中小企業に求められる情報セキュリティ
― SCS評価制度をご存じですか ―

筑波総研株式会社　システム開発課

はじめに

①中小企業にも広がるサイバー攻撃

近年、日本国内の企業を取り巻くサイバーリスクは急速に高まり、もはや一部の大企業だけが対策すればよいという段階ではありません。特に、サプライチェーン全体を狙った攻撃が増加していることは、企業規模に関係なく深刻な脅威となっています。攻撃者は、情報セキュリティ対策が比較的弱い中小企業を踏み台にし、その企業がつながる大企業や重要インフラ企業へ侵入する手口を多用しています。これは、単に一企業の問題にとどまらず、日本全体の産業基盤に影響を及ぼす重大なリスクです。

こうした状況を象徴する事例として、2022年に発生した自動車産業のサプライチェーンを巻き込んだサイバー攻撃があります。ある中小企業がランサムウェア攻撃を受け、その影響で大手自動車メーカーの国内工場が一時的に稼働停止に追い込まれました。このような攻撃手法は、今後さらに増加すると予想されています。なぜなら、攻撃者にとって中小企業は「侵入しやすく、価値のある情報につながる入口」だからです。中小企業は大企業と比べて情報セキュリティに対する投資が難しく、専任の担当者がいないケースも多いため、攻撃者にとって格好の標的となっています。

そのため、中小企業では、元請企業から情報セキュリティの対策状況を確認するためのチェックシートの提出が求められる機会が増加しています。しかし、多数の企業から受注している中小企業では、様式の異なるチェックシートを作成して提出しなければならず、過度な負担につながっている事例も散見されます。

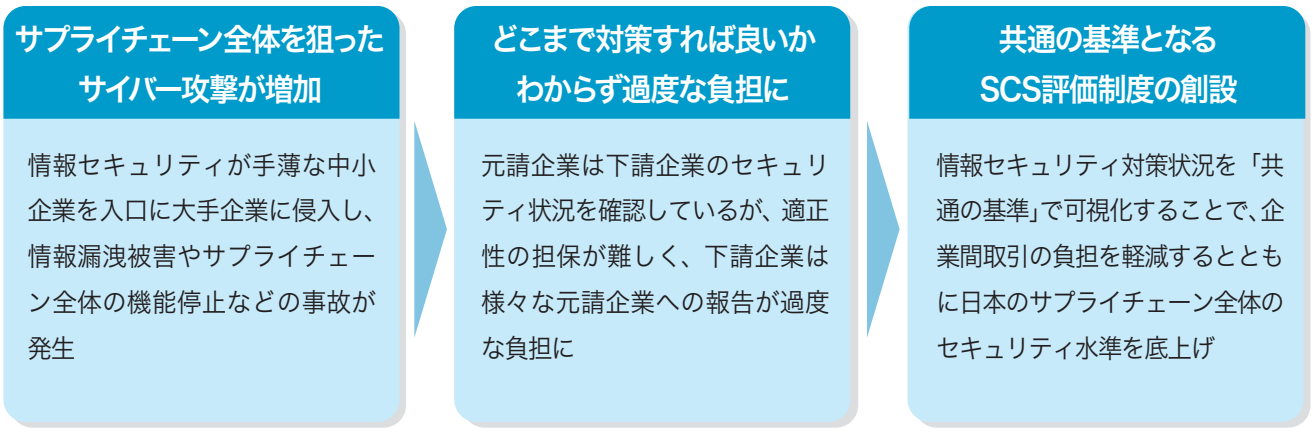
②SCS評価制度の創設

そうした中、経済産業省では日本のサプライチェーン全体の情報セキュリティ水準を底上げするための新たな仕組みとして「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）評価制度）」の導入を進めています。

この制度は、企業のセキュリティ対策状況を「★（星）」の数で可視化し、企業間で共通の基準を用いて対策状況を確認できるようにするものです。目的は、企業を格付けすることではなく、サプライチェーン全体の安全性を高めるために、共通の基準を用いて対策状況を確認できるようにすることです。

企業間で共通の基準を用いることで、チェックシートの乱立を防ぎ、企業の負担を軽減すること

図１．SCS 評価制度創設の背景



ができます。また、企業は自社のセキュリティレベルを客観的に把握し、必要な対策を段階的に進めることができます。

経済産業省では、2026年度末からの本格運用を目指して整備を進めており、すでに様々な情報が公開されています。

③制度開始に向けて早めの準備を

制度の内容を見る限り、日頃の業務を行いながら対策するのはなかなか大変なもので、元請企業に★の取得を求められてから対応しようとしても時間がかかると思われます。そのため、早めに制度の概要を理解するとともに、評価取得を支援する事業者に依頼する、といった対応が必要と考えられます。そこで本稿では、SCS評価制度の概要と、弊社筑波総研が行う制度への対応支援についてお知らせします。

1．SCS評価制度の概要

①中小企業の新しい信用指標

先ほど述べたように、SCS評価制度は企業のセキュリティ対策状況を「★（星）」の数で可視化します。中小企業は、この制度を単なる“国の新しいルール”として捉えるのではなく、むしろ、取引先からの信頼を獲得するための「新しい信用指標」として積極的に活用すべきものと考えるべきです。また、自社の情報セキュリティの現状を可視化し、必要な対策を講じることで、事業継続力を高めることにもつながります。

②SCS評価制度の基本構造

…★３・★４・★5の３段階

評価は、★３から★５までの3段階です。それぞれのレベルには明確な目的と求められる対策があり、企業は自社の業務内容や取引先の求めに応じて適切なレベルを選択することができます。

経済産業省の資料によると、★３は、「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として、基礎的なシステム防御策と体制整備を中心に実施する段階」としています。★４は、「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として、組織ガバナンス・取引先管理、システム防御・検知及びインシデント対応等包括的な対策を実施する段階」としています。★５は、「サプライチェーン企業等が到達点として目指すべき対策として、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プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施する段階」としています。

★3が、SCS評価制度の入口です。まずはここを目指して取り組むことをお薦めします。

2．★３に求められる主な要件

さて、★３に求められる要件とはどのようなものでしょうか。細かくみると、7つの分類の中に合計26項目の要求事項を定めています。本稿の最後（表１）にリスト化しましたので参考にしてください。非常に難しく感じてしまいますので、ここではもう少しかみ砕いて整理します。

①ガバナンスの整備

セキュリティ方針や守秘義務ルールを策定・周知し、責任と権限を明確にすることです。

②取引先管理

取引先との関係を把握し、機密情報の扱い方を明確にすることです。

図２．★３に求められる要件

- ①ガバナンスの整備
- ②取引先管理
- ③リスクの特定
- ④攻撃等の防御
- ⑤攻撃等の検知
- ⑥インシデントへの対応
- ⑦インシデントからの復旧

③リスクの特定

IT資産やネットワークの状況を把握する仕組みを整備し、情報管理ルールを運用することです。

④攻撃等の防御

ID・アクセス権の管理やウイルス対策・バックアップなど、基本的な防御を固めることです。

⑤攻撃等の検知

ネットワークやシステムに不審な動きがないか監視する仕組みを構築することです。

⑥インシデントへの対応

セキュリティインシデントの発生時に、具体的な対応手順や組織内の対応体制をあらかじめ定めることです。

⑦インシデントからの復旧

セキュリティインシデントの発生後に、速やかに元の状態へ復旧できるよう、必要な手順や準備を整えることです。

3．筑波総研がお手伝いします

専任の担当者がいない、IT管理が兼務である、といった理由から、セキュリティ対策に時間が割けない企業も多いのではないでしょうか。しかし、この新制度の流れに乗り、社内のセキュリティ対策を整えることで、リスクの軽減、信用力アップ、新規取引時に自社の情報セキュリティ対策についての説明が容易になるなど、大きなメリットがあります。

一方、はじめて認定を取得する際には、相応の時間と労力、専門的な知識が必要になります。認定は一年ごとの更新ですが、サイバー攻撃の手口が日々巧妙化・高度化する中では定期的なアシストが必要と考えています。

筑波総研には有資格者がおり、これまでもお客様のシステム構築やセキュリティ対策をサービスとして提供していることから、認定取得と継続のお手伝いをさせていただきます。

4．筑波総研の認定取得支援サービスの流れ

①制度のご案内（経営者層・IT担当者向け）

SCS評価制度の背景、対応することによって得られるメリット（対応しない場合のリスク）、そして弊社が提供するサービスの概要についてご説明します。そのうえでサービスをご利用いただく場合はご契約、サービスを開始します。

②現状把握支援（可視化）

社内のPC、サーバー、ネットワーク機器やデータの管理状況に加え、社内規程やセキュリティ設定をチェックし、現在のIT環境を正確に把握します。そのうえで認定の基準をクリアするために「今対策が不足している点はどこか」を可視化します。

③対策実装支援（導入・整備）

現状把握ができたら、実際に対策をします。多要素認証やウイルス対策ソフトの導入、ログ管理の導入、バックアップ体制の構築のような技術的な対策から、社内規程の作成・整備のような運用面の対策までサポートします。

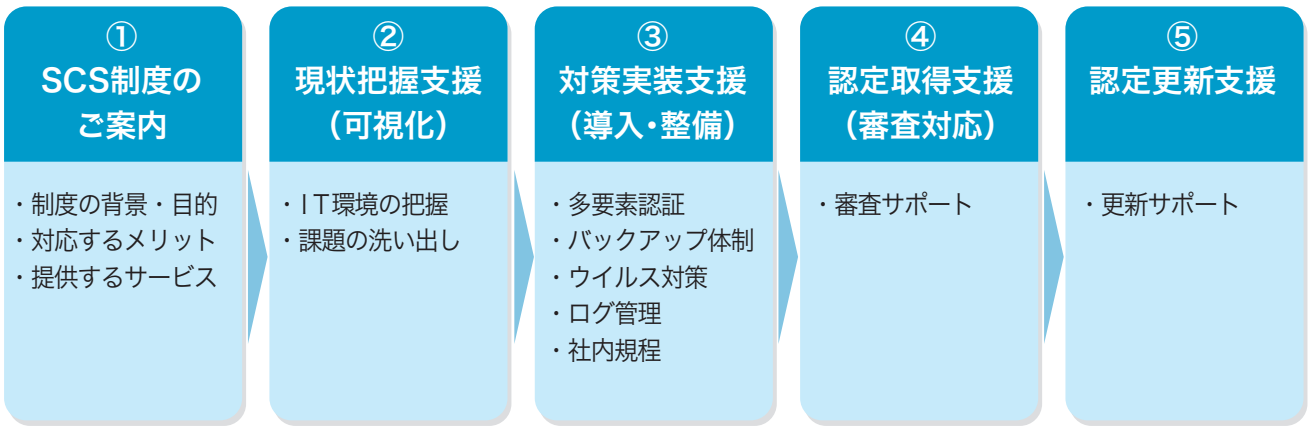
④認定取得支援（審査対応）

認定取得にはセキュリティ専門家による確認が必要となりますが、実際の審査中に受ける難しい指摘や改善要求への回答・対応について、最後までサポートします。

⑤認定更新支援

お客様の環境の変化や制度の改定に対応し、継続的な認定取得をサポートします。

図３．筑波総研の認定取得支援サービスの流れ



おわりに

SCS評価制度は、サプライチェーンリスクを改善し、安全に取引のできる環境を整えるものです。中小企業にとっては、「自社の未来を守るための投資」であり「取引先から選ばれるための戦略」です。本制度の正式運用は2026年度末が予定されていますが、IT資産の棚卸や基本的な対策の実装などには相応の時間がかかります。特に大手企業のサプライチェーンに属する企業では、早めの準備をお薦めします。お気軽に筑波総研にお問い合わせください。

【参考資料】
経済産業省HP
「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」
https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html
「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」
https://www.meti.go.jp/press/2025/03/20260327001/20260327001-br.pdf
「別添★３・★４要求事項及び評価基準」
https://www.meti.go.jp/press/2025/03/20260327001/20260327001-c.xlsx

【お問い合わせ先】
筑波総研株式会社　システム開発課
SCS評価制度担当
TEL 029-823-2411

表１．★３の要求事項

大分類 No.	分類	中分類	要求事項 No.	要求事項名	要求事項
1	ガバナンスの整備	役割、責任、権限	1	セキュリティ推進活動部門	セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。
			2	守秘義務のルール	守秘義務のルールを策定し、遵守させること。
		ポリシー	3	セキュリティ対応方針の策定	自社のセキュリティ対応方針を策定し、周知すること。
2	取引先管理	サイバーセキュリティサプライチェーンリスクマネジメント	4	取引先とのビジネス又はシステム上の関係	取引先と自社とのビジネス又はシステム上の関係を把握すること。
			5	機密情報の取扱い	自社の機密情報の取扱い方法を、共有先との間で明確にすること。
			6	セキュリティインシデント発生時の役割・責任	セキュリティインシデント発生時の他社との役割及び責任を明確にすること。
3	リスクの特定	資産管理	7	情報機器、OS及びソフトウェアに関する情報の把握	情報機器、OS及びソフトウェアに関する情報を把握すること。
			8	ネットワークに関する情報の把握	ネットワークに関する情報を把握するための仕組みを整備すること。
			9	外部情報サービスの管理	自社の機密情報を扱う外部情報サービスを管理すること。
			10	機密区分に応じた情報の管理	機密区分に応じた情報の管理ルールを定め、それに基づく管理を行うこと。
4	攻撃等の防御	アイデンティティ管理、認証、アクセス制御	11	ユーザIDの管理手続	ユーザIDの発行・変更・削除の手続を定めること。
			12	管理者IDの管理手続	管理者IDの発行・変更・削除の手続を定めること。
			13	認証の強度・実装方法の決定	システム及び情報の重要度に応じて認証の強度及び実装方法を決定すること。
			14	アカウントロック制御	パソコン及びスマートデバイスにはロック制御を行うこと。
			15	パスワード設定ルール	パスワード設定に関するルールを定め、周知すること。
			16	パスワード管理ルール	パスワードの管理に関するルールを定め、周知すること。
			17	アクセス権の管理ルール	アクセス権の管理ルールを定めること。
		意識向上とトレーニング	18	セキュリティインシデント発生時の教育・訓練	セキュリティインシデント発生時の対応に関する教育・訓練を行うこと。
		データセキュリティ	19	適切なバックアップ	適切なバックアップを行うこと。
			20	情報機器、OS及びソフトウェアの安全な構成	情報機器、OS及びソフトウェアの安全な構成を確立し、維持すること。
			21	セキュリティパッチ・アップデートの手続	情報機器、OS及びソフトウェアへのセキュリティパッチ及びアップデートの適用に係る手続を定めること。
		プラットフォームセキュリティ	22	マルウェア感染からの保護	システムをマルウェア感染から保護すること。
		技術インフラのレジリエンス	23	ネットワーク境界防護	ネットワークを適切に分離し、境界部分を防護すること。
5	攻撃等の検知	継続的監視	24	ネットワーク接続・データの監視	ネットワーク上の適切な場所でネットワーク接続及びデータ転送を監視すること。
6	インシデントへの対応	インシデント管理	25	インシデント対応手順	セキュリティインシデントへの対応手順、対応体制等を定めること。
7	インシデントからの復旧	インシデント復旧計画の実行	26	事業継続要件に沿った復旧準備	事業上重要なシステムについて、事業継続の要件に沿う復旧に必要な準備を行うこと。

出典：経済産業省HP「別添★３・★４要求事項及び評価基準」より抜粋