経済産業省

最近の産業サイバーセキュリティに関する動向について

令和4年2月

経済産業省　商務情報政策局

サイバーセキュリティ課

１．サイバーセキュリティに関する動向

２．産業サイバーセキュリティ研究会の検討状況
- 第３層TF
- 第２層TF
- ソフトウェアTF

３．IoT機器に対するセキュリティ対策

１．サイバーセキュリティに関する動向

２．産業サイバーセキュリティ研究会の検討状況

- 第３層TF
- 第２層TF
- ソフトウェアTF

３．IoT機器に対するセキュリティ対策

情報セキュリティ10大脅威　2022（1月27日公表）

順位	「組織」向け脅威	昨年順位
1	**ランサムウェアによる被害**	**1**
2	標的型攻撃による機密情報の窃取	2
3	**サプライチェーンの弱点を悪用した攻撃**	**4**
4	テレワーク等のニューノーマルな働き方を狙った攻撃	3
5	内部不正による情報漏えい	6
6	脆弱性対策情報の公開に伴う悪用増加	１０
7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
8	ビジネスメール詐欺による金銭被害	5
9	予期せぬIT基盤の障害に伴う業務停止	7
１０	不注意による情報漏えい等の被害	9

出典：IPA資料（ https://www.ipa.go.jp/security/vuln/10threats2022.html ）

工場におけるサイバー攻撃事例

- アルミニウム工場のマルウェア感染（2019年、ノルウェー）

事象

- ✓ ノルウェーのアルミニウム製造大手で大規模なマルウェア感染
- ✓ 「LockerGoga」と呼ばれるランサムウェアに感染
- ✓ 発生直後、プレス加工等の一部生産、オフィス業務に影響
- ✓ プラントは影響拡散防止のためシステムから分離
- ✓ 被害は、最初1週間で3億～3億5000万ノルウェークロネ（4000万ドル相当）と推定

- 石油化学プラントの安全計装システムを狙ったマルウェア（2017年、中東）

事象

- ✓ 中東の石油化学プラントで使用されていた Schneider Electric 社製の SIS コントローラー(Triconex)がマルウェア感染
- ✓ SISのエンジニアリング・ワークステーションへのリモートアクセスを取得、SISシステムのゼロデイ脆弱性を利用して改ざん
- ✓ プラントが緊急停止

- 自動車工場のマルウェア感染（2017年、日本）

事象

- ✓ 大手自動車メーカーの工場でコンピュータがWannaCryに感染
- ✓ 工場に据え付けの設備に付属するパソコンが感染
- ✓ 生産ラインの制御システムに影響が発生し、一時的にラインを停止
- ✓ 約1千台の車両生産に影響

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

<u>コロニアル・パイプライン</u>

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。

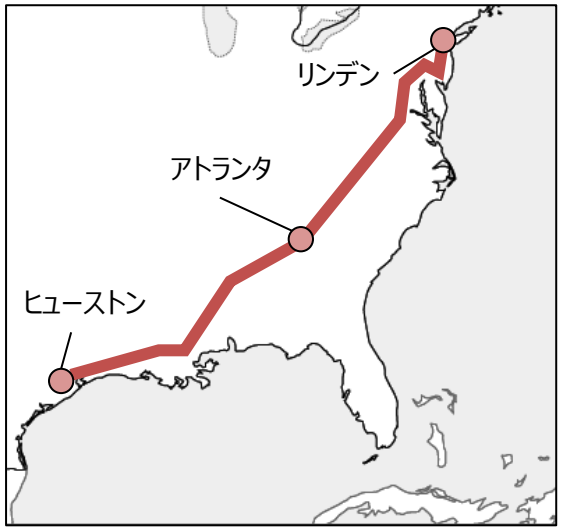
<u>米運輸省による緊急措置の内容</u>

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。

<u>米CISAによる声明のポイント</u>

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。

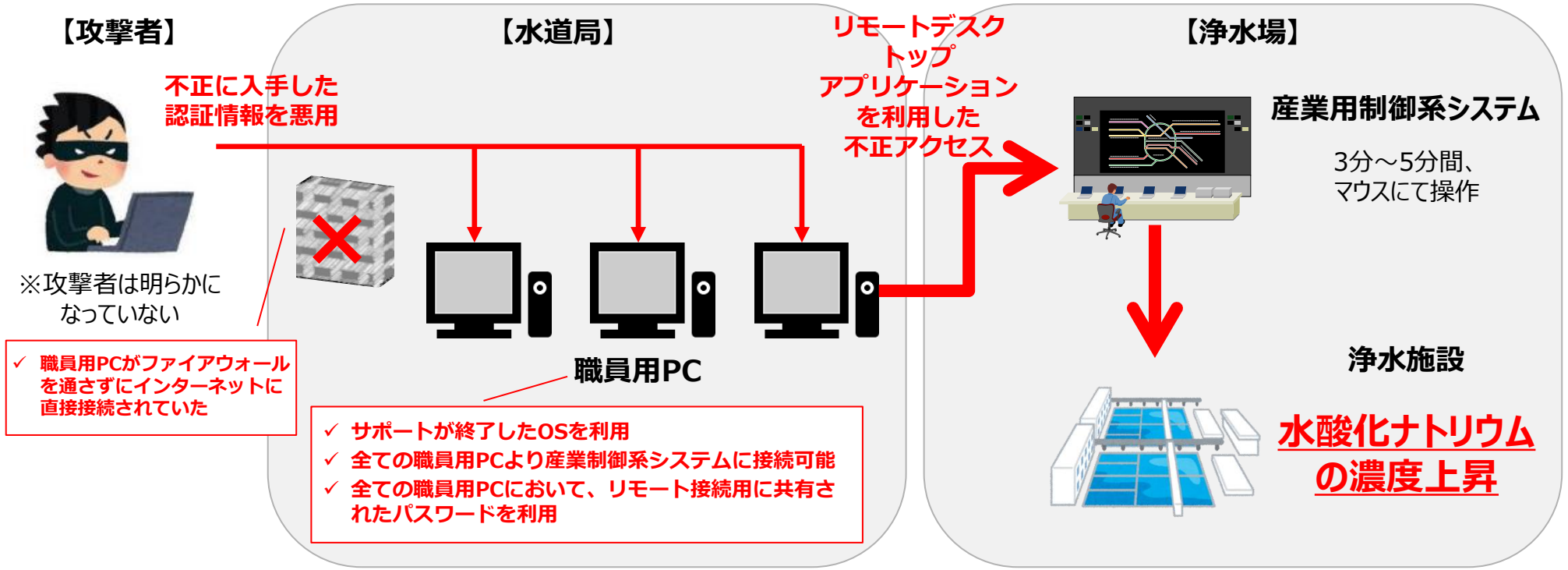
・被害企業と関係官庁とともに本事案に対処中。
・ランサムウェアは組織の規模、セクターに関係なく直面する脅威。
・この種の脅威に晒されるリスクを減らすためサイバーセキュリティ体制を強化する措置を講じることを各組織に推奨。



コロニアル・パイプラインの
主要パイプライン（イメージ）

水道システムへの不正アクセス事例

- 2021年2月、アメリカフロリダ州オールズマー市水道局は、**水道における産業用制御系システムを対象とした不正アクセス**によって、飲用水に含まれる水酸化ナトリウムの量が一時的に通常の約100倍に上昇したと発表した。なお、オペレーターが異常に気付き、即座に設定を戻したため、実際の被害はなかったとされる。
- 報道によると、**職員用PCよりリモートデスクトップアプリケーションを利用して、**産業用制御系システムへの不正アクセスが行われたとされている。

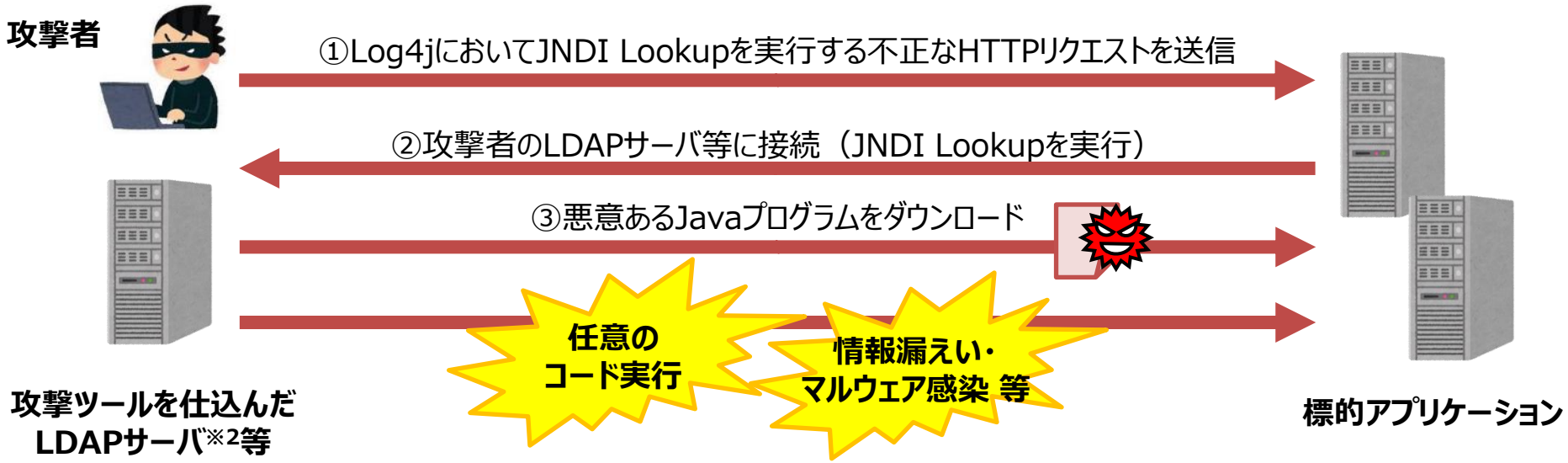


（出典）各種公開情報に基づき経済産業省作成

Apache Log4jの脆弱性：Log4Shell（CVE-2021-44228）

- 2021年12月9日、Javaベースのオープンソースログ出力ライブラリ**Apache Log4jにおける任意コード実行の脆弱性が発表**された。当該脆弱性はLog4jのJNDI Lookup※1機能に起因するもので、Log4Shellとも呼ばれる。
- この脆弱性を悪用することで、**Log4jが動作するアプリケーションに対して外部からの任意コード実行が可能**となり、情報漏えいやマルウェア感染等の被害に繋がる恐れがある。
- Log4jの脆弱性はその後も相次いで発見されており、12月14日には**情報漏えいや任意コード実行に関する脆弱性**（CVE-2021-45046）、12月18日には**DoS攻撃に関する脆弱性**（CVE-2021-45106）が公表された。
- 12月17日、米国CISAは、既に脆弱性が悪用されている状況を鑑み、**すべての連邦政府機関に対し、Log4jのバージョンアップや緩和策を講じることで脆弱性に対処するよう求める緊急指令を発出**した。

◆ **Log4Shell（CVE-2021-44228）を悪用した攻撃のイメージ**



https://logging.apache.org/log4j/2.x/security.html
https://www.ipa.go.jp/security/ciadr/vul/alert20211213.html
https://www.cisa.gov/news/2021/12/11/statement-cisa-director-easterly-log4j-vulnerability

※1：Javaプログラムで標準的に利用される機能で、必要なデータを含むJavaオブジェクトを検索する機能
※2：特定のキーに対応する情報を返すサーバ

１．サイバーセキュリティに関する動向

２．産業サイバーセキュリティ研究会の検討状況

- 第３層TF
- 第２層TF
- ソフトウェアTF

３．IoT機器に対するセキュリティ対策

産業サイバーセキュリティ研究会とWGの設置による検討体制

産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催
　アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日　開催
　アクションプランを加速化する３つの指針を提示
第４回：令和2年　　4月17日　開催（電話開催）
　産業界へのメッセージを発信
第５回：令和2年　　6月30日　開催
　サイバーセキュリティ強化運動の展開
第６回：令和３年　　４月２日　開催
　アクションプランの持続的発展と、新たな課題へのチャレンジへ

※2021年4月開催時点

構成員

- 泉澤　清次　三菱重工業株式会社取締役社長
- 遠藤　信博　日本経済団体連合会サイバーセキュリティ委員長、日本電気株式会社取締役会長等
- 大林　剛郎　日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、株式会社大林組代表取締役会長
- 櫻田　謙悟　経済同友会代表幹事、ＳＯＭＰＯホールディングスグループＣＥＯ取締役　代表執行役社長
- 篠原　弘道　日本電信電話株式会社取締役会長
- 中西　宏明　株式会社日立製作所取締役会長
- 船橋　洋一　アジア・パシフィック・イニシアティブ理事長
- 村井　純(座長)慶應義塾大学教授
- 渡辺　佳英　日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

オブザーバー

NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省

WG１（制度・技術・標準化）

第１回　平成30年2月7日
第２回　平成30年3月29日
第３回　平成30年8月3日
第４回　平成30年12月25日
第５回　平成31年4月4日
第６回　令和2年3月（書面開催）
第７回　令和2年10月（書面開催）
第８回　令和3年３月15日

１．サプライチェーン強化パッケージ

WG２（経営・人材・国際）

第１回　平成30年3月16日
第２回　平成30年5月22日
第３回　平成30年11月9日
第４回　平成31年3月29日
第５回　令和2年1月15日
第６回　令和2年8月25日
第７回　令和3年2月18日

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

WG３（サイバーセキュリティビジネス化）

第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日
第４回　令和元年8月2日
第５回　令和2年3月(書面開催)
第６回　令和3年3月10日

４．ビジネスエコシステム創造パッケージ

産業サイバーセキュリティの加速化指針

１．『グローバル』をリードする
２．『信頼の価値』を創出する~Proven in Japan~
３．『中小企業・地域』まで展開する

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

- **<u>7つの産業分野別サブワーキンググループ(SWG)</u>**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**<u>タスクフォース（TF）を設置。</u>**

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11月に第3回を開催
- **工場SWG**
  - 2022年1月に第1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を策定、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：
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。

１．サイバーセキュリティに関する動向

２．産業サイバーセキュリティ研究会の検討状況

- **第３層TF**
- 第２層TF
- ソフトウェアTF

３．IoT機器に対するセキュリティ対策

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

- 「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（仮題、以下フレームワーク）」の骨子案のパブコメを実施。（2021年7月15日～10月11日）
- **2022年2月2日から3月3日までの間、添付資料を加えた本文案について、パブコメ中。**

https://www.meti.go.jp/press/2021/02/20220202001/20220202001.html

【本文】

1. 新たなデータマネジメントの在り方
- 1-1 CPSFにおける第3層（サイバー空間におけるつながり）
  - 1-1-1 CPSF概論
  - 1-1-2 第3層の位置づけ
- 1-2 データの信頼性確保：データマネジメントの考え方の確立
- 1-3 本フレームワークの目的
- 1-4 本フレームワークの想定読者

2. 本フレームワークにおけるデータマネジメントのモデル
- 2-1 概要編
  - 2-1-1 データマネジメントのモデル化の概要
  - 2-1-2 リスク分析手順
- 2-2 詳細編
  - 2-2-1 モデル化（「イベント」）
  - 2-2-2 モデル化（「場」）
  - 2-2-3 モデル化（「属性」）

3. 活用方法
- 3-1 サプライチェーンを構成するステークホルダー間での活用
- 3-2 ルール間のギャップの分析

【添付資料】

添付A. ユースケース

添付B. イベントごとのリスクの洗い出しのイメージ

（参考）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

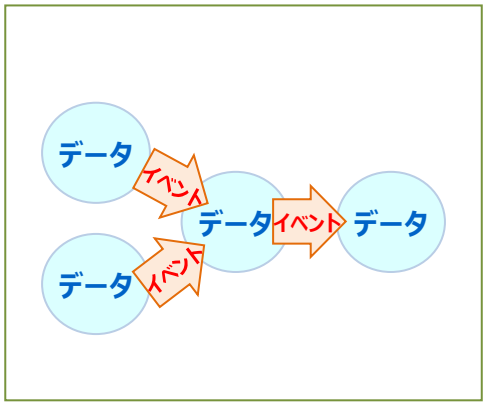
▶「データの "**属性**" が "**場**" における "**イベント**" により変化する過程をライフサイクル全体にわたって管理すること」

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

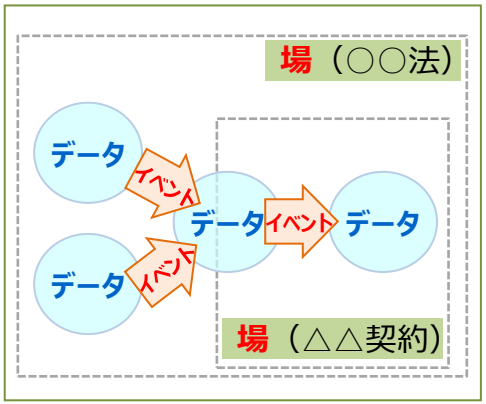
新たな捉え方への当てはめステップ

▶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。

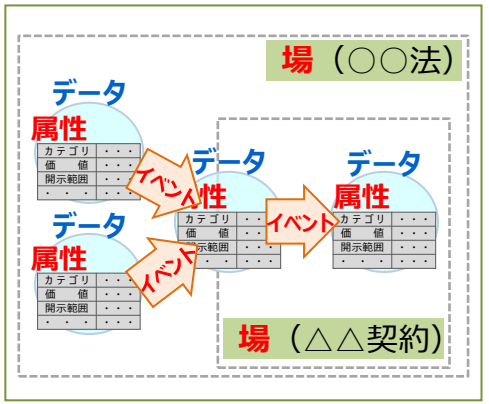
STEP 1
データ処理フロー（「イベント」）の可視化



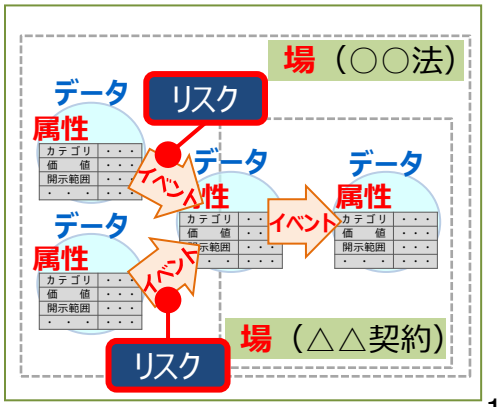
STEP 2
必要な制度的保護措置（「場」）の整理



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



（参考）添付A：ユースケース

- フレームワーク骨子案では、概念やモデル化の定義等が中心だったが、より理解を深めていただくために、実践的なユースケースに基づくモデル化とリスクの洗い出しのイメージを添付資料として作成。
- 添付Aでは、特徴的な以下4つのユースケースを選定した。

1

POSデータの分析
モデル化の全体像を把握しやすく単純化した事例

2

高齢者生活支援事業の提供
多数のステークホルダーが関係する事例

3

IaaS、PaaS、SaaSを利用してサービスを提供する例
クラウドサービスの多層化・重層化事例

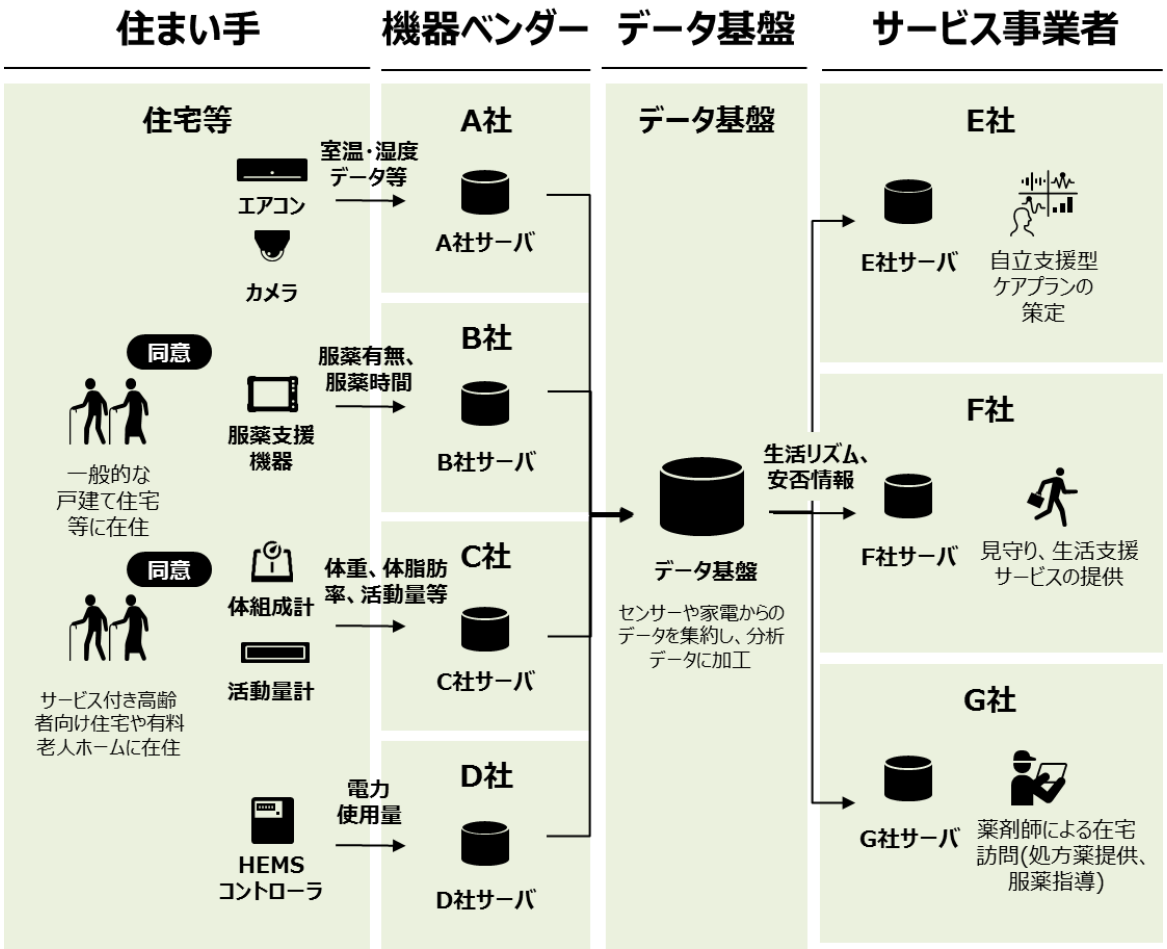
4

国内で提供されるITサービスに関して、海外で開発や運用等を実施する例
国外で開発や運用等を実施する事例（データの越境移転）

（参考）ユースケース ｜ 高齢者生活支援事業 概要

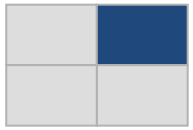
- 2018年に実施された国立研究開発法人　新エネルギー・産業技術総合開発機構（NEDO）／パナソニック株式会社他による「IoT家電・センサーからのライフデータによる高齢者の生活サポートサービス基盤の研究開発事業」を取り上げる。

  https://www.nedo.go.jp/news/press/AA5_101002.html



- 一般的な戸建て住宅や有料老人ホーム等に設置される多数の機器群を通じて、高齢者の生活や健康の状況に関するデータが**生成**され、各機器ベンダー（A社～D社）の運用するサーバに**蓄積**
- 各機器ベンダーは一定の収益を得る代わりに、第三者（プラットフォーム事業者）の運用するデータ基盤に各々が収集したデータを**提供**する。各機器ベンダーから提供されたデータは特定の個人を特定できない形でデータ基盤上に**集約**され、高齢者の生活リズム情報や安否情報というより高次なデータへと**加工**される。
- 高齢者の生活リズム情報や安否情報等のデータは、必要に応じてサービス事業者等に第三者提供され、データ主体の個人と紐づけたうえでより高度な支援サービスの提供等に**加工・利用**される。

（参考）ユースケース ｜ 高齢者生活支援事業 ステークホルダー



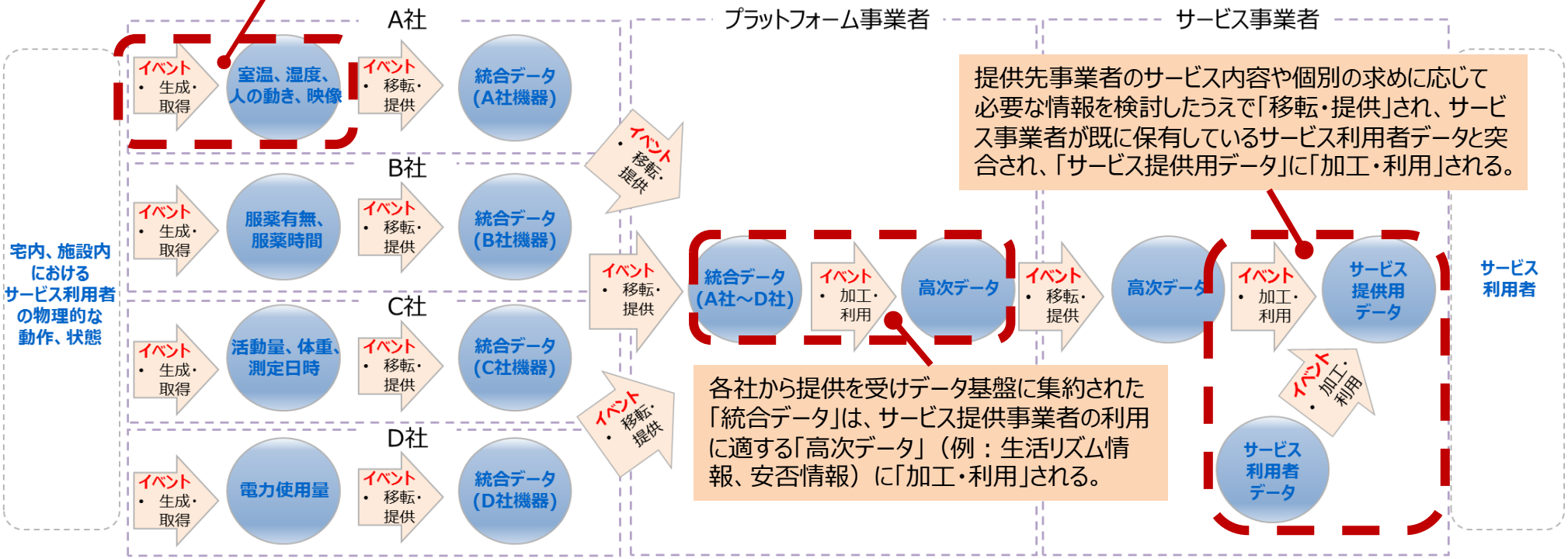
- 機器ベンダー（A社～D社）、プラットフォーム事業者、サービス事業者等は、コンソーシアムを組成し、共通して適用される規則の策定や適時の情報共有等を行っている 。
- 取り扱うデータには機微な個人データとなり得るものも含まれることから、コンソーシアム等での協議を実施し、サプライチェーンの全体で十分な水準のデータ保護措置を講じる必要がある。

ステークホルダー	説明
住まい手	日常生活の中で各種IoT機器・サービス等を利用し、それに伴って生成される自身に関するデータを同意等の適切な手続きを経たうえで事業者に提供する。 • 一般的な戸建て住宅等に在住する高齢者 • サービス付き高齢者向け住宅や有料老人ホームに在住する高齢者
機器ベンダー（A社～D社）	宅内や施設内に設置されている機器を製造・販売し、本人同意等の適切な手続きを経たうえで各々運用中の機器から取得したデータを収集し、管理している。
A社	エアコンや見守りカメラ等の家庭用IoT機器を製造・販売し、収集したデータを自社サービスで活用するだけでなく、プラットフォーム事業者にも提供する。
B社	処方薬の服薬有無や服用時間等をセンシングする服薬支援機器を製造・販売し、収集したデータを自社サービスで活用することに加え、プラットフォーム事業者にも提供する。
C社	体組成計や活動量計等のヘルスケア機器を製造・販売し、収集したデータを自社サービスで活用するだけでなく、プラットフォーム事業者にも提供する。
D社	スマートメータが実装された家庭向けに電力使用状況を可視化するサービスを提供し、収集したデータをプラットフォーム事業者にも提供する。
プラットフォーム事業者	各住宅、施設に設置した機器等からのデータを集約し、適宜加工・分析等を実施する。
サービス事業者（E社～G社）	プラットフォーム事業者からデータの提供を受け、より高度な高齢者支援サービスの提供等に活用する。

（参考）ユースケース ｜ 高齢者生活支援事業 STEP 1

- STEP 1として、**データ処理フロー（イベント）の可視化**を行う。

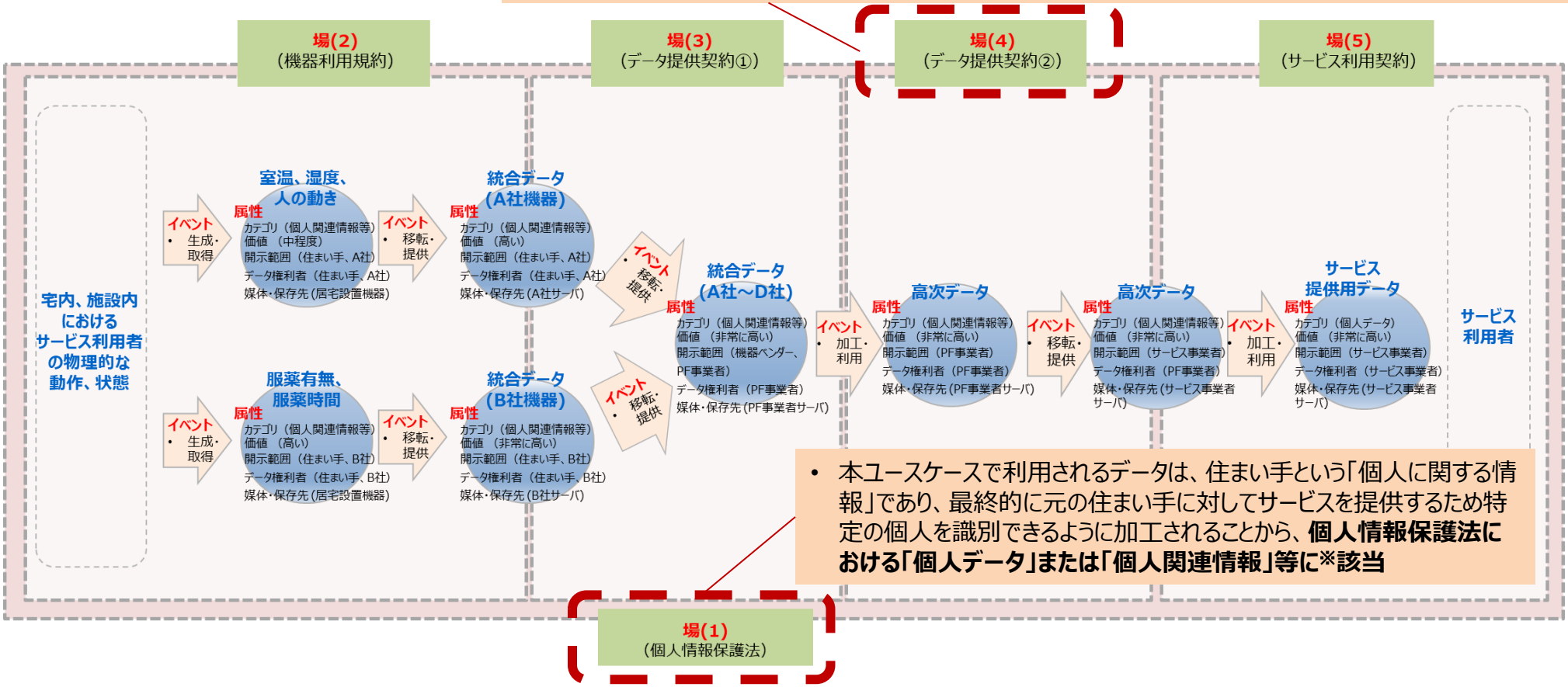
製造・販売者	名称	収集データ
A社	エアコン	室温・湿度情報
	電波センサーによる見守りシステム	ベッド上の呼吸有無・活動状態（動き）
	コミュニケーションカメラ	室温、人の動き、映像



（参考）ユースケース ｜ 高齢者生活支援事業 STEP 2

- STEP 2として、**必要な制度的な保護措置（場）の整理**を行う。

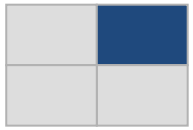
- 各機器ベンダーが保有するデータに加え、「統合データ」についても、匿名的な利用者IDや機器IDに基づいて必ずしも特定の個人に紐づかない形で管理されていることを仮定しているため、「個人データ」ではなく「個人関連情報」等に該当すると考えられるが、提供先のサービス事業者において個人データとして取得されることが容易に想定される。そのため、各機器ベンダー及びPF事業者においては、**個人関連情報取扱事業者として本人からの同意取得の確認、提供元における記録等の義務が生じる**点に留意が必要



- 本ユースケースで利用されるデータは、住まい手という「個人に関する情報」であり、最終的に元の住まい手に対してサービスを提供するため特定の個人を識別できるように加工されることから、**個人情報保護法における「個人データ」または「個人関連情報」等に※該当**

※令和2年の改正個人情報保護法において規定。令和４年４月１日に施行される予定。

（参考）ユースケース｜ 高齢者生活支援事業 STEP 3-1

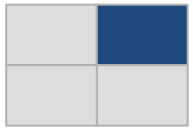


- STEP 3として、前STEPにて特定した「場」を踏まえ、**各種データの管理に資する属性を特定**する。
- 個人情報保護法制の他、開示範囲やデータ管理主体、利用期限等の事業者間の責任分解にも関連する内容を特定する際には、当事者間で締結される各種契約・規約が有用。

「属性」の検討において考慮すべきルール（場）

		個人情報保護法	機器利用規約	データ提供契約	サービス提供契約
カテゴリ	パーソナルデータ保護	○			
	知的財産（営業秘密を含む）保護			○	
	…	…	…	…	…
開示範囲		○	○	○	○
利用目的		○	○	○	○
データ管理主体			○	○	○
データ権利者		○	○	○	○
価値（重要度）			○	○	○
媒体・保存先			○	○	○
利用期限			○	○	○

（参考）ユースケース ｜ 高齢者生活支援事業 STEP 3-2



- STEP 3として、前STEPにて特定した「場」を踏まえ、**各種データの管理に資する属性を特定**する。

本ユースケースにて取扱うデータ（一部）の「属性」パラメータ例

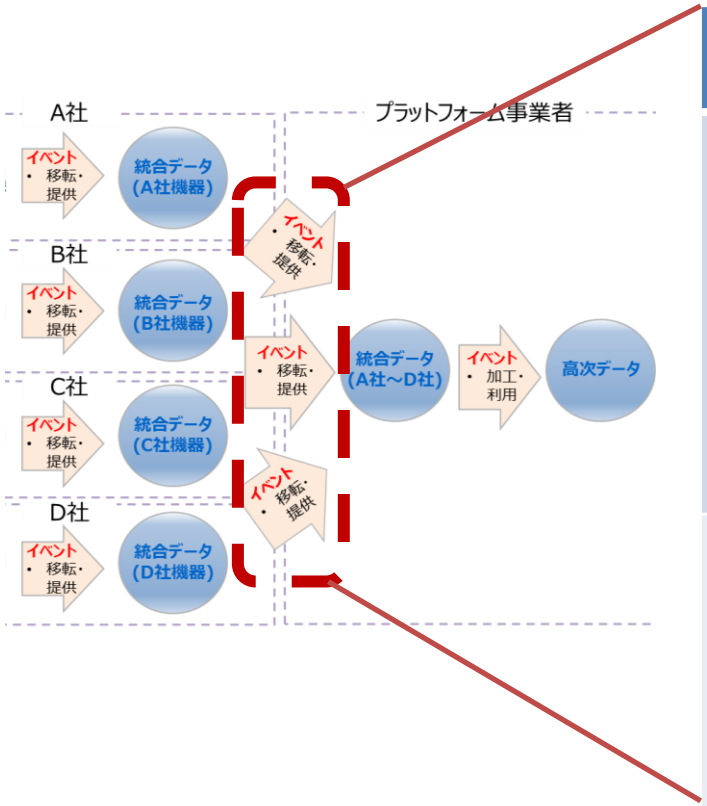
		統合データ（A社）	統合データ（A社～D社）	高次データ	サービス提供用データ
カテゴリ	パーソナルデータ保護※1	個人関連情報 等	個人関連情報 等	個人関連情報 等	個人データ
	知的財産※2（営業秘密を含む）	営業秘密 等（A社）	営業秘密（PF事業者）	営業秘密 等（PF事業者）	営業秘密（サービス事業者）
開示範囲		A社内	PF事業者内	PF事業者内	サービス事業者内
利用目的		取得データを活用した各種サービスの提供	左記と同様	左記と同様	左記と同様
データ管理主体		A社	PF事業者	PF事業者	サービス事業者
データ権利者		住まい手、A社	住まい手、機器ベンダー、PF事業者	住まい手、PF事業者	住まい手、サービス事業者
価値（重要度）		高い	非常に高い	非常に高い	非常に高い
媒体・保存先		A社サーバ	PF事業者サーバ	PF事業者サーバ	サービス事業者サーバ
利用期限		特になし	データ提供契約終了から1年	データ提供契約終了から1年	サービス提供期間終了まで

※1 対象のデータが、個人情報保護法上のいかなる情報の類型に属するかは、改正個人情報保護法の動向も踏まえつつ、適用主体において慎重な検討が必要である。
※2 上記のデータのうち、特定の事業者間で共有されるものについては、不正競争防止法上の「限定提供データ」に該当する場合も想定される。

（参考）ユースケース ｜ 高齢者生活支援事業 STEP 4

- STEP 4として、STEP 1～3で特定した内容を踏まえ、**イベントごとのリスクポイントの洗い出し**を行う。

各機器ベンダー「統合データ」のPF事業者への「移転・提供」にて想定されるリスクの例



大分類	中分類	各機器ベンダーが保有する「統合データ」のPF事業者への「移転・提供」にて想定されるリスク（例）
セキュリティの保護に係る観点	機密性	● 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、通信内容が漏えいする。 ● 悪意のある内外の主体が機器ベンダーの管理するサーバから当初接続を意図していなかったサーバ等にデータを送信する。
	完全性	● 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、データを改ざんする。
	可用性	● 悪意のある第三者がデータ基盤のAPI を無作為に呼び出すような DoS攻撃を行い、プラットフォーム事業者サーバの処理が停止する。
関連する法制度等に係る観点	パーソナルデータ保護	● 統合データの提供前に、提供元の機器ベンダーが提供先のプラットフォーム事業者において当該データが個人情報として取得されるかどうかを確認していない。 ● プラットフォームにて特定の個人の特定を行う場合に、住まい手の同意等を得ることなくデータがプラットフォーム事業者に提供される。
	知的財産（営業秘密を含む）保護	● 各社の統合データが悪意のある内外の主体により不正な手段で取得され、開示、使用される。

リスクを可視化した上で、各主体がそれぞれ実施すべき対策を他の主体と協議しながら取り組むことにより、データの信頼性を確保することが期待される。

１．サイバーセキュリティに関する動向

２．産業サイバーセキュリティ研究会の検討状況

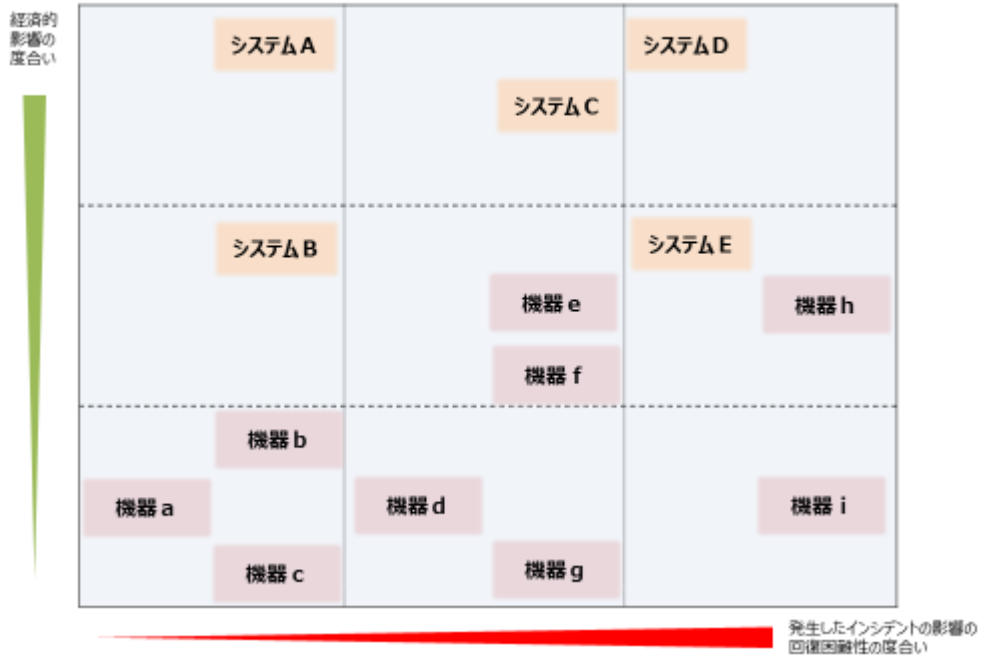
- 第３層TF
- **第２層TF**
- ソフトウェアTF

３．IoT機器に対するセキュリティ対策

IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の策定

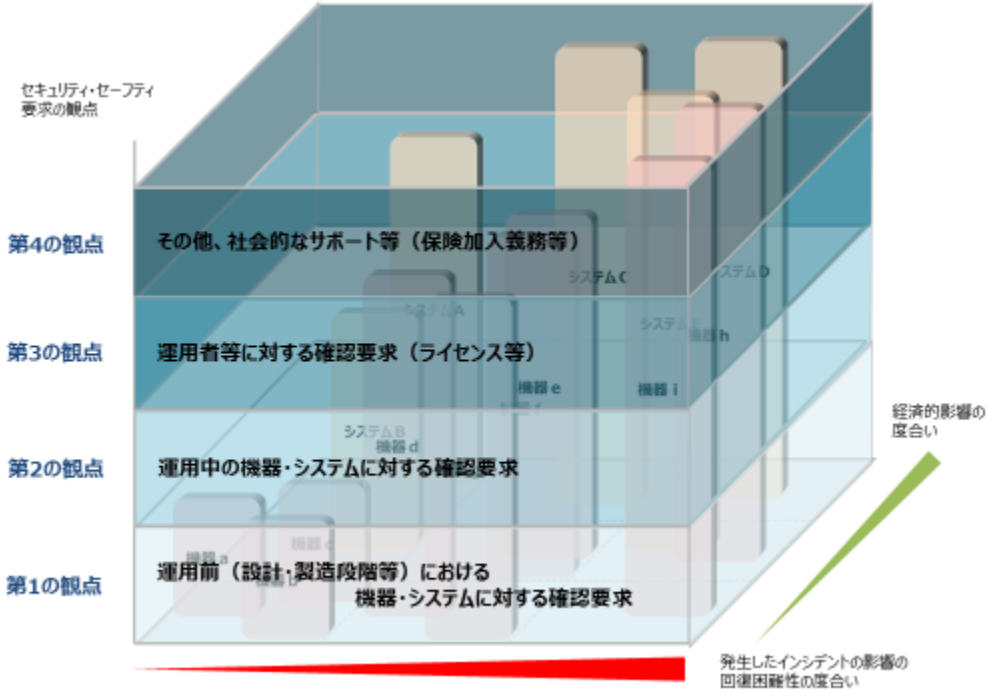
- **用途や使用環境によって課題が異なるIoT機器・システムに対するセキュリティ対策を、複数のステークホルダー間で合意する**際に活用できる**「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」を2020年11月5日に公開。**
- 本フレームワークで、IoT機器・システムをカテゴライズし、カテゴリごとに求められるセキュリティ・セーフティ要求の観点を把握・比較することにより、**それぞれに求める対策の観点・内容の整合性を確保できる**。

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



※　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。）

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

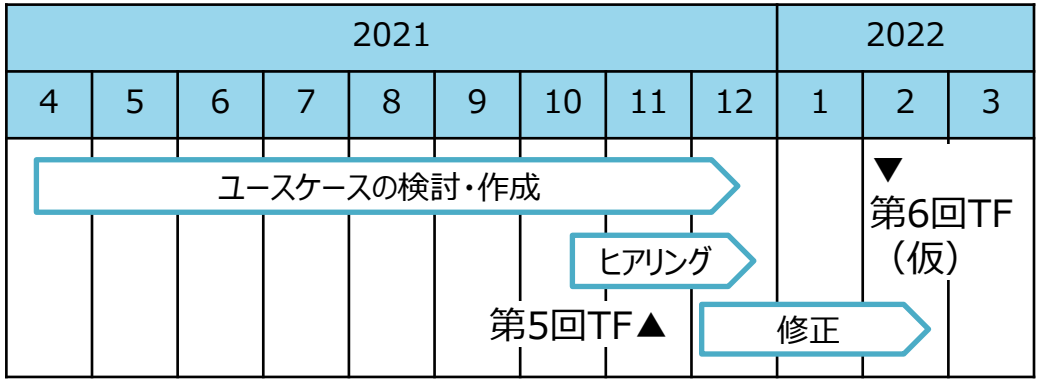


IoT-SSFのユースケース作成

- 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

ユースケース一覧

- 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
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

（参考）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

- 「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

（参考）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

（参考）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。

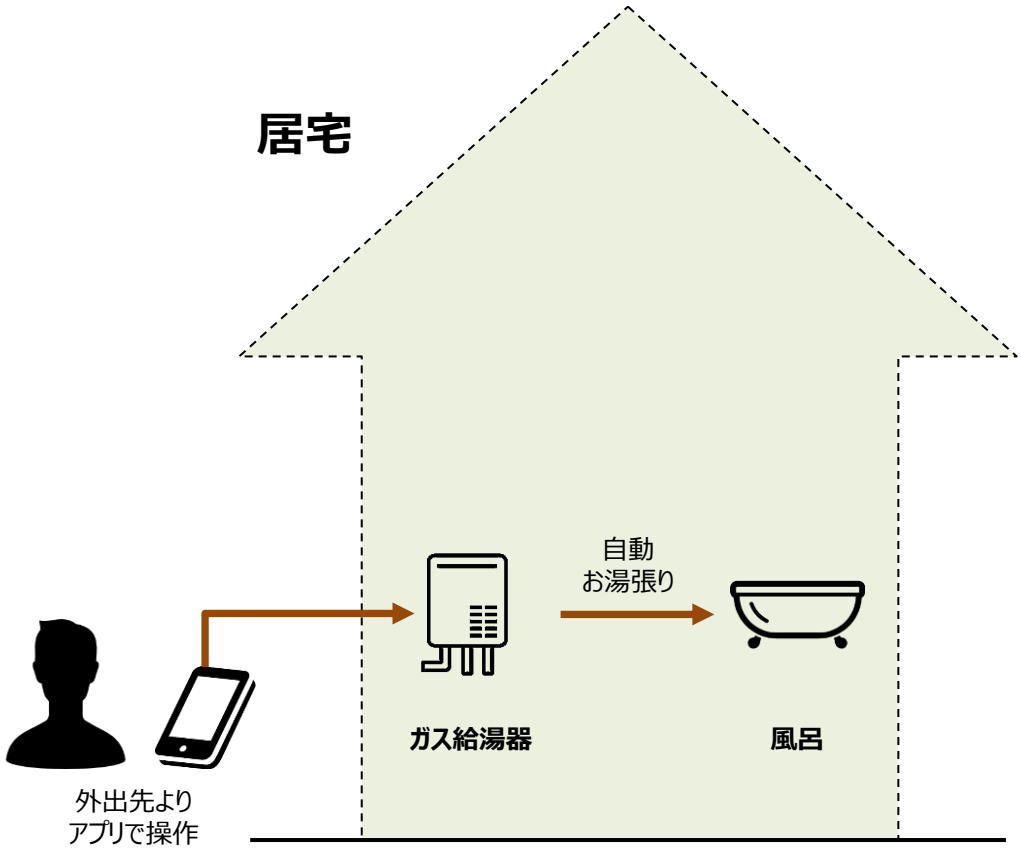
レベル	判断基準	（参考）IoT-SSFにおける判断基準
壊滅的な経済影響	• 影響の範囲が内部に限定されず、取引先やその他の関係者に及び、長期間影響が続くことが想定される。 • 影響を受ける機器・システムの機能を他の製品・サービスで補うことができない。 • 大規模な製品等の回収や損害賠償が生じ得る。	• 破産 • 社会の大混乱
重大な経済影響	• 影響の範囲が取引先やそれ以外の関係者に及び、長期間影響が及ぶものの、**他の製品等で影響の結果を補うことができる**。 • 影響の範囲が取引先やそれ以外の関係者に及び、影響の結果は他の製品・サービスで補えないものの、**影響は短期間で収束する。**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

（参考）ユースケース例：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）

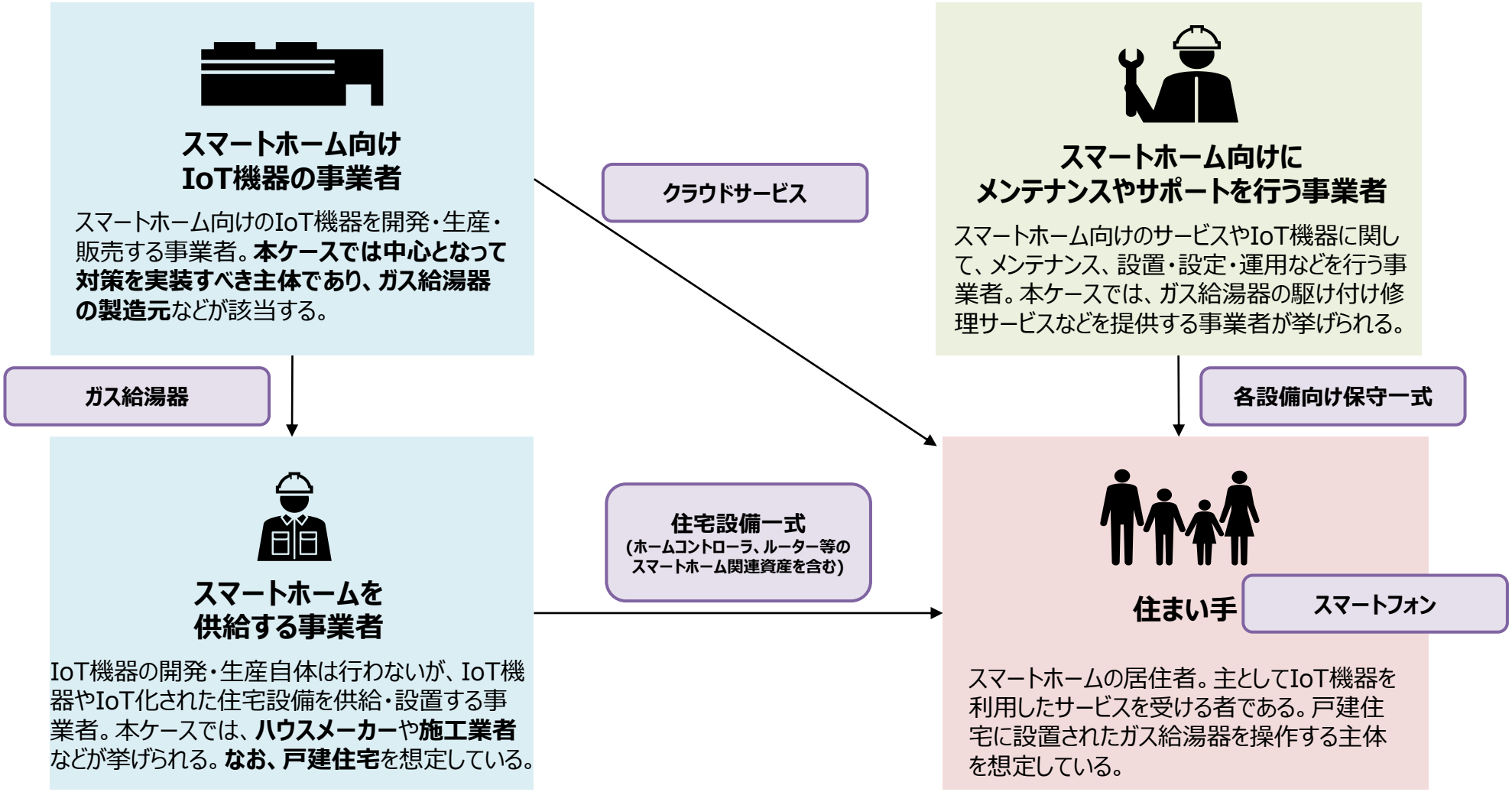
※1経済産業省「液化石油ガス器具等の技術上の基準等に関する省令の運用について」（令和2年7月）では、「自然吸排気式」及び「開放式」以外の機器において「リスク低減策を講じることにより遠隔操作に伴う危険源がないと評価されるもの等の基準に合致し、危険が生ずるおそれがないものは、操作可能」とされている。



[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

（参考）ユースケース例：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。

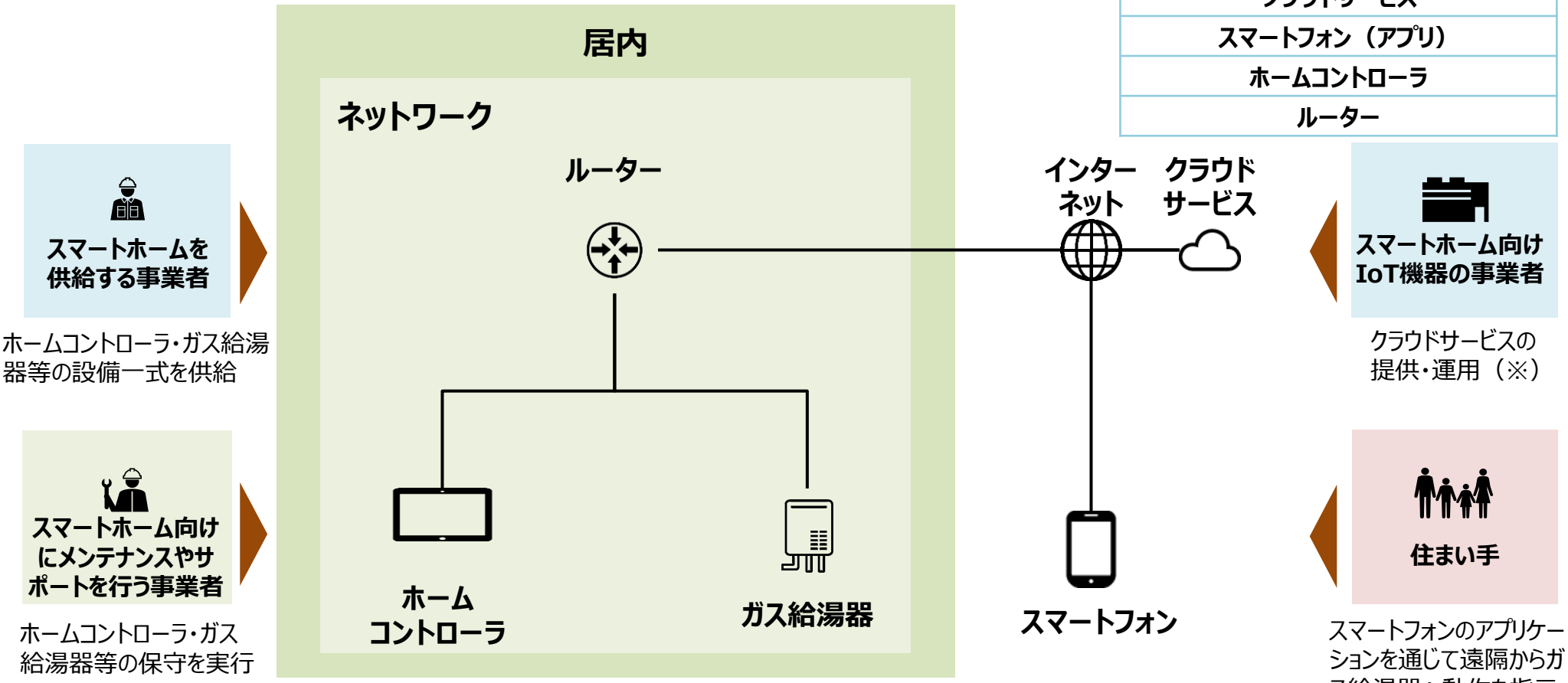


[出典] 経済産業省「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドラインスマートホームガイドライン」等を参考に作成

（参考）ユースケース例：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

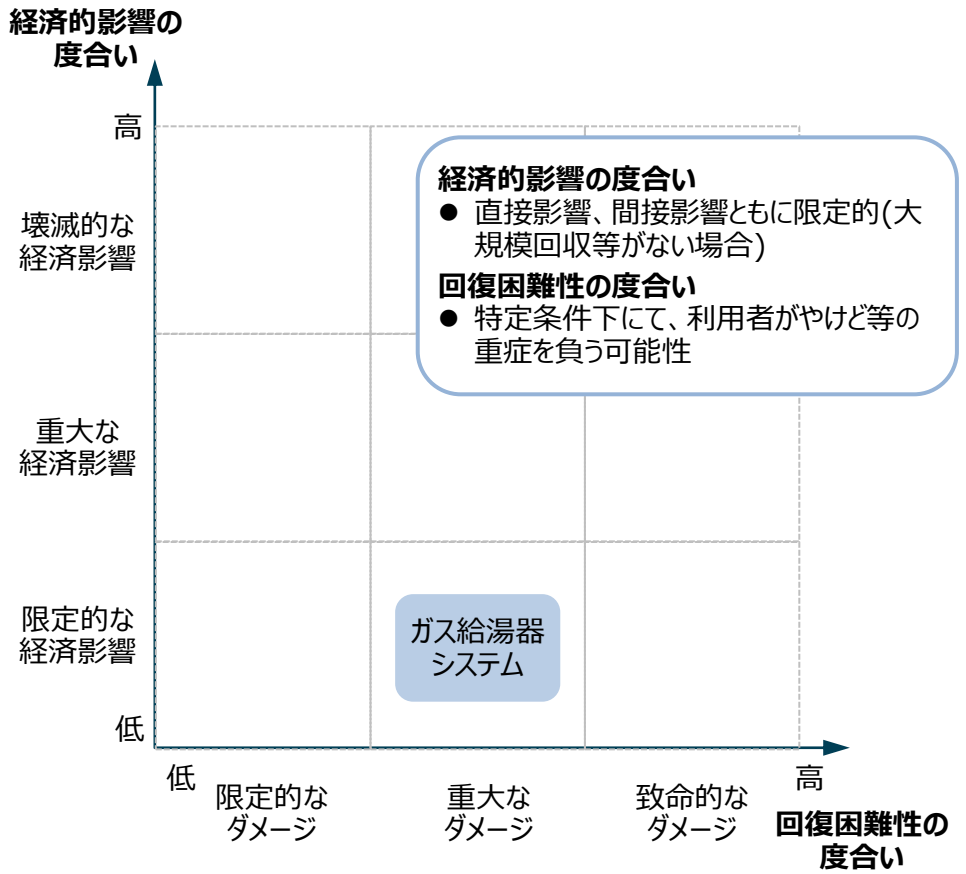
（参考）ユースケース例：ガス給湯器の遠隔操作（ガス給湯器）

- 「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。

（参考）ユースケース例：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

（参考）ユースケース例：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

（参考）ユースケース例：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

１．サイバーセキュリティに関する動向

２．産業サイバーセキュリティ研究会の検討状況

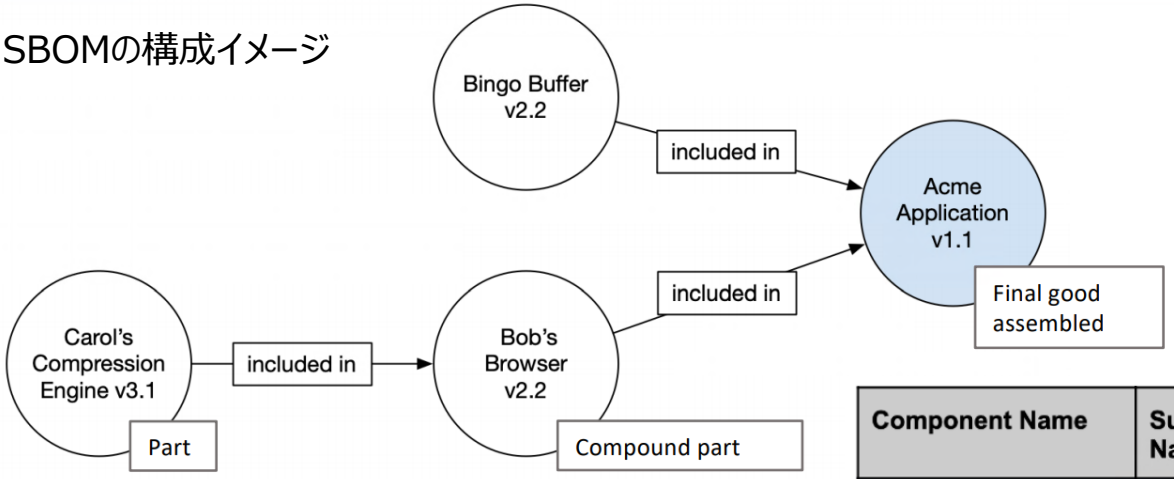
- 第３層TF
- 第２層TF
- **ソフトウェアTF**

３．IoT機器に対するセキュリティ対策

ソフトウェアTF： SBOMについて

- SBOM （Software Bill of Materials）とは、ソフトウェアの部品構成表のこと。ソフトウェアを構成する各コンポーネントを誰が作り、何が含まれ、どのような構成となっているか、等を示す。
- SBOMによりソフトウェアの構成情報を詳細に把握することができ、ライセンス管理や脆弱性対応への活用が期待できる一方、その作成や管理、サプライチェーンにおける共有等において課題が存在。
- 米国NTIA（電気通信情報局）では、 2018年に「Software Component Transparency」に関するMultistakeholder Meetingを設置し、ヘルスケア分野におけるPoC等を実施するなど、SBOMの構成や活用について議論を重ねている。

SBOMの構成イメージ



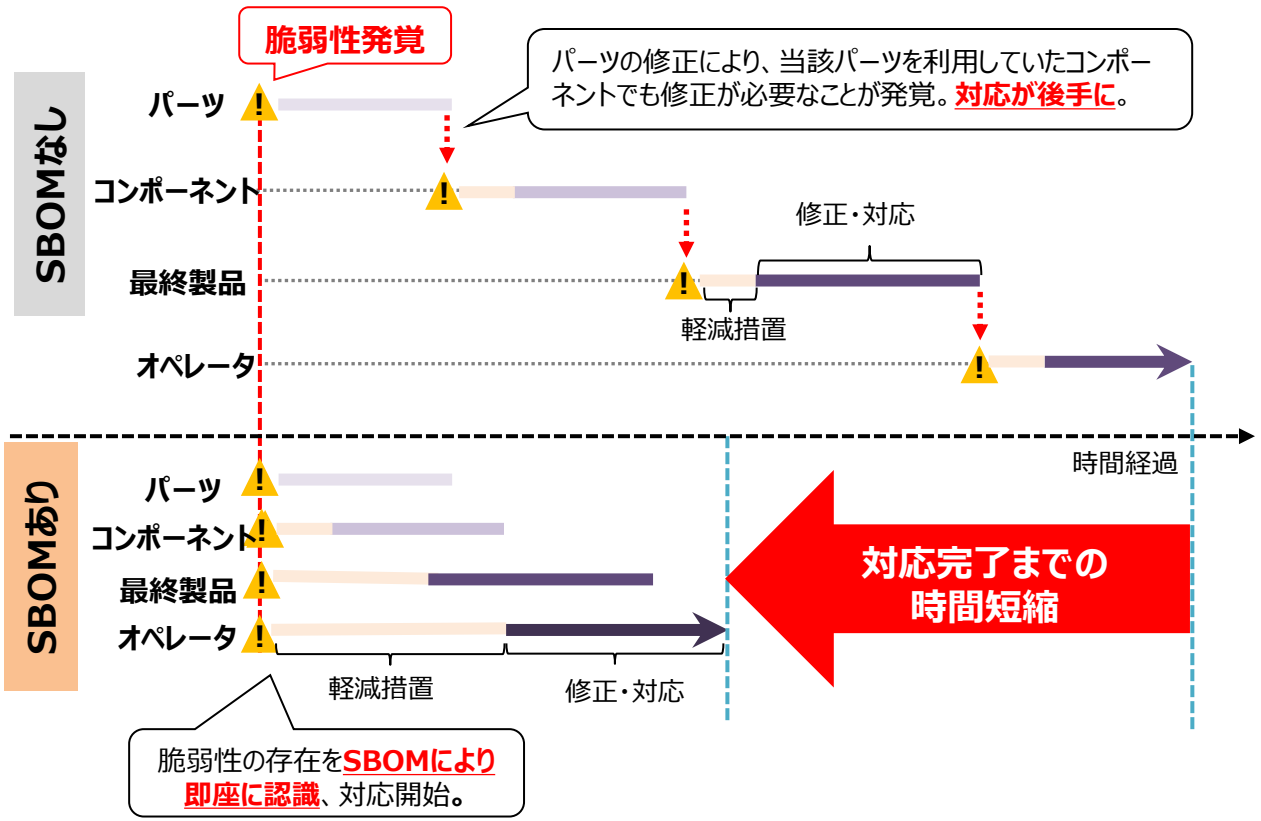
Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Self
|--- Browser	Bob	2.1	Bob	0x223	334	Included in
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

https://www.ntia.doc.gov/SoftwareTransparency

ソフトウェアTF：SBOM活用に向けた実証

- 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の実施を検討。

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。

自動車産業分野

Auto-ISACを中心としたサプライヤ中心のプロジェクト。12ヶ月ほどかけてサプライヤの推奨事項をとりまとめる予定。

電力分野

1/26キックオフ。米国エネルギー省からもプレゼンターとして参加。

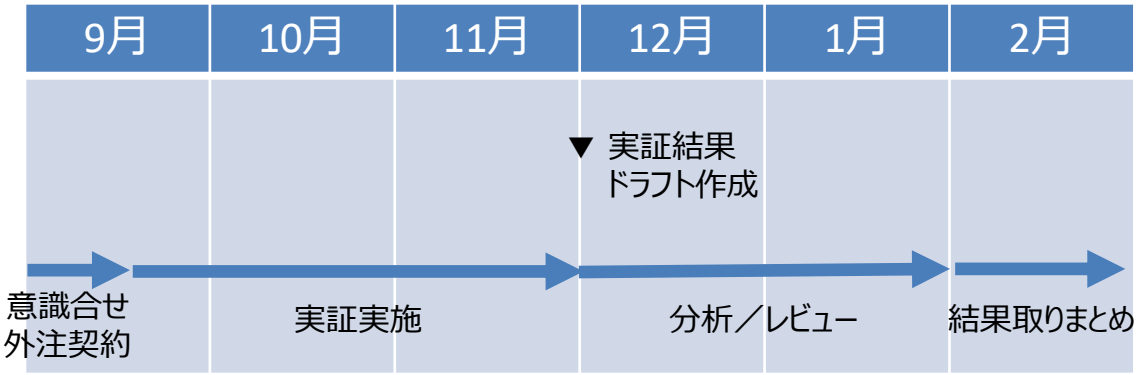
SBOM実証の対象ソフトウェア・体制・スケジュール

- 本年度は、ユーザー企業や製品ベンダーからのご協力が見込まれることから、**自動運転システム検証基盤ソフトウェア「GARDEN」を実証の対象ソフトウェアに選定し、実証事業を実施**。

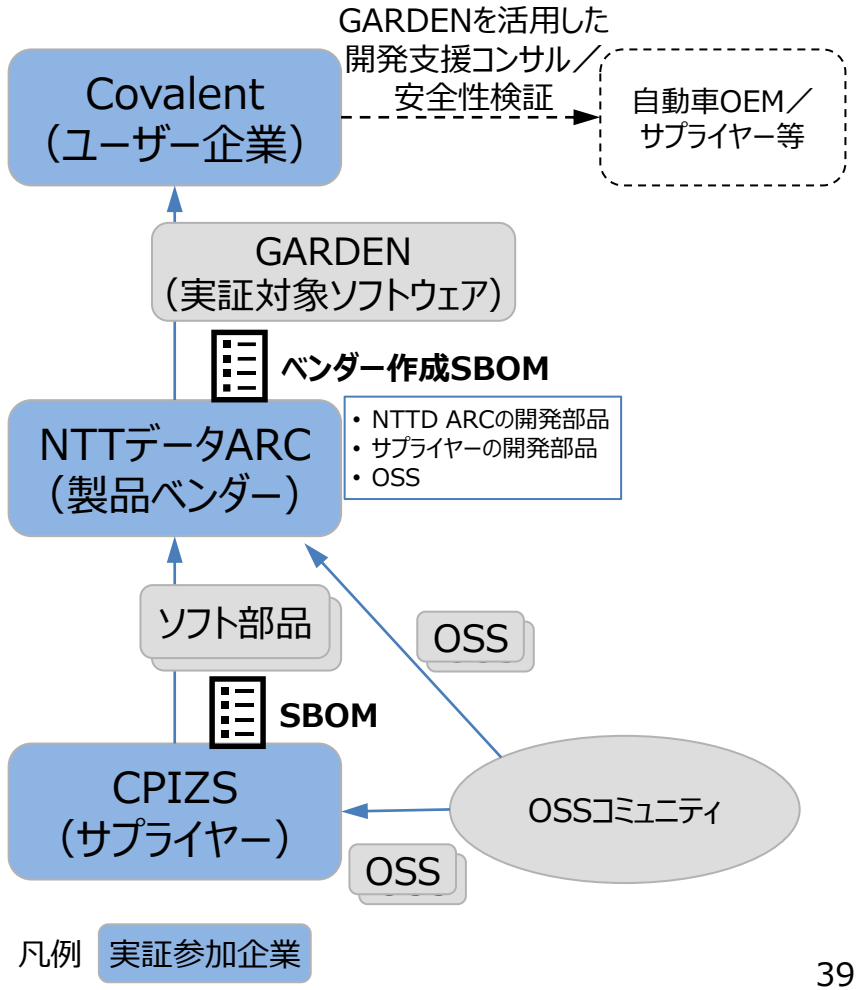
実証対象ソフトウェア 「GARDEN」

名称	GARDEN Scenario Platform
製品ベンダー	株式会社NTTデータ オートモビリジェンス研究所（NTTデータARC）
概要	• 自動運転システム開発向け検証基盤ソフトウェア。 • 自動運転ソフトウェアの安全性評価のための機能動作シミュレーションのシナリオ生成機能を提供。 ➢ モデリング、走行データ分類、軌跡抽出道路編集、シナリオ組合せテスト、シナリオ実行 • オープンソースとして、ソースコードを公開。

想定スケジュール



実証体制（GARDENのサプライチェーン）



１．サイバーセキュリティに関する動向

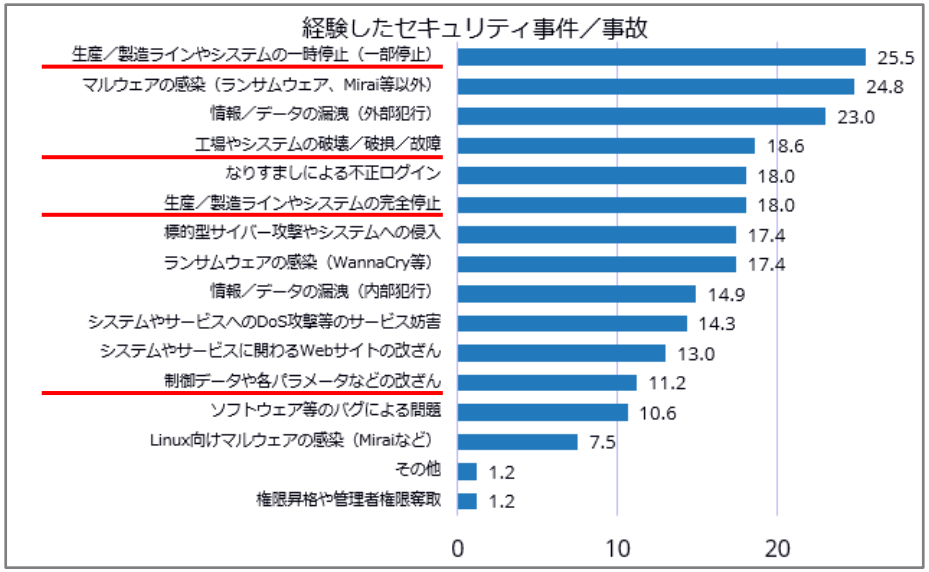
２．産業サイバーセキュリティ研究会の検討状況
- 第３層TF
- 第２層TF
- ソフトウェアTF

３．IoT機器に対するセキュリティ対策

IoT機器に対するセキュリティ対策の必要性

- DXの進展により、インターネットとIoT機器が繋がり始めたところであるものの、**セキュリティ事件/事故によるIoT機器やOTシステムの一時停止を約25%の企業が経験**しているといった調査結果からも、**こうした機器やシステムでセキュリティ対策を多くの者が導入しているとは言い難い**状況。
- 機器に対する十分なセキュリティ対策が実施されず、脆弱性が残存した場合、悪意ある攻撃者によって不正操作や誤作動が実行され、**機器の利用者へ影響を及ぼす恐れ**がある。
- また、**開発企業は脆弱性の対応に追われる**こととなる。過去には、**脆弱性によりリコールや利用者による訴訟に発展した事例**もあり、最悪の場合、**開発企業の経営に対して影響を与える可能性**もある。
- 今後さらなる脅威の増加・高度化が想定されるところ、**機器に対するセキュリティ対策の具備が不可欠**。

2021年 国内企業のIoT/OTセキュリティ対策実態調査結果



セキュリティ対策の不備により開発企業に影響を及ぼした事例

自動車における脆弱性の検出による140万台のリコール

販売中の自動車に対して外部から不正アクセス可能な脆弱性が公開された。**顧客からの問い合わせが殺到し、開発企業は140万台のリコールを実施**した。**リコールの対応には1,000万ドル以上の費用**を要した。

心臓ペースメーカーにおける脆弱性の検出による46.5万台のリコール

販売中の心臓ペースメーカーに対して心拍リズムを外部から制御可能な脆弱性が公開された。**開発企業は市場に流通している46.5万台を対象にリコールを実施**した。

脆弱な家庭用ネットワークカメラのメーカに対する訴訟

家庭用ネットワークカメラにおいて、認証不備に関する脆弱性が内在し、脆弱性を悪用した不正アクセスが行われた。不正アクセスの被害を受けた複数の利用者により、**開発企業に対して500万ドルを求める集団訴訟**が起こされた。

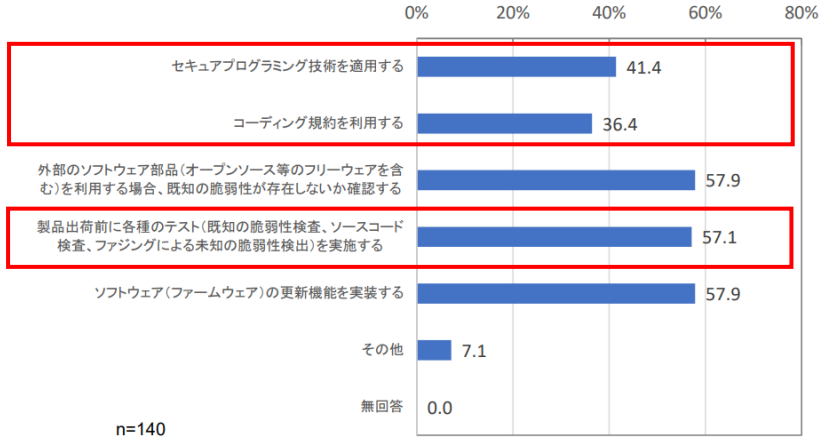
IDC「2021年 国内企業のIoT/OTセキュリティ対策実態調査」https://www.idc.com/getdoc.jsp?containerId=prJPJ47631521
※ 調査実施：2021年2月、調査対象：国内企業443社

IoT機器の脆弱性検証

- IoT機器に対するセキュリティの取組においては、「**セキュリティ・バイ・デザイン**」の考えに基づき、設計・開発段階で**セキュリティ対策が適切に導入されていることが必要**。
- 他方で、**開発段階でセキュリティ対策を行っている企業は現状限定的**であり、十分な脆弱性対策が実施されていないことにより、**1,000万円以上の損害に繋がった企業も存在**する。
- セキュリティ・バイ・デザインの考えに立脚し、**開発段階からの脆弱性検証を試験的に実施することで効果的な検証手法を整理する**とともに、**その効果を可視化**するために、令和３年度補正予算事業「**開発段階におけるIoT機器の脆弱性検証促進事業**」により、**中小企業による発売前のIoT機器の脆弱性検証を促進する。**

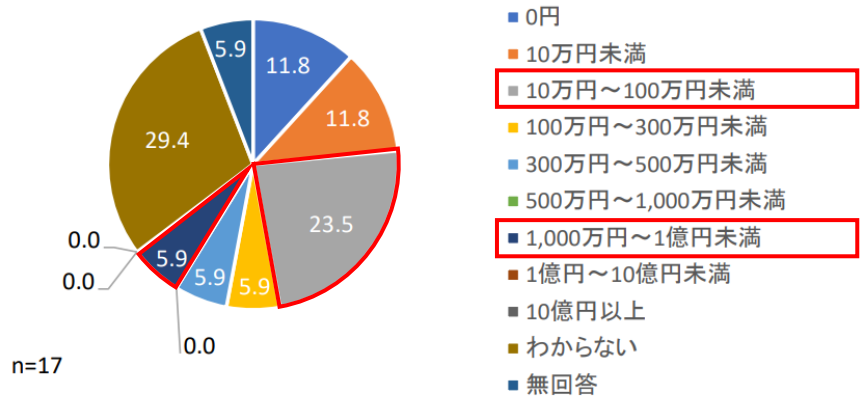
IoT機器に対するセキュリティの取組状況

（開発段階の脆弱性対策の考慮内容）



- **4割以上の企業が機器出荷前に検証を実施していない。**
- **6割程度の企業が開発段階のセキュリティ対策を行っていない。**

（脆弱性による金銭的な損害）



- **10万～100万円未満の損害が最も多いが、1,000万～1億円未満の損害が発生した企業も存在する。**

IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」https://www.ipa.go.jp/files/000065094.pdf
※調査実施：2017年11月、調査対象：国内企業205社

開発段階におけるIoT機器の脆弱性検証促進事業

令和３年度補正予算額　８．３億円

事業の内容

事業目的・概要

- 家庭内や職場環境、産業分野において、IoT機器の導入が進んでおり、IoT機器がネットワークにつながることによりサイバー攻撃といった新たな脅威が出てきています。
- 他方、中小企業が発売するIoT機器は安価であるもののセキュリティ対策が十分でないおそれがあるものもあり、購入・利用者側でサイバー攻撃の被害を受ける懸念があります。また、脆弱性の検証サービスの利用は中小企業にとって決して安いものではなく、費用面や開発に要する日数が増加する等の理由で現時点で必要性が必ずしも理解されていません。
- 市場投入後に機器に脆弱性が見つかれば緊急のアップデートだけでなく、場合によっては回収等の対応を求められる可能性もあり、中小企業の経営に大きな影響を及ぼすおそれがあることから、中小企業の負担軽減も考慮した効果的な検証手法の進め方の整理を早急に行う必要があります。
- このため、家庭や職場、産業向けに中小企業が発売するIoT機器について、開発段階からの効果的な脆弱性検証を試験的に実施することで効果的な検証手法を整理するとともに、その効果を可視化し、中小企業による発売前のIoT機器の脆弱性検証を促していきます。

成果目標

- 効果的な検証手法を実施する事業者を10者創出することを目指し、中小企業が検証を依頼しやすくします。

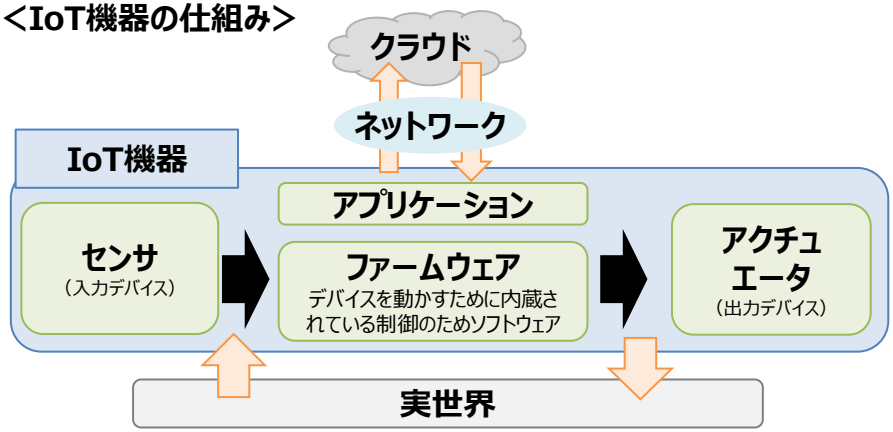
条件（対象者、対象行為、補助率等）

国 → 委託 → 民間事業者等

事業イメージ

開発段階におけるIoT機器脆弱性検証（ペネトレーションテスト）の例

＜IoT機器の仕組み＞



＜今回の検証手法（開発段階から実施）＞

①設計、製造段階の機器の設計書やファームウェアのソースコードを確認

②プロトタイプ（ファームウエアと動作部のハードウェアを組み合わせる）の動作解析

③アプリケーションに対し、ネットワークスキャン等を実施

検証効果の可視化

開発段階からセキュリティを意識するセキュリティ・バイ・デザインを採り入れた効果的な検証手法を整理し、
コスト低減を図りつつ、中小企業の検証を促進