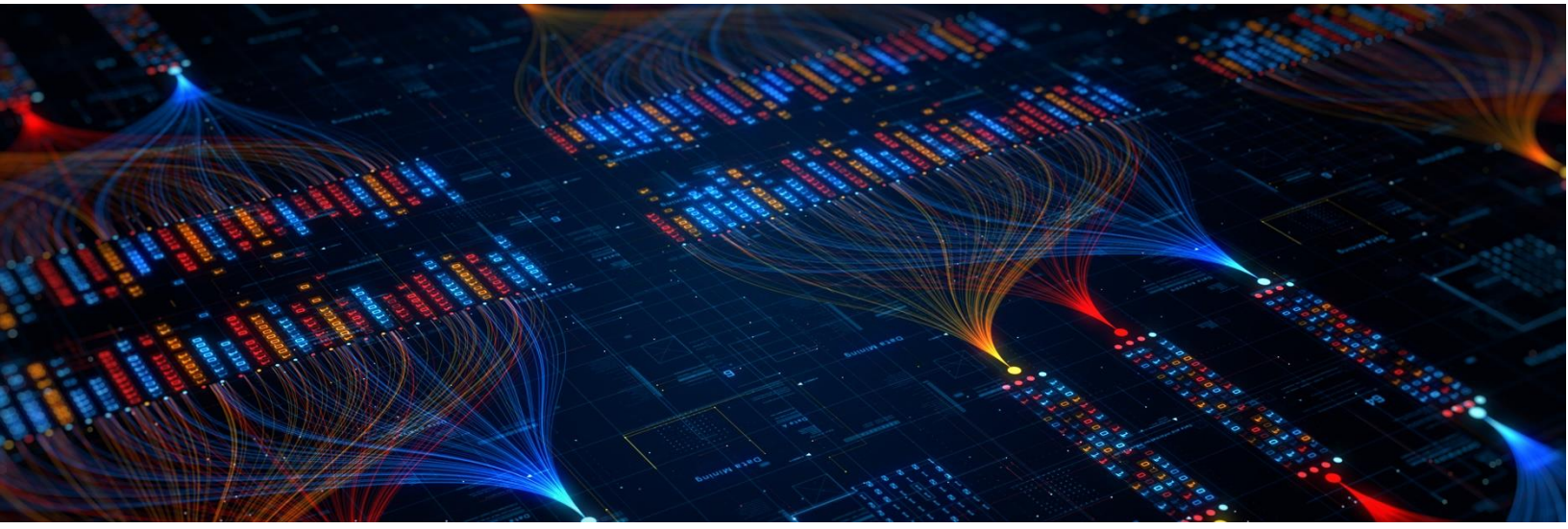
2026 ソフトウェア部品表（SBOM）の最小要素

公表：2026 年 7 月 29 日



概要

タイトル	2026 ソフトウェア部品表（SBOM）の最小要素
初版公開	July 29, 2026
概要	CISA は、共同作成機関と連携し、2021 年に米国商務省国家電気通信情報庁（NTIA）が公表した文書の中核原則を維持しつつ、現在の SBOM に関するニーズを反映するため、「ソフトウェア部品表（SBOM）の最小要素」を更新した。ソフトウェア・エコシステム全体における関係者による採用及び実装の進展により、SBOM データの新たなユースケース及び活用方法が明らかとなった。SBOM の採用及び実装の拡大に伴い、SBOM ツールは、2021 年当時に利用可能であったツールの能力及び機能を大きく超えて発達している。これらの進展により、SBOM の提出を求める組織は、自組織のソフトウェア・コンポーネント及びサプライチェーンに関して、より多くの情報を要求できるようになっている。
主要な対応事項	▪ 組織は、更新版の SBOM 最小要素を満たす SBOM の提出を求めるべきである。 ▪ 組織は、利用可能なツールを使用して、SBOM の生成、取り込み、分析を行うべきである。 ▪ 組織は、更新版の SBOM 最小要素を満たす SBOM を生成すべきである。
想定読者	ソフトウェアを開発、調達、又は運用する組織

版履歴

版	日付	改訂内容
1.0	2021 年 7 月 12 日	初版。
2.0	2025 年 8 月 22 日	2021 年以降の SBOM ツール及び技術実装の進展を反映した更新を含むドラフト文書を公表。
2.1	2026 年 7 月 29 日	共同作成機関と連携し、SBOM 最小要素ドラフトに対する意見募集へのコメントを踏まえて文書を更新。

目次

序論

ソフトウェア部品表（SBOM）は、ソフトウェア・セキュリティ及びソフトウェア・サプライチェーン・リスク管理における重要な構成要素として位置付けられるに至っている。SBOM とは、多層的なインベントリ、すなわちソフトウェア・アプリケーション及びシステムを構成する材料の一覧である。ソフトウェアを開発、調達、運用する組織は、SBOM データを用いることにより、自らのソフトウェア・サプライチェーンをよりよく理解することができる。ソフトウェア・サプライチェーンの可視性が高まることで、既知及び新たに発見された脆弱性やリスクへの対応を含む、リスク管理上の意思決定を促進し得る。

本書は、米国サイバーセキュリティ・インフラセキュリティ庁（CISA）及び以下のパートナー（以下「作成機関」という。）により作成されたものであり、国家電気通信情報庁（NTIA）が公表した「ソフトウェア部品表の最小要素（SBOM Minimum Elements）」を更新し、これに置き換えるものである。本書に示す要素は、SBOM に期待される最低限のデータフィールド並びにプラクティスとプロセスを定めるものである。

- アメリカ国家安全保障局（NSA）
- 米国連邦捜査局（FBI）
- オーストラリア通信情報局オーストラリアサイバーセキュリティセンター（ASD's ACSC）
- カナダサイバーセキュリティセンター（Cyber Centre）
- チェコ共和国国家サイバー情報セキュリティ庁（NÚKIB）
- フランス国家情報システムセキュリティ庁(ANSSI)
- ドイツ連邦情報セキュリティ庁（BSI）
- インドコンピュータ緊急対応チーム（CERT-In）
- イタリア国家サイバーセキュリティ庁（ACN）
- 経済産業省（METI）
- 内閣サイバー統括室（NCO）
- 韓国国家情報院／国家サイバー安全センター（NIS/NCSC）
- 韓国インターネット振興院（KISA）
- オランダ国家サイバーセキュリティセンター（NCSC-NL）
- ニュージーランド国家サイバーセキュリティセンター（NCSC-NZ）
- ポーランド学術・研究コンピュータネットワーク国立研究所（NASK）
- スロバキア国家安全保障庁（NBÚ）

NTIA が 2021 年に「ソフトウェア部品表の最小要素（SBOM Minimum Elements）」を公表して以降、ソフトウェア・エコシステム全体の組織、専門家及び実務担当者は、SBOM をソフトウェア開発及びセキュリティ実務に取り入れてきた。ソフトウェア・サプライチェーンの透明性における SBOM の役割は国際的にも認識されている。「Secure by Design」イニシアティブに参加している国際的なパートナーは、SBOM が安全な製品開発の中核的な製品開発プラクティスの一つであると認識している。

世界 18 のサイバーセキュリティ機関は、「サイバーセキュリティのためのソフトウェア部品表（SBOM）に関する共有ビジョン」において、SBOM の利点を示した。
日本の経済産業省は、「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」において、ソフトウェアサプライヤーが SBOM を導入するための指針を示している。
欧州連合（EU）のサイバーレジリエンス法（Cyber Resilience Act、EU 規則 2024/2847）は、デジタル要素を有する製品の製造者に対し、技術文書の一部として SBOM の提供を義務付けている。
ドイツ連邦情報セキュリティ庁（BSI）は、「BSI TR-03183-2：製造者および製品に対するサイバーレジリエンス要件 第 2 部：Software Bill of Materials（SBOM）」において、SBOM に関する技術要件を示している。
インドの CERT-In は、「Technical Guidelines on Bill of Materials」において、SBOM およびその他の部品表（Bill of Materials）に関する要件を示している。

SBOM ツールは、SBOM を生成、共有、利用、分析する組織の増加に後押しされて発展してきた。これらの発展により、SBOM の提出を求める組織は、2021 年当時に比べ、自組織のサプライチェーン及びソフトウェア・コンポーネントについて、より詳細な情報を要求できるようになっている。
本書で議論する最小要素は、すべてのソフトウェアに適用される。人工知能（AI）ソフトウェア・システム[1]やクラウド環境におけるサービス型ソフトウェア（SaaS）のような一部のソフトウェアは、さらなる要素を要する場合がある。異なる種類のソフトウェアについては、追加のデータフィールド、プラクティス及びプロセスが有益な場合がある。ソフトウェアの種類にかかわらず、ソフトウェアの透明性向上に向けたいかなる取組も、まず最小要素の適用から始めるべきである。

主な更新点

2026 年版の SBOM 最小要素の更新は、2021 年版の中核原則を維持しつつ、現在の SBOM ニーズを反映したものである。例えば、自動化は依然として大規模なセキュリティ推進に不可欠である。本改訂は、2025 年版「ソフトウェア部品表（SBOM）の最小要素」に対する意見募集に寄せられた公開コメントを取り込んでいる。これらの改訂により、データ品質が向上し、より広範な SBOM ユースケースを支援することができるようになっている。**SBOM 最小要素及び定義については附属書 A** を、**2021 年版からの変更点の詳細な要約については附属書 B** を参照されたい。
新たな SBOM 要素（ソフトウェア・セキュリティに関するよりリスク情報に基づく判断を支援するためのもの）：

- SBOM 作成主体の署名
- SBOM データフォーマット名
- SBOM データフォーマットバージョン
- SBOM 生成コンテキスト
- SBOM ツール名
- SBOM ツールのバージョン
- SBOM バージョン
- コンポーネントのハッシュ値
- コンポーネントのハッシュ・アルゴリズム
- コンポーネント・ライセンス

[1] CISA ならびに G7 の国際パートナーであるドイツ、カナダ、フランス、イタリア、日本、英国、欧州連合（EU）は共同で、2026 年 5 月にガイダンス「Software Bill of Materials for AI – Minimum Elements」を公開した。

主な更新（対象範囲の明確化及び期待事項の特定のためのもの）：

SBOM 作成主体
コンポーネント識別子
コンポーネント提供主体
コンポーネント・バージョン
SBOM データ更新への対応
カバレッジ
不明情報の明示
機械処理可能なデータ

軽微な更新（情報品質の向上及び技術的進展との整合のためのもの）：

SBOM タイムスタンプ
コンポーネント名
コンポーネント依存関係
配布及び提供
頻度

注: 本改訂では要素としての「アクセス制御」は削除し、アクセス制御に関する考慮事項を「配布及び提供」に取り込んでいる。

なぜSBOMか：透明性とセキュリティの向上

SBOM は、ソフトウェア及びサプライチェーンの透明性を高めるための重要な一歩であり、組織が自らのソフトウェア・システムに含まれるコンポーネントに関して、リスク情報に基づく判断を行うことを支援する。コンポーネントには、従来型ソフトウェア、ファームウェア、AI システム及び SaaS が含まれ得る。SBOM はソフトウェアの材料表として機能し、組織に対し、自らのソフトウェアの構成に関するデータを提供する。組織は、そのデータを、ソフトウェア・システムのセキュリティリスクを低減するための迅速かつ自動化された対応につながる実用的な情報へと変換できる。

SBOM は、おおむね階層構造となっている。ソフトウェアはコンポーネントから構成され、各コンポーネントは更なるサブコンポーネントを含む場合がある。さらに、それらのサブコンポーネントもまた別のサブコンポーネントから構成される場合があり、同様の構造が繰り返される。コンポーネント（及びサブコンポーネント）は、「ファーストパーティ」又は「サードパーティ」に由来し得る。ファーストパーティのコンポーネントは、SBOM を作成する主体に由来し、独立した追跡可能なソフトウェア単位として識別可能なものである。サードパーティコンポーネントは外部供給元に由来するものである。各コンポーネントは、そのサブコンポーネント及び依存関係の階層を把握できる SBOM を有するべきである。

ソフトウェア・データを共有し利用するための効果的な仕組みは、機械処理可能であり、かつ拡張可能であることが求められる。SBOM は、コンポーネント・データを機械処理可能な形式で記録し、分析、共有及び管理を支援する。組織は、SBOM データを、セキュリティアドバイザリや組織レベルの承認・不承認ソフトウェア・データベース等の他の情報ソースに対応付けることにより、安全なソフトウェア開発や脆弱性管理等の他の重要な実務の改善を行うことができる。SBOM は、ソフトウェア・セキュリティ及びサプライチェーンに関するすべての懸念を解消するものではないが、リスク情報に基づくセキュリティ上の意思決定を可能にし、それを後押しするための必要な一歩である。

なぜ最小要素か：大規模なセキュリティ推進

本最小要素は、SBOM が満たすべき基本的な基準を定めるものである。現代において組織が利用するソフトウェアの量は、手作業のプロセスで効果的にリスクを評価し緩和できる水準を超えている。重要な機能及び重要インフラを支える上でソフトウェアが果たす役割を踏まえると、誰にも追跡・管理されないソフトウェアは、重要インフラ及び政府システムを含め、重大なサイバーセキュリティ上の脅威となり得る。[2]SBOM について共有認識や期待事項を整理することで、組織が SBOM データをソフトウェア及びサプライチェーンのセキュリティ実務に適用しやすくなり、情報共有も促進される。
ソフトウェア・エコシステム全体にわたる組織及び世界中の実務担当者は、ソフトウェア及びサプライチェーンの透明性向上における SBOM の重要な役割を認識しており、SBOM 採用の拡大や SBOM 技術実装の進展に貢献してきた。SBOM の採用が世界的に産業及び分野を越えて広がり続ける中で、SBOM に関する期待値をすりあわせる重要性は、今後さらに高まっていく。

適用範囲

本書に示す最小要素は、オープンソースソフトウェア、AI ソフトウェア及び SaaS を含む、すべてのソフトウェアに関する SBOM に適用される。AI 又は SaaS のようなより複雑なソフトウェア・システムの透明性を確保するためには追加要素が必要となる場合があるが、SBOM にはなお最小要素を含めるべきである。特定の種類のソフトウェアに対して必要となり得る追加要素については、本書の対象範囲外である。
最小要素は新たな要求事項を作り出すものではなく、組織がどのように SBOM を生成し、及び求めるべきかをより細かく整理するものである。データ管理、保存に関する運用及び正確な符号化の仕様は本書の対象範囲外である。

SBOM最小要素

SBOM 最小要素は、技術面及び機能的動作の両方を捉えることで、進化し続けるソフトウェア透明性への取組を支援するものである。今後、ソフトウェア・サプライチェーンにおける透明性確保の能力は向上し、将来的な取組では、より詳細な情報及び技術進展が取り込まれていく。2021 年版 SBOM 最小要素に対する更新の変更履歴は、附属書 B に示す。最小要素は、以下の基礎的な期待事項を定めている。:
データフィールド：SBOM 文書を構成するデータ。
プラクティスとプロセス：組織が SBOM データをどのように取り扱い、文書化するか。

[2] CISA, "BOD 26-02: Mitigating the Risk from End-of-Support Edge Devices," 2026 年 2 月 5 日。 https://www.cisa.gov/news-events/directives/bod-26-02-mitigating-risk-end-support-edge-devices.

各**「データフィールド」**要素は、SBOM データフォーマット（データ形式）における個々のデータフィールドに直接対応している必要はない。また、実装上の一つのデータフィールドによって、複数の最小要素を満たすことができる。例えば、コンポーネント名とバージョンを組み合せたデータフィールドは、「コンポーネント名」及び「コンポーネント・バージョン」の要素を満たし得る。SBOM データフォーマットでは、異なるフィールド名が使用される場合もある。
「**プラクティスとプロセス**」要素は、ソフトウェア・ライフサイクル全体にわたる SBOM 運用を導くための原則を示している。SBOM の実装、すなわちデータがどのように生成、共有、分析、またその他の用途に利用されるかは、SBOM ユースケースが多岐にわたることもあり、大きく異なっている[3]。例えば、SBOM は、一つの大きな SBOM 文書の中で各サブコンポーネントに必要なデータを列挙することによりソフトウェア・サブコンポーネントを識別する場合もあれば、サブコンポーネントごとに別個の SBOM へリンクする場合もある。いずれの方法も、「カバレッジ」要素において定義されるソフトウェア・サプライチェーン可視性の基礎的な期待事項を満たし得る。

データフィールド

SBOM の中核となるのは、ソフトウェアを構成するコンポーネントを理解するために用いられる情報を、一貫した統一的構造で把握し、提示することにある。データフィールド要素は、対象コンポーネント（SBOM が生成される対象のコンポーネント）及び SBOM 文書に列挙される全てのサブコンポーネントに関する基礎的情報を記述する。これらの要素の目的は、コンポーネント及びそのサブコンポーネントを十分に識別可能とすることにある。識別情報は、ソフトウェア・サプライチェーン追跡のための組織的リスク管理実務及び、脆弱性データベース、変更管理データベース又はライセンス・データベース等の他の情報源との対応付けを支援する。多くのコンポーネント及びサブコンポーネントにまたがり、異なる文脈で類似のデータが示される場合もあるが、明確性及び識別性を確保するため、SBOM 作成主体は、情報が重複または冗長となる場合であっても、記載することが望ましい。
データフィールド要素には二つの区分がある。SBOM メタデータとコンポーネント・データである。SBOM メタデータ要素は SBOM 文書自体に関する情報を記録する。コンポーネント・データ要素は、対象コンポーネント及び SBOM 文書に列挙された全てのサブコンポーネントに関する情報を記録する。

SBOMメタデータ

SBOM メタデータ要素は、SBOM 文書自体に関する情報を記録する。このデータは SBOM 管理を支援し、SBOM 分析ツールは、これらのデータフィールドを活用することにより、SBOM データの利便性を向上させることができる。

[3] 具体例については、OWASP Foundation「Authoritative Guide to SBOM」（2025 年 10 月 21 日）https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-SBOM-en.pdf 及び Open Source Security Foundation「Improving Risk Management Decisions with SBOM Data」（2025 年 9 月 18 日）https://openssf.org/wp-content/uploads/2025/09/Improving_Risk_Management_Decisions_with_SBOM_Data.pdf. を参照のこと。

SBOM作成主体（主な更新）

定義：対象コンポーネントに関する SBOM データを作成する主体の名称。
「SBOM 作成主体」要素には、対象コンポーネントについて SBOM を生成した主体を識別する文字列を記載する。本要素は、SBOM 生成に用いられたツールそのものではなく、そのツールを運用して SBOM を生成した主体を記録するものである。この項目には正式名称を用いるべきであり、略語は用いるべきではない（ただし、作成主体の正式名称に略語が含まれている場合を除く）。
「SBOM 作成主体」要素は、「コンポーネント提供主体」要素とは区別される。後者は対象コンポーネントを作成した主体を識別するものである。対象コンポーネントを作成した主体と、その SBOM を生成した主体が同一である場合には、「SBOM 作成主体」と「コンポーネント提供主体」の内容は一致し得る。対象コンポーネントを作成していない主体が当該対象コンポーネントの SBOM を生成する場合には、両者の内容は異なることになる。

SBOM作成主体の署名（新設）

定義：「SBOM 作成主体」に紐づけられたデジタル署名。
「SBOM 作成主体の署名」要素は、署名者が当該情報に署名したこと、及び署名生成後に当該情報が改変されていないことを保証するものである。[4] デジタル署名には、関連当局による規則又は勧告に従い、安全な利用が承認された署名アルゴリズムを用いるべきである。例えば、米国国立標準技術研究所（NIST）のデジタル署名標準（DSS）、国際標準化機構／国際電気標準会議（ISO/IEC）14888-4:2024、又は欧州連合サイバーセキュリティ機関（ENISA）の Agreed Cryptographic Mechanisms 等が該当する。

SBOMデータフォーマット名（新設）

定義：SBOM データの表現に用いられるフォーマットの名称。
「SBOM データフォーマット名」要素は、SBOM を生成及び利用に用いられるフォーマットを識別するものである。SBOM フォーマットに関する情報については、「機械処理可能なデータ」を参照されたい。

SBOMデータフォーマットバージョン（新設）

定義：SBOM データフォーマットにより定められた、当該フォーマットのバージョンを指定する識別子。
「SBOM データフォーマットバージョン」要素は、「SBOM データフォーマット名」要素で示されたフォーマットのバージョンを識別するものである。フォーマットを維持管理する組織により非推奨と宣言されたバージョンは、使用すべきではない。

SBOM生成コンテキスト（新設）

定義：「SBOM 作成主体」が SBOM を生成した時点における、ソフトウェア・ライフサイクル上の相対的な段階及び利用可能なデータ。

---

[4] 米国国立標準技術研究所「Digital Signatures」参照。
https://csrc.nist.gov/Projects/Digital-Signatures

「SBOM 生成コンテキスト」要素は、SBOM に記録されたコンポーネント・データに関する情報を伝えるものである。コンポーネント・データは、SBOM が生成されたソフトウェア・ライフサイクルの段階によって異なり得る。「ビルド前」、「ビルド時」及び「ビルド後」といった一般的なライフサイクルの区分、又はより具体的な識別子によって、この要素を満たし得る。[5] 例えば、ソースコードから生成された SBOM は「ビルド前」として識別でき、バイナリ解析ツールによって生成された SBOM は「ビルド後」と識別できる。

SBOMタイムスタンプ（軽微な更新）

定義：SBOM データの最新更新日時の記録。

「SBOM タイムスタンプ」要素は、「SBOM 作成主体」が手作業又はソフトウェア・ツールによって最後に SBOM データを変更した時点を識別するものである。SBOM の各バージョンにはそれぞれ新たなタイムスタンプが付与される。本項目の内容は RFC 9557 に準拠すべきである。[6]

SBOMツール名（新設）

定義：「SBOM 作成主体」が SBOM の生成又は修正に用いたツールの名称。

「SBOM ツール名」要素には、「SBOM 作成主体」が SBOM 生成のために用いたソフトウェア・ツールを識別する文字列を記載する。本項目の入力には正式名称を用いるべきであり、略語は用いるべきではない（ただし、ツールの正式名称に略語が含まれている場合を除く）。

SBOMツールのバージョン（新設）

定義：「SBOM ツール名」要素で識別されたツールのバージョンを示す識別子。

「SBOM ツールのバージョン」要素は、ツールのバージョンを記録し、組織が特定のコード提供物を識別できるようにするものである。バージョン識別子が存在しない場合には、「SBOM 作成主体」は当該情報が不明であることを示すべきである。

[5] ここでいう「ビルド」とは、ソースコードを実行可能にするためのコンパイル、インタプリテーションその他の処理を指す。

[6] Ujjwal Sharma and Carsten Bormann, "Date and Time on the Internet: Timestamps with Additional Information," RFC 9557, 2024 年 4 月。https://www.rfc-editor.org/info/rfc9557

SBOMバージョン（新設）

定義：「SBOM 作成主体」が、以前に識別されたバージョンからの SBOM 文書の変更を特定し、又は初版であることを示すために付与する識別子。

「SBOM バージョン」要素は、以前の SBOM との関係を示し、「SBOM 作成主体」が以前のバージョンに変更を加えたことを示すものである。SBOM バージョンとは、コンポーネント名及びコンポーネント・バージョンの各組合せに対応する SBOM のバージョンである。SBOM バージョン要素では、セマンティック・バージョニングを用いることができる。[7] セマンティック・バージョニングを用いる場合、本最小要素に従って公表される SBOM のメジャー・バージョンは「1」とすべきである。[8]「SBOM 作成主体」は、SBOM 要素の内容変更に応じて、適切にマイナー・バージョン及びパッチ・バージョンを使用すべきである。シリアル番号のような識別子を用いて SBOM のバージョンを区別する場合には、その識別子の使用は関連規格（例えば、一意の識別子に関する RFC 9562）に準拠すべきである。[9]「SBOM 作成主体」は、特定のコンポーネント名／バージョンの組に関する対象コンポーネントのデータを編集した場合、その SBOM のバージョンを更新すべきである。

コンポーネント・データ

コンポーネント・データ要素は、対象コンポーネント（SBOM が生成されるコンポーネント）及び列挙されたすべてのサブコンポーネントに関する情報を記録する。このデータを分析することで、コンポーネント及びその関係性に関する情報が得られ、対象コンポーネントに関するより適切なリスク管理上の判断が可能となる。

コンポーネント提供主体（主な更新）

定義：コンポーネントを作成、定義、識別する主体の名称。

「コンポーネント提供主体」要素には、対象コンポーネントを作成または開発した主体を識別するための、人が読める形式の文字列を記載する。[10]「コンポーネント提供主体」要素は、ソフトウェア・セキュリティ上の懸念事項に関する連絡先を特定することに利用できる。特定のコンポーネントについて、「コンポーネント提供主体」として識別される組織は一つのみとすべきである。この運用により、異なる「コンポーネント提供主体」によって作成された同名のコンポーネントを区別しやすくなる。本項目の入力には正式名称を用いるべきであり、略語は用いるべきではない（ただし、「コンポーネント提供主体」の正式名称に略語が含まれている場合を除く。）。

---

[7] Tom Preston-Werner, "Semantic Versioning 2.0.0" 参照。https://semver.org/spec/v2.0.0.html

[8] 次のマイナー・バージョン番号は 1.1、次のメジャー・バージョン番号は 2 となる。

[9] K. Davis, B. Peabody, and P. Leach, "Universally Unique IDentifiers (UUIDs)," RFC 9562, 2024 年 5 月。https://www.rfc-editor.org/info/rfc9562

[10]「提供主体」という用語は、欧州連合（EU）においてソフトウェアの「製造者」を指す専門用語と混同すべきではない。すべての製造者は提供主体であるが、すべての 提供主体が製造者であるとは限らない。European Union, "Regulation (EU) 2024/2847 of the European Parliament and of the Council, Article 3," Official Journal of the European Union, 2024 年 10 月 23 日。https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847#enc_1

オープンソースソフトウェア・プロジェクトについても、「コンポーネント提供主体」フィールドは重要である。命名方式は、当該プロジェクトがどのようにパッケージ及びファイルを開発、配布、保守しているかによって異なり得る。一部のエコシステムでは、パッケージ・マネージャを通じて「コンポーネント提供主体」の命名規則が提供されている。それ以外の場合、「SBOM 作成主体」は、利用可能であれば元のプロジェクト又は保守組織を用いるべきである。「コンポーネント提供主体」を明確に示す情報がない場合、「SBOM 作成主体」は、そのコンポーネントの来歴が不明であることを明示し、追跡可能性が欠如していることを示すべきである。
「コンポーネント提供主体」要素は、2021 年版 SBOM 最小要素における「供給者名」要素を置き換えるものである。「供給者名」は、特にソフトウェアの配布者に関して、実務上曖昧であることが判明している。「コンポーネント提供主体」への変更により曖昧さは軽減されるが、ソフトウェアを作成する主体を識別するための合意手法が確立されるまでは、一定の曖昧さは残るであろう。

コンポーネント依存関係（軽微な更新）

定義：一方のコンポーネントが他方の動作に必要となる場合における、二つのコンポーネント間の関係。
「コンポーネント依存関係」要素は、あるコンポーネントが別のコンポーネントを含んでいることを表す。この情報は、対象コンポーネントとそのサブコンポーネントの一つとの関係を特定し、依存関係グラフを構築する機能を支援する。[11] SBOM データフォーマットでは、これらのサブコンポーネントに関する情報を、対象コンポーネントの SBOM 内に組み込まれた SBOM 要素として表現できる。また、SBOM 文書には、対象コンポーネントの各依存関係について個別の SBOM 文書へのリンクを含めることもできる。

コンポーネントのハッシュ値（新設）

定義：実行可能なコンポーネント成果物に暗号学的ハッシュ・アルゴリズムを適用して生成される出力値。
「コンポーネントのハッシュ値」要素には、実行可能なコンポーネント成果物を暗号学的ハッシュ・アルゴリズムに入力した結果として得られる、ASCII 形式の 16 進数表現によるハッシュ値を記載する。[12]「SBOM 作成主体」が当該実行可能成果物にアクセスできない場合には、「SBOM 作成主体」はその値が不明であることを示すべきである。

コンポーネントのハッシュ・アルゴリズム（新設）

定義：ソフトウェア・コンポーネントの「コンポーネントのハッシュ値」を計算するために用いた暗号学的アルゴリズム。

---

[11] 他のプロジェクトを利用する場合の望ましい実務は、内部フォークを作成し、名称を付け、必要に応じて編集し、当該ローカル・フォークに対して include 又は import 機能を用いることである。機能コードを他のプロジェクトからコピー＆ペーストするような持続可能性の低い実務に従う場合、コピーされたコードは実質的には依存関係であり、フォーク及び依存関係として追跡した方が望ましい。SBOM 作成主体は、借用したコードを、ローカル・フォークであるかのように命名することにより、包含依存関係として記録し得る。この方法で借用コードを追跡することにより、脆弱性管理が改善される。

[12] もしそのフォーマットが代替の形式やエンコーディングを許容する場合、それらの選択肢は機械処理が可能で、かつ自動化できる方法で提供されるべきである。

「コンポーネントのハッシュ・アルゴリズム」要素は、対象コンポーネントの完全性を検証できるようにするため、「コンポーネントのハッシュ値」を生成したアルゴリズムを記録するものである。「SBOM 作成主体」は、インターネット割当番号機関（IANA）の Hash Function Textual Names を用いてアルゴリズムを識別すべきである。当該アルゴリズムは、NIST 等の関連当局により承認されたものであるべきである。[13]

コンポーネント識別子（主な更新）

定義：コンポーネントを識別し、又は関連データベースの検索キーとして機能する識別子。

「コンポーネント識別子」要素には、対象コンポーネントに関連付けられたソフトウェア識別子を少なくとも一つ含める。[14] 機械処理可能で一意なソフトウェア識別子は、自動化された分析を可能とする。本項目では、共通プラットフォーム一覧（CPE）[15] 及び Package-URL（PURL）[16] のような一般的なソフトウェア識別子を用いるべきである。本項目には、UUID、組織固有の識別子、コミットハッシュ、OmniBOR[17] や Software Hash Identifier（SWHID）[18] のような内在的識別子を含めることもできる。複数のソフトウェア識別子が存在する場合、「SBOM 作成主体」はそれらすべてを含めるべきである。

コンポーネント・ライセンス（新設）

定義：当該ソフトウェア・コンポーネントが利用可能なライセンスを示す識別子。

「コンポーネント・ライセンス」要素は、当該ソフトウェア・コンポーネントが利用可能なライセンスの識別子を把握するものである。その識別子は、SBOM データを受領した組織が、ライセンスの完全な内容を確認できるものであるべきである。可能な場合には、「SBOM 作成主体」は、この情報を、System Package Data eXchange（SPDX）のライセンス識別子[19]を用いる等、機械処理可能な形で提供すべきである。 識別子が利用できない場合には、URL 等の別の手段によりライセンスの完全な情報がどこで参照できるかを示すべきである。また、本項目には独自ライセンス条件の存在に関する情報も含めるべきである。「SBOM 作成主体」がライセンス情報を把握していない場合には、情報が不明であることを示すべきである。

---

[13] 米国国立標準技術研究所「Hash Functions」参照。https://csrc.nist.gov/projects/hash-functions

[14] CISA, "Software Identification Ecosystem Option Analysis," 2023 年 10 月 26 日。https://www.cisa.gov/resources-tools/resources/software-identification-ecosystem-option-analysis

[15] 米国国立標準技術研究所「CPE: Common Platform Enumeration」参照。https://nvd.nist.gov/products/cpe

[16] Ecma International, "ECMA-427: Package-URL (PURL) Specification," 2025 年 12 月。https://ecma-international.org/publications-and-standards/standards/ecma-427/

[17] OmniBOR, "OmniBOR Specification v0.1" 参照。https://omnibor.io/spec/v0.1/

[18] SWHID, "The SWHID Specification Version 1.2"; ISO/IEC 18670:2025 参照。https://www.swhid.org/specification/v1.2/; 国際標準化機構（ISO）, "ISO/IEC 18670:2025," 2025 年 4 月。https://www.iso.org/standard/89985.html

[19] SPDX, "SPDX License List" 参照。https://spdx.org/licenses/

コンポーネント名（軽微な更新）

定義：「コンポーネント提供主体」がソフトウェア・コンポーネントに付与した名称。

「コンポーネント名」要素は、ソフトウェア・コンポーネントを人が読める形で識別するものである。コンポーネント名は「コンポーネント提供主体」によって決定される。本項目は、「コンポーネント識別子」項目とは区別される。「コンポーネント名」要素を実装するフォーマットは、別名を記録できるよう複数のエントリを許容すべきである。本項目の入力には正式名称を用いるべきであり、略語は用いるべきではない（ただし、そのコンポーネントの正式名称に略語が含まれている場合を除く。）。

コンポーネント・バージョン（主な更新）

定義：「コンポーネント提供主体」が、以前に識別された版からのソフトウェア・コンポーネントの変更を、又は初版であることを示すために用いる識別子。

「コンポーネント・バージョン」要素は、対象コンポーネントのバージョンを把握し、組織が特定のコード提供物を識別できるようにする。「コンポーネント提供主体」がバージョンを提供していない場合には、「SBOM 作成主体」は当該情報が不明であることを示すべきである。

プラクティスとプロセス

SBOM は、構造化されたデータの集合以上のものである。組織が SBOM データをどのように取り扱い、文書化するか、すなわち SBOM のプラクティス及びプロセスは、データそのものと同様に重要である。SBOM の提出を求め、又は提供するためのいかなる方針、契約又は取り決めにおいても、組織はこれらの要素を明示的に扱うべきである。これらの要素の一部、例えば頻度は、比較的明快である。他方、アクセスのように、既存のアプローチ及び新しい概念の両方に基づく複数の実務を伴うものもある。

SBOMデータ更新への対応（主な更新）

組織は、修正を含めた SBOM データの更新に対応できるようにすべきである。SBOM 作成主体は、誤りを速やかに修正すべきである。組織は、SBOM 作成主体の実務や不適切なツールの選定などに起因する誤りを、組織のリスク管理上の意思決定（判断）において考慮する場合がある。

カバレッジ（主な更新）

SBOM には、推移的依存関係を含め、対象ソフトウェアを構成するすべてのコンポーネントに関する情報を含めるべきである。依存関係の深度に最低限の基準は定められていない。ソフトウェア・コンポーネントの複数の実体があり、かつメタデータに差異がある場合には、それぞれの実体を適切な依存関係とともに個別に記載すべきである。SBOM にはコード以外のファイルを含めない場合もあるが、設定ファイル等のセキュリティ上重要なファイルを含めることもできる。SBOM は、受領者のリスクベースの判断を容易にするため、コンポーネントの包括的な一覧を提供すべきである。例えば、脆弱性管理の観点では、SBOM 受領者は、SBOM に当該脆弱性に関連するコンポーネントが記載されていない場合は、新たに報告された脆弱性の影響を受けないと判断できるべきである。サブコンポーネント又は依存関係に対して生成された SBOM 等、他の SBOM 文書へのリンクは、受領者がリンク先のすべての SBOM にアクセス可能であることを条件として、「カバレッジ」要素の要件を満たす上で有効である。

配布及び提供（軽微な更新）

SBOM は、それを必要とする者に対して速やかに利用可能であるべきである。アクセス制御によって、権限のない者との SBOM データ共有を制限することはよいが、権限を有する者同士の情報共有を妨げてはならず、また、組織が SBOM データを信頼できるセキュリティ・ツールに統合することを制限してはならない。SBOM データの共有方法は複数存在する。例えば、SBOM をインストール時に同梱することができる。あるいは、バージョン固有の URL、データベースに対するアプリケーション・プログラミング・インターフェース（API）、又は公開リポジトリを通じて SBOM を利用可能とすることもできる。そのようなソフトウェア・サービス又は提供形態は、いずれも提供者のセキュリティ・ポリシーに従って運用されるべきである。

不明情報の明示（主な更新）

いずれかのデータフィールドに必要な情報が提供されていない場合、SBOM 作成主体は、その情報が SBOM 作成主体にとって不明であるのか、又は SBOM から意図的に秘匿しているのかを明示的に記載すべきである。不明情報を明示することにより、SBOM 受領者は、対象ソフトウェア及び SBOM 作成主体の双方について有用な情報を得ることができる。SBOM 作成主体は、秘匿されたセキュリティ関連情報について受領者が照会できるプロセスを備えるべきである。SBOM 作成主体が重要なコンポーネント・データを提供しない場合、組織は当該 SBOM を不完全であると判断し得る。

頻度（軽微な更新）

各ソフトウェア・バージョン又は更新には、対応する SBOM が存在すべきである。コンポーネント提供主体が新たなビルド又はリリースを行う場合、当該主体（又は SBOM 作成主体）もまた、変更を反映する新たな SBOM を生成すべきである。これには、更新されたコンポーネント又は依存関係を統合したソフトウェア・ビルドも含まれる。コンポーネント提供主体（又は SBOM 作成主体）が、基盤となるコンポーネントについて新たな詳細情報を把握した場合、又は既存の SBOM データの誤りを修正した場合には、改訂版 SBOM を発行すべきである。

機械処理可能なデータ（主な更新）

特に組織境界をまたぐ場合、ソフトウェア・コンポーネント・データを大規模に管理するには自動化への対応が極めて重要である。SBOM 実装は、データ量の多さ、多様なユースケース及び SBOM に関連する多種多様なツールに対応して自動化を支援できるよう相互互換性を有すべきである。現在、ソフトウェア・エコシステムの関係者が SBOM を生成し、利用するために広く使用しているフォーマットは、SPDX [20]ならびに CycloneDX [21]である。
これらのフォーマットは、いずれもオープンかつ国際的なプロセスを経て作成されており、機械処理可能であると同時に、人が読める形式でもある。
自動化に必要な最低限の対応とは、広く利用され、オープンソースであり、既存のフォーマットと互換性を有するすべてのフォーマットをサポートすることである。対象となるフォーマットは、定期的に再評価されるべきである。ある形式が広範に互換性を欠き、維持されなくなり、又は SBOM ユースケースに対して有効でなくなった場合には、その形式は使用すべきではない。このアプローチにより、将来の進化及び拡張性を支援しつつ、既存ツールの利用によって導入を容易にするという目標を達成できる。
コンポーネント提供主体又は SBOM 作成主体は、組織、業界又は分野に固有の事情に応じて、好ましい SBOM データフォーマットを選択できる。組織は、広く用いられ、相互運用可能であり、かつ機械処理可能な SBOM 形式であれば受け入れるべきである。ただし、SBOM の利用及び管理ツールとの互換性を維持するため、組織は新規ソフトウェアについて、いずれの形式であっても非推奨[22]バージョン で生成された SBOM を受け入れることは避けるべきである。

考察

SBOM 及び SBOM ツールが発展を続ける中で、更なる検討及び追加的な指針策定が望まれる主要分野として、クラウド・ソフトウェア（SaaS を含む）、AI ソフトウェア、検証並びにセキュリティアドバイザリとの関連付けの四つが挙げられる。クラウド及び AI ソフトウェアについては、追加の SBOM 要素が必要となる可能性がある。検証及びセキュリティアドバイザリとの関連付けは、すべての SBOM にとって価値ある機会となる一方、課題も伴う。これらの論点は、継続した模索が進められている今後の検討課題である。

---

[20] SPDX, "The System Package Data Exchange"; ISO/IEC 5962:2021 https://spdx.dev/; 国際標準化機構（ISO）, "ISO/IEC 5962:2021," 2021 年 8 月 参照。https://www.iso.org/standard/81870.html
[21] CycloneDX,「CycloneDX」, https://cyclonedx.org/ ; Ecma International,「ECMA-424: CycloneDX Bill of Materials Specification」, 2025 年 12 月, https://ecma-international.org/publications-and-standards/standards/ecma-424/ 参照。
[22] 非推奨のバージョン又は機能は、将来削除される可能性がある又は互換性確保の目的のみに維持される場合があるため、使用は避けるべきである。MDN Web Docs「Browser Compatibility Data Project」参照：https://github.com/mdn/browser-compat-data/blob/main/schemas/compat-data-schema.md#status-information。

クラウド環境におけるサービスとしてのソフトウェア（SaaS）のためのSBOM

SaaS 提供主体と SaaS 運用主体との間でリスク低減に関する責任が共有されていること、及び SaaS が高頻度で変化することにより、オンプレミス・ソフトウェア向けの SBOM モデルを SaaS に適用することは複雑となる。SaaS 提供主体と運用主体は、双方がシステムの運用及び保護に関与する。この責任共有により、一部の SBOM ユースケースは適用が難しくなる。SaaS における SBOM 提供の頻度についても、更なる仕様化が必要となる可能性がある。クラウド・ソフトウェア及び現代的な開発実務の性質上、ソフトウェアには高頻度の変更が生じる。このような高い頻度で SBOM を提供し受領することは、SaaS 提供主体及び SaaS 運用主体の双方に過度な負担を与える可能性がある。もっとも、SaaS システムにおいてコンテナへデプロイされるソフトウェアは通常きわめて精密に指定されるため、当該課題は一定程度緩和し得る。さらに、API のような配布メカニズムは、スナップショットを取得することにより、継続的インテグレーション／継続的デリバリ（CI/CD）プロセスにおける急速なコード変更に対応可能となる。こうした課題は存在するが、クラウド及び SaaS のユースケースにおいても、SBOM が提供する通常のソフトウェア透明性上の利点は維持される。SaaS／クラウド・ソフトウェア向け SBOM に必要となる追加要素の可能性を含め、更なる仕様化については、今後の検討が必要になる。

AIソフトウェア・システムのためのSBOM

AI ソフトウェア・システムは、クラウド及び SaaS 環境と同様に、本最小要素では捉えられない追加的な構成要素を含むことがある。AI がソフトウェア・システムにますます組み込まれ、さらに重要インフラにおいて役割を果たす可能性がある中で、組織は、関連リスクを適切に管理するため、システム構成要素の可視性を維持し、かつ向上させるべきである。AI はソフトウェアであるため、最小要素は、組織が把握すべき多くの構成要素を明らかにする一方で、それに加えて有用なサプライチェーン・データが存在する可能性もあり、例えば、AI エンジニアの間で「モデルカード」や「データカード」として呼ばれるものに含まれる情報などが挙げられる。[23] しかし、本書は AI システム用 SBOM に関する追加要素は扱わない。

[23] G7 サイバーセキュリティ・ワーキンググループの共同ガイダンス「Software Bill of Materials (SBOM) for Artificial Intelligence – Minimum Elements」（CISA および G7 の国際パートナーが作成）を参照）Software Bill of Materials (SBOM) for Artificial Intelligence – Minimum Elements

検証

SBOM は、他のセキュリティ・データと同様に、異なるレベルの信頼性が求められることがある。SBOM を受領する組織は、SBOM データの出所を検証し、その完全性を確認できるかを重視する場合がある。「SBOM 作成主体の署名」要素は、受領者が、SBOM 作成主体により作成されたとおりの SBOM を受け取っていることを確認できるようにするための情報を含めるためのものである。この要素の実装には、既存のソフトウェア署名基盤、ツール及び鍵管理を用いるべきである。[24]

受領した SBOM が作成された SBOM と同一であることの保証に加え、組織は、SBOM データの正確性、カバレッジ及び完全性を確認しようとする場合がある。これらのプロセスに基づく特性は、単なる署名とは異なる品質評価及び保証の水準があり、SBOM 最小要素の対象範囲外である。これらの品質評価について、組織は、SBOM に記載されていないコンポーネントの検出に、オープンソース・ソフトウェア・リポジトリ又はバイナリ解析ツール等の情報源を用いることがある。

SBOM とセキュリティアドバイザリの関連付け

Vulnerability Exploitability eXchange（VEX）[25] 及び Common Security Advisory Framework（CSAF）[26] 文書のようなセキュリティアドバイザリは、関連するソフトウェア・コンポーネントに関する追加的なセキュリティ情報を提供する。セキュリティアドバイザリは、ソフトウェア・コンポーネントの脆弱性ステータス（脆弱性による影響や対応状況についての情報）を伝える。コンポーネント提供主体は、セキュリティアドバイザリを用いて、自らのソフトウェア・コンポーネントの一つに脆弱性が存在し、修正対応を進めていること（又はその他適切な脆弱性ステータスの情報）を下流利用者又は顧客に通知することができる。脆弱性ステータス情報の更新は、セキュリティ上の問題を明らかにするだけでなく、信頼できる情報源において潜在的リスクは実際のリスクに直結しないと判断されている場合に、不必要な対応を回避することにも資する。

このセキュリティ情報は、特に脆弱性管理において大きな効果を有する。新たな脆弱性情報を得た際、組織は、自らの SBOM に脆弱なコンポーネントが含まれているか、又は参照されているかを評価できるため、SBOM を持たない組織と比較して対応時間を大幅に短縮できる。VEX や CSAF のようなセキュリティアドバイザリは、リスクのあるソフトウェア・コンポーネントの範囲を絞り込むことにより、脆弱性管理プロセスの効率をさらに高めることができる。

---

[24] 例えば、米国国立標準技術研究所による「NIST 特別刊行物 800-57 第 1 部 改訂 5：鍵管理に関する勧告、第 1 部—一般」（2020 年 5 月、https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final）を参照。

[25] OpenVEX,「OpenVEX 仕様」, https://github.com/openvex/spec/blob/main/OPENVEX-SPEC.md.

[26] OASIS,「共通セキュリティアドバイザリフレームワーク文書」, https://oasis-open.github.io/csaf-documentation/.

結論

新たなユースケースが出現し、技術が進化するにつれて、SBOM 最小要素もまた、ソフトウェア・コンポーネントに対する透明性を継続して提供するために進化すべきである。SBOM それ自体は、ソフトウェア・コンポーネントに関するデータにすぎない。SBOM の分析によって、そのデータは関連リスクに関する洞察へと変換される。組織は、その洞察を用いて、自らのソフトウェア・システムに関するセキュリティ上の意思決定を行うことができる。SBOM を取り込み、データを分析し、他のデータ源と対応付けることができる脆弱性管理ツールにより、組織は SBOM に基づくデータ、知見及びアクションを活用できるようになる。

本文書の作成機関は、SBOM コミュニティ及びソフトウェア・エコシステム全体の関係者と連携しつつ、SBOM 導入及び実装の推進並びに精緻化において重要な役割を果たしている。SBOM コミュニティの各構成員の経験及び専門知見は、SBOM 導入及び実装上の課題を明らかにし、業界横断で教訓を共有し、SBOM の技術的側面を洗練するうえで極めて重要であった。本文書の作成機関は、今後もサイバーセキュリティ分野のリーダーとしての立場を生かし、情報共有を促進するとともに、コミュニティ全体の専門家を結集して、ソフトウェア・サプライチェーン上の課題に対する解決策を特定し、推進していく。

免責事項

CISA 及び本文書の作成機関は、本書内で言及又はリンクされるいかなる商業主体、製品、企業又はサービスも、支持するものではない。サービスマーク、商標、製造業者名その他の方法によって特定の商業主体、製品、プロセス又はサービスに言及している場合であっても、それは CISA 及び作成機関による承認、推奨又は優遇を構成又は示唆するものではない。

本書「ソフトウェア部品表（SBOM）の最小要素」は一般的な性質のものであり、コンプライアンス、規制対応、または法的目的に関する助言を提供することを意図するものではなく、またそれらを構成するものでもない。本書の内容は変更される可能性があり、必ずしも最新のガイダンス又は技術情報を反映するものではない。本書の読者は、それぞれの個別の状況に応じた助言を得るため、各自のアドバイザー及び専門分野の専門家に相談すべきである。

謝辞

CISA 及び本文書の作成機関は、本ドラフト文書に対して意見及びコメントを提供したすべての関係者に謝意を表する。

この文書の作成には、欧州委員会通信ネットワーク・コンテンツ・技術総局（DG CONNECT）が貢献した。[27]

[27] 本文書は EU 法を解釈するものではなく、また、EU 法の実施に関するガイダンスとして意図されたものでもない。本文書は欧州委員会を拘束するものではない。通信ネットワーク・コンテンツ・技術総局（DG CONNECT）は、サイバーセキュリティに関する共通原則について協力し、それを強調する目的で、本文書の起草に貢献した。しかし、本文書は多国間の協力のもとで作成された文書であるため、その内容のすべてが EU 法を反映しているわけではない。EU 法の適用対象となる主体は、本書を情報提供のみを目的とした資料として利用することができる。

参考文献

CycloneDX. "CycloneDX." https://cyclonedx.org/.

Davis, K., B. Peabody, and P. Leach. "Universally Unique IDentifiers (UUIDs)." RFC 9562, May 2024. https://www.rfc-editor.org/info/rfc9562.

Ecma International. "ECMA-424: CycloneDX Bill of Materials Specification." December 2025. https://ecma-international.org/publications-and-standards/standards/ecma-424/.

Ecma International. "ECMA-427: Package-URL (PURL) Specification." December 2025. https://ecma-international.org/publications-and-standards/standards/ecma-427/.

EU. "Regulation (EU) 2024/2847 of the European Parliament and of the Council, Article 3." Official Journal of the European Union, October 23, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847&qid=1778510136341#tit_1.

IANA. "Hash Function Text Names." December 16, 2024. https://www.iana.org/assignments/hash-function-text-names/hash-function-text-names.xhtml.

ISO. "ISO/IEC 5962:2021." August 2021. https://www.iso.org/standard/81870.html

ISO. "ISO/IEC 18670:2025." April 2025. https://www.iso.org/standard/89985.html

MDN Web Docs, "Browser Compatibility Data Project." https://github.com/mdn/browser-compat-data/blob/main/schemas/compat-data-schema.md#status-information.

OASIS. "Common Security Advisory Framework Documentation." https://oasis-open.github.io/csaf-documentation/.

OmniBOR, "OmniBOR Specification v0.1." https://omnibor.io/spec/v0.1/.

OpenVEX. "OpenVEX Specification." https://github.com/openvex/spec/blob/main/OPENVEX-SPEC.md.

SPDX. "SPDX License List." https://spdx.org/licenses/.

SPDX. "The System Package Data Exchange." https://spdx.dev/.

SWHID. "The SWHID Specification Version 1.2." https://www.swhid.org/specification/v1.2/.

Tom Preston-Werner. "Semantic Versioning 2.0.0." https://semver.org/spec/v2.0.0.html.

Ujjwal Sharma and Carsten Bormann. "Date and Time on the Internet: Timestamps with Additional Information." RFC 9557, April 2024. https://www.rfc-editor.org/info/rfc9557.

U.S. CISA. "Software Identification Ecosystem Option Analysis." October 26, 2023. https://www.cisa.gov/resources-tools/resources/software-identification-ecosystem-option-analysis.

U.S. NIST. "CPE: Common Platform Enumeration." https://nvd.nist.gov/products/cpe.

U.S. NIST. "Digital Signatures." https://csrc.nist.gov/Projects/Digital-Signatures.

U.S. NIST. "Hash Functions." https://csrc.nist.gov/projects/hash-functions.

附属書 A：最小要素データフィールド一覧表

最小要素のデータフィールドについては、表 1 を参照のこと。

表 1. 最小要素データフィールド

データフィールド	定義
コンポーネント依存関係	一方のコンポーネントが他方の動作に必要となる場合における、二つのコンポーネント間の関係。
コンポーネントのハッシュ・アルゴリズム	コンポーネントのハッシュ値を計算するために用いた暗号学的アルゴリズム。
コンポーネントのハッシュ値	実行可能なコンポーネント成果物に暗号学的ハッシュ・アルゴリズムを適用して生成される出力値。
コンポーネント識別子	コンポーネントを識別し、又は関連データベースの検索キーとして機能する識別子。
コンポーネント・ライセンス	当該ソフトウェア・コンポーネントが利用可能なライセンスを示す識別子。
コンポーネント名	コンポーネント提供主体がソフトウェア・コンポーネントに付与した名称。
コンポーネント提供主体	コンポーネントを作成、定義、識別する主体の名称。
コンポーネント・バージョン	コンポーネント提供主体が、以前に識別されたバージョンからのソフトウェア・コンポーネントの変更を特定し、又は初版であることを示すために用いる識別子。
SBOM 作成主体	対象コンポーネントに関する SBOM データを作成する主体の名称。
SBOM 作成主体の署名	SBOM 作成主体に紐づけられたデジタル署名。
SBOM データフォーマット名	SBOM データの表現に用いられるフォーマットの名称。
SBOM データフォーマットバージョン	SBOM データフォーマットにより定められた、当該フォーマットのバージョンを指定する識別子。
SBOM 生成コンテキスト	SBOM 作成主体が SBOM を生成した時点における、ソフトウェア・ライフサイクル上の相対的な段階及び利用可能なデータ。
SBOM タイムスタンプ	SBOM データの最新更新日時の記録。
SBOM ツール名	SBOM 作成主体が SBOM の生成又は修正に用いたツールの名称。
SBOM ツールのバージョン	SBOM ツール名要素で識別されたツールのバージョンを示す識別子。
SBOM バージョン	SBOM 作成主体が、以前に識別されたバージョンからの SBOM 文書の変更を特定し、又は初版であることを示すために付与する識別子。

附属書B：2021年版からの最小要素変更点の要約

本書と 2021 年版 NTIA SBOM 最小要素との間の変更点は以下の通りである。実装に重大な影響を与える変更について記載している。記載対象となる変更の例としては、項目名（例えば「サプライヤー名」）が更新された場合（例えば「コンポーネント提供主体」への変更）が挙げられる。記載対象としない変更の例としては、データフィールドの説明が新しいフィールドを参照するよう更新された場合が挙げられる。ほとんどの要素には、明確化のため、要素名に「SBOM」又は「コンポーネント」という修飾語が追加されたが、これらの変更は個別には記載していない。要素はアルファベット順に記載し、2021 年版 NTIA SBOM 最小要素に含まれていた要素は、2021 年版における名称で記載している。

アクセス制御（削除）

変更点：「アクセス制御」要素を SBOM 最小要素から削除した。

説明：2021 年以降の SBOM 実務の発展により、「アクセス制御」要素は独立した要求事項としては不要となった。現在では「配布及び提供」の要素に、アクセス制御上の考慮事項がすべて含まれている。

誤りへの対応（主な更新）

変更点：「誤りへの対応」要素を「SBOM データ更新への対応」要素に置き換え、どのような SBOM データの変更に対応すべきかについて、定義を精緻化した。

説明：2021 年当時は、SBOM 採用及び実装が相対的に未成熟であったため、誤りへの対応を明示的に規定する必要があった。その後の技術進展により、SBOM データ品質は大幅に向上しており、受領者は SBOM データが正確であることを期待できるようになっている。

SBOM データ作成者（主な更新）

変更点：「SBOM データ作成者」要素を「SBOM 作成主体」要素に置き換えた。

説明：「SBOM 作成主体」という用語は SBOM 関連の議論で一般的に使われており、SBOM を生成する主体の役割をより正確に表している。

自動化サポート（主な更新）

変更点：フォーマット一覧から Software Identification（SWID）タグを削除した。「自動化サポート」要素を「機械処理可能なデータ」要素に置き換え、当該要素を「プラクティスとプロセス」に移動した。

説明：SWID タグは、存在する複数のツールで広く利用される SBOM データフォーマットではない。SBOM データフォーマット及び SBOM ツールは、機械処理可能性を重視し発展してきており、機械処理可能なデータの利用は、SBOM 実装の中核的な実務となっている。

コンポーネント依存関係（軽微な更新）

変更点：「依存関係」とは、他のコンポーネントの動作に必要なコンポーネントを指すことを明確化した。

説明：更新後の定義は、組織がソフトウェア・コンポーネントに関連するリスクを評価及び監視するために必要な最低限の情報を把握できるよう、本要素の対象範囲をより適切に定めている。

コンポーネントのハッシュ・アルゴリズム（新設）

変更点：「コンポーネントのハッシュ・アルゴリズム」要素を追加した。

説明：ハッシュ値を有用なものとするには、その生成に用いられたアルゴリズムを特定できることが重要である。

コンポーネントのハッシュ値（新設）

変更点：「コンポーネントのハッシュ値」要素を追加した。

説明：ハッシュは、ソフトウェア及びサプライチェーン・セキュリティのプロセスにおいて重要な役割を果たしている。

コンポーネント・ライセンス（新設）

変更点：「コンポーネント・ライセンス」要素を追加した。

説明：ソフトウェア・コンポーネントのライセンスは、ソフトウェア・コンポーネントのライセンスは、そのライセンス条件に従ってソフトウェアを適切に利用できるようにすることにより、著作権侵害の申立てを受けるリスクの管理を支援することができる。組織は、リスク管理計画においてソフトウェア・コンポーネントのライセンス及び再ライセンス情報を考慮すべきである。これは、誤った又は不正なライセンス情報が、当該ソフトウェアの継続利用や提供主体からのサポートを受ける能力に影響を及ぼす可能性があるためである。

コンポーネント名（軽微な更新）

変更点：複数のエントリを許容した。

説明：複数のエントリを追加することで、組織はデータを適切なソフトウェア・コンポーネントにより適切に対応付けることができる。

深度（主な更新）

変更点：「深度」要素を「カバレッジ」要素に置き換え、「カバレッジ」を、ソフトウェア・コンポーネント情報の垂直的広がりに加え、水平方向の広がりも含むものとして定義した。

説明：「深度」要素は従来、トップレベル依存関係に関するソフトウェア・コンポーネント情報のみを把握するものとして定義されていた。この定義は、情報に基づくセキュリティ判断を行うために必要な情報の深さではなく、当時のSBOM ツールの能力を反映していたものとなる。依存関係情報として求められる深さの程度を定義するのではなく、「カバレッジ」には、ソフトウェア・コンポーネント情報の水平方向及び垂直方向の広がりも含まれる。2021 年以降のSBOM ツールの発展により、このようなソフトウェア・コンポーネント情報の広がりを特定することが可能となった。

配布及び提供（軽微な更新）

変更点：「配布及び提供」要素を簡素化し、明確化した。

説明：SBOM 共有実務の発展を踏まえると、より簡潔な定義が適切である。

頻度（軽微な更新）

変更点：現行の用語を用いて要素を書き直した。

説明：本更新は「頻度」要素を明確化し、現行の用語を反映するものであるが、その意図自体は変更していない。

既知の不明点（主な更新）

変更点：「既知の不明点」要素を「不明情報の明示」要素に置き換え、既知だが意図的に秘匿された情報と、SBOM 作成主体にとって不明な情報を区別した。

説明：SBOM 実装の拡大に伴い、関係者から「既知の不明点」要素の曖昧さに対する懸念があげられていた。本書は、コンポーネントに関する不明情報の特定が、フォーマットに含まれる単一データフィールドではなく、SBOM ライフサイクル全体を通じて実施されるべき実務であることを明確にするため、要素名を更新した。SBOM 作成主体に把握されているが意図的に秘匿された情報と、SBOM 作成主体にとって不明な情報を区別することにより、本要素の実装に関する更なる明確化を図っている。

その他の識別子（主な更新）

変更点：「その他の識別子」要素を「コンポーネント識別子」要素に置き換えた。少なくとも一つの一般的なソフトウェア識別子を含めるべきであることを明記し、当該フィールドには、ユニバーサルに一意な識別子、組織固有の識別子、コミットハッシュ、およびインストリンシック識別子を含めることができる旨を規定した。

説明：ソフトウェア識別の問題に対する普遍的な解決策は未だ存在しないものの、進展は見られる。これらの変更は、ソフトウェア識別に関する議論の成熟及びソフトウェア識別子形式そのものの成熟を反映している。

SBOM 作成主体の署名（新設）

変更点：「SBOM 作成主体の署名」要素を追加した。

説明：SBOM 作成主体のデジタル署名は、SBOM データの完全性及び真正性に関する保証を提供する。

SBOM データフォーマット名（新設）

変更点：「SBOM データフォーマット名」要素を追加した。

説明：データ・スキーマ内で SBOM フォーマットを識別することにより、SBOM ツールによる SBOM データの読み込み及び分析を支援できる。

SBOM データフォーマットバージョン（新設）

変更点：「SBOM データフォーマットバージョン」要素を追加した。

説明：SBOM データフォーマットのバージョン情報は、SBOM ツールによる SBOM データの読み込み及び分析を支援できる。

SBOM 生成コンテキスト（新設）

変更点：「SBOM 生成コンテキスト」要素を追加した。

説明：SBOM に表現されたデータの出所に関する追加情報を提供する。SBOM データは、SBOM 作成主体がソフトウェア・ライフサイクルのどの段階で SBOM を生成するかにより異なり得る。この追加的なコンテキストは、組織によるソフトウェア・リスク評価に有用な情報を与える。

SBOM ツール名（新設）

変更点：「SBOM ツール名」要素を追加した。

説明：この要素の追加により、SBOM 作成主体がどのような方法で SBOM を生成したかに関する情報が提供される。

SBOM ツールのバージョン（新設）

変更点：「ツールのバージョン」要素を追加した。

説明：SBOM 生成に用いられた SBOM ツールのバージョンは、SBOM データを効率的に取り込み分析するうえで重要となり得る。

SBOM バージョン（新設）

変更点：「SBOM バージョン」要素を追加した。

説明：コンポーネントには、時間の経過とともにデータの正確性を向上させるため更新された複数の SBOM が関連付けられる場合がある。バージョン追跡は、組織による SBOM の管理及びリスク監視を支援する。

サプライヤー名（主な更新）

変更点：「サプライヤー名」要素を「コンポーネント提供主体」要素に置き換えた。さらに、不明なコンポーネント提供主体に対する代替的な指定（来歴不明である旨の表示）を規定した。

説明：「コンポーネント提供主体」は、SBOM 関連の議論で一般的に用いられる用語との整合性が高い。また、この用語は、当該フィールドがソフトウェアの作成元となった主体を指すことをより明確にする。コンポーネント提供主体が不明な場合の代替的な表示（来歴不明の表示）を設けることにより、透明性を確保するとともに、ソフトウェア・サプライチェーンにおける潜在的リスクを示すことができる。

タイムスタンプ（軽微な更新）

変更点：RFC 9557 に準拠すべきことを明確化した。

説明：RFC 9557 に準拠することで、自動化及び相互運用性をより適切に支援できる。

コンポーネントのバージョン（主な更新）

変更点：「コンポーネントのバージョン」要素を「コンポーネント・バージョン」要素に置き換え、コンポーネント提供主体がバージョンを提供していない場合には、SBOM 作成主体がそのバージョンが不明であることを示すべき旨を明記した。

説明：ソフトウェア・コンポーネント・データを特定のバージョンに関連付けることは、脆弱性管理等のプロセスにおいて重要である。ソフトウェア・コンポーネントのバージョンが不明であることを示すことにより、組織はソフトウェアの来歴に関する SBOM 作成主体の把握状況について洞察を得ることができる。