経済産業省

経済産業省のサイバーセキュリティ政策について

商務情報政策局
サイバーセキュリティ課

１．諸外国の動向

２．サイバー・フィジカル・セキュリティ対策フレームワークとその具体化

２．１　IoTセキュリティ関連

２．２　ソフトウェアセキュリティ関連

２．３　OTセキュリティ関連

２．４　データセキュリティ関連

米国サイバー戦略　（令和5年3月3日）

- ２０２３年３月２日（現地時間）、米ホワイトハウスは、４年４ヶ月ぶりに「国家サイバー戦略」を公表。社会全体のデジタル技術への依存度の高まりや、中国、ロシア、イラン、北朝鮮及び非国家主体の悪意あるサイバー活動による、米国の安全保障や経済的への影響を踏まえ、以下の５つを柱として構成。
- これらの柱を実現するため、**①消費者や中小企業等の特定のプレイヤーに過度に依拠せず、重要システムの開発主体に取組を要請**、**②目先の脅威への対応にとらわれるのではなく、デジタルインフラの強靭化に向けた取組にインセンティブを付与する等により、長期的な防御能力を高めること**の２点を挙げている。

第一の柱　重要インフラの防護

１．１ 国家の安全保障や公共の安全を支えるサイバーセキュリティ要件の確立
１．２ 官民協力の拡大
１．３ 連邦政府のサイバーセキュリティーセンターの統合
１．４ 連邦政府のインシデント対応計画及びプロセスの改訂
１．５ 連邦政府防衛の現代化

第二の柱　脅威主体の阻止と解体（Disrupt and Dismantle）

２．１ 連邦政府による阻止活動の統合
２．２ 敵対者を阻止するための官民の運用協力の強化
２．３ インテリジェンス・シェアリング及び被害通知の加速と規模拡大
２．４ 米国内に存在するインフラの悪用阻止
２．５ サイバー犯罪への対抗、ランサムウェアの打倒

第三の柱　セキュリティ及び強靭性強化のための市場原理の形成

３．１ データ管理者の説明責任を果たさせる
３．２ 安全なIoTデバイス開発の推進
３．３ 安全性に問題のあるソフトウェア及びサービスに対する法的責任の転嫁
３．４ 安全を確保した設計に対する連邦政府の補助金及びその他のインセンティブの活用
３．５ 説明責任を向上させるための連邦政府調達の活用
３．６ 連邦政府によるサイバー保険安全措置の検討

第四の柱　強靭な未来（Resilient Future）への投資

４．１ インターネットの技術的基礎の安全確保
４．２ サイバーセキュリティーのための連邦政府の研究開発の再活性化
４．３ ポスト量子に対する備え
４．４ クリーンエネルギーの将来性の確保
４．５ デジタル・アイデンティティー・エコシステムの発展の支援
４．６ サイバー人材強化のための国家戦略の策定

第五の柱　共通の目標を追求する国際パートナーシップの形成

５．１ デジタル・エコシステムに対する脅威に対処するコアリションの形成
５．２ 国際的なパートナーの能力の強化
５．３ 同盟国及び同志国を支援する米国の能力の拡大
５．４ 国家の責任ある行動についてのグローバルな規範の強化のためのコアリションの形成
５．５ 情報、通信並びにオペレーショナルテクノロジー製品及びサービスのグローバルサプライチェーンの安全確保

米国サイバー戦略　（令和5年3月3日）

- ２０２３年３月２日（現地時間）、米ホワイトハウスは、４年４ヶ月ぶりに「国家サイバー戦略」を公表。社会全体のデジタル技術への依存度の高まりや、中国、ロシア、イラン、北朝鮮及び非国家主体の悪意あるサイバー活動による、米国の安全保障や経済的への影響を踏まえ、以下の５つを柱として構成。
- これらの柱を実現するため、**①消費者や中小企業等の特定のプレイヤーに過度に依拠せず、重要システムの開発主体に取組を要請**、**②目先の脅威への対応にとらわれるのではなく、デジタルインフラの強靭化に向けた取組にインセンティブを付与する等により、長期的な防御能力を高めること**の２点を挙げている。

第一の柱　重要インフラの防護

1．1 国家の安全保障や公共の安全を支えるサイバーセキュリティ要件の確立
1．2 官民協力の拡大
1．3 連邦政府のサイバーセキュリティーセンターの統合
1．4 連邦政府のインシデント対応計画及びプロセスの改訂
1．5 連邦政府防衛の現代化

第二の柱　脅威主体の阻止と解体（Disrupt and Dismantle）

2．1 連邦政府
2．2 敵対者を
2．3 インテリジ
…阻止
…ウェアの打倒

政権はIoTセキュリティ・ラベリング・プログラムの開発を引き続き推進する予定である。IoTセキュリティラベルの拡大を通じて、消費者はさまざまなIoT製品が提供するサイバーセキュリティ保護を比較できるようになり、IoTエコシステム全体でセキュリティを強化するための市場インセンティブが生まれる。

第三の柱　セ…

3．1 データ管理者の説明責任を果たさせる
3．2 安全なIoTデバイス開発の推進
3．3 安全性に問題のあるソフトウェア及びサービスに対する法的責任の転嫁
3．4 安全を確保した設計に対する連邦政府の補助金及びその他のインセンティブの活用
3．5 説明責任を向上させるための連邦政府調達の活用
3．6 連邦政府によるサイバー保険安全措置の検討

第四の柱　強靭な未来（Resili…re）への投資

4．1 インターネットの技術
4．2 サイバーセキュリティー
4．3 ポスト量子に対する
…展の支援
…定

- **ソフトウェアを保護するための合理的な予防措置を講じなかった事業者に責任を負わせる**ことを開始しなければならない。
- 政権は、議会や民間部門と協力して、**ソフトウェア製品とサービスの責任を確立する法律を策定する**。

第五の柱　共通の目…

5．1 デジタル・エコシステムに対する脅威に対処するコアリションの形成
5．2 国際的なパートナーの能力の強化
5．3 同盟国及び同志国を支援する米国の能力の拡大
5．4 国家の責任ある行動についてのグローバルな規範の強化のためのコアリションの形成
5．5 情報、通信並びにオペレーショナルテクノロジー製品及びサービスのグローバルサプライチェーンの安全確保

【米国】U.S. Cyber Trust Mark（検討中）

- **FCC（米連邦通信委員会）**が2023年8月にNPRM（立法案公告）を公表した、**任意のラベリング制度**。米時間9月25日までパブコメを実施。
- **想定対象は「消費者用IoT機器」**（詳細は下記）。ラベリングを得た機器とその機器に関する情報を全国登録簿に掲載し、ラベルに付随するQRコードを通じて全国登録簿が参照できるような仕組みを想定。
- 今まで**NIST(米国立標準技術研究所）が公表してきた基準に基づく見込み**。なお、**消費者向けルーター**（consumer grade router）**については、NISTが特別にそのセキュリティ要件を定義する**予定。
- **2024後半の運用開始を目指す。**

米FCC　NPRM（立法案公告）の主な内容

【対象について】

以下２つを満たすものを提案。

(1) 物理的世界と直接相互作用するための、1つ以上のトランスデューサー（センサーまたはアクチュエーター）を備え、意図的にラジオ周波数を放出することができる（※intentional radiatorに限定）インターネット接続デバイス

(2) デジタル世界と相互作用するための、1つ以上のネットワークインターフェース（Wi-Fi、Bluetoothなど）

※ただし、FCCのCovered listや、米商務省のEntity List、米国防総省のList of Chinese Military Companiesの機器、またはその企業が生産する機器は対象外とする。

- 対象をIoT「機器」とするべきか、NIST定義に基づくIoT「製品」とするべきか（IoT機器＋バックエンド、ゲートウエイ等必要な追加部品）
- 「消費者」IoTに限定するべきか、「商業用」目的のものも含むべきか、対象は「使用方法」で判断するべきか。

【スキーム・体制について】

第三者機関としてCyber LABs（Cybersecurity Labeling Authorization Bodies）を設置することを提案。

【基準策定について】

- NIST基準をどのように活用できるか。その他考慮するべき基準はあるか。
- よりリスクが高いIoT機器・機器の分類には、別途基準を策定するべきか。

U.S. CYBER TRUST MARK

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

【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

【米国】各省庁における「重要なソフトウェア」の対策実装に向けた覚書

- 2021年8月、OMBは、各省庁に対し、**各省庁が利用・調達している「重要なソフトウェア」を60日以内に特定**し、**当該ソフトウェアに対して必要なセキュリティ対策を1年以内に実装することを指示**した覚書に署名した。
- 各省庁のセキュリティ対策にあたって、**NISTが7月9日に公開したガイダンスに遵守すること**を求めた。
- また、NISTやCISAに対して、**「重要なソフトウェア」に含まれるソフトウェアカテゴリの定義**や、**当該ソフトウェアのセキュリティ対策に係るガイドラインを必要に応じて更新することを要求**した。

「重要なソフトウェア」のセキュリティ対策実装に向けた要件一覧

要求先	要件	期限
各省庁	使用中または調達中のすべての「重要なソフトウェア」を特定する。	本覚書発行後、60日以内
	■初期フェーズ セキュリティ上重要な機能を備えている、もしくは攻撃された場合に重大な危害の可能性があるスタンドアロンやオンプレミスの「重要なソフトウェア」を対象に、NISTのガイダンスに記載されたセキュリティ対策※を実装する。	本覚書発行後、1年以内
	■後続フェーズ 今後、NISTが「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を更新した場合に、「重要なソフトウェア」に対して当該ガイダンスに記載された対策を実装する。	NISTによるガイダンスの更新後、1年以内
	今後、CISAが「重要なソフトウェア」に新たなソフトウェアカテゴリを追加した場合に、NISTのガイダンスに記載されたセキュリティ対策を実装する。 【新たに対象となるソフトウェアの候補】 データへのアクセスを制御するソフトウェア、ソフトウェア開発ツール、OTのソフトウェアコンポーネント　等	CISAによる「重要なソフトウェア」の定義更新後、1年以内
NIST	「重要なソフトウェア」の定義と、当該ソフトウェアのセキュリティ対策に係るガイダンスを更新する。	必要に応じて
CISA	「重要なソフトウェア」の定義に含まれるソフトウェアカテゴリのリストを更新する。	必要に応じて

※ NISTが2021年7月9日に公開した、「重要なソフトウェア」のセキュリティ対策を示すガイダンスに記載されたセキュリティ対策を意味する。
なお、本覚書で要求されているとおり、当該ガイダンスの内容は今後更新される可能性があることに留意。

出所）OMB, “Protecting Critical Software Through Enhanced Security Measures”
https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf

【米国】セキュアなソフトウェアを開発するためのフレームワーク（SSDF）

- 2022年2月、NISTは、**ソフトウェアの脆弱性を軽減するためのソフトウェア開発者向けの手法**をまとめたフレームワークであるSSDF（Secure Software Development Framework）のVer. 1.1を公開。
- **各手法は4つに分類**され、**手法を実践するためのタスクが体系化**。各手法の実践により、**脆弱性を低減する**とともに、**未対処の脆弱性が悪用された場合の影響を軽減**し、**脆弱性の再発を防ぐ根本原因に対処可能**。
- また、大統領令の記載事項とSSDFの手法との対応関係を整理。**大統領令の記載事項に対処するために、SSDFを活用可能**であるとしている。

セキュアなソフトウェアを開発するための手法をまとめたフレームワーク（SSDF）

分類	手法
1. 組織の準備（PO） ソフトウェアを開発する組織は、組織レベルで安全なソフトウェアの開発を行うために、適した人材、プロセス、技術を準備する必要がある。	• ソフトウェア開発におけるセキュリティ要件を定義する（PO.1） • ソフトウェア開発における役割と責任を明確化する（PO.2） • ソフトウェア開発を支援するツールチェーンを明確化する（PO.3） • ソフトウェアのセキュリティを確認するための基準を定義し、活用する（PO.4） • ソフトウェア開発のための安全な環境を導入し、維持する（PO.5）
2. ソフトウェアの保護（PS） ソフトウェアを開発する組織は、ソフトウェアのすべてのコンポーネントを、改ざんや不正アクセスから保護する必要がある。	• あらゆる形態のコードを不正アクセスや改ざんから保護する（PS.1） • ソフトウェアリリースの完全性を検証する仕組みを提供する（PS.2） • 各ソフトウェアのリリースをアーカイブ化し、保護する（PS.3）
3. 安全なソフトウェアの開発（PW） ソフトウェアを開発する組織は、脆弱性を最小限に抑え、十分なソフトウェアを備えたソフトウェアをリリースする必要がある。	• セキュリティ要件を満足するとともにセキュリティリスクを軽減できるよう、ソフトウェアを設計する（PW.1） • ソフトウェア設計をレビューし、セキュリティ要件やリスクへの適合性を検証する（PW.2） • 実現可能な場合、機能を重複させずに既存の保護されたソフトウェアを再利用する（PW.4） • セキュアコーディングのプラクティスを遵守してソースコードを作成する（PW.5） • 実行可能なセキュリティを向上させるために、コンパイル、インタプリター及びビルドプロセスを構築する（PW.6） • コードをレビュー・分析することで、脆弱性を特定し、セキュリティ要求事項への準拠を検証する（PW.7） • 実行コードをテストして脆弱性を特定し、セキュリティ要求事項への準拠を検証する（PW.8） • ソフトウェアをデフォルトで安全な設定とする（PW.9）
4. 脆弱性への対応（RV） ソフトウェアを開発する組織は、リリースするソフトウェアに残存する脆弱性を特定し、適切に対応する必要がある。	• 脆弱性に対する継続的な把握と確認を実施する（RV.1） • 脆弱性の評価、優先順位付け及び修正を実施する（RV.2） • 脆弱性を分析することで、その根本原因を特定する（RV.3）

※ PW.3はPW.4の手法に統合されたため、定義されていないことに留意。また、PS.3のタスクの一つとして、SBOM等を用いたコンポーネントリストの生成・維持・共有に関するタスクが含まれている。

出所）NIST, SP 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

【米国】ソフトウェアサプライチェーンの確保に関する覚書の発行

- 2022年9月14日、OMBは、**安全なソフトウェア開発手法の実装を通じたソフトウェアサプライチェーンの確保に関する覚書を発行**した。
- 各省庁等の機関に対して、本覚書発行後一定期間内に、**機関が使用するソフトウェアの目録作成**や、**NISTのガイダンスに基づく自己適合証明書をソフトウェアベンダーに要求すること**などが求められている。
- なお、**SBOMに関しては、適合証明のために必要に応じてソフトウェアベンダーからSBOMを入手することができるとして推奨の位置付け**としている。

覚書の概要

政府関係機関は、**安全なソフトウェア開発手法（SSDF）の実装を証明できるソフトウェアベンダー**が提供するソフトウェアのみを使用すべきである。そのために、各機関の最高情報責任者（CIO）は、OMB及び最高調達責任者（CAO）と連携し、ソフトウェアベンダーによるSSDFの実装、実装の適合性を確保しなければならない。このために、機関は以下を実施する必要がある。

1. **機関は、ソフトウェア使用前に、SSDFの実装の適合性を証明する自己適合証明書の取得をソフトウェアベンダーへ要求する。**
2. **機関は、必要に応じて、自己適合証明書に付随する成果物（SBOM等）をソフトウェアベンダーから入手することができる。**

■ 対象ソフトウェア：
ファームウェア、OS、アプリケーション、アプリケーションサービス（クラウドベースのソフトウェア）、ソフトウェアに使用されるOSS、ソフトウェアを使用する製品
※ 機関によって開発されたソフトウェアや直接的に入手したOSSは対象外

■ 要件の適用範囲：
覚書発行日以降に開発されたソフトウェア（既存ソフトウェアのメジャーバージョンアップ含む）を機関が使用する場合に適用される。

出所）OMB, ” Enhancing the Security of the Software Supply Chain through Secure Software Development Practices”
https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

【米国】ソフトウェアサプライチェーンの確保に関する覚書の更新

- 2023年6月、OMBは、**安全なソフトウェア開発手法の実装を通じたソフトウェアサプライチェーンの確保に関する覚書（M-22-18）の内容を更新する新たな覚書（M-23-16）を発行**した。
- 本覚書では、**機関がソフトウェアベンダーからSSDFに準拠していることを示す自己適合証明書の取得期限の延長**のほか、**M-22-18の要求事項の明確化や補足的なガイダンスについて示されている。**

本覚書の記載概要

自己適合証明書の取得期限の延長	M-22-18によって連邦政府機関が求められているソフトウェアベンダーからの自己適合証明書の取得期限に関して、以下のとおり延長する。 • **「重要なソフトウェア」の自己適合証明書：** 当初予定：M-22-18発行後270日以内である2023年6月11日まで 延長後：CISAが発表した自己適合証明書フォームの承認後3ヶ月以内 • **すべてのソフトウェアの自己適合証明書** 当初予定：M-22-18発行後1年以内である2023年9月14日まで 延長後：CISAが発表した自己適合証明書フォームが承認後1年以内
M-22-18の要求事項の明確化	• **サードパーティコンポーネントに対する自己適合証明書の取得について** 自己適合証明書は、機関が使用するソフトウェアの最終ベンダーから取得されなければならない。そのため、機関は、使用するソフトウェアに組み込まれるサードパーティコンポーネントのベンダーから自己適合証明書を取得する必要はない。 • **無償で入手可能なプロプライエタリソフトウェアと一般に公開されているソフトウェアに対する自己適合証明書の取得について** 一般に無償で入手可能なプロプライエタリソフトウェアは自己適合証明書の取得の対象外とする。また、一般に公開されているWebブラウザ等のソフトウェアについても、自己適合証明書取得の対象外とする。ただし、機関は、このようなソフトウェアのリスクを評価し、適切な対処を講じなければならない。 なお、自由に入手可能な場合でも、無償で入手できないソフトウェアのデモやパイロット版は自己適合証明書の取得の対象となる。 • **連邦政府の請負業者によって開発されたソフトウェアに対する自己適合証明書の取得について** 連邦契約の下で開発されたソフトウェアが、M-22-18において対象外としている「機関によって開発されたソフトウェア」に該当するかは、機関がソフトウェア開発ライフサイクルを一貫して、安全なソフトウェア開発手法を実践することを実行できるかによる。
ソフトウェアベンダーが自己適合証明できない場合における補足的なガイダンス	ソフトウェアベンダーが自己適合証明書フォームに記載された事項の実施を証明できない場合であっても、証明できない事項を特定し、リスクを軽減するための実施事項を文書化し、自己適合証明書フォームの提出までの行動計画・マイルストーン（POA&M）を提出することで、機関はそのソフトウェアの使用が許可されている。本内容に関して、以下のとおり補足的なガイダンスを示す。 • 機関は、自己適合証明の期限延長をOMBへ申請しなければならない。 • リスクを軽減するための実施事項をまとめた文書が不十分またはPOA&Mが未提出の場合は、機関はソフトウェアの使用を中止しなければならない。また、機関が自己適合証明の期限延長を申請しない場合は、提出されたPOA&Mは有効とならず、機関はソフトウェアの使用を中止しなければならない。 • 自己適合証明できず、複数機関が影響を受ける場合、OMBは主導機関を指定し、主導機関に対して自己適合証明に関する調整・管理を要求する。 また、本覚書発行後1年以内に、OMBは、各機関のPOA&Mの承認、自己適合証明の期限延長（免除含む）に関する状況把握を開始する。

出所）OMB, "Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices"
https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf

EUにおけるIoT機器のセキュリティ政策の動向

- 欧州では、IoT機器を含む製品の認証スキームが検討されているほか、無線機器に対するセキュリティ対策が2024年8月から義務化される予定。

- 欧州全体のIoT機器の安全性確保に向けた近年の代表的な取組として、2019年に「EUサイバーセキュリティ法」が施行。欧州でのIoT機器を含む製品の認証スキームであるEUCC（Common Criteria based European Candidate Cybersecurity Certification Scheme）が検討。
- 無線機器に関する「EU無線機器指令（RED）（2014/53/EU）」にセキュリティに関する要件が追加され、2024年8月から欧州で販売する無線機器に対するセキュリティ対策が義務化される。
- 加えて、2022年9月にEU市場に投入されるデジタル製品のセキュリティ対応を義務付ける「EUサイバーレジリエンス法」の草案を発表。2025年後半の施行を予定しており、対象製品の上市にあたってはセキュリティ要件への適合性証明（自己適合宣言もしくは第三者認証）が求められる。

EU無線機器指令（RED）（2014/53/EU）（2022年2月発行、2024年8月より義務化予定）

- 2022年1月12日、欧州委員会は、Radio Equipment Directive（欧州無線機器指令）のサイバーセキュリティ関連条項の施行に関する委任規則（EU）2022/30が発行し、EU市場に投入される無線機器に対してセキュリティの強化を求めた。
- 具体的な規則は2024年8月1日より義務化。
- 対象機器について、直接・間接問わずインターネットに接続される無線機器が対象となる。

EUサイバーレジリエンス法（草案）

- 2022年9月に草案提出。2023年後半の発効、**2025年後半の適用**を目指す。
- 例外を除き、**デジタル要素を備えた全ての製品が対象。SBOM作成や更新プログラム提供等セキュリティ要件への適合（自己適合宣言/第三者認証）が求められる。**
- **重要なデジタル製品について、低リスク製品でEUCCやEN規格対象外の製品は第三者認証を、高リスク製品には第三者認証を求める。**（中小企業の認証手続き減額）
- 適合性評価証明書にはEU適合宣言書（CEマーク）/EUCC証明書を用いる。
- **脆弱性の悪用やインシデント発見後24時間以内にENISAへの報告を義務化。**
- **罰則あり。**（最高1,500万ユーロ又は当該企業の全世界売上高の2.5%以内）

注：EUCCとは、IoT製品を対象とする欧州サイバーセキュリティ認証。
EN規格とは、欧州整合化規格

【対象】デジタル要素を備えた全ての製品

・**デバイスやネットワークに直接的/間接的に接続されるものも含む。**
・医療機器規則、体外診断用医療機器規則、民間航空機規則、自動車の型式承認規則の対象製品は適用除外。
・国家安全保障に関するデジタル製品や軍事目的・機密情報処理目的のものは除外。
・SaaSなどのソフトウェアサービスは対象外。研究開発目的のOSSなども対象外。

【適合性評価】使用環境等のリスクレベル毎に以下を求める。

- **「デジタル製品」　・・・　自己適合宣言か第三者認証を選択**
- **「重要なデジタル製品」のうちクラスI（低リスク）・・・EUCCやEN規格の対象外は第三者認証**
- **「重要なデジタル製品」のうちクラスII（高リスク）・・・第三者認証**

【適合性評価証明書】

・**EU適合宣言書（CEマーク）に基づく証明書**
・**EUCCに基づく証明書**（必要に応じてEUCCを必要とする製品を指定）
※この他、**市場サーベイランスも行われる。**
※第三国（日本も含む）との相互承認も可能。※条文上は見当たらず。

CEマーク

重要なデジタル製品　以下の各クラスに規定された要素を主に有するデジタル製品

クラスI(低リスク)第三者認証(EUCC,EN規格以外)

1. ID管理システム、アクセス管理ソフト
2. スタンドアロン型/組込み型ブラウザ
3. パスワードマネジャー
4. マルウェア検知・削除・隔離ソフトウエア
5. VPN機能を持つ製品
6. ネットワーク管理システム
7. ネットワーク・コンフィグレーション管理ツール
8. ネットワーク・モニタリングシステム
9. ネットワーク・リソース管理
10. SEIM（セキュリティ情報イベント管理）
11. ブートマネジャーを含む更新・パッチ管理
12. アプリケーション構成管理システム
13. リモートアクセス/共有ソフトウェア
14. モバイル機器管理ソフトウェア
15. 物理ネットワークインターフェイス
16. OS（クラスII製品以外）
17. ファイアウォール、侵入検知・防止システム（産業用以外）
18. ルータ、モデム、スイッチ（産業用以外）
19. マイクロプロセッサ（クラスII製品以外）
20. マイクロコントローラ
21. NIS 2 指令の別添Iに示される目的でのASIC、FPGA
22. PLC、DCS、CNC、SCADAなどの産業用自動化制御システム（IACS）（クラスII製品以外）
23. 産業用IoT（クラスII製品以外）

クラスII(高リスク) 第三者認証

1. OSであってサーバ、デスクトップ、モバイル機器用のもの
2. OSや同様の環境の仮想化を実施するためのハイパバイザー及びコンテナー・ランタイム・システム
3. 公開鍵インフラ及びデジタル証明書発行
4. **産業用のファイアウォール、侵入検知・防止システム**
5. 汎用マイクロプロセッサ
6. **PLCやセキュアエレメントへの統合を目的としたマイクロプロセッサ**
7. **産業用のルータ、モデム、スイッチ**
8. セキュアエレメント
9. ハードウェア・セキュリティ・モジュール（HSMs）
10. セキュア暗号プロセッサ
11. スマートカード、スマートカードリーダー、トークン
12. **産業用のPLC、DCS、CNC、SCADAなどの産業用自動化制御システム（IACS）**
13. NIS 2 指令の別添Iに記載された**重要エンティティが使用する産業用IoT機器**
14. ロボットセンシング/アクチュエーターコンポーネント及びロボット
15. コントローラー

英国におけるIoT機器のセキュリティ政策の動向

- 英国では、2018年に消費者向けIoT製品のセキュリティに関する行動規範が発表されたほか、消費者向けIoT製品に対する対策の義務化を求める法律の検討が進められている。

- 英国政府におけるIoT機器の安全性確保に向けた近年の代表的な取組として、2018年にDCMS（デジタル・文化・メディア・スポーツ省）が、消費者向けIoT製品のセキュリティに関する13の行動規範である「Code of Practice for Consumer IoT Security」を公開した。
- DCMSは本規範をEU全体に普及させるべく技術仕様の国際標準化をETSIに提案し、本規範に基づく欧州規格であるEN 303 645が2019年11月に発表された。
- また、消費者向けIoT製品に対してセキュリティ対策の義務化を求める法律（Product Security and Telecommunications Infrastructure）の検討が現在進められている。

Code of Practice for Consumer IoT Security（2018年10月）

- 消費者向けIoT製品のセキュリティに関する13の行動規範で、消費者向けIoT製品の設計段階で安全性が確保されるよう、また利用者がデジタルの世界を安心して楽しめるようにガイドラインを設けることで、IoT製品の開発、製造、販売に携わる利害関係者を支援することを目的としている。
- 対象製品について、インターネットやホームネットワーク（両方又はその一方）と関連サービスに接続する消費者向けIoT製品を対象としている。
- 英国DCMSは本行動規範をEU全体に普及させるべく、技術仕様の国際標準化をETSIに提案。ETSIはこの提案に基づき、2019年11月に、EN 303 645として欧州規格化。ETSI EN 303 645はフィンランド、ドイツ、シンガポールのラベリング制度のベースとなっている。

IoT製品適合性評価関係の各国制度

法規制

米国
【カリフォルニア州】**SB-327 Information privacy: connected devices**
【オレゴン州】**HB-2395 (2019) Oregon Cybersecurity Bill**
- 他の法令やガイダンスに基づくセキュリティ要件の対象となっている製品を除く**インターネットに接続される機器**が対象
- **IoT機器を販売するメーカーに対し**、パスワードの管理等を含む**合理的なセキュリティ機能を具備することを要求**
- 【オレゴン州のみ】セキュリティ対策違反を起こした場合、調査措置や差止命令が行われる可能性があるほか、故意に違反していると判断された場合には、最高25,000ドルの罰金の支払いが命じられる可能性がある

日本
端末設備等規則（総務省令）
- **電気通信事業者のネットワーク（インターネット等）に直接接続するIoT製品**。
- **間接的にネットワークに接続するIoT機器**（ホームネットワークのみに繋がるスマートホーム機器、等）**は対象外。**

EU
Cyber Resilience Act（CRA）（草案提出中）
- 一部例外を除き**デジタル要素を備えた全ての製品に対して、EU全域に水平的なサイバーセキュリティ要件**を課す内容（罰則あり）
- **主として、製造業者への①上市前の設計製造に関する義務、②上市後の報告義務**に代別される。

Radio Equipment Directive（RED）（2024年8月から）
- **直接又は間接にインターネットに接続する無線製品**が対象
- ①ネットワーク・機能の損害/ネットワーク・リソース悪用/許容できないサービス低下の防止、②個人データ・プライバシー保護、③不正行為からの保護サポートを要求予定

英国
Product Security and Telecommunications Infrastructure (PSTI) Act 2022（2024年4月開始予定）
- **インターネットもしくはネットワークにつながる製品**に対して、セキュリティ対策を義務化する内容（罰則あり）
- 今後、下位法令にて具体的な内容が規定される。

任意制度（認証、ラベリング）

米国
U.S. Cyber Trust Mark Program（検討中）
- **消費者向けIoT機器**に対する任意の認証制度を2024年内に開始予定。
- 中でも消費者向けルーターは個別に要件策定がなされている。

ドイツ
IT-Sicherheitskennzeichen (IT Security Label)（導入済）
- **ブロードバンドルーター、電子メールサービス、スマートテレビ、スマートスピーカー等の消費者向けIoT製品**を対象
- 2022年8月22日時点（制度開始後8ヶ月）で34製品・サービスがラベル

オーストラリア
Labelling for Smart Devices（検討中）
- インターネットやホームネットワークに接続される前提で開発された**すべての消費者向けのスマートデバイスを対象**として検討中

EU
EU Cybersecurity Certification (EUCC)（検討中）
- ICT製品を対象とするCommon Criteria（ISO/IEC 15408）及び関連する共通評価方法（ISO/IEC 18045）に基づく認証スキーム

シンガポール
Cybersecurity Labelling Scheme (CLS)（導入済）
- **すべての消費者向けIoT製品を対象とする任意の認証制度。**4段階の認証がある。
- 2022年8月22日時点（制度開始後22ヶ月）で206製品がラベルを取得

相互運用を実施

フィンランド
Finnish Cybersecurity Label（導入済）
- **インターネットに接続され、デジタル形式でデータを処理・伝送する製品・サービスを対象**
- 2022年8月22日時点（制度開始後33ヶ月）で14製品がラベルを取得

相互運用を実施

１．諸外国の動向

２．サイバー・フィジカル・セキュリティ対策フレームワークとその具体化

２．１　IoTセキュリティ関連

２．２　ソフトウェアセキュリティ関連

２．３　OTセキュリティ関連

２．４　データセキュリティ関連

経済産業省におけるサイバーセキュリティ政策の全体像

- サイバー攻撃の高度化・多様化が生じている現状を認識しつつ、我が国**産業界へのサイバー攻撃を抑制・防御**し、事業活動への影響を最小化する。そのために国が行うべき政策を企画・実行する。
- その上で、サイバーセキュリティの確保に向けた各種の取組を、**我が国産業競争力の強化**につなげる。

①サプライチェーン全体での対策強化

- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化・実装
- 経営ガイドラインの活用促進
- サイバーセキュリティお助け隊サービスの普及促進
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）
- 日米欧によるインド太平洋地域向けの能力構築支援

サイバーセキュリティ お助け隊

IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

②国際連携を意識した認証・評価制度等の立上げ

- IoT適合性評価制度の検討、国際制度調和に向けた調整
- SBOM（Software Bill of Materials）の活用促進
- QUAD上級サイバー会合、G7等を通じた各国間連携

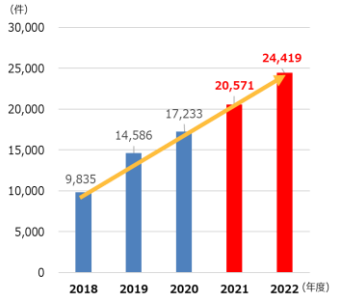
SBOMの概念的イメージ

ID	サプライヤー名	コンポーネント名	コンポーネントのバージョン	その他の一意の識別子	依存関係	SBOM作成者	タイムスタンプ
1	Company A	Application	1.1	234	Primary	Company A	05-09-2022 13:00:00
2	Company B	Browser	2.1	334	Included in #1	Company B	04-18-2022 15:00:00
3	Mr. C	Compression Engine	3.1	434	Included in #2	Company A	05-09-2022 13:00:00
4	Community P	Protocol	2.2	534	Included in #1	Company A	05-09-2022 13:00:00

③政府全体でのサイバーセキュリティ対応体制の強化

- 国境を越えて行われるサイバー攻撃へのJPCERT/CCの対処能力の向上
- 重要インフラ事業者等での事案発生時の初動支援を行うJ-CRATの体制強化
- 改正保安３法を踏まえた事故調査体制の構築
- サイバー攻撃被害情報の共有促進に向けた検討

サイバー攻撃事案の調整件数（年度集計）



④新たな攻撃を防ぎ、守るための研究開発の促進（サイバーセキュリティ産業新興）

- 先進的サイバー防御機能・分析能力の強化
- セキュリティ産業の成長加速化、製品/サービスの国内自給率向上に向けた政策検討

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
第７回：令和４年　　4月11日　開催
　産業界へのメッセージを発信

構成員

- 泉澤　清次　三菱重工業株式会社取締役社長　※2022年4月開催時点
- 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　代表執行役
- 船橋　洋一　一般財団法人アジア・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
第９回　令和4年4月4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
第８回　令和4年3月23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
第７回　令和4年4月6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2版の策定(2023.4)

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2.0版を公表(2022.4)

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
- 2023年３月にガイドラインVer1.1版を公表

工場SWG
- ガイドラインVer1.0を公表（2022.11）

・・・

分野横断SWG

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

検討事項：
「協調的なデータ利活用に向けたデータマネジメント・フレームワーク」を公開。

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

検討事項：
OSSの管理手法に関するプラクティス集を策定、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新たに公開。

「Society5.0」の社会を見据えた対策の検討

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能となる。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**となる。
- **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策定**し、必要な対策を検討。

https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html

サイバー空間で大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

CPSFのモデル

<3層構造>

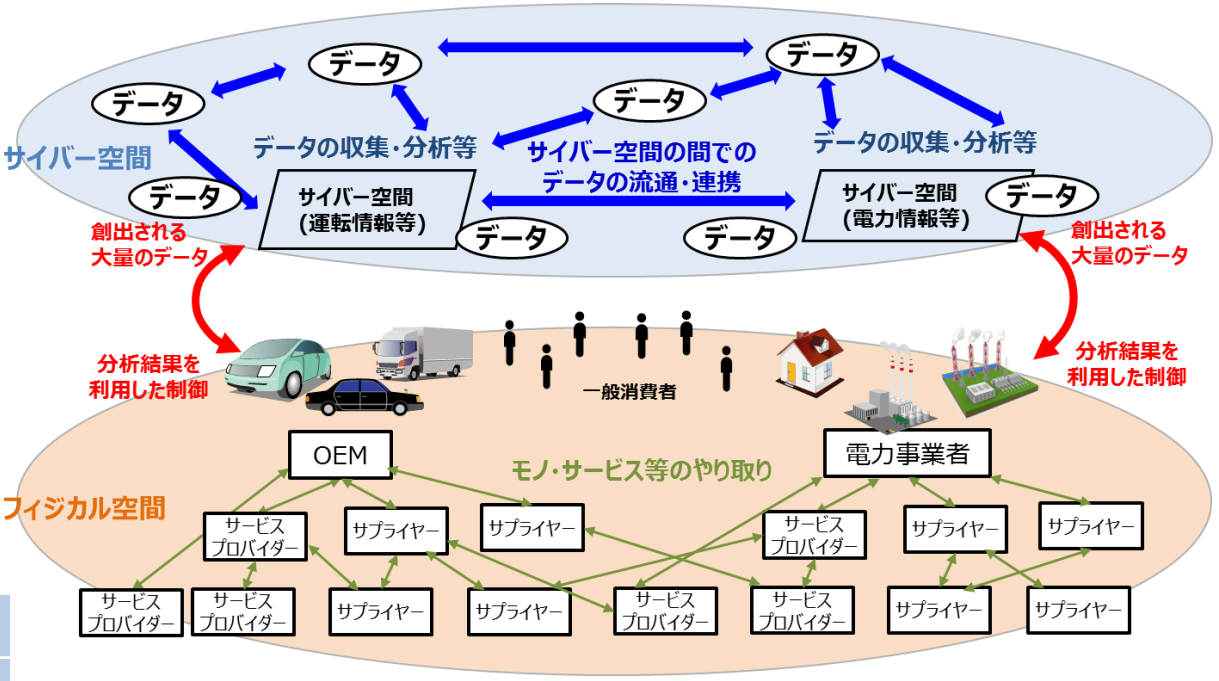
【第３層】
サイバー空間におけるつながり

【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

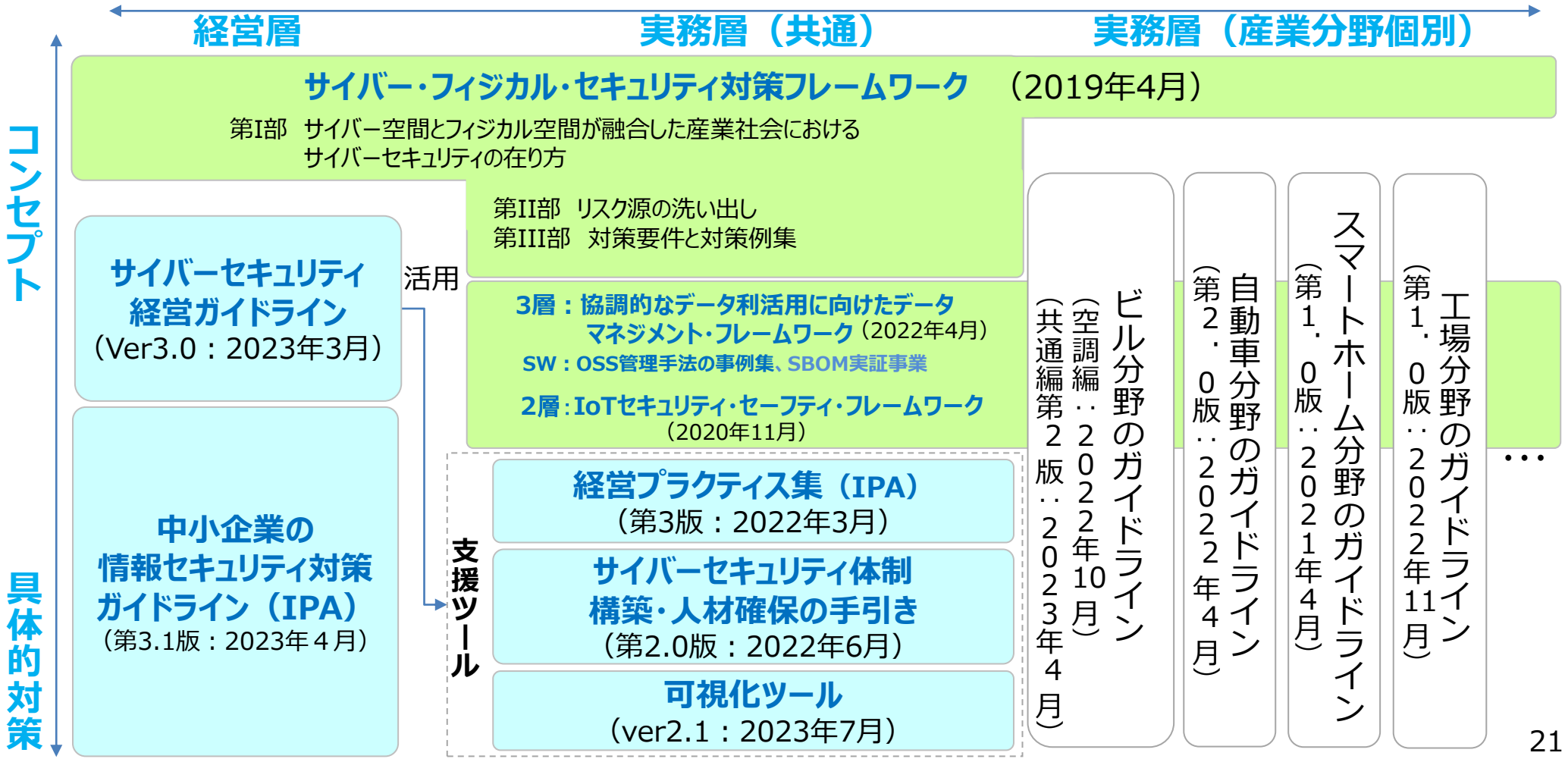


Society5.0の社会におけるモノ・データ等の繋がりのイメージ

サイバー・フィジカル・セキュリティ対策フレームワークを軸とした各種取組

- 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＞



１．諸外国の動向

２．サイバー・フィジカル・セキュリティ対策フレームワークとその具体化

２．１　IoTセキュリティ関連

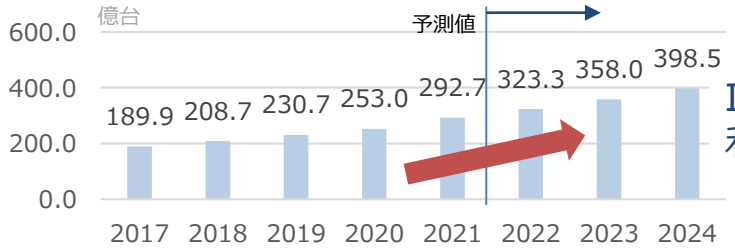
２．２　ソフトウェアセキュリティ関連

２．３　OTセキュリティ関連

２．４　データセキュリティ関連

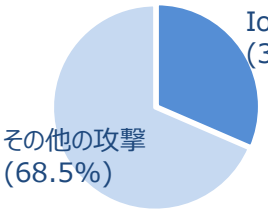
IoT機器の利用拡大に伴い増加するリスクと、その経営への影響

ネットワークに接続される機器(IoT機器)は増加傾向、IoT機器を狙った攻撃は多い



IoT機器の
利用数は増加

世界のIoT機器数の推移及び予測(※1)



ダークネットにおける年間観測パケット数の割合(※2)

不審な通信のうち
約1/3はIoT機器を狙った攻撃

[※1] 出所:総務省「情報通信白書令和4年版 データ集」(3章関連データ)
[※2] 出所:NICT「NICTER観測レポート2022」調査を除く攻撃パケットのうち、23/TCP、22/TCP、5555/TCP、81/TCPへのパケットを集計。

IoTにおけるセキュリティインシデントが経営に大きな影響を及ぼす可能性が高まっている

操業停止や逸失利益の発生を含む事業への直接的な影響

半導体製造工場の制御装置に対する攻撃によって、**3日間の操業停止、営業機会損失が発生(売上高(四半期)の3%損失)**[台湾:2018]

石油化学工場の安全計装システムを対象とした攻撃による**操業停止。プラント爆発のおそれ**[サウジアラビア:2017]

脆弱性対応や損害賠償を含む追加費用の発生

脆弱性発見による自動車140万台のリコールの発生。脆弱性等の対応で、**2億9900万ユーロ(約394億円)の赤字を計上**(四半期の最終損益) [米国:2015]

評判の低下等より生じる競合優位性の低下

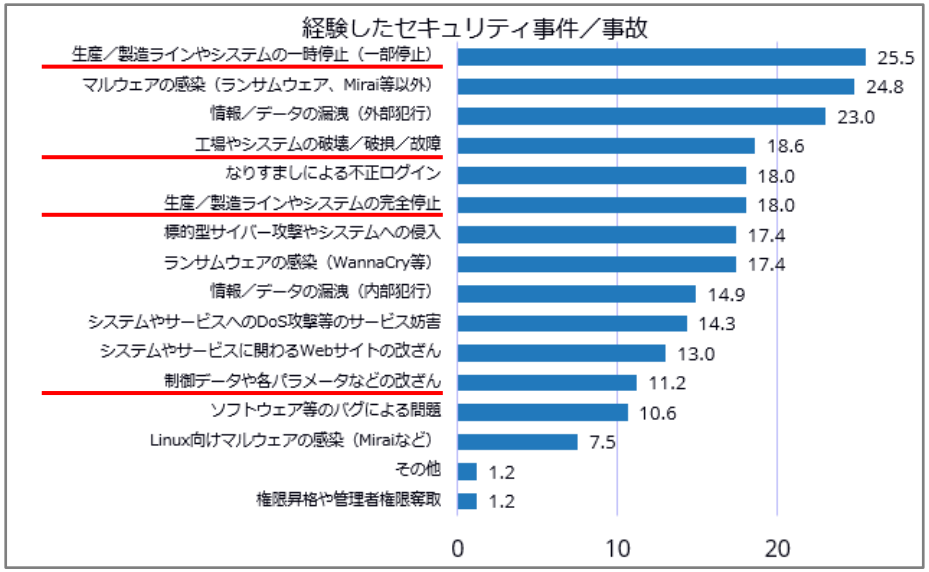
高級ホテルで客室のカードキー発行システムがランサムウェアに感染し、一切のシステム操作が不可能となった。客室扉の施錠、開錠が不可能となり、宿泊客が閉め出される事態が発生。**サービスの品質が著しく低下** [オーストリア: 2017]

[参考] 各公開情報を基に作成

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**。**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**。
- 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。**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**。**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**。

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**が提起。

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適合性評価制度検討会

経産省においてIoT適合性評価制度検討会立ち上げ

- **IoT機器の急増に伴い、IoT機器の脆弱性を狙ったサイバー脅威が高まってきた**ことから、**IoT製品のセキュリティ対策を適切に評価し、適切な対策が講じられているIoT製品が広まる仕組みの構築が必要**。また、我が国のIoT製品がグローバルマーケットから弾き出されないよう、諸外国の取組を考慮することが必要。
- こうした観点で制度の検討を行うため、2022年11月より「**IoT機器に対するセキュリティ適合性評価制度構築に向けた検討会**」を３回開催し、2023年5月に**中間報告をとりまとめた**。委員は、学術界、法曹界、業界団体、企業、消費者団体から構成。オブザーバとして、関係省庁、研究機関、認証機関が参画。 2023年度中の最終報告に向け議論を継続中。
- 国内での議論と並行して、米EU等の諸外国との制度調和を図るための国際的な対話も実施中。

中間報告（概要）

検討会において議論した事項

● **課題**

ベンダ、利用者、国民の三者において、以下の課題が存在。

✓ **ベンダ**： **対策が評価されず製品価値に繋がらない**。諸外国の制度対応負担が増加。
✓ **利用者**： **適切な対策の製品が可視化されていないため、適切な製品を選べない**。
✓ **国民**： 適切でない製品が多く流通した場合、IoTがボット化するなどして、**国内のシステムや国民生活に悪影響を及ぼす**。

● **構築すべき適合性評価制度**

✓ ベンダによる能動的なセキュリティ向上を促す観点や、特に中小企業の負担の観点から、**まずは任意制度として制度を運用することが適当**。**ただし、制度の浸透具合や、諸外国の動向によっては、法令に基づく義務化の検討も必要になり得る**。

✓ 対象製品範囲については、「**間接的又は直接的にインターネットに接続する製品**」とすることが適当。その上で、具体的な対象製品については今後要検討。

✓ 適合性評価基準については、国際的な標準を参照の上、**国際的な標準と整合的な形で構築していくことが適当**。その上で、具体的にいかなる製品にどのような基準を適用するかは今後要検討。

✓ 運用については、**既存の評価スキーム**を活用した制度とすることが適当。その上で、具体的にどのようなスキームを活用すべきかは今後要検討。

→ **JISEC制度**

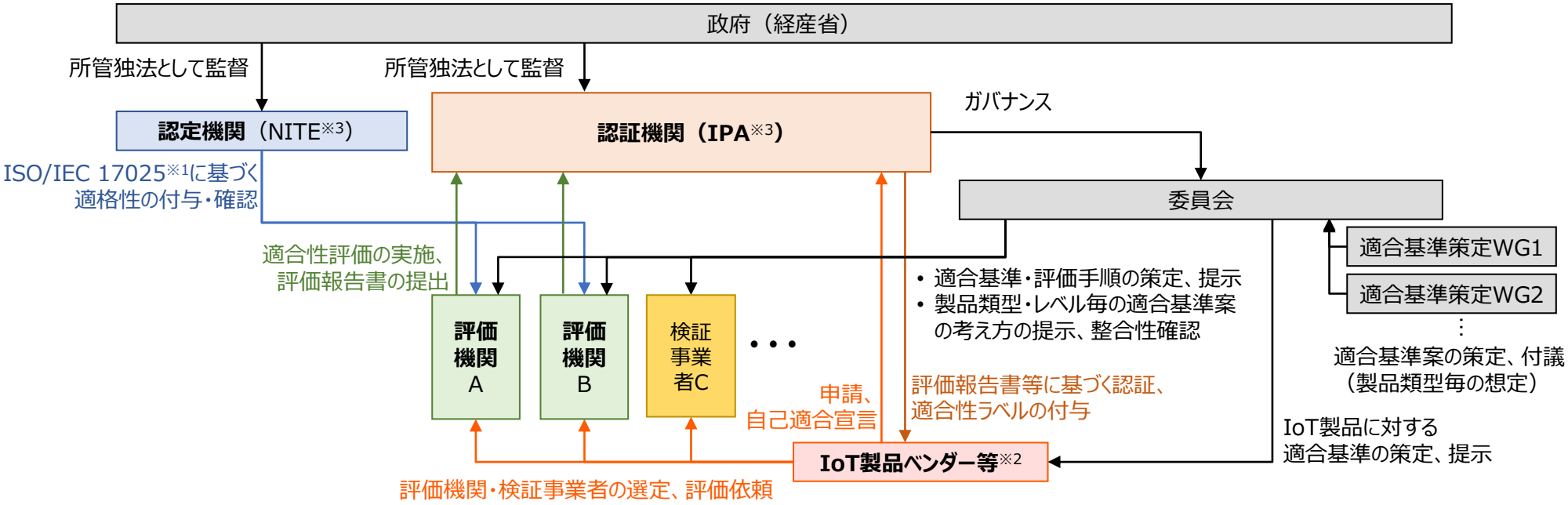
今後議論が必要な事項

上記に加え、政府の関与や検討体制のあり方、IoT製品ベンダーの能動的な制度活用を促す仕掛け、適合性評価済製品におけるセキュリティ事案への対応。

【IoT機器に対するセキュリティ適合性評価制度構築に向けた検討会】会議資料
ワーキンググループ3（IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会） （METI/経済産業省）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html

JISEC制度をベースとした適合性評価制度の全体像

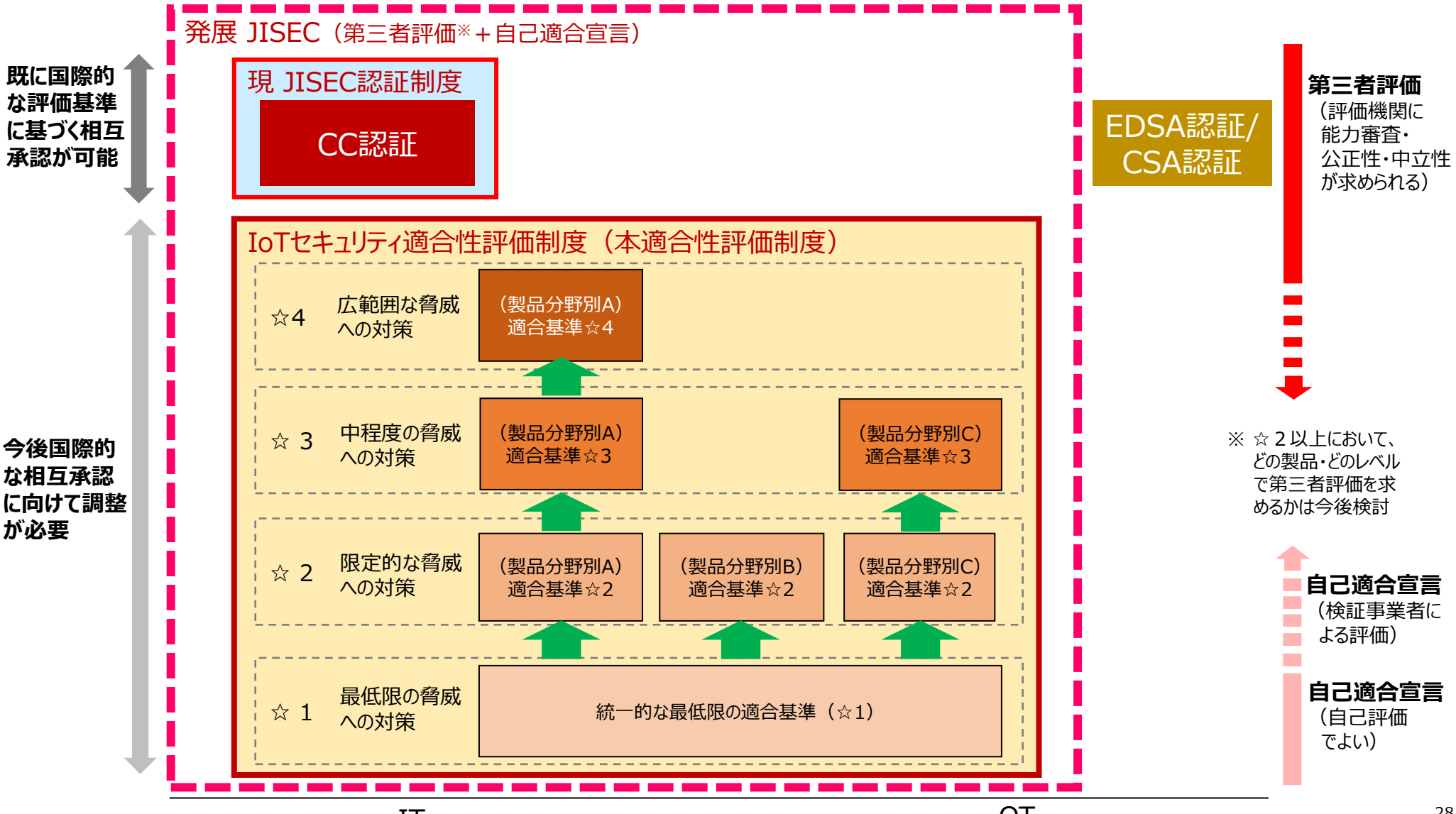
- これまでの議論を踏まえ、本制度の各主体の適格性について、政府のガバナンスが効く構造が重要。かかる観点から、**CC認証の知見があるIPAのJISEC認証制度**（ITセキュリティ評価及び認証制度）**を拡張する形の制度**を構築予定。
- **2023年度末までに要求基準・適合基準の検討**および**ルーター、スマート家電、ネットワークカメラ等を対象とした評価検証**を行う予定。



※1：ISO/IEC 17025（JIS Q 17025）は、試験所及び校正機関の試験・校正能力に関する一般要求事項を規定した国際標準であり、JISEC認証制度に基づくIT製品及びシステムのセキュリティ評価を行う試験事業者に求められる。なお、ISO/IEC 17065（JIS Q 17065）は、製品認証機関の認証能力に関する一般要求事項を規定した国際標準である。
※2：IoT製品を製造するベンダーだけでなく、海外からIoT製品を輸入・販売する輸入業者も含まれる。
※3：組織名称は制度発足時に変更となる可能性がある。

既存制度との関係性と評価方法

- CC認証のみを対象としている現行のJISEC認証制度を拡張し、本適合性評価制度を含む形の新たな枠組みを立ち上げる。
- 最低限の適合性評価レベル(☆1)では自己適合宣言を許容しつつ、リスクの高い分野の製品には第三者評価を求める。

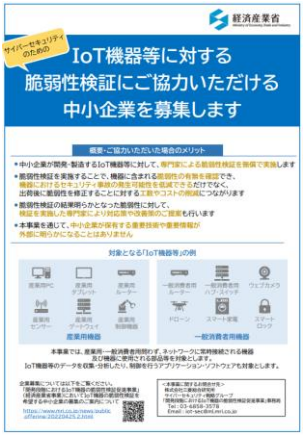


IoT機器等の開発時のセキュリティ向上

IoT機器に対する脆弱性検証の実証

- 令和３年度補正予算事業として、中小企業等が開発・販売するIoT機器の対策の現状を把握するとともに、セキュリティ検証の留意点や求められる対策を抽出するために、実証事業として、**IoT機器の脆弱性検証を希望する中小企業等を募集し、74社・155製品に対して、IoT機器検証（ペネトレーションテスト等）を実施した**ほか、**優れたIoTセキュリティ対策を行っている企業へのヒアリング**を実施した。

※「中小企業」の定義は中小企業基本法に基づき、製造業であれば資本金3億円以下又は従業員数300人以下の企業を中小企業としている。



応募のあった製品のうち、**74社・155製品**に対して、
検証事業者による脆弱性検証を実施

申込み企業の意向や各検証事業者の実績・能力を踏まえ、
各製品の検証を実施する検証事業者を割り当て

【本実証事業における検証事業者】

- 株式会社AGEST
- 株式会社FFRIセキュリティ
- GMOサイバーセキュリティ by イエラエ株式会社
- 株式会社ラック
- 株式会社ベリサーブ
- 株式会社ユビキタスAI
- 株式会社ベルウクリエイティブ
- サイバートラスト株式会社
- 株式会社SYNCHRO
- 大日本印刷株式会社
- 株式会社神戸デジタル・ラボ

【74社の主な業種】

- 製造業（電気機器器具、一般機械器具、輸送用機械器具、出版・印刷等）
- 通信業
- 卸売・小売業
- 情報サービス業
- 専門サービス業

等

【155製品の主な類型】

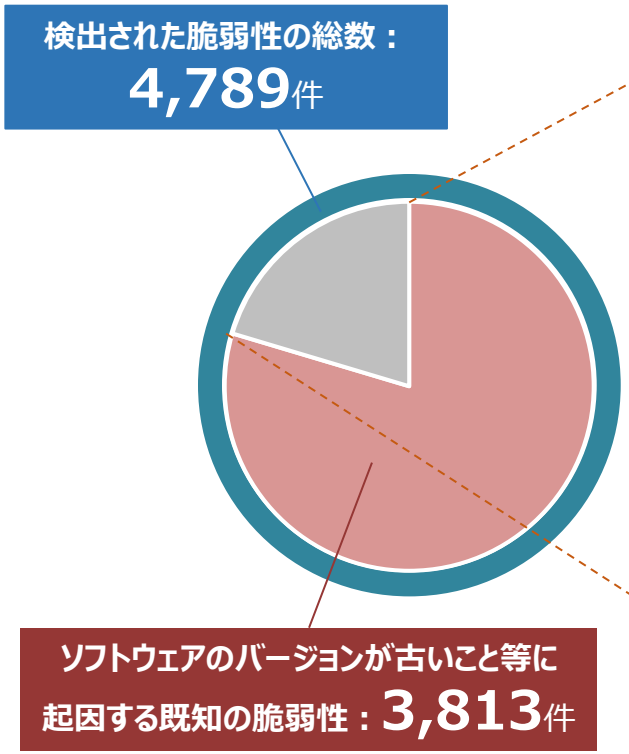
- ゲートウェイ・ルータ
- ネットワークスイッチ
- UTM・ファイアウォール
- ネットワークカメラ
- スマートロック
- 産業用センサ
- 産業用コントローラ
- 産業用ロボット
- ドローン
- 複合機
- スマートメータ
- スマート家電

等

検証の結果明らかになった脆弱性

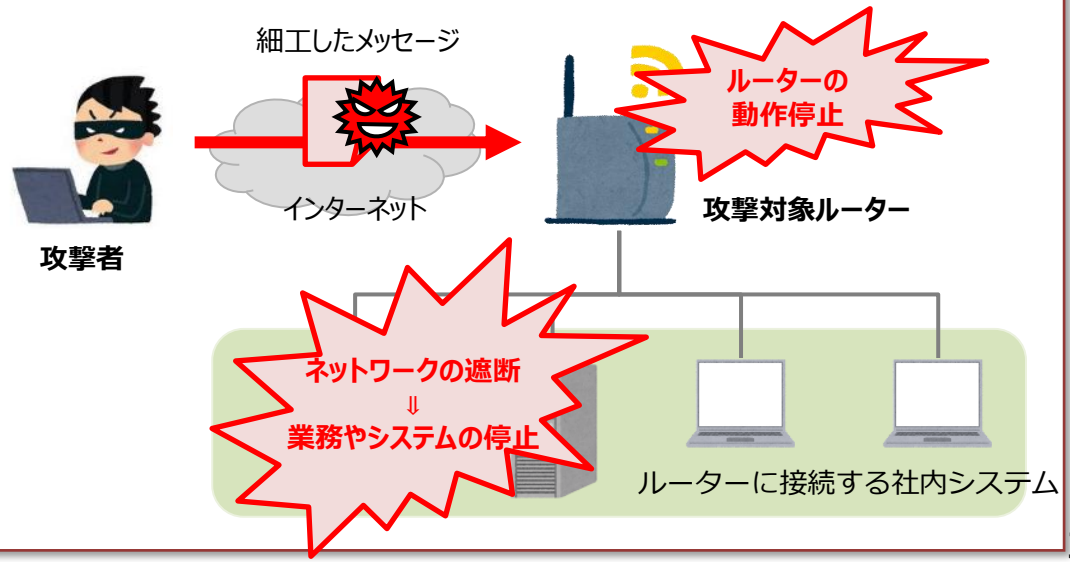
- 155製品に対する検証の結果、**計4,789件の脆弱性が検出**された。
  ※脆弱性が検出されなかった製品もあった一方で、多いものでは１製品につき900件の脆弱性が検出された。
- 検出された脆弱性のうち、**約80%の脆弱性**については、**IoT機器に搭載されているソフトウェアのバージョンが古いこと等に起因する既知の脆弱性**であった。これらの脆弱性が悪用された場合、**導入している企業の業務やシステムが停止するおそれ**や、**個人情報や機微情報などの重要情報が外部に漏えいするおそれ**がある。
- また、実証に協力いただいた**検証事業者からも、大手企業が開発・販売しているIoT機器と比較して、多くの脆弱性が検出**されたことが指摘された※。
  ※本事業の検証結果では、１製品あたりの脆弱性件数について、大企業製品のみでは18.57件だったに対し、中小企業製品のみでは35.48件だった。

検証の結果明らかとなった脆弱性の件数



ルーターにおいて検出された深刻度の高い脆弱性の悪用例

ルーターに搭載されている通信ソフトウェアのバージョンが古いと、処理能力を超える大量のデータや悪意あるデータを送られることでメモリの許容量を超えてしまう脆弱性（バッファオーバーフロー）に繋がり、この悪用されることで、サービス拒否を引き起こしたり、任意のコードが実行される可能性がある。この結果、ルーターの動作が停止し、ネットワークへの接続が遮断され、企業の業務やシステムが停止するおそれがある。
対策として、最新バージョンのソフトウェアにアップデートすることが必要となる。



IoT機器開発中小企業の効果的なセキュリティ対策事例

- 他方で、実証に協力いただいた中小企業の中には、IoT機器の開発段階から**効果的なセキュリティ対策を進めている事例**も見られた。

株式会社SYNCHRO（シンクロ）　IPカメラシステム“KATABAMI”

【取組内容】

- 株式会社SYNCHROは、セキュリティ設計が得意な開発請負業者とも連携し、開発初期の時点から、販売を行う前の最終的なセキュリティ確認の際に、いかなる検証を行うべきかの仕様を定めている。

→**セキュリティ機能が高く、かつ脆弱性が解消されている製品の出荷が可能に**。
　また、製品の機能やコンパクトさのみならず、**セキュリティ機能を付加価値とし
てユーザに訴求することも可能に。**

※当該企業は、IoT製品の開発者コミュニティを地域で立ち上げ、企業間で知見を共有することで地域
　一体となった人材のレベルアップの実現にも貢献。

企業概要

企業名	株式会社SYNCHRO
従業員数	10-19名
所在地	東京都
設立	2001年
主要製品	・静脈認証システム ・アクセス制御機能付きキャビネット ・入退室＆ログオン管理連動システム ・共連れ検知システム

製品の特徴

1.ネットワーク・セキュリティの強化
　暗号化通信機能の強化により「なりすまし」「中間者攻撃」等のサイバー攻撃を防御

2.コンパクト
　処理能力も実装サイズもコンパクト、IoT機器への組み込みを容易に

3.ネットワーク自体でセキュリティを確保
　アプリケーションではなくネットワークレイヤでセキュリティ機能を実装、様々なシステムへの応用が可能

IoT機器等を開発する中小企業向け製品セキュリティ対策ガイドの作成・普及

- このような優れた中小企業を増やすことが、我が国全体のIoT製品のセキュリティ向上には重要。しかし、IoTセキュリティに関するガイドラインは多数あるものの、内容が専門的であるなど中小企業にとってわかりやすいガイドにはなっておらず、「**何を参照していいかわからない**」「**どのような対策をすればいいかわからない**」という状況。
- そこで、中小企業がIoT製品の開発を行う際にセキュリティ面で考慮してほしいポイントをわかりやすく記載した「**IoT機器を開発する中小企業向け製品セキュリティ対策ガイド**」を策定し、公開（2023年6月）。本ガイドでは、**セキュアなIoT機器が数多く出荷**されていくためには、**出荷前の検証のみならず設計・開発といった初期段階からセキュリティ対策を実施することが重要**である旨を記載。また、既存ガイドの重要ポイントや優良企業の事例も記載。
- 今後、**中小企業関連政策や中小企業関連団体と連携**を行い、**IoT機器の設計・開発段階でのセキュリティ対策や検証の必要性をより多くの中小企業が認識するよう普及活動**を行っていく。

「IoT機器を開発する中小企業向け製品セキュリティ対策ガイド」の策定

関連ガイドラインから最初に実施すべき対策を抽出

ガイド目次

- 経営者の皆様へ
- 本ガイドの概要
- 各フェーズで求められる対策
- 設計・開発フェーズで検討すべき主な技術的対策
- IoT機器を開発する中小企業の対策事例集
- 付録

各フェーズで求められる対策

節	項目
方針・体制構築フェーズで求められる対策	【対策1】製品に関するセキュリティポリシーを策定・周知する
	【対策2】セキュリティポリシーを適切に運用するための体制を整備する
設計・開発フェーズで求められる対策	【対策3】IoT機器等において守るべきものを特定し、それに対するリスクを想定する
	【対策4】守るべきもの及びリスクを考慮した設計・開発を行う
検証フェーズで求められる対策	【対策5】セキュリティに関する要件が満たされているかを検証する
運用・保守フェーズで求められる対策	【対策6】出荷後もリスクに関する情報の収集や関係者とのコミュニケーションを行い、適切なサポートを行う

中小企業関連団体等を通じた周知

HP・メールマガジン等を通じた案内、セミナー等における案内、各都道府県を通じた地域の中小企業への周知

日本商工会議所 The Japan Chamber of Commerce and Industry
Be a Great Small. 中小機構
全国中小企業団体中央会

SC3を通じた中小企業関係者、業界団体等への周知・案内

SC3 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

設立：2020年11月1日
概要：産業界が一体となって、中小企業を含むサプライチェーン全体のサイバーセキュリティ対策を推進するコンソーシアム
会長：遠藤　信博（一般社団法人日本経済団体連合会副会長・サイバーセキュリティ委員長）

「IoT機器等を開発する中小企業向け製品セキュリティ対策ガイド」全体概要

ガイドの基本的な考え方

- サイバー攻撃の脅威が増している中、IoT機器等のセキュリティを確保することは極めて重要です。企業規模によらず、必要なセキュリティ機能を搭載させる対策を実施しましょう。

- IoT製品にセキュリティが実装されていることを確認するためには、セキュリティ検証が有効です。しかし、**出荷前の検証で問題が発見**された場合には、**製品の販売に影響が出る**ことも考えられるほか、必要な機能が実装できないなど**製品のセキュリティ自体に支障が出てしまう可能性**もあります。そのため、**設計や開発段階からセキュリティを考慮すること（セキュリティ・バイ・デザイン）がとても重要**です。

- しかし、IoTのセキュリティに関しては国内外に**複数のガイドラインや規格等が提示**されており、セキュリティ対策に取り組もうとする企業にとっては、**何から始めてよいかがわかりにくい**場合があります。
  → **IoT機器等のセキュリティ対策を行おうとする企業が第一歩として取り組む対策を提示**

- 本ガイドに示した対策それぞれを実施することが理想的ですが、中小企業においては**予算や人員が限られるなど、対策全てを網羅的に実施することは難しい**場合もあると考えられます。企業の経営方針、成長ステージ、人員の状況や体制、予算、製品の特性、顧客との関係など、**自社を取り巻く様々な環境を考慮しつつ、優先順位をつけて、まずできるところから対策を進めることが重要**です。
  → **リソースに限りがありながらも、セキュリティ対策を効果的に進める中小企業の事例集を掲載**

ガイドの想定読者の方

- IoT機器等を開発する中小企業の経営者
- IoT機器等を開発する中小企業のセキュリティ担当者・開発担当者・品質管理者

中小企業は、様々な経営課題の中でセキュリティ対策に取り組む優先順位が低くなる場合や、セキュリティ担当者が別の業務を兼務している場合が多いことから、**実施事項をわかりやすく示した本ガイドは、主に中小企業を対象**としています。

ただし、本ガイドに記載している事項は中小企業以外の企業にとっても参照されるべき事項であるため、**セキュリティ対策に取り組もうとしているIoT機器等を開発する皆様にご活用**いただけます。

各フェーズで求められる対策

方針・体制構築

対策1
製品に関するセキュリティポリシーを策定・周知する

対策2
セキュリティポリシーを適切に運用するための体制を整備する

設計・開発

対策3
IoT機器等において守るべきものを特定し、それに対するリスクを想定する

対策4
守るべきもの及びリスクを考慮した設計・開発を行う

運用・保守

対策6
出荷後もリスクに関する情報の収集や関係者とのコミュニケーションを行い、適切なサポートを行う

検証

対策5
セキュリティに関する要件が満たされているかを検証する

設計・開発フェーズで検討すべき主な技術的対策

IoT機器等で提供する機能と対応する主な技術的対策

(1) 通信機能を提供するIoT機器等	(2) データの送信・保存機能を有するIoT機器等	(3) 高い可用性が求められるIoT機器等
A 認証・認可機能の提供 B アップデート機能の提供 C ログの保存機能の提供	A データの暗号化・保護機能の提供 B データの削除機能の提供	A システムの復旧の提供 B 異常検知機能の提供

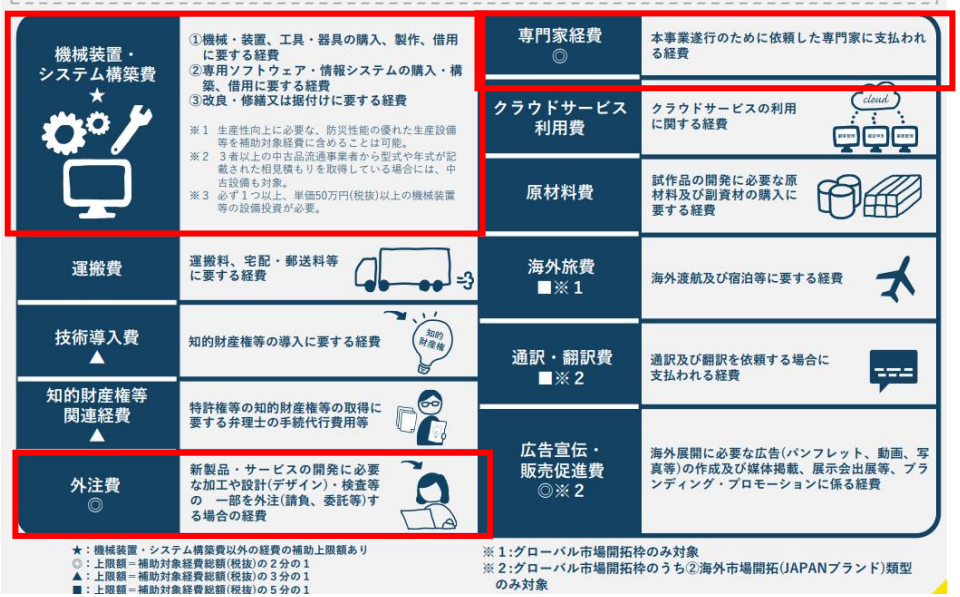
中小企業に対するセキュリティ・バイ・デザインの補助

- 前述のとおり、中小企業によるセキュアなIoT機器が数多く出荷されていくためには、**出荷前の検証のみならず、設計・開発といった初期段階からセキュリティ対策を行っていくことが重要**。
- 「ものづくり補助金」では、中小企業が開発するIoT機器に関連して、
  - ✓ **設計時にセキュリティ設計が得意な専門家のアドバイスを受けることに係る経費**
  - ✓ **生産性向上やセキュリティ向上に資する機械・ソフトウェア等の設備投資**
  - ✓ **ペネトレーションテスト等の検証費用**

  等に対する補助を行うことが可能。
- このように、**IoT機器の開発から出荷に至る一連のプロセスでサポートを行う**ことで、**中小企業がセキュアなIoT機器を数多く出荷していくことを後押し**していく。

- 予算額：2,000億円（R4年度2次補正）
- 補助下限額：100万円、補助上限額：750万円～5,000万円※
  補助率：1/2~2/3※

※従業員数や公募枠により補助上限・補助率が変動
※例年の採択件数は、1公募あたり、2,000～3,000件程度
※補助を受けるには50万円以上の設備投資が必要



設計・開発

設計・開発段階で、どのようなセキュリティ機能を搭載すべきかについて、セキュリティの専門家のアドバイスを受けたい。

生産

IoT製品の機能性を上げるために生産設備を導入したい。また、生産段階でセキュリティ上不正な機能が混入しないようセンサを導入したい。

検証

製品に脆弱性がないかを確認するために、ペネトレーションテストや脆弱性診断を行いたい。

もの補助で補助が可能

セキュアなIoT機器の出荷

IoT-SSF

IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の策定

- IoT機器は、出荷時のみならず、使用時において、ステークホルダー間で適切にリスク管理されていることが重要。
- **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**。

https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html
https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html

IoT-SSF(※3)活用によるリスクマネジメントのメリット

[※3] IoT-SSF:IoTセキュリティ・セーフティ・フレームワーク

セキュリティリスクへの対処には、
組織全体や関係者の現状を把握した上でリスクの抽出とそれらを考慮した対策が必要

IoT-SSFを活用することで、包括的にIoTにおけるリスクの抽出とそのリスクへの対策が可能

特徴1

関係者と協力することで
抜け漏れなく対策が可能

特徴2

けがや事業への被害を
考慮しつつ包括的に
IoTのリスクを特定可能

特徴3

既存の
製品安全分野の検討結果と
調整しつつ対策が可能

- IoTに関係するシステム・関係者の全体を把握できていない
- 攻撃を受けたときに想定している影響範囲に不安がある
- 効果的な対策や投資範囲がわからない

セキュリティリスクへの対処に
あたって想定される悩み(例)

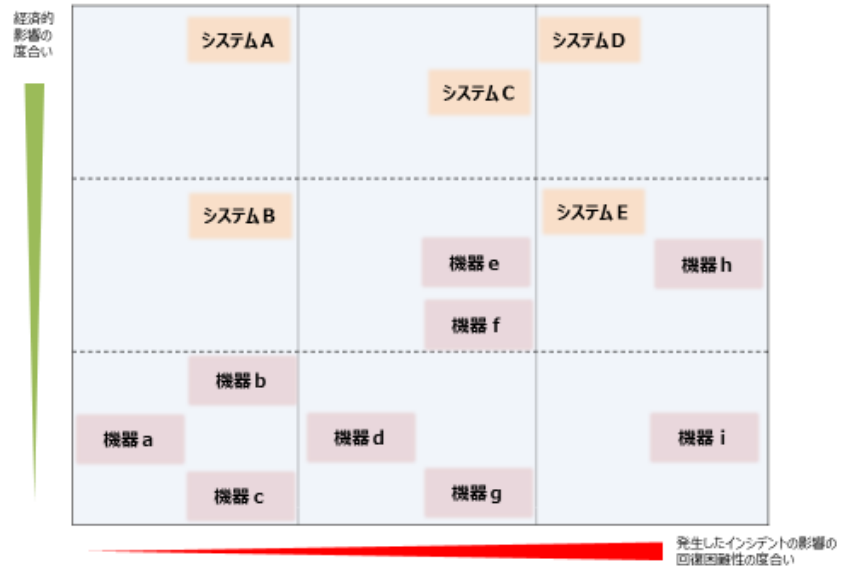
【適用実証に参加された事業者からお寄せいただいたお声】

- ◆ 組織外部の関係者におけるリスクを確認できた点にメリットを感じた。(家庭用機器製造事業者)
- ◆ 関係者間で共通の認識を持った上で、事業リスクを考慮しつつ脅威を整理することができた。(住宅メーカ/住宅設備製造販売事業者)
- ◆ 製品安全分野の技術者とセキュリティ分野の技術者間で認識をすり合わせつつ、IoT-SSFを適用できた。(制御機器メーカ)

IoT-SSFの枠組み

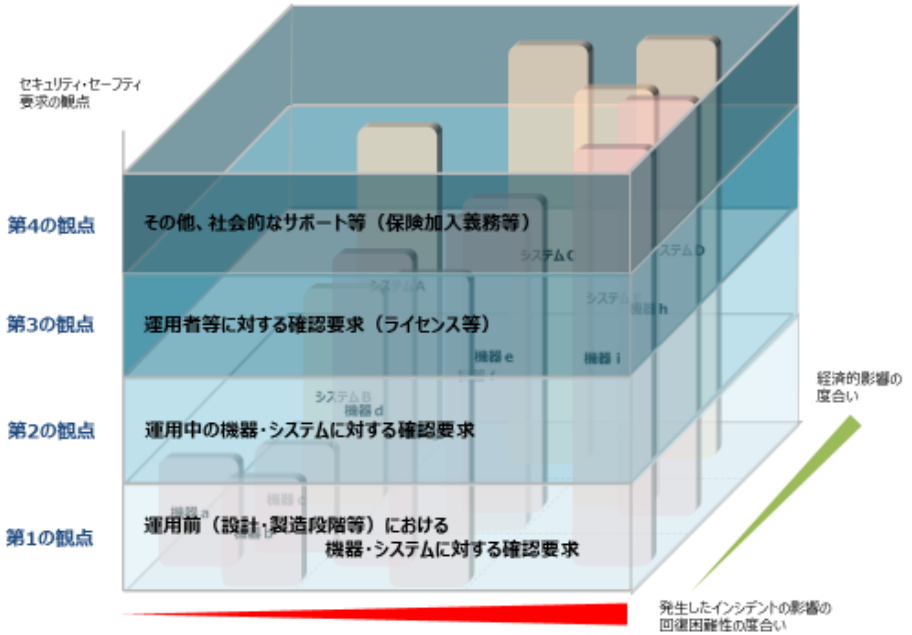
- 実現される仕組み・サービスの利用者側から見てインシデントが発生した場合の影響を適切に分析。
  - 第１軸：発生したインシデントの影響の回復困難性の度合い
  - 第２軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算）
- それぞれのカテゴリーに従って第３軸を活用してセキュリティ・セーフティ要求の観点・内容を適切に検討するための枠組み。
  - 第１の観点：運用前（設計・製造段階等）におけるフィジカル・サイバー空間をつなぐ機器・システムの確認要求
  - 第２の観点：運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求
  - 第３の視点：機器・システムの運用・管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

- 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。

2022年4月に公表

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

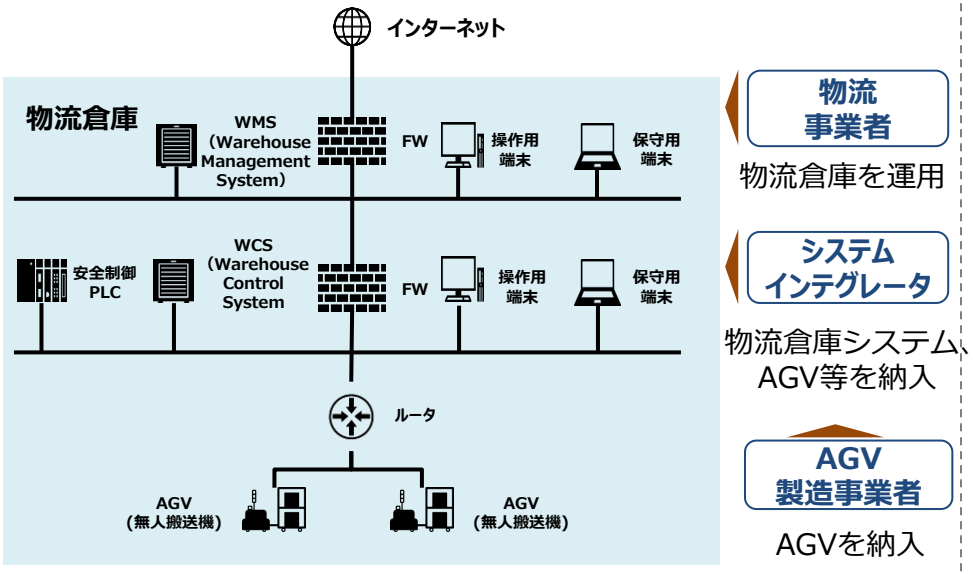
- 添付Aと添付Bは、各ユースケース固有の事情に依存しない一般的に適用し得る内容
- 想定読者において具体的な対策を検討する際に適宜参照

(例)物流倉庫内のAGVによる自動ピッキング（ケースの概要：事前準備）

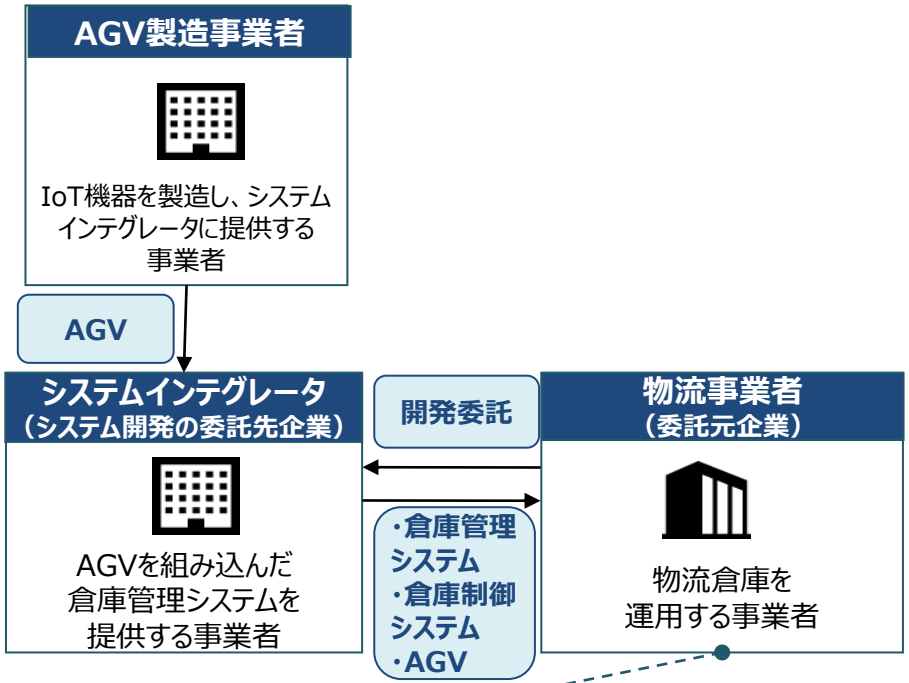
- 物流事業者がIoT-SSFの主たる適用主体となってリスクマネジメントを行うユースケース。
- 当該事業者は、事業規模拡大に伴って既存の物流倉庫において、省人化や効率化を目的として新たにAGVや倉庫制御システム等の導入を予定。

✓ 対象機器・システムの概要

- 工業用間接資材を扱う物流倉庫において、無人搬送車（AGV）が自動ピッキングを行う。
- 物流倉庫内の保管エリアにてAGVが保管棚をピッキングエリアにいる作業員のもと（ピッキングステーション）まで移動させ、作業員がピッキングを行う。



✓ 適用主体及び他のステークホルダーの情報



IoT-SSFの適用主体	**既存の物流倉庫**において、省人化や効率化を目的として**AGVや倉庫制御システム等の導入**を予定している。

(例)物流倉庫内のAGVによる自動ピッキング（リスクアセスメント）

- セキュリティインシデントによって「物流事業者」が保有する倉庫内の業務が停止し、倉庫内のみならず取引先、サプライチェーン規模で影響が波及し、結果として生じる経済的影響が大きくなる可能性がある。

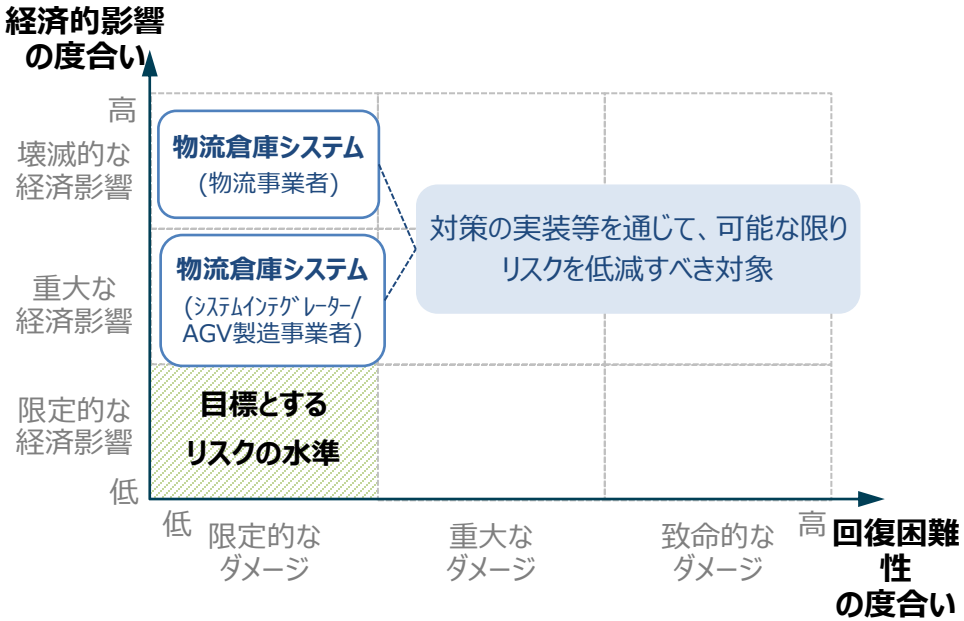
✓ 対象機器・システムにおいて想定されるリスク(例)

分類	想定されるリスク（例）
物流事業者にとってのリスク	• 外部から**倉庫管理システムが不正にアクセス。**保存されている在庫情報が改ざんされ、**配送の停止や誤配送が生じ得る**。 • 配送の停止や誤配送により、搬送会社や工業資材の利用者等、物流サービスの提供を受ける**倉庫外部の事業者等へ影響が及ぶ可能性がある**。
システムインテグレータにとってのリスク	• **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、物流工場が停止し、**大規模な製品回収が生じ得る**。
AGV製造事業者にとってのリスク	• **AGVに重大な脆弱性が発見**されることによって、**大規模な製品回収が生じ得る**。

※その結果として、各事象のステークホルダを含む関係者に対する損害賠償（配送遅延や誤配送への対応等）の事後的な対応が発生し得る

✓ 想定されるリスク(例)のマッピング結果

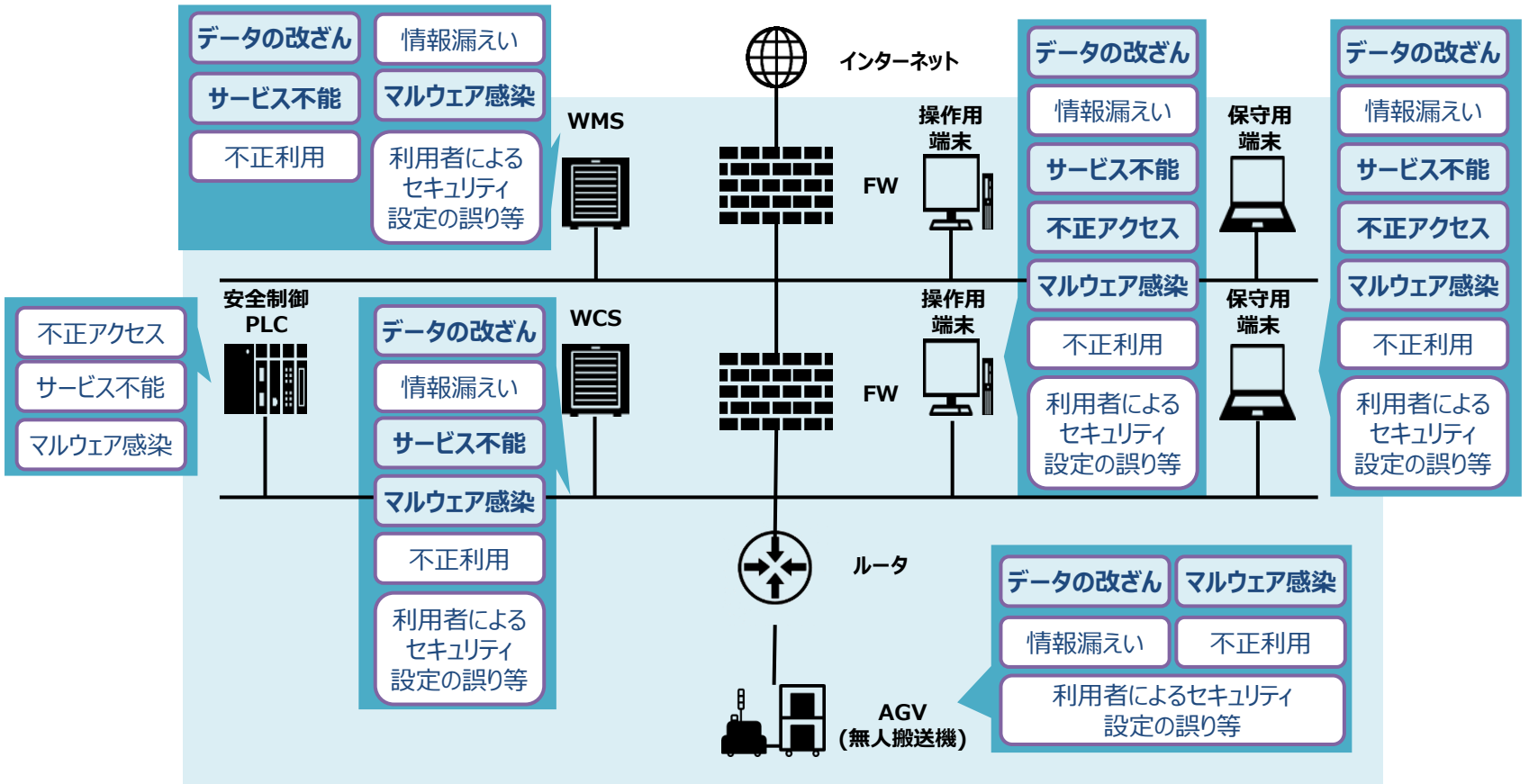
- 物流事業者、システムインテグレータ及びAGV製造事業者視点の物流倉庫システムの保有するリスクは、目標とする水準には収まっておらず、何らかの対処実施が望まれる。



(例)物流倉庫内のAGVによる自動ピッキング（リスク対応の検討）

- 影響度が大きいリスクにつながり得る脅威の例： 不正アクセス、サービス不能、マルウェア感染等。
- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

(例)物流倉庫内のAGVによる自動ピッキング（リスク対応の検討）

- 適用主体である物流事業者は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討。
- 行うべきと考えられる対策の例：様々なIoT機器を接続する際のセキュリティの確保 [第1の観点]、IoT機器・システムのモニタリング及びログの取得、分析[第2の観点]等。

物流事業者(自身)にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
セキュリティインシデントが発生したとしても、それらの被害を最小限にするための仕組みの構築	• **様々なIoT機器を接続する際のセキュリティの確保** • **適切なネットワークの分離**
信頼性の高い物流倉庫の操業を可能にするための仕組みの構築	• **IoT機器・システムの十分な可用性の確保** • **IoT機器・システムのモニタリング及びログの取得、分析**

システムインテグレータにとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
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	• **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** • **セキュリティ設計と両立するセーフティ設計の仕様化**
安全なアップデートプログラムの配信のための仕組みの構築	• **IoT機器・システムに対するアップデートの適用**

１．諸外国の動向

２．サイバー・フィジカル・セキュリティ対策フレームワークとその具体化

２．１　IoTセキュリティ関連

２．２　ソフトウェアセキュリティ関連

２．３　OTセキュリティ関連

２．４　データセキュリティ関連

OSS管理手法に関する事例集の策定

https://www.meti.go.jp/policy/netsecurity/wg1/ossjirei_20220801.pdf

- OSSの**留意点を考慮した適切なOSS利用の促進**

✓ 企業がOSSを利用するに当たって留意すべきポイントを整理。

✓ そのポイントごとに**参考となる事例を、具体的な個別企業ヒアリング等により取りまとめ**公開。

✓ 企業のOSS利用の障壁を取り除くことで、一層のOSS利活用を促進。

✓ 産業界において**OSSのメリットを享受することで競争力を向上**

OSSに関する課題例

ライセンス管理

脆弱性管理

サプライチェーン管理

組織体制

コミュニティ活動

OSS事例集で紹介する取組例

- スキャンツールを用いて**ソフトウェア部品構成表（SBOM）を作成**。
- **脆弱性やライセンス等について、抜け漏れのないリスク管理**を実施。
- **安全確認したOSSの登録・利用**、良質なOSS選定のため**評価結果のレーダーチャート化等に係るシステムの構築**。

- サプライヤからの部品・ソフトウェア納入の際に、**確認書を提出**。
- **OpenChain Japan WGを活用し、サプライヤの理解促進**。
- **サポート終了リスク、長期間利用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、顧客と事前合意**。

- OSS利活用プロセスを**全社ルール化して、トップダウンで適用を指示**。**適用プロジェクトを増やし、高い効果**に結実。

- 社員に対して、**就業時間内でのOSS開発等を容認**。
- **自社開発のソフトウェアをOSS化**し、**コミュニティ型開発**により**性能向上**。

（参考） OSS管理手法に関する事例集の主な掲載事例

- OSSの利用が広がる一方、自社だけでOSSを検証するための体制等を整える負担は大きく、ベストプラクティスを共有することに対するニーズが存在していることを踏まえ、**「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（2022年8月事例を拡充）**。

主な掲載事例

ヒアリング調査

- トヨタ自動車　：サプライチェーンにおけるソフトウェア使用状況把握
- ソニー　：各事業部による主体性のある取組
- オリンパス　：ヒヤリ・ハット事象を契機とした全社的取組
- 日立製作所　：製品化の過程における徹底したOSS管理
- オムロン　：PSIRTの連携を通じたOSS対応
- 東芝　：グループにおける一貫したOSS対応体制
- デンソー　：サプライチェーン全体における最適なOSS管理
- 富士通　：部門横断のOSS対応体制と全社統一的なソフトウェア管理
- NEC　：事業部毎の取組から全社的取組へ
- NTT　：OSSサポートに係る適切な役割分担
- 損害保険ジャパン　：ソフトウェア部品構成表を活用した脆弱性管理
- Visionalグループ　：自社状況に対して最適なツールの利用
- サイボウズ　：OSSエコシステムに貢献するOSSポリシー

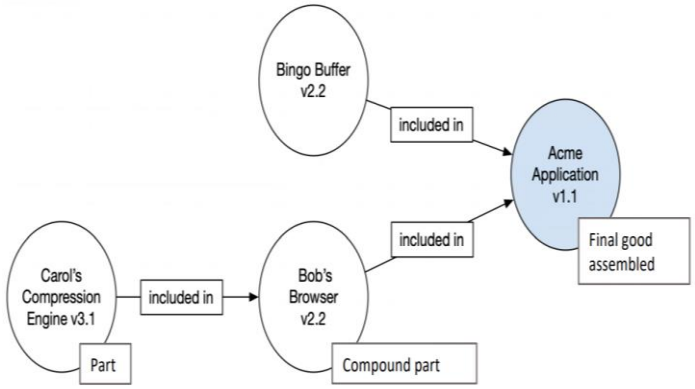
文献調査

- マイクロソフト　：OSSに係るセキュリティリスク緩和策
- ザランド　：OSSプロジェクトの全社的な推進
- Linux FoundationとハーバードによるCensus Ⅱプロジェクトの予備的レポート
  ：アプリケーションに最も利用されているFOSSコンポーネントに関する調査

ソフトウェアタスクフォースの検討の方向性（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**各部品（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るため、脆弱性情報の即時の特定が可能であり、**脆弱性対応などへの活用が期待**できる一方、その作成効果やコストなどの課題が存在するため、実証による検証を実施。
- 2021年5月に発令された米・大統領令においてもSBOM提供について言及されており、今後、政府調達要件として整備が進むものと想定。

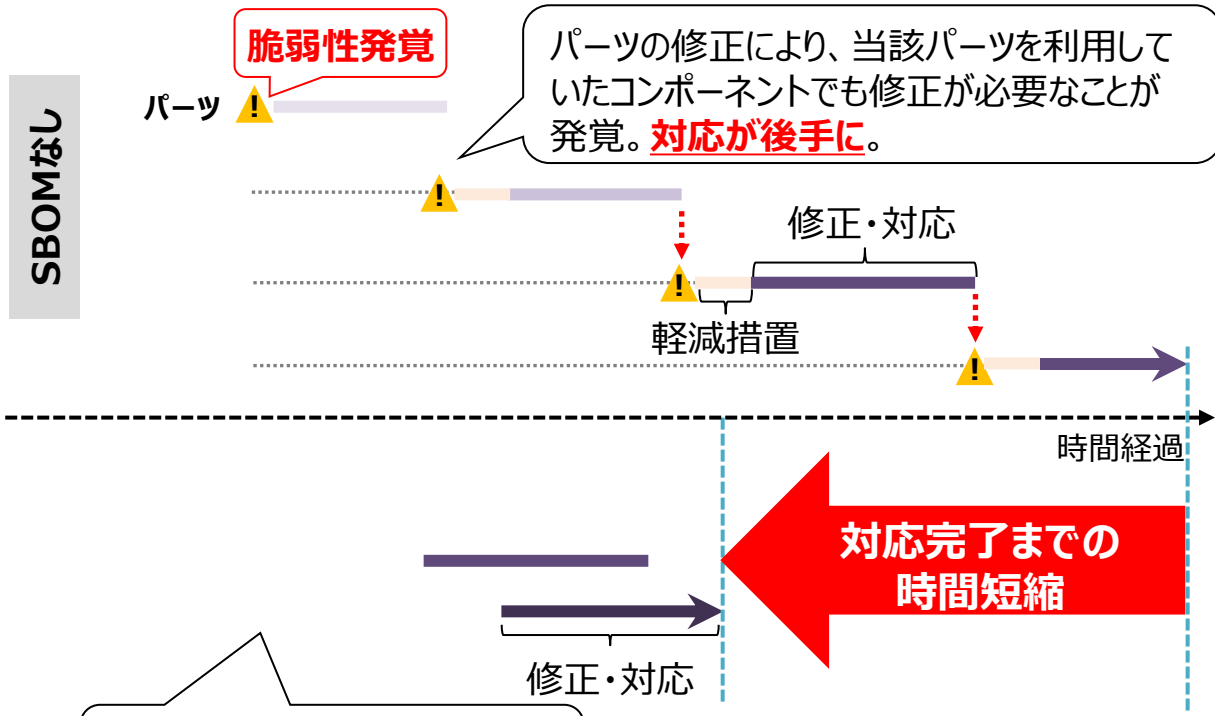
SBOMの構成イメージ



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

SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮



2022年度の実証内容・体制

- SBOMに関して**「規制や推奨化が見込まれる分野」**や**「効果が大きいと思われる分野」を候補**に、実証参加企業の選定、実証内容を設計。
- **実証結果や民間で進められているSBOM活用の取組について、知見等を共有し、実際の活用方法を検討**。

経済産業省

事業委託先

- 実証の対象分野／組織の選定
- SBOMの効果に係る評価の観点、項目の整理
  - 調達時のリスク評価（脆弱性、ライセンス、サポート期間、ベンダー評価）
  - 運用時の脆弱性対応（脆弱性および影響の特定～対応の時間短縮、特定漏れの低減等）
  - 資産管理（システムや機器の更新判断、計画）
  - 供給者管理（契約書における責任分界点等の規定）
- SBOM活用モデルの選択肢の整理
- 参加者の知見共有の仕組み（定期的な会議開催等）の検討
- これまでの調査、検討結果や、国内外の動向等の共有

自動車業界
（OEM/部品サプライヤー等）

医療機器業界
（医療機器メーカー等）

SBOMに関する規制や推奨化が見込まれる分野

知見を共有

ソフトウェア業界
（ITベンダーとそのサプライチェーン等）

SBOMの効果が大きいと思われる分野

- 規制等において定められる**SBOMへの要求事項を満たしつつ、効率的にSBOMを作成、活用していくモデル**（作成者、作成／共有方法、最低限含むべき項目やフォーマット等）を検討。
- 米国NTIAにおける既存のPoCについて得られる情報を確認、活用。

- 社内システム及び顧客向け**システム／サービスを多く管理**し、**SBOMを多様なサプライヤーやユーザーと共有**し、**メリットを最大限享受できる活用モデル**の検討。
- 開発環境や構成管理ツール等との連携など、ツール環境に関する知見や課題の整理。

ソフトウェア管理に向けたSBOMの導入に関する手引き

2023年7月28日、経済産業省は「ソフトウェア管理に向けたSBOM(Software Bill of Materials)の導入に関する手引」を策定。

経済産業省
Ministry of Economy, Trade and Industry

申請・お問合せ | English | サイトマップ | 本文へ | 文字サイズ変更 小 中 大 | アクセシビリティ閲覧支援ツール

ニュースリリース | 会見・談話 | 審議会・研究会 | 統計 | 政策について | 経済産業省について

ホーム ▶ ニュースリリース ▶ ニュースリリースアーカイブ ▶ 2023年度7月一覧 ▶ 「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引」を策定しました

印刷

「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引」を策定しました

2023年7月28日

▶ 安全・安心

【2023年7月28日発表資料差し替え】「ソフトウェア管理に向けたSBOMの導入に関する手引きVer１.０」に関して、ページ番号の記載がなかったため追記しました。

経済産業省は、ソフトウェアサプライチェーンが複雑化する中で、急激に脅威が増しているソフトウェアのセキュリティを確保するための管理手法の一つとして「SBOM」（ソフトウェア部品表）に着目し、企業による利活用を推進するための検討を進めてきました。今般、主にソフトウェアサプライヤー向けに、SBOMを導入するメリットや実際に導入するにあたって認識・実施すべきポイントをまとめた手引書を策定しましたのでお知らせします。

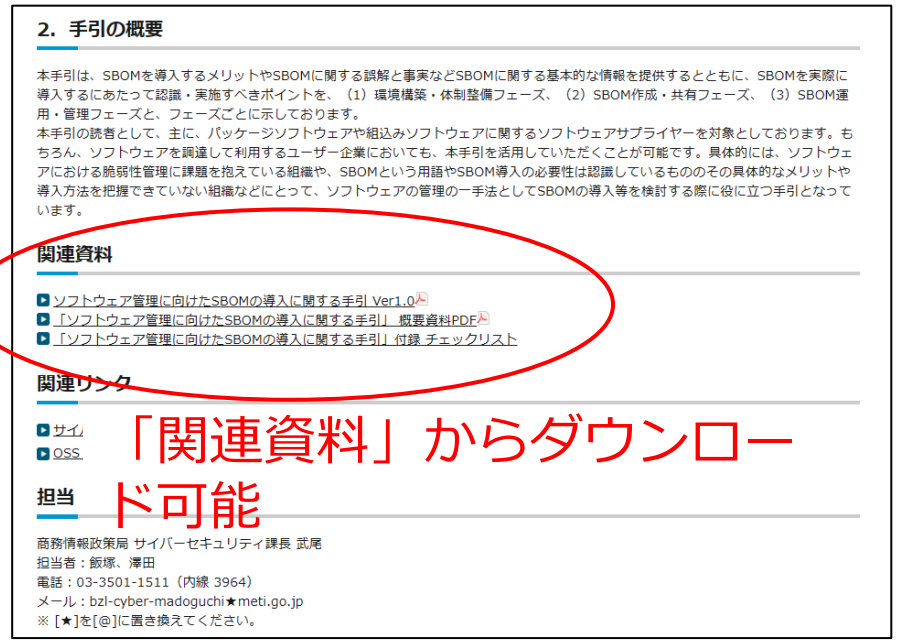
本手引の普及により企業におけるSBOMの導入が進むことで、ソフトウェアの脆弱性への対応に係る初動期間の短縮や管理コストの低減など、ソフトウェアの適切な管理が可能となり、企業における開発生産性が向上するだけでなく、産業界におけるサイバーセキュリティ能力の向上に繋がることが期待されます。

1. 背景・趣旨

近年、産業活動のサービス化に伴い、産業に占めるソフトウェアの重要性は高まっています。具体的には、産業機械や自動車等の制御にもソフトウェアの導入が進んでおり、また、IoT機器・サービスや5G技術においても、汎用的な機器でハードウェア・システムを構築した上で、ソフトウェアにより多様な機能を持たせることで、様々な付加価値を創出していくことが期待されているなど、企業においてOSSを含むソフトウェアの利用が広がっております。

このようにサイバー空間とフィジカル空間の融合が進む一方で、ソフトウェアの脆弱性が企業経営に大きな影響を及ぼすなど、ソフトウェアに対するセキュリティ脅威が増大しています。このため、自社のセキュリティを強化するためにソフトウェアを適切に管理していくことが重要になりますが、ソフトウェアサプライチェーンが複雑化し、OSSの利用が一般化する中で、自社製品において利用するソフトウェアであっても、コンポーネントとしてどのようなソフトウェアが含まれているのかを把握することが困難な状況という課題があります。

このようなソフトウェアの脆弱性管理に関し、ソフトウェアの開発組織と利用組織双方の課題を解決する一手法として、「ソフトウェア部品表」とも呼ばれるSBOM（Software Bill of Materials）を用いた管理手法が注目されています。米国では大統領令に基づき、連邦政府機関におけるSBOMを含めた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に向けた動きが進展しています。QUAD（日米豪印戦略対話）では、政府調達ソフトウェアのセキュリティ確保に向け、ソフトウェアの安全な開発・調達・運用に関する方針を示した共同原則が



2. 手引の概要

本手引は、SBOMを導入するメリットやSBOMに関する誤解と事実などSBOMに関する基本的な情報を提供するとともに、SBOMを実際に導入するにあたって認識・実施すべきポイントを、（1）環境構築・体制整備フェーズ、（2）SBOM作成・共有フェーズ、（3）SBOM運用・管理フェーズと、フェーズごとに示しております。

本手引の読者として、主に、パッケージソフトウェアや組込みソフトウェアに関するソフトウェアサプライヤーを対象としております。もちろん、ソフトウェアを調達して利用するユーザー企業においても、本手引を活用していただくことが可能です。具体的には、ソフトウェアにおける脆弱性管理に課題を抱えている組織や、SBOMという用語やSBOM導入の必要性は認識しているもののその具体的なメリットや導入方法を把握できていない組織などにとって、ソフトウェアの管理の一手法としてSBOMの導入等を検討する際に役に立つ手引となっています。

関連資料

- ソフトウェア管理に向けたSBOMの導入に関する手引 Ver1.0
- 「ソフトウェア管理に向けたSBOMの導入に関する手引」 概要資料PDF
- 「ソフトウェア管理に向けたSBOMの導入に関する手引」 付録 チェックリスト

関連リンク

- サイ
- OSS

「関連資料」からダウンロード可能

担当

商務情報政策局 サイバーセキュリティ課長 武尾
担当者：飯塚、澤田
電話：03-3501-1511（内線 3964）
メール：bzl-cyber-madoguchi★meti.go.jp
※ [★]を[@]に置き換えてください。

「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引」（2023年7月、経済産業省）：

https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引　～全体概要～

手引の背景・目的

- ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が一般化する中で、ソフトウェアにおける脆弱性管理やライセンス管理の重要性が高まっている。
- ソフトウェア管理の一手法として、Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目を集めている。
- 複数の産業分野における実証を通じ、SBOMを活用することで効率的なソフトウェア管理を実施できることが確認できた一方で、実際のSBOM導入に際しては様々なハードルが存在することが明らかとなった。
- 本手引では、**SBOMに関する基本的な情報やSBOMに関する誤解と事実を提供**するとともに、企業のSBOM導入を支援するために、**SBOM導入に向けた主な実施事項及び導入にあたって認識しておくべきポイント**を示す。

対象読者

- 主に、パッケージソフトウェアや組込みソフトウェアに関するソフトウェアサプライヤー※
  - ✓ ソフトウェア開発・設計部門
  - ✓ 製品セキュリティ担当部門（PSIRTなど）
  - ✓ 経営層
  - ✓ 法務・知財部門

※ このうち、以下に示すようなSBOM初級者を特に対象としている。

- ソフトウェアにおける脆弱性管理に課題を抱えている組織
- SBOMという用語は聞いたことがあるが具体的な内容やメリットは把握できていない組織
- SBOMの必要性は理解しているが、導入に向けた取組内容が認識できていない組織　など

SBOM導入の主なメリット

- **脆弱性管理のメリット**
  - ✓ 脆弱性残留リスクの低減
  - ✓ 脆弱性対応期間の低減
  - ✓ 脆弱性管理にかかるコストの低減
- **ライセンス管理のメリット**
  - ✓ ライセンス違反リスクの低減
  - ✓ ライセンス管理にかかるコストの低減
- **開発生産性向上のメリット**
  - ✓ 開発遅延の防止
  - ✓ 開発にかかるコストの低減
  - ✓ 開発期間の短縮

SBOM導入に向けたプロセス

フェーズ1　環境構築・体制整備フェーズ

- **1-1. SBOM適用範囲の明確化**
  - ✓ SBOMを作成する対象ソフトウェアに関する情報（言語、開発ツール、構成図、契約形態・取引慣行、規制要求事項、SBOM導入に関する組織内の制約等）を整理する。
  - ✓ 整理した情報を踏まえて、SBOM適用範囲を明確化する。
- **1-2. SBOMツールの選定**
  - ✓ SBOMツールの選定の観点を整理し、当該観点に基づきSBOMツールを評価・選定する。
    （選定観点の例：機能、性能、解析可能な情報・データ形式、コスト、対応フォーマット、解析方法、サポート体制、他ツールとの連携、ユーザーインタフェース、対応する言語、日本語対応等）
- **1-3. SBOMツールの導入・設定**
  - ✓ SBOMツールが導入可能な環境の要件を確認し、整備する。
  - ✓ 取扱説明書等を確認して、SBOMツールの導入・設定を行う。
- **1-4. SBOMツールに関する学習**
  - ✓ 取扱説明書等を確認して、SBOMツールの使い方を習得する。
  - ✓ ツールの使い方に関するノウハウや各機能の概要は記録し、組織内で共有する。

フェーズ2　SBOM作成・共有フェーズ

- **2-1. コンポーネントの解析**
  - ✓ SBOMツールを用いて対象ソフトウェアのスキャンを行い、コンポーネントの情報を解析するとともに、コンポーネントの解析結果について、コンポーネントの誤検出や検出漏れが無いかを確認する。
  - ✓ SBOMツールを用いることで、手動の場合と比較して効率的にコンポーネントの解析及びSBOMの作成を行うことができる。
  - ✓ パッケージマネージャーを用いることで、SBOMツールでは特定できない粒度の細かいコンポーネントを特定できる場合がある。
- **2-2. SBOMの作成**
  - ✓ 作成するSBOMの項目、フォーマット、出力ファイル形式等のSBOMに関する要件を決定し、当該要件を満足するSBOMを作成する。
- **2-3. SBOMの共有**
  - ✓ 対象ソフトウェアの利用者及びサプライヤーに対するSBOMの共有方法を検討した上で、当該方法に基づきSBOMを共有する。

フェーズ3　SBOM運用・管理フェーズ

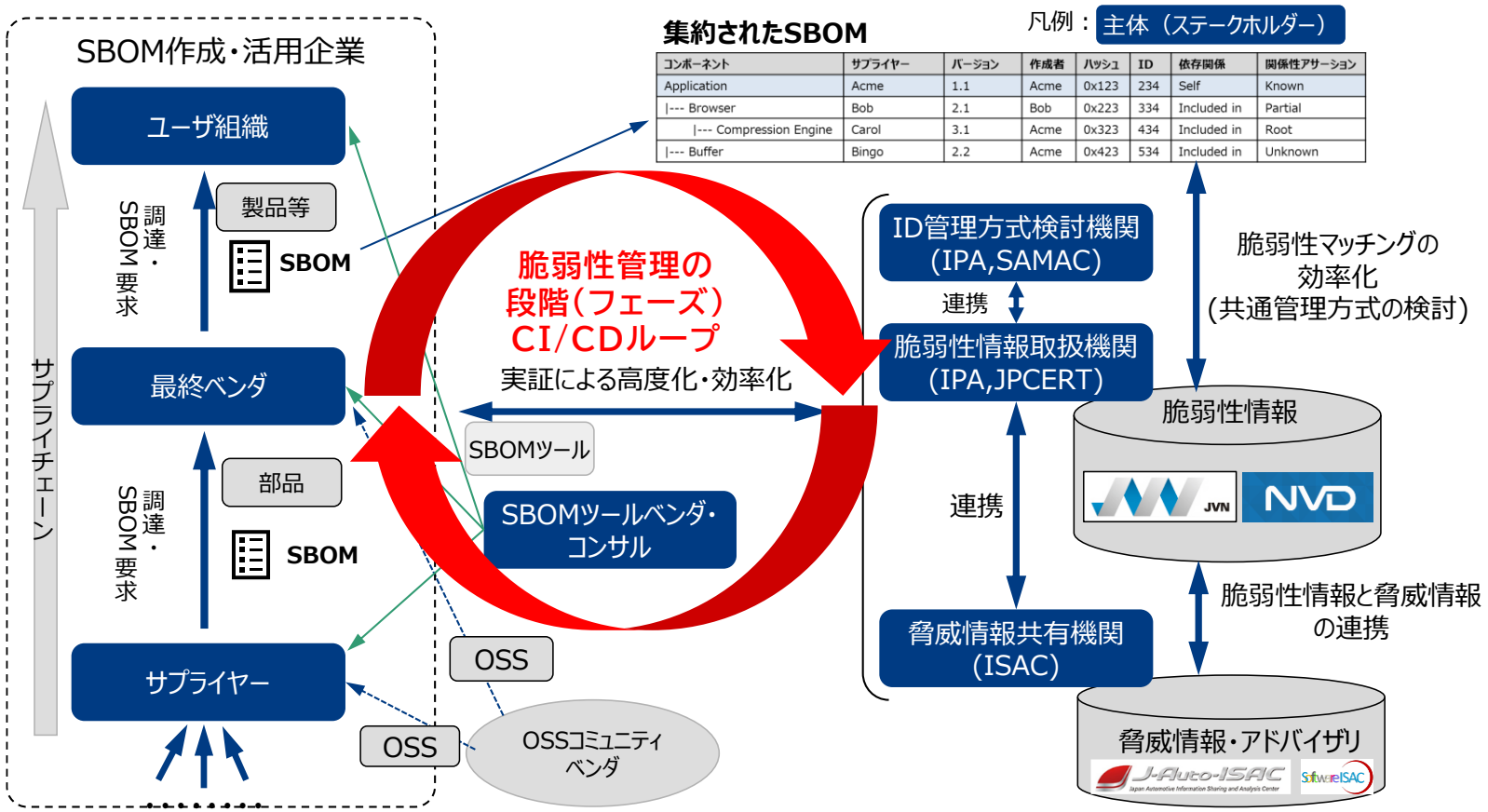
- **3-1. SBOMに基づく脆弱性管理、ライセンス管理等の実施**
  - ✓ 脆弱性に関するSBOMツールの出力結果を踏まえ、深刻度の評価、影響度の評価、脆弱性の修正、残存リスクの確認、関係機関への情報提供等の脆弱性対応を行う。
  - ✓ ライセンスに関するSBOMツールの出力結果を踏まえ、OSSのライセンス違反が発生していないかを確認する。
- **3-2. SBOM情報の管理**
  - ✓ SBOMに含まれる情報やSBOM自体を適切に管理する。
    ※ SBOMの管理は、組織内のPSIRTに相当する部門が対応することが効果的
  - ✓ 自動で脆弱性情報が更新・通知されるSBOMツールを用いることで、新たな脆弱性に関する情報を即座に把握することができる。ツールを用いた自動管理ができない場合、担当者を別途設置するなど運用面でカバーする。

2023年度SBOM実証の全体像： SBOMを活用した脆弱性管理の効率化

実証の目的（ポイント）

- 脆弱性管理プロセスを俯瞰し、SBOMを活用した脆弱性管理の効率的な方法について検討し、その効果評価、課題の整理を行う。**脆弱性情報の提供に係る機関（IPA, ISAC等）と連携**し、脆弱性情報を効率的に取得する方法を検討する。
- SBOMを活用した脆弱性管理を広く普及させるため、**中小企業を含む多くの企業が活用**できるように、脆弱性の深刻度、脅威、アドバイザリなども活用するための方策等について整理する。

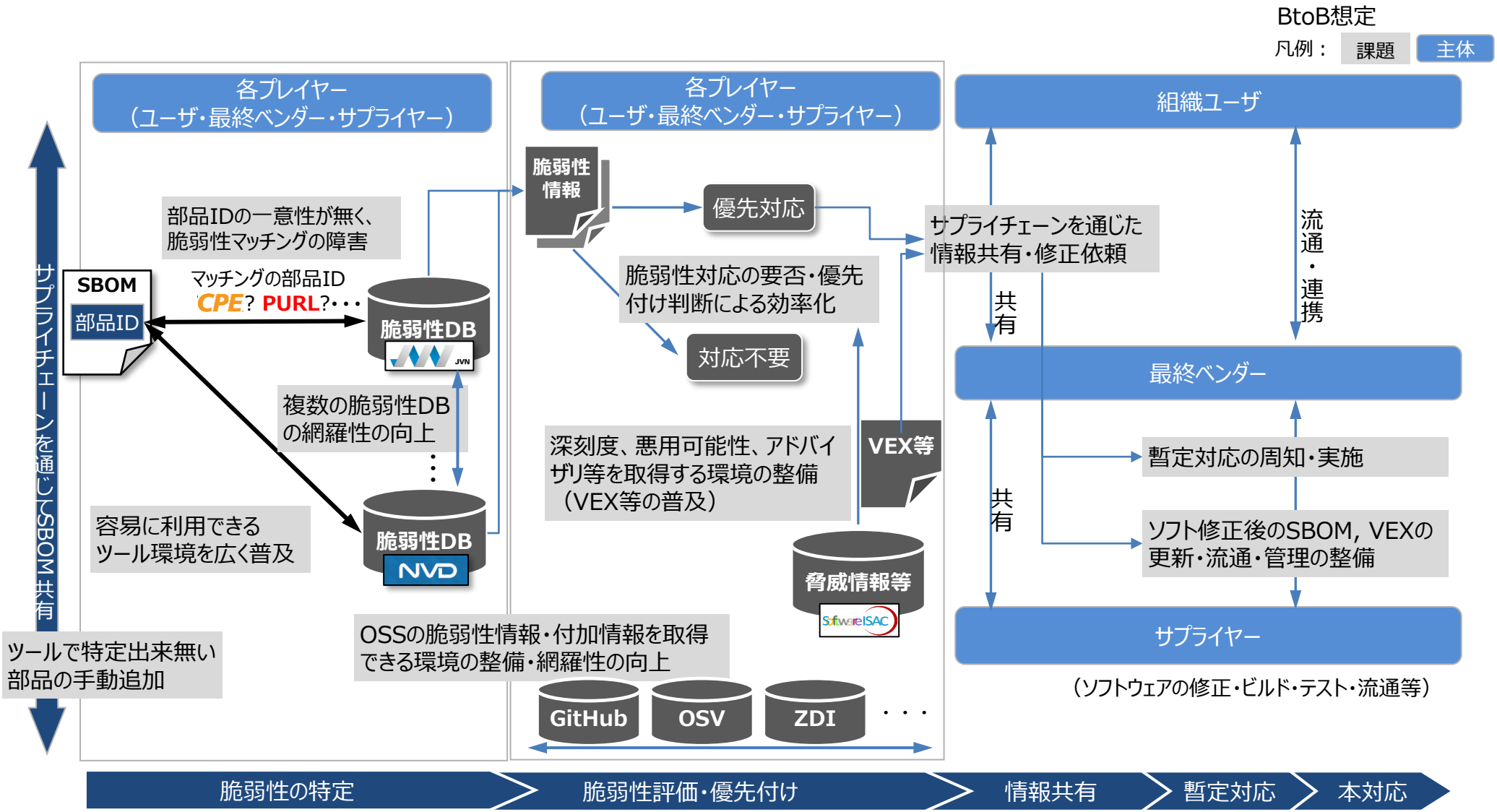
脆弱性管理の主なステークホルダとプロセスの全体像



コンポーネント	サプライヤー	バージョン	作成者	ハッシュ	ID	依存関係	関係性アサーション
Application	Acme	1.1	Acme	0x123	234	Self	Known
|--- Browser	Bob	2.1	Bob	0x223	334	Included in	Partial
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in	Root
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in	Unknown

SBOMを活用した脆弱性管理における課題（俯瞰図）

- SBOMを活用した脆弱性管理の効率化・普及促進に向けて、各プレイヤー、ユーザなどにおいて様々な対応が必要であり、特に脆弱管理プロセス（脆弱性の特定、脆弱性評価等、情報共有、対応）における課題が存在。



日米豪印（Quad（クアッド））第５回首脳会合について

- **5月20日（土）、第５回日米豪印（通称「Quad（クアッド）」）首脳会合を広島で対面開催。**
  第１回：2021年３月（オンライン）、第２回：同９月（米国）、第３回：ウクライナに関する臨時会合 2022年3月（オンライン）、第４回：同5月（日本）
- 岸田総理大臣からは、ASEANや南アジア、太平洋島嶼国といった地域の国々の声に耳を傾けながら、**「善を推進する力」として、地域に真に裨益する実践的協力を展開していく重要性**を強調。
- また会合後、**４カ国は共同声明を発出**。当省関連では、**重要・新興技術、気候、サイバーセキュリティ、インフラ、宇宙等での新たな協力を進めること**が記載された。その他、海洋安全保障、海洋状況把握、国際保健等での新たな協力が記載された。
- **来年の首脳会合は、インドで開催**することで一致した。

サイバーセキュリティ

- 地域のサイバー人材の能力向上支援を継続、サイバーセキュリティの啓発を目的とした**「日米豪印サイバー・チャレンジ」**の実施を歓迎。
- ソフトウェアの開発、利用、政府調達に係るセキュリティ向上を奨励する**「ソフトウェア・セキュリティに関する日米豪印共同原則」**及び**「重要インフラのサイバーセキュリティに関する日米豪印共同原則」**の発表を歓迎。

外務省HP：https://www.mofa.go.jp/mofaj/fp/nsp/page1_001702.html

日米豪印（Quad（クアッド））第５回首脳会合の成果

【首脳共同声明（仮訳） 抜粋】

- 我々は、より安全なサイバー空間と、全ての人々のためになる国際デジタル経済を促進することへのコミットメントを再確認する。日米豪印パートナーは、**サイバー事案及び脅威への地域の能力及び強靱性を高める**ため、引き続き協働する。
- 我々は、**サイバーに対する意識を高め、インド太平洋の参加者がオンライン上で自身を保護することを支援**するため、本年実施した初めての**日米豪印サイバー・チャレンジ**を歓迎する。
- また、**「ソフトウェア・セキュリティに関する日米豪印共同原則」**及び**「重要インフラのサイバーセキュリティに関する日米豪印共同原則」**並びにサプライチェーン・セキュリティと強靱性を確保するための指針となる枠組みを開発するための取組を歓迎する。
- これらの原則は、**ソフトウェア・サプライチェーンや重要インフラ及びサービスへのサイバー脅威に対する地域の防御を強化する**ために設計されている。

【ソフトウェア共通原則（概要）】

- 日米豪印上級サイバーグループは、政府のためのソフトウェアの開発、調達及び利用の指針となる最低限のサイバーセキュリティ・ガイドラインを構築することにより、ソフトウェア・セキュリティを共同で向上するとの我々のコミットメントを再確認する。

- 日米豪印は、以下のハイレベルの安全なソフトウェア**開発**慣行を追求し、既存の政府の政策にそれらを採り入れ、これらの慣行を満たすソフトウェアを取得し、ソフトウェア開発者/サプライヤにそれらの実施を奨励するとの意図を有する。

1. **組織の準備**：人々が適切に訓練され、プロセスが定義され、安全なソフトウェア開発を実行するためのテクノロジーソリューションが導入されていることを確認する。
2. **ソフトウェアおよびソフトウェア開発環境の保護**：ソフトウェアの全てのコンポーネントを改ざんおよび不正アクセスから保護し、各ソフトウェアリリースをアーカイブ化し保護し、各リリースで使用されるさまざまなコンポーネントの詳細**（例：ソフトウェア部品表（SBOM））**及びサプライチェーン関係の十分な記録を維持する。
3. **十分に安全が確保されたソフトウェアの作成**：：リリース時のセキュリティの脆弱性が最小限の、十分にセキュリティで保護され、テスト済みのソフトウェアを作成する。
4. **脆弱性への対応**：：継続的にそれらの脆弱性に対処し将来の同様の脆弱性の発生を防止するために、ソフトウェアリリースの脆弱性を特定し適切に対応する。

- 日米豪印は、ソフトウェア又はソフトウェアを含む製品の**政府調達**に関して、以下の最低限のガイドラインを追求する意図を有する。各国は、国際的義務、国内法、規制、及びそれぞれのサイバー空間の成熟度と整合的に、以下の慣行を奨励することにより、国内でガイドラインの実施を追求する意図を有する。

1. **ソフトウェアの開発が安全なソフトウェア開発慣行に準拠していることを示す第三者認証**が提供されない限り、**ソフトウェア開発者による自己申告を要求**する。
2. ソフトウェア開発者に対し、報告と開示のプロセスを含む各国の**脆弱性開示プログラムに報告するよう奨励**する。

- 日米豪印は、政府によるソフトウェアの**利用**のために以下のセキュリティ対策を追求する意図を有する。

1. ソフトウェア及びソフトウェア・プラットフォームを**不正なアクセスおよび利用から保護するための十分な管理およびプロセスを確保**する。
2. ソフトウェア及びソフトウェア・プラットフォームで使用される**データの機密性、完全性、可用性を保護するための十分な管理およびプロセスを確保**する。
3. **ソフトウェアを不正利用から保護**するため、ソフトウェア・プラットフォームと、それらのプラットフォームに展開されたソフトウェアを特定して維持する。
4. ソフトウェア及びソフトウェア・プラットフォームに関連する**インシデントを迅速に検出、対応し、回復**する。
5. ソフトウェア及びソフトウェアプラットフォームのセキュリティを促進する**人間の行動の理解及び遂行を強化**する。

外務省HP：https://www.mofa.go.jp/mofaj/fp/nsp/page1_001702.html

１．諸外国の動向

２．サイバー・フィジカル・セキュリティ対策フレームワークとその具体化

２．１　IoTセキュリティ関連

２．２　ソフトウェアセキュリティ関連

２．３　OTセキュリティ関連

２．４　データセキュリティ関連

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4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。
- 2022年11月16日にガイドラインを公表。
  https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

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

第４回　パブコメ意見を踏まえ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
市岡 裕嗣	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

Panasonic Cyber Security Team　7

工場(制御システム)のセキュリティ課題

- 長期運用と可用性重視のため、ITシステム同等の対応が困難
  ⇒ 脆弱な状態が前提と考え、侵入されることを前提とした対策が必要
- 制御システムの物理症状からサイバー攻撃の特定は困難
  ⇒ 迅速な対策・復旧には専門家によるサイバー空間での監視が不可欠

問題点	ITシステム（OA用PC）	制御システム（製造システム）	
機器・システムのライフサイクル	3-5年	10年以上	・長期運用 ・OSサポート終了後も稼働
サポート切れOS・ソフトの使用	禁止	禁止できない	・誤動作の可能性あり ・ベンダの保証対象外となる
ウィルス検査ソフト導入	導入必須	導入不可	・誤動作の可能性あり ・専用装置は導入方法無し
セキュリティパッチ適用	適用必須	適用不可	・誤動作の可能性あり ・設備メーカ保証外

JSIA　JEITA 一般社団法人 電子情報技術産業協会 半導体部会

③各社における工場セキュリティを取り巻く課題（1）

➢ 各社ともさまざまな課題を抱えている

- 製造装置は、導入時のシステムのまま使われることが多く、バージョンアップなどセキュリティ対策が実質できない。
- セキュリティ対策ソフトは、装置動作の保証ができないとの装置ベンダーからの回答があり、導入が困難。そのため直接的な保護、検疫ができない。
- 製造装置の保守時に装置や関係するベンダーによるコンピュータウィルスの持ち込みリスクがある。
- 製造装置の修理のためハードディスクなどの記憶媒体を修理に出した際、コンピュータウィルスの混入リスクがある。
- リモート診断・支援などが進む場合、社外からのアクセスに伴うセキュリティ対策をユーザー単独として対策することに限度がある。また、様々なツール、方式が乱立することにより、対応がより複雑になる。
- 導入したセキュリティソリューションにより工場システムへ予期しない影響が発生することがある。
- Cloudベースのセキュリティソリューションでは、自社でコントロールできない問題が発生して、工場のオペレーションに影響を及ぼす。
- 新たな技術/デバイスの登場に対するセキュリティ対策が追い付かない（IoT、Cloud、Mobile etc）。

第2回 産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化） 工場サブワーキンググループ　資料4-2,4-4より抜粋
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/002.html

工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

ガイドラインの背景・目的

- 工場の**IoT化やクラウド活用によるネットワーク接続機会の増加**に伴いサイバー攻撃リスクが増加。また、ネットワークの接続が少ない工場であっても不正侵入者等による攻撃の可能性あり。
- 意図的な攻撃の場合もあれば、たまたま攻撃される場合もある。

→**いかなる工場でもサイバー攻撃のリスクあり**。

- 本ガイドは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示した「手引き」**。

→**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、**工場のセキュリティの底上げを図ることが目的**。

想定する読者の方

- ITシステム部門
- 生産関係部門（生産技術部門、生産管理部門、工作部門等）
- 戦略マネジメント部門（経営企画等）
- 監査部門
- **機器システム提供ベンダ、機器メーカ**
  （サプライチェーンを構成する調達先を含む）

※想定読者が経営層（CTO、CIO、CISO）をはじめとした意思決定層と適切なコミュニケーションを行うことが重要。
※事務系の情報システム（IT）は対象外。

対策に取り組む効果

- **工場のBC／SQDC※の価値がサイバー攻撃により毀損されることを防止**。
- **経営目標(事業伸長、継続の観点等)**との連関
- セキュリティが担保されることで**IoT化や自動化が進み、多くの工場から新たな付加価値**が生み出されていくことを期待。

※ 安全確保(S：Safety)、
事業／生産継続(BC：Business Continuity)
品質確保(Q：Quality)
納期遵守・遅延防止(D：Delivery)
コスト低減(C：Cost)

セキュリティ対策企画・導入の進め方

ステップ 1　内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**
  セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2**　業務の整理
- **ステップ1-3**　業務の重要度の設定
- **ステップ1-4**　保護対象の整理
- **ステップ1-5**　保護対象の重要度の設定
- **ステップ1-6**　**ゾーン**の整理とその業務、保護対象の結びつけ
  （生産管理・監視、制御系、自動搬送、自動倉庫、リモートメンテナンス等）
- **ステップ1-7**　ゾーンと、セキュリティ脅威の影響の整理
  （俯瞰化、別ゾーンへの影響の抑止、被害の抑制）

ステップ 2　セキュリティ対策の立案

- **ステップ2-1**　セキュリティ対策方針の策定
- **ステップ2-2**　**(高・中・最低限)**
  想定脅威に対するセキュリティ対策の対応づけ

(1)システム構成面での対策
① ネットワークにおけるセキュリティ対策
② 機器におけるセキュリティ対策
③ 業務プログラム・利用サービスにおけるセキュリティ対策

(2)物理面での対策
① 建屋にかかわる対策
② 電源／電気設備にかかわる対策
③ 環境(空調など)にかかわる対策
④ 水道設備にかかわる対策
⑤ 機器にかかわる対策
⑥ 物理アクセス制御にかかわる対策

ステップ 3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  サプライチェーンを考慮した対策

(1)ライフサイクルでの対策
① 運用・管理面のセキュリティ対策
A) サイバー攻撃の早期認識と対処
（OODAプロセス）
B) セキュリティ対策管理(ID/PW管理、機器の設定変更など)
C) 情報共有

②維持・改善面のセキュリティ対策
・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
・組織・人材のスキル向上（教育、模擬訓練等）

(2) サプライチェーン対策
・取引先や調達先に対するセキュリティ対策の要請、対策状況の確認

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

１．諸外国の動向

２．サイバー・フィジカル・セキュリティ対策フレームワークとその具体化

２．１　IoTセキュリティ関連

２．２　ソフトウェアセキュリティ関連

２．３　OTセキュリティ関連

２．４　データセキュリティ関連

『第3層TF』の検討の方向性

- 本タスクフォースにおいて、データの信頼性確保のために、「**データの区分に応じた適切なセキュリティ対策要件**」及び「**データの信頼性の確認手法**」を検討。

データの区分に応じた適切なセキュリティ対策要件の検討

データをセキュアに管理すること
⇒マネジメント、プロセス、セキュリティポリシー、システム要件等のセキュリティ要件の明確化など

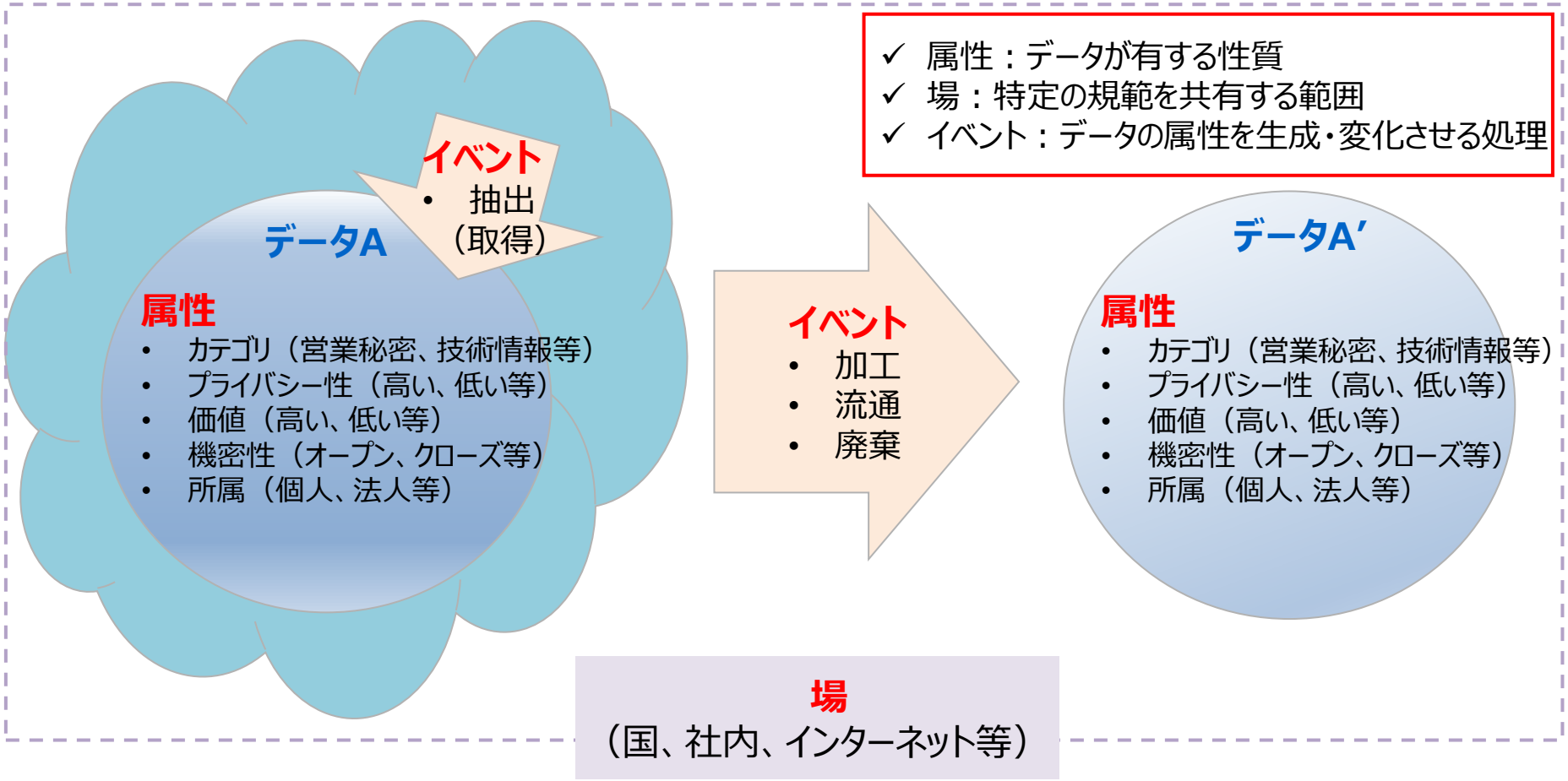
データの信頼性の確認手法の検討

データそのものや生成者の実体の確認
⇒データの真正性確認、モノ等の確認など

データの来歴の確認
⇒トレーサビリティの仕組みの検討など

『第3層TF』データマネジメントの新たな捉え方

- 既存のデータマネジメント等の考え方を参考にしつつ、第1回タスクフォースの議論を踏まえ、**データマネジメント**とは、「**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を踏まえて管理すること**」とここでは捉える。



データマネジメント・フレームワークの概要

- 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。
- **「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」を公開（2022年4月）**。

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。

ユースケース：小売業におけるPOSデータの活用事例

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

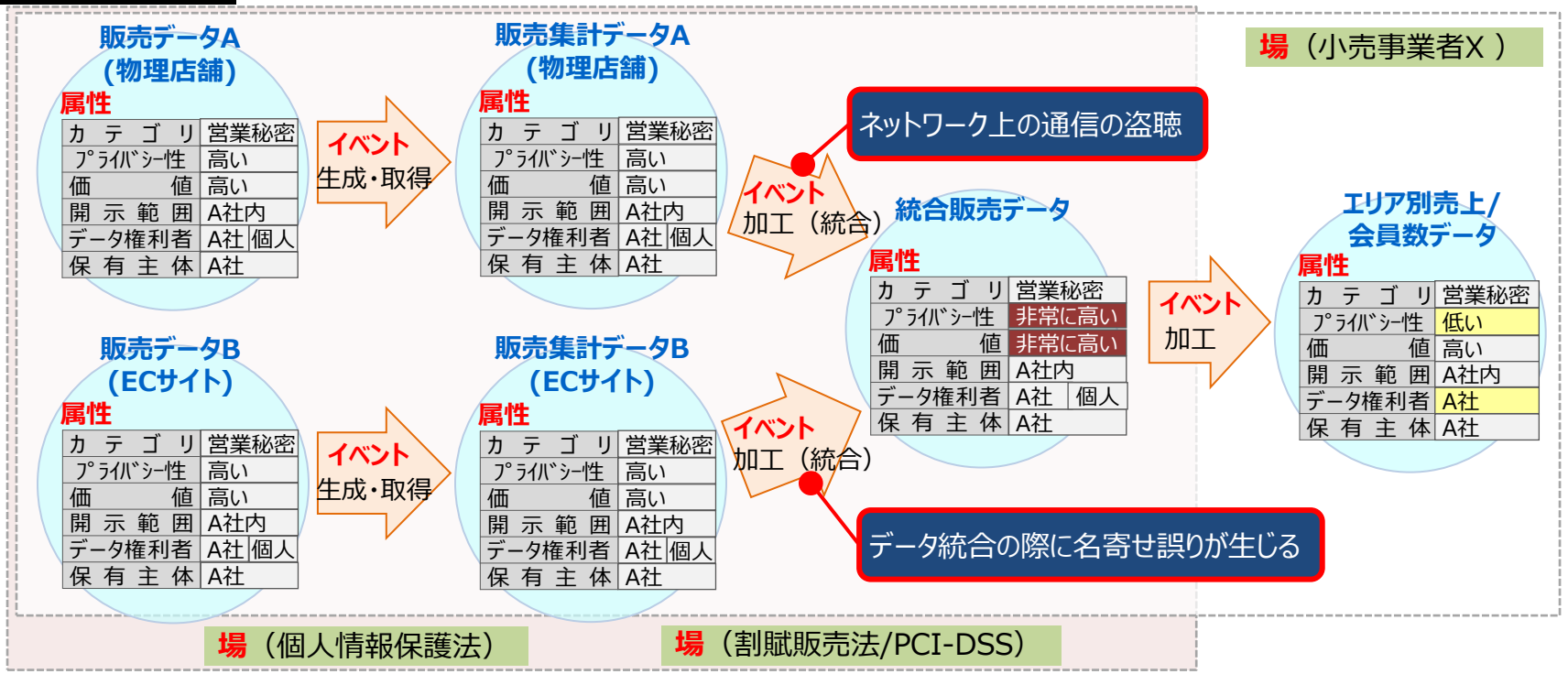
新たな捉え方への当てはめステップ

STEP 1
データ処理フロー(イベント)の可視化

STEP 2
必要な制度的な保護措置(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



- サイバー攻撃は規模や烈度が増大。DXの進展に伴い、IoT機器をはじめとして、攻撃拠点、攻撃の影響範囲が拡大。
- IT/IoT製品等の**製造事業者は、製品・サービスのセキュリティ対策に責任**を持つことが必要に。

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html