# 「医療機器における SBOM 導入・運用ガイドライン（第１版）（案）」に対する意見募集の結果について

令和８年８月６日
厚生労働省医薬局
医療機器審査管理課

「医療機器における SBOM 導入・運用ガイドライン（第１版）（案）」に対する意見の募集に関し、令和８年５月 19 日から同年６月 19 日までご意見を募集したところ、計 101 件の御意見をいただきました。

お寄せいただいたご意見の要旨とそれに対する厚生労働省の考え方は別紙のとおりです。なお、いただいたご意見等に対する考え方のうち、同様の趣旨のものは適宜集約してお示ししております。

皆様の御協力に深く御礼申し上げますとともに、今後とも厚生労働行政の推進に御協力いただきますよう、よろしくお願い申し上げます。

「医療機器におけるSBOM導入・運用ガイドライン（第１版）（案）」に対する意見募集の結果について（別紙）

| No. | 該当箇所 | ご意見 | 回答 |
|---|---|---|---|
| 1 | 全体 | 医療機器は人命に関わるものであることから、SBOMを介した情報共有及び説明責任の強化について、将来的な義務化を見据えた記載とすべきである。あわせて、オープンソースソフトウェアを使用せず、プロプライエタリソフトウェアのみで構成される医療機器に対するSBOMの考え方や取扱いについて、見解を示してほしい。 | 本ガイドラインは、SBOMの導入・運用に関する考え方を示すものであり、規制上の義務を定めるものではありません。また、SBOMの対象はオープンソースソフトウェアに限定されるものではなく、自社開発ソフトウェアを含むソフトウェアコンポーネント全般を対象としています。 |
| 2 | 全体 | 医療機関のネットワーク環境や運用実態を踏まえ、SBOMの運用に必要な技術的要件、責任分界点、導入・運用コスト及び支援策、並びにセキュリティ事案発生時の関係者の役割について明確化すべきである。 | 本ガイドラインは、製造販売業者等がSBOMを導入・作成し、継続的に活用できる体制の整備を支援することを目的としており、医療機関におけるネットワーク環境やSBOMの運用方法を対象とするものではありません。 |
| 3 | 全体 | 日本国内ではHIMSSのMDS2よりもJAHISのMDSが広く運用されているため、本ガイドラインの主な利用者や利用目的を踏まえ、MDS2の説明をMDSの説明へ置き換えることを検討してほしい。 | ご意見として参考にさせていただきます。 |
| 4 | 全体 | SBOM作成・管理の手順やガイドライン全体の流れを理解しやすくするため、全体像を俯瞰できるフローチャートの追加を検討してほしい。 | ご意見として参考にさせていただきます。 |
| 5 | 全体 | レガシー医療機器への適用方針を整理すべき。 | 令和６年３月31日以前に製造販売された医療機器に関する取扱いについては、「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（令和7年4月17日厚生労働省医薬局医療機器審査管理課長、医薬安全対策課長連名通知）」にてお示ししています。 |
| 6 | 全体 | SBOMを規制当局に提出するにあたっての取扱いや、SBOMを変更する場合の薬事手続きを明確化すべき。 | 本ガイドラインは製造販売業者におけるSBOMの運用に関するガイドラインであり、薬事上の手続きについては対象外です。 |
| 7 | 1.1 | 「近年」の係り受けが不明確であり、「高度なソフトウェア化」及び「高度なネットワーク接続」の表現も具体性に欠けるため、より分かりやすい記載とすべきである。また、「進展」よりも「普及」の方が適切であり、文章全体の表現を見直すべきである。 | ご指摘を踏まえて修正しました。 |
| 8 | 1.1 | サイバーセキュリティリスクそのものではなく、サイバーセキュリティ対策の重要性が高まっていることが分かる表現に見直すべきである。 | ご指摘を踏まえて修正しました。 |
| 9 | 1.1 | サイバーセキュリティ対策の重要性の高まりと、製造販売業者等によるソフトウェア管理との関係が分かりにくい。 | ご指摘を踏まえて修正しました。 |
| 10 | 1.1 | FDAガイダンスの名称が旧版ベースの記載となっているため、最新のガイダンス名称に更新すべき。 | ご指摘を踏まえて修正しました。 |
| 11 | 1.2 | 本ガイドラインを強制力のある位置付けにしてはどうか。 | 本ガイドラインは製造販売業者におけるSBOMの導入を支援するものであり、何らかの規制を設けるものではございません。 |
| 12 | 2.1 | 「本ガイドラインにおけるSBOMの位置づけ」の説明には、前段のSBOMの一般的な説明と重複する記載が含まれるため、本ガイドラインにおけるSBOMの位置づけや対象範囲に焦点を当てた記載とすべきである。 | ご指摘を踏まえて修正しました。 |
| 13 | 2.1 | 規制当局へのSBOM提出は現時点で法的義務ではないため、義務と受け取られかねない記載は見直してほしい。 | ご指摘を踏まえて修正しました。 |
| 14 | 2.1 | MDS2におけるSBOMの提供範囲について、一部だけのSBOMを提供するような記載となっているが、一般的な解釈ではない。 | ご指摘を踏まえて修正しました。 |
| 15 | 2.2 | SBOM導入の価値の記載について、現在の記載は自動化による効果の一つであり、SBOM導入の価値ではない。人による確認も重要である。 | ご意見として参考にさせていただきます。 |
| 16 | 2.2 | ライセンス管理はソフトウェア管理上の一般的な活動でありSBOMによる管理が必須ではない。Minimum Elementにも存在しないライセンスに関しては記載すべきではない。 | あくまでSBOMの活用事例を記載しております。 |
| 17 | 2.3 | SBOMの最小要素として記載されている「暗号化ハッシュ」は用語として適切ではないため、「暗号学的ハッシュ」又は「ハッシュ値」等の表現に修正すべきである。 | 「暗号学的ハッシュ」に修正しました。 |

| No. | 該当箇所 | ご意見 | 回答 |
|---|---|---|---|
| 18 | 2.3 | 以下の文章について、製版は手引き書を発行していないので、誤りである。<br>【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および製販から発行されている手引書を参考としつつ】 | ご指摘を踏まえて修正しました。 |
| 19 | 2.3 | 「固有識別子」「作成者」の表現をNTIA記載に準じるべき。 | ご指摘を踏まえて修正しました。 |
| 20 | 2.3 | タイムスタンプをUTCに限定すべきではない。 | ご指摘を踏まえて修正しました。 |
| 21 | 2.3 | サポート終了時期（EOL／EOS）の記載について、FDAの市販前ガイダンスでは「The software component's end-of-support date.」となっており、コンポーネントのサポート期限を要求しているだけで、EOL/EOSを求めてはいない。 | ご指摘を踏まえて修正しました。 |
| 22 | 2.3 | 「位置づける方向性が示されている」はミスリードであり、議論段階である旨を明確化すべき。 | ご指摘を踏まえて修正しました。 |
| 23 | 2.3 | SBOMの最小要素について、NTIA最小要素以外の国際動向も踏まえて見直すべき。 | 国際動向を踏まえて引き続き検討してまいります。 |
| 24 | 2.3、4.1 | SOUP（出所不明ソフトウェア）のSBOM上での取扱いを明確化すべき。 | 2.3項に既知の不明点（Known Unknowns）の運用例を追記いたしました。 |
| 25 | 2.3、4.1、6.1.3 | 既知の不明点（Known Unknowns）の取扱いを明確化すべき。 | 2.3項に既知の不明点（Known Unknowns）の運用例を追記いたしました。 |
| 26 | 2.3、6.2.5、6.3 | EOL/EOS後の補完的リスク低減策を明示すべき。 | 本ガイドラインはSBOMの導入・運用のためのガイドラインであり、サポート終了後の補完的リスク低減策の取扱いについては対象ではございません。 |
| 27 | 2.3、表1 | コンポーネントハッシュの付与を原則化すべき。 | ハッシュの付与は有用であり、可能な限り付与するが推奨されるものではあるものの、IMDRFにおいても必須とまではいえず、現行の記載とさせていただきます。 |
| 28 | 2.4 | SPDXはISO/IEC化はされているが、バージョンは2.2であることに注意が必要。また、ライセンス情報を必須とすることには法務上の課題があり慎重な扱いが必要。 | ご指摘を踏まえて修正しました。 |
| 29 | 2.4 | 脆弱性の影響通知（VEX）の説明について、「悪用可能かどうかを示す」ではなく「製品に影響するかどうかを示す」とすべき。 | ご指摘を踏まえて修正しました。 |
| 30 | 2.4 | SPDXとCycloneDXの選択基準をより明確化すべき。 | ご意見として参考にさせていただきます。 |
| 31 | 2.4 | SBOMを規制当局に提出するにあたっては、機械可読形式に限定すべき。 | ご意見として参考にさせていただきます。 |
| 32 | 2.4 | 人間可読資料の行政当局への提出を必須化してはどうか。 | 本ガイドラインは製造販売業者におけるSBOMの導入を支援するものであり、何らかの規制を設けるものではございません。 |
| 33 | 2.4 | SPDX/CycloneDX変換時の保持項目を明示すべき。また、相互変換の検証に資する参考情報（検証済みツール例等）の記載をしてほしい。 | 変換に際して保持すべき項目の考え方について修正しました。検証済みのツール例については、バージョンによって状況が異なることや中立性の観点から記載しないことといたします。 |
| 34 | 2.5 | SBOM管理は構成管理の一部であり、構成管理プロセスと連動されて運用するという表現は適切ではない。 | ご指摘を踏まえて修正しました。 |
| 35 | 2.5 | SBOMのフォーマットについて、Excelを否定しているように読めるため説明を補足すべき。 | Excelを内部管理で使用することは否定せず、最終的な出力形式としては、標準フォーマットが望ましい旨を明確化しました。 |
| 36 | 2.5 | SBOMの第三者への提供においては、秘密保持契約（NDA）等を前提とした上で、SBOMを共有するメリットがリスクを上回る場合としてはどうか。 | SBOMの情報開示については以下の通り、記載しています。<br>「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。」 |
| 37 | 2.5 | SBOMを活用する部門として、薬事部門を追加すべき。 | ご指摘を踏まえて修正しました。 |
| 38 | 3.1 | 脆弱性を出力する機能は「SBOMツール」ではなく脆弱性照合機能等を明確に記載すべき。 | ご指摘を踏まえて修正しました。 |
| 39 | 3.1、3.2 | 初期段階事業者向けに段階的な導入モデルを示すべき。 | ご意見として参考にさせていただきます。 |
| 40 | 3.1、3.2 | SBOMのExcel・CSVによる暫定運用を許容するべき。 | ガイドラインにおいて許容しないものではございませんが、脆弱性管理等への活用にあたって適切なフォーマットが望ましいと考えます。 |
| 41 | 3.1、3.2 | SBOM導入の段階的な到達目安（優先的に整備する品目等）を示してほしい。また中小事業者向けの支援の方向性を示してほしい。 | すでに医療機器の基本要件基準においてサイバーセキュリティ対応が求められており、優先的に作成する品目を示すことは困難です。また、中小事業者支援については、ガイドラインに記載するものではないことから、現行の記載とさせていただきます。 |

| No. | 該当箇所 | ご意見 | 回答 |
|---|---|---|---|
| 42 | 3.2 | 以下の文章はきれているのではないか。<br>【各役割における関係者は、SBOM 導入企業である製造販売業者と、外部ベンダーソフトウェアの提供元や開発委託先から提供される SBOM に及ぶ。】 | ご指摘を踏まえて修正しました。 |
| 43 | 3.2 | 専任PSIRTの設置を一律求めるものではなく兼務体制や外部専門家活用も認めるべき。 | 専任組織を必須とは記載しておりません。 |
| 44 | 3.2 | 法務部門が必ずしもソフトウェアライセンス管理を担当していない。図 2 について、特に開示についてはサービス部門が積極的に関与すべきであり、具体的な記述を追加すべき。 | 法務部門について例示であり、開示についてはサービス部門を例示として記載しています。 |
| 45 | 4.1 | 表2及び図5において同一の記号（A、B）が異なる意味で使用されており、誤解を招くおそれがあるため、記号の使い分け等により区別を明確にすべきである。 | ご指摘を踏まえて修正しました。 |
| 46 | 4.1 | 図 5 について、表では”Included in”, “Used by”の記載はあるが、どれに対してかの記載がない。また、自社開発OSは、BSP及び暗号化を使用していると記載されているが、表では暗号化が自社開発OSの下には記載されていない。 | ご指摘を踏まえて修正しました。 |
| 47 | 4.1 | 図の凡例や色分けが分かりにくい。 | ご指摘を踏まえて修正しました。 |
| 48 | 4.1 | SBOMの対象範囲を具体化してほしい。 | 医療機器に構成されるものすべてが対象なります。 |
| 49 | 4.1 表2 | 設計から実装まで自社開発コードで構築するのはスタンドアロン型ではなく、スクラッチビルド型ではないか。 | ご指摘を踏まえて修正しました。 |
| 50 | 4.1.1 | スタンドアロン型であれば、無線基板の搭載していないものではないか。 | スタンドアロン型が無線機能を持たない機器では必ずしもないことから、このままとさせていただきます。 |
| 51 | 4.1.2 B | 「主要モジュール単位」ではなく「識別可能なコンポーネント単位」とすべき。 | ご指摘を踏まえて修正しました。 |
| 52 | 4.1.2 B | 「再帰的」の用語は自身を呼び出す構成の場合に使用され、不適切である。 | ご指摘を踏まえて修正しました。 |
| 53 | 4.1.2、4.4 | 第三者からSBOMが取得できない場合の対応を明記すべき。 | 4.4項に第三者ソフトウェアについてのSBOM入手に関する記載を追加しました。 |
| 54 | 4.1.3 | 図にAPIの記載をしてはどうか。 | 今回の例においては、SaMD内部にAPI搭載を想定しているわけではないため、図への追記は不要としました。 |
| 55 | 4.1.3 | AI-SBOMの考え方を取り込むべき。 | 本ガイドラインはSBOMの導入・作成のためのガイドラインであり、いただいたご意見は今後の検討の参考にさせていただきます。 |
| 56 | 4.1.3、6.1.2 | 継続的に更新されるSaMDについて、動的なSBOM管理の考え方を導入すべき。 | ご意見として参考にさせていただきます。 |
| 57 | 4.1.4 | サーバープリケーションとは、サーバーアプリケーションの誤記か。 | ご指摘を踏まえて修正しました。 |
| 58 | 4.1.4 D | パターンDの医療機器の説明と実例が実態に合っていない。パターンDがパターンAとBの組み合わせであるように修正すべき。 | ご指摘を踏まえて修正しました。 |
| 59 | 4.2.1 | SBOM選定基準チェックリストとして利用しやすくするため、選定基準はマトリックス形式ではなく、1行につき1項目のチェックリスト形式に変更してほしい。 | ご意見として参考にさせていただきます。 |
| 60 | 4.2.1 | SBOMツールの選定表について、一覧表でまとめるなど見やすくしてほしい。 | ご指摘を踏まえて修正しました。 |
| 61 | 4.2.1 | ツール選定の妥当性を表3だけで判断できるよう、可能な範囲で表3の選定基準に集約してほしい。 | ご意見として参考にさせていただきます。 |
| 62 | 4.3.2、5.1.2 | SBOM生成ツール・脆弱性照合ツールについて、リスクベースでのバリデーションの考え方や確認方法の例を示すべき。 | SBOMツールについては、QMS省令に基づくバリデーションの対象となり得ますが、リスクに基づくアプローチを適用し、リスクに応じて管理の程度を定めることを否定するものではございません。 |
| 63 | 5.1.1 | ログ確認結果の記録方法を明確化すべき。 | ご意見も踏まえ修正いたしました。 |
| 64 | 5.2 | SBOMについて、デジタル署名（監査証跡があるもの）の要件を記載してはどうか。 | ご意見として参考にさせていただきます。 |
| 65 | 5.2.4 | 第三者提供のSBOMをインポートするかどうかは5.2.4ではなく、適用範囲を定める段階で検討すべき事項ではないか。 | ご指摘を踏まえて修正しました。 |
| 66 | 5.3 | 医療機関に提供されるSBOMについて、対象範囲、対象外の範囲及びその理由並びに医療機関が活用できる範囲を明確化すべきである。 | 医療機関に提供されるSBOMの範囲については、「5.3 SBOMの開示」において考え方を示しています。 |

| No. | 該当箇所 | ご意見 | 回答 |
|---|---|---|---|
| 67 | 5.3 | 医療機関における調達、契約、保守及び脆弱性対応等でSBOMを活用できるよう、契約書や仕様書への反映方法等の具体例を示すべきである。また、機械可読なSBOMに加え、医療機関が利用しやすい要約情報の提供を推奨すべきである。 | ご意見として参考にさせていただきます。 |
| 68 | 5.3、6.2.3、全体 | SBOMの作成・維持・活用について、製造販売業者と医療機関の責任及び役割分担を明確にすべき。 | 3.2項「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」「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」と記載していることから、現行の記載とさせていただきます。 |
| 69 | 5.3.1 | 医療機関等へのSBOMの提供にあたり、秘密保持契約（NDA）等の管理措置を本文に追記すべき。 | 第三者へのSBOMの提供については、5.3.3に契約等の手続きを記載していることから、現行の記載とさせていただきます。 |
| 70 | 5.3.1～5.3.3 | 脆弱性の影響通知（VEX）の位置付けを明確化すべき。 | 第二版の作成に向けて検討いたします。 |
| 71 | 5.3.3 | 脆弱性公表時の影響有無について、結論だけでなく、使用状況や悪用可能性等の判断根拠を示すべきである。 | 脆弱性公表時の影響有無の判断根拠等の取扱いについては、今後の改訂に向けた検討事項とさせていただきます。 |
| 72 | 6.1.2 | SBOM更新と構成管理との関係を明確化すべき。 | ご指摘を踏まえて修正しました。 |
| 73 | 6.1.3 | SBOM提示の根拠としてJIS T 2304を挙げるのは適切ではない可能性があるため、法令・ガイドライン上の根拠を再確認し、医療機関へのSBOM提供に関する記載を見直してほしい。 | ご指摘を踏まえて修正しました。 |
| 74 | 6.2.1、6.2.3 | JPCERT/CCとの連携手順を明示すべき。 | 本ガイドラインはSBOMの導入・運用のためのガイドラインであり、JPCERT/CCとの連携等の脆弱性対応の手順は対象ではございません。<br>脆弱性の管理については「医療機器のサイバーセキュリティを確保するための脆弱性の管理等について（令和６年３月28日付厚生労働省医薬局医療機器審査管理課長、医薬安全対策課長連名通知）」にてお示ししています。 |
| 75 | 6.2.2 | JIS T 14971との統合を前提とせず、異なる規格・ガイダンスの立場でも解釈可能な中立的表現に見直してほしい。 | ご指摘を踏まえて修正しました。 |
| 76 | 6.2.2 | トリアージにおいて、CVSS以外の指標の活用も必要と考える。 | CVSSは一例として示しております。 |
| 77 | 6.2.2 | CVSSのみでリスク許容の判断しないことを明確化すべき。 | CVSSは一例として示しており、CVSSのみをもってリスク許容不可とするものではございません。 |
| 78 | 6.3. | コンポーネントの利用者がコンポーネントの作成者に連絡するのではないか。 | ご指摘を踏まえて修正しました。 |
| 79 | 用語 | 用語「アップデート」の定義について、注釈の参照元や出典表記が原典と整合していない箇所があるため、原典に合わせて注釈・出典を修正してほしい。 | ご指摘を踏まえて修正しました。 |
| 80 | 用語 | 用語「攻撃」の出典について、特段の理由がなければ手引書経由の引用ではなく、定義の原典であるJIS Q 27000:2019を直接参照する記載にしてほしい。 | ご指摘を踏まえて修正しました。 |
| 81 | 用語 | 用語「サイバーセキュリティ」について、JISと手引書で定義・表現が異なるため、引用元をどちらか一方に統一し、その出典に整合した記載へ修正してほしい。特に「不正アクセス」のように日本国内で特定の意味を持つ用語の扱いには配慮してほしい。 | ご指摘を踏まえて修正しました。 |
| 82 | 用語 | 用語「ソフトウェア部品表（SBOM）」の出典として記載されている「製造販売業者向け手引書」に該当する記述が見当たらないため、出典の誤記を確認し、適切な出典へ修正するか削除してほしい。 | ご指摘を踏まえて修正しました。 |
| 83 | 用語 | 用語「情報共有分析機関（ISAOs）」の説明について、出典元の手引書に誤植が含まれているため、そのまま引用せず、意味が明確になるよう表記を修正してほしい。 | ご指摘を踏まえて修正しました。 |
| 84 | 用語 | 用語「メタデータ」の定義にある「情報データ」は冗長な表現であるため、簡潔かつ自然な定義に修正してほしい。 | ご指摘を踏まえて修正しました。 |
| 85 | 用語 | 用語集に記載されている参考資料等について、URLの更新が必要な箇所があるため修正すべきである。また、PSIRTに関する参考資料として、SBOMに関する内容が追記されたIPAの最新の「製品開発者向けガイド」についても参照先として記載を検討すべきである。 | ご指摘を踏まえて修正しました。 |
| 86 | 文献 | FDAガイダンス名を最新名称へ修正すべき。 | ご指摘を踏まえて修正しました。 |

| No. | 該当箇所 | ご意見 | 回答 |
|---|---|---|---|
| 87 | 文献 | 背景及び参考文献において引用しているFDA文書について、文書名や発行年に誤り又は古い情報が含まれており、最新の名称・内容に基づき記載を見直すべきである。また、関連する米国の規制として、FDAガイダンスだけでなくFD&C法の引用についても検討すべきである。 | ご指摘を踏まえて修正しました。 |
| 88 | 文献 | 文献リストで記載様式にばらつきがあり、一部で著者名や発行年も欠落しているため、引用・表記形式を統一してほしい。 | ご指摘を踏まえて修正しました。 |
| 89 | 文献 | 英語版文書を参照しているのであれば、文献タイトルも原文の英語表記で統一してほしい。 | ご指摘を踏まえて修正しました。 |