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

資料４

事務局説明資料

2026年2月5日

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
   - 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（案）
   - （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
   - ソフトウェアサプライチェーンに関わる国内外の取組
   - 評価チェックリスト
4. 実証事業
   - 評価チェックリストの実証
   - （参考）実証結果と反映事項
5. 御意見いただきたい事項

1. 検討会について

検討会について

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

- 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

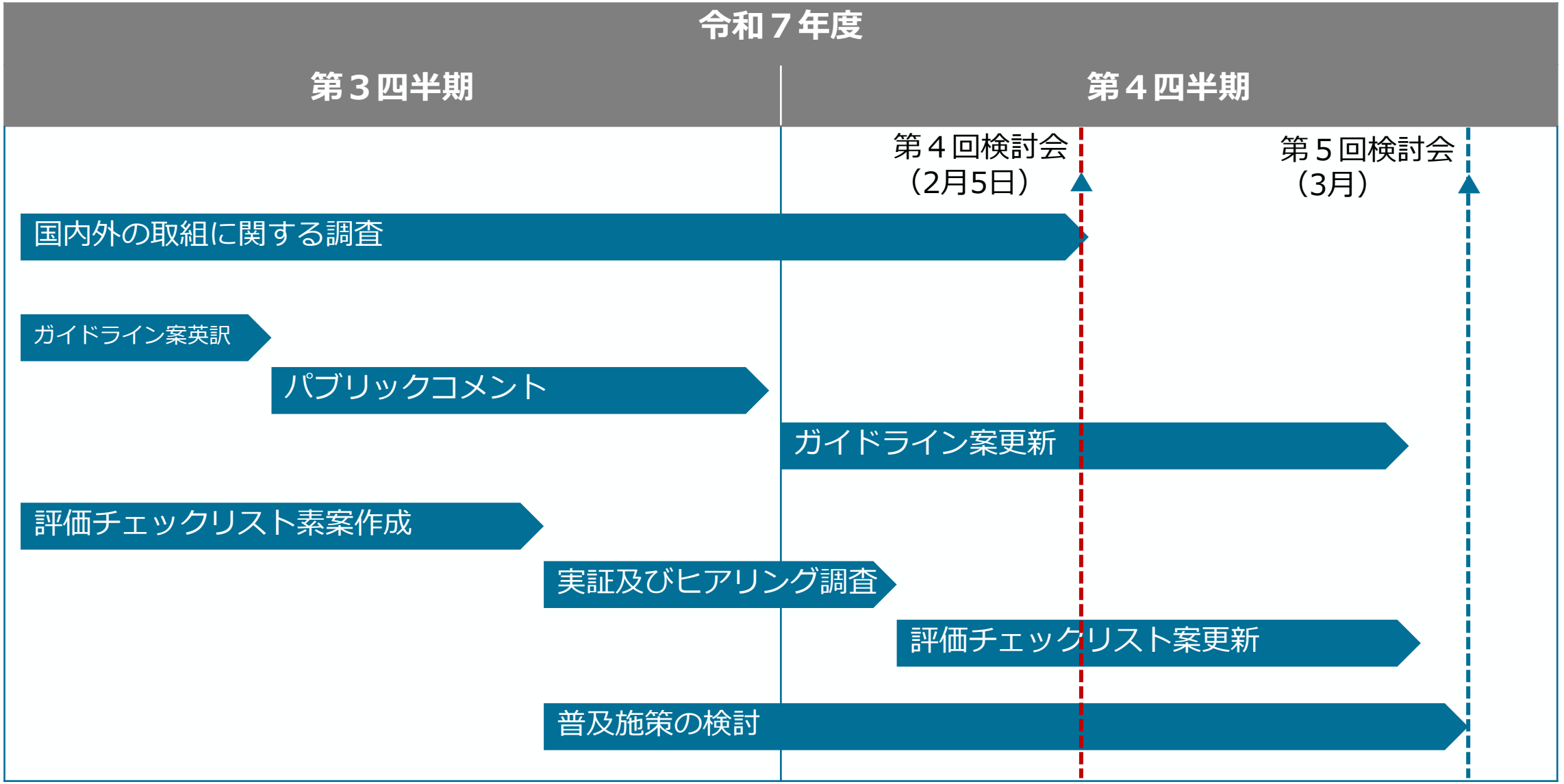
- ガイドライン本体案
  - サイバーインフラ事業者と顧客に求められる責務
  - 責務を果たすための要求事項
  - 参考情報　など
- 評価チェックリスト案
  - 評価導入手引き
  - 評価チェックリストとガイド

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
（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

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3月）	• ガイドラインの承認 • 評価チェックリストの承認 • 今後の普及方針の検討	

2. ガイドライン案

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、114件のご意見を受領。
- 頂いた御意見を踏まえ、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）	
意見数（※）	114件（23者）	
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

（※）1つの意見に複数種のコメントが含まれる場合は、分割して集計

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（案）

非公開

（参考）意見の概要と新旧の対照

非公開

（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

ソフトウェアサプライチェーンに関わる国内外の取組 ①

- 欧米を中心に、ソフトウェアサプライチェーンにおける脆弱性対策に関わる制度、ガイドライン類の整備が進む。
- セキュア・バイ・デザイン／デフォルトの概念が広まっており、サイバーインフラ事業者には、顧客との適切な役割分担のもと、自社が提供するソフトウェア製品のサイバーセキュリティ対策が求められている。

日本	
サイバーセキュリティ基本法	• 2025年7月の改正により、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（第7条第2項）。

欧州	
EU Cyber Resilience Act	• デジタル要素を備えた全ての製品（ソフトウエア含む）の製造者に対し、**セキュリティを考慮した設計、開発の評価や適合証明書を義務化。** • 2024年12月正式発効、2026年9月脆弱性報告義務化、2027年12月完全適用予定。

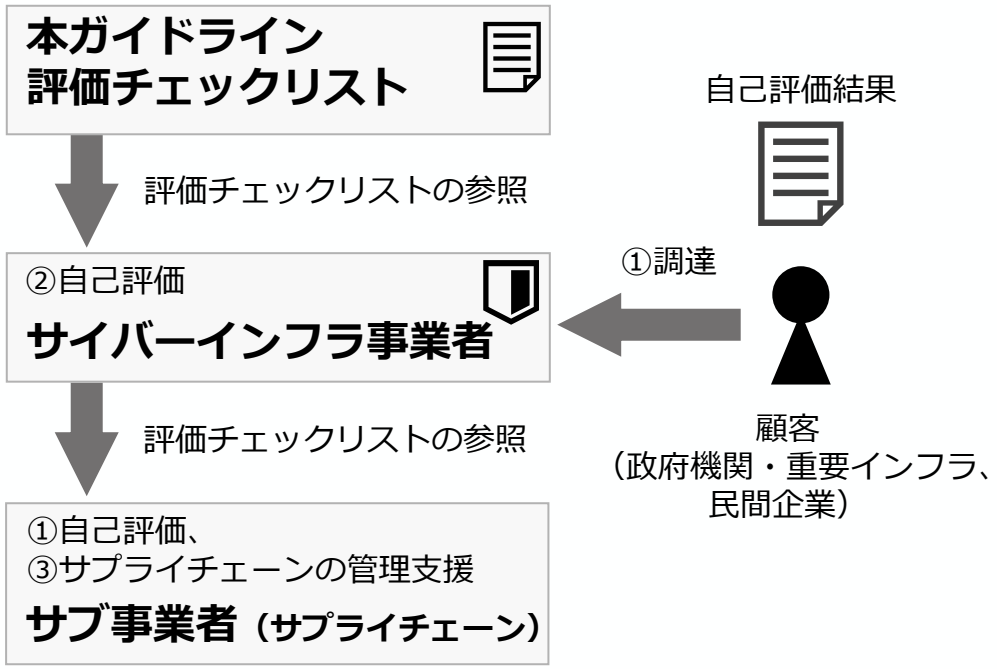
ソフトウェアサプライチェーンに関わる国内外の取組 ②

米国	
NIST SP800-218	• ソフトウェア開発者向けに、**ソフトウェアライフサイクル全体で**セキュアなソフトウェアを開発するための**フレームワーク**（Secure Software Development Framework：SSDF）。 • 2022年発行。
OMB M-22-18 （M-23-16に更新）	• DoDから、自己証明のみではなく、リスクベースアプローチに基づくSCRMプログラムを新たに開発する方針が発表。

英国	
Software Security Code of Practice	• 英国におけるソフトウェアサプライチェーンのセキュリティを向上させるための自主的ガイドライン。自己評価を基本。

評価チェックリスト －概要－

- ガイドラインの活用促進に向けた付属文書として、セキュリティの取組を責務として認識し実施していることを自己評価するためのチェックリストを整理した。
- 事業者の自主的な責務向上の取り組みを促すと共に、**顧客が開発運用を依頼するソフトウェアに対してリスクベースで求める水準を定義したうえで、これに基づき事業者が対策を実施**する際に、**一定程度の信頼性を確保**しながら顧客によるセキュアなソフトウェアの選択をサポートするためのツールとして位置付け。



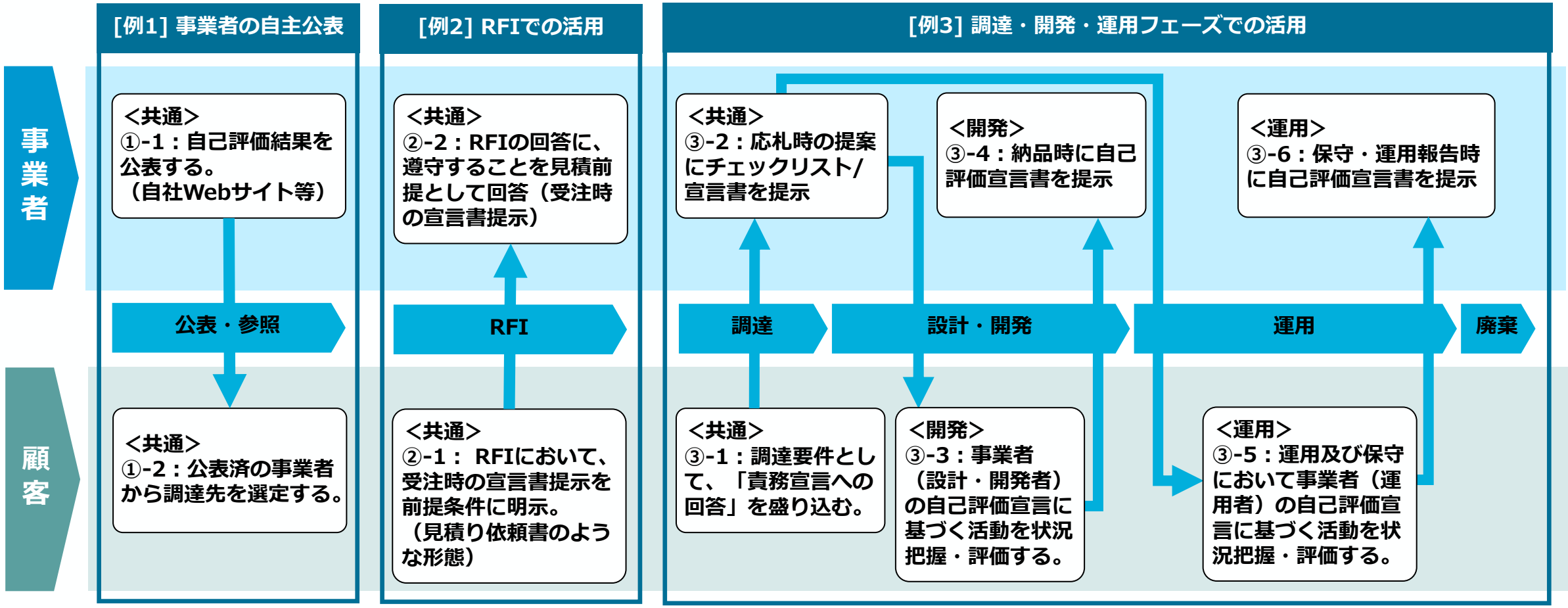
	用途例	概要	活用シナリオ例（次頁）
①	役割分担の明確化	• ソフトウェアの特性に応じて、事業者と顧客が担うべき役割や実施すべき対策を責務として特定し、役割分担とその実施状況の可視化に活用する。	【例2】 【例3】
②	事業者単体での責務レベルアップ	• 事業者が自社の取組レベルアップに活用する。	【例1】
③	サプライチェーン先の責務レベルアップ・管理	• プライム事業者がソフトウェアサプライチェーンを管理するためのツールとして利用する。	【例3】

評価チェックリスト －活用シナリオ－

事業者がセキュリティ対策への取組みをアピールできる。

RFIする際に、顧客の責務履行を前提として、事業者の責務への取組方針について回答する。
遵守事項として、取組方針（チェックリストに基づき業務を実施）を提出し、RFP以降のフェーズで実態との適合性を精査し、適合していない部分を是正していく。

顧客側が入札仕様として責務（チェックリスト）を提示する際に自組織の記入欄を埋めておき、事業者へ追記を依頼。事業者が追記した宣言内容を両者が共有することで、責務と役割分担の認識共有を支援する。その際、顧客が開発運用を依頼するソフトウェアに対してリスクベースで求める水準（満たすべき個別要求）を検討した上で、事業者はこれに基づき責務を実施する。



評価チェックリスト －文書構成－

ガイドライン（案）

本編

参考資料
（評価チェックリスト）

参考資料：評価基準案（一式）

評価導入手引（案）

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。

1. 評価導入の概要
   1.1. 自己評価とは（評価導入の意義）
   1.2. 自己評価結果の活用パターン
2. ガイドラインの要求を読み解く
   2.1. 適用範囲と役割分担
   2.2. 要求事項の構成
   2.3. 評価レベルとは
3. 自己評価の進め方
   3.1. 自己評価プロセスの全体像
   3.2. 自己評価の準備
   3.3. 自己評価の実施
   3.4. 評価結果の分析・是正対応
   3.5. 自己評価宣言書の作成
   3.6. 維持・改善
4. 評価チェックリスト兼記録票の使用方法
   4.1. 準備段階
   4.2. 評価実施段階
   4.3. 評価結果の分析・是正段階
   4.4. 自己評価宣言書の作成・利用段階
5. ケーススタディ
   評価例（全社単位、部門単位、 製品・サービス単位など）

参考情報

評価チェックリスト兼記録票 ＋ 評価ガイド（案）

「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を記録する。確認項目毎の評価ガイドを含む。

- 評価基準（※個別要件毎に複数の確認項目）
  - 評価レベル
  - 評価内容（≒適合基準）
  - 評価方法概説
  - 確認すべきエビデンス
    （ドキュメント、運用状況の確認・記録）
  - 適合判定基準解説（適合・改善予定・N/A）
- 評価結果
  - 適合判定（適合・改善予定・N/A）
  - 適合判断根拠（評価方法に沿って適合判断した根拠・理由
    （合否・N/Aいずれの場合も記載））
  - 改善計画
- 参考情報
  - 個別要求（※関連するガイドラインの項番）
  - 役割（※関連するガイドラインの役割）
  - 参考とすべき規定・ガイドとの関係

自己評価宣言書

評価チェックリスト －評価の流れ－

① 役割、評価レベルを選択し、実施すべき項目を一覧表でフィルタリング

役割	開発者
	供給者
	運用者
	顧客
評価レベル	最低限要求
	標準要求

② 評価項目ごとにガイドラインを参照しつつ、評価を実施。
「評価方法概説」に従い、「確認すべきエビデンス」の有無を確認。
「適合」「改善予定（未適合）」「N/A（対象外）」を自己評価。

■ 評価結果一覧表

評価ID	評価レベル	評価内容	役割	ガイドラインへの適合判定	検出事項・適合判定根拠（社内用）	検出事項・適合判定根拠（公開用）	改善計画
S(1)-1.1.1.1.1	最低限/標準			【評価結果入力A】	【評価結果入力B】	【評価結果入力C】	【評価結果入力D】
S(1)-1.1.1.1.2	標準						
		…					

■ 評価ガイドシート（評価項目別のワークシート）

評価基準	評価ID	S(1)-1.1.1.1.1
	評価レベル	最低限/標準
	評価内容	○○の資料や情報がある。
	評価方法概説	ドキュメント評価：ソフトウェアの脆弱性が発見された…
	確認すべきエビデンス	…○○ドキュメント
	適合判定基準概説	[最低限]の項目が満たすことが確認できる場合に限り、「適合」と判定する。
評価結果	ガイドラインへの適合判定	**【評価結果入力A】**
	検出事項・適合判定根拠（社内用）	**【評価結果入力B】**
	検出事項・適合判定根拠（公開用）	**【評価結果入力C】**
	改善計画	**【評価結果入力D】**
参考情報	個別要求ID	S(1)-1.1
	個別要求タイトル	リスクベースのセキュリティ要件の定義
	個別要求内容	開発するソフトウェア、あるいはソフトウェアで構成されるシステム・サービスに対して、リスクベースの分析…
	…	

③ 評価結果一覧表とワークシートの評価結果を相互反映。

自己評価宣言書

適合結果（宣言内容）
S(1)　適合
S(2)　適合
S(3)　適合
S(4)　適合
S(5)　適合

④ 評価結果は責務単位で自動集計（該当箇所が全て「適合」の場合に、「適合」）

自己評価宣言書（別紙）

S(1)-1.1：…
S(1)-1.2：…
…

⑤ 事業者が希望する場合、「検出事項（公開用）」の記載内容を、顧客に提示する。

４．実証事業

評価チェックリストの実証 －実証事業対象の選定－

- 評価チェックリストの有効性を確認するため、政府調達の実績を有するプライム事業者を中心に協力を依頼し、各社のソフトウェアプロジェクトに評価チェックリストを適用頂いた。

実証事業者	実証内容
A社	プライム事業者として政府調達での実績が豊富であり、**SI（開発委託）プロジェクト**を対象に実証に参加頂いた。
B社	大手企業であり、**IoT等の組み込み製品を含むプロジェクト**を対象に実証に参加頂いた。
C社	**中堅企業の観点でクラウドサービス**のプロジェクトを対象に実証に参加頂いた。

事前準備

11月下旬

- 評価チェックリスト等一式を事業者に配布し、事業者にWeb会議で説明。

実証

12月

- 「評価の骨子や基本コンセプトの受容性」、「事業者の開発運用プロセスとの根本的な不整合の洗い出し」を目的に、実証を通じて御意見を頂いた。
- 「具体的なチェック項目の実現可能性評価」を目的に、「評価チェックリスト」に実証コメントの記入欄を設け、評価項目毎に直接コメントを頂いた。

ヒアリング

1月上旬

- 実証後に、ヒアリングを実施し、実証全体を通じた評価作業への意見を詳細に収集。
- 評価基準の実効性を高める観点から、分析。

評価チェックリストの実証 －実証結果と反映事項（案）－

- 評価関連文書類の改善ポイントや考慮事項について、4つの観点から御意見いただいた。対応事項を、短期と中長期に分類した上で、今年度の反映事項案を検討。

頂いた主な御意見	今年度の反映事項（案）
評価基準の客観性	[1] 評価内容、評価方法等において補足説明を行う。 [2] 用語集を整備する。 [3] エビデンスについて補足説明と例示を追加する。 [4] 評価導入手引きを整備し、評価の方針・在り方を説明する。 [5] 評価項目が詳細すぎることで評価が難しくなっている部分は、評価内容を統合する。 [6] 個別要求（責務）と評価内容の対応関係の理解を促すよう、一覧表を用意する。
評価作業の負担	[4] 評価導入手引きを整備し、評価の方針・在り方を説明する。 [5] 評価項目が詳細すぎることで評価が難しくなっている部分は、評価内容を統合し評価工数を削減する。 [6] 個別要求（責務）と評価内容の対応関係の理解を促すよう、一覧表を用意する。
評価の有効性	[1] 評価内容、評価方法等において補足説明を行う。 [4] 評価導入手引きを整備し、評価の方針・在り方を説明する。 [7] 評価の目的を補足説明する。
評価結果の活用 （自己評価宣言を含む）	[4] 評価導入手引きを整備し、評価の方針・在り方を説明する。 [8] 御意見を踏まえた宣言内容を検討する。 [9] 評価チェックリストを拡充する。

（参考）実証結果と反映事項（案） – 評価基準の客観性 –

頂いた御意見のカテゴリ	頂いた主な御意見	御意見への対応の考え方（案）
用語／前提の曖昧さ	• 用語や前提の定義が曖昧であり、評価者の解釈差が客観性を損ねる可能性がある。	【今年度対応事項】 [1] 評価内容、評価方法等において補足説明を行う。（用語や前提の説明） [2] 必要に応じて、用語集を整備する。
役割の重複	• サービス、システム、開発インフラ、運用インフラごとに同じような項目があるように見える。 例：S(4)：開発ポリシーの評価と運用ポリシーの評価	【今年度対応事項】 [4] 評価導入手引きを整備し、評価の方針・在り方の説明を行う。（ガイドライン本体が役割別であることを説明）なお、責務・要求事項として開発と運用の役割分担を明確化する意図であるため、評価内容は現状を維持する。
評価内容の偏り・曖昧さ	• 評価内容が、サーバアプリ開発の実施例に偏っているように見える。 • 評価すべき事項が不明瞭である。 例：「設計がセキュリティリスクの緩和に効果があることが確認できるレビューの観点」	【今年度対応事項】 [1] 評価内容、評価方法等において補足説明を行う。
	• 評価内容単体で理解ができない。	【今年度対応事項】 [5] 評価項目が詳細すぎることで評価が難しくなっている部分は、評価内容を統合する。

（参考）実証結果と反映事項（案） – 評価基準の客観性 –

頂いた御意見のカテゴリ	頂いた主な御意見	御意見への対応の考え方（案）
必要なエビデンスが不明確	• 求められているエビデンスが不明確 例：S(1)-4：「資産の把握の手順の資料」	【今年度対応事項】 [3] エビデンスについて補足説明と例示を追加する。 【将来的な検討課題】 • 評価項目を「契約で担保すべき事項」「技術的に担保すべき事項」「運用で担保すべき事項」に分け、誰が何を出すかをセットで提示する。
	• 評価項目に直接合致しないエビデンスで適合を主張する方法がわからない	【今年度対応事項】 [4] 評価導入手引きを整備し、評価の方針・あり方の補足説明を行う。（代替エビデンスのあり方を説明）
評価方法が複雑	• 評価内容、評価項目、合否判定基準を全文読んだうえで内容をかみ砕いて判断するのは手間を要する。〇×だけで結果が出せるとよい • 特定のエビデンスがあればOKというレベルに落とし込めていないため、内容解釈から始めなければならない • どこまでで適合と言えるかの判断が難しい	【今年度対応事項】 [1] 評価内容、評価方法等において補足説明を行う。（判断が容易な表記に修正）
	• 何の対象か、どの項目とのつながりか等が読み取りにくく、評価内容単体で理解しづらい箇所がある	【今年度対応事項】 [6] 個別要求（責務）と評価内容の対応関係の理解を促すよう、一覧表を別途用意する。

（参考）実証結果と反映事項（案） – 評価基準の客観性 –

頂いた御意見のカテゴリ	頂いた主な御意見	御意見への対応の考え方（案）
評価対象の曖昧さ	• 評価単位（組織・事業・プロダクト・案件）が明確ではなく、評価コストが余計に生じる可能性がある 例：S(5)-2：自プロジェクトとしてはコミュニティに関与していないが事業者として関与しているケースの取り扱い	【今年度対応事項】 [1] 評価内容、評価方法等において補足説明を行う。（評価単位を補足説明）
客観性の向上	• 評価者向けのトレーニングや相互レビューが必要 • 重要項目はサンプリング監査（第三者/顧客）を検討すべき	【将来的な検討課題】 • 他制度との関係性を含む評価のサポートツールを整備する。

（参考）実証結果と反映事項（案） – 評価の負担 –

頂いた御意見のカテゴリ	頂いた主な御意見	御意見への対応の考え方（案）
評価項目数の多さ	• 項目数が多く、記入負担が増加しやすい。 • “やったほうが良い”レベルと“必須”が混在すると、現場は網羅埋めに引きずられがちになる • 実施して、全て適合しなければいけないのか • 評価項目ごとに「必須証跡（最低1つ）」と「代替証跡（いずれか）」を提示し、実態に即した確認を可能にする	【今年度対応事項】 [5] 評価項目が詳細すぎることで評価が難しくなっている部分は、評価内容を統合する。 なお、「標準パッケージ」を原則とすることから、評価項目数は現状を維持する。 【将来的な検討課題】 • 証跡リンク集約、入力チェック（未入力/矛盾）強化、依存関係表示の追加（上位の質問がNAなら下位もNA等）、Webフォーム化等
評価の判断の難しさ	• 項目間の依存関係（前提/後続）が読み取りにくく、記入負担が増加しやすい。 • 評価項目の大まかな分類などがわかると実施しやすい	【今年度対応事項】 [6] 個別要求（責務）と評価内容の対応関係の理解を促すよう、一覧表を別途用意する。
過剰なエビデンス	• エビデンスが過剰である 例：S(4)-2：経営層の認識を証跡に敢えて記録させることは過剰である。 • あらたにエビデンスを整備することは過剰である 例：S(1)-3：セキュリティに特化したテスト計画を別に作成するのは過剰 S(4)-2：セキュア開発のみの予算を切り出すことを評価項目とするのは過剰	【今年度対応事項】 [4] 評価導入手引きを整備し、評価の方針・在り方の説明を行う。（確認できれば手段は問わないこと、別のエビデンスを作成することを前提としていないことを明確化）

（参考）実証結果と反映事項（案） – 評価の負担 –

頂いた御意見のカテゴリ	頂いた主な御意見	御意見への対応の考え方（案）
過剰な要求事項	• 現実的ではない要求事項が存在する 例：S(2)-3：全ての外部調達ソフトウェアコンポーネントにセキュリティ要件の合意をすることは現実的ではない。 S(3)：運用現場では脆弱性情報が大量に流通するため、全件同一水準での対応を求めると運用不能になり得る	【今年度対応事項】 [4] 評価導入手引きを整備し、評価の方針・在り方の説明を行う。（評価内容について誤解のないよう補足）

（参考）実証結果と反映事項（案）－評価の有効性－

頂いた御意見のカテゴリ	頂いた主な御意見	御意見への対応の考え方（案）
評価の根拠が不明確	• 評価の内容が、セキュリティの確保につながることが理解できない。 例：S(1)-2：プラクティスの定義がある事業者が、定義のない事業者よりセキュアであるとは言えない S(5)-1：情報連携において、セキュアになる項目か理解できない	【今年度】 [7] 評価の目的を補足説明する。（セキュリティとの関連性を補足）
様々な評価対象への適合性	• 評価対象の全てのソフトウェア種別に対して評価を行うことが明確ではない • 全てのソフトウェア種別の評価が困難な評価内容が存在する。 例：S(2)-1：CaCを明示することで、レガシーなシステムを考慮していない • 組織やプロジェクトの規模などで整備状況や基準が変わると思われるため妥当かどうか判断が難しい • 組込み・サーバ開発・クラウド開発など開発のなかでも異なる視点や状況の評価判断をサポートされるとよい	【今年度】 [4] 評価導入手引きを整備し、評価の方針・在り方の説明を行う。（様々な評価対象に適用できるよう説明を補足） 【将来的な検討課題】 • 評価のサポートツールを整備する。
役割の偏り	• 特定の役割に責務が偏っている。 例：S(1)-1：ソフトウェアライフサイクル全体で維持管理する要件を開発者だけに課している	【今年度】 [1] 評価内容、評価方法等において補足説明を行う。（役割分担を前提としていることを補足）

（参考）実証結果と反映事項（案）－評価結果の活用－
（自己評価宣言時の課題）

頂いた御意見のカテゴリ	頂いた主な御意見	御意見への対応の考え方（案）
適切な事業者の取組を誤って判断される懸念	• 顧客から「N/A」項目を不適合判定される懸念 • オール適合が要求されることによるガイドライン自体の形骸化	【今年度】 [4] 評価導入手引きを整備し、評価の方針・在り方の説明を行う。（「N/A」の位置付けを補足説明する） 【将来的な検討課題】 • 改善途上にある場合にも、適切な主張ができるよう、改善計画欄を拡充する。
宣言書に公開すべき情報	• 対象範囲（組織/事業/プロダクト、バージョン、提供形態）、評価実施日、要求セット（必須/推奨） • 評価結果（達成レベル/未達項目の有無）と、未達がある場合の改善計画（期限・責任者） • 問い合わせ窓口（脆弱性報告窓口含む）と、更新ポリシー（再評価トリガ）	【今年度】 [8] 御意見を踏まえて、宣言内容を検討。
	• 事業者と顧客間での評価結果共有は、機密区分と開示範囲（顧客内/業界内/公表）を分ける必要がある。	【今年度】 [9] 評価チェックリストを拡充する。（評価時に、公開情報と機密情報を分ける欄を用意し、公開情報のみを宣言）
	• 公開できる情報と公開できない情報は企業によって考え方がまちまちであるため、国が統一的な見解を示すことも有効。 例：サイバーセキュリティ対策情報開示の手引き（総務省）	【将来的な検討課題】 • 情報開示の基準を検討する。

（参考）実証結果と反映事項（案） – 評価結果の活用 –

頂いた御意見のカテゴリ	頂いた主な御意見	御意見への対応の考え方（案）
プロセス改善への貢献	• 改善計画欄は、期限・担当（役割）・短期の暫定策/恒久策・残存リスク受容の判断者、まで記載できる形が望ましい。 • チェック結果を「リスクベースでの優先度（重大度×影響×露出）」に落とし込めると、改善計画に直結しやすい。	【将来的な検討課題】 • 改善計画欄を拡充する。 • 同一テーマの重複項目は集約（一括入力）し、改善アクションを対策パッケージごとに示す
セキュリティ意識の向上	• 役割別に「なぜ必要か（想定被害）」と「最低限の実装例」を併記すると、単なるチェック作業から学習に転換できる。	【将来的な検討課題】 • リスクと評価項目との対応関係を示す。
評価の推奨タイミング	• 調達/RFI（要求水準合意）→契約締結（責務・SLA）→基本設計/詳細設計（S(1)(2)）→リリース前（検証・証跡確定）→運用開始後の定期（S(3)(5)中心）を推奨。 • 大きな構成変更・重大脆弱性対応のタイミングで“臨時評価”を入れると実効性が高い。	【今年度】 [4] 評価導入手引きを整備し、評価の方針・在り方の説明を行う。（活用例として盛り込む）
支援コンテンツの整備	• 業界/企業規模により成熟度が大きく異なるため、段階的導入と支援コンテンツ（用語集・証跡例・テンプレ）が必要。 • 他の文書との関係を体系的に整理いただいた方が利用者としてはありがたい。	【将来的な検討課題】 • サポートツールを検討する。 • 既存取組との接続を検討する。

（参考）実証結果と反映事項（案）－評価結果の活用－

頂いた御意見のカテゴリ	頂いた主な御意見	御意見への対応の考え方（案）
下流（再委託・部品等）のリスク洗出し	• サプライチェーンとして見たとき、サブ事業者にもプライム事業者にも同じ項目を同じように適用する場合、重複した対応が必要となり、コスト増が想定される。	【今年度】 [4] 評価導入手引きを整備し、評価の方針・在り方の説明を行う。（プライム事業者に適用し、サブ事業者にはその責任範囲においてプライム事業者がとりまとめるチェックに協力する方針を例示）
	• S(2)の透明性（SBOM/部品情報）とS(3)の脆弱性対応を接続する取組を行う。	【将来的な検討課題】 • 下流に責務を求めるための契約条項（通知義務、EOL、サポート、SBOM提供等）の“標準例”を整備する
普及施策	• 評価チェックリストを使うことによる事業者側のメリットが明確でないと普及しづらい。このガイドラインに則った対応を行えばお墨付きがあるとよい。 • 提案要件にガイドライン準拠があれば、一定程度の義務感は生じる。 • 業界団体と連携した標準条項（通知SLA、SBOM、EOL等）等の提供。 • 「サプライチェーン強化に向けたセキュリティ評価制度」に取り組む上で、このガイドラインが有用である（満たすべき評価項目である）といった関連性があれば、ガイドライン普及の動機付けになる。 • リスクとの関係、ガイドとの関係、責務や要求事項と評価内容の関係がわからないとモチベーションが上がらない。	【将来的な検討課題】 • 既存取組との接続を検討する。

（参考）委員御意見と反映事項（案） – 評価結果の活用 –

頂いた御意見のカテゴリ	頂いた主な御意見	御意見への対応の考え方（案）
普及施策	• 所轄官庁による監督が明確な金融機関等と異なり、そうでない事業者もいるため、政府が発行する本ガイドラインには、より強制力を持たせても良いとの声があった。 • Excel形式の評価チェックリストについて、セキュリティ上の理由から企業によってはマクロの実行が制限されている可能性がある。	【将来的な検討課題】 • 既存取組との接続を検討する。 • サポートツール（Webシステム等）を検討する。

御意見をいただきたい事項

1．ガイドラインについて

- パブリックコメントをふまえたガイドラインの修正は適切か
- 付属文書として、評価チェックリストの内容は適切か
  - 評価内容、評価方法は適切か
  - 検討すべき事項があるか

2．今後の普及展開に向けて

- 評価チェックリストを含むガイドラインの今後の普及施策の検討について

（参考）サイバーインフラ事業者のセキュリティ対応強化に向けた支援策について

- 「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」で求められる取組には、**PSIRTの設置**（S(3)-1.1 脆弱性対応体制の設置）や**SBOMの導入**（S(2)-1.3 ソフトウェアコンポーネントのリスク評価）など、特にリソースの限られる**中小企業にとって実施のハードルが一定程度高い**ものも存在。
- 取組支援策として、令和７年度補正予算事業等により**実証及びガイド作成**等を実施予定。

PSIRTの構築・運用及びSBOMの導入支援

- 人的・予算的制約がある中でもPSIRTの構築・運用及びSBOMの導入を効率的かつ効果的に実現するための実証事業を行い、その成果物として、上記ノウハウを集約した実践ガイドを作成予定。

地域ITベンダー向け手引きの作成

- 中小企業にとってサイバーセキュリティ対策を実施する際の主たる相談相手となる地域のIT関連企業が、その重要な役割を果たすために活用可能な、人材育成・活用策を含めた手引きについて、「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」との整合性も確保しつつ、IPAにて別途作成中。

<PSIRT構築・運用等支援事業のイメージ>