SCS評価制度とPマーク・SOC 2・業界ガイドラインの関係

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（以下「SCS評価制度」）への準備で、PマークやSOC 2を取得済みなら、最初から仕組みを作り直す必要はありません。ただし、既存認証を持っているだけでSCS評価制度の要求を自動的に満たすわけでもありません。制度ごとに目的、対象範囲、評価方法が異なるためです。

実務上の結論は、既存の規程や証跡を制度別に管理するのではなく、「要求事項―社内統制―証跡―責任者」の対応表を一つ作り、共通利用できるものと不足部分を切り分けることです。例えば、アクセス権申請、ログ監視、インシデント対応訓練、委託先評価の記録は複数制度で活用できます。一方、Webアプリケーション診断やプラットフォーム診断、ペネトレーションテストなど、技術的な有効性を裏付ける追加検証が必要になる場合があります。

本記事では、従業員100～1,000名程度の企業を想定し、SCS評価制度とPマーク、SOC 2、金融・医療等の業界ガイドラインをどう整理し、監査・取引先回答・経営報告に使える証跡体系へまとめるかを解説します。なお、制度の詳細は今後更新され得るため、申請時点のIPA公式資料を必ず確認してください。

この記事で分かること

この記事を読むと、各制度の目的と守備範囲の違い、既存認証をSCS評価制度へ流用できる範囲、証跡の共通化手順、技術検証の組み込み方、社内稟議や外部支援会社の選定で確認すべき点が分かります。特に重要なのは、「認証を何個持っているか」ではなく、「必要な統制が対象範囲で実際に機能し、その事実を再現可能な証跡で説明できるか」という視点です。

SCS評価制度とは何か

SCS評価制度は、取引先を含むサプライチェーン全体のセキュリティ対策を段階別に可視化し、発注者と受注者の間で共通言語として使うことを想定した制度です。経済産業省と内閣官房国家サイバー統括室の監督のもと、IPAが運営します。委託元が取引先に適切な段階を示し、対策の実施状況を確認する利用場面が想定されています。

IPAの公表情報では、★3は一般的なサイバー脅威に対処し得る水準で、専門家確認付き自己評価です。★4は、初期侵入の防御だけでなく、被害拡大や攻撃目的の遂行を抑え、取引先のデータ・システム保護や自社の役割に応じたサプライチェーン強靭化策まで含む水準で、第三者評価と技術検証が予定されています。★5は高度な攻撃を想定したリスクマネジメントとベストプラクティスを念頭に、今

後さらに具体化される位置付けです。上位段階の申請に、下位段階の事前取得が必須という関係ではありません。★3・★4は2027年3月頃の運用開始が予定されています。

出典：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「SCS評価制度の詳細情報」https://www.ipa.go.jp/security/scs/details.html
IPA「よくある質問」https://www.ipa.go.jp/security/scs/faq.html

評価対象は会社全体とは限らない

SCS評価制度では、取得希望組織が適用範囲を決め、その中から対象をサンプリングして評価することが想定されています。したがって、最初に決めるべきなのは「全社で取るか」ではなく、どの取引、拠点、業務、システム、クラウドサービス、委託先を評価対象にするかです。重要顧客へ提供するサービスだけを狭く切り出すと準備負担は下がりますが、共通基盤や本社機能が範囲外になり、実態と説明が合わないことがあります。契約上の責任範囲、ネットワーク境界、データフロー、運用責任者を基準に決めることが重要です。

SCS評価制度とPマーク・SOC 2・業界ガイドラインの違い

複数制度は競合するものではなく、異なるリスクを異なる方法で確かめる仕組みです。Pマークを持つ企業がSCS評価制度にも対応し、クラウドサービスについてSOC 2報告書を顧客へ提示し、さらに金融・医療の業界要求を満たすことは矛盾しません。むしろ、目的の違いを理解せず、一つの認証で全要求を代替できると考えることが問題になります。

制度・基準	主な目的	主な対象	評価・確認の特徴	SCSとの関係
SCS評価制度	サプライチェーン上のサイバー対策を段階評価	組織が定めた取引・業務・システム等	★3は専門家確認付き自己評価、★4は第三者評価・技術検証を予定	比較の中心。取引要請への共通言語
Pマーク	個人情報保護マネジメントシステムの構築・運用	原則として国内事業者の法人単位	JIS Q 15001に基づく運用指針への適合を審査	規程、教育、委託先管理、事故対応等を部分流用
SOC 2	サービス組織の統制について利用者等へ保証を提供	対象サービスと、その提供に関係するシステム・統制	独立した監査人がTrust Services Criteriaに照らして報告	アクセス管理、変更管理、ログ、可用性等の証跡を部分流用
業界ガイドライン	業種固有の法規制・リスクへの対応	金融、医療、重要インフラ等の対象事業・システム	監督指針、契約、監査等と結び付く場合がある	SCSを土台に固有要求を追加する

Pマークは個人情報保護が中心

プライバシーマーク制度は、JIS Q 15001に基づく個人情報保護マネジメントシステム（PMS）を整備し、実際の事業活動で個人情報を適切に取り扱う体制を評価します。付与単位は原則として法人です。個人情報の特定、リスク分析、教育、委託先管理、事故対応、内部監査、マネジメントレビュー等はSCS評価制度の準備にも役立ちます。

ただし、Pマークはサイバー攻撃への技術的耐性だけを評価する制度ではありません。脆弱性管理、境界防御、侵害拡大防止、検知・対応能力などについては、Pマークの運用証跡だけでは説明が不足する可能性があります。Pマーク取得済み企業ほど、PMS文書を無批判に転用するのではなく、情報資産の範囲を「個人情報」から「取引先の重要情報、設計情報、認証情報、業務継続に必要なシステム」へ広げる作業が必要です。

出典：プライバシーマーク制度「制度の概要」
https://privacymark.jp/system/about/outline_and_purpose.html

SOC 2は対象サービスの統制を説明する保証報告

SOC 2は、AICPAのTrust Services Criteriaを用いて、サービス組織のシステムに関する統制を独立した監査人が検証する枠組みです。セキュリティを共通基準とし、契約やサービス特性に応じて可用性、処理のインテグリティ、機密保持、プライバシーを扱います。Type 1は特定時点の統制設計、Type 2は一定期間にわたる運用状況を対象とする点も、単純な認証マークとは異なります。

SOC 2報告書が対象とするサービス、システム境界、除外事項、サブサービス組織、対象期間を確認しなければ、SCS評価制度への利用可否は判断できません。例えば、クラウドサービスAのSOC 2報告書は、同じ法人が運営する受託開発部門Bや国内拠点全体を当然にはカバーしません。一方で、ID管理、特権アクセス、変更管理、バックアップ、ログレビュー、インシデント管理などの統制記述と運用証跡は、有力な基礎資料になります。

出典：AICPA & CIMA「SOC 2 - SOC for Service Organizations」
https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

業界ガイドラインは業種固有の上乗せ要件

金融機関向けのFISC安全対策基準、医療情報システムの安全管理に関するガイドラインなどは、事業停止時の社会的影響、取り扱う情報の機微性、システム構成、監督上の要請を踏まえた具体性を持ちます。SCS評価制度を取得しても、業界固有の責任分界、外部委託、クラウド利用、非常時運用等の要求が消えるわけではありません。

例えば金融機関向けサービスでは、顧客の外部委託先管理やシステムリスク管理に耐える説明が必要です。医療分野では、医療機関とサービス提供者の責任分界、認証・認可、保守接続、バックアップ、証跡レビュー等を具体化します。SCS評価制度は共通基盤、業界ガイドラインは追加レイヤーと考えると整理しやすくなります。

出典：FISC「安全対策」https://www.fisc.or.jp/publication/pubcat/sm/
厚生労働省「医療情報システムの安全管理に関するガイドライン 第6.0版」
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

なぜ今、複数制度を一体管理すべきなのか

取引先ごとの質問票、Pマーク更新、SOC 2監査、業界別監査を別々の担当者と文書で回すと、同じアクセス権一覧や教育記録を何度も収集することになります。回答内容が制度ごとに食い違えば、統制そのものより説明の不整合が問題になります。さらに、営業が顧客へ回答した内容と、情報システム部門の実運用が一致しないまま契約上の保証となることもあります。

一体管理の目的は、監査工数の削減だけではありません。経営者が重要取引の継続条件を把握し、投資の優先順位を決められる状態をつくることです。取引先から★4を求められる可能性があるのに、翌年度予算へ技術検証やEDR、ログ保管、復旧訓練の費用を織り込んでいなければ、運用開始直前の対応は難しくなります。制度対応を営業継続、受注資格、BCPの課題として扱う必要があります。

対応しない場合に起こり得る問題

SCS評価制度への未対応が直ちに法令違反や一律の取引停止を意味するわけではありません。しかし、発注者が調達条件として一定段階を求めるようになれば、評価未取得や説明不足が新規取引、契約更新、委託範囲の判断に影響する可能性があります。特に、自社が大企業の業務システムを運用する、機密設計情報を扱う、顧客ネットワークへ接続する、再委託先を多数利用するといった場合は優先度が高まります。

攻撃面では、VPN機器や公開サーバーの脆弱性から侵入され、認証情報を窃取され、委託元環境への接続口を踏み台にされるケースが考えられます。メールアカウント侵害による取引情報の流出、ランサムウェアによる納品停止、開発環境への侵入によるソースコード改ざんも、サプライチェーン上の影響が大きい事象です。Pマークの教育記録やSOC 2報告書があっても、未修正の公開脆弱性や過大な特権が残っていれば実害は防げません。

証跡と統制を共通利用する7つの手順

1. 経営が目標段階と対象取引を決める

最初に、主要顧客の調達方針、扱う情報、停止時の売上影響、代替困難性を踏まえ、目標とする★と期限を仮決定します。経営会議では、認証取得費だけでなく、改善投資、運用人員、維持費を含めて判断します。顧客要請が未確定なら、売上上位顧客、重要インフラ関連、機密情報を扱う業務から優先順位を付けます。

2. 適用範囲と責任分界を図にする

組織図だけでは不十分です。業務プロセス、情報の流れ、利用SaaS、クラウド、ネットワーク、拠点、再委託先、保守会社を一枚の構成図と台帳にします。自社が実施する統制、クラウド事業者に依存する統制、顧客側の責任を分けることで、証跡の所在が明確になります。

3. 制度横断のコントロールマトリクスを作る

各制度の要求をそのまま横に並べるのではなく、アクセス管理、脆弱性管理、ログ監視、インシデント対応、事業継続、委託先管理、教育などの統制テーマへ正規化します。行には統制、列にはSCS、Pマーク、SOC 2、業界ガイドラインを置き、該当要求、実施部署、頻度、証跡、保管先、不備、改善期限を記録します。これが監査回答の基礎台帳になります。

4. 証跡の品質を確認する

規程が存在するだけでは、運用の有効性は説明できません。アクセス権棚卸しなら、対象者一覧、承認記録、差異、是正結果、実施日、責任者まで必要です。教育なら受講率だけでなく、未受講者への督促や理解度確認も証跡になります。ログ監視では、ログを保存している事実に加え、アラートの判断基準、対応チケット、エスカレーション記録を確認します。個人情報や顧客機密を含む証跡は、閲覧権限、提出方法、マスキング、保管期限も定めます。

5. 不足をリスクで優先順位付けする

不備は件数順ではなく、取引への影響、攻撃可能性、被害規模、外部公開の有無、代替策の有効性で評価します。インターネット公開機器の重大な脆弱性、共有管理者ID、多要素認証の欠如、バックアップ復元未検証などは、文書表現の不足より先に改善すべきです。改善計画には、恒久対応、期限、責任者、予算、完了条件、暫定措置を含めます。

6. 技術検証で実装の有効性を確かめる

Webアプリケーション診断は、認証・認可不備や入力処理等、Web固有の脆弱性を確認します。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、クラウド設定などを調べます。ペネトレーションテストは、攻撃者の視点で複数の弱点を組み合わせ、重要資産へ到達できるかを検証します。目的が異なるため、単に「診断実施済み」とせず、対象資産、脅威、深度に応じて選びます。

RFPや見積依頼では、対象URL・IP・クラウド環境、認証後画面、API、実施時間、停止回避条件、再診断、報告会、機密情報の取扱い、再委託、事故時連絡、報告書サンプルを確認します。成果物には、経営向け要約、技術的根拠、再現条件、影響、リスク評価、推奨対策、優先順位、対象外範囲を含めるべきです。

7. 運用サイクルへ組み込む

評価取得を一度きりのプロジェクトにしないことが重要です。月次の脆弱性管理、四半期のアクセス権棚卸し、年次の教育・訓練、委託先見直し、インシデント対応演習、経営レビューなど、既存会議へ統制確認を組み込みます。組織変更、M&A、新規クラウド導入、重要な再委託、重大インシデントがあれば、定例を待たず適用範囲とリスクを再評価します。

準備資料、期間、費用を左右する要因

準備では、情報セキュリティ規程、資産台帳、ネットワーク・データフロー図、アカウント一覧、権限棚卸し記録、脆弱性・パッチ管理記録、ログ監視記録、インシデント対応計画と訓練記録、バックアップ・復旧試験、教育記録、委託先台帳・契約、過去の診断報告書、PマークやSOC 2の審査資料などを集めます。資料名より、最新版か、対象範囲が一致するか、承認と実施記録が残るかが重要です。

期間は、適用範囲、目標段階、拠点・システム数、既存認証の成熟度、証跡の蓄積期間、技術改善の量、評価機関との調整で変わります。初期ギャップ分析だけなら比較的短期間でも可能ですが、ログ運用や権限棚卸しなど一定期間の実績が必要な統制は、文書作成だけでは埋まりません。余裕を持って年度予算と人員計画へ組み込むべきです。

費用も申請・評価費だけでなく、コンサルティング、ツール導入、診断、ペネトレーションテスト、規程改定、教育、運用工数、再評価まで含めて見積もります。全社一律に高額な製品を導入するより、重要資産へ優先配分し、既存ツールの設定改善や運用統合で代替できる部分を見極める方が合理的です。

社内稟議で説明すべき内容

稟議では「認証取得のため」だけでは投資効果が伝わりません。①主要取引先と売上への影響、②求められる可能性のある段階と期限、③現状との差分、④事故時の事業停止・復旧・信用への影響、⑤既存のPマーク・SOC 2・業界対応を共通利用できる範囲、⑥初年度と維持年度の費用、⑦社内責任者と外部支援範囲、⑧取得できない場合の代替説明を示します。

特に、情報システム部門だけに責任を寄せないことが重要です。営業は顧客要求の把握、法務・購買は契約と委託先管理、人事は教育、事業部門は業務継続、経営はリスク受容と予算判断を担います。制度対応を横断プロジェクトとして位置付けることで、監査直前の資料集めから、平時の統制運用へ移行できます。

支援会社を選ぶ際の確認ポイント

支援会社には、制度文書の作成能力だけでなく、技術と経営の両面を確認します。具体的には、SCS要求事項と既存制度をマッピングできるか、適用範囲を事業・契約から設計できるか、診断やペネトレーションテストを含む技術検証に対応できるか、改善後の運用設計まで支援するかを確認してください。

見積比較では、成果物の名称だけで判断せず、ヒアリング回数、現地確認、対象拠点・システム、証跡サンプル数、規程改定、技術検証、再確認、経営報告、申請支援が含まれるかを揃えます。また、評価を担う立場と改善支援を担う立場の独立性、利益相反、機密情報の保管・削除、再委託先も確認が必要です。制度開始前の段階では、公式に登録・指定されたかのような不適切な説明がないことも重要です。

出典：経済産業省「SCS評価制度に係る不適切な勧誘に御注意ください」
https://www.meti.go.jp/policy/netsecurity/20260427_scs.html

よくある失敗と注意点

既存認証があれば追加対応は不要と考える

制度間で目的と範囲が違うため、認証書だけでは代替できません。報告書、適用範囲、統制記述、例外事項、証跡を要求事項単位で照合します。

規程を増やしすぎる

制度ごとに似た規程を作ると、更新漏れと矛盾が生じます。共通の基本規程と手順を中心にし、業界固有事項は付則や管理基準で補完する方が運用しやすくなります。

対象範囲を曖昧にしたまま診断を発注する

公開Webだけを診断しても、取引先接続端末やクラウド管理面が重要なら目的を満たしません。情報資産と攻撃経路を整理してから、診断対象と手法を決めます。

評価直前に証跡を作る

後から整えた記録は、継続運用の証明になりにくく、実態との不一致も起きます。日常業務から自動的に証跡が残るチケット、承認フロー、ログ保管の仕組みを設計します。

Librus株式会社が提供できる支援

Librus株式会社は、SCS評価制度に向けた現状分析、適用範囲の設計、Pマーク・SOC 2・業界ガイドラインとの要求事項マッピング、規程・証跡整備、改善計画、経営報告、運用定着まで一気通貫で支援します。単にチェックリストを埋めるのではなく、取引上の重要性と実際の攻撃経路を踏まえ、優先順位を設計します。

技術面では、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、レッドチーム演習、SOC／CSIRT構築・運用、インシデントレスポンス、デジタルフォレンジックを組み合わせられます。経営面では、リスクアセスメント、情報セキュリティ体制構築、教育、SBOM、M&A・IPO・取引先監査等の重要局面にも対応します。既存の認証やツールを生かしながら、企業ごとの環境、予算、期限に合わせて支援範囲を個別設計できる点が特徴です。

よくある質問

Q1. PマークがあればSCS評価制度を取得できますか？

Pマークだけで自動的に取得できるわけではありません。ただし、個人情報管理、教育、委託先管理、事故対応、内部監査等の規程と証跡は活用できます。SCS固有の対象範囲とサイバー対策との差分確認が必要です。

Q2. SOC 2 Type 2報告書はSCS評価の代わりになりますか？

原則として別の枠組みです。対象サービス、期間、統制、例外事項がSCSの適用範囲と一致する部分は有力な証跡候補になりますが、不足要求は別途対応します。

Q3. 業界ガイドラインとSCSはどちらを優先すべきですか？

法令、監督上の要請、契約上の義務を優先しつつ、SCSを共通基盤として統合します。片方を選ぶのではなく、業界固有要求を上乗せする考え方が実務的です。

Q4. ★3を取らずに★4を目指せますか？

IPAの公表情報では、★3の事前取得が★4取得の条件という関係ではありません。ただし、★4は★3相当を包含するため、現状とのギャップと準備負担を確認して目標を決めます。

Q5. どの部署が主管になるべきですか？

情報システムまたはセキュリティ部門が事務局を担う例が多いものの、経営、営業、法務、購買、人事、事業部門を含む横断体制が必要です。取引条件とリスク受容は経営判断です。

Q6. 診断とペネトレーションテストのどちらが必要ですか？

目的で選びます。個別資産の既知の弱点を網羅的に確認するなら脆弱性診断、攻撃経路を組み合わせて重要資産への到達可能性や検知・対応を確かめるならペネトレーションテストが適します。

Q7. 準備はいつ始めるべきですか？

対象範囲の整理とギャップ分析は早期に始めるのが合理的です。運用証跡の蓄積や予算化には時間がかかるため、顧客要請が確定してからでは選択肢が狭まる場合があります。

Q8. 既存の取引先質問票は使えますか？

利用できます。ただし、質問への回答だけでなく、対応する統制、証跡、対象範囲、責任者をひも付けてください。回答の根拠が明確になり、SCSや他の監査への再利用が容易になります。

まとめ：制度別対応から統制・証跡の一体管理へ

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）、Pマーク、SOC 2、業界ガイドラインは、目的も対象範囲も評価方法も異なります。したがって、一つの認証ですべてを代替することはできません。一方、アクセス管理、教育、委託先管理、ログ監視、インシデント対応、事業継続など、共通利用できる統制と証跡は多くあります。

実務では、対象範囲を定め、制度横断のコントロールマトリクスを作り、証跡の品質を確認し、技術検証で実装の有効性を確かめます。制度取得そのものをゴールにせず、重要取引の継続と事故時の被害抑制につながる運用へ落とし込むことが、経営上の価値になります。

SCS評価制度の準備を、既存資産を生かして始めたい企業へ

まず現状と不足項目を整理する

PマークやSOC 2の資料をどこまで使えるか分からない場合は、既存の規程・証跡とSCS要求事項のギャップを整理するところから相談できます。Librus株式会社は、対象範囲や目標段階が未確定の段階でも、重要取引とリスクを踏まえ、優先して確認すべき項目と準備の進め方を可視化します。

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
電話：03-6772-8015
お問い合わせフォーム：https://librus.co.jp/contact