

SBOMは、生成ツールだけでは完成しない。



医療機器のSBOM作成・補記・構成管理ツール



単一HTMLファイル

ファイル1つ。ブラウザで開くだけ



インストール不要

社内PCの構成を変更しません



外部通信なし

SBOMの内容は端末外に出ません

規制は「作れ」と言うが、「どう作るか」は書かれていない

2024年4月1日、医療機器の基本要件基準 第12条第3項の経過措置期間が満了し、適合が必須となりました。厚生労働省の通知は「構成管理プロセスは、当該医療機器のソフトウェア部品表（SBOM）を適切に作成することによって確認すること」と定めています。2026年8月25日発出の「医療機器におけるSBOM導入・運用ガイドライン（第1版）」は、「**SBOMツールを活用したSBOMの作成・管理を前提とし**」と明記しています。

実務で起きている3つの問題

01

生成ツールの出力は、そのままでは最小要素を満たさない

広く使われている npm sbom および cyclonedx-py の標準出力を検証したところ、Component Producer・Component Hash・SBOM Author のいずれも含まれていませんでした。

02

サポートレベルとEOSは、そもそも標準フィールドにない

FDA が求める各コンポーネントのサポート状態・サポート終了日（EOS）は、SPDX・CycloneDX いずれにおいても標準の必須フィールドではありません。人手による補記は例外ではなく、標準工程です。

03

再生成のたびに、補記した情報が消える

ソフトウェアを改訂すればSBOMは再生成され、補記したサプライヤー名・EOS・製造者情報は上書きされて失われます。補記は一度で終わらず、リリースのたびに繰り返されます。

問題は「SBOMを生成できないこと」ではなく、
「生成したSBOMを、提出できる状態まで仕上げて、維持し続けられないこと」です。

2製品の対比

MSC SBOM Inspector		MSC SBOM Editor
役割	読む・判定する・記録に残す	直す・作る・出す・維持する
機能	最小要素の適合判定／可視化／CSV出力・印刷／作業ファイルの保存	左記すべて＋不足項目の補記／CSVからのSBOM新規作成／機械可読SBOMの出力／差分マージ／構成管理・承認記録
提供	無償（申請制配布）	有償（買い切り）

読む。直す。作る。出す。維持する。

MSC SBOM Editor でできること

☑ 適合判定と補記

不足している項目を一覧で提示し、サポートレベル・EOS・製造者など、生成ツールが出力しない情報を画面上で補います。

📄 CSVからのSBOM新規作成

機械可読SBOMをまだ持っていないでも、コンポーネント一覧からSPDX／CycloneDX を作成できます。Excelでの手動作成から、ツールによる作成・管理への移行経路になります。

📄 機械可読SBOMと補助資料の出力

SPDX／CycloneDX に加え、当局提出時に添付が推奨される人間可読の一覧（PDF／Excel）を出力します。

🔄 差分マージと構成管理

再生成されたSBOMに前版の補記情報を引き継ぎ、版数・変更履歴・承認記録とともに管理します。補記のやり直しを終わらせます。

判定ロジックは、無償版と有償版で**完全に同一**です。両版は単一のソースコードから同時に生成され、判定基準層・判定層にバージョンによる分岐を持ちません。この一貫性はビルド時および自動回帰試験（102件）で機械的に検証され、配布時にSHA-256を併記します。

価格

製品・サービス（型式）	価格（税別）	内容
MSC SBOM Inspector (MSC-SBOM-I)	無償	申請制配布。判定・可視化・記録まで（CSV出力・印刷は対応。機械可読SBOMの編集・出力は不可）
MSC SBOM Editor (MSC-SBOM-E)	¥50,000（買い切り）	1事業所・永久利用権・改版の無償配布
MSC SBOM Editor + CSVパッケージ (MSC-SBOM-ECSV)	¥98,000（買い切り）	上記 + QMS省令第5条の6 対応のバリデーション文書一式6点
初回相談	無料	Eメールまたは、オンラインWEBミーティング
個別コンサルテーション	1時間 ¥15,000	30分単位
アドバイザー契約	月 ¥200,000	実働20時間以内／月。Editor + CSVパッケージを無償同梱

判定基準は「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）附属書A・7項目」を既定とし、「輸出・政府調達モード（CISA 2026・データフィールド17項目 + 実務プロセス6項目）」に切り替えることができます。

ご相談の流れ

1 STEP 1 | 無償版で判定

Inspector をお試しください。申請フォームからお申し込みいただき、貴社のSBOMをそのまま読み込んで判定できます。

2 STEP 2 | 初回相談（無料）

EメールまたはWEB会議で承ります。判定結果を見ながら、貴社の現状と必要な対応を整理します。

3 STEP 3 | 導入・規制対応

Editor は買い切りです。SBOMの記載規約策定、第12条第3項への適合説明、調達契約へのSBOM条項の組込み、SBOMとISO 14971リスクマネジメントの接続などは、個別コンサルテーションまたはアドバイザー契約にて承ります。

販売対象について

MSC SBOM Editor は、医療機器製造販売業者・製造業者（許可取得前のSaMD開発企業を含む）、受託開発会社・部品供給者を対象に販売しております。許可・登録の有無は自己申告で、許可番号・登録番号のご記載は不要です。

サポートについて

本製品にサポートは含まれておりません。ご質問・導入のご相談は、初回相談（無料）または個別コンサルテーションをご利用ください。

Medical Software Consulting（代表：酒井 由夫） | 設立：2025年6月1日 | インボイス登録番号：T4810470679426

医療機器メーカーにて約39年、ソフトウェア開発・品質保証・規制対応に従事。FDA査察対応、IEC 62304 の社内導入、医療機器工業会での規格検討および講師活動に従事。

お問い合わせ・初回相談のお申し込み <https://sbom.medicalsoftwareconsulting.com/contact/>

※ 本ツールの判定結果は、最小要素への充足状況を機械的に示すものであり、規制適合を証明するものではありません。

「該当しない」と、簡単には言わない。

既知脆弱性の簡易照会 —— Editor 限定機能

「医療機器のサイバーセキュリティ導入に関する手引書」6.2「SBOMに基づく脆弱性管理」のうち、最初のステップ——既知CVEとの照合だけを、Editorが簡易的に担います。トライージ・対処以降は、貴社の脆弱性管理プロセスまたはPSIRTが引き続き担ってください。

内蔵CVE表 or 外部リスト

内蔵CVE表（数件～十数件）、または外部CSVリスト（最大200件）と照合します。

3状態で判定

「該当の可能性あり／該当しない／判定不能」の3状態と判定根拠を画面に表示します。

結果をCSVで出力

照合結果はCSVで出力できます。社内記録・提出資料の下地としてお使いいただけます。

ブラウザ内で完結

外部通信は発生しません。単一HTMLファイル・外部通信なしという設計をそのまま引き継ぎます。

Editor v2.0 の脆弱性照合について

できること

内蔵CVE表（数件～十数件）または外部CSVリスト（最大200件）と照合します。「該当の可能性あり／該当しない／判定不能」の3状態と判定根拠を表示し、結果をCSVで出力できます。ブラウザ内で完結します。

できないこと

汎用の脆弱性データベースとの網羅照合、脆弱性情報の継続収集・通知、トライージ記録。照合はpurl／cpeの文字列一致による簡易方式で、版数比較はsemver・数値の点区切り形式のみです。

安全側に倒す設計

情報が不足するときは「該当しない」ではなく「判定不能」を返します。5.1.3「未特定は未特定として明示する」、6.2.2「すべての脆弱性に一律に対応することを前提としない」と同じ考え方です。

収録例

内蔵CVE表には、Log4Shell（CVE-2021-44228）・Heartbleed（CVE-2014-0160）・xz backdoor（CVE-2024-3094）など、影響の大きかった実例を含みます（数件～十数件を収録・随時見直し）。

ご利用の流れ（3ステップ）

1

既知CVE表・外部リストで照合

SBOMのコンポーネント一覧を、内蔵CVE表または外部CSVリスト（最大200件）と自動的に照合します。

2

「判定不能」も含めて確認

「該当の可能性あり」「判定不能」と表示された項目を優先的に確認します。「該当しない」の断定は行いません。

3

CSVで抜き出し、以降の工程へ

照合結果をCSVで出力し、対応が必要な項目を貴社の脆弱性管理プロセスまたはPSIRTへ引き渡します。

脆弱性照合は Editor 限定の機能で、Inspector には含まれません。工程全体とガイドライン条項との対応は次ページで解説します。

※ 脆弱性の簡易照合結果は、既知CVEとの限定的な照合であり、脆弱性が存在しないことを保証するものではありません。

ガイドラインは、生成の後ろに、長い工程を置いた。

医療機器における SBOM 導入・運用ガイドライン（第1版）／令和8年8月25日 医薬機審発0825第1号（厚生労働省医薬局医療機器審査管理課長通知）

発行されたガイドラインが、はっきりさせた3つのこと

ツールを使うことが前提になった

「SBOMツールを活用したSBOMの作成・管理を前提とし」とガイドラインは宣言しています。実務の前提はツールに移りました。

ガイドライン 4.2 / 5.1.6

「生成すれば正しい」は否定された

「ツールで出力したSBOMを無条件に正とみなすのは品質保証上リスクがある」。検出漏れ・誤検出を前提とした確認が必要です。

ガイドライン 2.5 / 5.1.2

ツール自体が管理対象になった

SBOMツールの調達はQMS省令第37～39条の購買管理、第5条の6のバリデーション・記録管理の対象となり得ます。

ガイドライン 4.3.2

ガイドラインの工程と、それを担うもの

解析・生成

5.1.1 コンポーネント解析の実施フロー / 5.1.6 SBOMツールを前提とした運用

SCA・SBOM生成ツールの領域（Syft／cdxgen／npm sbom／cyclonedx-py／有償SCA 等）

確認・補正・作成・開示・変更管理

5.1.2 解析結果の確認 / 5.1.3 手動補正・未特定コンポーネント / 5.2 SBOMの作成 / 5.3 SBOMの開示 / 6.1 SBOMの管理



読む・判定する・記録に残す



直す・作る・出す・維持する

生成ツールの多くは、この帯を持ちません。

脆弱性照合・トリージ・対処

6.2 SBOMに基づく脆弱性管理 / 6.2.2 脆弱性の影響評価と優先度付け（トリージ）

脆弱性管理プラットフォーム・PSIRTの領域 —— **うち「既知CVEとの照合」のみ Editor v2.0 が簡易的に担います**

ガイドラインの条項と、2製品の対応

ガイドライン条項	求められていること	MSC SBOM Inspector・Editor の対応
2.3 SBOMの最小要素	サプライヤー名・コンポーネント名・バージョン・固有識別子・関係・作成主体・タイムスタンプ。ハッシュは「可能な限り付与する」	Inspector : 最小要素の充足を項目別に判定・可視化。 Editor : 不足項目を画面上で補記
2.5 SBOMに関する誤解	「ツールで生成すれば正しい」を否定。生成ツール及び運用プロセスが意図した用途に適切に機能していることを、CSVの考え方を踏まえて確認する	Editor + CSVパッケージ : QMS省令第5条の6に対応するバリデーション文書一式6点
5.1.2 / 5.1.3 確認と手動補正	検出漏れ・誤検出を前提とした確認。特定できないコンポーネントは「未特定」「既知の不明点（Known Unknowns）」として明示する	Editor : 補記と未特定の明示。空欄のまま出さず、不明は不明として出す
5.2.2 名称・付加情報	社内でのみ使ってきたプロジェクト名称やバージョン表記が、そのまま外部へ共有されることを避ける	Editor : 製品識別情報・作成主体・タイムスタンプを利用者視点で整備
5.3.2 / 5.3.3 開示レベルと提供方法	当局向けは把握できている全件、医療機関向けは合意した範囲。当面は電子ファイル等の手動運用も許容	Editor : 開示範囲の切替と、機械可読（SPDX／CycloneDX）＋人間可読（PDF／Excel）の同時出力
6.1.2 更新・変更管理	改訂のたびに構成を反映し、「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	Editor : 差分マージで前版の補記を引き継ぎ、版数・変更履歴・承認記録とともに保持
6.1.3 保管及び完全性	改ざん・なりすましを防ぐため、可能な範囲でハッシュ値や電子署名を付与し検証できるようにする	両版 : 配布物にSHA-256を併記。コンポーネントハッシュの保持・出力に対応

この2製品の境界

・コンポーネント解析（ソースコード／バイナリのスキャン）は行いません。 ・脆弱性情報の継続収集とCVE通知は行いません。

ガイドライン4.2.2は「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」よう求めています。この2製品は解析ツールを置き換えるものではなく、その出力を、提出できる状態に仕上げて維持するための後段を担います。Editor v2.0 の既知CVE照合は、汎用の脆弱性データベースではありません（次ページ）。

どのツールと、どう組み合わせるか。

ガイドライン 4.2「SBOMツールの選定」・4.2.2「選定にあたっての留意事項」・4.2.3「評価・選定の進め方」を踏まえた整理

守備範囲で見た、ツールの区分

区分	解析生成	最小要素の判定	補記・未特定の明示	開示用の出力	更新・変更管理	脆弱性照合	費用感
表計算による手動管理	－	△	○	△	△	－	人件費のみ
無償の生成ツール	◎	－	－	△	－	－	無償（OSS）
無償の脆弱性照合	－	－	－	－	△	◎	無償（OSS）
有償SCA・製品セキュリティプラットフォーム	◎	△	△	○	○	◎	年額・規模課金（開発者数・コード量 等）
MSC SBOM Inspector 無償・申請制配布	－	◎	－	－	－	－	無償
MSC SBOM Editor 有償・買い切り	－	◎	◎	◎	○	△	¥50,000（買い切り）

◎ 中核機能 ○ 対応 △ 限定的・運用で補う － 対象外 本表はガイドライン表3の観点のうち「機能」「対応フォーマット」の軸による一般的な傾向の整理です。個々の製品の機能は版・エディション・構成により異なるため、4.2.3のとおり無償トライアル等による実機評価をお勧めします。本表は機能の守備範囲による一般的な整理であり、特定の製品の優劣を示すものではありません。

Editor v2.0 の△は、どこまでを指すか ―― 脆弱性照合は Editor 限定の機能で、Inspector には含まれません。

できること

内蔵CVE表（数件～十数件）または外部CSVリスト（最大200件）と照合します。「該当の可能性あり／該当しない／判定不能」の3状態と判定根拠を表示し、結果をCSVで出力できます。ブラウザ内で完結します。

できないこと

汎用の脆弱性データベースとの網羅照合、脆弱性情報の継続収集・通知、トリアージ記録。照合はpurl／cpeの文字列一致による簡易方式で、版数比較はsemver・数値の点区切り形式のみです。

安全側に倒す設計

情報が不足するときは「該当しない」ではなく「判定不能」を返します。5.1.3「未特定は未特定として明示する」、6.2.2「すべての脆弱性に一律に対応することを前提としない」と同じ考え方です。

3つの使い分けパターン

1これから着手する

無償の生成ツールでSBOMを作り、Inspector（無償）で最小要素の充足を判定する。不足が見えたところで、Editorで補記して出す。

判定までは費用がかかりません。

根拠：4.2.2「まずは無償ツールを用いてSBOMを作成し…有償ツールへの移行や追加導入の可否を判断するという段階的な進め方が有効」／3.1 第1段階

2すでに有償SCAを導入済み

解析は既存ツールに一本化したまま、その出力をInspectorで判定し、当局・医療機関へ出す形にEditorで仕上げる。

解析ツールを増やさないため、運用は複雑化しません。

根拠：4.2.2「複数のSBOMツールを目的別に使い分けるとは、運用が複雑化し…管理コストや人的負担が増大する要因となり得る」

3SBOMをまだ持っていない

Excelのコンポーネント一覧をEditorに読み込ませ、SPDX／CycloneDXを新規作成する。SaMD・小規模開発の出発点。

Excel運用から、標準フォーマットへ移行します。

根拠：2.5「Excelのみの運用では、表記揺れの抑止、更新漏れの防止…変更履歴の一貫管理に限界がある」／3.1

ガイドライン表3の選定観点に対する回答

提供形態

単一HTMLファイル。端末内で完結します。SaaS型ではないため、4.2.2が求める「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」の事前確認が生じません。

日本語対応

表3は「日本語対応している開発元は少ない」と指摘しています。UI・判定基準・出力とも日本語で、国内通知・手引書の用語に揃えています。

コスト

買い切り。解析コード量や開発者数による課金はありません。

サポート体制

本製品にサポートは含まれません。初回相談（無料）または個別コンサルテーションで承ります。

対応フォーマット

SPDX 2.2以上／CycloneDX 1.6以上の入出力。2.4が新規導入時の推奨フォーマットとする2形式です。

バリデーション

QMS省令第5条の6に対応する文書一式（CSVパッケージ）をオプションで提供します。

まずは Inspector（無償）で、いまのSBOMを判定してください。 <https://sbom.medicalsoftwareconsulting.com/inspector/>

※ 本ツールの判定結果は、最小要素への充足状況を機械的に示すものであり、規制適合を証明するものではありません。