初めての人のためのSBOM入門セミナー

HITACHI
Inspire the Next

短時間で要点だけ理解したい人のためのSBOM解説

2022/11/09

株式会社 日立ソリューションズ
ITプラットフォーム事業部 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

はじめに(想定聴講者)

- 最近「SBOM」という言葉をよく聞く方や、なんとなく気になっている方
- 概要は理解しているが改めて学びたい方
- SBOM対応を始めたいが何から手を付ければ良いのかわからない方

もっとハイレベルの業界動向を
知りたい！という方は、
こちらのセミナーをどうぞ

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

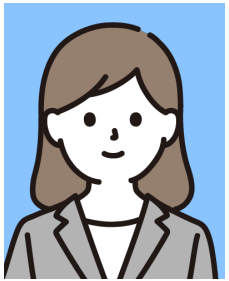
渡邊歩

ayumi.watanabe.ze@hitachi-solutions.com

- OSS管理コンサルタント、SBOMエバンジェリスト
- OpenChain公式認定パートナー(日本で唯一)

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

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」

そもそも
SBOMってなんですか？

HITACHI
Inspire the Next

Software Bill of Materials(SBOM)とは

SBOMの定義

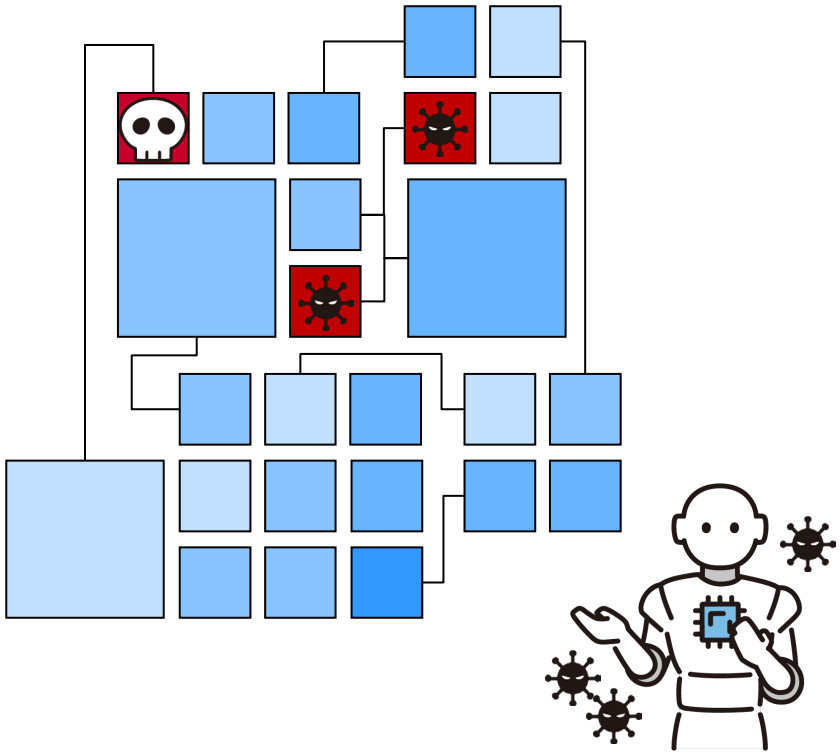
List of one or more identified components, their relationships, and other associated information
(コンポーネント(群)およびそれらの関連と関連情報の一覧)

※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

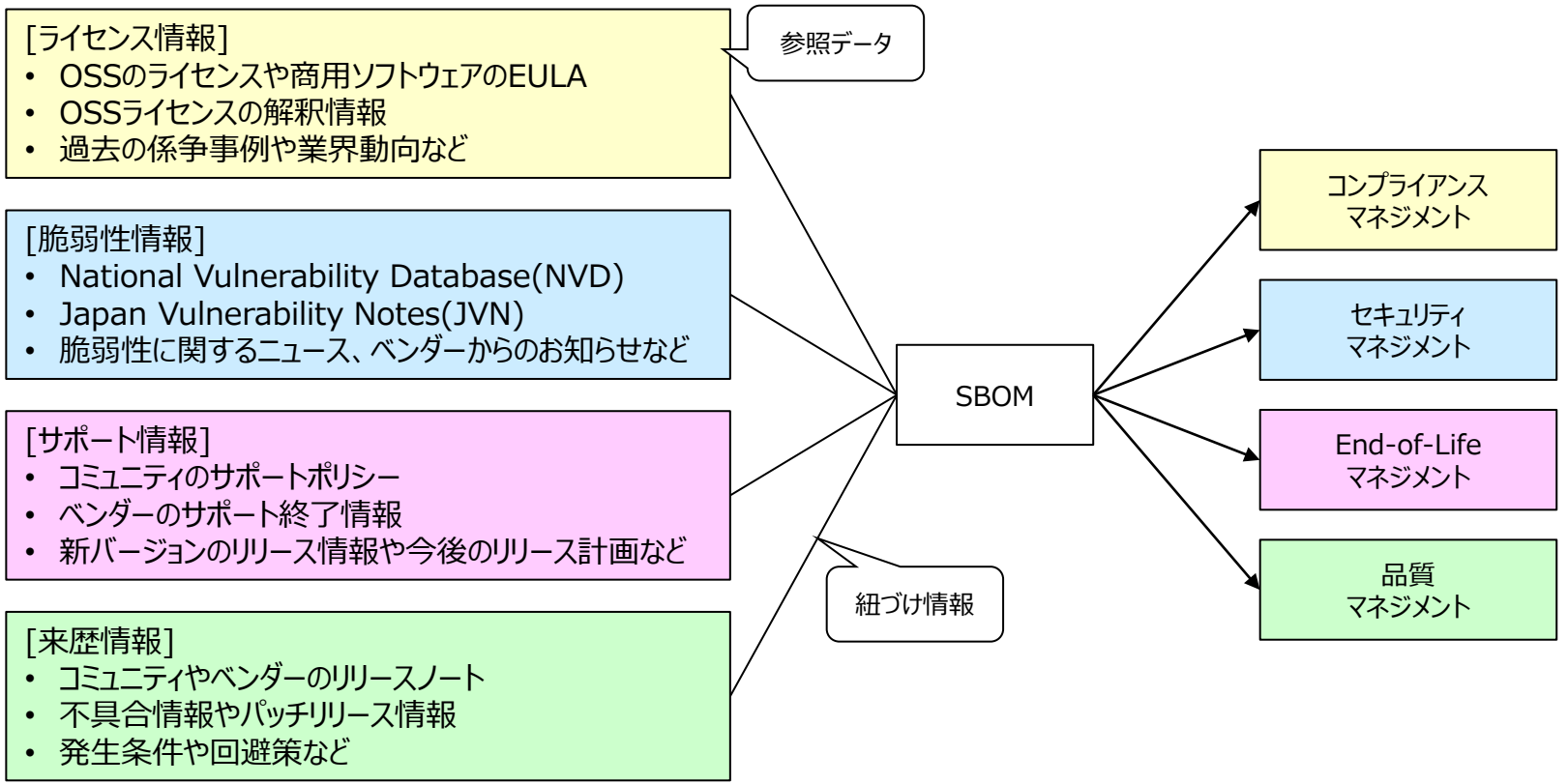
1 - 2 SBOMがソフトウェアサプライチェーンにもたらす効果



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)

1 - 3 SBOMの活用



2 日本企業におけるSBOMの重要性

SBOMは
私にも関係ありますか？

2-1 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。

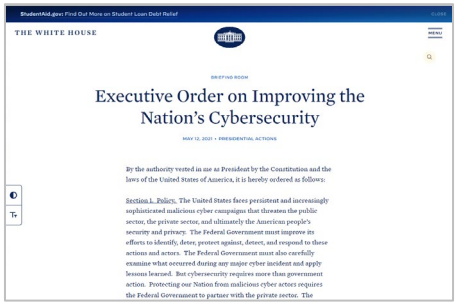
2-2 大統領令におけるSBOM関連の要求事項

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。

2-3 日本企業への影響


THE WHITE HOUSE

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The

- 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

我々日本企業も
SBOMへの対応を迫られている

3 SBOMの作り方

SBOMの作り方に
ルールはありますか？

3 - 1 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。

3 - 2 SBOM作成の観点とレベル毎の要件

HITACHI
Inspire the Next

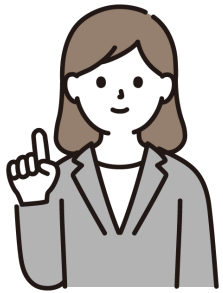
#	観点	レベル毎の要件		
		(低レベル)	一般的なレベル	(高レベル)
1	記載する情報	コンポーネント基本情報のコアサブセット部分のみ(コンポーネント名称、サプライヤー名称、バージョン情報、ユニークID)	すべてのコンポーネント基本情報(作成者名称、サプライヤー名称、コンポーネント名称、バージョン情報、コンポーネントハッシュ、ユニークID、依存関係情報)	より高度な保証のための追加情報まで含める
2	フォーマットおよび機械可読性	機械可読形式であること(csv等)	基本的な情報を網羅している機械可読なSBOMフォーマット(SPDX、CycloneDX、SWID)	機械可読で相互運用可能な形式であり、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。

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 v2.2.2(2022/4/28リリース)	CycloneDX 1.4 (2022/1/12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



- 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

SBOM対応
まず何から始めれば
良いのでしょうか？

4 - 1 SBOM対応の始め方の例

HITACHI
Inspire the Next

#	項目	エントリーレベル	ハイレベル
1	対象	頒布対象の製品や社外に提供するサービス (販売、提供、公開などの予定があるもの) スモールスタートでOK	自社ビジネスに関係するすべてのソフトウェア (内部利用ソフトウェアや研究開発フェーズのものなども含む)
2	対象の粒度	直接的に利用するサードパーティー製ソフトウェアおよびOSS 不明なものは不明で構わない	推移的な依存関係にあるすべての主要コンポーネント 未知の依存関係がないこと
3	記載内容	少なくとも以下を含む：コンポーネント名称およびバージョン、取得元情報(URLやベンダー名など)、依存関係、コンポーネントハッシュ、ライセンス、固有識別子(CPEやPURLなど)	SPDXやCycloneDXなどの標準フォーマットの必要要素がすべて網羅されていること 固有識別子(CPEやPURLなど)が漏れなく記載されていること
4	作成タイミング	頒布対象のバージョンに対して、頒布前に必ず作成されること	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 ビルドのタイミングなどで自動的に更新される仕組み
5	作成方法	まずは手書きでOK (エクセルなど人が読み書きしやすい形式)	ツールによる自動化 履歴管理可能かつ検索容易性を考慮したデータの蓄積
6	管理・対応	ライセンス遵守、頒布前の既知の脆弱性対応は必須	未知の脆弱性に対応するための定期的な監視とエスカレーション方法の確立 EOLや品質来歴を考慮したバージョンアップ計画

4 - 2 SBOM作成のステップ

インベントリ：サードパーティー製ソフトウェアのリストを作成する

調査：各コンポーネントに関して、必要な情報を収集する

レポート：SBOMフォーマットの形式で記述する

評価：フォーマットとして正しく動作するかを確認する

開示：顧客やステークホルダーに対して報告する(任意)

Software Composition Analysis(SCA)ツールを用いて自動化できる部分

Black Duck

Mend社のソフトウェアコンポジション解析ツール

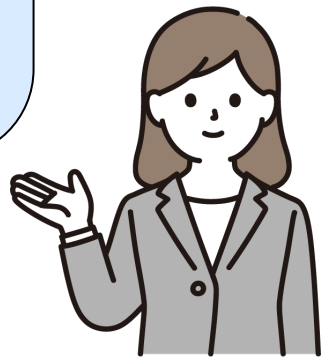
FOSSA

insignary

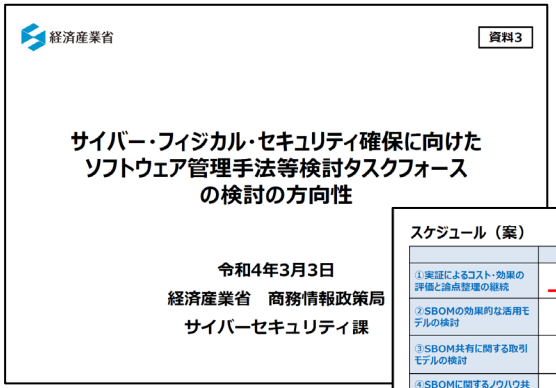
※NTIA Software Transparency Healthcare POC How-To Guide for SBOM Generation (https://www.ntia.gov/files/ntia/publications/howto_guide_for_sbom_generation_v1.pdf)を参考に作成。

HITACHI
Inspire the Next

本日のまとめ



私たちが注視しておくべきこと

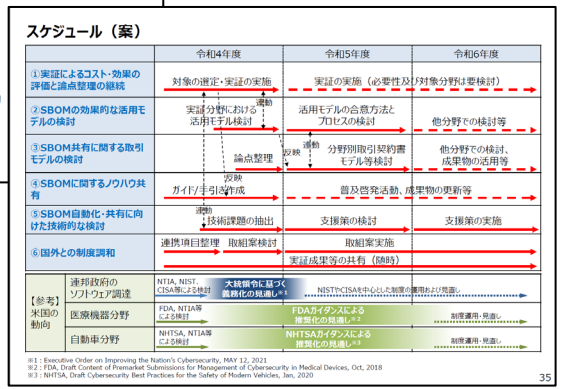

経済産業省

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

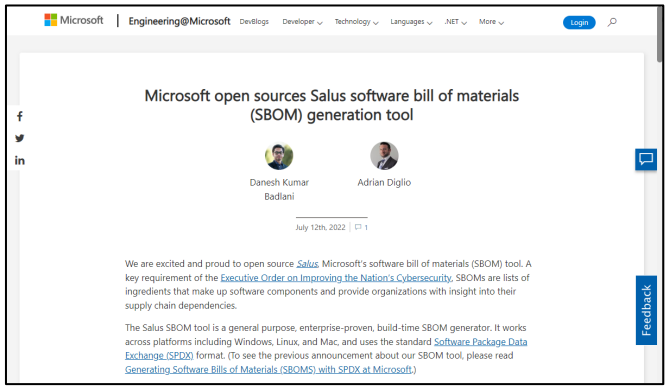
経済産業省による
ガイドラインの発行や
ベストプラクティスの共有


スケジュール（案）

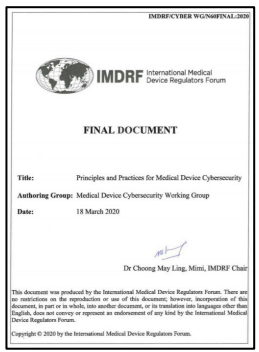
	令和4年度	令和5年度	令和6年度
①実証によるコスト・効果の評価と論点整理の継続	対象の選定・実証の実施	実証の実施（必要性及び対象分野は要検討）	
②SBOMの効果的な活用モデルの検討	実証分野における活用モデル検討	活用モデルの合意方法とプロセスの検討	他分野での検討等
③SBOM共有に関する取引モデルの検討	論点整理	分野別取引契約書モデル等検討	他分野での検討、成果物の活用等
④SBOMに関するノウハウ共有	ガイド/手引き作成	普及啓発活動、成果物の更新等	
⑤SBOM自動化・共有に向けた技術的な検討	技術課題の抽出	支援策の検討	支援策の実施
⑥国外との制度調和	連携項目整理　取組案検討	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やCISAを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ガイダンスによる推奨化の見通し※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ガイダンスによる推奨化の見通し※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



大手デジタルプラットフォーマーの動向


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.

コミュニティ動向

OPENCHAIN

各産業界のポリシーや動向

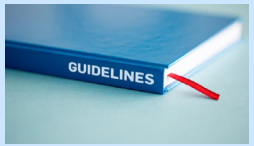
日立ソリューションズ「OSS管理ブログ」
(https://www.hitachi-solutions.co.jp/oms/sp/blog/)

(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/)

日立ソリューションズのオープンソース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OSS利活用をサポート


OSS管理プロセス策定支援/
OSPO支援



OSSガイドライン策定支援


OSS教育


SBOM導入支援/
SBOM活用支援


OSSチェック/
SBOM作成支援


ISO/IEC 5230
(OpenChain)認証


OSSライセンスに関する
コンサルティング


OSSよろず相談


OSSライセンス調査代行


OSSの審査・承認代行


OSS管理のための
専用ツール開発


勉強会やセミナーへの
講師派遣

先進的なツールを複数ラインアップ

Black Duck	Mend社の ソフトウェアコンポジション 解析ツール	FOSSA	insignary clarity	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	

HITACHI
Inspire the Next

END

短時間で要点だけ理解したい人のためのSBOM解説

2022/11/09

株式会社 日立ソリューションズ
ITプラットフォーム事業部 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