発注企業が構築すべき「取引先SCS管理」の実務

重要度分類・★取得要請・進捗管理・未達企業支援を一気通貫で設計する

SCS評価制度の取引先管理は「対象・期限・支援」の設計から始める

結論から言えば、発注企業が構築すべき「取引先SCS管理」は、全取引先に同じ星を一律要求する仕組みではありません。自社事業への影響を基準に取引先を分類し、必要な★（段階）と期限を定め、証跡を確認し、未達先には改善支援またはリスク低減策を講じる継続的な管理プロセスです。

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、委託元が委託先に適切な段階を提示し、対策を促し、実施状況を確認する利用を想定しています。したがって、発注企業に必要なのは「取得してください」という通知文だけではありません。誰を対象とし、どの水準を、いつまでに、誰が確認し、未達をどう扱うかを、調達・情報システム・法務・事業部の共通ルールとして定める必要があります。

この記事で分かること

- 取引先を事業影響で分類し、★3・★4の要請水準を決める方法
- 依頼、回答、証跡、期限、例外を管理する台帳と会議体の設計
- 未達企業を直ちに排除せず、改善計画と代替統制で支援する方法
- 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使い分ける考え方
- 予算、期間、稟議、RFP、ベンダー選定で押さえる実務ポイント

SCS評価制度とは何か

SCS評価制度は、取引先へのサイバー攻撃を起点とする情報漏えい、改ざん、サービス停止、踏み台化などのリスクに対し、必要な対策水準を段階別に示し、マーク取得を通じて対策状況を可視化する制度です。経済産業省と内閣官房国家サイバー統括室の監督のもと、IPAが運営します。

制度上、★3は一般的なサイバー脅威に対処し得る水準で、セキュリティ専門家の確認を経た自己評価が基本となります。★4は、初期侵入の防御だけでなく、被害拡大防止や取引先データ・システムの保護、サプライチェーン上の役割に応じた強靭化を求め、第三者評価と技術検証を伴います。★5は高度な攻撃への対応を想定するが、2026年9月時点では今後の具体化事項が残っています。上位段階は下位段階を包含するが、★4取得の前提として★3取得が必須という関係ではありません。

一次情報：IPA「SCS評価制度」／制度の詳細情報／要求事項・評価基準

なぜ今、発注企業に取引先SCS管理が必要なのか

チェックシート配布だけでは、残存リスクが分からない

従来の取引先調査では、自社独自の質問票を年1回送付し、回答が返れば完了とする運用が少なくありません。しかし、回答が自己申告のまま検証されない、重要な取引先と軽微な取引先が同じ設問になる、再委託先が管理対象から漏れる、といった弱点があります。SCS評価制度は共通水準を利用できるため、発注企業ごとの質問のばらつきを減らし、取引先との会話を「回答したか」から「必要水準を満たしたか」へ移しやすくなります。

サイバーリスクは財務・供給・信用の問題でもある

取引先のVPN機器やクラウド管理者アカウントが侵害されれば、攻撃者が発注企業の接続環境へ侵入するおそれがあります。受発注システムや生産管理システムを担う委託先がランサムウェア被害を受ければ、納品停止や代替調達費用が発生する可能性もあります。個人情報や設計情報を預ける先で漏えいが生じた場合、顧客説明や規制対応は委託先だけの問題では済みません。経営層は、SCS対応を情報システム部門の認証取得施策ではなく、事業継続と取引信用を守る施策として判断すべきです。

参考：経済産業省「サイバーセキュリティ経営ガイドライン Ver 3.0」、IPA「中小企業の情報セキュリティ対策ガイドライン 第4.0版」

対応しない場合に起こり得る問題

制度対応を先送りしただけで直ちに違法になるとは限りません。しかし、取引先管理が弱いままでは、事故後に「なぜ重要委託先を把握していなかったのか」「なぜ契約上の報告期限がなかったのか」「なぜ既知の未達を放置したのか」を説明できません。さらに、顧客や親会社からSCSマークを取引条件として求められた際、対象先の棚卸しから始めることになり、更新契約や新規案件に間に合わない可能性があります。

一方、要求水準を過度に高く設定すると、取引先の費用負担が増え、代替困難な技術・部材の供給者との関係を損なう可能性があります。重要なのは、事故ゼロを約束することではなく、リスクに比例した要求と、未達時の意思決定記録を残すことです。

対象となる取引先・システム・場面

管理対象は、ITベンダーだけに限定しません。個人情報・営業秘密・設計情報を扱う業務委託先、基幹システムやクラウドを運用する事業者、自社ネットワークに接続する保守会社、工場設備の遠隔保守先、物流・決済・コールセンターなど停止時の影響が大きい先が中心となります。再委託先や海外拠点を含めるかも、データフローと契約関係から判断します。

取引先SCS管理を構築する8つの手順

1. 経営方針と責任者を決める

取引先リスクの受容水準、★3・★4を求める基本方針、例外を承認できる役職を経営会議等で決めます。実務責任者は情報セキュリティ部門が担っても、取引継続の最終判断は事業責任者・調達責任者と共有します。

2. 取引先と委託内容を棚卸しする

契約台帳、支払先一覧、システム構成図、データフロー、外部接続一覧を照合します。取引先名だけでなく、提供サービス、委託データ、接続方式、再委託、代替可能性、契約更新月、インシデント連絡先を記録します。

3. 重要度を分類する

「機密性」「完全性」「可用性」「接続性」「代替困難性」の各観点で影響を評価します。取引金額が小さくても、管理者権限を持つ保守会社や単一供給源は高重要度となる可能性があります。

4. 必要な★と期限を設定する

一般的な脅威への基礎的対応を求める先には★3、高い事業影響、重要データ、特権接続、停止許容時間の短い先には★4を検討します。ただし制度文書、業界要請、契約責任を確認し、自社判断の基準として明文化します。

5. 取引先へ要請し、相談窓口を設ける

通知には、要請理由、対象範囲、求める★、期限、提出物、機密情報の送付方法、質問先、未達時の協議手順を記載します。一方的な通告では、誤解や形式対応を招きやすくなります。

6. 証跡と進捗を管理する

ステータスは「未案内、説明済、ギャップ分析中、改善中、申請中、取得済、例外承認、再評価予定」程度に統一します。担当者の主観的な「対応中」だけでなく、次の行動、期限、責任者、根拠資料を残します。

7. 未達企業を支援し、残存リスクを扱う

不足対策を重大度と実現難度で分け、短期是正、中期計画、代替統制に整理します。例えば多要素認証の即時導入が難しい場合、接続元制限、権限縮小、監視強化、利用時間制限を暫定策として検討します。

8. 年次更新と変更時レビューを行う

マーク取得だけで終了せず、契約更新、システム変更、再委託開始、M&A、重大インシデントの発生時に再評価します。取引先台帳とSCS台帳を分離すると更新漏れが起こるため、調達・契約のワークフローと連動させます。

重要度分類と★取得要請の判断基準

区分	典型例	基本方針	追加確認
重要度A	基幹・生産・決済、特権接続、重要データ、大規模停止影響	★4を軸に個別に判断します。取得までの移行計画を設定	第三者評価、技術検証、BCP、事故連絡、再委託
重要度B	業務SaaS、個人情報取扱、重要業務の一部委託	★3を基本に、影響が高ければ★4	適用範囲、改善計画、脆弱性管理、バックアップ
重要度C	機密情報や接続が限定的で代替可能	★要請の要否をリスクに基づき判断	最低限の契約条項、連絡先、定期見直し

※上表はLibrus株式会社による実務上の分類例であり、制度が全取引先に一律の★を指定するものではありません。自社の業種、規制、顧客要求、事業影響に合わせて調整します。

進捗管理台帳に必要な項目

最低限、取引先ID、契約・サービス名、事業オーナー、重要度、要求する★、現在の取得状況、適用範囲、有効性を確認した日、証跡の保管先、ギャップ、改善責任者、期限、暫定措置、残存リスク、例外承認者、次回レビュー日を記録します。証跡には機密情報が含まれる可能性があるため、閲覧権限、保存期間、暗号化、外部共有方法も決めます。

月次会議では、取得率だけをKPIにはしません。重要度Aの未達件数、期限超過、重大ギャップの平均滞留日数、暫定措置未実施件数、インシデント連絡先の確認率など、リスクが減ったかを示す指標を用います。

未達企業への支援方法

「排除」か「放置」かの二択にしない

未達先が代替困難である場合、取引停止は自社の供給リスクを高めます。まず、要求事項との差分を確認し、経営承認が必要な規程・体制、ツール導入が必要な技術対策、運用定着が必要な教育・訓練に分解します。そのうえで90日、180日などの改善計画を合意し、重大項目から是正します。期限内に取得できない場合は、対象データの削減、接続分離、権限の最小化、監視強化、バックアップ確認などで残存リスクを下げます。

診断・テストを目的に応じて使い分ける

Webアプリケーション診断は、取引先が提供するWebシステムの入力処理、認証、セッション、アクセス制御などを確認します。プラットフォーム診断は、サーバー、OS、ミドルウェア、ネットワーク機器の既知脆弱性や設定不備を確認します。ペネトレーションテストは、攻撃者の視点で複数の弱点を組み合わせ、重要資産へ到達できるかを検証します。SCSの証跡作成だけを目的に機械的に実施するのではなく、★4の技術検証や重大ギャップの有効性確認など、確認したいリスクから手法を選びます。

実施期間と費用を左右する要因

取引先管理の構築は、対象が数十社で台帳が整っていれば2〜3か月程度で初期設計できる場合があります。一方、数百社を超え、契約・システム・データの所在が分散している場合は、優先対象から段階導入する方が現実的です。制度側の審査期間や評価機関の稼働は別途考慮する必要があり、固定的な取得期間を約束することは適切ではありません。

費用は、対象取引先数、棚卸し精度、重要度評価の粒度、説明会や個別支援の回数、ギャップ分析の深さ、規程・契約改定、技術検証の範囲、複数拠点・海外対応、進捗管理ツール連携によって変わります。見積依頼では「SCS対応一式」ではなく、設計、展開、個社支援、診断、運用の各工程を分けると比較しやすくなります。

社内稟議とRFPで説明・確認すべき事項

稟議では事業損失と取引要請を起点にする

制度の概要だけでは予算判断につながりにくい傾向があります。重要委託先の停止許容時間、預託データ、外部接続、代替調達日数、顧客からの要求状況を示し、「どのリスクを、どの順番で、どこまで下げるか」を説明します。初年度に全社一斉導入せず、重要度Aから開始するロードマップも有効です。

RFP・見積依頼時の確認項目

- 制度文書と要求事項・評価基準を踏まえた支援範囲
- 発注企業側の取引先分類・管理プロセス設計の経験
- ★3の専門家確認、★4の第三者評価・技術検証との役割分担
- 診断結果を改善計画と運用へ接続できる体制
- 機密情報・個人情報の保管場所、再委託、削除方法
- 成果物、会議体、レビュー回数、追加費用条件
- 制度変更時の更新支援と、取得後の継続管理

サービス提供会社の選び方

重要なのは、制度説明ができることだけではありません。発注企業側の調達管理、取得企業側のギャップ改善、技術診断の三つをつなげられるかを確認します。成果物のサンプルでは、台帳や規程の体裁より、重要度の根拠、未達時の判断、改善後の検証まで追えるかを確認します。経営層向け報告と現場向け是正指示を分けて作成できることも重要です。

よくある失敗と注意点

全社一律で★4を要求する

リスクに比べ要求が過大となり、取引先の反発や形式対応を招きます。重要度分類と例外ルールを先に作ります。

取得マークだけで安全と判断する

評価には適用範囲があります。自社との取引に関係する拠点、システム、サービスが範囲内か確認します。

調達部門だけで運用する

技術的妥当性を判断できず、情シスだけでは取引継続を決められません。部門横断の責任分担が必要です。

未達先へ期限だけ通知する

原因が予算、人材、規程、技術のどこにあるか把握できず、改善が進みません。個社別のギャップと支援メニューを用意します。

診断を一度実施して終了する

システム変更や新たな脆弱性で状態は変わります。再診断、継続監視、教育、インシデント演習へつなげます。

Librus株式会社が提供できる支援

Librus株式会社は、SCS評価制度に関する現状把握、適用範囲の整理、取引先重要度分類、★取得要請方針、管理台帳・会議体・例外承認の設計、個社説明、ギャップ分析、改善ロードマップまで一気通貫で支援します。制度対応だけでなく、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、インシデントレスポンス、教育・訓練を組み合わせ、発見した課題を改善・運用までつなげます。

経営上の事業継続・取引信用と、現場のアクセス制御・脆弱性管理を同じリスク軸で整理できる点が特長です。大企業の統制要件と、中堅・中小取引先の人員・予算制約の双方を踏まえ、過不足のない個別設計を行います。

よくある質問

Q1. すべての取引先にSCSマーク取得を求めるべきですか？

一律要請は推奨しません。委託情報、外部接続、事業停止影響、代替可能性などで重要度を分類し、対象と水準を決めます。

Q2. ★3と★4はどう使い分けますか？

★3は一般的な脅威への対応水準、★4は被害拡大防止や第三者評価・技術検証まで含みます。重要データ、特権接続、停止影響が大きい取引先では★4を検討します。

Q3. 取引先が期限までに取得できない場合は？

未達理由と重大ギャップを確認し、改善期限、暫定措置、責任者を合意します。例外は期限付きで承認し、残存リスクと再評価日を記録します。

Q4. ISO 27001を取得済みならSCS確認は不要ですか？

制度や適用範囲、評価観点が同一とは限りません。既存認証を証跡として活用しつつ、自社取引に必要な範囲とSCS要求との差分を確認します。

Q5. Web診断やペネトレーションテストは必須ですか？

対象となる段階、評価・技術検証の具体的な要件、およびリスクによって異なります。診断を先に決めず、守る資産と確認目的から手法を選びます。

Q6. 管理の主管部門はどこが適切ですか？

セキュリティ部門または情報システム部門が制度・技術を統括し、調達が契約・台帳、事業部が重要度と継続判断、法務が条項と事故対応を担う形が現実的です。

Q7. どの程度の期間を見込むべきですか？

対象数と台帳整備状況に左右されます。重要先の選定、基準設計、試行、展開の順で進め、制度側の審査・評価期間は別に見込みます。

Q8. 制度の詳細が更新された場合はどうしますか？

IPAの公式ページ、基本規程、要求事項・評価基準を定期確認し、契約条項、社内基準、取引先案内を版管理します。

まとめ｜SCS評価制度を「取引先の継続管理」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）を実務で機能させる鍵は、★取得率ではなく、重要な取引先の残存リスクを把握し、改善を継続できることにあります。発注企業は、①棚卸し、②重要度分類、③★と期限の設定、④証跡・進捗管理、⑤未達支援、⑥例外承認、⑦定期見直しを一つの業務フローとして設計すべきです。

制度の詳細は今後も更新される可能性があります。最新の公式文書を確認しながら、最初から全取引先を完璧に管理しようとせず、事業影響の大きい委託先から段階的に始めることが、現実的かつ説明可能な進め方となります。

制度対応と技術対策を一体で進めたい企業へ

SCS評価制度への対応に加え、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実施範囲が決まっていない場合もご相談いただけます。制度上の要求と実際の攻撃リスクを結び付けることで、過不足の少ない対策計画と予算化につなげることが可能となります。

監修者

鎌田光一郎：青山学院大学法学部を卒業しました。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しました。金融機関に対するコンサルティング業務に従事しました。その後、Librus株式会社を設立、代表取締役に就任しました。

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

主な参考資料

- 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」
- IPA「SCS評価制度の詳細情報」
- IPA「要求事項・評価基準」
- IPA「中小企業の情報セキュリティ対策ガイドライン 第4.0版」
- 経済産業省「サイバーセキュリティ経営ガイドライン」