

SCS評価制度対応で必要になる社内規程・証跡・セキュリティ対策とは？

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）への対応では、「情報セキュリティ規程を作れば終わり」ではありません。重要なのは、要求事項に沿ったルールを整備し、そのルールが実際に運用されていることを証跡で説明でき、さらに必要な技術対策がシステムに実装されている状態をつくることです。

結論からいえば、SCS評価制度への準備は「規程」「運用証跡」「技術対策」の3つを同時に進める必要があります。規程だけが整っていても運用実績がなければ評価で説明しにくく、逆にツールを導入していても責任者や運用ルールが曖昧であれば、組織的な対策として不十分になる可能性があります。

IPAが公表している制度構築方針では、★3はセキュリティ専門家による確認を伴う自己評価、★4は第三者評価に加えて実地審査と技術検証を行う仕組みです。★4の実地審査では、脆弱性管理の体制・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などについて、証跡確認を含む評価が想定されています。

本記事では、従業員100～1,000名程度の企業を想定し、SCS評価制度への対応で準備すべき社内規程、証跡、セキュリティ対策、社内での進め方、診断やペネトレーションテストの位置づけまで実務的に解説します。

この記事で分かること

- SCS評価制度で「規程・証跡・技術対策」がセットで必要になる理由
- 準備しておきたい主な社内規程と、実際の運用を示す証跡の例
- ★3と★4で意識すべき評価方法の違い
- 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をどこで活用するか
- 経営層・情報システム部門・現場部門が分担して進める方法
- 取得準備で起こりやすい失敗と、外部支援会社を選ぶ際のポイント

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共通の基準で可視化し、発注者と受注者の双方が取引上必要な対策水準を判断しやすくすることを目的とした制度です。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。

制度では、一般的なサイバー攻撃への対応を想定した★3と、より包括的なガバナンス・検知・インシデント対応・取引先管理などを求める★4が設けられています。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。

対象は単一のWebサイトだけではありません。制度構築方針では、メールサーバ、Webサーバ、認証基盤、クラウド環境などを含む企業のIT基盤を対象としており、組織のガバナンス、取引先管理、自社IT基盤への防御・検知など、組織全体に影響する範囲を扱います。したがって、SCS評価制度対応は、情報システム部門だけの技術プロジェクトではなく、全社的な管理体制の整備と考える必要があります。

なぜ「社内規程・証跡・セキュリティ対策」の3点が必要なのか

SCS評価制度では、要求事項を満たしていると説明するために、方針やルール、実際の運用、技術的な実装が矛盾なくつながっていることが重要です。例えば「脆弱性を適切に管理する」という方針があっても、誰が情報を収集し、何日以内に対応を判断し、対応結果をどこに記録するかが決まっていなければ、実運用として安定しません。

逆に、EDRや多要素認証、バックアップ製品を導入していても、その対象範囲、例外管理、定期確認、障害時の復旧手順が整理されていなければ、対策が継続的に機能していることを説明しにくくなります。評価を意識するなら、「ルールに何を書くか」「誰が運用するか」「何を証跡として残すか」を一体で設計する必要があります。

SCS評価制度対応で準備したい主な社内規程

必要な文書名は企業によって異なります。既存のISMS文書や就業規則、IT運用手順がある場合は、それを活用できるケースもあります。重要なのは文書名ではなく、要求事項に対して必要なルールが明文化され、責任者と運用方法が明確になっていることです。

情報セキュリティ基本方針・管理規程

経営としてセキュリティに取り組む方針、適用範囲、責任体制、従業員の義務などを定めます。担当部署だけでなく、役員・管理職・従業員の責任と権限が分かる状態にしておくことが重要です。IPAが公開する★3ベースのセキュリティアセスメント資料でも、セキュリティ推進を担当する部署・役員・従業員を決定し、責任と権限を割り当てることや、自社のセキュリティ対応方針を策定し周知することが確認項目として示されています。

アクセス管理・アカウント管理規程

入退社・異動時のアカウント作成と削除、特権IDの管理、認証方式、パスワード、多要素認証、定期的な権限棚卸しなどを定めます。実務では、人事部門と情報システム部門の連携フローまで決めると証跡を残しやすくなります。

脆弱性・パッチ管理規程

OS、ネットワーク機器、VPN装置、クラウドサービス、Webアプリケーションなどについて、脆弱性情報の収集、影響判断、優先順位付け、パッチ適用、例外承認までの流れを決めます。重大な脆弱性が公表された際に「誰が、何を確認し、いつまでに対応するか」を具体化しておくことがポイントです。

ログ管理・監視規程

どのシステムのログを取得するか、保存期間、確認頻度、アラート発生時の対応、調査権限などを整理します。ログはインシデント発生後の原因調査だけでなく、日常の監視が実施されていたことを示す証跡にもなります。

インシデント対応規程

不審メール、マルウェア感染、アカウント侵害、情報漏えい、ランサムウェアなどが発生した際の連絡経路、初動、封じ込め、経営報告、顧客・取引先への連絡、フォレンジック調査、再発防止までの手順を定めます。★4の实地審査ではインシデント対応手順の確認が想定されているため、文書だけでなく訓練や対応記録も重要になります。

バックアップ・事業継続関連規程

バックアップ対象、取得頻度、保管場所、世代管理、復元テスト、災害・サイバー攻撃時の復旧優先順位を整理します。バックアップが存在するだけでなく、実際に復元できることを定期的に検証することが重要です。

委託先・取引先管理規程

外部委託先やクラウドサービスの選定、契約時のセキュリティ条件、再委託、定期評価、事故発生時の報告義務などを定めます。★4では、事業継続や情報管理の観点から自社に影響を及ぼす可能性のある重要な取引先について、セキュリティ対策状況を把握する考え方が示されています。

教育・誓約・秘密情報管理に関する規程

従業員教育の対象・頻度・受講管理、秘密保持義務、機密情報の分類、持ち出しや共有ルールなどを定めます。教育資料を配布するだけでなく、受講履歴や理解度確認を証跡として残せる仕組みにしておくといでしょう。

「証跡」として準備したいもの

証跡とは、規程に書かれたルールが実際に実行されていることを示す記録です。評価対応では、証跡が「存在する」だけでなく、対象期間・対象範囲・責任者が説明できることが重要です。代表的なものは次のとおりです。

- 組織図、役割分担表、責任者の任命記録、経営会議やセキュリティ委員会の議事録
- アカント一覧、権限棚卸し記録、入退社時のアカウント削除記録、特権ID利用記録
- 資産台帳、ソフトウェア一覧、外部公開IP・ドメイン・クラウド環境の一覧

- 脆弱性情報の確認記録、パッチ適用記録、脆弱性診断報告書、是正完了記録
- EDR・SIEM・ファイアウォール等の設定画面、アラート確認記録、ログレビュー記録
- インシデント対応訓練の実施記録、机上演習の記録、過去のインシデント対応票
- バックアップジョブの結果、復元テスト記録、BCP訓練結果
- 委託先一覧、選定時チェック結果、契約条項、定期評価結果、再委託先の確認記録
- セキュリティ教育資料、受講記録、標的型メール訓練結果、秘密保持誓約書

証跡を後から集めようとする、担当者ごとに保管場所が異なる、ログが保存期間を過ぎている、承認記録がメールに散在している、といった問題が起こりがちです。申請直前ではなく、ギャップ分析の段階から「どの要求事項を、どの証跡で説明するか」を一覧化しておくことが有効です。

SCS評価制度で意識したい主なセキュリティ対策

資産の把握と適用範囲の確定

最初に、PCやサーバだけでなく、クラウド、SaaS、ネットワーク機器、VPN、認証基盤、外部公開Webサイト、委託先が運用する環境などを棚卸しします。SCS評価制度では取得希望組織が適用範囲を決定し、その中からサンプリングして評価する考え方が示されているため、範囲の決め方が後工程に大きく影響します。

認証・アクセス制御の強化

管理者アカウントやクラウド管理画面、VPN、メールなど重要システムでは、多要素認証や最小権限、不要アカウントの削除、特権IDの分離などを進めます。特に退職者アカウントの残存や共有IDの常態化は、規程と実態の乖離が起こりやすいポイントです。

脆弱性管理とパッチ適用

OSやミドルウェア、ネットワーク機器の更新に加え、外部公開資産を定期的に確認します。VPN装置やルータなどインターネットから到達可能な機器は攻撃の入口になり得るため、脆弱性情報を継続的に追跡し、重大度と自社への影響に基づいて対応を優先します。

エンドポイント・ネットワークの防御と監視

EDR、アンチマルウェア、ファイアウォール、メール対策、ネットワーク分離、ログ監視などを組み合わせます。製品を導入するだけでなく、アラートを誰が確認し、重大な検知をどのようにエスカレーションするかまで運用設計することが重要です。

バックアップと復旧

ランサムウェア等を想定し、重要データのバックアップを取得し、攻撃者から容易に削除・暗号化されない構成を検討します。定期的な復元テストによって、RTO(目標復旧時間)やRPO(目標復旧時点)に照らして事業を再開できるか確認します。

インシデント対応と訓練

連絡網や手順書を整備したうえで、実際のシナリオを使った机上演習や訓練を行います。例えば「VPNの脆弱性が悪用され管理者アカウントが侵害された」「取引先を装うメールからマルウェアに感染した」といった想定で、初動判断、システム隔離、取引先報告、経営判断まで確認します。

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位置づけ

SCS評価制度への対応では、規程整備だけでなく技術的な弱点が残っていないか確認することも重要です。ただし、診断の種類ごとに目的が異なります。

Webアプリケーション診断

公開Webシステムや業務Webアプリケーションに対し、認証不備、アクセス制御不備、SQLインジェクション、クロスサイトスクリプティングなどの脆弱性を確認します。取引先情報や個人情報扱うシステムでは、事業影響と合わせて優先度を判断します。

プラットフォーム診断

サーバ、ネットワーク機器、VPN、公開ポート、OSやミドルウェアなどの脆弱性や設定不備を確認します。★4の技術検証では、インターネット公開機器のうち、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した脆弱性検査が想定されています。

ペネトレーションテスト

単一の脆弱性の有無だけではなく、実際の攻撃者を想定し、複数の弱点を組み合わせで重要情報や重要システムに到達できるかを検証します。SCSの要求を満たすために常にペネトレーションテストが必須という意味ではありませんが、重要なシステムや高リスクな取引を抱える企業では、実際の侵入経路を把握する手段として有効です。

SCS評価制度対応を進める実務ステップ

1. 取得する★と適用範囲を決める

取引先からの要求、扱う情報、事業継続上の重要性、外部からの接続関係などを整理し、★3か★4か、どの事業・拠点・IT基盤を対象とするかを決めます。経営層には、取得目的と取引上の必要性を説明します。

2. 要求事項と現状のギャップを可視化する

要求事項ごとに「適合」「一部対応」「未対応」を判定し、根拠となる規程・証跡・システム設定を紐づけます。この段階で、単に文書の不足だけでなく、運用が定着していない項目や技術的な不足も洗い出します。

3. 優先順位を付けて是正計画を作る

外部から攻撃されやすい箇所、重要情報への影響、取引継続への影響、是正にかかる期間を踏まえて優先順位を付けます。VPNや外部公開サーバの重大脆弱性、管理者アカウントの多要素認証未導入など、侵害に直結しやすい項目は早期対応が必要です。

4. 規程改定と技術対策を並行して進める

文書チームとITチームを分離しすぎると、規程に書いた運用がシステムで実現できないケースがあります。規程案、運用フロー、システム設定を同時に確認し、実行可能なルールにします。

5. 証跡を蓄積する

改定したルールを一定期間運用し、棚卸し、教育、ログ確認、バックアップ、脆弱性管理などの記録を残します。証跡のファイル名、保存先、対象期間、責任者を統一すると審査準備が効率化します。

6. 評価・審査を想定した事前確認を行う

★3では専門家確認付き自己評価、★4では第三者評価・実地審査・技術検証を想定し、要求事項と説明資料の対応関係を確認します。担当者へのヒアリングで回答がばらつかないか、操作画面やログをすぐ提示できるかも確認します。

経営層・情報システム部門が準備すべきこと

経営層は、SCS評価制度を「認証取得のためのコスト」だけで評価せず、取引継続、顧客からの信頼、事業停止リスク、サイバー事故時の損失を含めて判断する必要があります。特に★3では経営層による自己適合宣誓が評価プロセスに含まれるため、現場任せにせず、未対応事項と残存リスクを理解しておくことが重要です。

情報システム部門は、資産台帳、構成図、アカウント・権限一覧、外部公開資産、脆弱性管理記録、バックアップ・ログ監視の運用状況を整理します。また、法務・総務・人事・購買部門と連携し、秘密保持、従業員教育、委託先管理、退職者対応などIT部門だけでは完結しない項目を確認します。

社内稟議では、取得の目的、対象範囲、取引先から求められる水準、現状のギャップ、対応しない場合の取引・事業継続リスク、初期費用と継続運用費、社内工数を説明すると、単なるセキュリティ投資ではなく事業基盤整備として理解されやすくなります。

実施期間・費用を左右する要因

準備期間は、既存のセキュリティ管理体制やISMS等の整備状況、対象拠点・システム数、未対応項目の数、社内承認のスピードによって変わります。既存規程や運用記録が整理されている企業は比較的短期間で進めやすい一方、資産台帳が未整備、委託先一覧がない、アカウント管理が属人化している、といった状態では準備に時間を要します。

費用も、コンサルティングだけでなく、MFA・EDR・ログ管理などの製品導入、脆弱性診断、ネットワーク改修、バックアップ強化、教育・訓練など必要な是正内容に左右されます。見積依頼時は、単に「SCS取得支援一式」とするのではなく、ギャップ分析、規程整備、技術対策、証跡整備、評価前レビュー、診断の範囲を分けて確認すると比較しやすくなります。

支援会社を選ぶ際のチェックポイント

- SCS評価制度の要求事項だけでなく、実際のIT基盤や攻撃手法を理解しているか
- 規程作成だけで終わらず、設定変更・診断・改善・運用まで支援できるか
- 経営層向けの説明と、情報システム担当者向けの技術支援の両方に対応できるか
- Web、ネットワーク、クラウド、認証基盤、委託先管理などを横断的に評価できるか
- 機密情報や構成情報、診断結果の取り扱いルールが明確か
- 評価を行う立場と取得支援を行う立場の中立性・公平性について説明できるか

特に、規程作成と技術診断を別々の会社に依頼する場合は、発見事項が規程・運用改善に反映される仕組みを確認してください。診断結果を受け取るだけで終わると、審査時に「どのように是正し、再発防止したか」を説明できない可能性があります。

よくある失敗と注意点

テンプレートの規程をそのまま採用する

自社の組織やシステム構成に合わない規程は、実際に運用できません。実態と異なる承認フローや担当部署名が残っていると、審査時の説明にも矛盾が生じます。

証跡を申請直前に集める

運用実績が必要な項目は、過去の記録が残っていなければ短期間では補えません。早い段階から証跡の保存ルールを決めることが重要です。

ツール導入だけで対応したと考える

MFAやEDRの導入は有効ですが、対象外端末、例外ユーザー、アラート未確認など運用上の穴が残る可能性があります。設定と運用の双方を確認します。

適用範囲を必要以上に広げる

範囲を広げるほど、確認するシステム・拠点・証跡も増えます。一方で、取引上重要なシステムを不自然に除外すると説明が難しくなります。取引関係とリスクに基づいて合理的に決定することが重要です。

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、チェックシートへの回答支援だけで終わらせず、要求事項の整理、現状分析、規程整備、技術対策、診断、改善、運用まで一気通貫で支援します。企業ごとのIT環境や取引関係に応じて、必要な対策を個別に設計できる点が特徴です。

例えば、現状のギャップ分析から始め、経営層向けに優先順位と投資判断を整理し、情報システム部門には具体的な改善計画を提示します。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・運用支援、インシデントレスポンス、教育・訓練まで連携させることが可能です。

SCS評価制度は、規程・証跡・技術対策のどれか一つだけを整備すればよい制度ではありません。経営、組織、ITの三つをつなげる必要があるため、「何から着手すべきか分からない」「ISMSの既存文書をどこまで流用できるか知りたい」「診断が必要な範囲を決めたい」といった初期段階から整理することが有効です。

よくある質問

Q1. SCS評価制度では規程を新しく作り直す必要がありますか？

必ずしもすべてを新規作成する必要はありません。既存の情報セキュリティ規程、ISMS文書、IT運用手順などが要求事項を満たしていれば活用できます。ただし、実態と文書が一致しているか、必要な証跡が残る運用になっているかを確認する必要があります。

Q2. ISMSを取得済みなら、証跡もそのまま使えますか？

活用できる可能性はありますが、自動的にSCS評価制度の要求事項を満たすとは限りません。SCSの要求事項・評価基準と既存のISMS文書・記録を対応付けて確認することが必要です。

Q3. ★3でも証跡は必要ですか？

はい。★3は専門家確認付き自己評価で、セキュリティ専門家が取得希望組織の作成した書類を確認します。自己評価の根拠として、規程や運用記録を整理しておく必要があります。

Q4. ★4ではどのような証跡が特に重要ですか？

制度構築方針では、実地審査で脆弱性管理の体制・プロセス、インシデント対応手順、事業継続要件に沿った復旧準備などについて証跡確認を含む評価が想定されています。適用範囲に応じて、操作画面、ログ、台帳、訓練記録、診断結果などを説明できる状態にしておくことが重要です。

Q5. Webアプリケーション診断は必須ですか？

対象システムや要求事項との関係によります。SCS制度全体として常に特定の診断メニューが一律必須という意味ではありませんが、外部公開システムに脆弱性がないかを確認することは、実際のリスク低減と証跡整備の双方に有効です。

Q6. ペネトレーションテストまで実施した方がよいですか？

重要資産や高リスクな外部接続がある場合には有効です。単なる脆弱性の列挙ではなく、攻撃者がどこまで到達できるかを確認できるため、優先すべき改善策を判断しやすくなります。

Q7. 対応は情報システム部門だけで完結しますか？

完結しません。人事、総務、法務、購買、事業部門、経営層などとの連携が必要です。特に教育、秘密保持、委託先管理、事業継続、経営判断は複数部門にまたがります。

Q8. まだ対象範囲や取得する★が決まっていなくても相談できますか？

はい。取引先から求められている条件、扱う情報、システム構成、事業への影響を整理し、どの範囲から着手するべきかを検討する段階から外部専門家を活用できます。

まとめ：SCS評価制度対応は「文書作成」ではなく「運用できる仕組みづくり」

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）への対応では、社内規程、運用証跡、技術対策を一体として整えることが重要です。規程はルールを示し、証跡はルールが実行されていることを示し、技術対策は実際の攻撃リスクを低減します。

特に★4では、文書確認だけでなく実地審査と技術検証が想定されています。申請直前に文書を整えるのではなく、資産・適用範囲の整理、ギャップ分析、優先順位付け、規程改定、技術対策、証跡蓄積、診断・再確認までを計画的に進めることが現実的です。

SCS評価制度への対応を、単なる取得プロジェクトではなく、取引先からの信頼確保、事業継続、事故時の損失低減につながる経営基盤の整備として捉えることで、制度運用開始後も継続的に活用できるセキュリティ体制を構築しやすくなります。

SCS評価制度対応の現状整理からご相談いただけます

「どの規程が不足しているか分からない」「証跡として何を残せばよいか判断できない」「★3と★4のどちらを目指すべきか決まっていない」といった段階でも、準備を始めることは可能です。Librus株式会社では、現状の規程・システム・運用を確認し、要求事項とのギャップ、優先して改善すべき項目、必要な診断や技術対策を整理します。対象範囲や実施方法が固まっていない場合も、取引先との関係や事業リスクから優先順位を明確にすることで、過不足のない準備につながられます。SCS評価制度への対応方針を検討している企業は、初期整理の段階からご相談ください。

主な出典

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>

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・内閣官房国家サイバー統括室「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に関する制度構築方針」：
<https://www.ipa.go.jp/security/scs/rcu1hd0000007ajp-att/20260327001-br.pdf>

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>