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ver2.0」の 概要について

令和6年８月29日

経済産業省　商務情報政策局

サイバーセキュリティ課

「ソフトウェア管理に向けたSBOMの導入に関する手引」の改訂概要

- セキュアなソフトウェアの流通を促進するため、経済産業省では、**ソフトウェアの部品構成表であるSBOM（Software Bill of Materials）の企業による活用を推進**。
- 2023年7月28日、企業が**SBOMを導入するメリットや実際に導入するにあたって実施すべきポイント**をまとめた手引書を「**ソフトウェア管理に向けたSBOMの導入に関する手引ver1.0**」として公表。
- 今般、中小企業も含め、あらゆる企業にとって**SBOMをより効率的に活用できる方法等を検討**し、その内容を盛り込む形で、「**導入手引」を改訂。**

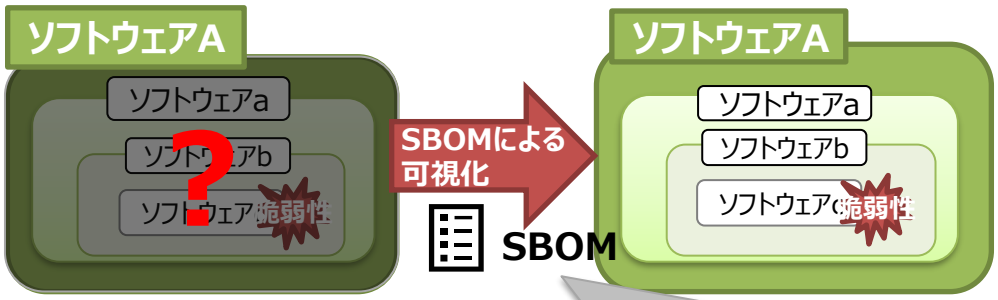
【主な改訂のポイント】

- ソフトウェアの脆弱性を管理する一連プロセスにおいてSBOMを効果的に活用するための具体的な手順と考え方をまとめた「**脆弱性管理プロセスの具体化**」
- SBOM導入の効果及びコストを勘案して実際にSBOMを導入することが妥当な範囲を検討するためのフレームワークである「**SBOM対応モデル**」
- 委託先との契約等においてSBOMに関して規定すべき事項（要求事項、責任、コスト負担、権利等）を示した「**SBOM取引モデル**」

ソフトウェア・セキュリティ確保手段としてのSBOM

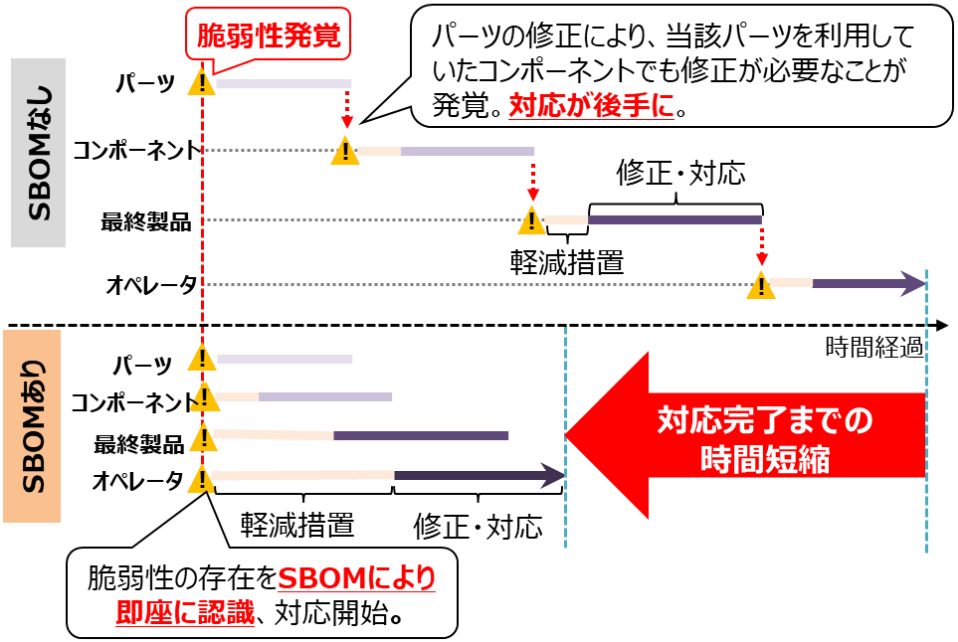
- SBOM （Software Bill of Materials）とは、**ソフトウェアの部品構成表**のこと。ソフトウェアを構成する**各部品（コンポーネント）を誰が作り、何が含まれ、どのような構成となっているか**等を示す。
- SBOMによりソフトウェアの構成情報を詳細に把握することができるため、脆弱性情報の即時の特定が可能であり、**脆弱性対応などへの活用が期待**できる一方、その作成効果やコストなどの課題が存在するため、実証による検証を実施。
- 2023年7月、**「ソフトウェア管理に向けたSBOMの導入手引ver1.0」を公表**。SBOMに関する基本的な情報や導入に向けた実施事項のポイントを示す。

＜SBOMイメージ＞



サプライヤ名	コンポーネント名	バージョン	製品URLなど	…
A会社	ソフトウェアA	Ver1.0	……	…
A会社	|…ソフトウェアa	Ver2.1	……	…
B会社	|…ソフトウェアb	Ver5.3	……	…
C会社	|…ソフトウェアc	Ver1.2	……	…

SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮



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　～全体概要～

手引の背景・目的

- ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェアの利用が一般化する中で、ソフトウェアにおける脆弱性管理やライセンス管理の重要性が高まっている。ソフトウェア管理の一手法として、Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目を集めている。
- 複数の産業分野における実証を通じ、SBOM活用の効果が確認できた。一方、SBOM導入・活用に際しては様々な課題(例：脆弱性管理の効率化、分野や用途に応じたSBOMの適切な範囲、ソフトウェアの調達者と供給者の立場間の取り決め）が存在することが明らかとなった。
- 本手引では、**SBOMに関する「基本的な情報」や「誤解と事実」を提供し、**企業のSBOM導入を支援するために、**SBOM導入に向けた主な実施事項及び認識しておくべきポイント**を示す。(ver1.0)
- 加えて、ソフトウェアの脆弱性を管理する一連プロセスにおいて**SBOMを効果的に活用するための具体的な手順と考え方**、SBOM導入の効果及びコストを勘案して**SBOMを導入することが妥当な範囲を検討するためのフレームワーク**、ソフトウェアの受発注において、**調達者と供給者の間でSBOMに関して契約に規定すべき事項（要求事項、責任、コスト負担、権利等）について参考例**を示す。(ver2.0)

対象読者

- 主にパッケージソフトウェアや組込みソフトウェアに関する **ソフトウェアサプライヤー**
  - ✓ ソフトウェア開発・設計部門
  - ✓ 製品セキュリティ担当部門（PSIRTなど）
  - ✓ 経営層
  - ✓ 法務・知財部門

SBOM導入の主なメリット

- **脆弱性管理のメリット**
  - ✓ 脆弱性残留リスクの低減
  - ✓ 脆弱性対応期間の低減
  - ✓ 脆弱性管理にかかるコストの低減
- **ライセンス管理のメリット**
  - ✓ ライセンス違反リスクの低減
  - ✓ ライセンス管理にかかるコストの低減
- **開発生産性向上のメリット**
  - ✓ 開発遅延の防止
  - ✓ 開発にかかるコストの低減
  - ✓ 開発期間の短縮

SBOM導入に向けたプロセス(ver1.0)

フェーズ1	環境構築・体制整備	● 1-1. SBOM適用範囲の明確化 ● 1-2. SBOMツールの選定 ● 1-3. SBOMツールの導入・設定 ● 1-4. SBOMツールに関する学習
フェーズ2	SBOM作成・共有	● 2-1. コンポーネントの解析 ● 2-2. SBOMの作成 ● 2-3. SBOMの共有
フェーズ3	SBOM運用・管理	● 3-1. SBOMに基づく脆弱性管理、ライセンス管理等の実施 ● 3-2. SBOM情報の管理

脆弱性管理プロセスの具体化(ver2.0)

- SBOMを活用することで、ソフトウェアの脆弱性管理を通じた脆弱性リスクの低減が効果として見込まれていることから、**SBOMを活用するプロセスの中でも、脆弱性管理に関するフェーズが特に重要**。
- 脆弱性管理の一連プロセスにおいてSBOMを効果的に活用するための**具体的手順と考え方をまとめることで、SBOM活用による効果を高めるための参考情報**を提供。

SBOMを活用した脆弱性管理プロセス

フェーズ1　脆弱性特定
- マッチング手法区分選択
- 利用可能なSBOMデータ特定
- 脆弱性DBの選択
- マッチング手法の選択・作成

フェーズ2　脆弱性対応優先度付
- 予備フィルタリング
- 優先度付情報の選択・取得
- 判断ツリーに基づくカテゴリ判定
- 優先度スコア評価

フェーズ3　情報共有
- 共有情報と共有相手の特定
- 共有方法の特定と実施

フェーズ4　脆弱性対応
- 脆弱性の暫定対応
- 脆弱性の根本対応

SBOM対応モデル(ver2.0)

- SBOM導入の効果及びコストを勘案してSBOMを導入することが**妥当な範囲を検討するためのフレームワーク(5W1Hを網羅するよう体系化)**。
- 実証を通じて、**医療機器、自動車、ソフトウェア製品等の分野**において、コスト・効果を考慮して妥当な対応範囲の参考例を提示。
- 当該フレームワークを用いることで、高度な管理を行えるソフトウェア、すなわちセキュアなソフトウェアが市場に適切に評価され、その流通が促進されることが期待できる。

SBOM取引モデル(ver2.0)

- ソフトウェア部品の受発注において、調達者と供給者の間でSBOMに関して**契約に規定すべき事項（要求事項、責任、コスト負担、権利等）**について参考となる例を示す。
- 既存のソフトウェアに関するモデル契約書と組合せることで、**SBOMに対応した契約書を作成する際の項目案を提示**するもの。

参考資料

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　～全体概要～

ver1.0の内容

手引の背景・目的

- ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が一般化する中で、ソフトウェアにおける脆弱性管理やライセンス管理の重要性が高まっている。
- ソフトウェア管理の一手法として、Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目を集めている。
- 複数の産業分野における実証を通じ、SBOMを活用することで効率的なソフトウェア管理を実施できることが確認できた一方で、実際のSBOM導入に際しては様々なハードルが存在することが明らかとなった。
- 本手引では、**SBOMに関する基本的な情報やSBOMに関する誤解と事実を提供**するとともに、企業のSBOM導入を支援するために、**SBOM導入に向けた主な実施事項及び導入にあたって認識しておくべきポイント**を示す。

対象読者

- 主に、パッケージソフトウェアや組込みソフトウェアに関するソフトウェアサプライヤー※
  - ✓ ソフトウェア開発・設計部門
  - ✓ 製品セキュリティ担当部門（PSIRTなど）
  - ✓ 経営層
  - ✓ 法務・知財部門

※ このうち、以下に示すようなSBOM初級者を特に対象としている。

- ソフトウェアにおける脆弱性管理に課題を抱えている組織
- SBOMという用語は聞いたことがあるが具体的な内容やメリットは把握できていない組織
- SBOMの必要性は理解しているが、導入に向けた取組内容が認識できていない組織　など

SBOM導入の主なメリット

- **脆弱性管理のメリット**
  - ✓ 脆弱性残留リスクの低減
  - ✓ 脆弱性対応期間の低減
  - ✓ 脆弱性管理にかかるコストの低減
- **ライセンス管理のメリット**
  - ✓ ライセンス違反リスクの低減
  - ✓ ライセンス管理にかかるコストの低減
- **開発生産性向上のメリット**
  - ✓ 開発遅延の防止
  - ✓ 開発にかかるコストの低減
  - ✓ 開発期間の短縮

SBOM導入に向けたプロセス

フェーズ1　環境構築・体制整備フェーズ

- **1-1. SBOM適用範囲の明確化**
  - ✓ SBOMを作成する対象ソフトウェアに関する情報（言語、開発ツール、構成図、契約形態・取引慣行、規制要求事項、SBOM導入に関する組織内の制約等）を整理する。
  - ✓ 整理した情報を踏まえて、SBOM適用範囲を明確化する。
- **1-2. SBOMツールの選定**
  - ✓ SBOMツールの選定の観点を整理し、当該観点に基づきSBOMツールを評価・選定する。
    （選定観点の例：機能、性能、解析可能な情報・データ形式、コスト、対応フォーマット、解析方法、サポート体制、他ツールとの連携、ユーザーインタフェース、対応する言語、日本語対応等）
- **1-3. SBOMツールの導入・設定**
  - ✓ SBOMツールが導入可能な環境の要件を確認し、整備する。
  - ✓ 取扱説明書等を確認して、SBOMツールの導入・設定を行う。
- **1-4. SBOMツールに関する学習**
  - ✓ 取扱説明書等を確認して、SBOMツールの使い方を習得する。
  - ✓ ツールの使い方に関するノウハウや各機能の概要は記録し、組織内で共有する。

フェーズ2　SBOM作成・共有フェーズ

- **2-1. コンポーネントの解析**
  - ✓ SBOMツールを用いて対象ソフトウェアのスキャンを行い、コンポーネントの情報を解析するとともに、コンポーネントの解析結果について、コンポーネントの誤検出や検出漏れが無いかを確認する。
  - ✓ SBOMツールを用いることで、手動の場合と比較して効率的にコンポーネントの解析及びSBOMの作成を行うことができる。
  - ✓ パッケージマネージャーを用いることで、SBOMツールでは特定できない粒度の細かいコンポーネントを特定できる場合がある。
- **2-2. SBOMの作成**
  - ✓ 作成するSBOMの項目、フォーマット、出力ファイル形式等のSBOMに関する要件を決定し、当該要件を満足するSBOMを作成する。
- **2-3. SBOMの共有**
  - ✓ 対象ソフトウェアの利用者及びサプライヤーに対するSBOMの共有方法を検討した上で、当該方法に基づきSBOMを共有する。

フェーズ3　SBOM運用・管理フェーズ

- **3-1. SBOMに基づく脆弱性管理、ライセンス管理等の実施**
  - ✓ 脆弱性に関するSBOMツールの出力結果を踏まえ、深刻度の評価、影響度の評価、脆弱性の修正、残存リスクの確認、関係機関への情報提供等の脆弱性対応を行う。
  - ✓ ライセンスに関するSBOMツールの出力結果を踏まえ、OSSのライセンス違反が発生していないかを確認する。
- **3-2. SBOM情報の管理**
  - ✓ SBOMに含まれる情報やSBOM自体を適切に管理する。
    ※ SBOMの管理は、組織内のPSIRTに相当する部門が対応することが効果的
  - ✓ 自動で脆弱性情報が更新・通知されるSBOMツールを用いることで、新たな脆弱性に関する情報を即座に把握することができる。ツールを用いた自動管理ができない場合、担当者を別途設置するなど運用面でカバーする。

ver2.0追加内容

脆弱性管理プロセスの具体化

背景・目的

- SBOMを活用した脆弱性管理の方法と手順についてプロセスに基づく具体例を示す。
- SBOMを活用した脆弱性管理においては、**現状では未解決の課題**が存在し、それらの課題を十分に解決するためには、新たな**技術開発、標準化、ツール環境整備**などが必要になる。
- 本章では、それらの課題も含めて、SBOM利用者側の運用によって課題を回避するための考え方や現状で可能なベストプラクティスについて示す。

主な課題と解決アプローチ・ノウハウ等

課題	解決アプローチ・ノウハウ
部品IDが併存し、脆弱性DBとの突合に障害	Purl2cpeなどID変換ツールの利用やAPIを用いたID部分照合
多様な脆弱性DBの網羅性の確保	リスクとコストの低減効果に基づく脆弱性DBの選択方法の提示
脆弱性対応の優先付けによる迅速対応と効率化	SSVCをベースとした判断ツリーによる優先付けカテゴリ判定法の提示
サプライチェーンを通じた情報共有と役割分担	情報共有のステップと開発者・ユーザによる実施項目の提示
脆弱性対応の役割分担	暫定対応・本格対応における開発者・ユーザによる実施項目の提示

SBOMを活用した脆弱性管理プロセス（概要）

フェーズ1 脆弱性特定

1. **マッチング手法区分の選択**
   組織の目的、技術力、利用環境に応じて、SBOM既成ツール、APIスクリプト利用、WebUIの３手法から選択する。
2. **利用可能なSBOMデータの特定**
   サプライヤーからのSBOM提供、ツールを用いたSBOM作成など、利用可能なSBOMデータを特定する。
3. **脆弱性DBの選択**
   脆弱性情報のカバレッジ拡大、自動化・効率化、優先付けの精度向上など、リスク低減、コスト低減などの目的に応じて重要度の高いDBを選択する。
4. **マッチング手法の選択・作成**
   以上の選択肢を総合して、脆弱性特定手法を決定する。

フェーズ2 脆弱性対応優先付け

1. **予備的フィルタリング**
   外部情報を活用した優先付けの前に、既知の情報から対応が必要な脆弱性情報を絞り込む。
2. **優先付け情報の選択・取得**
   リスクの構成要素に基づき、インシデントの有無、Exploitコードの流通状況、CVSS、VEX情報など自社のポリシーに従い必要な情報を選択・取得する。
3. **判断ツリーに基づくカテゴリ判定**
   SSVCに基づき整理した判断ツリーに従い、（開発者、ユーザ組織）×（技術力の高・低）応じて優先付けカテゴリ判定を行う。
4. **優先度スコア評価**
   1から３のステップと並行して、必要に応じて、必要に応じて定量的なスコアリングによりカテゴリ内の優先付けを行うことで詳細な優先付けを行う。

フェーズ3 情報共有

1. **共有情報と共有相手の特定**
   ・共有情報の特定：脆弱性情報、負荷情報、優先付け判定結果など共有情報を特定する。
   ・共有相手の特定：社会組織、社外（ユーザ、ベンダー、サプライヤー―）などの共有相手、順序を特定する。
   ・共有認知・トリガー：プッシュ型、プル型など共有のトリガーを特定する。
2. **共有方法の特定と実施**
   ・共有方法の特定：ファイル送受信、SaaSなど共有方法を特定。
   ・アクセス権限の特定：機密性に応じて、非公開、開示範囲、権限などを特定。
   ・共有実施：決定した共有方法、アクセス権限に基づき共有を行う。

フェーズ4 脆弱性対応

1. **脆弱性暫定対応**
   ・暫定策の検討：利用中断、縮退、回避策など暫定策の検討
   ・暫定策の適用：決定した暫定策について、ステークホルダーに周知し適用する。
2. **脆弱性根本対応**
   ・根本対応の実施：脆弱性に関わるソフトウェアの開発者を特定し、開発者が脆弱性を修正する
   ・SBOM/VEX更新：脆弱性修正に伴い、SBOM、VEX情報を更新する。
   ・SBOM/VEXの共有：供給先に更新したSBOM/VEXを提供し、必要に応じてSBOM履歴管理を行う。

ver2.0追加内容

SBOM対応モデルの概要

SBOM対応モデルの構成要素

- SBOMの作成・活用に関する選択肢について、コストと効果への影響の大きい項目について5W1Hを網羅するように体系化。実証および有識者委員会の意見を反映してSBOM対応項目を整理。
- 実証を通じて、医療機器、自動車、ソフトウェア製品等の分野において、コスト・効果を考慮して妥当な対応範囲の参考例を提示

SBOM対応項目の選択肢

	適用区分	主な適用項目（選択肢）	コスト	主な実施内容とコスト要素
生成・共有	(a)SBOM作成主体 (Who)	(a1)自社	小	自社開発で直接利用する部品を構成ファイルなどから特定し、SBOMを生成する。コード改変部品を含む。
		(a2)サプライヤ（開発委託先）取引契約あり	中	取引契約のある開発委託先のソフトウェアで利用する部品のSBOMを生成する。
		(a3)サプライヤ（サードパーティ）取引契約なし	大	取引契約によるSBOMの要件化できないOSSや既成部品ベンダーがSBOMを作成する。(b2)(c2)
	(b)部品範囲 (What, Where)	(b1)直接利用部品※1	小	開発者が直接利用する部品を構成ファイルなどから特定し、ツールなどでSBOMを生成する。
		(b2)間接利用部品※2	大	サードパーティ部品について、再帰的に利用される部品に対してSBOMを生成する。
	(c)生成手段(精査) (How)	(c1)手動で特定（構成管理情報利用）・ツールで生成	小	直接利用する部品情報を構成ファイルなどを用いて作成する。
		(c2)ツールで特定・生成・誤検知精査なし	中	ツールを用いてSBOMを生成し、精査は省略する。ツールの利用は再帰部品のSBOM生成を主に想定するため商用ツールの利用を想定する。
		(c3)ツールで特定・生成・誤検知精査あり	大	商用ツールを用いてSBOMを生成し、ソースコードレビューを行い、誤検知、検出漏れの精査を行う。（再帰利用部品を含む）
		(c4)開発委託元が、開発委託先の作成したSBOMを独立に検査	大	開発委託元が、開発委託先の作成したSBOMを受け入れる際に、ツールなどで独立してSBOMを作成するなどして信頼性を検査する。
	(c')生成手段（部品検出手法）	依存関係解析	中	パッケージマネージャ等の構成情報を静的に解析する。
		ファイル照合	中	ハッシュ値当を用いてソースコードのファイル単位の一致を検出する。 OSSのライブラリの検出なども含む。
		スニペット解析	大	ソースコードの部分的な文字列一致や類似性により検出する。
		バイナリ解析	大	バイナリファイルのビットパターンなどをもと類似性を検出する。
		実行形式内部の再帰的な依存解析	大	実行形式内にリンク済みのライブラリについて、そのライブラリをビルドする際の依存解析を再帰的に行う。
		上記に対応しない。	小	予め認識している部品をSBOMに変換する。
	(c'')生成手段（対象ソフト種別）	開発時に確定する部品	小	スタティックライブラリ、アプリケーション
		実行時に確定する部品	中	ランタイムライブラリ、サービス（ローカル、外部クラウド）、OS、ミドルウェア、実行環境（コンテナ、VM、APサーバ）
		周辺ツール環境	大	開発運用で使用するツール（インストーラ、アップデータ、配布パッケージ、開発環境、ツールチェーン、SBOMツール）
	(d)データ様式・項目 (What)	(d1)標準フォーマット（SPDX、CycloneDX、SPDX Lite等）	中	SPDXなどの標準フォーマットで作成する。
		(d2)大統領令におけるデータフィールドの最小要素を含む	中	大統領令におけるデータフィールドの最小要素を含むSBOMを作成する。
		(d3)上記を満たさない要素	小	独自の最小限の要素を作成する。
活用	(e)活用範囲 (Why)	(e1)脆弱性の特定	小	NVD, JVN等のDBを対象として脆弱性の検索・特定を行う。
		(e2)脆弱性の深刻度評価	中	CVSS値をベースとした深刻度を評価し、脆弱性対応の優先度を設定する。
		(e3)脆弱性の悪用可能性等の評価と対処	中	VEX情報等を用いて悪用可能性、脆弱性対処の必要性を評価する。必要に応じて対処策等のアドバイザリを発行する。
		(e4)ライセンス特定	中	ライセンスの特定と規約の取得を行う。
	(f)活用主体 (Who)	(f1)製品利用者	小	脆弱性が特定された場合、利用を中断し、ベンダーによる修正を待つ。業務中断コストも考慮すれば損害は大きい。
		(f2)最終製品ベンダー	中	利用者に脆弱性を通知するとともに、開発者への修正依頼、修正後のビルド・利用者への提供を行う。必要に応じて当局、ISAC等に報告する。
		(f3)各部品の開発者	大	開発者は、脆弱性の監視と修正を行い、調達者に修正版を提供する。必要に応じて当局、ISAC等に報告する。

ver2.0追加内容

SBOM取引モデルの概要

SBOM取引モデルの主な構成要素（契約で規定することが期待される事項）

- 契約で規定すべき事項として、SBOMに関する要求事項、責任、コスト負担、権利などの区分で整理される。業界の取引慣行、タスクフォース意見を網羅するように整理。脆弱性管理、ソフトウェア品質保証に重要な要件を言語化。主に要件定義後の請負契約が対象と想定。

凡例：基礎 分野共通で最低限期待される事項／発展 特定分野、要求レベルの高い分野で期待される事項

区分		規定すべき事項	レベル
SBOM要求事項	フォーマット・標準	**（SBOMフォーマット）※1** 採用するSBOM標準フォーマットについて規定する。（SPDX, CycloneDX, SWID等の標準とバージョンを規定）	基礎
		（ID標準）※1 採用する部品ID標準を規定する。（CPE, PURL, SWD, 独自形式等）	基礎
		（SBOM最小要素）※1 採用するSBOMフォーマットの要素項目のうち最小要素を規定する。NTIAのSBOM最小要素を参考にする。	基礎
	品質・信頼性 （SBOM対応モデルに該当）	**（対象サプライヤ契約形態）** SBOM作成範囲として、委託開発契約、サードパーティ利用規約（商用既製品、OSS）の契約形態による範囲を規定する。	基礎
		（再帰的利用部品）※1 SBOM作成範囲として、直接利用部品か再帰的な間接利用部品までとするか規定する。	発展
		（構成解析手法の適用範囲）※1 間接利用部品について、部品を特定する際に利用する構成解析手法の適用範囲を規定する。（依存関係解析、ファイル照合、スニペット解析等）	発展
		（部品精査の要否）※1 ツールによる部品特定の結果に対して、手動による誤検知・検出漏れの精査の要否を規定する。	発展
		（部品の対象フェーズ）※1 部品情報の範囲としてビルド時、ランタイム、クラウドサービス等の範囲を規定する。	発展
		（サードパーティ部品の事前合意） サードパーティ部品（商用部品、OSS）を利用する場合、事前の申告と合意の要否について規定する。	基礎
	保守・運用	**（共有方法）※1** SBOMファイルによる授受またはSaaS等によるリアルタイム共有について規定する。	基礎
		（VEX対応）※1 SBOMに関連する脆弱性情報について悪用可能性に基づくVEX情報の提供を行うか規定する。	発展
		（SBOM更新）※1 ソフトウェアのアップデート、SBOM不具合修正等に応じて、SBOMを更新する期限や頻度を規定する。	基礎
		（脆弱性監視・通知） ソフトウェアの運用フェーズにおいて、脆弱性を監視し、脆弱性が発見された場合に、調達者に通知の期限を規定する。	発展
		（脆弱性対応・優先付け）※1 脆弱性が発見された際に、脆弱性対応の要否、優先付け（トリアージ）について調達者に情報提供を行うか規定する。	発展
		（EOL・EOS） サードパーティ部品および委託開発部品のEOL、EOSやその期限変更に対する通知について規定する。	発展
責任と保証		**（エビデンス提出）** SBOM要求事項について適合していることを証明するエビデンス、第三者証明の提出の要否について規定する。	発展
		（契約不適合責任） SBOM要求事項に対する不適合が見つかった場合には、SBOM修正等の瑕疵対応の要否について規定する。	基礎
		（損害賠償）※2 SBOM要求事項の不適合が原因で事故が発生した場合、損害賠償額上限等について規定する。ライセンス違反の損害賠償を含む。	基礎
		（免責） SBOM要求事項への適合性エビデンスを提出している場合について、技術的制約（ツールの誤検知など）に帰する理由で、損害が発生した場合について損害賠償の制限、免責について規定する。	発展
コスト負担		**（見積）※2** SBOM要求事項、責任・保証に基づき見積の作成し、その合意金額に基づき対価支払について規定する。	基礎
権利・機密保持		**（知的財産権の帰属）** 作成したSBOMの知的財産権、使用権の帰属、第三者への提供可否について規定する。	発展
		（機密保持） SBOMの機密保持・管理およびSBOMを用いたリバースエンジニアリングの禁止について規定する。	発展

※1　発注仕様書に記載することも想定される。
※2　ソフトウェア開発一般の請負契約と共通化することが想定される。