

SCS評価制度は義務化される？対象企業・取引先への影響を解説

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）は、法律で全企業に一律の取得を義務付ける制度ではありません。しかし、制度は「委託元が委託先に必要なセキュリティ水準を示し、取引契約等でその実施状況を確認する」ことを想定しており、今後は取引条件や委託先選定の基準として★3・★4の取得を求められる可能性があります。特に、大企業や重要なサプライチェーンにサービスを提供する中堅・中小企業では、「法的義務ではないから様子を見る」よりも、自社がどの取引でどの水準を求められ得るかを早めに整理することが実務上重要です。

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）」
<https://www.meti.go.jp/policy/netsecurity/scs.html>

この記事で分かること

- ・SCS評価制度が法律上の義務なのか、取引上どのような影響が生じるのか
- ・★3・★4の違いと、どのような企業が対応を検討すべきか
- ・制度開始前に経営層・情報システム部門が準備しておくべき事項
- ・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がどこで関係するのか
- ・取得にかかる費用・期間を左右する要因と、支援会社を選ぶ際の確認ポイント

SCS評価制度とは

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の基準で評価し、可視化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が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）が制度運営を担います。★3・★4は2027年3月頃の運用開始が予定されています。

背景には、委託元にとって「取引先が十分な対策をしているか外から判断しづらい」という課題と、委託先にとって「顧客ごとに異なるチェックシートや監査に対応しなければならない」という課題があります。SCS評価制度は、取引先に求める対策水準を段階として示すことで、双方の確認負担を減らしながら、サプライチェーン全体のセキュリティ水準を引き上げることを目的としています。

SCS評価制度は義務化される？結論は「任意だが取引条件になり得る」

結論から言えば、SCS評価制度そのものは任意制度です。経済産業省のFAQでも、★3や★4の取得は必須ではなく、制度として規制を課すものではないと明記されています。したがって、「従業員数が一定以上なら必ず取得しなければならない」といった一律の法的義務ではありません。

一方で、同じFAQでは、★の取得は委託元または委託先との取引契約において決められるものとされています。ここが企業実務で最も重要なポイントです。制度が任意であっても、主要顧客が「重要システムに関わる委託先は★4」「一般的な業務委託先は★3」といった調達基準を定めれば、受注を維持・獲得するために対応が必要になる場合があります。

つまり、経営層が見るべき論点は「国から義務付けられるか」だけではありません。「主要顧客や親会社、元請企業がどのタイミングで取得を求めるか」「未取得のままでも取引継続できるか」「新規入札やRFPで加算・必須条件になるか」を確認する必要があります。

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

対象となる企業は？従業員100～1,000名でも無関係ではない

IPAは、SCS評価制度について「全てのサプライチェーン企業が対象」としています。したがって、製造業だけの制度ではありません。ITサービス、ソフトウェア開発、クラウド運用、BPO、物流、設備保守、人材、専門サービスなど、他社の事業や情報資産に接続する企業は幅広く対象になり得ます。

特に従業員100～1,000名規模の企業では、大手企業の一次・二次委託先として重要業務を担う一方、専任のセキュリティ人員や監査対応体制が十分でないケースもあります。そのため、要求事項を読んだから個別対応するのではなく、既存の規程、資産管理、アカウント管理、ログ、バックアップ、インシデント対応、委託先管理などを横断的に棚卸しすることが効率的です。

取引先から取得を求められやすい場面

たとえば、顧客の基幹システムや個人情報扱う業務、クラウド環境の管理権限を持つ運用業務、製品・サービスの継続提供に直結する外部委託、機密性の高い研究開発情報を扱う業務などは、取引先側か

ら見た影響が大きくなります。こうした場面では、単なる自己申告ではなく、第三者評価や技術検証を含む★4を求める考え方が採られる可能性があります。

逆に、影響範囲が限定的な業務でも、取引先が全委託先に共通基準を適用すれば★3を求められることがあります。自社の業種だけで判断せず、「どの顧客の、どの業務に、どの情報・システムで関与しているか」を基準に考えるべきです。

★3と★4の違い

★3は「専門家確認付きの自己評価」

★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行い、社内外のSCSセキュリティ専門家による確認・助言を受けます。そのうえで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、問題がなければ登録される仕組みです。有効期間は1年とされ、年次で対策状況を点検して更新することが想定されています。

★4は「第三者評価＋技術検証」

★4では、指定された評価機関による第三者評価を受けます。評価には文書確認や実地審査に加え、技術検証が含まれます。IPAは、技術検証事業者の主な対象として脆弱性診断・ペネトレーションテストのサービス提供事業者を挙げています。つまり、規程や手順が整っているだけでなく、実際のIT環境に対して必要な技術的確認を行える状態が求められます。

★4の有効期間は3年で、その間も1年ごとの自己評価が必要です。適用範囲や対策状況に大きな変更があった場合は、改めて評価を受けることが想定されています。大規模なクラウド移行、ネットワーク構成の変更、基幹システム刷新などは、取得後の維持にも影響するため、IT投資計画とSCS対応を別々に管理しないことが重要です。

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

出典:IPA「指定申請について(評価機関・技術検証事業者・研修事業者向け)」
<https://www.ipa.go.jp/security/scs/security-experts-organization/shiteishinsei.html>

対応しない場合に起こり得る問題

未取得であることだけを理由に、自動的に行政処分や罰則が科される制度ではありません。しかし、取引先が★取得を契約条件や調達基準に組み込んだ場合は、別の問題が生じます。たとえば、既存取引の

更新時に追加対応を求められる、新規案件の提案要件を満たせない、監査回答の工数が増える、競合企業との比較で説明力が弱くなる、といった影響です。

さらに、制度への対応準備が不十分な企業では、評価の直前になってアカウント管理台帳が揃わない、バックアップ復旧テストの記録がない、インシデント対応手順はあるが訓練実績がない、委託先の再委託先まで把握できていない、といった事実が判明しやすくなります。これらはSCS対応だけの問題ではなく、実際のサイバー攻撃が発生した際の事業継続や説明責任にも直結します。

経営上は、取得の有無そのものよりも、「重要顧客からの要求に期限内で応えられるか」「不足対策の費用をどの年度予算で確保するか」「重大な不備が見つかったときに事業側と優先順位を決められるか」を事前に整理しておくことが重要です。

制度開始前に企業が進めるべき対応手順

1. まず取引とシステムの関係性を可視化する

最初に行うべきなのは、要求事項を上から順に埋めることではありません。主要顧客、提供サービス、利用システム、保有データ、外部委託先、クラウドサービスの関係性を整理し、「どの取引に事故が起きると誰へ影響するか」を把握します。ここで対象範囲を曖昧にすると、後から評価対象が広がり、追加対応が増えます。

2. 現状と要求事項のギャップを確認する

次に、★3・★4の要求事項・評価基準に対して、現状がどこまで満たしているかを確認します。規程の有無だけでなく、実際に運用されているか、証跡を出せるかまで見る必要があります。たとえば「多要素認証を導入している」と回答しても、特権IDやリモートアクセスの一部が対象外なら、追加対応が必要になる可能性があります。

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

3. 不足をリスクと取引影響で優先順位付けする

すべての不足を同時に解消しようとする、予算も人員も不足します。外部公開システムの重大な脆弱性、管理者権限の不備、復旧できないバックアップ、検知・初動体制の欠如など、侵害時の影響が大きいものから優先します。その際、技術的な深刻度だけでなく、停止した場合の売上影響、顧客への通知義務、契約上の責任、代替手段の有無も合わせて判断すると、経営会議や稟議で説明しやすくなります。

4. 技術検証が必要な領域を早めに洗い出す

★4を見据える場合は、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などの技術検証をどこまで行う必要があるかを早めに整理します。Webアプリケーション診断は、認証・入力処理・権限管理などWebアプリ固有の脆弱性を確認するものです。プラットフォーム診断は、OS、ミドルウェア、ネットワーク機器などの設定や既知脆弱性を確認します。ペネトレーションテストは、想定した攻撃シナリオで侵入可能性や影響を実践的に検証する手法です。

重要なのは、診断を実施したという事実ではなく、「対象範囲が評価対象と一致しているか」「重大な指摘を是正したか」「再診断で改善を確認したか」です。外部公開資産の棚卸しが不十分なまま診断を発注すると、評価対象システムが漏れることがあります。

5. 証跡を残せる運用に変える

評価では、口頭で「やっています」と説明するだけでは不十分です。アクセス権棚卸し記録、教育実施記録、インシデント訓練記録、脆弱性対応履歴、バックアップ・復旧テスト記録、委託先評価記録などを、担当者が変わっても追跡できる形で残す必要があります。SCS対応を一度きりのプロジェクトにせず、月次・四半期・年次の運用サイクルに組み込むことが、更新時の負担を減らします。

準備しておきたい資料と社内体制

情報システム部門だけで完結させようとする、と、規程、委託契約、教育、人事異動、事業継続、個人情報管理などで情報が分断されます。実務では、経営層、情報システム・セキュリティ、法務・総務、人事、購買、事業部門をまたいだ責任分担が必要です。

事前に準備しておきたい資料としては、情報セキュリティ規程・手順書、IT資産台帳、ネットワーク構成図、クラウド利用一覧、アカウント・権限管理台帳、脆弱性管理記録、インシデント対応計画、BCP・バックアップ方針、委託先一覧と契約書、教育・訓練記録、監査結果、過去の診断報告書などがあります。資料があるだけでなく、最新状態に更新されているかも確認します。

経営層は、取得目標の★、対象となる事業・拠点・システム、責任者、改善予算、完了期限を決める役割を担います。特に複数事業を持つ企業では、「全社一括で取るのか」「特定サービスを適用範囲にするのか」で必要な工数が大きく変わるため、最初のスコープ設計が重要です。

費用と期間は何で決まる？

IPAが2026年9月18日に公表した料金設定では、2027年3月以降に受付開始予定の登録希望組織について、2028年3月31日までの登録料は★3が10,000円（1年分）、★4が60,000円（3年分）とされています。2028年4月1日以降は、★3が20,000円（1年分）、★4が60,000円（3年分）です。

ただし、企業が実際に負担する総費用は登録料だけではありません。★3では現状整理や専門家確認の支援費用、★4では評価機関による第三者評価や技術検証の費用、さらに不足対策の導入費用が加わります。自社の環境が複雑であるほど、対象拠点やシステムが多いほど、また証跡が未整備であるほど工数は増えます。

期間も同様です。既にISMS等の管理体系があり、資産管理・権限管理・インシデント対応・委託先管理が運用されている企業と、規程や台帳から整備する企業では準備期間が異なります。制度開始直前に外部支援を探すより、先にギャップ分析だけ実施して「制度開始までに何を直す必要があるか」を把握しておく方が、予算化と社内調整を進めやすくなります。

出典:IPA「SCS評価制度 料金設定のお知らせ」(2026年9月18日)

<https://www.ipa.go.jp/security/scs/rcu1hd00000075om-att/pricelist.pdf>

社内稟議では「認証取得」ではなく「取引継続とリスク低減」で説明する

SCS評価制度への対応を「セキュリティ部門の認証取得プロジェクト」として説明すると、経営層から費用対効果を問われやすくなります。稟議では、主要顧客から取得を求められる可能性、未対応時の受注・更新リスク、既存監査対応の効率化、インシデント発生時の損失低減など、事業上の効果と結び付けて説明することが重要です。

また、予算は「評価費用」と「改善費用」を分けて考えます。評価を受けるための費用を確保しても、診断で重大な脆弱性が見つかり、追加の改修や機器更新が必要になれば、別途予算が必要です。改善費を想定せずに評価日だけ決めると、指摘を解消できないまま期限を迎える可能性があります。

支援会社・評価関連事業者を選ぶ際のポイント

SCS評価制度への対応では、「チェックリストを埋める支援」と「実態を改善する支援」を区別して考えることが大切です。制度要求を読めるだけでなく、ネットワーク、クラウド、Webアプリケーション、ID管理、ロ

グ監視、インシデント対応などの技術面を理解し、経営・法務・購買を含む運用に落とし込める会社が望ましいでしょう。

見積依頼やRFPでは、対応可能な★の範囲、ギャップ分析の方法、技術検証との連携、成果物の内容、指摘事項の優先順位付け、改善支援の有無、再診断の条件、機密情報の取り扱い、担当者の経験を確認します。★4を目指す場合は、制度上の評価機関・技術検証事業者の指定状況も確認が必要です。IPAは評価機関を2026年12月末頃、SCSセキュリティ専門家を2027年1月頃から公表予定としています。

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>

よくある失敗と注意点

制度開始後に要求が来てから動く

取引先から期限付きで取得を求められてから現状確認を始めると、規程改定、システム改修、診断、再診断、社内承認が重なります。少なくとも主要顧客との契約更新時期と、2027年3月頃の制度開始予定を並べて、先に対応順を決めておく安全です。

適用範囲を広く取りすぎる、または狭く取りすぎる

対象範囲を必要以上に広げるとコストが膨らみます。一方、取引先に提供する重要サービスのシステムが対象外になっていれば、取得しても説明力が不足します。組織図ではなく、顧客へのサービス提供経路と情報・システムのつながりから範囲を決めることが重要です。

診断を「実施済み」で終わらせる

脆弱性診断やペネトレーションテストで問題が見つかった後、改修・再検証まで完了しなければリスクは残ります。特に外部公開サービスの重大な脆弱性は、SCS対応のためだけでなく事業継続上も優先して是正すべきです。

個人情報・機密情報の取り扱いを確認しない

評価支援や技術検証では、構成図、脆弱性情報、管理者権限、ログなど機密性の高い情報を外部へ共有する場合があります。秘密保持契約、データの保管場所、アクセス権、再委託、削除方法まで事前に確認しましょう。

Librus株式会社が提供できるSCS評価制度対応支援

Librus株式会社では、SCS評価制度への対応を「申請書類の作成」だけで終わらせず、現状把握、リスク整理、技術検証、改善、運用まで一気通貫で支援します。企業ごとの環境や取引条件に応じて、必要な範囲を個別に設計できることが特徴です。

具体的には、★3・★4を見据えたギャップ分析、要求事項に対応する規程・運用の整備、情報セキュリティ体制の構築、リスクアセスメント、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・運用支援、インシデントレスポンス、デジタルフォレンジック、教育・訓練などを組み合わせて支援できます。

制度対応では、技術部門だけに負荷を集中させないことも重要です。Librus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、現場部門の橋渡しを行います。M&A、IPO、取引先監査など、短期間でセキュリティの説明責任が高まる局面も含め、優先順位を付けて対応計画を設計します。

よくある質問

SCS評価制度は法律で義務化されますか？

現時点では任意制度であり、制度自体が全企業に取得を義務付けるものではありません。ただし、取引先が契約・調達条件として★取得を求める可能性があるため、取引上は実質的に必要となるケースがあります。

中小企業も対象ですか？

はい。IPAは全てのサプライチェーン企業を対象としています。特に大企業の委託先や重要なサービスを提供する企業では、企業規模にかかわらず対応を求められる可能性があります。

★3と★4はどちらを目指せばよいですか？

取引先から求められる水準と、自社が担う業務の重要性で判断します。★3は専門家確認付き自己評価、★4は第三者評価と技術検証を伴います。主要顧客の調達方針が未定の場合は、まず現状のギャップを把握し、どちらにも移行できる準備を進める方法があります。

SCS評価制度はいつ始まりますか？

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の公式サイトで確認してください。

登録料はいくらですか？

2026年9月18日公表の料金設定では、2028年3月31日までの登録料は★3が10,000円(1年分)、★4が60,000円(3年分)です。ただし、専門家支援、第三者評価、技術検証、改善対応などの費用は別途発生します。

脆弱性診断を実施していれば★4を取得できますか？

脆弱性診断だけで十分とは限りません。★4は要求事項全体に対する第三者評価と技術検証を伴うため、組織的な管理策、運用記録、インシデント対応、委託先管理なども含めて適合状況を確認する必要があります。

ISMSを取得済みなら対応は不要ですか？

既存の管理体系や証跡はSCS対応に活用できますが、SCS評価制度の要求事項・評価基準に対する確認は別途必要です。既存制度との重複を整理し、不足部分だけを補う進め方が効率的です。

制度の対象範囲がまだ決まっていなくても相談できますか？

可能です。むしろ、対象範囲の決定前に取引・システム・データの関係を整理することで、過大なスコープや対象漏れを避けやすくなります。

まとめ:SCS評価制度は任意でも、取引上の重要性は高まる

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、現時点で法律上の一律義務ではありません。しかし、委託元が委託先に必要な★を提示し、取引契約等で対策状況を確認する運用が想定されています。今後、主要顧客の調達基準や委託先管理の中で取得が求められれば、任意制度であっても事業上の対応優先度は高くなります。

重要なのは、制度開始を待つことなく、自社の取引先、重要サービス、IT資産、現在の対策と証跡を整理し、「要求された場合にどの程度の期間と費用が必要か」を把握しておくことです。特に★4を視野に

入れる場合は、文書整備だけでなく、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などの技術検証と、その後の改善まで計画に含める必要があります。

SCS評価制度への対応方針が決まっていない段階でもご相談いただけます

「取引先から求められる★がまだ分からない」「どこまでを評価対象にすべきか決められない」「現在の規程や技術対策で何が不足しているか知りたい」といった段階でも、対応準備を始めることはできます。

Librus株式会社では、現状のヒアリングとギャップ整理から、対象範囲の設計、改善計画、脆弱性診断・ペネトレーションテスト、運用体制の整備まで、企業ごとの状況に合わせて支援します。早い段階で不足と優先順位を可視化することで、取引先から要請を受けた後の突発的な対応を減らし、予算化や社内稟議を進めやすくなります。

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>

公的情報の確認先

SCS評価制度は運用開始に向けて規程・手続・評価機関等の情報が順次更新されています。公開前には、経済産業省およびIPAの最新情報を確認してください。

出典：経済産業省 SCS評価制度特設ページ <https://www.meti.go.jp/policy/netsecurity/scs.html>

出典:IPA SCS評価制度公式ページ <https://www.ipa.go.jp/security/scs/index.html>