

SCS評価制度★3とは？ 要求事項と取得に向けた対策を解説

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、一般的なサイバー脅威に対処するために、サプライチェーンを構成する企業が最低限実装すべきセキュリティ対策の水準です。取得では、企業自身が要求事項への適合状況の評価し、その内容をSCSセキュリティ専門家が確認したうえで、経営層による自己適合宣誓を含む申請を行う仕組みが予定されています。

★3への対応で重要なのは、チェックリストを埋めることではありません。情報資産やネットワークを把握し、責任体制、アカウント管理、脆弱性対策、マルウェア対策、取引先との役割分担、インシデント対応などを「実際に運用できる状態」にすることです。制度開始は2027年3月頃が予定されているため、従業員100～1,000名規模の企業では、現状把握と不足対策の洗い出しを先行して進めておくことが現実的です。

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「SCS評価制度」 <https://www.meti.go.jp/policy/netsecurity/scs.html>

この記事で分かること

- SCS評価制度★3の位置付けと、★4との違い
- ★3で求められる代表的な要求事項と実務上の対策
- 取得に向けて経営層・情報システム部門が準備すべきこと
- 申請までの進め方、期間や費用を左右する要因
- 脆弱性診断やペネトレーションテストをどのように活用すべきか
- SCS評価制度対応を支援する会社を選ぶ際の確認ポイント

SCS評価制度★3とは

SCS評価制度は、企業のセキュリティ対策状況を共通の基準で可視化し、委託元と委託先の双方が取引時に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の監督のもと、IPAが制度を運営します。制度では★3、★4を設け、★5については今後具体化される予定です。

★3は「一般的なサイバー脅威に対処しうる水準」とされ、広く認知された脆弱性の悪用、認証情報の窃取、マルウェア感染、不適切なアクセス権限など、企業が日常的に直面し得る脅威への基礎的な防御を重視します。経済産業省の資料では、★3は全てのサプライチェーン企業が最低限実装すべき対策として位置付けられています。

一方、★4では、初期侵入の防御に加えて、侵入後の被害拡大防止、監視・検知、インシデント対応、取引先管理などをより包括的に求めます。★3は専門家確認付きの自己評価、★4は第三者評価と技術検証という点でも違いがあります。なお、★4の取得前に★3取得が必須という仕組みではありません。

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

★3は「製品を買えば取得できる制度」ではない

★3対策というと、EDR、資産管理ツール、多要素認証製品などの導入を先に検討しがちです。しかし、経済産業省は、SCS評価制度の評価基準を達成するために特定のセキュリティ製品の導入を必須としていません。重要なのは、自社の規模やシステム構成に応じて要求事項を満たしているかです。

例えば、アカウント管理であれば「製品を導入していること」ではなく、入社・異動・退職時に権限を付与・変更・削除するルールがあり、不要な権限が残らないよう管理されているかが重要です。脆弱性対策も同様で、単に診断を実施した実績ではなく、対象資産を把握し、更新情報を確認し、必要なパッチを適用する運用まで含めて考える必要があります。

出典：経済産業省「SCS評価制度」 <https://www.meti.go.jp/policy/netsecurity/scs.html>

なぜ今、SCS評価制度★3への対応が必要なのか

SCS評価制度そのものは任意の制度です。ただし、取引先が調達条件や委託先管理の基準として★3を求める可能性があります。制度上の義務と、商取引上求められる条件は別に考える必要があります。経済産業省も、どの段階を契約上の要件とするかは取引当事者間で決めるものと説明しています。

従業員100～1,000名規模の企業では、大手企業のシステム開発、業務委託、製造、物流、BPO、クラウド運用などを担っているケースも多く、自社のセキュリティ事故が取引先の事業に波及する可能性があります。自社の情報漏えいだけでなく、VPNやリモートアクセス環境を経由した侵入、委託元から預かった認証情報の悪用、業務停止による供給遅延などがサプライチェーンリスクになります。

そのため、★3取得の検討は「認証マークを得るための作業」ではなく、取引継続に必要な最低限のセキュリティ水準を整理するプロジェクトとして扱う方が実務的です。営業部門や調達部門が取引先から受け取っているセキュリティチェックシートを集約すると、SCS評価制度への対応が既存の顧客対応負荷を減らすきっかけになる場合もあります。

出典：IPA「SCS評価制度」 <https://www.ipa.go.jp/security/scs/index.html>

SCS評価制度★3で求められる代表的な要求事項

★3・★4の正式な要求事項・評価基準はIPAから公開されています。★3を取得するには、定められた要求事項・評価基準を満たす必要があります。ここでは経営者や担当者が全体像をつかめるよう、★3で特に重要となる対策領域を実務の観点から整理します。

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

1. セキュリティ責任者と方針を明確にする

最初に必要なのは、誰がセキュリティに責任を持つのかを明確にすることです。情報システム部門が実務を担当していても、重大なインシデント対応や予算投入は経営判断を伴います。担当者名、責任範囲、報告経路、経営層へのエスカレーション方法を整理し、情報セキュリティ方針や関連規程に反映します。

実務では、規程が存在していても、退職者IDの削除期限、重要な脆弱性への対応期限、事故発生時の報告先などが曖昧なケースがあります。★3準備では、文書の有無だけでなく、そのルールが日常業務に組み込まれているかまで確認する必要があります。

2. 情報資産とネットワークを一覧化する

守る対象が分からなければ、対策の漏れを把握できません。サーバー、PC、ネットワーク機器、クラウドサービス、SaaS、外部公開システム、リモートアクセス環境などを棚卸しし、管理責任者と用途を明確にします。また、取引先と接続しているネットワークや外部情報システムも把握します。

特に注意したいのが、部署単位で契約したSaaS、保守終了したサーバー、管理者不明の公開IP、過去のプロジェクトで残ったVPNアカウントです。資産管理台帳と実際の環境が一致していない場合、脆弱性対応やアカウント削除の対象から漏れる可能性があります。

3. ID・パスワード・アクセス権限を管理する

不正アクセス対策の基本は、利用者を正しく識別し、必要な人に必要な権限だけを付与することです。アカウント発行、権限変更、退職時の削除、管理者権限の付与、共有IDの利用などについてルールを定めます。パスワードの設定・管理や、システムの重要度に応じた認証強化も確認対象になります。

例えば、退職者のクラウドアカウントが数か月残っていた、管理者権限が異動後も維持されていた、といった状態は実務上のリスクです。人事情報とID管理を連動させ、定期的な棚卸しを行う仕組みにすると、制度対応後も運用しやすくなります。

4. ソフトウェア更新と脆弱性管理を行う

OS、ミドルウェア、VPN機器、ファイアウォール、Webサーバー、業務アプリケーションなどについて、脆弱性情報を確認し、必要なアップデートを適切なタイミングで適用する体制が必要です。不要なソフトウェアを削除することも基礎的な対策に含まれます。

この領域では、Webアプリケーション診断やプラットフォーム診断が有効です。Webアプリケーション診断では、SQLインジェクションや認証・認可の不備などアプリケーション固有の問題を確認します。プラットフォーム診断では、公開サーバーやネットワーク機器の脆弱性、不要なポート、古いソフトウェアなどを確認します。ただし、診断を一度実施するだけでは不十分であり、発見事項の改修、再診断、継続的なパッチ運用につなげることが重要です。

5. マルウェア感染とネットワーク侵入に備える

端末やサーバーのマルウェア対策、内外ネットワーク境界の分離・保護など、侵入を防ぐ基礎的な対策も重要です。メール添付ファイルや偽のログインページから認証情報を盗まれた場合でも、被害が広がりにくい構成にしておく必要があります。

ペネトレーションテストは、実際の攻撃者に近い視点で、複数の弱点を組み合わせた侵入可能性を検証する手法です。★3取得にペネトレーションテストが一律に必須という意味ではありませんが、重要システムや外部公開環境について「設定上の弱点が攻撃経路にならないか」を確認したい場合には有効です。

6. 取引先との役割と機密情報の扱いを明確にする

SCS評価制度では、自社だけでなくサプライチェーン上の関係も重視されます。取引先や委託先とのシステムを接続しているか、どの情報を共有しているか、インシデント発生時に誰が何をするかを整理します。秘密保持契約や業務委託契約に事故時の報告義務が書かれていても、現場担当者が連絡経路を把握していなければ実効性は十分ではありません。

7. インシデント対応手順を整備する

攻撃を100%防ぐことは現実的ではありません。そのため、感染端末の隔離、管理者への報告、取引先への連絡、ログ保全、原因調査、復旧判断などを事前に決めておくことが重要です。最低限の手順書を作るだけでなく、誰が意思決定者なのか、夜間休日の連絡方法、外部専門会社への連絡方法まで整理すると実務で機能しやすくなります。

SCS評価制度★3の取得に向けた具体的な進め方

ステップ1. 適用範囲とプロジェクト責任者を決める

最初に、どの組織・拠点・IT基盤を対象として準備するかを整理します。SCS評価制度は主にインターネットに接続する自社IT基盤を対象としており、一般的にIT基盤に該当しない製造設備などのOTシステムや、委託元へ提供する製品そのものは直接の対象とはしない考え方が示されています。ただし、自社環境とOTが接続している場合などは、境界を機械的に切り分けず、実際の侵入経路を踏まえて確認する必要があります。

出典:経済産業省「SCS評価制度」 <https://www.meti.go.jp/policy/netsecurity/scs.html>

ステップ2. 要求事項に対する現状評価を行う

次に、IPAが公開している★3要求事項・評価基準に沿って、現状を「対応済み」「一部対応」「未対応」「確認が必要」などに分類します。この段階では、担当者へのヒアリングだけで判断せず、規程、設定画面、資産台帳、アカウント一覧、運用記録などの証拠を確認します。

準備しておきたい資料には、情報セキュリティ規程、組織図、情報資産台帳、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、脆弱性対応手順、バックアップ運用資料、インシデント対応手順、委託先管理資料などがあります。資料が存在しない場合は、ゼロから整備するのではなく、現場で既に行っている運用を確認し、必要な形に文書化する方が定着しやすくなります。

ステップ3. 不足項目をリスクと優先度で整理する

未対応項目を一度に解消しようとすると、予算と人的負荷が大きくなります。外部公開システム、管理者権限、既知の重大脆弱性、退職者アカウント、バックアップ不備など、事故に直結しやすい項目から優先します。対応の優先度は、技術的な深刻度だけでなく、停止した場合の売上影響、取引先への波及、個人情報・機密情報の有無も考慮して決めます。

ステップ4. 必要な対策を実装し、証跡を残す

規程を改定しただけでは、実装済みとは言えません。パッチ適用記録、アカウント棚卸し結果、教育実施記録、ログ確認記録、バックアップ復元テスト結果など、運用の証跡を残します。証跡は専門家確認を受ける際にも説明材料になります。

ステップ5. SCSセキュリティ専門家の確認を受ける

★3は専門家確認付き自己評価です。取得希望組織が自己評価を記入し、SCSセキュリティ専門家が内容を確認し、必要に応じて修正や助言を行います。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に申請します。IPAは、SCSセキュリティ専門家の公表を2027年1月頃から予定しています。

出典:IPA「SCSセキュリティ専門家・評価機関」<https://www.ipa.go.jp/security/scs/security-experts-organization/index.html>

実施期間と費用を左右する要因

★3対応に必要な期間は、会社規模だけでは決まりません。既存の規程や資産管理が整っている企業では短期間でギャップを整理できますが、拠点ごとにネットワーク管理が分かれている、クラウド契約が分散している、アカウント管理が手作業であるといった企業では、現状把握だけでも相応の時間が必要です。

実務上は、①対象範囲の決定、②現状評価、③不足対策の実装、④運用実績・証跡の整備、⑤専門家確認、⑥申請という工程に分けてスケジュールを引くと管理しやすくなります。制度開始直前に着手すると、機器更新や社内規程改定、予算承認が間に合わない可能性があるため、次年度予算の策定期間から逆算することが重要です。

IPAが2026年9月18日に公表した料金設定では、★3登録希望組織の登録料は、2028年3月31日まで1年間10,000円、2028年4月1日以降は1年間20,000円とされています。ここで注意したいのは、この金額は制度上の登録料であり、SCSセキュリティ専門家による確認、コンサルティング、システム改修、脆弱性診断などの費用とは別だという点です。

総費用を左右する主な要因は、対象拠点・システム数、既存規程の整備状況、資産棚卸しの難易度、アクセス管理やネットワーク改修の必要性、診断対象の数、専門家支援の範囲です。見積り依頼では「★3取得支援一式」だけで比較せず、現状評価、改善計画、文書作成、技術対策、専門家確認、申請支援のどこまで含まれるかを明確にしましょう。

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

社内稟議で説明すべきポイント

経営層への説明では、「制度対応が必要だから予算が欲しい」という説明だけでは判断しにくくなります。SCS評価制度★3への対応によって、どの経営リスクを下げるのかを具体化することが重要です。

例えば、主要顧客からのセキュリティ要求への対応、取引継続リスクの低減、ランサムウェア等による事業停止リスクの低減、委託元の情報漏えいリスクの低減、セキュリティチェックシート回答の効率化などを整理します。そのうえで、現状の不足項目、対応しない場合の影響、必要予算、完了時期、取得後の運用負荷を示すと、投資判断を行いやすくなります。

また、★3は任意制度であるため、「法律上必須」と説明するのは適切ではありません。主要顧客からの要求状況や、自社がサプライチェーン上で担う役割を踏まえて、必要性を説明することが重要です。

SCS評価制度★3の支援会社を選ぶポイント

制度の説明だけでなく、実装まで支援できるか

要求事項とのギャップを指摘するだけでは、担当者側に「何をどう直すか」という作業が残ります。規程整備、ネットワーク設計、アクセス制御、脆弱性対応、教育、インシデント対応まで、必要に応じて改善支援ができる会社かを確認しましょう。

技術評価とマネジメントの両方を扱えるか

SCS評価制度は、文書だけでも、技術対策だけでも完結しません。例えば「脆弱性管理を行う」という規程があっても、外部公開サーバーに重大な脆弱性が残っていれば実効性に問題があります。反対に、高価なセキュリティ製品を導入していても、責任者や運用手順が曖昧であれば継続性に課題が残ります。

RFPや見積依頼では、制度対応の経験、技術診断の対応範囲、改善後の再確認、専門家確認との役割分担、成果物の内容、個人情報・機密情報の取り扱い、プロジェクト管理方法を確認すると比較しやすくなります。

成果物が取得後の運用に使えるか

成果物は、単なるチェック表だけでなく、適用範囲、要求事項ごとの評価、確認した証跡、不足事項、リスク、改善案、優先度、担当部門、期限を追える形が望まれます。取得後に同じ状態を維持するには、年次のアカウント棚卸し、脆弱性診断、教育、インシデント訓練などを継続計画に落とし込む必要があります。

SCS評価制度★3対応でよくある失敗と注意点

規程作成だけを先行させる

規程が整っていても、現場の運用と一致しなければ実効性はありません。文書を作る前に実態を把握し、既存運用を生かして必要なルールを追加する方が現場に定着しやすくなります。

情報システム部門だけで完結させる

アカウント管理には人事、取引先管理には調達・営業、事故時の対外対応には法務・広報、予算には経営層が関係します。情報システム部門だけで進めると、要求事項は理解できても実装が止まることがあります。初期段階で関係部門を明確にしましょう。

脆弱性診断を「実施したこと」で終わらせる

診断は現状把握の手段です。重要なのは、発見事項を業務影響と悪用可能性で優先順位付けし、改修し、必要に応じて再診断することです。診断報告書を保管するだけでは、セキュリティ水準は改善しません。

制度開始直前まで準備を待つ

★3・★4の運用開始は2027年3月頃が予定されています。システム改修、予算確保、規程改定、証跡の蓄積には時間がかかります。正式申請の直前ではなく、現状評価だけでも早めに行うことが有効です。

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

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、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)への対応について、要求事項の読み合わせだけでなく、企業ごとの環境や取引関係を踏まえた実務設計を支援します。

具体的には、現状のセキュリティ対策と★3要求事項のギャップ整理、情報資産・ネットワーク・クラウド環境の棚卸し、規程・運用手順の整備、改善計画の策定、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、インシデント対応体制の整備、教育・訓練などを組み合わせて支援できます。

SCS評価制度だけを独立したプロジェクトとして考えるのではなく、既存のISMS、取引先監査、IPO準備、M&A、SOC/CSIRT、脆弱性管理などとの重複を整理することで、必要以上に運用を増やさないことも重要です。Librus株式会社は、技術と経営の両面から課題を整理し、経営層、情報システム部門、現場部門の間をつなぎながら、改善・運用まで一気通貫で支援します。

よくある質問

Q1. SCS評価制度★3は取得が義務ですか？

いいえ。制度自体は任意です。ただし、発注企業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、商取引上の必要性を判断することが重要です。

Q2. SCS評価制度★3はいつから申請できますか？

IPAは★3・★4について2027年3月頃の運用開始を予定しています。制度運営基盤の整備状況等により変更される可能性があるため、最新情報はIPA公式サイトで確認してください。

Q3. ★3を取得する前にISMSを取得する必要がありますか？

必須ではありません。SCS評価制度★3・★4は代表的な脅威を踏まえて管理策を定めるベースラインアプローチであり、ISMSとは目的や評価の考え方が異なります。既にISMSを運用している企業は、既存の規程や証跡を活用できる可能性があります。

Q4. EDRや多要素認証製品を導入すれば★3を取得できますか？

特定製品の導入だけで取得できる制度ではありません。要求事項を満たす方法は企業の規模やシステム構成によって異なります。製品導入と同時に、アカウント管理、資産管理、パッチ運用、インシデント対応などの運用も整備する必要があります。

Q5. 脆弱性診断やペネトレーションテストは必須ですか？

★3において、すべての企業に対して特定の診断サービスやペネトレーションテストを一律に必須とする考え方ではありません。ただし、外部公開システムや重要なIT基盤の技術的な弱点を把握するために、Webアプリケーション診断やプラットフォーム診断などが有効な場合があります。

Q6. ★3の登録料はいくらですか？

IPA公表の料金設定では、2028年3月31日まで★3登録料は1年間10,000円、2028年4月1日以降は1年間20,000円です。専門家確認、コンサルティング、診断、システム改修などの費用は別途発生します。

Q7. まだ対象範囲が決まっていなくても準備を始められますか？

始められます。まず、自社の主要なIT基盤、外部公開システム、クラウド利用、取引先との接続状況を整理し、要求事項とのギャップを把握することが有効です。対象範囲は、その結果を見ながら現実的に設計できます。

まとめ | SCS評価制度★3は「取得準備」と「実際の改善」を同時に進める

SCS評価制度★3は、サプライチェーンを構成する企業が、一般的なサイバー脅威に対処するための基礎的なセキュリティ対策を実装していることを示す仕組みです。専門家確認付き自己評価によって取得する制度であり、単なる書類作成ではなく、資産管理、アクセス管理、脆弱性対策、マルウェア対策、取引先管理、インシデント対応などを実際に運用できる状態にすることが重要です。

特に従業員100～1,000名規模の企業では、部門や拠点ごとにIT管理が分散していることも多く、最初の資産棚卸しとギャップ分析がプロジェクトの成否を左右します。2027年3月頃の制度開始を待ってから対策を始めるのではなく、現時点で公開されている要求事項を使って現状評価を行い、予算や改修期間を要する項目から対応を進めると、無理のない準備につながります。

SCS評価制度★3の対象範囲や進め方が決まっていない段階でもご相談いただけます

Librus株式会社では、「自社が★3を目指すべきか判断したい」「要求事項と現状の差を把握したい」「どのシステムまで対象にすべきか整理したい」「脆弱性診断やペネトレーションテストをどこまで行うべきか検討したい」といった初期段階からご相談いただけます。

現状の体制・IT環境・取引先からの要求を整理したうえで、優先度の高い課題と、取得までに必要な対応を具体化します。対象範囲や実施方法が固まっていない場合でも、最初に論点を整理することで、不要なツール導入や過剰な対策を避けながら、社内稟議や予算策定につなげやすくなります。SCS評価制度への対応を、取得のための作業ではなく、取引継続と事業継続に資する改善につなげたい企業はご相談ください。

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>