5分で分かるSCS評価制度｜企業が求められる対策

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）で企業に求められるのは、セキュリティ製品を導入することだけではありません。経営責任、情報資産の把握、アクセス制御、脆弱性への対応、インシデント対応、事業継続、委託先管理などを組織として実施し、その事実を証跡で説明できる状態にすることが中心です。

結論からいえば、企業が最初に行うべきことは「どの★を目指すか」よりも、発注元から期待される水準と自社の取引リスクを確認し、評価対象となる組織・IT基盤を定めることです。そのうえで公式の要求事項と現状の差を洗い出し、未達項目を優先順位に沿って改善します。

要点

★3はセキュリティ専門家の確認を伴う自己評価、★4は指定された評価機関による第三者評価と技術検証を求める仕組みです。★5は高度な攻撃への対応を想定していますが、2026年9月3日時点では今後の具体化事項です。上位段階の取得に、下位段階の事前取得が必須という関係ではありません。

この記事で分かること

- SCS評価制度の目的と対象
- ★3・★4・★5の種類と違い
- 企業が準備すべき資料・対策・証跡
- 取得までのやり方と社内体制
- 期間と費用を左右する要因
- 診断・ペネトレーションテストとの関係
- 支援会社への見積依頼で確認すべき事項

SCS評価制度とは

SCS評価制度は、サプライチェーンに参加する企業のセキュリティ対策を段階的に可視化し、発注者と受注者の間のリスクコミュニケーションに活用する制度です。経済産業省と内閣官房国家サイバー統括室が2026年3月に制度構築方針を公表し、独立行政法人情報処理推進機構（IPA）が運営します。制度運用は2026年度末頃の開始が予定されています。

背景には、攻撃者が必ずしも大企業本体を正面から狙うとは限らず、取引先や委託先の認証情報、VPN機器、クラウド設定、保守経路などを足掛かりにする現実があります。受注者側の停止が発注元の生産・物流・顧客対応を止めることもあるため、機密性だけでなく、可用性や完全性、製品・サービスの提供継続も評価上の重要な視点になります。

★3・★4・★5の違い

段階	想定水準	評価方法	実務上の位置づけ
★3	一般的なサイバー脅威に対処し得る水準	取得希望組織の自己評価＋登録されたセキュリティ専門家の確認・助言	基本対策を整え、取引先に説明できる状態を目指す
★4	侵入後の被害拡大防止、取引先のデータ・システム保護、役割に応じた強靭化	指定評価機関による第三者評価＋技術検証	重要情報・重要業務を扱うサプライヤー等で検討
★5	高度な攻撃を想定したリスク管理とベストプラクティス	第三者評価を想定	詳細は今後具体化。現時点で費用・手順を断定しない

★1・★2に相当する初歩的な取組は、IPAの「SECURITY ACTION」が担います。SCS評価制度は既存のISMS適合性評価制度や自工会・部工会ガイドライン等を置き換えるものではなく、相互補完的な活用が想定されています。

なぜ今、企業に必要なのか

取引要件になる前に準備期間を確保するため

制度は法令上すべての企業に一律取得を義務付けるものとして説明されているわけではありません。一方、発注元が取引先に望ましい段階を示し、取得状況を確認する利用が想定されています。つまり、実務上は調達条件、取引継続審査、入札時の

説明資料などを通じて対応が求められる可能性があります。要請を受けてから資産台帳、規程、ログ、バックアップ、訓練記録を一から整えると、商談や更新期限に間に合わないおそれがあります。

セキュリティ投資を経営課題として整理するため

「EDRを導入した」「毎年診断している」といった個別施策だけでは、経営層が残存リスクを判断しにくいものです。SCS評価制度の要求事項を共通の物差しにすれば、未達項目、取引への影響、必要予算、対応期限、責任部署を一つの改善計画にまとめられます。情報システム部門の要望を、売上維持、事業継続、信用、契約履行という経営言語に変換しやすくなります。

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行政処分や取引停止になると断定することはできません。ただし、発注元の調達方針や契約条件によっては、セキュリティ確認への回答負荷が増える、競合比較で不利になる、改善計画や追加説明を求められる、といった影響が考えられます。事故が発生すれば、復旧費用だけでなく、生産・サービス停止、顧客への通知、原因調査、契約上の責任、信用毀損が同時に生じます。

特に注意したいのは「評価を取得していないこと」そのものより、「重要な取引や情報を把握せず、説明可能な管理状態にないこと」です。SCS対応は、顧客アンケートへの回答作業ではなく、経営リスクを継続管理する仕組みづくりとして進める必要があります。

対象となる企業・システム・場面

制度が主に想定する対策実施主体は、二社間契約における受注者側のサプライチェーン企業です。ただし、一社が取引ごとに発注者にも受注者にもなるため、取得側と要請側の双方の役割を持ち得ます。申請主体は原則として法人または個人事業主単位ですが、専門家または評価機関が適用範囲の妥当性を確認したうえで、事業部・グループ単位などとする余地があります。

従業員100～1,000名の企業では、本社ITだけを見て工場、物流拠点、子会社、SaaS、外部保守、業務委託を漏らすことが典型的なリスクです。次の場面に該当する場合は早めの現状評価が有効です。

- 大企業・官公庁・重要インフラ事業者の取引先である
- 顧客の個人情報、設計情報、ソースコード、認証情報を扱う
- 停止すると顧客の生産、物流、決済、保守に影響する
- 複数拠点、工場、海外拠点、グループ会社を抱える
- M&A、IPO、主要契約更新、新規入札を控えている

企業に求められる対策――製品導入より「管理と証拠」が重要

正式な適否判断は、IPAが公開する最新の「★3・★4 要求事項・評価基準」に基づきます。実務では、要求事項を次のような管理テーマに分け、責任者、規程、運用、証跡、未達時の改善期限を紐づけると進めやすくなります。

管理テーマ	確認する内容の例	証跡の例
経営・体制	方針、責任者、会議体、リスク受容、予算	承認済み方針、議事録、組織図、年度計画
資産・情報管理	端末、サーバー、SaaS、重要情報、委託先の把握	資産台帳、データフロー、委託先台帳
ID・アクセス	最小権限、多要素認証、入退社・異動時の変更	権限一覧、申請記録、棚卸記録、設定画面
脆弱性・構成管理	パッチ、公開資産、設定、例外管理	脆弱性一覧、更新記録、診断報告書、是正票
検知・対応	ログ、監視、連絡、封じ込め、報告	ログ設定、アラート記録、対応手順、訓練記録
復旧・事業継続	バックアップ、復元、代替手段、優先業務	復元テスト、BCP、RTO/RPO、訓練結果
委託先・供給網	選定、契約、再委託、定期確認、終了時措置	契約条項、質問票、評価記録、改善依頼

Webアプリケーション診断は、Webサイトや業務アプリの入力・認証・セッション等の弱点を確認する技術検証です。プラットフォーム診断は、OS、ミドルウェア、ネットワーク機器、クラウド設定等の弱点を確認します。ペネトレーションテストは、想定した攻撃シナリオに沿って侵入可能性や到達範囲を検証します。いずれも有用ですが、制度全体は規程、運用、人的対策、復旧、委託先管理まで含むため、診断だけで取得準備が完了するわけではありません。

SCS評価制度に対応するやり方——取得までの7ステップ

1. 経営目的と取引要請を確認する

主要顧客が期待する★、契約更新時期、扱う情報、停止時の影響を整理する。経営層は目標、責任者、予算枠、許容できるリスクを決める。

2. 適用範囲を仮決定する

法人全体、事業部、拠点、グループのどこを含めるかを決める。人、業務、システム、クラウド、委託先、物理拠点の境界を一枚にする。

3. 公式基準でギャップ分析する

各要求事項について、適合・一部適合・未適合・非該当を判定し、根拠資料と責任部署を記録する。非該当には理由が必要になる。

4. 改善計画を作り稟議する

取引・事業継続への影響、緊急度、攻撃可能性、対応工数で優先順位を付ける。短期の設定変更、中期の製品導入、規程改定、教育をロードマップ化する。

5. 対策を実装し運用証跡を蓄積する

規程を作るだけでなく、権限棚卸、パッチ適用、バックアップ復元、インシデント訓練などを実施し、記録を残す。

6. 評価・技術検証に備える

★3では自己評価と専門家確認、★4では評価機関の文書確認、実地審査、技術検証を想定する。対象サンプリングに対応できるよう、拠点間の運用品質を揃える。

7. 申請後も改善を継続する

登録はゴールではない。組織変更、新規SaaS、M&A、重大脆弱性、事故、取引要件変更を契機にリスクと適用範囲を見直す。

実施前に準備したい資料

- 組織図、IT・セキュリティの役割分担表
- 情報セキュリティ方針、関連規程、手順書
- ハードウェア・ソフトウェア・SaaS・アカウントの台帳
- ネットワーク構成図、データフロー、外部接続一覧
- 主要取引・重要業務・重要情報・委託先の一覧
- アクセス権申請・棚卸、パッチ、ログ監視の記録
- バックアップ・復元試験、教育、インシデント訓練の記録
- 過去の監査、脆弱性診断、事故、是正措置の報告書

期間と費用を左右する要因

2026年9月3日時点で、すべての企業に当てはまる一律の取得費用や標準価格は公式には示されていません。費用は「評価・申請に関する費用」と「未達対策を改善する費用」を分けて考えるべきです。後者には、コンサルティング、規程整備、製品導入、診断、ログ監視、教育、運用人員などが含まれます。

変動要因	費用・期間への影響
目標段階	★4は第三者評価と技術検証を伴うため、★3より準備・評価の範囲が広がりやすい
適用範囲	拠点、端末、クラウド、事業部、子会社、委託先が増えるほど確認対象が増える
現状成熟度	台帳・規程・証跡が不足しているほど、評価前の整備期間と工数が増える
技術検証範囲	Webアプリ、外部公開資産、内部ネットワーク、クラウド等の対象数と方式で変動

是正の内容	設定変更で済むか、ネットワーク更改・認証基盤・監視体制の導入が必要かで大きく異なる
社内調整	経営、情シス、人事、法務、調達、現場、子会社の意思決定速度が工程を左右する

期間を見積もる際は、診断や審査の日数だけでなく、ギャップ分析、稟議、調達、実装、運用実績の蓄積、是正確認まで含めます。短期間で書類だけを整える計画は、実地審査や事故発生時に弱さが露呈します。まず4〜8週間程度の準備診断フェーズを置き、その結果から全体工程を精緻化する方法が現実的です。これは制度の公式標準期間ではなく、企業ごとの計画策定に用いる実務上の考え方です。

社内稟議で説明すべき内容

- 背景：主要顧客・業界での要請見込みと制度開始予定
- 目的：認証取得だけでなく、取引維持と事業継続を強化すること
- 対象：組織、拠点、システム、重要業務、委託先の範囲
- 現状：未達項目と、事故・取引への影響
- 費用：評価費、改善費、運用費を分けた予算
- 体制：経営責任者、事務局、各部門の役割
- 成果：登録結果、報告書、改善計画、残存リスク
- 継続：更新、再診断、監視、教育、訓練の年間計画

サービス提供会社の選び方

支援会社は、制度文書の読み替えだけでなく、技術と経営の双方を扱えるかで選びます。★4の正式評価を依頼する場合は、IPAの指定・登録状況と担当範囲を必ず確認してください。準備支援会社と評価機関の役割、独立性、利益相反の扱いも事前に明確にします。

- 公式要求事項に対する適合判断の根拠を説明できる
- 規程作成だけでなく、運用実装と証跡整備まで支援できる
- 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を説明できる
- 経営層向け報告と現場向け改善指示を分けて提供できる
- 機密情報、認証情報、診断データの保管・削除・再委託条件が明確
- 評価後の是正、再確認、SOC／CSIRT、教育まで継続支援できる

RFP・見積依頼時の確認項目

確認項目	見積依頼に記載する内容
目的・段階	取得目的、想定する★、顧客や業界からの要請
適用範囲	法人・事業部・拠点・子会社、対象システム、クラウド、委託先
役務範囲	ギャップ分析、改善支援、文書化、教育、技術検証、申請支援の区分
成果物	評価表、証跡一覧、リスク台帳、改善計画、経営報告書、診断報告書
前提条件	訪問回数、ヒアリング人数、対象IP・URL数、再診断、旅費
情報管理	NDA、保管場所、暗号化、アクセス権、再委託、保持期間、削除証明
品質・体制	責任者の資格・経験、レビュー方法、連絡体制、緊急時対応
追加費用	範囲変更、再評価、是正支援、ツール、ライセンスの扱い

よくある失敗と注意点

既存規程をそのまま証跡だと考える

規程に「定期的に棚卸する」と書いてあっても、実施記録がなければ運用の実効性を示せません。規程、実施記録、例外、是正を一つの証跡体系にします。

情報システム部門だけに任せる

教育は人事、契約は法務・調達、事業継続は各事業部、予算とリスク受容は経営が担います。部門横断の責任分担がなければ、回答は作れても改善が進みません。

対象範囲を狭く見せることを優先する

重要業務の実態と合わない境界設定は、取引先への説明力を損ないます。除外する拠点・システムにも、業務上の依存関係と除外理由を持たせます。

診断を実施して満足する

重大な脆弱性を直しても、退職者アカウント、バックアップ復元、委託先事故連絡などが未整備ならリスクは残ります。診断結果をリスク台帳と改善計画へ接続します。

費用を審査費だけで見積もる

本当に大きくなる可能性があるのは未達対策の実装・運用費です。評価費、改善費、継続運用費の三層で予算化し、優先順位と代替策を経営判断します。

Librus株式会社が提供できる支援

Librus株式会社は、SCS評価制度への対応を単なるチェックシート作成ではなく、取引と事業継続を支えるセキュリティ体制づくりとして支援します。制度要求の整理から技術検証、改善実装、運用まで一気通貫で扱えるため、複数事業者間の引継ぎや論点の分断を抑えられます。

- 経営目的・取引要請を踏まえた目標段階と適用範囲の整理
- ★3・★4要求事項に基づくギャップ分析と証跡一覧化
- 経営層、情報システム部門、現場部門をつなぐ実行計画の策定
- 規程、台帳、手順、委託先管理、インシデント対応の整備
- 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、教育・訓練、再診断による改善定着
- M&A、IPO、取引先監査など重要局面と一体化したリスク整理

グローバルスタンダードを参照しつつ、企業ごとの事業、組織、予算、既存統制に合わせて個別設計します。大企業だけでなく、中堅・中小企業についても、過剰な対策を一律に当てはめず、リスクと優先順位に沿った現実的なロードマップを提示します。

よくある質問

Q1. SCS評価制度はすべての企業に義務ですか？

A. 現時点で、すべての企業に一律取得を義務付ける制度とは公表されていません。ただし、発注元が取引先に望ましい段階を提示し、取得状況を確認する活用が想定されるため、契約・調達上の要請となる可能性があります。

Q2. ★3と★4は何が違いますか？

A. ★3は専門家確認付き自己評価です。★4は指定評価機関による第三者評価に加え、技術検証を求めます。保護する情報や業務の重要性、取引先の要請から選びます。

Q3. ★4の前に★3を取得する必要がありますか？

A. ありません。上位段階は下位段階の事項を包含しますが、★3の事前取得が★4の条件という関係ではないとIPAが説明しています。

Q4. SCS評価制度の費用はいくらですか？

A. 一律料金は公表されていません。目標段階、適用範囲、現状の未達、技術検証の対象、改善内容、拠点数等で変わります。評価費と改善・運用費を分けて見積もることが重要です。

Q5. 取得にはどのくらいの期間がかかりますか？

A. 公式の一律標準期間は示されていません。台帳や規程が整っていても、運用証跡の蓄積と是正には時間が必要です。まず準備診断を行い、顧客の期限から逆算して工程を作ります。

Q6. ISMSを取得していれば対応不要ですか？

A. 対応不要とはいえません。両制度には共通する管理項目がありますが、目的、適用範囲、評価方法が異なります。既存のISMS文書・証跡を再利用し、差分を確認するのが効率的です。

Q7. 脆弱性診断やペネトレーションテストは必須ですか？

A. 必要性と範囲は目標段階、公式基準、対象システム、評価機関の確認に従います。★4では技術検証が求められますが、一般的な診断を一度実施すれば全要求を満たすわけではありません。

Q8. 対象範囲が決まっていなくても相談できますか？

A. 可能です。重要な取引、業務、情報、システム、拠点、委託先の関係を可視化し、評価可能かつ事業実態に合う範囲を決めるところから支援できます。

Q9. 取得後は何をすべきですか？

A. 組織・システム変更の反映、脆弱性管理、ログ監視、教育、インシデント訓練、バックアップ復元試験、委託先確認を継続し、改善状況を経営層へ報告します。

まとめ

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、企業の対策を段階的に可視化し、発注者と受注者の間で信頼できる説明を行うための仕組みです。企業に求められるのは、製品導入や書類作成だけではなく、経営責任、資産把握、技術対策、検知・復旧、委託先管理を継続して運用し、その証拠を示せる状態です。

最初の一歩は、取引上必要な水準と適用範囲を仮決めし、IPAの最新要求事項でギャップ分析を行うことです。制度の詳細は今後も更新されるため、申請直前には必ず公式情報を確認してください。

取引先から要請を受ける前に、現状との差を可視化

既存のISMS、社内規程、脆弱性診断、監視運用を活かしながら、SCS評価制度の要求事項との差分を確認しましょう。Librus株式会社は重複投資を避け、取引期限とリスクに応じた現実的な改善ロードマップをご提案します。

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

出典・一次情報

- 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
- 経済産業省「SCS評価制度に関する制度構築方針」公表ページ（2026年3月27日）：https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html
- IPA「SCS評価制度」公式サイト：https://www.ipa.go.jp/security/scs/index.html
- IPA「SCS評価制度の詳細情報」：https://www.ipa.go.jp/security/scs/details.html
- IPA「要求事項・評価基準」：https://www.ipa.go.jp/security/scs/requirements-criteria.html
- IPA「制度規程・委員会」：https://www.ipa.go.jp/security/scs/regulation-advisory-committeess.html
- IPA「関連制度・施策」：https://www.ipa.go.jp/security/scs/related-regulations-policies.html
- IPA「中小企業の情報セキュリティ対策ガイドライン 第4.0版」：https://www.ipa.go.jp/security/guide/sme/about.html

注：制度は構築・運用準備段階にあり、解説書、評価機関、手続、費用等は更新される可能性があります。公開時および申請時には、上記の経済産業省・IPA公式情報で最新版を確認してください。