日立ソリューションズオンラインセミナー
「OSSマネジメントフォーラム 2023」(2023/12/19 - 21)
講演資料

HITACHI
Inspire the Next

経済産業省発行

ソフトウェア管理に向けたSBOMの導入に関する手引(Ver. 1.0)概要および解説

株式会社 日立ソリューションズ

はじめに：日立ソリューションズが提供するSBOMのソリューションについて

HITACHI
Inspire the Next

日立ソリューションズの

ソフトウェア部品管理ソリューション

経験豊富なコンサルタントがお客様のSBOM導入・活用をサポート

SBOM教育

SBOMの基礎知識から作成・活用の方法までを網羅した実践的な教育

SBOM導入支援/ SBOM活用支援

お客様がSBOMを作成し、効果的に活用する仕組みづくりを支援するサービス

SBOMガイドライン策定支援

SBOMに関するガイドラインをはじめ、各種ルールの策定を支援するサービス

SBOM作成代行

お客様に代わってソフトウェアを調査し、SBOMの作成を代行するサービス

SBOM動向調査

お客様に代わってSBOMに関する業界動向などを調査するサービス

特定業界向け SBOM支援

自動車・医療など、特定の業界に特化したSBOMに関するサービス

先進的なSBOM生成・管理ツールを複数ラインアップ

Black Duck	MEND (formerly WhiteSource)	FOSSA	insignary clarity	CYBELLUM	その他ツール 独自ツール
Black Duck	Mend社のソフトウェアコンポジション解析ツール (旧White Source)	FOSSA	Insignary Clarity	Cybellum	

はじめに：日立ソリューションズについて

HITACHI
Inspire the Next

1 SBOMとOSS管理に関する豊富な経験と実績

2 SBOMツールに関するノウハウと販売実績

3 グローバルおよび国内のOSSコミュニティや団体への参画

製造業や自動車業界大手
を中心に

60社以上

のお客さまをご支援した実績

多くのお客様から

SBOMのことなら
日立ソリューションズ

とご評価をいただいています

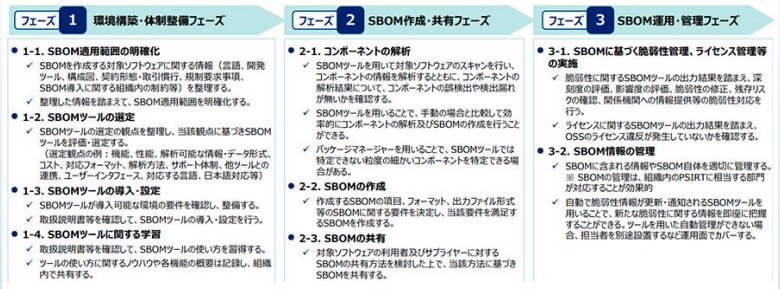
HITACHI
Inspire the Next

経済産業省様のSBOM実証実験、SBOM導入手引の策定に関するご支援実績

SBOM普及の本格化に向けた経済産業省の実証実験で、
参加企業へのツール導入を支援

株式会社三菱総合研究所は、経済産業省のSBOM＊の普及に向けた実証実験を推進。実証実験の再委託先として、日立ソリューションズは、参加企業へのツール導入を支援し、SBOM手引書に対するレビューを行いました。

＊SBOM：Software Bill of Materials（ソフトウェア部品表）



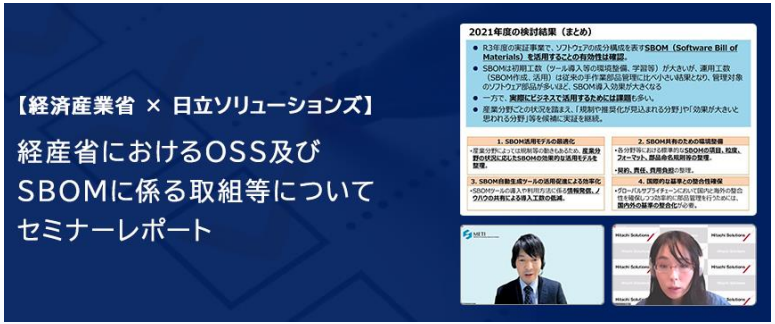
https://www.hitachi-solutions.co.jp/sbom/case01/

はじめに：日立ソリューションズのWebサイトについて

HITACHI
Inspire the Next

セミナーやブログなどで
お客さまに役立つ技術情報を発信

https://www.hitachi-solutions.co.jp/sbom/



はじめに：日立ソリューションズのSBOM導入支援について

HITACHI
Inspire the Next

経産省のSBOM導入手引のシナリオに沿ったSBOM導入のご支援が可能です

フェーズ	ステップ	実施概要
環境構築・体制整備フェーズ	SBOM適用範囲の明確化	SBOMの対象とするソフトウェアの情報（開発言語、契約形態、規制要求事項、社内の制約等）を整理して、SBOM適用範囲を明確化する。
	SBOMツールの選定	対象ソフトウェアの開発言語や組織内の制約を考慮したSBOMツールの選定の観点を整理し、当該観点に基づきSBOMツールを評価・選定する。
	SBOMツールの導入・設定	ツールの取扱説明書やREADMEファイル等を確認して、SBOMツールの導入・設定を行う。
	SBOMツールに関する学習	ツールの取扱説明書やREADMEファイル等を確認して、SBOMツールの使い方を習得する。
SBOM作成・共有フェーズ	コンポーネントの解析	対象ソフトウェアのコンポーネントを解析するとともに、解析結果について、誤検出や検出漏れが無いかを確認する。
	SBOMの作成	作成するSBOMの項目、フォーマット、出力ファイル形式等のSBOMに関する要件を決定し、当該要件を満足するSBOMを作成する。
	SBOMの共有	対象ソフトウェアの利用者及び納入先に対するSBOMの共有方法を検討した上で、必要に応じて、SBOMを共有する。
SBOM運用・管理フェーズ	SBOMに基づく脆弱性管理、ライセンス管理等の実施	脆弱性やライセンスに関するSBOMの情報を踏まえ、適切な脆弱性対応やライセンス管理対応を講じる。
	SBOM情報の管理	SBOMに含まれる情報やSBOM情報自体を適切に管理する。

お気軽にお問い合わせください！

日立ソリューションズ　SBOM

https://www.hitachi-solutions.co.jp/inquiry/products/form/?id=sbom

目次

§1. 背景と目的

HITACHI
Inspire the Next

背景

- 産業に占めるソフトウェアの重要性の高まり(「モノづくりのソフトウェア化」、「Software Defined」)
- ソフトウェアを利活用した製品の安心・安全の担保
  ➡ **脆弱性の確実な管理** (出荷後や保守・サポート終了後に発見された脆弱性への対処)
- 脆弱性管理における課題
  - ✓ **どのようなソフトウェアが含まれているのか把握できない**
    (サプライチェーンの複雑化、OSS利用の一般化による)
  - ✓ 資産台帳管理の場合、**間接的な脆弱性の影響を検知できない**
    (上位のコンポーネントのみが資産管理の対象)

SBOMの活用に注目が集まっている

SBOM(Software Bill of Materials : ソフトウェア部品表)
・・・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一覧

HITACHI
Inspire the Next

Linux Foundation Research：グローバル412の組織を対象に調査(2021年第3四半期)

調査対象組織の
47%
がSBOMを導入済

2023年の導入率は
88%
に達すると推測

2022年には
78%
がSBOM導入見込み

(The Linux Foundation / The State of Software Bill of Materials (SBOM) and Cybersecurity Readiness)

HITACHI
Inspire the Next

経済産業省における取組み

- 2019年に「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース」発足
  ➡ SBOMも含めたソフトウェア管理手法等に関して幅広く議論
- 2021年より、SBOM導入に向けた実証事業を推進
  ➡ **SBOM導入にかかるコストや効果の評価を複数の産業分野で実施**

実証参加企業の分野

2021年度

- 自動運転システム開発向け検証基盤ソフトウェア

2022年度

- 医療機器分野　：歯科用CT
- 自動車分野　：自動車ヒーターコントローラー
- ソフトウェア分野　：ネットワーク脅威検知ソフト等

HITACHI
Inspire the Next

実証を通じて確認されたSBOMのメリット・効果

① 手動管理と比べて、**SBOM活用時は管理工数が軽減**

② 脆弱性発見時の**影響有無特定までのリードタイム短縮、脆弱性残留リスクの低減、脆弱性対応工数の低減**

③ **ライセンス違反リスクの低減**や**ライセンス管理工数の低減**

SBOMツールを活用することで、更に得られる効果

- 初期工数は大きいものの、**SBOMツールを活用することで負担軽減**
- 有償SBOMツールを活用することで**OSS間の依存関係や再帰的な利用も効率的に検出・管理**できる
- より**効率的なライセンス管理が可能**になる(各ライセンスの内容表示や注意が必要なライセンスの警告等、コンプライアンス遵守のための機能が活用できる)

HITACHI
Inspire the Next

実証を通じて確認されたSBOMの課題

① 対象とするソフトウェア・システムの全体構成が把握できていない場合、SBOMツールの適用範囲を適切に設定できず、効果的なリスク管理が実施できない。

② SBOMツールを導入するための環境整備や学習に工数を要する。

③ 無償のSBOMツールは、環境整備や学習にあたっての情報が不足しており、導入に大きな工数を要する。また再帰的に利用される部品が十分に検出できない、取扱い可能なSBOMフォーマットに制限がある、ライセンスの検知漏れが発生する等、利用時に注意すべきことが多い。

④ SBOMツールを単に適用しただけでは、対象ソフトウェアに含まれるコンポーネントの検知漏れが発生する場合がある。

⑤ SBOMツールの出力結果について、コンポーネントの誤検知や検出漏れ、脆弱性情報の誤り等が発生する場合があるため、出力結果の精査が必要となる。

⑥ サードパーティのコンポーネントについて、内部の構成や活用されている技術を把握できない状況でSBOMツールの出力結果を精査することになるため、精査にかかる工数が大きくなる。

⑦ 現状では、異なるSBOMツールで生成したSBOMを読み込んで脆弱性管理に活用することができるSBOMツールが少なく、異なるSBOMツール間でのSBOMの相互共有が困難である。

⑧ 特定されたコンポーネントの脆弱性に対する対応要否、対応優先度の判断が困難である。

HITACHI
Inspire the Next

本手引作成の目的

- SBOMの概要やSBOM導入のメリット等、SBOMに関する基本的な情報を提供
- SBOM作成に向けた環境構築・体制整備、作成・共有、運用・管理に至る一連のプロセスを提示
  ➡ **ソフトウェア管理に向けたSBOMの作成・共有・運用・管理に関する様々な課題の解決**
- 各フェーズにおける主な実施事項やSBOM導入に当たって認識しておくべきポイントを提示
  ➡ **企業における効率的・効果的なSBOM導入を支援**

補足

- 本手引は**主にソフトウェアサプライヤーを対象としたもの**であるが、ソフトウェアを調達して利用する企業等においても、活用・参照することが可能
- SBOMはソフトウェア管理の一手法であるため、**作成することが目的ではなく、SBOMを用いたソフトウェアの適切な管理が重要**となることに留意が必要
- 「OSSの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」も参照のこと

HITACHI
Inspire the Next

経済産業省の事例集：日立製作所「製品化の過程における徹底したOSS管理とOSSに関わる人材の育成」

OSS の利活用及びそのセキュリティ確保に向けた
管理手法に関する事例集

経済産業省　商務情報政策局
サイバーセキュリティ課

令和４年８月１日

日立製作所の事例

② 商用ツールの活用による OSS の効果的な把握

日立製作所の IT セクターにおいては、開発初期段階における OSS のライセンス調査や、開発委託品[53]及びリリース前の製品に未認識の OSS が含まれてないかチェックする目的で商用ツールを導入している。これにより、管理システムへの登録だけでは把握しきれなかった OSS によるライセンス違反を防止している。また、商用ツールによって検知された OSS は、前述の管理システムに自動登録される。なお、製品リリース後のソフトウェア脆弱性対応においても商用ツールの機能（脆弱性発生時のメール通知機能）が活用されている。

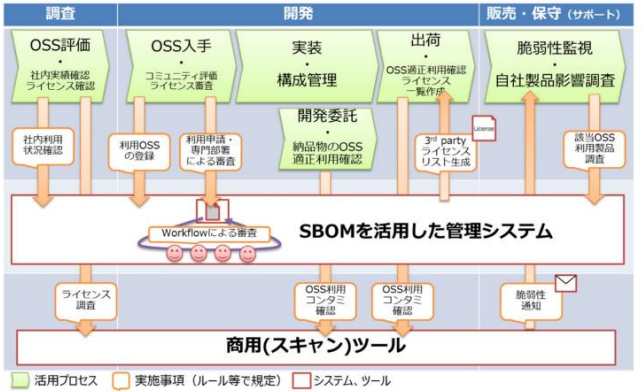


図 4.4-1 開発プロセスにおける管理システム及び商用ツールの活用状況[54]

（経済産業省　商務情報政策局　サイバーセキュリティ課 / OSSの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集）

§1.3 主な対象読者

HITACHI
Inspire the Next

本手引作成の主な対象読者

- ソフトウェアサプライヤーにおける開発・設計部門や製品セキュリティ担当部門(PSIRT等) 等の**ソフトウェアセキュリティに関わる部門**
  - ➡ SBOM導入に向けたプロセス、主な実施事項およびSBOM導入にあたって認識しておくべきポイントを記載
- ソフトウェアサプライヤーの**経営層**
  - ➡ SBOM導入に関する意思決定のためのSBOMの効果・メリットの情報、SBOMに関する誤解と事実を記載

補足

- **主にSBOM初級者向け**の内容
  - ✓ ソフトウェアにおける脆弱性管理に課題を抱えている組織
  - ✓ SBOMという用語は聞いたことがあるが具体的な内容やメリットは把握できていない組織
  - ✓ SBOMの必要性は理解しているが、導入に向けた取組内容が認識できていない組織など
- ライセンス管理に関する内容は**組織の法務・知財部門で活用できる**
- ソフトウェアサプライヤーに限らず、**ソフトウェアを調達して利用する企業においても一部活用可能**

§1.4 主な対象ソフトウェア、 §1.5 活用方法

本手引の主な対象ソフトウェア

- パッケージソフトウェアや組込みソフトウェアを対象としている

本手引の活用方法

- SBOMに関する基本情報を認識する
- SBOM導入に向けたプロセスを確認する
  - ➡ 各ステップにおける主な実施事項及びSBOM導入に当たって認識しておくべきポイントを確認する

§1.6「本手引のサマリー」は
経営層の課題認識を促す目的で活用可能

§2. SBOMの概要

HITACHI
Inspire the Next

SBOMとは

- 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一覧**
- ソフトウェアに含まれるコンポーネントの名称やバージョン情報、コンポーネントの開発者等の情報が含まれる
- **OSSだけではなくプロプライエタリソフトウェアに関する情報も含める**ことができる
- ソフトウェアサプライチェーンで**SBOMを相互共有することで、透明性が高まる**
  - ➡ 特に、**コンポーネントの脆弱性管理の課題に対する一つの解決策として期待されている**

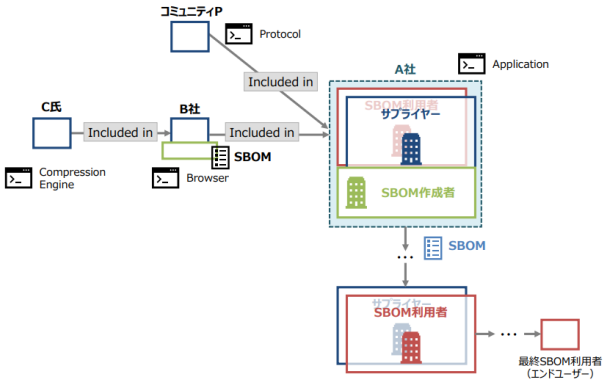


図 2-1 簡易シナリオにおけるプレイヤー間の関係性

表 2-1 簡易シナリオにおける SBOM の概念的イメージ

ID	サプライヤー名	コンポーネント名	コンポーネントのバージョン	その他の一意の識別子	依存関係	SBOM作成者	タイムスタンプ
1	Company A	Application	1.1	234	Primary	Company A	05-09-2022 13:00:00
2	Company B	Browser	2.1	334	Included in #1	Company B	04-18-2022 15:00:00
3	Mr. C	Compression Engine	3.1	434	Included in #2	Company A	05-09-2022 13:00:00
4	Community P	Protocol	2.2	534	Included in #1	Company A	05-09-2022 13:00:00

※依存関係も含めて管理することが重要

HITACHI
Inspire the Next

SBOM導入のメリット

メリット区分		メリット項目	主な内容
脆弱性管理のメリット	直接的メリット	脆弱性残留リスク低減	脆弱性情報を収集しSBOM情報と突合して脆弱性を検出 ➡ **ソフトウェアにおいて脆弱性が残留するリスクを低減**
		脆弱性対応期間短縮	SBOMツール等の利用により新たな脆弱性をリアルタイムで検出し影響を判断 ➡ **初動期間の短縮**
		脆弱性管理コスト低減	SBOMツールを用いた自動管理 ➡ (手動と比較して)**管理コストを低減**
	間接的メリット	製品価値・企業価値向上	製品に含まれる脆弱性の低減や脆弱性対応の迅速化 ➡ **製品や企業価値の向上**
		サイバー衛生向上 (Cyber Hygiene)	脆弱性の少ない製品の増加 ➡ **サイバー空間全体のセキュリティ向上**(踏み台リスクの低減)
ライセンス管理のメリット	直接的メリット	ライセンス違反リスク低減	OSSの特定漏れ低減 ➡ **ライセンス違反リスクの低減**
		ライセンス管理コスト低減	SBOMツールを用いた自動管理 ➡ (手動と比較して)**管理コストを低減**
	間接的メリット	製品価値・企業価値向上	製品のライセンス違反リスクの低減 ➡ **製品や企業価値の向上**
開発生産性向上のメリット	直接的メリット	開発遅延阻止	コンポーネントに関する問題を早期に特定 ➡ **開発遅延の発生防止**
		開発コスト低減	コンポーネントに関する問題を早期に特定 ➡ **対応コストの低減**
		開発期間短縮	コンポーネント選定時に類似製品のSBOM情報を活用 ➡ **選定工数の削減**

ライセンスも含めてSBOMで管理することで、ライセンス違反リスクの低減、管理コストの低減、財務リスクから組織を保護できる

51%が「開発者がより広範で複雑なプロジェクト間の依存関係を理解しやすくなる」メリットを感じている(LF Researchより)

HITACHI
Inspire the Next

SBOM導入のメリット (脆弱性管理のメリット)

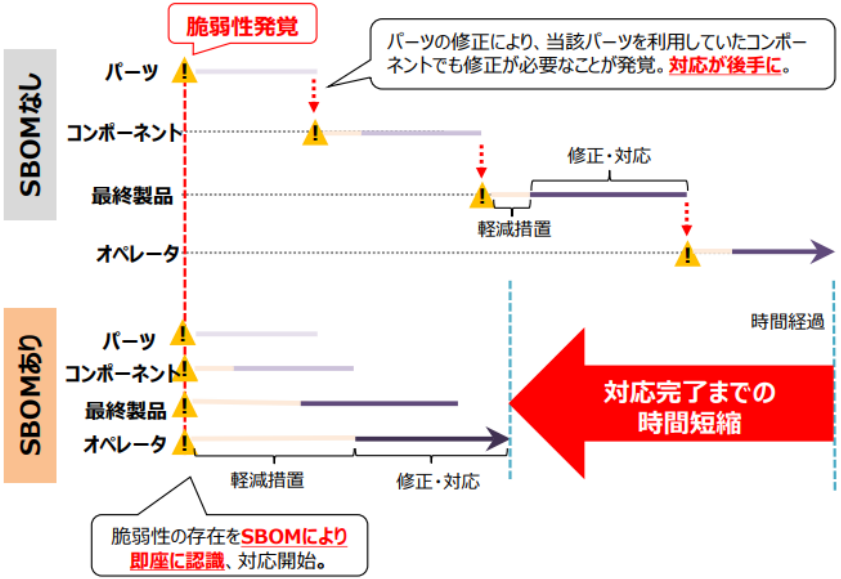


図 2-3 SBOM 導入による脆弱性対応期間短縮のメリット

※ 関係する組織間でSBOMや脆弱性の情報を共有することで、
脆弱性対応の効率化、対応期間の短縮化が可能になる

仮定
- 対象ソフトウェアに含まれるコンポーネント：80個
- 工数単価：¥10,000円/時

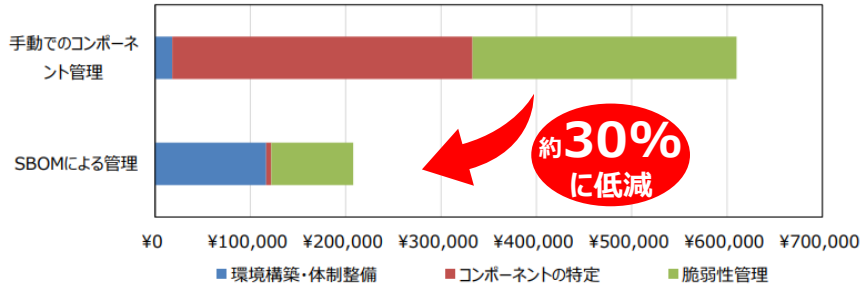


図 2-4 SBOM 管理による脆弱性管理コストの低減結果
（医療機器分野における 2022 年度の実証結果より）[9]

※ SBOMツールを活用する場合、
脆弱性管理にかかるコストを大幅に削減できる

HITACHI
Inspire the Next

NTIA※が定める「最小要素」の定義

※ National Telecommunications and Information Administration

カテゴリー名称	概要	定義
データフィールド (Data Fields)	各コンポーネントに関する基本情報を明確化すること	以下の情報をSBOMに含めること。 ● **サプライヤー名 (Supplier Name)** ● **コンポーネント名 (Component Name)** ● **コンポーネントのバージョン (Version of the Component)** ● **その他の一意な識別子 (Other Unique Identifiers)** ● **依存関係 (Dependency Relationship)** ● **SBOM作成者 (Author of SBOM Data)** ● **タイムスタンプ (Timestamp)**
自動化サポート (Automation Support)	**SBOMの自動生成や可読性等の自動化をサポートすること**	SBOMデータは**機械判読可能かつ相互運用可能なフォーマット**を用いて作成され、共有されること。 現状では、国際的な議論を通じて策定された、SPDX、CycloneDX、SWIDタグを用いること。
プラクティスとプロセス (Practices and Processes)	SBOMの要求、生成、利用に関する運用方法を定義すること	SBOMを利活用する組織は、以下の項目に関する運用方法を定めること。 ● SBOMの作成頻度 ● SBOMの深さ ● 既知の未知 ● SBOMの共有 ● アクセス管理 ● 誤りの許容

(NTIA, The Minimum Elements For a Software Bill of Materials (SBOM))

§2.4 SBOMフォーマットの例

HITACHI
Inspire the Next

代表的なSBOMフォーマット

日立ソリューションズ独自作成スライド
(経済産業省SBOM導入の手引きには掲載されていません)

#	項目	SPDX	CycloneDX	SWID
1	正式名称	Software Package Data Exchange	CycloneDX specification	Software Identification(SWID) Tags
2	仕様	SPDX Specification v2.3 (2022/11/3リリース)	CycloneDX 1.5 (2023/6/23リリース)	-
3	標準化	ISO/IEC 5962:2021 (SPDX v2.2.1)	-	ISO/IEC 19770-2:2015
4	サポート団体	The Linux Foundation SPDX Group	OWASP Foundation	-
5	起源	2010年(FOSSBazaar)	2017年	2006年
6	ファイル形式	RDF, XML, xlsx, tag-value, JSON, YAML	XML, JSON, Protocol Buffers(protobuf)	XML
7	備考	• **SPDX License List (Identifier) によりライセンスを一意に特定** • **ライセンス情報の表現に強い** • **SPDX Lite**というサブセットがある	• **セキュリティ情報の表現に強い** • 汎用性のあるBOM規格であり、SaaSBOMやHBOMなどもサポート	• ソフトウェアのライフサイクルに沿ってSBOMを管理することができる

共通的なフォーマットを用いる目的：

- **組織内の管理の効率化**
- **組織を越えてSBOMを共有する際の相互運用性の向上**

➡ **ソフトウェアサプライチェーンの透明性向上に寄与する**

HITACHI
Inspire the Next

NTIA「最小要素」との対応

#	NTIA 最小要素	SPDX	CycloneDX	SWID
1	サプライヤー名 (Supplier Name)	PackageSupplier	component/supplier/name	<Entity> @role(tagCreator) @name
2	コンポーネント名 (Component Name)	PackageName	component/name	<SoftwareIdentity> @name
3	コンポーネントのバージョン (Version of the Component)	PackageVersion	component/version	<SoftwareIdentity> @version
4	その他の一意の識別子 (Other Unique Identifiers)	DocumentNamespaceと SPDXIDの組合せ、ExternalRef	serialNumber、 component/cpe	<SoftwareIdentity>@tagId
5	依存関係 (Dependency Relationship)	Relationship (DESCRIBES; CONTAINSによる表現)	dependencies/dependency ref	<Link> @rel @href
6	SBOM作成者 (Author of SBOM Data)	Creator	metadata/authors/author/name	<Entity> @role(softwareCreator) @name
7	タイムスタンプ (Timestamp)	Created	metadata/timestamp	<Meta> @timestamp

HITACHI
Inspire the Next

NTIA「SBOM Myths vs. Facts」の内容

1	誤解	SBOMは攻撃者を支援する
	事実	SBOMが攻撃に利用される可能性はあるものの、「攻撃者からの防御」のメリットの方が大きい。攻撃者にとって、SBOMによる情報の効果は限定的であり、一般的に攻撃者はSBOMを必要としない。
2	誤解	SBOMだけでは有用・実用的な情報を得ることができない
	事実	ソフトウェアに対する攻撃を受けた時、SBOMにより、攻撃の影響を受けているか、攻撃の影響範囲はどこかを容易に判断できる。
3	誤解	SBOMは公開しなければならない
	事実	SBOMを公開する必要はなく、SBOM作成者やサプライヤーの判断で共有方法を判断することができる。
4	誤解	SBOMは知的財産や企業秘密を露呈する
	事実	SBOMには特許やアルゴリズム、ソースコードは含まれておらず、知的財産を公開するものではない。SBOMは単なる「材料の一覧」であり、特許やアルゴリズムのような「レシピ」ではない。
5	誤解	SBOMの導入を支援するプロセスは存在しない
	事実	ソフトウェア構成分析ツールは、一部の分野では、10年以上にわたって企業内で使用されてきた実績がある。ソフトウェアの透明性に関しては、NTIAの活動、大統領令、SBOMフォーマットの標準化等の活動が進んでいるほか、一部の分野では、ソフトウェアの透明性について5年以上にわたって議論や実証の取組みが進められており、他分野での導入をサポートしている。

(NTIA, SBOM Myths vs. Facts)

HITACHI
Inspire the Next

日本における実証(2022年)等を通じて明らかになった誤解と事実 ①

1	誤解	対象ソフトウェアが直接利用しているコンポーネントのみをSBOMの管理対象とすればよい
	事実	対象ソフトウェアが直接利用しているコンポーネントだけでなく、そのコンポーネントが**再帰的に利用するコンポーネントについても把握しないと、脆弱性対応が不十分となる可能性**がある。(「SBOMの深さ」については有識者による議論が進行中)
2	誤解	SBOM作成に用いるSBOMツールの選定において、特に留意すべき点はない
	事実	マニュアルやサポートの有無に起因する習得コスト、ツールのサポート範囲や性能などが異なるため、自社のSBOM導入の目的を踏まえて使用するツールを選定する必要がある。
3	誤解	SBOMツールを活用することで、対象ソフトウェアに含まれるコンポーネントを完全に特定することができる
	事実	SBOMツールにより効率化できるが、コンポーネントの誤検出や検出漏れの可能性があるため、**SBOMツールにより出力されたSBOMをレビューする工程が必要**である。ツールのサポート範囲(ランタイムライブラリの検出可否など)にも注意が必要。
4	誤解	SBOMツールが出力したすべての脆弱性に対応する必要がある
	事実	影響を受けない脆弱性もあるため、影響範囲、リスクの評価結果、対応に要するコスト等を踏まえ、**優先度を踏まえた脆弱性対応が必要**。手動でのSBOM管理の場合は膨大な管理コストを要する可能性がある。
5	誤解	作成するSBOMのコンポーネントの粒度はサプライチェーン全体で共通化し、必要なコンポーネント情報だけを保持するべきである
	事実	現状では、JVN や米国 NVD のような脆弱性情報データベースにおける「影響を受けるソフトウェア」の粒度が体系化されていないため、コンポーネントの粒度を限定すると脆弱性の特定で漏れが生じる可能性がある。

(次ページに続く)

HITACHI
Inspire the Next

日本における実証(2022年)等を通じて明らかになった誤解と事実 ②

6	誤解	SBOMの対象はパッケージソフトウェアや組込みソフトウェアのみである
	事実	**ソフトウェアに限らず、ITシステムもSBOMの対象。**なお、コンテナイメージに対するSBOM、SaaSソフトウェアに対するSBOM、クラウドサービスに対するSBOM等のオンラインアプリケーションに対するSBOMの議論も米国を中心に行われている。
7	誤解	SBOMのフォーマットとして、SPDX、CycloneDX、SWIDタグの3つのフォーマットのみが認められており、独自フォーマットに基づくSBOMは認められない
	事実	NTIAによれば、独自フォーマットであっても定義に合致する場合はSBOMとみなすことができる。ただし、SBOMの最小要素として「自動化サポート」が位置づけられており、まだ自動処理により効率化が図られることから、**可能な限り、自動処理可能なフォーマットの採用を検討することが望ましい。**

§3. SBOM導入に関する基本指針・全体像

§3.1 SBOM導入における基本方針

HITACHI
Inspire the Next

SBOM導入に先立ち実施しておくべきこと

- SBOMを作成する**ソフトウェアの範囲を決定する**
- SBOM導入により**解決したい自組織の課題とSBOM導入の目的を明確化する**

備考

具体例①

膨大な数のコンポーネントが存在する大規模製品について、コンポーネントの依存関係も含めたSBOMを作成し、共有したい

➡ 有償のSBOMツールを用いてSBOMを作成・管理する

具体例②

コンポーネント数が膨大ではない小規模な製品について、最低限の項目のみ手動でコンポーネントのバージョンを管理したい

➡ SPDX Liteフォーマットを用いたSBOMを作成する

§3.2 SBOM導入プロセス

フェーズ	ステップ	実施概要
環境構築・体制整備フェーズ	SBOM適用範囲の明確化	SBOMの対象とするソフトウェアの情報（開発言語、契約形態、規制要求事項、社内の制約等）を整理して、SBOM適用範囲を明確化する。
	SBOMツールの選定	対象ソフトウェアの開発言語や組織内の制約を考慮したSBOMツールの選定の観点を整理し、当該観点に基づきSBOMツールを評価・選定する。
	SBOMツールの導入・設定	ツールの取扱説明書やREADMEファイル等を確認して、SBOMツールの導入・設定を行う。
	SBOMツールに関する学習	ツールの取扱説明書やREADMEファイル等を確認して、SBOMツールの使い方を習得する。
SBOM作成・共有フェーズ	コンポーネントの解析	対象ソフトウェアのコンポーネントを解析するとともに、解析結果について、誤検出や検出漏れが無いかを確認する。
	SBOMの作成	作成するSBOMの項目、フォーマット、出力ファイル形式等のSBOMに関する要件を決定し、当該要件を満足するSBOMを作成する。
	SBOMの共有	対象ソフトウェアの利用者及び納入先に対するSBOMの共有方法を検討した上で、必要に応じて、SBOMを共有する。
SBOM運用・管理フェーズ	SBOMに基づく脆弱性管理、ライセンス管理等の実施	脆弱性やライセンスに関するSBOMの情報を踏まえ、適切な脆弱性対応やライセンス管理対応を講じる。
	SBOM情報の管理	SBOMに含まれる情報やSBOM情報自体を適切に管理する。

図 3-1 SBOM 導入プロセス

§４．環境構築・体制整備フェーズにおける実施事項・認識しておくべきポイント

§4.1 SBOM適用範囲の明確化

HITACHI
Inspire the Next

SBOM導入に向けた実施事項

- 対象ソフトウェアの開発言語、コンポーネント形態、開発ツール等、対象ソフトウェアに関する情報を明確化する
- 対象ソフトウェアの正確な構成図を作成し、SBOM適用の対象を可視化する
- 対象ソフトウェアの利用者及びサプライヤーとの契約形態・取引慣行を明確化する
- 対象ソフトウェアのSBOMに関する規制・要求事項を確認する
- SBOM導入に関する組織内の制約(体制の制約、コストの制約等)を明確化する
- 整理した情報に基づき、SBOM適用範囲(5W1H)を明確化する

SBOM導入に向け認識しておくべきポイント

- 組織内外の開発者の知見を活用することで、対象ソフトウェアに関する効率的な情報収集を行うことができる
- 対象ソフトウェアの正確な構成図を作成し、SBOM適用の対象を可視化することで、リスク管理の範囲を明確化することができる

§4.1 SBOM適用範囲の明確化

HITACHI
Inspire the Next

SBOM適用範囲(5W1H)

観点	主な適用項目(選択肢)
SBOMの作成主体【Who】	• 自組織でSBOMを作成する • 取引契約のあるサプライヤーにてSBOMを作成する • 取引契約のないサプライヤー(OSSコミュニティ等)にてSBOMを作成する
SBOMの作成のタイミング【When】	• 製品計画または開発計画時 • プログラム開発時 • ソフトウェアビルド時 • ソフトウェア納入時 • コンポーネントのバージョンアップ時
SBOMの活用主体【Who】	• ソフトウェア利用者 • 最終製品ベンダー • 開発ベンダー • 最終製品ユーザー
SBOMの対象とするコンポーネントの範囲【What, Where】	• 開発主体が直接利用するコンポーネントのみを対象とする • 既製品等、開発委託契約のないコンポーネントから再帰的に利用されるコンポーネントも含めて対象とする
SBOMの作成手段【How】	• 構成管理情報を踏まえて手動でSBOMを作成する • SBOMツールを用いて自動でSBOMを作成する • 手動作成と自動作成を併用する
SBOMの活用範囲【Why】	• 脆弱性管理 • ライセンス管理 • 開発生産性の向上 • 資産管理、トレーサビリティ • 利用者や納入先に対するコンポーネントに関する情報の共有
SBOMのフォーマット・項目【What】	• 標準フォーマット(SPDX, SPDX-Lite, CycloneDX, SWIDタグ) • 米国大統領令におけるデータフィールドの最小要素 • 規制・要求事項や業界の慣行として使用される独自のフォーマット

HITACHI
Inspire the Next

対象ソフトウェアに関する情報の整理

項目	例
開発言語	Python, Java, Go, JavaScript, Rust, Swift, Objective-C, C, C++, VisualBasic 等
コンポーネントの形態	ライブラリ、アプリケーション、ミドルウェア、データベースサービス 等
開発環境ツール	Visual Studio, Eclipse, Android Studio, Xcode 等
ビルドツール	Jenkins, Circle CI, Github Actions, Gradle, Maven 等
構成管理ツール	Github, GitLab, Team Foundation Server, Ansible 等
自組織で取扱うデータ形式	ソースコード、パッケージ、コンテナ、バイナリデータ 等
動作環境	OS, CPUアーキテクチャ 等

備考

- SBOMツールによって対応している言語やコンポーネント形態が異なる
  ➡ **開発言語とコンポーネントの形態については最低限把握することが必要**
- SBOMの対象とする範囲を明確化するために、対象ソフトウェアの構成を可視化すること

§４.１ SBOM適用範囲の明確化

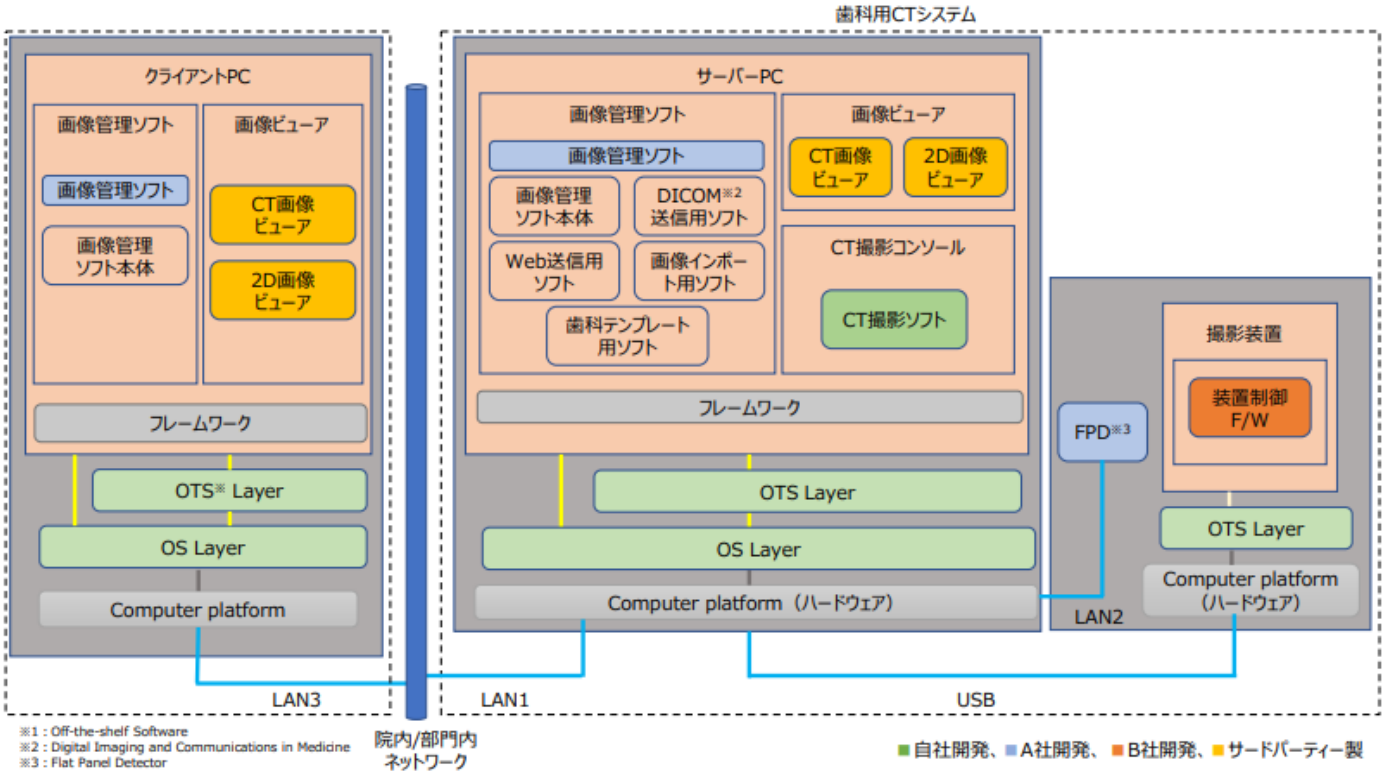


図 4-1 システム構成図の例（歯科用 CT の例）

HITACHI
Inspire the Next

契約形態・取引慣行等の情報の整理

項目	例
契約形態	開発委託、製品販売 等
コンポーネント情報の提供	提供なし、無償提供、要望された場合に提供可能 等
第三者コンポーネントの申告	すべてのOSSについて申告、ライセンスをふまえて一部のOSSについて申告 等
脆弱性の通知	修正すべきと判断された脆弱性に関してのみ通知 等
脆弱性の修正	修正すべきと判断された脆弱性に関してのみ修正 等
納品形態	バイナリパッケージ、機器組み込み、ライセンス情報(SaaS等)、実行モジュール 等
損害賠償責任	損害賠償責任有無
知的財産の帰属	自社に帰属、納入先に帰属、納入元に帰属 等
改変の有無	サードパーティから提供されたソフトウェアをそのまま使用している、自社にて改変して使用している 等

§4.1 SBOM適用範囲の明確化

HITACHI
Inspire the Next

SBOMに関する規制・要求事項の確認

- 米国
  米国大統領令で政府調達対象となるソフトウェアベンダーに対してSBOMの提供を推奨
- EU
  サイバーレジリエンス法において、EU市場に上市するデジタル製品に関してSBOMの作成を要求
- 医療機器分野
  薬機法による医療機器の規制に「医療機器サイバーセキュリティガイダンス(IMDRF ガイダンス)」を取り入れ運用

➡ **対象ソフトウェアに関する規制・要求事項について随時情報収集し、要求事項を整理する必要がある**

§4.2 SBOMツールの選定

HITACHI
Inspire the Next

SBOM導入に向けた実施事項

- 対象ソフトウェアの開発言語や組織内の制約を考慮したSBOMツールの選定の観点を整理する

  (観点の例：機能、性能、解析可能な情報、解析可能なデータ形式、コスト、対応フォーマット、コンポーネント解析方法、サポート体制、他ツールとの連携、提供形態、ユーザーインターフェース、運用方法、対応するソフトウェア開発言語、日本語対応等)

- 整理した観点に基づき、複数のSBOMツールを評価し、選定する

SBOM導入に向け認識しておくべきポイント

- 複数のSBOMツールの使い分けは非効率となる場合があるため、目的に対して最小限の運用が望ましい
- 無償のSBOMツールは、環境整備や学習時の情報不足のため、導入・運用に工数を要する可能性がある
- 有償ツールと比較して、無償のSBOMツールの機能・性能は限定的である場合が多い
- 導入環境が制限される可能性(オンプレミス型)、ソースコード情報が外部に送信される構造になっていないか(SaaS型)を確認する
- 開発効率低下を防ぐため、既存プロセスとの親和性など、開発者に負担をかけない運用を心がける
- 導入前に実際の使用感を体験することが効果的(複数のSBOMツールを扱う販売代理店に相談し、各ツールの特徴を比較評価して選定することも一案)

§4.2 SBOMツールの選定

HITACHI
Inspire the Next

SBOMツールの選定に関するポイント

- SBOMツール活用のメリット(実証を通じて明らかになったこと)
  - ✓ コンポーネント管理工数の低減
  - ✓ OSS間の依存関係やOSSの再利用の検出・管理の効率化
  - ✓ 脆弱性発表から特定までのリードタイム短縮

➡ **ツールを用いたSBOM作成・管理をおこなうことが現実的(手引書でもSBOMツール活用を前提とした記載)**

HITACHI
Inspire the Next

SBOMツール(有償・無償)の特徴

有償SBOMツール

使いやすい
(UIや機能充実、サポートあり)

ライセンス料が高額

※販売代理店やツールベンダーのサポートを受けられる

無償SBOMツール

導入しやすい
(ライセンス費用がかからない)

情報不足で工数がかかる
機能・性能が限定的

※無償ツールのサポートを提供している企業の支援を受けられる

有償ツールの例：
Black Duck(Synopsys, Inc.), Checkmarx SCA(Checkmarx, Ltd.), FOSSA(FOSSA, Inc.), FossID(FossID AB), Insignary Clarity(Insignary, Inc.), MEND SCA(Whitesource Software, Inc.), Revenera SCA(Flexera Software LLC), Snyk(Snyk, Ltd.), Sonatype Lifecycle(Sonatype, Inc.), Veracode SCA(Veracode, Inc.), yamory(株式会社アシュアード)

無償ツールの例：
Augur(CHAOSS), BOM Doctor(Sonatype, Inc.), Checkov(Bridgecrew, Inc.), Daggerboard(NewYork-Presbyterian Hospital), Dependency Track(OWASP Foundation), FOSSology(Linux Foundation), in-toto(Linux Foundation), OSS Review Toolkit(ORT)(Linux Foundation), SBOM Tool(Microsoft Corporation), ScanCode.io(nexB, Inc.), Scancode Toolkit(nexB, Inc.), SW360(Eclipse Foundation), SwiftBOM(CERT/CC), Syft&Grype(Anchore Enterprise), Trivy(Aqua Security Software, Ltd.)

HITACHI
Inspire the Next

SBOMツール選定の観点

機能

- ツールによってサポートしている機能が異なる
- **目的や適用範囲から必要機能を選定**する

性能

- 誤検出や検出漏れの発生度合い
- 新たな脆弱性が反映されるスピードなど

解析可能な情報

- 脆弱性やライセンスが自動で解析できるか
- **追加情報や精度などの強みがあるか**

解析可能なデータ形式

- **ファイル形式(拡張子別の対応可否)、パッケージマネージャー種類等のサポート範囲**

コスト

- ライセンス体系や料金体系の定義
- 課金方法(解析コード量や開発者数)
- スケールメリットの有無

対応フォーマット

- 出力できるフォーマット
- インポートできるフォーマットの種類(限定的である場合が多い)

コンポーネント解析方法

- コードマッチ、スニペットマッチ、バイナリ解析解析など
- **複数の解析がおこなえるツールもある**

サポート体制

- ツール以外の問合せが可能なプラン、無償ツールのサポート
- **担当者の知識レベルに応じてサポート契約**

他ツールとの連携

- 開発ライフサイクル全般の効率化のための連携(開発環境やビルドツール、コミュニケーションツール連携)

提供形態

- オンプレ版とクラウド版
- **サーバー維持管理費用も考慮する**
- クラウド版は機密性の担保に注意

ユーザーインターフェース

- CLIまたはGUI提供
- GUI対応ツールの場合直感的な操作と結果の可視化が可能

運用方法

- 開発環境と連携して開発者の負担軽減
- ポリシー機能等により解析結果の管理が容易になる

対応言語

- JavaやPython等であれば多くのツールがサポートしているが、**一部の言語は対応しているツールが限定的**

日本語対応

- 日本語対応しているツールは少ない
- **販売代理店が取扱説明書を日本語訳して提供している**場合あり

複数のSBOMツールを取り扱っている販売代理店に相談し、**各ツールの特徴や長所・短所を比較評価しながら選定する**ことも一案

§4.3 SBOMツールの導入・設定

HITACHI
Inspire the Next

SBOM導入に向けた実施事項

- SBOMツールが導入可能な環境の要件を確認し、整備する
- ツールの取扱説明書やREADMEファイルを確認し、SBOMツールの導入・設定をおこなう

SBOM導入に向け認識しておくべきポイント

- 有償のSBOMツールにおいては、サポートを提供している販売代理店やツールベンダーからの支援を受けることで、効率的に導入・設定をおこなうことができる
- 無償のSBOMツールにおいては、情報不足により試行錯誤的におこなう負担がかかるため、サポートサービスを提供している企業の支援を受けることで効率化できる
- SBOMツールを脆弱性管理に活用する場合、障害発生に備え、稼働監視やデータの定期バックアップを実施する

HITACHI
Inspire the Next

各段階における課題と対策

	課題	対策
導入環境整備	• インターネット接続必須 • 高スペックのマシンが必要 • Linux前提 • JavaやPythonの実行環境が必要　など	導入予定ツールの**動作条件を事前に確認し**、導入できる環境を整備する
導入・初期設定	• 環境構築や設定に関する情報が不足 • 参考ドキュメントが英語のみ • 試行錯誤的な対応が必要　など	SBOMツールの販売代理店が提供している**環境構築・初期設定の代行サービスやサポートサービスを利用**する
稼働後 (脆弱性管理)	• 障害発生によりSBOMツールが停止し、脆弱性の検知が滞る可能性	**稼働監視や定期バックアップの実施**

§４.４ SBOMツールに関する学習

SBOM導入に向けた実施事項

- ツールの取扱説明書やREADMEファイルを確認し、SBOMツールの使い方を習得する
- ツールの使い方に関するノウハウや各機能の概要は記録し、組織内で共有する

SBOM導入に向け認識しておくべきポイント

- 有償のSBOMツールにおいては、サポートを提供している販売代理店やツールベンダーからの支援を受けることで、効率的にツールの使い方を習得することができる
- サンプルSBOMの作成等を通じて試行錯誤的にツールを使うことで、効率的にツールの使い方を習得できる

すべての機能の使い方を習得するのに時間がかかる場合は、
自組織の目的を達成するのに必要な機能を
販売代理店やツールベンダーに確認し、
当該機能に絞って習得することも効果的

§５．SBOM作成・共有フェーズにおける実施事項・認識しておくべきポイント

HITACHI
Inspire the Next

SBOM導入に向けた実施事項

- SBOMツールを用いて対象ソフトウェアのスキャンをおこない、コンポーネントの情報を解析する
- SBOMツールの解析ログ等を調査し、エラー発生や情報不足による解析の中断や省略がなく、解析が正しく実行されたかを確認する
- コンポーネントの解析結果について、コンポーネントの誤検知や検出漏れがないかを確認する

SBOMツール利用により

99%以上
工数削減

医療機器分野の歯科用CTを対象とした実証の結果
(手動30人時間➡ツール0.15人時間)

SBOM導入に向け認識しておくべきポイント

- ツールにより、効率的に解析およびSBOM作成が可能
- パッケージマネージャーにより詳細な解析が可能
- 誤検出や検出漏れが生じる可能性(シンボリックリンクや深い階層等)、バージョン誤検知の可能性
- コンポーネント解析方法により結果が異なる(バイナリ解析の解析精度は一般的に低い)
- 解析環境(実行環境等)により結果が異なる可能性
- ツールのデータベースに存在しないOSSは検出できない
- 実運用時と同じ設定で解析をおこなう必要がある
- サブ階層やサードパーティコンポーネントに関する誤検知や検出漏れの確認には大きな工数がかかる
- SBOMツールの解析方式を考慮することで、効率的に誤検知や検出漏れを確認できる

HITACHI
Inspire the Next

日立ソリューションズ独自作成スライド
(経済産業省SBOM導入の手引きには掲載されていません)

SBOMツールの解析方法の種類

#	名称	解析アプローチ	特長
1	ファイルマッチング	各ファイルに対してハッシュ値等の識別情報を算出し、解析ツールのデータベース等により管理されているOSSの同識別情報と比較して、一致しているかどうかを確認する	• コンポーネントの誤検知やバージョンの誤検知など、**曖昧性を含んでいる**
2	スニペットマッチング	各ファイルの特定の一部分(スニペット)に対してハッシュ値等の識別情報を算出し、解析ツールのデータベース等により管理されているOSSのスニペットの同識別情報と比較して、一致しているかどうかを確認する	• コンポーネントの誤検知やバージョンの誤検知など、**曖昧性を含んでいる** • ファイルマッチングよりも曖昧性が高い一方、**粒度の細かい検知が可能**
3	ライセンスヘッダマッチング	特定のOSSライセンスで頻繁に用いられる用語や文章、ライセンス名称等が含まれているかを文字列検索する	• **OSSコンポーネントを検出することを目的としていない**
4	依存関係情報解析	解析対象のソフトウェアのビルドやパッケージ管理に利用されるツールの設定ファイルを解釈することにより、対象ソフトウェアのビルドや実行に使用されるOSSコンポーネントを検出する	• コンポーネントやバージョン検知の**曖昧性は低い** • 曖昧性は低いが、**誤検知ゼロではない**(実行時設定が効かない等)
5	バイナリ解析	解析対象バイナリファイルの特定の一部分に対するパターン(ビットパターンなど)を抽出し、解析ツールのデータベース等により管理されているOSSコンポーネントの同パターンと比較して、一致しているかどうかを確認する	• コンポーネントの誤検知やバージョンの誤検知など、**曖昧性を含んでいる**(ソースファイルを対象に解析する場合よりも誤検知が多い)
6	コンテナイメージ解析	解析対象のコンテナイメージの仕様上の構成や設定ファイルを解釈することにより、内包されるOSSコンポーネントを検出する	• **曖昧性は低いが、誤検知ゼロではない**(実行時設定が効かない等)

HITACHI
Inspire the Next

実証において明らかになった懸念

- スキャン対象にファイルの実体が含まれていないと検出されない(シンボリックリンクやランタイムライブラリ等)
- 最上位のコンポーネントと比較して、下位のコンポーネントの検出漏れ率が高い(ただし必ずしもコンポーネントの階層で検出率が変わるわけではなかった)
- 特定分野でのみ利用されている制御に関するコンポーネントが検出されなかった
- バージョンの情報の誤検知があった
- ツールの解析方法により出力結果が異なった(バイナリ解析の場合、1割程度しか検出されなかった)
- 解析する環境により解析結果が異なった(開発環境でスキャンした場合、製品に含まれないアンインストールパッケージが検出された)
- SBOMツールのデータベースに存在しないOSSは検出できない
- SBOMツールが特定したコンポーネントの関係性が、実際のソフトウェア構成と異なるケースがあった
- SBOMツールの解析結果と、別途パッケージマネージャーで抽出したコンポーネントが一致しないケースがあった

SBOMツールの解析結果をそのまま用いるのではなく、誤検知や検出漏れに関して出力結果を確認することが重要

SBOMツールのパラメータ設定の不足や、パッケージマネージャーの実行失敗等の理由により解析が正常に実施できておらず、誤検知や検出漏れが発生している可能性がある
➡エラーログの確認が必須

§5.2 SBOMの作成

HITACHI
Inspire the Next

SBOM導入に向けた実施事項

- 作成するSBOMの項目、フォーマット、出力ファイル形式等のSBOMに関する要件を決定する
- SBOMツールを用いて、当該要件を満足するSBOMを作成する

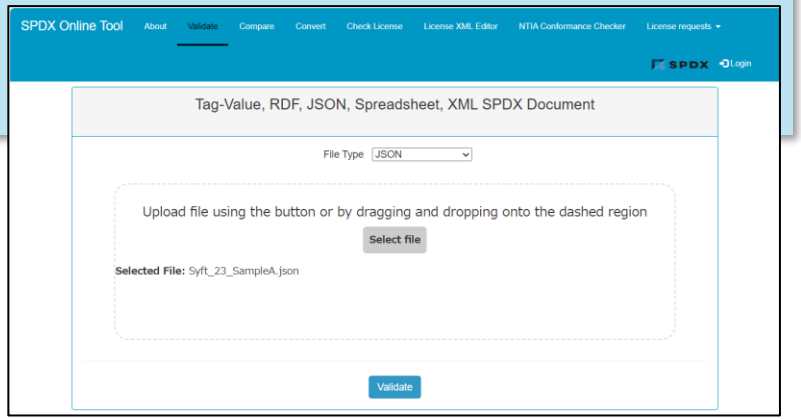
SBOM導入に向け認識しておくべきポイント

- SBOM作成と共有の目的を鑑み、正確な情報を不足なくSBOMに記載することが望ましい
- サードパーティやOSSコミュニティ等の第三者から提供されたコンポーネントを使用している場合は、当該コンポーネントのSBOMの提供を受けることができる場合もある(ただし、受領後に自組織で改変している場合はそのまま利用できないので注意)
- 名称について、利用者の視点で名称設定をおこなうことで、SBOM共有後の手戻りをなくすことができる

HITACHI
Inspire the Next

SBOMの作成に関するポイント

- 正確な情報を不足なく記載することが望まれる
  ➡「NO ASSERTION」も許容されるが、多用しない
- 第三者からSBOMの提供を受けられることもある
  ➡ 契約やライセンスの問題、**自組織で改変している場合はそのまま利用できない**ので注意
- 継続的管理の観点の要求
  ➡ SBOM作成日時を明確に記録する、**フォーマットの要件を満たしているか確認**する
- 異なる組織間での観点の要求
  ➡ **社内プロジェクトの名称やバージョン情報を用いない**



補足

- SPDXのフォーマットチェックができるツール
  (SPDX Online Tool / Validate)
- CycloneDXのフォーマットチェックができるツール
  (CycloneDX Web Tool / Validate)

§5.3 SBOMの共有

HITACHI
Inspire the Next

SBOM導入に向けた実施事項

- 対象ソフトウェアの利用者及び納入先に対するSBOMの共有方法を検討した上で、必要に応じてSBOMを共有する
- SBOMの共有にあたって、SBOMデータの改ざん防止のための電子署名技術等の活用を検討する

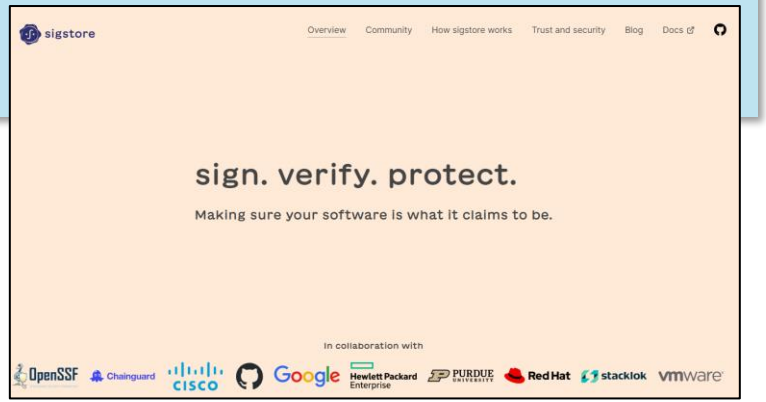
SBOM導入に向け認識しておくべきポイント

- 納入先が利用するSBOMツールによって、採用可能なSBOM共有方法が異なる
- 利用者に対してSBOM共有をおこなう場合、さまざまな方法が想定されるため、それぞれの方法の長所短所を踏まえて検討する

HITACHI
Inspire the Next

SBOMの共有に関するポイント

- コンポーネントのバージョンアップ等により作成後も動的に内容が変わる可能性が高い
  ➡ **ソフトウェア構成の更新に応じてSBOMも再作成・再共有する**ことが望ましい
- SBOMをインポートできるツールもあるが、形式やフォーマットに制約がある
  ➡ **クラウド上でツール自体を共有**する、**納入元と納入先で同じツールを採用する**等
- 利用者に対するSBOMの共有方法
  ➡ 対象ソフトウェアの特性や更新頻度、利用者のリテラシー等に応じて共有方法を検討する
- SBOMデータ自体の信頼性の確保
  ➡ **改ざん防止のための電子署名や分散型台帳技術の利用**



補足

- SBOMの電子署名
  (Sigstore)
- Linux系VTuber熊ケ谷リナさんによる解説
  (OSSマネジメントフォーラム2022セミナーレポート)

§６．SBOM運用・管理フェーズにおける実施事項・認識しておくべきポイント

§6.1 SBOMに基づく脆弱性管理、ライセンス管理等の実施

HITACHI
Inspire the Next

SBOM導入に向けた実施事項

- 脆弱性に関するSBOMツールの出力結果を踏まえ、以下の脆弱性対応をおこなう
  - ✓ 深刻度の評価
  - ✓ 影響度の評価
  - ✓ 脆弱性の修正
  - ✓ 残存リスクの確認
  - ✓ 関係機関への情報提供　など
- ライセンスに関するSBOMツールの出力結果を踏まえ、OSSのライセンス違反が発生していないかを確認する

SBOM導入に向け認識しておくべきポイント

- SBOMツールが出力した脆弱性情報やライセンスに関する情報が誤っている場合があり、出力結果を確認する必要がある
- SBOMツールでコンポーネントのEOLを特定できない場合、別途個別に調査する必要がある

HITACHI
Inspire the Next

SBOMに基づく脆弱性管理、ライセンス管理等の実施に関するポイント

- SBOMは、作成することではなくそれを用いて適切なソフトウェア管理をおこなうことが目的
  ➡ **第三者から提供されたSBOMデータについても脆弱性管理、ライセンス管理を実施**する
- 具体的な脆弱性対応の手順
  ① 脆弱性の箇所を特定して影響範囲を分析する
  ② リスクの推定および評価をおこない、リスクの受容可能性を確認、優先付け
  ③ 脆弱性の深刻度評価、緊急性を判断
  ➡ **ユーザーやサプライヤー等への通知も必要**
- SBOMツールの検出誤りの可能性
  ➡ **検出誤りにより、脆弱性の有無や深刻度が誤って出力されることがある**ので注意
- ライセンスやEOLの管理にも活用可能
  ➡ 脆弱性管理同様、**ツール利用により効率化**できる

§6.1 SBOMに基づく脆弱性管理、ライセンス管理等の実施

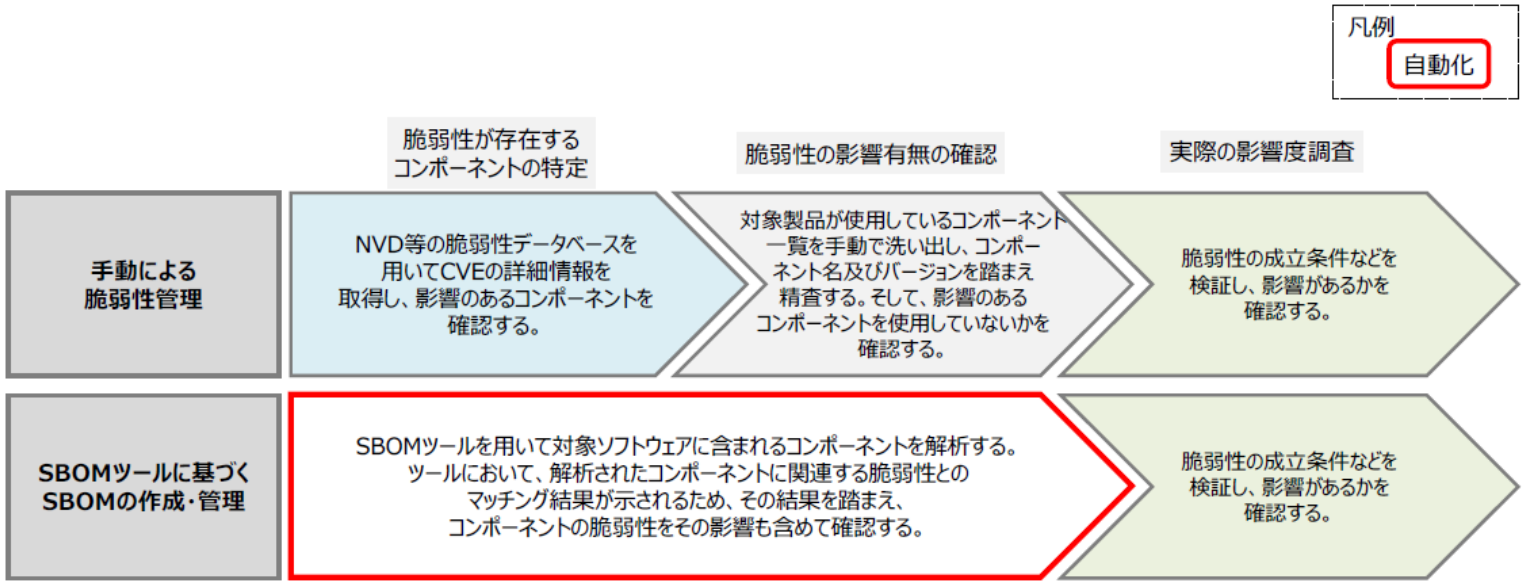


図 6-1 手動と SBOM ツールでの脆弱性管理手順の比較

- 脆弱性の情報は日々更新される(手動管理は非現実的)
- 有償ツールでは独自の詳細な脆弱性情報、定量化されたリスク値や対象方法を提供するものもある

有償ツールの活用にメリットあり

§6.2 SBOM情報の管理

HITACHI
Inspire the Next

SBOM導入に向けた実施事項

- 作成したSBOMは、社外からの問合せがあった場合等に参照できるよう、変更履歴も含めて一定期間保管する
- SBOMに含まれる情報やSBOM自体を適切に管理する

SBOM導入に向け認識しておくべきポイント

- 自動で脆弱性情報が更新・通知されるSBOMツールを用いることで、新たな脆弱性に関する情報を即座に把握することができる(ツールによる自動管理ができない場合、人的対応工数がかかる)
- SBOMの管理は、組織内のPSIRTに相当する部門(ない場合は、品質管理部門)が対応することが効果的

HITACHI
Inspire the Next

SBOM情報の管理に関するポイント

- 作成したSBOMは、社外からの問合せ対応等の目的で、**変更履歴も含めて一定期間保管**する
  保管期間の目安：
  - ✓ 対象製品が市場に流通している間、対象サービスが提供されている期間は最低限
  - ✓ 販売終了後も、保証期間・サポート提供期間・交換部品の提供期間等、必要に応じて
  - ✓ ライセンス条件により製品提供終了後3年等の個別指定がある場合もある
- **出荷済製品とSBOM情報とを紐付けられるようにしておく**
  ➡ SBOMの改変履歴も含めて資産管理システム等で保管する
- 脆弱性情報は日々更新される
  ➡ **SBOMツール活用により、新たな脆弱性情報を即座に把握可能**になる
- SBOM管理体制は、脆弱性管理の観点で主導する部門を決定する
  主導する組織の例：
  - ✓ PSIRTまたはそれに類する部門
  - ✓ 品質管理部門
  - ✓ 特定の製品開発チームで導入し、ノウハウを蓄積後、横展開

§７．付録：チェックリスト・用語集等

HITACHI
Inspire the Next

SBOM導入に向けた実施事項チェックリスト①

#	フェーズ	ステップ	実施事項	チェック
1	環境構築・体制整備フェーズ	SBOM適用範囲の明確化	対象ソフトウェアの開発言語、コンポーネント形態、開発ツール等、対象ソフトウェアに関する情報を明確化する	□
2			対象ソフトウェアの正確な構成図を作成し、SBOM適用の対象を可視化する	□
3			対象ソフトウェアの利用者およびサプライヤーとの契約形態・取引慣行を明確化する	□
4			対象ソフトウェアのSBOMに関する規制・要求事項を確認する	□
5			SBOM導入に関する組織内の制約(体制の制約、コストの制約等)を明確化する	□
6			整理した情報に基づき、SBOM適用範囲(5W1H)を明確化する	□
7		SBOMツールの選定	対象ソフトウェアの開発言語や組織内の制約を考慮したSBOMツールの選定の観点を整理する	□
8			整理した観点に基づき、複数のSBOMツールを評価し、選定する	□
9		SBOMツールの導入・設定	SBOMツールが導入可能な環境の要件を確認し、整備する	□
10			ツールの取扱説明書やREADMEファイルを確認して、SBOMツールの導入・設定をおこなう	□
11		SBOMツールに関する学習	ツールの取扱説明書やREADMEファイルを確認して、SBOMツールの使い方を習得する	□
12			ツールの使い方に関するノウハウや各機能の概要は記録し、組織内で共有する	□

(次ページに続く)

HITACHI
Inspire the Next

SBOM導入に向けた実施事項チェックリスト②

#	フェーズ	ステップ	実施事項	チェック
13	SBOM作成・共有フェーズ	コンポーネントの解析	SBOMツールを用いて対象ソフトウェアのスキャンをおこない、コンポーネントの情報を解析する	□
14			SBOMツールの解析ログ等を調査し、エラー発生や情報不足による解析の中断や省略がなく、解析が正しく実行されたかを確認する	□
15			コンポーネントの解析結果について、コンポーネントの誤検出や検出漏れが無いかを確認する	□
16		SBOMの作成	作成するSBOMの項目、フォーマット、出力ファイル形式等のSBOMに関する要件を決定する	□
17			SBOMツールを用いて、当該要件を満足するSBOMを作成する	□
18		SBOMの共有	対象ソフトウェアの利用者および納入先に対するSBOMの共有方法を検討した上で、必要に応じて、SBOMを共有する	□
19			SBOMの共有にあたって、SBOMデータの改ざん防止のための電子署名技術等の活用を検討する	□
20	SBOM運用・管理フェーズ	SBOMに基づく脆弱性管理、ライセンス管理等の実施	脆弱性に関するSBOMツールの出力結果を踏まえ、深刻度の評価、影響度の評価、脆弱性の修正、残存リスクの確認、関係機関への情報提供等の脆弱性対応をおこなう	□
21			ライセンスに関するSBOMツールの出力結果を踏まえ、OSSのライセンス違反が発生していないかを確認する	□
22		SBOM情報の管理	作成したSBOMは、社外からの問合せがあった場合等に参照できるよう、変更履歴も含めて一定期間保管する	□
23			SBOMに含まれる情報やSBOM自体を適切に管理する	□

日立ソリューションズオンラインセミナー
「OSSマネジメントフォーラム 2023」(2023/12/19 - 21)
講演資料

HITACHI
Inspire the Next

END

経済産業省発行
ソフトウェア管理に向けたSBOMの導入に関する手引(Ver. 1.0)
概要および解説

株式会社 日立ソリューションズ