

中小企業もSCS評価制度対応が必要？取引先から求められる可能性を解説

中小企業であっても、SCS評価制度への対応を早めに検討する価値があります。SCS評価制度（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）は、企業規模によって一律に取得を義務付ける制度ではありません。しかし、発注企業が委託先に対して必要なセキュリティ水準を示し、取引契約などで★の取得を求める使い方が想定されています。つまり、中小企業にとって重要なのは「法律で義務化されるか」だけでなく、「主要取引先の調達・委託条件として求められるか」という視点です。

特に、大企業の業務システムを運用する、個人情報や機密情報を預かる、クラウドサービスを提供する、取引先ネットワークへ接続する、といった企業は影響を受けやすいと考えられます。制度開始は★3・★4ともに2027年3月頃が予定されており、要求事項を満たすための規程整備、資産把握、脆弱性対策、ログ管理、教育、インシデント対応などには一定の準備期間が必要です。取引先から要請を受けてから慌てて始めるより、自社の現状との差分を先に把握しておく方が、予算・人員・優先順位を整理しやすくなります。

出典：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（SCS評価制度）」

<https://www.meti.go.jp/policy/netsecurity/scs.html>

出典：IPA「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）」<https://www.ipa.go.jp/security/scs/index.html>

この記事で分かること

- ・中小企業もSCS評価制度への対応を検討すべき理由
- ・取引先から★3・★4の取得を求められる可能性が高い企業の特徴
- ・★3と★4の違いと、Webアプリケーション診断・プラットフォーム診断・ペネトレーションテストとの関係
- ・取引先から要請される前に進めたい準備と社内稟議の考え方
- ・支援会社を選ぶ際に確認すべきポイント

SCS評価制度とは

SCS評価制度は、サプライチェーンを構成する企業のセキュリティ対策状況を共通の基準で評価・可視化する制度です。経済産業省と内閣官房国家サイバー統括室が制度構築方針を示し、IPAが制度を運営します。制度上は、発注企業が委託先に対して必要な段階（★）を提示し、委託先が必要な対策を実施したうえで、その状況を確認できる仕組みが想定されています。

制度の背景には、発注側と受注側の双方が抱える課題があります。発注側は、委託先のセキュリティ対策が十分かを外部から判断しにくく、独自チェックリストを作成しても水準が適切か判断しづらいという問題があります。一方、受注側は、複数の取引先から異なる質問票や証拠提出を求められ、対応負担が増えやすい状況です。SCS評価制度は、こうした確認を共通化し、サプライチェーン全体の対策水準を引き上げることを目的としています。

対象は、クラウド環境を含む企業等のIT基盤です。一般的にIT基盤に該当しない製造現場のOTシステムや、取引先へ提供する製品そのものは直接の評価対象とはせず、他の制度やガイドラインで対策する整理が示されています。

出典: IPA「SCS評価制度の詳細情報」<https://www.ipa.go.jp/security/scs/details.html>

中小企業もSCS評価制度への対応が必要になるのか

結論として、SCS評価制度は任意制度であり、すべての中小企業に一律の取得義務が課されるわけではありません。経済産業省も、★の取得は取引契約の中で決められるものであり、制度自体が規制を課するものではないと説明しています。

ただし、「任意だから自社には関係ない」と判断するのは早計です。制度では、2社間の取引契約等において発注側が委託先に適切な★を提示する利用が想定されています。したがって、法令上の義務ではなくても、取引先の調達条件、委託先管理基準、更新審査、RFP(提案依頼書)などを通じて対応が求められる可能性があります。

経済産業省とIPAは、中小企業向けに「サイバーセキュリティお助け隊サービス」の新類型を検討しています。これは、中小企業が★3・★4の要求事項へ対応しやすくするための支援策です。公的機関が中小企業向けの取得支援を具体化していることから、中小企業が制度の主要な利用対象として想定されていることが分かります。

出典: 経済産業省「SCS評価制度に係る不適切な勧誘に御注意ください」https://www.meti.go.jp/policy/netsecurity/20260427_scs.html

出典: 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)」https://www.meti.go.jp/policy/netsecurity/otasuketai_jissho.html

なぜ今、中小企業が準備を始めるべきなのか

取引先から要請されてからでは準備期間が不足しやすい

SCS評価制度への対応は、申請書を作成するだけでは完了しません。要求事項に照らして、自社の規程、システム設定、運用記録、教育実績、インシデント対応体制などを確認し、不足があれば改善する必要があります。たとえば、多要素認証の導入、不要アカウントの整理、バックアップ手順の見直し、脆弱性管理の定着、ログの保存・監視、委託先管理、従業員教育などは、社内調整や予算確保を伴うことがあります。

取引更新の1～2か月前に「★取得をお願いします」と言われても、すべての未対応事項を短期間で整えるのは難しい場合があります。制度開始前の段階で現状評価を行い、「すぐ直せるもの」「予算が必要なもの」「契約更新やシステム更改に合わせるもの」に分けておくと、対応が現実的になります。

発注企業は委託先リスクを経営リスクとして見るようになっている

サプライチェーン攻撃では、攻撃者が本命の大企業を直接狙うのではなく、セキュリティ対策が相対的に弱い取引先、保守事業者、クラウド運用会社などを経由して侵入するケースが想定されます。たとえば、委託先の

VPN機器の脆弱性を悪用して侵入し、認証情報を窃取したうえで発注企業の環境へアクセスする、委託先のアカウントを乗っ取って正規メールに見せかけた不正ファイルを送る、といった攻撃です。

このため、発注側にとって委託先の対策不足は「委託先だけの問題」ではありません。情報漏えい、サービス停止、顧客対応、復旧費用、監督当局や取引先への説明など、自社の事業継続や信用に直結します。SCS評価制度は、こうした委託先リスクを共通の物差しで確認するための仕組みとして活用されることが想定されています。

取引先から対応を求められる可能性が高い中小企業

企業規模だけで対象を判断するのではなく、「取引先との接続関係」「扱う情報」「提供サービスの重要度」で考えることが重要です。特に、次のような企業は早めに検討した方がよいでしょう。

- ・大企業や重要インフラ企業の業務を受託している企業
- ・顧客の個人情報、設計情報、営業秘密、認証情報を取り扱う企業
- ・SaaS、クラウド運用、システム開発、保守、ヘルプデスクなどITサービスを提供する企業
- ・取引先のネットワークやクラウド環境へ接続する企業
- ・調達先・再委託先を多数抱え、自社もサプライチェーン管理を求められる企業
- ・IPO、M&A、大口取引開始などを控え、セキュリティ体制を客観的に説明する必要がある企業

一方、上記に当てはまらない場合でも、主要顧客がSCS評価制度を調達基準に取り入れる可能性があります。営業・調達・法務・情報システム部門で主要顧客の契約更新時期やセキュリティ条項を確認し、顧客からの質問票や監査依頼が増えていないかを把握しておく、必要性を判断しやすくなります。

★3と★4は何が違うのか

★3は「一般的なサイバー脅威に対処しうる水準」とされ、取得希望組織による自己評価に、登録されたSCSセキュリティ専門家の確認・助言を加える仕組みです。最終的には経営層による自己適合宣誓を含めてIPAへ提出し、問題がなければ登録・公開されます。

★4は、初期侵入の防御だけではなく、侵入後の被害拡大防止や取引先のデータ・システム保護、サプライチェーン上の役割に応じた強靱化策まで求める水準です。評価機関による第三者評価に加え、文書確認、実地審査、技術検証が行われます。★3を先に取得しなければ★4へ進めない仕組みではありません。

2026年10月4日時点では、★3・★4はいずれも2027年3月頃の運用開始が予定されています。取得には各段階で定められたすべての要求事項・評価基準を満たす必要があります。

出典：IPA「要求事項・評価基準」<https://www.ipa.go.jp/security/scs/requirements-criteria.html>

Webアプリケーション診断・プラットフォーム診断は必要か

特に★4では、評価機関と技術検証事業者による技術検証が想定されており、IPAは技術検証事業者の業務として脆弱性診断を明示しています。実際の検証範囲は、自社が決めた適用範囲や評価対象のサンプリングなどによって変わるため、「SCS評価制度なら必ず同じ診断メニューを実施する」と決めつけることはできません。

ただし、外部公開しているWebシステムがある場合はWebアプリケーション診断、サーバやネットワーク機器が対象となる場合はプラットフォーム診断が候補になります。より高度な侵入経路や権限昇格、横展開まで確認したい場合は、ペネトレーションテストを組み合わせることも考えられます。重要なのは「診断を実施した」という事実ではなく、対象資産のリスクに応じて検証方法を選び、発見した脆弱性を改善し、再確認まで回せることです。

たとえば、インターネット公開サーバで重大な脆弱性が見つかった場合、CVSSなどの技術的な深刻度だけでなく、「顧客データへ到達できるか」「認証を回避できるか」「外部から攻撃可能か」「代替策があるか」といった事業影響を踏まえて優先順位を付ける必要があります。

中小企業が進めるSCS評価制度への対応手順

1. まず取引上の必要性を確認する

主要顧客の契約、セキュリティチェックシート、RFP、委託先管理基準を確認します。営業担当が把握している取引先の方針変更も重要な情報です。「取得要請が既にある」「次回更新で導入されそう」「まだ不明」の3段階程度に分類すると、優先順位を付けやすくなります。

2. 評価対象の範囲を決める

全社を一度に対象にするのではなく、どの事業、拠点、システム、クラウド環境、従業員、委託先までを評価対象とするかを整理します。取引先へ提供するサービスと直接関係するIT基盤から考えると、対象範囲を決めやすくなります。対象を狭くしすぎると取引先の期待と合わず、広げすぎると対応コストが膨らむため、契約関係と情報の流れを踏まえて設定する必要があります。

3. 現状と要求事項のギャップを洗い出す

規程類、資産台帳、アカウント一覧、ネットワーク構成図、クラウド構成、バックアップ手順、ログ管理方針、教育記録、インシデント対応手順、委託先一覧などを準備し、要求事項とのギャップを確認します。ここでは「実施しているが証跡がない」のか、「仕組み自体がない」のかを分けて整理することが重要です。

4. 優先順位を付けて改善計画を作る

未対応項目をすべて同じ優先度で扱う必要はありません。外部から悪用されやすい脆弱性、管理者権限、リモートアクセス、バックアップ、認証、重要データへのアクセス制御など、事業停止や情報漏えいに直結しやすいものから改善します。そのうえで、規程改定、教育、運用記録の整備などを並行して進めます。

5. 申請・評価に向けた証跡を整える

評価では、対策を「やっている」と説明するだけでなく、設定画面、台帳、ログ、議事録、教育履歴、点検記録などで確認できる状態が重要です。日常運用で記録が残る仕組みにしておけば、SCS評価制度だけでなく、取引先監査やISO27001、プライバシーマーク等の説明にも活用しやすくなります。

費用と期間は何で変わるのか

費用は、IPAへ支払う登録料だけでなく、専門家確認、第三者評価、技術検証、改善対応、ツール導入、社内工数などを含めて考える必要があります。IPAが2026年9月18日に公表した料金では、2028年3月31日までの★3登録料は1万円(1年分)、★4登録料は6万円(3年分)です。2028年4月1日以降は★3が2万円(1年分)、★4は6万円(3年分)とされています。これらは制度への登録料であり、外部専門家や評価機関、技術検証、コンサルティング等の費用は別に発生し得ます。

出典:IPA「SCS評価制度 料金設定のお知らせ」(2026年9月18日)
<https://www.ipa.go.jp/security/scs/rcu1hd00000075om-att/pricelist.pdf>

準備期間も企業ごとに異なります。すでにISMS等を運用し、資産管理・アクセス制御・教育・インシデント対応などが整っている企業は比較的短期間でギャップを埋められる可能性があります。一方、規程や資産台帳が未整備、クラウド利用が部門ごとに分散、管理者アカウントを共有している、といった状況では、数か月単位の改善計画が必要になることがあります。

稟議では「SCS評価制度取得費」だけで申請するより、主要顧客との取引継続、セキュリティ監査対応の効率化、事故発生確率と影響の低減、今後の新規営業での説明力向上といった事業上の効果を併せて示すと、経営判断につながりやすくなります。

対応しなかった場合に起こり得る問題

SCS評価制度を取得していないことだけを理由に、直ちに法律上の制裁を受けるわけではありません。しかし、主要顧客が調達条件として★取得を設定した場合は、取引上の影響が生じる可能性があります。たとえば、新規案件の提案条件を満たせない、契約更新時に追加説明を求められる、個別のセキュリティ監査や質問票対応が増える、といったケースです。

また、制度対応を見送った結果として本質的な対策不足が残れば、サイバー攻撃による事業停止、情報漏えい、復旧コスト、顧客への補償や説明、信用低下などのリスクも残ります。SCS評価制度への準備は、マーク取得そのものだけでなく、自社のセキュリティ運用を見直す機会として捉える方が有効です。

支援会社を選ぶときのチェックポイント

SCS評価制度の支援会社を選ぶ際は、チェックリストへの回答代行だけでなく、未達項目を技術面・運用面の双方から改善できるかを確認しましょう。特に、次の観点は見積依頼やRFPで確認しておきたい項目です。

- ・★3・★4の要求事項と最新の制度情報を踏まえて支援できるか
- ・現状評価だけでなく、規程整備、設定変更、運用設計まで支援できるか
- ・Webアプリケーション診断、プラットフォーム診断、ペネトレーションテスト等の技術支援が可能か
- ・発見事項を技術的重大度だけでなく、事業影響と改善コストで優先順位付けできるか
- ・評価時に扱う個人情報・機密情報・構成情報の管理方法が明確か
- ・取得後の再診断、継続監視、教育、インシデント対応体制まで相談できるか

特に★4を視野に入れる場合、文書整備だけではなく技術検証が関係します。コンサルティング会社と診断会社を別々に選ぶと、対象範囲や改善方針の調整に時間がかかる場合があります。支援体制や役割分担を事前に確認し、自社の負担が過度に増えない進め方を選ぶことが重要です。

よくある失敗と注意点

「製品を買えば取得できる」と考える

経済産業省は、評価基準を満たすために特定のセキュリティ製品の導入を必須としていません。EDR、UTM、SIEMなどの製品が役立つ場面はありますが、重要なのは要求事項に対して必要な対策が実施され、運用されていることです。製品導入だけで規程、教育、アカウント管理、インシデント対応が整うわけではありません。

証跡を後からまとめて作ろうとする

評価直前に過去の点検記録や教育記録をまとめて整えようとしても、実運用と一致しない資料になりがちです。日常業務の中で点検・承認・変更履歴が残るようにし、証跡を運用の副産物として生成する設計が望まれます。

取引先の要求水準を確認せず★を決める

自社が★3を取得しても、主要顧客が★4を条件とするなら追加対応が必要です。逆に、現時点で★3で十分な取引先に対して、必要性を確認せず★4を急ぐとコスト過多になる場合があります。営業・経営・情報システムが連携し、取引上の必要水準を確認してから計画を立てることが大切です。

Librus株式会社が提供できるSCS評価制度対応支援

Librus株式会社では、SCS評価制度への対応を「申請書を作る作業」と切り分けず、現状評価から改善、技術検証、運用定着まで一気通貫で支援します。企業ごとの事業内容、取引先との関係、システム構成、既存のセキュリティ施策を確認し、必要な対応を個別に設計します。

たとえば、要求事項とのギャップ分析、評価対象範囲の整理、規程・手順の整備、リスクアセスメント、Webアプリケーション診断、プラットフォーム診断、ペネトレーションテスト、教育・訓練、SOC／CSIRTの構築・運用支援まで、課題に応じて組み合わせることが可能です。診断で問題を指摘するだけでなく、改善の優先順位、実施方法、運用への落とし込みまで支援できる点を重視しています。

また、経営層には取引継続・事業停止・信用毀損といった経営リスクの観点から、情報システム部門には技術・運用の観点から整理し、部門間の認識差を埋めながら進めます。M&A、IPO、取引先監査など、セキュリティの説明責任が高まる局面とあわせた支援にも対応します。

よくある質問

Q1. 中小企業はSCS評価制度の取得が義務ですか？

いいえ。SCS評価制度は任意制度です。ただし、発注企業が取引条件として★取得を求める可能性があります。主要顧客の調達基準や契約条件を確認することが重要です。

Q2. 従業員100名程度でも対象になりますか？

企業規模だけで対象外にはなりません。SCS評価制度はサプライチェーンを構成する企業全体を想定しており、特に中小企業での活用効果が大きいとされています。

Q3. ★3と★4のどちらを目指せばよいですか？

まず主要取引先が求める水準と、自社が扱う情報・サービスの重要度を確認します。一般的な脅威への対策水準を確認する★3と、第三者評価・技術検証を伴う★4では準備負担が異なります。

Q4. ★3を取ってからでないと★4を取得できませんか？

いいえ。IPAは、上位段階が下位段階の要求を包括するものの、★3を事前取得しなければ★4を取得できない関係ではないと説明しています。

Q5. SCS評価制度の開始時期はいつですか？

2026年10月4日時点で、★3・★4は2027年3月頃の運用開始が予定されています。制度情報は更新される可能性があるため、IPAの最新情報を確認してください。

Q6. 取得費用はいくらですか？

IPAの登録料は、2028年3月31日まで★3が1万円(1年分)、★4が6万円(3年分)です。ただし、専門家確認、第三者評価、技術検証、改善対応などの費用は別途発生し得ます。

Q7. 脆弱性診断やペネトレーションテストを必ず実施する必要がありますか？

評価段階や対象範囲によります。特に★4では技術検証が行われますが、具体的な検証対象は適用範囲やサンプリングによって変わります。自社のシステムとリスクに応じて診断方法を設計する必要があります。

Q8. 取引先から何も言われていない場合でも準備した方がよいですか？

大口顧客や重要な委託関係がある場合は、少なくとも現状と要求事項のギャップ確認を先に行うことを推奨します。要請を受けてから不足項目を一度に解消するより、予算とスケジュールを組みやすくなります。

まとめ: 中小企業は「義務か」より「取引で求められるか」を確認する

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)は任意制度であり、中小企業だから一律に取得が義務付けられるものではありません。一方、発注企業が委託先に必要な★を提示し、取引契約の中で取得を求める活用が想定されています。そのため、中小企業にとっては「法令上の義務」よりも「主要取引先との取引継続や新規受注に必要なか」が実務上の重要な判断軸です。

2027年3月頃の制度開始に向けて、まずは取引先の動向と自社の現状を確認し、要求事項とのギャップを可視化することが第一歩です。必要な対策をすべて同時に実施するのではなく、事業影響が大きいリスクから優先順位を付け、予算・人員・システム更改のタイミングに合わせて改善していくことが、無理のない対応につながります。

SCS評価制度への対応方針が未定でもご相談いただけます

「取引先から求められる可能性はあるが、★3と★4のどちらを目指すべきか分からない」「自社のどのシステムまで対象にすべきか判断できない」「規程整備と脆弱性診断をどの順番で進めるべきか」といった段階でもご相談いただけます。Librus株式会社では、現在の体制と取引上の必要性を整理したうえで、過剰な対応を避けながら、優先度の高い施策と実施順序を具体化します。

対象範囲や実施方法が固まっていない場合でも、現状整理から始めることで、社内稟議に必要な論点、概算の進め方、技術検証の要否、改善計画を明確にしやすいです。SCS評価制度への対応を、取引先への説明のためだけでなく、今後の事業継続とセキュリティ運用の強化につなげたい場合は、Librus株式会社までご相談ください。

監修者

鎌田光一郎：青山学院大学法学部卒業。SMBC日興証券株式会社にて証券営業、経営管理業務に従事したのちPwCコンサルティング合同会社に転籍。金融機関に対するコンサルティング業務に従事。その後、Librus株式会社を設立、代表取締役に就任。

お問い合わせ先

Librus株式会社（代表取締役 鎌田光一郎）

105-0004東京都港区新橋6丁目13-12 VORT新橋Ⅱ 4F

03-6772-8015

お問い合わせフォーム：<https://librus.co.jp/contact>