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～

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。

経営者の皆様へ　～SBOMの導入に向けて～

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”

SBOMに関する誤解と事実

- 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

【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

- 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。

【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

- 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。

【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

- 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。