



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)

概要説明資料

2026年10月

独立行政法人

情報処理推進機構

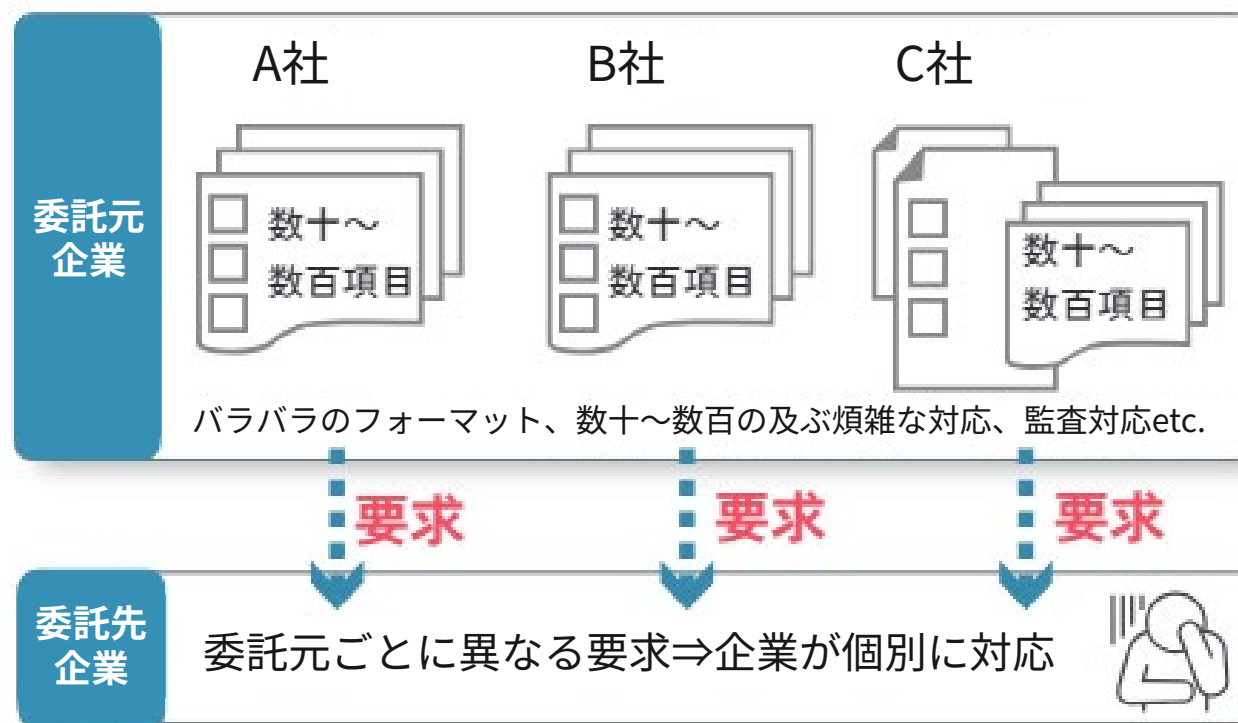
セキュリティセンター

© 2026 Innovation Platform Agency, Japan (IPA)

1. はじめに
2. 制度概要
3. 要求項目・評価基準
4. 評価
5. 対象組織・適用範囲
6. 評価機関・技術検証事業者・研修事業者
7. SCSセキュリティ専門家
8. 研修
9. 導入促進策

1. はじめに

- 近年、サプライチェーンを通じたセキュリティインシデントが頻発。委託先等、サプライチェーン全体のセキュリティ対策が求められる中、以下の課題が表面化しつつある。
 - 委託元企業：委託先における**セキュリティ対策が可視化しづらく、要求事項（チェックリスト等）の適正性の担保も難しい**
 - 委託先企業：複雑なサプライチェーン下で様々な委託元から**様々な要求事項**を求められ、**過度な負担**につながっている(特に中小企業を中心に)



委託元企業が委託先企業に対して求めるセキュリティ対策について、「共通のものさし」を提示するとともに、委託先のセキュリティ対策が確実に履行されているかをセキュリティ専門家や第三者が確認を行うことで、委託元、委託先双方の課題の解決を目指す。

- 本制度に基づくマークの取得を通じて、ビジネス・ITサービスサプライチェーンにおける、委託先へのサイバー攻撃等を起因とした自社事業・サービスの提供途絶／機密情報の漏えい、改ざんや委託先等を踏み台とした不正侵入等のリスクに対する適切なセキュリティ対策の実施を促し、**サプライチェーン全体でのセキュリティ対策水準の向上**を図る※¹。
- 具体的には、2社間の取引契約等において、委託元が、委託先に適切な段階(★)を提示し、示された対策を促すとともに実施状況を確認することを想定※²※³。
(再委託先は委託元から見た直接の管理対象にはならないが、直接の委託先を通じて必要に応じて管理することを想定※⁴)

(※1) 本制度は、サプライチェーンにおける企業の位置づけや想定リスク等を踏まえて求められるセキュリティ対策の水準を定め、企業の対応状況を可視化するものであり、事業者のセキュリティ対策レベルを競わせることを目的としたもの(格付け制度等)ではない。

(※2) なお、委託元からの要請が無くとも、各企業が自らのサイバーセキュリティ対策状況を可視化するために★を自主的に取得することも考えられる。

(※3) ★の取得はあくまで取得又は更新の時点において★ごとに定められた水準を満たしていることを示すものであり、セキュリティインシデントに対して完全なセキュリティが確保されていることを保証するものではない。

(※4) 対策基準の項目において、「重要な取引先におけるセキュリティ対策状況の把握」を求めることを想定。

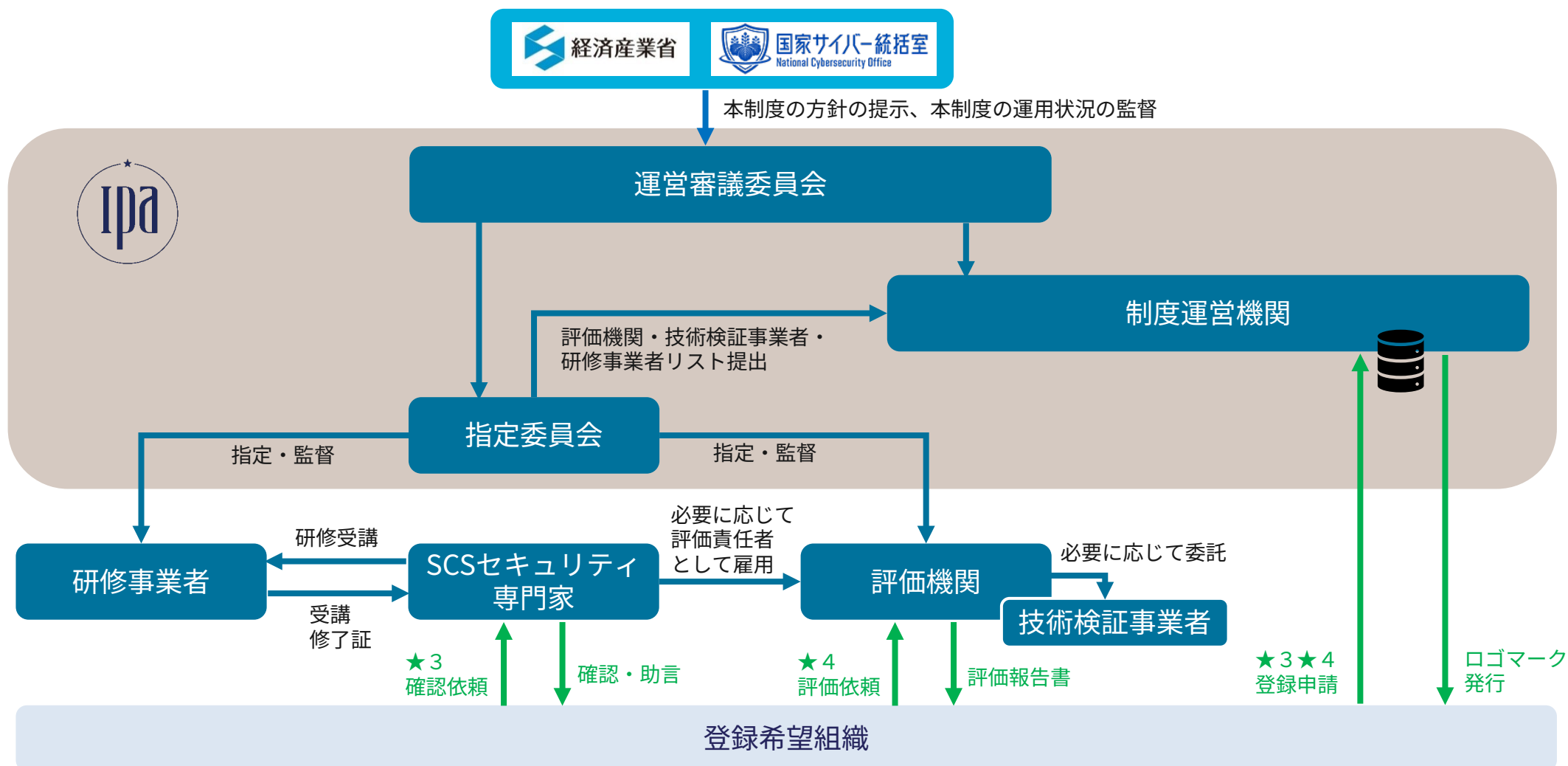
- サプライチェーンにおけるリスクを対象にした上で、その中での立ち位置に応じて必要な対策を提示することで、**企業が必要な対策を選定しやすくする。**
 - ・ 全てのサプライチェーン企業が対象となるが、特にサプライチェーンを構成する中小企業は、セキュリティ対策におけるリソースが限られていることや、自社のリスクを踏まえてセキュリティ対策を行うことはハードルが高いことから、セキュリティ対策のベースラインを提示することによる効果が大きい。
- 委託元企業・委託先企業双方にとって、適切なセキュリティ対策の決定や対策状況の説明が容易・適切となることが期待される。
 - 委託元企業への効果
 - ✓ 委託先に求めるセキュリティ対策の内容や水準の決定、対策実施状況の把握の容易化・適切化
 - ✓ 委託先におけるセキュリティ対策の適切な実装による、サプライチェーンに起因する自社セキュリティリスクの低減
 - 委託先企業への効果
 - ✓ 自社に必要なセキュリティ対策を明確化し、対策実施によるセキュリティリスク低減を促進
 - ✓ 対策に要する費用や効果の可視化（経営陣に対してセキュリティ対策を促す）
 - ✓ 委託元企業等に対する、セキュリティ対策に係る説明の説得力向上

- サプライチェーンを担う各企業のセキュリティ対策が可視化され、強化されることにより、結果として、サプライチェーン全体の底上げを通じた経済・社会全体でのサイバーレジリエンス※の強化が期待される。
 - ・ セキュリティサービスの標準化による選択肢拡大やコスト低減
 - ・ サイバー攻撃への備えのある企業等への適切な評価
 - ・ 対策状況の効率的・効果的な可視化による取引コスト（社会的コスト）の低減
 - ・ セキュリティ製品やサービスの市場拡大・競争力向上

※ サイバーレジリエンス(Cyber resiliency)： サイバー資源を使用する又はサイバー資源によって実現するシステムに対する不利な状況、ストレス、攻撃、侵害を予測し、それらに耐え、回復し、適応する能力 https://csrc.nist.gov/glossary/term/cyber_resiliency

2. 制度概要

- 経済産業省・内閣官房国家サイバー統括室の示す方針に従い制度を構築し、両省の監督のもと制度を運営するスキームオーナーは独立行政法人情報処理推進機構（IPA）が担う。



【参考】制度を構成する者の定義



制度所管省庁	本制度の方針の提示及び運用状況の監督を行う省庁で、経済産業省及び内閣官房国家サイバー統括室である。
制度運営機関	制度に関する運営及び登録に向けた手続の際に参考となる資料の作成及び公開、登録組織の一覧登録及び公開等を行う。
運営審議委員会	制度運営機関からの委託に基づき、本制度の規程、規則及びガイド、並びにその他、制度の運営に係る国 SWG への提言について、審議及び決定を行う。
指定委員会	制度運営機関からの委託に基づき、評価機関、技術検証事業者及び研修事業者の指定及び指定の取消し、並びに本制度の基準及び手順について、審議及び決定を行う。
評価機関	制度運営機関からの指定を受けたものであって、★4 を希望する登録希望組織が作成した自己評価の結果を評価するとともに、実地審査及び技術検証を行い、★4 要求事項・評価基準への適合判断結果（適合・不適合）をまとめた評価報告書を作成し、登録希望組織に提供する。
技術検証事業者	制度運営機関からの指定を受けたものであって、★4 登録希望組織に対する技術検証を行い、その結果をまとめた技術検証結果報告書を作成する。
研修事業者	制度運営機関からの指定を受けたものであって、★3 確認責任者、★3 確認従事者、★4 評価責任者及び★4 評価従事者となるために受講が必要な研修を実施する。
登録希望組織	★3、★4 又は★5 の登録を受けることを目的として、要求事項・評価基準に基づく対策を実施するとともに、当該要求事項・評価基準の全てを満たしていることについて、★3 においては★3 確認責任者による確認を、★4 においては評価機関による第三者評価を受けた上で、登録申請を行う組織である。
登録組織	制度運営機関により登録組織台帳への登録及び公開がなされている組織である。
SCSセキュリティ専門家	セキュリティに係る力量を一定以上有しており、それを継続的に維持していると認められる資格を有する者であって、研修事業者が提供する研修を受講し、制度運営機関に登録している者である。

階層	文書番号	文書名	主な対象者	公開範囲	公開日
規程	SCS-100	基本規程	本制度を構成するすべての者	一般公開	2026年8月28日
規則	SCS-110	制度運営機関規則	制度運営機関	一般公開	2026年8月28日
	SCS-111	運営審議委員会規則	運営審議委員会	一般公開	2026年8月28日
	SCS-112	指定委員会規則	指定委員会	一般公開	2026年8月28日
	SCS-210	評価機関指定規則	制度運営機関・指定委員会・評価機関	一般公開	2026年8月28日
	SCS-220	技術検証事業者指定規則	制度運営機関・指定委員会・技術検証事業者	一般公開	2026年8月28日
	SCS-230	研修事業者指定規則	制度運営機関・指定委員会・研修事業者	一般公開	2026年8月28日
基準 ガイド	SCS-310	評価機関指定基準	制度運営機関・指定委員会・評価機関	一般公開	2026年9月11日
	SCS-320	技術検証事業者指定基準	制度運営機関・指定委員会・技術検証事業者	一般公開	2026年9月11日
	SCS-330A	研修事業者指定基準	制度運営機関・指定委員会・研修事業者	一般公開	2026年9月11日
	SCS-330B	研修実施基準	制度運営機関・指定委員会・研修事業者	一般公開	2026年9月11日
	SCS-400	★3・★4 要求事項・評価基準	登録希望組織・SCSセキュリティ専門家・評価機関	一般公開	2026年3月27日
	SCS-410	★3・★4 自己評価等ガイド	登録希望組織・SCSセキュリティ専門家	一般公開	2026年10月28日
	SCS-420	★4 第三者評価ガイド	評価機関	一般公開	2026年10月28日
	SCS-430	★4 技術検証ガイド	登録希望組織・技術検証事業者	一般公開	2026年10月28日
手順 手引 解説書	SCS-510	評価機関指定手順	指定委員会・制度運営機関	一般公開	2026年9月11日
	SCS-520	技術検証事業者指定手順	指定委員会・制度運営機関	一般公開	2026年9月11日
	SCS-530	研修事業者指定手順	指定委員会・制度運営機関	一般公開	2026年9月11日
	SCS-610	★3・★4 登録申請の手引	登録希望組織	一般公開	今後公開予定
	SCS-620	★3・★4 要求事項・評価基準 解説書	登録希望組織・SCSセキュリティ専門家	一般公開	2026年10月28日

● 2026年9月18日以降の評価機関、技術検証事業者及び研修事業者の申請料及び指定料

対象	2028年3月31日迄の料金	2028年4月1日以降の料金
評価機関	申請料 150,000円 指定料 300,000円 (3年分)	申請料 300,000円 指定料 300,000円 (3年分)
技術検証事業者	【SSS2登録あり】 申請料 50,000円 指定料 150,000円 (3年分) 【SSS登録なし】 申請料 150,000円 指定料 150,000円 (3年分)	【SSS登録あり】 申請料 100,000円 指定料 150,000円 (3年分) 【SSS登録なし】 申請料 300,000円 指定料 150,000円 (3年分)
研修事業者	申請料 150,000円 指定料 300,000円 (3年分)	申請料 300,000円 指定料 300,000円 (3年分)

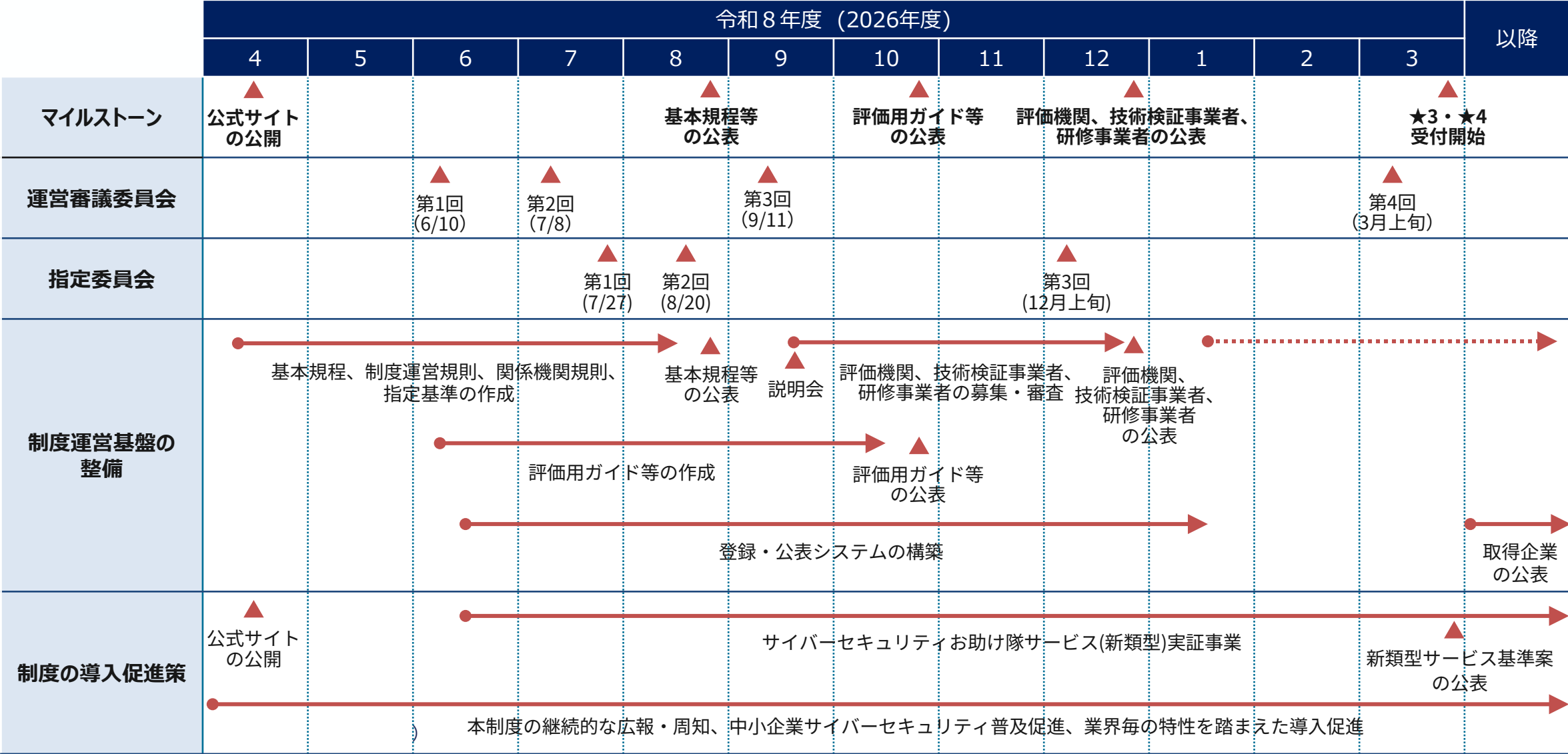
● 2027年1月以降に受付を開始する予定のSCSセキュリティ専門家の登録料

対象	料金
SCSセキュリティ専門家	無料

● 2027年3月以降に受付を開始する予定の登録希望組織の登録料

対象	2028年3月31日迄の料金	2028年4月1日以降の料金
★3登録希望組織	登録料 10,000円 (1年分)	登録料 20,000円 (1年分)
★4登録希望組織	登録料 60,000円 (3年分)	登録料 60,000円 (3年分)

● 2027年3月の★3・★4受付開始に向けて、制度運営基盤の整備及び導入促進策を進めていく。



3．要求事項・評価基準

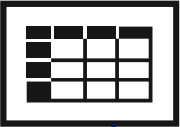
- ★3・★4 要求事項・評価基準は、以下に示す通り、7の大分類の下、16の中分類から構成され、★3については計26件、★4については計43件の要求項目からなる。
- 本制度は、NIST Cyber Security Framework(CSF)の6つの機能に対応している。

大分類		中分類		要求事項数		NIST CSF における機能
				★3 (計:26)	★4 (計:43)	
1	ガバナンスの整備	1-1	組織の状況	0	1	統治(GV)
		1-2	役割、責任、権限	2	3	
		1-3	ポリシー	1	1	
		1-4	監督	0	1	
2	取引先管理	2-1	サプライチェーンリスクマネジメント	3	5	識別(ID)
3	リスクの特定	3-1	資産管理	4	5	
		3-2	リスクアセスメント	0	1	防御(PR)
4	攻撃等の防御	4-1	アイデンティティ管理、認証、アクセス制御	7	9	
		4-2	意識向上とトレーニング	1	2	
		4-3	データセキュリティ	1	4	
		4-4	プラットフォームセキュリティ	3	5	
		4-5	技術インフラのレジリエンス	1	1	
5	攻撃等の検知	5-1	継続的監視	1	2	検知(DE)
		5-2	有害事象の分析	0	1	
6	インシデントへの対応	6-1	インシデント管理	1	1	対応(RS)
7	インシデントからの復旧	7-1	インシデント復旧計画の実行	1	1	復旧(RC)

自己評価・第三者評価（技術検証を含む）関連

その他

★3・★4 要求事項・評価基準



自己評価および★3における
確認に関する手続きを説明

評価機関が行う★4の
第三者評価の手続きを説明

評価基準No.4-4-4-3における
技術検証の手続きを説明

解釈に迷う点や
実装例などを解説

★3・★4
自己評価等ガイド

自己評価の実施方法
や適合基準を示す

アセスメント
シート*

★4
第三者評価ガイド

第三者評価の実施方法や
適合基準を示す

★4
技術検証ガイド

技術検証の実施方法や
対応時の留意事項を示す

★3・★4
要求事項・
評価基準 解説書

取得単位・適用範囲の
考え方や
対策の具体例を示す

別途公開予定

★3・★4
登録申請の手引

★3・★4の登録申請に
当たっての手続を示す

主な
想定読者・
使用者

登録希望組織
SCSセキュリティ専門家

評価機関

評価機関
技術検証事業者
登録希望組織

登録希望組織
評価機関
SCSセキュリティ専門家

登録希望組織

4 . 評価

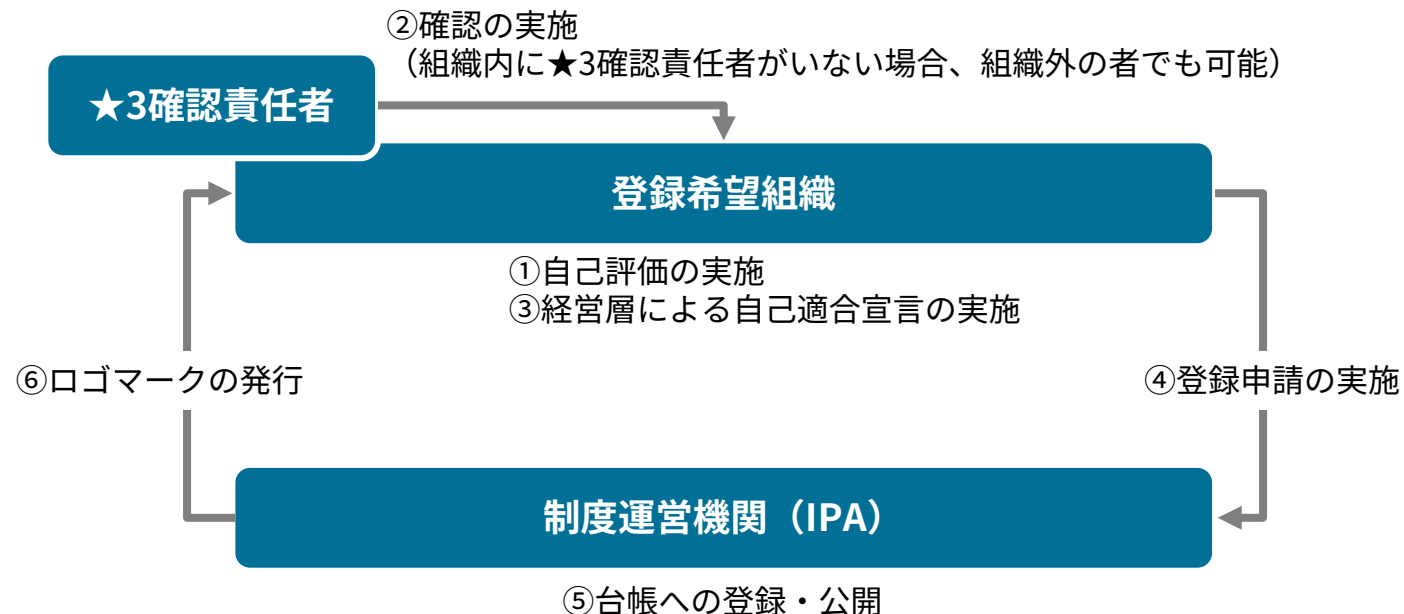
- 本制度は、★3、★4、★5という3つの段階を設けている。このうち★5については今後具体化が予定されている。
- 本制度では上位の段階には下位の段階で求められる事項が全て含まれる。そのため、例えば、★3を取得していなくても、★4の登録申請を行うことができる。

	★3	★4	★5 [検討中]
想定される脅威	・ 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	・ 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 ・ 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	・ 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が最低限実装すべきセキュリティ対策	サプライチェーン企業等が標準的に目指すべきセキュリティ対策	サプライチェーン企業等がさらに目指すべき高度な対策
要求事項	26件	43件	(今後検討)
有効期間	1年	3年	(今後検討)
評価スキーム	専門家確認付き自己評価	第三者評価	第三者評価

要求事項とは、本制度において、登録希望組織が登録を受けるための条件として定めるセキュリティ要件を示す。
評価基準とは、本制度の要求事項について、自己評価又は第三者評価に際し、要求事項を満たしていると判断するための基準を示す。

●★3は、登録希望組織が自己評価を実施し、SCSセキュリティ専門家による確認を受ける（専門家確認付き自己評価）。

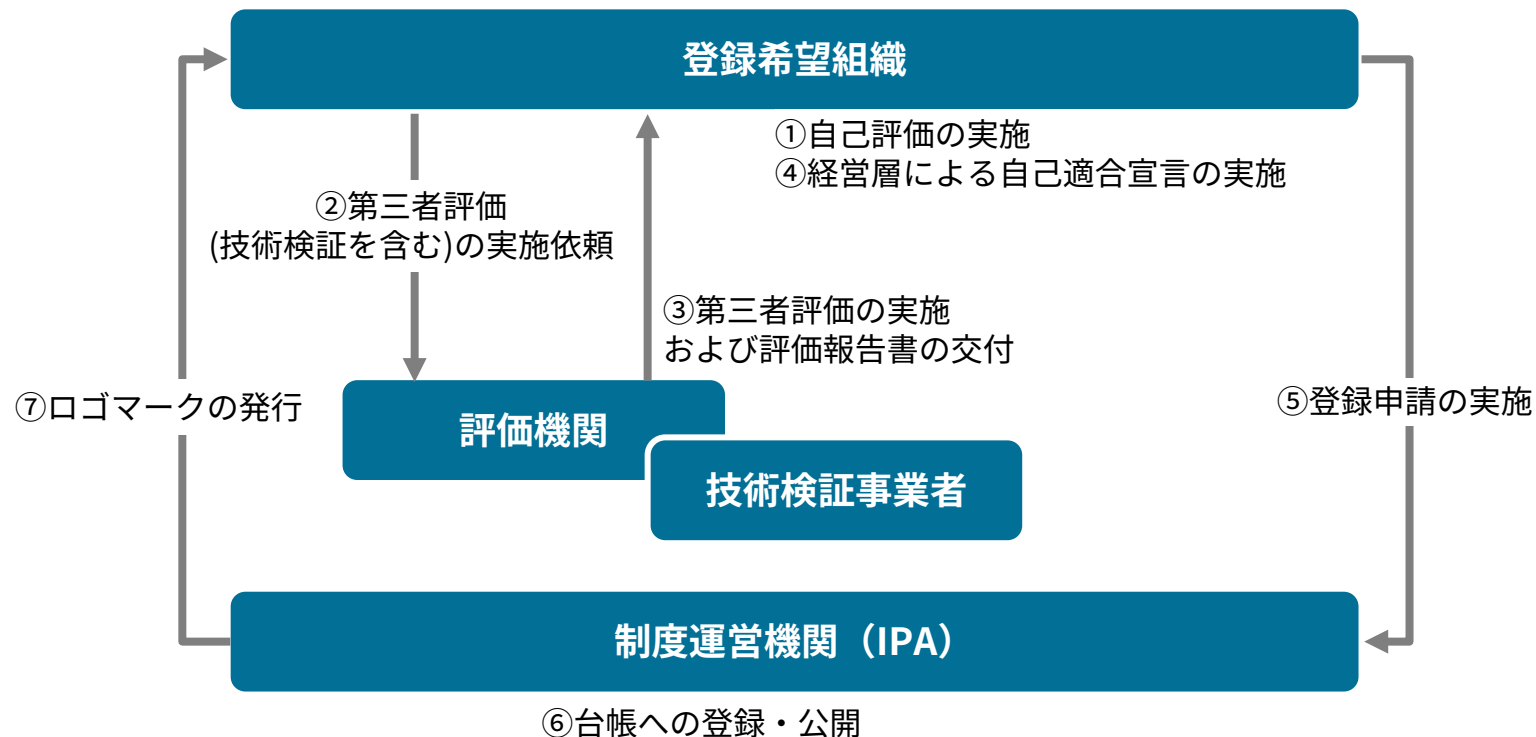
- ①登録希望組織は、★3要求事項・評価基準に基づき自己評価を記入する(必要に応じて社内外の★3確認責任者からの支援を得ることも可)。
- ②社内外の★3確認責任者は、登録希望組織が記入した内容を確認するとともに、必要に応じて評価結果の修正を含む助言を行い、最終的に事務局へ提出する内容に関して了承した場合に署名を実施する。
- ③登録希望組織は、経営層による自己適合宣言を行う。
- ④登録希望組織は、制度運営機関に★3の登録を申請する。
- ⑤制度運営機関は、申請内容に問題が認められない場合には台帳に登録し、公開する。
- ⑥制度運営機関は、ロゴマークを登録希望組織へ発行する。



●★4は、要求事項について評価機関による審査及び技術検証の実施を受ける（第三者評価）。

- ①登録希望組織は、★4要求事項・評価基準に基づき自己評価を記入する。
- ②登録希望組織は、評価機関に、第三者評価・技術検証の実施を依頼する。
- ③評価機関は、第三者評価・技術検証を実施し、評価報告書を登録希望組織へ交付する。(検証は必要に応じて他の技術検証事業者が実施する場合もある。)

- ④登録希望組織は、経営層による自己適合宣言を行う。
- ⑤登録希望組織は、制度運営機関に★4の登録を申請する。
- ⑥制度運営機関は、申請内容に問題が認められない場合には台帳に登録し、公開する。
- ⑦制度運営機関は、ロゴマークを登録希望組織へ発行する。



- ★3は★3確認責任者が、登録希望組織が作成した書類の確認を行う。
- ★4は評価機関・技術検証事業者が、文書確認に加え、実地審査及び技術検証（脆弱性検査）を行う。

評価プロセス	所要期間 (想定)	実施内容等	
		★3	★4
文書確認	1日~2日程度	登録希望組織が作成した自己評価の結果に係る文書について、本制度の要求事項・評価基準への適合性を確認又は評価する。	
実地審査	1日~2日程度 (事前準備、報告書作成は除く)	(実施なし)	登録希望組織へのヒアリングや提出された文書、記録、機器の操作画面等の目視等を実地又は遠隔地において実施することにより要求事項・評価基準への適合性を評価する。
技術検証	1日~2日程度 (事前準備、報告書作成は除く)	(実施なし)	登録希望組織が管理する適用範囲内のIT基盤等である機器、システム等に対して、技術的な手法によって要求事項・評価基準への適合性を評価する。
合格基準	-	★3・★4ともに、原則として、全ての評価基準への適合を求める。	
不適合の指摘及び改善	-	評価結果に不適合が発見された場合であっても、適切に是正対処し、セキュリティ専門家から当該是正について了承を得られれば★3を取得可能。	不適合事項の是正報告を、指摘時から一定期間内(例:評価機関からの指摘事項が通知されてから1ヶ月以内)に提出し、内容について了承を得られれば★4を取得可能。

- ★3は有効期間1年とし、対策状況を年次で点検し、基準全体の遵守を改めて確認する。
- ★4は有効期間3年とし、有効期間内は年次での自己評価結果を評価機関に提出する。
- ★4は、前回取得時に設定した適用範囲や要求事項・評価基準の遵守状況に影響※を及ぼす変更がある場合は、再度評価機関の確認・評価を受ける。

	★3	★4
評価実施主体	適合性評価の対象となる組織自身(自己評価)	指定委員会から指定を受けた評価機関(第三者評価)
有効期間	1年	3年
必要な手続き	有効期限を更新するため、要求事項の遵守状況について、年次で自己評価を実施し、SCSセキュリティ専門家の確認・助言を受ける。	- 有効期間内は、1年ごとに自己評価を実施 1年ごとに実施する自己評価について、前回取得時に設定した適用範囲の変更又は要求事項・評価基準の達成に顕著な影響を及ぼす変更がある場合は、再度評価機関の評価を受ける。 - 有効期限を更新する際(3年に1回)は第三者評価を受ける。
★の取消し等	内部通報等により、登録組織において虚偽報告、情報隠蔽等の不正行為が確認された場合、制度運営機関から★の取消しを行う場合がある。	

※以下のような変更が発生した場合を想定する。

- 要求事項・評価基準に関連する社内規程・手順書等の大幅な変更
- 要求事項・評価基準の達成方法や運用方法の大幅な変更(IT基盤を構成する端末やサーバ等の大規模なリプレイス、クラウド基盤への大規模な移行、ネットワーク構成の顕著な変更等)

5．対象組織・適用範囲

- 取得単位は、原則として法人又は個人事業主とする。ただし、法人においては、取得単位及び適用範囲について★3確認責任者又は評価機関から妥当性の確認を受けること※1を前提に、事業部、企業グループなどを取得単位とすることができる。
- 事業部、事業所、部署等、組織区分とサイバーセキュリティ対策の責任者が明確であれば、取得単位は規模の大小を問わない。また、取得単位には、登録希望組織の意向に応じて、国内の事業拠点に加えて、国外の事業拠点を含めることができる。
- 本制度では、継続的なセキュリティ対策の実施・改善を求めていることから、プロジェクト組織のような期間限定の主体ではなく、法人、企業グループ、事業部等の恒常的な組織を取得単位とすることを求める。

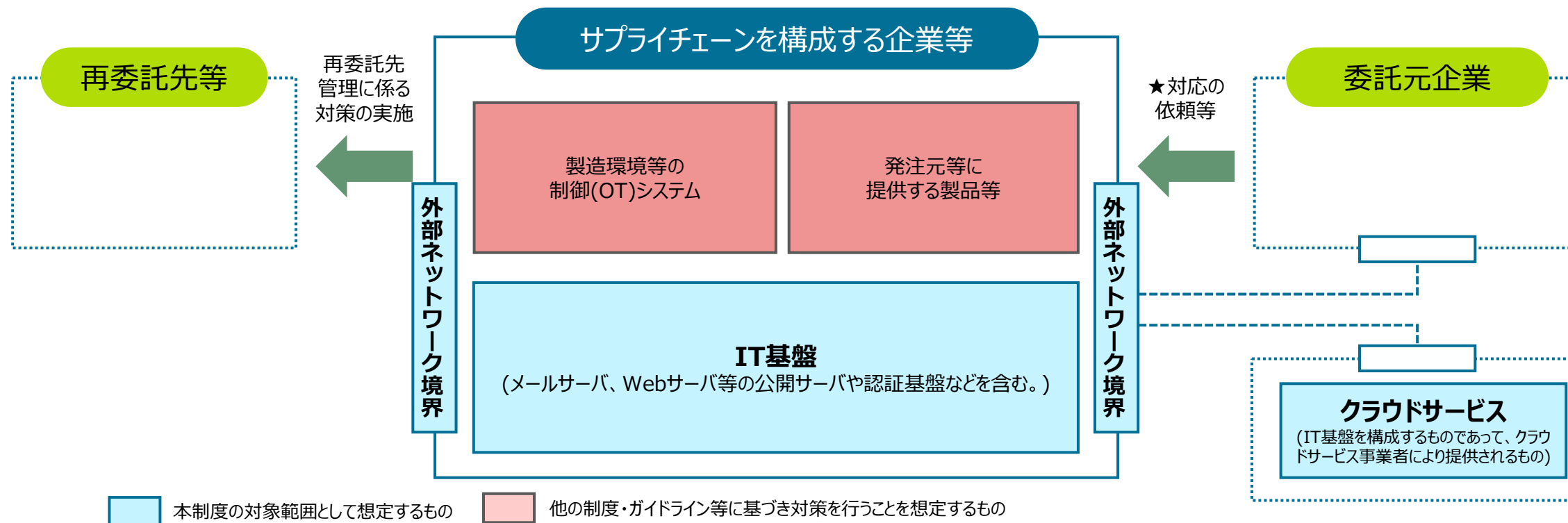
(取得単位の例)

- ・ 個社：株式会社〇〇
- ・ 企業グループ：〇〇グループ※2
- ・ 事業所：株式会社〇〇 × × 事業所

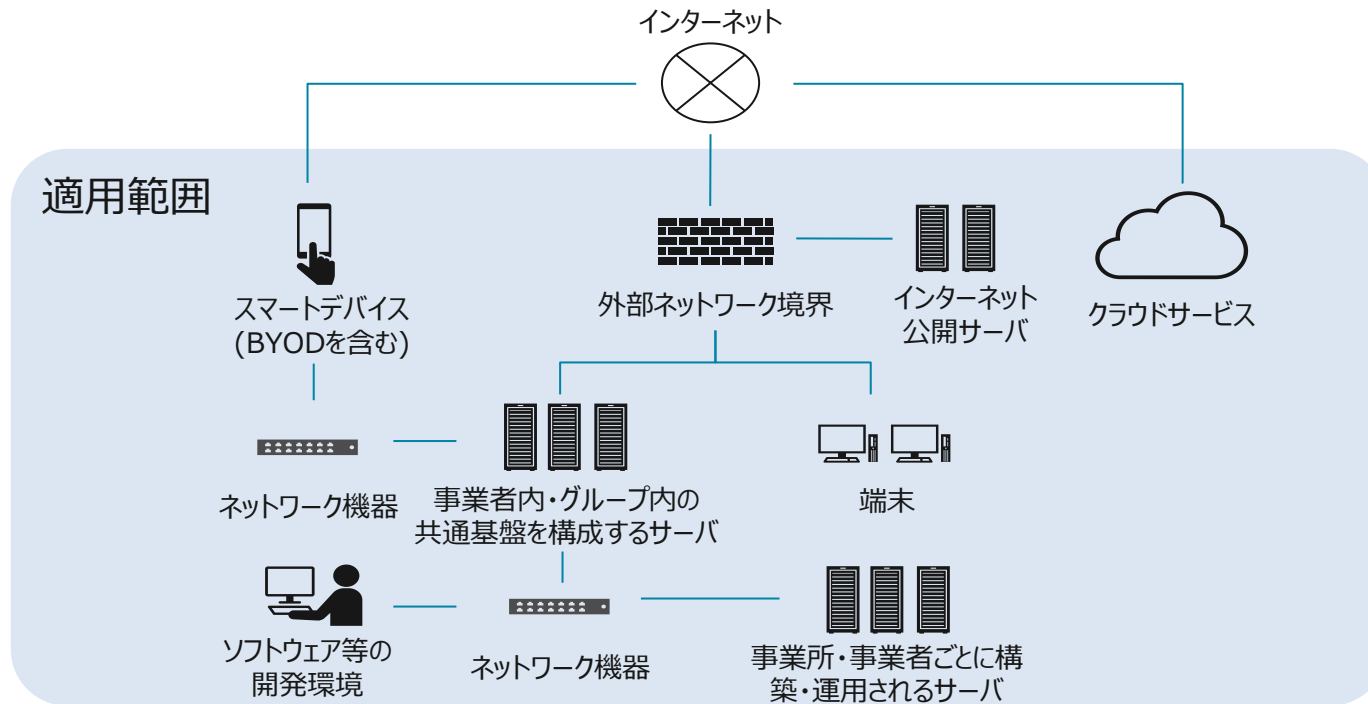
(※1) 具体的な確認項目については、「★3・★4 自己評価等ガイド」2.2を参照。

(※2) 複数法人を一括して申請する場合は、そこに含まれる法人をすべて列挙する必要がある。

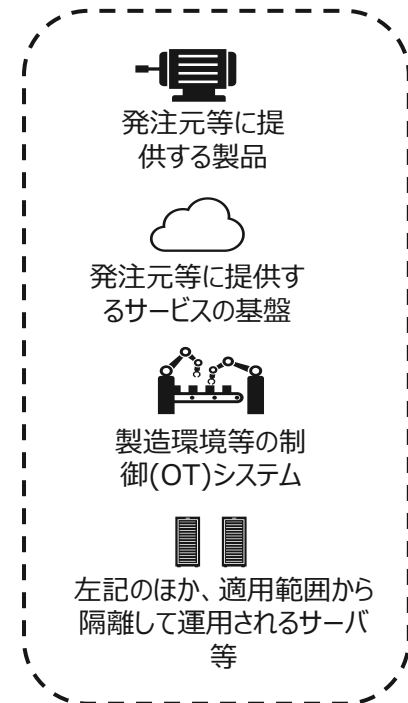
- 適用範囲は、登録希望組織のIT基盤（クラウド環境で運用するものも含む。）、外部ネットワーク境界等を含める必要がある。
- 製造環境等の制御（OT）システム、発注元等に提供する製品等については、対策実施の前提や求められる対応が基本的に異なることから直接の対象とはしない。



- IT基盤としては、登録希望組織が設定する取得単位において利用されるサーバ、利用者が直接操作するパソコン、スマートフォンなどの端末、ネットワーク機器等のうち、以下のいずれかの条件を満たすものを含める必要がある。
 - ・ インターネットに接続された機器からネットワーク接続を受けるもの
 - ・ インターネットを経由するアウトバウンド通信を行うもの
 - ・ 上記の機器とインターネット間のデータフローを制御するもの



適用範囲に含めないもの



6．評価機関・技術検証事業者・研修事業者

- 評価機関、技術検証事業者、及び研修事業者になるには、各指定基準の要件を満たし、指定委員会の審査を受け、制度運営機関に登録申請する必要がある。

分類	指定基準	主な指定要件	有効期間
評価機関	評価機関 指定基準 (SCS-310)	- SCSセキュリティ専門家として登録された者を、評価の責任者（★4評価責任者）として1名以上雇用し、配置していること（評価要員要件） - 評価の責任者と評価を行う者（★4評価従事者）に、IPAが定める研修を受講させること（評価要員要件） - 評価で取り扱う情報を適切に保護するためのルールや運用体制を整備していること（組織要件） - 品質管理の仕組みを整備し、評価結果の妥当性を確認するための手続を運用していること（組織要件） - ガイドに沿って整備した社内規程や手順書に従い、第三者評価を実施すること（評価業務要件）	3年
技術検証 事業者	技術検証事業者 指定基準 (SCS-320)	- 制度が定める専門性要件を満たす者を、技術検証の責任者（★4技術検証責任者）として1名以上雇用し、配置していること（技術検証要員要件） - 技術検証の責任者と技術検証を行う者（★4技術検証従事者）に、IPAが定める研修を受講させること（技術検証要員要件） - 技術検証で取り扱う脆弱性情報等を適切に保護するためのルールや運用体制を整備していること（組織要件） - 品質管理の仕組みを整備し、技術検証結果の妥当性を確認するための手続を運用していること（組織要件） - ガイドに沿って整備した社内規程や手順書に従い、技術検証を実施すること（技術検証業務要件）	3年
研修事業者	研修事業者 指定基準 (SCS-330A) 研修実施基準 (SCS-330B)	- 講義及び演習を担当するために必要な知識、経験及び指導能力を有する者を講師に任命していること（研修要員要件） - 情報セキュリティ分野の資格に関する研修の実績を有し、制度で求められる知識及び技能を習得させる研修を実施できること（組織要件） - 受講者情報等を適切に保護するためのルールや運用体制を整備していること（組織要件） - 研修運営管理体制を整備し、研修コースの品質向上に向けた改善活動を実施していること（組織要件） - 研修実施基準に沿って整備した研修コース仕様書に従い、研修及び修了試験を実施すること（研修コース管理要件）	3年

- ★3、★4の制度に関与する者は、それぞれの役割に応じて、「力量の保持」や「研修の受講」が必要となる。

評価種別	分類	役割	力量の保持	研修の受講		
				制度理解	知識	技能
自己評価	★3確認責任者※1	★3の要求事項・評価基準への適合性の確認を行う。	必要	必須	必須	必須
	★3確認従事者	★3確認責任者の指導・監督の下で、★3の要求事項・評価基準への適合性の確認を行う。	—	必須	必須	必須
第三者評価	★4評価責任者※1	評価過程全般を統括し、自らの責任において評価を行う。	必要	必須	必須	必須
	★4評価従事者	★4評価責任者の指導・監督下で、第三者評価に係る作業を行う。	—	必須	必須	必須
技術検証	★4技術検証責任者	技術検証過程全般を統括し、自らの責任において技術検証を行う。	原則として、「情報セキュリティサービス基準適合サービスリスト」(脆弱性診断サービス)における技術責任者	必須	—	—
	★4技術検証従事者	★4技術検証責任者の指導・監督下で、技術検証に係る作業を行う。	—	必須	—	—

(※1) 力量の保持とすべての研修の受講が必要。SCSセキュリティ専門家が担うことを求めている。

7. SCSセキュリティ専門家

- 本制度においてSCSセキュリティ専門家とは、セキュリティに係る力量を一定以上有しており、それを継続的に維持していると認められる資格を有する者であって、研修事業者が提供する研修を受講し、制度運営機関に登録している者である。
- SCS セキュリティ専門家は、本制度において次に掲げる役割を担うことができる。

分類	役割
★3確認責任者	★3登録希望組織が作成した自己評価の結果の妥当性を★3確認責任者として確認し、必要に応じて評価結果の修正を含む助言を行うとともに、当該確認及び助言を行った旨を署名により示す。
★4評価責任者	★4登録希望組織が作成した自己評価の結果を★4評価責任者として評価する

- SCSセキュリティ専門家になるには、「力量の保持」と「研修の受講」の要件を満たしたうえで、制度運営機関に登録申請する必要がある。

要件	詳細
力量の保持	所定のセキュリティ資格を保有していること ・ 情報処理安全確保支援士 ・ 公認情報セキュリティ監査人／公認情報セキュリティ主任監査人 ・ CISSP (Certified Information Systems Security Professional) ・ CISM (Certified Information Security Manager) ・ CISA (Certified Information Systems Auditor) ・ ISO27001 主任審査員
研修の受講	以下の内容を含む、研修事業者やIPAが提供する研修を受講していること ・ 制度理解 ・ 知識 ・ 技能

● SCSセキュリティ専門家の権利・責任範囲・不正行為への対処等については以下のとおり。

項目	該当文書	内容
SCSセキュリティ専門家の権利	基本規程4.2 (SCS-100)	SCSセキュリティ専門家は、自身が★3確認責任者や★4評価責任者として行った業務及び確認又は評価結果を理由として、不当な差別的扱いを受けない権利を有する。
SCSセキュリティ専門家の責任範囲	基本規程5.9 (SCS-100)	★3について、登録希望組織による自己評価の結果を★3確認責任者として確認する際は、全ての要求事項・評価基準を満たしていることを確認したうえで、確認結果に虚偽等が含まれない点について最大限の注意を払う責務を有する。★4について、第三者評価の評価責任者等として従事する場合は、本制度の狙いを阻害することのないように、確認又は評価に当たっては、利益相反を回避し、事実に基づき誠実に業務を遂行する責務を有する。
登録組織又はSCSセキュリティ専門家による不正行為への対処	基本規程6.3.1 (SCS-100)	制度運営機関は、登録組織が行った自己評価又はSCSセキュリティ専門家が★3確認責任者として行った確認若しくは★4評価責任者として行った第三者評価に関する業務において、不正行為が疑われる事象が発見された場合、調査を行い、弁明の機会を付与した上で、必要に応じて改善の指示を行う。改善の効果が認められない場合は、登録を取り消すことができる。
アセスメントシート等に記載された情報の真実性	★3・★4自己評価等ガイド4.1 (SCS-410)	アセスメントシート等に記載された情報の真実性については、登録希望組織が責任を負う。★3確認責任者及び★3確認従事者は、所定の確認を行ったこと及びその結果について責任を負うものであり、記載された情報が事実と異なっていたことをもって責任を負うものではない。

8 . 研修

- 研修事業者は、SCS評価制度における確認・評価業務を適切かつ一貫して遂行するために必要な知識と技能を習得する研修を提供する。
 - ・ 研修内容は研修実施基準に基づき作成、研修事業者によって内容・提供価格は異なる。
 - ・ 研修合格の有効期限は3年。
 - ・ 研修受講の前提条件としてIPAの動画研修（制度理解）を受講する。

科目	内容（例）
制度理解	・ SCS評価制度の概要説明 ・ 制度文書及び関連リソースの紹介 ・ SCSセキュリティ専門家の役割、倫理
知識	・ SCSセキュリティ専門家、★4評価従事者、★3確認従事者としての業務の理解 ・ ★3・★4要求事項・評価基準の理解 ・ 評価対象の分析と確認のポイント ・ 評価判断と評価結果の取りまとめ
技能	・ アセスメントシートレビュー演習 ・ ヒアリング・評価結果説明演習

【参考】ロールモデル及び確認・評価業務に求められるスキル



指定研修を受講し、修了の結果達成する人物像

近年のセキュリティ動向を踏まえ、SCS評価制度の背景や目的、要求事項・評価基準を正しく理解している。
客観的かつ一貫性のある判断を行い、その妥当性を責任者、従事者それぞれの立場で説明責任をもって確認・評価に臨むことができる人物。

	タスク	必要となる知識	必要となる技能
業務従事前	制度を理解する	・制度概要（目的・背景） ・制度に関わる者の倫理観 ・ガイドライン等制度ドキュメント体系概要 ・★3確認、★4評価（技術検証含む）概要 ・要求事項・評価基準の概要 ・アセスメントシートの記入方法の概要	・社会を取り巻くセキュリティの脅威状況から要求事項・評価基準が適正であることを説明できる。 ・要求事項・評価基準の主旨及び内容を説明することができる。 <SCSセキュリティ専門家> ・自ら実施計画を立案することができる。 ・★3確認従事者、★4評価従事者に計画を説明することができる。 ・★登録申請事業者に一連のプロセスを説明し、合意を得ることができる。
	確認・評価業務を理解する	・自己評価ガイド、第三者評価ガイド等の読み解き方 ・制度の信頼性維持を意識した行動	
業務従事中	確認・評価業務を実行する	・要求事項・評価基準に対する評価手法、及び専門的判断 ・適用範囲の妥当性の確認 ・（★4評価機関の場合）技術検証概要	・アセスメントシートを見て事業者のセキュリティ対策状況を読み取れる。 ・基準適合性について適切に確認、評価ができる。 ・確認、評価判断の根拠を明確に説明できる。 ・制度および★3の確認、★4の評価スキームの概要を説明することができる。 ・判断に迷うケース（グレーゾーン）において、根拠を明らかにして、妥当な認定・解釈を行うことができる。 ・不足する情報を特定し、情報提供を求めることができる。 ・ヒアリング、観察等の結果を整理した情報を基に、安全を優先した合理的判断を導き、申請者に適切に説明できる。 ・疑義がある場合等はヒアリング等により検証できる。 ・必要に応じて修正や改善に向けた助言ができる。 <SCSセキュリティ専門家> ・一連のプロセスに従い、確認、評価プロセスをリードすることができる。 ・★3確認従事者、★4評価従事者の誤りを指摘できる。 ・SCSセキュリティ専門家としての倫理観のもと公平・公正な確認を実施できる。
業務終了後	★登録申請事業者に応援申請手続きの助言ができる	・取得希望組織による★申請に係る手順の概要	・最終的に要求事項・評価基準を全て満たしていると判断した場合に、アセスメントシート記載事項について正しいことの責任を持つ（署名を行う）ことができる。 ・★登録申請事業者の申請において助言ができる。

● 知識

	科目及び履修内容	達成目標
1	SCSセキュリティ専門家、★3確認従事者、★4評価従事者としての業務の理解 ✓ オリエンテーション ✓ 確認・評価業務に従事するに当たって理解しておくべきこと（IPA動画振り返り） ✓ 確認・評価のプロセス	SCSセキュリティ専門家、★3確認従事者、★4評価従事者として、確認・評価業務に携わる前の基本的事項を理解できる。
2	★3・★4要求事項・評価基準の理解 ✓ 要求事項・評価基準の読み解き、評価手法の理解 ✓ 自己評価結果の見方、読み解き ✓ 技術検証レポートの読み解き（★4の場合）	★3・★4要求事項・評価基準を参照し、★3確認における自己評価結果の妥当性及び★4第三者評価における適合性の判断に必要な確認観点を理解できる。
3	確認・評価の対象と実施ポイント ✓ 適用範囲の妥当性確認 ✓ ★3・★4要求事項・評価基準におけるシステム・情報の分類 ✓ 確認・評価項目の抽出	確認・評価の対象となる適用範囲の妥当性を確認できる。必要な確認・評価項目を抽出できる。必要に応じて追加確認ができる。
4	評価判断と評価結果の取りまとめ ✓ 評価判断の根拠の整理 ✓ グレーゾーン事案における判断の考え方 ✓ 評価結果の記載方法 ✓ 改善推奨事項の整理と説明方法	グレーゾーン事案を含む評価項目について、根拠に基づく合理的な評価判断を行い、評価報告書（仮称）に分かりやすく記載することができる。

● 【技能】（120分）

	科目及び履修内容	達成目標
1	【ケーススタディ①】 自己評価結果のレビューの演習 ✓ 自己評価結果の読解 ✓ ★3確認における自己評価結果の妥当性及び★4第三者評価における適合性の判断 ✓ 不足情報の抽出 ✓ 追加確認事項の整理 ✓ ケーススタディ①に対する講師講評	自己評価結果から評価対象の状況を把握し、要求事項・評価基準との対応関係を整理できる。 ★3確認における自己評価結果の妥当性及び★4第三者評価における適合性の判断、不足情報の抽出及び追加確認事項の整理を行い、その判断理由を説明できる。
2	【ケーススタディ②】 ヒアリング・評価結果の説明の演習 ✓ グレーゾーンにおける評価判断 ✓ 判断根拠の説明 ✓ 確認報告書又は評価報告書の作成 ✓ 評価結果のフィードバック ✓ ケーススタディ②に対する講師講評	判断が難しい事案において、要求事項・評価基準に基づく客観的な評価判断を行い、その根拠を説明できる。確認・評価結果を整理し、登録希望組織に対して分かりやすく説明するとともに、改善に向けた助言を行うことができる。ただし、登録希望組織の具体的なセキュリティ対策の設計・実装を代行又は指示してはならない。

● 【まとめ】（15分）

	科目及び履修内容	達成目標
1	確認・評価業務における注意事項 ✓ 登録希望組織の機微な情報を取り扱うことを再認識させる。 ✓ 制度に携わるSCSセキュリティ専門家、★3確認従事者、★4評価従事者として倫理観をもった行動を意識させる。	SCSセキュリティ専門家、★4評価従事者、★3確認従事者として機密保持、公平性、客観性及び説明責任を踏まえた行動を実践できる。

9．導入促進策

● ★取得のための各プロセスにおいて推進している導入促進策

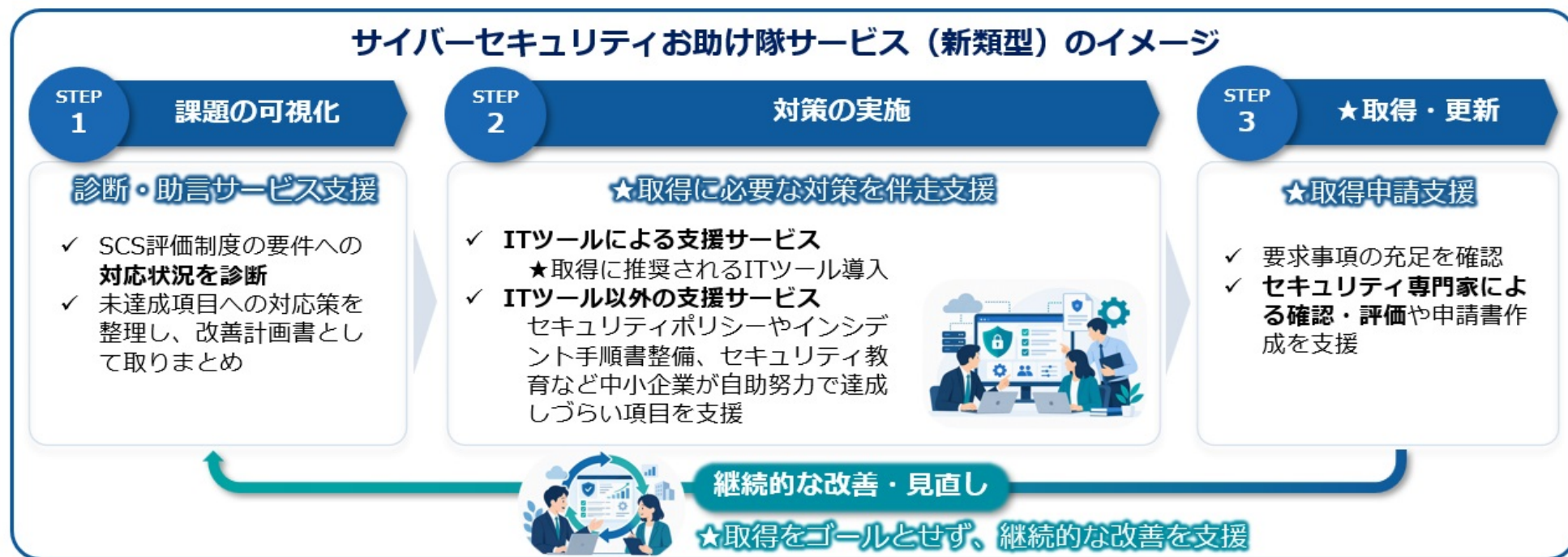
発注元企業	★の取得を求める 				
サプライヤー企業		制度について知る 	必要な対策を講じる 	★を取得する 	★を更新等する 
実施事項	■ ★の取得をサプライヤー企業に求めることを通じてサプライチェーン全体のサイバーレジリエンスを向上させる。	■ 制度についてインターネット等で情報収集する。 ■ セミナーや講習等に参加する。	■ 必要に応じてベンダーやセキュリティ専門家からの協力を得つつ、★取得に必要なセキュリティ対策を講じる。	■ セキュリティ専門家からの確認(★3)、又は評価機関等からの第三者評価(★4)を受け、★を取得する。	■ ★の有効期限に基づき、適宜更新及びそれに必要な手続き等を行う。
導入促進策	✓ 取引先への要請等に係る考え方の整理 サプライヤー企業への要請に係る独占禁止法等との考え方整理 ✓ 業界毎の特性を踏まえた導入促進 各業界のセキュリティガイドライン等において、本制度の要求基準等の活用や★取得確認の推奨を推進 ✓ 政府機関や重要インフラ事業者等における活用の推進 政府調達での参照や重要インフラ事業者等での活用推奨等について検討	✓ 本制度の継続的な広報、周知 制度に対する活用意欲を向上させる広報や周知活動を継続的に実施 ✓ 「中小企業の情報セキュリティ対策ガイドライン」の整備 中小企業の情報セキュリティガイドライン及び付録サンプル規程において★の取得を支援 ✓ 他のガイドラインや国内外の関連制度との整合性確保 「SECURITY ACTION」「自工会・部工会ガイドライン」等との整合性の確保や、評価結果の本制度での活用などの連携方策を検討	✓ 中小企業セキュリティ普及促進 ★3・★4に対応した、サイバーセキュリティお助け隊サービス(新類型)の実証事業を実施中 ✓ 専門家の活用促進 「中小企業向けサイバーセキュリティ専門家リスト」を整備し、主に中小企業と専門家とのマッチングの仕組みを構築	✓ 取引先への要請等に係る考え方の整理 発注元企業は、★取得による価格交渉に積極的に対応する必要がありかつ委託先にこれを周知する必要がある等 ✓ セキュリティ評価・対策支援人材の育成 本制度に関わる人材育成のための、コンテンツや研修機会を整備	✓ 取引先への要請等に係る考え方の整理 発注元企業は、★取得による価格交渉に積極的に対応する必要がありかつ委託先にこれを周知する必要がある等

- 中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順などを示したガイドライン
- 本編2部と付録より構成
 - ・ 経営者が認識すべき「**3原則**」、経営者がやらなければならない「**重要7項目の取組**」を記載
 - ・ 情報セキュリティ対策の具体的な進め方を分かりやすく解説
 - ・ 「情報セキュリティ基本方針（サンプル）」や「情報セキュリティ関連規程（サンプル）」などのすぐに使える**ひな形**を付録
- 第4.0版ではSCS評価制度の基本的な考え方を反映
 - ・ 「情報セキュリティ関連規程（サンプル）」は、SCS評価制度の★3・★4の要求事項に対応し、SCS評価制度の要求項目との対応表も掲載



● 本制度の★ 3・★ 4の取得支援を目的とする。具体的には、★ 3・★ 4の対策項目のうち**未達成の項目について、お助け隊サービス(新たな類型)の導入により達成させる**ものとする。

- STEP 1として、サービス提供に当たって**本制度の★取得及び更新時に中小企業の対策状況を評価**することをサービスに含める。
- STEP 2として、本制度の対策項目の中には、ITツールの導入により達成できる項目や、人的支援により達成できる項目があるため、お助け隊サービス（新類型）は「**ITツールによる支援**」のほか「**ITツール以外の支援**」を組み合わせて提供することをサービス内容とする。



- 「中小企業向けサイバーセキュリティ専門家リスト」を整備し、主に中小企業と専門家とのマッチングの仕組みを構築する。
- 2025年7月からリストを試行公開するとともに専門家による中小企業指導の支援ツールを公表。
2026年10月、本制度におけるセキュリティ専門家の確認・助言に資する支援ツールを追加。

- 国家資格「**情報処理安全確保支援士（登録セキスペ）※**」の資格者のうち、**中小企業向けのサイバーセキュリティ対策支援**が実施できる専門家の**得意分野・専門領域を可視化**したリスト（支援対象地域別）
- 現段階の情報を試行公開（HTML版）。今後、整備・拡充する予定
- URL：<https://www.ipa.go.jp/security/sme/shien/list.html>

※サイバーセキュリティ対策を推進する人材の国家資格。サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言等を行い、セキュリティの確保を支援する。国家資格として厳格な秘密保持義務、信用失墜行為の禁止義務を有する。<https://www.ipa.go.jp/jinzai/riss/index.html>

- 掲載専門家の**支援対象地域別**にリスト化
支援対象地域：北海道、東北、関東、甲信越、東海、近畿、中国、四国、九州、沖縄
- 掲載専門家が支援可能な**指導テーマ**、支援実績、得意とする**業界**、支援可能**形態**、支援**料金**、保有**資格**、保有**スキル**等を記載



- **【登録セキスペ向け】**
専門家による中小企業指導の支援ツール（実施要領）を整備・公表
 - ・ テーマ(1) 情報セキュリティ規程の整備
 - ・ テーマ(2) 情報資産の洗い出しとリスク分析
 - ・ テーマ(3) クラウドサービスの安全利用
 - ・ テーマ(4) セキュリティインシデント対応
 - ・ テーマ(5) 従業員向け情報セキュリティ教育
 - ・ テーマ(6) セキュリティアセスメント

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（概要）

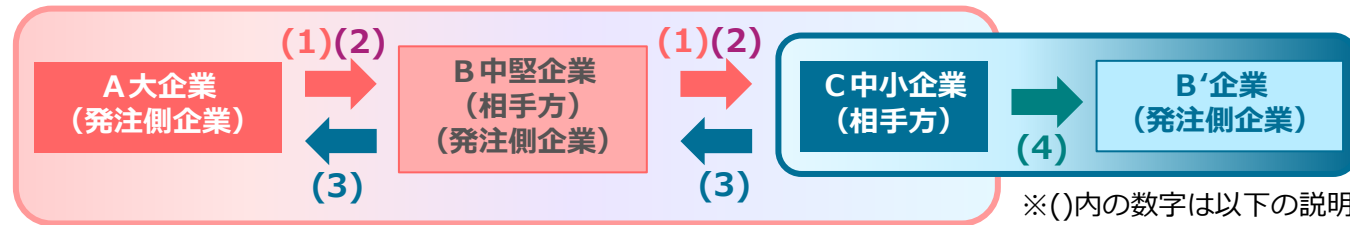


経済産業省・公正取引委員会

- 経済産業省及び公正取引委員会では、「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」を補足するため、発注者・相手方双方を対象とした、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を作成。
<https://www.meti.go.jp/policy/netsecurity/partnership2.html>
- 想定事例は、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に基づく対策要請を円滑に行い、発注者側・相手方がパートナーシップを構築してセキュリティ対策と価格交渉を実施し、円満に合意するものとしている。

【想定事例】

【サプライチェーンのイメージと想定事例の各場面】



※()内の数字は以下の説明文に対応

(1) セキュリティ対策実施の要請

A（大企業）は、相手方であるB（中堅企業）に対し、①組織ガバナンス・取引先管理、システム防御・検知、事案対応等の対策の実施（*）、②Bの相手方であるC（中小企業）に対し①と同様の対策を講ずることを要請
（*）「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）」中の「★4」に相当

(2) 要請に当たってのパートナーシップの構築

Aは、自社の対応方針を定め、B・Cに対する説明会を定期的開催（講ずべきセキュリティ対策の内容や国の支援策等を説明）。また、AからB、BからCに対し、費用負担の考え方、セキュリティ対策が価格交渉の対象になる旨、価格交渉に積極的に対応する旨を周知。

(3) 要請への対応と価格交渉の実施

B・Cは、それぞれ発注者側から受けた説明により対策の必要性を理解し、国の支援策を活用することで要請された対策を安価に実現。対策に要したコストに関し、発注者側による説明に基づき価格交渉を実施し、円満に合意。結果を双方が書面に記録して保存。

(4) 要請を行っていない発注者側企業への対応

Cは、要請を受けていないB'（中堅企業）とも価格交渉を行うため、取引かけこみ寺などの支援機関へ相談。得られた助言に基づき、Bとの交渉で用いた費用負担の考え方等を整理した上でB'に対し価格交渉を申し入れ、対策の必要性や同社との取引割合などを勘案した費用負担の考え方等を説明。交渉は円満に合意に達し、結果を双方が書面に記録して保存。

【想定事例解説】

想定事例を補足するため、以下の点について解説を作成。

- ① SCS評価制度に基づいたセキュリティ対策要請が合理的範囲を超えた負担を課すものではないこと。
- ② 発注者・相手方双方でパートナーシップを構築することの必要性や重要性。
- ③ セキュリティの経費が物件費や人件費などの間接経費として計上されること。
- ④ 価格交渉の考え方や、要請をしていない発注者側企業に対する価格交渉に当たって支援機関を活用すること。
- ⑤ 取引かけこみ寺や公正取引委員会の事前相談制度・一般相談・事例集の紹介。

【今後の取組】

本文書について、経済団体や中小企業支援機関等に協力いただきつつ、大企業・中小企業等の双方に対して、普及展開を進めていく。

- SCS評価制度に関する最新情報は、IPA公式サイトにて順次公開

- SCS評価制度公式サイト

<https://www.ipa.go.jp/security/scs/index.html>

※最新情報やセミナー案内をメールニュースで配信中



(QRコード：IPA公式サイト)



独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan

Beyond Digital