

SCS評価制度★4とは？第三者評価・技術検証の仕組みを解説

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）の★4は、自己申告だけで対策状況を示す制度ではありません。評価機関による第三者評価に加え、脆弱性診断などの技術検証を受け、その結果を踏まえて登録を目指す仕組みです。★3よりも、取引先のデータやシステムを守るための対策が実際に機能しているかを客観的に確認する点が重視されます。

2026年10月4日時点では、★3・★4は2027年3月頃の運用開始が予定されています。評価機関・技術検証事業者の指定手続は始まっている一方、取得希望企業向けの申請方法や一部の運用詳細は今後公表予定です。そのため、★4を検討する企業は制度開始を待つのではなく、適用範囲の整理、規程・証跡の整備、脆弱性診断、改善計画の策定までを先行して進めることが重要です。

この記事で分かること

- ・SCS評価制度★4と★3の違い
- ・★4における第三者評価と技術検証の役割
- ・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
- ・★4取得を見据えて企業が準備すべき資料、体制、技術対策
- ・評価機関・支援会社を選ぶ際の実務上のチェックポイント

SCS評価制度★4とは

SCS評価制度は、企業のサイバーセキュリティ対策を共通の基準で評価し、その結果を取引先などが確認しやすくするための制度です。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公表し、独立行政法人情報処理推進機構（IPA）が制度を運営します。

★4は、一般的なサイバー脅威への対処を主眼とする★3よりも一段高い水準です。IPAは、★4について「初期侵入の防御にとどまらず、内外への被害拡大防止・目的遂行のリスク低減によって取引先のデータやシステム保護に寄与すること」や、「サプライチェーンにおける自社の役割に適合した強靱化策」が講じられている水準と説明しています。

重要なのは、★4では書類上の整備だけでなく、第三者評価と技術検証が求められることです。規程が存在していても、実際のシステムに重大な脆弱性が残っている、運用手順が現場で機能していない、委託先管理が形骸化しているといった状態では、評価対応が難しくなる可能性があります。

出典：[IPA「SCS評価制度の詳細情報」](#)

★3を取得してからでなければ★4を取得できないわけではない

★4を目指す場合、先に★3を取得することが必須だと誤解されることがあります。しかしIPAは、上位段階が下位段階の要求を包括する一方で、★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明示しています。自社の取引要件や重要情報の取扱い、顧客から求められる保証水準によっては、最初から★4を目標に準備する選択肢もあります。

SCS評価制度★4で求められる「第三者評価」とは

★4の第三者評価では、IPAから指定を受けた評価機関が、取得希望組織の対策状況を客観的に確認します。2026年9月に公開された指定申請情報では、評価機関の業務として、文書確認・実地審査・技術検証を含む第三者評価を行い、評価報告書を交付することが示されています。

文書確認では「規程があるか」だけでなく運用証跡が重要になる

企業側で準備すべきものは、情報セキュリティ基本方針や各種規程だけではありません。アクセス権限の棚卸し記録、脆弱性対応履歴、バックアップ・復旧試験の記録、インシデント対応訓練の記録、委託先評価資料、教育実施記録など、「定めたルールを継続的に運用していること」を示す証跡が重要です。

たとえば、退職者のアカウントを削除する規程があっても、実際のアカウント棚卸し記録がなく、長期間利用されていない特権IDが残っていれば、統制が実効的に機能しているとは説明しにくくなります。規程と現場運用を一致させることが、★4準備の基本です。

実地審査では適用範囲の中からサンプリングされる想定

IPAは、★4では文書確認に加えて実地審査と技術検証を行い、取得希望組織が決定した適用範囲の中から対象をサンプリングして評価することを想定しています。したがって、一部の部署やシステムだけを評価直前に整えるのではなく、適用範囲全体で一定水準の運用を定着させておく必要があります。

特に従業員100～1,000名規模の企業では、本社の情報システム部門と事業部門、拠点、子会社、外部委託先でルールや管理方法が異なることがあります。評価対象を決める段階で、どこまでを同一の統制で説明できるのかを整理しておく、その後の準備が進めやすくなります。

SCS評価制度★4の「技術検証」とは

★4の大きな特徴が技術検証です。IPAの2026年度指定申請情報では、技術検証事業者は、評価機関から委託を受けて「技術検証（脆弱性診断）」を実施し、その結果報告書を評価機関へ交付する役割とされています。また、技術検証事業者の主な対象として、脆弱性診断やペネトレーションテストを提供する法人が示されています。

つまり、★4では「対策を実施していると説明できること」に加えて、システムの弱点が実際に残っていないかを技術的に確かめる工程が組み込まれます。これにより、書面上は対策済みでも、設定ミスや古いソフトウェア、認証設計の不備などが残っている状態を発見しやすくなります。

出典：[IPA「指定申請について（評価機関・技術検証事業者・研修事業者向け）」](#)

Webアプリケーション診断

Webアプリケーション診断は、Webサイトや業務システムのアプリケーション部分に存在する脆弱性を確認する診断です。認証・認可の不備、入力値検証の不足、セッション管理の問題などを確認します。顧客向けポータル、ECサイト、取引先向けシステム、クラウド上の業務アプリケーションなど、インターネットから利用できるサービスを持つ企業では重要な確認領域になります。

プラットフォーム診断

プラットフォーム診断は、サーバー、ネットワーク機器、OS、ミドルウェアなどの設定や既知の脆弱性を確認する診断です。不要なポートの公開、古いソフトウェア、危険な暗号設定、管理画面の露出などは、攻撃者の初期侵入につながる可能性があります。

ペネトレーションテストとの違い

ペネトレーションテスト(侵入試験)は、単に脆弱性を列挙するだけでなく、攻撃者の視点で複数の弱点を組み合わせ、どこまで侵入・権限拡大・重要情報への到達が可能かを検証する手法です。★4の技術検証がすべての企業に対して一律にペネトレーションテストを要求するという意味ではありません。具体的な対象や方法は、最新の制度文書、評価機関の指示、適用範囲、システムのリスクに沿って判断する必要があります。

実務では、Webアプリケーション診断やプラットフォーム診断で広く弱点を把握し、重要システムや高リスク領域では必要に応じてペネトレーションテストを組み合わせる考え方が有効です。制度対応のためだけに診断を行うのではなく、事業停止や情報漏えいにつながる経路を実際に減らすことが本来の目的です。

なぜ★4では技術検証まで求められるのか

サプライチェーン攻撃では、標的となる大企業を直接狙うのではなく、取引先や委託先を経由して侵入するケースがあります。取引先のシステムに侵入された結果、認証情報や接続経路が悪用されれば、自社だけでなく顧客や上流企業にも影響が波及する可能性があります。

そのため、重要な機密情報を扱う企業や、事業停止がサプライチェーン全体に波及し得る企業では、「規程を整備している」という説明だけでは十分な保証にならない場合があります。第三者評価と技術検証を組み合わせることで、ガバナンスと実システムの両面から対策状況を確認できる点が★4の特徴です。

出典：[経済産業省「SCS評価制度の構築方針」](#)

★4を取得しない場合に想定される事業上の課題

SCS評価制度は、2026年10月時点で、すべての企業に一律に★4取得を義務付ける制度として公表されているわけではありません。ただし、制度が普及すれば、発注企業が取引先選定や継続評価の際に★の取得状況を参照する場面が増える可能性があります。

特に、機密情報を受託する企業、基幹業務を担うIT事業者、製造ラインや物流など事業停止の影響が大きい企業では、取引先から高い保証水準を求められることがあります。未取得だから直ちに取引停止になると断定することはできませんが、セキュリティ質問票や個別監査への対応負荷、競争入札での説明力、顧客とのリスクコミュニケーションに影響する可能性は考慮すべきです。

SCS評価制度★4の対象をどう決めるか

★4準備で最初難しくなるのが適用範囲です。会社全体、特定事業、特定拠点、特定サービスなど、どこを対象とするかによって必要な資料、診断対象、費用、期間が大きく変わります。

経営層が判断すべきこと

経営層は、どの取引・事業・情報資産を守るために★4を取得するのかを明確にする必要があります。主要顧客から求められる可能性、売上に占める重要取引の比率、事業停止時の損失、機密情報の重要度、今後の新規取引や入札への影響などを踏まえ、取得の目的と優先順位を決めます。

情報システム部門が整理すべきこと

情報システム部門は、対象となるネットワーク、クラウド環境、Webアプリケーション、端末、ID管理基盤、外部公開資産、委託先との接続、バックアップ環境などを洗い出します。資産台帳と実態が一致していない場合、技術検証の対象漏れや、想定外の公開資産が見つかる原因になります。

★4取得に向けた具体的な準備手順

1. 要求事項・評価基準とのギャップを確認する

まず、IPAが公開している★3・★4の要求事項・評価基準を基に、自社の現状とのギャップを洗い出します。ここでは「規程がある・ない」だけで判断せず、責任者、実施頻度、対象範囲、証跡、例外管理まで確認します。

出典：[IPA「要求事項・評価基準」](#)

2. 適用範囲と重要資産を確定する

次に、評価対象となる組織、拠点、システム、サービス、委託先を整理します。対象範囲を広げれば説明力は高まりますが、審査・診断・改善の負荷も増えます。一方、狭すぎる範囲では、顧客が期待する事業やサービスをカバーできない可能性があります。営業部門や事業責任者も交え、取引上意味のある範囲を設定することが重要です。

3. 規程と運用証跡を整備する

情報セキュリティ規程、アカウント管理、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、教育などのルールを確認し、運用記録を残します。過去の証跡が不足している場合は、無理に取り繕うのではなく、現時点から運用を開始し、改善計画と実施記録を積み上げる方が実務的です。

4. 技術診断を先行実施し、重大な問題を改善する

評価直前に初めて脆弱性診断を行うと、重大な問題が見つかった際に改修期間を確保できません。制度対応とは別に、準備段階でWebアプリケーション診断やプラットフォーム診断を実施し、重大度の高い問題から改善しておくことが有効です。

優先順位は、脆弱性の深刻度だけでなく、インターネットから悪用可能か、機密情報や管理者権限に到達できるか、代替対策があるか、事業停止につながるかといった観点で決めます。技術的なスコアが同じでも、対象システムの重要度によって対応順序は変わります。

5. 模擬審査と是正確認を行う

評価機関への依頼前に、要求事項ごとに「何を提示すれば説明できるか」を確認します。責任者へのヒアリング、証跡の確認、サンプルとなる端末やアカウントの確認などを模擬的に行うと、規程と現場運用のずれを発見しやすくなります。

実施期間と費用を左右する要因

2026年10月4日時点で、★4取得企業が負担する申請・登録費用の詳細はIPAから今後公開予定とされています。また、第三者評価や技術検証の費用は、評価機関・技術検証事業者の料金体系や対象範囲によって変わるため、一律の金額を示すことはできません。

実務上、費用と期間を左右しやすいのは、対象拠点数、システム数、外部公開資産数、Webアプリケーションの画面・機能数、クラウド環境の複雑さ、委託先数、既存規程や証跡の整備状況、診断で発見された問題の改修量です。海外拠点や複数子会社を含める場合は、追加の調整期間も見込む必要があります。

制度開始後すぐに取得したい企業ほど、評価機関が公表されてから準備を始めるのではなく、今の段階でギャップ分析と改善を進めておく方がスケジュールを組みやすくなります。IPAは評価機関を2026年12月末頃から公表予定としています。

出典：[IPA「SCSセキュリティ専門家・評価機関」](#)

社内稟議で説明すべきポイント

SCS評価制度対応を単なる「認証取得費」として稟議に上げると、費用対効果が伝わりにくいことがあります。経営層には、主要顧客との取引維持・新規取引の要件、個別監査や質問票対応の効率化、インシデント発生時の事業停止リスク、サイバー保険やBCPとの関係など、事業上の目的を整理して説明することが重要です。

また、取得そのものだけでなく、事前診断、改修、規程整備、運用定着、再診断までを一つのプロジェクトとして予算化した方が現実的です。評価で不適合が見つかったから追加予算を申請すると、取得スケジュールが遅れる可能性があります。

評価機関・支援会社を選ぶ際のチェックポイント

★4の正式な第三者評価は、IPAから指定された評価機関に依頼する必要があります。評価機関が自ら技術検証も実施する場合と、別の指定技術検証事業者へ委託する場合があります。したがって、正式評価を依頼する際は、IPAの指定機関台帳で最新の指定状況を確認することが前提です。

一方、取得前のギャップ分析、規程整備、脆弱性診断、改善支援などは、正式評価とは役割が異なります。支援会社を選ぶ際は、要求事項の解釈だけでなく、Webアプリケーション、ネットワーク、クラウド、ID管理、インシデント対応まで技術面を理解しているかを確認するとよいでしょう。

RFPや見積依頼では、対象範囲、成果物、診断手法、再診断の有無、報告会、機密情報の取扱い、データ保管期間、再委託の有無、発見事項の優先順位付け方法を明確にします。「SCS対応一式」という依頼だけでは、各社の作業範囲が揃わず、見積比較が難しくなります。

SCS評価制度★4でよくある失敗と注意点

評価直前に規程だけを作る

規程を短期間で作成しても、実際の運用記録がなければ、第三者評価で説明が難しくなります。ルールを決めた後に、棚卸し、レビュー、訓練、教育などを実際に回し、証跡を残す期間を確保してください。

脆弱性診断を「報告書をもらう作業」にしてしまう

診断の目的は報告書を保管することではなく、攻撃につながる弱点を減らすことです。発見事項について、担当者、期限、暫定対策、恒久対策、再診断結果まで追跡する管理プロセスが必要です。

情報システム部門だけで進める

★4では、委託先管理、教育、事業継続、経営判断など、情報システム部門だけでは完結しない項目が含まれます。経営層、法務・総務、人事、営業、事業部門、購買部門などを巻き込み、役割分担を決めることが重要です。

正式評価と事前コンサルティングの役割を混同する

取得支援と正式な第三者評価は区別して考える必要があります。特に同一法人が複数の役割を担う場合は、中立性・公平性など制度上の要件を確認しなければなりません。依頼前に、誰が正式評価を行い、誰が改善支援を行うのかを明確にしておくことが重要です。

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、SCS評価制度の取得を見据えた現状整理から、技術対策、改善、運用まで一気通貫で支援します。制度文書の読み合わせだけでなく、企業ごとの事業構造、取引先から求められる水準、既存のセキュリティ体制、システム構成を踏まえて対応範囲を設計します。

具体的には、要求事項・評価基準に対するギャップ分析、規程・運用プロセスの整備、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、インシデント対応体制、SOC／CSIRT、教育・訓練、委託先管理などを組み合わせて支援できます。

★4対応では、経営・統制面の整備と技術検証を分断しないことが重要です。たとえば、診断で重大な脆弱性が見つかった場合、単に技術部門へ改修を依頼するだけでなく、脆弱性管理規程、責任者、対応期限、例外承認、再診断までの運用に落とし込む必要があります。Librusでは、診断結果を改善計画と継続運用につなげるところまで支援します。

なお、SCS評価制度における正式な★4第三者評価は、制度上指定された評価機関が実施するものです。支援を検討する際は、最新の制度要件と役割分担を確認しながら進めることが重要です。

SCS評価制度★4に関するよくある質問

Q1. SCS評価制度★4はいつから始まりますか？

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。2026年10月4日時点では、評価機関・技術検証事業者の指定手続が進行中です。

Q2. ★3を取得していないと★4を取得できませんか？

いいえ。IPAは、★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。自社の取引要件やリスクに応じて★4から目指すことも可能です。

Q3. ★4では第三者評価が必須ですか？

はい。★4は、指定された評価機関による第三者評価と技術検証を組み合わせるスキームです。文書確認だけでなく、実地審査や技術検証が行われる想定です。

Q4. 技術検証とは何をするのですか？

IPAの指定申請情報では、技術検証事業者の業務として脆弱性診断が示されています。具体的な対象・方法は、適用範囲や最新の制度文書、評価機関の指示に沿って決まります。

Q5. Webアプリケーション診断は必要ですか？

対象範囲にWebアプリケーションが含まれ、リスク上確認が必要と判断される場合は重要な検証手段になります。ただし、すべての企業・システムに同一の診断が一律に求められると断定することはできません。

Q6. ペネトレーションテストも必須ですか？

2026年10月4日時点の公表情報から、全企業に一律でペネトレーションテストが必須とは言えません。一方、技術検証事業者の対象にはペネトレーションテスト提供法人も含まれており、高リスク領域では有効な検証手法になり得ます。

Q7. 既に実施した脆弱性診断の報告書を使えますか？

既存診断結果の扱いは、診断時期、対象範囲、手法、実施事業者、最新の制度要件などによって判断が必要です。評価対応を前提にする場合は、正式評価を依頼する評価機関や最新ガイドを確認してください。

Q8. 準備はいつから始めるべきですか？

2027年の制度開始を待たず、ギャップ分析、資産棚卸し、規程整備、技術診断、改善を先行して進めることを推奨します。重大な問題ほど改修や社内調整に時間がかかるためです。

まとめ | SCS評価制度★4は「書類」と「技術」の両面で準備する

SCS評価制度★4は、第三者評価と技術検証によって、企業のセキュリティ対策が実際に機能しているかを客観的に確認する仕組みです。★3と比べて、被害拡大の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重視します。

取得を目指す企業は、要求事項への回答を作ることだけに集中するのではなく、適用範囲の確定、規程と運用証跡の整備、Webアプリケーション診断・プラットフォーム診断などの技術検証、発見事項の改善、再確認までを一つのプロジェクトとして進めることが重要です。

2026年10月4日時点では、取得希望企業向けの申請方法や申請・登録費用など、今後公表される情報も残っています。未確定情報を推測で補うのではなく、IPA・経済産業省の最新公表内容を確認しながら、現時点で確実に進められる基盤整備から着手することが現実的です。

SCS評価制度★4の準備段階からご相談いただけます

「★4を目指すべきか判断できていない」「どのシステムまで対象にすべきか分からない」「規程はあるが技術面に不安がある」「診断と制度対応を別々に進めると負荷が高い」といった段階でも、Librus株式会社へご相談いただけます。

現状の体制や取引先から求められる水準を整理したうえで、ギャップ分析、対象範囲の設計、技術診断、改善計画、運用定着まで、必要な範囲から支援します。制度対応を目的化せず、取引継続や事業継続に実際に役立つ対策へ落とし込むことで、社内稟議や経営層への説明もしやすくなります。対象範囲や実施方法がまだ決まっていない場合も、検討材料の整理から対応可能です。

制度情報の確認日：2026年10月4日

主な公的情報：

[IPA SCS評価制度](#)

[IPA SCS評価制度の詳細情報](#)

[IPA よくある質問](#)

[IPA 要求事項・評価基準](#)

[経済産業省 SCS評価制度の構築方針](#)

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>