SCS評価制度★4の技術検証とは？調査項目と準備を解説

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では、書類を整えるだけではなく、第三者評価に加えて実地審査と技術検証が行われます。結論からいえば、技術検証で確かめるのは「規程に書かれた対策が、対象システム上で実際に機能しているか」です。脆弱性診断だけを受ければ足りるとは限りません。外部公開システムの弱点、サーバーやネットワーク機器の設定、認証・権限管理、ログの取得と監視、バックアップからの復旧可能性などを、証跡と技術的な確認によって立体的に検証する準備が必要です。

ただし、2026年9月3日時点で、制度は2026年度末頃の申請受付開始に向けて詳細化の途中です。実際の検証項目、サンプリング方法、工数、提出様式は今後公表される文書で確定する部分があります。本記事では、公表済みの制度構築方針、★3・★4要求事項・評価基準、IPAの制度説明を基礎に、取得希望企業が今から準備すべき実務を解説します。未公表の事項を確定要件として扱わないことが重要です。

この記事で分かること

この記事を読むと、★4における第三者評価と技術検証の違い、想定される確認領域、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、社内で準備すべき資料、対象範囲の決め方、費用と期間を左右する要因が分かります。あわせて、経営層が決める事項と情報システム部門が進める作業を切り分け、評価直前の場当たり的な対応を避ける進め方を示します。

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と★4の概要

SCS評価制度は、発注者と受注者の間で求めるセキュリティ対策の水準を分かりやすく示し、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。IPAによれば、委託元には取引先の対策状況を把握しにくい問題があり、委託先には取引先ごとに異なる質問票への対応が重なる問題があります。共通の評価軸を設けることで、双方の確認負担を減らしながら、事業停止、情報漏えい、改ざん、踏み台化などのリスクを抑えることが制度の狙いです。

公表済みの枠組みでは、★3は一般的なサイバー脅威に対処できる基礎的な水準で、専門家確認付きの自己評価です。★4は、初期侵入の防御だけでなく、侵入後の被害拡大防止、検知、インシデント対応、取引先のデータやシステムの保護、サプライチェーン上の役割に応じた強靱化までを対象とし、評価機関による第三者評価と技術検証が求められます。★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は下位段階の要求を包含します。

なお、SCS評価制度は法令上の強制制度ではなく、二社間の契約などで活用される任意制度です。「取得しなければ直ちに取引が規制される」と断定する説明は正確ではありません。一方で、発注者が調達条件や取引先管理に用いる可能性はあるため、主要顧客の要請、入札方針、自社のサプライチェーン上の重要性を踏まえて取得方針を判断する必要があります。

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

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・内閣官房国家サイバー統括室「SCS評価制度に関する注意喚起」
https://www.meti.go.jp/policy/netsecurity/20260427_scs.html

★4の技術検証では何を調べられるのか

★4の技術検証は、評価対象企業が説明した統制や対策が、対象となるIT基盤で有効に実装されているかを技術的に確かめる工程です。IPAは、★4について文書確認に加え、実地審査と技術検証を行い、企業が定めた適用範囲から対象をサンプリングして評価する想定を示しています。したがって、すべての端末やサーバーを一律に検査する「全数点検」とも、外部公開サイトだけをスキャンする「脆弱性診断」とも同義ではありません。

技術検証の準備では、要求事項、評価証跡、技術的な確認方法を一対一で結び付けます。たとえば「多要素認証を導入している」という回答だけでなく、誰に、どのシステムで、どの認証方式を適用し、例外をどう承認し、退職者の権限をいつ削除するかまで説明できる状態が望まれます。以下は、公表資料の趣旨を踏まえて企業が想定しておくべき代表的な確認領域です。最終的な必須項目は、今後の評価ガイドや評価機関の正式な手順で確認してください。

1. 脆弱性診断：攻撃の入口になり得る弱点を確認する

脆弱性診断では、既知の脆弱性、不要な公開ポート、古いソフトウェア、安全でない通信方式、Webアプリケーションの実装不備などを調べます。対象は、コーポレートサイトだけではありません。VPN装置、リモートアクセス基盤、メール関連システム、クラウド上の公開サーバー、取引先向けポータル、APIなど、攻撃者がインターネットから到達できる資産を漏れなく把握することが先決です。

Webアプリケーション診断では、SQLインジェクション、クロスサイトスクリプティング、認証・セッション管理の不備、アクセス制御の欠陥などを確認します。プラットフォーム診断では、OS、ミドルウェア、ネットワーク機器、暗号設定、公開サービスなどを確認します。同じ「診断」でも対象と観点が違うため、システム台帳とデータフローを基に組み合わせる必要があります。

診断結果は、危険度の点数だけで判断しないことが重要です。外部から悪用可能か、管理者権限に到達するか、顧客情報や設計情報に接続するか、代替統制があるか、事業停止につながるかを加味

します。技術的な重大度が中程度でも、主要取引先とのファイル交換基盤に存在する弱点なら、経営上の優先度は高くなり得ます。

2. 設定確認：安全な製品でも危険な使い方になっていないか

設定確認では、ファイアウォール、VPN、クラウド、サーバー、端末、メール、ID管理基盤などが、自社の基準に沿って構成されているかを確認します。管理画面のインターネット公開、初期アカウントの残存、過度に広い通信許可、暗号化されていない管理通信、クラウドストレージの公開設定、監査機能の無効化などは、製品自体に脆弱性がなくても事故の原因になります。

ここで問われるのは、一時点の画面表示だけではありません。安全な標準設定を定めているか、構成変更を申請・承認・記録しているか、例外設定に期限と責任者があるか、定期的に差分を確認しているかという運用も重要です。設定値のスクリーンショットを大量に集めるより、基準、実設定、例外台帳、変更履歴を突合できる状態を作る方が実務的です。

3. 認証・権限：本人確認と最小権限が機能しているか

認証領域では、多要素認証、パスワード方針、特権IDの管理、共有アカウント、休眠アカウント、入社・異動・退職時の権限変更を確認します。特に、VPN、クラウド管理者、Microsoft 365やGoogle Workspace、サーバー管理、バックアップ管理など、侵害時の影響が大きいアカウントが焦点になります。

典型的な問題は「多要素認証を導入したが、一部の旧式認証や緊急用アカウントが除外されている」「退職者のSaaSアカウントが残っている」「委託先に管理者権限を恒常付与している」といった状態です。検証に備えるには、利用者一覧、権限一覧、承認記録、棚卸結果、例外と期限を整え、実際の設定と一致させます。

4. ログと監視：侵入後に気付けるか、説明できるか

ログは、攻撃の兆候を発見し、事故発生後に事実関係を追跡するための記録です。認証、管理者操作、端末検知、ネットワーク通信、クラウド監査、重要データへのアクセスなどについて、必要なログを取得しているかを確認します。さらに、保存期間、時刻同期、改ざん防止、閲覧権限、監視ルール、アラート対応、エスカレーションの仕組みまで見なければ、単に「ログがある」だけで終わります。

たとえば深夜の国外ログインを検知しても、通知先が退職者のメールアドレスなら対策は機能しません。EDRやSIEMを導入していても、重要サーバーが監視対象から外れていたり、アラートが長期間未処理だったりすれば、実効性に課題があります。技術検証前には、代表的な検知シナリオを使い、通知、一次判断、封じ込め、記録までの流れを確認するとよいでしょう。

5. バックアップ：取得ではなく復旧可能性を確認する

ランサムウェア対策では、バックアップの有無だけでなく、攻撃者から分離されているか、バックアップ管理権限が本番環境と分かれているか、必要な世代が保管されているか、復旧試験を実施しているかが重要です。本番の管理者アカウントでバックアップも削除できる構成では、同時に暗号化・消去されるおそれがあります。

復旧試験では、ファイルが一つ戻るかだけでなく、重要業務を所定の時間内に再開できるかを確かめます。復旧対象の優先順位、RTO（目標復旧時間）、RPO（許容できるデータ損失時間）、依存するID基盤やネットワーク、復旧担当者、連絡先を明確にします。テスト結果と発見事項、未達の場合の改善計画を残すことで、事業継続の説明資料にもなります。

6. ペネトレーションテスト：弱点を組み合わせた侵入可能性を確かめる

ペネトレーションテストは、許可された範囲で攻撃者の手法を模擬し、複数の弱点を組み合わせて重要資産へ到達できるかを確認する試験です。個別の脆弱性を網羅的に洗い出す脆弱性診断とは目的が異なります。たとえば、外部公開VPNの設定不備、弱い認証、端末上の過剰権限、ネットワーク分離の不足を連鎖させ、取引先データを保管するサーバーまで到達できるかを検証します。

制度上、すべての企業に同じ規模のペネトレーションテストが一律に必要と断定することはできません。ただし、外部公開資産が多い企業、重要情報を大量に扱う企業、遠隔保守や多数の委託先接続がある企業では、統制の実効性を確認する有力な方法です。実施時は、対象、禁止事項、試験時間、緊急連絡、停止条件、取得データの扱いを事前に合意します。

技術検証の対象となる企業・システム・場面

★4は、従業員数だけで決まる制度ではありません。従業員100〜1,000名規模でも、大手企業の業務を受託する、取引先の個人情報・設計情報を保管する、基幹業務をSaaSとして提供する、遠隔保守で顧客環境に接続する、物流・製造・決済など停止影響の大きい業務を担う企業は、早めの検討が有効です。

制度の主な対象はビジネス・ITサービスに関わるIT基盤です。一般にIT基盤に該当しない製造設備などのOTシステムや、取引先へ提供する製品そのものは直接の対象外とされ、他の制度・ガイドラインで対策する想定が示されています。ただし、社内ITと工場ネットワークの接続点、保守端末、認証基盤、バックアップなどは相互に影響します。形式的に「OTは対象外」と切り離さず、境界と依存関係を明示する必要があります。

★4技術検証に向けた実施手順

経営層が最初に決めること

最初に決めるのは製品ではなく、取得目的と適用範囲です。主要顧客の要請への対応、新規取引の条件整備、事故リスクの低減、監査回答の共通化など、投資目的を言語化します。その上で、対象法人、事業、拠点、システム、委託先、データを決め、対象外とする範囲には合理的な理由を持たせます。

経営会議では、評価取得だけをゴールにしないことが大切です。重大な不備が見つかった場合の改修予算、業務停止を伴う設定変更、例外リスクの受容、再検証まで含めて意思決定します。社内稟議には、制度の任意性、顧客・事業上の必要性、対象範囲、概算費用、担当部門、想定スケジュール、発見事項への対応費を記載すると、後工程の予算不足を防ぎやすくなります。

情報システム部門が準備する資料

実務の出発点は、現状を説明できる資料の整備です。組織図と責任分担、情報資産・システム台帳、ネットワーク構成図、データフロー、外部公開資産一覧、アカウント・権限一覧、委託先一覧、セキュリティ規程、設定基準、変更記録、脆弱性管理台帳、ログ設計、インシデント対応手順、バックアップ・復旧手順、教育記録などを集めます。

資料は「存在するか」だけでなく、更新日、責任者、実環境との一致を確認します。クラウドやSaaSが各部門で個別導入されている企業では、台帳にないサービスが評価範囲から漏れやすいため、経費データ、シングルサインオンの登録、ネットワーク通信、ヒアリングなどを組み合わせて棚卸しします。

ギャップ分析から改善、事前検証へ進む

次に、★4要求事項・評価基準と現状を照合し、未対応、部分対応、証跡不足を分けます。未対応は仕組みそのものがない状態、部分対応は一部拠点や一部システムだけに適用されている状態、証跡不足は実施していても記録で説明できない状態です。この三つを混同すると、ツール導入に偏った改善計画になります。

優先順位は、攻撃可能性、影響、取引先との関係、是正に必要な時間で決めます。インターネット公開機器の重大な脆弱性や、退職者の管理者IDなどは早急に対処します。規程の改定や全社教育は承認・展開に時間がかかるため、年度計画に組み込みます。改善後は、脆弱性の再診断、設定の再確認、アカウント棚卸し、ログ検知テスト、バックアップ復旧試験を行い、対策が機能した証拠を残します。

実施期間と費用を左右する要因

制度上の標準費用・標準期間が一律に決まっているわけではありません。準備から改善までの期間は、適用範囲、拠点数、システム数、クラウド利用状況、台帳の精度、既存認証の有無、診断対象、是正の難易度、評価機関の予約状況で変わります。小さく整理された範囲なら短く進みますが、資産台帳の作成から始める場合や、基幹システムの改修を伴う場合は複数の予算期にまたがる可能性があります。

費用は、コンサルティング、第三者評価、技術検証、システム改修、製品・サービス、社内工数に分けて考えます。見積額だけを比較すると、診断対象のIP数やURL数、クラウドテナント数、拠点訪問、再検証、報告会、緊急対応、報告書の粒度が違い、適正な比較ができません。RFP（提案依頼書）では、対象範囲、前提資料、検証方式、成果物、再検証の条件、機密情報の保管・削除、事故時の責任分担を揃えて提示します。

技術検証・支援会社の選び方

★4の正式な評価や技術検証は、制度に基づき指定された機関・事業者へ依頼する必要があります。IPAは、評価機関を2026年12月末頃から公表する予定としています。取得準備のコンサルティング会社と正式な評価機関が同一になる場合には、中立性・公平性に関する制度上の条件を確認しなければなりません。

選定時は、指定の有無だけでなく、Webアプリケーション、ネットワーク、クラウド、ID、ログ、バックアップの知見を横断して持つかを確認します。診断結果を列挙するだけでなく、事業影響を踏まえた優先順位と改善案を示せるか、経営層向けと技術担当者向けの双方の報告があるか、再検証まで支援できるかも重要です。

個人情報や機密情報の扱いも確認してください。秘密保持、作業者の権限管理、取得データの暗号化、保存場所、国外移転、再委託、保管期限、消去証明、脆弱性情報の連絡方法を契約前に合意します。ペネトレーションテストでは実データへ接触する可能性があるため、証跡として何を残し、何を持ち出さないかまで決めておく必要があります。

よくある失敗と注意点

最も多い失敗は、評価直前に証跡を集め始めることです。ログの保存期間が短ければ過去の運用を示せず、アカウント棚卸しや復旧試験をその場で再現することもできません。少なくとも一回の運用サイクルを回し、承認、実施、例外、改善の記録を残すことが重要です。

次に、脆弱性診断だけで★4に備えたつもりになることです。診断は重要ですが、設定、ID、ログ、バックアップ、インシデント対応、委託先管理などの統制を代替しません。逆に、規程だけを増やし、現場の設定や運用を確認しない対応も不十分です。

もう一つは、適用範囲を狭くすれば安く済むと考えることです。主要な顧客データや業務を支えるシステムを不自然に外せば、取得目的と整合しません。対象外の妥当性、依存関係、発注者が期待する範囲を説明できることが必要です。

Librus株式会社が提供できる支援

Librus株式会社は、SCS評価制度の★4取得を見据えた現状整理、適用範囲の設計、要求事項とのギャップ分析、改善計画、証跡整備、事前の技術検証を一気通貫で支援します。制度対応を単なるチェックリスト作成にせず、経営リスク、取引先対応、事業継続、実装可能性を同じ計画に落とし込むことを重視しています。

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、設定確認、ログ・監視設計、インシデントレスポンス、デジタルフォレンジック、SOC／CSIRT構築、SBOM導入などを組み合わせられます。診断で問題を見つけて終わるのではなく、改修の優先順位付け、運用定着、再診断まで支援できる点が特徴です。

また、経営層、情報システム部門、現場部門の間で、同じ課題を異なる言葉で説明できます。経営層には取引・財務・信用・事業継続への影響を、技術部門には具体的な設定と改善手順を示し、企業ごとの環境、既存投資、予算、稟議時期に合わせて現実的なロードマップを設計します。

よくある質問

Q1. ★4の技術検証は脆弱性診断と同じですか

同じではありません。脆弱性診断は技術検証に用いられる方法の一つです。★4では、文書確認と実地審査に加え、設定、認証・権限、ログ、バックアップなど、要求事項が実環境で機能しているかを確認することが想定されます。

Q2. すべてのサーバーや端末が検査されますか

IPAは、企業が決めた適用範囲から対象をサンプリングして評価する想定を示しています。具体的な抽出方法や件数は、正式な評価手順と評価機関の案内を確認する必要があります。重要資産の漏れを避けるため、全体の台帳整備は必要です。

Q3. ペネトレーションテストは必須ですか

現時点で、すべての取得希望企業に同一内容のペネトレーションテストが一律必須と断定できません。対象システムとリスクに応じ、脆弱性診断や設定確認などと組み合わせて検証方式を決めます。

Q4. クラウドサービスも対象になりますか

適用範囲内の事業や情報を支えるクラウドは対象となり得ます。利用企業が管理するID、アクセス権、ログ、データ保護、設定、委託先管理を整理します。クラウド事業者が担う責任との境界も確認が必要です。

Q5. ★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、★3を事前に取得しなければ★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★3相当の基礎的対策を含むため、現状把握では下位要求も併せて確認します。

Q6. SCS評価制度への対応は義務ですか

制度自体は任意です。ただし、発注者が契約や調達条件として一定の段階を求める可能性があります。主要顧客の方針や自社の事業上の必要性を確認して判断します。

Q7. 技術検証前に最低限そろえるものは何ですか

適用範囲、システム・情報資産台帳、ネットワーク構成図、外部公開資産一覧、ID・権限一覧、設定基準、ログ設計、バックアップ・復旧記録、過去の診断と改善記録を優先してください。資料と実環境の不一致も解消します。

Q8. 不備が見つかったら取得できませんか

正式な判定は制度文書と評価機関の手順によります。準備段階で不備が見つかること自体は、改善機会です。影響と悪用可能性で優先順位を付け、是正、代替統制、期限付き改善計画、再検証を進めます。

まとめ：★4は「ある対策」から「機能する対策」への確認

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の★4では、規程や自己申告だけでなく、第三者評価、実地審査、技術検証を通じて、対策が現場で機能しているかを確認します。想定される中心領域は、脆弱性診断、設定、認証・権限、ログ・監視、バックアップ・復旧です。必要に応じてペネトレーションテストを組み合わせ、個々の弱点が事業や取引先へどう波及するかを検証します。

準備の要点は、取得目的と適用範囲を経営層が決め、情報システム部門が資産・設定・運用証跡を整え、ギャップ分析、改善、再検証までを一つの計画として進めることです。制度の詳細は今後更新されるため、経済産業省とIPAの公表資料を継続的に確認し、未確定情報を前提に過剰な投資をしない姿勢も欠かせません。

出典：経済産業省「SCS評価制度に関する制度構築方針」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/20260327_report.html

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

出典：IPA「SCSセキュリティ専門家・評価機関」
https://www.ipa.go.jp/security/scs/security-experts-organization.html

SCS評価制度の対象範囲から整理したい企業へ

「主要顧客から将来の対応可能性を尋ねられたが、どこまでを対象にすべきか分からない」「診断は実施済みだが、★4との差分が見えない」という段階でもご相談いただけます。Librus株式会社が、事業・取引・システムの関係を整理し、必要な準備と優先順位を可視化します。早期に論点を把握することで、予算化や社内稟議を進めやすくなります。

技術検証の事前準備を具体化したい企業へ

Librus株式会社は、Webアプリケーション診断、プラットフォーム診断、設定確認、認証・権限、ログ、バックアップ、ペネトレーションテストの必要性を対象環境に応じて整理します。実施方法が決まっていなくても問題ありません。既存資料と現状を確認し、過不足のない検証計画と改善ロードマップの作成を支援します。

診断後の改善・運用まで一貫して進めたい企業へ

課題の発見後に、担当部門、期限、予算、再検証方法が決まらず止まるケースは少なくありません。Librus株式会社では、経営上の影響と技術的な重大度を結び付け、改修の優先順位、証跡整備、運用定着、再診断まで支援します。まずは現在の準備状況を共有いただくことで、次に着手すべき作業を明確にできます。

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