

SCS評価制度の★3・★4とは？違いと企業が目指すべき水準を解説

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）は、取引先に求めるセキュリティ対策の水準を共通化し、実施状況を可視化するための制度です。★3は「一般的なサイバー脅威に対処できる最低限の実装水準」、★4は「侵入後の被害拡大防止や技術検証まで含む標準的な水準」と位置付けられています。

従業員100～1,000名規模の企業では、まず取引先から求められる水準と自社の事業リスクを整理し、★3で十分なのか、★4までを目指すべきなのかを判断することが重要です。特に、機密情報や個人情報を預かる企業、重要な業務システムを運用する企業、停止時に取引先へ大きな影響が出る企業は、★4を視野に入れた準備が現実的です。

本記事では、2026年10月4日時点でIPA・経済産業省が公表している一次情報をもとに、★3・★4の違い、対象企業、対応手順、技術検証、費用・期間、社内稟議、支援会社の選び方まで実務目線で解説します。

この記事で分かること

- SCS評価制度の目的と、★3・★4の位置付け
- ★3と★4の要求水準・評価方法・技術検証の違い
- 自社が★3と★4のどちらを目指すべきかの判断基準
- 申請前に準備すべき資料、体制、診断・テストの考え方
- 費用・期間を左右する要因と、稟議・ベンダー選定のポイント

SCS評価制度とは

SCS評価制度は、サプライチェーンを通じたサイバーリスクへの対応を目的として、経済産業省と内閣官房国家サイバー統括室の監督のもと、独立行政法人情報処理推進機構（IPA）が運営する評価制度です。★3・★4は2027年3月頃の運用開始が予定されています。

背景にあるのは、委託元が取引先のセキュリティ対策を評価しにくい一方、委託先は複数の取引先から異なるチェックシートへの回答を求められ、双方に負担が生じているという問題です。SCS評価制度では、取引契約等において委託元が適切な段階を示し、委託先がその水準を満たしているか確認できる共通の枠組みを目指しています。

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>

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★3・★4の違い

結論からいえば、★3と★4の最大の違いは「求められる対策の深さ」と「評価の客観性」です。★3は専門家の確認を受けた自己評価で取得を目指します。一方、★4は指定された評価機関による第三者評価に加え、実地審査や技術検証まで行われます。

比較項目	★3 Basic	★4 Standard	実務上の意味
位置付け	最低限実装すべき対策	標準的に目指すべき対策	取引先への影響や扱う情報の重要性が高いほど★4を検討
要求事項数	26項目	44項目	★4は★3を包括し、より広い対策が必要
評価方法	専門家確認付き自己評価	第三者評価	★4は社外から説明できる客観性が高い
確認内容	主に書類確認	文書確認・実地審査・技術検証	★4は実装状況まで検証される
有効期間・登録料	1年・10,000円(2028年3月31日まで)	3年・60,000円	登録料以外に支援・評価・技術検証等の費用が発生し得る

出典:IPA「中小企業の情報セキュリティ対策ガイドライン第4.0版 説明資料」

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0_app_setsumeisiryoku.pdf

出典:IPA「料金設定のお知らせ」<https://www.ipa.go.jp/security/scs/rcu1hd00000075om-att/pricelist.pdf>

★3とは | 一般的な脅威に対処する最低限の実装水準

★3は、一般的なサイバー脅威に対処し得ることを水準として定めた段階です。IPAの整理では「最低限実装すべき対策(26項目)」とされ、取得希望組織が自己評価を行い、SCSセキュリティ専門家の確認と助言を経た上で、経営層による自己適合宣誓を含む申請を行う仕組みです。

ここで重要なのは、単なるチェックシート回答ではない点です。すべての要求事項・評価基準を満たす必要があり、「規程はあるが運用されていない」「端末対策はあるが、対象範囲に漏れがある」といった状態では適合が難しくなります。

★4とは | 侵入後の被害拡大防止と第三者評価まで求める水準

★4は、初期侵入を防ぐ対策だけではなく、侵入された場合の被害拡大防止、攻撃者による目的遂行のリスク低減、取引先のデータ・システム保護、サプライチェーンにおける自社の役割に応じた強靱化策まで求める段階です。要求事項は44項目で、評価機関による第三者評価と技術検証が行われます。

技術検証では、規程や設定値を読むだけでは見つからない弱点を確認します。例えば、インターネット公開されたWebアプリケーションに認証不備や入力値検証の欠陥がないかを確認するWebアプリケーション診断、サーバー・ネットワーク機器・クラウド基盤の設定不備や脆弱性を確認するプラットフォーム診断、さらに攻撃者と同様の観点で侵入経路や横展開の可能性を検証するペネトレーションテストなどが、対象範囲やリスクに応じて重要になります。

★3を取ってからでないと★4に進めないわけではない

★4は★3の内容を包括しますが、★3の取得が★4申請の前提条件ではありません。自社の取引上の立場や顧客要求から★4が必要であれば、最初から★4を目指すことも可能です。ただし、現状が★3相当にも達していない場合、いきなり第三者評価へ進むと是正項目が増え、期間や費用が膨らみやすくなります。実務上は、まずギャップ分析で★3相当の基礎を固め、その後★4要求へ広げる進め方が効率的です。

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

なぜ今、SCS評価制度への準備が必要なのか

SCS評価制度は法令上の一律義務として全企業に取得を求めるものではありません。しかし、制度が取引契約における共通の確認手段として使われることが想定されているため、調達条件や取引先監査の中で「★3以上」「重要委託先は★4」といった要求が出てくる可能性があります。

特に従業員100～1,000名規模の企業は、大企業の重要な委託先である一方、専任のセキュリティ人材や予算が十分でないことがあります。制度開始後に顧客から対応を求められてから着手すると、規程整備、資産棚卸し、アクセス権見直し、ログ管理、バックアップ、教育、脆弱性対応などを短期間で並行して進めることになり、現場負担が高くなります。

経済産業省は、2024年度の中小企業実態調査を踏まえ、サイバー攻撃の被害を受けた中小企業の約7割で取引先にも影響が及んだと紹介しています。セキュリティ対策は自社のIT課題だけではなく、取引継続や信用維持に関わる経営課題として考える必要があります。

出典:経済産業省「中小企業のための実例で学ぶサイバーセキュリティリスク事例集等を公表」

<https://www.meti.go.jp/press/2025/03/20260327002/20260327002.html>

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生じる制度ではありません。実務上の問題は、取引先から求められた水準を説明できないことです。新規取引のセキュリティ審査で追加資料を求められる、既存取引先の監査で改善計画を要求される、重要業務の委託先候補から外れるといった影響が考えられます。

また、評価取得とは別に、対策不足そのものが事業継続リスクになります。例えば、VPNや公開サーバーの脆弱性から侵入され、認証情報を窃取された後に社内ネットワークへ横展開されると、基幹システム停止やランサムウェア被害につながる可能性があります。Webアプリケーションの認可不備があれば、顧客情報や取引データの漏えいに発展することもあります。

経営層は「制度取得のためのコスト」だけでなく、「取引停止・復旧費用・顧客説明・信用毀損を含む損失を抑えるための投資」として判断することが重要です。

どの企業が★3・★4を目指すべきか

★3を基本線にしやすい企業

★3は、サプライチェーン企業としてまず共通の最低限水準を整えたい企業に向いています。重要情報の保有量が比較的限定され、顧客から高度な第三者評価を求められていない場合でも、取引先からのチェックシート対応を効率化したい企業や、社内対策を一度体系的に整理したい企業には有効です。

★4を優先的に検討したい企業

★4は、次のような企業で優先度が高くなります。取引先の機密情報や個人情報を大量に扱う、クラウドやSaaSを顧客へ提供する、顧客の基幹業務を受託する、停止時にサプライチェーンへ波及する、インターネット公開システムが多い、M&A・IPO・大手企業との新規取引などで客観的なセキュリティ説明が必要、といったケースです。

判断の軸は会社規模だけではありません。「侵害されたときに誰へ、どの程度の影響が及ぶか」「顧客からどの程度の証明を求められるか」「第三者に検証されても説明できる状態か」を基準にすると、目標水準を決めやすくなります。

SCS評価制度への具体的な対応手順

1. 経営層が目標水準と対象範囲を決める

最初に決めるべきなのは、★3か★4かだけではありません。どの法人、事業、拠点、システム、クラウド環境を評価対象とするかを明確にします。対象範囲が曖昧なまま規程整備や診断を始めると、後から不足が見つかり、再作業が発生します。

経営層は、主要顧客の要求、事業停止時の売上影響、扱う情報の重要性、海外取引の有無、既存のISMS・Pマーク等との重複を踏まえて、対象範囲と期限、予算責任者を決定します。

2. 現状と要求事項のギャップ分析を行う

次に、★3・★4の要求事項・評価基準に対して、現状がどこまで満たしているかを確認します。この段階では「対応済み・未対応」の二択ではなく、規程、運用、証跡、技術設定の4つに分けて確認すると実務的です。

例えばアクセス制御について、規程に「最小権限」と書いてあっても、退職者アカウントが残っている、管理者権限の棚卸し記録がない、SaaSごとに承認方法が異なる場合は、運用・証跡面の改善が必要です。

3. 情報システム部門が資料と証跡を整える

実施前に準備しておきたい資料は、情報セキュリティ基本方針・各種規程、組織図、情報資産台帳、システム構成図、ネットワーク構成図、クラウド・SaaS一覧、アカウント・権限管理台帳、ログ管理方針、バックアップ手順、インシデント対応手順、委託先一覧、教育実施記録、脆弱性対応記録などです。

重要なのは「文書を作ること」ではなく、「運用されている証拠が残っていること」です。承認記録、棚卸し結果、教育受講記録、パッチ適用記録、バックアップ復元テスト結果などを定期的に残す設計にすると、評価対応だけでなく日常運用も安定します。

4. 技術対策を実装し、必要に応じて診断・テストを行う

技術面では、多要素認証、端末保護、パッチ管理、ネットワーク分離、ログ収集、バックアップ、メール対策、クラウド設定管理などを要求事項に沿って整備します。★4を目指す場合は、外部から確認できる脆弱性だけでなく、侵入後の横展開や権限昇格を含めた検証が重要です。

Webアプリケーション診断では、SQLインジェクション、クロスサイトスクリプティング、認証・認可不備、セッション管理などを確認します。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・クラウド設定の脆弱性や不要ポート等を確認します。ペネトレーションテストは、個別の脆弱性を列挙するだけでなく、それらを組み合わせて実際にどこまで侵入・横展開できるかを検証する点が特徴です。

診断対象は「全システムを一律に実施」ではなく、公開範囲、重要情報、権限、顧客影響を基準に優先順位を付けます。対象が多い企業では、重要システムから段階的に実施し、年度計画へ落とし込む方が現実的です。

5. 指摘事項をリスクベースで是正する

改善項目は、重大度だけでなく、攻撃されやすさ、悪用時の事業影響、外部公開の有無、代替策の有無、修正難易度を合わせて優先順位付けします。例えば、外部公開VPNの重大な脆弱性や管理者アカウントへの多要素認証未導入は、社内向けの軽微な設定不備より優先して是正すべきです。

改善計画には、対応内容、責任部署、期限、暫定対策、再確認方法を明記します。システム改修に時間がかかる場合は、アクセス元制限やWAF、監視強化などの代替策を入れ、リスクを放置しないことが重要です。

6. ★3は専門家確認、★4は第三者評価・技術検証へ進む

★3では、取得希望組織が作成した自己評価をSCSセキュリティ専門家が確認し、必要に応じて修正助言を行います。★4では、指定された評価機関が文書確認、実地審査、技術検証を行い、評価報告書を作成します。

2026年10月4日時点では、IPAのFAQ上、★3・★4の申請方法や取得ガイド等は「2026年10月頃公開予定」とされています。公開後は、最新手順に合わせて申請準備を更新する必要があります。

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

費用と期間を左右する要因

IPAが2026年9月18日に公表した料金では、登録希望組織の登録料は、2028年3月31日まで★3が1年分10,000円、★4が3年分60,000円です。ただし、これは制度上の登録料であり、専門家確認、第三者評価、技術検証、コンサルティング、システム改修、診断などの費用は別途発生します。

総費用を大きく左右するのは、対象範囲、拠点数、端末・サーバー数、クラウド数、既存規程の成熟度、証跡の整備状況、Webアプリケーションの数、ペネトレーションテストの範囲、是正に必要なシステム改修です。単に「★4はいくら」と一律に見積もるより、最初にギャップ分析を行い、必要な作業を分解して予算化の方が精度が上がります。

期間についても一律ではありません。規程や台帳が整っている企業と、資産棚卸しから始める企業では準備量が大きく異なります。制度開始に合わせたい場合は、評価機関の予約や技術検証の実施枠も考慮し、社内の是正期間を十分に確保して逆算することが重要です。

社内稟議では何を説明すべきか

SCS評価制度対応の稟議では、「認証を取るため」という説明だけでは投資判断につながりにくいため、取引上の必要性和事業リスクをセットで示します。主要顧客から想定される要求、未対応時の取引影響、対象事業の売上規模、停止時の影響、情報漏えい時の対応コスト、既存施策との重複・流用可能性を整理すると説明しやすくなります。

また、費用を一括で示すのではなく、「現状評価」「規程・運用整備」「技術対策」「診断・テスト」「評価・登録」のように分けると、経営層が投資の意味を理解しやすくなります。複数年度での改善計画にできる項目と、制度開始前に必須となる項目を分けることも有効です。

支援会社・評価関連ベンダーの選び方

支援会社を選ぶ際は、制度文書を読めるだけでなく、現場へ実装できるかを確認することが重要です。規程作成だけを支援しても、実際の端末設定、クラウド構成、ログ管理、脆弱性対応、教育運用が伴わなければ評価時に不整合が生じます。

見積依頼やRFPでは、対象範囲、現状調査の方法、要求事項ごとの成果物、診断・技術検証の範囲、是正支援の有無、再確認の方法、個人情報・機密情報の取扱い、報告会の対象者、追加費用条件を明確にします。

特に★4を目指す場合は、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などを一貫して設計できるか、経営層向けと技術部門向けの双方に説明できる報告書を作成できるかを確認してください。評価機関としての第三者性が求められる場面では、コンサルティングと評価の役割分担や中立性についても、最新の制度規程に沿って確認する必要があります。

よくある失敗と注意点

規程作成だけで終わる

SCS評価制度では、文書が存在することと、実際に運用されていることは別です。規程を短期間で整えても、権限棚卸しやバックアップ復元確認、教育、ログ監視などが実施されていなければ不十分です。制度対応を日常運用へ組み込む設計が必要です。

対象範囲を広げすぎる、または狭めすぎる

全社を一度に対象にして準備量が膨らむケースもあれば、重要システムを対象外にして評価の目的と合わなくなるケースもあります。取引先へ提供するサービスや守るべき情報とのつながりから対象範囲を決めることが重要です。

診断を実施して報告書を保管するだけ

脆弱性診断やペネトレーションテストは、実施自体が目的ではありません。発見事項の是正、再診断、再発防止、設計標準への反映まで行って初めて対策として機能します。高リスク項目には経営層も含めた期限管理が必要です。

制度公開前の古い情報で計画を固定する

SCS評価制度は運用開始に向けて詳細化が進んでいます。2026年10月4日時点でも、申請方法や解説書等は公開予定段階のものがあります。過去の検討資料だけで対応を固定せず、IPA・経済産業省の最新情報を確認しながら計画を更新してください。

Librus株式会社が提供できるSCS評価制度支援

Librus株式会社では、SCS評価制度の取得そのものだけを目的にするのではなく、取引先から説明可能で、実際の攻撃にも耐えられるセキュリティ体制づくりを支援します。

具体的には、★3・★4要求事項に対するギャップ分析、対象範囲の整理、規程・運用プロセスの整備、リスクアセスメント、経営層向けのロードマップ策定に加え、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、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、セキュリティ教育まで一気通貫で対応できます。

制度対応と技術対策を別々のベンダーへ依頼すると、要求事項と実装内容が分断されることがあります。Librus株式会社では、経営・ガバナンスと技術検証をつなぎ、企業ごとの事業環境や予算、既存システムを踏まえて優先順位を設計します。診断で指摘して終わるのではなく、改善、再確認、継続運用までを含めた支援が可能です。

SCS評価制度の★3・★4に関するよくある質問

Q1. SCS評価制度はすべての企業に義務ですか？

一律の法的義務として全企業に取得を求める制度ではありません。ただし、取引先が契約や調達条件として一定の★を求める使われ方が想定されているため、自社の顧客要求を確認する必要があります。

Q2. ★3と★4はどちらを目指すべきですか？

一般的なサイバー脅威への最低限の備えを共通水準として整えるなら★3、重要情報や基幹業務を扱い、第三者評価・技術検証を通じてより客観的に対策状況を示す必要があるなら★4が有力です。

Q3. ★3を取得してからでない★4は取得できませんか？

いいえ。★3の事前取得は必須ではありません。自社の取引条件やリスクに応じて、最初から★4を目指すことも可能です。

Q4. ★3・★4は一部の要求事項だけ満たせば取得できますか？

IPAのFAQでは、★3・★4ともに、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。

Q5. 脆弱性診断は必ず必要ですか？

対象範囲や要求事項との関係で必要性を判断します。特に★4では技術検証が行われるため、外部公開システムや重要システムについて、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等を事前に実施して弱点を把握しておくことが有効です。

Q6. 申請前に何を用意すればよいですか？

規程類だけでなく、資産台帳、構成図、アカウント管理、ログ、バックアップ、教育、脆弱性対応、インシデント対応などの運用証跡を準備します。まず要求事項とのギャップ分析を行うと効率的です。

Q7. 登録料はいくらですか？

2026年9月18日公表の料金では、2028年3月31日まで★3は1年分10,000円、★4は3年分60,000円です。専門家確認、第三者評価、技術検証、コンサルティングや改修等の費用は別途考える必要があります。

Q8. ISMSを取得していればSCS評価制度への対応は不要ですか？

両制度は目的と評価の考え方が異なります。ISMSの仕組みや証跡をSCS評価制度の準備に活用できる場合がありますが、SCS評価制度固有の要求事項・評価基準への適合確認が必要です。

まとめ | SCS評価制度は「★の取得」ではなく取引継続に耐える体制づくりが重要

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は、一般的な脅威に対処する最低限の実装水準で、専門家確認付き自己評価が基本です。★4は、侵入後の被害拡大防止やサプライチェーン強靱化まで踏み込み、第三者評価と技術検証を伴う標準的な水準です。

企業が目指すべき段階は、従業員数だけでは決まりません。顧客要求、扱う情報の重要性、事業停止時の影響、公開システムの攻撃面、取引先への波及リスクを踏まえて判断する必要があります。制度対応を急いで書類だけ整えるのではなく、現状把握、優先順位付け、技術対策、運用証跡、再確認までを一つの改善プロセスとして設計することが重要です。

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判断できない」「要求事項と自社の現状を比較したい」「診断やペネトレーションテストをどこまで実施すべきか分からない」「社内稟議に必要な予算とロードマップを整理したい」といった段階でも、Librus株式会社へご相談いただけます。

現状の体制・システム・主要取引先から求められる水準を整理し、必要な対策を優先順位付きで可視化することで、不要な投資を抑えながら、制度対応と実効性のあるセキュリティ強化を同時に進めやすくなります。対象範囲や実施方法が決まっていない場合も、初期整理から支援可能です。

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>