SCS評価制度★3取得実務自己評価から専門家確認まで

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を、申請できる状態まで具体化する実務ガイド

SCS評価制度★3取得は「証跡を先に設計する」と進めやすい

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★3を目指す企業は、自己評価票に回答して終わりではありません。先に適用範囲を定め、要求事項ごとに実施状況を確認できる証跡をそろえ、不足を是正し、セキュリティ専門家の確認・助言・署名を受けます。そのうえで、経営層が自己適合を宣誓し、事務局へ申請するのが基本の流れです。

最も重要なのは、規程の有無ではなく、決めた対策が現場で継続運用されていることを説明できる状態にすることです。たとえば「多要素認証を導入している」という回答だけでは、対象アカウント、例外、設定状況、定期点検の記録が分かりません。自己評価票と証跡の対応関係を最初から台帳化すると、専門家確認での手戻りを減らせます。

この記事で分かること

- ★3の評価方式と、自己評価・専門家確認・経営層宣誓の関係
- 100〜1,000名規模の企業が社内で組むべき体制と実務手順
- 自己評価票にひも付ける証跡、技術確認、是正計画の作り方
- 期間・費用を左右する要因と、支援会社への見積依頼項目
- 申請を目的化せず、取引継続と事業継続につなげる方法

SCS評価制度と★3の位置づけ

取引先の対策水準を共通の尺度で確認する制度

SCS評価制度は、委託元と委託先の間でセキュリティ対策水準を可視化し、サプライチェーン全体の底上げを図る制度です。IPAは、委託元にとっては委託先の対策が見えにくいこと、委託先にとっては発注者ごとに異なるチェックリストへの対応が負担になっていることを背景として挙げています。取引契約等において、委託元が委託先に適切な段階を提示し、対策の実施状況を確認する利用が想定されています。出典：IPA「SCS評価制度」https://www.ipa.go.jp/security/scs/index.html

★3は、一般的なサイバー脅威に対処し得る水準です。★4は初期侵入の防御に加え、侵入後の被害拡大防止やサプライチェーン上の役割に応じた強靭化まで求め、第三者評価と技術検証を伴います。上位段階が下位段階を包含する設計であり、★3を先に取得しなければ★4に進めないわけではありません。出典：IPA「SCS評価制度の詳細情報」https://www.ipa.go.jp/security/scs/details.html

★3は専門家確認付き自己評価

★3では、取得希望組織が要求事項・評価基準に基づく自己評価を作成します。登録された社内外のセキュリティ専門家が内容を確認し、必要に応じて修正を含む助言を行い、提出内容を了承した場合に署名します。その後、取得希望組織は経営層の自己適合宣誓を含む評価結果を事務局へ提出し、申請内容に問題がなければ台帳に登録・公開されます。これは★4の第三者評価とは異なりますが、単なる無確認の自己宣言でもありません。

IPAによると、SCS評価制度のセキュリティ専門家は、所定の資格のいずれかを保有し、制度研修を受講したうえで事務局登録が必要です。資格保有者であれば誰でも直ちに署名できるとは限らない点に注意が必要です。出典：IPA「SCS評価制度の詳細情報」
https://www.ipa.go.jp/security/scs/details.html

なぜ今、★3取得の準備が必要なのか

制度対応の本質は、マークの取得よりも取引先に説明可能な統制を整えることです。製造、物流、IT、業務委託などの現場では、発注元の機密情報や接続権限を委託先が保有します。委託先のVPN装置が未更新で侵入される、保守アカウントの認証情報が窃取される、クラウド共有設定の誤りで設計資料が外部公開される、といった事態は、1社の問題にとどまりません。納品停止、顧客対応、調査費用、契約上の報告、信用毀損へ連鎖します。

特に従業員100〜1,000名の企業では、IT環境が十分に複雑である一方、専任のセキュリティ人員が少ないことがあります。情報システム部門がツール運用を担い、総務が規程を管理し、各事業部がSaaSを契約し、開発部門がWebサービスを運用する構造では、全社としての証拠が一か所に集まりません。★3対応は、この分散を可視化し、責任者、対象、頻度、記録を結び直す機会になります。

対応しない場合に起こり得る問題

SCS評価制度が直ちにすべての企業へ法的義務を課すという意味ではありません。しかし、発注企業が調達条件や契約更新条件として一定段階を求める運用が広がれば、未対応は営業・調達上の説明負担につながります。個別質問票への回答が続く、商談時に改善計画の提出を求められる、重要業務への参画範囲が限定される、といった影響が考えられます。

より直接的な問題は、統制の空白が残ることです。退職者アカウントが停止されていない、バックアップから復旧できるか試していない、インシデント時の連絡先が更新されていない、外部公開資産を把握していない状態は、感染や侵入が発生したときの被害を大きくします。★3の自己評価を、取引のための書類作成ではなく、事業継続上の弱点を発見する仕組みとして使うべきです。

★3の対象範囲はどう決めるか

最初に決めるべき事項は適用範囲です。法人全体を無条件に対象とすると、海外拠点、工場、子会社、レガシー環境まで確認が広がり、証跡収集が止まることがあります。一方、都合のよい一部システムだけに狭めると、取引先が期待する事業や情報処理を含まず、説明価値が下がります。対象となる契約、提供サービス、拠点、組織、情報資産、IT基盤、外部委託先を、サプライチェーン上の役割から逆算してください。

たとえば、大手メーカー向けに保守サービスを提供し、顧客環境へリモート接続する企業なら、当該サービス部門だけでなく、接続端末、ID基盤、VPN、ログ、端末管理、委託保守先、インシデント対応体制まで対象に含める必要があります。EC事業者なら、Webアプリケーション、クラウド基盤、決済・物流連携、顧客データ管理、開発委託先が重要です。

確認軸	対象範囲の決め方	残す資料
事業	取得目的となる取引・製品・サービスを特定	契約、業務フロー、サービス一覧
組織・拠点	運用、開発、営業、管理部門と拠点をひも付け	組織図、責任分担表、拠点一覧
情報・システム	扱う機密情報と処理するIT基盤を洗い出す	資産台帳、データフロー、構成図
外部委託	再委託、クラウド、保守、開発先を含める	委託先台帳、契約、評価記録

SCS評価制度★3取得の実務手順

1. 経営目的と責任者を決める

経営層は、取得理由を『取引先から言われたため』だけにせず、守るべき事業、許容できない停止時間、機密情報、予算枠、リスク受容者を決めます。プロジェクト責任者は情報システム部門に置く場合でも、経営企画、総務・法務、人事、調達、開発、営業を巻き込む必要があります。経営層の宣誓が最後にあるため、開始時と申請前の2回だけではなく、主要な不足事項が判明した時点で判断会議を設けると円滑です。

社内稟議では、制度概要、取得目的、対象範囲、予定時期、担当工数、外部費用、未達項目の改修費、専門家の役割、申請後の維持運用を説明します。診断費だけを予算化し、規程改定や設定変更、端末更新の費用が漏れるケースを避けてください。

2. 資料を収集し、現状を可視化する

自己評価の前に、規程、台帳、構成図、運用記録を集めます。規程が古い場合でも捨てず、現場との差分を確認する材料にします。準備資料の例は、情報セキュリティ方針、組織図、資産・アカウント・委託先台帳、ネットワーク構成図、アクセス権レビュー記録、パッチ適用記録、バックアップ・復旧試験記録、ログ監視記録、教育履歴、インシデント対応手順と訓練記録です。

この段階で証跡台帳を作ります。列には要求事項番号、評価結果、根拠文書、ファイルの保存先、対象範囲、責任部門、確認日、不足、是正担当、期限、専門家コメントを置きます。ファイル名だけでなく、規程の章番号や管理画面の確認箇所まで書くとレビューが速くなります。

3. 自己評価票を作成する

自己評価は、担当者の印象ではなく評価基準と証跡に基づいて行います。『実施済み』と判断する前に、①対象範囲全体へ適用されているか、②責任者と頻度が決まっているか、③例外が管理されているか、④実施記録が残っているか、⑤問題発生時に改善されるかを確認します。部分導入なら、その事実と残余リスクを明記し、適合を先取りしません。

複数部門の回答が食い違った場合は、文書上のルールではなく実運用を確認します。たとえば退職者IDを即日停止する規程があっても、SaaSごとに人事情報が連携されず手作業で漏れているなら、運用証跡と改善が必要です。自己評価票の文章は、第三者が読んでも『何を、誰が、どの範囲で、どの頻度で実施したか』を追えるようにします。

4. 不足事項をリスク順に是正する

不足を同じ優先度で並べると、規程の体裁調整に時間を使い、侵入につながる穴が残ります。優先順位は、インターネットからの悪用可能性、顧客情報・重要業務への影響、攻撃の起こりやすさ、代替策の有無、要求事項への影響、改修所要時間で決めます。外部公開VPNの重大な脆弱性、管理者IDの多要素認証未導入、公開サーバの不要ポート、復旧不能なバックアップは、早期対応候補です。

Webサービスを提供する企業では、Webアプリケーション診断によりSQLインジェクション、認可不備、セッション管理などを確認します。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、クラウド設定の脆弱性を調べます。さらに、複数の弱点を組み合わせて重要資産へ到達できるかを検証する必要があれば、合意した範囲でペネトレーションテストを実施します。これらは★3申請のために機械的に全部行うのではなく、対象範囲とリスクに応じて選びます。診断結果は、深刻度だけでなく、事業影響、悪用条件、改修責任者、期限、代替策、再確認結果まで管理してください。

5. 証跡を整え、模擬レビューを行う

証跡は『存在する資料』ではなく『評価結果を裏付ける資料』です。規程は設計、設定画面は実装、ログやチケットは運用を示します。三者を組み合わせると説明力が上がります。スクリーンショットには取得日、対象システム、取得者を付け、機密情報や個人情報を必要以上に含めません。外部へ共有する前にマスキング、アクセス制御、保存期限、削除方法を合意します。

正式な専門家確認の前に、要求事項ごとに自己評価票から証跡をたどる模擬レビューを行います。リンク切れ、古い日付、対象範囲の不一致、責任者未承認、サンプル不足を洗い出します。専門家への提出パッケージは、適用範囲説明書、自己評価票、証跡台帳、主要証跡、不足事項と是正結果、未解消リスクの扱いで構成すると確認しやすくなります。

6. セキュリティ専門家の確認・助言を受ける

専門家は、自己評価の記載と証跡が評価基準に照らして妥当かを確認し、必要に応じて修正を助言します。署名だけを依頼するのではなく、範囲設定、判断根拠、例外、サンプリング、是正結果まで説明できるレビュー工程を確保してください。社内の専門家を起用する場合も、制度上の登録要件を満たすか、評価対象の運用に関与しすぎて確認の客観性を損なわないかを検討します。

初回打合せでは、専門家の登録状況、対応実績、確認方法、必要資料、レビュー回数、追加費用、機密情報の扱い、成果物、署名条件を確認します。専門家が問題を指摘した場合は、自己評価票を修正し、是正またはリスク判断を行い、差し替えた証跡を再提示します。

7. 経営層が自己適合を宣誓し、申請する

経営層の宣誓は、現場が作った回答への形式的な押印ではありません。経営層は、適用範囲、主要なリスク、未解消事項、例外、必要予算、維持体制を確認し、提出内容に責任を持てるか判断します。申請前の経営報告は、要求事項を一つずつ読み上げるより、重要リスク、是正完了状況、残余リスク、取引への影響、次年度の維持費を中心にまとめると判断しやすくなります。

事務局への提出内容、申請方法、公開項目は最新規程に従います。公開台帳に載ることを前提に、対象範囲の表現が取引先に誤解を与えないかも確認してください。基本規程等はIPAの制度ページから確認できます。出典：IPA「制度規程・委員会」
https://www.ipa.go.jp/security/scs/regulation-advisory-committeess.html

期間と費用を左右する要因

公的資料で一律の取得期間や総費用が保証されているわけではありません。実務上は、現状把握、自己評価、是正、専門家確認、経営承認、申請準備を逆算します。規程と運用記録がそろう企業は短く、資産台帳がない、拠点が多い、ID管理が分散している、レガシー機器が残る、委託先管理が未整備といった企業は長くなります。数週間で書類を整える前提ではなく、技術改修や運用実績を作る期間を含めて計画してください。

費用は、対象範囲、拠点・システム数、自己評価の初期成熟度、規程整備量、診断の要否、是正支援、専門家確認の回数、現地確認、再レビュー、申請後の運用支援で変動します。見積では『コンサルティング一式』ではなく、ギャップ分析、文書作成、証跡整備、診断、是正支援、専門家確認、申請支援を分けて確認すると比較しやすくなります。制度上の申請費用等はIPAの最新案内で確認が必要です。

支援会社・専門家を選ぶ際のチェックポイント

SCS評価制度の説明ができるだけでなく、規程、IT運用、技術検証、経営報告を横断できるかを確認します。自己評価票を埋める支援だけでは、脆弱性や運用不備の是正まで進みません。一方、診断だけでは経営層宣誓や委託先管理の仕組みを整えられません。★3の取得工程全体と、その後の運用を一貫して設計できることが重要です。

- SCS評価制度の最新文書と評価基準を参照しているか
- 専門家確認を担う者の資格・研修・登録状況を明示できるか
- 自己評価の代筆ではなく、根拠と判断過程を残すか
- 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リスクに応じて提案できるか
- 機密情報の取扱い、再委託、保存場所、削除、事故時報告が契約で明確か
- 是正計画、再診断、教育、継続監視まで支援範囲を選べるか

RFPまたは見積依頼には、取得目標、希望時期、対象事業・拠点・システム、従業員数、既存認証、利用クラウド、外部公開システム、過去の診断、希望成果物を記載します。成果物として、ギャップ分析報告書、自己評価票、証跡台帳、適用範囲説明書、是正計画、専門家コメント・署名、経営報告資料、申請書類一覧を確認すると、納品後に何が残るか明確になります。

よくある失敗と注意点

規程を作っただけで適合と判断する

規程は必要ですが、運用記録がなければ実効性を示せません。アクセス権棚卸し、教育、バックアップ復旧試験、脆弱性対応など、定期実施が必要な対策は早めに回し、記録を残します。

適用範囲を後から変える

自己評価の途中で対象システムが増えると、証跡や診断範囲が連鎖して変わります。営業が説明したい取引範囲と、情シスが管理できるIT範囲を開始時にすり合わせてください。

専門家を最後に探す

制度登録された専門家の確保やレビュー日程がボトルネックになり得ます。初期段階で候補を決め、正式確認の前に証跡の粒度や進め方を合意することが有効です。ただし、助言者と最終確認者の関係や客観性については制度規程に従います。

診断結果を申請資料から切り離す

技術診断を実施しても、発見事項の是正記録が自己評価票と結び付いていなければ説明が弱くなります。チケット番号、改修日、再診断結果、例外承認を証跡台帳に戻します。

取得後の維持担当を決めない

組織変更、システム追加、委託先変更、重大インシデントがあれば、評価時点の状態は変わります。月次の運用確認、四半期の証跡更新、年次の自己評価、教育、診断、経営報告を年間計画に組み込みます。

Librus株式会社が提供できる支援

Librus株式会社は、SCS評価制度★3に向けた現状分析から、適用範囲の設計、自己評価票、証跡台帳、規程・運用の整備、技術的な確認、是正計画、経営層向け説明、専門家との連携、申請準備まで一気通貫で支援します。企業ごとのIT環境、取引構造、予算、社内稟議を踏まえ、過剰な対策を一律に導入するのではなく、リスクと要求事項の双方から優先順位を整理します。

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・訓練まで接続できます。診断結果を報告して終わらず、改善担当と期限を定め、再確認と継続運用までつなげることが特長です。経営層には取引・財務・事業継続の言葉で、情報システム部門には設定・運用・証跡の言葉で説明し、社内合意形成を支援します。

よくある質問

Q1. ★3は自己評価だけで取得できますか。

いいえ。取得希望組織が自己評価を作成しますが、セキュリティ専門家の確認・助言・署名と、経営層による自己適合宣誓を含む申請が必要です。

Q2. 社内の有資格者が専門家確認を担当できますか。

社内外の専門家が想定されていますが、所定資格の保有、制度研修、事務局登録などの要件があります。実際の起用時は登録状況と最新規程を確認してください。

Q3. ISMSを取得済みなら、そのまま★3を取得できますか。

既存の方針、リスク管理、監査記録は有力な証跡になり得ます。ただし、SCS評価制度の適用範囲と要求事項に照らした自己評価および所定手続は別途必要です。

Q4. 脆弱性診断やペネトレーションテストは必須ですか。

すべての企業に同じ検査を機械的に実施するものではありません。評価基準、対象システム、リスク、既存証跡に応じて必要性と範囲を判断します。

Q5. どの部門が主管すべきですか。

情報システム部門が実務主管となる例は多いものの、経営企画、総務・法務、人事、調達、開発、事業部門の参加が必要です。経営層は範囲、予算、残余リスクを判断します。

Q6. どのくらい前から準備すべきですか。

台帳、規程、ログ、復旧試験等がそろっているかで変わります。運用実績や技術改修が必要なら時間を要するため、希望申請日から逆算して早期にギャップ分析を始めるのが安全です。

Q7. ★3取得後は何をすべきですか。

証跡の更新、アカウント・資産・委託先の見直し、教育、脆弱性対応、訓練、経営報告を定常化します。対象事業のリスクが高い場合は★4も検討します。

Q8. 対象範囲が決まっていなくても相談できますか。

可能です。取引先からの要求、扱う情報、接続権限、重要業務を整理し、説明価値と実行可能性の両面から範囲を設計します。

まとめ：★3は書類作成ではなく、説明可能な運用を作る取り組み

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★3取得では、対象範囲を定め、要求事項に沿って自己評価し、規程・設定・運用記録を証跡としてそろえます。不足をリスク順に是正した後、登録されたセキュリティ専門家の確認・助言・署名を受け、経営層の自己適合宣誓を含めて申請します。

成功の鍵は、自己評価票を先に埋めることではなく、経営目的、適用範囲、証跡台帳、是正責任、維持運用を一つの計画にすることです。これにより、申請時の手戻りを抑えるだけでなく、取引先への説明、事故時の初動、事業継続の実効性も高められます。

取得後も機能するセキュリティ体制を作りたい企業へ

SCS評価制度への対応を、取引条件を満たすための一度きりの作業で終わらせたくない企業には、改善・運用まで含む支援が適しています。Librus株式会社は、診断、ペネトレーションテスト、SOC／CSIRT、教育、インシデント対応を必要に応じて組み合わせます。対象範囲や実施方法が固まっていない段階から、事業リスクと予算に合うロードマップをご一緒に設計します。

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：https://librus.co.jp/contact