サプライチェーンリスク対応のための技術検証体制構築等に関する調査

概要報告書

2023年6月
内閣官房内閣サイバーセキュリティセンター（NISC）

※本調査はNISCの委託により、株式会社三菱総合研究所が実施したものです。

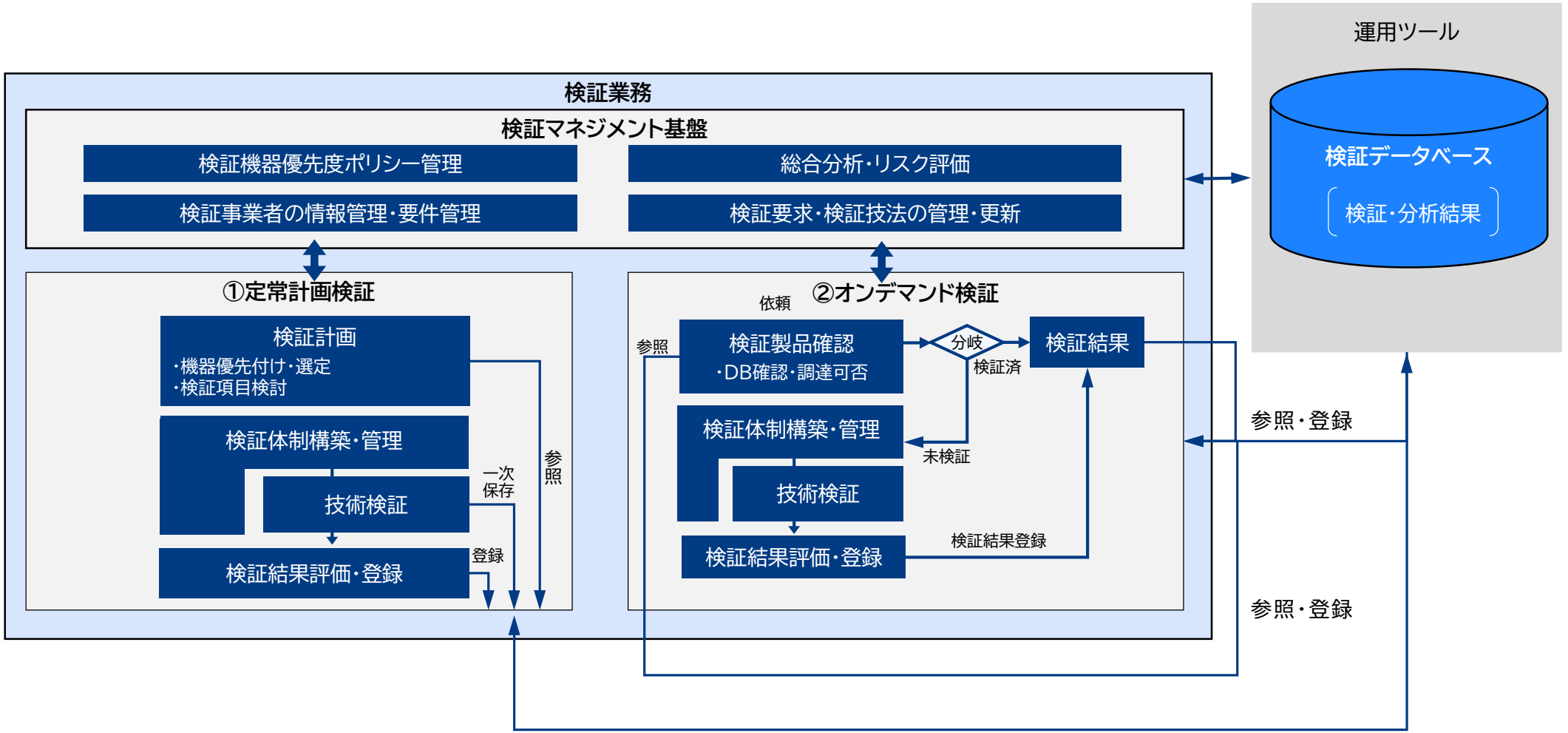
調査概要・目的

サイバー空間と実空間の一体化が加速的に進展し、情報通信機器のみならず様々な機器がサイバー空間を介して国民の生活に結びついている現状において、これらの機器の信頼性を確保することはより一層不可欠なものとなっている。また、機器の信頼性を確保するためには、サプライチェーンリスクについても技術的な検証により信頼性が確保されていることが不可欠である。

本件は、機器のサプライチェーンリスクに係る信頼性確保に対し、その高度化および効率化に資する検討を行うものである。

検証スキームの全体像

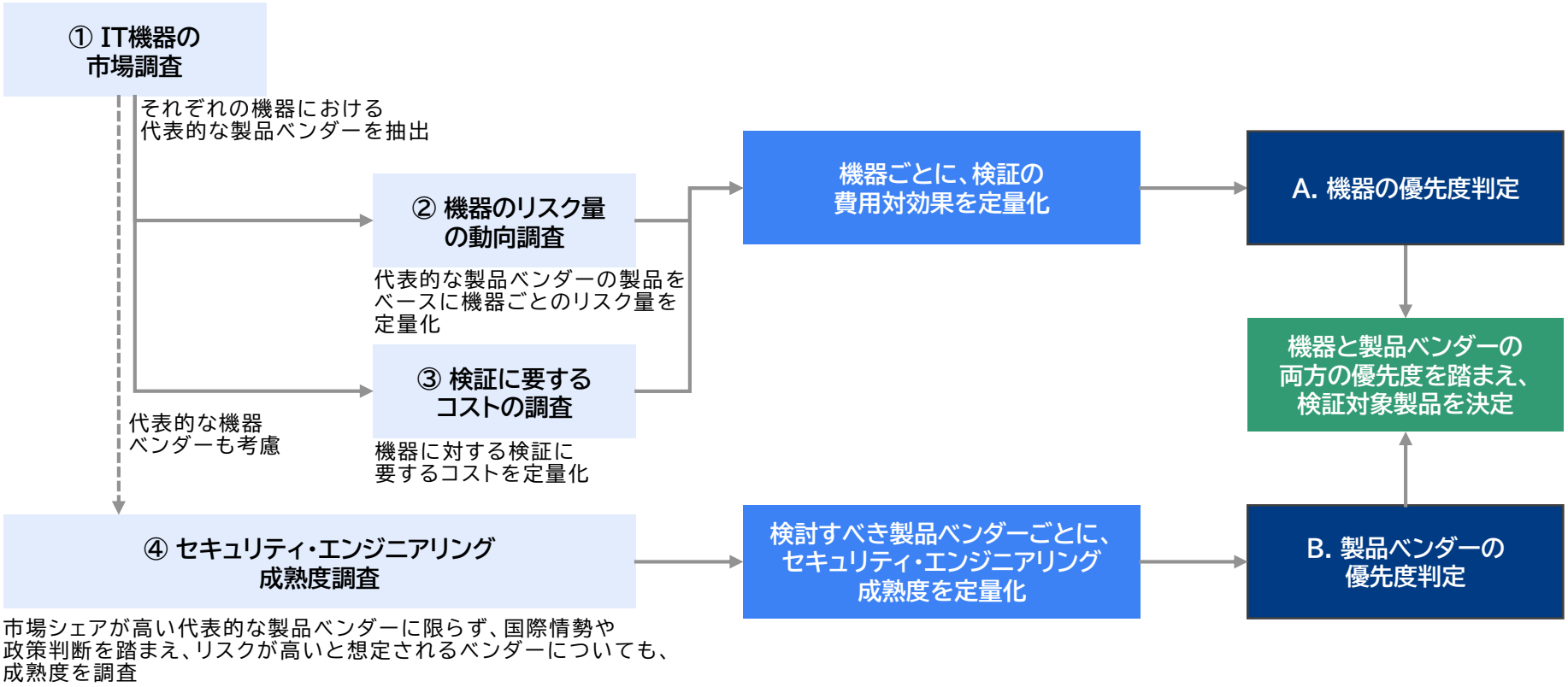
- 検証業務は、運用ツールのデータベースを介して脆弱性情報、脅威情報を一元的に管理分析を可能にする。



検証優先度ポリシーの全体像

- 検証優先度ポリシーは、①機器の市場調査、②機器のリスク量に関する動向調査、③検証に要するコストの調査、④セキュリティ・エンジニアリング成熟度調査の４つの観点に基づき整理した。
- 検証対象製品の優先度付けに当たっては、「機器の優先度」と、各機器の「製品ベンダーの優先度」の両方を検討する必要がある。そのため、①～③の観点は「機器の優先度」の判断に主に用い、「製品ベンダーの優先度」の判断においては④の観点を主に用いた。

４つの観点に基づく検証優先度ポリシー



検証優先度ポリシーの具体化

検証優先度の判定基準

- ４つの観点を更に構造化した判断基準に基づき「機器の優先度」と「製品ベンダーの優先度」を整理した。
- 製品ベンダーのセキュリティ・エンジニアリング成熟度の調査に当たっては、CSIRT/PSIRTやバグ報奨金プログラム有無等の調査に加え、米国等の規制動向や国際情勢も判断基準に加えた。

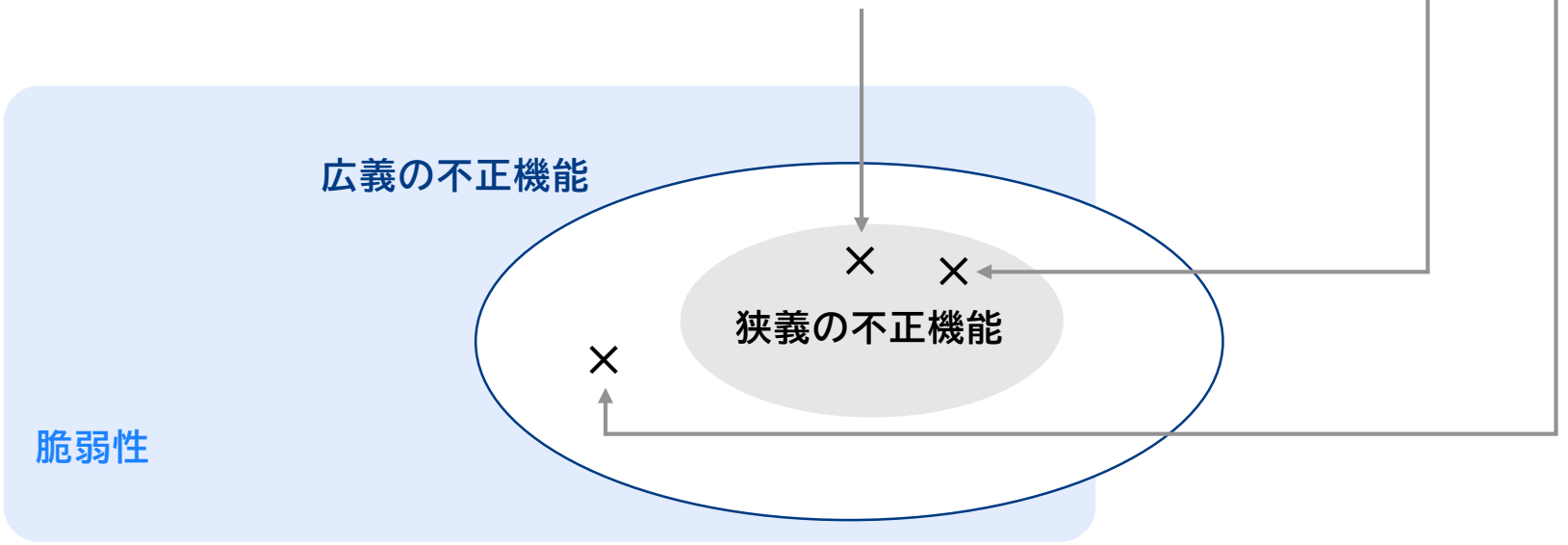
	観点	項目	判断基準
	① IT機器の市場調査	機器の市場シェア	1. 各機器の国内市場シェア上位ベンダーはどの企業か。
機器ごとに整理	② 機器のリスク量の動向調査	機器における事故発生確率	1. 代表的な製品ベンダーの機器において、過去に脆弱性が何件報告されているか。 2. 報告された脆弱性のうち、攻撃難易度が低い脆弱性は何件か。 3. 報告された脆弱性のうち、影響が大きい脆弱性は何件か。 4. 当該機器においてどの程度のエクスプロイトコードが公開されているか。 5. 機器に対する物理的／論理的アクセスはどの程度容易か。
		攻撃の影響度	6. 当該機器はどの程度の個人情報を扱うか。（機密性の観点） 7. 攻撃によって、データの完全性にどの程度の影響を与えるか。（完全性の観点） 8. 攻撃によって当該機器が停止した場合の緊急度合いはどの程度か。（可用性の観点）
	③ 検証に要するコストの調査	検証に要するコスト	1. 当該機器の検証・解析にかかる時間はどの程度か。 2. 当該機器自体の購入費用はどの程度か。
		検証に要するスキル・設備等	3. 当該機器の検証には特殊な設備が必要か。
代表的なベンダーごとに整理	④ セキュリティ・エンジニアリング成熟度調査	製品ベンダーのセキュリティ・エンジニアリング成熟度	1. 代表的な製品ベンダーにおけるセキュリティ上の懸念はどの程度か。 2. 当該製品ベンダーにおいて、セキュリティ体制・インシデント対応体制は構築されているか。 3. 当該製品ベンダーにおいて、バグ報奨金プログラムは用意されているか。 4. 当該製品ベンダーにおいて、国際的なセキュリティ認証制度の取得製品数はどの程度か。 5. 当該製品ベンダーにおいて、サプライチェーンセキュリティに関する取組やリスク等がどの程度存在するか。

【参考】本事業における不正機能の定義

- 脆弱性について、悪意を持って埋め込まれた不正機能か、過失によるものか、技術的には決定できない場合が多い。不正機能に関してコンセンサスの得られた明確な定義は未だ存在しないが、ここでは、以下の2段階の定義により、リスク管理上の漏れを回避する。

① **広義の不正機能**
不正機能の可能性がある脆弱性。検証要求のうち第1階層（p.8）が不正機能のカテゴリに該当するバックドア、無断送信、不正ロジック等の脆弱性。（具体例は検証要求の第4階層の検証項目に該当するもの。）これらの脆弱性のうち、**悪意が低いと想定されるものであっても、悪意が無いと立証することは難しい**ため、グレイなものも含めて管理漏れが無いように不正機能の可能性のあるものを広く対象とする。（例えば、解放ポートの残存など、故意か過失か判断は難しい）

② **狭義の不正機能（一般的に認識される不正機能）**
広義の不正機能のうち、悪意の可能性が高いと説明できる脆弱性。（例えば、機能仕様上必要のないレジストリ情報の外部送信や、セキュリティ成熟度の高いベンダーが、管理者パスワードをハードコードする初歩的な脆弱性など、**存在する正当な理由が説明できない脆弱性**）



脆弱性と留意事項の定義と追加検証の要否判断に関する整理

脆弱性と懸念事項の区分・定義は、各種標準の定義に整合させ、以下の案が考えられる。

- 脆弱性＝悪用されることでリスクとなる弱点。(「悪用される可能性」を拡張)
  判断の観点として、(1) 弱点に該当するかどうか？ (2)悪用によるリスクが存在するか？の2点あり。
- 懸念事項＝脆弱性には該当しないリスクとなる個所。

(1) 弱点に該当するか？
→ セキュリティポリシーによっては弱点とは言えない場合がある場合は脆弱性に含めない。→ユーザや利用環境によって脆弱性とは言えない。過剰な設定ポリシー。例：デーモン制限、多要素認証の要否など。

(2) 悪用によるリスクに該当するか？
→ 悪用される可能性が確認できないもの、再現性が十分確認できないものは脆弱性に含めない。

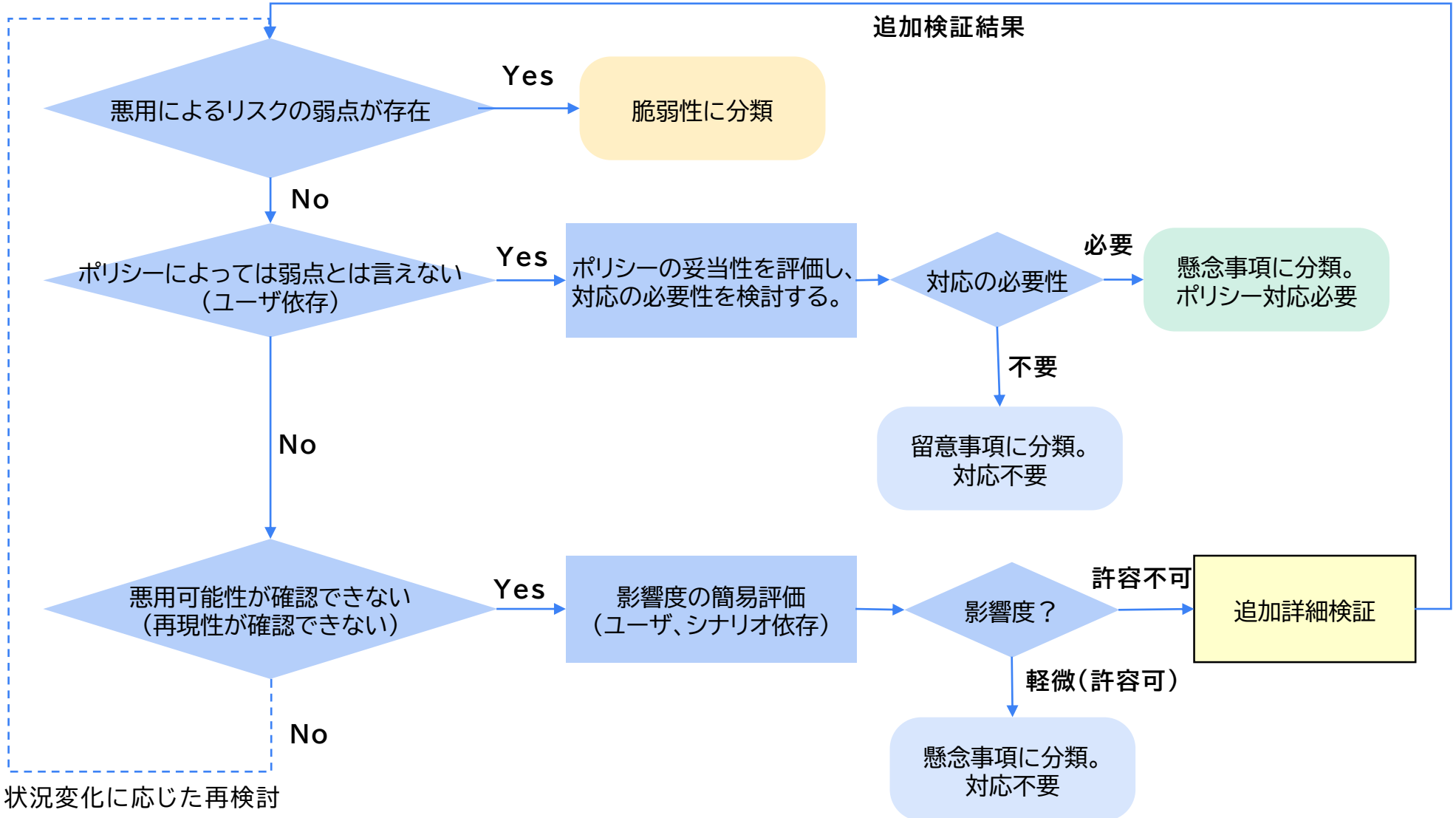
- (リスク)＝(発生可能性)×(影響度)＝(被攻撃可能性)×(脆弱性)×(影響度)の定義に基づき対応の要否を判断する。
- リスクのうち影響度が大きいものについては、追加詳細検証を行い、悪用可能性(発生可能性のサブセット)の評価につなげる。
- 影響度が不明のものについては、必要に応じて利用環境に応じた簡易的な影響度評価を行い、追加詳細検証の要否を判断する。

<table>
<tr><th colspan="3" rowspan="3"></th><th colspan="3">悪用可能性の確認状況</th></tr>
<tr><th colspan="2">確認できていない</th><th rowspan="2">確認できる</th></tr>
<tr><th>影響度：許容可</th><th>影響度：許容不可</th></tr>
<tr><td rowspan="3">弱点の該否</td><td rowspan="2">ポリシーによって異なる</td><td>対応が必要</td><td colspan="3">懸念事項
(ポリシー対応必要)</td></tr>
<tr><td>対応が不要</td><td colspan="3">留意事項
(ポリシー対応不要)</td></tr>
<tr><td colspan="2">該当</td><td>留意事項
(対応不要)</td><td>(追加検証)</td><td>脆弱性</td></tr>
</table>

悪用(外部からの攻撃)には依らない障害の原因となる不具合は脆弱性に含まない(一般的なバグ)。例：デッドロックなど。

脆弱性・留意事項の判別・対応ロジック

前頁の考え方に基づき、脆弱性と懸念事項の判断および対応のロジックは以下のように整理できる。



課題の全体像

- 本年度事業を通じて集約・整理した主な課題について、課題分類（技術、組織・体制）と実施時期（短期、中長期）に基づき全体像を以下に示す。

	短期課題（3年以内）	中長期（3年超）
技術	• セキュリティ検証先端技術の調査・探索 • 検証達成度に関するセキュリティ検証メトリクスの整備 • 不正機能検証・評価の高度化	• 自動検査手法（SCAP, SBOM,VEX）の活用方法の検討・実証 • 検証結果に基づく機器ベンダーのセキュリティ・エンジニアリング成熟度の評価手法の検討
組織・体制	• 脅威インテリジェンスに基づくリスク評価手法の調査 • オンデマンド検証プロセスの高度化（調達期間短縮、プロセス標準化、リソース管理など） • オンデマンド検証結果を踏まえた申合せ事務への反映プロセスの検討 • 本事業特有の用語の再整理・明確化（不正機能、懸念事項、達成度など）	• 検証事業者の評価選定のためのKPIと情報蓄積 • 検証事業者の拡大、知見の整備

達成度評価の高度化：セキュリティ検証メトリクスの構築

- セキュリティ検証の本質的な目的である脆弱性リスクが低いことを示すためには、検証のカバレッジや達成度に係るメトリクスを定義し評価することが必要である。
- ソフトウェア・テストにおいては、テストの達成度とその結果のソフトウェア品質の評価に用いられるテスト・メトリクスが体系化されており、それらを参考にセキュリティ分野においても検証メトリクスを定義することができる。
- これらは個々の脆弱性を挙げることとは本質的に異なる情報を持ち、本来検証に求められることである。

ソフトウェア・テスト分野では不具合の残留リスクが低いことを定量的に示すことが追求されている※。

セキュリティ業界では検証達成度の考え方が不十分

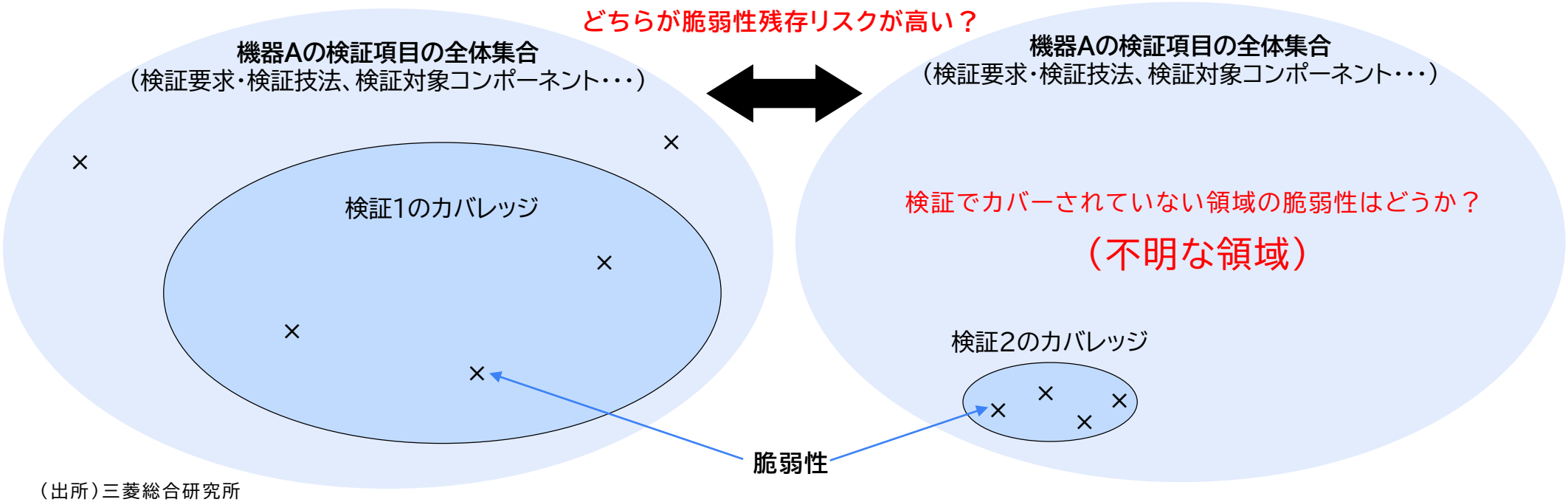
区分	ソフトウェア・テスト・メトリクス（既存）	セキュリティ検証メトリクス（新規提案）
プロダクト品質	テストカバレッジ（命令網羅C0，分岐網羅C1，条件網羅C2，複合条件網羅MCC，実行パス網羅、境界値網羅等）	CVE/CWEカバレッジ、検知ルールカバレッジ、脆弱性DBカバレッジ、製品・機器別検知ルール数、Exploitカバレッジ
	欠陥密度（/LOC）	脆弱性密度（/コード規模、/コスト、/検証達成度）
	テスト密度/欠陥密度比率	検証コスト/脆弱性密度比率
	ファンクションポイント	検証要求達成度（認証要求、アクセス制御、ネットワーク防御、データ管理、リソース管理、バックドア、無断通信、改ざん等）
	コンポーネントカバレッジ	コンポーネットカバレッジ、部品/SBOMカバレッジ
プロセス品質	バグ曲線（信頼性成長曲線）	脆弱性曲線（脆弱性検出飽和曲線）
	テスト技法カバレッジ（同値分割、境界値分析、全数検査、ランダム検査、HAYST法、状態遷移検査、モデル検査、形式検証、静的解析、CFD法、タイミング検査等）	検証技法達成度（脆弱性検査、ファジング、通信解析、パスワード解析、マルウェア解析、ソースコード解析、構成解析、形式検証等）
	テストプロセス適合性（テスト要求分析、テスト計画、テスト設計、テストケース生成、テスト評価・報告）	検証プロセス適合性（検証要求分析、検証設計、対象分析、検証実施、検証評価等）

（出所）三菱総合研究所

※：ISO/IEC/IEEE 29119 part 1-5: Software and systems engineering — Software testing

【参考】セキュリティ検証の本質的な目的と検証達成度の意義、今後の課題

- セキュリティ検証の目的は、脆弱性を見つけることが本質ではなく、脆弱性の残留リスク（脆弱性リスク）が低いことを示すことが本質。
- 脆弱性リスクを示すことができなければ、機器調達の判断には有効ではない。（セキュリティ・アシュアランスの必要性）
- 脆弱性をいくら沢山見つけても、検証項目の網羅性が低ければ、残留する脆弱性が少ないことの説明にはならない。
- ソフトウェアテスト※1においてはその達成度を評価するための方法としてテストメトリクス※2が定義されている。それらを参考に、検証メトリクスを定義することで、脆弱性リスクが低いことを評価することが可能になると考えられる。
- 本事業ではその一環として、検証要求・検証技法の達成度を評価することで脆弱性リスク捉えるアプローチを検討してきた。今後の課題として、検証メトリクスとして、検証対象範囲（コンポーネント）のカバレッジ、脆弱性検出曲線（検証項目数に対する検出脆弱性の成長曲線飽和度）などを組合わせることが有効と考えられる。



（出所）三菱総合研究所

※1：ISO/IEC/IEEE 29119 part 1-5: Software and systems engineering — Software testing
ISO/IEC 33063:2015 Information technology — Process assessment — Process assessment model for software testing
※2：テストメトリクス＝テストカバレッジ、テスト技法カバレッジ、バグ曲線（信頼性成長曲線）、テストプロセス評価なのテスト品質を評価する尺度

検証事業者の評価選定のためのKPIと情報蓄積

- 検証事業者の委託選定においては、全体のリスクを最小化するための技術検証における外部リソース活用の最適化の観点で検討する必要がある。国内外の検証事業者のリソースに限りがある中で、それぞれの能力・リソースを把握し、検証の目的や要求ニーズに応じて、適材適所の選定により費用対効果を最大化しなければならない。
- そのためには検証要求を明確にするとともに、それらに適した検証事業者の選定方法を検討するだけではなく、選定した検証事業者の進捗管理、モニタリング、成果物の評価を通じて検証事業者の評価情報を蓄積することが必要である。検証のパフォーマンスを最大化するという観点では、以下のQCDRの要素を考慮に入れて可視化、透明性の確保が重要である。

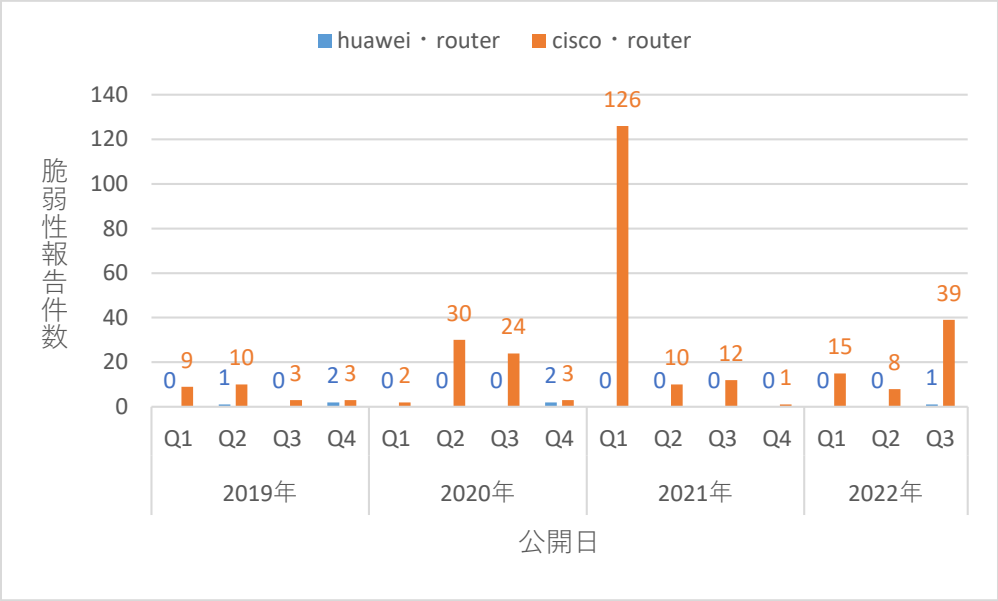
区分	評価指標(KPI)
品質(Quality)	検証の成果(脆弱性の検出結果、検証達成度)、報告書の品質。検証結果におけるミスの件数、報告書ページあたり等の単位あたりのレビューコメント件数、修正依頼件数などから報告書品質を定量化する。
コスト(Cost)	検証事業者の要員クラスの人件費単価、要員クラスの分類体系
納期(Delivery)	オンデマンド検証等における計画に対する納期の遵守、調達の迅速性
リスク(Risk)	期間制約における人員リソースの不足等

(出所)三菱総合研究所

目的

- 脆弱性情報など運用ツールで管理される情報を用いて、未検証機器のリスクの大小を推定し、機器調達の可否の判断の参考となる分析結果を提供することを目的とする。
- そのために、運用ツールで管理される情報（検証結果（脆弱性情報、検証達成度）、外形情報（外部の脆弱性情報、機器情報、ベンダー情報等））のうち対象とする情報を明確にし、適用する分析手法の特徴に基づき、推定方法を定式化することで、算出する推定値の意味とその活用方法、課題等について整理する。

脆弱性情報（例）



リスク値推論

リスク値（例）

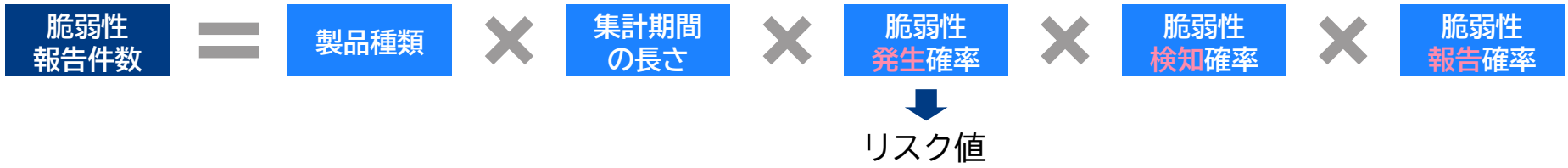
	ベンダA	ベンダB
〇年〇月～〇年△月	0.X	0.Y
〇年〇月～〇年△月	0.X	0.Y
〇年〇月～〇年△月	0.X	0.Y

出所）NVDより三菱総合研究所が作成

米国NISTが公開するNational Vulnerability Database（NVD）において、2019年1月から2022年9月までの間に公開されたHuawei製ルータ、Cisco Systems製ルータの脆弱性報告件数を四半期ごとに集計した。

推定アプローチ（考え方）

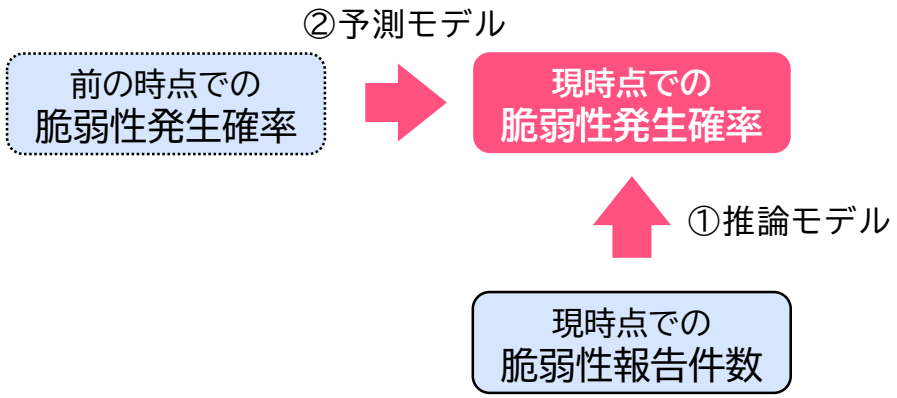
- **脆弱性報告件数を以下のように要素分解し、「脆弱性発生確率が高くなる確率」をリスク値として推論。**



- **推論にあたっては以下の仮定をおいた。**
- 「脆弱性検知確率」、「脆弱性報告確率」は一定
  - ある製品において**脆弱性が検知される**確率や**報告される**確率は、ベンダや製品によらず一定になると仮定。
  - 実際にはベンダが展開する**地域や利用者に応じて**変動すると考えられるが、簡略化のため上記のように仮定。
- 「脆弱性発生確率」は同一ベンダであれば一定
  - あるベンダにおいて**脆弱性が発生する**確率は、製品によらず一定になると仮定。
  - 実際には**製品によって**開発チームが異なるなど変動すると考えられるが、簡略化のため上記のように仮定。
- 「製品種類」は集計期間中の全社売上に比例
  - あるベンダの製品種類は、事業規模（具体的には**集計期間中の全社売上**）に比例すると仮定。
  - 実際には、同じ売上であっても、少ない種類の製品を展開するベンダより多くの種類の製品を展開するベンダのほうが脆弱性報告件数が大きくなると考えられるが、簡略化のため上記のように仮定。

推定方法(1/2)

- 前頁の要素分解を踏まえ、リスク値(脆弱性発生確率が高くなる確率)は、脆弱性報告件数と事業規模を入力として推定を行う。
- これらは時間変化する値であるため、下図に示す推論モデルと予測モデルを組み合わせることで「過去から現在までの脆弱性報告件数と事業規模」から「現在の脆弱性発生確率」を推定する。
- 推論モデルと予測モデルの計算にはベイズの定理をもとに時間変化する値を扱うことを前提とするベイズフィルタ[1]という手法を用いた。

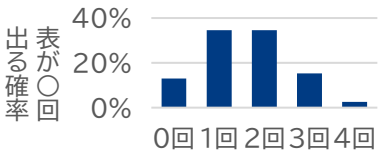


①推論モデル	現在の入力(脆弱性報告件数、事業売上)を踏まえ、現在の脆弱性発生確率を推論するモデル。
②予測モデル	過去の脆弱性発生確率を踏まえ、脆弱性発生確率がどのように変化するか予測するモデル。

[1] Thrun, S., Burgard, W., Fox, D., (2005), Probablistic robotics, The MIT Press.(上田隆一訳(2007),「確率ロボティクス」, 毎日コミュニケーションズ)

推定方法（2/2）

- **推定手法に関するパラメータは以下のとおり。**

集計期間の単位	**本年度事業では四半期（※）単位で集計。** 時期に応じた変動を捉えるため、可能な限り短く設定。ただし短すぎる場合、脆弱性報告件数に人為的な偏り（クリスマスの時期は件数が少ない等）が生じる懸念が存在するため、四半期単位とした。 ※1Q：1月～3月、2Q：4月～6月、3Q：7月～9月、4Q：10月～12月
脆弱性発生確率の確率分布（リスク値の定義）	**脆弱性発生確率は「高」または「低」のいずれかの値をとる。** 正規分布に従う等の選択肢も存在するが、簡略化のため二値とした。 なお、リスク値は脆弱性発生確率が高くなる確率であるため、0から1の間の値をとる。
脆弱性発生確率の変動確率（前述のモデル②）	**脆弱性発生確率はベンダによらず一定の確率で四半期ごとに変動する。** 「高⇒高」「高⇒低」「低⇒高」「低⇒低」の4パターンがあり、それぞれの確率を設定する。 技術力が高いベンダであれば、脆弱性の迅速な解消（「高⇒高」より「高⇒低」が大きい）や脆弱性の予防（「低⇒高」より「低⇒低」が大きい）が期待される。このように脆弱性発生確率の時間変動確率は、ベンダによって異なる可能性があるが、簡略化のためベンダによらず一定とした。
脆弱性報告件数の確率分布（前述のモデル①）	**脆弱性報告件数は二項分布に従うものとする。** 二項分布は確率pと正規化母数Nの2つのパラメータを持つ確率分布。例えば、「確率pで表が出るコインをN回投げたときに表が出る回数」は二項分布に従う。リスク値推論においては「確率p」が「脆弱性発生確率」であり、「正規化母数」は「全社売上」（後述）とする。 【参考】 「確率0.4で表が出るコインを4回投げたときに表が出る回数」の分布は右図のとおり。 
正規化母数	**上述の「正規化母数」は集計期間中の売上（百万米ドル単位）とする。** 製品種類が多いベンダほど脆弱性報告件数は大きくなると考えられるため、売上が大きいベンダほど正規化母数が大きくなるようにパラメータを設定。これは、売上が大きいベンダほど製品種類（＝コインを投げる回数）が多くなることのモデル化である。

課題の整理

リスク値推論における主な課題は以下のとおり。

- リスク推定モデルの高度化
  - ベンダーの機器区分ごと脆弱性発生状況、検証結果の脆弱性区分などの情報を活用したセキュリティエンジニアリング成熟度の評価を考慮したリスク推定モデルの高度化。
  - 実際の**「脆弱性発生確率」は、同一ベンダでも製品によって異なる**可能性が存在。そのため、モデルでも同様の仮定をおくことが有効と考えられる。ただし、NVDでは製品種別を機械的に判別困難のため、データ取得がボトルネックと考えられる。
  - **「脆弱性発生確率」は0から1の間の値を取る**ほうが、「高」「低」の二値を取るよりも実態と合致する可能性が存在。ただし、高度な計算ソフトの導入が必要になる可能性が高い。
  - **「脆弱性発生確率」の変動確率**は、脆弱性の解消に要する期間や脆弱性の予防能力に関わるため、**ベンダで異なることを仮定**することが有効となる可能性が存在。ただし、ベンダごとにパラメータを設定する必要があるため、モデルが複雑化することが懸念される。
- NVDにおける脆弱性報告件数が実態よりも過小となるベンダが存在する可能性
  - **「脆弱性検知確率」と「脆弱性報告確率」はベンダによって異なる可能性**が存在。例えば米国におけるシェアが小さいベンダは、製品の脆弱性が検知・報告される機会が少なく、NVDに掲載されにくい可能性がある。その場合、NVDを入力とする本モデルでは実態よりも小さいリスク値が推論されることが懸念される。
- 正規化母数として全社売上を用いることの適切性
  - 同じ売上であっても、**展開する製品が多いベンダのほうが脆弱性報告件数が大きくなる可能性**が存在。また、製品単価や他事業分野への参入等の影響により、**製品種類と全社売上が連動しない可能性**が存在。
- パラメータチューニングの必要性
  - パラメータによって本モデルの挙動は変化する。そのため、より多くの実データに適用し、目的に沿った結果となるようパラメータチューニングをする必要がある。
    （高度な計算ソフトを用いることで自動で学習するようなモデルを構築することも可能だが、目的を定量的に定義づけする必要がある。）

サプライチェーンリスク対応のための技術検証体制構築等に関する調査（不正機能に関する調査）

2023年6月
内閣官房内閣サイバーセキュリティセンター(NISC)

※本調査はNISCの委託により、株式会社FFRIセキュリティが実施したものです。

背景と目的

- サイバー空間と実空間の一体化が加速的に進展し、情報通信機器のみならず様々な機器がサイバー空間を介して国民の生活に結びついている現状において、これらの機器の信頼性を確保することはより一層不可欠なものとなっている

- 機器の信頼性を確保するためには、サプライチェーンリスクについても技術的な検証により信頼性が確保されていることが不可欠である

- 実際の製品に不正機能や未知の脆弱性等が存在しないかどうかの技術的な検証の精度の向上および効率化を行う上で、不正機能の脅威の定量化が望まれる

- ITシステムを構成する様々な情報通信機器およびソフトウェアに組み込まれた不正機能について、体系整理と傾向分析、不正機能事例に関する事例に基づいた技術的な調査を実施し、不正機能の脅威の定量化について検討した結果を報告する

調査の進め方

- 本調査では、「１．不正機能の事例収集と分析」「２．不正機能の脅威の定量化の検討」「３．定量化方法の妥当性の確認」および「４．課題と知見の抽出」の４つの検討プロセスを約５週間のサイクルで３回実施する反復型のアプローチを採用した（図1-1　参照）

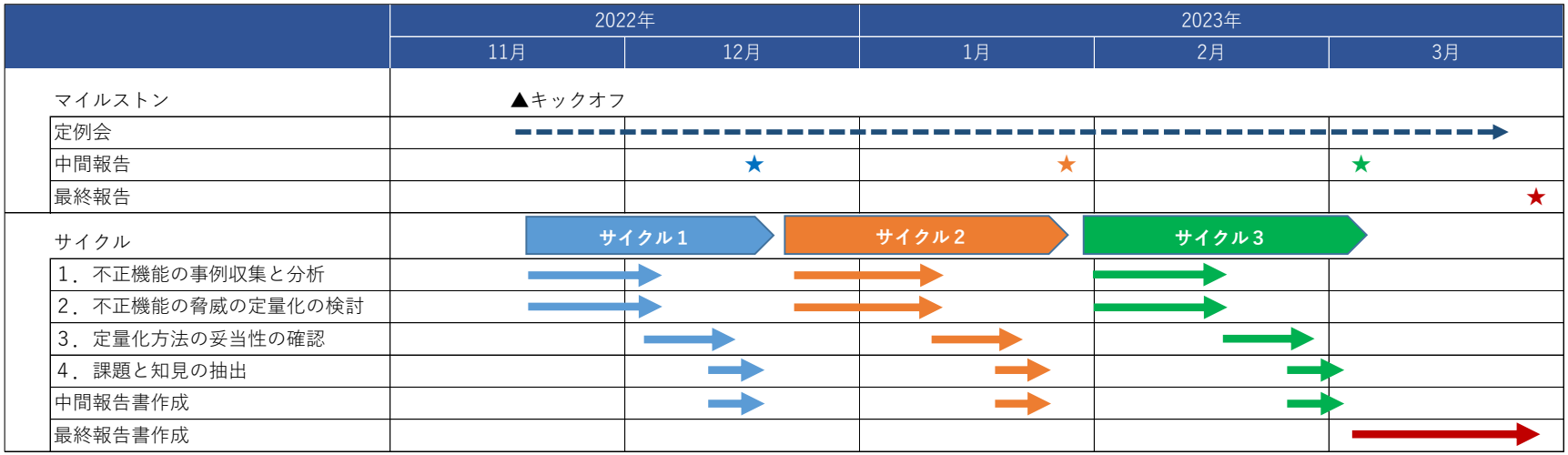


図1-1　反復型アプローチ

調査の進め方

- 本調査では、一つ前のサイクルで得た知見と課題をインプットとして、不正機能の脅威の定量化の検討を繰り返した
- また、昨年度の分析事例および１つ前のサイクルの分析事例について、当該サイクルで検討した定量化手法でスコア化し、個々の事例の周辺情報などから定性的に判断した「事例分析者の主観による評価」との差異を評価することで、課題を抽出した

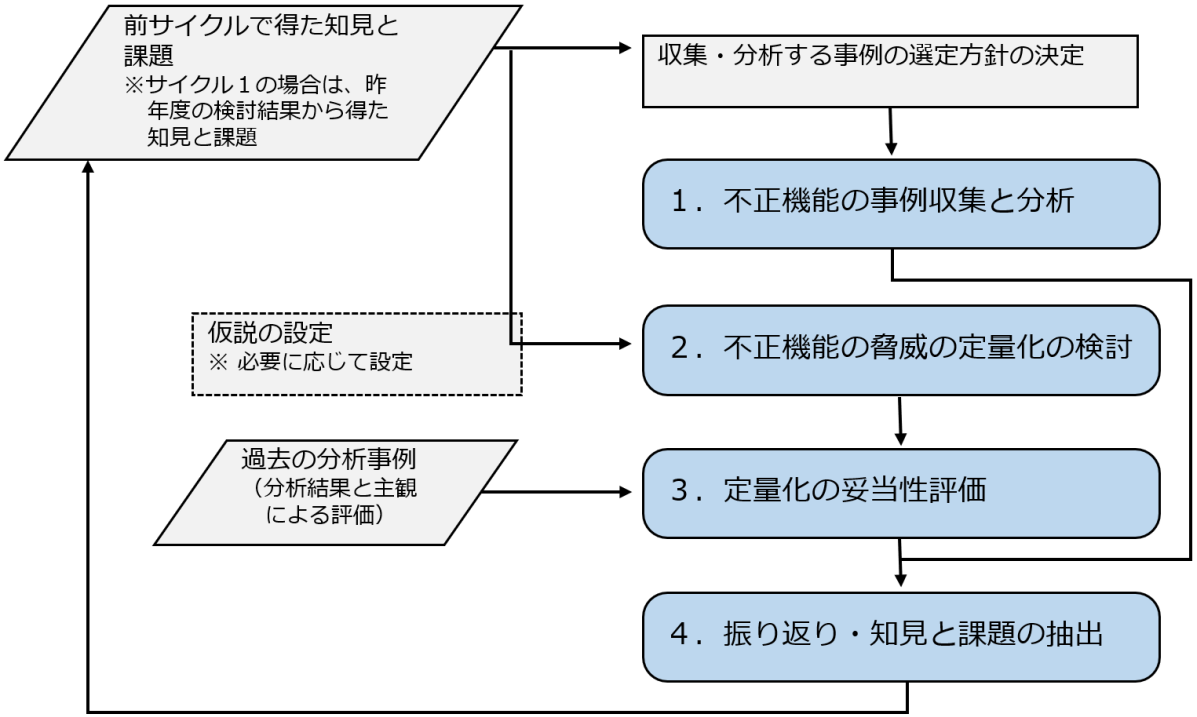
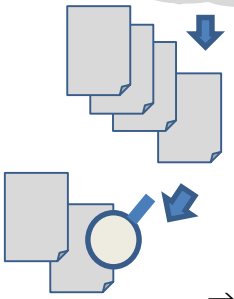


図1-2　各サイクルの進め方イメージ

結果まとめ

- 本調査において、不正機能が疑われる事例の収集と分析を行い、分析結果から不正機能の程度を計る指標として**「攻撃意図性の高さ」**を数値化することを試みた

1．事例収集と分析



下記の通り事例の収集・分析を行った

- 61件の事例を収集
  - 2021年度：44件
  - 2022年度：17件（New）
- 33件の事例を分析
  - 2021年度：16件
  - 2022年度：17件（New）

→ 未分析の事例に優先順位をつけて分析

2．不正機能の脅威の定量化の検討

不正機能かどうかを判定するためには、不正機能の疑義のある機能が意図的に実装されたものか否かの判断が重要となる

「攻撃意図性の高さ」を数値化して不正機能かどうか判定する目的で、以下の計算式と判定の基準を定義した

[計算式] **攻撃意図性の高さ（X） ＝ 「隠ぺいの意図」のスコア**
× 重みA（機能実装者の攻撃容易性のスコア × 影響度数）
× 重みB（標的型攻撃との関連性のスコア × 影響度数

[判定の基準]

X＝0～5 ：攻撃意図性は低い	X＝21～99：攻撃意図性は高い
X＝6～20 ：判定不能	X＝100～ ：攻撃意図性は非常に高い

【計算式の意味について】

・「機能実装者の攻撃容易性」と「標的型攻撃との関連性」は「隠ぺいの意図性」のスコアを算出するための評価項目すべてに影響を及ぼすと考え、積算によって「攻撃意図性の高さ」を算定

・「影響度数」として、「機能実装者の攻撃容易性」と「標的型攻撃との関連性」の攻撃意図性に対する影響度を数値化

【判定の基準ついて】

・分析事例の主観的な評価に基づいて、判定の基準を設定

・それぞれの意味は下記の通り

攻撃意図性は低い：不正機能ではない可能性が高い
攻撃意図性は高い：不正機能である可能性が高い
攻撃意図性は非常に高い：不正機能かつ標的型攻撃である可能性が高い
判定不能：不正機能かどうか判断がつかない領域

3．定量化方法の妥当性の確認

事例分析者の主観による評価と「攻撃意図性の高さ」による判定結果を突合し、下記の結果が得られた

- 明らかに不正機能と思われる事例は不正機能と正しく判定できている
- 主観的な評価では不正機能か否かの判断がつかなかった事例の判定ができた
- 誤った判定も存在し、改善の余地も残されている

4．課題の抽出

今後の課題として下記が考えられる

- 事例の種類と分析事例の積み増し
- 「当該箇所で何ができるか」の評価項目に関する再検討
- 「判定不能」や誤った判定の改善
- 定量化手法の最適性評価

サプライチェーンリスク対応のための技術検証体制構築等に関する調査
(SBOMの活用に関する調査)

2023年6月
内閣官房内閣サイバーセキュリティセンター(NISC)

※本調査はNISCの委託により、NRIセキュアテクノロジーズ株式会社が実施したものです。

(１)SBOMに係る既存技術・研究の調査
(ア)SBOMの標準に関する調査

調査結果サマリ：主要なSBOMフォーマットの調査

■ 一般的なSBOMユースケースとして、ライセンス管理、セキュリティ管理、ソフトウェア識別管理がある。この３つのユースケースに対して各標準フォーマットがどのように対応しているか、それぞれのデータフォーマット(データフィールド)を分析すると、SPDXはライセンス管理、CycloneDXはセキュリティ管理、SWIDはソフトウェア識別管理、SPDX-Liteは運用性を重視したライセンス管理、といった際立った特徴を有することが明らかとなった。

	各標準のデータフォーマット					米国大統領令(2021年5月)からのフォーマットの構成の変化				サプライチェーンへの活用事例報告(国内)	特徴分析
	最小要素への対応	最小要素以外の要素									
		スニペット	ライセンス管理	セキュリティ管理	ソフトウェア識別管理	相互運用性	ライセンス管理	セキュリティ管理	ソフトウェア識別管理		
SPDX	○	○	◎	○	○	追加対応	—	追加対応	—	✓ 確認できず	✓ ライセンスの詳細管理が可能 ✓ スニペットの識別も可能 ✓ 公開された実例報告は確認できず
SPDX-Lite	**2項目未対応** ● Dependency Relationship ● Component Hash	×	○	△	○	—	—	—	—	✓ トヨタ、日立等の国内メーカーにおける普及活動	✓ 運用性を重視(詳細識別、網羅的な管理は行わない) ✓ エクセル管理を想定している ✓ 国内メーカーでの利用が進んでいる
CycloneDX	○	×	○	◎	○	—	—	VEX対応	—	✓ 確認できず	✓ セキュリティ管理に焦点 ✓ 公開された実例報告は確認できず
SWID	**1項目未対応** ● timestamp	×	×	×	◎	—	—	—	—	✓ 確認できず	✓ ソフトウェア識別子としての活用に焦点 ✓ 公開された実例報告は確認できず

凡例：◎：他規格と比べて詳細度が高い、○：対応している、△：対応可能、×：対応していない(把握できない場合も含む)

調査結果サマリ：主要なSBOMフォーマットの調査 考察

- SBOM標準フォーマットは国際標準化されているものもあり、非常に表現力の高いフォーマットになっている
- しかし自由度の高さから依存関係をどこまで記載するか、どのデータフィールドを採用するか等、SBOMの粒度はSBOM作成者の判断に委ねられている
- 同じフォーマットを使っていても作成側・受取側の双方の基準が一致しないと十分に活用できないため、各業界毎の標準が求められることになる

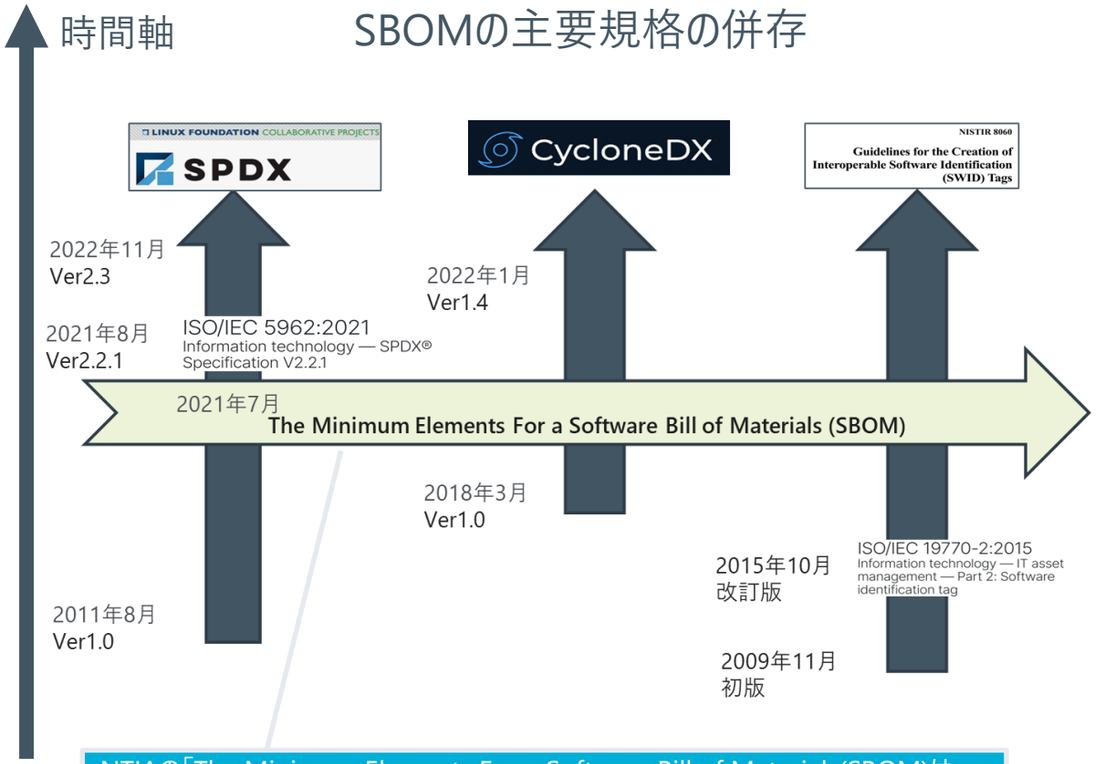
- その結果、
  - 日本では経産省の実証実験、また製造業を中心にSPDX-Liteの実践が行われている
  - 海外でも政府機関や業界団体が主導し、規制の枠組みの検討が行われている
  - 特に自動車、医療機器、エネルギー業界等で活発な議論が行われている

- つまり、
  - ✓ **SBOMフォーマットはSBOM社会実装の必要条件だが、十分条件ではない**
  - ✓ **業界標準の整備がSBOM社会実装の十分条件である**

調査結果サマリ：主要なSBOMフォーマットの調査 考察

- 当面、複数規格の併存、派生規格・ローカライズでの対応が継続すると考えられる
- ツール選定やSBOM管理においては、複数フォーマットに対応していることが重要と考えられる

規格数	派生規格・ローカライズ：あり	派生規格・ローカライズ：なし
複数	＜現状＞ ➢ ３つの規格が併存 ➢ リスクの大きさに応じ、最小要素ガイドライン(後述)に沿った管理とより簡素な管理の二極の動きが起きている ● リスク管理の観点で最小要素ガイドライン(後述)に沿った管理を志向するアプローチ(米国医療機器業界等) ● 広範な実践重視の観点で簡素管理を志向するアプローチ(SPDX-Lite)	動き無し
統合	相互運用性を高める動きはあるが、統合の動きは無し	



NTIAの「The Minimum Elements For a Software Bill of Materials(SBOM)は、SBOMに最低限含まれるべき要素を示すために作成された文書である。
従来からあるSBOM標準規格を統一するために作成された文書ではない。

調査結果サマリ：主要なSBOMフォーマットの調査 考察

- NTIA Minimum Elementsガイドラインでは「プラクティスとプロセス」の項目で、関係者間で合意形成すべき事項への言及がある。
- この項目ではSBOMの作成を開発プロセスへ統合すること、カスタマーによるサプライヤーへのSBOM提供の要求等、方針・契約、その他の取り決めにおいて明示的に合意すべき実施事項が提示されている。
- ただし、合意形成の水準までは明示されていない。

プラクティス領域	要件
Frequency SBOMの作成頻度	● ソフトウェアコンポーネントが新しいビルドまたはリリースで更新された場合は、新しいバージョンのソフトウェアが反映された新しいSBOMを作成する必要がある ● 既存のSBOMデータを修正したい場合は、サプライヤーは新しい改訂されたSBOMを発行する必要がある
Depth SBOMの深さ	● SBOMには全てのプライマリ (トップレベル) コンポーネントが含まれ、全ての推移的な依存関係がリストされている必要がある ● 少なくとも全てのトップレベルの依存関係は、推移的な依存関係を再帰的に検索するのに十分な詳細とともにリストされる必要がある
Known Unknowns 既知の未知数	● SBOMで完全な依存関係グラフが列挙されていない場合、SBOM作成者は「既知の不明」を明示的に識別する必要がある。つまり、依存関係データは、それ以上の依存関係を持たないコンポーネントと依存関係の存在が不明で不完全なコンポーネントを明確に区別する。 ● 誤った仮定を避けるために、データのデフォルトの解釈は、データが不完全と設定するべきである。
Distribution and Delivery 配布と共有	● 必要とするユーザがSBOMをタイムリーに利用できるようにする必要があり、適切なアクセス許可とロールを用意する必要がある
Access Control アクセス管理	● アクセス制御が必要な場合は、SBOMデータをユーザのセキュリティツールに統合するための条件を指定する必要がある
Accommodation of Mistakes ミスの調整	● 最初のSBOM実装においては、データの欠落やエラーの発生を許容し、それらのミスを調整するプロセスを用意する必要がある ● サプライヤーは過去のSBOMの問題に直面した際に更新されたデータを提供し、利用者は落ち度なく提供されたSBOMについてはペナルティなしで補正や修正を受入れることで、SBOMの更新を促す必要がある

調査結果サマリ：主要なSBOMフォーマットの調査 考察

- 他方、NTIAが発行している別文書(※SBOM Options and Decision Points)においても、SBOMの要求者と供給者の間で下表に掲げる事項について合意形成を行う必要があること、さらに合意形成のレベル(水準)についても指針が示されている。
- 合意形成のレベルについては下記3段階が示されており、初期コンセンサスについては最小要素と同程度の要求事項が記載されている。
  - 現代の開発プロセスで可能なこと (初期コンセンサス)
  - 初期コンセンサスより高保証のユースケースのための機能強化(+)
  - 業界の導入時間とレガシープロセス/テクノロジーに対応するためのフォールバック(−)
- SBOM最小要素の実装のためには標準フォーマットを選択するだけでは十分ではない。その活用方法について、関係者間で合意形成することが必要となる。

区分	−	初期コンセンサス	+	備考
ベースラインコンポーネント情報	ベースラインコンポーネント情報の コアサブセット*を含む	全てのベースラインコンポーネント情報* 属性を含む	高保証のユースケースをサポートする ベースラインを超えるコンポーネント情報を含む	データフォーマットとして記載
フォーマットと機械可読性	任意の機械可読形式のSBOM (例:csv)	ベースライン対応で機械可読形式のSBOM*	全ての機械可読、相互運用可能な形式のSBOM*、 標準の進化や出現に合わせて維持	自動化のサポートとして記載
深さ(粒度)	直接の依存関係と既知の不明が宣言された 全ての主要コンポーネント	全ての推移的な依存関係と既知の未知が 宣言された全て主要コンポーネント	未知数の無い全ての推移的な依存関係を持つ 全ての主要コンポーネント	Depthとして記載
発生頻度	事前/購入時 および/または 要求に応じて提供されたx時間以内	コードの更新や 変更 (メジャー/マイナーリリースやパッチ) 毎	全てのバージョンのアーカイブでホスト	Frequencyとして記載
配信と相互運用性	サプライヤが電子メールで送信 またはホスト/アーカイブ	全ての製品バージョンにバンドルされ サプライヤーによってアーカイブされる	マシンインターフェイス(例:API)と隣接する相互運用性 (例:DBOM、MUD、OpenC 2)をサポート	Minimum Elements では触れられていない
隣接する拡張:脆弱性のクレーム	サプライヤーは、要求に応じて潜在的に 悪用可能な脆弱性の証明を行う	サプライヤーは新たな脆弱性のx時間以内に 悪用される可能性のある脆弱性の証明を行う	SBOMコンポーネントに対する製品固有のリスクの 証明のために標準化されたAPIクエリ	Minimum Elements では触れられていない

※ ベースラインコンポーネント情報のコアサブセット:コンポーネント名、サプライヤ名、バージョン文字列、一意の識別子
※ ベースラインコンポーネント情報:作成者名、サプライヤ名、コンポーネント名、バージョン文字列、コンポーネントハッシュ、一意の識別子、関係
※ SBOM形式:SPDX、CycloneDX、SWID

※出所)SBOM Options and Decision Points

調査結果サマリ：The Minimum Elements For a Software Bill of Materials(NTIA)

■ 米国大統領令(EO14028)を受け、NTIA(米国商務省電気通信情報局)は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7月12日に公開した。

- 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ている。
- これら3つのカテゴリーは、脆弱性管理、ソフトウェアインベントリ管理、ソフトウェアライセンス管理の基本的なユースケースを可能にするSBOMの最小要素を定義したものである。
- 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。
- 定義された「最小要素」に基づきソフトウェア購入者へのSBOM提供に関するガイダンスが整備される他、 将来的には各省庁のソフトウェアに関する取組が本定義に基づき実施されることが明記されている。

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

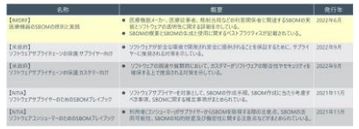
出所)サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性
令和3年10月29日 経済産業省 商務情報政策局 サイバーセキュリティ課

調査結果サマリ：SBOMの活用に関するガイドライン

- 2021年7月に公開された「The Minimum Elements For a Software Bill of Materials」以降、ソフトウェア購入者(カスタマー)やソフトウェア供給者(サプライヤー)向けに、SBOMの作成や提供に関するガイダンスが整備されている。
- 本調査では米国で発行されたガイドラインの内、発行年が新しい以下の6つのガイドラインを取り上げる。

名称	概要	発行年
【IMDRF】 医療機器のSBOMの原則と実践	● 医療機器メーカー、医療従事者、規制当局などの利害関係者に関連するSBOMの実装とソフトウェアの透明性に関する詳細を示している。 ● SBOMの概要とSBOMの生成と使用に関するベストプラクティスが記載されている。	2022年6月
【米政府】 ソフトウェアサプライチェーンの保護:サプライヤー向け	● ソフトウェアが安全な環境で開発され安全に提供されることを保証するために、サプライヤーに推奨される対策を示している。	2022年9月
【米政府】 ソフトウェアサプライチェーンの保護:カスタマー向け	● ソフトウェアの調達や展開時において、カスタマーがソフトウェアの整合性やセキュリティを確保する上で推奨される対策を示している。	2022年9月
【NTIA】 ソフトウェアサプライヤーのためのSBOMプレイブック	● ソフトウェアサプライヤーを対象として、SBOMの作成手順、SBOM作成に当たり考慮すべき事項、SBOMに関する補足事項がまとめられている。	2021年11月
【NTIA】 ソフトウェアコンシューマーのためのSBOMプレイブック	● 利用者(コンシューマー)がサプライヤーから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などがまとめられていいる。	2021年11月

調査結果サマリ：【IMDRF】医療機器のSBOMの原則と実践



■ 医療機器メーカー、医療従事者、規制当局等の医療機器に関連する利害関係者が関係するSBOMの実装とソフトウェアの透明性に関する詳細情報を提供することを目的とし、SBOMの概要とSBOMの作成と使用に関するベストプラクティスが記載されている。

医療機器メーカーが考慮すべきこと

- **SBOMコンテンツの収集**
  SBOMを作成するためのコンテンツ収集において、ソースの中身が不完全/古いものである可能性があることに留意する。
- **SBOMの作成**
  SBOMの一貫した出力を確保するためにも、確立されたSBOM作成方法に従う必要がある。
- **SBOMの配布**
  医療従事者に対しSBOMの存在を認識させると共に、SBOMを配布またはアクセスできるようにする。
- **脆弱性の監視**
  SBOMに脆弱性情報は含まれていないため、SBOMを他のリソース(VEX等)と組み合わせて医療機器の脆弱性を監視する。
- **SBOMの課題**
  レガシーな医療機器に対してSBOMを作成する際、利用できる情報に制限がある可能性がある。

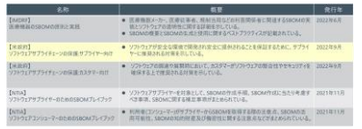
医療従事者が考慮すべきこと

- **SBOMの取り込みと管理**
  ハードウェアやネットワーク上で実行されているソフトウェアのインベントリを把握するためには、SBOMの活用が重要となる。デバイスで実行されているソフトウェアのインベントリ情報の収集は、医療機器メーカーからの情報提供が必要。SBOMは医療機器メーカーと医療従事者の間で、この情報を透過的に共有する際に有効的な方法である。
- **SBOMの取り込みと管理の方法**
  SBOMは時間の経過と共に更新される可能性があるため、効率的に管理を行うためにもSBOMの取り込みは自動化される必要がある。
  SBOMを直接取り込む、またはカスタムツールを使用する場合、医療従事者は電子フォーマットの独自性を考慮する必要がある。(SBOMをシステムに統合するために必要な権限を所持しているかどうか等)。

ユースケース

- **リスク管理**
  SBOMはデバイスソフトウェアに何が含まれているか、可能性のあるリスクに関してより高い透明性を提供するために使われる。医療従事者はデバイスがTPLC(トータル製品ライフサイクル)を進行するにつれて利点とリスクをより理解し、デバイスのライフサイクル全体でリスク管理手段と軽減戦略をより効果的に適用することが可能となる。
- **脆弱性管理**
  SBOMを使用することで、医療機器メーカーは関連する脆弱性情報から影響を受けるソフトウェアコンポーネントに基づいて、脆弱性の影響が及ぶ可能性のある医療機器を効率的に特定することができる。
- **インシデント管理**
  体系的な情報収集、相関、評価を通してサイバーセキュリティ関連のイベントを検出することで、インシデント処理を改善していくことが可能となる。

調査結果サマリ：【米政府】ソフトウェアサプライチェーンの保護:サプライヤー向け



■ ソフトウェアが安全な環境で開発され安全に提供されることを保証するために、サプライヤーに推奨される対策を示している。

ソフトウェアサプライチェーンの保護:サプライヤー向け 概要

※サイバーセキュリティおよびインフラストラクチャセキュリティ局(CISA)、国家情報長官室(ODNI)、国家安全保障局(NSA)

ソフトウェアの配付、開発、運用/保守フェーズにおける脅威と対策がそれぞれ示されている。

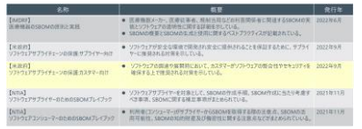
■ 脆弱性への対応 -継続的な脆弱性の特定、分析、修復-

- サプライヤーは、顧客に提供されるソフトウェアに脆弱性が存在しないことを保証する必要がある。
- ソフトウェアの脆弱性を診断することで、侵害され得る脆弱性を顧客に提供してしまうことを未然に防ぐことができる。

■ 推奨緩和策

- アーキテクト、開発者、テスター等で構成される脆弱性診断チームを作成し、ソフトウェアの脆弱性を特定する。
- ソフトウェア機能について、ファジング(ファズテスト)を実施する。
- 静的・動的テストツールについて、それらを最新の状態に保ち、提供元の文書に従って実装する。
- PSIRTチームを作成し、組織のPSIRT情報を外部に公開する。組織は全ての脆弱性について責任ある開示を実践すべきである。
- 既知のセキュリティ問題や脆弱性は全て、バグ追跡ツールで確認する必要がある。
- ソフトウェアコンポーネントまたはパッケージを構成する可能性のある要素に対して、十分な人的/コンピューティングリソース、ソフトウェアテスト、およびテスト時間を確保する。
- 特定した脆弱性を排除または文書化する。
- **開発したソフトウェアに関連するサードパーティ製ソフトウェア、およびオープンソースコンポーネントのSBOMを確認する。**
- ソフトウェアコンポーネントを変更する場合は、そのユニットとシステムに対してここで推奨される手順を繰り返す。
- サードパーティ製ソフトウェア(例：バイナリソフトウェア構成分析の使用)のレビューを実施し、同梱されているモジュールのセキュリティを保証する。

調査結果サマリ：【米政府】ソフトウェアサプライチェーンの保護:カスタマー向け



■ ソフトウェアの調達や展開時において、カスタマーがソフトウェアの整合性やセキュリティを確保する上で推奨される対策を示している。

※サイバーセキュリティおよびインフラストラクチャセキュリティ局(CISA)、国家情報長官室(ODNI)、国家安全保障局(NSA)

ソフトウェアの調達時

要件定義、製品評価、契約のフェーズにおいて生じ得る脅威とそれに対する対策が示されている。その中でSBOMについて言及されているのは以下の通り。

- **製品評価**
  評価対象のソフトウェアに対してSBOMの内容を確認し、脆弱性を発見すると共に、関連するリスクの軽減を目的として関連するサードパーティーを特定し、評価対象に含める。
- **契約**
  SBOMが欠落していることによりソフトウェアの整合性が保証できなかったり、ソフトウェア提供前にサプライヤーによってコンポーネントを変更されるといった脅威を防ぐためにも、サプライヤーに対してアーティファクトを、標準化されたSBOM形式で要求する必要がある。
  また、全てのアップデートに対してSBOMを提供するように要求し、SBOMにアップデートにおける変更点が記載されていることを確認する必要がある。

ソフトウェアの展開時

製品の受け入れ、機能テスト、セキュリティテスト、動作環境への統合、運用開始時などのフェーズにおいて生じ得る脅威とそれに対する対策が示されている。その中でSBOMについて言及されているのは以下の通り。

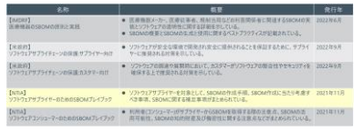
- **製品の受け入れ**
  注文したソフトウェアが改竄されていないか、他の製品に置き換えられていないかをSBOMを通じて確認する。
- **機能テスト**
  機能の変化を把握するためにも、機能テストの結果と環境を必ず保存し、最終ステップとしてSBOMの内容の検証を行う必要がある。
- **製品のアップデート**
  アップデート時に脆弱性やリスクを取り込んでしまう危険性を避けるために、ソフトウェアに対して更新されたSBOMを確認し、サプライヤーによるセキュリティへの署名がされていることを確認する。

ソフトウェアの使用時

ソフトウェア使用時、ソフトウェアの更新、セキュリティ/サプライチェーンリスク管理業務のそれぞれのフェーズにおいて生じ得る脅威とそれに対する対策が示されている。その中でSBOMについて言及されているのは以下の通り。

- **ソフトウェアの更新**
  信頼できないソースより更新があった場合に、その発信元を確認する手段が無かったり、更新によって既存の機能の操作性が妨げられるといった脅威が考えられる。それらの対策として、専用のチャネルを利用して信頼できるソースからの更新のみを受け付けるようにすることや、更新されたSBOMの中身を確認してソフトウェアの詳細な更新内容を把握する必要がある。

調査結果サマリ：【NTIA】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 (米国商務省電気通信情報局)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の作成手順、SBOM作成に当たって考慮すべき事項、SBOMに関する補足事項がまとめられている。

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

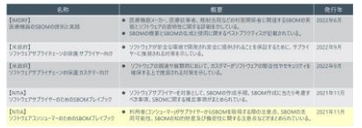
- **SBOMの知的財産/機密性**
  SBOM情報は中間サプライヤーを介して最終利用者に提供される必要がある。SBOMの配布を妨げるのではなく、契約上の機密情報としてSBOMを扱うように機密保持体制を構築することが望まれる。
- **SBOMフォーマットの検証**
  SBOMのフォーマットが有効であるか（必要な情報が存在し、構造化されているか）を確認する。活用できるツールの例は以下のとおり。
  ・SPDXOnline Tool: SPDX形式の検証ツール
  ・SWID Tools: SWID形式の検証ツール
  ・CycloneDX CLI Tool、Web Tool: CycloneDX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

出所)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

調査結果サマリ：【NTIA】ソフトウェアコンシューマーのためのSBOMプレイブック



- 2021年11月、NTIA (米国商務省電気通信情報局)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

出所)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

調査結果サマリ：SBOMの活用に関するガイドライン 調査全体像

■ 参照したガイドラインに共通するポイントは以下の通り

- ソフトウェアの作成者のみならず、ソフトウェアのユーザも含むソフトウェア流通過程に関わる主体全体に対して、それぞれの役割(責務)が明記されている
  - ◆ ソフトウェア部品を提供、あるいはそれらの部品を組み合わせて開発する事業者に対しては、SBOMを作成し、ソフトウェアユーザに提供する旨の役割が明記されている
  - ◆ ソフトウェアを利用するソフトウェアユーザには、「ソフトウェア開発者やサプライヤにSBOMを要求し、SBOMを確認(検証)してライセンス管理やセキュリティ管理に活用する」等の役割が明記されている

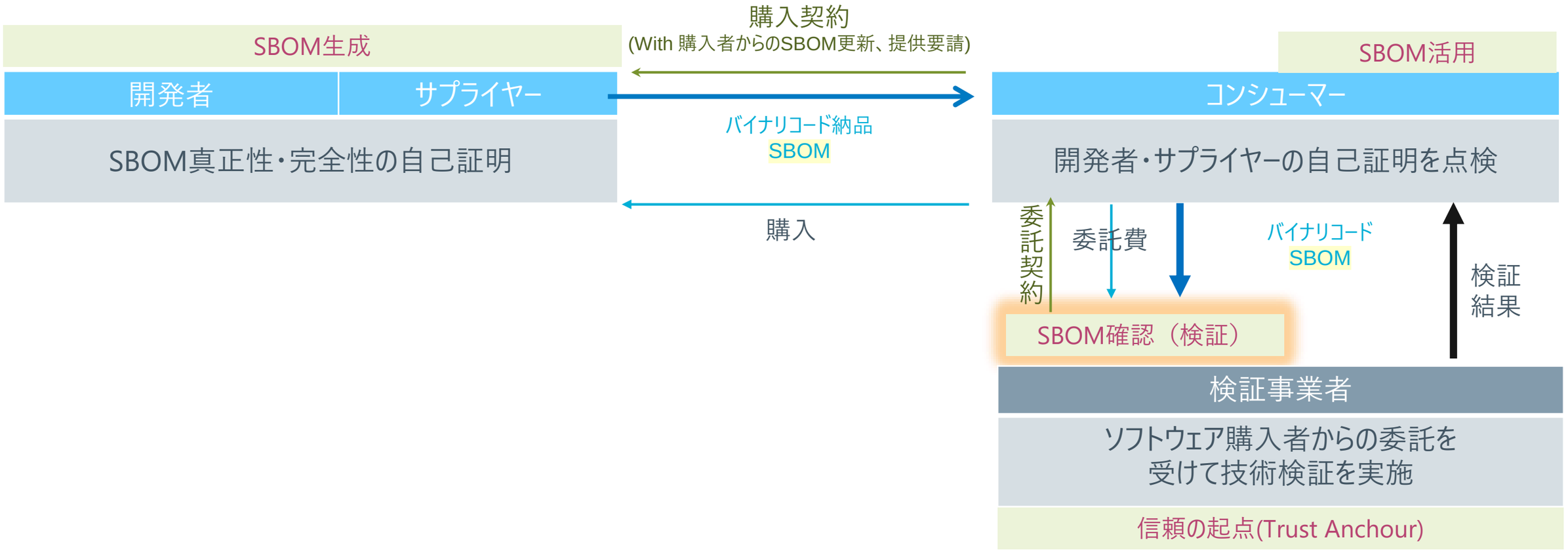
- ソフトウェア流通過程に関わる主体全体に対して役割(責務)を負わせることで、重大な脆弱性の残存やライセンス違反を予防、検知・対処するための動機づけを行うことを企図していると考えられる。

調査結果サマリ：主要なガイドライン・指針の調査 考察　SBOM確認(検証)体制のあり方

- 前述の通り、各種ガイドラインではソフトウェア購入者がSBOMを確認(検証)したうえで、活用を行う体制作りが推奨されている。
- ソフトウェア開発者およびサプライヤーが実物を反映した正確なSBOMの作成を行い、ソフトウェア購入者がSBOMの提供や更新を要請し、提供されたSBOMの活用や確認(検証)を行う体制作りは、SBOMの実効性を確保するためにも必要であると考える。

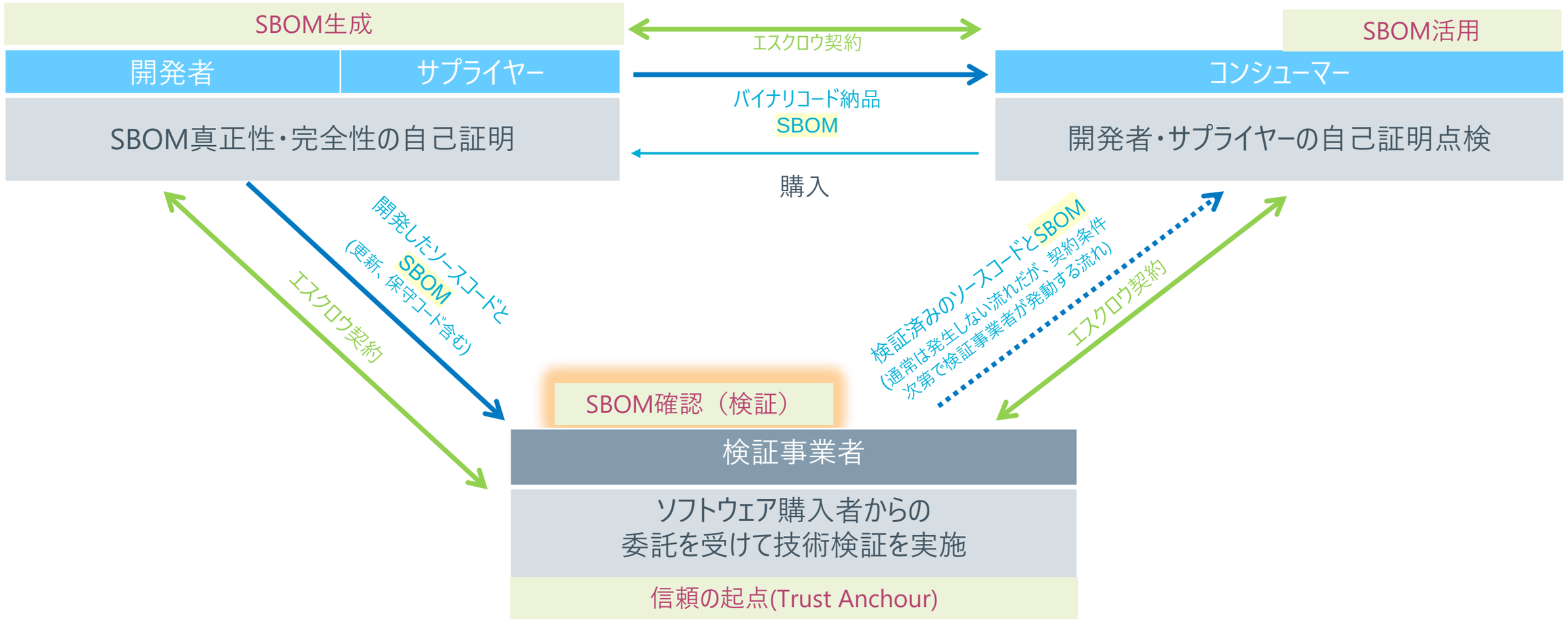
調査結果サマリ：主要なガイドライン・指針の調査 考察　SBOM確認(検証)体制のあり方

- ただし、実際にはソフトウェア購入者がSBOMの技術的な確認(検証)を行うことは少なく、技術的にも難しいことが考えられる。
- リスクを許容できるソフトウェア購入者は、サプライヤーから提供されるSBOMの真正性・完全性を信頼し、追加で技術的な確認(検証)を行うことは少ないと考えられる。
- 対象ソフトウェアのリスクが大きい場合や費用負担力がある場合は、SBOMの確認(検証)をアウトソースすることが考えられる。



調査結果サマリ：主要なガイドライン・指針の調査 考察　SBOM確認(検証)体制のあり方

- 重大なリスクが想定される機器・サービスに対し、信頼できる第三者中立的な検証事業サービスがあれば、費用負担力のあるソフトウェア購入者は、このようなサービスの利用を検討することが考えられる。
- 下記は、検証事業者がソースコードベースでSBOMの確認(検証)を行うスキームのイメージ図(エスクロウスキーム)。

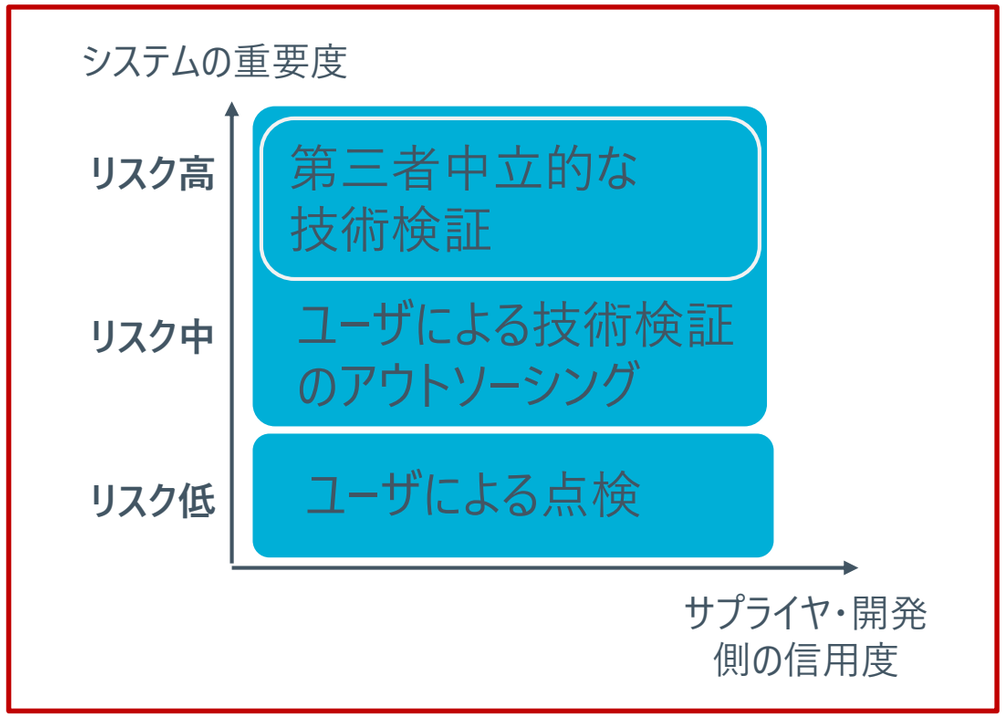


調査結果サマリ：主要なガイドライン・指針の調査 考察　SBOM確認(検証)体制のあり方

■ 前頁までのまとめは以下の通り

SBOM活用のあるべき姿の実現

信頼できるSBOM利活用のあり方　＝　セキュリティ開発体制　＋　SBOM作成ツールの信頼性向上　＋　SBOM確認・検証スキームの確立※　＋　ユーザのSBOM運用体制



本調査の範囲

本項の考察範囲

**注：左記は、説明用の概念図であり、
実態を反映したものではない**

調査結果サマリ：主要なガイドライン・指針の調査 考察　SBOM確認(検証)体制のあり方

＜補足＞

- 前述した３つのスキーム以外には、開発者・サプライヤー側が自身の検証体制を検証し、その結果をユーザ側に示すスキームもある。
- 本調査では技術検証をユーザ側で行う前提としているため、上述の通り、その存在を示すにとどめる。

(１)SBOMに係る既存技術・研究の調査
(イ)SBOM作成に関する技術の調査

調査結果サマリ：SBOM作成ツール(SCA)の概要

- SBOM作成ツール(SCAツール)は当初ライセンス管理に重点を置いていたが、OSSの利用増加に伴い、次第にソフトウェアのセキュリティ管理が主なユースケースとなる
- 近年ではソフトウェアサプライチェーンリスク管理や米国国家サイバーセキュリティ改善に関する大統領令(EO 14028)が公表されたことを受け、SCAツールが標準フォーマットに対応したSBOMの出力機能を追加する動きが見られる

SCAの変遷

初期のSCA	• 当初は、ライセンス管理やコンプライアンスの遵守に重点を置いていた • しかし、OSSの利用が急速に増加したことに伴い、主なユースケースはソフトウェアのセキュリティ管理へと次第に移行していく
近年のSCA	• ソフトウェアサプライチェーンリスク管理の観点で、OSSを含むサードパーティ製コンポーネントの可視化の必要性が注目されるようになった • 2021年5月に米国にて国家サイバーセキュリティ改善に関する大統領令(EO 14028)が公表されたことを受け、SCAツールが標準フォーマットに対応したSBOMの出力機能を追加する動きが見られる • その一方でSBOM作成そのものを目的としたツールについても、開発の動きが見られる 例としてMicrosoft社は、SBOM作成ツールをOSSで公開している

調査結果サマリ：SBOM作成ツール(SCA)の机上調査

■ 調査の狙い

- 商用目的もしくはOSSとして公開されているSBOM作成ツールの実態を把握する目的で調査を実施。SPDX、CycloneDXに対応したツールを対象とする。
- 複数フォーマット(SPDX、CycloneDX等の複数)に対応したツール、SPDX/CycloneDXのみに対応したツールを抽出した上で、以下の観点から実態把握を行う。
  - ◆ 商用ツールとOSSの割合と件数
  - ◆ 国内サポートを受けられるツールの割合と件数
  - ◆ バイナリコードを対象としたSBOM作成を行うことができるツールと、ソースコードを対象としたツール、両者を対象としたツールの割合と件数

■ 調査対象

- SPDX、CycloneDXが公式サイトにリストアップしているツールを対象とする。
- 調査対象件数

表：SBOM作成ツール調査対象件数(2022/11/24時点)※内重複2件

	商用ツール	OSSツール	合計	掲載先
SPDXツールリスト	7	13	20	https://spdx.dev/resources/tools/
CycloneDXツールリスト	25	21	46	https://cyclonedx.org/tool-center/

■ 調査対象件数の違いについての考察

- ➢ CycloneDXの掲載件数が多いのは、公式サイト掲載へのリクエスト方式の違い(SPDXは管理者へ掲載を申請する方式、CycloneDXは掲載者自らがリストの編集を行える方式であり自由度が比較的高い)と、サポーター参加企業の多さ(SPDX：39件、CycloneDX：98件)が影響していると考えられる。

調査結果サマリ：SBOM作成ツール(SCA)の机上調査

■ 本調査におけるSBOM作成ツールの定義

- NTIAのSBOM Tool Classification Taxonomyによれば、SBOMツールは厳密には9種類のタイプを持ったツールに分類できるとされている。【下表参照】
- 本調査においては、ビルド段階やソースファイルまたはバイナリファイルの分析によりSBOMを生成するツールをSBOM作成ツールとしてとらえており、NTIAの上記分類に従えば、「大区分：作成、中区分：ビルド、分析」に該当する機能を備えたツールと解釈できる。
- なお、選定したツールの中にカテゴリー：編集の機能を持つツールは除外していないため含まれている可能性がある。

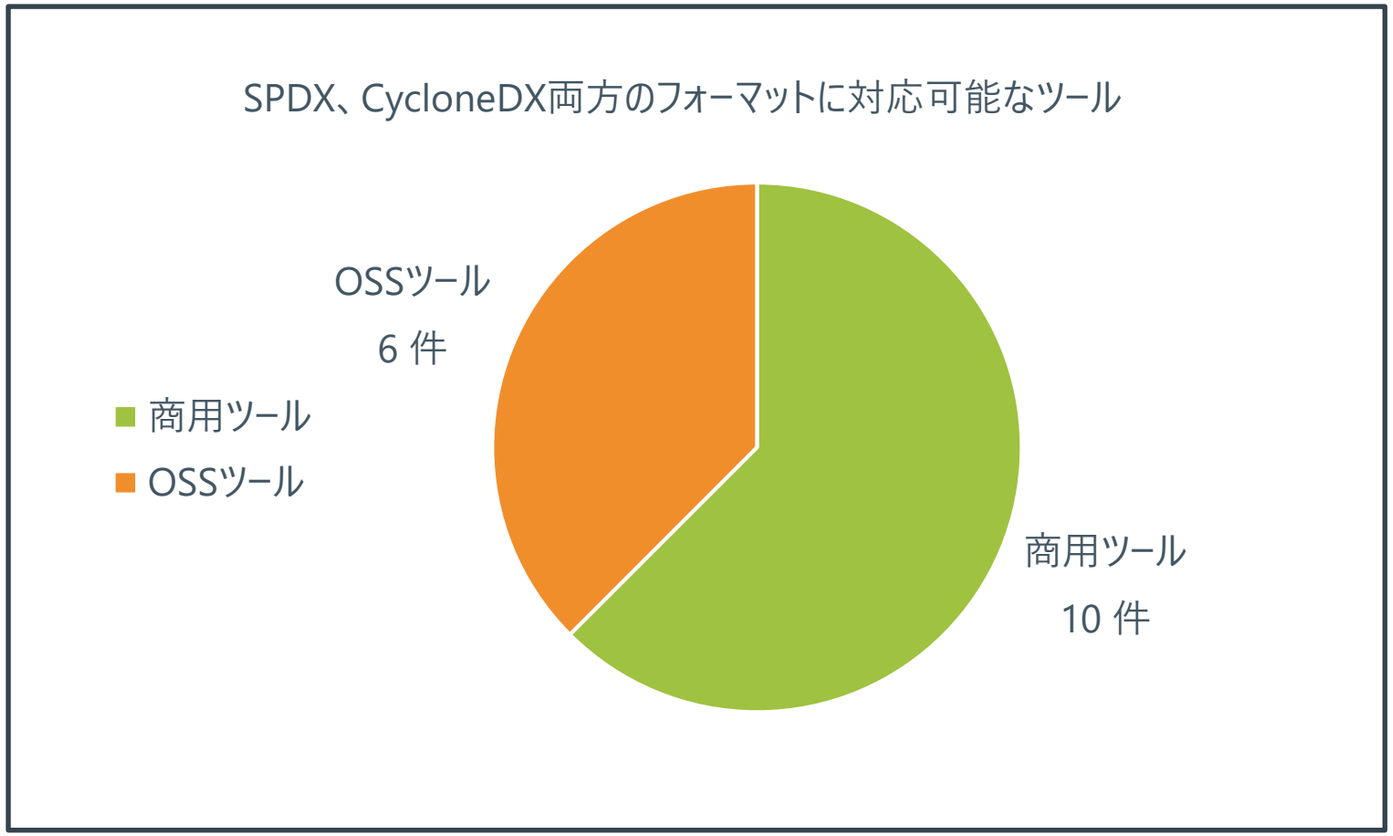
NTIA：SBOM Tool Classification Taxonomy

カテゴリー	タイプ	説明
作成	ビルド	SBOMは、ソフトウェアアーティファクトのビルドの一部として自動的に作成され、ビルドに関する情報が含まれる
	分析	ソースファイルまたはバイナリファイルの分析では、アーティファクトと関連するソースの検査によってSBOMが生成される
	編集	SBOMデータの手動入力または編集を支援するツール
活用	ビュー	内容を人間が判読できる形式(例えば、絵、図、表、テキストなど)で理解できる。意思決定・業務プロセス支援に活用
	差分	複数のSBOMを比較し、違いを明確に確認できる(例えば、ソフトウェアの2つのバージョンを比較する)
	インポート	SBOMを検出、取得し、システムにインポートして、さらに処理と分析を行うことができる
変換	形式変更	同じ情報を保持しながら、あるファイルタイプから別のファイルタイプに変更する
	マージ	SBOMとその他のデータの複数のソースを分析と監査の目的で組み合わせることができる
	ツールサポート	API、オブジェクトモデル、ライブラリ、トランスポート、その他のリファレンスソースによる他のツールでの使用のサポート

出所)https://www.ntia.gov/files/ntia/publications/ntia_sbom_tooling_taxonomy-2021mar30.pdf

調査結果サマリ：SBOM作成ツール(SCA)の机上調査 結果

- OSSツールも複数フォーマットに対応するようになっている
- 商用ツールにおいても複数フォーマットに対応することがベースラインとなり、その結果、複数フォーマットに対応したツールが増えると見込まれる



SPDXフォーマットのみに対応可能なツール

CycloneDXフォーマットのみに対応可能なツール

調査結果サマリ：SBOM作成ツール(SCA)の机上調査 結果

- 複数フォーマットが併存している状況であるため、複数フォーマットに対応したSCAツールを選定すべきである
- 複数フォーマットに対応したSCAツールの特性は以下の表に掲げる通りである(青背景の箇所を参照)
- 複数フォーマットに対応したSCAツールは国内サポート体制の整備も早く、バイナリコードにも対応できるケースが多い

調査内容	明らかとなった実態	考察
■ 複数フォーマットに対応するSBOM作成ツールの状況	● 商用ツールは全体の6割(10件)を占める ● OSSツールは全体の4割(6件)	● OSSであっても複数フォーマットに対応するようになっていることから、商用ツールにおいては複数フォーマットに対応していることが今後ベースラインとなり、対応ツールは増加傾向になることが見込まれる
■ 複数フォーマットに対応する国内サポートのある商用SBOM作成ツールの状況	● 国内サポートのあるツールは全体の5割(5件)を占める ● 国外サポートのみは全体の5割(5件)	● 複数フォーマットに対応したツールは単一フォーマットのみに対応したツールよりも幅広く需要を取り込むことができるため、国内においては複数フォーマットに対応したツールの展開が多くなると見込まれる
■ 複数フォーマットに対応するバイナリとソースコードベースのSBOM作成ツールの状況	● バイナリベースツールは全体の3割(5件)を占める ● ソースコードベースツールは全体の3割(4件) ● 両者に対応するツールは全体の4割(7件)	● 複数フォーマットに対応するツールは、ソースコードとバイナリの両方に対応しているケースが多いことが分かる ● 商用ツールとしては複数フォーマットに対応するだけでなく、ソースコードとバイナリの両方に対応することが、機能拡張の方向性として有力であると考えられる

調査結果サマリ：SBOM作成ツールベンダーへのヒアリング

- SBOM作成ツール(SCAツール)は解析の結果ツール内で独自のSBOMを作成し、そのSBOMを標準フォーマット等で出力できる機能を追加で実装している。つまり、SCAツールにとってSBOM標準フォーマットの出力はあくまでもおまけの機能である。

- プロプライエタリを含むSBOMを自動で生成するツールは存在しない(現調査の範囲において)
  - ツールベンダーはOSSのコンポーネントを検出するための照合用DBを整備しているが、プロプライエタリソフトウェアのコンポーネントを検出するための照合用DBは整備していない。(商用ソフトウェアの照合用DBを整備するケースはある)

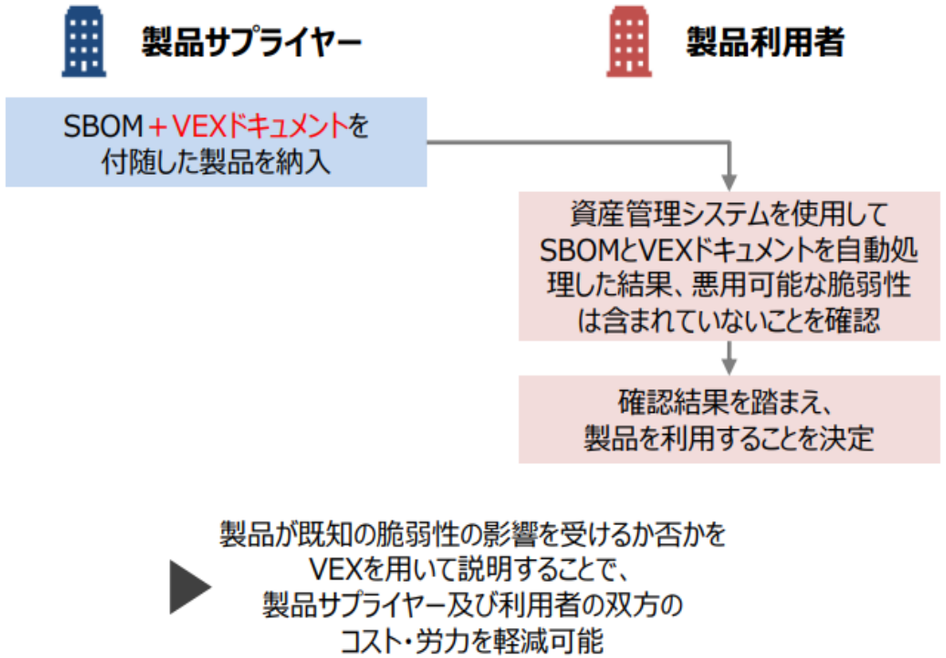
- ソースコード、バイナリコードのいずれか一方、もしくは両方の形式に対応してコンポーネントの検出を行うことが可能なツールがある
  - 開発者がOSSを利用した開発を行う場合、当該OSSのライセンスチェックやセキュリティチェックを自ら行うために、ソースコード形式に対応したコンポーネントの検出が可能なツールが必要となる。
  - バイナリコード形式のツールは、機器に実装されたソフトウェア(ファームウェア等)の解析を行う現場で多く使われてきた経緯がある。バイナリコード解析の場合、暗号化・難読化処理がされると解析を行うことが全くできない。

- SBOM作成ツール(SCAツール)は、セキュア開発(いわゆるシフトレフト)を志向する企業、規制対応のためにSBOM作成が必要な業界(例：自動車業界、医療機器業界)が需要開拓先となっている。

調査結果サマリ：主要な関連研究の調査「VEX(Vulnerability Exploitability eXchange)」

VEXドキュメントによる脆弱性ステータスの明示化

VEXドキュメント・・・機械判読可能なセキュリティ通知情報の一形態



CISAは、VEXドキュメントの最小要素として、メタデータ、製品の詳細、脆弱性の詳細、脆弱性のステータスを含めるべきとしている。

最小要素	最小要素の具体的な定義
VEXドキュメントのメタデータ	以下の情報を含めること VEX文書の識別子、VEX文書の識別子文字列、VEX文書の作成者、VEX文書のタイムスタンプ、VEX文書の作成者の役割
製品の詳細	以下のいずれかの情報を含めること 製品の識別子、製品群の識別子(一意の識別子、サプライヤー名・製品名・バージョン文字列の組み合わせ)
脆弱性の詳細	以下の情報を含めること 脆弱性の識別子(CVEまたは他の識別子) 脆弱性の説明(CVEの説明など)
脆弱性のステータス	以下のいずれかの情報を含めること NOT AFFECTED(影響を受けない)、FIXED(修正済み AFFECTED(影響を受ける)、UNDER INVESTIGATION(調査中)

出所：経済産業省,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
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/008_03_00.pdf

本調査への示唆
- **VEXの活用・普及が進むことで、技術検証における既知脆弱性の評価効率の向上に繋がる可能性が想定できる(VEX自体の信頼性が担保されることが前提)**

調査結果サマリ：主要な関連研究の調査「DBoM(Digital Bill of Materials)」

- 証明書に対して否認防止と監査可能性を保証しながら、チャネルを介してサプライチェーン上で共有を可能にするツールおよびサービスのフレームワーク
- DBoMコンソーシアムおよびテクノロジーは、サプライチェーンにおける証明書共有に対して整備されたインフラストラクチャを提供するために誕生

証明書共有における課題(SBOM活用)

・SBOM共有のための統一されたプラットフォームの欠如

組織間でSBOMがシームレスに共有され、ソフトウェアに関する情報を常に正確に示すには、SBOMの作成、配布、および利用をソフトウェアライフサイクルに統合することが重要となる。しかし、これらのタイプの情報をシームレスに共有するための確立されたプラットフォームが無い。

・ベンダーやフォーマットによるロックイン

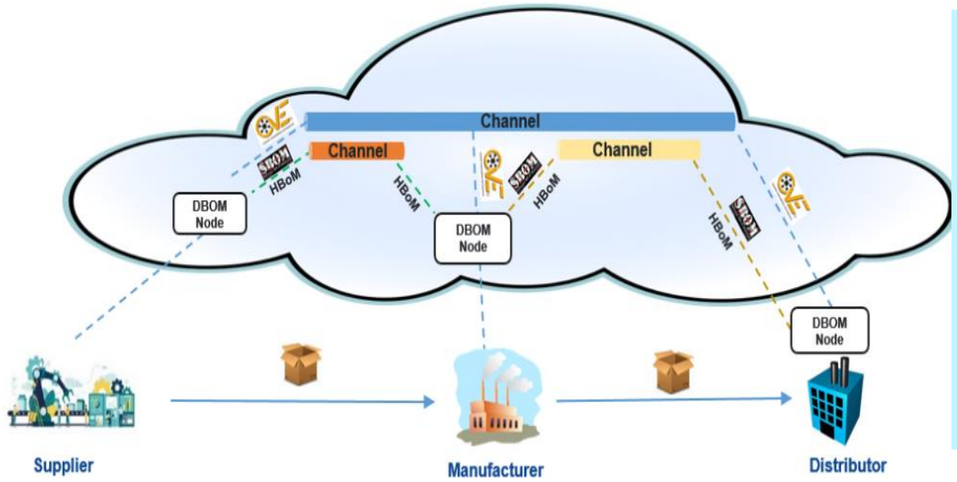
企業ごとに採用するSBOMフォーマットは異なるが、様々なSBOMフォーマット(SPDX、CycloneDX、SWIDなど) 間でシームレスに変換するための相互運用性の確保が課題。

・共有SBOMへのアクセス制御の複雑性

組織が公開したくないデータがSBOMに含まれている場合があるため、セキュリティの観点から、プラットフォームには共有するSBOMへのアクセス権を細かく制御するためのプリミティブを組み込むことが必要となる。

DBoMでの証明書共有

- DBoMでは、リポジトリ(データベース、プライベートおよび許可された分散型台帳、パブリックブロックチェーンから構成される)を用いて証明書(SBOMやHBOMなど)を共有し、各企業やパートナーはリポジトリに接続されたDBoM Nodeを介してリポジトリの情報の取得/記録を行う。
- リポジトリ内にはパブリックおよびブロードキャストのチャネルを開設することができ、パートナー間での情報のやり取りはチャネルを通じて行われる。
- DBoM SDKを使用することでDBoMを既存のコードに統合したり、異なる構成証明形式間での交換が可能になる。



DBoM Node

リポジトリへのゲートウェイとして機能し、1つ以上のチャネルをリポジトリ内に開設することができる。
チャネルでは、作成者によって設定されたポリシーに準拠し、関係者間のみで証明書が共有されるため、否認防止や監査可能性を担保することが可能。

本調査への示唆

- サプライチェーンにおける安全かつ利便性の高いSBOM共有には課題が多く、解決のためのプラットフォームが求められている
- SBOM自体の信頼性、否認防止を担保するためには、このような技術を活用することが求められる

出所:DBOM Project, Usecase, https://dbom-project.readthedocs.io/en/latest/use-cases.html

(１)SBOMに係る既存技術・研究の調査
(ウ)SBOMの運用方法に関する調査

SBOM運用事業者へのヒアリング　考察：SBOMの作成・利用の現状

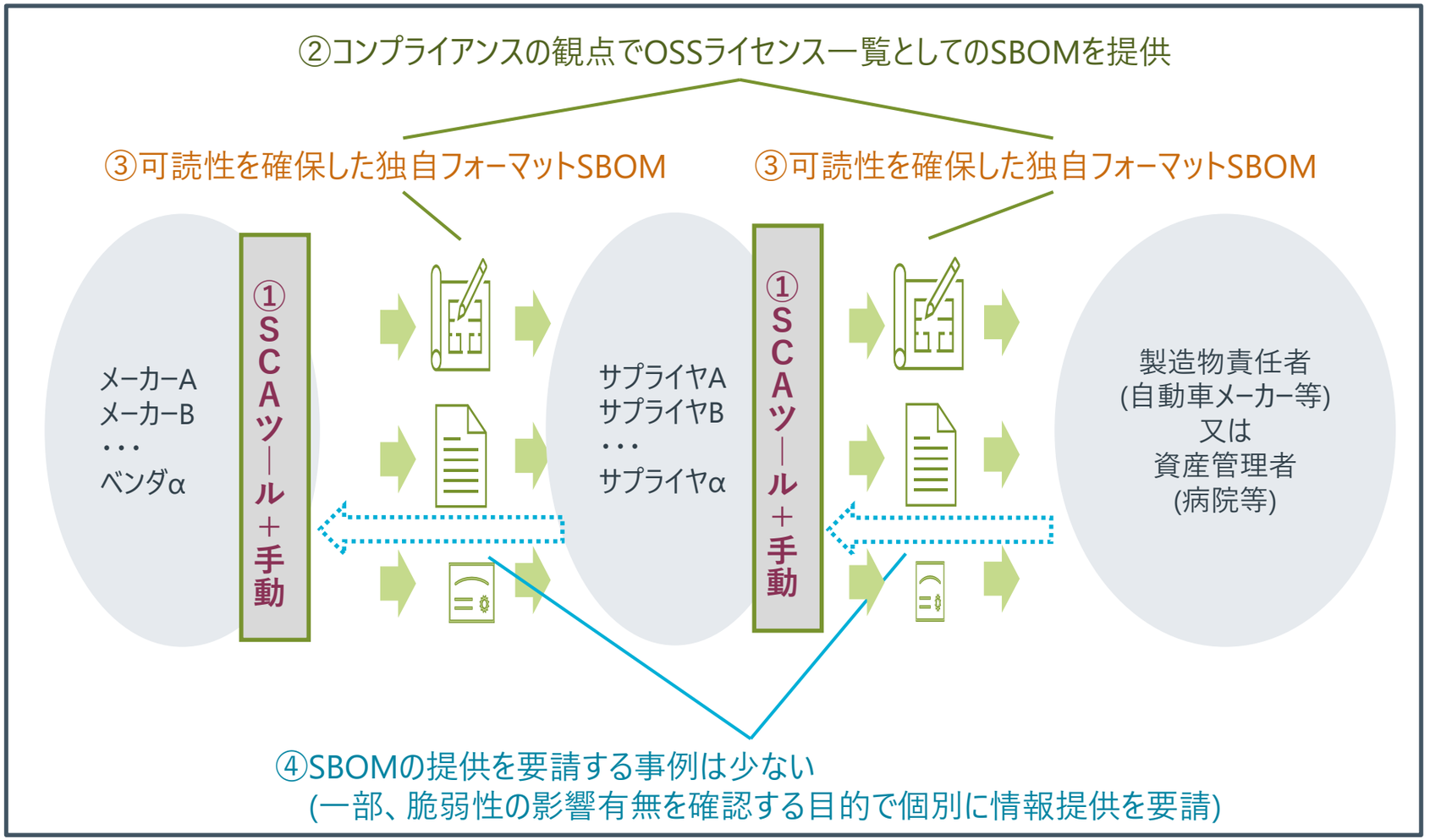
■ SBOMの費用対効果については総じて肯定的評価が多い

- ソフトウェアがどのようなコンポーネントから構成されているかどうかを把握することは、ライセンス管理やセキュリティ管理の基本と認識されている。
- ソフトウェアの正確な構成管理は必須であり、製品開発において本来必要となるコストである。そのため、コストメリットだけを念頭に検討すべきではなく、必須の取組であることを前提に、SBOMの導入について検討すべきとの意見がみられた。

- その一方、同じソフトウェア製品であっても表記にブレが生じており、名寄せに大きな手間がかかっていることが課題として挙げられた。その理由として、ソフトウェア製品名の記述ルール、管理識別子が整備されていないことが指摘されている。
- この問題を改善するためには、CPEをはじめとしたソフトウェア製品を一意に識別するための識別子の整備が重要との意見が複数社より挙げられている。

OSSのライセンス管理を主目的として、「自社独自フォーマット」でのSBOM利活用が行われている

- 機器・システムの開発元事業者は、設計情報等を元に、各々独自のフォーマットでSBOMを作成し、ライセンス管理や脆弱性管理を行っている
- 取引先に対してSBOMの提供を要請する事例(または提供を求められている事例)は少ない



① コンプライアンス違反を防ぐため、意図せず混入したOSSを検出する目的でSCAツールが用いられている

② コンプライアンスの観点でOSSライセンス一覧としてのSBOMが提供されている

③ 製品を製造する場合、使用しているOSSのライセンス一覧を人が可読できる形式で提示する必要があるため、機械可読でないフォーマットが用いられている

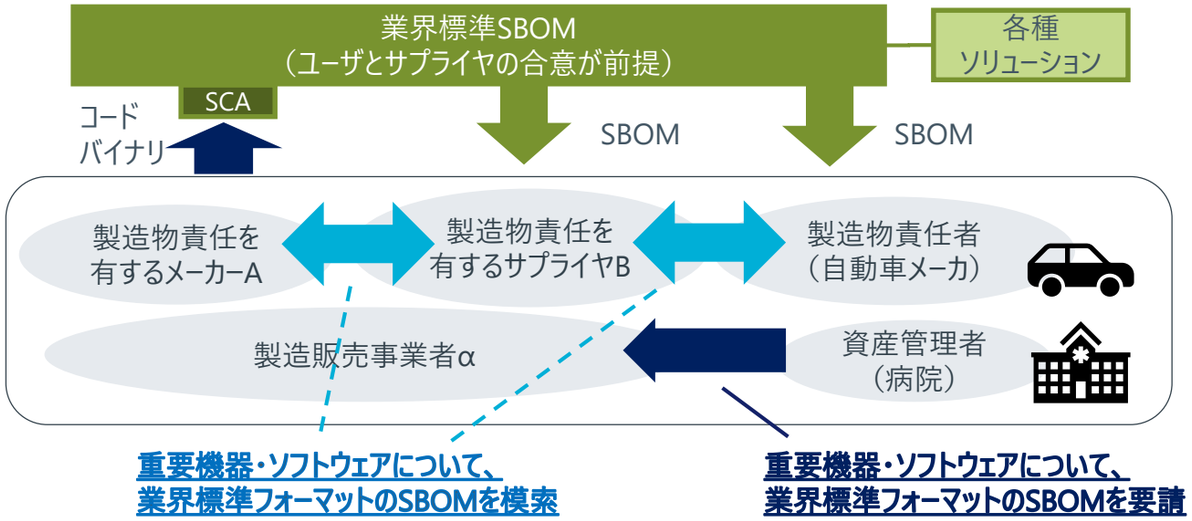
④ サプライヤ/ユーザ間でのSBOMの共有はOSSライセンス管理を目的としたものが現状ほとんどであり、脆弱性管理目的で共有されている事例は少ない

自動車・医療機器業界において、「業界標準フォーマット」のSBOM作成、利用を模索する動きが見られる

- セキュリティ侵害が人体に影響を及ぼす恐れがある業界から先行して、業界で仕様を標準化したSBOMの作成、利用を模索・検討する動きが見られる
- 医療機器業界では資産管理責任を有するユーザ側(病院等)の要請に従い、サプライヤが業界標準されたSBOMを提供する体制作りが検討されている
- SBOMにはOSSのみならず、COTS、OTS、プロプライエタリソフトウェアも含めることが想定されている
- 標準フォーマットのSBOMを活用することで、脆弱性管理の実効性向上が期待されている
  - 例１：脆弱性情報が公開された際、サプライヤがSBOMを利用してユーザへの影響評価を行い、素早く対処方針を立案する
  - 例２：インシデント発生時、サプライヤがSBOMよりソフトウェアの脆弱性等に起因するインシデントであるか分析を行い、対処方針を立案する
- 自動車業界においても、製造物責任を有するメーカー/サプライヤ間で、業界標準フォーマットのSBOMを作成、提供する仕組み作りが模索されている

「業界標準フォーマット」のSBOM(業界標準SBOM)

- SBOMを構成する以下の要素に関する業界の合意内容を文書化したものを想定
  - ❑ Data Fields
  - ❑ Automation Support
  - ❑ Practices and Processes
- **具体的には、業界のガイドライン、NTIAが提示するSBOM最小要素や標準規格(SPDX, CyclonDX)、業界固有のユースケース等を踏まえて定められたものを想定する**



**重要機器・ソフトウェアのOSSやサードパーティ製ソフトウェアコンポーネントの脆弱性やEOL等を検出する。
また、新たな脆弱性の公開時やインシデント発生時に迅速に対処する。これらにより人体に係るリスク発生を未然に防止する。**

業界標準フォーマットのSBOMの実現のためには、制度面・供給面・需要面の各方面から見た諸条件が整う必要がある

■ 医療機器業界・自動車業界が先行すると想定されるが、複数の条件を満たす必要があることを考慮すると、実現までには一定の期間を要すると見込まれる。

①コンポーネントの名称統一

②標準ルールの確立（SBOM仕様の業界標準）

【制度面】

③ユースケースに応じたモデル契約

業界標準フォーマットのSBOM活用の容易性向上

【需要面】（開発側）

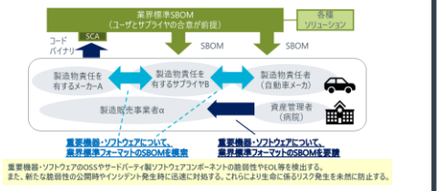
①OSSリスク管理体制構築

②セキュア開発体制構築

SBOM作成ニーズ

■ 個社独自フォーマットのSBOM

■ 業界標準フォーマットのSBOM
(医療機器、自動車等)



SBOM活用ニーズ

【需要面】（運用側）

①脆弱性監視体制構築

②インシデント監視体制構築

技術開発の進展によるSBOM活用の費用対効果の向上

①コンポーネントの検出

【供給面】

②運用環境でのモニタリング

③ツール開発への助成【制度面も含む】

SBOMの効果的な利活用には、ソフトウェア名称(識別子等を含む)が標準化・統一化されることが必要

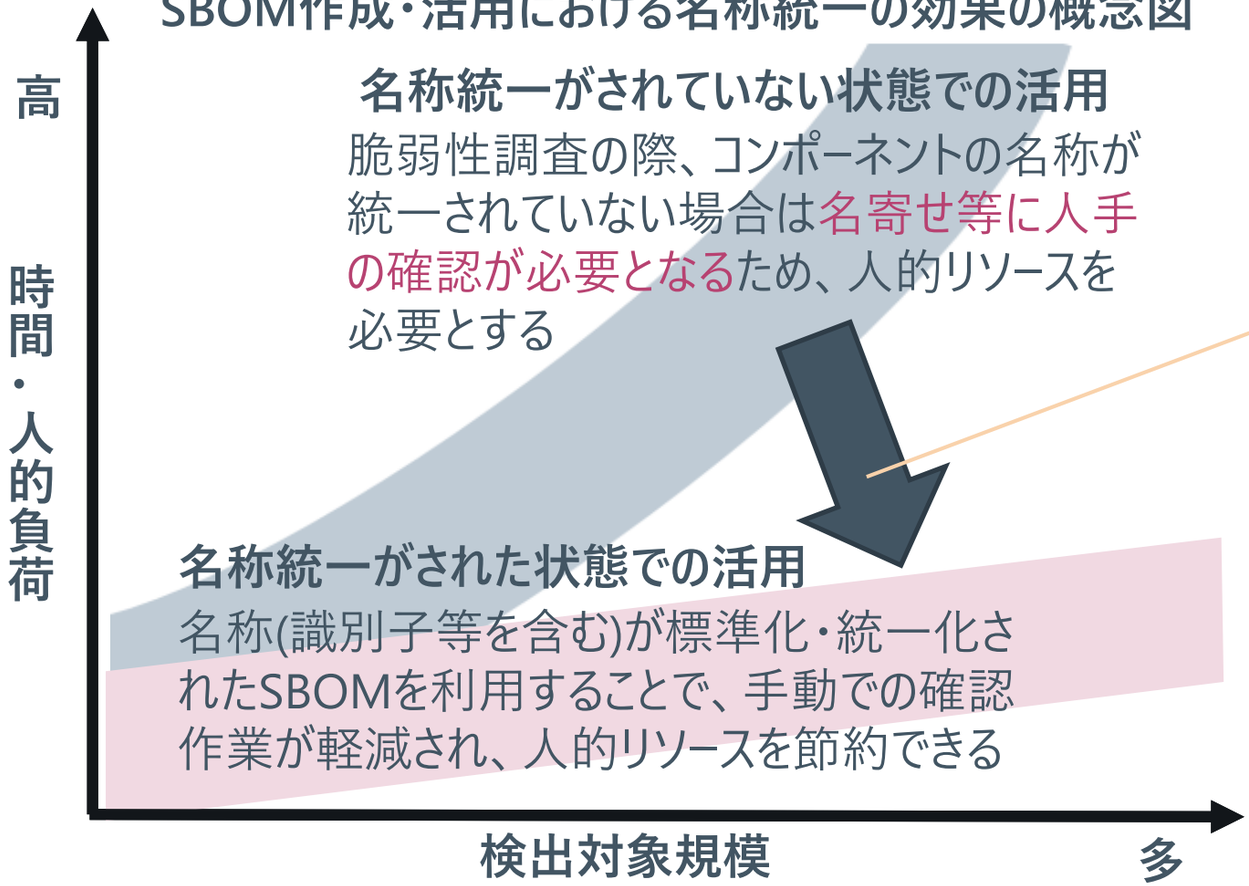
①コンポーネントの名称統一

【制度面】

②標準ルールの確立
（SBOM仕様の業界標準）

③ユースケースに応じたモデル契約

SBOM作成・活用における名称統一の効果の概念図



■ コンポーネントの名称統一による識別精度の向上

対象	従来の活用	望ましい姿
製品識別名称、CPE (製品名、ベンダ名、バージョン等)	CPEが定義されている製品が限定されており、汎用的に利用できる製品識別体系がない	OSSのみならず、COTS、OTSを識別するための標準的な製品名称が定義されること
コンポーネント識別子 (ハッシュ値等)	同じソフトウェアであってもSBOM作成ツールの使用条件の違いから、コンポーネントハッシュ値が異なる可能性がある	同じソフトウェア・コンポーネントであれば、一意なハッシュ値を特定できるように使用条件を定めること
サプライヤID	汎用的に利用できるサプライヤIDがない	サプライヤを識別するためのサプライヤIDが定義されること

現在、SBOM実装のための業界標準は未確立もしくは十分ではない

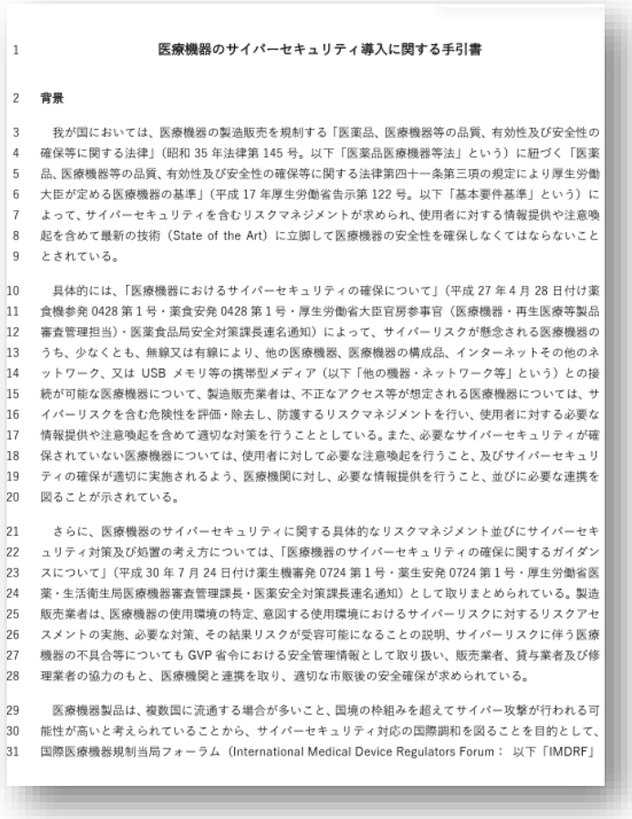
①コンポーネントの名称統一

②標準ルールの確立（SBOM仕様の業界標準）

【制度面】

③ユースケースに応じたモデル契約

■ 厚生労働省「医療機器のサイバーセキュリティ導入に関する手引書」



医療機器のサイバーセキュリティ導入に関する手引書

背景

我が国においては、医療機器の製造販売を規制する「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」（昭和 35 年法律第 145 号。以下「医薬品医療機器等法」という）に紐づく「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。以下「基本要件基準」という）によって、サイバーセキュリティを含むリスクマネジメントが求められ、使用者に対する情報提供や注意喚起を含めて最新の技術（State of the Art）に立脚して医療機器の安全性を確保しなくてはならないこととされている。

具体的には、「医療機器におけるサイバーセキュリティの確保について」（平成 27 年 4 月 28 日付け薬食機参発 0428 第 1 号・薬食安発 0428 第 1 号・厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当）・医薬食品局安全対策課長連名通知）によって、サイバーリスクが懸念される医療機器のうち、少なくとも、無線又は有線により、他の医療機器、医療機器の構成品、インターネットその他のネットワーク、又は USB メモリ等の携帯型メディア（以下「他の機器・ネットワーク等」という）との接続が可能な医療機器について、製造販売業者は、不正なアクセス等が想定される医療機器については、サイバーリスクを含む危険性を評価・除去し、防護するリスクマネジメントを行い、使用者に対する必要な情報提供や注意喚起を含めて適切な対策を行うこととしている。また、必要なサイバーセキュリティが確保されていない医療機器については、使用者に対して必要な注意喚起を行うこと、及びサイバーセキュリティの確保が適切に実施されるよう、医療機関に対し、必要な情報提供を行うこと、並びに必要な連携を図ることが示されている。

さらに、医療機器のサイバーセキュリティに関する具体的なリスクマネジメント並びにサイバーセキュリティ対策及び処置の考え方については、「医療機器のサイバーセキュリティの確保に関するガイダンスについて」（平成 30 年 7 月 24 日付け薬生機審発 0724 第 1 号・薬生安発 0724 第 1 号・厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知）として取りまとめられている。製造販売業者は、医療機器の使用環境の特定、意図する使用環境におけるサイバーリスクに対するリスクアセスメントの実施、必要な対策、その結果リスクが受容可能になることの説明、サイバーリスクに伴う医療機器の不具合等についても GVP 省令における安全管理情報として取り扱い、販売業者、貸与業者及び修理業者の協力のもと、医療機関と連携を取り、適切な市販後の安全確保が求められている。

医療機器製品は、複数国に流通する場合が多いこと、国境の枠組みを超えてサイバー攻撃が行われる可能性が高いと考えられていることから、サイバーセキュリティ対応の国際調和を図ることを目的として、国際医療機器規制当局フォーラム（International Medical Device Regulators Forum： 以下「IMDRF」

- 製造販売業者は、医療機関の製品導入の検討の際に、SBOM(サードパーティ製アプリケーションおよびソフトウェアコンポーネントを含むソフトウェア部品表」)及びMDS２(製造販売業者による医療機器セキュリテイ開示書)の開示を求められる場合がある。
  （注）MDS2は、医療機器の意図する使用及び使用環境に対して設計したセキュリティ機能を俯瞰可能な、製造販売業者による医療機器セキュリティ開示書

	販売開始(商用リリース)	製品寿命終了 EOL	サポート終了 EOS
セキュリティを含む文書	• セキュリティポリシー • 取扱説明書、セキュリティ文書 • MDS2、SBOM	• その他の更新情報	• 保守計画を除く その他の更新情報
その他	• EOL 及び EOS 計画（日程） • アップグレード計画 • 保守計画(限定的サポート段階含む)	• EOL の通知 • EOS 計画 • その他の更新情報	• EOS の通知 • 保守計画を除く その他の更新情報

出所）厚生労働省　医療機器のサイバーセキュリティ導入に関する手引書
https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000245820

機器・システムの開発元事業者と購入者との間で、SBOMに関する合意を円滑に行うための雛形契約が求められる

①コンポーネントの名称統一

②標準ルールの確立
（SBOM仕様の業界標準）

【制度面】

③ユースケースに応じたモデル契約

■ 米国医療業界におけるモデル契約例(SBOMに言及した条文のみを抜粋し、以下に掲げる)


Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTH INDUSTRY CYBERSECURITY -

Model Contract-language for Medtech Cybersecurity

March 2022

条項44: 脆弱性管理

- ■ サプライヤーは、必要とされるデータ要素をすべて含むソフトウェア部品表(SBOM)を提供するものとする。
- ■ 医療機器のサポート期間中、サプライヤーはこれらのソフトウェアコンポーネントのセキュリティの脆弱性を監視し、リスクベースのアプローチを使用して深刻で悪用可能な脆弱性を軽減するものとする。
- ■ SBOMには、FDAまたはその他の業界のガイダンス、標準、または規制によって定義されている最小限の要素を含める必要がある。
- ■ ソフトウェアコンポーネントがアクティブに保守されなくなった場合、サプライヤーは顧客に通知し、ソフトウェアコンポーネントをアクティブに保守された同等のものに置き換えるか、ソフトウェアコンポーネントの内部でアクティブな保守を行うものとする。
- ■ ソフトウェアコンポーネントのメンテナーが新しいメンテナーに変更された場合、サプライヤーは、新しいバージョンを実際に使用する前に顧客に通知し、ソフトウェアコンポーネントのその後のリリースのサイバーセキュリティテストを実施するものとする。

※医療・公衆衛生セクター調整協議会(HSCC)：国家インフラ保護計画の下で組織された民間の重要な医療インフラ事業者の連合体
公衆にサービスと資産を提供する同セクターが直面する戦略的脅威と脆弱性の特定と緩和において政府と協力し、助言することを目的としている。
HSCCサイバーセキュリティ・ワーキング・グループ(CWG)は、HSCCの常設ワーキンググループで、300以上の業界団体で構成され、医療分野におけるサイバーセキュリティの新たな課題や進行中の課題に対処するための戦略を共同で策定している。

開発元事業者、購入事業者のニーズ(具備すべき要件)を全て満たすツールは存在しない

①コンポーネントの検出　【供給面】　②運用環境でのモニタリング

③ツール開発への助成【制度面も含む】

■ コンポーネント検出ツールとして、国内環境に適したSBOM作成ツールが具備すべき要件と課題

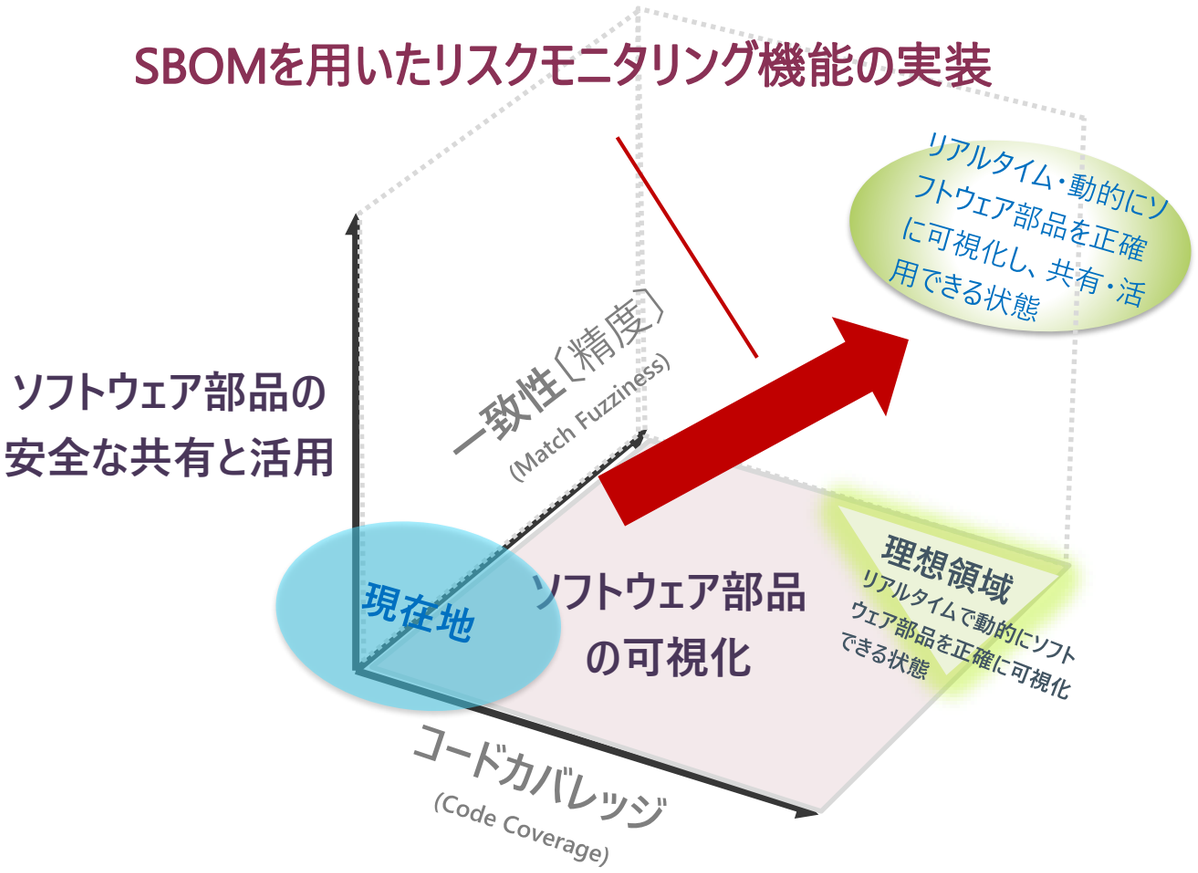
観点	具備すべき要件	現行ツールの対応状況	要件充足にむけた共通課題	
			新たな技術開発が必要な課題	制度面で対処すべき課題
1. 標準フォーマットへの対応	● 複数フォーマットに対応 (国内企業に普及しているSPDX-Liteを含む)	• 主要なSCAツールは対応済み	—	—
2. ソフトウェア種別	● OSS以外のソフトウェア(COTS、OTS等の市販ソフトウェア)にも対応	• 基本的にOSS以外は検出対象としていない • COTS、OTS等の一部を検出できるツールも存在する • プロプライエタリについては手動で登録できるツールもある	• COTS、OTSの検出が可能なツールの開発 • プロプライエタリについては設計情報等の連携ツールの開発	—
3. コード形式	● ソースコード、バイナリ形式の双方に対応	• ソースコード、バイナリ形式の双方に対応できるツールがある	—	—
4. 検出精度・カバレッジ・スピード	● パッケージマネジャーで定義されたコンポーネントに加えて、シグネチャファイルや再利用されたコードスニペットを高精度で検出	• パッケージマネジャーで定義されたコンポーネントの検出を行うツールは多く、精度も高く、スピードも速い • パッケージマネジャーで定義されていないシグネチャファイルや再利用されたコードスニペットを検出できるツールは限定されるだけでなく、検出精度は低くなる傾向がある	• パッケージマネジャーで定義されていないシグネチャファイルや再利用されたコードスニペットを高精度で検出できるツールの開発	—
5. 製品名(識別子)	● 異なるツールでも相互運用可能な製品名(識別子)の採用	• ツールによって採用されている製品名(識別子)の体系は異なる	—	• 異なるツールでも相互運用可能な製品名(識別子)の整備
6. 可読性	● 検出結果を人間が確認し活用するための可読性の確保	• 個社の思想に基づいたユーザフレンドリーな管理インターフェースが提供されている	—	—
7. 照合DBの準拠法	● 照合DBは国内法下にて管理	• 国内リージョンのクラウド上に管理基盤を置いているツールがある	—	—
8. 導入／運用時のサポート	● 国内企業向けの導入支援、技術的な問い合わせに対するサービスレベルが明らかであること	• ツールベンダによってサポートのサービスレベルは異なる	—	—
9. 他社作成SBOMの取り込み	● SBOMのインポートと品質のチェック	• 一部の商用ツールで実装済み	—	—

SBOMを用いた、システム運用におけるリスクモニタリング機能が求められている

①コンポーネントの検出　【供給面】　②運用環境でのモニタリング

③ツール開発への助成【制度面も含む】

SBOMを用いたリスクモニタリング機能の実装



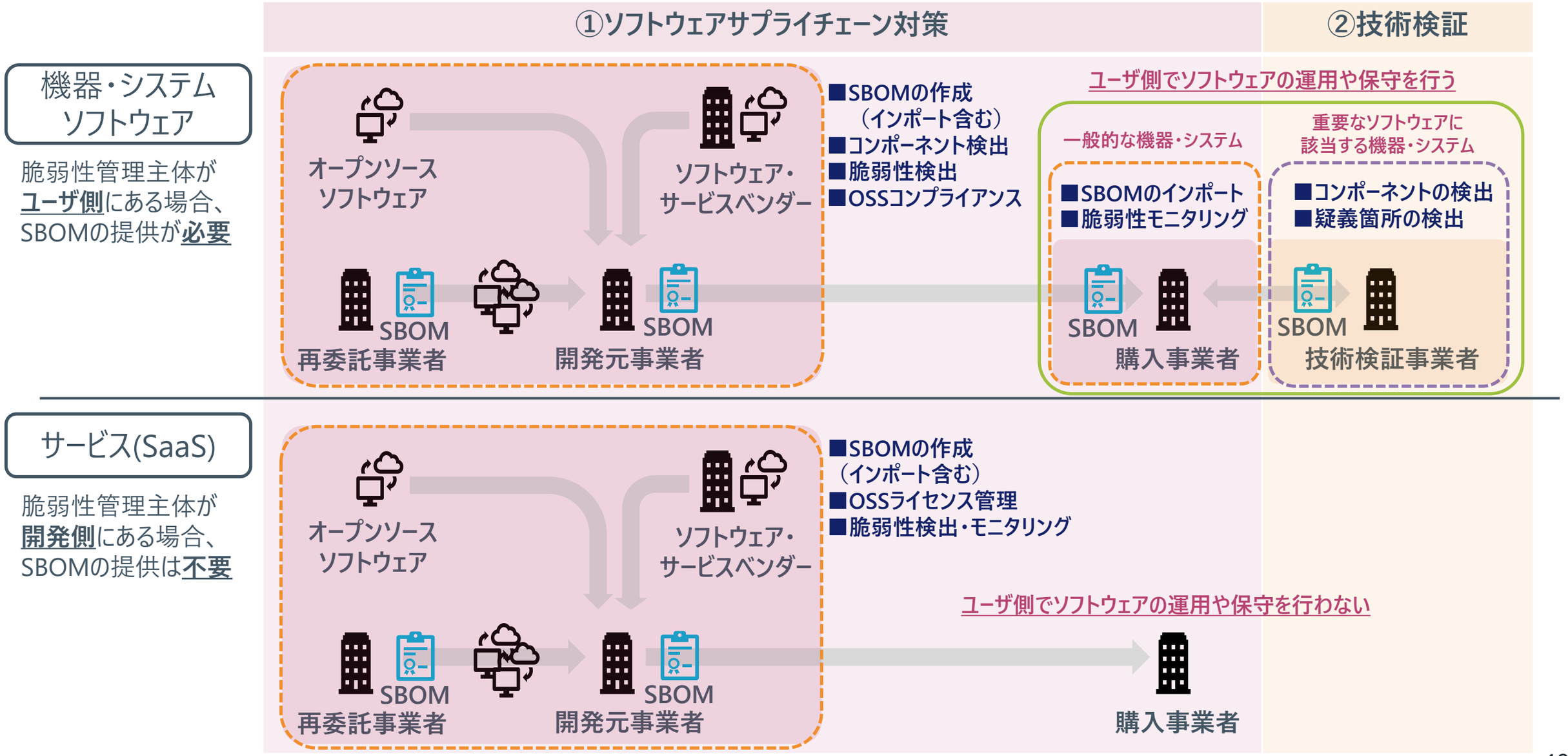
■ SBOMを用いたリスクモニタリング機能の実装

	従来の姿	望ましい姿
脆弱性の該否判定	コンポーネント検出のリードタイムに多くの人的負荷	コンポーネント検出の自動化によるリードタイムの大幅短縮
コンポーネントの呼び出し回数の取得分析	把握困難	脆弱性発生時の影響範囲の推定
OSSコンプライアンス確認	スニペットレベルでのライセンス違反等を見逃す可能性	スニペット単位でのライセンス違反等を検出
EOL/EOS判定	EOL/EOSの把握に遅れが発生する恐れ	EOL/EOSのタイミングを適切に把握

(2)国内環境に適した SBOMツールの実現性の検討

(2)国内環境に適したSBOMツールの実現性の検討

SBOMツールを①ソフトウェアサプライチェーン対策用途と②技術検証用途に分けた上で、国内環境に適したツールの要件を整理する



(2)国内環境に適したSBOMツールの実現性の検討

「①ソフトウェアサプライチェーン対策用途」：SBOM活用によるソフトウェアサプライチェーンリスク対処能力の向上

1） SBOM活用のフレームワーク

●関係主体の責務および管理対象毎にみた役割

		開発元事業者	購入事業者
		製品(機器・システム)に含まれるソフトウェアの瑕疵対応とライセンス順守の責任を有する	製品(機器・システム)に含まれるソフトウェアの瑕疵による影響を把握し対処方針の判断を行う責務を担う
管理対象	製品	• ライセンス違反や重大な脆弱性の無い製品開発・製造を行う	• 製品利用環境において脆弱性モニタリングと対処判断を行う
	サービス(SaaS)	• 上記に加え、運用環境において脆弱性モニタリングと対処判断を行う	• ― (対応無し)
	SBOM	• 購入事業者の要請を踏まえて、上記を証明するエビデンスの一つとしてSBOMを作成・提供する	• SBOMの作成と提供を開発元事業者へ要請し、取得したSBOMを脆弱性モニタリングと対処判断に活用する

●対象とするソフトウェアの範囲

- **サードパーティソフトウェア、OSSを利用するあらゆる機器・システム、ソフトウェアを対象とする**
  - プロプライエタリソフトウェアのコンポーネントとして、利用されているケースを含む

●対象とする業種の範囲

- **あらゆる業種を想定する**
  - 医療機器、自動車、IT等、SBOMを先行して活用している業種をはじめとして、全業種でのSBOM活用が進むことを想定する

2） 実現に向けた課題

- SBOMの普及率が低いため、認知度を高めるための啓発活動が必要である
- 制度面・供給面・需要面で多くの課題があるため、関係主体が時間をかけて連携して取り組む必要がある

「②技術検証用途」：技術検証へのSBOMの活用

1）SBOM活用のフレームワーク

●関係主体の責務および管理対象毎にみた役割

		技術検証業者
		購入事業者からの委託を受け、調達する製品に不正機能が含まれていないかどうかを検証する
管理対象	製品	• 調達予定の製品に含まれるバイナリコードを解析し、不正機能が製品に含まれているかどうかを検証する
	サービス(SaaS)	• ― (対応無し)
	SBOM	• 開発事業者から入手したSBOMの品質をチェックして、不正機能が疑われるかコンポーネントがあるかどうかを確認する

●対象とするソフトウェアの範囲

- **政府の業務上、重要と定義された機器・システムに含まれるソフトウェア**
  - プロプライエタリソフトウェアのコンポーネントとして、利用されているケースを含む

●対象とする業種の範囲

- **あらゆる業種を想定する**
  - 医療機器、自動車、IT等、SBOMを先行して活用している業種をはじめとして、全業種でのSBOM活用が進むことを想定する

2）実現に向けた課題

- 技術投資を促す制度的な支援の検討が必要である

(3)SBOMに係る課題の整理

(3)SBOMに係る課題の整理

SBOMの活用に向けた条件と課題

- 業界標準フォーマットのSBOM実現のためには、制度面・供給面・需要面の各方面から見た諸条件が整う必要がある
- また、SBOMを活用した技術検証ソリューションは現在妥当なものが存在しないため、新たな技術開発が必要である

①コンポーネントの名称統一

②標準ルールの確立（SBOM仕様の業界標準）

【制度面】

③ユースケースに応じたモデル契約

業界標準フォーマットのSBOM活用の容易性向上

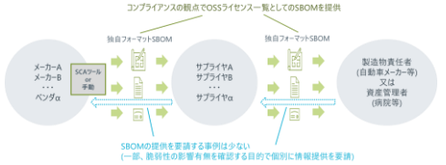
【需要面】（開発側）

①OSSリスク管理体制構築

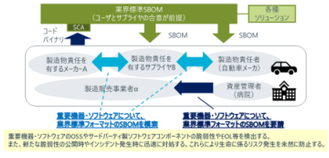
②セキュア開発体制構築

SBOM作成ニーズ

■ 個社独自フォーマットのSBOM



■ 業界標準フォーマットのSBOM(医療機器、自動車等)



■ SBOMを活用した技術検証

SBOM活用ニーズ

【需要面】（運用側）

①脆弱性監視体制構築

②インシデント監視体制構築

技術開発の進展によるSBOM活用の費用対効果の向上

①コンポーネントの検出

【供給面】

②運用環境でのモニタリング

③ツール開発への助成【制度面も含む】

今後の展望：制度面から見た考察

ソフトウェアのセキュリティリスクを未然に防止する「責任」を、法令等で明確化する動きが見受けられる

■ **ドイツ：ITセキュリティ法2.0 (2021年6月施行)**

- 重要インフラ事業者はインフラの構成要素である重要部品について、製造者による信頼性保証書を政府機関へ提出を義務化
- また、一般消費者のために、製品のセキュリティ機能の情報を表示するITセキュリティラベルを導入

■ **米国：国家サイバーセキュリティ戦略 (2023年3月公布)**

- 政権は、議会および民間部門と協力して、ソフトウェア製品およびサービスに対する責任(Liability)を確立する法律を策定する予定
- また、ソフトウェア製品とサービスを安全に開発・維持する企業を、責任(Liability)から隔離する適応可能なセーフハーバーの枠組みの開発を推進する予定

■ **EU：欧州サイバーレジリエンス法 (2025年後半適用予定)**

- 例外を除いた、デジタル要素を備えた全ての製品に対して、SBOMの作成や更新プログラム提供等セキュリティ要件への適合(自己適合宣言/第三者認証)が求められる

■ **日本：経済安全保障推進法 (2024年 事前審査開始予定)**

- 基幹インフラ事業者は設備の導入前に、設備や管理体制、管理システムの概要や仕入先、部品の詳細等を政府へ報告し、サイバー攻撃に対するリスクの審査を受ける必要が生じる

■ **考察：**
ソフトウェア開発のセキュリティリスクの責任が法令等で明確になり、セーフハーバー相当の基準としてSBOMの作成が適用される結果、開発元事業者はセキュアな開発を行ったことのエビデンスとしてSBOMを作成し、必要に応じて購入事業者へ提供する動きが強まっていくと考えられる

関係主体の責務と管理対象毎にみた役割

		開発元事業者	購入事業者
		製品(機器・システム)に含まれるソフトウェアの瑕疵対応とライセンス順守の責任を有する **セーフハーバーの適用** 一定の条件などの基準を満たした場合には、違反や罰金の対象にならない基準	製品(機器・システム)に含まれるソフトウェアの瑕疵による影響を把握し対処方針の判断を行う責務を担う
管理対象	製品	• ライセンス違反や重大な脆弱性の無い製品開発・製造を行う	• 製品利用環境において脆弱性モニタリングと対処判断を行う
管理対象	サービス(SaaS)	• 上記に加え、運用環境において脆弱性モニタリングと対処判断を行う	• ― (対応無し)
管理対象	SBOM	• 購入事業者の要請を踏まえて、上記を証明するエビデンスの一つとしてSBOMを作成・提供する	• SBOMの作成と提供を開発元事業者へ要請し、取得したSBOMを脆弱性モニタリングと対処判断に活用する

今後の展望：需要面から見た考察

- **Society5.0に向けた社会の変化や科学技術の進展の結果、IoTやファームウェアの利用が拡がる一方、リスクもそれに合わせて大きくなることが見込まれる**
- **考察**
  - IoTやファームウェアはサイバーフィジカル空間において、現実世界と結びついている。そのため攻撃脅威が顕在化した場合は、社会経済へのインパクトは大きくなる可能性がるため、法令上の責任を伴うケースが多い。
  - 医療機器業界や自動車業界がSBOMについて先進的な動きを見せているのは、こうした背景があるためと考えられる。
  - 今後、重要インフラ分野では、医療機器業界、自動車業界に倣った動きが活発化する結果、開発元事業者が安全な開発を行ったことのエビデンスとしてSBOMを作成し、購入事業者に提供する動きが強まっていくと考えられる。