Source

NTIA Multistakeholder Process on Software Component Transparency

> SBOM at a Glance (Last revised: 2021-04-27)
> https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdf

---

SBOM at a Glance

Last revised: 2021-04-27

翻訳：一般社団法人JPCERTコーディネーションセンター

本資料について / Purpose

本資料は、Software Bill of Materials （以下、SBOM）の活用方法や参考文献、また、エコシステムに存在するソフトウェアコンポーネントの透明性確保においてSBOMが果たす重要な役割等について概説する資料です。 SBOMを利用することで、ソフトウェアサプライチェーンにおけるさまざまな問題に対して、影響の有無や必要な対応などを素早く正確に判断できるようになることが期待されます。

SBOMとは何か? / What is an SBOM?

SBOMとは、ソフトウェアコンポーネントやそれらの依存関係の情報も含めた、機械処理可能なインベントリーです。ソフトウェアコンポーネントやその依存関係をすべて表現している場合もあります。また、どこの部分が欠けているかという情報が含まれている場合もあります。OSSだけではなくプロプライエタリソフトウェアに活用することもでき、広く一般に公開するほか関係者だけに提示するという使用方法もあります。[1]

SBOMには、ソフトウェアコンポーネントを確実に識別するための基本アトリビュート情報（Baseline Component情報）を含めてください。ソフトウェア開発プロセスの中でソフトウェア自体と一緒にSBOMを作成することが最も効率的です。

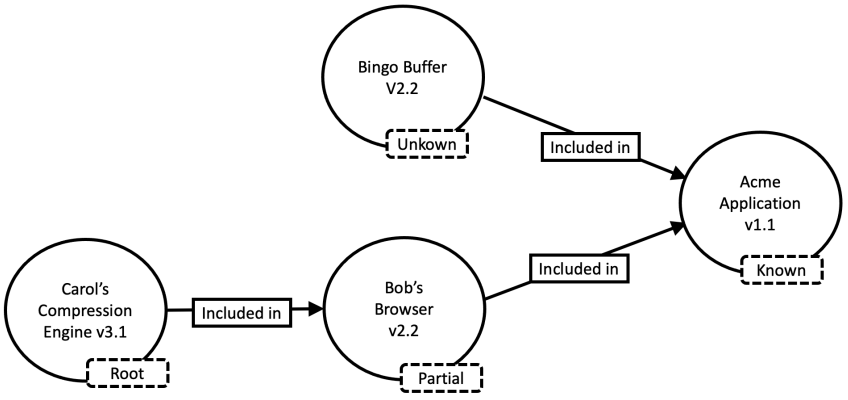

図: コンポーネント間の依存関係を記述したSBOMツリーの例

SBOMのユースケースや利点について / Benefits and Use Cases

ソフトウェアの開発（Produce）、選定（Choose）、そして運用（operate）それぞれの場面において、SBOMのユースケースや利点は数多く存在します[2]。

SBOMのユースケースとしては、ソフトウェア開発やソフトウェアサプライチェーン情報・脆弱性情報の管理、また、そして製品調達や品質確保などがあります。SBOMの利点としては、コスト削減に加え、セキュリティ対応における多くのリスクの削減、ライセンス違反やコンプライアンス違反などのリスクの削減が期待できます。

これらユースケースや利点について、現在、医療関係者によって実証実験が行われており[3]、米国の自動車業界ならびに電力業界にも同様の試みが広がっています。

Baseline Component情報 / Baseline Component Information

ソフトウェアコンポーネントとそれらの関係性を明確に識別するために、右の図にあるBaseline Component情報（SBOMを構成する必要最低限の情報）を組み合わせて使用してください。Baseline Component情報だけでは対応できないユースケースも想定されますので、必要に応じてそれ以外の情報も追加してください。

Baseline Component Information
Author Name（開発者）
Supplier Name（会社名）
Component Name（コンポーネント名）
Version String（バージョン）
Component Hash（コンポーネントのハッシュ値）
Unique Identifier（識別子）
Relationship（関係）

データフォーマットとツールについて / Machine-Readable Formats and Tools

SBOMを有効活用するためには、機械処理と自動化、また、エコシステムに存在する複数の組織にまたがる共通運用性を確保することが非常に重要です。そのためには、共通のデータフォーマットやスキームが必要です。

以下の3つのデータ形式は、ソフトウェアコンポーネントの識別やメタデータの伝達に適しており、Baseline Component情報も全て含めることが可能です[4]。これらの形式のデータを生成・使用・変換するためのツールが存在します[5]。

データ形式	仕様	ツール
SPDX	https://spdx.github.io/spdx-spec/	https://tiny.cc/SPDX
CycloneDX	https://cyclonedx.org	https://tiny.cc/CycloneDX

データ形式	仕様	ツール
SWID	ISO/IEC 19770-2:2015	https://tiny.cc/SWID

SBOMの共有方法について / Sharing and Exchanging

エコシステムには多様なニーズが存在します。そのため、SBOM情報を共有する方法は一つではありません。各状況に合わせて共有方式を検討してください[6]。その際、既存のプロセスにSBOM共有手順を追加する形を取ることで、組織間における運用上のずれの発生ならびに新たなツール導入の必要性を最低限に抑え、相互運用を促進しやすくなると考えられます。

さらに詳しく / Learn More

SBOMに関するより詳しい情報については、www.ntia.gov/sbomを参照してください。追加の入門資料としてSBOM Overview（2ページ版）[7] やSBOM FAQ[8]、また、解説ビデオ[9]も用意されています。SBOMデータの生成や変換には、SwiftBOM[10]というツールがあります。SBOMに関する議論が行われているマルチステークホルダープロセスへの参加を希望される方は、www.ntia.gov/SoftwareTransparencyを参照してください。

日本国内におけるSBOMの状況について、また日本語でのご質問等がありましたら、本資料を翻訳したJPCERTコーディネーションセンター（vuls@jpcert.or.jp）にご連絡ください。

参考情報 / References

1. Framing Software Component Transparency: Establishing a Common Software Bill of Material（SBOM）
   https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf
2. Roles and Benefits for SBOM Across the Supply Chain
   https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf
3. .Software Component Transparency: Healthcare Proof of Concept Report
   https://www.ntia.gov/files/ntia/publications
   /ntia_sbom_healthcare_poc_report_2019_1001.pdf
4. Survey of Existing SBOM Formats and Standards
   https://www.ntia.gov/files/ntia/publications/ntia_sbom_formats_and_standards_whitepaper_-_version_20191025.pdf
5. SBOM Tool Classification Taxonomy
   https://www.ntia.gov/files/ntia/publications/ntia_sbom_tooling_taxonomy-2021mar30.pdf
6. Sharing and Exchanging SBOMs
   https://www.ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf
7. Two-Page SBOM Overview
   https://www.ntia.gov/files/ntia/publications/sbom_overview_20200818.pdf
8. SBOM FAQ
   https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf
9. Explainer Videos
   https://www.youtube.com/playlist?list=PLO2lqCK7WyTDpVmcHsy6R2HWftFkUp6zG
10. SwiftBOM - SBOM Generator Tool
    https://democert.org/sbom/