SCS取得までのロードマップ｜準備から登録までの全工程

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を、適用範囲の決定、自己評価、改善、専門家確認・第三者評価、登録まで時系列で解説します。

SCS評価制度の取得は、申請書を整えるだけの作業ではありません。最初に「どの組織・拠点・業務・情報システムを評価対象にするか」を決め、要求事項ごとに証拠を集め、不足を改善し、★3では登録されたセキュリティ専門家の確認、★4では指定評価機関による第三者評価と技術検証を経て、事務局へ登録を申請する流れです。

実務上の成否を分けるのは、評価直前の対症療法ではなく、適用範囲と責任者を早期に確定し、規程・設定・運用記録が一致する状態をつくることです。本稿では、従業員100〜1,000名程度の企業を想定し、経営判断、社内稟議、情報システム部門の準備、Webアプリケーション診断やプラットフォーム診断、ペネトレーションテストの位置付けまで説明します。

この記事で分かること

この記事を読むと、SCS評価制度の★3と★4の違い、自社に適した段階の考え方、準備から登録までの順序、各工程で必要になる資料、期間と費用を左右する要因、外部支援会社を選ぶ際の確認点が分かります。なお、IPAは★3・★4を2027年3月頃に運用開始する予定とし、申請方法や取得ガイドは2026年10月頃、申請・登録費用は今後公開予定と案内しています。以下のロードマップには、公表済みの制度要件と、企業が先行して進められる実務準備を区別して記載します。

出典：IPA「SCS評価制度の詳細情報」「よくある質問」制度詳細／FAQ

SCS評価制度とは——★3と★4の違い

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、取引関係にある企業のセキュリティ対策を共通の「★」で可視化し、委託元と委託先の双方が適切な対策水準を判断しやすくする制度です。経済産業省と内閣官房国家サイバー統括室の監督のもと、IPAが運営します。

★3は、一般的なサイバー脅威に対処し得る水準です。取得希望組織が自己評価し、SCS評価制度に登録されたセキュリティ専門家が内容を確認・助言して署名します。最後に経営層が自己適合宣誓を行い、事務局へ提出します。

★4は、初期侵入の防御だけでなく、侵入後の被害拡大防止、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靭化までを求める水準です。指定評価機関による第三者評価と、

指定技術検証事業者による技術検証が必要です。★3を先に取得しなければ★4を申請できない仕組みではありませんが、★4は★3以下の要求を包括します。

したがって、取引先から最低限の共通水準を求められる企業では★3が出発点になりやすく、重要情報や基幹業務を預かる受託事業者、広範な接続権限を持つIT事業者、事業停止時の波及が大きい企業では★4を検討する余地があります。最終判断は、取引先要求、扱う情報、接続形態、停止時の影響、投資可能額を合わせて行います。

なぜ今、取得準備が必要なのか

SCS評価制度は、単なる情報システム部門の認証対応ではなく、取引継続と受注競争力に関わる経営課題になり得ます。発注者は、委託先ごとに異なる質問票を作り続けるより、共通評価を利用する方が確認負担を抑えやすくなります。委託先にとっても、複数顧客へ同じ説明を繰り返す負担を減らせる可能性があります。

一方、準備を後回しにすると、重要案件の入札や更新時に短期間で証拠提出を求められ、場当たり的な規程作成や高額な緊急対応につながります。さらに、ランサムウェアによる操業停止、委託先アカウントを踏み台にした侵入、Webアプリケーションの脆弱性を起点とする情報漏えいが起きれば、復旧費だけでなく、代替調達、顧客説明、契約上の責任、信用毀損まで影響が広がります。

今から着手すべき理由は、制度開始まで待たずとも、資産台帳、アカウント管理、バックアップ、ログ、インシデント対応、委託先管理などの基礎整備は無駄になりにくいからです。正式な様式が公開された後に差分を調整できるよう、証拠を残す運用を先行させることが合理的です。

対象となる企業・システム・場面

SCS評価制度は、特定業種だけを対象とする制度ではありません。特に検討優先度が高いのは、大手企業や公共分野のサプライチェーンに参加する企業、顧客データや設計情報を扱う企業、クラウド運用・システム保守・BPOを受託する企業、工場や物流を止めると取引先へ影響が波及する企業です。従業員100〜1,000名規模では、複数拠点、子会社、SaaS、オンプレミス、外部委託が混在し、管理主体が曖昧になりやすいため、適用範囲の設計が重要です。

対象は「会社全体」と決め打ちする必要はありません。ただし、都合の悪いシステムだけを除外すると、事業や情報の流れと評価範囲が矛盾します。顧客へ提供するサービス、扱う重要情報、利用する端末・ネットワーク・クラウド、運用する部門と委託先を一本の業務フローとして捉え、境界と除外理由を説明できる状態にします。

SCS取得までのロードマップ——準備から登録まで

工程0：経営方針と目標段階を決める

最初に経営層が決めるのは、取得目的、目標段階、責任者、予算、期限です。「顧客から求められたから」だけでなく、どの取引の維持・拡大に効くのか、停止するとどの事業に損失が出るのかを明確にします。CISOや情報システム責任者だけに任せず、事業部門、法務、総務、人事、購買、内部監査を含む横断体制にすると、規程と現場運用の乖離を減らせます。

社内稟議では、制度の概要、対象取引、目標段階、適用範囲案、現状とのギャップ、概算費用、必要な社内工数、未対応時の受注・事業継続リスクを示します。制度の申請費用が未公表である点は、外部支援費・製品導入費・評価費と分け、「確定後に追加稟議」として扱うのが安全です。

工程1：適用範囲を決定する

適用範囲は、組織図だけでは決められません。対象サービス、顧客、契約、拠点、従業員、端末、ネットワーク、クラウド、アプリケーション、データ、委託先を関連付けます。たとえば顧客向けWebサービスを対象にするなら、公開Webアプリケーションだけでなく、認証基盤、運用端末、ソースコード管理、監視、バックアップ、保守委託先まで確認対象に含み得ます。

この段階で作るべき資料は、適用範囲記述書、組織図、業務フロー、ネットワーク構成図、システム・資産台帳、データフロー、クラウド／SaaS一覧、委託先一覧、責任分担表です。除外項目には「関係がない」という結論だけでなく、情報や接続が分離されている根拠を残します。

工程2：要求事項に沿って自己評価する

次に、★3または★4の要求事項・評価基準ごとに、適合・不適合・確認中を判定します。重要なのは、規程の存在だけで適合としないことです。たとえばアカウント棚卸しを年1回行う規程があっても、実施記録がなければ運用実態を説明できません。判定欄には、根拠資料名、保管場所、対象範囲、責任者、最終実施日を紐付けます。

確認資料には、情報セキュリティ方針、リスクアセスメント、アクセス権限一覧、パッチ適用記録、バックアップ・復元試験記録、ログ監視記録、教育・訓練記録、インシデント対応手順、BCP、委託先契約・評価記録などが含まれます。個人情報や機密情報を外部専門家・評価機関へ提示する場合は、秘密保持契約、閲覧権限、保存期間、返却・削除方法、再委託条件を事前に合意します。

工程3：ギャップを優先順位付けし、改善する

不適合を一律に処理すると、予算と人員が足りなくなります。優先順位は、①取得上の必須性、②攻撃される可能性、③影響の大きさ、④短期で実施できるか、⑤他の対策への波及効果で付けます。インターネット公開資産の重大な脆弱性、多要素認証がない特権アカウント、復元できるか未確認のバックアップ、連絡網のないインシデント対応は、一般に優先度が高い項目です。

改善は「製品導入」で終わりません。責任者、手順、例外承認、記録様式、確認頻度まで決め、一定期間の運用証跡を残します。経営層には、件数ではなく、重大リスクの残存状況、期限超過、追加予算、受注・停止リスクへの影響を報告します。

工程4：必要な技術検証を行う

★4では文書確認と実地審査に加え、技術検証が求められます。具体的な対象は適用範囲とリスクに応じて設計されます。公開Webサービスには Webアプリケーション診断、サーバー・ネットワーク機器・クラウド基盤にはプラットフォーム診断が候補です。重要システムでは、攻撃者の視点で侵入可能性と到達範囲を確かめるペネトレーションテストが有効な場合があります。

脆弱性診断は既知の弱点を広く確認する手法、ペネトレーションテストは複数の弱点や設定を組み合わせ、現実にどこまで侵入・権限拡大できるかを検証する手法です。目的が異なるため、名称だけで選ばず、評価基準、資産の重要度、停止許容度に合わせます。実施前には対象IP・URL、環境、本番影響、禁止行為、実施時間、緊急連絡先、取得データの扱いを合意してください。

工程5：★3の専門家確認、または★4の第三者評価を受ける

★3では、自己評価結果をSCS評価制度の登録セキュリティ専門家が確認し、必要に応じて修正助言を行います。専門家が最終提出内容を了承した場合に署名し、経営層が自己適合宣誓を行います。支援を受けたコンサルタントが、そのまま制度上の確認者になれるとは限りません。登録要件と独立性の扱いを確認する必要があります。

★4では、取得希望組織が指定評価機関へ検証・評価を依頼し、文書、実地、技術面の確認を受けます。評価機関から評価報告書が提供された後、取得希望組織が事務局へ登録を申請します。評価機関や技術検証事業者は公表された指定先から選定し、事前支援と正式評価の役割分担、利害関係、再評価条件を契約前に確認します。

工程6：是正、経営層の承認、登録申請を行う

確認・評価で指摘が出た場合は、原因、影響範囲、暫定措置、恒久措置、担当者、期限、再確認方法を是正計画にまとめます。単に設定を変更するだけでなく、同種システムへの横展開と手順改訂まで行うことが重要です。

★3は、専門家署名を含む自己評価結果と経営層の自己適合宣誓を事務局へ提出します。★4は、評価機関の評価報告書を踏まえて登録を申請します。事務局は申請内容に問題がなければ台帳へ登録し、公表します。申請様式、提出方法、費用は最新のIPA公表資料で確認してください。

工程7：登録後の運用を定着させる

登録はゴールではありません。人事異動、システム更改、M&A、クラウド移行、新規委託先の追加で、評価時の状態は変わります。少なくとも、資産台帳と権限の定期見直し、脆弱性管理、バックアップ復元試験、インシデント対応訓練、委託先評価、経営報告を年間計画に組み込みます。重大な構成変更や新サービス開始時には、臨時のリスク評価と再診断を行います。

実施期間と費用を左右する要因

準備期間は一律ではありません。公的制度としての標準所要期間が公表されていない段階で、確定的な月数を示すのは適切ではありません。実務上は、限定された範囲で管理が整っている企業ほど短く、複数拠点・子会社・レガシーシステム・多数の委託先を含む企業ほど長くなります。正式評価の予約や是正期間も考慮し、取引先の期限から逆算して余裕を持たせます。

費用を左右する主な要因は、目標段階、適用範囲の広さ、拠点数、対象システム数、現状の成熟度、規程整備の量、技術検証の深さ、診断対象数、現地訪問、再評価の回数です。見積りでは、①現状評価、②改善支援、③製品・設定変更、④脆弱性診断等、⑤制度上の専門家確認または第三者評価、⑥申請・登録費用を分けると、比較しやすくなります。

支援会社・評価機関の選び方

支援会社には、SCSの要求事項を説明する力だけでなく、技術・規程・運用・経営報告をつなぐ実装力が必要です。RFPや見積依頼では、対象段階、適用範囲案、対象拠点・システム、希望時期、既存認証、成果物、会議頻度、機密情報の扱いを提示します。

確認すべき成果物は、適用範囲記述書、要求事項別ギャップ一覧、証拠台帳、改善ロードマップ、規程・手順案、技術検証報告書、是正管理表、経営報告資料です。さらに、担当者の資格・経験、診断とコンサルティングの連携、再診断条件、報告書の具体性、緊急時の対応力を確認します。★3

の制度上の専門家確認、★4の正式な第三者評価については、IPAに登録・指定された主体かを必ず確認してください。

よくある失敗と注意点

適用範囲を狭くしすぎる

評価負担を減らすために範囲を狭めても、対象事業と認証基盤や運用端末がつながっていれば、説明が成立しません。最初にデータと接続の流れを可視化し、境界を技術的・契約的に裏付けます。

規程だけを短期間で作る

テンプレートを整えても、アクセス権限の棚卸しや復元試験の記録がなければ、実施を証明できません。評価日から逆算して、運用記録が蓄積される期間を確保します。

診断を一度行えば十分と考える

診断は重要ですが、対象外資産、認証後の攻撃経路、運用ミス、委託先管理、初動対応までは自動的に解決しません。診断結果をリスク台帳と改善計画へ戻し、再診断と継続監視につなげます。

正式評価と取得支援を混同する

取得準備の支援者と、制度上の確認者・評価機関は役割が異なります。利益相反や独立性に関する制度規程、契約上の責任分界を確認し、誰が何を保証するのかを明文化します。

Librus株式会社が提供できる支援

Librus株式会社は、SCS評価制度への対応を、チェックリスト記入だけで終わらせず、適用範囲の設計、ギャップ分析、規程・体制整備、改善実装、技術検証、運用定着まで一気通貫で支援します。経営層には取引・財務・事業継続の観点で判断材料を整理し、情報システム部門には実装可能な優先順位と証拠管理の仕組みを提示します。

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、インシデントレスポンス、デジタルフォレンジック、教育・訓練を組み合わせられるため、評価で見つかった課題を別々の会社へ引き継ぐ負担を抑えられます。大企業から中堅・中小企業まで、既存のISMS、顧客監査、M&A、IPO準備との重複も整理し、各社の環境に合わせたロードマップを設計します。

なお、正式な★3確認や★4評価が必要な場面では、制度上の登録・指定状況と独立性要件を確認したうえで、適切な役割分担をご案内します。

SCS評価制度についてよくある質問

SCS評価制度はいつ始まりますか？

IPAは、★3・★4を2027年3月頃に運用開始する予定と公表しています。申請方法は2026年10月頃に公開予定です。最新情報はIPA公式サイトで確認してください。

★3を取らないと★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。ただし、★4は下位段階の要求を包括します。

★3は自己評価だけで取得できますか？

自己評価だけではなく、登録セキュリティ専門家の確認・助言と署名、経営層による自己適合宣誓、事務局への提出が必要です。

★4では何が行われますか？

指定評価機関による文書確認・実地審査と、指定技術検証事業者による技術検証が行われます。その後、評価報告書を踏まえて事務局へ登録申請します。

Webアプリケーション診断は必ず必要ですか？

一律に必須と断定できません。適用範囲、評価段階、対象システムとリスクに応じて、技術検証の内容を設計します。公開Webサービスが重要資産であれば有力な検証手段です。

取得準備では何から始めるべきですか？

取得目的と目標段階を決め、対象サービス・拠点・システム・データ・委託先を含む適用範囲を整理します。その後、要求事項別の自己評価と証拠収集へ進みます。

申請・登録費用はいくらですか？

2026年9月4日時点で、IPAは今後公開予定としています。準備支援、製品導入、診断、正式評価、申請・登録を分けて予算化してください。

ISMSを取得済みでも追加対応は必要ですか？

既存の規程や監査記録を活用できる可能性はありますが、SCSの適用範囲と全要求事項への適合を別途確認する必要があります。認証保有だけで自動的にSCS登録となるわけではありません。

まとめ——SCS評価制度は「範囲・証拠・改善」の順で進める

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）の取得準備は、目標段階を決め、適用範囲を定義し、要求事項に沿って自己評価し、不足を改善することから始まります。★3は専門家確認付き自己評価、★4は第三者評価と技術検証を経て、事務局への登録申請へ進みます。

最も重要なのは、評価書類と実際の運用を一致させることです。資産、権限、バックアップ、ログ、インシデント対応、委託先管理の記録を継続的に残せる体制を整えれば、SCS対応は取引先説明のためだけでなく、自社の事業継続力を高める活動になります。

SCS取得準備を、対象範囲の整理から相談したい企業へ

「★3と★4のどちらを目指すべきか」「どの拠点やシステムを含めるべきか」「顧客監査やISMSの資料をどこまで流用できるか」が未確定でもご相談いただけます。Librus株式会社では、初期ヒアリングと現状資料の確認を通じて、優先課題、必要な技術検証、社内体制、予算化の考え方を整理します。早い段階で論点を可視化することで、不要な製品導入や評価直前の手戻りを抑え、現実的な取得計画を立てやすくなります。

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
https://librus.co.jp/contact/

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。

主な公的情報・一次情報

経済産業省「SCS評価制度に関する制度構築方針」
IPA「SCS評価制度」公式サイト

IPA「SCS評価制度の詳細情報」

IPA「要求事項・評価基準」

IPA「よくある質問」

IPA「制度規程・委員会」