

SCS評価制度を営業力に変える方法 | 新規取引・取引継続につなげるには

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）は、企業のセキュリティ対策状況を共通の尺度で可視化し、発注・委託などの取引場面で確認しやすくする制度です。2027年3月頃に★3・★4の運用開始が予定されており、制度の活用が広がれば、セキュリティは「情報システム部門の守りの施策」だけではなく、営業・調達・経営にも関わる要素になります。

結論から言えば、SCS評価制度への対応は、適切に活用すれば新規取引の入口を広げ、既存取引の継続性を高める材料になり得ます。ただし、★を取得した事実だけを営業資料に載せれば十分というわけではありません。顧客が確認したいのは、自社の重要情報や業務を安全に預けられるか、問題が起きたときに事業を継続できるか、再委託先まで含めて管理できているかという点です。

SCS評価制度を営業力に変えるポイントは、「★取得」を売るのではなく、取引先のリスク低減にどう貢献できるかを説明できる状態にすることです。

この記事で分かること

- SCS評価制度が営業・新規取引・契約更新に影響する理由
- 発注側が取引先選定で確認する可能性があるポイント
- ★取得や対応状況を営業資料・RFP回答で活用する方法
- 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営業上の信頼につなげる考え方
- SCS評価制度への対応を「コスト」で終わらせないための社内連携と運用方法

SCS評価制度とは何か

SCS評価制度は、サプライチェーンを構成する企業のIT基盤について、一定のセキュリティ対策が実施されていることを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示し、IPA（独立行政法人情報処理推進機構）が制度を運営します。

IPAは、委託元企業には「委託先の対策状況を把握しにくい」、委託先企業には「複数の委託元から異なるチェックリストを求められ負担が大きい」という課題があると説明しています。SCS評価制度では、二社間の取引契約などにおいて、委託元が委託先に必要な段階（★）を示し、その対策状況を確認する利用方法が想定されています。

2026年10月22日時点では、★3・★4は2027年3月頃の運用開始予定です。★3は「専門家確認付き自己評価」、★4は「第三者評価」が基本となり、★4では文書確認に加えて実地審査や技術検証も行われる設計です。

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>

出典：IPA「SCS評価制度の詳細情報」

<https://www.ipa.go.jp/security/scs/details.html>

なぜSCS評価制度が営業に影響するのか

取引先のセキュリティ確認が「個別質問」から「共通評価」へ変わる可能性がある

これまで企業間取引では、取引開始前に情報セキュリティチェックシートを提出したり、ISMS認証の有無、脆弱性診断の実施状況、事故発生時の連絡体制などを個別に回答したりする運用が一般的でした。発注企業ごとに質問項目が異なるため、受注側では営業・法務・情報システム部門が毎回資料を集めて回答するケースも少なくありません。

SCS評価制度が普及すると、「どの★を取得しているか」「要求事項をどの範囲で満たしているか」が取引前の確認材料として利用される可能性があります。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、取引先からの対策要請による活用促進、利害関係者への情報開示による対話の促進を掲げています。

価格・技術だけではなく「安心して委託できるか」が比較軸になる

BtoB取引では、価格や機能、納期が優れていても、委託先のセキュリティ管理に不安があれば採用しにくいケースがあります。とくに顧客情報、設計情報、認証情報、ソースコード、機密文書などを扱う業務では、事故が起きた場合の影響が発注企業にも及ぶためです。

そのため営業活動では、「当社はセキュリティに力を入れています」という抽象的な説明より、SCS評価制度の要求事項に沿った管理状況や、客観的な診断結果、是正状況を説明できる方が、社内稟議や取引先審査を進めやすくなります。

既存取引でも契約更新・委託範囲拡大の判断材料になり得る

SCS評価制度は新規取引だけに関係するものではありません。既存顧客がサプライチェーン管理を強化した場合、契約更新時や業務範囲の追加時に、セキュリティ対策の確認を受ける可能性があります。特に大企業や重要インフラ関連企業、製造業、金融、流通など、サプライチェーンの影響が大きい分野では、委託先管理の高度化が進むことが考えられます。

受注企業にとっては、「事故を起こしていないから大丈夫」ではなく、要求された対策を継続的に実施し、その証拠を説明できることが取引維持の観点でも重要になります。

SCS評価制度を営業力に変える5つの方法

1. 提案書・会社案内で「対策の事実」を簡潔に示す

営業資料では、SCS評価制度への対応状況を長々と説明する必要はありません。重要なのは、顧客が安心材料として確認したい情報を短時間で理解できることです。たとえば、取得している★、適用範囲、主要なセキュリティ対策、インシデント対応体制、定期的な診断の実施状況などをまとめます。

なお、取得前の段階で「SCS対応済み」「SCS認証取得」と誤認される表現を使うべきではありません。制度上の状態と、自社で進めている準備状況を区別して説明することが信頼につながります。

2. RFP・セキュリティチェックへの回答スピードを上げる

新規商談でRFP(提案依頼書)やセキュリティチェックシートを受け取った際、回答に時間がかかる企業は営業機会を逃すことがあります。SCS評価制度への対応過程で、規程、資産管理、アクセス管理、脆弱性管理、インシデント対応、委託先管理などを整理しておけば、回答に必要な情報を取り出しやすくなります。

営業部門が毎回ゼロから情報システム部門に確認するのではなく、回答テンプレート、証跡の保管場所、開示可能範囲、承認フローを決めておくと、提案スピードを落とすにくくなります。これは制度取得そのものとは別の効果ですが、営業実務では大きな差になります。

3. 「★取得」ではなく顧客のリスク低減として説明する

営業担当者が制度名や要求事項を詳しく説明しても、顧客にとっての価値が伝わらないことがあります。顧客が知りたいのは、自社が安全かどうかではなく、「この会社に業務を委託したとき、自社の事業リスクを許容できるか」です。

たとえば、アクセス権限の定期棚卸しを行っているなら「退職者や異動者の不要な権限が残り続けるリスクを低減する運用」、バックアップと復旧訓練を行っているなら「ランサムウェア等で業務停止した場合の復旧可能性を高める仕組み」と説明すると、経営・調達部門にも意義が伝わりやすくなります。

4. 技術的な裏付けを示す

規程やチェックシートだけでは、システムに実際の弱点がないことまでは確認できません。顧客からインターネット公開システムやクラウド基盤の安全性を問われる場合には、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的検証が有効です。

Webアプリケーション診断は、Webサービスにおける入力処理や認証、権限制御などの脆弱性を確認します。プラットフォーム診断は、サーバー、ネットワーク機器、OS、ミドルウェア等の設定や既知の脆弱性を確認します。ペネトレーションテストは、想定する攻撃シナリオに基づいて実際に侵入可能性や影響範囲を検証する手法です。

営業で重要なのは「診断を実施した」という事実だけではありません。重大な問題が見つかった場合に優先順位を付け、是正し、必要に応じて再診断していることまで説明できると、継続的な改善能力を示しやすくなります。

5. 営業・情報システム・法務・経営を同じ説明軸でつなぐ

SCS評価制度への対応を営業力に変えるには、情報システム部門だけに任せないことが重要です。営業は顧客が何を懸念しているかを把握し、情報システム部門は技術・運用の実態を整理し、法務・管理部門は契約や情報開示の範囲を管理し、経営層は投資優先順位とリスク許容度を判断します。

この連携ができていない企業は、商談中にセキュリティ要件が追加されても、実現可能性、費用、対応時期を早く判断できます。結果として、セキュリティが商談のブレーキになるのではなく、顧客との信頼形成に活用しやすくなります。

どのような企業で営業上の効果が出やすいか

SCS評価制度はサプライチェーンを構成する企業を広く対象としています。営業上の効果が特に表れやすいのは、取引先から情報セキュリティチェックを受ける機会が多い企業です。

具体的には、大手企業の業務委託先、ITサービス・SaaS事業者、システム開発会社、製造業のサプライヤー、物流・流通、金融関連サービス、機密情報を扱うBPO事業者などが考えられます。また、IPO準備、M&A、重要顧客との大型契約など、取引先や投資家からガバナンスを確認される局面でも、セキュリティ管理状況を整理しておく意義があります。

対応しない場合に起こり得る営業上の問題

SCS評価制度の★取得は一律の法的義務ではありません。しかし、特定の取引において発注者が一定の★や相当する対策を要求した場合、未対応であることが商談条件に影響する可能性があります。

想定されるのは、セキュリティ審査に時間がかかる、追加質問や現地確認が増える、契約開始が遅れる、競合企業との比較で説明材料が不足する、対応計画の提出を求められる、といった事態です。場合によっては、委託する情報やシステムの重要度に応じて、業務範囲を限定される可能性もあります。

したがって、営業上は「取得していないから取引できない」と単純化するのではなく、自社の主要顧客、契約更新時期、顧客が求める水準を確認し、優先順位を付けて準備することが現実的です。

営業活用まで見据えたSCS評価制度対応の進め方

Step 1. 重要顧客と取引条件を整理する

最初に、売上や事業継続への影響が大きい顧客、今後獲得したい大手顧客、更新予定の主要契約を洗い出します。そのうえで、現在どのようなセキュリティチェックを受けているか、ISMS等の認証を要求されているか、診断報告書の提出を求められるかを整理します。

Step 2. SCS要求事項とのギャップを確認する

次に、SCS評価制度の要求事項・評価基準と現状を比較します。規程が存在するだけでなく、実際の運用、記録、責任者、対象範囲、改善サイクルまで確認します。営業上重要な顧客に係るシステムや拠点を優先すると、投資判断もしやすくなります。

Step 3. 重大なギャップを優先して改善する

すべてを同時に改善するのではなく、事業停止、情報漏えい、不正アクセス、取引停止につながるリスクから優先します。多要素認証、不要アカウントの削除、パッチ適用、バックアップ、ログ監視、インシデント連絡体制などは、技術面と運用面の両方を確認します。

Step 4. 必要な技術検証を実施する

外部公開Webサービスや重要システムがある場合は、Webアプリケーション診断、プラットフォーム診断、必要に応じたペネトレーションテストを実施し、実装上の弱点を把握します。検出事項はリスクと事業影響で優先順位付けし、是正計画を作成します。

Step 5. 営業向けの説明資料を作る

取得状況、適用範囲、主要対策、診断・改善の実施状況、事故発生時の連絡体制などを、顧客向けに開示できる範囲で整理します。機密情報や具体的なネットワーク構成、脆弱性の詳細は不用意に営業資料へ記載せず、必要に応じてNDA締結後に限定開示します。

Step 6. 契約更新と定期レビューに組み込む

取得後も人事異動、クラウド変更、新規システム導入、再委託先変更などでリスクは変化します。主要顧客の契約更新前にセキュリティ対策の棚卸しを行い、営業・情報システム・管理部門で説明内容を更新する運用が有効です。

費用と期間を左右する要因

SCS評価制度対応に必要な費用や期間は、取得を目指す★、対象範囲、現状の成熟度、拠点数、システム数、既存規程の整備状況、技術的な改善の必要性などによって変わります。

特に費用が大きくなりやすいのは、認証・審査そのものより、現状とのギャップを埋めるための技術・運用改善です。たとえば、認証基盤の見直し、EDRやログ管理の導入、バックアップ構成の改善、脆弱性診断、ネットワーク分離、委託先管理の再設計などが必要になる場合があります。

営業部門から見ると、単なる「セキュリティ費」として稟議を上げるより、重要顧客の契約継続、新規顧客の参入条件、審査工数削減、事故による事業停止リスクの低減という経営上の効果とセットで説明する方が、投資判断につながりやすくなります。

SCS評価制度の支援会社を選ぶポイント

支援会社を選ぶ際は、要求事項の説明だけでなく、現状評価から改善、技術検証、証跡整備、取得後の運用まで支援できるかを確認するとよいでしょう。営業活用まで見据える場合は、経営・取引先対応の観点から「どこまで対策すべきか」を整理できることも重要です。

RFPや見積依頼では、対応可能な★、ギャップ分析の方法、成果物、対象範囲の決め方、技術検証の対応範囲、再診断の条件、機密情報の取扱い、改善支援の有無、取得後の伴走支援などを確認します。単に制度申請を代行するだけでなく、実態として対策水準を高められるかが重要です。

よくある失敗と注意点

「★を取れば営業で勝てる」と考える

SCS評価制度は取引先の判断材料になり得ますが、製品・サービスの品質、価格、納期、実績の代わりになるものではありません。セキュリティは「選定候補から外れにくくする」「審査を通しやすくする」「安心して委託できる根拠を増やす」要素として位置付ける方が現実的です。

営業資料で機密情報を出し過ぎる

セキュリティをアピールするために、ネットワーク構成、利用製品、脆弱性の詳細、監視ルールなどを広く開示すると、逆にリスクを高める場合があります。営業資料、NDA締結後資料、評価機関向け資料の開示レベルを分けることが重要です。

規程だけ整えて運用記録がない

セキュリティポリシーや手順書が整っていても、実際にアカウント棚卸し、パッチ管理、教育、バックアップ確認、インシデント訓練などを実施していなければ、実態を説明しにくくなります。取引先に対する信頼を高めるためにも、証跡を残す運用が必要です。

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、制度要求への形式的な対応だけでなく、企業の事業環境・顧客構成・システム構成に合わせたセキュリティ強化として支援します。

現状のギャップ分析、対象範囲の整理、規程・運用・証跡の整備、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、教育・訓練などを組み合わせ、一気通貫で対応可能です。

また、営業・経営・情報システム部門の間で、「顧客に何を説明する必要があるか」「どの対策を優先するか」「どこまで投資すべきか」を整理する支援も行います。SCS評価制度への対応を単なる認証取得プロジェクトで終わらず、取引先からの信頼獲得と継続的なセキュリティ改善につなげることを重視しています。

よくある質問

Q1. SCS評価制度を取得すれば新規取引で有利になりますか？

取引先がSCS評価制度を選定条件や確認材料として利用する場合、説明負担の軽減や信頼性の提示につながる可能性があります。ただし、取得すれば必ず受注できる制度ではありません。顧客が求める水準、適用範囲、実際の対策内容を合わせて説明することが重要です。

Q2. SCS評価制度の★取得は必須ですか？

2026年10月22日時点では、一律の法的義務ではありません。一方、取引先が契約条件として一定の★や対策水準を求めるケースは想定されています。主要顧客の調達基準や今後の更新条件を確認して優先順位を決める必要があります。

Q3. ISMSを取得済みでも営業上SCS評価制度は必要ですか？

ISMSとSCS評価制度は目的や評価の仕組みが異なります。ISMS取得が有効な説明材料になる一方、取引先がSCS評価制度を指定した場合には別途対応が必要になる可能性があります。既存のISMS運用を活用しながらギャップを確認する方法が効率的です。

Q4. 営業資料にSCS評価制度への対応状況を記載してよいですか？

事実に基づく範囲で記載できます。ただし、未取得段階で取得済みと誤認される表現は避けるべきです。「取得準備中」「要求事項とのギャップ分析を実施」など、実態が分かる表現にします。

Q5. 脆弱性診断をしていれば十分ですか？

脆弱性診断は重要な技術対策ですが、それだけで組織全体のセキュリティ管理を説明できるわけではありません。アクセス管理、資産管理、インシデント対応、教育、委託先管理、バックアップなど、組織的・技術的対策を組み合わせる必要があります。

Q6. ペネトレーションテストは必ず必要ですか？

対象となる★、システム、評価範囲、リスクによって必要性は異なります。外部公開システムや重要資産について高度な技術検証が必要な場合には有効ですが、実施目的を明確にしたうえで範囲を設計することが重要です。

Q7. どの部門がSCS評価制度を担当すべきですか？

情報システム・セキュリティ部門だけで完結させるより、経営、営業、法務・管理、事業部門を含めた体制が実務的です。取引条件、契約、技術対策、顧客への説明をそれぞれ連携させる必要があるためです。

Q8. 対象範囲が決まっていなくても相談できますか？

可能です。主要顧客、提供サービス、扱う情報、システム構成、既存認証などを確認し、どの範囲から着手すべきか整理するところから進められます。

まとめ | SCS評価制度を「守りのコスト」から「取引の信頼」に変える

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、企業のセキュリティ対策状況を取引場面で可視化する仕組みです。今後、発注・委託時に制度が活用される場面が増えれば、セキュリティ対応は情報システム部門だけの課題ではなく、新規取引や契約継続にも関わる経営課題になります。

営業力につなげるために重要なのは、★取得そのものを目的化しないことです。顧客が安心して業務を委託できるよう、要求事項に沿った管理、技術検証、改善実績、インシデント対応体制を整え、それを過不足なく説明できる状態をつくる必要があります。

主要顧客からセキュリティチェックを受ける機会が増えている企業、今後大手企業との取引を拡大したい企業は、制度開始後に対応を迫られてから準備するのではなく、現在の対策状況と顧客要求の差を早めに把握しておくことが有効です。

SCS評価制度への対応を、取引先への説明力まで含めて整理したい企業様へ

Librus株式会社では、「どの★を目指すべきか分からない」「取引先から求められる前に現状を確認したい」「SCS対応を営業・契約更新にも活用したい」といった段階からご相談いただけます。

制度要求とのギャップ分析だけでなく、規程・証跡・技術対策の整備、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、改善計画、取得後の運用まで一気通貫で整理することで、重複投資を抑えながら実効性のある対策を進めやすくなります。

対象範囲や実施方法がまだ決まっていない場合でも、主要顧客、事業、システム、既存のセキュリティ体制を確認し、優先順位を整理するところから支援可能です。セキュリティ対策を取引先への信頼や事業継続につなげた場合は、現状整理の段階からご相談ください。

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>