取引先のセキュリティチェックが厳しくなる？SCS評価制度で調達・委託はどう変わるか

結論から言えば、SCS評価制度の開始によって、すべての企業の取引先チェックが一律に「厳格化」されるわけではありません。一方で、発注企業が委託先に求めるセキュリティ水準を★3・★4という共通基準で示し、契約や取引先評価に組み込む運用は今後広がる可能性があります。受注側の企業にとっては、従来のセキュリティチェックシートへの回答だけでなく、必要な★の取得や、要求事項を満たしていることを証跡付きで説明できる状態が、取引継続・新規受注の判断材料になることが考えられます。

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（SCS評価制度）は、委託元と委託先の双方が共通の基準で対策状況を確認できるようにする制度です。2027年3月頃の★3・★4の運用開始が予定されており、経済産業省は、2社間の取引契約等において委託元が委託先に適切な段階（★）を提示し、対策の実施と実施状況の確認を行う活用を想定しています。

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

この記事で分かること

- SCS評価制度によって調達・委託時のセキュリティ確認がどう変わり得るか
- 発注側が取引先に★3・★4を求める際の考え方と注意点
- 受注側が取引停止や失注リスクを避けるために準備すべきこと
- 既存のセキュリティチェックシート、ISMS、脆弱性診断との関係
- 社内稟議、見積依頼、RFP、契約更新で確認すべき実務ポイント
- Librus株式会社がSCS評価制度対応で支援できる範囲

SCS評価制度とは？取引先の対策状況を共通基準で可視化する制度

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・可視化する仕組みです。制度の背景には、発注側から見て取引先の対策状況を外部から判断しにくいこと、反対に委託先側では複数の顧客から異なるセキュリティ要求を受け、個別回答の負担が大きいことがあります。

制度は任意であり、法律によって一律に★取得を義務付けるものではありません。ただし、どの★を取引条件として扱うかは契約当事者間で決められるため、実務上は「取引先が求める基準」として影響を持つ可能性があります。

IPAは、全てのサプライチェーン企業が対象となり得ると説明しており、業種や企業規模によって一律に除外される制度ではありません。中堅・中小企業であっても、大企業の委託先、ITサービス提供企業、個人情報や機密情報を取り扱う事業者などは、早い段階から自社の対応水準を確認しておくことが重要です。

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評価制度で調達・委託はどう変わる？

大きな変化は、発注側が「セキュリティ対策をしているか」を抽象的に確認するのではなく、取引の重要度や扱う情報に応じて、必要な対策レベルを★で示しやすくなることです。これは、従来のチェックシートを完全に置き換えるとは限りませんが、取引先評価の共通言語になり得ます。

1. 取引先選定の条件に★が加わる可能性がある

新規取引や委託先選定では、価格・品質・納期・実績に加えて、セキュリティ対策状況が評価項目に入るケースが増えています。SCS評価制度が普及すれば、RFPや見積依頼書に「SCS評価制度★3取得済み、または同等水準の対策を実施していること」などの条件が記載されることも想定されます。

ただし、制度開始時点で★取得企業が当然に存在するわけではありません。経済産業省のFAQでも、制度開始は申請受付の開始を意味するとされており、開始直後から一律に未取得企業を排除する運用が制度上定められているわけではありません。発注側には、移行期間や代替確認の方法を含めた現実的な設計が求められます。

2. 契約更新時にセキュリティ条件が見直される可能性がある

既存取引でも、基本契約や個別契約の更新時に、情報セキュリティ条項、事故報告義務、再委託管理、監査協力義務などとあわせて、SCS評価制度の取得状況を確認する運用が考えられます。特に長期契約では、必要な★を契約期間中維持することを求める運用も想定されています。

受注側は、契約更新直前に初めて対応を始めるのではなく、主要顧客がどのレベルを要求しそうか、現在の自社対策で不足する項目は何かを事前に整理しておく方が、価格交渉や改善計画の説明を行いやすくなります。

3. 「独自チェックシートへの回答」から「共通基準＋追加確認」へ

SCS評価制度の狙いの一つは、複数の取引先から異なるチェックシートへの回答を求められる委託先の負担を軽減することです。そのため、制度が定着すれば、SCS評価制度の取得状況や要求事項への適合状況をベースにし、取引固有の事項だけを追加確認する形に整理される可能性があります。

一方で、金融、医療、重要インフラ、個人情報を大量に扱う業務、委託元固有のシステムへ接続する業務などでは、SCS評価制度だけで十分とは限りません。発注側は、自社特有のリスクについては追加の契約条件や質問項目を残す必要があります。

4. 技術的な確認の重要性が高まる

★4では、評価機関による文書確認だけでなく、実地審査と技術検証が求められます。IPAは、技術検証事業者について「脆弱性診断・ペネトレーションテストのサービスを提供する法人」を主な対象としており、★4の技術検証として脆弱性診断を実施する役割を示しています。

そのため、規程やチェックシート上は適切に見えても、インターネット公開資産に重大な脆弱性が残っている、不要なポートが開放されている、Webアプリケーションに認証・認可上の欠陥がある、といった技術的な問題は無視できません。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、制度対応とは別物として切り離さず、実装状況を検証する手段として活用することが重要です。

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

発注側企業は、取引先に何を求めるべきか

発注側にとって重要なのは、すべての取引先へ同じ水準を機械的に要求することではありません。委託内容、扱う情報、システム接続の有無、代替可能性、停止時の事業影響などを踏まえ、必要な対策水準を合理的に決めることです。

取引の重要度を分類する

最初に、委託先を「止まった場合の事業影響」「自社ネットワークへの接続」「機密情報・個人情報の取扱い」「再委託の有無」「顧客向けサービスへの影響」などで分類します。基幹業務や顧客サービスの提供に直結する委託先と、限定的な情報しか扱わない委託先とでは、求める水準を分ける方が合理的です。

★の取得だけでなく、未取得時の代替確認も決める

制度開始直後は、取引先が申請中である、改善対応中である、制度上の評価をまだ受けられていないといった状況が想定されます。そのため、調達基準には「取得済みか否か」だけでなく、未取得の場合にどの資料や証跡で確認するか、いつまでに改善を求めるかを設けておくと運用しやすくなります。

契約条件と費用負担をセットで検討する

発注側が新たなセキュリティ対策や認証・評価の取得を求める場合、委託先にはシステム改修、診断、教育、運用体制整備などの追加コストが生じることがあります。経済産業省と公正取引委員会は、発注者が取引先にセキュリティ対策を要請すること自体は直ちに独占禁止法上問題になるものではない一方、コスト上昇分を考慮せず一方的に著しく低い対価を定めることなどは問題となり得ると示しています。

そのため、調達部門と情報システム・セキュリティ部門だけで決めるのではなく、法務・購買・事業部門を含めて、要請内容、必要性、導入期限、費用負担、価格改定の考え方まで整理することが重要です。

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

受注側企業は何を準備すべきか

受注側にとってSCS評価制度対応は、単なる「認証取得プロジェクト」ではありません。重要なのは、顧客に対して、自社がどの範囲でどの対策を実施し、その運用をどの証跡で説明できるかを整理することです。

1. 主要顧客と取引条件を棚卸しする

売上構成上重要な顧客、契約更新が近い顧客、情報セキュリティチェックが厳しい顧客を洗い出します。そのうえで、現在の契約にセキュリティ基準、監査、認証、インシデント報告、再委託等の条項があるかを確認します。これにより、SCS評価制度への対応優先度を経営判断しやすくなります。

2. 自社の適用範囲とIT資産を明確にする

クラウドサービス、社内ネットワーク、端末、認証基盤、インターネット公開サーバー、SaaS、委託先、テレワーク環境などを整理し、どの範囲を評価対象にするかを検討します。資産台帳が不完全な状態では、脆弱性管理やアクセス管理の説明も不十分になりやすいため、まず「何を守るのか」を明確にする必要があります。

3. 規程・運用・証跡のギャップを確認する

情報セキュリティ基本方針、アカウント管理、端末管理、脆弱性管理、バックアップ、ログ管理、インシデント対応、委託先管理、教育などについて、規程が存在するだけでなく、実際に運用されているかを確認します。例えば「退職者アカウントを速やかに削除する」と規程に書かれていても、棚卸記録や削除履歴がなければ、実施状況を説明しにくくなります。

4. 技術面の弱点を先に洗い出す

外部公開システムがある企業は、制度審査の直前ではなく、早期にWebアプリケーション診断やプラットフォーム診断を行い、重大な脆弱性を把握しておくことが有効です。攻撃経路や権限昇格を含めた実効性の確認が必要な場合は、ペネトレーションテストも選択肢になります。

発見事項はCVSS等の技術的な深刻度だけでなく、「顧客情報への到達可能性」「業務停止の可能性」「外部から悪用可能か」「修正の容易さ」などを踏まえ、事業影響と合わせて優先順位を決めます。

対応しない場合に起こり得る問題

SCS評価制度は任意制度であるため、未取得だけで直ちに法令違反になるわけではありません。しかし、取引先が★取得や一定の要求事項への適合を契約・選定条件にした場合には、営業上の影響が生じる可能性があります。

具体的には、新規RFPで候補から外れる、契約更新時に改善計画の提出を求められる、セキュリティチェックへの回答負担が増える、競合企業が★取得済みである場合に比較上不利になる、といった状況が考えられます。また、実際に事故が起きた際には、委託元への報告・復旧対応・原因調査に加えて、信用低下や事業停止が経営課題となります。

ただし、「★がない会社とは取引できない」と一律に考えるのは適切ではありません。制度上も契約当事者間での合意が前提です。発注側・受注側の双方が、必要な水準、移行期間、改善コストを共有しながら運用することが重要です。

SCS評価制度を調達・委託プロセスに組み込む実務手順

1. 経営層が、重要取引先に求めるセキュリティ水準と許容リスクを決める
2. 調達・購買部門が、委託先を重要度別に分類し、確認項目を標準化する
3. 情報システム・セキュリティ部門が、SCS評価制度の要求事項と既存チェック項目をマッピングする
4. 法務部門が、契約条項、監査権、事故報告、再委託、費用負担の条件を確認する
5. 既存取引先には移行期間を設け、取得状況または同等対策を確認する
6. 新規RFPでは必要な★と、その根拠、未取得時の代替要件を明確にする
7. 年次または契約更新時に、取得状況、重大インシデント、改善状況を再確認する

社内稟議・RFP・見積依頼で確認したいポイント

SCS評価制度対応の稟議では、「制度対応だから必要」とだけ説明するより、主要顧客から要求される可能性、売上への影響、対象システム、現状との差分、必要な改善費、取得・維持に必要な運用工数を整理すると、経営判断につながりやすくなります。

外部支援会社へRFPや見積依頼を出す場合は、SCS評価制度のギャップ分析だけを依頼するのか、規程整備、証跡設計、脆弱性診断、改善支援、専門家確認や★4評価に向けた準備まで含めるのかを明確にします。また、診断で扱う個人情報・機密情報の範囲、データの保管・削除方法、再委託の有無、報告書の取扱いも確認が必要です。

SCS評価制度の支援会社を選ぶ際のチェックポイント

支援会社は、制度文書の説明だけでなく、実際のIT環境と業務プロセスを理解し、必要な改善までつなげられるかで選ぶことが重要です。特に、規程作成だけで終わる支援では、技術的な脆弱性や運用実態との不整合が残る可能性があります。

- SCS評価制度の要求事項・評価基準を、具体的な業務とシステムに落とし込めるか
- 経営・法務・調達・情報システムの各部門を横断して支援できるか
- 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など技術検証にも対応できるか
- 不足事項を「重要度」「対応コスト」「取引影響」で優先順位付けできるか
- 取得後の継続運用、再評価、教育、インシデント対応まで支援できるか

よくある失敗と注意点

取引先すべてに同じ★を要求する

取引リスクを見ずに一律の要求を設定すると、必要以上のコストを委託先に負わせたり、調達先の選択肢を狭めたりする可能性があります。重要度に応じたリスクベースの設計が必要です。

未取得＝セキュリティが低いと判断する

SCS評価制度は開始前後の移行期があり、未取得でも要求事項相当の対策を実施している企業はあり得ます。取得状況と実態を分けて確認する視点が重要です。

チェックシートの回答だけで安心する

自己申告だけでは、実装上の問題を見逃す場合があります。重大なシステムについては、設定確認、ログ、運用記録、脆弱性診断など客観的な証拠を組み合わせることが有効です。

セキュリティ強化の費用を委託先だけに負担させる

発注側の追加要請によってコストが発生する場合は、価格交渉や導入期限を含めて十分に協議することが必要です。調達部門だけでなく、法務・事業部門も交えて運用ルールを定めるべきです。

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、チェックリストへの回答支援だけで終わらせず、経営・組織・技術の三つの観点から一気通貫で支援します。

例えば、現状の規程・運用・システム構成を確認したギャップ分析、対象範囲の整理、改善ロードマップ策定、社内規程・手順の整備、証跡の設計、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、インシデント対応体制やSOC／CSIRTの整備、教育・訓練まで、企業の状況に応じて組み合わせることが可能です。

また、取引先からSCS評価制度への対応を求められた受注側だけでなく、調達基準や委託先管理を整備したい発注側企業についても、必要な★の考え方、既存チェックシートとの整理、RFP・契約条件への落とし込みなどを支援できます。M&A、IPO、取引先監査など、経営上の重要局面に合わせた対応も可能です。

よくある質問

Q1. SCS評価制度が始まると、取引先は必ず★取得が必要ですか？

いいえ。SCS評価制度は任意制度です。ただし、委託元が契約条件として必要な★を提示することは想定されているため、個別の取引では実質的な条件になる可能性があります。

Q2. ★を取得していないと取引停止になりますか？

制度上、一律に取引停止となるルールはありません。契約上どのように扱うかは当事者間で合意する必要があります。未取得時の代替確認や改善期限を設ける運用も考えられます。

Q3. 既存のセキュリティチェックシートは不要になりますか？

必ずしも不要にはなりません。SCS評価制度を共通基準として使いながら、業界固有・取引固有の確認項目を追加する形が現実的です。

Q4. ISMSを取得していればSCS評価制度への対応は不要ですか？

不要とは限りません。両制度は目的や評価方法が異なり、相互補完的と位置付けられています。SCS評価制度の要求事項との差分確認が必要です。

Q5. 発注側はすべての委託先に★4を求めるべきですか？

一律に★4を求めるのではなく、委託内容、情報の重要度、システム接続、事業継続への影響等から必要水準を決めることが望まれます。

Q6. ★4では脆弱性診断が必要ですか？

★4では第三者評価に加えて技術検証が求められます。IPAは技術検証事業者の業務として脆弱性診断を示しており、評価機関が文書確認・実地審査・技術検証を行う仕組みが示されています。

Q7. どのくらい前から準備すべきですか？

社内規程、資産管理、アクセス管理、脆弱性管理、教育、証跡整備などに改善が必要な場合、短期間では整いません。主要顧客の契約更新やRFP予定から逆算し、早期にギャップ分析を始めるのが現実的です。

Q8. 取引先から突然SCS評価制度への対応を求められた場合、何から始めればよいですか？

まず、相手が求める★、対象範囲、期限、未取得時の代替条件を確認します。そのうえで自社の現状を要求事項と照合し、重大な不足から改善計画を作成します。

まとめ｜SCS評価制度は「取引先チェックの共通言語」になり得る

SCS評価制度によって、すべての取引先チェックが一律に厳しくなるわけではありません。しかし、発注側が委託先に求めるセキュリティ水準を★3・★4で示し、契約・RFP・取引先評価に活用する仕組みが整うことで、調達・委託におけるセキュリティ確認の位置付けはこれまで以上に明確になると考えられます。

受注側企業は、★取得の有無だけに注目するのではなく、規程、運用、証跡、技術対策を実態として整えることが重要です。発注側企業も、必要性を説明できる合理的な水準設定と、費用・移行期間を含む取引先との協議が求められます。SCS評価制度を「選別のためのラベル」ではなく、サプライチェーン全体のリスクを共通言語で整理する仕組みとして活用することが、制度の趣旨に沿った対応です。

SCS評価制度への対応方針が固まっていない段階からご相談いただけます

「取引先から★取得を求められそうだが、どこから手を付ければよいか分からない」「自社が★3と★4のどちらを目指すべきか判断できない」「調達先にどの水準を求めるべきか整理したい」といった段階でも、Librus株式会社へご相談いただけます。

現状の規程・運用・IT環境を確認したうえで、SCS評価制度の要求事項とのギャップ、優先的に改善すべき項目、診断や技術検証が必要な範囲、社内稟議で説明すべき論点を整理します。対象範囲や実施方法がまだ決まっていない場合でも、過剰投資を避けながら、取引上必要となる水準に向けた現実的なロードマップを検討できます。

主な公的情報・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

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

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「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

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