経済産業省

SBOMに関する日本及び米国における動向や取組について

経済産業省　商務情報政策局

サイバーセキュリティ課

三田　真史

１．はじめに
～ソフトウェアに関する事例、SBOMに関する国内外の動向・取組等

２．ソフトウェアタスクフォースにおける取組（１）
～OSS管理手法に関する事例集策定

３．ソフトウェアタスクフォースにおける取組（２）
～SBOMの利活用に関する実証

SolarWinds Orion Platformのアップデートを悪用した攻撃

- 2020年12月13日、SolarWinds社は同社のネットワーク監視ソフトウェア「Orion Platform」に、**正規のアップデートを通じてマルウェアが仕込まれた**ことを公表。米政府機関等を含む**最大約18,000組織が影響**を受けたとされる。

Kaseya VSAの脆弱性を利用したサプライチェーンランサムウェア攻撃

- 2021年7月、米国のKaseya社は、同社のリモートIT管理サービス**「Kaseya VSA」をオンプレミスで利用している企業に対するランサムウェア攻撃が発生**していると発表。
- Kaseya VSAはマネージドサービスプロバイダー（MSP）に導入されていることが多く、複数のMSPが攻撃を受けたことで被害範囲が拡大し、**攻撃を受けた可能性のあるユーザー企業は全体で1,500組織と推計**されている。

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

- 2021年12月、Javaベースのオープンソースログ出力ライブラリ**Apache Log4jにおける任意コード実行の脆弱性が発表**。
- この脆弱性を利用することで、**Log4jが動作するアプリケーションに対して外部からの任意コード実行が可能**となり、情報漏えいやマルウェア感染等の被害に繋がる恐れがあり、**脆弱性に対処するよう注意喚起**がなされた。

米国の動向・取組等

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)
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)
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)**
4. サイバー安全審査委員会の創設 (Section 5)
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)
6. 調査及び修復能力の向上 (Section 8)

- 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。

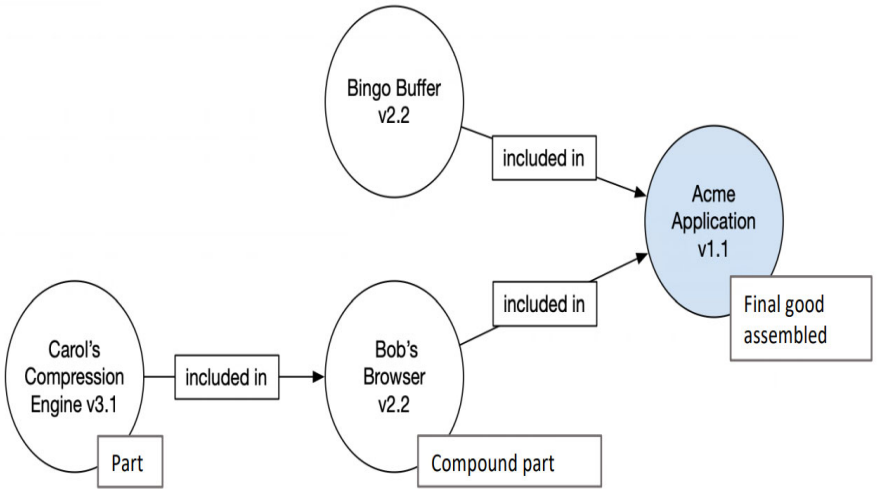
- 大統領令では、**ソフトウェア・サプライチェーンの確保に向け、NISTが中心となりガイドラインを策定する**旨を指示しており、この**ガイドラインには製品購入者に対するSBOM提供に関する項目も含まれる**。
- 将来的には、公開されたソフトウェア・サプライチェーンに関するガイダンスの要求事項に基づき、**連邦政府のソフトウェア調達に関するFAR（連邦調達規則）が改正される予定**である。

（出典）各種公開情報より作成

（参考）SBOMについて

- SBOM （Software Bill of Materials）とは、ソフトウェアの部品構成表のこと。ソフトウェアを構成する各コンポーネントを誰が作り、何が含まれ、どのような構成となっているか、等を示す。
- SBOMによりソフトウェアの構成情報の透明性を高めることで詳細を把握することができ、ライセンス管理や脆弱性対応への活用が期待される。

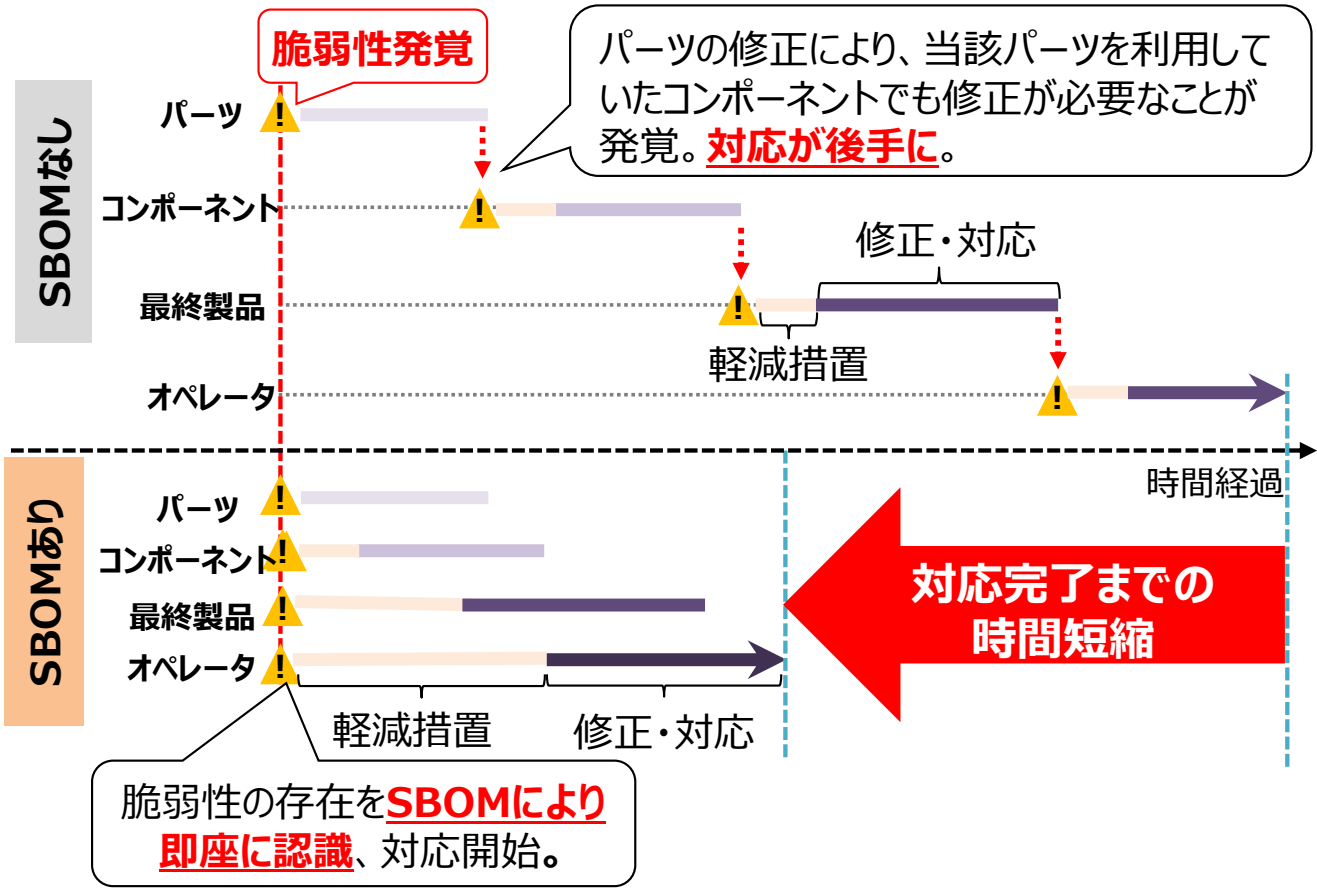
SBOMの構成イメージ



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

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

SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮



（参考）SBOMの「最小要素」の定義

- 大統領令を受け、NTIAは当該定義に関するパブリックコメントを実施。**ソフトウェア関連の企業や専門家からの意見を踏まえ、SBOMの「最小要素」の定義を2021年7月12日に公開**。
- SBOMの「最小要素」には、**「データフィールド」、「自動化サポート」、「プラクティスとプロセス」**の3つのカテゴリが含まれ、**コンポーネントを一覧化した部品表に含まれる情報だけでなく、SBOMの利活用者が実施すべき事項**も規定されている。

3つのカテゴリ	「最小要素」の概要	「最小要素」の具体的な定義
データフィールド（Data Fields）	**各コンポーネントに関する基本情報を明確化すること**	以下の情報をSBOMに含めること。 • 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 • その他の一意な識別子 • 依存関係 • SBOMの作成者 • タイムスタンプ
自動化サポート（Automation Support）	**SBOMの自動生成や可読性などの自動化をサポートすること**	SBOMデータは機械判読可能かつ相互運用可能なフォーマットを用いて作成され、共有されること。現状では、国際的な議論を通じて策定された、SPDX、CycloneDX、SWIDタグを用いること。
プラクティスとプロセス（Practices and Processes）	**SBOMの要求、生成、利用に関する運用方法を定義すること**	SBOMを利活用する組織は、以下の項目に関する運用方法を定めること。 • SBOMの作成頻度 • SBOMの深さ • 既知の未知 • SBOMの共有 • アクセス管理 • 誤りの許容

出所）NTIA, “The Minimum Elements For a Software Bill of Materials (SBOM)”
https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom

【米国】ソフトウェアサプライヤーのためのSBOMプレイブック

- 2021年11月、NTIAはソフトウェアサプライヤーを対象としたSBOM作成に関するプレイブックを公開。
- 本プレイブックでは、**SBOM作成手順、SBOM作成に当たって考慮すべき事項及びSBOMに関する補足事項**についてまとめられている。

ソフトウェアサプライヤーのためのSBOMプレイブックの概要

SBOM作成手順

ソフトウェア開発組織は多様であり、様々なソフトウェアやシステムに対してSBOMを作成することが必要である。

開発組織は様々なツールやプロセスを用いて、SBOMを作成することが可能である。SBOM作成手順は一般的に以下の手順となる。

1. **コンポーネントの特定**
   対象となるソフトウェアに含まれるソフトウェアコンポーネントを特定する。
2. **コンポーネント情報を取得**
   特定したソフトウェアコンポーネントに関する情報を取得する。
3. **SBOM形式への出力**
   コンポーネント情報を、構造化されたSBOM形式へ出力する。
4. **SBOMの検証**
   作成したSBOMフォーマットが有効であるかを検証し、コンポーネントに最低限の属性情報が存在することを確認する。

SBOM作成に当たって考慮すべき事項

- **SBOM作成の自動化**
  ビルド前のソースレベルのSBOMの生成にあたっては、ソフトウェアバージョン管理ツールやCI/CDパイプライン※1などを活用することで、SBOMを自動作成することが可能となる。
- **コンテナイメージに対するSBOMの作成**
  コンテナイメージには、様々なソフトウェアアプリケーションや、様々なレイヤに組み込まれたアーティファクトが含まれる。そのため、全レイヤの全ソフトウェアを特定し、SBOMに記述する必要がある。
- **SBOM作成日時の明確化**
  ビルド後に作成されたSBOMの場合、いつSBOMが作成されたかを明確化するために、SBOMの作成日時に関する情報を含める必要がある。
- **SBOMに含まれる情報の明確化**
  アプリケーションとともに利用者に提供される追加のコンポーネント情報（ダイナミックリンクライブラリ、共有ライブラリ 等）がSBOMに含まれるか、利用者に明示する必要がある。
- **外部サービスの明確化**
  アプリケーションが機能を実行するために、インターネットサービスを呼び出す場合、当該サービスに関する情報を可視化する必要がある。ただし、これは検討段階であるため、SBOMの最小要素としては含まれていない。

SBOMに関する補足事項

- **SBOMの知的財産/機密性**
  SBOM情報は中間サプライヤーを介して最終利用者に提供される必要がある。SBOMの配布を妨げるのではなく、契約上の機密情報としてSBOMを扱うように機密保持体制を構築することが望まれる。
- **SBOMフォーマットの検証**
  SBOMのフォーマットが有効であるか（必要な情報が存在し、構造化されているか）を確認する。活用できるツールの例は以下のとおり。
  ・SPDXOnline Tool: SPDX形式の検証ツール
  ・SWID Tools: SWID形式の検証ツール
  ・CycloneDX CLI Tool、Web Tool: CycloneDX形式のSBOM検証ツール
- **コンポーネント情報の検証**
  SBOMに含まれるコンポーネント情報の確からしさを検証する。活用できるフレームワークの例は以下のとおり。
  ・OWASP SCVS: ソフトウェアコンポーネントの評価や改善方法の参考となるフレームワーク
  ・OpenChain（ISO/IEC 5230:2020）: ソフトウェアコンポーネントの正確な特定と監視に必要となるプロセス管理標準

※1: ソフトウェア配信プロセスにおけるステップの自動化を支援するツール

出所）NTIA, ” Software Suppliers Playbook: SBOM Production and Provision”
https://www.ntia.gov/files/ntia/publications/software_suppliers_sbom_production_and_provision_-_final.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**（SP 800-218）**。
- **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**。

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】SBOMに係る取組の進展

- ヘルスケア分野における実証事業（PoC）のほか、自動車分野・電力分野のSBOMの取組を実施。

ヘルスケア分野 (病院、医療機器)

病院、医療機器メーカー、ベンダーが参加。2回のPoCを経てSBOM活用の手法、課題等を公開。医療機器メーカーにおけるSBOM活用に向けたガイドライン案を公開。2022年のPoCでは、SBOMの自動化やSBOMとVEXとの連携方法について検討するほか、多数の関係者を巻き込んだ場合のより現実的なSBOM共有方法について検討。

自動車産業分野

Auto-ISACを中心としたサプライヤー中心のプロジェクト。自動車産業分野でのSBOMの普及促進を目的として、SBOM活用に関するベストプラクティス文書を策定。

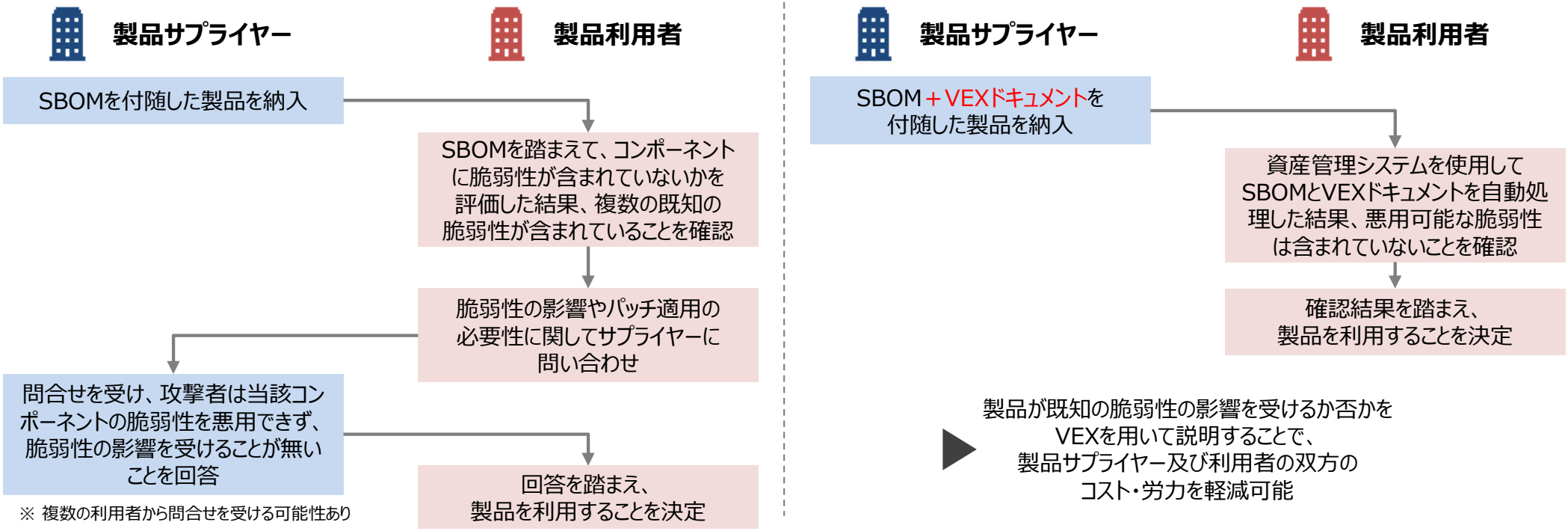
電力分野

INL主導で、電力会社、電力機器ベンダー、ソフトウェアベンダー、電気協会等が参加。米国エネルギー省からもプレゼンターとして参加。2022年のPoCでは、SBOMの作成方法やVEXの活用方法に関して検討。

（参考）VEXとは

- Vulnerability Exploitability eXchange（VEX）とは、**ある製品が既知の脆弱性の影響を受けるかどうかを示す機械判読可能なセキュリティ勧告の一つ**であり、米国NTIAを中心として開発された。
- VEXの主な目的は、製品利用者に対して、**製品が特定の脆弱性の影響を受けるかどうか**、そして**影響を受ける場合に是正するために推奨されるアクションがあるかどうかの追加情報を提供**し、**製品サプライヤー及び利用者の双方のコスト・労力を軽減すること**にある。

VEXを導入することのメリットの例



出所）NTIA, ”Vulnerability Exploitability eXchange(VEX) – An Overview” https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf
NTIA, “Framing Working Group” https://www.ntia.doc.gov/files/ntia/publications/framing_2021-04-29_002.pdf

経済産業省の取組等

産業分野別での具体化 と 分野横断的な検討

- **7つの産業分野別サブワーキンググループ（SWG）**を設置。CPSFに基づくセキュリティ対策の具体化・実装。
- 分野横断の共通課題を検討する、**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(2022.4)

自動車産業SWG
- ガイドライン2.0版の策定(2022.4)

スマートホームSWG
- ガイドライン1.0版の策定(2021.4)

宇宙産業SWG
- ガイドライン1.0版の策定(2022.8)

工場SWG
- ガイドライン1.0版の策定（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」の策定

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事例集の策定**
- ✓ **SBOM活用促進に向けた実証事業（PoC）の実施**

『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)」の策定
- ✓ IoT-SSFをわかりやすく理解するためのユースケースの策定

(参考)「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。

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>

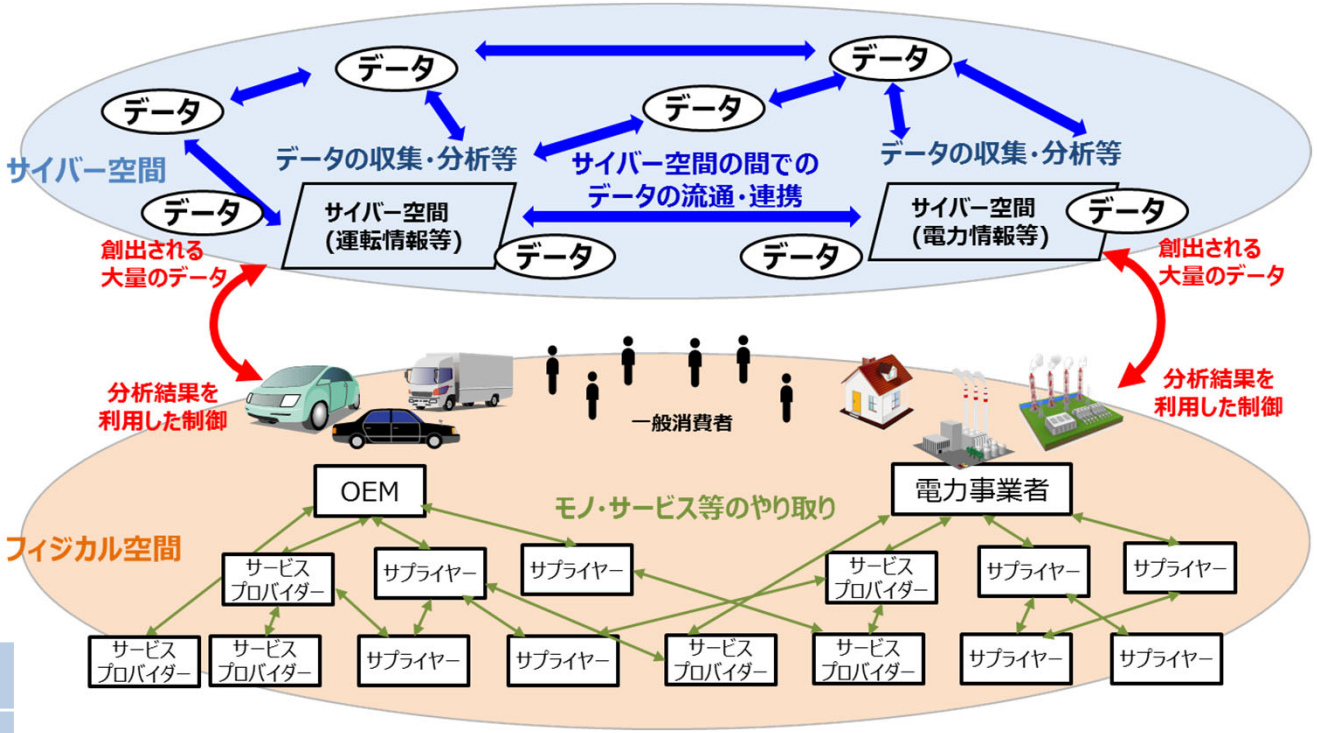
【第３層】
サイバー空間におけるつながり

【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

１．はじめに
　～ソフトウェアに関する事例、SBOMに関する国内外の動向・取組等

２．ソフトウェアタスクフォースにおける取組（１）
　～OSS管理手法に関する事例集策定

３．ソフトウェアタスクフォースにおける取組（２）
　～SBOMの利活用に関する実証

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を利活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

１．はじめに
　～ソフトウェアに関する事例、SBOMに関する国内外の動向・取組等

２．ソフトウェアタスクフォースにおける取組（１）
　～OSS管理手法に関する事例集策定

３．ソフトウェアタスクフォースにおける取組（２）
　～SBOMの利活用に関する実証

SBOM導入・活用に向けた課題

- SBOM活用による効果が想定される一方で、**導入コスト等が障壁となり、活用が進んでいない**。
- **実証事業において、どうSBOMを活用すれば、導入効果が大きくなり、普及に繋がるか**を確認。

- **SBOM導入にかかるコスト**
  - 効果に対してどの程度のコストをかけるべきか判断に必要な情報が少ない。
  - 多数のSBOMを手動で管理するとコストが膨大になるためツールによる自動化が考えられるが、下記のような課題が存在。
    - ツールの導入コスト・ランニングコストが発生。
    - ソフトウェアIDやSBOM形式が統一されていないなど、自動化の障害が存在。

- **SBOM生成・情報開示に対するサプライヤーの強い抵抗感**

2021年度 SBOM実証事業の内容

SBOM作成手段や作成者等の条件を設定して、効果やコストを比較し、今後の検討事項を整理。

比較項目

- **SBOMの効果**
  - 脆弱性管理　　脆弱性特定工数、脆弱性修正までの期間、脆弱性残留リスク等の低減
  - ライセンス管理　　ライセンス特定工数、ライセンス違反残留リスク等の低減
- **SBOMのコスト**
  - 初期コスト　　体制構築、環境整備
  - SBOM作成コスト　　作成工数、作成ツール費用
  - SBOM活用コスト　　部品管理工数（脆弱性の影響特定など）、管理ツール費用

比較条件

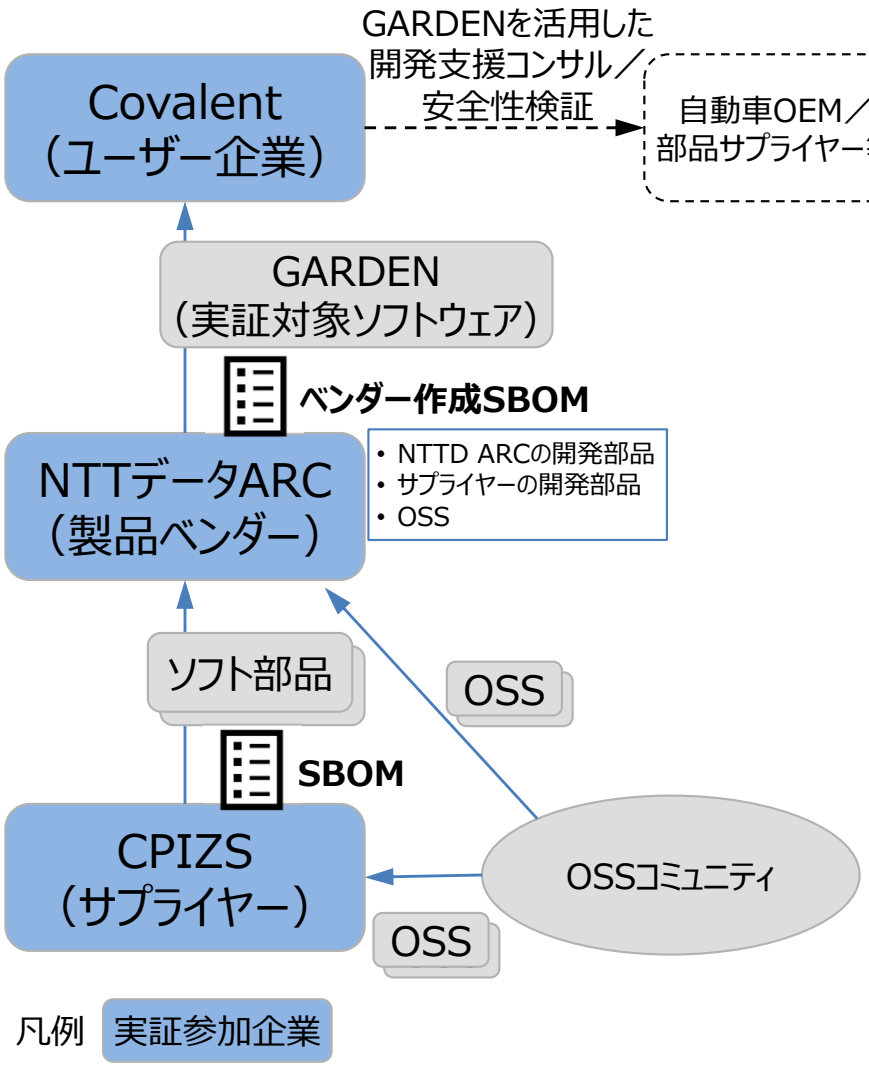
- そもそもソフトウェアの部品管理を行わない場合
- SBOMという形ではないが、何らか部品管理を実施する場合
- SBOMをユーザーが作成する場合
- SBOMをベンダーが作成する場合（手動で行う場合、ツールを利用する場合）

- **実証を通じてSBOMの実際の効果やコストを算出。**
- **国外の取組の進展も踏まえ、SBOMの効果的な活用方法を検討、今後の検討事項を整理。**

SBOM実証のシナリオ、まとめ（2021年度の取組）

- 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。

実証体制（GARDENのサプライチェーン）



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。

（参考）実証における比較条件

- NTTデータARC社が従来から行っていた独自形式の部品管理と、SBOMを使った部品管理について、**SBOM等の作成、脆弱性管理、ライセンス管理の費用・工数を計測**。
- ツールは、SBOM標準への準拠性から、**SPDX projectおよびNTIA Formats and Tooling WGの提供一覧から選出**。中小企業への普及も考慮し、**無償ツールと有償ツール間も比較**。

シナリオ	SBOM等（部品情報）の作成	脆弱性管理	ライセンス管理
①従来の部品管理 (独自形式)	ベンダーおよびサプライヤーが、手作業で、Excel独自形式の「OSS一覧」を作成。	NVD等の脆弱性DBの手動検索や公開情報収集を通じて脆弱性の発生を確認。	Web検索によりライセンス情報を確認。
②SBOM (手動作成)	ベンダーおよびサプライヤーが、SBOM作成ツールのフォーマットに合わせ手作業。	作成したSBOMを、脆弱性管理ツールに入力して脆弱性の有無を特定。 使用ツール：Grype	SBOMを活用したライセンス管理ツールによりライセンス情報を確認。 （他ツールで作成したSBOMファイルが読み込めず、SBOM作成機能も持つツールを用い、ソースコード検索により実施。） 使用ツール：FOSSology
③SBOM (無償ツール)	ベンダーおよびサプライヤーが、部品構成ファイルを無償ツールに読み込ませて作成。 使用ツール：Scancode-Toolkit、Syft、FOSSology		
④SBOM (有償ツール)	有償ツールの機能により、SBOM作成、脆弱性管理、ライセンス管理をシームレスに実施。 ユーザーが、ベンダーから受領したPython仮想環境（ソースコード、部品構成ファイル、実行に必要なOSSを含む）をツールに読み込ませてSBOMを作成。 使用ツール：Black Duck		

※ 本事業では、SBOMの定義は、NTIAの定義「ソフトウェアを構成する部品の詳細情報とサプライチェーンにおける関係を標準的な形式で記録したもの」を採用し、個社独自形式で企業間での共有を前提しない部品情報とは区別。

SPDX project : https://spdx.dev/spdx-tools/
NTIA Formats & Tooling WG : https://ntia.gov/files/ntia/publications/ntia_sbom_tooling_2021-q2-checkpoint.pdf

2021年度の検討結果（まとめ）

- R3年度の実証事業で、ソフトウェアの成分構成を表す**SBOM（Software Bill of Materials）を活用することの有効性は確認**。
- 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
- 一方で、**実際にビジネスで活用するためには課題**も多い。
- 産業分野ごとの状況を踏まえ、「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」等を候補に実証を継続。

1. SBOM活用モデルの最適化

- 産業分野によっては規制等の動きもあるため、**産業分野の状況に応じたSBOMの効果的な活用モデルを整理**。

2. SBOM共有のための環境整備

- 各分野等における標準的な**SBOMの項目、粒度、フォーマット、部品命名規則等の整理**。
- **契約、責任、費用負担**の整理。

3. SBOM自動生成ツールの活用促進による効率化

- SBOMツールの導入や利用方法に係る**情報発信、ノウハウの共有による導入工数の低減**。

4. 国際的な基準との整合性確保

- グローバルサプライチェーンにおいて国内と海外の整合性を確保しつつ効率的に部品管理を行うためには、**国内外の基準の整合化**が必要。

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。

実証の全体構成

- 実証の目的や産業分野ごとの法制度等を考慮し、以下の実施体制等により実証を実施。

● 成果目標

– 産業分野ごとのリスク、法制度に応じて、SBOMを用いた部品のリスク管理を効果的に行うための方法についてコスト・効果の比較評価を行い、現実的な適用範囲と課題について整理する。
– 実証を通じて、初級者向けSBOM導入ガイダンス、SBOMの適用範囲を例示するSBOM対応モデル、取引契約の例示によりSBOM導入を促進するSBOM取引モデルの主な契約事項を整理することを目的とする。
– 法的な要件化が進む医療機器分野、自動車分野および、効果が期待できるソフトウェア分野について、実ソフトウェアに対するサプライチェーンを考慮した体制により、評価を行う。

実施体制等（実証の実施者・関係者及び対象製品など）

分野	関連する業界団体	実証実施企業及び関係企業など					関連法制度（前提となる基準等）	対象製品
		ユーザ	最終ベンダ（製品ベンダ、インテグレータ）	ティア1サプライヤ	ティア2サプライヤ	サードパティサプライヤ		
医療機器	日本医療機器産業連合会	ヒアリング協力：大学附属病院	近畿レントゲン工業（製品ベンダ）	ライフサイエンスコンピューティング		Microsoft, Google等	(厚労省) 医療機器　基本要件基準　一部改正案 JIS T 81001-5-1制定案 医療機器製販業者向けサイバーセキュリティ手引書改訂(案) 医療機関向けサイバーセキュリティ手引書(案) (国際)N60 IMDRFガイダンス N73 IMDRF追補ガイダンス案 (米国) FDA 市販前ガイダンス案	歯科用CT
自動車	（日本自動車工業会）	個人	(トヨタ自動車助言)（製品ベンダ）	東海理化	サニー技研	BROADCOM,OSSベンダ等	(国交省)道路運送車両の保安基準 (国際)UN-R155, 156 (米国)NHTSAガイダンス	自動車ヒーターコントローラ
ソフトウェア	ソフトウェア協会	法人（ヒアリング協力）	トレンドマイクロ、さくらインターネット、コラボスタイル(製品ベンダ、インテグレータ)			Adobe, Amazon, Microsoft等	(米国)NISTサプライチェーンガイダンス, FedRAMP	ネットワーク脅威検知、データセンター、業務フロー管理SaaS

実証で抽出された主な課題と解決策（抜粋）

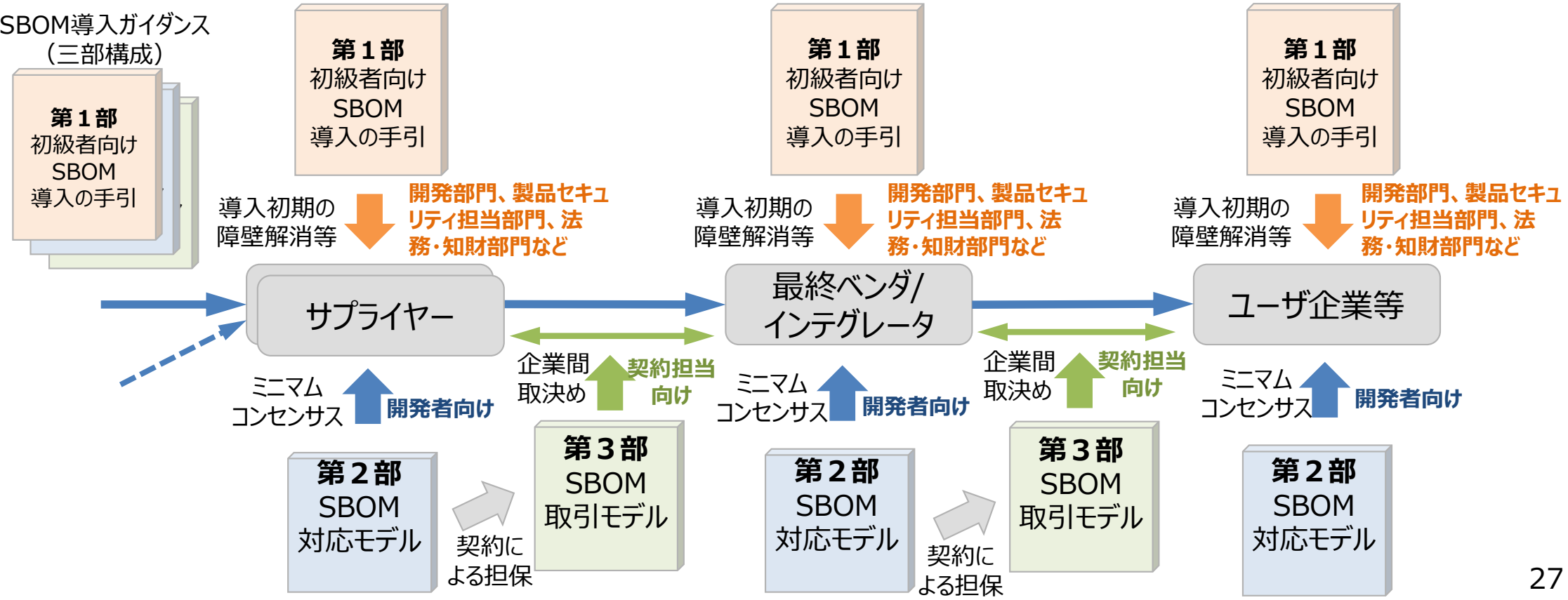
実証で抽出された課題に基づき、解決ノウハウの検討や今後の取組施策の整理。

区分	実証から抽出した課題	解決ノウハウ （導入ガイダンスに反映予定）	今後の課題 （国、民間）	医療機器	自動車	ソフト
技術	検出した脆弱性の対応要否、優先度の判断が困難	医療機器分野の脆弱性対応フローなどを参考にアドバイザリ、脅威情報を活用し、対応の要否、優先度を判断。	脆弱性管理の高度化、脅威情報の普及促進	●		
	SBOMツールの使い分け・変更による負担増大	機能ニーズを洗い出し、ツール比較情報をもとに選択	—	●	●	●
	CI/CDなど継続的なアップデートへの対応負担	ツールによる自動化可能な範囲で管理	CI/CDに対応した自動管理			●
	SBOM初期導入、ツール等のコスト負担が大きい	ツールの効率的な導入方法、OSSツールの選択活用	OSSベースのツール整備	●	●	●
管理	SBOMに要求される精査のレベルが不明確	SBOM対応モデルの選択肢やSBOMツールの機能に応じて精査の要否を判断する。	—	●	●	
	SBOM生成の対象範囲が不明確	OS,MWを含めて対象全体の上位構成を事前に明確化	—	●	●	●
	ツールの環境構築、SBOM共有のコストが大きい	SaaS型SBOMツールで初期導入と共有の工数を低減	サプライチェーンを通じた脆弱性管理	●	●	●
	ユーザ組織によるSBOMの活用・管理が困難	SBOMツール導入、ベンダ支援の活用	—	●	●	●
	部品の脆弱性残存期間に応じたリスク評価	SBOMの履歴管理により脆弱性残存期間を特定	脆弱性の履歴評価			●
	開発部署、PSIRTなど部署ごとの脆弱性管理が非効率	社内でSBOMを一元管理することで、脆弱性管理を効率化	SBOMによる脆弱性の社内一元管理		●	●
	サプライヤごとの部品粒度のバラつき	取得したすべての粒度をツールで自動管理	脆弱性マッチングの高度化		●	
	サプライヤのサポート切れなどのリスク対応	部品のEOL等に基づくサポート計画・管理を実施	—	●		
取引	サードパーティからのSBOM取得が困難、バイナリ納品物の脆弱性の監視・修正が負担	ソースコード取得とSBOMツールの適用、（バイナリ納品の場合）SBOM提供と脆弱性修正を契約で要件化	—	●	●	●
	サプライヤ部品の精査コストが大きい	SBOMの提供と信頼性に関する責任を契約で規定	—	●	●	

本実証結果等を踏まえた検討について

- 本実証結果等を踏まえ、導入の手引、対応モデル、取引モデルから構成されるSBOMに関するガイダンス（SBOM導入ガイダンス）を作成予定。
- 初級者向けSBOM導入の手引→ 対応モデル → 取引モデル を順次活用し、サプライチェーンにおける信頼を確保。

SBOM導入ガイダンスは、以下の３部から構成予定。
第１部　初級者向けSBOM導入の手引：導入初期の課題、阻害要因を解消するための開発者向けのヒント・TIPS等。
　　効率的な適用方法。（実証の成果やNTIA SBOM Playbook等の関連する内容を盛り込む）
第２部　対応モデル：業界として期待される開発者向けのSBOM対応レベル（ミニマム・コンセンサス）。
第３部　取引モデル：対応モデルを契約でどのように担保するか契約担当向けの例示。要件・責任関係の明確化



実証で抽出された主な課題と解決策（抜粋）（再掲）

実証で抽出された課題に基づき、解決ノウハウの検討や今後の取組施策の整理。

区分	実証から抽出した課題	解決ノウハウ （導入ガイダンスに反映予定）	今後の課題 （国、民間）	医療機器	自動車	ソフト
技術	検出した脆弱性の対応要否、優先度の判断が困難	医療機器分野の脆弱性対応フローなどを参考にアドバイザリ、脅威情報を活用し、対応の要否、優先度を判断。	脆弱性管理の高度化、脅威情報の普及促進	●		
	SBOMツールの使い分け・変更による負担増大	機能ニーズを洗い出し、ツール比較情報をもとに選択	—	●	●	●
	CI/CDなど継続的なアップデートへの対応負担	ツールによる自動化可能な範囲で管理	CI/CDに対応した自動管理			●
	SBOM初期導入、ツール等のコスト負担が大きい	ツールの効率的な導入方法、OSSツールの選択活用	OSSベースのツール整備	●	●	●
管理	SBOMに要求される精査のレベルが不明確	SBOM対応モデルの選択肢やSBOMツールの機能に応じて精査の要否を判断する。	—	●	●	
	SBOM生成の対象範囲が不明確	OS,MWを含めて対象全体の上位構成を事前に明確化	—	●	●	●
	ツールの環境構築、SBOM共有のコストが大きい	SaaS型SBOMツールで初期導入と共有の工数を低減	サプライチェーンを通じた脆弱性管理	●	●	●
	ユーザ組織によるSBOMの活用・管理が困難	SBOMツール導入、ベンダ支援の活用	—	●	●	●
	部品の脆弱性残存期間に応じたリスク評価	SBOMの履歴管理により脆弱性残存期間を特定	脆弱性の履歴評価			●
	開発部署、PSIRTなど部署ごとの脆弱性管理が非効率	社内でSBOMを一元管理することで、脆弱性管理を効率化	SBOMによる脆弱性の社内一元管理		●	●
	サプライヤごとの部品粒度のバラつき	取得したすべての粒度をツールで自動管理	脆弱性マッチングの高度化		●	
	サプライヤのサポート切れなどのリスク対応	部品のEOL等に基づくサポート計画・管理を実施	—	●		
取引	サードパーティからのSBOM取得が困難、バイナリ納品物の脆弱性の監視・修正が負担	ソースコード取得とSBOMツールの適用、（バイナリ納品の場合）SBOM提供と脆弱性修正を契約で要件化	今後の課題として脆弱性管理・マッチングに係るものが多い	●	●	●
	サプライヤ部品の精査コストが大きい	SBOMの提供と信頼性に関する責任を契約で規定		●	●	

サイバーセキュリティに関する米国国土安全保障省（DHS）との大臣級MOC

- **2023年1月6日、マヨルカス国土安全保障長官と西村経産大臣が会談**し、人権タスクフォースへの協力を確認するとともに、**サイバーセキュリティに関するMOCに署名**。
- 今回のMOCでは、①「国家安全保障戦略」の改定を踏まえた経済産業省と国土安全保障省との協力関係の深化、②「開かれたインド太平洋（FOIP）」の実現に向けたインド太平洋における能力構築、③サイバーセキュリティ制度調和の促進、の実現を目指す。

【MOC概要】

経済産業省と米国国土安全保障省は、高度化し増加し続けるサイバー攻撃への対応のため、関係機関からの協力も得ながら、以下のサイバーセキュリティ分野について協力を行う。

＜協力分野＞

- 運用面での協力
- 制御システムセキュリティの向上
- インド太平洋地域等の能力向上に関する協力
- サイバーセキュリティ関連規制及びスキームの調和のための対話促進

＜MOC改定のねらい＞

①「国家安全保障戦略」改定を踏まえた経済産業省とDHSとの協力深化

②「FOIP」実現に向けたインド太平洋地域での能力構築

③制度調和の促進

＜今回のMOCにおいて追加された協力分野＞

・インド太平洋地域等の能力向上

・日米間のサイバーセキュリティ関連規制・制度の調和に向けた対話
（SBOMやIoT機器ラベリング制度等の調和を想定）

https://www.meti.go.jp/press/2022/01/20230110002/20230110002.html

QUADにおける取組

- 2022年5月、QUAD首脳会合にて、「日米豪印サイバーセキュリティ・パートナーシップ」を立上げ。

「日米豪印サイバーセキュリティ・パートナーシップ」共同原則

- 重要インフラのサイバーセキュリティ
- サプライチェーンリスクのマネジメント
- **ソフトウェア・セキュリティ**
- 人材育成発展の強化　　の分野で協力。

ソフトウェア・セキュリティについては、以下の協力を行う。

- ベースライン・セキュリティ標準の国内・国際的な実施及び継続的な整合化
- 政府調達におけるソフトウェア・セキュリティに係る枠組みの整合的な開発

- サイバー攻撃は規模や烈度が増大。DXの進展に伴い、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