SCS評価制度★4取得に必要な対策｜第三者評価・技術検証を解説

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、サプライチェーン企業が標準的に目指すべき対策水準として位置づけられています。★3よりも広い範囲で、組織ガバナンス、取引先管理、システム防御・検知、インシデント対応、復旧までを包括的に求める点が特徴です。

結論から言えば、★4取得の準備では「規程を整える」「チェックシートを埋める」だけでは足りません。評価機関による第三者評価では文書確認に加えて実地審査が行われ、技術検証では対象IT基盤に対する脆弱性診断が実施されます。そのため、制度要求を満たすルール、実際の運用、設定・ログ・台帳などの証跡、外部公開資産の技術的な安全性を一体で整える必要があります。

本記事では、従業員100～1,000名程度の企業を想定し、SCS評価制度★4の水準、第三者評価と技術検証の仕組み、取得前に実施すべき対策、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の使い分け、費用・期間を左右する要因、支援会社の選び方まで実務に即して解説します。

この記事で分かること

- ・SCS評価制度★4が求める対策水準と★3との違い
- ・第三者評価で確認される文書・運用・証跡の考え方
- ・技術検証（脆弱性診断）に備えて確認すべきIT基盤
- ・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の位置づけ
- ・★4取得に向けた準備手順、費用・期間、ベンダー選定のポイント

SCS評価制度★4とは

SCS評価制度は、取引先ごとに異なりやすいセキュリティ要求を共通化し、サプライチェーンに参加する企業の対策状況を可視化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、IPAが制度を運営します。★3・★4は2027年3月頃の運用開始が予定されています。

★4は、供給停止によってサプライチェーンに大きな影響を及ぼし得る企業や、漏えい時の影響が大きい機密情報等を扱う企業も念頭に、標準的に目指すべき水準として設計されています。初期侵入を防ぐだけでなく、侵入後の被害拡大防止、攻撃の検知、インシデント対応、復旧、取引先管理までを含めた対策が求められます。

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

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

★3との違いは「対策の広さ」と「評価方法」

★3は一般的なサイバー脅威に対処する基礎的な水準で、専門家確認付き自己評価です。一方、★4では★3を包含しながら、継続的改善につながるリスク管理、取引先管理、防御・検知、インシデント対応等をより包括的に求めます。評価も自己評価だけでは完結せず、指定された評価機関による第三者評価と技術検証が必要です。

なお、★4を取得するために★3を先に取得する必要はありません。自社のサプライチェーン上の役割、取引先から要求される水準、扱う情報・業務の重要性などから、目指す段階を判断します。

SCS評価制度★4の第三者評価は何を確認するのか

★4では、取得希望組織が要求事項・評価基準に沿って自己評価を行った後、評価機関へ評価・技術検証を依頼します。IPAの制度構築方針では、★4の評価は「文書確認」「実地審査」「技術検証」で構成される考え方が示されています。評価対象は、企業が定めた適用範囲からサンプリングして確認する想定です。

出典：IPA「制度構築方針」 https://www.ipa.go.jp/security/scs/rcu1hd0000007ajp-att/20260327001-br.pdf

文書確認では自己評価の根拠が問われる

文書確認では、自己評価の記載内容に矛盾がないか、評価基準から見て必要な事項が十分に記載されているかなどが確認されます。社内規程や方針を用意するだけでなく、要求事項と実際の運用が対応していることを説明できるよう、資産台帳、ネットワーク構成図、権限管理記録、パッチ管理記録、委託先管理資料、教育記録、インシデント対応手順などを整理しておくことが重要です。

実地審査では「実際に運用されているか」が確認される

制度構築方針では、実地審査は取得希望企業へのヒアリング、規程、操作画面等の確認によって行う想定です。相対的に重要性の高い対策について、証跡を含めて評価するとされており、例として脆弱性管理体制・管理プロセス、セキュリティインシデント対応手順、事業継続要件に沿った復旧準備が挙げられています。

つまり、規程に「毎月確認する」と記載していても、実施記録がない、担当者が手順を理解していない、操作画面上では設定されていないといった場合は説明が難しくなります。★4では、文書と運用実態を一致させることが重要です。

SCS評価制度★4の技術検証とは

IPAは、★4の技術検証事業者について「委託元評価機関の委託を受けて技術検証（脆弱性診断）を実施し、技術検証結果報告書を評価機関に交付する」役割としています。評価機関自身が技術検証を行う場合もあれば、指定された別の技術検証事業者へ委託する場合もあります。

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）」
https://www.ipa.go.jp/security/scs/security-experts-organization/shiteishinsei.html

技術検証は外部公開機器の脆弱性を実際に確認する

制度構築方針では、技術検証の例として、取得希望企業がインターネットに公開している機器のうち、脆弱性を悪用された場合に組織内部へ侵入されるリスクが高い機器を対象に、既知脆弱性の悪用など一般的な攻撃パターンを試行する脆弱性検査が示されています。VPN装置やルータなどが例示されています。

ここで重要なのは、評価直前に診断を受けることよりも、日常的に外部公開資産を把握し、脆弱性情報を収集し、修正期限を定め、パッチや設定変更を行うプロセスを確立することです。技術検証で問題が見つかったときに、資産の存在そのものを把握していなかった状態では、根本的な管理プロセスの見直しが必要になります。

Webアプリケーション診断・プラットフォーム診断との関係

Webアプリケーション診断は、Webアプリケーションの入力処理、認証・認可、セッション管理などを確認し、SQLインジェクション、クロスサイトスクリプティング、アクセス制御不備といった脆弱性を検出するために用います。一方、プラットフォーム診断は、サーバー、VPN、ルータ、クラウド公開資産などについて、公開ポート、ソフトウェアの既知脆弱性、設定不備などを確認する手法です。

SCS評価制度★4の技術検証は制度で指定された方法に従う必要があるため、一般の脆弱性診断を受ければ自動的に技術検証を代替できるとは限りません。ただし、取得前の準備として外部公開資産を診断し、重大な脆弱性を先に是正しておくことは有効です。制度構築方針では、直近の脆弱性検査結果など相当する証跡をもって技術検証の代替とみなす案も検討対象として示されているため、最終的な運用ルールは申請時点のIPA資料で確認する必要があります。

ペネトレーションテストは★4の技術検証と同じではない

ペネトレーションテストは、攻撃者の目的やシナリオを設定し、複数の脆弱性や設定不備を組み合わせて、どこまで侵入・権限拡大・重要資産への到達が可能かを検証する手法です。★4の技術検証としてIPAが示している「脆弱性診断」と同義ではありません。

一方、重要システムや取引先データを扱う環境では、脆弱性の有無だけでなく「侵害された場合に何が起きるか」を把握することが経営判断に役立ちます。そのため、制度取得とは別のリスク管理施策としてペネトレーションテストを組み合わせる価値があります。

★4取得に向けて実施すべき主な対策

★4では、経営の責任、サプライチェーンの防御、IT基盤の防御という観点をまたいで、対策を継続的に運用することが重要です。以下は制度要求を実務に落とし込む際の主要な確認ポイントです。

1. 経営層への報告と継続的改善の仕組みを作る

セキュリティ担当者だけで改善を進めるのではなく、経営層がリスクと対策状況を定期的に把握し、不備の是正や投資判断につなげる仕組みを整えます。報告内容には、重大脆弱性、インシデント、未対応リスク、取引先からの要求、改善計画の進捗などを含めると、技術課題を経営リスクとして判断しやすくなります。

2. 資産・ネットワーク・外部公開面を継続的に把握する

サーバー、端末、ネットワーク機器、クラウド、SaaS、外部公開IP・ドメイン、取引先との接続を一覧化し、変更時に更新される運用を作ります。特にVPN装置、リモートアクセス基盤、クラウド管理画面、公開Webシステムなどは、攻撃者が最初に狙いやすい入口です。棚卸しを年1回のイベントにせず、構成変更や新規導入のプロセスと連動させます。

3. 脆弱性管理を「発見から是正完了まで」のプロセスにする

脆弱性情報の収集、影響判定、対応期限の設定、パッチ適用、例外承認、再確認までを一連の管理プロセスとして整備します。CVSSなどの技術的深刻度だけでなく、インターネット公開の有無、攻撃コードの公開状況、業務重要度、代替策の有無も加味して優先順位を決めることが実務的です。

診断で「高危険度」と判定された項目を放置するのではなく、修正担当者、期限、暫定対策、恒久対策、再診断結果まで追跡できる台帳を用意すると、実地審査でも説明しやすくなります。

4. ID・特権権限・リモートアクセスを強化する

侵入後の被害拡大を防ぐには、一般アカウントと管理者権限の分離、多要素認証、不要アカウントの削除、権限の定期棚卸しが重要です。特に外部から利用できるVPN、クラウド管理コンソール、サーバー管理画面、委託先用アカウントなどは重点的に確認します。共有アカウントや恒久的な保守権限が残っている場合は、利用目的と必要性を見直します。

5. ログ監視と検知・初動対応を整備する

★4は初期侵入の防止だけでなく、侵入後の被害拡大防止も重視します。認証ログ、VPNログ、EDR、サーバー、クラウド、ファイアウォール等から必要なログを取得し、異常を検知した場合の確認・エスカレーション手順を定めます。SOCを自社で持たない場合でも、MDRや外部SOCの活用、重要ログの集中管理など、自社規模に合った方法を選択できます。

6. インシデント対応と事業継続・復旧を実動レベルにする

手順書を作るだけでなく、ランサムウェア感染、情報漏えい、VPN侵害など具体的なシナリオで、連絡・隔離・証拠保全・取引先通知・経営判断・復旧を訓練します。バックアップについても、取得しているだけでなく、復元可能性、保管場所、アクセス権限、ランサムウェアからの保護を確認します。

7. 取引先・委託先のセキュリティ管理を強化する

サプライチェーン上の重要な委託先について、接続範囲、取り扱う機密情報、再委託、事故報告、契約終了時のデータ削除などを整理します。重要度に応じて要求水準を変えることで、全取引先へ一律に過剰な対応を求めることを避けながら、リスクの高い委託先を重点的に管理できます。

★4取得に向けた具体的な準備手順

ステップ1：適用範囲と取得目的を経営層と合意する

「取引先から求められそうだから」という理由だけで始めると、対象範囲や投資判断が曖昧になります。どの事業・拠点・IT基盤を対象にするか、どの取引を守るために★4を目指すのか、経営層と合意します。取引先から具体的な要求がある場合は、期限や対象組織も確認します。

ステップ2：要求事項・評価基準とのギャップ分析を行う

IPAが公表している★4要求事項・評価基準に沿って、現状を「適合」「一部適合」「未対応」に分類します。規程の有無だけでなく、証跡、設定、運用頻度、担当者の理解まで確認します。既存のISMSやPマーク、社内監査資料がある場合は流用できる部分を整理し、二重作業を減らします。

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

ステップ3：技術的な事前診断を行う

評価直前に重大脆弱性が見つかると、パッチ適用やシステム更改が間に合わない可能性があります。外部公開資産を中心にプラットフォーム診断を行い、重要なWebサービスにはWebアプリケーション診断を実施します。必要に応じてペネトレーションテストを加え、攻撃経路や被害範囲を把握します。

ステップ4：不適合・不足事項を改善し、証跡を残す

発見した問題は、事業影響と攻撃可能性を踏まえて優先順位を付けます。緊急度の高い外部公開機器の脆弱性、管理者アカウント、多要素認証、サポート切れ製品などから対策し、変更記録、承認記録、再診断結果を残します。実地審査では「改善した」という説明だけでなく、その事実を確認できる証跡が重要です。

ステップ5：模擬審査と関係部署ヒアリングを行う

情報システム部門だけでなく、総務、人事、法務、調達、事業部、経営層など、要求事項に関係する部署へ模擬ヒアリングを行います。規程上の責任者と実際の担当者が異なる、契約上の事故報告期限を現場が知らないなど、部署横断の不整合を事前に発見できます。

ステップ6：指定評価機関へ評価を依頼する

IPAは2026年度の評価機関・技術検証事業者の指定申請を2026年9月18日から10月26日まで受け付け、指定機関台帳への登録・公表を2026年12月下旬に予定しています。実際に★4を申請する際は、IPAが公表する最新の指定機関台帳から評価機関を確認し、評価範囲、日程、技術検証の実施体制、見積条件などを比較します。

★4の費用と期間を左右する要因

★4の総コストは制度の登録料だけではありません。第三者評価費、技術検証費、取得支援費、事前診断費、改善に必要な機器・ライセンス費、社内工数などを含めて考える必要があります。費用を大きく左右するのは、対象拠点数、外部公開資産数、システム数、既存統制の成熟度、改善が必要な不適合の量、診断対象、現地審査の範囲などです。

期間も同様です。すでに資産管理・権限管理・脆弱性管理・ログ監視・インシデント対応が運用されている企業であれば証跡整理が中心になりますが、サポート切れ機器の更改やネットワーク再設計が必要な場合は数か月単位の準備が必要になる可能性があります。制度上の審査日数だけで逆算せず、改善期間を含めて計画します。

社内稟議・予算申請で説明すべきポイント

★4対応の稟議では、「認証取得費」とだけ説明すると投資の必要性が伝わりにくくなります。取引継続・新規受注への影響、重要システム停止による売上影響、顧客・取引先データ漏えい時の対応負荷、サイバー保険や監査対応、インシデント復旧費用など、経営リスクと結び付けて説明することが重要です。

予算は、①ギャップ分析・支援、②事前診断、③不足対策の導入・更改、④第三者評価・技術検証、⑤不適合是正・再確認、⑥取得後の維持運用に分けると、追加費用の発生理由を整理しやすくなります。

★4支援会社・ベンダーを選ぶポイント

制度要求と技術対策の両方を理解しているか

規程作成だけに強い会社と、脆弱性診断だけに強い会社では、★4対応全体を一貫して整理できない場合があります。要求事項の解釈、ギャップ分析、運用整備、技術診断、是正支援まで対応できるかを確認します。

第三者評価を行う主体との役割分担が明確か

★4の第三者評価はIPAの指定を受けた評価機関が実施します。コンサルティング会社へ支援を依頼する場合、取得支援と正式な第三者評価を混同しないことが重要です。見積書やRFPでは、「取得支援」「事前診断」「正式評価」「技術検証」のどこまでを誰が担当するのかを明確にします。

RFP・見積依頼時に確認したい項目

見積依頼では、対象組織・拠点、対象システム、外部公開IP・URL、クラウド利用状況、希望取得時期、既存認証、規程・台帳の有無、診断可能時間、個人情報・機密情報の取扱い、再診断の条件、成果物の内容を伝えます。情報が不足すると追加費用や日程変更につながるため、分からない項目は「未整理」として共有し、調査工程を見積もってもらう方法が現実的です。

よくある失敗と注意点

評価直前に証跡を作り始める

★4では実地審査があるため、直前に帳票だけを整えても、継続運用の実態を説明できない可能性があります。月次・四半期・年次で実施する統制は、早めに運用を開始して記録を蓄積します。

診断結果を危険度だけで処理する

診断ツールの危険度が低くても、外部公開された管理画面や重要取引先への接続点など、事業影響が大きい場合があります。技術スコアと業務影響を合わせて優先順位を決めます。

「製品を導入すれば取得できる」と考える

経済産業省は、SCS評価制度の評価基準を達成するために特定のセキュリティ製品の導入を必須としているわけではないとしています。EDR、SIEM、多要素認証などは有効な手段ですが、要求事項を満たす運用プロセスと組み合わせて初めて効果を発揮します。

Librus株式会社が提供できる支援

Librus株式会社では、SCS評価制度★4への対応を、申請書類の準備だけでなく、経営・運用・技術を横断したセキュリティ改善プロジェクトとして支援できます。適用範囲の整理、要求事項とのギャップ分析、改善計画、規程・運用整備、証跡設計、事前診断、是正支援まで、企業ごとの環境に合わせて設計します。

技術面では、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・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などを組み合わせることが可能です。診断結果を列挙するだけではなく、事業影響や取引先への影響を踏まえて改善の優先順位を整理し、運用までつなげます。

また、経営層、情報システム部門、調達・法務、現場部門など複数部署にまたがる論点を整理し、稟議や予算化に必要な説明材料を作る支援も可能です。対象範囲や取得時期が決まっていない段階でも、現状把握から相談できます。

よくある質問

Q1. SCS評価制度★4はいつから取得できますか？

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。評価機関等の指定機関台帳は2026年12月下旬に公表予定です。最新日程は申請前にIPA公式情報を確認してください。

Q2. ★4を取得する前に★3の取得は必要ですか？

必要ありません。上位段階は下位段階の要求を包含しますが、★3を事前取得していなければ★4を申請できないという関係ではありません。

Q3. ★4は自己評価だけで取得できますか？

できません。★4は自己評価を記入したうえで、指定評価機関による第三者評価と技術検証を受け、評価報告書を取得してから事務局へ登録申請する仕組みです。

Q4. 技術検証では何をするのですか？

IPAの最新案では、技術検証は脆弱性診断として実施されます。制度構築方針では、インターネット公開機器のうち侵入リスクが高い機器に対し、既知脆弱性の悪用など一般的な攻撃パターンを試行する例が示されています。

Q5. ペネトレーションテストを受ければ技術検証の代わりになりますか？

ペネトレーションテストと制度上の技術検証は目的・方法が同一ではありません。正式な代替可否は、申請時点の制度ルールと評価機関の指示に従う必要があります。事前のリスク把握としてペネトレーションテストを行うことは有効です。

Q6. ISMSを取得していれば★4対応は不要ですか？

不要とはいえません。ISMSで整備した方針・リスク管理・証跡を活用できる可能性はありますが、SCS評価制度には独自の要求事項・評価基準と評価スキームがあります。ギャップ分析が必要です。

Q7. 第三者評価にはどのくらいの期間がかかりますか？

制度構築方針では文書確認、実地審査、技術検証それぞれに想定日数が示されていますが、事前準備・報告書作成・不適合是正は別です。実際の期間は対象範囲と改善量によって大きく変わるため、準備期間を含めて計画してください。

Q8. 何から始めるのが最も効率的ですか？

最初に適用範囲を決め、★4要求事項とのギャップ分析を行うことを推奨します。その後、外部公開資産や特権権限などリスクの高い領域から技術確認・改善を進め、証跡を蓄積すると手戻りを減らせます。

まとめ｜SCS評価制度★4は「運用実態」と「技術的な有効性」まで整える

SCS評価制度★4は、サプライチェーン企業が標準的に目指すべきセキュリティ水準として、組織ガバナンス、取引先管理、システム防御・検知、インシデント対応、復旧を包括的に確認する制度です。★4では、評価機関による第三者評価に加え、実地審査と技術検証が行われるため、文書だけでなく実際の運用と技術的な安全性を説明できる状態が必要です。

準備では、適用範囲を定め、要求事項とのギャップを把握し、外部公開資産や脆弱性管理、ID・権限管理、ログ監視、インシデント対応、取引先管理を重点的に改善します。Webアプリケーション診断やプラットフォーム診断を事前に実施し、必要に応じてペネトレーションテストで侵害時の影響まで確認しておくことで、評価直前の大きな手戻りを抑えやすくなります。

2027年3月頃の制度開始に向け、評価機関の指定や運用詳細は今後も更新されます。制度開始を待ってから準備するのではなく、いま公表されている要求事項・評価基準を基に、自社の不足を整理して改善を始めることが現実的です。

SCS評価制度★4への対応を、対象範囲の整理から相談できます

Librus株式会社では、「★4を目指すべきか判断したい」「第三者評価に向けて何が不足しているか確認したい」「技術検証の前に外部公開資産を診断したい」といった初期段階からご相談いただけます。対象範囲や具体的な実施方法が決まっていなくても、事業・取引先・IT環境を整理し、要求事項とのギャップと優先順位を可視化することで、必要な対策、予算、スケジュールを具体化できます。

制度対応、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、改善支援、SOC／CSIRT支援まで一気通貫で検討できるため、制度取得だけで終わらず、実際のセキュリティ水準向上につなげることが可能です。

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