SCS評価制度への対応状況を確認するには？ ギャップ分析と現状診断の進め方

結論から言えば、**SCS**評価制度への対応状況を正確に把握するには、要求事項を読んで「できている／できていない」を自己申告するだけでは不十分です。適用範囲を決め、規程や台帳などの証跡を確認し、実際の運用がルールどおり行われているかを確かめ、必要に応じて技術的な検証も組み合わせる必要があります。ギャップ分析の目的は、★取得の可否を早急に断定することではなく、現在地を可視化し、限られた予算と人員で何から改善すべきかを判断できる状態にすることです。

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（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共通の基準で評価・可視化する制度です。IPAによれば、★3・★4は2027年3月頃の運用開始が予定されており、★3は専門家確認付き自己評価、★4は第三者評価に加えて実地審査・技術検証を伴います。

本記事では、従業員100～1,000名程度の企業を想定し、SCS評価制度への対応状況を確認するためのギャップ分析・現状診断を、経営判断と実務の双方に役立つ形で解説します。

この記事で分かること

- SCS評価制度におけるギャップ分析と現状診断の意味
- ★3・★4を見据えた適用範囲の決め方
- 現状診断で確認すべき資料・証跡・運用実態
- 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を使う場面
- 未対応項目を経営リスクと結び付けて優先順位付けする方法
- 社内稟議、RFP、外部ベンダー選定で確認すべきポイント

SCS評価制度における「ギャップ分析」とは

ギャップ分析とは、**SCS**評価制度の要求事項・評価基準と、自社の現状との差分を整理する作業です。ここで重要なのは、規程が存在するかどうかだけを見るのではなく、「誰が責任を持つのか」「定期的に運用されているか」「証跡が残っているか」「技術的に有効か」まで確認することです。

IPAが公開している★3・★4の要求事項・評価基準は、ガバナンス、リスクの特定、取引先管理、攻撃等の防御、攻撃等の検知、インシデント対応、復旧といった領域を横断して確認する構造です。★3・★4を取得するには、それぞれで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。そのため、一部の技術対策だけを強化しても、組織的な運用や証跡が不足していれば取得準備としては不十分です。

なぜ今、現状診断を始める必要があるのか

SCS評価制度は**2027**年**3**月頃の運用開始が予定されていますが、準備は制度開始後に始めればよいとは限りません。取引先から★取得を求められた時点で、社内規程、資産台帳、アクセス権限、委託先管理、ログ、バックアップ、インシデント対応手順などが未整備であれば、短期間での是正は難しくなります。

また、SCS評価制度は二社間の取引契約等で、委託元が委託先に適切な段階（★）を提示し、対策を促すことを想定しています。つまり、制度対応は情報システム部門だけのテーマではなく、営業、調達、法務、経営企画、内部監

査、事業部門にも関係します。取引先からセキュリティ水準を問われた際に、回答に必要な資料が部署ごとに分散していること自体が、実務上の大きなギャップになり得ます。

現状診断をしないまま対応を進めると起こりやすい問題

対策の優先順位を誤る

新しいセキュリティ製品の導入が目立つ一方、退職者アカウントの削除手順や委託先管理、バックアップ復元テストなど、基本的な運用が後回しになるケースがあります。SCS対応では、要求事項全体を俯瞰してボトルネックを見つけることが重要です。

「規程はあるが運用されていない」状態を見落とす

情報セキュリティ規程に年1回のアクセス権レビューと書かれていても、実施記録が残っていなければ評価時に説明しにくくなります。現状診断では文書と実態を突き合わせる必要があります。

技術対策の有効性を過大評価する

WAFやEDRを導入済みでも、設定不備、監視対象外、アラート放置、脆弱な管理画面の公開などがあればリスクは残ります。構成確認や脆弱性診断を通じて、導入済み対策が実際に機能しているか確認する視点が必要です。

稟議や予算化が遅れる

「SCS対応が必要」という説明だけでは投資判断が難しくなります。現状診断で不足項目、事業影響、対策費用、実施順序を整理すると、経営層に説明しやすくなります。

最初に決めるべきは「何を診断対象にするか」

現状診断で最も初期に判断すべき事項は適用範囲です。 全社を一括で見るのか、特定事業・拠点・IT基盤・顧客向けサービスを対象とするのかによって、必要資料、関係部署、工数、費用が大きく変わります。

特に、取引先の機密情報を扱うシステム、受発注に関わる基幹システム、インターネット公開サーバ、クラウド管理基盤、VPNやリモートアクセス環境、重要拠点のネットワークなどは、サプライチェーンへの影響を踏まえて優先的に確認すべき候補です。M&AやIPO、重要取引の更新前であれば、その場面で説明責任が生じる範囲を優先して診断する考え方もあります。

SCS評価制度へのギャップ分析・現状診断の進め方

STEP1：対象範囲と目標水準を決める

まず、★3を目指すのか、★4を視野に入れるのか、取引先から具体的な要求があるのかを確認します。★3は一般的なサイバー脅威に対処しうる水準として専門家確認付き自己評価、★4はサプライチェーンへの影響が大きい企業・資産を想定し、第三者評価・実地審査・技術検証を伴います。なお、★3を先に取得しなければ★4を取得できない制度ではありません。

STEP2：要求事項と自社統制を対応付ける

各要求事項に対し、どの社内規程、手順、システム、担当部署が対応しているかをマッピングします。1つの要求事項に複数部署が関係する場合は、責任部署と証跡保管場所も明確にします。

STEP3：文書と証跡を収集する

情報セキュリティ基本方針、組織図、IT資産台帳、アカウント管理台帳、委託先一覧、リスク評価記録、教育記録、ログ監視記録、インシデント対応手順、バックアップ・復元テスト記録などを収集します。規程の有無だけでなく、実施記録があるかを確認します。

STEP4：関係者ヒアリングで運用実態を確認する

情報システム部門だけでなく、経営層、総務、人事、調達、営業、開発、事業部門などにヒアリングします。例えば「退職時にアカウントを何日以内に止めるか」「外部委託先の権限を誰が棚卸しするか」といった具体質問にすると、運用上の抜けを見つけやすくなります。

STEP5：技術面の実装状況を確認する

設定確認、ログ確認、Webアプリケーション診断、プラットフォーム診断などを必要に応じて実施します。インターネット公開資産の脆弱性、不要ポート、古いソフトウェア、認証設定、アクセス制御などを確認し、文書上のルールと実環境が一致しているかを見ます。

STEP6：ギャップを分類し、是正優先度を決める

不足を「未整備」「一部整備」「運用不十分」「証跡不足」「技術的有効性に懸念」などに分類します。その上で、事業影響、悪用可能性、取引先要求、是正難易度を掛け合わせて優先順位を付けます。

STEP7：改善ロードマップと経営報告に落とし込む

短期、中期、継続運用に分けて計画化します。すぐに対応できるアカウント棚卸しと、予算が必要なログ基盤整備やネットワーク更改を同じ扱いにしないことが重要です。

現状診断では「適合・不適合」以外も見る

実務では、次の4つの観点をセットで評価すると、改善計画につながりやすくなります。

確認軸	確認する内容	典型的な問題
証跡	規程、台帳、記録、承認履歴が残っているか	実施しているが記録がない
運用実態	ルールが定期的に実行されているか	棚卸しが担当者依存で止まっている
技術的有効性	設定・監視・脆弱性対策が実際に機能しているか	EDR導入済みだが未監視端末がある
経営管理	責任者、報告、改善判断が機能しているか	リスクが経営会議に上がらない

脆弱性診断・ペネトレーションテストはどこで使うか

Webアプリケーション診断

顧客向けWebサービス、会員サイト、管理画面、APIなどについて、SQLインジェクション、認証・認可不備、クロスサイトスクリプティング等の脆弱性を確認します。現状診断では、インターネット公開資産に対する防御が文書どおり実装されているかを確かめる材料になります。

プラットフォーム診断

OS、ミドルウェア、ネットワーク機器、クラウド公開設定などを確認します。不要ポート、古いソフトウェア、弱い暗号設定、管理インターフェースの公開など、基盤側の弱点を洗い出すのに有効です。

ペネトレーションテスト

単一の脆弱性の有無だけでなく、複数の弱点を組み合わせてどこまで侵入・権限拡大・情報到達が可能かを検証します。★4では技術検証が制度上求められるため、重要資産への攻撃経路を理解する観点で、より実践的な検証が重要になります。ただし、具体的な技術検証の範囲は制度の正式な評価手順や対象環境に沿って設計する必要があります。

経営層が現状診断で判断すべき事項

経営層が判断すべきなのは、技術的な脆弱性の個数ではなく、どのギャップが事業継続・取引・信用に影響するかです。例えば、顧客データを扱うシステムの重大な脆弱性、バックアップ復元不能、インシデント時の意思決定者不在、主要委託先の管理不備などは、取引停止やサービス停止につながる可能性があります。

社内稟議では「制度対応費」だけにしない

稟議では、①現状の主要ギャップ、②想定される事業影響、③取引先要求との関係、④対応しない場合のリスク、⑤改善後の状態、⑥必要費用・期間、⑦継続運用費をセットで説明すると、単なる認証・制度対応費ではなく、事業継続と取引基盤を守る投資として説明しやすくなります。

現状診断の期間・費用を左右する要因

期間や費用は一律ではありません。特に次の要因で大きく変わります。

- 対象拠点・システム・クラウド環境の数
- ★3のみか、★4を見据えるか
- 規程・台帳・証跡の整備状況
- ヒアリング対象部署の数
- Webアプリケーション診断やプラットフォーム診断等の技術検証を含めるか
- 委託先・再委託先の数
- 是正支援や再診断まで含めるか

従業員数だけで見積もるのではなく、対象となるIT基盤と業務プロセスを整理した上で見積依頼を行う方が、後から追加費用が生じにくくなります。

現状診断の成果物に含めたい項目

単なる「○×一覧」では、その後の改善に使いにくくなります。実務で使える成果物には、少なくとも以下の要素を含めることが望まれます。

- 対象範囲と前提条件
- 要求事項ごとの現状評価
- 確認した証跡と不足証跡
- 運用上の課題
- 技術的な課題
- リスク・事業影響
- 是正優先度
- 推奨対応と担当部署
- 対応期限の目安
- 再確認方法

ギャップ分析・現状診断を依頼する会社の選び方

制度理解と技術評価の両方を確認する

SCS評価制度は、ガバナンスや証跡確認だけでなく、IT基盤の防御・検知、インシデント対応、サプライチェーン管理まで横断します。制度文書だけに詳しい支援会社、あるいは脆弱性診断だけを得意とする会社ではなく、両方をつなげて評価・改善できるかを確認するとよいでしょう。

RFP・見積依頼で確認したい項目

- 対象範囲の決め方を支援できるか
- 要求事項ごとの証跡確認まで含むか
- 技術診断の実施範囲と方法
- 経営層・関係部署へのヒアリングを含むか
- ギャップの優先順位付け方法
- 是正支援・再診断まで対応できるか
- 機密情報・個人情報の取り扱いとデータ保管方法
- 成果物を社内稟議や取引先説明に使える形で提供できるか

SCS評価制度の現状診断でよくある失敗

チェックシートを埋めることが目的になる

回答欄を埋めても、根拠となる証跡や運用実態が伴わなければ改善にはつながりません。

情報システム部門だけで完結させる

取引先管理、人事異動、教育、契約、インシデント時の対外説明などは他部署の関与が不可欠です。

全部を同時に直そうとする

重大な事業影響がある項目から優先し、短期是正と中長期投資を分ける方が実行可能性が高まります。

診断後に再確認しない

改善策を実施しても、設定変更ミスや運用定着不足が残ることがあります。再診断や定期レビューまで計画に含めることが重要です。

Librus株式会社が支援できること

Librus株式会社では、**SCS**評価制度への対応を「チェックシート作成」だけで終わらせず、現状把握から改善・運用まで一気通貫で支援します。企業ごとの事業、IT環境、取引先要求を踏まえ、対象範囲の整理、ギャップ分析、規程・証跡確認、リスクアセスメント、技術診断、改善ロードマップ作成、運用定着まで個別に設計します。

必要に応じて、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、SOC／CSIRT構築、インシデントレスポンス、教育・訓練、SBOM、M&AにおけるIT・サイバーセキュリティデューデリジェンスなどを組み合わせることで、制度対応と実際のセキュリティ強化を分離せずに進められる点が特徴です。

よくある質問

Q1. まず★3と★4のどちらを目指すべきですか？

取引先要求、自社のサプライチェーン上の役割、扱う情報・システムの重要性を基に判断します。★3は一般的な脅威への最低限の対策水準、★4はより包括的な対策と第三者評価・技術検証を伴う水準です。

Q2. ギャップ分析だけ先に実施できますか？

可能です。対象範囲や目標水準が確定していない段階でも、現状診断によって主要な不足を可視化し、その結果を基に目標水準を決める方法があります。

Q3. ISMSを取得していればSCS対応は不要ですか？

別制度であるため、ISMS取得だけでSCS評価制度の適合を自動的に判断することはできません。既存の規程・統制を活用しつつ、SCSの要求事項との差分確認が必要です。

Q4. 脆弱性診断は必須ですか？

★3の評価を単純に「脆弱性診断必須」と言い切ることは適切ではありません。ただし、公開システムやIT基盤の防御状態を実証的に確認する方法として有効です。★4では技術検証が評価スキームに含まれます。

Q5. 現状診断にはどの資料を準備すればよいですか？

情報セキュリティ規程、組織図、資産台帳、アカウント管理、委託先一覧、教育記録、ログ監視、インシデント対応、バックアップ関連の資料から始めるとよいでしょう。

Q6. 取引先から要求されてから始めても間に合いますか？

規程整備、システム改修、予算化、教育、証跡蓄積には時間がかかるため、要請前に主要ギャップだけでも把握しておく方が対応しやすくなります。

Q7. 一度診断すれば十分ですか？

十分ではありません。組織変更、新システム導入、委託先変更、脆弱性の発見などにより状態は変わるため、継続レビューと必要に応じた再診断が重要です。

まとめ｜SCS評価制度対応は「現在地の可視化」から始める

SCS評価制度への対応で最初に必要なのは、製品導入でも申請書作成でもなく、自社の現在地を正確に把握することです。要求事項と社内統制を対応付け、証跡、運用、技術的有効性、経営管理の観点からギャップを確認すれば、何を先に改善すべきかが明確になります。

特に、取引先との接続環境、顧客情報を扱うシステム、インターネット公開資産、委託先管理、インシデント対応、バックアップ・復旧などは、事業継続や信用に直結します。SCS評価制度への準備をきっかけに、制度取得だけでなく、自社のサイバーリスク管理そのものを強化することが重要です。

SCS評価制度への対応状況が分からない段階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決まっていない」「要求事項を読んでも、自社のどの規程・システムが対応しているか整理できない」「取引先から要請される前に主要な不足だけ把握したい」といった段階でも、現状診断から進めることができます。Librus株式会社では、制度要件と実際のIT環境・業務運用を照らし合わせ、優先順位の高い課題から改善計画に落とし込みます。対象範囲や実施方法が未確定でも、必要な準備を整理することで、過剰な対策や手戻りを抑えながら、取引先への説明や将来の★取得に備えられます。

参考情報

IPA「**SCS**評価制度」
https://www.ipa.go.jp/security/scs/index.html

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

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

IPA「不正アクセスによる漏えい等の事案を踏まえ、速やかに実施すべき対策等について」
https://www.ipa.go.jp/security/security-alert/2026/alert20261009.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