企業の情報セキュリティ対策を「見える化」

セキュリティ対策（SCS）評価制度とは

近年、取引先に影響を与えるようなサイバー攻撃事案が頻発しており、サプライチェーン全体でのサイバーセキュリティ対策の強化が求められています。そうした中、取引先のセキュリティ対策状況を外部から判断することが難しいといった発注元企業側の課題や、複数の取引先から様々な対策を要求されるといった委託先企業側の課題が生じています。

■セキュリティ対策（SCS）評価制度とは
セキュリティ対策（SCS）評価制度とは、経済産業省と内閣官房国家サイバー統括室が進める、企業のIT基盤における基本的なサイバーセキュリティ対策の実施状況を、客観的に評価・認定する制度です。この制度の目的は、これまで各企業が独自に行ってきたセキュリティ対策の状況を「見える化」し、サプライチェーン全体でセキュリティレベルを把握・向上させるための共通の枠組みを提供することにあります。正式名称は「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」（SCS＝Supply Chain Security）で、本年2026年度に本格運用が予定されている制度です。

■制度の目的
サプライチェーンを構成する企業のセキュリティ対策状況を共通の基準で評価・可視化することで、委託元企業・委託先企業双方の負担を軽減しつつ、サプライチェーン全体のセキュリティ水準の底上げを図る仕組みとして位置付けられています。
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（★3～★5の3段階）を評価提示して見える化し、示された対策を促すとともに実施状況を確認することが想定されています。
※本制度は、企業のセキュリティ対策へ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）ではありません。

■制度の対象範囲
本制度は、サプライチェーンを構成する企業等のIT基盤（クラウド環境で運用するものも含む。）を対象としています。なお、一般的にIT基盤に該当しないと考えられる製造環境等の制御（OT）システムや委託元等に提供する製品等については、サプライチェーン全体での共通化が難しいことから直接の対象とはせず、他の制度・ガイドライン等に基づき対策を行うことが想定されています。

■評価レベルの概要
セキュリティ対策の段階を★3・★4（★5については今後検討）に区分し、★3の要求事項・評価基準を基礎として、★4ではより段階的に広い範囲や対策を含む要求事項・評価基準に基づき、自己評価（専門家の確認を経たもの）や第三者評価機関により評価されます。

構築する評価制度

	★3		★4		★5 [検討中※5]
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： • 基礎的な組織的対策とシステム防御策を中心に実施		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： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施		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： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
要求事項	26件	有効期間 1年	43件	有効期間 3年（毎年自己評価を実施し結果を評価機関へ提出）	（今後検討）
評価スキーム	**専門家確認付き自己評価** ※4		**第三者評価**		第三者評価

［※4］専門家：登録セキスペ、CISSP等の資格を有し、かつ制度が定める研修を受講したセキュリティ専門家　［※5］ISMS適合性評価制度、★3・4との整合性も踏まえ、対策事項を今後検討

出典：経済産業省 「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関する制度構築方針（案）」

セキュリティ対策段階★1と★2は、すでにIPA（情報処理推進機構）が実施している「SECURITY ACTION（セキュリティアクション）」という制度によって位置づけられることになっています。比較的容易に取り組める「自己宣言」のレベルです。
★1: IPAの「情報セキュリティ5か条」に取り組むことを自己宣言する。
★2:「5分でできる！情報セキュリティ自社診断」で状況を把握したうえで、情報セキュリティ基本方針を定めて公開することを自己宣言する。

■制度開始の時期
セキュリティ対策段階★3及び★4：2026年度末頃の制度開始（申請受付の開始）を目指しています。
セキュリティ対策段階★5：2026年度以降、要求事項・評価基準や評価スキームの具体化の検討を進めています。
（※上記は制度運営基盤の整備状況等により変更となる可能性があります。）

SCS評価制度は、サプライチェーン全体でサイバー攻撃に対する対策を強化する狙いがあります。今後の制度開始を見据え、早めに自社のIT・情報セキュリティの現状把握を進めてみてはいかがでしょうか。

参照：「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関する制度構築方針」（SCS評価制度の構築方針）を公表しました（経済産業省）
https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html