SCS評価制度対応を外部委託するメリット｜支援会社の選び方を解説

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）への対応は、要求事項を読んでチェックシートを埋めれば終わるものではありません。適用範囲の決定、現状との差分分析、規程・手順の整備、技術対策、証跡の準備、経営層への説明、さらに★4では第三者評価や技術検証への対応まで必要になります。

結論からいえば、社内に十分なセキュリティ人材や制度対応の経験がない企業ほど、外部の支援会社を活用するメリットは大きくなります。ただし、すべてを丸投げするのではなく、経営判断・対象範囲・リスク受容・日常運用は自社が主体となり、外部には専門知識、プロジェクト推進、技術検証、改善設計などを任せることが重要です。

本記事では、従業員100～1,000名程度の企業を想定し、SCS評価制度対応を外部委託するメリット、委託しやすい業務と社内に残すべき業務、★3・★4で必要となる支援、支援会社を選ぶ際の確認ポイントを実務目線で解説します。

この記事で分かること

- SCS評価制度対応で外部支援を利用するメリット
- ★3と★4で外部委託の考え方がどう変わるか
- 支援会社に任せやすい業務と、自社で判断すべき業務
- 支援会社の選定時に確認すべき技術力・制度理解・独立性
- RFP・見積依頼時に伝えるべき情報と費用を左右する要因
- 脆弱性診断、プラットフォーム診断、ペネトレーションテストをどう位置づけるか

SCS評価制度とは｜外部委託を考える前に押さえたい仕組み

SCS評価制度は、企業のサプライチェーンにおけるセキュリティ対策状況を段階的に評価し、その結果を登録・公表する制度です。制度は経済産業省と内閣官房国家サイバー統括室の方針に基づいて構築され、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。

IPAは、委託元企業が取引先に適切な段階の対策を求め、委託先がその実施状況を示す場面を想定しています。したがって、SCS評価制度への対応は「認証を取ること」だけが目的ではなく、取引先に説明できる形で自社のセキュリティ対策を整備し、継続運用できる状態を作ることが本質です。

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

★3は専門家確認付き自己評価、★4は第三者評価・技術検証

★3では、取得希望組織が自己評価を行い、SCS評価制度で定めるセキュリティ専門家による確認・助言を受けたうえで申請します。★4では、指定された評価機関による第三者評価に加え、技術検証が必要です。評価機関は文書確認だけでなく実地審査も行い、技術検証事業者は脆弱性診断を実施する仕組みが示されています。

2026年10月22日時点では、評価機関・技術検証事業者の指定申請が進められており、指定機関台帳への登録・公表は2026年12月下旬の予定です。そのため、★4取得を検討する企業は、支援会社と評価機関の役割を分けて考える必要があります。

出典：IPA「指定申請について（評価機関・技術検証事業者・研修事業者向け）」
https://www.ipa.go.jp/security/scs/security-experts-organization/shiteishinsei.html

なぜSCS評価制度対応は外部委託と相性がよいのか

制度対応は「規程」「技術」「運用」「経営判断」を横断する

SCS評価制度への対応が難しい理由は、情報システム部門だけでは完結しにくいことです。例えば、アクセス制御や多要素認証、ログ取得、脆弱性管理といった技術対策は情報システム部門が中心になります。一方、委託先管理、インシデント対応体制、教育、責任分担、事業継続、経営層への報告などは、法務・総務・人事・調達・事業部門も関係します。

従業員100～1,000名規模では、専任のセキュリティ担当が少なく、制度資料の読み込みと通常業務を並行して進めるだけでも負荷が大きくなります。外部支援を利用すると、要求事項を社内業務に落とし込み、担当部署を決め、必要資料と改善施策を整理する作業を短縮しやすくなります。

公表資料だけでは自社への当てはめが難しい

制度の要求事項は共通でも、実際の対策は企業ごとに異なります。同じ従業員数でも、オンプレミス中心の企業、SaaS中心の企業、自社開発Webサービスを持つ企業、工場や拠点ネットワークを持つ企業では、重要資産も攻撃経路も異なります。

そのため、「要求事項に書いてある製品を入れる」のではなく、自社の適用範囲、情報資産、取引先との接続、外部公開システム、権限管理の実態を確認し、どの対策が必要かを判断する必要があります。経験のある支援会社は、制度文言を単純にチェックリスト化するのではなく、自社環境に合わせて実装方法と証跡を設計できます。

SCS評価制度対応を外部委託する6つのメリット

1. 要求事項の読み違いと手戻りを減らしやすい

制度対応では、「対策しているつもり」と「評価基準を満たしている」が一致しないことがあります。例えば、バックアップを取得していても復旧テストを行っていない、管理者権限を制限していても棚卸し記録がない、といったケースです。外部専門家を早い段階から入れることで、何を実施し、何を証跡として残すべきかを整理しやすくなります。

2. ギャップ分析から改善計画まで一気通貫で進められる

効率的な進め方は、まず現状を評価し、不足項目を「すぐ直せるもの」「予算が必要なもの」「経営判断が必要なもの」に分けることです。支援会社がプロジェクト管理まで担えば、規程改定だけが先行したり、ツール導入だけが進んだりする状態を避けやすくなります。

3. 社内リソースを本来業務に集中させやすい

証跡収集、会議設定、規程と実運用の突合、課題管理、ベンダー調整は想像以上に工数がかかります。外部支援を利用すると、社内担当者は意思決定や現場調整に集中し、専門的な資料作成や技術整理を外部に任せることができます。

4. 技術対策の実効性まで確認できる

制度対応では、文書を整えるだけでなく、実際のシステムに弱点がないかを確認することが重要です。外部公開Webシステムがある場合はWebアプリケーション診断、サーバやネットワーク機器にはプラットフォーム診断、複数の弱点を組み合わせた侵入可能性や被害範囲を確認したい場合はペネトレーションテストが有効です。

例えば、規程上は「外部公開システムの脆弱性を管理する」と定めていても、古いミドルウェア、不要な管理画面、設定不備、認証回避につながる実装上の問題が残っていればリスクは低減しません。制度対応と技術診断を別々に扱わず、検出した問題を改善計画に反映することで、実効性のある対策につながります。

5. 経営層・取引先へ説明しやすい材料を作れる

セキュリティ投資は、単に「危険だから必要」と説明するだけでは稟議が通りにくいことがあります。外部支援では、要求事項とのギャップ、想定される事業影響、改善優先度、必要予算、対応期限を整理し、経営層が判断しやすい形にできます。取引先からセキュリティ体制を問われた際にも、制度に沿った説明資料や改善状況を提示しやすくなります。

6. 取得後の継続運用まで見据えられる

★3は有効期間1年、★4は3年で、★4も有効期間中に年次の自己評価が求められる考え方が示されています。つまり、取得時だけ集中的に整備しても、運用が続かなければ更新時に負担が戻ります。外部支援を選ぶ際は、取得支援だけでなく、定期点検、教育、再診断、ログ運用、インシデント対応訓練などを継続支援できるかも重要です。

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に関する制度構築方針」
https://www.ipa.go.jp/security/scs/rcu1hd0000007ajp-att/20260327001-br.pdf

外部委託しても自社に残すべき判断

SCS評価制度対応は、支援会社へ全面的に任せればよいわけではありません。特に次の判断は、自社の経営層や責任部門が主体となるべきです。

- どの事業・組織・拠点・システムを適用範囲とするか
- どの情報資産や業務を重要と位置づけるか
- 残存リスクをどこまで受容するか
- 改善予算と優先順位をどう決めるか
- 取引先や顧客にどの水準を示す必要があるか
- 日常運用の責任者・承認者を誰にするか

支援会社は判断材料を整理し、選択肢とリスクを示す役割です。最終判断まで外部任せにすると、取得後に社内で運用できず、手順書だけが残る状態になりやすいため注意が必要です。

★3と★4で外部委託の考え方はどう変わるか

★3：自己評価の精度と改善実行力を高める支援が中心

★3では自己評価が中心となるため、支援会社には要求事項の解釈、現状調査、ギャップ分析、規程・手順整備、証跡確認、技術対策の実装支援が期待されます。最終的な申請には制度上の要件を満たすセキュリティ専門家による確認が必要です。

支援会社を選ぶ際は、「SCS評価制度の資料を読んでいる」だけでなく、実際に情報セキュリティ規程、アクセス管理、脆弱性管理、バックアップ、教育、委託先管理などを設計・運用した経験があるかを確認するとよいでしょう。

★4：第三者評価を見据えた事前整備と技術検証への対応が重要

★4では指定評価機関による第三者評価があるため、支援会社には「評価を代行する」ことではなく、評価に耐えられる状態を作る支援が求められます。文書と現場運用の不一致、ログや棚卸し記録の不足、技術対策の未実装があれば、実地審査や技術検証で課題になります。

なお、IPAのFAQでは、★4の第三者評価と、取得に向けたコンサルティングや製品・サービス提供を同一法人が行うことを一律に否定していない一方、中立性・公平性に関する要件が論点となっています。実際に依頼する際は、評価業務とコンサルティング業務の責任分離、利益相反管理、指定状況を確認することが重要です。

出典：IPA「よくある質問」 https://www.ipa.go.jp/security/scs/faq.html

SCS評価制度の支援会社を選ぶ7つのポイント

1. 制度要求だけでなく、実装・運用まで支援できるか

チェックシート回答や文書作成だけの支援では、実運用との乖離が残る可能性があります。アクセス権限、端末管理、クラウド設定、ログ監視、バックアップ、脆弱性管理など、技術領域まで踏み込める会社を選ぶと、改善計画を実装までつなげやすくなります。

2. Web・プラットフォーム・ペネトレーションテストの能力があるか

自社でWebサービスを提供している企業はWebアプリケーション診断、インターネット公開サーバやネットワーク機器を持つ企業はプラットフォーム診断の経験を確認します。重要システムについて、単発の脆弱性列挙ではなく侵入経路や権限拡大、横展開まで確認したい場合は、ペネトレーションテストの実績も有効な判断材料です。

3. 経営と技術の両方を説明できるか

技術担当者には設定レベルまで説明でき、経営層には事業停止、信用毀損、取引影響、投資優先度として説明できる会社が望まれます。制度対応は複数部門にまたがるため、専門用語だけで会話する会社より、経営会議や稟議で使える説明に変換できる会社の方が実務では進めやすくなります。

4. 自社規模・業種に合わせた設計ができるか

大企業向けの重い統制をそのまま中堅企業に持ち込むと、運用負荷が高くなります。逆に最低限の形式整備だけでは、取引先が求める水準に届かない可能性があります。既存のISMS、Pマーク、社内規程、Microsoft 365やGoogle Workspace、EDRなどを活用し、追加投資を必要最小限にできる設計力を確認してください。

5. 評価機関・専門家との役割分担を理解しているか

特に★4では、コンサルティング支援と第三者評価の役割を明確に分ける必要があります。2026年10月22日時点では、指定評価機関・技術検証事業者の公表は2026年12月下旬予定です。公表後に依頼先を決める場合は、IPAの指定機関台帳で正式な指定状況を確認することが重要です。

出典：IPA「SCSセキュリティ専門家・評価機関」
https://www.ipa.go.jp/security/scs/security-experts-organization/index.html

6. 成果物が取得後も使えるか

成果物は「監査のための資料」ではなく、日常運用で使えることが重要です。最低でも、ギャップ分析結果、改善ロードマップ、規程・手順、対象システム一覧、責任分担、証跡一覧、リスクと優先順位、残課題、次回点検時期が整理されているかを確認しましょう。

7. 機密情報の取り扱いが明確か

SCS評価制度対応では、ネットワーク構成図、アカウント管理情報、脆弱性情報、委託先情報、インシデント記録など機微な情報を外部へ共有することがあります。秘密保持契約、アクセス制御、データ保管場所、再委託の有無、作業終了後のデータ削除、診断時の安全管理を事前に確認してください。

RFP・見積依頼時に支援会社へ伝えるべき内容

見積金額の比較だけでは、支援範囲が異なり適切に比較できません。RFP（提案依頼書）や見積依頼では、少なくとも自社の希望する★、対象組織、拠点数、従業員規模、主要システム、外部公開システム、既存認証、利用中のセキュリティ製品、希望時期、支援してほしい範囲を伝えるとよいでしょう。

また、「現状評価だけ」「改善計画まで」「規程改定まで」「技術対策導入まで」「診断まで」「申請・評価対応まで」のどこまでを依頼するかを分けて見積もると、不要な作業を減らしやすくなります。

費用と期間を左右する主な要因

SCS評価制度対応の外部委託費用は、企業規模だけで決まるものではありません。対象範囲、現状の成熟度、規程整備状況、拠点数、システム数、技術診断の対象、改善施策の量、希望スケジュールで大きく変わります。特に★4は第三者評価・技術検証が必要となるため、★3よりも準備と評価対応の工数が増えることが想定されます。

期間についても、既存のISMS運用があり証跡が揃っている企業と、資産台帳や権限棚卸しから始める企業では大きく異なります。予算化の際は「コンサルティング費」「評価・確認費」「脆弱性診断等の技術検証費」「製品・設定変更など改善費」「社内工数」を分けて見積もると、経営層にも説明しやすくなります。

よくある失敗と注意点

取得直前に支援会社へ相談する

要求事項への不足が見つかっても、製品導入、規程改定、教育、ログ蓄積などには時間がかかります。特に「運用実績」を示す項目は短期間では準備できない場合があります。取引先から取得を求められる可能性がある企業は、早めにギャップ分析だけでも実施しておくと対応しやすくなります。

文書作成だけで対策が完了したと考える

実態のない規程や手順は、インシデント発生時に機能しません。例えば「脆弱性を定期的に確認する」と規程に書いても、診断対象、頻度、責任者、重大度の判断、修正期限、再診断方法が決まっていなければ運用は止まります。外部委託では、文書と運用をセットで設計できるかを確認してください。

支援会社と評価主体を同じものと考える

SCS評価制度では、支援会社がそのまま制度上の評価主体になるとは限りません。★3では要件を満たすSCSセキュリティ専門家、★4では指定評価機関・技術検証事業者が制度上の役割を持ちます。コンサルティング契約を結ぶ前に、「誰が改善支援をするのか」「誰が制度上の確認・評価をするのか」を明確にしてください。

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単なる申請準備としてではなく、企業のセキュリティ水準を実際に高めるプロジェクトとして支援します。制度要求の整理、適用範囲の検討、ギャップ分析、リスクアセスメント、規程・手順整備、技術対策の設計、証跡準備、経営層向け説明まで、企業ごとの環境に合わせて支援内容を設計できます。

また、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・運用支援、インシデントレスポンス、デジタルフォレンジック、セキュリティ教育、SBOM、M&AにおけるIT・サイバーセキュリティデューデリジェンスなど、制度対応の前後で必要になる技術・運用施策を一気通貫で支援できる点が特徴です。

「★3と★4のどちらを目指すべきか」「どこまでを適用範囲にすべきか」「既存のISMSやPマークの仕組みをどこまで流用できるか」といった初期段階から相談可能です。まず現状を整理し、取引先要件、予算、期限を踏まえて優先順位を付けることで、過剰投資を避けながら実効性のある対応を目指します。

よくある質問

Q1. SCS評価制度への対応は必ず外部委託する必要がありますか？

いいえ。社内に制度を理解したセキュリティ人材がおり、要求事項の評価、規程整備、技術対策、証跡管理まで対応できれば内製も可能です。ただし、★3では制度要件を満たすセキュリティ専門家の確認が必要で、★4では指定評価機関による第三者評価・技術検証が必要です。

Q2. 外部委託するなら、どの段階から相談するのがよいですか？

取得直前よりも、適用範囲を決める前または現状評価の段階から相談する方が効率的です。初期の設計を誤ると、不要なシステムまで対象に含めたり、逆に重要な範囲が漏れたりする可能性があります。

Q3. ★3と★4のどちらを目指すか決まっていなくても相談できますか？

可能です。取引先から求められる水準、自社が扱う情報、事業停止時の影響、外部接続や委託の状況を整理し、必要な段階を判断します。★3を先に取得しなければ★4を取得できない制度ではありません。

Q4. ISMSやPマークを取得済みでも外部支援は必要ですか？

必須ではありませんが、既存認証とSCS評価制度では目的や要求範囲が異なります。既存の規程・教育・リスク管理を再利用しつつ、SCS評価制度で追加確認が必要な技術対策やサプライチェーン対策をギャップ分析すると効率的です。

Q5. Webアプリケーション診断はSCS評価制度対応で必ず必要ですか？

対象環境や取得する段階、評価・技術検証の設計によって異なります。自社が外部公開Webシステムを持つ場合は、制度対応とは別にリスク管理上の重要性が高く、必要に応じて診断を行うことが有効です。

Q6. ペネトレーションテストと脆弱性診断は同じですか？

同じではありません。脆弱性診断は既知の脆弱性や設定不備などを体系的に確認することが中心です。ペネトレーションテストは、実際の攻撃を想定して複数の弱点を組み合わせ、侵入や権限拡大、重要情報への到達可能性を検証します。

Q7. 支援会社を選ぶ際に最も重視すべき点は何ですか？

制度理解だけでなく、技術・運用・経営の3つをつなげられるかが重要です。現状評価から改善、診断、運用定着まで対応できるか、また★3の専門家確認や★4の第三者評価との役割分担を正しく説明できるかを確認してください。

Q8. 2026年10月時点で★4の評価機関は選べますか？

IPAは指定機関台帳への登録・公表を2026年12月下旬に予定しています。2026年10月22日時点では公表前のため、正式な依頼先を決める際は公表後にIPAの台帳で指定状況を確認することが重要です。

まとめ｜外部委託は「取得代行」ではなく、実効性を高めるために活用する

SCS評価制度対応を外部委託する最大のメリットは、社内負荷を減らすことだけではありません。制度要求を自社の事業・システムに落とし込み、優先順位を付け、技術対策と運用をつなげ、第三者へ説明できる状態を効率よく作れることにあります。

一方で、適用範囲、リスク受容、予算、責任体制といった経営判断まで外部へ丸投げすべきではありません。支援会社には専門知識と実行力を求め、自社は意思決定と継続運用の主体になる。この役割分担が、SCS評価制度を単発の取得プロジェクトで終わらせないためのポイントです。

支援会社を選ぶ際は、SCS評価制度の知識だけでなく、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などの技術力、規程・体制整備、経営層への説明力、取得後の運用支援まで確認するとよいでしょう。

SCS評価制度への対応方法が固まっていない段階でもご相談いただけます

Librus株式会社では、「まず何から確認すべきか分からない」「★3と★4のどちらが自社に適しているか判断したい」「取引先から対応を求められる前に準備したい」「既存のISMS・Pマークやセキュリティ製品を活用して追加投資を抑えたい」といった段階からご相談いただけます。

現状の体制やシステム、取引先から求められる水準、予算・スケジュールを整理したうえで、必要な対象範囲と優先順位を明確にすることで、社内稟議やベンダー選定を進めやすくなります。制度対応だけでなく、診断・改善・運用まで含めた一気通貫の支援が必要な場合も、企業ごとの課題に応じて支援内容を設計します。

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