SCS評価制度への対応は何から始める？企業が取り組むべき7つの準備ステップ

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）への対応を検討しているものの、「まず何を確認すべきか」「★3と★4のどちらを目指すべきか」「規程や技術対策をどこまで整えればよいか」が分からず、着手できていない企業は少なくありません。結論からいえば、最初に製品導入や脆弱性診断を発注するのではなく、取引先から求められる水準と自社の適用範囲を整理し、公式の要求事項・評価基準に対するギャップを可視化することが出発点です。そのうえで、規程・証跡・技術対策を優先順位付きで整備し、評価に耐えられる運用状態を作ることが重要です。

重要な結論：SCS評価制度対応は「要求事項を読む→足りないものを買う」という進め方ではなく、取引上の必要性、取得単位・適用範囲、現状ギャップ、是正計画、証跡整備を一つのプロジェクトとして管理すると進めやすくなります。

出典：IPA「SCS評価制度」 https://www.ipa.go.jp/security/scs/index.html
出典：IPA「要求事項・評価基準」 https://www.ipa.go.jp/security/scs/requirements-criteria.html
出典：IPA「よくある質問」 https://www.ipa.go.jp/security/scs/faq.html

この記事で分かること

- SCS評価制度への対応を始める際の優先順位
- ★3・★4のどちらを目指すか判断する考え方
- 取得単位・適用範囲を決める際の実務ポイント
- 社内規程・証跡・技術対策を整理する方法
- 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実施するタイミング
- 社内稟議やベンダー選定で確認すべき事項
- 評価後も取引先から信頼される継続運用の考え方

SCS評価制度とは

SCS評価制度は、企業のセキュリティ対策の実施状況を段階別に可視化し、サプライチェーン全体のセキュリティ水準向上を図る制度です。経済産業省と内閣官房国家サイバー統括室が公表した制度構築方針に基づき、IPAが運営します。取引契約などにおいて、委託元が委託先に適切な段階（★）を示し、対策の実施状況を確認する活用が想定されています。

そのため、SCS評価制度は「取得すれば終わる認証」ではなく、取引先への説明、調達・委託管理、サイバーリスクの低減をつなぐ仕組みとして捉える必要があります。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なく、経営層、営業、法務、総務、事業部門が関与するケースが多く、早い段階で役割分担を決めることが実務上のポイントになります。

★3と★4の違いを最初に理解する

項目	★3	★4
評価の中心	自己評価＋SCSセキュリティ専門家による確認	第三者評価。文書確認に加えて実地審査・技術検証を実施
技術検証	原則として制度上の技術検証は実施しない	技術検証事業者等による脆弱性検査を含む技術検証
有効期間	1年	3年（途中年度は自己評価等が必要）
向いている場面	取引先から一定水準の可視化を求められる場合、まず制度対応を進めたい場合	より高い客観性が必要な重要取引、重要システムを含む場合

なお、2026年11月17日時点でIPAは、★の登録申請方法を示す「登録申請の手引」を2026年11月末頃に公表予定としています。申請画面や提出方法などの最終手続きは、公開後に必ず最新情報を確認してください。

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

なぜ今、準備を始める必要があるのか

SCS評価制度は2027年3月の開始が予定されています。制度開始直前になってから対応を始めると、規程の改定、ネットワーク構成の見直し、アカウント管理、ログ管理、インシデント対応、バックアップ、脆弱性管理など、複数部門にまたがる是正が短期間に集中する可能性があります。

さらに、SCS評価制度では、単に規程が存在するかではなく、要求事項に対する実施状況を説明できることが重要です。たとえば、アクセス権限の棚卸しを「年1回実施する」と規程に書いていても、実際の実施記録がなければ十分な説明ができません。運用実績を証跡として残すには時間がかかるため、制度開始を待たず準備を始める合理性があります。

出典：**IPA** 不正アクセス対策特設サイト（**SCS**評価制度は**2027**年**3**月開始予定と案内） https://www.ipa.go.jp/security/support/incident-support.html

SCS評価制度への対応で企業が取り組むべき7つの準備ステップ

ステップ1：取引上の必要性と目指す★を確認する

最初に確認すべきなのは、「自社が何となく取得したいか」ではなく、「どの取引・顧客・事業で、どの水準が必要になる可能性があるか」です。既存顧客のセキュリティチェックシート、RFP、基本契約、委託先管理基準、調達方針を洗い出し、SCS評価制度への言及や今後の要求方針を営業・法務・調達部門と確認します。

経営層は、重要顧客の売上、契約更新時期、取引停止時の影響、取得に必要な投資を踏まえて★3・★4の優先順位を判断します。全社一律に高い水準を目指すより、重要取引で求められる水準から逆算する方が、予算と工数を配分しやすくなります。

ステップ2：取得単位と適用範囲を決める

SCS評価制度では、取得単位や適用範囲を適切に決めることが重要です。会社全体を一律に対象にするのか、特定の事業・拠点・サービスを中心にするのかで、必要な資料と対策量は大きく変わります。IPAの自己評価等ガイドも、取得単位と適用範囲の決定を評価準備の重要な手続きとして位置付けています。

適用範囲を決める際は、顧客データや機密情報を扱う業務、外部公開システム、VPNやクラウド管理環境、委託先との接続、重要な業務プロセスを確認します。範囲を狭くしすぎると取引先への説明力が弱くなる一方、必要以上に広げると是正コストが膨らむため、事業リスクと取引要求の両面から決めることが必要です。

ステップ3：要求事項・評価基準に対するギャップ分析を行う

次に、IPAが公開する「★3・★4 要求事項・評価基準」と解説書を基準に、現状がどこまで満たせているかを確認します。規程の有無だけではなく、責任者、手順、実施頻度、対象範囲、記録、例外管理まで確認すると、後工程で手戻りが減ります。

ギャップは「未整備」「部分対応」「対応済みだが証跡不足」「対応済み」のように分類し、重要取引への影響、攻撃リスク、是正の難易度、必要期間を加えて優先順位を付けます。ここで製品ありきにしないことが重要です。IPAのFAQでも、組織規模やシステム構成によって必要な対応は同一ではなく、特定製品の導入を一律に求める制度ではないとされています。

ステップ4：社内規程と運用証跡を整備する

SCS評価制度への対応では、情報セキュリティ方針、アカウント管理、アクセス制御、脆弱性管理、ログ管理、インシデント対応、バックアップ・復旧、委託先管理、教育など、複数のルールを整備する必要があります。ただし、新しい文書を大量に作ることが目的ではありません。既存のISMS規程、IT運用手順、BCP、就業規則、委託先管理手順などを棚卸しし、不足部分を追加する方が効率的です。

さらに重要なのが証跡です。アカウント棚卸し表、パッチ適用記録、脆弱性対応チケット、ログ確認記録、教育受講記録、バックアップ復旧テスト結果、インシデント訓練記録など、「実際に運用したこと」が分かる資料を保存します。評価前だけ整えるのではなく、日常業務の中で証跡が自然に残る仕組みに変えることが理想です。

ステップ5：不足する技術対策を実装し、必要に応じて診断する

ギャップ分析で技術面の不足が見つかった場合は、重要度に応じて是正します。代表例は、多要素認証、不要アカウントの削除、特権ID管理、外部公開機器のパッチ適用、ネットワーク分離、ログ取得・監視、バックアップの保護、EDR等のエンドポイント対策などです。

脆弱性診断もこの段階で検討します。Webアプリケーション診断はWebサービス固有の脆弱性、プラットフォーム診断はサーバ、ネットワーク機器、ミドルウェア等の既知脆弱性や設定不備の確認に向きます。ペネトレーションテストは、複数の弱点を組み合わせて実際にどこまで侵入・権限取得が可能かを検証したい場合に有効です。★4では第三者評価に加え技術検証が行われるため、評価直前に初めて問題が発覚するより、事前に重要な外部公開資産を把握・診断し、是正できる状態にしておく方が進めやすくなります。

ステップ6：自己評価と模擬評価で「説明できる状態」にする

規程や技術対策を整えた後は、公式のアセスメントシートを用いて自己評価を行い、各評価項目について、担当者が根拠資料をすぐ提示できる状態にします。評価で重要なのは、担当者だけが理解していることではなく、組織として一貫した説明ができることです。

特に★4を目指す場合は、実地審査を想定し、規程、管理台帳、操作画面、チケット、ログ、教育記録、復旧テスト記録などを使った模擬ヒアリングを実施すると有効です。「規程ではできているが現場運用が異なる」「説明者によって答えが変わる」といった不整合を事前に潰せます。

ステップ7：評価後の是正・継続運用まで計画する

SCS評価制度は取得時点だけを整えるプロジェクトにしないことが重要です。脆弱性やクラウド構成、利用サービス、担当者、取引先は変化するため、定期的な棚卸しと改善が必要です。

評価で指摘を受けた場合の是正責任者・期限を決め、再診断や設定確認の必要性も判断します。★3は1年更新、★4は3年更新であり、途中期間にも自己評価等が求められます。取得後の年間運用計画まで予算化しておくことで、更新時の負担を減らし、取引先からの追加質問にも迅速に対応しやすくなります。

出典：IPA「★3・★4 自己評価等ガイド／第三者評価ガイド／技術検証ガイド」 https://www.ipa.go.jp/security/scs/requirements-criteria.html

準備を後回しにした場合に起こり得る問題

対応が遅れると、取引先から★取得や同等水準の説明を求められた際に、短期間で複数の是正を行う必要が生じる可能性があります。特に、外部公開機器の更新、認証方式の変更、ログ基盤の整備、バックアップ方式の見直し、委託先契約の改定などは、情報システム部門だけでは完結しません。

また、技術的な問題より「証跡不足」で説明できないケースにも注意が必要です。実際には運用していても、記録が残っていなければ評価や取引先監査で説明が難しくなります。SCS評価制度対応をきっかけに、セキュリティ活動を経営・取引上の説明材料に変える視点が重要です。

実施期間と費用を左右する要因

準備期間は、現在のセキュリティ成熟度、対象範囲、既存のISMS等の仕組み、システム数、外部公開資産、委託先数、必要な技術改修によって変わります。すでに規程と運用証跡が整っている企業は比較的短期間で進められる一方、アカウント管理や脆弱性管理が属人的な場合は、仕組みづくりから必要です。

費用も、IPAへの登録料だけでなく、専門家・評価機関への費用、脆弱性診断や技術検証、セキュリティ製品・設定変更、規程整備、社内工数、再診断などを含めて考える必要があります。2026年11月17日時点で、★3の登録料は通常20,000円／年（2028年3月31日までは10,000円／年）、★4は60,000円／3年です。これらは制度の登録料であり、評価や対策に必要な外部費用を含むものではありません。

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

社内稟議で説明すべきポイント

社内稟議では「セキュリティを強化するため」だけでは、投資判断が難しい場合があります。重要顧客との取引継続、新規取引の参加条件、委託先管理への対応、事故時の事業停止リスク、監査対応工数の削減といった経営上の効果を明確にすることが有効です。

予算は、①現状評価・ギャップ分析、②規程・運用整備、③技術対策、④診断・評価、⑤取得後の継続運用に分けると説明しやすくなります。また「全てを一度に実施する案」と「重要取引に必要な範囲から段階的に実施する案」を比較できるようにすると、経営判断につながりやすくなります。

支援会社を選ぶ際のチェックポイント

SCS評価制度への支援会社を選ぶ場合、要求事項を解説できるだけでなく、現状評価から技術対策、脆弱性診断、是正支援、証跡整備まで実務をつなげられるかを確認することが重要です。制度対応は、コンサルティング文書だけでは完了しないためです。

- ・★3・★4の要求事項・評価基準と最新ガイドを理解しているか
- ・取得単位・適用範囲の設計を支援できるか
- ・規程と実際のIT運用の両方を確認できるか
- ・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必要性に応じて使い分けられるか
- ・指摘事項の優先順位付けと是正まで支援できるか
- ・個人情報・機密情報の取扱い、再委託、データ保管方法を明確に説明できるか
- ・取得後の更新・継続監視・教育まで見据えた提案ができるか

RFPや見積依頼では、対象範囲、希望する★、希望時期、既存認証、システム構成、想定成果物、診断の要否、是正支援の範囲、再評価の条件を伝えると、見積条件を比較しやすくなります。

よくある失敗と注意点

製品導入から始めてしまう

SCS評価制度は特定製品の導入を一律に求める制度ではありません。まずギャップ分析を行い、必要な対策を見極めます。

適用範囲を曖昧なまま進める

対象事業・拠点・システムが曖昧だと、評価資料や診断対象が膨らみます。取引上必要な範囲から明確にします。

規程だけ作り、運用証跡を残さない

規程と実運用が一致していることを示す記録が必要です。日常業務の中で証跡を残す仕組みを作ります。

情報システム部門だけで抱える

営業・法務・総務・人事・事業部門が持つ資料や業務が評価に関わるため、横断チームで進める方が効率的です。

診断結果を修正せず保管するだけ

脆弱性診断は報告書を受け取ることが目的ではありません。リスクに応じて是正し、必要に応じて再診断で確認します。

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、要求事項のチェックだけで終わらせず、経営・取引上の目的から逆算して設計します。企業ごとの事業、既存のセキュリティ体制、取引先から求められる水準を踏まえ、取得単位・適用範囲の整理、ギャップ分析、規程・証跡整備、技術対策の優先順位付けまで一気通貫で支援できます。

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などの技術サービスと組み合わせることで、制度上の説明と実際のリスク低減を同じ計画の中で進められます。診断で問題を見つけた後の改善・再確認まで対応できる点も、制度対応を実務に定着させるうえで重要です。

よくある質問

Q1. SCS評価制度対応は、まず何から始めればよいですか？

取引先から求められる水準と、自社が対象にしたい事業・システムを整理したうえで、公式の要求事項・評価基準に対するギャップ分析から始めるのが基本です。

Q2. ★3と★4のどちらを目指すべきですか？

重要顧客の要求、扱う情報、事業停止時の影響、第三者評価の必要性を基準に判断します。★4は実地審査と技術検証を含むため、より客観性が求められる取引で検討されやすい水準です。

Q3. ISMSを取得済みなら、SCS評価制度対応は不要ですか？

不要とは限りません。既存の規程、リスク管理、監査、教育等は活用できますが、SCSの要求事項・評価基準に照らして不足を確認する必要があります。

Q4. SCS評価制度のために新しいセキュリティ製品は必須ですか？

一律に必須ではありません。IPAも特定製品の導入を求める制度ではないと説明しています。自社のリスクとギャップに応じて必要な対策を選びます。

Q5. 脆弱性診断はいつ実施すべきですか？

ギャップ分析後、評価前に重要な外部公開資産やWebサービスの状態を把握し、是正期間を確保できる時期に実施するのが実務的です。大きな改修後や新規公開時には再診断も検討します。

Q6. どのような証跡を準備すればよいですか？

アカウント棚卸し、パッチ適用、ログ確認、教育、バックアップ復旧テスト、インシデント訓練、委託先評価など、要求事項に対応する実施記録を整理します。

Q7. 準備にはどれくらいの期間がかかりますか？

既存の規程・運用状況、対象範囲、技術的な是正量によって異なります。特にインフラ改修や運用実績の証跡を作る必要がある場合は、制度開始直前より早めの着手が有効です。

Q8. 申請方法はもう確定していますか？

2026年11月17日時点で、IPAは「登録申請の手引」を2026年11月末頃に公表予定としています。申請時には最新の公式情報を確認してください。

まとめ｜SCS評価制度対応は「ギャップの可視化」から始める

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）への対応で最も重要なのは、いきなり製品導入や申請準備に入るのではなく、取引上必要な水準と適用範囲を決め、要求事項・評価基準とのギャップを明確にすることです。

その後、規程・証跡・技術対策を優先順位付きで整備し、自己評価と模擬確認を通じて「実施していることを説明できる状態」にします。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も、制度取得のためだけに実施するのではなく、実際の事業リスクを下げるための手段として位置付けることが重要です。

制度開始が近づくほど、評価機関や技術検証事業者への相談が集中する可能性もあります。重要顧客との取引継続や新規取引での要求が想定される企業は、現状把握だけでも早めに着手しておくと、その後の予算化と意思決定を進めやすくなります。

SCS評価制度への対応方針が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」「どこまでを適用範囲にすべきか判断できない」「規程はあるが証跡が十分か不安」「脆弱性診断をどの範囲で実施すべきか整理したい」といった段階でもご相談いただけます。Librus株式会社では、制度対応のための形式的なチェックにとどまらず、取引上の優先度と実際のサイバーリスクを踏まえて、必要な対策を整理します。

対象範囲や実施方法が決まっていない段階で現状を整理することで、不要な製品導入や過剰な診断を避けつつ、社内稟議に必要な費用・スケジュール・優先順位を明確にできます。既存のISMSや社内規程を活かしたい場合、評価前に技術的な弱点を確認したい場合、取得後の継続運用まで含めて検討したい場合も、企業ごとの状況に合わせて支援します。

参考情報

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

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

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

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

出典：**IPA**「評価用ガイド等を公開」**2026**年**10**月**28**日 https://www.ipa.go.jp/pressrelease/2026/press20261028.html

出典：経済産業省「**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