SCS評価制度とは？制度の概要・対象企業・開始時期をわかりやすく解説

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）は、企業のセキュリティ対策状況を段階別に可視化し、取引先との間で必要な対策水準を確認しやすくするための制度です。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示し、独立行政法人情報処理推進機構（IPA）が運営します。

結論から言えば、SCS評価制度は特定の業種や大企業だけを対象にした制度ではありません。サプライチェーンを構成する幅広い企業が対象となり得ます。★3・★4は2027年3月頃の運用開始が予定されており、取引先から取得を求められる可能性がある企業だけでなく、自社のセキュリティ対策を客観的に整理したい企業にとっても重要な制度です。

一方で、SCS評価制度は現時点で法律によって一律に取得を義務付けるものではありません。実務上は、発注企業が委託先に一定の★を求めるなど、取引条件の一部として活用されることが想定されています。そのため、「義務ではないから様子を見る」だけではなく、自社の主要取引先や事業上の重要性を踏まえて準備時期を判断することが重要です。

この記事で分かること

- SCS評価制度の目的と仕組み、★3・★4・★5の位置付け
- 対象となり得る企業と、特に対応を検討すべき企業
- 2026年10月時点で公表されている開始時期と今後のスケジュール
- 取得に向けて必要になる規程、証跡、技術対策、診断の考え方
- 費用・期間を左右する要因と、社内での準備の進め方

SCS評価制度とは何か

SCSは「Supply Chain Security」の略称です。SCS評価制度は、取引関係を通じてつながる企業群の中で、各社がどの程度のセキュリティ対策を実施しているかを可視化し、委託元と委託先が必要な対策水準を共有しやすくする仕組みです。

背景には、サプライチェーン経由のサイバー攻撃があります。攻撃者が大企業を正面から狙うのではなく、取引先や委託先のネットワーク、リモート接続、クラウドアカウント、公開サーバーなどを足掛かりに侵入し、機密情報の窃取や業務停止につなげるケースが問題となっています。発注企業側から見ると、委託先の対策状況を外部から判断しにくいことが課題です。一方、受注企業側も複数の顧客から異なるチェックシートへの回答を求められ、対応負担が大きくなっています。SCS評価制度は、こうした双方の課題を軽減することを狙っています。

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・★4・★5は何が違うのか

制度は段階別の評価を採用しています。2026年10月時点で具体的な運用準備が進められているのは★3と★4です。★5は、より高度な脅威への対応を想定した水準として検討中です。

区分	想定する位置付け	評価方法	主な考え方

★3	全てのサプライチェーン企業が最低限実装すべき水準	専門家確認付き自己評価	基礎的な組織対策とシステム防御を中心に確認
★4	標準的に目指すべき水準	第三者評価	ガバナンス、取引先管理、防御・検知、インシデント対応等を包括的に確認
★5	到達点として目指す高度な水準	第三者評価を想定	未知の攻撃も含む高度な脅威への対応。詳細は検討中

★3では、取得希望組織が自己評価を行い、登録されたSCSセキュリティ専門家が書類を確認します。★4では、評価機関による文書確認と実地審査に加え、技術検証事業者による技術検証が行われる想定です。制度上の「★」は単なる自己宣言ではなく、段階に応じた確認・評価プロセスを伴います。

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

SCS評価制度の対象企業は？

SCS評価制度は、業種や企業規模を限定した制度ではありません。経済産業省のFAQでは、業種や事業規模を問わず幅広い事業者が対象となり得るとされています。特に、取引先のシステムや情報資産にアクセスする企業、重要な業務を受託する企業、製造・物流・金融・ITサービスなどサプライチェーンへの依存度が高い企業は、早めに制度との関係を確認しておく必要があります。

従業員100～1,000名規模の企業では、顧客からセキュリティチェックシートへの回答を求められている一方、情報システム部門や管理部門の人員が限られているケースも少なくありません。SCS評価制度が取引先管理に活用されるようになると、従来の個別チェックシートに加えて「★3を取得しているか」「★4相当の対策があるか」といった確認が行われる可能性があります。

特に対応優先度が高い企業

次のような企業は、制度開始前から現状把握を進める価値があります。

- 大企業や重要インフラ企業から業務委託を受けている企業
- 顧客の個人情報、営業秘密、設計情報、ソースコードなどを扱う企業
- リモート接続やAPI連携などで顧客環境に接続する企業
- 製造、物流、保守、IT運用など、停止すると顧客業務に影響するサービスを提供する企業
- 新規取引や入札、RFPでセキュリティ要件が増えている企業
- 取引先監査、IPO、M&Aなどでセキュリティ体制の説明が必要な企業

SCS評価制度はいつ始まる？

IPAのFAQでは、★3・★4は2027年3月頃の運用開始が予定されています。2026年10月時点では、要求事項・評価基準、制度規程、評価機関・技術検証事業者等の指定手続など、運用開始に向けた具体化が進められています。評価機関は2026年12月末頃、SCSセキュリティ専門家は2027年1月頃から公表予定です。

したがって、2027年3月になってから準備を始めるのではなく、2026年度中にギャップ分析、対象範囲の整理、規程整備、証跡収集、技術的な弱点の洗い出しまで進めておく方が現実的です。特に★4を目指す場合、実地審査や技術検証に備え、運用実績を示せる状態にしておく必要があります。

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

なぜ今、企業にSCS評価制度への準備が必要なのか

最大の理由は、セキュリティ対策が情報システム部門だけの課題ではなく、取引継続や営業機会に関わる経営課題になっているためです。SCS評価制度は任意制度ですが、発注企業が委託先に必要な★を提示し、契約や取引判断に活用することが想定されています。

例えば、同じ価格と品質で競合する2社があり、一方が★3を取得して対策状況を説明でき、もう一方が規程や運用証跡を提示できない場合、発注側のリスク管理では前者が選ばれやすくなる可能性があります。逆に、既存取引先から一定水準を求められたときに準備が整っていなければ、改善計画の提出や追加監査を求められ、営業・管理・情報システム部門に急な負担が生じます。

対応しなかった場合に起こり得る問題

SCS評価制度を取得しないこと自体に直ちに罰則があるわけではありません。しかし、取引先が調達基準に活用する場合、実務上の影響は別です。新規取引の条件を満たせない、契約更新時に追加説明を求められる、個別のセキュリティチェックが長期化するといった可能性があります。

また、制度対応を先送りした結果、ランサムウェア、認証情報窃取、VPNや公開サーバーの脆弱性悪用などによる事故が発生すれば、復旧費用だけでなく、取引先への報告、信用低下、受注停止、調査対応など事業面の影響が大きくなることがあります。制度対応は「マーク取得のための作業」ではなく、実際のリスク低減とセットで考えることが重要です。

取得・対応に向けて企業が準備すべきこと

SCS評価制度への準備は、最初から全項目を完璧にするのではなく、対象範囲を決め、現状と要求事項の差分を把握し、優先順位を付けて改善する方法が現実的です。

1. 目標とする★と対象範囲を決める

主要顧客から求められる可能性、自社サービスの重要度、扱う情報、システム構成を踏まえ、★3か★4かを検討します。全社を一度に対象とするのではなく、制度上認められる適用範囲を整理することも重要です。

2. 要求事項に沿ってギャップ分析を行う

規程、組織体制、アカウント管理、脆弱性管理、ログ監視、バックアップ、委託先管理、インシデント対応などについて、現在できていることと不足していることを整理します。

3. 規程と実運用を一致させる

情報セキュリティ規程を作るだけでは不十分です。退職者アカウントの削除記録、パッチ適用記録、教育記録、インシデント訓練記録、バックアップ復旧確認など、実際に運用していることを示す証跡が必要です。

4. 技術的な弱点を確認する

インターネット公開資産、Webアプリケーション、クラウド、VPN、OSやミドルウェアなどの弱点を確認します。Webアプリケーション診断やプラットフォーム診断により既知の脆弱性や設定不備を洗い出し、重要度に応じて改修します。

5. 必要に応じてペネトレーションテストを検討する

脆弱性の有無だけでなく、複数の弱点を組み合わせて実際にどこまで侵入・権限拡大・重要情報への到達が可能か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。★4等を視野に入れる場合、単なるチェックリスト対応ではなく、実環境の耐性を検証する発想が重要です。

6. 改善計画と経営判断を結び付ける

発見事項をすべて同じ優先度で対応するのではなく、事業影響、攻撃可能性、顧客要請、改善費用を踏まえて優先順位を付けます。経営層には「制度対応費」ではなく、取引継続、受注機会、事故損失の低減という観点で説明すると意思決定しやすくなります。

実施前にそろえておきたい資料

準備段階では、組織図、情報セキュリティ関連規程、IT資産台帳、ネットワーク構成図、クラウドサービス一覧、アカウント管理手順、委託先一覧、インシデント対応手順、バックアップ方針、教育記録、脆弱性対応記録、監視ログや点検記録などを集めます。資料が散在している場合は、それ自体が運用上の課題です。審査に備えるだけでなく、平時の運用を効率化する観点から保管場所や責任者も整理します。

費用と期間を左右する要因

SCS評価制度への対応費用は、単純な「申請料」だけでは決まりません。実際には、現在のセキュリティ成熟度、対象範囲、★3か★4か、不足している規程数、システム改修、診断・技術検証、専門家支援の範囲などで大きく変わります。

特に期間を左右するのは、証跡です。規程は短期間で作成できても、教育、点検、バックアップ復旧、脆弱性対応などの運用記録は、一定期間実施しなければ蓄積できません。そのため、制度開始直前に文書だけを整えるより、早い段階で運用を開始して記録を残す方が効率的です。

なお、IPAは2026年9月18日にSCS評価制度の料金設定に関する情報を公開していますが、評価を受ける企業の総費用は、評価機関や技術検証、改善対応等を含めて個別に異なります。見積依頼時には「評価そのもの」「事前ギャップ分析」「規程整備」「技術診断」「改修支援」「再確認」のどこまで含むかを分けて確認すると比較しやすくなります。

支援会社を選ぶときのチェックポイント

SCS評価制度の支援会社を選ぶ際は、制度文書を説明できるだけでなく、現場の技術対策まで支援できるかが重要です。規程だけを整えても、公開サーバーの脆弱性、クラウドの設定不備、特権アカウント管理、ログ監視不足などが残れば、実態との乖離が生じます。

RFPや見積依頼では、SCS要求事項とのギャップ分析方法、成果物の形式、改善優先順位の付け方、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、経営層向け報告、評価後の継続支援まで確認するとよいでしょう。また、機密情報やネットワーク構成図を渡すことになるため、情報管理体制やNDA、データ保管・削除方針も確認が必要です。

よくある失敗と注意点

よくある失敗は、制度対応を「規程作成プロジェクト」にしてしまうことです。実際には、規程、運用、技術対策、証跡がつながっている必要があります。また、IT部門だけに任せると、購買・人事・法務・営業・経営層が関与する要求事項で進まなくなることがあります。

もう一つの注意点は、★取得をゴールにしないことです。サイバー攻撃の手法や自社システムは変化します。取得後も脆弱性管理、定期診断、ログ監視、教育、インシデント訓練、委託先管理を継続し、必要に応じて再診断や改善を行う運用が求められます。

Librus株式会社が提供できる支援

Librus株式会社では、SCS評価制度への対応を、制度文書の解釈だけでなく、実際のセキュリティ改善まで一気通貫で支援します。企業ごとの事業環境や取引先要件を踏まえて対象範囲を整理し、要求事項とのギャップ分析、規程・証跡の整備、改善計画の策定を支援します。

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、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、教育・訓練など、技術面・運用面の改善にも対応できます。診断だけで終わらせず、発見された課題を経営リスクや取引リスクに置き換え、優先順位を付けて改善することを重視しています。

経営層、情報システム部門、営業・管理部門の間で認識がそろっていない場合も、制度対応の目的、投資効果、取引先への説明方法まで含めて整理できます。M&A、IPO、取引先監査など、セキュリティ体制を外部に説明する重要局面と合わせた支援も可能です。

よくある質問

Q1. SCS評価制度は義務ですか？

制度自体は任意です。ただし、委託元が取引条件として一定の★取得を求める可能性があります。自社の主要顧客や業界動向を確認したうえで対応時期を判断する必要があります。

Q2. 中小企業も対象ですか？

はい。業種や企業規模を問わず幅広い企業が対象となり得ます。IPAは特にサプライチェーンを構成する中小企業にとって活用効果が大きいと説明しています。

Q3. ★3・★4はいつ始まりますか？

IPAは2027年3月頃の運用開始を予定しています。評価機関は2026年12月末頃、SCSセキュリティ専門家は2027年1月頃から公表予定です。

Q4. ISMSを取得していれば対応不要ですか？

必ずしもそうではありません。ISMSとSCS評価制度は目的や評価スキームが異なります。既存のISMS文書や運用を活用できる部分はありますが、SCSの要求事項に照らしたギャップ確認が必要です。

Q5. ★3と★4のどちらを目指すべきですか？

取引先からの要求、事業の重要性、扱う情報、システム接続範囲などで判断します。取引先から指定がない段階では、まず現状を評価して、費用対効果を見ながら決める方法が現実的です。

Q6. 脆弱性診断は必須ですか？

必要な技術対策は対象範囲や要求事項によります。ただし、公開資産やWebアプリケーションの弱点を把握せずに実効性のある対策を説明することは困難です。診断はギャップ把握と改善優先順位付けに有効です。

Q7. どのくらい前から準備すべきですか？

不足項目の多さによります。規程だけでなく運用証跡を蓄積する必要があるため、取引先から要請されてから着手するより、数か月単位で前倒しして準備する方が安全です。

Q8. 何から始めればよいですか？

まずは対象範囲と目標水準を仮決めし、SCSの要求事項に沿ったギャップ分析を行うことをおすすめします。対象範囲や取得水準が決まっていない段階でも、現状整理から始められます。

まとめ｜SCS評価制度は「取引に使われるセキュリティ基準」として早めの準備を

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を段階別に可視化し、委託元と委託先の間で必要な水準を共有しやすくする制度です。★3・★4は2027年3月頃の開始が予定され、業種や企業規模を問わず幅広い企業が対象となり得ます。

重要なのは、制度が始まってから申請書を作ることではありません。規程、実際の運用、証跡、技術対策を一致させ、自社のリスクと取引先要求に応じて改善しておくことです。特に、主要顧客からセキュリティチェックを受けている企業、重要な業務や情報を扱う企業は、制度開始前からギャップ分析を進めることで、急な取引先要請にも対応しやすくなります。

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流用できるか確認したい」「取引先から要請される前に準備したい」といった段階でも、Librus株式会社では現状整理から支援できます。制度対応と技術対策を分けて考えるのではなく、取引継続・新規受注・事故リスク低減まで含めて優先順位を整理することで、必要な投資を判断しやすくなります。対象範囲、実施方法、予算が固まっていない場合も、現状の課題と想定される対応範囲の整理からご相談ください。

主な公的情報

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 よくある質問：https://www.ipa.go.jp/security/scs/faq.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 SCS評価制度に関するFAQ：https://www.meti.go.jp/press/2025/03/20260327001/20260327001-gr.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