

取引先からSCS評価取得を求められたら？受注を守る対応方法

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への実務対応

取引先から「SCS評価を取得してほしい」と連絡を受けた場合、最初に行うべきことは、回答期限、求められる段階、対象となる契約・拠点・システム、未取得期間中の取扱いを確認することです。そのうえで、要求事項との差分を調べ、受注継続に直結する不足から改善します。申請だけを急いでも、規程・運用・技術対策・証跡が繋がっていなければ評価対応は進みません。

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、取引先ごとに異なりがちなセキュリティ要求を共通の基準で可視化し、サプライチェーン全体の対策水準を高めるための制度です。従業員100～1,000名規模の企業にとっては、情報システム部門だけの認証対応ではなく、営業、法務、総務、人事、経営層を含む「受注を守るプロジェクト」として扱うことが重要です。

この記事で分かること

- 取引先からSCS評価取得を求められた直後に確認すべき事項
- ★3・★4の違いと、自社に求められる段階の考え方
- 要求事項へのギャップ分析、改善、技術検証、証跡整備の進め方
- 期間・費用を左右する要因と、社内稟議・ベンダー選定のポイント
- 取得準備を一過性で終わらせず、受注維持と事業継続につなげる方法

SCS評価制度とは

SCS評価制度は、企業のサプライチェーン上の立ち位置や想定リスクに応じて必要な対策水準を示し、実施状況を段階（★）で可視化する制度です。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、独立行政法人情報処理推進機構（IPA）が運営します。委託元が取引契約などで委託先に適切な段階を提示し、対策の実施を促して確認する利用場面が想定されています。

2026年9月6日時点で、★3・★4は2027年3月頃の運用開始が予定されています。★5の要求事項、評価方法、開始時期は検討中です。また、★3・★4を取得するには、それぞれに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ります。申請方法や申請・登録費用は今後公表予定であり、未確定の費用を確定情報のように予算化しない注意が必要です。

制度の最新情報：[IPA「SCS評価制度」公式サイト](#)／[IPA「よくある質問」](#)

★3と★4は単なる優劣ではなく、想定リスクに応じて選ぶ

制度は企業同士を競わせる格付けを目的とするものではありません。取引先がどの段階を求めているかを確認し、自社の判断だけで低い段階に置き換えないことが基本です。一般に、★3は基礎的な組織対策とシステム防御を確実に行う水準、★4はより高度な組織ガバナンスや継続的改善、第三者評価を伴う水準として準備されます。正式な判断は、IPAが公開する要求事項・評価基準と取引先の指定条件に基づいて行います。

なぜ今、SCS評価取得が取引条件になり得るのか

委託元にとって、委託先の停止や情報漏えいは自社の事業停止、顧客対応、監督責任に波及します。典型例は、保守用アカウントの侵害から委託元環境へ侵入されるケース、受発注システムがランサムウェアで止まり納品できなくなるケース、委託先が保管する設計図・顧客情報が漏えいするケースです。Webサービス企業であれば、脆弱なWebアプリケーションから顧客情報を窃取される経路も考えられます。

従来は発注企業ごとの質問票に回答する運用が中心でした。しかし、質問の粒度や証拠の要求がばらばらだと、委託元は比較しにくく、委託先には回答負担が積み上がります。SCS評価制度は、この非効率を共通基準によって緩和する狙いがあります。したがって今後、調達要件、契約更新、入札参加、取引先監査の確認資料として利用される可能性があります。法令上の一律義務と決めつけるのではなく、個別契約上の要請として重要性を判断すべきです。

対応しなかった場合に起こり得る問題

未取得だけで直ちに取引停止になるとは限りません。問題は、取引先からの要請に対して、責任者も計画もなく「検討中」としか答えられない状態です。調達部門から代替候補との比較材料に使われたり、契約更新時に改善計画や追加保証を求められたりする可能性があります。新規案件では、提案内容や価格が優れていてもセキュリティ条件を満たさず、選定対象から外れるおそれもあります。

さらに、形式的な回答で実態を伴わない場合、事故発生後に説明の整合性が問われます。信用毀損、復旧費用、顧客対応、売上停止が重なるため、SCS評価対応は情報システム予算だけでなく、売上防衛、事業継続、取締役のリスク管理という観点で扱う必要があります。

まず取引先に確認する5つの事項

1. 期限と取引上の位置づけ

回答期限、取得期限、契約更新日を確認します。「推奨」「将来の必須化を検討」「契約条件」「入札参加条件」では緊急度が異なります。取得まで猶予がある場合は、改善ロードマップの提示で取引継続が可能かも協議します。

2. 求められる段階と対象範囲

★3か★4か、全社か特定事業か、国内拠点だけか海外拠点も含むかを明確にします。契約対象サービスに利用するクラウド、データセンター、開発・保守委託先、リモートアクセス環境が範囲に入るかも確認します。

3. 提出を求める証拠

マーク取得だけを求めるのか、申請前の自己評価、改善計画、脆弱性診断報告書、教育実績、インシデント対応体制なども必要かを確認します。報告書の原本提出は機密情報の露出につながるため、要約版、閲覧方式、秘密保持契約の利用も検討します。

4. 未取得期間中の暫定措置

取得予定日、責任者、未達項目、代替統制を記載した計画書で暫定対応できるか確認します。制度開始前であれば、その事実を共有しつつ、要求事項に沿った準備状況を説明するのが現実的です。

5. 再委託先への要求

自社だけが整備しても、重要業務を担う再委託先やSaaS事業者の管理が抜ければリスクは残ります。再委託の許可、事故報告期限、アクセス権管理、契約終了時のデータ削除など、委託先管理の範囲を取引先とそろえます。

SCS評価取得に向けた具体的な対応手順

ステップ1. 経営責任者と推進体制を決める

経営層は、対象事業、目標段階、取得目標時期、許容できる残余リスク、予算枠を決定します。実務責任者を情報システム部門に置く場合でも、規程は総務・法務、教育は人事、委託先管理は購買、顧客説明は営業が担います。部門横断の会議体と意思決定者を先に定めると、改善が停滞しにくくなります。

ステップ2. 必要資料と資産情報を集める

最初に、組織図、情報セキュリティ規程、資産台帳、ネットワーク構成図、アカウント一覧、クラウド・SaaS一覧、委託先一覧、事故対応手順、バックアップ設計、教育記録、過去の診断・監査報告書を集めます。文書があるだけでなく、承認日、最新版、実施記録、対象者、例外処理まで確認します。

ステップ3. 要求事項とのギャップを可視化する

各要求事項について「適合」「一部適合」「未適合」「対象外候補」に分け、根拠資料と責任部門をひも付けます。対象外は自己判断で除外せず、業務やシステム構成から妥当性を説明できるようにします。ギャップ表には、現状、必要な改善、優先度、担当者、期限、概算費用、確認方法を記載します。

ステップ4. 事業影響を基準に改善順位を決める

優先順位は、単に項目数や導入の容易さで決めません。インターネット公開、特権ID、機密情報、停止時の売上影響、既知の脆弱性、攻撃可能性を組み合わせます。たとえば、多要素認証がない管理者アカウント、外部公開機器の重大な脆弱性、復元試験をしていないバックアップは、早期に是正すべき候補です。

ステップ5. 規程・運用・技術対策を一体で改善する

規程だけを作っても運用記録がなければ実効性を示せません。一方、製品を導入しても責任者や監視手順がなければ継続しません。アクセス権の申請・承認・棚卸し、パッチ適用期限、ログ監視、バックアップ復元試験、インシデント連絡網、委託先評価、教育・訓練を、担当と頻度を含めて設計します。

ステップ6. 技術検証で実態を確認する

Webアプリケーション診断は、認証、入力処理、セッション管理などWeb固有の弱点を確認します。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や既知脆弱性を調べます。ペネトレーションテストは、攻撃者の視点で複数の弱点を組み合わせ、重要情報や権限に到達できるかを検証するものです。目的が異なるため、「診断を1回実施した」だけで一律に代替できるわけではありません。対象資産と評価基準に応じて組み合わせます。

ステップ7. 証跡を整え、模擬評価を行う

成果物には、適用範囲、要求事項ごとの判定、判定根拠、参照証跡、未達事項、是正計画、リスク受容の承認記録を含めます。規程、設定画面、ログ、会議議事録、教育受講記録などの証跡は、取

得日と責任者が分かる状態にします。最後に第三者の視点で模擬評価を行い、文書と実態の不一致、説明の属人化、証跡の欠落を洗い出します。

対象範囲の決め方

範囲を狭くすれば安く早くなるとは限りません。共通の認証基盤やネットワークが全社で共有されている場合、特定部署だけを切り出しても依存関係の確認が必要です。反対に、契約対象と無関係な拠点まで含めると負担が膨らみます。まず守るべき取引・情報・サービスを特定し、それを支える人、端末、サーバー、クラウド、委託先、物理拠点をたどって境界を決めます。境界外との接続と責任分界も文書化します。

期間と費用を左右する要因

公式の申請・登録費用は2026年9月6日時点で未公表です。したがって予算は、制度側に支払う費用と、自社の準備・改善に必要な費用を分けて考えます。後者は、対象拠点・システム数、目標段階、既存規程の成熟度、資産台帳の精度、クラウドや委託先の数、技術診断の範囲、製品導入の有無、証跡の不足量によって変動します。

実務上は、初動確認と簡易ギャップ分析、詳細評価、改善、証跡蓄積、評価準備の順に進めます。小規模な範囲でも運用記録を一定期間蓄積する必要があるため、短期集中だけでは完了しない場合があります。取引先の期限から逆算し、まず重大な不足と暫定措置を示し、その後に中期改善を続ける二段階の計画が有効です。

社内稟議で説明すべき内容

稟議では「認証取得費」だけを提示せず、対象取引の売上・粗利、更新時期、未対応時の営業影響、事故時の停止影響、現状の不足、必要な人員と外部費用を説明します。成果を、①取引先への回答、②SCS評価取得準備、③重大リスクの低減、④今後の監査回答の共通化に分けると、投資効果を理解してもらいやすくなります。

また、規程整備や診断で終わらず、改善後の再診断、ログ監視、アカウント棚卸し、教育、インシデント訓練を運用費として見込む必要があります。初年度だけ予算を確保すると、更新時に証跡が不足し、再び突貫対応になりかねません。

支援会社の選び方とRFPで確認する項目

支援会社は、制度の説明だけでなく、要求事項を現場の設定・運用へ落とし込めるかで選びます。RFP（提案依頼書）や見積依頼では、対象範囲、目標段階、期限、既存認証、希望成果物、機密情報の取扱条件を伝え、次の点を確認します。

- ギャップ分析、改善設計、技術検証、証跡整備、評価準備のどこまで含むか
- 要求事項ごとの判定根拠と、対象外判断の考え方を示せるか
- 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目的別に設計できるか
- 発見事項を技術的な深刻度だけでなく、事業影響と期限で優先順位付けするか
- 報告書の再利用権、保管場所、暗号化、再委託、削除方法を明示するか
- 改善後の再確認、継続監視、教育・訓練まで支援できるか
- 制度上の評価機関・専門家としての役割と、取得準備コンサルティングの役割を混同していないか

特に、支援会社が制度上の登録評価機関であるかのような誤認を招く説明には注意が必要です。準備支援と正式評価は役割を切り分け、最新のIPA公表情報で確認します。

よくある失敗と注意点

質問票を埋めることが目的になる

回答を完成させても、設定や運用が伴わなければ証跡確認で止まります。要求事項を業務プロセスへ変換し、誰がいつ何を記録するかまで決めます。

すべてを情報システム部門に任せる

委託先契約、採用・退職、教育、事故広報は情報システム部門だけでは完結しません。経営スポンサーのもとで各部門の責任を明確にします。

診断範囲が資産台帳と一致しない

公開資産の漏れや、開発・検証環境の除外があると、実際の攻撃面を見落とします。資産棚卸しを先に行い、除外理由を残します。

重大度の高い脆弱性だけを直して終わる

個別の脆弱性を修正しても、特権管理、ログ監視、バックアップ、事故対応などの仕組みが弱ければ再発します。技術対策と管理策を同じ改善計画で管理します。

取引先に機密情報を渡しすぎる

構成図や診断報告書は攻撃者に有用な情報を含みます。必要性、閲覧者、保存期間、二次利用、廃棄方法を確認し、必要に応じて要約やマスキングを行います。

Librus株式会社が提供できる支援

Librus株式会社は、SCS評価制度への対応方針整理から、対象範囲の設定、要求事項とのギャップ分析、規程・運用設計、技術的な対策、証跡整備、改善後の確認まで一気通貫で支援します。診断結果を渡して終えるのではなく、経営層、情報システム部門、現場部門の間に立ち、実行可能な改善計画へ落とし込みます。

必要に応じて、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、SOC／CSIRT構築・運用、インシデント対応、デジタルフォレンジック、教育・訓練を組み合わせます。グローバルスタンダードを踏まえながらも、日本企業の稟議、予算、人員、委託構造に合わせて個別設計する点が特徴です。大企業との取引を持つ中堅・中小企業、M&A・IPO・取引先監査など重要局面にある企業にも対応します。

よくある質問

Q1. SCS評価制度への対応は法律上の義務ですか？

制度自体をすべての企業に一律に義務付けるものと捉えるべきではありません。ただし、委託元が契約や調達条件として取得を求める場合、受注・契約更新に実質的な影響が生じます。個別契約と要請文を確認してください。

Q2. ★3と★4のどちらを目指すべきですか？

取引先の指定がある場合は、その段階が出発点です。指定がない場合は、扱う情報、サービス停止の影響、サプライチェーン上の役割、既存対策を踏まえて判断します。単純に企業規模だけでは決まりません。

Q3. 制度開始前でも準備できますか？

可能です。公開済みの要求事項・評価基準を使い、対象範囲の整理、ギャップ分析、重大リスクの改善、証跡の蓄積を始められます。今後公開される解説書や申請方法に合わせて更新します。

Q4. ISO/IEC 27001やプライバシーマークがあれば十分ですか？

既存の管理体制や証跡は活用できますが、SCS評価制度の要求事項を自動的にすべて満たすとは限りません。重複を生かしながら、項目単位で差分を確認します。

Q5. 脆弱性診断は必須ですか？

必要な技術検証は対象システムと要求事項により判断します。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目的が異なるため、リスクと評価範囲に合う手法を選びます。

Q6. 取得までどの程度かかりますか？

一律には決まりません。対象範囲、未達項目、製品導入、社内承認、委託先調整、運用証跡の蓄積期間で変わります。まず短期間のギャップ分析を行い、取引先期限に対する現実的な工程を作ることが重要です。

Q7. 費用はいくらですか？

公的な申請・登録費用は今後公表予定です。準備費用は、対象数、目標段階、診断範囲、規程・運用の成熟度、改善内容によって変わります。範囲と成果物をそろえた見積比較が必要です。

Q8. 取引先への最初の回答はどうすべきですか？

受領した旨を伝え、段階、範囲、期限、契約上の位置づけ、必要証跡を確認します。その後、現状評価の日程、責任者、暫定措置、取得・改善計画の提示日を回答します。根拠なく取得可能と断言しないことが大切です。

まとめ | SCS評価対応は受注を守る経営課題

取引先からSCS評価取得を求められたら、まず要請条件を明確にし、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の要求事項と自社の実態との差を確認します。その後、事業影響の大きいリスクから改善し、規程・運用・技術対策・証跡を一つの計画で整えます。

SCS評価制度への対応は、マーク取得だけが目的ではありません。取引先への説明力を高め、事故による供給停止を減らし、営業部門が安心して案件を提案できる基盤を作る取り組みです。制度の詳細は今後も更新されるため、公式情報を確認しながら、期限に余裕を持って準備を進めることが受注維持につながります。

SCS評価取得の準備段階からご相談いただけます

「取引先から要請が来たが、何を回答すべきか分からない」「★3・★4のどちらが必要か整理できていない」「対象範囲や予算が決まっていない」という段階でもご相談いただけます。Librus株式会社が要請内容と事業影響を整理し、必要なギャップ分析、改善の優先順位、技術検証、社内稟議に使える工程を具体化します。早期に論点を可視化することで、過剰投資を避けながら、取引先への説明と受注継続に必要な準備を進めやすくなります。

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に関する制度構築方針」](#)
- [IPA「SCS評価制度」](#)
- [IPA「要求事項・評価基準」](#)
- [IPA「よくある質問」](#)
- [IPA「関連制度・施策」](#)

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>