SCS評価制度とサプライチェーン攻撃対策｜委託先・取引先管理の重要ポイント

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、自社だけのセキュリティ対策を評価するための制度ではありません。委託元と委託先が、取引上必要なセキュリティ水準を共通の「★」で確認し、サプライチェーン全体の対策を底上げすることを目的としています。

結論からいえば、企業が最初に取り組むべきことは、すべての取引先に一律の対策を求めることではなく、「どの委託先・取引先が自社の事業継続や重要情報に大きな影響を持つか」を把握し、リスクに応じて管理水準を変えることです。SCS評価制度は、その判断と確認を標準化するための有力な仕組みになります。

> 重要なポイント：サプライチェーン攻撃対策では、「自社の境界線の外にあるリスク」を管理対象に含める必要があります。委託先の**VPN**、クラウド、保守アカウント、開発環境などが侵入口になれば、自社のシステムが直接攻撃されていなくても被害が波及する可能性があります。

この記事で分かること

この記事では、SCS評価制度とサプライチェーン攻撃対策の関係、委託先・取引先を管理する際の考え方、契約・評価・監査・技術検証の実務、そして自社の負担を過度に増やさずに管理を継続する方法を解説します。特に、従業員100～1,000名程度の企業で、情報システム部門だけでは取引先全体を把握しきれないケースを想定しています。

SCS評価制度とは？サプライチェーン全体の対策水準を可視化する仕組み

SCS評価制度は、経済産業省と内閣官房国家サイバー統括室が2026年3月に制度構築方針を公表し、IPAが運営する制度です。2026年11月4日時点のIPA公表情報では、★3・★4の登録申請は2027年3月から開始予定とされています。

制度の特徴は、委託元が委託先に対して求めるセキュリティ水準を、個別のチェックリストだけではなく、共通の段階評価で示せる点です。★3は一般的なサイバー脅威に対処しうる水準、★4は初期侵入の防御だけでなく、被害拡大防止や事業継続への影響低減まで含め、サプライチェーン企業が標準的に目指すべき水準として設計されています。

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

なぜ委託先・取引先管理が重要なのか

IPAの「情報セキュリティ10大脅威2026」では、「サプライチェーンや委託先を狙った攻撃」が組織向け脅威の2位に挙げられています。攻撃者は、標的企業そのものよりも対策が弱い関連会社、業務委託先、保守事業者などを狙い、そこから秘密情報を窃取したり、正規の接続経路を利用して侵入したりします。

出典：IPA「情報セキュリティ10大脅威 2026」 https://www.ipa.go.jp/security/10threats/10threats2026.html

典型的なサプライチェーン攻撃のパターン

例えば、システム保守を委託している事業者のVPNアカウントや管理者IDが窃取されると、攻撃者が正規の保守経路を使って自社ネットワークへ侵入する可能性があります。また、開発委託先の端末やソースコード管理環境が侵害されれば、改ざんされたプログラムが納品されるリスクもあります。SaaSやMSP（Managed Service Provider：IT運用を継続的に代行する事業者）のように、多数の企業へサービスを提供する事業者が侵害された場合、影響が複数社へ同時に波及することもあります。

つまり、自社のファイアウォールやEDRを強化するだけでは、サプライチェーンリスクを十分に管理できません。自社と外部組織の「接点」を把握し、その接点ごとに必要な対策を決める必要があります。

委託先の事故でも、自社の経営リスクになり得る

委託先で情報漏えいが発生した場合でも、自社が委託した個人データが対象であれば、委託元側にも個人情報保護委員会への報告や本人通知が必要となる場合があります。セキュリティ事故は「委託先の問題」で完結するとは限りません。対応費用、顧客説明、事業停止、信用低下、契約上の責任などを通じて、委託元の経営課題に直結します。

出典：個人情報保護委員会「委託先での漏えい対応について」 https://www.ppc.go.jp/all_fad_index/fad2-1-2-q10/

SCS評価制度で委託先・取引先管理はどう変わるのか

SCS評価制度の実務的な価値は、委託先のセキュリティ対策を「各社独自の質問票だけで確認する状態」から、「共通の評価水準を利用して確認する状態」へ移行できる点にあります。IPA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、対策を促すとともに実施状況を確認する利用を想定しています。

出典：IPA「SCS評価制度」 https://www.ipa.go.jp/security/scs/index.html

すべての取引先に同じ★を求める制度ではない

重要なのは、★3・★4を一律に要求するのではなく、取引先が持つ情報管理リスクと事業継続リスクを踏まえて水準を決めることです。例えば、自社の基幹システムを運用し、停止すると受発注が止まる委託先と、一般公開情報のみを扱う外部事業者では、求める管理水準が同じとは限りません。

経済産業省・IPAの制度構築方針でも、取引先の事業中断が自社の事業継続に大きく影響する場合などには★4を求める考え方が例示されています。したがって、委託先管理の第一歩は「取引先一覧」ではなく、「取引先ごとのリスク分類」を作ることです。

出典：IPA「SCS評価制度 制度構築方針」 https://www.ipa.go.jp/security/scs/rcu1hd0000007ajp-att/20260327001-br.pdf

委託先・取引先管理で押さえるべき7つの重要ポイント

1. 委託先・再委託先を会社全体で棚卸しする

最初に必要なのは、情報システム部門が把握しているITベンダーだけでなく、各事業部、営業、管理部、人事、マーケティングなどが個別に契約している外部事業者まで含めて棚卸しすることです。クラウドサービス、給与計算、コールセンター、データ入力、システム保守、開発、物流など、情報やシステムに接触する委託先は多岐にわたります。

さらに、再委託がある場合には、直接契約していない事業者が自社データへアクセスしている可能性があります。契約書に再委託条件を設け、再委託先の把握・承認・管理責任を明確にすることが重要です。

2. 事業影響と情報影響でリスクを分類する

委託先ごとに、少なくとも「止まった場合の事業影響」と「漏えい・改ざんが起きた場合の情報影響」を評価します。判断材料には、取り扱う個人情報・機密情報の種類、システム権限、ネットワーク接続の有無、代替可能性、復旧に要する時間、売上や顧客対応への影響などを含めます。

経営層は、どの取引先を重要委託先として管理するか、どこまでの停止時間を許容するかを決める必要があります。この基準が曖昧なままだと、現場は「全社に厳しい要求を出す」か「重要な委託先にも最低限しか求めない」かのどちらかに偏りやすくなります。

3. 契約段階でセキュリティ要求と責任分界を明確にする

セキュリティ条件は、事故が起きてから協議するのではなく、契約・更新時に決めておく必要があります。確認すべき事項として、要求するSCS評価制度の段階、事故発生時の報告期限、ログ保存、脆弱性対応、再委託条件、監査への協力、契約終了時のデータ返却・削除、インシデント調査への協力などが挙げられます。

経済産業省のサイバーセキュリティ経営ガイドラインでも、ビジネスパートナー等との契約において、サイバーセキュリティリスクへの対応に関する役割と責任範囲を明確化することが求められています。

出典：経済産業省「サイバーセキュリティ経営ガイドライン」 https://www.meti.go.jp/policy/netsecurity/mng_guide.html

4. 取得マークだけでなく、適用範囲と実態を確認する

取引先が★を取得している場合でも、自社との取引に関係する部門・拠点・システムが評価の適用範囲に含まれているかを確認する必要があります。評価済みの本社環境と、実際に自社データを処理する別拠点・別システムが異なるケースも考えられるためです。

重要委託先については、取得状況だけでなく、適用範囲、評価日、有効期間、重大な変更の有無、直近のインシデント、是正状況などを確認すると、より実効性のある管理になります。

5. 技術的な接点は診断・検証で確認する

質問票や認証情報だけでは、実際のシステムに脆弱性が残っているかは分かりません。外部公開Webシステムを委託している場合にはWebアプリケーション診断、VPN・サーバー・ネットワーク機器などにはプラットフォーム診断が有効です。重要な業務システムや複数の経路を組み合わせた侵入可能性まで確認したい場合には、ペネトレーションテストを検討します。

SCS評価制度の★4では、評価機関・技術検証事業者による文書確認、実地審査、技術検証（脆弱性検査）が想定されています。一方、企業が自社の取引先管理として実施する診断は、制度上の評価そのものとは別に、リスクに応じて対象・頻度を設計することが重要です。

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

6. 事故発生時の連絡・初動を共同で決めておく

委託先でランサムウェア感染や不正アクセスが起きた場合、自社への影響確認には時間制約があります。事故連絡の窓口、緊急連絡先、報告すべき情報、初報の期限、ログ提供方法、ネットワーク遮断やアカウント停止の判断者などを平時に決めておくべきです。

「原因が確定してから報告」では、委託元側の初動が遅れる可能性があります。初報では事実が未確定でも、影響の可能性がある段階で連絡し、その後アップデートする運用の方が実務的です。

7. 一度の確認で終わらせず、継続的に見直す

委託先のセキュリティ状態は固定ではありません。システム更改、クラウド移行、M&A、再委託先変更、担当者変更、新しい脆弱性の公開などによりリスクは変わります。そのため、契約更新時の確認、定期的なSCS評価制度の取得状況確認、重大変更時の再評価、必要に応じた再診断を組み合わせることが重要です。

SCS評価制度に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り、★を取得していないことだけを理由に制度上ただちに取引停止になるわけではありません。ただし、★の取得を取引条件とするかどうかは契約当事者間で決められます。今後、発注企業が重要委託先に一定の★を求める運用を採用すれば、未対応企業は追加説明、個別監査、改善計画の提出などを求められる可能性があります。

出典：IPA「SCS評価制度 よくある質問」 https://www.ipa.go.jp/security/scs/faq.html

逆に発注側の企業にとっては、委託先の対策状況を把握できていないと、事故発生時に「なぜこの委託先に重要情報を預けたのか」「どの基準で選定したのか」を説明しにくくなります。制度対応は単なる認証取得ではなく、取締役会や監査、顧客からの説明要求に耐えられる委託先管理プロセスを作る機会として捉えることが重要です。

対象となる企業・システム・取引場面

特に優先して管理すべきなのは、基幹システムの開発・運用、クラウド基盤、ネットワーク保守、顧客情報・従業員情報の処理、決済・受発注、製造・物流、コールセンター、外部SOC・MSPなど、自社の重要業務や重要情報に直接関与する委託先です。

また、M&AやIPO、重要顧客との新規取引、大規模なシステム更改などの局面では、既存の取引先管理が十分かを改めて確認する必要があります。セキュリティデューデリジェンスや取引先監査の結果を、SCS評価制度への準備と共通化すると、重複作業を抑えやすくなります。

委託先管理を実施する具体的な手順

Step 1：委託先台帳とデータフローを作る

契約先名だけではなく、委託業務、主管部門、取り扱う情報、接続方式、利用システム、再委託の有無、契約更新日、緊急連絡先を整理します。可能であれば「どのデータが、どこからどこへ移動するか」を簡単なデータフローとして可視化します。

Step 2：重要度を分類し、求める水準を決める

事業継続と情報管理の両面から重要度を分類し、SCS評価制度の★3・★4を参考に、必要な水準を決めます。すべての委託先を同じ水準にするより、重要委託先に管理リソースを集中する方が現実的です。

Step 3：現状との差分を確認する

既存の契約条項、セキュリティチェックシート、Pマーク・ISMS等の認証、脆弱性診断結果、インシデント履歴を集め、必要水準との差分を確認します。すでに整備済みの仕組みを再利用できる場合は、SCS対応のためにゼロから文書を作り直す必要はありません。

Step 4：改善計画と期限を設定する

不足事項を「重大度」「悪用可能性」「事業影響」「対応期間」で優先順位付けします。すぐに対応できない項目は、代替策、期限、責任者を決め、経営層に残存リスクを説明できる状態にします。

Step 5：契約・運用・技術の**3**面で定着させる

契約書だけを改定しても運用されなければ意味がありません。調達時の確認、契約更新、定期モニタリング、事故連絡訓練、技術診断などを年間スケジュールに組み込み、主管部門と情報システム・セキュリティ部門の役割を決めます。

費用と期間を左右する要因

委託先管理の費用は、取引先数だけでは決まりません。重要委託先の数、再委託構造、扱う情報の機密性、ネットワーク接続、現行契約の整備状況、既存認証の有無、診断対象システム数、評価・監査の頻度などで変わります。

短期間で全取引先を一斉に評価しようとすると、主管部門や調達部門の負荷が高まりやすいため、まず重要委託先から着手し、その後対象を拡張する進め方が現実的です。予算申請では、「制度取得費」だけでなく、台帳整備、規程改定、契約見直し、技術対策、診断、教育、継続モニタリングまで含めて整理すると、後から追加稟議が発生しにくくなります。

支援会社を選ぶ際のチェックポイント

SCS評価制度への対応支援会社を選ぶ際は、制度文書を説明できるだけでなく、実際の委託先管理・情報セキュリティ体制・技術診断まで一貫して扱えるかを確認することが重要です。特に、以下の観点をRFPや見積依頼に含めると比較しやすくなります。

- SCS評価制度の★3・★4要求事項を、自社の既存規程や運用へマッピングできるか
- 委託先の重要度分類、契約条項、再委託管理まで支援できるか
- 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等の技術検証に対応できるか
- 発見事項を経営リスク・事業継続・取引リスクへ翻訳して説明できるか

- 改善後の再確認や継続運用まで支援範囲に含められるか

よくある失敗と注意点

チェックシートの回収をゴールにしてしまう

回答が「実施済み」でも、証跡や実装状況を確認しなければ実効性は分かりません。特に重要委託先では、規程、ログ、設定画面、診断結果など、客観的な根拠を確認する仕組みが必要です。

重要度を付けず、全社一律に要求する

小規模な委託先に過大な要求を行うと、取引コストが増え、対策が形式化するおそれがあります。SCS評価制度の段階を参考に、リスクに応じて要求を調整することが重要です。

情報システム部門だけで管理する

委託契約を持つのは各事業部であることが多く、情報システム部門だけでは委託先を把握できません。調達、法務、管理部、事業部、セキュリティ担当が連携し、契約開始前から管理するプロセスが必要です。

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、要求事項への形式的なチェックだけで終わらせず、実際の経営・業務・IT環境に合わせて設計します。委託先・取引先の棚卸し、リスク分類、SCS評価制度の要求事項とのギャップ分析、規程・契約・運用の整備、技術的な弱点の検証、改善計画まで一気通貫で支援可能です。

また、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、レッドチーム演習、SOC／CSIRT支援、インシデントレスポンス、デジタルフォレンジックなどの技術領域と、情報セキュリティ体制構築、リスクアセスメント、M&A・IPO等の経営上の重要局面を組み合わせて支援できます。

制度対応のためだけに過剰な仕組みを増やすのではなく、既存のISMS、Pマーク、社内規程、取引先チェックシートなどを活用しながら、必要な部分を補強する設計を重視しています。

よくある質問

SCS評価制度はすべての委託先に取得を求める必要がありますか？

いいえ。制度自体は任意であり、どの取引先にどの段階を求めるかは契約当事者間で決めます。事業継続や情報管理への影響を踏まえ、重要度に応じて要求水準を設計するのが現実的です。

★3と★4はどのように使い分ければよいですか？

★3は一般的なサイバー脅威に対処しうる水準、★4は供給停止等によりサプライチェーンへ大きな影響を及ぼす企業等が標準的に目指す水準です。自社との接続、扱う情報、停止時の影響などを基に判断します。

取引先がISMSやPマークを持っていれば十分ですか？

既存認証は重要な参考情報ですが、SCS評価制度とは目的・要求事項が完全には同じではありません。認証の適用範囲と、自社取引に関わるシステム・業務が含まれているかを確認する必要があります。

委託先への脆弱性診断は必須ですか？

すべての委託先に一律で必須とは限りません。重要システムやインターネット公開環境など、技術的リスクが高い対象では診断の有効性が高くなります。★4の制度評価では技術検証が組み込まれています。

再委託先まで管理する必要がありますか？

自社の重要情報やシステムに影響する再委託先は、可能な範囲で管理対象に含めることが重要です。契約上、再委託の承認、同等のセキュリティ義務、事故報告を求める方法があります。

SCS評価制度への対応はどの部署が担当すべきですか？

情報システム・セキュリティ部門だけではなく、調達、法務、管理部門、各事業部、経営層の連携が必要です。特に委託先の重要度判断や許容リスクは経営判断を伴います。

何から着手すればよいか分からない場合は？

まず委託先一覧、契約、取り扱い情報、システム接続、既存のチェックシートや認証状況を整理します。対象範囲や★3・★4の判断が未確定でも、現状把握から着手できます。

まとめ｜SCS評価制度を「取引先管理の共通言語」として活用する

SCS評価制度は、サプライチェーン攻撃を直接なくす制度ではありません。しかし、委託元と委託先が必要なセキュリティ水準を共有し、対策状況を確認しやすくすることで、これまで属人的・個別的だった取引先管理を改善する基盤になります。

重要なのは、★の取得状況だけを見るのではなく、委託先の重要度、適用範囲、契約、実際の技術対策、事故対応、継続的な見直しまでを一つの管理プロセスとして設計することです。サプライチェーン攻撃対策は、情報システム部門だけの仕事ではなく、事業継続・信用・取引維持に関わる経営課題として進める必要があります。

SCS評価制度・委託先管理の準備段階からご相談いただけます

> 「どの委託先を対象にすべきか分からない」「★3と★4のどちらを想定すべきか判断できない」「既存のチェックシートやISMSをどこまで流用できるか確認したい」といった段階でもご相談いただけます。Librus株式会社では、制度要求とのギャップ整理から、委託先のリスク分類、規程・契約の整備、脆弱性診断・ペネトレーションテスト、改善後の運用設計まで、企業の環境に応じて必要な範囲を個別に設計します。早い段階で現状と不足点を可視化することで、不要な対策への投資を避けながら、取引先からの要求や2027年の制度開始に備えやすくなります。

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