SCS評価制度に脆弱性診断は必要？評価基準との関係と実施時のポイント

結論から言えば、SCS評価制度で「すべての企業が一律に同じ脆弱性診断を受けなければならない」わけではありません。ただし、★4では第三者評価の一部として技術検証（脆弱性検査）が行われるため、脆弱性診断に相当する技術的な確認が制度上明確に組み込まれています。★3では技術検証そのものは実施されませんが、広く認知された脆弱性を悪用する一般的な攻撃への備えが前提となるため、脆弱性管理や更新管理を実効的に運用できていることが重要です。

そのため、企業がSCS評価制度への対応を検討するときは、「診断をやるか、やらないか」だけで判断するのではなく、取得を目指す★の水準、対象となるIT基盤、インターネット公開資産、取引先から求められるセキュリティ水準を整理したうえで、必要な技術検証を設計する必要があります。

この記事で分かること

- SCS評価制度と脆弱性診断の関係
- ★3と★4で求められる技術確認の違い
- 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
- 診断対象を決めるときの実務上の判断基準
- 診断結果をSCS評価制度の証跡として活かすための考え方
- 費用や期間を左右する要因と、社内稟議で説明すべきポイント

SCS評価制度とは

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、サプライチェーンを構成する企業のセキュリティ対策状況を一定の基準で可視化する制度です。制度運営は独立行政法人情報処理推進機構（IPA）が担い、★3・★4は2027年3月の登録申請受付開始が予定されています。

★3は、広く認知された脆弱性などを悪用する一般的なサイバー攻撃への対処を想定した水準です。★4は、供給停止や重要情報の漏えいなど、サプライチェーンに大きな影響を与える攻撃への対応を想定しており、組織的対策だけでなく、システム防御、検知、インシデント対応、復旧まで含む包括的な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「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

SCS評価制度に脆弱性診断は必要なのか

★3では技術検証は実施されない

IPAが公表している評価スキームでは、★3は「専門家確認付き自己評価」です。登録希望組織が自己評価を行い、SCSセキュリティ専門家が文書を確認します。★3の評価プロセスには、★4で行われる実地審査や技術検証は含まれていません。

したがって、★3取得のために外部の脆弱性診断会社による診断を必ず実施しなければならない、と単純に理解するのは適切ではありません。ただし、★3は一般的な脆弱性を悪用する攻撃を想定した水準であり、OS、ミドルウェア、ネットワーク機器、クラウドサービス等の脆弱性を把握し、必要な更新・緩和策を実施する管理体制は重要です。

★4では技術検証として脆弱性検査が行われる

一方、★4では評価機関による第三者評価が行われ、文書確認、実地審査に加えて「技術検証（脆弱性検査）」が実施されます。IPAは、★4の技術検証について、登録希望組織が管理する適用範囲内のIT基盤等に対して脆弱性検査を実施すると説明しています。

この点は、SCS評価制度と脆弱性診断の関係を理解するうえで最も重要です。★4を目指す企業では、規程やチェックリストだけでなく、実際のシステムに重大な弱点が残っていないかを技術面から確認されます。

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

出典：IPA「SCS評価制度の評価用ガイド等を公開」 https://www.ipa.go.jp/pressrelease/2026/press20261028.html

★3と★4で脆弱性診断の位置づけはどう違うか

項目	★3	★4
評価方式	専門家確認付き自己評価	評価機関による第三者評価
文書確認	あり	あり
実地審査	なし	あり
技術検証	なし	あり（脆弱性検査）
主な実務ポイント	脆弱性管理の仕組みと運用証跡を整える	技術検証を前提に対象機器・公開資産・是正計画を整理する

重要なのは、★3で技術検証がないからといって、脆弱性対策が不要になるわけではないことです。逆に★4では、単に「定期的に診断しています」と説明するだけでは不十分で、評価対象と診断対象が整合しているか、発見された脆弱性をどのように是正しているかまで説明できる状態が求められます。

★4の技術検証では何を確認されるのか

IPAの2026年10月公開資料では、★4の技術検証は、評価機関または技術検証事業者が実施する手続きとして具体化されています。制度の初期設計では、インターネットに公開されている機器のうち、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とする考え方が示されています。典型例としてVPN装置やルータなどが挙げられています。

つまり、SCS評価制度における技術検証は「企業が保有するすべてのシステムを網羅的に診断すること」と同義ではありません。企業が定めた適用範囲から、重要性やリスクを踏まえて対象を選び、検証する仕組みです。

診断対象の候補になりやすいシステム

実務上は、外部から直接アクセス可能なVPN装置、ファイアウォール、ルータ、リモートアクセス基盤、公開サーバー、クラウド上の公開サービスなどを優先的に確認することが考えられます。また、自社の事業特性によっては、顧客情報を扱うWebシステムや取引先と連携するAPI、重要な業務ポータルなども、別途診断の必要性を検討すべき対象です。

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の違い

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Webシステムのアプリケーション層を対象に、認証・認可の不備、入力値処理の問題、セッション管理の不備、APIのアクセス制御不備などを確認する診断です。インターネット向けの顧客サイトや取引先向けポータルが重要資産である場合、SCS対応とは別に実施価値が高い施策です。

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、公開ポート、暗号設定など、システム基盤側の弱点を確認します。SCS評価制度の★4で想定される技術検証との親和性が高く、特にインターネット公開資産の既知脆弱性や設定不備を確認する場面で重要になります。

ペネトレーションテスト

ペネトレーションテストは、個々の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・情報到達が可能かを検証するテストです。SCS評価制度の★4取得のために、すべての企業が必ずペネトレーションテストまで行うと制度上決められているわけではありません。一方、重要システムや高い事業リスクを持つ企業では、診断結果の深掘りや経営リスクの可視化に有効です。

脆弱性診断を実施しない場合に起こり得る問題

脆弱性診断を必要以上に形式的な作業として捉えると、規程は整っているのに実際の機器には既知脆弱性が残る、公開不要なポートが開いている、古いVPN機器が放置される、といったギャップが生じます。

この状態では、SCS評価制度への対応以前に、取引先との接続環境や顧客情報を扱うシステムを経由してインシデントが発生する可能性があります。ランサムウェアなどでは、外部公開機器の既知脆弱性が初期侵入に悪用されるケースがあるため、脆弱性情報の収集、パッチ適用、設定見直し、技術的検証を一連の管理プロセスとして設計することが重要です。

SCS評価制度を見据えた脆弱性診断の進め方

1. まずSCS評価制度の適用範囲を決める

最初に決めるべきなのは診断ツールではなく、SCS評価制度の取得単位と適用範囲です。対象拠点、対象事業、ネットワーク、クラウド環境、関連する委託先を整理し、どこまでを評価対象とするかを明確にします。対象範囲が曖昧なまま診断を発注すると、必要なシステムが抜けたり、逆に不要な対象まで診断して費用が膨らんだりします。

2. 資産一覧と外部公開資産を棚卸しする

情報システム部門は、サーバー、ネットワーク機器、VPN、クラウドサービス、ドメイン、グローバルIP、Webアプリケーション、APIなどを棚卸しします。特にインターネット公開資産は、攻撃者から直接到達可能なため優先度が高くなります。

3. 診断種類をリスクに応じて選ぶ

外部公開VPNやネットワーク機器を中心に確認するならプラットフォーム診断、顧客向けWebサービスを確認するならWebアプリケーション診断、侵入後の横展開まで確認したい場合はペネトレーションテストというように、目的に合わせて選択します。SCS評価制度への対応だけを理由に、すべての診断メニューを一律に発注する必要はありません。

4. 結果を「指摘一覧」で終わらせず、是正計画に落とす

報告書には、脆弱性の内容だけでなく、影響、再現条件、優先度、推奨対策、対象資産、対応責任者、期限を整理できる情報が必要です。SCS評価制度の実務では、診断を実施した事実より、発見事項を適切に是正できているかのほうが重要です。

5. 必要に応じて再診断する

重大な脆弱性を修正した場合は、修正が正しく反映されているかを再診断で確認します。設定変更やパッチ適用による副作用もあるため、単なる「対応済み」という社内記録ではなく、技術的な確認結果を残すことで証跡の信頼性が高まります。

実施前に準備しておきたい資料

診断ベンダーやSCS対応支援会社へ相談する前に、資産一覧、ネットワーク構成図、外部公開IP一覧、システム構成図、利用クラウド一覧、委託先一覧、脆弱性管理ルール、パッチ適用ルール、過去の診断報告書、過去のインシデント記録などを準備しておくと、対象範囲の決定が進めやすくなります。

既にISMSや取引先監査への対応で資料を整備している企業は、それらを流用できる場合があります。新しい制度だからといって、すべてをゼロから作成する必要はありません。

診断結果をSCS評価制度の証跡として活かすポイント

証跡として重要なのは、「診断を実施した」という1枚の完了証明だけではありません。対象範囲、実施日、実施方法、発見事項、リスク評価、是正状況、再確認結果まで追える状態にしておくことが望まれます。

また、診断対象がSCS評価制度の適用範囲と一致しているかを確認します。例えば、評価対象の中心が本社ネットワークとVPN環境であるにもかかわらず、診断実績がコーポレートサイトだけでは、重要なリスクを十分に説明できない可能性があります。

費用や期間を左右する要因

脆弱性診断の費用や期間は、IP数、サーバー数、Web画面数、API数、認証の有無、クラウド環境、検証深度、報告書の粒度、再診断の有無などによって変わります。SCS評価制度の技術検証に関する費用も、評価機関や技術検証事業者のサービス内容によって異なるため、一律の金額を想定するのは適切ではありません。

予算策定では、「診断費」だけではなく、診断前の棚卸し、設定変更、パッチ適用、機器更新、規程整備、是正後の再診断、外部専門家への相談なども含めて見積もる必要があります。特に古いVPN装置やサポート切れOSが残っている場合、診断そのものより機器更新費用のほうが大きくなることがあります。

社内稟議で説明すべき内容

経営層への説明では、「SCS評価制度取得のための診断」という狭い目的だけではなく、取引継続、顧客データ保護、ランサムウェア対策、事業停止リスクの低減という経営上の目的と結び付けることが重要です。

稟議資料では、対象システム、診断の目的、診断しない場合のリスク、想定費用、是正費用の予備枠、実施時期、取引先から求められている期限を整理します。これにより、診断が「IT部門だけのコスト」ではなく、取引・事業継続のための投資であることを説明しやすくなります。

脆弱性診断会社・SCS支援会社の選び方

ベンダー選定では、SCS評価制度の要求事項を理解しているか、診断結果を制度対応の証跡や是正計画に接続できるかを確認します。診断だけを実施して大量の指摘一覧を渡すだけでは、制度対応や経営判断に活かしにくい場合があります。

RFPや見積依頼では、診断対象、手法、手動診断の範囲、停止リスクへの配慮、緊急連絡体制、報告書サンプル、再診断条件、機密情報の取り扱い、再委託の有無、診断後の是正支援まで確認しておくとよいでしょう。

よくある失敗と注意点

診断を一度実施して終わりにする

脆弱性は新たに公表され続けます。制度取得前に一度診断しただけで長期間放置すると、診断後に公開された脆弱性への対応が抜けます。診断と日常的な脆弱性管理を分けず、継続的な運用として設計する必要があります。

重要な公開資産が診断対象から抜ける

情シスが把握していないクラウド環境、部門独自のWebサービス、買収した会社の公開システムなどが抜けることがあります。診断前の資産棚卸しが不十分だと、最も危険な資産が対象外になる可能性があります。

重要度ではなく件数だけで是正する

脆弱性の件数が多いからといって、すべて同じ優先順位で対応する必要はありません。インターネットから悪用可能か、重要データへ到達できるか、既知の悪用事例があるか、代替対策があるかを踏まえて優先順位を決めます。

Librus株式会社が提供できる支援

Librus株式会社では、SCS評価制度への対応を、チェックリストへの回答だけで終わらせず、現状把握、適用範囲の整理、要求事項とのギャップ分析、規程・証跡整備、技術対策、脆弱性診断、ペネトレーションテスト、是正計画、継続運用まで一気通貫で支援できます。

企業ごとのシステム構成や取引関係に応じて、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必要性を整理し、過剰な診断を避けながら、制度対応と実際のリスク低減の両方につながる計画を設計します。

また、経営層、情報システム部門、営業・調達部門の間で目的や優先順位がずれている場合には、技術的な指摘を経営リスクや取引リスクに翻訳し、社内稟議や取引先説明に利用できる形へ整理することも可能です。

よくある質問

Q1. ★3でも脆弱性診断は必須ですか？

★3では★4のような技術検証は評価プロセスに含まれていません。ただし、脆弱性管理や更新管理などの対策は必要です。自社のリスクに応じて診断を実施することは有効です。

Q2. ★4では必ず脆弱性診断を受けますか？

★4では第三者評価の一部として技術検証（脆弱性検査）が行われます。具体的な対象や方法は、IPAの★4技術検証ガイド等に基づいて評価機関・技術検証事業者と調整します。

Q3. Webアプリケーション診断をすれば★4の技術検証を満たせますか？

一律には言えません。SCS評価制度の適用範囲や技術検証対象と、Webアプリケーション診断の対象が一致する必要があります。公開VPNやネットワーク機器が重要対象であれば、Web診断だけでは不足する可能性があります。

Q4. ペネトレーションテストは必須ですか？

制度上、すべての★4取得企業にペネトレーションテストが一律必須とされているわけではありません。重要資産や事業リスクに応じて、より深い検証が必要な場合に検討します。

Q5. 過去に実施した脆弱性診断結果は使えますか？

対象範囲、実施時期、診断方法、是正状況などによります。古すぎる診断や対象がずれている診断は、現在の状態を示す証跡として十分でない場合があります。

Q6. 診断で脆弱性が見つかると★を取得できないのですか？

不適合が見つかった場合でも、適切な是正を行い、必要な確認を受けることで取得につなげられる仕組みが示されています。重要なのは発見を避けることではなく、適切に管理・是正できることです。

Q7. 診断対象がまだ決まっていなくても相談できますか？

可能です。むしろ、資産棚卸しや適用範囲の決定前に相談することで、不要な診断を避け、SCS評価制度と実際の事業リスクに合った対象を設計しやすくなります。

まとめ｜SCS評価制度では「診断の実施」より、リスクに合った技術確認と是正が重要

SCS評価制度における脆弱性診断の位置づけは、★3と★4で異なります。★3では技術検証は行われませんが、一般的な脆弱性を悪用する攻撃への備えが必要です。★4では第三者評価の一部として技術検証（脆弱性検査）が行われるため、技術的な確認が制度上明確に求められます。

ただし、SCS評価制度への対応は「診断を受ければ完了」ではありません。適用範囲を決め、資産を把握し、リスクに応じた診断を選び、発見事項を是正し、その結果を継続的な脆弱性管理へつなげることが重要です。

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にはそれぞれ異なる役割があります。自社の事業、取引先から求められる水準、公開資産、重要データを踏まえて、必要な施策を選択することが、コストを抑えながら実効性のあるSCS評価制度対応につながります。

SCS評価制度と脆弱性診断の進め方に迷った段階からご相談いただけます

SCS評価制度への対応を検討していても、「★3と★4のどちらを目指すべきか分からない」「どのシステムを診断対象にすべきか判断できない」「既存の診断結果が証跡として使えるのか確認したい」といった段階では、具体的な発注内容を決めることが難しいケースがあります。

Librus株式会社では、対象範囲が固まっていない段階から、現状のセキュリティ対策や取引先要件を整理し、必要な診断・技術対策・規程整備を優先順位付きで設計できます。診断だけでなく、発見事項の改善や運用まで一気通貫で整理することで、SCS評価制度への対応を実際のリスク低減と取引先への説明力向上につなげることができます。

参考情報

- IPA「SCS評価制度の詳細情報」 https://www.ipa.go.jp/security/scs/details.html
- IPA「要求事項・評価基準」 https://www.ipa.go.jp/security/scs/requirements-criteria.html
- IPA「よくある質問」 https://www.ipa.go.jp/security/scs/faq.html
- IPA「SCS評価制度の評価用ガイド等を公開」 https://www.ipa.go.jp/pressrelease/2026/press20261028.html
- 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」 https://www.meti.go.jp/policy/netsecurity/scs.html

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