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５年２月２８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. ソフトウェアの管理手法等に関する国内外の動向

2. SBOM実証の結果等（全体概要）

3. 実証結果等を踏まえた検討

①初級者向けSBOM導入手引の要点
②SBOM対応モデルの要点
③SBOM取引モデルの要点

4. 今後の取組課題等

【米国】サプライチェーンセキュリティ保護に関するガイダンス（3部作）の発表

- 2022年、CISA、NSA、ODNIは共同で、**ソフトウェアサプライチェーンのセキュリティ保護に関するガイダンスを発表**した。
- ガイダンスは3部作であり、**ソフトウェア開発者向けの第1部**を9月、**ソフトウェアサプライヤー向けの第2部**を10月、**ソフトウェア消費者向けの第3部**を11月にそれぞれが発表した。
- 本ガイダンスシリーズでは、**安全なソフトウェアサプライチェーンを確保するための各役割に対する推奨事項が整理**されており、具体的にはSBOMの作成・要求、脆弱性の管理・対処・報告等が推奨されている。

安全なソフトウェアサプライチェーンの確保のための推奨事項（一部抜粋）

ソフトウェア開発者向けの推奨事項（第1部）

- **安全なソフトウェアの基準と管理**
  セキュリティに焦点を当てた原則とガイドラインを確保するためのポリシーを策定する。
- **セキュアコードの開発**
  安全な開発手法を実践し、使用するOSSの管理や脆弱性情報の取得・評価を実施する。
- **サードパーティコンポーネントの検証**
  SBOMを作成し、更新する。また、コンポーネントの脆弱性管理や対処を実施する。
- **ビルド環境のハード化**
  外部ネットワークからの保護やデータ漏洩の管理等によるビルド環境のセキュリティ対策を実施する。
- **安全なソフトウェアの提供**
  配信システム（リポジトリ）に対するセキュリティ対策を実施する。また、消費者への納品前に最終パッケージを検証する。

ソフトウェアサプライヤー向けの推奨事項（第2部）

- **安全なソフトウェアを提供するための組織の構築**
  安全なソフトウェアを提供するため、必要な基準やプロセスを確立し、実施する。プロセスには、脆弱性対応やサポート期限に関する情報を消費者へ通知する内容を含める。
- **ソフトウェアの保護**
  アクセス制御やデジタル署名によって、ソフトウェアへの不正アクセスを防止し、完全性を担保する。
- **安全性の高いソフトウェアの提供**
  サードパーティのソフトウェアが、セキュリティ要件を満たすかを確認し、脆弱性の存在を解析する。
- **脆弱性への対応**
  既知の脆弱性が消費者へ提供されるソフトウェアに存在しないことを保証するため、ソフトウェアの脆弱性テストを実施し、必要に応じて脆弱性を取り除く。また、継続的に、セキュリティに関する情報を消費者へ通知する。

ソフトウェア消費者向けの推奨事項（第3部）

- **ソフトウェアの調達**
  ソフトウェアセキュリティ、サプライチェーンリスク管理（SCRM）に関する活動をサプライヤーへ要求し、評価する。また、サプライヤーによる安全性の自己適合証明（提出物にはSBOMを含める）を要求する。
- **ソフトウェアのデプロイメント**
  SBOMと取得したソフトウェアを照合する等で、ソフトウェアが調達前の評価と同一であるかを確認する。また、テスト環境の多層防御、ログの管理等により、ソフトウェアの統合プロセスにおける脅威を軽減する。
- **ソフトウェアの運用**
  バグや異常を報告（サプライヤーへの通知を含む）する体制や仕組み（例：ヘルプデスク、SOC）を構築し運用する。また、ソフトウェアアップデート時に発生するセキュリティリスクに対処するため、SBOMの自動更新を実現する。

出所）CISA, NSA, ODNI, ”Securing Software Supply Chain”
https://www.cisa.gov/uscert/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF
https://media.defense.gov/2022/Oct/31/2003105368/-1/-1/0/SECURING_THE_SOFTWARE_SUPPLY_CHAIN_SUPPLIERS.PDF
https://media.defense.gov/2022/Nov/17/2003116445/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_CUSTOMER.PDF

1. ソフトウェアの管理手法等に関する国内外の動向

2. SBOM実証の結果等（全体概要）

3. 実証結果等を踏まえた検討

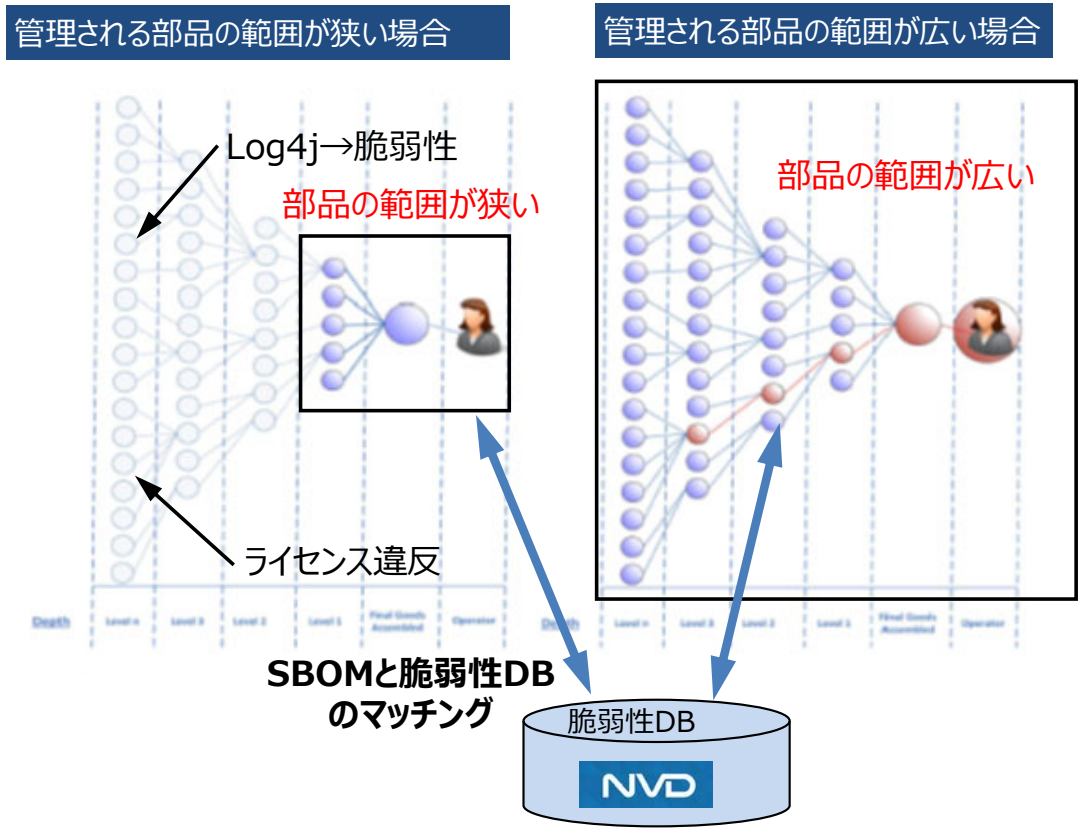
①初級者向けSBOM導入手引の要点
②SBOM対応モデルの要点
③SBOM取引モデルの要点

4. 今後の取組課題等

SBOM実証の目的（ソフトウェア部品管理に係る問題認識）

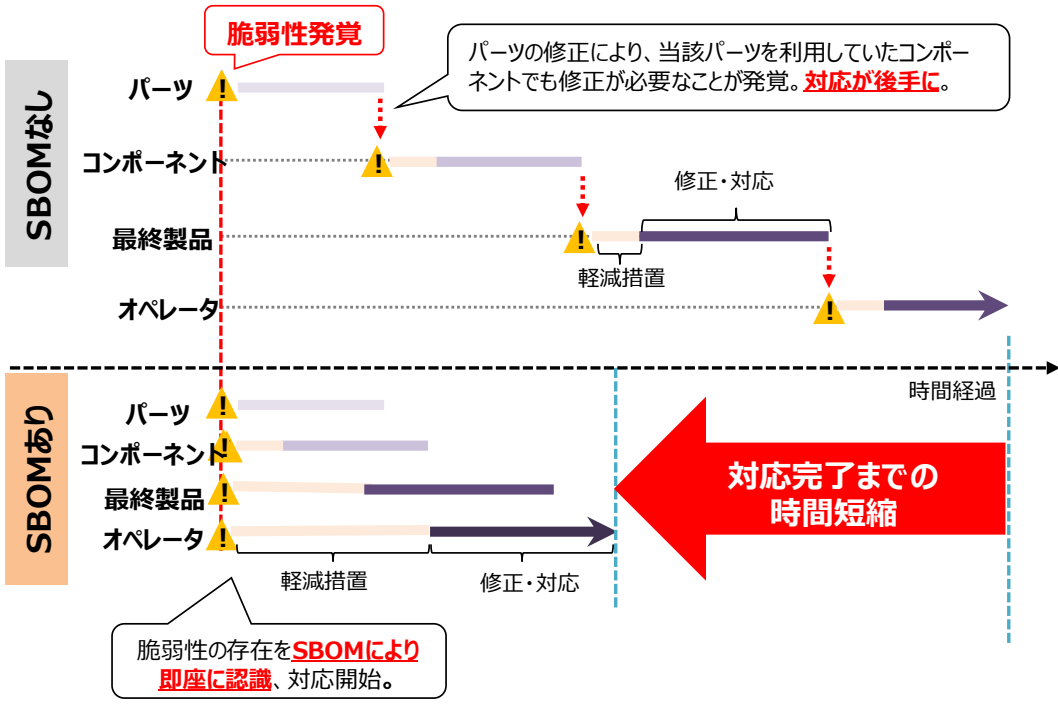
- 公開される脆弱性情報について、自社のソフトウェアがその影響を受けるのか効率的、迅速に特定するためには、自社およびサプライヤーの部品情報を共有・管理することが重要である。
- SBOM実証により、ソフトウェア管理を効率化するためのフィージビリティ、課題、ノウハウ等を整理する。

サプライチェーンを通じた脆弱性特定のカバレッジ課題



- 管理する部品の範囲が広い程、脆弱性管理によるリスク低減効果は大きい
- SBOMを単に使っているかではなく、どこまで管理しているかによって効率的に特定できる脆弱性の範囲は全く異なることに留意。

サプライチェーンを通じた脆弱性対応の所要時間の課題



- サプライチェーンを通じてSBOMを共有し、脆弱性情報のマッチングを効率化・自動化できれば、コスト低減が図れるとともに、脆弱性の対応期間短縮できる。
- SBOMにより脆弱性管理を効率化し、対応期間を短縮する程、コスト低減効果、リスク低減効果は大きい。

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

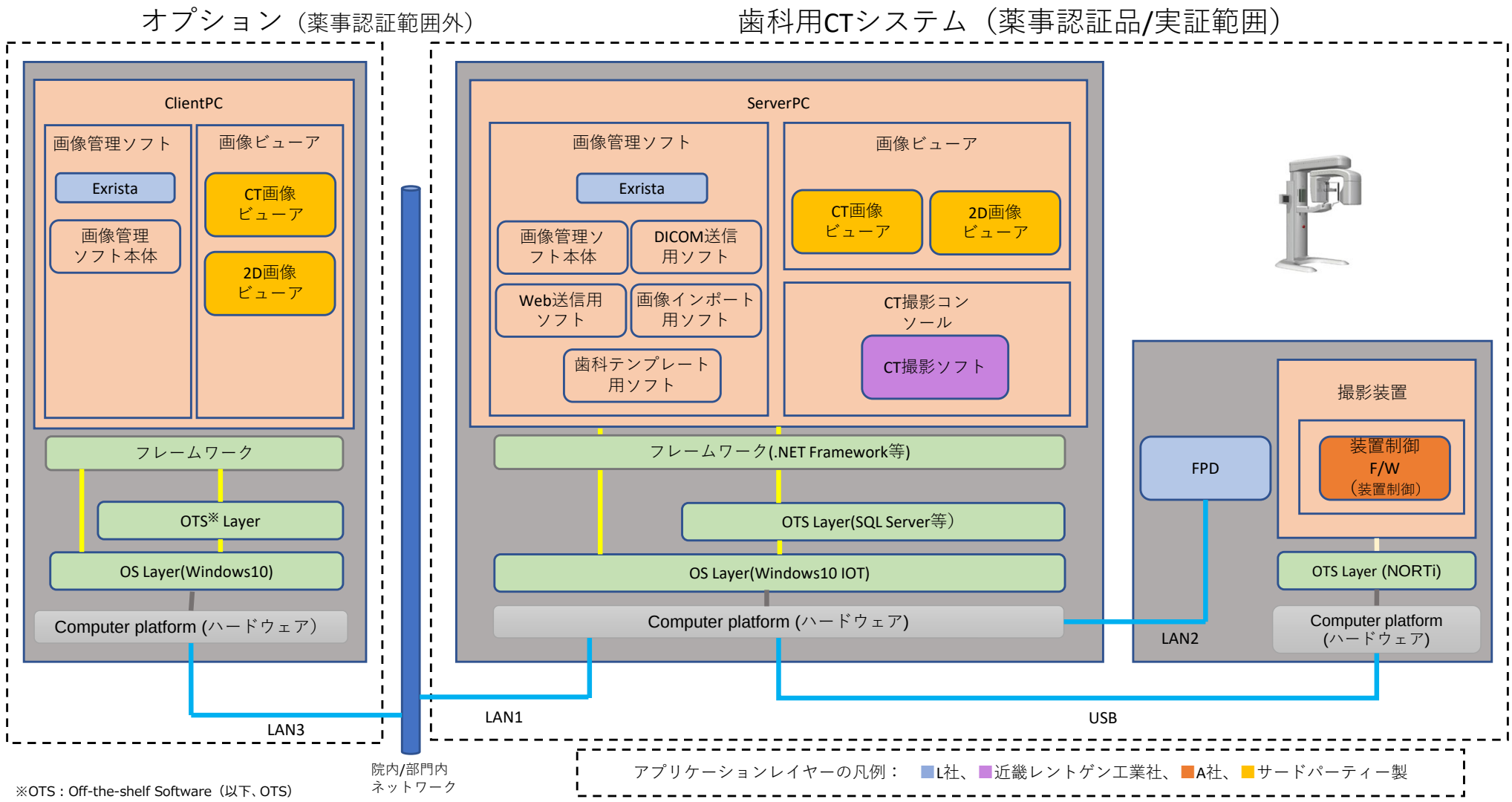
– 産業分野ごとのリスク、法制度に応じて、SBOMを用いた部品のリスク管理を効果的に行うための方法についてコスト・効果の比較評価を行い、現実的な適用範囲と課題について整理する。
– 実証を通じて、初級者向けSBOM導入ガイダンス、SBOMの適用範囲を例示するSBOM対応モデル、取引契約の例示によりSBOM導入を促進するSBOM取引モデルの主な契約事項を整理することを目的とする。
– 法的な要件化が進む医療機器分野、自動車分野および、効果が期待できるソフトウェア分野について、実ソフトウェアに対するサプライチェーンを考慮した体制により、評価を行う。

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：東京大学医学部附属病院 企画情報運営部 新秀直先生	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

SBOM実証対象システムの例（システム構成）

- SBOM作成・活用にあたり、対象範囲の明確化は、ツールを適用するファイル群の特定やリスク管理の網羅性の観点で重要



（資料）実証企業株式会社近畿レントゲン工業社作成

分野ごとの前提条件（法制度、取引慣行、開発環境等）の整理

- 産業分野の法制度、取引慣行、開発環境についてSBOMに対する前提状況や要件が異なるため整理する。

前提等	医療機器分野	自動車分野	ソフトウェア分野（情報系）
サプライチェーンの構造	• ソフトウェアの委託開発は一段階層程度が多い • サードパーティ部品（既製品）の構成管理が義務化されており、OSSは対応の困難さから避ける傾向がある。（※ただし、AI/MLを搭載したプログラム医療機器等ではOSSは少なからず利用あり。）	• サプライチェーンは多段階層も多く、中小、海外も含めて裾野が広い。 • サプライチェーンを通じたCSMSが要件化されており、サプライヤに対してもリスク管理のエビデンスが求められる（ISO/SAE21434）。	• 商用、OSS等のサードパーティ部品を使うケースも多い。 • パッケージソフトのサプライチェーンの階層は浅い • 情報システム構築では、多段階層のサプライチェーンも多い。
規制、法制度	• IMDRFガイダンスや米国FDAの市販前ガイダンス案において、既成ソフトウェアコンポーネントに関する機械判読可能なSBOMの生成・提出を推奨。 • IMDRF追補SBOMガイダンス案においてSBOMを推奨化しており、日本もそれに整合する方向性。 • 構成管理は医療機器の基本要件基準第12条第2項の適用。第3項にサイバーセキュリティ要件新設予定。 • 業の許認可がある。	• 日欧など型式認証で要求される国連協定規則UN-R155から参照されるISO/SAE21434では、構成管理が要求され、例としてソフトウェア部品表の作成が挙げられる。 • 米国NHTSAガイダンス(2021年)により、OEMやサプライヤーに対して、ECUや各車両のソフトウェアに関するSBOMの作成・維持が推奨される	• 米国大統領令に基づき、連邦政府のソフトウェア調達においてSBOMを開示等することが義務化される見通し(2022年度内)。
開発対象・開発環境等	• C/C++が多く、アセンブラ、Java、Pythonも利用実績あり。 • AI/MLを搭載したプログラム医療機器ではOSS利用もあり。 • Nessus（脆弱性チェックツール）がFDA対応でよく用いられる。	• 制御系でC/C++/アセンブラが多い。 • 情報系でOSSの利用増加が見込まれる • ECUの場合、納品はバイナリ/ソースコードの両ケースがある。 • 構成管理ツールとして、Git, Subversionなど利用するケースがある。	• Java, C/C++, Python、JavaScriptなどを含め多様な開発言語 • SaaS等のクラウドやオンプレミスなど • ビルド・構成管理ツールはJenkins,GitHubなど、開発環境は, VisualStudio, Eclipseなどが多い
取引慣行・契約	• 開発委託、保守委託が多い。 • 市販後は修理業が対応する場合もある。	• 請負契約、準委任契約など各種存在。 • OSS使用については報告を要件化する場合あり • 脆弱性の監視と連絡を要件化する場合あり	• ユーザ向けライセンス契約あり • 将来の部品情報、SBOMの提供は要件化の有無は両ケースあり
実証の論点	• サードパーティの再帰的な利用部品などの精度の高いSBOM作成 • 脆弱性管理プロセスへの対応における課題	• 商用部品、OSS等のSBOMの現実的な生成範囲 • サプライチェーンを通じたSBOM共有と迅速な脆弱性対応	• 商用部品、OSSのサプライヤーに依存しないSBOM作成 • 開発環境、開発言語のSBOMツールへの影響

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を行った。

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	—	●	●	

1. ソフトウェアの管理手法等に関する国内外の動向

2. SBOM実証の結果等（全体概要）

3. 実証結果等を踏まえた検討

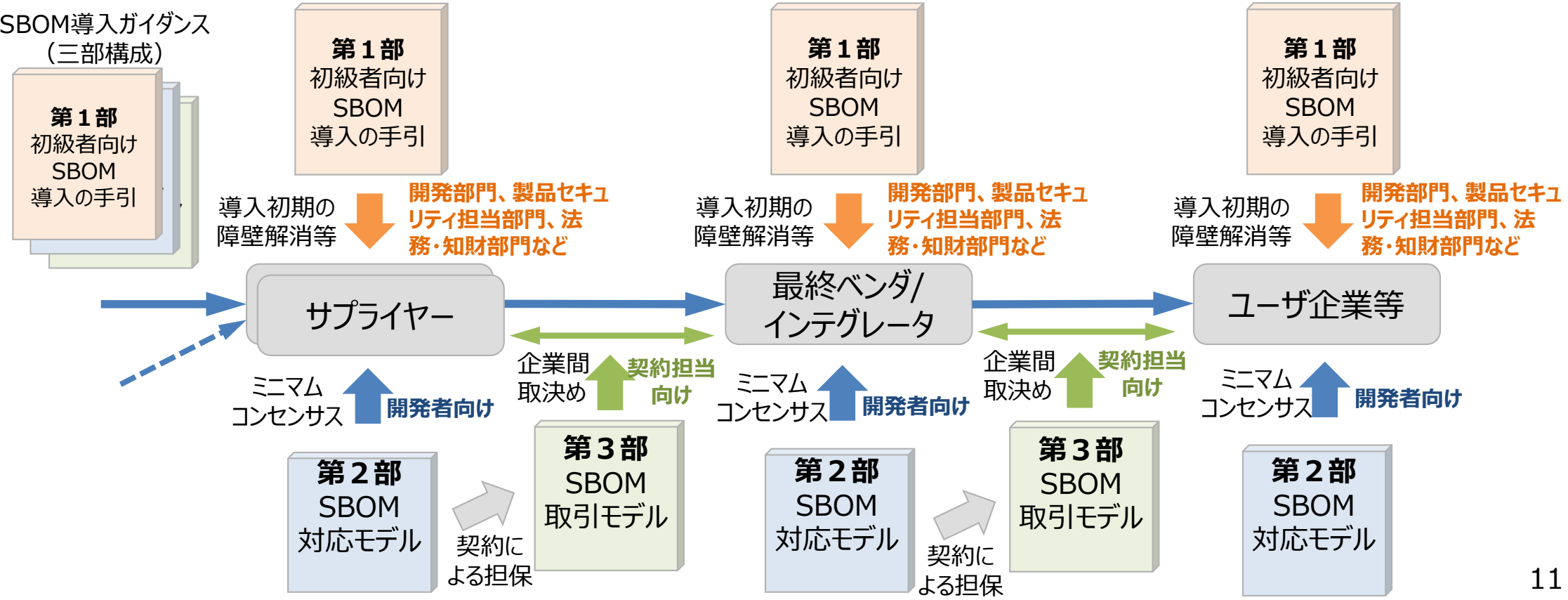
①初級者向けSBOM導入手引の要点
②SBOM対応モデルの要点
③SBOM取引モデルの要点

4. 今後の取組課題等

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。
- 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かなものとする。

SBOM導入ガイダンスは、以下の３部から構成する。
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
※　Ver1.0として第１部を盛り込みつつ、第２部、第３部は整理・検討後、Ver2.0に盛り込む予定。



①初級者向けSBOM導入手引の要点

①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。

①初級者向けSBOM導入手引　経営者へのメッセージ

SBOM導入が求められる背景｜ソフトウェア・サプライチェーンに対する脅威の増大

- 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、**ソフトウェアに対するセキュリティ脅威が近年増大**。2021年12月に発見されたApache Log4jの脆弱性は世界中に影響を及ぼしたほか、ある調査※1によれば、2019年から2022年にかけてのソフトウェア・サプライチェーン攻撃の年平均増加率は742%であった。
- **ソフトウェアに対するセキュリティ脅威は企業経営へ大きな影響を及ぼす**。グローバル企業を対象としたある調査※2では、SolarWindsのサイバー攻撃の影響を受けた企業は、平均して年間収益額の約11%の損害を被ったというデータもある。
- ソフトウェアに対するセキュリティを強化し、企業の信頼・安全につなげていくためには、ソフトウェアを適切に管理していくことが重要。

SBOMの概要・メリット

- このようなソフトウェア・サプライチェーンに対する脅威の状況に対し、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。
- **SBOMとは、ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト**のことで、**世界的に導入企業が増加**している。
- SBOM導入による代表的なメリットとして、**ソフトウェアにおける脆弱性管理のメリット、ライセンス管理のメリットがあり、その結果、開発生産性向上のメリットが得られる**。
- 特に脆弱性管理のメリットに関して、医療機器を対象とした実証では、**SBOMを活用した場合に要する工数が手動での脆弱性管理と比較して30%程度に低減**されたところ、**SBOMを活用したソフトウェア管理によって、脆弱性対応にかかるコストの低減や脆弱性残留リスクの低減が期待**される。
- 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。

手引の目的

- 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、企業の効率的・効果的な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SBOM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のソフトウェアサプライヤーにおけるソフトウェア設計・開発部門、製品セキュリティ担当部門 (PSIRTなど)
  （このうち、特にSBOM初級者を対象）

※1: Sonatype, “8th Annual State of the Software Supply Chain Report”
※2: IronNet, “2021 Cybersecurity Impact Report”

①初級者向けSBOM導入手引　環境構築・体制整備フェーズの概要

- 環境構築・体制整備フェーズでは、対象ソフトウェアに関するSBOM適用範囲を明確化した上で、活用するSBOMツールを選定する。
- SBOMツールの導入・設定を行った後、SBOM作成に向け、SBOMツールに関する学習を行う。

フェーズ 1　環境構築・体制整備フェーズ

ステップ	SBOM導入に向けた実施事項	SBOM導入に向け認識しておくべきポイント
1-1: SBOM適用範囲の明確化	□ 対象ソフトウェアの開発言語、コンポーネント形態、開発ツール等、対象ソフトウェアに関する情報を明確化する。 □ 対象ソフトウェアの正確な構成図を作成し、SBOM適用の対象を可視化する。 □ 整理した情報に基づきSBOM適用範囲を明確化する。 等	● 組織内外の開発者の知見を活用することで、対象ソフトウェアに関する効率的な情報収集を行うことができる。 ● 対象ソフトウェアの正確な構成図を作成し、SBOM適用の対象を可視化することで、リスク管理の範囲を明確化することができる。
1-2: SBOMツールの選定	□ 対象ソフトウェアの開発言語や組織内の制約を考慮したSBOMツールの選定基準を整理する。 （選定基準の例：機能、性能、解析可能な情報、コスト、対応フォーマット、OSS解析方法、サポート体制、他ツールとの連携、提供形態、開発言語、日本語対応等） □ 整理した基準に基づき、複数のSBOMツールを評価し、選定する。	● 単一のSBOMツールを選定することが効果的である。 ● 有償のSBOMツールは一般に高価である一方で、無償のSBOMツールは、ツール自体のコストは無料であるものの、環境整備や学習にあたっての情報が不足しているおり、導入・運用に大きな工数を要する可能性がある。 ● 有償のSBOMツールと比較して、無償のSBOMツールの機能・性能は一般に劣後する。
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。 □ ツールの取扱説明書やREADMEファイルを確認して、SBOMツールの導入・設定を行う。	● サポート体制が整備されている有償のSBOMツールにおいては、販売代理店やツールベンダに対して問い合わせを行うことで、効率的にツールの導入・設定を行うことができる。 ● 無償のSBOMツールでは、ツールの構築や設定に関する情報が不足している場合があるため、試行錯誤的に設定を行うことが効果的である。
1-4: SBOMツールに関する学習	□ ツールの取扱説明書やREADMEファイルを確認して、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。	● サポート体制が整備されている有償のSBOMツールにおいては、販売代理店やツールベンダに対して問い合わせを行うことで、効率的にツールの使い方を習得することができる。 ● サンプルSBOMの作成等を通じて試行錯誤的にツールの使うことで、効率的にツールの使い方を習得できる。

①初級者向けSBOM導入手引　SBOM作成・共有フェーズの概要

- SBOM作成・共有フェーズでは、SBOMツールを活用してコンポーネントを解析した後、実際にSBOMを作成する。コンポーネントの解析結果には誤検出や検出漏れが含まれる可能性があるため、内容を確認する必要がある。
- また、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の共有を検討する。

フェーズ 2　SBOM作成・共有フェーズ

ステップ	SBOM導入に向けた実施事項	SBOM導入に向け認識しておくべきポイント
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。 □ 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、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。SBOMツールを用いることの効果はコンポーネント数が多いほど大きい。 ● パッケージマネージャーの構成情報を活用することが効果的な場合がある。また、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。 ● コンポーネントの誤検出や検出漏れが生じる場合がある。例えば、シンボリックリンクやランタイムライブラリ等のコンポーネント、深い階層のコンポーネント、分野固有のコンポーネント等を検出できない場合があるほか、コンポーネントを特定できてもバージョン情報が誤っている場合がある。 ● コンポーネントを解析する環境（実行環境、開発環境等）によって、解析結果が異なる場合がある。　等
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する。 □ SBOMツールを用いて、当該要件を満足するSBOMを作成する。	● SBOM内の名称について、SBOM利用者の視点で名称設定を行うことで、SBOM共有後の手戻りを無くすことができる。
2-3: SBOMの共有	□ 対象ソフトウェアの利用者及び納入先に対するSBOMの共有方法を検討した上で、必要に応じて、SBOMを共有する。	● 納入先が利用するSBOMツールによって、採用可能なSBOM共有方法が異なる。 ● 利用者に対するSBOM共有について、様々な方法が想定される。利用者に対してSBOM共有を行う場合、それぞれの方法の長所短所を踏まえて検討する。

①初級者向けSBOM導入手引　SBOM運用・管理フェーズの概要

- SBOM運用・管理フェーズでは、作成されたSBOMに基づき、脆弱性管理、ライセンス管理等の対応を実施する。
- また、SBOM作成後も、SBOMに含まれる情報やSBOM自体を適切に管理する必要がある。

フェーズ 3　SBOM運用・管理フェーズ

ステップ	SBOM導入に向けた実施事項	SBOM導入に向け認識しておくべきポイント
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。	● SBOMツールが出力した脆弱性情報が誤っている場合があり、出力結果を確認する必要がある。 ● SBOMツールでコンポーネントのEOL、EOSを特定できない場合、別途個別に調査する必要がある。
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。	● 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必要があるが、対応工数を要する。 ● 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である。PSIRTに相当する部門が存在しない場合、品質管理部門にて対応することが効果的である。

②SBOM対応モデル

②SBOM対応モデル（目的と問題認識）

- 脆弱性管理は、SBOM作成・活用の範囲が広いほど効果は大きい。SBOM対応モデルは、部品管理をどの程度行っているか可視化し、分野や企業のニーズに応じて調達・運用時のリスク管理に活用することができる。
- 分野ごとに法制度や取引慣行等に応じて、SBOMを生成・活用の範囲について可視化することで、サプライチェーンを通じたリスクの管理を可能にする。SBOM対応項目の選択肢の組合せとして、対応レベルに関するミニマムラインのコンセンサスを形成する。

【SBOM生成・活用に係る主な対応項目】

	適用区分	主な適用項目（選択肢）
生成・共有	(a)SBOM作成主体 (Who)	(a1)自社
		(a2)サプライヤ（開発委託先）取引契約あり
		(a3)サプライヤ（サードパーティ）取引契約なし
	(b)依存関係 (What, Where)	(b1)直接利用部品※1（開発主体が直接利用する部品）
		(b2)間接利用部品※2（既製品など開発委託契約のない部品から再帰的に利用する部品）
	(c)生成手段(精査) (How)	(c1)手動で特定（構成管理情報利用）・ツールで生成
		(c2)ツールで特定・生成・誤検知精査なし
		(c3)ツールで特定・生成・誤検知精査あり
		(c4)開発委託元が、開発委託先の作成したSBOMを独立に検査
	(d)データ様式・項目 (What)	(d1)標準フォーマット（SPDX、CycloneDX、SPDX Lite等）
		(d2)大統領令におけるデータフィールドの最小要素を含む
		(d3)上記を満たさない要素
活用	(e)活用範囲 (Why)	(e1)脆弱性の特定
		(e2)脆弱性の深刻度評価
		(e3)脆弱性の悪用可能性等の評価と対処
		(e4)ライセンス特定
	(f)活用主体 (Who)	(f1)製品利用者
		(f2)最終製品ベンダー
		(f3)各部品の開発者

実証等を踏まえ、対応レベルに応じて色分け

【SBOM対応範囲の可視化】

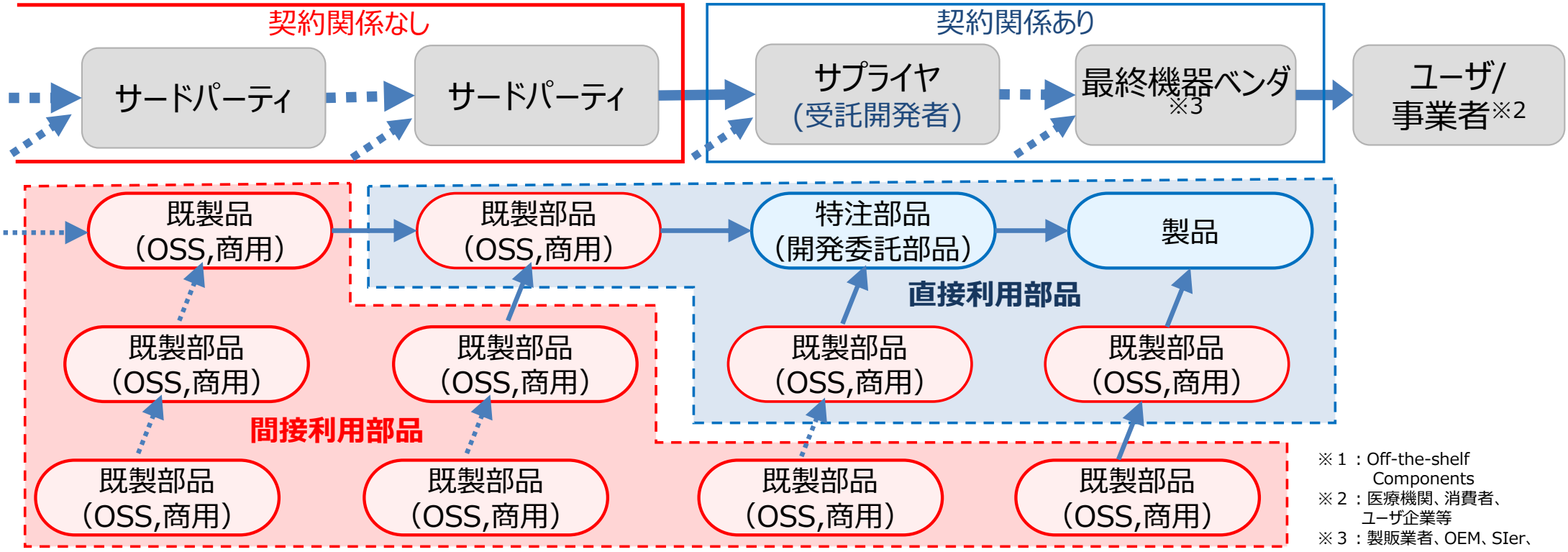
SBOM作成主体	作成範囲	生成方法	生成項目	活用法
(a1)自社	(b1)直接利用部品	(c1)手動で特定（構成管理情報利用）・ツールで生成	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記の一部のみ	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c1)手動で特定（構成管理情報利用）・ツールで生成	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
(a2)サプライヤ（開発委託先）取引契約あり	(b1)直接利用部品	(c1)手動で特定（構成管理情報利用）・ツールで生成	(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c1)手動で特定（構成管理情報利用）・ツールで生成	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c4)開発委託元が、開発委託先の作成したSBOMを独立に検査なし	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価

- SBOM生成・活用範囲（カバレッジ）は、SBOM適用項目選択肢の組み合わせとして整理を検討。
- 実証を通じて、比較可能な部分について、選択肢の範囲について参考情報などを提示する。

※１：直接利用部品：サプライチェーンにおいて契約関係のある開発者が直接利用する部品
※２：間接利用部品：サプライチェーンにおいて契約関係のないサプライヤが提供する部品から再帰的に利用される部品

【参考】 間接利用部品と直接利用部品について

- Log4jの脆弱性は、サードパーティの既成品(OTS※1:OSS, 商用）から再帰的に利用される部品も特定することが求められている。
- EU CRA（草案）のトップレベルコンポーネントを拡張して間接利用部品、直接利用部品として整理。



※1：Off-the-shelf Components
※2：医療機関、消費者、ユーザ企業等
※3：製販業者、OEM、SIer、パッケージベンダ

SBOM対応項目の選択肢（実証を通じた改訂結果）

- SBOM対応項目は、多様な選択肢があり、特にコストと効果に与える影響の大きい項目を整理。実証を通じて、分野ごとにこれらの組合せについて期待される対応範囲について検討した。

	適用区分	主な適用項目（選択肢）	コスト	コスト区分の判断理由（主なコスト要素、前提等）
生成・共有	(a)SBOM作成主体 (Who)	(a1)自社	小	自社開発で直接利用する部品を構成ファイルなどから特定し、SBOMを生成する。コード改変部品を含む。
		(a2)サプライヤ（開発委託先）取引契約あり	中	取引契約のある開発委託先のソフトウェアで利用する部品のSBOMを生成する。
		(a3)サプライヤ（サードパーティ）取引契約なし	大	取引契約によるSBOMの要件化できないOSSや既成部品ベンダーがSBOMを作成する。(b2)(c2)
	(b)部品範囲 (What, Where)	(b1)直接利用部品※1	小	開発者が直接利用する部品を構成ファイルなどから特定し、ツールなどでSBOMを生成する。
		(b2)間接利用部品※2	大	サードパーティ部品について、再帰的に利用される部品に対してSBOMを生成する。
	(c)生成手段(精査) (How)	(c1)手動で特定（構成管理情報利用）・ツールで生成	小	直接利用する部品情報を構成ファイルなどを用いて作成する。
		(c2)ツールで特定・生成・誤検知精査なし	中	ツールを用いてSBOMを生成し、精査は省略する。ツールの利用は再帰部品のSBOM生成を主に想定するため商用ツールの利用を想定する。
		(c3)ツールで特定・生成・誤検知精査あり	大	商用ツールを用いてSBOMを生成し、ソースコードレビューを行い、誤検知、検出漏れの精査を行う。（再帰利用部品を含む）
		(c4)開発委託元が、開発委託先の作成したSBOMを独立に検査	大	開発委託元が、開発委託先の作成したSBOMを受け入れる際に、ツールなどで独立してSBOMを作成するなどして信頼性を検査する。
	(c')生成手段（部品検出手法）	依存関係解析	中	パッケージマネージャ等の構成情報を静的に解析する。
		ファイル照合	中	ハッシュ値当を用いてソースコードのファイル単位の一致を検出する。 OSSのライブラリの検出なども含む。
		スニペット解析	大	ソースコードの部分的な文字列一致や類似性により検出する。
		バイナリ解析	大	バイナリファイルのビットパターンなどをもと類似性を検出する。
		実行形式内部の再帰的な依存解析	大	実行形式内にリンク済みのライブラリについて、そのライブラリをビルドする際の依存解析を再帰的に行う。
		上記に対応しない。	小	予め認識している部品をSBOMに変換する。
	(c'')生成手段（対象ソフト種別）	開発時に確定する部品	小	スタティックライブラリ、アプリケーション
		実行時に確定する部品	中	ランタイムライブラリ、サービス（ローカル、外部クラウド）、OS、ミドルウェア、実行環境（コンテナ、VM、APサーバ）
		周辺ツール環境	大	開発運用で使用するツール（インストーラ、アップデータ、配布パッケージ、開発環境、ツールチェーン、SBOMツール）
	(d)データ様式・項目 (What)	(d1)標準フォーマット（SPDX、CycloneDX、SPDX Lite等）	中	SPDXなどの標準フォーマットで作成する。
		(d2)大統領令におけるデータフィールドの最小要素を含む	中	大統領令におけるデータフィールドの最小要素を含むSBOMを作成する。
		(d3)上記を満たさない要素	小	独自の最小限の要素を作成する。
活用	(e)活用範囲 (Why)	(e1)脆弱性の特定	小	NVD, JVN等のDBを対象として脆弱性の検索・特定を行う。
		(e2)脆弱性の深刻度評価	中	CVSS値をベースとした深刻度を評価し、脆弱性対応の優先度を設定する。
		(e3)脆弱性の悪用可能性等の評価と対処	中	VEX情報等を用いて悪用可能性、脆弱性対処の必要性を評価する。必要に応じて対処策等のアドバイザリを発行する。
		(e4)ライセンス特定	中	ライセンスの特定と規約の取得を行う。
	(f)活用主体 (Who)	(f1)製品利用者	小	脆弱性が特定された場合、利用を中断し、ベンダーによる修正を待つ。業務中断コストも考慮すれば損害は大きい。
		(f2)最終製品ベンダー	中	利用者に脆弱性を通知するとともに、開発者への修正依頼、修正後のビルド・利用者への提供を行う。必要に応じて当局、ISAC等に報告する。
		(f3)各部品の開発者	大	開発者は、脆弱性の監視と修正を行い、調達者に修正版を提供する。必要に応じて当局、ISAC等に報告する。

分野ごとのSBOM対応モデルの整理（全体俯瞰）

- SBOM対応項目選択肢について、実証を通じて評価検討を行い改訂した部分および未評価の仮説を含めて色分けにより整理。
- いずれの分野もOSSを含むサードパーティからのSBOM取得は困難であるため、委託開発企業またはツールでの対応が考えられる。
- 医療機器、自動車分野は、委託開発先も含めてSBOM生成・共有し、ソフトウェア分野については、委託開発先は部分対応が考えられる。
- 医療機器分野は法的に構成管理を要件化されているため、間接利用部品を含めて説明責任を果たすことが考えられる。
- OSSの間接利用部品の完全な特定は技術的な課題があるため、ソフトウェア分野については部分的な対応としている。

医療機器分野

適用主体	作成範囲	生成方法	生成項目	活用法
製販業者	直接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	
			(d3)上記の一部のみ	
		(c2)ツールで特定・生成・誤検知精査なし	(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)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(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)上記を満たさない要素	
	間接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(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)上記を満たさない要素	
		(c2)ツールで特定・生成・誤検知精査なし	(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)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(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)上記を満たさない要素	
委託開発先	直接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(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)上記の一部のみ	
		(c2)ツールで特定・生成・誤検知精査なし	(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)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(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)上記を満たさない要素	
	間接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(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)上記を満たさない要素	
		(c2)ツールで特定・生成・誤検知精査なし	(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)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDXLite等)	
			q	
			(d3)上記を満たさない要素	
開発者自身		(c1)手動で特定(構成管理情報利用)・ツールで生成	(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)上記を満たさない要素	
		(c2)ツールで特定・生成・誤検知精査なし	(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	
			(d1)	

間接利用部品

間接利用部品

開発委託先

自動車分野

適用主体	作成範囲	生成方法	生成項目	活用法
ECUベンダ（ティア１）	直接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
	間接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
開発委託先（ティア２等）	直接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
	間接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
開発者自身		(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット(SPDX、SPDXLite	
			(d2)大統領令最小要素を含む	
			(d3)上記を満たさない要素	

間接利用部品

サードパーティ

ソフトウェア分野(例：セキュリティソフト)

適用主体	作成範囲	抽出・生成・検査手段	生成項目	活用法
最終ベンダー	直接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(d1)標準フォーマット(SPDX、SPDXLite等)	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	
			(d3)上記の一部のみ	
		(c2)ツールで特定・生成・誤検知精査なし	(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)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(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)上記を満たさない要素	
	間接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(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)上記を満たさない要素	
		(c2)ツールで特定・生成・誤検知精査なし	(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)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(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)上記を満たさない要素	
開発委託先	直接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(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)上記を満たさない要素	
		(c2)ツールで特定・生成・誤検知精査なし	(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)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(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)上記を満たさない要素	
	間接利用部品	(c1)手動で特定(構成管理情報利用)・ツールで生成	(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)上記を満たさない要素	
		(c2)ツールで特定・生成・誤検知精査なし	(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)上記を満たさない要素	
		(c3)ツールで特定・生成・誤検知精査あり	(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)上記を満たさない要素	
開発者自身		(c1)手動で特定(構成管理情報利用)・ツールで生成	(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)上記を満たさない要素	
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット	
			(d2)大統領	

凡例：

適用可能・必須	部分適用（事例依存）	適用困難	不要または対象外

黒文字：実証で評価、青文字：未評価

SBOMの効果的な対応案（医療機器分野：近畿レントゲン等）

- 医療機器分野では、法制度上、構成管理は、製販業者に責任となっていることから、開発委託先にもSBOM作成を要件化や、脆弱性の特定、深刻度・影響評価、悪用可能性、アドバイザリの作成まで求められることが想定されるため、下記表のとおりの対応範囲等が考えられる。

SBOM対応項目	実証結果	規制等により期待が想定される対応範囲	課題や考えられる対応など
作成主体	製販業者、委託先ともに、ツールも活用しSBOMを作成。委託先との契約にSBOM提示要件を含めるなどの対応。 サードパーティについては、SBOM提供が不可能な場合でも製販業者として責任を負う必要がある。	法制度上、構成管理は製販業者の責任となっていることから、開発委託先にもSBOM作成を要件化する。 サードパーティについて、SBOM提供が無い場合でも、製販業者が部品検査などにより構成管理の責任を果たせる場合のみ部品を利用する。	• 中小企業が多く、ツール費用、初期導入工数を含めコスト負担が大きい。 →導入ガイダンスの利活用検討、活用できる補助制度などの利用検討 • サードパーティについてはSBOM取得は難しく、完全な部品特定のハードルが高く、制度上のリスクマネジメントの観点からOSSの利用が難しい →ソフトウェア部品のライフサイクル、リスクを評価した上でソフトウェアを選択するなど
作成範囲（カバレッジ）	直接利用部品のSBOMは作成可能。間接利用部品は、完全な部品特定は難しい。	直接利用部品のSBOM作成の必須。Windows等のCOTS※を含め、間接利用部品に対して説明責任を果たせる構成管理は必須（JIS T 2304 への適合）。	説明責任を果たせる構成管理について、SBOM作成の具体的な基準作成が期待される。 →規格JIS T 2304、IEC 81001-5-1:2022（JIS T 81001-5-1制定予定）の対応などの検討
精査（信頼性確保）	ツールの誤検出があるため精査が必要。手動とツールによる精査を実施。	構成管理が制度上求められ、ツールの誤検出があるため精査が必要とされる。	合理的に説明責任を果たせる精査の程度が期待される。
活用範囲	脆弱性評価、悪用可能性評価はツール検証結果を確認。脆弱性マネジメントフローの検討及び、フローに則った対応について机上評価。 ソフトウェアの中で1つ取り上げてOSのライセンス、EOL、EOSを特定、製品のサポート計画等を検討した。	制度上、脆弱性マネジメントが必要であり、脆弱性の深刻度・患者危害の影響評価、悪用可能性評価、アドバイザリレポート作成まで実施。ソフトウェア部品のライセンス、EOL、EOSを特定し、更新計画なども市販前に計画し、顧客、規制当局に開示が必要。	脆弱性評価、悪用可能性評価から、医療機器に対する影響、及び患者危害の影響度を含めたアドバイザリレポート作成。 →PSIRT設置。IPAへの相談、JPCERT/CCとの情報共有。行政機関、業界団体の説明会、研修等を踏まえた検討。 脆弱性マネジメントフローに対応するため件数が大きいため効率化が必要。 →検討が必要な脆弱性の絞り込みなど
フォーマット	SPDX（ツールの機能による）	定め無し。SPDX、CycloneDX、SWID tag等	VEXに対応する場合、CycloneDXも想定される。 →フォーマット変換ツールの利用検討

※Commercial Off-The-Shelf（以下、COTS）：商用ソフトウェア製品

SBOMの効果的な対応案（自動車分野：東海理化等）

- 自動車分野では、法制度上、構成管理が求められている。
- 法制度や取引慣行、実証結果を踏まえると、下記表のとおり、より効果的に活用していくための課題及び対応等が考えられるところ、これを案として自動車業界と調整を図っていく。

SBOM対応項目	実証結果	より効果的に活用していくための課題や考えられる対応など
作成主体	開発委託先にもSBOMを要件化可能。サードパーティについてはSBOM提供は無く、コードレビューにより部品の特定を実施。	法制度上、構成管理が求められるため、開発委託先にもSBOMを要件化する。OSSなどサードパーティからSBOM取得ができ無い場合、委託先の開発者が部品を特定し、委託元に対して利用するOSS の申告と合意を得る。 →今後、策定する取引モデルの活用の検討。
作成範囲 (カバレッジ)	直接利用部品の作成は可能。間接利用部品はパッケージマネージャの構成情報などを用いて効率的に実施できる部分は対応。	直接利用部品の作成必須。間接利用部品は、ツールやレビューにより可能な範囲で作成する。 →業界におけるコンセンサス形成の検討、SBOM取引モデルに基づいた受発注者間の契約の検討など
精査 (信頼性確保)	ツールの誤検出があるため、精査は必要。効率的に精査可能な直接利用部品について実施可能。	ツールだけでは誤検出があるため、効率的に精査可能な部品については実施。 →取引モデル等の活用により、受発注者間で契約などを締結することの検討、ツールの構成解析機能（依存関係解析、スニペット解析、ファイル照合等）に応じて、誤検知、検出漏れ有無を判断し、コードレビューなどにより効率的な精査の方法の検討。
活用範囲	脆弱性・ライセンスの特定まで可能。深刻度評価、悪用可能性評価はツール無しではコストが大きい。	脆弱性・ライセンスの特定までとし、深刻度評価、悪用可能性評価はリスクの大きい場合に限定 →ISAC,ベンダーからのVEX文書の活用方法の組織導入の検討
フォーマット	SPDX(ツール出力)	ー

SBOMの効果的な対応案（ソフトウェア分野：トレンドマイクロ、コラボスタイル、さくらインターネット）

- ソフトウェア分野は、明確な法的要件は定まっておらず、事業環境、取引慣行が多様であることから、企業ごとに選択肢の幅が大きい。
- そのため、実証結果を参考にしつつも、より効果的・効率的な対応のため、各企業において課題へのノウハウも参考にしながら、活用していくことが考えられる。

SBOM対応項目	実証結果	より効率的に実施していくための課題や考えられる対応など
作成主体	実証企業３社ともに、最終ベンダーのみが対応	委託先の技術力も考慮し、当面、委託先にSBOMを要件化できない状況。ただし、開発当事者がSBOMを作成した方が効率的で、正確となることから委託先のSBOM要件化は期待される。サードパーティは、業界の状況に依存して異なる。 →SBOM導入ガイダンス利用によるSBOM導入検討、SBOMに対応できる委託先の確認・選定等
作成範囲（カバレッジ）	実証企業３社ともに、ツールで生成可能な直接利用部品、間接利用部品に対応。	ツールによる間接利用部品の特定は限定的である。 →リスクに応じてOSSの再帰的な依存関係に従いソースコードを取得し、SBOMツールによるSBOM生成などの方法を検討
精査（信頼性確保）	直接利用部品は部分的に精査可能。間接利用部品の精査は効率的な方法が現状ない	工数を考慮すれば、間接利用部品の精査は限定的と考えられ、誤検知、検出漏れの課題がある。 →導入ガイダンスを参照しつつ、コスト制約のもとで精査できる範囲を検討
活用範囲	脆弱性・ライセンスの特定まで可能 深刻度評価、悪用可能性評価はツール無しではコストが大きい	深刻度評価、悪用可能性評価により不要な脆弱性修正を省き効率化していくことが考えられる。 そのためにはツールによる深刻度、悪用可能性情報の取得、VEX等の普及などが期待される。 →ISAC,ベンダーからのVEX文書の活用方法の組織導入の検討
フォーマット	SPDX(ツール対応)	ー

SBOM導入ガイダンス付録 A. SBOM対応モデルの構成

- SBOM対応モデル・ガイダンスの全体構成は以下のような案を想定し、**今年度はこれらの主要な要素（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・項目等やステークホルダーの合意形成の在り方）について整理**。
- SBOM適用項目のコスト・効果については多数の組合せがあり、今年度実証で、比較評価できない項目組合せについては、例示という位置付け。

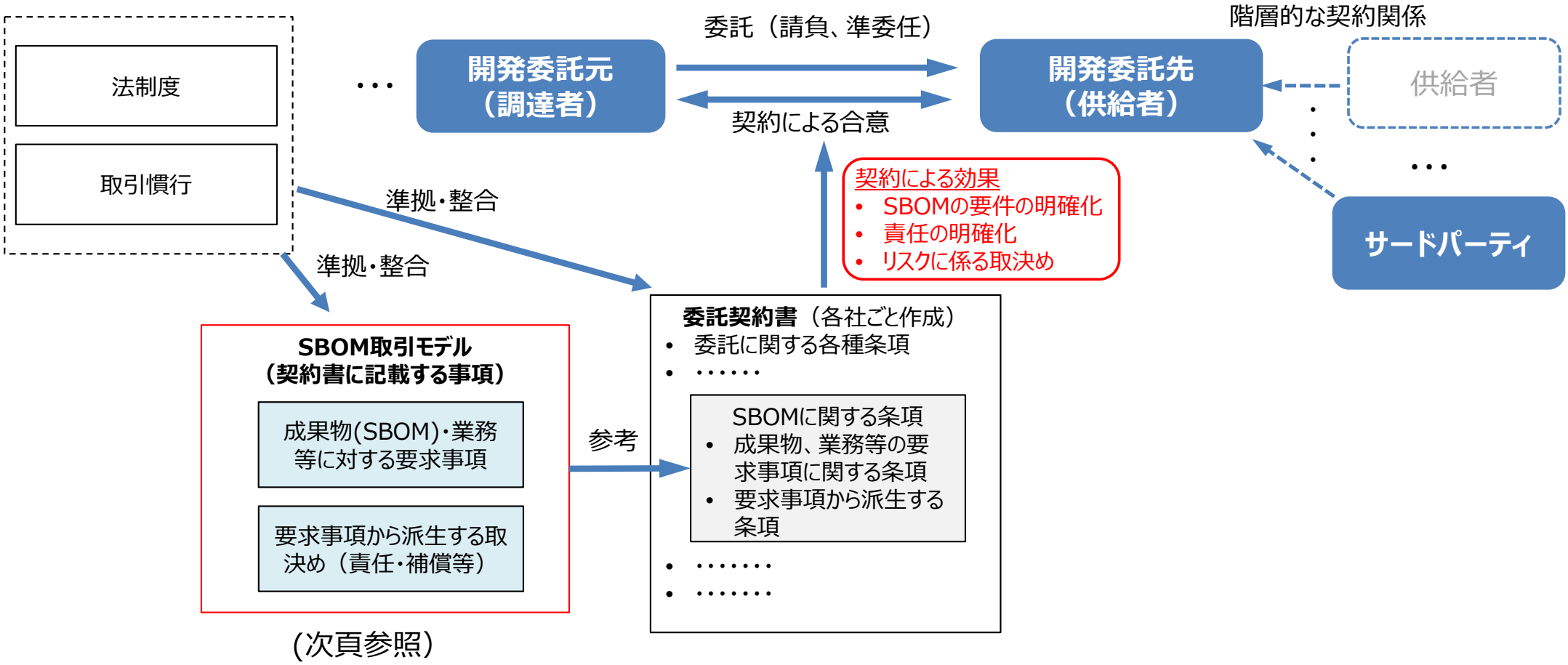
章	項	主な記載内容	実証項目との関係
付録A1. 背景と目的	1.1 背景と問題認識 1.2 SBOM対応モデルの必要性 1.3 本書の目的	• SBOM普及における課題や問題認識等の背景を記載 • 問題認識に基づきSBOM対応モデルの必要性を示す。 • それらを踏まえて本書の目的を示す。	（昨年度調査・実証結果等に基づき整理。）
A2. 概要	2.1 SBOM対応モデルとは？ 2.2 想定読者 2.3 本書の全体構成	• SBOM対応モデルの概要、対象読者についてまとめる。 • 本書の全体構成を示す。	３分野での実証に基づき対象者を示す（開発部署関係者を想定）。
A3. SBOM対応モデルの考え方	3.1 基本的な考え方 3.2 活用方法	• SBOM対応モデルの基本的な考え方、活用方法についてまとめる。	実証結果全体をもとに考え方を整理。
A4. SBOM対応モデルの枠組み	3.1 SBOMの適用区分と選択肢 3.2 SBOMの対応モデルの定義方法	• SBOM対応モデルの枠組みを定義する上で必要になる、適用項目の選択肢とそれらの組合せによる適用範囲について記載	SBOM適用選択肢の整理結果をもとに作成。
A5.SBOMに関する法制度、条件等	4.1 法制度の全体概要 4.2 医療機器分野 4.3 自動車分野 4.4 ソフトウェア分野 4.5 その他分野	• SBOM対応モデルのコンセンサスを整理するにあたり前提となる法制度や条件などを分野ごとに整理する。	SBOM実証の前提条件等の調査検討結果に基づき整理。
A6.産業分野ごとのSBOM対応モデルの参考例	5.1 検討アプローチ 5.2～5.4 各分野（医療機器分野、自動車分野、ソフトウェア分野） - 基本要件と考え方 - 対応モデル案 - 留意点とカスタマイズ	• SBOM対応モデルの検討アプローチを明示 • 分野ごとに、基本要件を踏まえた考え方の整理 • 分野ごとに、事業者、業界団体の意見をもとに検討整理した対応モデル案（適用範囲のモデルケース）の提示 • 対応モデルに関する留意点、カスタマイズ方法	分野ごとに実証するSBOM適用モデルケースに対するコスト評価、フィージビリティ検討結果に基づき整理。ただし、比較検証は部分的となる。
付録 A7	6.1 用語集と参考情報	• 参考となる情報源	関連文書に整合させる。

③SBOM取引モデル

SBOM取引モデルの意義と位置付け（全体像）

- SBOMのメリットは、サプライチェーンを通じて標準化された部品情報の共有と自動処理による効率化が挙げられる。特にSBOMを受け取る委託元の便益は大きいが、委託先はそのために追加負担を強いられることもあり、受発注者間で得られる便益が異なる。
- そのようなことから、サプライチェーンを通じたSBOMの普及のためには、受発注者間で得られる便益に応じた対価負担の取決めが必要であり、委託契約において、SBOMの対応範囲とそれに対する対価負担、責任の明確化が必要。
- SBOM取引モデルは、そのようなSBOMに対する要求事項と派生する対価負担、責任関係について取り決める事項を示すものである。SBOM取引モデルは各社ごとの契約書作成において参考となり、SBOMの効果的な利活用に資するものである。

サプライチェーンにおける委託契約に基づくSBOMの普及促進



SBOM導入ガイダンス 付録B: SBOM取引モデル・ガイダンスの構成

- SBOM取引モデル・ガイダンスの全体構成は以下のような案を想定し、**今年度は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などに関する検討・構成案の一部要素を整理**。

章	項	主な記載内容	実証項目との関係
付録 B1. 背景と目的	1.1 問題認識 1.2 SBOM取引モデルの必要性 1.3 本書の目的	• SBOM普及における課題や問題認識等の背景を記載 • 問題認識に基づきSBOM取引モデルの必要性を示す。 • それらを踏まえて本書の目的を示す。	（昨年度調査・実証結果等に基づき整理。）
付録 B2. 全体概要	2.1 SBOM取引モデルとは 2.2 対象読者 2.3 本書の全体構成	• SBOM取引モデルの概要、対象読者についてまとめる。 • 対象読者については、製品メーカー、サプライヤー、ユーザ企業などの候補について本書との関係性を示す。 • 本書の全体構成を示す。（主な内容は3～6章）	３分野での実証に基づき対象者を示す（契約担当部署、開発部署関係者を想定）。
付録 B3. 取引モデルの活用方法	3.1 SBOM取引モデルの考え方 3.2 SBOM取引モデルの活用方法	• SBOM取引モデルの基本的な考え方、活用方法についてまとめる。	実証結果全体をもとに考え方を整理。
付録 B4.責任関係の明確化	4.1 部品管理における役割と責任関係 4.2 ライセンス規約と脆弱性対応 4.3 損害賠償責任	• SBOMに係る規定の前提となる部品管理に関する役割や責任関係、ライセンス規約、脆弱性対応に関する規定例を示す。 • 損害賠償責任に関する規定例を示す。	文献調査、ヒアリングにより整理。（今年度は一部のみ調査）
付録 B5. SBOM 管理	5.1 SBOM適用範囲に関する規定 5.2 SBOMの必要要素、フォーマットに関する規定 5.3 SBOMの信頼性に関する規定 5.4 SBOMの更新に関する規定 5.5 見積要求と費用負担	• 取引企業間のSBOMに関する具体的な規定例について示す。 • また、SBOMがサプライチェーンを通じて無理なく普及するように見積もりや費用負担に関する規定例を示す。	実証に基づき作成したSBOM対応モデル・ガイダンスをもとに、その後、契約条項の文献調査を踏まえてサンプルを整理。
付録 B6. プロセス・手順	6.1 プロセスの全体像 6.2 開発プロセスにおける手順等 6.3 運用プロセスにおける手順等	• SBOMに具体的に対応するためのプロセス・手順に関する規定を示す。	SBOM実証結果に基づき、その後、SBOM生成・活用の全体プロセスを整理。
付録 B7. 付録	7.1 用語集 7.2 参考情報・事例	• 用語集及び参考情報源	関連文書に整合させる。

③SBOM取引モデル：取引契約に規定すべき事項（案）

- 分野ごとの前提条件（付録の法制度、取引慣行、開発環境）に基づき取引契約で規定すべき事項を整理
- 現状で取引契約に記載される事例が存在するものは赤文字、分野固有で考慮すべき事項・条件は備考に記載
- 取引契約においてSBOMに係る事項として下記について過不足等の意見を頂きたい。

要求レベル	SBOMに対する要求事項 (成果物・業務等)	要求事項から派生する取決め (責任、補償等)	想定分野例
基本事項 (最小限)	• 利用するサードパーティ部品（OSS、商用部品）に関する受発注者間の事前合意と申告 • SBOMによる部品情報の納品（対ユーザ、対サプライヤ） • SBOMのフォーマット、受け渡し方法の規定（ファイル、SaaS等）	• ライセンス違反に関する責任・損害賠償責任 • 最小限のSBOM作成・活用の見積と対価負担の規定 • SBOMの知財権の帰属	全分野 （基本事項のみは、安全性や決済に関係の無いソフトウェア等）
追加事項 (ハイレベル)	• 悪用可能性、アドバイザリ等の情報(VEX)の要否 • 納品・市販後の脆弱性情報監視・通知とその頻度 • 納品・市販後の脆弱性の修正対応の要否、トリアージ • SBOMのカバー範囲と信頼性等のSBOM対応レベルに関する要求と説明 • ソフトウェアのアップデートに伴うSBOMの更新とその頻度に関する規定 • サードパーティ部品のEOL、EOSや予定外の変更に対するサポート計画の要否	• 納品した部品情報またはSBOMの瑕疵責任の規定 • 納品したSBOMの瑕疵に伴う損害賠償の責任主体とその範囲 • SBOM作成・活用の範囲に応じたコストの見積（受託開発者およびサードパーティ部品）	• 医療機器、自動車制御系、重要インフラ

【参考】 実証等を踏まえたSBOMの効果に関するまとめ

- SBOM初期導入・SBOM作成・活用におけるコスト・効果を計測評価し、一定数以上の脆弱性管理を行う場合、初期導入コストを上回る効果が得られるところ、SBOMの効果に関する全体像を整理した。
- 本実証では、主要な直接効果について評価・確認。間接効果は、直接効果の組合せによって社会への波及効果として創出される。

効果区分		効果項目	主な内容
リスク低減	直接効果	脆弱性残留リスクの低減	サプライチェーンを通じた部品情報の共有・範囲拡大により脆弱性の特定漏れのリスクを低減。調達元、ユーザ企業等も含めてリスク対応可能となる。
		脆弱性対応期間の短縮	SBOMによる脆弱性情報のリアルタイム自動検出により初動期間を短縮
		ライセンス違反リスクの低減	部品特定漏れによるライセンス違反のリスクを低減
	間接効果	製品価値向上・企業価値向上	上記直接効果により製品の品質・価値向上、企業価値向上に繋がる。
		サイバー環境の改善(Cyber Hygiene）、外部経済効果	脆弱性の少ない製品が増えることで、サイバー空間全体のセキュリティ環境が向上（踏み台悪用による攻撃を受けるリスクが低減）
コスト低減・生産性向上	直接効果	脆弱性管理等にかかるコストの低減	脆弱性管理、ライセンス管理を行う上で、SBOMによる自動化、網羅範囲拡大により、従来手法に比べて同等の効果を得るためのコストが低減できる。 なお、脆弱性管理をどこまで徹底するかは、リスク定量化の課題。
		コンプライアンス対応の効率化	調達管理（製品・部品選定等）、運用管理（脆弱性管理）、法令対応、貿易制限対応・論証の効率化
	間接効果	生産性向上、開発現場の意欲改善	手動による脆弱性管理など非効率な業務の解消による生産性の向上、開発現場意欲の改善

1. ソフトウェアの管理手法等に関する国内外の動向

2. SBOM実証の結果等（全体概要）

3. 実証結果等を踏まえた検討

①初級者向けSBOM導入ガイダンスの要点
②SBOM対応モデルの要点
③SBOM取引モデルの要点

4. 今後の取組課題等

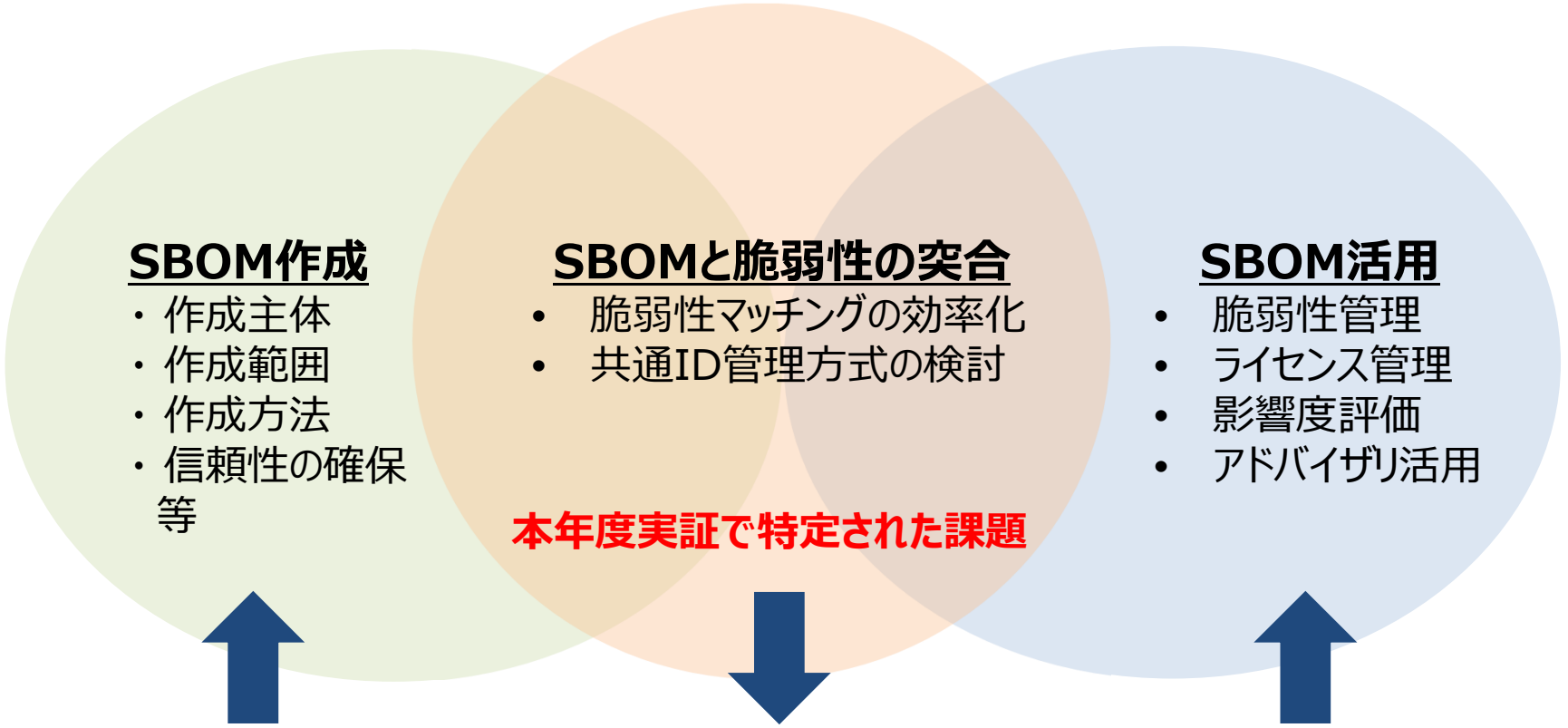
実証で抽出された主な課題と解決策（抜粋）（再掲）

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を行った。

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		●	●	

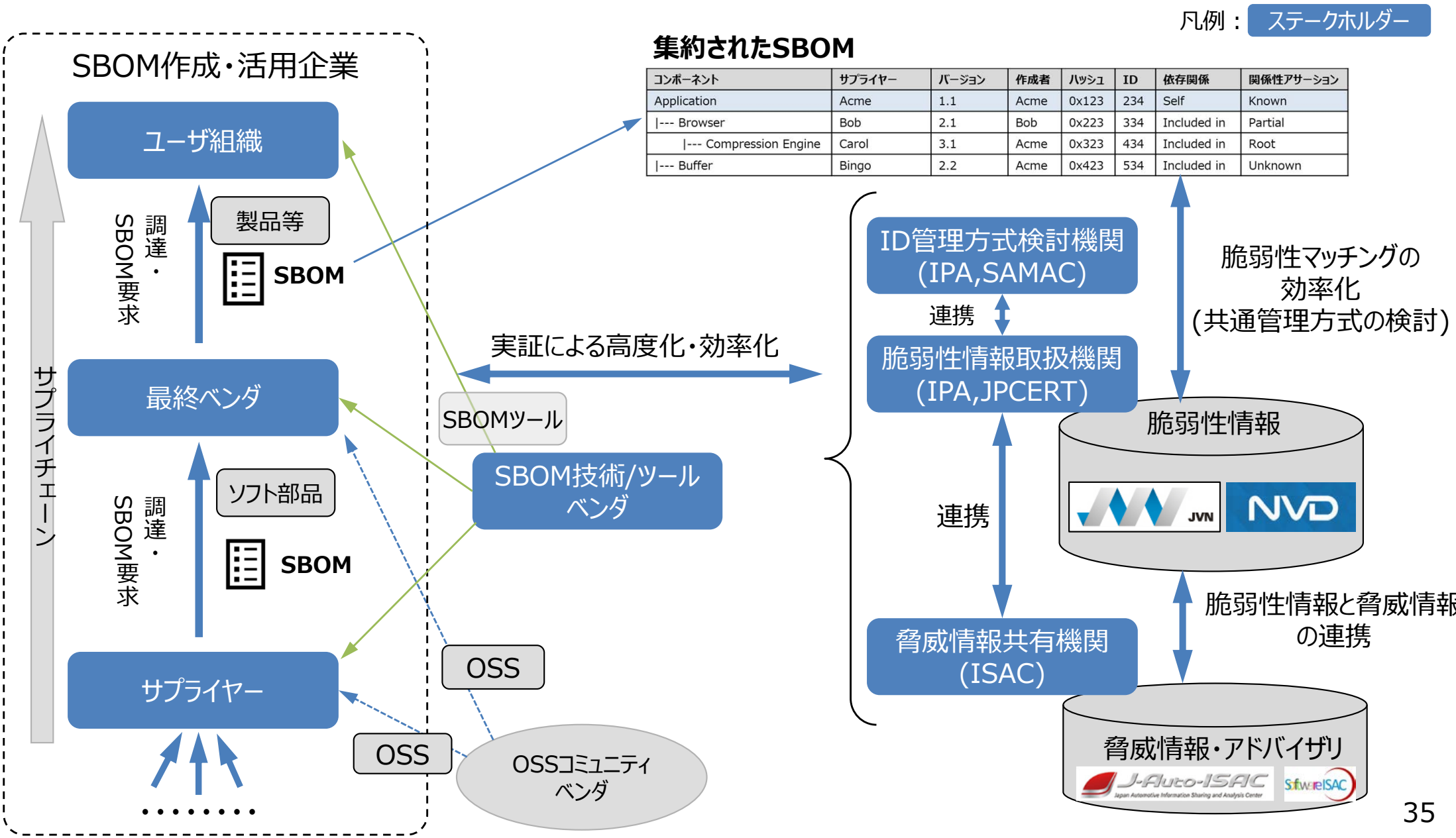
SBOMのスコープと課題領域

- サプライチェーンを通じてソフトウェアを安全に利活用する上で、構成管理、脆弱性管理の基盤としてSBOMは有効。
- その効果を高める上で、本年度実証では、SBOM作成とSBOM活用のフィージビリティスタディと効率化の検討を行ったところ、本年度の調査から、SBOMの効果を高める上で、SBOM作成とSBOM活用の間をつなぐ、脆弱性マッチングとそのための共通ID管理が課題であることが判明。
- 来年度は、SBOM作成とSBOM活用の間をつなぐ、脆弱性マッチングとそのための共通ID管理についての高度化、効率化について実証に基づき検討を進める。



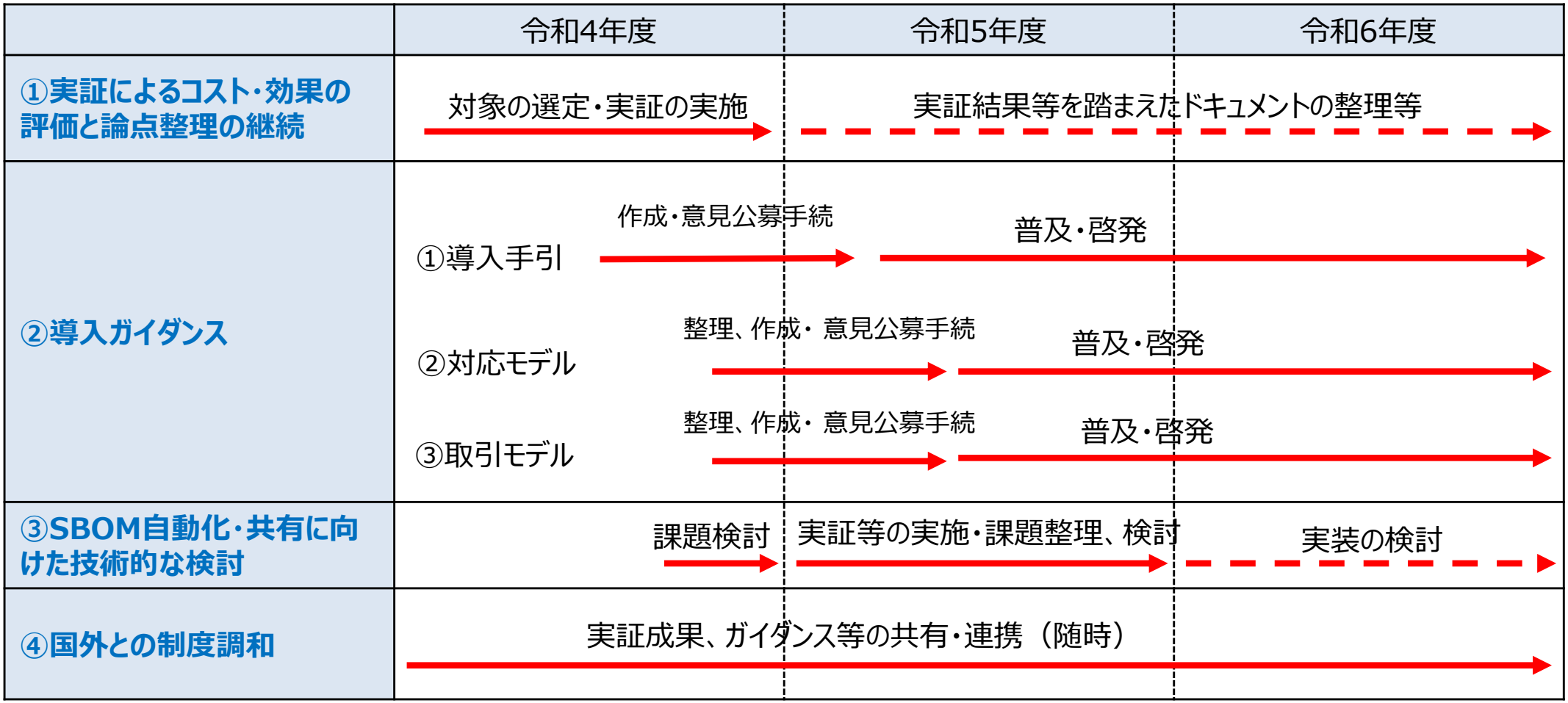
【取組課題】 SBOMを活用した脆弱性管理の効率化・高度化

- 本年度抽出された課題を踏まえ、来年度はSBOMを活用した脆弱性管理の効率化・高度化の方式について実証し、主なステークホルダーと連携し、共通管理方式、脆弱性マッチング、脅威情報活用策、国際連携について検討を行う。



スケジュール（案）

- 導入ガイダンスのうち、導入手引部分については、本TFにおける意見等を反映しつつ、意見公募手続を実施することとしたい。また、対応モデル、取引モデル部分についても整理作成後に御意見等を踏まえつつ、来年度に意見公募手続を実施することとしたい。



御議論いただきたい事項

- 主に以下の点につきまして御意見等をいただきたく存じます。

- **SBOM導入ガイダンスの構成、内容に関する御意見・御提案**
  - 特にサマリー、経営者向けの観点、メッセージについて
- **SBOM対応モデルに関する御意見・御提案**
  - 特に対応モデル案について
- **SBOM取引モデルの契約条項に入れるべき事項に対する過不足等の御意見・御提案**
- そのほか、今後の取組検討など資料に対する御意見等