経済産業省　国家サイバー統括室 National Cybersecurity Office

資料３

事務局説明資料

令和８年２月

サイバーインフラ事業者に求められる役割等の検討会 事務局

1. 検討会について
   - 検討会について
   - 取組の全体像
   - 今年度の取組の進め方
   - 今年度の検討会について
2. ガイドライン案
   - サイバーインフラ事業者に求められる役割等に関するガイドライン（案）全体概要
   - パブリックコメントの概要
   - パブリックコメントで頂いた主な御意見に対する考え方
   - 委員から頂いた主な御意見に対する考え方
   - （参考）意見の概要と新旧の対照
   - （参考）ガイドライン（案）の全体構成
3. 評価チェックリスト
   - 評価チェックリスト案の更新
4. 御意見をいただきたい事項

1. 検討会について

検討会について

第4回検討会資料の再掲

趣旨

現代社会において、ソフトウェアは社会活動の基盤となっており、その重要性は増大している。そのため、ソフトウェアの脆弱性を悪用するサイバー攻撃は社会インフラに甚大な影響を及ぼす可能性がある。ソフトウェアを提供・運用する事業者の責任は、その重要性から従来と変わらないものの、役割の変容に伴い、特に大規模システムを提供する事業者にはより一層の責任が求められている。

また、国際的にも、セキュア・バイ・デザイン（ソフトウェア等が設計段階から安全性を確保されていること）やセキュア・バイ・デフォルト（顧客が追加コストや手間をかけることなく、購入後すぐにソフトウェア等を安全に利用できること）といった概念が支持を集めており、これに関連する国際文書が策定されている。

我が国のサイバーセキュリティ基本法第７条においては、サイバー関連事業者（※1）その他の事業者の責務が規定されているところ（第7条第1項）、**令和7年7月の同法の改正により、情報システム等の供給者に対して、利用者によるサイバーセキュリティ確保に必要な支援を行う努力義務が規定**されることとなった（第7条第2項）。このうち、一定の社会インフラの機能としてソフトウェアの開発・供給・運用を行っている事業者（※2）（以下、「**サイバーインフラ事業者**」という。）に関しては、官民が連携した取組の在り方や、コストとのバランスを踏まえたソフトウェアサプライチェーン（※3）セキュリティ確保のための取組の体系的な整理に関する調査・検討が求められている。

本件に関してはこれまで経済産業省及び内閣官房国家サイバー統括室においてサイバーインフラ事業者に求められる役割等につき調査研究を実施してきたところ、これを踏まえ、**サイバーインフラ事業者と顧客に求められる責務**と、**責務を果たすための要求事項（役割別の具体的な取組の在り方）**を含むガイドライン（以下「ガイドライン案」という。）の策定及びその普及策の検討を目的として本検討会を開催する。

※1 インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者
※2 政府機関及び重要インフラ事業者をはじめ広く社会で活用される情報・通信システム、ソフトウェア製品及び ICT サービスを開発し提供する事業者並びに当該情報・通信システム等のソフトウェアのライフサイクルとサプライチェーンに関わる事業者
※3 ソフトウェアの開発、供給、運用のすべてに関わるライフサイクルと、関連する組織及びソフトウェアの相互依存関係

取組の全体像

第4回検討会資料の再掲

- ソフトウェアの開発・供給・運用に関わる**サイバーインフラ事業者と顧客に求められる責務**、及び**責務を果たすための要求事項**（役割別の具体的な取組の在り方）をまとめたガイドライン案を策定すると共に、その普及策の検討を通じて、ソフトウェアサプライチェーンのレジリエンス向上を図ることが目標。
- 今年度は、パブリックコメント、実証、及びサイバーインフラ事業者へのヒアリングを通じて、**ガイドライン**を成案化すると共に、新たに、ガイドラインの活用促進に向けた付属文書として責務向上のための評価基準（**評価チェックリスト**）の整備を優先。
- 来年度以降は、**将来的な検討課題への対応、普及施策**（評価チェックリストの活用策等）を検討予定。

今年度実施予定の内容

実施事項

- パブリックコメント
- サイバーインフラ事業者での実証
- サイバーインフラ事業者へのヒアリング
- ガイドライン案の成案化
- 評価チェックリストの検討

成果物例

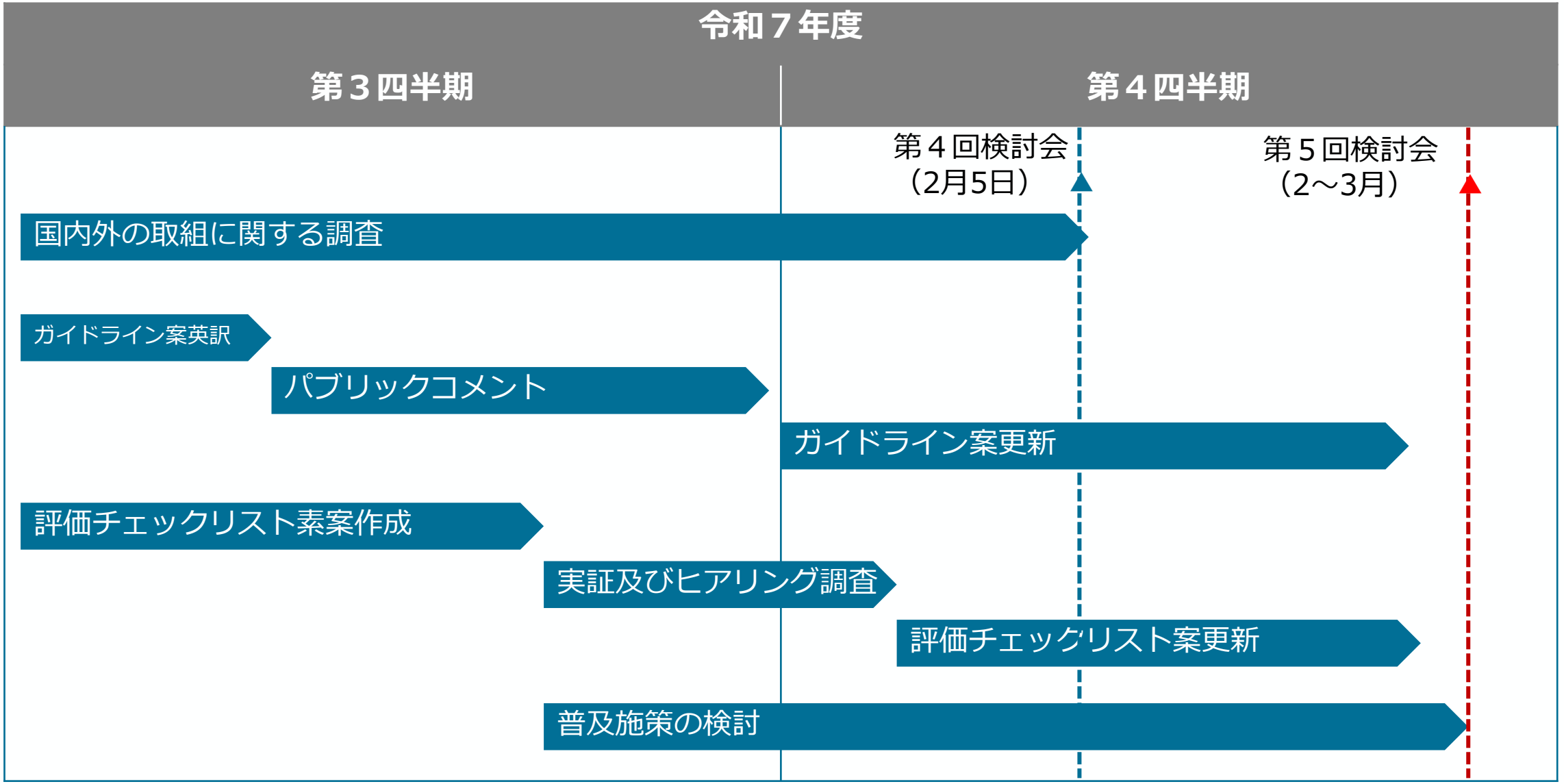
- ガイドライン本体案
  - サイバーインフラ事業者と顧客に求められる責務
  - 責務を果たすための要求事項
  - 参考情報　など
- 評価チェックリスト案
  - 評価導入手引き
  - 評価チェックリストとガイド

来年度以降実施予定の内容

実施事項

- 将来的な検討課題への対応
- 普及施策（評価チェックリストの活用策等）の検討　など

今年度の取組の進め方


令和７年度
第３四半期
第４四半期
第４回検討会
（2月5日）
第５回検討会
（2～3月）
国内外の取組に関する調査
ガイドライン案英訳
パブリックコメント
ガイドライン案更新
評価チェックリスト素案作成
実証及びヒアリング調査
評価チェックリスト案更新
普及施策の検討

今年度の検討会について

第4回検討会資料の再掲

検討内容

- ガイドラインの成案化
- ガイドラインの活用促進に向けた付属文書としての評価チェックリストの拡充
- 政府機関・重要インフラをはじめ、顧客となる事業者等によるガイドラインの活用を促す枠組み等、サイバーインフラ事業者のレジリエンス向上の実効性を強化する施策全般

検討スケジュール

検討会及び開催時期	主な議題	備考
第４回検討会 （令和8年2月5日）	• 検討の進め方について • 実証実験及びヒアリング結果の御報告 • ガイドライン案（更新版）の審議 • 評価チェックリストの審議	• パブリックコメントに寄せられた御意見の確認 • 評価チェックリストの活用施策
第５回検討会 （令和8年2～3月）	• ガイドラインの承認 • 評価チェックリストの承認	

2. ガイドライン案

サイバーインフラ事業者に求められる役割等に関するガイドライン（案）全体概要

- ソフトウェアサプライチェーンのサイバーセキュリティに関するレジリエンス向上のため、サイバーインフラ事業者と顧客に求められる責務(基本理念に類する事項)、及び責務を果たすための要求事項を6つに整理。ガイドラインを活用するための評価チェックリストも作成。

ガイドライン（案）

6つの責務 サイバーセキュリティに関するレジリエンス向上のため、認識すべき基本理念	６つの要求事項 サイバーセキュリティに関するレジリエンス向上のため、共通して取組むべきサイバーセキュリティ対策	対象組織
セキュリティ品質を確保したソフトウェアの設計・開発・供給・運用	セキュアな設計・開発・供給・運用	サイバーインフラ事業者
ソフトウェアサプライチェーンの管理	ライフサイクル管理、透明性の確保	
残存脆弱性への速やかな対処	残存する脆弱性の速やかな対処	
ソフトウェアに関するガバナンスの整備	人材・プロセス・技術の整備	
サイバーインフラ事業者・ステークホルダー間の情報連携・協力関係の強化	サイバーインフラ事業者・ステークホルダー間の関係強化	
顧客の経営層のリーダーシップによるリスク管理とソフトウェア調達・運用	顧客によるリスク管理とセキュアなソフトウェアの調達・運用	顧客

評価チェックリスト（案）

評価導入手引

ソフトウェアサプライチェーンのレジリエンス向上に資する評価を進めるための手引き。活用パターン、評価の進め方、評価チェックリストの使用方法等について容易に理解できるように説明するもの。

評価チェックリスト兼記録票 ・ 評価ガイド

「評価導入手引き」に従いサイバーインフラ事業者が評価基準への適合状況を評価する際に活用する評価用のチェックリスト。エビデンスを含む評価の過程・結果を記録する。評価内容毎の評価ガイドを含む。

自己評価宣言書

評価基準とした全ての評価内容について評価を実施した結果を、自己宣言するもの。

活用のシナリオ（例）

事業者の自主公表

事業者が本ガイドライン案の責務への取組状況をアピールするために活用する。

RFI（情報提供依頼）に活用

RFIの際に、顧客も本ガイドライン案の責務に対応することを前提として、事業者が責務への取組方針について回答する。

調達・開発・運用に活用

顧客側が入札仕様として評価チェックリストを提示する際に自己評価結果を埋めておき、事業者へ追記を依頼する。事業者が追記した宣言内容を両者が共有し、責務と役割分担の認識を共有する。調達・開発・運用の各フェーズで活用可能。

パブリックコメントの概要

- 「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）」について、パブリックコメントを実施し、20者の法人・個人等からご意見を受領。
- 頂いた御意見および検討会でのご意見を踏まえ、記載内容の補足や具体化、誤解を招く可能性がある表現の修正等の観点から修正を行った。

実施期間	令和7年10月30日（木）～令和7年12月30日（火）	
御意見等の総数	20者の法人・個人等	
頂いた御意見のカテゴリ	① 事業者の責務と個別要求 ② 顧客の責務と個別要求 ③ SBOMの義務 ④ インシデント対応 ⑤ ガイドラインの運用 ⑥ 予算とコスト ⑦ 関連文書類の整備 ⑧ 既存取組との関係	⑨ OT環境の責務 ⑩ ステークホルダー・対象事業者 ⑪ 取組例 ⑫ パッケージ ⑬ 役割 ⑭ 用語等 ⑮ その他

パブリックコメントで頂いた主な御意見に対する考え方（1/4）

頂いた御意見のカテゴリ	該当箇所	頂いた主な御意見	御意見への対応の考え方（案）
①事業者の責務と個別要求	3.2章	• **脆弱性に関する一律に詳細な情報開示や通知を求める運用には慎重であるべき**【No.12-2】 • 事業運営において法令を遵守することは当然の責務であり、明示することに違和感がある【No.7-1】 • サードパーティ製ソフトウェアコンポーネントに自組織の要件を課すことは困難である【No.10-2】 • リスク管理が事業者と顧客との共同作業であることを明確化すべき【No.14-10】 • 検知後の対応における説明性・可視性の確保について、補足すべき【No.16-4】	• 脆弱性情報の取り扱いについて、留意すべき事項を追記する。 • 事業運営において法令を遵守することが当然の責務として記載しており、原案のとおりとする。 • 該当の要求事項は、自社製品のセキュリティ品質を確保するための受入基準を明確にするもので、サードパーティに対して同一の開発プロセスを求めるものではないため、原案のとおりとする。 • その他については、御意見の趣旨は原案に含まれている、もしくは責務を示すものとして概念レベルの記載とするため、原案のとおりとする。
②顧客の責務と個別要求	3.2章	• **顧客と連携先であるセキュリティコミュニティとの双方向の活動が必要である**【No.10-2】 • セキュリティ要件の定義について顧客と事業者間の関係性を明確化すべき【No.18-6】	• 双方向の活動（貢献）が必要であることを明確化する。 • 御意見の趣旨は原案に含まれており、原案のとおりとする
③SBOMの義務	3.2章	• **SBOMの過度な提供義務は、事業者の負担が過大となる懸念がある**【No.10-3】	• SBOMの導入を推奨するものであり、すべてのケースで完全な導入を強制するものではないため、原案のとおりとする。なお、5.4章の取組例の記載が、SBOMが必須と誤解を生む可能性があり見直し。

（**太字**の御意見を採用）

パブリックコメントで頂いた主な御意見に対する考え方（2/4）

頂いた御意見のカテゴリ	該当箇所	頂いた主な御意見	御意見への対応の考え方（案）
④インシデント対応	3.2章	• インシデント検知から隔離までの迅速な対応を標準要件として明記すべき【No.16-6】	• 責務と個別要求の中で具体化されるべきものであり、御意見の趣旨は原案に含まれていることから、原案のとおりとする。
⑤ガイドラインの運用	—	• ガイドラインや制度が現場において形骸化することを防ぐため、定期的なガイドライン改訂の仕組みを設けるべき【No.17-3】	• 国内外の動向に合わせて適宜見直しを行うことを検討する。なお、ガイドラインは、原案のとおりとする。
⑥予算とコスト	3.2章	• **納品前や運用期間中に不測の事態等が発見された場合には、開発会社と顧客企業で協調して対応することを明確化すべき**【No.7-3】	• 協調した対応を5.4章の取組例に追加する。
⑦関連文書類の整備	5.5章	• 他の法令・ガイドラインについても、相互の関係性をイメージできるような資料があるとわかりやすい【No.5-2】 • このガイドの要求事項を現実的に適用していくための進め方のガイダンス整備が必要【No.13-4】	• 標準化動向などを踏まえつつ、今後の検討とする。
⑧既存取組との関係	全般	• 既存の国際基準を満たしている事業者が自己評価宣言を行う際に確認が二度手間にならないようにすべき【No.11-1】	• 具体的な第三者監査・認証制度、及び調達要件との接続は、今後の検討とする。
⑨OT環境の責務	全般	• ITとOTで前提条件が異なる点について、ガイドライン上で補足説明を加えるべき【No.16-3】	• OT環境における制約や特性を踏まえ、事業者がリスク評価に基づき適切な手段を選択することを前提としており、御意見の趣旨は原案に含まれていることから、原案のとおりとする。

パブリックコメントで頂いた主な御意見に対する考え方（3/4）

頂いた御意見のカテゴリ	該当箇所	頂いた主な御意見	御意見への対応の考え方（案）
⑩ステークホルダー・対象事業者	1.3章	• ステークホルダーに法規制当局を入れるべき【No.5-1】 • 供給者から、販売会社を除外するか、もしくは開発側と販売側の責務・役割を明確に変更し定義するべき【No.9-1】	• 「その他関連機関」の一部であり、御意見の趣旨は原案に含まれていることから、原案のとおりとする。 • 役割と責務は実態に合わせて分担可能な構造であり、御意見の趣旨は原案に含まれていることから、原案のとおりとする。
⑪取組例	5.4章	• **経済産業省と公正取引委員会による「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」について言及すべき**【No.14-6】 • チェックリスト・事例集に RA、TPM、PQC の活用例を盛り込むべき【No.4-4】	• サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を推薦いただいたが、顧客と事業者の関係性構築の観点から、より具体的な記載のある「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説」を参考情報として追記する。 • 責務を示すものとして概念レベルの記載とするため、原案のとおりとする。
⑫パッケージ	全般	• 事業規模、サービス停止時の社会的影響度、取り扱うデータの機密性などに応じて、どちらのパッケージを適用すべきか、より客観的で具体的な判断基準を示すべき【No.13-2】	• 本ガイドは責務を示すものとして整理していることから、原案のとおりとする。

パブリックコメントで頂いた主な御意見に対する考え方（4/4）

頂いた御意見のカテゴリ	該当箇所	頂いた主な御意見	御意見への対応の考え方（案）
⑬役割	1.4章	• 役割を兼務する事業者の存在を前提とした補足的な説明や考え方を示すべき【No.12-1】	• 兼務は記載しており、ご意見の趣旨は原案に含まれていることから、原案のとおりとする。
⑭用語等	3.1章	• **図７責務の概念図について、説明を補足すべき**【No.14-7】 • 定期的作業としている項目について、理想的な期間の目安を記載すべき【No.14-20】 • **ステークホルダ・対象に関する用語不統一の個所がある（例：責務での「ベンダー」と「開発者」の表記）**【No.18-1】 • **「IT製品」の用語は「S(2)-3」のみで使用されている**【No.18-7】 • **「S(2)-3.2」で、「サプライチェーンセキュリティ要件」の定義が必要である**【No. 18-8】 • **「脆弱性に基づき、開発と運用のプロセスを見直す」は、運用プロセスは、「脆弱性に基づき見直す」ものではなく、「根本原因に基づき見直す」もの**【No. 18-9】 • **リスク適合など、表現・用語の統一が必要である**【No.18-12】	• 図7に説明を追加する。 • 多種多様なソフトウェアや事業形態を対象としており、実施頻度を一律の期間で規定することは適当ではないため、原案のとおりとする。 • 必要な用語の整理、統一を行う。なお、「ベンダー」表記は、責務部分について修正を行う。
⑮その他	4.2章	• 4.2 章「注意事項」のタイトルは、前提条件（もしくは推奨事項）となるべき【No.14-23】	• 要求事項を各事業者が実務に適用する際の手順や、判断に迷いやすいケースにおける補足を示すことを目的としており、原案のとおりとする。

委員から頂いた主な御意見に対する考え方

頂いた御意見のカテゴリ	該当箇所	頂いた主な御意見	御意見への対応の考え方（案）
⑮その他	5.3章	• ガイドラインにおいて「IT部門」と記載されている箇所について、スリーラインズ・オブ・ディフェンスの観点から、セキュリティのレビュー等を担う**「情報セキュリティ部門」も併記**し、両部門が活用できるような記載とすることが望ましいとの声があった。 • 取組例に「IT部門に必要に応じて拒否する権限を明確に与える」とあるが、ユーザー企業は自社のガイドラインに本ガイドラインの内容を取り込むため、「必要に応じて」といった表現を削除し、**より強い表現とする**ことを望む声があった。	• 「IT部門・情報セキュリティ部門」とする。 • より強い表記として、基準を満たさない製品の購入に異議を唱える権限をIT部門に与えることを明確化する。

（**太字**の御意見を採用）

（参考）意見の概要と新旧の対照（1/5）

カテゴリ	No.	意見の概要	修正箇所（案）	
			旧	新
①事業者の責務と個別要求	12-2	• 脆弱性に関する一律に詳細な情報開示や通知を求める運用には慎重であるべき。	＜記載なし＞	5.4章「システム・サービスのソフトウェアの脆弱性対応の課題と対応」節 • **脆弱性情報の提供については、開示のタイミングや範囲について慎重な配慮が求められる場合もある。**
②顧客の責務と個別要求	7-2	• 顧客とコミュニティの双方向の活動が必要である	＜記載なし＞	5.4章 S(6)-1.3 協力体制の活用　取組例 • **以下に例示する。** 　• **ISAC（SoftwareISAC など）やCSIRT 協議会に参加** 　• **民間企業の有志団体が集まったコミュニティ、地域のセキュリティコミュニティ（地域SECUNITY）を通じた連携**
			P.47 S(6)-1.3 協力体制の活用 P.94 S(6)-1.3 協力体制の活用 ソフトウェアセキュリティの改善を目的とするコミュニティや協力体制を活用する。	ソフトウェアセキュリティの改善を目的とするコミュニティや協力体制**に積極的に参画及び活用**
			P.22 2.2章 責務 セキュリティ改善を目的とするコミュニティや協力体制の活用	**顧客、サイバーインフラ事業者を含む関係者間における**セキュリティ改善を目的とするコミュニティや協力体制**に積極的に参画及び活用**
③SBOM	10-3 10-4 14-21 19-1	• SBOMの過度な提供義務は、事業者の負担が過大となる懸念がある。	5.4章 S(6)-1.2 リソース整備 ソフトウェア製品のセキュリティ実装に係る証明情報（SBOM、SSDFの実装の適合性を証明する自己適合証明書など）を要求・検証する。	ソフトウェア製品のセキュリティ実装に係る証明情報（**推奨される**SBOM、SSDFの実装**について、そ**の適合性を証明する自己適合証明書など）を要求・検証する。

（参考）意見の概要と新旧の対照（2/5）

カテゴリ	No.	意見の概要	修正箇所（案）	
			旧	新
⑥予算とコストについて	7-3	• 納品前や運用期間中に発見された場合には、開発会社と顧客企業で協調して対応することを明確化すべき。	＜記載なし＞	**5.4章 S(6)-2.4** **• OSSやサードパーティ製コンポーネント等において開発・運用期間中等に脆弱性が発見される等のリスクを予見し相応のコスト準備をする。**
⑪取組例	14-6 14-25	• 経済産業省と公正取引委員会による「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」について言及すべき	＜記載なし＞	**5.4章 S(6)-1.1** **• 経済産業省及び公正取引委員会で作成した「サプライチェーン全体のサイバーセキュリティの向上のための取引先とのパートナーシップの構築に向けて」を補足する、発注者・相手方双方を対象とした、セキュリティ対策上の独占禁止法・取適法上「問題とならない」想定事例及びその解説文書についても参照する。https://www.meti.go.jp/press/2025/12/20251226001/20251226001-e.pdf**
⑭用語等	14-7 14-8	• 図７責務の概念図について、説明を補足すべき。	＜記載なし＞	**3.1章** **• 外縁は、責務とソフトウエアライフサイクルの対応を示す。** **• グラデーションは、ソフトウェアライフサイクルのフェーズ間の切れ目のない連続性と役割の融合・連携を表現している。** **• なお、3.2章以降の個別要求においても、本図表を引用しており、個別要求の当該節で解説するカテゴリ部分のみを色付けして強調（ハイライト）している。**

（参考）意見の概要と新旧の対照（3/5）

カテゴリ	No.	意見の概要	修正箇所（案）	
			旧	新
⑭用語等	18-1	• ステークホルダ・対象に関する用語不統一の個所がある。	P.21 「（３） 残存脆弱性への速やかな対処」の本文 • ベンダーは、クラウドサービス・ソフトウェアの脆弱性の特定と開示...ベンダーはバージョンアップ・パッチ適用プロセスを文書化して...	• **開発者、供給者及び運用者**は、クラウドサービス・ソフトウェアの脆弱性の特定と開示...**開発者、供給者及び運用者**はバージョンアップ・パッチ適用プロセスを文書化して...
	18-7	• 「IT製品」の用語は「S(2)-3」のみで使用されている	P34 S(2)-3 • IT 製品（自社のソフトウェアで再利用するための商用ソフトウェアコンポーネントを含む）又はサービスを… • 提供するIT製品又はサービスを… • サードパーティ製のIT製品またはサービスが…	• **サードパーティ製ソフトウェア**（自社のソフトウェアで再利用するための商用ソフトウェアコンポーネントを含む）又はサービスを… • 提供する**サードパーティ製ソフトウェア**又はサービスを… • サードパーティ製の**ソフトウェア**またはサービスが…
	18-8	「S(2)-3.2」で、「サプライチェーンセキュリティ要件」の定義が必要	P34 S(2)-3　本文 • SDLC全体を通じてセキュリティ要件（サプライチェーンを対象に含む）を考慮することができる。	• SDLC全体を通じてセキュリティ要件（サプライチェーンを対象に含む**。例：開発環境の管理、再委託先の管理、調達物品の検査基準**）を考慮することができる。
	18-9	「脆弱性に基づき、開発と運用のプロセスを見直す」は、運用プロセスは、「脆弱性に基づき見直す」ものではなく、「根本原因に基づき見直す」もの	P.38 要求事項（３） P.78 • ソフトウェアに発見された問題の根本原因が再発しない、若しくはその可能性を低減するよう、脆弱性に基づき、開発と運用のプロセスを見直す。	• ソフトウェアに発見された問題の根本原因が再発しない、若しくはその可能性を低減するよう、脆弱性**の分析結果（根本原因）**に基づき、開発と運用のプロセスを見直す。

（参考）意見の概要と新旧の対照（4/5）

カテゴリ	No.	意見の概要	修正箇所（案）	
			旧	新
⑭用語等	18-12	「リスク情報」は他に合わせて「リスク」とした方がよい	P27 S(1)-1 P60 S(1)-1 • 識別されたリスク情報に十分に対応していることを確認し、レビュー結果を反映する。	• 識別された**リスク**に十分に対応していることを確認し、レビュー結果を反映する。
		「リスクへの適合性」の表現は適切か	P27 S(1)-1 本文 • セキュリティ要件やリスクへの適合性を検証することは、ソフトウェアがセキュリティ要件を満たし、特定されたリスク情報に十分に対処できることを確認するのに役立つ。	• セキュリティ要件や**リスクへの対応の妥当性**を検証することは、ソフトウェアがセキュリティ要件を満たし、特定されたリスク情報に十分に対処できることを確認するのに役立つ。
		「リスク対処」は他に合わせて「リスク対応」とした方が良い	P.34 S(2)-3 P.50 S(2)-3 P.71 S(2)-3 付録 • セキュリティ要件を満たさないリスクへの対処プロセスの整備 • 受領・取得するサードパーティ製のIT 製品又はサービスが満たさないセキュリティ要件がある場合のリスクに対処するプロセスを整備する。 • ソフトウェアの運用に必要なIT 製品やサービス等のセキュリティ要件の合意、及び関連するリスク対処プロセスの整備支援など	• セキュリティ要件を満たさないリスクへの**対応**プロセスの整備 • 受領・取得するサードパーティ製のIT 製品又はサービスが満たさないセキュリティ要件がある場合のリスクに**対応**するプロセスを整備する。 • ソフトウェアの運用に必要なIT 製品やサービス等のセキュリティ要件の合意、及び関連するリスク**対応**プロセスの整備支援など

（参考）意見の概要と新旧の対照（5/5）

カテゴリ	No.	意見の概要	修正箇所（案）	
			旧	新
⑭用語等	18-12	「ソフトウェアのセキュアな利用方法を保証するための情報～」は、「ソフトウェアをセキュアに利用するための情報」と一般化した表現の方がよい。	P.35 S(2)-4 本文 • ソフトウェアの開発者、及び供給者に対して、ソフトウェアのセキュアな利用方法を保証するための情報を利用者に提供することを求めている。	• ソフトウェアの開発者、及び供給者に対して、**ソフトウェアをセキュアに利用**するための情報を利用者に提供することを求めている。
		「セキュリティを確保(保障)する」にて、「確保」と「保障」は意味が違う。	P.42 S(4)-4 本文 • そのセキュリティを確保（保障）する	• そのセキュリティを**確保**する
		「サプライチェーン先」は「取引先」とした方が伝わりやすい。	P.45 S(5)-1情報連携のための組織体制 P.92 S(5)-1情報連携のための組織体制 • 業界固有の必須かつ重要なセキュリティ関連情報を選別・識別して、サプライチェーン先に提供する。	• 業界固有の必須かつ重要なセキュリティ関連情報を選別・識別して、**サプライチェーン上の取引先**に提供する。
⑮その他	—	「IT部門」と記載されている箇所について、「情報セキュリティ部門」も併記する。	P99 S (6)-2 取組例 • IT部門	• IT部門・情報セキュリティ部門
		「IT部門に必要に応じて拒否する権限を明確に与える」は、より強い表現がのぞましい。	P99 S (6)-2 取組例 • IT部門がソフトウェア購入前にそのセキュリティを評価すること、及び必要な情報源を要求することを定めたポリシーを作成し、IT部門に必要に応じて拒否する権限を明確に与える。	• IT部門・**情報セキュリティ部門に対し**、ソフトウェア購入前にそのセキュリティを評価すること、及び必要な情報源を要求することを定めたポリシーを作成**するとともに、基準を満たさないソフトウェアの購入に異議を唱える権限を**IT部門・**情報セキュリティ部門**に与える。

（参考）ガイドライン（案）の全体構成

1.総論	1.1 背景と目的	諸外国の取組の動向、及びソフトウェアサプライチェーン上でのセキュリティ対策の必要性を簡潔に説明。取組の必要性を喚起するためインシデント事例を記載。
	1.2 ガイドライン（案）の位置付け	顧客と事業者に求められる責務と、責務を満たすための要求事項を整理することを説明。
	1.3 適用対象	「サイバーインフラ事業者」の範囲、対象ソフトウェア、本文書が想定するリスク概要を説明。
	1.4 役割分担の考え方	ソフトウェアの特性、開発・供給体制、契約形態による役割分担モデルを説明。
	1.5 代表的なユースケース例	複数のサイバーインフラ事業者による役割分担について例示し説明。
2.サイバーインフラ事業者と顧客の責務と役割分担	2.1 責務と役割分担の考え方	事業者と顧客が協調しつつそれぞれの責務を果たす必要があることを説明。
	2.2 責務	事業者の5つの責務と、顧客の1つの責務を整理。
3.責務を果すための要求事項	3.1 要求事項の全体像	要求事項（6カテゴリ、21要求事項）の全体像を説明。
	3.2 要求事項	個別要求単位の説明。
4.要求事項の利活用	4.1 要求事項の要求パッケージ化	要求事項を、その目的・目標に応じて２分類し、パッケージとして整理。
	4.2 役割分担に応じた要求事項の適用に関する注意点	要求事項を適用する際のポイントを説明。
5.参考情報	5.1 要求事項チェックリスト	要求事項に関する情報を一覧で確認できるチェックリストを別紙として整理。
	5.2 セキュリティインシデントと要求事項の対応関係例	インシデント事例に対して、要求事項がどのようにリスクを軽減するのか、対応関係を説明。
	5.3 システムライフサイクルにおける脅威と要求事項の対応関係	脅威と要求事項の対応関係を参考情報として説明。
	5.4 要求事項に対する取組例	要求事項（個別要求）を実現するために対応すべき実施事項の例を参考情報として説明。
	5.5 統一基準群と本ガイドライン（案）との関係	統一基準群と本ガイドライン（案）の対応関係を整理。
	5.6 策定指針と本ガイドライン（案）との関係	策定指針と本ガイドライン（案）の対応関係を整理。
	5.7 参照情報	関連文書リスト、関連文書との対応関係を整理。
	5.8 用語	用語説明。
6.本ガイドライン（案）の検討体制		検討体制を説明。

3. 評価チェックリスト

評価チェックリスト案の更新

- 第４回検討会およびヒアリングのご意見を踏まえた主な更新内容は以下の通り。

①　より分かりやすい評価方法の説明および表記への見直し

②　評価の在り方の明確化

③　評価チェックリストの構成を検討

評価チェックリスト案の更新

① より分かりやすい評価方法の説明および表記への見直し

一定程度の信頼性を確保しつつ適切な自己評価を行えるよう、よりわかりやすい表記に見直し、および記載を補充。

見直しの観点	事務局対応案
表記の見直し	• 評価方法概説、評価エビデンスの記載を見直し 例えば、個別要求（(3)-2）の評価方法において、問題が発見された場合にセキュリティ勧告を作成することが明確になるように修正。
本チェックリストの位置付けの明確化	• 本ガイドラインに基づく自己評価により何らかの認証が得られるものではないことを明確化。
評価情報の取り扱いの注意点を補足	• 評価チェックリストの内容は機密情報に該当するケースもあり、取扱いに注意すべきことを補足。

評価チェックリスト案の更新

② 評価の在り方の明確化

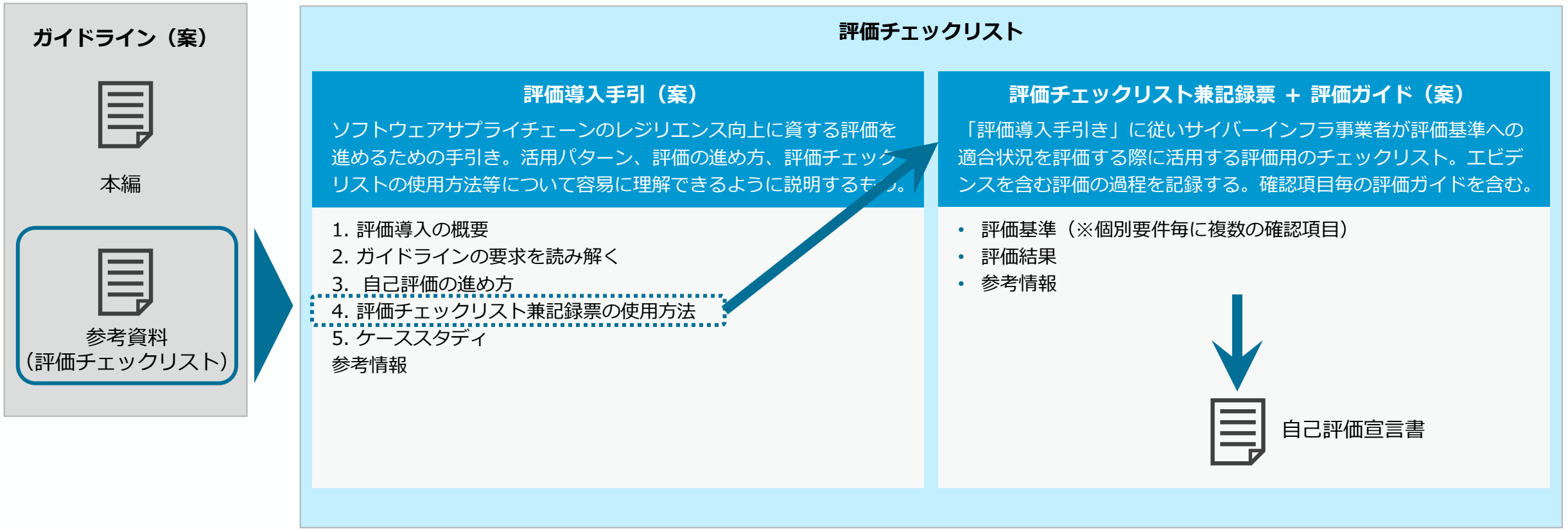
一定程度の信頼性を確保しつつ、評価負担を軽減するために評価項目を統合、削減。

評価の在り方の観点	事務局対応案
評価の在り方の明確化	• 評価の客観性担保と事業者の負担軽減のバランスを踏まえ、責務の各評価内容に対してエビデンスとなる文書・情報・記録・手続きなどの存在を確認することで、責務を理解しているか、対応する取組を行っているかどうかを評価することを明確化。 • その上で、必要に応じて（評価の深さに応じて）資料を双方で確認する方法や、宣言主体（事業者）と評価対象の差異を確認するために、個別のエビデンスを確認してもよいことを補足。 • 事業者の都合で評価項目を簡略化するのではなく、事業者と顧客の合意の下、対応する必要がない評価項目として、「N/A」という回答が選択できることを補足。
評価項目の統廃合	• 評価作業の負担を軽減するため、一定程度の信頼性を念頭におきつつ、評価項目を統廃合。
評価の活用方法の追加	• 役割分担の明確化という活用用途の一つとして、求められる評価基準と自社の取り組みとの「距離」を可視化するリスクコミュニケーションに活用することを追加。 • 顧客が自らの責務（S(6)）を記入し、事業者と役割分担の認識を共有することを明確化 • 顧客が、事業者に対応をもとめるS(1)からS(5)の個別要件を明確化する活用方法を追加。

評価チェックリスト案の更新

③　評価チェックリストの構成を検討

形骸化を防ぐため、評価チェックリストは、ガイドライン本体とは別文書として位置付け。



４．御意見をいただきたい事項

御意見をいただきたい事項

ガイドラインについて

① 検討会のご意見をふまえたガイドラインの修正は適切か

② 検討会のご意見をふまえた評価チェックリストの修正は適切か