IMDRF International Medical Device Regulators Forum

最終文書

IMDRF/CYBER WG/N73FINAL:2023

医療機器サイバーセキュリティのためのソフトウェア部品表の原則及び実践

AUTHORING GROUP

IMDRF サイバーセキュリティワーキンググループ

序文

Andrzej Rys, IMDRF 議長

目次

1. はじめに

医療機器がデジタルに接続できることで、患者ケアは、より効率的になり、データに基づいて行われ、効果的になってきている。そうした医療機器の開発は、サードパーティのソフトウェアコンポーネントを活用し、必要とすることで、さらに経済的になり、信頼性が向上し、イノベーションが加速している。サードパーティのコンポーネントを活用することによって、多くのベネフィットが提供される一方で、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のリスクがもたらされる可能性がある。

共通のソフトウェアコンポーネントを使用することによって、脆弱性が様々な製造業者の一見セキュアで無関係な医療機器に対していろいろな影響を及ぼす可能性があり、この点でサイバーセキュリティの脆弱性は、独特である。この問題は、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。この世界的な問題に取り組むため、2018 年に NTIA（National Telecommunications and Information Administration、米国電気通信情報管理局）は、関係する様々な分野の主導的立場の人を会議に招集して、ソフトウェアの透明性について議論した。アウトプットの一つは、SBOM（Software Bill of Materials、ソフトウェア部品表）の概念であり、NTIA は、特定した複数のコンポーネント、それらの関係及びその他の関連情報のリストとして SBOM を定義した。この取組みは、SBOM の開発及び採用に国際的に影響を与えてきた。

SBOM は、市販前及び市販後の両方の活動において［すなわち、製品ライフサイクルの全体（TPLC、Total Product Life Cycle）において］、サイバーセキュリティのリスクマネジメントプロセスを改善するために活用可能なリソースである。例えば、市販前の段階においては、MDM（Medical Device Manufacturer、医療機器製造業者）は、SBOM リソースを機器開発中に用いて、既知のソフトウェア脆弱性を追跡し、既知のサイバーセキュリティリスクがある状態でのリリースを防ぐことが可能である。市販後においては、MDM は、脆弱性監視プロセスを補助するリソースとして、市場にあるリスクのある機器を特定するために、SBOM を使用することが可能である。

SBOM は、一次又は二次リソースとして、製品ライフサイクルの全体にわたるサイバーセキュリティのリスクマネジメントプロセスの改善を支援することが可能である。ベネフィットには次を含めてよいが、これに限定するものではない。

- 機器のソフトウェアコンポーネントのより速い、より包括的な特定
- 情報を受けたうえでの意思決定をさらに徹底して行う、よりセキュアなソフトウェア開発
- ベンダー及び利害関係者間におけるソフトウェア透明性の向上

SBOM のベネフィットを最大限に得るためには、SBOM は、その他のサイバーセキュリティのリスクマネジメントツール及び「医療機器サイバーセキュリティの原則及び実践（IMDRF/CYBER WG/N60FINAL:2020。以下、IMDRF N60 ガイダンスという。）」に記載された手順とともに用いることが望ましい。IMDRF N60 では、SBOM は、製造業者が作成して機器のユーザーに提供する、顧客セキュリティ文書の一部としている。医療機器の SBOM は、製品ライフサイクルの全体を通して MDM 及びヘルスケアプロバイダーの両方にメリットがある。例えば、SBOM は、ソフトウェアコンポーネントの EOL（End of Life、製品寿命終了）を追跡して準備するための効果的な管理ツールである。MDM がソフトウェアコンポーネント及びその EOL 期日に対する知識を有する場合は、MDM は、

関連するリスクに対して、自社及びその顧客のよりよい準備をすることが可能になり、MDM の品質管理能力を改善する。機器のユーザーは、透明性の向上及びサイバーセキュリティの情報開示によってベネフィットを得ることができ、それによって個々のリスクプロファイル及びサイバーセキュリティ能力に基づいてサイバーセキュリティ活動を実施することが促される。例えば、ヘルスケアプロバイダーは、購入前及びインストール前に提供される SBOM によって、どの機器が自身のリスクプロファイルに合致してデプロイ可能か、サイバーセキュリティの問題を引き起こしかねない古いソフトウェアが含まれていないかを購入前に知ることが可能である。製造業者は、製品とともにソフトウェア部品表（SBOM）を供給することが望ましい。SBOM は、これら全ての HCP の様々なニーズ、リソース及び能力をサポートする必要がある。SBOM の採用が増え、ツール、サービス及びサイバーセキュリティの成熟度が進展することで、HCP は、SBOM を最大限に活用できるようになるだろう。加えて、SBOM が提供される場合は、顧客（HCP や患者の場合がある）は、機器のサイバーセキュリティのリスクをより適切に評価可能である。

市販前申請において規制当局に提出される SBOM は、MDM が成熟したサイバーセキュリティプログラムを有することの一つの指標である。SBOM によって、規制当局は、製品についてのベネフィットリスク評価をより完全に行えるようにもなる。市販後においては、市場のどの製品が SBOM にアクセスできるかをさらに広範囲に理解することで、MDM、HCP（Healthcare Providor、ヘルスケアプロバイダー）及び規制当局は、MDM からのインプットを受けて、脅威、脆弱性及びエクスプロイトの影響を見積もり、対応するサポートが可能である。

SBOM の採用が分野内又は分野を超えて増えているので、組織に対する SBOM の価値も増加している。各利害関係者には、SBOM の生成、管理、配布、取込み及び利用といった、SBOM に対するそれぞれ別の役割及び使用がある。

このガイダンスは、SBOM の概要説明並びに SBOM の生成及び使用に対するベストプラクティスを提供する。この文書の目的は、MDM、HCP 及び規制当局などの医療機器の利害関係者に関連する、SBOM の実装及びソフトウェアの透明性について詳細に説明することである。このガイダンスにおいては、HCP には、医療機関が含まれる。

SBOM のベネフィットについては、NTIA の FAQ 文書及び“Roles and Benefits of SBOM Across the Supply Chain（サプライチェーンにおける SBOM の役割とベネフィット）”という文書に追加の考察事項が記載されている。

2. 適用範囲

この文書は、ファームウェア及びプログラマブルロジックコントローラーを含むソフトウェアを有する医療機器（例：ペースメーカー、輸液ポンプ）、又はソフトウェア単独で存在する医療機器［例：プログラム医療機器（SaMD）］に関するサイバーセキュリティについて検討している。この文書は、MDM 及び HCP の役割及び責任を重要視しており、SBOM の実装及び体外診断用（IVD）を含む医療機器に用いるソフトウェアの透明性向上に対する推奨事項を提供している。主に MDM 及び HCP に注力している一方で、その他の利害関係者（医療機器のユーザー、規制当局及びソフトウェアコンポーネントベンダーを含むが、これらに限定しない）も、この文書で示す概念の有用性を認識することになると考える。

ヘルスケアのサイバー環境を保護することは、HCP 及び MDM の共同責任である。SBOM は、患者危害の可能性を軽減することを助けることができるので、安全を支える共通のツールである。この文書は、次を意図している。

- SBOM の作成、管理及び配布について、医療機器製造業者に対する推奨事項を提供する。
- SBOM の取得及び管理について、ヘルスケアプロバイダーに対する推奨事項を提供する。
- リスクマネジメント、脆弱性マネジメント及びインシデント対応について、医療機器製造業者及びヘルスケアプロバイダーの観点からユースケースを示す。

SBOM は、包括的なセキュリティリスクアセスメントの代わりにはならない。デバイスレベルでセキュリティリスクアセスメントを行うためには、機器の意図する使用、アーキテクチャー及び機器全体の設計の知識を用いる。

ほとんどの規制当局は、その権限が医療機器の安全性及び性能に限定されているため、この文書の適用範囲は、規制対象の医療機器に関連する患者危害の可能性に関する検討に限定されている。医療機器の種類及び各国の規制の違いによって、別の又は追加の検討事項が必要になる状況が生じることがある。例えば、医療機器の性能に影響を与える、臨床活動に悪影響を及ぼす、又は誤った診断若しくは治療に繋がる脅威は、この文書の適用範囲とみなされる。データプライバシーの侵害に関連する等、その他の種類の危害は、この文書の適用範囲とはみなされないが、これらについても重要であり、SBOM が有益な軽減ツールかもしれないことを認識している。

この文書は、遠隔コンピューティング環境で提供されるクラウドサービスに固有の SBOM 関連事項及び推奨事項については扱わない。（クラウドサービスとは、例えば、ネットワーク、サーバー、ストレージ、アプリケーションなどのコンピューティングサービスへのオンデマンドのインターネットアクセスである。）クラウドサービスが、規制対象の医療機器システムのコンポーネントである場合は、安全及び有効性に対するリスクをもたらすこともある。規制対象の医療機器の製造業者は、クラウドサービス及びクラウドソフトウェアについてもリスク評価においてレビューしなければならないことを認識することが望ましい。クラウドサービスは複雑であり、製造業者が、自社がコントロールするプライベートクラウドではなく、サードパーティのクラウドを活用する場合にはさらに複雑になるので、この最初の IMDRF SBOM ガイダンスでは、SBOM について、クラウド技術を明確に含めてはいない。しかし、技術が進化し、規制の観点からのクラウドに対する理解が深まるにつれ、SBOM の文

脈においてクラウド技術の残留リスクに対応することが重要になるだろう。クラウド及びその他のリスクについては、今後の作業となることが予想される。

この文書は、IMDRF N60 ガイダンスの補完文書であり、関連する医療機器の適用範囲は同様であり、患者への危害が発生する可能性にフォーカスしていることに変わりはない。この文書は、サイバーセキュリティは、全ての利害関係者間の共同責任であることを引き続き認識している。

SBOM は、ライセンスや知的財産などの様々なソフトウェア透明性に関する問題に対応することもできるが、この文書では、SBOM に関するサイバーセキュリティの懸念事項に注力している。

3. 定義

この文書では、IMDRF/GRRP WG/N47 FINAL:2018 で定められている用語及び定義、並びに次を適用する。

3.1 **アプリケーションプログラミングインターフェイス**（Application programming interface、API）：アプリケーションプログラムが、ネットワークサービス、機器又はオペレーティングシステムにアクセスするために使用可能な、標準的なソフトウェア割り込み、呼び出し、関数及びデータフォーマットの集まり（**ISO 10303-1**:2021）

3.2 **資産**（Asset）：個人、組織又は政府にとって価値のある物理的又はデジタルのエンティティ（**ISO 81001-1**:2021）

3.3 **資産管理**（Asset management）：資産からの価値を実現するための調整された組織的活動（**ISO/IEC 19770-5**:2015）

3.4 **変更管理**（Change management）：全ての変更を記録し、調整し、承認し、監視するためのプロセス（**ISO 81001-1**:2021）

3.5 **構成**（Configuration）：情報処理システムのハードウェア及びソフトウェアの編成及び相互接続の仕方（**ISO/IEC 2382**:2015）

3.6 **サイバーセキュリティ**（Cybersecurity）：情報及びシステムが不正な活動（アクセス、使用、開示、中断、変更、破壊など）から保護されており、機密性、完全性及び可用性の侵害に関連するリスクがライフサイクル全体を通して受容可能なレベルに維持されている状態（**ISO 81001-1**:2021）

3.7 **サイバーセキュリティのインシデント**（Cybersecurity Incident）：組織に影響を及ぼすと判断され、対応及び復旧の必要が生じるサイバーセキュリティの事象（National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.）

注記：サイバーセキュリティの事象は、組織の運用（ミッション、能力、又は評判を含むが、これには限らない。）に影響を与えるかもしれないサイバーセキュリティの変化である。

3.8 **コンポーネント**（Component）：システムの物理的又は論理的な一部分を構成し、特定の機能及びインターフェイスをもち、（例えば、ポリシー又は仕様によって）システムの他の部分から独立して存在していると扱われる、システムのリソースの集まり（**ISO 81001-1**:2021）

注記：医療機器の文脈においては、コンポーネントには、完成し、梱包され、ラベル付けされる機器の一部として含めることを意図する、あらゆる原材料、物質、部品、ソフトウェア、ファームウェア、ラベリング、又は組立部品が含まれる。

3.9 **ハッシュ、ハッシュ値**（Hash, hash-value）：任意の長さのデータから固定長のランダムな値を生成するために用いる計算方法である、ハッシュ関数によって計算される値（**ISO 17090-4**:2020）

3.10 **レガシー医療機器（レガシー機器）**［Legacy Medical Device（Legacy Device）］：現在のサイバーセキュリティの脅威に対して合理的に保護できない医療機器（IMDRF/CYBER WG/N60FINAL:2020）

3.11 **ライフサイクル**（Life cycle）：製品又はシステムの初期構想から最終的な使用停止及び廃棄に至るまでの一連の全ての段階（**ISO 81001-1**:2021）

3.12 **製品**（Product）：組織と顧客との間の処理・行為なしに生み出され得る、組織のアウトプット（**ISO 81001-1**:2021）

3.13 **リリース及びアップデート**（Releases and Update）：医療機器ソフトウェアを対象とした修正、予防、適応又は完全化に関する変更

注記 1：ISO/IEC 14764:2006 に規定するソフトウェア保守活動に由来する。

注記 2：アップデートには、パッチ及び設定変更が含まれることがある。

注記 3：適応及び完全化に関する変更は、ソフトウェアの改良である。その変更は、医療機器の設計仕様になかったものである。

3.14 **レポジトリー**（Repository）：データ検索を可能にする、体系化され持続的なデータストレージ（**ISO/IEC/IEEE 26511**:2018）

3.15 **リスクマネジメント**（Risk management）：リスクの分析、評価、コントロール及び監視に対する、マネジメント方針、手順及び実施の体系的な適用（ISO/IEC Guide 63:2019）

3.16 **ソフトウェア部品表**（Software Bill of Materials、SBOM）：一つ又は複数の識別したコンポーネント、それらの関係及びその他の関連する情報のリスト

注記：依存関係のない単一のコンポーネントの SBOM は、そのコンポーネント一つだけのリストである。“ソフトウェア”は、“ソフトウェアシステム”と解釈可能なため、ハードウェア（ファームウェアではない真のハードウェア）及び［中央処理装置（CPU）のマイクロコードのような］非常に低レベルのソフトウェアを含むことがことがある。（NTIA Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM) 2021-10-21)

3.17 **ソフトウェアコンポーネント**（Software component）：ソフトウェアシステム又はモジュール、ユニット、データ、文書などの要素を参照するために用いる一般的な用語（**IEEE 1061**）

注記：一つのソフトウェアコンポーネントは、複数のユニット又は複数のより低レベルなソフトウェアコンポーネントを含む可能性がある。

3.18 **ソフトウェアコンポジション解析**（Software composition analysis）：コードベースをスキャンして、どんなコード（例えば、クローズドソースソフトウェア、フリーソフトウェア、オープンソースソフトウェア、ライブラリー、パッケージ）が含まれているかを特定する一つ以上のツールの使用

注記：これらのツールは、含まれているコードに関係する既知の脆弱性のチェックも行うかもしれない。（https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8397.pdf）

3.19 **ソフトウェア透明性**（Software transparency）：ソフトウェアの全ての枠組み、階層及びコンポーネントを概観するソフトウェアの概略構造

3.20 **システム**（**System**）：一つ以上の目的のために組織された、相互に作用する要素の組合せ

3.21 **サードパーティのソフトウェア**（Third party software）：関係者から独立していると認識される人又は団体から提供されるソフトウェア（ISO/IEC 25051:2014 を一部変更）

注記：関係者は、通常、供給者（“ファーストパーティ”）及び購入者（“セカンドパーティ”）の利害関係者である。

3.22 **ユースケース**（Use case）：システム（又はその他のエンティティ）がシステムのアクターと相互作用して実行可能な、変異を含む、一連の動作の仕様（**ISO/IEC 23643**:2020）

3.23 **VEX**（**Vulnerability** Exploitability eXchange、脆弱性の悪用可能性についての情報交換）：特定の製品における脆弱性の状態についての機械可読な宣言

3.24 **脆弱性**（**Vulnerability**）：一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点（**ISO/IEC 27000**:2018）

3.25 **脆弱性マネジメント**（Vulnerability management）：ソフトウェアの脆弱性を特定し、分類し、優先順位をつけ、修正し、軽減することを繰り返し行うこと

4. SBOM フレームワークの概要

概要としては、MDM は、SBOM コンテンツを収集し、ソフトウェアコンポーネントリポジトリーに格納する。（NTIA の“Software Suppliers Playbook: SBOM Production and Provision（ソフトウェアサプライヤーのプレイブック：SBOM の作成及び提供）”を参照。）次に、MDM は、機器 SBOM を集めて生成し、HCP が活用できるように、リリースして配布する。以降のセクションでは、SBOM の生成、配布及び取込みに関する詳細について、MDM 及び HCP の両方の観点から情報提供する。

図 1 に、フレームワークの概要を示す。このフレームワークでは、MDM 及び HCP 間の SBOM 生成・取得を通じて、情報共有が可能であり、ソフトウェア透明性が高まる。このフレームワークの下で、MDM 及び HDO の考慮事項に取り組む。

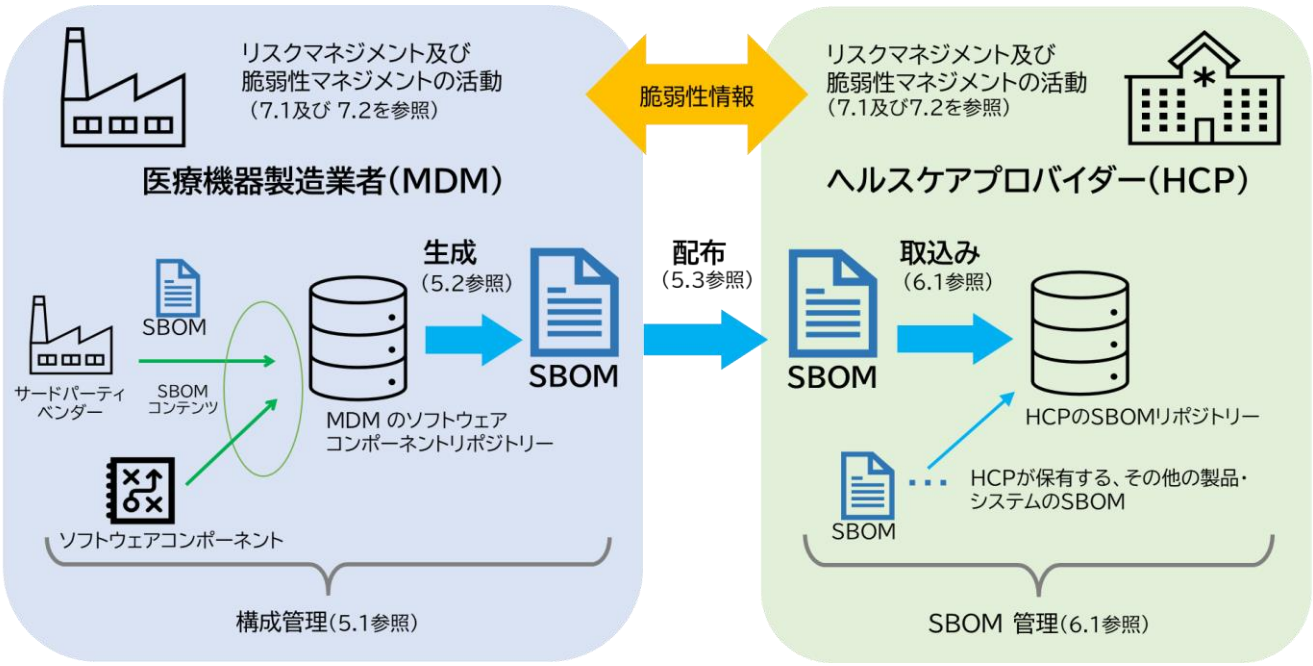

図 1―SBOM フレームワークの概要

5. 製造業者の考慮事項の概要

このセクションでは、SBOM コンテンツ収集、SBOM 生成、SBOM 配布及び SBOM コンテンツの維持（脆弱性の監視及び変更管理を含む）などの、SBOM に対する MDM の考慮事項の概要を示す。新たな機器 SBOM が作成されて新しい製品バージョンとともにリリースされるので、機器 SBOM 自体が維持されるわけではないことに注意する。しかし、新たな機器 SBOM を受け取るエンドユーザーの観点からは、以前の機器 SBOM の更新である。こうした更新は、SBOM コンテンツの関連文書及びプロセスが維持されている場合においてだけ可能である。「SBOM コンテンツを維持する」という言い方及びその背後にある意図については、図 2 でさらに説明されている。

ソフトウェア開発ライフサイクルの設計、コード・ビルド・テストの段階において、様々な種類のソフトウェアコンポーネントが医療機器に組み込まれる。構成管理活動の一環として、それらのコンポーネントの SBOM コンテンツは、収集され、その他の関連情報とともに MDM のソフトウェアコンポーネントリポジトリーに格納される。SBOM は、このリポジトリーから生成され、デプロイ・リリース段階の活動として HCP に配布される。HCP は、調達プロセス中又はソフトウェアリリースの時点で SBOM を入手可能である。SBOM がリリースされた後は、脆弱性監視によって、関連するソフトウェアコンポーネントの変更管理がトリガーされ、SBOM コンテンツ収集及び SBOM コンテンツリポジトリーにフィードバックされる。図 2 は、ソフトウェア開発ライフサイクルの全体における SBOM の管理について、さらに詳細を示している。

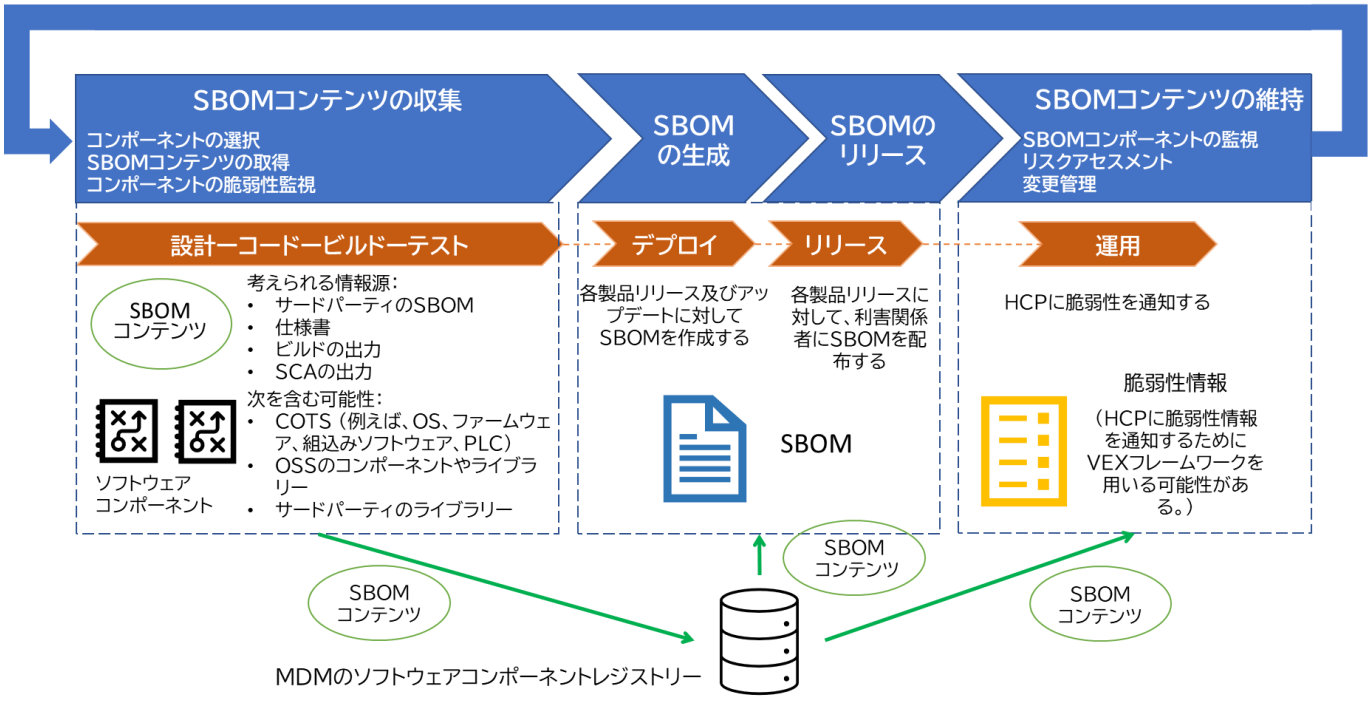

図 2：ソフトウェア開発ライフサイクル（SDLC）全体における SBOM 管理

5.1. SBOM コンテンツの収集

SBOM コンテンツの収集は、ソフトウェア開発ライフサイクルの設計段階に始まる。SBOM コンテンツは、次のような様々な情報源からもたらされることがある。

- 自社製のソフトウェアの開発文書
- 商用ソフトウェアのベンダーから提供されるサードパーティーの SBOM 文書
- オープンソースソフトウェアとともに提供される文書
- SCA（Software Composition Analysis、ソフトウェアコンポジション解析）ツールの出力結果

該当する SBOM コンテンツは、設計―コード―ビルド―テストの間に収集され、MDM のソフトウェアコンポーネントリポジトリに維持される。SBOM コンテンツは、医療機器システムに対して収集する必要があり、これには医療機器システムの部分である周辺機器のコンポーネントも含める。これには、様々な情報源及びツールを必要とするかもしれない。例えば、関連コンポーネントが、製品をスキャンするのに用いた SCA ツールで特定されるかもしれない。その代わりに、ファームウェア、組込みソフトウェア及び PLC（Programmable Logic Controller、プログラマブルロジックコントローラー）などのコンポーネントのベンダーが、MDM がソフトウェアコンテンツリポジトリーに組込み可能な SBOM を提供するかもしれない。

MDM のソフトウェアコンポーネントリポジトリーに含まれる可能性があるコンポーネントの種類及びコンテンツを収集するためのツールについての詳細は、附録 9.1 に記載している。

5.2. SBOM の生成

SBOM の生成においては、製造業者は、ソフトウェアサプライチェーン全体を考慮する必要がある。SBOM を生成するために、該当する SBOM コンテンツは、各製品のリリース及びアップデートに対する機器 SBOM に集約されることが望ましい。各製品のリリース及びアップデートに対する最終的な機器 SBOM は、維持され、配布できるようにすることが望ましい。SBOM の生成は、定義され、確立された方法論に従って行い、一貫した出力を確実にすることが望ましい。これによって、SBOM は、機器のライフサイクルの全体を通して、更新され維持される。

次のセクションでは、SBOM の要素及びフォーマットについての考慮事項についても記載している。SBOM 生成及びツールについての追加考察は、NTIA の“How to Guide for SBOM Generation（SBOM 生成のハウツーガイド）”にも記載されている。

5.2.1. SBOM の要素及びフォーマット

各 SBOM エントリーには、各ソフトウェアコンポーネントを識別するための情報を含めることが望ましい。SBOM エントリーに含める入手可能な情報は、変わる可能性があるが、一般的に、SBOM の深さがその有用性に影響するので、SBOM は、可能な限り完全であることが望ましい。より完全な SBOM 情報にアクセスすることで、より早い脆弱性の特定及び評価が可能となり、機器のサイバーセキュリティの改善をサポートする。医療機器のサイバーセキュリティに対して、SBOM には、最低限、NTIA の推奨事項に一致する次の要素を含むことが望ましい。

- 作成者名：SBOM ファイルを作成したエンティティ（すなわち、個人、組織又はそれに類するもの）
- タイムスタンプ：SBOM データの構築を行った日時の記録
- ソフトウェアコンポーネントのベンダー（サプライヤー）：コンポーネントを作成、定義、識別するエンティティ。ソフトウェアコンポーネントのベンダー名は、一般に、商用ソフトウェアの法的なビジネス名を参照することが望ましい。
- ソフトウェアコンポーネントの名称：元のサプライヤーが定義した、ソフトウェアユニットに割り当てられた名称
- ソフトウェアコンポーネントのバージョン：以前に識別した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
- 関係：上流コンポーネント X がコンポーネント Y に含まれるという関係の説明

SBOM に含める要素は、基本情報によって特徴づけして、特定できるようにする。その他の情報は、必要に応じて、追加の要素として又は SBOM 本体に対する補足として、必要に応じて追加可能である。例えば、コンポーネントハッシュは、コンポーネントの存在を関連するデータソースに対応付けするのに役立つので推奨される。それに加えて、機器のライフサイクルに関連する考慮事項［例えば、ソフトウェアの EOS（End of Suport、サポート終了）期日］は、製品ライフサイクル全体を通じた医療機器のリスクマネジメントの助けになるので、補足情報として提供可能だろう。

最低限含める要素に加えて、MDM は、SBOM フォーマットについても検討することが必要である。現時点では、いくつかの自動化可能な SBOM フォーマットがある。CycloneDX、SPDX（Software Package Data Exchange）及び SWID（Software Identification）である。これらのフォーマットについての追加情報並びに医療機器に対する SPDX 及び SWID の詳細例が、NTIA の“How to Guide for SBOM Generation（SBOM 生成のハウツーガイド）”に記載されている。

5.3. SBOM の配布

SBOM の配布は、SBOM 情報を製造業者から HCP 又はユーザーに対してどのように転送するかというプロセスである。MDM は、SBOM をどのように配布するのがベストなのかについて、認識の向上、アクセスの提供及びアップデートのプッシュ通知を含めて検討しなければならない。これは、製品内又は製造業者のウェブサイトの、電子ファイル又は API（Application Programming Interface、アプリケーションプログラミングインターフェイス）の可能性がある。ある時点で、SBOM を配布するための最良の方法は一つだけではないが、標準化され、自動化可能な開示・交換メカニズムを使用することが推奨される。

まず、HCP は、SBOM の存在を認識する必要がある。SBOM は、調達プロセスの一環として最初に HCP に対して提供されることが望ましい。例えば、SBOM は、製品の顧客向けセキュリティ文書（IMDRF/CYBER WG/N60FINAL:2020）、医療機器セキュリティのための製造業者開示説明書（MDS2、ANSI/NEMA HN 1-2019）、出版・購読型システムなどの共有コミュニケーションチャネル、又は医療機器の公開用インターフェイスに含まれる可能性がある。医療機器は、頻繁に更新されるので、自動更新をサポートするために、ネットワーク越しに標準化した方法で製品及びソフトウェアバージョンを簡単に特定するメカニズムが推奨される。

次に、MDM は、SBOM が HCP に配布されるようにする又は HCP が SBOM をアクセスできるようにすることが望ましい。既存の方法は、一般に次の三つのカテゴリーのいずれかに該当する。

- SBOM は、MDM から HCP に直接提供される。
- SBOM は、医療機器に内蔵される。
- SBOM は、リポジトリー経由で HCP が入手する。SBOM リポジトリーには、同じ又は異なる製造業者の様々な製品の SBOM を集約したものが含まれる。

    - 製造業者管理のリポジトリーは、一つの製造業者の機器 SBOM だけを含むが、集中型リポジトリーは、複数の製造業者の機器 SBOM を含む。
    - 集中型リポジトリーは、サードパーティの管理かもしれないし、ヘルスケアプロバイダーの管理かもしれない（つまり、HCP は、製造業者から受け取った機器 SBOM を、使いやすいように一元的に集約する可能性がある。）。ヘルスケアプロバイダー管理のリポジトリーについての更なる情報は、**6.1.1** を参照。

網羅的リストではないが、次の表は、SBOM 配布方法について MDM が検討すべき長所及び短所を概説している。

表 1：SBOM 配布方法ごとの長所及び短所

配布方法	長所	短所
製造業者からの顧客向けセキュリティ文書に含める	• 特殊なツールを必要としない	• 自動化ではない • 文書を頻繁に更新してユーザーに配布しなければならない • 文書を機器自体にリンクする方法が必要となる（強力な資産管理） • SBOM アクセスの制御が困難
製造業者が、別途（電子）文書で提供する	• 特殊なツールを必要としない • SBOM アクセスの制御が容易 • おそらく機械可読性がある	• 自動化ではない • 文書を頻繁に更新してユーザーに配布しなければならない • 文書を機器自体にリンクする方法が必要となる（強力な資産管理）
ディスプレイ、（間接的な）参照又はダウンロードを通して医療機器からアクセス可能	• 常に正しいバージョンである • ユーザーの制御のもとにある • SBOM アクセスの制御が容易	• 自動化ではない • 情報にアクセスするために、機器へのアクセスが必要 • 機器には情報を取り出す手段（例えば、ユーザーインターフェイス、USB ポート、ネットワーク接続）がないかもしれない • 機器に十分な空き容量が必要 • （バッテリー動作の医療機器の場合）バッテリー容量を余計に使用する必要があるかもしれない
医療機器の API からアクセス可能	• SBOM アクセスの制御が容易 • 自動化プロセスで使用可能	• API の標準が定まっていない • ツールが必要 • ネットワーク接続が必要
製造業者が管理するリポジトリー	• SBOM アクセスの制御が容易 • 自動化プロセスで使用可能	• 顧客が、情報を求めて複数の製造業者のサイトやリポジトリーをチェックしなければならない
集中型リポジトリー	• 顧客が情報アクセスするためのより効率的な方法である（つまり多くの個別の製造業者サイトやリポジトリーをチェックする必要がない） • 自動化プロセスで使用可能	• サードパーティのサービスを使用する場合、知的財産、法的責任、その他の考慮事項がある • 組織によっては、アップデート状態が異なるために同じ機器に対して複数のバージョンがある可能性があるので、最新バージョンだけでなく、該当する全ての SBOM をアクセスする必要があり、バージョン付けにおいて課題がある

SBOM 配布におけるもう一つの考慮事項は、SBOM 情報を保護する必要性である。医療機器の SBOM は、業界のベストプラクティスに従って、機密情報として分類されることが望ましい。MDM から外部の受信者、規制当局及び HCP へのコミュニケーションチャネルは、文書が漏洩して、結果としてリスクへの露出が増えることになる可能性を減らすために、保護手段をサポートする必要がある。さらに、これらの外部組織（すなわち、機器 SBOM を受け取る組織）は、SBOM の完全性、真正性及び機密性を保護するために、組織内のセキュリティポリシー及び実践を厳格に維持する必要がある。

5.4. SBOM コンテンツの維持

SBOM は、ソフトウェアコンポーネントに脆弱性があるかどうかを明示的に示すものではない。しかし、SBOM は、医療機器の脆弱性監視のために、その他のリソースとともに用いられる可能性がある。MDM が脆弱性情報を HCP に通知する方法の一つは、VEX（Vulnerability Exploitability Exchange、脆弱性の悪用可能性についての情報交換）である。

医療機器のライフサイクルにおいて、各利害関係者は、サードパーティのソフトウェアコンポーネントについての正確で最新の情報を頼りにしている。MDM は、機器のソフトウェア脆弱性に関連する患者安全のリスクの可能性を特定し、評価し、軽減するために SBOM を使用することがある。HCP は、購入前及びデプロイ中に機器を評価するために SBOM を使用することがあり、それによって、HCP は、製造業者と協力して、サイバーセキュリティのリスクを管理することが可能である。

脆弱性の監視は、関連するソフトウェアの変更が必要であると判断した場合には、変更管理のきっかけになることがある。MDM は、既存の変更管理コントロール（すなわち IT 環境に対する変更を特定し、文書化し、許可するために用いるプロセス）を活用して、機器のソフトウェアに対する全ての変更を SBOM 内に確実にとらえ、適切なフォローアップを確実に行うことが望ましい。最終的に、SBOM コンテンツのあらゆる変更によって、変更されたコンポーネントを含む機器 SBOM が更新されて生成され、適切な利害関係者に配布されることが望ましい。

5.4.1. SBOM 及び変更管理

近年、ソフトウェア開発ライフサイクル（SDLC）が、医療機器開発の市販前及び市販後の変更管理プロセスに組み込まれてきているが、サードパーティのコンポーネントの変更管理は、多くの製造業者にとって依然として新しい領域である。機器のソフトウェアの変更を引き起こす全ての事象は、新たな SBOM につながるということを理解することが重要である。変更を引き起こす事象には、次があるが、これらには限らない。

- アップグレード、アップデート又はパッチによる脆弱性の改善
- 医療機器ソフトウェアに対する新たな機能の追加
- ソフトウェアコンポーネントの交換
- ソフトウェアコンポーネントの追加又は削除
- 機器のハードウェア上又はオペレーティングシステム（OS）内部にあるサードパーティのコンポーネントの変更［EOL 若しくは EOS の到達、（セキュリティ）パッチ、又は市場への新たなバージョンの投入によるもの］

変更管理は、SBOM に適用することが望ましく、これには自社製の医療機器ソフトウェア及びサードパーティのソフトウェアライブラリーが含まれる。この情報は、内部のバージョン管理に対して重要であるだけでなく、MDM が HCP に対して軽減策が導入されたことを通知する手助けにもなる。

SBOM に対する変更は、HCP に定期的に通知し、適切な配布プラットフォームにおいて、利用可能で機械可読性のあるフォーマットで入手可能にすることが望ましい。

5.5. 課題

SBOM は、ソフトウェアの透明性を通じて患者安全を高めるという期待が大きい。市販前及び市販後活動の一部として、包括的な SBOM を生成し、監視し、配布することが、MDM に対する課題となる可能性がある。適切なツール及び内部プロセスが必要である。

このセクションでは、ソフトウェア開発ライフサイクルの全体にわたって SBOM を実装する際のいくつかの課題について取り上げる。

a. **現在市販されている機器又はレガシー機器の SBOM**：SBOM は、比較的新しい概念であり、現在も導入が続いている。一般的に、過去に生産された古い機器の SBOM を作成する際には、基本的な情報及び要素だけを含む SBOM であっても、入手が困難な場合がある。MDM は、サードパーティーから情報が入手可能でない場合のコンポジション解析ツールによる SBOM の補完方法も含めて、サードパーティーのサプライヤーから提供される SBOM を組み込むために、最善の判断を行うことが望ましい。範囲や深さが限定的であっても、可能な限り SBOM を構築することが望ましい。特に、オペレーティングシステム、市販ソフトウェア、OSS などの主要要素をとらえる場合に望ましい。そうすることで、SBOM の中核となるコンテンツを拡張し、改善することが余地が生じる。これは、HCP や他の関係者が様々なツールを用いることによって、達成できるかもしれない。MDM は、組織のニーズに最もよく適合する能力のツールを注意深く選択することが望ましい。（例えば、MDM のビジネスに関連するリスクに対して適切な考察を行う。）ある種の SCA ツールによって、望んだ範囲や深さで SBOM を生成することができるかもしれない。SCA は、さらに、コンパイラー設定がセキュリティや強化を促進するように設定されているかを確認し、コンパイラーが脆弱性のあるコードの混入を回避できたか、システムのネットワークツールが不要なのに含まれていないか、デバッグ情報を含むファイルが含まれていないかを判断することも可能である。
b. **規格及びツール**：SBOM の収集、生成、配布、及び脆弱性監視のための使用は、規格及びツールによってサポート可能である。規格及びツールに関する考慮事項の概略は、次に示す通りであり、SBOM コンテンツを収集するためのツールについては、附録 9.1 に追加詳細を示している。ソフトウェア及び作成者を安定して世界的なレベルで識別することについては、さらに明確化する必要がある。国際規格は、最新の技術を規定するための一つの方法である。
    i. 規格及びツールは、進化し、成熟し続けており、MDM がそれらの“確定”を待つのは望ましくない。むしろ、SBOM の基本的・基礎的な概念を適用して、最初の SBOM を生成することが望ましい。例えば、SBOM コンテンツを特定するためのツールが存在するかもしれないが、SBOM コンテンツを機械可読なフォーマットに変換したり、脆弱性のあるコンポーネントを［NIST 米国脆弱性データベース（National Vulnerability Database、NVD）などの］中央データベースを使って識別したりする際に課題があるかもしれない。脆弱性データベースは、時間がたつにつれて変更される可能性があり、完全ではないかもしれない。

ii. 多くの組織が、規格及びツールの策定に向けて引き続き作業しているので、中長期的には、MDM は、利用可能になったより新しいプラットフォームに、SBOM を移行できるかもしれない。

c. **SBOM の深さ**：SBOM は、各製品のリリース又はアップデートに対して作成されるので、SBOM は、動的であり、時間がたつにつれて変わる可能性がある。SBOM に含める SBOM コンテンツの適切な深さを定めることは、SBOM を最新の状態に保つために必要なリソースの量及び種類に影響する。SBOM の深さが深いほど高品質の SBOM を生成し、エンドユーザーに対して高い価値を提供する。しかし、深さが深ければ、複雑性も増し、SBOM の生成及び解析に課題が生じる。

d. **SBOM の配布**：SBOM の配布に関連して、多くの課題があることが認識されている。課題には次があるが、これらには限定されない。(a) ソフトウェアアップデートの頻度、(b) ソフトウェアアップデートに対応する SBOM 更新の必要性、(c) ユーザーの資産管理システムにおいて配布した SBOM を維持する必要性。HCP は、同じ機器の複数のバージョンを異なる構成で持つ可能性、及び／又は、異なるタイミングで新しいソフトウェアリリースにアップデートする可能性がある。HCP は、各機器に対して適切な SBOM を保持する必要がある。

6. ヘルスケアプロバイダーの考慮事項の概要

ヘルスケア環境は、ここ 10 年でデジタル化が進行しており、デジタル技術は、ヘルスケア業界のあらゆる部分に浸透してきている。このデジタルトランスフォーメーションは、管理及び臨床機能の両方を実施するために、ソフトウェア及びソフトウェアが動かす機器への依存を生み出してきている。残念ながら、このデジタル化と同時に、サイバーセキュリティの脅威が劇的に増加してきている。HCP の状況は、デジタルへの依存及び接続性がますます高まってきているので、デジタル化は、大規模なヘルスシステム、地方の小規模な施設、ますます増加している外来部門、在宅医療などの様々な HCP に対して影響を与えている。

製造業者は、ソフトウェア部品表（SBOM）を製品とともに供給することが望ましい。このセクションでは、SBOM の取込み及び管理を含む、ヘルスケア組織の考慮事項についての概要を示す。SBOM のフレームワーク全体については、図 1 を参照。

6.1. SBOM の取り込み及び管理

SBOM は、調達時から始まる HCP のリスクマネジメントの一部として用いられる。ヘルスケアプロバイダーは、自らのネットワークインフラストラクチャーへの統合を意図する全ての機器について、製造業者に SBOM を要求することが望ましい。SBOM を活用可能にするためには、組織は、SBOM を取り込む能力をもつことを確実にすることが望ましい。HCP が資産のインベントリ管理を完全かつ正確に行うことが極めて重要である。インベントリ管理リストは、他の資産管理システムや、SBOM のような資産を強化するデータソースとの相関を可能にする機器固有識別子（UDI）をもつ医療機器の最新のリストを含むことが望ましい。一旦取り込んだら、SBOM は、組織のベネフィットを最大化するよう管理することが望ましい。

このセクションでは、SBOM の取込み及び管理を含む、ヘルスケア組織における SBOM の考慮事項、並びにヘルスケアプロバイダーが管理する SBOM リポジトリーに特有な考慮事項を提供する。

6.1.1. SBOM の取り込み及び管理に対する考慮事項

HCP は、HCP のネットワーク環境に存在し動作しているハードウェア資産及び関連するソフトウェア、並びにプログラム医療機器（SaMD）について理解することが必要である。HCP は、情報技術及び資産管理の確立したプラクティスを、開発者から直接購入した又はカスタム開発したインベントリ管理ソフトウェアに対して使用可能である。しかし、購入した機器上で動作するソフトウェアについては、これらの確立したプラクティスでは、容易にインベントリ管理できない。SBOM は、この情報を MDM と HCP との間で透明性を強化して共有する方法である。次は、SBOM 及びヘルスケアプロバイダー管理の SBOM リポジトリーに関する考慮事項である。

a. **調達**：SBOM は、調達プロセスの間に入手可能にすることが可能である。これによって、HCP は、機器のコンポーネントをレビュー可能である。HCP は、調達から配送までの間に SBOM が変更される可能性があることを認識しておくことが望ましい。
b. **標準的なフォーマット及び配送**：SBOM の配送は、標準的なフォーマット及び自動化した配送・取り込みメカニズムで行うことが望ましい。これによって、HCP は、情報を効率的に取り込み、データの完全性を保護するセキュアな場所に保存可能である。考慮すべき三つの著名なフォーマットは、CycloneDX、SPDX 及び SWID である。
c. **機器固有識別子（UDI）**：HCP が複数の型式及びバージョンを所有することが多いので、機器 SBOM は、理想的には機器固有識別子に対応付けて、SBOM を各機器との間で正確に相関をとれるようにする。機器及び製造業者への正しいマッピングを確実にするために、IMDRF の UDI アプリケーションガイドに記載されている通り、機器固有識別子（UDI）を製品レベルで参照することが望ましいが、医療機器ソフトウェア及び医療機器自体のバージョン番号についても、該当する場合は、含めることが望ましい。ソフトウェア及びハードウェアコンポーネントには標準化された固有識別子がないので、手動の対応付けが必要になる。
d. **網羅性**：SBOM の網羅性のレベルは、活用できる範囲に影響する。最低限、SBOM コンテンツには、次を含めることが望ましい。作成者名（会社名及び／又は人名）、タイムスタンプ、ソフトウェアコンポーネントのベンダー（サプライヤー）、ソフトウェアコンポーネントの名称、ソフトウェアコンポーネントのバージョン、固有識別子及び関係。（5.2.1 を参照。）
e. **コミュニケーション**：機器 SBOM に既知の脆弱性があるソフトウェアコンポーネントが見つかった場合には、脆弱性に対応するための処置を（必要に応じて HCP の国・地域の規制当局の承認を得て）MDM が確実に提供するために、MDM と HCP との間でのコミュニケーションをとることが強く推奨される。
f. **機器管理の強化**：HCP は、内部的な SBOM リポジトリーを確立して管理するための能力が必要である。内部的な SBOM は、機器管理を強化するために、自身の環境内の各機器を特定の SBOM に結び付けるものである。
    1. 検索・照会機能：リポジトリーは、HCP の機器のリスク（既知の脆弱性を含む）を正確に特定し管理するために、検索・照会機能をもつ必要がある。

       HCP によっては、脆弱性があるかを知るために、購入した機器に含まれるネスト化したソフトウェアを何レベルかにわたって追跡したいと考えるかもしれない。

    2. 更新及び維持：リポジトリーは、情報が正確で最新であることを確実にするために、機器のライフサイクル全体を通して、SBOM コンテンツの更新及び維持をサポートする必要がある。確実に管理できるようにするために、自動化プロセスが必要である。

       機器及びリポジトリーの製品寿命の間に、フォーマット及びソフトウェア識別子が変更される可能性があるので、機器の識別子とあらゆるフォーマットの SBOM 情報の文書との間の対応付けを行う汎用的な機能が、SBOM リポジトリーのもっとも重要な機能である。（ISO/IEC 19770-2:2015 の SWID タグは、ソフトウェアをタグ付けする一つの手段である。）

    3. セキュアなリポジトリー：SBOM リポジトリーは、その情報が悪意のある人によって改ざんされたり、機器や HCP のネットワークを攻撃するためのロードマップに用いられたりすることを防ぐために、セキュアであることが望ましい。（例えば、ヘルスケア組織の中で、必要な人に役割ベースのアクセス制限を行う。）

注記：上記の a～f は、SBOM に関する一般的な考慮事項であり、MDM に対しても適用するものなので、セクション 5 でも説明している。

6.1.2. SBOM の取り込み及び管理の方法

SBOM は、手動でも自動化されたプロセスでも取り込むことが可能である。しかし、手動プロセスはすぐに面倒になるので、管理上の負担を低減するために、自動化プロセスが全ての規模の HCP に対して推奨される。自動化は、SBOM の管理を進展させるためにも役立つ。ヘルスケアプロバイダーの運営の一部として、組織は、SIEM（security information and event management、セキュリティ情報及びイベント管理）ソフトウェアソリューションを活用している可能性がある。SIEM は、その他の機能に加えて、ネットワーク接続する機器やサーバーなどのデータの収集、保存、集計、分析などが可能なソリューションである。SIEM が SBOM フォーマットを読み込み可能な場合は、SBOM の取込みに使用可能である。SBOM の使用を長期間にわたって維持するために、一部のヘルスケア組織は、CMDB（Configuration Management Database、構成管理データベース）又は CMMS（Computerized Maintenance Management System、コンピューター保守管理システム）を通して、ヘルスケア組織の VRM（Vendor Risk Management、ベンダーリスクマネジメント）システムに SBOM をリンク又は統合することを検討している。場合によっては、HCP は、これらの技術に SBOM を直接取り込むことを検討している。カスタム開発したソフトウェアツールやスクリプトも、SBOM を取り込むために使用可能である。直接取込み及び／又はカスタムツールの使用については、HCP は、自身のデータマネジメントシステムの電子的フォーマットが独自仕様かどうかを考慮する必要がある。

網羅的リストではないが、次の表は、SBOM を取込み管理するために HCP が使用可能な方法に対する長所及び短所のいくつかを概説している。

表 2：SBOM の取込み及び管理方法ごとの長所及び短所

SBOM の取込み又は管理方法	長所	短所
SIEM	● 直接取り込み可能	● SBOM フォーマットとの互換性 ● 独自仕様の SBOM との使用可能性 ● 検索のためのアクセスを低減
CMDB/CMMS	● 高度な検索性 ● 直接取込み可能 （Nuvolo、ServiceNow などのベンダーが、NTIA パイロットプログラムに参加している） ● 各資産に対する直接の相関	● SBOM フォーマットとの互換性 ● 独自仕様の SBOM との使用可能性
VRM	● 検索可能、直接取込み可能	● SBOM フォーマットとの互換性 ● 独自仕様の SBOM との使用可能性 ● 個々の資産へのリンクの欠如
カスタムスクリプト	● 個々の個別のニーズに対して調整可能	● 作成に時間がかかる又はリソースの集中が必要な可能性 ● エラーの発生確率が高い

SBOM の管理に関連する特定のユースケースについては、セクション 7.0 の SBOM のユースケースに追加詳細を示している。

7. SBOM のユースケース

SBOM は、利害関係者によって幅広い範囲で使用されている。例えば、HCP の機器ライフサイクルの観点からは、SBOM は、デプロイ、統合、構成、使用、保守、及び機器の構成管理に対して手助けする（例えば、機器は同じタイミングで更新されないので、HCP は、同じ機器の複数のバージョンを所有する可能性がある）。

SBOM は、設計段階からサポート終了及び使用停止までの、医療機器の製品ライフサイクル全体を通して、MDM によっても使用されるかもしれない。全体論的には、SBOM は、組織が機器のライフサイクル全体にわたってより積極的なセキュリティの姿勢をとるために利用することが可能である。

このセクションでは、次に対する補助的なツールとしての SBOM について、ユースケースの例を紹介する。

- リスクマネジメント
- 脆弱性マネジメント
- インシデントマネジメント

以降のセクションでは、これらのユースケースの概要を示している。主に MDM 又は HCP の観点から解説しているが、これらのユースケースの中には、他の利害関係者グループにも適用できるものもあるかもしれない。

資産管理及び調達のユースケースについては、この文書には含めていない。これらのユースケースについての追加情報は、NTIA ソフトウェアコンポーネント透明性による Healthcare Proof of Concept Report（ヘルスケア概念実証レポート）を参照されたい。

7.1. リスクマネジメント

7.1.1. MDM の観点

典型的なリスクマネジメントの活動については、IMDRF サイバーセキュリティガイダンス（IMDRF/CYBER WG/N60FINAL:2020）の 5.2 に記載している。SBOM の生成については、製造業者は、ソフトウェアサプライチェーン全体を考慮する必要がある。これは、機器に組み込まれるソフトウェアコンポーネントを含む。SBOM は、外部の脆弱性情報源を用いることによって、それらのソフトウェアコンポーネントに存在する脆弱性を特定することを助けることが可能である。脆弱なソフトウェアコンポーネントが見つかった場合は、ソフトウェアの依存関係も考慮してリスク分析プロセスを開始する。

依存関係には、ライブラリー、オペレーティングシステム、TCP/IP スタック、その他のソフトウェア及びシステムを動かすのに必要なコンポーネントなどが含まれる。次のリストは、SBOM の使用でベネフィットがもたらされるリスクマネジメントの活動を示している。

a. **リスク評価**：潜在的な脆弱性を特定するために、SBOM を外部の脆弱性情報源とともに用いることが可能である。SBOM は、存在する可能性のある脆弱性について、その悪用可能性及び影響を含めた情報を提供する。この脆弱性情報は、特定の脆弱性に関連するリスクレベルを推定し、評価するために使用可能である。
b. **リスクコントロール**：SBOM を監視して、SBOM にリストされているコンポーネントに脆弱性があるかどうかを定期的に検証することによって、リスクを受容可能なレベルに保つことを助ける。（ユースケース 7.2 の脆弱性マネジメントについても参照。）
c. **評価及び監視**：新しいソフトウェアリリースに対し、必要に応じて SBOM を更新する。
d. **ライフサイクルのリスクマネジメント**：SBOM を機械可読性のあるフォーマットで製品セキュリティ文書の一部として HCP に対して購入時に提供し、機器のライフサイクル全体を通して更新する（機器が EOS に近づくと、最新の SBOM をヘルスケアプロバイダーの管理が容易になるように提供する）。詳細については、IMDRF/CYBER WG/N70DRAFT:2022 を参照。

7.1.2. HCP の観点

SBOM は、調達時から始まる HCP のリスクマネジメントの一部として用いられる。SBOM は、機器のソフトウェアに含まれているもの及びそれに関連するリスクについて、透明性を提供する。これによって、HCP は、製品ライフサイクルの進行に伴う機器のベネフィット及びリスク、並びに機器のライフサイクルにおけるリスクコントロール手段及び軽減戦略の効果的な適用方法について、さらに理解することが可能となる。

7.2. 脆弱性マネジメント

このセクションでは、医療機器の脆弱性マネジメントに対して SBOM を効果的に使用するためのユースケース及び考慮事項を示す。

7.2.1. MDM の観点

脆弱性マネジメントは、医療機器のリスクが受容可能であることを確実に維持するための、MDM の市販後アプローチにおける極めて重要な側面である。サイバーセキュリティの一環として、製造業者は、脅威及び脆弱性についての情報源を監視する。医療機器の潜在的な脆弱性が出現して、それが時とともに変化するので、SBOM はそうした脆弱性をタイムリーに識別するための支援を行ううえで不可欠な活用すべきリソースである。SBOM を使用することで、MDM は、関連する脆弱性情報から、影響を受けるソフトウェアコンポーネントに基づいて、脆弱性の影響を受ける可能性のある医療機器を特定可能である。報告された脆弱性から、医療機器の SBOM 情報と影響を受けるソフトウェアコンポーネント情報との比較を自動化することで、脆弱性特定の適時性及び正確性をさらに改善することが可能である。これによって、製造業者は、リスクアセスメントを行う能力を改善し、必要に応じてコミュニケーションし修正する。リスクアセスメントの一つの成果として、脆弱なコンポーネントが交換される可能性があり、これが最終的に SBOM の改訂につながる。

7.2.2. HCP の観点

脆弱性マネジメントは、ヘルスケア施設が IT 環境の脆弱性を継続的に検出、評価及び修正できるようにするための重要なプロセスである。新たな脆弱性が日々見つかっているので、これが、重大な脆弱性を効果的に検出し、タイムリーに修正するためのひとつの方法である。このセクションでは、様々な SBOM のユースケースを検討して、HCP の脆弱性マネジメントプロセスを支援する。

網羅的ではないが、次のリストは、SBOM の利用がベネフィットをもたらす脆弱性マネジメントの活動を示している。

a. **新たな脆弱性発生に対するヘルスケア施設の資産の監視**：SBOM は、脆弱性情報とともに用いて、所有する医療機器が新たな脆弱性によって影響を受けるかどうか、どのような影響を受けるかを理解するために用いることが可能である。VEX は、脆弱性に対する補完的なコミュニケーションメカニズムの可能性がある。
b. **暫定的な軽減策の推進**：SBOM 情報によって、HCP は、MDM やサプライヤーが正確な影響評価を行う間又は脆弱性を修正するためにアップデートを開発している間に、必要に応じて暫定的な軽減策を実行可能にする。

    - 暫定的な軽減策が、機器の意図する仕様に対してどのような影響を与える可能性があるかについて、MDM がよく理解しているかもしれないので、HCP は、暫定的な軽減策について、MDM と関わることが推奨されることに変わりはない。製造業者は、VEX（脆弱性の悪用可能性についての情報交換）を使用して、暫定的な軽減策の手引きを提供するかもしれない。

c. **ライフサイクルマネジメント**：SBOM は、新しい機器及び既に現場にある機器について、現時点におけるサポート対象及び非サポート対象ソフトウェアを理解する上での助けとなる。HCP が機器を置換えできない場合には、MDM が（企業及び患者の双方に対する）リスクを評価するために十分な時間を HCP に与えるサポートスケジュールを提供することが役に立つ。
d. **積極的セキュリティ活動によるヘルスケアプロバイダーの支援**：セキュリティスキャンが実行できない又は適切でない場合（例えば、組込み機器や SaMD の場合）に、SBOM は、脆弱性の特定及びセキュリティスキャン活動を補完する。

7.3. インシデントマネジメント

MDM 又は HCP が、医療機器に影響を及ぼす可能性のあるセキュリティインシデントに気付くきっかけは、数多くある。どのように気付いたかにかかわらず、SBOM は、頑健なインシデント対応プロセスと併用された場合には、MDM 及び HCP がサイバーセキュリティのインシデントを、インシデント

マネジメントの 5 つの段階[1]でよりよく管理するための助けとなるリソースの一つである。MDM にとっては、SBOM リポジトリーによって、危険にさらされている機器を特定し評価するためにかかる時間を低減可能である。HCP にとっては、SBOM リポジトリーは、初級レベルのサポートチーム及びサイバーセキュリティチームの行動を助けることが可能である。特にリポジトリーは、サイバーセキュリティに関連する事象を検出するための情報の体系的な収集、相関及び評価を改善し、最終的には、インシデント処理を改善する。まとめると、この改善された対応によって、不完全なリスク評価及び証拠の破壊につながるデータ損失でもたらされるリスクを低減可能である。

[1] ISO/IEC 27035 によれば、5 つの段階とは、次である。

- 計画及び準備
- 検出及び報告
- 評価及び決定
- 対応
- 得られた教訓

8. 参考文献

8.1. IMDRF 文書

1. Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations IMDRF/SaMD WG/N12:2014 (September 2014)

2. Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices IMDRF/GRRP WG/N47 FINAL:2018 (November 2018)

3. Principles and Practices for Medical Device Cybersecurity IMDRF/CYBER WG/N60: FINAL:2020 (April 2020)

4. Principles and Practices for the Cybersecurity of Legacy Medical Devices IMDRF/ CYBER WG/N70 FINAL:2023 (April 2023)

8.2. 規格

5. AAMI TIR57:2016 Principles for medical device security—Risk management AAMI TIR57:2016 Principles for medical device security—Risk management

6. AAMI TIR 97:2019, Principles for medical device security—Postmarket risk management for device manufacturers

7. ANSI/NEM HN 1-2019, Manufacturer Disclosure Statement for Medical Device Security

8. IEC 60601-1:2005+AMD1:2012, Medical electrical equipment - Part 1: General requirements for basic safety and essential performance

9. IEC 62304:2006/AMD 1:2015, Medical device software – Software life cycle processes

10. IEC 62366-1:2015, Medical devices - Part 1: Application of usability engineering to medical devices

11. IEC 80001-1:2010, Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities

12. IEC TR 80001-2-2:2012, Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

13. IEC TR 80001-2-8:2016, Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

14. ISO 13485:2016, Medical devices – Quality management systems – Requirements for regulatory purposes

15. ISO 14971:2019, Medical devices – Application of risk management to medical devices

16. ISO/TR 80001-2-7:2015, Application of risk management for IT-networks incorporating medical devices – Application guidance – Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1

17. ISO/IEC 27000 family - Information security management systems

18. ISO/IEC 27035-1:2016, Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management

19. ISO/IEC 27035-2:2016, Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response

20. ISO/IEC 29147:2018, Information Technology – Security Techniques – Vulnerability Disclosure

21. ISO/IEC 30111:2013, Information Technology – Security Techniques – Vulnerability Handling Processes

22. ISO/IEC 5962:2021 Information technology — SPDX® Specification V2.2.1

23. ISO/IEC 19770-2:2015 Information technology — IT asset management — Part 2: Software identification tag

24. ISO/TR 24971:2020, Medical devices – Guidance on the application of ISO 14971

25. UL 2900-1:2017, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

26. UL 2900-2-1:2017, Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems

8.3. 規制ガイダンス及びガイダンス案

27. ANSM (Draft): Cybersecurity of medical devices integrating software during their life cycle (July 2019)

28. China: Guidance for Premarket Review of Medical Device Cybersecurity (March 2022)

29. European Commission: REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (May 2017)

30. European Commission: REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (May 2017)

31. Medical Device Coordination Group (MDCG) 2019-16: Guidance on Cybersecurity for medical devices (December 2019)

    https://ec.europa.eu/docsroom/documents/41863/attachments/1/translations/en/renditions/native

32. FDA (Draft): Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (April 2022) [このガイダンスは、N73 文書の発行時点ではドラフトであり、実施されていない。最終ガイダンスで置き換えられる予定である。]

33. FDA: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (January 2005)

34. FDA: Design Considerations for Devices Intended for Home Use (November 2014)

35. FDA: Postmarket Management of Cybersecurity in Medical Devices (December 2016)

36. Germany: Cyber Security Requirements for Network-Connected Medical Devices (November 2018)

37. Health Canada: Pre-market Requirements for Medical Device Cybersecurity (June 2019)

38. Japan: Ensuring Cybersecurity of Medical Device: PFSB/ELD/OMDE Notification No. 0428-1 (April 2015)

39. Japan: Guidance on Ensuring Cybersecurity of Medical Device: PSEHB/MDED-PSD Notification No. 0724-1 (July 2018)

40. Singapore Standards Council Technical Reference 67: Medical device cybersecurity (2018)

41. TGA: Medical device cybersecurity - Consumer information (July 2019)

42. TGA: Medical device cybersecurity guidance for industry (July 2019)

43. TGA: Medical device cybersecurity information for users (July 2019)

8.4. その他の文献等

44. NTIA FAQ

https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf

45. NTIA “Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)” Second Edition

https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf

46. NTIA “Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)”

https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf

47. NTIA “Roles and Benefits of SBOM Across the Supply Chain”

https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

48. NTIA Software Component Transparency Healthcare Proof of Concept Report

https://www.ntia.gov/files/ntia/publications/ntia_sbom_healthcare_poc_report_2019_1001.pdf

49. NTIA Healthcare POC “How to Guide for SBOM Generation”

https://www.ntia.gov/files/ntia/publications/howto_guide_for_sbom_generation_v1.pdf

50. NTIA Vulnerability-Exploitability eXchange (VEX) Overview

https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf

51. NTIA Software Suppliers Playbook: SBOM Production and Provision

https://ntia.gov/files/ntia/publications/software_suppliers_sbom_production_and_provision_-_final.pdf

52. Dept of Commerce, Minimum Elements for a SBOM Pursuant to Executive Order 14028 on Improving the Nation’s Cybersecurity

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

53. OASIS Profile 5: VEX

    https://docs.oasis-open.org/csaf/csaf/v2.0/csd01/csaf-v2.0-csd01.html#45-profile-5-vex

54. CERT® Guide to Coordinated Vulnerability Disclosure

    https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

55. The NIST Cybersecurity Framework

    https://www.nist.gov/cyberframework

56. NIST's Secure Software Development Framework (SSDF)

    https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf

57. NIST SP 800-115:2008, Technical Guide to Information Security Testing and Assessment

    https://doi.org/10.6028/NIST.SP.800-115

58. Medical Device and Health IT Joint Security Plan (January 2019)

    https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-v1.pdf

59. MITRE medical device cybersecurity playbook (October 2018)

    https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and

60. MITRE CVSS Healthcare Rubric

    https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

61. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)

    https://www.phe.gov/Preparedness/planning/405d/documents/hicp-main-508.pdf

62. Open Web Application Security Project (OWASP)

    https://www.owasp.org/index.php/Main_Page

63. Manufacturer Disclosure Statement for Medical Device Security (MDS^2)

    https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

64. National Telecommunications and Information Administration (NTIA) / US Department of Commerce, Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group

    https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

65. https://republicans-energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf

66. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

9. 附録

9.1. SBOM コンポーネントの種類及びツール

SBOM コンテンツは、様々な情報源からもたらされる可能性がある。含まれるかもしれないコンポーネントの種類及び SBOM を生成するために使用されるかもしれないツールの例について、次に示す。

a. サードパーティのソフトウェアコンポーネントの種類

SBOM に組み入れるコンポーネントの種類の範囲は、次の要因に依存する可能性がありうるが、その限りではない。MDM の能力、HCP の期待、利用可能な SBOM ソフトウェアの成熟度、及び SBOM 規制要件の可能性又は期待。

しかし、SBOM を管理する際、コンポーネントによっては、インベントリ管理及び運用管理のために様々な方法やツールが必要になるかもしれないので、様々な種類のコンポーネントを認識することが重要である。次のような種類に分けられる。

i. 自社製の医療機器ソフトウェアにリンクされる又は組み込まれるサードパーティのソフトウェアライブラリー
ii. 仮想マシン、オペレーティングシステム、及びサードパーティのソフトウェアコンポーネントでドライバー、データベースソフトウェア、管理ツール、アプリケーションフレームワークなどオペレーティングシステムの内部にあるもの
iii. 医療機器に使用する、ベンダー供給のハードウェアに附属するサードパーティのソフトウェアコンポーネント：ファームウェア、組込みソフトウェア及び PLC（Programmable Logic Controller、プログラマブルロジックコントローラー）

次のセクションでは、SBOM のインベントリ管理、運用管理及び様々な種類のコンポーネントに対して利用可能なツールについて、詳しく述べる。

b. サードパーティのソフトウェアライブラリー

現代のソフトウェア開発においては、あるソフトウェアにおいて、製造業者が内製するコードよりもかなり多くのプログラム行数のサードパーティのコンポーネントのコードを使用することは、珍しいことではない。これらのライブラリーを含む SBOM の作成・管理は、MDM が全てのライブラリーのリストを追跡・作成して、そのリストを、使用するライブラリーに影響を及ぼす全てのソフトウェア変更に対して確実に更新することによって行うことが可能である。このように SBOM の追跡及び更新を手動で行うことは、SBOM の使用を開発プロセスに組み込むための最初の“基本的な”手順である。組織が成熟するにつれ、プロセスをより効率的で正確にするために、自動化のような、より進んだ手順を適用するようになるかもしれない。より進んだ手順の例としては、既存の開発プラットフォーム及び DevOps（訳注：DevOps は、開発と運用を組み合わせた混成語）環境の活用がある。特に、自動化ツールやプラグインは、開発パイプラインの一つ又は複数の段階に組み込むことができるだろう（つまり、DevOps にセキュリティ手法を統合した SecDevOps）。

SBOM の利点は、サードパーティのライブラリー及びライブラリーの既知の脆弱性の特定を可能な限り早期に行えることである。既知の脆弱性を早期に検出することで、早期の改善が容易になり、後で検出することに比較してより費用効果が高くなる。ソフトウェア開発の初期段階における手続き的な作業負荷は、例えば検証及びバリデーション段階などの後に比べてはるかに少ないため、脆弱なコンポーネントを開発プロセスの早い段階で脆弱でないコンポーネントに置き換えることは、コスト削減になる。また、ソフトウェア開発ライフサイクルの最終段階になるとコードの複雑さ及び依存性が増してしまうので、コーディングのやり直しも広い範囲には及ばなくなる。さらに、早期発見により、ソフトウェア開発ライフサイクル全体を通した SBOM の管理が可能となる。一般的にソフトウェアの変更があれば必ず SBOM のソフトウェア構成が変更になる。

そうしたツールやプラグインは、ソフトウェアを分析して、オープンソースソフトウェアが組み込まれている又はリンクされていることを検出する。同様に、商用のサードパーティのソフトウェアを検出可能なものもある。その種のツールは、通常、利用可能なセキュリティパッチがある古いライブラリーといった既知の脆弱性を特定する。脆弱性の監視は、次の段階における SBOM コンテンツの収集にフィードバックされる。

i. **コーディング**：例えば、静的コード分析を実行する場合（すなわち、実行されないソースコードにおける脆弱性の検出を試みるツールの活用）。
ii. **ビルド**：例えば、スプリントの終わりにソフトウェアをビルドする場合。ここでスプリントとは、特定の作業を完了し、レビューを準備完了にするために設定された期間をいう。
iii. **テスト**：例えば、静的アプリケーションセキュリティ試験（SAST）を実行する場合。

これらのツールやプラグインは、通常、ソフトウェアコンポジション分析（SCA）ソフトウェアと呼ばれるが、SBOM を作成するために手動入力は必要とせず、利用可能なリポジトリーを使用して一般に次を特定する。

i. ソフトウェアコンポーネントの名称
ii. ソフトウェアコンポーネントのベンダー（サプライヤー）
iii. ソフトウェアコンポーネントのバージョン
iv. コンポーネントハッシュ
v. 関係（一層又は多層の依存性）
vi. コンポーネントの脆弱性
vii. ライセンスモデル及びコンプライアンス情報

SCA ベンダーの大企業からだけでなく、他にもコード・ビルド・テストで使用可能な、同様の成果を生み出すツール及びプラグインが利用可能であることに注意する。フリーで使用可能なものもあり、全ての規模の医療機器製造業者が自動化のために利用可能であるが、MDM は、MDM のニーズに最もよく適合する能力のツールを注意深く選択することが望ましい。

c. オペレーティングシステムのコンポーネント

医療機器が使用する仮想マシン及びオペレーティングシステムは、SBOM の重要な構成要素である。医療機器ソフトウェアが構築されているオペレーティングシステムに依存するサードパーティのソフトウェアコンポーネントが存在し、これには、データベースソフトウェア、アプリケーションフレー

ムワーク、及び機器のその他の重要な機能に対するソフトウェアコンポーネント（セキュリティソフトウェア、システム管理ツール、リモートサポートソフトウェア、ネットワークコンポーネントなど）が含まれる。

オペレーティングシステム上のサードパーティのソフトウェアコンポーネントの検出及び管理を自動化する選択肢がいくつか存在する。SCA ベンダーの中には、前節で説明したコンポーネントと、自社製ソフトウェアに直接リンクしていない又は組み込まれていないオペレーティングシステム上のその他のソフトウェアコンポーネントとの両方に注力しているベンダーがある。しかし、ソフトウェアに内在するリスク及び価値を管理するガバナンスの実践である、ソフトウェア資産管理（SAM）に特化したベンダーも存在する。

そのようなツールが医療機器製造業者にとっての選択肢ではない場合には、専用スクリプト（例えば Windows の PowerShell スクリプトや Linux の Bash スクリプト）を実行することによって、オペレーティングシステム上のソフトウェアの一覧リストを生成可能である。また、脆弱性マネジメントのスキャンツールを使用する方法もある。後者の利点は、検出したコンポーネントの脆弱性情報も提供されることである。

d. ファームウェア、組込みソフトウェア、及び PLC

サードパーティのファームウェア、組込みソフトウェア及び PLC は、脆弱性が見つからない限り、医療機器のライフサイクルにおいて最も変更の可能性が低いコンポーネントである。組込みソフトウェアは、ボードのサポートパッケージ、バイナリーのドライバー、ソフトウェア開発キット（SDK、Software Development Kit）、CPU マイクロコード及びその他のライブラリーから構築される。これには、オープンソースソフトウェアにかなり依存しているものも含まれる可能性がある。最終製品に含まれる全てのソフトウェアコンポーネントを特定することが重要である。

この種のソフトウェアコンポーネントは、機器のハードウェアと結びついているため、医療機器の通常の BOM（部品表）の一部となる。BOM は、機器を製造するのに必要な原材料及びコンポーネントの包括的なリストであるので、ソフトウェアコンポーネントだけよりも多くの情報を含んでいる。したがって、BOM は、これらのサードパーティのソフトウェアコンポーネントの一覧リスト及び管理のための良い出発点となる。SBOM と同様に、通常の BOM は、MDM の開発活動やサードパーティが提供する BOM などの様々な情報源から取得される可能性がある。ソースコード管理システムとバイナリーソフトウェアコンポジション解析とを組み合わせて、この情報の生成を自動化し、検証するために用いることが可能である。用いられる全てのツールは、組込みシステムに対応したものであることが望ましいことに注意する。

BOM が PLM（Product Lifecycle Management、製品ライフサイクル管理）ソフトウェアや ERP（Enterprise Resource Planning、企業資源計画）ソフトウェアで管理されている場合、エクスポート機能を使ってソフトウェアコンポーネントを抽出することが可能である。利用可能な場合、ファームウェア、ソフトウェア又は PLC のベンダーの上流 SBOM を利用して、サードパーティのコンポーネントのより深い層を必要な場合に追加することが可能である。

これらのソフトウェアコンポーネントが内製されたものである場合（例えば、医療機器製造業者が開発したコンポーネントの場合）、セクション 9.1 の「サードパーティのソフトウェアライブラリー」で説明したのと同じアプローチが適用される。