

SCS評価制度の取得方法とは？申請から取得までの流れを解説

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★3・★4は、2027年3月頃の運用開始が予定されています。取得の基本は、対象範囲を決め、要求事項に対する自己評価と不足対策を行い、★3ではSCSセキュリティ専門家の確認、★4では指定評価機関による第三者評価・技術検証を経て、IPAへ登録申請する流れです。

重要なのは、申請書を作ること自体よりも、「自社のIT基盤が要求事項を実際に満たしている状態」を先に作ることです。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などが必要になる場面もありますが、制度対応は技術診断だけで完結しません。規程、権限管理、教育、インシデント対応、取引先管理などを含め、経営と現場を横断して準備する必要があります。

なお、2026年10月14日時点でIPAは★3・★4の詳細な申請方法や取得ガイドを「2026年10月頃に公開予定」と案内しています。したがって、本記事では公表済みの制度構築方針、評価スキーム、料金設定に基づき、現時点で確定している取得の流れと、企業が先行して準備できる実務を整理します。

この記事で分かること

- ・SCS評価制度の★3・★4を取得する基本的な流れ
- ・申請前に経営層・情報システム部門が準備すべき事項
- ・★3と★4で異なる評価方法と技術検証の位置付け
- ・取得期間・費用を左右する主な要因
- ・コンサルティング会社や診断会社を選ぶ際の確認ポイント

SCS評価制度とは

SCS評価制度は、サプライチェーンを構成する企業のセキュリティ対策状況を共通基準で評価・可視化し、委託元と委託先の双方がセキュリティ水準を確認しやすくする制度です。経済産業省と内閣官房国家サイバー統括室が制度構築方針を公表し、IPA（独立行政法人情報処理推進機構）が制度を運営します。

制度の直接の対象は、企業等のIT基盤です。クラウド環境も対象に含まれます。一方、一般的な製造設備のOTシステムや提供製品そのものは直接対象から外し、他制度・ガイドラインでの対応を想定しています。

★3と★4の違い

★3は、広く認知された脆弱性などを悪用する一般的なサイバー攻撃への対応を想定し、「全てのサプライチェーン企業が最低限実装すべき対策」という位置付けです。評価方式は、取得希望組織による自己評価にSCSセキュリティ専門家の確認を加える「専門家確認付き自己評価」です。

★4は、供給停止や機密情報漏えいなど、取引先や社会への影響がより大きい企業を念頭に、ガバナンス、取引先管理、システム防御・検知、インシデント対応まで包括的に確認します。指定評価機関による第三者評価に

加え、文書確認、実地審査、技術検証が行われます。なお、★3を先に取得しなければ★4を取得できない仕組みではありません。

なぜ今、SCS評価制度の取得準備が必要なのか

SCS評価制度は任意制度であり、法律によってすべての企業に取得が義務付けられるものではありません。ただし、制度は二社間の取引契約等で、委託元が委託先に求めるセキュリティ水準を★で提示する運用を想定しています。そのため、制度上は任意でも、特定の顧客との新規取引や継続取引の条件として取得が求められる可能性があります。

特に、自動車、半導体、流通、金融などサプライチェーンの結び付きが強い分野では制度利用の促進が想定されています。顧客から要請を受けてから着手すると、規程改定、端末・アカウント管理の見直し、脆弱性対応、ログ管理、教育、委託先管理など複数部門にまたがる改善が必要となり、取引上の回答期限に間に合わないことがあります。

SCS評価制度の取得方法：申請から登録までの基本フロー

1. 取得する★と適用範囲を決める

最初に、★3または★4のどちらを目指すかを決めます。判断材料は、取引先から求められている水準、自社の事業継続上の重要性、扱う情報の機密性、障害時の影響、現行のセキュリティ成熟度です。

同時に、評価対象となる適用範囲を整理します。本社だけを見るのか、支店・開発拠点・テレワーク環境を含めるのか、どのクラウド環境や業務システムを対象とするのかを曖昧にすると、後工程で証跡が不足します。ネットワーク構成図、システム一覧、クラウド利用一覧、端末台帳、アカウント管理表などを使って対象を可視化すると進めやすくなります。

2. 要求事項・評価基準に沿って自己評価する

IPAは★3・★4の要求事項・評価基準を公開しています。取得には、各段階で定められたすべての要求事項・評価基準を満たす必要があるとしています。まずは各項目について「実施済み」「一部実施」「未実施」を棚卸しし、根拠となる証跡があるかまで確認します。

ここで注意したいのは、担当者が「実施している」と認識しているだけでは十分ではないことです。例えば、退職者アカウントを削除するルールがあっても、実際の削除記録や定期レビュー記録が残っていなければ、運用の証明が難しくなります。規程と実態、システム設定と運用記録の両方を確認することが重要です。

3. 不足している対策を改善する

自己評価でギャップが見つかったら、取得日から逆算して改善計画を作ります。優先順位は、外部から悪用されやすい重大な脆弱性、特権IDや多要素認証など認証・権限管理、バックアップ、ログ監視、インシデント対応体制といった、攻撃時の被害拡大に直結する項目から付けると実務的です。

Webサービスを提供している企業ではWebアプリケーション診断、インターネット公開サーバーやネットワーク機器を保有する企業ではプラットフォーム診断が有効です。より実戦的に侵入経路や被害拡大可能性を確認した

い場合は、ペネトレーションテストを組み合わせる選択肢もあります。ただし、診断を実施しただけで要求事項が自動的に満たされるわけではありません。発見事項を是正し、再確認し、継続運用へ組み込むところまでが重要です。

4. 評価に必要な証跡・資料を整える

評価前には、情報セキュリティ方針、社内規程、組織図、責任分担、資産台帳、アカウント管理、パッチ適用記録、教育記録、インシデント対応手順、バックアップ実施記録、委託先管理資料、脆弱性診断報告書などを整理します。すべてを新規作成する必要はありません。既存のISMS資料、社内監査資料、取引先回答票などを流用できる場合があります。

実務上は、要求事項ごとに「担当部署」「対応状況」「根拠資料」「保存場所」「不足事項」「改善期限」を対応表にしておくと、審査準備と経営報告を一本化できます。

5. ★3はSCSセキュリティ専門家の確認を受ける

★3では、取得希望組織が作成した自己評価結果を、登録されたSCSセキュリティ専門家が確認します。専門家は内容を確認し、必要に応じて評価結果の修正を含む助言を行います。最終的に提出内容を了承した場合に署名し、取得希望組織は経営層による自己適合宣誓とともに事務局へ提出します。

SCSセキュリティ専門家については、2027年1月頃からIPAが公開する予定です。情報処理安全確保支援士、CISSP、CISA、CISM、ISO27001主任審査員などの資格要件に加えて、所定の研修受講等が求められます。

6. ★4は指定評価機関による第三者評価・技術検証を受ける

★4では、取得希望組織が自己評価を行った後、指定評価機関へ評価を依頼します。評価機関は文書確認、実地審査、技術検証を実施し、評価報告書を交付します。技術検証は、評価機関自身または指定された技術検証事業者が実施します。IPAは、技術検証事業者の主な対象として脆弱性診断・ペネトレーションテストのサービス提供法人を挙げています。

評価機関は2026年12月末頃から公開予定です。したがって★4を検討する企業は、制度開始直前に評価機関を探すのではなく、今のうちに対象範囲とギャップを整理し、公開後すぐ見積依頼できる状態にしておくスムーズです。

7. IPAへ登録申請し、台帳への登録・公表を受ける

★3では専門家確認済みの自己評価結果と経営層の自己適合宣誓等を、★4では評価機関から交付された評価報告書等を用いて、IPAの事務局へ登録申請する流れです。事務局が申請内容を確認し、問題が認められなければ台帳へ登録・公表されます。

2026年10月14日時点では、登録希望組織向けの詳細な提出様式やオンライン申請手順はまだIPAサイト上で公開待ちです。制度開始は2027年3月頃が予定されているため、最新の申請様式・取得ガイドが公開された段階で、最終的な提出物を確認してください。

申請前に経営層が判断すべきこと

SCS評価制度対応を情報システム部門だけの仕事にすると、途中で止まりやすくなります。経営層は少なくとも、取得する★、適用範囲、目標時期、予算、部門横断の責任者を決める必要があります。特に★4では実地審査や技術検証を伴うため、情報システム部門だけではなく、総務、人事、法務、購買、開発、事業部門が関係する可能性があります。

稟議では「認証・登録のための費用」とだけ説明するのではなく、主要顧客との取引継続、新規案件の参加要件、サイバー事故による供給停止の防止、既存の取引先セキュリティチェック対応の効率化といった経営上の目的に結び付けると、投資判断がしやすくなります。

情報システム部門が準備すべき資料

実施前に準備したい代表的な資料は、システム・端末・ネットワーク・クラウドの一覧、アカウントと権限の管理資料、脆弱性・パッチ管理記録、バックアップ設計と復旧手順、ログ取得・監視方針、インシデント対応フロー、委託先一覧、教育記録です。

個人情報や機密情報を外部の評価機関・診断会社へ提供する場合は、秘密保持契約、データの保存場所、再委託の有無、アクセス権限、評価終了後のデータ削除方法まで確認します。RFPや見積依頼書に最初からこれらの条件を入れておくと、後工程の調整を減らせます。

SCS評価制度の取得期間はどのくらいか

公的資料では、企業が★3・★4を取得するまでの標準期間は現時点で示されていません。実際の期間は、適用範囲、現状の成熟度、規程の整備状況、技術的な不足対策、評価機関の日程などで変わります。

そのため実務では、申請日だけを目標にするのではなく、「ギャップ分析」「改善」「証跡蓄積」「専門家確認または第三者評価」「申請」の各工程に期間を置いて計画することが重要です。特に、ログ保存や定期点検など運用実績そのものが証跡になる項目は、制度開始直前に仕組みを導入しても十分な記録が揃わない可能性があります。

SCS評価制度の取得費用を左右する要因

IPAが2026年9月18日に公表した料金設定では、登録希望組織の登録料は、2028年3月31日まで★3が1万円（1年分）、★4が6万円（3年分）です。2028年4月1日以降は★3が2万円（1年分）、★4が6万円（3年分）とされています。料金には消費税・地方消費税を含みます。

ただし、この登録料だけで取得できるわけではありません。★3では専門家確認の費用、★4では第三者評価や技術検証の費用が別途発生し得ます。また、MFA導入、端末管理、ログ監視、規程整備、脆弱性診断、ペネトレーションテスト、教育などの改善費用も企業ごとに異なります。

見積を比較するときは、単純な総額だけでなく、現状分析、改善支援、規程作成、技術診断、再確認、申請支援のどこまで含まれるかを確認してください。対象システム数や拠点数が後から増えると追加費用が発生するため、見積前のスコープ定義が重要です。

サービス提供会社を選ぶ際のチェックポイント

SCS評価制度への対応支援を依頼する際は、制度文書の解説だけでなく、実際の技術対策まで支援できるかを確認することが重要です。規程の整備だけ進めても、公開サーバーに重大な脆弱性が残っていれば評価準備として不十分です。逆に、脆弱性診断だけを実施しても、組織体制やインシデント対応、委託先管理が整っていないければ制度全体への対応にはなりません。

RFP・見積依頼では、SCS評価制度の要求事項への対応経験、★3・★4の支援範囲、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への対応可否、改善後の再診断、証跡整理、評価機関との役割分担、機密情報の管理方法を確認するとよいでしょう。★4の場合は、コンサルティング支援と第三者評価の独立性・公平性に関するルールにも注意が必要です。

よくある失敗と注意点

制度開始まで待ってから準備する

申請受付が始まってから準備すると、規程整備やシステム改修だけでなく、運用記録の蓄積が間に合わない可能性があります。要求事項はすでに公開されているため、現時点でもギャップ分析は始められます。

チェックリストを埋めることを目的にする

SCS評価制度は「書類を提出すれば取得できる制度」ではありません。★3でも専門家確認があり、★4では実地審査・技術検証があります。実態のない規程を増やすのではなく、現場で回る運用に落とし込む必要があります。

脆弱性診断を一度実施して終わる

診断で問題が見つかった場合は、事業影響、悪用可能性、外部公開の有無などを踏まえて優先順位を付け、改修後に再診断を行います。取得後も、資産変更や新たな脆弱性に対応するため、継続的な監視・教育・再評価が必要です。

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、単なるチェックリスト作成ではなく、経営・組織・技術を横断した改善プロジェクトとして支援します。企業ごとのシステム構成、取引先からの要求、既存のISMSや社内規程、予算・期限を踏まえ、必要な対策を個別に設計します。

対応範囲は、要求事項とのギャップ分析、対象範囲の整理、改善ロードマップ策定、規程・運用の整備、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、教育・訓練、インシデント対応体制の整備などです。診断で課題を発見して終わるのではなく、改善・再確認・継続運用まで一気通貫で支援できる点を重視しています。

経営層には投資判断や取引リスクの観点、情報システム部門には具体的な技術・運用の観点、現場部門には実行可能性の観点から整理し、関係者間の認識をそろえながら取得準備を進めます。

よくある質問

Q1. SCS評価制度はいつから申請できますか？

IPAは★3・★4について2027年3月頃の運用開始を予定しています。2026年10月14日時点では、登録希望組織向けの詳細な申請手順・提出様式は公開待ちです。

Q2. ★3と★4はどちらから取得すべきですか？

★3を取得してからでなければ★4を取得できない仕組みではありません。取引先の要求、事業への影響、扱う情報の重要性、自社の成熟度を踏まえて選択します。

Q3. SCS評価制度の取得は義務ですか？

制度自体は任意です。ただし、取引契約等で委託元が委託先に特定の★を求める運用が想定されているため、取引上の要件になる可能性があります。

Q4. ISMSを取得していればSCS評価制度への対応は不要ですか？

不要とは限りません。SCS評価制度とISMSは相互補完的な制度と位置付けられており、SCSの要求事項・評価基準への適合を別途確認する必要があります。既存のISMS文書や運用証跡を活用できる場合があります。

Q5. ★4では必ず脆弱性診断が必要ですか？

★4は第三者評価に加えて技術検証を求めています。IPAは技術検証事業者の業務として脆弱性診断を明示しています。具体的な検証範囲は適用範囲や評価プロセスに応じて決まります。

Q6. 取得費用はいくらですか？

IPAの登録料は、2028年3月31日まで★3が1万円（1年分）、★4が6万円（3年分）です。ただし、専門家確認、第三者評価、技術検証、改善対応などの費用は別途考慮する必要があります。

Q7. 何から始めればよいですか？

まず、取引先から求められる可能性のある★と対象範囲を確認し、公開済みの要求事項・評価基準に対するギャップ分析を行うのが有効です。対象範囲が決まっていない段階でも、主要システムと現行ルールとの棚卸しから始められます。

まとめ：SCS評価制度は「申請」より前の準備が取得を左右する

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）の取得は、申請書を提出するところから始まるものではありません。対象範囲を決め、要求事項とのギャップを把握し、技術・規程・運用の不足を改善し、証跡をそろえる準備が中心です。

★3では専門家確認付き自己評価、★4では第三者評価と技術検証が求められます。2027年3月頃の制度開始を見据える企業は、詳細な申請様式の公開を待つだけでなく、すでに公開されている要求事項・評価基準を使って現状分析を進めておくことが、短期間で無理なく対応するための現実的な方法です。

SCS評価制度への対応範囲が決まっていない段階でも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」「既存のISMSや社内規程をどこまで活用できるか確認したい」「技術診断まで含めた予算感を整理して稟議にかけたい」といった初期段階でもご相談いただけます。

Librus株式会社では、現状のシステム環境と取引上の要求を整理したうえで、必要な対策と優先順位を明確にし、過不足のない取得準備計画へ落とし込みます。制度対応と実際のセキュリティ強化を同時に進めることで、申請のためだけの作業を減らし、取引先への説明や継続的な運用にも活用できる体制づくりを支援します。

参考情報・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（SCS評価制度）」:

<https://www.meti.go.jp/policy/netsecurity/scs.html>

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「よくある質問」:<https://www.ipa.go.jp/security/scs/faq.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>

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>