SCS評価制度とペネトレーションテストの関係｜技術検証で確認すべき内容

SCS評価制度への対応を検討する企業の中には、「★4を取得するにはペネトレーションテストが必須なのか」「脆弱性診断と何が違うのか」と疑問を持つ担当者も少なくありません。結論から言えば、SCS評価制度★4の公式な技術検証は、ペネトレーションテストそのものを必須としているわけではありません。IPAの「★4 技術検証ガイド」では、インターネットとの境界に設置されたVPN装置、ルータ、ファイアウォール等を対象に、外部から脆弱性診断を行い、CVSS基本値7.0以上の脆弱性がないことを確認する仕組みが示されています。

一方、ペネトレーションテストは、実際の攻撃者に近い視点で複数の弱点を組み合わせ、侵入や権限拡大、横展開が可能かを検証する手法です。したがって、SCS評価制度の技術検証とペネトレーションテストは目的と範囲が異なります。ただし、SCS対応を「評価に通るための作業」で終わらせず、取引先や事業継続に影響する実際の攻撃リスクまで低減したい場合、両者を適切に組み合わせることには大きな意味があります。

この記事では、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）における技術検証の正式な位置づけと、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、実施前の準備、ベンダー選定、費用・期間を左右する要因まで、実務の観点から解説します。

この記事で分かること

- SCS評価制度★4で求められる「技術検証」の正式な内容
- 脆弱性診断とペネトレーションテストの違い
- SCS評価制度対応でペネトレーションテストを活用する場面
- 技術検証の対象範囲、準備資料、実施時の注意点
- 診断会社・支援会社を選ぶ際の確認事項

SCS評価制度とは

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し、取引先間で必要な対策水準を共有しやすくするための制度です。企業規模や業種を限定する制度ではなく、サプライチェーンを構成する幅広い企業が対象となり得ます。制度は任意ですが、実際の取引では、委託元企業が取引条件として特定の★水準を求めることが想定されています。

2026年11月時点で、★3は専門家確認付き自己評価、★4は第三者評価という評価スキームです。★4では文書確認や実地審査に加えて技術検証が行われます。技術検証は、規程や運用記録だけでは判断しづらいIT基盤の技術的な状態を確認するための工程です。

出典：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）」
https://www.ipa.go.jp/security/scs/index.html

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

SCS評価制度★4の技術検証で何を確認するのか

SCS評価制度★4の技術検証では、評価基準No.4-4-4-3への適合状況を確認するため、脆弱性診断またはそれに相当する証跡の確認が行われます。対象は、適用範囲内のIT基盤のうち、脆弱性を悪用された場合に攻撃の起点となり得るインターネット境界のネットワーク機器です。

対象となる主な機器

IPAの技術検証ガイドでは、外部から直接アクセス可能なVPN装置、ルータ、ファイアウォール、その他これらに類する通信制御機能を有する機器を対象としています。つまり、SCS★4の技術検証は、社内の全サーバーや全Webアプリケーションを網羅的に診断するものではありません。まずSCS評価制度上の適用範囲を決め、その中から条件に該当するインターネット境界機器を整理する必要があります。

確認する脆弱性の基準

診断方式は外部診断です。対象機器へ外部から疑似的な攻撃通信を行い、CVSSの基本値が7.0以上の脆弱性が存在しないかを確認します。CVSSとは、脆弱性の深刻度を共通尺度で数値化する仕組みです。基本値7.0以上は一般に「High」以上に該当し、悪用された場合の影響が大きい脆弱性として優先的な対応が必要になります。

技術検証で脆弱性が検出された場合は、是正対応を行い、必要に応じて再診断やリスク低減策の確認が行われます。したがって、評価直前に初めて診断を行うより、事前に脆弱性を洗い出し、修正期間を確保しておく方が現実的です。

出典：IPA「★4 技術検証ガイド（SCS-430）」
https://www.ipa.go.jp/security/scs/rcu1hd0000007a2i-att/SCS-430-vuln-assess-guide-v1.0.pdf

技術検証とペネトレーションテストは同じではない

ここはSCS評価制度対応で特に誤解しやすい点です。★4の技術検証は、公式ガイド上「脆弱性診断」を中心とした手続きとして定義されています。一方、ペネトレーションテストは、発見した脆弱性や設定不備を組み合わせて、実際にどこまで侵入・権限拡大・横展開できるかを確認する攻撃シナリオ型の検証です。

項目	**SCS★4技術検証**	脆弱性診断	ペネトレーションテスト
主目的	指定された評価基準への適合確認	既知の脆弱性や設定不備の発見	攻撃経路・侵入可能性・影響の実証
主な対象	インターネット境界の対象機器	Web、サーバー、NW機器等	重要システムや想定攻撃シナリオ
手法	外部からの脆弱性診断	ツール＋手動確認等	攻撃者視点の手動検証を中心に実施
SCSでの位置づけ	★4の第三者評価の一部	技術検証の中核となる手法	必須手法ではないが補完的に有効

たとえば、VPN装置に既知の深刻な脆弱性が残っているかを確認するのはプラットフォーム診断の領域です。一方、そのVPNを突破した後に社内ネットワークへどこまで侵入できるか、認証情報の再利用によって重要サーバーまで到達できるかを確かめるのは、ペネトレーションテストの領域になります。

SCS評価制度対応でペネトレーションテストを実施する意味

ペネトレーションテストがSCS★4技術検証の必須手法ではないからといって、SCS対応と無関係というわけではありません。むしろ、取引先から見た事業影響が大きい企業や、機密情報・重要データを多く扱う企業では、制度要求への適合確認に加えて、現実の攻撃シナリオに対する耐性を確認することに意味があります。

複数の弱点が組み合わさったときのリスクを把握できる

個々の設定不備が単独では中程度のリスクでも、複数の弱点が連鎖すると重大な侵入につながる場合があります。例えば、公開システムの設定不備、弱い認証、過剰な権限、ネットワーク分離不足が連鎖すれば、外部から重要情報へ到達できる可能性があります。ペネトレーションテストは、このような「攻撃経路」を検証する点に強みがあります。

経営層へリスクを説明しやすくなる

経営会議や投資稟議では、「脆弱性が何件あるか」だけでは優先順位を判断しにくいケースがあります。「この経路を使うと受発注システムまで侵入可能」「この認証情報が奪われると顧客データへアクセスできる」といった事業影響まで示すと、予算や改善優先度を説明しやすくなります。SCS対応を経営リスク管理へ接続するうえで、ペネトレーションテストは有効な材料になります。

SCS評価制度の技術検証に向けて準備すべきこと

1. SCS評価制度の適用範囲を決める

最初に、どの事業・拠点・IT基盤をSCS評価制度の対象とするかを明確にします。評価対象を曖昧にしたまま診断を先に発注すると、診断した機器が評価対象外だったり、逆に重要な境界機器が漏れたりする可能性があります。事業上の重要性、取引先との関係、機密情報の所在を踏まえて範囲を定めることが重要です。

2. インターネット境界機器を棚卸しする

技術検証事業者は、対象機器について製造元、モデル、グローバルIPアドレス、利用ポート、OS・ファームウェアのバージョンなどの情報を確認します。VPN、ファイアウォール、ルータ、クラウド上の境界機能などが誰の管理下にあるかも整理してください。外部サービス事業者の管理下にある場合、診断許可や免除条件の検討が必要になることがあります。

3. 診断実施の許可と責任範囲を整理する

脆弱性診断ではポートスキャンなどの疑似的な攻撃通信を行うため、実施許可、責任範囲、秘密保持について事前に合意する必要があります。特に本番環境では、負荷や予期しないサービス影響を考慮し、夜間・休日・メンテナンス時間帯に実施するかを判断します。

4. 是正期間を含めたスケジュールを確保する

診断結果に重大な脆弱性が含まれていた場合、ファームウェア更新、設定変更、機器更改、代替的なリスク低減策などが必要になります。調達や変更申請を伴う場合は数週間以上かかることもあります。第三者評価の直前に診断を行うのではなく、「事前診断→是正→再確認→正式評価」という順序で余裕を持つことが重要です。

ペネトレーションテストの対象範囲はどう決めるか

SCS評価制度対応と並行してペネトレーションテストを行う場合、闇雲に全システムを対象にする必要はありません。事業停止や情報漏えいが取引先に波及する経路を優先して対象を決めると、費用対効果が高まります。

例えば、インターネット公開資産から社内基盤への侵入経路、VPNなどリモートアクセス環境、特権ID管理、Active Directory等の認証基盤、顧客情報や設計情報を扱う重要システム、取引先とネットワーク接続している領域などが候補になります。Webサービスが重要な入口となる場合には、Webアプリケーション診断を先行させ、発見事項を踏まえてペネトレーションテストのシナリオを設計する方法もあります。

Webアプリケーション診断・プラットフォーム診断との使い分け

Webアプリケーション診断は、認証、入力処理、アクセス制御、セッション管理などWebアプリケーション固有の弱点を確認します。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、公開ポート、既知の脆弱性などを確認する手法です。SCS★4技術検証は後者に近く、インターネット境界機器に対する外部脆弱性診断が中心です。

一方、ペネトレーションテストは、診断で見つかった弱点を含め、攻撃者が目的を達成できるかを検証します。したがって、三者は競合するサービスではなく、確認したいリスクに応じて組み合わせるものです。

技術検証で発見された問題の優先順位付け

SCS評価制度では評価基準への適合が重要ですが、実務ではすべての問題を同じ優先度で扱うべきではありません。CVSSだけでなく、インターネットからの到達可能性、悪用コードの公開状況、対象資産の重要度、認証の有無、代替対策の有無、取引先や事業継続への影響を合わせて判断します。

例えば、インターネットに公開されたVPN装置に高深刻度の脆弱性があり、悪用が確認されている場合は、優先度を高く設定すべきです。一方、同じCVSSでも外部から到達できず、追加の制御が機能している場合は、事業影響を踏まえた是正計画を立てる余地があります。

実施期間と費用を左右する要因

SCS★4の技術検証自体は対象機器が一定のルールで選定されるため、診断対象数を整理しやすい一方、全体の準備期間は企業ごとに異なります。費用・期間を左右する主な要因は、適用範囲の複雑さ、対象機器数、複数拠点の有無、クラウドや外部サービスの利用状況、診断可能時間帯、脆弱性発見後の再診断、ペネトレーションテストを追加するかどうかです。

ペネトレーションテストは、シナリオ数や対象ネットワークの規模、内部侵入後の検証範囲、ソーシャルエンジニアリングを含むかなどで工数が大きく変わります。見積依頼時には、「SCS技術検証対応」と「追加のペネトレーションテスト」を分けて範囲・成果物・前提条件を確認すると比較しやすくなります。

診断会社・支援会社を選ぶときのチェックポイント

SCS評価制度対応では、単にペネトレーションテストの技術力だけでなく、制度要件に沿って評価準備を進められるかを確認する必要があります。★4の技術検証を正式に実施する主体については、IPAが指定する技術検証事業者の制度があります。2026年度の指定機関は2026年12月下旬に公表予定とされています。

- SCS評価制度の要求事項・評価基準と★4技術検証ガイドを理解しているか
- プラットフォーム診断とペネトレーションテストの役割を区別して提案できるか
- 対象範囲の整理、資産棚卸し、証跡整備まで支援できるか
- 重大な脆弱性が見つかった後の是正支援・再診断まで対応できるか
- 機密情報、診断データ、認証情報の保管・廃棄方法が明確か
- 経営層向けと技術担当者向けの双方に説明可能な報告書を提供できるか

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

よくある失敗と注意点

「ペネトレーションテストをやれば★4技術検証になる」と考える

通常のペネトレーションテストを実施しただけで、SCS★4技術検証を自動的に代替できるわけではありません。公式ガイドには、過去1か月以内に同等以上の範囲で脆弱性診断を実施し、その実施事業者が技術検証事業者として指定を受けている場合など、免除に関する条件が定められています。既存の診断実績を活用したい場合は、評価機関と早期に確認する必要があります。

診断対象の資産一覧が整っていない

グローバルIPアドレスやネットワーク機器の管理者が分からない状態では、対象範囲の確定に時間がかかります。特に複数拠点、クラウド、通信事業者管理機器が混在する企業では、資産棚卸しを先行させることが重要です。

診断結果を報告書のまま放置する

診断の価値は、問題を発見することではなく、事業リスクに応じて是正し、再発しにくい運用へつなげることにあります。パッチ適用だけでなく、変更管理、脆弱性情報の継続監視、定期診断、アクセス制御、インシデント対応体制などへ反映する必要があります。

社内稟議で説明すべきポイント

SCS評価制度対応の稟議では、「セキュリティを強化するため」という抽象的な目的だけでなく、取引継続、受注条件、サプライチェーン上の信用、事故発生時の事業停止リスクと結び付けて説明すると判断されやすくなります。

技術検証やペネトレーションテストについては、対象範囲、目的、期待する成果、実施リスク、作業時間帯、発見事項の是正費用、再診断の有無を事前に示してください。特に本番システムを対象とする場合は、業務影響を抑えるための実施条件も承認事項に含めるべきです。

Librus株式会社が提供できるSCS評価制度対応支援

Librus株式会社では、SCS評価制度への対応を、制度要件の確認だけで終わらせず、実際のセキュリティリスクの低減まで一気通貫で支援します。企業ごとの事業、IT環境、取引先との関係を踏まえ、★3・★4のどの水準を目指すべきか、どこまでを適用範囲とするかを整理したうえで、ギャップ分析、規程・証跡整備、リスクアセスメント、技術対策へつなげます。

また、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支援、インシデントレスポンス、教育・訓練まで対応できるため、評価前の準備から改善・運用まで分断せずに設計できます。経営層向けには取引継続や事業影響の観点で、情報システム部門には技術・運用の観点で整理し、社内の合意形成を支援します。

よくある質問

Q1. SCS★4を取得するにはペネトレーションテストが必須ですか？

必須ではありません。IPAの★4技術検証ガイドでは、インターネット境界の対象機器に対する外部脆弱性診断を中心に、CVSS基本値7.0以上の脆弱性の有無を確認します。ペネトレーションテストは、より実践的な攻撃経路を確認する補完的な施策として活用できます。

Q2. ★3でも技術検証は必要ですか？

★3は専門家確認付き自己評価であり、★4の第三者評価に含まれる技術検証と同じ手続きが必須になるわけではありません。ただし、要求事項への適合や実態把握のため、事前に脆弱性診断を実施することは有効です。

Q3. Webアプリケーション診断は**★4**技術検証に含まれますか？

公式の技術検証は、主にインターネット境界のVPN装置、ルータ、ファイアウォール等が対象です。Webアプリケーション診断は別の観点の検証であり、重要なWebサービスを運営している場合には追加対策として有効です。

Q4. 既に実施した脆弱性診断を技術検証に使えますか？

一定の条件を満たす場合は、過去の診断実績を証跡として免除申請できる仕組みがあります。実施時期、診断範囲、実施事業者の指定状況などの条件があるため、評価機関への確認が必要です。

Q5. 技術検証で脆弱性が見つかったら**★4**は取得できませんか？

検出後に是正し、再診断やリスク低減策の確認を経て適合判定へ進む手続きが用意されています。重要なのは、是正に必要な期間を見込んで早めに検証することです。

Q6. ペネトレーションテストはどのタイミングで行うべきですか？

SCS評価前のギャップ分析後に、事業上重要な攻撃シナリオを絞って実施すると効果的です。脆弱性診断で見つかった弱点の実影響を確認したい場合や、★4取得後の継続的な高度化にも適しています。

Q7. SCS対応のためにどの診断サービスを選べばよいか分かりません。

適用範囲、公開資産、重要システム、取引先との接続状況を整理したうえで、プラットフォーム診断、Webアプリケーション診断、ペネトレーションテストの役割を分けて選定します。対象範囲が未確定の段階から支援会社へ相談する方法もあります。

まとめ｜SCS技術検証とペネトレーションテストは目的を分けて活用する

SCS評価制度★4の技術検証は、ペネトレーションテストを必須とする制度ではありません。公式ガイドでは、インターネット境界のネットワーク機器に対して外部脆弱性診断を行い、CVSS基本値7.0以上の脆弱性がないことを確認することが中心です。

一方、ペネトレーションテストは、複数の弱点を組み合わせた攻撃経路や、実際に重要資産まで到達できるかを確認するための手法です。SCS評価制度への適合確認と、実際のサイバー攻撃への耐性確認は目的が異なるため、必要に応じて組み合わせることが重要です。

SCS評価制度対応では、最初から診断メニューを決めるのではなく、適用範囲、取引先から求められる水準、重要資産、既存対策を整理したうえで、必要な技術検証を設計することが、コストと期間の最適化につながります。

SCS評価制度の技術検証・診断範囲の整理からご相談いただけます

「★3と★4のどちらを目指すべきか分からない」「技術検証の対象機器を整理できていない」「脆弱性診断とペネトレーションテストのどちらが必要か判断できない」といった段階でも、Librus株式会社へご相談いただけます。

Librus株式会社では、SCS評価制度の要求事項とのギャップ整理から、対象範囲の設定、必要資料・証跡の整理、リスクアセスメント、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、改善計画の策定まで、企業ごとの環境に応じて支援します。先に評価対象と優先順位を整理することで、不要な診断や重複投資を避けながら、取引先への説明に耐え得る対策計画を作りやすくなります。

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