# SCS審査で求められる証跡とは規程だけでは足りない理由

ログ・台帳・申請記録・教育記録・議事録を、審査で説明できる状態へ

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）の準備では、規程を作るだけでは十分ではありません。審査や確認で問われるのは、定めたルールが対象範囲で実際に運用され、その結果を第三者が追跡できるかどうかです。規程は「何をするか」を示しますが、ログ、資産台帳、申請・承認記録、教育記録、会議議事録などの証跡は「実際にしたこと」を示します。

結論から言えば、証跡整備の要点は、要求事項ごとに「ルール・実施・結果・改善」を一本の線でつなぐことです。大量のスクリーンショットを直前に集めるのではなく、日常業務から証跡が自然に残る仕組みをつくる必要があります。本稿では、従業員100〜1,000名規模の企業を想定し、証跡の種類、整理手順、審査で説明しやすい判断基準、技術検証との関係まで実務的に解説します。

## この記事で分かること

- SCS評価制度で規程だけでは足りない理由
- ログ、台帳、申請記録、教育記録、議事録を証跡として成立させる条件
- ★3と★4を見据えた準備の違いと、証跡台帳の作り方
- 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証跡につなげる方法
- 準備期間・費用を左右する要因と、支援会社を選ぶ際の確認事項

## SCS評価制度と「証跡」の基本

### SCS評価制度は何を評価する制度か

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を共通の基準で評価・可視化し、委託元と委託先の双方が適切な対策水準を判断しやすくする制度です。IPAの公式説明では、委託先への攻撃に起因する事業・サービスの提供途絶、機密情報の漏えい・改ざん、委託先を踏み台とした不正侵入などのリスクを対象にしています。全てのサプライチェーン企業が対象とされ、特にリソースの限られる中小企業での活用効果が想定されています。

2026年9月時点の公表情報では、★3は一般的なサイバー脅威に対処できる水準、★4は初期侵入の防御だけでなく、被害拡大の防止や取引先のデータ・システム保護、サプライチェーン上の役割に応じた強靭化策まで含む水準です。★3はセキュリティ専門家の確認を伴う自己評価、★4は評価機関による第三者評価と技術検証が予定されています。★3・★4の運用開始は2027年3月頃の予定です。今後公開される解説書や申請要領によって実務詳細が更新される可能性があるため、申請前には最新版を確認してください。

**出典：**IPA「SCS評価制度」

**出典：**IPA「SCS評価制度の詳細情報」

**出典：**IPA「要求事項・評価基準」

### 証跡とは、運用の事実を再現できる記録

ここでいう証跡とは、ルールに沿った行為やシステム処理が、いつ、誰によって、何を対象に、どのような結果で行われたかを確認できる記録です。文書、システムログ、チケット、メール、ワークフロー履歴、診断報告書など形式は問いません。ただし、単にファイルが存在するだけでは弱く、対象範囲、期間、責任者、承認、結果、例外処理が読み取れることが重要です。

たとえば「退職者のアカウントは速やかに削除する」と規程に書いてあっても、退職者一覧とアカウント削除チケット、実施日時、確認者が結び付かなければ、運用実績を十分に説明できません。反対に、入退社ワークフローからID管理システムへ連携され、削除完了ログと月次照合記録が残るなら、ルールが継続的に機能していることを示しやすくなります。

## なぜ規程だけでは足りないのか

### 規程は設計図であり、運用実績そのものではない

規程は統制の出発点です。しかし、審査対象は規程の文章力ではありません。担当者がルールを認識し、対象システムに対策を実装し、定期的に確認し、問題があれば是正しているかが焦点となります。規程の最終改定日が古い、実際のクラウド利用と記載内容が一致しない、例外承認の手続が形骸化しているといった状態では、文書と実態の不整合が生じます。

★3では専門家が作成書類を確認し、★4では文書確認に加えて実地審査と技術検証が想定されています。また、適用範囲から対象をサンプリングして評価する考え方が示されています。つまり、代表的な一件だけを整えるのではなく、どの拠点・部署・システムが選ばれても、一定品質の証跡が提示できる状態が必要です。

### 証跡が弱いと、実効性と説明責任の両方が崩れる

証跡不足は審査対応の遅れだけでなく、実際のインシデント対応にも影響します。ログの保存期間が不明なら侵入経路を追えず、資産台帳が古ければ脆弱な機器の所在を特定できません。申請記録がなければ過剰権限の付与理由を検証できず、教育記録がなければ対象者の未受講を把握できません。議事録が残っていなければ、経営層がどのリスクを認識し、どの対策を承認したかを説明しにくくなります。

取引先から短期間でSCS評価制度への対応を求められた場合、証跡が分散している企業は収集と整合確認に時間を取られます。回答の遅れや説明のばらつきは、セキュリティ部門だけの問題にとどまらず、入札、契約更新、新規受注、事業継続にも影響し得ます。経営層はSCS対応を「認証の取得費」ではなく、取引維持と説明責任のための経営基盤整備として捉えることが重要です。

# SCS審査に備えて整理すべき主な証跡

## ログ：取得しているだけでなく、確認と対応まで示す

認証ログ、管理者操作ログ、EDRやアンチウイルスの検知ログ、ファイアウォール・VPNログ、クラウド監査ログ、バックアップジョブログなどは、技術対策の稼働状況を示す基礎資料です。ただし、ログが保存されているだけでは、異常を検知して対応する運用までは証明できません。監視ルール、アラートのトリアージ記録、インシデントチケット、月次レビュー結果まで関連付けておくと、検知から対応までを説明できます。

証跡としては、対象システム名、ログ種別、取得元、保存先、保存期間、時刻同期、閲覧権限、レビュー頻度、異常時の連絡先を一覧化します。スクリーンショットだけに依存すると改ざん防止や網羅性を説明しにくいため、可能であれば管理画面からのエクスポート、設定ファイル、チケット番号など原記録へたどれる情報を残します。機密情報や個人情報を含むログは、提出用にマスキングした写しと、原本の保管場所・閲覧手順を分けて管理します。

## 台帳：資産・アカウント・委託先を同じ範囲で管理する

資産台帳は、端末やサーバの一覧だけではありません。クラウドサービス、ネットワーク機器、業務アプリケーション、外部公開資産、ソフトウェア、重要データ、管理者アカウント、委託先との接続点まで含めて考えます。台帳の更新責任者と頻度を定め、購買・入社・異動・退職・廃棄などの業務イベントと連動させることが重要です。

審査で説明しやすい台帳には、識別子、所有部門、管理責任者、用途、重要度、設置・利用場所、OSやバージョン、サポート期限、外部公開の有無、バックアップ、最終確認日を持たせます。すべてを一つの台帳に詰め込む必要はありません。CMDB、端末管理、SaaS管理、契約管理など複数の仕組みを使う場合は、どれを正本とするか、相互の照合方法は何かを明確にします。

## 申請・承認記録：権限付与と例外の妥当性を示す

アカウント発行、特権付与、外部接続、ソフトウェア導入、USBメモリ利用、データ持出し、設定変更などは、申請者、承認者、対象、理由、期限、実施者、完了確認が追跡できる記録を残します。特に期限付きの特権や例外は、失効処理までを一つの案件として管理する必要があります。

ありがちな失敗は、メールで承認を得た後に担当者の受信箱だけへ残るケースです。共有ワークフローやチケットへ集約し、検索可能な案件番号を付けます。緊急変更は事前承認が難しいこともあるため、事後承認の期限、影響確認、ロールバック結果を定めておくと、現実の運用と規程を両立できます。

### 教育記録：受講率だけでなく、対象と改善を説明する

教育記録では、教材名、実施日、対象者、受講結果、未受講者への督促、理解度テスト、追加教育、教材改定履歴を残します。全社員向け研修だけでなく、管理者、開発者、情報システム担当者、インシデント対応要員など役割別教育も整理すると、職務に応じた力量管理を示せます。

標的型メール訓練では、開封率など単一の数字を競うより、報告手順が機能したか、再教育が必要な部門はどこか、次回の改善策は何かを記録する方が実務的です。個人を責める運用にすると報告が遅れるため、教育の目的と個人データの利用範囲を明確にしてください。

### 議事録：経営判断と改善サイクルを残す

経営会議、リスク委員会、情報セキュリティ委員会、インシデント振り返り会議などの議事録は、セキュリティが経営課題として管理されていることを示します。日時と出席者だけでなく、報告されたリスク、判断の根拠、決定事項、予算、責任者、期限、継続課題を記載します。

経営層が判断すべき事項は、取得を目指す段階、適用範囲、受容する残余リスク、重大インシデント時の権限、改善予算、取引先への要求水準です。議事録とリスク台帳、改善計画、次回会議のフォロー結果がつながれば、PDCAが動いていることを説明できます。

## 証跡を審査で使える状態にする6つの手順

### 1. 目標段階と適用範囲を決める

最初に★3または★4のどちらを目指すか、対象とする法人、拠点、部門、業務、システム、委託先を決めます。取引先のデータやシステムへのアクセス、サービス停止時の影響、機密情報の取扱いを基準に境界を引きます。範囲を狭めること自体が目的になると、実際のリスクや取引要件とずれるため、除外理由も記録します。

### 2. 要求事項と証跡を対応付ける

要求事項ごとに、関連規程、実施部門、利用システム、証跡名、保存場所、対象期間、責任者、不足点を整理した証跡台帳を作ります。一つの証跡が複数要件を支える場合も、逆に一つの要件に複数証跡が必要な場合もあります。ファイル名の羅列ではなく、何を証明する資料かを一文で記載します。

### 3. サンプルで一連の流れを再現する

入社者のアカウント発行、重大脆弱性の対応、インシデント訓練など代表的な案件を選び、起点から完了確認まで追跡します。規程、申請、承認、システム反映、レビューの間に欠落があれば、証跡収集ではなく業務プロセスを修正します。

### 4. 証跡の品質を確認する

良い証跡は、真正性、完全性、追跡可能性、期間整合性、再現性を備えます。作成者や日時が分からない、対象範囲が曖昧、編集可能なファイルだけ、別資料との数字が不一致といった問題を点検します。原本、提出用写し、機密情報のマスキングルールも定めます。

### 5. 技術検証で実装を確かめる

★4を見据える場合、文書の整合だけでなく技術的な有効性も確認します。Webアプリケーション診断では認証・認可や入力処理、プラットフォーム診断ではOS・ミドルウェア・ネットワーク機器の設定や既知脆弱性を検証します。ペネトレーションテストでは、現実的な攻撃経路を用いて複数の弱点が連鎖した場合の到達可能性や影響を確認します。対象、前提、実施日、検出事項、リスク評価、是正責任者、再確認結果を報告書と改善台帳へ反映します。

### 6. 定例運用へ組み込む

証跡は審査直前の特別作業にしないことが重要です。月次のアカウント棚卸し、四半期の資産照合、年次教育、変更時のリスク評価など、頻度とトリガーを業務カレンダーへ組み込みます。証跡台帳の更新状況をKPIとして確認し、未完了や例外を会議で扱います。

## 審査準備の期間と費用を左右する要因

準備期間は、従業員数だけでは決まりません。適用範囲の拠点・システム数、クラウドとオンプレミスの混在、委託先数、既存のISMS等の運用状況、台帳の精度、ログ保存期間、規程と実態の差、技術検証の範囲、是正に必要なシステム改修によって変わります。既に運用が定着していても、証跡の保管場所が部門ごとに分散していると収集に時間がかかります。反対に、規程が未整備でも対象範囲が限定され、意思決定が速ければ段階的に進められる場合があります。

実務では、現状把握、ギャップ分析、改善計画、規程・手順改定、ツール設定、運用実績の蓄積、模擬審査の順で進めます。短い準備期間では、設備投資だけを先行させず、取引上の重要度とリスクに基づいて優先順位を付けるべきです。緊急度の高い外部公開資産、多要素認証、特権管理、バックアップ復旧、脆弱性対応、インシデント連絡体制などから着手し、中長期項目は責任者と期限を伴う改善計画にします。

社内稟議では、制度対応そのものに加え、対象となる主要取引、未対応時に想定される契約・入札上の影響、対象範囲、現状ギャップ、必要な社内工数、外部費用、運用開始後の維持費、成果物を説明します。認証・登録取得だけを目的にすると、更新時に再び証跡が不足します。平時の運用品質向上と取引先への説明時間短縮も投資効果に含めると、経営判断につながりやすくなります。

# 支援会社の選び方とRFPで確認すべきこと

SCS評価制度への対応支援会社を選ぶ際は、規程雛形の提供だけでなく、現場の実装、証跡設計、技術検証、改善運用まで支援できるかを確認します。制度要求をそのままチェックリスト化するだけでは、実態とのずれや過剰投資が生じやすいためです。経営層、情報システム部門、総務・人事、開発、営業、購買など複数部門の役割を整理し、現行の稟議やワークフローへ落とし込める会社が適しています。

見積依頼時には、目標段階、対象法人・拠点・システム、重要取引、既存認証、希望時期を共有します。そのうえで、ギャップ分析の方法、成果物、証跡台帳の有無、技術検証の範囲、是正支援、模擬審査、再確認、機密情報の取扱い、再委託、データ保存場所、削除方法、制度更新への対応を確認してください。支援と評価を同じ法人が担う場合の中立性・公平性については今後の制度詳細も確認する必要があります。

成果物には、適用範囲定義書、要求事項別ギャップ一覧、証跡台帳、規程・手順の改定案、技術検証報告書、リスク別の改善計画、経営報告資料、審査時の説明要領を含めると実務で使いやすくなります。報告書は問題点の列挙ではなく、事業影響、悪用可能性、対応難易度、依存関係を踏まえて優先順位を示すことが重要です。

# よくある失敗と注意点

## 審査直前にスクリーンショットを集める

画面証跡は一時点の状態しか示さず、継続運用や母集団全体を説明できないことがあります。設定値のエクスポート、チケット履歴、定期レビュー記録などと組み合わせ、取得日と対象を明記してください。

## 規程と現場で使う手順が別物になっている

規程では情報システム部門の承認が必要でも、現場が独自にSaaSを契約していると、シャドーITが台帳から漏れます。購買・経費精算・SSOの情報を照合し、現実の業務フローに合わせて統制を設計します。

## 証跡の量を品質と取り違える

大量の資料は、かえって矛盾を生みます。要求事項ごとに主証跡と補助証跡を定め、審査者が短時間で結論へ到達できる索引を用意します。最新版、承認済み、対象期間内の資料を優先します。

### 診断を実施して終わる

Webアプリケーション診断やプラットフォーム診断で問題を発見しても、改修、リスク受容、代替統制、再診断の記録がなければ改善サイクルを説明できません。診断結果をチケット化し、責任者と期限を割り当て、残課題を経営層へ報告します。

### 個人情報・機密情報を過剰に提出する

審査用証跡には従業員情報、顧客情報、IPアドレス、認証情報などが含まれ得ます。必要最小限の範囲に絞り、マスキング、暗号化、アクセス制御、受渡し方法、保管期限、返却・削除を事前に合意してください。秘密保持契約だけでなく、実際の取扱手順を確認することが大切です。

## 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）に向けた現状評価から、適用範囲の設計、要求事項とのギャップ分析、規程・手順整備、証跡台帳の構築、改善計画、模擬確認まで一気通貫で支援します。企業ごとのシステム構成、組織体制、取引先要求、予算策定と稟議プロセスを踏まえ、過不足のない進め方を個別に設計します。

特徴は、文書整備だけで終わらない点です。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、SOC／CSIRT構築・運用支援、インシデントレスポンス、デジタルフォレンジック、教育・訓練などを組み合わせ、規程と技術実装、日常運用の整合を確認できます。経営上のリスクを整理しながら、情報システム部門と現場部門の実務へ落とし込むことが可能です。

大企業との取引継続、取引先監査、M&A、IPOなど重要局面では、限られた期間で優先順位を明確にする必要があります。Librus株式会社は、グローバルスタンダードを踏まえつつ、日本企業の意思決定や現場運用に合わせ、取得準備後の改善・継続運用まで見据えて支援します。

## よくある質問

### SCS評価制度では、規程があれば証跡として認められますか。

規程は重要な証跡の一つですが、それだけで運用実績を示すことは困難です。申請・承認記録、ログ、台帳、点検結果、是正記録などを組み合わせ、規程どおりに実施していることを説明します。

### 証跡は何か月分用意すればよいですか。

必要期間は要求事項、運用頻度、今後の申請要領によって異なります。現時点で一律の期間を断定せず、月次・四半期・年次など各統制が少なくとも一度は実施されたことを示せるよう、早めに記録を蓄積してください。

### Excelの台帳でも問題ありませんか。

形式より、正確性、更新責任、変更履歴、アクセス制御、他の記録との整合性が重要です。Excelを使う場合も、正本の保存場所、更新者、承認方法、バックアップを明確にします。

### ★3と★4では証跡準備がどう違いますか。

★3は専門家確認付き自己評価、★4は第三者評価と技術検証が想定されています。★4では文書の整合に加え、実地での運用確認や技術的な有効性を説明できる準備がより重要です。

### ISMSを取得していればSCS対応は不要ですか。

既存のマネジメントシステムや証跡は活用できますが、SCS評価制度の適用範囲と要求事項に照らした確認が必要です。自動的に代替できると決めつけず、差分を整理してください。

### 脆弱性診断は必ず必要ですか。

必要な技術検証は目標段階、対象範囲、システムの性質、最新の制度文書によって判断します。ただし、外部公開Webや基盤の弱点を客観的に把握し、是正まで追跡することは、実効性の説明に役立ちます。

### 証跡が不足している場合、申請を諦めるべきですか。

まず不足を要求事項別に整理し、短期で補える記録と、運用実績の蓄積が必要な項目を分けます。優先度、責任者、期限を設定すれば、段階的に準備できます。

### 対象範囲がまだ決まっていなくても相談できますか。

可能です。主要取引、扱う情報、停止時の影響、外部接続、委託関係を整理し、事業上合理的な範囲を設計するところから進められます。

## まとめ：SCS評価制度対応は「残す運用」から始める

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）で重要なのは、規程を増やすことではなく、決めた対策が現場で実施され、その事実と改善結果を追跡できる状態をつくることです。ログ、台帳、申請記録、教育記録、議事録を要求事項と結び付け、規程・実施・結果・改善の連鎖を示せるようにします。

まずは目標段階と適用範囲を定め、代表的な業務を一件たどってください。途中で承認、実装、確認、是正の記録が途切れるなら、そこが改善の出発点です。制度の最新文書を確認しながら、審査のためだけではなく、取引先への説明、インシデント対応、事業継続に役立つ証跡管理を整えることが、持続的なセキュリティ向上につながります。

## SCS評価制度の準備状況を、証跡から確認しませんか

「どの範囲を対象にすべきか分からない」「規程はあるが、どの記録を証跡として示せるか不安」「★3と★4のどちらを目指すべきか整理したい」といった段階でも相談可能です。Librus株式会社では、制度要求と現場運用の両面から現状を確認し、既存資料を活かせる部分、追加対策が必要な部分、優先順位を整理します。準備範囲や実施方法が固まっていなくても、主要取引やシステム構成を伺い、社内で判断しやすい進め方をご提案します。

## 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