2026 年 6 月 10 日　全 4 頁

取引先のセキュリティが経営リスクに

サプライチェーンセキュリティ評価制度の全貌

デジタルソリューション研究開発部 シニアセキュリティ・スペシャリスト　横平 健

近年、サイバー攻撃は特定企業を直接狙う形から、取引先や委託先を起点に被害を拡大させる「サプライチェーン攻撃」へとシフトしており、中小企業への侵害が発注元企業や社会インフラに波及する事例が相次いでいます。このような状況を踏まえ、政府は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ため、「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（以下、「SCS 評価制度」）」の構築を進めています。

本稿では、SCS 評価制度の背景と概要を解説した上で、企業に求められる対応を考察します。

制度導入の背景

サプライチェーン攻撃が増加する背景には、企業活動を取り巻く環境の変化が関係しています。近年、業務の効率化やコスト削減を目的として、クラウドサービスや外部委託などの活用が進み、企業間のデジタル接続が急速に拡大しています。その結果、攻撃者にとって狙いうる対象領域、いわゆるアタックサーフェスも飛躍的に拡大しました。

このようなリスクに対応するため、多くの企業は契約締結時に秘密保持契約やセキュリティ条項を整備し、チェックリストやアンケートを通じて対策状況の確認を行っています。しかし、その多くは自己申告に依存しており、実際の運用状況を正確に把握することが難しく、対応が形式的にとどまる傾向があります。また、取引先ごとに異なるチェック項目や書式への対応は、特に中小企業にとって大きな負担となっています。

こうした背景から、委託先管理の課題を体系的に整理し、企業のセキュリティ対策水準を客観的に示す枠組みとして、「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 評価制度）」が導入されるに至りました。

SCS 評価制度の概要

SCS 評価制度は、経済産業省と内閣官房 国家サイバー統括室を中心に検討が進められている制度で、2026 年度末頃の運用開始を目指し、制度設計や運用方法の具体化が進んでいます。

本制度の目的は、国が定める業界横断の共通基準を通じて、企業間でセキュリティ対策の水準や到達度を客観的に共有できる環境を整備することです。これにより、発注側企業は取引先に求めるセキュリティ水準を

株式会社大和総研 本社　〒135-8460 東京都江東区冬木 15-6

効率的かつ合理的に判断でき、受注側企業においても取引先ごとに異なるセキュリティチェックへの対応負荷を軽減することが期待されています。さらに、制度の普及に伴い、一定水準以上の対策を講じる企業が増加することで、サプライチェーン上の脆弱性が低減し、結果として社会全体のサイバーセキュリティ強化にもつながるとみられています。

SCS 評価制度では、セキュリティ対策の成熟度に応じて、「★3」「★4」「★5」の三段階の評価レベルが設定されており、それぞれ想定される脅威や評価方法などが体系的に整理されています。評価が★3 から開始されているのは、IPA（独立行政法人情報処理推進機構）が 2017 年から運用する「SECURITY ACTION」において、初期段階に相当する★1 および★2 が既に定義されているためです。SCS 評価制度は、これを基盤とする上位の枠組みであり、専門家による確認や第三者による評価を導入することで、対策の実装状況を客観的に可視化し、取引先や関係者間で共通の評価基準を持つことが可能となっています。

図表 1：SCS 評価制度における各評価レベルの概要

	★3	★4	★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	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など	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	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	サプライチェーン企業等がさらに目指すべき高度なセキュリティ対策
評価方法	専門家による確認付きの自己評価	第三者評価	
有効期間	1年	3年 （1年ごとに自己評価を実施）	検討中
運用開始時期	2026年度末頃		未定（2027年度以降）

（出所）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』（※1）を基に大和総研作成

中小企業支援策と制度普及に向けた仕組み

SCS 評価制度では、中小企業が無理なく評価の取得に取り組めるよう、普及と定着を見据えた多面的な支援策が整備・検討されています。

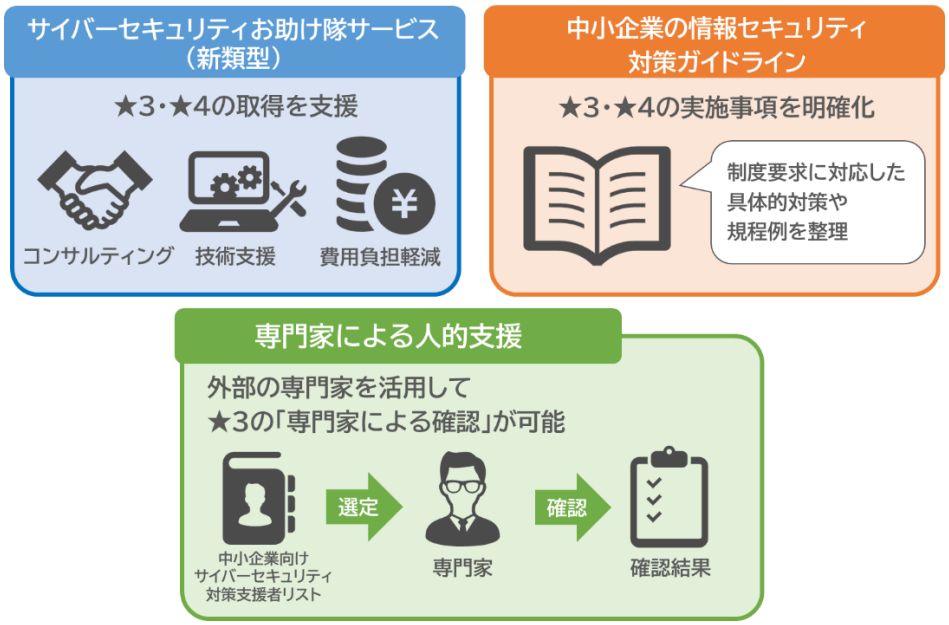
その一つとして、中小企業向けの支援サービスである「サイバーセキュリティお助け隊サービス」において、本制度への対応を支援する新類型の創設が予定されています（※2）。これにより、中小企業は★3・★4 の取得に向けたコンサルティングや技術支援を受けられ、費用面・実務面の負担を抑えつつ対応を進めることが可能となります。提供は 2026 年度末頃から開始される見込みです。

また、実務面での指針として、IPA は 2026 年 3 月に「中小企業の情報セキュリティ対策ガイドライン」の改訂版を公表しています（※3）。同ガイドラインでは、制度要求に対応した具体的対策や規程例を整理しており、★3・★4 の取得に向けた実施事項を明確化する実践的な資料となっています。

さらに、専門家による人的支援の強化も進められています。IPA は、SCS 評価制度への対応を支援可能な

情報処理安全確保支援士を整理して「中小企業向けサイバーセキュリティ対策支援者リスト」（※4）に追加し、公表する予定です。これにより、社内に専門人材を有しない場合も、★3 の取得に必要となる「専門家による確認」を受けることが可能となります。

図表 2：SCS 評価制度における中小企業への支援策



（出所）大和総研作成

企業はどう向き合うべきか

SCS 評価制度の開始に向け、各企業は自社の状況に応じた戦略的な準備を進める必要があります。発注側と受注側では求められる対応が異なるため、それぞれの立場に即した計画的な対応が求められます。

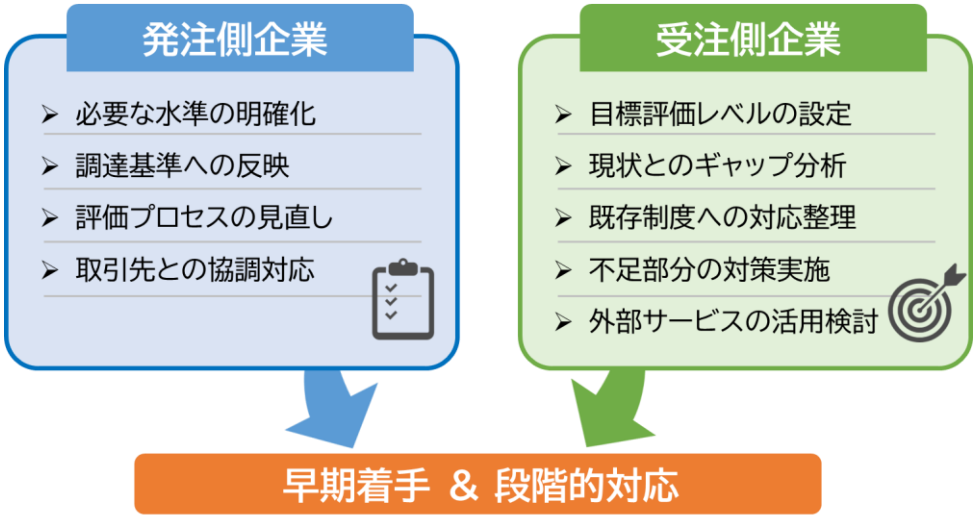
発注側企業は、まず自社に必要なセキュリティ水準を明確化し、取引や委託関係ごとに★3 または★4 の取得要件を整理の上、契約条件や調達ポリシーに反映させる必要があります。あわせて、既存のチェックシートや評価プロセスを見直し、制度に準拠した基準へ移行するため、社内ルールの整備と関係部門間の連携を進めることが求められます。また、既存の委託先に対しては、一方的な負担転嫁を避け、取引先の対策向上を支援するなど、パートナーシップを重視した運用が求められます。制度適用に際しては、政府が示す独占禁止法や中小受託取引適正化法（旧下請法）との関係性を踏まえ、公正で配慮ある対応が不可欠です（※5）。

一方、受注側企業においても、本制度を競争力強化や取引維持に資する取り組みとして捉え、主体的かつ計画的に対応を進めることが求められます。まず、自社の事業特性や取引関係を踏まえ、求められるセキュリティ水準を整理し、目標とする評価レベルを明確化する必要があります。その上で、要求事項と現状とのギャップを分析し、セキュリティポリシーや社内規程、運用体制の整備・見直しを段階的に進めることが求められます。SCS 評価制度は、ISMS や業界ガイドライン等を参照して相互補完するよう設計されていることから、既存制度に基づく対策を実施している場合は、それらとの対応関係を整理し、不足部分を補完する形で対応を進めることが効果的と考えられます。

さらに、こうした対応を推進するにあたっては、サイバーセキュリティお助け隊サービスや外部企業の活用も有効となります。

このように、発注側・受注側の双方に共通して重要となるのは、「早めのスタート」と「段階的な対応の積み上げ」です。評価取得には一定の準備期間が必要と考えられるため、各企業は余裕を持った計画のもと、着実に準備を進める必要があります。

図表 3：SCS 評価制度の評価取得に求められる対応



（出所）大和総研作成

おわりに

SCS 評価制度は法的強制力を伴わない任意の制度ですが、サプライチェーンリスクの高まりを背景に、その実務上の重要性は今後一層高まっていくと考えられます。制度の普及が進めば、評価取得の有無が取引先選定や契約判断における重要な判断要素となる可能性も十分に考えられます。

そのため、本制度を限定的なものと捉えるのではなく、自社へ影響する可能性を適切に見極めた上で、対応を主体的に検討していくことが望まれます。

(※1) 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』
(※2) 経済産業省「サイバーセキュリティお助け隊サービス（新類型）」
(※3) IPA「中小企業の情報セキュリティ対策ガイドライン」
(※4) IPA「中小企業向けサイバーセキュリティ対策支援者リストの紹介」
(※5) 経済産業省「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」