写

医薬機審発 0825 第１号
令和８年８月 25 日

各都道府県衛生主管部（局）長 殿

厚生労働省医薬局医療機器審査管理課長
（ 公 印 省 略 ）

医療機器における SBOM 導入・運用ガイドライン（第１版）について

ソフトウェア部品表（Software Bill of Materials: SBOM）は、医療機器を構成するソフトウェアコンポーネントを可視化し、脆弱性の把握及び管理に資するものであり、医療機器のサイバーセキュリティの確保に有用な手法として、国内外で活用が進められています。

今般、「令和７年度医療機器サイバーセキュリティ対応の推進事業」において、「医療機器における SBOM 導入・運用ガイドライン（第１版）」を別添のとおり取りまとめました。つきましては、医療機器のサイバーセキュリティの確保に当たって、同ガイダンスを参考として、必要な対応を行うよう、貴管下関係事業者等に周知方お願いいたします。

なお、本通知の写しを独立行政法人医薬品医療機器総合機構理事長、一般社団法人日本医療機器産業連合会会長、一般社団法人米国医療機器・IVD 工業会会長、欧州ビジネス協会医療機器・IVD 委員会委員長、一般社団法人日本臨床検査薬協会会長及び医薬品医療機器等法登録認証機関協議会代表幹事長宛てに送付することとしています。

別添

医療機器における
SBOM 導入・運用ガイドライン（第１版）

令和 7 年度医療機器のサイバーセキュリティの推進事業

目 次

1. 背景と目的

1.1. 背景

近年、医療機器におけるソフトウェア機能の高度化およびネットワーク接続の拡大に伴い、サイバーセキュリティ対策の重要性が一層高まっている。
一方で、多くの製造販売業者等においては、ソフトウェア構成要素の把握や更新履歴の管理が十分とは言えず、インシデント発生時の対応や医療機関からの技術的な問い合わせに対し、迅速かつ的確に対応できない事例も多い。

規制面では、「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第 41 条第 3 項の規定により厚生労働大臣が定める医療機器の基準」(平成 17 年厚生労働省告示第 122 号。以下「基本要件基準」という。)第 12 条第 3 項や米国 FD&C 法第 524B 条など、国内外の当局がサイバーセキュリティに関する規制要求事項を強化しており、ソフトウェア部品表（Software Bill of Materials、以下「SBOM」という。）を利用したリスクマネジメントへの活用が国際的な潮流となりつつある。また、10 年以上にわたり使用される医療機器もあり、オープンソースソフトウェア（OSS）や既製（Off-The-Shelf、以下「OTS」という。）ソフトウェアを含むソフトウェアコンポーネントのライフサイクル管理を怠ると、長期にわたりセキュリティリスクが放置される懸念がある。

医療現場からも、インシデント発生時や脆弱性公表時に「どの医療機器がどのような影響を受けるのかを迅速に知りたい」、「メーカーから十分な情報が提供されていない」などの声が上がっており、製造販売業者等は SBOM を介した情報共有と説明責任の強化が求められている。

注記：本来、OTS ソフトウェアの定義には OSS が含まれるが、本ガイドラインでは保守管理の面で扱いが異なることから、「OTS」を、OSS を除く OTS ソフトウェアを表す用語として用いている。

1.2. 目的

本ガイドラインは、こうした背景を踏まえ、製造販売業者が SBOM を実務に取り入れ、継続的に活用できる体制へ段階的に移行できるよう支援することを目的とする。製造販売業者が適切に SBOM を導入・運用している場合、その手順、手法等の変更を求めるものではない。

具体的には、

- 第 1 段階として、米国商務省電気通信情報局(National Telecommunications and Information Administration、以下「NTIA」という。)の SBOM の最小要素等を踏まえた SBOM を作成・更新できる体制を整え、SBOM を作成・変更管理すること
- その後、SBOM を脆弱性管理・ライセンス管理・EOL／EOS 管理など既存の品質管理システム（Quality Management System、以下「QMS」という。）及び市販後安全管理プロセスと統合し、医療機器ライフサイクル全体のリスクマネジメントに活用すること

という段階的なストーリーラインを示す。

本ガイドラインは、すべての企業に一足飛びの高度運用を求めるものではなく、各組織の成熟度を踏まえた「段階的導入」の道筋を提示することを重視している。

1.3. 主な対象読者

本ガイドラインの主な対象は、以下のような製造販売業者等の担当者である。

- SBOM の整備をこれから開始しようとしている企業
- 既に SBOM を試行的に導入しているものの、運用方法や体制に課題を抱えている企業

具体的な読者としては、

- ソフトウェア開発部門
- 品質保証・QMS 担当部門
- 薬事・規制申請部門
- PSIRT・情報セキュリティ担当部門
- フィールドサービス・保守対応部門

など、医療機器のソフトウェア構成管理やサイバーセキュリティ対応に関わる実務担当者を想定している。
本ガイドラインはこれらの部門が共通の前提知識と指針をもつことを目的としており、組織横断的な SBOM を活用するための共通指針として位置付けるものである。
なお、本ガイドラインは医療機関や医療情報システム事業者、規制当局など、医療に関わる関係者が製造販売業者側の SBOM の位置付けや運用イメージを理解する際の参考資料として活用することも想定している。

2. SBOM の概要

2.1. SBOM とは

SBOM とは、医療機器ソフトウェアの透明性を確保するために、医療機器に組み込まれたソフトウェアを構成するコンポーネント（OSS、OTS ソフトウェア、自社開発モジュールなど）の一覧と、その属性情報を体系的に記録したものである。脆弱性管理、ライセンス管理、ライフサイクル管理などのリスクベースアプローチの根拠となる情報となる。

- MDS2 と SBOM の関係

医療分野では MDS2（Manufacturer Disclosure Statement for Medical Device Security）により、医療機器製品単位でのセキュリティ機能や運用要件を医療機関へ開示する枠組みが広く用いられている。
MDS2 は SBOM の形式や内容を規定する文書ではないが、SBOM 提供に関する項目が設けられており、SBOM の提供の有無や提供方法を医療機関に示す実務上の手段の一つとして活用できる。

- 本ガイドラインにおける SBOM の位置づけ

本ガイドラインで扱う SBOM は、医療機器に含まれている全てのソフトウェアを対象とし、医療機関に提示する SBOM については、データ通信等に使用されるハードウェアユニット又はコンポーネントのソフトウェアに限定して提示することも可能である。ただし、この場合、部分的な SBOM であることを明示する必要がある。

2.2. SBOM の導入効果

SBOM は、医療機器に含まれるソフトウェア構成を可視化し、脆弱性管理・ライセンス管理・開発生産性向上を支える情報基盤である。従来のように構成情報を人手で追跡する運用と比べて、調査工数と見落としリスクの大幅な低減が期待できる。

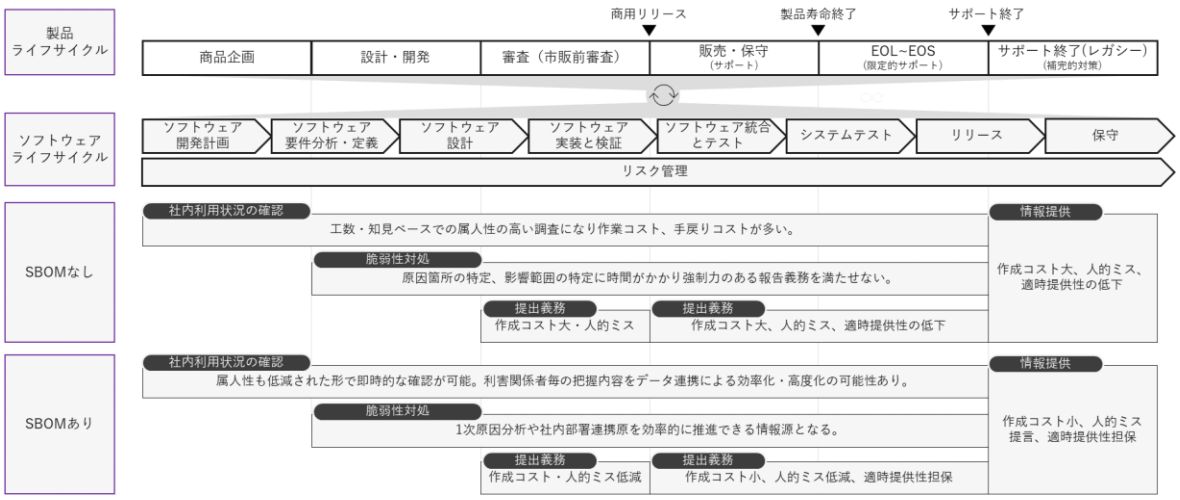


図 1：SBOM の導入効果

医療機器のライフサイクルに沿った SBOM の具体的な価値として、例えば次のようなものが挙げられる。

- 社内利用状況の確認：社内評価や試験導入の段階で SBOM を用いることで、脆弱性やライセンス違反の有無を一覧で確認でき、問題のあるコンポーネントを早期に把握できる。

- 脆弱性対処：新たな脆弱性（CVE）が公表された際に SBOM と突合することで、影響を受け得る製品・バージョンを即時に特定でき、パッチ計画の立案を迅速化できる。これにより、関係者への報告にも根拠をもって対応しやすくなる。

- 情報提供：医療機関や規制当局からの照会に対し、SBOM を根拠として「脆弱性等に対して、どの機器が影響を受けるか」を説明できるため、情報提供に要する時間と担当者依存を低減し、MDS2 やアドバイザリー情報等の顧客向けセキュリティ文書を効率的に提供できる。

このように SBOM は、単に規制要求を満たすための資料ではなく、医療機器ライフサイクル全体にわたり、リスクマネジメントと業務効率の双方を底上げする仕組みとして位置付けられる。

2.3. SBOM の最小要素

SBOM に含めるべき情報の量や種類は、活用目的や組織の成熟度によって変わり得る。本ガイドラインでは第 1 版の最低限の要素として、NTIA による「The Minimum Elements for a Software Bill of Materials (SBOM)」に基づき、厚生労働省から発出されている「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)」（以下「手引書」という。）の附属書 A に示された最小要素（表１）を採用する。

具体的には、ソフトウェアコンポーネントのサプライヤーの名前、コンポーネント名、バージョン、その他の固有識別子（例：purl、CPE 等)、コンポーネント間の関係、SBOM の作成主体、タイムスタンプを、少なくとも医療機関等に提供される最終的な SBOM に含めることを基本とする。コンポーネントハッシュは、手引書においてオプション要素とされているが、後述する脆弱性管理や完全性検証の観点から、可能な限り付与する。

表 1: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
その他の固有識別子	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を識別するために用いる暗号学的ハッシュ（オプション）
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
SBOM の作成主体	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 (※1)

※1：タイムスタンプは、ISO 8601 形式で表記

さらに、米国 FDA のガイダンスでは、医療機器の市販前申請において NTIA ベースライン属性に従った機械可読な SBOM を提出することが推奨されるとともに、各ソフトウェアコンポーネントのサポート状態（例：保守継続／保守終了）やコンポーネントサポート情報（EOS、サポートレベル等）といったライフサイクル情報を把握し、医療機器のライフサイクルを通じたサイバ

ーセキュリティリスクマネジメントに活用することが求められている。

一方、米国では SBOM の項目や水準についての検討が進められており、上記の基本要素に加えて、ライセンス情報や SBOM の生成に用いたツールに関する情報、どの開発段階で生成された SBOM であるかを示す情報（例：ビルド時／リリース時など）を追加・強化すべき要素として位置付ける方向性が議論されている。また、SBOM は可能な限り完全なコンポーネント及び依存関係の一覧であることが望ましいとされており、依存関係を表現できない部分や情報が取得できない部分については、その旨を「既知の不明点（Known Unknowns)」として明示することが推奨されている。(例：外部からバイナリ形式で提供され、内部の依存関係を把握できないコンポーネントがある場合、その旨と理由を明記する。)

このように、本ガイドライン第 1 版における「最小要素」は、NTIA 最小要素及び厚労省から発行されている手引書を参考としつつ、国際的な動向を踏まえて、コンポーネントサポート情報（EOS、サポートレベル等）やライセンス情報といった要素を段階的に取り込んでいくことを前提とするものである。SBOM に求められる属性や粒度は今後も発展することが見込まれるが、製造販売業者等は、自社の成熟度や製品ポートフォリオに応じて、本節で示す最小要素を出発点とし、必要に応じて追加情報を拡張していくことが望ましい。

2.4. SBOM のフォーマット

SBOM データは機械可読かつ相互運用可能なフォーマットを用いて作成・共有されることが求められる。この際、共通的なフォーマットを用いることで組織内の管理が効率化されるほか、組織を越えて SBOM を共有する際の相互運用性が高まり、ソフトウェアサプライチェーンの透明性向上に寄与する。

なお、医療機器のサイバーセキュリティ導入に関する手引書では SWID（Software Identification Tag）も SBOM 用途に用いられるフォーマットの一つとして言及されているが、本ガイドラインでは新規導入時の推奨フォーマットとして SPDX 及び CycloneDX を基本とし、既存資産で SWID を用いている場合には、必要に応じて併用又は変換を検討するものとする。

医療分野で推奨される SBOM フォーマット（機械可読）は以下のとおりである。

・SPDX（Software Package Data Exchange）2.2 以上

・CycloneDX 1.6 以上

ただし、SBOM が複数のファイルで構成されている場合は、必ず SBOM の構成（フォルダを含む）を説明する文書を添える。

SPDX は、製品に含まれるソフトウェアをライセンス・著作権・入手元・依存関係など、法務・監査に必要な情報まで含めて細かく記録できる ISO/IEC 5962:2021 として国際標準化されたフォーマットである。その特徴は、単なるコンポーネント一覧だけでなく、ファイル単位の著作権情報やライセンス条件、コンポーネントの入手経路など、コンプライアンスに必要となる要素を体系的に整理できる点にある。

これにより、製品を構成するソフトウェアを「どこから取得し、どのライセンスのもとで利用しているか」を明確にでき、医療機器に求められる説明責任や品質保証の要求に対応しやすくなる。また、依存関係の階層構造を含めて詳細に記述できるため、複雑なソフトウェア構成の可視化や、開発から保守までの一貫した管理にも適している。

CycloneDX は、脆弱性管理や依存関係の評価を効率化するために設計された、セキュリティ重視の SBOM フォーマットである。ソフトウェア構成を記述する点は SPDX と同様だが、脆弱性情報、悪用可能性情報及びソフトウェアが提供・利用するサービスや外部インターフェイスといった運用・公開形態に関する情報など、サイバーセキュリティの実務に直結する要素を、軽量な構造で扱える点が特長となる。
特に、脆弱性が当該製品に影響するかどうかを示す VEX（Vulnerability Exploitability eXchange）と連携しやすく、医療機器のサイバーセキュリティ運用における対応判断を迅速化できる。

両者は目的や強みが異なり、SPDX は法的コンプライアンスに重点を置き、CycloneDX はセキュリティリスクの可視化と管理に特化している。どちらを採用するかは、製造販売業者等における優先事項や利用シナリオによって判断する必要がある。SBOM を異なるフォーマット間で変換する場合は、SBOM として必要な最小要素を保持するとともに、各国・地域の規制要求等に基づき個別に求められる要素についても、欠落なく維持されることを確認することが望ましい。

2.5. SBOM に関する誤解

SBOM には導入初期段階において様々な誤解が存在し、それが導入判断や運用定着の阻害要因となることが多い。本章では、医療機器分野で特に見られる代表的な誤解事例と、その事実関係を整理し、SBOM を正しく理解した上で活用するための考え方を示す。

・「SBOM を公開すると攻撃リスクが高まる」
SBOM は「攻撃者にとってのロードマップになり得る」と指摘されることがあるが、どのように管理・共有されるかが重要である。SBOM は主として防御側のための情報であり、透明性を高めることで脆弱性対応や影響範囲の特定を迅速化する役割を担う。一方で、SBOM に含まれる情報は、開示範囲や提供先によってはセキュリティ上の配慮が必要となるため、無制限な公開を前提とすべきものではない。攻撃者は SBOM が存在しなくてもリバースエンジニアリングという手法や既知の脆弱性情報を用いて攻撃を行うため、SBOM 非公開が攻撃抑止に直結するわけではない。医療機器においては、SBOM を適切に管理・共有することによる防御上のメリットが、リスクを上回ると考えられる。

・「SBOM では有益な情報も実用的な情報も得られない」
SBOM は単なる部品の一覧ではなく、ソフトウェアの構成可視化を通じて、サプライヤー、製造業者、並びに医療機器の運用・保守・セキュリティ対応を担う関係者を支援する実用的な

情報基盤である。例えば、サイバー攻撃や脆弱性情報が公表された際、SBOM を用いることで自社製品が影響を受けるか否か、影響範囲がどこまで及ぶかを迅速に判断できる。これは市販後安全対策やインシデント対応が重視される医療機器分野において、実務上有用である。

・「SBOM はセキュリティ部門だけが使うもので、開発や品質保証、薬事には関係ない」
SBOM はセキュリティ部門専用の情報ではない。開発部門にとっては、使用コンポーネントの把握や依存関係の整理、保守性の低下要因や将来的な更新・置換が必要となる要素の可視化に有用である。品質保証部門にとっては、変更管理や影響分析、規制当局対応の裏付け情報として活用できる。フィールドサービスや保守担当にとっても、個別機器の構成確認やアップデート計画立案の際の基礎情報として有用である。医療機器における SBOM は、開発・品質・セキュリティが連携するための共通言語として位置付けるべきである。

・「SBOM は作成だけすればよく、保守・管理は不要」
SBOM は一度作成して終わりではなく、ソフトウェア改訂やライブラリ更新に応じて継続的に更新・管理されることが前提となる。特に医療機器では、市販後も長期間にわたり製品が使用されるため、SBOM の陳腐化は脆弱性管理の形骸化につながる。SBOM はソフトウェアライフサイクル管理の一部として位置付け、構成管理・変更管理プロセスとして運用することが重要である。

・「SBOM ツールが出力したすべての脆弱性に対応する必要がある」
SBOM ツール内の脆弱性検索機能や脆弱性スキャンツールが検出する結果には、実際には悪用不可能なものや、当該製品構成では影響を受けないものも含まれる。医療機器では、患者安全や装置の安定稼働を考慮し、リスク評価、影響範囲、対応コストを踏まえた優先順位付けが不可欠である。SBOM は意思決定を支援する情報であり、すべての検出結果に機械的に対応することを求めるものではない。

・「SBOM は導入にコストがかかりすぎて、中小規模の製造販売業者には不向き」
SBOM 導入には、概念理解やツールの操作・運用に関する学習コスト、並びにツール導入等の初期コストが生じる。しかし、無償の OSS ツールや段階的導入を活用することで、過度な負担を避けることが可能である。また、脆弱性対応の効率化、規制対応の簡素化、インシデント発生時の対応迅速化といった中長期的な効果を考慮すれば、SBOM は規模を問わず合理的な投資と位置付けられる。重要なのは、自社の導入目的に応じた範囲で SBOM を活用することである。

・「SBOM は OSS だけ管理すればよく、自社開発コードや商用コンポーネントは対象外」
SBOM は、製品に含まれる OSS のみを対象とするものではなく、自社開発ソフトウェア、商用ソフトウェアコンポーネント（OTS ソフトウェア）、サードパーティ製ライブラリ等を含む、ソフトウェア構成全体を可視化するための情報である。医療機器においては、市販後の長期使用および患者安全への影響を考慮し、OSS に限定しない包括的な SBOM 管理を行うことが必

要である。

・「SBOM は一つの Excel があれば十分で、ツールや正規化までは不要」

SBOM は、単なるソフトウェア部品の一覧表ではなく、構成情報を標準化された形式で記述し、機械的に解釈・活用できる状態で管理することを前提とした情報基盤である。医療機器分野においても、国際的な動向を踏まえ、SBOM フォーマットとして SPDX や CycloneDX の利用が求められている。SBOM 導入は一度にすべてを実現する必要はなく、導入初期に Excel 等で主要コンポーネントを可視化し、関係者間で構成認識を揃えることは有効である。ただし、Excel のみの運用では、表記揺れの抑止、更新漏れの防止、ソフトウェア識別子を用いた自動照合、変更履歴の一貫管理に限界がある。実運用として SBOM を継続的に活用するためには、運用成熟度に応じて、標準フォーマットへの対応、ツールによる一元管理、並びに複数 SBOM 間の表記揺れを吸収する正規化を段階的に導入する必要がある。

・「SBOM ツールを導入さえすれば、それ自体が完全なセキュリティ対策となり SBOM 対応は完了となる」

SBOM ツールは、構成情報の収集、整理及び更新を効率化するための手段に過ぎず、それ自体が脆弱性の除去やインシデントの防止を自動的に実現するものではない。SBOM を実効的なセキュリティ向上につなげるには、まずソフトウェアライフサイクル管理、変更管理、是正措置対応など、組織内の既存プロセスに SBOM 運用を組込み、運用手順を整えることが前提となる。

その上で、SBOM を基に脆弱性管理やインシデント対応を継続運用することで初めて実効的なセキュリティ向上にはつながる。ツール導入だけに留まる場合、形式的な対応に終わりやすい点に留意する。

・「ツールで SBOM を生成しさえすれば、その内容は自動的に正しいので、特に検証は要らない」

ツールで出力した SBOM を無条件に正とみなすのは医療機器ソフトウェアの品質保証上リスクがある。SBOM の正確性・完全性は、解析対象の定義、ビルド手順、ツール設定や検出能力、運用プロセスに依存し、静的リンク OSS や改変コンポーネント、生成物の取り扱いについては注意が必要である。

そのため、重要なのは SBOM を生成するツールおよびその運用プロセスが、意図した目的に照らして妥当であることを確認するという考え方である。SBOM 生成ツールについてもコンピュータ化システムバリデーションの考え方を踏まえ、意図した用途に対して適切に機能していることを確認した上で、その成果物を有効な情報として扱う。

SBOM は生成時点で完成するものではなく、検証・評価・改善を前提とした運用により、サイバーセキュリティリスクマネジメントおよび規制対応に資する信頼性を継続的に確保する必要がある。

3. SBOM 導入・運用に関する基本方針

3.1. SBOM 導入・運用の基本方針

医療機器における SBOM の導入は、単なる文書作成や規制対応に留まるものではなく、ソフトウェアのライフサイクル全体を通じた安全性・品質・保守性の向上を目的とするものである。
特に、脆弱性情報の公開やインシデント発生時において、ソフトウェア開発部門や品質保証部門、PSIRT を含む関係者が影響範囲を迅速に特定し、適切な初動対応を行う必要がある。このため、ソフトウェア構成および影響範囲を把握するための情報として、SBOM の整備は市販後を含む運用フェーズにおいて実務上の有用性が高まっている。
製品に組み込まれるソフトウェアは、自社開発ソフトウェアに限らず、OSS、購入ライブラリや OTS ソフトウェア等の多様な構成要素から成り立っている。これら全てのソフトウェアアイテムについて、安全性およびセキュリティへの影響度に応じた分類を行い、リスクマネジメントの対象として管理することが求められる。
製造販売業者は、製品全体としての安全性・セキュリティリスク管理について最終的な責任を負う一方で、OTS ソフトウェアの修正や保守については、サプライヤー等との契約関係に基づき、各当事者が役割分担して対応することが一般的である。SBOM は、このような責任分担を前提としてソフトウェア構成要素を可視化し、脆弱性発生時における影響範囲の迅速な把握および対応判断を支援するための共通情報として位置づけられる。
SBOM の自動生成は、それだけで目的を達成するわけではないものの、開発者の認識と実際のビルド成果物との乖離を検出し、ソフトウェア構成の事実関係を客観的に把握するための有効な手段として位置づけられる。一方で、製品規模やソフトウェア構成、組織体制は企業ごとに大きく異なるため、初期段階から網羅的かつ高度な SBOM 運用を求めることは、かえって形骸化を招く恐れがある。
そのため、本ガイドラインでは、SBOM を段階的に導入・拡張していくことにより、現場で実効性のある運用を確立することを基本方針とする。まずは自組織が SBOM によって解決したい課題と導入目的を明確化し、それに応じた最小限の範囲・項目から着手し、組織の成熟度や運用実績に応じて段階的に高度化していくことが重要である。

第 1 段階：SBOM 作成・更新体制の確立（導入フェーズ）
第 1 段階では、SBOM の最小要素を踏まえ、SBOM を作成・更新できる体制を整備し、対象製品に対して SBOM を作成し、変更管理できる状態を確立することを目的とする。
この段階においては、SBOM のフォーマットとして SPDX や CycloneDX など、国際的に広く認知された標準仕様を土台とすることが重要である。独自仕様に閉じた SBOM を初期段階から採用することは、将来的な規制要求への対応や、サプライヤー・取引先との情報連携を阻害する要因となり得るため、国際標準との接続性を前提とした設計とする必要がある。これにより、将来的な SBOM の拡張やツール導入、規制当局からの情報提供要請への対応を円滑に行うことが可能となる。
SBOM に記載する情報については、導入初期段階では SBOM の最小要素を中心とした構成情報

を対象とし、ソフトウェアコンポーネントの識別、名称、バージョン、サプライヤー情報等の基本的な項目を正確に管理できることを重視する。また、SBOM は一度作成して終わりとするものではなく、ソフトウェア改訂や構成変更に応じて更新される情報資産であることから、変更管理プロセスと紐づけて管理する運用を確立することが求められる。
あわせて、SBOM の作成、更新、保管、社内外への提供に関する役割と責任を明確化し、開発部門のみならず、品質保証、薬事・規制対応、PSIRT・セキュリティ部門など、関係部門間で共通認識を形成することが重要である。初期フェーズでは、特定製品や限定的な範囲で運用を開始し、運用負荷や課題を把握したうえで、対象範囲を段階的に拡大していくことが現実的な進め方となる。

第 2 段階：QMS・市販後安全管理との統合（高度化フェーズ）
第 2 段階では、第 1 段階で整備した SBOM 作成・管理体制を、脆弱性管理、ライセンス管理、EOL／EOS 管理などの既存の QMS および市販後安全管理プロセスと統合し、SBOM を医療機器ライフサイクル全体のリスクマネジメントへと発展させることを目指す。
医療機器は、市販後における長期使用および継続的な保守管理が前提となるため、SBOM は開発段階のみで参照される情報ではなく、市販後対応を含むライフサイクル全体を通じて活用される情報資産として位置付ける必要がある。そのため、製品の想定使用期間や保守契約期間を考慮した SBOM の保管期間を設定するとともに、ソフトウェア改訂履歴、是正措置、セキュリティ対応履歴等と紐づけて管理することが求められる。
この段階では、SBOM に記録する情報についても、導入初期の最小要素に留まらず、コンポーネント間の依存関係、ライセンス情報、EOL／EOS 情報など、脆弱性影響評価や保守判断において実務上の有用性が高い情報を段階的に拡充していくことが望ましい。これにより、外部で公表された脆弱性情報が自社製品に与える影響を迅速かつ体系的に評価し、是正措置や顧客対応を一貫した判断基準のもとで実施することが可能となる。
また、SBOM を中心とした情報連携を通じて、PSIRT 活動や市販後安全管理、品質マネジメントとの連動を強化することで、SBOM は単なる構成情報の一覧ではなく、医療機器の安全性・信頼性を支える実効的なリスクマネジメントとして機能するようになる。

3.2. SBOM 導入・運用体制およびプロセス

医療機器における SBOM 導入・運用は、単なる一覧作成ではなく、製品ライフサイクル全体を通じたソフトウェア構成管理及びサイバーセキュリティ対応を支える中核的な管理手段として位置付ける必要がある。そのため、SBOM は開発活動の一部として限定的に扱うのではなく、組織横断的な運用体制のもとで一貫したプロセスとして確立しなければならない。
SBOM 導入・運用に関する役割を整理し、各役割における主な実施事項及び概要を下記に示す。なお、医療機器の SBOM の作成責任は原則として製造販売業者が負うものとする。OSS、OTS ソフトウェア、外部ベンダー製ソフトウェア等についてサードパーティから SBOM 情報の提供を受ける場合であっても、その内容の妥当性確認、統合、管理は製造販売業者が実施する。

			社内関係者					
フェーズ	ステップ	実施概要	開発部門	品質保証部門	薬事部門	法務部門	サービス部門	PSIRT
環境構築・体制整備	適用範囲の明確化	対象ソフトウェアを精査し適用範囲を明確化する。	✓					✓
	ツールの選定	選定観点を整理し、評価・選定を行い潜在課題整理を行う。	✓					✓
	ツールの導入・設定	選定評価時の顕在課題を解決し、導入・設定を行う。	✓					✓
作成・共有	コンポーネント定義	対象ソフトウェアの構成要素を識別・整理し根拠立てを行う。	✓	✓				✓
	SBOMの作成	要件(記載要素、フォーマットなど)に沿った作成を行う。	✓					✓
	SBOMの管理	統合、編集などのプロセス、アクセス権限等のルールを定める。	✓	✓				✓
運用	脆弱性情報の収集	脆弱性情報との効果的・効率的な照会方法を定める。		✓				✓
	ライセンスの管理	ライセンス評価ポリシーを定める。	✓	✓		✓		✓
	影響調査と対応要否	優先度付け(トリアージ)定義したプロセスを定める。	✓	✓				✓
	対処	製品・事業の対外的関係者を考慮したプロセスを定める。	✓	✓			✓	✓
	開示	決定方針に沿った開示・情報提供を行う。		✓	✓		✓	✓

図 2：SBOM 導入・運用に関するプロセスと関係者の関与例

役割	主管部署	所掌範囲例
SBOMの導入を主管する	PSIRT	› 企業内でのSBOM導入推進（啓蒙・構想・利害関係者明確化など） › 外部ベンダー調査・情報収集 › 外環境情報の収集
SBOMを作成する	開発	› ツール利用による解析・特定フォーマットでの出力
申請・開示を行う	薬事/法務	› SBOM内容から申請・開示内容に沿った形式へ変換
SBOMを運用・管理する	品質管理	› SBOMの運用・管理方針の策定（アクセス制御・保管ポリシーなど）
脆弱性を管理する	セキュリティ統括/PSIRT	› 管理下にある脆弱性情報との照合 › 自社インシデント対応プロセス効率化
ライセンスを管理する	開発/品質管理/法務	› SBOM内容からライセンス利用状況・種別を確認 › ライセンスの監査（ライセンス違反の確認）

図 3：SBOM 導入・運用に関するプロセスと関係者の役割例

SBOM を導入した後、その効果を最大限に発揮するためには、組織内の複数部門が一体となって取り組む体制が不可欠である。開発、品質保証、薬事並びに法務部門、サービス部門及び PSIRT/セキュリティ担当部門に加え、外部ベンダーソフトウェアや開発委託先など、SBOM の作成・評価・活用にそれぞれ異なる役割をもつ関係者が、相互に情報を共有し、プロセス全体を通じて継続的に連携することが求められる。この協力体制が確立されることで、脆弱性の迅速な把握と

対応が可能となり、製品ライフサイクル全体にわたってセキュリティ水準と品質が大幅に向上する。さらに、外部からの問い合わせや規制要求に対しても一貫性のある説明が可能となり、組織としての信頼性向上にも寄与する。SBOM の運用は単なる技術的取り組みに留まらず、組織全体のガバナンス強化を促す仕組みとして位置づけるべきである。

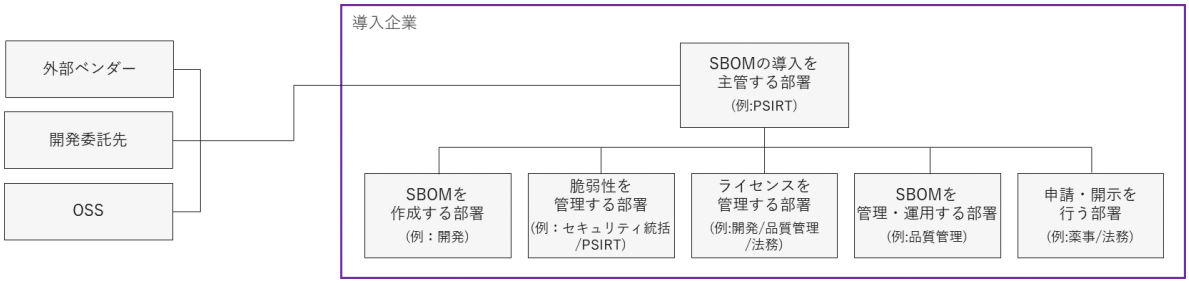


図 4：社内外の関係組織例

4. 計画段階（環境構築・体制構築）における実施事項

4.1. SBOM 適用範囲の明確化

SBOM を実効的に運用するためには、対象とする医療機器、並びに機器内部のどのハードウェアコンポーネント上で動作するソフトウェアを SBOM の適用範囲とするかを、計画段階で明確に定義しておくことが重要である。適用範囲が曖昧なまま SBOM を作成すると、重要なコンポーネントの漏れや、実務上過大な範囲を対象とすることにつながり、リスクマネジメントや保守運用に支障を来す恐れがある。

本項では、対象ソフトウェアの構成や特性を整理し、SBOM の適用範囲を体系的に可視化するための検討事項を示す。

医療機器における SBOM の適用範囲は、ソフトウェアの構成やアーキテクチャに応じて大きく異なる。本ガイドラインでは、典型的な医療機器ソフトウェア構成を以下の 4 パターン（A～D）に分類し、それぞれについて SBOM の適用範囲を検討する。

表 2:ソフトウェア構成例

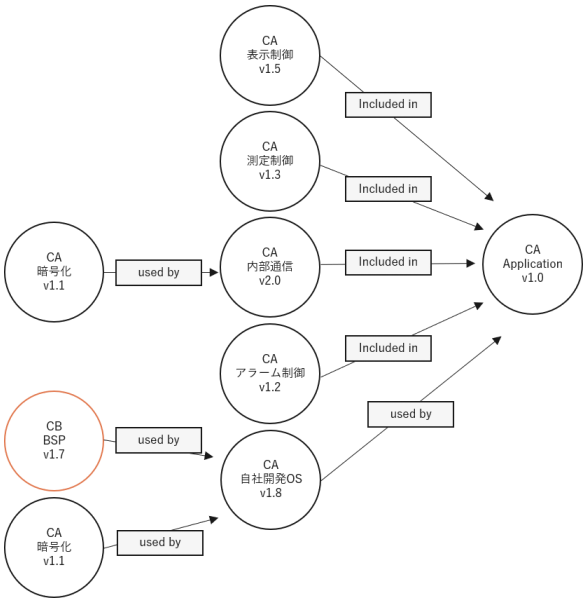
パターン	ソフトウェアの構成	製品例
A	自社開発コード主体の組込みソフトウェア	➢ 電子血圧計 ➢ パルスオキシメーター ➢ 携帯型心電計 ➢ 小型輸液ポンプ
B	自社開発コードと商用 OS 上で動作する機器搭載ソフトウェア	➢ ベッドサイドモニター ➢ 人工呼吸器 ➢ 透析装置 ➢ 検体検査装置
C	SaMD（Software as a Medical Device）として提供されるソフトウェア	➢ 画像解析プログラム ➢ AI 診断補助プログラム ➢ 病態管理支援アプリ
D	A～C を組み合わせて構成されるソフトウェア	➢ MRI システム ➢ CT システム ➢ 生体情報モニタリングシステム

これらは SBOM 適用範囲を検討する際のモデルケースであり、実際の製品は複数のパターンが混在する場合もある。その場合は、対象製品を構成する各ソフトウェア部分を本パターンに当てはめ、それぞれについて SBOM の適用範囲を明確化する。

個々の構成要素ごとの SBOM に加え、それら構成要素間の関係性を示すシステム全体の SBOM 又は構成図を用意することで、ライフサイクル全体を通じたリスクマネジメントに活用しやす

くなる。図 5 は医療機器におけるソフトウェア構成が確定した段階で整理される SBOM の最終的な構成イメージを示したものである。具体的には、機器を構成するハードウェアコンポーネントごとに動作するソフトウェア要素を整理し、それらの依存関係や階層構造をコンポーネントツリーとして可視化するとともに、各コンポーネントの名称、バージョン、提供元、依存関係等の情報をコンポーネント表として整理した状態を示している。

実際の SBOM 作成プロセスでは、設計・実装の進行に伴いソフトウェア構成が段階的に明確化されるが、最終的には図 5 に示すような構成関係が整理された形で SBOM が生成されることを想定している。本図はその完成形の一例を示すものであり、各医療機器のアーキテクチャに応じて階層構造や構成要素の粒度は適宜調整される。



ID	Component Name	Supplier	Version	Author	Hash	UID	Relationship	Relationship Completeness
1	Application	CA	1.0	CA	0x111	111	Primary	Known
2	表示制御	CA	1.5	CA	0x222	222	Included in ID1	None
3	測定制御	CA	1.3	CA	0x333	333	Included in ID1	None
4	内部通信	CA	2.0	CA	0x444	444	Included in ID1	Known
5	暗号化	CA	1.1	CA	0x555	555	Used by ID4,ID7	None
6	アラーム制御	CA	1.2	CA	0x666	666	Included in ID1	None
7	自社開発OS	CA	1.8	CA	0x777	777	Used by ID1	Known
8	BSP	CB	1.7	CA	0x888	888	Used by ID7	Unknown

※CA…Company A, CB…Company B の略式表現

図 5:構成要素間における SBOM 概念図表

4.1.1. A. 自社開発コード主体の組込みソフトウェア

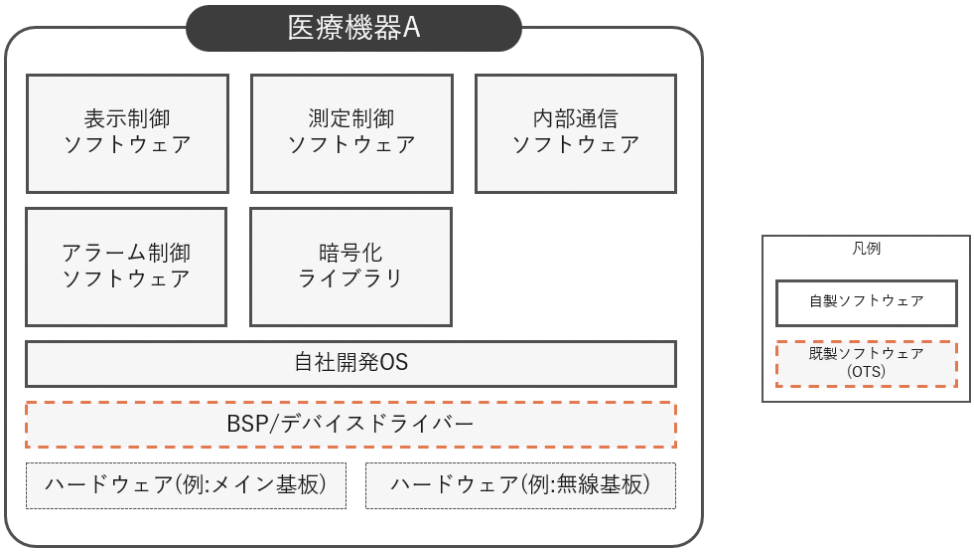


図 6:医療機器 A のソフトウェア構成（例）

◆　ソフトウェア構成に関する前提

専用ハードウェア上で動作するファームウェアが中心であり、商用 OS は使用せず、ベアメタル又は簡易なランタイム上に自社開発コードを実装する構成を前提とする。場合によっては、タスクスケジューリングやメモリ管理などの基本機能のみを備えた自社開発の軽量 OS を用いる構成も含まれる。一部、コンパイラに付属する標準ライブラリやベンダーが提供する数値計算・暗号化・通信などの外部ライブラリなどの自社開発以外のソフトウェアコンポーネントを利用する場合がある。

◆　特徴

ソフトウェア構成の大部分が自社管理下にあるため、コンポーネントの把握や変更管理は比較的容易である。一方で、外部ライブラリやツールチェーン、ボードサポートパッケージ（BSP）、ベンダー提供の組込みライブラリ等に含まれるコンポーネントが暗黙的に利用されていることがあり、一般的な SBOM ツールによる自動検出が難しく、これらに含まれるサードパーティコンポーネントが SBOM から漏れやすい。

また、ネットワーク接続性が限定的であることから、アップデート頻度が低く、古いコンパイラ／ライブラリ由来の脆弱性や非推奨アルゴリズムが長期間残存するリスクがある。

◆　SBOM の適用範囲

このパターンでは、少なくとも次のようなコンポーネントを SBOM の対象に含める。

- 自社開発ファームウェア本体（識別可能な範囲のコンポーネント単位）
- リンクしている外部ライブラリ（コンパイラ付属ライブラリ、数学・暗号・通信ライブラリ等）
- ベンダー提供のミドルウェア相当コンポーネント（評価ボード用ライブラリ等）を利用している場合は、その名称・バージョン

- SoC/FPGA や周辺機器（通信モジュール等）の更新可能なファームウェア
- ベンダー提供のボードサポートパッケージ（BSP）、スタートアップコード等に含まれるサードパーティコンポーネント
- ビルドツールチェーン（コンパイラ、リンカ等）に起因するランタイムライブラリで、医療機器内に組み込まれるもの

一方、ビルド専用ツールや試験専用のテストコード等、最終的な医療機器製品に組み込まれないコンポーネントは、通常 SBOM の対象外とできる。

4.1.2. B. 自社開発コードと商用 OS 上で動作する機器搭載ソフトウェア

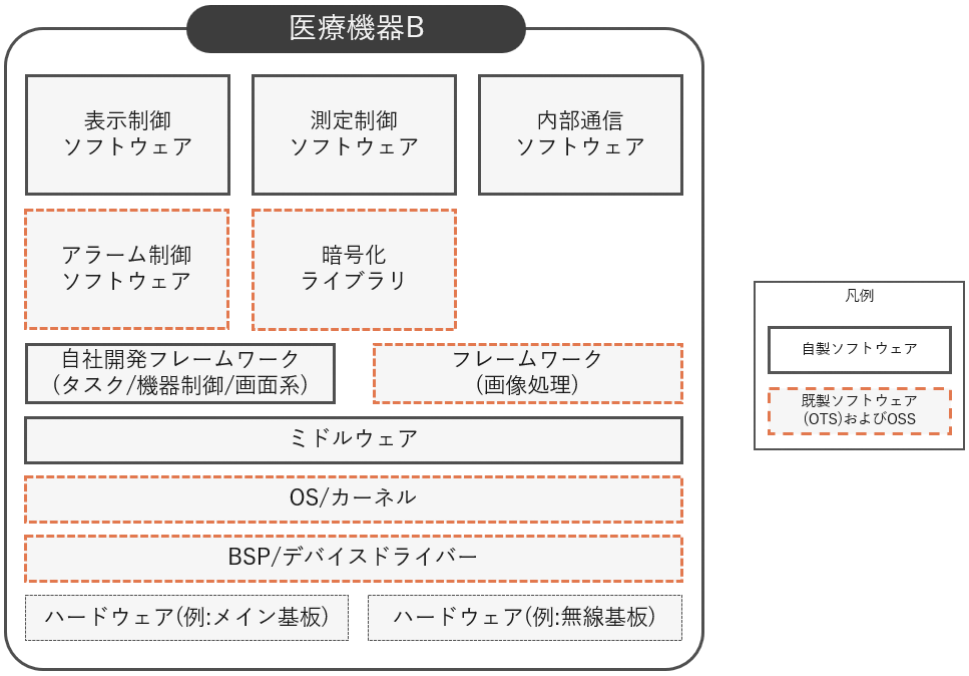


図 7：医療機器 B のソフトウェア例

◆ ソフトウェア構成に関する前提

本パターンに該当する医療機器は、Windows、Linux、RTOS 等の商用 OS 上で動作し、その上で複数のソフトウェア層が相互に依存しながら動作する構成を前提とする。典型的には、OS、デバイスドライバー、ミドルウェア、ランタイム、アプリケーションソフトウェアといった階層構造を有しており、各層は明示的・暗黙的な依存関係によって結合されている。

また、製品内部で動作するソフトウェアは、自社開発コードのみで完結するものではなく、外部ベンダーが提供する OTS ソフトウェア、オープンソースソフトウェア（OSS）、及びそれらに内包される推移的依存コンポーネントを含む複合的な構成となる。このため、SBOM の対象範囲を定義する際には、単一の成果物や表層的な構成に限定せず、ソフトウェア全体の実行環境を俯瞰した整理が必要となる。

◆ 特徴

本パターンの最大の特徴は、ソフトウェア構成の一部が自社による完全な管理下にない点にあ

る。
製品には、商用 OS そのものに加え、OTS ソフトウェア、OSS などが組み込まれており、これらの中にはソースコードが公開されていない、あるいは詳細な内部構成が把握しにくいものも含まれる。
さらに、アプリケーションが利用するライブラリが別のライブラリに依存し、その依存先がさらに別のモジュールに依存する、といった多段的な依存構造が一般的に形成される。このような構造は、機能拡張性や開発効率の面では有効である一方、脆弱性が発見された場合には、影響範囲が OS レベルからアプリケーション層まで広範に波及する可能性が高いというリスク特性を有する。そのため、SBOM を用いた脆弱性管理や影響分析を実効的に行うためには、依存関係を含めたソフトウェア構成の全体像を正確に可視化することが不可欠となる。

◆ SBOM の適用範囲

本パターンにおける SBOM の適用範囲は、製品内部で動作するすべてのソフトウェアコンポーネントを原則とする。対象は自社が開発したアプリケーションやモジュールに限定されるものではなく、以下を含めて包括的に整理する必要がある。商用 OS 及びその構成要素、製品に組み込まれている外部提供ソフトウェア、オープンソースソフトウェア、開発委託契約を伴わずに導入されたツール類、並びにそれらが内部的に依存しているすべてのソフトウェア要素が SBOM の対象となる。
特に、直接的に製品機能を構成していないように見えるランタイム、フレームワーク、ユーティリティライブラリ、パッケージ管理システム経由で導入されるコンポーネントについても、実行環境の一部として SBOM に含めることが重要である。これにより、脆弱性情報やライセンス情報が公開された際に、当該医療機器への影響有無を迅速かつ客観的に判断できる体制を構築することが可能となる。

このパターンでは、少なくとも次のようなコンポーネントを SBOM の対象に含める。

- 機器搭載アプリケーション本体（自社ソフトウェアを含み、主要機能単位又はモジュール単位で識別可能な範囲）
- アプリケーションが直接利用する外部ライブラリ（数値計算、画像処理、通信等）及びそれらの依存ライブラリ
- 製品に組み込まれているオープンソースソフトウェア（OSS）コンポーネント
- 商用 OS 上に追加インストール又は同梱しているミドルウェア、フレームワーク、ランタイム（例：.NET Framework、Java、Python 等）
- 製品機能の実現や安全性・基本性能に直接関与する OS 上のサービスや追加コンポーネント（特定の Web サーバー、DB サーバー、通信スタック、デバイスドライバー等）
- 外部ベンダーから提供される OTS ソフトウェアや、開発委託契約を伴わずに導入されているツール類

本パターンにおける SBOM の適用範囲は、原則として当該医療機器の製品内部で動作するすべてのソフトウェアコンポーネントを対象とする。ただし、すべての階層を一度に網羅することが

現実的でない場合も多いため、導入初期段階では、機器搭載アプリケーション、製品に組み込まれているミドルウェアやランタイム、OS 上のサービスや追加コンポーネント等のトップレベルコンポーネントを対象とする段階的導入が有効である。その上で、パッケージマネージャーの依存関係情報やサプライヤーから提供される SBOM 等を活用し、取得可能な範囲から順次、下位の依存コンポーネントへと適用範囲を拡張していく。

4.1.3. C. SaMD（Software as a Medical Device）として提供されるソフトウェア

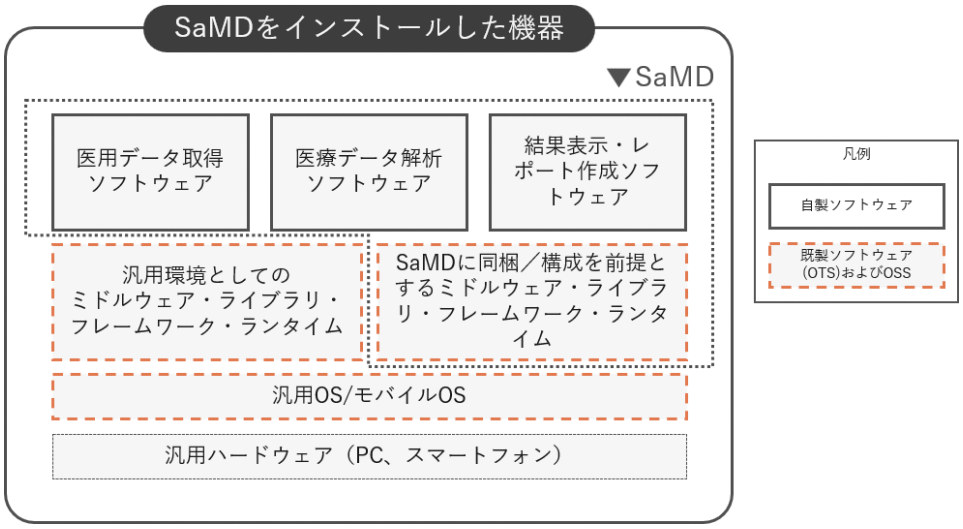


図 8:医療機器 C のソフトウェア構成（例）

◆ ソフトウェア構成に関する前提

汎用 OS（例：Windows、Linux）やモバイル OS（例：iOS、Android）上で動作するプログラム医療機器（SaMD）を対象とする。CT／MRI 画像から病変候補を検出する画像解析ソフト、心電図データを解析する診断補助ソフト、スマートフォン上の糖尿病管理アプリ等が典型例である。アプリケーション本体に加え、ランタイム（.NET Framework、JVM、Python 等）、Web／GUI フレームワーク、外部ライブラリ（画像処理、数値計算、暗号・通信等）、データベースや Web サーバー等のミドルウェアが組み合わさる構成を前提とする。

◆ 特徴

OSS や OTS ソフトウェアを含む多数のコンポーネントに依存しており、ソフトウェア構成は層構造かつ多段の依存関係を形成する。また、ランタイムやフレームワークが動的リンクライブラリやプラグインを自動的に取得・ロードし、外部 API やクラウドサービスに依存することで実行時に構成が変化することもあり、開発チームだけでは実際の利用コンポーネントを完全に把握することは難しい。このように、SaMD の特定バージョンにおいてどのコンポーネントが用いられているかを明確にしないまま運用を続けると、後から脆弱性やサポート終了の影響範囲を特定することが困難になる。

◆ SBOM の適用範囲

このパターンでは、少なくとも次のようなコンポーネントを SBOM の対象に含める。

- SaMD 本体のアプリケーションモジュール（フロントエンド／バックエンド等を含む）
- 使用しているフレームワーク及びランタイム（例：.NET Framework、Java、Python 等）
- 外部ライブラリ（画像処理・数値計算・暗号・通信等）、及び組み込みデータベースやメッセージング等のミドルウェア
- SaMD の安全性・性能に直接関与する OS 上の追加コンポーネント（特定の DB サーバー、Web サーバー、ドライバー等）

汎用 OS に標準搭載される全コンポーネントを過不足なく列挙することまでは必ずしも求めないものの、SaMD の基本性能・安全性に直接関与するコンポーネント、及び標準構成から追加でインストール・同梱しているコンポーネントを中心に、SaMD の機能に支障が生じる又は安全性の懸念が生じるサイバーセキュリティに係る危険性を低減する管理ができるよう SBOM の範囲を定義する必要がある。

なお、SaMD がクラウドサービスや SaaS 型サービスに依存する場合であっても、本ガイドラインでは、当該クラウドサービス内部のすべてのコンポーネント情報を製造販売業者等が把握し SBOM に含めることまでは求めない。

ただし、

- 医療機器の安全性・基本性能に直接関与するクラウドコンポーネント（例：医療データを保管するマネージド DB、画像解析エンジンなど）
- 製造販売業者等が契約や仕様書により、バージョンやサポートポリシーを管理しているコンポーネント

については、可能な範囲で SBOM 又は関連文書に構成情報を記録し、SaMD の機能に支障が生じる又は安全性の懸念が生じるサイバーセキュリティに係る危険性を低減する管理ができるようリスクマネジメントに活用する必要がある。

4.1.4. D. A～B を組み合わせて構成されるソフトウェア

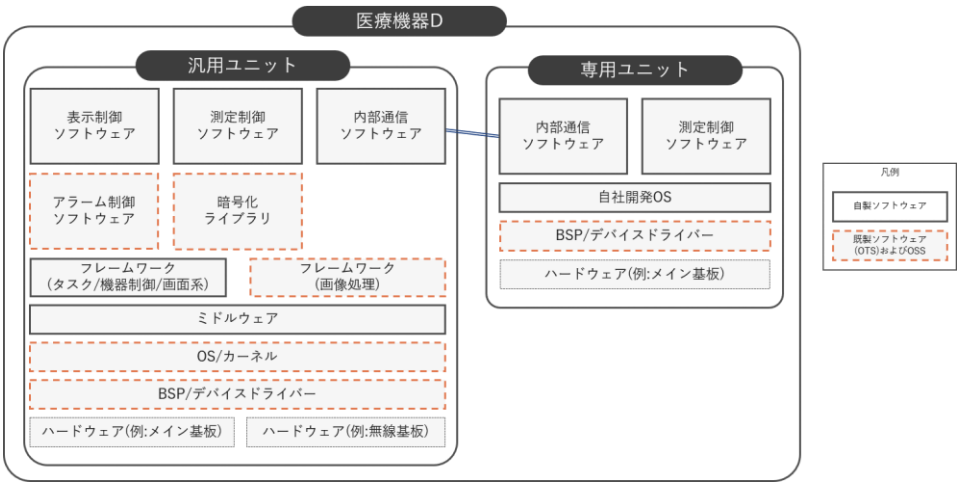


図 9:医療機器 D のソフトウェア構成（例）

◆　ソフトウェア構成に関する前提

本パターンは、複数のソフトウェア構成パターン（A、B）を組み合わせて、1 つのシステムとして提供される医療機器を想定する。

MRI／CT システム、生体情報モニタリングシステム、検体検査システム等が典型例であり、例えば以下のような構成要素を含む。

- 測定ユニット等、自社開発コード主体の組込みソフトウェア（パターン A）
- 撮像装置やベッドサイド端末や制御コンソール等、OS 上で動作する機器搭載ソフトウェア（パターン B）
- 装置本体とは別に設定された端末やクラウド上で動作する解析用ソフトウェアやビューワ等のソフトウェア

これらがネットワークで相互接続され、システム全体として 1 つの医療機器、あるいは一体的に使用される医療機器群として設計・提供される構成を前提とする。

◆　特徴

システムを構成する各要素は、それぞれ異なるライフサイクルや更新サイクル（機器ソフトウェアの更新、周辺機器の追加・交換等）を持ち、部分的な更新や構成変更が行われることが多い。

個々の構成要素のソフトウェアは、

- メーカーが自社で完全に管理している部分（パターン A）と、
- 商用 OS やミドルウェア、OSS／OTS 等のサードパーティコンポーネントに依存する部分（パターン B）

が混在する。

システム単位で医療機関に導入される際、導入サイト固有の構成（接続される端末数、モジュールの有無、ネットワーク構成等）が設定されることが多く、「製品全体」と「個々の構成要素」の両方の観点で構成を把握することが、脆弱性管理やレガシー医療機器管理において重要となる。

◆ SBOM の適用範囲

このパターンでは、「構成要素ごとの SBOM」と「システム全体を俯瞰する SBOM」の二層構造で考える。

- 構成要素ごとの SBOM
  - システムを構成する各ソフトウェア部分（例：撮像装置、制御コンソール、解析ワークステーション、サーバーアプリケーション等）ごとに、医療機器 A、B の考え方に従って SBOM を作成する（各パターンの詳細はそれぞれの項を参照）。
- システム全体を俯瞰する SBOM／構成情報
  - システムとしての製品型番や構成パターンと、それを構成する各要素（A、B の各医療機器）との対応関係を整理し、「どのシステム構成・どの設置サイトに、どの構成要素が含まれているか」を把握できるようにする。
  - このとき、構成要素ごとの SBOM への参照（ファイル名やドキュメント ID 等）を持たせておくことで、特定のコンポーネントに脆弱性やサポート終了が発生した際に、影響を受け得るシステム構成を迅速かつ効率的に特定できる。

4.2. SBOM ツールの選定

SBOM 導入組織は、あらかじめ明確化した SBOM 適用範囲に基づき、適切な SBOM を作成・管理できる環境及び体制を整備する必要がある。SBOM 作成・管理を実施する上で中心的な役割を担うのが SBOM ツールであり、対象ソフトウェアの規模や構成、組織の開発体制を踏まえたツール選定が極めて重要となる。
SBOM は必ずしもツールを用いなければ作成できないものではなく、手動で作成・管理することも理論上は可能である。しかしながら、医療機器ソフトウェアのように構成が複雑化・高度化する環境においては、開発者が明示的に認識していない間接的な依存関係や、ビルド工程により自動的に取り込まれるコンポーネントまで含めて構成を把握することが求められる。

このような要求に対し、SBOM ツールを活用することで、コンポーネント管理に要する工数が大幅に削減されること、コンポーネント間の依存関係や再利用部品を効率的に把握できること、さらに、新規の脆弱性公表から影響する製品や範囲を特定するまでのリードタイムを短縮できること、など、SBOM ツールを利用するメリットは大きい。
本ガイドラインでは、SBOM ツールを活用した SBOM の作成・管理を前提とし、ツール選定にあたって考慮すべき観点及び留意事項を整理する。

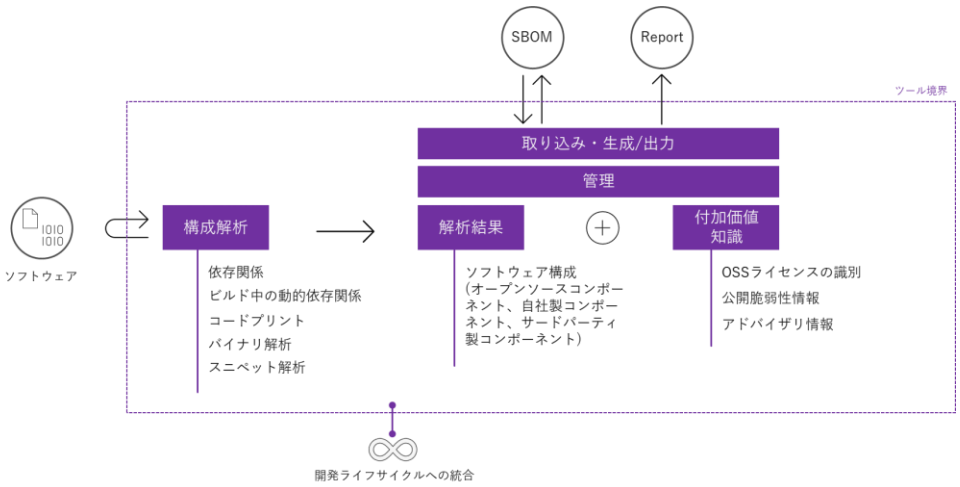


図 10:SBOM ツールの選定時における概要整理参考例

4.2.1. SBOM ツール選定の観点

SBOM ツールを評価・選定する際には、SBOM 導入の目的及び適用範囲を踏まえ、以下のような観点についてあらかじめ整理する。

表 3：SBOM ツールの選定基準の一例

機能	ツールによってサポートしている機能が異なる
	目的（SBOM 作成、脆弱性管理、開発支援、規制対応等）や適用範囲から必要機能を選定する
性能	誤検出（OSS 検出や脆弱性ライセンス情報のマッチング精度）や検出漏れの発生度合い
	新たな脆弱性が反映されるスピードはどうか
解析可能な情報	脆弱性やライセンスが自動で解析できる
	追加情報や精度などの強みがあるか
解析可能なデータ形式	ファイル形式（拡張子別の対応可否）、パッケージマネージャー種別などのサポート範囲
コスト	ライセンス体系や料金体系の定義
	課金方法（解析コード量や開発者数）
	スケールメリットの有無
対応フォーマット	出力できるフォーマット
	インポートできるフォーマットの種類（SPDX,CycloneDX）
コンポーネント解析方法	事前に定めた解析方法（コード解析、ビルド情報解析、バイナリ解析など）を満たした解析方法か
	解析方法によって正確度が落ちるが、許容可能か
	コードマッチ、スニペットマッチ、バイナリ解析など
	複数の解析が使えるツールもある
サポート体制	ツール以外の問い合わせが可能なプラン、無償ツールのサポート
	担当者の知識レベルに応じてサポート契約
他ツールとの連携	開発～ライフサイクル全般の効率化のための連携（開発環境やビルドツール、コンテナスキャンツール連携など）
提供形態	オンプレ版とクラウド版サーバー維持管理費用も考慮する
	クラウド版は機密性の担保に注意が必要
日本語対応	日本語対応している開発元は少ない
	販売代理店が取扱説明書を日本語訳している場合もあり
ユーザーインターフェイス	CLI 又は GUI 提供
	GUI 対応ツールの場合、直感的な操作と結果の可視化が可能
運用方法	開発環境と連携して開発者の負担軽減
	自動化の簡易さにより解析精度の向上や運用効率化が見込める
ソフトウェア開発言語	C 言語や C++等であれば多くのツールがサポートしているが、一部の言語は対応しているツールが限定的

4.2.2. SBOM ツール選定にあたっての留意事項

SBOM ツールの選定においては、単に機能の多さや価格のみで判断するのではなく、導入目的や運用形態との適合性を総合的に評価することが重要である。まず、複数の SBOM ツールを目的別に使い分けることは、運用が複雑化し、結果として管理コストや人的負担が増大する要因となり得る。そのため、特段の理由がない限り、目的に対して最小限のツール構成で運用できるかどうかを検討する。
SBOM ツールには有償・無償のものが存在するが、有償／無償という区分はあくまで提供形態の違いであり、機能や実用性を一律に評価できるものではない。以下は、あくまで一般的な傾向として理解し、最終的には自組織の要件に基づいて個別に判断する。

- 一般に有償の SBOM ツールでは、Web UI の管理画面や直感的な操作性が提供されている場合が多く、SBOM の生成・閲覧・管理を GUI 上で行えることがある。また、導入・運用時の不明点について、ベンダーや販売代理店に相談できるケースも多い。さらに、ソフトウェアのビルドやテスト、リリースを自動的に実行する仕組み（CI/CD）や、ソースコードや成果物の変更履歴を管理する仕組み（バージョン管理システム）と連携し、既存の開発環境との連携機能を組み込みやすい点が利点となることがある。

- 無償の SBOM ツールは初期費用を抑えて導入でき、小規模な試行や概念実証に適している場合が多い。まずは無償ツールを用いて SBOM を作成し、自社ソフトウェアの構成把握や SBOM 運用の流れを実体験として理解することで、運用上の課題や必要な機能要件を整理することができる。その結果を踏まえ、有償ツールへの移行や追加導入の要否を判断するという段階的な進め方が有効である。また、OSS コミュニティを中心に継続的な改良が行われているものも存在し、将来的な機能向上が期待できるケースも見られる。ただし、無償ツールを利用する場合には留意点もある。環境構築や設定に関する情報が十分に整備されていない場合がある。また、多くの無償ツールは海外で開発されており、参考となるドキュメントが英語のみで提供されているケースも少なくない。そのため、導入時にはサンプルコードを用いて期待どおりの SBOM が出力されるかを確認するなど、試行錯誤を前提とした設定作業が必要となることがある。こうした負担を軽減するため、無償 SBOM ツールに関する導入支援やサポートサービスを提供している企業の支援を受けることも選択肢の一つである。

ツールの提供形態についても慎重な検討が求められる。オンプレミス型のツールでは導入可能な OS やネットワーク環境が制約される場合がある一方、SaaS 型のツールでは、ソースコードなどの秘匿性の高い技術情報が安全に管理される構造となっていないかを事前に確認する必要がある。さらに、SBOM 導入が開発効率の低下を招かないよう、既存の開発プロセスに無理なく組み込めるツールを選定し、開発者の負担を最小限に抑えた運用を設計することが重要である。
SBOM ツールは、出力フォーマット、解析方式、脆弱性連携機能などに応じて多様な種類が存在する。代表的な SBOM フォーマットとしては、OWASP が策定する CycloneDX および、The

Linux Foundation が策定する SPDX がある。各フォーマットに対応したツール群やコンバータも公開されており、例えば以下の情報を参考に比較検討することができる。
https://cyclonedx.org/tool-center/
https://spdx.dev/use/spdx-tools/

4.2.3. 評価・選定の進め方

SBOM ツールの評価・選定にあたっては、整理した観点に基づき複数のツールを比較検討することが望ましい。無償トライアルを活用し、自社の代表的な製品やプロジェクトのソースコードを用いて試験的に解析を行うことで、操作性、学習コスト、解析結果の妥当性を具体的に評価することができる。
また、選定が困難な場合には、複数の SBOM ツールを取り扱う販売代理店に相談し、各ツールの特徴や長所・短所を比較しながら検討することも有効な手段である。

4.3. SBOM ツールの導入・設定

医療機器における SBOM 運用を開始するために必要となる SBOM ツールの導入及び初期設定について、実務的観点から留意すべき事項を整理する。SBOM ツールは、単に導入すれば直ちに効果を発揮するものではないため、対象とするソフトウェア構成や運用目的に適合した環境整備と設定が不可欠である。

4.3.1. 導入前の環境要件の確認と整備

SBOM ツールは、製品やベンダーごとに導入可能な環境要件が大きく異なる。そのため、導入に先立ち、対象ツールが求める動作環境を十分に確認し、必要なインフラを整備する必要がある。具体的には、ツールを実行する PC やサーバーについて、インターネット接続の有無、CPU・メモリ・ストレージ等のマシンスペック、対応 OS の種類及びバージョン、対応ブラウザの指定、ソフトウェアのビルド環境などが要件として定義されている場合がある。
また、一部の SBOM ツールでは Linux 環境のみをサポートしており、Windows 端末で利用する場合には仮想マシンやコンテナ環境の構築が前提となることもある。医療機器開発においては、社内 IT ポリシーやセキュリティルールとの整合も重要であるため、ツール要件と自社環境のギャップを事前に把握した上で、計画的に導入環境を整備することが求められる。

4.3.2. SBOM ツールの導入及び初期設定

導入可能な環境が整備された後、SBOM ツールのインストール及び初期設定を実施する。基本的な手順は、各ツールが提供する取扱説明書や README ファイル等の公式ドキュメントに従って進めることとなる。初期設定では、SBOM の出力形式（SPDX、CycloneDX）、対象とするソースコードやバイナリの範囲、解析オプション、出力ファイルの保存先など、SBOM 作成に直

接影響する項目を適切に設定する必要がある。
有償の SBOM ツールを利用する場合、販売代理店やツールベンダーによるサポート体制が整備されていることが多く、導入・設定に関する問い合わせや技術支援を受けることで、効率的かつ確実に初期構築を進めることが可能である。
なお、SBOM ツールの導入にあたり、利用する販売代理店やツールベンダー等については、「医療機器及び体外診断用医薬品の製造管理及び品質管理の基準に関する省令」（平成 16 年厚生労働省令第 169 号。以下「QMS 省令」という。）第 37 条から第 39 条に基づく購買管理の対象となり得ることに留意すること。また、導入する SBOM ツールについては、QMS 省令第 5 条の 6 に基づき、SBOM ツールに係るバリデーションの実施、記録の管理及び変更管理が必要になり得る点についても留意すること。

4.3.3. 脆弱性管理用途を想定した運用上の配慮

SBOM ツールを脆弱性管理として活用する場合、SBOM の生成時に既知の脆弱性情報（CVE 等）を参照・突合し、対象ソフトウェアに含まれる脆弱性を把握できることが重要である。これにより、使用している OSS や OTS ソフトウェアに起因するセキュリティリスクを、開発段階および市販後を通じて可視化することが可能となる。
また、SBOM により脆弱性が確認された場合には、その情報を問題解決プロセス（影響評価、リスク分析、是正・予防措置、変更管理等）に連携し、技術的対策や運用上の対応を通じて解決できる体制を整備することが求められる。医療機器分野においては、市販後の脆弱性対応が患者安全および事業継続に直結するため、SBOM ツールは脆弱性の検知を支援する手段として位置付け、組織として確立された品質・リスクマネジメントプロセスの中で活用することが重要である。

4.3.4. コンポーネントを識別するための情報と特性

SBOM におけるコンポーネントの識別精度および網羅性は、対象ソフトウェアに含まれる構成要素をどのような根拠情報に基づいて識別・整理するかによって、その精度や網羅性が左右される。SBOM ツールでは、依存関係情報、ソースコードやバイナリに含まれる特徴情報、ビルド成果物に付随するメタデータなど、複数の情報源を用いてコンポーネントを識別・整理する仕組みが提供されている。
依存関係情報は、パッケージマネージャーやビルドツールのメタデータを解析して直接的・間接的な依存関係を特定する手法であり、誤検出が少ない一方、パッケージ管理外のコンポーネントは検出できない。ソースコードやバイナリの特徴情報に基づく識別は、既知の OSS と照合する手法であり、コピー＆ペーストされたコードなども検出できる利点がある一方、誤検出や検出漏れが発生する可能性がある。また、ツール等によって明示的に管理されていないコンポーネントも SBOM 上の構成要素として定義できる可能性があるが、定義単位や真正性の判断については、組織としての解釈ルールをあらかじめ定めておく必要がある。

4.4. 第三者ソフトウェアに関する SBOM 情報の取得及び供給者管理

4.4.1. 基本方針

本項では、第三者ソフトウェアに起因するサプライチェーンリスクへの対応として、供給者からの情報取得及び供給者管理に関する基本方針を示す。本方針は、「3.1. SBOM 導入・運用の基本方針」を前提に、第三者ソフトウェア及び供給者管理の観点から具体化するものである。
供給者管理の目的は、SBOM という成果物を単に入手することではなく、医療機器のセキュリティ及び安全性に影響を及ぼす脆弱性やサポート終了等のサプライチェーンリスクを適切に管理することにある。そのため、SBOM に加え、脆弱性情報やサポート情報等の必要な情報を供給者から継続的に取得できる関係性及び体制を維持することが重要である。
なお、契約条項や調達仕様として具体化する際の要求事項については、「6.3. 調達・契約における SBOM 要求事項」を参照すること。

4.4.2. 供給者との情報共有体制

製造販売業者は、第三者ソフトウェア又は外部サービスの採用を検討する際には、機能、性能及び品質に加え、ソフトウェア構成及び脆弱性情報を継続的に提供できる供給者であるかを評価項目の一つとして考慮する。
供給者との契約、発注又は導入に当たっては、提供フォーマットと項目、提供タイミングと更新頻度、ライフサイクル情報の提供、脆弱性通知と SBOM 更新などを可能な範囲で事前に確認する。
また、供給者から取得した情報が製品ライフサイクルを通じて継続的に更新されるよう、契約条件又は運用手順に反映し、セキュリティインシデント又は重要な脆弱性が公表された際には速やかに情報を取得できる体制を維持することが重要である。供給者への情報提供依頼、その回答内容及び情報提供の可否については、後から確認可能な形で記録を維持することが望ましい。

4.4.3. 情報を取得できない場合の代替管理

供給者の方針、契約条件又は製品特性により、SBOM、脆弱性情報又は EOL/EOS 情報が提供されない場合がある。特に、汎用オペレーティングシステム、クラウドサービス、大規模ソフトウェアプラットフォーム等については、個別の SBOM が提供されない場合も想定される。
そのため、製造販売業者は、入手可能な情報を用いて合理的な影響評価を実施し、その結果に基づきリスクマネジメントを継続することが重要である。代替情報としては、公開されているセキュリティアドバイザリー、製品仕様書、リリースノート、脆弱性データベース、供給者のサポート情報、契約情報その他の公開情報を活用することが考えられる。
さらに必要に応じて、Software Composition Analysis（SCA）、バイナリ解析、コンテナイメージ解析、脆弱性スキャンその他の技術的手法を利用し、対象製品に含まれるソフトウェア構成及び既知脆弱性の把握を補完することも有効である。ただし、これらの結果は供給者が作成

した正式な SBOM を代替するものではなく、検出精度、網羅性及び真正性に限界があることを考慮して利用する必要がある。

4.4.4. 継続的な見直し及び文書化

供給者から SBOM 等の情報を取得できなかった場合には、その理由、供給者への問い合わせ内容及び回答、実施した代替管理、参照した公開情報、影響評価の結果、採用したリスクコントロール及び残余リスクの評価結果を文書化する。
また、情報を取得できない状態を恒久的なものとみなすのではなく、契約更新、ソフトウェア更新、保守契約の見直し又は定期レビュー等の機会において供給者への再確認を実施し、新たな SBOM や脆弱性情報が提供された場合には、速やかに影響評価及びリスク評価を見直すことが望ましい。

5. SBOM 作成・開示段階における実施事項

5.1. コンポーネント解析の考え方と実施手順

本項では、医療機器ソフトウェアにおける SBOM 作成・開示段階の中核となる「コンポーネントの解析」について、SBOM ツールを前提とした実施事項及び留意点を整理する。
本工程は、SBOM の網羅性・正確性を左右する重要な工程であり、後続の脆弱性管理、ライセンス管理、規制当局や納入先への説明において判断の前提となる。

5.1.1. 【手順】コンポーネント解析の実施フロー

本ガイドラインにおけるコンポーネント解析は、以下の流れに沿って実施することを基本とする。

1．SBOM 作成対象及び範囲の明確化（対象ソフトウェア・成果物の明確化）
SBOM 作成に先立ち、対象とするソフトウェアおよびその適用範囲を明確に定義する。具体的な対応方法については、「4.1.SBOM 適用範囲の明確化」を参照し、これに従って実施すること。第三者 SBOM がある場合は、[5.2.4. 第三者から提供された SBOM をインポートする際の注意点]を参照。

2．コンポーネント解析に用いる作業環境の決定
SBOM 作成を実施する環境として、開発環境、ビルド環境、又は製品相当環境のいずれを用いるかを決定する。どの環境を選択するかによって、検出されるコンポーネントやバージョン情報が異なる可能性があるため、SBOM の利用目的（市販前提出、市販後管理、社内管理等）を踏まえ、再現性と妥当性の観点から適切な環境を選定する。

3．SBOM ツールの設定及びコンポーネント解析の実行
導入した SBOM ツールについて、コンポーネントの解析方式、対象ディレクトリ、除外条件、パッケージマネージャーとの連携設定等を事前に確認・設定したうえで、対象ソフトウェアのスキャンを実行する。ツールによって GUI 又は CLI による実行方法が異なるため、取扱説明書や README 等を参照し、組織内で標準化された手順に従って定義を行う。

4．結果の確認
コンポーネント解析後は、SBOM ファイルが生成されたことのみで判断せず、ツールの解析ログや警告・エラー出力を確認する。また、ツールが途中で中断・省略されていないか、内部処理が正常に完了しているかを確認し、表面的には正常終了している場合であっても、一部処理がエラーによりスキップされていないかを検証する。

5.1.2. 【確認】解析結果の確認方法

コンポーネント解析結果には、誤検出や検出漏れが含まれる可能性があることを前提に、体系的な確認プロセスを実施する必要がある。特に、シンボリックリンクやランタイムライブラリ、深い階層に存在するコンポーネント、特定分野でのみ利用される制御系固有のコンポーネントなどは検出漏れが生じやすい。また、コンポーネント自体は検出されていても、バージョン情報が誤って検出される場合がある点にも留意する。
確認にあたっては、パッケージマネージャーが管理する構成情報や、詳細設計書、ビルド設定情報等と突き合わせることで、検出結果の妥当性を評価することが有効である。パッケージマネージャーを利用している場合、依存関係ツリーを用いることで、管理範囲内のコンポーネントについては比較的信頼性の高い確認が可能となる。

5.1.3. 【補正】手動補正および未特定コンポーネントの扱い

SBOM ツールのデータベースに存在しない OSS や、特定できないコンポーネントについては、ツールのコンソール等を用いて手動で情報を補正・追加する必要が生じる場合がある。その際、不明な情報が残る場合には、その事実を整理し、SBOM 上で明示的に管理する必要がある。SBOM を規制当局、医療機関、OEM／ODM 先、共同開発先等に開示する場合には、完全に特定できていない情報についても未特定のコンポーネントとして共有することで、情報の透明性を確保し、過度な誤解を防ぐことができる。

5.1.4. 【運用】確認工数と正確性の考え方

コンポーネント解析結果の精査は基本的に人手による作業を伴い、特にサブ階層のコンポーネントやサードパーティコンポーネントの確認には多大な工数を要する場合がある。一方で、すべてのコンポーネントについて検出漏れがないことを保証することは、実務上必ずしも現実的ではない。このため、ソフトウェアの重要度、セキュリティリスク、依存関係の複雑さ、提供元、更新頻度などを踏まえ、どの範囲まで確認を行うかを事前に定義することが重要である。SBOM ツールの出力結果にはパッケージマネージャーが管理する依存関係情報、設計書、ビルド設定、使用ライブラリ一覧等と突き合わせ、解析結果が実際のソフトウェア構成を適切に反映しているかを評価する。

5.1.5. 【運用】解析環境・設定による影響

解析結果は実施する環境（開発環境、ビルド環境、製品相当環境等）や、SBOM ツールの設定内容によって異なる場合がある。例えば、開発環境で解析を行った場合、製品には含まれないライブラリが検出されることがある。このため、どの環境を SBOM 作成基準とするかを明確にしたうえで解析を実施する必要がある。また、ツールのリポジトリ設定や解析パラメータによって、SBOM 上のコンポーネント構成や依存関係の表現が実際のソフトウェア構成と乖離する場合が

あるため、初期導入時には設定内容の妥当性を確認する。

5.1.6. 【運用】SBOM ツールを前提とした運用

SBOM ツールを用いることで、手動によるコンポーネント定義及び SBOM 作成と比較して、作業工数の削減が期待できる。医療機器ソフトウェアのように多数の OSS を含む製品においては、SBOM ツールを前提としたコンポーネント解析及び SBOM 作成・管理を行うことが現実的かつ有効な手法である。このため、本ガイドラインでは SBOM ツールの活用を前提として SBOM 作成および管理を実施するものとする。

5.2. SBOM の作成

SBOM は単なる成果物ではなく、規制対応、脆弱性管理、サプライチェーンの透明性確保を目的とした重要な管理情報である。そのため、作成段階においては、提供先や規制要求を踏まえた要件定義と、正確性及び網羅性を十分に確保した SBOM を生成することが求められる。

5.2.1. SBOM 作成の基本的な考え方

SBOM は、解析したソフトウェアコンポーネントの情報に基づいて作成する。作成に先立ち、SBOM に含める項目、使用するフォーマット、フォーマットのバージョン、出力ファイル形式等の要件を事前に決定する必要がある。規制や要求事項において、SBOM のフォーマットや必須項目が指定されている場合があるため、規制・ガイダンス、顧客や納入先からの要求、自社の運用方針を総合的に勘案して定める。

5.2.2. SBOM 内の名称及び付加情報の留意点

SBOM には、コンポーネント情報に加え、プロジェクト名称や製品識別情報など、SBOM ツール上で設定した情報が含まれる場合がある。これらの情報が SBOM 利用者にとって理解しやすく、活用可能な内容となっているかを検討することが重要である。
特に、開発段階から SBOM ツールを用いてコンポーネント管理を行っている場合、社内でのみ使用してきたプロジェクト名称やバージョン表記が、そのまま SBOM として外部に共有される可能性がある。SBOM 共有後の手戻りや問い合わせを防止するためにも、SBOM 利用者の視点に立った名称や識別情報を設定することが望ましい。

5.2.3. SBOM 作成における実施事項

SBOM 作成における主な実施事項を以下に示す。

1．要件を踏まえた作成方針の決定
　提供先や自社で定めた要件に基づき、SPDX や CycloneDX のフォーマット、フォーマット

のバージョン、出力ファイル形式を決定する。

2．SBOM ツールを用いて要件を満足する SBOM を作成する
決定したフォーマット、バージョン、出力ファイル形式に従い、SBOM ツールを用いて SBOM を生成する。

5.2.4. 第三者から提供された SBOM をインポートする際の注意点

サードパーティ製ソフトウェアや OSS コミュニティ等の第三者から提供されたコンポーネントを使用している場合、当該コンポーネントの SBOM が公開又は提供されていることがある。第三者から提供された SBOM を活用することで、SBOM 作成の効率化が図れるだけでなく、自社で実施したコンポーネント解析結果の精度向上や精査作業への活用も期待できる。
一方で、第三者から提供された SBOM をインポートして SBOM を作成する場合、自組織におけるコード改変やビルド条件の違いにより、実際の製品構成と不整合が生じる可能性がある。その結果、誤った情報が SBOM に記載されるリスクがあるため、インポート後には必ず自社の実装状況との整合性を確認し、必要に応じて修正を行うことが求められる。

5.3. SBOM の開示

5.3.1. 開示におけるベースライン

SBOM は医療機器のサイバーセキュリティに関する透明性を高め、医療機関等が自らの環境における脆弱性や、レガシー医療機器となり得るリスクを把握するための基礎情報である。このため製造販売業者は、SBOM を顧客向けセキュリティ文書の一つとして位置付け、医療機器の導入時及び重要なソフトウェア変更時を中心に、医療機関等に提供可能な体制を整備する。少なくとも製品のサポート期間を通じて、医療機関等からの要請に応じて SBOM を提示できることを、本ガイドラインのベースラインとする。
なお、医療機関等に提供される SBOM は主として脆弱性管理およびセキュリティ影響評価を支援することを目的としたものであり、ソフトウェアの利用条件、再配布条件又はライセンス義務に関する最終的な法的見解を示すものではない。SBOM 中に記載されるライセンス情報は、ライセンス管理やリスク評価のための参考情報であり、OSS を含む各コンポーネントの正式な利用条件・義務については、当該ソフトウェアに付随するライセンス文書や契約書その他の公式なドキュメントに基づき判断されるものとする。

5.3.2. 開示レベル

規制当局への申請等に用いる SBOM は、把握できているすべてのコンポーネント情報を記載することを原則とする。医療機関向けには、医療機関との合意に基づき、当該医療機関のリスクマネジメントに必要な範囲の情報を記載した SBOM を提供する。
医療機関向け SBOM には、少なくとも主要な OSS／OTS コンポーネントについて、サプライ

ヤー名、コンポーネント名、バージョン、その他の固有識別子など、NTIA 最小要素に相当する構成管理情報を含めることを基本とする。さらに、技術的・契約的に支障がない範囲であれば、医療機関側のニーズや合意内容に応じて、ソフトウェア内部構造や汎用 OS に標準搭載されるコンポーネントについても可能な限り幅広く開示することが望ましい。

5.3.3. 提供方法

SBOM の提供方法としては、当面、MDS2 等の顧客向けセキュリティ文書への添付や、個別依頼に応じた電子ファイルの提供など、手動による運用も許容される。製造販売業者は、SBOM を当該ソフトウェア（バイナリ又はソース）の引渡し時点までに提供することを基本とし、少なくとも製品リリースの際には顧客に提示可能な状態とする。中長期的には、ウェブサイトや認証付きポータル、API 等を用いた標準化された配付メカニズムを活用し、自動的な検出・取得が可能な形で SBOM を提供することが望ましい。

将来的には、SBOM に対して VEX（Vulnerability Exploitability eXchange）等の形式を組み合わせ、個々の脆弱性が当該医療機器に与える影響の有無等を併せて提供することで、医療機関側の優先度付けと対応判断を一層効率化できると考えられる。SBOM は医療機器の構成を詳細に示す情報であることから、覚書・契約等に基づき機密情報として適切に保護し、暗号化や認証を備えた通信手段を用いるなど、第三者への漏洩によるサイバーリスクの増大を抑制するための配慮が必要である。

6. SBOM 運用・管理段階における実施事項

6.1. SBOM の管理

6.1.1. SBOM の管理上の位置づけ

SBOM は一度作成して終わりとなる静的な文書ではなく、医療機器ソフトウェアのリリースやアップデートに応じて更新される情報として管理する必要がある。製造販売業者は、JIS T 2304 のソフトウェア構成管理プロセスを土台としつつ、必要に応じて JIS T 81001-5-1 のソフトウェア構成管理プロセスの要求事項も踏まえ、SBOM の作成・更新・保管を既存の構成管理・変更管理の枠組みに位置付ける必要がある。

6.1.2. SBOM の更新・変更管理

製造販売業者は、製品ごとの SBOM を個別に管理するだけでなく、SBOM に含まれるコンポーネント情報を集約した「SBOM コンポーネントリポジトリ（マスターデータベース）」を構築し、内部の構成管理に取り込むことが望ましい。また、開発委託先や OEM／ODM 先、サードパーティベンダーから入手した SBOM についても、個別に保管するだけでなく、このリポジトリに統合し、自社製品全体で共通に利用するコンポーネントを横断的に把握できるようにすることが重要である。これにより、複数製品に共通して利用されているコンポーネントについて、脆弱性や EOL／EOS、ライセンス情報の更新を一括して反映できるようになり、製品ごとの SBOM を個別に点検する場合と比べて、漏れや重複を抑えつつ効率的にリスク評価を行うことが可能となる。さらに、SBOM コンポーネントリポジトリを運用する際には、コンポーネント名やサプライヤー名の表記揺れを吸収し、複数の SBOM 間で一貫した扱いができるようにする「正規化」の仕組みを設けることが有効である。例えば、米国 MITRE による医療機器向けの白書では、複数の SBOM に含まれる名称を統一的に扱うための中央エイリアスデータベース（Central Alias Database）等の活用が提案されている。

更新管理の観点では、ソフトウェアの改訂（新規リリース、パッチ、機能追加等）に伴い、当該リリースの構成を反映した SBOM を維持し、「どの製品・バージョンにどの SBOM が対応するか」を追跡可能に管理する必要がある。SBOM の更新が完了していることをソフトウェアリリース承認の条件の一つと位置付けることで、構成情報の漏れや齟齬を防止できる。SBOM に記載されたコンポーネント情報は、脆弱性情報や EOL／EOS 情報と組み合わせてリスク評価やアップグレード計画の根拠として活用されるため、日常的な変更管理プロセスの中で確実に更新されていることが重要である。

また、生成ツールの限界やサプライヤーから入手した情報の不備等により SBOM の記載に誤りや欠落が判明した場合には、ソフトウェア改訂の有無にかかわらず SBOM 自体を訂正し、その経緯を変更管理記録に残すこと。

6.1.3. SBOM の保管及び情報提供

保管については、SBOM を医療機器の設計記録（設計履歴簿等）やリスクマネジメントファイル、市販後安全管理（GVP）の記録等と同様に、製品のサポート期間及び関連法令・規制が求める期間にわたり保管する必要がある。特に、販売開始（商用リリース）、製品寿命終了（EOL）、サポート終了（EOS）といったライフサイクル上のマイルストーンにおいては、厚生労働省通知「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」や「医療機器のサイバーセキュリティ対策に関連する情報提供について」に従い自社開発・OSS・市販ソフトウェア等の構成要素を SBOM として提示できる仕組みを構築し、レガシー医療機器の管理にも活用できるようにしておくことが求められる。

実務的な活用のためには、SBOM と製品型番、ソフトウェアバージョン等の構成管理情報を対応付けて管理し、「どの製品・バージョンにどのコンポーネントが含まれているか」を迅速に追跡できるようにすることが不可欠である。これにより、脆弱性の公表やコンポーネントのサポート終了等があった場合に、影響を受ける可能性のある製品・型番を特定し、必要なアップデートや情報提供につなげることができる。

なお、SBOM の生成・更新・利用に関する記録（作成・改訂の履歴、レビュー・承認状況等）は、既存の文書・記録管理プロセスや変更管理プロセスの中で管理し、内部監査や当局査察、QMS 適合性調査等において説明可能な状態を維持すること。

さらに、SBOM 情報の改ざんやなりすましを防止し、受領者がその出所と完全性を確認できるようにするため、可能な範囲で SBOM にハッシュ値や電子署名を付与し、既存のコード署名や公開鍵基盤を活用して検証できる仕組みを整備することが望ましい。CISA が公開している SBOM フレーミング文書でも、SBOM エコシステムにおいては、著者が SBOM にデジタル署名を行い、利用者がその署名を検証することによって真正性と完全性を担保することが重要であるとされている。

6.2. SBOM に基づく脆弱性管理

SBOM は、ソフトウェアに含まれるライブラリやコンポーネントが既知の脆弱性をもっていないか確認し、問題があれば迅速に影響範囲を特定するための情報基盤である。
医療機器のソフトウェアには多数のコンポーネントが含まれ、それぞれについて脆弱性情報が公表され得る。SBOM は、どの製品のどのバージョンにどのコンポーネントが含まれているかを把握することで、脆弱性管理プロセスにおける影響範囲の特定を支援する。

本ガイドラインでは、SBOM を活用した脆弱性管理を、概ね次の流れで実施することを基本とする。

1. 脆弱性情報の収集と SBOM との照合
2. 影響評価と優先度付け（トリアージ）
3. 対応方針の決定及び実施並びに情報提供

4. 結果の記録

6.2.1. 脆弱性情報の収集と SBOM との照合

製造販売業者等は、JVN や NVD 等の脆弱性情報データベース、ソフトウェアベンダーのセキュリティアドバイザリー、情報共有分析機関（ISAO／ISAC）からの情報などを継続的に収集し、自社製品に関係する可能性のある脆弱性を把握する。収集した情報に含まれるコンポーネント名・バージョン・その他の固有識別子を SBOM と照合し、影響を受ける可能性のある製品・バージョンを特定する。SBOM 作成段階でその他の固有識別子やハッシュ値を可能な限り付与しておくことは、自動照合の精度と効率を高めるうえで有用である。
さらに、SBOM を登録（インポート）することで脆弱性情報データベース等と自動的に照合し、該当する脆弱性情報やアラートを継続的に提供するプラットフォーム／ツールも存在するため、これらを適切に活用して照合の自動化・省力化を図ることは有効である。

6.2.2. 脆弱性の影響評価と優先度付け（トリアージ）

SBOM やツールの解析結果として把握される脆弱性の件数は、少数の場合も多数の場合もあり得るため、医療機器のリスクマネジメントの観点から対応の優先度を整理することが重要である。優先度付け（トリアージ）にあたっては、例えば次の観点を考慮する。

- 公表されている深刻度（例：共通脆弱性評価システム(CVSS)スコア）
- 悪用の可能性（既に攻撃が観測されているか、既知悪用脆弱性カタログや PoC の有無等）
- 当該コンポーネントの医療機器内での役割（安全性・基本性能への影響度）
- 実際の使用環境における露出状況（ネットワーク経由で到達可能か等）
- 回避策・代替手段の有無（設定変更やネットワーク分離で緩和可能か等）

これらの観点に基づき、当該脆弱性がその医療機器において実際に悪用可能か、悪用された場合に安全性・基本性能および臨床環境にどの程度の影響をもたらすかを評価する。（例えば、CVSS 等のスコアを医療機器の使用環境に合わせて再評価し、各社のリスクマネジメントと整合させて、受容可能性を判断するなど）
SBOM に記載されたコンポーネントに関する公表済み脆弱性については、原則としてすべてを評価対象とするが、上記の観点に基づくリスク評価の結果、装置全体としてのリスクが十分に低いと判断されるものについては、能動的な修正を行わずリスク受容（モニタリングのみ）とする判断もあり得る。これらを踏まえ、「直ちに対応すべきもの」「次回の定期アップデートで対応するもの」「リスク受容としてモニタリングのみ行うもの」など、現実的なレベルで優先度付けを行う。SBOM ツールが出力したすべての脆弱性に一律に対応することを前提とせず、医療機器のリスクマネジメントの枠組みに沿って合理的な対応範囲を決定する。

6.2.3. 対応方針の決定及び実施並びに情報提供

対応が必要と判断した脆弱性については、ソフトウェアアップデートやパッチ適用、コンポーネ

ントの置換、設定変更、ネットワーク構成の見直し等の具体的対策を検討・実施する。OS やクラウドサービス等、第三者が管理するコンポーネントに起因する脆弱性については、製造販売業者による修正、医療機関側の運用対策、リスク受容と継続モニタリングといった方針に整理して対応することが有効である。

患者安全や診療継続に影響し得る重要な脆弱性については、協調的な脆弱性開示（CVD）の枠組みに沿って、影響を受ける製品・バージョン、概要と影響、推奨される暫定対策及び恒久対策等を含むセキュリティアドバイザリーを提供する必要がある。この際、SBOM を用いて影響範囲となる製品・バージョンを明確にすることで、医療機関側の優先度付けと対応判断を支援できる。対応の根拠となった脆弱性情報、リスク評価結果、選択した対策内容については記録し、品質記録としての取扱い及び保存方法は次項に従うものとする。

6.2.4. 結果の記録と SBOM への反映

ソフトウェア構成に変更が生じた場合は、その都度、変更後の構成に対応した SBOM を作成し、最新版を維持する。例えば、脆弱なコンポーネントの置き換え等の脆弱性対応を行った場合には、その結果が SBOM にも反映されるようにする。同時に、脆弱性情報の受領から評価、リスク判断の内容とその根拠、対応要否の決定およびその承認内容、実施した対策の内容と実施結果に至るまでの一連の情報を記録し、設計記録やリスクマネジメントファイル、市販後安全管理（GVP）の記録と同様に、この記録は保管、管理する必要がある。

これらの記録は、関連法令・規格が求める期間にわたり保存し、内部監査や当局査察において、特定の脆弱性について「どの製品・機器が影響を受けたか」「どのように評価し、どのような対策を講じたか」を時系列で追跡できる状態としておく必要がある。SBOM と製品型番、ソフトウェアバージョン等の構成管理情報及び脆弱性対応記録を相互に紐付けて管理することで、レガシー医療機器も含め、将来の問い合わせや追加対策に対して効率的かつ一貫した説明が可能となる。また、評価の結果「影響なし」あるいは「特定条件下でのみ影響あり」と判断した場合でも、その判断理由を品質記録として残し、必要に応じて将来的に VEX 等の形式で SBOM と紐付けて管理・提供できるようにしておくことが望ましい。

6.2.5. SBOM に基づくライセンスおよびライフサイクル管理

ライセンス管理及びライフサイクル管理では、SBOM を用いて医療機器に含まれるソフトウェアコンポーネントを特定し、その情報を法務・品質保証等が保有する情報（ライセンス情報、契約条件、EOL／EOS 情報等）と突き合わせて活用する。医療機器は長期間にわたり使用されることが多く、コンポーネントのライセンス違反やサポート終了は、法的リスクに加えて、サイバーセキュリティ上のリスクや製品供給継続性にも影響を及ぼす。

本ガイドライン第 1 版では、医療機関等に提供する SBOM の最小要素として NTIA 最小要素を採用しており、ライセンス情報は必須要素とはしない。一方で SBOM は社内のライセンス管理

における「コンポーネント棚卸し情報」として有用であるため、社内用途として SBOM（又は SBOM コンポーネントリポジトリ）とライセンス情報・証跡（入手元、ライセンス文書、改変有無、配付形態等）を紐付けて管理することが望ましい。ライセンス適合性の判断は、OSS 管理規程やライセンスレビュー記録、個々のライセンス文書・契約書等からなる別途のライセンス管理プロセスに基づき行う。

なお、SBOM にライセンス情報を記載する場合、例外条項やデュアルライセンス等の簡略表記により誤解が生じ得るため、外部提供の有無、記載粒度（例：SPDX 識別子の扱い）、レビュー・承認、SBOM 本体と OSS ライセンス文等の切り分け方針を、あらかじめ組織として定めておくことが望ましい。
ライフサイクル管理の観点では、製造販売業者等は、サプライヤーとの契約や利用許諾に基づき、各コンポーネントの製品寿命終了（EOL）およびサポート終了（EOS）に関する情報を把握し、自社 SBOM コンポーネントリポジトリに取り込むことが求められる。これにより、どの製品・バージョンが、どのコンポーネントのサポート終了や開発停止の影響を受け得るかを横断的に把握し、アップグレードや置換、補完的対策の要否を早期に検討できるようになる。

これらのライセンス管理及びライフサイクル管理の結果（ライセンス適合性の評価、是正措置の内容、EOL／EOS を踏まえた対応方針等）は、リスクマネジメントファイルや設計記録、市販後安全管理（GVP）の記録と整合を取りつつ、QMS における品質記録として保存する。SBOM によりコンポーネント情報が体系的に整理されていれば、次期製品やソフトウェアアップデートにおけるコンポーネント選定にも知見をフィードバックでき、TPLC（Total Product Life Cycle）全体を通じた法的コンプライアンスとサイバーセキュリティ水準の維持・向上に資する。

6.3. 調達・契約における SBOM 要求事項

SBOM を継続的かつ一貫した形で整備するためには、自社製品に対して SBOM を作成するだけでなく、ソフトウェアサプライヤーや開発委託先、OEM／ODM 先との契約・調達仕様において、SBOM の提供と更新を明確な要件として組み込むことが重要である。開発委託等により第三者が実装したソフトウェアについても、最終的な SBOM の正確性と網羅性に責任を負うのは製造販売業者であるため、契約段階で SBOM に関する期待値を具体的に共有しておく必要がある。

実務上は、RFP、基本契約、個別取引契約等において、少なくとも次のような SBOM 関連条項を検討するとよい。

- **提供フォーマットと項目：**NTIA 最小要素に準拠した機械可読な SBOM（SPDX 又は CycloneDX 等）を提供すること。サプライヤー名、コンポーネント名、バージョン、その他の固有識別子、関係、作成主体、タイムスタンプ等の基本項目に加え、可能な範囲でコンポーネントハッシュ及びライセンス種別を含めること。
- **提供タイミングと更新頻度：**ソフトウェア又はコンポーネントの引渡し時までに SBOM を提供すること。バージョンアップ、パッチ提供、重要な構成変更が行われた場合は、その変更に対応する SBOM を合理的な期間内（例：リリースから〇日以内）に提供すること。

- **ライフサイクル情報の提供：**各コンポーネントのサポート終了予定日（EOS）及び製品寿命終了（EOL）が公表されている場合は、その情報を SBOM 又は別紙として提供すること。EOL／EOS 情報に変更があった場合は、予め合意した手段（メール通知、ポータル掲示等）で通知すること。
- **脆弱性通知と SBOM 更新：**重大な脆弱性（例：CVSS v3.1 で High 以上）がコンポーネントに判明した場合、当該コンポーネントの提供先（本契約の発注者を含む）に対して、脆弱性情報、影響範囲、推奨される対策方針、及び必要に応じた SBOM の更新を通知する責任を負うこと。

これらの条件を契約に明記することで、第三者コンポーネントや開発委託部分を含むソフトウェアサプライチェーン全体について、SBOM 情報を欠落なく取得しやすくなる。また、複数のサプライヤーから取得した SBOM を SBOM コンポーネントリポジトリに統合し、名称やバージョン表記の正規化を行うことで、製品横断でのライセンス管理・脆弱性管理・EOL／EOS 管理が効率的に実施できる。

製造販売業者等は、社内の調達部門・法務部門と連携し、SBOM 要求事項を自社の標準契約書式や調達ポリシーに反映させることが必要である。

文献

1) FDA、Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions ｜2026
2) NTIA、Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) Second Edition ｜2021
3) NTIA、The Minimum Elements for a Software Bill of Materials (SBOM) ｜2021
4) ANSI/NEMA、HN 1-2019 Manufacturer Disclosure Statement for Medical Device Security ｜2019
5) CISA、2025 Minimum Elements for a Software Bill of Materials (SBOM) Public Comment Draft ｜2025
6) IMDRF、N70 Principles and Practices for the Cybersecurity of Legacy Medical Devices ｜2023
7) IMDRF、N73 Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity ｜ 2023
8) 日本規格協会、JIS T 2304:2017　医療機器ソフトウェア－ソフトウェアライフサイクルプロセス｜2017
   IEC、IEC 62304:2006+A1:2015 Medical device software — Software life cycle processes
9) 日本規格協会、JIS T 81001-5-1:2023　ヘルスソフトウェア及びヘルスＩＴシステムの安全,有効性及びセキュリティ―第５－１部｜2023：セキュリティ―製品ライフサイクルにおけるアクティビティ
   IEC、IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security Part 5-1: Security — Activities in the product life cycle ｜2021
10) ISO/IEC、IEC/TS 81001-2-2:2025: Health software and health IT systems safety, effectiveness and security Part 2-2: Guidance for the implementation, disclosure and communication of security needs, risks and controls｜2025
11) ISO/IEC、ISO/IEC 5962:2021 Information technology - SPDX® Specification V2.2.1 ｜2021
12) MITRE、DATA NORMALIZATION CHALLENGES AND MITIGATIONS IN SOFTWARE BILL OF MATERIALS (SBOM) PROCESSING ｜2024
13) ENISA SBOM LANDSCAPE ANALYSIS ｜2025
14) CISA、Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) Third Edition ｜2024
15) 医療情報システムの安全管理に関するガイドライン(安全管理ガイドライン）第 6.0 版
16) 厚生労働省、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）｜2023
17) 厚生労働省、医療機関における医療機器のサイバーセキュリティ確保のための手引書｜2023
18) 厚生労働省事務連絡「「医療情報システムの安全管理に関するガイドライン」に関する「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生

時の対応フローチャート」について」｜2021/10
19）厚生労働省通知「医療機関等におけるサイバーセキュリティ対策の強化について」｜2018/10/29
20）医療法／医療法施行規則…医療情報・医療機器の安全管理
21）厚生労働省通知「医療機器におけるサイバーセキュリティの確保について」｜2015/04/28
22）厚生労働省通知「医療機器のサイバーセキュリティの確保に関するガイダンスについて」｜2018/07/24
23）厚生労働省通知「IMDRF ガイダンスの公表について」｜2020/05/13
24）厚生労働省通知「医療機器のサイバーセキュリティの確保及び徹底に係る手引書について」｜2021/12/24
25）IMDRF、Principles and Practices for Medical Device Cybersecurity｜2020/03/18
26）厚生労働省事務連絡「医療機関を標的としたランサムウェアによるサイバー攻撃について（注意喚起)」｜2021/06/28
27）医薬品、医薬部外品、化粧品、医療機器及び再生医療等製品の製造販売後安全管理の基準に関する省令
28）経済産業省、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｜2024/08/29

用語（五十音順）

五十音順	用語	出典
あ	**アップデート** 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 注釈 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。 注釈 2:　アップデートには、パッチ及び設定変更が含まれる。 注釈 3:　適応及び完全化に関する変更は設計仕様時になかったソフトウェアの改良である。	IMDRF ガイダンス和訳より （製造販売業者向け手引書より）
き	**共通脆弱性評価システム（CVSS）** 情報システムの脆弱性に対するオープンで汎用的な評価手法であり、事業者に依存しない共通の評価方法を提供。CVSS を用いると、脆弱性の深刻度を同一の基準の下で定量的に比較可能である。 IPA　共通脆弱性評価システム CVSS v3 概説 https://www.ipa.go.jp/security/vuln/scap/cvssv3.html FIRST Common Vulnerability Scoring System Version 4.0 https://www.first.org/cvss/v4-0/	（製造販売業者向け手引書より）
こ	**攻撃** 資産の破壊、暴露、改ざん、無効化、盗用、認可されていないアクセス若しくは使用の試み	JIS Q 27000:2019
	コンピュータ化システムバリデーション（Computerized System Validation） 「コンピュータシステム」と「業務プロセス」を統合した「コンピュータ化されたシステム」のバリデーションのことである。	品質管理監督システム（QMS）に係るコンピュータソフトウェアの適用に関するバリデーション並びに電磁的な文書及び記録の管理に関するガイダンス 2020
	コンポーネント システムやソフトウェアの機能を構成する個別の部品や要素である。 これらの部品は、独立して機能しつつ、他のコンポーネントと連携して全体のシステムやアプリケーションを実現する。	
さ	**サイバーセキュリティ** 情報及びシステムが不正な活動（不正なアクセス、使用、開示、中断、改変、破壊等）から保護されており、機密性、完全性、可用性に関するリスクがライフサイクル全体に渡って受容可能なレベルに維持されている状態	JIS T 81001-1:2022、
	サポート終了（End of Support：EOS） 製品のライフサイクルにおいて、製造業者が全てのサポート活動を中止する時点。サービスサポートは、この時点を超えない。	IMDRF ガイダンス和訳より（製造販売業者向け手引書より）

五十音順	用語	出典
し	**情報共有分析機関(Information Sharing and Analysis Organizations：ISAOs)** サイバーセキュリティ関連情報の収集、分析、共有及び発信のために設置された組織。製造販売業者が ISAO に積極的に参加することで、患者やユーザーとの連絡や調整を含む展開を通じて、サイバーセキュリティの脆弱性に積極的に取り組み、悪用を最小限に抑えることで、企業、医療機器コミュニティ、医療・公衆衛生分野を支援することが可能である。情報共有分析センター（Information Sharing and Analysis Centers：ISAC）と呼ばれる組織もある。 国際的な組織として、H-ISAC（Health Information Sharing and Analysis Center: https://h-isac.org/）、MedISAO（https://www.medisao.com/）がある。国内では、NISC（内閣サイバーセキュリティセンター）によって立ち上がった情報共有組織セプターのひとつである医療セプター（事務局：日本医師会情報システム課）がある。医機連（一般社団法人日本医療機器産業連合会）及び JAHIS（一般社団法人保健医療福祉情報システム工業会）はオブザーバーとして参加しており、この各加盟団体及び加盟企業は医療セプターのサイバーセキュリティ情報を活用できる。	（製造販売業者向け手引書より、一部修正）
せ	**脆弱性** システムのセキュリティポリシーを破るために悪用される可能性のある、システムの設計・実装又は運用・管理における欠陥又は弱点 一つ以上の脅威によって悪用される可能性のある資産又は管理策の弱点	JIS T 81001-1:2022 より JIS Q 27000:2019 （製造販売業者向け手引書より）
	セキュリティアドバイザリー 次のような情報を提供する。 ・他社製品あるいは一般的な技術に関する脆弱性で自社製品に大きな影響を与えるもの ・自社関連の脆弱性に関する情報の捕捉、追加 ・まだ修正モジュールが作成されていない脆弱性に関する情報	（製造販売業者向け手引書より）
	製品寿命終了（End of Life：EOL） 製品のライフサイクルにおいて、製造業者が定めた有効期間を超えた製品の販売を終了し、製品について正式な EOL プロセス（ユーザーへの通知等）を実施する段階。	IMDRF ガイダンス和訳より（製造販売業者向け手引書より）
ひ	**PSIRT（Product Security Incident Response Team）** 組織が提供する製品の脆弱性に起因するリスクに対応するための組織内機能。自社製品の脆弱性への対応、製品のセキュリティ品質管理・向上を目的とした組織 JPCERT/CC　https://www.jpcert.or.jp/research/psirtSF.html （一般社団法人コンピュータソフトウェア協会、JPCERT/CC） 製品開発者向けガイド（IPA） https://www.ipa.go.jp/security/guide/vuln/rcu1hd000000a5en-att/guide_for_dev.pdf PSIRT Services Framework 1.0 日本語版 https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.0_jp.pdf	（製造販売業者向け手引書より）
め	**メタデータ** あるデータを説明するためのデータ	
り	**リバースエンジニアリング（Reverse Engineering）** 既存の製品やソフトウェアを分解・解析し、その構造、動作原理、設計情報、製造方法などを明らかにする技術手法である。 通常のエンジニアリングが設計図から製品を作り上げる「順方向」のプロセスであるのに対し、完成品から設計情報を逆算的に抽出する「逆方向」のアプローチを採用することからこの名称がつけられている。	
れ	**レガシー医療機器** 現在のサイバーセキュリティの脅威に対してアップデート又は補完的対策等の合理的な手段で保護できない医療機器で、販売開始以降の年数にかかわらない。	IMDRF ガイダンス和訳より、一部修正（製造販売業者向け手引書より）

五十音順	用語	出典
C	**CI/CD** ソフトウェア開発における自動化プロセスの概念で、「Continuous Integration（継続的インテグレーション）」と「Continuous Delivery/Continuous Deployment（継続的デリバリー／継続的デプロイメント）」 継続的インテグレーション（CI）: 開発者が作成したソフトウェアの変更を、頻繁かつ自動的に統合（マージ）し、ビルドや自動テストを実行する仕組み。これにより不具合の早期発見や統合時の手戻り削減が可能となる。 継続的デリバリー（CD）: CI によって統合されたソフトウェアを、品質基準に従って自動的にステージング環境や本番環境に配信するプロセス。人手による介入を最小化し、安全かつ迅速なリリースを支援する。 医療機器開発においては、CI/CD を用いることでソフトウェア変更の追跡、品質保証、SBOM の自動生成・更新などを効率化できる。	
	CPE（Common Platform Enumeration：共通プラットフォーム一覧） 情報システムにおけるハードウェア、オペレーティングシステム、アプリケーション等の IT 製品を一意に識別するための標準化された命名規則。 NIST（米国国立標準技術研究所）が管理し、脆弱性管理・測定・評価を自動化するための基準である SCAP（Security Content Automation Protocol）の構成要素の一つである。URI 形式で記述され、NVD などの脆弱性データベースにおいて脆弱性の影響を受ける製品の特定に広く利用されている。	SCAP（Security Content Automation Protocol）
	CVE（Common Vulnerabilities and Exposures（共通脆弱性識別子）） ソフトウェアやハードウェアに存在する個々の脆弱性に対して、一意の識別番号（CVE-ID）を付与する国際的な仕組みである。米国の非営利団体 MITRE 社が中心となり管理・運用しており、「CVE-年-番号」の形式（例：CVE-2021-44228）で採番される。CVE-ID により、異なるベンダーやツール、データベース間で同一の脆弱性を正確に参照・突合することが可能となる。CNA（CVE Numbering Authority）と呼ばれる採番権限をもつ組織が CVE-ID を発行する。	
J	**JVN（Japan Vulnerability Notes）** JPCERT/CC（JPCERT コーディネーションセンター）と IPA（独立行政法人 情報処理推進機構）が共同で運営する、日本国内向けの脆弱性対策情報ポータルサイトである。国内外のソフトウェアやハードウェアに関するセキュリティ脆弱性情報および対策方法を公開している。関連サービスとして JVN iPedia（脆弱性対策情報データベース）や MyJVN（脆弱性対策情報収集ツール）も提供されている。	
M	**MDS2（製造業者による医療機器セキュリティ開示書）** Manufacturer Disclosure Statement for Medical Device Security 医療機器製造業者が、ヘルスケア事業者（医療機関）に対してセキュリティ関連情報を開示するための記載様式を提供するセキュリティ宣言書。米国において HIPAA 法におけるセキュリティ規則対応のため、HIMSS が 2004 年 12 月に作成、公表したテンプレート文書のことで、2019 年に最新版が公開された。MDS2 は、医療機関と製造販売業者との間の情報共有ツールとして定着し、広く利活用されている。 一般社団法人日本画像医療システム工業会（JIRA）のホームページに和訳掲載 https://www.jira-net.or.jp/publishing/security.html	ANSI/NEMA HN 1-2019（製造販売業者向け手引書より）
N	**NVD（National Vulnerability Database（国家脆弱性データベース））** NIST（米国国立標準技術研究所）が管理・運営する、世界最大規模の脆弱性情報データベースである。CVE-ID を基に脆弱性情報を収集・整理し、CVSS（共通脆弱性評価システム）による深刻度スコア、CPE による影響製品情報、CWE（共通脆弱性タイプ一覧）による脆弱性分類など、詳細な技術情報を付加して公開している。SCAP 準拠のリポジトリとして、自動化された脆弱性管理やコンプライアンス検証の基盤となっている。	

五十音順	用語	出典
P	**purl（Package URL）** 様々なソフトウェアパッケージ管理エコシステム（npm、Maven、PyPI、deb、rpm、Docker など）を横断して、パッケージやライブラリを一意に識別するための標準化された URL 形式の識別子である。 CPE が製品・プラットフォーム単位の識別に向いているのに対し、purl は OSS パッケージ（部品）レベルの識別に特化しており、SBOM（Software Bill of Materials）や脆弱性管理において広く活用されている。	
S	**SWID（Software Identification Tag（ソフトウェア識別タグ））** ソフトウェア製品ごとに一意に生成される XML 形式のメタデータであり、ソフトウェア資産管理（SAM）の効率化を目的として ISO/IEC 19770-2 で規定されている国際規格である。ソフトウェアの名前、ベンダー、バージョン、エディションなどの情報を構造化して記述し、インストールされたソフトウェアの識別・検出・管理の自動化を可能にする。日本国内では JIS X 0164-2:2018 として同等規格が採用されている。SBOM の構成要素としても活用されている。	JIS X 0164-2:2018