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10月31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海外の動向

２．SBOM実証に関する中間報告

３．SBOM取引モデル概要

４．SBOM事業の成果物を活用した取組みの方向性

【米国・日本等】セキュアバイデザイン・セキュアバイデフォルトの実践に向けた推奨事項の発表

- 2023年10月、CISA及び米国内外の17のパートナー機関*1は、セキュアバイデザイン*2・セキュアバイデフォルト*3の実践に向けた推奨事項をまとめたガイダンスを改訂し、**ソフトウェア開発者に対し、安全な製品を出荷するために必要な措置**を講じるよう促した。日本からは、**NISC及びJPCERT/CCが共同署名**している。
- 文書では、**ソフトウェア開発者**に対し、**セキュリティに関する3つの基本原則と各原則を実現するためのプラクティス**が示されている。一部のプラクティスでは、**経産省の文書（OSS事例集及びSBOM導入手引）が参考文書として引用**されている。
- また、ソフトウェア開発者に対して**セキュアバイデザイン・セキュアバイデフォルトを実践するための手法を示している**ほか、**ソフトウェア利用者に対する推奨事項**も示している。

*1 米NSA、米FBI、豪ACSC、加CCCS、英NCSC-UK、独BSI、蘭NCSC-NL、諾NCSC-NO、新CERT NZ、新NCSC-NZ、韓KISA、以INCD、日NISC、日JPCERT/CC、米OAS/CICTE、昭CSA、捷NÚKIB
*2 ソフトウェア製品が、サイバー攻撃者による端末、データ、インフラ等への不正アクセスを合理的に阻止可能なように構築されていること。
*3 ソフトウェア製品が、ソフトウェア利用者による追加の作業無しに、一般的なサイバー攻撃に対して耐性を持つこと。

※ **下線:** 経産省の文書が参考文書として引用されているプラクティス

ソフトウェア開発者に対する推奨事項

3つの基本原則

原則１ 顧客にもたらされるセキュリティの結果に責任を負う

【セキュアバイデフォルトのプラクティス】
- 共通のデフォルトパスワードの廃止
- 実地テストの実施
- ハードニングガイドの縮小
- セキュアでないレガシー機能の使用停止　など

【セキュアな製品開発のプラクティス】
- 安全なSDLCの枠組み（SSDF等）への適合の文書化
- 脆弱性管理の実施
- **責任を持ったOSSの利用**　など

【ビジネス上のプラクティス】
- 追加費用なしでのログ記録機能の提供
- 隠された負担の排除
- オープンスタンダードの採用
- アップグレードツールの提供　など

原則２ 徹底的な透明性と説明責任を果たす

【セキュアバイデフォルトのプラクティス】
- セキュリティ関連の総合的な統計・傾向の公表
- パッチ適用の統計の公表
- 未使用の管理者特権データの公表

【セキュアな製品開発のプラクティス】
- 内部セキュリティ管理の確立
- ハイレベルな脅威モデルの公表
- 安全なSDLCの枠組みへの自己適合証明の公表　など

【ビジネス上のプラクティス】
- 担当取締役の指名・公表
- セキュアバイデザインのロードマップの公表
- メモリに安全なプログラミング言語の使用に関するロードマップの公表　など

原則３ トップ主導

- 財務報告に対するセキュアバイデザインのプログラムの詳細の追記
- 取締役会に対する定期的な報告
- 担当取締役の権限強化
- 意味のある企業内インセンティブの構築　など

セキュアバイデザインの実践策

- メモリ安全なプログラミング言語の使用
- セキュアなハードウェア基盤の構築
- セキュアなソフトウェアコンポーネントの使用
- セキュリティ保護機能を持つWebフレームワークの使用
- パラメータ化されたクエリの使用
- SAST/DASTによるセキュリティ評価の実施
- コードレビューの実施
- **SBOMの作成**
- 脆弱性開示プログラムの確立
- CVEの完全性を担保多層防御による保護
- CISAのCyber Performance Goalsを満たす

セキュアバイデフォルトの実践策

- 共通のデフォルトパスワードの廃止
- 管理権限のあるユーザーに対する多要素認証
- シングルサインオン（SSO）の実装
- セキュアなログの管理
- ソフトウェア認可プロファイルの役割や使用例に関する利用者への提示
- 後方互換性ではなく将来を見据えたセキュリティの優先
- セキュリティ強化(ハードニング)ガイドの縮小
- ソフトウェア利用者によるセキュリティ設定の負担軽減、UXの向上

ソフトウェア利用者に対する推奨事項

- セキュリティ上の結果に関するソフトウェア開発者の責任の追求
- セキュリティバイデザインやセキュリティバイデフォルト慣行を取り入れた製品の優先購入
- 開発者と戦略的な連携関係の構築、要望の調整、セキュリティの優先
- （クラウド利用の場合）責任分担の明確化、透明性の高い企業の優先

出所） CISA, "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software" https://www.cisa.gov/resources-tools/resources/secure-by-design
【日本語仮訳】https://www.nisc.go.jp/pdf/policy/kokusai/Provisional_Translation_JP_Principles_Approaches_for_Security-by-Design-Default_October.pdf

【米国】国家サイバーセキュリティ戦略の実装計画を発表

- 2023年7月、ホワイトハウスは、同年3月に発表した**国家サイバーセキュリティ戦略**に対する**実装計画**を発表した。
- 本計画では、国家サイバーセキュリティ戦略における**5つの柱と27の戦略目標ごとに**、実装計画**（どの連邦政府機関が、何を、いつまでに実施するか）**を整理している。
- SBOMや脆弱性管理に係る実施事項として、SBOM活用によるサポート対象外ソフトウェアのリスク軽減プロセスの開発、協調的な脆弱性開示（CVD）の推進に向けた国内外との連携等の計画等が示されている。
- 序章において**「能力のあるアクターに対して責任を明確化し、インセンティブを増加させること」の重要性**が述べられている※。

国家サイバーセキュリティ戦略の5つの柱と27の戦略目標

柱1. 重要インフラの防衛	1.1 国家安全保障と公共安全を支えるためのサイバーセキュリティ要件の確立	1.2 官民協力の拡大	1.3 連邦政府のサイバーセキュリティセンターの統合
	1.4 連邦政府のインシデント対応計画やプロセスの明確化	1.5 連邦政府における防衛の近代化	
柱2. 脅威主体の破壊と解体	2.1 破壊的活動の統合	2.2 脅威主体を破壊するための官民協力強化	2.3 情報共有や被害者通知の速度と規模の拡大
	2.4 米国拠点のインフラ悪用の防止	2.5 サイバー犯罪への対抗とランサムウェアの撲滅	
柱3. セキュリティとレジリエンスを促進させるための市場原理の形成	3.1 データ管理者への説明責任の付与	3.2 セキュアなIoT機器の開発促進	3.3 安全でないソフトウェア製品とサービスに対する責任の再構築
	3.4 連邦政府の補助金やその他のインセンティブを利用したセキュリティの構築	3.5 連邦政府調達を活用した説明責任の向上	3.6 連邦政府によるサイバー保険市場の支援検討
柱4. レジリエンスな未来への投資	4.1 インターネットの技術的基盤の確保	4.2 サイバーセキュリティのための連邦政府研究開発の活性化	4.3 ポスト量子暗号への備え
	4.4 クリーンエネルギーの未来におけるセキュリティ確保	4.5 デジタルIDを活用したデジタルエコシステムの開発支援	4.6 サイバー人材強化のための国家戦略の策定
柱5. 共通的な目標の追求のための国際的なパートナーシップの構築	5.1 デジタルエコシステムへの脅威に対抗するための連合体の構築	5.2 国際的なパートナーの能力の強化	5.3 同盟国やパートナーを支援する米国の能力の拡大
	5.4 責任ある国家行動の世界的規範を強化するための連合体の構築	5.5 情報・通信・運用技術製品およびサービスのための安全なグローバルサプライチェーンの構築	

実施計画（SBOMや脆弱性管理に係る事項抜粋）

- **SBOMの活用による、サポート対象外のソフトウェアのリスクを軽減（実施計画 3.3.2）**
  SBOMのさらなる開発を促進することで、広く使用されている又は重要インフラを支えるサポート対象外のソフトウェアがもたらすリスクを特定し、軽減するためのプロセスを開発する。このために、2025年度第2四半期までに、**CISA**は以下の事項を実施する。
  - ✓ 政府機関のSRMA（Sector Risk Management Agencies）と協力し、重要インフラを支えるサポート対象外のソフトウェアの使用状況を収集し、SBOMの規模及び実施における問題を特定し、解決を推進する。
  - ✓ 世界的にアクセス可能な**EOLやEOSのソフトウェアに関するデータベースの要件**を検討し、SBOMに関する国際的な作業部会を開催する。
- **協調的な脆弱性開示に向けた国内外との連携（実施計画 3.3.3）**
  安全なソフトウェア開発の実践を奨励するため、国内外問わず、すべての技術タイプ及びセクターにわたって、協調的な脆弱性の開示（CVD）を推進するため、2025年度第4四半期までに、**CISA**は以下の事項を実施する。
  - ✓ 国際的な**脆弱性コーディネーターに関する実践共同体の創設**を含め、あらゆる技術タイプやセクターにわたる官民の組織間で、協調的な脆弱性開示（CVD）を実現するための国内的・国際的な連携を確立する。なお、本事項には、国際的なCSIRTやその他の機関を支援し、協調的な脆弱性開示に関する世界的な認識と能力を確立することも含まれる。

[1] White House, ” National Cybersecurity Strategy Implementation Plan”
https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf
[2] White House, ” National Cybersecurity Strategy”
https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

※ 関連して、国家サイバーセキュリティ戦略[2]では、**「政府機関の調達力」を活用**してインセンティブを確保することの重要性が明記されている。

【米国】CISA サイバーセキュリティ戦略計画（2024-2026年度）を発表

- 2023年8月、CISAはサイバーセキュリティ戦略計画（2024-2026年度）を発表した。
- 本戦略計画では、**CISAの取組の指針として、3つの目標と9つの目的**を示している。さらに、本戦略計画では、**各目的を実行するための手段と期待する効果**を示しており、将来的に**実行した手段がもたらす効果を測定**することに重点を置いている。
- 脆弱性管理や安全なソフトウェア製品開発に係る事項として、**既知の悪用された脆弱性（KEV）の評価、協調的な脆弱性開示（CVD）の推進、安全な製品を開発するための基準の策定等が示されている。**

CISA サイバーセキュリティ戦略計画の3つの目標と9つの目的

目標1：サイバー攻撃からの差し迫った脅威に対処	1.1 サイバーセキュリティに関する脅威やサイバー攻撃活動の可視性を高め、対処能力を向上させる
	1.2 重大で悪用可能な脆弱性の開示・探索・対策を推進する
	1.3 合同サイバー防衛作戦を計画、演習、実行し、重大なサイバーセキュリティインシデントへ備える
目標2：デジタル環境のセキュリティ強化	2.1 サイバー攻撃がどのように発生し、どのように防ぐかを理解する
	2.2 効果的なサイバーセキュリティ投資の実施を推進する
	2.3 サイバーセキュリティ強化における問題を解決に導き、解決の進捗を測定するのに役立つ情報やサービスを提供する
目標3：広範囲にわたるセキュリティ確保の推進	3.1 信頼できるソフトウェア製品の開発を推進する
	3.2 新興技術がもたらすサイバーセキュリティリスクを理解し、低減する
	3.3 国のサイバー人材育成の取組に貢献する

目的に対する実行手段と期待する効果（脆弱性管理や安全なソフトウェア製品開発に関する事項抜粋）

【実行手段】
- ✓ 重要インフラや連邦政府システム全体の脆弱性、特に既知の悪用された脆弱性（KEV）に関する可視性を評価する。
- ✓ 協調的な脆弱性開示（CVD）の取組を推進することによって、研究団体や民間企業との連携を高める。

【期待する効果と尺度】
- ✓ 重要インフラと連邦政府システムにおける既知の悪用された**脆弱性に対する対処時間を短縮**する。
- ✓ CISAの脆弱性評価及びリスク評価からの推奨事項が、採用される割合が増加する。
- ✓ 適切な調整や必要な緩和策なしに開示される脆弱性の数が減少する。

【実行手段】
- ✓ 安全な製品を開発・維持するための基準と方法を策定する。また、製品が、策定した方法をどの程度採用しているかを評価するため、関係者と連携を進める。

【期待する効果と尺度】
- ✓ 製品開発者による**脅威モデル（何を、誰から守るかを説明したもの）を認識した数が増加**する。
- ✓ **SSDFの実装を宣言する製品開発者の数が増加**する。
- ✓ 製品に関する脆弱性情報が、正確で完全であることのコミットメントを公開する製品開発者の数が増加する。
- ✓ セキュリティ・バイ・デザインのロードマップを公開した製品開発者の数が増加する。
- ✓ MFA（他要素認証）の採用、安全でないレガシープロトコルの使用、未サポート製品を使用している顧客の割合等、セキュリティ関連の統計やトレンドを定期的に公開する製品開発者の数が増加する。

出所） CISA, ”CISA CYBERSECURITY STRATEGIC PLAN FY2024 – 2026”
https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf

【米国】CISA OSSセキュリティロードマップ（2024-2026年度）を発表

- 2023年9月、CISAは、**OSSの安全な使用や開発**を支援するための**CISAの取組策**を示すOSSセキュリティロードマップ（2024-2026年度）を発表した。
- 本ロードマップでは、**連邦政府内外におけるOSSの使用及び開発**においてセキュリティ強化を推進するためのCISAの取組として、**4つの目標と15の目的**を示している。
- SBOMや脆弱性管理に係る事項として、**OSSのサプライチェーン全体での包括的なSBOM共有に向けた要件整理・課題解決**、**OSSの脆弱性情報開示・対処を促進するための取組**等が示されている。

CISA OSSセキュリティロードマップの4つの目標と15の目的の概要

目標	目的	概要
1. OSSのセキュリティを支援するためのCISAの役割の確立	1.1 OSSコミュニティとの連携	OSSコミュニティとのリアルタイム連携を可能にするチャンネルを設立する。
	1.2 中央集権型のOSSエンティティのセキュリティ確保の推進	中央集権型のOSS関連システムのセキュリティ確保のための原則を策定する。
	1.3 国際的なパートナーとの連携と協力の拡大	国際的なパートナーや同盟国と、共通の関心分野での協力機会を拡大する。
	1.4 CISAのOSSセキュリティに関する業務の組織化	CISA内に、OSSセキュリティワーキンググループを設立する。
2. OSSの使用状況とリスクの可視性の向上	2.1 OSSの使用状況の把握	政府や重要インフラにおけるOSS使用状況の評価方法を開発し、状況を把握する。
	2.2 OSSにおけるリスク評価のためのフレームワークの開発	OSSのリスクを評価するためのフレームワークを開発し、**OSS使用に関する分類**を行う。
	2.3 連邦政府や重要インフラ組織におけるOSSのリスク評価	政府や重要インフラで使用されるOSSのリスク評価結果リストを作成する。
	2.4 OSSに含まれる重要なリスクの理解	リスクとなりうる重要なOSSを継続的に評価するプロセスを開発する。
3. 連邦政府のOSS使用のリスクの削減	3.1 OSSの安全な使用を支援するソリューションの評価	OSSの安全な使用を支援するソリューションの実現性や効果を評価する。
	3.2 OSPO※1の実装ガイダンスの策定	政府機関がOSPOを実装するためのベストプラクティスをまとめたガイダンスを策定する。
	3.3 OSS使用におけるセキュリティ強化のための連邦政府の取組推進	OS3I※2と連携し、OSSエコシステムのセキュリティやレジリエンスを強化する。
4. OSSエコシステムのセキュリティ強化	**4.1 OSSサプライチェーン内でのSBOMの推進**	サプライチェーン全体での**SBOM共有に向け、自動化の要件整理・課題解決**を行う。
	4.2 OSSの開発者のためのセキュリティ教育の促進	OSSの開発者がセキュリティに関する情報を収集するためのツールキットを公開する。
	4.3 OSSを安全に使用するためのベストプラクティスの公表	政府や重要インフラ等がOSSを安全に使用するためのベストプラクティスを公開する。
	4.4 OSSにおける脆弱性の情報開示や対処の促進	OSSコミュニティと連携して、OSSの脆弱性特定や情報開示プロセス等を確立する。

※1 Open Source Program Officeの略で、OSS活用環境の整備、関連部署とのOSS活用における連携、OSSコミュニティとの連携等、OSS関連活動を支援する組織のこと。
※2 Open Source Software Security Initiativeの略で、OSSのセキュリティを強化し、政府のリソース活用拡大を目的とした省庁間のワーキンググループのこと。

出所） CISA, "CISA Open Source Software Security Roadmap" https://www.cisa.gov/sites/default/files/2023-09/CISA-Open-Source-Software-Security-Roadmap-508c%20%281%29.pdf

その他諸外国におけるSBOMに関する取組

- **ドイツBSI（連邦政府情報セキュリティ庁）**は、EUの**サイバーレジリエンス法**によって将来的に製造業者に課される要件を**事前に周知する目的**で、**SBOMのフォーマットに関する要件及び技術的な要件をまとめた技術ガイドライン**を2023年8月に公開した。
- **オランダNCSC（国家サイバーセキュリティセンター）**は、組織におけるSBOM導入を支援する目的で、**SBOMに関する基礎知識やSBOMの作成・管理・共有に係るプロセス**を示した「SBOMスターターガイド」を2023年7月に公開した。

- ドイツBSIは、EUサイバーレジリエンス法によって将来的に製造業者に課される要件を事前に周知する目的で、製造業者に対する技術指針（BSI TR-03183 Cyber-Resilienz-Anforderungen）を検討している。
- 2023年8月、当該技術指針のパート2として、SBOMの要件を示した技術ガイドライン「SBOM-Anforderungen（SBOM要件）」を公開した※。
- 技術ガイドラインでは、ソフトウェアベンダーを主な対象とし、SBOMのフォーマットに関する要件及び技術的な要件を記載している。
- フォーマットに関する要件について、CycloneDX v1.4以上及びSPDX 2.3以上を求めている。
- SBOMに含めるべき情報について、米国NTIA「最小要素」で定義された「データフィールド」に加え、本ガイドラインでは各コンポーネントのライセンスに関する情報を「必要最低限のデータフィールド」として含めることを求めている。

※ EUサイバーレジリエンス法の一般的な要求事項を解説したパート1は2023年末までに発行される予定。

- オランダNCSCは、2023年7月に、組織におけるSBOM導入を支援するガイドである「SBOM-startersgids（SBOMスターターガイド）」を公開した。
- ガイドでは、SBOMやVEXに関する基礎知識が概説されているほか、組織がSBOMを作成・管理・共有するためのプロセス、サプライヤーとの連携に向けたTipsを概説している。
- 加えて、代表的な脆弱性識別子に関する解説がなされているほか、組織内の脆弱性管理においてSBOMを活用する方法についても示されている。

出所）BSI, SBOM-Anforderungen: TR-03183-2 stärkt Sicherheit in der Software-Lieferkette https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/TR-03183-2-SBOM-Anforderungen.html, NCSC, SBOM startersgids https://www.ncsc.nl/documenten/publicaties/2023/juli/5/sbom-startersgids

１．ソフトウェアの管理手法等に関する海外の動向

２．SBOM実証に関する中間報告

３．SBOM取引モデル概要

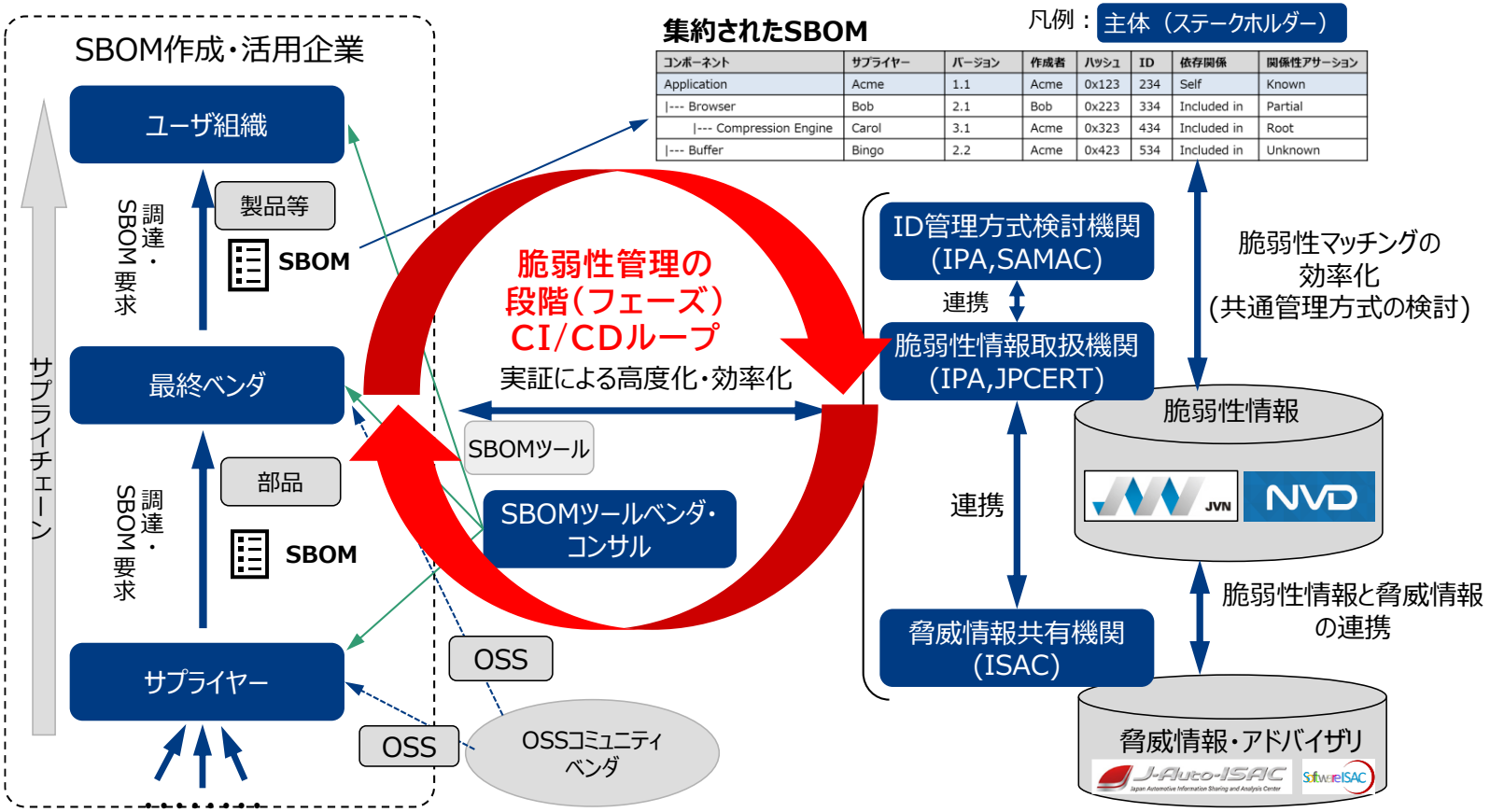
４．SBOM事業の成果物を活用した取組みの方向性

SBOM実証の全体像：SBOMを活用した脆弱性管理の効率化

実証の目的（ポイント）

- 脆弱性管理プロセスを俯瞰し、SBOMを活用した脆弱性管理の効率的な方法について検討し、その効果評価、課題の整理を行う。**脆弱性情報の提供に係る機関（IPA, ISAC等）と連携**し、脆弱性情報を効率的に取得する方法を検討する。
- SBOMを活用した脆弱性管理を広く普及させるため、**中小企業を含む多くの企業が活用**できるように、脆弱性の深刻度、脅威、アドバイザリなども活用するための方策等について整理する。

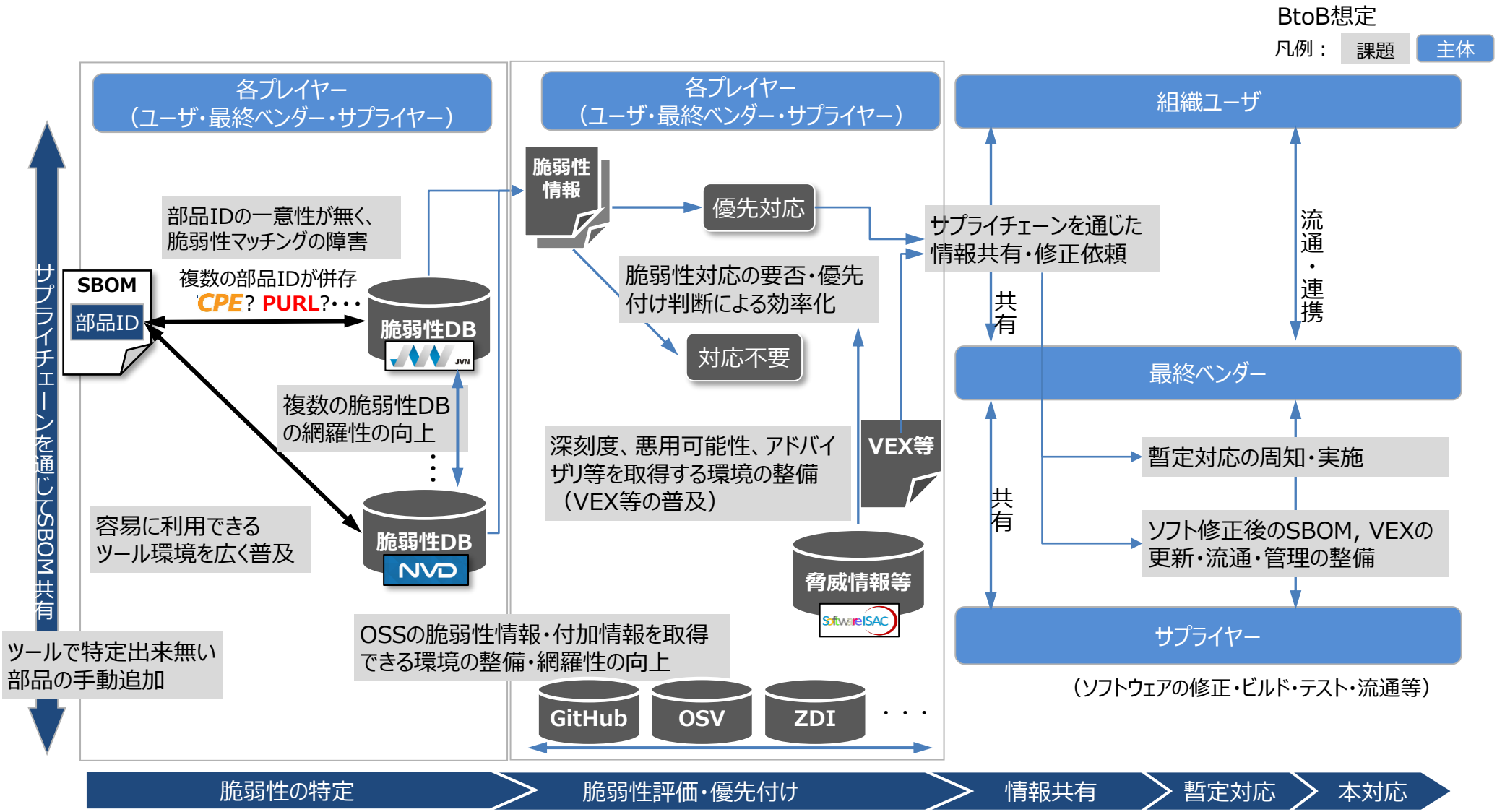
脆弱性管理の主なステークホルダとプロセスの全体像



（前回TF資料再掲）

SBOMを活用した脆弱性管理における課題（俯瞰図）

- SBOMを活用した脆弱性管理の効率化・普及促進に向けて、各プレイヤー、ユーザなどにおいて様々な対応が必要であり、特に脆弱管理プロセス（脆弱性の特定、脆弱性評価等、情報共有、対応）における課題が存在。



脆弱性管理プロセス

実証で評価・検討すべき事項（実証の要件）

（前回TF資料再掲）

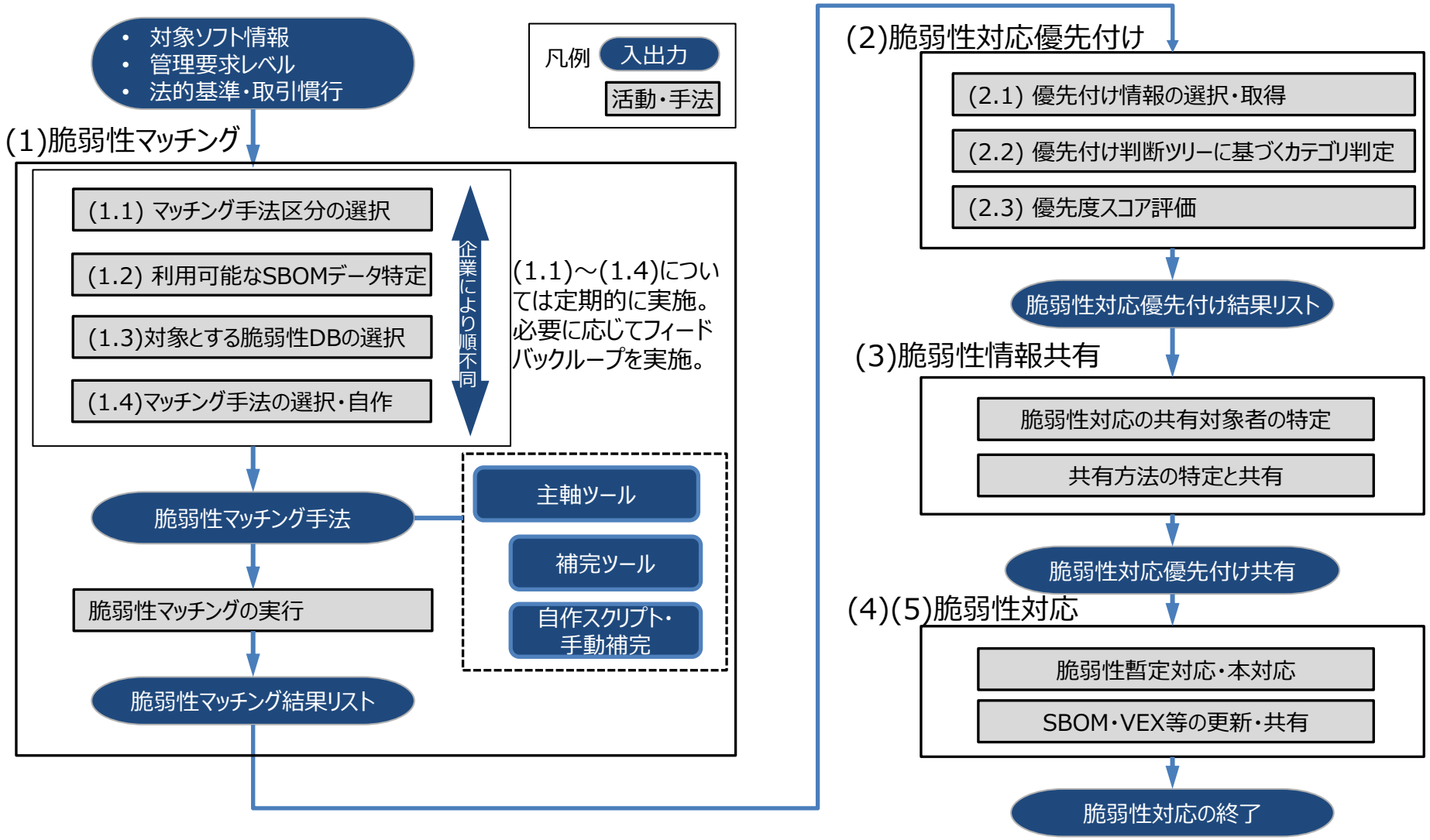
- 脆弱性管理を行うSBOM利用者について、初心者と上級者を想定し、(1)mjcheck等のツールをベースに基礎的な対応と、(2)ツールの選定、APIの活用、独自の脆弱性対応優先付けなど高度な対応を対象とする。両者にとって有益な手引きがまとめられるよう実施項目を整理する。
- また、ツールで対応できることの機能ニーズの整理と、SBOM利用者による人の対応が必要な事項について整理する。

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

SBOMを活用した脆弱性管理プロセスの検討

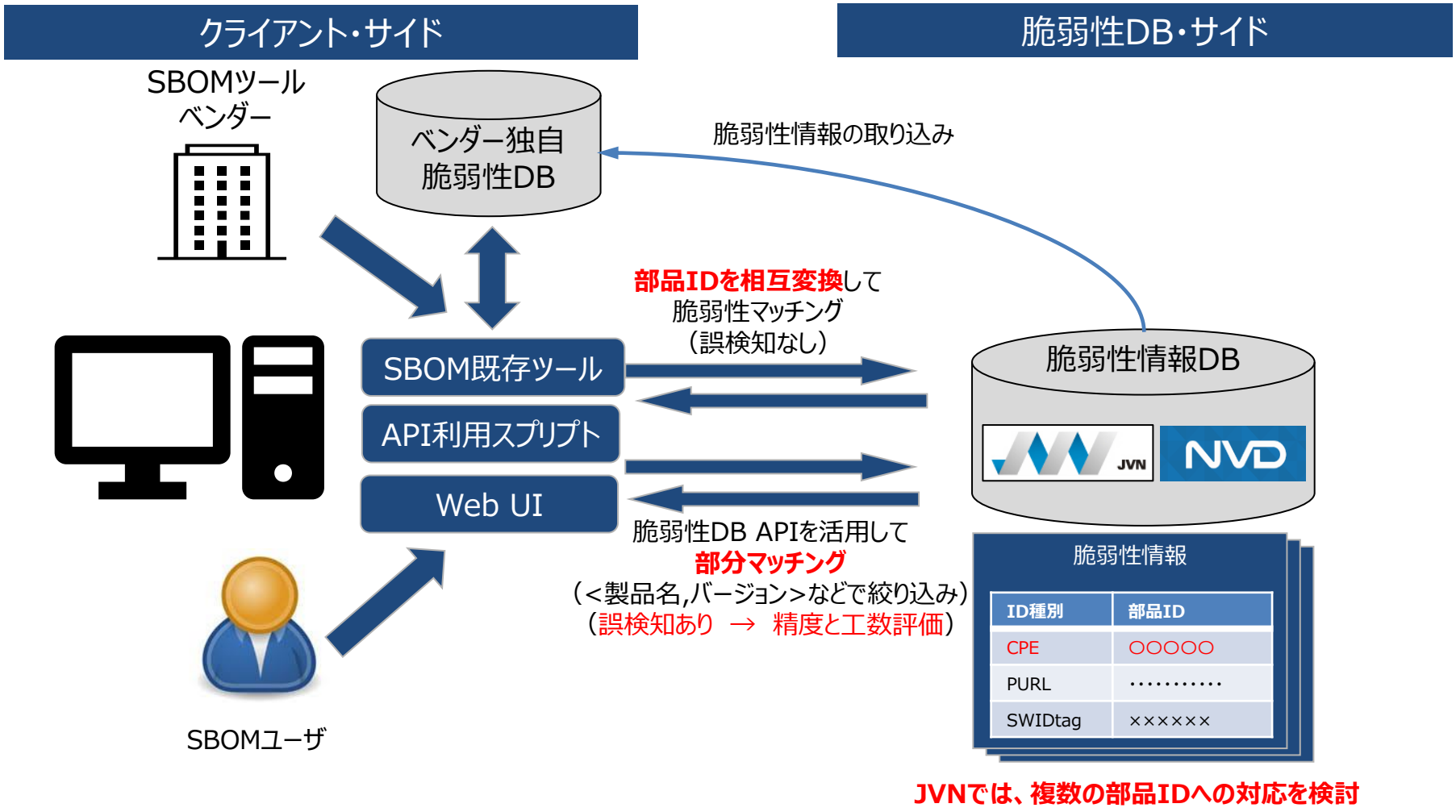
脆弱性管理プロセスの各フェーズについて、本事業で検討している実施ステップを整理する。

プロセス全体を通じて、主軸なるツールの検討や、必要に応じて補完的なツールや自作スクリプト・手動作業など組合わせを想定。



(1.1)マッチング手法区分の選択：区分の整理

- 脆弱性マッチングは、**クライアント・サイドのアクセス形態**と**対象とする脆弱性DB**の**組合せ**によって分けられる。
- クライアント・サイドについては、大まかに分けて、**SBOM既存ツール、API利用スクリプト、Web UIの３通り**が考えられる。
- これらの区分は、**脆弱性DBの網羅性　ユーザの技術力、費用などが制約・要件**となり、判断が求められる。
- SBOM既存ツールは、API利用スプリプトに比べ、コーディングの負担が抑えられるが、検索方法が固定的であり柔軟性に欠ける場合がある。



(1.1)マッチング手法区分の選択：選択の考え方

脆弱性管理の要求レベル、脆弱性DBの管理範囲、技術力、人的リソースなどに応じて、３つの手法区分についてユースケース、主なユーザ、メリット・デメリットを整理すると以下のようになる。

マッチング手法区分	ユースケース・必要性	主なユーザ	メリット・デメリット
APIの利用	既存ツールでは検索できない脆弱性DBに対して、APIを用いて脆弱性検索が可能となり、脆弱性検出の網羅性を高めることができる。	ソフトウェアに対する高い要求レベル（脆弱性リスクが低い）が求められるソフトウエアベンダ（メーカー、サプライヤー）が主なユーザと想定される。また、重要インフラ事業者など要求レベルの高いユーザ企業についても、自律的にAPIを用いた網羅性の高い脆弱性検索が求められるケースがある。	**（メリット）APIを利用して部品IDの変換や脆弱性DBの範囲拡大など柔軟にカスタマイズして、常時自動監視**を行うことができる。検出漏れや誤検出などを防止する検索手法の作りこみ、検索後のアラート連動など可能になる。 **（デメリット）**APIを用いたコーディングの技術力と工数等のリソースが求められる。
既存ツールの利用	限られた人員、技術などのリソースの元で、既存ツールで検索可能な脆弱性DBに限定して、最小限対応すべき脆弱性に対応する。	有償ツールの場合、予算に余裕のある大企業。無償ツールは、中小のユーザ組織、ベンダーなどの場合、APIコーディングを行う人員、技術などが限られる組織。	**（メリット）APIコーディングなしに、限られた人員で脆弱性を特定**できる。 （デメリット）既存ツールが提供されるDBに対象が限定され、特定される脆弱性の網羅性が限定的になる。
Web UI利用	APIを用いたコーディングの前に、工数を抑えて、試行的に脆弱性の検索方法の検討や脆弱性の状況を確認する。	高度なセキュリティレベルを求められるAPI利用者や、既存ツールの利用者が、定常業務前の試行的な脆弱性検索に利用する。	**（メリット）**APIコーディングや既存ツールの利用による定常業務化前に、**脆弱性検索の試行検討や脆弱性状況の把握ができる。** **（デメリット）**WebUIの利用は、手動操作が必要となるため、定常業務化できるAPIや既存ツールの利用よりも非効率となる。

(1.2) 利用可能なSBOMデータ特定

- 対象ソフトウェア（部品）について、利用可能なSBOMデータに応じて、利用可能なSBOMツール、検索可能な脆弱性DBが異なるため、SBOMデータの特定が必要になる。

① 対象ソフトウェアについてSBOMを外部から取得

- **<u>サードパーティソフトウェアのSBOM提供状況の確認</u>**
  OSSや既存のサードパーティソフトウェアについては、提供されるSBOMが予め決まっており、契約により必要なSBOMフォーマットを要求することが難しいため、事前に確認することが必要である。
- **<u>委託開発契約におけるSBOMの規定</u>**
  開発委託ソフトウェアについては、開発者の技術力、体制により契約書などによりSBOMフォーマット、部品ID標準について合意を取ることが必要になる。

②ツールを用いたSBOMを生成

利用するソフトウェア（部品）について、ベンダー（サプライヤー）から取得することができない場合、SBOMツールを用いた自動生成、または、パッケージマネージャの構成情報等を利用したSBOM作成が必要となる。

【参考】 SBOMフォーマット・部品ID標準の概要

SBOMフォーマット	開発主体	特徴
SPDX	Linux Foundation	知財・ライセンス管理を主目的に標準化。パッケージ、コンテナ、スニペットなどの対象を管理できる。
CycloneDX	OWASP	セキュリティ管理を主目的に策定。VEXを包含することが可能。
SWID	ISO/IEC, NIST	ソフトウェアID体系を含むソフトウェア管理の標準。

部品ID	開発主体	特徴
PURL	OSSコミュニティ(gitter)	OSSなど、パッケージマネージャを中心にレポジトリに応じてIDが決定される分散割当方式である。
CPE	NIST	セキュリティ情報共有標準SCAPの要素として規定。主に脆弱性が報告された際にCPEが割り当てられる。
SWID	ISO/IEC, NIST	CPEの上位互換で、NVDにおいてCPEからSWIDに移行を宣言しているが、現時点で採用は進んでいない。

(1.3)対象とする脆弱性DBの選択

- 脆弱性DBの選択は、リスク低減、コスト低減の観点から比較し、**個社ごとに優先度ポリシーを考慮して判断**することが期待される。

  - 脆弱性DBの選択は、脆弱性情報のカバレッジ拡大、脆弱性対応の迅速化、コスト効率化の観点から判断することが期待される。
  - これらの観点の優先度は、個社によってポリシーが異なるため、個社ごとに脆弱性DBを選択するこが期待される。
  - 例えば、コスト制約の強い中小企業は、費用、簡易ツールの利用を優先してDBを選択し、リスク低減の要求が高い企業は、カバレッジ拡大や対応の迅速化に対応したDBを優先的に選択する。

個社で優先度ポリシーを検討

比較優先事項			評価上位の脆弱性DB			基準例
リスク低減	脆弱性情報のカバレッジ拡大	脆弱性件数	民間DB 1	公的DB1	公的DB 2	件数カバー率7割以上
		CVE以外の脆弱性	民間DB2	民間DB3	民間DB4	CVE以外対象
		日本製品重点化	公的DB 2	—	—	日本製最大集合
		OSS重点化	民間DB4	民間DB2	民間DB5	重点化明示
リスク低減 / コスト低減	脆弱性対応の迅速化・効率化（優先付け）	インシデント有無	公的DB1	民間DB 1	民間DB8	専用フィールド有
		Exploit有無	民間DB6	民間DB7	民間DB 1	専用フィールド有
		CVSS有無	公的DB1	公的DB 2	民間DB 1	必須上位3件
		アドバイザリ有無	公的DB1	公的DB 2	民間DB 1	専用フィールド、上位3件
コスト低減	自動化	部品ID標準	公的DB1	公的DB 2	民間DB 1	標準指定
		API・ツール提供	公的DB1	公的DB 2	民間DB2, 民間DB4	API有
		スクリプト作成容易	公的DB1	公的DB 2	—	標準ID∧API有
	情報無償提供		公的DB1	公的DB 2	その他7件	無料2件
	日本語情報提供		公的DB 2			

枠内の和集合として対象を選定

(1.4)マッチング手法の選択

	仕様上の可否	動作確認
◎	可能	確認済み
○	可能	未確認
△	仕様不明（動作不備）	
×	仕様上不可	

- **マッチング手法区分、入力SBOM形式、対象の脆弱性DBの選択結果や制約条件**に基づき、どの手法が利用可能か判断する。
- 下記整理表は、実証調査時点の仕様および事例動作確認に基づく参考判断を示す。

適用可能なマッチング手法の一覧表（簡易表示※）

脆弱性DBの種類 →

手法区分・入力SBOMデータの種別 ↕

手法区分	SBOM形式	部品ID標準	公的DB1	公的DB2	公的DB３	民間DB1	民間DB2	民間DB3	民間DB4	民間DB5	民間DB6	民間DB7	民間DB8
API利用	SPDX	CPE	×	○	◎	○	○	○	○	×	×	×	○
		PURL	△	△	◎	○	○	○	○	×	×	×	○
		独自ID	△	△	○	○	○	○	○	×	×	×	○
	Cyclone DX	CPE	×	○	○	○	○	○	○	×	×	×	○
		PURL	△	△	○	○	○	○	○	×	×	×	○
		独自ID	△	△	○	○	○	○	○	×	×	×	○
	SWID	SWID	×	×	×	×	×	×	×	×	×	×	×
		CPE	×	○	○	○	○	○	○	×	×	×	○
		PURL	△	○	○	○	○	○	○	×	×	×	○
		独自ID	△	○	○	○	○	○	○	×	×	×	○
Web UI利用	SPDX	CPE	○	○	○	○	○	○	○	○	○	×	○
		PURL	○	○	○	○	○	○	○	○	○	×	○
		独自ID	○	○	○	○	○	○	○	○	○	×	○
	Cyclone DX	CPE	○	○	○	○	○	○	○	○	○	×	○
		PURL	○	○	○	○	○	○	○	○	○	×	○
		独自ID	○	○	○	○	○	○	○	○	○	×	○
	SWID	SWID	×	×	×	×	×	×	×	×	×	×	×
		CPE	○	○	○	○	○	○	○	○	○	×	○
		PURL	○	○	○	○	○	○	○	○	○	×	○
		独自ID	○	○	○	○	○	○	○	○	○	×	○
既成ツール	SPDX (json)	CPE	×	×	×	×	×	×	×	×	×	×	×
		pURL	×	×	×	×	○ツール3	○ツール3	×	×	×	×	×
		その他	×	×	△ツール２	◎ツール２	×	×	×	×	×	×	×
	Cyclone DX (json)	CPE	×	×	×	×	×	×	×	×	×	×	×
		pURL	×	×	×	×	○ツール3	○ツール3	×	×	×	×	×
		その他	×	×	△ツール２	◎ツール２	×	×	×	×	×	×	×
	SWID	CPE	×	○ツール１	×	×	×	×	×	×	×	×	×
		pURL	×	×	×	×	×	×	×	×	×	×	×
		その他	×	×	×	×	×	×	×	×	×	×	×

※補足情報の詳細表記は省略

(2.1)優先付け情報の選択･取得

- 優先付け情報として、リスクの構成要素に応じて分類整理した案を以下に示す。
- 各社ごとにこれらの情報の取得可否を判断し、脆弱性DBから取得する。

- **（脆弱性対応優先付けの尺度）＝（リスク）/ （コスト）**
  ＝（脅威発生可能性）×（脆弱性残留可能性）×（影響度）／（コスト）

優先付けに利用する情報の整理

評価カテゴリ			評価項目	説明・重要性の考え方
リスク	発生可能性	脅威発生可能性(外部要因)	インシデント(有・無・不明)	実際に悪用・事件が発生しており緊急性が高い。
			Exploitコードの公開（有・無・不明）	悪用コードが公開されており、悪用される可能性が高い。
		脆弱性残留可能性(内部要因)	VEX脆弱性ステータス（影響：有・無・不明）	脆弱性に係る部品を利用した開発者が直接評価したものであり精度が高い。
			VEX以外の悪用可能性独自評価（悪用：可・否・不	VEXが取得できない場合、独自に悪用可能性を評価する。部品開発主体の作成を前提とするVEXとは異なり、精度が低い可能性が存在する。
			アドバイザリ対処策適用可否（可・否・不明）	脆弱性に対する一般的な対処策であり、部品ID・脆弱性IDが完全に一致する場合以外は、悪用可能性の精度は高くない。
			脆弱性修正パッチの有無（ゼロデイ）	ベンダーにとって、脆弱性修正パッチを未提供である場合、ユーザ・調達者に対する責任が大きいため優先度が高い。
	影響度		CVSSスコア（特に影響評価）	一般的なケースにおける影響度および深刻度の評価であり、ユーザ環境に基づく評価ではないため、精度は高くない。
			ユーザ影響度評価（情報資産の重要性CIA）	ユーザの情報資産(CIA)に特化した評価であり実態に基づく評価であり精度が高いと想定される。外部提供サービスは、社内システムより影響度が高い。(CIA各要素2,1,0の合計値など)
			多数の製品・サービスに影響、問合せ多数	後半に影響する可能性がある。(3段階評価3,2,1)
コスト			サービス中断・縮退	社内外のサービス中断・縮退の影響を考慮し、タイミングを検討(3,2,1)
			ソフトウェア修正	サプライヤーの修正が遅い場合、自社で修正する場合のタイミングを検討
			修正の影響テスト・修正の適用	修正適用の影響テストが可能か検討
			悪用可能性評価コスト	悪用可能性評価をサプライヤーに代わり自社で行う場合のコストを評価し対応判断。

(2.2)優先付け判断ツリーに基づくカテゴリ判定

- 脆弱性情報の分析に基づく対応区分の判断手法であるSSVC※を活用し、判断ツリーを用いてカテゴリ判定する（４区分：即対応、通常保守より優先、通常保守、対応保留）
- SSVCでは、悪用可能性、悪用容易性、技術的影響度、ユーザ影響度の観点で、条件分岐を行う判断ツリーを用いる(下図)
- 本実証では、整理した脆弱性付加情報を用いて、判断ツリーの各条件分岐の考え方を整理した。

脆弱性付加情報に基づく判断ツリーの構成

悪用可能性	悪用効率性	技術的深刻度	ユーザ影響度	対応優先度
高	高	高	高	即対応
			中	即対応
			低	優先
		低	高	即対応
			中	優先
			低	優先
	低	高	高	即対応
			中	優先
			低	保留
		低	高	優先
			中	保留
			低	保留
中	高	高	高	優先
			中	通常保守
			低	保留
		低	高	優先
			中	保留
			低	保留
	低	高	高	優先
			中	通常保守
			低	保留
		低	高	通常保守
			中	保留
			低	保留
低	高	高	高	優先
			中	保留
			低	保留
		低	高	通常保守
			中	保留
			低	保留
	低	高	高	通常保守
			中	保留
			低	保留
		低	高	保留
			中	保留
			低	保留

脆弱性情報

脆弱性対応優先付けカテゴリ判定(4区分)

区分	基本的な対応内容
即対応（immediate）	全てのリソースを集中し、 必要に応じて組織の通常業務を停止して可能な限り迅速に対応を行う
優先保守（out-of-cycle）	通常よりも迅速に行動し、計画外の次の利用可能な機会に、必要に応じて通常業務時間外を含めて緩和策または修復策を実施する
通常保守（scheduled）	定期メンテナンス時に対応する
対応保留（defer）	現時点では対応しない。状況を注視する。

※ SSVC(Stakeholder-Specific Vulnerability Categorization)
CISAが公開する脆弱性対応の優先付けを行うフレームワーク

(2.2)優先付け判断ツリーに基づくカテゴリ判定

- 判断ツリーの条件分岐における判断基準として、実証・調査に基づき、脆弱性付加情報に基づく判断の考え方を整理。
- 判断基準は、ステークホルダーのタイプを４区分に分けて整理。タイプ分類は、（開発企業、ユーザ企業）×（技術が高い、技術が高くない）。
- ユーザ影響度は、開発企業での判断は難しく、システムの一般的な用途に基づき判断し、明確な判断が難しい場合、高リスクとみなす。

条件分岐の判断基準（構成）

主なステークホルダーの分類

条件分岐		ソフトウェア開発企業		ソフトウェアユーザ企業	
		技術が高い	高くない	技術が高い	高くない
悪用可能性	高				
	中				
	低				
悪用容易性	高				
	低				
技術的影響度	高				
	低				
ユーザ影響度	高				
	中				
	低				

条件分岐の区分

条件分岐の判断基準（抜粋詳細）

		ソフトウェア開発企業	
条件分岐		技術が高い	技術が高くない
悪用可能性（Exploitation）	インシデント（実攻撃）あり	下記のいずれか一つ以上を満たす場合。 ・**[インシデント（実攻撃）の有無]**自社製品に対して、この脆弱性をついた実際の攻撃事例を把握しているが、まだ修正パッチが準備できていない場合（ハニーポッドに対する攻撃含む。社内での発見、社外からの脆弱性やインシデントの報告含む） ・**[インシデント（実攻撃）の有無]**製品に含まれるOSSやサプライヤー提供のコンポーネントに対して該当脆弱性をついた実際の攻撃が報告されている（インシデントあり） ・**[ゼロデイ脆弱性]**自社製品の修正パッチや回避策が準備されていないにもかかわらず、セキュリティ研究者などにより該当製品の脆弱性が公開されてしまった場合（ゼロデイ脆弱性となる場合） ・**[PoCコード公開（実攻撃なし）の有無][OSS浸透度]**攻撃事例は報告されていないものの、該当コンポーネントが広く使用されていて、PoCコードが存在している（攻撃者が悪用する可能性が高い場合）	下記のいずれか一つ以上を満たす場合。 ・**[インシデント（実攻撃）の有無]**自社製品に対して、この脆弱性をついた実際の攻撃事例を把握しているが、まだ修正パッチが準備できていない場合（社内での発見、社外からの脆弱性やインシデントの報告含む） ・**[インシデント（実攻撃）の有無]**製品に含まれるOSSやサプライヤー提供のコンポーネントに対して該当脆弱性をついた実際の攻撃が報告されている（インシデントあり） ・**[ゼロデイ脆弱性]**自社製品の修正パッチや回避策が準備されていないにもかかわらず、セキュリティ研究者などにより該当製品の脆弱性が公開されてしまった場合（ゼロデイ脆弱性となる場合） ・**[OSS浸透度]**該当のコンポーネントが広く使用されている

(2.3)優先付けスコア評価

- 優先付けカテゴリ判定とは別に、定量的な優先付けスコアを評価して、同一カテゴリ内の脆弱性の優先付けや参考情報として利用する。
- スコア評価は、評価項目ごとの値（有、無、不明）などに数値を割当て、ウェイトをかけた総和で評価する。
- 参考ウェイトをベースに、個社ごとの優先ポリシーに応じてウェイトを調整する。

優先付けスコア評価の評価項目と参考ウェイト

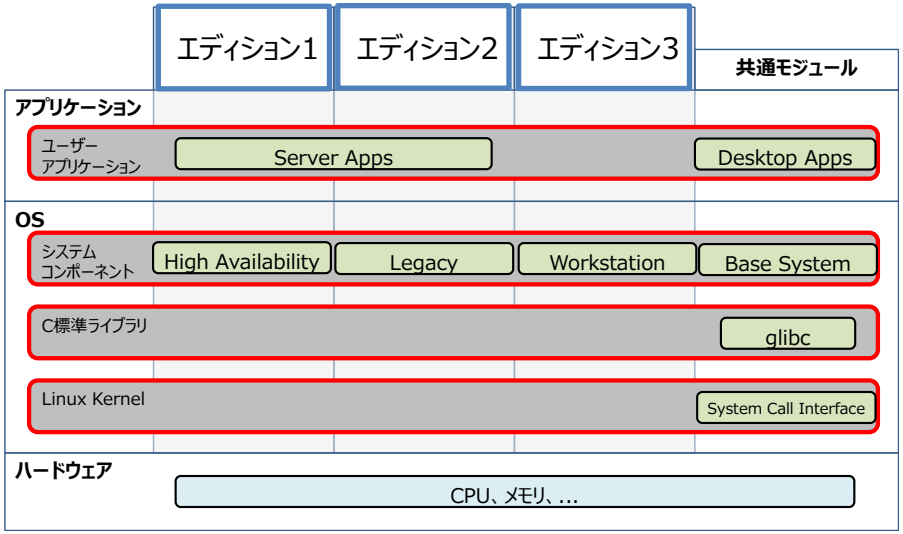
個社のポリシーで設定

評価カテゴリ			評価項目	値	ウェイト(重要性)	参考ウェイト
リスク	発生可能性	脅威発生可能性(外部要因)	インシデント(有・無・不明)	有		3
			Exploitコードの公開（有・無・不明）	無		2
		脆弱性残留可能性(内部要因)	VEX脆弱性ステータス（影響：有・無・不明）	無		3
			VEX以外の悪用可能性独自評価（悪用：可・否・不	可		2
			アドバイザリ対処策適用可否（可・否・不明）	可		1
			脆弱性修正パッチの有無（ゼロデイ）	有		3
	影響度		CVSSスコア（特に影響評価）	8.5		2
			ユーザ影響度評価（情報資産の重要性CIA）	3		3
			多数の製品・サービスに影響、問合せ多数	2		3
コスト			サービス中断・縮退	2		3
			ソフトウェア修正	1		1
			修正の影響テスト・修正の適用	2		2
			悪用可能性評価コスト	1		2
総合評価						

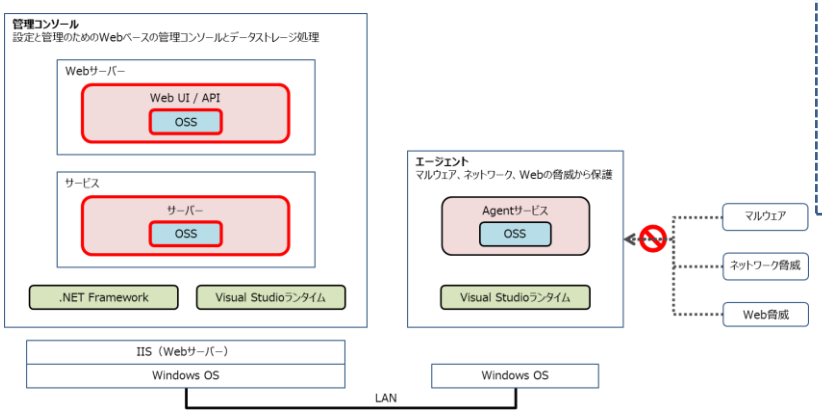
実証概要：対象システム全体構成とSBOM対象範囲

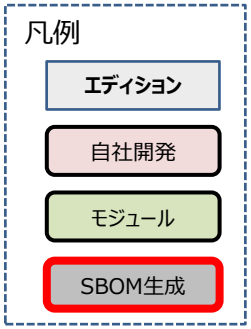
- 2つのソフトウェアを対象として、SBOMの取得、生成を行い、脆弱性管理の対象範囲を設定した。

(1) Linux系OSにおけるSBOMの構成



(2)企業向けエンドポイントセキュリティ製品における SBOMの構成





Linux系OSのインストールメディアは各エディションに必要なモジュールを含み、これらを組み合わせることで複数エディションのインストールに対応

検証対象	入手可能SBOM フォーマット	入手可能ファイル フォーマット	入手先	実証で利用したSBOM
Linux系 OS	SPDX	json	外部サイトから取得	SPDX/json
	CycloneDX	json		
企業向けエンドポイントセキュリティ製品	SPDX	json, tag-value, yaml, rdf	社内SBOMツールにて作成	SPDX/json
	CycloneDX	json		

各エディションに含まれるアプリケーションおよびOSコンポーネントすべてがSBOM該当範囲

実証状況（１）脆弱性マッチング

- 脆弱性マッチング手法区分ごとに整理した項目(1.1)～(1.4)についてフィージビリティを実証。
- APIやWeb UIを用いて、部品ID変換や部分マッチングが可能であることを確認。ただし、現状CPEベースの検索自動化は課題も多い
- 無償ツールの場合、入力SBOMフォーマットの制約があるため、中小企業などの脆弱性マッチングの障壁となる可能性がある。

(1.1) 手法区分	(1.2) 利用可能なSBOMデータ特定・変換 (1.3) 対象とする脆弱性DB (1.4) マッチング手法の選択・自作	成果・課題	補足
API	(1.2) 対象データ： SPDX/json (1.3) 対象DB： JVNiPedia, NVD (1.4) マッチング方法 Splunkを用いて、データ操作やAPI連携を実施 1. SBOMファイルを読み込ませる 2. SBOMファイル内のpURLをCPE2.2またはCPE2.3に変換*1 3. 変換後のCPEを用いてMyJVN, NVDから該当する脆弱性情報を取得	• 部品IDの変換、複数の脆弱性DBの検索など、APIと組合せて柔軟に脆弱性の自動監視可能。 • SBOMはPURLの採用が多く、脆弱性DBはCPEの採用が多いため、変換が必要となるケースが多い • PURL上の部品名とCPEの製品名が一致せず、期待するマッチができない状況も複数確認 • Vendor名に*を入れたCPEの場合、MyJVNで検索がマッチせず • 有償ツール作成のSBOMではpURLがないコンポーネントもあり	pURLからCPEへの変換は以下のように実施 1. OSS*1の利用(CPE2.3利用時のみ) 2. 1で変換ができない場合には、pURLの文字列から再構成するコードを作成（python; CPE2.2/2.3）。変換に使えるデータがない場合は*を使用
既存ツール	**無償ツール** (1.2) 対象データ： SWIDtag/xml (1.3) 対象DB： JVNiPedia (1.4) マッチング方法 無償ツールを利用 1. 説明書をもとに、SWID形式のSBOMファイルをサンプルとして作成（CPEを情報として含む） 2. インポート機能を用いて読み込み 3. JVNiPediaに登録されている情報の取得	• APIを用いたコーディングなしにバッチ等による脆弱性監視可能 • マッチングができることは確認できたが、以下の理由により、現状中小企業での脆弱性対応に適用することは難しいケースが想定される。 1. 無償ツールの入力フォーマットのSWIDを提供する例が少ないため、データ変換が求められる。 2. 中小企業ではITに詳しくない社員がシステム管理を実施していることが多く、脆弱性という概念の理解そのものが難しい場合もある	—
	有償ツール (1.2) 対象データ： SPDX/json (1.3) 対象DB： NVD+KEVC, 有償ツールの独自データベース * ツール側で処理されるため、ユーザ側の作業は不要 (1.4) マッチング方法 1. webコンソール上からSBOMインポート機能を用いて読み込み	• 読み込んだSBOMに対して、脆弱性の検出が可能であり、手動での脆弱性DB連携などは不要だった • 同じバージョンの同ツールで生成されたSBOMはインポートできたが、Linux系OSのSBOMや、2022年版の同有償ツールで生成されたSBOMはエラーによりインポートできず	
Web UI	(1.2) 対象データ： SPDX/json (1.3) 対象DB：JVNiPedia, NVD (1.4) マッチング方法 SBOMファイルよりコンポーネント名（およびバージョン）を抽出し、JVNiPediaおよびNVDの脆弱性検索ページにてキーワード検索	• 試行的にAPIに近い動作確認、暫定的な脆弱性動向把握が可能。 • コンポーネント名やバージョン情報との組み合わせなどを用いた検索自体は容易。 • コンポーネントやマッチしたアドバイザリの数が多いと、手間がかかる • 複数DBを確認する場合に、DB間の情報差異を確認するのも時間は必要	—

*1: https://github.com/scanoss/purl2cpe

実証状況（２）脆弱性対応･優先付け(1/2)

- 検出した脆弱性について、脆弱性対応･優先付けの判断ツリーに基づきカテゴリ分類を行った。
- 検出漏れを防止するため、脆弱性マッチの条件を緩和すると、脆弱性件数は385件と増加したため、誤検知の精査が困難となるケースがあることが分かった。
- ベンダーが、ユーザ影響度を判断する場合、情報が少ないため、リスク評価を厳しくするように設定した。

対象ソフト	(2.1)優先付け情報の選択･取得	(2.2)優先付けカテゴリ判定	(2.3)総合評価（優先度スコア付加）	成果･課題の考察
企業向けエンドポイントセキュリティ製品	悪用可能性情報：有償SCAツール（KEVCの情報含む） CVSS: NVD + 有償SCAツール	**[1]コンポーネント名＋バージョンで検索した場合** マッチしたユニークな脆弱性数: 10件 付加情報に基づくカテゴリ判定結果 即対応：0件 優先対応：0件 通常対応：2件 対応保留：8件 (開発企業･上位）のケース **[2]コンポーネント名のみ（バージョンは*指定）で検索した場合** マッチしたユニークな脆弱性数：385 誤検知の可能性が高く、件数が多いため定常的な精査が難しい。	（検討予定）	• コンポーネントのみで検索した場合はマッチ数が多いため、カテゴリ判定未着手 • 「ユーザ影響度」についてはソフトウェア企業側では判断が難しいケースが多いことがわかったため、判断方法をチューニング。 • 判断方法のチューニング後については、優先付けはスムーズに行えるようになった。 • インシデントの有無が対応の優先度に大きく影響する
Linux系OS		(脆弱性マッチング結果0のためカテゴリ判定できず。 有償ツールでSBOMを読み込めず、またAPI部分マッチでは、pURLから作成したCPEにマッチする脆弱性が検出されず。)	（検討予定）	• pURLから生成したCPEにマッチする脆弱性がなく、優先付けのプロセスを実施できなかった • ツールでも該当SBOMがインポートできないため、検証不可

実証状況（２）脆弱性対応･優先付け(2/2)

- 検出した脆弱性１０件について、優先付けカテゴリ判定を行った結果は以下の通り。

悪用可能性	悪用効率性	技術的深刻度	ユーザ影響度	対応優先度
高	高	高	高	即対応
			中	即対応
			低	優先
		低	高	即対応
			中	優先
			低	優先
	低	高	高	即対応
			中	優先
			低	保留
		低	高	優先
			中	保留
			低	保留
中	高	高	高	優先
			中	通常保守
			低	保留
		低	高	優先
			中	保留
			低	保留
	低	高	高	優先
			中	通常保守
			低	保留
		低	高	通常保守
			中	保留
			低	保留
低	高	高	高	優先
			中	保留
			低	保留
		低	高	通常保守
			中	保留
			低	保留
	低	高	高	通常保守
			中	保留
			低	保留
		低	高	保留
			中	保留
			低	保留

2件

6件

2件

区分	基本的な対応内容
即対応（immediate）	全てのリソースを集中し、 必要に応じて組織の通常業務を停止して可能な限り迅速に対応を行う
優先保守（out-of-cycle）	通常よりも迅速に行動し、計画外の次の利用可能な機会に、必要に応じて通常業務時間外を含めて緩和策または修復策を実施する
通常保守（scheduled）	定期メンテナンス時に対応する
対応保留（defer）	現時点では対応しない。状況を注視する。

区分	カテゴリ判定結果
即対応	0
優先保守	0
通常保守	2
対応保留	8

実証状況：プレイヤーに応じた脆弱性管理の実施内容の検討整理

- 開発企業とユーザ企業で、脆弱性管理において利用する情報は、開発企業がユーザ企業より多く、ユーザ企業は開発企業（SIer, サプライヤ）からの情報提供に依存するケースがある。
- 開発企業の製品提供範囲、ユーザ企業のサービス提供範囲に応じて、要求される管理レベルに違い想定される。
- 中小企業ではスキル面・システム面の制約から、現実的に実施できることは限られることが想定される。

脆弱性管理プロセス	ソフトウェア開発企業	ユーザ企業
脆弱性特定	SCAツールによる通知や 社内外での脆弱性に関する報告が起点	サプライヤーからの通知やニュースサイトがソース。企業によっては脆弱性スキャナーからの情報もある
脆弱性評価・優先付け	ゼロデイ脆弱性であるか、インシデント報告があるか、CVSSスコアがメイン。 複数の自社製品への影響や、問い合わせ数などビジネス面での影響で優先度を変更することも	社外に接するシステムかどうか、インシデントの有無、実際に自社システムの攻撃に使えるかどうか、CVSSスコアなどから判断。対応速度にはシステム停止に関するビジネス影響も関わる。 中小企業では判断が難しい
情報共有	社内関係者含む顧客向けのコミュニケーションと、脆弱性の報告者（外部からの報告の場合）の観点	事象、リスクや、パッチの有無などの情報。ベンダー直接ではなく、SIerから情報をもらうこともある。 中小企業は大手SIがいないところも多く、かなり人依存
暫定対応	原則は本対応実施。修正に時間がかかる場合には暫定策を提供。機能や脆弱性により暫定策は異なるが、特定機能の無効化などで対応	ベンダー提供の暫定策があれば適用。きわめて重大かつ大きな問題であれば、システム停止を検討する可能性もなくはない
本対応	重要な脆弱性の修正については、外部公開パッチで対応。それ以外の場合にはほかの修正と同時。 個人向け・中小企業向け製品では、インターネット経由の自動更新機能あり	優先度順に対応。 SaaS製品の場合には、ユーザ側では特に実施するアクションはないことがほとんど

１．ソフトウェアの管理手法等に関する海外の動向

２．SBOM実証に関する中間報告

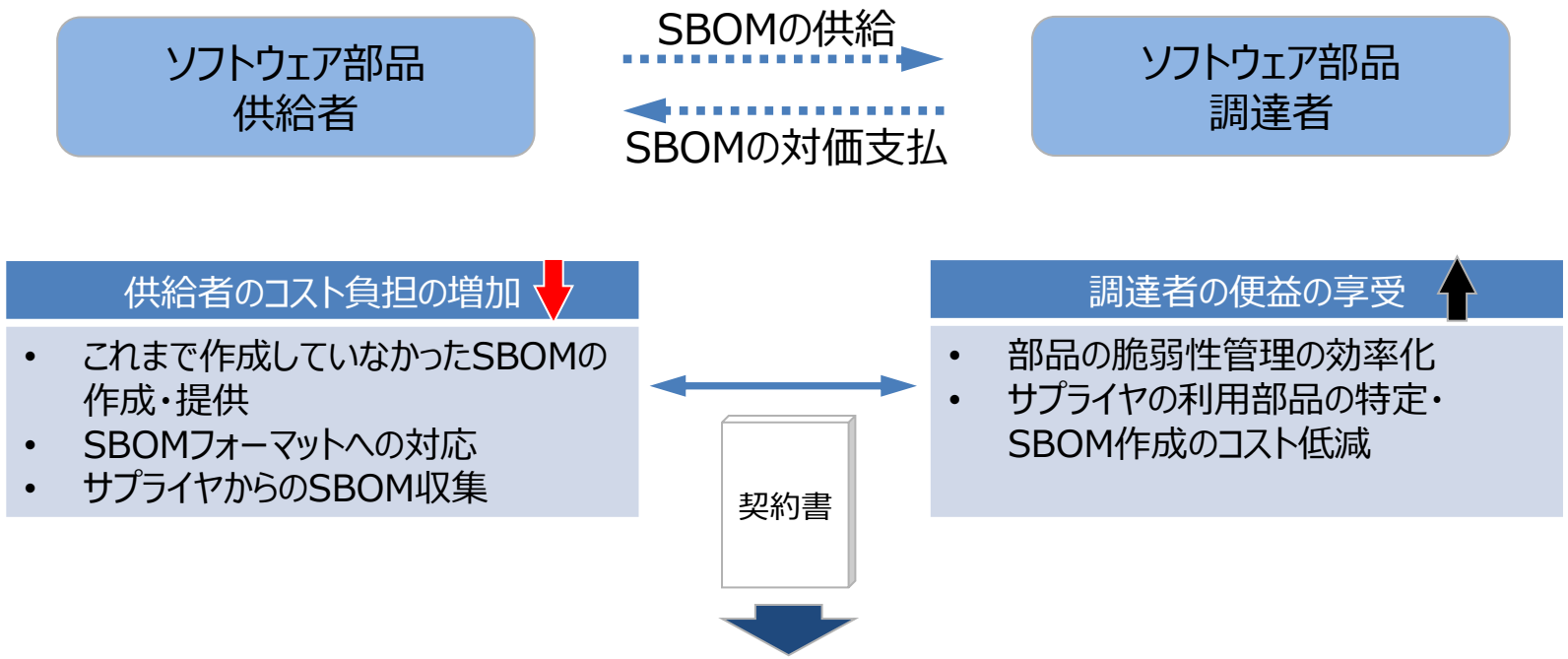
３．SBOM取引モデル概要

４．SBOM事業の成果物を活用した取組みの方向性

SBOM取引モデルの必要性（問題認識）

- ソフトウェア部品の供給者と調達者の立場によって、SBOM作成のコストと脆弱性管理の効率化の便益に偏りが存在する。
- 調達者と供給者の間で、SBOMに関する要求と費用について明確にして、合意を図ることが期待される。
- SBOMの導入手引きの提供だけでなく、取引契約において、SBOMに関する要求を明確化し、それに応じた対価支払を規定することで、SBOMの普及促進の障害を解消する。

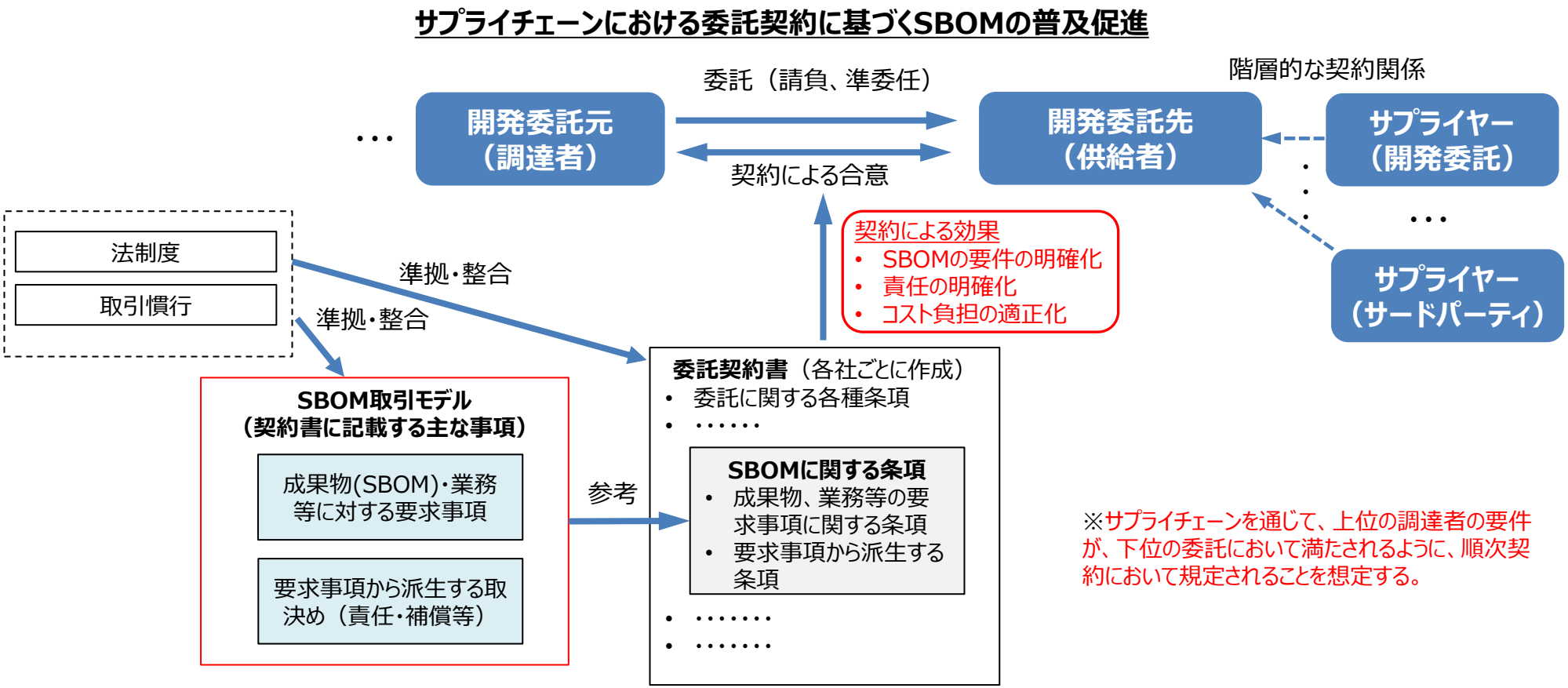
SBOM普及促進の障害
（サプライチェーンにおけるSBOMに係るコストと便益の非対称性）



取引契約書によりSBOMの要求と対価を規定
→ コスト負担と便益享受の非対称性を解消
→ SBOMの普及促進を図る

SBOM取引モデルの考え方

- サプライチェーン全体で最適化を図るため、受発注者間で生じるコストと便益の関係から契約書により取決めを明確化する。
- SBOM取引モデルは、契約を通じてSBOMに関する要求や責任を明確化するための取決めを例示すことで、受発注者間の実施事項とコストと契約レベルで明確にし、SBOMの対応と信頼性を確保するものである。



※サプライチェーンを通じて、上位の調達者の要件が、下位の委託において満たされるように、順次契約において規定されることを想定する。

SBOM導入ガイダンス 付録B: SBOM取引モデルの構成

- 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。

SBOM取引モデル（契約で規定すべき主な事項案）

凡例：基礎 分野共通で最低限期待される事項 / 発展 特定分野、要求レベルの高い分野で期待される事項

契約で規定すべき事項として、SBOMに関する要求事項、責任、コスト負担、権利などの区分で整理される。業界の取引慣行、タスクフォース意見を網羅するように整理。脆弱性管理、ソフトウェア品質保証に重要な要件を言語化。**主に要件定義後の請負契約が対象と想定。**

区分		規定すべき事項	レベル
SBOM要求事項	フォーマット・標準	**（SBOMフォーマット）※1** 採用するSBOM標準フォーマットについて規定する。（SPDX, CycloneDX, SWID等の標準とバージョンを規定）	基礎
		（ID標準）※1 採用する部品ID標準を規定する。（CPE, PURL, SWD, 独自形式等）	基礎
		（SBOM最小要素）※1 採用するSBOMフォーマットの要素項目のうち最小要素を規定する。NTIAのSBOM最小要素を参考にする。	基礎
	品質・信頼性 （SBOM対応モデルに該当）	**（対象サプライヤ契約形態）** SBOM作成範囲として、委託開発契約、サードパーティ利用規約（商用既製品、OSS）の契約形態による範囲を規定する。	基礎
		（再帰的利用部品）※1 SBOM作成範囲として、直接利用部品か再帰的な間接利用部品までとするか規定する。	発展
		（構成解析手法の適用範囲）※1 間接利用部品について、部品を特定する際に利用する構成解析手法の適用範囲を規定する。（依存関係解析、ファイル照合、スニペット解析等）	発展
		（部品精査の要否）※1 ツールによる部品特定の結果に対して、手動による誤検知・検出漏れの精査の要否を規定する。	発展
		（部品の対象フェーズ）※1 部品情報の範囲としてビルド時、ランタイム、クラウドサービス等の範囲を規定する。	発展
		（サードパーティ部品の事前合意） サードパーティ部品（商用部品、OSS）を利用する場合、事前の申告と合意の要否について規定する。	基礎
	保守・運用	**（共有方法）※1** SBOMファイルによる授受またはSaaS等によるリアルタイム共有について規定する。	基礎
		（VEX対応）※1 SBOMに関連する脆弱性情報について悪用可能性に基づくVEX情報の提供を行うか規定する。	発展
		（SBOM更新）※1 ソフトウェアのアップデート、SBOM不具合修正等に応じて、SBOMを更新する期限や頻度を規定する。	基礎
		（脆弱性監視・通知） ソフトウェアの運用フェーズにおいて、脆弱性を監視し、脆弱性が発見された場合に、調達者に通知の期限を規定する。	発展
		（脆弱性対応・優先付け）※1 脆弱性が発見された際に、脆弱性対応の要否、優先付け（トリアージ）について調達者に情報提供を行うか規定する。	発展
		（EOL・EOS） サードパーティ部品および委託開発部品のEOL、EOSやその期限変更に対する通知について規定する。	発展
責任と保証		**（エビデンス提出）** SBOM要求事項について適合していることを証明するエビデンス、第三者証明の提出の要否について規定する。	発展
		（契約不適合責任） SBOM要求事項に対する不適合が見つかった場合には、SBOM修正等の瑕疵対応の要否について規定する。	基礎
		（損害賠償）※2 SBOM要求事項の不適合が原因で事故が発生した場合、損害賠償額上限等について規定する。ライセンス違反の損害賠償を含む。	基礎
		（免責） SBOM要求事項への適合性エビデンスを提出している場合について、技術的制約（ツールの誤検知など）に帰する理由で、損害が発生した場合について損害賠償の制限、免責について規定する。	発展
コスト負担		**（見積）※2** SBOM要求事項、責任・保証に基づき見積の作成し、その合意金額に基づき対価支払について規定する。	基礎
権利・機密保持		**（知的財産権の帰属）** 作成したSBOMの知的財産権、使用権の帰属、第三者への提供可否について規定する。	発展
		（機密保持） SBOMの機密保持・管理およびSBOMを用いたリバースエンジニアリングの禁止について規定する。	発展

※1　発注仕様書に記載することも想定される。
※2　ソフトウェア開発一般の請負契約と共通化することが想定される。

１．ソフトウェアの管理手法等に関する海外の動向

２．SBOM実証に関する中間報告

３．SBOM取引モデル概要

４．SBOM事業の成果物を活用した取組みの方向性

本事業の成果物を活用したSBOM普及促進策案

基本的なアプローチ
- **規制・業法がある分野：**基準・ガイドラインやそれに関連付いた解説文書、講習セミナーなどからSBOM導入手引き・対応モデルが参照されるよう働きかける。SBOM対応モデル案は実証に基づく参考例であり、必要に応じて業界主体で、基準に対応した対応レベルのコンセンサスを形成する。
- **規制等がない分野：**業界団体やIPAなど分野横断的な取組み機関と連携し、SBOM導入手引き・対応モデル等の活用を推奨する。

各分野のステークホルダーとの連携を通じたSBOM普及促進

リスク区分※		分野等	規制・制度等	社会実装アプローチ（方針案） ステークホルダーとの連携等
規制・業法あり				
I	人命に影響	医療機器	薬機法，基本要件基準，JIS規格，手引書	基準・ガイドラインに関連付いた業界の解説文書、業界セミナーなどでSBOMガイダンスの参照・推奨を受けデファクト化を推進。(規制当局・認証機関におけるSBOMガイダンスの活用促進)
		自動車	保安基準、告示、協定規則	業界団体と連携し、会員向けにSBOM手引き、対応モデルの活用・推奨など働きかけを依頼。
		人命に係る重要インフラ（ガス等）	有り（一部自主規制）	—
II	社会・経済への波及的影響が大きい（重要インフラ）	電力等（重要インフラ）	有り（業法、自主規制）	関係省庁と連携を行う
		政府・行政	政府調達基準	関係省庁と連携を行う
		通信機器	技適・認証等	関係省庁と連携を行う
		重要ソフトウェア(OS,NW機器上のソフトウェア等)	任意、CC等	関係省庁と連携を行う
規制等なし				
III	社会・経済への影響が限定的 (波及範囲が狭い)	波及的影響が限定的なインフラ（B2B EC等）	自主規制等	関係団体と連携し、SBOM活用の方策についての検討を行う。
		セキュリティソフト	任意、CC等	関係団体と連携し、関連業界の普及を促進する。
IV	影響が個人・個社に限定	パッケージソフト、業務ソフト、SaaS	任意・認証等	業界団体と連携し、会員企業へのSBOM手引き・対応モデルの推奨、活用の働きかけを図る。
		コンシューマIoT機器	任意・ラベリング	既存制度の中でSBOMを促進すべく検討を行う

※高信頼化ソフトウェアのための開発手法ガイドブック(IPA)におけるリスク分類に基づき設定

QUAD/SSDFへの整合化と本事業SBOM成果物の活用策（案）（1/2）

- QUADのセキュリア開発への政府ポリシー対応は、４つのプラクティス概要のみが示されており、具体化が期待される。
- ソフトウェアの保護、安全なソフトウェア開発、脆弱性への対応のうち、SBOMに係わる部分については、本事業SBOM成果物（SBOM手引き、対応モデル等）を活用し、具体策を示すことが期待される。
- 国際整合の観点で、政府間の定期的な対話が期待される。

セキュアソフトウェア開発フレームワーク（SSDF）への対応におけるSBOM事業の成果の活用策

QUADの言及範囲

プラクティス分類	SSDF実装例（National Implementation Examples） 各国の裁量に委ねられるか
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）

施策 SBOM事業の成果をベースに対応できる項目の具体化

施策 SBOM脆弱性管理の実証結果をもとに運用フェーズの具体化

- 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

QUAD/SSDFとの整合化と本事業SBOM成果物の活用策（案）(2/2)

QUADで要求されるSSDFのうち、プロセス・手法の例示と参考文献については、各国の検討が必要に応じて求められる。手法・プロセスの例示と参考文献のうちSBOMや脆弱性管理に係るものについて、本事業の成果物（SBOM手引き、対応モデル、事例集等）を対応づけることで、日本企業にとっての負担を解消するとともに、SBOMの普及促進を図る。

SSDFにおける各プラクティスの構成と日本におけるカスタマイズ取組の方向性

プラクティス(実践項目) Practices	タスク(要件) Tasks	米国の実装例（手法・プロセス等） Notional Implementation Examples	参考文献 References
Provide a Mechanism for Verifying Software Release Integrity (PS.2): Help software acquirers ensure that the software they acquire is legitimate and has not been tampered with.	**PS.2.1**: Make software integrity verification information available to software acquirers.	**Example 1**: Post cryptographic hashes for release files on a well-secured website. **Example 2**: Use an established certificate authority for code signing so that consumers' operating systems or other tools and services can confirm the validity of signatures before use. **Example 3**: Periodically review the code signing processes, including certificate renewal, rotation, revocation, and protection.	**BSAFSS**: SM.4, SM.5, SM.6 **BSIMM**: SE2.4 **CNCFSSCP**: Securing Deployments—Verification **EO14028**: 4e(iii), 4e(ix), 4e(x) **IEC62443**: SM-6, SM-8, SUM-4 **NISTCSF**: PR.DS-6 **NISTLABEL**: 2.2.2.4 **OWASPSAMM**: OE3-B **OWASPSCVS**: 4 **PCISSLC**: 6.1, 6.2 **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-8 **SP800161**: SA-8 **SP800181**: K0178
Archive and Protect Each Software Release (PS.3): Preserve software releases in order to help identify, analyze, and eliminate vulnerabilities discovered in the software after release.	**PS.3.1**: Securely archive the necessary files and supporting data (e.g., integrity verification information, provenance data) to be retained for each software release.	**Example 1**: Store the release files, associated images, etc. in repositories following the organization's established policy. Allow read-only access to them by necessary personnel and no access by anyone else. **Example 2**: Store and protect release integrity verification information and provenance data, such as by keeping it in a separate location from the release files or by signing the data.	**BSAFSS**: PD.1-5, DE.1-2, IA.2 **CNCFSSCP**: Securing Artefacts—Automation, Controlled Environments, Encryption; Securing Deployments—Verification **EO14028**: 4e(iii), 4e(vi), 4e(ix), 4e(x) **IDASOAR**: 25 **IEC62443**: SM-6, SM-7 **NISTCSF**: PR.IP-4 **OWASPSCVS**: 1, 3.18, 3.19, 6.3 **PCISSLC**: 5.2, 6.1, 6.2 **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-10, SA-15, SA-15(11), SR-4 **SP800161**: SA-8, SA-10, SA-15(11), SR-4
	PS.3.2: Collect, safeguard, maintain, and share provenance data for all components of each software release (e.g., in a software bill of materials [SBOM]).	**Example 1**: Make the provenance data available to software acquirers in accordance with the organization's policies, preferably using standards-based formats. **Example 2**: Make the provenance data available to the organization's operations and response teams to aid them in mitigating software vulnerabilities. **Example 3**: Protect the integrity of provenance data, and provide a way for recipients to verify provenance data integrity. **Example 4**: Update the provenance data every time any of the software's components are updated.	**BSAFSS**: SM.2 **BSIMM**: SE3.6 **CNCFSSCP**: Securing Materials—Verification, Automation **EO14028**: 4e(vi), 4e(vii), 4e(ix), 4e(x) **NTIASBOM**: All **OWASPSCVS**: 1.4, 2 **SCSIC**: Vendor Software Delivery Integrity Controls **SCTPC**: MAINTAIN3 **SP80053**: SA-8, SR-3, SR-4 **SP800161**: SA-8, SR-3, SR-4

QUAD内で共通項目として期待されると想定

米国における例示。必要に応じて各国の検討が求められる。

タスクに対する確立された手法の文献例。必要に応じて各国の検討が求められる。

- SBOMについては、PW4.1に部品のリスク評価のためSBOM等を取得すると抽象的に書かれている。
- 脆弱性対応についてプラクティスは3件、タスクは9件

SBOM手引き、対応モデル等をもとにプロセス・手法のカスタマイズ、具体化

SBOM手引き、対応モデル等で代替できるものを例示し、日本企業の対応の負担を軽減する。

討議いただきたい事項について

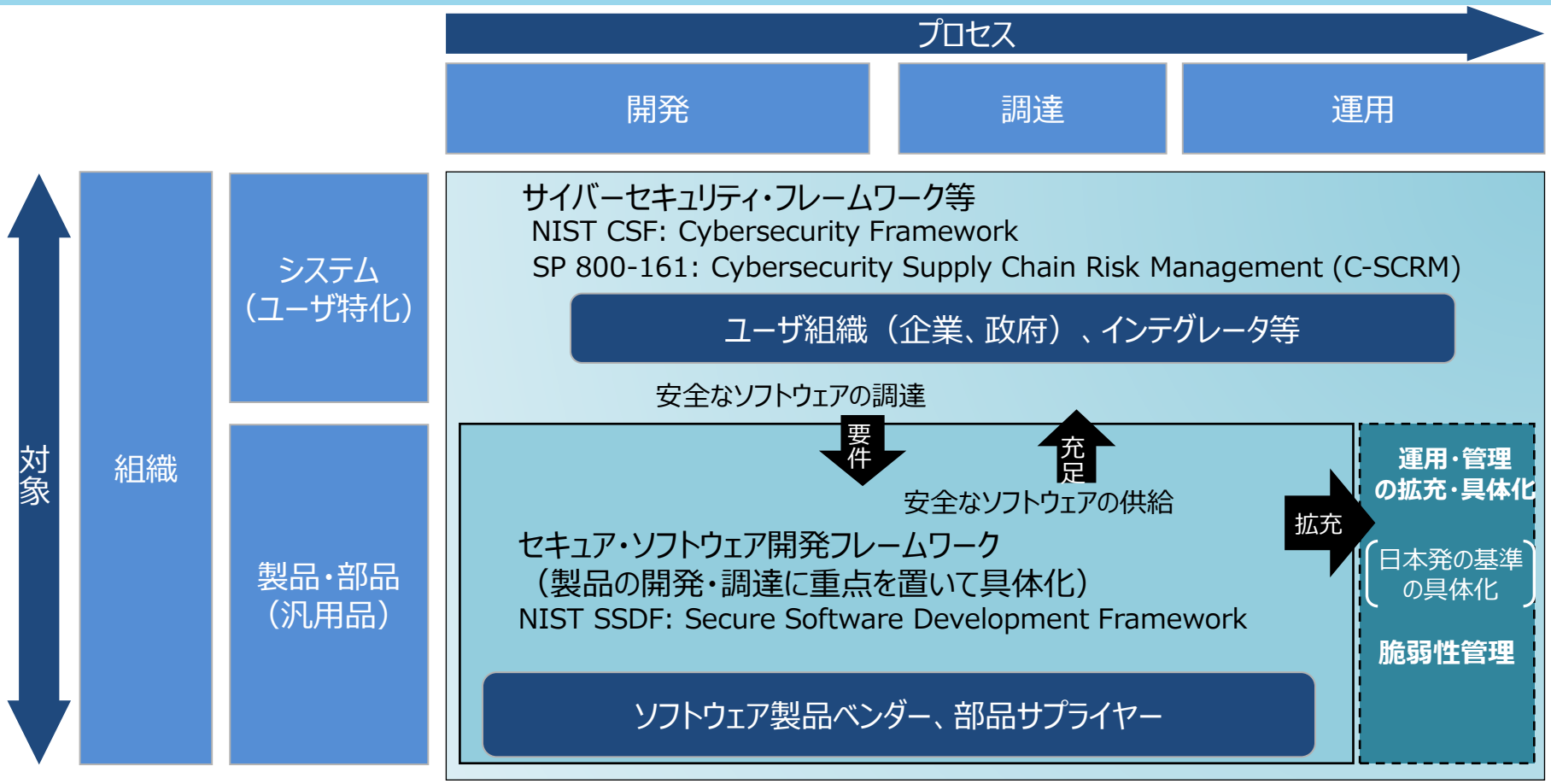
① SBOM実証の今後の方向性について

② SBOM取引モデルと成果物の活用の今後の方向性

参考

セキュア・ソフトウェア管理手法に関する取組みの整理と期待

- SSDFは、包括的なサイバーセキュリティフレームワークに対して、システムではなく製品を対象とし、開発・調達フェーズについて具体化した開発者向けの基準であり、大統領令に基づき政府調達基準として義務化される。
- ソフトウェアの安全な利活用においては、開発・調達フェーズのみならず、脆弱性管理等の運用フェーズの重要性が高まっていることから、今後、SSDFを運用フェーズにも重点を置いたフレームワークの拡張と具体化が期待される。
- QUADの４か国共同原則においては、SSDFの４つのプラクティスに該当する項目について、各国ごとの実装が求められる。
- SSDFは、米国主体のガイダンス等を例に整理しているが、国際整合を図りつつ、日本企業の実装を促進するため、本事業におけるSBOM導入手引きや脆弱性管理手法の実証成果を活用した実装方法のガイダンスを示すことが期待される。



【参考】包括的なセキュリティ基準等の俯瞰的な比較とNIST SSDFの位置付け

- 包括的なセキュリティ基準・ガイダンスの位置付けを俯瞰的にとらえるため、プロセス、対象、組織など主なスコープについて重視する領域を比較した。
- NIST CSFなど包括的なサイバーセキュリティフレームワークはセキュリティ全般をスコープとしつつ、インフラ事業者等のユーザ事業者・インテグレータを想定し、システムの構築・運用フェーズに重点を置いた基準を示している。
- 一方、NIST SSDFは、多数の利用者から調達される「ソフトウェア製品」を対象とし、開発・流通フェーズに重点を置いて開発者向けに具体化した基準であり、政府調達の義務的な基準として策定されたことが特徴である。

			プロセス			対象			区分		要求強度		対象組織			分野					
国	作成主体	基準・文書名	開発	流通・調達	運用	組織	システム	製品	基準・標準	ガイダンス	義務	推奨	最終ベンダー	サプライヤ	ユーザ	汎用	制御系	情報系	政府	自動車	医療機器
米国	NIST	SSDF: SP 800-218 Secure Software Development	●	●	△	●		●	●		●		●	●		●			●		
米国	NIST	SP 800-161: Cybersecurity Supply Chain Risk Mana		●	●	●	●		●			●		●	●	●			●		
米国	CISA, NSA	Securing Software Supply Chain Series – Recomme	●			●		●		●		●	●			●					
米国	CISA, NSA	Securing Software Supply Chain Series – Recomme		●		●		●		●		●		●		●					
米国	CISA, NSA	Securing Software Supply Chain Series – Recomme			●	●		●		●		●			●	●					
米国	NIST	Security Measures for EO-Critical Software Use			●	●		●		●		●			●				●		
米国	NIST	Recommended Minimum Standards for Vendor or D	●					●	●			●	●			●					
米国	NIST	Software Supply Chain Security Guidance Under Ex		●	●	●		●		●		●			●				●		
米国	NTIA	Software Suppliers Playbook: SBOM Production and	●	●				●		●		●	●	●		●					
米国	NTIA	Software Consumers Playbook: SBOM Acquisition,			●	●		●		●		●			●	●					
国際	ISO	ISO/SAE 21434	●	●	●	●		●	●		●		●	●						●	
国際	IMDRF	IMDRF Code IMDRF/CYBER WG/N73 Principles an	●		●	●				●		●	●	●	●						●
国際	IMDRF	IMDRF Code IMDRF/CYBER WG/N60 Principles an	●		●	●				●		●	●	●	●						●
米国	NIST	CSF:Cybersecurity Framework	●		●	●	●		●			●	●	●		●					
国際	IEC	IEC 62443	●	●	●	●	●	●	●			●	●	●	●	●	●				
国際	ISO/IEC	ISO/IEC 27000 Series	●	△	●	●	●		●			●	●	●	●	●					
米国	NIST	SP 800-53 Security and Privacy Controls for Infor	●		●	●	●		●		△	●	●			●		●	●		
米国	NIST	SP 800-171 Rev. 3 (Draft) Protecting Controlled U	●	●	●	●	●		●		△	●	●	●		●			●		