HITACHI
Inspire the Next

わかる、作れる、活用できる！
ソフトウェア構成表「SBOM」のすべて

2022/07/26

株式会社 日立ソリューションズ
デジタルシフト開発支援本部　プロセス改善ソリューション部

渡邊歩 (シニアOSSスペシャリスト)

はじめに(自己紹介)

株式会社　日立ソリューションズ
デジタルシフト開発支援本部
プロセス改善ソリューション部

シニアOSSスペシャリスト

渡邊歩

ayumi.watanabe.ze@hitachi-solutions.com

- OSS管理コンサルタント
- OpenChain公式認定パートナー(日本で唯一)

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

株式会社 日立ソリューションズ

- 好きなライセンス
  Beerware License
- 趣味
  旅行、鯛焼き
- 好きなことば
  「限定」「特別」「贅沢」

はじめに(ビジネス紹介～オープンソース管理ソリューション～)

HITACHI
Inspire the Next

リスクの管理

- 自社の製品・サービスがOSSライセンスに違反していないか確認したい。
- 自社で利用しているOSSのセキュリティ脆弱性を把握したい。
- 他社を含めたサプライチェーンに潜むOSSとそのリスクを管理したい。

ツール導入・効率向上

- スキャンツールでOSS混入をチェック・解析したい
- OSSリスト（SBOM）の作成と管理を効率的に行いたい
- ツールを導入したいがどれが良いかわからない

体制構築・プロセス改善

- OSSの取り扱いに関するルールを整備し、ポリシーやガイドラインを作りたい。
- 社員向けにコンプライアンス教育を行いたい。教育コンテンツが欲しい。
- OSPOを立ち上げ、ISO/IEC 5230（OpenChain）認証を取りたい。

HITACHI
Inspire the Next

Contents

1．わかる！～SBOMの概要と普及の背景～

HITACHI
Inspire the Next

Software Bill of Materials(SBOM)とは

SBOMの定義

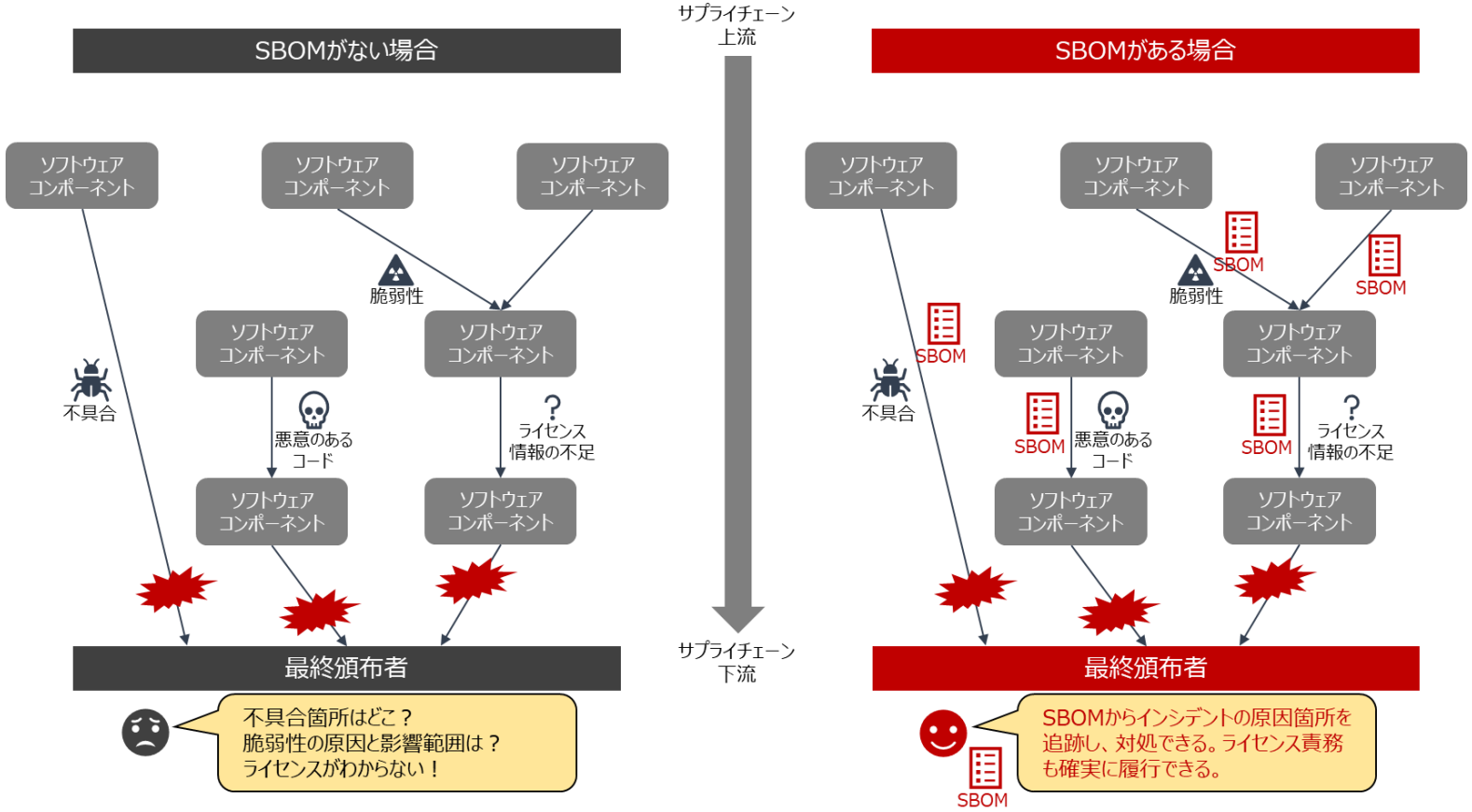
List of one or more identified components, their relationships, and other associated information
(コンポーネント(群)およびそれらの関連と関連情報の一覧)

※ここでいうコンポーネントとは、ソフトウェアライブラリやモジュール等であり、
OSSや商用ソフトウェアが含まれる(有償無償は問わない)

Component Name	Supplier	Version	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Primary
|--- Browser	Bob	2.1	Bob	0x223	334	Included in
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

「Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)」Table2より

1 - 2 SBOMがサプライチェーンにもたらす効果



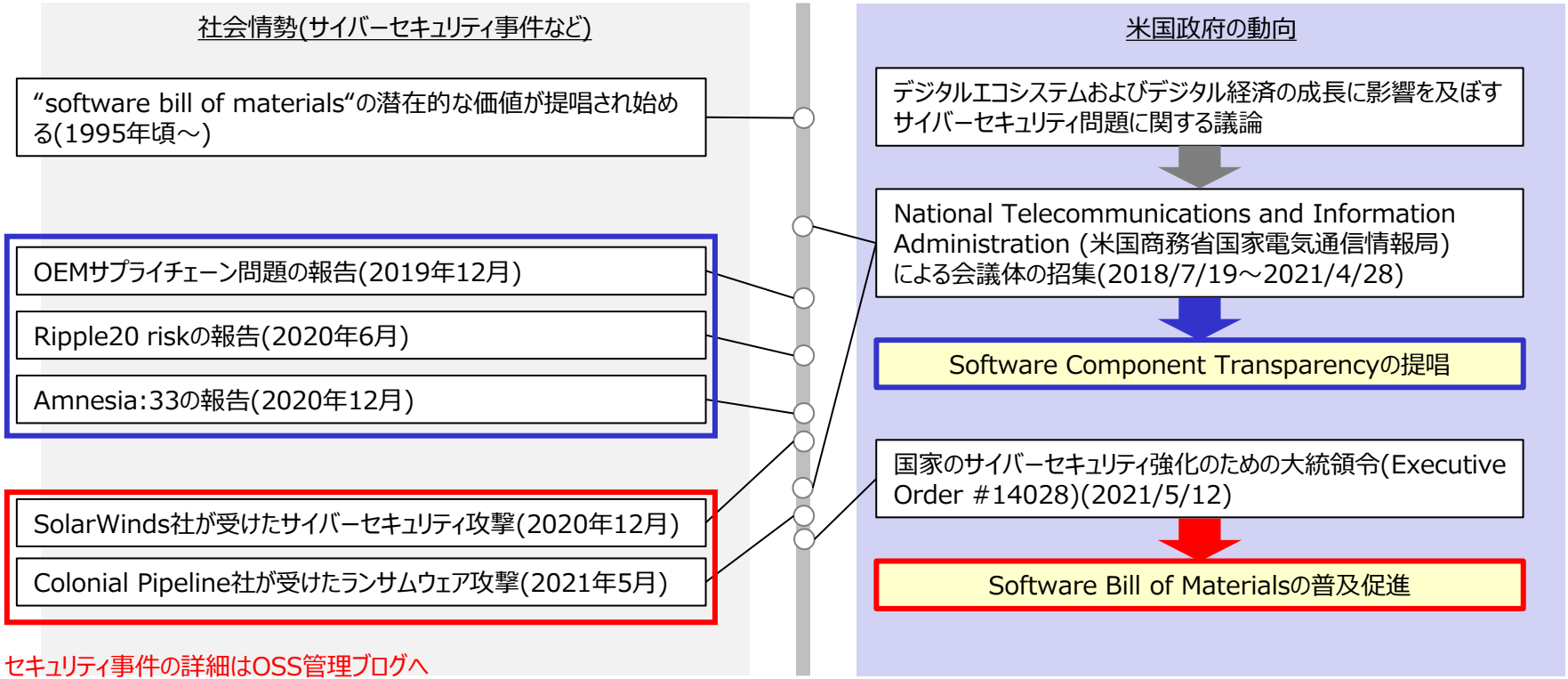
1 - 3 SBOMは何の役に立つのか？

SBOMの流通によってサプライチェーンにもたらされる2つの効果

トランスペアレンシー (Transparency/透明性)	トレーサビリティ (Traceability/追跡可能性)

- 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
- ソフトウェアに含まれているライセンスの把握とライセンスの要求事項の確実な実施
- ソフトウェアパッケージに潜むリスクの評価(マルウェアの侵入や疑わしいコードの特定等)
- 新しい脆弱性が発見された際の影響範囲調査やレビュー等、予定外の追加コストの削減
- 情報提供を怠らない優良なベンダーの選定や差別化

1 - 4 SBOMが注目されるようになった背景



セキュリティ事件の詳細はOSS管理ブログへ
→https://www.hitachi-solutions.co.jp/oms/sp/blog/2022060103/

1-5 米国政府機関におけるサイバーセキュリティ改善に係る大統領令

HITACHI
Inspire the Next

#	主な項目	概要	該当箇所
1	脅威情報の共有	政府・プライベートセクター間の脅威情報の共有を推進し、攻撃とそれによる影響(特に侵害)の情報を早期に把握することで国家のサイバーセキュリティを向上させる。	Section 2
2	連邦政府のサイバーセキュリティの近代化	ゼロトラストセキュリティモデルの採用、クラウドサービスのセキュリティの加速、多要素認証・暗号化等の基本的なセキュリティツールの展開など、セキュリティのベストプラクティスを採用し、連邦政府におけるサイバーセキュリティ基準の近代化と実装を実現する。	Section 3
3	**ソフトウェアサプライチェーンセキュリティの推進**	**ソフトウェアの可視化やセキュリティ情報の提供等を含む、政府調達ソフトウェアの開発のためのベースラインのセキュリティ標準を作成し、ソフトウェアサプライチェーンセキュリティを推進する。**	Section 4
4	サイバーセキュリティ安全審査委員会の設立	政府と民間部門のリーダーが共同議長を務めるサイバーセキュリティ安全審査委員会(重大なサイバー事件の後に召集され、何が起こったのかを分析し、サイバーセキュリティを改善するための具体的な提案を行う組織)を設立する。	Section 5
5	サイバーインシデント対応のためのプレイブックの作成	すべての連邦政府機関が脅威を特定して軽減するための統一された手順を実行するため、サイバーインシデント対応のための標準的なプレイブックを作成する。	Section 6
6	連邦政府ネットワークにおおけるサイバーセキュリティインシデント検出の向上	EDR(Endpoint Detection and Response)の実現および情報共有の改善により、連邦政府ネットワークにおけるサイバーセキュリティインシデントの検出を向上させる。	Section 7
7	連邦政府の調査および修復機能の改善	連邦省庁におけるサイバーセキュリティイベントログの要件を作成し、調査および修復機能を改善する。	Section 8

※FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks (https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/)を翻訳して抜粋。

1 - 6 大統領令におけるSBOM関連の要求事項

HITACHI
Inspire the Next

該当箇所	要求事項
Section 4.(e)	以下を含む、ソフトウェアサプライチェーンセキュリティの強化のためのガイドラインを発行する。
(i)	隔離されたビルド環境の使用、信頼関係の監査、多要素かつリスクベースの認証および条件付きアクセスの確立、開発やビルド等の環境の一部である商用製品への依存の文書化と最小化、データ暗号化の採用、運用とアラートの管理およびサイバーインシデントへの対応等を含むセキュアなソフトウェア開発環境を利用する。
(ii)	(i)のプロセスに適合していることを示す成果物を生成し、購入者から要求された場合に提供する。
(iii)	信頼性の高いソースコードサプライチェーンの維持のため、コードの整合性を確認する(自動化ツールまたは同等のプロセスにより)。
(iv)	定期的、もしくは少なくとも製品、バージョン、更新プログラムのリリース時に、既知の脆弱性や潜在的な脆弱性をチェックし修復する(自動化ツールまたは同等のプロセスにより)。
(v)	購入者から要求された場合に、(iii)コードの整合性の確認および(iv)脆弱性のチェックと修復の実行結果を提供し、評価および軽減されたリスクの概要を含むこれらのアクションの完了に関する情報を公開できるようにする。
(vi)	正確で最新のデータ、ソフトウェアコードまたはコンポーネントの出所(起源)、ソフトウェア開発プロセスに存在する内部およびサードパーティのソフトウェアコンポーネント、ツール、サービスの管理と監査を実施する。
(vii)	**購入者に対して、各製品のソフトウェア部品表 (SBOM) を直接提供するか、ウェブサイトで公開する。**
(viii)	報告および解決を含む脆弱性の対策プログラムに参画する。
(ix)	ソフトウェアのセキュア開発手法に準拠していることを証明する。
(x)	製品の任意の部分で使用されるOSSの完全性と来歴を、実行可能な範囲で保証および証明する。

※Executive Order on Improving the Nation's Cybersecurity(https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)より翻訳して抜粋。

1-7 我々日本企業も対応を迫られている

HITACHI
Inspire the Next

- ベストプラクティスの共有
- 国際標準を参照した国内標準の成立
- 契約等による責任の発生

- 増加するサイバー攻撃への対応
- サプライチェーン共通のリスクマネジメント
- エンドユーザーからの期待

SBOMの作成と提供

SBOMの活用

どんなものを作らなければならないのか？

どうやって作ればいいのか？

どんな用途に活用できるのか？

どうやって活用すればいいのか？

HITACHI
Inspire the Next

2. 作れる！～SBOMの構成要素、フォーマット、作り方～

2 - 1 SBOM作成の観点とレベル毎の要件

#	観点	レベル毎の要件		
		(低レベル)	一般的なレベル	(高レベル)
1	記載する情報	コンポーネント基本情報のコアサブセット部分のみ(コンポーネント名称、サプライヤー名称、バージョン情報、ユニークID)	すべてのコンポーネント基本情報(作成者名称、サプライヤー名称、コンポーネント名称、バージョン情報、コンポーネントハッシュ、ユニークID、依存関係情報)	より高度な保証のための追加情報まで含める
2	フォーマットおよび機械可読性	機械可読形式であること(csv等)	基本的な情報を網羅している機械可読なSBOMフォーマット(SPDX、CycloneDX、SWID)	機械可読で相互運用可能な形式であり、標準の進化や出現に追従できること
3	記述の深さ	直接的な依存関係にあるすべての主要コンポーネントおよび既知/未知の宣言	推移的な依存関係にあるすべての主要コンポーネントおよび既知/未知の宣言	推移的な依存関係にあるすべての主要コンポーネントで、未知の依存関係がないこと
4	作成の頻度	購入前や購入時、または要求に応じてN時間以内に提供など	メジャー/マイナーリリースやパッチを含む、アップデートや変更の度に毎回	全バージョンのアーカイブに格納
5	配布および相互運用性	メールで送付、サプライヤーにより提供など	各バージョンやアーカイブにバンドルしてサプライヤーより提供	API等のマシンインターフェースや相互運用可能な仕組み
6	脆弱性に関する要求	サプライヤーが要求に応じて潜在的に悪用可能な脆弱性のアテステーションを実施	サプライヤーが新しい脆弱性の発見からN時間以内に潜在的に悪用可能な脆弱性のアテステーションを実施	製品固有のリスクのアテステーションのための標準化されたAPIクエリを提供

※SBOM Options and Decision Points(https://www.ntia.gov/files/ntia/publications/sbom_options_and_decision_points_20210427-1.pdf)より翻訳して抜粋。

2-2 SBOMの最小構成

カテゴリ	概要	具体的な定義
データフィールド (Data Field)	コンポーネントの基本情報の定義	サプライヤー名称、コンポーネント名称、コンポーネントバージョン、ユニークID、依存関係、SBOM作成者名称、タイムスタンプ
自動化サポート (Automation Support)	自動化のための定義	自動化されたプロセスにおいてSBOMデータを活用するため、SPDXやCycloneDX、SWID等の共通で機械読み取り可能なデータフォーマットが必要
プラクティスとプロセス (Practices and Processes)	SBOMをいつ、どのように更新して配信するべきかに関する要件の定義	SBOM作成における頻度、深さ、未知/既知の記載、配布と配信、アクセス制御、誤りの許容

＋

追加のデータフィールド (Recommended Data Field)	SBOMの更なる活用を促進するための追加のデータフィールド	コンポーネントのハッシュ値、ライフサイクルフェーズの情報、コンポーネント間の関係性の説明、ライセンス情報

Component Name	Supplier	Version	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Primary
|--- Browser	Bob	2.1	Bob	0x223	334	Included in
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

- あくまで「最小」構成であり、利用目的に応じて必要な項目を検討するべき
- 流通することにより他社(者)と共有する情報であることを意識して作成する

※The Minimum Elements For a Software Bill of Materials (SBOM) (https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf)より翻訳して抜粋。

2 - 3 SBOMのフォーマット

HITACHI
Inspire the Next

代表的なSBOMフォーマットの例

#	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 v2.2.1(2020/9/29リリース)	CycloneDX 1.4 (2022/1/12リリース)	-
3	標準化	ISO/IEC 5962:2021	-	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	XML, JSON, Protocol Buffers(protobuf)	XML

- いずれのフォーマットも既に広く活用されているもの
- 特定のビジネスドメインにおいて実質的な業界標準となっているものもある

ユースケースやステークホルダーの要求に応じて柔軟に対応できるようにしておく必要がある

※Survey of Existing SBOM Formats and Standards (https://www.ntia.gov/files/ntia/publications/sbom_formats_survey-version-2021.pdf)より翻訳して抜粋。

HITACHI
Inspire the Next

SPDXフォーマットのSBOMの例

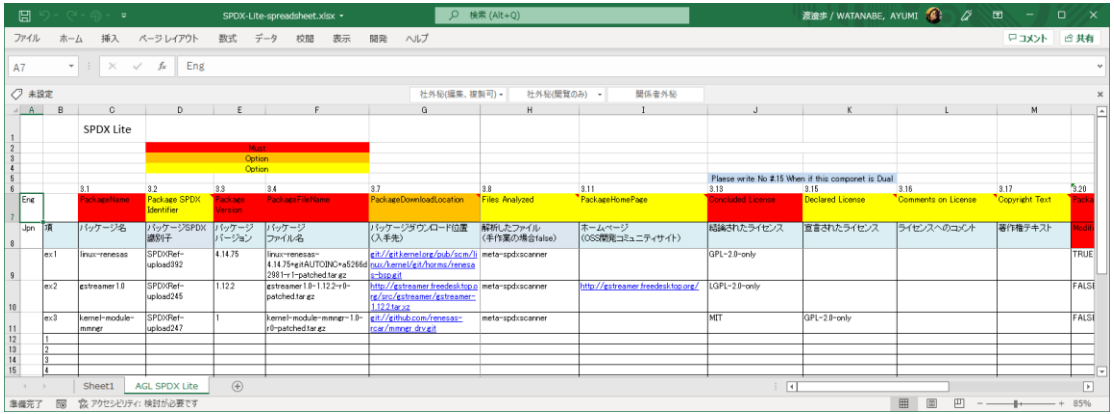
```
## Document Header
SPDXVersion: SPDX-2.1
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: ACME-INFUSION-1.0-SBOM-DRAFT
DocumentNamespace: http://www.hospitalproducts.acme
Creator: Organization: ACME-Hospital-Division()
Created: 2022-03-19T06:39:56Z
CreatorComment: <text>Draft ACME INFUSION PoC II SBOM document in SPDX form
demonstration purposes only</text>

## Packages
## 2.4 Primary Component (described by the SBOM)
PackageName: INFUSION
SPDXID: SPDXRef-4547b9db-bc49-1b28-40d2-3b17cec1daaa
PackageComment: <text>PURL is pkg:supplier/ACME/INFUSION@1.0 </text>
ExternalRef: PACKAGE-MANAGER purl pkg:supplier/ACME/INFUSION@1.0
PackageVersion: 1.0
PackageSupplier: Organization: ACME
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-4547b9db-bc49-1b28-40d2-3
Relationship: SPDXRef-4547b9db-bc49-1b28-40d2-3b17cec1daaa CONTAINS NONE
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: true
PackageLicenseConcluded: NOASSERTIN
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageFileName: INFUSION.iso
PackageChecksum: SHA256: c266f0196b28b49c427251f7a28fe28b40983a9ed2ad4663

## 2.4 All-Levels Components
##
PackageName: Windows Embedded Standard 7
SPDXID: SPDXRef-c3e304f0-6e7c-b74b-4d47-f508081e08ec
PackageComment: <text>PURL is pkg:supplier/Microsoft/Windows%20Embedded%205
ExternalRef: PACKAGE-MANAGER purl pkg:supplier/Microsoft/Windows%20Embedded%
PackageVersion: 6.1.7601
PackageSupplier: Organization: Microsoft
Relationship: SPDXRef-d2edcf56-44b9-b7cf-d8c0-9f5d73e0a578 CONTAINS SPDXRef-
f508081e08ec
Relationship: SPDXRef-c3e304f0-6e7c-b74b-4d47-f508081e08ec CONTAINS NOASSER
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: true
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
```

SPDX Lite = SPDX仕様の必要最小限のサブセット

- 特別なツールを使用せずに手動で生成可能
- エントリーレベルのサプライヤや非エンジニアリングスタッフでも作成・取扱い可能
- 実際のビジネスで実証済み



(https://github.com/OpenChain-Project/OpenChain-JWG/tree/master/License-Info-Exchange/SPDX-Lite)

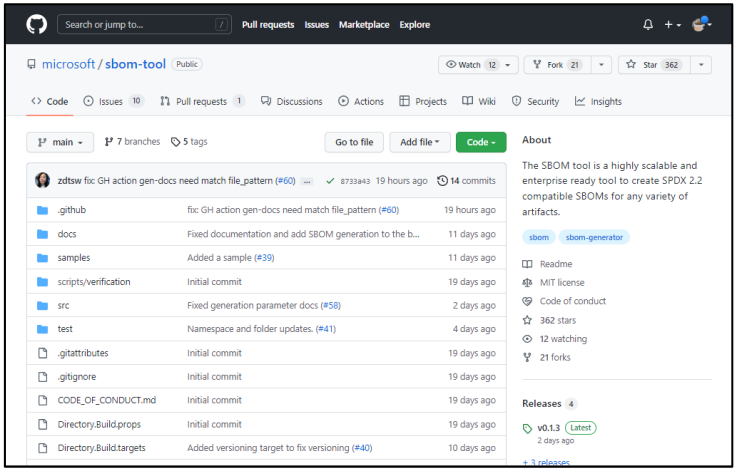
(ご参考)SPDX作成のためのガイド

日立ソリューションズのOSS管理ブログ

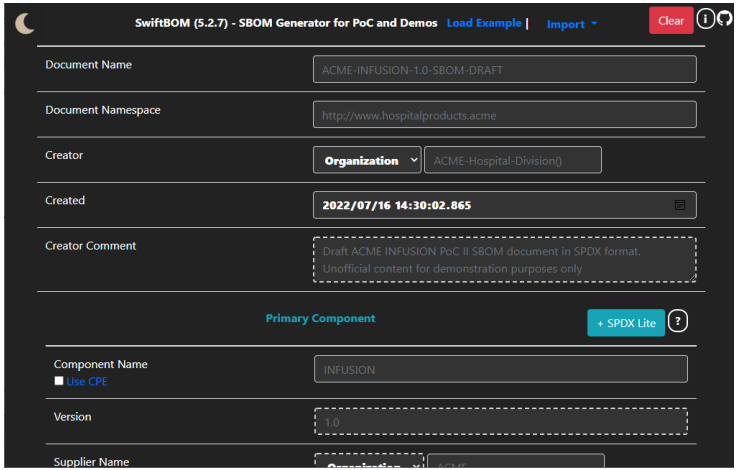
SPDX Documentを理解する
(https://www.hitachi-solutions.co.jp/oms/sp/blog/2021120101/)

SPDX-LiteでSBOMを作ってみよう
(https://www.hitachi-solutions.co.jp/oms/sp/blog/2021120102/)

2 - 5 SBOM作成ツールの活用



MicrosoftのSBOM生成ツール「Salus」
(https://github.com/microsoft/sbom-tool)



NTIA Healthcare PoCのSBOM生成サイト「SwiftBOM」
(https://sbom.democert.org/sbom/)

OSS Review Toolkit

fossology

SBOM作成機能のあるOSSツール

Black Duck

WhiteSource

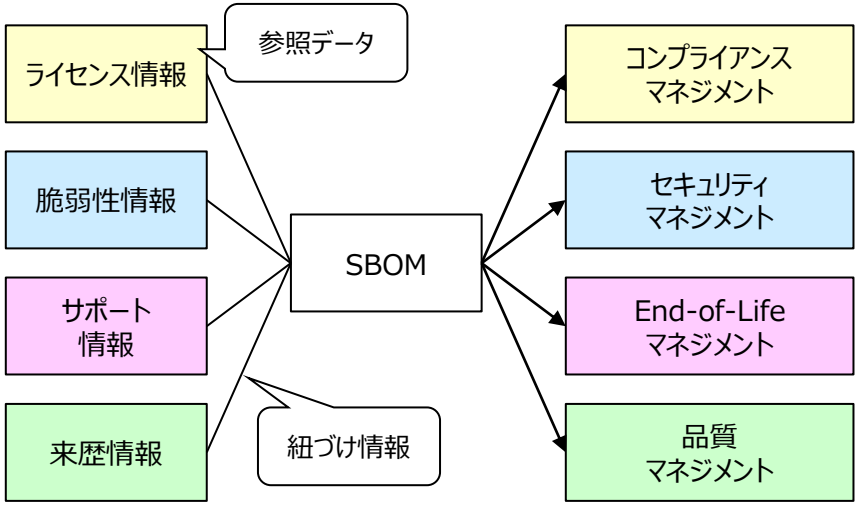
FOSSA

OSS管理ツールでの作成は簡単＆高精度！
(https://www.hitachi-solutions.co.jp/oms/sp/solution/lineup_tools/)

HITACHI
Inspire the Next

3．活用できる！～SBOMのユースケースと活用方法具体例～

3 - 1 SBOMのユースケース



SBOMの代表的なユースケース

SBOM活用のポイント

- 参照データ
  充実度・鮮度・信頼性および体系化されていることが担保できる参照データを準備すること

- 紐づけ情報
  SBOMの構成要素と適切な情報を一意に紐づけできる識別子であること
  識別子自体の正確性が担保されていること

HITACHI
Inspire the Next

■ SBOMを活用したセキュリティマネジメント

セキュリティマネジメントの対象となるソフトウェアの脆弱性

既知の脆弱性(known vulnerability)
開発時点や出荷時点など、ある特定のタイミングにおいて既に発見されている脆弱性のこと。【比較的管理しやすい】

未知の脆弱性(unknown vulnerability)
将来的に発見される可能性のある脆弱性のこと。【定期的な監視が必要】

【参照データの例】
- National Vulnerability Database(NVD)
  (https://nvd.nist.gov/)
- Japan Vulnerability Notes(JVN)
  (https://jvn.jp/)

その他、有償サービスなど

【紐づけ情報の例】
- Component Name & Version of the Component
  例：Log4j version.2.4.1
- Common Platform Enumerations (CPE)
  例：cpe:2.3:a:apache:log4j:2.4.1:*:*:*:*:*:*:*

【マッピングの工夫】
- 紐づけ情報としてCPEを利用することにより、影響を受ける脆弱性のみにフィルタリング可能
- cve-search(https://github.com/cve-search/cve-search)で定期モニタリングとアラート

HITACHI
Inspire the Next

■ SBOMを活用したコンプライアンスマネジメント

コンプライアンスマネジメントの対象となるライセンス情報

プロプライエタリソフトウェアのライセンス
End User License Agreement(EULA)など、当該ソフトウェアの使用許諾条件。購入時に明確に提供される。

OSSソフトウェアのライセンス
当該OSSに付属するライセンス。著作者の意志により変更される可能性や依存関係による複合的な条件などを考慮する必要がある【複雑化する傾向】。

【参照データの例】
- 当該ソフトウェアに付属するライセンス条件書
- (OSSライセンスの場合)Open Source Initiative (https://opensource.org/licenses)
- (OSSライセンスの場合)tl;dr Legal (https://tldrlegal.com/)

【紐づけ情報の例】
- License Name & License Version
  例：Apache License Version.2.0

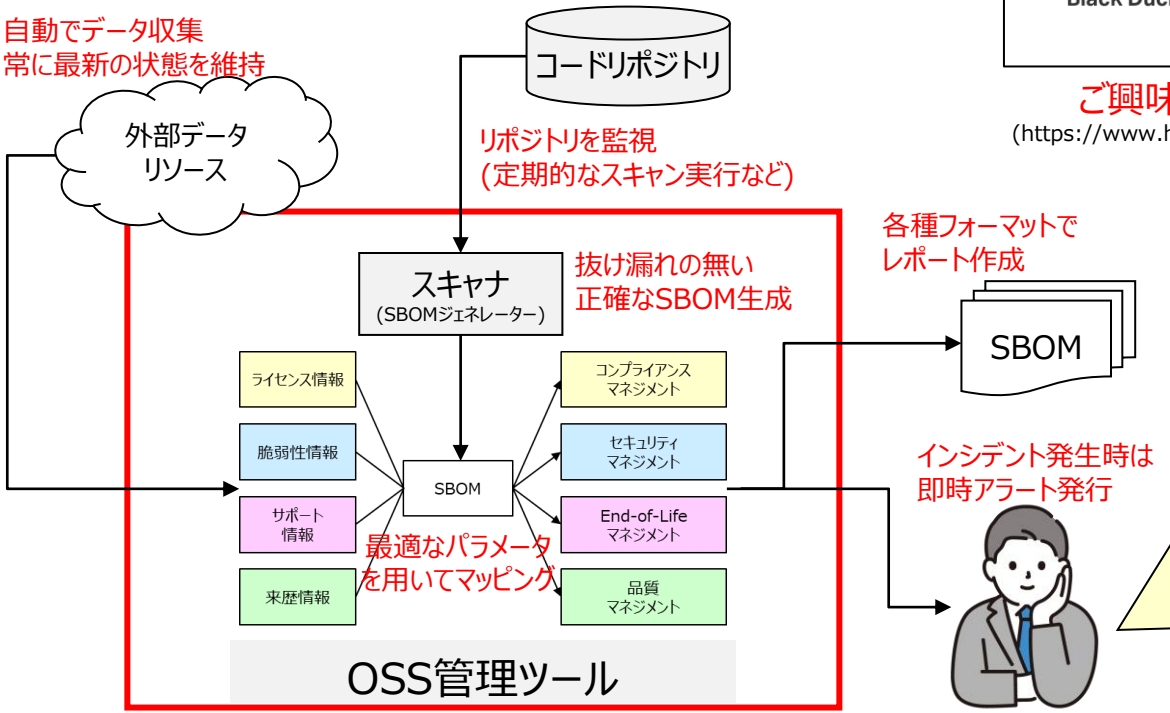
【マッピングの工夫】
- ライセンスのバージョンに注意
- OSSのバージョンアップの際にライセンスが変更される可能性があるので必ず確認する
- 依存関係(直接的な依存関係、推移的な依存関係)を考慮し、適用されるすべてのライセンス条件を確認する

HITACHI
Inspire the Next

■ OSS管理ツールの活用

Black Duck | WhiteSource | FOSSA

ご興味のある方は是非お問合せください
(https://www.hitachi-solutions.co.jp/oms/sp/solution/lineup_tools/)



OSS管理ツールを使えば圧倒的にラクできる！

- スキャナにより正確なSBOMを生成、ライセンスなどの付随情報を自動で補足
- 最適化された紐づけ情報が整備されており正確なマッピングが可能
- 参照データを自動で更新、常に最新の情報を維持
- アラート発行ポリシーやトリアージ条件の設定も可能

４．まとめ

HITACHI
Inspire the Next

SBOMの課題

SBOMの作成に関する課題

- SBOMにどのような情報を含めるべきかがわからない
- SBOM作成に関する新たなコストが発生する
- ソフトウェアIDやSBOMの形式が統一されていないなど、自動化の障害が存在する

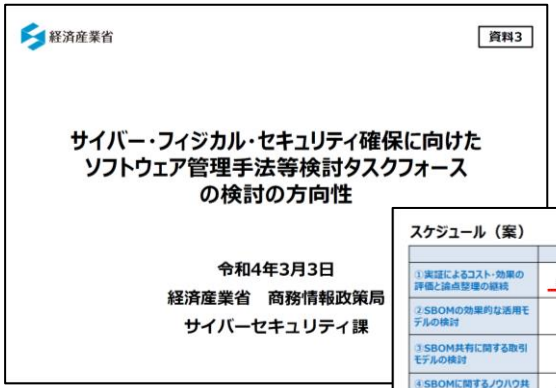
SBOMの提供に関する課題

- 顧客にとってのメリットが不明、SBOM受領者から合理性のない対応を求められる懸念がある
- ソフトウェア開発契約書面のような、更新頻度に課題がある正本が別に存在し、SBOMとそれ以外の文書との整合性が取れない
- 他社にソフトウェアの構成要素を知られたくない
- 知的財産の流出の懸念がある

SBOMの活用に関する課題

- SBOMに記載されている情報をどのように活用できるかわからない
- 記載されているコンポーネントの名称やIDが共通ではなく、管理しにくい
- 対象に合わせて自動化された管理方法が必要である

4 - 2 私たちが注視しておくべきこと

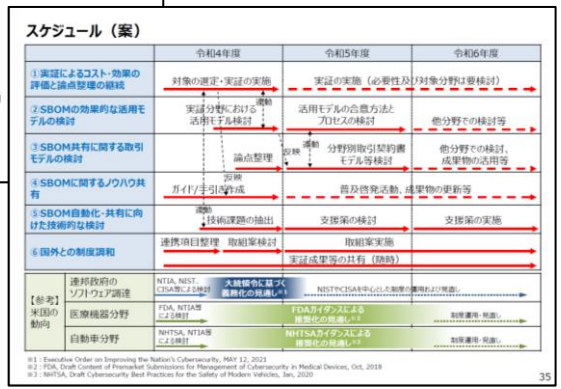

経済産業省

資料3

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
の検討の方向性

令和4年3月3日
経済産業省　商務情報政策局
サイバーセキュリティ課

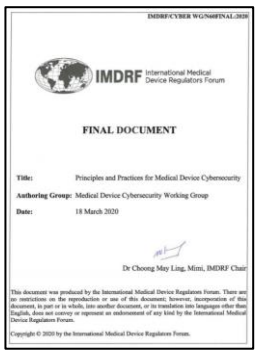
経済産業省による
ガイドラインの発行や
ベストプラクティスの共有


スケジュール（案）

	令和4年度	令和5年度	令和6年度
①実証によるコスト・効果の評価と論点整理の継続	対象の選定・実証の実施	実証の実施（必要性及び対象分野は要検討）	
②SBOMの効果的な活用モデルの検討	実証分野における活用モデル検討	活用モデルの合意方法とプロセスの検討	他分野での検討等
③SBOM共有に関する取引モデルの検討	論点整理	分野別取引契約書モデル等検討	他分野での検討、成果物の活用等
④SBOMに関するノウハウ共有	ガイド/手引き作成	普及啓発活動、成果物の更新等	
⑤SBOM自動化・共有に向けた技術的な検討	技術課題の抽出	支援策の検討	支援策の実施
⑥国外との制度調和	連携項目整理　取組案検討	取組案実施	
		実証成果等の共有（随時）	
【参考】米国の動向 連邦政府のソフトウェア調達	NTIA, NIST, CISA等による検討	大統領令に基づく義務化の見通し※1	NIST・CISA等中心とした制度の運用および見直し
【参考】米国の動向 医療機器分野	FDA, NTIA等による検討	FDAガイダンスによる義務化の見通し※2	制度運用・見直し
【参考】米国の動向 自動車分野	NHTSA, NTIA等による検討	NHTSAガイダンスによる義務化の見通し※3	制度運用・見直し

※1：Executive Order on Improving the Nation's Cybersecurity, MAY 12, 2021
※2：FDA, Draft Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Oct, 2018
※3：NHTSA, Draft Cybersecurity Best Practices for the Safety of Modern Vehicles, Jan, 2020

35


IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity
Authoring Group: Medical Device Cybersecurity Working Group
Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

Copyright © 2020 by the International Medical Device Regulators Forum.

各産業界のポリシーや動向

コミュニティ動向

OPENCHAIN


Microsoft | Engineering@Microsoft

Microsoft open sources Salus software bill of materials (SBOM) generation tool

Danesh Kumar Badlani　Adrian Diglio

July 12th, 2022

We are excited and proud to open source Salus, Microsoft's software bill of materials (SBOM) tool. A key requirement of the Executive Order on Improving the Nation's Cybersecurity, SBOMs are lists of ingredients that make up software components and provide organizations with insight into their supply chain dependencies.

The Salus SBOM tool is a general purpose, enterprise-proven, build-time SBOM generator. It works across platforms including Windows, Linux, and Mac, and uses the standard Software Package Data Exchange (SPDX) format. (To see the previous announcement about our SBOM tool, please read Generating Software Bills of Materials (SBOMS) with SPDX at Microsoft.)

Feedback

大手デジタルプラットフォーマーの動向

日立ソリューションズ「OSS管理ブログ」
(https://www.hitachi-solutions.co.jp/oms/sp/blog/)

(https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/006_03_00.pdf)
(https://devblogs.microsoft.com/engineering-at-microsoft/microsoft-open-sources-salus-software-bill-of-materials-sbom-generation-tool/)

HITACHI
Inspire the Next

END

わかる、作れる、活用できる！
ソフトウェア構成表「SBOM」のすべて

2021/07/26

株式会社 日立ソリューションズ
デジタルシフト開発支援本部　プロセス改善ソリューション部
渡邊歩 (シニアOSSスペシャリスト)