令和7年度産業サイバーセキュリティ対策の強化に向けた環境整備事業
（サイバーインフラ事業者に関わる責務と基本的取組等の調査）

調査報告書

2026年3月
みずほリサーチ＆テクノロジーズ株式会社

目　次

1. 事業の目的、実施内容

(1) 事業目的

- 我が国の「サイバーセキュリティ基本法」（平成26年法律第104号）第７条においては、サイバー関連事業者（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）その他の事業者の責務が規定されている。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（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）（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・検討が求められており、上記の調査・検討のため、令和６年度に「サイバーインフラ事業者に求められる役割等の検討会（経済産業省 産業サイバーセキュリティ研究会 ワーキンググループ１及びサイバーセキュリティ戦略本部 重要インフラ専門調査会の合同ワーキンググループ）」が開催されてきた。
- 本事業は、同検討会の成果である「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）」（以下、「ガイドライン案」という。）を踏まえた、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」という。）の策定に向けて、必要となる調査の実施、「サイバーインフラ事業者に求められる役割等の検討会」（以下、「検討会」という。）の運営、ガイドライン案の更新、ガイドラインの活用促進に向けた自己適合宣言制度の案の作成とその実証等を行うことを通じて、サイバーインフラ事業者によるレジリエンスの向上及びサイバーセキュリティの根本的確保の推進を目的として実施する。

1. 事業の目的、実施内容

(2) 実施内容

- 本事業で実施した調査は次表の通りである。調査結果の詳細は本報告書第2章以降で示す。

No.	実施項目	実施内容
1	国内外の関連動向に関する文献調査	• ガイドライン及び自己評価宣言に必要な要素を検討するため、自己適合宣言制度を念頭に国内外のサイバーセキュリティ対策に関する取組等を調査した。
2	検討会の運営	• 顧客も含めた様々なサイバー関連事業者が合意し取組が可能なガイドラインとするために、有識者や有志のサイバーインフラ事業者等12名の有識者からなる検討会を設置し、2回にわたる開催にあたっての事務局運営を担当した。 • 検討会での議論を受けて、関連するサイバーインフラ事業者等にヒアリング等を実施し、検討会へインプットした。
3	ガイドライン案の更新等	• 調査や検討会の内容も踏まえ、ガイドライン案の更新、ガイドラインの活用促進に向けた自己評価宣言案等の作成を行った。
4	自己適合宣言制度の実行性確保に向けた実証	• 自己適合宣言制度の一部として、自己評価宣言について、企業の協力を得て、実証に向けた評価項目を検討のうえ実証事業を実施し、実証結果についての評価を行った。 • 実証事業では、ガイドラインにおいて示す、サイバーインフラ事業者が求められる責務を果たすための要求事項について、サイバーインフラ事業者における達成度を確認した。
5	英訳	• ガイドライン案の本編及びガイドライン案概要説明資料の２点を英訳対象文書とし、事業開始後及び更新後の２回英訳を行った。

2. 国内外動向に関する文献調査

(1) 調査概要

- 調査目的
  - これまでサイバーインフラ事業者に関わる具体的な「責務と基本的取組」の調査研究が実施されてきたところ、同調査研究の成果である具体的なガイドライン（案）に基づく自己評価宣言に必要な要素を検討するため、国内外のサイバーセキュリティ対策に関する法、制度、取組及び動向を調査する。

- 実施方法
  - 本事業で実施した調査は次表の通りである。

対象国・地域	• 米国、欧州の他、先進的な取組を進める英国を対象とした。
出典	• 当該対象国のガイドライン、法令の他、国際標準も対象とした。

2. 国内外動向に関する文献調査

(2) 調査結果

- 本事業で実施した調査対象文献は次表の通りである。

地域・国等	公表年	文献名称
日本	2005	JIS Q 17050
英国	2014	UK Cyber Essentials
英国	2022	Product Security and Telecommunication Infrastructure Act
英国	2025	Software Security Code of Practice
EU	2024	EU Cyber Resilience Act
米国	2023	OMB M-23-16

2. 国内外動向に関する文献調査

(3) 調査結果詳細　―諸外国のサイバーセキュリティ確保の取組―

- JIS Q 17050
  - 製品やサービス、プロセス、マネジメントシステムなどが規定された要求事項に適合していることを、供給者自身が宣言する際の一般的なルールを定めた国際規格ISO/IEC 17050を日本国内での運用に合わせて翻訳・調整したもの

JIS Q 17050（適合性評価 ー 供給者適合宣言 ー）	
公表年	2005年7月20日（JIS Q 17050-1の場合）
出所	日本産業規格（JIS）
対象事業者（顧客 or 事業者）	供給者（事業者：第一者が対象）
適用範囲	宣言の中で被監査主体、監査対象組織の責任者が指定。次の事項により構成される。 ①組織（本社／拠点等）②事業・業務・情報資産等 ③関係する人（例：全従業員）
宣言の責任者	宣言者が自ら指定（通常、組織の責任者／代表者）
評価者	自己評価（第一者）、必要に応じて第二者／第三者評価も可
有効期間	明示されていない。対象の適合性や信頼性に重大な影響を及ぼす可能性のある、設計・仕様・規格・経営構造の変更、または不適合の可能性を示す情報の発生があったタイミング
保証方法	適用範囲・セキュリティ水準を設定し、自己適合宣言書を作成し、内部監査を実施する。
開示範囲	開示範囲に制限はなくリスクレベルに合わせて設定（例：自組織のPRを目的→一般公開、業務委託契約締結目的等→個別提示）
宣言の様式	印刷物／電子媒体／その他の適切な形式

2. 国内外動向に関する文献調査

(3) 調査結果詳細　―諸外国のサイバーセキュリティ確保の取組―

- UK Cyber Essentials
  - 英国政府が策定したサイバーセキュリティ認証制度
  - 自己評価に基づくCyber Essentialsと、第三者検証が必要なCyber Essentials Plusの2種類の認証レベルがある

UK Cyber Essentials	
公表年	2014年6月5日施行
出所	英国政府（IASME（NCSC公認認証機関））
対象事業者（顧客 or 事業者）	インターネット接続のあるシステムを使用するすべての組織（商用、非営利、教育、官公庁問わず）
適用範囲	組織のITインフラ全体（PC、サーバー、ネットワーク機器、BYOD等）
宣言の責任者	組織内のセキュリティ担当者
評価者	Cyber Essentials：自己評価（第一者）、Cyber Essentials Plus：自己評価に加え、第三者によるテスト・検証実施
有効期間	認証取得後1年間有効。毎年更新が必要。
保証方法	2種類の認証レベルが存在する5つの技術的コントロールに基づき、自己宣言または第三者検証を実施
開示範囲	政府調達・取引先への信頼証明として利用
宣言の様式	Webフォーム（自己評価）または監査報告書により認証申請
運用スキーム	■ Cyber Essentials：**自己申告**（Webフォーム）＋認証機関によるレビュー ■ Cyber Essentials Plus：Cyber Essentialsの要件に加え、**外部審査員によるシステムテストと構成検証**

※2025年時点の情報に基づき整理。 UK Cyber Essentials は定期的に内容が更新されており、2026年4月に大幅な更新予定。

2. 国内外動向に関する文献調査

(3) 調査結果詳細　―諸外国のサイバーセキュリティ確保の取組―

- Product Security and Telecommunication Infrastructure Act
  - 英国におけるIoT製品のセキュリティと通信インフラを強化するための法令
  - IoT製品を輸入・販売・製造する者に対して3つのセキュリティ要件を課している

製品セキュリティおよび通信インフラストラクチャ法規制（PSTI法: Product Security and Telecommunication Infrastructure Act）	
公表年	2022年12月7日成立、2024年4月29日施行
出所	英国議会による法令（UK Public General Acts（PGA）2022/46）
対象事業者（顧客 or 事業者）	英国における製品の市場流通関係者（**製造者、輸入者、販売者**）。輸入・販売する場合もPSTI法に準拠した製品かを確認する必要あり。
適用範囲	英国で販売されるインターネットもしくはネットワークに繋がる製品（例：スマートフォン、スマートスピーカー、ハブ、ウェアラブルヘルストラッカ、GPS機器、ホームオートメーションシステム、洗濯機や冷蔵庫などのスマート家電等）
宣言の責任者	**製造者**（輸入者・販売者は製造者の宣言（SoC: Statement of Compliance）の確認義務あり）※ 役職に関して明確な記載なし
評価者	自己評価（第一者）、必要に応じて第二者／第三者評価 ※ 明確な記載なし
有効期間	明確な記載なし
保証方法	セキュリティ要件（**①デフォルトパスワード禁止 ②脆弱性報告窓口設置 ③セキュリティ更新期間明示**）の遵守およびSoC作成と添付
開示範囲	製品にSoCを添付して提供
宣言の様式	アクセス可能なもの（印刷物／電子媒体／その他の適切な形式）
運用スキーム	製造者がSoCを作成し、輸入者・販売者がそれを用いて販売するのが基本。製造者が提供しない場合は輸入者・販売者が代理作成。

2. 国内外動向に関する文献調査

(3) 調査結果詳細　―諸外国のサイバーセキュリティ確保の取組―

- 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

Software Security Code of Practice	
公表年	2025年5月7日公表
出所	英国政府（National Cyber Security Centre（NCSC）およびDepartment for Science, Innovation & Technology（DSIT））
対象事業者（顧客 or 事業者）	主にソフトウェアの開発者・提供者（SaaSベンダー等）※ 一部再販会社・社内開発者にも適用
適用範囲	商用ソフトウェア
宣言の責任者	組織の上級管理職（SRO: Senior Responsible Owner）
評価者	**自己評価**を基本とする
有効期間	明確な記載なし（提供者はサポート終了の1年前に通知すべきと記載）
保証方法	14の原則（テーマ：①セキュアな設計・開発、②ビルド環境のセキュリティ、③安全な展開と保守、④お客様とのコミュニケーション）に従い、**組織内で各原則の実施と文書化**が必要。
開示範囲	**法的強制はない**が、顧客や調達先との契約交渉で活用
宣言の様式	原則ごとに複数の項目が用意され、その証拠を入力できる**自己評価フォームが用意されている**
運用スキーム	法的強制力はないが、ソフトウェアを開発・販売する事業者に実施を奨励している

2. 国内外動向に関する文献調査

(3) 調査結果詳細　―諸外国のサイバーセキュリティ確保の取組―

- Cyber Resilience Act
  - EU域内で流通するすべてのデジタル要素を含む製品に対して、統一されたサイバーセキュリティ要件を課すもの
  - 製品またはパッケージに対してCEマークを貼付することで認証されたことを明示

Cyber Resilience Act（CRA）：Regulation（EU）2024/2847	
公表年	2024年11月20日公布、2024年12月10日発行、2027年12月11日主要義務適用予定
出所	欧州委員会および欧州議会
対象事業者（顧客 or 事業者）	英国における製品の市場流通関係者（製造者、輸入者、販売者）
適用範囲	デジタル要素を含むすべての製品（ハード・ソフト・クラウド等）※ 一部除外：医療機器、車載システム、OSS単体等
宣言の責任者	原則として製造者が責任を負う（役職に関して明確な記載なし） ※ EU適合宣言（DoC: Declaration of Conformity）作成
評価者	一般製品：自己評価（第一者）、重要製品（重大リスク）：第三者評価機関による審査が原則必要
有効期間	明確な記載なし ※ 技術文書とDoCは、市場投入後10年間の保存義務
保証方法	①リスクアセスメントの実施 ②技術文書の作成 ③DoC作成・署名 ④（必要に応じて）第三者適合性評価 ⑤CEマーク貼付 ※ CEマークが表示されている製品はEU内で販売可
開示範囲	■ CEマークは製品またはパッケージに明示 ■ 技術文書とDoCは、必要に応じて取引先・市場当局に開示できる状態にしておく必要あり
宣言の様式	アクセス可能なもの（印刷物／電子媒体／その他の適切な形式）
運用スキーム	EU規則として全加盟国に直接適用

2. 国内外動向に関する文献調査

(3) 調査結果詳細　―諸外国のサイバーセキュリティ確保の取組―

- OMB M-23-16
  - 連邦政府調達ソフトウェアに対して、安全な開発プロセスを自己証明することを義務付ける枠組み
  - NISTのSecure Software Development Framework（SSDF）に基づいている

OMB M-23-16	
公表年	2023年6月9日（M-22-18の改正）
出所	Office of Management and Budget（OMB）
対象事業者（顧客 or 事業者）	ソフトウェア製造業者（米連邦政府向け）
適用範囲	■ 2022年9月14日以降開発されたソフト ■ それ以前に開発されたものでも大幅バージョン変更後、または継続的変更を伴うSaaS等の場合 ※ 連邦機関開発／OSS／無料ソフト等は除外
宣言の責任者	CEO
評価者	SSDFを基準とした自己宣言（第一者）、第三者評価機関（3PAO: Third Party Assessor Organization）による評価も可
有効期間	明確な記載なし ※ 継続的に有効であることが前提
保証方法	SSDFに基づく実践及びフォーム署名、または3PAOによる評価
開示範囲	Cybersecurity and Infrastructure Security Agency（CISA）のRepository for Software Attestations and Artifacts（RSAAへ）の提出義務あり。※ 一部機密要素を除き一般省庁が確認可能
宣言の様式	CISAが提供する「Secure Software Development Attestation Form」

3. 検討会の運営

3.1 検討会の運営

(1) 有識者の選定

- 顧客も含めたさまざまなサイバー関連事業者が合意し取組可能なガイドラインとするために、下表に示す有識者で構成される有識者会議「産業サイバーセキュリティ研究会ＷＧ１・内閣官房国家サイバー統括室合同ワーキンググループ　サイバーインフラ事業者に求められる役割等の検討会」を設置した。

氏名（敬称略）		所属
	阿部 恭一	株式会社レオンテクノロジー相談役
	稲垣 隆一	稲垣隆一法律事務所　弁護士
	鴨田 浩明	株式会社NTTデータ ソリューション事業本部セキュリティ＆ネットワーク事業部長
	木谷 浩	一般社団法人 情報サービス産業協会 サイバーセキュリティ部会 部会長 （キヤノンＩＴソリューションズ株式会社 サイバーセキュリティ技術開発本部先進セキュリティ技術アセスメント課）
	立石 聡明	一般社団法人 IT団体連盟理事（日本インターネットプロバイダー協会副会長）
	津田 宏	富士通株式会社　富士通研究所　フェロー
［座長］	土居 範久	慶應義塾大学　名誉教授
	板東 直樹	一般社団法人 ソフトウェア協会（SAJ）フェロー (Software ISAC 共同代表)
	日高 昇治	一般社団法人 日本クラウド産業協会（ASPIC）執行役員
	淵上 真一	日本電気株式会社 Corporate Executive CISO
	古田 朋司	トヨタ自動車株式会社 情報セキュリティ・トラスト部　主査
	山口 雅史	NRIセキュアテクノロジーズ株式会社　事業戦略推進統括本部長
オブザーバー：		警察庁、総務省、厚生労働省、防衛装備庁、デジタル庁、一般社団法人 日本医療機器産業連合会
事務局：		経済産業省、内閣官房国家サイバー統括室

3.1 検討会の運営

(2) 検討会の開催状況

- (1)に示した構成員にて、昨年度に引き続き下表に示す計2回の検討会を開催した。
- 委員意見や実証事業等を踏まえて見直しを行ったガイドラインおよび評価チェックリストが承認された。

会議	開催日	主な議題及び会議要旨
第4回検討会	令和8年2月5日	【議題】 • 実証実験及びヒアリング結果を踏まえたガイドライン（案更新版）と評価チェックリストの審議、及び今後の普及方針の検討に関する議論 【会議要旨】 • ガイドライン（案）の更新内容と評価チェックリストに関する審議、及びガイドライン（案）の活用促進に向けた取組及び普及施策の議論を実施。
第5回検討会	令和8年2月26日 ～3月4日 （書面開催）	【議題】 • ガイドライン（案）と評価チェックリストの審議に関する議論 【会議要旨】 • ガイドライン（案）と評価チェックリストに関する審議を実施。

3.1 検討会の運営

(3) 検討会における主なご意見

- 「産業サイバーセキュリティ研究会ＷＧ１・内閣官房国家サイバー統括室合同ワーキンググループサイバーインフラ事業者に求められる役割等の検討会」における委員の主な意見は次の通りである。

- ガイドライン（案）に関する主な意見は次の通り。

観点	主なご意見
SBOMについて	• SBOMへの懸念は、脆弱性管理や資産管理など、人により想起するイメージが異なることに起因するとも考えられる。本質はトレーサビリティ確保であり、SBOMはその手段の一つという位置づけを明確にすべきである。 • SBOMに関連する個別要求は、トレーサビリティの観点から、OSS（オープンソースソフトウェア）等については将来的には必須化も視野に入れ、「推奨する」「標準である」という方向性にしておくべきである。
用語の表記	• 用語の法的効果について、意図しない法的責任を招かぬよう配慮が必要である。国際標準との整合性について、将来的には、ISO等で用いられる「SHALL」や「MUST」といった表現と整合性を取ることが望ましい。 • 海外にもソリューションを提供するため、ISO等の国際標準で用いられる「SHALL」や「MUST」といった表現との対応関係を示すなど、国際的な整合性を検討すべきである。
法定位置付け	• 「責務」「要求事項」「～すべき」といった表現は、損害賠償請求の根拠等に用いられ、ガイドラインが意図しない法的効果を生む懸念がある。「責任や規制を課すものではない」というスタンスを明確にするため、「要求事項」という言葉は使用せず、「～すべき」は「～することが有効である」等の推奨表現に修正すべきである。あるいは、定義集を設けて「本ガイドラインは裁判所の判断や企業の法的責任の根拠となることを意図していない」と明記し、用語の解釈をコントロールする方法も考えられる。
他制度との位置づけ	• 本ガイドラインの実施が、何らかの認証や認定を標榜できるものであるとの誤解を防ぐため、あくまで契約関係における確認ツールであることをユースケース等で改めて強調すべきである。

3.1 検討会の運営

(3) 検討会における主なご意見

- 評価チェックリストに関する主な意見は次の通り。

観点	主なご意見
情報の取り扱い	• 評価チェックリストは事業者のセキュリティ対策レベルを示す機密情報に該当するため、その取扱いには十分な注意を要する旨を明記すべきである。 • 評価チェックリストの評価項目は文書の有無を問うものが多く、内容の妥当性までは確認しないことから、実質的な合意形成には、NDA（秘密保持契約）締結下の資料確認などが必要になるのではないか。
活用時の留意事項	• 企業としての取り組み評価が、個別の案件における実施を約束するものではないことを明確にすべきである。一方で、合意内容を後続の要件定義等に有効活用できる仕組みも望ましい。 • 供給者に含まれる販売店にとって、単独では実現困難な要求事項がガイドラインに記載されている。販売店がチェックリストで「N/A」と回答した場合に不利に扱われないか懸念があり、その点の解釈を明確に説明すべきである。 • 業者は案件ごとに顧客にも供給者にもなり得るため、「供給者という組織だからこの役割」という固定的な役割分担の誤解を生まないよう、役割は案件ごとに決まることを明記すべきである。
評価の効率化	• 評価項目を「実施しないとセキュリティが低下するもの」と、コミュニティ活動など「直接的ではないが推奨されるもの」に分類すれば、企業規模に応じた適用がしやすくなるのではないか。

3.1 検討会の運営

(3) 検討会における主なご意見

- 普及・広報施策に関する主な意見は次の通り。

観点	主なご意見
ガイドライン案関連ドキュメントの整備	• 「セキュアビルド」等の各項目について、具体的に何を実施すべきか利用者が理解できるよう、NIST SP800-218等の関連ガイドラインを詳細に提示することが、ガイドラインの普及につながる。
ツールの整備	• 普及には、発注元の事業会社がプライム会社やグループ会社に内容を適切に説明できるかが鍵となる。分量の多い文書の読解は困難なため、動画教材のような説明しやすいツールを作成することが有効である。 • 業界でのチェックリスト普及の経験から、説明会、解説書、Q&A、チャットボットの設置など、誤解を生まないための丁寧な説明を繰り返し行うことが不可欠である。
他制度や取組との連携	• 経済産業省が推進する「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）」等の他制度と連携し、相互に普及を促進していくことが望ましい。 • 厚労省の「医療情報システムの安全管理に関するガイドライン」に基づくチェックリスト（MDS/SDS）医療機関のサイバーセキュリティ対策チェックリストは、「ガイドラインで顧客である医療機関が、事業者に提出を求めること」という通達により一文が入ったことで急速に普及した成功例である。顧客側がチェックリストを要求する仕組みが普及には効果的である。 • 業界団体として、経済産業省から講師を招いたセミナーを開催するなど、普及に向けた協力が可能である。
活用方法	• 本ガイドラインと評価チェックリストは、責務実施の可否の表明を通じて、契約相手がリスクを判断するための「リスクコミュニケーションツール」であると位置づけるべきである。一方で、行政機関が行政指導を行う際に尊重すべき要件とするという考え方は、残す余地があるのではないか。 • 普及施策として、まず自社で本ガイドラインを活用し、サプライヤーである開発会社等にも展開したい。また、顧客の多くは社内規程にない対策は実施しない傾向があるため、顧客の社内規程に本ガイドラインの適用を推奨する等の働きかけが実効性を高める上で重要である。

3.1 検討会の運営

(3) 検討会における主なご意見

- その他のご意見は次の通り。

観点	主なご意見
実証事業の拡充	• 実証事業において、ガイドラインの主要な利用者と想定される発注者（顧客側）での検証が行われていない。エンドユーザーである一般企業が適切に活用できるか検証するため、顧客側の実証事業が必要である。 • 評価チェックリストの実証が大企業から中規模企業までであったため、リソースの限られる小規模企業における実施可能性についても検証が必要である。
ガイドラインのメンテナンス	• IPAの「情報セキュリティ10大脅威 2026」でAIを悪用した攻撃が初めて上位に挙げられた動向等を踏まえ、ガイドラインの冒頭事例やAIに関する内容を今後の改定で拡充していくべきである。 • 評価チェックリストは、利用者の規模や業種に応じて評価方法が異なり、継続的に改善されるものである旨を記載することで、利用しやすくなるのではないか。

3.2 ヒアリング

(1) 調査概要

- 調査目的
  - 検討会の議論に資するよう、関連するサイバーインフラ事業者等にヒアリングを実施した。

- 実施状況
  - 2026年1月に、サイバーインフラ事業者等にヒアリングを実施した。
  - 幅広いサイバーインフラ事業者や顧客が活用できる実行可能性の高いガイドラインとするため、SI、クラウドサービス等、複数の異なるソフトウェア・サービスの提供実績を有する事業者を対象にヒアリングを実施した。プライム事業者だけではなく、2次請け以降の受託実績を有する事業者なども対象とし、企業規模にも留意した。

3.2 ヒアリング

(2) ヒアリングの結果概要

- 要件調整、役割分担・責任分担の実態／ソフトウェアの利用及び運用に係る契約形態・商流の実態／ソフトウェアサプライチェーン管理の実態の観点からヒアリングを行った。結果の概要を以下に示す。

分類	概要
要件調整、役割分担・責任分担の実態	• 要件調整や責務分担は契約・商流に強く依存し、海外ベンダ/顧客への要求は難易度が高い。
ソフトウェアの利用及び運用に係る契約形態・商流の実態	• 請負/準委任、クラウド/SaaS、再委託の有無により、供給者が担保できる範囲（運用、監視、パッチ適用等）が変わる。
ソフトウェアサプライチェーン管理の実態（構成管理・脆弱性対応等）	• OSS管理は進められているが、SBOMの取組には幅がある。

4. ガイドライン案の更新等

4.1 ガイドライン案の更新

(1) 調査概要

- パブリックコメントおよび検討会のご意見等を踏まえ、昨年度事業のガイドライン（案）を更新した。
- ガイドライン案の更新に当たっては、検討会及びヒアリング等でのサイバーインフラ事業者から顧客までを含めたステークホルダーの意見等に基づき、当該事業者の実行可能性も踏まえたものとした。
- セキュリティ専任の職員を配置できない等、知見・人材等のリソースが十分でない事業者やユーザーについても考慮し、専門用語には注釈を付与した。

4.1 ガイドライン案の更新

(2) 実施事項

- パブリックコメントの実施
  - 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・個人等から御意見を受領した。
  - 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更新方針を検討した。

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	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

4.1 ガイドライン案の更新

(2) 実施事項

- 以下に、頂いた御意見と対応の考え方を示す。

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
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 • 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 • 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 • 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 • 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	• 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 • 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	• 双方向の活動（貢献）が必要であることを明確化する。 • その他については、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	• 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。

4.1 ガイドライン案の更新

(2) 実施事項

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
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	• 責務と個別要求の中で具体化されるべきものであり、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	• 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	• 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 • 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	• 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	• 具体的な第三者監査・認証制度、およ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	• 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、原案のとおりとする。
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 • 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	• 「その他関連機関」の一部であり、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、原案のとおりとする。

4.1 ガイドライン案の更新

(2) 実施事項

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
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 • 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	• 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	• サイバーインフラ事業者及び顧客に求められる責務を示すものとして検討しており、概念レベルの記載として、原案のとおりとする。
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	• 役割の兼務については記載しており、原案のとおりとする。

4.1 ガイドライン案の更新

(2) 実施事項

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
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 • 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 • ステークホルダ・対象に関する用語不統一の個所がある • 「IT製品」の用語は「S(2)-3」のみで使用されている • 「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 • 「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 • リスク適合など、表現・用語の統一が必要である	• 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いることから、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	• 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。

4.1 ガイドライン案の更新

(2) 実施事項

- 更新したガイドラインと関連資料の概要は以下の通り。

ガイドライン

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

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。

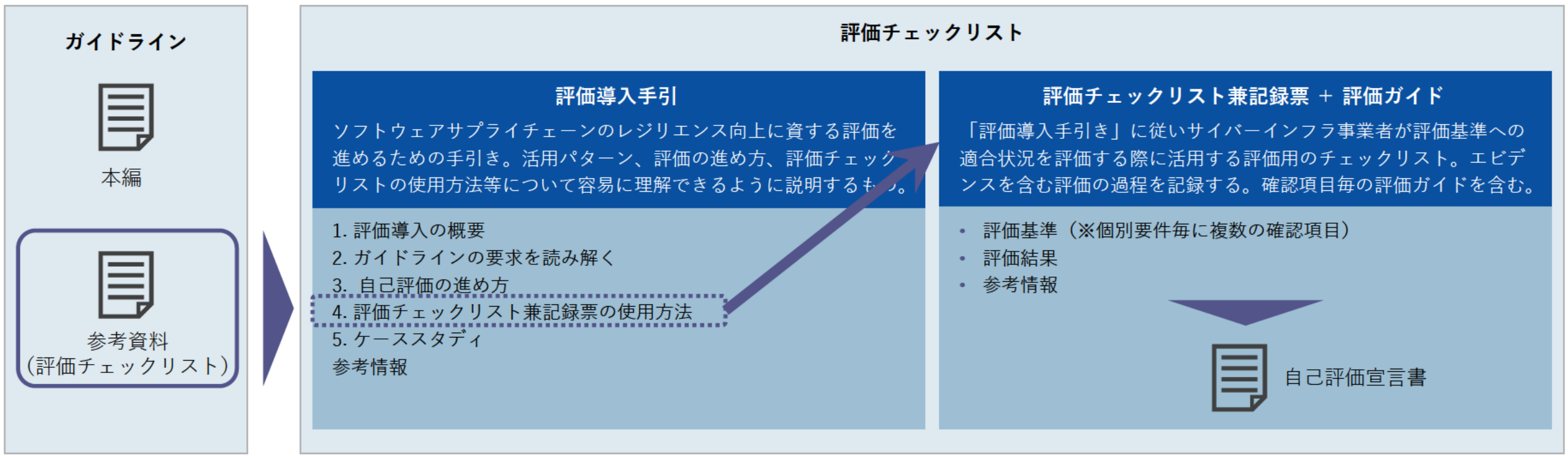
調達・開発・運用に活用

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。

4.2 評価チェックリストの作成

(1) 調査概要

- 評価チェックリストの目的
  - 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上で、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。



4.2 評価チェックリストの作成

(2) 実施事項

■ 作成した評価チェックリストを活用した評価の流れは以下の通り。

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

■ 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						
		…					

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。

■ 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]の項目を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	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…
	…	

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。

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

自己評価宣言書（別紙）

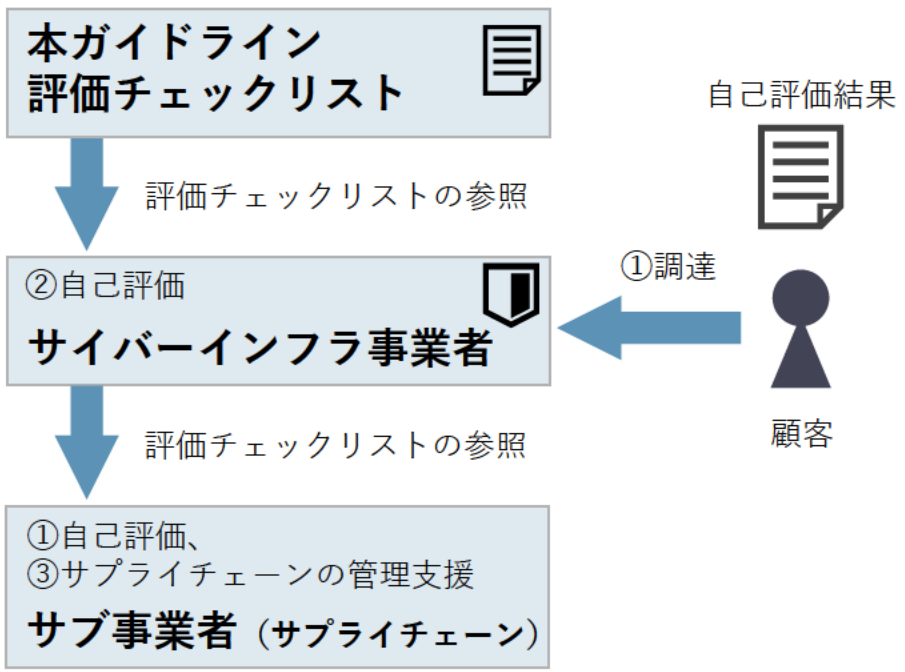
S(1)-1.1：…
S(1)-1.2：…
…

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。

4.2 評価チェックリストの作成

(2) 実施事項

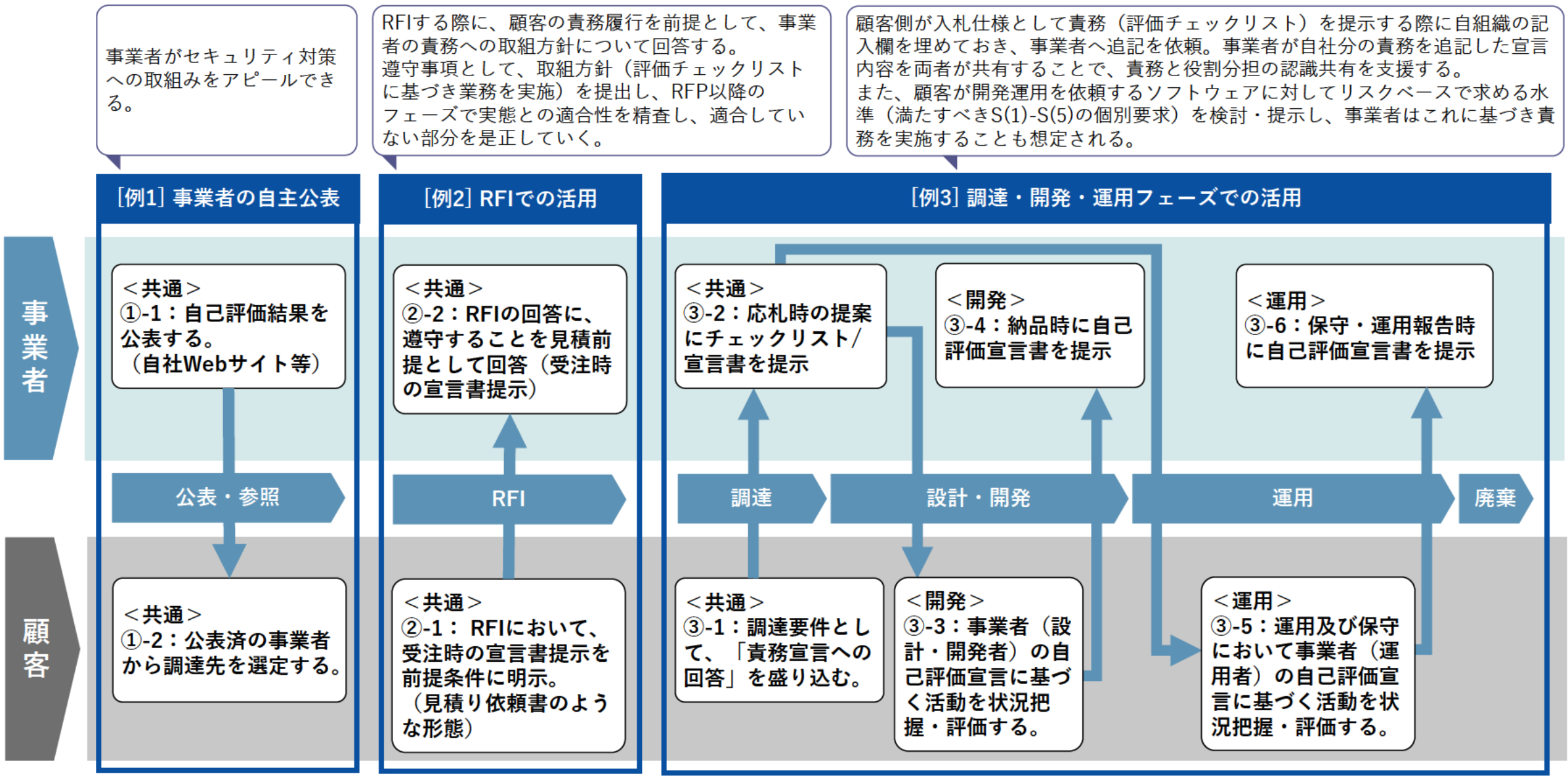
- 評価チェックリストの活用例
  - 実証等のご意見を踏まえ、ソフトウェアサプライチェーンのレジリエンス向上を目的に評価チェックリストを活用する用途を検討し、用途を実現するための活用例を検討した。次頁に、活用例を示す。



	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】

4.2 評価チェックリストの作成

(2) 実施事項



5. ガイドラインの実効性確保に向けた実証

5.1 実証

(1) 調査概要

- 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はじめとした事象者に協力を依頼し、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。

(2) 実施事項

- 3事業者にご協力を頂き、以下の通り実施した。

実証事業者	概要
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	実証	ヒアリング
2025年11月 • 評価チェックリスト等一式を協力頂く事業者に配布し、Web会議にてご説明。	**2025年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、実証を通じてご意見を頂いた。 • 「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」の評価項目毎に直接コメントを頂いた。	**2026年1月** • 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。

5.1 実証

(3) 実施結果

- 評価チェックリストへのご意見：概要
  - 改善ポイントや考慮事項について、4つの観点からご意見いただいた。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し、実施した。

頂いた主な御意見	今年度の反映事項
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] ご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。

5.1 実証

(3) 実施結果

■ 評価チェックリストへのご意見詳細：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
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。
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
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」
	• 評価内容単体で理解ができない。
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」
	• 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
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
	• 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
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
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

5.1 実証

(3) 実施結果

- 評価チェックリストへのご意見詳細：評価の負担

頂いた御意見のカテゴリ	頂いた主な御意見
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
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
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
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

5.1 実証

(3) 実施結果

- 評価チェックリストへのご意見詳細：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
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
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
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

5.1 実証

(3) 実施結果

■ 評価チェックリストへのご意見詳細：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
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
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）
	• 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。
	• 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）
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。
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。
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。
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。

5.1 実証

(3) 実施結果

- 評価チェックリストへのご意見詳細：評価結果の活用（続き）

頂いた御意見のカテゴリ	頂いた主な御意見
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。
	• 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。
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。

6. 英訳

6.1 英訳

(1) 調査概要

- ガイドライン案の本編及びガイドライン案概要説明資料の 2 点を英訳対象文書とし、事業開始後及び更新後の 2 回英訳を行う。
- 事業開始後の英訳は、昨年度作成したガイドライン案を対象に国内外からパブリック・コメントを収集することを目的とするため、受託後に速やかに英訳にとりかかる体制を整備した。
- パブリックコメントおよび検討会でのご意見を踏まえた更新後のガイドライン案の英訳については、事業開始後時点からの更新部分を対象とした。

(2) 実施内容

- ガイドライン案の本編及びガイドライン案概要説明資料の 2 点について英訳を実施した。

7. まとめ

- 本事業では、サイバーインフラ事業者によるレジリエンスを向上し、サイバーセキュリティの根本的確保を推進することを目的として、国内外動向に関する文献調査、検討会の運営、ガイドライン案の更新、実証および英訳業務を実施した。
- 文献調査では、ガイドライン及び自己評価宣言の検討に必要な要素を検討するため、国内外のサイバーセキュリティ対策に関する取組等を調査した。欧米を中心に、自己評価の枠組み整備が進んでいる。
- 検討会の開催業務では、ガイドライン（案）と評価チェックリストに関する意見が出され、当該意見に基づきガイドライン（案）と評価チェックリストを更新した。
- 実証業務では、策定した評価チェックリストに基づく自己評価宣言について、実証に向けた評価項目を検討、企業の協力のもと実証事業を実施し、実証結果についての評価を行った。
- ガイドライン案の更新業務では、文献調査、検討会及び実証のご意見および結果を踏まえ、サイバーインフラ事業者と顧客に求められる責務の考え方と責務を果たすための要求事項を更新した。また、本ガイドラインの責務の実施状況を自己評価するための評価チェックリストを作成した。ガイドライン（案）および評価チェックリストをサイバーインフラ事業者と顧客が活用することで、自社の取組を高度化するとともに、将来的な自己適合宣言への活用を通じて国内のサイバーセキュリティ取組の高度化も期待される。
- 英訳業務では、ガイドライン（案）について幅広いご意見を伺うこと、多くの関係者にガイドラインを利用いただくために英訳を行った。