SCS評価制度は義務なのか―取得しない企業に起こり得ること

SCS評価制度の★取得は、現時点で民間企業に一律に課された法的義務ではありません。ただし、発注者が取引条件・選定基準・契約更新条件として求めることは想定されており、未取得が受注機会や取引継続に影響する「事実上の要請」へ発展する可能性があります。したがって、法律上の強制の有無だけで判断せず、自社の取引構造と求められる★水準を確認し、取得準備と実質的な対策を並行して進めることが重要です。

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（以下「SCS評価制度」）は、企業のIT基盤におけるセキュリティ対策を共通の基準で評価し、星の段階で可視化する制度です。IPAの公表情報では、★3・★4は2027年3月頃の運用開始が予定されています。本稿は2026年9月3日時点の公表資料に基づき、法的義務と取引上の要請の違い、未取得時のリスク、実務的な準備方法を整理します。

この記事で分かること

- 未取得の場合に想定される取引・経営上の影響
- ★3と★4の違いと、自社が目指す水準の考え方
- 経営層・情報システム部門が今から進める準備

SCS評価制度とは何か

SCS評価制度は、サプライチェーンを構成する企業のセキュリティ対策状況を共通基準で評価・可視化し、委託元と委託先の双方が対策水準を確認しやすくする仕組みです。制度は経済産業省および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。

制度が想定する中心的な場面は、二社間の取引です。発注者が受注者に適切な★水準を提示し、受注者が対策を実施したうえで、その状況を確認できるようにします。従来、発注者ごとに異なる質問票が送られ、受注者が似た質問へ何度も回答することがありました。共通の評価基準が普及すれば、発注者は取引先を評価しやすくなり、受注者も自社の対策状況を説明しやすくなります。

★3と★4の違い

★3は「一般的なサイバー脅威に対処し得る水準」とされ、取得希望企業による自己評価に、登録されたSCSセキュリティ専門家の確認・署名と経営層の自己適合宣誓を組み合わせる仕組みです。★4は、初期侵入の防御だけでなく被害拡大防止や取引先のデータ・システム保護まで含む水準で、評価機関による第三者評価と技術検証が求められます。上位段階は下位段階を包括しますが、★4の取得に★3の先行取得が必須という関係ではありません。

対象は原則として、メールサーバー、Webサーバー、認証基盤、端末、ネットワーク、クラウド環境など企業のIT基盤です。製造設備を制御するOTシステムや、取引先へ提供する製品そのものは基本的に直接対象とせず、別の制度・ガイドラインによる対応が想定されています。ただし、ITとOTの接続点や製品開発環境が企業IT基盤と共通化している場合、境界の整理が欠かせません。

SCS評価制度は義務なのか

法律上、一律の取得義務ではない

2026年9月3日時点の公表資料を見る限り、すべての民間企業に★取得を直接命じ、未取得そのものに罰則を科す法律上の義務として設計されているわけではありません。対象業種や企業規模を限定せず、サプライチェーンに属する幅広い企業が活用できる制度ですが、「制度の対象になり得ること」と「取得が法的に強制されること」は別問題です。

また、個人情報保護法、業法上の安全管理措置、契約上の秘密保持義務など、企業が別途負う法令・契約上の責任はSCS評価制度の取得有無で消えるものではありません。★を取得していなくても必要な安全管理措置は実施しなければならず、反対に★を取得しても、あらゆる法令遵守や事故防止が自動的に保証されるわけではありません。

取引上は「対応必須」になる可能性がある

重要なのは、法的義務と取引上の要請を分けて考えることです。制度は、発注者が取引先に適切な★水準を提示する利用を想定しています。発注者がRFP（提案依頼書）、新規取引の審査、委託先選定、契約更新、重要業務への参画条件などに★取得を組み込めば、受注者にとっては事実上の必須条件となり得ます。

たとえば「★4取得済み、または期限までの取得計画を提出できること」が入札条件になれば、法律による強制がなくても、条件を満たさない企業は比較対象から外れる可能性があります。一方、発注者側も、取引上の立場を利用して一方的に過大な費用負担を押し付けてよいわけではありません。経済産業省と公正取引委員会は、セキュリティ対策の要請と価格交渉を円滑に行うための想定事例を示しています。要請内容、必要性、費用、期限を協議し、契約条件へ明確に落とし込む姿勢が双方に求められます。

SCS評価制度を取得しない企業に起こり得ること

新規案件の候補から外れる

最も現実的な影響は、新規取引の入口で評価されにくくなることです。大手企業が多数の委託先を短期間で選別する場合、共通マークは確認項目を標準化する材料になります。未取得企業が直ちに失格になるとは限りませんが、個別質問票への回答、追加監査、証憑提出が必要になり、営業提案のスピードと比較可能性で不利になるおそれがあります。

既存取引の更新条件が厳しくなる

基幹業務、顧客情報、設計情報、認証情報を扱う委託では、契約更新時にセキュリティ条項が見直されることがあります。未取得のままでは、改善計画の提出、現地監査、診断結果の提示、事故時報告期限の短縮、再委託先管理の強化など、個別条件が追加される可能性があります。対応できなければ、委託範囲の縮小や代替ベンダーへの切替が検討される場合もあります。

質問票・監査対応の負担が残る

SCS評価制度を取得しない場合、自社の安全性を別の証拠で説明する必要があります。ISMS認証、SOC報告書、社内規程、資産台帳、教育記録、脆弱性診断報告書、インシデント対応訓練記録などを取引先ごとに組み直すと、情報システム部門だけでなく営業、法務、総務、内部監査にも作業が波及します。取得コストだけでなく、未取得のまま個別対応を続ける運用コストも比較すべきです。

事故発生時の説明が難しくなる

未取得そのものが事故原因になるわけではありません。しかし、ランサムウェア感染、委託先アカウントの不正利用、Webアプリケーションからの情報漏えいなどが起きた際、経営層は「どの基準で対策水準を判断したか」「既知の不足をなぜ放置したか」を説明する必要があります。公的な共通基準に照らしたギャップ分析や改善記録がなければ、顧客、株主、金融機関、監督官庁への説明が属人的になりやすく、復旧以外の対応負荷が増えます。

予算化が後手に回る

取引先から短い期限で取得を求められてから着手すると、年度予算外の対応になりやすくなります。規程の整備だけでなく、多要素認証、端末管理、バックアップ、ログ管理、脆弱性対応、委託先管理など技術・運用双方の改善が必要になる場合があります。複数部門やクラウド事業者との調整もあるため、単なる申請作業として扱うと期限と予算が合いません。

どの企業が優先して準備すべきか

従業員100名以上の規模では、IT環境が複雑化する一方、専任のセキュリティ人材が限られるケースがあります。特に、次のような企業は早めに発注者の意向と自社ギャップを確認する価値があります。

- 大企業、政府機関、重要インフラ事業者との取引が多い企業
- 顧客情報、設計情報、ソースコード、認証情報などを預かる企業
- クラウドサービス、システム開発、運用保守、BPOを提供する企業
- 重要業務を再委託し、多層のサプライチェーンを構成する企業
- M&A、IPO、大型提携、取引先監査を予定している企業

目標水準は「会社規模」だけで決めません。取扱情報の重要性、システム停止時の影響、外部接続、委託元から受ける権限、代替可能性、発注者の要求を踏まえます。一般的な脅威への備えを対外的に説明したい企業は★3が起点になり得ます。重要なデータやシステムへ深く関与し、技術検証を含む第三者評価が取引上重視される企業は★4を検討します。

取得に向けた具体的な対応手順

1. 経営目的と責任者を決める

最初に「マークを取ること」ではなく、守る事業と取引を決めます。主要顧客からの要求、売上依存度、停止時の損失、機密情報の種類を整理し、目標★、対象組織、希望時期、予算枠を経営会議で合意します。CISOがいない場合でも、経営責任者、実務責任者、各部門の協力者を明確にしてください。★3では経営層による自己適合宣誓が想定されており、情報システム部門だけに任せ切る進め方は適しません。

2. 評価範囲と資産を可視化する

組織、拠点、ネットワーク、クラウド、端末、アカウント、重要データ、委託先を一覧化し、評価範囲を定めます。必要資料の例は、情報セキュリティ方針、組織図、資産台帳、ネットワーク図、アカウント管理台帳、バックアップ設計、ログ保存方針、脆弱性管理記録、教育・訓練記録、インシデント対応手順、委託先管理基準です。文書が存在するだけでなく、実際の運用記録と一致していることが重要です。

3. 要求事項との差分を評価する

IPAが公開する★3・★4の要求事項・評価基準に照らし、「適合」「一部適合」「不適合」「対象外」に分類します。対象外とする場合は根拠を残します。優先順位は、単純な項目数ではなく、事業影響、攻撃可能性、取引期限、改善に要する時間、他施策への波及効果で決めます。認証基盤の多要素認証、外部公開資産、バックアップ復旧、特権IDなど、重大事故につながりやすい領域は先行させるのが実務的です。

4. 技術検証で「実装されているか」を確認する

規程と自己評価だけでは、実装上の弱点を見落とすことがあります。Webアプリケーション診断は、SQLインジェクションや認可不備などアプリ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、クラウド設定などの既知の脆弱性や設定不備を確認します。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、実際にどこまで侵入・権限拡大・情報到達が可能かを検証します。

これらは同じ検査ではありません。評価対象、取引先のリスク、★水準に合わせて組み合わせ、発見事項を要求事項へ紐付けると、診断が単発の技術報告で終わらず、取得準備と経営判断に使える証拠になります。診断時には本番影響、試験時間、禁止事項、連絡体制、個人情報・機密情報の取扱い、ログ保存、再委託の有無を事前に合意します。

5. 改善し、証跡を蓄積する

改善計画には、課題、リスク、担当部門、期限、費用、暫定対策、完了条件、証跡を記載します。技術的な修正が難しい場合でも、アクセス制限、監視強化、手作業の承認など代替策を検討し、残余リスクを経営層が承認します。規程改定、設定変更、教育実施、復旧訓練、委託先契約の見直しは、実施日と結果を残して初めて評価に耐える運用になります。

6. 模擬評価・再診断を行う

申請前に、評価者の視点で証跡の不足、規程と実態の不一致、対象範囲の漏れを確認します。脆弱性を修正した箇所は再診断し、改善済みであることを確かめます。取得後も、組織変更、クラウド移行、新規拠点、M&A、新サービス開始などで前提が変わるため、継続監視、定期診断、教育、インシデント対応訓練へつなげる必要があります。

期間と費用を左右する要因

制度上の申請・登録費用は、2026年9月3日時点で今後公表予定とされています。そのため、現段階で一律の取得費用を断定することはできません。実務上の総費用は、制度への支払額だけでなく、現状調査、コンサルティング、規程整備、ツール導入、設定変更、診断・技術検証、教育、評価対応、再診断を含めて見積もります。

期間は、対象拠点・法人・クラウドの数、資産台帳の精度、既存認証の活用可否、要求事項とのギャップ、経営承認や購買手続、技術改修の難易度に左右されます。規程・証跡が整っていれば数か月単位で準備できる場合がありますが、認証基盤やネットワークの改修を伴えば半年以上の計画が必要になることもあります。正式な申請手順、評価機関、費用の公表時期を確認しつつ、まずギャップ分析と長納期項目の着手を進めるのが安全です。

社内稟議で説明すべきポイント

稟議では「制度対応費」だけを示すと、任意認証への投資と受け取られやすくなります。対象顧客の売上、更新時期、RFPで想定される水準、未対応時の追加監査工数、事故による停止・復旧費用、既存施策との重複を整理し、受注維持と事業継続の投資として説明します。

承認事項は、目標★、対象範囲、責任者、予算上限、実施期限、外部支援の利用範囲、残余リスクの承認方法です。費用は「必須改善」「推奨改善」「中長期改善」に分けると判断しやすくなります。制度要件が更新される可能性も踏まえ、段階的な発注や変更管理を契約に入れることも有効です。

支援会社を選ぶ際の確認事項

SCS評価制度への対応では、チェックリストを埋める能力だけでなく、実装と運用を改善する力が重要です。見積依頼やRFPでは、次の点を確認してください。

- 対象範囲と目標★を決めるギャップ分析に対応できるか
- 要求事項を規程、運用、技術設定、証跡へ具体化できるか
- 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等を適切に使い分けられるか
- 重大度だけでなく事業影響と改修難易度で優先順位を提示できるか
- 改善支援、再診断、教育、継続運用まで一貫して支援できるか
- 評価支援と第三者評価を同一法人が担う場合の中立性・公平性を説明できるか
- 機密情報の保管場所、アクセス権、保存期間、削除、再委託を契約で明確にできるか

成果物には、適用範囲、前提・制約、要求事項別の評価、根拠証跡、技術検証結果、リスク評価、改善優先度、ロードマップ、担当部門、概算費用、残余リスクを含めると、その後の稟議・評価・運用へ転用しやすくなります。単に「未対応」の一覧を受け取るのではなく、経営判断と実装の双方に使えるかを確認しましょう。

よくある失敗と注意点

取得だけを目的にして実態が伴わない

審査直前に文書だけを整えても、設定や運用記録と食い違えば改善は定着しません。★は安全性の絶対保証ではなく、一定時点・一定範囲の対策状況を示すものです。取得プロジェクトを、資産管理や脆弱性管理を平常運用へ組み込む機会として設計する必要があります。

評価範囲を狭くし過ぎる、または広げ過ぎる

負担を減らすために重要システムを不自然に除外すると、取引先が確認したいリスクを説明できません。反対に全法人・全拠点を一度に対象とすると、準備が止まりやすくなります。データと権限の流れを起点に、取引上の説明力と実行可能性のバランスを取ります。

既存認証や診断結果をそのまま代用できると思う

ISMSなどの既存認証や診断は有力な証拠になり得ますが、SCS評価制度の要求事項と評価範囲が同一とは限りません。既存資料を要求事項へマッピングし、不足分だけを追加することで、重複投資を抑えられます。

発注者からの要請を無条件で受ける

受注者は、求められる★水準、対象業務、期限、費用負担、代替的な証明方法を確認してください。発注者も、業務リスクに比して過大な要求とならないようにし、価格・納期を含む協議を行うことが望まれます。セキュリティを一方的な転嫁ではなく、サプライチェーン全体の共同課題として扱うことが継続的な改善につながります。

Librus株式会社が提供できる支援

Librus株式会社は、SCS評価制度に向けた現状評価から、対象範囲の設計、要求事項とのギャップ分析、規程・運用整備、技術検証、改善、再確認までを一気通貫で支援します。企業ごとのIT環境、取引先要請、予算、社内体制を踏まえて個別に設計し、経営層・情報システム部門・現場部門の間で論点を整理します。

制度対応の過程で技術的な確認が必要な場合は、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に応じて組み合わせます。診断結果は改善優先度と事業影響に結び付け、必要に応じてSOC／CSIRT構築・運用、インシデントレスポンス、デジタルフォレンジック、教育・訓練、SBOM導入、M&A時のIT・サイバーセキュリティデューデリジェンスまで継続して支援可能です。

制度の詳細が更新される局面では、確定事項と検討中事項を分け、将来の変更に耐えられる準備を優先します。診断だけで終わらず、改善と運用まで伴走することで、★取得に加え、取引先へ説明できる実質的なセキュリティ体制の構築を目指します。

よくある質問

Q1. SCS評価制度の取得は法律上の義務ですか。

2026年9月3日時点では、すべての民間企業に一律の★取得を課す法律上の義務ではありません。ただし、発注者が取引条件として求めれば、受注のための事実上の要件になる可能性があります。

Q2. 制度はいつ始まりますか。

IPAは★3・★4を2027年3月頃に運用開始する予定と公表しています。今後の正式情報をIPA公式サイトで確認してください。

Q3. 未取得だと直ちに取引停止になりますか。

直ちに取引停止になる制度ではありません。実際の扱いは契約、調達基準、業務リスク、発注者の方針によります。追加監査や改善計画で対応できる場合もあるため、早めに取引先へ確認することが重要です。

Q4. ★3と★4のどちらを目指すべきですか。

取扱情報、システム権限、停止時の影響、顧客要求で判断します。一般的な脅威への対策を示す場合は★3、重要業務に関与し第三者評価・技術検証が重視される場合は★4が候補です。

Q5. ★4の前に★3を取得する必要がありますか。

ありません。上位段階は下位段階の要求を包括しますが、★3の先行取得が★4取得の条件ではないとされています。

Q6. ISMSを取得済みなら対応不要ですか。

対応不要とは限りません。既存の規程・証跡は活用できますが、SCS評価制度の要求事項と対象範囲へマッピングし、差分を確認する必要があります。

Q7. 脆弱性診断だけで★を取得できますか。

脆弱性診断は技術対策を確かめる重要な手段ですが、制度はガバナンス、資産管理、教育、インシデント対応、委託先管理なども含みます。診断だけで全要求を満たすものではありません。

Q8. 費用はいくらですか。

制度上の申請・登録費用は現時点で今後公表予定です。総費用は対象範囲、現状の成熟度、技術改修、診断や評価の内容によって変わります。まずギャップ分析で概算を作るのが適切です。

Q9. 対象範囲が決まっていなくても相談できますか。

可能です。主要取引、重要データ、システム構成、顧客要求から対象候補を整理し、段階的な対応計画を作れます。

まとめ：取引上の必要性で判断する

SCS評価制度は、現時点で全企業に一律の取得を強制する法律上の義務ではありません。しかし、発注者が調達・契約条件として★取得を求める使い方が想定されているため、未取得は新規受注、既存取引、監査対応、事故後の説明に影響し得ます。重要な結論は、「任意制度だから待つ」でも「すべて急いで取得する」でもなく、自社の取引先、扱う情報、事業停止の影響から必要水準と時期を決めることです。

まず主要取引先の意向を確認し、IPAの要求事項に基づくギャップ分析を行い、長納期の改善から着手してください。制度のための書類作成ではなく、実際の攻撃と事業継続に耐える仕組みへつなげることが、取得後も残る投資価値になります。

SCS評価制度への対応方針を整理したい企業の方へ

「自社は★3と★4のどちらを目指すべきか」「顧客から要請される前に何を準備するか」「既存のISMSや診断結果をどう活用するか」といった初期段階からご相談いただけます。Librus株式会社では、対象範囲や実施方法が決まっていない場合でも、取引構造と事業リスクを整理し、優先順位、概算期間、必要な技術検証を具体化します。社内稟議に使える説明材料まで整えることで、過不足のない投資判断につなげます。

診断から改善・継続運用まで一気通貫で支援

SCS評価制度への対応を、書類整備だけで終わらせたくない企業向けに、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、規程・運用改善、教育、継続監視まで支援します。技術と経営の両面から課題を整理し、取得準備と実際のリスク低減を同じロードマップで進められることがメリットです。

参考資料・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）」
- 経済産業省「制度構築方針」（2026年3月27日）
- IPA「SCS評価制度」公式サイト
- 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」
- 経済産業省・公正取引委員会「取引先とのパートナーシップ構築に向けて」関連資料

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