SCS評価制度★4取得実務｜第三者評価・技術検証の備え方

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取得では、規程を整えるだけでは足りません。評価機関による第三者評価に加え、実地審査と技術検証を通じて、定めた対策が現場とシステムで実際に機能していることを示す必要があります。準備の要点は、①適用範囲を経営判断として確定する、②要求事項と証跡を対応付ける、③サンプリングされても説明できる運用を全社に定着させる、④Webアプリケーション診断やプラットフォーム診断等を是正・再確認まで完結させる、の4点です。

本稿は2026年9月4日時点の公表情報を基にしています。IPAによれば、★3・★4は2027年3月頃の運用開始予定です。申請方法、解説書、取得ガイド、申請・登録費用など、公表前または更新予定の事項があります。実際の申請時には必ず最新版の制度文書をご確認ください。

この記事で分かること

★4の評価スキーム、実地審査で確認され得る内容、サンプリングへの備え、技術検証の対象範囲、指摘後の是正対応を一連の実務として理解できます。また、従業員100〜1,000名規模の企業が、どの部署を巻き込み、どの資料を揃え、どのように予算とスケジュールを組むべきかを整理します。

SCS評価制度と★4の位置付け

SCS評価制度は、委託元が委託先の対策状況を把握しにくいこと、委託先が取引先ごとに異なる質問票へ回答する負担が大きいことを背景として、サプライチェーンに必要な対策水準を段階別に示す制度です。IPAは、取引契約等において委託元が委託先に適切な段階を提示し、その実施状況を確認する利用場面を想定しています。制度の対象はサプライチェーンを構成する企業全般です。

★4は、一般的なサイバー脅威への対処を水準とする★3より一段深く、初期侵入後の被害拡大防止、攻撃目的の遂行リスク低減、取引先データ・システムの保護、自社の役割に応じたサプライチェーン強靭化を求める水準です。★3を先に取得しなければ★4を申請できない、という順序関係ではありません。

★4は「書類審査＋現場確認＋技術的な確認」

IPAの公表スキームでは、取得希望組織が自己評価を行い、指定された評価機関に検証・評価を依頼します。評価機関は第三者評価を行い、技術検証は評価機関自身または委託を受けた指定技術検証事業者が実施します。評価報告書を受領後、取得希望組織が事務局へ登録申請し、問題がなければ台帳に

登録・公開されます。★4では文書確認だけでなく実地審査と技術検証が行われ、適用範囲内から対象をサンプリングする想定です。

なぜ今、★4取得の準備が必要なのか

制度開始後に要求事項を読み始めても、日々の運用実績は短期間では作れません。アクセス権の棚卸し、脆弱性対応、バックアップ復旧試験、教育、インシデント訓練などは、規程の制定日ではなく実施記録によって有効性を説明します。取引先から取得予定や対応状況を尋ねられたとき、ギャップ、責任者、改善期限、予算を示せる状態にしておくことが重要です。

経営上も、★4対応は単なる認証費用ではありません。取引継続条件、入札・調達要件、秘密情報の取扱条件に影響する可能性があり、対応の遅れは営業機会の損失や個別監査の増加につながり得ます。他方、制度マークだけを目的に過剰投資をすると、維持できない仕組みが残ります。守るべき取引、情報、サービス停止時の損失を起点に優先順位を決めるべきです。

対応しなかった場合に起こり得る問題

第一は、取引先への説明力の低下です。委託元から対策水準を求められた際、計画も証跡もなければ、追加質問票、個別監査、契約条件の厳格化を招く可能性があります。第二は、攻撃を受けた際の被害拡大です。例えば、VPN機器の未修正脆弱性から侵入され、共通の管理者権限を使ってファイルサーバやバックアップ領域まで暗号化されるケースでは、境界防御だけでは事業停止を抑えられません。

第三は、委託先を経由した信用毀損です。開発環境の認証情報が漏えいし、顧客環境への接続に悪用されれば、自社の復旧費用だけでなく、顧客調査、契約上の報告、損害対応が発生します。★4の準備では、こうした連鎖を想定し、権限分離、ログ監視、インシデント対応、再委託先管理を一つの仕組みとして確認します。

対象範囲はどう決めるか

適用範囲は「審査を通りやすい最小範囲」ではなく、取引先へ約束したい業務と、その業務を支える人・拠点・システム・委託先から逆算します。たとえば顧客向けSaaSを対象とするなら、本番環境だけでなく、開発・保守端末、ソースコード管理、ID基盤、監視、バックアップ、クラウド運用、外部委託を含めるべきかを判断します。除外する対象には、業務上の依存関係がないかを確認し、理由を文書化します。

経営層が決める事項

経営層は、対象とする事業・契約、許容する停止時間と情報漏えいリスク、改善投資の上限、責任役員を決めます。情報システム部門だけに任せると、営業が締結した顧客契約、開発部門の例外運用、総務が管理する入退室、購買部門の再委託先管理が評価範囲から漏れやすくなります。

情報システム部門が準備する事項

情報システム部門は、ネットワーク構成図、資産台帳、アカウント・権限一覧、脆弱性管理台帳、ログ管理方針、バックアップ構成、インシデント対応手順を現状と一致させます。台帳上は廃止済みでも実機が稼働している、退職者アカウントが残っている、規程とクラウド設定が異なる、といった差異は技術検証で表面化しやすい点です。

★4取得に向けた具体的な実施手順

1. 経営目的と適用範囲を確定する

まず、主要顧客から求められる水準、売上への影響、守る情報、重要サービスを整理します。適用範囲記述書には、法人・部門、拠点、業務、システム、ネットワーク、クラウド、委託・再委託、除外理由を記載します。評価中に範囲が変わると、証跡収集や技術検証のやり直しが生じるため、経営会議等で合意を得ておくことが有効です。

2. 要求事項と現状のギャップを評価する

IPAが公開する★3・★4要求事項・評価基準を基準に、適合、部分適合、不適合、対象外を判定します。自己評価の点数を埋めることよりも、判定根拠を一行で説明できることが重要です。各項目に、統制責任者、規程、実施手順、証跡、対象システム、残課題、是正期限を紐付けます。IPA FAQでは、★4取得には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るとされています。

3. 規程と実運用を一致させる

規程は現場で守れる粒度にします。「定期的に確認する」では、頻度、実施者、承認者、記録先が分かりません。「四半期ごとにシステム責任者が特権IDを棚卸しし、部門長が承認、結果をチケットに保存する」まで具体化すると、運用と証跡が結び付きます。既存のISMS文書があっても、対象範囲や実態が異なる場合は流用だけで済ませないことが肝要です。

4. 証跡パッケージを作る

実施前には、組織図、責任分担表、適用範囲、情報資産・システム台帳、ネットワーク図、リスクアセスメント、各種規程、教育記録、アクセスレビュー、パッチ適用記録、脆弱性診断報告書、インシデント訓練・復旧試験結果、委託先評価、例外承認記録などを準備します。文書名を並べるだけでなく、要求事項ごとに参照ページと証跡保管場所を示す索引を用意すると、評価対応を効率化できます。

5. 実地審査とサンプリングに備える

実地審査では、責任者へのインタビュー、管理画面や設定の確認、記録の突合、拠点の物理的対策の確認などが想定されます。サンプリングは、適用範囲内の一部の拠点、端末、アカウント、変更記録、教育記録等を選んで運用状況を確かめる考え方です。どのサンプルが選ばれるかを予測して一部だけ整えるのではなく、母集団を明確にし、同じ手順が全件に適用されていることを示します。

有効な事前演習は、評価者役が無作為に「直近3件の入社者」「管理者ID5件」「重大パッチ3件」「委託先2社」などを選び、申請内容、承認、設定、記録が一貫しているかを追跡することです。説明担当者だけでなく、実際の運用担当者が自分の業務を説明できる状態を目指します。

6. 技術検証を実施する

技術検証の具体的方法と範囲は、最新の制度文書および評価機関との調整に従う必要があります。実務上は、インターネット公開資産、Webアプリケーション、サーバ・ネットワーク機器、クラウド設定、端末、認証・権限、ネットワーク分離、ログ等について、要求事項への適合を裏付ける検証計画を作ります。無断で本番環境を試験せず、対象、時間帯、試験元IP、禁止事項、停止判断、連絡網、データ取扱いを事前合意します。

Webアプリケーション診断は、SQLインジェクション、認証・認可不備、セッション管理、設定不備等を確認します。プラットフォーム診断は、OS、ミドルウェア、ネットワーク機器の既知脆弱性や不要サービス、暗号・設定の問題を確認します。ペネトレーションテストは、複数の弱点を組み合わせて重要資産へ到達できるかを、合意したシナリオと安全管理の下で検証するものです。自動スキャンだけでは、権限設計や業務ロジック、侵入後の横展開まで十分に確認できない場合があります。

7. 指摘を是正し、再確認する

指摘はCVSS等の技術的深刻度だけでなく、悪用可能性、公開範囲、保有情報、権限、事業停止影響、代替統制を合わせて優先順位付けします。重大な認証回避や外部公開機器の既知脆弱性は迅速に封じ込め、恒久対応へ移行します。一方、直ちに改修できない基幹システムは、アクセス制限、監視強化、ネットワーク分離などの代替策を経営が期限付きで承認します。

是正管理票には、指摘、根本原因、影響範囲、暫定対応、恒久対応、責任者、期限、完了証跡、残余リスク、再確認結果を残します。設定変更の画面だけでなく、同種資産への横展開確認と、運用手順の修正まで完了させることが再発防止につながります。

成果物・報告書に含めるべき内容

社内準備の成果物には、適用範囲記述書、要求事項別ギャップ一覧、証跡索引、技術検証計画、診断報告書、是正管理票、経営報告資料を含めます。診断報告書には、対象・除外、実施日時、手法、制約、発見事項、再現条件、影響、リスク評価、推奨対策を記載し、経営向け要約と技術担当者向け詳細を分けると活用しやすくなります。

経営報告では、未解決件数だけでなく、重要事業への影響、必要投資、期限、リスク受容の要否を示します。評価報告書を取得すること自体ではなく、その後も統制を維持できる責任分担と予算を承認することが経営層の役割です。

期間と費用を左右する要因

IPAが示す申請・登録費用は2026年9月4日時点で公表待ちです。したがって、総費用は「制度上の申請・登録費用」と「評価機関・技術検証の費用」と「不足対策の改修費」を分けて見積もる必要があります。期間も一律ではなく、適用範囲、拠点数、システム数、クラウド数、文書整備度、既存認証の活用可否、技術検証の深さ、重大指摘の件数、繁忙期や変更凍結期間で変わります。

準備計画は、短期間の書類作成ではなく、予備診断、是正、運用実績の蓄積、模擬審査、本評価を逆算して組みます。予算稟議では、取得目的、対象取引、適用範囲、制度関連費、診断費、改修予備費、社内工数、取得後の維持費を分けて示すと、追加費用の理由を説明しやすくなります。

評価・支援ベンダーの選び方

評価機関と技術検証事業者は、制度上の指定状況を必ず確認します。取得支援を依頼する場合は、制度要求の解釈だけでなく、Web、プラットフォーム、クラウド、認証基盤の技術検証から是正支援、運用設計まで対応できるかが重要です。第三者評価とコンサルティングを同一法人が行う場合の中立性・公平性要件は制度文書で確認し、役割分離を契約と体制図で明確にします。

RFP・見積依頼で確認したい項目

見積依頼では、対象組織・拠点・システム、希望時期、既存認証、技術検証の対象と方式、報告書言語、再診断回数、出張、緊急連絡、機密情報の保管・削除、再委託、賠償・責任分界を明記します。価格だけでなく、前提条件と除外事項、追加費用が発生する条件を比較してください。診断データに

は構成情報、アカウント、脆弱性など機密性の高い情報が含まれるため、暗号化、アクセス制御、保管地域、保持期間、廃棄証明も確認します。

よくある失敗と注意点

よくある失敗は、①申請直前に規程だけ作る、②適用範囲と資産台帳が一致しない、③一部の模範的な拠点・端末だけ整える、④自動スキャン結果を技術検証の全てと考える、⑤診断指摘を修正したが再確認しない、⑥情報システム部門だけで対応する、⑦制度上の確定事項と支援会社の推奨事項を混同する、というものです。

また、診断のために本番データを複製した結果、管理外の環境へ個人情報が残る事態も避けなければなりません。テストデータの匿名化、最小権限の試験アカウント、ログ取得、データ削除の確認を計画に含めます。制度文書は更新されるため、申請時点の版番号と参照日も証跡に残してください。

Librus株式会社が提供できる支援

Librus株式会社は、SCS評価制度の要求事項整理から適用範囲設計、ギャップ分析、規程・運用整備、証跡作成、模擬審査、技術検証に向けた準備、是正計画、継続運用まで一気通貫で支援します。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、レッドチーム演習、SOC／CSIRT構築、インシデントレスポンス、教育を組み合わせ、企業ごとの事業・IT環境・予算に合わせて設計します。

特徴は、診断結果を渡して終わらず、経営リスクと技術課題を接続し、改善の実行と運用定着まで伴走する点です。経営層には取引・事業継続・投資判断の言葉で、情報システム部門には設定・手順・証跡の言葉で、現場部門には日常業務の変更点として説明し、社内の橋渡しを行います。

よくある質問

Q1. ★3を取得してからでないと★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事項を包括するものの、★3の事前取得を★4取得の条件とはしていません。自社の取引要件とリスクに応じて選択します。

Q2. ★4は自己評価だけで取得できますか。

できません。★4は評価機関による第三者評価と技術検証が必要で、文書確認に加えて実地審査が行われる想定です。

Q3. サンプリング対策として何をすべきですか。

母集団を明確にし、全件に同じ統制が適用されている状態を作ります。アカウント、端末、拠点、変更記録等を無作為に選ぶ模擬確認が有効です。

Q4. 脆弱性診断とペネトレーションテストは同じですか。

目的が異なります。脆弱性診断は個々の弱点を網羅的に確認するのに適し、ペネトレーションテストは弱点を組み合わせて重要資産へ到達できるかを攻撃シナリオに沿って確認します。必要性は対象とリスクに基づいて決めます。

Q5. 既にISMSを取得していれば準備は不要ですか。

既存の管理体系や証跡は活用できますが、自動的に★4適合になるわけではありません。SCS評価制度の要求事項、適用範囲、技術検証に照らした差分確認が必要です。

Q6. 申請費用はいくらですか。

2026年9月4日時点で、IPAは★3・★4の申請・登録費用を今後公開予定としています。評価、技術検証、改修等の費用は別に見込み、範囲を明確にして見積もります。

Q7. 準備にはどれくらいかかりますか。

一律の期間はありません。対象規模、現状の成熟度、技術的な不備、運用記録の有無に左右されます。制度開始や顧客期限から逆算し、予備診断と是正期間を確保してください。

Q8. 対象範囲がまだ決まっていなくても相談できますか。

可能です。主要取引、重要情報、業務依存関係を整理する初期段階から支援を受けることで、過不足のある範囲設定や見積もりの手戻りを減らせます。

まとめ｜★4は「説明できる運用」と「技術的な裏付け」で備える

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★4取得準備では、要求事項を満たす規程、実際の運用、客観的な証跡、技術検証の結果が一貫していなければなりません。実地審査やサンプリングを直前対策として捉えず、どの拠点・端末・担当者が選ばれても同じ仕組みを説明できる状態を作ることが本質です。

まずは、取引と事業継続の観点から適用範囲を決め、ギャップ評価、予備診断、是正、模擬審査を進めてください。制度の最新情報を追いながら、未公表事項を仮定で埋めず、変更に対応できる計画を持つことが重要です。

SCS評価制度★4の準備を、現状整理から相談したい企業様へ

Librus株式会社では、対象範囲や実施方法が決まっていない段階でもご相談いただけます。主要取引、重要システム、既存規程・診断の状況を整理し、取得に向けた課題、優先順位、必要な技術検証、概算スケジュールを可視化します。社内稟議に必要な論点も整理できるため、まず何から着手すべきかを明確にしたい企業様に適しています。

参考情報

- 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）」
- 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」
- 経済産業省「SCS評価制度」特設サイト

※制度の名称、評価方法、日程、費用等は今後変更・更新される可能性があります。申請・契約時はIPAおよび経済産業省の最新版をご確認ください。

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