SMBC
SMBCグループ
協力　日本実業出版社
SMBCコンサルティング
NETPRESS
2026. 8. 3
第 2522 号

【「SCS評価制度」とは？】

サプライチェーン リスクに備える新制度

さくら情報システム株式会社
プラットフォーム事業本部　企画部
事業開発グループ
CYBER Healthcare プロダクトマネジャー
鈴木 優一

Point

1. サプライチェーン全体でのセキュリティ対策が求められる背景を解説します。
2. SCS評価制度の概要と、セキュリティ対策の可視化における活用方法を整理します。
3. 制度対応を進めるうえで、企業がまず取り組むべき実務ステップを紹介します。

1. サプライチェーンに潜む「見えないリスク」

近年、企業のセキュリティ対策は「自社だけを守る」段階から「取引先を含むサプライチェーン全体を守る」段階へと、大きく変わりつつあります。

背景にあるのは、対策が手薄な取引先や委託先を「踏み台」にする攻撃の増加です。攻撃者は、強固なセキュリティをもつ大企業を直接狙うだけでなく、周辺の企業や委託先を侵入経路として利用します。

国内でも、部品メーカーを経由した攻撃により大手製造業の操業に影響が出た事例や、委託先を起点とした攻撃で医療機関の業務継続に深刻な影響が生じた事例が報道されています。

このように、自社がどれほど強固な対策を講じていても、取引先や委託先を起点に被害が広がれば、自社の事業継続に深刻な影響が及んでしまいます。

一方、こうしたリスクの高まりを受け、取引先間でセキュリティ対策状況を確認し合う動きが強まっており、各社独自のチェックシートが乱立することで、現場に大きな実務負荷を生んでいることが新たな課題です。

2. 国が整備を進める「SCS評価制度」のポイント

このような社会課題を受け、国が整備を進め、2026年度（令和8年度）末頃の運用開始が予定されている仕組みが**「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（略称：SCS評価制度）」**です。

本制度の狙いは、企業のセキュリティ対策状況を共通の基準で評価・可視化し、サプライチェーン全体のセキュリティ水準の底上げと、発注側・受注側双方の確認負荷軽減を図ることにあります。

制度の特徴は、単なる技術対策の有無だけでなく、経営層の関与、組織体制、取引先管理といったガバナンス面を重視する点にあります。取得した評価は、取引先に対して自社の対策状況を説明する際の客観的な材料となり、個別チェックシートへの重複対応を減らす効果が期待されます。

この評価は段階（★）で示され、実務上の中心となる「★3」と「★4」の概要は以下の通りです。

★3	サプライチェーンに関わる企業が取り組むべき基礎的な水準であり、セキュリティ専門家の確認・助言を経た自己評価により、対策状況を確認する段階。

（次頁に続く）

★4	サプライチェーン上の役割や取引先からの要求水準に応じて、より広範な対策を実施する段階。第三者評価・技術検証を通じて対策状況を客観的に確認。

なお、★1・★2は、情報セキュリティ対策への取り組みを自己宣言する既存制度「SECURITY ACTION*」に相当し、主に初歩的な取り組み状況を示す区分です。「★5」は、今後、詳細が具体化される予定です。

*「SECURITY ACTION」は、IPA（独立行政法人 情報処理推進機構）が創設した制度

3. 制度適合を進める3つのステップ

制度適合に向けて、具体的には以下のステップで進めることを推奨します。

●STEP1【要求事項分析（現状把握）】 まずは制度が求める項目（★3・★4の要求事項）と自社の現状のギャップを可視化する。「できているつもり」を排除し、証跡に基づき客観的に分析する。
●STEP2【ロードマップ策定】 STEP1の結果に基づき、対応の優先順位とスケジュールを定める。特に「多要素認証の導入」や「規程類の整備」など予算や時間を要する項目は早期に洗い出す。
●STEP3【各施策の実行と定着】 STEP2で定めた計画に沿って施策を実行し、証跡を残しながら継続的に改善することで運用・定着を図る。

これらのステップのなかで特に難しいのは、STEP2【ロードマップ策定】において、限られた予算と人員のなかで何から着手するかを決めることです。

ここでは、自社が保有する情報資産を起点に、「情報が漏洩した場合」「システムが停止した場合」に経営へ大きな影響を与える対象を見極め、対策の順番と範囲を絞り込むことが有効です。

最後に、制度対応を進めるうえで意識したいのは、サイバーリスクを完全にゼロにすることは不可能だという前提です。本制度は「要求事項を満たしたから安心」と考えるためのものではなく、「自社セキュリティ対策の成熟度」を測るための指標として活用するものです。

ゴールは★の取得そのものではなく、実効性あるPDCAを組織文化として根付かせることにあります。

4. 持続可能な経営のために

SCS評価制度の本格化により、セキュリティ対策は企業の信頼性を示す重要な要素になります。

しかしながら、多岐にわたる要求事項を正しく読み解き、必要な証跡を整え、日々の運用に落とし込むことは、容易ではありません。

特に、前述したSTEP1～3の対応は、専門知見の有無によって判断の質や実行スピードに大きな差が生じます。

こうした課題に対しては、自社の状況を理解し、適切なアドバイスをくれる外部の専門家が心強い存在となります。信頼できる相談先をもつことは、実効性ある対策を着実に定着させるための戦略的な投資といえるでしょう。

これからのデジタル社会では、セキュリティ対策の状況を客観的に示し、説明責任を果たすことが、企業に求められるようになります。

SCS評価制度を単なる対応事項と見るのではなく、持続可能な経営を支える仕組みとして活用することが、取引先との信頼関係を強め、さらには競争力を高める大きな後押しとなります。

本稿に関するご照会窓口
SMBCコンサルティング
ソリューション開発部　経営相談グループ
TEL:0120-874-809