SCS評価制度の取得費用は？評価料金と対策コスト・予算の考え方

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）の取得を検討するとき、経営層や情報システム部門が最初に気になるのが「結局、いくら必要なのか」という点です。結論から言えば、SCS評価制度の費用は、IPAに支払う登録料だけで判断できません。実際の予算は、登録料に加えて、★3の専門家確認、★4の第三者評価・技術検証、社内規程や証跡の整備、脆弱性対策、必要に応じた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、さらに社内担当者の工数まで含めて考える必要があります。

2026年9月18日にIPAが公表した料金では、2028年3月31日までの申請について、★3登録希望組織の登録料は10,000円（税込・1年分）、★4は60,000円（税込・3年分）です。2028年4月1日以降は、★3が20,000円（税込・1年分）、★4は60,000円（税込・3年分）とされています。ただし、これは制度運営側に支払う登録料であり、取得に必要な総費用ではありません。

本記事では、従業員100～1,000名程度の企業を想定し、SCS評価制度の費用構造、予算を左右する要因、見積もり時の確認事項、社内稟議での説明方法、費用を抑えながら実効性を高める考え方まで実務的に解説します。

この記事で分かること

- SCS評価制度で公式に公表されている登録料
- 登録料以外に発生する専門家確認・評価・技術検証・改善対応の費用
- ★3と★4で予算構造が異なる理由
- 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予算に入れる判断基準
- 経営層・情報システム部門が社内稟議で説明すべきポイント
- 見積依頼時に確認すべき項目と、支援会社の選び方

SCS評価制度の取得費用は「登録料＋評価・確認＋改善費用」で考える

SCS評価制度の費用を考える際は、少なくとも「制度上の登録費用」「評価・確認に関する外部費用」「要求事項を満たすための改善費用」「社内工数」の4つに分けると整理しやすくなります。登録料だけを見ると負担は限定的ですが、実務では現状と要求事項の差分を埋めるための対策費が総額を大きく左右します。

費用区分	主な内容	金額の決まり方
登録料	IPAの台帳に★3・★4を登録するための費用	IPAが公表
確認・評価費用	★3の専門家確認、★4の第三者評価・実地審査等	専門家・評価機関との契約で決定
技術検証費用	★4で必要となる脆弱性診断等の技術検証	対象範囲・方式・事業者で変動
改善・対策費用	規程整備、MFA、端末防御、ログ、バックアップ、脆弱性対応等	現状とのギャップで変動
社内工数	資料収集、証跡整理、部門調整、審査対応、稟議等	組織規模・対象範囲・成熟度で変動

IPAが公表している★3・★4の登録料

IPAの「SCS評価制度 料金設定のお知らせ」（2026年9月18日）では、登録希望組織の登録料が次のとおり示されています。料金には消費税・地方消費税が含まれ、適用時期は申請日が基準です。

区分	2028年3月31日までの申請	2028年4月1日以降の申請
★3	10,000円（1年分）	20,000円（1年分）
★4	60,000円（3年分）	60,000円（3年分）

重要なのは、この金額を「取得費用の総額」と誤解しないことです。★3では要求事項への適合確認、★4では第三者評価と技術検証が必要であり、これらの外部費用は登録料とは別に発生します。評価機関や技術検証事業者のサービス料金は制度として一律に決められているわけではなく、対象範囲や作業量に応じて個別に見積もられるのが基本です。

なぜ今、SCS評価制度の予算を検討しておく必要があるのか

SCS評価制度は任意制度ですが、委託元が取引先に対して必要な★を提示し、対策状況を確認する利用方法が想定されています。そのため、自社が制度対応を後回しにしている間に、主要顧客の調達基準や委託先評価に★3・★4が組み込まれる可能性があります。特に、大企業のサプライチェーンに入っている企業、機密情報や個人情報を預かる企業、システム運用・開発を受託する企業では、セキュリティ評価が営業・調達・契約更新に影響しやすくなります。

予算面では、制度開始直前にまとめて対策しようとすると、規程整備、システム改修、製品導入、診断、審査準備が同時並行になり、費用と社内負荷が膨らみやすくなります。反対に、現状分析を先に行い、必須対策・優先対策・中長期対策に分けて年度予算へ落とし込めば、無駄な製品導入や重複投資を抑えやすくなります。

★3と★4では費用の構造が異なる

★3は「要求事項への適合」と「確認可能な証跡」が予算の中心

★3を目指す場合、まず要求事項・評価基準に対して自社の現状を棚卸しし、不足項目を埋めます。費用が発生しやすいのは、アクセス権限管理、多要素認証、端末保護、バックアップ、パッチ・脆弱性管理、インシデント対応手順、委託先管理、教育、ログ管理などです。すでにISMS等を運用している企業は既存規程や証跡を活用できる可能性がありますが、文書が存在するだけでは十分ではありません。実際の運用記録や承認履歴、棚卸し結果など、実施を説明できる証跡が必要です。

外部のSCSセキュリティ専門家による確認を依頼する場合、その費用も予算化します。金額は制度で一律に定められていないため、対象拠点数、資料量、事前支援の有無、確認回数などを見積条件として明示することが重要です。

★4は第三者評価・実地審査・技術検証まで含めて考える

★4では、評価機関による第三者評価に加え、技術検証が求められます。IPAは評価機関の業務として、文書確認・実地審査・技術検証を含む第三者評価を示しています。技術検証は、外部公開資産や対象システムに対する脆弱性診断等が中心になるため、対象IP数、Webアプリケーション数、認証有無、ネットワーク構成、クラウド利用範囲などによって費用が変動します。

ここで、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同じものとして扱わないことが重要です。Webアプリケーション診断はWeb機能の脆弱性、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

器等の脆弱性を確認します。ペネトレーションテストは、想定シナリオに基づき実際に侵入可能性や影響を検証するため、一般に対象設計や試験内容がより個別化されます。SCS評価制度に必要な技術検証の範囲と、自社がリスク低減のために追加で実施したい検証を切り分けることで、過不足のない予算を組みやすくなります。

SCS評価制度の総コストを左右する7つの要因

1. 現状のセキュリティ成熟度

既存の規程、ISMS、端末管理、ID管理、バックアップ、ログ、教育、脆弱性管理が整っているほど追加対策は少なくなります。反対に、ルールが部門ごとに分散していたり、運用証跡が残っていなかったりすると、整備工数が増えます。

2. 対象範囲

本社だけか、複数拠点・工場・子会社まで含むかで資料数と審査対応が変わります。システムについても、社内IT、クラウド、外部公開サービス、委託先環境のどこまでを対象とするかを先に定める必要があります。

3. 目指す段階

★3と★4では確認方法が異なり、★4は第三者評価・技術検証を含むため外部費用が増える可能性があります。取引先から要求される水準、自社の営業戦略、扱う情報の重要性から目標を決めます。

4. 不足している技術対策

MFA、EDR、資産管理、ログ収集、バックアップ強化、脆弱性管理などを新規導入する場合は初期費用と継続費用の両方が発生します。製品購入ありきではなく、要求事項とリスクに対して必要な対策を選ぶべきです。

5. 診断・技術検証の対象量

IP数、Web画面数、API数、認証方式、クラウド資産、試験環境の有無、再診断回数などが見積金額に影響します。

6. 社内の証跡整備状況

アクセス権棚卸し、教育記録、インシデント訓練、委託先評価、バックアップ復旧テスト等の記録が整理されていると、審査準備が効率化します。

7. 外部支援の範囲

ギャップ分析のみ、規程整備まで、ツール選定まで、診断まで、審査対応までなど、委託範囲によって支援費用が変わります。

予算は「取得費」ではなく3段階で組む

社内稟議では、SCS評価制度の予算を一括の「認証取得費」として申請するより、次の3段階に分けると説明しやすくなります。

第1段階：現状把握・ギャップ分析

要求事項に対して何が満たせており、何が不足しているかを確認します。ここで対象範囲と優先順位を固めることで、後工程の見積精度が上がります。

第2段階：不足対策の実装・運用

規程、技術対策、教育、証跡取得、委託先管理、インシデント対応などを整えます。複数年度で対応できる項目と、申請前に必須の項目を分けることが重要です。

第3段階：確認・評価・登録

★3の専門家確認、★4の第三者評価・技術検証、必要な是正・再確認、IPAへの登録を行います。

この分け方にすると、「登録料は小さいのに、なぜ数十万～数百万円規模の予算が必要になる可能性があるのか」といった経営層の疑問に対して、制度費用と改善投資を分離して説明できます。なお、ここで示した金額レンジは例示していません。2026年10月22日時点で、専門家・評価機関・技術検証・コンサルティングの公式な一律料金は公表されておらず、個社の条件によって変動するためです。

費用を抑えるために最初にやるべきこと

対象範囲を広げすぎない

「会社全体を全部見てもらう」と曖昧に依頼すると、調査・資料収集・診断対象が膨らみます。取引上どの事業・拠点・システムに★が必要なのかを確認し、その範囲から着手します。ただし、形式的に範囲を狭めて実際のリスクを外すのは適切ではありません。情報の流れや委託関係を踏まえ、説明可能な範囲設定にする必要があります。

既存のISMS・社内規程・監査証跡を再利用する

すでにISMS、Pマーク、取引先監査、内部統制、BCP、IT資産管理などを運用している場合、既存文書や証跡をSCS評価制度の要求事項にマッピングすると、ゼロから作り直す費用を抑えられます。重要なのは「既存資料があるか」ではなく、「要求事項に対して何を根拠に適合と説明できるか」です。

製品導入の前に運用で解決できるか確認する

セキュリティ対策では、新しいツールを入れれば解決するとは限りません。権限棚卸し、アカウント廃止、パッチ適用ルール、委託先管理、教育、バックアップ復旧訓練など、既存機能と運用改善で対応できる項目もあります。ギャップ分析の前に製品を購入すると、過剰投資になりやすいので注意が必要です。

見積依頼前に準備するとよい資料

支援会社や評価関連事業者へ見積もりを依頼する前に、組織図、拠点一覧、ネットワーク概要図、システム・クラウド一覧、外部公開資産一覧、情報資産管理台帳、セキュリティ規程、アクセス権限管理の記録、教育・訓練記録、委託先一覧、インシデント対応手順、バックアップ方針、直近の脆弱性診断報告書などを整理しておくと、見積精度が上がります。すべてがそろっていなくても、欠落している資料自体がギャップの把握につながります。

RFP・見積依頼で確認すべきポイント

- ★3・★4のどちらを前提とした支援か
- ギャップ分析、規程整備、証跡作成支援、技術対策、診断、審査対応のどこまでが含まれるか
- Webアプリケーション診断・プラットフォーム診断・技術検証の対象数と単価条件
- 再診断・是正確認の回数と追加料金条件
- 現地対応が必要な場合の交通費・出張費の扱い
- 報告書・成果物の内容、経営層向け説明資料の有無

- 機密情報・個人情報・診断データの保管方法と削除方針
- 評価機関との独立性・利益相反に問題がないか
- 取得後の運用・更新支援が別料金かどうか

価格だけを比較すると、後から「規程整備は対象外」「再診断は追加費用」「評価機関との調整は含まれない」といった差が出やすくなります。総額と作業範囲を同時に比較することが重要です。

SCS評価制度の予算策定でよくある失敗

登録料だけを予算化する

最も起きやすい失敗です。登録料は制度上の費用の一部であり、不足対策や専門家確認、評価、技術検証の費用は別です。まずギャップ分析を行い、総費用を見積もる必要があります。

診断費用だけ計上し、是正費用を入れない

脆弱性診断で問題が見つかった場合、設定変更、改修、機器更新、クラウド構成変更などの是正費用が発生します。また、是正後に再診断が必要になる場合もあります。診断費と是正費を別枠で考えると予算超過を防ぎやすくなります。

各部門の工数を無視する

SCS評価制度対応は情報システム部門だけで完結しません。総務、人事、法務、購買、営業、開発、経営層などが関わる場合があります。資料収集、承認、契約見直し、教育、委託先管理などの社内工数もスケジュールと予算の一部として扱うべきです。

取得を目的化し、運用費を見ない

セキュリティは取得時だけ整えれば終わるものではありません。ログ監視、端末保護、脆弱性管理、教育、バックアップ確認、権限棚卸しなどには継続費が発生します。初年度の構築費と翌年度以降の運用費を分けて稟議することが重要です。

SCS評価制度の支援会社を選ぶポイント

支援会社を選ぶ際は、制度文書の読み解きだけでなく、実際のセキュリティ対策まで対応できるかを確認します。SCS評価制度では、規程・運用・技術対策・証跡がつながっていることが重要です。そのため、コンサルティングだけでなく、脆弱性診断、ペネトレーションテスト、SOC／CSIRT、インシデント対応、教育など、発見した課題を改善までつなげられる体制があると、複数ベンダー間の調整コストを抑えやすくなります。

また、経営層向けには取引継続・信用・事業継続の観点、情報システム部門には技術対策と運用負荷、現場部門には具体的な変更点を説明できる支援会社が望ましいでしょう。制度取得だけでなく、その後の運用を前提に設計できるかが重要です。

Librus株式会社が支援できること

Librus株式会社では、SCS評価制度への対応について、要求事項の読み解きだけでなく、現状分析、対象範囲の整理、ギャップ分析、優先順位付け、規程・証跡整備、技術対策、診断、改善、運用まで一気通貫で支援できます。

特に、SCS評価制度の費用を検討する段階では、「何にいくらかかるか」を先に断定するのではなく、自社の現状と目標とする★、取引先から求められる水準、対象システム、既存対策を確認したうえで、必須対応と推奨対応を分

けることが重要です。Librus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、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、リスクアセスメントなどの技術サービスとコンサルティングを組み合わせ、企業ごとの環境に応じた計画を設計します。

大企業から中堅・中小企業まで、M&A、IPO、取引先監査など経営上の重要局面を含め、技術と経営の両面から支援できることがLibrusの特徴です。SCS評価制度についても、取得そのものだけでなく、取引継続や営業上の信頼性向上につながる運用を重視します。

SCS評価制度の費用に関するよくある質問

Q1. SCS評価制度の取得費用はいくらですか？

公式に確定している登録料は、2028年3月31日までの申請で★3が10,000円（税込・1年分）、★4が60,000円（税込・3年分）です。ただし、専門家確認、第三者評価、技術検証、不足対策、社内工数は別途必要です。

Q2. ★3と★4ではどちらの方が費用が高くなりますか？

一般に、★4は第三者評価・実地審査・技術検証を伴うため、外部費用は増えやすいと考えられます。ただし、総額は現状の対策状況と対象範囲で変わります。

Q3. ISMSを取得していれば費用を抑えられますか？

既存の規程、リスク評価、教育、監査、アクセス管理等を活用できる場合は、整備工数を抑えられる可能性があります。ただし、SCS評価制度の要求事項に対して不足がないかを別途確認する必要があります。

Q4. 脆弱性診断は必ず必要ですか？

★4では技術検証が求められます。具体的な対象や方法は制度文書・評価機関との調整に基づき決めます。★3でも、自社のリスクや取引先要求に応じて診断が有効な場合があります。

Q5. ペネトレーションテストまで必要ですか？

必ずしも全社がペネトレーションテストを実施するとは限りません。要求事項、対象システムの重要性、既存診断の結果、取引先要求を踏まえて必要性を判断します。

Q6. 取得までの期間はどの程度見ておくべきですか？

一律には決められません。規程や技術対策が整っている企業と、ゼロから整備する企業では大きく異なります。制度開始前からギャップ分析を実施し、改善期間を確保することが重要です。

Q7. 予算申請では何を説明すればよいですか？

登録料、外部確認・評価費、技術検証費、改善費、継続運用費を分け、取引継続、顧客要求、事業継続、信用毀損リスクとの関係を説明すると理解を得やすくなります。

Q8. まだ★3か★4か決まっていなくても相談できますか？

可能です。主要取引先、扱う情報、事業の重要性、現在の対策状況を確認し、どの水準を目指すべきか、どこから予算化すべきかを整理するところから進められます。

まとめ｜SCS評価制度の予算は「登録料」より「不足対策」を見積もる

SCS評価制度の登録料は、2028年3月31日までの申請で★3が10,000円（1年分）、★4が60,000円（3年分）と公表されています。しかし、企業が実際に確保すべき予算は登録料だけではありません。専門家確認、第三者評価、技術検証、規程・証跡整備、Webアプリケーション診断やプラットフォーム診断、必要に応じたペネトレーションテスト、システム改修、社内工数、取得後の継続運用まで含めて考える必要があります。

費用を適正化する最も有効な方法は、いきなり製品や診断を発注するのではなく、まず自社の対象範囲と現状を整理し、SCS評価制度の要求事項とのギャップを把握することです。必須対応と中長期改善を分ければ、稟議の精度を高めながら、取引先から求められるセキュリティ水準にも計画的に対応できます。

SCS評価制度の費用・対象範囲がまだ決まっていない段階からご相談いただけます

「★3と★4のどちらを目指すべきか分からない」「登録料以外にどの程度の対策が必要か把握できていない」「来年度予算にどこまで計上すべきか整理したい」といった段階でも問題ありません。Librus株式会社では、現状のセキュリティ対策、主要取引先からの要求、対象システム、既存のISMSや社内規程などを確認し、優先して対応すべき項目と後から改善できる項目を整理します。これにより、必要以上に対策範囲を広げたり、不要なツールを先に購入したりすることを避けながら、取得・取引継続に必要な予算の全体像を把握しやすくなります。対象範囲や実施方法がまだ固まっていない場合も、初期整理からご相談いただけます。

参考情報

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

IPA「SCS評価制度 料金設定のお知らせ」（2026年9月18日）:
https://www.ipa.go.jp/security/scs/rcu1hd00000075om-att/pricelist.pdf

IPA「SCS評価制度の詳細情報」: https://www.ipa.go.jp/security/scs/details.html

IPA「要求事項・評価基準」: https://www.ipa.go.jp/security/scs/requirements-criteria.html

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（SCS評価制度）」:
https://www.meti.go.jp/policy/netsecurity/scs.html

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