

SCS対応を一過性にしない——取得後の継続運用モデル

SOC・CSIRT・脆弱性管理・教育・内部点検・更新管理を実務で回す方法

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）への対応で重要なのは、マーク取得をゴールにしないことです。取得時に整えた規程や証跡が、その後の組織変更、クラウド移行、新規取引、脆弱性の発見に追随しなければ、実際の防御力は低下します。

結論から言えば、SCS対応を継続させる鍵は、要求事項を「担当者が保管する審査資料」ではなく、「月次・四半期・年次で回る業務」に変換することです。SOCによる監視、CSIRTによる事故対応、脆弱性管理、従業員教育、内部点検、更新管理を一つの運用台帳と経営報告に接続すれば、更新前の慌ただしい再整備を避けやすくなります。

この記事で分かること

- SCS評価制度の取得後に必要となる継続運用の全体像
- SOC・CSIRT・脆弱性管理・教育・内部点検を連動させる方法
- ★3・★4の有効期間と、変更時に再評価を検討すべき場面
- 年間計画、証跡管理、経営報告、予算化の実務ポイント
- 継続運用を支援する会社を選ぶ際の確認事項

SCS評価制度は「取得時点の確認」であり、将来の安全を保証するものではない

SCS評価制度は、サプライチェーンにおける企業の立ち位置や想定リスクに応じて必要な対策水準を示し、対応状況を可視化する制度です。経済産業省と内閣官房国家サイバー統括室が2026年3月に制度構築方針を公表し、IPAが運営します。★3・★4は2027年3月頃の運用開始が予定されています。

出典：[IPA「SCS評価制度の詳細情報」](#)、[IPA「よくある質問」](#)

★3と★4では、評価方法と有効期間が異なる

制度構築方針では、★3は一般的なサイバー脅威に対処できる水準とされ、セキュリティ専門家の確認を伴う自己評価が想定されています。有効期間は1年です。★4は、侵入防御だけでなく、被害拡大防止、インシデント対応、事業継続、取引先管理まで含む標準的・包括的な水準で、第三者評価と技術検証を伴います。有効期間は3年ですが、期間中も毎年の自己評価と評価機関への提出が想定されています。

また、取得時の適用範囲や基準の達成に大きな影響を与える変更があった場合は、有効期限前でも専門家または評価機関による確認・評価が必要になる想定です。大規模な端末・サーバ更改、クラウドへの大規模移行、ネットワーク構成の顕著な変更、規程や運用方法の大幅変更などが例示されています。

出典：[経済産業省・国家サイバー統括室「SCS評価制度に関する制度構築方針」](#)

継続運用が必要な理由

攻撃者は審査日程に合わせて待つはくれません。公開サーバの既知脆弱性、盗まれた認証情報、取引先を装うメール、クラウド設定ミスは、日々発生します。例えばVPN装置の脆弱性が公表されたのに資産台帳が古く、対象機器の有無を判断できなければ、パッチ適用の意思決定が遅れます。退職者アカウントが残ったままなら、取得時にアクセス管理規程が整っていても実効性はありません。

制度上の更新だけを目的にすると、現場には「年に一度、証跡を集める仕事」と映ります。これを避けるには、通常業務の成果物がそのまま評価の証跡になる仕組みが必要です。

取得後に起こり得る問題——形骸化は取引と事業継続にも影響する

規程と実態がずれる

取得後に組織再編やシステム変更が進む一方、責任者一覧、ネットワーク図、クラウド利用台帳、委託先一覧が更新されないケースがあります。事故時の連絡先が旧担当者のままでは、初動が止まりかねません。更新審査では、文書の有無だけでなく、定めた手順が実際に運用されていることを説明する必要があります。

脆弱性対応が担当者の勘に依存する

脆弱性情報を受け取っても、対象資産、事業影響、悪用状況、代替策を結び付ける仕組みがなければ優先順位が定まりません。CVSSの点数だけで判断すると、外部公開された重要システムの脆弱性と、隔離された検証端末の脆弱性を同列に扱うおそれがあります。結果として、本当に急ぐべき対応が後回しになります。

取引先への説明力が低下する

委託元から「直近の教育実施率」「重大脆弱性の是正状況」「インシデント時の通知期限」を尋ねられた際、資料を即時に提示できなければ、対策自体を行っていても信頼を得にくくなります。SCS

評価制度は取引契約等で委託元が委託先に段階を提示し、実施状況を確認する利用が想定されています。継続運用は、営業・調達・法務にとっても取引継続の基盤です。

経営判断が遅れる

セキュリティ情報が情報システム部門内に閉じると、経営層は予算の必要性を判断できません。技術的な指摘件数だけでなく、停止し得る事業、影響する顧客、復旧時間、契約上の通知義務まで翻訳する必要があります。経済産業省の「サイバーセキュリティ経営ガイドライン Ver3.0」も、経営者のリーダーシップと継続的な改善を重視しています。

出典：[経済産業省「サイバーセキュリティ経営ガイドラインと支援ツール」](#)

SCS取得後の継続運用モデル——6つの機能を一つの管理サイクルにする

従業員100～1,000名規模の企業では、専任の大組織を新設するより、既存の情報システム、総務・人事、法務、事業部門、経営会議の役割を明確にし、不足部分を外部サービスで補う設計が現実的です。以下の6機能を別々に導入せず、共通のリスク台帳、改善計画、証跡保管ルールでつなぎます。

1. SOC：監視結果を改善につなげる

SOC (Security Operation Center) は、ログやアラートを監視し、不審な挙動を検知・分析する機能です。導入後は、検知件数だけでなく、重大度、初動時間、誤検知率、同種アラートの再発、ログ未取得資産を月次で確認します。監視対象に入っていないクラウドや拠点があれば、リスク台帳に登録し、追加時期を決めます。

SOCを外部委託する場合も、社内の判断責任は残ります。「誰が遮断を承認するか」「夜間に誰へ連絡するか」「取引先への通知を誰が決めるか」を事前に定め、半年に一度は連絡テストを行うと実効性を確認できます。

2. CSIRT：事故対応手順を訓練で検証する

CSIRT (Computer Security Incident Response Team) は、インシデント発生時の対応を統括する体制です。常設の専任部署でなくても、情報システム、法務、広報、人事、事業責任者、経営層から役割を指定できます。

年1回の机上訓練では、ランサムウェアで受発注システムが停止した、委託先から情報漏えいの連絡が来た、管理者アカウントが乗っ取られた、といった自社固有のシナリオを使います。連絡網、証

抛保全、復旧優先順位、顧客・委託元への報告、経営判断を時系列で試し、訓練後に手順書を改訂します。

3. 脆弱性管理：資産把握から是正確認まで閉じる

脆弱性管理は、単発の診断ではなく、①資産把握、②情報収集、③影響判定、④優先順位付け、⑤修正または緩和策、⑥再確認、⑦例外承認の一連のプロセスです。インターネット公開資産は継続的に把握し、重大な脆弱性は期限と責任者を設定します。期限内に修正できない場合は、アクセス制限、WAF、監視強化などの代替策と、残余リスクを承認者が記録します。

Webアプリケーション診断は、認証、入力処理、権限管理などアプリ固有の問題を確認します。プラットフォーム診断は、OS、ミドルウェア、ネットワーク機器などの設定や既知脆弱性を確認します。ペネトレーションテストは、複数の弱点を組み合わせることで実際にどこまで侵入・権限拡大・情報到達が可能かを検証します。目的に応じて使い分け、重大改修や公開前、定期点検のタイミングに組み込みます。

4. 教育：受講率ではなく行動変容を測る

全社員向け教育は、パスワード、フィッシング、情報持ち出し、事故報告を基本とし、入社時と年次で実施します。ただし受講率100%だけでは不十分です。標的型メール訓練の報告率、誤送信の再発、端末放置、委託先データの扱いなど、実際の行動指標を確認します。

管理者、開発者、営業、人事、調達には役割別教育が必要です。例えば開発者にはセキュアコーディングと依存ライブラリ管理、調達担当には委託先評価と契約条項、経営層には重大事故時の判断訓練を行います。

5. 内部点検：証跡の有無と運用実態を確認する

内部点検では、要求事項ごとに規程、実施記録、システム設定、担当者ヒアリングを突き合わせます。「規程がある」だけで適合とせず、例えばアカウント棚卸しなら、対象一覧、実施日、差異、削除結果、承認記録まで確認します。点検担当者は可能な範囲で実施担当者と分け、自己確認の盲点を減らします。

指摘事項は、重大度、事業影響、期限、責任者、是正方法、再確認結果を一つの改善台帳で管理します。更新直前に資料を集めるのではなく、月次の運用記録を所定の場所へ保管するルールが有効です。

6. 更新管理：変更をトリガーに再評価する

更新管理は、毎年のカレンダーだけでは不十分です。M&A、事業譲渡、新拠点、クラウド移行、基幹システム刷新、大規模なネットワーク変更、重要な委託先の変更、重大インシデントを「臨時評価

のトリガー」として定義します。経営企画や購買部門から情報システム部門へ変更情報が届くワークフローを設けます。

★3は1年ごとの更新、★4は毎年の自己評価と3年ごとの第三者評価が想定されています。正式な申請方法、費用、解説書などは公表予定の情報を必ず確認し、制度の具体化に応じて計画を更新してください。

月次・四半期・年次で回す実務スケジュール

月次：変化と未対応を把握する

月次では、重大アラート、インシデント、外部公開資産、重大脆弱性、パッチ未適用、入退社アカウント、バックアップ失敗、改善課題の期限超過を確認します。会議は60分程度でも構いません。件数の報告だけで終わらず、事業影響が大きい上位課題について、担当者と期限を決めます。

四半期：部門横断でリスクを見直す

四半期ごとに、システム変更、委託先変更、教育結果、アクセス権棚卸し、復旧テスト、SOCの検知ルール、例外承認の期限をレビューします。経営層には、重大リスクの残高、是正遅延、必要予算、取引への影響を簡潔に報告します。

年次：要求事項全体と経営方針を再確認する

年次では、適用範囲、資産・データ・取引先、規程、リスク評価、教育、訓練、診断、内部点検、経営者レビューを一巡させます。★3または★4の手続きに必要な自己評価へ接続し、前年との差分と未解決事項を明示します。年度予算の編成前にギャップを洗い出せば、診断費、監視費、ツール更改、人材育成費を稟議に載せやすくなります。

実施前に準備すべき資料と、成果物に含めるべき項目

継続運用の設計時には、情報セキュリティ規程、組織図、責任分担表、IT資産・クラウド・外部公開資産の一覧、ネットワーク図、データ分類、委託先一覧、契約上のセキュリティ条項、インシデント記録、教育記録、診断報告書、改善台帳、バックアップ・復旧記録を準備します。すべてが揃っていないくても、欠落自体を課題として管理すれば着手できます。

成果物には、適用範囲、現状評価、要求事項とのギャップ、リスク評価、優先順位、改善ロードマップ、責任者、期限、概算費用、代替策、残余リスク、必要な証跡、更新・臨時評価の条件を含めるべきです。技術部門向けの詳細版と、経営判断向けの要約版を分けると、稟議と実行の双方に使えます。

期間と費用を左右する要因

継続運用モデルの立ち上げ期間は、対象範囲、拠点数、システム数、既存規程の成熟度、委託先数、★3・★4のどちらを目指すかによって変わります。現状調査から運用開始まで数か月単位で設計し、重大な技術課題は別途改修計画を置くのが現実的です。制度申請そのものの費用は、2026年9月時点で今後公表予定とされています。

費用を左右する主な要因は、支援範囲、現地確認の可否、Webアプリケーション診断・プラットフォーム診断の対象数、ペネトレーションテストの範囲、SOCの監視対象と時間帯、ログ量、CSIRT訓練の複雑さ、文書作成支援の程度です。見積もりでは「適合支援」「技術対策」「運用代行」「評価・申請関連」を分けると比較しやすくなります。

社内稟議で説明すべき内容

稟議では、マーク取得だけを目的にすると投資対効果が伝わりにくくなります。対象となる重要取引、停止時の売上・顧客影響、機密情報の種類、既存契約上の義務、現状の不足、取得後の維持費、担当工数を示します。さらに、診断・監視・訓練で得られる成果を「更新対応」「事故低減」「取引先への説明」「復旧力向上」に分けて説明します。

経営層が判断すべきなのは、目標段階、適用範囲、許容する残余リスク、優先する事業、予算、責任者です。情報システム部門だけに取得責任を負わず、経営企画、人事、法務、調達、現場部門の協力を経営判断として明確にすることが重要です。

支援会社の選び方とRFP・見積依頼時の確認事項

支援会社は、制度文書を作る能力だけでなく、技術検証と日常運用をつなげられるかで選びます。RFPや見積依頼では、制度の最新情報への追従方法、★3・★4ごとの経験・支援方針、ギャップ評価の手法、成果物、担当体制、秘密情報の保管・削除、再委託、事故時の連絡、診断後の再確認、SOC・CSIRT支援、更新時の支援範囲を確認してください。

評価とコンサルティングを同一法人が提供する場合の中立性・公平性に関する要件は、今後詳細化される予定です。評価機関の指定状況や利益相反管理を確認し、取得支援と正式評価の役割を契約上も明確にする必要があります。

よくある失敗と注意点

適用範囲を狭くしすぎる

審査負担を下げるために範囲を狭くすると、重要な受発注システム、クラウド、拠点、委託先が外れ、取引先が期待する説明と一致しない場合があります。法人単位だけでなく、部門、拠点、システム、データ、取引関係を図示して決めます。

ツール導入を対策完了と考える

EDRやSIEMを導入しても、アラートを確認する人、遮断判断、例外管理、障害時の代替手順がなければ運用されません。製品の導入記録ではなく、検知から是正までの実績を確認します。

診断結果を放置する

診断報告書を受領しても、改修責任者と期限が決まらなければリスクは残ります。事業影響と悪用可能性で優先順位を付け、修正後は再診断または設定確認を行います。受容する課題は、理由と期限を経営または権限者が承認します。

証跡に個人情報や機密情報を残しすぎる

評価用証跡には、従業員情報、構成情報、脆弱性、ログなどの機密情報が含まれます。提出目的に必要な範囲へ限定し、マスキング、暗号化、アクセス制限、保管期限、削除確認を定めます。支援会社との秘密保持、再委託、国外保管の有無も確認が必要です。

Librus株式会社が提供できる支援

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）への対応を、現状把握から取得準備、技術対策、取得後の運用まで一気通貫で支援します。制度要求と現場の実装を分断せず、経営・財務・事業継続・取引先対応の観点を含めて設計します。

具体的には、適用範囲の整理、ギャップ評価、規程・手順の整備、改善ロードマップ、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、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、SBOM導入・運用、内部点検、更新支援に対応可能です。企業ごとの環境や予算に合わせ、優先順位を付けて段階的に進めます。

よくある質問

Q1. SCS評価制度はいつ始まりますか。

IPAのFAQでは、★3・★4は2027年3月頃の運用開始予定です。申請方法や取得ガイドは2026年10月頃、評価機関は2026年12月末頃、セキュリティ専門家は2027年1月以降の公開予定とされています。最新情報はIPA公式サイトで確認してください。

Q2. ★3を取得してからでないと★4を取得できませんか。

いいえ。IPAの制度説明では、上位段階は下位段階の事項を含みますが、★3の事前取得が★4取得の条件になる関係ではありません。自社の取引上の要請とリスクに応じて目標を選びます。

Q3. 取得後は毎年何を行いますか。

★3は有効期間1年で、年次点検と専門家の確認・助言を経た自己評価更新が想定されています。★4は有効期間3年ですが、毎年自己評価を実施し、評価機関へ提出する想定です。日常的には月次の監視・脆弱性管理と、四半期の横断レビューを行うと年次評価へ接続しやすくなります。

Q4. 取得後にクラウド移行した場合、更新まで待つてよいですか。

大規模なクラウド移行やネットワーク変更など、適用範囲や基準達成に大きく影響する変更では、再度の確認・評価が必要になる想定です。変更計画の段階で影響評価を行い、専門家または評価機関へ確認してください。

Q5. SOCを必ず内製する必要がありますか。

内製に限定する必要はありません。外部SOCを活用する場合は、監視範囲、対応時間、重大度基準、連絡先、初動権限、ログ保管、再委託、サービス終了時のデータ返却を明確にします。社内には事業判断と連携を担う責任者が必要です。

Q6. 脆弱性診断は毎年一度で十分ですか。

システムの重要性和変更頻度によります。重大な改修、公開範囲の変更、新機能追加、基盤更改があれば、その都度の診断を検討します。定期診断の間も資産把握、脆弱性情報収集、パッチ管理、外部公開面の監視を継続します。

Q7. ISMSを取得済みでもSCS対応は必要ですか。

制度構築方針ではSCSとISMSは相互補完的な位置付けです。ISMSの規程、リスク評価、内部監査などは活用できますが、SCS固有の要求事項、適用範囲、取引先管理、技術検証との差分を確認する必要があります。

Q8. 何から相談すればよいですか。

目標段階や対象範囲が決まっていなくても、重要な取引、システム、データ、委託先、現状の対策を整理するところから始められます。最初に簡易ギャップ評価を行うと、必要な施策と予算の優先順位が見えやすくなります。

まとめ——SCS評価制度を経営と現場の改善サイクルに変える

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）は、取得時点の対策状況を可視化する仕組みです。取得後も安全が自動的に維持されるわけではありません。SOC、CSIRT、脆弱性管理、教育、内部点検、更新管理を月次・四半期・年次の業務へ落とし込み、システムや事業の変更時には臨時評価を行うことが重要です。

継続運用によって、更新準備の負担を抑えるだけでなく、事故の早期検知、復旧力、取引先への説明力、予算判断の質を高められます。規程と技術、経営と現場をつなぎ、通常業務の記録がそのまま適合の証跡になる状態を目指してください。

SCS取得後の運用設計から相談できます

「取得後に誰が運用を担うか決まっていない」「既存のISMSや社内規程を生かしたい」「診断、SOC、教育をどの順番で進めるべきか分からない」といった段階でもご相談いただけます。Librus株式会社は、対象範囲と現状の対策を整理し、事業影響と予算に応じた優先順位、年間運用計画、必要な証跡、技術的な改善策まで具体化します。取得準備だけでなく、その後も無理なく維持できる体制を設計することで、取引先への説明と実際のリスク低減を両立しやすくなります。

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>