SCS評価制度の★3取得に必要な対策とは？要求事項と準備方法を解説

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）の★3は、一般的なサイバー攻撃に対して、企業が最低限実装すべき基礎的な組織対策とシステム防御策を備えていることを示すための段階です。2026年10月時点では、★3・★4は2027年3月頃の運用開始が予定されています。

結論から言えば、★3取得に向けて最初に行うべきことは、セキュリティ製品を追加購入することではありません。自社のIT基盤と業務範囲を整理し、公開されている★3要求事項・評価基準とのギャップを確認し、不足する対策を実装して、その実施を説明できる証跡をそろえることが重要です。

また、★3は単なる自己チェックではありません。取得希望企業が自己評価を行い、所定の要件を満たすセキュリティ専門家による確認・助言と署名を受け、さらに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。したがって、情報システム部門だけで完結させるのではなく、経営層、管理部門、現場部門を含めた準備が必要になります。

この記事で分かること

・SCS評価制度の★3が求めるセキュリティ水準

・★3取得までの評価スキームと専門家確認の役割

・企業が優先して整備したい組織面・技術面の対策

・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使い分け

・申請前にそろえておきたい資料・証跡と社内体制

・準備期間や費用を左右する要因、支援会社の選び方

SCS評価制度の★3とは

SCS評価制度は、取引先ごとに異なっていたセキュリティ確認を共通化し、サプライチェーンに参加する企業の対策状況を分かりやすく可視化することを目的とした制度です。制度は任意であり、取得しなければ一律に商取引が禁止されるものではありません。ただし、発注企業が契約や調達の中で、取引先に一定の★取得や同等水準の対策を求める活用が想定されています。

★3は、広く認知された脆弱性などを悪用する一般的なサイバー攻撃への対応を想定した水準です。経済産業省は、★3を「全てのサプライチェーン企業が最低限実装すべきセキュリティ対策」と位置付け、基礎的な組織的対策とシステム防御策を中心に実施する段階と説明しています。

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

出典：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）」
https://www.meti.go.jp/policy/netsecurity/scs.html

★3は「専門家確認付き自己評価」

★3の評価主体は取得希望企業自身です。ただし、企業が記入した自己評価について、社内外のセキュリティ専門家が内容を確認し、必要に応じて修正を含む助言を行います。最終的に専門家が提出内容を了承した場合に署名し、企業は経営層による自己適合宣誓を含めて事務局へ提出します。

ここで注意したいのは、単に「社内の情報システム担当者が確認した」だけでは足りない点です。IPAが示す専門家には、情報処理安全確保支援士、公認情報セキュリティ監査人、CISSP、CISA、CISM、ISO27001主任審査員などの資格保持に加え、制度上必要な研修・登録要件が設けられています。

★3取得には全ての要求事項・評価基準への適合が必要

IPAのFAQでは、★3・★4の取得には、それぞれで定められた全ての要求事項・評価基準を満たす必要があると明示されています。「重要な項目だけできていればよい」「一定点数を超えれば取得できる」という考え方ではありません。

そのため、申請直前にチェックリストを埋めるよりも、まず現状を棚卸しし、不適合項目に対して担当者・期限・予算を設定した改善計画を作る方が現実的です。特に従業員100～1,000名規模では、拠点、クラウドサービス、端末、委託先、部門ごとの例外運用が増えやすく、規程だけ整っていて実運用が追いついていないケースに注意が必要です。

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

★3取得で企業が整備したい主な対策

★3の具体的な判定はIPAが公開する要求事項・評価基準に沿って行う必要があります。以下は、公開されている制度方針と一般的な実務を踏まえ、企業が準備時に優先して確認したい領域を整理したものです。実際の申請では必ず最新の公式要求事項・評価基準と照合してください。

1. 経営責任とセキュリティ体制を明確にする

最初に必要なのは、誰がセキュリティ対策を決定し、誰が実行し、インシデント時に誰が判断するかを明確にすることです。情報セキュリティ方針、責任者、担当部門、報告経路が曖昧な状態では、技術対策を導入していても継続的な運用につながりません。

経営層は、★3を単なるIT部門の認証取得業務として扱うのではなく、取引継続、顧客情報保護、事業停止リスクの低減に関わる経営課題として位置付ける必要があります。最終申請には経営層による自己適合宣誓が含まれるため、対策状況を経営会議等で説明できる状態にしておくことが望まれます。

2. 対象となるIT資産を把握する

対策の前提は、守る対象を把握することです。PCやサーバだけではなく、クラウドサービス、ネットワーク機器、VPN、アカウント、外部公開システム、管理者端末なども含めて棚卸しします。誰が管理しているか、どの業務で

使われているか、インターネットからアクセス可能かといった情報も整理すると、その後の優先順位付けがしやすくなります。

SCS評価制度は企業等のIT基盤を主な対象として設計されています。製造設備のOTシステムや、委託元へ提供する製品自体は直接の評価対象とは異なる整理が示されているため、自社の業務範囲と制度対象を混同しないことも重要です。

3. アカウントとアクセス権限を管理する

サイバー攻撃では、盗まれたID・パスワードや過剰な管理者権限が侵入・被害拡大の起点になります。入社・異動・退職時のアカウント管理、管理者権限の限定、不要アカウントの削除、認証強化、リモートアクセスの制御などを確認します。

特に、退職者のアカウントが残っている、共有IDを複数人で使っている、管理者権限が日常業務用PCに付与されているといった運用は、ルールと実態の両面から見直す必要があります。規程だけではなく、アカウント一覧や棚卸し記録を残すことで、実施状況を説明しやすくなります。

4. 脆弱性管理とパッチ適用を仕組み化する

★3が想定する脅威には、広く認知された脆弱性を悪用する一般的な攻撃が含まれます。そのため、OS、ミドルウェア、ネットワーク機器、VPN、Webサーバなどの脆弱性情報を収集し、影響を判断し、更新プログラムや回避策を適用する流れを定めておくことが重要です。

実務では、「重大な脆弱性が公表されたら誰が確認するか」「何日以内に対応方針を決めるか」「業務都合でパッチを当てられない場合に代替策をどう承認するか」まで決めておくと、属人的な対応を減らせます。

5. マルウェア対策、バックアップ、ログ管理を確認する

ランサムウェアや不正プログラムへの備えとして、端末・サーバの防御、メールやWeb経由の感染対策、バックアップ、復旧手順を確認します。バックアップは取得しているだけでは不十分で、復元できることを定期的に確認することが重要です。

また、インシデント発生時には、いつ、どの端末から、どのアカウントで何が行われたかを追跡できるログが必要になります。すべてのログを長期間保存すればよいわけではありませんが、重要システムや管理者操作を中心に、取得対象、保管期間、確認方法を定めることが実務上有効です。

6. インシデント対応手順と連絡体制を整える

セキュリティ対策は、侵入を防ぐ施策だけでは完結しません。感染や不正アクセスが疑われた場合に、初動判断、端末隔離、経営報告、取引先への連絡、外部専門家への相談をどのように行うかを事前に決めておく必要があります。

例えば、取引先から預かったデータを扱うシステムで不審な通信が発生した場合、情報システム部門だけで調査を続けると、報告判断が遅れることがあります。法務、管理、広報、経営層を含む連絡経路と、重大度に応じたエスカレーション基準を用意しておくと、事業継続と信用毀損の双方に対応しやすくなります。

7. 従業員教育と委託先管理を運用に組み込む

フィッシングメール、パスワードの使い回し、機密情報の誤送信など、人を起点としたリスクは技術製品だけでは抑えきれません。入社時教育だけでなく、定期的な教育、注意喚起、必要に応じた標的型メール訓練などを実施し、受講記録を残すことが有効です。

また、クラウド事業者、保守会社、業務委託先など、自社のシステムや情報へアクセスする第三者についても、契約・権限・セキュリティ条件を確認します。取引先管理を「契約書を締結したら終わり」にせず、重要度に応じて継続的に見直すことが重要です。

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は必要か

SCS評価制度は、特定のセキュリティ製品やサービスの導入を一律に義務付ける制度ではありません。そのため、すべての★3取得企業に同じ内容の脆弱性診断やペネトレーションテストが必須になる、と単純に考えるべきではありません。自社のシステム構成、公開範囲、リスク、要求事項への適合状況を踏まえて必要性を判断します。

Webアプリケーション診断

顧客向けWebサービス、会員サイト、管理画面、APIなどを公開している場合は、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・認可の不備などを確認するWebアプリケーション診断が有効です。自社開発だけでなく、外部ベンダーが開発したシステムでも、運用責任を自社が負う場合は診断範囲を検討する価値があります。

プラットフォーム診断

インターネット公開サーバ、VPN装置、ファイアウォール、クラウド上の仮想マシンなどについて、不要なポート、古いソフトウェア、危険な設定、既知の脆弱性を確認するのがプラットフォーム診断です。資産棚卸しと組み合わせることで、外部から攻撃可能な箇所を効率的に把握できます。

ペネトレーションテスト

ペネトレーションテストは、個別の脆弱性の有無だけでなく、複数の弱点を組み合わせた場合に実際に重要情報や管理権限まで到達できるかを検証する手法です。★3取得のために一律実施するというより、重要システムの事業リスクが高い場合や、単純な診断では把握しにくい攻撃経路を確認したい場合に適しています。

★3取得に向けた準備手順

ステップ1：対象範囲と責任者を決める

まず、対象となる組織、拠点、IT基盤、クラウド環境、委託関係を整理し、プロジェクト責任者を決めます。営業部門や製造部門が独自に利用しているクラウドサービスなど、情報システム部門が把握していないITがないかも確認します。

ステップ2：公式要求事項とのギャップ分析を行う

IPAが公開する★3・★4要求事項・評価基準を用いて、現状が適合しているかを確認します。「規程あり」「運用あり」「証跡あり」を分けて評価すると、不足が明確になります。例えば、パッチ適用ルールがあっても実施記録が残っていなければ、証明可能性の面で課題が残ります。

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

ステップ3：不足対策をリスクベースで改善する

ギャップが見つかったら、すべてを同時に実施するのではなく、外部公開システム、管理者権限、重要データ、ランサムウェア対策など、事故時の影響が大きい領域から着手します。改善内容は、担当、期限、必要予算、完了条件を設定し、経営層が進捗を確認できる形にします。

ステップ4：証跡を整備する

自己評価を説明するためには、「実施している」と口頭で説明するだけでなく、実施状況を裏付ける資料が必要です。規程、組織図、資産台帳、アカウント一覧、パッチ適用記録、バックアップ記録、教育記録、インシデント対応手順、委託先管理記録などを整理します。

証跡には個人情報や機密情報が含まれることがあります。外部専門家へ共有する場合は、NDA、アクセス制御、保存場所、削除方法を事前に確認し、必要以上の情報を渡さない運用にします。

ステップ5：セキュリティ専門家による確認を受ける

自己評価がまとまった段階で、制度要件を満たすセキュリティ専門家に確認を依頼します。申請直前に初めて依頼すると、大きな不備が見つかった際に改善期間を確保できません。早い段階でギャップ分析やプレチェックを受け、最終確認までの修正期間を確保する方法が効率的です。

ステップ6：経営層が適合状況を確認し、申請準備を行う

最終的には経営層による自己適合宣誓が必要です。経営層には、技術的な項目をそのまま説明するのではなく、未対応事項の有無、残存リスク、取引先への影響、取得・維持コスト、次年度の改善計画をまとめて説明すると判断しやすくなります。

準備期間と費用を左右する要因

★3取得までの準備期間は、企業規模だけでは決まりません。ISMSやPマーク等を運用していて資産管理・規程・教育・委託先管理の基盤が整っている企業は、既存資料を活用できる可能性があります。一方、拠点やクラウドサービスが多い、アカウント管理が部門ごとに分かれている、脆弱性管理が属人化している場合は、改善に時間を要します。

費用も同様で、申請・登録に関する費用だけでなく、専門家確認、コンサルティング、脆弱性診断、製品・サービス導入、社内工数、規程改定などを含めて考える必要があります。最初から大規模な製品導入を予算化するのではなく、ギャップ分析を行って必要な対策だけを見極めることで、過剰投資を避けやすくなります。

社内稟議で説明すべきポイント

SCS評価制度への対応を稟議に上げる際は、「認証を取るための費用」とだけ説明すると、経営上の優先度が伝わりにくくなります。取引先からのセキュリティ要求への対応、サイバー事故による事業停止や信用毀損の低減、既存統制の標準化、将来の★4取得への基盤整備といった効果を整理すると、投資目的が明確になります。

特に、主要顧客が自社のサプライチェーン管理を強化している場合は、取引先アンケートや監査対応にかかる工数削減、一定水準を客観的に説明できることも経営上のメリットになり得ます。

支援会社を選ぶときのチェックポイント

外部支援を利用する場合は、チェックリストの記入代行だけでなく、現状分析、技術対策、証跡整備、専門家確認への準備、取得後の改善まで一貫して支援できるかを確認します。

見積依頼やRFPでは、支援範囲、対象拠点・システム、成果物、打合せ回数、脆弱性診断の有無、専門家確認との関係、追加費用が発生する条件、機密情報の取扱いを明記すると比較しやすくなります。また、制度上の専門家確認を行える人材と、コンサルティングや技術診断を担当する人材の役割分担も確認しておくと安心です。

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、特定製品の導入を必須とする制度ではありません。現状を確認せずにEDR、資産管理、ログ管理製品などを先に購入すると、既存機能との重複や運用負荷の増加につながることがあります。まず要求事項とのギャップを把握し、運用改善で対応できるものと、技術投資が必要なものを分けることが重要です。

規程だけ整えて実運用を確認しない

ルール上は定期棚卸しを行うことになっていても、実際には半年以上実施されていない、といった差異は珍しくありません。専門家確認を見据えるなら、規程、実運用、証跡の3点が一致しているかを確認する必要があります。

申請直前まで専門家に相談しない

専門家確認で大きな不足が判明すると、技術対策の導入や社内ルールの変更に時間がかかります。制度開始後すぐの取得を目指す場合は、正式申請前に現状評価と改善計画を進めておく方が現実的です。

Librus株式会社が提供できるSCS評価制度★3支援

Librus株式会社では、SCS評価制度への対応を、チェックリスト作成だけで終わらせず、企業ごとの環境と事業上の重要性を踏まえて支援します。現状把握、要求事項とのギャップ分析、改善計画策定、規程・運用整備、脆弱性診断、ペネトレーションテスト、教育、SOC／CSIRT、インシデント対応体制などを必要に応じて組み合わせることが可能です。

また、経営層に必要な判断事項と、情報システム部門が実行すべき技術対策を切り分け、取得のためだけではなく、取引先から説明を求められた際にも継続的に運用できる体制づくりを重視します。既にISMSやPマーク等の仕組みがある場合は、既存の規程・証跡を活かしながら、重複作業を抑える設計を検討します。

よくある質問

Q1. ★3は中小企業だけが対象ですか？

いいえ。SCS評価制度は業種や事業規模を問わず幅広い事業者を対象とする設計です。従業員100～1,000名規模の企業も対象になり得ます。

Q2. ★3を取得しないと取引できなくなりますか？

制度自体は任意です。一律に取引が禁止されるものではありません。ただし、個別の取引契約や調達条件で、発注企業が一定の★取得や同等水準の対策を求める可能性はあります。

Q3. ★3は自己評価だけで取得できますか？

自己評価だけでは完結しません。所定の要件を満たすセキュリティ専門家による確認・助言と署名、経営層による自己適合宣誓が必要です。

Q4. すべての要求事項を満たす必要がありますか？

IPAは、★3取得には★3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説明しています。

Q5. EDRや資産管理ツールは必須ですか？

特定のセキュリティ製品を一律に導入することは求められていません。自社の規模、システム構成、既存対策を踏まえ、要求事項を満たす方法を選択します。

Q6. 脆弱性診断は必須ですか？

すべての企業に同一内容の診断が一律必須とは限りません。ただし、外部公開システムの脆弱性を把握し改善することは、一般的なサイバー攻撃への備えとして有効です。自社の対象範囲と要求事項に照らして必要性を判断します。

Q7. ISMSやPマークがあれば★3対応は不要ですか？

不要とはいえません。既存認証の規程や証跡を活用できる可能性はありますが、SCS評価制度独自の要求事項・評価基準との照合が必要です。

Q8. ★3を取得してからでないと★4を申請できませんか？

いいえ。IPAは、上位段階が下位段階の事項を包含するものの、★3を事前取得しなければ★4を取得できない関係ではないと説明しています。

まとめ｜★3取得は「現状把握→改善→証跡→専門家確認」の順で進める

SCS評価制度の★3は、一般的なサイバー攻撃に備えるために、すべてのサプライチェーン企業が最低限実装すべきセキュリティ対策を可視化する段階です。取得には公開された要求事項・評価基準をすべて満たし、専門家確認付き自己評価と経営層の自己適合宣誓を行う必要があります。

重要なのは、申請書作成から始めるのではなく、自社のIT基盤を把握し、公式要求事項とのギャップを確認し、必要な対策と証跡を整えることです。Webアプリケーション診断やプラットフォーム診断、ペネトレーションテストも、目的と対象を明確にしたうえで活用すれば、技術的な弱点の把握と改善に役立ちます。

2027年3月頃の制度開始を見据える場合、制度開始後に初めて準備するよりも、現在の対策状況を把握し、時間を要する改善から先に進めておく方が、予算・人員・稟議の面でも進めやすくなります。

SCS評価制度★3の準備段階からご相談いただけます

「どこまでが対象になるのか分からない」「要求事項とのギャップを自社だけで判断しにくい」「既存のISMSやPマークの資料をどこまで活用できるか確認したい」といった段階でも、Librus株式会社へご相談いただけます。

Librus株式会社では、対象範囲の整理、現状評価、改善計画、規程・証跡整備、技術診断、取得に向けたプロジェクト推進まで、企業ごとの環境に合わせて支援します。最初から実施方法が決まっていなくても、必要な対策と優先順位を整理することで、過剰な投資を避けながら、取引先への説明や将来の★4対応も見据えたロードマップを検討できます。

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