経済産業省

資料3

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の検討の方向性

令和4年3月3日

経済産業省　商務情報政策局

サイバーセキュリティ課

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. 最近のインシデント事例

3. ソフトウェア管理等に関する国内外の取組状況

4. 本タスクフォースにおける報告事項

・ OSS管理手法に関する事例集の拡充

5. 本タスクフォースにおける検討事項

・ 国内でのSBOM活用促進に向けた実証

分野別SWGにおけるサイバー・フィジカルセキュリティ対策フレームワーク（CPSF）の具体化 とテーマ別TFにおける検討

- **7つの産業分野別サブワーキンググループ(SWG)**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 分野横断の共通課題を検討するために、3つの**タスクフォース（TF）を設置**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
(分野ごとに検討するためのSWGを設置)

- **ビルSWG**
  - ガイドライン第1版の策定(2019.6)
- **電力SWG**
  - 小売電気事業者ガイドライン策定(2021.2)
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドライン1.0版を公表(2020.12)
- **スマートホームSWG**
  - ガイドライン1.0版を公表(2021.4)
- **宇宙産業SWG**
  - 2022年2月に第4回を開催
- **工場SWG**
  - 2022年2月に第2回を開催
- ・・・

分野横断SWG

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

検討事項：
データの信頼性確保に向け「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮）」案のパブリックコメント（2回目）を実施（3/3まで）。

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

検討事項：
OSSの管理手法に関するプラクティス集を策定、SBOM活用促進に向けた実証事業（PoC）を実施。

『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」を公開。

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. 最近のインシデント事例

3. ソフトウェア管理等に関する国内外の取組状況

4. 本タスクフォースにおける報告事項

・OSS管理手法に関する事例集の拡充

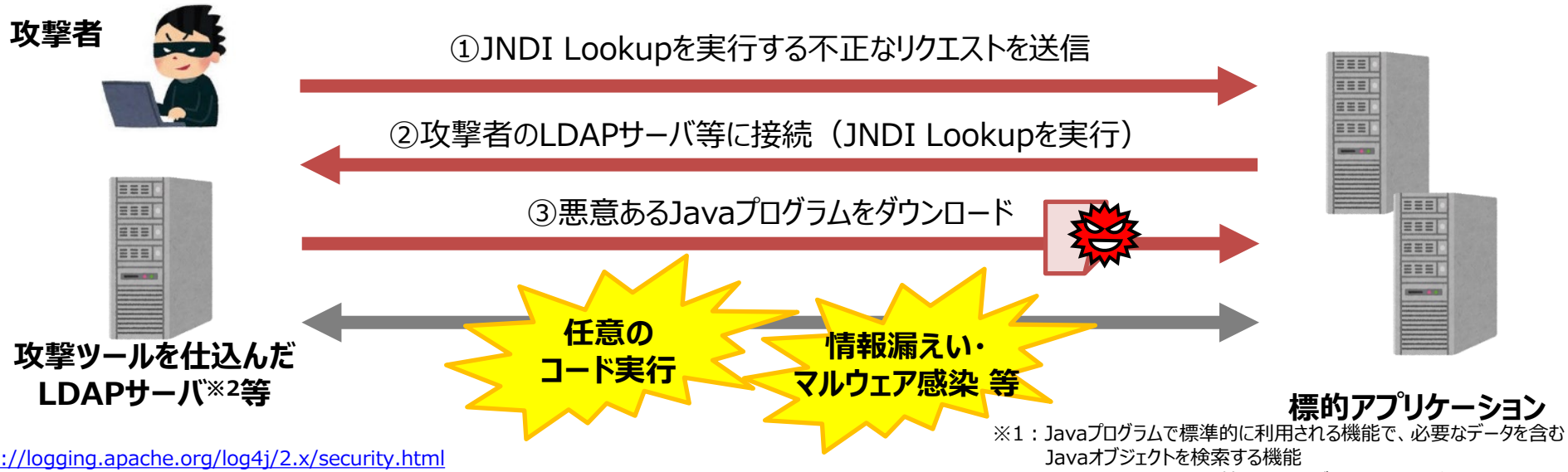
5. 本タスクフォースにおける検討事項

・国内でのSBOM活用促進に向けた実証

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**された。当該脆弱性はLog4jのJNDI Lookup※1機能に起因するもので、Log4Shellとも呼ばれる。
- この脆弱性を利用することで、**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る。
- 脆弱性の公表をうけて、**NISCから重要インフラ事業者等へ注意喚起を発出。**多くのユーザーへの影響が考えられることから、**一般向けにも注意喚起**を公開。前後して、**専門機関（IPA、JPCERT/CC）からも、Log4jのバージョンアップや回避策を講じることで脆弱性に対処するよう注意喚起**がなされた。
- その後、この脆弱性の悪用を試みる通信が観測されているほか、Microsoft社より本脆弱性を利用したランサムウェアの存在が報告されるなどしている。

◆ **Log4Shell（CVE-2021-44228等）を利用した攻撃のイメージ**



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

https://logging.apache.org/log4j/2.x/security.html
https://www.nisc.go.jp/press/pdf/20211213NISC_press.pdf
https://www.ipa.go.jp/security/ciadr/vul/alert20211213.html
https://www.jpcert.or.jp/at/2021/at210050.html

1. 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）とその実装へ向けた取組の方向性

2. 最近のインシデント事例

3. ソフトウェア管理等に関する国内外の取組状況

4. 本タスクフォースにおける報告事項

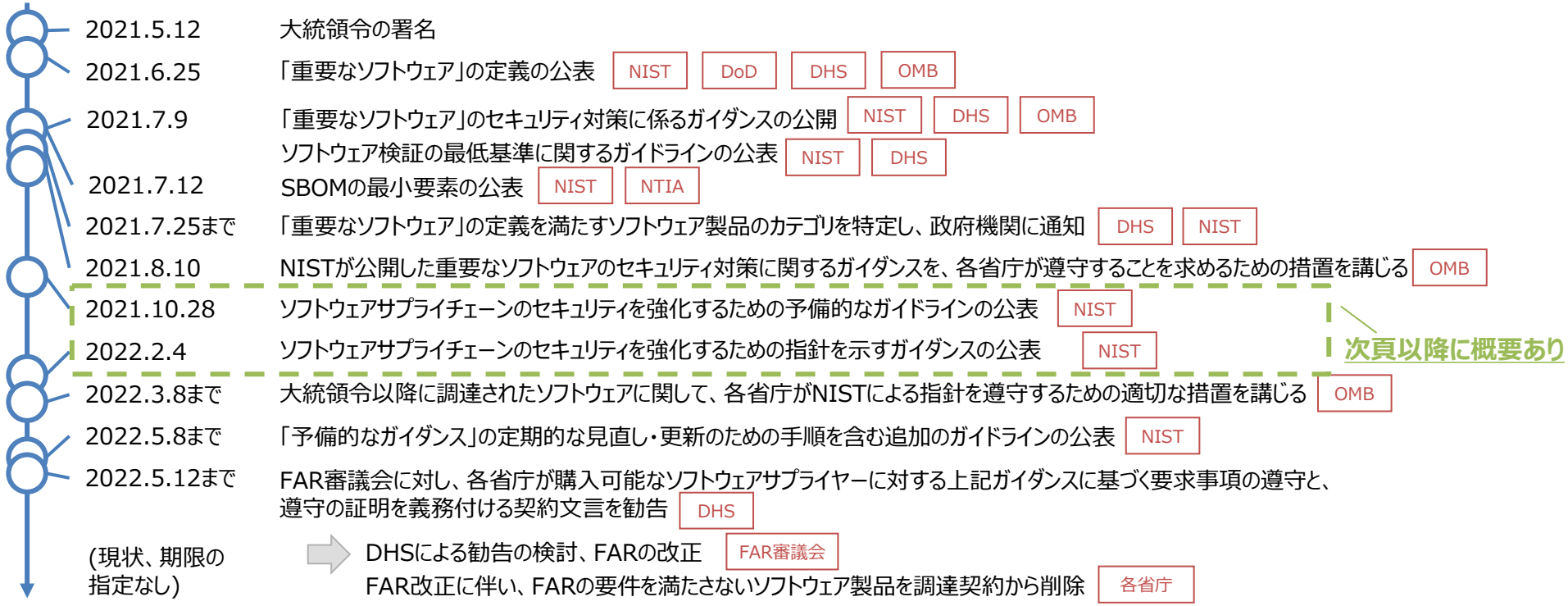
・OSS管理手法に関する事例集の拡充

5. 本タスクフォースにおける検討事項

・国内でのSBOM活用促進に向けた実証

【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。



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】ソフトウェアサプライチェーンのセキュリティ強化のための予備的ガイドライン

- 2021年10月、NISTは、SP 800-161（Cybersecurity Supply Chain Risk Management (C-SCRM) Practices for Systems and Organizations）Rev. 1のドラフト版を公開。**ソフトウェアサプライチェーンのセキュリティ強化に向けた予備的なガイドライン**を付録として添付。
- 本ガイドラインでは、**大統領令に対するNISTの取組とSP 800-161 Rev.1で規定されたC-SCRMの管理策との対応関係**や、**ソフトウェアサプライチェーンのセキュリティ確保のための新たな概念**を概説。
- 大統領令に準拠するために採用すべきC-SCRMの管理策や新たな概念を確認することが可能。

大統領令に対するNISTのこれまでの取組とC-SCRMとの対応関係

- 大統領令で指示されたソフトウェアサプライチェーンに関する3つの取組と、NIST SP 800-161 Rev.1やC-SCRMの管理策との対応関係について概説。

「重要なソフトウェア」の定義と求められる対策	• 各政府機関が優先的にセキュリティ対応を行う対象となる「重要なソフトウェア」の定義及び「重要なソフトウェア」のセキュリティ対策に関する取組。 • **C-SCRMの管理策や補足ガイダンスは、「重要なソフトウェア」に求められるセキュリティ対策を実施するための有効な手段**である。
ソフトウェア検証の最低基準	• サプライヤー（ベンダーや開発者など）によるソフトウェア検証の際に推奨される最低基準に関する取組。 • **C-SCRMの管理策や補足ガイダンスを用いて、最低基準を満たしたソフトウェア検証が実施されていることを確認**できる。
消費者向けIoTやソフトウェアのサイバーセキュリティラベリングプログラム	• 消費者向けのIoTデバイスやソフトウェアに対するラベリングのための仕組み構築に向けた取組。 • この取組はまだ検討段階にあるが、**C-SCRMには、この検討に関する直接的な内容が記載**されている。

ソフトウェアサプライチェーンのセキュリティ確保のための新たな概念

- ソフトウェアサプライチェーンのセキュリティ確保のための新たな4つの概念について、それぞれの事項を実施する際に各省庁が留意すべき点、各概念を採用することによる効果、今後の発展可能性を概説。

SBOM	• 各省庁は、ソフトウェア製品やサービスのサプライヤーが、**大統領令及びNTIAが公表しているガイドラインに準拠したSBOMを作成していることを、確認すべきである**。
サプライヤーにおけるリスク評価の強化	• サプライヤーが作成したソフトウェアだけではなく、**サプライチェーンにおいてソフトウェアに関与する事業体に対してもリスク評価を強化すべき**である。
OSSの管理	• 各省庁は、**サプライヤーのソフトウェアにおけるOSSの使用状況をより深く理解するよう努めるべき**である。
脆弱性管理	• ゼロトラストアーキテクチャの議論を踏まえ、**各省庁の戦略は、検出された脆弱性をいかに効率的かつ包括的に管理するかについて焦点を当てるべき**である。

出所）NIST, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2nd Draft)
https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft

【米国】ソフトウェアサプライチェーンのセキュリティ強化のための指針を示すガイダンス

- 2022年2月、大統領令の指示を受け、NISTは、**連邦政府機関が調達するソフトウェア※のサプライチェーンセキュリティ強化のための指針を示したガイダンス**を発表。
- 特に、**ソフトウェア調達に関わる連邦政府職員を対象に、SSDF（SP 800-218）の手法を実装する開発者からセキュアなソフトウェアを調達するために必要な、4つの最低限の勧告事項を明記**している。
- ガイダンスでは、**4つの勧告事項が調達するすべてのソフトウェアに適用**されるために、**各政府機関の調達プロセスに含まれるべき**としている。各政府機関の調達プロセスに含まれた場合、**連邦政府の調達対象となるソフトウェアは、SSDFの手法を実装することが必須**となる。

※ 本ガイダンスの対象となる「連邦政府機関が調達するソフトウェア」には、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及びソフトウェアを使用する製品が含まれる。オンプレミス・クラウドの両方のソフトウェアが含まれるが、連邦政府機関によって開発されたソフトウェアや連邦政府機関が直接的に入手したOSSは対象外となる。

連邦政府機関がセキュアなソフトウェアを調達するための4つの勧告事項

- **SSDFで定義された用語に基づき、安全なソフトウェア開発要件に関する共通言語を整理する**。
  - これにより、ソフトウェア開発者が連邦政府機関へ納入するための適合性を証明する際に、同じ共通言語を用いてコミュニケーションを取ることができる。
- **ソフトウェアのライフサイクルを通じて実践される、安全なソフトウェア開発の手法に関する証明を要求する**。
  - 今日のソフトウェアは非常に動的であるため、一つのソフトウェアに関して証明を求めるより、プロセスや手順を含んだ組織の開発手法を確認する方が一般的に価値がある。
- 安全なソフトウェア開発の対応に関する証明の要求に際して、第二者又は第三者による認証が必要であると判断されない限り、**第一者認証によるSSDF適合の証明を認める**。
- **適合性を示すためのアーティファクトを要求する場合、上位レベルのアーティファクトを要求する**。
  - 上位レベルのアーティファクトとは、組織のソフトウェア開発プラクティスを要約した文書であり、セキュアなソフトウェア開発のための方法、手順及びプロセスが記載された文書を指す。
  - 他方、ソフトウェア開発の過程で生成される脅威モデル、ソースコード、ソースコードの脆弱性スキャンレポート等は下位レベルのアーティファクトと定義される。

出所）NIST, Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e
https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.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リスクマネジメントに関する法案

- 2021年10月、米国下院においてDHSのソフトウェアサプライチェーンに関する法案が可決した。
- 本法案が成立した場合、**DHSがIT機器やサービス※を調達する際に、機器・サービスのベンダーに対して、機器・サービスのSBOM、脆弱性情報及び脆弱性がある場合の対処方法を提示することが義務化**される。
- また、機器・サービス納入後も、**SBOMに変更が発生した際に変更内容を随時提示することが義務化**される。
- 本法案は大統領令に基づき策定されたもので、成立した場合、**成立日から180日後に有効**となる。
- その他、会計検査院に対して、本法案成立日から1年以内に、本法案の実施状況のレビューや対象となる契約に関するサプライチェーン改善に向けた推奨事項等を報告書としてまとめ、DHSや国土安全保障委員会等に提出することを求めている。

DHSと調達契約を行うベンダーに対する要求事項

新規・既存の調達契約におけるSBOM、脆弱性情報、脆弱性がある場合の対処方法の提示	• **SBOMの提示：** 入札提案時に、使用予定のコンポーネントに関するSBOMを提示する必要がある。 （既存の契約の場合は、DHSからの要請に応じて使用中のSBOMを提示する必要がある。） • **脆弱性が無いことの提示：** 使用予定（または使用中）のコンポーネントにおいて、最終製品やサービスのセキュリティに影響を与える既知の脆弱性や欠陥が存在しないことを認証し、その認証結果を提示する必要がある。 • **脆弱性がある場合の対処方法の提示：** 使用予定（または使用中）のコンポーネントに脆弱性や欠陥が存在する場合は、脆弱性と欠陥の情報及び、それらを軽減・対処するための計画を提示する必要がある。
SBOMの更新内容の提示	• **SBOMの更新内容を提示：** DHSへ提示したSBOMに変更が発生した場合、変更内容を随時提示する必要がある。

※「IT機器やサービス」には、米国通信法で定義された「電気通信機器」及び「電気通信サービス」や、合衆国法典で定義された「情報システム」及び「情報技術」が含まれ、具体的な例として、NISTの定義に基づくと、ルーターやスイッチ等の通信機器、OS、ソフトウェア、ファームウェア、アプリケーションのほか、産業制御システム等が挙げられる。

出所）H.R.4611 - DHS Software Supply Chain Risk Management Act of 2021
https://www.congress.gov/bill/117th-congress/house-bill/4611/text

【米国】消費者向けソフトウェアのサイバーセキュリティラベルの推奨基準

- 2022年2月、NISTは、大統領令に基づき**消費者向けソフトウェアのセキュリティラベルの推奨基準**を公開。
- 本文書では、**ベンダーがソフトウェアにラベリングするための技術的な基準、ラベリングの基準、ラベリングの適合性評価基準等の推奨基準に関して検討・整理**されている。
- なお、現状でNISTが特定のラベリング制度を確立しているわけではなく、**ラベリング制度に必要な要件や基準を特定することが本文書の目的**であることに留意。

Executive Order on Improving the Nation's Cybersecurity (2021/5/12公開)
Sec.4. ソフトウェアサプライチェーンセキュリティの強化
(s) IoT機器のセキュリティ機能とソフトウェアの開発方法について一般の人々を教育するためのパイロットプログラムを開始。
(u) 発令から270日以内に、消費者向けソフトウェアラベリングプログラムの安全なソフトウェア開発方法または基準を特定。

消費者向けソフトウェアサイバーセキュリティラベリングにおける推奨基準の概要

ラベリングのための技術的な推奨基準（Section 2）	• 消費者向けソフトウェアに関して**セキュリティを担保するための技術的な評価項目と評価基準**を定義。 • 文書では、ラベリング制度のオーナーに対し、**ラベルを付与する際は、以下の2つにカテゴリ分けされたすべての基準をラベリング申請者に求めることを推奨**している。 1. 基本情報：ラベル申請者の情報、ラベルの対象スコープ、ラベル発行日、セキュリティ更新の有無、セキュリティサポートの最小期間、セキュリティ更新方法等、対象となるソフトウェアに関する情報が明示されているか 2. 安全なソフトウェア開発：SSDFが実装されているか、脆弱性が発見された際に利用者に通知されるか、多要素認証を使用しているか、機密情報はハードコードされていないか、強力な暗号化方式を使用しているか、ユーザーデータが適切に識別され保護されているか
ラベリングの基準（Section 3）	• **ソフトウェアに対して付与されるラベルの種類**を定義。 • 具体的なラベルとして、製品が推奨基準を満たしたことを示す唯一のラベルである「バイナリラベル」や、追加情報と併せて消費者に提供される「階層化ラベルアプローチ」※という種類・アプローチが記載されている。 • NISTは、ソフトウェアに対するサイバーセキュリティラベリングにおいて、**「バイナリレベル」を採用することを推奨**している。
適合性評価基準（Section 4）	• ソフトウェアベンダーが**ラベリングの対象となるソフトウェアを定義し、ラベルを付与、そして消費者に対して適合宣言を実施するための基準**を定義。 • 適合宣言のための基準として、供給者適合宣言 (Supplier's Declaration of Conformity) の概念に基づき、**ソフトウェアベンダーが宣言に含めるべき項目及びソフトウェアが満たすべき基準**がまとめられている。 • なお、第三者適合性評価プログラム等の外部の評価結果を活用して宣言を補足する際の必要な情報についてもまとめられている。

※「階層化ラベルアプローチ」とは、複数の階層に分けて製品に関する情報を開示するアプローチ（例：第一層として製品のパッケージにおいて代表的な情報を記載、第二層として製品に関するウェブサイトでより詳細な情報を記載）であり、厳密には「ラベルの種類」ではないことが明記されている。

出所）NIST, Recommended Criteria for Cybersecurity Labeling of Consumer Software
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-1.pdf

【米国】SBOMに対する誤解と事実を示す文書の公開

- 2021年11月、NTIAは**SBOMが提供するメリットを正しく示すことを目的**として、**SBOMに関する代表的な誤解（神話）と、その誤解を解くための事実を整理した文書**を公開。

誤解	事実
SBOMは、攻撃者による攻撃を支援する	SBOMは攻撃に利用可能であるが、SBOMにより透明性を確保することによる「攻撃者からの防御」におけるメリットの方が大きい。 攻撃者にとってのSBOMやソフトウェアの透明性は、次のように位置付けられる。 • 一般的に攻撃者はSBOMを必要としない。例えば、WannaCryによるランサムウェア攻撃は、SBOM情報が攻撃のための前提条件ではなかった。 • 攻撃のためのツールは、SBOMを活用せずとも、攻撃対象となるソフトウェアコンポーネントを簡単に特定できる。
SBOMだけでは、有用・実用的な情報を得ることができない	SBOMは、ソフトウェアの開発者、購入者、運用者をサポートする。 例えば、攻撃を受けている際、SBOMを使用することで、攻撃の影響を受けているか、攻撃の影響範囲はどこかを容易に判断できる。 コンポーネント情報があることでソフトウェアの透明性が向上し、管理が容易となり、開発、購入、運用段階以外での活用も可能となる。
SBOMは公開しなければならない	SBOMを公開する必要はない。「SBOMの作成」と「SBOMを前向きに活用できる人との共有」は別の観点である。SBOM作成者の判断でSBOMを共有することができる。 業界における規制や法定要件により、SBOMへのアクセスを求められる場合がある点には留意する必要がある。 また、大統領令でもSBOMの公開はSBOM作成者の判断であり、必須ではないことが明確に記載されている。「ソフトウェア購入者にSBOMを直接提供するか」、「公開WebサイトにSBOMを公開するか」という点については、SBOM作成者が判断できる。
SBOMは知的財産や企業秘密を露呈してしまう	SBOMはソフトウェアに含まれているコンポーネントの概要であり、特許やアルゴリズムは含まれておらず、知的財産を公開するものではない。 SBOMの内容や知的財産に関して考慮すべき点は以下のとおり。 • SBOMは単なる「材料の一覧」であり、特許やアルゴリズムのような「レシピ」とは異なる。 • 第三者が開発したコンポーネントの特許やアルゴリズムなどの知的財産は、コンポーネントの開発者または著作権所有者に帰属する。 • 使用するソフトウェアコンポーネントのライセンス条項において、情報開示を要求されることが近年増加している。 • SBOMには、ソフトウェアのソースコード自体は含まれない。 • 契約、法的等の要件で、特定のコンポーネント開示が禁止されている場合がある。この際、「既知の不明なコンポーネント」の存在を示す必要がある。
SBOMを活用するためのサポートは存在しない	ソフトウェア構成分析（SCA）ツールは、一部の分野では、10年以上にわたって企業内で使用されてきた実績がある。 ソフトウェアの透明性に関しては、NTIAの活動、大統領令、SBOMフォーマットの標準化などの活動が進んでいるほか、一部の分野では、ソフトウェアの透明性について5年以上にわたって議論やPoCの取組が進められており、他分野での導入をサポートしている。

出所）NTIA, "SBOM Myths vs. Facts"
https://www.ntia.gov/files/ntia/publications/sbom_myths_vs_facts_nov2021.pdf

【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】ソフトウェア利用者のためのSBOMプレイブック

- 2021年11月、NTIAはソフトウェア利用者を対象としたSBOM利用に関するプレイブックを公開。
- 本プレイブックでは、**サプライヤーからSBOMを取得する際の注意点、SBOMの活用可能性、SBOMの知的財産及び機密性に関する注意点等**がまとめられている。

ソフトウェア利用者のためのSBOMプレイブックの概要

サプライヤーからSBOMを取得する際の注意点

- **SBOM取得のタイミング**
  ソフトウェア利用者は、以下のような場合に、SBOMを取得することができる。
  - ✓ ソフトウェアやサービスの契約や調達時
  - ✓ プロプライエタリ・ソフトウェアのダウンロード時
  - ✓ ソフトウェアの開発・提供に係る専門サービスの契約や調達時
  - ✓ 開発時などの社内展開用として、OSSアプリケーションまたはコンポーネントの取得時
  - ✓ デバイスのネットワーク接続時
    (SBOM検出プロセスが自動で実行する場合)
- **SBOMの対象となるソフトウェアの範囲**
  ソフトウェアの定義は以下のように様々である。
  - ✓ 単一のアプリケーション
  - ✓ 外部と依存関係のあるアプリケーション
  - ✓ ソフトウェアコンテナ
  - ✓ 複数のエンドポイントを持つシステム

  利用者は、SBOMの対象となるソフトウェアを確認する必要がある。
- **ソフトウェアコンポーネントの特定**
  コンポーネントを正確に特定することで、脆弱性とのマッピングや、構成管理・ソフトウェア資産管理の曖昧さの排除が可能となる。

SBOM活用のプロセスおよびプラットフォーム

- **SBOMの活用可能性**
  SBOMの活用が組織内で十分に成熟すると、以下のプロセスやプラットフォームにおいて、SBOMを効果的に活用できる。
  - ✓ 構成管理データベース (CMDB)
  - ✓ ソフトウェア資産管理 (SAM)
  - ✓ セキュリティオペレーションセンター (SOC)
  - ✓ 調達に関するワークフロー
    (調達前調査、サプライヤー管理、サードパーティ/コンプライアンスのリスク管理など)
  - ✓ ソフトウェアサプライチェーンリスク評価管理
- **SBOMの継続的な監視**
  利用者は、脆弱性対処ステータスについてサプライヤーと情報共有を継続することで、脆弱性の状況認識に係る利用者とサプライヤーとのギャップを取り除くとともに、SBOMの継続的な信頼性確保に寄与する。
  - ✓ 脆弱性を検出する前の情報共有
  - ✓ 脆弱性を検出し、脆弱性に対処する前の情報共有
  - ✓ 脆弱性対処後、消費者へ共有する前の情報共有

SBOMの知的財産および機密保持

ベンダー、請負業者、OSSコミュニティ等、どの立場によってSBOMが提供されるかで、SBOMの知的財産や機密保持に対する考え方は異なる。

- **ベンダーや請負業者によってSBOMが提供される場合**
  SBOM自体に適用される守秘義務条項は契約上、明示的に定義される。ソフトウェア利用者の視点では、SBOMを内部目的で使用することが許可されるべきである。
- **OSSコミュニティによってSBOMが提供される場合**
  OSSコミュニティが提供するSBOMは、ライセンスの下で明確に位置付けられるべきである。利用者は、SBOMに関するOSSのライセンスを確認する必要がある。
- **中間サプライヤーへSBOMを提供する場合**
  SBOM利用者が中間サプライヤーである場合、最終消費者へ提供するSBOMが、中間サプライヤーへ提供されるSBOMの機密保持条件を満たしていることを確認する必要がある。SBOMの知的財産や機密性の規定により中間サプライヤーのコンポーネントの特定が妨げられる場合、最終消費者のサプライチェーン透明性が損なわれる可能性がある。特に、省略、改訂及び「既知の未知」を特定するために、これらの規定の存在をSBOMで伝える必要がある。

出所）NTIA, ” Software Consumers Playbook: SBOM Acquisition, Management, and Use”
https://www.ntia.gov/files/ntia/publications/software_consumers_sbom_acquisition_management_and_use_-_final.pdf

【米国】SBOMに関するイベント“SBOM-a-rama”の開催

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

“SBOM-a-rama” 1日目の講演アジェンダ・講演者

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

“SBOM-a-rama” 2日目の議論により抽出された主要な課題

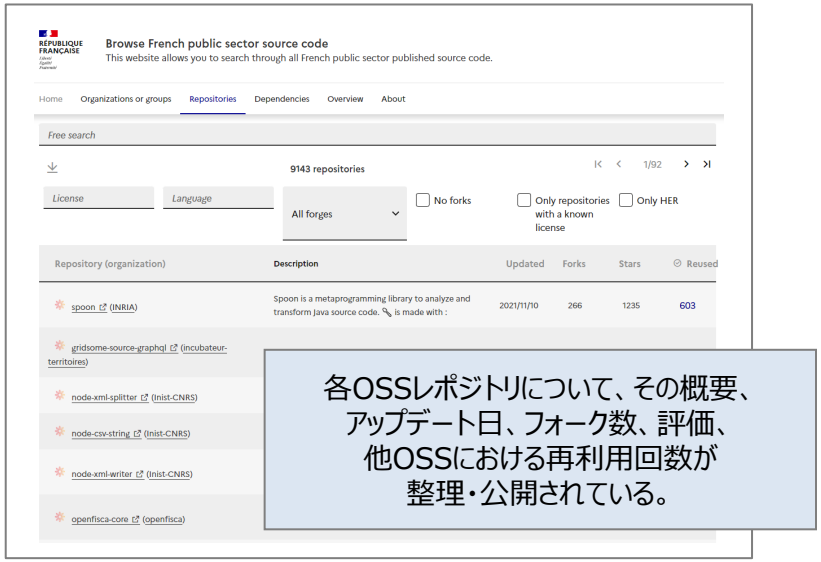
観点	議論により抽出された主要な課題（抜粋）
クラウド	• クラウドサービスに対するSBOMユースケースの作成 • クラウドネイティブコンポーネントに対するSBOM生成方法
データマネジメント	• **SBOM生成に必要なデータの提供方法** • OSSコミュニティも含めた適切なデータの統合方法
ツール	• コンテナ環境、仮想環境、AI/ML等に対するSBOM生成ツール • **SBOM共有・活用ツール**
普及・促進	• SBOM活用に向けた教育 • **各国の規制基準への適用** • **SBOMの出所と明確化や信頼性の確保**
共有・交換	• SBOMのアーカイブを残す方法 • **SBOM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

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

【仏国】公的機関が公開するOSSレポジトリに関するWebサイト

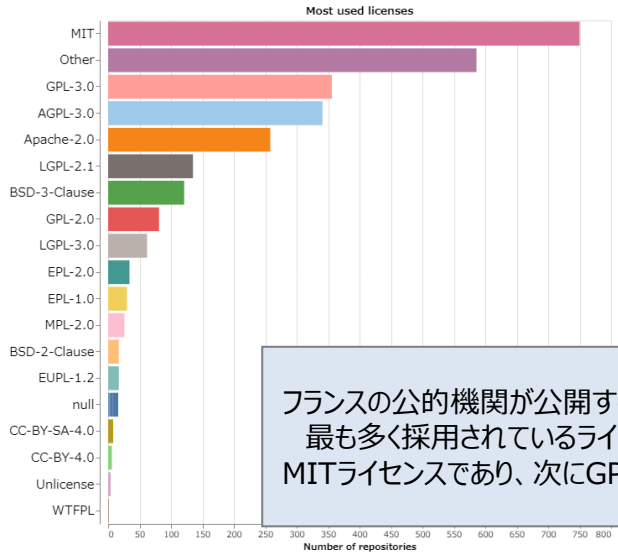
- 2021年11月10日、仏デジタル省庁間総局（DINUM）の一部門であるEtalabは、**フランスの公的機関が公開しているOSSレポジトリを集めたWebサイト※1の公開**を開始した。
- 当該サイトは2019年10月の政令※2に基づき公的機関におけるOSSの活動を促進する目的で構築・公開され、2022年1月時点で**1,000組織を超える公的機関の9,000を超えるOSSレポジトリ情報**が公開されている。
- 各OSSレポジトリについて、公開している公的機関のプラットフォームへのリンクが用意されているほか、**対象OSSで採用されているライセンスの割合や、対象OSSで再利用している他のOSS等の統計情報も確認可能**。
- なお、米国においても、米国政府機関のOSSレポジトリを公開するサイト※3が2016年11月より運用されている。

フランスの公的機関によるOSSレポジトリを集めたWebサイトの概要



各OSSレポジトリについて、その概要、アップデート日、フォーク数、評価、他OSSにおける再利用回数が整理・公開されている。

フランスの公的機関が公開するOSSが多く採用しているライセンスの種類



フランスの公的機関が公開するOSSにおいて最も多く採用されているライセンス形態はMITライセンスであり、次にGPL 3.0が多い。

※1：https://code.gouv.fr/
※2：Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique
情報通信システムの分野に関する行政省庁の連携・調整を進めるデジタル省庁間総局（DINUM）を設置し、情報通信システムに関する国全体としての管轄について定めた法令。
DINUMの所掌任務の一つとして、公的機関の監督化にあるデータの利活用を最大限促進することを規定しており、この規定に基づきOSSレポジトリを集めた上記Webサイトが公開された。
※3：https://code.gov/

【日本】OpenChain Japan WGの取組

- OpenChain Japan WGは、OpenChainプロジェクトに参加する国内企業が日本語で議論する場を作ることを目的に、2017年に設立。（第3回TF資料4参照）
- 現在、**OpenChainに関する文書やSPDX仕様の翻訳、OSSの管理や透明性向上に向けたOSSマネジメントに関するスキル標準作成等の活動を実施中**。

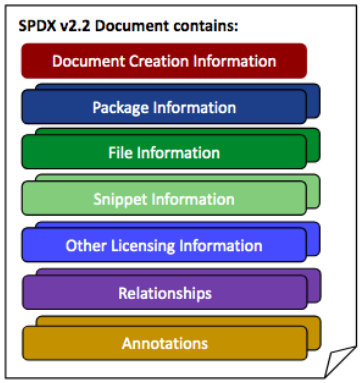
OpenChain文書やSPDX仕様の翻訳

- **関連する英語文書の日本語翻訳の取組を有志にて実施中**。
- 現在対応している文書は下記のとおり。
  - OpenChain ISO/IEC 5230 Security Assurance Reference Guide（OpenChain（ISO/IEC 5230:2020）の使用方法のガイダンス。）
  - SPDX2.2（ISO/IEC 5962:2021）仕様　※翻訳作業中（仕様策定において、OpenChain Japan WGはSPDX Lightを作成。）
- **翻訳後は順次公開**予定。


OPENCHAIN　OpenChain セキュリティアシュアランスリファレンスガイド 1.0

目次

OpenChain ISO/IEC 5230 – Security Assurance Reference Guide（日本語版）：
https://qiita.com/kida_oss/items/bf6a9d005dd1b50b5875



SPDX仕様（英語版）：https://spdx.dev/specifications/

OSSマネジメントに関するスキル標準作成

- システム開発におけるOSS利用が増え、OSS管理業務が複雑化、**使用OSSやライセンス・脆弱性の把握が困難**に。
- OSS に関わる人材育成や役割分担のため、**OSSライセンスコンプライアンス・脆弱性対応業務等に関するスキル標準の作成**を検討。
- 第1歩として「スキル標準フレームワーク（全体マップ）及び職種別業務」を作成。
- **既存のITSS+等との整合性も図りつつ作成を継続**予定。

		業務		職種別業務									
				エンジニア		調達・営業		情報セキュリティ		法務・知財		マネジメント	
業務フェーズ	企画	1)コミュニティ投資	13) ガバナンス 14) 教育 15) コントリビューション	1)	13) 14) 15)	4)	13) 14) 15)	2)	13) 14) 15)	1)	13) 14) 15)	1)	13) 14) 15)
		2)OSS活用検討		2)						2)		2)	
		3)特許調査		3)						3)			
		4)調達契約策定		4)						4)			
	開発	5)OSS活用		5)		7)		8)		7)		8)	
		6)SBOM作成		6)						8)		9)	
		7)サプライヤ管理		7)						9)		10)	
		8)活用可否判断		8)						10)			
		9)ライセンス対応		9)									
		10)OSS化検討		10)									
	保守	11)脆弱性対応		11)		12)		11)		12)			
		12)ユーザ対応		12)									

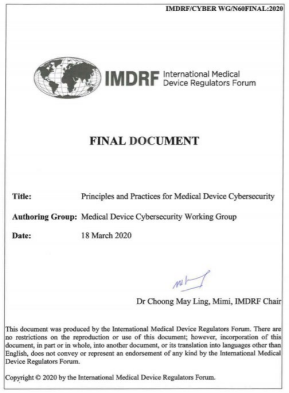
スキル標準フレームワーク（全体マップ）及び職種別業務
（企画～保守における業務と各職種が行うべき業務をマッピング）

OpenChain Japan WG : https://openchain-project.github.io/OpenChain-JWG/index.html

【日本】医療機器分野のサイバーセキュリティに関する規制・検討の状況

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

IMDRFガイダンス※1の概要


IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

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

Copyright © 2020 by the International Medical Device Regulators Forum.

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

○一般原則

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

○ベストプラクティス

・市販前（主に医療機器製造業者向け）
・市販後（全ステークホルダー向け）

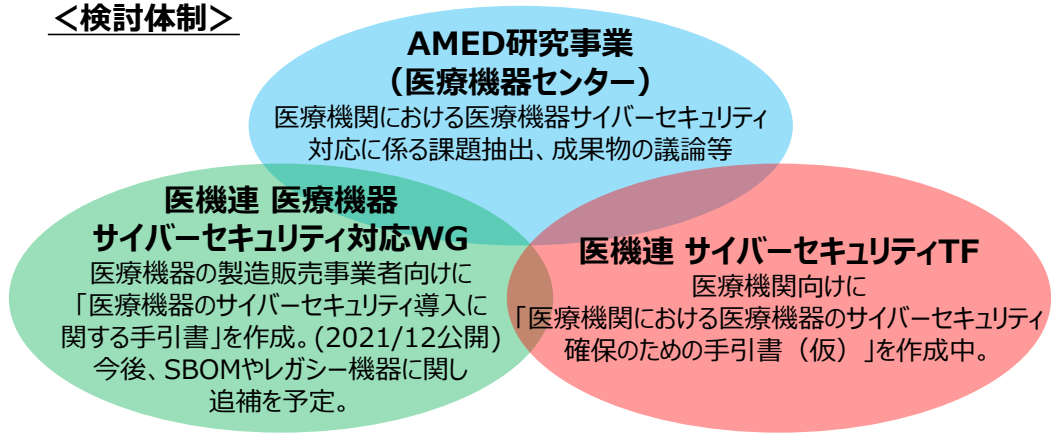
○SBOMに関する記載

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

国内における規制と対応状況

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

＜検討体制＞



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

1. 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）とその実装へ向けた取組の方向性

2. 最近のインシデント事例

3. ソフトウェア管理等に関する国内外の取組状況

4. 本タスクフォースにおける報告事項

・ OSS管理手法に関する事例集の拡充

5. 本タスクフォースにおける検討事項

・ 国内でのSBOM活用促進に向けた実証

OSS管理手法に関する事例集の拡充

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

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

1. 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）とその実装へ向けた取組の方向性

2. 最近のインシデント事例

3. ソフトウェア管理等に関する国内外の取組状況

4. 本タスクフォースにおける報告事項

・OSS管理手法に関する事例集の拡充

5. 本タスクフォースにおける検討事項

・国内でのSBOM活用促進に向けた実証

これまでのソフトウェアタスクフォースにおけるSBOMの議論の振り返り

- SBOM等ソフトウェア管理手法は、その必要性が認識されていたものの検討の枠組みが存在せず。
- 過去５回のタスクフォースにおいて、SBOM導入に向けた課題や国内での実証の内容を議論。

第１回～第３回タスクフォース

ソフトウェアセキュリティ確保に向けた課題の１つとして、**SBOMを含むソフトウェア管理手法について議論**。

＜SBOMについての主なご意見＞

- ✓ SBOM作成・運用の自動化
- ✓ SBOMの必要情報、粒度
- ✓ SBOM共有の方法、契約、秘匿性確保
- ✓ コスト負担
- ✓ OSSの更新等に合わせたSBOMの更新やメンテナンス
- ✓ 対応不要と判断した脆弱性の扱い
- ✓ 日本固有の問題の洗い出し
- ✓ 中小企業のリソース等への配慮

第4回タスクフォース

SBOMの導入コストや効果を示すべく、国内でのSBOM活用促進に向けた**実証を提案**。

＜SBOM導入の課題についての主なご意見＞

- ✓ フォーマットを統一化して活用できるガイドラインの作成
- ✓ サプライヤーの巻き込み
- ✓ 活用に関しメリットを享受できるモデルの検討

＜SBOM実証への主なご意見＞

- ✓ ツールの費用、検出精度や誤検出、名称問題の解決
- ✓ 実証の対象（できるところから、複数組織にまたがった実証を）
- ✓ 管理対象の特性の考慮（システム、パッケージ、言語等）
- ✓ SBOMの管理単位、運用・更新コスト

第5回タスクフォース

国内でのSBOM**実証の対象や内容について報告**して議論。

＜SBOM実証や今後の検討へ向けた主なご意見＞

- ✓ 効果・コスト（個社／複数社の連携、システム規模、SBOM粒度による違い）
- ✓ コストや責任の分担（サプライチェーンのコスト分配、契約の問題）
- ✓ ノウハウの共有（実証における記録、プラクティス集の公開）
- ✓ ツール（ツールの信頼性、相互運用性）
- ✓ フォーマット・項目（必要／不要な項目、標準化、SPDXの翻訳）
- ✓ 産業界における既存の取組（企業へのヒアリング）
- ✓ 政府機関でのSBOM活用（実証の実施、政府統一基準）
- ✓ 国際協力（米国の複数組織との関係構築）

SBOMに関する施策の進め方（案）

第5回TF資料再掲

- 国内施策および国際連携により、SBOMに係る対応を進める。
- 令和3年度の実証を通じてSBOMの効果的な活用方法を検討（STEP1）。
- STEP1の結果を踏まえて令和4年度以降、実証の対象を拡大し必要な制度、ツール整備を図る。

＜施策テーマ＞

	施策テーマ	施策
国内施策	(1) 国内産業のSBOM対応促進	**① 国内産業のSBOM普及啓発** • 実証やガイダンス等により国内産業へのSBOM普及促進を図る。
		②SBOM普及に向けた論点整理 ①で明らかにした論点を整理し、必要な制度・ツール等を整備する。 例：費用負担やリスク負担、知財権保護等の整理。自動化に向けたツール環境やソフトウェアID等の整備。
国際連携	(2) 日米の協力関係構築	**③SBOM検討に係る日米協力** OSS事例集や国内実証のコスト評価結果などを提供することにより、日米検討の協力関係を構築し、ツール等の整備における必要な調整を図る。

＜検討のステップ＞

STEP1：【R3年度実施】

実証を通じたSBOMの効果的な活用方法の検討

STEP2：【R4年度実施】

実証の対象拡大による課題整理（サプライチェーンにおける共有等）

STEP3：【R4年度～】

制度、ツールの検討・整備
国外との制度調和

SBOM実証の内容（案）

第5回TF資料再掲

- 実証においては、作成手段や作成者等の条件を設定して、SBOMの実際の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実証の対象ソフトウェア・体制・スケジュール

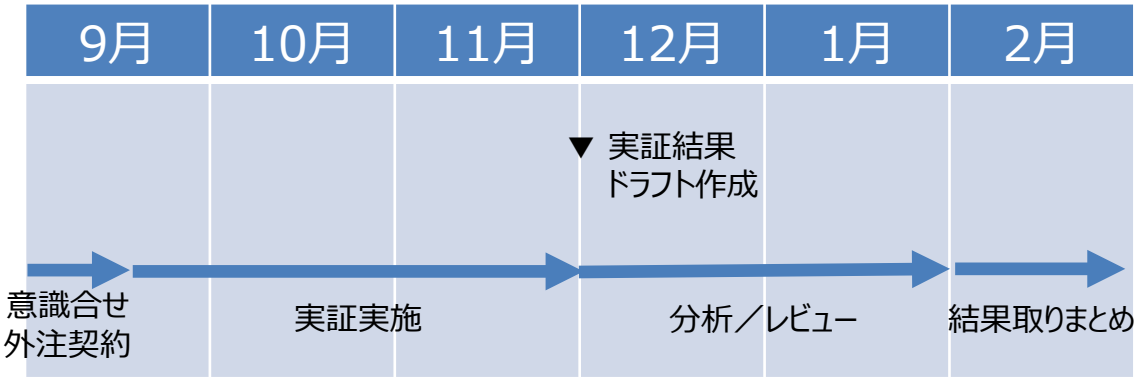
第5回TF資料再掲

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

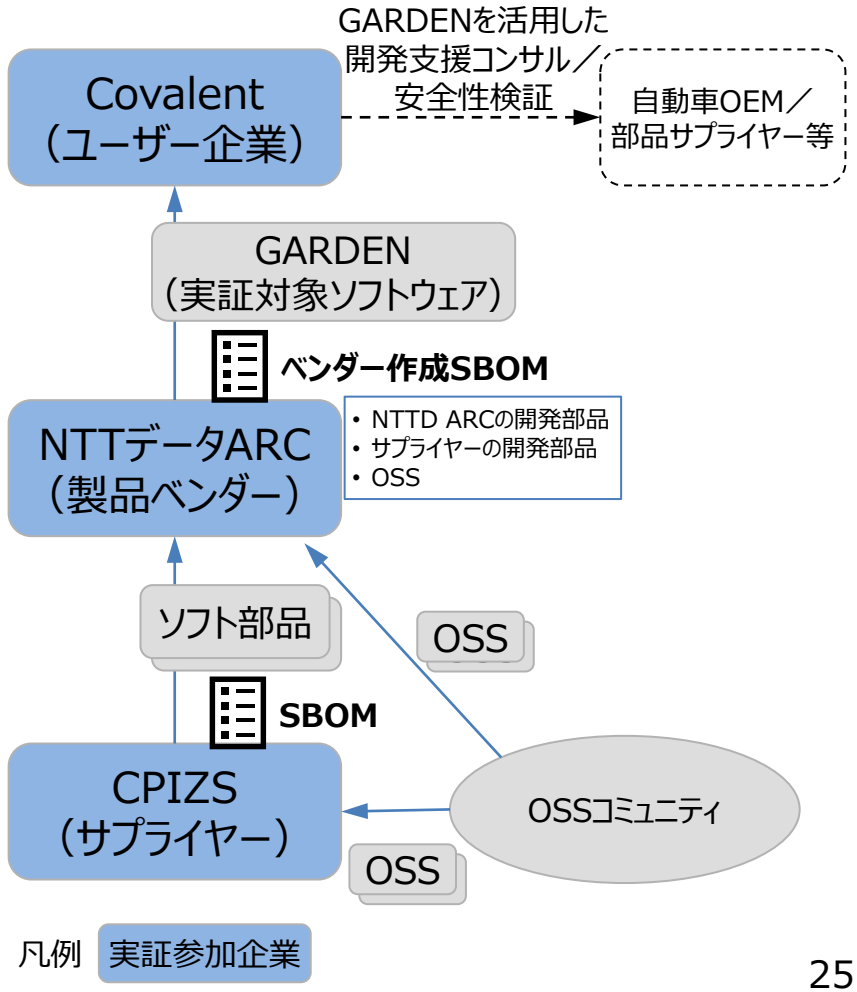
実証対象ソフトウェア 「GARDEN」

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

想定スケジュール

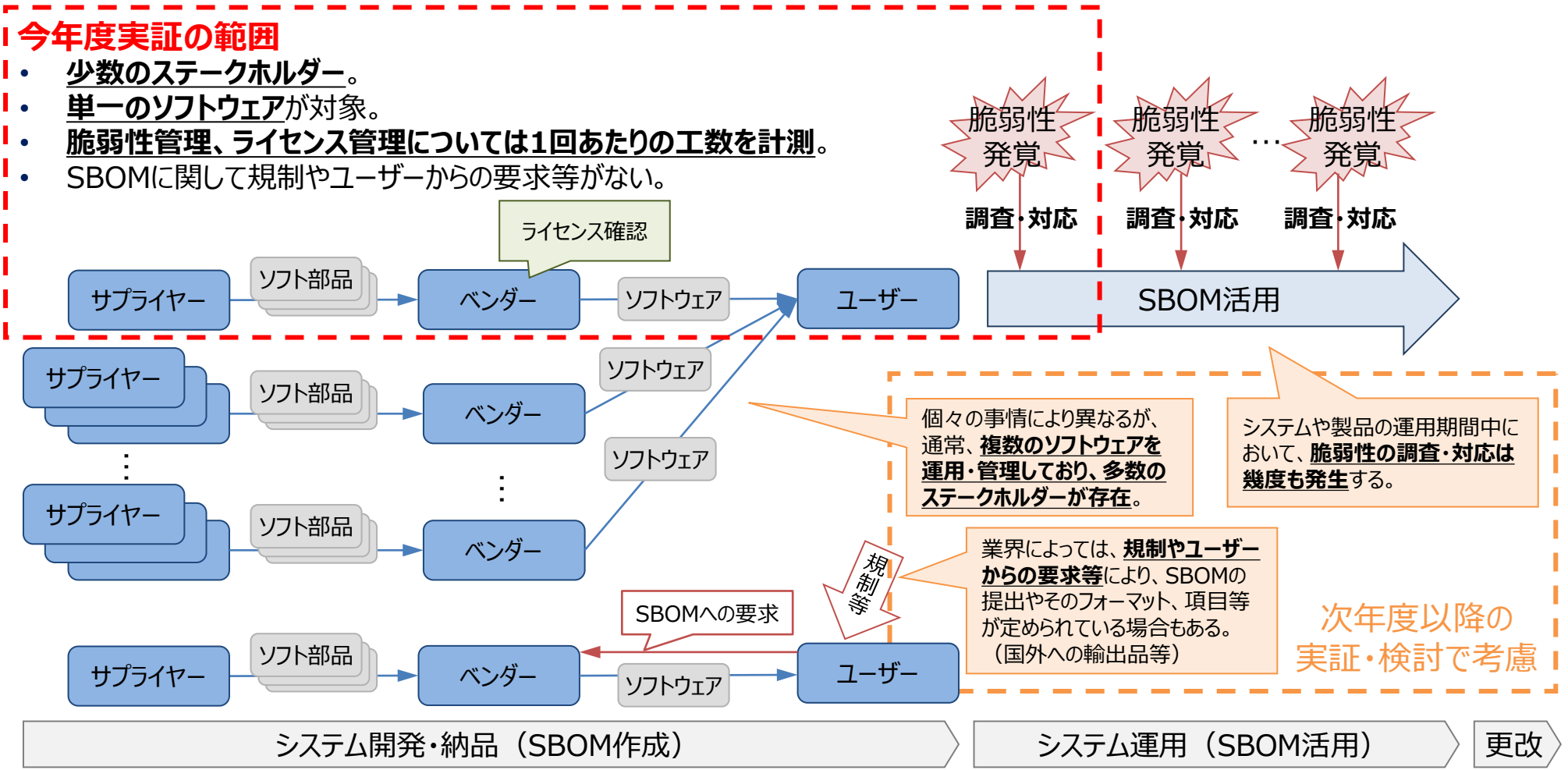


実証体制（GARDENのサプライチェーン）



今年度の実証の範囲

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



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標準への準拠性が高いと思われることから、**SPDX project※1およびNTIA Formats and Tooling WG※2が提供する一覧等から選出**。中小企業への普及も考慮し、**無償のツールと有償のツールの比較**も実施。

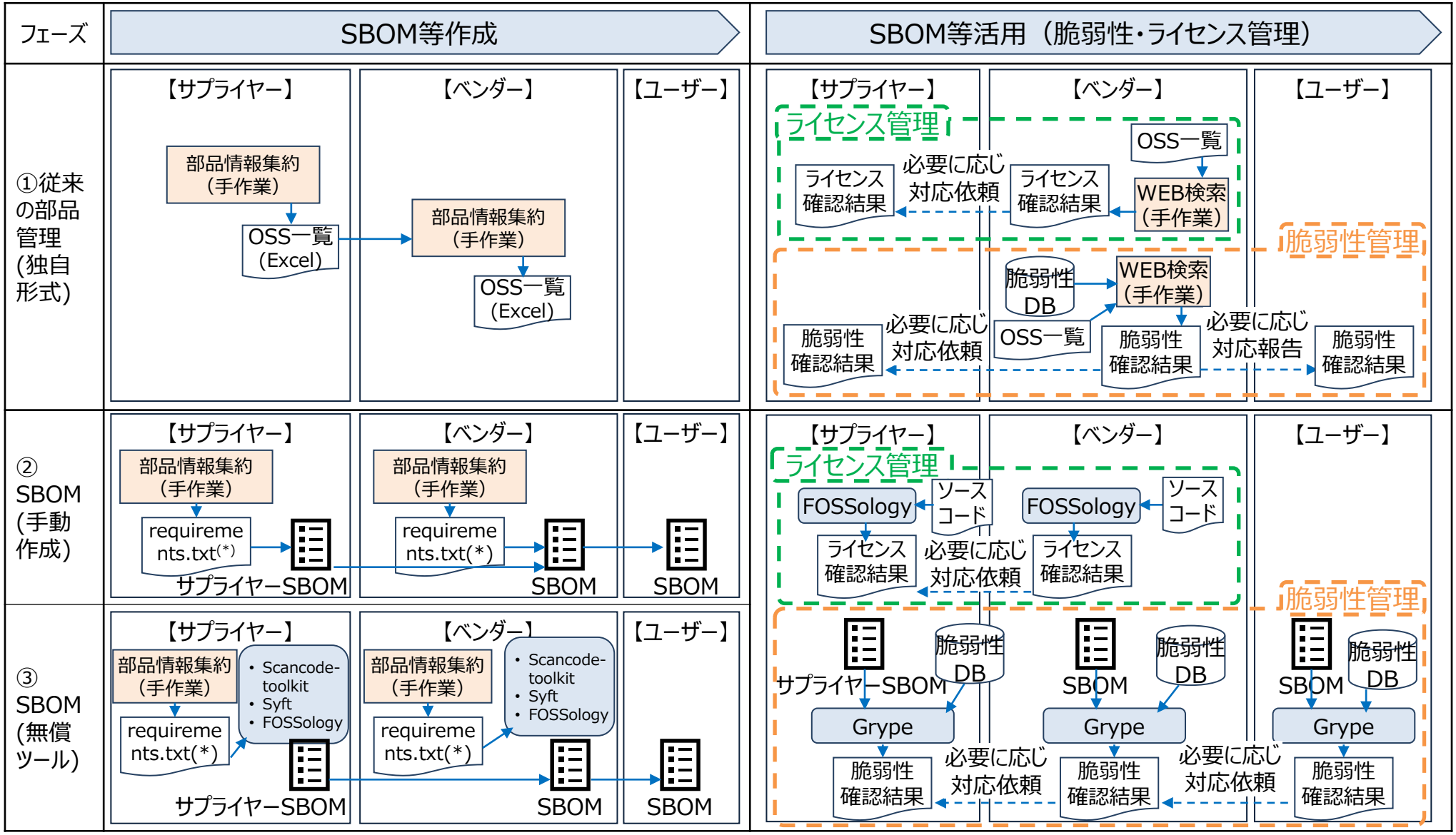
シナリオ	SBOM等（部品情報）の作成	脆弱性管理	ライセンス管理
①従来の部品管理 (独自形式)	ベンダーおよびサプライヤーが、手作業で、Excel独自形式の「OSS一覧」を作成。	NVD等の脆弱性DBの手動検索やニュースはじめとする公開情報収集を通じて脆弱性の発生を確認。	Web検索によりライセンス情報を確認。
②SBOM (手動作成)	ベンダーおよびサプライヤーが、SBOM作成ツールのフォーマットに合わせて手作業で作成。	作成したSBOMを、脆弱性管理ツールに入力して脆弱性の有無を特定。 使用ツール：Grype	SBOMを活用したライセンス管理ツールによりライセンス情報を確認。 （他ツールで作成した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て、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のSBOM作成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区別する。

※1：https://spdx.dev/spdx-tools/
※2：https://ntia.gov/files/ntia/publications/ntia_sbom_tooling_2021-q2-checkpoint.pdf

（参考）本実証における想定シナリオ

- ①～③の想定シナリオは以下の通り。④は1つのツールでユーザーが実施（図は省略）。



(*)ソフトウェアインストールに必要なOSSモジュールが記載。SW自体のデバッグ（インストール可否確認）を通じて記載漏れが検知されるため、部品の記載漏れは開発過程で防止される。

実証におけるコスト・効果に関する計測結果

- 実証により、工数・費用の項目を確認。今回の比較条件では、SBOMは導入のための初期工数（環境整備、学習等）が大きいが、運用工数（SBOM作成、活用）はツールの活用により従来の手作業部品管理に比べ小さい結果となり、**管理対象のソフトウェア部品が多いほど、SBOM導入効果が大きくなると想定**される。
- 脆弱性特定をツールで自動化することで、都度の確認にかかる工数を増やさず確認頻度を多く設定できるため、**脆弱性発表から特定までのリードタイムの短縮と工数の削減に繋がる**と考えられる。

シナリオ	初期工数		運用工数				ツール費用(初期・運用)
	環境整備工数	体制構築・学習工数	SBOM(部品情報)作成工数		脆弱性特定工数	ライセンス特定工数	
			作成工数	精査工数			
①従来の部品管理(独自形式)	1.3人時間 (フォーマットの定義)	0.5人時間 (フォーマット・運用の連携)	3.0分/部品	3.8分/部品 (OSS一覧のレビュー)	6分/部品・回 (頻度:1.5カ月)	10分/部品 *別途法務チェックに2-5営業日	(なし)
②SBOM(手動作成)	102.1人時間 (活用ツール導入・処理調査、テンプレート整備) *全社の合計値	48.2人時間 (SBOM作成方法の学習、作業手順書作成) *全社の合計値	2.9分/部品	(なし) *開発者が手動作成した部品情報が正確と仮定	0分/部品・回 (頻度:即時)	0分/部品 *別途法務チェックに2-5営業日 *ライセンスの検知漏れが発生	
③SBOM(無償ツール)	71.1人時間 (作成・活用ツール導入) *全社の合計値	57.2人時間 (作業手順書作成、学習) *全社の合計値	0.2分/部品	1.4分/部品 (検知結果確認)			
④SBOM(有償ツール)	3.0人時間 (商談、スキャン用アプリ導入)	6.5人時間 (学習、開発元問い合わせ)	0.3分/部品	1.4分/部品(検知結果確認) (81.5分/部品(OSSの依存関係の解析によって新たに検知した部品に関する精査及びベンダー確認))	0分/部品・回 (頻度:即時)	0分/部品 *別途法務チェックに2-5営業日	ユーザー数やデータ量等に応じたライセンス費用が発生

- **管理するソフトウェア部品数が多い場合や脆弱性特定頻度が高い場合等、各シナリオにおいて網掛けした工数が支配的**となる。
- 本実証における部品件数は7件（Pythonのrequirement.txtにより規定されるOSS部品の粒度）。有償ツールでは追加で再利用部品11件を検知。
- **本実証では、工数測定にあたって各ツールの検出精度や対象ソフトウェアの特性は考慮していない。実際に導入を検討する際は、工数だけではなく精度についても検討・評価が必要であり、本事例の計測値をもって直接的にSBOMの有効性を一般化して主張するものではない点に留意**。

（参考）実証でツールにより作成されたSBOMとSPDX仕様等との対応関係

- 本実証において、ツールで作成されたSPDX準拠のSBOMについて、SPDX仕様の主な要素（「Package Information」の23項目等）との対応関係を比較。Black Duckが最も多くの項目に対応。
- 実証に用いたOSS SBOMツールは、SPDXやNTIAの「最小要素（Data Fields）」全てに対応しているわけではないため、各項目の必要性の精査、ツール機能拡張（相互運用性の向上等）の注視、他のツールの選択などについて考慮する必要。
- その他形式のSBOMについては、SPDX仕様との対応関係の特定には至らず。

各ツールから出力されたSPDX形式のSBOMの項目について、SPDXv2.2.1に対応すると考えられる項目に「○」を記載。
※今回の実証ではツール間の機能差を厳密に調査したわけではないため、設定等により結果が変わり得る点に留意。

SPDX項目（主な項目）		米NTIA最小要素	実証で作成したSPDX準拠のSBOMにおける有無		
			Syft	FOSSology	Black Duck
DCI	6.8 Creator	○	△※	×	△※
	6.9 Created	○	○	○	○
Package Information	7.1 Package name field	○	×	×	○
	7.2 Package SPDX identifier field	○	○	×	○
	7.3 Package version field	○	×	×	○
	7.4 Package file name field	○	×	○	○
	7.5 Package supplier field	○	×	×	○
	7.6 Package originator field		×	×	×
	7.7 Package download location field		×	○	○
	7.8 Files analyzed field		○	×	○
	7.9 Package verification code field		×	○	×
	7.10 Package checksum field		×	○	×
	7.11 Package home page field		×	×	○
	7.12 Source information field		○	×	×
	7.13 Concluded license field		○	○	○
	7.14 All licenses information from files field		×	○	×
	7.15 Declared license field		○	○	○
	7.16 Comments on license field		×	○	○
	7.17 Copyright text field		×	○	○
	7.18 Package summary description field		×	×	×
	7.19 Package detailed description field		×	×	○
	7.20 Package comment field		×	○	○
	7.21 External reference field		○	×	○
	7.22 External reference comment field		×	×	×
	7.23 Package attribution text field		×	×	×
Relationship between SPDX Elements Information		○	×	○	○

DCI: Document Creation Information

※ SBOM作成ツール情報／ツールベンダー情報が記載

＜SPDX非準拠のSBOMについて＞

Scancode-ToolkitおよびSyftで出力されたSPDX以外のSBOMの項目と、SPDXその他国際規格との対応関係、および各項目の定義についての情報は公開情報から確認されず。
SBOM生成ツールの開発元に問い合わせを実施したが、対応関係を特定可能な情報取得には至らず。
各社からの回答結果は以下の通り：

【Scancode-Toolkit開発元回答】

- JSON形式で出力されたSBOM上の項目と、SPDXその他国際規格との対応関係は整理していない。
- JSON形式で出力されたSBOM上の各項目の定義につき、文書などは整備していない。

【Syft開発元回答】

- （回答無し）

＜ツール/フォーマットの相互運用性＞

米国でも、ツールやフォーマット間の相互運用性は重要視。複数のツールベンダー等が相互運用性のテストを行うイベントも定期的に開催されている（Plugfest）。
https://www.ntia.gov/files/ntia/publications/ntia_sbom_tooling_2021-q2-checkpoint.pdf

SBOM実証成果（まとめ）

SBOMのメリット等

- ソフトウェア製品のサプライチェーン（サプライヤー、ベンダー、ユーザー企業）において、SBOMの作成、共有、活用（脆弱性管理、ライセンス管理）の一連の実証を行い、**主なコスト・効果の項目を特定**。
- 従来の手作業による部品管理に対し、**SBOMは導入するための初期工数（ツール導入等の環境整備や使用方法習得のための学習等）が大きいが、ツールを活用することで運用（SBOM作成、活用）工数は小さく**なった。
  - 本実証事例では、部品あたりの脆弱性特定、ライセンス管理の工数低減効果から、**部品数が355件以上で、全体として無償のOSSツールを用いたSBOMによる部品管理が手作業による従来の部品管理に比べコストが低減**することを確認。
  - 本実証事例の場合、下記の条件において、ツールを用いたSBOMによる部品管理がコスト面で有効と確認。
    - ✓ 条件１：SBOMツールの初期工数・費用が十分に低い。
    - ✓ 条件２：ツールで作成したSBOMの精度が、手作業による部品管理と同程度。
    - ✓ 条件３：OSS等のサードパーティ部品から再利用される部品管理は対象としない。

    ※条件を満たさない場合、SBOM活用がコスト低減に繋がるとは必ずしも言えない点に留意。
- **SBOMツールにより脆弱性発表から特定までのリードタイムを短縮可能**（手作業の場合は脆弱性特定業務の頻度に依存）。
- 有償ツールでは、**OSSの依存関係を解析し、構成ファイルから特定できなかった、OSSによる他のOSSの再利用も検知**。
- SBOMツールと既存の構成管理ツールを連携させることで、脆弱性の影響範囲特定の工数削減につながる可能性。

確認した課題

- SBOMツールは環境整備や学習に工数が発生。無償ツールはドキュメントやノウハウが不足しており、機能・精度面でも、再利用部品の検知ができない、読み込み可能なSBOMフォーマットに制限がある、ライセンスの検知漏れが発生する等、十分とはいえない。
  - ツールに関する**使用方法、留意事項等のノウハウを整理した日本語ドキュメント整備のような対応**が考えられる他、**ツール自体の精度、機能の向上に期待**。

- 開発者以外がSBOMを作成する場合、ツールにより検出されるOSSの再利用やソースコード改変部品などの精査に係る工数が大きくなる、もしくは精査が困難。開発者自身が認識していない部品が検出された場合の管理責任が曖昧になり得る。
  - **開発者（ベンダーやサプライヤー）自身がソフトウェア部品を特定し、標準的なSBOMフォーマットで共有することが、サプライチェーン全体における部品管理の効率化や責任の明確化につながる**と考えられる。

SBOMに関する取組のヒアリング

- SBOM活用の取組に関して**実態を確認するため、委員の所属企業に対しヒアリング**を実施。
- 共通的な課題として、**「SBOM共有のためはフォーマットや部品粒度等を揃える（要件化する）必要」「委託先やOSSの再帰的な利用（OSSによる他のOSSの再利用等）を含めてSBOM管理を徹底する場合のコストが大きい」**などが挙げられた。

ヒアリング先	取組概要	課題
トヨタ自動車	● 著作権法やライセンス規約への準拠のため、OSSを使用している一部のECUについて、SBOM管理を実施。 ● 部品サプライヤーの理解を得て、部品情報の提供を契約で規定し、脆弱性の管理にも活用している。	● 事業者間で**SBOMを共有するためには、部品の粒度を揃えることが必要**。 ● ライセンス準拠等に関する部品サプライヤーの責任を明確化しているが、Tier2以下については、部品情報が網羅されているか確認することが難しい。
日本電気（NEC）	● OSSについては、SBOM相当の部品管理を実施。 ● 委託先に対するSBOMの要件化はできていないが、OSSの利用申告は規定している。	● **サプライチェーンで部品粒度を整合化しなければ非効率**。 ● **スニペットなど、SBOMツールは検出精度に課題が**あったことから、十分に比較検証を行った上でツールを選定。 ● **OSSの再帰的な利用も含めた厳格な検査はコスト的に困難であるが、改善について継続的に検討**を実施している。 ● 委託先開発部分やOSS利用も含め、完全な管理は難しいが、最終製品ベンダーとしての責任において適切な対応を模索中。
富士通	● 脆弱性管理、ライセンス管理を目的にSBOMを導入。 ● 厳格にSBOMを管理運用する場合コストが非常に高額となるためビジネスインパクトに応じて簡約している。 ● 直接の取引相手とはSBOMを共有しているが、サプライチェーン全体でほとんど共有はできていない。	● **再帰的なOSS利用も含めた解析も可能な限り実施しているが**、様々な形態の製品/サービスを社内/社外向けに提供しており、それら**すべてのビジネスタイプにおいて徹底することはコスト的に困難**。 ● また、ビジネスタイプによる**フォーマットやプロセスの違いから、サプライチェーン全体で特定のSBOMフォーマットを要件化できず、共有の障害となっている**。 ● 契約にSBOMの瑕疵責任を規定しても、最終的な責任は最終製品ベンダーにあり、レピュテーションリスクを考慮すれば**SBOMの検査は受入側でやらざるを得ない**。

今後の課題（案）

- SBOM実証および各企業へのヒアリング結果、タスクフォースにおける議論、国内外の動向等を踏まえ、今後の課題を下記のように設定してはどうか。

令和3年度のSBOM実証および各企業へのヒアリング結果

- SBOM導入のための初期工数は発生するが、ツール活用により運用工数が低減。**管理対象のソフトウェアが多いほど効果が大きく**なり得る。
- ツールによる**脆弱性特定のリードタイムの短縮効果**を確認。
- 特に無償ツールは導入工数が大きく機能・精度も不十分。**ノウハウ共有**や**ツール自体の精度、機能向上**が必要。
- 開発者自身が**標準的なSBOMフォーマットで部品情報を共有**することが有効だが、**部品粒度等を揃える（要件化する）必要**。
- OSSの**再利用等も含め管理する場合のコスト**（精査工数等）が大きい。
- **管理対象のソフトウェアやステークホルダーが多い場合の実証**や、**繰り返し発生する脆弱性対応工数の評価**は未実施。

タスクフォースにおける議論（抜粋）

- **効果・コスト評価**（複数社の連携、システム規模の差、SBOMの更新）
- SBOM共有時の**コストや責任の分担**、**契約の整理**
- **自動化・ツール**（費用、精度、信頼性、相互運用性）
- メリットを享受できる**活用モデルの検討**
- **脆弱性の対応要否判断**
- **SBOMフォーマットや必要項目、管理単位、粒度の整理、標準化**
- **中小企業**への配慮、巻き込み
- **ノウハウの共有**（プラクティス集、ガイドライン）
- **政府機関での活用**（実証の実施、政府統一基準）

国内外の動向等

- 大統領令に基づき、米国政府調達におけるSBOM提供の**義務化に向けた動き**が進展。**SBOMの最小要素**公表。
- CISA SBOM a ramaでは、今後の主要な課題が抽出。（SBOM生成に必要な**データの提供方法**、SBOM共有・活用**ツール**、**各国の規制基準**への適用、SBOM**共有にあたっての信頼性や完全性**の確保 等）
- **医療機器分野では、IMDRFガイダンスに基づき、国内でも規制改正によるSBOM提供義務化**の動き。

今後の課題

1. SBOM活用モデルの最適化

- SBOMの作成主体や作成対象範囲、作成手段等によりコストや効果が異なり、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

- **多数のステークホルダーがSBOMを共有・活用するケースの実証**。
- 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. 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**。
- ツール自体の**機能および精度向上**。

4. 国際的な基準との整合性確保

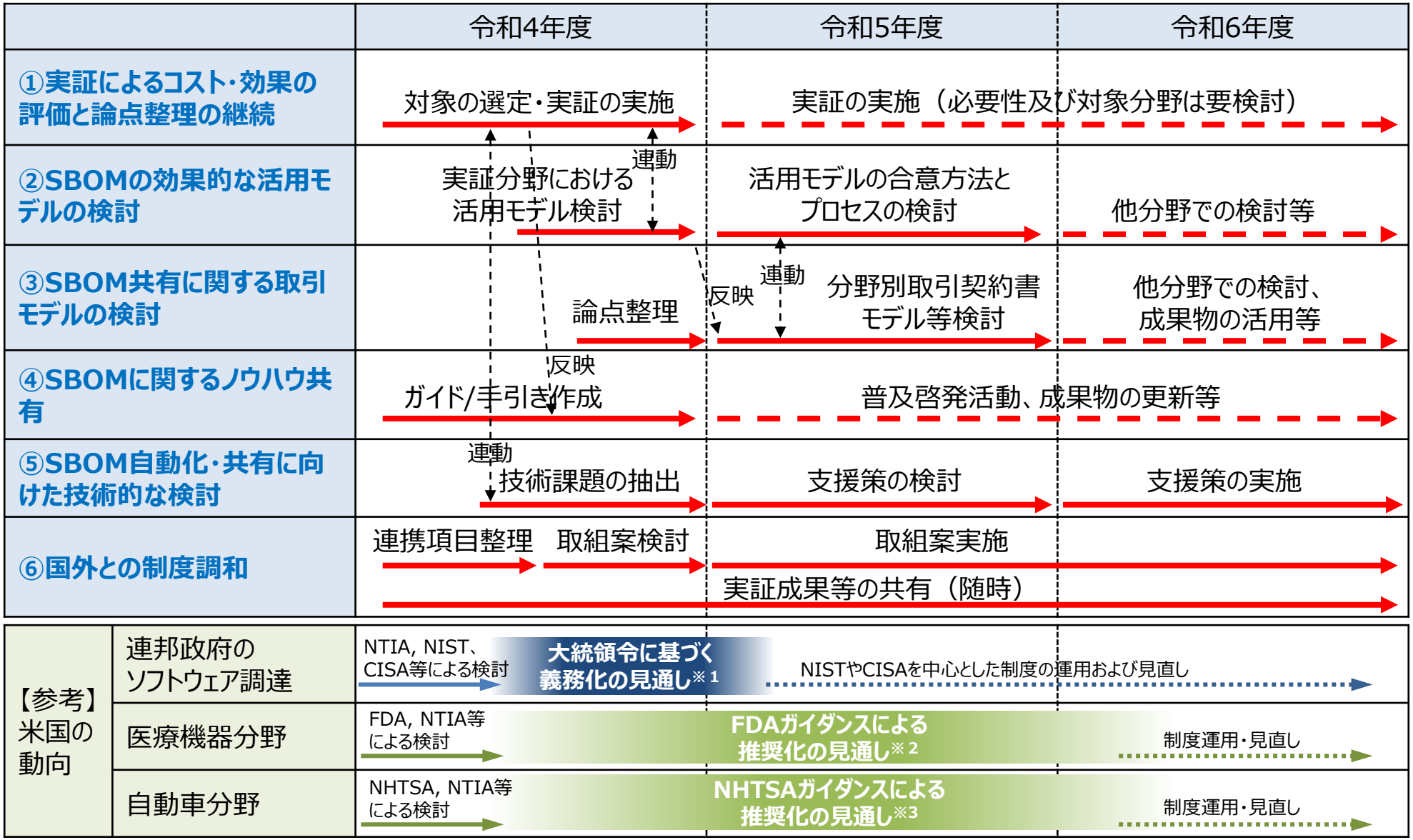
- グローバルサプライチェーンにおいて国内と海外の整合性を確保しつつ効率的に部品管理を行うためには、**国内外の基準の整合化**が必要。

来年度以降の取組（案）

- 前頁で設定した課題から、次年度以降の取組を下記のように整理してはどうか。

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

スケジュール（案）

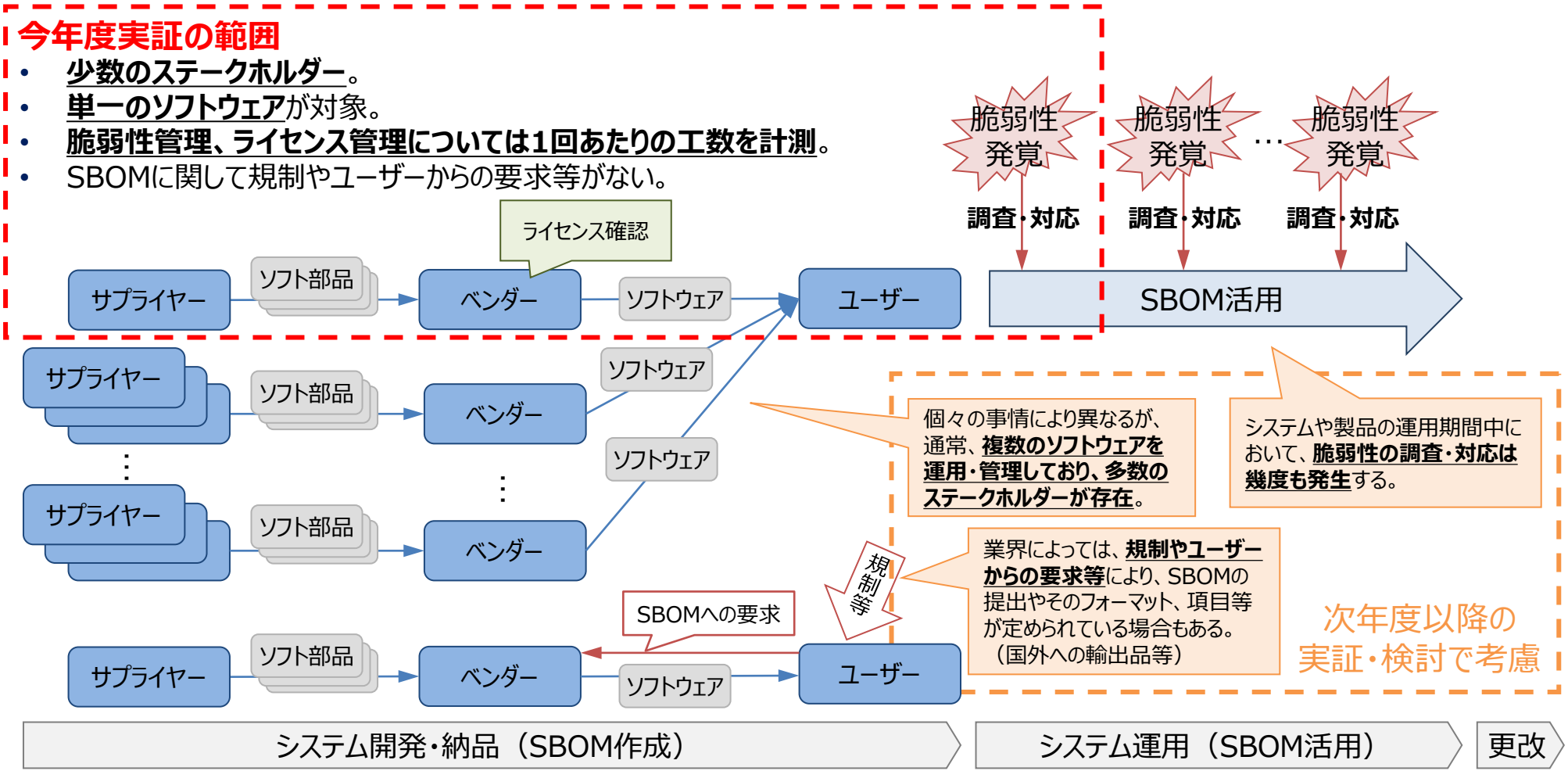


※1：Executive Order on Improving the Nation's Cybersecurity, MAY 12, 2021
※2：FDA, Draft Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Oct, 2018
※3：NHTSA, Draft Cybersecurity Best Practices for the Safety of Modern Vehicles, Jan, 2020

今年度の実証の範囲（再掲）

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

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



SBOM活用モデルの検討イメージ

- SBOMの作成・活用においてコストや効果に対する影響の大きい選択肢を整理し、実証の対象分野における妥当な組合せを検討。実証による評価を通じて活用モデルを整理。

STEP1　SBOM活用モデルの検討における選択肢の整理

＜整理例＞

区分	選択肢（コスト・効果への影響が大きいものを想定）
(a) 作成主体	(a1)ベンダーのみ
	(a2)ベンダー＋サプライヤー（受託開発）
	(a3)ベンダー＋サプライヤー（受託開発）＋サプライヤー（既成部品ベンダー、サードパーティ・OSSベンダーを含む。）
(b) 対象部品	(b1)直接利用する部品のみ（ビルドツール、構成ファイルなどを利用できる）
	(b2)間接的・再帰的に利用する部品まで（商用ツール利用が前提か）
(c) 作成手段	(c1)手動で特定・作成
	(c2)ツールで作成・精査無し
	(c3)ツールで作成・手動で精査
(d) データ形式・項目	(d1)標準フォーマット（SPDX、SPDXLite等）
	(d2)大統領令最小要素を含む
	(d3)上記を満たさない
(e) 活用の範囲	(e1)脆弱性の特定
	(e2)脆弱性の深刻度評価
	(e3)ライセンスの特定

STEP2　各分野における妥当な組合せを検討

＜考慮事項の例＞

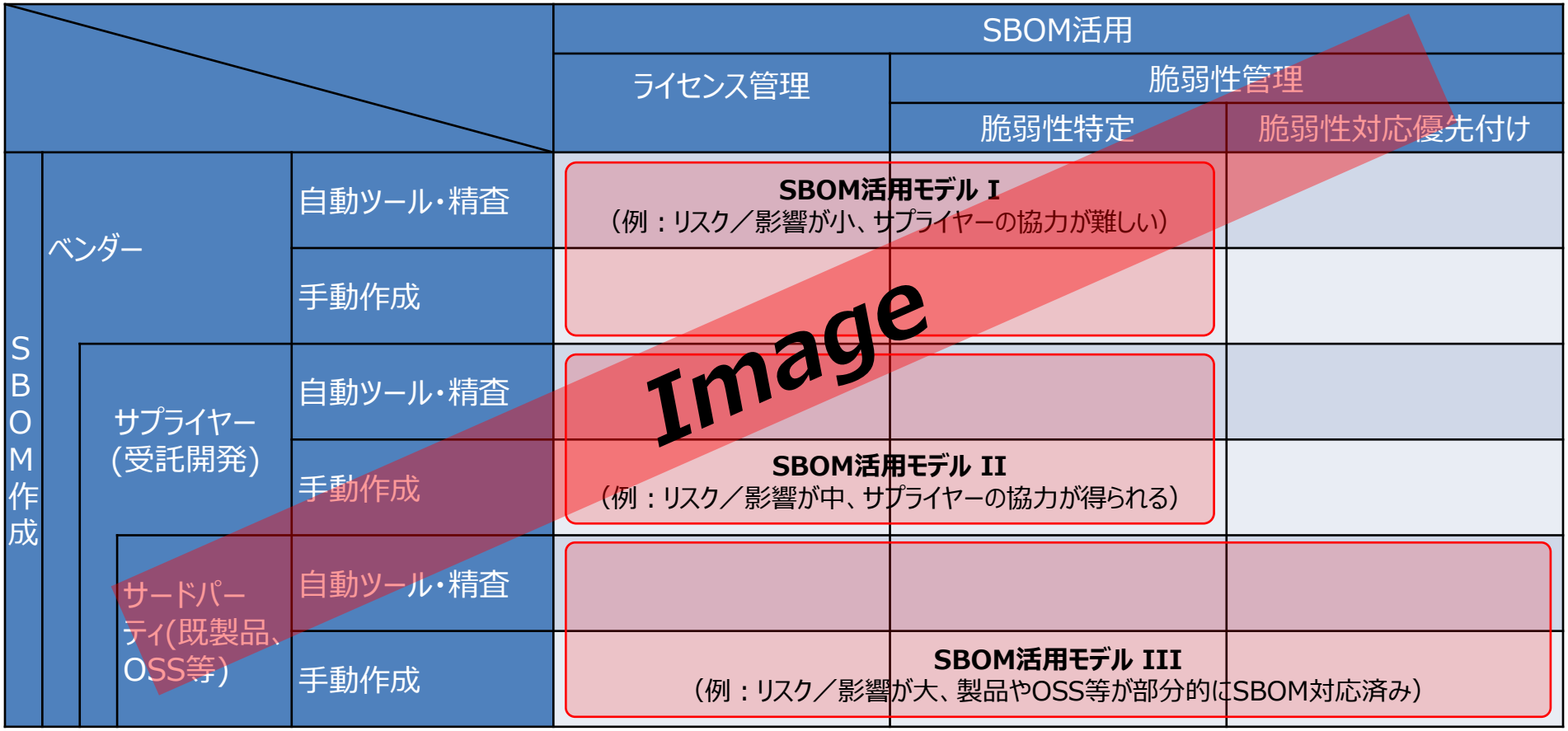
- 規制等における要求事項
- サプライチェーン構造や商慣習
- リスクの大きさ　　等

STEP3　実証による評価

- 実証におけるSBOM活用のシナリオを設定。
- 各分野、各シナリオにおけるコスト、効果を評価。
- **評価結果を踏まえ、各分野における効果的、効率的なSBOM活用モデルを整理**。

SBOM活用モデルの検討イメージ

- SBOM活用モデルの選択肢の整理、実証での評価結果をもとに、各分野における効果的、効率的なSBOM活用モデルについて、例えば下表のように分類、整理することを想定。



※ SBOM作成の手動、自動の効果は、それぞれ一長一短があり、一方が全面的に良いわけではない。