経済産業省

SBOMに関する国内外の最新動向および日本の取組について

経済産業省　商務情報政策局

サイバーセキュリティ課

飯塚　智

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。

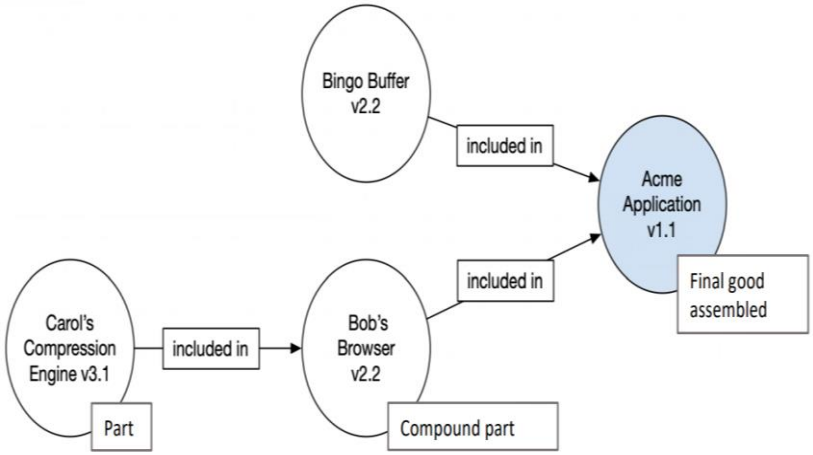
- 大統領令では、**ソフトウェア・サプライチェーンの確保に向け、NISTが中心となりガイドラインを策定する**旨を指示しており、この**ガイドラインには製品購入者に対するSBOM提供に関する項目も含まれる**。
- 将来的には、公開されたソフトウェア・サプライチェーンに関するガイダンスの要求事項に基づき、**連邦政府のソフトウェア調達に関するFAR（連邦調達規則）が改正される予定**である。

（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。

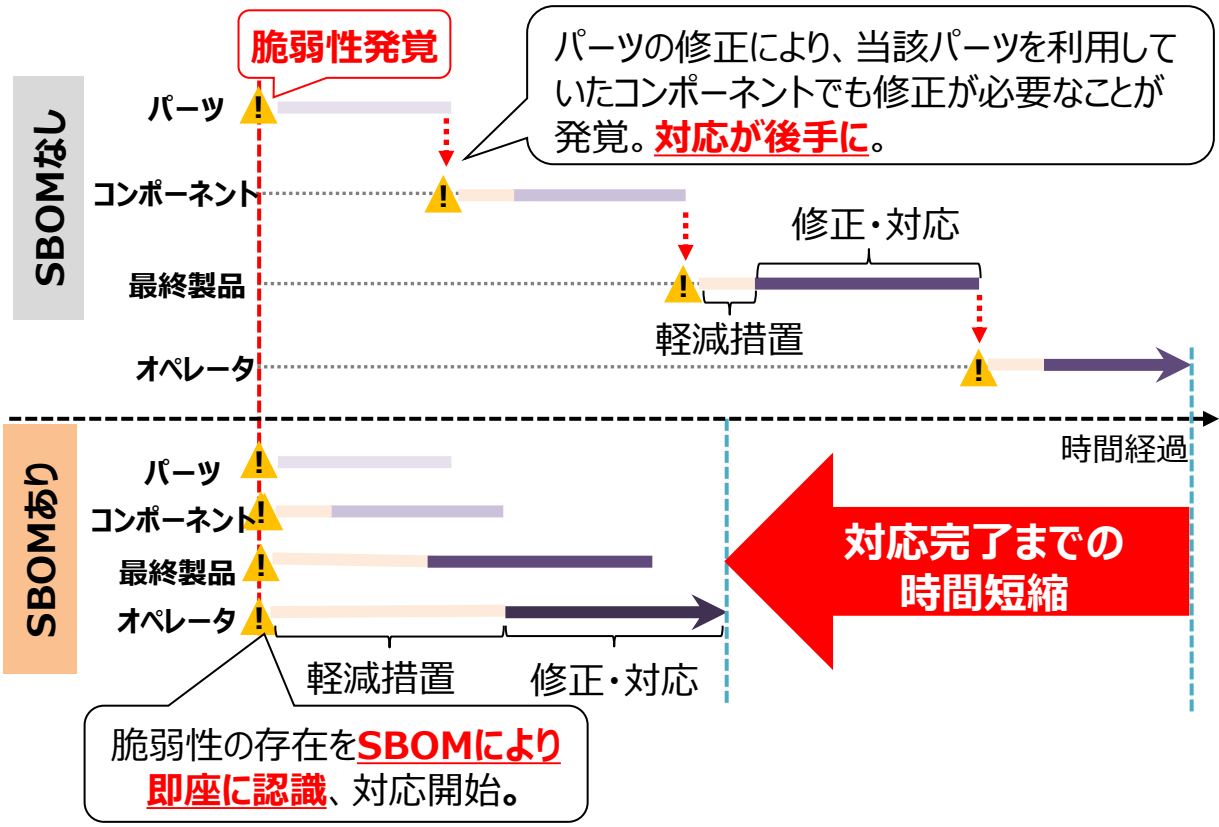
SBOMの構成イメージ



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】SSDF実装の適合性を証明するための共通フォームに関する草案の公開

- CISAは、OMB覚書（M-22-18）を受け、2023年4月、**連邦政府機関が調達するソフトウェアに対して、ソフトウェアベンダーがSSDF（Secure Software Development Framework）の実装の適合性を証明するための共通フォーム案を公開**し、**パブリックコメントを開始**した。（2023年6月26日まで）
- 本案では、**自己適合証明書フォームの対象となるソフトウェア、フォームの提出方法、提出免除、フォームの具体的な記載事項等が示されている**。

案の概要

対象ソフトウェア	以下のソフトウェアは、自己適合証明書フォームの提出が求められる。 • 2022年9月14日以降に開発されたソフトウェア • 2022年9月14日以降にメジャーバージョンアップにより変更される既存のソフトウェア • ソフトウェアベンダーがソフトウェアコードを継続的に変更し、配信するソフトウェア（例：SaaS製品） 以下のソフトウェアは**対象外**であり、自己適合証明書フォームは不要である。 • 連邦政府機関によって開発されたソフトウェア • 連邦政府機関が**直接、自由に入手できるソフトウェア**（例：フリーウェア、OSS）
自己適合証明書フォームの提出方法	以下のいずれかで自己適合証明書フォームを提出することができる。 • オンラインフォームによる提出 • 自己適合証明書（PDFファイル）を添付したメール送信による提出
提出されない場合における連邦政府機関の対処	自己適合証明書フォームを取得できず、ソフトウェアを使用する場合、連邦政府機関は以下の事項を実施しなければならない。 • ソフトウェアベンダーから自己適合証明書フォームを取得できない旨を特定する文書を取得 • ソフトウェアベンダーから自己適合証明書フォームを**取得できないことによって生じるリスクを軽減するため、連邦政府機関が実施している事項をまとめた文書**を作成 • ソフトウェアベンダーに対して、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）の作成を要求
自己適合証明フォームの提出免除	対象ソフトウェアが、**FedRAMP制度において認定された第三者評価機関**又は適切な認定機関が認定した第三者評価機関によって、**関連するNISTガイダンスに基づき評価**された場合、ソフトウェアベンダーは自己適合証明書フォームを提出する必要はない。 ただし、対象ソフトウェアを評価した第三者評価機関が作成した関連文書の提出は必要である。
自己適合証明書フォームにおける記載概要	セクション1：対象ソフトウェアに関連する情報 セクション2：ソフトウェアベンダーに関連する情報 セクション3：SSDF適合の宣誓、添付文書（提出免除のための関連文書を含む）に関する情報

出所）CISA, ”Request for Comment on Secure Software Self-Attestation Common Form”
https://www.cisa.gov/secure-software-attestation-form

【米国】VEXドキュメントの最小要件に関する文書の発表

- 2023年4月、CISAは、**Vulnerability Exploitability eXchange（VEX）ドキュメントの最小要件を示した文書**を公開した。
- 本文書では、VEXドキュメントを構成する項目と各項目に含まれる要素が示され、それぞれにおける**必須項目・必須要件が定義**されている。文書では、**必須要件をVEXドキュメントの最小要件と位置づけ**ている。

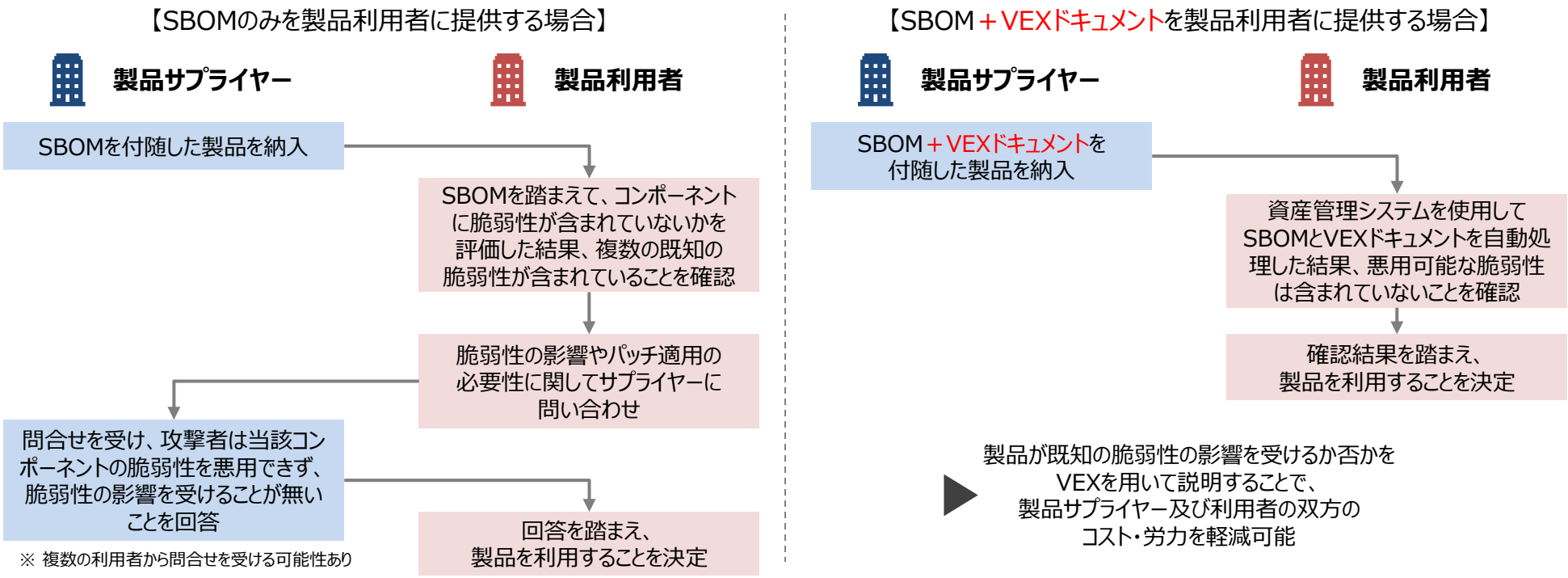
VEXドキュメントの項目		各項目に含まれる要素（下線は必須要素を意味する）
VEXドキュメントのメタデータ（必須）		• VEXドキュメントの識別子 • VEXドキュメントのバージョン • VEXドキュメントの作成者 • VEXドキュメントの作成者の役割（例：製品ユーザー、ベンダー） • VEXドキュメントの作成ツール • VEXドキュメントの作成時のタイムスタンプ • VEXドキュメントの更新時のタイムスタンプ
VEXのステートメント（1つ以上含めることが必須）	VEXのステートメントのメタデータ	• VEXステートメントの識別子 • VEXステートメントのバージョン • VEXステートメントの作成時のタイムスタンプ • VEXステートメントの更新時のタイムスタンプ
	脆弱性のステータス	• 脆弱性のステータス • ステータスノート（例：ステータスが決定された経緯や補足情報） ✓ 脆弱性の影響を受けない ✓ 脆弱性の影響を受ける ✓ 脆弱性を修正済み ✓ 脆弱性について調査中 • 脆弱性の影響受けない理由（正当化情報がない場合は必須） • 脆弱性の影響受けない理由の記述時のタイムスタンプ • 脆弱性の影響を受けないことの正当化情報（以下のいずれか） ➢ 脆弱性のあるコンポーネントは存在しない ➢ 脆弱性のあるコードは存在しない ➢ 脆弱性のあるコードは実行パスに存在しない ➢ 脆弱性のあるコードは攻撃者に悪用されない ➢ 脆弱性対策が組み込まれている • 脆弱性に対する修正または緩和策 • 脆弱性に対する修正または緩和策の記述時のタイムスタンプ （各ステータスにおいて個別要素が定義されている）
	脆弱性の詳細	• 脆弱性の識別子（例：CVE、その他の既存の識別子） • 脆弱性の説明（例：CVEのURL）
	製品の詳細	• 製品の識別子 • サブコンポーネントの識別子 • 製品、サブコンポーネントのサプライヤー名

出所）CISA, "Minimum Requirements for Vulnerability Exploitability eXchange (VEX)"
https://www.cisa.gov/resources-tools/resources/minimum-requirements-vulnerability-exploitability-exchange-vex

（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

【米国】SBOMに関するイベント“SBOM-a-rama”の開催

- 米国CISAが主催で、**SBOMコミュニティの醸成を目的**として、**第2回“SBOM-a-rama”がハイブリッドで開催**（2023年6月）。合計で30か国900名以上が参加した。
- 本イベントでは、各国のSBOMに関する取組状況、米国の自動車・金融・ヘルスケア分野のSBOMの検討状況、SBOMに関する個別課題の検討WGの状況について発表された。また、SBOMが実装された社会と実装に向けてCISAに求める施策について議論された。
- 各国のSBOMに関する状況の発表の一部として、**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。

“SBOM-a-rama”における発表内容

1. **各国のSBOMに関する状況**
   米国：SSDFの自己適合宣言フォームの状況、FDAにおける医療機器のSBOM対応状況について発表
   欧州：サイバーレジリエンス法の検討状況、サイバーレジリエンス法におけるSBOMに関する要件について発表
   日本：2022年度の実証と今年度の実証予定について発表

2. **米国の産業分野のSBOMの検討状況**
   金融：金融分野におけるSBOMのPoCの実施状況、PoCから見えてきた課題について発表
   ヘルスケア：ヘルスケア分野におけるSBOMのPoCの実施状況、PoCを基に開発したOSSについて発表
   自動車：自動車ISACで実施したSBOMのPoCの実施状況、SBOMツールのワークショップなどの実施したイベントについて発表

3. **SBOMに関する個別課題の検討WG**
   以下のWGにおける活動状況、文書の公表状況、WGへの参加募集について発表：
   VEX検討WG、SBOM共有WG、クラウド・オンラインアプリケーションWG
   SBOMツール・実装WG、SBOM初心者サポートWG

“SBOM-a-rama” において主に議論された課題について

発表・議論内容	発表・議論内容を基に確認された主要な課題（抜粋）
米国のPoC	• **SBOMの品質（SBOMがカバーしている部品の範囲など）** • **SBOMにおけるID付け（脆弱性ID、製品ID等の対応付け）**
SBOMの各種検討WG	• SBOMの適切な共有方法 • **SBOMの品質（SBOMの最小要素の定義やSBOMが発行されたタイミングなど）** • SBOM・VEX連携の実装方法 • SaaS・クラウドにおけるSBOMの在り方・標準 • SBOMの自動化におけるベストプラクティスの作成 • SBOMについての企業間における検討のギャップ
ディスカッション	• 経営層向けのSBOMに関する説明資料の必要性 • PoCにおける成果や各企業のSBOM成功事例の取りまとめ • 検討WGで出た仮説の検証の実施 • **共通的な定義となるSBOMの成熟度モデルやSBOMにおける用語の定義**

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

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>

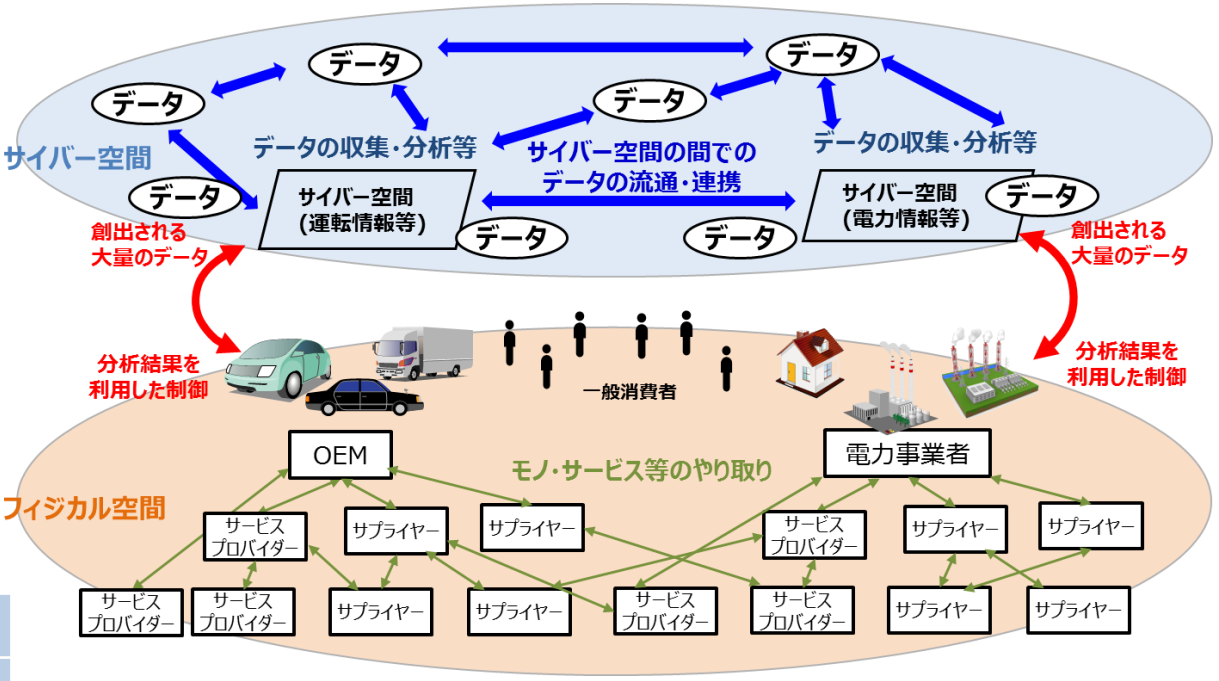
【第３層】
サイバー空間におけるつながり

【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

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

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

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）

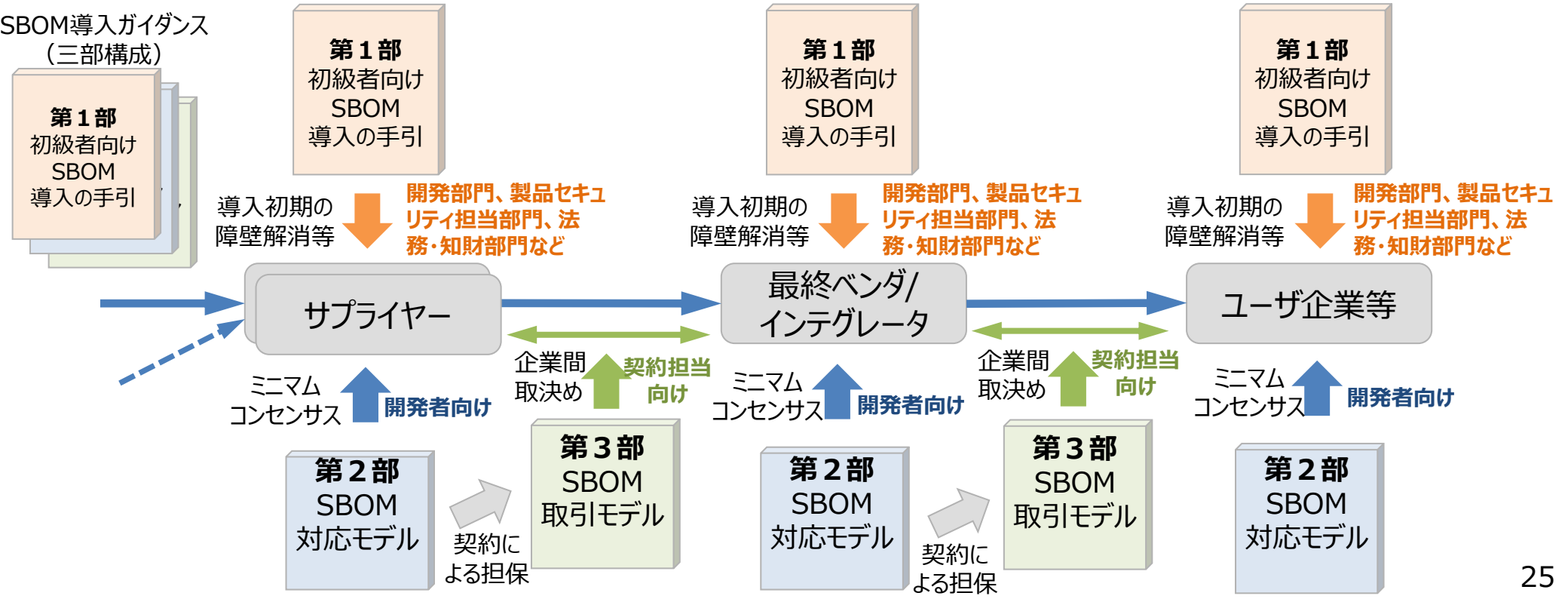
実証で抽出された課題に基づき、解決ノウハウの検討や今後の取組施策の整理。

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



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

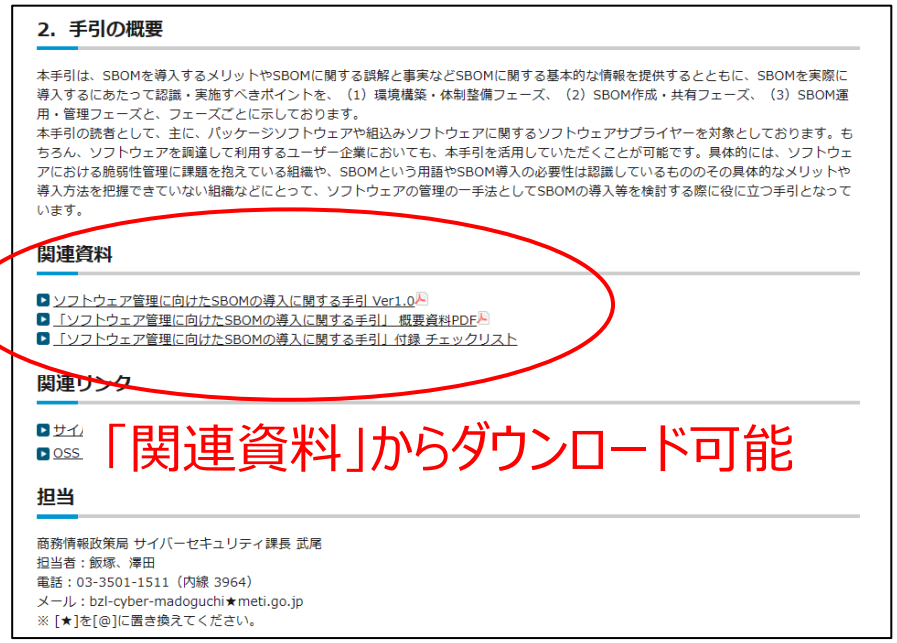
【2023年7月28日発表資料差し替え】「ソフトウェア管理に向けたSBOMの導入に関する手引きVer 1.0」に関して、ページ番号の記載がなかったため追記しました。
経済産業省は、ソフトウェアサプライチェーンが複雑化する中で、急激に脅威が増しているソフトウェアのセキュリティを確保するための管理手法の一つとして「SBOM」（ソフトウェア部品表）に着目し、企業による利活用を推進するための検討を進めてきました。今般、主にソフトウェアサプライヤー向けに、SBOMを導入するメリットや実際に導入するにあたって認識・実施すべきポイントをまとめた手引書を策定しましたのでお知らせします。
本手引の普及により企業における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

- サイバ
- 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

初級者向けSBOM導入手引　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※
  - ✓ ソフトウェア設計部門
  - ✓ ソフトウェア開発部門
  - ✓ 製品セキュリティ担当部門（PSIRTなど）
  - ✓ 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

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ツールの選定基準を整理し、当該基準に基づきSBOMツールを評価・選定する。（選定基準の例：機能、性能、コスト、対応フォーマット、サポート体制、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。

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。

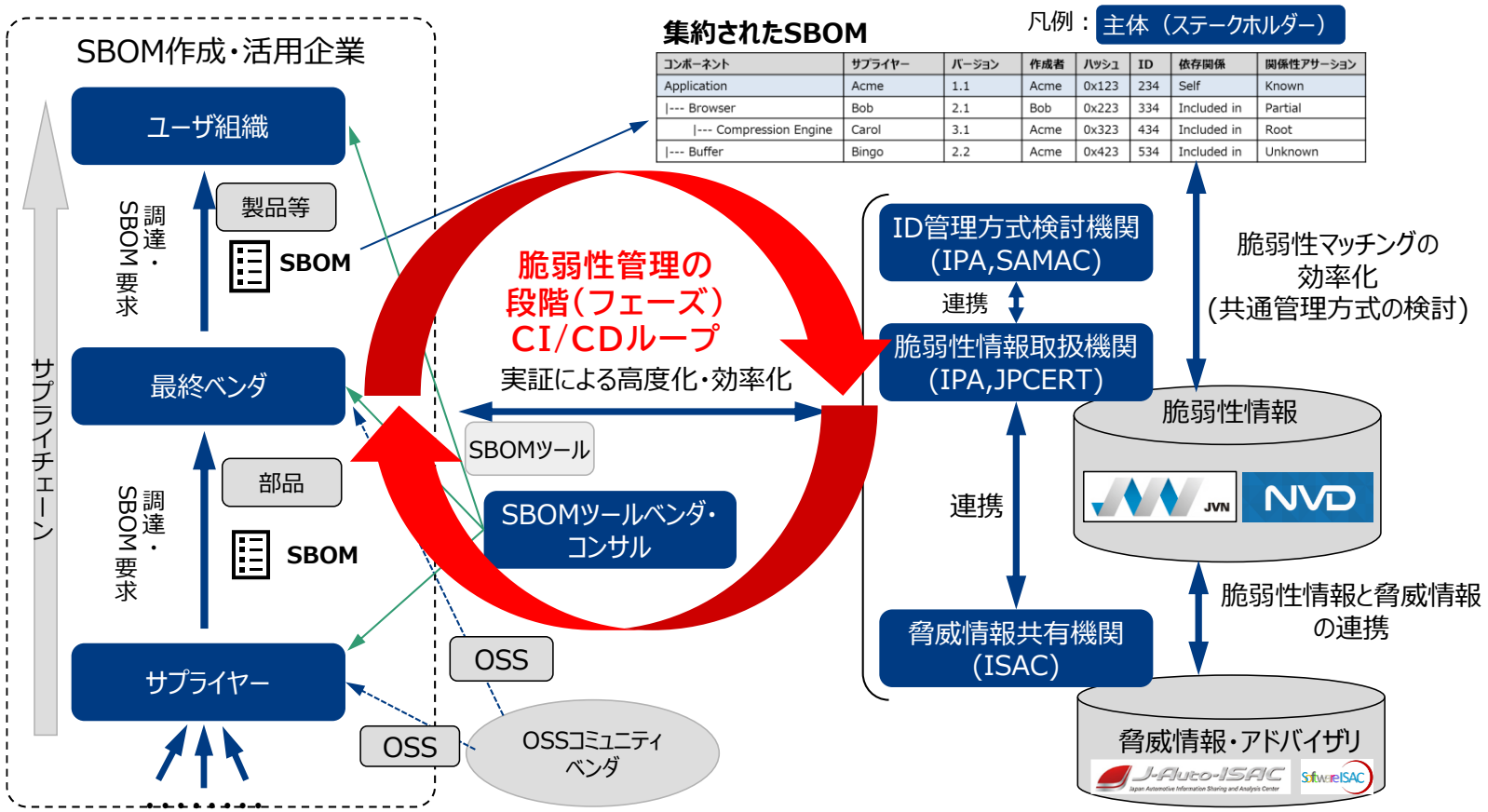
区分	実証から抽出した課題	解決ノウハウ （導入ガイダンスに反映予定）	今後の課題 （国、民間）	医療機器	自動車	ソフト
技術	検出した脆弱性の対応要否、優先度の判断が困難	医療機器分野の脆弱性対応フローなどを参考にアドバイザリ、脅威情報を活用し、対応の要否、優先度を判断。	脆弱性管理の高度化、脅威情報の普及促進	●		
	SBOMツールの使い分け・変更による負担増大	機能ニーズを洗い出し、ツール比較情報をもとに選択	—	●	●	●
	CI/CDなど継続的なアップデートへの対応負担	ツールによる自動化可能な範囲で管理	CI/CDに対応した自動管理			●
	SBOM初期導入、ツール等のコスト負担が大きい	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		●	●	

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。

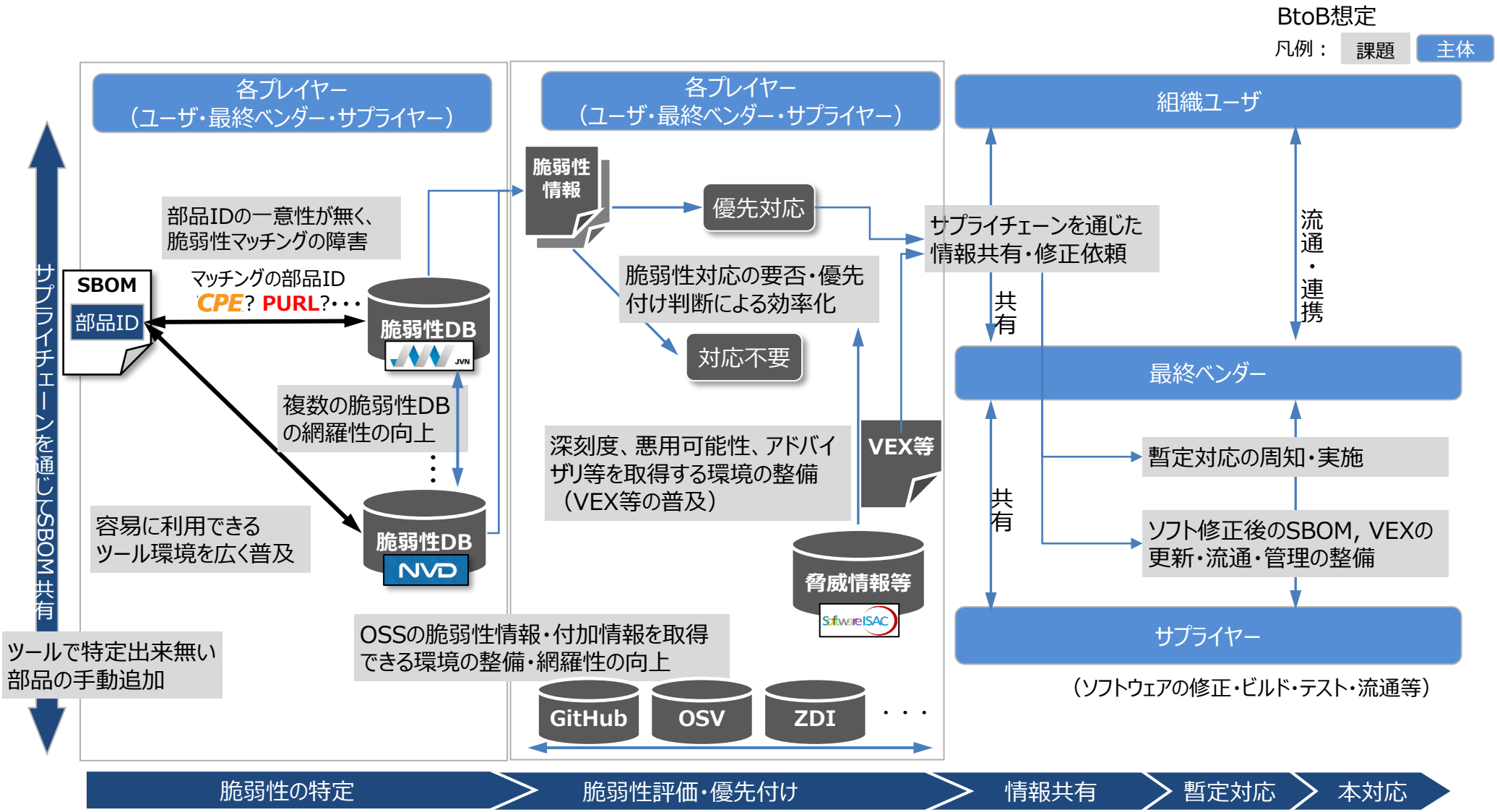
脆弱性管理の主なステークホルダとプロセスの全体像



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。



実証における重点項目：脆弱性特定に係る課題の詳細

- SBOMを用いた脆弱性特定においては、SBOMで用いられる部品IDと脆弱性情報DBの共通性や、照合する脆弱性情報DBのカバー率によって、脆弱性の特定および脆弱性管理の成果に大きな影響を与える。

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

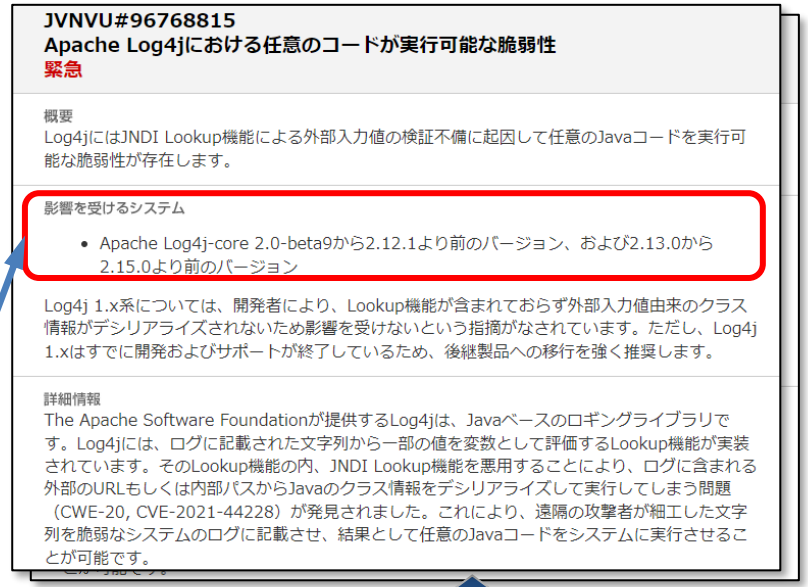
ツールSBOMフォーマット対応？ SPDXフォーマット（tag-value形式）のSBOM

```
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
DocumentNamespace: http://www.spdx.org/spdxdocs/8f141b09-1138-4fc5-aefb-fc10d9ac1eed
DocumentName: SBOM Example
SPDXID: SPDXRef-DOCUMENT
Creator: Organization: Company A
Created: 2022-05-09T13:00:00Z
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-Application-v1.1

PackageName: Application
SPDXID: SPDXRef-Application-v1.1
PackageVersion: 1.1
PackageSupplier: Organization: Company A
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: false
PackageChecksum: SHA1: 75068c26abbed3ad3980685bae21d7202d288317
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
ExternalRef: SECURITY cpe23Type cpe:2.3:a:company_a:application:1.1:*:*:*:*:*:*:*
Relationship: SPDXRef-Application-v1.1 CONTAINS SPDXRef-Browser-v2.1
Relationship: SPDXRef-Application-v1.1 CONTAINS SPDXRef-Protocol-v2.2

（以下省略）
```

部品IDは、ツールにより、CPE, PURL等の標準IDやベンダー独自IDなど多様



課題１：部品ID形式により検出漏れ・誤検出

脆弱性情報DBとの照合

課題2:脆弱性情報DBのカバー率拡大

実証で評価・検討すべき事項（実証の要件）

- 脆弱性管理を行うSBOM利用者について、初心者と上級者を想定し、(1)mjcheck等のツールをベースに基礎的な対応と、(2)ツールの選定、APIの活用、独自の脆弱性対応優先付けなど高度な対応を対象とする。両者にとって有益な手引きがまとめられるよう実施項目を整理する。
- また、ツールで対応できることの機能ニーズの整理と、SBOM利用者による人の対応が必要な事項について整理する。

脆弱性管理プロセス	課題	課題解決のために実証すべき事項（実証の要件）
脆弱性の特定（VM）	VM1：部品の識別子の一意性	SBOMで用いられる複数の部品ID標準(CPE, PURL等)について、SBOM作成時の部品ID選択の考え方の整理しつつ、脆弱性DBのAPI・ツールを用いて脆弱性マッチングを行う方法等を特定する。
	VM2:照合する脆弱性DBの網羅性確保	JVN, NVDなど複数の脆弱性DBについて、API・ツールを用いることで脆弱性マッチングの網羅性を拡大する方法を整理する。
	VM3：広く利用可能なツールの整備	• SBOMツールの選定などSBOM利用者がすべき事項を特定し、選定観点を整理する（選定観点の例：対応する部品ID,脆弱性DBのカバー率など）。 • 操作性、ドキュメント、価格などの点で中小企業なども利用しやすいツールの要件や課題について検討する。（候補：mjcheck等）
脆弱性評価・対応優先付け（VT）	VT1:脆弱性関連情報の活用	脆弱性情報に加え、民間組織、ベンダーにより提供される脆弱性付加情報の種類（深刻度、悪用可能性、アドバイザリ等を）や取得可能性ついて評価する。（ZDIなどを含む）
	VT2:脆弱性評価に基づく対応方針ロジック	脆弱性対応の優先付けにの基本的な考え方を検討し、必要となる付加情報の種類を特定する。（個社の優先付けポリシーの考え方などツールで出来ないことを特定する）
	VT3:OSSの脆弱性付加情報取得	GitHub, OSVなどからOSSに関する脆弱性付加情報の取得可否、課題を確認する。
情報共有・対応分担方針検討(RP)	RP1:情報共有基盤	特定した脆弱性、付加情報を共有する方法、フォーマット等を検討し、妥当性を確認する。
	RP2:サプライチェーン上の役割分担検討	原因特定、修正・対応などの依頼・役割分担する方法を検討し、ツールでは対応できない情報の共有方法等について整理する。
暫定対応(TR)	TR1:暫定対応の整理	暫定対応の選択肢を整理し、影響を受ける組織による周知について整理する。
本対応(FR)	FR1:本格対応の共有・適用	修正コードに対応したSBOMの更新、通知、履歴管理について整理する。

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

【Quad】ソフトウェアセキュリティに関する共同原則を公表

- 2023年5月、Quad（日米豪印戦略対話）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を発表**した。
- 安全なソフトウェア開発に関して、**4つの実践※に基づく安全なソフトウェア開発手法の実践を政府方針に取り入れる**こと、**ベンダーに対して同手法の実践を推奨する**ことを目指している。

※ SSDF（NIST SP 800-218）の4つの分類に相当する。

Quadにおけるソフトウェアセキュリティに関する共同原則

ソフトウェアベンダーによる安全な開発の実践に関する原則	安全なソフトウェア開発手法が実践されたソフトウェアを調達するため、当該手法を実践することを政府方針に取り入れるとともに、ソフトウェアベンダーに対して、当該手法の実践を推奨することを目指す。 • **組織の準備** 安全なソフトウェア開発手法を実践するため、適切な教育を受けた人材、プロセス、技術を適切に整備する。 • **ソフトウェアと開発環境の保護** ソフトウェアに含まれるコンポーネントを、改ざんや不正アクセスから適切に保護する。また、ソフトウェアは、リリースされたバージョンごとに管理し、バージョンごとに使用されているコンポーネントの詳細情報（SBOM等）やサプライチェーン情報を適切に管理する。 • **安全なソフトウェアの開発** 脆弱性を最小限に抑え、セキュリティに関するテストを経て十分なセキュリティを備えたソフトウェアをリリースする。 • **脆弱性への対応** ソフトウェアに存在する脆弱性を特定し、特定した脆弱性に適切な対処を行い、同様の脆弱性が今後発生することを防止する。
安全なソフトウェアの調達に関する原則	ソフトウェアまたはソフトウェアを含む製品の政府調達に関して、国際的義務、国内における法律・規制及びサイバー空間の成熟度に合わせ、各国は、以下の事項をソフトウェアベンダーに対して要求することを目指す。 • 安全なソフトウェア開発手法の実践に準拠していることを示す**自己適合証明書**を要求する。（第三者評価を受けた場合を除く） • 各国の脆弱性開示プログラム（脆弱性情報の報告や開示プロセスを含む）に準拠することを要求する。
ソフトウェアの運用におけるセキュリティ対策に関する原則	政府がソフトウェアを運用する際には、以下のセキュリティ対策を実施することを目指す。 • ソフトウェアやソフトウェアプラットフォームへの**不正アクセスおよび使用を防止**するため、適切な管理とプロセスを実施する。 • ソフトウェアやソフトウェアプラットフォームが使用するデータの機密性、完全性、可用性を保護するため、適切な管理とプロセスを実施する。 • ソフトウェアが悪用されるのを防ぐため、ソフトウェアプラットフォームやプラットフォームに展開されるソフトウェアを特定し、管理する。 • ソフトウェアやソフトウェアプラットフォームに関する**インシデントを迅速に検出・対応・回復**する。 • ソフトウェアやソフトウェアプラットフォームの**セキュリティ対策を推進する者へのサポートを強化**する。

出所）Australian Government Department of the Prime Minister and Cabinet, "Quad Cybersecurity Partnership: Joint Principles for Secure Software"
https://www.pmc.gov.au/resources/quad-cybersecurity-partnership-joint-principles-secure-software

- 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。
- ソフトウェアサプライチェーンリスクへの対応が必要に。

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