2020 年度成果報告書

戦略的イノベーション創造プログラム（ＳＩＰ）第２期／ＩｏＴ社会に対応したサイバー・フィジカル・セキュリティ/ＩｏＴ社会に対応したサイバー・フィジカル・セキュリティに係るサプライチェーンにおけるＯＳＳの活用状況調査

2021 年 3 月

国立研究開発法人新エネルギー・産業技術総合開発機構

委託先　　日本シノプシス合同会社

目次

1　研究開発の成果と達成状況

1.1　要約

1.1.1　和文要約

OSS の活用状況についての文献調査から、OSS 利用は拡大傾向にあり、年々コードベースにおける OSS の割合が増加していることが分かりました。国内の IOT を活用するプロジェクトへの聞き取り調査を行った結果においても、その傾向に違いがないことが確認されました。
サプライチェーンにおける、組み込み機器やソフトウェア・サービスでの品質保証と製品セキュリティに関する文献調査を行ったところ、コンポーネント管理の強さにより、製品セキュリティと品質保証の取り組みが「プロセスと検証活動」、「OSS 管理のベストプラクティス」および「Software Bill of Materials（以下「SBOM」という）利用の標準化」の 3 つに分類されることが分かりました。
IOT を利用する業界においては、複雑なソフトウェアのサプライチェーンに対して、プロセスと検証活動によってセキュリティを担保しようとする試みが行われています。国内のプロジェクトを調査した結果、社会の影響度が高い業界、ライフクリティカルな業界では、関連する規制が存在し、プロプライエタリなコードに加えて、利用する OSS に対しても、広範囲に検証活動が実施されていることが分かりました。
使用するコンポーネントの可視化を行っていない場合、インシデントが発生した際に、脆弱なコンポーネントの特定が難しくなるため、サイバーセキュリティのリスクが増大します。この透明性（可視化）の課題への対策の前提条件として必要になるのが、SBOM です。SBOM を利用した OSS 管理のベストプラクティスは、最新のいくつかのガイドラインの中で、重要な項目の一つとして紹介されています。国内プロジェクト調査の結果、多くのプロジェクトで SBOM が作成されており、SBOM を OSS 調達時のリスク分析や脆弱性管理、開発時の OSS の評価、運用時の保守など様々な用途で使用していることが分かりました。調査した範囲では、SBOM は文書またはエクセルベースで作成されており、機械可読可能な形式で SBOM の作成を行っているケースはなく、SBOM 利用の自動化が今後の課題であることが分かりました。これは SBOM 作成のためのツールや手順が標準化されていないためと考えられます。自動化のツールや手順が整備されるにつれ、SBOM 利用の自動化が普及していくと予測します。
2018 年から米国商務省国家電気通信情報庁（National Telecommunications and Information Administration：NTIA）（以下 NTIA という）で実施されている、ソフトウェアのサプライチェーンに対する透明性についての議論において、OSS に加えて商用ソフトウェアに対しても SBOM 利用を標準化し、組織におけるベストプラクティスを超えた、エコシステム全体での強靭なソフトウェアのサプライチェーンの構築を検討しています。 ヘルスケア・セクターの SBOM 利用の概念実証が成功裏に進行中で、その取り組みは自動車業界とエネルギー業界に拡大しています。

1.1.2 英文要約

A literature search on the status of OSS utilization revealed that OSS usage is on the rise and that the ratio of OSS in the code base is increasing year by year. As a result of interviews with projects that utilize IOT in Japan, it was confirmed that there is no difference in the tendency.
A literal search on quality assurance/product security activities against embedded devices and/or IoT related services revealed that due to the strength of component management, it was found that it was classified into three categories: "process and verification activities", "OSS management best practices", and "standardization of SBOM usage".
In the IOT industry, attempts are being made to secure the complex software supply chain through process and verification activities. As a result of investigating domestic projects, it was found that there are related regulations in industries with high social impact and life-critical industries, and in addition to proprietary code, a wide range of verification activities are carried out for the OSS used.
Without visibility into the components used, cybersecurity risks increase because it is difficult to identify vulnerable components in the event of an incident. SBOM is required as a prerequisite for countermeasures against this transparency (visualization) issue. Best practices for OSS management using SBOM are introduced as one of the important items in some of the latest guidelines. As a result of domestic project surveys, SBOMs have been created for many projects, and SBOMs are used for various purposes such as risk analysis and vulnerability management during OSS procurement, OSS evaluation during development, and maintenance during operation. In the investigated projects, SBOM was created on a document or Excel basis, and there were no cases where SBOM was created in a machine-readable format, and it was found that automation of SBOM usage is a future challenge. This is probably because the tools and procedures for creating the SBOM have not been standardized. We predict that automation of the use of SBOM will become widespread once automation tools and procedures are in place.
Discussions on software supply chain transparency have been underway at the National Telecommunications and Information Administration (NTIA) since 2018. , they are looking to build a robust software supply chain across the ecosystem that goes beyond "organizational best practices" by standardizing SBOM usage for commercial software in addition to OSS.

1.2　本文

1.2.1　調査の目的

「戦略的イノベーション創造プログラム(SIP)第 2 期/IoT 社会に対応したサイバー・フィジカル・セキュリティ」（以下「本プロジェクト」という。）においては、セキュアな Society5.0 の実現に向け、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、IoT システム・サービス及び中小企業を含む大規模サプライチェーン全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証に取り組んでいます。

近年ソフトウェアの重要性が増し、企業においても Open Source Software（以下「OSS」という。）の活用が進む中、安全な OSS の選定や、利活用するソフトウェアの脆弱性管理など、ソフトウェアの利活用に起因するサプライチェーン・セキュリティ・リスク対策の必要性が顕在化してきています。

本調査では、サプライチェーンにおける、OSS の活用、組み込み機器やソフトウェア・サービスでの品質保証と製品セキュリティの関わりや、国内外の SBOM の動向について、その状況や意見、課題を調査・分析することを目的とします。

1.2.2　OSS 活用状況の調査

1.2.2.1　OSS 活用状況

シノプシスでは、オープンソース・セキュリティ&リスク分析（OSSRA）レポート[1] として、2016 年より毎年、商用ソフトウェアに含まれる OSS の利用状況調査を行い、OSS のリスクの現状をセキュリティ、コンプライアンス、およびコード品質の面から詳しく分析し、レポートを公開しています。シノプシスの Black Duck 監査サービス・チームは、多くの場合、顧客企業の合併・買収取引を支援する形で、毎年数千ものコードベースを対象に OSS 監査を実施しており、これらの監査結果を匿名化したものを主なデータ・ソースとして使用しています。

分析した匿名化データは、「エンタープライズ・ソフトウェア /SaaS」、「医療、ヘルステック、生命科学」、「金融サービス、フィンテック」、「インターネット / ソフトウェア・インフラストラクチャ」といった様々な業界を含みます。2020 年のレポートにおいて、17 の業種で 1,250 を超える商用コードベースを対象にした監査から得られた結果は以下の通りでした。

- **ほぼ 99% の商用ソフトウェアに OSS が含まれています。**

- **コードベースに含まれる OSS の割合は増加しています。**

[1] https://www.synopsys.com/ja-jp/software-integrity/resources/reports/2020-open-source-security-risk-analysis.html (2021/3 月時点で確認済み)

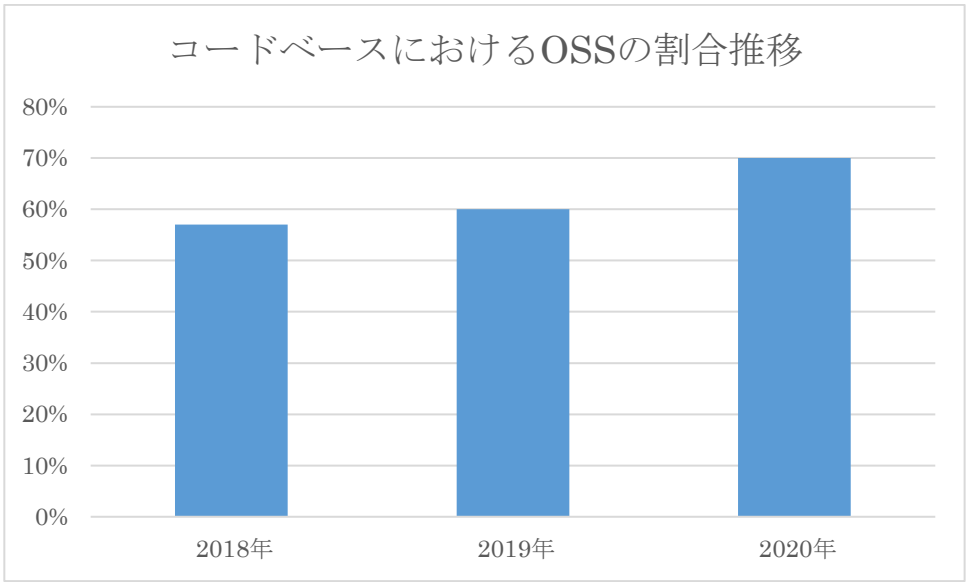

図 1 コードベースに含まれる OSS の割合推移

ソフトウェア開発において、コードベースとはアプリケーションやサービス、ライブラリの基盤となるソースコードおよびライブラリを指しています。

図 2 は 2020 年 OSSRA レポートの調査対象各業種における、コードベースに含まれる OSS の割合を示すものです。利用状況は、業界ごとにばらつきはあるものの、OSS の利用が拡大していることに変わりはありません。

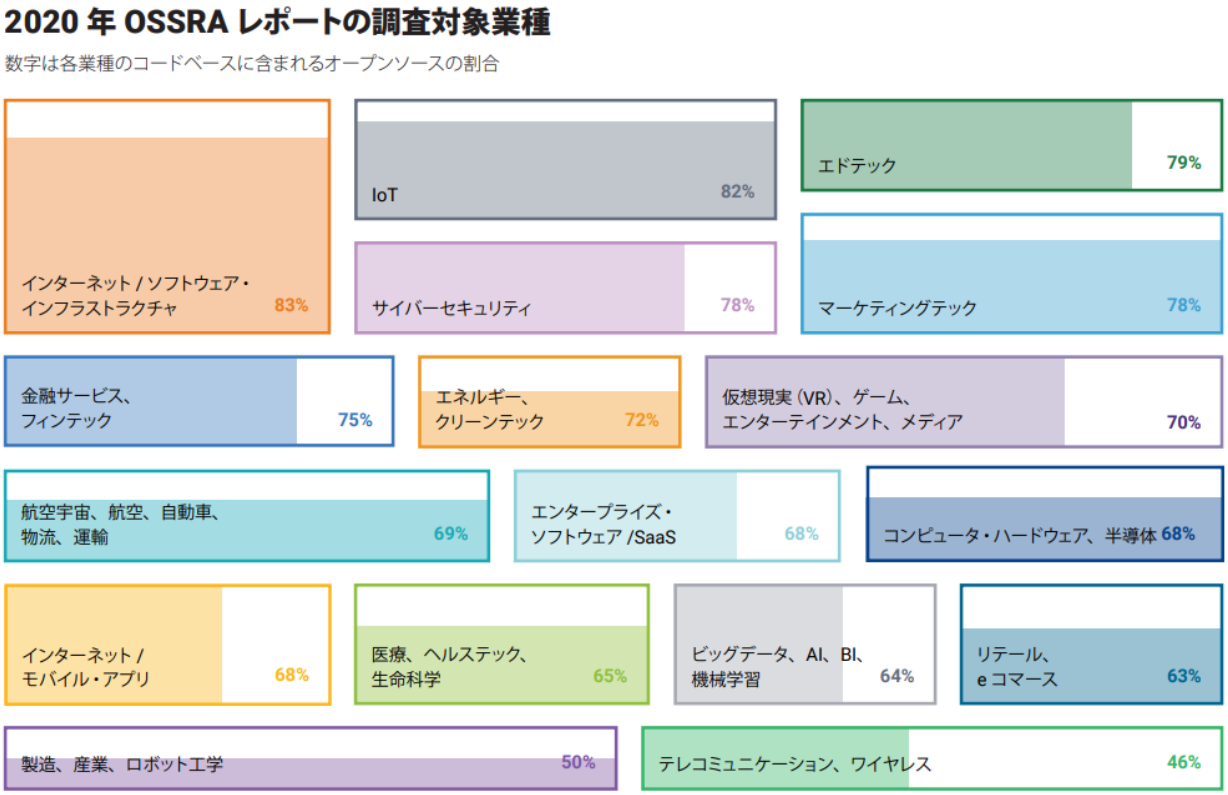

図 2 業種ごとのコードベースに含まれる OSS の割合[2]（出典：2020 年 オープンソース・セキュリティ&リスク分析レポート）

依頼に応じて、シノプシスのサービス・チームはソフトウェア開発企業のコードベースを監査しています。ソフトウェア企業の主な価値は、そのプロプライエタリ・コードにあるため、こうした企業ではコードベースに占めるプロプライエタリ・コードの比率が比較的高くなります。一方、Forrester などのアナリストは基本的にエンタープライズの IT 部門を調査対象としています。これらの企業はビジネスをサポートする目的で、ソフトウェアを利用しており、コードベースに占める OSS コードの比率は高くなる傾向があります。この調査会社のレポートでは、IT 部門の 90%以上が基幹業務系ワークロードで OSS ソフトウェアを使用しており、多くの場合、新規コードベースの最大 90%を OSS が占めているという結果が出ています。

1.2.2.1.1 OSS 活用状況調査

[2] https://www.synopsys.com/ja-jp/software-integrity/resources/reports/2020-open-source-security-risk-analysis.html (2021/3 月時点で確認済み)

国内の OSS 利用状況に関して、実プロジェクトを選定し、OSS がどの程度活用されているのか、アンケート及びヒアリングを通して調査を行いました。
調査はヒアリングの前に、アンケートで使用している OSS コンポーネントとその使用時期を申告してもらう方法を取りました。6 社の企業のプロジェクトから調査協力が得られ、医療、エネルギー、自動車、IOT、電機などの業界の OSS 利用状況について聞き取りを行いました。ヒアリングにあたり、業界の傾向を見ることが目的であり、個社の名前を記載せず、プロジェクトが特定されないような報告書記述を行うという前提で、ヒアリングに協力いただきました。

図 3 に調査対象プロジェクトの内訳を示します。

図 3 調査対象プロジェクト

表 1 に、ヒアリングした OSS 利用の事例を示します。

表 1 OSS 利用国内事例

OSS 利用国内事例	
A 社	現在、多くの医療機器で Windows や Tron のシステムが採用されており、OSS コンポーネントの利用は限定的となっています。今後は Linux ベースの機器の開発に伴い、OSS コンポーネントの採用が増加する見込みです。（医療機器メーカー、開発責任者）
B 社	IT 系を含む企業グループに対して OSS の活用を支援する部門によると、以前より多くの OSS を利用してきた IT 系と比較すると、IoT を利用する電機、自動車、エネルギーに関するプロジェクトは、OSS の活用が始まったばかりであるとのことでした。今後 OSS の利用の割合は増加する見込みであるとのことです。（企業グループ、OSS 支援提供者）
C 社	機器の制御部分のソフトウェアは自社開発を行っています。インターネット接続部分に OSS を利用しており、この部分の OSS の利用率は特に増加しています。（複合機メーカー、開発責任者）
D 社	自社開発の組み込みプラットフォーム上に Linux 系の OSS が動作する製品の開発・サービス・保守を行っています。製品でもサービスでも、ツールとしての社内利用でも多くの OSS を使用しています。（組み込みプラットフォーム製品メーカー、起業家）
E 社	OSS を使用して、IOT 機器の製品やサービスを提供しています。（企業グループ、製品セキュリティ責任者）
F 社	製品開発に多くの OSS コンポーネントを使用している。（IOT 機器開発メーカー、製品セキュリティ担当）

今回の調査では、サプライチェーンにおいて、製品およびサービスに含まれる OSS の活用状況を調査しました。最終的な製品やサービスに含まれない開発ツール（コンパイラーなど）の OSS 利用の調査は含まれていません。

以下は OSS の利用状況のヒアリングのまとめです。

- ヒアリングしたすべてのプロジェクトで OSS が利用されていることが分かりました。

- OSS の利用はどのプロジェクトでも拡大傾向にあることが分かり、今回ヒアリングした国内の調査対象プロジェクトにおいても、グローバルな OSS の利用状況を年次でレポートする、OSSRA レポートの内容と相違ないことが確認されました。

- 調査したプロジェクトにおける差異は、OS の違いによる影響が大きく、Linux 系の OS の採用が拡大すると、OSS の利用が増える傾向にあることが分かりました。

業界における違いについては、業界で採用される OS のシェアの違いが影響していると推測されます。例えば、医療機器業界では Windows のシェアが大きく、その結果、OSS として使用されるソフトウェア・コンポーネントの割合が少数となっています。自動車業界においては、制御系やボディ系の自動車部品に対して、商用の組み込み OS が使用されることが多く、これらの部品に使用される OSS コンポーネントは少数となります。その一方、利用が拡大している新しい技術分野である、自動運転システムやナビゲーション・システムなどには、Linux 系の OS が多く採用されており、多数の OSS が利用されています。

1.2.3　OSS の品質保証とセキュリティ保証

1.2.3.1　サプライチェーンのセキュリティ確保のアプローチ

サプライチェーンのセキュリティ確保の取り組みについて、文献調査を行った結果、以下の３つのアプローチに分類できることが分かりました。

- プロセスと検証活動によるセキュリティ確保の取り組み

産業用制御システムにおけるサプライチェーンのセキュリティ標準文書である IEC62443 シリーズや自動車業界におけるサプライチェーンのセキュリティを含む ISO/SAE 21434（以下 ISO 21434 という）においては、システム全体をプロセスや検証活動によって、品質やセキュリティの向上をめざすアプローチが採用されています。

- ソフトウェア部品表(SBOM)を利用したベストプラクティス

SBOM を作成し、脆弱性管理やライセンス管理などの OSS 管理を行うベストプラクティスを紹介したガイドラインが存在します。ENISA IOT セキュリティ・ガイドライン、ソフトウェア開発プラクティスをベンチマークする、学界、政府、および業界のソフトウェア開発者の大規模なグループである BSIMM のガイドラインなどで OSS 管理の推奨項目が紹介されています。

- SBOM 利用を標準化

2018 年から米国 NTIA において、ソフトウェアのサプライチェーンにおける透明性についての課題が議論されています。NTIA では、OSS に加えて、商用コンポーネントを含む、SBOM 利用の標準化を通して、ソフトウェアの透明性を向上させることにより、サプライチェーンのエコシステム全体でセキュリティを向上させようとする試みが行われています。

これらのアプローチをコンポーネント管理の強度で分類すると、図 4 のように表すことができます。

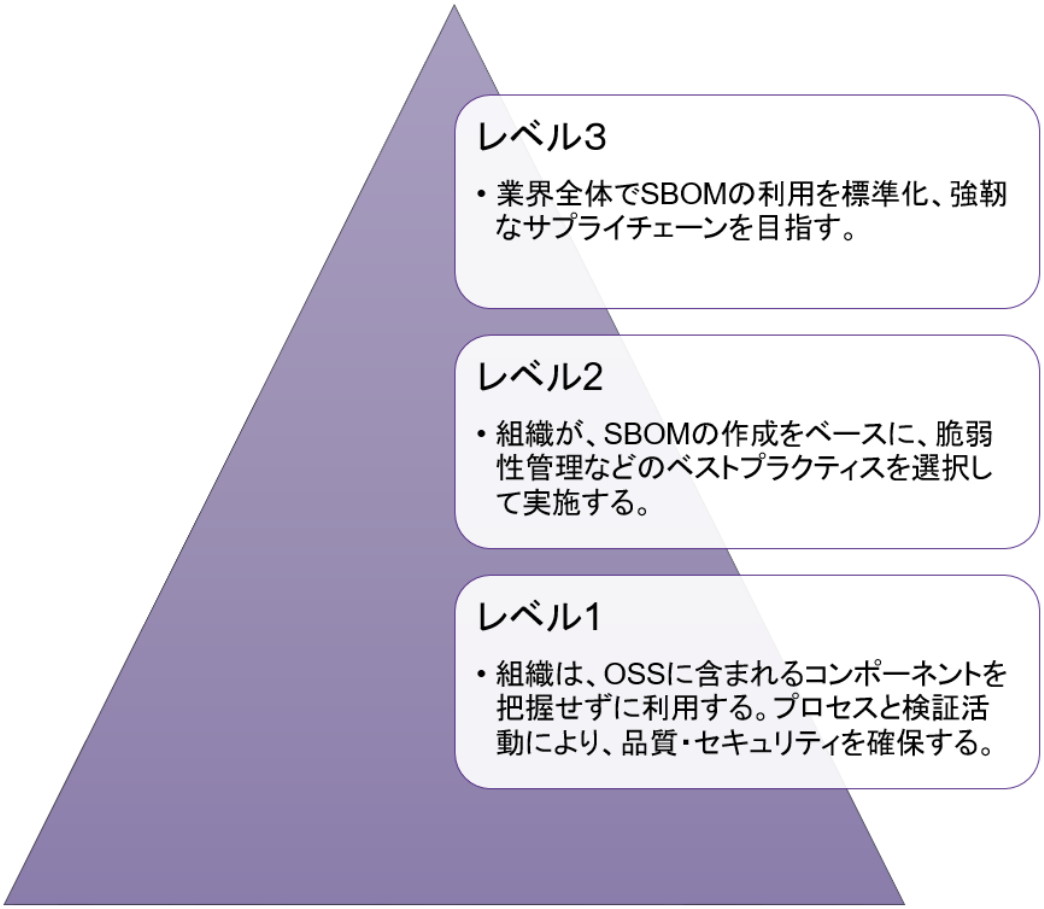

図 4 コンポーネント管理レベル

1.2.3.2 ［レベル１］プロセスと検証活動による品質・セキュリティの確保

自動車業界におけるサプライチェーンのセキュリティを定義した ISO21434 や産業用制御システムにおけるサプライチェーンのセキュリティ標準文書である IEC62443 シリーズにおいては、OSS などのコンポーネント管理に関する、具体的な言及はなく、主にプロセスと検証活動による品質・セキュリティ確保のアプローチがとられます。

欧州連合サイバーセキュリティ機関（ENISA）は、Guidelines for Securing the Internet of Things[3]（以降 ENISA IOT セキュリティ・ガイドラインという。） を公開して IoT のサプライチェーンを保護するための推奨事項を定義しています。このガイドラインにおいても、検証活動に

[3] https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things (2021/3 月時点で確認済み)

関する項目が存在します。
これらの検証活動は OSS に特化した規定はありませんが、ソフトウェア製品の品質およびセキュリティを担保するための取り組みがそのまま OSS にも適用できます。

表 2 に、OSS 利用に適用可能な検証活動のまとめを示します。

表 2 OSS 利用に適用可能な検証活動のまとめ

検証活動	ISO21434	IEC62443-4-1	ENISA IOT ガイドライン
脅威モデリング、 脅威分析	○	○	○
静的解析	○	○	○
コード・レビュー	○	○	○
ペネトレーション・テスト	○	○	○
ファジング・テスト	○	○	

○：検証活動の記載あり、印なし：検証活動の記載なし

1.2.3.2.1 ISO21434

自動車業界におけるサイバーセキュリティに対応するプロセス構築・運営するために作成された規格であり、要求管理、設計、実装、検証、配布の製品ライフサイクル全般にわたり、あるべき姿を規定しています。この規格はまだドラフトの段階ですが、その内容はほぼ最終版に近いと考えられています。その中で、検証活動に関する項目は以下の通りです。

コード・レビュー

レビューは、関係者が特定の目的および基準に照らしてドキュメントまたは作業成果物をチェックする検証方法です。

OSS はソースコードが提供されているので、対象となる OSS のソースコード・レビューを行うことが可能です。特に OSS コミュニティの「健全度」が低く、継続的なメンテナンスを期待できない場合には、コード・レビューを行い、詳細なソースコードの分析を行う選択肢があります。(検証項目：コード・レビュー)

既存のコンポーネントの再利用分析

既存のアイテムまたはコンポーネントの再利用分析では、既存の脅威の分析とリスク評価を行います。たとえば、既存のアイテムまたはコンポーネントが開発されたときと比較して、新しい資産の脅威シナリオまたはリスクについて検討します。

OSS に関しては、OSS コンポーネントの既知の脆弱性を入り口とする、脅威シナリオの分析が挙げられます。(検証項目：脅威モデリング、脅威分析)

静的解析

静的解析ツールを使用して、固有の弱点、人為的エラー、既知および目に見えるシステムの欠陥、およびサイバーセキュリティ要件の仕様に関する全体的な一貫性、正確性、完全性をチェックすることができます。静的解析ツールの例としては、MISRA-C および CERT-C のルールに対してチェックする静的ソフトウェア・コード分析ツールが挙げられます。

OSS はソースコードが提供されているので、対象となる OSS に対して、それらのツールを使用することができます。静的解析ツールを使用することにより、「バッファー・オーバー・フロー」や「クロスサイト・スクリプティング」などの脆弱性を検出することが可能です。 (検証項目：静的解析)

ペネトレーション・テスト

ペネトレーション・テストは、システムに存在する脆弱性を見つけるために使用される一連のテスト方法であり、攻撃者が制御を奪ったり、特権アクセスを取得したり、特権データを公開したり、単にシステムの誤動作を引き起こしたりする可能性を検査します。
ペネトレーション・テストでは、実際の攻撃者が使用するのと同じツールと手法を使用して、実際のシステムとデータに攻撃を仕掛けます。

OSS に関しては、OSS の脆弱性を入り口としてシステムに侵入するテストが考えられます。ペンテスト・ツールや SCA ツールなどを使い OSS コンポーネントを特定し、そのコンポーネントに既知の脆弱性を入り口とした攻撃を行います。(検証項目：ペネトレーション・テスト)

ファジング・テスト

ファジング・テストは、システムへの入力として大量の予測不能なデータが（通常は自動または半自動の方法で）提供され、弱点や脆弱性（障害やコーディングエラーなど）を探すタイプのテストです。 システムがクラッシュするか、通常の定義された動作から逸脱すると、出力はエラーとして報告されます。 ファジング・テストは、システム・レベルまたはインターフェイス・レベルで実行できます。テスト対象のソフトウェアのすべての変数を一覧表示し、コード内の各ソフ

トウェア変数のランダム値をファジングすることで、より広範囲に実行することができます。ファジング・テストは、侵入テストの手法として使用できます。

OSS コンポーネントに対して、ファジングを行い、脆弱性を発見することができます。(検証項目：ファジング・テスト)

1.2.3.2.2 IEC 62443 シリーズ

サプライチェーンのセキュリティに対処するための、ガイドラインが標準として定義されています。

産業用制御システムのセキュリティ確保のための規定が定義されており、セキュリティ技術仕様を定義した文書群が提供されています。

IEC62443-4-1 は 制御システムを構成する個々のコントローラの開発要件を規定した国際標準（IS）です。セキュアなコンポーネントを開発するための方法を規定しており、ソフトウェア開発のライフサイクルのセキュリティに関する要求事項を記載しています。

この文書の中で、セキュリティの検証項目として以下が挙げられています。検証活動の内容は ISO21434 と同様です。

脅威分析

脆弱性データベースを参照して脅威モデリングの改良を行うことができます。例えば、TLS プロトコルをトランスポートセキュリティとして使用した場合、TLS の既知の脆弱性をチェックし、そのセキュリティ対策を行います。

コード・レビュー

セキュリティに関する問題の分析にコード・レビューを行います。

静的コード解析

セキュア・コーディング標準のチェックに静的解析ツールなどの自動化ツールを使用します。

ファジング・テスト、脆弱性テスト

脆弱性テストの一つとして、ファジング・テストを行うことが可能です。

ペネトレーション・テスト

ペネトレーション・テストを行うことによって、例えば認証機能のバイパス、管理者権限などの特権モードの奪取などを行うことができるかどうかを確認することができます。

1.2.3.2.3 ENISA IOT セキュリティ・ガイドライン

ENISA は IOT セキュリティ・ガイドラインを公開して IoT のサプライチェーンを保護するためのガイドラインを定義しています。

IoT メーカー、開発者、インテグレーター、および IoT のサプライチェーンに関与するすべての利害関係者が、IoT テクノロジーを構築、展開、または評価する際のセキュリティに関する意思決定を改善するのに役立つようにガイドラインが開発されています。

このガイドラインの中では、ソフトウェア開発におけるセキュリティ検証活動が紹介されています。

セキュア・コーディングとペネトレーション・テスト

適切なセキュリティ機能を実装および検証するために、セキュリティに焦点を当てたセキュア・コーディングとテスト（ペネトレーションテストなど）の実施を IoT サプライチェーンの適切な段階に含める必要があります。

OSS に関連する検証項目としては、OSS のソースコードに対する静的解析（バッファー・オーバー・フローなどの脆弱性の発見）やペネトレーション・テストなどの検証活動が考えられます。（検証項目：静的解析、ペネトレーション・テスト）

IOT サプライチェーン向けの脅威モデルの開発

脅威モデルを作成し、重要度に応じて脅威の相対的な重要性を評価し、サプライチェーンのセキ

ュリティを保護するためのセキュリティ対策実装するため、リスク評価方法を確立する必要があります。

OSS コンポーネントも脅威モデリングに含むことができます。(検証項目：脅威モデリング、脅威分析)

サードパーティ・ソフトウェアを特定する

OSS を含むサードパーティ・ソフトウェアの使用は、サプライチェーンのセキュリティに対する脅威をもたらします。これらのソフトウェア・コンポーネントは、その選択のために従う基準を、サプライチェーンのセキュリティ・プロセスの一部として文書化する必要があります。組織は、評価および認証プロセスに合格したものを優先し、保守計画を定める必要があります。

OSS の維持管理者や業界の利害関係者の信頼できるコミュニティを特定できない OSS のケースでは、ソースコードの包括的な分析が推奨されます。(検証項目：コード・レビュー、静的解析)

1.2.3.3 [レベル 2] OSS 管理のベストプラクティス

OSS の利用における、ベストプラクティスを紹介したガイドラインやレポートがいくつか存在します。このベストプラクティスは SBOM の作成をベースに、脆弱性管理、資産管理、ライセンス管理、リスク管理などのユースケースから、その組織がそれらを選択して実施することが前提となっています。それらガイドラインから品質とセキュリティに関する OSS 管理のベストプラクティスを抽出しました。

表 3 OSS 利用のベストプラクティス

ENISA IOT セキュリティ・ガイドライン	
PRO-04:	脅威モデル作成のために、NVD などの脆弱性データベースに示されている攻撃戦術と手法の知識ベースは、脅威モデルを開発するための基盤として役立つ可能性があります。
PRO-05:	OSS コンポーネントは、その選択のために従う基準を含め、サプライチェーンのセキュリティ・プロセスの一部として文書化する必要があります。組織は、評価および認証プロセスに合格したものを優先し、保守計画を含める必要があります。

PRO-13:	SBOM は、オープンソースと商用の両方のパッケージまたはライブラリを含む、特定の製品のビルディングブロックとして使用されるソフトウェア・コンポーネントを網羅的に記述します。これらのリストにより、製品の可視性が高まり、製造元と外部ユーザーの両方が既知の脆弱性をチェックし、セキュリティの観点からデバイスを検証できるようになります。
BSIMM 11	
SR2.4:	ソフトウェア・ポートフォリオに含まれ、実行時に統合される OSS コンポーネントを特定し、レビューを通じてこれらの依存関係を十分に理解します。
SR3.1:	OSS コンポーネントの使用、および関連する依存関係（実行時に統合される依存関係を含む）に伴って生じるリスクを管理します。例えば、事前に定義済みのプロジェクトにのみ OSS の使用を制限し、承認されたセキュリティ審査プロセスを完了し、容認できない脆弱性が修正され、特定の社内リポジトリおよびコンテナを通じてのみ提供されるごく一部のオープン・ソース・バージョンのみ使用を許可するといった方法が考えられます。
CMVM2.3:	組織におけるソフトウェアのデプロイメントを、それぞれのオーナー情報も含めた形で作成しておきます。こうすると、ある 1 つのソフトウェア資産に変更が必要な場合、運用チームまたは、そのステークホルダーおよび変更のデプロイが必要な箇所をすべて正確に特定できます。
SE3.6:	運用を成功させるには、本番環境におけるアプリケーションとその場所をリストにした情報が欠かせません。すべての本番ソフトウェアに関してコンポーネント、依存関係、構成、外部サービスなどを詳細に記述したマニフェストがあれば、攻撃者や攻撃が進化しても、また、パッチを適用すべき項目が非常に多くなっても、迅速な対処が可能となり、組織のセキュリティ体制が強化されます。
OSSRA レポート	
O-1:	OSS コンポーネントおよびライブラリの管理
O-2:	OSS の品質、セキュリティに関するリスクの評価および軽減
O-3:	使用している OSS の脆弱性、アップグレード、および全体的な健康状態の継続的モニターに関するプロセスとポリシーの作成

抽出したベストプラクティスをソフトウェア開発の役割、「開発」、「調達」、「運用」で分類し、表 4 に示します。

表 4 ソフトウェア開発の役割と OSS 利用のベストプラクティス

	ベストプラクティス	内容	ENISA 推奨番号	BSIMM 要件番号	OSSRA 推奨番号
開発	SBOM の作成	OSS の特定（ビルドシステムの出力、コンポジション解析） SBOM 作成	PRO-05	SR2.4	O-1
		配布用の SBOM 作成	PRO-13	CMVM2.3	
調達	調達時におけるリスク管理	オープンソースの特定 コンポジション解析 配布された SBOM の利用	PRO-04 PRO-05	SR3.1	O-1 O-2
		設計時における OSS の脅威・リスク管理 脅威リスク分析における脆弱性データベースの使用	PRO-04		O-2
		ポリシーの策定（ホワイトリスト化、ブラックリスト化）	PRO-05	SR3.1	
運用	運用時の SBOM のメンテナンス	運用 SBOM の作成 運用時の SBOM のメンテナンス 運用 SBOM に紐づく脆弱性管理	PRO-13	SE3.6	O-3

複数のガイドラインから OSS 利用のベストプラクティスを抽出したものを以下に列挙します。

(1) 開発者は、コンポジション解析やビルドシステムからの情報を集めて OSS コンポーネントの特定を行い、SBOM を作成します。

(2) 開発者は、ソフトウェアの調達または運用で使用する目的で、配布用の SBOM を作成します。

(3) 調達者は、ソフトウェアの調達時（設計時）に、開発者が配布した SBOM を利用、あるいはコンポジション解析を行い、OSS を特定し、公開された脆弱性データベースを参照するなどして、OSS の脅威・リスク管理に役立てます。

(4) 調達者は、脅威・リスク分析の結果に基づき、「承認された OSS のみを使用する」あるいは「特定の OSS の使用を禁止する」などのポリシーやプロセスを適用します。

(5) 運用者は、開発者が配布した SBOM を利用、あるいはコンポジション解析を行い、運用 SBOM の作成を行います。インシデントが発生した場合に、OSS の特定ができるようにします。

(6) 運用者は、運用 SBOM のメンテナンスを行い、公開された脆弱性データベースを参照するなどして、OSS の新規脆弱性の監視を行います。

上記の項目に関して､SBOM の階層が 1 つである単純なケースを図示すると以下のようになります。

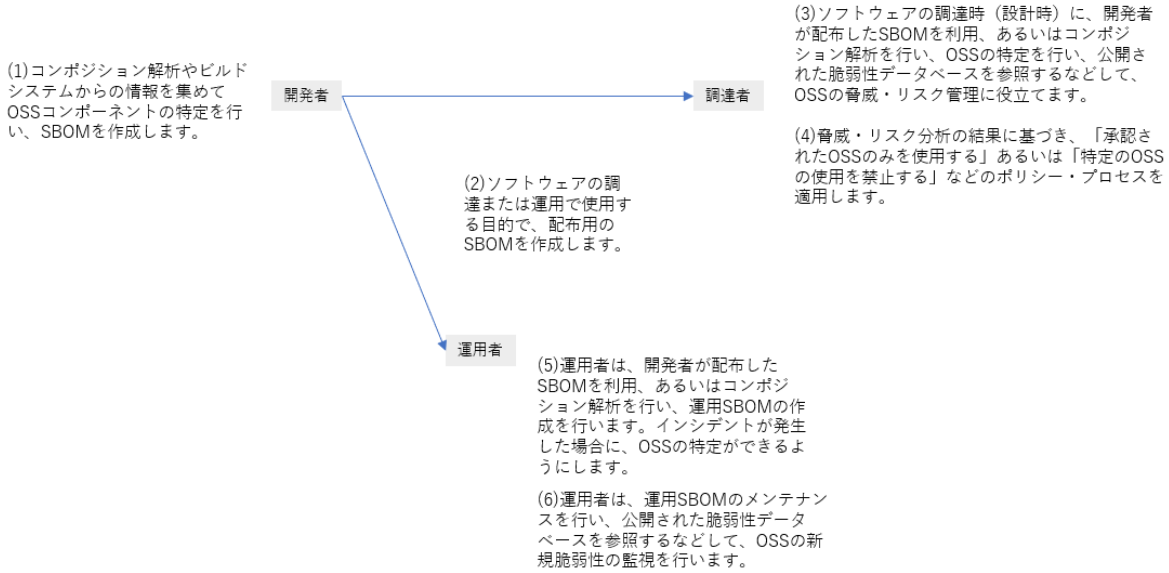

図 5 ベストプラクティス役割関連図（単階層）

1.2.3.4 ［レベル 3］サプライチェーン・エコシステム全体の取り組み

NTIA では、SBOM の利用において、エコシステムで共有されるべき SBOM 利用を標準化し、組織におけるベストプラクティスを超えた、エコシステム全体にわたる、強靭なソフトウェアのサプライチェーンの構築を検討しています。NTIA の活動の概要を以下に示します。より詳しい取り組みついては、1.2.4.1 NTIA の活動で記述します。

(1) ベースライン情報の定義

基本的かつ重要な機能をサポートするための、必要最小限の情報を定義します。

(2) SBOM ユースケースの特定

SBOM のユースケースを特定します。「脆弱性管理」、「ライセンス管理」、「高度な保証」です。各ユースケースでは、上記のベースライン情報の定義に加えて、追加情報の定義が必要となります。

(3) 役割ごとの SBOM 利用の価値

ソフトウェア利用における役割を「作成する」、「選択する」、「運用する」に分類し、それぞれの役割における SBOM 利用の価値を分析しています。

(4) 機械読み取り可能なフォーマットの検討

現存する、SBOM に利用可能な機械可読な主要フォーマットである SWID と SPDX の両方の形式を使用して SBOM データを生成、交換、および使用できることを確認しています。また、より相互運用可能なエコシステムを可能にするために「最小実行可能」SBOM モデルを、2 つのフォーマット間で変換するための明示的なガイドを提供しています。

(5) ヘルスケア・セクターにおける概念実証

上記のように NTIA で定義した SBOM の取り組みが、医療機器メーカーと医療提供組織が参加して、実際に機能するのか、概念実証に取り組んでいます。フェーズ１の結果、医療機器メーカーから提供された SBOM を利用して、ソフトウェアの脆弱性を特定し、リスク・スコアなどの外部の脆弱性評価と組み合わせて SBOM の情報を利用できることが実証されました。以前は不可能だった方法でリスクを特定でき、ソフトウェアの透明性の取り組みに参加しているその他の業界にとっても価値があることが確認できました。現在は概念実証が、自動車業界とエネルギー業界に拡大しています。ヘルスケア・セクターの概念実証フェーズ２ではより複雑なユースケースの実証を行っています。

1.2.3.5　コンポーネント管理と品質・セキュリティ保証の取り組みまとめ

文献調査から、OSS の品質・セキュリティを保証するアプローチが 3 つ存在することがわかりました。まず、エネルギー業界や自動車業界でのサプライチェーン・セキュリティの標準

文書で定義されている、プロセスや検証活動による、製品やサービス全般の品質およびセキュリティの向上を目指す試みが存在します。これらの標準文書で定義された、脅威リスク分析、コード・レビュー、静的解析、ファジング・テスト、ペネトレーション・テストなどの検証活動は、プロプライエタリなソフトウェアに加えて、OSS に対しても適用することが可能です。しかしながら、使用する OSS コンポーネントの特定を事前に行っていない場合、新たに OSS の脆弱性が発見された際には、サプライチェーンで使用した OSS の特定を行い、使用するコンポーネントの分析を通して、システムを修正するためのパッチを発行する必要があり、そのタイムラインは、数か月または数年に及ぶ可能性があります。

OSS 管理のベストプラクティスとして、脆弱性管理に SBOM を利用すると、サプライチェーンの利害関係者は、すぐに使用する OSS を特定することができるので、新規の OSS 脆弱性が見つかった場合、迅速にリスク評価を行うことが可能となります。その結果、それに起因するソフトウェアの修正にかかるタイムラインの短縮を期待することができます。

さらに、NTIA で検討を行っている取り組みにみられるような、OSS に加えて商用ソフトウェアを含む、業界全体での標準化された SBOM 利用が進むと、サプライチェーンのエコシステム全体で、ソフトウェアの透明性が向上し、よりよいサプライヤーが選択され、自然淘汰と同様のプロセスを経て、サプライチェーンのエコシステム全体が品質やセキュリティに対して強靭なものとなります。

コンポーネント管理の強度と OSS の品質及びセキュリティ保証の取り組みを表 5 に示します。

表 5 コンポーネント管理の強度と OSS の品質・セキュリティの取り組み

コンポーネント管理レベル	説明	保証方法
レベル１	組織は、OSS に含まれるコンポーネントを把握せずに利用します。	OSS に対して、静的解析、機能テスト、ファジング・テスト、ペネトレーション・テストなど、ISO21434 や IEC62443 などの方法論で示される検証活動を実施します。最終製品・サービスでインシデントが発生した場合のリスク対応としては、アドホックなものとなり、コンポーネントの特定から修正パッチの配布まで、数か月から数年の単位となります。
レベル２	組織が、ソフトウェア部品表（SBOM）の作成をベースに、脆弱性管理などのベストプラクティスを選択して実施します。	コンポーネントが特定されているため、OSS コンポーネントの新規脆弱性を監視して、インシデント発生前にセキュリティ対策を実施することなどが可能となります。インシデントが発生した場合においても、コンポーネントの特定ができているので迅速な対応が可能となります。
レベル３	業界あるいは業界をまたがって、SBOM の利用を標準化します。米国 NTIA でソフトウェアの透明性の議論が続いています。（OSS だけでなく、商用ソフトウェアも管理します）	業界のエコシステム全体で品質・セキュリティの保証を行います。サプライヤーが淘汰されて強靭なエコシステムが出来上がります。

1.2.3.6　OSS の品質・セキュリティ保証方法調査

1.2.3.6.1　OSS の品質・セキュリティ保証方法調査方法

文献調査を基に定義したコンポーネント管理の強度のレベルごとの品質・セキュリティ保証方法が、国内のプロジェクトにおいて、どの程度行われているのかヒアリング調査を行いました。具体的には、レベル１の品質・セキュリティの検証活動、レベル２の OSS 管理のベストプラクティスについて、各プロジェクトでどの程度実施されているのかを確認しました。レベル３のサプライチェーン全体での SBOM 利用の取り組みについては NTIA のみで概念実証が行われているため、この項目のヒアリング調査は行いませんでした。なお、この調査は業界の傾向を見ることを目的とし、個社の状況を本報告書に記載しないこと、また、聞き取りを行った内容やユースケースに関しても、業界だけ記載し、企業名を出さないことを条件に、ヒアリングの協力をいただきました。調査を行ったプロジェクトは、1.2.2.1.1　OSS 活用状況調査で記載したプロジェクトと同様です。

図 6 に調査対象プロジェクトの内訳を示します。

図 6 調査対象プロジェクト

図　7　に NTIA の SBOM ワーキング・グループで検討中のサプライチェーンの役割モデルを示します。

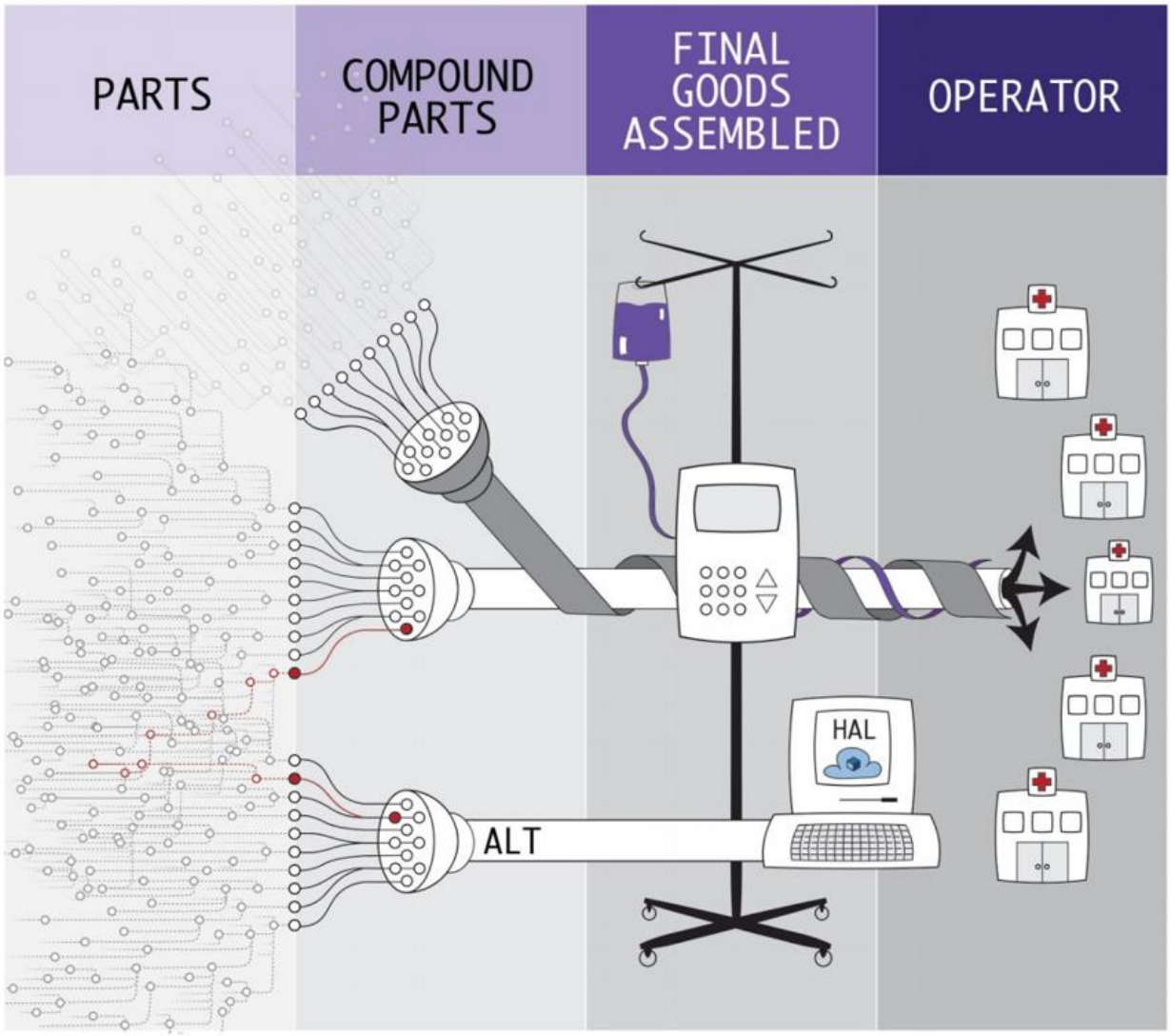

図 7　NTIA のサプライチェーンにおける役割のモデル[4]（出典：NTIA – Roles and Benefits for SBOM Across the Supply Chain）

図 7 のモデルは、医療機器業界におけるサプライチェーンを表しています。医療機器メーカーにより、「Final Goods Assembled（最終製品）」として、複数の医療機器が「Operator（運用者）」としての病院などの組織に提供されます。提供された医療機器は運用者の病院システムの一部として機能します。最終製品は、別の組織が提供する複数の「Compound Parts（構成部品）」から構成されています。その構成部品もまた別の組織が提供する、構成部品あるいは「PARTS（部品）」から構成されています。これらの階層構造全体でサプライチェーンのエコシステムを構成しています。

[4] https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf (2021/3 月時点で確認済み)

聞き取り対象のプロジェクトは、最終製品として組み込み機器を提供する組織、またはその基盤のソフトウェアを提供する組織が担当するプロジェクトであり、最終製品をシステムにとりこみ運用するプロジェクトはヒアリングの対象となりませんでした。 図 6 の「調査対象プロジェクト」における図 7 の「サプライチェーンの役割」の分類を表 6 に記載します。

表 6 対象プロジェクトのサプライチェーンにおける役割

	PARTS	COMPOUND PARTS	FINAL GOODS ASSEMBLED	OPERATOR
医療			A 社（医療機器）	
IoT		E 社（IOT 機器開発）	C 社（複合機） D 社(組み込みプラットフォーム製品) F 社（IOT 関連通信機器製品）	
自動車		B 社(自動車部品開発)		
エネルギー		B 社(制御機器)		

1.2.3.6.2 OSS の検証活動ヒアリング

品質・セキュリティ保証方法として、OSS に対しての検証活動が行われているかどうかは、各業界で異なることが予想されました。例えば、エネルギー業界では IEC62443 シリーズの EDSA 認証(Embedded Device Security Assurance)において、ファジングが検証項目として定義されており、この業界ではファジングが広く行われていることが推測されました。自動車業界で DIS となっている ISO21434 においては、脅威分析、ペネトレーション・テストなどの項目が見られます。この標準文書は、現時点でドラフトとなっていますが、最終版の内容に近いとされていますので、自動車業界のサプライヤーはこの内容に従って、プロセス構築と検証活動の準備をすすめていると推測されます。医療機器業界においては、米国食品医薬品局（FDA）で医療機器に関しての脅威分析レポートなどが義務付けられているケースがあり、これらの検証項目が行われていることが予想されました。

調査項目として、OSS に対して、以下に示すこれらの検証活動が実プロジェクトで実施されている

かどうかをヒアリングしました。

OSS の既知の脆弱性を含む脅威リスク分析

OSS を含む製品やサービスにおいて、システム全体の脅威リスク分析を行う際に、OSS の既知の脆弱性を対象として取り扱っているかどうかを確認します。典型的には NVD などの公開された脆弱性の情報をもとに、システムで利用する OSS の機能の一部を使用しているかどうか、すなわち対象となる脆弱性がどのようにシステムに影響するか分析し、セキュリティの対策を決定します。

OSS に対する静的解析

使用する OSS に対して、セキュア・コーディング・ルールをチェックする静的解析ツールなどを使用して、脆弱性が存在するかどうか確認します。静的解析ツールを利用すると、ソフトウェアの品質の問題を見つけることにもつながります。組み込みソフトウェアで広く使用されている、C 言語などは、バッファー・オーバー・フローなど、影響度の高い脆弱性が入り込みやすく、メンテナンスのされなくなった、あるいはサポート力の弱い OSS コミュニティのコンポーネントを利用する場合などで、あらかじめ、静的解析ツールを実行して、品質やセキュリティに関して、調査・分析することが考えられます。

OSS のコード・レビュー

サポートされなくなった古い OSS を利用する場合、あるいは人命や影響度の高いシステムで OSS を使用する場合、使用するコンポーネントのコードをレビューすることにより、品質・セキュリティに問題がないかどうかの確認を行うことができます。

OSS に対するファジング・テスト

組み込みデバイスのプロトコルスタックや、圧縮ファイルや画像ファイルの処理に OSS が使用されているケースがあります。このようなデバイスに対して、ファジングツールなどを使用して、予測不能なデータをこれらの OSS の機能への入力として送り、動作に問題がないかどうか確認することができます。ファジング・テストはペネトレーション・テストにおけるテスト項目の一部として行われることがあります。

OSS の既知の脆弱性に対するペネトレーション・テスト

ペネトレーション・テストを実施する際、OSS の既知の脆弱性を入り口とする検証を行うことが可能です。侵入者は OSS の既知の脆弱性を起点として、実際に運用されているシステムに侵入するケースがあります。この脆弱性を利用したペネトレーション・テストを行うことにより、効率的

にセキュリティに関する確認を行うことができます。

1.2.3.6.3　OSS の検証活動ヒアリング結果まとめ

表 7 に OSS の検証活動に関するヒアリング結果のまとめを示します。
実施していることが認められる場合に、「〇：実施している」として記載しています。印がない部分は実施が認められないケースです。

表 7 品質・セキュリティの検証項目ヒアリングまとめ

	医療 A 社	自動車・エネルギー B 社	IOT C 社	IOT D 社	IOT E 社	IOT F 社
OSS の脅威分析	〇	〇	〇		〇	
OSS の静的解析	〇					〇
OSS の コード・レビュー	〇					
OSS のファジング・テスト	〇	〇	〇		〇	〇
OSS のペネトレーション・テスト		〇			〇	
規制	FDA など	ISO21434 WP29 IEC62443 など			カリフォルニア州 IoT セキュリティ法など	カリフォルニア州 IoT セキュリティ法など

〇：実施している、印なし：実施が認められない

以下はヒアリングのまとめです。

- 社会の影響度が高い業界、ライフクリティカルな業界では、規制が存在し、広範囲に検証活動が実施されていることがわかりました。

- その他の IOT 機器の業界では、カリフォルニア州 IoT セキュリティ法など、ローカルな規制が取り決められている段階であり、各地で規制強化の動きが活発化しています。しかしながら、現時点では、エネルギー業界や医療業界などの包括的な規制は存在せず、検証活動を OSS コミュニティに依存する傾向が見て取れました。

- ヒアリングを行ったプロジェクトでは、検証活動で品質とセキュリティの問題を発見した場合、OSS コミュニティに報告・連絡して修正してもらう方法がとられていることがわかりました。

1.2.3.6.4 OSS 管理ベストプラクティスのヒアリング

以下の OSS 管理ベストプラクティスが実プロジェクトで実施されているかどうかのヒアリングを行いました。

ヒアリングにおいては、各プロジェクトが SBOM の作成を行っているか、また、どのような形式で SBOM を作成しているか、さらにその SBOM をどのように利用しているかに関して、聞き取り調査を行いました。

SBOM の作成

SBOM の作成は、OSS 管理のベースとなります。ソフトウェアに含まれる OSS の目録を作成することにより、様々なユースケースで SBOM の利用を行うことが可能になります。SBOM の形式は文書やエクセル・ファイルなどで作成する場合と、機械可読可能な形式、すなわち SPDX や SWID、あるいは CycloneDX などの形式で作成する場合があります。これらの機械可読可能な形式は SBOM 利用の自動化の前提となります。SBOM の利用が大規模になり、組織が様々なサプライヤーからの大量の SBOM データを照合及び管理する必要がある場合には、これらの機械可読可能な形式での SBOM 作成が重要な要件となります。
ソフトウェアを開発する場合には、SBOM は上流コンポーネントを含むソフトウェアの構築と保守を支援するために使用されます。ソフトウェアの設計時に、SBOM は OSS の既存の脆弱性のリスク評価に使用されます。ソフトウェアを運用する場合には、SBOM を脆弱性管理やライセンス管理に利用し、サプライチェーンのリスクを迅速に特定するために使用することができます。

SBOM の配布

SBOM は様々なソフトウェアで利用可能であるため、ソフトウェアのサプライヤーが下流工程で使用するために SBOM を利用者に配布し、コンポーネントの情報を共有することができます。配布された SBOM をシステムに取り込むことによって、運用時の脆弱性管理などのユースケースに役立てることが可能です。また、SBOM を顧客または下流工程のパートナーに提供して、サプライヤーが顧客の法的およびセキュリティのニーズを満たす高品質の製品を提供していることをアピールすることができます。 SBOM の共有に積極的であることは、SBOM の採用が増えるにつれて、競争上の優位性を確立することにつながります。ヒアリングにおいて、SBOM の配布が行われているかどうかを調査しました。

SBOM 利用のユースケース：脆弱性管理

SBOM に記載された OSS コンポーネントの情報をもとに、NVD の脆弱性データベースで開示された脆弱性を特定することができます。理想的には、脆弱性の検索を自動化し、環境に潜む脆弱性を早期に警告する仕組みが実装されていれば、新規の脆弱性が公開された際に、必要に応じて製品やサービスが攻撃される前にパッチを運用システムに供給することができます。

SBOM 利用のユースケース：ライセンス管理

SBOM の使用により、使用されている OSS コンポーネントのライセンス義務を認識し、遵守することができます。 ライセンス・ポリシーを適用しやすくなり、ライセンス・コンプライアンスの自動化に役立ちます。ライセンス管理のユースケースでは、OSS の利用を検討しているユーザーは、SBOM を使用して、構成コンポーネントのライセンスを可視化します。これにより、ユーザーは、製品を選択する際の認識が高まり、ビジネスニーズやアプリケーションに適したライセンス契約を結ぶことができます。

SBOM 利用のユースケース：脅威リスク分析

製品設計時あるいは OSS コンポーネントの調達時に、SBOM を使用して、脅威・リスクの分析を行うことができます。NVD などの脆弱性データベースを参照し、既存の脆弱性を特定し、その脆弱性が悪用可能であるかなどを判定して、リスクの評価を行います。判定されたリスクの影響度に応じて、適切なセキュリティの対策を行うことが可能となります。また、OSS コンポーネントのサービス終了（EOL:End Of Life）を判定して、メンテナンス上のリスクを検出するようなユースケースも考えられます。

1.2.3.6.5 OSS 管理ベストプラクティスのヒアリング結果まとめ

表 8 に OSS 管理ベストプラクティスのヒアリングのまとめを示します。

表 8　OSS 管理ベストプラクティスのヒアリング結果まとめ

	医療 A 社	自動車・エネルギー B 社	IOT C 社	IOT D 社	IOT E 社	IOT F 社
SBOM の作成	文書ベース	文書ベース	文書ベース	文書ベース	文書ベース	文書ベース
SBOM の配布	顧客から依頼があれば文書で配布	顧客から依頼があれば文書で配布				
脆弱性管理	設計時、開発時、運用サポート時に脆弱性を確認する	設計時、開発時、運用サポート時に脆弱性を確認する	設計時、開発時、運用サポート時に脆弱性を確認する	開発時、運用サポート時に脆弱性を確認する	設計時、開発時、運用サポート時に脆弱性を確認する	設計時、開発時、運用サポート時
ライセンス管理	エクセルベースで SBOM を作成し、ライセンスやコンプライアンスの問題がないように管理している。	設計時、開発時に SBOM を作成し、OSS 評価や意図しない OSS 混入によるライセンス遵守違反を抑止している。	ホワイトリストを作成して、使用したことのない OSS に関しては法務部門および開発部門に連絡が入るようになっている。			

リスク、脅威分析	SBOM をベースに、開発時には既存の脆弱性があるか、運用・サポート時は新規の脆弱性があるかどうか、手動で確認している。	EOL（End Of Life, OSS コンポーネントのサポート終了）に関しては、各プロジェクトに情報を配信している。	脆弱性データベース（NVD）を参照して、脅威分析に役立てている		OSS の既知の脆弱性を評価し脅威分析を行う	

記述あり：実施している、記述なし：実施が認められない

以下はヒアリングのまとめです。

- 聞き取り調査の結果、各プロジェクトで、SBOM を作成し、使用する OSS コンポーネントを把握していることがわかりました。この結果については、調査協力依頼時に SBOM 利用有無についても確認させていただく旨をお伝えしているため、SBOM を作成している企業だけがヒアリングを受けてくれた可能性があります。

- 聞き取りを行った対象プロジェクトは、最終製品あるいはその一部のソフトウェア開発を担当しており、SBOM を OSS 調達時のリスク分析や脆弱性管理、開発時の OSS の評価、運用時の保守など様々な用途で使用しています。

- SBOM は文書またはエクセルベースで作成されており、SPDX などの機械可読可能な形式で、SBOM の作成を行い、SBOM 利用を自動化しているプロジェクトはありませんでした。

- SBOM の配布に関しては、一部のプロジェクトで限定的に行われていることがわかりました。サプライヤーは顧客から要求がある場合のみ、文書ベースで配布を行っています。機械可読可能な形式で SBOM の配布が行われる事例は見当たりませんでした。

- 脆弱性の管理に関して、運用サポートにおいて、SBOM をベースに手動で NVD などの脆弱性データベースの確認を行い、新規の脆弱性を監視することが行われていました。ただし、脆弱性の監視を自動化している事例は見られませんでした。

- 作成された SBOM をベースに手動でライセンス管理やリスク脅威分析に利用していることが判明しました。リスクの分析は、脆弱性に加えて、コンプライアンス、OSS コンポーネントのサポート終了（EOL）のリスクの管理にも利用されています。

1.2.3.6.6 OSS の品質・セキュリティ保証方法調査まとめ

複雑なソフトウェアのサプライチェーンに対して、プロセスと検証活動によってセキュリティを担保しようとする試みは、エネルギー業界、医療機器業界、自動車業界などの社会の影響度が高い業界、ライフクリティカルな業界では、関連する規制が存在し、プロプライエタリなコードに加えて、利用する OSS に対しても、広範囲に検証活動が実施されていることが分かりました。その他の IOT 業界に関しても、規制強化の動きがみられますので、OSS に対する検証活動が拡大することが予想されます。

国内プロジェクト調査の結果、多くのプロジェクトで SBOM が作成されており、SBOM を OSS 調達時のリスク分析や脆弱性管理、開発時の OSS の評価、運用時の保守など様々な用途で使用していることが分かりました。しかしながら、調査した範囲では、SBOM が文書またはエクセルベースで作成されており、機械可読可能な形式で SBOM の作成を行っているケースはありませんでした。SBOM 利用が進んだ場合、大量の SBOM を効率よく処理するために、機械可読可能な SBOM を使用して、自動化を行う方法を確立することが今後の課題となります。

1.2.3.7 OSS の品質保証や製品セキュリティ維持に関わる組織・団体

ここでは、OSS の品質保証や製品セキュリティの維持に関わる団体について記載します。

1.2.3.7.1 NIST

NIST（National Institute of Standards and Technology：米国国立標準技術研究所）は、情報セキュリティ強化のための規格としての FIPS（Federal Information Processing Standards：連邦情報処理標準）やガイドライン（SP800 シリーズ）の開発を行っています。NIST は SCAP（Security Content Automation Protocol：セキュリティ設定共通化手順）を開発し、「脆弱性管理、コンプライアンス管理の一部を機械化(自動化)することにより、情報システムに対するセキュリティ対策の負荷軽減と情報セキュリティ施策の推進の両立を目的とした仕様群」を定義しています(NIST 800-126,NIST 800-117,NISTIR 7511 rev2)。この仕様は米国の National Vulnerability Database (NVD)や JPCERT/CC と情報処理推進機構(IPA)が共同管理している、脆弱性データベースの Japan Vulnerability Notes（JVN)や JVN iPedia で使用されています。これらのデータベースには、OSS の脆弱性も含まれています。

1.2.3.7.2 MITRE Corporation

MITRE は米国政府の支援を受けている非営利団体で、CVE（Common Vulnerabilities and Exposures：共通脆弱性識別子）を管理しています。新しい脆弱性情報が公開される際に、「CVE 識別番号（CVE-ID)」が割り振り振られます。この割り振りを行うのは CVE Numbering Authorities (CNAs）の役割です。CVE は多くのセキュリティ・ツールで使用されています。

1.2.3.7.3 NTIA

米国 NTIA(電気通信情報局)において、ソフトウェアのサプライチェーンに対する可視性について議論が進められています。SBOM の仕様を作成、SBOM ユースケースの検討分析、ヘルスケア業界などで概念実証を行うなど、業界全体のエコシステムにおける、品質およびセキュリティに関する、強靭なソフトウェアのサプライチェーンの構築を検討しています。

1.2.3.7.4 SPDX (Linux Foundation)

SPDX プロジェクトは、ソフトウェア・コンポーネントに関連するコンポーネント、ライセンス、著作権、およびセキュリティ情報を複数のファイル形式で通信するための標準言語の仕様を取り

決めています。SPDX は交換できるデータを記述するための拡張性のある言語で、ソフトウェア・パッケージおよび関連コンテンツに関する情報を簡単に収集および共有することができます。SPDX は NTIA SBOM　のワーキング・グループの議論の中で SBOM の機械可読なフォーマットの一つとして検討されています。

1.2.3.7.5　JPCERT/CC

JPCERT コーディネーションセンター（JPCERT/CC）は、インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティ・インシデントについて、日本国内に関するインシデント等の報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっています。特定の政府機関や企業からは独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいます。

1.2.3.7.6　独立行政法人情報処理推進機構（IPA）

IPA では、日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的として脆弱性対策情報ポータルサイト「Japan Vulnerability Notes（JVN)」を運営しています。JVN は、JPCERT コーディネーションセンターと共同で運営されています。

(1) 脆弱性対策情報ポータルサイト「Japan Vulnerability Notes（JVN)」
JVN には、CERT/CC など海外の調整機関と連携した脆弱性情報が公表されています。

(2) 脆弱性関連情報の届出受付窓口の運営
IPA では、以下脆弱性関連情報の届出を受付けている[5]。

- ソフトウェア製品脆弱性関連情報
- ウェブアプリケーション脆弱性関連情報

[5] 独立行政法人情報処理推進機構 脆弱性関連情報の届出受付

https://www.ipa.go.jp/security/vuln/report/index.html (2021/3 月時点で確認済み)

1.2.4　SBOM の動向（国内、海外）

1.2.4.1　NTIA の活動

ここでは、NTIA で行われている SBOM の活動の取り組み状況をまとめ報告します。

2018 年から NTIA において、ソフトウェアのサプライチェーンに対する可視性についての課題が議論されています。

現在、ほとんどのソフトウェアはサードパーティのコンポーネント（ライブラリ、実行可能ファイル、またはソースコード）に依存していますが、ソフトウェアのサプライチェーンに対する可視性はほとんど存在せず、十分に識別または記録されていない多数のサードパーティ・コンポーネントが含まれているのが一般的です。このソフトウェアの構成に対するこの体系的な透明性の欠如は、サイバーセキュリティのリスク、開発、調達、および保守のコストにも大きく影響しています。

ソフトウェアは複数の業界にまたがっており、基盤となるコンポーネントは、OSS と商用ソフトウェアの共通の基盤から得られます。 このため、どのソリューションもエコシステム全体で機能する必要があります。NTIA で議論されているソリューションはソフトウェアの「成分リスト」です。 これはソフトウェア部品表（SBOM）として知られており、この SBOM により、ソフトウェアの透明性を高めて、潜在的に脆弱なシステムを早期に特定し、情報に基づいた購入決定をサポートし、安全なソフトウェア開発慣行を奨励します。

SBOM の導入で、システムまたはデバイスにインストールされているソフトウェアの「要素」を知ることで、リスク分析、脆弱性管理、および修復プロセスで数百時間を節約できるとしています。

現在、NTIA では SBOM に関して以下の 6 つのワーキング・グループに分かれて活動が行われています。

- フレーミング・ワーキング・グループ（以降、フレーミング WG という）
- 意識と採用(Awareness and Adoption)
- フォーマットとツール
- ヘルスケアの概念実証
- 自動車業界の概念実証
- エネルギーの概念実証

以下の２つのワーキング・グループは 2019 年で活動を完了させています。

- ユースケースと事例
- 標準とフォーマット

表 9　NTIA の SBOM に関するワーキング・グループの活動内容

ワーキング・グループ	活動内容
フレーミング（問題を理解する）	SBOM の仕様の定義とその改良を行う。フェーズ１では、SBOM データの共有方法など、ソフトウェアの透明性の概念の範囲と、ソフトウェアが解決しようとしている問題について分析しました。成果物には、（1）ベースライン SBOM 要素の説明、（2）目標、問題の説明、および範囲の特定、（3）有用な用語、（4）基本的なプロセスと実装ガイドの概要が含まれています。現在の、フェーズ 2 としての取り組みは、脆弱性の悪用可能性ステータス（VEX と呼ぶ）に関する仕様と一般的な用語セットの定義に焦点を当てて活動しています。
ユースケースと事例（Use Cases & State of Practice ）	各業界において SBOM がどのように使用されているかユースケースを調査し、SBOM の役割とその利点について以下の文書として公開しています。

	サプライチェーン全体での SBOM の役割と利点(Roles and Benefits for SBOM AcrOSS the Supply Chain)[6]
意識と採用(Awareness and Adoption)	2020 年から「ユースケースと事例」ワーキング・グループを引き継いで、SBOM を促進するためのアウトリーチ活動を行います。NTIA SBOM のウェブサイト[7]の更新、SBOM のイントロダクション文書[8]や FAQ 文書[9]の作成を担当しています。
標準とフォーマット	ソフトウェア製品の構築に使用される、商用または OSS の外部コンポーネントと共有ライブラリの識別に適用される既存の標準とイニシアチブを調査し、この透明性が機械で読み取り可能な方法ですぐに利用できることを保証することに関連する、コミュニティおよび業界で進行中の取り組みを調査分析した。 2020 年以降、「フォーマットとツール」ワーキング・グループで、引き継いで活動を行っている。
フォーマットとツール	2020 年から「標準とフォーマット・ワーキンググループ」を引き継いで、ツールの文書化、ツーリング・ギャップ、プロセスの文書化に焦点を当て活動している。現在、以下の SBOM の作成者と利用者側のガイドライン文書を作成している。 • Supplier Playbook • Consumer Playbook
ヘルスケアの概念実証	SBOM が医療機器に関連する、リスクを軽減するために提供する価値を実証することを目的としています。医療機器メーカー（MDM）と医療提供組織（HDO）が、病院の医療機器に対する運用およびリスク管理を行うためのいくつかのユースケースで、SBOM をうまく活用できることを実証することが目的です。現在

[6] https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf (2021/3 月時点で確認済み)

[7] https://www.ntia.gov/SBOM (2021/3 月時点で確認済み)

[8] https://www.ntia.gov/files/ntia/publications/sbom_overview_20200818.pdf （2021/3 月時点で確認済み）

[9] https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf （2021/3 月時点で確認済み）

	は 2019 年にされたフェーズ 1 の概念実証[10]の追加のユースケースをフェーズ 2 として、概念実証を継続しています。
自動車業界の概念実証	米国 NHTSA (National Highway Traffic Safety Administration)から「現代の車両の安全のためのサイバーセキュリティのベストプラクティスのドラフト 2020 アップデート」において、SBOM 関連のベストプラクティスが記載されました。この内容を受けて、NTIA において自動車業界における SBOM の概念実証プロジェクトが計画されています。 このプロジェクトはサプライヤー主導のプロジェクトで以下が目的です。 • SBOM の原則と運用を研究して理解する • 自動車業界で SBOM の事例を作成する • 自動車メーカー/パートナーからのインプットによる実用的なアプローチとソリューション • 実装の演習を実施 • 業界からの推奨と同意の取得 • サプライヤーによる自主的な採用を奨励/促進 このプロジェクトの成果物として、自動車メーカーに対する、業界標準に関するサプライヤーの推奨事項を記載した報告書作成が予定されています。（作成期間は約 12 か月間の予定）
エネルギー業界の概念実証	NTIA において、ヘルスケア業界と自動車業界の概念実証に続いて、エネルギー業界においても概念実証を行うことになりました。 NTIA のエネルギー・セクターの概念実証は、ヘルスケア・セクター、自動車セクターの概念実証同様、規制を促進するためのガイドラインを作成するものではなく、民間部門による重要な新技術の使用を促進しようとするものです。

[10] https://www.ntia.gov/files/ntia/publications/ntia_sbom_healthcare_poc_report_2019_1001.pdf (2021/3 月時点で確認済み)

1.2.4.1.1 問題の特定と SBOM の利用によるリスク軽減

フレーミング WG は、その成果物[11]のなかでソフトウェア・システムの以下の問題を特定しています。

- 複雑で動的なサプライチェーンが含まれる最新のソフトウェア・システムにおいて、システムの構成と機能に対する体系的な可視性の欠如がサイバーセキュリティのリスクに大きく影響し、さらに開発、調達、および保守のコストも増加させる結果につながっています。

- システムが相互接続されるにつれ、リスクとコストは個人や組織だけでなく、公安や国家安全保障などの公共財にも影響を及ぼしています。

SBOM により、サプライチェーンの透明性を高めることで、サイバーセキュリティのリスクと全体的なコストを次のように減らすことができるとしています。

- サイバーセキュリティ・インシデントの原因となる脆弱なソフトウェア・コンポーネントを特定する機能を向上させます。

- 複雑なサプライチェーンによる計画外の非生産的な作業を削減します。

- 透明性をサポートするベンダーが、市場でより簡単に差別化できるようにします。

- 複数のセクターにまたがるフォーマットを標準化することにより、作業の重複を減らします。

- 疑わしいまたは偽造されたソフトウェア・コンポーネントの識別を容易にします。

1.2.4.1.2 SBOM の仕様

[11] Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)

https://www.ntia.gov/files/ntia/publications/ntia_sbom_healthcare_poc_report_2019_1001.pdf（アクセス 2021.1）

フレーミング WG により、NTIA で取り扱う SBOM の仕様の定義[12]が進められています。SBOM を構成する必要最低限の情報であるベースライン情報や SBOM 利用における役割などを定義しています。

フレーミング WG は、ゴールを以下のように設定しています。

サプライチェーンの透明性を高めるためには、業界全体で普遍的かつ透過的に共有できるソフトウェア・コンポーネント情報のモデルを作成することが必要です。このモデルは、ソフトウェアの部品表である SBOM を定義および記述します。コンポーネント間の関係、SBOM の作成と共有、参加者の役割、およびサプライチェーン間の SBOM の統合に対応させる必要があります。このモデルを普遍的に使用できるようにするには、ソフトウェア・コンポーネントの特定をユニバーサルに識別および定義するという難しい問題に対処する必要があります。したがって、最初の中間的な目標としては、十分な相対的一意性を持つコンポーネントを識別するために必要な、コアとなるベースラインの属性セットを選択することになります。もう 1 つの目標は、各種 SBOM ユースケースを分析し、ベースライン・セットを超えて必要になる可能性のある、追加のオプションの属性と外部要素を検討することです。

フレーミング WG による SBOM の定義

SBOM は、ネストされたインベントリであり、ソフトウェア・コンポーネントを構成する要素のリストです。 SBOM は、ソフトウェア・コンポーネント、それらのコンポーネントに関する情報、およびそれらの間のサプライチェーン関係を識別して一覧します。特定の SBOM に含まれる情報の量と種類は、業界やセクター、SBOM の利用者のニーズなどの要因によって、異なる場合があります。基本的かつ重要な機能をサポートするために必要な最小限の情報とプロセスの概要を示すベースライン SBOM を作成するための最小限のセットを抽出することに焦点が当てられます。

ベースラインの情報セットを定義することにより、SBOM に関連する、さまざまな利害関係者が SBOM を採用することを容易にし、その後、時間をかけて、より堅牢な属性のセットを持つ SBOM 利用を発展させていくようなアプローチを採用することができるようになります。

コアまたは最小ベースライン SBOM を超えて、さまざまなセクター内で、さらなる開発と実践が成熟するにつれて、追加情報が必要になる場合があります。 SBOM は、ソフトウェア・システムを構

---

[12] Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM) (2021/3 月時点で確認済み)

https://www.ntia.gov/files/ntia/publications/ntia_sbom_healthcare_poc_report_2019_1001.pdf (2021/3 月時点で確認済み)

成するサプライチェーンを通じて、各コンポーネントを、他のコンポーネントに関連付ける必要もあります。コンポーネント間でこれらのリンクを取得して交換することは、SBOM の重要な機能です。

構造化されたデータ形式と交換プロトコルは、機械可読性と自動化を可能にするため、SBOM をより機能的にするために必要な、重要な特徴です。大規模な SBOM 利用者組織は、さまざまなサプライヤーからの大量のデータを照合および管理する必要があるため、このデータの利用者が効率と拡張性のために機械可読形式でこれを管理できるようにすることが重要です。

SBOM は、他のデータ・ソースから完全に分離された独立した要素としては存在しません。 たとえば、脆弱性管理で SBOM を使用するには、既知の脆弱性のカタログ（CVE など）、脆弱性とコンポーネントの関連付け（NVD による CPE の使用など）、および場合によっては一時的な悪用可能性を伝達する手段が必要です。 ライセンス管理に SBOM を使用するには、ライセンスとその制限が、コンポーネントに関連付けされている必要があります。

ベースライン情報

SBOM の主な目的は、コンポーネントとそれらの相互関係を一意かつ明確に識別することです。そのためには、以下のベースライン情報の組み合わせが必要です。すべての SBOM エントリが、各ベースライン属性を必要とする、または提供できるとは限らない可能性があります。特定の属性（コンポーネント・ハッシュなど）は、より高い一意性または明確性を提供します。特定されたベースライン・コンポーネント情報を表 10 に示します。

表 10　SBOM ベースライン情報

属性	英語名	説明
記載者名	Author Name	SBOM エントリの記載者（これは常にサプライヤーであるとは限りません）。
サプライヤー名	Supplier Name	SBOM エントリ内のコンポーネントのサプライヤーの名前または ID。複数の名前またはエイリアスを記録する機能を含みます。記載者とサプライヤーが同じである場合、サプライヤーはファースト・パーティの信頼できるコンポーネントを定義しています。記載者とサプライヤーが異なる場合、記載者は異なるサプライヤーのコンポーネントについてアサーションを行います。このアサーションの信頼性は指定されません。

コンポーネント名	Component Name	複数の名前またはエイリアスを記録する機能を含む、1 つ以上のコンポーネント名。コンポーネント名は、サプライヤー名を伝えることができます。コンポーネント（およびサプライヤー）の名前は、汎用の namespace：name 構文を使用して伝達できます。
バージョン文字列	Version String	バージョン情報は、コンポーネントの識別に役立ちます。どのように記載者、サプライヤー、またはコンポーネントを特定して、名前を付けるのか、その方法は指定されません。基本的な一貫性とロジック（セマンティック・バージョニングなど）を期待する以外は、バージョン情報の構文も指定されません。
ユニーク ID	Unique Identifier	一意の識別子を生成して、コンポーネントの識別に役立てることができます。この識別子のため、バージョン 4 またはバージョン 5 の UUID が利用可能です。
コンポーネント・ハッシュ	Component Hash	コンポーネントの暗号化ハッシュを追加することは、SBOM 内のバイナリの構築済みコンポーネントを識別する最も正確な方法です。ハッシュは事実上コンポーネントの一意の識別子ですが、他のベースライン識別情報も有用であり、必要です。暗号化署名はハッシュの代わりに使用できますが、鍵の配布と署名の検証の複雑さが増します。
関係	Relationship	関係は SBOM の設計に内在しているものです。デフォルトの関係タイプは「含む」includes です。

SBOM は、ベースライン情報に加えて、さまざまなユースケースをサポートするために、追加のコンポーネント情報を必要とします。 必要な特定の情報はユースケースによって異なり、すべての追加情報が、各ユースケースをサポートするわけではありません。

コンポーネントの関係

SBOM を開発する最初のステップは、多くの場合、第 1 レベルのコンポーネントの単純なリストから始めることです。しかしながら、SBOM を効果的に拡張するためには、コンポーネント間のネストされたサプライチェーン関係を、それらの関係が、分かっている範囲で取得する必要があります。物理コンポーネントの部品表では、これらの関係は「マルチレベル BOM」と呼ばれます。SBOM は多くのタイプの関係を説明する場合がありますが、ベースライン情報では、含む（または含まれる）という単一のタイプの関係で定義されます。つまり、上流または子のコンポーネントは、下流または親のコンポーネントに含まれます。

図 8 では、Q 社の通信機能は P 社のアプリケーションの上流であり、Q 社は P 社の上流サプライヤーです。 「含まれる」と「上流」という言葉は同義語です。「含まれる」関係に加えて、他のタイプの関係が、必要または有用な場合があります。現在、既存の SBOM フォーマット（SPDX や SWID など）は、さまざまなタイプの関係がサポートされています。

SBOM の例

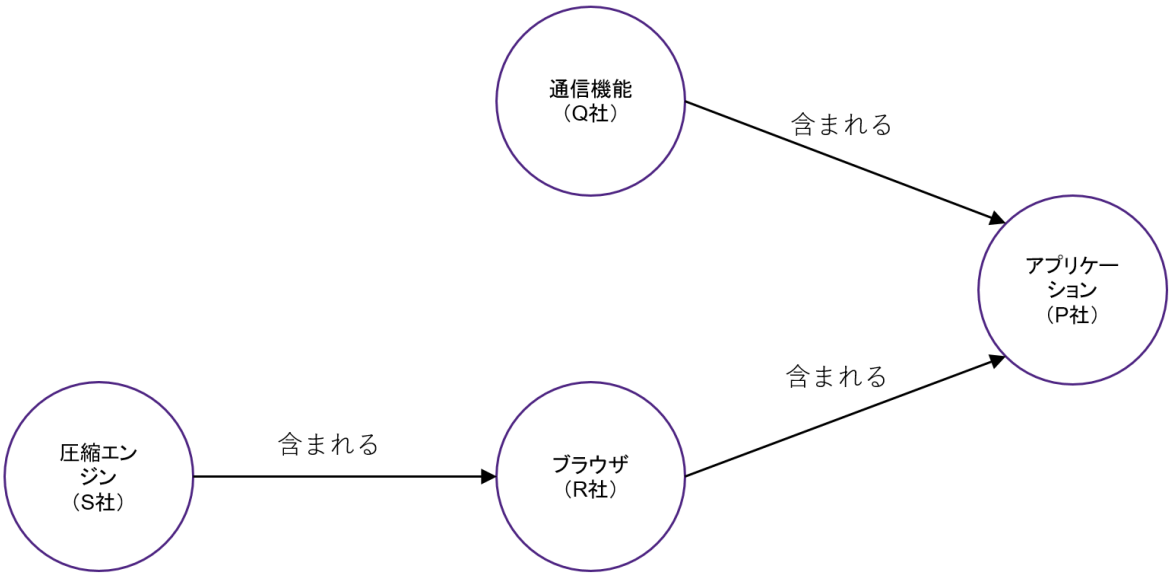

図 8　SBOM ツリー概念図

図 8 を異なる方法で、SBOM 情報と関係を表示したものが表 11 です。

表 11　SBOM 表概念図

コンポーネント名	サプライヤー名	バージョン文字列	記載者名	コンポーネント・ハッシュ	ユニーク ID	関係
アプリケーション	P 社	1.1	P 社	0x123	234	自身
|-- ブラウザ	R 社	2.1	R 社	0x223	334	含まれる
|-- 圧縮エンジン	S 社	3.1	P 社	0x323	434	含まれる
|-- 通信機能	Q 社	2.2	P 社	0x423	534	含まれる

図 8 と表 11 では、P 社アプリケーションの SBOM には 4 つのコンポーネントがあります。これは、各 SBOM に、それ自体が含まれているためです。 P 社は、R 社ブラウザと Q 社の通信機能の 2 つのサードパーティ・コンポーネントを使用する、「アプリケーション」という名前のコンポーネントを作成します。 次に、R 社のブラウザは、S 社の圧縮エンジンを使用し、他のコンポーネントも使用する場合があります。 S 社の圧縮エンジンには、それ以上のサブコンポーネントは含まれていませんが、通信機能にはそれ以上の依存関係がある場合と、ない場合があります。

サブコンポーネントは、上位コンポーネントまたは親コンポーネントのいくつかの依存機能を提供することを目的としていますが、サブコンポーネントの一部に関しては、その依存関係の一部が機能しないのが一般的です。たとえば、ソフトウェア・プログラムにライブラリ・サブコンポーネントが含まれていても、ライブラリによって提供される機能の一部のみを使用する場合があります。これは、一部の SBOM ユースケース、特に脆弱性管理で重要になります。脆弱性がサブコンポーネントに影響を与える場合、そのサブコンポーネントを親コンポーネントに含めると、親コンポーネントが脆弱になる場合と、そうでない場合があります。

SBOM は 1 つ以上のコンポーネントで構成され、各コンポーネントは事実上、別の SBOM であり、複数のコンポーネントが含まれている場合があります。 SBOM には少なくとも 1 つのプライマリ・コンポーネントが含まれている必要があり、このプライマリ・コンポーネントは、コンポーネントと SBOM の両方を定義および識別します。 SBOM にリストされている、他のすべてのコンポーネントは、「含まれる」関係にあります。

関係の知識

理想的には、すべてのサプライヤーがコンポーネントの SBOM を作成して提供し、すべての利用者が、これらの信頼できる SBOM の完全な構造を取得できることです。この場合、すべてのコンポーネントについて、記載者名はサプライヤー名と等しくなります。しかしながら、SBOM の記載者がすべてのコンポーネントを特定できない場合などでは、不完全な SBOM を提供することにより、利

用者にその SBOM を過度に信用させてしまう恐れがあります。こうした SBOM の信頼の状態を区別するために、関係アサーションを行うことができます。

関係アサーションは、ベースライン情報に、追加のコンポーネント属性を使用して、SBOM の記載者が記録することが可能です。*表 12*に示す、4 つのカテゴリーによって、別のサプライヤーのコンポーネントに関する、記載者の知識の範囲を区別します。

表 12 関係アサーション

関係アサーション	説明
不明	これがデフォルトです。上流コンポーネントに関する知識、または主張はまだありません。隣接した上流コンポーネントは現在不明であるため、まだリストされていないか、上流コンポーネントがない可能性があります。
ルート	上流の関係はありません。サプライヤーによって、コンポーネントには、サブコンポーネントが存在しないことが示されます。
部分的	少なくとも 1 つの、すぐ上流の関係があり、他の関係がある場合とない場合があります。既知の関係がリストされます。
既知	すぐ上流の関係について、完全なセットがわかっており、リストされています。

関係アサーションはコンポーネントに適用され、そのすぐ上流の関係を記述します。図 9 と表 13 は、図 8 と表 11 の例に関係アサーションを追加しています。

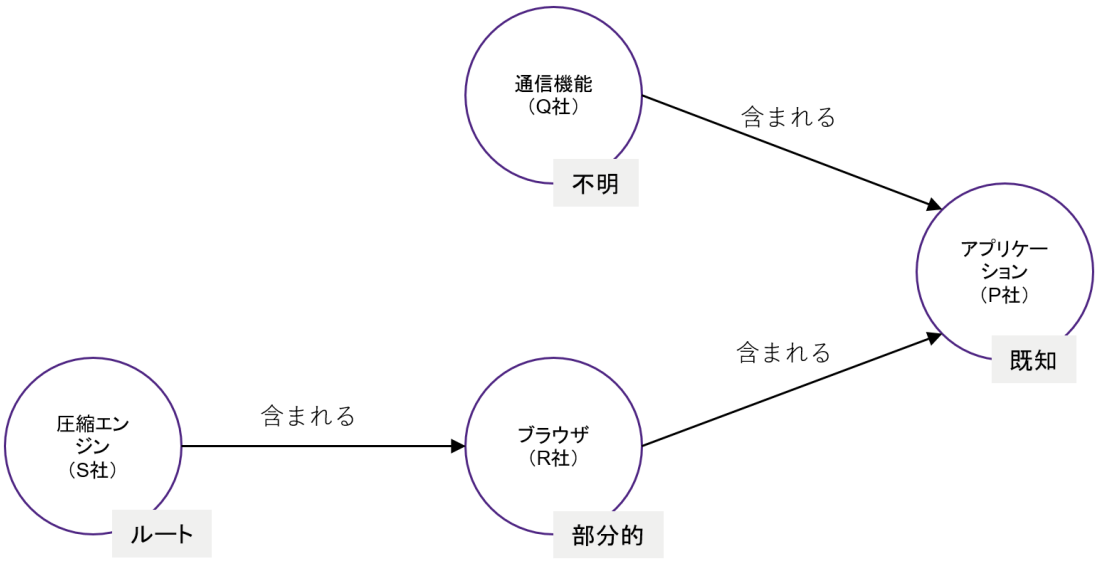

図 9　SBOM ツリー概念図（関係アサーション）

表 13　SBOM 表概念図（関係アサーション）

コンポーネント名	サプライヤー名	バージョン文字列	記載者名	コンポーネント・ハッシュ	ユニークID	関係	関係アサーション
アプリケーション	P 社	1.1	P 社	0x123	234	自身	既知
|-- ブラウザ	R 社	2.1	R 社	0x223	334	含まれる	部分的
|-- 圧縮エンジン	S 社	3.1	P 社	0x323	434	含まれる	ルート
|-- 通信機能	Q 社	2.2	P 社	0x423	534	含まれる	不明

SBOM は、ベースライン情報に加えて、さまざまなユースケースをサポートするために、追加の要素とコンポーネント属性を必要とします。 必要な特定の情報はユースケースによって異なり、すべての追加情報が、各ユースケースに必要になるわけではありません。

SBOM システムは、SBOM 情報を暗号化技術で認証する機能をサポートする必要があります。
一般に、これは、記載者が SBOM に、デジタル署名できる必要があることを意味します。 認証はオプションで、記載者は SBOM に署名する必要はありません。認証には、適切なデジタル署名と公開鍵インフラストラクチャが必要です。

データ・フォーマット

SBOM データを機械で生成、共有、および処理できる場合、ソフトウェア・コンポーネントの透過性の利点の多くは、より簡単に実現できます。機械処理と自動化には、サプライチェーン全体にわたる広範な相互運用性が必要であり、そのためには、標準化されたデータ形式と識別スキームが必要です。

利害関係者は、既存の標準と形式を列挙してレビューするためのワーキング・グループを結成しました。このワーキング・グループは、SBOM のユースケースのみに対応するように、明示的に設計された単一の標準はないものの、広く使用されている 2 つの形式を特定しました。それは、SPDX と SWID です。SPDX は、LinuxFoundation が管理するオープンソースの機械可読形式です。 SWID は、商用ソフトウェア発行者によって使用され、NIST によって適合された国際的な XML ベースの標準です。これらの標準は、両方とも、ベースライン SBOM 情報の要件に合致しています。どちらの形式も、ソフトウェア・エンティティの識別と、関連するメタデータの伝達という、主要な問題に焦点を当てており、ベースライン SBOM のニーズを満たすために必要なフィールドがあります。さまざまなコミュニティが、ニーズに合った形式を選択できますが、ベースライン SBOM データは、簡単な変換を行うことによって、サプライチェーン全体で使用することができます。

SBOM プロセス

ソフトウェアを作成、選択、および操作する、3 つの利害関係者の観点から、SBOM 情報を作成および交換する方法について定義します。

SBOM の作成方法

SBOM を作成するために、サプライヤーは、サプライヤーが自分で作成するコンポーネントを定義し、ベースライン・コンポーネント情報と、それらのコンポーネントの追加属性を生成し、直接含まれる、すべてのコンポーネントのリストを列挙します。SBOM 情報は、理想的には、サプライヤーのソフトウェア・ビルドおよびパッケージング・プロセスの不可欠な部分として生成されます。これは、既存の開発ツールを変更することで実現できます。ソフトウェアまたはソフトウェア・システムを作成、変更、パッケージ化、および配信する役割は、サプライヤーと見なされるため、サプライヤーは、コンポーネントの定義と、SBOM の作成を担当することになります。
組織は、社内で開発されたコンポーネントのサプライヤーとして機能することもできます。含まれているコンポーネントの SBOM が、上流のサプライヤーから入手できる場合、それらの SBOM は、プライマリ SBOM とともに提供されるか、プライマリ SBOM に追加されます。そのような情報が利用できない場合、サプライヤーは「ベストエフォート」SBOM を提供することになります。これは、含まれるコンポーネント SBOM の記載者が、コンポーネントのサプライヤーと同じではないということを示します。SBOM 記載者が、その上流のサプライヤーが SBOM を提供していない、間接的に含まれる上流コンポーネントについてのアサーション（その上流コンポーネントの一部が、部分的または不明であることを宣言する）を作成することで、「ベストエフォート」SBOM かどうかを区別することができます。
SBOM には、コンポーネントを識別するために使用される属性と、コンポーネントの特性、または、コンポーネントに関する情報を取得するための追加の属性が含まれています。 ID 属性が必要であり、ユースケースに応じて、追加の属性が必要な場合と不要な場合があります。コンポーネントのサプライヤーからの SBOM は、コンポーネントに関する記録システムまたは信頼できる情報源として機能します。一部の情報は、他の外部ソースで検証する必要がある場合があります。たとえば、コンポーネントに関する脆弱性情報は、Common Platform Enumeration (CPE) を使用して、National Vulnerability Database (NVD) から取得できる場合があります。

SBOM の作成のタイミング

コンポーネントの新しいリリースごとに、新しい SBOM を作成する必要があります。コンポーネントを変更するには、SBOM に対応する変更が必要です。コンポーネントへの変更は、多くの場合、更新、アップグレード、リリース、およびパッチとして示されます。理想的には、コンポーネントへの変更は、ベースラインのバージョン文字列属性の変更によって示されます。 SBOM は、コン

ポーネント自体が変更されていない場合でも、含まれているコンポーネントに関する情報が変更されたときに作成または更新する必要があります。たとえば、含まれているコンポーネントが変更されたとき、およびサプライヤーが新しい SBOM 情報の提供を開始または提供し始めたときに、SBOM を更新する必要があります。前者の場合、基盤となるソフトウェア・コンポーネントが変更されています。後者では、コンポーネントは変更されていませんが、新しい SBOM 情報が利用可能です。最新の SBOM 情報を維持することは不可欠です。既存のコンポーネントを変更（パッチ適用または更新を含む）する場合、変更自体を既存の SBOM に追加された別個の新しいコンポーネントとして扱うか、理想的には新しいバージョン文字列を使用して、新しいコンポーネントを作成します。表 14 の例では、アップデート 37 の R 社ブラウザ v1.1 は、R 社ブラウザ v1.1.1 と同等です。 SBOM の記載者は、一貫して 1 つの方法を採用する必要があります。

表 14 パッチまたは更新のオプション

タイムライン	追加のコンポーネント	新しいバージョン文字列
変更前	R 社ブラウザ v1.1	R 社ブラウザ v1.1
変更後	R 社ブラウザ v1.1 R 社ブラウザ アップデート 37	R 社ブラウザ v1.1.1

SBOM の交換

SBOM 情報を交換する必要があります。一次交換は、サプライヤーから利用者に直接行われます。コンポーネントの提供の一環として、サプライヤーは SBOM、または URL やその他の参照などの、ユーザーが SBOM を簡単に取得できる手段も提供します。この直接配信は、サプライヤー、利用者、またはその他による、SBOM 情報のカタログ化を妨げるものではありません。ソフトウェアとデバイスのエコシステムはさまざまであるため、1 つの SBOM 交換メカニズムでは、十分であるとは考えられません。一部の既存の形式、つまり SWID と SPDX は、コンポーネントの配布または配信の一部として、追加ファイルとして提供されます。ストレージと電力に制約のあるデバイスの場合、オプションとして、一意の ID を持つ URL を提供して、サプライヤーの Web サイトで SBOM 情報を検索する方法をとることができます。 SBOM への動的アクセスは、そのようなデバイスにも適したオプションです。 ROLIE[13]、OpenChain[14]、ATOM[15]などのプロトコルを活用して、オンデマンドで、効率的な方法で大量の情報を収集することができます。これらの動的プロトコルの一部を使用した SBOM の可用性（ソフトウェア開発環境から資産管理システムなどの環境向け）は、SBOM を継続的に採用するための鍵となります。

サプライチェーン・ネットワーク

SBOM システムの参加者には、SBOM 情報を作成するサプライヤーと、それを受け取る利用者が存在します。多くの場合、ソフトウェアは、他の上流のソフトウェアで構成されているため、1 つの SBOM 情報が、SBOM 作成者と利用者、両方の機能を提供します。参加者は一連のネットワーク・ルールに従って、SBOM を利用可能であり、エコシステム内のすべての関係者にとって有用であることを確認します。 SBOM には、次のようなコンポーネントがリストされています。

---

[13] https://tools.ietf.org/html/rfc8322 (2021/3 月時点で確認済み)

[14] https://www.openchainproject.org/ (2021/3 月時点で確認済み)

[15] https://tools.ietf.org/html/rfc4287 (2021/3 月時点で確認済み)

1. ソフトウェアの信頼できるソースであるサプライヤーによって新たに作成されたもの

2. SBOM を提供する、上流のサプライヤーからのコンポーネントを統合したもの

3. SBOM を提供しない、上流のサプライヤーからのコンポーネントを統合したもの

サプライヤーは、サプライヤーが定義するコンポーネントの SBOM を作成します。コンポーネントの関係に関する前のセクションで説明したように、SBOM は、SBOM 自体をコンポーネントとして識別して、少なくとも 1 つのプライマリ・コンポーネントをリストする必要があります。

コンポーネントをユーザーに提供する一環として、サプライヤーは関連する SBOM も提供するか、利用者が SBOM を簡単に入手できるようにします。 SBOM には、サプライヤーが、自身で作成したコンポーネントと、サプライヤーが、他の上流のサプライヤーから取得したコンポーネントの両方が含まれます。

このような構造（図 8、図 9 および図 10）に示すように、最上流またはルート・サプライヤーは、自身のコンポーネントのみを作成し、他の上流サプライヤーからのコンポーネントは含みません（つまり、依存関係はありません)。図 9 では、S 社はルート・サプライヤーの例です。コンポーネントは、グラフ全体で、これらのルート・サプライヤーの下流に流れます。ツリーの右端では、リーフの運用者は、コンポーネントと SBOM のみを取得します。コンポーネントを生成したり、SBOM を作成したりすることはありません。ツリーの中央全体で、ほとんどの参加者は、サプライヤーと利用者の両方の役割を果たします。エンドユーザー組織でさえ、サプライヤーとして機能し、社内コンポーネントまたは Web サイト、モバイルアプリケーション、デバイスなどの外部コンポーネント用の SBOM を作成する場合があります。

サプライヤーは、作成するコンポーネントと含まれるコンポーネントに責任があります。サプライヤーは、収集したコンポーネントのセットを、下流の利用者に提供する責任もあります。マクロ経済の意味では、サプライヤーは、コンポーネントに関する高品質の信頼できる情報と、その情報を生成および共有するにあたり、コンポーネントを低コストに抑えるための取り組みを行っているため、コストを最小限に抑えることができます。このモデルは、ソフトウェアのサプライヤー市場全体に、SBOM 情報を生成するためのコストが分散されることを表しています。

このネットワークでは、サプライヤーがサードパーティ・コンポーネントの SBOM を作成するシナリオがいくつかあり、サプライヤーはコンポーネントの作成者ではなく SBOM の記載者として機能します。サプライヤーは、依存関係の有無にかかわらず、選択した数のサードパーティ SBOM を作成できます。サプライヤーが、そのような SBOM を作成する場合、サプライヤーは、それらが SBOM の記載者のみであり、コンポーネントのサプライヤーではないことを明確にすることが期待されます。「記載者名」と「サプライヤー名」が異なることによって、直接の信頼できる SBOM 情報の

欠如を利用者に知らせます。

SBOM 交換とネットワーク・ルールに関する概念は、ソフトウェアを選択して操作する人が、さまざまなサプライヤーやサプライチェーンで使用するコンポーネントの包括的なリストを取得できるように設計されています。図 10 は、図 9 の例を拡張して、2 つの異なるサプライチェーンからの 2 つのソフトウェア・コンポーネントを使用する運用者を表しています。

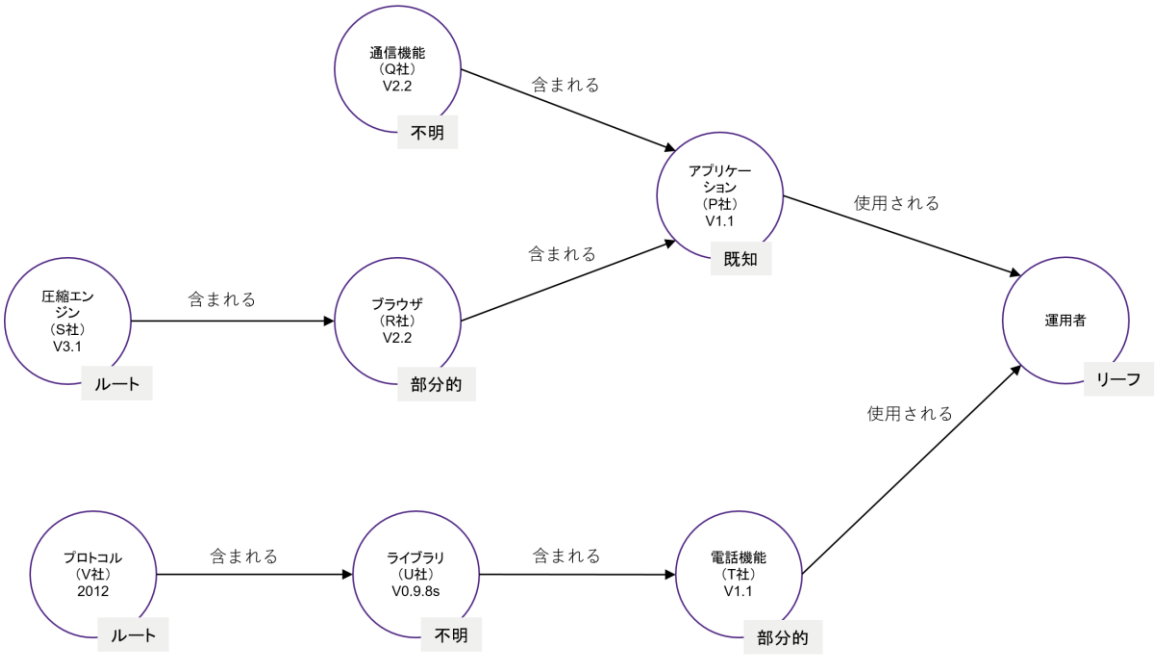

図 10　2 つのサプライチェーンを示す運用者の SBOM ツリー

SBOM を利用する役割

SBOM の利用にあたり、作成者、調達者および運用者の 3 つの役割を定義しています。表 15 に NTIA の SBOM の役割の定義を示します。

表 15　NTIA の SBOM の役割

役割	説明
作成者	ソフトウェアの作成者は、常にではありませんが、通常はサプライヤーです。この SBOM システムの目標は、すべての作成者がコンポーネントの SBOM を作成することです。SBOM を作成している 1 つのサプライヤーが、別のサプライヤーのコンポーネント用に SBOM を作成する必要がある場合があります。

	サプライヤーが自社製品に含まれる、上流のコンポーネントに関連付けられた SBOM を受け取ることで恩恵を受けます。サプライヤーが、サブコンポーネントに関する SBOM 情報を提供しない場合、この明確さの欠如により、下流のユーザーが、製品の未知の部分について最悪の事態を想定しなければならない可能性が高くなります。サプライヤーにとっての追加の利点は、上流コンポーネントの脆弱性の修正を取得するために連絡する組織を決定できることです。 SBOM の脆弱性管理ユースケースの一部には、上流コンポーネントの脆弱性が下流コンポーネントにどのように影響するかを伝える機能を含むことがあります。 SBOM が、上流コンポーネントの脆弱性を下流コンポーネントで悪用できないことを示している場合、下流コンポーネントのサプライヤーは、最終バージョンの修正が不要であることを認識します。これは、修正を作成する必要がないサプライヤーと、修正を適用する必要がない顧客の両方にとって大きなメリットとなります。
選択者	SBOM が関連付けられているコンポーネント、または製品の使用を検討している、将来の選択者が、SBOM を利用できます。これらのユーザーは、ベースライン・コンポーネントやライセンス情報など、製品に直接起因する情報に関心を持つ可能性があります。ライセンス、脆弱性、およびサポート・ライフサイクルに関する、SBOM 情報は、選択プロセスに影響を与える可能性があります。 ライセンス管理のユースケースでは、選択者は、製品自体に加えて、使用を検討している製品のすべての構成コンポーネントのライセンスを可視化できます。これにより、ユーザーは、製品を選択する際、ビジネスニーズやアプリケーションに適したライセンス契約を結ぶことができます。 脆弱性管理のユースケースでは、選択者はベースライン・コンポーネント情報を使用して、製品の公開された脆弱性の履歴と、これらの脆弱性に対するベンダーの対応の適時性を特定できます。これにより、選択者は製品のセキュリティ・ライフサイクルを考慮して、情報に基づいた決定を下すことができます。
オペレーター	どの業界でも、運用時に、サポートが期待される、コンポーネントまたは製品に関する完全な情報が不足しています。 SBOM は、ソフトウェアとそのコンポーネントの可視性を提供するために、この不足する情報に対して、非常に

	関連性の高いものになります。ライセンス情報などの一部の情報を除き、ソフトウェアの動的な性質により、SBOM 情報の一部が、製品の最初の配布後に変更または更新される可能性があります。 オペレーターが継続的に関心を持っている情報のほとんどは、SBOM の更新に含まれていると予想され、最新の SBOM 情報を使用して、サイトまたはビジネスで、本番環境に移行する前に、ソフトウェアの状態を確認することができます。

SBOM ユースケース

SBOM は、ベースライン情報に加えて、さまざまなユースケースをサポートするために追加の要素とコンポーネント属性を必要とします。 必要な情報はユースケースによって異なり、すべての追加情報が各ユースケースで必要になるわけではありません。
SBOM ユースケースの多くは、新しい属性や外部データ接続など、ベースライン SBOM で取得できる以外の追加属性を必要とします。追加情報は SBOM ユースケースごとに以下のように特定されます。

脆弱性管理：

脆弱性管理は、最も有名なユースケースの 1 つです。脆弱なサブコンポーネントが使用されているかどうか、および脆弱性が下流コンポーネントを、一時的に、脆弱または悪用可能にするかどうかを判断することは、多くの場合、費用と時間のかかる作業となります。 SBOM データは、サプライチェーン関係の背後に隠されている、最終バージョンの、脆弱なコンポーネントによってもたらされるリスクを、サプライヤー、ユーザー、およびその他の防御者がより迅速かつ正確に評価するのに役立ちます。

[必要な追加情報] CVE や NVD などの脆弱性情報のソース

ライセンス管理：

含まれているコンポーネントのソフトウェア・ライセンス（使用または再配布の制約を含む）の管理、および資格の追跡（コンポーネントのコピーまたは機能の使用許可）を行います。 コンポーネントの内容を決定するには、ソフトウェア構成分析ツールが役立ちます。

[必要な追加情報] コンポーネントへのさまざまなライセンスおよびライセンスのタイプの関連付け、および、さまざまなライセンスを持つコンポーネントの正味の効果を評価する方法。

高度な保証：

コンポーネントの出所と整合性の高い保証が必要な SBOM ユースケースは、 サプライヤー、コンポーネントの構築方法、コンポーネントがサプライチェーン内を移動する際の管理過程、および変更の方法に関する詳細情報が必要です。

[必要な追加情報] コンポーネントの製造方法など、コンポーネントの血統と出所に関する情報。

1.2.4.1.3 ソフトウェアの「作成者」の視点による SBOM 利用の価値

コードの再利用は、最新のソフトウェア開発の不可欠な要素です。ソフトウェアの作成者は、独自のコードを作成するだけでなく、サードパーティのコードとコンポーネントを、ソフトウェアに定期的に統合します。ソフトウェアを作成する組織は、コンポーネントを最初から作成するか、他の場所からコンポーネントをインポートするかを、常に検討しています。プロジェクトを高速で進行させ続けるために、この意思決定は、チームで行われたり、個々の開発者が行ったり、一貫していないことがあります。それでも、製品の成分を考慮することは、高品質の製品を製造するための重要な要素です。NTIA が特定した、ソフトウェアの作成者が、SBOM を使用した場合に受ける利点を表 16 に示します。

表 16　SBOM 利用の利点(作成者)

利点	説明
予定外の作業の削減	SBOM 利用で、コードベースの可視性を向上させることにより、予定外の作業を減らすことができます。これにより、コード更新の優先順位付けが向上し、配信が迅速化されます。 たとえば、SBOM なしで、新しい脆弱性が発生した場合、開発チームは、すべてのソフトウェアを確認して、問題があるかどうかを判断する必要があります。 SBOM を使用すると、その脆弱性を含む可能性のあるソフトウェアを簡単に特定できます。 組織は、必要なバグ修正の優先度を決定することができ、特定されたコンポーネントをさらに確認する必要がなくなり、ソフトウェアの残りの問題の確認に集中することで、時間を節約できます。
コードの膨張の抑制	コンポーネントを追跡すると、コードの膨張を、より簡単に減らすことができます。 特に OSS コンポーネントは、同じ機能を実行する、わずかに異なる数十のバージョンで利用されることが多く、バージョンごとに異なる固有の欠陥が存在する可能性があります。 SBOM を使用すると、組織は共通のコンポーネント・セットを簡単に特定できるため、脆弱性は 1 つのコンポーネントに対する修正のみで済みます。
広範で複雑なプロジェクトにおける適切な依存関係の把握	開発者が、より広範で、複雑なプロジェクト内の依存関係を適切に理解しやすくすることで、より多くの責任と、より良い品質管理を促進できます。 コードの再利用に対する、より体系的なアプローチにより、プロセス全体が改善され、その結果、製品に対する信頼を高めることができます。特定のチームまたは製品に必要な経験/専門知識を、より適切に追跡し、潜在的な将来のメンテナンスが、サポート可能であることを確認し、下流工程の顧客がソフトウェアを評価するときの「驚き」を回避することができます。
ライセンス義務の認識と遵守	SBOM の使用により、使用されているコンポーネントのライセンス義務を認識し、遵守することができます。 ライセンス・ポリシーを使いやすくするシステムは、ライセンス・コンプライアンスの自動化に役立ちます。
コンポーネントの脆弱性の監視	コンポーネントの脆弱性を、より簡単に監視できるため、チームはリスクをより積極的に評価して修正できます。 セキュリティ研究者が新しいセキュリティ・リスクを発見した場合、特定の製品が潜在的に脆弱であるかどうかを特定する作業は、長期にわたる可能性があります。 簡単にアクセスできるコンポーネントのリストにより、この作業をはるかに効率的にすることができます。 コンポーネントの認識を高めることで、顧客を安心させるまでの期間を短縮し、顧客の信頼を向上させることもできます。
保守終了に対する対応	ソフトウェア・コンポーネントが保守終了に達し、その上流サプライヤーによってサポートされなくなったり、サプライヤーが完全に消滅したりす

	る場合があります。 ソフトウェア作成者はこれを積極的に監視し、不測の事態が発生する前に対応を計画する必要があります。 SBOM を使用すると、代替ソリューションを特定して実装するなど、サプライチェーンに積極的に取り組むことができます。
禁止されているコンポーネントのブラックリスト化	コンポーネントの使用状況を追跡することで、禁止されているコンポーネントのブラックリスト化や、優先コンポーネントのホワイトリスト化、あるいはその両方などの戦略を支援することができます。 ブラックリストを使用すると、既知の問題、サポートされなくなったプロジェクト、またはセキュリティ、パフォーマンス、信頼性の問題など、多くの問題を抱えてきたコンポーネントを回避することができます。 ホワイトリストは、それほど一般的ではありませんが、企業が信頼できるサードパーティ・コンポーネントを推奨したり、優先プロバイダーのリストを作成したりすることができるようにします。
SBOM を顧客に提供する	SBOM を顧客または下流工程のパートナーに提供して、企業が顧客の法的およびセキュリティのニーズを満たす、高品質の製品を提供していることを保証できます。SBOM の採用が増えるにつれて、競争上の優位性を提供できるようになり、最終的には、SBOM の提供が、一般的な市場の期待または要件になる可能性があります。最新の SBOM は、所有している製品の、現在のセキュリティの状態について、下流工程のソフトウェアの利用者を安心させることもできます。

1.2.4.1.4 ソフトウェアの「選択者」の視点による SBOM 利用の価値

ソフトウェアのほとんどすべての選択は、長期にわたる取り組みであるため、あるソフトウェア製品またはコンポーネントを購入するか、別のソフトウェア製品またはコンポーネントを購入するかの決定は、事前の検討と計画によって行われることが非常に重要です。この取得プロセスは、公式または非公式の場合があり、要件の確認、市場調査、サプライヤーと製品の評価、ソフトウェアの購入と実際のソフトウェアの受け取りなどの手順が含まれます。

SBOM のないソフトウェアの利用者は、ソフトウェア・サプライヤーによって公開されていないコード内におそらく OSS コンポーネントがあることを知っています。これらの中には、サポートされていない（「孤立した」）ライブラリまたは既知の脆弱性を持つコンポーネントが含まれる可能性があります。悪意のあるサプライヤーは、有用な機能を実行するコンポーネント内にマルウェアを隠す可能性があります。

表 17 に、ソフトウェアを選択するときにもたらされる SBOM の利点を示します。

表 17　SBOM 利用の利点(選択者)

利点	説明
潜在的に脆弱なコンポーネントの特定	基盤となるコンポーネントの可視性は、潜在的に脆弱なコンポーネントを特定するのに役立ちます。　SBOM により、購入する前に、基本的なリスク分析を実施して、システムに、何をインストールしようとしているのかを理解することができます。
より的を絞ったセキュリティ分析	より成熟したリスクプロセスを持つ組織は、どのコード・コンポーネントが危険信号を発する可能性があるか（たとえば、標準以下の保護を提供する暗号化ライブラリ）、どのコンポーネントが、信頼できるソースによってすでに精査されているかを決定することにより、より的を絞ったセキュリティ分析を行います。
出所の確認	SBOM にコンポーネントの署名ハッシュが含まれている場合、組織はサードパーティ・コンポーネントの調達を確認して、偽造またはバックドアされたコンポーネントが、サプライヤーのサプライチェーンに滑り込むリスクを制限できます。　(SBOM は、攻撃者が正当な出所に干渉するのを直接防ぐことはできませんが、攻撃が検出された場合、修復作業を大幅に簡素化できます。)
ポリシーへの準拠	組織は、サプライチェーンの出所に関する規制や、その他の規則に直面する可能性があり、SBOM は、組織で使用する必要があるものと、使用してはならないものに関するポリシーへの準拠を可能にします。
サポート終了済みコンポーネントの認識	将来のサポートが利用できなくなるコンポーネントを認識することができます。　これらのコンポーネントは、ソフトウェアを最初に取得した段階では、リスクがない可能性がありますが、あとで見つかった問題は修正されない可能性があります。
主張を確認する	コードベースとその品質に関する、サプライヤーの主張を、よりよく検証できるようになります。　どのコンポーネントのどのバージョンかを知ることが、ソフトウェアの品質とセキュリティに関する、すべての質問に答えるわけではありませんが、サプライヤーの注意深さについての意識を、評価することにつながります。
ソフトウェアの統合を理解する	ソフトウェアの既存の資産および脆弱性管理システムへの統合を、よりよく理解できるため、総所有コストを削減し、不十分な統合から生じるリスクの可能性を最小限に抑えることができます。
購入前およびインストール	脆弱である可能性のあるソフトウェアや、継続して購入する予定があるソフトウェア、あるいは古いソフトウェアに対して、購入前およびインストール前の計画を立てることができます。　購入の決定は多くの理由で行われ、購

前の計画	入と使用のメリットがセキュリティ・リスクを上回る場合があります。 この場合、セキュリティ・チームは、セグメント化されたネットワーク、またはホワイトリストに登録されたアクセス・システムの設計や、システムのインストールと保守を行う運用チームのチェックリストの準備など、よりリスクの高いシステムを通常と異なる方法で対処する決定を下すことができます。
市場シグナル	SBOM は、サプライヤーがコンポーネントから発生するリスクについて考えているという、市場シグナルを提供します。これは、サプライヤーが優れたソフトウェア開発を実践しており、いくつかのベストプラクティスを遵守していることを示します。 セキュリティと品質のプロセスに投資する人々に報酬を与えることにより、サプライヤーにも顕著な影響を与える可能性があります。

1.2.4.1.5 ソフトウェアの「運用者」の視点による SBOM 利用の価値

ソフトウェア・パッケージまたはコンポーネントを選択して調達した後、インストール、構成、保守、および管理する必要があります。これらの責任は「業務」のカテゴリーに分類されます。それらは組織によって異なり、管理者からネットワーク・オペレーションセンター（NOC）またはセキュリティ・オペレーションセンター（SOC）、最高情報セキュリティ責任者（CISO）などのリスクまたはコンプライアンスを担当するエグゼクティブに至るまで、さまざまな潜在的な役割が考えられます。これらの役割は、産業用またはオペレーショナル・テクノロジー（OT）設定の組み込みソフトウェアなどの非 IT パッケージにも適用される場合があります。
表 18 に、ソフトウェアを運用するときにもたらされる SBOM の利点を示します。

表 18 SBOM 利用の利点（運用者）

利点	説明
コンポーネント使用状況の迅速な評価	コンポーネントのリストにより、現在の環境のソフトウェアに適用される新しい脆弱性の発見と、関連付けが可能になります。特定のコンポーネントに新しい欠陥が発見された場合、そのコンポーネントを使用しているかどうか、つまり、そのコンポーネントがリスクにさらされているかどうかを、すばやく評価できます。
独立した緩和策の推進	潜在的にリスクのあるコンポーネントを認識することで、サプライヤーが実際のリスクを評価し、必要に応じてソフトウェアの更新を提供するのを待つ間、独立した緩和策を推進できます。 一部の組織は、既知の脆弱なソフトウェアによるリスクを最小限に抑えるために、独自に防御措置を講じることを決定することができます。 考えられる措置の例として、手続き型制御に

	よる対策、影響を受けるシステムの技術的分離、またはシステム・アクティビティの監視の強化が挙げられます。 欠陥のあるソフトウェア・コンポーネントがサプライヤーによって、積極的にサポートされていない場合、またはサプライヤーが存在しない場合は、これらの対策が、唯一可能な緩和策である可能性があります。
より多くの情報に基づいたリスクベースの意思決定を行う	運用者は、セキュリティとリスクに対する独自のアプローチに基づいて、ネットワーク上にある資産、および対応に優先順位を付ける方法について、より多くの情報に基づいた、リスクベースの決定を行うことができます。
潜在的な寿命に関するアラート	サードパーティのコンポーネントを注意深く理解することで、潜在的な保守終了状況に関するアラートを有効にすることができます。 SBOM のデータを他のデータ・ソースと組み合わせることにより、コンポーネントがサプライヤーによってサポートされなくなる時期を把握することができます。 これにより、その組織は、これらのコンポーネントを使用するソフトウェアの潜在的な波及効果を理解し、サプライヤーと協力するか、代替案を探すための積極的な決定を下すことができます。
より良いサポート・コンプライアンスとレポート要件	コンポーネントに関する詳細情報は、コンプライアンスとレポートの要件をより適切に支援できます。 SBOM は、より詳細な資産インベントリであることに加えて、展開されたシステムのセキュリティ・リスクを監視する要件を支援します。
より合理化された効率的な管理を通じてのコスト削減	文書化されたソフトウェア・コンポーネントは、より合理化された効率的な管理を通じてコストを削減できます。責任者は懸念事項をすばやく特定でき、ソフトウェアに欠陥のあるコンポーネントが含まれていないことを、SBOM から判断できる場合は、サプライヤーへの連絡に時間を費やす必要はありません。

1.2.4.1.6 SBOM フォーマット

二つの主要フォーマット

標準とフォーマット・ワーキンググループは、広く使用されている 2 つの形式を特定しました。LinuxFoundation によって事実上の業界標準として管理されている OSS の機械可読形式である Software Package Data eXchange (SPDX) と、正式な業界標準である Software Identification (SWID) です。

これらの 2 つの形式には重複する情報が含まれており、ソフトウェア・ライフサイクルのさまざまな時点で使用され、さまざまなタイプのユーザーによって使用さます。OSS ソフトウェア開発コミュニティの製品である SPDX は、開発者のワークフロー内での取り込みを容易にすることを目的としています。

SWID タグは、ソフトウェアの資産管理と資格管理を念頭に置いて設計されました。SWID タグは、ソフトウェアに関連付けられた SWID タグを見つけることにより、デバイスにインストールされている商用および OSS ソフトウェアの資産管理を支援します。

ワーキング・グループは、両方の形式を使用して SBOM データを生成、交換、および使用できることを確認しています。特定のユースケースは特定の形式に適している場合がありますが、このワーキング・グループは、どちらも具体的に推奨しておらず、各ユーザーはニーズに合ったものを選択する必要があると考えています。

SBOM のライフサイクル

表 19 に SBOM のライフサイクルを示します。

表 19　SBOM のライフサイクル

SBOM のライフサイクル	説明
作成	SBOM に入力される情報は、ソフトウェア・ライフサイクルの各段階で使用されるツールとプロセスから最もよく取得できます。 既存のツールとプロセスを活用して、SBOM を生成することができます。 このようなツールとプロセスには、知的財産のレビュー、調達のレビューとライセンス管理のワークフロー・ツール、コード・スキャナー、プリプロセッサー、コード・ジェネレーター、ソースコード管理システム、バージョン管理システム、コンパイラー、ビルドツール、継続的インテグレーション・システム、パッケージャー、コンプライアンス・テスト・スイート、パッケージ配布リポジトリとアプリ・ストアが含まれます。 現在、すべての既製または OSS のソフトウェア・ライフサイクル・ツールが SBOM を生成する機能を備えているわけではありません。 ソフトウェアの分析は、最初の生成後に行われる場合があります。 サプライヤーは、SBOM を生成および維持するために、既存のツールおよびプロセスを強化、または改造することを検討する必要があります。

	ソフトウェア・ライフサイクルの段階で追加または削除された資料に関する情報が欠落しているか、記録されていない場合、SBOM は不完全であると見なされる可能性があります。SBOM が不完全な場合、サプライヤーはそれを明確にして、利用者が利用可能なデータに基づいて、SBOM を使用できるようにする必要があります。
配布	現時点では、SBOM データを下流工程の次のユーザーに送信するための単一の方法は定義されていません。 OSS 製品では、SBOM データは、コンポーネントへのポインターとともにメタデータとして保存できます。 コンパイルされたソフトウェアの場合、SBOM はソフトウェア製品自体と一緒にバンドルされ、インストールされたソフトウェアとともに保存されます。データは、サプライヤーまたはその他のサードパーティが管理するポータルで利用できるようにすることもできます。
更新	SBOM は、ソフトウェアの現在の状態を反映する必要があります。 ソフトウェアまたはソフトウェアの基盤となるコンポーネントが更新された場合は、それに応じて基盤となるコンポーネントのリストも更新して、SBOM データ自体が最新であることを確認する必要があります。 ソフトウェア成果物自体から派生した情報を除いて、SBOM 内のその他の情報は、宣言的であるか、SBOM データの記載者によって表明されます。 たとえば、コンポーネント名のダウンロード場所を SBOM の一部にすることができます。 同様に、ソフトウェアに関する既知の情報が変更された場合、または元の SBOM でエラーが発生した場合、サプライヤーは基礎となるコードを更新せずに SBOM を更新できます。宣言された情報は、時間の経過とともに修正、変更、または追加する必要が出てくる場合があります。このような変更は、元帳ベースの SBOM に追加できます。 エラッタは、特定の SBOM で供給および繰り越す必要がある場合があります。
利用	SBOM 情報を最も効果的に利用するには、データが機械可読である必要があります。その利用には、機械間の自動化プロセスを組み込む必要があります。各ユースケースは、自動化されたプロセスに統合することによってのみ最大の効果を達成できます。 また、フォーマットを人間が読める形式に変換できることも重要です。 利用者は、以下をサポートするツールへの入力として SBOM を使用できます。 • 資産管理 • ライセンスと資格の管理

	• 知的財産管理 • 規制およびコンプライアンス管理 • プロビジョニング • 構成管理 • 脆弱性管理 • インシデント対応 リスク管理に SBOM を使用するには、SBOM に含まれていない可能性のある、追加のリスクデータが必要になる場合があります。

1.2.4.1.7 SPDX

Software Package Data Exchange（SPDX）仕様は、ソフトウェア・コンポーネントに関連するコンポーネント、ライセンス、著作権、およびセキュリティ情報を複数のファイル形式で通信するための標準言語を提供します。

世界中のソフトウェア開発チームが同じ OSS コンポーネントを使用していますが、2010 年の時点では、コラボレーションや分析を容易にしたり、分析活動の結果を共有したりするために利用できるインフラストラクチャがほとんどありませんでした。その結果、多くのグループが同じ作業を行っていたため、作業が重複し、情報が冗長になりました。時間を節約し、データの精度を向上させるために、SPDX プロジェクトは、ソフトウェア・パッケージおよび関連コンテンツに関する情報を収集および共有できるように、共通のデータ交換形式を作成するために結成されました。

SPDX ドキュメントは、特定のソフトウェア・コンポーネントまたはコンポーネントのセット、個々のファイル、またはコードのスニペットに関連付けることができます。 SPDX プロジェクトは、SBOM の一部として交換できるデータを記述するための「言語」の作成と拡張に重点を置いており、その言語を複数のファイル形式（RDFa、.xlsx、.spdx など）で表現できます。これにより、ソフトウェア・パッケージおよび関連コンテンツに関する情報を簡単に収集および共有して、時間を節約し、精度を向上させることができます。

SPDX 仕様では、有効な SPDX ドキュメントを作成するために必要なセクションとフィールドについて説明しています。 これらのセクションのすべてが、すべてのドキュメントで必要なわけではありません。ドキュメントごとに「ドキュメント作成情報」セクションを用意することは必須です。共有する予定のソフトウェアとメタデータ情報を説明するセクションを使用する必要があります。

SPDX のセクションの構成を表 20 に示します。

表 20　SPDX の構成

セクション	英語名	説明
ドキュメント作成情報	Document Creation Information	作成される SPDX ファイルごとに、1 つのインスタンスが必要です。処理ツールの上位互換性と下位互換性に必要な情報（バージョン番号、データのライセンス、作成者など）を提供します。
パッケージ情報	Package Information	SPDX ドキュメントのパッケージを使用して、製品、コンテナ、コンポーネント、パッケージ化された上流プロジェクト・ソース、tarball のコンテンツなどを記述できます。これは、いくつかの共通のコンテキストを共有するアイテムをグループ化する方法です。
ファイル情報	File Information	ファイルの名前、チェックサム・ライセンス、著作権など、ファイルの重要なメタデータがここに要約されています。
スニペット情報	Snippet Information	スニペットは、ファイルに、別のソースから含まれているコンテンツが、含まれていることがわかっている場合に、オプションで使用できます。これらは、ファイルの一部が、元々別のライセンスで作成された可能性があることを示すのに役立ちます。
その他のライセンス情報	Other Licensing Information	SPDX ライセンスリストは、ファイルに含まれるすべてのライセンスを表すわけではないため、このセクションでは、説明されているソフトウェアに存在する可能性のある、その他のライセンス情報を要約する方法を提供します。
関係	Relationships	SPDX ドキュメント、パッケージ、ファイルを相互に関連付けることができる、さまざまな方法のほとんどは、これらの関係で説明できます。
注釈	Annotation	注釈は通常、誰かが SPDX ドキュメントをレビューし、レビューからの情報を伝えたいときに作成されます。SPDX ドキュメントの作成者が、他のカテゴリーに当てはまらない追加情報を保存したい場合は、このメカニズムを使用できます。

SPDX のユースケース

- ソフトウェア・コンポーネントの SBOM
- ソフトウェア・コンポーネントの知的財産（ライセンス、著作権）の追跡
- ソフトウェア配布の内容の一覧表示
- コンテナ内容物の在庫
- CPE を特定のパッケージに関連付ける
- ファイルに埋め込まれたコード行の出所の特定

SPDX の主要な機能

- 文書化されたアーティファクトは、提供されたハッシュ値を使用して確認できます
- 知的財産およびライセンス情報のための豊富な仕様
- スニペットやファイルからパッケージ、コンテナ、さらにはオペレーティング・システムのディストリビューションまで拡張できる柔軟なモデル
- 他のパッケージ参照システムにマッピングを追加する機能。

SPDX と SBOM

SPDX ドキュメントは、従来のソフトウェア開発で見られるすべてのコンポーネントを表すことができるため、SBOM データを取り扱うことができます。 SPDX ドキュメントは、ディストリビューション.iso イメージ、コンテナ、ソフトウェア・パッケージ、バイナリファイル、ソースファイル、パッチ、さらには他のファイルに埋め込まれたコードのスニペットを表すために使用されています。 ドキュメント内およびドキュメント間でソフトウェア要素をリンクするために、豊富な関係のセットを利用できます。 SPDX ドキュメントは、NVD およびその他のパッケージング・システム・メタデータへの外部参照を介してリンクできます。

1.2.4.1.8 SWID

ソフトウェア識別（SWID）タグは、組織が管理対象デバイスにインストールされている、ソフトウェアを追跡するための透過的な方法を提供するように設計されています。これは、2012 年に ISO

によって定義され、2015 年に ISO / IEC 19770-2：2015 として登録されました。 SWID タグファイルには、ソフトウェア製品の特定のリリースに関する説明情報が含まれています。

SWID 標準は、ライフサイクルを定義します。SWID タグは、ソフトウェア製品のインストールプロセスの一部としてエンド・ポイントに追加され、製品のアンインストール・プロセスによって削除されます。このライフサイクルでは、特定の SWID タグが存在するかどうかで、ソフトウェア製品に SWID タグのソフトウェア・コンポーネントが含まれることを表現します。表 21 に SWID のタグを示します。

表 21 SWID のタグ

タグ名	説明
プライマリ・タグ	ソフトウェア製品を識別および説明する SWID タグがコンピューティング・デバイスにインストールされます。
パッチ・タグ	コンピューティング・デバイスにインストールされているソフトウェア製品に、段階的な変更を加えた、パッチを識別して説明する SWID タグです。
コーパス・タグ	インストール前の状態の、インストール可能なソフトウェア製品を、識別および説明する SWID タグです。コーパス・タグを使用して、ソフトウェア製品、ソフトウェア・アップデート、またはパッチのインストール・パッケージまたはインストーラーに関するメタデータを表すことができます。
補足タグ	参照される SWID タグに、追加情報を関連付けることができる SWID タグです。これにより、ソフトウェア・プロバイダーが提供する SWID プライマリ・タグとパッチ・タグがソフトウェア管理ツールによって変更されないようにすると同時に、これらのツールが独自のソフトウェアメタデータを提供できるようになります。

SWID のユースケース

- ソフトウェア・コンポーネントの SBOM
- インストールされているソフトウェア・インベントリーの継続的な監視を行います。

- エンド・ポイント上の脆弱なソフトウェアを特定します。
- インストールされているソフトウェアに適切なパッチが適用されていることを確認します。
- 許可されていない、または破損したソフトウェアのインストールを防止します。
- 破損したソフトウェアの実行を防止します。
- ソフトウェア資格の管理

SWID の主要な機能

- ビルド時に作成された、安定したソフトウェア識別子を提供します。
- ソフトウェア・インストール・プロセスの一環として、ソフトウェア提供者と利用者の間で交換できるソフトウェア情報を標準化します。
- 関連するパッチまたはアップデート、構成設定、セキュリティ・ポリシー、脆弱性と脅威に関する助言など、ソフトウェアに関連する情報の関連を表現します。

SWID タグと SBOM

SWID タグは、ソフトウェア・コンポーネントの識別情報、ソフトウェア・コンポーネントを構成する、構成アーティファクトのファイルと暗号化ハッシュのリスト、および SBOM（タグ）作成者とソフトウェア・コンポーネントに関する来歴情報を提供するため、SBOM として使用できます。タグは他のタグに明示的にリンクでき、依存関係ツリーの表現を可能にします。

1.2.4.1.9 SBOM フォーマットの課題

フレーミング WG によって定義された、1 つのユースケースは、SBOM で既知および未知のものについて明示することです。 つまり、SBOM の利用者は、コンポーネントにサブコンポーネントがある場合と、コンポーネントにサブコンポーネントがない場合について、見分けることができる必要がありますが、現在まで、SWID も SPDX も、この「既知と未知」のユースケースを明示的に取得して伝達することはできません。 両方のサポートコミュニティのメンバーは、この情報を伝えるために、どのようにフォーマットを変更するのか検討しています。
より広義には、サードパーティの依存関係の追跡は、ソフトウェア・エンジニアリングとコンピューター・サイエンスにおける他の多くの重要な課題に関連しています。 これらの課題を表 22

に示します。

表 22　SBOM フォーマットの課題

課題	説明
ソフトウェア ID	複数のツール、システム、またはデータベース間で、単一のコンポーネントに関する情報を、自動的かつ正確に関連付けるには、ソフトウェア・コンポーネントを明確かつ一意に識別する「主キー」が必要です。このような ID キーは、時間の経過とともに変更されるべきではなく、中央の発行機関を必要とすべきではありません。他の情報が利用できない場合は、ソフトウェア・コンポーネント自体に基づいて、この識別キーを決定する必要があります。 広く使用されているアプローチ（CPE など）が、いくつかありますが、これらは普遍的ではなく、上記の完全なニーズを満たしていません。より完全な識別子（パッケージ URL やソフトウェア・ヘリテージ ID など）を開発するための研究が行われていますが、現在は広く使用されていません。これらのフォーマットを成熟させ、エコシステム全体に関連させるには、さらに多くの努力が必要です。中期的なソリューションは、さまざまなコミュニティが独自のルールを定義し、特定の用途に合わせて調和する、いくつかのエイリアス・データベースを備えたフェデレーション・モデルのようになります。
ツール	SBOM プラクティスを広く採用するには、自動化が必要であり、それにはツールが必要です。 SBOM データの作成、配布、および使用を実証および促進するには、既存のツールと、その機能の広範な調査が不可欠です。 これには、そのような SBOM ツールのカタログを維持するための、継続的なコミュニティの取り組みが必要になります。
配布	より良いサプライヤーの選択を可能にするために、利用者が製品を購入する前に SBOM を比較できるよう、無料でオープンな SBOM データが不可欠です。 利用者が sbom-request@example.com や http://example.org/sbom などの標準の連絡先を介してサプライヤーから SBOM を取得するための一連の方法を標準化することには利点があります。 既存の標準では、これらの標準化された方法がありません。

1.2.4.1.10 SBOM の高度な保証のユースケース

一部のユースケースでは、ソフトウェアまたはSBOM自体に関する詳細情報が必要になる場合があります。 コンポーネントのIDだけでなく、サプライチェーンの利害関係者は、コンポーネントの整合性、作成者の血統、コンポーネントの組み立て方法、SBOM自体のコンパイル方法などの詳細情報を知りたい場合があります。 より高い保証を必要とする組織は、悪意を持って変更または汚染されたソフトウェアを受け入れることによって悲惨な結果を被る可能性を排除するため、SBOMのさらなる要素を必要とする場合があります。表 23に示す３つの機能の詳細は今後のNTIAのワーキング・グループで議論される予定です。

表 23　高度な保証ユースケースの要素

要素	説明
来歴	SBOM の来歴は、ソフトウェアとそのソフトウェアを構成するすべての構成コンポーネントの管理過程に関する情報を持ち、コンポーネントが取得された作成者と場所に関する情報を取得するための用語です。 コンポーネントがサプライヤーの配布サイトから直接提供されているのか、それとも他の場所から提供されているのかは、組織によっては懸念される場合があります。 同様に、サプライヤーの正確なIDを理解することは、組織が更新の入手先を確立したり、バグや拡張機能について連絡したりするのに役立ちます。 作成者を判別することにより、組織はコンポーネントに関する経験を作成者に関連付け、ソフトウェア・プロバイダーの評判のようなスコアリングを通じて選択のための優先順位をランク付けできます。
血統	SBOM の血統は、ソフトウェアの一部の作成に由来するすべてのコンポーネントと、それらをまとめるプロセスに関する情報を持つことを表す用語です。 これには、コンパイラオプションなど、コンポーネント以外の詳細を含めることができます。 たとえば、ASLR(アドレス空間のランダム化) を呼び出すコンパイルオプションが使用されたかどうかを理解することは、結果として得られる展開可能なコードの一部が特定の種類の攻撃に対して強化されていることを示します。 実行可能ファイルを作成するためにソースコードと組み込まれたコンポーネントおよびライブラリを取得する際に使用されるプロセスを理解することは、実行可能ソフトウェアの作成に使用されたオプションの選択を知る必要がある人にとって重要な情報源です。

整合性	SBOM の整合性とは、暗号化技術を使用して、SBOM が作成者によって作成されてから変更されていないことを示すか、変更があった場合は、後続の SBOM 編集者による変更を示すことです。 SBOM の整合性を判断できることは、攻撃者が SBOM を意図的に変更して、脆弱性の分析に SBOM を使用している人を欺く可能性があるかどうかが懸念される状況で役立ちます。脆弱性のあるバージョンのコンポーネントを使用している場合、誰かが SBOM を編集して、脆弱性のないバージョンを使用していることを示すように変更すると、組織はその脆弱性に対する攻撃を受けやすくなります。同様に、SBOM の編集者または情報源の情報を変更すると SBOM の来歴が損なわれ、ソフトウェア作成方法の詳細を変更すると SBOM の血統が損なわれます。暗号化技術を使用して、SBOM が作成者によって、作成されてから変更されていないことを示すか、変更があった場合は、後続の SBOM 作成者による変更を示します。 SBOM の整合性を判断できることは、たとえば、攻撃者が SBOM を意図的に変更して、脆弱性の分析に SBOM を使用している人を欺く可能性があるかどうかが懸念される状況で役立ちます。誰かが SBOM を編集して、コンポーネントの新しい、脆弱性のないバージョンがあることを示した場合、変更された SBOM が脆弱性のないバージョンを使用していることを示していても、組織はその脆弱性に対する攻撃を受けやすくなります。同様に、SBOM の編集者または情報源の情報を変更すると、SBOM の来歴が損なわれ、ソフトウェア作成方法の詳細を変更すると、SBOM の血統が損なわれます。

1.2.4.1.11 ヘルスケアの概念実証

ここでは、、NTIA で行われたヘルスケアの概念実証の取り組みをまとめて報告します。

すべての業界にとって、重要な課題は、複雑なサプライチェーンのソフトウェア・コンポーネントを組み込んだデバイスとシステムを保護することです。特に、ソフトウェアの購入者とユーザーは、通常、ソフトウェアのコンポーネントの出所を確認できないため、ソフトウェアの運用上のリスクとサイバーリスクを十分に把握することができません。
医療機器メーカー（MDM: medical device manufacturers：このセクションでは「機器メーカー」という）と医療提供組織（HDO: healthcare delivery organizations：このセクションでは「医療提供組織」という）が主導するソフトウェア部品表（SBOM）の概念実証（PoC）について記載し

ます。

概念実証は、医療提供組織が医療機器に関連する、運用リスクとサイバーリスクを管理する方法において、SBOM が重要な役割を果たすことができることを実証しました。第一に、機器メーカーは、標準化された業界にとらわれない形式を利用して、医療機器用の SBOM を正常に作成し、その SBOM は、医療提供組織によって正常に取り込まれました。第二に、参加者の医療提供組織は、機器メーカーから提供された SBOM を利用して、セキュリティ対策が必要な、サポート終了コンポーネントを含む、ソフトウェアの脆弱性を特定し、リスク・スコアなどの外部の脆弱性評価と組み合わせて、SBOM 情報を利用することができました。以前は不可能だった方法で、リスクを特定するための医療機器セキュリティに関する、製造業者の開示声明を行うことができました。 概念実証は、SBOM 形式を強化する機会、および SBOM を生成する際の機器メーカーの利点と課題を特定しました。

SBOM 概念実証の参加者は、SBOM の作成とその利用が、医療提供組織によって展開される医療機器を保護する上で、その役割を果たすことができると考えています。 この概念実証は、将来、実施される、ヘルスケア業界以外での概念実証において、SBOM の実用化に関する研究の基盤を提供します。概念実証の結論と教訓は、NTIA が主導するソフトウェアの透明性の取り組みに参加している複数の業界にとって価値があることが証明されると推測されます。さらに、ヘルスケア概念実証は、医療機器のエコシステムを保護する上で、SBOM が果たすことができる役割について、食品医薬品局（FDA）に、検討事項を通知します。

1.2.4.1.11.1 概念実証の背景

NTIA は、2018 年 6 月に、さまざまな業界の利害関係者と協力して、ソフトウェアの透明性について話し合いました。そこで明らかになった、ソフトウェア・コンポーネントの透明性に関する NTIA の複数の利害関係者プロセスの使命は、次のように説明できます。

「メーカーとベンダーが、最新のソフトウェアと IoT デバイスを構成する、サードパーティおよび組み込みソフトウェア・コンポーネントに関する、有用で実用的な情報を伝達する方法と、企業がこのデータを使用して、セキュリティの決定と実践を促進する方法を探ります。目標は、組織に、より高い透明性を提供する市場を育成することです。組織は、このデータをリスク管理に利用することができます。」

この取り組みの基本は、ソフトウェア・サプライチェーンの複雑さが、情報システムとデバイスの調達とサポートのコストだけでなく、サイバーセキュリティ・リスクにも大きく影響することを確認することです。したがって、サプライチェーンの透明性は、次の方法でサイバーセキュリティのリスクと全体的なコストを削減できます。

- サイバーセキュリティのリスクを軽減するために、脆弱なソフトウェアの特定を容易にします。

- ソフトウェアの脆弱性と欠陥を特定することにより、計画外のダウンタイムを削減します。

- 強力なソフトウェア開発プログラムにより、システムおよびデバイス・メーカーのより多くの情報に基づいた購入決定と市場の差別化を支援します。

- 疑わしい、または偽造されたソフトウェア・コンポーネントを特定します。

1.2.4.1.11.2 概念実証の目的

2018 年 6 月の NTIA 対面ワーキングセッションから、ソフトウェアの透明性のさまざまな側面を検討するために、さまざまなワーキング・グループが召集されました。SBOM 概念実証を主導するワークグループは、機器メーカーと医療提供組織が、いくつかのユースケースで SBOM をうまく活用できることを実証しようとしました。SBOM が医療機器に関連するリスクを軽減するために、提供する価値を実証することを目的としています。FDA が明確に述べているように、医療機器が、サイバー侵入から保護されることを保証することは、医療機器エコシステム全体で共有される責任となっています。

概念実証参加者は、概念実証が SBOM 生成に使用される既存の標準と整合する必要性を認識し、評価のユースケースについては、他の業界で見られるユースケースと一致します。概念実証の高レベルの目標は次のユースケースが含まれます。

- 参加者の医療提供組織で使用されている実際の医療機器の SBOM を生成し、その SBOM を医療提供組織に提供します。

- 医療提供組織で、実際に使用されている医療機器の SBOM を取得し、それを利用します。

- SPDX および SWID を SBOM 形式として評価し、これらの標準の実際の利用に対する拡張の機会と潜在的な障害を特定します。

1.2.4.1.11.3 概念実証の範囲

概念実証の詳細な計画を開始する前に、参加者は、概念実証の範囲内にあるものと範囲外にあるものを定義しました。 これにより、参加者は、概念実証を実証するために重要な側面、および将来の作業によって解決される可能性があるその他の側面を特定することができました。 2 つのケースでは、元々スコープ内にあった項目がスコープ外に変更されました。これは、合理的な期間で簡単に対処できない問題を解決することを意味するか、概念実証を完了するために不要であると後で識別されたためです。

概念実証の範囲内の項目

概念実証の範囲を表 24 に示します。

表 24　ヘルスケア概念実証のスコープ内の項目

項目	説明
標準フォーマットへの準拠	参加者が使用する新しいフォーマットを作成するのではなく、既存のフォーマットを使用するために、必要な作業が少なくて済み、既存のツールとの互換性が高くなることが期待されていました。　SWID と SPDX の両方が使用されましたが、どちらの場合も、これらのフォーマット間での SBOM の情報伝達を意図するように行うことができることを確認する必要がありました。
コンポーネントの依存関係	特にネストされた SBOM の最初のホップを超えて、依存関係情報を提供することは、機器メーカーにとって、解決するのが難しい問題と見なされていました。この概念実証では、ネストされた依存関係は、機器メーカーによって、極力現実の世界に近づけるよう「ベストエフォート」ベースで提供されます。
コンポーネントのサプライヤー名	これは SBOM に含まれる必須要素として識別されており、決定できる場合は機器メーカーによって提供される必要があります。
コンポーネントのバージョン番号	ビルド番号まで、可能な限り詳細なレベルでバージョン番号を提供することが不可欠であると考えられていました。それぞれの場合に利用可能な詳細レベルを決定するのは機器メーカーに任されていました。
医療提供組織プルによるインターネット経由の配信	SBOM の実際の使用をモデル化するために、医療提供組織は必要に応じてリポジトリからデータを取得します。　API アクセスが最初に提案されましたが、最終的にはクラウド・ファイル共有がこの目的で使用されました。

概念実証の範囲外の項目

概念実証の範囲外と見なされました項目を表 25 に示します。

表 25　ヘルスケア概念実証のスコープ外の項目

項目	説明
BOM にハードウェアを含める	これにより、BOM は SBOM ではなくサイバーセキュリティ BOM または CBOM（FDA によって定義されたもの）になります。ハードウェアを含めると、ハードウェアの識別と指定において、いくつかの困難な問題が発生します。これは、概念実証を完了するには重要ではありません。
単一の標準形式の特定	目標は、特定の形式を推奨するのではなく、情報を医療提供組織に転送するために使用できる 1 つ以上の形式を特定することでした。データが正常に生成および利用される限り、伝達に使用される形式を解決することは重要ではありませんでした。
SBOM に脆弱性情報を含める	脆弱性管理は、最初から明確な医療提供組織のユースケースでしたが、一旦、生成された SBOM の脆弱性に関する情報を提供してしまうと、将来提供される脆弱性情報が表現できなくなると感じられました。SBOM が提供された後は、いつでも、医療提供組織が、コンポーネントに関連する脆弱性を識別できることが重要でした。これは、予想される実際の SBOM の使用をモデル化したものです。
グローバルに一意のコンポーネント識別子	これは SBOM の広範な使用にとって重要であると見なされていましたが、これを行う方法を解決することは、真に難しい問題であり、他のワーキング・グループによってすでに取り上げられていました。
コンポーネント・コンテキスト	コンポーネントが医療機器に含まれている可能性があるものの、サイバーセキュリティの脆弱性を示す方法で使用されていないことを SBOM 利用者に伝える方法を提供することは、当初は範囲内でしたが、これを提供する SBOM の情報は、概念的にも、使用されているフォーマット（SPDX と SWID)その情報を表現することにおいても困難でした。なので、この件で概念実証を完了する必要はありませんでした。

SBOM データへのプログラムによるアクセス	医療提供組織が機器メーカーによって維持されているリポジトリから SBOM を直接取得できるメカニズム（API など）を提供することは、当初は範囲内でしたが、概念実証に不可欠ではなかったため、除外されました。

1.2.4.1.11.4 概念実証のユースケース詳細

調達ユースケースの概念実証実施状況を表 26 に示します。

表 26 調達ユースケースの概念実証実施状況

項目	ステータス
サポートされていないソフトウェアまたは脆弱なソフトウェアを特定して、機器メーカーが代替の緩和策またはセキュリティ対策を開始できるようにします。	実施
潜在的なサイバーセキュリティの懸念を特定することにより、資産管理に通知します。	実施
デバイス内のソフトウェア・コンポーネントの寿命に関する明確さ、たとえば、デバイスには将来寿命が尽きる（サポートが切れる）ことが知られている Windows 7 があり、移行スケジュール、終了するコンポーネントを持つデバイスのセキュリティ・カバレッジに関する問いかけを行うことが可能です。	部分的に実施されました（サポートされていないサポート終了ソフトウェアは自動的に識別されませんでしたが、手動分析が実行されました）
新しいデバイスおよびすでにフィールドにあるデバイスのライフサイクル管理（現在サポートされているソフトウェアとサポートされていないソフトウェアの理解）	部分的に実施されました（サポートされていないサポート終了ソフトウェアは自動的に識別されませんでしたが、手動分析が実行されました）
SBOM が MDS2 を補完できるため、記入する必要のある質問票の数を減らすことができます。	未実施
カスタマイズされたソフトウェアの IT システムへの導入に関する認識	未実施（カスタム・ソフトウェアは簡単に識別できなかった）
インターフェースまたはシステムの存在に関する、医療 IT システムなどとの競合の認識	未実施

資産管理ユースケースの概念実証実施状況を表 27 に示します。

表 27 資産管理ユースケースの概念実証実施状況

項目	ステータス
各コンポーネントの十分な詳細を提供することにより、資産を保護するために実行できる活動	実施
資産管理のリスク評価の標準化による医療提供組織の支援	実施
ソフトウェアとデバイスのサポート終了に関する情報を提供し、サポート終了時の計画を支援します。	部分的に実行されました（サポートされていないサポート終了ソフトウェアは自動的に識別されませんでしたが、手動分析が実行されました）
SBOMの変更/更新が医療提供組織に伝達される場合の資産インベントリ	未実施
カスタマイズされたソフトウェアの IT システムへの導入に関する認識	未実施（カスタム・ソフトウェアは簡単に識別されなかった）
インターフェースまたはシステムの存在に関する、医療 IT システムなどとの競合の認識	未実施
SBOM が MDS2 を補完できるため、記入する必要のある質問票の数を減らすことができます。	未実施

リスク管理ユースケースの概念実証実施状況を表 28 に示します。

表 28 リスク管理ユースケースの概念実証実施状況

項目	ステータス
ソフトウェアの統合前に病院ネットワークに追加されている新製品の評価を行う（ネットワークに追加する前にデバイスの潜在的なリスクを判断する）	実施
特定の脆弱性に関連するリスクのレベルの評価（SBOM を使用すると、製品に存在する脆弱性を確認し、CVE などを調べてリスク評価を行うことができます）	実施
新しい脆弱性が発生したときの医療提供組織インベントリの監視	実施
サポートされていないソフトウェアまたは脆弱なソフトウェアを特定して、医療提供組織が代替の緩和策またはセキュリティ対策を実施できるようにします	部分的に実施された（サポートされていない保守終了ソフトウェアは自動的に識別されませんでしたが、手動分析が実行されました）
新しいデバイスおよびすでに運用済みのデバイスのライフサイクル管理（現在サポートされているソフトウェアとサポートされていないソフトウェアの理解）	部分的に実施された（サポートされていない保守終了ソフトウェアは自動的に識別されませんでしたが、手動分析が実行されました）

脆弱性管理ユースケースの概念実証実施状況を表 29 に示します。

表 29 脆弱性管理ユースケースの概念実証実施状況

項目	ステータス
統合前に病院ネットワークに追加されている新製品の評価（ネットワークに追加する前にデバイスの潜在的なリスクを判断する）	実施
特定の脆弱性に関連するリスクのレベルの評価（SBOM を使用すると、製品にまだ存在する脆弱性を確認し、CVE などを調べてリスク評価を行うことができます）	実施
サポートされていないソフトウェアを特定して、代替の緩和策またはセキュリティ対策を開始できるようにします。	実施
新しい脆弱性が発生したときの医療提供組織インベントリの監視	実施
新しいデバイスおよびすでに運用済みのデバイスのライフサイクル管理（現在サポートされているソフトウェアとサポートされていないソフトウェアの理解）	部分的に実施された（サポートされていない保守終了ソフトウェアは自動的に識別されませんでしたが、手動分析が実行されました
補足的なネットワークスキャンや補足的な組織侵入テストなどのプロアクティブなセキュリティ活動で医療提供組織を支援します。	未実施

参加者の役割

NTIA SBOM ヘルスケア概念実証における役割を表 30 に示します。

表 30 ヘルスケア概念実証での役割

役割	説明
NTIA	関連する SBOM ワーキング・グループと結果を統合するために、概念実証の目的と要件に関する情報を提供します。
医療提供組織	概念実証の目的と要件に関する情報を提供し、機能要件に関連する SBOM 統合プロセスに関するフィードバックを提供します。また、ユースケース定義とドラフト最終レポートの作成を支援します
機器メーカー	概念実証の目的と要件に関する情報、および SBOM 作成プロセス、開発ツール、統合プロセスに関するフィードバックを提供します。 また、ユースケース定義とドラフト最終レポートの作成を支援します。

概念実証の方法論

この概念実証の実行方法は、参加している機器メーカーが、医療提供組織の資産インベントリ内の製品の SBOM を作成する知識と能力を持っているという前提で実施されています。医療提供組織には、SBOM を取り込むための知識、プロセス、およびプラットフォームがあることが前提です。これらの前提から、SBOM 作成のユースケースと SBOM 取得のユースケースを実行するために 2 つの主要なワーキング・グループが形成されました。

SBOM 作成ユースケースのワーキング・グループ

SBOM 作成ユースケースのワーキング・グループは、機器メーカーが確立されたプロセスを使用して SBOM を作成し、それらの SBOM を医療提供組織に配信して取り込む責任を負いました。 各機器メーカーは、SBOM を作成するために、別々に作業を行いました。 機器メーカーの経験の共有と、SBOM の作成（フォーマットとコンテンツ）に重点を置いています。

SBOM 取得ユースケースのワーキング・グループ

SBOM 取得ユースケースのワーキング・グループは、医療提供組織が SBOM の取り込み、処理、および分析をシミュレートする責任を負いました。 各医療提供組織は、構成管理データベース（CMDB）、セキュリティ情報およびイベント管理（SIEM）システム、脆弱性スキャナー、およびカスタム開

発されたソフトウェアツールを利用して、このシミュレーションを実行しました。 医療提供組織の経験、成功、課題、および学んだ教訓が共有されました。

SBOM 概念実証ワーキング・グループ

SBOM 概念実証ワーキング・グループは、アプローチ、目的、懸念、条件、設定の確立および説明を担当し、ガイドラインと結果を確立することにより、概念実証を開発および報告する責任を負いました。

1.2.4.1.11.5 概念実証で発見した課題

SBOM 作成における課題

初期の概念実証の範囲は、既存の医療機器装置のインベントリを管理する医療提供組織によって定義されました。次に、この情報はそれぞれの機器メーカーに提供されました。概念実証を実行する目的で、インベントリ内の少数 (1〜2) のデバイスが機器メーカーによって選択されました。SBOM の生成は、機器メーカー間でわずかに異なりましたが、手動プロセスと半自動プロセスの両方の組み合わせで行われ、多くの場合、一般的なスクリプト言語や既存のソフトウェア構成分析ツールの支援を受けて、SBOM が作成されました。 SBOM の作成全体を通じて、機器メーカーは、医療提供組織に配信する前に、ファイル形式を調整することを目的として、協調的かつ反復的なアプローチを利用しました。 「ソフトウェア ID 名」や「サプライヤー名」などの属性の標準的な命名規則がないため、機器メーカーは、コンポーネントの常識的な名前または妥当な名前で、命名を行いました。これらの課題にありましたが、機器メーカーは SBOM 作成タスクを完了し、概念実証タイムラインから逸脱しませんでした。

この概念実証のために、医療機器メーカー参加者は、次の情報を含む医療機器 SBOM を生成しました。

1. 記載者

    - 記載者
    - 記載日時
    - 記載のコメント

2. SBOM ドキュメント名

3. 以下の情報で構成される SBOM コンポーネントのリスト。

- コンポーネント名
- バージョン
- コンポーネント・サプライヤー
- 識別子
- ダウンロード場所分析されたファイル
- ライセンス
- 著作権テキスト

SBOM の生成には、手動と自動の両方のアプローチが使用されました。一部の機器メーカーには、SBOM の生成を自動化するために使用できる内部システムがありませんでしたが、すべての機器メーカーには、データを取得するための内部プロセスがありました。医療機器 SBOM を生成する場合、複数のソースから情報を収集する必要がある場合があります。 機器メーカーによって構築された、独自のアプリケーションに統合された、OSS および商用コンポーネントは、ソフトウェア・ビルドおよび関連ドキュメントから取得できます。ただし、オペレーティング・システムやデータベースなど、ハードウェア・プラットフォームの一部として含まれているコンポーネントは、デバイスの仕様などの他のソースから取得する必要がある場合があります。したがって、医療機器 SBOM の生成を完全に自動化するには、複数のデータ・ソースを考慮する必要があります。機器メーカーが自動化を使用した場合、最初に手動プロセスを使用して情報を収集し、次に自動化を利用してコンテンツ仕様に基づいてデータを整えました。

現在、コンポーネント名、バージョン、およびサプライヤーの値を取得するための信頼できる参照元はありません。 概念実証の場合、機器メーカーは、これらの値を定義するためにベストエフォート型のアプローチを採用しました。したがって、機器メーカーは、同じコンポーネントの医療機器 SBOM で異なる値を持つ場合があります。 製品版として SBOM を配布する際には、記載者がこの情報を識別するための明確で一貫性のあるメカニズムを持っていることが重要になります。

パッケージ URL（purl）構文がコンポーネント識別子に使用されました。これは、次の purl 構造を使用したコンポーネント名とバージョンの組み合わせに基づいていました。

```
pkg: commonname/<component name@<component version
```

構成にオプションの「名前空間」を含め、次のようにコンポーネント・サプライヤー名を使用することで、この定義を改善することができます。

pkg: commonname/<component supplier name/<component name@<component version

この構文を使用すると、コンポーネントの一意で一貫性のある識別子が得られます。

ダウンロード場所、分析されたファイル、ライセンス、および著作権テキストの要素は、概念実証ではオプションでした。 機器メーカーは、これらのフィールドの値は SPDX データベースですぐに利用できず、情報を見つけるために時間が許された場合にのみ提供されたと述べました。

概念実証では、機器メーカーは依存関係情報を提供しませんでした。これは、抽出するのが難しい情報であり、取得する方法が複雑です。機器メーカーは、医療提供組織のリスク管理に依存関係情報が必要かどうか分かりませんでした。

概念実証に使用される SBOM 形式は、SBOM に記載される、医療機器の識別情報が提供されませんでした。したがって、機器メーカーは、SBOM ファイルに含まれている追加のドキュメントを通じて、医療機器の識別情報を提供しました。概念実証からの観察では、SBOM コンポーネントを定義するために使用されたのと同じ情報を、医療機器を明確に識別するために、SBOM に含めることも可能です。基本的に、これらの方法を任意の SBOM に適用して、SBOM 記載者に SBOM コンポーネント・リストを作成するときに必要な情報を、追加で提供することができます。

機器メーカーは、SBOM を SPDX および/または SWID 形式で提供しました。 ワーキング・グループは、概念実証用に選択された SBOM コンテンツに基づいて、各フォーマットの仕様について合意する必要がありました。 2 つの形式の変動性と柔軟性には、SBOM 全体の一貫性のために制約された仕様を確立する必要がありました。

概念実証の場合、SBOM のバージョンを管理したり、医療機器と関連する SBOM の複数のバージョンを管理したりする必要はありませんでした。これらは、医療機器のライフサイクル全体を通じて、対処する必要がある重要な考慮事項です。 このトピックの議論中に、1 つ以上の独自仕様、COTS、または OSS コンポーネントが変更されたため、機器メーカーは医療機器のバージョンごとに異なる SBOM バージョンを持つ必要があると判断されました。

SBOM 利用における課題

医療提供組織と機器メーカーの両方が、医療機器調達プロセス全体で、医療機器 SBOM 利用における、サイバーセキュリティの上の利点を特定しました。SBOM の生成、配布、取り込み、処理、および分析は、構成管理データベース（CMDB）、セキュリティ情報およびイベント管理（SIEM）システム、脆弱性スキャナー、およびカスタム開発を活用して、複数のユースケースで実行されました。

すべてのユースケースでの主な課題は、SBOM 属性の標準の URI(Universal Resource Identifier)がないことでした。これにより、手動のマッピングを実行する必要がありました。

さらに、信頼できる「ソフトウェアの保守終了データベース」はなく、手動による介入やカスタム・クエリの作成なしにカスタム・ソフトウェアを簡単に特定することもできませんでした。同様に、特定のソフトウェア名とバージョン情報が示されていましたが、パッチ・ステータス（つまり、インストールされているオペレーティング・システムのリスト）が存在しなかったため、別の方法で特定する必要がありました。

最後に、SBOM で提供される情報の完全性は、概念実証中に「現状のまま」受け入れられました。ただし、医療提供組織は、提供された情報の正確性と完全性を確認するための定義済みの監査または検証プロセスがないことに満場一致で気づきました。

調達ユースケースにおける課題

SBOM が生成されると、SBOM ファイルはオンライン・コラボレーション・ツールを使用して共有されました。しかし、将来の配布チャネルには、デバイスが開始する API 配信、Web アクセス可能なカスタマー・ポータル、またはデバイスに個別のファイルとして含まれる SBOM が含まれる可能性があります。 SBOM は、調達ツールに直接インポートされませんでした。しかしながら、SBOM の取り込みと、その後の分析は、SIEM またはカスタム・スクリプトのいずれかを使用することで迅速に実行できました。これらの補足技術を活用して、この SBOM 分析ステップが、調達活動を実質的に妨げないことが医療提供組織の期待です。

SBOM 取り込み後、このデータは、前述の分析ツールを使用して既存の National Vulnerability Database (NVD) データと関連付けられ、デバイスに含まれるソフトウェア・コンポーネントの既知の脆弱性が特定されました。この既知の脆弱性情報は、既存のデータとドキュメント（つまり、自己問診、医療機器セキュリティ（MDS2）の製造元開示ステートメント）を補足して、包括的なリスク・プロファイルを作成するために使用されました。既知の脆弱なコンポーネントの識別は、すべての医療提供組織によって迅速に実行されました。理想的には、この分析中に保守終了ソフトウェアを特定する必要がありましたが、医療提供組織は、解析された SBOM データと関連する包括的な保守終了データベースを見つけることができませんでした。

医療提供組織間のコンセンサスは、カスタム・クエリを合理的に使用して、SBOM 全体の既知の保守終了コンポーネントを特定できるというものでした。ただし、この情報は複数のソースから収集するか、手動で生成して検証する必要があります。 概念実証のタイムラインにより、保守終了コンポーネントの分析は範囲外と見なされました。

調達中に、既知の脆弱なコンポーネントを備えたデバイスを迅速に特定することで、実装前の適切な補償管理の特定がサポートされる可能性が高いと判断されました。たとえば、ネットワーク分離などの代償的なセキュリティ対策を、調達ライフサイクルの開始に向けて慎重に提案し、医療提供組織と機器メーカーの間で、より焦点を絞ったアーキテクチャ、設計、およびロードマップの議論を行うことができます。

資産管理ユースケースにおける課題

(一般)
医療提供組織は、SBOM の取り込みポイントとして、それぞれの CMDB の使用法を調査しました。しかしながら、これらのシステムの現在の実装は、解析された SBOM データを適切にインポートまたはマッピングするように構成されていないと判断されました。 カスタマイズを実行したり、これをサポートするツールを開発したりすることもできますが、概念実証の時間制限のため、これについてはこれ以上検討しませんでした。 この結論に続いて、医療提供組織は対応する CMDB ベンダーと連携し、この演習へのベンダーの関心を高めることに成功しました。

(リスク管理)
調達のユースケースと同様に、SBOM は専用のリスク管理ツールから直接利用されることはありませんでした。それでも、ガバナンス、リスク、およびコンプライアンスのソリューションは、継続的なリスク管理の目的で、分析後の SBOM データを利用できることがわかりました。

新たに発見された脆弱性に対する、デバイスの継続的な監視は実用的です。医療提供組織は、Common Vulnerability Scoring System (CVSS) を活用しました。これは、エンドユーザーに脆弱性の主要な特性と、影響を表す定量的な数値スコア（なし、低、中、高、および重大）の両方を提供します。

SBOM を利用する際、構成の脆弱性に関して、制限があることが特定されました。構成の脆弱性は SBOM ファイルで合理的に表すことができないためです。構成リスクは、デバイスのテストまたは手動で特定される可能性がありますが、リスク管理プラットフォーム上の SBOM データと一緒に、認識および追跡する必要があります。調達のユースケースで最初に特定されましたが、標準の命名規則の欠如はリスク管理のユースケースにも影響を与えました。

（脆弱性管理）

脆弱性管理のユースケースは、いくつかの独自のテストおよび悪用シナリオの可能性を浮き彫りにしました。脆弱性管理チームは、この SBOM データへのアクセスにより、調査、デモンストレーション、および攻撃的なセキュリティの目的で使用できるいくつかの固有の攻撃ベクトルを可視化できると述べました。 さらに、SBOM リスク・プロファイル情報を既存の脆弱性スキャン結果と

組み合わせて、デバイスの攻撃対象領域の全体像を提供し、依存するコンポーネント全体で、あまり知られていない脆弱性を強調することができます。

1.2.4.1.11.6 概念実証で観測されたもの

概念実証参加者は、SWID および SPDX 形式を利用した SBOM の使用に関して以下の観察を行いました。

Strengths

- 医療提供組織は、SBOM データへのアクセス、インポート/取り込み、および SBOM データを個別にクエリし、データを外部リソースと相関させて定量分析と定性分析の両方を実行することに成功しました。

- 機器メーカーは SWID 形式と SPDX 形式の両方を作成しました

- 医療提供組織および機器メーカーが特定した SBOM サイバーセキュリティは、調達プロセス、資産管理、リスク管理、および脆弱性管理の実践全体を通じてメリットをもたらします。

Weaknesses

- 標準フォーマットに準拠

- 異なる機器メーカーの医療機器は、医療機器 SBOM で異なる値を持つ場合があります

- CMDB には、SBOM データツールのインポートまたはマップがありません

- 現在、コンポーネント名、バージョン、およびサプライヤーの値を取得するための信頼できる情報源はありません。

- 依存関係情報の抽出が難しく、取得が複雑

- SBOM 構成の脆弱性の制限

- パッチ・ステータス

Opportunities

- 部品表にハードウェアを含める

- 単一の標準フォーマットを特定する
- SBOM に脆弱性情報を含める
- グローバルに一意のコンポーネント識別子
- SBOM データへのプログラムによるアクセス
- 使用済みコンポーネントの分析
- データの解析を支援するための SBOM と一緒の XML スキーマ定義（XSD）ファイルの付属
- 配布チャネル、API 配信、Web アクセス可能なカスタマー・ポータル、デバイス上のファイル

Threats

- SBOM 属性の標準の URI（Universal Resource Identifier）の欠如
- 提供された SBOM 情報の正確性と完全性を確認するための定義済みの監査または検証プロセスがない

1.2.4.1.11.7 ヘルスケアの概念実証まとめ

ヘルスケア SBOM 概念実証は、ソフトウェアの部品表が医療機器メーカーによって正常に作成され、医療提供組織によって消費されることを実証しました。 概念実証用に作成された SBOM に含まれる情報は、以前は医療提供組織が利用できなかったソフトウェアの透過性を提供し、全体的なリスク管理と運用アプローチを改善しました。 概念実証はまた、業界にとらわれない標準フォーマットをヘルスケア業界で活用でき、業界固有のフォーマットは不要であることを示しました。さらに、概念実証の調査結果は、NTIA が主導するソフトウェアの透明性を向上させるための業界を超えた取り組みに、情報を提供する必要があります。

概念実証の参加者は、追加の機器メーカーおよび医療提供組織参加者を含み、この最初の取り組みで学んだ教訓を取り入れた、2 番目の概念実証について話し合いました。この 2 番目の概念実証には、SBOM の進行中の開発、公開、利用、および保守をサポートするために、エコシステムが最終的に必要になるという認識の下で、非機器メーカーおよび医療提供組織のサードパーティによる参加も含まれる可能性があります。

1.2.4.1.12 自動車業界における概念実証

NHTSA (National Highway Traffic Safety Administration)から「現代の車両の安全のためのサイバーセキュリティのベストプラクティスのドラフト 2020 アップデート」[16]において、SBOM 関連のベストプラクティスが記載されました。その内容を表 31 に示します。

表 31 車両の安全のためのサイバーセキュリティのベストプラクティス

4.2.6 車両のソフトウェア資産管理	
G.10	製造業者は、各自動車 ECU、組み立てられた各車両で使用される運用ソフトウェア・コンポーネントのデータベース、および車両の寿命にわたって適用されるバージョン更新の履歴ログを維持する必要があります。
G.11	製造業者は、ソフトウェア・コンポーネントに関連する十分な詳細を追跡する必要があります。これにより、オープンソースまたは既製のソフトウェアに関連して新たに脆弱性が特定された場合、製造業者は、影響を受ける ECU および車両を迅速に特定します。

この内容を受けて、NTIA において自動車業界における SBOM の概念実証プロジェクトが計画されています。

このプロジェクトはサプライヤー主導のプロジェクトで以下が目的です。

- SBOM の原則と運用を研究して理解する
- 自動車業界で SBOM の事例を作成する
- 自動車メーカー/パートナーからのインプットによる実用的なアプローチとソリューション
- 実装の演習を実施
- 業界からの推奨と同意の取得

16 https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf (2021/3 月時点で確認済み)

- サプライヤーによる自主的な採用を奨励/促進

このプロジェクトの成果物として、自動車メーカーに対する、業界標準に関するサプライヤーの推奨事項を記載した報告書作成が予定されています。(作成期間は約 12 か月間の予定)

1.2.4.1.13 エネルギー業界の概念実証

NTIA において、ヘルスケア業界と自動車業界の概念実証に続いて、エネルギー業界においても概念実証[17]を行うことになりました。
一般的なソフトウェア製品には、プロプライエタリと OSS の両方の多くのコンポーネントが含まれています。脆弱性を管理するためには NVD にソフトウェア・パッケージの名前を入力して、それに適用される脆弱性（CVE）を特定します。しかしながら、ソフトウェア製品のコンポーネントの脆弱性を管理しようとするエネルギー組織はほとんどないのが現状です。
製品の SBOM がないと、その製品にどんなコンポーネントが含まれているのか、特定できないからです。Treck 社の開発した TCP/IP ライブラリの中には Ripple20 と名付けられた複数の深刻な脆弱性が存在し、世界中の数億のデバイスに影響を与えていると推定されます。Ripple20 の脆弱性に対応する際に、Ripple 20 の影響を受けたネットワーク上のすべてのソフトウェアまたはハードウェア製品のリストがあれば作業がはるかに簡単になります。ただし、そのリストを作成するには SBOM が必要です。SBOM は部分的なものであっても、全く使用しないより使用するほうが得策です。SBOM が多いほど完全であるほど、より効果的な結果が得られるようになります。NTIA のエネルギー・セクターの概念実証は、ヘルスケア・セクター、自動車セクターの概念実証同様、規制を促進するためのガイドラインを作成するものではなく、民間部門による重要な新技術の使用を促進しようとするものです。

1.2.4.2 SBOM の事例

[17] https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_energy_usecasesalrich.pdf

(2021/3 月時点で確認済み)

1.2.4.2.1 Linux Foundation[18]

Software Package Data Exchange（SPDX）は、ソフトウェア・コンポーネントの正確な識別、コンポーネント間の関係の明示的なマッピング、およびセキュリティとライセンス情報と各コンポーネントの関連付けをサポートする、ソフトウェア部品表（SBOM）情報を伝達するためのオープンスタンダードです。 SPDX 形式は、最近、LinuxFoundation と JointDevelopment Foundation によって、国際標準の承認を得るために ISO の JTC1 委員会に提出されました。

5 つの医療機器メーカーと 3 つの医療提供組織（病院システム）で構成される 8 つの医療業界組織のグループが、最近、医療用 SPDX 標準の初めての概念実証（POC）に参加しました。

医療機器業界と SBOM

ソフトウェア部品表（SBOM）は、デバイスまたはシステムの作成に使用されるソフトウェア・コンポーネントを構成する、ネストされたインベントリまたは成分のリストです。これは、医療機器業界や医療提供組織内で、元のサプライチェーンからのソフトウェア・コンポーネントの運用リスクとサイバーリスクを適切に理解するために特に重要です。

一部のサイバーリスクは、既知の脆弱性を持つコンポーネントの使用に起因します。既知の脆弱性は、Open Web Application Security Project（OWASP）のトップ 10 Web アプリケーションセキュリティリスクの既知の脆弱性など、ソフトウェア業界で広く見られる問題です。既知の脆弱性は、これらの脆弱性の悪用が人命の損失または不具につながる可能性があるため、特に医療機器に関連しています。これらの脆弱性は通常、コンポーネントが開発および組み込まれた後に発見されるため、1 回限りのレビューでは役に立ちません。代わりに、必要なのは、食品成分を可視化する方法と同様に、医療機器のコンポーネントの可視性です。

2020 年 POC の目的

この 2020 年の概念実証（POC）の目標は、NTIA SBOM ワーキング・グループ（Linux Foundation が寄稿者）によって作成された、医療機器およびヘルスケア業界向けの以前の POC からのフレーミング・ドキュメントの実行可能性を証明することでした。

この NTIA フレーミング・ドキュメントは、SPDX の対応するフィールド要素にマッピングできる

[18] https://www.linuxfoundation.org/blog/healthcare-industry-proof-of-concept-successfully-uses-spdx-as-a-software-bill-of-materials-format-for-medical-devices/ (2021/3 月時点で確認済み))

任意の SBOM 形式のソフトウェア・コンポーネントを識別するために使用する必要がある特定のベースライン・データ要素またはフィールドを定義します。

SPDX SBOM の実行と実装

参加した医療提供組織は、組織内で使用されている展開済みの医療機器のインベントリを提供しました。
ソフトウェア・パッケージが知られている名前は「あいまい」であり、誤解される可能性があるため、ベストエフォート・アプローチを使用してソフトウェア ID を決定しました。
SPDX の例は、医療提供組織インベントリ演習で特定された医療機器で使用するために従う機器メーカーのガイダンスドキュメントとともに作成されました。
機器メーカーは、17 の異なる SPDX ベースの SBOM を、手動で、ジェネレーターツールを使用して作成しました。
SBOM は、エンタープライズ Box アカウントを使用した、安全な転送を介して配信され、各機器メーカーが提供する、安全なカスタマー・ポータルを介した配信をシミュレートしました。

SPDX POC での SBOM の利用

2020 POC の結果、参加しているすべての医療提供組織が SPDX SBOM をそれぞれの SIEM ソリューションに正常に取り込み、データをすぐに検索して、製品群全体のセキュリティの脆弱性を特定できるようになりました。この情報は、他のデータ分析システム用に人間が読める表形式に変換することもできます。

複数の医療提供組織がすでにベンダー・パートナーと協力して、デバイス調達の一環として医療機器資産/リスク管理ソリューションへの直接取り込みを模索しています。 医療提供組織の 1 つは、ベンダー・パートナーの 1 つと協力して、ヘルスケア・ベンダー・リスク管理 (VRM) ソリューションへの直接取り込みを調査しており、別の医療提供組織は、正規表現を使用してパッケージフィールドを正しく解析する方法に焦点を当てた「ハウツーガイド」を開発しています。

資産管理システムで使用した場合の SPDX の適合性の肯定的な指標として､2 つの医療提供組織が、ソフトウェアの依存関係とサブコンポーネントを追跡するために、それぞれの内部追跡システムの構成を開始しました。さらに、複数の医療提供組織がベンダー・パートナーと協力して、定期的な更新と監査証跡を可能にすることで、デバイスの耐用年数を通じてデバイスを医療デバイスの資産/リスク管理ソリューションとして管理しています。

医療機器向けの SPDX ベースの SBOM に関する継続的な考慮事項

SPDX ベースの SBOM の使用に関連する参加医療提供組織では、リスク管理、脆弱性管理、および法

的考慮事項が進行中です。

危機管理

応答するすべての医療提供組織は、調達時（つまり、SBOM の SIEM への最初の取り込み時）および継続的に（つまり、SIEM、CMDB / CMMS、VRM）脆弱性を調査しています。参加している医療提供組織は、脆弱なコンポーネントを特定し、悪用可能性を測定し、リスク削減対策を実装し、SBOM と一緒にこのデータを文書化するために実行される緩和計画/補償制御演習を調査する予定です。

SPDX コミュニティは、これらの演習から学び、SPDX 仕様の将来のバージョンを改善して、リスクを効果的に管理するために必要であると判断された、要求を含める予定です。

医療提供組織での脆弱性管理

医療提供組織は、すでに SBOM データから抽出された情報に対して、脆弱性管理プロセスを手動で実行しています。

もう 1 つは、脆弱性管理チームと協力して、同じデバイスの資格情報付き/非資格情報スキャンに関連付けられた SBOM データを評価します。これは、情報監査のユースケースで役立つ場合があります。

結論

POC は、医療業界に固有の独自の SBOM フォーマットは必要ないという NTIA ワーキング・グループの結論を検証することができました。この 2020 年の POC は、SPDX 標準が、医療業界プロバイダーが使用する SBOM のオープン・フォーマットとして使用できることを示しました。さらに、SPDX 形式を SIEM ソリューションにインポートする機能は、医療提供組織が医療機器ソフトウェア・コンポーネントの運用上およびサイバー上のリスクを元のサプライチェーンから適切に理解するのに役立ちます。

ソフトウェア・コンポーネントの自動識別や、特定のシステムで悪用可能なコンポーネントの脆弱性の特定など、SPDX ベースの SBOM の自動化を改善するための作業が進んでいます。参加している医療提供組織は、この情報に基づいてリスク削減手法を特定および実装するための補償管理演習を実行する予定です。 医療提供組織は、SPDX が脆弱性管理の他の改善をどのようにサポートできるかも評価しています。要約すると、この POC は、SPDX が今日の運用リスクとサイバーリスクに対処する上で不可欠な部分である可能性があることを示しました。

1.2.4.2.2　日立製作所

日立製作所では、OSS コンプライアンスの取り組みとして、OSS 専門組織を設立して日立グループ内の OSS 活用の取りまとめを行っています。[19]その内容は OSS 活用のノウハウ及びサポートの定期協力で、SBOM を扱う OSS コミュニティ Open Chain に参加しています。独自開発の OSS 管理システムで、ライセンスの解釈情報、OSS 導入時の暗号有無や脆弱性有無などの判定を行っています。OSS に起因する脆弱性の把握には、Black Duck が利用されています。日立製作所は、業務で OSS をダウンロードする際はプロキシを経由させる仕組みを構築しています。このプロセスにおいて API を介し、 OSS のダウンロードと同時にバックエンドで Black Duck を連動させてライセンス情報をスキャンし、自動的にデータベースに登録するシステムを開発しました。担当者はコマンドラインや Web インターフェースで、このプロセスの結果をチェックできる仕組みとなっています。

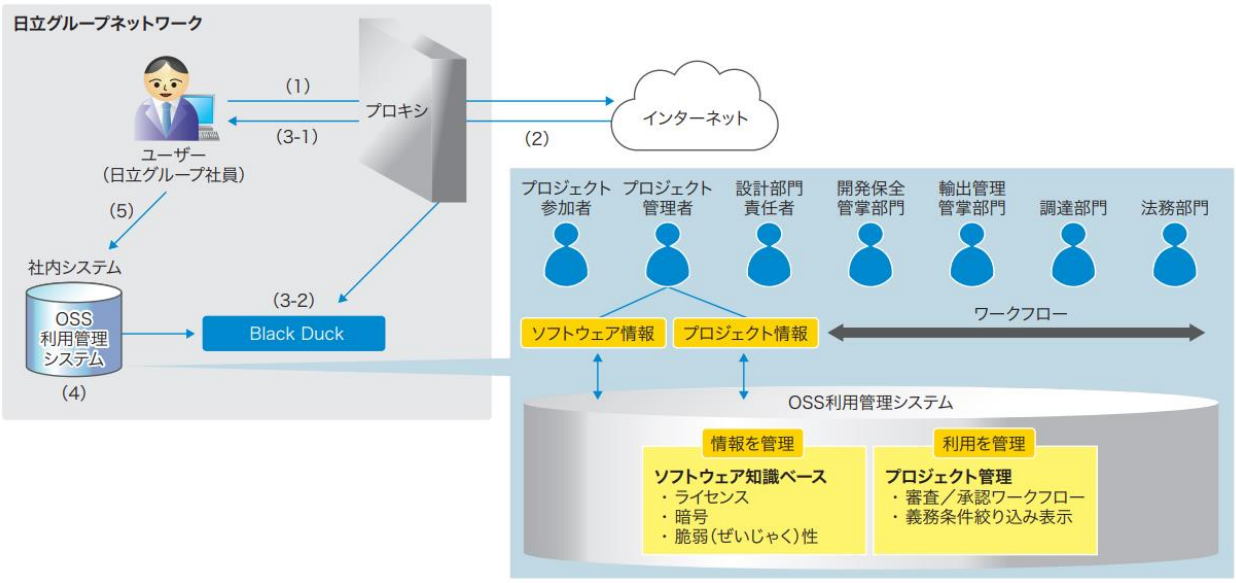

図 11　日立製作所自社開発の OSS 管理システム

日立製作所が導入した OSS のライセンスをスキャンし、登録する仕組み（注） ※注 ： 図中の記号の意味は次の通り。(1)：OSS ダウンロードリクエスト、(2)：ファイルレスポンス、(3-1)：ファイルレスポンス、(3-2)：ファイルを Black Duck にアップロード、 (4)：OSS 名、バージョン、ライセンス情報を取得、(5)：取得した OSS のライセンス確認。

19 https://www.synopsys.com/content/dam/synopsys/japan/software-integrity/case-studies/hitachi-blackduck-case-study.pdf(2021/3 月時点で確認済み)

1.2.4.2.3 オリンパスソフトウェアテクノロジー株式会社（O-Soft）[20]

オリンパス株式会社の一部門であるオリンパスソフトウェアテクノロジー株式会社(O-Soft)は、医療機器、産業機器、デジタルカメラなど、さまざまなオリンパス製品向けのソフトウェアを開発しています。O-Soft 開発者は、プロプライエタリ・ソフトウェアと OSS ソフトウェア（OSS）を組み合わせて製品開発を行います。特に OSS ライセンスの問題に関連するガバナンスの課題が存在します。

O-Soft は、包括的な OSS コンプライアンス管理ポリシーを研究開発するための OSS 委員会を設立することから始めました。委員会はオリンパスの品質および環境部門が主導し、法務、知的財産、IT、および研究開発部門の代表者が参加しました。各ビジネスユニットのソフトウェア開発者も、ポリシーを策定するための取り組みに参加しました。

製品チームの個々のソフトウェア開発プロセスに大きな変更を加えることなく、OSS ライセンスの使用と再利用のコンプライアンスを改善する取り組みを実施しました。リスクレベルは製品ごとに異なるため、OSS 委員会は製品ごとに適用される個別の OSS 使用ガイドラインを作成しました。

委員会が直面した課題の 1 つは、開発者や他の従業員が新しいガイドラインに準拠することを保証することでした。また、企業ポリシーを個々の製品グループの開発プロセスに統合する方法を決定し、コードスキャン用の信頼できるツールとソリューションを選択し、OSS を継続的に使用してアジャイルソフトウェア開発を可能にする必要がありました。

SCA ツールを他の既存の開発ツールと統合することにより、ソフトウェア・コードの出所を自動的にスキャン、検出、および識別することができます。 コンポーネントのスキャンから得られる情報が有用なことが確認されて、開発者の間で新しいポリシーを推進することに賛同を得られました。

海外子会社が多いため、ソフトウェアがどこで開発されたのか、OSS が含まれているかどうかを知るのは困難でしたが、SCA ツールを使用することにより、意図しない OSS が使用されている場所を特定するのが簡単になり、その結果、ライセンス侵害のリスクを軽減することができるようになりました。

---

[20] https://www.synopsys.com/software-integrity/customers/olympus.html

(2021/3 月時点で確認済み)

各製品ライン内のソフトウェア開発は、異なる基準の対象となります。 そのため、各グループの OSS 使用ガイドラインは、OSS 監視の責任者の任命、外部委託されたソフトウェアの意図しない OSS の検査など、これらの標準要件を反映するようにカスタマイズされました。 これらの標準を社内で共有しやすくするために、O-Soft は OSS ナレッジサイトと呼ばれる企業ナレッジデータベースを作成しました。 このサイトには、OSS 使用ガイドラインに関する社内教育に使用されるレポート形式、ガイド、テンプレート、および資料が含まれています。
オリンパス全体の開発者がアクセスできる OSS ナレッジサイトは、企業の OSS の使用に関するライセンス情報、ユースケース、およびソリューション情報を提供します。 また、海外子会社への企業方針の普及を促進するための研修資料も提供しています。

1.2.4.2.4 マニエッティ・マレリ (Magneti Marrelli)[21]

自動車業界への、国際的なコンポーネントおよびシステムサプライヤーであるマニエッティ・マレリは、GENIVI ベースの車載インフォテインメント・システムが、OEM 顧客の厳格な OSS コンプライアンスの期待を確実に満たすように、部品表を実装しました。

課題

ヨーロッパの大手自動車メーカーは、GENIVI AllianceOSS プラットフォームに基づく車載インフォテインメント（IVI）システムの開発を、マニエッティ・マレリと契約しました。プロジェクトの合意では、GENIVI ルールとフリーおよび OSS ソフトウェアライセンス要件の厳格な遵守が規定されていました。自動車メーカーは、コンプライアンスの明確な証拠がない限り、製品の納品を受け入れません。

2 年以上のプロジェクトの作業により、700 万から 800 万行のコードが蓄積されました。コードの大部分は、マニエッティ・マレリと外部サプライヤーによって開発されました。残りは、自動車メーカーによるものです。OSS ライセンスへの準拠については、コードの全量を確認する必要がありました。これは、手動で処理すると、人為的エラーが発生しやすい困難な作業です。一部の外部サプライヤーは、コンポーネントに適切な部品表を提供していましたが、大多数は提供していませんでした。社内で開発されたコードであっても、コンプライアンスの証明を提供することは不可能でした。マニエッティ・マレリは、何千もの異なる OSS スニペットがコードベースのどこかに埋め込まれているのではないかと疑っていましたが、それらを識別したり、出所やライセンス義務を検出したりする簡単な手段がありませんでした。

アプローチ

Black Duck ソリューションがインストールされ、BearingPoint Consulting がプロジェクトに参加し、専門家のアドバイス、トレーニング、およびベースライン・サービスを支援しました。

結果と利点

Black Duck の使用で分析された大量のコードにより、レビュー対象の多くのコンプライアンス領域が特定されました。潜在的な問題の候補を特定し、それらに対処する方法を決定するために、

---

[21] https://www.synopsys.com/software-integrity/customers/magneti-marelli.html

(2021/3 月時点で確認済み)

アナリストによる綿密な検査が必要でした。たとえば、ヘッダーが欠落していたり、コンポーネントのソースを特定できなかったりして、コンプライアンスを達成するために一部のコードを書き直す必要がある場合がありました。

Black Duck は、コードがクリーンで準拠していることをマニエッティ・マレリの顧客に証明する部品表、レポート、およびドキュメントを自動的に生成します。
マグネティマレリの開発者は、OSS・コンポーネントを使用する際に適切なプロセスとツールへのコンプライアンスを確保する必要性を認識しています。プロジェクトのライフサイクルの早い段階で効果的な OSS 管理インフラストラクチャを設定すると、全体的なコストと労力が大幅に削減されることが期待されます。これまでの経験は、BearingPoint の支援を受けて定義された、同社の将来の OSS ポリシーの健全な基盤として機能します。マニエッティ・マレリの経験は、ライセンス・コンプライアンスの確立と維持が実際に達成可能であることを示しています。自動化ツールと OSS 使用のベストプラクティスへの継続的な注意を払って正しく行われると、このプロセスは、準拠した高品質の製品に関して継続的かつ永続的な結果を生み出します。

2　研究発表・講演、文献、特許等の状況

(1) 研究発表・講演

なし

(2) 論文

なし

(3) 特許等（知財）

なし

(4) 受賞実績

なし

(5) 成果普及の努力（プレス発表等）

なし

契約管理番号：	20002281-0