

SCS評価制度に未対応だと取引できない？企業間取引への影響を解説

結論から言えば、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）に対応していないからといって、制度上ただちに取引が禁止されるわけではありません。SCS評価制度は任意の制度であり、★3・★4の取得を一律に義務付ける規制ではないためです。

ただし、企業間取引では事情が異なります。発注企業が自社のリスク管理方針に基づき、取引先に一定のセキュリティ水準や★取得を求め、それを新規取引・契約更新・委託範囲拡大の条件とすることは想定されています。つまり、SCS評価制度そのものが取引を止めるのではなく、「取引先の調達基準」が変わることで、未対応企業が商談や契約の場面で不利になる可能性があります。

特に、製造業、金融、流通、重要インフラ関連など、サプライチェーン上の結び付きが強く、停止や情報漏えいの影響が大きい業界では、セキュリティ対策の説明責任が今まで以上に重くなると考えられます。本記事では、SCS評価制度と企業間取引の関係、未対応時に起こり得る影響、発注側・受注側それぞれが準備すべき事項を実務の観点から解説します。

この記事で分かること

- SCS評価制度に未対応でも直ちに取引禁止になるわけではない理由
- 発注企業が★3・★4を取引条件として求める可能性
- 新規取引、契約更新、取引先監査で起こり得る変化
- 従業員100～1,000名規模の企業が今から準備すべき実務
- 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どのように位置付けるか
- 社内稟議やベンダー選定で確認すべきポイント

SCS評価制度とは何か

SCS評価制度は「取引先に説明できるセキュリティ水準」を可視化する制度

SCS評価制度は、企業が実施しているサイバーセキュリティ対策を共通の基準で評価し、その結果を登録・公表する仕組みです。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示し、IPAが制度運営を担います。★3と★4は2026年度末頃、すなわち2027年1～3月頃の申請受付開始が予定されています。

制度の背景には、発注企業から見ると「取引先のセキュリティ対策が十分か外部から判断しにくい」、受注企業から見ると「複数の取引先から異なるチェックシートや対策を求められる」という双方の課題があります。SCS評価制度は、こうしたばらつきを減らし、取引先の重要度に応じて必要な対策レベルを伝えやすくすることを目的としています。

★3と★4の違い

★3は、一般的なサイバー攻撃への対処を念頭に、基礎的な組織対策やシステム防御を整備する水準です。取得希望企業による自己評価に、SCSセキュリティ専門家の確認を加える方式が想定されています。

★4は、供給停止によってサプライチェーンに大きな影響を与える企業や、重要な機密情報を扱う企業などを念頭に、より包括的な対策を求める水準です。組織ガバナンス、取引先管理、検知、インシデント対応などに加え、第三者評価と技術検証が行われます。重要なのは、会社規模だけで★3・★4が決まるわけではなく、取引上の役割や扱う情報、停止時の影響を踏まえて必要水準を判断する点です。

SCS評価制度に対応しないと取引できなくなるのか

制度上は「未取得＝取引禁止」ではない

経済産業省のFAQでは、SCS評価制度は任意の制度であり、★3・★4の取得を制度として強制するものではないことが明記されています。そのため、「SCS評価制度が始まったら、取得していない会社は法律上取引できない」という理解は正確ではありません。

一方で、★の取得を契約条件として扱うかどうかは、委託元と委託先など、契約当事者間で決められます。ここが経営上の重要ポイントです。制度そのものは任意でも、取引先が必要水準として指定すれば、個別の商取引では実質的な要件になる可能性があります。

発注企業がセキュリティ対策を取引条件とすることは想定されている

経済産業省と公正取引委員会は、発注企業が取引先にサイバーセキュリティ対策の実施を要請することについて考え方を整理しています。一定のセキュリティ対策を実施していることを取引条件とすること自体が、直ちに独占禁止法上問題となるものではないとされています。

さらに、SCS評価制度の★4相当の対策を発注企業が取引先に求め、必要なコストについて価格交渉を行う想定事例も公表されています。つまり制度設計の段階から、SCS評価制度が企業間の調達条件・契約条件・取引先評価に利用されることが想定されています。

公共調達や重要インフラでの活用も検討対象

経済産業省は、政府調達や重要インフラ事業者等での活用推進を掲げています。ただし、2026年10月時点で、SCS評価制度が一律に公共事業の入札要件になると決まっているわけではありません。公的調達・重要インフラ・大手企業のサプライチェーンでどのように使われるかは、今後の運用を確認する必要があります。

したがって、現時点で必要なのは「取得しないと全取引が停止する」と過度に捉えることなく、自社の主要顧客や業界でSCS評価制度がどの程度調達基準に組み込まれそうかを確認することです。

未対応企業に起こり得る企業間取引への影響

新規取引の候補から外れる可能性

新規取引では、営業提案の前後に情報セキュリティチェックシート、委託先審査、ISMS取得状況、インシデント対応体制などを確認されることがあります。SCS評価制度が普及すれば、発注企業が「★3取得済み」「★4取得済み」などを取引先選定の判断材料に加える可能性があります。

同じ価格・品質・納期の候補が複数ある場合、セキュリティ対策を客観的に説明できる企業が選ばれやすくなることは十分考えられます。これは制度上の強制ではなく、購買・リスク管理の評価項目が変化するという意味です。

契約更新時に追加条件を求められる可能性

既存取引でも安心とは限りません。契約更新、委託範囲の拡大、個人情報や機密情報の追加共有、クラウド接続、拠点間接続などを契機に、取引先審査が再実施されることがあります。

その際、「次回更新までに★3相当の対策を整備する」「一定期間内に★取得を目指す」といった改善計画を求められる可能性があります。契約期間が長期にわたる場合、必要な★を維持し続ける運用も考えられると経済産業省は説明しています。

セキュリティ質問票への回答だけでは足りなくなる可能性

従来は、取引先から送られてきたExcelの質問票に「はい／いいえ」で回答すれば審査が完了するケースもありました。しかし、SCS評価制度では、対策が実際に運用されているか、技術的な防御が有効かといった実態が重視されます。

規程に「脆弱性管理を実施する」と書いていても、インターネット公開サーバに古いソフトウェアが残っている、管理者アカウントに多要素認証が設定されていない、ログを取得しているだけで監視していない、といった状態では、実務上のリスクは残ります。

事故発生時に取引継続の判断が厳しくなる

ランサムウェア感染、顧客情報の漏えい、認証情報の窃取などが発生すると、復旧費用だけでなく、取引先への報告、委託停止、再発防止策の提示などが必要になります。特に、自社が踏み台となって取引先へ攻撃が波及した場合や、委託されたデータが漏えいした場合は、信用への影響も大きくなります。

SCS評価制度への対応は事故を完全に防ぐ保証ではありませんが、経営層が責任を持って対策を整備し、その実施状況を説明できる状態を作ることにつながります。

どの企業が特に早く準備すべきか

大手企業のサプライチェーンに入っている企業

自動車、半導体、電機、化学、物流など、サプライチェーンが多層化している業界では、自社の障害が上位企業の生産やサービス提供に影響する場合があります。一次請けだけでなく、二次・三次の取引先でも、重要部品、専門技術、データ処理などを担っている企業は、早めに対応状況を整理する価値があります。

顧客の機密情報・個人情報を扱う企業

システム開発、BPO、コールセンター、士業、コンサルティング、マーケティング支援など、顧客データを預かる企業も注意が必要です。自社システムが停止しなくても、取引先の営業秘密や個人情報が漏れれば大きな影響が生じます。

取引先ネットワークやクラウド環境に接続する企業

VPN、リモート保守、API、クラウド連携、アカウント連携などで取引先環境と技術的につながる企業は、侵入経路として悪用されるリスクがあります。境界装置や公開サーバだけでなく、ID管理、端末管理、権限設計、ログ監視まで含めた確認が必要です。

M&A、IPO、重要顧客との大型契約を控える企業

M&AのデューデリジェンスやIPO準備では、情報セキュリティ体制が経営管理上の論点になります。また、大型案件では、契約前に詳細なセキュリティ審査を受けることもあります。SCS評価制度を契機に体制を整備しておくことで、こうした重要局面で説明しやすくなります。

企業が今から準備すべき実務手順

1. 主要取引先と自社のサプライチェーン上の役割を整理する

まず、どの取引を守るべきかを明確にします。売上規模だけでなく、「停止すると顧客業務にどれだけ影響するか」「どの機密情報を預かっているか」「取引先システムへの接続権限があるか」を確認します。経営層は、★取得を単なる情報システム部門の課題ではなく、主要顧客との取引継続リスクとして捉える必要があります。

2. SCS評価制度の要求事項と現状のギャップを確認する

情報セキュリティ規程、組織図、資産台帳、アカウント管理、脆弱性管理、バックアップ、ログ監視、インシデント対応、委託先管理、教育記録などを整理し、要求事項に対して現在どこまで対応できているかを確認します。

重要なのは、文書があるかどうかだけでなく、実際に運用されているかを確認することです。例えば、退職者アカウントの削除ルールがあっても、実際に無効化が遅れていれば改善が必要です。

3. 技術面の弱点を診断する

外部公開システムや重要システムについては、Webアプリケーション診断、プラットフォーム診断、必要に応じたペネトレーションテストを活用し、技術的な弱点を把握します。

Webアプリケーション診断では、認証、アクセス制御、入力値処理などWeb固有の脆弱性を確認します。プラットフォーム診断では、サーバ、ネットワーク機器、クラウド設定、公開ポートなどを確認します。ペネトレーションテストは、実際の攻撃者に近い視点で複数の弱点を組み合わせ、重要資産に到達できるかを検証する手法です。

すべての企業が同じ診断を実施すべきではありません。対象システムの重要度、インターネット公開の有無、扱う情報、顧客との接続形態を踏まえ、必要な検証を選ぶことが重要です。

4. 課題を「経営リスク」で優先順位付けする

脆弱性の深刻度だけで優先順位を決めると、事業への影響が見えにくくなります。改善順序は、攻撃の容易さ、悪用された場合の影響、対象資産の重要度、取引先への波及、修正コストなどを総合して決めます。

例えば、公開サーバの重大な脆弱性、多要素認証がない特権アカウント、復旧確認をしていないバックアップなどは、事業継続や取引先への影響が大きいため、優先度を高くする判断が考えられます。

5. 改善計画と予算を経営会議・稟議に乗せる

社内稟議では「SCS評価制度に対応するため」という説明だけでは、投資判断が難しくなります。主要顧客からの要求可能性、取引停止・受注機会損失のリスク、事故時の事業停止、必要な改善項目、対応しない場合の残存リスクを整理して説明すると、経営判断につながりやすくなります。

また、規程整備、EDR・MFA等の導入、診断、教育、ログ監視などを一度に実施できない場合は、2027年の制度開始を見据えて段階的なロードマップを作ります。

6. 取引先から問い合わせを受けた際の回答体制を整える

SCS評価制度の取得前であっても、「現在どこまで対応しているか」「いつまでに何を改善するか」を説明できる企業は、取引先との協議を進めやすくなります。営業、法務、情報システム、経営企画が別々に回答すると内容が食い違うため、セキュリティ質問票や監査対応の窓口を明確にしておくことが有効です。

実施期間と費用を左右する要因

取得そのものより、事前改善に時間がかかるケースが多い

SCS評価制度の準備期間は企業ごとに大きく異なります。規程や資産管理が整っており、MFA、バックアップ、ログ監視、脆弱性管理などが既に運用されている企業は比較的進めやすい一方、IT資産の棚卸しから必要な企業では準備に時間がかかります。

特に複数拠点、グループ会社、オンプレミスとクラウドが混在する環境では、対象範囲を整理するだけでも一定の工数が必要です。制度開始直前に着手するのではなく、まずギャップ分析を行い、改善が必要な項目を予算化するのが現実的です。

費用は対象範囲と不足対策の数で変わる

費用を左右するのは、申請・登録料だけではありません。規程整備、コンサルティング、セキュリティ製品導入、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、教育、監視運用など、現状とのギャップに応じて必要な費用が変わります。

そのため、見積依頼では「SCS評価制度対応一式」だけで比較するのではなく、現状調査、適用範囲設定、ギャップ分析、改善支援、診断、申請支援、評価後の是正支援がどこまで含まれるかを確認することが重要です。

SCS評価制度の支援会社を選ぶポイント

制度だけでなく技術対策まで理解しているか

要求事項の解説だけでは、実際の脆弱性や設定不備を解消できません。Web、ネットワーク、クラウド、ID管理、ログ監視など技術領域まで確認できる支援会社を選ぶと、文書と実態の乖離を減らしやすくなります。

改善後の運用まで支援できるか

評価取得はゴールではありません。アカウント棚卸し、脆弱性管理、教育、バックアップ確認、インシデント訓練などは継続的な運用が必要です。取得時だけ支援するのか、改善・運用・再評価まで支援できるのかを確認します。

RFP・見積依頼で確認したい事項

見積依頼時には、対象範囲、想定する★、現状調査の方法、成果物、診断の範囲、再診断の扱い、改善支援の範囲、個人情報・機密情報の取扱い、再委託の有無、スケジュール、責任分界を確認します。

成果物については、単なるチェック結果だけでなく、経営向けの要約、要求事項ごとの適合状況、根拠資料、技術的な発見事項、リスク評価、優先順位、改善ロードマップが含まれていると、その後の社内説明や取引先対応に活用しやすくなります。

よくある失敗と注意点

「取引先から言われてから対応する」

取引先から正式な取得要請が来てから着手すると、改善に時間が必要な場合に契約更新や新規案件のスケジュールへ影響することがあります。少なくとも、自社のギャップと改善期間だけは先に把握しておくことが重要です。

規程だけ整えて技術対策を後回しにする

文書上は整っていても、外部公開サーバに重大な脆弱性がある、管理者権限が過剰、バックアップから復元できない、といった状態では実効性がありません。制度対応と実際のリスク低減を同じ計画で進める必要があります。

すべてのシステムを無条件に対象にする

対象を広げすぎると、コストと工数が膨らみます。どの事業・拠点・システム・データが主要取引に関係するかを整理し、制度上の考え方と取引先要求の両方を踏まえて範囲を設計します。

情報システム部門だけで完結させる

取引先契約、調達、委託先管理、事故報告、教育、BCPなどは、法務、総務、人事、営業、経営企画など複数部門にまたがります。責任者と役割分担を決め、経営層が優先順位を判断できる体制が必要です。

Librus株式会社が提供できるSCS評価制度対応支援

制度対応から技術改善・運用まで一気通貫で支援

Librus株式会社では、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）への対応を、単なるチェックリスト対応ではなく、企業の取引継続・事業継続・信用維持に関わる経営課題として整理します。

現状把握、対象範囲の設計、要求事項とのギャップ分析、規程・体制整備、リスクアセスメントに加え、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などの技術検証、改善支援、SOC／CSIRT構築・運用支援、教育・訓練まで一気通貫で対応できます。

企業ごとにシステム構成、顧客要求、予算、優先すべき事業が異なるため、すべてを同じ形で実施するのではなく、必要な施策を個別に設計します。また、経営層向けの投資判断材料と、情報システム部門が実行できる改善項目を分けて整理し、社内の合意形成を進めやすい形にすることも重視しています。

よくある質問

Q1. SCS評価制度に対応していないと2027年から取引できなくなりますか？

一律に取引できなくなるわけではありません。SCS評価制度は任意の制度です。ただし、発注企業が★取得や一定の対策を契約・調達条件として設定した場合、その個別取引では対応が必要になる可能性があります。

Q2. ★3・★4の取得は法律上の義務ですか？

2026年10月時点では、一律の法的義務ではありません。どの水準を取引条件として求めるかは、個別の契約や発注企業のリスク管理方針によって異なります。

Q3. 大企業だけ対応すればよい制度ですか？

いいえ。業種や企業規模を問わず幅広い事業者が対象になり得ます。特に、重要な部品・サービスを提供する企業、顧客データを扱う企業、取引先システムに接続する企業は、自社規模にかかわらず準備の優先度が高くなります。

Q4. 取引先からまだ要請されていません。今から対応する必要がありますか？

直ちに取得申請をする必要があるとは限りませんが、要求事項とのギャップを把握し、改善に必要な期間と費用を確認しておくことをおすすめします。要請後に重大な不足が判明すると、契約スケジュールに影響するためです。

Q5. ISMSを取得していればSCS評価制度への対応は不要ですか？

既存のISMS運用は重要な基盤になりますが、SCS評価制度とは評価の目的や要求事項、評価スキームが同一ではありません。既存の規程・管理策を活用しつつ、SCS評価制度の要求事項との差分を確認する必要があります。

Q6. 脆弱性診断やペネトレーションテストは必ず必要ですか？

必要な技術検証は、目指す★、対象範囲、システムの重要度、制度上の詳細要件によって異なります。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を無条件に全部実施するのではなく、リスクに応じて設計することが重要です。

Q7. 取引先から★4を求められた場合、まず何をすればよいですか？

まず、要求期限、対象となる契約・事業・システム、取引先が★取得そのものを求めているのか、★4相当の対策を求めているのかを確認します。そのうえで、★4要求事項とのギャップ分析を行い、第三者評価・技術検証の前に不足項目を改善する計画を立てます。

Q8. SCS評価制度への対応費用を取引価格に反映できますか？

個別契約や取引条件によりますが、経済産業省・公正取引委員会は、発注側からのセキュリティ対策要請を踏まえて、発注側と取引先が対策費用について価格交渉する想定事例を公表しています。対策内容、追加コスト、必要性を整理し、双方で協議することが重要です。

まとめ：未対応が直ちに取引停止を意味するわけではないが、取引条件化への備えは必要

SCS評価制度は任意の制度であり、★3・★4を取得していないことだけを理由に、制度上すべての企業間取引が禁止されるわけではありません。

しかし、SCS評価制度は発注企業が取引先に必要なセキュリティ水準を示し、その実施状況を確認するための仕組みとして設計されています。今後、主要顧客の調達基準、新規取引審査、契約更新、取引先監査などで★取得や相当する対策が求められる場面は増える可能性があります。

企業が今取り組むべきことは、焦って形式的な取得準備を進めることではありません。まず、自社がサプライチェーンの中でどのような役割を担い、どの顧客・システム・情報を守る必要があるかを整理し、SCS評価制度の要求事項とのギャップを確認することです。そのうえで、規程・体制・技術対策を優先順位に沿って改善し、取引先から求められた際に説明できる状態を作ることが重要です。

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★取得を求められる可能性があるが、どこから確認すべきか分からない」「★3と★4のどちらを目指すべきか判断できない」「既存のISMSや社内規程をどこまで活用できるか整理したい」「技術診断まで含める必要があるか確認したい」といった段階でも、Librus株式会社にご相談いただけます。

現状の取引関係、システム構成、扱う情報、既存対策を確認したうえで、必要な対象範囲と優先順位を整理することで、過剰な対策投資を避けながら、取引先への説明力と実際のセキュリティ水準を同時に高めることができます。SCS評価制度の取得そのものだけでなく、取引継続、事業継続、社内稟議、技術改善まで見据えた対応方針をご検討の際は、お気軽にご相談ください。

主な出典

- 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>
- IPA「SCS評価制度の詳細情報」：<https://www.ipa.go.jp/security/scs/details.html>
- IPA「よくある質問」：<https://www.ipa.go.jp/security/scs/faq.html>
- IPA「要求事項・評価基準」：<https://www.ipa.go.jp/security/scs/requirements-criteria.html>

- 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>

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>