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（案）に寄せられた御意見及び御意見に対する考え方

No.	提出者			該当箇所	御意見	御意見に対する考え方
	提出者番号	枝番	組織・個人			
1	1	1	-	5.3	意見1: 改ざん防止の観点が無い --- SBOMファイルの中身を改ざんされては本末転倒なため、改ざん防止も考えなければならない。使える技術としてはデジタル署名とブロックチェーン（分散台帳）がある。 ただし、内容としては高度であるため、手引に含めていいかどうかはわからない。 参考1: CISAのレポート。洗練度:高として「分散台帳の活用」を挙げている。 https://www.cisa.gov/resources-tools/resources/software-bill-materials-sbom-sharing-lifecycle-report 参考2: CNCFのSoftware Supply Chain解説。デジタル署名を用いた改ざん防止の仕組みも挙げている。 https://github.com/cncf/tag-security/tree/main/supply-chain-security	御意見を踏まえ、5.3節の記載について、SBOMを共有する場合の留意事項としてSBOMの改ざん防止に留意する必要があることを追記いたします。
2	1	2	-	2.3	意見2: 手作業でつくれるSPDX-Liteへの逃避を防ぐべきではないか --- 大前提として、SBOMの生成は機械的に完結できるべきである。手作業の介在はミスや過失、SBOMの提供や更新の鈍化に繋がる。人が絡むのは、生成したSBOMのレビューと（意見1でも書いたが）改ざん防止のための署名作業程度が理想であろう。 手作業だと、怠惰や保身などから「脆弱性が多そうなコンポーネントX」を「意図的に」リストから外す、といったことも容易に行えてしまう。そしてSBOMのリストは数百もの長大サイズになることも多く、「心理的にも面倒くさく感じる」。このようなことは十分起こり得ると考える。 SPDX-Lite は、IT後進的な組織にとっては至極魅力に移るはずだが、だからといってその逃避を許してしまえば手作業品質が待っている。警笛を鳴らしておきたいところではある。	御意見を踏まえ、2.3節のSPDX-Liteに関する記載について、SPDX-LiteフォーマットのSBOMを手作業で管理する場合、自動管理の場合と比較して管理工数がかかることを追記いたします。なお、SPDX-Liteは、SPDXのサブセットとしている国際標準にも含まれているほか、将来的にSBOMの自動処理を検討している組織における第一歩として採用される可能性もあるところ、明確にSPDX-Liteの利用を否定することはせず、その他の記載については原案のとおりとさせていただきます。
3	1	3	-	2.5	意見3: 誤解としていくつか追加したい --- 以下の誤解も追加するべきと考える。 > 誤解「SBOMはソフトウェアのBOMであるため、対象はソフトウェアのみである」 いいえ。 ソフトウェアの他にシステムもある。たとえば本番稼働している「Windows Server 2022」にインストールされたソフトウェア達、社内開発環境として使っている AWS EC2 インスタンス「Amazon Linux 2023」にインストールされたソフトウェア達など。出典を明示することはできないが、大手SIerはすでに「システム」のBOMを管理するための仕組みを持っているはずである。もっと言えば、会社によって全く異なった独自の管理方法になっていると考える。 ちなみに、SBOMの主要3フォーマットには、システムを扱うポテンシャルはない（たとえば「サーバー1台」を表す概念がない）。 > 誤解「SBOMとはSPDX、CycloneDX、SWIDのことである。独自フォーマットのリストはSBOMではない」 いいえ。 独自フォーマットでも良い。ただし最小要素など要件は満たしたものであることが望ましい。そういう意味では、無理にSPDXなどの既存フォーマットを使う必要はなく、独自に自製する策も考えられる。それこそ日本向けの独自フォーマットを開発するベンチャーが生まれるかもしれない。 すでにSPDX-Liteが開発されているように、日本は（単にIT後進的であるという点もあるが）独自の事情と文化を抱えたガラパゴスな国である。だからこそ、既存フォーマットだけでなく、自らに合ったものを創造するという発想も重宝するのではないか。	御意見を踏まえ、2.5節のSBOMに関する誤解と事実を修正いたします。

4	1	4	-		意見4: SBOMファイル解読の解説があっても良いかもしれない --- SBOMファイル（jsonファイル）そのものを解読することも、場合によっては必要であろう。そのための導入も解説しておくと優しいかもしれない。 具体的には、まず各種フォーマットの仕様の場所（たとえばSPDXの場合は https://spdx.dev/specifications/ となる）を明示することと、jsonファイルを解析する手段（jqコマンドが知られている）の二点。	御意見を踏まえ、7.3.3項の記載について、代表的な各種フォーマットの仕様が記載されているWebページを明示するとともに、各形式の解読に関する参考情報を追記いたします。
5	2	1	個人		ソフトウェアタスクフォースで議論したとあるが、他の資料と異なり、タスクフォース参加者が記載されていない。これは不誠実である。改善願う。	ソフトウェアタスクフォース（サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース）の委員名簿等につきましては、下記URLにおいて公開されております。 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/softw
6	2	2	個人	4.1	開発言語においてVISUALBASICがないのは何故か。この列挙方法だと列挙されていない言語で開発すればSBOMは不要といらぬ誤解を与えてしまう。逆に言語ごとに必要な理由を逐条明記するほうが望ましい。（たとえ膨大になっても）	お寄せいただいた御意見は、4.1節の記載内容の修正に当たって参考にさせていただきます。
7	2	3	個人	9	「食品表示は食品製造後に変更されることはほとんどない」との文言は違和感あり。農林水産省に確認したのか。思いつく限りでも温度帯変更や保存帯変更、保存方法変更など食品表示が変わる要素はある。また、食品表示は原産地表示の手法もあるし、原産地表示だと頻繁に変更されるので、本文脈で言わんとしたいことは理解するももう少し限定条件を付すよう改善願う。	お寄せいただいた御意見を参考に、2.1節のコラムにおける食品表示に関する記載を修正いたします。
8	3	1	-		昨今のソフトウェア管理に関してはさまざまな技術やコミュニティが出てきている。どのような技術やオープンソース・コミュニティを使うかによって、(運用のコストなどの観点から)望ましいサプライチェーン管理のシステムは変わってくる。画一的なフォーマットに押し込めることで、イノベーションを阻害することにならないか懸念している。	御意見ありがとうございます。 イノベーションの阻害要因とならないように留意しながら引き続き検討を進めてまいります。
9	4	1	-	2	P2「国内では、経済産業省が・・・設置し」と記載されているところ、「審議会等の整理合理化に関する基本的計画」（平成11年４月27日閣議決定）別紙４（懇談会等行政運営上の会合の開催に関する指針）２．（１）において「懇談会等に関するいかなる文書においても、当該懇談会等を『設置する』等の恒常的な組織であるとの誤解を招く表現を用いないものとする。」とされていることを踏まえて、「開催し」等と修正すべきではないか。	御意見のとおり、当該箇所を修正いたします。
10	5	1	個人	1.6.本手引のサマリー	経営層への説明資料として使うことを想定しているのであれば、文章量が多く少し読みづらいと感じます。 例えば、各チェック記号の文章に対して下記のように抽象化した見出しを付けると、可読性もあがるのではないでしょうか。 ・チェック1から3をまとめて、ソフトウェアサプライチェーンの脅威 ・チェック4から7をまとめて、ソフトウェア管理手法としてのSBOMのメリット ・チェック8から9をまとめて、本手引きの活用ポイント	御意見のとおり、当該箇所を修正いたします。
11	6	1	組織	7.3.2	「7.3.2 SBOM に関するツール 」について意見を差し上げたく存じます。 OSSライセンス＆セキュリティ管理ツール「FossID」も、SBOMを作成・管理するためのツールとして、BlackDuckと並び国内で広く採用されております。 FossIDも、掲載を頂けませんでしょうか？	御意見を踏まえ、7.3.2項において、FossIDに関する記載を追加いたします。

12	7	1	個人	5.1項P41 【SBOM導入に向け認識しておくべきポイント】	【意見内容】 バイナリ解析におけるメリットを考慮せず、一概にバイナリ解析を「バイナリしか用意できない場合を除いてバイナリスキャンを補助的に用いる」ことに異議がございます。 【理由】 以下の通りバイナリ解析におけるメリットを列挙し、バイナリスキャンがたんなる補助ツールではないことの理由といたします。 メリット１：分析の完全性 バイナリ静的分析は、ソースコードの可用性に依存しない包括的な方法です。これは、ソースコードが利用できないことが多い現実のシナリオ、特にサードパーティのコンポーネントを扱う場合には非常に重要です。対照的に、依存関係ベースの分析では、既知の依存関係に関する情報しか提供できないため、未知のコンポーネントや不明瞭なコンポーネントが検出されないままになる可能性があります。 メリット２：最終製品の精度: バイナリ分析では、ソースコードだけではなく、出荷される実際の製品を検査します。最終的なバイナリには、コンパイラの最適化や追加ライブラリの組み込みなど、ビルドプロセス中に導入された変更が含まれる可能性があるため、これは有益な場合があります。これらの変更は、ソフトウェア構成を正しく表現し、実際の製品の完全な攻撃対象領域を考慮してSBOMに含める必要がありますが、残念ながらソースコードには表示されず、バイナリ分析の重要性が強調されています。 メリット３：誤検出の管理: バイナリ分析によって誤検出や欠落が発生する可能性があるのは事実ですが、依存関係ベースの分析やソースコード分析でも同じことが発生する可能性があります。エラーを完全に回避できるメソッドはありません。ただし、高度なツールとバイナリ分析アルゴリズムの継続的な開発により、誤検出の割合は大幅に減少します。 メリット４：補完的な手法: バイナリ分析を依存関係ベースまたはソースコード分析と併用することで、組織はソフトウェアのセキュリティ体制をより完全かつ正確に把握できます。 メリット５：バイナリのみ存在するケース: 組み込みシステム、レガシーシステム、または独自のソフトウェア・コンポーネントを使用する場合、通常、ソースコードは利用できません。したがって、バイナリ分析はこれらの状況において単なる補足ではなく、不可欠なツールです。 変化する状況への対応: ソフトウェアの開発と配布が進化し続けるにつれて、バイナリ解析はさらに重要になります。コンテナ化、サーバーレスコンピューティング、プリコンパイル済みライブラリの使用の台頭により、多くの場合、ソフトウェアのコンポーネントを包括的に理解するにはバイナリ分析が唯一の実行可能な方法になります。	御意見を踏まえ、5.1節におけるバイナリスキャンに関する記載を修正いたします。

13	7	2	個人	5.1項P43 1行目	【意見内容】 特定の状況やそれほど高度ではないツールではSBOMの検出精度が高くない状況が見受けられますが、それらの結果が全てマイナスな結果とも限らず、バイナリ解析の独自の利点と可能性について考慮する必要があります。 【理由】 本分析がどのようなツールを使ったものか、記載はありませんが、バイナリ分析の検出率がツールやコンテキストによって異なることは事実ですが、その検出レベルは、使用するツールの高度さに大きく依存します。 高度なバイナリ分析ツールは、高い割合のコンポーネントを検出でき、多くの場合、他の方法の検出率と同等、さらにはそれを上回ります。 これは、ソース コードがない場合でも、コンポーネントを識別する複雑なアルゴリズムとそれぞれのツールベンダごとの経験則に基づいて実現されます。 ほかに検出率「１割」が意味する理由について以下が考えられます。 最終ソフトウェアの真の表現: バイナリ分析は、出荷されて実行される実際の製品を検査します。 これは、最終製品に存在するコンポーネントが検出されることを意味しますが、依存関係リストには必ずしも表示されない可能性があります。 その結果、検出されるコンポーネントの数は少なく見えるかもしれませんが、バイナリ分析により、実際に存在する実行可能なコンポーネントが確実に検出されます。 誤検知の削減: バイナリ分析では、誤検知 (依存関係にはリストされているが実際には最終バイナリに存在しないコンポーネント、またはソースコードに存在する「デッドコード」) が報告される可能性が低いため、検出されるコンポーネントが少なくなる可能性があります。 ただし、コンパイルされたファイル内にあるとは限りません。 したがって、量は少ないように見えますが、結果の質 (つまり、実際の製品との関連性) は高くなります。 すべての手法で検出漏れが発生する可能性: バイナリ分析に限らず、どの分析方法でも検出漏れが発生する可能性があります。 たとえば、依存関係ベースの分析では、ビルドプロセス中にソフトウェアにバンドルされているが、依存関係リストで明示的に宣言されていないコンポーネントが見逃される可能性があります。 逆に、バイナリ分析では実際の最終製品を検査するため、多くの場合、これらの「隠れた」コンポーネントを検出できます。 バイナリ分析の性質: バイナリ分析は、実行可能ソフトウェアに存在するコンポーネントを検出するように設計されています。 そのため、依存関係にリストされているが最終製品には実際には存在しないコンポーネントが省略される場合や、ソースコードには存在するがコンパイルされたファイルには必ずしも存在しない「デッドコード」が省略される場合があります。 これは検出漏れのように見えるかもしれませんが、実行されるソフトウェアのより正確なイメージを提供するため、長所とも見ることができます。 ツールの品質: バイナリ分析における検出漏れの割合は、使用されるツールの品質に大きく依存します。 より高度なツールには、漏れの発生を大幅に減らす高度なアルゴリズムと技術が備わっています。 特定の場面でのバイナリ分析必要性： プリコンパイルされたライブラリ、組み込みシステム、または独自のソフトウェアを扱う場合など、バイナリ解析が唯一の利用可能なオプションである状況は数多くあります。 このような場合、バイナリ解析により検出されない可能性と、バイナリ解析がなければ見つけ出すことができない可能性を比較検討する必要があります。 補完的な役割: 最後に、バイナリ分析は単独で見るのではなく、SBOM 管理への総合的なアプローチの一部として見るべきです。 他の手法と併用すると、全体的な漏れのリスクが大幅に軽減されます。 したがって、バイナリ分析では検出漏れが発生する可能性がありますが、独自の洞察を提供し、他の分析方法を補完する、包括的なソフトウェア分析の重要なコンポーネントであることに変わりはありません。 さらに、テクノロジーが進化し、改善し続けるにつれて、誤検知率は減少すると予想されます。	御意見を踏まえ、5.1節におけるバイナリスキャンに関する記載を修正いたします。また、バイナリ解析の独自の利点と可能性について、本手引の更なる検討を進めていくに当たって参考にさせていただきます。
14	7	3	個人	7.3.2	本項記載のツール以外にもSBOMツールが存在し、特定の製品のプロモーションとも捉えられる可能性があるため、削除、もしくは全てのツールを網羅する等、再考が必要と思われます。	御意見を踏まえ、7.3.3項のツールに関する記載を修正いたします。

15	8	1	個人	―	1．手引において最も重要なポイントは「SBOMをいかに活用するか、導入によるメリットが生じるか」 手引においてはSBOMのとは何か（What）、どうやって導入するのか（How）よりもなぜ導入するのか、導入することによりどんなメリットが生じるのか（Why）を伝えることを最重要目的とするべきだと考えます。 SBOMに関する情報に溢れていますが、一般企業がSBOMを導入することによる明確なメリットがイメージし辛い状況です。言葉の上では説明してあっても、具体的な解説や指導がなく、現実のアクションや利益につなげられる方は少ないでしょう。 金銭、時間、安全、信用の何がどう良くなるのか、「具体的に」説明するべきだと考えます。そうでなければ、SBOMの導入することが目的となってしまい。社会のサイバーセキュリティを確保するという本質的な目的が達成し辛いと考えます。 私の考えるSBOM導入目的は「利用ソフトウェア情報を組織間で共有する」「利用ソフトウェア情報に基づき脆弱性監視を有効に実施する」です。 この2点の具体的なアクションを例として提示できると良いと考えます。	お寄せいただいた御意見を踏まえ、SBOM導入のメリットをより明示的に記載する等、全体構成などの見直しも含めて記載内容の修正を検討いたします。
16	8	2	個人	―	2．細部の解説を「具体的に」する （案）ではSBOMのフォーマットやツール選定に関して、おおまかな考え方を提示するに留め、組織毎、ツール毎に最適化して実行する旨が推奨されています。 しかし、一般の組織目線ではその「最適化」や細かいニュアンスが分からずに実施に踏み切れない組織が多いでしょう。 実施におけるやり方や基準を可能な限り「具体的に」例示するべきだと考えます。 例１　P.27「影響を受けるソフトウェア」の粒度が体系化されていない 誤解と事実として数行で記載されている内容だが、実務において極めて重要なポイントだと考えます。 ソフトウェア粒度といっても、とらえ方や分け方で様々なやり方がある。分け方や類型を具体的に示して業界の認識を共通化するべきです。 また、すべての粒度を再帰的にSBOM化するのは現実的ではありません。SBOM側、脆弱性情報発信側にて粒度の基準を作るべきです。 ・製品ソフトウェア -スクリプト、ツール -使用OSS -ライブラリ（静的、動的） -言語、関数 例２　P.47　「脆弱性対応を行う。」 本ページはSBOMによるメリットを享受に関する重要ポイントだと考えます。脆弱性情報に従い脆弱性対応を実施する旨が記述されています。専門家ならばこれを聞いただけで業務イメージが湧きますが、一般組織担当者はこの文言だけで行動に移れないでしょう。 より具体的に、SBOMのサンプル、どうやって、どのような頻度で監視行動を行うか、脆弱性を発見した際の対処判断のパターンなどを説明するべきです。 例３　P.49　「社外からの問合せがあった場合等に参照できるよう」 問い合わせに対し活用するのは当然ですが、組織間のSBOM共有はこれだけではありません。また、実施に際する各種判断を組織の事情に合わせて実施するニュアンスが書かれていますが、こちらも例示が必要と考えます。 SBOMを公開する理由、公開しない理由、公開する目的やきっかけを複数パターン提示し、読み手が自分に合ったケースを選択することで、どう動けばよいか理解できるようにするべきと考えます。	お寄せいただいた御意見は、手引の更なる検討を進めていくに当たって参考にさせていただきます。

17	9	1	個人	ー	◆よかった点 ・SPDXの説明の中に見方が説明されている点 ・SBOM導入メリットが明確かつ網羅的に記載されている点 ・SBOMある/なしの脆弱性対応スピードやコストの差について言及されている点 ・社内でOSSの管理プロセス(ライセンス/脆弱性管理)を検討する上で有益な情報が記載されている点(3章、4章部分) ・SBOMツールの検証項目について記載されている点	本手引に対する肯定的な御意見として承ります。
18	9	2	個人	表2-2	◆改善いただきたい点 ・表2-2 米国NTIAによるSBOMの「最小要素」の定義について、SBOMの運用方法に定めるべき項目として「既知の未知」と「誤りの許容」とありますが、イメージができなかったので、補足もしくはイメージが分かる文言への修正をお願いします。	御意見を踏まえ、「既知の未知」と「誤りの許容」に関する補足説明を追加いたします。
19	9	3	個人	表4-2	・「表4-2　SBOMツールの選定基準」について、基準ではなく観点が記載されているように見受けられるため、「選定基準」⇒「選定の観点」に修正をお願いします ※基準の例)OSS検出精度90%以上	御意見のとおり、表4-2及び関連する4.2節の記載について、修正いたします。
20	9	4	個人	7.3.2	・SBOMツールの説明として、言語で対応しているか判断できるツール（ソースコードスキャン）もあればファイルフォーマット、OSで対応しているか判断できるツール(バイナリースキャン)もあることを補足したほうがいいのではと思いました。（全てのツールが開発言語で対応している or していないを判断しているように読み取れました）	御意見を踏まえ、7.3.2項の記載について、ツールによって機能、性能、解析可能情報等が異なるため、4.2で記載しているツール選定の観点を踏まえた評価・選定が望まれることを追加いたします。
21	10	1	個人	ー	1. PDFは最低限でもしおり付きPDFで公開すべき。これによりデジタルでの可読性が向上する。できれば英国政府のようにPDFを禁止して、htmlでの公開も検討すべきでは。	手引の公開にあたっては、しおり付きのPDF形式で公開予定です。そのほかいただいた御意見は、手引の更なる検討を進めていくに当たって参考にさせていただきます。
22	10	2	個人	P.1	2. P1において「脆弱性情報と資産管理台帳を照らし合わせるだけでは、下位のコンポーネントとして利用されるOSS のようなコンポーネントにおいて脆弱性が発見された場合に、間接的な脆弱性の影響を検知することができない。」と記載されている。間違いではないですが、下位のコンポーネントにおいて脆弱性が発見された場合は、その上位のコンポーネントのベンダーが適切にその脆弱性の情報を開示することが望まれる。このように責任範囲を明確にして管理する必要がある。	お寄せいただいた御意見は、手引の更なる検討を進めていくに当たって参考にさせていただきます。
23	10	3	個人	P.10 図2-2	3. P10図 2-2 食品サプライチェーン及び食品表示の概念的イメージの図の中に記載されている製造者の住所は、製造者ではないが実在する住所なので、できれば実在しないものを記載例としたほうがいいのではないか。	御意見のとおり、当該箇所を修正いたします。
24	10	4	個人	P.31 表4-1	4. P31表４-1において、Whoにおいて、「最終製品ユーザ」などもあると、医療機器の場合はいいのではないかと思います。医療機器を使用する医療機関は、ソフトウェアユーザでもないし、ベンダーでもないため。	御意見のとおり、当該箇所を修正いたします。
25	10	5	個人	P.31 表4-1	5. P31表４-1において、SBOMの作成手段（How）において、ある部分のみ自動で、その他が手動で作成する場合も多いのではないかと思います。既製品は手動で、OSS等は自動で作成して手動で確認する。	御意見を踏まえ、当該箇所を修正いたします。
26	10	6	個人	P.31 表4-1	6. P31表４-1において、SBOM の活用範囲（Why）の脆弱性管理は、製造業者がする場合と、製品のユーザがする場合と、それらの両方がある。このため、自社を中心に書くならば、「脆弱性管理の情報のユーザへの提供」などを追加してもいいのではないか。	御意見を踏まえ、当該箇所を修正いたします。
27	10	7	個人	P.37	7.P37 表のユーザインターフェースの列で「CLI（グラフィカルユーザーインターフェース）」となっているが、ここはGではなくCなので「CLI（コマンドラインインターフェース）」の誤りではないかと思われます。	御意見のとおり、当該箇所を修正いたします。

28	10	8	個人	P.57～61	8.P57 米国NTIA Roles and Benefits for SBOM Across the Supply Chain（2019年11月）において、ハイパーリンクが表記が2行の1行目だけになってしまってリンクしても参照できない。 その他のリンクも2行にわかれているものの多くがリンクされない。	御意見を踏まえ、当該箇所を修正いたします。
29	10	9	個人	P.61	9. P61 米国CISAから最近2つのドキュメントが公開されている。これも参考文献に追加しておくと参考になると思われる。 Types of Software Bill of Materials (SBOM) https://www.cisa.gov/resources-tools/resources/types-software-bill-materials-sbom Minimum Requirements for Vulnerability Exploitability eXchange (VEX) https://www.cisa.gov/resources-tools/resources/minimum-requirements-vulnerability-exploitability-exchange-vex	御意見を踏まえ、新たにCISAから発表された文書について、7.3.1の参考文書に追加いたします。
30	11	1	組織	-	昨今の企業におけるOSSを含むソフトウェアの利用が広がっていますが、他方、セキュリティに対するソフトウェアの脆弱性が企業経営に大きな影響を及ぼし、ソフトウェアの適切な管理が必要不可欠となっています。このような状況において、御省がソフトウェア管理の一手法として、SBOMの基本的な情報や導入に向けたポイントを整理された手引を取りまとめられたことは、誠に時宜を得たものであります。本手引につきましては、特段の意見はなく、賛同致します。 本手引きにより、SBOMの導入が促進され、ソフトウェアの適正な管理が図られることを期待しております。	本手引に対する肯定的な御意見として承ります。
31	12	1	組織	-	シスコは、日本におけるSBOM（Software Bill of Materials）の導入に関する日本政府の様々な取組を歓迎する。ソフトウェア透明性に向けたSBOMなどの取組は、Cisco's Trust Principles[1]の中心となっている。シスコは、SBOMなどに関連する標準化における主導的役割を果たしており、Software Package Data Exchange （SPDX）、Common Security Advisory Framework（CSAF）、またOmniBOR等のSBOMメタデータの自動的な生成・共有・利用に向けたフォーマット・ツール・メカニズムの開発をサポートし続けている。シスコのSBOMに関する立場は米国国立標準技術研究所（NIST）への意見書[2]でも表明しているところである。 SBOM 生成をめぐる状況は、複雑で依然として早期の段階にあり、ツールセットはまだ開発中である。全てのソフトウェアのソースが信頼性があり検証可能であるわけではなく、ソフトウェアのサプライチェーンが複雑であるために複数の組織にまたがり管理範囲が生じる結果となっている。機械可読であるソフトウェアのメタデータを表現するための普遍的標準の概念が非常に新しいことによって、不完全または不正確なSBOMが生成される可能性がある。更に、生成方法が全て同じであるわけではないため、バイナリスキャニングでは、ビルド段階で生成するSBOMほど正確にはならない。 基礎的な製品であってもソフトウェアの量は膨大であるため、人間に依存するプロセスは横展開が可能であると見なしてはならず、避けるべきである。現在の SBOM プロセスが比較的非効率で成熟していないことを考慮すると、SBOM の生成にかかるコストは予想よりもはるかに高くなる傾向があり、これは、各組織がこの機能を自ら提供しようとするなかで明らかになりつつある。 SBOM のあるべき使用を巡る議論はグローバルに継続している。現時点で、産業界は、どうすればSBOMを検証可能な形で、正確で完全なものとすることができるかという問題をまだ解決できていない。更に、SBOM にリストされた第三者製ソフトウェアのコンポーネントがそれに関連する脆弱性の存在を知られている場合、このSBOM の該当ソフトウェアに脆弱性があることを示すものでは必ずしもない。SBOM と、Vulnerability Exploitability eXchange (VEX) メタデータを含む製品のメタデータを組み合わせることで、実務者はソフトウェアの脆弱性の機械可読かつ自動の分析を可能にし、脆弱なコンポーネントが脆弱な製品ということになるかどうかについての理解を確立できることになる。このような取組は、SBOM を利用可能かつ価値のあるものにするために不可欠である。 ベンダーと利用者の双方にとって、ソフトウェア環境全体にわたりSBOMとVEXの標準化、ツール開発、導入に関して、するべきことはまだ多くある。以上のような正確性と信頼性	本手引に対する肯定的な御意見として承るとともに、手引の更なる検討を進めていくに当たって参考にさせていただきます。

					が十分でないという問題を念頭に置いて、SBOM をどのように利用するか慎重なアプローチが必要である。利用者は、現在利用可能な他の多くの安全なソフトウェア開発手法、サイバーセキュリティツールの改善、リスクマネジメントの取組と比較しながら、SBOM への投資の利点を慎重に検討するべきである。 ソフトウェアを生産するベンダーが SBOMの生成を担当するべきである。ソフトウェア開発チームは、バイナリ スキャンではなく、ビルド段階でSBOMを生成する自動化技術を利用すべきである。SBOM導入の手引書（案）に提案されているように、顧客への連絡と製品の脆弱性に関する問い合わせの管理については、ベンダーの製品インシデントチームが責任を負うべきである。これらのチームは、SBOMの導入に伴い、顧客からの連絡が大幅に増加することに備える必要がある。 我々は、現在のSBOM導入の手引書（案）が日本におけるSBOM利用への重要なスタートであると考えている。そして、同案が想定する読者がどのようなステークホルダーかがより明確にされると良いと考える（例えば、内部導入を検討する利用者の経営層か、あるいはSBOMの作成者または利用者に対し、一貫性のある導入のあり方についてガイダンスを行うため、など）。 シスコは、この件に関して日本政府とさらなる議論ならびに我々の経験を共有する機会を歓迎するところである。 以上 [1] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-trust-principles.pdf [2] https://www.nist.gov/system/files/documents/noindex/2021/06/08/Cisco%20Position%20-%20NIST%20Software%20Supply%20Chain%20Security%20Call%20for%20Papers.pdf	
32	13	1	組織	2.3.(1) p16	意見内容 ：SPDX-Liteにつき、以下の観点で加筆が望ましいと考えます。 ・本規格の利用が適切な条件 例：「手作業によりライセンス情報を作成する組織において、SPDX準拠のライセンス情報が膨大で運用が困難な場合に、必要な情報のみ授受する場合を想定して設計されている。」 ※出所1 ・SPDXよりも情報項目が限定されることによる弊害と対策 例：「項目数が限定的なため、サプライチェーン内でSBOM共有を行う際に上流側企業の求める要件に合致しない可能性も有るため、利用可否判断においては取引先への確認を十分に行うことが望まれる。」 理由：SPDX-Liteにつき、限定された項目でSBOMとして成立することによる運用の簡便さの魅力を伝えるのみではなく、留意点も含めて慎重に記載するのが望ましいと考えました。そこで、本規格利用が適切な条件や、弊害と対策の加筆が望ましいと考えます。 ※出所1 https://github.com/OpenChain-Project/OpenChain-JWG/blob/master/subgroups/sbom-sg/outcomes/SPDX-Lite/Guideline/SPDX-Lite-Guideline_jp.md	御意見を踏まえ、当該箇所を修正いたします。

33	13	2	組織	4.1 p31	意見内容 ：対象ソフトウェアに関して整理する情報として、以下追記が望ましいと考えます。 「・自組織で取り扱うデータ形式：ソースコード、パッケージ、コンテナ、ファームウェア等バイナリデータ 等 ・対象ソフトウェアの動作環境：OS、CPUアーキテクチャ」 理由：自組織で取り扱うデータ形式は、SBOMツール選定時のコンポーネント解析方法の要件に影響します。例えば、組込み機器業界を中心にバイナリ納品の可能性があるため※出所2、バイナリスキャンに対応したツールが必要な場合があります。 対象SWの動作環境も選定時の要件に影響する場合があります。ファームウェア等バイナリからのコンポーネント解析に対応するSBOMツールが、解析するバイナリの動作するOS・CPUに基づく解析可否の条件を定めています※出所3。 ※出所2 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_04_00.pdf（2頁） https://www.meti.go.jp/meti_lib/report/2020FY/000727.pdf（3頁/61頁） ※出所3 https://assets.website-files.com/5edfaa63fc3fa9835200afbd/63565e5073b8d50020afdfa5_BlackBerry%20JARVIS%202.0.pdf（5頁）	御意見を踏まえ、当該箇所を修正いたします。
34	13	3	組織	表 4-2 p37	意見内容 ：ツールの選定基準として、表内に以下追記が望ましいと考えます。 「項目：解析可能なデータ形式 説明：SBOMツールは、コンポーネント解析時に読込可能なデータ形式に条件がある。ファイル形式（拡張子別の対応可否）や対応パッケージマネージャ種類、バイナリ解析時における（解析するソフトウェアの動作可能な）OS・CPUアーキテクチャ等、解析に使用するデータの形式を整理の上、ツールが読込可能か確認することが望まれる。」 理由：コンポーネント解析の際に解析対象データが読込できない旨が導入後に発覚すると、事業者の適切なSBOM運用を妨げ、ツール再選定等で多大な負担が生じる可能性があるため、ツール選定時の対応可否評価は慎重に行うべきと考えます。 この点、表4-2では「対応するソフトウェア開発言語」が言及されている一方、SBOMツールにおいては言語以外の項目にも条件があるため※出所3、当該項目の追記が望ましいと考えます。 ※出所3 https://assets.website-files.com/5edfaa63fc3fa9835200afbd/63565e5073b8d50020afdfa5_BlackBerry%20JARVIS%202.0.pdf（5頁）	御意見を踏まえ、当該箇所を修正いたします。
35	13	4	組織	表 4-2 p35	意見内容 ：表内「性能」につき、説明欄に以下追記が望ましいと考えます。 「性能の検証には、無償トライアルを利用し、実際に解析するソフトウェア・利用するSBOM等をツールに読み込ませ、正確な情報をツールが出力可能か確認することが最も有効である。その他、以下に例示する様な仕様を開発元・代理店に確認することで、上記に挙げた正確性・迅速性の期待値を把握可能である。 ・OSSデータベースの収録OSS数 ・脆弱性データベースの収録脆弱性数 ・脆弱性情報の情報元（NVD/JVN等） ・OSSデータベース・脆弱性データベースの更新頻度」 理由：性能の観点は、OSS管理、脆弱性・ライセンスリスク最小化のため重要と認識します。そこで、具体的な評価方法の例を記載する方が、本観点での選定方法を理解しやすく、事業者の適切なツール選定に繋がり適切と考えます。	御意見を踏まえ、当該箇所を修正いたします。

36	13	5	組織	表 4-2 p38	意見内容 ：表内「日本語対応」につき、説明欄に以下追記が望ましいと考えます。 「なお、日本語対応ツールを優先する場合の大前提として、OSSを正しく管理し、ライセンスリスク・脆弱性リスクを低減することがSBOMツール導入の目的であることに留意すべきである。本表の他項目で選定要件に合致しない日本語対応ツールを、日本語対応のみを理由に選定すべきかは慎重な検討が望まれる。 また、自社海外拠点や、海外提携先、外資サプライヤと共同運用する可能性がある場合、日本語対応を優先することの妥当性は慎重に検討することが望まれる。」 理由：SBOM利用の大前提として、OSSを正しく管理し、ライセンスリスク・脆弱性リスクを低減することが優先と考えます。 「日本語対応しているツールの優先度を高めることが考えられる」との記述により、事業者がツール選定時に、日本語非対応のツールを一律選外とする等、最適なツール選定を妨げると懸念されます。例えば、日本語対応ツールを選定した結果、SBOM生成機能が無いことが導入後判明し再選定を強いられた事例も弊社では把握しています。 別の観点ですが、自社海外拠点や海外提携先・外資サプライヤと共同運用する可能性がある場合、そもそも日本語対応を優先することが望ましくない場合もあります。	御意見を踏まえ、当該箇所を修正いたします。
37	13	6	組織	4.2 p38	意見内容 ：販売代理店の利用に関する記述につき、以下記述の追記が望ましいと考えます。 「ただし特定の販売代理店が、自社で取扱の無いツールについて情報を保有しているとは限らないため、複数の販売代理店に相談することが望まれる。」 理由：販売代理店があらゆるツールについて情報を有しているとは限らないと考えます。特定一社の販売代理店のみに依存すると、取扱の無いツールが検討対象にならない・十分に評価されない等で、事業者の適切なツール選定を妨げると懸念されます。そこで、複数の代理店利用につき言及することが望ましいと考えます。	御意見を踏まえ、当該箇所を修正いたします。
38	13	7	組織	4.2 p34・p38	意見内容 ：複数ツールの使い分けは非効率となる場合があるとの記載につき、貴省が想定する留意点まで言及するのが望ましく、「なお、複数のSBOM ツールの使い分けが非効率となる場合があるため、目的に対して最小限のSBOMツールを用いて運用することが望ましい。」程度の表現が望ましいと考えます。 また、以下追記も望ましいと考えます。 「ただし、自社が複数業界向けにソフトウェア開発を手掛けている、ソフトウェアサプライチェーンの複数領域を担っている等で、事業部門・開発プロジェクトによって最適なツールの基準が異なる場合も、複数ツールの使い分けが非効率かは慎重な検討が望まれる。」 理由：追記案は、弊社顧客の以下事例を受け、一概に複数SBOMツールの使い分けを非推奨とすることが妥当でない可能性を考慮し、追記を提案しております。 事例：下記理由で、部門別に最適なSBOMツールを導入予定 ・開発部門ではスニペットも含めたソースコードスキャンを重視 ・調達部門ではサプライヤ納品バイナリの高精度なスキャンを重視 ・PSIRTでは上市版ファームウェアからの脆弱性特定を重視 ・部門間で（解析対象ソフトウェアの開発進度が異なるため）SBOM共有が不要	御意見を踏まえ、当該箇所を修正いたします。

39	13	8	組織	4.2 p38	意見内容 ：「可能であれば、SBOM ツールの導入前に無償トライアル等を利用して～」の文につき、以下変更が望ましいと考えます。 ・「可能であれば、」を削除 ・「実際の使用感を体験すると良く」を、「実際の使用感を体験し、操作学習の難易度および必要期間を評価し、」に変更 また、以下追記が望ましいと考えます。 「なお、トライアル期間は数週間程度と短い場合があり、うち操作学習やトラブルシューティング等で一定期間が費やされるため、トライアル前に検証したい機能・ユースケースを整理し具体的なテスト計画を策定して実施しないと、期間内に選定に必要な情報を取得できない点に留意したい。」 理由：SBOMツールは、カタログスペックだけで評価可能な範囲が限定的なため、無償トライアルを選定時の必須作業と位置付けるべきと考えます。 例えば、誤検知・検知漏れ件数は実際にトライアルで解析を行わない限り測定困難な他、操作学習の工数・期間はカタログに掲載されること自体が稀です。学習コストや誤検知・検知漏れについては、「1.1. 背景」でもSBOM導入の課題に挙がっており、トライアルで正確な評価を行うことを解決策として推奨すべきと考えます。 この点、「可能であれば、」との記述がトライアル実施が必須ではない旨と解釈されること、操作感評価のみでは事業者の学習コスト評価が曖昧になることを懸念し、変更を提案しております。 トライアル時のテスト計画策定については、弊社で過去にテスト計画無く複数ツールのトライアル実施した際に、期間内で必要機能・ユースケース全ての検証に至らなかった経験を踏まえ追記を提案しております。	御意見を踏まえ、当該箇所を修正いたします。
40	13	9	組織	5.1 p41・ p43・p44	意見内容 ：「また、バイナリファイルを対象とした解析の場合、解析精度が下がる可能性があるため、バイナリファイルしか用意できない場合を除いてバイナリスキャンは補助的に用いることが効果的である。」との記述について、当該評価内容の論拠が不明確のため追記頂きたく存じます。 論拠の提示が難しい場合、個々の方式の解析精度について一般的な評価を記載するのではなく、以下の変更案程度の表現が望ましいと考えます。 「解析方式に応じて解析可能なデータや解析範囲等の仕様、および解析結果に差異が生じるため、SBOM生成の目的・利用可能なデータ等状況に応じて適切な解析方式を検討することが望ましい。」 理由：意見内容に記載の通り、評価の論拠が不明なため追記頂きたい趣旨です。 43頁「バイナリスキャンの結果について、通常スキャンで検出されたコンポーネント数と比較して 1 割程度しか検出されなかった。 」や、44頁「また、バイナリファイルに基づくスキャンの場合、多くの検出漏れが発生したことが実証で明らかとなった。」といった、実証での結果を論拠とされているものと推察しますが、これらは個別事例の結果であり、バイナリスキャンに対する一般的な評価の論拠とするには不十分と考えます。 本文書の読者が精度高くOSS検出・SBOM生成できる状態を実現するには、個々の方式の評価を述べるよりも、ツール選定段階について言及している4.2.において無償トライアルでの誤検知・検知漏れ検証の重要性を強調する方が効果的と考えます。	御意見を踏まえ、当該箇所を修正いたします。
41	13	10	組織	6.1 p47	意見内容 ：脆弱性対策に関する記述として、以下追記が望ましいと考えます。 「なお、脆弱性の影響範囲分析の実務では、ソースコードのみならず、要件定義書・仕様書・テスト仕様書等開発文書の要更新範囲の特定も必要な点に留意すべきである。この点の対策例として、2021年度の実証では、SBOMツールと既存の構成管理ツール（トレーサビリティ管理ツール ZIPC TERAS）を連携させることで、脆弱性の影響範囲特定の工数削減につながる可能性が検討された。」 理由：貴省の2021年度実証成果※出所4を反映する趣旨です。脆弱性対応の実務上、影響範囲特定の負担は大きな課題のため、本文書でも指摘し、解決策の例を提示することが望ましいと考えます。 ※出所4 https://www.meti.go.jp/meti_lib/report/2021FY/000644.pdf（151頁）	御意見を踏まえ、当該箇所を修正いたします。

42	13	11	組織	7.3.2.	意見内容 ：「7.3.2. SBOMに関するツール」で例示されたツールの抽出基準が不明のため、その点追記が望ましいと考えます。 貴省が利用を推奨するツールとして例示されていない場合、以下追記が望ましいと考えます。 「本項に記載のツールは一例であり、経済産業省が利用を推奨するツールを示すものではない。適切なツール選定のため、本項記載のツールに限定せず、市場に存在する様々なツールを事業者が十分探索・検討し選定すべきことに留意したい。」 理由：事業者が本項に記載のツールを貴省の推奨・認定ツールと誤解し、本文書に記載されたツールのみに絞り込んで選定を実施することが懸念されます。その結果、事業者が本来適切なSBOMツールを選定・導入することを妨げ、不適切なSBOM運用によるソフトウェアサプライチェーン上のセキュリティリスクの発生に繋がる可能性を危惧します。 上記懸念への対策として、貴省の推奨・認定ツールではない旨を明記し、市場に存在する様々なツールからの選定を奨励することが望ましいと考えます。	御意見を踏まえ、当該箇所を修正いたします。
43	14	1	個人	P.22 SBOM ツールに関する記述	意見：「コンポーネントの解析・特定を自動で行うことができるため、ほとんど工数はかからない。」とありますが、実際の設計・開発現場では、正しく判別するために設計者による丹念なチェックが必要で、多大な工数がかかっております。それでも100%抽出できているかの確証はございません。 対案：ツールの解析精度は、100%ではないことを踏まえた上で、ツールを導入・利用する上での指針や注意事項も合わせて記載いただきたいと考えております。	御意見を踏まえ、当該箇所を修正いたします。
44	14	2	個人	P.23 図 2-8 SBOM 管理による脆弱性管理コストの低減結果	意見：「SBOM ツールのコストは含まず」と補足されておりますが、コストは導入における大切な指標のため、明確化頂けないでしょうか。更にイニシャルコストかランニングコストなのか分けて記載頂きたいと考えております。 対案：SBOM ツールのコストテーブルを記載いただきたく、よろしくお願いします。	SBOMツールの費用は一般に公開されておらず、また、特定のツールの利用を推奨するものではないことから、原案のとおりとさせていただきます。
45	14	3	個人	P.42 実証に関する記述	意見：具体的な情報をご提示頂きたいと考えております。 対案：客観的な判断材料、例えば条件やプロセスの明記をお願い致します。条件を記載例として挙げますと、サンプルとした歯科用CT のコード容量（＊＊GB 等）、解析ツールのスペックなどの記載が望ましいと考えております。誤検出や検出漏れの確認工数も合わせて記載頂けると、なお一層具体性が増すと考えております。	御意見を踏まえ、実証における誤検出や検出漏れの確認工数を追加いたします。
46	14	4	個人	タイトルの「SBOM の導入」について	意見：「SBOM を導入する」という言葉について具体化をして頂きたい。 対案：例えば「SBOM 表示の導入」、「SBOM 作成の導入」、「SBOM 見える化の導入」、あるいは「SBOM 見える化の適用」等として頂ければと考えております。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） 「導入」という単語の示す意味としては「人や物をある場所、状態に導き入れること。また学問、技術、方法など選んでとり入れること。」と考えております。「SBOM」は「ソフト部品表」の言い換えですので、製品プログラムがある組織であれば、ソフト部品表は既に同組織に存在することとなり、新たに「導入」するようなものではないと考えております。 9 ページの表現では「食品表示→食品に含まれる原材料を可視化」とあり、SBOM にもこの考えを適用すると「SBOM 表示→ソフト一覧リストの可視化」になると考えられます。 よってSBOM 導入は、食品表示の導入ではなく食品成分の導入となってしまうと考えております。	本手引における「SBOMの導入」の定義について、1.2節で説明を追加いたします。

47	14	5	個人	p3 1.2.目的 ～ソフトウエアサプライヤーにおけるSBOM 導入に向けたプロセスを示す～	意見：本手引の期待する読者（対象）をソフトウエア・サプライヤに限定しているように見えます。読者を限定する目的でないことを示して頂きたいと考えております。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） 次節で「対象読者を～などのソフトウエアセキュリティにかかわる部門と経営層」と示しておられるように、各業界のサプライチェーンの中でソフトウエア設計を担うOEM、ベンダ、サプライヤのすべてのステークホルダがSBOM を作る対象となるように記載頂きたいと考えております。	御意見を踏まえ、当該箇所を修正いたします。
48	14	6	個人	p5 1.6.本手引きのサマリー <本手引きの背景・概要>	意見：SBOM 導入による管理のメリットについて補足頂きたいと考えております。 対案：以下のような背景等が書かれることが望ましいと考えております。 「構成するソフトウェアを管理する際に従来のハードウェアの部品表と異なり、情報量が膨大になって人の手で管理できる範疇を超えることが、機械処理可能な一覧表が必要な理由の一つであり、SBOM を使った方法が脆弱性管理やライセンス管理のためのメリットにつながる。」 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） 従来はソフトウェア開発ではSBOM を作成していない組織も有りえるため、SBOM のメリットを強調しておく方が良いと考えております。	御意見を踏まえ、当該箇所を修正いたします。
49	14	7	個人	p11 表2-2 プラクティスとプロセス SBOM の深さ	意見：SBOM の“深さ”とは何かをイメージさせるような具体的な説明や例があったほうが良いと考えております。 対案：例えばSBOM の深さが粒度を表すとすれば、SBOM の構成例などを簡単に記載するのが良いと考えております。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） 深さがSBOM の構成構造の粒度を表すとした際、どこまで（どの粒度まで）SBOM を作成するかという指針を示して頂いた方が良いと考えております。	御意見を踏まえ、「SBOMの深さ」に関する補足説明を追加いたします。
50	14	8	個人	p20 4 行目	意見：代表的なツールを例に示すだけですと、8 ページに記載の「SBOM を作成することで～当該コンポーネントに関するSBOM が誰によって作成されたかを特定・管理することが可能になる」という目的が達成できなくなると考えております。 対案：多数あるツールを選ぶときの注意点や、評価ポイント、ツール使用の考え方を示して頂きたいと考えております。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） ツールは各々の目的によって機能や性能が違っているため、ツール選定の際に指針を示して頂き、判断できるようにして頂けると良いと考えております。	SBOMツールの選定にあたっての観点や注意点等については、4.2節で記載しております。
51	14	9	個人	p20 表2-8 脆弱性管理のメリット 既知の脆弱性に関する情報を自動で検出～	意見：「SBOM 導入の主なメリット」というタイトルの表であり、SBOM を作れば自動で脆弱性情報を検出できるように見えるため、補足が必要と考えております。 対案：補足として、「ユーザーが脆弱性情報を収集しSBOM とマッチングすることで検出できる」と書いて頂いた方が良いと考えております。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） 対案に記載の通りです。	御意見を踏まえ、当該箇所を修正いたします。
52	14	10	個人	p26	対案：「サプライチェーンの上位から下位にSBOM 情報を要求する場合に、両者の合意に基づき知的財産情報や機密情報を侵害する独自のソフトウエアライブラリ等についてはSBOM に加える必要はない」といった補足を入れるのが望ましいと考えております。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） 独自に研究・開発したソフトウェアの名称、バージョン等の情報がSBOM に記載され、知的財産情報や機密情報が侵害されるリスクを負うことが無いようにしたいと考えております。	当該箇所の記載は、米国NTIAの「SBOM Myths vs. Facts」に基づく記載を参照したものであるため、原案のとおりとさせていただきます。

53	14	11	個人	p28 3.1 SBOM 導入における基本指針 7 行目	意見：SBOM を作ることは、同じ目的に向けて行われるべきだと考えており、目的に応じ、作成者によって別のものができてしまうことを懸念しております。 対案：設計者はSBOM を使って解決する必要がある課題を整理し、作成する目的にあわせてSBOM を活用（運用）することが求められる…などを補足頂ければと考えております。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） 基本的には、SBOM の使い方等状況に合わせてフォーマット等が変わっても互換性があれば問題ないと考えております。しかしながら、「目的に応じて作成・・」となりますと、組織によって、統一感の無いSBOM が作られることを懸念しております。SBOM 作成の具体的な目的は、8 ページで「各コンポーネントがいつ、誰によって開発され、他のコンポーネントとどのような依存関係があり、当該コンポーネントに関するSBOM が誰によって作成されたかを特定・管理すること」と記載がありますので、それに応じて脆弱性管理やライセンス管理、資産管理等の目的は共通であると考えております。	御意見を踏まえ、当該箇所を修正いたします。
54	14	12	個人	p28 3.1.SBOM 導入における基本指針 9 行目	意見：解決すべき課題（個々の目的は違っても、それらが包含される共通の大きな目的）があり、それに対応するためにSBOM を活用・運用するというロジックであると考えております。 対案：「設計者はSBOM を使って解決する必要がある課題を整理し、作成する目的にあわせてSBOM を活用（運用）することが求められる…」等を補足して頂きたいと考えております。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） SBOM の活用・運用に統一感を持たせるため	御意見を踏まえ、当該箇所を修正いたします。
55	14	13	個人	p31 表4.1 SBOM 適用範囲(5W1H) SBOM の活用範囲(why)	意見・対案：主な適用項目として、資産管理（またはトレーサビリティ）を追加して頂きたいと考えております。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） 8 ページで「SBOM を作成することで、各コンポーネントがいつ、～作成されたかを特定・管理することが可能となる」と述べており、トレーサビリティは活用範囲の主の目的になると考えております。	御意見を踏まえ、当該箇所を修正いたします。
56	14	14	個人	p44 5.2 SBOM の作成 SBOM 導入に向け認識しておくべきポイント SBOM 作成と共有の目的を鑑み、正確な情報を不足なくSBOM に記載することが望ましい（p45 の 2-3 行目も同じ）	意見：ツールによってスキャン方法が異なり誤検出や未検出が発生することを考慮すると、正確な情報を過不足なく記載する指針や考え方が必要であると考えております。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） （良い解決策はございませんが）正確な情報管理に向けて、複数のツールを利用し、ソースコードのスキャンとバイナリコードのスキャンとを整合させてSBOM をより正確に管理することが考えられます。または既知の情報を手入力で修正する等もあり得ると考えております。そのような指針を補足頂けたらと考えております。	お寄せいただいた御意見は、手引の更なる検討を進めていくに当たって参考にさせていただきます。

57	15	1	個人	7.3.2 SBOMに関するツール	「7.3.2　SBOMに関するツール」、「（1）有償ツール」に掲載されている製品はどのような調査・基準でこちらに記載をされていますでしょうか。 リストを拝見しますと、例えば、第三者機関で評価されているSCA製品（注１）やSAST分野のリーダー会社（注２）にて販売しているSCA製品が抜けております。 このリストに掲載されている「代表的な」と判断されたSBOMツールは、どの様な調査を行い、どの様な基準で記載がなされているのでしょうか。 「4.2. SBOMツールの選定」「表4-2 SBOMツールの選定基準」の条件を満たしたものとなりますでしょうか。 もし現在のリストで掲載を行うのであれば、調査日時、調査業者名、調査範囲、選定基準、選定基準の適合/不適合部分等を明記していただき、公平性に努めていただけたらと思われます。 また、上記から漏れているツールの掲載など、より網羅したほうが良いと考えます。 すべての有償ツールを掲載する訳にはいかない都合も想定されますが、掲載されなかったツールは「代表的ではない」ツールと判断されかねないことにもつながります。 WGに関連する方々が既知の製品が「有償ツール」に記載されやすいのかと推察いたしますが、こういう民間のツールのリストアップに際しては、各ベンダーからの情報提供の機会を設けていただけたらとも思います。 注１：https://www.sonatype.com/company/analyst-recognition-and-insights のサイトのThe Forrester Wave Software Composition Analysis (SCA), Q3 2021 reportの図で、Strong Performerは「有償ツール」リストにほぼ掲載されておりません。 注２：https://www.synopsys.com/ja-jp/software-integrity/resources/analyst-reports/gartner-magic-quadrant-appsec.html のサイトの* Gartner, Inc. “Magic Quadrant for Application Security Testing” by Dale Gardner, Mark Horvath, and Dionisio Zumerle, April 18, 2022 の図のLeaderのベンダーは、「有償ツール」リストに１社のみしか掲載されていません。	御意見を踏まえ、当該箇所を修正いたします。
58	16	1	組織	全般	全体的に見て、SBOMのメリットというよりは、ツールのメリットの説明になっているように感じます。SBOM自体が脆弱性やライセンス管理上の利便性に貢献しているとは読み取りにくいと感じます。	お寄せいただいた御意見を踏まえ、SBOM導入のメリットをより明示的に記載する等、全体構成などの見直しも含めて記載内容の修正を検討いたします。
59	16	2	組織	全般	SBOM生成ツールが、CVE情報の取得をサポートしていない場合、SBOM生成ツールとCVE情報を取得するツールとの連携が必要になってくるので、その管理方法についての説明があると良いと思います	お寄せいただいた御意見は、手引の更なる検討を進めていくに当たって参考にさせていただきます。
60	16	3	組織	全般	「有償ツールの方が無償より使える」と取れる書き方になっていますが、"The Open Source Software Security Mobilization Plan"をきっかけに Linux Foundation/OpenSSF などの Open Source コミュニティでの動きが活発になってきており、今後コミュニティにおいて無償ツールが大きく成長する可能性があると思われます。	御意見を踏まえ、ツールに関する表現を修正いたします。
61	16	4	組織	全般	「ライセンス管理」、「脆弱性管理」は、解釈の幅が広いため、明確な用語の定義が必要だと思われます。	御意見を踏まえ、「ライセンス管理」、「脆弱性管理」に関する補足説明を追加いたします。
62	16	5	組織	2.4 SBOM導入のメリット	「表 2-8 SBOM 導入の主なメリット」 「脆弱性管理のメリット/直接的メリット/脆弱性残留リスクの低減」 脆弱性の検出は、SBOM生成ツール自体が対応もしくは脆弱性を検出するツールと組み合わせてSBOMを生成しないと出来ないので、単純にSBOMを使うことで既知の脆弱性を自動検出できるというのは誤解を招く可能性があるのではないでしょうか。	御意見を踏まえ、当該箇所を修正いたします。

63	16	6	組織	2.4 SBOM導入のメリット	「表 2-8 SBOM 導入の主なメリット」 「脆弱性管理のメリット/直接的メリット/脆弱性対応期間の短縮」 新たな脆弱性をリアルタイムで検出するのは、SBOM単体でできることではないと思われます。	御意見を踏まえ、当該箇所を修正いたします。
64	16	7	組織	2.4 SBOM導入のメリット	コードが内在しうる脆弱性の話が中心になっていますが、サプライチェーン自体への攻撃についても触れた方がよいと思われます。 例えば SBOM作成時/チェック時に、依存するコンポーネントを攻撃者がすりかえていることに気がつくなどの対策が必要です。	御意見を踏まえ、当該箇所を修正いたします。
65	16	8	組織	2.4 SBOM導入のメリット	ライセンス管理上のメリットでライセンス違反のリスクを回避できるとありますが、例としてあげられているのが、GPL違反にしか触れていないため、GPL以外に気をつけることはないかのように読めてしまいます。	御意見を踏まえ、当該箇所を修正いたします。
66	16	9	組織	【4.2. SBOMツールの選定】→【参考情報：付録 7.3.2 SBOMに関するツール】	どのフェーズに利用できるツールなのか記載すべきだと思います。例えば、(1)（有償ツール）に記載されているツールはほとんど SBOM 生成のためのツールのように思われます。	御意見を踏まえ、各ツールの特徴に関する表現を修正いたします。
67	16	10	組織	5.3. SBOMの共有	納入先が利用する SBOM ツールによって、採用可能な SBOM 共有方法が異なることは多いと思います。システム管理者としてSBOMを管理する場合、フォーマットや含まれる情報が違う複数のSBOMを管理していくためのプラクティスがあると良いと思います。	お寄せいただいた御意見は、手引の更なる検討を進めていくに当たって参考にさせていただきます。
68	16	11	組織	5.3. SBOMの共有	OSSのプロジェクトなどは通常、自社のコントロール下にないので効率的にSBOMを管理していく方法が重要になると思われます。SBOMは自社で作成し、作成したSBOMの内容を精査する手段として、提供されたSBOMを使うという方法も考えられます。	御意見を踏まえ、第三者からSBOM提供を受ける場合のメリットについて、修正いたします。