OpenSSF
OPEN SOURCE SECURITY FOUNDATION

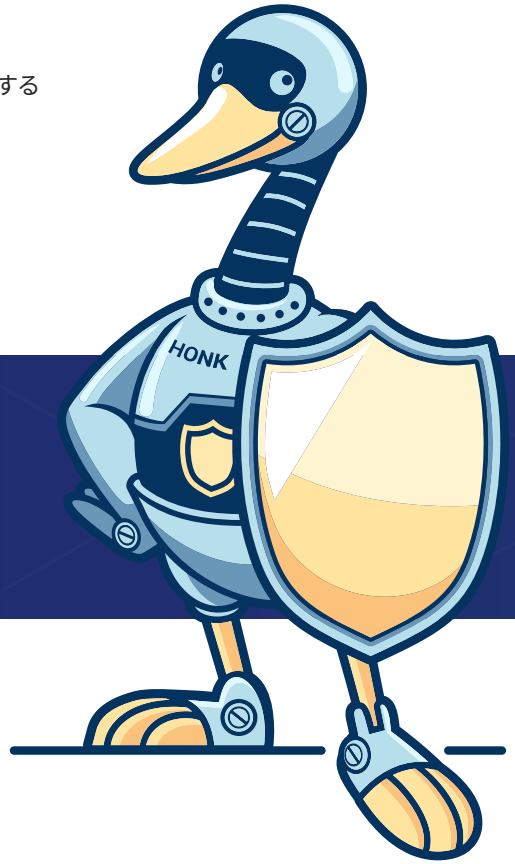
# SBOMデータによるリスク管理の意思決定の改善

2025年9月18日

# 免責事項

この文書は、サイバーセキュリティ・インフラセキュリティ庁（CISA）の支援を受け、ソフトウェア部品表（SBOM）の専門家コミュニティによってオープンプロセスで起草されました。CISAはこの文書を起草しておらず、著者でもありません。また、この文書はCISAまたは米国政府の公式な政策を代表するものではありません。CISAおよび米国政府は、この文書に記載されている見解を具体的に採用または支持するものではありません。[1]

この文書の内容はいかなる組織に対しても拘束力を持つものではなく、SBOM の消費と使用に関する将来の要件の基礎を形成するものとして捉えるべきです。



# 目次

# エグゼクティブサマリー

このドキュメントの目的は、ソフトウェア・プロデューサーとコンシューマーにとってのソフトウェア部品表（SBOM）の利点を示すことです。「SBOMを生成または受け取ったら、どうすればいいですか?」そして「SBOMから組織に役立つどのような追加の洞察やインテリジェンスが得られますか?」という疑問に答えることを目指しています。

このドキュメントでは、主に次の 2 つの方法でこれらの質問に答えています。1) ソフトウェア・プロデューサーによる SBOM の生成からコンシューマーによる分析と使用までの SBOM に何が起こるかを説明および図示することで、SBOM ライフサイクルを定義します。2) さまざまな関係者が SBOM を使用して組織に利益をもたらす方法を示す 13 の実用的なユースケースを示します。

SBOMライフサイクルは、SBOMのライフサイクルにおける3つの主要フェーズ（生産、共有、消費）を通じて発生するオペレーションを表します。さらに、これらのオペレーションは3つの成熟度レベルに分類されます。

- 基本的な SBOM 操作には、SBOM の生成、検証、公開、保存および消費が含まれます。
- 高度な SBOM 操作では、プロデューサーまたはコンシューマーが SBOM を活用してさらなる価値を引き出す方法について説明します。たとえば、SBOM を比較、強化、またはマージしたり、さまざまなリスクについて SBOM を分析したりできます。
- 継続的に実施される脆弱性管理オペレーションは、新たに発見されたリスクに対する SBOM のリリース後の定期的な監視など、最も成熟しています。

13のユースケースでは、プロデューサーまたはコンシューマーがSBOMを活用して組織にとって価値のある情報を抽出する実際の状況が説明されています。これらのユースケースはSBOMのライフサイクル全体にわたり、ソフトウェアバージョン間の差異の特定、セキュリティ、ライセンス、コンプライアンスリスクの特定、ソフトウェアコンポーネントのサポート終了が近づいている場合に組織に警告を発すること、影響を受けるソフトウェアについてインシデント対応者に通知すること、調達または合併買収（M&A）の意思決定を支援することなど、SBOMの活用方法といったトピックを網羅しています。各ユースケースについて、本書では簡潔な説明文と、ユースケースのアクター、ビジネス上の動機、目的、目的達成のための手順、米国商務省電気通信情報局（NTIA）が定める最低限必要な要素、その他の補足データ、そして得られるメリットをまとめた表を提供しています。

ユースケースから得られる重要なポイントは、ドキュメントの最後に記載されています。

# はじめに

2018年に米国商務省電気通信情報局（NTIA）がソフトウェアコンポーネントの透明性に関するマルチステークホルダープロセスを開始して以来、ソフトウェア部品表（SBOM）の採用は増加し、多様化しています。SBOMの実装も、技術の進歩や新たなユースケースへの対応を反映して成熟してきました。SBOMの採用と実装を推進する要因の一つは、SBOMデータを分析することで、最新のアプリケーション、コードの再利用、外部開発ライブラリの使用状況を理解•管理し、透明性が向上することです。このドキュメントでは、ソフトウェア•プロデューサーとコンシューマーがSBOMデータに対して実行できる具体的な操作について説明します。これらの操作によって、ソフトウェアのセキュリティリスクに関する意思決定の改善に役立つ貴重な洞察が得られます。

## モチベーション

ソフトウェア•インベントリとしての役割に加えソフトウェア•プロデューサーとコンシューマーの両方にとってのSBOMの有用性は十分に理解されていません。このドキュメントでは、「SBOMを生成または受け取ったら、どうすればいいのか?」と「 SBOMから組織に役立つどのような追加の洞察やインテリジェンスが得られるのか?」という主要な疑問に答えます。

このドキュメントの目的は、SBOMを生成するソフトウェア•プロデューサーと、ベンダーやパートナーからSBOMを受け取るコンシューマーの両方にとって、SBOMの利点を示すことです。このドキュメントでは、既に実装されている、または将来実装される可能性のあるユースケースを提示することでこれを実現します。例えば、SBOMデータを他のデータセットと相互参照することで、組織がセキュリティ、ライセンス、その他のサプライチェーンリスクに積極的に対処できるようにします。これらのユースケースは、組織がSBOM全体に対して実行できる実用的なタスクを提供し、ソフトウェアに関するインテリジェンスと洞察を抽出します。

## 目標

この文書は、サイバーセキュリティ・インフラセキュリティ庁（CISA）[1]が推進するコミュニティ主導のワークストリームであるSBOM運用ワーキンググループによって作成されました。この文書の最終的な目標は、実務者がSBOMを使用して、より情報に基づいた技術的およびビジネス上の意思決定を行うための基盤を構築することです。二次的な目標は、外部データセット[1]に関する議論を促進することです。SBOMの活用によって可能になる、業界全体のソフトウェアの透明性をさらに向上させるプロセスです。ユースケースを特定するために、本ドキュメントでは「SBOMライフサイクル」という概念を紹介します。これは、個人、組織、ツールがSBOMデータを拡充、分析、安全に共有するために実行できるプロセスを特定します。関係者から提出された議論とユースケースを期限内に絞り込み、焦点を絞るため、本ドキュメントの範囲は **図1** に示すSBOMライフサイクルのハイライトされたセクションに限定しました。

このドキュメントでは、プロデューサーからコンシューマーに提供された SBOM に対して実行できる操作に焦点を当てています。コンシューマーとプロデューサーの関係は、組織エンティティ間での SBOM 共有に限定されず、同じ組織内でも共有できます。SBOM の有用性に焦点を当てるために、プロデューサーが提供するデータは正確かつ完全であると想定されています。また、プロデューサーは、コンシューマーと共有する

1 このようなデータセットの例としては、**https://endoflife.dateなどがあります。**

前に、SBOM の内容と構造を積極的に検証しているものと想定しています。正確性や完全性などのデータ品質の問題については、このドキュメントの範囲外で、焦点を絞った詳細な議論が必要です。さらに、このドキュメントでは、組織内または組織間での SBOM の保存、転送、共有方法については説明していません。データ抽出の目的で、このドキュメントでは、SBOM が機械可読であり、SPDX やCycloneDXなどの広く使用されている形式であると想定しています。コンシューマー ワークフローが承認された SBOM 情報に基づいて動作することを保証するため、プロデューサーによって共有されるすべての SBOM には、コンシューマーがその整合性を判断できる署名が関連付けられ、SBOM データまたはファイル形式が変更されると、一意に識別できる新しい SBOM が生成されるものと想定されます。

本文書では、過去のSBOM文書 [2] で概説されている特定の組織的役割は用いず、ソフトウェアを利用、運用、および製造する組織に一般的に見られる多様な役割について、より一般的な用語を用いています。これらの役割には、アーキテクト、シニアエンジニア、セキュリティチーム、サプライチェーンリスクマネジメント担当者、調達担当者、セキュリティ担当役員、法務チーム、リスク管理担当者などが含まれます。また、本ユースケースは特定のソフトウェアシステムに焦点を当てたものではありません。様々な業界や政府機関における、多くの種類のソフトウェアに適用できる一般的なプロセスについて説明しています。

## SBOMライフサイクル内の分析

### SBOMライフサイクルとSBOMライフサイクル管理の定義

SBOM運用ワーキンググループは、SBOMライフサイクルを、SBOMが生成されてから、SBOMで記述されたソフトウェアのコンシューマーによって分析および使用されるまでの過程と定義しています。また、SBOMライフサイクル管理を、ビジネス目標の達成、または組織への何らかの利益の実現のために実行されるアクションとオペレーションと定義しています。これらの利益の例としては、ソフトウェアシステムのコンポーネントにおけるセキュリティ、ライセンス、またはサポート性の問題に関するより深い洞察、規制コンプライアンスの達成、インシデント対応時の脆弱なコンポーネントの迅速な特定などが挙げられます。

この文書で説明するSBOMライフサイクルは、SBOMが堅牢なSBOMオーサリングワークフローに従って既に作成されているか、プロデューサーが提供するSBOMからインポートされているという前提に基づいています。開発者やソフトウェアベンダーがSBOMを技術的に生成し、保守するために行う作業は明確に除外されています。このライフサイクルは、学術研究者 [3] によって既に説明されています。

### SBOMライフサイクル図の起源

**図1** は、プロデューサーによる最初の作成から、少なくとも1人のコンシューマーによる使用までのSBOMライフサイクルの概念図を示しています。この図は、主に2つの目的で作成されました。1)「SBOMは作成後どうなるのですか?」や「個人や組織はSBOMをどのように活用するのですか?」といったよくある質問への回答、2)SBOMのプロデューサーとコンシューマーが議論、問題、要件、解決策を整理するのに役立つ、SBOMライフサイクルのメンタルモデルを提供することです。SBOMの作成、共有、使用は、初期の技術や実践を伴う、新しい専門分野です。そのため、SBOMライフサイクル図は、共通の概念モデルと用語を提供し、関係者間のコミュニケーションや、新しい技術とニーズの整合を促進します。

ワークフロー図の初期内容を作成するにあたり、CISA [4] [5] やNTIA [6] が招集したSBOMコミュニティが作成した文書、国家安全保障局（NSA） [7]のガイダンス、業界のSBOMユーザーから聞いた要件や事例などから、SBOMの使用方法に関する情報を統合しました。 さらに、このドキュメントの **セクション2** で紹介したユースケースから収集した情報、SBOM運用ワーキンググループのメンバーからの定期的なフィー

ドバック、改良された図が掲載された会議のプレゼンテーションへの反応 [8] に基づいて、図を改良しました。最終的なワークフローを **図1**に示します。

図に示されているSBOMライフサイクルは「一度きり」のものではなく、その後も改訂が繰り返されることになります。組織がSBOMを導入・活用するにつれて、SBOMライフサイクルも進化し、より詳細な情報、洞察、そしてテクノロジーが拡張される可能性が高くなります。

最後に、個々の組織がSBOMライフサイクルのすべてのプロセスに取り組むことはまずありません。各組織は、役割、事業目標、契約上の義務、規制要件、サプライチェーンの成熟度に基づいて、自らをこの道筋における独自の位置付けに位置づけます。この図は、この位置付けを支援し、その位置の前後に何があるのかを理解するために設計されています。

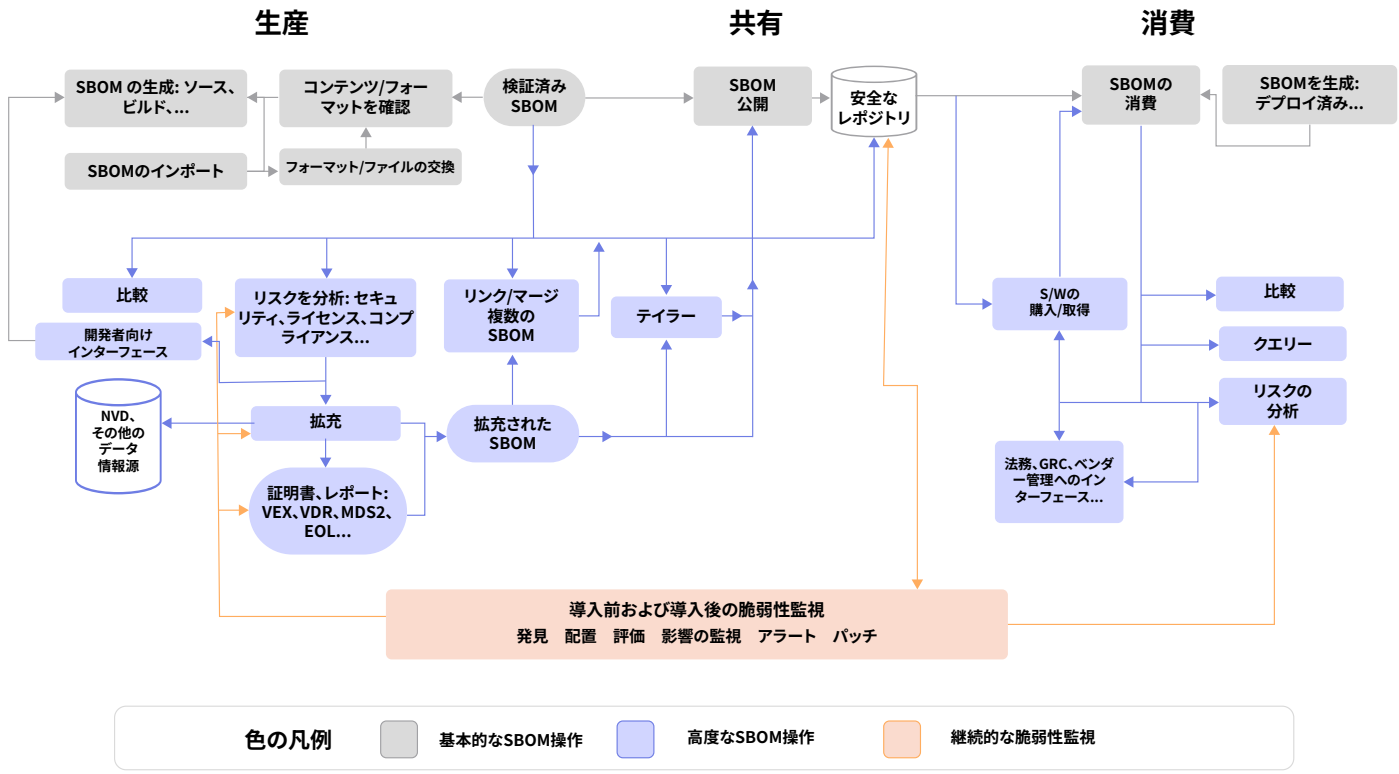
## SBOMライフサイクル図

**図1** に示すSBOMライフサイクル図は、左から右へ、SBOMのライフサイクルにおける3つの主要なフェーズ（**生産**、**共有**、**消費**）に対応しています。また、上から下へは、SBOM運用の成熟度を示す3つのレベル（**基本**（灰色）、**高度**（青色）、**継続的監視**（オレンジ色））に対応しています。SBOMライフサイクル管理は新興分野であるため、運用や分析の洗練度や成熟度は様々です。例えば、SBOM共有入門書 [9] では、SBOMの普及に適用される技術とプロセスの3つの異なる洗練度レベルについて説明しています。SBOMライフサイクル管理において、SBOM運用ワーキンググループは、ライフサイクル運用を図中の3つの成熟度カテゴリに分類しました。

SBOM のライフサイクルの最も基本的な形態では、SBOM は (ツールまたは人間による監査を介して) 生成されるか、SBOM 管理ソリューションにインポートされ、内容 (NTIA SBOM 最小要素 [10]を満たしているなど) と形式 ( CycloneDXまたは SPDX など) が検証され、安全な場所に保管され、コンシューマーによってアクセスされます。図では、これらの基本的な SBOM 管理操作は灰色のボックスで表されており、このドキュメントのユース ケースでは扱われていません。**セクション1.2**で説明したように、SBOM 運用ワーキング グループは、SBOM の生成、保管、またはコンシューマーへの転送という基本的な操作を分析から除外しました。私たちの焦点は、SBOM が生成され、プロデューサーとコンシューマーによる分析と監視に移行した後に SBOM に何が起こるかにあります。

図1

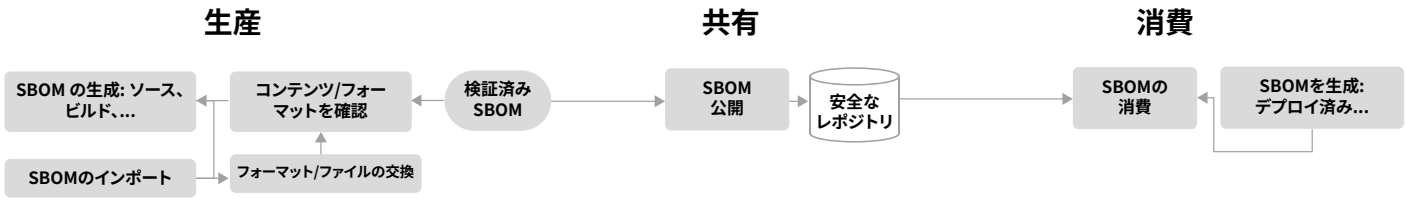
## SBOMライフサイクル図



## 基本的なSBOM操作

基本的な SBOM 操作を 図2に示します。

図2
### 基本的なSBOM操作




ソフトウェア・プロデューサーは、図の左上に示すように、多くの異なるタイプの **SBOM を生成**します。コンシューマーも、デプロイされたソフトウェアの SBOM を生成する場合があります。組織も **SBOM をインポート**しますが、NSA の SBOM 管理に関する推奨事項 [7] によれば、SBOM は SPDX [11] またはCycloneDX [12] 仕様に準拠し、JSON、XML、CSV など、仕様に適したファイル形式でインポート可能である必要があります。プロデューサーまたはコンシューマー (インポートされた SBOM の場合) は、**コンテンツと形式を検証**して、法律、規制、業界標準、および/または契約で要求される要素が含まれていること、および適切な SBOM 仕様に準拠していることを確認します。米国では、SBOM の最小要素は、2021 年に米国商務省電気通信情報局 (NTIA)[10] または関連する米国政府機関による後継によって定義された要素であることが多いです。 NSA ( [7] の8ページ目) は、SPDXとCycloneDXの両方のインポートとサポートを推奨しています。

検証プロセスは重要なステップであり、適切に実施されない場合、ライフサイクルの後半でコンシューマーがSBOMをインポートおよび分析する際に支障をきたす可能性があります。この検証プロセスの一環として、プロデューサーは**SBOMの形式を別の形式に変換**する必要が生じる場合があります。また、コンシューマーもSBOMを受け取った際に、SBOMの形式を変換する必要がある場合があります。

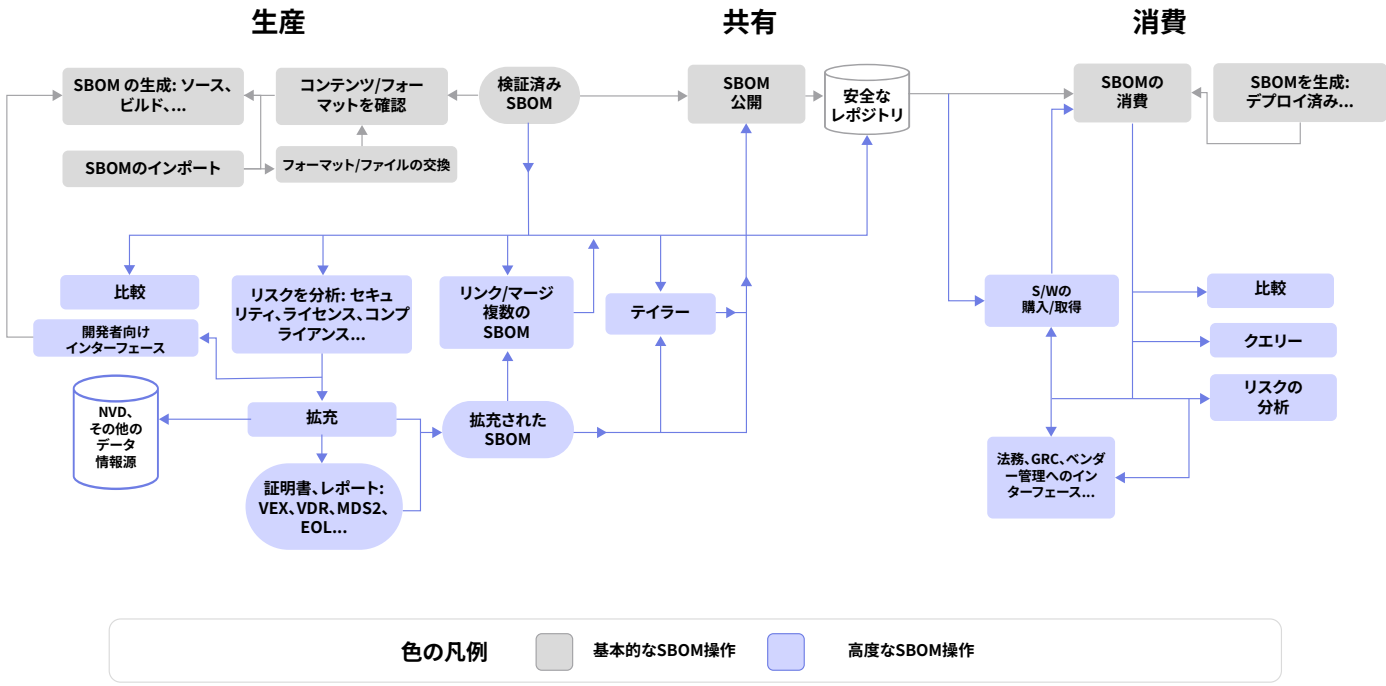
ライフサイクルの基本レベルでは、プロデューサーがSBOMを**公開**し、**セキュア**ストアまたは共通の交換ポイントに保存して、他のユーザーがコンシューマーに**配布**できるようにします。SBOMを受け取るコンシューマー [5] は、ソフトウェアを導入するエンドユーザー、配布用にSBOMを保有する第三者、またはソフトウェア開発プロセスの一環としてSBOMを使用するソフトウェア・プロデューサーなどです。

## 高度なSBOM操作

この文書で説明されているユースケースは、主に高度なSBOM操作に依存しており、図3では青色で示されています。ライフサイクルのこの部分における操作は、仕様への準拠が検証された SBOM に依存します。

図3

### 高度なSBOM操作



*SBOM分析は、セキュリティリスクにとどまらない洞察をもたらします。ライセンス、コンプライアンス、サポート性に関するリスクも特定し、インシデント対応、ベンダーリスク管理、ソフトウェア対応デバイスのフィールドサービスといったサポートプロセスも提供します。*

図の「生産」側と「消費」側の両方に表示される**比較**操作は、同じソフトウェアのビルドまたはバージョン間の違いを明確に確認するために実行されます。

**リスク分析**は、プロデューサーとコンシューマーの両方が従事する重要な操作であり [13] 、セキュリティ、ライセンス、非準拠、保守性 [2] [14] [15] に関連するリスクが含まれます。脆弱なコンポーネントをソフトウェアに組み込むことに関連するセキュリティリスクは、SBOM を分析する最も頻繁に引用される根拠の 1 つです [15]。セキュリティリスク分析では、SBOM で特定されたコンポーネントは、NIST 国家脆弱性データベース (**NVD**) またはその他のソースからアクセス可能なサードパーティコンポーネントの既知の脆弱性のリストと相互参照されます。リスク分析の結果は、組織内の他の人に送信される場合があります。たとえば、ソフトウェア・プロデューサーは、SBOM セキュリティ分析を使用して、独自のソフトウェアで脆弱なコンポーネントを発見し、ソフトウェア開発チームに修正のために通知できます。下流のサプライヤーからの SBOM [3] のコンシューマーとして機能する開発チームは、発見された脆弱性についてサプライヤーとそのチームの両方に警告することができます。リスク分析レポートは、購入の決定、法令遵守、ベンダーおよびサプライ チェーンのリスク管理に役立てることができる外部のコンシューマーと共有することもできます。

SBOM を**拡充**するプロセスは、追加の**レポート**や証明 [16] に必要な情報を SBOM に補足するために使用されます。たとえば、プロデューサは、ソフトウェアが特定の脆弱性の影響を受けない理由に関する声明や勧告を含めることができます。セキュリティ勧告は、Common Security Advisory Framework (CSAF) や Vulnerability Exploitability eXchange (VEX) [17]など、さまざまな形式で伝達されます。業界によっては、ソフトウェア・プロデューサが、規制コンプライアンス要件を満たすために、サポート終了 (EOL) またはサポート終了 (EOS) データを追加します。たとえば、米国食品医薬品局 (FDA) の医療機器・放射線保健センター (CDRH) は、NTIA の最小限の SBOM 要素に加えて、サポート ステータス、サポート終了日、およびサポート終了日 [18] を提供することを求めています。エンリッチメントはライフサイクル全体を通じて発生する可能性があり、SBOMを作成するプロデューサー、SBOMを保存および共有するサードパーティのプロバイダー、SBOMを受信するコンシューマー [5]、またはSBOM分析サービスを提供するサードパーティ組織によって実行される場合があります。

拡充されたSBOMは、コンシューマーと共有するために直接保存することも、他のSBOMとの調整やマージなどの追加操作の一部にすることもできます。各SBOMは、ソフトウェアの特定の時点におけるスナップショットです。SBOMは一度作成されると変更できないため、SBOMの内容を変更する処理は、更新されたSBOMではなく、適切な変更が加えられた新しい個別のSBOMを生成します。これは、特定の時点における最新のスナップショットです。

**SBOMのカスタマイズ**には、対象読者に合わせてSBOMの内容と形式をカスタマイズすることが含まれます。これは、補足データ、配布前にエンリッチドSBOMに含まれる推移的依存関係のレベル、または機密データ [14] などのコンテンツに影響を与える可能性があります。カスタマイズはいくつかの理由で行われる可能性があります。契約上の要件によって

特定のフィールドと形式が規定される場合があります。規制によって詳細レベルが規定される場合があります。例えば、EUのサイバーレジリエンス法（CRA）では、直接的な依存関係のみが要求されます。社内プロセスに役立つ情報のスーパーセットを含む社内用SBOMは、公開前に法務部門によって編集される場合があります。

**SBOMのリンク/マージ**（NSAではこれを集約と呼びます）は、SBOM同士を関連付け、共通システムの一部としてタグ付けするなど、比較的単純なものから複雑なものまであります。一方、システムSBOMは、それを構成するサブシステムのすべてのSBOMの階層から作成されます。例えば、自動車インフォテインメントシステムのマージSBOMには、ナビゲーションSBOM、メディアSBOM、車両機能SBOMが含まれ、これら3つのSBOMはそれぞれ多数の「子」SBOMで構成されている場合があります。階層的にマージされたSBOMは、「システムSBOM」、「SysBOM」、「製品SBOM」と呼ばれることもあります。

SBOMは、プロデューサーがコンシューマーにSBOMを電子メールで送信するなどの単純なものから、サードパーティのディストリビューター[19]、によって管理される**セキュアリポジトリ**にSBOMを公開し、適切に認証されたコンシューマー[20].がアクセスできるようにするなどの高度なソリューションまで、さまざまなメカニズムを通じて共有されます。

コンシューマーは様々な方法でSBOMから価値を得ます。最も最初の接点は、**ソフトウェアの購入または取得**の決定時でしょう。この時点で、コンシューマーは対象となるソフトウェアが組織にもたらす**リスク**（セキュリティ上の脆弱性、ソフトウェアコンポーネントのライセンス、出所、サポート可能性など）**を分析**できます。この情報は、組織の**法務、ガバナンス、ベンダー管理**などの部門と交換され、今回の購入に活用されるか、ソフトウェアのサプライヤーや正規販売代理店から将来購入する際のための参考資料として保存されます。これが新しいバージョン、または以前購入したソフトウェアの更新バージョンである場合、コンシューマーは新しいSBOMと古いSBOMを**比較**し、変更点を記録します。

購入後、SBOM はコンシューマーのソフトウェア インベントリの一部となり、コンシューマーは SBOM をクエリーして、インシデント対応の一環としての特定のソフトウェアコンポーネントの存在、コンポーネントの今後のサポート終了、脆弱性の悪用可能性ステータス、法令遵守のための出所データなどの貴重な情報を取得できます。

## 継続的な監視

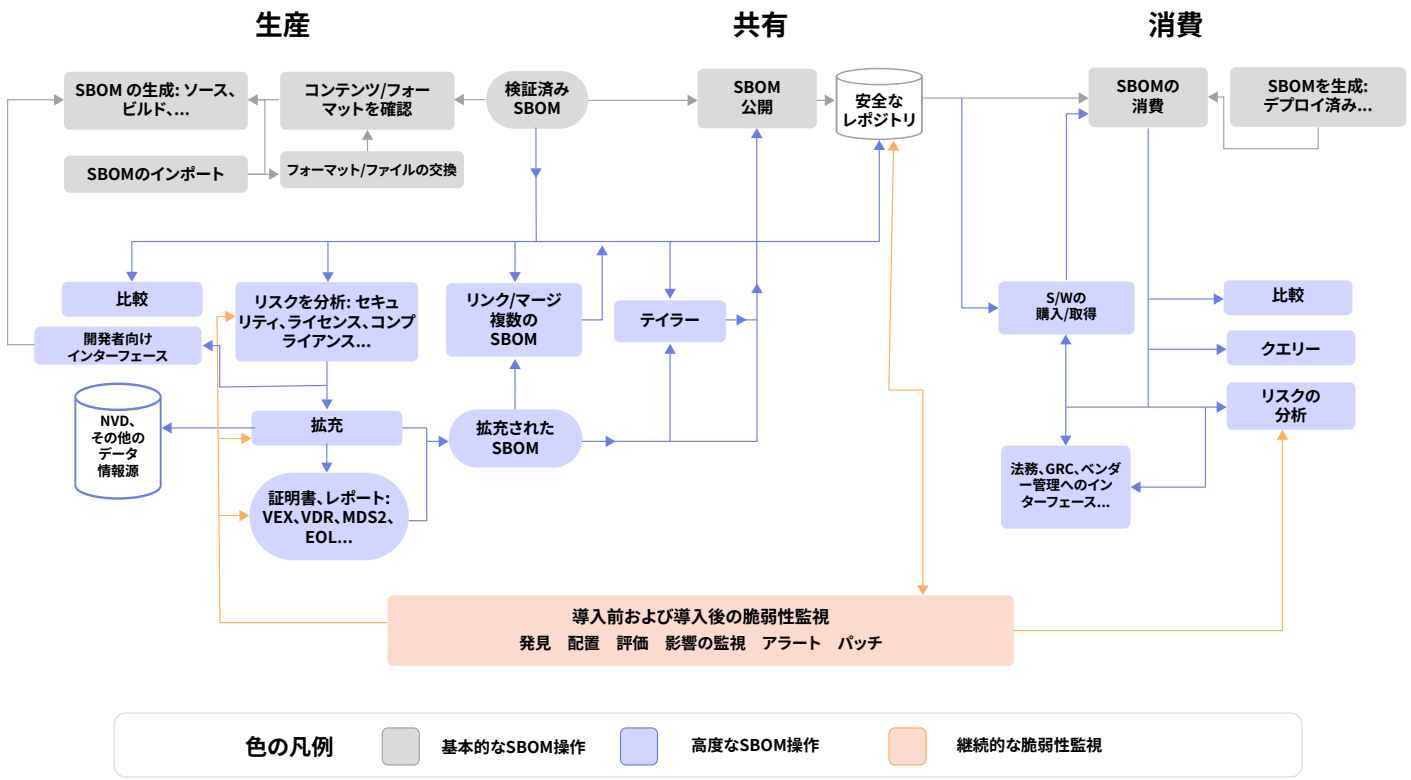
図4にオレンジ色で示されている SBOM ライフサイクル管理内の最も高度な操作は、SBOM で識別されたコンポーネントの**継続的な監視**に関連する操作です。

ソフトウェアのすべてのコンポーネントと依存関係を含むSBOMを活用すれば、セキュリティチームは、これらのコンポーネントがもたらすリスクが変化したかどうかを定期的に評価できます。具体的には、 NVDからの毎日の更新を通じてSBOMで特定されたコンポーネントにおける新たな脆弱性を**発見**すること、これらの脆弱性の悪用可能性、影響、および必要な修復措置を判断するための**処置**、リスク軽減のためのコンポーネントへの**パッチ適用**、SBOMリポジトリにおける新たな脆弱性の存在を**監視**すること、そして新たな脆弱性についてソフトウェアユーザーに**警告**することなどが挙げられます。NSAは、継続的な監視の基盤となる脆弱性追跡および分析の多くの運用について、「SBOM管理に関する推奨事項」[7]で説明しています。

**継続的な監視**は、SBOM のプロデューサー、SBOM を保存および配布するディストリビューター、および SBOM によって表されるソフトウェアを使用しているコンシューマーによって実行される場合があります。

図4

## 継続的な脆弱性監視




*SBOMライフサイクル管理は、専門的な実践と共通の責任へと発展しつつあります。データの拡充、複数のSBOMの統合、そしてカスタマイズを促進するツールとプロセスは、組織のソフトウェアガバナンス戦略においてますます中心的な位置を占めるようになるでしょう。これは将来的に自動化と拡張の機会が数多くある有望な分野です。*

# ユースケース

SBOM運用ワーキンググループは、個人や組織がリスク管理を支援するためにSBOMから価値を引き出す多くのユースケースについてブレインストーミングを行いました。ユースケースとして認められるためには、以下の2つの主要な基準を満たす必要がありました。

- これは、SBOMの初期生成と標準規格への準拠の検証後に、SBOMに対して、またはSBOMを用いて行われる活動について記述したものです。「SBOMは作成できたけど、次は何をすればいいの？」という問いに答えます。
- これらの活動は、組織に利益、価値、または洞察を提供することを目的として行われます。

2 番目の基準を満たすには、プロデューサーに関していくつかの重要な前提があります。

- プロデューサーは、SBOM がその形式の適切な仕様 (例: SPDX またはCycloneDXファイル)に準拠していることを確認しています。
- SBOM 内で表現されるデータは、データ要素の要件に基づいて正しくフォーマットされています (例: PURL 識別子は構文的に正しい)
- プロデューサーは、SBOM 署名などの SBOM の整合性を検証するための手段をコンシューマーに提供します。
- SBOM がコンシューマーに提供されると、その SBOM は不変になります。

現状では、SBOMの検証は一貫性を欠いており、SBOMの信頼性のある精度は未解決の問題であることは認識しています。しかしながら、ユースケースに焦点を当てるために、信頼性の高い検証、不変性、そして精度を前提としました。

脆弱性情報を必要とするワークフローで SBOM を使用する場合、プロデューサーが使用する脆弱性識別子が、コンシューマーに対して同じ脆弱性を一意に識別することが重要です。提示されたユースケースでは、「**脆弱性情報ソース**」という用語は、国家脆弱性データベース (NVD) や国固有の NVD などの共有の場所に保存される可能性のある CVE 識別子などの情報、または民間組織が GitHub セキュリティ アドバイザリ (GHSA) 識別子などの共有情報ソースを公開する場所を示すために使用されます。これらの識別子は、多くの場合、CISA 既知の悪用可能な脆弱性 (KEV) カタログやエクスプロイト予測スコアリング システム (EPSS) 情報などの追加または拡張された情報ソースへのインデックスとして機能します。ユースケースで使用される「脆弱性情報」という用語は、ユースケースの目的を文脈的に満たすために必要なすべての潜在的な情報を網羅する拡張的な用語です。

***ほぼすべてのSBOMプロデューサーは、SBOMコンシューマーでもあります。プロデューサーがコードベースに外部コンポーネントを組み込んでいる場合、コンシューマーの役割も担っていることになります。***

特定の脆弱性の潜在的影響範囲を判断する際にサードパーティの脆弱性情報源が有用な場合もありますが、特定のアプリケーションにおける悪用可能性や潜在的な緩和策に関するサプライヤーの主張に代わるものではありません。ここで紹介するユースケースでは、「**サプライヤーセキュリティアサーション**」という用語は、VEXステートメントや製品エラッタなど、サプライヤーが行う主張を指します。アサーションは、セキュ

リティまたはソフトウェアの「**アテステーション**」とは異なり、アテステーションとは、サプライヤーがソフトウェアが特定の標準規格や規制要件に準拠していることを示すアテステーションのことです。

プロデューサーとコンシューマーの役割は独立した組織間で発生すると考えるのが一般的ですが、そのようなアプローチはSBOMの有用性を人為的に制限してしまいます。ここで紹介したユースケースの多くは、固有の要件を満たすために単一の組織内で発生する可能性があります。SBOMを効果的に活用するための鍵の一つは、SBOMは特定の要件に合わせて変換、拡充、またはカスタマイズできること、そしてSBOMの内容を変更すると、プロデューサーの想定とコンシューマーの期待を満たす新しいSBOMが作成されることを認識することです。

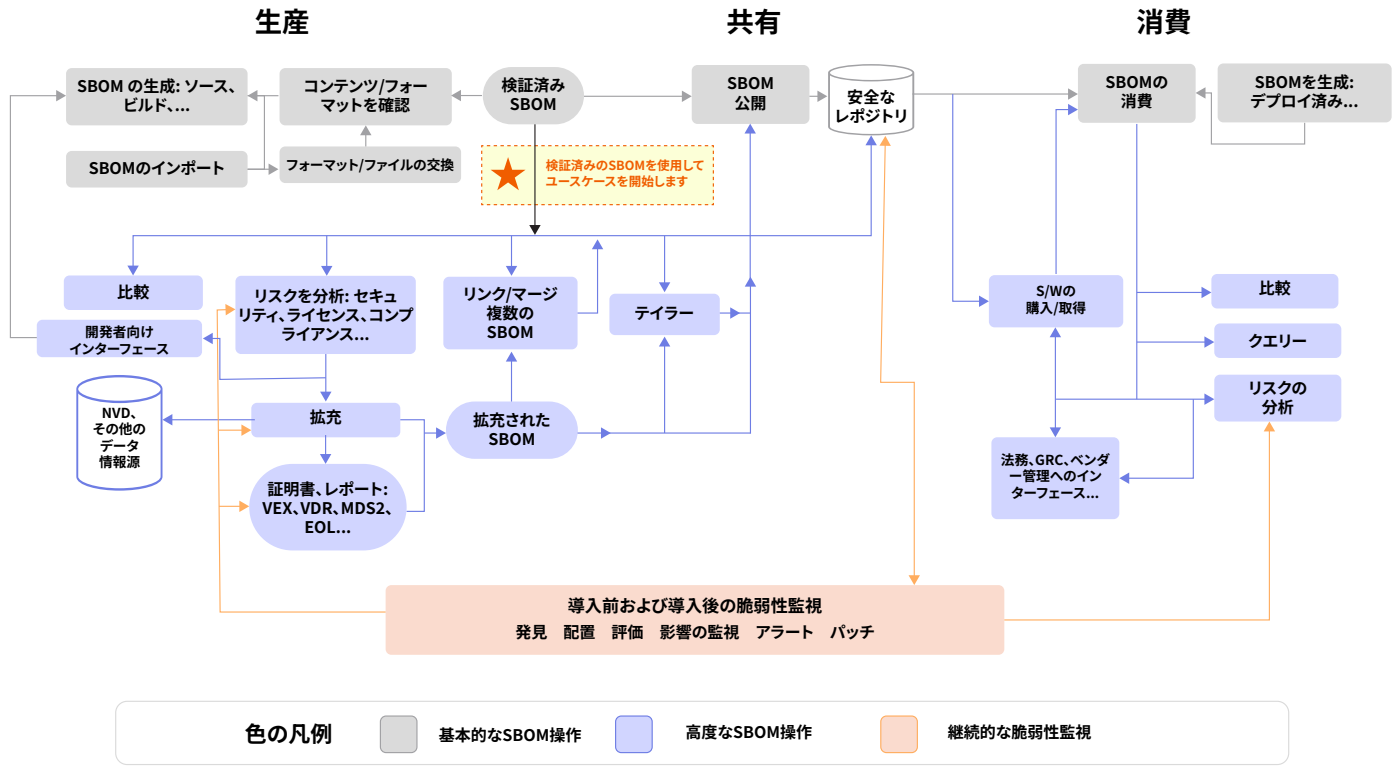
SBOMの送信または保存に関連するユース ケースも除外しました。SBOMライフサイクル ダイアグラム内では、ユース ケースは、**図5**に示すように、検証済み SBOM を受信した時点から始まり、その図に示されている基本的な SBOM 操作は除外されます。

グループは、より広範なユースケースセットから、SBOMライフサイクルの文脈における厳選された13のユースケースセットに絞り込みました。以下にリストアップします。これは、考えられるすべてのユースケースを網羅したリストではなく、SBOM運用ワーキンググループの専門家にとって最も馴染みのあるユースケースを反映しています。

ユースケースは、読者が組織内でそのユースケースに遭遇する可能性に基づいて、3 つのカテゴリに分類されています。この可能性は、ユースケースに対処するソリューションの成熟度と適用範囲の広さによって左右されます。たとえば、「導入前 CVE 脆弱性」ユースケースは、CVE データと SBOM フィールドを相互リンクするソリューションがすでに存在し、CVE 脆弱性は業種を問わずほぼすべての政府機関および商業組織に影響するため、最初のカテゴリに分類されます。「フィールド サービス ソフトウェア対応デバイスの SBOM サポート」ユースケースは、デバイスのビルド SBOM を現場のデバイスから直接収集された情報 (リモートで生成されたランタイム SBOM など) と比較するプロセス/テクノロジがまだ成熟しておらず、このユースケースに携わる業種が少ないため (医療技術、電子機器、エネルギー センサーなど)、3 番目のカテゴリに分類されます。

図5

## ユースケースは検証済みのSBOMから始まり、基本的なSBOM操作は除外される



**最も成熟した / 最も幅広い適用範囲**

1. **展開前の共通脆弱性識別子 (CVE) の脆弱性:**
   リリース前にソフトウェア製品の脆弱性を発見します。
2. **展開後の CVE 脆弱性：**リリース後のソフトウェア製品の脆弱性を検出します。
3. **ライセンスリスク：**外部開発コンポーネントのライセンスが組織にとってリスクとなるかどうかを判断します。これにはオープンソース・ソフトウェアとクローズドソース・ソフトウェアが含まれます。
4. **EOL およびメンテナンス対象外コンポーネントのアラート：**サポート終了が近いソフトウェアパッケージを特定して、アップグレードまたは交換を計画します。
5. **購入前のリスク評価：**購入または取得前にソフトウェアのリスクを評価します。
6. **組織全体でのコンポーネントの使用状況：**使用されているすべてのソフトウェア コンポーネントと、組織内でのそれらの普及状況を特定します。

**中程度に成熟 / 中程度の適用性**

7. **インシデント対応：**セキュリティ インシデントに関係するコンポーネントに依存するすべてのアプリケーションを特定します。
8. **合併と買収 (M&A) および投資リスク評価：**第三者による合併、買収、または投資の前に、対象ソフトウェアのリスクを評価します。
9. **アクセサリ ソフトウェアの検証：**すべてのアクセサリ コンポーネントがコア ソフトウェアの SBOM に含まれていることを確認し、アクセサリのセキュリティ、ライセンス、コンプライアンスのリスクを分析します。
10. **ビルドまたはバージョン間のコンポーネントの違い：**ソフトウェア ビルドまたはソフトウェア バージョン間でのコンポーネントの違いを確認します。

**成熟度が最も低い / 適用範囲が限定的**

11. **さまざまなガバナンス、規制、コンプライアンス (GRC)仕様への準拠：**SBOM またはソフトウェアインベントリのさまざまな規制および契約要件に準拠します。
12. **運用技術 (OT) と分離されたネットワークの整合性と脅威管理：**ネットワーク境界を越えたバージョンと依存関係の管理を標準化および合理化し、攻撃対象領域やその他のリスクを最小限に抑えます。
13. **ソフトウェア対応デバイスのフィールドサービス：**メンテナンスとトラブルシューティングを支援するために、フィールドサービス担当者は、デバイスの以前に生成されたSBOMと、運用中に展開されたデバイスから収集されたデータを比較します。

図6 は、ユースケースをこれら 3 つのカテゴリ別に整理し、プロデューサー、コンシューマー、またはその両方に対する関連性を示しています。

図6

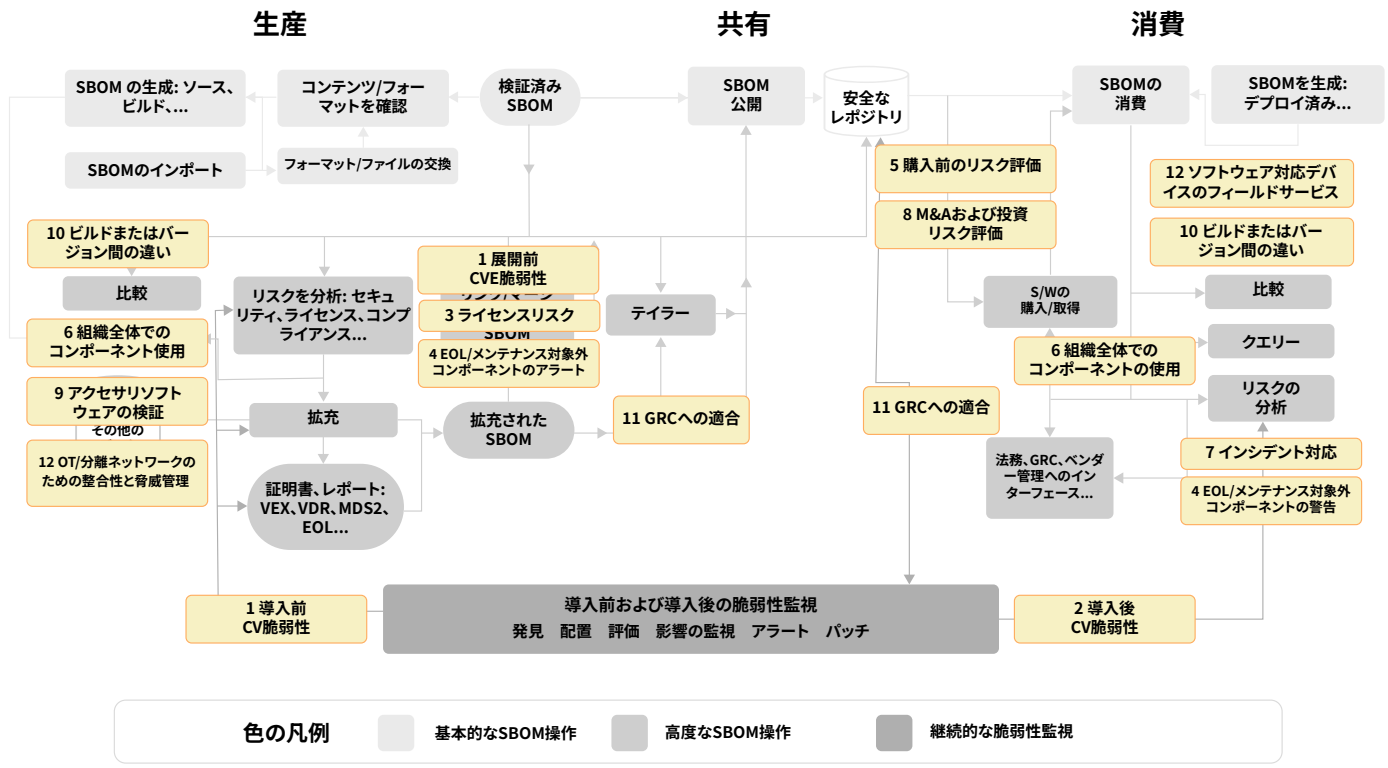
## 成熟度/適用性および利害関係者の役割別にグループ化されたユースケース

| ユースケース # | 成熟度 / 適用性 | 役割 | |
|---|---|---|---|
| | **最も成熟した / 最も幅広い適用範囲** | **プロデューサー** | **コンシューマー** |
| 1 | 導入前のCVE脆弱性 | ✗ | |
| 2 | 導入後のCVE脆弱性 | | ✗ |
| 3 | ライセンスリスク | ✗ | ✗ |
| 4 | EOLおよびメンテナンス対象外コンポーネントの警告 | ✗ | ✗ |
| 5 | 購入前リスク評価 | | ✗ |
| 6 | 組織全体でのコンポーネントの使用状況 | ✗ | ✗ |
| | **中程度に成熟 / 中程度の適用性** | | |
| 7 | インシデント対応 | | ✗ |
| 8 | M&Aおよび投資リスク評価 | | ✗ |
| 9 | アクセサリソフトウェアの検証 | | ✗ |
| 10 | ビルドまたはバージョン間のコンポーネントの違い | ✗ | ✗ |
| | **成熟度が最も低い / 適用範囲が限定的** | | |
| 11 | 異なるGRC仕様への準拠 | ✗ | ✗ |
| 12 | OTおよび分離されたネットワークの整合性と脅威管理 | ✗ | |
| 13 | ソフトウェア対応デバイスのフィールドサービス | ✗ | ✗ |

これらのユースケースは、図7に示すように、SBOM ライフサイクル ダイアグラムにもマッピングされます。

図7

## SBOMライフサイクル図にマッピングされたユースケース



これらのユースケースそれぞれについて、グループは簡潔な説明文と、ユースケースをさらに詳細に説明する7つの属性からなる表を作成しました。これらの属性は、アクター、ビジネス上の動機、機能目標、目標達成のためのステップ、NTIAフィールド [10]追加または相互リンクされたデータ、そして達成されたメリットです。

各ユースケースは個別に提示されていますが、グループは多くのユースケースが相互に関連していることを認識しています。たとえば、展開後のCVE 脆弱性に関するユースケースは、単独で存在することも、購買決定や M&A および投資リスク評価の一部となることもできます。

## ユースケース: 導入前のCVE脆弱性

ソフトウェアメーカーは、自社製品が既知かつ対処可能なセキュリティリスクに晒されていないことを保証または証明する必要があります（例えば、リリース前にセキュアソフトウェア開発フレームワーク（SSDF）への準拠を証明するなど）[21]。市場投入前の段階では、SBOMはソフトウェアおよびファームウェアにおけるサイバーセキュリティリスクを管理するための基盤ツールとして機能します。SBOMを脆弱性情報と組み合わせて使用することで、ソフトウェアメーカーは脆弱性を体系的に特定し、計画中の製品に対して分析を行うことができます。この分析は、製品が市場に投入された後にエクスプロイトの可能性を最小限に抑える、または排除するための、新たな設計要件、サプライヤー管理、テストなどの潜在的な対策を推進します。この活動は、規制当局への申請を支援し、市場参入を容易にし、購入者に一定の信頼を提供します。この分析の文書化は、セキュリティ証明を裏付ける証拠として役立ちます。関連するセキュリティ情報を積極的に共有することで、ソフトウェアメーカーは透明性を高め、説明責任を実証し、サプライチェーン全体にわたる情報に基づいた意思決定を支援することができます。

表 1 では、このユースケースの主な属性について説明します。

**表1**

### ユースケース: 導入前のCVE脆弱性

| | |
|---|---|
| アクター | 部品、規制、エンジニアリング、製品セキュリティチーム |
| ビジネスモチベーション | ソフトウェア製品の未対処の脆弱性によるソフトウェア製作者へのリスクと責任を最小限に抑える |
| 機能目標 | ソフトウェアのリリース前に脆弱性を発見し、ソフトウェア製品のリスクに対処する |
| 目標を達成するためのプロセスまたは手順 | SBOM コンポーネントを、NVD、GitHub セキュリティ アドバイザリ、その他の信頼できるリポジトリなど、さまざまなソースからの脆弱性情報と相互参照します。 |

| | |
|---|---|
| 目標を達成するためのプロセスまたは手順 | 各コンポーネントに関連するCVEを特定し、さらに分析するために文書化します。<br>製品に統合されているサードパーティ製ソフトウェアのサプライヤー提供の脆弱性評価レポートを確認する<br>脆弱性情報やコンポーネントの依存関係などの他の要因に基づく受け入れ基準とリスクスコアリング要因に基づいて、リスクを評価し、脆弱性の優先順位を決定<br>脆弱性を修正するには、セキュリティ制御を実装し、未使用または必須でないコンポーネントにパッチを適用または削除します。<br>修復に大幅な変更が必要な場合は、製品の設計または実装を再評価し、新たなリスクを導入することなく脆弱性が効果的に対処されていることを確認します。<br>修復後に脆弱性評価を実施し、特定されたすべての脆弱性が軽減され、新たな脆弱性が導入されていないことを確認します。<br>脆弱性に対処するために講じたすべての手順を記録します。これには、特定の脆弱性が対処されないままの場合のリスク受け入れの根拠も含まれます。<br>必要に応じて、脆弱性管理アクションと実施されたリスク軽減措置に関する最新情報を利害関係者、顧客、または規制当局に提供します。 |
| NTIA使用フィールド | サプライヤー、コンポーネント名、コンポーネントのバージョン、その他の一意の識別子、依存関係 |
| 追加または相互リンクされたデータ | 脆弱性情報源<br>サプライヤーセキュリティアサーション（例：VEX）と脅威モデルの洞察 |
| 達成されたメリット | 発見された脆弱性に基づいて、展開および現場での使用前に製品ソフトウェアが可能な限り安全であることを確認します。<br>プロデューサーの責任を最小限に抑えます。<br>ソフトウェア調達者が要求する可能性のあるセキュリティ認証とセキュリティ アドバイザリをサポートします。 |

## ユースケース: 導入後の CVE 脆弱性

ソフトウェアの導入後、ソフトウェアのライフサイクル全体を通じてセキュリティリスクを軽減するために、プロデューサーとコンシューマーの両方にとって継続的な脆弱性監視が不可欠になります。新たな脆弱性は継続的に発見されるため、SBOMで特定されたソフトウェアコンポーネントをNVDに保存されているCVEに対して定期的にスキャンすることは、コンシューマーが悪用される前に実行できる重要な予防措置となります。

定期的なスキャンに加え、コンシューマーのセキュリティ、IT、コンプライアンスチームは、導入後のセキュリティ運用にSBOM監視を積極的に統合できます。これには、新たに発見された脆弱性に関するアラートの自動化、導入済みシステムへの潜在的な影響の評価、悪用可能性、ソフトウェアの依存関係、重要なシステムの露出といった現実的なリスク要因に基づいた修復作業の優先順位付けなどが含まれます。

プロデューサーのエンジニアリングチームまたは製品セキュリティチームは、ソフトウェア製品のライフサイクル全体を通じてこれらのリスクを検出し、軽減するための継続的なプロセスに従事する役割を担う場合があります。適切に管理されたSBOMを活用することで、プロデューサーは特定のコンポーネントにおける脆弱性を追跡し、的を絞った修復活動と効率的なリソース配分が可能になります。SBOMを協調的脆弱性開示システムと組み合わせることで、プロデューサーはコンシューマーに通知し、ソフトウェアまたはファームウェアにおける脆弱性の悪用の可能性を低減または排除するためのアップデートを提供できます。

ソフトウェア・プロデューサーとコンシューマーは両方とも、SBOM と CVE データベースとの定期的な相関関係と一貫したコミュニケーションを通じて、導入されたソフトウェア製品の新しい脆弱性によるリスクを軽減し、導入されたソフトウェアの信頼を構築します。

プロデューサーとの継続的なフィードバック ループを維持することにより、コンシューマーはセキュリティ アドバイザリ、パッチ、または緩和策を迅速に受け取ることができ、展開されたソフトウェアが安全で、準拠しており、新たな脅威に対して耐性があることを保証できます。

表 2 では、このユース ケースの主な属性について説明します。

**表2**

## ユースケース: 導入後のCVE脆弱性

| | |
|---|---|
| アクター | リスク/コンプライアンス担当者、規制、エンジニアリング、セキュリティチーム、製品セキュリティチーム（PSIRT）、コンシューマーセキュリティチーム（CSIRT） |
| ビジネスモチベーション | 市場で安全な製品を維持し、規制遵守を維持し、高額な費用や評判低下につながる事態を回避する。 |
| 機能目標 | 新しい CVE が展開されたソフトウェアのソフトウェア コンポーネントにどのような影響を与えるかを確認する。<br>導入されたソフトウェアにおける新たな脆弱性のセキュリティとコンプライアンスのリスクを評価する。 |

| | |
|---|---|
| 目標を達成するためのプロセスまたは手順 | 正確なSBOMを維持する。<br>プロデューサー - 組織がすべての製品に対して正確な SBOM を生成し、維持していることを確認する。<br>コンシューマー - ソフトウェアプロバイダーに依存している場合は、リリース、アップデート、パッチごとに正確なSBOMを提供するように要求する。<br>脆弱性評価レポートを確認する。<br>製品に統合されたサードパーティソフトウェアのサプライヤーから提供される脆弱性レポートを分析する。<br>サードパーティのスキャンツールの結果でこれを補う。<br>定期的な脆弱性監視を実行する。<br>SBOM 内のコンポーネントに関連する新しい脆弱性を特定するために、脆弱性情報ソースを定期的に監視する。<br>情報共有分析組織（ISAO）、脅威インテリジェンスフィード、セキュリティアドバイザリからのサイバーセキュリティシグナルを監視し、脆弱性と脅威の傾向に関する最新情報を常に把握する。<br>新たに特定されたCVEをSBOMコンポーネントにマッピングする。<br>発見された脆弱性を製品の受け入れ基準に照らして評価する。<br>必要に応じて、封じ込め、アップデート/パッチ、補償制御、報告またはリコールの決定に関連する決定を下す。 |
| NTIA使用フィールド | サプライヤー、コンポーネント名、コンポーネントのバージョン、その他の一意の識別子、依存関係 |
| 追加または相互リンクされたデータ | 脆弱性情報源<br>サプライヤーセキュリティアサーション（例：VEX）<br>実行時データを含む在庫システム |
| 達成されたメリット | ソフトウェア プロデューサーとコンシューマーは、NVD に投稿された新しい CVE の影響を受ける可能性のある、展開されたソフトウェア製品のセキュリティとコンプライアンスを維持する。 |

| | |
|---|---|
| 達成されたメリット | プロデューサーとコンシューマーのサポート機能は、新しい脆弱性が悪用される前に、適切なアクションを実行して、脆弱性を封じ込め、軽減し、報告することができる。 |

## ユースケース: ライセンスリスク

ソフトウェアは、著作権法を含む様々な法律の規制を受けます。外部で開発されたソフトウェアコンポーネントを組み込む場合、そのソフトウェアコンポーネントが意図された用途および配布方法において合法的に組み込めることが極めて重要です。実質的には、許可（ライセンス）が必要です。

例えば、研究によると、現代のソフトウェアアプリケーションは平均して70% [31] から 90% [32] がオープンソース・ソフトウェア (OSS) であることが示されています。これは、OSSが典型的な現代のアプリケーションの開発に不可欠であり、インフラストラクチャからエンドユーザー機能まですべてを駆動していることを意味します。ただし、外部で開発されたコンポーネントと同様に、OSSコンポーネントは、特に再配布されたソフトウェアに対して重大な法的および運用上の義務を課す可能性のあるさまざまなライセンス要件を導入します。たとえば、保護ライセンス (コピーレフトライセンスなど) では、実行可能ファイルを配布するときに、受信者にソースコード (場合によっては実行可能ファイル全体) を受け取るオプションを提供する必要があります。保護ライセンスを持つコンポーネントを含めることは、意図された使用と配布に応じて、深刻な問題になるか、まったく問題にならない可能性があります。

OSSだけがライセンスの問題を引き起こす可能性があると想定するのは間違いです。クローズドソース・ソフトウェア（CSS）とは、OSSとしてライセンスされていない外部で開発されたソフトウェアのことです。CSSを合法的に使用するには、そのライセンスに従うことも必要です。CSSの販売者がコピーごとにロイヤルティの支払いを要求する場合があり、ライセンスが追跡されていない場合、CSSライセンスに違反しやすくなります。CSSライセンスに従わなかった場合に裁判所が科す罰則は、特に販売者が法務チームを抱え、不正使用を特定してライセンス条項を強制適用するために熱心に取り組んでいる場合には、非常に厳しいものになる可能性があります。さらに、OSSプロジェクトでは通常、CSSを含む貢献が禁止されています。CSSの特殊なケースとして、ライセンスが全くない無許可ソフトウェアがあります。状況によっては、そのようなソフトウェアを組み込むことが許可されない場合があります。

このユースケースは、SBOMをアプリケーション内のすべてのソフトウェアコンポーネントとそれぞれのライセンスの包括的なインベントリとして活用することで、ライセンスリスクを効果的に管理する方法を示しています。ライセンスの詳細、完全なライセンステキスト、著作権情報（NTIA最小要素準拠のSBOMには含まれていない可能性のある要素）を含む充実したSBOMは、ライセンス管理に必要な追加のアーティファクトを提供できます。クローズドソースの場合、詳細なライセンステキストがなくても、クローズドソースであることを示すだけでも価値があります。

SBOMをライセンスデータベースと統合し、組織のライセンスポリシーと整合させることで、ライセンス上の競合を積極的に特定・軽減し、コンプライアンス義務を追跡し、法的リスクをもたらす可能性のあるライセンス条件の変更に対処できるようになります。この構造化されたアプローチにより、法務、開発、コンプライアンスの各チームが効果的に連携し、ライセンス要件の遵守を徹底し、法的リスクを最小限に抑え、安全でコンプライアンスに準拠したソフトウェアサプライチェーンを構築できます。

表 3 では、このユース ケースの主な属性について説明します。

表3

## ユースケース: ライセンスリスク

| | |
|---|---|
| アクター | 法務・コンプライアンスチーム、オープンソース・プログラムオフィス（OSPO）、エンジニアリング/開発チーム、調達オフィス、セキュリティチーム、経営/管理チーム |
| ビジネスモチベーション | 不適切にライセンスされたコンポーネントに関連する法的リスクから会社を保護する。 |
| 機能目標 | すべての関係者が、外部で開発されたソフトウェアを合法的に共同で管理できるようにする。<br>使用中のさまざまなライセンスの遵守とコンプライアンスを確保し、高額な法的罰則や違反を回避する。<br>ライセンスの競合を識別するためにソフトウェア サプライ チェーンの可視性を提供する。 |
| 目標を達成するためのプロセスまたはステップ | 許容されるライセンスの種類、使用制限、コンプライアンス義務など、組織の OSS ライセンス ポリシーの特定の要件を決定する。<br><br>ソフトウェアサプライチェーン内の異なるコンポーネント間で使用されている様々なライセンスの互換性を確認する。この手順により、互換性のないライセンス条項を持つコンポーネントを組み合わせることで発生する可能性のある競合を回避できる。<br><br>ライセンス条件の変更、特定のライセンスに関連する法的リスクの発見に基づいて、外部で開発されたコンポーネントを更新または置き換える必要があるかどうかを判断する。<br><br>ソフトウェア リリース バージョンの配布に使用されているライセンスを識別する。<br><br>ライセンス データベースを活用して、SBOM にリストされている各コンポーネントに関連付けられているソフトウェア ライセンスを識別する。<br><br>独自のコードに義務を課す可能性のある制限的なライセンスや、ソースコードの開示を必要とするライセンスなど、潜在的なライセンス リスクを特定する。 |

| | |
|---|---|
| 目標を達成するためのプロセスまたはステップ | 外部で開発されたコンポーネントを組み込んだソフトウェア、特に再配布される製品に対する法的義務とコンプライアンス義務を特定する。 |
| NTIA使用フィールド | サプライヤー、コンポーネント名、コンポーネントのバージョン、その他の一意の識別子、依存関係 |
| 追加または相互リンクされたデータ | SPDX [22]、OSI [23]、または ecosystem.ms [24] データベースによって維持されているライセンスデータベース |
| 達成されたメリット | SBOMのライセンスデータに基づき、組織を潜在的な法的リスクから保護するために法務チームが取るべき具体的なアクションを提供する。これには、コンポーネントの更新、交換、ライセンスの競合解決に関するポリシーの設定が含まれる。<br>ソフトウェア ベンダーと社内チームが確立されたライセンス要件とポリシーに準拠していることを確認する。 |

## ユースケース: サポート終了 (EOL) およびメンテナンス対象外コンポーネントのアラート

サポート終了（EOL）とは、サプライヤーが決定する指定であり、特定の製品またはバージョンの保守を終了するという組織的な正式かつ明確な決定を反映しています。この指定は、ベンダー（製品ベンダーとプロフェッショナルサービス企業の両方を含む）と顧客の間に存在する法的および契約上の義務の文脈で理解される必要があります。

EOLデータソースは公開されていません（つまり、この情報は企業のウェブサイトやセキュリティアドバイザリに掲載されています）が、組織は独自にこのデータを作成し、監視する責任があります。コンポーネントとそのバージョンに関するEOL情報（https://endoflife.date/などの情報源を参照）を取得したら、組織はこの情報をSBOMと組み合わせて使用することで、EOLステータスが近いソフトウェアコンポーネントを特定し、アップグレード、移行、またはセルフメンテナンスを計画することができます。

オープンソースのパッケージやソフトウェアコンポーネントに関して、「EOL」は「メンテナンスされていない」、つまりパッケージが放棄されたという意味でよく使われます。よく使われているライブラリのバージョンのように、明示的に「EOL」とマークされたプロジェクトと、メンテナンスが終了したプロジェクトには違いがあります。ライブラリのEOLバージョンには、移行可能な新しいバージョンが存在する可能性があります。メンテナンスされていないプロジェクトには、明確かつ容易な代替手段がない可能性があります。メンテナンスされなくなったオープンソース・コンポーネントの場合、セルフメンテナンスを利用することは妥当な選択肢となる可能性があります。

非メンテナンスは、ソフトウェアセキュリティ、運用リスク、そして統合コストの観点から重要です。EOLとは異なり、アクティブメンテナンスのしきい値はコンシューマーによって定義され、SBOM分析の文脈で管理されます。

プロデューサーの開発チームにとって、コンポーネントのメンテナンス状

況に関するSBOM分析は、これらのコンポーネントの使用をリクエストしているチームに早期のフィードバックを提供し、使用を最小限に抑えるか、パッケージを早期にアップデートするかを決定します。コンシューマーにとって、SBOM分析はソフトウェアのEOL（サポート終了）またはメンテナンス終了のトリガーを特定し、サポート対象外ソフトウェアの置き換えやセルフメンテナンスのためのリソース割り当てを計画するために活用できます。

表 4 では、このユース ケースの主な属性について説明します。

**表4**

## ユースケース: EOLおよびメンテナンス対象外コンポーネントのアラート

| | |
|---|---|
| アクター | セキュリティ/コンプライアンス/リスク管理、エンジニアリング/開発チーム、プログラム マネージャー、オープンソース・プログラム オフィス (OSPO)、調達オフィス (商用コンポーネント用) |
| ビジネスモチベーション | 使用の廃止とリスク軽減の計画 |
| 機能目標 | ソフトウェア コンポーネントがサポート終了 (EOL) に近づくと、製品やサービスがその前にコンポーネントをアップグレードまたは交換できるほど早めに警告する。<br>コンポーネントがアクティブにメンテナンスされていない場合は、アップストリームの貢献、フォーク、バックポートのいずれかによってコンポーネントを更新するか、コンポーネントのアクティブなメンテナンスに参加できるほど早い時期に警告する。 |
| 目標を達成するためのプロセスまたはステップ | サプライヤーからの連絡、リリース サイクル、または一般的な観察に基づいて、特定のコンポーネントの EOL 日付を設定する。<br>製品またはサービスのリリース サイクル内で EOL イベントを計画する。<br>アップグレードによって発生する可能性のある問題に備えた計画を立てる。<br>コンポーネントのアクティブメンテナンスのしきい値を決定する。 |
| NTIA使用フィールド | サプライヤー、コンポーネント名、コンポーネントのバージョン、依存関係、タイムスタンプ |
| 追加または相互リンクされたデータ | 製品EOLステータスデータ<br>脆弱性情報源 |

| | |
|---|---|
| 達成されたメリット | ソフトウェアのアップグレードによる予期せぬダウンタイムを削減<br>ソフトウェア製品の耐障害性の向上 |

## ユースケース: 購入前のリスク評価

ソフトウェアを購入または取得する前に、組織内の様々な関係者（購買担当者、契約担当者、リスク管理担当者、ネットワーク管理者、法務担当者など）は、対象となるソフトウェアが組織にリスクをもたらすかどうかを判断する必要がある場合があります。ソフトウェアのSBOMを分析し、SBOMデータを他の一般的な情報源と相互参照することで、ソフトウェア導入時に組織が引き継ぐ可能性のあるセキュリティ、ライセンス、コンプライアンス、保守性に関する潜在的なリスクを明らかにすることができます。この分析により、組織は購入前にこれらのリスクを軽減する機会を得ることができ、リスクへの露出を減らすことができます。

さらに、組織のセキュリティ、リスク、またはベンダーコンプライアンスチームは、同じベンダーから提供された複数の SBOM (異なるソフトウェアアプリケーションまたは同じアプリケーションの異なるバージョン) の分析から得た情報を使用して、ベンダーのソフトウェアの進化するリスク レベル、そのリスクが時間の経過とともに増加しているか減少しているか、追加の軽減策が必要かどうかを評価できます。

表 5 では、このユース ケースの主な属性について説明します。

***サプライヤーSBOMの集中リポジトリは、組織内の複数の利害関係者やユースケースに対応します。これにより、重複した作業を削減できます。一貫したリスクスコアリングを促進します。***

**表5**

## ユースケース: 購入前リスク評価

| | |
|---|---|
| アクター | 調達、購買、契約担当者、リスク/コンプライアンス担当者、法務、セキュリティチーム、ネットワーク防御担当者 |
| ビジネスモチベーション | 購入または取得を検討しているソフトウェアによって組織に新たなセキュリティ、コンプライアンス、またはサポート性のリスクが導入されないようにする。 |

| | |
|---|---|
| 機能目標 | 取得するソフトウェアのセキュリティリスクを評価する。<br>取得するソフトウェアのライセンスリスクを評価する。<br>サプライヤーのSBOMを要求する規制に準拠する。<br>同じベンダーから提供される複数の SBOM に基づいてベンダー リスクを評価する。<br>新しいソフトウェアの取得に伴うリスクを軽減するための緩和策を特定する。 |
| 目標を達成するためのプロセスまたはステップ | SBOMで識別されたコンポーネントを使用して、対象ソフトウェアの脆弱性を発見する。<br>脆弱性が組織にリスクをもたらすかどうかを判断する。<br>リスクを軽減するための緩和策を決定する。<br>対象ソフトウェアのコンポーネントに関連付けられたライセンスを識別する。<br>ソフトウェアライセンスに関連するリスクを特定する。<br>保守性、信頼性、互換性に関連する将来のリスクをもたらすソフトウェア コンポーネントのサポート終了 (EOL) に関する考慮事項があるかどうかを判断する。<br>制裁対象または禁止されているサプライヤーから供給された部品があるかどうかを確認する。<br>SBOMを活用して潜在的な取得ソフトウェアのリスクスコアリングを実施し、そのリスクレベルを評価する。<br>同じベンダーが提供する複数の SBOM からの情報をベンダー リスク スコアへの入力として使用する。 |
| NTIA使用フィールド | サプライヤー、コンポーネント名、コンポーネントのバージョン、<br>その他の一意の識別子、依存関係、著者<br>SBOMデータ、タイムスタンプ |
| 追加または相互リンクされたデータ | EOL<br>ライセンス<br>所有権および支配権に関する情報 |

| | |
|---|---|
| 追加または相互リンクされたデータ | 米国連邦通信委員会の対象事業体リストなどの制裁リスト [25]<br>脆弱性情報源 |
| 達成されたメリット | 購買担当者に対象ソフトウェアのリスクを評価するための情報を提供し、サプライヤーとリスク軽減の話し合いを行う。<br>リスク評価プロセスを通知するために、購買担当者が法務担当者やリスク/コンプライアンス担当者に配布するための情報を提供する。<br>リスク軽減策を特定する。 |

## ユースケース: 組織全体でのコンポーネントの使用

組織は、エンジニアリング、セキュリティ、コンプライアンス、法務などの機能をサポートするために、ソフトウェア資産インベントリを管理しています。SBOMは、これらの資産インベントリを各ソフトウェアアプリケーションを構成するコンポーネントレベルまで拡張します。組織はこのコンポーネントレベルのインベントリを使用することで、組織全体でよく使用されるソフトウェアコンポーネントを特定し、それらの普及が組織のセキュリティと運用効率に与える影響を評価できます。

例えば、一般的に使用されているコンポーネントがゼロデイ脆弱性や悪用された脆弱性に関連付けられた場合、セキュリティ部門とエンジニアリング部門による修復には、組織内でその脆弱なコンポーネントに依存するすべてのソフトウェアアプリケーションに関する知識が必要となります。また、一般的に使用されているコンポーネントのサポートが信頼できないことが判明した組織は、そのコンポーネントのメンテナンスのためにエンジニアリングリソースを積極的に割り当てる場合があります。

SBOM は、エンジニアリング、セキュリティ、インシデント対応、コンプライアンス、およびその他の組織機能が分析して脆弱性、ライセンス、サポート終了 (EOL) またはサポート終了 (EOS) などの情報と相関させ、よく使用されるコンポーネントからのリスクを評価し、それらの軽減、修復、継続的なサポートを効率的に計画できる初期コンポーネント インベントリを提供します。

表 6 では、このユース ケースの主な属性について説明します。

***組織はSBOMのコンポーネントレベルのインベントリを使用して、よく使用されるコンポーネントを特定できます。組織全体のソフトウェアコンポーネントを監視し、その普及が組織のセキュリティと運用効率に与える影響を評価します。***

表6

## ユースケース: 組織全体でのコンポーネントの使用

| | |
|---|---|
| アクター | エンジニアリング管理、セキュリティインシデント対応、監査、コンプライアンス、ガバナンス、リスク管理 |
| ビジネスモチベーション | 資産管理、長期リスクの評価 |
| 機能目標 | 複数のソフトウェア システムまたは組織全体にわたるセキュリティとライセンスのリスクを評価する。<br>組織全体のコンプライアンスとリスク軽減の進捗状況を評価する。<br>組織内で特定のコンポーネントまたはシステムを採用することによって発生する長期的なリスクを評価する。 |
| 目標を達成するためのプロセスまたはステップ | 組織内で使用されているすべてのソフトウェア アプリケーションに取り込まれた SBOM を特定する。<br>組織全体で最も一般的に使用されているソフトウェア コンポーネントを特定する。<br>複数のソフトウェア システムに影響を与えるソフトウェア コンポーネントのセキュリティ、ライセンス、または EOL の問題を特定する。<br>異なるバージョンのソフトウェア コンポーネントの普及状況を特定する。<br>同様の目的を果たすさまざまなコンポーネントの普及状況を特定する。<br>複雑なシステム全体にわたる脆弱なコンポーネントの増殖を特定する。<br>組織内の重要なソフトウェア コンポーネントを特定する。<br>EOLとなったコンポーネントを特定する。 |
| NTIA使用フィールド | サプライヤー、コンポーネント名、コンポーネントのバージョン、<br>その他の一意の識別子、依存関係 |
| 追加または相互リンクされたデータ | EOL<br>ライセンス |

| | |
|---|---|
| 追加または相互リンクされたデータ | 脆弱性情報源<br>実行時データを含む在庫システム |
| 達成されたメリット | エンジニアリング管理に、管理下にある複数のソフトウェア システムに影響を与えるコンポーネントを理解する能力を提供する。<br>広範囲にわたるソフトウェア コンポーネントを維持するために、どこにさらにリソースが必要なのかを計画するための洞察をエンジニアリング管理に提供する。<br>監査およびコンプライアンス担当者に、ソフトウェア コンポーネントに関する調査結果が組織に与える影響についての理解を提供する。<br>脆弱なコンポーネントに関連するインシデントの規模と影響についての情報をインシデント対応担当者に提供する。 |

## ユースケース: インシデント対応

SBOM（ソフトウェア部品表）は、インシデントの特定、封じ込め、修復を迅速化することでインシデント対応プロセスを大幅に強化し、最終的には組織全体のセキュリティ体制とレジリエンス（回復力）を向上させることができます。インシデント対応チームは、SBOMを構成管理データベース（CMDB）やセキュリティインシデントイベント管理（SIEM）ツールにインポートするなどしてSBOMポートフォリオを分析し、環境内のどのシステムやアプリケーションが脆弱なコンポーネントの影響を受けているかを特定したり、サプライヤーのサイバーセキュリティ認証においてサプライヤー間で共通する脆弱性が指摘されている箇所を特定したりすることができます。

例えば、セキュリティインシデントの原因が特定のコンポーネントの脆弱性である場合、SBOMリポジトリは新しい脆弱性をプロアクティブに警告し、簡単にスキャンまたはクエリを実行して、脆弱なコンポーネントをアクティブに使用しているすべてのアプリケーションを特定できます。このプロセスにより、特定と修復の作業が簡素化され、分析と調査の平均検出時間（MTTD）が大幅に短縮されます。これらのタスクを効率化することで、組織はリソースコストを削減し、より効果的に労力を配分し、影響を受ける脆弱なアプリケーションへの優先順位付けと対処をより効率的に行うことができます。

さらに、組織は SBOM を使用して、影響を受けるシステムを隔離したり、脆弱性の影響を軽減するために一時的な保護手段を展開したりするなど、インシデント対応プロセスの一環として即時に実行可能な手順を実施できます。

SBOMは、セキュリティ研究者、ソフトウェア発行者、脆弱性コーディネータ間の連携のための標準化されたフレームワークを提供することで、インシデント対応活動をさらに改善します。この共通言語は、CVEステータスの共有を含む脆弱性に関する効果的なコミュニケーションと開示を促進し、セキュリティ問題のより迅速かつ正確な解決を可能にします。

表 7 では、このユース ケースの主な属性について説明します。

表7

## ユースケース: インシデント対応

| | |
|---|---|
| アクター | 実施チーム：インシデント対応、エンジニアリング/開発、 DevSecOpsおよびIT、セキュリティ、法務および規制 |
| ビジネスモチベーション | サイバーセキュリティインシデントに迅速かつインテリジェントに対応する。<br>事故によるビジネスへの影響を最小限に抑える。<br>積極的かつ効果的な行動を通じてリスクを最小限に抑える。<br>脆弱性の検出と対処にかかる平均時間の改善。<br>インシデント対応に関連する財務コストを削減する。<br>対応作業を効率化することでリソースを節約する。 |
| 機能目標 | セキュリティインシデント対応チームに権限を与え、脆弱なコンポーネントとその使用によって影響を受けるシステムを迅速に特定できるようにする。<br>ソフトウェア エンジニアやサイバー防御者が脆弱性を修正するために迅速かつ効果的なアクションを実行できるようにする。 |
| 目標を達成するためのプロセスまたはステップ | 影響を受けるシステムの SBOM から根本原因のコンポーネントとバージョンを特定する。<br>影響を受けるシステムに関連付けられた SBOM を使用して、インシデントの影響を評価する。<br>影響を受けるシステムの意図された SBOM をシステムの現在の状態と比較する。 |
| NTIA使用フィールド | サプライヤー、コンポーネント名、コンポーネントのバージョン、その他の固有識別子、SBOMデータの作成者、タイムスタンプ |
| 追加または相互リンクされたデータ | 複数の SBOM タイプ (設計、ビルド、ランタイム)<br>ソフトウェア認証<br>脆弱性情報源<br>サプライヤーセキュリティアサーション（例：VEX） |

| | |
|---|---|
| 達成されたメリット | 平均検出時間 (MTTD) の短縮は、組織の回復力に直接結びついており、ベンダーの評判と収益にプラスの影響を与える。 |

## ユースケース: M&Aおよび投資リスク評価

企業を買収または投資する組織は、買収対象企業が開発したソフトウェアに、買収または投資を困難にする可能性のあるリスクを特定するために、デューデリジェンスを実施する必要があります。例えば、買収側は知的財産 (IP) やライセンスコンプライアンスのリスクを負うことを望まず、パッチが適用されていないソースコードはリスクが高すぎると考える場合があります。SBOMは、対象ソフトウェアで使用されているコンポーネント、そのサプライヤー、および各コンポーネントのライセンスを把握するための手段を提供します。サプライヤーと公開されているライセンスに基づいて、買収チームはIPの競合や未解決の義務の有無を判断し、それらの問題を解決または是正するためのコストを算出できます。

買収者や投資家は、対象ソフトウェアの未修正の脆弱性によるリスクを評価・管理し、開発チームの依存関係リストが最新かどうかを確認する必要があります。SBOMに未更新のコンポーネントが多数含まれている場合、更新プロセスが未熟である可能性があります。NVDで公開されている脆弱性を持つコンポーネントのみが最新の状態に保たれている場合、開発チームは最新のコードベースの維持よりも、公開されている脆弱性へのパッチ適用を優先していると考えられます。

買収対象企業も、M&Aの初期段階でソースコードではなくSBOMを共有することでメリットを得られます。これにより、ソースコードの早期公開に伴う知的財産リスクを軽減できます。買収企業は、バイナリソフトウェアコンポジション分析 (SCA) などのツールを使用してアプリケーションからSBOMを抽出し、抽出したSBOMを買収対象企業から提供されたSBOMと比較することで、買収対象企業が提供するSBOMの整合性を検証できます。

買収者と投資家は、SBOM の分析を通じて収集された情報を使用して、対象ソフトウェアのメンテナンス、セキュリティ、ライセンス、IP、または規制コンプライアンスに関連するリスクを特定し、そのリスク評価を対象ビジネスの評価に使用できます。

表 8 では、このユース ケースの主な属性について説明します。

***SBOMが主要なサプライチェーンと相互リンクされると、サプライチェーンの透明性と信頼性が向上します。運用データ。EOLやエンティティステータスといった運用上重要なデータを拡充することで、コンポーネントの供給元やメンテナンスの有無が明確になり、より信頼性の高いサプライチェーンを構築できます。***

表8

## ユースケース: M&Aおよび投資リスク評価

| | |
|---|---|
| アクター | 技術デューデリジェンスチーム、リスク/コンプライアンス担当者、法務 |
| ビジネスモチベーション | 買収または投資の対象となる企業が、ソフトウェア セキュリティ、ライセンス、IP、または規制コンプライアンスの問題による責任を負わないことを確認する。<br>買収後も、ターゲットの商用ソフトウェア、OEM (Original Equipment Manufacturer) 製ソフトウェア、またはその他のサードパーティ製ソフトウェアへの依存が中断なく維持されることを確認する。<br>対象ソフトウェアのメンテナンスおよび更新方法の許容可能性を判断する。 |
| 機能目標 | オープンソースおよびクローズドソースソフトウェアを含む、対象企業のソフトウェア製品の継続的な開発と展開に不可欠なサードパーティソフトウェアへの依存関係を特定する。<br>対象ソフトウェアのセキュリティ、ライセンス、または商用/OEM 関係に関連する潜在的なソフトウェア製品責任を特定する。<br>「ソフトウェアインベントリ」情報を要求する規制、法律、業界標準への準拠を判断する。<br>ソフトウェア保守プラクティスの適切性を評価する。 |
| 目標を達成するためのプロセスまたはステップ | 重要な依存関係：<br>対象企業の SBOM を分析し、オープンソース、クローズドソース、契約ソフトウェアを含むすべてのコンポーネントが含まれているか確認する。<br>SBOMを分析して、オープンソース・ソフトウェアとクローズドソース・ソフトウェアの両方を含む、対象ソフトウェアで最も一般的に使用されている外部開発コンポーネントを特定する。<br>各商用/OEM開発者関係について、ライセンスの譲渡可能性を特定する。<br>潜在的な責任：<br>対象企業のSBOMをCVEについて分析する。 |

| | |
|---|---|
| 目標を達成するためのプロセスまたはステップ | 対象ソフトウェアのセキュリティアドバイザリとセキュリティリリースドキュメントを分析する。<br><br>対象ソフトウェアの管轄に基づいて、対象ソフトウェアに互換性のない IP ライセンスがあるかどうかを判断する。<br><br>各商用/OEMサプライヤーについて、ソフトウェアのSBOMを分析し、パッチ未適用の脆弱性とセキュリティアドバイザリを確認する。<br><br>各商用/OEMサプライヤーについて、適切なライセンスのためにソフトウェアのSBOMを分析する。<br><br>規制コンプライアンス：<br><br>対象ソフトウェアの SBOM を分析して、制裁対象または禁止対象になる可能性のあるサプライヤーを特定する。<br><br>サプライチェーンのリスク評価のために、すべての商用/OEMサプライヤーソフトウェアサプライヤーを分析する。<br><br>多くの規制はSBOMが主流になる以前から存在し、ソフトウェア依存関係のインベントリの維持に言及しています。SBOMは、こうした規制の精神に沿ったコンプライアンス対策を提供する。<br><br>ソフトウェアメンテナンス：<br><br>部品の平均年齢を決定する。<br><br>パッチ未適用のCVEの数を決定する。<br><br>SBOM生成プロセスを決定する。<br><br>新しいソフトウェアバージョンの頻度を決定する。 |
| NTIA使用フィールド | サプライヤー、コンポーネント名、コンポーネントのバージョン、<br>その他の一意の識別子、依存関係、SBOMデータの作成者、タイムスタンプ |
| 追加または相互リンクされたデータ | SBOMにはOSSだけでなく、独自仕様、商用、契約、COTSなどすべてのコンポーネントを含める必要がある。 |

| | |
|---|---|
| 追加または相互リンクされたデータ | 相互リンクされたデータには、出所データ、コンポーネントライセンス、サードパーティコンポーネントの適合宣言、およびサードパーティコンポーネントの輸出入コンプライアンス文書が含まれている必要がある。<br>追加のSBOMデータが存在する場合は、既存のプロセスの一部として使用する必要がある。 |
| 達成されたメリット | 開発プロセスの透明性を通じて、新しく買収した企業の統合コストを削減する。<br>進行中または将来の事業運営に最もリスクのある分野に技術デューデリジェンスの取り組みを集中させる。<br>取引を破棄または変更するリスク要素を早期に特定する。 |

## ユースケース: アクセサリソフトウェアの検証

プロデューサーとコンシューマーは共に、開発または展開するソフトウェア製品全体のセキュリティとコンプライアンスのリスクを評価する必要があります。多くのソフトウェア製品には、インストーラー、ダウンロードマネージャー、ランタイム依存関係、ソフトウェア開発キット（SDK）など、インストール、アップデート、または他のシステムとの統合を容易にするアクセサリソフトウェアが含まれています。これらのコンポーネントはコア実行ファイルに直接コンパイルされないため、コア製品のSBOM（ソフトウェアベースオブミッション）から除外されることがよくあります。アクセサリソフトウェアには独自のSBOMが存在する場合もありますが、コア製品のSBOMのセキュリティおよびコンプライアンスレビューで見落とされ、組織に重大なリスクをもたらす可能性があります。

セキュリティの観点から見ると、インストーラーやSDKは昇格された権限で実行されたり、外部コードを取得したりするため、アクセサリソフトウェアは攻撃者にとって魅力的な標的となります。検証されていないアクセサリコードは攻撃対象領域を拡大し、悪用されるリスクを高めます。コンプライアンスの観点から、組織はアクセサリソフトウェアが制裁対象または禁止対象のサプライヤーから提供されていないことを確認する必要があります。たとえ主要ベンダーが制裁対象でなくても、禁止されているコンポーネントが含まれているとコンプライアンス違反につながる可能性があります。

これらの懸念に対処するには、コアソフトウェアとアクセサリソフトウェアの両方に対するSBOM分析が必要です。この包括的なアプローチにより、昇格された権限や外部統合を持つすべてのコンポーネントがプログラム的に検証され、誤認検証のリスクが低減され、セキュリティ、ライセンス、コンプライアンスの維持に役立ちます。最終的には、アクセサリソフトウェアのSBOMに基づく検証のユースケースはコア製品のユースケースと類似しており、包括的でエンドツーエンドのリスク管理戦略を強化します。

表 9 では、このユース ケースの主な属性について説明します。

表9

## ユースケース: アクセサリソフトウェアの検証

| | |
|---|---|
| アクター | セキュリティチーム、インシデント対応チーム、エンジニアリング管理、規制、ガバナンス、ベンダー管理、監査およびコンプライアンス |
| ビジネスモチベーション | 組織のセキュリティ体制と規制コンプライアンスを維持する。<br>ベンダーが契約条件を遵守していることを確認する。<br>サイバー保険契約の条件の遵守を確保する。 |
| 機能目標 | アクセサリソフトウェアのセキュリティリスクを評価する。<br>アクセサリソフトウェアのライセンスリスクを評価する。<br>サプライヤーのSBOMを要求する規制に準拠する。<br>同じベンダーから提供される複数の SBOM に基づいてベンダー リスクを評価する。 |
| 目標を達成するためのプロセスまたはステップ | ソフトウェア機能にパッケージ化されたすべてのアクセサリソフトウェアの完全なインベントリを要求する。<br>サプライヤーがアクセサリソフトウェアの各部分と関連するすべてのアップデートおよびサービスパックのSBOMを提供していることを確認する。<br>SBOM を分析してアクセサリ コード内のリモート アクセス ユーティリティを特定し、その後の削除または監視を行う。 |
| NTIA使用フィールド | サプライヤー、コンポーネント名、コンポーネントのバージョン、<br>その他の一意の識別子、依存関係、SBOMデータの作成者、タイムスタンプ |
| 追加または相互リンクされたデータ | 指定または除外されたソフトウェアの脆弱性情報ソース、ライセンス、およびその他のコンプライアンス関連データベース |
| 達成されたメリット | ソフトウェア製品のすべてのパッケージコンポーネントのサプライチェーンの可視性 |

## ユースケース: ビルドまたはバージョン間のコンポーネントの違い

ソフトウェアのプロデューサー、流通者、そしてコンシューマーは、ソフトウェアの脆弱性、不適切なライセンス、コンプライアンス違反、そしてサポート不足から生じるリスクを理解し、伝達し、対応する必要があります。しかし、ソフトウェアに関連するリスクは静的なものではなく、時間の経過とともに変化するため、ソフトウェアの新しいビルドやバージョンに合わせて再評価する必要があります。SBOMはソフトウェアのある時点のスナップショットであるため、ソフトウェアアプリケーションのメジャービルドやバージョンごとに作成されるSBOMは、新たな時点のスナップショットとなります。これらの新しいSBOMを分析することで、ソフトウェアのコンポーネントがもたらすリスクの重要な変化を経時的に把握することができます。

例えば、ソフトウェアの初期バージョンでは既知の脆弱性がなかったコンポーネントが、将来のバージョンで新たに発見された脆弱性と関連付けられる可能性があります。また、初期リリース時には適切にサポートされていた外部開発コンポーネントが、時間の経過とともにサポートが縮小または終了する可能性があります。このような変化は、ソフトウェアのビルドまたはバージョン間でSBOMを分析することで追跡できます。SBOMの情報は、脆弱性やその他の情報と相関関係にあるため、リスクがいつ発生または特定されたか、そしてそれらのリスクがいつ軽減または修正されたかを把握できます。

プロデューサー組織とコンシューマー組織の両方におけるセキュリティ、エンジニアリング、コンプライアンス、ガバナンス機能は、これらの分析を使用して、リスクの導入と修復の進捗状況を追跡し、ソフトウェアのサポート可能性の削減を計画し、長期にわたってコンプライアンスを維持できます。

表 10 では、このユース ケースの主な属性について説明します。

**表10**

### ユースケース: ビルドまたはバージョン間のコンポーネントの違い

| | |
|---|---|
| アクター | エンジニアリング（開発、運用、セキュリティ）、エンジニアリング管理、ガバナンス、監査、コンプライアンス |
| ビジネスモチベーション | 脆弱性への露出を減らし、ライセンスコンプライアンスと社内ポリシーの遵守を確保し、規制遵守を維持する。 |
| 機能目標 | 時間の経過に伴うセキュリティとライセンスのリスクを評価する。<br>コンプライアンスとリスク軽減の進捗状況を経時的に評価する。 |
| 目標を達成するためのプロセスまたはステップ | ビルドまたはバージョン間のソフトウェア コンポーネントの変更を識別する。<br>ソフトウェア コンポーネントの変更によって、以前のセキュリティ、ライセンス、またはサポートの問題が修正されたか、あるいは新しい問題が生じたかどうかを識別する。 |

| | |
|---|---|
| 目標を達成するためのプロセスまたはステップ | ビルドとバージョン間で永続的または繰り返し発生するセキュリティ、ライセンス、またはサポートの問題を特定する。<br>ソフトウェアの構成を追跡して、新しいリスクと既存のソフトウェアを相関させる。<br>メトリック ベースのパフォーマンス追跡とコンプライアンスのために、時間の経過に伴う問題を追跡する。 |
| NTIA使用フィールド | サプライヤー、コンポーネント名、コンポーネントのバージョン、<br>その他の一意の識別子、依存関係、SBOMデータの作成者、タイムスタンプ |
| 追加または相互リンクされたデータ | EOL<br>ライセンス<br>脆弱性情報源<br>実行時データを含む在庫システム |
| 達成されたメリット | 脆弱性の修正、ライセンスの問題への対処、サポート性の評価の進捗状況を追跡する機能をエンジニアリングに提供する。<br>経営陣に、ビルドとバージョン全体にわたるリスク軽減の進捗状況を追跡する機能を提供する。<br>リスクの変化に対処するためのリソースの割り当てに関する洞察をエンジニアリング管理に提供する。<br>監査およびコンプライアンス担当者に、コンプライアンスの調査結果を正確に特定し、特定のソフトウェア プロジェクト/製品のコンプライアンスの進捗状況を追跡する機能を提供する。<br>バージョン間で修正された脆弱性をコンシューマーに提供する。<br>新しいソフトウェア バージョンによる組織へのリスクを更新し、ベンダーのリスク スコアを更新するための情報をコンシューマーに提供する。 |

## ユースケース: 異なるガバナンス、規制、コンプライアンス (GRC) 仕様への準拠

現在、多くのソフトウェア提供契約では、コンテンツと詳細に関する特定の仕様を定めたSBOMの提供が義務付けられています。プロデューサーはソフトウェアの提供時にこれらの要件を満たす必要があり、コンシューマーはソフトウェアの取得と展開前にこれらの要件が満たされていることを確認する必要があります。

さらに、新たな規制では、SBOMまたは類似のソフトウェアインベントリをコンシューマーおよび／または規制当局に提供することが義務付けられており、プロデューサーとコンシューマーが内部リスク管理にSBOMを使用することが想定されています。例えば、

- 米国食品医薬品局 (FDA) は、議会が行った食品医薬品化粧品法 (FDA) の改正を実施し、医療機器メーカーに対し、FDAへの特定の規制申請においてSBOM (品質システムに関する考慮事項と市販前申請の内容) の提出を義務付ける第524b条 [26] を制定しました。FDAの「医療機器におけるサイバーセキュリティ：品質システムの考慮事項と市販前申請の内容」[27] では、SBOMの要件が詳述されています。

- 欧州サイバーレジリエンス法 (EU-CRA) (EU規則2024/2847) [28] 第13条 (24) は、SBOMを製造業者の義務として規定しており、附属書IパートII (1) では、最上位レベルのコンポーネントを含む最低限の詳細レベルでSBOMを作成することが求められています。SBOMのフォーマットや要素に関する詳細は、2025年12月までに公表される予定です。

- 米国国防総省 (US DoD) のシステムエンジニアリング標準および仕様DI-SESS-82433は、陸軍省の「ソフトウェア部品表ポリシー」に関するメモ [29] に基づいて要求されており、NTIAの最小フィールドと最新のSPDXまたはCycloneDX仕様の利用可能なフィールドの両方を超えるSBOMデータ要素の詳細を示しています。

*さまざまな規制や契約上の要件に準拠する必要があるソフトウェア プロデューサにとっては、SBOM に含めることができるデータのスーパーセット (最小要素を超えて) を用意し、プロデューサがそこからデータを取得して、特定のコンシューマの要件に合わせた SBOM を提供することが効率的です。*

プロデューサーの社内技術、法務、コンプライアンスチームは、様々な契約要件や規制要件への適合性を確保するために、SBOMの評価、拡充、カスタマイズに協力しています。初期の自動生成されたSBOMに含まれていないデータは、他のソースから取り込まれ、規制仕様に準拠したSBOMを補完または拡充するために使用されます。

コンシューマーは、独自の GRC 制約に従い、プロデューサーが提供する強化された SBOM を使用して、プロデューサーのソフトウェアを展開する前、またはコンシューマーの製品に組み込む前に、ソフトウェアが個別の規制要件と契約要件に準拠しているかどうかを評価します。

表 11 では、このユース ケースの主な属性について説明します。

表11

## ユースケース: 異なるGRC仕様への準拠

| | |
|---|---|
| アクター | リスク/コンプライアンス責任者、監査人（社内および社外）、法務、取締役会 |
| ビジネスモチベーション | 特定の管轄区域、市場セグメント、または垂直セクター内の法的および規制上の要件に関連する内部ガバナンスのプロセスとプラクティスを満たす。 |
| 機能目標 | プロデューサーが事業を展開している、または製品やサービスを提供している管轄区域によって定められた特定の要件を満たす SBOM を提供する。<br>サプライヤーSBOMに記載されているリスクが特定の規制に関連し、それらのリスクがコンシューマーにとって規制上の課題となるかどうかを評価する。 |
| 目標を達成するためのプロセスまたはステップ | SBOM 要件を指定する規制、またはソフトウェア インベントリの必要性を参照する規制を特定する。<br>必要な SBOM データのレベルを決定する (例: 直接依存関係のみ)。<br>必須データフィールドを外部データソースから補足する必要があるかどうかを確認する（例：商用サポート契約の有効期限など）。<br>直接サプライヤーからのSBOMについては、コンプライアンスに必要な情報が存在するかどうかを確認し、不足している情報や不適合なコンポーネントに関するポリシーを実装する。<br>開示の期間と場所を含む開示要件を決定する（例：新しいリリースから x 日以内に SBOM を指定のリポジトリにアップロードする必要がある）。<br>個々の契約や規制の要件に基づいて、補足情報で充実させたり、過剰な開示をすることなく、規制の特定の要件を満たすように公開された SBOM をカスタマイズする。<br>SBOM共有の制約と、それらが遵守されることを確認するプロセスを特定する。 |
| NTIA使用フィールド | SBOM には、規制で指定されたデータ要素を含める必要があるが、NTIA の最小フィールドを参照することはできない。 |

| | |
|---|---|
| NTIA使用フィールド | 米国以外を拠点とする規制活動では、NTIA の要素を参照できない場合がある。<br>SBOM は、関連する法律や規制を包括的に検討して必要なフィールドを特定した後、これらの規制への準拠を促進できる。 |
| 追加または相互リンクされたデータ | 規制により異なる。<br>さまざまな GRC 要件を満たすために、プロデューサーは、オープンソース、クローズドソース、契約によるものなど、すべてのコンポーネントを含める必要がある場合がある。<br>独自仕様、商用、COTSなどの用語を探す。<br>GRC指向のSBOMに含めることができる相互リンクされたデータには、所有権と管理情報、サードパーティコンポーネントの適合ステートメント、サポートステートメント、インシデント対応プロセスのドキュメント、およびサードパーティコンポーネントの輸出入コンプライアンスドキュメントも含まれる場合がある。 |
| 達成されたメリット | ソフトウェアのプロデューサーとコンシューマーが契約および規制の要件を満たしていることを確認する。 |

## ユースケース: 運用技術 (OT) と分離されたネットワークの整合性と脅威管理

重要インフラ、産業用途、高セキュリティ環境、あるいは隔離されたネットワークに導入されるソフトウェアは、通常、セキュリティ問題に対処するためにソフトウェアアップデートをシステムにプッシュするようなクラウドネイティブやDevSecOpsの運用モデルには従いません。ソフトウェアは隔離されている場合もありますが、隔離されているからといって、依存関係や既知のセキュリティ問題を理解する必要性がなくなるわけではありません。こうした知識は、アップデート／アップグレードプロセス管理だけでなく、脅威管理やコンプライアンス対策においても非常に貴重となります。

例えば、サイバーフィジカルデバイスのサプライヤーは、多くの場合、デバイスを一括製造し、長期間にわたって販売します。売れ残ったデバイスは製造在庫であるため、在庫にある間は最新のパッチが適用されません。SBOMがない状態で販売され、隔離された環境に設置されると、新しく設置されたデバイスが未解決の脆弱性、またはサポート終了や旧式の依存関係の弱点によってリスクを高めているかどうかを判断することは困難です。

SBOMは、アプリケーション内で使用されるコンポーネント、ライブラリ、そして場合によってはランタイムツールの包括的なリストを提供することで、ソフトウェア依存関係の透明性を実現します。適切な透明性を確保することで、SBOMはネットワーク境界を越えたバージョン管理と依存関係管理を標準化・合理化し、攻撃対象領域やその他のリスクを

最小限に抑えることを可能にします。このアプローチは、コンプライアンスとセキュリティのレビューを簡素化し、トレーサビリティを確保することで、環境間でのソフトウェア転送における繰り返し可能なパッケージ化を可能にします。例えば、コンテナイメージのレジストリ/リポジトリ、ソースリポジトリ、ローカルファイルなどのソースからアーティファクトと依存関係を収集し、アーティファクトリポジトリにバンドルすることで、シームレスなデプロイメントを実現します。

SBOMを用いて分離されたネットワーク環境内の依存関係を標準化するプロセスは、宣言されたコンポーネントのみが収集・配布されていることを検証することで、ターゲット環境の整合性を確保します。各コンポーネントの安全なハッシュを計算し、それを含めることで、SBOMはメタデータの追加レイヤーを提供し、コンシューマーがソフトウェアバンドルの真正性と整合性を検証できるようにすることで、改ざんや不正な変更から保護します。

表 12 では、このユース ケースの主な属性について説明します。

**表12**

## ユースケース: OTおよび分離されたネットワークの整合性と脅威管理

| | |
|---|---|
| アクター | ソフトウェア開発者、デプロイメントエンジニア、セキュリティエンジニア、 DevSecOps 、メンテナンス、コンプライアンス、法務 |
| ビジネスモチベーション | エアギャップ環境での安全なソフトウェア配布を可能する。<br>インターネットに依存せずに、制御されたパッチ適用と展開を容易にする。<br>コストを削減し、運用を効率化し、セキュリティを強化する。<br>コンテナ イメージや組み込みシステムなどのバンドル ソフトウェアの法的要件とコンプライアンスを確保する。<br>監査を簡素化し、リスクを軽減し、利害関係者の信頼を構築する。<br>セキュリティおよび規制要件へのコンプライアンスを維持する。<br>より迅速なインシデント対応とより強力な回復力。<br>ミッションクリティカルなアプリケーションの信頼性とトレーサビリティを向上。 |
| 機能目標 | システムまたはネットワーク間のデータ転送に含めるコンポーネントを宣言する。<br>システムとネットワーク間の転送後のシステム構成を追跡する。<br>政府または組織の「運用権限」（ATO）決定の一環として、移管前に満たされるセキュリティ制御を特定する。 |

| | |
|---|---|
| 目標を達成するためのプロセスまたはステップ | 収集 - PURL などのコンポーネントの一意の識別子を使用して、パッケージ リポジトリ、Git リポジトリ、コンテナー レジストリからコンポーネントをダウンロードする。<br>プロセス - ウイルス対策チェック、CVE 検索、署名検証など、ダウンロードしたコンポーネントの検証チェックを完了させる。<br>バンドル - ダウンロードして処理したコンポーネントをバンドルし、ネットワーク ギャップを越えて移動する。<br>展開 - 転送されたバンドルが分離されたネットワークで利用可能になったら、コンポーネントを展開して分離されたパッケージ リポジトリまたはコンテナー レジストリに移動する。 |
| NTIA使用フィールド | サプライヤー、コンポーネント名、コンポーネントのバージョン、<br>その他の一意の識別子、依存関係、SBOMデータの作成者、タイムスタンプ |
| 追加または相互リンクされたデータ | ライセンス<br>コンポーネントハッシュ<br>制裁対象または禁止対象サプライヤーリスト<br>脆弱性情報源 |
| 達成されたメリット | パブリックインターネットに接続されていないネットワーク上で開発または展開を行うユーザーは、政府または組織の運用権限（Authority to Operate）に基づき、すべてのコンポーネントがセキュリティ管理基準を満たしていることを証明する必要がある。SBOMは、導入内容を明確に理解し、含まれるすべての内容を検証するための手段を提供する。 |

## ユースケース: ソフトウェア対応デバイスのフィールドサービス

医療機器、セキュリティセンサー、暖房制御装置などのソフトウェア対応デバイスのメーカーは、製品リリース時にSBOMを発行します。これらのデバイスは運用技術（OT）環境に導入され、デバイスの寿命（多くの場合、数年または数十年）にわたって現場でのサービスとメンテナンスの対象となります。その寿命中に、関連するファームウェアを搭載した交換用ハードウェアがインストールされ、ファームウェアの更新が必要になる場合がありますが、デバイス技術者が必要なメンテナンスを実行するための完全なアクセス権を持っていない可能性があります。

フィールドサービス担当者は、日常的な保守とトラブルシューティングの一環として、ソースSBOMを運用デバイスのデータ（SBOM、コンポーネントハッシュ、ファームウェアリビジョンの比較など）と比較し、保守とトラブルシューティングを行います。また、セキュリティログやエラーログを収集することで、エスカレーション前に侵入や障害を検出することも可能です。例えば、病院の患者モニターを管理している医療機器メーカーは、これらのデバイスに不正なソフトウェアが混入し、患者の安全を脅かす事態に遭遇しました。リファレンスSBOMは、想定されるソフトウェアを特定するための基準となり、保守や修理に役立ちます。

フィールドサービス担当者は、ソースSBOMとその想定される内容を、導入済みデバイスから収集したデータと比較することで、デバイスの導入以降のソフトウェアコンポーネントの変更を特定できます。これらの差異は、デバイスの動作に必要な必須コンポーネントの修理または交換、コンシューマー側でのデバイスへの不要なソフトウェアの追加、悪意のあるコンポーネントの挿入など、さまざまな理由で発生する可能性があります。これらの差異を特定することで、フィールドサービス担当者はデバイスの動作に関する問題を診断し、メンテナンスを実施できるようになります。また、メーカーの製品セキュリティチームにとっても貴重な情報となります。

フィールド サービス担当者は、展開されたデバイス内のコンポーネントのパッチ レベルを製造元推奨のパッチ レベルと比較して、展開されたデバイスで何をアップグレードする必要があるかを判断することもできます。

サイバーフィジカルデバイスの寿命は長いため、SBOMはデバイス内の想定されるソフトウェアの正確な記録を維持することで、プロデューサーとコンシューマーの両方の保守コストを削減する手段となります。デバイスソフトウェアのフィールドカスタマイズが可能な場合、SBOMを使用することで、フィールドサービス担当者はデバイスが正常なリスクプロファイルまたは想定されるリスクプロファイル内で動作しているかどうかを判断し、必要な軽減策を決定することができます。

表 13 では、このユース ケースの主な属性について説明します。

**表13**

## ユースケース: ソフトウェア対応デバイスのフィールドサービス

| | |
|---|---|
| アクター | プロデューサーフィールドサービス担当者、製品セキュリティチーム、コンシューマーITチーム、コンシューマーセキュリティチーム |
| ビジネスモチベーション | ソフトウェア対応デバイスの信頼性を維持する。<br>ソフトウェア対応デバイスのサポート性、パフォーマンス、可用性を維持する。<br>不要なコンポーネントによる脆弱性の露出を減らす。 |
| 機能目標 | 導入されたデバイスのソフトウェア インベントリを、デバイスのリリース時に製造元から提供されたソフトウェア インベントリと比較する。 |

| | |
|---|---|
| 目標を達成するためのプロセスまたはステップ | 最新の検証済み展開済みデバイス SBOM を取得する。<br>展開されたデバイスの SBOM を生成する。<br>2つのSBOMの違いを特定する。<br>意図的か意図的でないかを問わず、差異の潜在的な理由を特定する。<br>導入されたデバイスのコンポーネントのパッチレベルをメーカーの推奨レベルと比較する。<br>デバイスのソフトウェアへの意図しない追加や、展開されたデバイスのセキュリティ上の問題について、製造元の製品セキュリティチーム、コンシューマーのセキュリティチーム、ITチームに通知する。 |
| NTIA使用フィールド | サプライヤー、コンポーネント名、コンポーネントのバージョン、<br>その他の一意の識別子、依存関係、SBOM データの作成者、タイムスタンプ。 |
| 追加または相互リンクされたデータ | コンポーネントの製造元推奨パッチレベル<br>メーカーのインストール手順<br>コンポーネントハッシュ |
| 達成されたメリット | ソフトウェア対応デバイスが信頼性と安全性を確保して動作することをコンシューマーに保証する。<br>デバイスのソフトウェアが最新のパッチレベルであることをコンシューマーに保証する。<br>メーカーのフィールドサービス担当者にメンテナンスに必要なソフトウェアのステータスを提供する。 |

# 重要なポイント

以下の重要なポイントは、13のユースケースから得られた最も重要なポイントと、表に参照されている裏付けデータです。 15と 16. これらは、この文書の分析から得られる高レベルの洞察、結論、または指針をまとめたものであり、幅広く適用可能ですぐに実行可能な方法で組織の戦略および運用の実践に情報を提供することを目的としています。

**SBOMデータと外部インテリジェンスを組み合わせることで、セキュリティと脆弱性管理が大幅に改善されます。** SBOMフィールド（サプライヤー、コンポーネント、バージョン、依存関係など）を脆弱性情報ソースとリンクさせることで、組織は新たなセキュリティ問題を迅速に評価し、修正することができます。この継続的な相互リンクにより、パッチ適用の意思決定が迅速化され、優先順位付けが強化され、インシデント発生時の平均検出時間（MTTD）が短縮されます。

**SBOM主導のワークフローは、異なるソフトウェア環境におけるコンプライアンスとライセンスリスクを軽減します。** ライセンス義務の確認からコンポーネントの出所がポリシーに違反していないことの確認まで、SBOMは複数のコンプライアンスチェックを統合するのに役立ちます。SBOMにリストされたソフトウェアコンポーネントをライセンスデータベースや制裁対象エンティティリストと比較することで、組織はコストのかかる法的リスクを回避し、サプライチェーンの盲点を回避できます。

**SBOMを複数のユースケースの一元管理されたインベントリとして活用することで、運用効率が向上します。** 本書に記載されている13のユースケース（導入前のCVEチェックから導入後の脆弱性監視まで）の多くでは、異なる分析に同じSBOMフィールドが再利用されています。組織のSBOMデータ（および追加・相互リンクされたデータ）を統合することで、手戻り作業が削減され、リスクスコアリングの一貫性が促進され、ベンダーや買収に関する意思決定が迅速化されます。

**ビルドまたはバージョン間でSBOMスナップショットを比較することで、メンテナンスとライフサイクル計画の効率性が向上します。** いくつかのユースケースと表15〜16は、「バージョン」および「作成者」フィールドとEOLデータを組み合わせることで、新規ビルド、製品ライン、またはメジャーリリース間の違いを明確に示す方法を示しています。この明確な情報により、チームはリスクの進化（新たに導入された脆弱性やライセンスの変更など）を追跡し、アップグレードやリファクタリングをより体系的に計画できるようになります。各SBOMはライフサイクルを経て、SBOMからインテリジェンスと価値を抽出するアクターが、ユースケースに応じて分析、エンリッチメント、クロスリンク、マージ、その他の操作を実行します。

**SBOMライフサイクル管理は専門的な業務になりつつありますが、同時に共有責任も担っています。** 表15と16のデータ列の幅広さ、そしてSBOMライフサイクル管理の図からもわかるように、SBOM主導のリスク管理は、セキュリティ、エンジニアリング、法務、調達など、部門横断的なステークホルダーからのインプットに依存しています。データの拡充、複数のSBOMの統合、GRC要件への適合を促進するツールとプロセスは、組織のソフトウェアガバナンス戦略においてますます中心的な役割を果たすようになるでしょう。これは将来的に自動化と拡張の機会が数多くある有望な分野です。例えば、いくつかのユースケースでは、価値を引き出すための手順の一部として、拡充、相互リンク、統合といった一般的な操作が用いられています。

**SBOMは、効果的な相関関係を実現するために追加情報を必要とします。** 多くのユースケースでは、NTIA最小要素リストよりも多くのデータをSBOMに含めることが求められます。SBOM内のデータを他のデータセットと相互参照する機能も必要です。この操作は脆弱性分析で既に行われており、ライセンスコンプライアンスや、サポート終了およびメンテナンス対象外のソフトウェアコンポーネントに関するアラート通知など、他のユースケースにも利用できます。しかし、相互参照を正確に実行するには、NTIA最小要素ごとに共通の命名規則、または既知の命名規則セットが必要です。

**SBOMに主要な運用データが追加提供されると、サプライチェーンの透明性と信頼性が向上します。**表からわかるように、リスク評価やライセンス確認では、SBOMの基本フィールドに加えて、EOL、法的証明、制裁対象事業体チェックといった追加データが頻繁に利用されています。こうした運用上重要なデータを追加することで、部品の供給元やメンテナンス状況が明確になり、より信頼性の高いサプライチェーンを構築できます。

**規制および契約上の要件を満たすには、NTIAの最低限のフィールド以上の情報が必要です。**表15および16に示すように、NTIAの「最低限の要素」（サプライヤー、コンポーネント、バージョン、その他の固有識別子など）は確固たるベースラインを形成しますが、新たな規制（FDA、EUサイバーレジリエンス法など）や特定の業界のGRC仕様を満たすために、サポート終了日（EOL）、脆弱性悪用可能性（VEX）情報、所有権の詳細など、追加データや相互リンクデータで補完する必要があることがよくあります。

結論として、このドキュメントは、SBOMデータを静的な成果物としてではなく、現代のソフトウェアリスク管理における動的かつ多目的なツールとして捉えるべき理由を解説しています。それぞれのポイントは、SBOMデータの拡充によってコスト削減、インシデント対応の迅速化、ライセンスおよびコンプライアンス戦略の策定、そして最終的にはソフトウェアエコシステム全体にわたる信頼性の向上が実現できることを示す実例から導き出されています。

表14

## ユースケースで使用される NTIA フィールド

| ユースケース | NTIAフィールド使用 | | | | | | |
|---|---|---|---|---|---|---|---|
| | サプライヤー | 成分 | バージョン | その他のユニークな識別子 | 依存関係 | 著者 | タイムスタンプ |
| 2.1 導入前のCVE脆弱性 | ✔ | ✔ | ✔ | ✔ | ✔ | | |
| 2.2 導入後のCVE脆弱性 | ✔ | ✔ | ✔ | ✔ | ✔ | | |
| 2.3 ライセンスリスク | ✔ | ✔ | ✔ | ✔ | ✔ | | |
| 2.4 EOLおよびメンテナンス対象外コンポーネントの警告 | ✔ | ✔ | ✔ | | ✔ | | ✔ |
| 2.5 購入前のリスク評価 | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| 2.6 組織全体でのコンポーネントの使用状況 | ✔ | ✔ | ✔ | ✔ | ✔ | | |
| 2.7 インシデント対応 | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ |
| 2.8 M&Aと投資リスク評価 | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| 2.9 アクセサリソフトウェアの検証 | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| 2.10 ビルドまたはバージョン間のコンポーネントの違い | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |

| ユースケース | NTIAフィールド使用 | | | | | | |
|---|---|---|---|---|---|---|---|
| | サプライヤー | 成分 | バージョン | その他のユニークな識別子 | 依存関係 | 著者 | タイムスタンプ |
| 2.11 異なるGRC仕様への適合 | ✔ | ✔ | ✔ | ✔ | | ✔ | |
| 2.12 OTおよび孤立ネットワークの整合性と脅威管理 | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| 2.13 ソフトウェア対応デバイスのフィールドサービス | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |

*NTIAの最小要素だけでは、ほとんどのユースケースの目的を満たすには不十分です。セキュリティ、ライセンス、コンプライアンス、サポート性に関するリスクを把握するには、追加データを最小要素に相互リンクさせる必要があります。例えば、ほとんどのユースケースでは脆弱性情報への相互リンクが必要であり、多くのユースケースではライセンスデータへのリンクも必要です。*

表15

## ユースケースの目的を満たすために SBOMS に追加またはクロスリンクされたデータ

| ユースケース | 追加または相互リンクされたデータ | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 脆弱性ソース | | ライセンス | EOL | 証明書 | ランタイムデータ | 複数のSBOMタイプ | 所有 | 制裁対象団体 | 誠実性 | ベンダードキュメント |
| | データベース | サプライヤー | | | | | | | | | |
| 2.1 導入前のCVE脆弱性 | ✔ | ✔ | | | | | | | | | |
| 2.1 導入後のCVE脆弱性 | ✔ | ✔ | | | | ✔ | | | | | |
| 2.3 ライセンスリスク | | | ✔ | | | | | | | | |
| 2.4 EOLおよびメンテナンス対象外コンポーネントの警告 | ✔ | | | ✔ | | | | | | | |
| 2.5 購入前のリスク評価 | ✔ | | ✔ | ✔ | | | | ✔ | ✔ | | |
| 2.6 組織全体でのコンポーネントの使用状況 | ✔ | | ✔ | ✔ | | ✔ | | | | | |
| 2.7インシデント対応 | ✔ | ✔ | | | | | ✔ | | | | |
| 2.8 M&Aと投資リスク評価 | | | | | ✔ | | | | ✔ | | ✔ |

| ユースケース | 追加または相互リンクされたデータ | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 脆弱性ソース | | ライセンス | EOL | 証明書 | ランタイムデータ | 複数のSBOMタイプ | 所有 | 制裁対象団体 | 誠実性 | ベンダードキュメント |
| | データベース | サプライヤー | | | | | | | | | |
| 2.9 アクセサリソフトウェアの検証 | ✔ | | ✔ | | | | | | | | |
| 2.10 ビルドまたはバージョン間のコンポーネントの違い | ✔ | | ✔ | ✔ | | ✔ | | | | | |
| 2.11 異なるGRC仕様への適合s | | | | | ✔ | | | ✔ | ✔ | | ✔ |
| 2.12 OTおよび孤立ネットワークの整合性と脅威管理 | ✔ | | ✔ | | | | | | ✔ | ✔ | |
| 2.13 ソフトウェア対応デバイスのフィールドサービス | | | | | | | | | | ✔ | ✔ |

# 参考文献


1. サイバーセキュリティ・インフラセキュリティ庁（2024年1月）。SBOMコミュニティの法的説明。 **https://www.cisa.gov/sites/default/files/2024-01/SBOM-Community-Legal-Explanation_508c.pdf**
2. 米国商務省電気通信情報局（NTIA）（2019年11月）「サプライチェーン全体におけるSBOMの役割とメリット」。 **https://www.ntia.gov/sites/default/files/publications/ntia_sbom_use_cases_roles_benefits-nov2019_0.pdf**
3. Bi, T., Xia, B., Xing, Z., Lu, Q., & Zhu, L. (2024). SBOMへの道：実践における設計上の課題と解決策の調査. ACM Transactions on Software Engineering and Methodology, 33(6), 1-25。 **https://doi.org/10.1145/3654442**
4. サイバーセキュリティ・インフラセキュリティ庁（2023年4月21日）ソフトウェア部品表（SBOM）ドキュメントの種類。 **https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf**
5. サイバーセキュリティ・インフラセキュリティ庁 (2023年4月17日)。ソフトウェア部品表 (SBOM) 共有ライフサイクルレポート。 **https://www.cisa.gov/resources-tools/resources/software-bill-materials-sbom-sharing-lifecycle-report**
6. 米国商務省電気通信情報局（NTIA）、NTIA SBOMフォーマットおよびツールワーキンググループ（2021年11月）。SBOMツール分類タクソノミー。 **Ntia_sbom_tooling_taxonomy-2021mar30_0.pdf**
7. 米国国家安全保障局（2023年12月）。ソフトウェア部品表（SBOM）管理に関する推奨事項。**CSI-SCRM-SBOM-MANAGEMENT.PDF (defense.gov)**
8. D'Amico, Anita and Zalevsky, Ken. (2024, October). (2024年10月). 「SBOMの生涯：それはどこへ行き、人々はそれに対して何をし、それを使って何をするのか?」 BSidesNYC 2024年10月19日。スライドは **https://www.linkedin.com/feed/update/urn:li:activity:7276685538156244993/** に掲載されています。
9. サイバーセキュリティ・インフラセキュリティ庁（2024年2月5日）SBOM共有入門書。 **https://www.cisa.gov/resources-tools/resources/sbom-sharing-primer**
10. 米国商務省および米国商務省電気通信情報局（2021年7月）。ソフトウェア部品表（SBOM）の最小要素。 **https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf**
11. SPDX は ISO 標準です。**https://www.iso.org/standard/81870.html**
12. CycloneDXは ECMA 標準です。**https://ecma-international.org/publications-and-standards/standards/ecma-424/**
13. Woody, C. (2024年2月5日). SEI SBOMフレームワークの適用. ソフトウェア工学研究所。 **https://doi.org/10.58012/5eh5-5862**
14. インド政府電子情報技術省インドコンピュータ緊急対応チーム（CERT-In）（2024年10月3日）。ソフトウェア部品表（SBOM）に関する技術ガイドライン バージョン1.0。 **https://www.interlynk.io/post/sbom-technical-guidance-for-india**
15. Berend Kloeg 、Aaron Yi Ding、Sjoerd Pellegrom、Yury Zhauniarovich (2024). SBOM導入への道筋：ビジネスステークホルダー中心のアプローチ。ASIA CCS '24: 第19回ACMアジアコンピュータ通信セキュリティ会議議事録 1770〜1783ページ。 **https://doi.org/10.1145/3634737.363765**

16. 米国商務省電気通信情報局（NTIA）「ソフトウェアコンポーネントの透明性に関するNTIAマルチステークホルダープロセス」（2021年4月27日）。SBOMのオプションと意思決定ポイント。 **https://www.ntia.gov/sites/default/files/publications/sbom_options_and_decision_points_20210427-1_0.pdf**

17. サイバーセキュリティ・インフラセキュリティ庁（SBOM）VEXワーキンググループ（2023年4月）。脆弱性悪用可能性交換（VEX）の最低要件。 **https://www.cisa.gov/sites/default/files/2023-04/minimum-requirements-for-vex-508c.pdf**

18. Wilkerson, J. (2023年5月31日). FDAの医療機器サイバーセキュリティプログラムとSBOM. 食品医薬品局。 **https://csrc.nist.gov/csrc/media/Presentations/2023/fda-s-medical-device-program-and-sbom/images-media/JWilkerson-ssca-forum-053123.pdf**

19. CISAコミュニティ SBOM共有・交換ワーキンググループ（2024年3月22日）。SBOM共有の役割と考慮事項。 **https://www.cisa.gov/sites/default/files/2024-03/SBOM%20Sharing%20Roles%20and%20Considerations.pdf**

20. 米国商務省電気通信情報局（NTIA）によるソフトウェアコンポーネントの透明性に関するマルチステークホルダープロセス（2021年2月10日）。SBOMの共有と交換。 **https://www.ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf**

21. 一般調達局（GSA）政府全体政策局（2024年5月14日）。調達レターMV-2023-02補足2。 **https://www.gsa.gov/system/files/MV-2023-02%20w%20sups%201-2.pdf**

22. Linux Foundation。SPDXライセンスリスト。 **https://spdx.org/licenses**

23. オープンソース・イニシアティブ (OSI)。OSI 承認ライセンス。 **https://opensource.org/licenses**

24. Ecosyste.ms。ライセンス。 **https://licenses.ecosyste.ms**

25. セキュアネットワーク法第2条の対象となる機器およびサービスのリスト。 **https://www.fcc.gov/supplychain/coveredlist**

26. 米国食品医薬品局（2024年3月）。市販前サイバーセキュリティガイダンスの抜粋更新：FD&C法第524B条：業界および食品医薬品局職員向けガイダンス草案。 **https://www.fda.gov/regulatory-information/search-fda-guidance-documents/select-updates-premarket-cybersecurity-guidance-section-524b-fdc-act**

27. 米国食品医薬品局（2023年9月）。医療機器におけるサイバーセキュリティ：品質システムの考慮事項と市販前申請の内容：業界および食品医薬品局職員向けガイダンス。 **https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions**

28. 欧州連合（2024年10月23日）。デジタル要素を含む製品に対する水平的サイバーセキュリティ要件に関する規則（EU）2024/2847。 **https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng**

29. 米国陸軍省メモ（2024年10月17日）。ソフトウェア部品表ポリシー。 **https://api.army.mil/e2/c/downloads/2024/10/17/4072ab1e/asaalt-software-bill-of-materials-policy-signed.pdf**

30. サイバーセキュリティ・インフラセキュリティ庁。SBOMコミュニティツールおよび実装ワーキンググループ。(2024年10月15日)「ソフトウェアコンポーネントの透明性の枠組み：共通ソフトウェア部品表（SBOM）の確立」第3版。 **https://www.cisa.gov/sites/default/files/2024-10/SBOM%20Framing%20**

Software%20Component%20Transparency%202024.pdf

31. Black Duck (2025年2月) 2025年オープンソース・セキュリティおよびリスク分析レポート。 https://www.blackduck.com/resources/analyst-reports/open-source-security-risk-analysis.html

32. Sonatype . (2024) 第10回ソフトウェアサプライチェーンの現状®。 https://www.sonatype.com/state-of-the-software-supply-chain/introduction

33. 国防総省中小企業プログラム局 (2025年) FOCIリソース。 https://business.defense.gov/Resources/FOCI/

# 略語

**API**
アプリケーション・プログラミング・インターフェース

**ATO**
運営権限

**CDRH**
医療機器・放射線保健センター

**CDX**
CycloneDX

**CISA**
サイバーセキュリティ・インフラセキュリティ庁

**CSAF**
共通セキュリティ諮問フレームワーク

**CSIRT**
コンシューマー・セキュリティチーム

**CSS**
クローズド・ソース・ソフトウェア（OSSではないソフトウェア）

**CSV**
カンマ区切り値

**CVE**
共通脆弱性と露出

**CVSS**
共通脆弱性評価システム

**DevSecOps**
開発、セキュリティ、運用

**EO**
大統領令

**EOL**
サポートの終了

**EOS**
販売の終了

**EPSS**
エクスプロイト予測スコアリングシステム

**FDA**
食品医薬品局

**FOCI**
外国人による所有、支配、または影響力

**GRC**
ガバナンス、規制、コンプライアンス

**GSA**
一般調達局

**IP**
知的財産

**JSON**
JavaScript オブジェクト表記

**KEV**
既知の脆弱性

**M&A**
合併と買収

**MDS2**
医療機器セキュリティに関するメーカー開示声明

**MTTD**
平均検出時間

**NSA**
米国国家安全保障局

**NIST**
米国国立標準技術研究所

**NTIA**
米国商務省電気通信情報局

**NVD**
国家脆弱性データベース

**OEM**
オリジナル機器メーカー

**OSPO**
オープンソース・プログラムオフィス

**OSI**
オープンソース・イニシアティブ

**OSS**
オープンソース・ソフトウェア

**OT**
運用技術

**PSIRT**
製品セキュリティチーム

**PURL**
パッケージURL

**SBOM**
ソフトウェア部品表

**SCRM**
サプライチェーンリスク管理

**SDK**
ソフトウェア開発キット

**SDLC**
ソフトウェア開発ライフサイクル

**SPDX**
ソフトウェアパッケージデータ交換

**SSDF**
安全なソフトウェア開発フレームワーク

**VDR**
脆弱性開示レポート

**VEX**
脆弱性悪用可能性交換

**XML**
拡張マークアップ言語

# 用語

**著者** - 著者はメタデータの出所を反映します。これは、SBOMで記述されているソフトウェアの作成者、上流のコンポーネントサプライヤー、またはサードパーティの分析ツールなどから取得される場合があります。これはソフトウェア自体の著者ではなく、記述データのソースであることに注意してください。 [10]

**選択**者 - 選択者は、使用するソフトウェア/製品/サプライヤーを決定する個人/組織です。 [30] この文書では、ソフトウェア/製品/サプライヤーの選択者は、ユースケース#5購入前リスク評価では購入者、調達または契約担当者として、ユースケース#8 M&Aおよび投資リスク評価では買収者または投資家として登場します。

**コンポーネン**ト - コンポーネントとは、サプライヤーが製造、パッケージング、または納品時に定義するソフトウェアの単位です。多くのコンポーネントには、サブコンポーネント、つまり上流コンポーネントが含まれます。コンポーネントの例としては、ソフトウェア製品、ライブラリ、単一のファイルなどがあります。サプライチェーンにおける視点に応じて、コンポーネント（多くの場合、主コンポーネント）は、製品、中間製品、最終製品、または最終組立品とみなされます。 [30]

**コンシューマー** - コンシューマーは転送されたSBOMを受け取ります。これには、第三者、作成者、インテグレーター、エンドユーザーなどの役割が含まれます。 [5] [19]

**CycloneDX** - 広く利用されている、機械可読なオープンソースのSBOM形式。ECMA-424 CycloneDX部品表仕様は、 **https://ecma-international.org/publications-and-standards/standards/ecma-424/** でご覧いただけます。

**依存関係** - 依存関係は 2 つのコンポーネント間の関係です。

**ディストリビューター** - ディストリビューターは、SBOMをSBOMコンシューマーまたは他のディストリビューターと共有する目的で受け取ります。 [5] [19]

**NTIA最小要素** - 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を含むSBOM全体の最小構成要素。最小データフィールドは、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、その他の一意の識別子、依存関係、SBOMデータの作成者、およびタイムスタンプです。 [10]

**オペレータ** - オペレータとは、ソフトウェアコンポーネントを操作する個人または組織です。 [2] この文書では、「コンシューマ」という用語はオペレータとして考えることができます。

**所有権** - ソフトウェアの文脈において、所有権とは、開発中のソフトウェアに対する影響力を持つ者を特定するための規制上の概念です。所有権は、「外国の所有、支配、または影響力（FOCI）」と表現され、外国の事業体が企業およびその製品の経営または運営を指揮または影響を与える力を持つことを意味します。 [33]

**SBOMライフサイクル** - SBOMが最初の生成から利用に至るまでの過程。SBOMの作成、検証、分析、拡充、共有、監視といったすべてのフェーズが含まれます。

**セキュアストア** - SBOM を安全な方法で格納し、整合性を確保して、承認された関係者のみにアクセスを制限するリポジトリまたはシステム。

**セキュリティアドバイザリ** - 特定のソフトウェアに関連する脆弱性やパッチについて、サプライヤーまたはセキュリティ研究者から提供される情報。SBOMは、影響を受けるバージョンまたはコンポーネントを特定するのに役立ちます。

**ソフトウェア部品表（SBOM）** - SBOMは、ソフトウェアコンポーネントと依存関係、それらのコンポーネントに関する情報、およびそれらの関係を機械で読み取り可能な形式で表したものです。 [30]

**SPDX** - 広く使用されている、機械可読なオープンソースのSBOM形式。ISO/IEC 5962:2021 SPDX仕様V2.2.1は、 **https://www.iso.org/standard/81870.html**でご覧いただけます。

**サプライヤー** - サプライヤーとは、ソフトウェアコンポーネントの考案者または製造者を指します。 [10]

**システムSBOM** - 相互接続されたSBOMの集合を表す最上位レベルのSBOM。複数のSBOM（例えば、異なるモジュールやマイクロサービス用）をリンクまたはマージして、製品またはソリューション全体を表します。

**調整** - 契約要件や規制要件を満たすため、あるいは対象者固有のニーズに対応するために、SBOMを変更すること（例：独自のデータの編集やGRC固有のフィールドの追加）。通常、SBOMを共有する前に実施されます。

**ユースケース** - SBOMを様々なステークホルダーがどのように活用し、組織にメリットをもたらすかを示すシナリオ（脆弱性スキャン、ライセンスコンプライアンスなど）です。このドキュメントでは、13のユースケースを紹介します。

**検証** - SBOM に法律、規制、業界標準、契約で要求される要素が含まれており、適切な仕様に準拠していることを確認するプロセス。

**VEX (Vulnerability Exploitability eXchange )** - サプライヤーが自社製品における既知の脆弱性の悪用可能性を明確にするために使用する標準化されたフォーマット（通常はJSON、XMLまたはCSAF）。CVEが特定のコンポーネントに実際に影響を与えるかどうかを確認するために、SBOMと頻繁に相互参照されます。

**脆弱性情報** - 本文書のユースケースで使用される「脆弱性情報」という用語は、ユースケースの目的を文脈的に満たすために必要なあらゆる潜在的情報を網羅する広範な用語です。例えば、脆弱性情報には、国家脆弱性データベース（NVD）や各国固有のNVDなどの共有場所に保存されるCVE識別子、あるいはGitHubセキュリティアドバイザリ（GHSA）識別子のように民間組織が共有情報ソースを公開している場所に保存されるCVE識別子などが挙げられます。これらの識別子は、CISAの既知の悪用可能な脆弱性（KEV）カタログやエクスプロイト予測スコアリングシステム（EPSS）情報などの追加または拡張された情報ソースへのインデックスとして機能することがよくあります。

# 謝辞

この文書に記載されている謝辞は、その内容の承認を意味するものではありません。

SBOM運用ワーキンググループのリーダー一同は、貴重な時間と専門知識、そしてチームの目標達成への献身に対し、グループメンバー全員に心から感謝申し上げます。また、主催者であるCISA SBOMチーム（Allan Friedman氏、Victoria Ontiveros氏を含む）には、業界主導のワーキンググループの開催にご協力いただき、多くのセッションに積極的にご参加いただいたことに感謝申し上げます。

この取り組みは、グループを設立したNisha Kumar氏（Oracle）のリーダーシップ、そして共同リーダーであるDeanna Medina氏（United Airlines）とRicardo A. Reyes氏（Chainguard）のリーダーシップなしには実現しませんでした。コミュニティグループのリーダーシップには多大な時間と労力が必要であり、この役割は後にBunny Hernández Banowsky氏（SHE BASH）とAnita D'Amico氏（Cotopaxi ConsultingおよびVigilant Ops）に引き継がれました。

この文書の草稿作成、アウトライン作成、そして技術レビュー（構想から最終版まで）には、組織力とリーダーシップを発揮する独自の能力が求められました。アニタ・ダミコはこの極めて重要な役割を担い、SBOMオペレーションの専門家たちが「SBOMはどのように組織に価値をもたらすのか？」という中心的な問いに答える、明確で具体的かつ実践的なコンテンツの作成を促し、効果的に"自由奔放な専門家たちをまとめあげる"役割を担いました。

以下に、文書の各セクションの主要執筆者、あるいは特定のセクションを批判的にレビューする指定技術レビュアーを務めてくださったワーキンググループメンバーの多大な貢献に感謝の意を表します。また、オープンコメント期間中に貴重なフィードバックを提供してくださったSBOMコミュニティの貢献者にも感謝いたします。これらのコメントは、最終版文書の質を高めるための視点と洞察を提供してくれました。

| 著者 | 指定技術レビュー担当者 | その他の貢献者 |
|---|---|---|
| Bunny Hernández Banowsky<br>(SHE BASH) | Bunny Hernández Banowsky<br>(SHE BASH) | David A. Wheeler<br>(OpenSSF, The Linux Foundation) |
| Anita D'Amico<br>(Cotopaxi Consulting, Vigilant Ops) | Cassie Crossley<br>(Schneider Electric) | Ralph Bean<br>(Red Hat) |
| Ian Dunbar-Hall<br>(Lockheed Martin) | Anita D'Amico<br>(Cotopaxi Consulting, Vigilant Ops) | Josh Bressers<br>(Anchore) |
| Bill Hansen<br>(Hansen Enterprises LLC)) | JC Herz<br>(Exiger) | John Cavanaugh<br>(ProCap360) |
| JC Herz<br>(Exiger) | Nisha Kumar<br>(Oracle) | Brindusa Curcaneanu<br>(NeuroPace) |

| 著者 | 指定技術レビュー担当者 | その他の貢献者 |
|---|---|---|
| Nisha Kumar<br>(Oracle) | Tim Mackey<br>(Black Duck) | Anthony Harrison<br>(APH10) |
| Tim Mackey<br>(Black Duck) | Mike Lieberman<br>(Kusari) | Charlie Hart<br>(Hitachi America, Ltd.) |
| Mike Lieberman<br>(Kusari) | Bob Martin<br>(MITRE) | Syed Zaeem Hosain<br>(Aeris Communications, Inc.) |
| Victoria Ontiveros<br>(CISA) | John Nuckles<br>(ODNI) | Philippe Ombredanne<br>(AboutCode.org, Package-URL, and nexB Inc.) |
| Anusha Penumacha<br>(Splunk) | Allan Friedman<br>(CISA) | Melissa Rhodes<br>(Medtronic) |
| Ricardo Reyes<br>(Chainguard) | Kayra Otaner<br>(Roche) | Duncan Sparrell<br>(sFractal) |
| David A. Wheeler<br>(Linux Foundation, OpenSSF) | Animesh Pattanayak<br>(PNNL) | Kate Stewart<br>(Linux Foundation, SPDX) |
| Ken Zalevsky<br>(Vigilant Ops) | Vijaya Ramamurthi<br>(Accenture Federal Services) | Takashi Ninjouji<br>(Honda Motor) |
| | Ricardo Reyes<br>(Chainguard) | |
| | Ria Schalnat<br>(HPE) | |
| | Anant Shrivastava<br>(Cyfinoid Research) | |
| | Gaurav Srivastava<br>(Siemens) | |
| | Ken Zalevsky<br>(Vigilant Ops) | |

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Thank you! Join us..

**openssf.org/getinvolved**

**openssf.org**

この日本語文書は、英語版を機械翻訳し、Improving Risk Management Decisions with SBOM Dataの参考訳として、
The Linux Foundation Japanが便宜上提供するものです。
翻訳協力：佐藤 巧