BLACKDUCK®

ガイド

「単なる文書」で終わらせない SBOM 作成のための処方箋 第二版

ソフトウェア部品表の作成、維持管理、
使用に当たって押さえておくべきポイント

例えばチョコチップ・クッキーのパッケージに記載された原材料名欄を見ると、そこには小麦粉、砂糖、バター、チョコレートチップなどの成分が記載されています。そして、このチョコレートチップもまた砂糖、チョコレート、ココアバター、無脂肪乳などの原材料からできています。

では、このチョコレートチップが使用しているココアバターに品質上の問題が見つかり、このチョコレートチップを使用しているすべての製品が自主回収の対象になったとしたらどうでしょうか。クッキーの製造業者はこのチョコレートチップに対しても責任があり、顧客が問題のあるクッキーを口にしないようにする必要があります。

ソフトウェア開発企業も同様に、脆弱性やソフトウェア・ライセンスの問題を抱えたコンポーネントが自社およびエンド・ユーザーに損害を与えないように、自社が開発したソフトウェア・アプリケーションの「原材料」を把握しておく必要があります。しかし、アプリケーションのコンポーネントが完全かつ動的に可視化されていなければ、アプリケーションの開発元も、その利用者も、そしてコンポーネントのベンダーも、問題のあるコンポーネントの所在を確実に特定することができません。

SBOM とは

ソフトウェア部品表（SBOM）とは、ソフトウェア・アプリケーションにとっての「原材料名欄」に相当するものです。この中には、オープンソース・コード、自前コード、商用コードのほか、関連するライブラリ、バージョン、パッチ・ステータスなどの情報がすべて記録されます。

SBOM を作成してソフトウェア・アプリケーションのすべてのコンポーネントをリアルタイムに可視化しておけば、攻撃者に悪用される前にリスクと脅威を特定することができます。SBOM は、開発チームがソフトウェアの品質、安全性、信頼性を評価するのに役立ちます。このように、SBOM は直接攻撃を防ぐものではなく、ソフトウェア・サプライチェーンのセキュリティ・プログラムを成功へ導く基盤としての役割を果たします。

しかし、SBOM を一度作成しただけで満足してしまっては、十分な効果は期待できません。ソフトウェアは常に変化しています。新しい依存関係が追加され、古い依存関係が更新または削除されます。脆弱性が見つかり、パッチが適用されます。SBOM は、更新作業を継続しなければすぐに古く不正確なものとなり、役に立たなくなります。包括的な SBOM を常に最新の状態に維持しておけば、組織は先手を打ってリスクを軽減し、サプライチェーンのセキュリティとコンプライアンスを徹底することができます。

誰が SBOM を必要とするのか

ソフトウェアを開発している組織、そしてソフトウェアを利用している組織は、SBOM とは無縁ではいられません。SBOM を生成することにより、そのアプリケーションの開発チームと利用者は、アプリケーションのリスクをよりよく理解するために必要不可欠な情報を手にすることができます。SBOM を出発点とすることで、セキュリティ侵害やポリシー違反の回避と対応、あるいは不具合や危険性など何らかの問題を抱えたソフトウェアの修正をより効果的に進めることができます。ソフトウェアのセキュリティと品質に懸念を抱いている組織は今、ソフトウェア開発ライフサイクル（SDLC）全体で SBOM をベスト・プラクティスの一部に取り入れるようになっています。

商用コードベースのほぼ 100% にオープンソース・ソフトウェアが使用されている現在、サプライチェーンは多くのリンクや依存関係によって、これまで以上に複雑で不明瞭になっています。リスクを軽減する唯一の方法、それはソフトウェアのすべてのコンポーネントを常に可視化した上で、リスク領域を特定して対処することです。

リスクを管理できていないと何が起こるのか

Gartner の予測では、2025 年には世界中でソフトウェア・サプライチェーン攻撃を受ける組織の割合が 45% に達すると考えられています。現在のアプリケーションは多くの依存関係や相互接続を含んでいるため、あるアプリケーションの欠陥や脆弱性が攻撃者に悪用されると、非常に多くの組織がリスクにさらされる可能性があります。過去に発生した攻撃のうち、特に有名なものをいくつか挙げてみます。

- **Log4J（2021）：**Apache Log4J の深刻な脆弱性により、攻撃者による任意のリモート・コード実行が可能となりました。この脆弱性は、NVD の CVSS スコアが最高の 10 点となっています。
- **SolarWinds（2019）：**攻撃者は、世界中で 30,000 の組織が使用する SolarWinds Orion プラットフォームに悪意のあるコードを挿入することにより、検知されることなくアカウントやユーザーになりすまして不正アクセスを成功させました。被害を受けた組織には、Fortune 500 企業数社と米国政府機関も名を連ねています。
- **Equifax（2017）：**攻撃者は、パッチ未適用の Apache Struts の既知の脆弱性を利用し、Equifax の顧客苦情ポータルから同社のシステムに侵入しました。
- **Heartbleed（2014）：**広く使用されている OpenSSL の暗号化ソフトウェアのバグにより、サーバーが RAM の内容を誤って送信し、パスワードや個人情報が漏洩した事件で、Google、Dropbox、Reddit、Facebook、カナダ歳入庁など多くの組織が被害を受けました。

ソフトウェア・サプライチェーンに対するサイバー攻撃の頻度と深刻度が高まる中、世界各国の業界や政府が多くの規制や義務を制定するようになっています。この結果、SBOM はこれまで以上に義務化が進み、今やほとんどの組織のコンプライアンス戦略において極めて重要な要素と考えられるようになっています。SBOM を必須または推奨としている規制や基準には以下のものがあります。

米国

- 大統領令 EO 14028 は、米国標準技術研究所（NIST）に対して SBOM の作成と発行に関するガイドラインを策定し、連邦政府の調達プロセスにおける SBOM の使用基準を確立するよう指示しました。
- 米国サイバーセキュリティ・社会基盤安全保障庁（CISA）は、セキュア・ソフトウェア開発向けガイダンスの中で SBOM の使用を推奨しています。
- 米国電気通信情報庁（NTIA）は、SBOM に含めるべき最小要素を定義しています。

EU

- 欧州ネットワーク情報セキュリティ庁（ENISA）が発行した「Guidelines for Securing the Internet of Things（IoT のセキュリティに関するガイドライン）」では、IoT 機器における SBOM の使用が推奨されています。

英国

- 国家サイバーセキュリティセンター（NCSC）は、組織が使用しているソフトウェア・コンポーネントのリスクの理解と脆弱性管理のために SBOM の使用を推奨しています。

オーストラリア

- オーストラリア・サイバーセキュリティ・センター（ACSC）の「Information Security Manual: Guidelines for Software Development（情報セキュリティ・マニュアル：ソフトウェア開発のためのガイドライン）」では、利用者にとってのサイバー・サプライチェーンの透明性を高めるために SBOM の使用が推奨されています。

カナダ

- カナダ通信安全保障局（CSE）の「Recommendations to Improve the Resilience of Canada's Digital Supply Chain（カナダのデジタル・サプライチェーンのレジリエンス強化に向けた勧告）」では、透明性およびセキュリティ攻撃への対応能力の向上のために SBOM の使用が強く推奨されています。

これを見ても明らかなように、SBOM を作成および維持管理することは、セキュリティとコンプライアンスの要件を満たしたソフトウェア・アプリケーションを構築するための極めて重要なベスト・プラクティスとなっています。では一体、その作業にどこから手を付けたら良いでしょうか。そして SBOM の作成が完了したらどうすれば良いのでしょうか。こうした疑問に答えるため、以下にいくつかの重要な提言をまとめました。

提言 1

SBOM の作成を 1 回限りのプロセスにしない

伝統的に、SBOM とはソフトウェア・アプリケーションに含まれるコンポーネントの目録を意味します。しかし現在では、単に静的なリストの域を超え、組織がソフトウェアの目録を作成する際に使用するプロセスも含めて SBOM と呼ぶようになっています。

ブラック・ダックは、SBOM をより広い意味で 1 つの管理システムと考えることを推奨しています。SBOM の作成と維持管理に関連するプラクティス、プロセス、アクティビティをすべて標準化し、予測可能性と再現性を持たせることが望まれます。これには、SBOM の生成をアプリケーション開発パイプラインにどのように組み込むかを特定すること、SBOM をいつ生成すべきか（リリースごと、コミットごと、など）を決定すること、SBOM の生成をビルド・ツールやリポジトリと統合して自動化することなどが含まれます。

SBOM ソリューションを検討する際に鍵となるのが、自動化です。NTIA 準拠の SBOM とするには、あらゆる情報を網羅していること、そして機械可読性を備えていることが条件となります。このレベルの詳細情報を手作業で収集するのはほとんど不可能です。また、ソフトウェア開発企業はスケーラブルなソリューションを必要としており、このような要求も手作業によるプロセスでは満たすことができません。

強力なソフトウェア・コンポジション解析（SCA）ツールなら、サードパーティのカスタム・コンポーネントを含む完全なオープンソース SBOM を容易に生成できます。SCA ツールの最も重要な特長は、SBOM の情報を継続的に提供してくれるため、リスクを最も完全な形でリアルタイムに可視化できることにあります。SDLC に直接統合して SBOM を生成できる SCA ツールを選べば、このプロセスはさらに容易になります。

提言 2
標準化されたフォーマットで SBOM を生成する

現在、SBOM の標準フォーマットには SPDX（Software Package Data Exchange）、CycloneDX、SWID（Software Identification）の 3 つがあります。

- **SPDX** は ISO で標準化されており（ISO/IEC 5962:2021）、多数のオープンソース・ツールや商用プロバイダーがサポートしています。
- **CycloneDX** は、アプリケーション・セキュリティおよびサプライチェーン・コンポーネント解析に使用する目的で OWASP コミュニティによって開発されました。
- **SWID** は NIST によってサポートされ、ISO/IEC 19770-2:2015 規格で定義されています。

ソフトウェア開発チームがソフトウェア・パッケージに含まれるコンポーネントについてのメタデータを容易に共有できるようにするには、ここに挙げた標準フォーマットのいずれかを採用することを推奨します。共通のデータ交換フォーマットを使用することにより、SBOM の生成プロセスを自動化することも容易になります。

提言 3
SBOM にはさまざまな種類があることを理解する

SBOM にはさまざまな種類があります。その中には、SDLC の複数のステージで効果的に使用できるものもあれば、特定のフェーズでしか使用できないものもあります。また、同じ種類の SBOM であっても、そこに含まれるデータは SDLC のフェーズや業界によって異なることがあります。

SBOM には以下の種類があります。

- Design（デザイン）
- Source（ソース）
- Build（ビルド）
- Analyzed（解析済み）
- Deployed（デプロイ済み）
- Runtime（実行時）

このように SBOM にはいろいろな種類があること、そして種類ごとの利点と制限を理解しておくことを強く推奨します。例えば実行時 SBOM は動的にロードされるコンポーネントや外部接続など、システムの動作中に何が使用されているのかを可視化してくれますが、その一方で、オーバーヘッドが大きく作成に時間がかかるという弱点もあります。

また、組織で使用する SBOM の種類には一貫性を持たせることを推奨します。SBOM は種類ごとの時点のデータが異なるため、SBOM 間でデータが異なることに注意が必要です。

提言 4
信頼できる配布方法を計画する

SBOM を作成できたら、次にそれをどのような方法で配布するかを検討する必要があります。SBOM を安全でない方法や十分に管理できない方法で配布すると、悪意のあるなしにかかわらず内容が改変される可能性があります。安全な配布方法を計画することは、ソフトウェア・サプライチェーンのセキュリティ、完全性、コンプライアンス、評判、透明性を保護し、リスクを軽減することにつながります。

また、個々の SBOM をアプリケーションの正しいバージョンに対応付けることも重要です。SBOM はソフトウェアの特定のリリースに紐付くため、新しいバージョンのコードをリリースするたびに新しい SBOM を作成する必要があります。組織が管理するアプリケーションが数十もあり、それぞれに複数のバージョンが存在するような場合、混乱が容易に予想されます。SBOM の基本要素として、コンポーネント名とバージョン文字列は必ず含めるようにしてください。

提言 5

業界特有の要件を満たした SBOM を作成する

以前は SBOM に何を含めるべきかについての定義が標準化されておらず、アプリケーションを構成するソフトウェア・コンポーネントについてどれだけの情報を購入者やエンド・ユーザーが必要としているかをそれぞれの組織が独自に判断していました。同様に、生成した SBOM の取り扱い方法についても、多くの組織が自分で答えを出さなければなりませんでした。

そこで、いくつかの業界では SBOM が満たすべき最小要件を規制機関が定義するようになっています。例えば、EO 14028 と NIST は米国連邦政府とそのベンダーに対して SBOM の生成と管理に関するガイドラインを定めています。また、NTIA も医療機器向けに同様の基準を定めています（ただし、この中で「…このガイダンスは業界を問わず SBOM の生成と管理に適用できるものと考えられる」とあるように、この基準は医療以外の業界にも適用できます）。また、ネットワーク機能を備えた医療機器については FDA が追加の基準を設けています。

SBOM の最小要素として NTIA が定義しているのは、次の 3 つです。

- **データ・フィールド：**サプライヤー名、コンポーネント名、コンポーネントのバージョン、その他の一意な識別子、依存関係、SBOM データの作成者、タイムスタンプなど。
- **自動化サポート：**これは、ソフトウェア・エコシステムや組織の垣根を越えて SBOM を活用できるようにする上で重要な要素です。これを可能にするには、SBOM を 3 つの標準フォーマット（SPDX、CycloneDX、SWID）のいずれかで伝達する必要があります。
- **プラクティスとプロセス：**SBOM 作成の頻度、SBOM の深さ、既知の未知、配布と配信、アクセス管理、ミスの許容など。

医療機器のソフトウェアに関しては、完全性と正確性に対するニーズの高まりを理由に FDA が追加の要素を要求しています。FDA 準拠の SBOM には、NTIA が定義した標準のデータ・フォーマットに加え、サポート・レベル、サポート終了日、既知の脆弱性に関する情報も含める必要があります。これらの追加要素は、オープンソース・プロジェクトだけでなくアプリケーションに含まれるサードパーティ / 商用コンポーネントにも広く適用されます。

自動車業界では、ソフトウェアのライセンスに関する情報を SBOM に含めることが ISO 5230/OpenChain によって要求されています。

ここで強調しておきたいのは、コードベースにツールを適用するだけでは、要件を十分に満たした SBOM を生成できないという点です。SBOM は、自社がビジネスを展開している業界に特有の要件をすべて満たしている必要があります。この確認を怠ると、罰則、監査、あるいは市場での認可停止といった結果を招く可能性があります。政府と取引のあるメーカーは、調達契約やパートナーシップを失い、サプライチェーンの混乱や商機の逸失を引き起こす危険があります。また、SBOM の要件を遵守していないと組織の評判に傷を付け、顧客やパートナー、規制機関からの信用を失うことにもなりかねません。

提言 6

SBOM にはすべてのコードを含める

「SBOM にはオープンソースおよびサードパーティ・ソフトウェア・コンポーネントだけを記録すれば良い」というのは、よくある誤解の 1 つです。冒頭に挙げたたとえで言えば、これはチョコチップ・クッキーの原材料名欄にチョコレートチップの原材料だけを記載するようなものです。SBOM を網羅的なものとするには、ソフトウェア・アプリケーションの「すべての」コンポーネントを含める必要があります。

SBOM には以下のものを含めるようにします。

- 自前のコード
- 商用ソフトウェア開発キット
- 商用プライベート・ライブラリ
- 受託開発ソフトウェア
- 商用オフザシェルフ・コード
- オープンソース・ソフトウェア

「何事も少ない方が良い」という考え方は、SBOM には当てはまりません。さまざまなソースから要素を追加することに比べれば、特定の顧客向けに要素を削除するのは簡単なことです。例えば、FDA は SBOM に多くのフィールドを含めるように要求していますが、病院によってはその一部しか必要としないこともあるでしょう。そのような場合でも、まずは包括的かつ最新の SBOM を作成することを優先してください。そこから不要な情報を削除すれば、特殊なケースにも容易に対処できます。

提言 7

SBOM を使って何をするのかを明確にする

SBOM を生成できたとして、それをどのように活用するのでしょうか。SBOM をどのようにしてリスク領域に対応付けるのでしょうか。ソフトウェア・サプライチェーンを統制・管理するツールとして SBOM をどのように活用するのでしょうか。これらの質問に答えることにより、SBOM のメリットを最大限に引き出し、サプライチェーンのリスク低減、顧客からの信頼の向上、およびコンプライアンスの達成につなげることができます。

このガイドに示した 7 つの提言に従って SBOM を生成、管理、使用することで、セキュリティとコンプライアンスの要件を満たしたソフトウェア・アプリケーションの構築が可能となり、SBOM を使用して攻撃者に悪用される前にリスクと脅威を特定できるようになります。しかし、SBOM を一度作成しただけで満足してしまっては、十分な効果は期待できません。ソフトウェアは常に変化しています。新しい依存関係が追加され、古い依存関係が更新または削除されます。脆弱性が見つかると、パッチが適用されます。SBOM は、更新作業を継続しなければすぐに古く不正確なものとなり、役に立たなくなります。

SBOM の生成、管理、使用についての詳細はこちら

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社

www.blackduck.com/jp