

取引先から「SCS★3を取得してください」と言われる前に準備すべきこと

取引先からSCS★3の取得を求められた時点で、社内体制や規程、IT資産、証跡を一から整理し始めると、対応期限に間に合わない可能性があります。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、単に申請書へチェックを付ければ取得できる制度ではありません。要求事項・評価基準を満たす対策を実際に行い、その状況を説明できる証拠をそろえ、セキュリティ専門家の確認を受けたうえで、経営層が自己適合を宣誓する仕組みです。

結論からいえば、取引先から正式な要請が来る前に着手すべきなのは「申請作業」ではなく、①適用範囲の整理、②IT資産とアカウントの棚卸し、③規程・運用・証跡の整備、④脆弱性や設定不備の是正、⑤インシデント対応とバックアップの実効性確認、⑥経営層を含む推進体制の構築です。これらはSCS★3への準備であると同時に、日常のサイバーリスク低減にもつながります。

SCS評価制度は2027年3月頃の★3・★4運用開始が予定されています。制度自体は任意ですが、委託元が取引契約等で委託先に必要な★を提示し、その対策状況を確認する利用が想定されています。そのため、法令上の義務ではなくても、取引継続・新規受注・調達要件の観点で対応が必要になる企業は今後増える可能性があります。

出典:IPA「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>

この記事で分かること

- SCS★3が取引先との関係でどのように使われる可能性があるか
- 正式な取得要請を受ける前に準備しておくべき項目
- 経営層・情報システム部門・現場部門それぞれの役割
- 規程だけでなく、運用証跡や技術対策まで必要になる理由
- 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どの場面で活用するか
- 社内稟議、予算化、外部支援会社の選定で確認すべきポイント

SCS評価制度とSCS★3の基本を押さえる

SCS評価制度はサプライチェーンの対策状況を可視化する制度

SCS評価制度は、委託元から見えにくい委託先のセキュリティ対策状況を共通の尺度で確認しやすくするとともに、委託先が複数の取引先から異なるチェックシートを求められる負担を軽減することを狙った制度です。IPAが制度を運営し、経済産業省と内閣官房国家サイバー統括室が監督する枠組みで構築されています。

対象は特定業種だけに限定されていません。IPAは全てのサプライチェーン企業を対象とし、とりわけ対策リソースに限られる中小企業にも活用効果が大きいとしています。従業員100～1,000名規模の企業では、取引先が大企業、重要インフラ事業者、製造業、金融業などである場合、自社が「委託先」「システム運用会社」「開発会社」「業務受託会社」などの立場で要求を受ける場面を想定しておくべきでしょう。

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

★3は「一般的なサイバー脅威に対処しうる水準」

★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に対処しうることを水準としており、基礎的な組織対策とシステム防御策を中心に、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。★4はこれより広く、組織ガバナンス、取引先管理、検知、インシデント対応などを含む包括的な水準です。

★3の評価方法は「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行い、登録されたセキュリティ専門家が内容を確認・助言し、経営層の自己適合宣誓を含む評価結果を事務局へ提出します。IPAのFAQでは、★3取得には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示されています。したがって、「大部分はできているから申請する」というより、不足項目を事前に洗い出し、運用まで定着させる準備が重要です。

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

なぜ「取引先に言われてから」では遅れやすいのか

規程作成よりも、実際の運用と証跡づくりに時間がかかる

セキュリティ評価では、方針や規程が存在することと、実際に運用されていることは別問題です。たとえばアカウント管理規程を作成していても、退職者アカウントが残っている、管理者権限の棚卸し履歴がない、アクセス権の承認記録を保存していないといった状態では、運用実態を説明しにくくなります。

同様に、バックアップを「実施している」だけでは、復元できるか、ランサムウェア感染時にも利用できるか、担当者不在でも復旧手順を実行できるかという実効性までは確認できません。取得要請を受けてから数週間で、規程・設定・記録・教育・訓練を同時に整備するのは現実的でない場合があります。

部門横断での調整が必要になる

SCS★3準備を情報システム部門だけの仕事と考えると、途中で止まりやすくなります。人事部門は入退社や異動に伴う権限管理、総務・法務は委託契約や機密情報管理、購買部門は外部委託先の管理、経営層は方針と予算、人員配置に関与します。クラウドサービスを各部門が独自契約している企業では、SaaSの棚卸しだけでも時間を要します。

取引先から「1～2か月以内に取得方針を回答してほしい」といった相談が来たとき、社内責任者や対象範囲が決まっていなければ、技術対策以前に意思決定で時間を消費します。事前準備の価値は、対策そのものだけでなく、社内の判断速度を上げる点にもあります。

対応が遅れた場合に起こり得る経営上の問題

SCS評価制度自体は任意の制度であり、★3を取得していないことだけを理由に法律違反になるものではありません。一方、経済産業省のFAQでは、★の取得は委託元または委託先との取引契約で決められるものとされています。つまり、実務上重要なのは「制度上の義務か」だけではなく、「自社の主要顧客が調達条件として何を求めるか」です。

出典：経済産業省「SCS評価制度に関するよくあるお問い合わせ」

<https://www.meti.go.jp/press/2025/03/20260327001/20260327001-gr.pdf>

取得や準備が間に合わなければ、取引先から追加のセキュリティ説明を求められたり、是正計画の提出、契約条件の見直し、競合企業との比較で不利になる可能性があります。特に自社が顧客データを預かる、基幹システムへ接続する、システム開発・保守を担う、製造ラインや物流を支えるといった役割を持つ場合、サイバー事故は自社だけでなく取引先の事業継続に影響します。

経営層はSCS★3を「認証を取るためのコスト」とだけ捉えず、売上維持、調達要件への対応、信用毀損リスクの低減、事故時の復旧力向上に関係する経営課題として判断することが重要です。

取引先からSCS★3を求められる前に準備すべき7項目

1. 適用範囲と重要業務を先に整理する

最初に決めるべきなのは、どの会社・拠点・業務・IT基盤を対象にするかです。対象範囲が曖昧なまま規程や診断を始めると、後から対象システムが増え、見積りやスケジュールが崩れます。主要取引先へ提供している業務、預かっている情報、外部接続、クラウド利用、重要な拠点を整理し、「停止すると取引先に影響する業務」から優先順位を付けます。

経営層は、主要顧客・売上・事業継続の観点から対象範囲を判断し、情報システム部門は対象に含まれるサーバ、ネットワーク、クラウド、端末、アプリケーションを具体化します。

2. IT資産・アカウント・外部公開資産を棚卸しする

セキュリティ対策は、守る対象が分からなければ設計できません。PCやサーバだけでなく、VPN装置、ファイアウォール、ルーター、クラウド環境、SaaS、ドメイン、Webサイト、管理画面、開発環境、外部委託先が管理するシステムも含めて整理します。

特に見落としやすいのが、過去案件で作成したテスト環境、利用者の少ない管理画面、旧VPN装置、退職者や委託先のアカウントです。攻撃者は「重要な本番システム」だけを狙うとは限りません。古い機器や公開設定の不備を侵入口として利用し、内部へ移動するケースを想定する必要があります。

3. 規程と運用証跡をセットで整備する

情報セキュリティ基本方針、アカウント管理、端末管理、脆弱性管理、バックアップ、ログ管理、インシデント対応、委託先管理などのルールは、実態に合わせて整備します。既存のISMS規程や社内規程がある企業は、ゼロから作り直すのではなく、SCS★3の要求事項との対応関係を確認する方が効率的です。

同時に、アカウント棚卸し記録、パッチ適用記録、教育受講記録、インシデント訓練記録、バックアップ確認記録、外部委託先の確認記録など、実施を示せる証跡を残す運用へ変えます。「やっているが記録がない」は、評価時の説明負担を増やします。

4. 脆弱性と設定不備を把握し、優先順位を付けて是正する

インターネットからアクセス可能なシステムや重要システムは、設定ミスや既知の脆弱性が放置されていないか確認します。プラットフォーム診断では、サーバ、ネットワーク機器、OS、ミドルウェアなどの脆弱性や不要ポート、危険な設定を確認できます。Webアプリケーション診断では、認証・認可、入力値処理、セッション管理など、Web固有の問題を確認します。

なお、★3の評価スキームは書類確認を中心とする専門家確認付き自己評価であり、★4のような第三者による技術検証そのものが評価スキームとして必須とされているわけではありません。それでも、自社の実装状況を客観的に把握し、重大な弱点を申請前に解消する目的で脆弱性診断を活用する価値があります。ペネトレーションテストは、個別の脆弱性だけでなく、複数の弱点を組み合わせた侵入可能性や影響を検証したい場合に有効です。

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

5. インシデント対応とバックアップを「使える状態」にする

ランサムウェア感染、不正アクセス、情報漏えいなどが発生した際の連絡先、初動責任者、判断基準、取引先への報告経路、外部専門会社への連絡方法を決めておきます。文書を作るだけでなく、机上訓練を行い、「休日に検知した場合」「担当者が不在の場合」などを想定すると実効性を確認できます。

バックアップについては、取得頻度、保存先、世代数、アクセス権、復元手順を確認し、定期的な復元テストを行います。攻撃者が本番環境と同じ権限でバックアップまで削除できる構成では、復旧手段として十分とはいえません。事業継続の観点から、重要システムごとに許容停止時間や復旧優先順位も整理しておく、経営判断につながりやすくなります。

6. 従業員教育と委託先管理を定常業務にする

フィッシングメール、パスワードの使い回し、クラウド共有設定の誤りなど、人の行動を起点とするリスクは技術製品だけでは抑えられません。入社時教育だけでなく、定期教育、注意喚起、標的型メール訓練などを組み合わせ、受講記録も残します。

また、自社が再委託やクラウドサービスを利用している場合、自社だけの対策でサプライチェーンリスクを完結させることはできません。契約時のセキュリティ確認、アクセス権付与、事故時の連絡義務、契約終了時のデータ返却・削除など、外部委託先管理を購買・法務・情報システム部門で連携して運用する必要があります。

7. 経営層が「取得方針・予算・責任者」を決める

★3では経営層による自己適合宣誓が評価プロセスに含まれます。したがって、情報システム担当者が最後に社長印をもらうだけのプロジェクトではありません。どの取引を守るために取得するのか、どの範囲を対象にするのか、是正にどこまで予算を使うのか、残るリスクを誰が受容するのかを経営レベルで判断する必要があります。

推進責任者を定め、情報システム、人事、総務・法務、購買、事業部門を含む体制を作っておくと、正式な取得要請を受けた後の意思決定が速くなります。

実施前に準備しておきたい資料

外部のセキュリティ専門家やコンサルティング会社へ相談する場合、最初から全資料を完璧にそろえる必要はありません。ただし、以下の情報があると現状把握と見積りが進みやすくなります。

- 会社・拠点・主要業務の概要と組織図
- 主要取引先との業務内容、預かる情報、接続関係
- ネットワーク構成図、システム構成図、クラウド利用一覧
- サーバ・端末・ネットワーク機器・SaaS等の資産一覧
- 既存の情報セキュリティ規程、ISMS文書、社内ルール
- アカウント管理、パッチ適用、バックアップ、ログ管理等の運用記録
- 過去の脆弱性診断・監査・セキュリティチェックシートの結果
- インシデント対応手順、緊急連絡網、訓練記録
- 外部委託先・再委託先・主要クラウドサービスの一覧

資料が存在しない場合も、それ自体が現状把握の結果です。まず「何がないか」を明らかにし、要求事項とのギャップを優先順位順に埋めていく方が、形式的な文書を急いで大量に作るより有効です。

SCS★3取得までの進め方

ステップ1: 現状評価とギャップ分析

IPAが公開する★3・★4要求事項・評価基準を基準に、自社の対策状況を確認します。各項目について「規程あり／運用あり／証跡あり」を分けて見ると、文書不足と実装不足を混同せずに整理できます。取得には全ての要求事項・評価基準への適合が求められるため、未対応項目を一覧化し、担当者と期限を決めます。

ステップ2: 是正計画と予算化

ギャップを、短期間で直せる項目、システム改修が必要な項目、社内ルール変更が必要な項目に分類します。緊急度は「攻撃されやすさ」だけでなく、漏えい時の影響、取引先への影響、復旧難易度も含めて判断します。MFA導入、古いVPN機器の更新、EDR導入、バックアップ分離、ログ保存基盤の整備などは費用や調整を要するため、早期に予算化することが重要です。

ステップ3: 運用定着と証跡蓄積

是正した対策は、実施して終わりではありません。月次のアカウント棚卸し、定期的なパッチ管理、教育、バックアップ確認など、継続運用に組み込みます。担当者依存を避け、異動後も同じ水準で運用できるよう、手順と責任分担を明確にします。

ステップ4: 自己評価とセキュリティ専門家による確認

★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記入し、SCS評価制度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含む助言を行い、提出内容を了承した場合に署名します。制度上のセキュリティ専門家には資格・研修等の要件が定められているため、依頼先を選ぶ際は「一般的なセキュリティ資格者」ではなく、制度上登録された専門家かを確認する必要があります。

ステップ5: 経営層の自己適合宣誓と申請

専門家確認後、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、申請内容に問題がなければ台帳へ登録・公開される流れが示されています。運用開始時の申請方法、様式、料金などはIPAの最新案内を必ず確認してください。制度の詳細は運用開始に向けて更新される可能性があるため、古い資料だけで申請準備を完結させないことが重要です。

準備期間と費用を左右する要因

SCS★3準備に必要な期間は、従業員数だけでは決まりません。同じ300名規模でも、単一拠点でSaaS中心の企業と、複数拠点・オンプレミス・製造設備・多数の外部委託先を持つ企業では作業量が大きく異なります。

期間を左右する主な要因は、対象範囲の広さ、IT資産台帳の整備状況、既存規程の有無、ISMS等の既存認証、未是正の脆弱性、クラウド・SaaSの数、外部委託先の数、経営会議や稟議の頻度です。特に機器更改やシステム改修が必要になる場合は、調達期間を含めて計画する必要があります。

費用についても、制度への申請・登録に関する公的な料金だけでなく、専門家確認、コンサルティング、規程整備、脆弱性診断、製品導入、システム改修、教育・訓練などが発生し得ます。見積りでは「★3取得支援一式」という総額だけを見るのではなく、何が含まれるかを分解して確認しましょう。

社内稟議で説明すべきポイント

稟議では「SCS★3取得が必要だから費用がかかる」という説明だけでは、優先順位を上げにくいことがあります。経営者や財務部門には、①主要取引先から将来要求される可能性、②取得準備が遅れた場合の受注・更新への影響、③既存のセキュリティ課題も同時に改善できること、④事故時の停止・漏えい・復旧コストの低減につながること、⑤今回の投資が次回評価や他社チェックシートにも再利用できることを整理して説明すると判断しやすくなります。

また、取得期限が確定していない段階でも「現状評価だけ先に行い、改修費用はギャップ確認後に段階承認する」という進め方が可能です。最初から大規模投資を決裁するのではなく、フェーズを分けることで予算化の不確実性を下げられます。

支援会社を選ぶ際のチェックポイント

SCS★3の支援会社を選ぶ際は、制度説明だけでなく、要求事項を実際のシステム・運用へ落とし込めるかを確認します。RFPや見積依頼では、現状評価、適用範囲設定、規程整備、技術対策、診断、証跡整備、専門家確認前のレビュー、取得後の運用支援のうち、どこまで対応するかを明示すると比較しやすくなります。

また、診断会社とコンサルティング会社を別々に利用する場合、診断結果が「脆弱性一覧」のままで終わり、SCS要求事項や経営リスクとの関係が整理されないことがあります。技術的な問題を、業務影響、是正優先度、必要予算まで翻訳できる支援会社を選ぶと、社内調整が進みやすくなります。

個人情報や機密情報を外部へ共有する可能性もあるため、秘密保持、データ保管場所、アクセス権、再委託、作業終了後のデータ削除、事故時の連絡体制も契約前に確認してください。

よくある失敗と注意点

取得直前に規程だけ大量に作る

規程を整えることは重要ですが、現場で運用できないルールを増やすと、評価後に形骸化します。現在の業務フローを確認し、実施可能な頻度・責任者・記録方法まで決めることが重要です。

対象範囲を広げすぎる、または狭めすぎる

全社の全システムを無条件で対象にすると負担が膨らみます。一方、取引先に影響する重要システムを外すと、取得の目的と合わなくなります。取引関係、情報、接続、業務継続への影響から対象範囲を説明できるようにします。

脆弱性診断を実施して満足する

診断は課題発見の手段です。重要なのは、発見事項をリスクに応じて是正し、再診断や設定確認で改善を確かめ、再発防止の運用へつなげることです。特に「高リスク」と判定された問題は、システム所有部門と経営層で対応期限を合意しておくことと放置を防げます。

Librus株式会社が支援できること

Librus株式会社では、SCS評価制度への対応を「申請書作成だけのプロジェクト」とせず、現状評価から技術対策、改善、運用まで一気通貫で支援します。企業ごとの業務、IT環境、主要取引先との関係を確認したうえで、必要な範囲と優先順位を個別に設計します。

具体的には、SCS★3要求事項とのギャップ分析、対象範囲の整理、規程・運用・証跡の整備、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、インシデント対応体制やSOC／CSIRTの構築・運用、セキュリティ教育などを組み合わせられます。診断結果を提示して終わるのではなく、改善策の優先順位付け、経営層への説明、実施後の再確認まで支援できる点が特徴です。

また、SCS評価制度への対応だけでなく、M&A、IPO、取引先監査などの経営上の重要局面を踏まえて、技術と経営の両面から課題を整理します。情報システム部門と経営層、現場部門の間で認識がずれている場合にも、共通の判断材料を作ることで意思決定を進めやすくします。

よくある質問

Q1. SCS★3は法律上、必ず取得しなければなりませんか？

いいえ。SCS評価制度自体は任意の制度です。ただし、委託元と委託先の取引契約で取得が求められる場合は、実務上の取引条件になる可能性があります。自社の主要顧客や業界でどのように利用されるかを確認することが重要です。

Q2. 取引先からまだ何も言われていません。それでも準備する必要がありますか？

全ての企業が直ちに取得プロジェクトを開始する必要はありません。ただし、主要顧客からセキュリティチェックシートを頻繁に求められる企業、顧客情報を預かる企業、顧客システムに接続する企業は、少なくとも現状評価とギャップ把握を先に行うメリットがあります。

Q3. ISMSを取得していればSCS★3は自動的に取得できますか？

自動的に取得できるわけではありません。既存のISMS規程や運用はSCS対応に活用できる可能性があります。SCS★3の要求事項・評価基準に照らして不足がないかを個別に確認する必要があります。

Q4. SCS★3取得に脆弱性診断は必須ですか？

★3は専門家確認付き自己評価であり、★4の評価スキームで行われる第三者の技術検証と同じ仕組みではありません。ただし、外部公開資産や重要システムの実装上の弱点を客観的に把握するため、Webアプリケーション診断やプラットフォーム診断を実施することは有効です。

Q5. ペネトレーションテストまで実施した方がよいですか？

全ての企業で一律に必要とは限りません。重要システムへの侵入経路や、複数の弱点を組み合わせた場合の事業影響を検証したい場合には有効です。まず資産とリスクを整理し、目的に応じて診断方法を選ぶことが重要です。

Q6. 取得準備は情報システム部門だけで進められますか？

難しいケースが多いです。人事、総務・法務、購買、事業部門、経営層も関係します。特に入退社管理、外部委託、教育、インシデント時の顧客報告、予算判断は部門横断での対応が必要です。

Q7. 取引先から急に取得を求められた場合、最初に何をすべきですか？

まず期限、求められている★、対象となる契約・業務、適用範囲を取引先と確認します。そのうえで要求事項に対する現状評価を行い、短期では正できる項目とシステム改修が必要な項目を分け、現実的な対応計画を作ります。

Q8. 取得後は何もしなくてよいですか？

いいえ。セキュリティ対策は継続運用が前提です。資産や脅威、取引先要件は変化するため、アカウント棚卸し、パッチ管理、教育、バックアップ確認、診断、インシデント訓練などを定期的に見直す必要があります。

まとめ | SCS★3は「要請を受けてから」ではなく、平時の準備が重要

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、一般的なサイバー脅威に対処しうる基礎的なセキュリティ水準を可視化する仕組みです。制度自体は任意でも、取引先が調達・契約上の要件として★取得を求める場面は想定されています。

そのため、正式な依頼を受ける前に、適用範囲、IT資産、規程、運用証跡、脆弱性、バックアップ、インシデント対応、教育、委託先管理、経営責任を整理しておくことが重要です。早めに現状を把握しておけば、取引先から要請を受けた際も、必要な追加対策と費用、スケジュールを具体的に説明できます。

SCS★3対応を「認証取得のためだけの作業」にせず、自社の事業継続と取引先からの信頼を強化する機会として活用することが、結果として最も実務的な進め方です。

SCS★3対応の準備段階からご相談いただけます

Librus株式会社では、「自社がSCS★3の対象になりそうか分からない」「取引先から求められる前に現状だけ確認したい」「要求事項と自社規程の差分を整理したい」「技術対策がどこまで必要か判断できない」といった初期段階からご相談いただけます。

対象範囲や実施方法が決まっていない段階でも、主要取引先との関係、IT環境、既存のセキュリティ対策を確認し、優先順位を整理することで、過剰な対策や重複投資を避けながら現実的な準備計画を作ることが可能です。制度対応に加えて、脆弱性診断、ペネトレーションテスト、インシデント対応、SOC／CSIRT支援、教育などを必要に応じて組み合わせ、改善・運用まで一貫して支援します。

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>