

SCS評価制度の取得費用はいくら？想定されるコストと対策費用を解説

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）の取得を検討する企業にとって、最も判断しづらい論点の一つが「結局、いくらかかるのか」です。結論から言えば、2026年10月22日時点で、IPAが公表している登録料は★3が10,000円／1年、★4が60,000円／3年です。いずれも税込みで、2028年3月31日までに申請した場合の料金です。2028年4月1日以降は★3が20,000円／1年となり、★4は60,000円／3年のままです。

ただし、この登録料だけでSCS評価制度を取得できるわけではありません。★3ではSCSセキュリティ専門家による確認が必要で、★4では評価機関による第三者評価に加え、脆弱性診断等の技術検証が求められます。さらに、自社の現状が要求事項を満たしていなければ、規程整備、端末・ネットワーク対策、ログ監視、教育、インシデント対応体制の整備などにも費用が発生します。

したがって、経営判断や社内稟議では「登録料はいくらか」ではなく、「登録料＋評価・専門家費用＋技術検証費用＋不足対策の改善費用＋社内工数」という総コストで考えることが重要です。本記事では、従業員100～1,000名程度の企業を想定し、SCS評価制度の取得費用の考え方、★3と★4で異なるコスト構造、予算化の進め方、費用を抑えるための実務ポイントを解説します。

この記事で分かること

- SCS評価制度の★3・★4の公式登録料
- 登録料以外に発生する専門家確認・第三者評価・技術検証・改善対応の費用
- 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が費用に影響する場面
- 取得費用が高くなりやすい企業の特徴と、予算を適切に配分する方法
- 社内稟議やRFPで確認すべきポイント

SCS評価制度とは何か

サプライチェーンの取引先評価を共通化する制度

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、企業のセキュリティ対策状況を共通の基準で評価し、その結果を登録・公表する制度です。IPAが運営し、★3・★4は2027年3月頃の運用開始が予定されています。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、必要な対策を促す利用方法が想定されています。

SCS評価制度は、単に「認証マークを取得する」ための制度ではありません。自社のIT基盤、ガバナンス、取引先管理、サイバー攻撃への防御・検知、インシデント対応、復旧までを確認し、サプライチェーン上のリスクを抑えることが目的です。

★3と★4では評価方法が異なる

★3は、企業が要求事項・評価基準に沿って自己評価を行い、その結果についてSCSセキュリティ専門家の確認・助言を受ける仕組みです。最終的に経営層による自己適合宣誓を含む申請を行います。

一方、★4は評価機関による第三者評価です。文書確認だけでなく、実地審査と技術検証が行われます。IPAは技術検証事業者の業務として、評価機関からの委託を受けて脆弱性診断を実施し、技術検証結果報告書を評価機関へ交付することを示しています。そのため、★4では★3よりも外部評価にかかる費用が大きくなりやすい構造です。

SCS評価制度の公式登録料はいくらか

★3は1万円、★4は6万円が現時点の登録料

IPAが2026年9月18日に公表した料金設定によると、2028年3月31日までに申請する登録希望組織の登録料は、★3が10,000円(税込、1年分)、★4が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。

重要なのは、これはあくまで「制度への登録料」であり、取得に必要な総コストではないという点です。★3の専門家確認費用や、★4の評価機関による第三者評価・技術検証費用は、この登録料には含まれていません。

登録料だけを見て予算を組むと不足しやすい

「★3なら1万円で取得できる」「★4なら6万円で済む」と捉えるのは適切ではありません。取得に向けた現状把握、要求事項とのギャップ分析、規程や証跡の整備、必要なセキュリティ対策の導入、技術検証、改善対応などを含めると、実際に必要な予算は企業ごとに大きく変わります。

経営層への説明では、公式登録料と、取得準備にかかる実務費用を分けて提示すると理解されやすくなります。

SCS評価制度の取得費用は5つに分けて考える

1. IPAへの登録料

まず確定しているのがIPAへの登録料です。★3は1年単位、★4は3年単位という違いがあります。更新時にも継続的な費用が発生する前提で、中期予算に反映しておく必要があります。

2. ★3のSCSセキュリティ専門家による確認費用

★3では、自己評価結果についてSCSセキュリティ専門家による確認・助言が必要です。社内に所定の力量要件を満たし、制度上の登録を受けた専門家がいれば内製できる可能性があります。一方、社外の専門家に依頼する場合は、その確認・助言に対する委託費が発生します。

2026年10月22日時点では、SCSセキュリティ専門家の公開は2027年1月頃から予定されており、全国一律の確認料金は公表されていません。したがって、現時点で特定の相場を断定するべきではありません。

3. ★4の第三者評価・技術検証費用

★4では、評価機関による第三者評価と技術検証が必要です。第三者評価には、自己評価結果や規程類の確認、関係者へのヒアリング、実地審査などが含まれます。技術検証は、評価対象となるIT基盤等に対して脆弱性診断を実施するものです。

費用は、評価対象となる拠点数、システム数、インターネット公開資産の数、ネットワーク構成、クラウド環境、対象範囲の複雑さなどに左右されると考えるのが現実的です。評価機関・技術検証事業者は2026年12月末頃から公表予定であり、各社のサービス料金はその後の見積確認が必要になります。

4. 要求事項を満たすための改善費用

実務上、最も差が出やすいのが不足対策の改善費用です。すでにISMS等を運用し、資産管理、アクセス制御、バックアップ、ログ管理、教育、インシデント対応などが整っている企業は、新規投資を抑えられる可能性があります。

一方、端末管理が部門ごとに異なる、管理者権限が整理されていない、インターネット公開資産を一覧化できていない、脆弱性管理が定期運用されていない、バックアップからの復旧確認をしていない、といった企業では、ツール導入や運用見直しに追加費用が必要です。

5. 社内工数とプロジェクト管理費用

見落とされやすいのが社内工数です。SCS評価制度への対応では、情報システム部門だけで完結しない場合があります。経営層、総務・法務、調達・購買、事業部門、システム管理者、委託先管理担当などから情報を集め、規程と実態を突き合わせる必要があるためです。

外部費用だけを予算化しても、社内担当者の時間を確保できなければプロジェクトは進みません。取得費用を検討する際は、人件費換算まではるかとは別として、必要工数と担当者を事前に明確にしておくべきです。

★3と★4で費用構造はどう違うか

★3は「自己評価＋専門家確認」が中心

★3では、要求事項・評価基準に沿った自己評価と、SCSセキュリティ専門家による確認が中心です。そのため、費用を左右するのは、現状の対策水準、自己評価を社内ですべて作成できるか、専門家にどこまで支援を依頼するかです。

たとえば、社内規程や証跡が整理されており、情報資産台帳、アカウント管理、教育記録、バックアップ記録、インシデント対応手順などがすぐ提出できる企業は、外部支援の範囲を限定しやすくなります。逆に、資料が各部署に散在している場合は、制度対応そのものよりも棚卸しと運用整理に工数がかかります。

★4は第三者評価と技術検証が加わる

★4では、第三者評価に加えて技術検証が必要です。特に技術検証では、脆弱性診断の対象範囲によって費用が変わります。Webアプリケーション、サーバー、ネットワーク機器、クラウド上の公開資産など、対象が多いほど検証工数は増えます。

また、診断で重大な脆弱性が見つければ、修正後の再診断が必要になる可能性があります。取得時の初回診断だけでなく、改修・再確認までを予算に入れておくことが重要です。

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と費用の関係

Webアプリケーション診断

Webアプリケーション診断は、Webサービスに対して認証・認可、入力値処理、セッション管理などの脆弱性を確認する診断です。対象画面数、機能数、API数、認証パターン、権限種別などにより工数が変わります。

SCS評価制度への対応を目的とする場合でも、むやみに全Webシステムを診断対象にするのではなく、評価対象範囲とリスクを踏まえて対象を整理することが重要です。

プラットフォーム診断

プラットフォーム診断は、サーバー、ネットワーク機器、OS、ミドルウェア、公開ポートなどの設定や既知脆弱性を確認する診断です。対象IP数や機器数が増えるほど費用に影響しやすいため、インターネット公開資産の棚卸しができていない企業では、まず資産を把握する必要があります。

ペネトレーションテスト

ペネトレーションテストは、単に脆弱性の有無を列挙するだけではなく、実際の攻撃者の視点で複数の弱点を組み合わせ、侵入や権限昇格、重要情報への到達可能性などを検証する手法です。一般に個別設計の割合が高く、脆弱性診断より工数が大きくなりやすい傾向があります。

SCS評価制度への対応だからといって、常にペネトレーションテストまで必要になるとは限りません。制度要求、取引先から求められる水準、自社のリスク、システムの重要度に応じて使い分けるべきです。

取得費用が高くなりやすい企業の特徴

対象範囲が広い、または決まっていない

複数拠点、複数クラウド、子会社、オンプレミス環境、外部委託先などを一度に評価対象とすると、確認する資産・証跡・運用が増えます。最初に「どの事業・組織・IT基盤を対象にするのか」を明確にすることが、費用管理の第一歩です。

IT資産とアカウントを把握できていない

端末、サーバー、クラウドサービス、ネットワーク機器、管理者アカウント、委託先アカウント等の棚卸しが不十分だと、評価前の調査作業が増えます。シャドーITや管理者不明の機器が多い企業ほど、取得準備に時間と費用がかかりやすくなります。

規程はあるが運用証跡がない

セキュリティ規程に「定期的に確認する」と記載されていても、実施記録が残っていなければ評価時に説明できません。アクセス権レビュー、バックアップ確認、教育受講、脆弱性対応、委託先評価などは、実施記録まで含めて整える必要があります。

改善を申請直前にまとめて行う

制度開始直前や取引先から取得要請を受けた後に、複数の対策を同時導入すると、緊急対応費用や社内調整コストが増えやすくなります。早い段階でギャップ分析を行い、短期・中期に分けて改善する方が、予算を平準化しやすくなります。

費用を抑えながらSCS評価制度に対応する進め方

最初にギャップ分析を行う

製品購入や診断の発注から始めるのではなく、公開されている要求事項・評価基準と自社の現状を突き合わせます。すでに満たしている項目、証跡を追加すれば満たせる項目、新規投資が必要な項目を分類すると、不要な支出を減らせます。

既存のISMS・Pマーク・社内統制を再利用する

既存のISMS、Pマーク、委託先管理基準、情報セキュリティ規程、BCP、内部監査、教育制度などにSCS評価制度と重なる要素がある場合、すべてを作り直す必要はありません。既存文書と運用をベースに、SCS評価制度の要求事項との差分だけを補う方法が合理的です。

技術検証の対象範囲を事前に整理する

★4を目指す場合、インターネット公開資産や対象IT基盤の一覧を事前に整理しておく、評価機関や技術検証事業者から適切な見積を取りやすくなります。対象が曖昧なままでは、見積に余裕分が上乗せされたり、後から追加費用が発生したりする可能性があります。

改善施策に優先順位を付ける

すべての改善を同時に行う必要はありません。事業停止や情報漏えいに直結する高リスク項目、制度上の必須項目、比較的少ない工数で改善できる項目を整理し、優先順位を付けます。経営会議では「取得のため」だけでなく、「既存の事業リスク低減にも効く投資」であることを説明すると、予算の妥当性を示しやすくなります。

社内稟議で説明すべき費用項目

初年度費用と継続費用を分ける

稟議では、初年度に発生するギャップ分析、規程整備、ツール導入、技術診断、評価対応の費用と、翌年度以降に発生する登録更新、運用、教育、定期診断、監視等の費用を分けることが重要です。初年度だけを見ると高額に見えても、複数年で見ると一時費用と継続費用の違いが明確になります。

「取得しない場合のコスト」も整理する

SCS評価制度はサプライチェーン取引での利用が想定されています。将来的に主要取引先から特定の★を求められる場合、未対応が新規取引や契約更新の障害となる可能性があります。稟議では、取得費用だけでなく、取引先対応、受注機会、監査対応負担、インシデント発生時の事業影響といった観点も併せて説明すると、経営判断につながりやすくなります。

見積依頼・RFPで確認すべきポイント

見積の内訳を分けてもらう

コンサルティング、ギャップ分析、規程整備、専門家確認、第三者評価、技術検証、再診断、改善支援を一式価格だけで提示されると、どこに費用がかかっているか判断しづらくなります。可能な限り工程別・対象別の内訳を確認しましょう。

追加料金が発生する条件を確認する

対象IP数の増加、追加ヒアリング、現地訪問、再診断、文書修正回数、対象拠点追加など、追加料金が発生する条件を契約前に確認します。★4では評価機関と技術検証事業者が別組織になる場合もあるため、窓口と責任分界も重要です。

機密情報の取り扱いを確認する

評価・診断では、ネットワーク構成、資産情報、アカウント運用、脆弱性情報、インシデント対応手順など、機密性の高い情報を扱います。秘密保持、データの保存場所、アクセス制御、再委託の有無、データ削除方法まで確認すべきです。

サービス提供会社の選び方

制度理解だけでなく技術と運用の両面を見られるか

SCS評価制度の取得支援では、チェックリストを埋めるだけでは不十分です。規程整備、資産管理、脆弱性管理、ログ監視、インシデント対応、委託先管理などを実際の運用に落とし込めることが重要です。

診断後の改善まで支援できるか

Webアプリケーション診断やプラットフォーム診断で脆弱性が見つかったも、修正方針や優先順位を決められなければ制度対応は進みません。報告書を納品して終わるのではなく、改修・再診断・運用改善まで支援可能かを確認しましょう。

経営層への説明を支援できるか

従業員100～1,000名規模の企業では、セキュリティ施策を情報システム部門だけの予算で判断できないことがあります。取引リスク、事業継続、信用、監査対応など、経営の言葉に置き換えて説明できる支援会社であれば、社内合意形成を進めやすくなります。

よくある失敗と注意点

公式登録料だけを「取得費用」と考える

最も避けたいのは、登録料だけで予算申請し、後から専門家確認や技術検証、改善費用が必要になるケースです。総コストを工程別に分解して見積もる必要があります。

高額なセキュリティ製品を先に導入する

SCS評価制度は特定製品の一律導入を求めるものではありません。現状分析をせずにEDR、SIEM、SOCサービス等を導入しても、別の要求事項に不足が残る可能性があります。まず要求事項とのギャップを確認してください。

診断を実施して終わる

脆弱性診断は重要ですが、見つかった問題を放置すれば対策水準は上がりません。リスクに応じた修正期限を決め、改修後の再診断や継続監視につなげる必要があります。

Librus株式会社が提供できるSCS評価制度対応支援

制度対応から技術検証・改善まで一気通貫で支援

Librus株式会社では、SCS評価制度への対応を単なる書類作成プロジェクトとしてではなく、実際のサイバーリスクを下げる取り組みとして支援します。現状把握、要求事項とのギャップ分析、対象範囲の整理、改善計画、規程・運用整備、脆弱性診断、ペネトレーションテスト、改善後の再確認まで、企業ごとの状況に応じて設計できます。

また、技術面だけでなく、経営層への説明、社内稟議、取引先からのセキュリティ要求への対応、M&AやIPOなど経営上の重要局面も含めて整理できる点が特徴です。必要以上の製品導入や対策を前提とせず、既存資産を活用しながら優先順位を付けることで、クオリティ、コスト、スピードのバランスを取った支援を目指します。

よくある質問

Q1. SCS評価制度の取得費用はいくらですか？

2026年10月22日時点でIPAが公表している登録料は、2028年3月31日までの申請で★3が10,000円／1年、★4が60,000円／3年です。ただし、専門家確認、第三者評価、技術検証、改善費用などは別途必要です。

Q2. ★3は1万円だけで取得できますか？

いいえ。1万円はIPAへの登録料です。SCSセキュリティ専門家による確認を社外に依頼する場合の費用や、要求事項を満たすための改善費用、社内工数は別途発生します。

Q3. ★4は6万円だけで取得できますか？

いいえ。6万円は3年分の登録料です。★4では評価機関による第三者評価と技術検証が必要であり、その費用は別途発生します。

Q4. ★3と★4ではどちらが費用を抑えられますか？

一般に、第三者評価と技術検証を伴う★4の方が外部費用は増えやすいと考えられます。ただし、必要な段階は取引先から求められる水準や自社のリスクによって判断すべきであり、費用だけで決めるべきではありません。

Q5. ISMSやPマークを取得済みなら安くできますか？

既存の規程、資産管理、アクセス管理、教育、委託先管理、監査記録等を再利用できれば、対応工数や改善費用を抑えられる可能性があります。ただし、既存認証があるだけでSCS評価制度の要求事項を自動的に満たすわけではありません。

Q6. 脆弱性診断はいくらかかりますか？

対象となるWebアプリケーションの機能数、IP数、機器数、認証方式、診断手法などにより変動します。SCS評価制度向けの技術検証については、評価対象範囲を整理したうえで指定評価機関・技術検証事業者へ見積りを依頼する必要があります。

Q7. ペネトレーションテストは必須ですか？

制度対応だから常にペネトレーションテストが必須とは限りません。必要な技術検証の内容、対象システムの重要性、取引先要件、自社のリスクに応じて判断します。

Q8. 費用がまだ確定していない段階でも準備できますか？

可能です。要求事項・評価基準はすでに公開されているため、現状分析、対象範囲の整理、資産棚卸し、証跡収集、改善項目の優先順位付けは先に進められます。先行して準備することで、正式な評価時の追加作業を減らしやすくなります。

まとめ | SCS評価制度の取得費用は「登録料」だけで判断しない

SCS評価制度の公式登録料は、2028年3月31日までの申請で★3が10,000円／1年、★4が60,000円／3年です。しかし、企業が実際に予算化すべきなのは、登録料だけではありません。★3ではSCSセキュリティ専門家の確認、★4では第三者評価と技術検証が必要であり、さらに要求事項を満たすための改善費用や社内工数が加わります。

費用を適正化するには、最初に対象範囲を決め、要求事項とのギャップを確認し、既存の規程・運用・認証を再利用することが重要です。そのうえで、高リスク項目から優先的に改善し、診断や外部支援の対象を適切に設定すれば、不要な投資を避けやすくなります。

SCS評価制度への対応は、単なる認証取得費ではなく、取引先からの信頼、事業継続、サプライチェーンリスク低減のための投資として捉えることが重要です。

SCS評価制度の費用・進め方で迷っている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」「対象範囲をどこまで含めるべきか決められない」「取得に必要な総予算を整理したい」といった段階でも、Librus株式会社へご相談いただけます。

Librus株式会社では、公開されている要求事項をもとに現状を整理し、既存の規程やセキュリティ対策をできる限り活用しながら、不足項目と優先順位を明確にします。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、改善支援、運用設計まで一気通貫で検討できます。

対象範囲や実施方法が固まっていない段階で整理を始めることで、過剰な対策への投資を避け、必要な予算とスケジュールを社内で説明しやすくなります。SCS評価制度への対応方針や費用感の整理から、お気軽にご相談ください。

出典

- IPA「SCS評価制度」: <https://www.ipa.go.jp/security/scs/index.html>
- 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>
- 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「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>
- IPA「よくある質問」: <https://www.ipa.go.jp/security/scs/faq.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>