されるリスク（例）
事業者X (アセットオーナ)	• 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(空燃比制御等)を変更する。その結果、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。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。** • 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、**作業者・管理責任者の個人情報等の情報が流出し得る。**
ボイラーメーカ (アセットメーカ)	• 制御装置の入れ替えに伴い、脆弱性を含むアップデートを行うことにより、同端末及び制御情報系ネットワーク内の他のサーバや端末がマルウェアに感染し、**製品回収が発生し得る**。 • アセットオーナーに対する注意喚起を怠ることで、**サービス提供における過失が認められ得る。**
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ことで、**大規模な製品回収が生じ得る。**
ボイラー据付事業者/ボイラー整備事業者	• 適切な手順でボイラーを据付(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ことで、過失が認められ得る。**

✓ 想定されるリスク(例)のマッピング結果

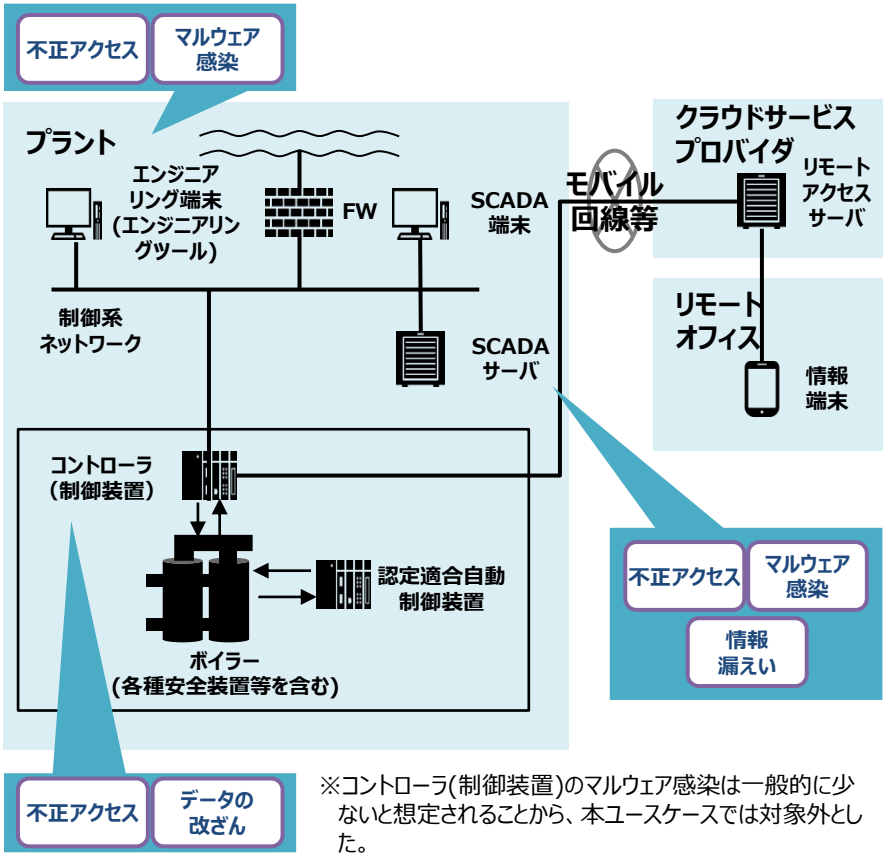
- ボイラー据付事業者/ボイラー整備事業者視点からみたボイラーシステムの保有するリスクは、目標とする水準内に収まっている。
- しかし、アセットオーナ及びボイラーメーカ、ボイラー制御機器メーカ視点のボイラーシステムの保有するリスクは、目標とする水準には収まっておらず、何らかの対処実施が望まれる。



3. ボイラーの遠隔監視

✓ 影響度が大きいリスクにつながり得る脅威の例

- 遠隔監視の仕組みを新たに導入することによって、エンジニアリング端末(エンジニアリングツール)、SCADAサーバ、コントローラ(制御装置)にて脅威が生じ得ると想定した。



※コントローラ(制御装置)のマルウェア感染は一般的に少ないと想定されることから、本ユースケースでは対象外とした。

✓ 行うべきと考えられる対策の例

事業者Xにおけるリスクを低減するため
事業者Xもしくはボイラーメーカが実施する対策(例)

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	• **【第1の観点】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**[ボイラーメーカ] • **【第2の観点】事故被害抑制マニュアルの作成**[事業者X] • **【第3の観点】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）**[事業者X] • **【第3の観点】ボイラーの制御機器の機能の検査の実施**[事業者X /ボイラーメーカ]
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	• **【第4の観点】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/ボイラーメーカ]

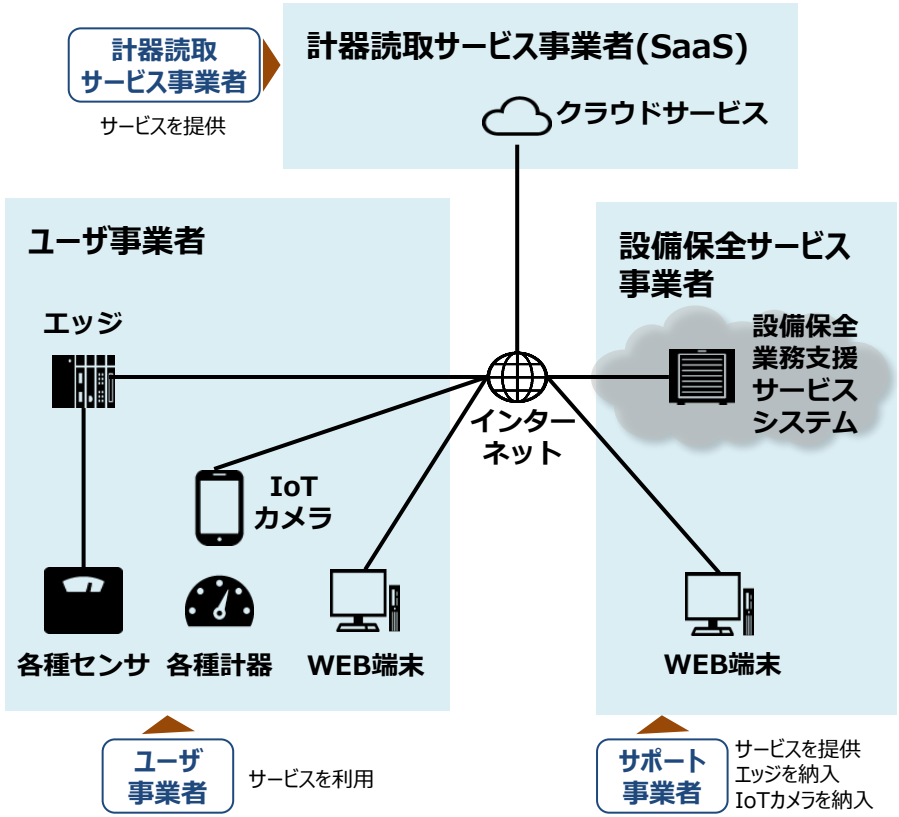
3. ボイラーの遠隔監視

分類	主なご意見
適用した際に感じたメリット/デメリット	• **製品安全分野における既存の規定に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**。
適用して気付いた新たなリスク	• 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)
適用の際の問題点/悩んだ点	• 第3の観点における対策を検討する際、ボイラー取扱作業主任者に対して求めるセキュリティの知識レベルで悩んだ。**ボイラー取扱作業主任者が持っているとされる知識を考慮しつつ、現実的なセキュリティ対策とするための調整に時間を要した**。 • 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。**
IoT-SSF改訂に向けた要望	• 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。
効果的と考えられるIoT-SSFの活用場面	• IoT化に伴い、製品安全分野においてもセキュリティリスクアセスメントが必要となる場合にIoT-SSFを活用することが可能な場合がある。
作業工数	**合計　7.0人日** (以下、内訳) • 事前準備 **合計1.75人日** • リスクアセスメント　**合計2.0人日** • リスク対応 **合計3.25人日**

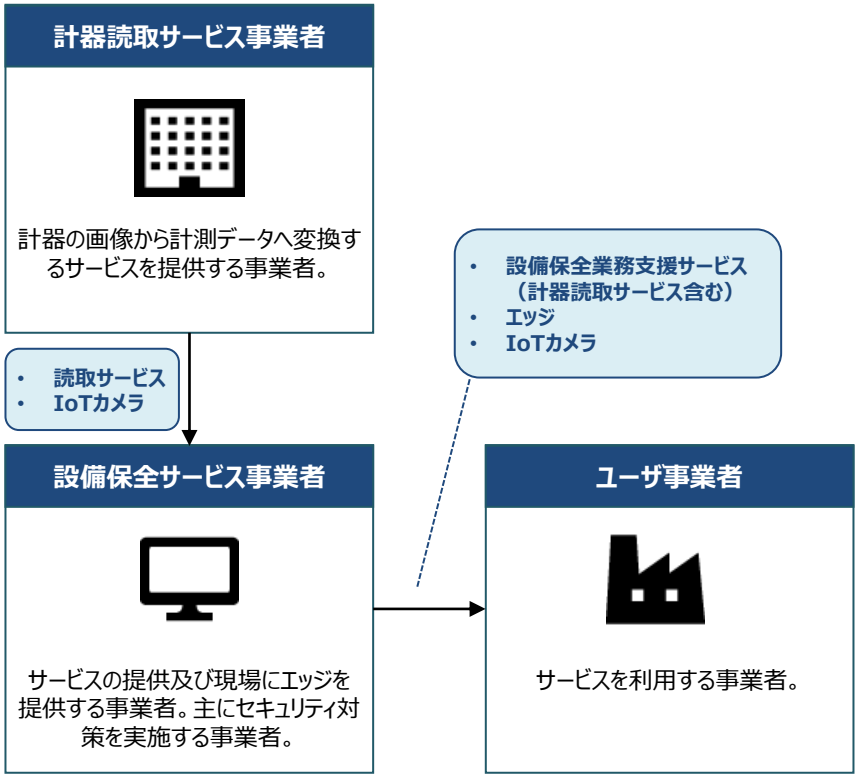
4. 設備保全業務支援サービス

- ユーザ事業者にサービスを提供する設備保全サービス事業者は、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サービスを企画しており、リスクアセスメント及びリスク対応を実施。

✓ 対象機器・システムの概要



✓ 適用主体及び他のステークホルダーの情報



4. 設備保全業務支援サービス

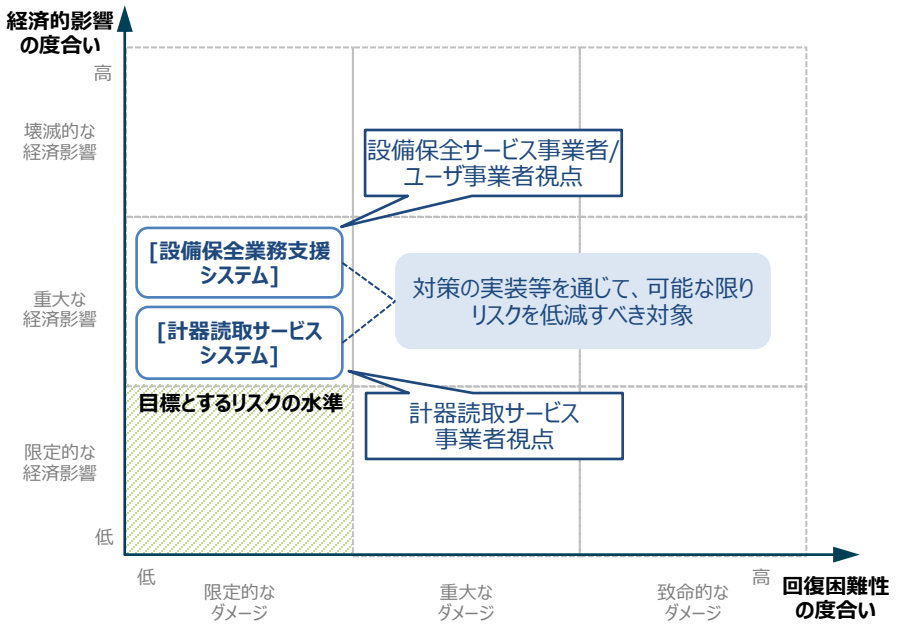
- 例えば、インターネット経由で設備保全サービス事業者が管理する設備保全業務支援システムがマルウェア(例:ランサムウェア)に感染することで、被害が大きくなり得る。「設備保全サービス事業者」のサービス提供に影響を及ぼし得るリスクの低減に努める必要がある。

✓ 対象機器・システムにおいて想定されるリスク(例)

分類	想定されるリスク（例）
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が停止することで、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、設備に係る顧客データの漏洩によって、**設備保全サービス事業者の信頼が低下**する。
ユーザ事業者	• 悪意のある攻撃者又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設備保全業務支援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)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**。また、サービスが利用できなくなることで、**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	• 悪意のある攻撃者によってIoTカメラ及びクラウド通信において、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、**契約解除されるおそれがある**。

✓ 想定されるリスク(例)のマッピング結果

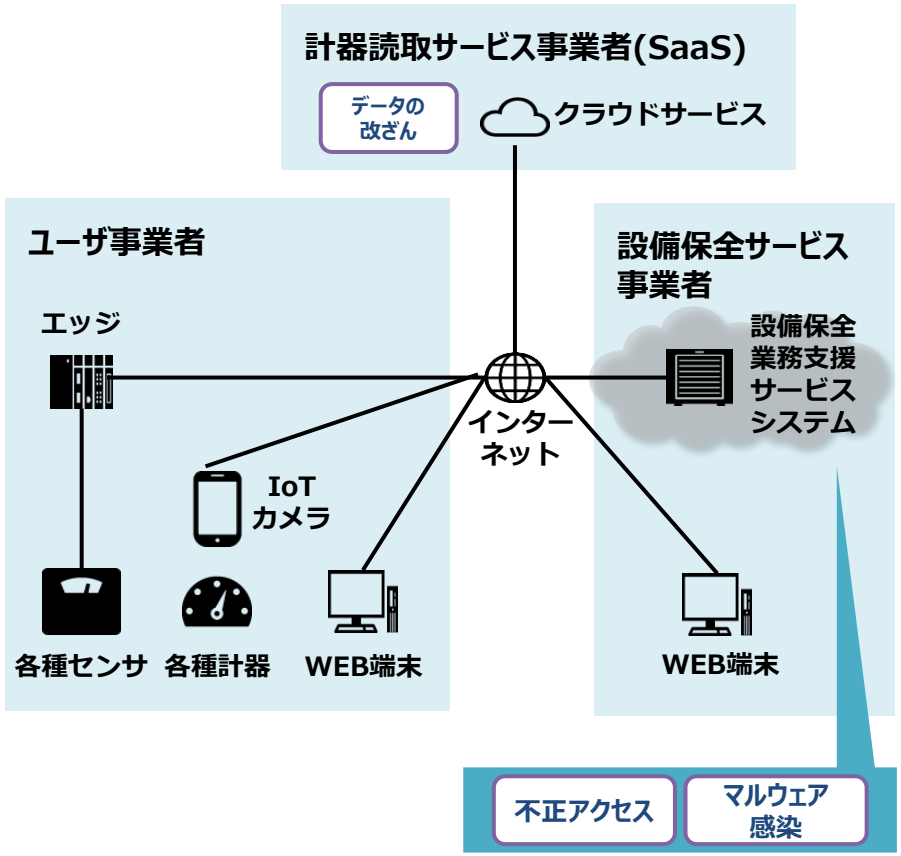
- ユーザ事業者や設備保全サービス事業者視点の設備保全業務支援システムの保有するリスク及び、計器読取サービス事業者視点の計器読取サービスシステムの保有するリスク目標とする水準には収まっておらず、何らかの対処実施が望まれる。



4. 設備保全業務支援サービス

✓ 影響度が大きいリスクにつながり得る脅威の例

- 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について検討することとした。



✓ 行うべきと考えられる対策の例

設備保全サービス事業者/ユーザ事業者にとってのリスクを低減するため設備保全サービス事業者が実施する対策(例)

「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	• 【第1の観点】適切な水準のアクセス制御の実装 • 【第1の観点】マルウェア対策の実施 • 【第2の観点】IoT 機器・システムに対するアップデートの適用

計器読取サービス事業者のリスクを低減するため設備保全サービス事業者の対策(例)

「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	• 【第1の観点】適切な水準のアクセス制御の実装 • 【第1の観点】マルウェア対策の実施 • 【第2の観点】IoT 機器・システムに対するアップデートの適用

4. 設備保全業務支援サービス

分類	主なご意見
適用した際に感じたメリット/デメリット	• メリット:システム構成図をデフォルメして、俯瞰してリスクを確認できる点。また、**組織外部のステークホルダーにおけるリスクも確認できた点にメリット**を感じた。例えば、今回のユースケースにおける「計器読取サービス事業者」にとってのリスクは、通常の業務では考慮していないケースが多い可能性がある。 • メリット: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**点。 • メリット:**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。
適用して気付いた新たなリスク	• (今回の適用実証では既に対策済みのリスクを対象とした。適用実証で新たに気付いたリスクはない。)
適用の際の問題点/悩んだ点	• 悩んだ点：(4-2)データフロー図の①, ②, …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。 • 「リスクアセスメント」のワークシートは、ステークスフォルダ毎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。 • 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)
IoT-SSF改訂に向けた要望	• 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。**
効果的と考えられるIoT-SSFの活用場面	• システム運用中ではなく、**システム企画段階にIoT-SSFを適用するとより効果的**である可能性がある。 • ただし、受発注時に使用した場合、**全てのリスクを網羅できているかを発注者が判断できない**ケースがある可能性がある。例えば、コンサル事業者に判断いただくか、リスクアセスメントを受注業者と発注事業者が一緒に実施する必要がある可能性がある。
作業工数	**合計　5.6人日** (以下、内訳) • 事前準備 **合計2.2人日** • リスクアセスメント　**合計1.1人日** • リスク対応 **合計2.3人日**

第3軸の具体化に関するヒアリング調査

- 「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」の具体化を見据えて、適用実証参画団体及び関連事業者等を対象として、ヒアリング調査を実施した。

	第3の観点	第4の観点
目的	● 「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」の具体化を見据え、「機器・システムの運用・管理を行う者」に求められる能力と今後の検討内容を明らかにする。	● 「第4の観点:その他、社会的なサポート等の仕組みの要求」の具体化を見据え、事業者にとって有効と考えられる「社会的なサポート」や今後の検討内容について明らかにする。
ヒアリング対象	● 適用実証参画団体 ● 関連サービス提供事業者 ● 民間団体 **合計　7団体**	● 適用実証参画団体 ● 関連サービス提供事業者 ● 民間・公共団体 **合計　7団体**
ヒアリング内容	● 「機器・システムを運用・管理する者」に関するセキュリティ能力のあるべき姿と現状について ● 「機器・システムを運用・管理する者」に関するセーフティ能力のあるべき姿と現状について　等	● 既存の社会的なサポートの活用状況について ● 既存の社会的なサポートの改善点について ● 新たなサポートの可能性について　等
スケジュール	● 12月中旬～1月上旬	● 12月中旬～1月上旬

第3軸の具体化(第3の観点の具体化)

- 第3の観点を具体化する目的で、「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」について、企業側と業界団体・政府機関に対してヒアリングを行った。

ヒアリング結果

IoT機器・システムの運用・管理を行う者に求められるセキュリティ能力	
質問への回答	• **IoTセキュリティにはセキュリティとセーフティを理解する技術者**が必要となる。(民間・公共団体) • **全てのセキュリティ能力を1人が備えている必要はなく、事業部として能力を備えていればよい**。業務によって求められる能力を整理することが重要である。(適用実証参画事業者) • **事業部門(OT部門)の技術者には、安全確保の能力が必要**となる。機器・システムで不具合が発生した場合、後からセキュリティインシデントの発生に気付く場合が多く、発生した当初は判断ができない。その上で、素早く適切にエスカレーションをする能力が求められる。(関連サービス提供事業者)
問題意識	• 業務ごとに求められる能力が異なるが、その定義が難しい。(適用実証参画事業者) • IoTセキュリティにはセキュリティとセーフティを理解する技術者が必要となるがその数は非常に少ない。(民間・公共団体)

求められるセキュリティ能力の習得方法/確認方法	
質問への回答	• 組織としてセキュリティ能力を得るためには、**製品開発や保守のセキュリティを扱う各事業部と本社の情報システム部門での情報連携が重要**となる。(民間・公共団体) • 継続的にセキュリティに関する情報を得る必要があるが、業界団体を通じて情報を取得することができている。(適用実証参画事業者)
問題意識	• **セキュリティとセーフティを理解する技術者が不足している**。したがって、**現場作業者よりまずはその監督者へかかる知識を身に付けさせることが効果的**である。(民間・公共団体) • 組織内の人材の能力は確認可能であるが、**組織外の人材においては確認が難しい**。(適用実証参画事業者) • 求められるセキュリティリテラシーも専門的＆高度であるため、人材が不足している。(適用実証参画事業者)

第3軸の具体化(第3の観点の具体化)

- ヒアリング等で共有いただいた問題意識に対する取組み・アプローチ方法(案)を整理した。
- 例えば、各従業員に対して全てのセキュリティ能力を備えさせるのではなく、求められるセキュリティ能力を特定した上で組織(例:事業部単位)として備えさせるための仕組みを検討することも有効と考えられる。

	問題意識	取組み・アプローチ方法(案)
求められる能力	● 業務ごとに求められる能力が異なるが、その定義が難しい。 ● IoTセキュリティにはセキュリティとセーフティを理解する技術者が必要となるがその数は非常に少ない	● セキュリティやOT人材に求められるセキュリティ知識・技能を参照しつつ、「機器・システムを運用・管理する者」(IoTセキュリティ人材)の役割や知識・技能を定義したモデル案を検討することも有効と考えられる。 ● また、セキュリティ能力について、共通する部分と能力ごとに異なるものがあると考えられることから、「機器・システムを運用・管理する者」に求められる能力のうち、共通する部分を特定することも有効と考えられる。
求められるセキュリティ能力の習得方法/確認方法	● 求められるセキュリティリテラシーも専門的＆高度であるため、セキュリティ能力の習得が進まず人材が不足している。 ● 組織内の人材のセキュリティ能力は確認可能であるが、組織外の人材においては難しい。	● 全てのセキュリティ能力を1人が備えている必要はなく、組織(例:事業部単位)として能力を備えていればよいため、以下の観点からセキュリティ能力の習得方法を検討することも有効と考えられる。 ✓ 事業部として求められる役割と役割ごとに求められるセキュリティ能力 ✓ 他の事業部との連携体制

第3軸の具体化(第4の観点の具体化)

- 第4の観点を具体化する目的で「その他、社会的なサポート等の仕組みの要求」について、社会的なサポートを受ける側である事業者と社会的なサポートを提供する側である事業者に対して、ヒアリングを行った。

ヒアリング結果

金銭的なサポート	
質問への回答	• **リスク移転の方法としてサイバー保険は有効である**。一方で、**一般的に言われるサイバー保険は主にITセキュリティ領域を対象としており、物理的な被害については火災保険等の従来型保険で補償対象としている。**理由としてリスクの大きさを測ることが難しい点やIoT機器・システムにおける被害が現時点で少ない点が挙げられる。(関連サービス提供事業者) • リスクが業界ごとに異なるため、保険が成立するかを分野別に検討する必要がある。(民間・公共団体) • 企業に対して加入を促すメッセージを伝えることができることから、**サイバー保険を業界団体を経由して募集することは有効**と考えられる。(民間・公共団体) • サイバーセキュリティお助け隊サービスにおける簡易保険において、補償範囲の拡大を検討している。(民間・公共団体)
問題意識	• 保険業界では、既存の財物保険や賠償責任保険等における潜在的なサイバー関連の損失リスクであるサイレントサイバーリスクについて議論がなされている段階である。かかるリスクは既存の保険(例:火災保険)で対処することとなるが、免責事項に含まれている。免責事項を復活されることも考えられるが、保険料を設定することが難しい。(関連サービス提供事業者)

モノ・情報面でのサポート	
質問への回答	• **IoT機器の認証を取得を促す製品に対する取組みがなされるとよい。**製品が認証を取得することによって消費者の安心感を醸成できる。(適用実証参画事業者) • **業界団体や関連団体からセキュリティに関する情報(例:セキュリティ対策や脆弱性情報)について継続的に入手することは有効**である。また、他社事例を知りたい。(適用実証参画事業者)
問題意識	• **新たに求める社会的なサポートは、「ネットワークの見える化」及び「問題のある通信への自動的な遮断等の対応」**である。ルータ等への不審な大量のパケット受信によって住まい手はサービスを利用不可になる場合がある。瑕疵ではないものの、メーカ側で対応をする必要があり、不要なコストとなっている。(適用実証参画事業者) • 企業の枠組みを超えた支援があるとよい必要と感じる。例えば業界ごとの対応も一定程度有効であると考えられる。(適用実証参画事業者)

第3軸の具体化(第4の観点の具体化)

- ヒアリング等で共有いただいた問題意識に対する取組み・アプローチ方法(案)を整理した。
- 例えば、対象となる業界や業種を絞った上で、サイバー保険の提供方法に関して業界団体による検討を行うことが有効と考えられる。

	問題意識	取組み・アプローチ方法(案)
金銭的なサポート	● 保険業界では、既存の財物保険や賠償責任保険等における潜在的なサイバー関連の損失リスクであるサイレントサイバーリスクについて、既存保険における補償可否が議論されている。 ● サイバーリスクが巨額になる場合には民間の保険会社では対応が難しい。	● 民間での検討状況を踏まえつつ、サイバー保険の提供方法についても業界団体による検討を行うことが有効と考えられる。
モノ・情報面でのサポート	● ルータ等への不審な大量のパケット受信によって消費者はサービスを利用不可になる場合がある。瑕疵ではないものの、メーカ側で対応を行う必要があり、不要なコストとなっている。例えば、「問題のある通信への自動的な遮断等の対応」を国等が行っていただけるとよい。 ● 企業の枠組みを超えた支援(例:脆弱性情報管理の仕組みに係る支援)があるとよい必要と感じる。	● IoTに関わる通信において不審な通信への自動的な遮断等の方法を検討することが有効と考えられる。また、ユーザ側(消費者)においても脆弱性やインシデントに対処するために、ユーザが実施すべき事項をガイドラインとしてとりまとめることも有効と考えられる。 ● 効率的な脆弱性管理の仕組みが未導入である企業が多いため、脆弱性管理の仕組みに関する事例集を作成することが有効と考えられる。また、脆弱性対応を支援する業界団体等を巻き込んだ仕組みを検討することも有効と考えられる。

③IoT-SSFの有効性検証

- IoT-SSFの適用実証と並行して、過去に生じたインシデント・事故事例を対象にした机上検討を進め、IoT-SSFの定義する軸や観点の有効性検証、今後の改善に向けた課題の特定等を進めている。
- 適用実証での適用事業者への確認結果とも照らし合わせて、最終的な有効性検証の結果として取り纏めることを想定。

机上検討

過去のインシデント等に対する机上でのIoT-SSFの適用、課題の特定 等

＜検証事項の例＞
- 第1軸・第2軸によるリスクアセスメントの有効性
- 第3軸の4つの観点による対策整理の有効性

有効性に関する仮説の提示

適用実証

実際の機器/サービスに対するIoT-SSFの適用を通じた課題の特定 等

成果の統合

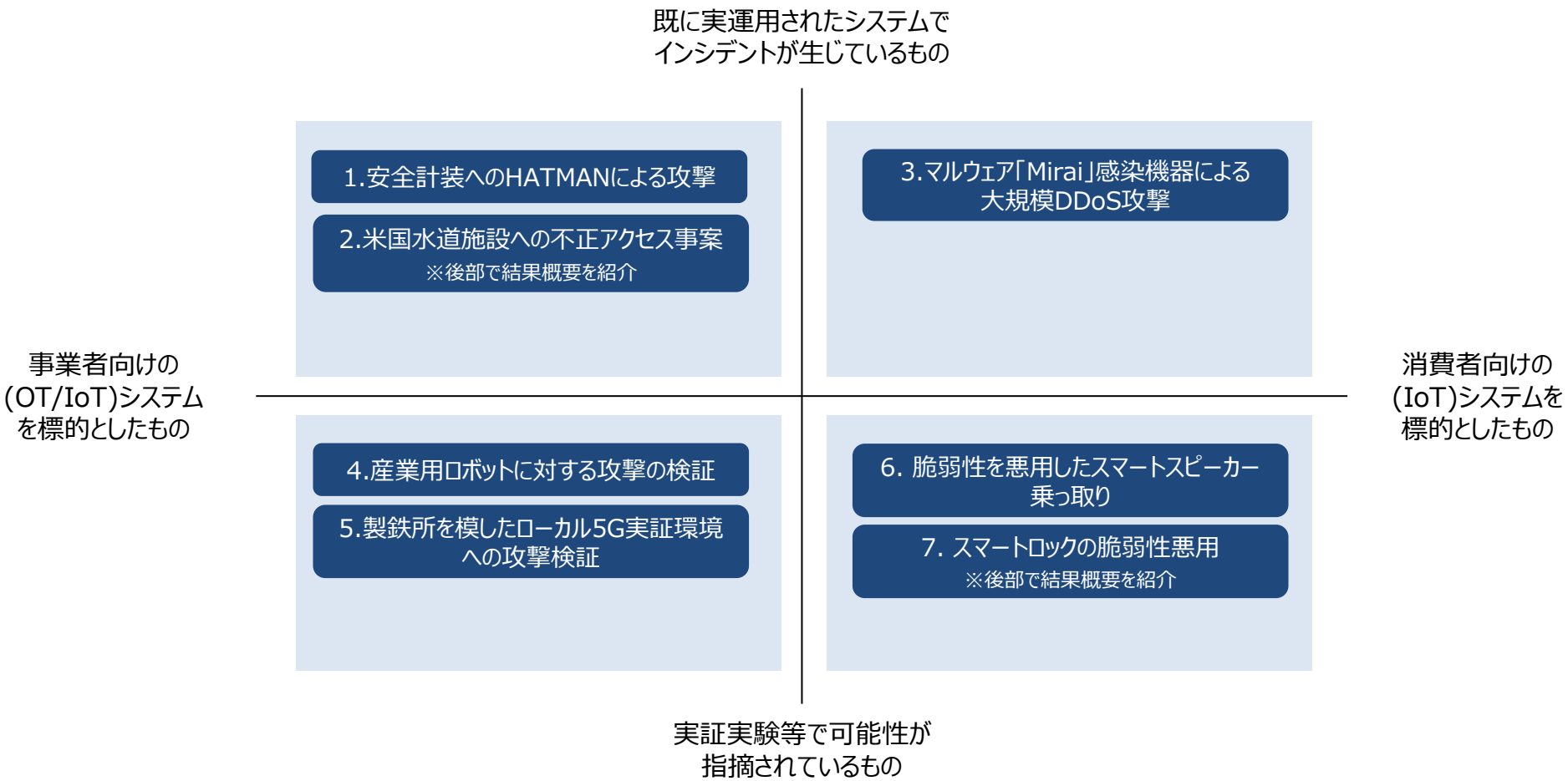
有効性検証結果

IoT-SSFの適用が有効と考えられるケース、
有効とは言えないケースをそれぞれ整理し、より利便性の高い内容とするために必要な修正等を具体化する。
第7回TF開催時までを目途に取り纏める。

適用実証の成果とも合わせて、現状のIoT-SSFの改善に向けた課題を特定し、今後の検討へのインプットとする。

事例選定の考え方

- 有効性検証の対象事案としては、過去のTF等でも紹介しているような事業者向け・消費者向けの双方について、既に実運用されたシステムで生じたインシデントと実証実験等で可能性が指摘されているような事案を計7件取扱った。

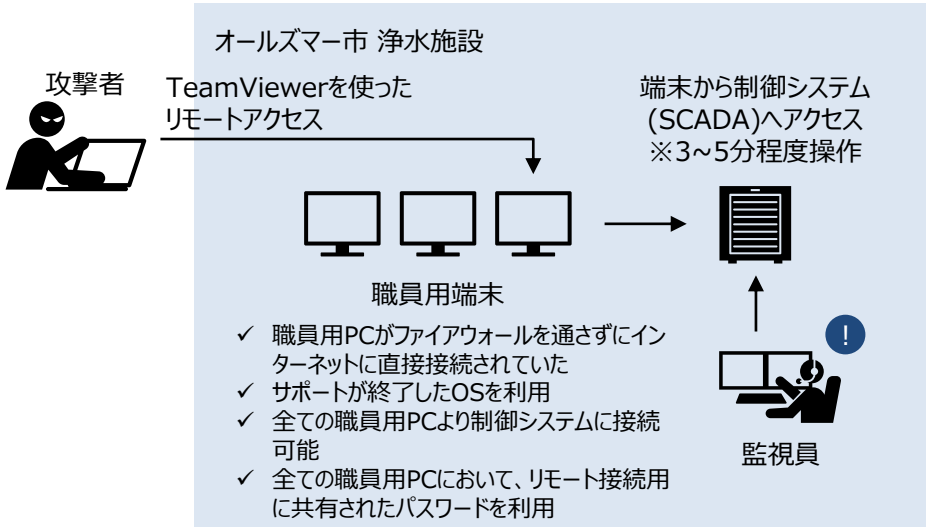


ケース２［対象事案の概要］

- 有用性検証に向けたケーススタディのため、オールズマー市水道施設への不正アクセス事案を取扱った。

対象とするインシデントの概要

項目	概要
名称	オールズマー市水道施設への不正アクセス事案
概要	2021年2月、米国フロリダ州オールズマー市の水道施設(浄水場)がサイバー攻撃を受け、飲用水に含まれる水酸化ナトリウムの濃度の設定値が100ppmから1万1100ppmに引き上げられた。最終的には、職員がすぐに気づいたために実害は生じなかった



［出典］ 水道施設に「毒混入」狙ったサイバー攻撃、お粗末すぎるセキュリティーの恐怖
(https://xtech.nikkei.com/atcl/nxt/column/18/00676/021700072/)

攻撃経路の想定

1. 施設外より、リモートアクセスソフトTeamViewerを使って施設内の端末に接続する。(施設外からトラブル対応等が可能なように、端末はインターネット経由でアクセス可能となっており、ファイアウォール等による防護もなかったとされている。)
2. 上記端末を3～5分間遠隔操作し、飲用水に投入される水酸化ナトリウムの量を変更した。
3. 現地の職員がすぐに異常に気づき設定を元に戻したため実害はなかった。

推奨緩和策

- 米国WaterISACは事象発覚後、以下の対策の実施を推奨している。
  - ネットワーク上のインターネットにアクセス可能なOT機器を特定する
  - ネットワーク・セグメンテーションを導入する
  - リモートアクセスが必要な場合は、安全に構成されたVPNを使用する
  - ホワイトリストやジオ・ブロッキングなどの方法でトラフィックをフィルタリングし、許可されていない人や場所からのアクセスを防ぐ
  - トラフィックを暗号化する
  - 簡単すぎない認証方法を使用する
  - 強力なパスワードを適用する
  - タスク実行のための絶対に必要な人のみに特権を与えるユーザーアカウントのアクセス網を構成する

ケース２ [対象事案に係る評価]

- オールズマー市水道施設への不正アクセス事案への現状の見解は以下の通り。

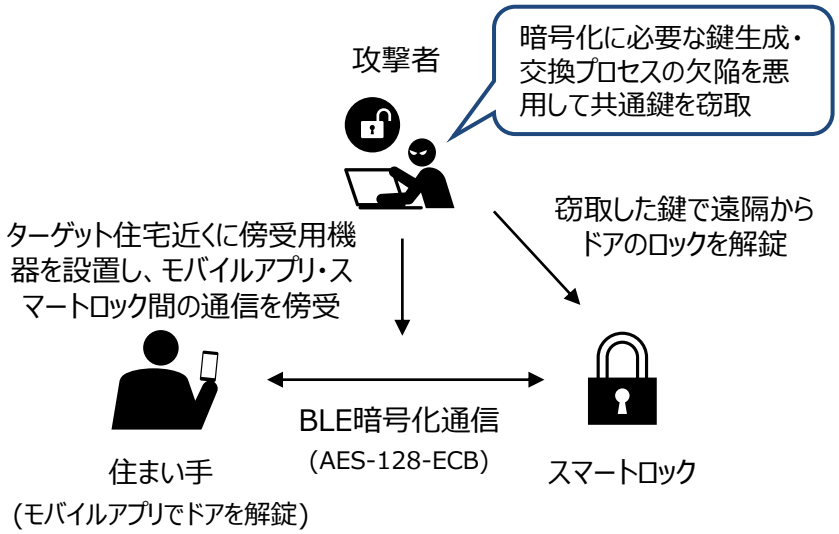
検証項目		概評	根拠
第1軸/第2軸の有効性	リスクアセスメントを事前に実施しておくことの有用性	• アセスメントが適切に実施されていれば容易に想定され得るシナリオであり、**有効に機能する**	• 本事案の発端になったリモートアクセスツールの導入等において、最低限のリスクアセスメントが実施され、通信経路の保護や強固な認証の導入等がなされていれば、事象発生の可能性を大きく低減することができていたと考えられる。
	リスクアセスメントをIoT-SSFの提示する第1軸、第2軸を通じて実施することの有用性	• 「起こりやすさ」が対策優先度の評価にポジティブな影響をもたらし得る事案であり、第1軸、第2軸に基づく機器・システム単位の評価による**効用は限定的と考えられる**	• 本事案は、飲用水等の供給停止に伴う経済的影響に加え、健康被害等の回復困難性の度合いにおいても多大な被害を伴うものであり、単に影響の度合いとして評価される場合と比較しても最終的に整合する評価を与え得るものとなっている。 • 一方で、本事案におけるリモートアクセス機能の悪用は、必ずしも高度な攻撃能力を要求するものではなく、**評価時に起こりやすさに留意することがシナリオの成立を防ぐために有益だったと考えられる**。 • また、対象のシステムでは影響度や起こりやすさの異なる多数のリスクシナリオが想定されるところ、**リスクシナリオごとのリスク値割り当てを考慮することが有益になり得た**。
第3軸の有効性	第3軸が示す4つの観点が有効な対策を「括る」枠組みとして有効に機能することの評価	• 第１の観点及び第２の観点で主要な対策を包括できている点で、**有効に機能した**	• WaterISACにより示された**推奨策は、概ね第1の観点及び第2の観点に含まれる**ものであり、第3軸に示される観点の包括性を否定するものとはなっていない。
	4つの観点を考慮することで、既存の枠組みでは抽出できなかった対策を特定することができるかの評価	• 第3の観点が明確化され、適切な施策が講じられるならば、**有効に機能する**	• 本事案の主要な原因のひとつとして、設備の運用・管理を担当する者のセキュリティに関する能力の低さが挙げられることから、**第3の観点としてこうした重要システムにの運用・管理に従事する者が満たすべき最低限の能力について検討される余地**が議論され得る。

ケース７［対象事案の概要］

- 有用性検証に向けたケーススタディのため、スマートロックの脆弱性悪用を取扱った。

対象とするインシデントの概要

項目	概要
名称	スマートロックの脆弱性悪用
概要	フィンランドのセキュリティ会社F-Secureは、2019年、KeyWe社が開発・販売するスマートロックサービスの脆弱性悪用を通じて、第三者がスマホアプリとスマートロック間のBLE(Bluetooth Low Energy)通信を傍受して鍵を取得し、ドアの解錠／施錠などが可能になる点を報告した。



攻撃経路の想定

1. ターゲット住宅近くに傍受用機器を設置＊1し、住まい手が施錠／解錠するモバイルアプリ・スマートロック間の通信を傍受
2. 暗号化に必要な鍵交換プロセスの欠陥を悪用(傍受で得たBluetoothアドレスから共通鍵を生成)して共通鍵を窃取＊2
3. 窃取した共通鍵で遠隔からドアのロックを解錠

＊1 ターゲットの玄関から15メートル範囲(BLE通信が届く範囲)とされる
＊2 Bluetoothアドレスは、デバイス名やBLE接続が可能であることを周囲のデバイスに知らせる無線信号に含まれている一方、共通鍵の生成アルゴリズムはアプリの解析から割り出すことが可能であった。

推奨緩和策

- 設計段階での安全な暗号鍵生成・交換メカニズムの採用
- より安全なバージョンへのファームウェアのアップデート
- 上記の実施が困難な場合、スマホアプリでの解錠／施錠をあきらめて旧来の物理鍵に戻す

[出典] Smart lock has a security vulnerability that leaves homes open for attacks
(https://www.cnet.com/home/security/smart-lock-has-a-security-vulnerability-that-leaves-homes-open-for-attacks/)

ケース７ [対象事案に係る評価]

● スマートロックの脆弱性悪用への現状の見解は以下の通り。

検証項目		概評	根拠
第1軸/第2軸の有効性	リスクアセスメントを事前に実施しておくことの有用性	• アセスメント時に当該脅威を適切に識別していることを前提とすれば、有効に機能したと考えられる。一方で、未知の脅威を事前に想定できるかという点については対応の限界がある。	• 基本的な対策の漏れ等を防止するにあたり、リスクアセスメントを通じて具体的にリスクを特定し、対応として実装することは有用である。 • 一方で、事前に攻撃シナリオすべてを特定して、(未知のものを含めて)識別された脆弱性に対応することは事実上不可能なため、**事前の対応には限界も**ある。
	リスクアセスメントをIoT-SSFの提示する軸や方法で実施することの有用性	• 本ケースの「起こりやすさ」(実施容易性)や、スマートホームにおけるリスクシナリオの多様性を考慮すると、**有効に機能しない可能性がある**	• スマートロックの解除は、住居への不法侵入やその先の盗難等につながるものであり、「経済的な影響の度合い」及び、場合によっては「回復困難性の度合い」が高くなることも想定されるが、かかる評価が対策の導出等に与える効果は未知数。 • 傍受用デバイスのチップやハードウェアは安価に入手・製作可能とされており、**「起こりやすさ」に関連して、高度なスキルを要するものかを判断することが、シナリオの実現を防ぐにあたり、有益に作用し得る。** • スマートロックやそれを含むスマートホームシステムを狙ったリスクシナリオが多数想定されるところ、**リスクシナリオごとのリスク値割り当てを考慮することが有益になり得た**。
第3軸の有効性	第3軸が示す4つの観点が有効な対策を「括る」枠組みとして有効に機能することの評価	• 第１の観点及び第２の観点で主要な対策を包括できている点で、**有効に機能した**	• **提案されている対策は、概ね第1の観点または第2の観点に位置づけられる**ものと言える。
	4つの観点を考慮することで、既存の枠組みでは抽出できなかった対策を特定することができるかの評価	• 住まい手が実施すべき具体的な対策が明確化されるならば、**有効に機能する。**	• 本ケースでは主たる「機器・システムの運用・管理を行う者」は住まい手となるが、高度なスキル等を有しているとは想定しがたい一方で、「より安全なバージョンへのファームウェアのアップデート」等の実施にあたって一定の役割が求められるところ、**「第3の観点」または「第4の観点」として、かかる能力ギャップを埋め合わせるような取組みを喚起し得る**。

検証結果の概要

- ７件の検証の結果、以下のような結論を得た。

観点	評価結果(現状案)
リスクアセスメントを事前に実施しておくことの有用性	• 一般的に、生じ得る被害を回避、あるいは低減するにあたり、評価時に発生し得るシナリオを抜け漏れなく特定できていたならば、事前のリスクアセスメントの実施は有効に機能する。 • 一方で、評価時点では未知の脅威・脆弱性を含めて対処することは困難であり、その点については、事前のアセスメントに加えて、サービス等の運用時にあっても別途迅速な脆弱性対応に資する体制構築・運営等が必要である点に留意が必要と考える。 • また、評価に際して(ユーザーに用途等が委ねられており)機器・システムの稼働する環境を事前に明確化する必要がある点や、機器の踏み台化(＃2)のように最終的な被害がどの程度生じるかが事前にはわからない場合に正確な評価の実施に限界がある点に留意が必要である。
リスクアセスメントをIoT-SSFの提示する軸や方法で実施することの有用性	• IoT-SSFの第1軸・第2軸の利用は、事業リスクを複数の観点で評価し、適切なリスクレベルを割り当てる際に有益であった。 • IoT-SSFはリスク値の算定にあたり、基本的に「起こりやすさ」を考慮しないモデルとなっているが、脅威や脆弱性の悪用に高度なスキルを要するものかを判断することで、仮想的に「起こりやすさ」を算定することが対処の優先度決定の精度を向上させ得る点に留意する必要がある。 • 単一の機器・システムに多数の重要なリスクシナリオが想定される場合、機器・システム単位で一つのリスク値を割り当てるのではなく、リスクシナリオ単位でリスク値を割り当てることが有用になり得る点に留意すべき。
第3軸が示す4つの観点が有効な対策を「括る」枠組みとして有効に機能することの評価	• 今回扱った事象で提案されている軽減策等は、第3軸が示す4つの観点の対策のいずれか(多くの場合、第1の観点または第2の観点)に当てはまるものであり、第3軸の包括性を損なうものではなかった。
4つの観点を考慮することで、既存の枠組みでは抽出できなかった対策を特定することができるかの評価	• 第3の観点に該当する施策は、第1の観点及び第2の観点で提案される技術的な対策を人材面から補うものと位置づけられ、事象の早期検知・対応に資するものである場合は、一定の有効性が認められた。(例えば、機器・システムの挙動等を監視するシステム的な仕組みを導入したとしても、ログやアラート等を監視、分析する十分な能力を有した要員がいなければ、事象の早期検知・対応の効果は限定的になる。) • また、「機器・システムの運用・管理を行う者」のセキュリティ能力が十分期待できないケースでは、第3の観点、第4の観点として、求められる水準の能力と実際の能力のギャップを埋め合わせるような取組みも含まれ得る。(例：製品ラベルを通じた適時の情報提供等)

IoT-SSFの適用実証及び有効性検証の関係性

	IoT-SSFの適用実証	IoT-SSFの有効性検証
目的	● 事業者の実際のIoTシステム/サービスにIoT-SSFを適用し、今後の更なる適用拡大に際して参考となる事例を蓄積する。 ● 適用を通じて、IoT-SSF及びユースケース集の改善点を洗い出す。	● IoT-SSFの適用が有効と考えられるケース、有効とは言えないケースをそれぞれ整理し、より利便性の高い内容とするために必要な修正等を具体化する。
実施主体	● 適用実証に参画いただいた事業者	● 事務局(委託先:日立製作所)
対象	● **現在運用**しているIoTシステム・サービス ● **将来的に運用**が予想されるIoTシステム・サービス	● **過去に発生した**インシデント事例 ● 研究者等により実証実験等で可能性が指摘された事案