経済産業省

『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3年11月29日

経済産業省 商務情報政策局
サイバーセキュリティ課

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

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

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

4. 本タスクフォースにおける検討事項

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

- **6つの産業分野別サブワーキンググループ(SWG)**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 分野横断の共通課題を検討するために、3つの**タスクフォース（TF）を設置**

産業サイバーセキュリティ研究会WG１（制度・技術・標準化）

標準モデル（CPSF）

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

- **ビルSWG**
  - ガイドライン第1版の策定(2019.6)
- **電力SWG**
  - 小売電気事業者ガイドライン策定(2021.2)
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドライン1.0版を公表(2020.12)
- **スマートホームSWG**
  - ガイドライン1.0版を公表(2021.4)
- **宇宙産業SWG**
  - 2021年3月に第2回を開催
- ・・・

分野横断SWG

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

検討事項：
データの信頼性確保に向け「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮）」骨子案のパブリックコメントを実施。

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

検討事項：
OSSの管理手法に関するプラクティス集の策定、SBOM活用促進に向けた実証事業（PoC）を検討。

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

検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」を公開。

第3層TF：サイバー空間における価値創造を支えるデータマネジメントの枠組みの策定

- データマネジメントに関する定義を明確化し、フレームを設定することで、主体間を転々流通するデータに関する**リスクポイントの洗い出しを可能に**する。
- また、本枠組みを**共通の定規として利用**することで、各国・地域などの**主体間のデータに関するルールのギャップ/データの流通プロトコルの問題を可視化、データの囲い込みを回避する**取組につなげる。
- 「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮）」の**骨子案を取り纏め、パブリックコメントを実施**。（2021/7/15～10/11）

https://www.meti.go.jp/press/2021/07/20210715005/20210715005.html

データマネジメントの新たな捉え方

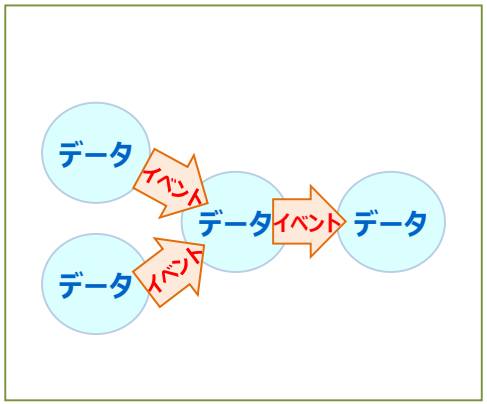
▶「データの "**属性**" が "**場**" における "**イベント**" により変化する過程をライフサイクル全体にわたって管理すること」

属性	✖	**場**	✖	**イベント**
データが有する性質		特定の規範を共有する範囲		データの属性を生成・変化させる処理

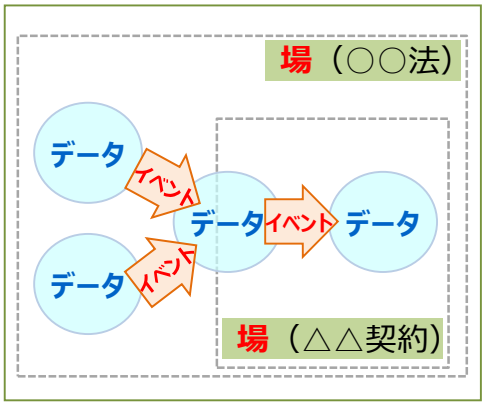
新たな捉え方への当てはめステップ

▶4つのステップに沿ってバリュークリエイションプロセスにおけるデータの状態を可視化しリスクを洗い出す。

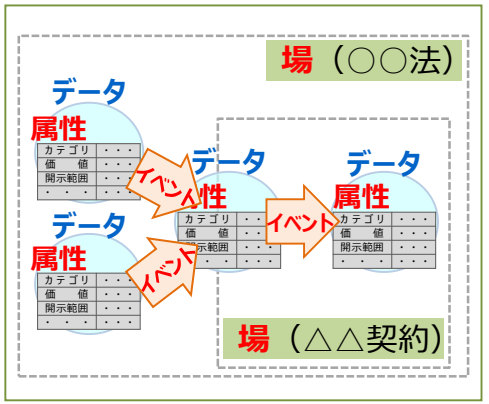
STEP 1
データ処理フロー（「イベント」）の可視化



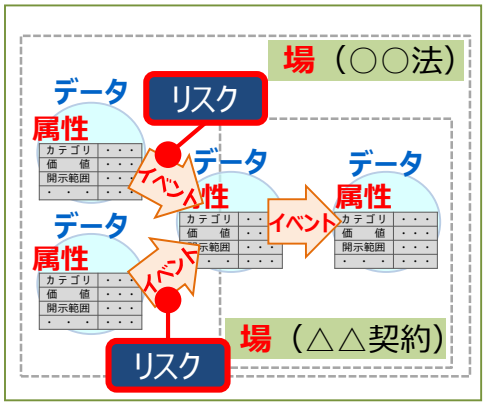
STEP 2
必要な制度的保護措置（「場」）の整理



STEP 3
「属性」の具体化



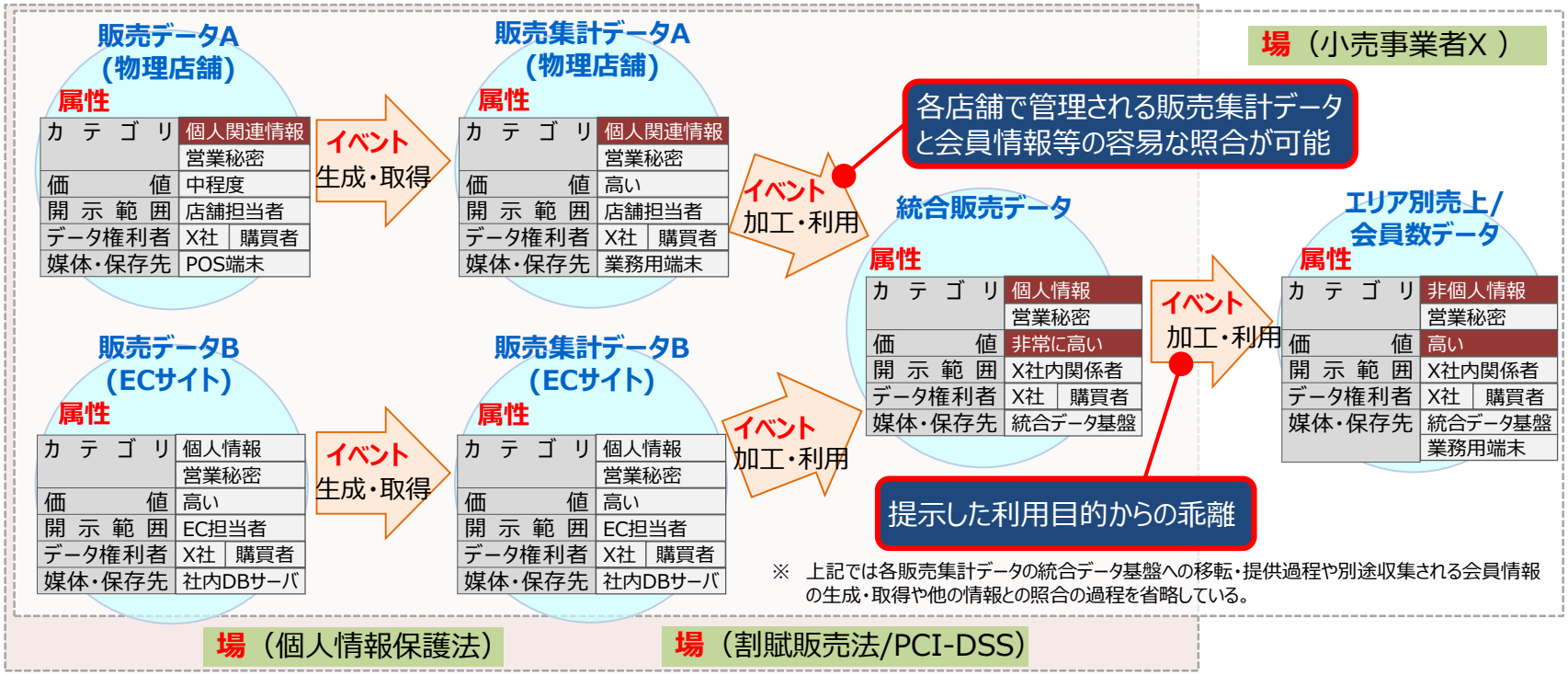
STEP 4
「イベント」ごとのリスクの洗い出し



第3層TF：フレームワークのユースケースに係る検討（POSデータ活用事例）

- ユースケースのひとつとして、小売業におけるPOSデータの活用事例にフレームワークを適用。
- 販売データの生成・取得からマーケティング目的での加工・利用に至るまでの一連の利活用プロセスを可視化するとともに、今後のセキュリティ水準等の向上のために必要なアクションを明確化。

新たな捉え方の適用（小売業におけるPOSデータの活用事例）



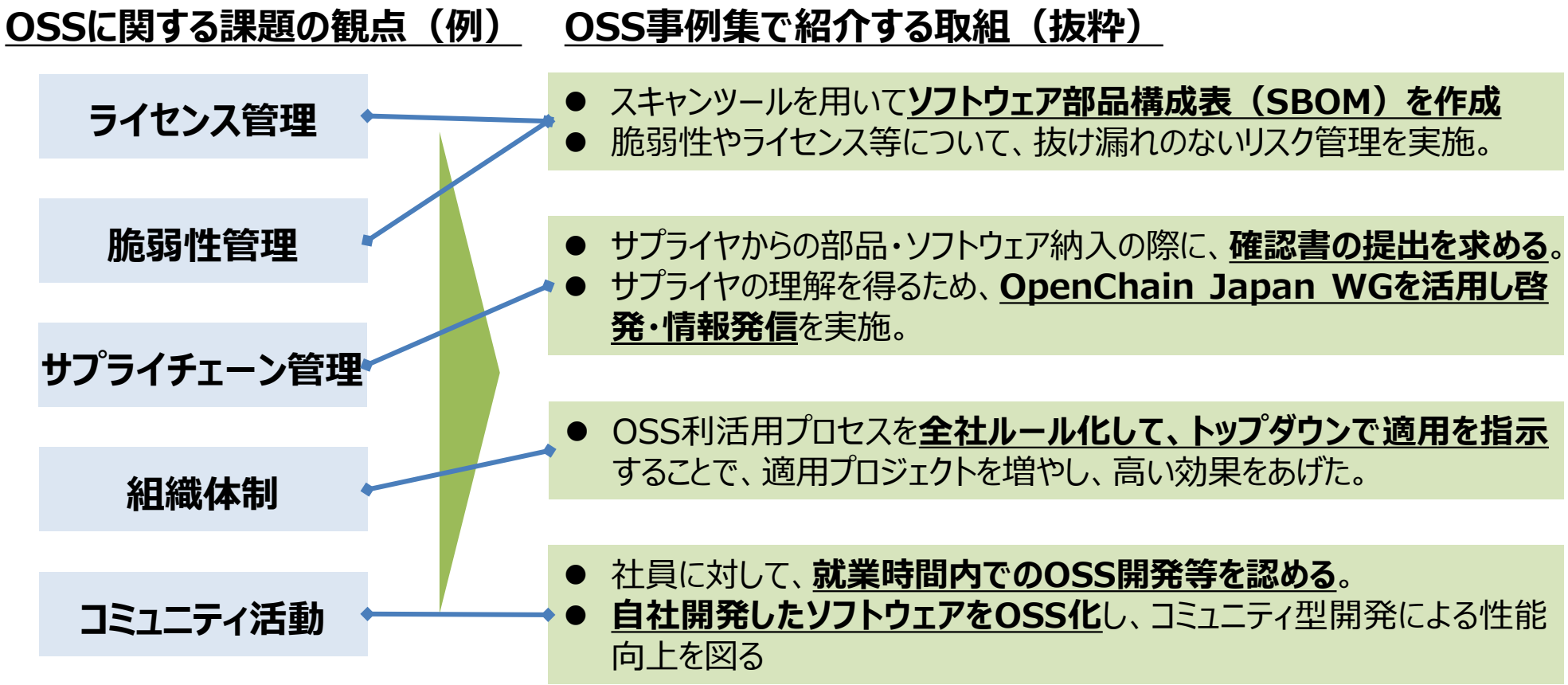
新たな捉え方の適用を通じてx社が導き得るアクション（例）

- 一律のデータ保護水準を確保することが難しい各物理店舗において、他データとの照合等を通じて個人情報に該当するデータが保有されないことを改めて確実なものとすべく、統合データ基盤で管理される会員情報に対する各店舗、支社によるアクセス状況のレビュー、アクセス制御ポリシーその他の運用規定のレビュー等を行う
- 購買者に関するデータの利用実態を踏まえ、自社の個人情報保護方針や会員規約等の一部（利用目的に関する条項等）を改定する

ソフトウェアTF：OSS管理手法に関する事例集の拡充

- **「OSSの利活用及びセキュリティ確保に向けた管理手法」をまとめた事例集を作成し、2021年4月21日に公開**。参考となる事例を共有して企業における適切なOSS利用を促進。日本から働きかけることで日米でOSSの活用・管理に関するベストプラクティスを共有する機会の確保を目指す。
- 令和3年度も、事例の拡充に向けてヒアリングおよび机上調査を継続。

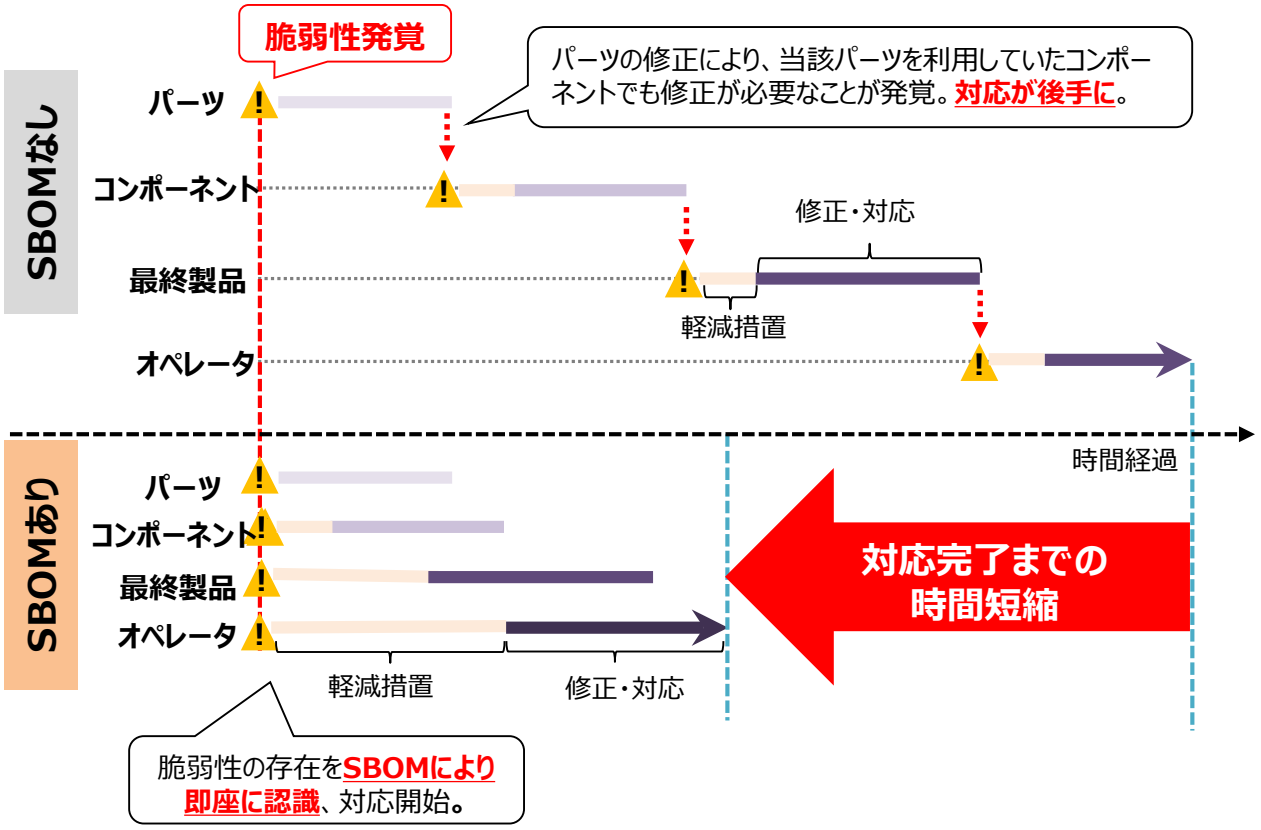
https://www.meti.go.jp/press/2021/04/20210421001/20210421001.html



ソフトウェアTF：SBOM

- ソフトウェアの成分構成を表す**SBOM（Software Bill of Materials）**を活用することにより、**ソフトウェアに何が含まれ、誰が作り、どのような構成となっているか**等の把握が容易になる。
- 米国NTIAが2018年から主導するSoftware Component Transparencyでは、ヘルスケア分野における実証事業（PoC）に続いて、自動車産業・電力分野にも取組が拡大。
- 日本においても業界構造や商習慣を考慮しつつ、SBOM活用に向けた実証事業を実施中。

SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮



米国NTIAにおけるSBOMのPoC

ヘルスケア分野（病院、医療機器）

病院、医療機器メーカー、ベンダーが参加。2回のPoCを経てSBOM活用の手法、課題等を公開。4/29のNITA会合にて、医療機器メーカーにおけるSBOM活用に向けたガイドラインを取りまとめる予定と発表。

自動車産業分野

Auto-ISACを中心としたサプライヤー中心のプロジェクト。ヘルスケア分野のPoCを参考にしつつ、自動車産業分野でのSBOMの普及促進を目的として、SBOM構築方法や得られた教訓・課題等を確認する。12ヶ月ほどかけてサプライヤー向けの推奨事項がとりまとめられる予定。

電力分野

INL主導で、電力会社、電力機器ベンダー、ソフトウェアベンダー、電気協会等が参加。米国エネルギー省からもプレゼンターとして参加。2021年中のPoC実施完了に向け、目的、実施内容、スケジュールに関する議論を経て、9/1からPoCを実施中。

スマートホーム、自動車業界におけるCPSFをベースにしたガイドライン策定

- 策定・公表済みのビルガイドライン以外に、**CPSFをベースにした業界別ガイドラインの策定が進行**。
- 特に、**スマートホーム、自動車業界では、ガイドラインを公表**。

スマートホームSWG

ガイドライン1.0版を公表（2021.4.1）

目的

- スマートホームにおける安全で安心な生活の実現のため、**幅広いステークホルダーに必要なセキュリティ対策の指針を示す**。

対象範囲

- IoTに対応した住宅設備・家電機器などがサービスと連携することで様々な便益が提供されるスマートホームにおける**多様なステークホルダーが対象**
  - スマートホーム向けの **IoT 機器関連事業者**
  - スマートホーム向けの**サービス事業者**
  - スマートホームの**管理者・住まい手**　　等

ポイント

- 知識やバックグラウンドが様々なステークホルダーに対応するため、ユースケースから想定されるインシデントを基に、**シンプルな対策ガイドから、具体的な対策要件や他の標準との対比まで、階層的に整理**。

今後の方針

- ガイドラインの普及促進。
- **ガイドライン2.0版**に向けた論点の整理。

参考： https://home.jeita.or.jp/smarthome/security/

自動車産業SWG

ガイドライン1.0版を公表（日本語：2020.12.1、英語：2021.3.26）

目的

- **業界全体のセキュリティのレベルアップ**
- 対策レベルの効率的な点検の推進

対象範囲

- 自動車業界の全ての企業の**エンタープライズ領域**
- OEMから小規模会社で最低限必要な必須項目を策定（ただし、強制するものではない）。

ポイント

- 部品やサービス/ソフトウェアのサプライチェーン対応
- **CPSFの対策要件をベースに、業界の実態に即した実施事項レベルや記載方法を検討**して作成。
- チェックリストを活用することにより、各社が自社**の取組状況をセルフチェックできる**。
- **トライアルを踏まえ記載を充実**させ、1.0版として公表。

今後の方針

- さらなる**レベルアップに向けた項目の拡充**。
- ガイドライン対応状況の集約・分析。
- 工場セキュリティに関する課題対応。

参考：http://www.jama.or.jp/it/cyb_sec/cyb_sec_guideline.html

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

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

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

4. 本タスクフォースにおける検討事項

サイバー攻撃による米国石油パイプラインの操業停止について

- 5月7日、米石油パイプライン最大手のコロニアル・パイプラインがランサムウェアによるサイバー攻撃を受け、全ての業務を停止したと発表。直接の影響を受けたのはITシステムだが、脅威を封じ込めるためにOTシステムをオフラインにし、全てのパイプラインの運用を停止した。停止されたサービスは12日から再開され、15日までに供給網全体が復旧したとされる。
- 米運輸省は9日、燃料の輸送に関して緊急措置の導入を宣言。また、CISAのサイバーセキュリティ部門トップも声明を公表。
- FBIはロシア系攻撃集団「ダークサイド」の関与を断定、同グループは「目的は金銭であり社会に影響を与えることは意図していない」と表明（※）。

※：同グループは略取した身代金の一部を対価に開発したランサムウェアをグループ外の実行犯に提供するスキームを運用しており、実行犯がもたらした影響に同グループは関知しない、とのスタンス

コロニアル・パイプライン

メキシコ湾岸の製油所と米東部・南部を結ぶ全長8,850kmのパイプライン。
東海岸の需要の約半分にあたる１日約１億ガロンを輸送。

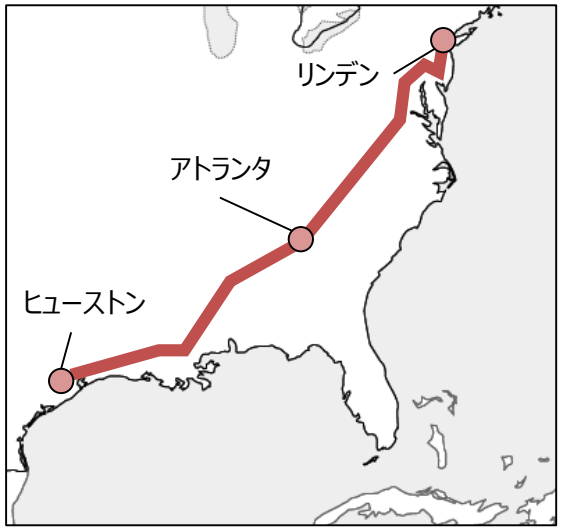
米運輸省による緊急措置の内容

影響を受ける１７州と首都ワシントン向けに
燃料を輸送する運転手の労働時間規制を一時的に緩和。

米CISAによる声明のポイント

CISAは、サイバーセキュリティ部門トップのGoldstein氏名で声明を公表。

・被害企業と関係官庁とともに本事案に対処中。
・ランサムウェアは組織の規模、セクターに関係なく直面する脅威。
・この種の脅威に晒されるリスクを減らすためサイバーセキュリティ体制を強化する措置を講じることを各組織に推奨。

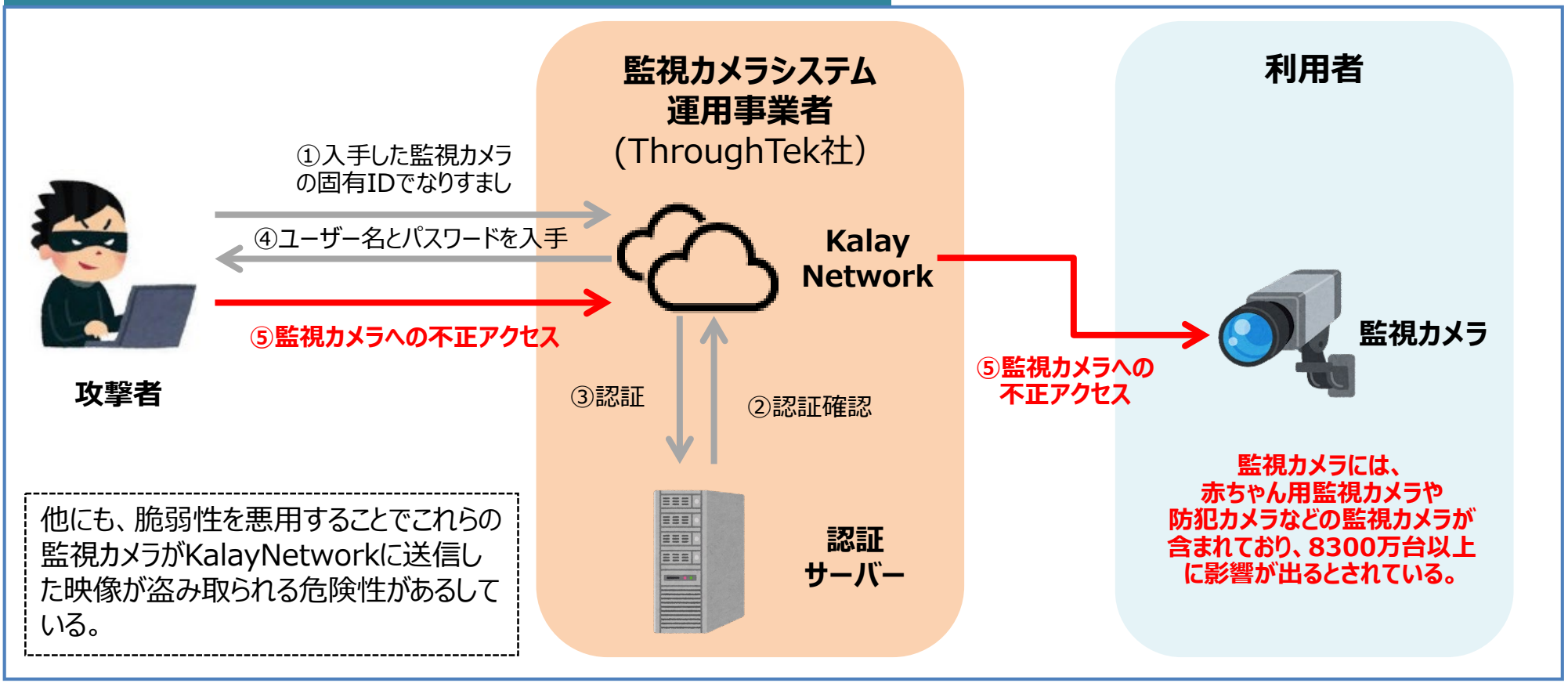


コロニアル・パイプラインの
主要パイプライン（イメージ）

8300万台以上のIoT機器が影響を受ける脆弱性

- 2021年8月、Mandiantは監視カメラを含む8300万台以上のIoT機器が影響を受ける脆弱性「CVE-2021-28372」を発表。KalayNetworkで不適切なアクセス制御がなされる可能性があり、本脆弱性によって、ネットワークカメラの映像を盗み取られたり、家庭内の機器に不正アクセスされる可能性があるとされている。

攻撃者が監視カメラに不正アクセスするイメージ

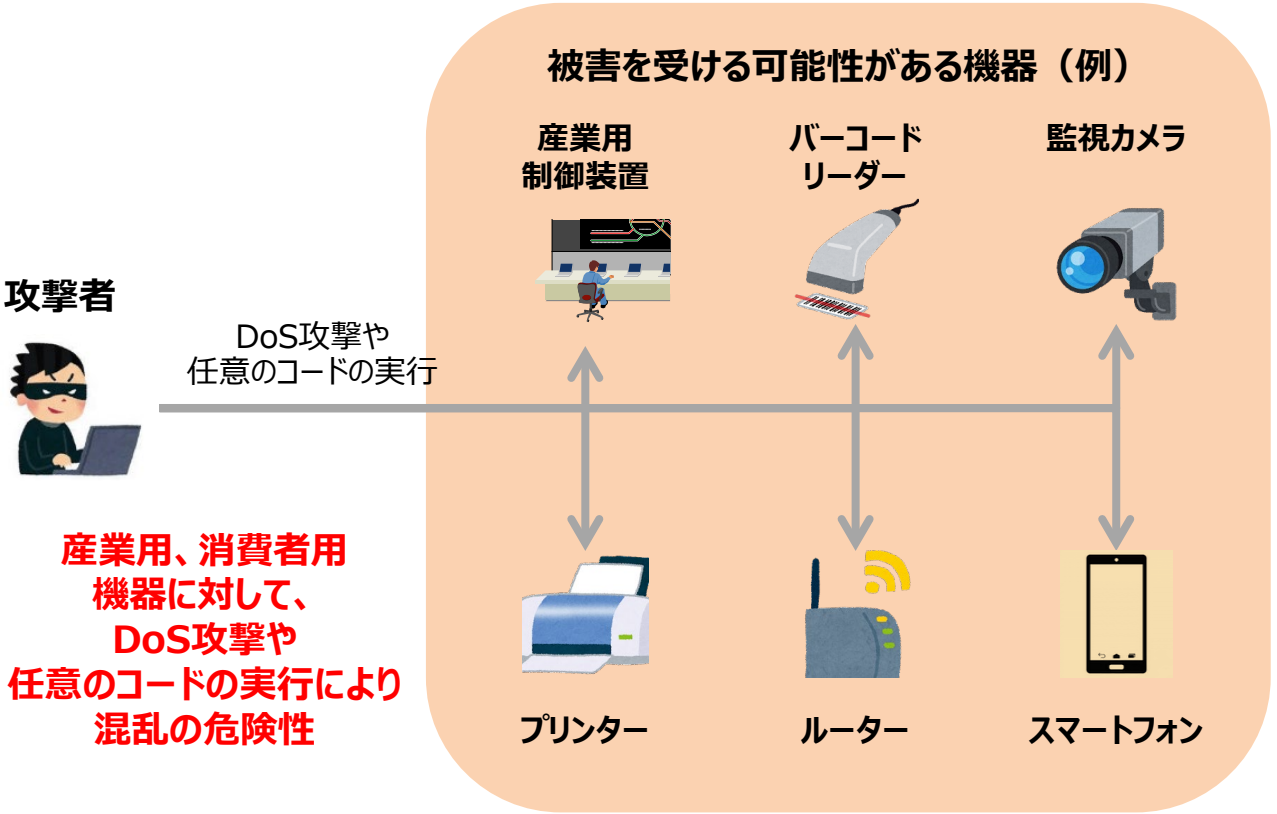


他にも、脆弱性を悪用することでこれらの監視カメラがKalayNetworkに送信した映像が盗み取られる危険性があるとしている。

TCP/IPスタックの脆弱性

- 2020年12月、Forescoutは、複数のオープンソースTCP/IPスタックに「Amnesia33」と呼ばれる脆弱性を発見した。また、2021年4月、ForescoutとJSOFは、複数のオープンソースTCP/IPスタックに「NAME:WRECK」と呼ばれる脆弱性を発表した。
- IoT機器におけるTCP/IPスタックに脆弱性が相次いで発見されており、それぞれの脆弱性が及ぼす影響は100万台から数100万台と言われている。

脆弱性の悪用イメージ



産業用、消費者用機器に対して、DoS攻撃や任意のコードの実行により混乱の危険性

脆弱性「Amnesia33」の影響範囲

以下のTCP/IPスタックを使用している機器

- uIP、Contiki OS、Contiki-NG
- Nut/Net
- FNET
- picoTCP、picoTCP-NG

脆弱性「NAME:WRECK」の影響範囲

以下のTCP/IPスタックを使用している機器

- FreeBSD
- IPnet
- Nucleus NET
- NetXzz

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

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

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

4. 本タスクフォースにおける検討事項

【米国】NIST IR 8259シリーズ

- IoT機器を管理する組織向けの推奨事項をまとめたNIST IR 8228に対し、**NIST IR 8259として、IoT機器の製造者に推奨される6つのサイバーセキュリティに関連する活動を整理**(2020年5月公開)。同時に公開された6つのコアサイバーセキュリティ機能を示したNIST IR 8259Aに続き、2021年8月には4つの非技術的サポート機能を定義したNIST IR 8259Bを公開。

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

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

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

IoT機器が備えるべき**6つのコアサイバーセキュリティ機能**を定義。

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

製造業者が製造するIoT機器をサポートするために導入を検討すべき、**4つの非技術的サポート機能（※）**を定義。
※①ドキュメンテーション（情報作成・収集）、②情報提供及び問合わせの受付、③情報発信、④教育及び意識醸成

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

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

NIST IR 8259D (Draft) 2020年12月ドラフト公開
Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government

8259Cに記載されているプロセスを用いて作成した**連邦政府向けプロファイル**を提供。

（参考）NIST IR 8259、8259A、8259B

- IoT機器の製造者に推奨される6つのサイバーセキュリティに関連する活動(NIST IR 8259)、6つのコアサイバーセキュリティ機能(8259A)、4つの非技術的サポート機能(8259B)を定義。

NIST IR 8259	販売前に影響する活動	活動1：想定顧客の特定、想定ユースケースの定義 活動2：顧客が有するサイバーセキュリティのニーズ及び目的の調査 活動3：顧客のニーズ及び目的への対処方法の決定（NISTIR 8259Aにてベースラインとなるコアサイバーセキュリティ機能を定義） 活動4：顧客のニーズ及び目的の適切なサポートに向けた計画（ハードウェア、ソフトウェアの適切なプロビジョニング、ビジネスリソースの考慮）
	販売後に影響する活動	活動5：顧客とのコミュニケーション手段の定義 活動6：顧客に伝える内容と伝達方法の決定（製造業者の設計・開発時のリスク関連の仮説、サポートと寿命、デバイス構成・機能、ソフトウェアの更新、デバイスの廃止オプション、技術的及び非技術的手段）

8259A	（１）**機器の識別**： IoT機器を論理的・物理的に一意に識別できる。	（４）**インターフェイスへの論理アクセス**： IoT機器のインターフェースへの論理アクセス、及びインターフェイスで利用されるプロトコルとサービスを正規のエンティティのみに制限できる。
	（２）**デバイスの構成**： IoT機器のソフトウェアの構成変更を、正規のエンティティのみが行うことができる。	（５）**ソフトウェアの更新**： IoT機器のソフトウェアは、安全かつ設定可能なメカニズムを用いる正規のエンティティにみによってのみ更新できる。
	（３）**データ保護**： IoT機器が保存・伝送するデータを不正アクセス及び改ざんから保護することができる。	（６）**サイバーセキュリティ状態認識**： IoT機器は自身のセキュリティに関する状態を報告し、その情報に対するアクセスを正規のエンティティのみに制限する。

8259B	（１）**ドキュメンテーション**： IoT機器の開発及びライフサイクル全体を通じて、IoT機器のサイバーセキュリティに関連する情報を作成、収集、保存する能力	（３）**情報発信**： IoT機器のサイバーセキュリティに関連する情報を発信する能力
	（２）**情報及び問合せの受付**： 顧客等からのIoT機器のサイバーセキュリティに関連する情報や問合せを受け付ける能力	（４）**教育及び意識**： IoT機器のサイバーセキュリティに関連する情報や考慮事項、機能等について、顧客等の意識を高め、教育する能力

【米国】国家のサイバーセキュリティの改善に係る米国大統領令の署名

- 2021年5月12日、バイデン大統領は、連邦政府機関におけるサイバーセキュリティ改善に係る大統領令に署名。
- **官民での脅威情報の共有**、**ソフトウェアサプライチェーンセキュリティ対策**の強化、**ゼロトラストアーキテクチャ**への移行等を通じて、連邦政府機関のサイバーセキュリティ対応能力の向上を図っている。

本大統領令における主な指示事項

1 **官民の脅威情報共有における障害の除去** (Section 2)	● ITサービスプロバイダーが連邦政府と確実に脅威情報を共有できるようにしたうえで、特定のインシデント情報の共有を義務づける。
2 **連邦政府におけるより強力な標準の近代化と導入** (Section 3)	● FedRAMP改定等を通じて、**連邦政府が安全なクラウド及びゼロトラストアーキテクチャに移行することを支援**し、多要素認証と暗号化の導入を義務づける。
3 **ソフトウェア・サプライチェーンのセキュリティ向上** (Section 4)	● NISTを通じて**政府が調達するソフトウェアの開発に関するセキュリティ基準(安全な開発環境の確保や構成要素に関する詳細（SBOM）の開示等を含む)を確立**し、特に**重要なソフトウェアに対して一定の対策を義務づけ**る。 ● 商務省は、既存のラベル表示などを参考にして、消費者向けの情報提供に関するパイロット制度を開始する。
4 **サイバー安全審査委員会の創設** (Section 5)	● 国土安全保障省は、**重大なインシデントが生じた際に政府と民間事業者が共同議長を務める「サイバー安全審査委員会」を設置**し、サイバーセキュリティ向上に向けた具体的な提言を行う権限を与える。
5 **インシデント対応のための標準プレイブックの策定** (Section 6, 7)	● 国土安全保障省は、連邦政府機関によるインシデント対応のためのプレイブックを策定する。 ● 連邦政府機関は、エンドポイント検知・対応(EDR)イニシアチブを展開し、インシデントの検知、積極的なサイバーハンティング、有事対応をサポートする。
6 **調査及び修復能力の向上** (Section 8)	● 連邦政府機関に対してセキュリティイベントログの要件を設け、侵入を検知し、対処する組織能力の向上を支援する。

（出典）各種公開情報より作成

【米国】DRAFT Baseline Security Criteria for Consumer IoT Devices

- 5月に公表された大統領令に基づき、NISTは消費者向けIoT機器、製品のベースラインセキュリティ基準のドラフトを公表。10月17日までの期間で意見募集を実施。
- 上記基準を活用した適合性評価やラベルの基準等については今後の検討事項とされる。

Executive Order on Improving the Nation's Cybersecurity (2021/5/12公開)
Sec.4. ソフトウェアサプライチェーンセキュリティの強化
(s) IoT機器のセキュリティ機能とソフトウェアの開発方法について一般の人々を教育するためのパイロットプログラムを開始
(t) 本命令の日付から270日以内に、**消費者向けラベリングプログラムのためのIoTサイバーセキュリティ基準**を特定

大統領令(EO)を受けて策定

DRAFT Baseline Security Criteria for Consumer IoT Devices (2021/8/31公開)

- **消費者向けIoT機器、製品* のベースラインセキュリティ基準(ドラフト)を提案**、同年10月17日まで意見募集を実施。
- 上記基準は、NIST IR 8259A及びNIST IR 8259Bを参照して策定された以下の機能群から構成されている。

1. IoT製品サイバーセキュリティ機能
- 資産の識別
- 製品の構成
- データ保護
- インターフェイスへの論理アクセス
- ソフトウェアの更新
- サイバーセキュリティ状態認識
- 製品セキュリティ

2. 非技術的サポート機能
- ドキュメンテーション
- 情報及び問合せの受付
- 情報発信
- 教育及び意識向上

3. 潜在的な追加のIoT製品基準
- 1. の分類に従って、特に複数の構成要素を含むIoT製品に適用され得る追加の基準を示している。

- 上記基準を活用した**適合性評価やラベルの基準等の策定については今後の検討事項**とされる。
- NISTは独自のプログラムを設けるのではなく、プロバイダや顧客がそれぞれの機器や環境に最適なソリューションを選択できるように望ましい成果を明示するとされている。

* 文書の表題では"IoT Devices"向けの基準とされているが、具体的な機能を記述している箇所ではIoT機器単体だけでなく関連する構成要素も含む概念である"IoT product"が対象として言及されている。

【欧州】NLF関連指令の改訂

- 欧州では、各NLF（New Legislative Framework）関連指令・規則にサイバーセキュリティの要素を盛り込む検討が進行。
- 今年4月に「機械製品規則案」、6月には「一般製品安全規則案」が公開。双方ともに現行「指令」を域内で直接適用する「規則」に置き換える。

名称	対象	サイバーセキュリティ関連措置等の概要
機械製品規則案 (Regulation on machinery products) **2021年4月21日公開**	機械、交換可能装置、安全構成部品等 (安全性に関する他のEU法の適用を受ける製品やその他の適用除外とされる製品カテゴリを除く) [Article 2, 3]	● 加盟国ごとの法制化が必要な「指令」を域内で直接適用する「規則」に置き換える。 ● 悪意のある第三者の行為で引き起こされ得る機械製品の安全性に係るリスクに対処する観点から、本提案では、Annex IIIにて必須安全要件(EHSR) 1.1.9を追加し、制御システムの安全性と信頼性に関するEHSR 1.2.1を明確化している。 ● EUサイバーセキュリティ法に従って採択されたスキームに基づいて認証された、または適合証明書が発行された機械製品で、参照先がEU官報に掲載されているものは、EHSRの上記要件に適合していると推定される。[Article 17(5)]
一般製品安全規則案 (Regulation on general product safety) **2021年6月30日公開**	EUの消費者を対象とする、または消費者が利用し得る全ての製品 (食品や医療製品、航空機等、安全性に関する他のEU法の適用を受ける製品を除く) [Article 2, 3]	● 機械製品規則案と同様、現行「指令」を域内で直接適用する「規則」に置き換える。 ● 製品の安全性評価において、以下の点を考慮することを求めている。[Article 7] (h) 悪意のある第三者を含む外的な勢力が製品の安全性に影響を与える可能性がある場合、当該勢力から製品を保護するために必要な適切なサイバーセキュリティ機能を備えていること ● 上記はサイバーセキュリティリスクの考慮を求めるものだが、本規則案において具体的なセキュリティ要件は定められていない。

【欧州】サイバーセキュリティ認証フレームワーク

- 「Cybersecurity Certification Framework」の創設を含む「Cybersecurity Act」は、2019年4月9日に欧州理事会で採択され、6月27日に発効。
- 「Cybersecurity Act」に基づき、ENISAが具体的な産業分野毎に「候補スキーム(Candidate Scheme)」を欧州委員会に提案し、順次、認証フレームワークが策定される予定。

欧州委員会、ENISAの動向

- 2019年4月、規則（Regulation）として、「Cybersecurity Act」が欧州理事会で採択、6月27日に発効。
- 2020年2月、ENISAがIoT、クラウドインフラ及びクラウドサービス、電子医療記録、トラストサービス等の4分野について、欧州サイバーセキュリティ認証フレームワークの「候補スキーム(Candidate Scheme)」を提案するホワイトペーパーを公開。
- 2020年7月、ENISAが最初の候補スキームでありCommon Criteriaに基づく「EUCC Candidate Scheme」のドラフト版を公開。
- 2020年12月、ENISAがクラウドサービスに関する候補スキーム「EUCS – CLOUD SERVICE SCHEME」のドラフト版を公開。
- 2021年2月、欧州委員会がENISAに5Gネットワークのための認証スキームの立案を指示。(2021年6月、アドホックWGの公募を実施)

Cybersecurity Actの概要

- 欧州委員会は、欧州サイバーセキュリティ認証スキームの対象となるICT製品、サービス、プロセス、カテゴリのリストを含む「Union rolling work programme」を発行。最初の「Union rolling work programme」は2020年6月28日までに発行される（Article 47）。
- 本スキームでは、ICT製品等について、インシデントの可能性と影響の観点を考慮し、「basic」、「substantial」または「high」のいずれかの保証レベルを1つ以上特定する（Article 52）。
- ICT製品等の製造者又は提供者は、保証レベル「basic」に対応する低リスクを示すICT製品等について、本スキームに示されている要件の充足が実証されていることを示すEU適合宣言をボランタリーに発行することができる（Article 53）。
- 本スキームには、評価に適用される国際規格、欧州規格又は国内規格への参照及び第三国との認証制度の相互承認のための条件等が含まれる（Article 54）。
- 欧州委員会は、サイバーセキュリティ認証スキームが義務づけられることによって、ICT製品等の適切なレベルのサイバーセキュリティを確保し、国内市場の機能を改善することに効果があるか定期的にアセスメントを行う。最初のアセスメントは2023年末までに行われ、その後は少なくとも2年ごとに行われる（Article 56）。

（参考）ENISA：Cybersecurity Certification - EUCC Candidate Scheme

- EUCC Candidate Schemeは、ICT製品を対象とするCommon Criteria（CC：ISO/IEC15408）と、関連する共通評価方法（ISO/IEC 18045）に基づく欧州サイバーセキュリティ認証フレームワークにおける最初の候補スキーム。欧州においてSOG-IS※1の下で運用されていた既存のCCのスキームの後継として機能させることが目的。**2021年5月、ドラフト版への意見募集を経て、用語の定義や他ステークホルダーとの協力について追記されたV.1.1.1が発行。**

※1欧州におけるCC加盟国の認証機関間の調整を行う組織

- 本文書では、評価はCCに基づくものであること（3章）、保証レベルは「substantial」か「high」の2段階であること（4章）、自己適合性評価は認められないこと（5章）、認証証明書の有効期間は最長5年間であること（20章）等、**Cybersecurity Actにより候補スキームに必要とされる要件**（認証取得の際に実装すべき要求事項やその評価プロセス、認証制度の運用等に関する事項等）**を網羅的に規定**。

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

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

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

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

(参考) ENISA : EUCS - Cloud Services Scheme

- EUCS–Cloud Services Schemeは、 欧州クラウドサービスを対象にEUサイバーセキュリティ認証制度を構築することを目的として作成された認証スキームである(2020年12月ドラフト版発行)。
- 本文書にはクラウドサービスプロバイダーが認証取得するために満たすべき技術的要件及び目的等が定められており、個別の技術的要件ごとに、「Cybersecurity Act」によって定義された「high」、「substantial」、「basic」の3つの保証レベルが定められている。なお、本スキームはvoluntaryであるとしている。

認証取得するために満たすべき技術的要件(大項目)

No.	項目	No.	項目
1	情報セキュリティのための組織	11	ポータビリティ及び相互運用性
2	情報セキュリティポリシー	12	変更管理及び構成管理
3	リスクマネジメント	13	情報システムの開発
4	人的資源	14	調達管理
5	資産の管理	15	インシデント管理
6	物理的セキュリティ	16	事業継続
7	運用のセキュリティ	17	順守
8	ID、認証及びアクセス管理	18	ユーザードキュメント
9	暗号化及び鍵管理	19	政府機関からの調査依頼への対応
10	通信のセキュリティ	20	製品のセーフティ及びセキュリティ

３つの保証レベル

保証レベル	説明
high	**<対象> mission-criticalなデータ、システムを扱うサービス** <攻撃者プロファイル> 高度なスキルを持ったチーム <評価> substancialに加え、管理策の自動監視及び適切な要員によって実施される**複数年に渡り計画されるペンテストや技術的レビュー**
substantial	**<対象> business-criticalなデータ、システムを扱うサービス** <攻撃者プロファイル> 様々な既知のハッキング手法にアクセスできるが、リソースが限られている小さなチーム <評価> basicに加え、インタビューやサンプル検査、**設計どおり実装されているかの検証**を含むオンサイト監査、**既知の攻撃手法を使ったペンテスト**
basic	**<対象> 重要でないデータ、システムを扱うサービス** <攻撃者プロファイル> 限られたスキルのみを有し、限られたリソースにより既知の攻撃を繰り返す一人の人物 <評価> 事前定義された監査計画に沿った、技術的・組織的な措置(CSP自身による**自動化された既知の脆弱性やコンプライアンスに係る検査**を含む)の履行を確認するための**書類確認**

【欧州】NIS指令の改正

- 2020年12月、欧州委員会は、域内の重要インフラ事業者等のサイバーセキュリティ対策について規定するNIS指令(Directive (EU) 2016/1148)の改訂案を公表。
- 現行指令から、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）。

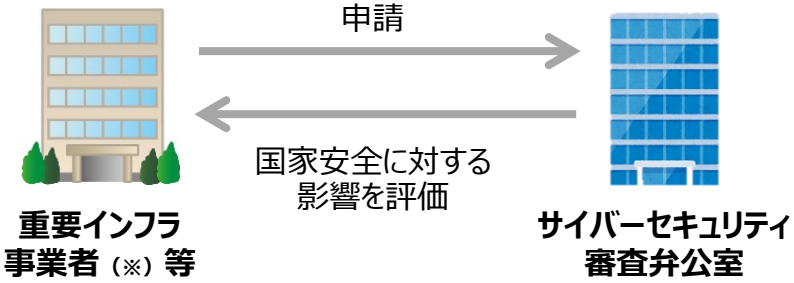
【中国】サイバーセキュリティー審査弁法改定に向けた意見募集の実施

- サイバーセキュリティー審査弁法は、2017年に施行されたサイバーセキュリティ法を受け、重要インフラ事業者を対象に、ネットワーク製品やサービス調達後の国家安全へのリスク判定を行うためのサイバーセキュリティ審査弁室への審査申請を義務づけることを目的として施行された法律である。（2020年6月施行）
- 2021年7月10日に、新たに改正されたサイバーセキュリティー審査弁法が意見募集に付された。（2021年7月24日期限）なお、改正にあたって、審査の適用範囲が拡大されている。

サイバーセキュリティー審査弁法

- **重要インフラ事業者はネットワーク製品、サービスを調達する場合には、導入後の国家安全へのリスク判定が必要であり、国が実施するサイバーセキュリティ審査に合格しなければならないと、当該法では定められている。**
- **当該法は、2017年6月に施行されたサイバーセキュリティ法を受けて施行された。**

■イメージ



改正によって新たに設けられた条文（例）

- 100万件を超える個人情報を保有する事業者が**国外で上場する**際、サイバーセキュリティ審査弁公室にサイバーセキュリティ審査を申請する必要がある。（6条）
- サイバーセキュリティ審査を申請する際に、当該事業者が上場を計画している場合、**IPO（新規株式公開）の審査書類を提出**しなければならない。（8条）

※重要インフラ事業者とは、公共通信・情報サービス、エネルギー、交通、水利、金融、公共サービス、電子行政サービスなどの重要な産業および分野、ならびにひとたび機能の破壊、喪失またはデータの漏えいに遭遇した場合、国の安全、国民経済と民生、公共の利益に重大な危害を与え得るその他の重要情報インフラの事業者を指す

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

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

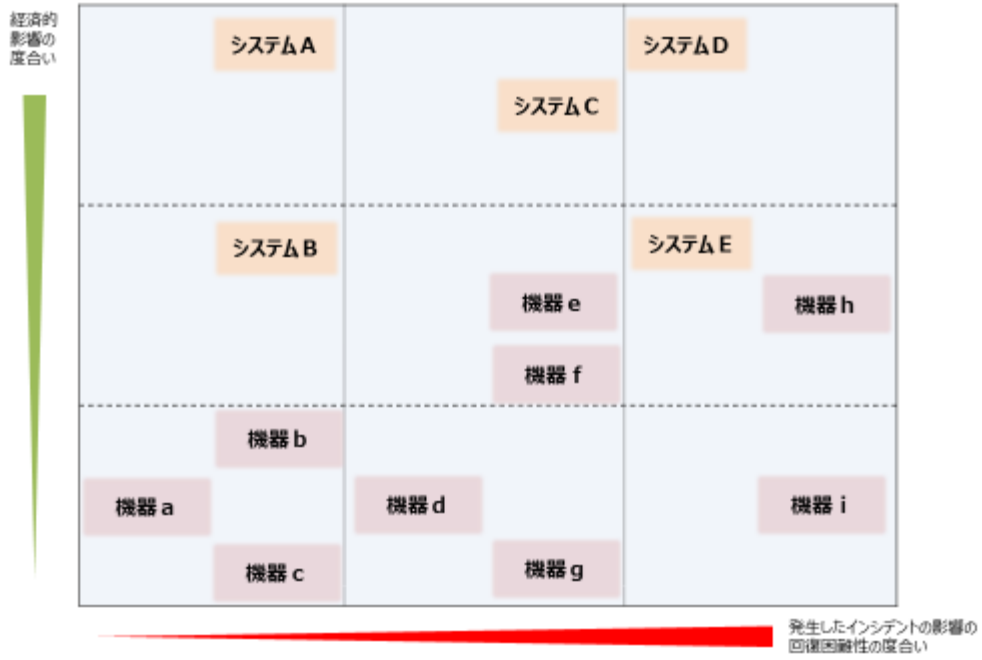
3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に向けた諸外国の検討状況

4. 本タスクフォースにおける検討事項

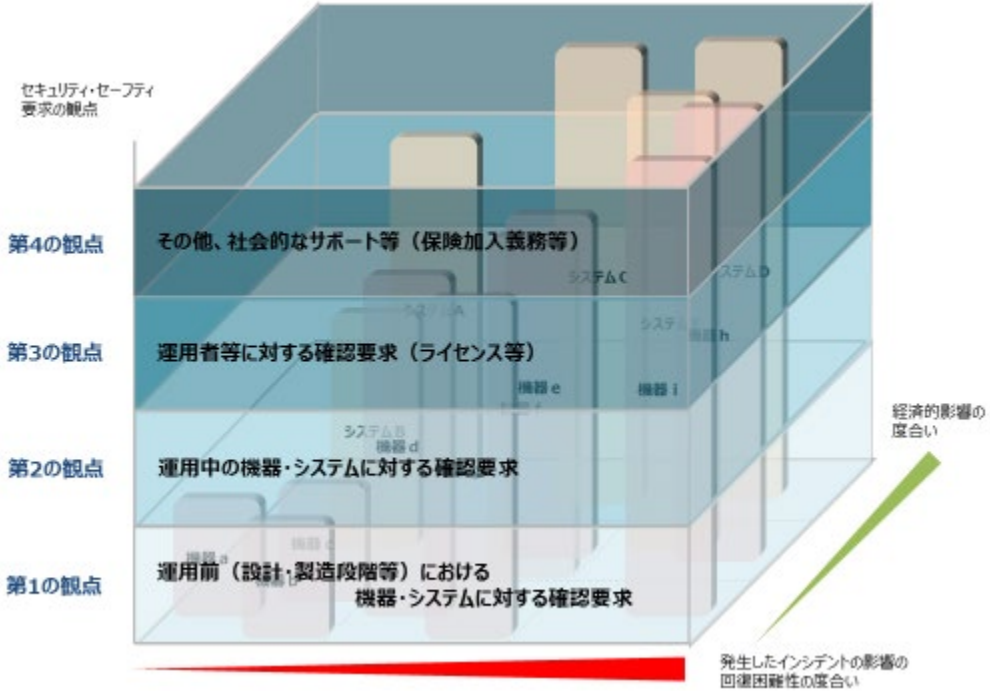
IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の策定

- **用途や使用環境によって課題が異なるIoT機器・システムに対するセキュリティ対策を、複数のステークホルダー間で合意する**際に活用できる**「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」を2020年11月5日に公開。**
- 本フレームワークで、IoT機器・システムをカテゴライズし、カテゴリごとに求められるセキュリティ・セーフティ要求の観点を把握・比較することにより、**それぞれに求める対策の観点・内容の整合性を確保できる**。

フィジカル・サイバー間をつなげる
機器・システムのカテゴライズのイメージ



カテゴリに応じて求められる
セキュリティ・セーフティ要求の観点のイメージ



※　同じ機器・システムでも使用形態などによってマッピング先が異なり得る。
例えば、機器ｇと機器ｈが同じ機器で異なる使用形態である場合などがあり得る。）

IoT-SSFのユースケース作成

- 前回までのTFやパブリックコメントにて寄せられたご意見を踏まえ、IoT-SSFをより活用しやすいものにすることを目的として、IoT-SSFのユースケースを作成する。

＜寄せられたご意見＞

- IoT-SSFがIoT機器・システムのセキュリティに係る様々な主体に適用可能な「基本的共通基盤」を提供していることを評価する。
- 一方で、IoT-SSFには抽象度が高い部分も含まれているため、読者にとって理解が難しい部分がある可能性がある。
- IoT-SSFにて示されたリスクのマッピング手法やカテゴライズ手法に関する指針もしくはガイドラインの整備が必要ではないか。

＜本文での記載＞

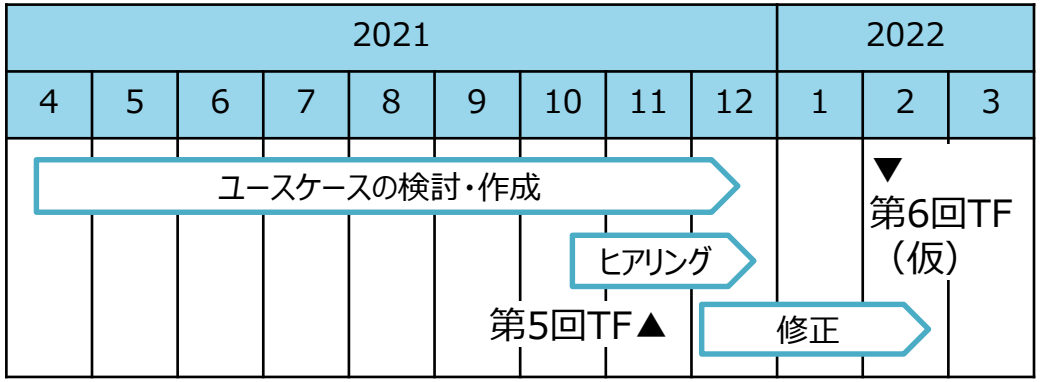
- 今後、本フレームワークに基づいて、具体的な仕組み・サービスをユースケースとして整理していくことで、IoT が広く活用されるサイバー空間とフィジカル空間が高度に融合した社会におけるセキュリティ・ セーフティ対策を適切に実施していく制度的対応の整備を進めていくための基礎的条件を整えて行く必要がある。

IoT-SSFのユースケース作成

- R3年度内に、IoT-SSFのユースケース集を作成し、IoT-SSFの付属文書として公表予定。

＜作成スケジュール＞

- 令和3年度内に、5つ程度のユースケースを検討・作成する。
  （ユースケースの対象については、
  次頁以降を参照のこと。）
- ユースケースの作成前後に、各ユースケースに関連する企業等へヒアリングを行う。



＜アウトプットイメージ＞

- ユースケース集（詳細をまとめた文書と概要スライド）を、IoT-SSFの付属文書として公表予定。

文書の目次（案）

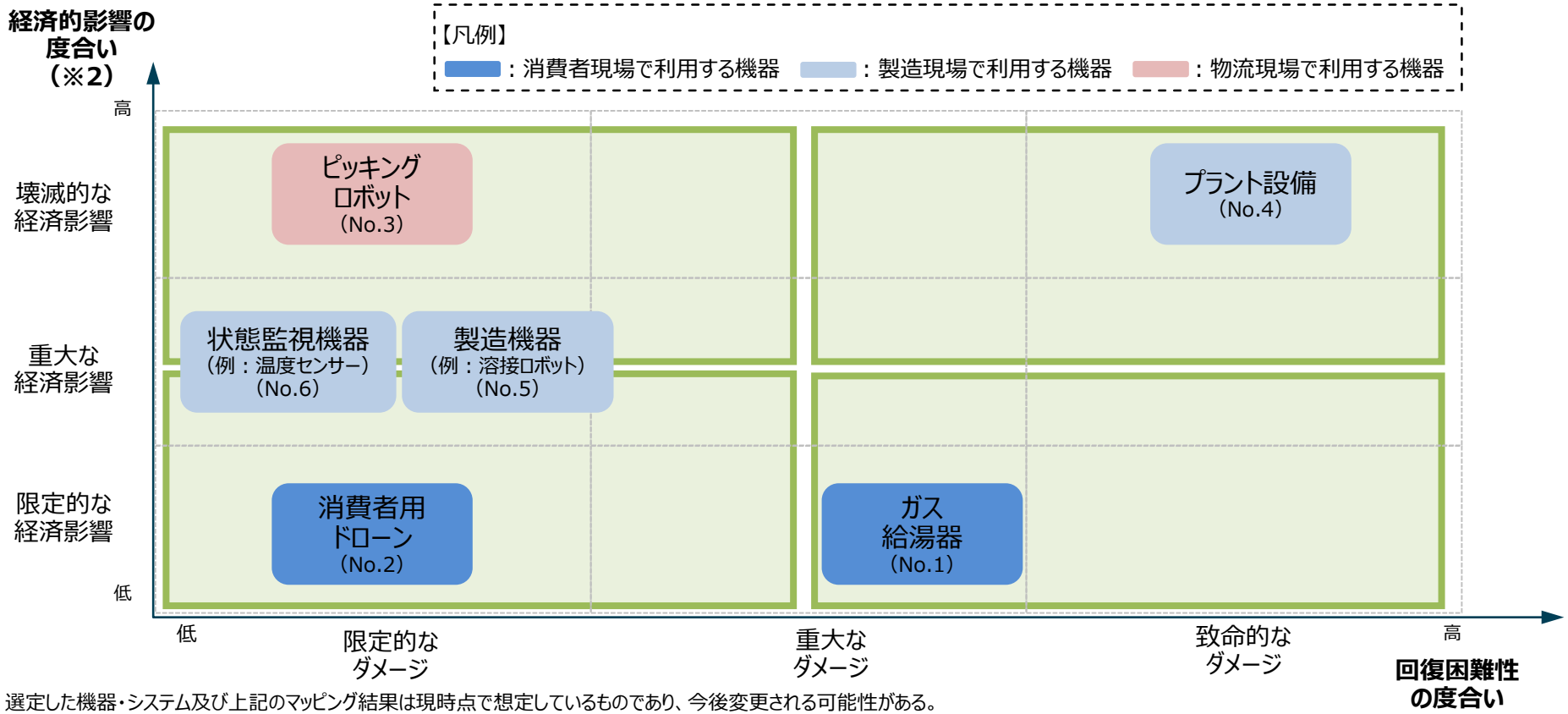
1. 本文書の位置付けと構成
   - 1-1「IoTセキュリティ・セーフティ・フレームワーク」の概要
   - 1-2 本文書の目的と構成
   - 1-3 想定読者
2. 「IoTセキュリティ・セーフティ・フレームワーク」実践に係るユースケース集
   - 2-1 対象となるユースケース
   - 2-2 ユースケースにおける記載事項
   - 2-3 具体的なユースケース

添付A 対策要件

添付B 対策例

ユースケース選定の考え方

- IoT機器・システムが導入される用途の例として、消費者用および産業用（製造、物流）を想定し、わかりやすさや多様性を考慮して選定。
- その上で、第１軸：回復困難性の度合いと、第２軸：経済的影響の度合いに応じ、なるべくマッピングの偏りが少なくなるように配慮し、各々の現場の分類から具体的な機器・システムを選定※１。



※1：選定した機器・システム及び上記のマッピング結果は現時点で想定しているものであり、今後変更される可能性がある。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

ユースケース一覧（案）

- 前頁の考え方に基づき、詳細化を進める対象として、以下の6ケース（※）を選定した。

No	ユースケース	IoT機器を導入する現場	（参考）リスクの大きさ	
			回復困難性の度合い	経済的影響の度合い
本TFにて提示するユースケース				
1	ガス給湯器の遠隔操作（ガス給湯器）	消費者現場	大	小
2	ドローンを活用した個人による写真撮影（ドローン）	消費者現場	小	小
3	物流倉庫における自動ピッキング（ピッキングロボット）	物流現場	小	大
4	プラント施設内の設備（プラント設備）	製造現場	大	大
5	工場における部材加工作業の自動化（例：溶接ロボット）	製造現場	小	中
6	金属製造現場における状態監視用機器（例：温度センサー）	製造現場	小	中

※オレンジ網掛けは、現在作成中のユースケース。なお、オレンジ網掛け以外のユースケースについては、今後具体化予定

リスク評価、リスク対応に向けた事前準備の記載イメージ
人の注意が行き届かない状態で動作する家電製品、ガス製品の遠隔操作

- 「サイバー・フィジカル・セキュリティ対策フレームワーク」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する。

1 リスク評価、リスク対応に向けた事前準備	2 リスク評価	3 リスク対応 (ステークホルダー別の対策要件一覧)
●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	●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。	● 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

分野共通のリスク評価に関する考え方（１）

- 分野共通のリスク評価に関する考え方をIoT-SSFの記載を具体化する形で整理した。

回復困難性の度合い

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

分野共通のリスク評価に関する考え方（２）

- 分野共通のリスク評価に関する考え方をIoT-SSFの記載を具体化する形で整理した。

経済的影響の度合い

※：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

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

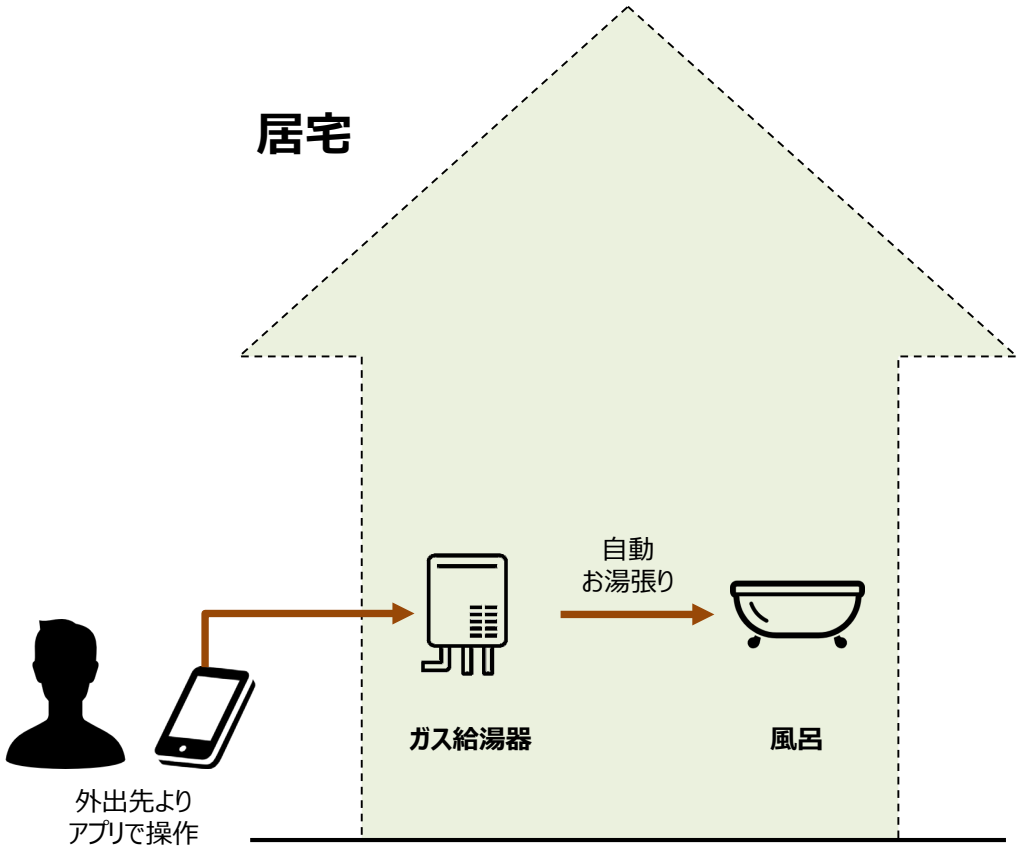
リスク評価、リスク対応に向けた事前準備の記載イメージ

ガス給湯器の遠隔操作（ガス給湯器）

- 「人の注意が行き届かない状態で動作するガス給湯器の遠隔操作」では以下を想定している。

- 外出先よりスマートフォンの専用アプリケーションを活用して、自宅のお風呂のお湯張りを行う。
- なお、ガス給湯器は「自然給排気式・開放式」以外の機器を想定している。これは、「液化石油ガス器具等の技術上の基準等に関する省令の運用について」（令和2年7月）にて「自然給排気式・開放式」の遠隔操作が禁止されているため。（※1）

※1経済産業省「液化石油ガス器具等の技術上の基準等に関する省令の運用について」（令和2年7月）では、「自然吸排気式」及び「開放式」以外の機器において「リスク低減策を講じることにより遠隔操作に伴う危険源がないと評価されるもの等の基準に合致し、危険が生ずるおそれがないものは、操作可能」とされている。



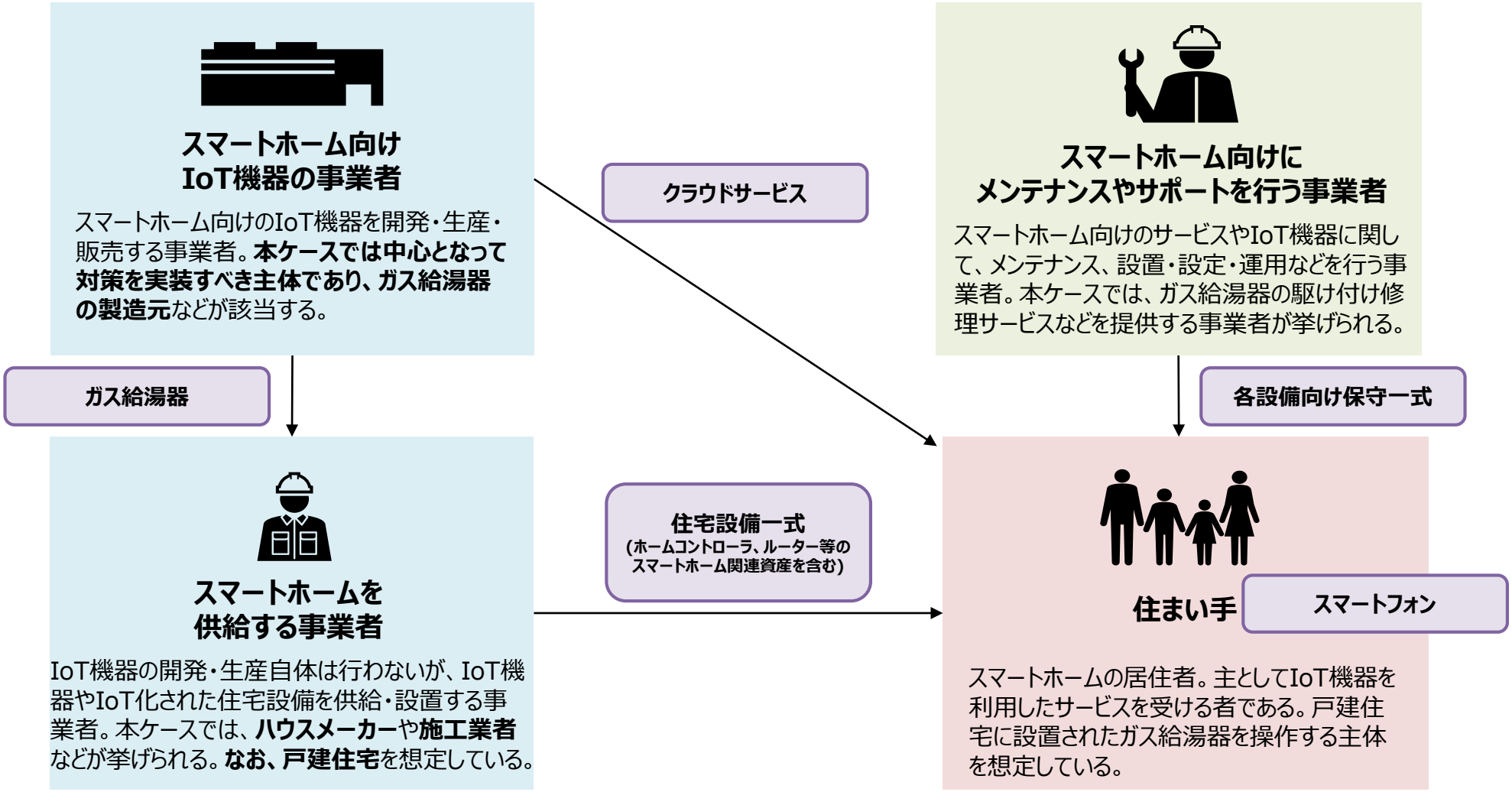
[出典] 経済産業省「令和２年度 産業保安等技術基準策定研究開発等事業 （電気用品等製品の IoT 化等による安全確保の在り方に関する動向調査）」等を参考に作成

リスク評価、リスク対応に向けた事前準備の記載イメージ

事前準備 リスク評価 リスク対応

ガス給湯器の遠隔操作（ガス給湯器）

- 本ユースケースにおけるステークホルダー関係図は以下を想定している。



[出典] 経済産業省「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドラインスマートホームガイドライン」等を参考に作成

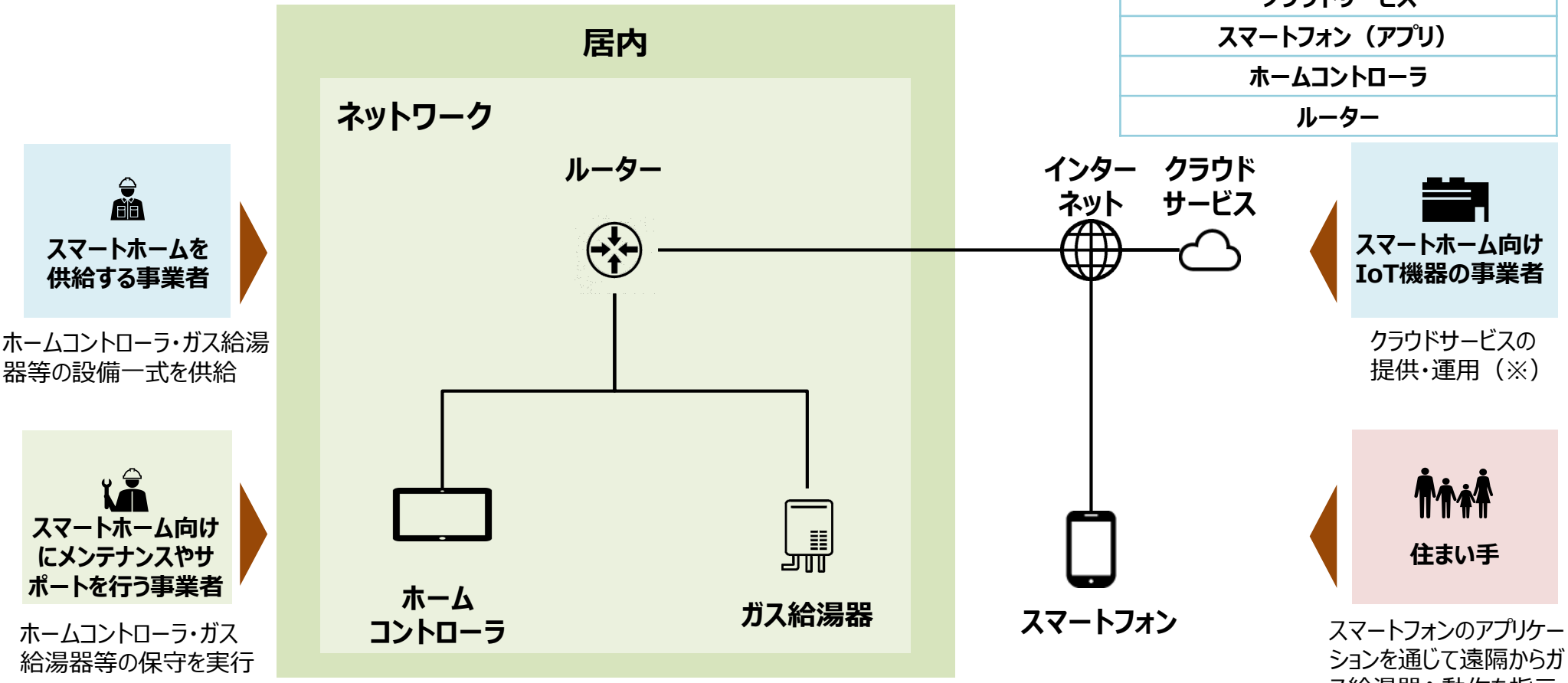
リスク評価、リスク対応に向けた事前準備の記載イメージ

事前準備 リスク評価 リスク対応

ガス給湯器の遠隔操作（ガス給湯器）

- システム構成図、システムを構成する機器の一覧は以下を想定している。

システムを構成する機器の一覧
ガス給湯器
クラウドサービス
スマートフォン（アプリ）
ホームコントローラ
ルーター



※実際の運用は他のITサービス事業者に委託する場合がある。

[出典] 経済産業省「令和２年度 産業保安等技術基準策定研究開発等事業 （電気用品等製品の IoT 化等による安全確保の在り方に関する動向調査）」等を参考に作成

リスク評価に係る内容の記載イメージ

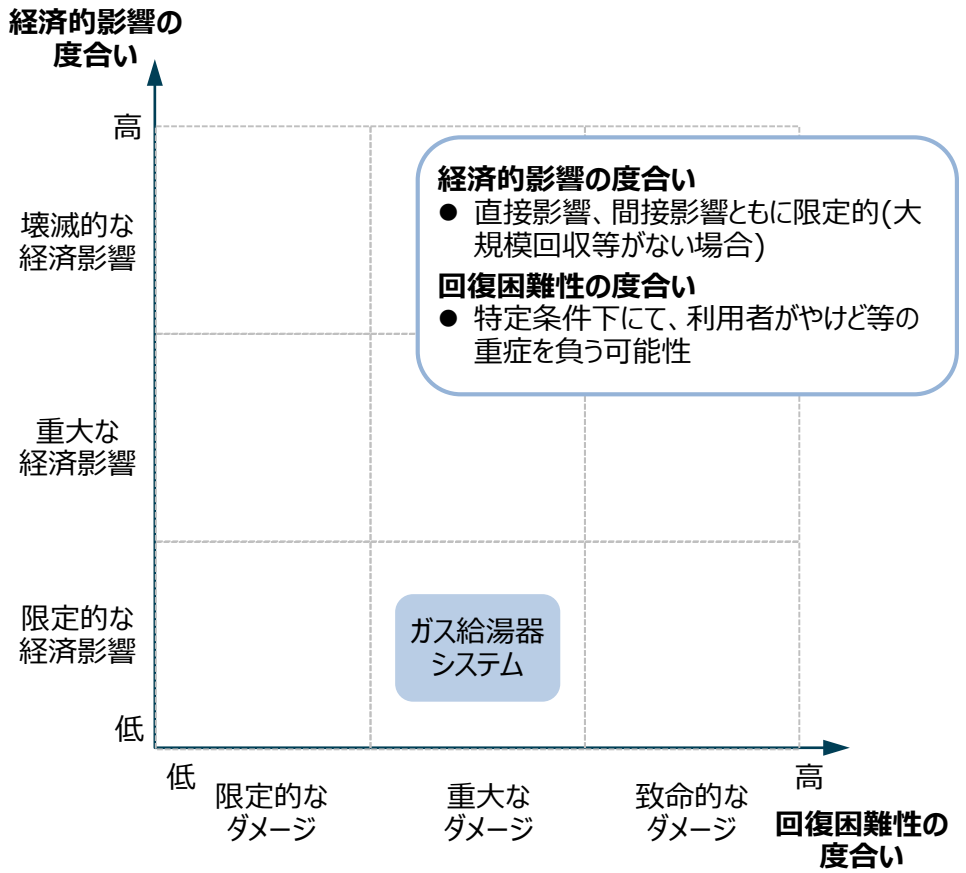
ガス給湯器の遠隔操作（ガス給湯器）

- 「回復困難性の度合い」及び「経済的影響の度合い」の判断基準を考慮し、ガス給湯器システムをマッピングした。

リスクの大きさ

回復困難性の度合い		経済的影響の度合い	
重大なダメージ	[プライバシーの観点] スマートフォン・アプリのアカウント情報が漏洩する可能性がある。	限定的な経済影響	[内部への経済影響] 経済活動の中断等は生じ難い。
			[外部への経済影響] 利用環境(住居)外部への影響は及びにくい。
			[影響の継続時間] ガス給湯器の修理や交換に一定の時間を要する可能性がある。
	[セーフティの観点] 利用者がやけど等の重症を負う可能性がある。		[代替可能性] 停止期間中、給湯が不可能になるものの、外部サービスを利用できる場合が一般的。
			[間接被害の規模] ガス給湯器の修理や交換に一定のコストを要する可能性があるものの、範囲は限定的。

マッピング結果



※：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

リスク対応に係る内容の記載イメージ
ガス給湯器の遠隔操作（ガス給湯器）

- 「リスク評価、リスク対応に向けた事前準備」にて整理した資産ごとに脅威を整理する。

システムを構成する機器の一覧	想定される脅威（例）
ガス給湯器	情報漏えい
	マルウェア感染
	不正利用
	利用者による誤操作
ホームコントローラ	マルウェア感染
	不正利用
ルーター	不正アクセス
	不正利用
スマートフォン・アプリ	情報漏えい
	マルウェア感染
	不正利用
	利用者による誤操作
クラウドサービス	データの改ざん
	情報漏えい
	サービス不能
	不正アクセス
	マルウェア感染
	利用者による誤操作

[出典] 情報処理推進機構「IoT開発におけるセキュリティ設計の手引き」等を参考に作成

リスク対応に係る内容の記載イメージ
ガス給湯器の遠隔操作（ガス給湯器）

- 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」における観点及び主に対策を実施すべき主体ごとに、有効と考えられる対策を列挙する。

第3軸「求められるセキュリティ・セーフティ要求」の観点ごとに対策を整理した上で、主に対策を実施すべき主体ごとに対策を振り分けることが望ましい。

No	第3軸	適用対象	主に対策を実施すべき主体	想定される脅威（例）	対策要件	対策（例）
1	第1の観点	ソシキ・ヒト	スマートホーム向けIoT機器の事業者	• 全般	**運用前（設計・製造段階）IoTセキュリティを目的とした体制の確保**	• 経営陣の支援を得た上で、セキュリティ対応部門を立ち上げ、所掌範囲にガス給湯器システム等やその他の自社の製品・サービスを含める等、総合的にセキュリティ対策を実施できる体制を整える。 • ・・・
2					・・・	・・・
3		システム		• 不正アクセス • マルウェア感染	IoT機器・システムの提供における安全な初期設定と構成	• スマートフォンアプリやガス給湯器等におけるユーザーログイン用のパスワードを一定のポリシーに沿って統合的に管理する。 • ・・・
4					・・・	・・・
5		ソシキ・ヒト	住まい手		・・・	・・・
6		システム			・・・	・・・
7		・・・	・・・		・・・	・・・
8	第2の観点	ソシキ・ヒト	・・・		・・・	・・・
9		プロシージャ	・・・		・・・	・・・
10		システム	・・・		・・・	・・・
11	第3の観点	・・・	・・・		・・・	・・・
12	第4の観点	・・・	・・・		・・・	・・・

[出典] 経済産業省「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドラインスマートホームガイドライン」等を参考に作成

リスク対応に係る内容の記載イメージ
ガス給湯器の遠隔操作（ガス給湯器）

- 機器・システムの能力や利用環境の特性、かかるコスト、関連する法令の規定等の各ユースケースにおける個別の事情を勘案し、実際に講じる対策を調整することで、効果的かつ効率的な要件の具体化を行う。
- 各主体にとって許容可能な範囲までリスクを低減することを前提に、効率的に（低コストで）かつ、各事業者の負荷を軽減させる形で要件を実装することが重要。

主に対策を実施すべき主体	対策要件	実際に講じる対策（例）
スマートホーム向けIoT機器の事業者	運用前（設計・製造段階）IoTセキュリティを目的とした体制の確保	• ガス給湯器システムを対象としたセキュリティ管理責任者及びセキュリティ対策担当者の任命
	IoT機器・システムの提供における安全な初期設定と構成	• ガス給湯器システムを構成する機器の不要なネットワークポート、その他USBやシリアルポートなどの物理的または論理的な閉塞
	…	…
スマートホームを供給する事業者	IoT機器・システムにおける運用開始時の正しい設置、設定	• IoT機器の事業者の想定する仕様に適合したネットワーク環境の整備
	…	…
スマートホーム向けにメンテナンスやサポートを行う事業者	サービス提供や管理のポリシーの提示・遵守	• セキュリティパッチの適用手順の提示
	…	…
住まい手	IoT 機器・システムの用途・用法を守った使用	• 仕様書や手順書を把握し、想定された用途・方法でのガス給湯器の利用
	…	…

機器・システムの能力や利用環境の特性、かかるコスト、関連する法令の規定等を勘案し、実際に講じる対策の内容を調整する。

[出典] 経済産業省「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドラインスマートホームガイドライン」等を参考に作成

ご議論いただきたい事項

- ユースケースの対象 【Ｐ28】
  - 現在、提示しているケースについて
  - 今後、ユースケースに追加することを念頭に議論すべきケースについて
- 回復困難性の度合い、経済的影響の度合いの判断基準 【Ｐ30,31】
- ユースケースの整理の仕方 【Ｐ32～38】
- ユースケース作成後の扱い（普及のあり方等）
- その他