

SCS評価制度とは？2027年開始の新しいセキュリティ評価制度をわかりやすく解説

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、企業間取引で求めるセキュリティ水準を「★」で分かりやすく示し、委託元と委託先の双方が対策状況を確認しやすくするための制度です。★3・★4は2027年3月頃の運用開始が予定されており、IPA（独立行政法人情報処理推進機構）が運営します。

重要なのは、この制度が単なる「認証取得」の話ではない点です。SCS評価制度は任意制度ですが、実際の取引では委託元が委託先に必要な★を示し、その取得や対策水準を取引条件として確認することが想定されています。したがって、特に大手企業のサプライチェーンに入る中堅・中小企業にとっては、営業、調達、事業継続、情報システムの各部門に関わる経営課題として準備する必要があります。

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>

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>

この記事で分かること

- SCS評価制度の目的と、★3・★4の違い
- どのような企業が対応を検討すべきか
- 2027年の制度開始に向けて、経営層と情報システム部門が準備すべきこと
- 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などの技術検証との関係
- 対応期間や費用を左右する要因、支援会社を選ぶ際の実務的なポイント

SCS評価制度とは

SCS評価制度の正式名称は「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」です。2026年3月に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公表し、その方針に基づいてIPAが制度を運営します。

背景には、委託先や取引先を経由したサイバー攻撃の増加があります。発注企業にとっては「取引先がどの程度の対策をしているか分かりにくい」、受注企業にとっては「取引先ごとに異なるセキュリティチェックシートへの回答負担が大きい」という双方の課題があります。SCS評価制度は、必要な対策水準を共通の段階で表し、サプライチェーン全体のセキュリティ水準を高めることを狙っています。

制度上は、2社間の取引契約などで委託元が委託先に適切な段階（★）を提示し、必要な対策を促したうえで、その実施状況を確認する使い方が想定されています。対象は特定業種だけに限定されておらず、IPAは「全てのサプライチェーン企業が対象」と説明しています。

★3と★4は何が違うのか

2027年3月頃に運用開始が予定されている中心的な段階は★3と★4です。★3は、一般的なサイバー脅威に対処し得る水準を想定しています。★4は、侵入防止だけではなく、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までを求める、より高い水準です。

区分	評価の考え方	主な評価方法
★3	一般的なサイバー脅威に対処し得る水準	取得希望組織による自己評価＋SCSセキュリティ専門家による確認・助言
★4	被害拡大防止や取引先保護、サプライチェーン強靱化まで含む水準	評価機関による第三者評価＋実地審査＋技術検証
★5	より高度な攻撃への対応を想定	今後、要求事項・評価基準や評価スキームを具体化

なお、★4を取得する前に★3を取得しておく必要はありません。上位段階は下位段階の要求を包含する考え方ですが、取得手順として★3→★4が必須という制度ではありません。

SCS評価制度は義務なのか

結論から言えば、SCS評価制度そのものは任意制度です。経済産業省は、★3や★4の取得を法令上義務付ける制度ではなく、取引契約において委託元と委託先の間で取得要否が決められるものと説明しています。

一方で、任意であることと「事業上の影響がない」ことは別です。委託元が調達基準や取引先管理の中で一定の★を求める場合、受注企業にとっては実質的な商談要件になる可能性があります。大手企業との新規取引、既存取引の更新、重要システムの委託、機密情報を扱う業務などでは、早めに自社の現状を確認しておく意味があります。

なぜ今、企業にSCS評価制度への準備が必要なのか

★3・★4の運用開始は2027年3月頃が予定されています。2026年4月には★3・★4の要求事項・評価基準が公開され、2026年8月には基本規程なども公開されました。制度の輪郭はすでに具体化しており、運用開始直前になって初めて対策を始めるより、現時点でギャップを把握し、予算・人員・技術対策を計画しておく方が現実的です。

特に従業員100～1,000名規模の企業では、情報システム部門が少人数で運用している一方、取引先監査、クラウド管理、端末管理、脆弱性対応、インシデント対応、教育などが分散しているケースが少なくありません。SCS評価制度への対応は、単に申請書を作る作業ではなく、組織・規程・運用・技術対策が実態として整っているかを確認するプロジェクトとして捉える必要があります。

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

出典:IPA「制度規程・委員会」 <https://www.ipa.go.jp/security/scs/regulation-advisory-committeess.html>

経営層が判断すべき3つの事項

第一に、自社がサプライチェーンの中でどのような役割を担っているかです。顧客の機密情報を扱うのか、顧客システムへ接続するのか、自社サービス停止が顧客事業に影響するのかによって、求められる対策水準は変わります。

第二に、SCS評価制度への対応を「情報システム部門だけの課題」にしないことです。契約、調達、営業、経営企画、総務、人事などが関与するため、責任者と意思決定ルートを明確にする必要があります。

第三に、制度対応を取引維持のコストとしてだけでなく、顧客への説明力を高める投資として評価することです。セキュリティ対策の内容を共通の評価軸で説明できれば、取引先監査や新規商談における説明負担の軽減につながる可能性があります。

対応しなかった場合に起こり得る問題

SCS評価制度に対応しないこと自体に法的な罰則があるわけではありません。しかし、委託元が取引条件として一定の★や同等水準の対策を求める場合には、商談の遅延、追加監査、改善要求、契約条件の見直しなどにつながる可能性があります。

また、制度対応の有無とは別に、サプライチェーン攻撃によって委託先から認証情報が窃取され、顧客環境へ不正アクセスされるケースや、脆弱な公開サーバーを起点にランサムウェア被害が拡大するケースは、事業継続や信用に直結します。SCS評価制度への準備を機に、対策の「有無」だけでなく、実際に機能するかを確認することが重要です。

例えば、規程上は「脆弱性管理を実施する」と書かれていても、インターネット公開資産の棚卸しができていなければ、診断対象から漏れたシステムが攻撃の入口になる可能性があります。同様に、バックアップを取得していても、復旧テストをしていなければ、インシデント時に事業を予定どおり再開できるとは限りません。

SCS評価制度への対応を優先して検討したい企業・場面

特に優先度が高いのは、大手企業や重要インフラ関連企業のサプライチェーンに参加している企業、顧客の機密情報・個人情報を扱う企業、顧客ネットワークやクラウド環境へ接続する企業、SaaS・システム開発・運用保守などを提供する企業です。

また、M&A、IPO、重要な業務提携、新規大型取引の開始といった経営上の重要局面でも、セキュリティ体制を外部に説明できる状態が求められます。SCS評価制度への対応準備は、こうした場面で必要になる証跡、規程、資産台帳、脆弱性管理記録、インシデント対応体制の整備にもつながります。

SCS評価制度への具体的な対応手順

制度対応は、最初から申請書を埋めるのではなく、対象範囲と現状を整理し、要求事項との差分を把握してから改善するのが効率的です。以下は、実務上取り組みやすい進め方です。

1. 対象範囲と目指す段階を決める

まず、どの法人・拠点・部門・システム・業務を評価対象にするかを整理します。取引先から具体的な要求がある場合は、その契約や委託業務との関係を確認します。要求がまだない場合でも、主要顧客の業種、取り扱う情報、システム接続の有無、サービス停止時の影響を踏まえ、★3または★4のどちらを目標にするか検討します。

2. 必要資料を集める

現状確認では、情報セキュリティ基本方針、各種規程、組織図、資産台帳、ネットワーク構成図、アカウント管理ルール、クラウド利用台帳、委託先一覧、脆弱性対応記録、教育記録、インシデント対応手順、バックアップ・復旧手順などを確認します。資料が存在するだけでなく、実際の運用と一致しているかが重要です。

3. 要求事項とのギャップ分析を行う

IPAが公開している★3・★4の要求事項・評価基準に照らし、「適合」「一部適合」「未対応」「対象外」を整理します。未対応項目は、取引先への影響、攻撃可能性、改善難易度、必要予算などを加味して優先順位を付けます。

4. 技術面の実効性を確認する

文書・規程だけでなく、実際のシステムに弱点がないかを確認します。Webサービスを提供している企業ではWebアプリケーション診断、サーバーやネットワーク機器にはプラットフォーム診断が有効です。さらに、実際の攻撃者の視点で侵入可能性や侵入後の影響を確認したい場合は、ペネトレーションテストを組み合わせます。

★4では第三者評価に加えて技術検証が求められます。そのため、運用開始直前に初めて脆弱性を確認するのではなく、事前に主要システムの弱点を洗い出し、改修と再確認まで済ませておくことが合理的です。なお、どの技術検証が制度上の正式な評価に該当するかは、IPAが定める評価機関・技術検証事業者の仕組みと最新ルールに従う必要があります。

5. 規程・運用・技術対策を改善する

ギャップ分析の結果に応じて、アクセス権管理、ログ管理、脆弱性管理、バックアップ、インシデント対応、委託先管理、教育などを改善します。ここで重要なのは、ルールを増やすことではなく、担当者、実施頻度、承認者、証跡の残し方まで運用可能な形にすることです。

6. 自己評価・第三者評価に備える

★3では、取得希望組織が自己評価を作成し、SCSセキュリティ専門家による確認・助言を受け、経営層による自己適合宣誓を含めて申請する流れが示されています。★4では、評価機関による第三者評価と技術検証を経た後に登録申請を行います。★3・★4とも、すべての要求事項・評価基準を満たす必要があるとIPAは案内しています。

出典:IPA「よくある質問」 <https://www.ipa.go.jp/security/scs/faq.html>

対応期間と費用を左右する要因

SCS評価制度の申請・登録費用は、2026年9月時点では今後公開予定です。そのため、現時点で一律の金額を断定することはできません。一方、企業側が準備に必要とする期間や支援費用は、自社の現状によって大きく変わります。

実務上、期間を左右しやすいのは、対象範囲の広さ、既存規程の整備状況、資産台帳の精度、クラウドや拠点の数、脆弱性診断の対象数、改修の必要量、委託先管理の複雑さ、社内承認に要する期間です。特に、診断で重大な脆弱性が見つかった場合は、改修・テスト・再診断までを計画に含める必要があります。

目安としては、すでにISMS等の管理基盤があり運用証跡も揃っている企業と、規程・資産管理・技術対策をゼロから整備する企業では、準備工数が大きく異なります。制度開始に合わせて取得を目指す場合は、

まず短期間のギャップ分析を行い、その結果をもとに社内スケジュールと予算を確定する方法が現実的です。

出典:IPA「よくある質問」 <https://www.ipa.go.jp/security/scs/faq.html>

社内稟議で説明しておきたい内容

稟議では、「制度対応が必要だから」という説明だけでなく、主要取引先との関係、対象業務、現状のリスク、求める★、不足している対策、対応しない場合の事業影響、必要予算、完了予定時期をセットで示す意思決定しやすくなります。

特に経営層には、セキュリティ施策をITコストとしてではなく、取引継続、顧客信用、サービス停止リスク、事故対応費用を含めた経営リスクの低減として説明することが重要です。

SCS評価制度の支援会社を選ぶ際のポイント

支援会社を選ぶ際は、制度文書の解説ができるだけでは不十分です。実際のギャップを埋めるには、規程整備、リスクアセスメント、脆弱性診断、ペネトレーションテスト、インシデント対応、教育など複数領域の実務能力が必要になるためです。

RFPや見積依頼では、①SCS要求事項とのギャップ分析の方法、②対象範囲の決め方、③技術検証の実施可否、④発見事項の優先順位付け、⑤規程や運用設計まで支援できるか、⑥改善後の再確認方法、⑦機密情報の取り扱い、⑧成果物の内容、⑨制度改定時のフォロー方針を確認するとよいでしょう。

また、★3の正式な確認を依頼する場合はSCSセキュリティ専門家としての登録要件、★4の正式評価や技術検証についてはIPAの指定・登録制度に基づく評価機関・技術検証事業者であるかを確認する必要があります。制度上の役割と、取得準備のコンサルティング支援は分けて考えることが大切です。

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

よくある失敗と注意点

よくある失敗の一つは、要求事項をチェックリストとして埋めること自体が目的になってしまうことです。形式上「実施済み」と回答できても、実運用が伴わなければ、事故時に機能しません。規程、設定、ログ、教育記録などの証跡と、実際の現場運用を一致させる必要があります。

二つ目は、対象範囲を曖昧なまま進めることです。どの拠点・システム・サービスを対象にするかが曖昧だと、診断や資産棚卸しに漏れが生じ、後から追加作業が発生します。

三つ目は、技術対策を最後に回すことです。脆弱性診断やペネトレーションテストで重要な問題が見つかり、改修には開発部門やベンダー調整が必要です。申請直前では間に合わない可能性があるため、早い段階で技術的な現状確認を行う方が安全です。

四つ目は、情報システム部門だけで対応することです。SCS評価制度は取引先管理、教育、契約、インシデント対応など部門横断の取り組みです。経営層を含めた責任分担を明確にして進めることが重要です。

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、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）への対応を、制度要件の確認だけで終わらせず、実際のリスク低減まで一気通貫で支援します。

具体的には、現状ヒアリング、対象範囲の整理、要求事項とのギャップ分析、リスクアセスメント、情報セキュリティ体制・規程の整備、運用プロセスの設計、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、SOC／CSIRT構築・運用支援、インシデントレスポンス、デジタルフォレンジック、セキュリティ教育・訓練などを、企業ごとの環境に応じて組み合わせることが可能です。

SCS評価制度への対応では、「どこまでを対象にすべきか」「★3と★4のどちらを目指すべきか」「規程はあるが技術対策が十分か分からない」といった初期段階の整理が重要です。Librusでは、技術面と経営面の双方から課題を整理し、経営層、情報システム部門、現場部門の間にある認識差を埋めながら、実行可能な改善計画へ落とし込みます。

また、診断で問題を発見して終わるのではなく、改善の優先順位付け、改修後の再診断、継続監視、教育、インシデント対応体制まで含めた支援が可能です。M&A、IPO、取引先監査など、期限と説明責任が伴う局面にも対応します。

SCS評価制度に関するよくある質問

Q1. SCS評価制度はいつ始まりますか？

IPAは★3・★4について、2027年3月頃の運用開始を予定しています。ただし、制度運営基盤の整備状況などにより変更される可能性があるため、最新情報はIPA・経済産業省の公式情報で確認する必要があります。

Q2. SCS評価制度への対応は義務ですか？

制度自体は任意です。法令で一律に★の取得を義務付けるものではありません。ただし、取引先が契約や調達条件として一定の★を求める可能性はあります。

Q3. 中小企業も対象ですか？

はい。IPAは全てのサプライチェーン企業を対象としています。特に、対策リソースが限られる中小企業では、共通の評価軸を活用する効果が大きいと説明しています。

Q4. ★3と★4のどちらを目指すべきですか？

顧客からの要求がある場合はそれを起点に検討します。要求がない場合は、扱う情報の重要度、顧客システムへの接続、サービス停止時の影響、サプライチェーン上の役割などから判断します。

Q5. ★3を取得してからでないと★4は取得できませんか？

いいえ。IPAは、★3を事前に取得していなければ★4を取得できないという関係ではないとしています。

Q6. ISMSを取得していればSCS評価制度への対応は不要ですか？

一律に不要とはいえません。既存の管理体制や証跡を活用できる可能性はありますが、SCS評価制度固有の要求事項・評価基準との適合状況を個別に確認する必要があります。

Q7. 脆弱性診断やペネトレーションテストは必要ですか？

対象とする★やシステム、要求事項への対応状況によって異なります。★4では技術検証が制度上の評価プロセスに含まれます。取得準備の段階でも、公開システムや重要システムの弱点を把握するために診断を実施することは有効です。

Q8. 申請費用はいくらですか？

2026年9月時点で、★3・★4の申請・登録にかかる費用は今後公開予定です。コンサルティング、診断、改修など取得準備の費用は、自社の対象範囲と現状によって変動します。

Q9. 何から始めればよいですか？

まず、主要取引先との関係と対象業務を整理し、IPAの要求事項・評価基準を使って現状とのギャップを把握することをおすすめします。その後、優先度の高い改善項目から計画化します。

出典：IPA「よくある質問」 <https://www.ipa.go.jp/security/scs/faq.html>

まとめ：SCS評価制度は「申請」より前の準備が重要

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、企業間取引におけるセキュリティ水準を共通の段階で示し、サプライチェーン全体の対策を底上げするための制度です。★3・★4は2027年3月頃の運用開始が予定されています。

制度自体は任意ですが、取引先が求めるセキュリティ水準として利用されることが想定されています。そのため、対応の可否を「法的義務があるか」だけで判断するのではなく、主要顧客との取引、扱う情報、事業継続への影響、自社の営業戦略まで含めて判断することが重要です。

実務では、対象範囲の整理、ギャップ分析、規程・運用の改善、Webアプリケーション診断やプラットフォーム診断、必要に応じたペネトレーションテストなどを早めに進めることで、制度開始後の申請や取引先からの要求に対応しやすくなります。

SCS評価制度への対応方針が固まっていない段階でもご相談いただけます

Librus株式会社では、「自社がSCS評価制度の対象になるのか分からない」「★3と★4のどちらを目指すべきか判断したい」「現在の規程やセキュリティ対策でどこまで対応できるか確認したい」といった初期段階からご相談いただけます。

現在の体制や取引先との関係を整理したうえで、必要な対象範囲、優先して改善すべき項目、技術検証の要否、社内で準備すべき資料や進め方を具体化します。対象範囲や実施方法が決まっていなくても、現状をもとに対応の全体像を整理できるため、社内稟議や予算化に向けた検討材料としても活用いただけます。

SCS評価制度への対応を、単なる制度対応ではなく、取引先への説明力向上と実効性のあるセキュリティ体制づくりにつなげたい企業は、Librus株式会社までご相談ください。

主な公的情報

出典:IPA「SCS評価制度」 <https://www.ipa.go.jp/security/scs/index.html>

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

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

出典:IPA「よくある質問」 <https://www.ipa.go.jp/security/scs/faq.html>

出典:経済産業省「SCS評価制度」 <https://www.meti.go.jp/policy/netsecurity/scs.html>

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>