SCS評価制度は義務化される？対象企業・取引先からの要求・未対応リスクを解説

結論から言うと、2026年10月22日時点で、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・★4取得は、法律によって一律に義務付けられているものではありません。経済産業省も、SCS評価制度を「任意の制度」と明記しています。

一方で、実務上は「任意だから対応不要」とは言い切れません。SCS評価制度は、発注企業が取引先に対して必要なセキュリティ水準を示し、契約や調達の場面で実施状況を確認することを想定しています。つまり、法令上の義務ではなくても、取引先から★3や★4の取得・同等対策を求められる可能性があります。

特に、製造業、ITサービス、SaaS、システム開発、業務委託、重要なデータを扱う企業など、他社の事業継続に影響を与え得る企業では、早めに自社の対応状況を把握し、必要な改善を進めることが重要です。

この記事で分かること

・SCS評価制度は法的に義務化されているのか

・どのような企業が対象になり得るのか

・取引先から★3・★4を求められる可能性がある場面

・未対応のままにした場合に起こり得る事業上のリスク

・取引先から要請される前に準備しておくべき事項

・Librus株式会社が支援できる範囲

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・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、IPA（独立行政法人情報処理推進機構）が制度を運営します。★3と★4は2027年3月頃の運用開始が予定されています。

制度の背景には、発注企業から見て「取引先のセキュリティ水準が外部から分かりにくい」という問題と、受注企業から見て「取引先ごとに異なるセキュリティチェックへ対応しなければならない」という問題があります。SCS評価制度は、共通基準によって双方の確認負担を軽減し、サプライチェーン全体の対策水準を引き上げることを狙っています。

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

出典：IPA「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.ipa.go.jp/security/scs/index.html

SCS評価制度は義務化される？現在の公式見解

2026年10月時点では「任意制度」

経済産業省のFAQでは、★3・★4の取得は必須ではなく、SCS評価制度そのものが規制を課す制度ではないと明示されています。したがって、「SCSを取得していない企業は営業できない」「未取得企業は一律に入札できない」といった説明は正確ではありません。

さらに経済産業省は2026年4月、SCS評価制度を引き合いに「今すぐ取得しないと商取引が規制される」「入札から除外される」とする不適切な勧誘への注意喚起を公表しています。制度対応を検討する際は、IPA・経済産業省の公式情報を基準に判断する必要があります。

出典：経済産業省「SCS評価制度に関する注意喚起」
https://www.meti.go.jp/policy/netsecurity/20260427_scs.html

ただし、取引契約上の要件になる可能性はある

重要なのは、制度が任意であることと、個別取引で取得を求められないことは別問題だという点です。制度は、2社間の取引契約などで、発注企業が受注企業に適切な★を提示し、その対策の実施を促し、実施状況を確認する使い方を想定しています。

たとえば、大手企業が重要なシステムの運用を外部委託している場合、委託先で侵害が起きれば発注企業のサービス停止や情報漏えいにつながります。このため、調達条件や更新条件、委託先管理基準の一部として「SCS★3取得」「★4相当の対策」といった要求が置かれることは十分に考えられます。

なお、取得を契約条件としてどのように扱うかは当事者間で合意すべきであり、独占禁止法や取適法にも配慮した適切な運用が求められます。経済産業省と公正取引委員会は、発注側がSCS評価制度に基づく対策を要請する際の価格交渉やパートナーシップの考え方も整理しています。

出典：経済産業省「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」 https://www.meti.go.jp/policy/netsecurity/partnership2.html

公共調達での活用は「今後検討」

経済産業省のFAQでは、政府機関や重要インフラ事業者などにおける調達でSCS評価制度を活用することについて「今後検討」とされています。したがって、2026年10月時点で公共事業の一律の入札要件になったと断定するのは適切ではありません。ただし、将来的な調達・制度連携の動向は継続的に確認する必要があります。

SCS評価制度の対象企業は？中小企業だけではない

SCS評価制度は、特定業種や中小企業だけを対象にした制度ではありません。IPAは、業種・事業規模を問わず幅広い事業者が対象になり得ることを示しています。従業員100～1,000名規模の企業でも、サプライチェーン上の役割や扱う情報、接続関係によっては重要な対象となります。

特に早めに検討したい企業

・大企業や重要インフラ事業者の取引先になっている企業

・顧客データ、個人情報、設計情報、営業秘密を預かる企業

・クラウド、SaaS、ネットワーク、システム運用などを提供する企業

・リモート保守やVPN、API連携などで取引先環境へ接続する企業

・製造、物流、医療、金融など事業停止の影響が大きい業界のサプライヤー

・M&A、IPO、大型案件への参入、取引先監査を予定している企業

判断基準は「会社規模」よりも「侵害された場合に取引先へどこまで影響が波及するか」です。自社が攻撃者の踏み台になった場合、顧客企業のシステムや情報へ到達できる構造になっていないかを確認する必要があります。

未対応の場合に起こり得る4つのリスク

1. 新規取引・契約更新で説明できない

取引先からSCS★3・★4、あるいは同等のセキュリティ対策を求められた際、自社の現状、対象範囲、証跡、改善計画を説明できなければ、回答に時間がかかります。契約締結や更新のスケジュールが厳しい案件では、この遅れそのものが営業上の不利になる可能性があります。

2. 短期間での追加投資が必要になる

対策を求められてから準備を始めると、規程整備、資産棚卸し、アクセス権の見直し、バックアップ改善、ログ監視、教育、脆弱性対応などを短期間に同時進行しなければなりません。結果として、通常の年度予算や調達計画では吸収しにくい追加費用が発生しやすくなります。

3. セキュリティ事故が取引停止・信用毀損につながる

サプライチェーン攻撃では、自社だけでなく顧客企業へ被害が波及します。侵害を受けた企業が取引先ネットワークへの入口となれば、インシデント対応費用だけでなく、顧客説明、契約上の責任、サービス停止、信用低下など経営への影響が広がります。SCS対応は単なる認証取得ではなく、こうした事業リスクを減らす取り組みとして位置付けることが重要です。

4.「取得だけ」を急ぐと運用が定着しない

文書やルールだけを短期間で整備しても、実際の運用が伴わなければ継続的なリスク低減にはつながりません。★3は有効期間1年を想定し、年次で対策状況を確認する設計です。★4も有効期間内に年次自己評価を行う想定であり、一度取得して終わりではありません。

出典：経済産業省「SCS評価制度 制度構築方針」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/20260327_report.html

★3・★4のどちらを目指すべきか

項目	★3	★4
想定水準	一般的なサイバー脅威に対処し得る水準	初期侵入だけでなく被害拡大防止・取引先保護まで含む、より高い水準
評価方法	セキュリティ専門家の確認付き自己評価	評価機関による第三者評価
確認内容	主に書類確認	文書確認に加え実地審査・技術検証
有効期間の想定	1年	3年（年次自己評価あり）
向きやすいケース	まず共通基準で自社の対策を示したい企業	重要システム・重要データを扱い取引先への影響が大きい企業

★3を先に取得しなければ★4を取得できない制度ではありません。自社の顧客要求、サプライチェーン上の重要性、対象システム、事業継続への影響を踏まえて水準を決める必要があります。

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

取引先から求められる前に準備すべきこと

1. 対象範囲を整理する

最初に行うべきは、SCS対応を会社全体で考えるのか、特定事業・拠点・IT基盤を中心に考えるのかを整理することです。顧客との接続点、重要データ、クラウド環境、リモートアクセス、委託先などを洗い出し、「どの範囲が侵害されると取引先へ影響するか」を明確にします。

2. 現状と要求事項のギャップを把握する

IPAが公開する★3・★4の要求事項・評価基準を基に、現状の規程・技術対策・運用・証跡を照合します。重要なのは「対策を実施しているつもり」ではなく、第三者や専門家に説明できる根拠があるかです。

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

3. 技術面の実装状況を確認する

規程が整っていても、インターネット公開システムに未修正の脆弱性が残っていたり、不要なポートが公開されていたり、多要素認証が未導入だったりすれば、実際のリスクは残ります。Webアプリケーション診断やプラットフォーム診断は、こうした実装上の弱点を把握する有効な手段です。

さらに重要システムでは、攻撃者が複数の弱点を組み合わせてどこまで侵入・権限昇格・横展開できるかを確認するペネトレーションテストも検討できます。ただし、個別の診断やテストを実施するだけでSCS取得が保証されるわけではありません。制度要求との対応関係を整理して活用する必要があります。

4. 証跡を残せる運用にする

SCS対応では、規程そのものだけでなく、実際に運用されていることを示せる状態が重要です。アクセス権棚卸し記録、教育受講記録、バックアップ試験、脆弱性対応履歴、ログ確認、インシデント訓練、委託先評価などを継続して残す仕組みを整えます。

5. 経営層が優先順位と予算を判断する

情報システム部門だけで全対策を完結させるのは現実的ではありません。購買、法務、人事、事業部、内部監査など複数部門にまたがるため、経営層が「どの取引を守るための投資か」「未対応時にどの売上・事業継続リスクがあるか」を理解し、優先順位を決める必要があります。

社内稟議では何を説明すべきか

SCS対応を「新しい認証費用」とだけ説明すると、投資判断が難しくなります。稟議では、主要顧客との取引継続、将来の調達要件への備え、サプライチェーン事故の低減、複数顧客からのセキュリティ質問への対応効率化といった事業上の効果を整理すると説明しやすくなります。

・主要取引先から現在求められているセキュリティ要件

・今後SCS★3・★4を求められる可能性がある顧客・案件

・現状のギャップと重大なリスク

・対応しない場合に想定される契約・売上・事業継続への影響

・規程整備、技術対策、診断、教育などに必要な予算

・対応スケジュールと担当部門

費用と期間を左右する要因

SCS対応に必要な費用や期間は、企業規模だけでは決まりません。対象範囲、既存のISMSやセキュリティ体制、クラウド・拠点数、端末数、委託先数、現在の脆弱性管理や監視体制、必要な診断・改善の量などによって変わります。

制度への申請・登録費用だけでなく、ギャップ分析、文書整備、技術対策、専門家確認、第三者評価、技術検証、再診断などを含めた総コストで考えることが重要です。2026年10月時点でも制度詳細は更新が続いているため、最新のIPA公表情報を確認しながら予算化してください。

支援会社を選ぶ際のチェックポイント

SCS対応では、制度文書を読めるだけでなく、現場のシステムや運用へ落とし込める支援会社を選ぶことが重要です。特に、評価対応だけを切り離すのではなく、ギャップ分析から技術改善、証跡整備、診断、運用定着まで支援できるかを確認してください。

・SCS評価制度の最新要求事項・評価基準を把握しているか

・経営・規程・技術の三層でギャップを整理できるか

・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まで対応できるか

・発見した課題を重要度と事業影響で優先順位付けできるか

・機密情報や個人情報の取扱いルールが明確か

・評価・取得後の継続運用や再評価まで支援できるか

よくある失敗と注意点

「まだ任意だから」と準備を先送りする

制度が任意であっても、主要取引先が調達条件として求める時期は企業ごとに異なります。要請後にゼロから準備すると、営業案件のスケジュールに間に合わない可能性があります。

ツール導入だけで対応できると考える

SCS評価制度は特定製品の導入を必須としていません。EDRや資産管理製品を導入していても、権限管理、委託先管理、教育、インシデント対応、証跡などが不足していれば全体として十分とは限りません。

制度取得を目的化する

取得自体を最終目標にすると、現場に負担だけが残りやすくなります。顧客への説明力向上、事故リスク低減、監査対応の標準化など、事業上の成果につなげる設計が重要です。

Librus株式会社が提供できる支援

Librus株式会社では、SCS評価制度への対応を、単なる申請準備や文書整備だけでなく、企業の実際のリスク低減につなげる観点から支援します。

現状評価と要求事項のギャップ分析から、適用範囲の整理、経営層向けのリスク整理、規程・運用の改善、脆弱性診断、プラットフォーム診断、ペネトレーションテスト、SOC／CSIRT、インシデントレスポンス、教育まで、一気通貫で組み合わせることが可能です。

特に「★3と★4のどちらを目指すべきか分からない」「取引先からまだ正式な依頼はないが先に準備したい」「診断結果をSCS対応の改善計画に結び付けたい」といった段階でも、事業・システム・取引関係を踏まえて優先順位を整理できます。

よくある質問

Q1. SCS評価制度は法律で義務化されていますか？

いいえ。2026年10月22日時点では任意制度です。ただし、個別の取引契約や調達条件として取引先から取得・対応を求められる可能性はあります。

Q2. SCSを取得していないと取引できなくなりますか？

制度そのものが一律に取引を禁止するものではありません。どの水準を契約条件とするかは当事者間の合意によります。

Q3. 公共事業の入札では必須ですか？

現時点で一律の必須要件ではありません。政府機関や重要インフラ事業者等の調達での活用は今後検討するとされています。

Q4. 中小企業だけが対象ですか？

いいえ。業種・事業規模を問わず幅広い事業者が対象になり得ます。

Q5. ISMSを取得していればSCSは不要ですか？

同一制度ではありません。経済産業省は相互補完的な制度と位置付けています。既存のISMS運用はSCS対応の基盤として活用できる可能性があります。

Q6. セキュリティ製品を導入すれば取得できますか？

特定製品の導入だけで取得できる制度ではありません。要求事項・評価基準全体を満たす必要があります。

Q7. Webアプリケーション診断やペネトレーションテストは必須ですか？

すべての企業に一律で同じ診断が必須とは限りません。対象システムや要求水準に応じて、技術的な弱点を確認する手段として検討します。★4では技術検証を含む評価が想定されています。

Q8. いつから準備すべきですか？

主要取引先から要請される前に、対象範囲の整理とギャップ分析を始めることを推奨します。規程や技術対策の改善には時間がかかるためです。

まとめ｜SCS評価制度は「任意」でも、取引上の重要性は高まる可能性がある

SCS評価制度は、2026年10月22日時点では法令による一律の義務制度ではありません。しかし、制度は発注企業と受注企業の取引において必要なセキュリティ水準を共有する仕組みとして設計されており、今後、取引先から★3・★4取得や同等レベルの対策を求められる企業は増える可能性があります。

そのため、「義務化されたら対応する」のではなく、自社がサプライチェーンの中でどのような役割を担い、侵害時にどの取引先へ影響を与えるのかを先に整理することが重要です。現状とのギャップを把握し、経営上の重要度に応じて規程・運用・技術対策を改善しておけば、取引先から要請を受けた際にも対応しやすくなります。

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

「主要取引先からSCSについて聞かれ始めた」「★3と★4のどちらを想定すべきか判断できない」「自社のどこが不足しているか分からない」といった段階では、まず対象範囲と現状の整理から始めることが有効です。

Librus株式会社では、SCS評価制度の要求事項と自社の事業・システム環境を照合し、優先的に改善すべき課題を整理できます。制度対応だけでなく、脆弱性診断、ペネトレーションテスト、体制整備、運用改善まで一気通貫で検討することで、過剰投資を避けながら、取引継続と実際のセキュリティ強化の両立を目指せます。対象範囲や実施方法、予算がまだ決まっていない段階でもご相談いただけます。

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