令和6年度　医療機器製造販売業者のサイバーセキュリティ対策周知等事業

ソフトウェア部品表（SBOM）の作成と運用

一般社団法人　日本医療機器産業連合会
医療機器サイバーセキュリティ対応WG

Ministry of Health, Labour and Welfare of Japan

令和6年度医療機器製造販売業者のサイバーセキュリティ対策周知事業

■ 医療機器サイバーセキュリティにおける、医療機関との連携に向けた取組と諸課題

1. 医療機器のサイバーセキュリティに関する国内規制の動向

2. 医療機器サイバーセキュリティの実践

- 医療機器のサイバーセキュリティについて
- サイバーセキュリティに係る規格について（IEC 81001-5-1:2021）
- 医療機器のサイバーセキュリティ要件に対するJIS T 81001-5-1の適用について

3. 医療機関とのPSIRTの実践

4. 「製造業者/サービス事業者による医療情報セキュリティ開示書」の概要

5. ソフトウェア部品表（SBOM）の作成と運用

医療機器
製造販売業者等

医療機関、
医療情報システム製造業者等

目　次

医療機器は、高機能化やネットワーク接続等によるシステム化によって多くのベネフィットを提供するために、サードパーティ製ソフトウェアコンポーネントを導入又は必要環境とすることが増えている。これにより、医療機器の開発は、経済的になり、信頼性が向上し、イノベーションが加速している。一方で、患者安全並びにネットワーク接続する医療機器の機密性、完全性及び可用性に影響を及ぼす可能性のあるサイバーセキュリティに関連するリスクも増加している。

共通のソフトウェアコンポーネントを使用していることによって、複数の製造販売業者の一見無関係な医療機器に対して、ある脆弱性が様々な影響を及ぼすかもしれないという点で、サイバーセキュリティの脆弱性は特別である。この問題は、一般的に機器内部の共通コンポーネントのトレーサビリティが低いことで悪化している。このため、**ソフトウェアの透明性の確立が重要であり、その対策の一つとして、ソフトウェア部品表（SBOM）の概念が定義**された。SBOMは、製品の全ライフサイクル（TPLC）を通じて、市販前及び市販後活動において活用され、製造販売業者と医療機関との間の重要なコミュニケーションツールである。

本稿では、整備されつつある医療機器のSBOMが、より効果的に活用されるように、**SBOMに関する国際的な動向並びに課題等**について説明する。

1. 医療機器のSBOMに関する国際的要件
2. SBOMフレームワークの確立
3. SBOM関連の課題と緩和策
4. まとめ

※本資料中の英文の和訳は参考訳です。正確な表現が必要な場合は、元となる英文を参照してください。
※本資料中に参照される法令、規格、ガイダンス等の情報は、2025年1月20日時点のものです。
※本資料中の記述は、発表者の個人的解釈が含まれており、**IMDRF**や各国規制当局が認めた内容ではない事を了承ください。
※本資料中には、各社の商標が含まれている場合があります。

1. 医療機器のSBOMに関する国際的要件

IMDRF（International Medical Device Regulators Forum）の動向

- 医療機器のサイバーセキュリティに関して、2019年1月にWGキックオフ → 2020年4月公開
  - 医療機器サイバーセキュリティの原則及び実践：Principles and Practices for Medical Device Cybersecurity
    原文：http://imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf
    邦訳：https://dmd.nihs.go.jp/cybersecurity/IMDRF_Guidance_Japanese_version.pdf
    - 医療機器規制当局としての対応指針（**ハイレベルで包括的な国家ルール**）

一般原則
① 国際調和
② 製品ライフサイクル
③ 共同責任
④ 情報共有
⇒ 市販前の考慮事項 ⇒ 市販後の考慮事項

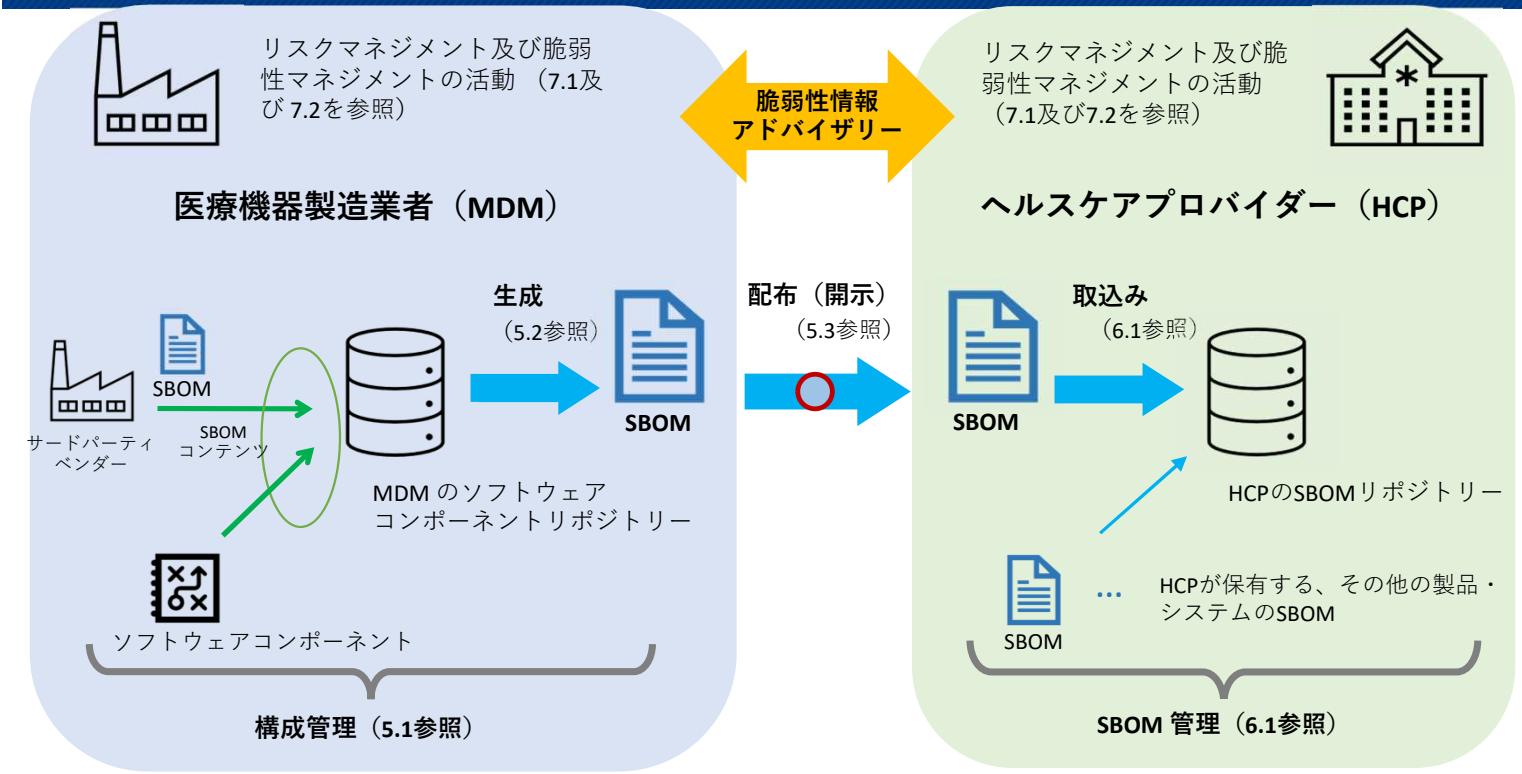
- SBOM及びレガシー医療機器に関するNWIE(Extension)についてガイダンス追補の策定のため、2021年2月にWG作業を再開 → 2023年4月公開
  - レガシー医療機器：Principles and Practices for the Cybersecurity of Legacy Medical Devices
    https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices
  - ソフトウェア部品表（**SBOM**）：Principles and Practices for the Software Bill of Materials for Medical Devices
    https://www.imdrf.org/documents/principles-and-practices-software-bill-materials-medical-device-cybersecurity

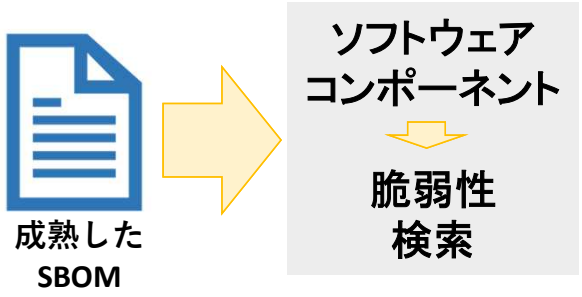
「国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について（周知依頼）」
（令和2年5月13日、薬生機審発0513第1号・薬生安発0513第1号）
2020年 ※IMDRFガイダンス

「医療機器のサイバーセキュリティ導入に関する手引書」
・初版：令和3年12月24日、薬生機審発1224 第1号 薬生安発 1224第1号
・改訂：令和5年 3月31日、薬生機審発0331第11号 薬生安発 0331第4号
2023年改訂 にて通知された

国内導入へ 2023年

ソフトウェア部品表（SBOM）の作成・運用の確立 ― ソフトウェアの透明性確保



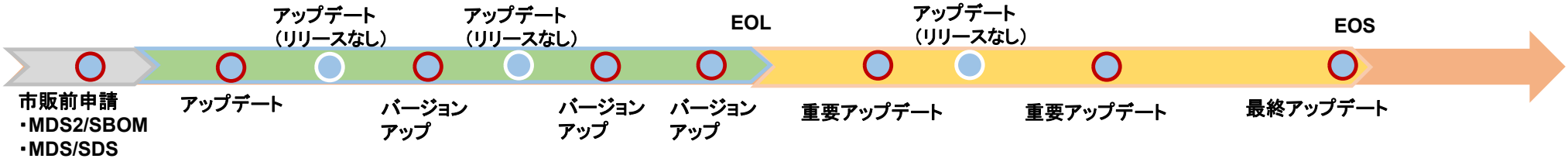


全分野対象に進められている
脆弱性マネジメント自動化のフロー
（SBOM起点）

SBOM（Software Bill of Materials）の導入に関する手引（2023/7/28）
https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

IMDRF N73 図1—SBOMフレームワークの概要を引用

参考）ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引 Ver. 2.0
https://www.meti.go.jp/press/2024/04/20240426001/20240426001-2.pdf



脆弱性関連情報（セキュリティ アドバイザリー） ー 製造販売業者と医療機関との連携

Windows DNS サーバーのリモートでコードが実行される脆弱性(CVE-2020-1350)

2020年7月14日、Microsoft社は「パッチチューズデイ」と呼ばれるWindowsの定期アップデート「2020 年 7 月のセキュリティ更新プログラム」（**緊急：CVSS 10.0**）を公開しました。中でも、Windows DNSサーバのRCE（リモート遠隔コード実行）脆弱性「CVE2020-1350」は発見者のCheck Point社により**「SIGRed」と命名され「ワーム活動に利用可能」**な脆弱性として注視されています。（トレンドマイクロ社）
https://blog.trendmicro.co.jp/archives/25567

製造販売業者（SBOM提供済み）

■ セキュリティアドバイザリーの開示

影響を受けるのはDNSサーバだけであり、クライアントに影響はないので、影響範囲は大きくないと判断している。

2020年7月21日　CVE-2020-1350| Windows DNS Server Remote Code Execution Vulnerability

MITRE CVE-2020-1350

概要

弊社は、弊社が製造する医用画像機器への本脆弱性の適用可能性の調査を継続しています。

- **対象となる可能性のある製品**

- 該当なし

- **該当しない製品**

- すべてのコンピュータ断層撮影装置
- すべての超音波画像診断装置

- **調査中の製品**

- なし

注：この脆弱性は、現在更新された分析を待っているものであり、最新の改訂版の時点での当社の最善の知見を示したものです。そのため、更なる解析が行われ、その結果が更新された場合には、内容が変更される可能性があります。

本件の問合せ先

……..

医療機関（医療機器のソフトウェアを管理）

■保有する医療機器のSBOM情報を確認

医療機器を構成するOS、ソフトウェアを確認

■ 公開CVE情報からNVD脆弱性情報を確認

影響を受けるOS,ソフトウェアの構成を確認
＞　影響を受ける可能性がある医療機器を確認

■製販業者のアドバイザリー情報で検証

影響を受ける医療機器を確認
＞　リスクアセスメントを実施し、至急対応、問合せ等

対応の実施

ソフトウェア部品表（SBOM）の変遷

IEC 62304 にみるSBOMの基礎情報

8 ソフトウェア構成管理プロセス
8.1 構成識別（クラス A、B、C）
8.1.2 SOUP の特定（クラス A、B、C）
現在使用中の SOUP 構成アイテム（標準ライブラリを含む）のそれぞれについて、次を文書化
a) 名称
b) 提供業者（サプライヤー）
c) SOUP を特定する識別子
識別子の例: バージョン、リリース年月日、パッチ番号、アップグレードの識別子など

3要素

8.1.3 システム構成文書の特定（クラス A、B、C）
構成アイテム及びそのバージョン一式の文書化

ただし、ここでは、SOUPはサードパーティ製コンポーネントとする。

OTS（サードパーティ製）
ソフトウェアの透明性確保

手引書改定案 表A-2 SBOMの最小限の要素

要　素	内　容
ソフトウェアコンポーネントのサプライヤーの名前	コンポーネントの作成、定義又は識別を行うエンティティ
ソフトウェアコンポーネントの名前	サプライヤーが定義してソフトウェアユニットに割り当てた名称
ソフトウェアコンポーネントのバージョン	以前のバージョンからの変更を特定するためにサプライヤーが用いる識別子
固有識別子	コンポーネントを識別するために使用する、又は関連するデータベースのルックアップキーとして機能する識別子
コンポーネントハッシュ（オプション）	コンポーネントのバイナリーを識別するために用いる暗号化ハッシュ
依存関係	上流のコンポーネントXがソフトウェアYに含まれているという関係を特徴づける情報
作成者名	SBOMエントリーの作成者
タイムスタンプ	SBOMデータの集約を行った日時の記録

7要素

MDS2（医療機器セキュリティ情報開示）の附属書　SBOM
（機械可読を目的としていない）

Software Name	Version	Creator
Windows 10 IoT enterprise 2019 LTSC	1809	Microsoft
Microsoft Visual C++ 2017 Redistributable (x64)	14.14.26429.4	Microsoft
SQL Server Browser for SQL Server 2014	12.2.5000.9	Microsoft

SQL Server、Visual C++、Visual Studio、Windows、Microsoftはマイクロソフトグループ企業の商標です。

サプライヤーのSBOM提供

製販業者のツール等を利用した探索

SBOMのフォーマットの例（機械可読の電子ファイル）

(1) SPDX（Software Package Data Exchange）ISO/IEC 5962:2021
・ライセンス情報含む）
・Tag-Value(txt)形式、RDF形式、xls形式、json形式、xml形式等
(2) CycloneDX　（セキュリティに特化）
(3) SWIDタグ（Software Identificationタグ）　ISO/IEC 19770-2:2015

id	サプライヤーの名前	コンポーネントの名前	コンポーネントのバージョン	固有識別子	関係	作成者	タイムスタンプ
1	Microsoft	Windows 10 IoT enterprise 2019 LTSC	1809	cpe:2.3:o:microsoft:windows_10:2019:*:*:*:enterprise_ltsc:*:*:* 0402EE03-3BF6-4243-A257-7FFFC088EEFF	Included in System Console	IKIREN	2023-08-19 T08:14:01Z
2	Microsoft	Microsoft Visual C++ 2017 Redistributable (x64)	14.14.26429.4	cpe:2.3:a:microsoft:visual_studio:2017:*:*:*:*:*:*:* or cpe:2.3:a:microsoft:visual_c++:*:*:*:*:*:*:*	Included in id#1	IKIREN	2023-01-21 T03:14:07Z
3	Microsoft	SQL Server Browser for SQL Server 2014	12.2.5000.9	cpe:2.3:a:microsoft:sql_server:2014:sp2:*:*:*:*:*:*	Included in System Console	IKIREN	2023-01-13 T05:54:00Z

医療機器のSBOMに関する要件（日本）

医療機器のSBOMに関連する代表的な通知等

令和5年3月31日　薬生機審発0331第11号 薬生安発 0331第4号　医療機器のサイバーセキュリティ導入に関する手引書の改訂について

医療機器のサイバーセキュリティ導入に関する手引書（第2版）（一部抜粋）

附 属 書　A.3 SBOMの要素と推奨フォーマット

医療機器のサイバーセキュリティについては、SBOMに用いるソフトウェア部品の構成管理情報として、最小限、IMDRFガイダンスに従った要素（表4)を含むことが望ましい。SBOM フォーマットについても検討することが必要であり、現時点（令和5年3月31日）では、自動化が可能な標準的なSBOM フォーマットは、限定的である（CycloneDX、SPDX及びSWID）。

表4 SBOM の最小限の要素

要素	内容
ソフトウェアコンポーネントのサプライヤーの名前	コンポーネントの作成、定義又は識別を行うエンティティ
ソフトウェアコンポーネントの名前	サプライヤーが定義してソフトウェアユニットに割り当てた名称
ソフトウェアコンポーネントのバージョン	以前のバージョンからの変更を特定するためにサプライヤーが用いる識別子
固有識別子	コンポーネントを識別するために使用する、又は関連するデータベースのルックアップキーとして機能する識別子
コンポーネントハッシュ	コンポーネントのバイナリーを識別するために用いる暗号化ハッシュ（オプション）
関係（依存関係）	上流のコンポーネント「X」がソフトウェア「Y」に含まれているというソフトウェアアーキテクチャー上の関係を特徴づける情報
作成者名	SBOMエントリーの作成者
タイムスタンプ	SBOMデータの集約を行った日時の記録

医療機器のSBOMに関する要件（日本）

医療機器のSBOMに関連する代表的な通知等

令和5年5月23日　薬生機審発0523第1号　医療機器の基本要件基準第12条第3項の適合性の確認について（一部抜粋）

高度管理医療機器若しくは管理医療機器の承認申請又は認証申請を行う製造販売業者等は、当該医療機器について基本要件基準第12条第3項への適合を示すため、JIS T 81001-5-1等への適合性を確認する際には、次の事項について留意して、当該結果を示すか又は当該結果をまとめた社内文書等を特定すること。なお、一般医療機器についても同様に確認が必要であること。

2. JIS に関連する既存通知等の要求事項

下記の項目については、規格への適合性を確認する際、追加で確認すること。

（4）JIS T 81001-5-1の箇条8のソフトウェア構成管理プロセスについて

構成管理プロセスは、当該医療機器のソフトウェア部品表（SBOM）を適切に作成することによって確認すること。

令和5年7月20日　事務連絡　医療機器の基本要件基準第 12 条第3項の適用に関する質疑応答集（Q&A）について（一部抜粋）

Q6：SBOM の構成として定められているものはあるか。

A6：SBOM は、JIS T 81001-5-1の箇条8の構成管理プロセスが対象としている全てのコンポーネント（ソフトウェアアイテム）で、自社製（開発委託したものも含む）及び外部調達ソフトウェア（OSS（オープンソースソフトウェア）を含む）が含まれるように作成すること。少なくとも製品の最上位のコンポーネント及びそれに直接含まれるコンポーネントの情報を含めること。

また、コンポーネントの各々について、①サプライヤの名前、②コンポーネントの名前、③バージョン、④固有識別子、⑤上流のコンポーネントとの関係、⑥作成者名（これらの情報を作成した組織名または担当者名）、⑦タイムスタンプ（情報を登録した日時）を明示すること。

（製販向け手引書通知の附属書 A ソフトウェア部品表（SBOM）の扱い参照）

BSI: サイバーレジリエンス要求事項に関する技術ガイドライン パート2 ソフトウェア部品表（SBOM）

サイバーレジリエンス法（CRA）は、2024年10月23日に正式に採択され、11月20日にOffice Journalに掲載され、12月11日に発効された。

CRAは製造業者にSBOMの作成を義務付けており、脆弱性管理プロセスを継続的に運用し、製品に関する情報を透明性があり包括的な形式で提供することを義務付けている。

欧州サイバーレジリエンス法（抜粋）

付属書I　サイバーセキュリティ必須要求事項　パート II 脆弱性ハンドリング要求

デジタル要素を含む製品の製造業者は次の事項を実施しなければならない：

1. デジタル要素を含む**製品に含まれる脆弱性とコンポーネントを特定し、文書化**する。

   これには、少なくとも製品の最上位レベルの依存関係を網羅する、一般的に使用され、機械可読な形式でソフトウェア部品表を作成することも含まれる。

付属書VII　技術文書の内容

8. 該当する場合、ソフトウェア部品表、市場監視当局からの合理的な要求に応じて付属書 I に規定されているサイバーセキュリティ必須要求事項への準拠を確認できるようにするために必要である。

※現時点（2025年1月20日）で、MDRとIVDR製品がサイバーレジリエンス法（CRA）の対象とされていないことにご注意ください。

BSI: Technical Guideline

- (V.2.0.0)TR-03183: Cyber Resilience Requirements for Manufacturers and Products, Part 2: Software Bill of Materials (SBOM)
  パート 2「ソフトウェア部品表（SBOM）」は、**ソフトウェア部品表（SBOM）の形式的及び技術的な要件について説明**

※上記技術ガイドラインの発行は2024年9月時点でのものであるため、CRAの文書に変更があった場合、修正される可能性があることに注意。

※ BSI（Bundesamt fur Sicherheit in der Informationstechnik、ドイツ連邦共和国IT・セキュリティ当局）の技術ガイドラインであり、CRA、MDR等のEU法令の要求・義務を満たすことを保証するものではない。

日本、米国、欧州の各規制、ガイドライン等におけるSBOMの詳細レベル

欧州サイバーレジリエンス法*

付属書I サイバーセキュリティ必須要求事項 パートII 脆弱性ハンドリング要求

デジタル要素を含む製品の製造業者は次の事項を実施しなければならない：

1. デジタル要素を含む製品に含まれる脆弱性とコンポーネントを特定し、文書化する。これには、**少なくとも製品の最上位レベルの依存関係を網羅する、一般的に使用され、機械可読な形式でソフトウェア部品表を作成**することも含まれる。

令和5年7月20日 事務連絡 医療機器の基本要件基準第 12 条第3項の適用に関する質疑応答集（Q&A）

Q6：SBOM の構成として定められているものはあるか。

A6：**少なくとも製品の最上位のコンポーネント及びそれに直接含まれるコンポーネントの情報**を含めること。

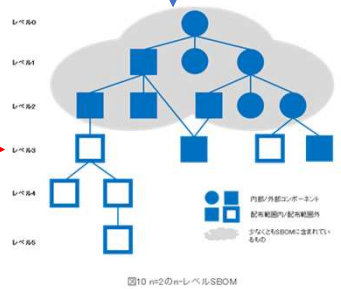


図10 n=2のn-レベルSBOM

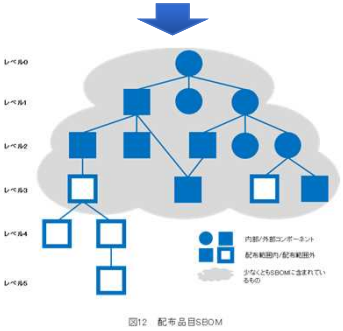


図12 配布品目SBOM

TR-03183 Part 2 8.2の図引用

NTIAフレーミング文書第3版

依存関係

最低限：プライマリコンポーネントと直接の依存関係に対して宣言された依存関係及び依存関係の完全性。

推奨： SBOMにリストされる全ての含まれているコンポーネントに対して宣言された依存関係及び依存関係の完全性。

高い目標： 可能な限り多くの動的コンポーネントやリモートコンポーネントとの依存関係及び関係の依存完全性を識別。

※ NTIAフレーミング文書第3版の「高い目標」はTR-03183 Part 2の「完全なSBOM」に該当しうるが、「推奨」については必ずしも該当するものがないことに注意する。FDAの申請時には、「完全なSBOM」又はそれに近い詳細レベルが求められる可能性がある。

BSI TR-03183 Part 2

コンテンツに要求される詳細レベル

本技術ガイドラインに準拠するには、**少なくとも配布範囲外にある最初のコンポーネントまでの各パスの下方で、配布範囲に含まれる各コンポーネントに対して再帰的な依存関係の解決を実行**する必要がある（「**配布アイテムSBOM**」を参照）。

https://www.bsi.bund.de/dok/TR-03183-en

***欧州サイバーレジリエンス法**
(https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act)
- **MDR及びIVDR対象製品には除外規定**がある。（2025/1/20現在）
- **電子カルテが具体的に記載**されている（MDRには該当しない）。
- **医療機関から医療機器のSBOMを提供を求められる可能性**が高い。

（参考） CRAのSBOMフォーマットとコンテンツへの要求

SBOMフォーマット

次の仕様とバージョンを満たし、且つ、JSONまたはXMLのフォーマット。

- CycloneDX　バージョン1.5以上
- Software Package Data eXchange (SPDX)　バージョン 2.2.1以上

コンテンツに要求される詳細レベル

- 技術ガイドラインTR-03183 Part 1に準拠するには、少なくとも配布範囲外にある最初のコンポーネントまでの各パスの下方で、配布範囲に含まれる各コンポーネントに対して再帰的な依存関係の解決を実行する必要がある（「配布アイテムSBOM」を参照）。
- このSBOMにはビルドプロセス中に利用できる情報と同じもの、またはビルドプロセスが存在しない場合には同等の情報が含まれている必要がある（「ビルドSBOM」を参照）。

SBOMの分類

SBOMが作成される方法やライフサイクル（コンポーネントの開発、配布、インストール、実行プロセスの一環として）に応じて、特定の状況で利用できるデータは異なり、SBOMに含めれる情報も異なる。一般的に次のSBOM分類がある。

1. 設計SBOM

SBOMは、新しいソフトウェア成果物に含まれるコンポーネント計画に基づいて作成される。
この時点ではコンポーネントがまだ存在する必要はない。

2. ソースSBOM

SBOMは、開発環境、ソースファイル、及び使用する依存関係から作成される。

3. ビルドSBOM

SBOMは、ソースファイル、依存関係情報、既成コンポーネント、揮発性ビルドプロセスデータ、その他のSBOMなどに基づいて、ビルドプロセスの一環として作成される。

4. 解析されたSBOM

SBOMは、ビルドプロセス後に、実行ファイル、パッケージ、コンテナ、仮想マシンイメージなどの成果物を解析して作成される。
このタイプは、「サードパーティSBOM」とも呼ばれている。

5. デプロイされたSBOM

SBOMは、システム上のソフトウェアのインベントリを提供する。
これは構成オプションと（シミュレートされた）デプロイ環境での実行動作の検証を考慮した他のSBOMのコンパイルの可能性がある。

6. ランタイムSBOM

SBOMはソフトウェアを実行するシステムにより作成され、実行中のコンポーネントと外部（プログラム）呼び出し、及び実行時にのみ動的にロードされるコンポーネントをキャプチャする。
このタイプは「動的SBOM」と呼ばれる。

「CISA Open Working Group on SBOM Tooling and Implementation. Types of Software Bill of Materials (SBOM) Documents. 2023」に上記と同様な分類と説明があり、「CISA: Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) 3rd Ed.」にも参照されている。（タイプ（Type ）要素）
https://www.cisa.gov/sites/default/files/2024-10/SBOM%20Framing%20Software%20Component%20Transparency%202024.pdf

SBOMの国際的な技術的仕様　「BSI TR-03183 Part 2ソフトウェア部品表 (SBOM)」のまとめ

この技術ガイドラインは医療機器開発においても参考になる。

- サイバーレジリエンス法（CRA）は、2024年10月23日に正式に採択され、11月20日にOffice Journalに掲載され、12月11日に発効された。
- CRAは製造業者にSBOMについて、**脆弱性マネジメントプロセスを継続的に運用し、製品に関する情報を透明性があり包括的な形式で提供することを義務付け**ている。
- EU CRAの付属書 I と付属書 II で課される、製造業者及び製品への要求事項、推奨事項、検証、評価手順を事前確認することを目的に、より実践的な技術ガイドラインTR-03183が発行され、その内Part 2がSBOMについての詳細を規定している。
- SBOMフォーマットには、**CycloneDXバージョン1.5以上またはSPDXバージョン2.2.1以上の仕様**と、**JSONまたはXMLのフォーマット**が求められる。

ヒント：**フォーマットは今後も変化し、また医療機関の求めに応じて指定されたフォーマットで提出することになるので、開発者は SBOM情報が欠落しないような何らかの中間ファイルで管理し、必要なフォーマットに変換する手順をもつ**とよい。

- コンテンツに要求される詳細レベルとして、配布アイテムSBOMが求められ、且つ、含まれるべき情報として、**SBOM分類の「ビルドSBOM」かそれと同等の情報**が求められる。

2. SBOM運用フレームワークの確立

CISA: Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)　September 3, 2024

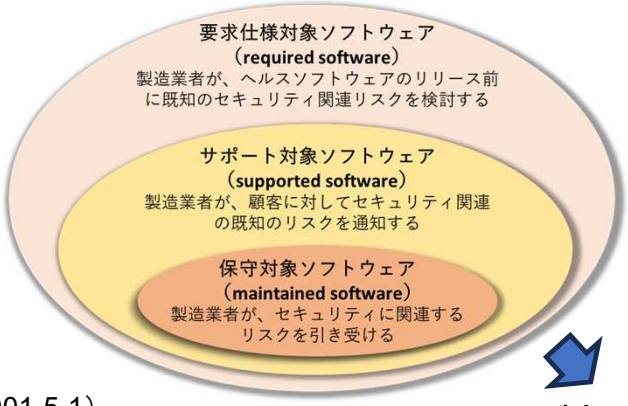
ソフトウェアコンポーネント透明性のフレーミング：共通のソフトウェア部品表（SBOM）の確立、第3版

https://www.cisa.gov/sites/default/files/2024-10/SBOM%20Framing%20Software%20Component%20Transparency%202024.pdf

NTIAフレーミング文書の「第2版 (2021年)」と「第3版 (2024年)」の間の主な変更点

第2版(2021年)と第3版(2024年)との間の主な変更点

- SBOMの各ベースライン属性への期待値を明確化
  - ライセンスと著作権所有者の2つのベースライン属性を追加
  - 複数の要素に対して、成熟度レベルの導入
  - 未宣言のSBOM情報に対して選択肢を追加
- SPDX及びCycloneDXフォーマットへの要素のマッピングを更新
  - 既存フォーマットとしてのSWIDを削除
- SBOM利用プロセスの一環としてリスクマネジメントの概念を追加
- 用語の追加、　他



IEC 81001-5-1(JIS T 81001-5-1)
4.3 リスク移転に関連するソフトウェアアイテムの分類

第2版(2021年)と第3版(2024年)の間のベースライン属性(属性)の比較

第2版	第3版
作成者名	作成者名
タイムスタンプ	タイムスタンプ
	タイプ
	プライマリーコンポーネント
サプライヤー名	サプライヤー名
コンポーネント名	コンポーネント名
バージョン	バージョン
コンポーネントハッシュ (オプション)	コンポーネントハッシュ
固有識別子	固有識別子
依存関係	依存関係
	ライセンス
	著作権所有者

サプライチェーンの透明性

ソフトウェアサプライ チェーンの透明性を高めるために、第3版では、SBOMの作成と共有、役割及び サプライチェーンのSBOM統合について説明している。

製品のEOL/EOS決定のベース

SBOMの要素

- 最低限の要求として**ベースライン属性**が必要。
  メタ情報は、作成者名、タイムスタンプ、プライマリーコンポーネント(もしくは依存関係のルート)の要素を含み、その他の要素はプライマリーコンポーネントの直接的または推移的な依存関係のあるコンポーネントに適用される。
- その上で様々なSBOMユースケース(脆弱性マネジメント、VEX情報共有等)を有効としていくためにも、必要に応じて、補足属性及び要素を含めることを推奨。

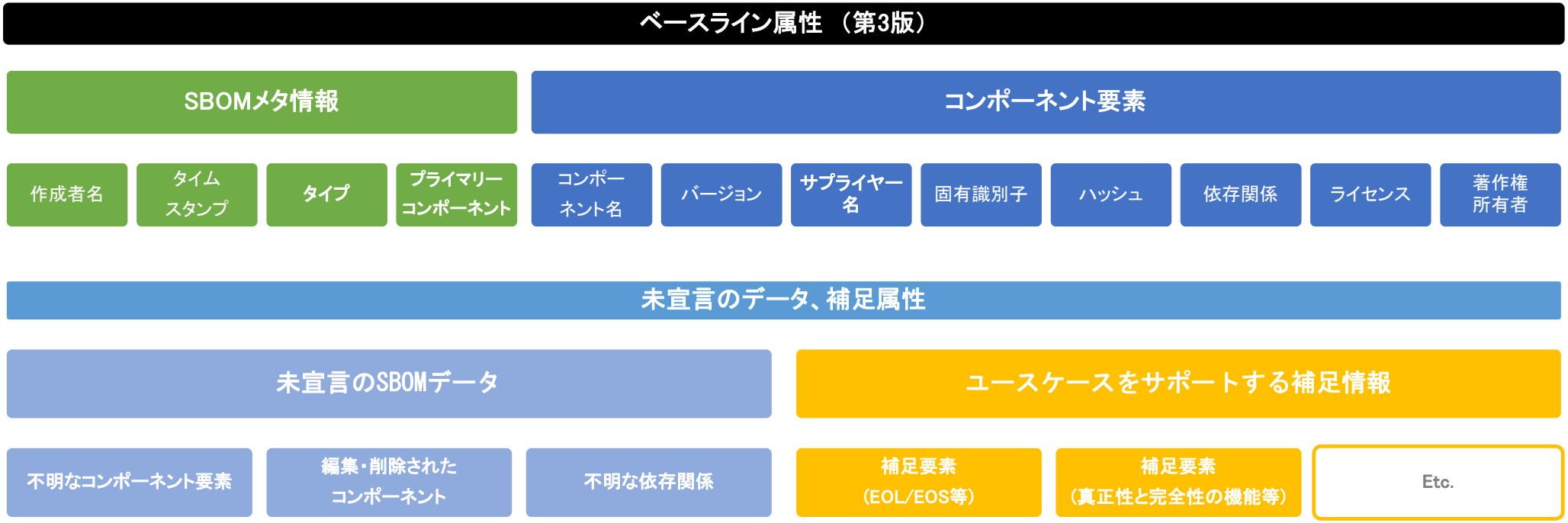


図1 ベースライン属性と追加的、補足的な要素と要素 （第3版）

ベースライン属性

要素における3つの成熟度レベル（「最低限期待されるもの」、「推奨プラクティス」、「高い目標」）は、各要素で提供される内容と、成熟度を高めるために可能なアプローチを説明している。

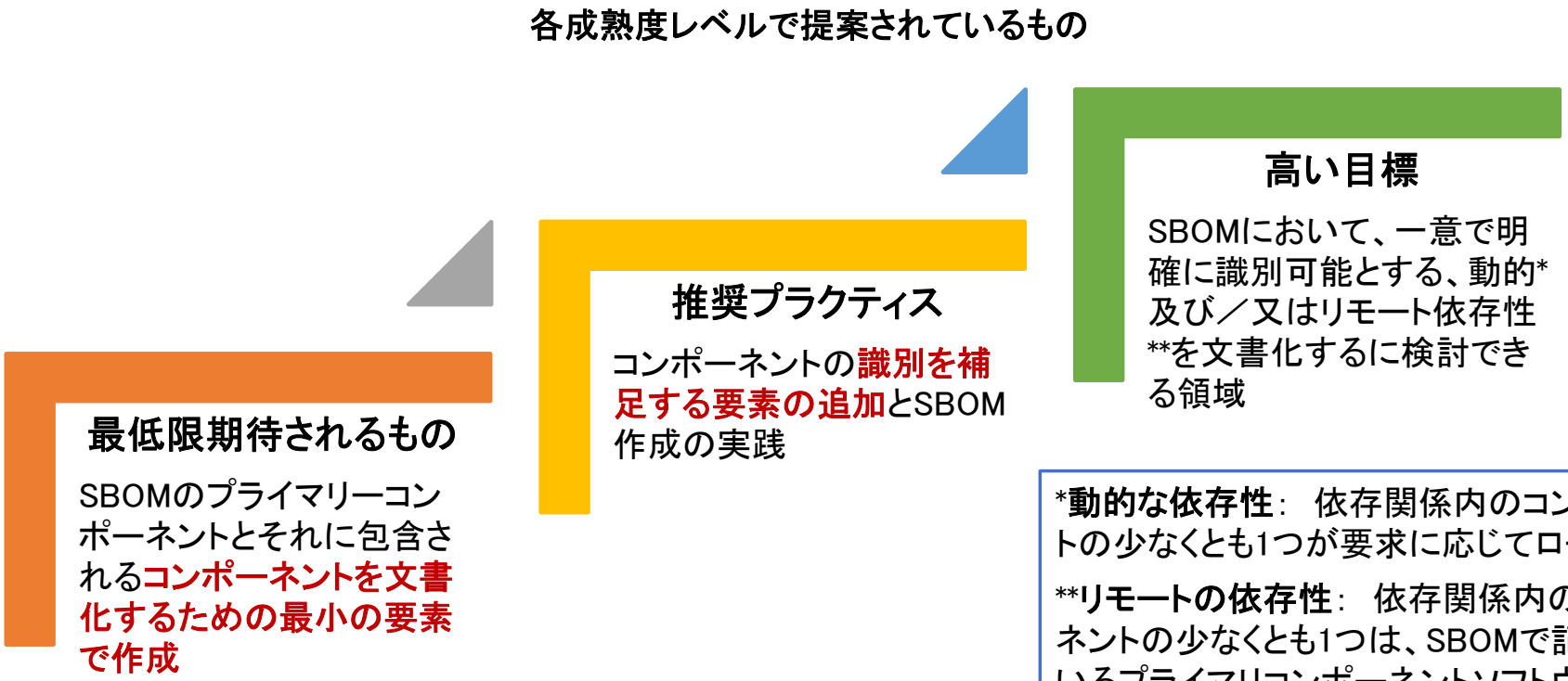


図3 SBOM成熟度レベル（第3版）

SBOM情報と依存関係の事例

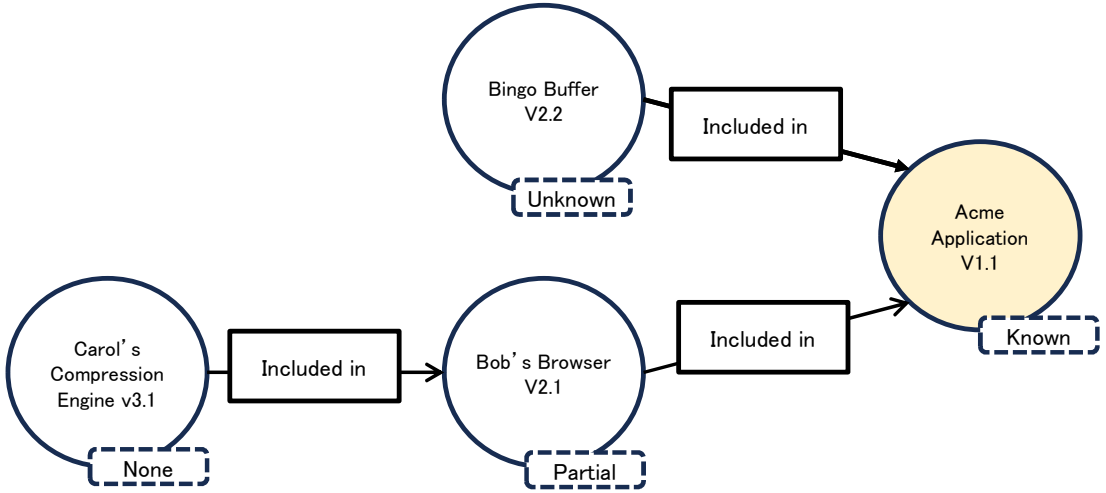


図6 上流の依存関係の完全性を伴った概念的SBOM図

表8 上流の依存関係の完全性を伴った概念的なSBOM表

コンポーネント名	サプライヤー名	バージョン文字列	作成者	ハッシュ	個別識別子	依存関係	依存関係の完全性
Application	Acme	1.1	Acme	0x123	234	Primary	Known
|--Browser	Bob	2.1	Bob	0x223	334	Included in	Partial
|--Compression Engine	Carol	3.1	Acme	0x323	434	Included in	None
|--Buffer	Bingo	2.2	Acme	0x423	534	Included in	Unknown

*表は例示のために、タイムスタンプ要素は省略され、他の要素名は短縮されていることに注意する。

ソフトウェア利用者が所有するSBOMの事例 ― 羅層構造

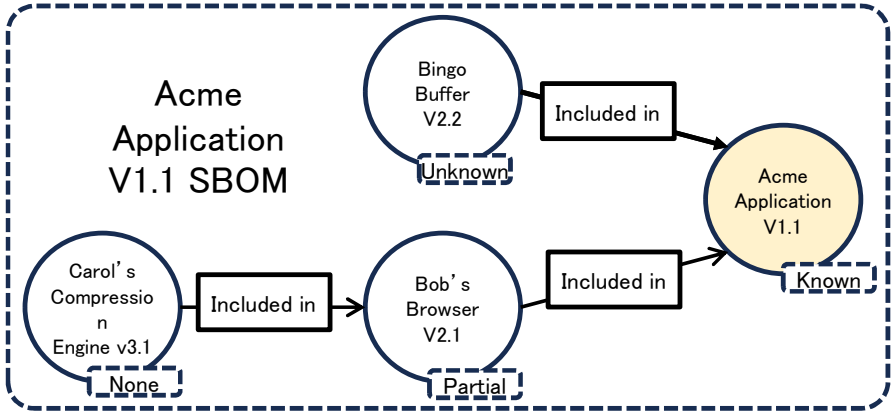


図6 のサプライチェーンのSBOM図（一つのSBOM）

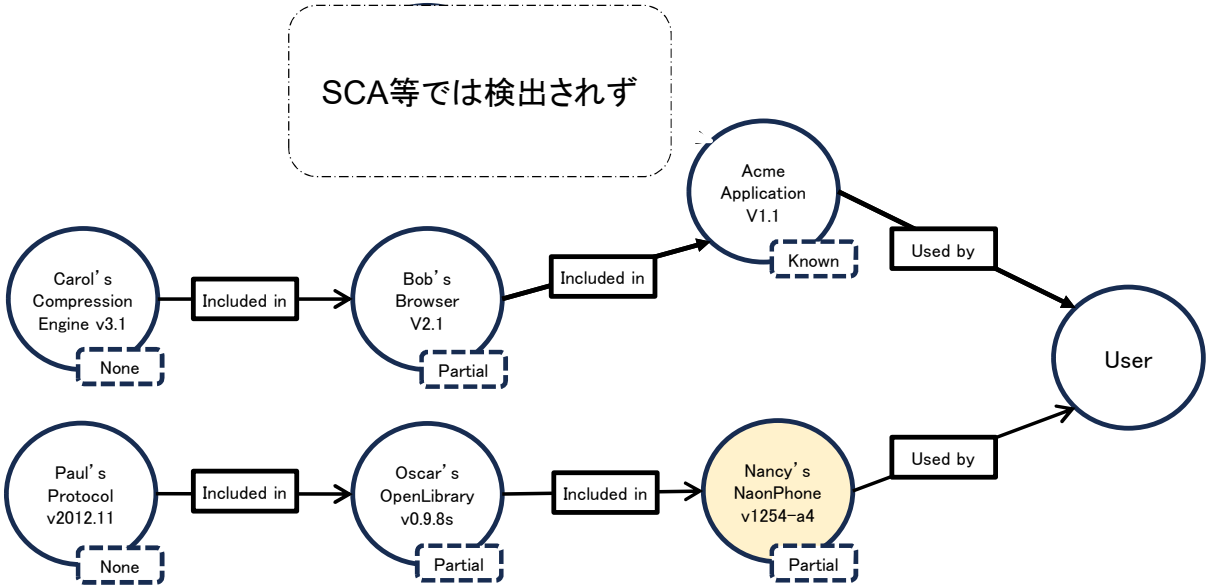


図7 2つのサプライチェーンを含むSBOM図

表9 NancyのNanoPhoneの概念的なSBOM表の例

コンポーネント名	サプライヤー名	バージョン文字列	作成者	ハッシュ	個別識別子	依存関係	依存関係の完全性
NanoPhone	Nancy	v1254-a4	Nancy	0x523	237	Primary	Partial
|--OpenLibrary	Oscar	0.9.8s	Nancy	0xA23	394	Included in	Partial
|--Protocol	Paul	2012.11	Nancy	0xB53	934	Included in	None

*表は例示のために、タイムスタンプ要素は省略され、他の要素名は短縮されていることに注意する。

ソフトウェア利用者が所有するSBOMの事例 ー 羅層構造

サプライヤー提供の
SBOM活用

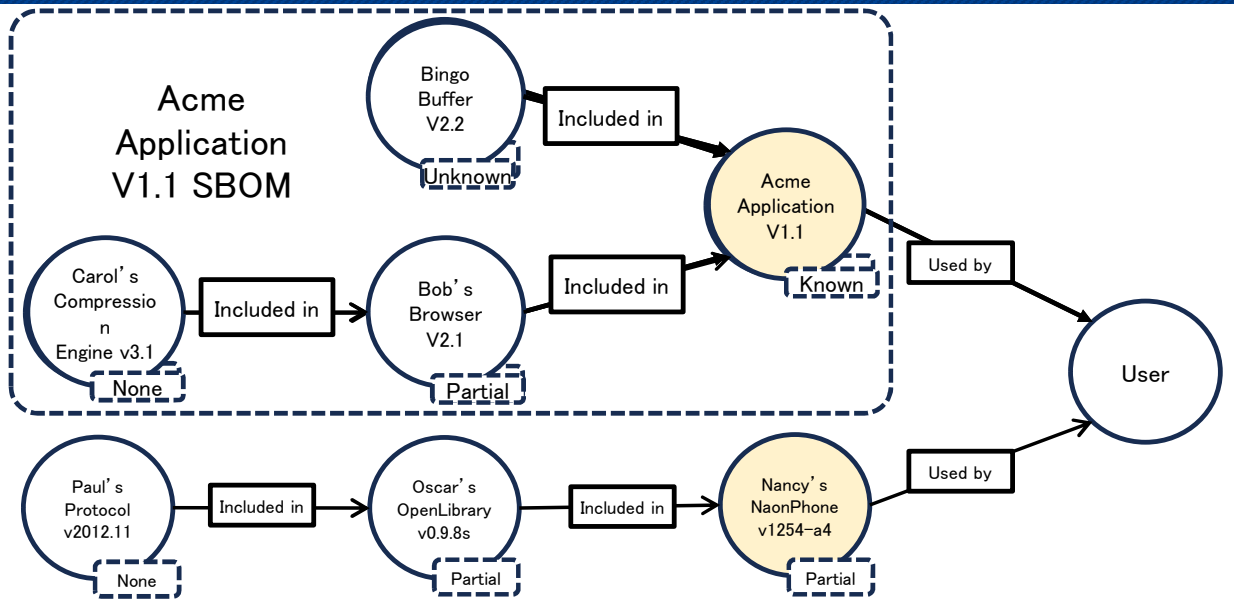


図7 2つのサプライチェーンを含むSBOM図

表9 NancyのNanoPhoneの概念的なSBOM表の例

コンポーネント名	サプライヤー名	バージョン文字列	作成者	ハッシュ	個別識別子	依存関係	依存関係の完全性
NanoPhone	Nancy	v1254-a4	Nancy	0x523	237	Primary	Partial
|--OpenLibrary	Oscar	0.9.8s	Nancy	0xA23	394	Included in	Partial
|--Protocol	Paul	2012.11	Nancy	0xB53	934	Included in	None

*表は例示のために、タイムスタンプ要素は省略され、他の要素名は短縮されていることに注意する。

SBOM運用フレームワークの確立

- 医療機器ソフトウェアの透明性を高め、医療機関がネットワークのセキュリティをより適切に管理できるようにし、医療機関の管理者がコンポーネントを監視できるようにする方法の一つとして、**国際調和のとれたSBOM運用のフレームワークの確立が必要**である。
- 迅速なSBOMの導入のために最低限のベースライン属性が定義されており、基本的に、SPDX、CycloneDXなどの既存フォーマットと一致しているが、**これらのベースライン属性のみでは多数のユースケースに対応するに不十分**である。それ故、**CISAフレーミング文書の第3版では様々なSBOMユースケースを有効にしていくために、補足要素を含めることも推奨**している。
- **信頼できるサプライヤー提供のSBOMを活用**して、製品全体のSBOMを構成する。
- **SBOM使用の成熟度が増すと、より調整・標準化されたSBOMの共有手法・管理手法の確立が促進される**。

製品ライフサイクルとSBOMをリンクするような仕組みをSBOM情報に含める動き → SBOM構造の拡張・更新

医療機器の製品ライフサイクル（EOL/EOS等）を決定する**背景情報の一部として管理**

3. SBOM関連の課題と緩和策

Data Normalization Challenges and Mitigations in Software Bill of Materials Processing（MITRE） Oct 24, 2024

ソフトウェア部品表処理におけるデータ正規化の課題と緩和策

https://www.mitre.org/news-insights/publication/data-normalization-challenges-mitigations-software-bill-materials-processing

SBOM関連の課題　ー　SBOM要素の正規化

- 課題を理解した上で、利用ルールを検討

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	固有識別子	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

Naming Rule

作成の単位で割りつけられる

CPEの問題は未解決
（この例は、serialNumber、component/cpe）

多数の言い回しがある
マージした場合にID＃の
リンクが壊れないように注意

※ CPEの命名規則

- **CPE：Common Platform Enumeration**、共通プラットフォーム一覧
  - CPEは、米国政府が推進している情報セキュリティにかかわる技術面での自動化と標準化を実現する技術仕様SCAP(Security Content Automation Protocol)(*2)の構成要素のひとつ
    - IPAの解説： https://www.ipa.go.jp/security/vuln/scap/cpe.html
- cpe：/{種別}:{ベンダ名}:{製品名}:{バージョン}:{アップデート}:{エディション}:{言語}
  - 大文字と小文字の区別はない
  - 基本構成のそれぞれの箇所が空白の場合、「全て」を意味する。例えばバージョンが空白の場合、全てのバージョンの意味。

CPE例
microsoft:windows_2000::sp4:pro

SBOMベースライン属性とデータ正規化の課題

NTIAフレーミング文書（第2版）*が定義するコンポーネントとその依存関係を識別するためのSBOMベースライン属性

*Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM), 2nd edition
ソフトウェアコンポーネント透明性のフレーミング：共通のソフトウェア部品表（SBOM）の設立、第2版
https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf

表1 SBOMベースライン属性

要素名	要素タイプ	説明
作成者名	メタ情報	SBOM作成者
タイムスタンプ	メタ情報	SBOMが最後に更新された日時
サプライヤー名	コンポーネント要素(必須)	SBOMエントリ内のコンポーネントのサプライヤーの名前またはその他の識別子
コンポーネント名	コンポーネント要素(必須)	コンポーネントの名前またはその他の識別子
バージョン文字列	コンポーネント要素(必須)	コンポーネントのバージョン
コンポーネントハッシュ	コンポーネント要素(推奨)	コンポーネントの暗号化ハッシュ
固有識別子	コンポーネント要素(必須)	コンポーネントを一意に定義するのに役立つ追加情報
依存関係	コンポーネント要素(必須)	SBOMコンポーネント間の関連付け

これらの要素の内容・中身、フォーマットの不一致があると、データ正規化の課題が発生する可能性がある。

データ正規化の課題：

- SBOMの要素全体に共通する課題
- 特定のSBOM要素に特有の課題

IMDRF N73 Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity
「医療機器のサイバーセキュリティ導入に関する手引書（第2版）」でも推奨されている最小限のSBOM要素の構成（表4参照）

データ正規化の課題

- データ正規化の課題の根本要因
- SBOMの要素全体に共通する課題と検討事項
- 特定のSBOMの要素に特有の課題と検討事項

課題につながる根本要因

- SBOM採用の成熟度
- SBOM作成プロセスの複雑さ
- 製品ラインの複雑さ
- 規格の限界

SBOMの要素全体に共通する課題

- 内容/フォーマット
- エンコーディング（符号化）
- 日付/時刻
- 欠測データ
- 複数の「信頼できる情報源」
- 経時的な変更

特定のSBOMの要素に特有の課題

- コンポーネント名
- サプライヤー名
- バージョン
- 依存関係
- 識別子のその他の問題
- 追加の要素
- 脆弱性情報

課題につながる根本要因

SBOM採用の成熟度

SBOMを作成する組織の成熟度の段階はそれぞれ異なるため、**様々な情報源（サードパーティーサプライヤー等）から入手するSBOM要素に正規化の課題**が生じる。

SBOM作成プロセスの複雑さ

様々なSBOM作成のバリエーション（サプライヤーから受領、自社でのマニュアル作成、開発のビルドツール、パッケージマネージャ、ソフトウェアコンポジション解析ツール）**により、命名法、データのフォーマット等が異なりデータ正規化の問題**が生じる。

製品ラインの複雑さ

複数の製品ライン間でのソフトウェア構成管理、SBOM管理のプロセス（異なる取得手法、異なるツール・レポジトリ、異なるフォーマット設定、複数のSBOM管理、異なる開発環境下）が複雑化して、データ正規化の問題の原因となる。

規格・仕様の限界

異なるSBOM規格(SPDX、CycloneDX等)はSBOM要素を指定して、それらがNTIAのベースライン属性にマップされるが、**要素の内容とフォーマットは厳格には指定されておらず、複数の命名とフォーマット設定の使用に至る**。

SBOMの要素全体に共通する課題

課題	説明	例	
内容/フォーマット	使用されているフォーマットによって異なる可能性	大文字小文字の区別 略語 単語区切り ディレクトリ区切り文字 頭字語	大文字、小文字、混在 “Corp.” 、“Corporation” “Product Name”、“Product-Name” “/” 、“¥" “ACME Bow Company [ABC]”
エンコーディング	エンコーディングの不一致で、元データが保持されず文字化け等が発生する可能性	必ずしもユニバーサルエンコーディング（UTF-8など）が使用されていない。	
日付/時刻	異なる方法で表現可能なため、不整合が発生し、ツールが同等の日付を照合するのを困難にさせる。	2024年3月26日	“2024-03-26”（ISO 8601*）、”03/26/24”
欠測データ	複数コンポーネントのSBOMを、より大きなSBOMに統合するために解析をして、重複コンポーネントを検出する際、欠測データがあると重複が検出できない可能性がある。		
「信頼できる情報源」	異なるSBOMツールにより作成されるデータ要素にバリエーションが生じ、単一の「信頼できる情報源」が存在しない。	パブリックでは利用されないプロプライエタリコンポーネント	自動化メカニズムによる異なる結果の作成の可能性 （機械学習により構築されたモデル等）
経時的な変更	経時的な変更が適切に対処されない場合、重複情報を特定・除去する作業の妨げになる。	名称の変更	• リブランディング、合併等による組織名変更 • オープンソースにおける派生による製品名又はコンポーネント名の変更

特定のSBOM要素に特有の課題

課題	説明	例	
コンポーネント名	同一製品とバージョンであっても、異なる規格(例：CPEやPURL（package URL）)の導入によりSBOM内で異なる表示が存在する可能性		
サプライヤー名	同一サプライヤーであっても異なる名称のため、複数のSBOMを処理する際に統一性の問題が生じる場合 同一製品について複数の異なるサプライヤー名が存在する場合	接尾辞 所属 製品を開発・配布する組織とは別に、製品を販売する法人が存在	Co.” or Limited Liability Company “LLC” “X,” “Y,” 、“X, a Y Company” “DBA”、“doing business as”
バージョン	商品の名称、識別、引用方法に多くのバージョンが存在	番号 日付 コード名 バージョンインジケーター Gitハッシュ/タグ	“4.10.8”、アドホックなスキーム バージョンがタイムスタンプを含む場合 Apple MacOS 12 “Monterey” “version”、“v”、“6.x before 6.10” コードの「バージョン」に関連付けるラベル
依存関係	SBOM作成ツール、その他手法により、依存関係の表現が異なる可能性 広く認知されているフォーマット（Cyclone DX、SPDX等）以外での、データ表現がある可能性		
識別子に関するその他の問題	SBOMに含まれる全てのコンポーネントに対して、単一の固有識別子を提供する規格は存在しない。	**組織がCPEフォーマットに従って作成したとしても、プライベートな識別子となる。**	PURLは同一コンポーネントが複数の名前をもつ可能性がある。
脆弱性情報	**製品名、バージョン、コンポーネント名等の要素の正規化問題が、脆弱性評価と管理の不正確さにつながる可能性**		

データ正規化に関する課題に対する緩和策例

- 技術的な緩和策
- ポリシー及びプロセスによる緩和策
- SBOMエコシステムの確立

技術的な緩和策

- 正規の名称と表現の使用
- ツールの検討
- ベースライン属性と追加情報

ポリシー及びプロセスによる緩和策

- SBOMレポジトリの一元化
- SBOM収集の仕組み整備
- SBOMプロセスの改善

SBOMエコシステムの確立

- ツール進化の促進
- SBOM関連規格の改訂等
- 集中型情報源とサービスの提供

データ正規化に関する課題に対する緩和策例

- **技術的な緩和策**
- ポリシー及びプロセスによる緩和策
- SBOMエコシステムの確立

技術的な緩和策

正規の名称と表現の使用

ツールの検討

ベースライン属性と
追加情報

技術的な緩和策

正規の名称と表現の使用

- **正規の名前/表現のセットを作成し、生データとして表示される名前/表現に対してマッピング**を行う。この際、「SBOMの要素全体に共通する課題」と「特定のSBOM要素に特有の課題」で説明がある各要素の正規化を考慮すること。

ツールの検討

- **データ項目の照合、異なるエンコーディング方式の検出・解決、異なるフォーマット間の変換の正規化の問題解決に役立つツールを入手または開発を検討**する。ツールには限界があるのでアドホックなスクリプトの作成も検討する。

ベースライン属性と追加情報

- EOL/EOSの日付
  サプライヤーがEOLとEOSに対して独自の用語を使用する可能性があるため、**IMDRFの用語を採用して、それら独自の用語にマッピング**する。

正規化のルール化（文書）とツール化

データ正規化に関する課題に対する緩和策例

- 技術的な緩和策
- **ポリシー及びプロセスによる緩和策**
- SBOMエコシステムの確立

ポリシー及びプロセスによる緩和策

- レポジトリの一元化
- SBOM収集の仕組み整備
- SBOMプロセスの改善

ポリシー及びプロセスによる緩和策

レポジトリの一元化

- **一元化されたサービスリポジトリ**/集約エイリアスデータベース(CAD)を開発・維持して、主要な情報源を確保する。

SBOM収集の仕組み整備

- **サプライヤー等との契約文書に機械可読なフォーマットのSBOM開示要求を含める**。

SBOMプロセスの改善

- **SBOM手順を確立して、文書化、変更等への対応を確実**にする。
- **SBOM作成プロセスの定期的な評価**、必要に応じて問題解決を行い、ツール取得要件やプロセス改善も検討する。
- **SBOMの成熟度の目標を計画**する。

SBOMプロセスのサプライチェーンへの展開

データ正規化に関する課題に対する緩和策例

- 技術的な緩和策
- ポリシー及びプロセスによる緩和策
- SBOMエコシステムの確立

SBOMエコシステムの確立

- ツール進化の促進
- SBOM関連規格の改訂等
- 集中型情報源とサービスの提供

SBOMエコシステムの確立

ツール進化の促進

- **ツールは今後急速に進化することが期待**されており、ツール選定にあたって正規化の問題に対応可能かも考慮され、比較・評価されていく。評価は製造販売業者でも業界団体でも行うことができ、**ツールの進化を促進**させる。

SBOM関連規格の改訂等

- SBOMデータフォーマット等はでは十分に規定されておらす、規格のアップデートまたは補足文書、事例で対処されていく。**製造販売業者が標準化WGに参画して改善へ貢献する**ことも期待される。

集中型情報源とサービスの提供

- 業界団体はデータ正規化の課題に対処するため、**集中型情報源とサービスを検討**することが期待される。

SBOMエコシステム確立活動への参画

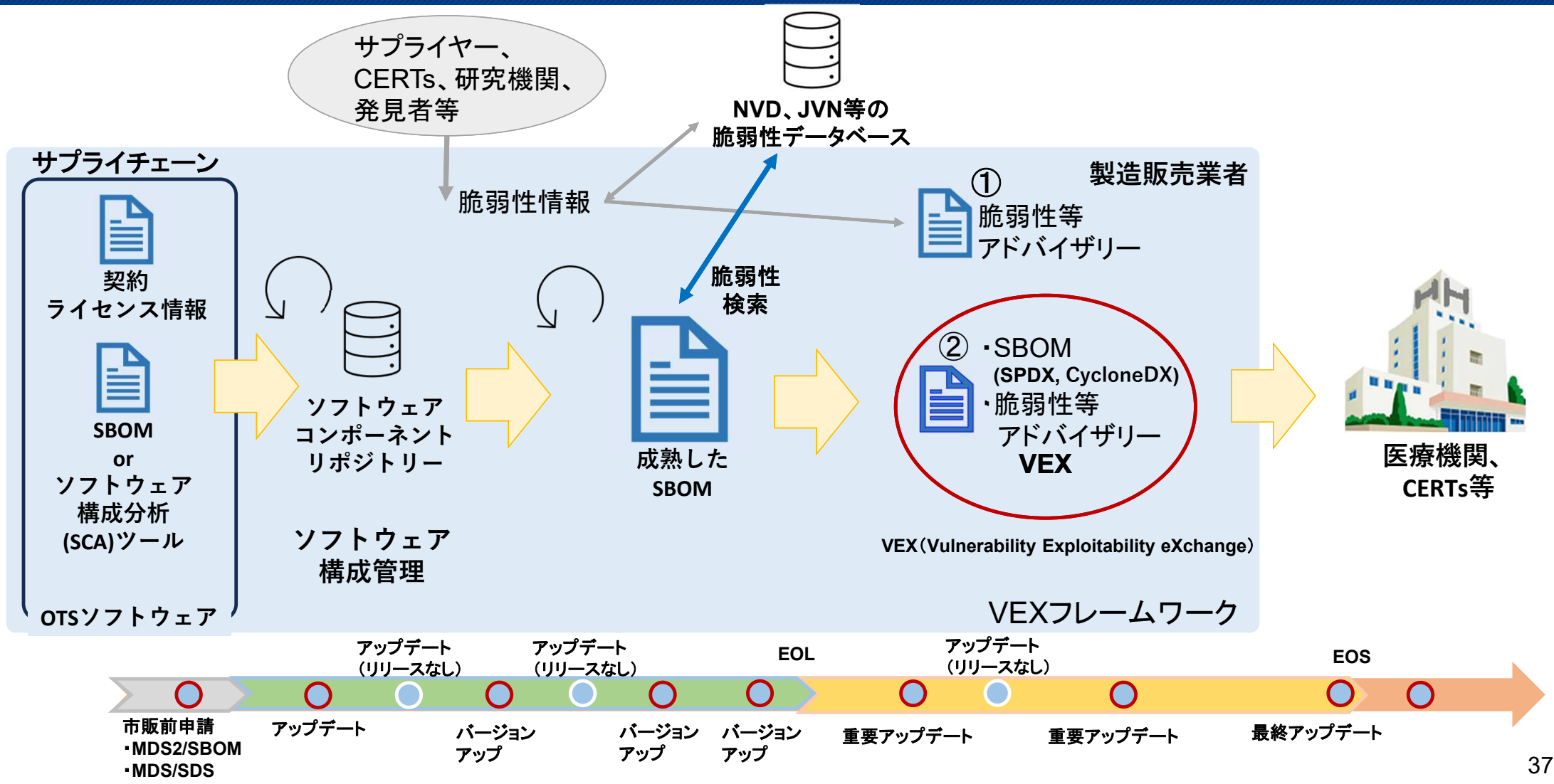
SBOMにおけるデータの正規化課題と緩和策

- SBOMは、医療機器のソフトウェアセキュリティ及びソフトウェアサプライチェーンのリスクマネジメントにおける強力なツールであるが、**正規化の課題がSBOMの作成と活用の有効性を妨げている恐れ**がある。
- SBOMデータ、特にベースライン属性と追加データ等を効果的に使用するには、**一貫した命名法とデータフォーマットを使用して正規化する必要**がある。
- データ正規化の課題には大別すると、「ベースライン属性に共通するもの」と「個々の要素に関係するもの」があるが、これらの課題に対処するため、**ベースライン属性と追加情報に関わる正規化の課題への技術的な推奨事項やプロセス・ポリシーによる推奨事項等、考え得る緩和策が提案**されている。
- ツールの改善・発展、SBOM規格の改訂、業界団体主導の集中型情報源とサービスも、SBOMエコシステムの発展の観点から提案されている。

SBOMの正規化ルールとプロセス確立が重要　⇔　SBOM仕様の拡張・更新、ツールの改善

4. まとめ

SBOMの効果的活用　ー　自動化に向けて



SBOMの効果的活用　―　製造販売業者が継続して取り組む課題

SBOMの効果的活用

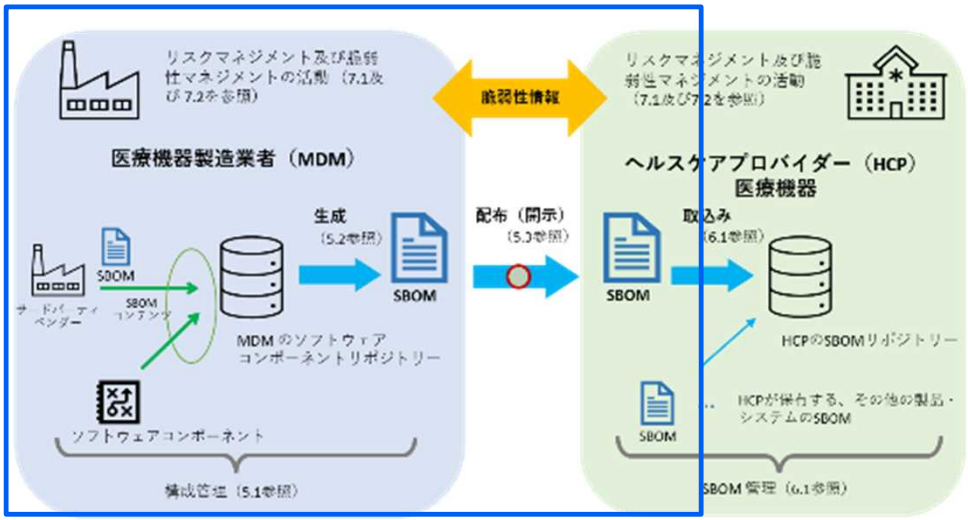
SBOMは、医療機器のソフトウェアセキュリティ及びソフトウェアサプライチェーンのリスクマネジメントにおける強力なツールである。しかし、正規化等の課題がSBOMの生成と活用の有効性を妨げている。
効果的にSBOMを活用するためには、SBOMデータ及びプロセスに関する課題を緩和し、将来のVEXフレームワーク構築のための基礎を確立することが重要である。

継続して取り組む課題

- ソフトウェアの管理強化
- **セキュリティポリシーの明確化（脆弱性情報、SBOM、アドバイザリーの扱い等）**
- **サプライチェーンマネジメントの強化**
- **医療機関との連携及び積極的な情報提供**

国際的エコシステム確立に関する活動への参画

- SBOM関連規格
- VEXフレームワーク



VEXフレームワークの構築及び確立

ソフトウェア部品表（SBOM）の作成と運用

ご清聴ありがとうございました。