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※1）の概要

[※1] SCS（supply chain security）評価制度

- 「対策状況は**外部から判断が難しい**」「**複数の取引先から様々な対策を要求**される」等の課題に対し、サプライチェーンにおける重要性を踏まえた上で満たすべき対策を提示しつつ、その状況を可視化する仕組みを構築。※2
- **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の”★”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。 本制度の活用促進を通じ、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。※3
- ３段階の水準のうち、★３・★４について、**令和８年**(2026年)**度末頃の制度開始**を予定。

[※2] 企業等のIT基盤が対象。また、評価は取得又は更新の時点において定められた水準を満たしているかを示すものであり、完全なセキュリティの確保等を保証するものではない。
[※3] 発注時等に、必要なセキュリティ対応状況の可視化を目的としたもので、いわゆる「格付け」制度ではない。

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	43件	（今後検討）
有効期間	1年	3年（毎年自己評価を実施し結果を評価機関へ提出）	
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

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進。

普及施策の例

想定される課題	中小企業等における★取得の負担	中小企業等におけるセキュリティ専門家の確保	サプライヤー企業への★取得要請時の関係法令の適用
施策の概要	**サイバーセキュリティお助け隊サービス（新類型）の創設** ★3・★4取得を目的とした、サイバーセキュリティお助け隊サービス（新類型）を創設し、安価な”★”取得を実現	**中小企業ガイドライン整備** 中小企業の情報セキュリティ対策ガイドライン及び付録サンプル規程の整備により、”★”の取得を容易化	**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」の整備により、中小企業と専門家とのマッチングを促進	**取引先への要請等に係る考え方の整理** 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案により、費用に係る円満な価格交渉を促進