

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）に関するよくあるお問い合わせ（FAQ）

最終更新日：令和 8 年 3 月 27 日

注：本 FAQ は、SCS 評価制度における制度構築方針に対してよく寄せられる質問に対し、最終更新日時点での回答を記載したものであり、今後の制度詳細化に当たって内容が変更される可能性があることを、あらかじめ御承知おき下さい。

Q1 SCS 評価制度の具体的な開始時期はいつですか？

現時点では、SCS 評価制度の開始時期（**申請の受付開始時期**）は令和 8 年度末頃（1 月～3 月頃）を予定しています。詳細なスケジュールや提出様式等については、令和 8 年度に具体化される予定ですので、SCS 評価制度のスキームオーナーである独立行政法人情報処理推進機構（IPA）の公表をお待ちください。

Q2 ★3 や★4 の取得は必須ですか？ それとも任意ですか？

本制度は、事業者間で委託元から委託先に対して求めるセキュリティ水準を分かりやすく提示し、サプライチェーン全体のセキュリティ水準を高めることを目的とした**任意の制度**です。

★の取得は委託元（または委託先）との取引契約において決められるものであり、**本制度として何らかの規制を課すものではありません**。

関連ワード：強制、義務、取引停止

Q3 各★の取得情報（取得企業）は公開されるのでしょうか？

★3 や★4 を取得した企業については、制度オーナーである独立行政法人情報処理推進機構（IPA）の WEB サイトで公開することを予定しています。詳細は令和 8 年度の制度具体化後に IPA から公表する予定です。

Q4 ★3 の取得に必要となる、「専門家」とはどのような人材ですか？

★3 の「**専門家確認付き自己評価**」における「**専門家**」とは、制度構築方針 p.20 に記載の要件を満たす「**セキュリティ専門家**」を指します。具体的には、情報処理安全確保支援士、公認情報セキュリティ監査人、CISSP、CISM、CISA 又は ISO27001 主任審査員等の資格保持者のうち、本制度における所定の研修を受講した者を想定しています。詳細な要件については、制度の具体化に伴い改めて IPA から公表する予定です。

関連ワード：登録セキスペ

Q5 評価機関はどこに公開されていますか？

★4 の第三者評価における評価機関は、制度構築方針 p.39 に記載の通り、令和 8 年 12 月頃を目途に IPA から公表される予定です。現時点では、指定・公表は行われていません。

Q6 SCS 評価制度は、どのような業種や企業規模に適用されるのですか？

業種や事業規模を問わず、幅広い事業者が対象となり得ます。サプライチェーンを構成する企業等を対象としていますが、取引先からの要請が無くても、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、マーク（★）を自主的に取得することも考えられます。

Q7 サイバーセキュリティお助け隊サービス（新類型）は、どのような支援を提供するのですか？

サイバーセキュリティお助け隊サービス（新類型）は、★3や★4の取得支援を目的としたサービスです。具体的には、セキュリティポリシー策定などの組織的対策の支援をサービス内容とする予定です。

詳細は下記 URL をご参照ください。

https://www.meti.go.jp/policy/netsecurity/otasuketai_jissho.html

Q8 ★取得しないと委託契約を打ち切られると聞きました。本当ですか？

本制度は、2社間の取引契約等において、発注企業が、受注側に適切な段階(★)を提示し、示された対策の実施を促すとともに、実施状況を確認することを想定しています。

したがって、★取得をどのような要件として契約上扱うかは、契約当事者同士で円満に合意されるべきものであり、独占禁止法上及び取適法上適切に本制度を活用することが求められます。

詳細は、下記 URL を御参照ください。

<https://www.meti.go.jp/policy/netsecurity/partnership2.html>

Q9 ISMS と SCS 評価制度は何が違うのですか？

SCS 評価制度の★3及び★4は、代表的な脅威を参考に、効果の高い管理策を抽出するベースラインアプローチを採用しています。ISMS（情報セキュリティマネジメントシステム）とは相互補完的な制度と位置づけていますが、詳細な比較については制度構築方針 p.28 をご参照ください。

Q10 EDR や資産管理システムなど、特定のセキュリティ対策製品を導入しなければならないのですか？

★の取得を希望する組織の規模やシステム構成によって求められる対応が必ずしも同一では無いことから、本制度の評価基準を達成するにあたっては、**特定のセキュリティ対策製品の導入を求めるものではありません。**

Q11 ★3 の取得に必要なチェックリストはどこで入手できますか？ 判定方法や合格基準も教えてください。

★3・★4 要求事項及び評価基準は制度構築方針と共に公開しています。詳細な評価方法は、来年度の制度具体化の過程で IPA から公表予定です（ガイダンス資料として、令和8年秋頃目途で公開予定です。）。

Q12 ★3 取得の際、社内の情報システム担当者が確認すれば良いのでしょうか？

★3 の取得にあたっては、「**セキュリティ専門家**」による確認が必要です。単に社内の情報システム担当者であれば良いというものではありません。セキュリティ専門家の要件については、制度構築方針 p.20 をご参照ください。

Q13 ★3 や★4 の取得後、どのように「基準を達成しています」と宣言すれば良いですか？

★3 や★4 の取得後の、取得企業における社外周知・広報活動に係る活用方法については、令和8年度の制度具体化の中で IPA から公表します。

関連ワード：ラベル, マーク

Q14 ★4 の評価機関とは具体的にどのような機関ですか？

★4 の評価機関については、制度構築方針 p.21 にて要件が示されています。現時点では、評価機関の指定・公表は行われておりません。制度構築方針 p.39 のスケジュール上で公表していないものについては、令和8年度の制度具体化の過程において、制度開始までに IPA から公表します。

Q15 制度の詳細や提出様式、受付開始時期などはいつ公表されますか？

制度の詳細や提出様式、受付開始時期等については、令和8年度の制度具体化の過程において、制度開始までに IPA から公表します。公表までお待ちください。

Q16 サプライチェーンのどの範囲まで評価対象となりますか？（例：在宅勤務者や出向者の業務環境も含まれますか？）

現時点では、制度構築方針にて制度の方針が示されている段階です。詳細な評価対象の範囲については、令和8年度の制度具体化の過程において、制度開始までに IPA から公表します。公表までお待ちください。

関連ワード：テレワーク、社外常駐者

Q17 ★の取得は公共事業の入札要件になりますか？

政府機関等や重要インフラ事業者等における調達等での活用は、今後検討してまいります。

関連ワード：調達要件

Q18 中小企業だけが対象ですか？ 大企業も評価対象になりますか？

制度構築方針に記載の通り、**業種や事業規模を問わず、幅広い事業者が対象**となり得ます。中小企業だけでなく、大企業も評価対象とすることが可能なように制度を設計しています。

Q19 ★3 の有効期間は1年とありますが、取引期間が1年を超える場合はどうなりますか？

本制度は、2社間の取引契約等において、発注企業が、受注側に適切な段階(★)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しています。

したがって、契約上で★の取得状況をどのような要件として取り扱うかは、契約当事者同士で合意されるべきものでありますが、制度の趣旨に鑑みると、例えば当該契約の満了までは、必要な★の評価を維持し続けることを求める等の運用が考えられます。

Q20 ★によって想定される脅威が異なると聞きましたが、どのような違いがありますか？

★によって想定される脅威については、制度構築方針にて「一般的なサイバー攻撃」と「未知の攻撃も含めた高度なサイバー攻撃」等の違いが示されています。詳細は制度構築方針をご参照ください。

関連ワード：脆弱性

Q21 全ての要求事項・評価基準を満たさないと、制度開始後直ちに取引停止等になるのでしょうか？

本制度は、事業者間で委託元から委託先に対して求めるセキュリティ水準を分かりやすく提示し、サプライチェーン全体のセキュリティ水準を高めることを目的とした**任意の制度**です。

したがって、契約上で★の取得状況をどのような要件として取り扱うかは、契約当事者同士で合意されるべきものではあります。例えば、★取得の有無のほかに、本制度の**要求事項・評価基準を共通のチェックリストとして**必要なセキュリティ基準を満たしているか確認するといった活用方法も想定されます。

なお、**本制度の開始は申請受付の開始を意味**しており、制度開始時点において★を取得している企業は存在しません。

関連ワード：強制, 義務, ★取得できない, 一部不適合