

SCS評価制度はいつから？2027年開始までに企業が準備すべきこと

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。制度開始まで待ってから準備するのではなく、2026年度中に「どの★を目指すか」「どの事業・拠点・システムを対象とするか」「現在の対策と要求事項の差分は何か」を整理し、規程・運用・技術対策を順に整えることが重要です。

特に従業員100～1,000名規模の企業では、情報システム部門だけで完結しない点に注意が必要です。経営層の関与、取引先管理、インシデント対応、アクセス管理、脆弱性管理、教育、証跡の整備など、複数部門をまたぐ準備が求められます。★4を想定する場合は、文書確認だけでなく実地審査や技術検証も視野に入れるため、Webアプリケーション診断、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など、技術面の弱点を事前に把握しておくことも有効です。

本記事では、2026年10月4日時点で公表されている経済産業省・内閣官房国家サイバー統括室・IPAの情報を基に、制度開始までに企業が実務として何を進めるべきかを整理します。

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

この記事で分かること

- SCS評価制度の開始時期と、2026年10月時点の最新状況
- ★3と★4の違い、どちらを検討すべきかの考え方
- 2027年3月頃までに経営層・情報システム部門が準備すべきこと
- 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準備にどう組み込むか
- 費用・期間を左右する要因と、支援会社を選ぶ際の確認ポイント

SCS評価制度とは何か

SCS評価制度は、企業が自社のセキュリティ対策の実施状況について評価を受け、その結果を登録・公表する仕組みです。経済産業省と内閣官房国家サイバー統括室が2026年3月27日に公表した制度構築方針に基づいて構築され、IPAが制度を運営します。

制度の背景には、サプライチェーンを構成する企業の対策状況を、取引のたびに個別の質問票や監査で確認する負担があります。発注側から見れば取引先の対策水準が見えにくく、受注側から見れば顧客ごとに異なる要求への対応が重くなりがちです。SCS評価制度は、共通の評価軸を設けることで、取引先との間で必要なセキュリティ水準を確認しやすくすることを狙っています。

出典：[IPA「SCS評価制度の詳細情報」](#) / [経済産業省「制度構築方針」](#)

★3と★4の違い

★3は、一般的なサイバー脅威に対処し得る水準として位置付けられています。取得希望組織が自己評価を行い、SCSセキュリティ専門家による確認・助言を受け、経営層による自己適合宣誓を含めて事務局へ申請する「専門家確認付き自己評価」が基本です。

★4は、初期侵入を防ぐだけでなく、侵入後の被害拡大を抑え、取引先のデータやシステムを保護することまで重視する水準です。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。文書を整えるだけでなく、実際のシステムや運用が要求事項に沿って機能しているかを確認される点が大きな違いです。

なお、★4を取得するために先に★3を取得しておく必要はありません。自社の事業上の役割、取引先から求められる水準、扱う情報やシステムの重要度を踏まえて、目指す段階を判断します。

SCS評価制度はいつから？2027年3月頃に★3・★4の運用開始予定

IPAのFAQでは、★3・★4は2027年3月頃の運用開始予定とされています。2026年9月には、★4の第三者評価を担う評価機関や、技術検証を担う技術検証事業者などの指定申請が開始されました。指定機関は2026年12月下旬頃、SCSセキュリティ専門家は2027年1月頃から公表される予定です。制度開始に向け、評価を実施する側の体制整備は既に具体的な段階に入っています。

一方、取得希望企業向けの要求事項・評価基準の解説書や取得ガイドは、2026年10月4日時点のIPAページでは「2026年10月頃公開予定」とされています。申請方法も同様に10月頃公開予定と案内されています。そのため、現時点では細かな申請様式を待つより、既に公開されている要求事項・評価基準を基にギャップを把握し、改善に時間がかかる項目から着手するのが実務的です。

出典：[IPA「よくある質問」](#) / [IPA「要求事項・評価基準」](#) / [IPA「指定申請について」](#)

なぜ制度開始前の準備が必要なのか

取引先から求められてからでは、改善に時間がかかる

SCS評価制度は、単に申請書を提出すれば取得できるものではありません。IPAのFAQでは、★3・★4を取得するには、それぞれ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されています。未達項目が見つかった場合、規程を作るだけで解決するものもあれば、システム改修、権限設計の見直し、ログ取得、バックアップ方式の変更、委託先契約の改定、教育・訓練の実施など、数か月単位の対応が必要なものもあります。

評価のためではなく、取引継続と事業継続のために整える

制度対応を「認証マークを取る作業」と捉えると、書類作成が目的化しやすくなります。本来の目的は、サプライチェーンを通じた情報漏えい、不正侵入、サービス停止、ランサムウェア被害などのリスクを低減することです。発注企業が取引条件や選定基準に一定のセキュリティ水準を組み込むようになれば、対応状況は営業・調達・経営にも関係するテーマになります。

特に重要な取引先への依存度が高い企業では、セキュリティ要件への対応遅れが、商談機会の減少、取引条件の追加、監査対応の長期化などにつながる可能性があります。経営層は、制度取得の費用だけでなく、取引維持、事業継続、信用毀損の回避という観点で投資判断を行うことが重要です。

SCS評価制度の対象をどう考えるか

制度では、企業が決定した適用範囲の中から対象をサンプリングして評価することが想定されています。したがって、最初の実務は「会社全体を対象にするのか」「特定事業・拠点・サービスを対象にするのか」を整理することです。対象が曖昧なまま準備を始めると、必要以上に範囲が広がり、費用と期間が膨らみます。逆に狭く設定しすぎると、実際の取引や重要データの流れを反映できません。

対象範囲を決める際は、主要顧客との取引に使うシステム、顧客データや機密情報を扱う環境、インターネットに公開しているWebアプリケーション、基幹システム、クラウドサービス、リモートアクセス環境、委託先との接続点などを洗い出します。業務上の重要性和攻撃を受けた際の影響を基準に整理すると、経営層にも説明しやすくなります。

2027年の制度開始までに企業が準備すべき7つのこと

1. 目指す★と対象範囲を経営判断する

まず、★3と★4のどちらを目指すか、対象となる事業・拠点・情報資産をどこまで含めるかを決めます。主要取引先から求められそうな水準、扱う情報の重要度、システム停止時の事業影響、自社がサプライチェーンの中で担う役割を判断材料にします。経営層が決めるべきなのは、取得そのものではなく「どの事業リスクを、どの水準まで低減するか」です。

2. 要求事項・評価基準に対するギャップ分析を行う

公開されている★3・★4の要求事項・評価基準に対し、現状が適合しているか、証跡を示せるかを確認します。ここで重要なのは「実施しているつもり」と「第三者が確認できる状態」を分けることです。たとえば退職者アカウントを削除していても、手順や実施記録が残っていなければ、評価時に説明が難しくなります。規程、手順、設定、ログ、教育記録、監査記録などを紐付けて確認します。

3. 不足している規程・運用・証跡を整備する

ギャップは、規程不足、運用不足、技術対策不足、証跡不足に分類すると改善計画を立てやすくなります。たとえば情報資産管理台帳、アカウント管理手順、脆弱性対応ルール、インシデント対応手順、委託先管理基準、バックアップ方針などです。文書を新たに作る場合も、現場で実行できない内容を形式的に定めるのではなく、既存業務に組み込める形にします。

4. 技術的な弱点を事前に確認する

★4では技術検証が想定されています。制度上の正式な技術検証は指定された枠組みに従って行われますが、制度開始前の準備として、自社の弱点を先に把握することは有効です。Webアプリケーション診断では、認証・認可、入力値処理、セッション管理などWeb固有の問題を確認します。プラットフォーム診断では、OS、ミドル

ウェア、ネットワーク機器、クラウド設定などの脆弱性や設定不備を確認します。さらに、実際の攻撃者に近い観点で侵入可能性や横展開を検証したい場合は、ペネトレーションテストを組み合わせます。

5. インシデント対応と復旧の実効性を確認する

規程があっても、攻撃を検知した際に誰が判断し、誰が顧客へ連絡し、どこまでシステムを停止するかが決まっていなければ、実際の事故では動けません。情報システム部門だけでなく、経営、法務、広報、営業、総務などを含めた連絡体制を確認し、机上訓練や演習を行います。ランサムウェアを想定する場合は、バックアップからの復旧手順と復旧時間も確認しておくべきです。

6. 委託先・クラウド・取引先との関係を整理する

自社が強固でも、委託先のアカウントや接続経路が侵入経路になることがあります。外部委託、クラウド、SaaS、保守ベンダーなどについて、アクセス権限、契約上のセキュリティ条項、事故時の報告、再委託、ログ取得、アカウント停止手順を確認します。調達部門や事業部門を巻き込み、契約更新のタイミングも考慮して改善を進めます。

7. 2027年初頭の評価・申請を見据えて社内稟議を準備する

制度対応は、コンサルティング費用だけでなく、診断、システム改修、ツール導入、教育、評価機関への依頼など複数の費用が発生し得ます。年度内の予算確保が必要な企業では、2026年中に概算を作り、経営会議や稟議に載せられる状態にしておくことが重要です。稟議では「制度対応費」だけでなく、主要取引先との関係、停止時の損失、既存監査の効率化など、事業面の効果を説明すると判断されやすくなります。

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の位置付け

IPAが2026年9月に公表した指定申請情報では、技術検証事業者は、評価機関からの委託を受けて「技術検証（脆弱性診断）」を実施する事業者とされています。また、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を提供する法人が示されています。

ただし、制度対応のために自社で実施した脆弱性診断やペネトレーションテストが、そのまま★4の正式な技術検証に代替できるとは限りません。正式な評価では、指定された評価機関・技術検証事業者、評価手順、対象範囲に従う必要があります。準備段階の診断は「不適合や弱点を本番評価前に減らすための予備検証」と位置付けるのが適切です。

出典：[IPA「指定申請について」](#)

対応を先送りした場合に起こり得る問題

制度開始後に取引先から★の取得状況を確認され、その時点で準備を始めると、短期間で複数部門の対応を進めなければならない可能性があります。規程整備は比較的短期間でも、システム改修や委託先契約の見直し、ログ基盤の整備、教育の定着には時間がかかります。結果として、取得時期が取引先の要求時期に間に合わない、緊急対応でコストが上がる、通常業務にしわ寄せが出るといった問題が起こり得ます。

また、評価のために急いで文書だけを整えると、実際の運用と規程が一致しない状態になりやすくなります。制度対応を機に、現在のセキュリティ対策が事業の実態に合っているかを棚卸しすることが、長期的には監査対応や顧客説明の効率化にもつながります。

実施期間の目安はどの程度か

準備期間は、現在の成熟度、対象範囲、目標とする★、技術改修の有無で大きく変わります。既にISMS等の管理体制が整い、証跡も蓄積されている企業と、規程や資産管理から整備する企業では必要な期間が異なります。

実務では、最初に2～4週間程度で対象範囲とギャップを整理し、その後、優先度の高い改善を数か月かけて実施する進め方が考えられます。★4を想定し、診断やシステム改修、再診断まで行う場合は、さらに余裕を持たせるべきです。これは制度が定める標準期間ではなく、準備プロジェクトを設計する際の実務上の目安です。

費用を左右する要因

2026年10月4日時点で、取得希望組織が★3・★4を申請・登録する際の費用はIPAのFAQで「今後公開予定」とされています。2026年9月に公表された申請料・指定料は、評価機関・技術検証事業者・研修事業者として指定を受ける側の料金であり、★を取得したい一般企業の申請費用とは別です。混同しないよう注意が必要です。

企業側の総コストは、制度上の申請・評価費用だけでは決まりません。対象拠点やシステム数、現状とのギャップ、規程整備量、診断対象のIP数・URL数・画面数、クラウド構成、ペネトレーションテストの範囲、システム改修の有無、再診断の回数、社内教育の規模などで変動します。見積りでは「制度取得支援」「技術診断」「改善支援」「本番評価」を分けて確認すると、比較しやすくなります。

出典：[IPA「よくある質問」](#) / [IPA「指定申請について」](#)

支援会社を選ぶ際のチェックポイント

SCS評価制度の準備では、制度文書の読み込みだけでなく、現場の技術対策まで落とし込める支援会社を選ぶことが重要です。RFPや見積依頼では、①★3・★4のどちらを想定するか、②ギャップ分析の範囲、③規程・手順の整備支援を含むか、④Webアプリケーション診断・プラットフォーム診断等に対応できるか、⑤改善後の再確認を含むか、⑥経営層向け報告を用意できるか、⑦機密情報の取り扱いとデータ保管方法、⑧正式評価との役割分担をどのように整理するか、を確認します。

特に★4では、取得支援を行う会社と正式な第三者評価を行う評価機関の関係について、中立性・公平性の観点が重要になります。準備支援を依頼する段階から、将来の評価プロセスで利益相反や役割の混同が生じないよう確認しておくで安心です。

SCS評価制度の準備でよくある失敗と注意点

規程作成だけで終わる

文書は必要ですが、実態と一致していなければ意味がありません。アカウント棚卸し、パッチ適用、バックアップ復旧、教育、インシデント連絡など、実運用と証跡まで確認します。

対象範囲を最初に決めない

後から対象システムが増えると、診断や証跡収集をやり直すことがあります。主要取引・重要データ・外部接続を起点に範囲を定義します。

診断結果を修正せずに終える

脆弱性診断は発見が目的ではありません。重大度だけでなく、悪用可能性、外部公開状況、扱うデータ、事業影響を踏まえて優先順位を付け、期限と担当者を決めます。修正後は再診断または設定確認を行います。

情報システム部門だけで進める

委託先契約、教育、顧客報告、事業継続などは他部門の協力が不可欠です。経営責任者、情報システム、法務・総務、営業・調達、主要事業部門の役割を早期に決めます。

成果物・報告書に含めるべき内容

準備支援を外部に依頼する場合、最終的に何が残るかを確認してください。少なくとも、対象範囲、要求事項ごとの現状評価、根拠資料、未達事項、リスク、改善優先度、担当部門、期限、技術診断結果、再確認結果、経営層向けの要約があると、その後の社内推進や本番評価につなげやすくなります。

改善優先度は、単にCVSSなどの技術的な重大度だけで決めるのではなく、外部から到達可能か、権限昇格や横展開につながるか、重要データにアクセスできるか、停止時の影響が大きいかといった事業上の観点を合わせて判断します。

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対応ではなく、企業ごとの事業・IT環境・取引関係に合わせて設計します。制度要求と現在の運用を照合するギャップ分析から、情報セキュリティ体制の整備、リスクアセスメント、規程・運用の改善、技術診断、教育、インシデント対応体制の構築まで、一気通貫で支援可能です。

技術面では、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、レッドチーム演習などを通じて、文書上では見えにくい実際の攻撃経路や設定上の弱点を確認できます。発見事項については、事業影響と対応難易度を踏まえて優先順位を整理し、診断だけで終わらず改善・再確認まで支援します。

また、経営層に対しては、セキュリティ上の論点を投資判断、事業継続、主要取引先への影響という言葉に置き換えて整理し、情報システム部門と経営・現場部門の橋渡しを行います。大企業だけでなく、中堅・中小企業にも対応し、M&A、IPO、取引先監査など経営上の重要局面を踏まえた支援も可能です。

SCS評価制度に関するよくある質問

Q1. SCS評価制度はいつから始まりますか？

★3・★4は2027年3月頃の運用開始予定です。2026年10月4日時点では、IPAが制度運営の準備を進めており、評価機関等の指定申請も始まっています。

Q2. 2027年3月まで何もしなくても問題ありませんか？

おすすめできません。要求事項を満たすためにシステム改修や契約見直しが必要になると、数か月を要することがあります。まずギャップ分析を行い、時間がかかる項目を先に進めるべきです。

Q3. ★3を取らないと★4は取得できませんか？

いいえ。IPAは、★3を事前に取得していなければ★4を取得できない関係ではないと説明しています。自社のリスクと取引上の要請に応じて目標を選びます。

Q4. ★3は自己評価だけで取得できますか？

単独の自己評価ではありません。取得希望組織による自己評価に対し、SCSセキュリティ専門家の確認・助言と署名を受け、経営層による自己適合宣誓を含めて申請する仕組みです。

Q5. ★4では脆弱性診断が必要ですか？

★4では第三者評価と技術検証が求められます。IPAの指定申請情報では技術検証を「脆弱性診断」と表現しています。正式な対象・方法は制度の手順に従う必要があります。

Q6. ペネトレーションテストを実施すれば★4を取得できますか？

ペネトレーションテストだけで取得できるわけではありません。★4は要求事項全体への適合、第三者評価、技術検証などを含む制度です。ペネトレーションテストは準備段階で実効的な弱点を把握する手段の一つです。

Q7. 申請費用はいくらですか？

2026年10月4日時点で、★3・★4の取得希望組織が支払う申請・登録費用は今後公開予定です。9月に公開された評価機関等の申請料・指定料とは別の料金です。

Q8. まだ対象範囲や目指す★が決まっていなくても相談できますか？

可能です。むしろ初期段階で、主要取引先、重要システム、扱う情報、既存認証・監査、今後の事業計画を整理すると、過不足のない対象範囲とロードマップを設計しやすくなります。

まとめ:SCS評価制度は「制度開始前のギャップ把握」が重要

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。2026年中に取り組むべきことは、申請書を待つことなく、目標とする★と対象範囲を定め、公開済みの要求事項・評価基準に対して現状のギャップを把握し、改善を始めることです。

とりわけ、技術対策、委託先管理、インシデント対応、証跡整備は短期間では完成しにくい領域です。★4を視野に入れる企業では、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を活用し、本番評価前に重大な弱点を減らしておくことが現実的です。制度取得を目的化せず、取引継続と事業継続の両方を強くする機会として進めることが重要です。

SCS評価制度への対応方針が固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」「対象範囲をどこまで含めるべきか判断できない」「現在の規程やセキュリティ対策で不足している点を知りたい」といった初期段階でも、Librus株式会社にご相談いただけます。

現状を整理したうえで、制度要求とのギャップ、優先して改善すべき項目、診断が必要なシステム、社内稟議に必要な費用・スケジュールの考え方まで整理することで、過剰な対策や手戻りを抑えながら準備を進めやすくなります。SCS評価制度の取得支援だけでなく、脆弱性診断、ペネトレーションテスト、体制構築、改善支援まで一気通貫で対応可能です。

主な公的情報

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>

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>

経済産業省・内閣官房国家サイバー統括室「制度構築方針」(2026年3月27日):

<https://www.ipa.go.jp/security/scs/rcu1hd0000007ajp-att/20260327001-br.pdf>

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>