公開版

5分で分かる
経済産業省の

サイバー攻撃への備えを！「SBOM」（ソフトウェア部品構成表）を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引（案）を公表します

「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver2.0(案)」の意見公募を開始します

総関西サイバーセキュリティLT大会（第41回） LT

2024-05-15

hogehuga
脆弱性対応勉強会

TLP:CLEAR

公開版

もう少し、掲示しやすい
タイトルにしておくれ…

5分で分かる
経済産業省の

サイバー攻撃への備えを！「SBOM」（ソフトウェア部品構成表）を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引（案）を公表します

「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver2.0(案)」の意見公募を開始します

総関西サイバーセキュリティLT大会（第41回） LT

LT発表時間は限られるので、
30秒位でスライドが自動で進みます。

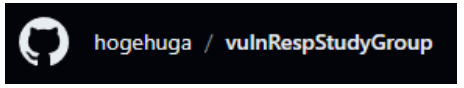
2024-05-15
hogehuga
脆弱性対応勉強会

TLP:CLEAR

whoami

脆弱性
対応
勉強会

- hogehuga
  - 所属
    - 個人主催の勉強会「脆弱性対応勉強会」主催
  - 活動履歴等
    - (脆弱性対応勉強会 | サイバーセキュリティ勉強会in塩尻) 運営
    - (Internet Week 2023 | NCA Annual Conference 2023) Speaker
    - OWASP Nagoya Chapterミーティング第33回 /OWASP 758 Day Speaker
    - InternetWeek Showcase福岡（07/25-26）登壇予定
    - 他
  - その他
    - バイク移動が趣味（今日もバイク移動）
    - 水風呂が大好き（冷泉をご存じの方は教えてください）
    - 脆弱性管理についてしゃべる、脆弱性漫談師

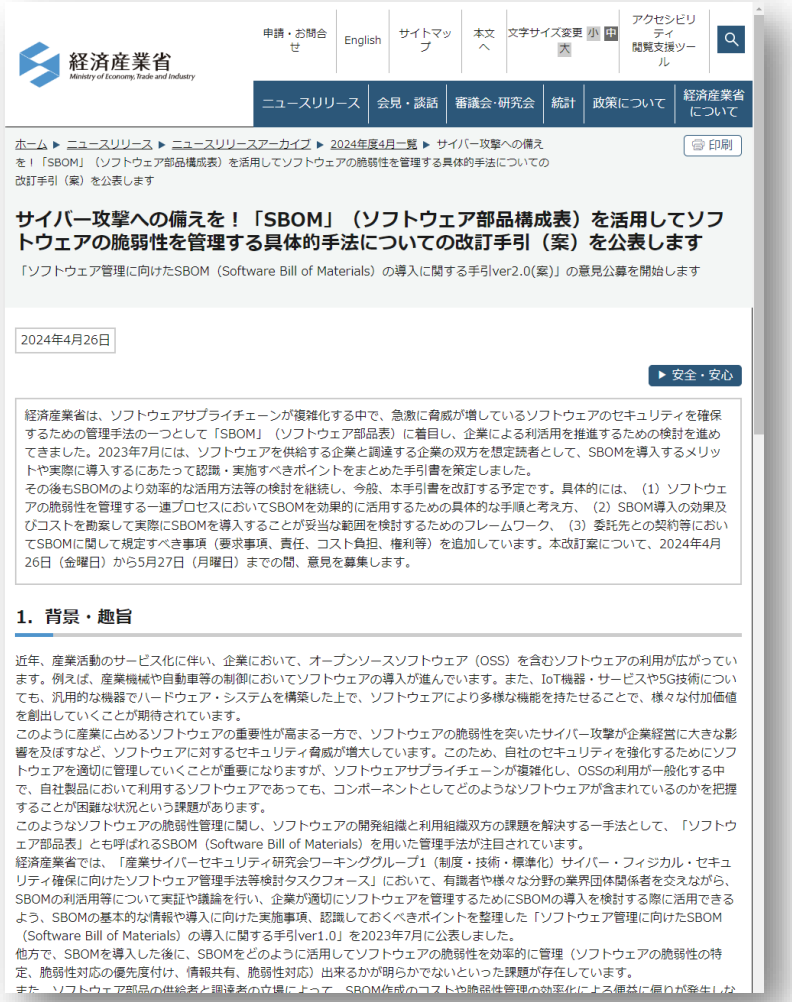


TLP:CLEAR

はじめに

経済産業省から、「SBOMを導入するメリットや実際に導入するにあたって認識・実施すべきポイントをまとめた手引書」が策定されました。本件について2024-04-26から2024-05-27までの間に意見募集（所謂パブリックコメント）がされています。

- https://www.meti.go.jp/press/2024/04/20240426001/20240426001.html



本LT5分間で、おおよその内容を把握できるような話をします。

- 本イベント後もパブリックコメントの期間内なので、興味のある方は、読んでコメントを出していただけると良さそうです。
- 私は所謂「SBOMの専門家」ではないため、脆弱性管理の研究者及び複数のセキュリティベンダの人と話した結果得られた知見でお話しします。
- 本LTの内容は私（hogehuga）の個人的な意見であり、現職の意見とは異なる場合があります。

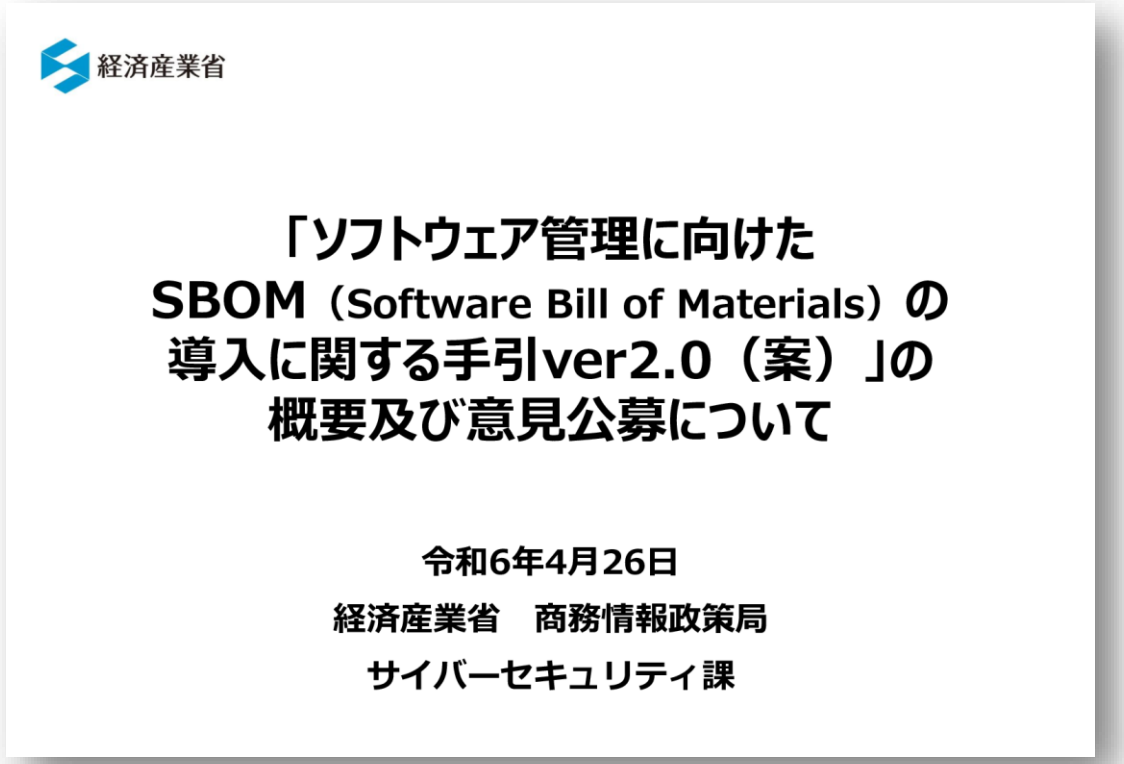
今回の目的

- SBOMについて“なんとなく”（興味を持ってもらう|次のアクション）がわかる
- （可能なら）読んでパブリックコメントを出してほしい

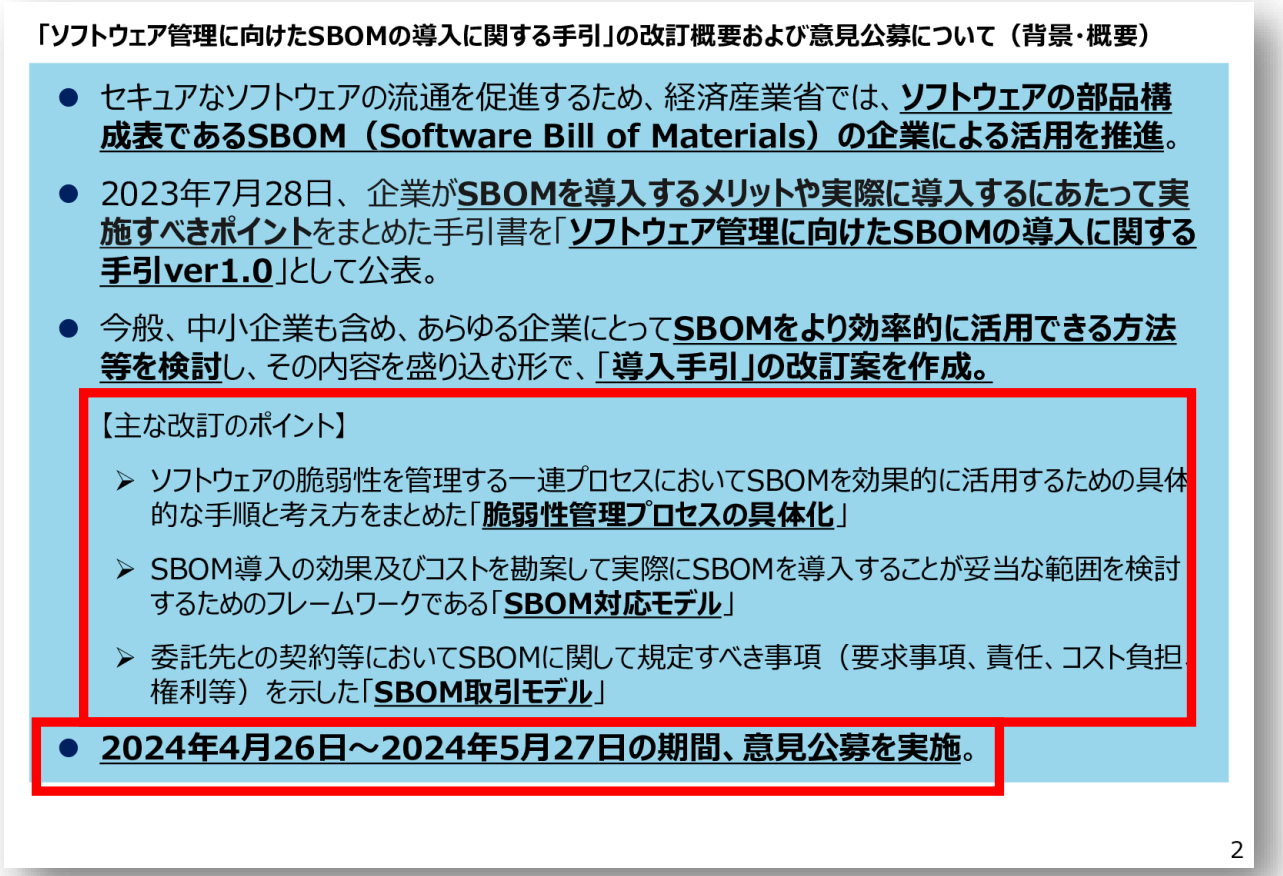
TLP:CLEAR

経済産業省の資料を読み解く

本資料は162ページあるので、今回は「概要資料」（16ページ）でのご紹介をします。



- 「導入に関する手引き」といいながら、「どのように活用するのか」に注視した資料となっている。
  - 脆弱性管理に使え
  - 委託先との契約をどうすべきか
- 対象読者
  - ソフトウェアサプライヤーにおける開発・設計部門
  - PSIRT等のソフトウェアセキュリティに関わる部門
  - 経営層



「ソフトウェア管理に向けたSBOMの導入に関する手引」の改訂概要および意見公募について（背景・概要）

- セキュアなソフトウェアの流通を促進するため、経済産業省では、**ソフトウェアの部品構成表であるSBOM（Software Bill of Materials）の企業による活用を推進**。
- 2023年7月28日、企業が**SBOMを導入するメリットや実際に導入するにあたって実施すべきポイント**をまとめた手引書を「**ソフトウェア管理に向けたSBOMの導入に関する手引ver1.0**」として公表。
- 今般、中小企業も含め、あらゆる企業にとって**SBOMをより効率的に活用できる方法等を検討**し、その内容を盛り込む形で、「**導入手引**」の改訂案を作成。

【主な改訂のポイント】

- ソフトウェアの脆弱性を管理する一連プロセスにおいてSBOMを効果的に活用するための具体的な手順と考え方をまとめた「**脆弱性管理プロセスの具体化**」
- SBOM導入の効果及びコストを勘案して実際にSBOMを導入することが妥当な範囲を検討するためのフレームワークである「**SBOM対応モデル**」
- 委託先との契約等においてSBOMに関して規定すべき事項（要求事項、責任、コスト負担、権利等）を示した「**SBOM取引モデル**」

- **2024年4月26日～2024年5月27日の期間、意見公募を実施**。

2

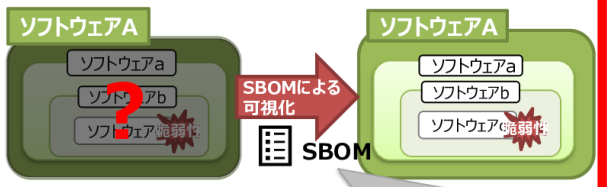
- 改訂ポイント
  - 脆弱性管理プロセスの具体化
  - 導入範囲検討のフレームワーク
  - 委託先との契約にかかるモデル

SBOMそれ自体を作るというより、より踏み込んだ、どのように活用するかに重点を置いているように見える。

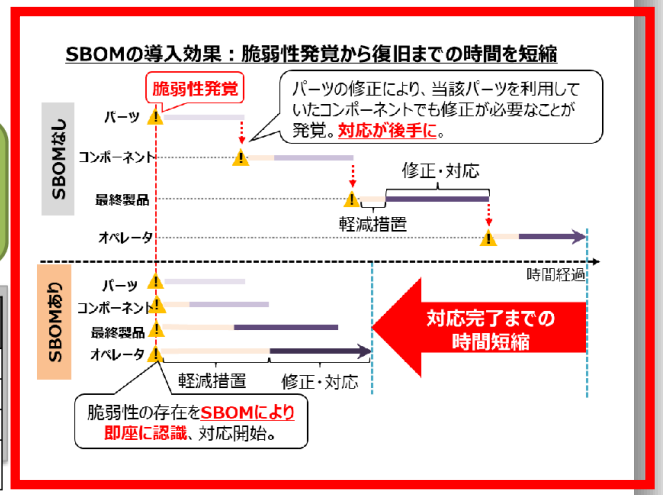
ソフトウェア・セキュリティ確保手段としてのSBOM

- SBOM （Software Bill of Materials）とは、**ソフトウェアの部品構成表**のこと。ソフトウェアを構成する**各部品（コンポーネント）を誰が作り、何が含まれ、どのような構成となっているか**等を示す。
- SBOMによりソフトウェアの構成情報を詳細に把握することができるため、脆弱性情報の即時の特定が可能であり、**脆弱性対応などへの活用が期待**できる一方、その作成効果やコストなどの課題が存在するため、実証による検証を実施。
- 2023年7月、**「ソフトウェア管理に向けたSBOMの導入手引ver1.0」を公表**。SBOMに関する基本的な情報や導入に向けた実施事項のポイントを示す。

<SBOMイメージ>



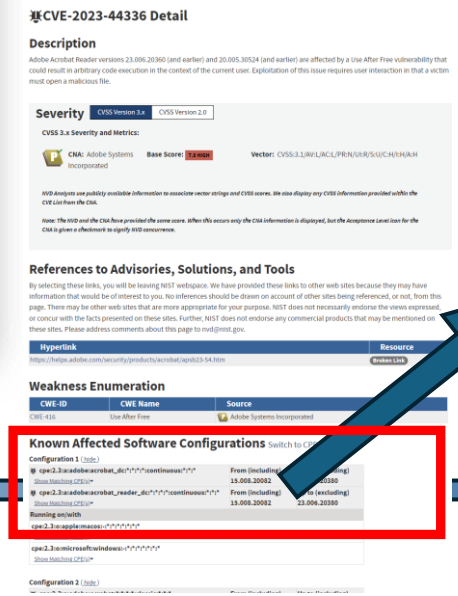
サプライヤ名	コンポーネント名	バージョン	製品URLなど	…
A会社	ソフトウェアA	Ver1.0	……	…
A会社	|…ソフトウェアa	Ver2.1	……	…
B会社	|…ソフトウェアb	Ver5.3	……	…
C会社	|…ソフトウェアc	Ver1.2	……	…

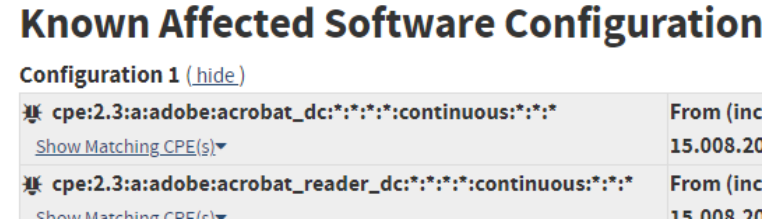


3

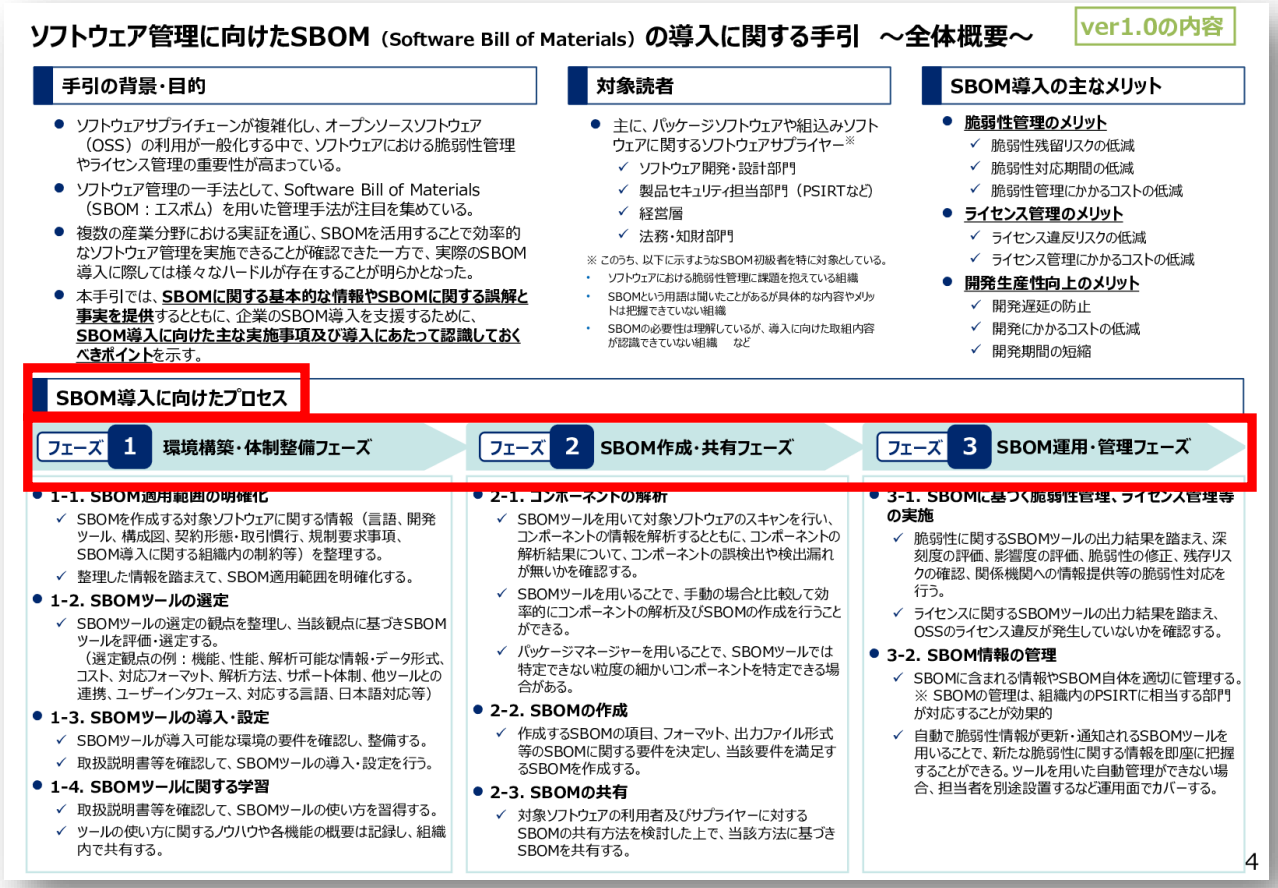
- SBOMとは、ソフトウェアの部品表
  - 故に、何を使っているかが判明するため、脆弱性管理で活用が期待できる

具体的には、利用ソフトウェアをCPE/PURL形式で記載し手置くことで、NVDの脆弱性情報データベースとマッチングさせることを期待している





TLP:CLEAR



ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引　～全体概要～

ver1.0の内容

手引の背景・目的

- ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が一般化する中で、ソフトウェアにおける脆弱性管理やライセンス管理の重要性が高まっている。
- ソフトウェア管理の一手法として、Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目を集めている。
- 複数の産業分野における実証を通じ、SBOMを活用することで効率的なソフトウェア管理を実施できることが確認できた一方で、実際のSBOM導入に際しては様々なハードルが存在することが明らかとなった。
- 本手引では、**SBOMに関する基本的な情報やSBOMに関する誤解と事実を提供**するとともに、企業のSBOM導入を支援するために、**SBOM導入に向けた主な実施事項及び導入にあたって認識しておくべきポイント**を示す。

対象読者

- 主に、パッケージソフトウェアや組込みソフトウェアに関するソフトウェアサプライヤー※
  - ✓ ソフトウェア開発・設計部門
  - ✓ 製品セキュリティ担当部門（PSIRTなど）
  - ✓ 経営層
  - ✓ 法務・知財部門

※ このうち、以下に示すようなSBOM初級者を特に対象としている。
- ソフトウェアにおける脆弱性管理に課題を抱えている組織
- SBOMという用語は聞いたことがあるが具体的な内容やメリットは把握できていない組織
- SBOMの必要性は理解しているが、導入に向けた取組内容が認識できていない組織　など

SBOM導入の主なメリット

- **脆弱性管理のメリット**
  - ✓ 脆弱性残留リスクの低減
  - ✓ 脆弱性対応期間の低減
  - ✓ 脆弱性管理にかかるコストの低減
- **ライセンス管理のメリット**
  - ✓ ライセンス違反リスクの低減
  - ✓ ライセンス管理にかかるコストの低減
- **開発生産性向上のメリット**
  - ✓ 開発遅延の防止
  - ✓ 開発にかかるコストの低減
  - ✓ 開発期間の短縮

SBOM導入に向けたプロセス

フェーズ1 環境構築・体制整備フェーズ

- **1-1. SBOM適用範囲の明確化**
  - ✓ SBOMを作成する対象ソフトウェアに関する情報（言語、開発ツール、構成図、契約形態・取引慣行、規制要求事項、SBOM導入に関する組織内の制約等）を整理する。
  - ✓ 整理した情報を踏まえて、SBOM適用範囲を明確化する。
- **1-2. SBOMツールの選定**
  - ✓ SBOMツールの選定の観点を整理し、当該観点に基づきSBOMツールを評価・選定する。（選定観点の例：機能、性能、解析可能な情報・データ形式、コスト、対応フォーマット、解析方法、サポート体制、他ツールとの連携、ユーザーインタフェース、対応する言語、日本語対応等）
- **1-3. SBOMツールの導入・設定**
  - ✓ SBOMツールが導入可能な環境の要件を確認し、整備する。
  - ✓ 取扱説明書等を確認して、SBOMツールの導入・設定を行う。
- **1-4. SBOMツールに関する学習**
  - ✓ 取扱説明書等を確認して、SBOMツールの使い方を習得する。
  - ✓ ツールの使い方に関するノウハウや各機能の概要は記録し、組織内で共有する。

フェーズ2 SBOM作成・共有フェーズ

- **2-1. コンポーネントの解析**
  - ✓ SBOMツールを用いて対象ソフトウェアのスキャンを行い、コンポーネントの情報を解析するとともに、コンポーネントの解析結果について、コンポーネントの誤検出や検出漏れが無いかを確認する。
  - ✓ SBOMツールを用いることで、手動の場合と比較して効率的にコンポーネントの解析及びSBOMの作成を行うことができる。
  - ✓ パッケージマネージャーを用いることで、SBOMツールでは特定できない粒度の細かいコンポーネントを特定できる場合がある。
- **2-2. SBOMの作成**
  - ✓ 作成するSBOMの項目、フォーマット、出力ファイル形式等のSBOMに関する要件を決定し、当該要件を満足するSBOMを作成する。
- **2-3. SBOMの共有**
  - ✓ 対象ソフトウェアの利用者及びサプライヤーに対するSBOMの共有方法を検討した上で、当該方法に基づきSBOMを共有する。

フェーズ3 SBOM運用・管理フェーズ

- **3-1. SBOMに基づく脆弱性管理、ライセンス管理等の実施**
  - ✓ 脆弱性に関するSBOMツールの出力結果を踏まえ、深刻度の評価、影響度の評価、脆弱性の修正、残存リスクの確認、関係機関への情報提供等の脆弱性対応を行う。
  - ✓ ライセンスに関するSBOMツールの出力結果を踏まえ、OSSのライセンス違反が発生していないかを確認する。
- **3-2. SBOM情報の管理**
  - ✓ SBOMに含まれる情報やSBOM自体を適切に管理する。※ SBOMの管理は、組織内のPSIRTに相当する部門が対応することが効果的
  - ✓ 自動で脆弱性情報が更新・通知されるSBOMツールを用いることで、新たな脆弱性に関する情報を即座に把握することができる。ツールを用いた自動管理ができない場合、担当者を別途設置するなど運用面でカバーする。

4

- SBOM導入に関した概観の提示
  - 環境構築・体制整備フェーズ
  - SBOM作成・共有フェーズ
  - SBOM運用・管理フェーズ

作るだけではだめで、運用が必要なことを明確化している。

改訂では次頁のように詳細化している。

ver2.0追加内容

脆弱性管理プロセスの具体化

背景・目的

- SBOMを活用した脆弱性管理の方法と手順についてプロセスに基づく具体例を示す。
- SBOMを活用した脆弱性管理においては、**現状では未解決の課題**が存在し、それらの課題を十分に解決するためには、新たな**技術開発、標準化、ツール環境整備**などが必要になる。
- 本章では、それらの課題も含めて、SBOM利用者側の運用によって課題を回避するための考え方や現状で可能なベストプラクティスについて示す。

主な課題と解決アプローチ・ノウハウ等

課題	解決アプローチ・ノウハウ
部品IDが併存し、脆弱性DBとの突合に障害	Purl2cpeなどID変換ツールの利用やAPIを用いたID部分照合
多様な脆弱性DBの網羅性の確保	リスクとコストの低減効果に基づく脆弱性DBの選択方法の提示
脆弱性対応の優先付けによる迅速対応と効率化	SSVCをベースとした判断ツリーによる優先付けカテゴリ判定法の提示
サプライチェーンを通じた情報共有と役割分担	情報共有のステップと開発者・ユーザによる実施項目の提示
脆弱性対応の役割分担	暫定対応・本格対応における開発者・ユーザによる実施項目の提示

SBOMを活用した脆弱性管理プロセス（概要）

フェーズ1 脆弱性特定

1. **マッチング手法区分の選択**
   組織の目的、技術力、利用環境に応じて、SBOM既成ツール、APIスクリプト利用、WebUIの３手法から選択する。
2. **利用可能なSBOMデータの特定**
   サプライヤーからのSBOM提供、ツールを用いたSBOM作成など、利用可能なSBOMデータを特定する。
3. **脆弱性DBの選択**
   脆弱性情報のカバレッジ拡大、自動化・効率化、優先付けの精度向上など、リスク低減、コスト低減などの目的に応じて重要度の高いDBを選択する。
4. **マッチング手法の選択・作成**
   以上の選択肢を総合して、脆弱性特定手法を決定する。

フェーズ2 脆弱性対応優先付け

1. **予備的フィルタリング**
   外部情報を活用した優先付けの前に、既知の情報から対応が必要な脆弱性情報を絞り込む。
2. **優先付け情報の選択・取得**
   リスクの構成要素に基づき、インシデントの有無、Exploitコードの流通状況、CVSS、VEX情報など自社のポリシーに従い必要な情報を選択・取得する。
3. **判断ツリーに基づくカテゴリ判定**
   SSVCに基づき整理した判断ツリーに従い、（開発者、ユーザ組織）×（技術力の高・低）応じて優先付けカテゴリ判定を行う。
4. **優先度スコア評価**
   1から３のステップと並行して、必要に応じて、必要に応じて定量的なスコアリングによりカテゴリ内の優先付けを行うことで詳細な優先付けを行う。

フェーズ3 情報共有

1. **共有情報と共有相手の特定**
   ・共有情報の特定：脆弱性情報、負荷情報、優先付け判定結果など共有情報を特定する。
   ・共有相手の特定：社会組織、社外（ユーザ、ベンダー、サプライヤー）などの共有相手、順序を特定する。
   ・共有認知・トリガー：プッシュ型、プル型など共有のトリガーを特定する。
2. **共有方法の特定と実施**
   ・共有方法の特定：ファイル送受信、SaaSなど共有方法を特定。
   ・アクセス権限の特定：機密性に応じて、非公開、開示範囲、権限などを特定。
   ・共有実施：決定した共有方法、アクセス権限に基づき共有を行う。

フェーズ4 脆弱性対応

1. **脆弱性暫定対応**
   ・暫定策の検討：利用中断、縮退、回避策など暫定策の検討
   ・暫定策の適用：決定した暫定策について、ステークホルダーに周知し適用する。
2. **脆弱性根本対応**
   ・根本対応の実施：脆弱性に関わるソフトウェアの開発者を特定し、開発者が脆弱性を修正する
   ・SBOM/VEX更新：脆弱性修正に伴い、SBOM、VEX情報を更新する。
   ・SBOM/VEXの共有：供給先に更新したSBOM/VEXを提供し、必要に応じてSBOM履歴管理を行う。

5

- プロセスの具体化
  - 委託先等との共有の具体化
  - 運用管理としての脆弱性対応

SBOMで脆弱性対応をさせることについて、手段や対応が明確に示された。

サプライチェーンでのSBOM共有についても明確に示された。

- あくまで経済産業省が想定しているモデルでの話であることに注意が必要

ver2.0追加内容

SBOM対応モデルの概要

SBOM対応モデルの構成要素

- SBOMの作成・活用に関する選択肢について、コストと効果への影響の大きい項目について5W1Hを網羅するように体系化。実証および有識者委員会の意見を反映してSBOM対応項目を整理。
- 実証を通じて、医療機器、自動車、ソフトウェア製品等の分野において、コスト・効果を考慮して妥当な対応範囲の参考例を提示

SBOM対応項目の選択肢

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

6

- SBOM作成・活用時に、どこにコストがかかるかを一覧にまとめている

SBOMへの対応は「やる」「やらない」の2択ではなく、コスト見合いで進めていくのが良い。それを検討するのにちょうどよい比較表となっている。

ver2.0追加内容

SBOM取引モデルの概要

SBOM取引モデルの主な構成要素（契約で規定することが期待される事項）

- 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, SWID, 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

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

※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。

7

- サプライチェーンを意識した、SBOM取引モデルの構成要素を提示

自社コントロール不能な「取引先」へのアプローチについて、規定すべき項目とレベル（必須/特定分野で必須）が示される。これにより、始める際に必要なコストを選択できる。

TLP:CLEAR

ここからが参考資料扱いになっている

改訂前の版（ver.1）の内容も説明されている。

(参考) 経営者の皆様へ　～SBOMの導入に向けて～

ver1.0の内容

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

- ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が一般化する中で、**ソフトウェアに対するセキュリティ脅威が近年増大**。2021年12月に発見されたApache Log4jの脆弱性は世界中に影響を及ぼしたほか、ある調査※1によれば、2019年から2022年にかけてのソフトウェアサプライチェーン攻撃の年平均増加率は742%であった。
- **ソフトウェアに対するセキュリティ脅威は企業経営へ大きな影響を及ぼす**。例えば、SolarWindsのサイバー攻撃の影響を受けた企業は、平均して年間収益額の約11%の損害を被ったというデータ※2もあるほか、製品に脆弱性が残存することで製品回収や販売停止につながった事例もある
- ソフトウェアに対するセキュリティを強化し、企業の信頼・安全につなげていくためには、ソフトウェアを適切に管理していくことが重要。

SBOMの概要・メリット

- このようなソフトウェアサプライチェーンに対する脅威の状況に対し、ソフトウェアの透明性を高めるためのソフトウェア管理の一手法として、**Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目**を集めている。
- **SBOMとは、ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト**のことで、**世界的に導入企業が増加**しているほか、医療機器分野など、**一部の分野では規制や制度化が検討**され始めている。
- 情報量が膨大となるソフトウェア管理に対し、機械処理可能なSBOMを導入することで、**ソフトウェア管理に要する対応コストや人的コストを低減**することができ、これにより**開発生産性向上に繋がる**。事実、経済産業省が実施した医療機器分野を対象とした実証では、**SBOMを活用した脆弱性管理を行うことで、手動での管理と比較して、管理工数が70%程度低減**した。
- また、脆弱性管理上のメリットとして、SBOMを作成し、継続的に管理することで、ソフトウェアの透明性を高め、**脆弱性残留リスクの低減**が期待されるほか、**サプライチェーンを通じた脆弱性対応の効率化**にも繋がる。
- さらに、ライセンス管理上のメリットとして、SBOMを導入し、OSSのライセンス情報を管理することで、**ライセンス違反リスクの低減**にも寄与する。
- 実証を通じて、SBOM活用によるメリットが確認できた一方で、実際のSBOM導入に際しては様々なハードルが存在することが明らかとなった。

手引の目的

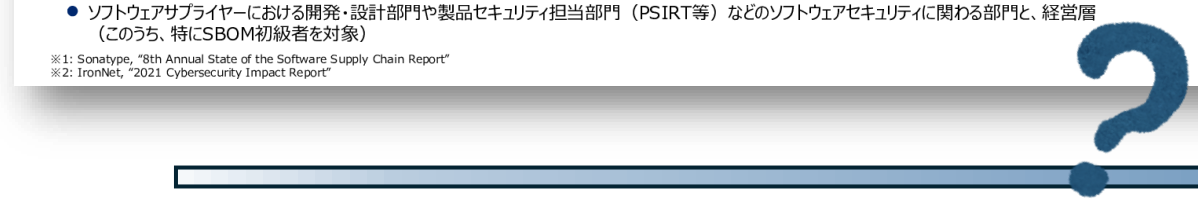
- 本手引では、**SBOMに関する基本的な情報を提供する**とともに、企業の効率的・効果的なSBOM導入を支援するために、**SBOM導入に向けた主な実施事項及びSBOM導入にあたって認識しておくべきポイント**を示す。

対象読者

- ソフトウェアサプライヤーにおける開発・設計部門や製品セキュリティ担当部門（PSIRT等）などのソフトウェアセキュリティに関わる部門と、経営層（このうち、特にSBOM初級者を対象）

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

9



経営者に向けた「SBOM導入に向け」たメリット説明のページだが…

私見だが…

- SBOM導入は、法的要件等により仕方なく導入することが大半であり、メリット/デメリットで好意的に導入する組織は大組織以外ありえないと思われる
  - 現状でさえ脆弱性管理ができていないのに、追加コストがかかることは無理であろう
  - SBOMは脆弱性管理の「銀の弾丸」という誤ったメッセージが見受けられるが、そうはならない

- 本書は、SBOMを導入しようとしている組織には非常に有益だが、SBOMを導入する余力のない組織にはあまり意味がないように見える
  - しかしながら、国としてどのように考えているかを示す点では、非常に重要と思われる

TLP:CLEAR

(参考) SBOMに関する誤解と事実

ver1.0の内容

- 手引では、米国NTIAが発表した文書※やSBOM導入に関する実証の結果を踏まえ、以下に示すようなSBOMに関する誤解と事実を記載。

誤解：対象ソフトウェアが直接利用しているコンポーネントのみSBOMの管理対象とすればよい

（事実）対象ソフトウェアが直接利用しているコンポーネントだけでなく、そのコンポーネントが再帰的に利用するコンポーネントについても把握しないと、脆弱性対応が不十分となる可能性がある。どの階層のコンポーネントまでSBOMを作成するかという「SBOMの深さ」の観点に関しては、有識者による議論が進行中である。

誤解：SBOM作成に用いるSBOMツールの選定において、特に留意すべき点はない

（事実）SBOM作成を支援するツールについて、有償のツール及びOSSとして提供される無償のツールが既に複数公開されている。無償のツールを活用することで、ツール自体はコストをかけずに入手できるものの、有償ツールと比較して、導入・活用に関するマニュアルやサポートが限定的であることが多く、ツールの習得に多大なコストがかかる可能性がある。また、有償ツールと比較してサポート範囲や性能が限定的であることが多く、SBOM導入の目的を達成できない可能性もある。SBOMの作成に当たっては、SBOMツールを活用することで効率的にSBOMを作成することができるが、自社のSBOM導入の目的を踏まえて使用するツールを選定する必要がある。

誤解：SBOMツールを活用することで、対象ソフトウェアに含まれるコンポーネントを完全に特定することができる

（事実）SBOMツールを用いることで効率的にSBOMを作成することができるが、SBOM作成に当たってのコンポーネントの誤検出や検出漏れが発生し、正確なSBOMを作成することができない場合もある。そのため、例えば、SBOMツールにより出力されたSBOMをレビューするなどの取組も検討することが大切である。

誤解：SBOMツールが出力したすべての脆弱性に対応する必要がある

（事実）SBOMツールが出力した脆弱性に関する結果を踏まえて脆弱性へのリスク対応を行う際、脆弱性の影響範囲、リスクの評価結果、対応に要するコスト等を踏まえ、優先度を踏まえた脆弱性対応が必要となる。この際、必ずしもすべての脆弱性が利用可能ではなく、影響を受けない脆弱性も存在することに留意する必要がある。

誤解：作成するSBOMのコンポーネントの粒度はサプライチェーン全体で共通化し、必要なコンポーネント情報だけを保持するべきである

（事実）現状では、JVNや米国NVDのような脆弱性情報データベースにおける「影響を受けるソフトウェア」の粒度が体系化されていないため、コンポーネントの粒度を限定すると脆弱性の特定で漏れが生じる可能性がある。そのため、OSSのみならず、自社製品なども含めてコンポーネント情報を保持することが有効である。

誤解：SBOMの対象はパッケージソフトウェアや組込みソフトウェアのみである

（事実）ソフトウェアに限らず、ITシステムもSBOMの対象となりうる。なお、コンテナイメージに対するSBOM、SaaSソフトウェアに対するSBOM、クラウドサービスに対するSBOM等のオンラインアプリケーションに対するSBOMの議論も米国を中心に行われている。

誤解：SBOMのフォーマットとして、SPDX、CycloneDX、SWIDタグの3つのフォーマットのみが認められており、独自フォーマットに基づくSBOMは認められない

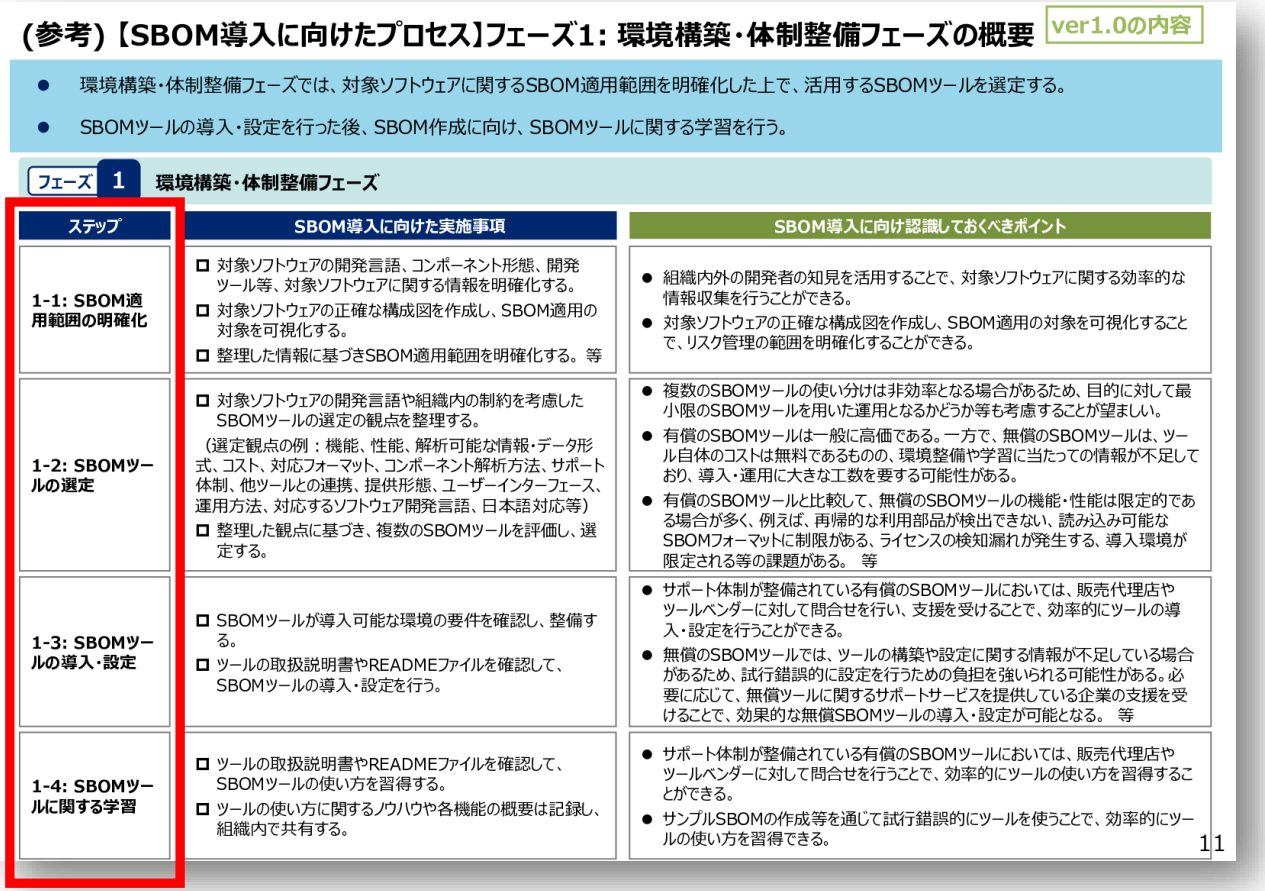
（事実）米国NTIAの定義に拠れば、SBOMとは「ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト」のことであり、独自フォーマットであってもこの定義に合致する場合はSBOMとみなすことができる。ただし、SBOMの「最小要素」として「自動化サポート」が位置づけられており、また、自動処理により効率化が図られることから、可能な限り、自動処理可能なフォーマットの採用を検討することが望ましい。

※ NTIA（National Telecommunications and Information Administration）, SBOM Myths vs. Facts https://www.ntia.gov/files/ntia/publications/sbom_myths_vs_facts_nov2021.pdf

10

大半は同意できるが…

- SBOMはあくまで「ソフトウェア部品表」であり、脆弱性対応に活用することを必須とするものではない、ことに留意が必要
- フォーマットは、今のところ「最小要件」が共通して使えるので、各フォーマット間で最小要件をコンバートして使えばいいじゃない、というのがOpenSSFでの志向と思われる
  - 現状のフォーマットは必ずしも現在の運用に最適というわけではないので、今後新しいフォーマットが発生する可能性は十分あり得る



(参考)【SBOM導入に向けたプロセス】フェーズ1：環境構築・体制整備フェーズの概要 ver1.0の内容

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

フェーズ 1 環境構築・体制整備フェーズ

ステップ	SBOM導入に向けた実施事項	SBOM導入に向け認識しておくべきポイント
1-1: SBOM適用範囲の明確化	□ 対象ソフトウェアの開発言語、コンポーネント形態、開発ツール等、対象ソフトウェアに関する情報を明確化する。 □ 対象ソフトウェアの正確な構成図を作成し、SBOM適用の対象を可視化する。 □ 整理した情報に基づきSBOM適用範囲を明確化する。等	● 組織内外の開発者の知見を活用することで、対象ソフトウェアに関する効率的な情報収集を行うことができる。 ● 対象ソフトウェアの正確な構成図を作成し、SBOM適用の対象を可視化することで、リスク管理の範囲を明確化することができる。
1-2: SBOMツールの選定	□ 対象ソフトウェアの開発言語や組織内の制約を考慮したSBOMツールの選定の観点を整理する。 （選定観点の例：機能、性能、解析可能な情報・データ形式、コスト、対応フォーマット、コンポーネント解析方法、サポート体制、他ツールとの連携、提供形態、ユーザーインターフェース、運用方法、対応するソフトウェア開発言語、日本語対応等） □ 整理した観点に基づき、複数のSBOMツールを評価し、選定する。	● 複数のSBOMツールの使い分けは非効率となる場合があるため、目的に対して最小限のSBOMツールを用いた運用となるかどうか等も考慮することが望ましい。 ● 有償のSBOMツールは一般に高価である。一方で、無償のSBOMツールは、ツール自体のコストは無料であるものの、環境整備や学習に当たっての情報が不足しており、導入・運用に大きな工数を要する可能性がある。 ● 有償のSBOMツールと比較して、無償のSBOMツールの機能・性能は限定的である場合が多く、例えば、再帰的な利用部品が検出できない、読み込み可能なSBOMフォーマットに制限がある、ライセンスの検知漏れが発生する、導入環境が限定される等の課題がある。 等
1-3: SBOMツールの導入・設定	□ SBOMツールが導入可能な環境の要件を確認し、整備する。 □ ツールの取扱説明書やREADMEファイルを確認して、SBOMツールの導入・設定を行う。	● サポート体制が整備されている有償のSBOMツールにおいては、販売代理店やツールベンダーに対して問合せを行い、支援を受けることで、効率的にツールの導入・設定を行うことができる。 ● 無償のSBOMツールでは、ツールの構築や設定に関する情報が不足している場合があるため、試行錯誤的に設定を行うための負担を強いられる可能性がある。必要に応じて、無償ツールに関するサポートサービスを提供している企業の支援を受けることで、効果的な無償SBOMツールの導入・設定が可能となる。 等
1-4: SBOMツールに関する学習	□ ツールの取扱説明書やREADMEファイルを確認して、SBOMツールの使い方を習得する。 □ ツールの使い方に関するノウハウや各機能の概要は記録し、組織内で共有する。	● サポート体制が整備されている有償のSBOMツールにおいては、販売代理店やツールベンダーに対して問合せを行うことで、効率的にツールの使い方を習得することができる。 ● サンプルSBOMの作成等を通じて試行錯誤的にツールを使うことで、効率的にツールの使い方を習得できる。

11

以下、各フェーズでの検討点が書かれている。

- 1-1:SBOM適用範囲の明確化
- 1-2:SBOMツールの選定
- 1-3:SBOMツールの導入・設定
- 1-4:SBOMツールに関する学習

フェーズごとに閉じる話ではなく、すべてのフェーズに対して検討をしてから動く必要がある。

- SBOMツールを選定したが、サプライチェーン上では利用がしづらいツールで再検討が必要になる、等がある

(参考)【SBOM導入に向けたプロセス】フェーズ2: SBOM作成・共有フェーズの概要

ver1.0の内容

- SBOM作成・共有フェーズでは、SBOMツールを活用してコンポーネントを解析した後、実際にSBOMを作成する。コンポーネントの解析結果には誤検出や検出漏れが含まれる可能性があるため、内容を確認する必要がある。
- また、対象ソフトウェアの利用者及びサプライヤーに対するSBOMの共有を検討する。

フェーズ 2 SBOM作成・共有フェーズ

ステップ	SBOM導入に向けた実施事項	SBOM導入に向け認識しておくべきポイント
2-1: コンポーネントの解析	□ SBOMツールを用いて対象ソフトウェアのスキャンを行い、コンポーネントの情報を解析する。 □ SBOMツールの解析ログ等を調査し、エラー発生や情報不足による解析の中断や省略がなく、解析が正しく実行されたかを確認する。 □ コンポーネントの解析結果について、コンポーネントの誤検出や検出漏れがないかを確認する。	● SBOMツールを用いることで、手動の場合と比較し、効率的にコンポーネントの解析及びSBOMの作成を行うことができる。SBOMツールを用いることの効果はコンポーネント数が多いほど大きい。 ● パッケージマネージャーの構成情報を活用することが効果的な場合がある。また、パッケージマネージャーを用いることで、SBOMツールでは特定できない粒度の細かいコンポーネントを特定できる場合がある。 ● コンポーネントの誤検出や検出漏れが生じる場合がある。例えば、シンボリックリンクやランタイムライブラリ等のコンポーネント、深い階層のコンポーネント、特定分野でのみ利用されているコンポーネント等を検出できない場合があるほか、コンポーネントを特定できてもバージョン情報が誤っている場合がある。 ● SBOMツールにおけるコンポーネント解析方法によって、出力結果が異なる。依存関係に基づく解析の場合、誤検出の発生可能性は極めて低いが、その他の解析方法の場合、誤検出・検出漏れが発生する可能性がある。 等
2-2: SBOMの作成	□ 作成するSBOMの項目、フォーマット、出力ファイル形式等のSBOMに関する要件を決定する。 □ SBOMツールを用いて、当該要件を満足するSBOMを作成する。	● SBOM作成と共有の目的を鑑み、正確な情報を不足なくSBOMに記載することが望ましい。 ● サードパーティやOSSコミュニティなどの第三者から提供されたコンポーネントを使用している場合は、当該コンポーネントのSBOMの提供を受けることができる場合もある。ただし、そのコンポーネントを自組織にて改変して使用している場合は、提供を受けたSBOMをそのまま利用できなくなるので注意が必要である。 等
2-3: SBOMの共有	□ 対象ソフトウェアの利用者及び納入先に対するSBOMの共有方法を検討した上で、必要に応じて、SBOMを共有する。 □ SBOMの共有に当たって、SBOMデータの改ざん防止のための電子署名技術等の活用を検討する。	● 納入先が利用するSBOMツールによって、採用可能なSBOM共有方法が異なる。 ● 利用者に対するSBOM共有について、様々な方法が想定される。利用者に対してSBOM共有を行う場合、それぞれの方法の長所短所を踏まえて検討する。

12

(参考)【SBOM導入に向けたプロセス】フェーズ3: SBOM運用・管理フェーズの概要

ver1.0の内容

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

フェーズ 3 SBOM運用・管理フェーズ

ステップ	SBOM導入に向けた実施事項	SBOM導入に向け認識しておくべきポイント
3-1: SBOMに基づく脆弱性管理、ライセンス管理等の実施	■ 脆弱性に関するSBOMツールの出力結果を踏まえ、深刻度の評価、影響度の評価、脆弱性の修正、残存リスクの確認、関係機関への情報提供等の脆弱性対応を行う。 ■ ライセンスに関するSBOMツールの出力結果を踏まえ、OSSのライセンス違反が発生していないかを確認する。	● SBOMツールが出力した脆弱性情報やライセンスに関する情報が誤っている場合があり、出力結果を確認する必要がある。 ● SBOMツールでコンポーネントのEOLを特定できない場合、別途個別に調査する必要がある。
3-2: SBOM情報の管理	■ 作成したSBOMは、社外からの問合せがあった場合等に参照できるよう、変更履歴も含めて一定期間保管する。 ■ SBOMに含まれる情報やSBOM自体を適切に管理する。	● 自動で脆弱性情報が更新・通知されるSBOMツールを用いることで、新たな脆弱性に関する情報を即座に把握することができる。ツールを用いた自動管理ができない場合、担当者を別途設置するなど運用面でカバーする必要があるが、対応工数を要する。 ● SBOMの管理は、組織内のPSIRTに相当する部門が対応することが効果的である。PSIRTに相当する部門が存在しない場合、品質管理部門にて対応することが効果的である。

13

ver2.0追加内容

(参考) 8.付録：SBOM対応モデルの概要（1/2）

本章の背景・目的

- SBOM対応モデルは、SBOMの作成・活用に関する対応範囲を可視化し比較可能にする方法（フレームワーク）を提供し、それを用いることで、ソフトウェア取引において、脆弱性管理などのソフトウェア管理レベルの高い製品が評価される仕組みを提供する。
- SBOM対応モデルにより、SBOM対応範囲を判断するための情報が提供され、ソフトウェア取引市場において必要なレベルに自律的な調整が進むことが期待される。

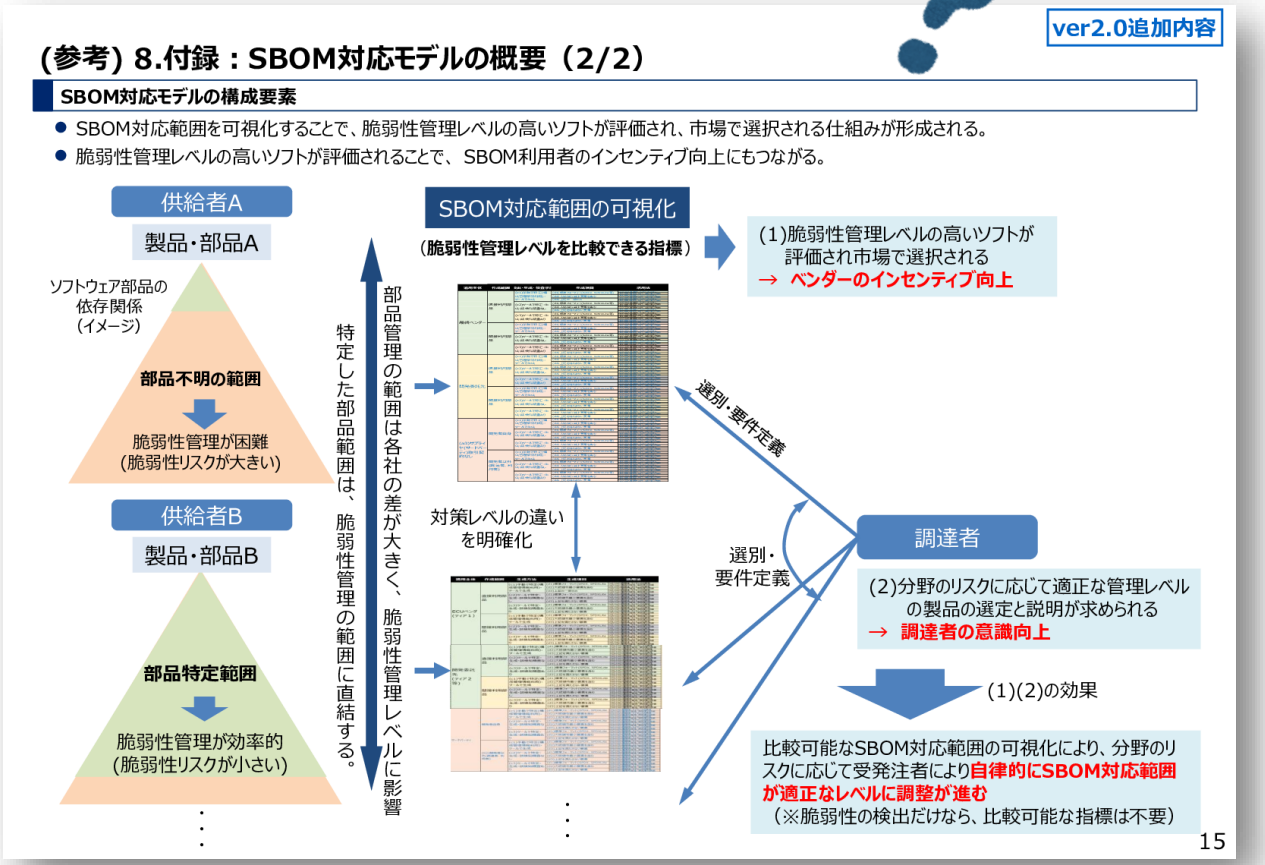
SBOM対応モデルの章構成

章	項	主な記載内容	実証項目との関係
付録 8.1. 背景と目的	1 目的 2 問題認識 3 想定読者 4 本書の全体構成	• SBOM普及における課題や問題認識等の背景を記載 • 問題認識に基づきSBOM対応モデルの必要性を示す。 • それらを踏まえて本書の目的を示す。 • SBOM対応モデルの概要、対象読者についてまとめる。 • 本書の全体構成を示す。	実証・調査事業の結果等に基づき整理。 ３分野での実証に基づき対象者を示す（開発部署関係者を想定）
付録 8.2. SBOM可視化フレームワーク	1 SBOM対応モデルとは？ 2 基本的な考え方 3 SBOM可視化フレームワーク	• SBOM対応モデルの基本的な考え方、活用方法についてまとめる。	実証結果全体をもとに考え方を整理。
付録 8.3. SBOM対応モデルと活用方法	1 SBOM対応モデルの位置付け 2 活用方法	• SBOM対応モデルの枠組みを定義する上で必要になる、適用項目の選択肢とそれらの組合せによる適用範囲について記載 • 規制・法制度との関係、位置づけについて示す。	SBOM適用選択肢の整理結果をもとに作成。
付録 8.4. SBOM対応モデルの参考例(自動車)	1 法制度・基準の概要 2 実証に基づくSBOM対応モデル（案） 3 活用方法と留意点	• 自動車分野を例に、規制分野におけるSBOM対応モデルを検討するにあたり前提となる法制度や条件を整理し、たたき台としてのSBOM対応モデル（案）を示す。 • 分野ごとのガイドラインとして検討を進めるための留意点、課題等を挙げる。	SBOM実証の前提条件等の調査検討結果に基づき整理。
付録 8.5. SBOM対応モデルの参考例(ソフトウェア分野)	1 法制度・基準の概要 2 実証に基づくSBOM対応モデル（案） 3 活用方法と留意点	• ソフトウェア分野を例に、規制分野におけるSBOM対応モデルを検討するにあたり前提となる法制度や条件を整理し、たたき台としてのSBOM対応モデル（案）を示す。 • 分野ごとのガイドラインとして検討を進めるための留意点、課題等を挙げる。	SBOM実証の前提条件等の調査検討結果に基づき整理。
付録 8.6. SBOM対応モデルの参考例(医療機器分野)	1 法制度・基準の概要 2 実証に基づくSBOM対応モデル（案） 3 活用方法と留意点	• 医療機器分野を例に、規制分野におけるSBOM対応モデルを検討するにあたり前提となる法制度や条件を整理し、たたき台としてのSBOM対応モデル（案）を示す。 • 分野ごとのガイドラインとして検討を進めるための留意点、課題等を挙げる。	SBOM実証の前提条件等の調査検討結果に基づき整理。

14

対応範囲などを、自動車/ソフトウェア分野/医療機器分野 はどう考えているのかが、なんとなく記載されている

TLP:CLEAR



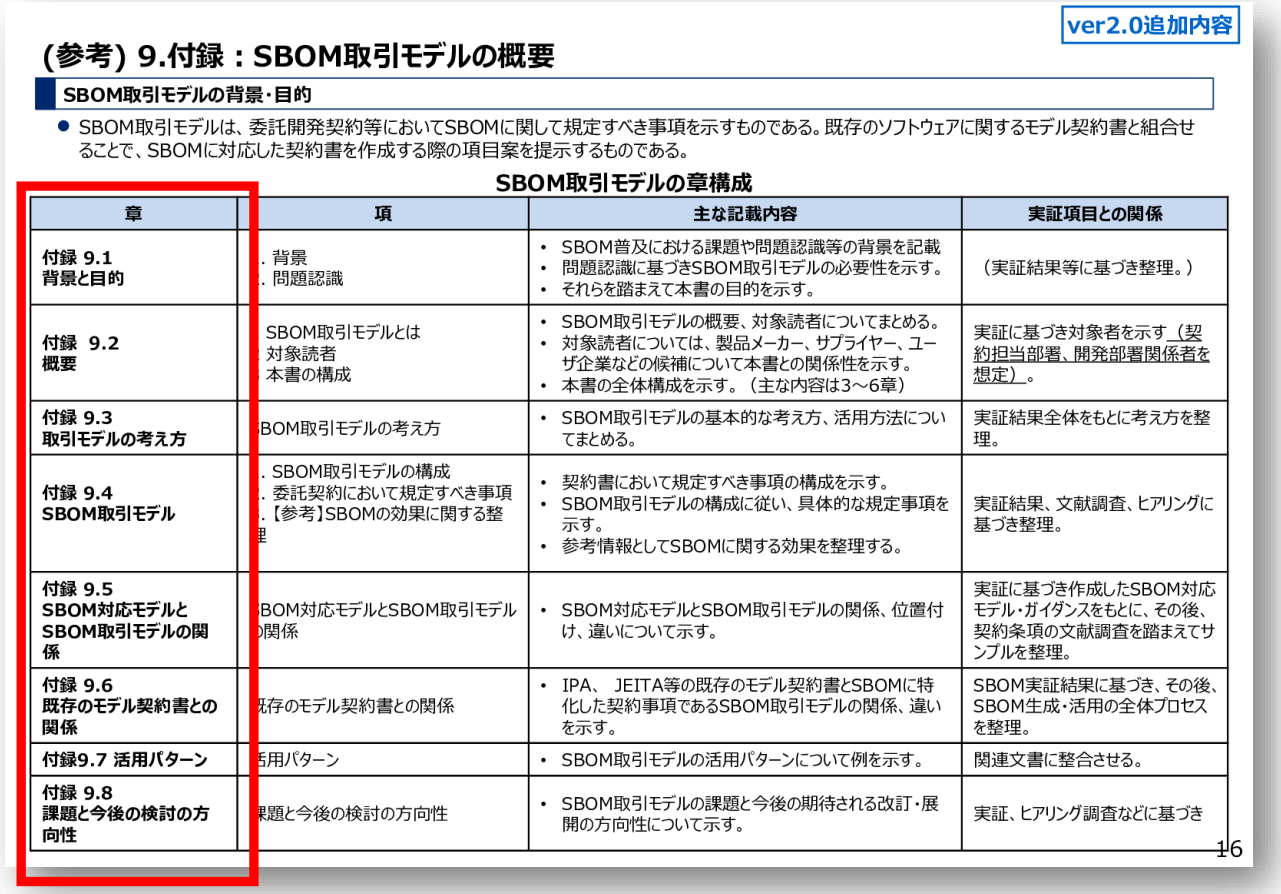
SBOM導入メリットの説明か

- SBOM対応範囲が高く脆弱性管理レベルた高ければ市場の評価が高まる、という理想論の表現。

個人的には…

- 法的要件がなければ、まずは「自社製品が何を使っているかの資産棚卸をする」という意味合いで、SBOMを利用ソフトウェア一覧を出すという目的で用意してみる
- 余裕が出てくれば脆弱性管理に使う（オプショナル）

という考えでないと普及しないと考えられる。



ver2.0追加内容

(参考) 9.付録：SBOM取引モデルの概要

SBOM取引モデルの背景・目的

- SBOM取引モデルは、委託開発契約等においてSBOMに関して規定すべき事項を示すものである。既存のソフトウェアに関するモデル契約書と組合せることで、SBOMに対応した契約書を作成する際の項目案を提示するものである。

SBOM取引モデルの章構成

章	項	主な記載内容	実証項目との関係
付録 9.1 背景と目的	. 背景 . 問題認識	• 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。	（実証結果等に基づき整理。）
付録 9.2 概要	SBOM取引モデルとは . 対象読者 . 本書の構成	• 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）	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 9.3 取引モデルの考え方	BOM取引モデルの考え方	• 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 9.4 SBOM取引モデル	. SBOM取引モデルの構成 . 委託契約において規定すべき事項 . 【参考】SBOMの効果に関する整理	• 契約書において規定すべき事項の構成を示す。 • SBOM取引モデルの構成に従い、具体的な規定事項を示す。 • 参考情報としてSBOMに関する効果を整理する。	実証結果、文献調査、ヒアリングに基づき整理。
付録 9.5 SBOM対応モデルとSBOM取引モデルの関係	BOM対応モデルとSBOM取引モデル 関係	• SBOM対応モデルとSBOM取引モデルの関係、位置付け、違いについて示す。	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 9.6 既存のモデル契約書との関係	既存のモデル契約書との関係	• IPA、 JEITA等の既存のモデル契約書とSBOMに特化した契約事項であるSBOM取引モデルの関係、違いを示す。	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9.7 活用パターン	活用パターン	• SBOM取引モデルの活用パターンについて例を示す。	関連文書に整合させる。
付録 9.8 課題と今後の検討の方向性	課題と今後の検討の方向性	• SBOM取引モデルの課題と今後の期待される改訂・展開の方向性について示す。	実証、ヒアリング調査などに基づき

16

SBOMを取引先に要求する場合の検討事項が示されている。

対応にはコストがかかるため、強権/高圧的な下請けへの要求は法的に問題がある

- 要法的議論
  - =>ISOG-Jで弁護士との議論あり

まずは自社、その後順次 次のTirに波及させる/ある程度のコストを負担する、ということが必要と思われる。

まとめ

- SBOMは、(本来)法的要件がなければ導入必須ではない
  - 自動車業界、医療業界、製造業界（EU サイバーレジリエンス法等）などは、法的要求によりSBOM対応が必要になる
  - しかしながら、国内向け/ソフトウェア産業では、必須ではない状況も多々ある
    - とはいえ、今後は必要になっていくことが推定される
  - 自社サービス/製品が何を使っているかという、**利用ソフトウェアの棚卸**としてまずは使っていくのが良いと考える
    - 脆弱性管理は、二の次でよいと個人的には考える
- 導入にあたり、全体設計が大切
  - 適用範囲（対象製品、サプライチェーンの深さ、等）
  - SBOM運用（更新、データ流通）
  - 活用（脆弱性管理にどの程度組み込むか）
    - SBOMツールを入れればすべて解決という**”銀の弾丸”では **ない****
- 経産省資料により、コストを考慮した適用範囲や対応方針を検討できるようになった
  - もしSBOM導入を検討しているのであれば、参考になると思われる
- 必要に応じて、パブリックコメント出しましょう！

Appendix I: 関連リンク

脆弱性
対応
勉強会

- who am I（脆弱性管理に興味のある方向け）
  - https://github.com/hogehuga/
  - https://zeijyakuseitaioukenkyukai.connpass.com/
  - https://www.facebook.com/groups/zeijyakuseitaioukenkyukai
- 私の、脆弱性管理その他の過去の話
  - InternetWeek2023
    - 告知： https://scan.netsecurity.ne.jp/article/2023/10/31/50171.html
    - 発表： https://www.nic.ad.jp/ja/materials/iw/2023/proceedings/c6/
  - NCA Annual Conference 2023
    - 車座： https://annualconf.nca.gr.jp/program/day0/1550_1800_1/
    - CFP： https://annualconf.nca.gr.jp/program/day2/1600_1620_2/
  - 総裁LT
    - 34回： https://sec-kansai.connpass.com/event/253980/
  - 参加し、議論できる団体
    - JNSA： https://www.jnsa.org/
    - ISOG-J： https://isog-j.org/
    - NCA： https://www.nca.gr.jp/
- 経済産業省
  - **サイバー攻撃への備えを！「SBOM」（ソフトウェア部品構成表）を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引（案）を公表します**
    - https://www.meti.go.jp/press/2024/04/20240426001/20240426001.html
  - 「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引」を策定しました（所謂 ver1.0）
    - https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html
- SBOM関連
  - CISA： https://www.cisa.gov/sbom
  - OpenSSF： https://openssf.org/ （Slack等で議論されている）
  - CISA Allan Friedman： https://twitter.com/allanfriedman , https://www.cisa.gov/speaker/allan-friedman

関連するリンク氏

TLP:CLEAR