2026 年 6 月 2 日　全 13 頁

SCS 評価制度とは何か

サプライチェーンリスクに対する新たな共通基準と企業が取るべき対応

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

[要約]

- サプライチェーン攻撃の増加により、委託先の脆弱性が発注元企業や社会全体に影響を及ぼすリスクが顕在化しています。自己申告に依存する従来型の委託先管理では、発注元企業が委託先のセキュリティ対策の妥当性を適切に評価することは難しく、対策水準を共通の基準で客観的に示す仕組みの整備が求められています。

- 「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）」は、国が示す共通の基準により、各企業のセキュリティ対策の状況を評価・可視化する新たな枠組みです。企業間取引の円滑化とサプライチェーン全体のリスク低減を図ることを目的としており、2026 年度末頃の運用開始を目指し、準備が進められています。

- SCS 評価制度は、既存のセキュリティ関連制度やガイドラインを参照しつつ、それらと競合することなく補完する形で設計されています。国内外の枠組みとの整合性を確保しながら、セキュリティ対策の水準を共通の尺度で可視化することを目的とした、業界横断的な共通基盤として位置付けられます。

- 企業は制度開始を見据えて発注側と受注側のそれぞれの立場に応じて早期に準備を進め、制度への適用を図ることが望まれます。特に受注側は制度対応を取引継続や競争力向上につながる取り組みとして積極的に活用すべきです。

株式会社大和総研 本社　〒135-8460 東京都江東区冬木 15-6

1. はじめに

近年、サイバー攻撃は特定の企業を直接狙うものから、取引先や委託先を起点として被害を拡大させる「サプライチェーン攻撃」へと大きくシフトしています。特に、セキュリティ対策が相対的に手薄になりがちな中小企業や委託先企業が侵害され、その結果として発注元企業や社会インフラ全体に影響が及ぶ事例が相次いで発生しています。こうした状況を踏まえ、政府はサプライチェーン全体のセキュリティ水準を底上げするための新たな枠組みとして、「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（以下、「SCS 評価制度」という。）」[1]の構築を進めています。

本稿では、この SCS 評価制度の背景と設計思想、既存制度との関係を整理したうえで、企業が本制度をどのように受け止め、どう向き合うべきかを考察します。

2. サプライチェーン攻撃と委託先管理の課題

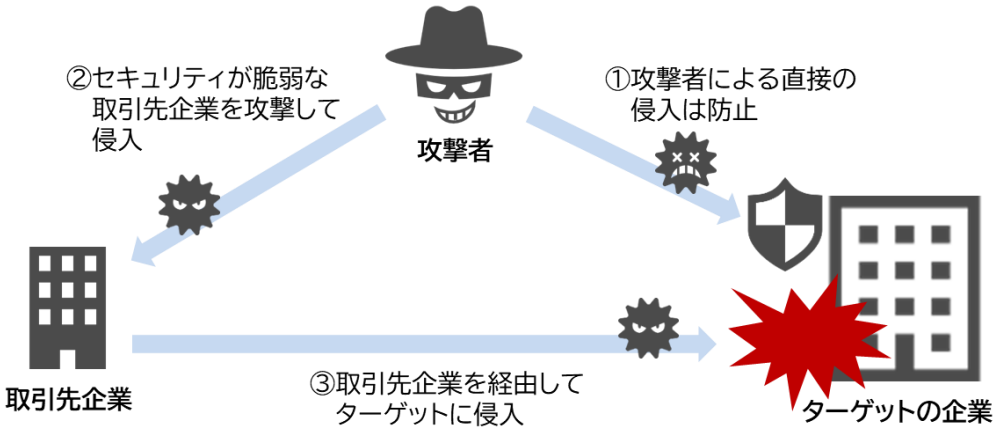
(1) 深刻化するサプライチェーン攻撃

「サプライチェーン」とは、製品・サービスにおける原材料の調達から製造、流通、販売に至るまでの一連の過程や、それに関わる企業や組織のネットワークを指します。例えば、自動車の製造であれば、部品メーカー、組立工場、物流業者、販売店などがサプライチェーンの一部となり、これらの関係者が連携して製品やサービスを消費者に提供する仕組みを形成しています。

サプライチェーン攻撃は、この複雑で多様な関係者の中で、比較的セキュリティ対策が手薄な取引先や委託先、関連会社などを狙い、そこを足がかりに最終的な標的企業へ被害を広げるサイバー攻撃の一種です。たとえ標的となる企業自身が高度なセキュリティ対策を講じていたとしても、サプライチェーン上に弱点が存在すれば、攻撃者はそこを突いて侵入経路を確保します。

[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」（SCS 評価制度の構築方針）を公表しました」

図表１　サプライチェーン攻撃のイメージ



（出所）大和総研作成

IPA が公表する『情報セキュリティ 10 大脅威』[2]において、サプライチェーン攻撃は 2019 年以降、組織向け脅威として継続的に上位に位置付けられています。これは、サプライチェーン攻撃が一過性の現象ではなく、企業活動に構造的に内在するリスクとして定着していることを示しています。

図表２　『情報セキュリティ１０大脅威』（組織向け）における過去順位の推移

順位	2022年	2023年	2024年	2025年	2026年
1	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害	ランサム攻撃による被害	ランサム攻撃による被害
2	標的型攻撃による機密情報の窃取	サプライチェーンの弱点を悪用した攻撃	サプライチェーンの弱点を悪用した攻撃	サプライチェーンや委託先を狙った攻撃	サプライチェーンや委託先を狙った攻撃
3	サプライチェーンの弱点を悪用した攻撃	標的型攻撃による機密情報の窃取	内部不正による情報漏えい等の被害	システムの脆弱性を突いた攻撃	AIの利用をめぐるサイバーリスク
4	テレワーク等のニューノーマルな働き方を狙った攻撃	内部不正による情報漏えい	標的型攻撃による機密情報の窃取	内部不正による情報漏えい等	システムの脆弱性を悪用した攻撃
5	内部不正による情報漏えい	テレワーク等のニューノーマルな働き方を狙った攻撃	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	機密情報等を狙った標的型攻撃	機密情報を狙った標的型攻撃

（出所）IPA 『情報セキュリティ１０大脅威』（組織向け）を基に大和総研作成

(2) サプライチェーン攻撃が増加する背景

サプライチェーン攻撃が増加している背景には、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

[2] IPA 「情報セキュリティ 10 大脅威」

活用が進み、企業間のデジタル接続は急速に拡大しています。その結果、攻撃者にとって狙い得る対象領域、いわゆるアタックサーフェスも飛躍的に拡大しています。

また、サプライチェーンを構成する企業間で、セキュリティ対策の水準に大きなばらつきがあることも問題を深刻化させています。発注元となる大企業では、十分な予算や専門人材を確保し、高度なセキュリティ対策が講じられる一方で、その取引先や委託先、特に中小企業では、予算や人材の制約から、十分な対策を実施できないケースも多くみられます。攻撃者はこうしたサプライチェーン上の脆弱な部分を狙うことで、少ない労力で標的企業への侵入を試みることが可能となっています。

(3) 従来型の委託先管理の課題

これらのリスクに対応するため、多くの企業ではこれまで、契約締結時に秘密保持契約（NDA）やセキュリティに関する条項を設け、必要に応じてチェックリストやアンケートで対策状況を確認する手法がとられてきました。こうした取り組みは一定の抑止効果はあるものの、主に自己申告に依存するため、実際の運用状況をどこまで正確に反映しているかを発注元が判断しづらいという課題があります。証拠の確認や技術的観点からの妥当性の評価にまで踏み込むことが難しく、「一応、確認はした」という形式的な対応にとどまりがちです。

また、取引先ごとに異なるチェック項目や様式への対応が求められることも、委託先、とりわけ中小企業にとっては大きな負担となっています。限られた人員や予算の中で、重複する確認依頼や形式の異なる書類作成への対応を繰り返す結果、対応が形式的になり、実質的なリスク低減につながりにくいという問題も生じます。さらに、このような状況下で再委託が関係すると、どの企業がどこまで対策を講じているのか把握することは一層困難になります。委託関係が複雑になるほど、サプライチェーン全体の状況を見渡すことは、従来のチェックリスト中心の管理手法では限界があるのが実情です。

このように、従来型の委託先管理は、個別企業の努力の積み重ねだけでは対応しきれない課題を抱えています。発注側・受注側双方にとって過度な負担とならず、実効性のある管理を実現するためには、企業ごとの対応に委ねるだけでなく、共通の考え方に基づく仕組みが必要です。こうした背景から、委託先管理の課題を整理し、サプライチェーンの中での役割や立ち位置に応じたセキュリティ対策の水準を客観的に示す仕組みとして、SCS 評価制度が検討・導入されるに至りました。

3. サプライチェーン攻撃と委託先管理の課題

(1) 制度の目的

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が中心となって検討を進めている制度で、サプライチェーンを構成する企業のセキュリティ対策の実施状況を、国が示す共通

の基準に基づいて評価・可視化する枠組みです。本稿執筆時点では、2026 年度末頃の運用開始を目指し、制度設計や運用方法に関する検討が進められています。

本制度は、業界を横断した共通の評価基準を通じて、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を目的としています。発注側企業にとっては、取引先に求めるセキュリティ水準を効率的かつ合理的に判断しやすくなり、受注側企業にとっても、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ます。さらに、本制度が普及することによって、社会全体のサイバー攻撃リスクの低減にもつながるとみられています。多くの企業が本制度に基づき一定水準以上の対策を講じることで、サプライチェーン上の弱点が減少し、結果としてサプライチェーン攻撃が発生しにくい状況が形成されるとともに、国全体のサイバーセキュリティ強化に寄与することが期待されます。

図表 3　SCS 評価制度で期待される効果

受注企業への効果	・取引先ごとに異なるセキュリティチェック対応の負荷軽減 ・共通基準に基づき対策状況を客観的に説明可能
発注企業への効果	・取引先に求めるセキュリティ水準を効率的・合理的に判断可能 ・サプライチェーンに起因するリスクの低減
社会全体での効果	・サプライチェーン上の弱点の減少によるサイバー攻撃リスクの低下 ・国全体のサイバーセキュリティ水準の底上げ

（出所）大和総研作成

なお、本制度は対策レベルの優劣を競い合う「格付け」制度ではないことが、政府から明確に示されています。法的な強制力を持つものではなく、あくまで任意の枠組みとして、取引契約に基づく自主的な取り組みとして運用される予定です。

(2) 評価レベルの設計と SECURITY ACTION との関係

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 3 段階で評価レベルが設定されています。これらの評価レベルは、企業の規模やサプライチェーン上での立ち位置、想定されるリスクの大きさに応じて、それぞれ以下のような位置付けが想定されています。

図表 4　SCS 評価制度における各評価レベルの対策の位置づけ

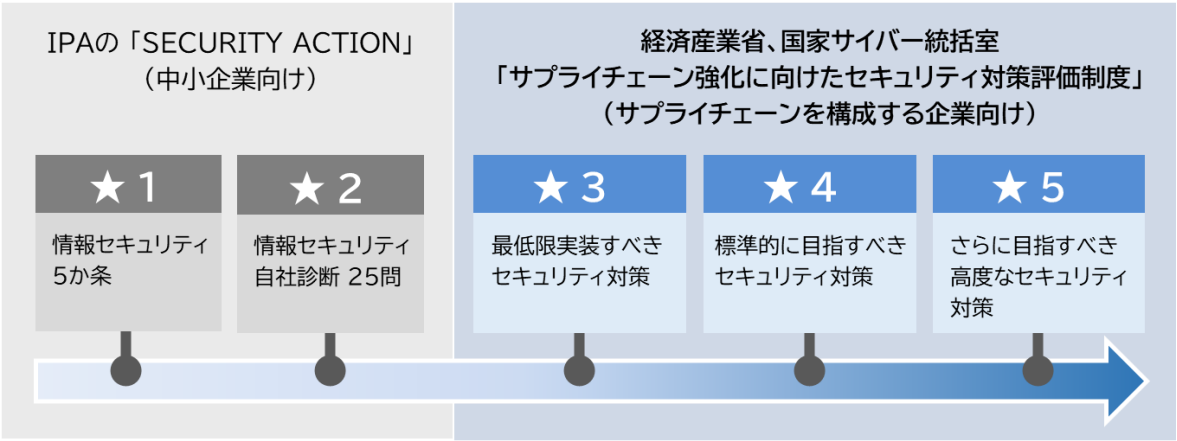
★3	全てのサプライチェーン企業が最低限実装すべきセキュリティ対策
★4	サプライチェーン企業等が標準的に目指すべきセキュリティ対策
★5	サプライチェーン企業等がさらに目指すべき高度なセキュリティ対策（今後詳細検討）

（出所）大和総研作成

この評価が★3 から始まっている理由は、IPA が 2017 年から運用している「SECURITY ACTION」において、初期段階に位置付けられる「★1」「★2」がすでに定義されているためです。SECURITY ACTION は、中小企業を主な対象として、セキュリティ対策への第一歩を促すことを目的とした制度であり、企業が自らの取り組み状況を確認し、自己宣言（自己申告）する形で登録する仕組みとなっています。基本的な対策の実施や意識向上を促す制度として、これまで多くの企業に活用されてきました。

SCS 評価制度は、こうした SECURITY ACTION の取り組みを土台としつつ、その上位の枠組みとして、段階的にセキュリティ水準を高められるよう設計されています。また、自己宣言を前提とする SECURITY ACTION とは異なり、第三者による確認・評価を取り入れることで、セキュリティ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 5　SCS 評価制度と SECURITY ACTION の関係



（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』[3]を基に大和総研作成

(3) 各段階（★３～★５）の詳細

SCS 評価制度では、★3 から★5 の各評価レベルに応じて、評価方法や確認主体、有効期間などがそれぞれ整理されています。このうち、2026 年度末頃から運用開始を予定しているのは★３と★４であり、★５の運用開始は 2027 年度以降になる見込みです。

まず★3 は、広く認知された脆弱性を悪用する一般的なサイバー攻撃を主な想定脅威とし、サプライチェーンに関わる全ての企業が最低限実施すべき基本的なセキュリティ対策を求める水準となります。対策の重点は、代表的な脅威に対して有効性が確認されている対策を確実に講じることです。評価方法は企業自身による自己評価を基本とし、その内容をセキュリティ専門家（例：情報処理安全確保支援士や CISSP などの有資格者）が確認する形が想定されています。有効期間は 1 年です。

[3] 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』

次に★4 は、機密情報の漏えいや事業継続に重大な影響を及ぼし得るサイバー攻撃など、より深刻なリスクを想定した水準です。要求される対策の範囲は、初期侵入の防止にとどまらず、侵入後の被害拡大の防止も含めた、より広範な対策が求められます。評価機関による客観的な評価が前提となり、有効期間は 3 年とされています。ただし、取得後も 1 年ごとに自己評価の実施が必要とされており、対策の継続的な運用と改善を促す仕組みとなっています。

最後に★5 は、未知の攻撃を含む高度なサイバー攻撃への対応を想定した最上位の水準です。現時点でのベストプラクティスに基づく対策の実行が想定されていますが、具体的な要求事項や評価基準などの詳細は今後検討される予定です。

なお、本制度は上位の★評価ほど広範かつ高度な対策を求める設計となっていますが、実務上、必ずしも★3 から順に取得しなければならないわけではなく、自社の役割や取引要件に応じて、初めから★4 の取得を目指すことも可能となっています。この場合でも、★4 の取得には★3 相当の対策が含まれるため、結果として下位水準の対策も網羅されることになります。

図表 6　SCS 評価制度の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）

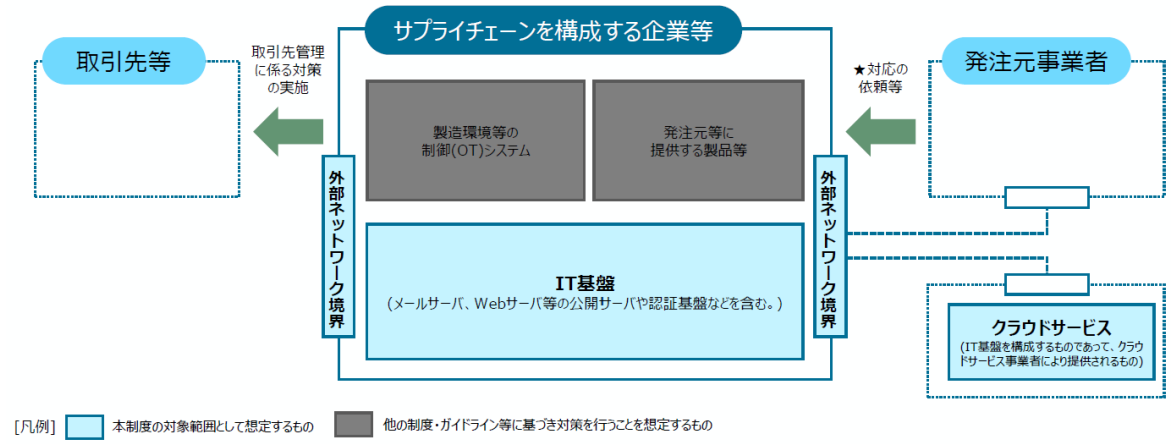
（出所）経済産業省『サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針』を基に大和総研作成

(4) 対象範囲

SCS 評価制度における評価対象は、企業が業務上利用・運用する IT 基盤（情報システム領域）となっています。具体的には、全社で利用されるサーバー群が対象となり、特にインターネットに公開されている Web サーバーやメールサーバーは必ず評価範囲に含めることとされています。加えて、社員が業務で使用する PC やスマートデバイス、クラウドサービスなども評価対象に含まれます。また、インターネット等の外部ネットワークと社内ネットワークの境界に配置されるファイアウォールやルーター、VPN 装置といった機器に加え、他組織の内部システムへ接続する際の境界を構成する機器も、SCS 評価制度における評価対象として位置付けられています。

一方、製造現場における制御システム（OT：Operational Technology）や、企業が提供する製品自体のセキュリティは、想定されるリスクの性質や必要な対策がIT基盤とは異なるため、本制度の評価対象には含まれていません。ただし、これら対象外の領域と IT 基盤の間に接続点やデータ連携、リモート保守経路などが存在する場合は注意が必要です。これらはサイバー攻撃の侵入経路や影響拡大の起点となる可能性があるため、評価対象の IT 基盤との境界を明確にし、その区分を説明可能な状態で整理する必要があります。

図表 7　SCS 評価制度の対象範囲



（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』より抜粋

4. 既存制度・ガイドラインとの関係

SCS 評価制度は、既存のセキュリティ関連制度やガイドラインと競合するものではなく、それらと相互に補完し合う形で設計されています。

例えば、ISO/IEC 27001 に基づく ISMS（情報セキュリティマネジメントシステム）認証は、リスクアセスメントや方針の策定、運用、継続的改善といった一連のマネジメントプロセス全体を重視する、包括的な枠組みです。これに対して SCS 評価制度の★3・★4 では、主要なサイバー脅威や既存の制度を参考に、実効性が高いと考えられる具体的な対策に焦点を当て、各評価レベルにおいて「この水準までは満たすべき」という共通のベースラインを提示する手法が採られています。こうした特徴から、すでに ISMS 認証を取得し、継続的な運用を行っている企業では、SCS 評価制度で求められる要件の多くを、実質的にすでに満たしているケースも十分に考えられます。そのため、SCS 評価制度への対応は、新たな対策の負担を一から追加するというよりも、自社の ISMS 運用状況や対策の実効性を客観的に点検・強化するための契機として位置付けられるでしょう。

また、SCS 評価制度は業界横断的な共通基盤として機能することを目指しており、既存の業種別ガイドラインとの連携や整合性も重視されています。例えば、自動車業界団体（JAMA/JAPIA）が策定した「自工会/部工会・サイバーセキュリティガイドライン」では、取

引先に求める対策レベルを「Lv1」「Lv2」などの形で定義していますが、これらのレベルをSCS 評価制度の★3・★4 に対応付け、双方の基準を一連の取り組みで満たせるよう調整が進められています。

SCS 評価制度では、その他の既存制度・ガイドラインも参照し、それぞれの要求事項との対応関係を整理しています。これにより、企業が複数の制度やガイドラインに個別対応することによる重複や過度な負担を抑えつつ、共通の指標として効率的に活用できる仕組みの構築を図っています。

5. 諸外国の類似制度との比較

サプライチェーン全体のセキュリティ水準を高める取り組みは、日本に限らず、海外でもさまざまな形で進められています。

英国政府が運用する Cyber Essentials 認証制度は、その代表的な例の一つであり、あらゆる組織に推奨される基本的なセキュリティ対策の実装状況を確認・認証する枠組みとして知られています。本制度は、主に自組織の技術的な基礎対策の徹底を目的とした制度であり、サプライチェーンの対策強化を直接対象としているわけではありませんが、基礎的なセキュリティ水準を底上げするという観点では、SCS 評価制度の★3 が想定する水準や方向性と共通しています。このため、★3 の要求事項の設計にあたり、Cyber Essentials 認証制度で整理されている評価基準が多く参照されています。

一方、米国では、国防総省が防衛産業向けに CMMC（Cybersecurity Maturity Model Certification）を導入しています。CMMC は、防衛関連情報を取り扱う企業に対し、情報の重要性に応じて段階的なセキュリティ要件を定め、一定水準以上は第三者による認証取得を義務付ける制度です。契約要件として位置付けられており、国家安全保障を背景に、強い拘束力と高い規律性を有しています。これに対し、SCS 評価制度は特定の業界や契約形態に限定されるものではなく、企業がサプライチェーンにおける自社の役割や取引関係に応じて、任意に活用できる仕組みとして設計されており、企業間取引における説明や合意形成の円滑化に主眼が置かれています。

また、ドイツの自動車業界では、TISAX（Trusted Information Security Assessment Exchange）が業界共通の評価の枠組みとして広く活用されています。TISAX の特徴は、自動車メーカーと取引先企業との間で個別に実施され、重複が生じていたセキュリティ審査を共通化し、一度の評価結果を業界内で共有できる仕組みを整備していることです。これにより、サプライチェーン全体の負担軽減と、セキュリティ対策状況の可視化が実現されています。こうした枠組みは、SCS 評価制度の方向性とも共通していますが、TISAX が自動車産業という特定分野を対象としているのに対し、SCS 評価制度は業界横断で利用可能な基盤の構築を目指している点に違いがあります。

図表 8　SCS 評価制度と諸外国の類似制度の関係

	本制度	Cyber Essentials/ Cyber Essentials Plus	CMMC 2.0	TISAX
制度所管	• 経済産業省/ 内閣官房国家サイバー統括室	• 英国 国家サイバーセキュリティセンター (NCSC)	• 米国 国防総省(DoD)	• ドイツ自動車工業会(VDA)
目的	• **サプライチェーン全体でのセキュリティリスク**(情報漏えい、事業の停止等)**の低減** • 様々な取引先から様々な要求事項を求められる状況下における**基準統一による企業の負担軽減**	• **企業の規模によらず一般的に想定されるサイバー攻撃全般からの組織の保護**	• **国防サプライチェーン全体のサイバーセキュリティ強化** • 管理対象非機密情報(CUI)、連邦契約情報(FCI)の保護	• **自動車業界のサプライチェーンにおけるサイバーセキュリティ強化** • 各自動車メーカー(OEM)等における基準統一による企業の負担軽減
主な対象	• ビジネスサプライチェーンを構成する企業等(物資・役務の調達等) • ITサービスサプライチェーンを構成する企業等(MSP[1]、クラウドサービス等を含む。) *1 Managed Service Provider	• 英国内に拠点を置く全ての企業	• 国防総省から発注を受ける防衛産業基盤(DIB：Defense Industrial Base)企業	• 自動車メーカー(OEM)及びそのサプライヤー等
要件・要求事項	• レベルごと達成すべき「経営の責任」、「サプライチェーンの防御」、「IT基盤の防御」等に資する要求事項を提示	• 「ファイアーウォール」、「セキュアな構成」、「セキュリティアップデート管理」、「ユーザアクセス制御」、「マルウェア対策」の５つのカテゴリで要求事項を提示	• NIST SP800-171等から抽出された要求事項	• ISO/IEC 27001等をベースとした要求事項に加え、「試作品保護」、「データ保護」に係る要求事項
評価スキーム	• ★3:専門家確認付き自己評価 • ★4、★5:第三者評価	• CE：自己診断後、認証機関が回答を評価 • CE+：評価機関による技術検証(CE取得が前提)	• LV1:自己評価 • LV2:取り扱う情報の種類に応じて、第三者評価又は自己評価 • LV3: 防衛産業基盤サイバーセキュリティ評価センター(DIBCAC)による評価(LV2取得が前提)	• 審査機関による審査

（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』より抜粋

こうした各国・各産業の制度やガイドライン等で、広く参照されている汎用的な枠組みとして、米国国立標準技術研究所（NIST）が策定するサイバーセキュリティフレームワーク（NIST CSF）が挙げられます。NIST CSF は、組織の規模や業種を問わず適用可能な汎用フレームワークとして、「ガバナンス」「識別」「防御」「検知」「対応」「復旧」といった主要カテゴリを軸に構成され、セキュリティ基準や認証制度の基盤として活用されています。SCS 評価制度における★3・★4 の要求事項も、NIST CSF の主要カテゴリに「取引先管理」の要素を加えた 7 つの分類で体系的に整理されています。

このように、SCS 評価制度は国際的なセキュリティ基準との整合性を意識して設計されており、国際的な制度動向とも調和を有する制度と言えます。

6.　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、制度の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、SCS 評価制度への対応を支援する新類型が創設される予定です。この新類型では、★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、費用面や実務面の負担を抑えながら、取り組みを進めることが可能となります。新類型のサービスは、今後の実証事業を経たうえで、SCS 評価制度の開始時期にあたる 2026 年度末頃から先行的に提供が開始される見込みです[4]。

[4] 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）」

また、実務面での指針として、IPA から「中小企業の情報セキュリティ対策ガイドライン」[5]が、2026 年 3 月に SCS 評価制度に対応した改訂版として公表されました。本ガイドラインでは、SCS 評価制度の要求事項に対応した具体的な対策例や、規程・ルールのサンプルがまとめられており、中小企業が★3・★4 の取得を目指す際に、何から着手すべきかを判断しやすい実践的な内容となっています。

さらに、専門家による人的な支援体制の整備も進められています。IPA では、情報処理安全確保支援士（通称「登録セキスペ」）の中から、SCS 評価制度への対応支援が可能な人材を整理して「中小企業向けサイバーセキュリティ対策支援者リスト」[6]に追加し、公表することが予定されています。中小企業はこのリストを活用することで、専門家に相談や助言を受けられるほか、★３の取得に必要となる「専門家による確認」を受けることも可能となります。これにより、社内に専門人材を有していない中小企業であっても、外部の専門家を活用しながら、効率的に★３取得に向けたセキュリティ対策を進められる環境が整備されつつあります。

7. 企業はどう向き合うべきか

SCS 評価制度の開始に備え、各企業は自社の置かれた環境に応じて戦略的な準備を進める必要があります。特に、発注側企業と受注側企業では求められる対応の観点が異なるため、それぞれの立場に応じた計画的な対応が重要です。

(1) 発注側企業の対応

まず発注側企業では、自社のビジネスに必要とされるセキュリティ水準を整理したうえで、どの取引や委託関係において★3 または★4 の取得を求めるのかを検討し、その方針を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、現在運用しているセキュリティ関連のチェックシートや評価プロセスについても見直しを行い、SCS 評価制度に準拠した基準へ移行するため、社内ルールの整備や関係部門との連携を進めていくことが求められます。

既存の委託先に対しては、一律に即時対応を求めるのではなく、契約更新のタイミングや取引の重要度を踏まえた移行計画を策定し、必要に応じて一定の移行期間を設けるなど、段階的な対応が望まれます。その際、発注側が一方的に新たな負担を押し付けるのではなく、取引先のセキュリティ対策の向上を主体的に支援するなど、パートナーシップを重視した姿勢が重要です。

経済産業省と公正取引委員会は、SCS 評価制度に基づく対策の実施や★取得を取引先に求める際に、独占禁止法や取適法（旧下請法）上問題とならない考え方や想定事例を整理・提示し

[5] IPA 「中小企業の情報セキュリティ対策ガイドライン」
[6] 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」

ており、発注側企業にはこれらの指針を踏まえた公正で配慮ある運用が求められます[7]。

(2) 受注側企業の対応

一方、受注側企業でも、SCS 評価制度を自社の競争力強化や取引継続につながる取り組みとして前向きに捉え、計画的な対応を進めていくことが重要です。まずは、自社の事業内容や取引形態の特性、取引先から求められるセキュリティ水準を整理し、自社として目指すべき評価レベルを明確にすることが求められます。

そのうえで、SCS 評価制度の要求事項を踏まえ、現在のセキュリティ対策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、運用ルールの整備・見直しを段階的に進めていく必要があります。★3・★4 の具体的な要求事項と評価基準は経済産業省のウェブサイトで公開[8]されているため、まずはこれらを確認し、自社の現状とのギャップを把握しておくことが有効です。

すでに ISMS や業界ガイドライン等に基づくセキュリティ対策に取り組んでいる企業では、これらを土台として SCS 評価制度の要求事項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。

また、中小企業の場合、限られたリソースの中で短期間に全ての要件を満たすことが難しいケースも想定されます。★の取得にあたっては原則全ての要求事項・評価基準への適合が求められるものの、実務上は発注側企業との対話を通じて、自社の対応状況や体制、対応上の制約等についての実態を共有し、段階的な対応への理解を得ながら進めていくことが重要となります。発注側からの要求を待つだけでなく、自社の対応方針や進捗状況を主体的に説明することで、★の取得のみを前提とした過度な要求や認識の齟齬を未然に防ぐことにもつながります。

こうした対応を推進するときは、前章で述べたサイバーセキュリティお助け隊サービス（2026 年度末頃開始予定）や外部企業を活用することも有効な解決策の一つとして挙げられます。

このように、発注側・受注側のいずれの立場でも重要となるのは「早めのスタート」と「段階的な対応の積み上げ」です。制度開始までの時間は限られており、初回の評価取得には一定の準備期間が必要になると考えられます。各企業は余裕を持った計画を立て、段階的に対策を実施・強化していくことが望まれます。

---

[7] 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」

[8] 経済産業省 「別添★3・★4 要求事項及び評価基準（Excel 形式）」

8. 制度普及に向けた論点

SCS 評価制度の実効性は、評価基準そのものに加え、評価実務を担う事業者全体の体制や供給力に大きく依存すると考えられます。特に★4 では、文書審査・実地審査・技術検証（脆弱性検査）といった多段階の評価が必要となるため、相応の専門人材と体制を備えていることが前提となります。

しかし現状では、こうした評価を実施できる事業者は限られているとみられ、制度開始後に評価需要が集中した場合、評価待ちが発生するおそれがあります。また、評価機関の独立性も重要です。制度上、コンサルティングと評価を同一事業者が担うことは必ずしも否定されるものではないとしていますが、その場合には利益相反が生じることも懸念されるため、評価の中立性や公平性をどのように確保するかが問われます。

このように、評価機関の確保と適切な役割分担を含む体制整備は、制度の普及を進めるうえでの課題であり、その整備状況は制度の実効性を左右する要因となり得ます。これらの具体的な運用上の課題や対応の方向性は、今後の制度運用の詳細とあわせて整理が進められるものとみられ、スケジュール上は 2026 年 10 月頃を目途に、より明確になってくることが見込まれます。

9. おわりに

SCS 評価制度は法的な強制力を伴わない任意の制度として位置付けられますが、サプライチェーンにおけるリスクの増大を背景に、その実務上の重要性は今後より一層高まっていくと考えられます。制度が広く浸透すれば、SCS 評価制度に基づく評価の取得状況が、取引先選定や取引判断における前提条件の一つとして扱われるケースが増加することも十分に考えられます。

一方で、前章で述べたとおり、本制度の実効性は評価実務を支える体制の整備状況にも大きく左右されます。評価を担う事業者の供給力や評価の中立性の確保といった課題に適切に対応していくことが、制度の円滑な普及と定着に向けて極めて重要となります。

当社では、これまで培ってきたセキュリティ分野の知見と実務経験を活かし、SCS 評価制度への対応を支援するコンサルティングサービスの提供を開始しています。サービスの詳細は、当社ウェブサイトをご参照ください[9]。

以上

[9] 大和総研 「セキュリティ対策評価制度 コンサルティングサービス」