SCS評価制度の★3と★4を徹底比較｜自社はどちらを目指すべきか

はじめに

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（以下「SCS評価制度」）は、取引先との間で求めるサイバーセキュリティ対策の水準を共通化し、その実施状況を可視化する仕組みです。★3と★4では、単にチェック項目の数が違うだけではありません。守るべき範囲、侵入後を見据えた対策、評価の客観性、技術検証の有無が大きく異なります。

経済産業省と内閣官房国家サイバー統括室が2026年3月に制度構築方針を公表し、IPAが制度を運営します。★3・★4は2027年3月頃の運用開始が予定されています。2026年9月3日現在、申請・登録費用や申請方法の詳細は未公表です。そのため、本記事では確定情報と実務上の見立てを明確に分けて説明します。

この記事で分かること

- ★3と★4の対象企業、要求水準、評価方式の違い
- 自社がどちらを目指すべきかを判断するための基準
- 準備期間と費用を左右する要因、社内稟議での説明ポイント
- 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
- 取得準備から改善・運用までの具体的な進め方

SCS評価制度とは

SCS評価制度は、発注者が受注者に適切な対策段階を示し、受注者がその水準の対策を実施していることを評価・登録する制度です。対象の中心は、企業活動を支えるIT基盤です。

製造設備などのOTシステムや、顧客へ納入する製品そのものは、原則として直接の対象外です。OTとは、工場設備などを監視・制御する技術を指します。これらには別の制度やガイドラインによる対策が想定されています。

星3は、一般的なサイバー脅威へ対処できる水準です。星4は初期侵入を防ぐだけでなく、侵入後の被害拡大、攻撃目的の遂行、取引先への波及を抑える対策まで求めます。

上位段階は下位段階の内容を含みますが、星3を取得してからでなければ星4へ進めないという前提ではありません。

★3と★4の違いを一覧で比較

比較項目	★3	★4
位置付け	一般的なサイバー脅威に対処し得る基礎水準	侵入後の被害拡大や取引先への波及まで抑える標準的水準
主な対象	幅広い企業。まず共通的な対策基盤を整えたい企業	重要な情報・接続・業務を担い、停止や漏えいの波及が大きい企業
評価方式	セキュリティ専門家の確認を受けた自己評価	指定された評価機関による第三者評価
確認方法	作成書類を専門家が確認し、助言・署名	文書確認に加え、実地審査と技術検証
経営層の関与	自己適合宣誓を含む	組織的運用と客観的な証跡提示がより重要
技術面	基本的な防御、検知、対応、復旧を整備	セグメント分離、監視、侵入・横展開耐性などをより深く検証
費用・期間	外部専門家の確認、文書整備、改善範囲に左右される	第三者評価、実地審査、技術検証、対象拠点・システム数により増えやすい

出典：IPA「SCS評価制度の詳細情報」および経済産業省「SCS評価制度」よりLibrus株式会社作成（2026年9月3日確認） IPA / 経済産業省

対象企業の違い：規模ではなく、取引上の役割で判断する

従業員100人から1,000人という規模だけで、★3か★4かは決まりません。判断の中心は、サプライチェーンにおける自社の役割と、事故が起きた際の影響度です。取引先から預かった個人情報や設計情報を大量に扱う、取引先ネットワークへ常時接続する、基幹部品や重要サービスを代替困難な形で供給するといった企業は、★4の必要性が高まります。

一方、外部との接続が限定的で、重要情報の取扱いが比較的少なく、まず全社の基本対策と運用証跡を整える段階であれば、★3を目標にするのが現実的です。ただし、発注者が契約・調達条件として★4を求める場合は、自社判断だけで★3にとどめることはできません。営業、調達、法務、情報システム部門で主要取引先の要請を確認する必要があります。

★3を目指すべき企業

★3は「セキュリティ製品を一通り導入している企業」ではなく、基本対策がルール、責任者、実装、証跡までつながっている企業に適します。情報資産台帳が未整備、退職者アカウントの削除が部門任せ、バックアップの復元試験をしていないといった状態では、製品導入済みでも評価準備は不足しています。まず★3を通じて、全社共通の最低ラインを作る意義があります。

★4を目指すべき企業

★4は、侵入が起こり得ることを前提に、被害を局所化し、早期に検知し、事業と取引先への影響を抑える能力まで示したい企業に向きます。大手企業の重要委託先、クラウド・SaaS事業者、システム開発・運用会社、物流・決済・BPOなど停止時の影響が広い企業、M&AやIPOでセキュリティ管理の客観性を示したい企業が典型です。

要求水準の違い：★4は『侵入させない』から『広げない・止めない』へ

★3でも、ガバナンス、取引先管理、リスク特定、攻撃防御、検知、インシデント対応、復旧といった一連の管理が必要です。★4ではこれらをより深く実装し、第三者が追跡できる証跡として提示する必要があります。たとえば、多要素認証を導入したという事実だけでなく、どのアカウントを対象にし、例外を誰が承認し、設定が継続しているかまで説明できる状態が重要です。

攻撃例で考えると分かりやすくなります。VPN機器の脆弱性から侵入された場合、★3では機器の把握、更新、アクセス制御、ログ取得、連絡体制などの基本対策が焦点です。★4ではさらに、侵入された端末から基幹システムへ横展開できないネットワーク分離、特権IDの厳格管理、異常挙動の監視、封じ込め手順、取引先への連絡判断まで含めて実効性を確認します。

評価方式の違い：★3は専門家確認付き自己評価、★4は第三者評価

★3の評価プロセス

★3では、取得希望組織が要求事項・評価基準に沿って自己評価を行い、登録された社内外のセキュリティ専門家が内容を確認します。専門家は必要に応じて評価結果の修正を助言し、提出内容を了承した場合に署名します。その後、経営層による自己適合宣誓を含む評価結果を事務局へ提出し、問題がなければ台帳へ登録されます。自己評価であっても、担当者の感覚だけで丸を付ける制度ではありません。

★4の評価プロセス

★4では、自己評価を出発点に、指定された評価機関へ検証・評価を依頼します。評価機関と技術検証事業者は、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。取得希望組織はその結果をもとに事務局へ登録を申請します。評価対象は、組織が決めた適用範囲からサンプリングされる想定です。適用範囲を狭く見せるのではなく、取引リスクに照らして合理的に説明できることが重要です。

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の位置付け

★4の技術検証では、書類上のルールだけでなく、実装上の弱点がないかを確かめます。Webアプリケーション診断は、認証、入力処理、セッション管理、アクセス制御などWeb特有の脆弱性を調べる手法です。プラットフォーム診断は、サーバー、ネットワーク機器、OS、ミドルウェアの設定不備や既知脆弱性を確認します。

ペネトレーションテストは、現実的な攻撃シナリオに沿って侵入可能性や侵入後の影響を検証する試験です。脆弱性診断が弱点を網羅的に見つけることを得意とするのに対し、ペネトレーションテストは弱点を組み合わせたときに、重要情報への到達や権限昇格が可能かを確かめます。両者は代替関係ではありません。対象資産、脅威シナリオ、制度上の技術検証仕様に応じて組み合わせる必要があります。

なぜ今、準備を始めるべきか

制度開始まで待ってから着手すると、台帳や規程は作れても、運用実績という証跡が不足しがちです。アクセス権棚卸し、教育、脆弱性対応、バックアップ復元試験、インシデント訓練は、一度実施して終わるものではありません。計画、実施、記録、改善のサイクルが回っていることを示すには時間がかかります。

また、日本企業では次年度予算の要求、相見積もり、稟議、契約、対象部門との日程調整に数か月を要することがあります。特に★4では、第三者評価の前に不足事項を直す期間と、技術検証の対象システム所有者との調整が必要です。2027年3月頃の運用開始を見据えるなら、現状評価と適用範囲の整理は早めに着手する価値があります。

対応しなかった場合に起こり得る問題

SCS評価制度は任意制度として設計されていますが、取引の現場では発注者の調達条件や取引先評価へ組み込まれる可能性があります。未取得が直ちに取引停止を意味するわけではありません。しかし、同等の品質・価格で競合が必要な段階を取得している場合、選定上の説明力で差がつくことは考えられます。

より本質的な問題は、取得できない背景にある管理不備です。資産が把握できていなければ、重大な脆弱性が公表されても影響範囲を判断できません。ネットワークが分離されていなければ、一台の端末感染が生産、受発注、会計へ広がる可能性があります。連絡基準がなければ、取引先への報告が遅れ、信用毀損や契約上の問題を拡大させます。評価対応は、取引資格のためだけでなく事業継続の整備として捉えるべきです。

★3・★4取得に向けた具体的な進め方

1. 経営層が目標段階と適用範囲を決める

最初に、主要取引先の要請、自社が保有する情報、システム停止時の影響、取引先ネットワークとの接続を整理します。そのうえで★3・★4のどちらを目指すか、全社か特定事業・拠点か、責任者と予算枠を決定します。適用範囲は評価工数と費用へ直結しますが、重要な業務を恣意的に除外すると制度の利用目的に合いません。

2. 要求事項とのギャップを可視化する

規程の有無だけではなく、実装と運用証跡を確認します。必要資料は、組織図、情報セキュリティ方針・規程、情報資産台帳、ネットワーク構成図、クラウド利用一覧、アカウント・権限一覧、ログ管理方針、脆弱性管理記録、バックアップ設計、委託先一覧、教育記録、インシデント対応手順などです。資料が存在しても現状と一致しなければ、不備として扱って改善します。

3. リスクに応じて改善の優先順位を付ける

すべてを同時に直すのではなく、悪用可能性と事業影響で優先順位を付けます。インターネットへ公開された既知脆弱性、管理者アカウントへの多要素認証未導入、バックアップの同一ネットワーク保管、退職者IDの残存などは優先度が高い典型です。規程改定だけで解決する項目と、製品導入・設計変更・教育が必要な項目を分けると、稟議と実行計画が組みやすくなります。

4. 技術検証とリハーサルを行う

★4を目指す場合は、本番の第三者評価前に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を実施し、重大な不備を修正します。★3でも、自己評価の確度を高めるため診断は有効です。診断では対象IP、URL、アカウント、試験時間帯、禁止事項、障害時連絡先、個人情報・機密情報の取扱いを事前に合意します。

5. 経営層の確認を経て申請し、取得後も運用する

評価直前だけ帳尻を合わせると、更新時や取引先監査で運用実態とのずれが表面化します。発見事項は、責任者、期限、暫定対策、恒久対策、再確認方法を付けて管理します。再診断、ログ監視、教育、インシデント訓練を年間計画へ組み込み、システムや組織の大きな変更時には適用範囲と評価への影響を見直します。

費用と期間を左右する要因

2026年9月3日現在、★3・★4の申請・登録費用は公表されていません。したがって、確定額として見積もれるのは制度料金ではなく、自社の準備・改善、専門家支援、診断・技術検証などの周辺費用です。★4は第三者評価、実地審査、技術検証を伴うため、一般に★3より工数が大きくなる構造ですが、正式価格は公表後に確認する必要があります。

費用と期間を左右する主な要因は、対象拠点・法人・システム数、クラウドとオンプレミスの混在、規程・台帳の整備度、ネットワーク構成の複雑さ、技術検証対象の数、重大不備の改修難易度、証跡の蓄積状況です。従業員数が同じでも、一拠点で標準化された企業と、買収した複数法人が別々のIT環境を持つ企業では大きく異なります。

実施期間の目安は、制度の正式な審査日数ではなく準備プロジェクトとして見積もるべきです。現状評価、改善計画、規程・実装の改修、運用証跡の蓄積、事前確認、本評価という工程へ分け、各工程に社内承認と調整期間を加えます。短期間の取得を約束する事業者より、前提条件とボトルネックを明示する事業者の方が信頼できます。

社内稟議で説明すべき内容

稟議では「制度対応が必要だから」だけでなく、売上防衛と事業継続の両面を示します。主要取引先の売上比率、求められる段階、未対応時の入札・更新への影響、事故時の停止業務、法務・広報・復旧費用への波及を整理します。そのうえで、取得支援費、改善費、評価費を分け、今年度と次年度の予算へ配置します。

経営層が判断すべき事項は、目標段階、適用範囲、許容する残余リスク、責任者、予算、重大不備の是正期限です。情報システム部門だけに丸投げせず、法務は契約・報告義務、人事は教育と入退社、調達は委託先管理、事業部門は重要業務と復旧目標を担う体制が必要です。

支援会社・評価関連事業者の選び方

制度取得支援と、★4の第三者評価は役割が異なります。支援会社を選ぶ際は、要求事項の説明だけでなく、技術面の検証と改善、経営層への説明、取得後の運用まで一貫して支援できるかを確認します。第三者評価を担う評価機関については、IPAが公表する指定状況と、中立性・公平性に関する最新要件を必ず確認してください。

RFPまたは見積依頼では、対象範囲、前提資料、現地訪問の有無、診断対象数、成果物、再確認の条件、追加費用、機密情報の保管場所と削除時期、再委託の有無、インシデント発生時の責任分界を明記します。成果物には、要求事項別の適合状況、根拠資料、ギャップ、リスク評価、優先順位、改善案、担当部門、期限、評価前に残る論点が含まれるかを確認しましょう。

よくある失敗と注意点

製品導入をそのまま適合と考える

SCS評価制度は特定製品の導入を必須としていません。EDRやMFAを導入していても、対象漏れ、設定不備、アラート放置があれば実効性は不足します。製品名ではなく、要求事項に対してどの仕組みがどう機能し、誰が証跡を確認するかを説明できる状態にします。

適用範囲をIT部門だけで決める

重要な委託業務や取引先データの流れは、事業部門や営業部門にしか分からないことがあります。ネットワーク図だけで範囲を決めると、業務委託先、SaaS、個人端末、海外拠点が漏れます。業務フローとデータフローを重ねて判断してください。

診断を一度実施して終える

診断結果は、その時点の対象と設定に対するスナップショットです。新しい脆弱性、システム変更、アカウント追加で状況は変わります。重大度だけでなく、外部公開、保有データ、悪用経路、代替策を踏まえて期限を決め、修正後の再診断まで完了させる必要があります。

制度の未公表事項を確定情報として扱う

申請料金、申請手順、解説書などは順次公表予定です。古い検討資料や民間記事だけで稟議を確定すると、後で条件が変わる可能性があります。IPAと経済産業省の公式ページを基準日付きで確認し、見積書にも未確定事項を明記することが大切です。

Librus株式会社が提供できる支援

Librus株式会社は、SCS評価制度への対応を単なるチェックリスト作成で終わらせず、経営リスクと技術リスクを一つの改善計画へ落とし込みます。現状評価、適用範囲の整理、規程・台帳整備、リスクアセスメント、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、教育・訓練、インシデントレスポンスまで一気通貫で支援可能です。

企業ごとの業務、既存製品、予算、取引先要請を踏まえて個別設計するため、過剰な製品導入を前提にしません。経営層には事業継続・取引維持・投資優先順位の言葉で、情報システム部門には実装・証跡・運用の言葉で整理し、両者の意思決定をつなぎます。M&A、IPO、取引先監査など、短期間で説明責任が高まる局面にも対応します。

よくある質問

Q1. ★3を取得してからでなければ★4を取得できませんか。

いいえ。★4は★3の内容を含みますが、★3の事前取得は必須ではありません。現状の成熟度と取引先要請が合えば、最初から★4を目指せます。

Q2. 従業員数が多い企業は必ず★4ですか。

いいえ。規模だけでは決まりません。重要情報の取扱い、取引先との接続、供給停止の影響、発注者の要求で判断します。

Q3. ★3は完全な自己評価ですか。

いいえ。取得希望組織が自己評価を行いますが、登録されたセキュリティ専門家の確認・助言・署名と、経営層の自己適合宣誓が必要です。

Q4. ★4では何が追加されますか。

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。侵入後の被害拡大や取引先への波及を抑える対策も重要になります。

Q5. ★4にはペネトレーションテストが必須ですか。

技術検証の具体的な対象・手法は制度の最新文書と評価機関の計画で確認が必要です。制度構築方針では、技術検証事業者の対象となる脆弱性診断サービスにペネトレーションテストを含む整理が示されています。

Q6. 申請費用はいくらですか。

2026年9月3日現在、申請・登録費用は未公表です。準備支援、改善、診断、第三者評価などを分けて見積もり、制度料金は公表後に更新してください。

Q7. 準備にはどのくらいかかりますか。

一律の期間はありません。対象範囲、資料整備、重大不備、技術検証対象、社内承認で変わります。まず短期間のギャップ分析を行い、工程別に見積もる方法が現実的です。

Q8. ISO/IEC 27001を取得済みなら対応不要ですか。

既存の管理策や証跡は活用できますが、自動的にSCS評価制度へ適合するとは限りません。SCSの要求事項・評価基準との対応関係を確認する必要があります。

まとめ：★3を基礎線、★4を取引・事業影響に応じた目標として判断する

SCS評価制度の★3と★4の本質的な違いは、★3が一般的な脅威へ対処するための専門家確認付き自己評価であるのに対し、★4は侵入後の被害拡大と取引先への波及まで見据え、第三者評価・実地審査・技術検証で客観性を高める点にあります。

自社が目指す段階は、従業員数ではなく、取引先の要求、扱う情報、外部接続、供給停止の影響で決めます。迷う場合は、★3・★4の両方に対して現状ギャップを可視化し、必要な改善費と事業上の効果を比較するのが近道です。制度開始前から証跡を蓄積すれば、取得対応を一過性の作業ではなく、取引継続と事業継続を支える仕組みにできます。

★3・★4の選択から整理したい企業さまへ

取引先から具体的な段階を指定されていない場合でも、主要業務、データ、接続先、停止影響を整理すれば、自社が目指す水準は見えてきます。Librus株式会社では、対象範囲や実施方法が決まっていない段階から、★3・★4それぞれのギャップと概算工程を整理します。社内説明に使える判断材料を先に作りたい場合もご相談いただけます。

出典・参考資料

- 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）

- 経済産業省｜制度構築方針の公表
- IPA｜SCS評価制度の詳細情報
- IPA｜要求事項・評価基準
- IPA｜よくある質問

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