経済産業省

資料4

事務局説明資料

産業サイバーセキュリティ研究会
WG１・分野横断SWG　合同会議

令和４年４月４日

経済産業省　商務情報政策局

サイバーセキュリティ課

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
東原　敏昭	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、デジタル庁

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

- **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
- 防衛産業サイバーセキュリティ基準の改訂を公表(2022.4)

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
- 2022年2月に第4回を開催

工場SWG
- 2022年3月に第3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）」案のパブリックコメント（2回目：22年2月～3月）を実施。

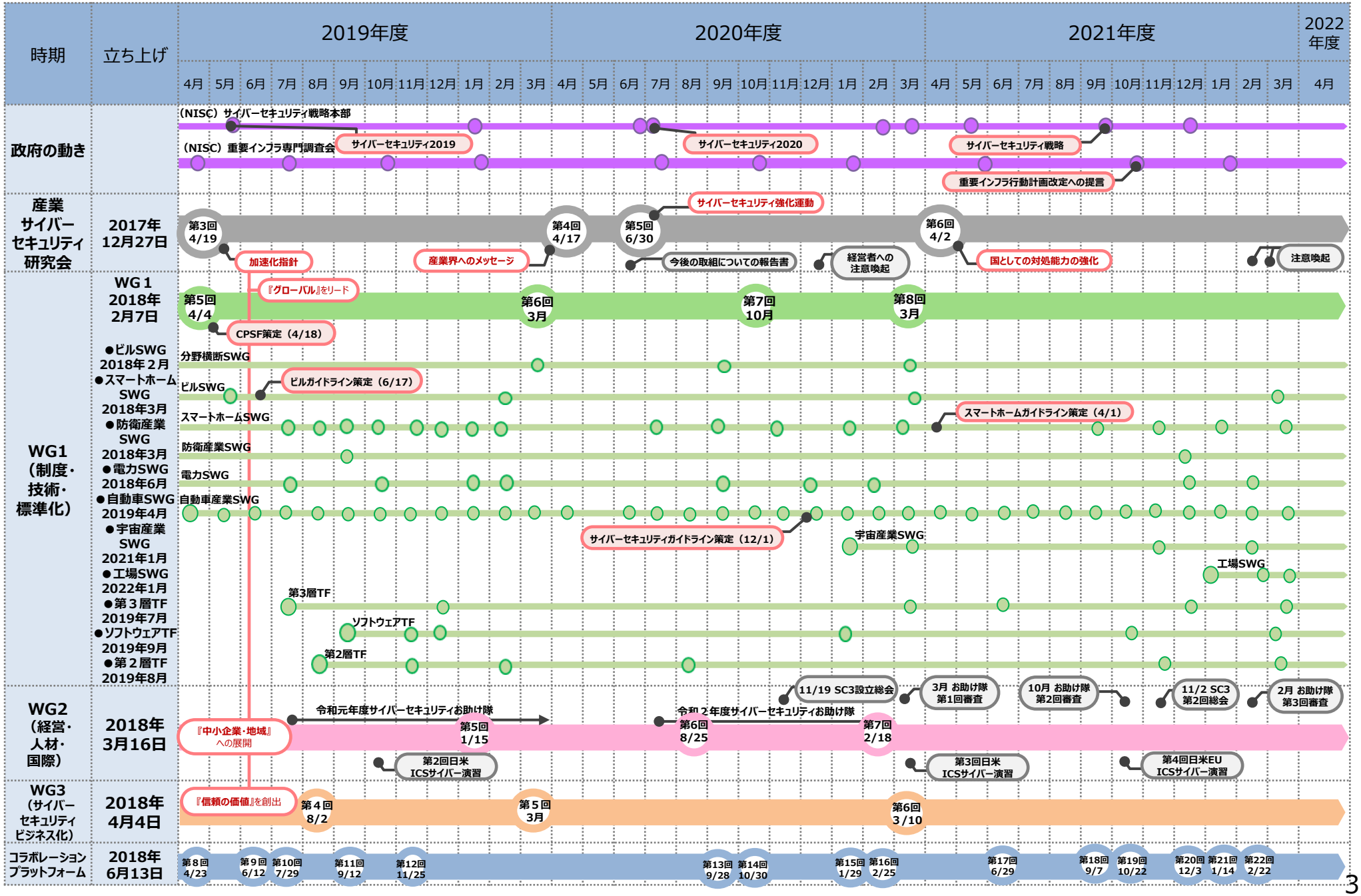
ソフトウェアTF：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース

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。このIoT-SSFをわかりやすく理解するためのユースケースを策定（公開準備中）。

（参考）産業サイバーセキュリティ研究会関連会議の実績



（参考）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）を軸とした各種取組

- **「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）」では、Society5.0における産業社会でのセキュリティ対策の全体枠組みを提示。**
- 全体の枠組みに沿って、対象者や具体的な対策を整理し、『サイバーセキュリティ経営ガイドライン』や産業分野別のガイドラインなどの実践的なガイドラインを整備。

＜各種取組の大まかな関係＞

目次

主なトピックに関する諸外国の動き

ソフトウェア

米国

- ✓ 2021年５月に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に署名がなされて以降、「重要なソフトウェアのセキュリティ対策に係るガイダンス」等の関連文書や「SBOMの最小要素の公表」など、ソフトウェアセキュリティに関する制度整備が相次いでなされている状況。
- ✓ 今後は、連邦調達規則（FAR： Federal Acquisition. Regulations）の改正が見込まれており、これに伴いFARの要件を満たさないソフトウェア製品は各省庁の調達契約からは削除されることが見込まれている。
- ✓ さらに、自動車や医療機器などの重要分野のガイダンスにおけるSBOMの推奨等、政府調達以外の領域についても、制度設計が進むことが見込まれている。

IoT機器

米国

- ✓ 米国国立標準技術研究所（NIST）は、これまでIoT製造者向けの推奨事項として、2020年5月にNIST IR 8259を公開、さらに2021年11月に連邦政府向けガイダンスとして、NIST SP 800-213を公表した。
- ✓ また、NISTは、大統領令に基づき、消費者向けIoT製品のサイバーセキュリティ・ラベリングにおける推奨基準の最新版を公表しており、2022年5月までに総括報告書を発行する予定。

欧州

- ✓ 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しており、2021年4月には「機械製品規則案」、同年6月には「一般製品安全規則案」が公開されている。

中国

- ✓ サイバーセキュリティ法において、セキュリティ製品の認証等の際の法的責任や罰則等について規定。

データ

米国

- ✓ データに関する個人情報保護上の規制について、カリフォルニア州等、州単位で規制を制定している動きが見られる。

欧州

- ✓ EU一般データ保護規則（GDPR）において、データの越境移転がなされる際の許容される要件等を定めている。

中国

- ✓ データセキュリティ法が2021年9月に施行、さらに、国内で収集した個人情報及び重要データを国外へ移転する際に実施する安全評価の要求及び手順を規定した個人情報域外移転安全評価弁法の意見募集が2021年11月より開始されている。

（参考）【ソフトウェア】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上で、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

（参考）【ソフトウェア】米国：大統領令におけるソフトウェア・サプライチェーンに関するタイムライン

- 大統領令では、**ソフトウェア・サプライチェーンの確保に向け、NISTが中心となりガイドラインを策定する**旨を指示しており、この**ガイドラインには製品購入者に対するSBOM提供に関する項目も含まれる**。
- また、NISTに対して、NTIAと連携して**SBOMの最小要素を公表すること**を指示している。
- 将来的には、公開されたソフトウェア・サプライチェーンに関するガイダンスの要求事項に基づき、**連邦政府のソフトウェア調達に関するFAR（連邦調達規則）が改正される予定**である。

2021.5.12	大統領令の署名
2021.6.25	「重要なソフトウェア」の定義の公表 NIST DoD DHS OMB
2021.7.9	「重要なソフトウェア」のセキュリティ対策に係るガイダンスの公開 NIST DHS OMB
	ソフトウェア検証の最低基準に関するガイドラインの公表 NIST DHS
2021.7.12	SBOMの最小要素の公表 NIST NTIA
2021.7.25まで	「重要なソフトウェア」の定義を満たすソフトウェア製品のカテゴリを特定し、政府機関に通知 DHS NIST
2021.8.10	NISTが公開した重要なソフトウェアのセキュリティ対策に関するガイダンスを、各省庁が遵守することを求めるための措置を講じる OMB
2021.10.28	ソフトウェアサプライチェーンのセキュリティを強化するための予備的なガイドラインの公表 NIST
2022.2.4	ソフトウェアサプライチェーンのセキュリティを強化するための指針を示すガイダンスの公表 NIST
2022.3.8まで	大統領令以降に調達されたソフトウェアに関して、各省庁がNISTによる指針を遵守するための適切な措置を講じる OMB
2022.5.8まで	「予備的なガイダンス」の定期的な見直し・更新のための手順を含む追加のガイドラインの公表 NIST
2022.5.12まで	FAR審議会に対し、各省庁が購入可能なソフトウェアサプライヤーに対する上記ガイダンスに基づく要求事項の遵守と、遵守の証明を義務付ける契約文言を勧告 DHS
(現状、期限の指定なし)	⇒ DHSによる勧告の検討、FARの改正 FAR審議会
	FAR改正に伴い、FARの要件を満たさないソフトウェア製品を調達契約から削除 各省庁

出所）White House, “Executive Order on Improving the Nation’s Cybersecurity” https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ , NIST, “Executive Order” https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/executive-order

（参考）【ソフトウェア】米国：SBOMに関するイベント“SBOM-a-rama”の開催

- 2021年12月、米国CISAが主催する**オンラインイベント“SBOM-a-rama”が2日間にわたり開催**された。
- 本イベントは**SBOMコミュニティの醸成を目的**としており、1日目は初級者向けにSBOMの情報を提供することを目的として、SBOMに関する複数の観点について**有識者から講演及び有識者に対するQ&Aが実施**された。
- 2日目は、**日本のSBOMに関する取組状況について経済産業省より発表**した後、SBOMの利活用に向けた課題について**参加者による議論が実施され、様々な観点に基づく課題が抽出・整理**された。
- イベントのまとめにおいて、今後整理した課題を優先度付けし、**解決に向けた検討を推進**する旨が発表された。

“SBOM-a-rama” 1日目の講演アジェンダ・講演者

1. **SBOMに関するモチベーション**
   SBOMの歴史、SBOMの役割や効果、SBOM利用にあたっての実務者の視点、SBOMの定義について、計5件の講演。
   ※ 登壇者：CISA, Schneider Electric, New York-Presbyterian, CERT/CC等
2. **SBOMのフォーマット及びツール**
   SBOMツールの分類法、SPDXの概要、CycloneDXの概要について、計3件の講演。
   ※ 登壇者：Linux Foundation, Microsoft, OWASP
3. **SBOMの実装**
   NTIAが公開したソフトウェアサプライヤー及びソフトウェア利用者のためのプレイブックの概要、VEX (Vulnerability-Exploitability Exchange)の概要、大統領令で定義されたSBOMの「最小要素」の概要について、計3件の講演。
   ※ 登壇者：Ion Channel, 独BSI, CISA
4. **SBOMに関するPoC**
   ヘルスケア分野、エネルギー分野及び自動車分野のSBOM PoCの概要について、計3件の講演。
   ※ 登壇者：Siemens, INL, Hitachi America

“SBOM-a-rama” 2日目の議論により抽出された主要な課題

観点	議論により抽出された主要な課題（抜粋）
クラウド	• クラウドサービスに対するSBOMユースケースの作成 • クラウドネイティブコンポーネントに対するSBOM生成方法
データマネジメント	• **SBOM生成に必要なデータの提供方法** • OSSコミュニティも含めた適切なデータの統合方法
ツール	• コンテナ環境、仮想環境、AI/ML等に対するSBOM生成ツール • **SBOM共有・活用ツール**
普及・促進	• SBOM活用に向けた教育 • **各国の規制基準への適用** • **SBOMの出所と明確化や信頼性の確保**
共有・交換	• SBOMのアーカイブを残す方法 • **SBOM共有にあたっての信頼性や完全性の確保**
技術導入	• SBOMのハッシュ化方法や署名方法
他分野との融合	• ファームウェアやハードウェアに対するSBOMユースケースの作成

https://www.cisa.gov/cisa-sbom-rama

（参考）【IoT機器】米国：IoT機器を対象にしたサイバーセキュリティガイダンス文書

- 米国NISTは、IoT機器製造者向けに**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)。
- 2021年11月、連邦政府機関向けのガイダンスとしてNIST SP 800-213シリーズを公表。

製造者向けガイダンス

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

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基本的な活動**を定義。

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

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
IoT Non-Technical Supporting Capability Core Baseline
2021年8月公開

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。

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

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)
Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government
2021年11月 廃止

2021年11月に、NIST IR 8259D (Draft)が廃止され、NIST SP 800-213Aとして公表

連邦政府機関向けガイダンス

NIST SP 800-213
(IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements)
2021年11月公開

連邦政府機関向けに、**IoT機器を既存システムに統合する際の検討に資する推奨事項**を定義。

NIST SP 800-213A
IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog
2021年11月公開

連邦政府機関向けに詳細化された**IoT機器のサイバーセキュリティ機能と非技術的サポート機能**のカタログを提供。

NIST SP 800-213は、**NIST SP 800-53 Rev.5**をサポートするために必要となり得る技術的/非技術的な機能を特定するもの

（参考）【IoT機器】米国：大統領令を受けたIoT製品のサイバーセキュリティ・ラベルの検討

- 2021年5月に公表された米国大統領令に基づき、NISTは消費者向けIoT製品のサイバーセキュリティ・ラベリングにおける推奨基準の最新版を公表。
- 2022年5月12日までに、NISTは、上記サイバーセキュリティラベリングに関する総括報告書を発行する予定。

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NISTにて策定

Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products (2022/2/4公開)

- 消費者向けに提供されるIoT製品*を対象にしたラベリング制度を確立しようとする者(制度オーナー)が、実際にプログラムを開発する際に考慮すべき、以下のような検討事項と推奨事項を示している。

* IoT製品(IoT product)には、IoT機器だけではなく、当該機器を利用するために必要な製品コンポーネント(ネットワーク機器、モバイルアプリケーション等を含む)を含み得る。

推奨ベースライン製品基準 (2章)

- IoT製品及びその開発者に期待されるサイバーセキュリティ関連の成果を定義

✓ **資産の識別**	✓ **サイバーセキュリティ状態認識**
✓ **製品の構成**	✓ **ドキュメンテーション**
✓ **データ保護**	✓ **情報及び問合せの受付**
✓ **インターフェイスのアクセス制御**	✓ **情報の発信**
✓ **ソフトウェアの更新**	✓ **教育と意識向上**

ラベリングに関する考慮事項 (3章)

- 推奨するIoTラベルのアプローチ、ラベルを消費者に提供する際の検討事項、消費者教育に関する検討事項等を提示

推奨アプローチ	バイナリーラベル(基準準拠を示す単一のラベル)に、URL等を記載し、追加情報を提供するレイヤーアプローチを推奨。
提示方法	消費者が購入前、購入時、購入後に確認できる必要があり、物理またはデジタルのフォーマットをサポートする。
消費者教育	消費者がアクセスできる内容に、ラベルの意図とスコープ、準拠基準、基準への適合宣言、消費者の責任等が含まれる。

適合性評価に関する考慮事項 (4章)

- IoT製品が製品基準に適合していることを証明するために活用できるIoT適合性評価活動には以下が含まれる。

自己適合宣言	製品提供者自身による基準への適合宣言
第三者による検査・試験	第三者機関によるIoT製品を対象にした試験または検査
第三者認証	総合的な審査に基づき第三者機関が付与する認証

（参考）【IoT機器】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。

「データの越境移転に関する研究会　報告書（概要説明資料）」より抜粋

（参考）【データ】関連規制の現状

- 越境移転規制の対象となる情報や越境移転が許容されるための要件、国内保存・国内保管義務の有無や内容といった各国法令における規定ぶりが国によって大きく異なっており、グローバルに事業展開を行う企業の各国法令への対応コストは、近年ますます大きくなってきている状況。
- 「データ」という存在自体、多面的な性質を持っているため、目的や文脈によって様々な分類が可能でありながら、その境界線には常に解釈の問題が存在しており、シンプルかつ履行しやすい形で一般的なタクソノミー（定義・分類）することは困難。

	越境移転規制							国内保存・国内保管義務			
	法令名	規制の対象となる情報	規制の対象者	越境移転が許容されるための要件				法令名	規制されるデータ	規制の対象者	義務の内容
				当局の認証等	所定の契約	本人の同意	その他				
EU	GDPR	個人データ（識別され又は識別可能な自然人に関する情報）	管理者又は処理者	可能（十分性認定）	可能（SCC、ad hoc契約）	可能	拘束力ある社内規程、公的機関の認証、契約の履行の確保、重大な公益・生命の保護等	個人情報保護法制上は、規制なし			
米国	個人情報保護法制上は、規制なし							個人情報保護法制上は、規制なし			
カナダ	個人情報保護法制上は、規制なし							個人情報保護法制上は、規制なし			

「データの越境移転に関する研究会　報告書（概要説明資料）」より抜粋

	越境移転規制							国内保存・国内保管義務			
	法令名	規制の対象となる情報	規制の対象者	越境移転が許容されるための要件				法令名	規制されるデータ	規制の対象者	義務の内容
				当局の認証等	所定の契約	本人の同意	その他				
中国	個人情報保護法	個人情報（識別され又は識別可能な自然人に関する匿名化していない情報）	個人情報取扱者	他の手続（本人同意）と組み合わせて可能（※）	他の手続（本人同意）と組み合わせて可能（※）	他の手続（安全評価等）と組み合わせて可能	安全評価、法令の定めるその他の条件（※）	個人情報保護法	個人情報	①国家機関、②重要情報インフラ運営者、③一定数に達する個人情報の取扱者	国内保存義務・安全評価
										個人情報取扱者	国外の政府機関への提供につき主管機関の認可
	サイバーセキュリティ法	①個人情報（自然人の身分を識別可能な氏名等の情報）、及び②重要データ（国の安全、経済発展等に密接に関連するデータ）	重要情報インフラ運営者	（規定なし）	（規定なし）	（規定なし）	安全評価	サイバーセキュリティ法	個人情報及び重要データ	重要情報インフラ運営者	国内保存義務・安全評価
	データセキュリティ法	国の安全・利益や国際的義務の履行の維持に関連する管理品目のデータ	（規定なし）	（規定なし）	（規定なし）	（規定なし）	輸出管理	データセキュリティ法	重要データ	重要情報インフラ運営者	国内保存義務・安全評価
										その他のデータ処理者	別途法令で定める
		重要データ	重要情報インフラ運営者	（規定なし）	（規定なし）	（規定なし）	安全評価		（規定なし）	中国国内の組織又は個人	国外の政府機関への提供につき主管機関の認可
			その他のデータ処理者	（規定なし）	（規定なし）	（規定なし）	別途法令で定める				

※重要情報インフラの運営者又は取り扱う個人情報が一定数に達する個人情報取扱者に該当する場合には依拠不可

「データの越境移転に関する研究会　報告書（概要説明資料）」より抜粋

	越境移転規制							国内保存・国内保管義務			
	法令名	規制の対象となる情報	規制の対象者	越境移転が許容されるための要件				法令名	規制されるデータ	規制の対象者	義務の内容
				当局の認証等	所定の契約	本人の同意	その他				
インド	個人情報保護法制上は、規制なし							支払システム情報の保存に関する政令	支払システム情報（エンドツーエンドの取引詳細及び情報）	認可対象となる支払システムの提供者	国内のみでの保存義務
								電気通信分野における統一ライセンス法	サービス利用者の財務情報及び利用者情報	電気通信サービス事業者	国外への移転禁止
ベトナム	個人情報保護に関する政令案	個人情報（個人に関する情報、又は特定の個人を識別し若しくは識別可能な情報）	個人情報に関係する機関、組織及び個人	他の手続（同意、国内保存等）と組み合わせて可能	（規定なし）	他の手続（国内保存、当局承認等）と組み合わせて可能	（規定なし）	サイバーセキュリティ法	個人情報に関するデータ、サービス利用者の関係に関するデータ又はサービス利用者の作成したデータ	ネットワーク上のサービス提供事業者	国内保存義務及び国内拠点設置義務
								政令72号	（規定なし）	オンラインサービス事業者	国内サーバー設置義務
インドネシア	2019年政令及び2016年省規則	個人情報（直接又は間接に個人を識別できる情報）及び個人データ（保管・管理され、秘密性が保護されなければならない情報）	電子システム提供者	（規定なし）	（規定なし）	（規定なし）	通信情報大臣との連携	2019年政令	（規定なし）	公的機関から任命された電子システム提供者	国内での管理・処理・保存義務
	個人データ保護法案	個人データ（保管及び管理された一定の個人データであって、その秘密性が保護されるべき情報）	管理者	（規定なし）	可能	可能	移転先国の規制の同等性、国家間同意の存在	金融庁規則	（規定なし）	ノンバンク金融機関、商業銀行等	国内保存義務

注：水色部分は法案段階のもの

（参考）【IoT機器、データ】中国：主なセキュリティ関連法規

- 中国では、2017年6月のサイバーセキュリティ法施行を皮切りに、「サイバーセキュリティ審査弁法」や「自動車データセキュリティー管理若干規定（試行）」等の付随規定が盛んに策定されていることに加え、特に2021年に同法とともにデータ管理の法的枠組みを構成するデータセキュリティ法、個人情報保護法が施行された。

中国におけるセキュリティ規制3法

2017年6月施行

サイバーセキュリティ法
[中华人民共和国网络安全法]

- 国家の安全保障を目的として、個人情報の保護、機密情報の保全、国外へのデータ移転規制、セキュリティ製品の認証、法的責任と罰則等について規定 (以下、「CS法」と表記)

2021年9月施行

データセキュリティ法
[中华人民共和国数据安全法]

- 中国国内におけるデータの収集、保存、加工、使用、提供、取引、公開等の行為に関連して、政府によるデータ分類・等級分類及び重要データ管理に関する制度の構築、事業者のデータセキュリティ保護に係る義務等を規定 (以下、「データ法」と表記)

2021年11月施行

個人情報保護法
[中华人民共和国个人信息保护法]

- 個人情報の処理や越境移転に係る規則、個人が行使できる権利等を規定 (以下、「個情法」と表記)

3法の規定に関連して定められた下位法令等(例)

- 左記の3法は内容が原則的であり、詳細は以下に例を挙げる下位の法令(条例、弁法、ガイドライン等)にて順次明確化されている。

サイバーセキュリティ等級保護条例	**2018年6月公布**

CS法21条に基づき、データのサイバーセキュリティ等級と、対応する保護措置を規定

工業情報化分野データセキュリティ管理弁法（試行）	**2021年9月意見募集開始**

データ法第21条等に基づき、工業・情報化分野におけるデータ処理活動に関する規律を規定

重要情報インフラセキュリティ保護条例	**2021年9月施行**

CS法における重要情報インフラ運営者のセキュリティに係る責任と義務を規定

サイバーセキュリティ審査弁法	**2022年2月施行**

CS法第35条、データ法第24条に基づき、重要情報インフラ事業者が特定のIT製品・サービスを調達する際に、国が実施する審査に係る申請手続等を規定

個人情報域外移転安全評価弁法	**2021年11月意見募集開始**

CS法第37条、データ法第31条、個情法第38-41条に基づき、国内で収集した個人情報及び重要データを国外へ移転する際に実施する安全評価の要求及び手順を規定

自動車データセキュリティ管理若干規定（試行）	**2021年10月施行**

データ法第30条等に基づき、自動車産業に関連する個人情報及び重要データについて、国内保存の義務付け、国外移転時の国による安全評価等を規定

目次

１．産業分野別SWG

２．第３層タスクフォース

３．ソフトウェアタスクフォース

４．第２層タスクフォース

５．CPSFの国際規格化

前回のWG1・分野横断SWG合同会議における主なご指摘

【産業分野別SWGについて】

- 産業サイバーセキュリティ研究会WG１で策定したCPSFを標準モデルとして、用途別、業界別という観点でSWGが立ち上がってきており、スマートホームや宇宙産業での議論が進んできている。産業分野別ガイドラインによる日本社会全体の底上げを、サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)等の議論や人材育成、ビジネス化など他のＷＧの議論と連携して進める必要がある。
- **各産業分野別SWGにおけるガイドライン作成や展開によって知見が溜まってきており、その知見をフィードバックしてCPSF本体の改定やレベルアップの議論にもつなげていただきたい。**
- 産業分野別に色々な枠組みを作っている一方で、**分野間で共通の部材やIoTデバイスなどが結構出てきているので、全体を見たような対策も考えていただきたい。**
- 各産業分野別SWGにおいて、それぞれ良い成果が出てきているので、**第2層TFでのアウトプットの枠組みを使い、産業分野別に具体的な事例などを検討していくのが良いのではないか。**サイバーセキュリティエンジニアリングについては、開発プロセス等のマクロな議論は進んでいるが、詳細なところは安全分野ほどできてきていない印象。そのようなところに第2層TFの結果などもうまく使っていけるかもしれない。
- 本WGの資料を産業分野別SWGやガイドラインがない分野に紹介すると、自分の仕事にどのように影響するのか、というような反応がある。自分たちも業界ガイドラインのようなものを自主的に作らないといけないのかと感じている方へのメッセージのようなものが必要な段階なのではないか。

電力SWG（座長：渡辺 研司 名古屋工業大学大学院 教授）

- 電力分野のサイバーセキュリティを取り巻く現状、諸外国の状況を分析し、**官民が取り組むべき課題と方向性**について、**短期・中長期という時間軸を加味**しつつ、広く検討。
- **CPSFも踏まえ、さらに取組が加速している諸外国の動きも視野に、電力分野における様々なセキュリティの課題への対応を強化。**

＜構成員＞

有識者（大学教授、弁護士等）、電気事業者、業界団体、情報セキュリティ関係機関

＜2021年度開催実績＞

第12回：2021年12月24日、第13回：2022年2月21日

- **東京オリンピック・パラリンピック**における電力分野のサイバーセキュリティ対策
  →**経済産業省と電力各社における対策強化の取組**の内容と結果の報告
- **大手電気事業者**のサイバーセキュリティ対策について
  →大手電気事業者におけるサイバーセキュリティの対策状況に係る実態把握ついて、**国内外のフレームワークを踏まえた共通枠組みによるアセスメントの実施**
- **新規プレーヤーのサイバーセキュリティ対策について**
  →**小出力発電設備※について、設備設置者、関連機器メーカー等のステークホルダーを対象とした系統連系技術要件の対策実装例の策定** ※ 系統連系する50kW未満の太陽光発電設備、20kW未満の風力発電設備、10kW未満のコジェネレーション設備 等
- **サプライチェーンリスクへの対応について**
  →国際的な検討枠組みへの参加及び最新動向も踏まえた**サプライチェーンリスクへの対応の検討**
- **電力分野のセキュリティ対策の高度化について**
  →電力システムのサイバーセキュリティ対策の高度化に係る**今後の方向性の検討**

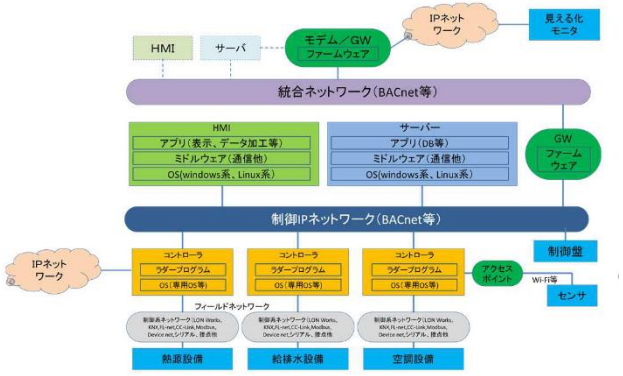
ビルSWG（座長：江崎 浩 東京大学 教授）

- ビルの管理・制御を行うビルシステムに係る各種**サイバー攻撃のリスクと、それに対するサイバーセキュリティ対策を整理**し、ビルシステム全般に共通的な要件をまとめた共通編として、2019年6月17日に**ガイドライン第1版を公開**。
- 2021年度は共通編に続く個別編として「**空調システム」のガイドラインを作成すべく取組中。あわせて、インシデントレスポンス**に対する要求の方針案の整理を行っているところ。

ビルシステムサイバーセキュリティガイドライン（個別編：空調システム）の概要

セントラル空調方式

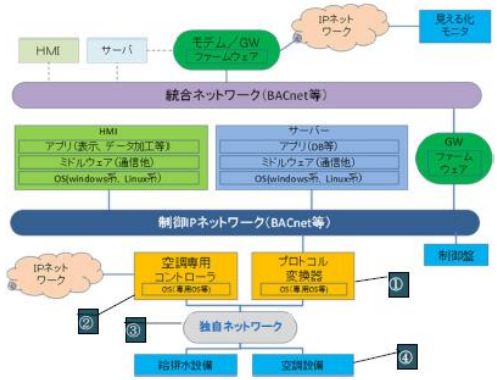
熱源機器（冷凍機、ボイラー等）と空気調和機（エアハンドリングユニット、ファンコイル）とを組み合わせて空調する方式で、一般には熱源機器を一カ所に集中設置し、冷温水を空気調和機に送水して空調する中央式空調とも呼ばれる。



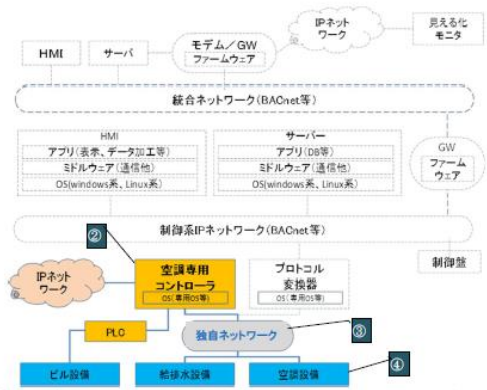
大規模ビル　セントラル空調システム

個別分散空調方式

空調を必要とする部屋毎に空調機を設置する空調方式で、主として冷媒を使用する空調機（ルームエアコン、パッケージエアコン、ビル用マルチエアコン等）が使用される。熱源は、必要箇所に分散して設置することができる。



大規模ビル　個別分散空調システム



中小規模ビル　個別分散空調システム

想定されるビルの空調システムごとのサイバーセキュリティ対策の考え方や、機器・システムごとのリスクや管理策を提示

防衛産業SWG（防衛装備庁 情報セキュリティ官民検討会）

● 我が国の防衛調達におけるセキュリティ強化のための新情報セキュリティ基準制定に向け議論中。

我が国の防衛調達における情報セキュリティ強化の方策について、防衛装備庁と主要な防衛関連企業（２２社４団体）との間で「**防衛調達における情報セキュリティ強化に関する官民検討会**」を開催

＜検討の背景＞

1. **我が国におけるサイバー攻撃の増大**：高度化するサイバー攻撃により、我が国のサプライチェーンが標的となる可能性。
2. **米国の情報セキュリティ強化の動き**：米国の新標準（NIST SP800-171）を満たすことが、今後の米国をはじめとする国際共同研究・開発への参加を継続する最低条件となる可能性。

＜対応方針＞

契約企業が保護すべき情報を取り扱う際に適用される情報セキュリティ基準を、**米国の新標準と同程度まで強化した新情報セキュリティ基準を策定**。【令和４年４月１日策定】

＜開催の状況＞

	開催日	検討テーマ
第１回	平成２９年　２月２８日	米国の防衛調達における情報セキュリティ強化の動向
		我が国の防衛調達における情報セキュリティ強化の方向
第２回	平成２９年　４月　５日	情報セキュリティ強化のためのルールのあり方
第３回	平成２９年　５月１９日	
第４回	平成２９年　６月１５日	中間的論点整理
第５回	平成２９年１１月２８日	これまでの振り返り及び現在の検討状況
第６回	平成３０年　３月２９日	新基準適合に向けた取り組み
第７回	平成３０年　９月　５日	防衛調達におけるサイバーセキュリティの強化に向けて
第８回	平成３１年　２月２８日	サイバー攻撃に関する留意事項、米国企業のNIST SP800-171対応状況
第９回	令和　元年　８月２６日	新情報セキュリティ基準（案）
第１０回	令和　３年１２月　９日	新情報セキュリティ基準（案）等

第６回検討会より、経済産業省 産業サイバーセキュリティ研究会と連携を図るため「**産業サイバーセキュリティ研究会WG1防衛産業SWG**」として実施。

自動車産業SWG (一般社団法人　日本自動車工業会　総合政策委員会)

- 日本の自動車業界として対象のセキュリティフレームワーク・ガイドライン・実現レベルを定め、活用を推進することで、適切なセキュリティ対策の実施を図る。
- 2021年度は、**「自工会／部工会サイバーセキュリティガイドライン1.0版」の展開**および**レベルアップ版の作成**、**工場セキュリティの課題検討**等を実施。

＜メンバー構成＞
日本国内の乗用車、二輪車、商用車生産の14社

＜開催状況＞
- 2019年4月16日 第1回 電子情報委員会／サイバーセキュリティ部会を開催。
- 2020年12月4日 第1回 総合政策委員会／ICT部会／サイバーセキュリティ分科会を開催。
  （自工会の組織体制変更に伴い名称変更）
- 2021年度も月1回の会合を継続して開催し、自動車業界のサイバーセキュリティ対応を推進。

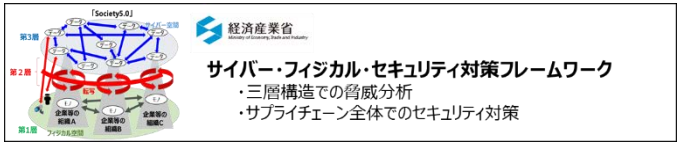
＜2021年度進捗＞
- 2020年度に公開した**「自工会／部工会サイバーセキュリティガイドライン1.0版」をサプライチェーンに展開**し約2300社の適用状況を集約。**自社の取組状況を業界平均と比較し取組の優先順位付けに活用可能なツールを作成**して集計結果と共にフィードバック。
- レベルアップに向けて**項目を拡充したガイドライン2.0版の作成**を実施。2022年4月公開予定。
- 情報共有ルールを定め、**自工会内での脆弱性、脅威、サイバー攻撃等の情報交換活動**を開始。
- **工場セキュリティの課題対応**のため、共通的な資産およびその管理情報リストの作成、工場領域へ上記ガイドラインを適用する場合のFit & Gap分析を実施。
- 令和4年度は工場SWGとも連携しつつ**工場分野で最低限守るべきルール等の標準化や文書化を予定**。

スマートホームSWG (JEITA　スマートホームサイバーセキュリティWG)

- 製品安全の観点も含めた**スマートホーム分野のサイバー・フィジカル・セキュリティ対策ガイドライン**を発行（2021年4月）
- 経済産業省の「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）を参照しつつ、スマートホーム特有の　脅威に基づいて、セキュリティ対策を検討。スマートホームに関係する幅広い関係者に向けたガイドラインをまとめた。
- 2021年度は、**ガイドラインの普及啓発に向けた活動、ガイドラインの課題整理、識者・最新事例共有**を実施。
- 今後は、「デジタル田園都市構想」における家庭生活／シーンのユースケースやモデルについて検討を行うなど、更なる普及啓発に向けた活動を行っていく予定。

ガイドラインの普及・啓発

＜ガイドラインの発行＞



スマートホーム特有の脅威
① **膨大な攻撃対象**（世帯数はおよそ5300万世帯）
② **マネジメント不在**に起因する脆弱性
③ 利用者側の**誤操作等**による想定外のインシデント

＜ガイドラインの普及啓発パンフレットの制作＞

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

ガイドラインの課題整理

【SWG有識者会議 及び WG1（令和3年3月15日（月））からのご意見 】
・各ステークホルダーがガイドラインの内容を理解し、特に事業者において、**それぞれの事業や業務の具体的な手順や設定への落とし込み**。
・ガイドラインの判読性を高めたり、住まい手に関心を持ってもらうための工夫。**セキュリティの考え方を国民全体の利益として実践**（普及啓発）。
・**バージョンアップ対策**・**IoT デバイスの誤設定・ヒューマンエラーをどう防ぐかという教育**も重要。

【JEITA内における追加的な論点整理】
・スマートホームが収集するデータとそのデータに紐づいた**個人情報の保護への対応**についての検討。
・**データ連携時やシステム間連携時のセキュリティ**に関する検討（プライバシー含）。

宇宙産業SWG（座長：坂下 哲也 JIPDEC 常務理事）

- 「民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインβ版」を作成し、パブコメを実施したところ。今後、パブコメ結果を整理の上、発行手続きを進めていく予定。

＜メンバー構成＞

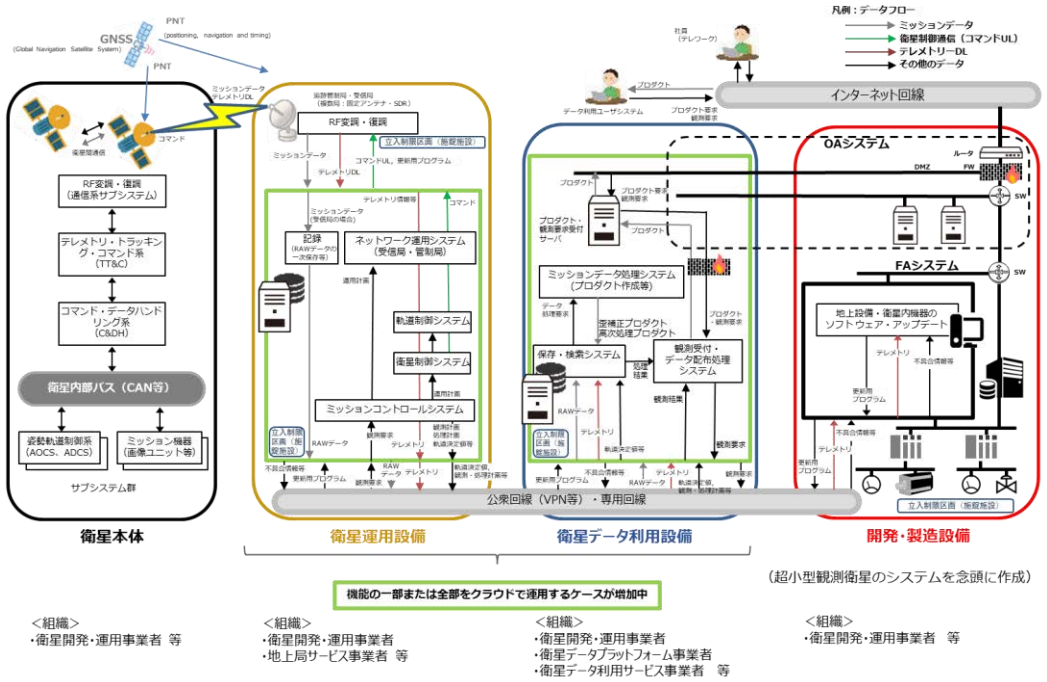
宇宙産業事業者、宇宙関係の業界団体・NPO、有識者（大学、産業サイバーセキュリティ専門家等）

＜開催状況＞

2022年2月にSWGの第4回を開催。また、作業部会を計2回、作業部会コアメンバー会議を計5回開催。

＜2021年度進捗＞

- ガイドラインβ版を開発し、2022年2月からパブコメを実施。
- ガイドライン開発の目的は、民間宇宙事業者のビジネス振興及びサイバー攻撃による倒産等の経営リスク軽減の観点から、宇宙システムに係るセキュリティ上のリスク、検討すべき基本的対策等について分かりやすく整理して示し、自主的な対策を促すこと。
- 右記の標準的なモデルを開発し、リスク分析を行い、サブシステムごとの対策を整理。



民間宇宙システムの標準的なモデル

工場SWG （座長：江崎 浩　東京大学 教授）

- 2022年1月6日に工場SWGを設置し、これまでに計3回開催。委員、オブザーバー、ヒアリング対象など、主な関係団体・企業も広く参画し、工場セキュリティガイドラインの策定に向けて活動。
- 3月23日の第3回SWGでは、パブコメ実施に向けたガイドライン案を審議した。現在、パブコメ実施に向けた修正作業を実施中。

開催実績

第１回　工場SWG設置について

第２回　主な産業界団体・企業からのヒアリング

日本自動車工業会、電子情報技術産業協会半導体部会、NEC プラットフォームズ、パナソニック、日本鉄鋼連盟、日本医療機器産業連合会、日本工作機械工業会

第３回　パブコメに向けたガイドライン案の審議

委員名簿

江崎 浩（座長）	東京大学 教授
岩﨑 章彦	電子情報技術産業協会
榎本 健男	日本工作機械工業会
桑田 雅彦	日本電気株式会社
斉田 浩一	ファナック株式会社
佐々木 弘志	フォーティネットジャパン株式会社
斯波 万恵	株式会社東芝
高橋 弘宰	トレンドマイクロ株式会社
中野 利彦	株式会社日立製作所
西雪 弘	三菱電機株式会社
藤原 剛	ビー・ユー・ジーDMG森精機株式会社
松原 豊	名古屋大学　准教授
村瀬 一郎	技術研究組合制御ｼｽﾃﾑｾｷｭﾘﾃｨｾﾝﾀｰ
渡辺 研司	名古屋工業大学　教授

ガイドラインの目的

- 一般的に、製造業／工場では、事業／生産継続(BC：Business Continuity)、安全確保(S：Safety)、品質確保(Q：Quality)、納期遵守・遅延防止(D：Delivery)、コスト低減(C：Cost)という価値が重視されている 。
- 工場と言っても、業界・業種ごとに実施すべき事項は異なることから、本ガイドラインは**特定の業界・業種や製造する製品という観点で対象を限定したものではない。**
- 業界団体や個社が**自ら対策を企画・実行するに当たり、参照すべき考え方やステップを「手引き」として示し** 、また、**必要最小限と考えられる対策事項として脅威に対する技術的な対策から運用・管理面の対策までを明記**している。
- 重要なことは、業界団体や個社が、本ガイドラインに示した考え方やステップ、対策を参照しつつ、業界・業種の事情に応じたガイドラインを作成するなどしながら工場へのセキュリティ対策を進めていく、といった行動に移すことである。
- 本ガイドラインは、**各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティレベルの底上げを図ることを目的**としている。

目次（検討中）

１．産業分野別SWG

２．第３層タスクフォース

３．ソフトウェアタスクフォース

４．第２層タスクフォース

５．CPSFの国際規格化

前回のWG1・分野横断SWG合同会議における主なご指摘

【第3層TFの検討内容について】

- なかなかデータ流通が進まないところに対し、転々流通と加工を前提にデータへ着目して整理していくというアプローチはとても良い。**<u>責任主体、ステークホルダーがどのような責任を持つのか、色々なバリエーションがあるので、ユースケースとして整理していくと良い。</u>**
- 第3層TFの領域は、トラストもしくはデジタルトラストと言われている領域にかなり関係すると理解しており、デジタルトラストという言葉一つとっても、語る人によって大分範囲が違うという印象を持っている。デジタルトラストもしくはトラスト全体をどのような枠組みや建付けと捉え、その中で第3層TFはどのような部分を詰めていくのか整理いただけるとありがたい。
- APIとプロトコルをしっかり区別することが重要。APIを公開すればつながるだろうという議論が行われることがあるが、そこだけで実装するのは非常に困難で、共通のプロトコルが必要になる。第3層TFの議論はこの課題に対応したものになる。
- アンバンドル化が目標の一つに掲げられているが、第3層が処理されるクラウド等の場を考えると、非常に適した考え方。
- 産業機器のデータについて欧州と議論するとGAIA-Xの話が出てくる。**<u>日本の製造業各社の機器のデータが日本の各社に戻ってくるようにするためにも、GAIA-Xなどとの整合性も視野に入れると良い。</u>**
- 基準となる属性のセット、オントロジーのようなものが決まっているとよい。国で議論している日本版NIEMや共通語彙基盤のようなところの議論と組み合わせて検討いただけるとありがたい。

データマネジメント・フレームワークの概要

- 2022年２月から３月に、「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）」のパブリックコメントを実施。
- パブリックコメントでいただいた御意見の反映を行うとともに、タイトルを「**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**」に決定。**本日、ご報告の上、発行に向けた手続きを進める予定。**

基本情報

◆ フレームワークの目的

- **主体間を転々流通するデータの信頼性を確保**することで、バリュークリエイションプロセスが付加価値を生み出す
- **データを軸に置き、ライフサイクルを通じて、データの置かれている状態を可視化**してデータに対するリスクを洗い出し、そのセキュリティを確保するために**必要な措置を適切なデータマネジメントによって実現**
- フレームワーク適用の具体的な効果としては、主に以下を想定。

① as is の対策の検討

- ガバナンスを含めた**必要な措置をステークホルダーが協調して実施**
- 洗い出されたリスクへの対策要件例として、これまでに公表されてきた情報セキュリティに関する様々な国際標準等を参照

② to be の対策の検討

- **データ流通を促進するために必要な条件を明確化**。プロトコル設計が容易に
- オープン化された環境で**データ連携やシステムの組み合わせの自由を確保**することを可能に
- **各国の制度間のギャップ分析**を行い必要な調整措置を明らかに

◆ 想定読者

- バリュークリエイションプロセスに参加する者
- データ利活用に関するサービスを提供する者
- データ利活用に関するサービスを提供するシステムの設計・構築・運用に関わる者
- トラストサービスを提供しようとする者
- データセキュリティに関わるガイドライン等のルール設定に関わる者

フレームワークの構成

◆ 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

フレームワークに基づくリスク分析の手順

- **下記の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**。
- 「属性」、「場」、「イベント」が相互に依存する関係にあることから、STEP1～3の**各ステップは不可逆的なものではなく、互いにフィードバックをかけながら検討されることが適切**。
- リスクの洗い出しに当たっては、機密性・完全性・可用性といったサイバーセキュリティに係る観点の他、各法制度等に係るコンプライアンスの観点でのリスクについても洗い出す必要。

◆ フレームワークに基づくリスク分析の手順

STEP 1
データ処理フロー（「イベント」）の可視化

- **データの生成・取得から廃棄に至るまで、想定されるデータ利活用プロセスにおける大まかなデータフロー及び「イベント」を可視化**する。
- 「イベント」をどの程度詳細に記述するかは、データフロー整理の目的に応じて調整する必要がある。

STEP 2
必要な制度的な保護措置（「場」）の整理

- **データ保護に資する「場」(必要な制度的な保護措置)を検討**し、法律・契約の観点から適切なものを設定する。
- 一つのデータに対して複数の「場」が重なり合う、つまり、**データに対して様々な観点からの要求がなされることが考えられる**。

STEP 3
「属性」の具体化

- **設定されたデータや「イベント」、「場」に基づいて、管理上あるべき「属性」を特定**する。
- 場合によっては、データの「属性」を整理していく中で、本データが取り扱われるべき「場」や実施されるべき「イベント」に漏れがあった場合、適宜追加等を実施する。

STEP 4
「イベント」ごとのリスクの洗い出し

- 設定された「場」という観点から、**「イベント」ごとに想定されるリスクを抽出し、設定した「属性」をレビュー**する。
- 機密性・完全性・可用性といった**サイバーセキュリティに係る観点のほか、各法制度等に係るコンプライアンスの観点でのリスクについても洗い出す必要**がある。

添付A：ユースケース

- フレームワーク本文では、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

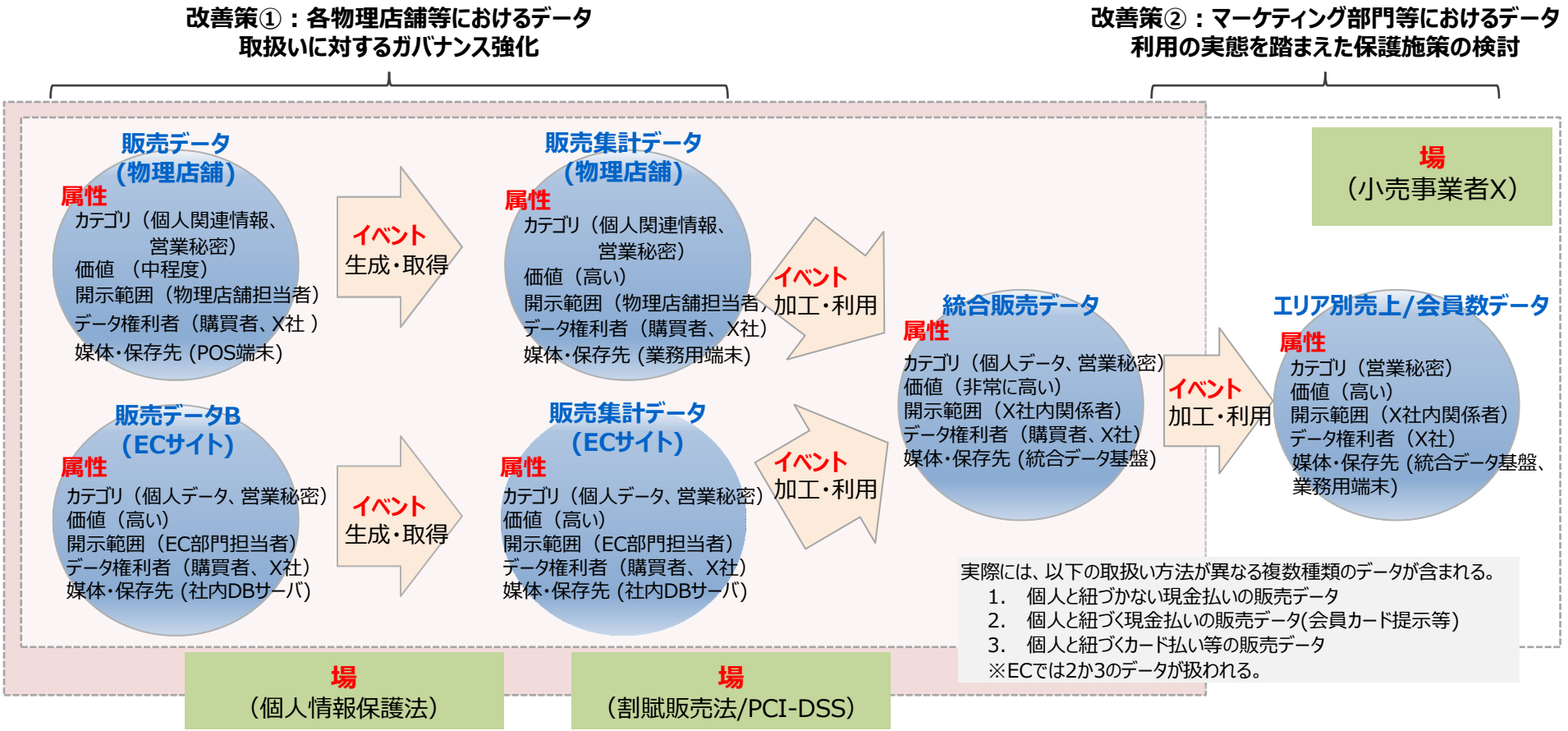
4

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）①POSデータの分析

- 小売業におけるPOSデータの活用事例では、物理店舗及びECサイトの利用顧客から収集した販売データを統合し、マーケティング等の目的で活用する過程を対象に、データ管理の高度化に向けた課題、改善策の検討を実施。

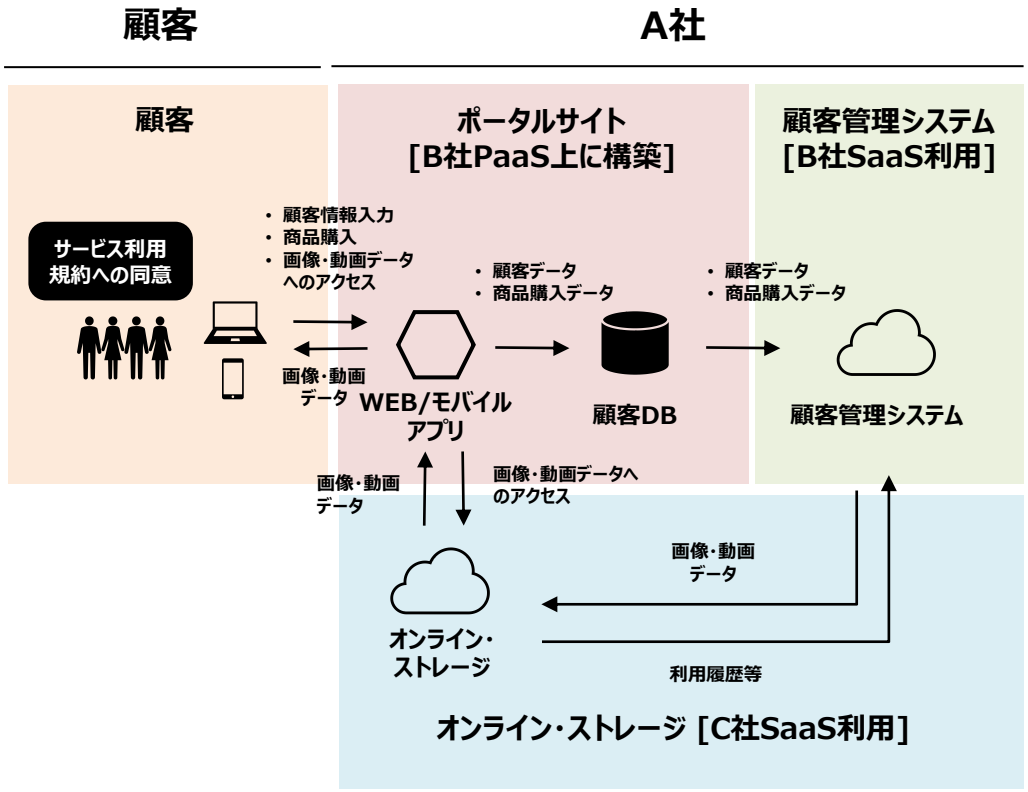
◆ 小売業におけるPOSデータの活用事例



（参考）③IaaS、PaaS、SaaSを利用してサービスを提供する例

- サービス・物販事業者が提供する画像・動画データ管理を行うクラウドサービス事例を取り上げる。
- クラウドサービスを活用することで、コスト低減、技術革新対応力・柔軟性の向上等のメリットが得られる一方、サービス提供者と利用者の間の責任分界に対する認識が曖昧になりがちであったり、データの地理的所在等の透明性の不足等の課題が存在する。

システム・サービス概要

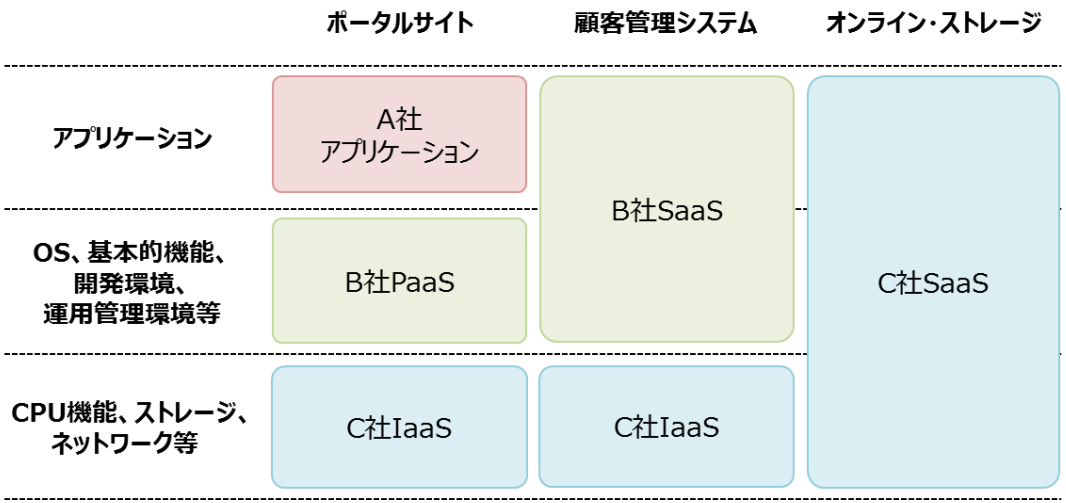


- サービス・物販事業者を運営するA社は、従来の店舗サービスの提供に加え、顧客向けポータルサイトにて画像・動画データをダウンロードするサービスを提供している。
- A社のポータルサイトは、B社の提供するPaaS上に構築され、さらにB社SaaSとして提供される顧客管理システムにもデータ同期を行う。
- データはC社IaaSとして提供されるオンライン・ストレージに格納され、顧客はポータルサイトを経由してアクセスすることができる。

（参考）③IaaS、PaaS、SaaSを利用してサービスを提供する例

- 本ユースケースで考慮すべきステークホルダーは以下の通り。
- 本ユースケースでは、A社のシステム構築のため契約するB社SaaS及びPaaSが、実際はC社IaaS上で構築されるといった関係がある。こうした「クラウドサプライチェーン」を米国国立標準技術研究所（NIST）等の分類を元に整理する。

クラウドサービス提供に係るサプライチェーンの概要



経済産業省「クラウドセキュリティガイドライン活用ガイドブック 2013 年度版」 クラウドサプライチェーンにおける一般的な課題

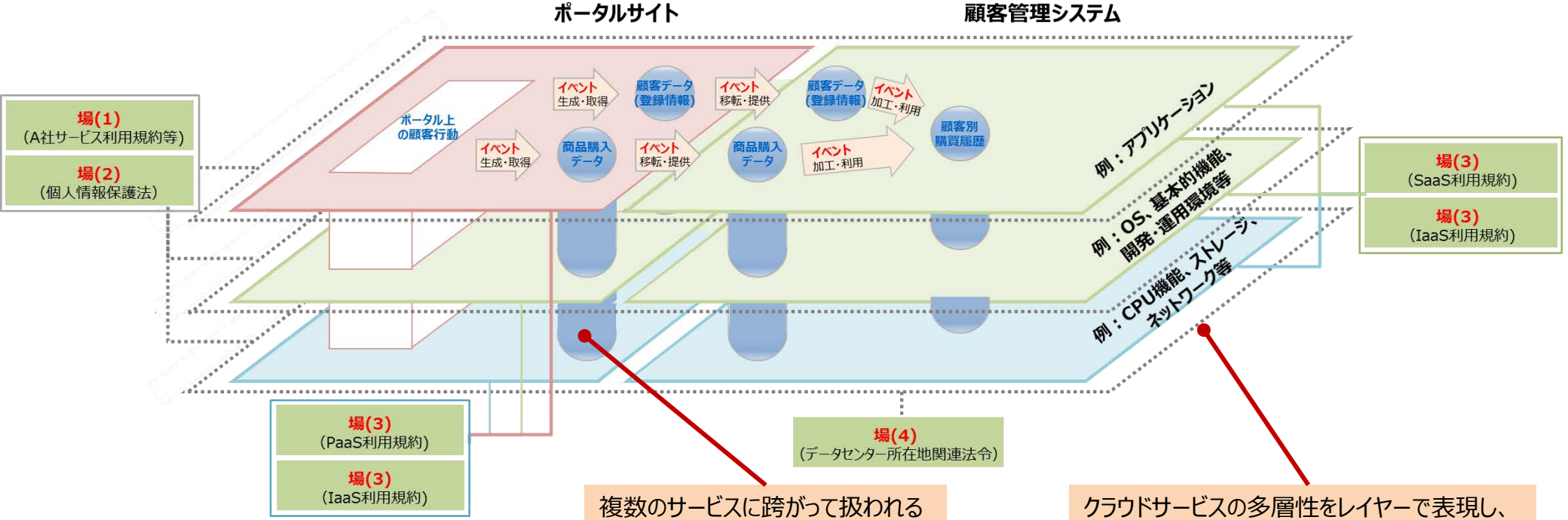
- A社のようなクラウドカスタマから見た直接の契約先（ここではB社）に問題がない場合にも、**配下に存在する PaaSやIaaSに問題が生じた際、連鎖的な問題に巻き込まれる。**
- 障害が要因となり事業活動に何らかの損害が生じた場合に**事業者間で責任分界があいまいになりやすい。**
- 法規制上の問題やクラウドサービスカスタマのセキュリティポリシー等に関連して、外国や外国法適用配下に情報を置くべきでないとされているにも関わらず、サプライチェーンの配下に該当する事業者が存在し、**カスタマの意図に反する状態に陥ってしまう。**

（参考）③IaaS、PaaS、SaaSを利用してサービスを提供する例

- 多層的なサービスにおけるデータ処理フローの可視化と必要な制度的な保護措置を整理する。

今回のデータ処理フローで取り扱う部分
- ポータルサイト上では顧客による自身のデータの入力や製品等の注文、その他の行動に応じて、「顧客データ」、「商品購入データ」等が「生成・取得」され、顧客DBに格納される。
- 当該データは、適時にB社が提供する顧客管理システムに「移転・提供」され、A社内の個別のニーズに応じてA社従業員により「加工・利用」される。

今回のデータ処理フローで取り扱わない部分
- A社所有の撮影機材により、顧客の画像・動画データが「生成・取得」され、
- A社従業員によりC社の提供するオンライン・ストレージへ「移転・提供」され、「保管」される。
- 画像・動画データは、顧客からの求めに応じて「加工・利用」（オンライン・ストレージ上での画像編集等）されたうえで顧客所有の端末（PC、スマートフォン等）に「移転・提供」される。



複数のサービスに跨がって扱われるデータを円柱で表現した。

クラウドサービスの多層性をレイヤーで表現し、各社の責任分界を含む「場」を示した。

（参考）経済産業省 データの越境移転に関する研究会

- 2019年1月、ダボス会議において日本がDFFT（Data Free Flow with Trust）を提唱し、同年6月のG20貿易・デジタル閣僚会合でDFFTを盛り込んだ閣僚宣言に同意。
- 2023年に日本で開催される予定のG7に向けて、研究会では各国における規制状況の把握、相互運用可能な枠組みに向けた検討を進める。

【第１段階】データの取扱に関する制度の問題点をお互いに指摘し合う

- 2021年秋に勉強会を立ち上げ、2021年度内に成果を公表。
  - 越境流通のニーズが高いデータ（具体例）
  - 各国のデータ取り扱いに関する制度の概要
  - 比較分析に必要な枠組みの要素
  - ペインポイントの特定

【第２段階】各国間のギャップ分析をOECDなど国際機関と連携して実施

- データ取扱に関する各国の制度を同じ尺度で比較分析する調査を2022年度中に実施
- 比較分析の枠組みとして、日本で検討中の「データ・マネジメント・フレームワーク」※を応用することも選択肢

※データを軸に置き、データのライフサイクルを通じて、その置かれている状態を可視化してリスクを洗い出し、そのセキュリティを確保するために必要な措置を適切なデータマネジメントによって実現することを可能とするフレームワーク。経産省が提案（2021年10月一次パブコメ終了）。

【第３段階】各国間のギャップの調整措置を行うための体制の構築を決定（2023年G7）

- 各国間のギャップを調整する措置の実行とモニタリングを行う体制を有志国で構築することをG7（2023年日本開催）で宣言。

（参考）オンラインアプリ会社における、商品開発における利活用ニーズ

■ データ利用の概要・目的

顧客の基本データと当該顧客のアプリ利用実績から、顧客のタイプごとの利用傾向などを分析し、公的データなどの外部から入手した データと組み合わせ、既存アプリの改善や新規アプリの開発に利用する。

■ データ管理方法

顧客から収集したデータは、リージョンごとのクラウドに保存されるが、加工開発チームが属するリージョンのクラウドに移転され、統合・分 析され、新製品・サービス開発に利用されている。

データのライフサイクル

生成・取得

- 顧客の基本データ（ユーザーがサービス利用登録時に入力）
- 顧客の利用状況データ（サービスの利用により生成されるデータ）
- オープンソース・公的データ

＜越境移転の状況＞
基本的にリージョンごとクラウドに保存されているが、保存先の地域外から、「越境アクセス」する可能性がある。

＜ペインポイント＞
- 越境移転の定義があいまい（アクセスかデータの所在か）
- リージョンを超えた収集が必要でも移転元・先との法令の違いに合わせて移転できるもの・域内保存するデータの範囲を調べるのが煩雑
- 法令解釈の不透明性

＜想定される対応策＞
政策ガイドラインの策定など

加工

- 個人情報と非個人情報の切り分け、個人情報を匿名化
- 検索履歴や公的データ等は、パラメーターごとに整理（いわゆる構造化）
- 整理されたデータを商品開発の用途によって組合せ・統合

＜越境移転の状況＞
構造化までは各リージョンで行う。製品開発の用途に応じて、統合前後に、「越境移転」もしくは「越境アクセス」する可能性がある。

＜ペインポイント＞
- 個人情報や越境移転の定義があいまい。特にライフサイクルの中で加工・統合が進むと確認 がより困難に。
- リージョンを超えた収集が必要でも、移転元・先との法令の違いの調査コストや法令解釈の不透明性から対応できない

＜想定される対応策＞
政策ガイドラインの策定など

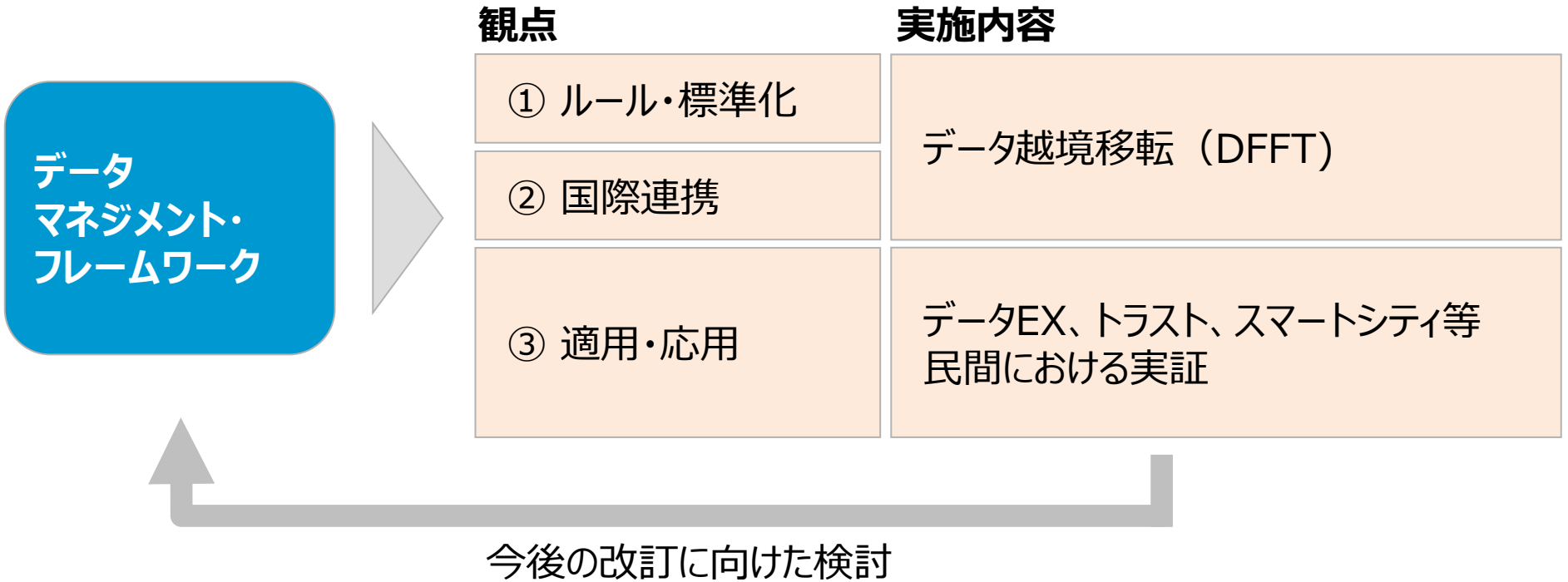
利用

- 統合されたデータを新製品・サービス開発に利用

＜越境移転の状況＞
任意のクラウドに各リージョンから集約したデータを保存し、各地の開発担当者がアクセスする場合がある。

3層TFの今後の取組（案）

- 現在のフレームワークの理解が難しい点もあり、まずは包括的視点でアーキテクチャを整理している行政分野での取組における適用・応用を目指す。そこから民間への横展開や基盤・ツールでの展開が考えられる。
- 経産省「データの越境移転に関する研究会」のデータの取扱に関する各国の制度のギャップ分析において、本フレームワークの応用が進行中。今後国際機関との連携も視野に。
- 民間においても先進的なユーザ・事業を対象に、実証を通じて有効性の検証を行えないか。
- これらの取組を通して得られた知見や課題を、今後のフレームワーク改訂の参考とする。



直近の第３層TFでの主なご意見

【フレームワークのユースケースについて】

- 高齢者生活支援事業の提供においてサービス事業者に渡す情報は、**個人情報や個人関連情報など、色々な可能性がある**のではないか。個別事案の話に**実務的なことを持ち込むと具体性が出て良い反面、普遍性がなくなるというジレンマ**があるため、そのバランスは今後も検討する必要。また、改正個人情報保護法を踏まえた記載であることなど、パブコメの際に誤解が無いよう明確にしてほしい。
- 将来的には、具体的なユースケースとして、コレクティブなことが求められるような場においてどのようなリスク分析をすれば各主体がリスク認識を共有できるのか、体制や利害とかが異なる中で、どのようにコレクティブマネジメントを実現していくのかの深堀にも期待。
- 新たなデータマネジメントのフレームワークが浸透していけば力になるだろうと思う一方で、**概念が難しい**ため、分かりやすいものとすることが、浸透させるうえでは非常に重要。

【今後の取組について】

- フレームワークの適用・応用先として**行政分野が端緒**となる点は承知した。デジタル庁の重点取組み対象である教育や防災、介護のいずれも基礎自治体が関与するが、その点で様々な制約が生じていると聞いている。可能であれば自治体を巻き込んでケーススタディができると望ましい。改正個人情報保護法では官民一体化が掲げられていることから、それらの問題も順次改善されていくものと想定している。

１．産業分野別SWG

２．第３層タスクフォース

３．ソフトウェアタスクフォース

４．第２層タスクフォース

５．CPSFの国際規格化

前回のWG1・分野横断SWG合同会議における主なご指摘

【ソフトウェアTFにおけるSBOMの実証事業について】

- SBOMの実証を我が国でも実施したいという話には賛同。他方、米国のように金融やヘルスケアへ適用するには様々な問題や課題もある。分野横断SWGを活用し、適用分野を含め検討するとよい。また、**実証の中で、脆弱性管理の負担をシェアできる等の具体的なメリットを示せると良い。**

- 大手サプライヤーは個々にSBOMのようなソフトウェアの構成情報を登録し、脆弱性等の影響分析等を行っているが、業界として取り組むことに意味がある。他方、組込みソフトウェアの多い業界では、どのようなソフトウェアを使っているのか自体が競争力の源泉である場合もあり、SBOMの共有には抵抗感もある。競争力ではないところを選んで共有できるとか、他社には知られないが、登録しておけば自分のところが使っているソフトウェアの脆弱性を知ることができるシステム等、安心感を与えるような形で進めることが重要。

- 中小企業や組織にとっては、SBOMの活用も含めOSS管理が大変なためにOSSの活用が進んでいないという現状があると認識。実証においてそのような課題が解決されることを期待。

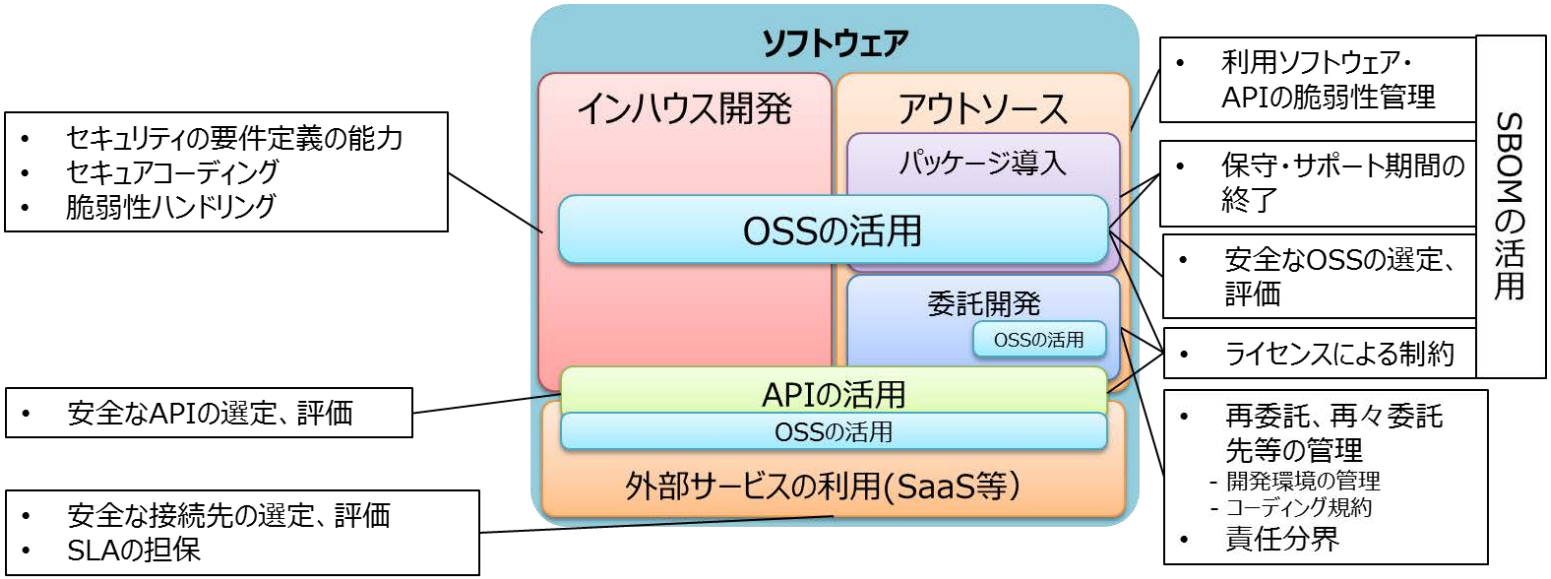
- OSSだけではなく商用ソフトウェアも含めて名称の統一化などができていないと、非常に手間もかかり共有が難しいため、**名称およびフォーマットの統一のようなところの取組があると良い。**

前回資料再掲

ソフトウェアタスクフォースの検討の方向性

- 仮想化技術の進展などにより、**OSSを含むソフトウェア技術への依存が高まる中**で、**ソフトウェアの管理手法、脆弱性対応やライセンス対応等の重要性が増している**。
- 2018年、**米国NTIA（電気通信情報局）は、「Software Component Transparency」を設立**し、ソフト部品構成表である**SBoM (Software Bill of Material）の活用に関する議論**を推進。
- ソフトウェアタスクフォースでは、**適切なソフトウェア（特にOSS）の管理手法、脆弱性対応やライセンス対応等を検討**。

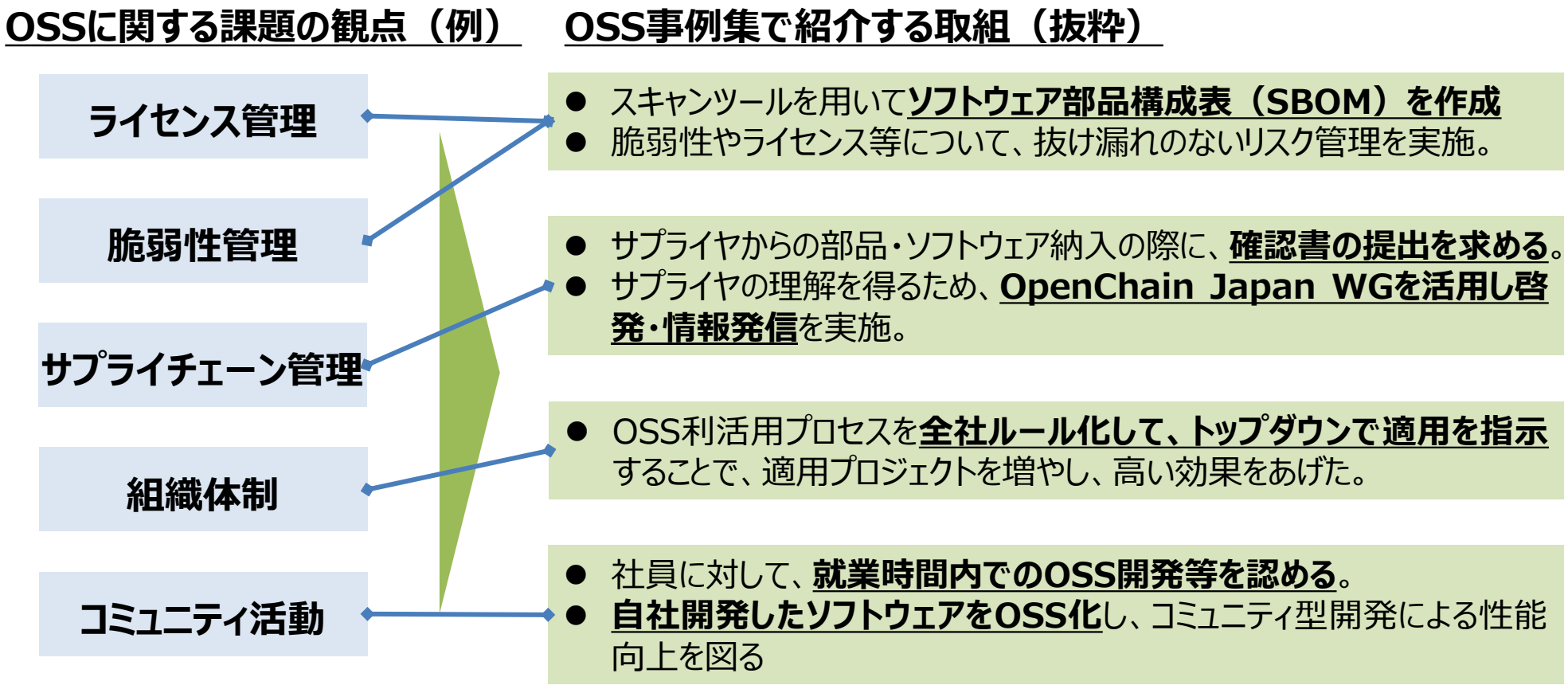
ソフトウェアを利用する際に考慮すべき観点



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



OSS管理手法に関する事例集の拡充

- 令和3年度もOSS利活用に関するヒアリングおよび机上調査を実施。
- 2021年4月21日に公開した「OSSの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」に追記のうえ公開予定。

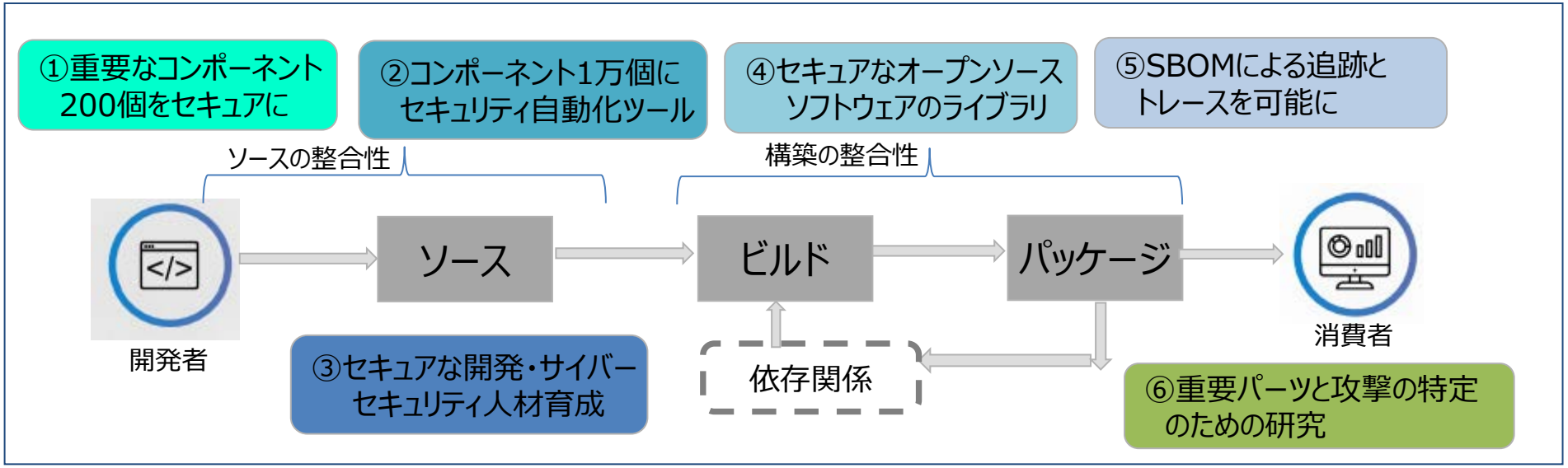
企業・組織	事例の概要
SCSK	意図しないOSSが混入していないかを検査するOSS混入検査システム、安全性を確認したOSSを登録し、OSS調達時に利用できる選定調達システムを構築。また、良質なOSSの選定のため、独自のOSS評価結果をレーダーチャートで可視化するシステム（OSS Radar Scopeとして公開）を開発し、OSS利活用に係る課題やリスクに対応している事例。
OSSTech	中小企業のシステム開発でも構成管理が可能な例として、ビルドシステム等のOSSに備わっているパッケージ管理システム等の機能を活用しながら、ソフトウェアの依存関係を開発者自らが管理し、省力化及び効率化した構成管理を実施している事例。
三菱電機インフォメーションシステムズ（MDIS）	通信キャリア向けにOSSを含んだソリューションを提供する際、OSSコミュニティによるサポート終了のリスクや、OSSを長期間利用する上での脆弱性管理やアップデート対応に係るコストの考え方等について、顧客と事前に合意することの重要性を示した事例。
NEC PSIRT	PSIRTを設立し、CVE Numbering Authority（CNA）としても活動を開始。脆弱性情報の収集、対応方針の整理、対応の社内調整を行っている。また、開発するシステムの構成情報を登録し、構成情報とともに脆弱性対策の有無及び報告を管理するシステムを構築・運用することで、構成管理と脆弱性対策の効率化、対策漏れ防止を実施している事例。
ラキール	あるOSSでの商用利用を制限するライセンス変更をきっかけに、利用しているOSS全てをチェックするために、ツールを利用。従来のExcel管理による管理漏れを防止し、ツールによって早い段階で危険なOSSを把握できるようになった事例。

（参考）Linux FoundationによるOpenSSF

- Linux Foundation（LF）は、SBOM開示等を含む米大統領令の署名以降、OpenSSFを立ち上げ、セキュリティ自動化ツールの開発・サイバーセキュリティ人材教育等を行っている。
- 2021年末のLog4j脆弱性発覚以降、米ホワイトハウスがセキュリティサミットを開催し、LFも参加。
- ソフトウェア脆弱性にグローバルに対応するため、日本企業の経営層（CTO/CIO等）の認識を得て、日本企業からOpenSSFへの積極的な参画を切望。春頃、東京でのセミナー開催を検討。

Linux Foundation
41カ国の2300以上の組織が加盟する非営利の技術コンソーシアム

Open SSF（Open Source Security Foundation）
SBOMフォーマットの標準（SPDX）をサプライチェーンにて適用すべく、日本を含め国際的な協調を目指し、以下のような仕組みを構想中。



国内でのSBOMの活用促進に向けて（実証事業（PoC）の実施）

前回資料再掲

- 米国NTIAが主導するSoftware Component Transparencyでは、ヘルスケア分野におけるPoC等を通じて、ベストプラクティス等を記した成果物が作成・公表されつつある。
- 他方、ソフトウェア分野における業界構造や商習慣が異なる日本においては、総論としてSBOMの有用性は理解されているものの、実際の活用促進に向けては、導入コストをはじめとして様々なハードルがある。
- 第４回TF（2021年１月）において、適切なSBOMの活用を推進するために、実証事業の実施および検証事項等について議論いただいた。

NTIAが公開したドラフト文書の概要（10月22日時点）

Requirements for Sharing of Vulnerability Status Information ("VEX") v0.1

SBOMによって明らかになる脆弱性が必ずしも悪用可能であるわけではないため、そのexploitabilityを評価する仕組みの検討等を示唆

Playbook for SBOM Consumers

SBOMを受領したソフトウェア利用者がそのSBOMをセキュアに管理するための観点（契約や知的財産等）、ソースコード納品の場合/バイナリ納品の場合それぞれのSBOMの完全性の検証、特にコンパイルやコンテナ実行時などに追加の依存関係が生じることへの注意など、実践的な内容を多く含む

HDO SBOM PoC 2.0 Quick Start Guide v1.2

ヘルスケア部門におけるPoCにおいて、活用した技術、SBOMに含まれる項目、SBOMの取込から脆弱性/リスク管理等、ユースケースに基づく情報を紹介

SBOMのPoCで示したい内容

（SBOMの導入にかかるコスト）＜（SBOM導入により削減できる脆弱性対応・ライセンス管理のコスト）

SBOMの活用促進に向けて検証すべき事項（仮説）

●適切なSBOMの活用レベル

・自社におけるSBOMの活用
・サプライチェーンにおけるSBOMの共有
・共有したSBOMの活用　etc.

低 ↓ 高

・導入コスト
・コスト削減効果

●適切なSBOMの活用・共有の範囲

業界、サプライチェーン、個社　etc.

●SBOMの導入に適した分野

業界構造・商慣習等を踏まえる必要がある　etc.

●SBOM導入に向けた技術的検討が必要な観点

SBOM生成・共有・検証・管理手法
各コンポーネントの名称等、フォーマットの統一方法　etc.

●その他

実効性の担保方法（契約への盛り込み、ガイドライン等）

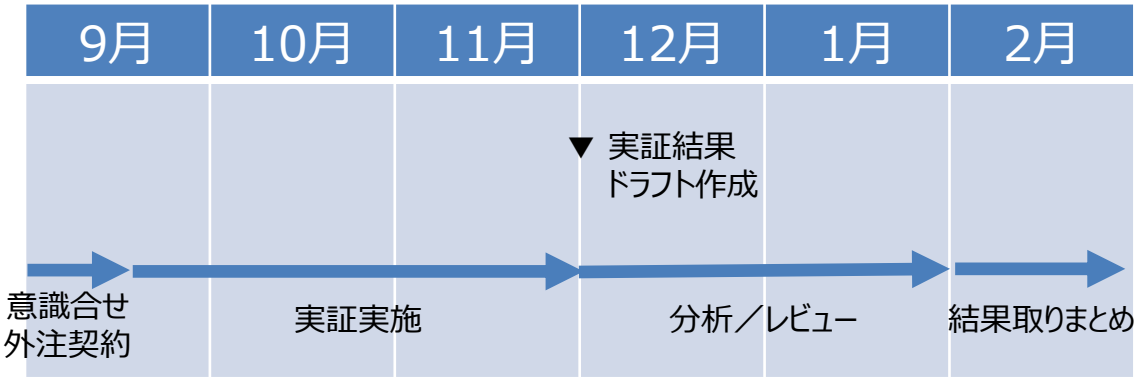
SBOM実証の対象ソフトウェア・体制・スケジュール

- 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**。

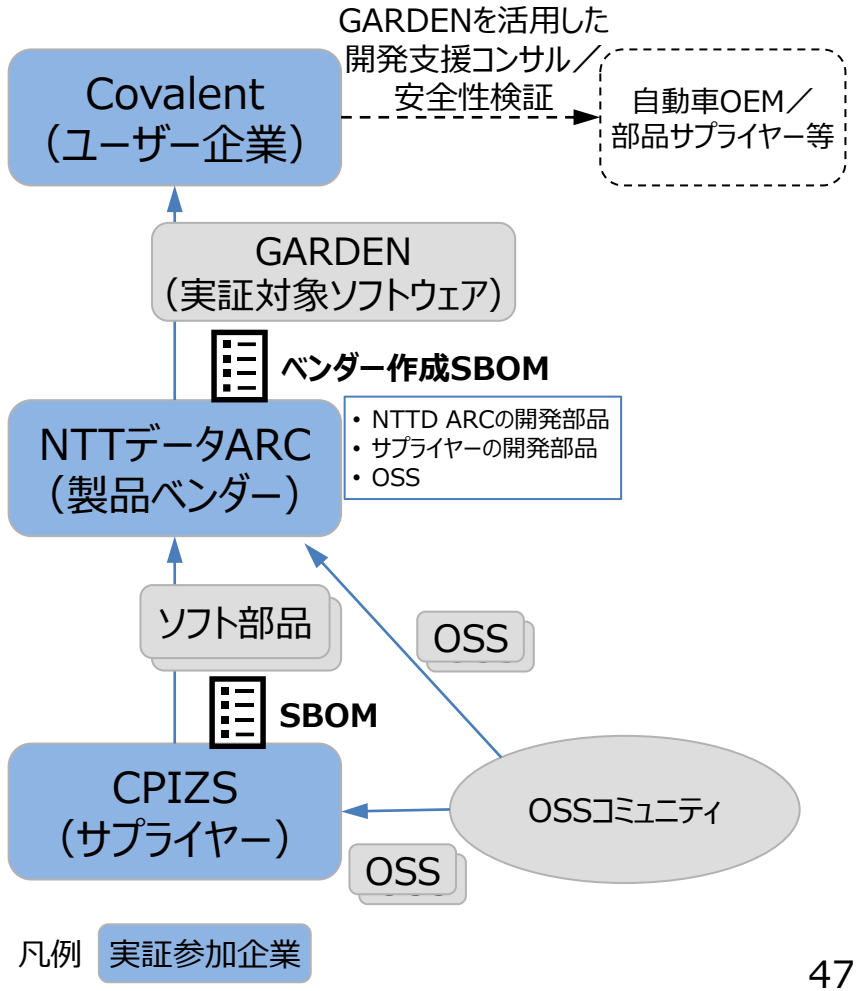
実証対象ソフトウェア 「GARDEN」

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）



SBOM実証のシナリオ、まとめ

- 実証では、従来の部品管理を含む4つのシナリオに関し、SBOM等の作成、活用に係る工数・費用を計測。
- 今回の比較条件では、SBOMは初期工数（ツール導入等の環境整備、学習等）が大きいが、運用工数（SBOM作成、活用）は従来の手作業部品管理に比べ小さい結果となり、**管理対象のソフトウェア部品が多いほど、SBOM導入効果が大きくなると想定**。
- ツールによる脆弱性特定の自動化により、**脆弱性発表から特定までのリードタイム短縮と工数削減**に繋がる。

実証のシナリオ

①従来の部品管理(独自形式)

Excelの独自形式で手作業管理。
脆弱性やライセンスの情報は手作業で検索。

②SBOM(手動作成)

ツールのフォーマットに合わせて手作業でSBOMを作成。
脆弱性やライセンスの特定はそれぞれOSSの無償ツールで実施。

③SBOM(無償ツール)

OSSの無償ツールによりSBOMを作成。
脆弱性やライセンスの特定はそれぞれOSSの無償ツールで実施。

④SBOM(有償ツール)

有償ツールにより、SBOM作成、脆弱性管理、ライセンス管理をシームレスに実施。

まとめ

SBOMのメリット等

- ツールにより**脆弱性が発表されてから、ソフトウェアの影響を特定するまでのリードタイムが短縮**。
- **SBOMは導入するための初期工数（ツール導入等の環境整備や使用方法習得のための学習等）が大きいが、ツールを活用することでSBOMの作成や脆弱性特定等の工数は小さく**なった。
- 特に有償ツールでは、**OSS部品の再利用も検出。**
  ※ただし、検知結果の精査工数は大きかった。

確認した課題

- SBOMの**作成主体や作成対象範囲、作成手段等によりコストや効果が異なる**。
- 開発者自身が標準的なSBOMフォーマットで部品情報を共有することが有効だが、**部品粒度等を揃える（要件化する）必要**。
- 特に**無償ツールはドキュメントやノウハウが不足**。機能・精度面も十分とはいえない。
- 開発者自身が認識していない部品が検出された場合など、契約等で関係が整理されていない場合に**関係者間の責任が曖昧になり得る**。
- ツールにより検出されるOSSの再利用やソースコード改変部品が見つかった場合には、これの精査に係る工数が大きくなる、もしくは精査が困難。

ソフトウェアTFの今後の取組

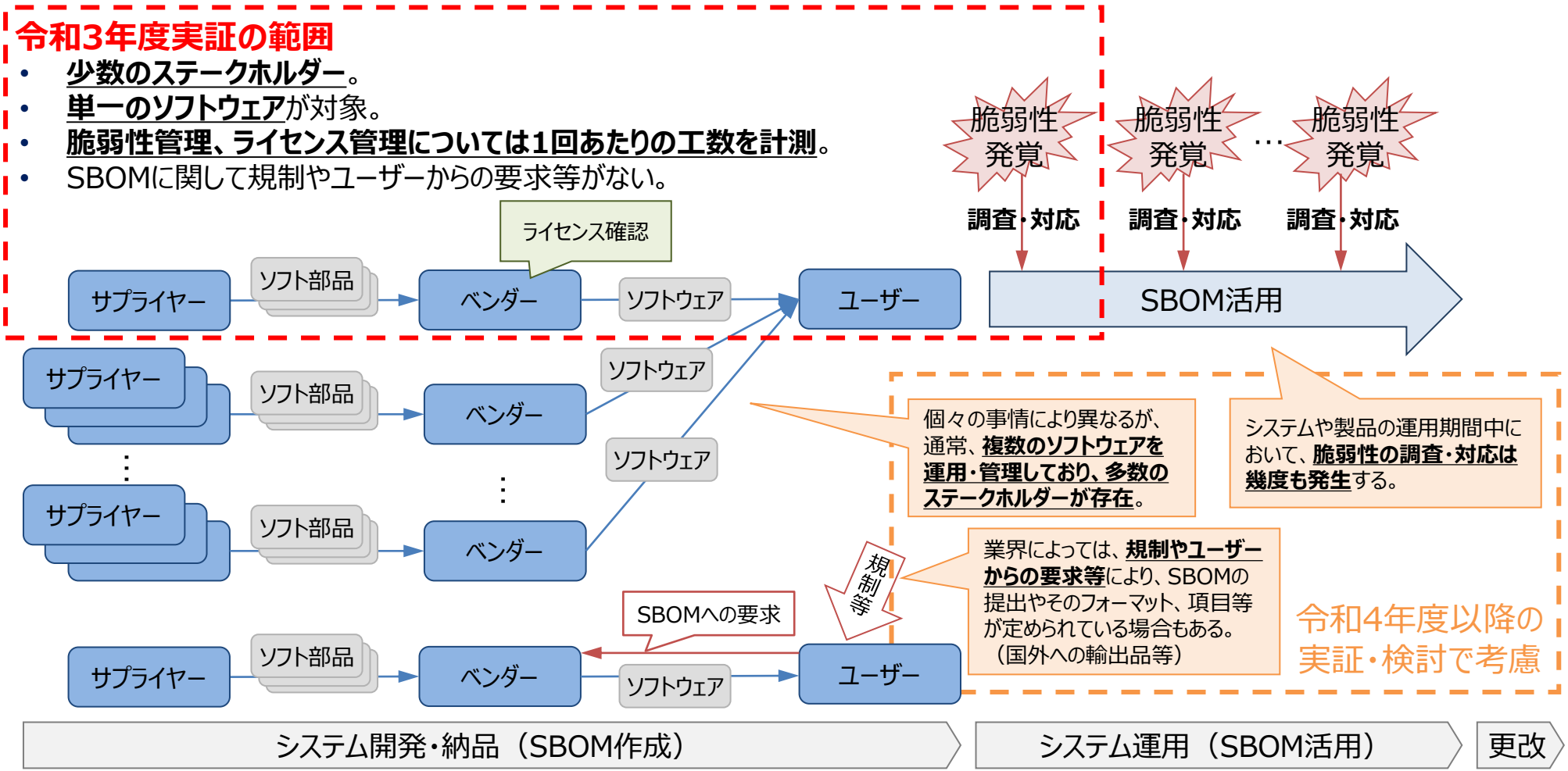
- 設定した課題から、令和4年度以降の取組を下記のように整理。

令和4年度以降の取組	実施時期	実施主体
①実証によるコスト・効果の評価と論点整理の継続 規制等が進む分野やSBOM導入効果が大きい分野等を候補に、複数分野で実証を行うとともに、コスト・効果の評価、個別の課題等に係る知見を共有。成果を他の取組においても活用。	R4年度	国・民間
②SBOMの効果的な活用モデルの検討 各産業分野における規制の内容やリスク等を踏まえた、効率的／効果的な活用モデル（分野ごとの標準的なSBOM作成主体、対象部品、手段、データ形式・項目等）、およびステークホルダーの合意形成の在り方について検討。	R4年度	国
③SBOM共有に関する取引モデルの検討 サプライチェーンの部品管理に関する責任、部品情報共有の要件化、費用負担等、取引契約における論点を整理。産業分野ごとの取引契約書モデル等を検討。	R4年度以降	国・民間
④SBOMに関するノウハウ共有 実証で得たSBOMツールのノウハウ、コスト情報等についてガイド／手引きを作成。 NTIAのプレイブック等との対応も意識し、調整が必要な事項を整理。	R4年度	国
⑤SBOM自動化・共有に向けた技術的な検討 SBOMツールの調査、SBOMに係る基準や国際標準等への対応、構成管理ツールとの統合、脆弱性DBにおけるソフトウェアの識別子の整備、SBOM信頼性確保等に向けた検討や研究開発。	R4年度以降	国・民間 （国はツールの研究開発に関する技術課題の整理等を実施）
⑥国外との制度調和 米国と意見交換や成果の共有ができる関係を維持。制度等、必要な調整を実施。	R4年度	国

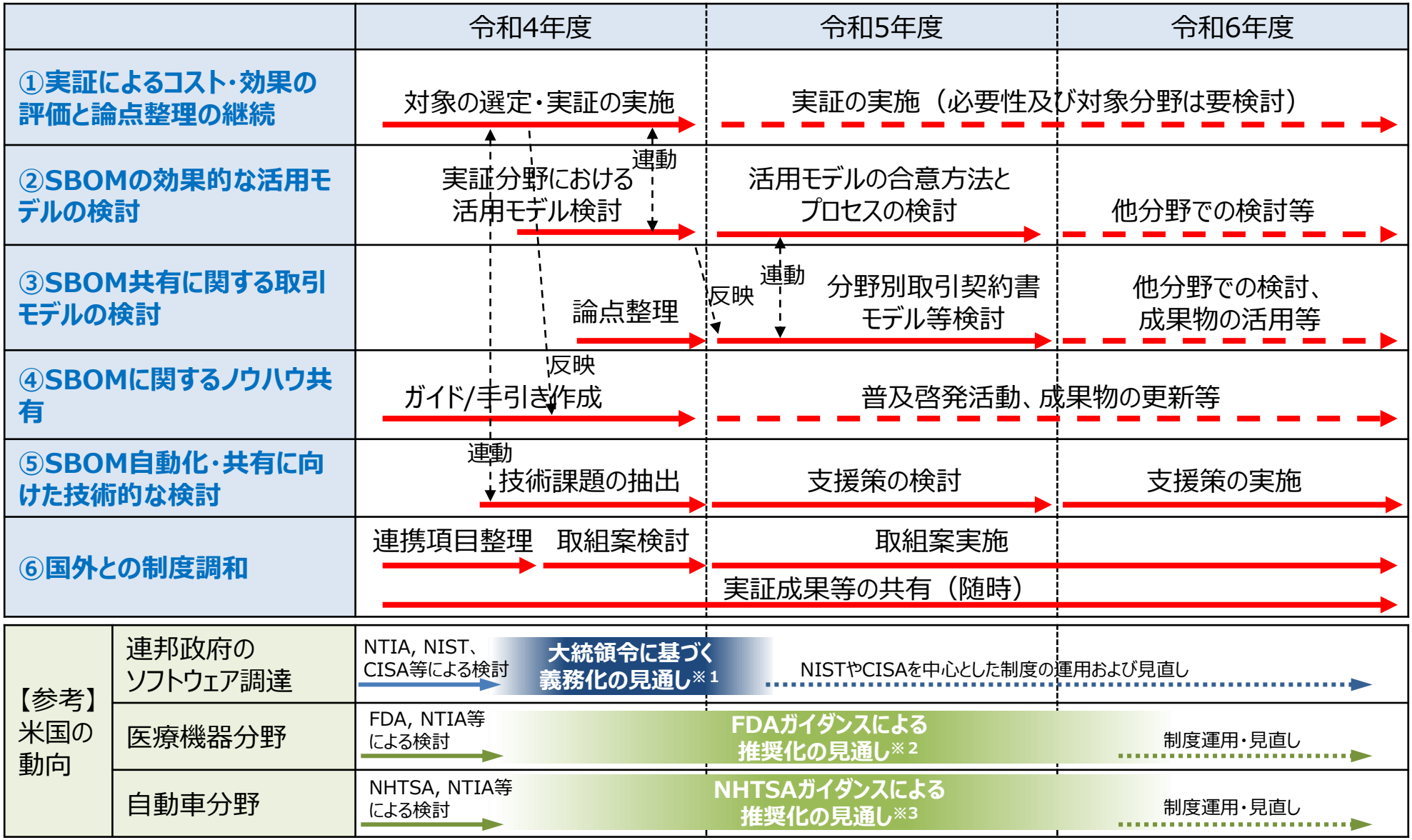
（参考）実証の範囲

- **SBOMの作成・活用に関しては様々なパターン**が考えられる。
- **初年度である令和3年度実証は、少数のステークホルダーが関係するソフトウェアを対象**にSBOMを作成して脆弱性およびライセンス管理へ活用するケースについて、効果とコストを比較。

令和3年度実証の範囲
- **少数のステークホルダー**。
- **単一のソフトウェア**が対象。
- **脆弱性管理、ライセンス管理については1回あたりの工数を計測**。
- SBOMに関して規制やユーザーからの要求等がない。



スケジュール（イメージ）



※1：Executive Order on Improving the Nation's Cybersecurity, MAY 12, 2021
※2：FDA, Draft Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Oct, 2018
※3：NHTSA, Draft Cybersecurity Best Practices for the Safety of Modern Vehicles, Jan, 2020

（参考）医療機器分野のサイバーセキュリティに関する規制・検討の状況

- **2020年3月、国際医療機器規制当局フォーラム（IMDRF）より**、医療機器のサイバーセキュリティ対策に関する**ガイダンスが発行**。
- **日本においても**、国際整合の観点から**導入に向けて検討中**。**2023年を目途に各種の基準等の改正**を予定。

IMDRFガイダンス※1の概要


IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

Copyright © 2020 by the International Medical Device Regulators Forum.

医療機器のサイバーセキュリティに関する国際整合を図るため、「一般原則」と「ベストプラクティス」を提供。

○一般原則

医療機器の全体的なサイバーセキュリティを向上させるために重要な一般原則として「国際整合」「製品ライフサイクル全体を通じたリスク検討／対策」「ステークホルダーの共同責任」「情報共有」の4つを提示。

○ベストプラクティス

・市販前（主に医療機器製造業者向け）
・市販後（全ステークホルダー向け）

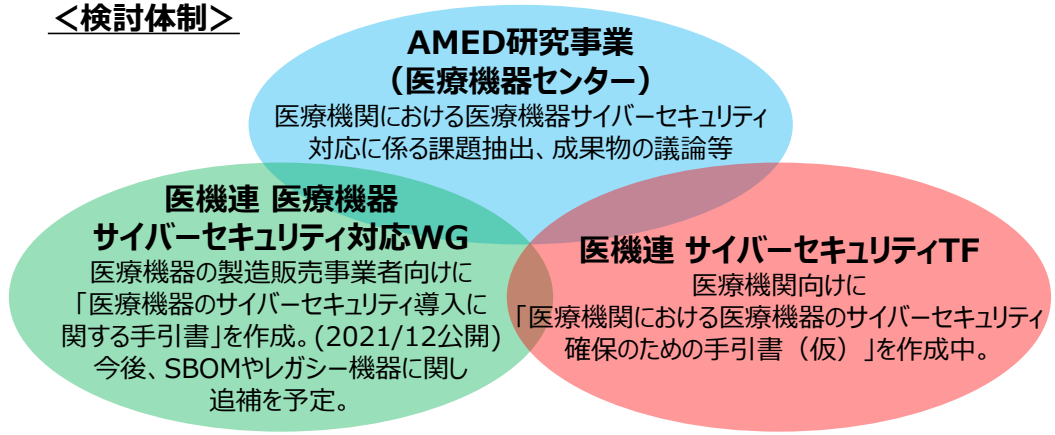
○SBOMに関する記載

- 【市販前】ソフトウェアの透明性確保や脆弱性対応等のため、**顧客へのSBOM提供を医療機器製造業者に対して推奨**。形式や構文等は業界の**ベストプラクティスの活用が望ましい**としている。
- 【市販後】**医療機関によるSBOMの要求**と、**インシデント対応や機器のライフサイクル管理での活用**について記載。

国内における規制と対応状況

- 日本においても、**国際整合の観点からIMDRFガイダンスを導入すべく**※2、日本医療研究開発機構（AMED）の研究事業※3および日本医療機器産業連合会（医機連）において、**医療機器のサイバーセキュリティに係る開発目標や技術要件を検討中**。
- **2021年12月「医療機器のサイバーセキュリティ導入に関する手引書」発行**。
- 今後、開発目標や評価基準が策定され、**2023年を目途に**「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第四十一条第三項の規定により厚生労働大臣が定める医療機器の基準」（平成17年厚生労働省告示第122号）等の**所要の改正が行われる予定**※4。

＜検討体制＞



※1 https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf
※2 https://www.mhlw.go.jp/hourei/doc/tsuchi/T200521I0040.pdf
※3 AMED 医薬品等規制調和・評価研究事業「医療機関における医療機器のサイバーセキュリティに係る課題抽出等に関する研究」
※4 https://www.mhlw.go.jp/hourei/doc/tsuchi/T211228I0070.pdf

直近のソフトウェアTFでの主なご意見

＜取組の方向性について＞

- 本取組はセキュリティ政策における重要な基盤であり、国際競争上も重要。**実現すべき具体的な目標を「旗」として立てていただきたい。**
- 開発生産性の向上や脆弱性に関する問合せ対応の短縮化のような**SBOMの正のメリットも共有して普及を進められるとよい。**

＜中小企業等への普及について＞

- 令和4年度以降の対象の選定にあたって、**中小のソフトウェアベンダーにも参加いただき、事例を作成できると良いのではないか。**
- 中小企業ではSBOMを手動で構築する労力を確保できず、自動で確認できるツール等が必要。ツール利用の施策を、ナレッジを共有し進められるとよい。

＜SBOMの活用について＞

- **どのような粒度でSBOMを作るべきかが重要。**OSSを作る側だけでなく、利用者側の義務も重要。
- Cyclone DXのプロジェクトにおいて提唱されているVEXの活用による脆弱性確認の自動化の方向性も検討する必要。
- 1月にホワイトハウスがOSSコミュニティや関連企業を集めてOSSを守るための会議を実施している。日本でも同様の取組を実施できるとよい。

＜人材育成について＞

- 官民だけでなく、アカデミーを利用し人材育成を含むエコシステムを構築できるとよい。
- SBOMに関わる者の意識は時間をかけて形成する必要があり、研究機関や高度教育機関の役割が重要。

＜政府機関等における取組について＞

- **サイバーセキュリティ政策に関する日米の政府間対話でも、本内容について意見交換できるとよい。**
- 影響力の大きいチャレンジは国で実施すべきではないか。

１．産業分野別SWG

２．第３層タスクフォース

３．ソフトウェアタスクフォース

４．第２層タスクフォース

５．CPSFの国際規格化

前回のWG1・分野横断SWG合同会議における主なご指摘

- （再掲）産業分野別に色々な枠組みを作っている一方で、分野間で共通の部材やIoTデバイスなどが結構出てきているので、全体を見たような対策も考えていただきたい。
- （再掲）各産業分野別SWGにおいて、それぞれ良い成果が出てきているので、第2層TFでのアウトプットの枠組みを使い、産業分野別に具体的な事例などを検討していくのが良いのではないか。サイバーセキュリティエンジニアリングについては、開発プロセス等のマクロな議論は進んでいるが、詳細なところは安全分野ほどできてきていない印象。そのようなところに第2層TFの結果などもうまく使っていけるかもしれない。

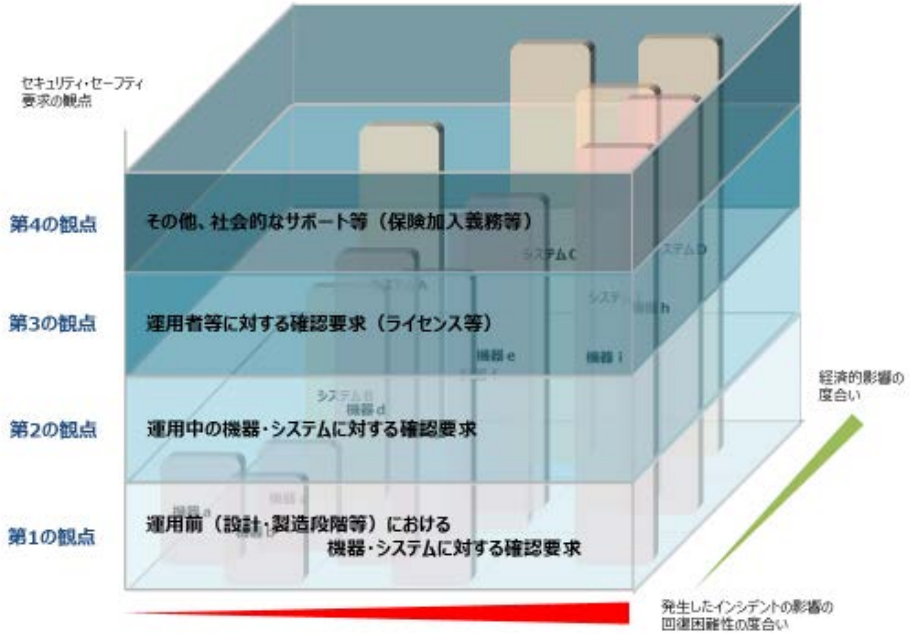
IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の枠組み

- 実現される仕組み・サービスの利用者側から見てインシデントが発生した場合の影響を適切に分析。
  - •第１軸：発生したインシデントの影響の回復困難性の度合い
  - •第２軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算）
- それぞれのカテゴリーに従って第３軸を活用してセキュリティ・セーフティ要求の観点・内容を適切に検討するための枠組み。
  - •第１の観点：運用前（設計・製造段階等）におけるフィジカル・サイバー空間をつなぐ機器・システムの確認要求
  - •第２の観点：運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求
  - •第３の観点：機器・システムの運用・管理を行う者の能力に関する確認要求
  - •第４の観点：その他、社会的なサポート等仕組みの要求

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



ユースケース集の作成（令和３年度）

- IoT-SSFは、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」であるが、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。
- IoT-SSFの普及、具体的な活用に向けては、IoT-SSFで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。

1. ユースケース集の位置付けと構成
   「IoTセキュリティ・セーフティ・フレームワーク」の概要ほか
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
   ・ユースケースにおける記載事項
   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（ステークホルダー別の対策例一覧）
   ・具体的なユースケース
   ① 家庭用ガス給湯器の遠隔操作
   ② ドローンを活用した個人による写真撮影
   ③ 物流倉庫内のAGVによる自動ピッキング
   ④ 化学プラント施設内の蒸留工程の自動制御
   ⑤ 工場内のロボットによる部材加工作業（溶接工程）の自動化
   ⑥ 金属製造現場の温度センサ等による製造設備の状態監視

添付A 対策要件

添付B 対策例

ユースケースの選定は以下の要素を勘案
- 利用者の区分（個人・家庭/事業者）
- 利用環境（家庭/公共空間/事業所）
- 想定する適用主体の特徴

- 添付Aと添付Bは、各ユースケース固有の事情に依存しない一般的に適用し得る内容
- 想定読者において具体的な対策を検討する際に適宜参照

（参考）IoT-SSFに基づくリスクマネジメントのプロセス

- 既存の国際標準（ISO 31000等）や本文書の上位の文書である「サイバー・フィジカル・セキュリティ対策フレームワーク」を踏まえて、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

- 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

2 リスクアセスメント

- 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

3 リスク対応（ステークホルダー別の対策要件一覧）

- 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

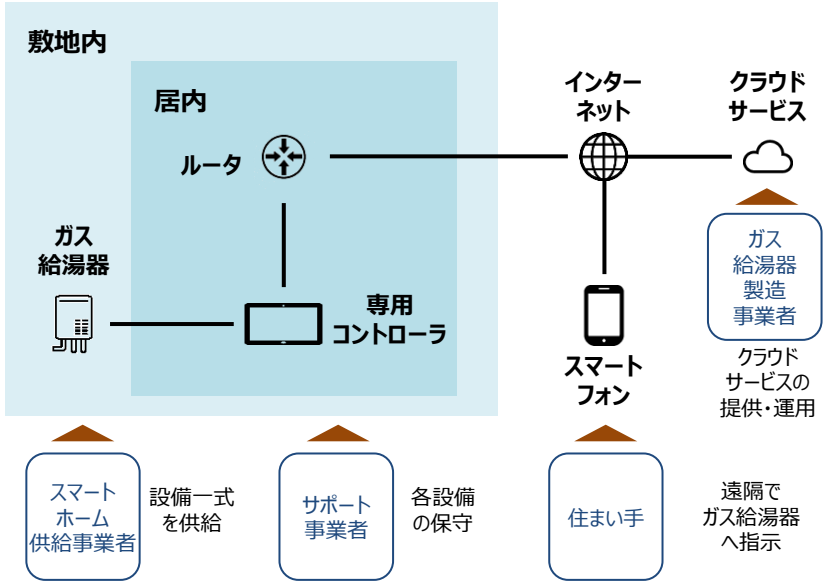
※IoT利用者、IoTサービス開発者、IoTサービス提供者においては、現場の担当者だけではなく経営層と一体となって全社的にリスクに対応することが望ましい。

（参考）ユースケース：家庭用ガス給湯器の遠隔操作

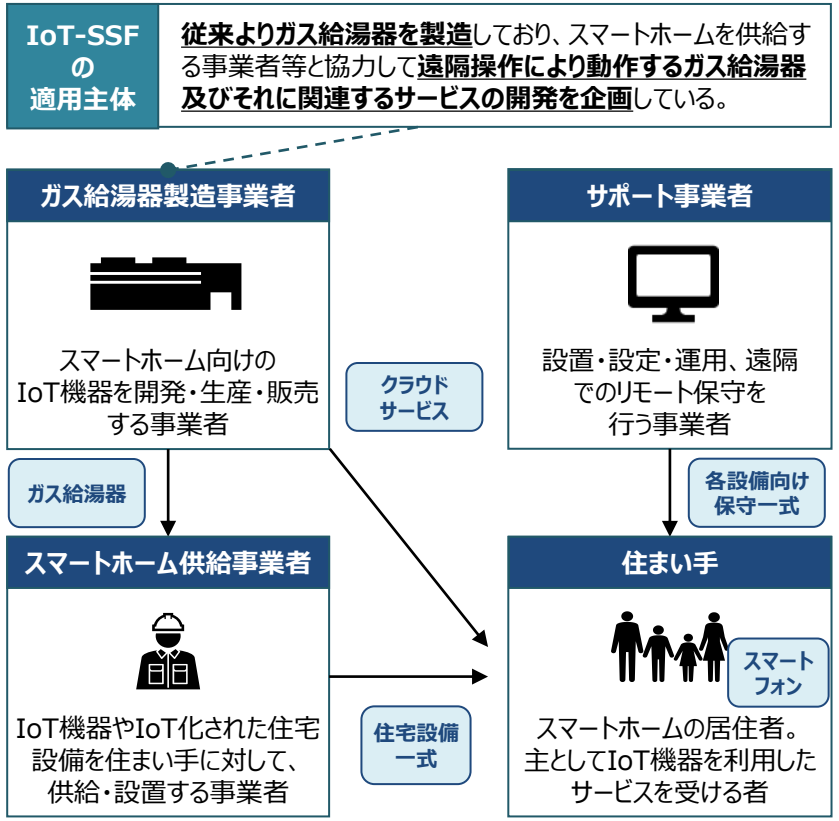
- スマートホーム向けIoT機器・サービスの事業者（ガス給湯器の製造元）がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- 住まい手が外出先よりスマートフォン用アプリを通じて、居内のガス給湯器を遠隔操作。

✓ 対象機器・システムの概要

- 住まい手が外出先よりスマートフォン用のアプリケーションを通じて、居内のガス給湯器を遠隔操作し、自動で浴槽のお湯張り等を実施するケースを想定する。
- 遠隔操作が許容される方式を用いた製品の利用を前提とする。



✓ 適用主体及び他のステークホルダーの情報



（参考）ユースケース：家庭用ガス給湯器の遠隔操作

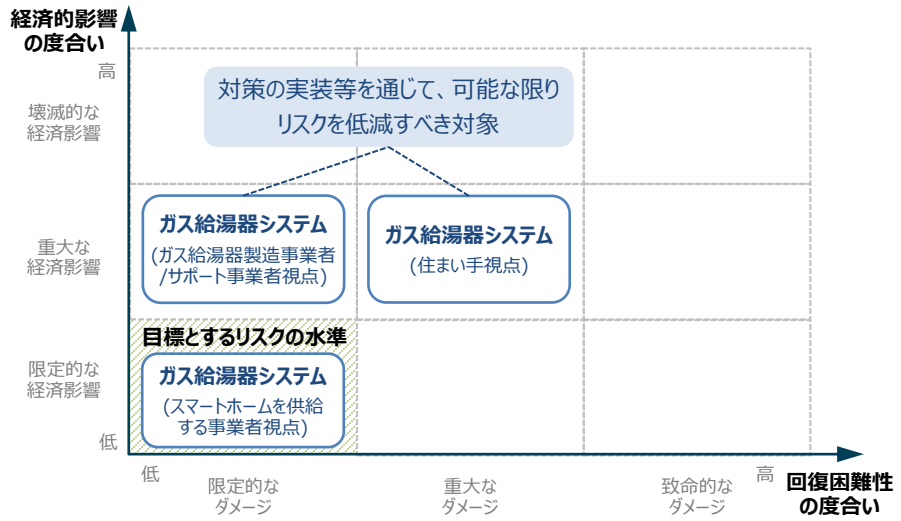
- 誤動作等により被り得るリスクが大きくなり得ると想定される「住まい手」は、一般にセキュリティに関する知見を十分に持たない場合が多いため、IoT-SSFの適用主体である「ガス給湯器製造事業者」は、これらを考慮してリスクの低減に努める必要がある。

✓ 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）
ガス給湯器製造事業者にとってのリスク	• クラウドサービスから送信される指示データ等が改ざんされ、**ガス給湯器が誤動作し得る。**その結果、**製品回収が発生し得る。**また、製品・サービスの品質について利用者の間に**疑念が広がる可能性**がある。
サポート事業者にとってのリスク	• 自社環境が不正アクセスされ、配信前のアップデートを改ざんされることで、**ガス給湯器が誤動作し得る。**その結果、**サポート事業者の責任で製品回収が発生し得る。**また、サポートの品質について利用者の間に**疑念が広がる可能性**がある。
住まい手にとってのリスク	• クラウドサービスに不正アクセスされることで、自身の**個人情報が流出**する可能性がある。 • 専用コントローラに対するアップデートを改ざんされ配信先のコントローラがマルウェアに感染する、クラウドサービスから送信される指示データがネットワーク上で改ざんされる等により、**給湯器が誤動作し得る。**その結果、住まい手がやけど等を負うことで、**生活に支障をきたし得る。**
スマートホームを供給する事業者にとってのリスク	• 想定される**リスクは限定的**と考えられる。

✓ 想定されるリスク(例)のマッピング結果

- スマートホームを供給する事業者視点からみたガス給湯器システムの保有するリスクは、目標とする水準内に収まっている。
- しかし、住まい手、ガス給湯器製造事業者及びサポート事業者視点のガス給湯器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。

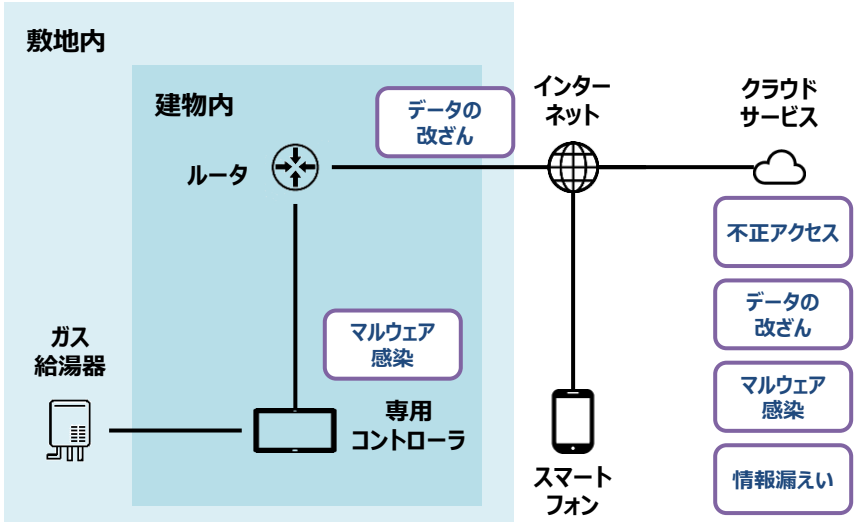


（参考）ユースケース：家庭用ガス給湯器の遠隔操作

- 影響度が大きいリスクにつながり得る脅威の例：クラウドサービスに対する不正アクセス、専用コントローラのマルウェア感染及び、それらによるガス給湯器の誤動作等。
- 行うべきと考えられる対策の例：企画・設計段階におけるセキュリティ要求事項の分析及び仕様化[第1の観点]、IoT機器・システムに対するアップデートの適用[第2の観点]等。

✓ 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、情報漏えい、マルウェア感染に加えて、クラウドサービスからの通信情報に対するデータの改ざん、専用コントローラのマルウェア感染及び、それらによるガス給湯器の誤動作が、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

ガス給湯器製造事業者(自身)にとってのリスクを低減するための対策(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、セキュリティ・バイ・デザインの取組みの推進

- **【第1の観点】運用前（設計・製造段階）における法令および契約上の要求事項の遵守**
- **【第1の観点】企画・設計段階におけるセキュリティ要求事項の分析及び仕様化**
- **【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**

サポート事業者にとってのリスクを低減するため対応を要請する対策(例)

ガス給湯器に対する安全なアップデート等の脆弱性対応の実施

- **【第2の観点】プログラムソースコード及び関連書類の保護**
- **【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**

住まい手にとってのリスクを低減するための対策(例)

自社製品・サービスの利用者をけがややけどから守るための対策の徹底

- **【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**
- **【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**

※セキュリティインシデントによっては、ガス給湯器製造事業者はガス供給事業者と連携して対応することが必要となる場合がある。

直近の第2層TFでの主なご意見

- **必要とする人たちが自ら作っていくということで、多くの事例が出てくるのかと思う。**その時に、フィードバックを集めることができると良いと思う。また、**同じ対象であっても違った分析結果が出てくると、なぜ、そのような違いが生まれたのかが分かって面白いのではないか。**
- 本ユースケース集では「起こりやすさ」を考慮せずリスクを定義しており、ISOの定義等とは異なっているため、ISO等の簡略版として位置づけて本ユースケース集を普及するとよい。
- 事業者側としては、過失、もしくは免責されるかどうかというところが裁判所で問題になってくるので、やれることをしたということを説明するための資料として、今回のフレームワークやユースケース集、特に、添付Ａや添付Ｂは非常に参考になると思う。
- 今回のようなまとめ方をしている文書は国際的に見てもほとんどない。最終的に、こういうガイドラインを日本が初めて作っているということが、将来的な課題の提起、提案につながれば良いと思う。
- **第3軸の第3の観点、第4の観点が重要であり、普及が進む中で拡充されていくことを期待する。**

１．産業分野別SWG

２．第３層タスクフォース

３．ソフトウェアタスクフォース

４．第２層タスクフォース

５．CPSFの国際規格化

Like-mindedの関係強化
～サイバー・フィジカル・セキュリティ対策フレームワークが盛り込まれた国際規格の策定

- ISO/IECの国内エキスパートの協力のもと、**CPSFのモデル等を盛り込んだ国際規格策定**を推進。
- **CPSFのモデルをサイバー・フィジカル・システム（CPS）をとらえるモデルの一つとして位置づけ**、SC 27/WG 4 に**Technical Specification（TS）として提案**。（タイトル：Security frameworks based on the conceptual model of cyber-physical systems）
- 当初、CPSF単独の内容でTRとして提案していたが、これまでの議論を通じて、CPSに関連する他の議論（IoT、Digital Twin等）との整合性を確保しながら進めることとなりTS策定を目指す方向に。

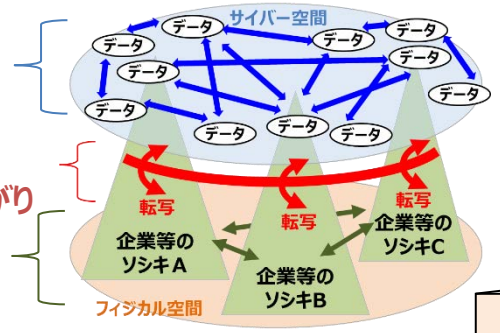
CPSFのモデル

＜3層構造＞

【第３層】
サイバー空間におけるつながり

【第２層】
フィジカル空間とサイバー空間のつながり

【第１層】
企業間のつながり



＜6つの構成要素＞

ソシキ	ヒト	モノ
データ	プロシージャ	システム

・「3層構造」
・「6つの構成要素」
というCPSFのモデル等を盛り込んだドラフトを提案

国際標準化団体へ提案

ISO / IEC
↓
JTC 1
↓
SC 27
↓
WG 4

2020.4～2021.10
1st ～ 5th PWI
(Preliminary work Item)

2021.11
NWIP
(New work item Proposal)

TS発行

※今後のスケジュールは経済産業省および対応中のエキスパートによる想定

（参考）EUCCのスキーム

- 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。**
- 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）標準化をめぐる環境変化（１）：対象分野の拡大

- 標準化の対象分野が、**モノから「サービス・マネジメント」、「社会システム」、「SDGs・環境」など、様々な分野へ大きく拡大。**

標準の伝統的な利用例 → 標準の対象分野の拡大

物の互換性 品質の確保

形や寸法が統一され
どこでも、誰でも利用できる

物の安心・安全の確保

発火防止

幼児対策ロック

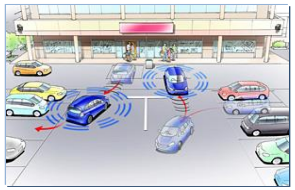
形や寸法の統一
強度等の要求により
安心・安全な利用を担保

サービス・マネジメント分野

ロボットサービス

小口保冷配送

社会システム分野



自動運転システム

サイバーセキュリティ

SDGs・環境分野

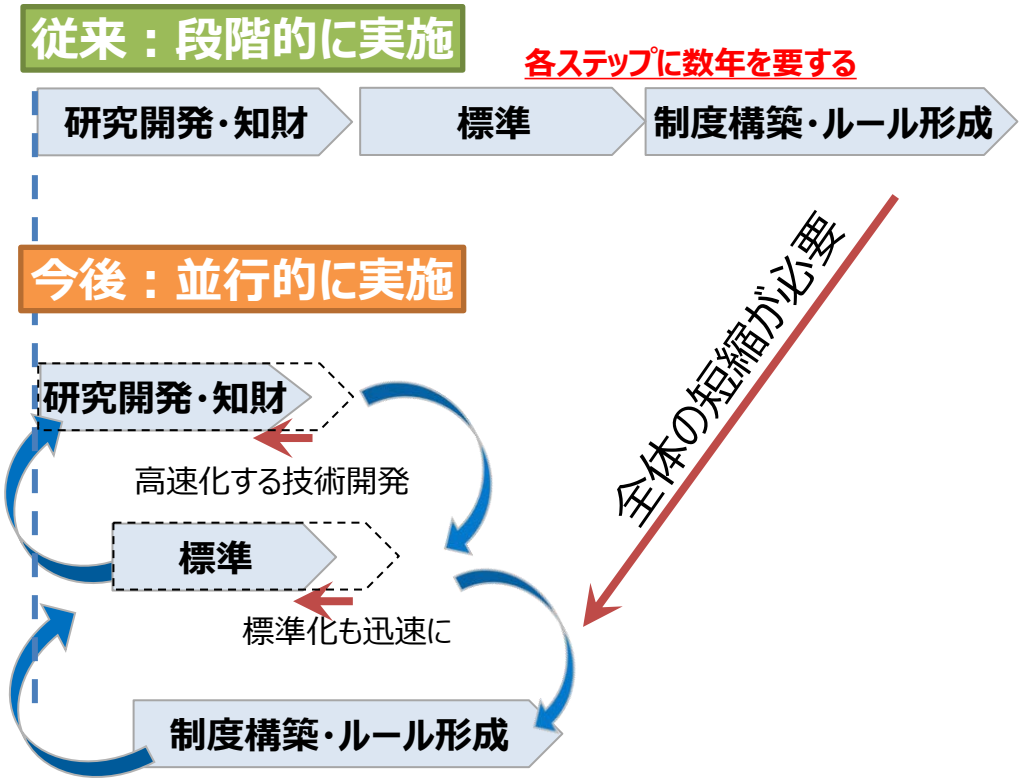
サステナブルな投資

循環社会

出所：経済産業省 新たな基準認証の在り方について（一部改）（写真はISO、EC、ヤマトホールディングスHP等より引用）

（参考）標準化をめぐる環境変化（２）：研究開発と標準化の同時進行

- 技術開発スピードが高まる中、新しい技術の普及を促す市場環境整備のツールとして、**研究開発の初期段階から制度構築や標準化の検討の重要性が増大**。



【事例】 生活支援ロボットの安全要求事項

～ NEDO「生活支援ロボット実用化プロジェクト」（2009~13）～

- 生活支援ロボットの研究開発、社会実装を進める上で、**安全の評価方法に関する基準がなく、**規制・制度に引用され得る安全性評価規格開発が必要と判断。
- 研究開発と並行して、安全関係データの収集、検証試験方法の確立、安全要求事項に関する国際標準提案等の**標準化活動を実施**。

→ 2014年、ISO 13482（生活支援ロボットの安全要求事項）制定。

Prof. Sankai, University of Tsukuba / CYBERDYNE Inc.

→ プロジェクト終了の翌年に国際標準化を実現

目次

今後の方向性

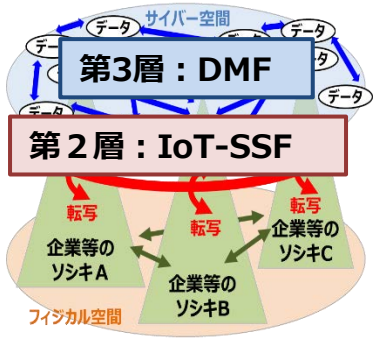
- これまでCPSF及びこれに連なる文書（IoT-SSF・ユースケース、データマネジメント・フレームワーク）や分野別ガイドラインの整備が進んできたところ。
- 今後は、セキュリティレベルの底上げに向けて政府と産業界の協業を進めつつ、国際的なルール形成の推進に向けた取組や、サプライチェーン全体のセキュリティ向上に向けた取組に取り組んでいく。

これまでの取組

- ✓ CPSFとこれに連なる文書（IoT-SSF・ユースケース、データマネジメント・フレームワーク）の整備
- ✓ OSS事例集の横展開
- ✓ SBOM実証の実施
- ✓ 分野別ガイドラインの整備

分野別ガイド

CPSF



ソフトウェア：
OSS事例集
SBOM実証

今後の取組

- セキュリティレベルの底上げに向けた政府と産業界の協業
- 分野横断と分野別の協業による産業界ごとのサプライチェーンセキュリティの向上
- 標準化も含めた国際的なルール形成の推進

分野別ガイド

第　３　層

- 行政分野（DFFT、スマートシティ、データEX等）において、フレームワークの適用・応用を推進
- 先進的な取組を行うユーザとの実証を検討

第　２　層

- IoT-SSF及びユースケースの普及啓発
- 自立的な活用の促進に向けた制度設計

ソフトウェア

- 実証によるコスト・効果の評価と論点整理の継続
- SBOMの実証と活用/取引モデル開発
- SBOMに関するノウハウ共有、自動化・共有に向けた技術的な検討
- 国外との制度調和

CPSF等文書の改訂スキームの構築（案）

- CPSFは、発行から３年が経過しようとしている（2019年4月18日発行）。サイバーセキュリティを取り巻く環境の変化は速く、諸外国も文書を続々整備していることから、CPSF等文書の陳腐化も進んでいくおそれ。
- 本来、こうした環境変化に基づく修正は即座に反映されることが望ましいものの、CPSF策定時のような、累次にわたって審議会やパブリックコメントを行い、それらの意見を取りまとめていくという方法では、変化のスピードについていけない可能性がある。
- そこで、以下に示すスキームを構築することで、環境変化に即応できるCPSF文書等の修正体制を構築すべきではないか。