「ソフトウェア管理に向けたSBOMの導入に関する手引ver2.0（案）」に対する意見募集で寄せられた御意見に対する考え方

No	提出者		組織・個人	該当箇所	提出意見	ご意見に対する考え方
	番号	枝番				
1	1	1	ー	全般	ソフトウェア管理に向けたSBOMの導入に関する手引ver 2.0（案） 根本的に脆弱性の考え方がおかしいです。 一般企業なら正常ですが、あなた方は政府なのです。 外国OSや外国サーバや外部ソフトウエアを使うこと事体が脅威なのです。 セキュリティを第一に考えると政府専用のソフトウエア開発専門家を囲うことが正解です（OSSを使ったり雇ったりしたら結局スパイが入り込む余地のある外部委託と変わりません）。	お寄せいただいた意見を踏まえ、脆弱性の考え方に留意しつつ、引き続き検討を進めてまいります。
2	2	1	個人	全般	今回は、パブコメの段階から、PDFをしおり付きPDFで公開され、電子的な可読性が高まっていると思います。前回(第1版)では、パブコメ段階ではしおりなしのPDF、公開版はしおり付きのPDFでした。また、今回は、第2版のため、前版との見え消し版の提供をすべきだと思います。	お寄せいただいた意見を踏まえ、今後の手引の改訂に際しては、見え消し版の提供等、変更点が分かるような形での提供に努めます。
3	2	2	個人	1.1	1.1の「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。」の記載は、第1版のパブコメで「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。」とのコメントに対して、「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。」とされているが、どのように参考され、何が修正されたかを開示すべきではないかと考えます。	ver 1.0のパブリックコメントでいただいたコメントも参考にしつつ、今回ver 2.0で新たに追加したSBOM取引モデルにおいて、サプライチェーンにおける責任範囲や取引契約における留意事項の検討を行いました。
4	2	3	個人	表2-1	表2-1 SBOMの概念的イメージ 　IDがあり、1,2,3,4とあり、依存関係でIncluded in #1のように使用している。ID(Identification: 識別子)はあくまでコンポーネント名、Version等であるべき。つまり、この表でIDを#に変更して、単なるリストの番号にして、依存関係ではその番号を使わないで、Included in Applicationのようにコンポーネント名で示すべき。さらに、別な表(例えば、図2-6など)も同様。これにより、NTIAのSBOM最小要素のデータフィールドと整合化される。	御意見を踏まえ、表2-1、図2-6、図2-7、図2-8、図2-9において、依存関係では番号を使わず、コンポーネントに関する依存関係を示す形で修正いたします。
5	2	4	個人	2.3	NTIAのminimum elementsは、data fields以外に、automation support、practices and processesが記載されている。しかし、本書ではdata fieldsだけが抜き出し説明されてしまっている。他の2つの項目も本書に説明を追加すべきでは。	御意見として承ります。 Automation supportとPractices and processesについては表2-3で整理しており、一部用語については、脚注にて補足を記載しております。

6	2	5	個人	表2-2	表2-2のSBOM導入の主なメリットで、コンプライアンス対応の効率化(輸出規制管理対応など)を追加記載した。SBOMのようにソフトの一覧を管理するものに、ライセンス管理、輸出管理等があるが、どれもソフトの一覧を管理することは変わりないが、観点が少しずつ異なる。セキュリティの管理では、どのコンポーネントのどのVersionがどのPatchが当たっているかを管理する。輸出管理では、米国原産品及び輸出規制等で制限を受けやすい暗号モジュールが含まれているか注目して管理する。ライセンスではそのソフトの調達方法、契約などを管理する。全てソフトの一覧ではあるが、その観点、主旨が異なる。このため、これらをすべて満足できる管理にするためには、その粒度が異なる。ライセンス管理では、そのライセンス単位で部品が管理されればいいし、輸出管理では使用している注目すべきモジュールを管理する必要がある。このように全てを1つのリストで管理することは、セキュリティ管理のためのSBOMを必要以上に肥大化してその運用が手間になる可能性が高い。他の分野でもSBOMが活用できることを示すことはいいが、あまりそれをメリット等にしないほうがいいのではないかと考えます。	御意見を踏まえ、2.2節の末尾において、どのメリットを重視するかを組織内で検討することの重要性を追記いたします。
7	2	6	個人	7.1	7.1に「脆弱性管理による脆弱性リスクの低減」とあるが、脆弱性リスクが非常にわかりにくい。一般的に、リスクとは脅威の大きさとその確率とで定義される。脆弱性が悪用される脅威に関するリスクを低減するために、悪用される脆弱性を低減させる。	いただいた御意見も参考に、修正いたします。 修正箇所：7.1節に脆弱性リスクについて補足説明を追加致します。
8	2	7	個人	図7-2	「7. 脆弱性管理プロセスの具体化」が記載されている。例えば、図7-2において「(1.1)？(1.4)については定期的に実施。必要に応じてフィードバックループを実施。」の部分が非常に重要で、ここのプロセスの設計ができていないとSBOMによる脆弱性管理はできないと思います。具体的には、ある製品でSBOMが存在して、それを元にNVD等を検索する。すると大量のCVEが取得できる。その中で、既にPatch等で対策してあるもの、直近に対策するもの、優先度(影響度)がない又は低く対策が不要なものに分類する。ある時間がたつと、さらに新しい脆弱性がDBに登録されている。既に調査、判断済のものも含めて検索されてしまう。これの扱いをどうするかを設計しておくことが重要であり、それがないと脆弱性の管理ができないと考えます。	いただいた御意見も参考に、修正いたします。 7.4.1項に、対応済みの脆弱性の情報管理は課題であることを挙げつつ、今後、SBOMツールやVEX等を活用して管理することの重要性を挙げます。
9	2	8	個人	7	「7. 脆弱性管理プロセスの具体化」が記載されている。SBOMを元にNVD等のDBを検索することもあるが、それ以外に、新規にセキュリティサイト(例えばCISAのKEVのCatalogや、JPCERT/CCのAlert等)に公開された脆弱性が、自社の製品に含まれているかどうかをSBOMで確認する等のプロセスも必要になる。公開されている情報にコンポーネント名、ベンダー名があれば、それをあいまい検索でSBOMを検索して、その結果を人が確認するのが、現時点では適切なプロセスではないかと考えます。このようなプロセスも追記すべきではないかと考えます。	いただいた御意見も参考に、修正いたします。7.4.1(4)に、部品IDの課題をあげ、コンポーネント名、ベンダー名などの部分マッチングによる現実策を示します。

10	2	9	個人	7.4.1	P60 7.4.1 「図7-4 利用可能なSBOM データの特定」 この図が、組織内のIT環境でのSBOMのような表に見えてしまいます。本書では、ソフトウェアを含む製品開発をする組織を主たる対象にされているので、それに合わせて、記載するのがいいのではないかと思います。まず、必要なのは、自社製品のソフトウェアのSBOMであり、他社、第三者のコンポーネントを含んで開発されていることを想定したSBOMが必要になる。第三者のSBOMは、入手が困難なのでツールを用いて自動生成と説明しているが、その第三者がSBOMを提供しなくても脆弱性管理などのセキュリティマネジメントを実施し、それを保証されている限り、そのコンポーネントのSBOMは不要ではないかと考えます。	いただいた御意見も参考に、修正いたします。サプライヤーに依存せず脆弱性管理をする必要性も考慮してSBOMの取得について但し書きを記載しました。
11	2	10	個人	7.4.1	P60 7.4.1(3) 対象とする脆弱性DB の選択 「脆弱性DB の選択は、リスク低減、コスト低減の観点から比較を行い、個社ごとに優先度ポリシーを考慮して判断することが期待される。」の「個社ごとに」と記載されている。個社で判断する必要はあるが、あくまで、その製品の特性を考慮して、製品ごとに判断されるべきかと思います。リスクの高い製品とリスクの低い製品とでは、個社でも判断が異なるべきだと思います。	いただいた御意見を踏まえ、修正いたします。製品ごとに脆弱性DBを対象範囲を選択することが期待されることを示しました。
12	2	11	個人	7.4.1	P62 7.4.1(4) 図7-6 脆弱性マッチング手法の選択の参考となる一覧表（イメージ） 図中で,"PURL"と“pURL"との表記があるがPURLで統一したほうがいいのでは。	いただいた御意見のとおり、修正いたします。PURLに統一します。
13	2	12	個人	全体	ぶら下がり段落(hanging paragraph) ISO/IEC, JIS等では、ぶら下がり段落(hanging paragraph)の文書構成は禁止されている。本書は、ISO/IEC, JIS等ではないので、厳格に従う必要は必須ではないですが、それらデジュール標準での過去の有識者等の経験に基づいたルールに、明確な理由がない限り準じたほうがいいと考えます。部局は違いますが、JISを管掌されている経産省の文書においては、特にJISのルールを尊重してもいいのかと思います。 主なぶら下がり段落の箇所 (1) 4.1が存在するときに4の直下に文書を書かない (2) 5.1が存在するときに5の直下に文書を書かない (3) 6.1が存在するときに6の直下に文書を書かない (4) 7.4.1が存在するときに7.4の直下に文書を書かない (5) 8.4.1が存在するときに8.4の直下に文書を書かない (6) 8.5.1が存在するときに8.5の直下に文書を書かない (7) 8.6.1が存在するときに8.6の直下に文書を書かない	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。
14	2	13	個人	8.1.1	P79 8.1.1 「SBOM の生成・活用に関する対応範囲の違い可視化する方法について示し、」と記載されているが、「違いを可視化する方法」と「を」を補ったほうが読みやすいと思います。	いただいた御意見のとおり、修正いたします。修正箇所8.1.1項。

15	2	14	個人	8	8.SBOM対応モデル 「SBOM の生成・活用に関する対応範囲の違い可視化する方法」に関しては、非常に重要な取組みだと思います。しかし、「ソフトウェア取引において」、これだけが使用されることは適切ではないと思います。SBOMはあくまでツールの1つであり、ソフトウェアを含む製品を出荷後の、脆弱性、セキュリティの対応が評価されるべき軸だと考えます。例えば、自動車、医療機器等で、膨大なSBOMをそのままエンドユーザに提供しても意味がない。	いただいた御意見は、ガイドライン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。なお、SBOM対応モデルは、ソフトウェア取引において部品網羅性、脆弱性対応の網羅性を可視化するもので、調達時だけでなく、脆弱性管理、運用時にもSBOMが利用されることを前提としています。
16	2	15	個人	8.6.1	P113 「第十二条第三項が新設され、はセキュリティ要件が明確化された。」は「第12条第3項が新設され、サイバーセキュリティ要件が明確化された。」にしたほうが、いいのでは。	いただいた御意見のとおり、修正いたします。
17	2	16	個人	8.6.1	8.6.1に法律の第何条、第何項との記載があるが、漢数字と数字とが混在している。基準、公知、通知名等は原文のまま関数値にして、それ以外は算用数値に統一したらどうか。 (1) P112 「これにより薬機法における基本要件基準第十二条第三項にサイバーセキュリティ要件が明示された。」は、「基本要件基準第12条第3項」に修正 (2)P113 「医療機器製造販売業者には薬機法における基本要件基第十二条第二項で」 は、(i)基本要件基は、基本要件基準の誤植 (ii) 第12条第2項に修正 (3)P113 「第十二条第三項が新設され、はセキュリティ要件が明確化された。第十二条第三項に」は、「第12条第3項が新設され、サイバーセキュリティ要件が明確化された。第12条第3項に」に修正 (4)P114 「基本要件基準第十二条第 3 項の適合性の確認に用いることができる。」は「基本要件基準第12条第3項」に修正	いただいた御意見のとおり、修正いたします。基準、公知、通知名等は原文のまま漢数字にして、それ以外は算用数値に統一します。
18	2	17	個人	8.6.1	P112 また、今般、「IMDRF/CYBER WG/N73FINAL:2023 Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity（以下、IMDRF 追補SBOM ガイダンス」及び「IMDRF/CYBER WG/N70FINAL:2023 Principles and Practices for the Cybersecurity of Legacy Medical Devices（以下、IMDRF 追補レガシー医療機器ガイダンス」2 つの追補ガイダンスが発出された。 と記載されているが、(1)括弧 (鍵括弧、通常の括弧)が対になっていない。(2)「2つの追補」の前に「の」を補い「の2つの追補」にしたほうが読みやすい。	いただいた御意見のとおり、修正いたします。
19	2	18	個人	図8-8	図 8-8 医療機器の市販後のセキュリティに関わる規制の概要 市販後に関して、下記も最近発出されているため、追記したほうがいいのでは。 「医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について（令和 6 年 1 月 15 日付け医薬安発 0115 第 2 号）	いただいた御意見のとおり、追記致します。
20	2	19	個人	8.6.1	P114 「SBOM は，IEC 62443-4-1 では要求されないが，IEC TR 60601-4-5 では要求される顧客向け文書である。」と記載されている。IEC62443-4-1は制御分野のセキュリティプロセス規格であり、IEC TR 60601-4-5は、医療機器分野のセキュリティケーパビリティの規格。分野の異なるものを併記するのはどうかと思います。より正確には、 「SBOM は，JIST81001-5-1, IEC81001-5-1 (制御分野のIEC 62443-4-1を元にした医療機器分野の規格) では要求されないが，IEC TR 60601-4-5(制御分野のIEC62443-4-2を元にした医療機器分野の規格) では要求される顧客向け文書である。」	いただいた御意見のとおり、修正いたします。

21	2	20	個人	9	9.SBOM取引モデル サプライチェーンにけるSBOMに関する費用負担を考慮することは重要だと考えます。しかし、本書では、主にソフトウェアを含む製品を取り扱っている製造業者を主たる読者とした場合、その製品のソフトウェアは(1)自社開発、(2)委託開発、(3)サードベンダー等のソフトの利用、(4)OSS等の利用に大きく分けられる。委託開発においては、本9章で記載されていることが当てはまるが、(3)(4)に関しては当てはまらない場合が多い。(3)(4)においては、SBOMを提供してくれるかで評価するのではなく、そのソフトを提供後に脆弱性の管理、情報共有を実施するかどうかが重要になる。SBOMに費用を払うのではなく、その脆弱性管理及びその対策のアクティビティに費用が支払うべきである。現状の本9章は、主たる(3)を含めない(2)を中心な記載になっている。例えば、Microsoftは、SBOMを一般的には提供しないが脆弱性情報及びそのPatch等を継続的に開示している。SBOMがなくてもそのような活動で十分ではないかと考えます。 例えば、Windowsを使った医療機器を製品化した製造業の場合、脆弱性の管理及びパッチの適用に関しての費用は、マイクロソフト、医療機器メーカ、医療機関、患者でどのように考えたらいいかなどの指針があると非常に有効ではないかと考えます。自動車業界では、最終製品を扱い自動車会社が、サプライチェーンの中で、規模が大きいのに対して、医療機器業界では、OS等のベンダー、ソフト開発会社、医療機関に比べて、規模の小さい医療機器会社も多く存在する。その場合の責任、費用の在り方などの考え方が日本の国益も考慮した上で有識者の先生方で十分議論されるといいのかと思います。	いただいた御意見は、ガイドライン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。論点として、サプライヤによる脆弱性対応の有無だけでなく、サプライヤの企業としての存続、脆弱性対応の即時性、ライセンス管理、開発の生産性向上等の観点で、SBOMの有効性が考えられます。
22	2	21	個人	全体	全体 全体を通して、対象読者を2種類に分類して、本書を分割(章、文書など)したほうがわかりやすいかと思います。分類1：自身の企業で使用しているIT製品のSBOMの管理、分類2：自身の企業が提供している製品、サービスでのSBOMの管理。分類2は、さらに、SIとかSEとかの作業とか、保守契約を含む製品や多くのサービスと、販売が中心の製品とで異なる。これらは、共通する部分もあるが、他方にはあてはまらない場合、理解しにくくなっている部分も多い。例えば、5.3は分類2、5.1、5.2は、分類1と分類2とでフォーカスする部分が異なる。6、7も、分類1と分類2とでフォーカスする部分が異なる。8は、特に各分野の例は分類2、9は主は分類1。	いただいた御意見は、ガイドライン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。現状版では、章の依存関係が多々あるため、文書の分割は今後の課題と致します。
23	3	1	―	図2-2	図2-2 に食品サプライチェーン及び食品表示の概念的イメージがあるが、この図はだいぶ改良されこの図に注文はないが、SBOMだったらこうなる、という図があるとより対比が出ると思う。 また、2.5. SBOM に関する誤解と事実　の節の追加はとても評価する。 ところでこれが情報処理技術者試験やその他の類似試験の試験範囲となるのはいつであろうか。そろそろこのあたりを明確にする時期ではなかろうか。 他省庁の国家試験とも足並みそろえて頂き度。	本手引に対する肯定的な御意見として承ります。また、試験制度に関してお寄せいただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
24	4	1	―	全体	PC系アプリケーションは導入しゃすいと思われるが、組み込みシステムでは現実的に難しいと考えます。 マイコン、OS等変われば同じ機能でも別モノ扱いであり、脆弱性レベルもそれぞれなので、ソフト名でひとくくりに信頼のある・ないを判断できません。 一般のシステムは導入はあくまで任意でよいと考えます。	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。
25	5	1	―	2.1	食品表示に例えていますが、食品表示自体がすでに重要な成分情報を記載することができていません。 例えばコオロギパウダーは、「アミノ酸等」と書けばOKであるし、総菜は一番主となる食材の産地しか書いていないため、食べたくない昆虫や外国産食材を知らないうちに口にしていることがあたりまえに起きています。 食品はしっかりやれてるように見えてますが、現実は「ザル表示」になってしまっており、そもそもの趣旨にそぐわない結果になっています。食品が、なぜうまくいってないのか検証することが必要だと思われます。	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。

26	6	1	―	全体	産業側で採用可能かどうかの意見を取り入れることなく、行政側や学識者が机上の論理で編纂した資料になっており、産業側との乖離が大きい。企業側の立場の見解が反映されているセクションが無いのも問題がある。一般企業が参加した意見交換会を設けて資料全体を見直すべきである（このようなパブコメの形式で部分的な指摘では限界がある）。	いただいた御意見は、ガイドライン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。これまで企業のサプライチェーンを通じた実ソフトウェアに対する６つの実証を行い、委員会形式で民間企業の意見を取り入れながら検討しておりますが、今後の実証も検討致します。それらの結果を反映し、企業におけるフィージビリティを確保していきたいと考えております。
27	6	2	―	全体	SBOMは、その利用意義から、自社開発して自社でしか使用していないコンポーネントは開示する必要がないはずだが、それが明示されていない。コンポーネント構成自体に開発ノウハウが反映されているため、構成全体を開示することは、開発ノウハウの開示を意味するため、企業側としてはデメリットでかなく受け入れられない。企業活動の大前提すら反映されていない内容となっているのは、資料の作成プロセスに問題があるためと思われる。	いただいた御意見は、ガイドライン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。9.3節に「SBOMのメリットは、サプライチェーンを通じて標準化された部品情報の共有と自動処理による効率化」と記載し、SBOMは企業間での共有を前提と考えてまとめています。また、SBOMの公開、知財については、2.5節に以下のように記載しております。 「誤解：SBOMは公開しなければならない」 「誤解：SBOMは知的財産や企業秘密を露呈する」
28	6	3	―	全体	また、SBOMを利用してセキュリティ向上に寄与できるのは大企業のみと思われる。中小企業、特にソフトウェアを利用するだけのIT専門技術者を擁しない多くの企業において、SBOM自体よりも、SBOMがどのように実際の業務に関わるかが重要なのであって、ソフトハウスがいくらSBOMを整備しようとも脆弱性が放置されるだけで終わる。	いただいた御意見は、ガイドライン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。中小企業への普及促進策については、引き続き検討させて頂きます。

29	6	4	―	全体	SBOMを利用することにより社会全体のセキュリティ向上を目指しているのは理解できるが、その効果の根拠が示されていない。実際の企業活動から乖離したアカデミックな学識者の意見で編纂するのでなく、実際の企業（中小企業を含むのが望ましい）の技術者が参加した状態で編纂しないと、この乖離は埋まらず、結果として産業側に無視されるだけのものとなる。	いただいた御意見は、ガイドライン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。本手引きは、これまで中小企業、大企業などサプライチェーンを含む６つの実システムを対象に実証を行うとともに、委員会形式で民間企業の意見を取り入れながら検討しており、そこでの知見の共有に主眼を置いています。今後も実証を検討し、中小企業への普及促進策の検討を進めて参ります。
30	7	1	―	全体	今の時流でもある小林製薬の紅麹事件をどこかに入れるべきである。 原材料に包含される、最終消費者には不可視のサプライチェーン、SBOMと共通点は同じである。 消費者庁で現在この問題をとりまとめしていると認識しているので、消費者庁との連携を必要に応じて行い、文書に反映させるべきである。	お寄せいただいた御意見に関して、ソフトウェアサプライチェーンに共通する点はあるかと存じますが、対象の事案とSBOMとの関連性について検討が必要であること等を鑑み、今回の改訂では追記を見送りさせていただきます。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。
31	8	1	組織	全体	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、御省が昨年7月に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、また、今般、中小企業も含め、あらゆる企業にとってSBOMを効率的に活用できる方法等を反映された「導入手引」の改訂案を作成されたことは、誠に時宜を得たものであります。本改訂案につきましては、特段の意見はなく、賛同致します。本手引書により、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。
32	9	1	組織	7.3. p57	意見内容 ：プロセスにつき、以下加筆が望ましいと考えます。 ・(1)脆弱性特定　の中に、「脆弱性マッチング結果の検証」を「脆弱性マッチングの実行」後の手順として追記 ・(3)情報共有　の中に、「脆弱性マッチングの検証結果通知」を追記 理由：59頁に例示されるような脆弱性マッチング手法の正確性は、現在の技術水準では完全には担保されていないと理解しております。 例えば、SBOMはSW部品を構成するファイル・ソースコードの粒度まで起票されているとは限らないため、当該粒度で脆弱性が発生しているか区別することは困難です。結果、処理に関係のない、いわゆるデッドコード部分で発生した脆弱性がマッチングされる余地がございます。 また、同じSW部品でも脆弱性の発生有無はバージョンにより異なる所、脆弱性データベースによっては、SW部品のバージョンで脆弱性を絞込検索ができないものも存在します（例：JVN）。結果、管理対象のSW部品のバージョンには該当しない脆弱性がマッチングされる余地がございます。 実際には発生していない脆弱性対応に対し、「7.4.2. 脆弱性対応優先付けフェーズ」のプロセスを実施すると、不要な対応工数が発生する他、他の重要な脆弱性対応が遅れるなどセキュリティ上も悪影響があるため、脆弱性マッチング結果の検証を実施することが望ましいと考えます。 SWサプライチェーンの中でSBOMを共有している場合、上記検証結果対応不要と判明した脆弱性についても通知し、サプライチェーン全体で対応を停止すべきです。当該通知実施のため、情報共有の中に「脆弱性マッチングの検証結果通知」を追記が望ましいと考えます。 なお、本来は上記の追加プロセスに対応した詳細説明が、後段の「7.4.2. 脆弱性対応優先付けフェーズ」「7.4.3. 情報共有フェーズ」にも追加すべきところ、当該節には実際の脆弱性マッチング・情報共有の実行時に関する説明箇所が無いため、追記案の提示は割愛させて頂きました。	いただいた御意見も参考に、修正いたします。 「脆弱性マッチング結果の検証」については、7.4.1の最後から第２節に追記。 「脆弱性マッチングの検証結果通知」については、表 7-3 (3.2.3)に記載。

33	9	2	組織	7.3. p57, 7.4.2. p62, 7.4.2.(2) p63	意見内容 ：プロセス「(2.1) 優先付け情報の選択・取得」を「(2.1) 優先付け情報の選択・取得・検証」に変更が望ましいと考えます。 また、7.4.2. 脆弱性対応優先付けフェーズ　内の「(2) 優先付け情報の選択・取得」内の末尾に、以下の様な記述の追加が望ましいと考えます。 「優先付け情報自体に誤りがあると優先付けも誤るため、個々の優先付け情報の導出プロセスや前提条件・評価基準の妥当性、評価根拠となるエビデンスの有無・内容等から、優先付け情報の検証を行うことも推奨される。」 理由：優先付け情報自体に誤りがあると優先付けも誤るため、情報の検証が望ましいと考えます。その旨反映する目的で、(2.1)のプロセス名に「・検証」を追記することを提案します。 特に、今後VEXの利用が加速した場合、VEXの妥当性評価が必要になると予想しております。VEXが信頼に足るツールで発行されると仮定しても、VEX発行時の当該ツールへの入力・設定内容次第で正しいセキュリティアドバイザリが生成されない可能性があるためです。現状のCSAFの仕様上は、アドバイザリの妥当性を根拠づける情報が提供されるとは限らないと承知しております※出所1。 事業者での運用の中では、VEX生成のプロセスの妥当性説明や、エビデンス等をVEX発行元に求める等の対応が必要となり得るため、当該対応がプロセス(2.1)に含まれることを明記することが上記提案の目的です。 ※出所1　https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html	いただいた御意見も参考に、修正いたします。追記指摘「優先付け情報自体に誤りがあると優先付けも誤るため、個々の優先付け情報の導出プロセスや前提条件・評価基準の妥当性、評価根拠となるエビデンスの有無・内容等から、優先付け情報の検証を行うことも推奨される。」は優先付け情報ではなく、（３）カテゴリ判断における評価者の判断により生じるものであるため、それに応じて修正したものを7.4.2.(3)の末尾に追記します。
34	9	3	組織	7.3. p57	意見内容 ：本書で示す脆弱性対応プロセスと、既存のサイバーセキュリティ関連国際法規・規格で定義されている脆弱性評価・対応プロセスとの対応関係を整理した図表の追加が望ましいと考えます。 理由：脆弱性対応プロセスについては、ISOをはじめとした国際団体による規格や、CISA・FDAをはじめとした各国政府による法規・ガイドライン等で議論されております。そのような文書との対応関係が示されていると、本書の脆弱性対応プロセスの各手順の具体的な運用を事業者が設計する際に有用と期待されます。 本書の読者の中には、既存の国際法規・規格に則った脆弱性対応の運用を構築済または検討中の事業者も含むと考えます。当該事業者にとって、自社が本書の定める脆弱性対応プロセスのどの範囲に対応済で、今後対応必要な範囲はどこかが特定できると、今後の対応検討を効率的に推進でき有用と考えます。 また、既存の国際法規・規格との対応関係を示すことで、本書の脆弱性対応プロセスが国際的にも説明責任を果たせるものであることが把握でき、読者が安心して本書を利用いただけると考えます。	いただいた御意見も参考に、修正いたします。図7-2の脚注に、NTIA, CISAの関連文書を参考にしていることを示しました。
35	9	4	組織	7.3. p57	意見内容 ：本書で示す脆弱性対応プロセスの実務で使用できるツールチェインを例示した図表の追加が望ましいと考えます。 理由：脆弱性リスクは対応までのリードタイムに比例して増大するため、脆弱性対応は迅速に実行される必要があります。また、欧州サイバーレジリエンス法では重大インシデント・悪用済脆弱性発生時に、把握後72時間以内に緩和措置をENISAに通知する義務がある※出所2等、法令対応の意味でも脆弱性対応プロセスの迅速化の重要性が増しております。 上記を踏まえると、本書に示された脆弱性対応プロセスは可能な限りツールにより自動化されることが望ましいと考えます。ツールチェインの例示は、事業者が導入すべきツールを把握するのに役立ちます。 例えば、「(2)脆弱性対応優先付け」以降のプロセスでのコミュニケーション・進捗管理にはチケット管理システムが利用できると考えます。「(2.1) 優先付け情報の選択・取得」においては構成管理・トレーサビリティ管理ツールにより情報取得の工数削減可能性がある旨、貴省の2021年度実証において示されています※出所3。 SBOMツールを導入済・検討開始した事業者も増加している中、SBOMツールで対応可能なプロセスと、他ツールによる補完が必要なプロセスを明確化し、重複投資の防止を図る意味でも、ツールチェインの例示が有用と考えます。 ※出所2　https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html ※出所3　https://www.meti.go.jp/meti_lib/report/2021FY/000644.pdf（151頁）	いただいた御意見は、ガイドライン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。

36	9	5	組織	7.4.1.(2) p60	意見内容 ：利用可能なSBOMデータ特定時の留意点として、SBOMの作成タイミングの確認が望ましい旨言及すべく、以下の対応が望ましいと考えます。 ・以下の様な記述の追加 「なお、利用しようとしているSBOMが、脆弱性マッチング対象のソフトウェアのどのタイミングを反映したものかを確認することが推奨される。 この点、CISAは”Types of Software Bill of Materials (SBOM) Documents”の中で、SBOMが作成タイミングごとに種類分けされ、種類別に利点・欠点があることを指摘している。例えば、ソースコードから生成されたSBOM（”Source SBOMs”）は、実行・コンパイル対象外のSW部品の脆弱性をハイライトする可能性を欠点に挙げている。 SBOMデータを取得する際は、脆弱性対応の対象システム・ソフトウェアの性質を踏まえ、どの作成タイミングのSBOMデータが必要かを定義することが推奨される。また、実際に取得できたSBOMデータがどのタイミングで作成されたかを確認の上、正確な脆弱性対応のために必要な作業を適宜調整することが推奨される。 関連して、利用しようとしているSBOMが、脆弱性マッチング対象のソフトウェアのバージョンに適用可能なことを確認することが推奨される。異なるバージョンに対するSBOMを利用した場合、脆弱性マッチング対象のバージョンに含まれるSW部品が正しく反映されておらず、脆弱性マッチングでの誤検知・検知漏れが発生する恐れがある。」 ・上記の様な記述に続く形で、CISA “Types of Software Bill of Materials (SBOM) Documents”内Table 1”・Table2※出所4を日本語で要約した図表の追加 理由：追記案に記載の通り、同じソフトウェアに対するSBOMが作成タイミングごとに異なり、脆弱性マッチングの精度に影響を与えることから、SBOMの作成タイミング観点での妥当性確認を推奨する記載を含めることが本提案の趣旨です。 作成タイミングの定義としては、CISAの”Types of Software Bill of Materials (SBOM) Documents”での定義が国際的にも普及している理解ですので、その種類分けや種類別の利点・欠点が本書の中で把握できるよう、当該CISA文書の定義の要約を付記することで、読者の理解も高まると期待しております。 独BSIも、SBOMについての技術ガイドライン”TR-03183”内で上記のCISAの定義を引用しつつ、SBOMの種類別に利用可能な情報が異なる旨言及しています※出所5。 ※出所4　https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf ※出所5　https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03183/BSI-TR-03183-2.pdf?__blob=publicationFile&v=3（11頁”6.2 SBOM-Typen”）	いただいた御意見を踏まえ、7.4.1.(2) を修正します。
37	9	6	組織	表 7-2 p64	意見内容 ：「VEX脆弱性ステータス（影響：有・無・不明）」に対する「説明・重要性の考え方」欄を、「脆弱性に係る部品を利用した開発者が直接評価したものであり、VEX発行時に適切なプロセス・評価基準で評価が行われる限り精度が高い。」に変更が望ましいと考えます。 理由：VEXはデータフォーマットに過ぎず、それ自体がセキュリティアドバイザリの妥当性を保証するものではないと認識しております。VEXが信頼に足るツールで発行されると仮定しても、VEX発行時の当該ツールへの入力・設定内容次第で正しいセキュリティアドバイザリが生成されない可能性がございます。現状のCSAFの仕様上は、アドバイザリの妥当性を根拠づける情報が提供されるとは限らないと承知しております※出所1。 誤ったVEXが信頼され、脆弱性対応優先付けを誤る事態を防ぐ目的で、VEXの精度については「VEX発行時に適切なプロセス・評価基準で評価が行われる限り」との留保を付加するのが望ましいと考えます。 ※出所1　https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html	いただいた御意見のとおり、表7-2を修正します。

38	9	7	組織	p67（組織カテゴリーごとの優先付け判断方法）	意見内容 ：判断ノードのそれぞれの観点で利用し得る、既存のサイバーセキュリティリスク評価のフレームワークの例示の追加が望ましいと考えます。 理由：事業者が本書に基づく優先付け判断の運用設計を実施する中では、事業者別の事情を踏まえた各判断ノードの判断基準設計が必要と理解しております。基準設計の際に依拠できる既存のフレームワークがわかると、判断基準具体化・明確化に寄与し、優先付けの妥当性も対外的に説明しやすくなると期待されます。 例えば、71頁の「ユーザー影響度」には、自動車業界のサイバーセキュリティ規格であるISO/SAE 21434がimpact ratingに用いるSFOP（Safety, Financial, Operational, Privacy）の観点・基準を援用し得ると考えます※出所6。 ※出所6　ISO/SAE 21434:2021（URL割愛）	いただいた御意見も参考に、修正いたします。「組織カテゴリーごとの優先付け判断方法」表の下に「判断ノードの各々について、企業の既存利用のフレームワーク、業界のフレームワークを参考とすることも考えられる。」を追記します。
39	9	8	組織	7.4.2.(4) p73, 7.4.3. p74, 7.4.4. p77	意見内容 ：優先度スコアの評価結果の、情報共有フェーズ・脆弱性対応フェーズでの活用方法例示の追加が望ましいと考えます。 理由：「(4) 優先度スコア評価」の目的は、スコアリングをすること自体ではなく、その後のプロセスを脆弱性毎に濃淡を付けて、総体としてセキュリティリスクを最小化することと理解しております。 「7.4.3. 情報共有フェーズ」「7.4.4. 脆弱性対応フェーズ（暫定対応・根本対応）」に、優先度スコアに応じてどのように対応を変化させるかを記載することで、優先度スコアの活用が進むと期待されます。 例えば、優先度スコアの高い脆弱性には、以下の様な対応が推奨されると想定しております。なお、例示を追加頂く際は、既存のサイバーセキュリティ関連法規・規格・ガイドライン・ベストプラクティス・学術研究等を踏まえて例示内容を検討すべきところ、本稿の例示は必ずしもそのような裏付けはございませんので何卒ご容赦頂けたら幸いです。 ・共有相手の範囲を、優先度低い脆弱性より広く設定すべき ・ソフトウェア利用者もプル型通知で開発者に情報共有を要求すべき ・関連当局からの指示を待たず、情報共有・進捗報告をプッシュ型で実施すべき ・アクセス権限の特定を、暫定対応が完了するまでは限定的な範囲に設定すべき（暫定対応完了までに悪用され重大な影響が発生するのを防止するため） ・(4.2)脆弱性根本対応の目標完了時期を短期に設定すべき ・高スキル人員配置・機動的な予算配分等リソースを優先的に確保すべき ・進捗確認を厳密に実施し、進捗報告等のコミュニケーション頻度を高めるべき	いただいた御意見は、記載内容の今後の修正に当たって参考にさせていただきます。
40	9	9	組織	7.4.2.(4) p73	意見内容 ：優先度スコア評価のウェイト設定に関する記述につき、以下の追加が望ましいと考えます。 ・参考ウェイトの導出根拠 ・「個社ごとの優先ポリシーに応じてウェイトを調整する」際、調整後のウェイトの妥当性を検証する作業や、取引先との調整を推奨する、以下の様な記述 「個社ごとの優先ポリシーに応じて調整したウェイトから脆弱性に対し妥当な優先度設定が可能か、脆弱性対応の実務に適用前に検証することが望ましい。検証方法として、過去の脆弱性対応事例のうち、深刻度が異なる複数の例を抽出の上、調整したウェイトで優先度設定を実施し、妥当とは言い難い優先度設定とならないかを検証することが挙げられる。また、取引先と脆弱性対応を共同で実施する場合、調整したウェイトが取引先と合意可能かという点も重要である。」 理由：参考ウェイトの導出根拠・前提条件が記載されていないと、本書に記載の参考ウェイトをそのまま適用する場合にそ理由を事業者内部で説明することや、事業者がウェイトを調整する際に調整すべき箇所の特定・その理由説明をすることが困難になると懸念されるため、参考ウェイトの導出根拠の追記を要望します。 また、個社別のウェイト調整余地を与える場合も、サプライチェーン全体でのサイバーセキュリティリスク削減の観点から、調整結果の妥当性の検証が実施されるのが望ましいと考えます。	いただいた御意見は、記載内容の今後の修正に当たって参考にさせていただきます。

41	9	10	組織	7. 全体	意見内容 ：本書の脆弱性対応プロセスに基づく脆弱性対応のケーススタディの追加が望ましいと考えます。 理由：本書の脆弱性対応プロセスは、事業者各位で業務プロセスや判断基準等具体的な運用設計への落とし込みが必要と理解しております。運用設計でどの程度具体的に検討が必要かを把握できるよう、本書の脆弱性対応プロセスに基づく脆弱性対応のケーススタディの追加を提案します。 ケーススタディは、脆弱性の事例を挙げ、それに対し事業者が脆弱性管理プロセスに則りどのように作業・判断評価していくかを解説するものです。 事業者が脆弱性管理プロセスの運用イメージを具体的に把握できることがゴールです。 弊社が想定しているケーススタディのイメージを把握頂くための参考として、ISO/SAE 21434のAnnex Hを参照することを推奨します。自動車のヘッドランプシステムを例に、ISO/SAE 21434が定めるサイバーセキュリティ脅威分析・リスク評価をどのように実施するかが紹介されております※出所6。 ※出所6　ISO/SAE 21434:2021（URL割愛）	いただいた御意見は、記載内容の今後の修正に当たって参考にさせていただきます。
42	10	1	組織	全体	BSA｜The Software Alliance（BSA｜ザ・ソフトウェア・アライアンス、以下BSA）（1）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 ver 2.0 （案）」（以下、手引案）に関し、経済産業省（以下、貴省）に意見を提出する機会（2）を得られたことに感謝します。 BSAは、政府やグローバル市場において、世界のソフトウェア産業を代表する主唱者です。BSAの会員企業は、世界で最もイノベーティヴな企業であり、企業や政府の競争力と効率性を高めるソリューションを提供することで、デジタルトランスフォーメーション（DX）の推進に貢献しています。BSAの会員企業は、IDおよびアクセス管理、データアナリティクス、クラウド・ストレージおよびデータ処理サービス、CRM（顧客管理）ソフトウェア、人事管理プログラム、コラボレーション・システムなど、様々なツールを提供しています。 ソフトウェアのセキュリティに関しては、BSAも貴省と同様の懸念があります。サイバーセキュリティに関する提言をまとめたBSAの「2024 Global Cyber Agenda(2024年度グローバル・サイバー・アジェンダ、以下、アジェンダ)」（3）においては、「ソフトウェア・セキュリティの強化」を最優先事項としています。 ソフトウェア・セキュリティの向上には、多面的なアプローチが必要です。BSAのアジェンダではSBOMに関する考えも示しており、SBOMの標準化に向けて産業界と政府が継続して協力していくことを推奨しています。SBOMは万能薬ではありませんが、顧客がSBOMを利用する準備が整えば、インシデント対応を迅速化することが可能となります。この点に関し、貴省が企業の自主的取り組みを支援し、SBOM導入の課題とメリットを評価するための実証をいくつかの産業分野で実施したことを我々は高く評価しています。	本手引に対する肯定的な御意見として承ります。

43	10	2	組織	2.5	＜SBOM（Software Bill of Materials）は有望だが限定的なツールであると認識すること＞ 最新のソフトウェア、特にサービスとして提供されるクラウドベースのソフトウェアには、状況に応じて変化する、動的（ダイナミック）なコンポーネントの一覧が利用される可能性が高く、これらのコンポーネントの数は数千になることもあります。このようなコンポーネントの動的な特性と数は、SBOM の作成と活用の両方を複雑にします。このため、SBOM によってサイバーセキュリティを確実に向上させるには、慎重な検討が必要です。手引案が示すように、SBOM は効率的なソフトウェア管理のために利用することは可能ですが、SBOM を実装する上では、対処しなければならない様々な課題があります。SBOMは、現在開発されているツール、標準、自動化と組み合わせることで、サイバーセキュリティを向上させますが、包括的な解決策ではありません。SBOMは、広く信頼されるために必要な成熟度にはまだ達しておらず、現段階では一般的に利用されている規格も存在しません。例えば、コンポーネント名を決定する、グローバルな単一の規程された手法はありません。そのため、二つの異なるSBOM作成者が同じコンポーネントに対して二つの異なる識別子を使用する可能性があります。これは、ソフトウェアコンポーネントのサプライヤーが、それぞれのニーズに応じてコンポーネント名を定義するからです。さらに、特定の SBOM フォーマットのバージョンは、製品に含まれるコンポーネントの記載に加え、脆弱性の記録に使用することができますが、それはフォーマットの意図された用途ではありません。製品のリリース後に脆弱性が発見されたり、脆弱性の特性が変化することもあります。したがって、脆弱性が発見・変更される度にSBOM全体を再公開することは、非効率です。 多様な主体が参加するサイバーセキュリティのコミュニティは、検証可能な精度を備えた SBOM の作成に取り組んでいます。手引案の「2.5. SBOMに関する誤解と事実」で触れているように、SBOM にソフトウェアコンポーネントに関する既知の脆弱性が記されたとしても、 それが必ずしも、SBOMで示されているソフトウェアが脆弱であるということにはなりません。例えば、手引案の脚注 17 に記されているように、一部の実務者は、ソフトウェアの脆弱性を機械判読可能なかたちで自動分析できる方法の 一つとして、SBOM および製品のメタデータをVEX（Vulnerability Exploitability eXchange）と組み合わせることをしています。これにより、脆弱なコンポーネントが脆弱な製品につながるかどうかを判別することが可能となります。このような取り組みは、SBOMを実用的かつ有益にしていく上で、非常に重要となります。	お寄せいただいた御意見に関して、SBOMがソフトウェア管理に向けた一手法であることは手引に多数記載しており、対処しなければならない課題があることも記載しております。また、部品IDに一意性がない課題についても言及しているほか、VEXと組み合わせることで効果的な脆弱性対応が可能となることについても記載しております。
44	10	3	組織	2.5	＜クラウド環境特有の課題＞ 手引案の「2.5. SBOMに関する誤解と事実」では、「コンテナイメージに対するSBOM、SaaS ソフトウェアに対するSBOM、クラウドサービスに対するSBOM 等のオンラインアプリケーションに対するSBOM の議論も米国を中心に行われている」と記されています。この点に関し、クラウド環境特有の課題があることを挙げておきます。例えば、SaaS（Software-as-a-Service）におけるアップデートやパッチは、通常、継続的に（自動化されて）行われ、脆弱性の迅速な解決につながっています。このため、SBOMをクラウドの文脈で採用しても、すぐにSBOMが最新状態を反映していないこととなり、効果を発揮できません。このため、SBOMを自主的に導入する上では、オンプレミス・ソフトウェアの方が実装上の課題が少ないかもしれません。	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。
45	10	4	組織	全体	＜SBOMに含む詳細のレベルを制限することにより、SBOMの普及と利用を促進する＞ BSA は、SBOM の開発と利用を支持しますが、少なくとも当面は、SBOM に含む情報の範囲を限定し、SBOMの土台を構築することに集中することを推奨します。SBOMに含む情報の詳細と範囲を限定することで、企業はSBOMのメリットをより早く享受することが可能となります。このアプローチは、産業界がより詳細で包括的なSBOMを実施するために必要な人材、プロセス、技術を開発するにつれて、追加条件を構築する可能性を排除するものではありません。	お寄せいただいた御意見は、手引やSBOMに関する更なる検討・取組を進めていくに当たって参考にさせていただきます。

46	10	5	組織	2.5	＜デジタルな要素を特定の状況で使用する製品のみにSBOMを推奨すること＞ SBOMの利用を推奨するのは、特定の文脈で使用されるデジタルな要素（エレメント）を持つ製品に限定するべきです。初期段階において、SBOMが特定の状況で利用されることがあるかもしれません。「2.5. SBOMに関する誤解と事実」では、「SBOM を公開する必要はなく、SBOM 作成者やサプライヤーの判断でSBOM の共有方法を判断することができる」と記されています。また「SBOM はソフトウェアに含まれているコンポーネントの一覧リストであり、特許やアルゴリズムは含まれておらず、知的財産を公開するものではない」とも記しています。ここで言及されているように、SBOMの公開は、製品のセキュリティだけでなく、知的財産に対するリスクももたらす可能性があることを強調しておくことが重要です。本記載にあるように、SBOM だけではソースコードのような機密性の高い企業秘密は提供されませんが、他の専有情報が含まれる可能性があります。例えば、特定の製品を製造するために使用されるソフトウェアプロバイダ、ベンダー、およびパートナー等の特定の組み合わせです。これらは貴重な知的財産および専有情報を構成するものです。企業は、SBOM を顧客に提供することはできますが、その情報を公開したり、秘密保持契約などの適切な保護措置なしにその情報を開示したりすることを要求されるべきではありません。また、脆弱性の開示に SBOM を使用したり、技術文書に SBOM を完全に含めることは、悪意ある行為者による脆弱性の悪用を招くことになりかねません。 最後に、SBOMを理論から具体的なセキュリティ改善につなげるためには、欠落している要素を特定し、埋めることが必要となります。現在、このために産業界と政府による重要な取り組みが進んでいることを強調しておきます。この取り組みが完了する前にSBOMを実施することに対し、政府は引き続き慎重であるべきです。 ＝結論＝ BSAと会員企業は、ソフトウェアの脆弱性を制御し、ソフトウェアのセキュリティを強化するという目標を支援するために、貴省に協力していけることを期待しています。SBOM はこの取り組みの重要な一部です。また、BSA会員企業を含む、グローバルなソフトウェアベンダーが議論に貢献し、詳細な提言をすることを可能とするために、今後は意見募集の段階で手引案の英訳を準備することを奨めます。本取り組みに我々がどのように協力できるかを話し合う機会を頂ければ幸いです。 ＜脚注＞ （1）BSAの活動にはAdobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Cohere, Dassault, Databricks, DocuSign, Dropbox, Elastic, ESTECO SpA, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc. が加盟企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。 （2）https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595224009&Mode=0 （3）https://www.bsa.org/files/policy-filings/2024cyberagendabsa.pdf	御意見を踏まえ、2.5節のSBOMに関する誤解と事実において、専有情報が含まれる可能性について言及いたします。 また、意見募集段階での英訳については、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。

47	11	1	組織	1. 背景と目的（特に1.2および1.5）	本手引の位置付けや記載された活動の主体をより明確に追記していただくのが良いと考える。 背景として欧米の動向が述べられており、そうした関係諸国の政府や市場の動向を見て自らSBOM導入の要否を判断することを期待されている文書と推察するが、明確な記載は見当たらない。 また、本手引では、述べられている様々なポイントを認識した上でSBOM導入を進めることを「要求する」、もしくは「望む」、もしくは「期待する」といった記述に対して主語が無く、これらの主体が不明である。本手引の発行元（経済産業省）が特に推奨しているとの明確な記載も見当たらない。 日本の産業界としてSBOM導入に今取り組むべきなのか、どういった要請の応えるべきか、予算確保や体制構築の判断材料として本手引は重要であると考えており、そうした点を追記していただければと考える。	御意見として承ります。 本手引は経済産業省にて発行しており、1.6節において、「SBOM 導入に向けた具体的な取組を進めることが期待される」旨を記載しております。
48	11	2	組織	2.2 SBOM導入のメリット	P.14 の8行目に「サプライチェーン上で第三者によりコンポーネントの書換えや不正な追加が行われた場合にも、その実態把握に資するものとなる」とあり、本手引ではSBOMを出力する際にSBOMの出力者は現物と整合を取り、サプライチェーン間はSBOMの正確性を契約で担保する運用が想定されているように読める。 しかし、ここにあるように第三者の介入やそもそもミスによって脆弱性のあるライブラリの情報が含まれていなかった場合、SBOMから得た構成情報からは脆弱性のあるライブラリの情報が取得できずSBOMのメリットを生かしきれないと考えられる。 そのため、サプライヤーからSBOMとソフトウェア（コンポーネントやライブラリ等）を受け取る場合でも、その二つの整合性をバイナリ解析等で確認する必要があると考える。	御意見を踏まえ、5.2節において、サプライヤーからSBOMとソフトウェアを受け取る場合の整合性確認に関する記述を追記いたします。
49	11	3	組織	7.4.1 脆弱性特定フェーズ	記載されている「API」が何を指しているのかが不明瞭である。 表7-1で脆弱性マッチング区分の１つとして何のAPIを利用できると述べているのかが不明瞭である。MyJVN APIのような脆弱性データベースのAPIと推察するが、明確な記載はない。 こうしたことに明るくない読者にも理解できるよう、可能な限り具体例を記載することが良いと考える。同様にWeb UI利用についても、現在利用可能なWeb UIの例を挙げると良いと考える。	いただいた御意見も参考に、修正いたします。表7-1の脚注に、APIの説明と公的な例を追記しました。
50	11	4	組織	8. 付録：SBOM対応モデル　および　9. 付録：SBOM 取引モデル	SBOM対応モデルとSBOM取引モデルが付録とされている意図を追記されるのが良いと考える。 7章までの内容も、SBOMの導入において特に推奨しているのではなくリファレンスという論調になっているため、付録とされているのは、これらモデルはあくまでリファレンスであり、業界や個社で最適なモデルを設計すれば良いとの意図と推察するが、1.5あるいは8.の冒頭等で簡単に説明があると良いと考える。	いただいた御意見は、ガイドライン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。

51	11	5	組織	8.2.2. 基本的な考え方と期待される効果	効果２について、「SBOM 対応範囲を可視化することで脆弱性管理レベルの高さを示すことが可能になる。これにより調達者の評価が高まり、製品の価値が高まる。」と言えるためには、例えば表8-2等に示されたSBOM対応範囲の可視化フレームワークを用いて、どの範囲まで対応できていれば調達者側にとって脆弱性管理レベルが高いと言えるかについての広範なコンセンサスが必要と考える。 脆弱性管理を重視する調達者ほどSBOMに高い網羅性と精度を期待するが、そのために必要となるコストも高くなる。現状、完璧なSBOMを作成することは技術的にもコスト的にも困難であり、各国政府機関が要求するレベルやコスト対効果を踏まえた妥当な水準作りの重要性にも触れていただければと考える。	いただいた御意見は、ガイドライン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。
52	11	6	組織	8.2.3. SBOM 可視化フレームワーク	表8-2および表8-3において、SBOM対応範囲における対応項目選択肢の対応区分を４種の色のみで分類されているが、この淡い色分けは色覚弱者にとって区別しにくいと考える。それ以外の人にとっても、各色の意味を覚えていないと区別がつき難い。 対応区分の上位ほど文字サイズを大きくする、太字にする等、形状でも判別できる配慮があると、その点もSBOM対応範囲の可視化手法として参考になると考える。	いただいた御意見も参考に、修正いたします。フォントサイズ、太字で対応致しました。
53	12	1	組織	１．全体について	ー経済産業省が発表したガイドラインは、主要なサイバーセキュリティリスクの一つであるソフトウェアサプライチェーン攻撃について市場を啓蒙するための非常に有用な文書であると考える。 （MergeBase believes that this guideline is an extremely useful document to educate the market on one of the key cybersecurity risks, software supply chain attacks.） ー御省のタスクフォースでも検討されているが、日本は輸出主導型の経済であり、主要な輸出市場として 米国とEUに大きく依存している。これらの市場では、異なるアプローチが取られている。EUではCRA(サイバーレジリエンス法)、米国ではCISA(米国サイバーセキュリティ・インフラセキュリティ庁)の「セキュア・バイ・デザイン」である。後者は「自主的」であり、日本の経済産業省のガイドラインに類似している。 （As discussed in the task force of METI, Japan is an export driven economy and relies heavily on the US and the EU as key export markets. In those markets, different approaches are pursued. The CRA in the EU and the “Secure by Design” from CISA in the US. The last is “voluntary,” and so similar to METI’s guidelines in Japan.） ー米国とEUに輸出する日本企業は、今後数年のうちにこの政策に従わざるを得なくなるだろう。それを支援するためには、経済産業省が本ガイダンスとこれら2つの政策とを連携させる努力をすることが有益であろう。 （These two initiatives likely will force Japanese exporters to comply in the next few years. To help Japanese exporters be successful with compliance in these markets, it will be beneficial to make more efforts to align METI’s guidance with these two initiatives. ） ー表面的には米国とEUのアプローチは非常に異なっているように見えるが、規制するかどうかという要素を取り除けば、両者の取り組みはよく似ている。 （On the surface European and US approaches look quite different, but if you remove the element of regulation, they are quite similar.） ーEUと米国のアプローチは経済産業省が今回ガイドラインで示した政策と似通っているが、対象範囲はより広範で、ソフトウェアのサプライチェーンセキュリティに関する詳細な記述、解説は少なく、一般論として検知された脆弱性が（時間を経て）排除されることを求めている。 （The EU/US approaches are broader but do overlap with the area of METI’s guidance. They have less detail on software supply chain security and set out more a general expectation that known vulnerabilities will be eliminated (over time).） ーソフトウェアサプライチェーンのグローバル化の中で、日本のソフトウェア産業及びこれを利用する日本の製造業を含む産業全体の競争力を確保	本ガイドラインに対する肯定的な御意見として承ります。いただいた御意見は、ガイドライン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。ご指摘の点は重要な課題と認識しています。

					し、また海外製品・サービスを輸入・利用する産業及び日本国民をサイバーセキュリティリスクから守るために、日本と海外、特にEU/米国のサイバーセキュリティ規制の相互運用性を確保していくことが重要だと考える。 （With the globalization of the software supply chain, in order to ensure the competitiveness of the Japanese software industry and Japanese manufacturing and other industries that use this industry as a whole, and to protect Japanese citizens and industries that import and use foreign products and services from cybersecurity risks, we believe that it is important to ensure interoperability between Japan and foreign countries, especially the EU/US. We believe that it is important to ensure interoperability of cybersecurity regulations between Japan and foreign countries, especially the EU/US.） ー分析と優先順位付けに関する多くの議論があるが、これは事実上すべての大組織で見られることである。 しかし、経済産業省は、確認された脆弱性について、長期的にどのように考えているのだろうか？明確なビジョンを示すことは、大きな価値をもたらす。 確認された脆弱性を将来にわたって許容するのか？ もしそうでないならば、脆弱性を排除するために、ソフトウェア開発エコシステムにおける様々なプレーヤーはどのような役割を果たす必要があるのだろうか？　日本政府としての政策目標、最終的なゴールは何か、それを明確化することが日本の産業、国民にとって望ましいと考える。 （There is a lot of discussion around analysis and prioritization, which is something we see in virtually every large organization. However, what is the long-term view of METI on the topic of known vulnerabilities? It might provide a lot of value to state a clear vision. Are known vulnerabilities acceptable in the future? If not, what is the role of different players in the software development ecosystem to eliminate known vulnerabilities? We believe that it would be desirable for Japanese industry and citizens to clarify what the policy objectives and ultimate goals of the Japanese	
54	12	2	組織	２．P.24　表2-6	意見内容 ーNTIAが最小要素で規定しているデータ項目として、SBOM作成者（Author of SBOM Data)の提出を要求している。しかし、我々の経験では、オープンソースプロジェクトは、このSBOM作成者情報について、信頼に足る十分な一貫性と品質で提供していない。手書きでは、有効となりそうだが、ツールでは意味のないデータとなりうるので、ツールベンダーへの要求もしくは、使用上の注意事項とすべきである。 （The NTIA minimum elements set requires the AUTHOR filed. However, in our experience, open-source projects do not provide this information with sufficient consistency and quality for it to be relied upon. It may be valid for handwritten data, but it may be meaningless for tool data, so it should be a requirement for tool vendors or a precaution for use.）	お寄せいただいた意見に関して、作成されたSBOMの内容について検証・確認することの重要性は既に手引に記載しております。
55	12	3	組織	３．P.30　2.5 SBOMに関する誤解と真実　誤解：SBOM のフォーマットとして、SPDX、CycloneDX、SWID タグの3つのフォーマットのみが認められており、独自フォーマットに基づくSBOMは認められない	意見内容 ーソフトウェアサプライチェーンセキュリティの発展を妨げている主な問題の一つは、特定の標準がないことである。米国NTIAに始まり、すべての政府は、SPDXがISO標準になったにもかかわらず、特定の標準にコミットすることを避けてきた。このことは、業界やツールベンダーがすべての標準に対応しなければならず、多くの追加作業が発生し、進歩が遅れることを意味する。 （One of the main issues in holding back the development of software supply chain security is the lack of a specific standard. Starting with the US NTIA, all governments have shied away from committing to a specific standard, even though SPDX has become an ISO standard. This means that industry and tool vendors have to cater for all standards. This creates a lot of additional work and slows down progress.） ー経済産業省は、望ましい技術標準（複数可。ただしグローバルに通用するもの）を指定することを検討すべきである。そうすれば、エコシステム内のすべての関係者にとって長期的な効率性が生まれる。ただし、一部の関係者には短期的な痛みを伴うかもしれないが。 （METI should consider specifying a preferred technical standard, but one that is globally accepted. That will create long-term efficiencies for all parties in the ecosystem. Although it might create some short-term pain for some.） ーツールとして、MergeBase社製品のように、SPDX、CycloneDXのインポート、エクスポート機能を標準装備しているものを推奨すべきと考える。 （As a tool, we believe that METI should recommend the product that has SPDX and CycloneDX import and export capabilities as standard, such as the MergeBase product.）	いただいた御意見は、ガイドライン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。現在、CISA, EUなどにおいても特定の標準を選定していないことから、国際整合の観点で今後検討を進めたいと存じます。

56	12	4	組織	4．P.145 10.3.2.　SBOMに関するツール (1)有償ツール	意見内容 　ーこのツールリストに、後述のようにMergeBaseを加えていただきたい。 　（It is our hope that you will add our MergeBase to this list of tools described below.） 名称MergeBase 開発者　MergeBase Software Inc. 特徴 ーMergeBase は、コードとバイナリをスキャンし、脆弱性情報、ライセンス情報、年数情報、推移的依存性情報を含んだSBOM を生成して管理するアプリケーションを統合したソフトウェア サプライチェーン セキュリティ ソリューションで、脆弱性を効率的に分析し、修復を行う。 ーMergeBaseは、アプリケーションへの攻撃対象領域を自動的に縮小し、組織が脆弱性にさらされるリスクを減らすとともに、改善方法を提案することで、ソフトウェア開発エンジニアがコードを修正するために必要な労力を劇的に削減する。 ーMergeBaseは日本の脆弱性ノート（JVN）を完全に統合している。 ー日本では、Meristem Inc.をパートナーとして提携し、マニュアル等ドキュメントの翻訳、日本語による技術サポートを提供している。	御意見を踏まえ、7.3.2項において、 MergeBaseに関する記載を追加いたします。
57	13	1	組織	「9.8. 課題と今後の検討の方向性」 「●取引モデルの規定事項の契約書条項化」 　・・・既存のソフトウェア開発一般の請負契約と、SBOM 取引モデルの条項案を契約書雛形として一体化することによりSBOM モデル契約書に発展させることができる。 「●SBOM取引モデルの解説書」 　ソフトウェア	・意見内容 　既存のソフトウェア開発モデル契約書をベースにSBOM取引モデルの規定事項を反映した契約書を作成するのはSBOM取引モデルの利用者であることを明確にする必要があります。 従って、下記のように修正すべきだと考えます。 「●取引モデルの規定事項の契約書条項化」 　・・・既存のソフトウェア開発一般の請負契約と、SBOM 取引モデルの条項案を、SBOM取引モデルの利用者が一体化した上で契約書雛形として発展させることができる。 「●SBOM取引モデルの解説書」 　SBOM取引モデルの利用者が、ソフトウェア開発モデル契約書にSBOM 契約書条項を統合した契約書雛形を作成し、各条項に対する活用法の解説を示すことが期待される。 ・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。） 　参照されている「JEITAソフトウェア開発モデル契約の解説」では、SBOMに関する条項を加味しておらず、ソフトウェア開発モデル契約書にSBOM 契約書条項を統合するのは、SBOM取引モデルの利用者であることを明確にする必要があるため。	いただいた御意見のとおり、9.8節を修正いたします。
58	14	1	組織	・全体	全体的なボリュームが多いため、SBOM の導入部分と活用部分を分けて二分冊とすることも検討すべきと感じます。	いただいた御意見は、ガイドライン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。章の依存関係を考慮し、分冊化の検討を致します。

59	14	2	組織	・4.2. SBOM ツールの選定 ・4.3 SBOM ツールの導入・設定 ・10.3.2. SBOM に関するツール	ツールの選定を「有償」と「無償」で分類し整理されています。 OSSとして公開されているものを無償ツールに分類した上で、学習コストと設定情報の不足を無償ツールの劣る点として挙げています。 たしかに「無償の SBOM ツールは OSS コミュニティを中心に活発に開発されているため、機能・性能が向上していく可能性があることに留意する必要がある。なお、無償の SBOM ツールに関するサポートサービスを提供している企業もあり、無償の SBOMツールを活用する場合に必要に応じて支援を受けることも想定される。」との記載はありますが、例えば「10.3.2. SBOM に関するツール」で無償ツールに分類されている “Trivy” のように有償のサポートサービスが提供されており、有償ツールと同等の情報を入手することができるものについては、その旨を記載しないと読者に誤解をあたえるのではないかと懸念されます。	表4-2の「サポート体制」に関する記載において、お寄せいただいた内容に関する記載がございます。
60	14	3	組織	・図 2-6 簡易シナリオにおける SPDX フォーマット（Tag-Value 形式）の SBOM 例	SPDX フォーマットはどのバージョンによるものか、注釈などを入れるべきと考えます。SPDX は現在も活発に開発が進められており、バージョンにより具体的表記方法が異なります。バージョン情報を記載することで、読者はより正確な理解を得ることができると思われます。	御意見のとおり、当該箇所を修正いたします。
61	14	4	組織	・7.2. 脆弱性管理における課題・問題認識	「また、脆弱性DB は複数存在し、脆弱性情報の網羅性を高めるには対象とする脆弱性の拡大が課題となる」の意図がわかりにくいと感じます。 複数の DB を参照して脆弱性情報を収集すべきという意味でしょうか？ある脆弱性 DB に格納されている脆弱性情報を拡充すべきという意味にも取れます。	いただいた御意見を踏まえ、修正いたします。
62	14	5	組織	・7.4.1. 脆弱性特定フェーズ (3) 対象とする脆弱性 DB の選択	誤記と思われる個所があります。 ・誤 ： 個社ごとに脆弱性DB を選択するこが期待される ・正 ： 個社ごとに脆弱性DB を選択することが期待される	いただいた御意見のとおり、修正いたします。
63	14	6	組織	・7.4.2. 脆弱性対応優先付けフェーズ (3) 優先付け判断ツリーに基づくカテゴリー判定	表記揺れと思われる個所があります。 ・図 7-7 内：「悪用効率性」「技術的深刻度」 ・図 7-8 内：「悪用容易性」「技術的影響度」 SSVC の「Utility」と「Technical Impact」を翻訳した際、日本語の語句選択が揺れているものと推測します。	いただいた御意見も参考に、修正いたします。「悪用効率性」「技術的影響度」に統一します。
64	14	7	組織	・7.4.2. 脆弱性対応優先付けフェーズ (2)優先付け情報の選択・取得 (3)優先付け判断ツリーに基づくカテゴリー判定	(2) 表7-2「脆弱性対応優先付けに必要な情報一覧」と、(3) 「組織カテゴリーごとの優先付け判断方法」内の各要素の関係が不明確に感じます。この間の関連をガイドする解説があると、読者の理解を促進できると考えます。	いただいた御意見も参考に、修正いたします。表7-3の前に、表7-2と表7-3の関係と位置付けを示します。

65	14	8	組織	・8.2.3. SBOM可視化フレームワーク	「(a3)サプライヤ（サードパーティ）取引契約なし」の場合に OSS が一律でコスト大になり SBOM 管理レベルが低いと読み取れますが、OSSコミュニティの活動も評価の考慮に入れるべきかと思います。 例えば ・OpenSSF の Scorecard によるプロジェクト品質の高低評価 ・重要なプロジェクトについて精査した Alpha-Omega プロジェクト ・OSS をサポートするベンダーの利用も有効	いただいた御意見は、ガイドライン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。挙げて頂いたOSSコミュニティの活動も踏まえ、SBOM対応モデルで可視化するための具体化の検討が出来ればと存じます。
66	15	1	組織	10.3.2. SBOMに関するツール(1) 有償ツール	以下のツールの掲載についてご検討お願いいたします。 名称：Finite State Platform 開発者：Finite State, Inc. 特徴： ・SBOMおよび脆弱性の統合管理プラットフォームを提供 ・バイナリ・ファームウェアからコンポーネントを可視化しSBOMを生成 ・組み込み機器の様々なアーキテクチャに対応 ・SBOMおよび、150種類以上の他社ツールの診断結果を取り込むことで脆弱性の一元管理が可能 ・攻撃発生状況など緊急度の高い脆弱性をトリアージし、対応優先度を判断可能 ・SaaS、プライベートクラウド、オンプレミス、ニーズに合わせてご提供 ・理由 他社には無いツールの特徴により、SBOM生成および管理において有益でありSBOM普及促進に貢献できるため	御意見を踏まえ、7.3.2項において、Finite State Platformに関する記載を追加いたします。
67	16	1	組織	15ページ「OSSライセンス違反による訴訟事例が複数存在し、例えば、2010年に家電メーカーら 14 社が GNU General Public License（GPL）違反で起訴された事例」	追加された7 - 9章に関し、対応優先度の評価が提供者と利用者で異なることがトラブルを生むなど、SBOMの脆弱性管理への活用に向けての具体的な課題と対策の例が記載されており共通理解を広めることに非常に有益な文書だと思います。ありがとうございました。 いくつか改善できそうな点やコメントがありましたので以下に記載します。 ・意見内容 家電メーカーら 14 社が GNU General Public License（GPL）違反で起訴された事例は、2010年ではなく2009年（12月）ではないでしょうか？ ・理由 おそらくこの事例（https://www.itmedia.co.jp/enterprise/articles/0912/15/news084.html）を取り上げておられるのかと推察しました。	御意見のとおり、当該箇所を修正いたします。

68	16	2	組織	15ページ「例えば GPL の場合、派生物も GPL が適用されるほか、GPL を他のソフトウェアと組み合わせて新たなソフトウェアを作成した場合、当該ソフトウェアにも GPL が適用される。」	・意見内容 該当箇所の後半部分である「当該ソフトウェアにも GPL が適用される。」という表現はGPL汚染（またはGPL感染）を想起させる表現であり適切ではないと思われます。「例えば GPL の場合、派生物も GPL が適用されるほか、GPL を他のソフトウェアと組み合わせて新たなソフトウェアを作成し頒布した場合、当該ソフトウェアは全体としてGPLが課す条件 に従わなければならない。」とするのはどうでしょうか。 ・理由 たしかにGPLと組み合わせたソフトウェアはGPLが課す条件に従わなければならないものの、GPLが課す条件に従う必要があるというにすぎず、そのソフトウェアのライセンス自体がGPLになる（GPLが適用される）わけではないためです。 （参考：https://licenses.opensource.jp/GPL-2.0/GPL-2.0.html　第２章　第２段落）原文：https://www.gnu.org/licenses/old-licenses/gpl-2.0.html	御意見のとおり、当該箇所を修正いたします。
69	16	3	組織	「どこでも(一案として4.2 SBOMツールの選定)」	・意見内容 参考情報としてビルド時にSBOMを自動生成する例を記載していただけると嬉しいです。 YoctoでのSBOM(SPDX)作成方法 https://docs.yoctoproject.org/dev/dev-manual/sbom.html AOSPでのSBOM(SPDX)作成方法 https://source.android.com/docs/setup/create/create-sbom?hl=ja ZephyrでのSBOM(SPDX)作成方法 https://docs.zephyrproject.org/latest/develop/west/zephyr-cmds.html ・理由 一般的に利用されている大きなプロジェクトでビルド時にSBOMを自動生成するビルド環境、ツールの利用例が公開されているためです。	御意見を踏まえ、5.1節において、ビルド時にSBOMを自動生成する例を参考情報として追記いたします。
70	16	4	組織	p135 10.2.1. SBOM やソフトウェアに関する用語の定義内「また、脆弱性 DB は複数存在し、脆弱性情報の網羅性を高めるには対象とする脆弱性の拡大が課題となる。」	・意見内容 「脆弱性情報の収集範囲を拡大して情報の網羅性を高める」という意図でしょうか。意図が読み取りづらく、言葉が抜けているように感じました。 ・理由 「脆弱性情報の網羅性を高めるには」と「対象とする脆弱性の拡大が課題となる。」の繋がりが分からなかったためです。"	該当箇所は7.2節と思われます。いただいた御意見を踏まえ、修正いたします。言葉を補い修正します。

71	16	5	組織	p81の「SBOM対応範囲を可視化することで脆弱性管理レベルの高さを示すことが可能になる。これにより調達者の評価が高まり、製品の価値が高まる。」の２文	・意見内容 調達者が非常に広いSBOM対応範囲を期待し供給者に過剰な負担とならないよう、両者が受け入れられるSBOM対応範囲に一定の基準を確立することが、上記２文が示す状態の実現には必要と考えます。その旨を一言添えていただくことはできますでしょうか。 ・理由 セキュリティに関わる判断の指標となる情報には、一般的に非常に高い網羅性や信頼性が求められ、コスト的・技術的に可能なSBOM対応範囲を可視化した場合に脆弱性管理レベルが高いと認められるとは限らないため。"	いただいた御意見を踏まえ、修正いたします。但し書きを加えます。「調達者によるSBOM対応範囲の要求は、調達者が一定の負担をするなど供給者に過剰な負担とならない仕組みが期待される。」
72	16	6	組織	p.81 「サプライチェーンを通じてSBOM 作成のコストを負担する者と、SBOM を用いた脆弱性管理の便益を受ける者が異なるため、それらの間で適正な対価が支払われなければ SBOM の普及の障害となる。」	・意見内容 SBOM作成コストはサプライチェーンのすべての場所で発生するので、そのすべてに対して適正な対価が支払われることが重要と思います。SBOMを用いた脆弱性管理の便益を受ける者が負担するという考え方による、供給者と調達者間での対価の支払いも効果的ですが、供給者は同時にさらに上流からの調達者でもあり、また、調達者のみならず最終のProductの利用者や社会全体が便益を受ける者と考えることができると思います。また、一人の供給者に対して複数の調達者という関係もあります。継続的な議論や試みが行われるところではないかと思います。 ・理由 -	いただいた御意見は、ガイドライン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。サプライチェーンを通じた便益とコスト負担について継続的に検討します。

73	16	7	組織	p.19, 2.4.「(1) SPDX（Software Package Data Exchange）」、他	・意見内容 SPDXについて、SPDX 2.3 までは記載の通り ""Software Package Data Exchange"" ですが、2024年4月に発行された SPDX 3.0 からは ""System Package Data Exchange"" を意味するものとしています。SPDX 3.0はプロファイルを導入することで、SPDX Lite としての Lite Profile は当然のこと、p.151にあるように Security Profile により脆弱性管理も扱うなどの拡張がなされています。同月にはCycloneDX 1.6のリリースがあり、こちらも扱う情報の拡張が図られています。また、いずれのSBOM仕様も相互のデータ交換性を向上させる努力が続いています。グローバルなソフトウェアサプライチェーンにかかるSBOMに関する議論が活発な情勢で最新動向の扱いは難しいところもあるかと思われますが、我が国の企業におけるそのような動向の把握にも支援を頂けると助かります。 ・理由 当該文書発行時期を鑑みての動向との整合性への配慮のため	御意見を踏まえ、SPDXの正式名称に関する補足説明を追記いたします。また、SPDX 3.0やCyclone DX 1.6のリリースに関する情報を追記します。加えて、フォーマットは今後も継続的にアップデートされることが予想されるため、最新バージョンの把握が望まれることを追記いいたします。
74	16	8	組織	p.20, 1行目他、「SPDX-Lite」の表記、及び、p.19, 最終行他、「必要最低限の項目のみ」とする説明、について	・意見内容 「SPDX Lite」が正しいつづりになります。SPDX 3.0, 同2.3の仕様書及び ISO/IEC5962 (SPDX Specification)もご参照ください。また、SPDX Lite について「必要最低限の項目のみ」とありますが、ISO/IEC 5230 (OpenChain Specification) が示すオープンソースライセンスコンプライアンスのプロセスマネジメント標準、ISO/IEC 18974 (OpenChain Security Assurance Specification) が示すセキュリティアシュアランスのプロセスマネジメント標準などで必要となるSBOMとしての要素を満たす程度に必要最小限のもの、として記載頂いていると推察します。そのように補足頂けるかご検討ください。 ・理由 明確化のため	御意見を踏まえ、「SPDX Lite」と表記を修正いたします。また、SPDX Liteの位置づけについて、御意見のとおり、当該箇所を修正いたします。
75	16	9	組織	p.155, 2行目、「SPDX のレベルではなく、」	・意見内容 該当箇所にある「レベル」が何を基準とするのかを明らかにして頂きたいです。SPDXが定義するプロパティ全体の粒度に渡るのではないことを意図すると推察されますが、文意を明確にして頂けると助かります。 ・理由 明確化のため	御意見を踏まえ、SPDX Liteの位置づけに関する記載を修正いたします。
76	16	10	組織	「どこでも(一案として10.2 用語集)」	・意見内容 SPDX3.0についてはRCの公開が言及されていますが、CycloneDX含め最新バージョンに関するSBOMフォーマットについて概要を言及されてはいかがでしょうか。この際、OpenChain Japan WGでもSPDX3.0への貢献(SPDX Lite)を行っているので、作成の際の議論に参加できる機会があると、仕様を作成しているコミュニティの考えも反映できるのではないかと考えております。 ・理由 CycloneDXは4/10にv1.6が、SPDXも4/16にv3.0が新しく発行され、どちらのフォーマットもセキュリティやライセンスコンプライアンスに特化したものでは無くなりつつあるためです。	御意見を踏まえ、SPDX 3.0やCyclone DX 1.6のリリースに関する情報を追記します。加えて、フォーマットは今後も継続的にアップデートされることが予想されるため、最新バージョンの把握が望まれることを追記いたします。

77	16	11	組織	p.2「OSS の再帰的な利用（再利用部品）」について	・意見内容 「再帰的な利用」についての他の箇所での記述では「再利用部品」とは思えないので、混乱しています。 「再帰的な利用」の定義を示していただくと理解の助けになると思います。 ・理由 p.29に「対象ソフトウェアが直接利用しているコンポーネントだけでなく、そのコンポーネントが再帰的に利用するコンポーネントについても把握しないと、脆弱性対応が不十分となる可能性がある。」とあるので、依存関係の連鎖の意味で「再帰的」と説明されていると思います。一方、p.30に「ランタイムライブラリのような実行時に動的に追加されるライブラリは、SBOM ツールがライブラリの実体を解析しないため、特定することができない。そのような場合は、パッケージマネージャー等を用いてライブラリに対する構成情報と実行環境を個別に用意し、SBOM ツールにそれを認識させることで再帰的なコンポーネントを特定できるようにする必要がある。」とあるので、「再帰的」なコンポーネントとは、実行時にリンク結合されるコンポーネントと思われます。企業間でSBOM対応レベルの調整の際にも共通に認識された用語があることは助けになると思います。	いただいた御意見も参考に、修正いたします。用語集に説明を追加しました。
78	16	12	組織	全般	・理由 SBOMについて、各国の行政、業界、コミュニティで議論が重ねられ、運用の広がりと並行して、これからも議論が続けられると思います。この手引はこれまでの議論や運用実態を踏まえてまとめていただいたものと思いますが、今後、SBOMのさらなる普及のための強制化の予定はありますでしょうか。	いただいた御意見は、ガイドライン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。今後、国際的な制度調和の観点で、検討できればと存じます。
79	16	13	組織	p.1 背景と目的	・意見内容 背景や目的など文書冒頭部分で消費者視点でのSBOMの必要性について少し触れていただけると嬉しいです。 ・理由 SBOMの本来の目的は消費者に安全・安心な製品やサービスを届けることのはずです。実際、海外のガイドラインや手引書のいくつかにおいては消費者保護の観点からの課題とSBOMが果たす役割が説明されています。 実際には消費者が詳細なSBOMを目にすることは無いかもしれませんが、消費者にとって、何故SBOMが必要になっているなどについて冒頭で少し触れていただけると嬉しいです。	御意見を踏まえ、1.1節において、消費者視点でのSBOMの必要性について追記いたします。
80	16	14	組織	全般	・意見内容 Executive Orderから始まり、Linux Foundation、CISA、OWASPなど世界中の資料を基に分かりやすく記載されており、グローバルなSBOMへの期待と各国法規制を見据えた資料となっていると感じました。今後も日本独自ではなく各国の動向を踏まえた文書アップデートを継続していただけると嬉しいです。 ・理由 -	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。
81	16	15	組織	「SBOMツール」のユースケースを説明している箇所全般	・意見内容 文中におけるSBOMツールの特定の機能に関する内容の場合は単に「SBOMツール」ではなく「SBOMツールのｘｘ機能」と書いていただけると理解しやすくなると思われます。 ・理由 SBOMツールについては2ページの脚注や、153ページの「10.2. 用語集」でご説明いただいておりますが、この説明通りSBOMツールにはさまざまな機能が含まれているため。	御意見を踏まえ、対象機能が限定される記載については、対象となるSBOMツールの機能を補足いたします。

82	16	16	組織	全般	・意見内容 このような手引きの整備にあたり、その作成段階からオープンなプロセスを設けることを検討を頂くのはいかがでしょうか。たとえば、米国CISA は自身がオーガナイズする SBOM関連のWorking Groupについて、米国に限ることなく各国の様々な組織や企業などが参加できるオープンなものとして運営し、課題やノウハウの共有、コンセンス形成、文書化とその公開を行っています。そこで、先にあるCISAのWorking Gourp にリエゾンをおき、日本時間で同じくオープンな議論の場を設けることで、国内向けの情報共有を図るとともに、国内での議論等成果をグローバルな文書作成にフィードバックすることや、CISAが公開するドキュメントの日本語版の提供などにも寄与する可能性があります。これは、SPDXやCycloneDXをはじめSBOMの標準化、SBOMの管理運用のコンセンサス形成、SBOM関連の技術開発等々に関心を持つ者の参加の敷居をさげるとともに、オープン化に基づくソフトウェア開発の強靱化にも連なると期待されます。SBOMはグローバルなソフトウェアサプライチェーンに係る事案のため、日本の産業界を支援する取組として検討頂けるとありがたいです。 ・理由 グローバルなソフトウェアサプライチェーンに向けて、我が国におけるよりセキュアなソフトウェア開発の導入推進策が望まれるため。	いただいた御意見は、ガイドライン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。今後、委員会形式と不特定多数が参加するオープンプロセスのメリット・デメリットの検討、類似実績などから検討できればと存じます。
83	16	17	組織	全般例）「有償の SBOM ツールと比較して、無償の SBOM ツールの機能・性能は限定的である場合が多く、例えば、再帰的な利用部品が検出できない、読み込み可能な SBOM フォーマットに制限がある、ライセンスの検知漏れが発生する、導入環境が限定される等の課題がある。」	・意見内容 全体を通して、有償ツールであれば無償のツールよりも完璧に運用できると読み取れる表現が繰り返し使われていますが、その裏付けとなる調査等はありますでしょうか。例えば、どのような制限がある、というような例を挙げていただくと理解が深まると思います。 ・理由 有償ツールでも無償ツールと同様に完全なSBOMを生成するには限界があるためです。	1.1節で記載のとおり、今回の手引は2021年度・2022年度に実施した実証（有償ツール・無償ツールの両方を活用）で得られた結果に基づき策定しています。また、無償ツールの課題についても1.1節などで記載しているほか、有償ツールであっても誤検出や検出漏れ等が発生する場合があることを記載しています。
84	16	18	組織	どこでも（一案としては巻末）	・意見内容 もし可能でしたら、巻末などに索引があるととても助かると思いますので次回改版時などにご検討いただけますと幸いです。 ・理由 151ページ以降で「10.3.3. SBOM のデータフォーマット」として SPDX / SPDX-Lite / CycloneDX / SWIDタグ 等が詳しく説明されているなど、135ページ以降の「10.2. 用語集」で説明されているもの以外にも文章中に専門用語が出てくる場所が散見され、かつ、ボリュームも多い文章であり、読みづらさを感じたため。	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。

85	17	1	―	7.2 脆弱性管理における課題・問題認識	・意見内容 多くの要件が「推奨」として記載されておりますが、一部の要件については「必須」としていくことをご検討いただけますと幸いです。 ・理由 IoT機器等のハードウェアを伴う製品にはPL法に基づき、顧客に販売された製品には10年間の保証が義務付けられております。そのため、SBOMの管理は必須であるべきと考えます。政府が公開する「手引」に「推奨」と記載されていると、多くの企業が必須ではないと判断し、その結果要件の実装が行われないケースが増えるのではないかと懸念しております。 脆弱性を管理することで製品の品質を高めるためにご尽力いただき作成いただいた手引きが、意図に反し、結果的に製品の品質を下げる方向へ働くことは避けるべきと考えます。 【出典：PL法第4章】	いただいた御意見は、ガイドライン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。分野により必須項目の違いがあり、業界関係者を交えた検討を継続します。
86	17	2	―	7.4 各フェーズの手順と方法	・意見内容 HWチップなども含むSBOM管理の重要性を明記し、ソフトウェアだけでなくハードウェアを含む脆弱性管理の推奨事項を追加いただけますと、さらに実効性が高まると考えます。 ・理由 現在の手順では、全ての要件を守ることで製品の脆弱性を完全に管理できるとは限らない場合があります。特にHWチップの危殆化はシステムを脆弱にする要因の一つであるため、ソフトウェアだけでなくハードウェアを含むSBOMの管理が重要と考えております。 【出典：デジタル庁 デジタル社会推進実践ガイドブック DS-200 政府情報いステムにおける「セキュリティ・バイ・デザインガイドライン」】	いただいた御意見は、ガイドライン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。1.4章にハードウェアの脆弱性を含む部品管理の重要性を追記し、現状版ではソフトウェアを対象範囲とすることを記載します。ハードウェアについては検討を進めたいと思います。
87	17	3	―	7.4 各フェーズの手順と方法	・意見内容 セキュリティバイデザインの概念を取り入れ、セキュアな設計がなされている部分についてはSBOM管理の対象外とする基準を設けることをご検討いただければと思います。 ・理由 セキュリティバイデザインの導入により、セキュアな設計がなされている部分では脆弱性が発生しても、外部からの攻撃が及ばない領域にあるソフトウェアは、脆弱性の影響を最小限に抑えられるため、脆弱性を無視することができ、SBOM管理のコストを削減することができます。これにより、全体の管理コストを効果的に削減し、効率的な脆弱性管理を実現できると考えます。 【出典：デジタル庁 デジタル社会推進実践ガイドブック DS-200 政府情報いステムにおける「セキュリティ・バイ・デザインガイドライン」】	いただいた御意見は、ガイドライン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。SBOMを含むセキュリティバイデザインを想定し、脆弱性が発見された場合のSBOMを活用した対応について検討させて頂きます。

88	17	4	―	8.2 SBOM可視化フレームワークと対応モデル	・意見内容 企業が実施している著作権管理、輸出管理、ライセンス管理、特許管理のプロセスと、SBOM管理を統合することを示唆する文言の追記を検討いただければと思います。 ・理由 著作権法や輸出管理、特許管理などの法規制に基づくソフトウェア管理プロセスは、ほとんどの企業が実施済みと考えており、SBOM管理を追加で実施すると二重管理になる懸念がございます。SBOM管理の実施を機に、これまでの管理で重複していた作業を削減し、管理コストの最適化を目指すことを提示できると企業は投資しやすくなり、導入の促進に役立つと考えます。 【出典：日本の著作権法、外国為替及び外国貿易法（外為法）、特許法】	いただいた御意見は、ガイドライン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。1.3節にSBOM用途を挙げ、現状版の対象範囲を記載させて頂きます。
89	17	5	―	9.1 背景と目的（問題認識）	・意見内容 SBOM取引モデルにおいて、セキュリティバイデザインによる設計がなされている場合は、SBOM管理を緩和または免除する制度を導入することを提案いたします。また、既存のソフトウェア管理プロセスとSBOM管理の統合を推進することも併せて提案いたします。 ・理由 セキュリティバイデザインの導入により、脆弱性が発生しても影響が最小限に抑えられるため、SBOM管理の対象外とすることで管理コストを削減できます。また、既存のソフトウェア管理プロセスと統合することで、全体の管理効率を高めることができると考えます。 【出典：デジタル庁 デジタル社会推進実践ガイドブック DS-200 政府情報いステムにおける「セキュリティ・バイ・デザインガイドライン」】 【出典：日本の著作権法、外国為替及び外国貿易法（外為法）、特許法】	いただいた御意見は、ガイドライン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。セキュリティバイデザインとSBOMの両方の重要性を考慮し、統合的なアプローチについて検討させて頂きます。
90	18	1	個人	全体	SBOMについて、脆弱性管理のソリューションの一つという印象を受けましたが、本質的には資産管理のソリューションではないでしょうか。脆弱性管理への転用は、SBOMによる資産管理・インベントリ管理の向上による副次的な効果であることを示すべきです。理由は以下の通りです。 理由1: NIST GlossaryやNIST SPの定義： NIST GlossaryやNIST SPでは「formal record containing the details and supply chain relationships of various components used in building software.」とある通り、コンポーネント（資産）間の関係性を示すレコードと書かれているからである。 NIST Glossary: https://csrc.nist.gov/glossary/term/sbom NIST SP800-40: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf Some vendors might also provide machineconsumable data on their assets' software composition, such as a software bill of materials (SBOM), 理由２: 脆弱性に関するSBOM上の属性： 脆弱性に関するSBOM上の属性は特定ベンダーフォーマット（例: CycloneDX）にしかなく、最低限必要な要素にはないように見受けられました 理由３: ガイドラインの記載： （本文書は民間向けではありますが）、「政府機関等の対策基準策定のためのガイドライン（令和5年度版）」の基本対策事項4.1.1(3)-1 f）「セキュリティ脅威に対処するための資産管理・リスク評価」において、「ソフトウェアバージョンや設定情報の文書化や変更による悪影響の防止等の適切な構成管理を実施すること」と書かれています。統一基準群が求める情報は、本文書2.1「SBOMとは」で述べられているSBOMの最低限の要素（ソフトウェアに含まれるコンポーネントの名称等）にかなり近いです。これにより、SBOMは本来的には資産管理に必要な情報を主に記載していることがわかります。 理由４: 実例の記載	いただいた御意見は、ガイドライン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。表４－１のSBOM活用範囲（WHY)として、脆弱性管理、ライセンス管理、資産管理が位置づけているため、ご意見を踏まえた位置付けの整理について検討していきたいと存じます。

					p.16で、「Log４jの脆弱性（Log４Shell）に対するSBOMの導入の効果でも「Log4p.16で、「Log4jの脆弱性（Log4Shell）に対するSBOMの導入の効果でも「Log4jのコンポーネントが存在する場合、ソフトウェア利用者は認識していないものの（略）影響を及ぼす可能性がある」と書かれており、本文書でも資産管理としてLog4jの課題があることを認めています（その結果、脆弱性管理が効果的にできないとなっています）。 これらのことから、本文書では脆弱性管理はSBOMを資産管理に活用することで生じる副次的効果といったほうがいいのではないでしょうか。資産管理で依存関係がわかるため、脆弱性管理におけるAssuranceが高まるといった具合かと思われます。 なお、図2-4では「手動でのコンポーネント管理」となっており、本文書内でもその目的に関して統一的見解が得られていないように見受けられます。	
91	18	2	個人	1.2 目的	「SBOMはソフトウェア管理の一手法」と述べているのに対し、「SBOMを用いたソフトウェアの適切な管理が重要」と、まるでSBOMが唯一の手法であるかのような表現が続いています。これでは、SBOMが唯一の手法であるという印象を与えてしまう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。
92	18	3	個人	1.6 本手引きのサマリー	SolarWindsのサイバー攻撃で露見した課題は、SBOMで解決できるのでしょうか。SolarWindsはソフトウェアのビルド環境が侵害され、攻撃者のコードが挿入されたことが契機となっています。それをどのようにSBOMで解決できたのか明示できなければ、例として適当ではないのではないでしょうか。 - https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/ - https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/ - https://www.youtube.com/watch?v=1-tMRxqMwTQ	1.6節での記載は、ソフトウェアサプライチェーンの脅威が増大していることを主張するものであり、SBOMによる解決を明示的に示すことを意図しているものではありませんので、御意見として承ります。なお、SolarWindsの製品において、適切なコンポーネント管理が実施されていた場合に攻撃者の悪意あるコードの挿入を検出できた可能性は示唆されております。

93	19	1	組織	1.手引ver2.0(案)全体への意見	経済安全保障推進法が制定・施行されるなど、サプライチェーンのセキュリティの重要性の認識が増す中、「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」が策定されることを歓迎します。 我々は、一般社団法人　沖縄オープンラボラトリにてTrusted Network Projectを2022年に立上げ、プロジェクト参加各社とともにSBOMによる脆弱性管理も含めてサプライチェーンで供給される製品のトラストを確保するためのプラットフォームのプロトタイプ開発と実証を通して、社会実装に向けた活動を続けております。 この手引きが広く普及活用されるために、このprojectで得られた知見を踏まえて意見を申し上げます。 ・SBOMはソフトウェア製品の脆弱性を管理するための重要な情報の一つであり、SBOM利活用の仕組みを確立することが脆弱性管理の大きな進化の一要因であることは、デジタル庁/内閣府による令和3年度補正予算Trusted Webの実現に向けたユースケース実証事業参画における報告や沖縄オープンラボラトリにおいて弊社が幹事会社を務めるオープンPJ活動の推進で得られた知見、見出された方向性とも完全に適合しており、参加各社の意見（期待）とも合っている。 ・本手引きでは、かなり実践的かつ実効的な内容が、合理的なアプローチや方法論、そしてノウハウが体系化され具体的に示されており、相応の時間と労力は要するものの、SBOM導入に向けた手引きという意味では大変有為性が高いと考える ・一方、手引きに提示されている課題も含め、ソフトウェア製品の脆弱性管理やライセンス管理を目的とした場合、現段階でSBOM自体が不完全かつ成熟初期段階にあることから、どのようなアプローチを選択しても、SBOM利活用の目標達成には大変な労力と中長期的な時間を要するという観点においては課題感が大きい。 　また、読み手のSBOMに関する知識や知見といったノウハウによっては、手引きの通りに対処すれば概ねの対応が出来ると安易に捉えてしまうリスクや、手引きで示されている内容自体を十分に理解できないため最初の一歩を踏み出せず様子見となってしまうリスクもあると考える。	本手引に対する肯定的な御意見として承ります。併せて、お寄せいただいた課題感に関する御意見は、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。
94	19	2	組織	２．２章・３章・４章に関連した意見（一部九章を含む）	・SBOMの内容という観点について、前提として最低限のバラつき回避、すなわち共通的プロセスと生成手法に関する標準化の確立と遵守、そして標準に適合するツールチェーンの提供による自動化が求められることは、本手引きで述べられている通りであり、強く賛同するとともに、社会実装に貢献していく所存である。SBOMはビルド環境から機械的に自動収集できる様々な情報と、人間の介入による追加情報を元に生成されるため、むしろSBOMツールよりもSBOMツールへの入力情報のレベルに関する手引きが重要となる。 　ソースやライブラリの構成管理ルールやソースコードやビルドファイルの記述ルール、ビルドファイルのソフトウェアコンポーネントの名称付与規則の確立やコンポーネント情報とのマッピングルール、コンポーネントのID化など、数多くの取り組みが現在進行形であるとともに、大小の課題が山積している。これらの課題の中には、個社の自律的かつ自主的な取り組みによって適切に解決できるものと、サプライチェーンのステークホルダが民主的かつ共創的に取り組むことでしか解決できないものが存在する。このような手引書において、課題毎の最適な解決アプローチ、もしくは最適な解決アプローチを導出するための方程式が示されることにより、個社とサプライチェーン全体における取組みのバランスと最適化を誘起することができると考える ・SBOMの提供にかかる労力、すなわちコストの観点においても、SBOM生成自体の成熟度がまだ十分とは言えない状況にあり、継続的な運用への投資に踏み切るための経営判断材料の安定性と十分性が棄損されており、一義的にSBOM提供責任を負うべき組織、すなわち当該ソフトウェアを開発し、品質と維持管理に関する責任を負う主体の取り組みを阻害している。これによって、網羅性の向上が進みにくい結果を産み出している。 　また、SBOMの提供と流通の態様がサプライチェーンの下流から上流に多段的に集約されていく構造となることから、SBOMの生成や流通にかかるコスト的負担が最上流のステークホルダに集約されることも大きな課題となる。 ・SBOM適用対象となるソフトウェアの分類の観点では、OSSに関するSBOM提供の仕組みをどう確立していくべきかという課題がある。OSSの利用は受益者負担が原則であるが、同一OSSについて全ての利用者がSBOMを作成し提供するのは分割損が大きすぎる。 　また、一般にソフトウェア製品として流通していない製品固有の自社開発内部ソフトウェア（特に製品固有のファームウェア）をどう管理していくか、などの課題がある。 　我が国に流通しているソフトウェアのサプライチェーンは中国や新興国を含めグローバル化しており、セキュリティ産業の成長加速化、製品／サービスの国内自給率向上に向けた取り組みは政策検討課題の一つとなっている。 （https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/010_03_00.pdf）	本ガイドラインに対する肯定的な御意見として承ります。一方で、サプライチェーンを通じたコスト負担、最適化、OSSのSBOM作成の効率化など個社では解決が難しい課題であることはご指摘の通りであり、重要な論点の一つであるため、制度的な観点等から継続的に検討します。特に、コスト負担の在り方については、SBOMの導入・活用の価値を明確化した上で、SBOMの導入・活用の目的や適用範囲を考慮しながら社会的な共通認識の醸成を図っていく必要があるため、引き続き今後の課題として継続的に検討します。

					SBOM適用対象ソフトウェアに関する分類や整理、合意形成については、取引を行う個社間での対応が実質的に不可能であり、官学民一体となった国際的な取り組み、具体的にはEU CRAや米国大統領令などの取り組みとの相互運用性の確立が必須となると考えられる。 ・SBOMを利用する側の労力の観点においても、仮にSBOMを入手したとしても、機械的な自動処理によって得られる脆弱性情報が極めて限定的であることは、冒頭に記載したプロジェクトにおける3年近い取り組み、具体的には価値実証実験の結果が示している。この要因はSBOMだけに起因するのでは無く、脆弱性データベースの機械可読性・理解容易性や情報網羅性が低いことも大きな要因であり、SBOMを使った脆弱性管理を実現するためには、ソフトウェア脆弱性管理における高い専門スキルと成熟した経験、そして無視できない労力の投入が伴う。本手引きにも脆弱性データの適切な選択の重要性が示されているが、各主体の要求レベルと選択結果を適切に結びつけるにはその十分性について広範囲な個別検証が必要となるため、このような手引きにおいてより具体的なノウハウやベストプラクティスを継続的に共有していく必要があると考える。	
95	19	3	組織	3．9章に対する意見	・SBOMの流通という観点では、 - SBOM自体がソフトウェアの品質及び維持管理責任を有する多数の供給者からバラバラに提供されることから、ソフトウェアのコンパイルやビルドにより一つの実行モジュールが生成されるのと同様に、単位SBOM情報の結合化が重要な要素となる。この結合化においてミスや恣意的な情報操作（改ざん）も可能となるばかりか、SBOM定義粒度の一致性を保証するためのコストの多大化が懸念され、粒度の一致確認が出来ない場合、この結合が非常に難しい業務となる - サプライチェーンの最上流から最下流までの経路において、途中で一社でも抜けがあるとSBOMの流通が途切れてしまうこと - 情報の重要性からエンドツーエンドで十分な改ざん対策と改ざん検証性を講じる必要性があること - 脆弱性対応パッチの提供を含め定常的かつ一定頻度でアップデートされる性質の情報であること - ゼロディリスク対策として情報の流通にリアルタイム性と確実な流通管理が求められること - SBOMに格納される情報には企業にとって機微な情報が含まれる可能性があるため、厳密かつ詳細な情報開示制御と管理が求められること などから、高度な流通の機構化が求められると考える。	いただいた御意見は、ガイドライン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。各課題について順次検討が必要と考えられます。
96	19	4	組織	4．上記コメントを踏まえた全体的な手引きに関する意見	上記のような背景から、沖縄オープンラボラトリのPJで得られた知見と現状の方針を踏まえ、手引Ver2.0案全体的な意見を下記に申し上げる。 ・上記のような背景を踏まえても、提供するSBOMの完全性を合理的に可視化し、検証性を提供することには十分な意義・優位性がある。完全を目指しつつ、完全性を合理的に可視化・検証するためのクライテリアを定め、そのクライテリアをベースにした提供側と利用側の二社間の債務定義と合意形成、そしてその合意形成の連続的な接続と透明化の仕組み（これを当PJではTrust Chainと呼んでいる）を確立することは急務である	本ガイドラインに対する肯定的な御意見として承ります。また、利用者、提供者の合意形成については今後の課題とします。
97	20	1	個人	8. 付録：SBOM対応モデル	*意見内容 金融関連を対象とする検討とあわせてPCI-DSSやPCI-SSFなどをはじめ、その他のインフラやサービスにおけるSBOM観点での留意事項、また、関連してサービスに関するSBOMの動向などの解説もあれば、追記を検討頂くことは可能でしょうか。 参考 PCI https://www.pcisecuritystandards.org/ とくに、PCI-DSS v4.0, PCI-SSF v1.2.1 CISA. Software Transparency in SaaS Environments https://www.cisa.gov/resources-tools/resources/software-transparency-saas-environments-0 *理由 重要インフラやサービスに関するSBOMの理解度向上のため。	いただいた御意見は、ガイドライン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。分野ごとの基準とのマッピングについては今後の課題とさせていただきます。

98	20	2	個人	8.6. SBOM 対応モデルの参考例（医療機器分野）	*意見内容 IMDRFのガイダンスへの言及があるため、FDAについても言及があっても良さそうに思われました。 また、医療機器特有のSBOMとして扱うべき要素があれば、その解説があっても良さそうに思われました。 参考 https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity *理由 産業別のSBOMに関する必要事項の理解度向上のため。	いただいた御意見は、ガイドライン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。FDAへの言及については今後の課題とさせていただきます。
99	20	3	個人	全般	*意見内容 SBOMについては、その流通性の確保と向上に向けた取り組みがなされている状況と理解しております。最新のおよその合意事項や論点なども移ろいやすい中で、このような文書の取組に感謝申し上げます。一方で、発行時期を鑑みて、更新または補訂などを検討頂ければと思われるところも見受けられました。NTIAが示した最小要素の見直しに掛かる動き、SBOMで扱う依存の深さなどの要素に基づくSBOMの成熟度モデルに関する議論、SBOMの共有や提供に関する議論、CycloneDX 1.6やSPDX 3.0などの最新仕様に関する情報も扱う必要がありそうに思われます。また、国際共同文書 Secure By Design にて本稿初版への言及があるところ、更新版となる本稿ではよりグローバルなソフトウェアサプライチェーンにおけるセキュアなソフトウェア開発を啓蒙、推進する要素を取り入れて頂けることがあれば、より一層良さそうに思われる次第です。 *理由 初版以降の最新動向に関する理解度向上のため。 参考 CycloneDX 1.6 https://cyclonedx.org/ SPDX 3.0 https://spdx.github.io/spdx-spec/v3.0/ BSIのTR-03183-2は2024年1月に改訂版が発行されており初版よりも明確化がなされている https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html CISA. SBOM Sharing Roles and Considerations https://www.cisa.gov/resources-tools/resources/sbom-sharing-roles-and-considerations CISA. SBOM Sharing Primer https://www.cisa.gov/resources-tools/resources/sbom-sharing-primer	御意見を踏まえ、当該箇所を修正いたします。
100	20	4	個人	全般	*意見内容 本件のような手引きの作成過程をよりオープンにしてはどうでしょうか。SBOMに関しては、オープンソースコミュニティであるLinux Foundation の OpenSSF、CNCF、SPDX Project、OpenChain Project、また、OWASP CycloneDX などはいずれもオープンな場ですが、米国CISAによるワーキンググループもオープンです。このような場に参加する国内企業や関係者からの手引き策定への参画は、より国際的な動向を踏まえての国内の理解度向上とあわせて、国内意見も踏まえての国際的な合意形成とその普及促進に資すると考えられます。 *理由 セキュアなソフトウェア開発の導入推進と併せて、オープンソースを活用するソフトウェア産業の発展のため。	いただいた御意見は、ガイドライン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。ステークホルダーが参加する委員会形式と、不特定のオープンなコミュニティによる検討については、比較検討したいと存じます。