THE LINUX FOUNDATION | Research

SBOMの導入による ライセンス遵守と ソフトウェア セキュリティ の強化

企業向けのSBOM決定版ガイド

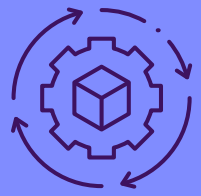
Ibrahim Haddad, Ph.D., *The Linux Foundation*
序文 Melissa Evers, *Intel*

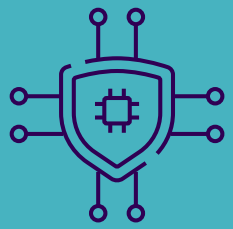
2024年8月

SBOMの導入によるライセンス遵守とソフトウェアセキュリティの強化

The Linux Foundationは、2009年にソフトウェアパッケージデータ交換（SPDX）プロジェクトを立ち上げ、**SBOM標準化に向けた重要なマイルストーンを達成しました。**

アメリカの大統領令14028は、サイバー脅威の高まりに対処するため、**連邦機関がソフトウェア調達にSBOMを使用することを義務付けています。**これにより、**サプライチェーンのセキュリティが強化されます。**





EUの**サイバー レリジエンス法**の重要な要素の一つは、**推奨されるSBOM**の導入であり、製品が設計段階から安全（セキュア バイ デザイン）であることを保証します。

SBOMは、ソフトウェア サプライチェーンを**保護**し、業界や技術領域に関係なく、**国家のサイバーセキュリティ体制を強化します。**

SBOMは包括的で機械可読なインベントリで、アプリケーション、システム、またはソフトウェアスタック内の構成要素となるソフトウェアコンポーネントを詳述しています。

SBOMは通常、**5つの主要な要素**で構成されています。コンポーネント インベントリ、起源情報、依存関係、脆弱性情報、およびメタデータと注釈です。

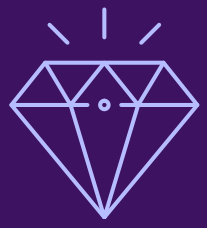
SBOMはライセンス遵守とサイバーセキュリティにおいて重要であり、組織に対してソフトウェア コンポーネントに関する重要な洞察を提供し、**ライセンスの遵守を確保し、サイバー防御を強化します。**

SBOMはライセンス遵守チームに対し、ライセンス違反に伴う**法的、評判的、技術的、および財務的リスクを軽減する**力を与えます。

SBOMは早期警告システムとして機能し、セキュリティリスクの事前軽減を可能にし、インシデントレスポンスやパッチ管理の取り組みを円滑にします。

SBOMの機能は通常、**ソフトウェアコンポジション分析（SCA）ツール**の一部として組み込まれ、オープンソースライセンスの遵守を確保し、コードのセキュリティを向上させます。

効果的な実施のために、組織はSBOMをコンプライアンスおよびセキュリティの実践に統合するのを助ける**明確なポリシーと役割を確立する**必要があります。



組織はSBOMの**定期的かつ適時な更新を行い**、その**実施の効果を監視する**必要があります。

概要

SBOM（ソフトウェア部品表）は、ソフトウェア サプライチェーンにおける透明性の向上、ライセンス遵守、セキュリティ強化において重要なツールとして注目されています。本稿では、SBOMの役割に焦点を当て、ライセンス遵守の確保、サイバーセキュリティ リスクの軽減、規制遵守の促進におけるその重要性を論じます。また、SBOMの歴史的背景を含む包括的な概要を提供し、今日の複雑なソフトウェア環境におけるその重要性を強調しています。さらに、米国のサイバーセキュリティ強化を目指す大統領令14028やEUのサイバー レジリエンス法、Linux Foundationによる業界主導のSBOM表記標準であるSPDXなど、SBOMを取り巻く法的文脈も探求しています。最後に、組織が透明性を高め、リスクを軽減し、より強固なソフトウェア エコシステムを構築するためのSBOM実装に向けた具体的な提言を示しています。

目次

序文

今日の複雑なソフトウェア サプライチェーンにおいて、SBOM（ソフトウェア部品表）は、ソフトウェア インフラの透明性、遵守、セキュリティを高めるための青写真でありツールセットとして機能しています。単なるツールに留まらず、SBOMは無数のソフトウェア コンポーネントやライセンス、潜在的な脆弱性に対する理解と管理を深めるための戦略的な要となっています。

SBOMの価値は単なる記録管理を超えています。ライセンス遵守を可能にし、サイバーセキュリティ リスクを軽減し、厳格な規制フレームワークの要求に応える上で重要な役割を果たしています。現在では、ソフトウェアが単一の開発者によって完全に作られることは稀です。ほとんどのソフトウェアは、無数のオープンソース プロジェクトや商業的ベンチャーからの貢献が複雑に絡み合ったモザイクのような構造をしています。この複雑な依存関係の中で、単一のコンポーネントが全体のセキュリティにおける重要な要素となることがあります。ソフトウェアの抽象化が進み、複合的なAIシステムのユースケースが主流になるにつれて、業界全体としてソフトウェアの複雑さと相互依存がさらに注目を集めています。そして、ソフトウェアシステムの相互接続が進むにつれ、SBOMがこれらのシステムを脅威から守り、運用の健全性を維持する役割はますます重要になっています。

最近の政府の命令により、SBOMはサイバーセキュリティ戦略の最前線に押し上げられ、ソフトウェアの透明性に関する標準化された手法の必要性が世界的に認識されています。この急速に変化する状況の中で、Linux Foundationの指導のもと、Intelやその他の参加企業による長年の貢献が、SPDX（ソフトウェア パッケージ データ交換）、OpenChainなどのプロジェクトを通じて実現されています。これらのプロジェクトは、SBOMの表現に関するオープン標準とその取り扱いプロセスを確立し、業界の関係者が連携してコンプライアンスの効率化と改善を目指す共通の目標に向かっています。

SBOMの戦略的導入を推進する際、私たちは単なる一連の手法を提唱しているわけではなく、デジタル インフラの基盤を強化するためのオープン性、協力、再利用の文化を育んでいます。SBOMの採用と改良に向けた集団的な取り組みは、業界が強靭なソフトウェア エコシステムを構築することに専心している証です。

私たちは今、今日の決断が明日のセキュリティとコンプライアンスの未来を形作る岐路に立っています。SBOMやSPDX、OpenChainといった協力的な取り組みを受け入れることで、ソフトウェアが世界を支えるだけでなく、最大限の誠実さと信頼性をもって機能する未来を確実にすることができます。透明性が強化された時代へようこそ—共に築き上げる安全な未来が待っています。

Melissa Evers, Intel Corporation Vice President,
Software and Advanced Technology

はじめに

今日の急速に進化するテクノロジーの環境において、ソフトウェア全般、特にオープンソース ソフトウェアは、イノベーションと競争力を推進する上でますます重要な役割を果たしています。そのため、ライセンス遵守とセキュリティを確保するための強固なガバナンス メカニズムが求められています。ここで登場するのが、ソフトウェア部品表（SBOM）です。これは、組織のエコシステム内のソフトウェア コンポーネントに対する前例のない可視性とコントロールを提供する、洗練された不可欠なツールです。本稿の目的は、SBOMの戦略的重要性を強調し、ソフトウェア セキュリティとライセンス遵守の実践を強化すること、法的要件や業界イニシアティブを考慮しながら、SBOM導入計画を支援するための具体的な戦略を提供することです。

歴史的な視点

製品サプライチェーンにおいて部品表の概念は過去50年間標準的な存在でしたが、機能がソフトウェアに移行するにつれて、ソフトウェア サプライチェーンの重要性が高まっています。SBOMの概念は、ソフトウェア サプライチェーンの複雑さの増大と、ソフトウェア開発における透明性と説明責任の重要性の高まりに応じて、年々進化してきました。最初は、航空宇宙、自動車、防衛などの厳格な規制がある業界でSBOMが注目を集め、厳密なコンプライアンス要件によりソフトウェア コンポーネントの詳細な文書化が求められました。しかし、オープンソース ソフトウェアの普及とクラウド コンピューティングの登場によって、SBOMはさまざまなセクターでより広く注目を集めるようになりました。ソフトウェア エコシステムが拡大し、依存関係が増える中で、標準化されたSBOMフレームワークの必要性がますます明らかになり、SBOMの導入を促進するための業界主導のイニシアティブが基盤を築くこととなりました。

Linux Foundationは2009年にSPDX（ソフトウェア パッケージ データ交換）プロジェクトを立ち上げ、SBOMの標準化に向けた重要なマイルストーンを築きました。SPDXは、SBOMを文書化し共有するための共通の標準を開発し、相互運用性と協力を促進することを目的としています。最近では、OWASPのCycloneDXのような取り組みも登場し、SBOMのための軽量で機械可読なフォーマットとして依存関係の追跡の必要性に応え、SBOM標準化の推進に寄与しています。

SBOMの動きは、2021年5月に発表されたアメリカ合衆国の**大統領令14028**「国家サイバーセキュリティの向上」によって加速しました。この大統領令は、増大するサイバー脅威を背景にソフトウェア サプライチェーンのセキュリティ強化の重要性を強調し、連邦機関に対してソフトウェア調達のためにSBOMを採用するよう指示しました。また、SBOMの最小要素の確立（後のセクションで議論）を求め、協力的な取り組みを通じてより広範な採用の基盤を築きました。その結果、SBOMは特定の厳格な規制のある業界での狭い文脈から、業界の種類や技術領域にかかわらずソフトウェア サプライチェーンを保護し、国家のサイバーセキュリティの構えを強化するための立法および規制の取り組みの広範な要素へと移行しました。

SBOMの基礎

SBOMがソフトウェアのセキュリティとコンプライアンスを向上させる上での重要な役割を理解するためには、その有用性と構成に関する基本的な概念を学ぶことが不可欠です。SBOMは、アプリケーション、システム、またはソフトウェア スタック内の構成ソフトウェア コンポーネントを詳細に記載した包括的かつ機械可読なインベントリとして機能します。従来の製造における部品表に似て、SBOMはソフトウェア サプライチェーンの透明性と可視性を提供し、強固なソフトウェア ガバナンスやリスク管理の実践を促進します。

SBOMは通常、以下の五つの主要な要素で構成されています：コンポーネント インベントリ、来歴情報、依存関係、脆弱性インテリジェンス、メタデータおよび注釈です。これらの要素について、以下の小節で簡単に説明します。

コンポーネント インベントリ

コンポーネント インベントリは、すべてのソフトウェア コンポーネントの詳細なリストであり、オープンソースおよび商用コンポーネントの両方を含むとともに、それぞれのバージョンや依存関係も記載されています。

来歴情報

来歴情報は、各ソフトウェア コンポーネントの出所と所有権に関するメタデータを含み、ライセンス条件、著作権の帰属、貢献者の情報などが含まれます。

依存関係

依存関係は、ソフトウェア コンポーネント間の依存関係を示す階層的な関係であり、トレース可能性や影響分析を容易にします。

脆弱性インテリジェンス

脆弱性インテリジェンスは、コンポーネント インベントリ内の各ソフトウェア コンポーネントに関連する既知のセキュリティ脆弱性に関する詳細な情報を含みます。この情報の目的は、リスクの積極的な軽減と脆弱性管理を可能にすることです。

メタデータおよび注釈

メタデータおよび注釈は、SBOMをより詳細にする追加の文脈情報であり、ビルド手順、リリースノート、コンプライアンスの証明などが含まれます。

SBOMの重要性

SBOMは、ライセンス遵守とサイバーセキュリティの両面で重要な役割を果たします。商用ライセンスやオープンソース ライセンスを含む適用可能なライセンスの遵守を確保し、サイバー脅威に対する防御を強化することで、SBOMは組織にとってソフトウェア コンポーネントに関する貴重な洞察を提供します。以下の小節では、ライセンス遵守とセキュリティの観点からSBOMが果たす役割についてさらに詳しく掘り下げます。

ライセンスの遵守

ライセンス遵守の観点から、SBOMは組織の運営を支えるソフトウェア コンポーネントの複雑なネットワークに関する包括的な洞察を提供することで、戦略的な利点をもたらします。今日の環境では、組織がソフトウェア スタックを構築する際にオープンソース ソフトウェアに依存しているため、オープンソースおよび商用ソフトウェア資産をカタログ化し、ライセンスの義務を理解し、それを実行し、履行するための計画を立てることが重要です。**Synopsysの2024年の報告書**によると、スキャンした全コードベースの77%がオープンソースからのものであるとされています。この数字は、オープンソース ソフトウェアへの依存度の高さを示しています。SBOMは、ライセンス遵守チームがライセンス違反に伴う法的、 評判的、技術的、財務的リスクを軽減するのを支援します。SBOMがない場合、組織は多くのライセンス遵守の落とし穴にさらされ、手動でのエラーが発生しやすいソフトウェア資産の追跡方法に頼ることになり、運用効率を損ない、不必要なリスクにさらされることになります。

セキュリティ

サイバーセキュリティの分野において、SBOMはソフトウェア サプライチェーン内の進化する脅威に対する組織のレジリエンスを向上させるための重要な資産として浮上します。第三者コンポーネントの脆弱性を事前に特定し対処することで、SBOMは早期警戒システムとして機能し、組織がセキュリティ リスクを深刻な侵害に発展する前に予防的に軽減できるようにします。さらに、SBOMはインシデント対応やパッチ管理の取り組みを効率化し、組織に重要な資産を保護し、セキュリティ脆弱性の悪用を避けるために必要な敏捷性と先見性を提供します。

法的文脈

米国

増大するサイバー脅威と規制の厳格化を背景に、アメリカの**大統領令14028**（前述）などの立法努力は、ソフトウェア サプライチェーンのセキュリティを強化することの戦略的重要性を強調しています。この行政命令の中心には、SBOMの最小要素を明確にする指示があり、SBOMをソフトウェア開発ライフサイクル全体における透明性と説明責任を促進するための重要な要素として位置付けています。次のセクションでは、EO 14028によって定義されたSBOMの最小要素を強調し、認識と可視性を高めることを目指します。

EO 14028の発表に至る重要なマイルストーン：

1. **2013年2月:** 国家標準技術研究所（NIST）サイバーセキュリティ フレームワークの確立： NISTは、組織のサイバーセキュリティ インフラを改善するためのガイドラインとベストプラクティスを提供するサイバーセキュリティ フレームワークの初版を発表しました。
2. **2013年2月:** 大統領政策指令21：大統領政策指令21は、重要インフラの強化とセキュリティを高めるために、国家的な取り組みを進めることを目的としました。これにより、レジリエンスとセキュリティの向上が図られました。
3. **2015年6月:** アメリカ人事管理局（OPM）のデータ侵害：アメリカのOPMは大規模なデータ侵害を受け、2100万人以上の連邦職員の個人情報が漏洩しました。この侵害は、政府機関内の重大なサイバーセキュリティの脆弱性を浮き彫りにしました。
4. **2017年5月: EO 13800:** トランプ大統領は、連邦ネットワークおよび重要インフラのサイバーセキュリティを強化するためのEO 13800に署名しました。この大統領令は、連邦ネットワークと重要インフラのサイバーセキュリティの向上に重点を置いています。
5. **2019年1月:** サイバーセキュリティ成熟度モデル認証（CMMC）イニシアティブ：国防総省（DoD）は、サプライチェーンのサイバーセキュリティの構えを強化するために、サイバーセキュリティの実践に対する第三者認証を要求するCMMCを導入しました。
6. **2020年12月:** SolarWindsサイバーセキュリティ侵害：SolarWinds攻撃は重要なサプライチェーンのサイバー インシデントであり、複数の連邦機関や民間企業が侵害され、サイバーセキュリティ対策の強化の必要性が強調されました。
7. **2020年1月:** 2021年度国家防衛権限法（NDAA）：NDAAにはサイバーセキュリティを改善するための規定が含まれ、特にDoDサプライチェーン内でのSBOMの重要性が強調されました。
8. **2021年5月:** コロニアル パイプライン ランサムウェア攻撃：コロニアル パイプラインのランサムウェア攻撃は、アメリカ東海岸の燃料供給を混乱させ、重要インフラがサイバー脅威に対して脆弱であることをさらに浮き彫りにしました。
9. **2021年5月12日:** EO 14028の発表：バイデン大統領はEO 14028「国家のサイバーセキュリティの向上」に署名しました。このEOは連邦機関にSBOMの採用、ソフトウェア サプライチェーンのセキュリティの強化、および包括的なサイバーセキュリティ対策の実施を義務付けています。

増大するサイバー脅威と規制の厳格化を背景に、アメリカのEO 14028（前述）などの立法努力は、ソフトウェア サプライチェーンのセキュリティを強化することの戦略的重要性を強調しています。

EU

さらに、2024年3月12日、欧州議会は**EUサイバー レリジエンス法（CRA）**を大多数で承認しました。この法律は、地域内で販売されるハードウェアおよびソフトウェア製品に対して包括的な要件を設定することで、EU全体のサイバーセキュリティを強化することを目的としています。この法律は、製造業者に対して、製品が設計段階から安全（セキュアバイ デザイン）であり、定期的に更新され、サイバー脅威に対して強靭であることを確保する必要性を強調しています。法律の重要な要素の一つは、暗黙のSBOM要件の導入であり、製造業者は市場監視当局の要求に応じてSBOMを作成する必要があります。この透明性は、潜在的な脆弱性を特定し、第三者およびオープンソース ソフトウェアを含むすべてのコンポーネントがセキュリティ基準を満たしていることを保証します。これらの措置を実施することで、法律はデジタル製品の全体的なセキュリティを強化し、消費者や企業をサイバー リスクから保護することを目指しています。

日本

日本の**経済産業省（経産省；METI）**は、サプライチェーンがますます複雑化する中で、ソフトウェア セキュリティへの脅威を管理するためにSBOMの重要性を強調しています。経産省は、ソフトウェア サプライヤー向けにSBOMの採用の利点と主要な実施ポイントを概説したガイドを作成しました。このガイドは、企業に対してSBOMの採用を促進し、ソフトウェア管理の向上、脆弱性への対応時間の短縮、管理コストの削減、開発生産性やサイバーセキュリティのパフォーマンスの向上を図るよう促しています。

経産省は、このガイドの広範な採用がより良いソフトウェア管理の実践につながり、業界全体のサイバーセキュリティを強化することを期待しています。

カナダ

カナダでは、SBOMの使用を義務付ける特定の法律はまだ実施されていません。しかし、国の行政がSBOMの重要性を認識している兆しがあります。**カナダ サイバーセキュリティ センター**は、SBOMを透明性とリスク管理ツールとして採用することを含むサイバーセキュリティのベストプラクティスを積極的に推進しています。組織がSBOMをソフトウェア開発および調達プロセスに統合することを奨励し、脆弱性管理や全体的なサイバーセキュリティ姿勢の向上を目指しています。これらの取り組みは、現段階では法的要件ではなく、ガイダンスやベストプラクティスの採用に焦点を当てています。

中国

中国は、SBOMの実施を支援するために立法枠組みを強化する積極的な取り組みを行っています。2024年の立法アジェンダの一環として、中国政府はサイバーセキュリティとソフトウェア脆弱性管理に強い重点を置いており、国家の安全保障と技術の進展を強化するという広範な目標を反映しています。全国人民代表大会常務委員会は、これらの問題に対処するためにいくつかの立法プロジェクトを進めています。これらのイニシアティブには、サイバー ガバナンスの改善、ソフトウェア サプライチェーンリスクの管理、ソフトウェア コンポーネントのセキュリティ確保に向けた努力が含まれています。SBOMを義務付ける特定の法律は明示的に言及されていませんが、立法努力は、ソフトウェアの透明性や脆弱性管理といったSBOMの目的に沿ったより広範な原則を包含しています。

SBOMの最小単位

先に述べたように、アメリカ合衆国のEO 14028は、連邦ネットワークとソフトウェア サプライチェーンのサイバーセキュリティを強化するためのいくつかの措置を義務付けています。その要件のキーの一つは、SBOMの最小要素を定めることです。これらの最小要素は以下の通りです。

ソフトウェア コンポーネントの識別

SBOMは、システムまたはアプリケーション内の各ソフトウェア コンポーネントを識別する必要があります。これには、オープンソース ソフトウェアや独自のサードパーティ製商用コンポーネントが含まれます。

バージョン番号

SBOMは、依存関係の正確な追跡と管理を確保するために、各ソフトウェア コンポーネントのバージョン番号を明示する必要があります。

来歴情報

SBOMは、各ソフトウェア コンポーネントの出所と所有権に関するメタデータを含める必要があります。これには、ライセンス情報、著作権の帰属、貢献者に関する情報が含まれます。

依存関係

SBOMは、ソフトウェアコンポーネント間の階層的な関係を明示する必要があります。これには、さまざまなモジュールやライブラリ間の依存関係や相互作用が含まれます。

セキュリティ属性

SBOMは、各ソフトウェア コンポーネントに関連する既知のセキュリティ脆弱性に関連付けられた情報と組み合わせることができるため、組織はセキュリティ リスクを評価して軽減することができます。セキュリティ情報は通常、公開されたセキュリティ脆弱性のデータベースであるCVE（Common Vulnerabilities and Exposures）から取得されます。

SBOMフォーマット

SBOMは、異なる組織やシステム間での相互運用性や情報の交換を促進するために、標準化されたフォーマットまたはスキーマに準拠するべきです。

これらのSBOMの最小要素は、ソフトウェア サプライチェーンにおける透明性、説明責任、およびセキュリティを促進するための基本的なフレームワークを提供し、組織がサードパーティ ソフトウェア コンポーネントに関連するリスクをよりよく理解し管理できるようにします。

システム[1] パッケージ データ交換オープン スタンダード

Linux FoundationのオープンソースプロジェクトSPDXは、2009年からSBOMの標準化とその採用促進の最前線に立っており、EO 14028の11年以上前から活動を行っています。Linux Foundationは、オープンソースライセンスのコンプライアンス プラクティスを支援するための共通フレームワークの必要性を認識し、ソフトウェアコンポーネント情報の交換を促進するための素晴らしいリーダーシップを発揮してきました。SPDXは、さまざまな業界の組織を集めて、SBOMの作成、共有、分析のための標準化されたフォーマットとツールを開発しています。典型的なオープンソースの協力的な取り組みとコミュニティの参加を通じて、SPDXはSBOMの採用と実装を支援するためのツール、リソース、ベストプラクティスの堅固なエコシステムを確立しました。ガイダンスを提供し、仕様を開発し、協力を促進することで、Linux FoundationはSPDXの取り組みを通じてSBOMの標準化を進め、組織が透明性を向上させ、ライセンス コンプライアンスを効率化し、ソフトウェア サプライチェーン内のセキュリティを改善するための重要な役割を果たしています。

効果的なSBOM実装のための推奨事項

SBOMの潜在能力を最大限に活用するために、組織は、自動化と戦略的活用を基盤とした実装に向けた戦略的アプローチを採用する必要があります。本セクションでは、業界のリーディング企業との交流を通じて得た推奨される実践例をいくつか紹介します。

明確なポリシーと手順を確立する

組織は、ソフトウェア開発ライフサイクル全体にわたるSBOMの生成、維持、および活用に関する包括的なポリシーと手順を策定する必要があります。これらのポリシーと手順は、通常、組織の内部コンプライアンスおよびセキュリティ インフラを定義する大規模な取り組みの一環として設けられます。

明確な役割と責任を定義する

組織は、すべての従業員がSBOMに関する自身の役割と責任を理解し、より広い視点では適用されるソフトウェア ライセンスの遵守やソフトウェア セキュリティ ガイドラインを確実に守るための実践について理解していることを確認する必要があります。企業によっては、この機能を果たすためのチームを中央集権型にするか、あるいは専任のオープンソース コンプライアンス オフィサーを含むクロス ファンクショナル チームを設けて、DevOps、エンジニアリング、法務などの各部門と連携しながら対応するケースもあります。オープンソース ライセンス コンプライアンスのインフラを整備する方法については、Linux Foundationが発行する「Open Source License Compliance in the Enterprise」第2版を参照することをお勧めします。

SBOMの生成を自動化する

組織は、継続的インテグレーションおよびデリバリー パイプラインの一環としてSBOM生成を統合し、各ソフトウェア ビルド時にSBOMが自動的に作成されるようにする必要があります。SBOMの機能は、一般的にソフトウェア開発チームがオープンソース ライセンスのコンプライアンスを確保し、コードのセキュリティを向上させるために使用するソフトウェア コンポジション分析 (SCA) ツールに組み込まれています。SCA

1　リリース3.0以前は、システム パッケージ データ交換はソフトウェア パッケージ データ交換と呼ばれていました。

ツールの主な機能には、ソースコード ベースの自動スキャン、オープンソース コンポーネントとそのライセンスの特定、既知の脆弱性の警告、そしてスキャンされたコードのSBOM生成が含まれます。

メタデータと脆弱性情報を追加する

組織は、SBOMの生成を強化するために、ソフトウェア コンポーネントに関する追加のメタデータ（バージョン番号、依存関係、ライセンス、および各ソフトウェア コンポーネントに関連する既知のセキュリティ脆弱性など）を含めるべきです。

コンプライアンスおよびセキュリティの実践に統合する

組織は、堅牢なガバナンスと効果的なリスク管理を示すために、SBOMをオープンソース ライセンス コンプライアンスおよびセキュリティの実践に組み込むことが推奨されます。

スタッフの教育とトレーニング

組織は、ライセンス コンプライアンスとセキュリティ プラクティスに携わるスタッフにトレーニングと教育を提供する必要があります。Linux Foundation は、ライセンス コンプライアンスとソフトウェア セキュリティに関する**無料のトレーニング コース**を提供しており、簡単にアクセスできます。

SBOMを定期的に更新およびレビューする

組織は、ソフトウェア コンポーネントの使用状況が変化したり、新たな脆弱性が発見されたりするたびに、SBOMを定期的に維持する必要があります。通常、組織は変更を監視し、SBOMが展開または使用されているソフトウェア資産の現在の状態を正確に反映するようにするためのプロセスを確立します。コンプライアンスとセキュリティの維持は継続的な取り組みであり、規律とこうした活動を既存の実践に組み込むことへのコミットメントが必要です。効果的な実践の一つは、すべてのソースコードに対して定められた間隔でオープンソース リスク監査を実施し、SBOMを常に最新の状態に保つことです。

SPDXに参加して協力する

組織は、SBOM標準化の取り組みを行っている業界のイニシアティブにさまざまなレベルで関与または参加するべきです。このような関与は、SBOMの実践やツールに関する最新の動向を把握し、ベストプラクティスや新たなトレンドについての洞察を得るのに役立ちます。Linux Foundation**SPDX**プロジェクトは主要なプロジェクトであり、その参加には多くの利点があります。例えば、仲間と協力してベストプラクティスを共有したり、支援ツールを共同開発したり、オープン スタンダードを広めたり、SBOMの普及を進めることに貢献したりすることが含まれます。

効果を監視し評価する

組織は、SBOMの実装の効果を監視するためのメカニズムを導入する必要があります。具体的には、SBOMポリシーに基づくライセンス コンプライアンスの追跡、セキュリティ インシデントの対応時間への影響の評価、脆弱性管理プロセスの改善の測定などが含まれます。組織はこれらの洞察を活用して、時間をかけてSBOMの実践を洗練させ、改善していくことがよくあります。

これらの推奨事項に従うことで、組織はSBOMを効果的に実装し、ソフトウェア サプライチェーン全体の透明性、ライセンス コンプライアンス、セキュリティを強化することができます。

まとめ

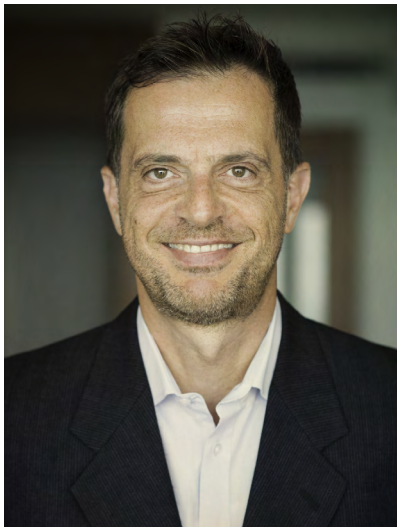
SBOMをソフトウェア開発およびガバナンス プロセスに統合することは、サイバーセキュリティとライセンス コンプライアンスにおける重要な進展です。本稿で述べたように、SBOMはソフトウェア コンポーネントの構造的かつ包括的な視点を提供し、組織がソフトウェア サプライチェーンに関連するリスクをより効果的に管理し、軽減することを可能にします。

SBOMはライセンス コンプライアンスとサイバーセキュリティに大きく貢献し、組織がソフトウェア コンポーネントを綿密に追跡・管理できるようにし、ライセンス条件の遵守を確保し、セキュリティの脆弱性に対処するための積極的な手段を提供します。SBOMを採用することで、組織は透明性を高め、セキュリティを強化し、ソフトウェア サプライチェーン全体で堅牢なコンプライアンスを確保することができ、今日の技術的な複雑性を自信とレジリエンスをもって乗り越えることができます。

謝辞

著者は、Linux Foundation ResearchのスタッフであるHilary Carter（SVP, Linux Foundation Research）およびKate Stewart（VP, Dependable Embedded Systems, Linux Foundation）に感謝の意を表します。彼らのレビューと貴重な提案は、本稿を大いに改善する助けとなりました。

著者について



Dr. **Ibrahim Haddad**は、LF AI & Data Foundationのエグゼクティブディレクターを務めており、オープンソースAIプラットフォームの進展を促進するベンダーニュートラルなエコシステムを育成しています。この役割では、開発者がオープンソースAIプロジェクトを革新、管理、スケールアップするための信頼できる持続可能な環境を確保しています。Haddadのキャリアには、Ericsson Research、Open Source Development Labs、Motorola、Palm、Hewlett-Packard、Samsung Researchなどの著名な組織での研究、技術、管理職が含まれています。彼はカナダのモントリオールにあるConcordia Universityでコンピュータサイエンスの博士号を優秀な成績で取得しました。

本訳文について

この日本語文書は、**Strengthening License Compliance and Software Security with SBOM Adoption** の参考訳として、The Linux Foundation Japan が便宜上提供するものです。英語版と翻訳版の間で齟齬または矛盾がある場合（翻訳版の提供の遅滞による場合を含むがこれに限らない）、英語版が優先されます。

この日本語文書を引用する際には、下記の一文を記載してください。
引用：Strengthening License Compliance and Software Security with SBOM Adoption参考訳（The Linux Foundation Japan 提供）

翻訳協力：小笠原徳彦

THE LINUX FOUNDATION | Research

2021 年に設立された **Linux Foundation Research** は、拡大するオープン ソース コラボレーションを調査し、新たな技術トレンド、ベストプラクティス、 オープンソース プロジェクトのグローバルな影響に関 する洞察を提供しています。プロジェクトのデータベースやネットワークを活用し、定量的・定性的手法 のベストプラクティスに取り組むことで、Linux Foundation Research は、世界中の組織にとって有益 なオープンソースの知見を提供するライブラリを構築しています。

x.com/linuxfoundation

facebook.com/TheLinuxFoundation

linkedin.com/company/the-linux-foundation

youtube.com/user/TheLinuxFoundation

github.com/LF-Engineering

この著作物を参照する際には、以下のように引用してください。
Ibrahim Haddad, “Strengthening License Compliance and Software Security with SBOM Adoption: A Definitive SBOM Guide for Enterprises,” foreword by Melissa Evers, The Linux Foundation, August 2024.