SCS評価制度は大企業だけではない｜中堅・中小企業に対応が求められる理由

メタディスクリプション：SCS評価制度は大企業だけの制度ではありません。元請・一次請けから取得要請が波及する仕組みと、中堅・中小企業が今から進める準備を実務目線で解説します。

導入文

結論からいえば、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（以下「SCS評価制度」）は、大企業だけを対象とする制度ではありません。業種や企業規模を問わず、サプライチェーンを構成する企業が対象になり得ます。とりわけ、従業員100〜1,000名規模で、大企業の業務、システム運用、製造、物流、ソフトウェア開発などを受託する企業は、早めに準備を始める意義が大きいといえます。

SCS評価制度そのものは任意制度であり、国がすべての企業に★の取得を一律に義務付けるものではありません。しかし制度は、委託元が取引契約などで委託先に適切な段階（★）を示し、対策の実施と確認を促す使い方を想定しています。そのため、法令上の義務ではなくても、入札、取引開始、契約更新、委託先審査の条件として対応を求められる可能性があります。

本稿では、元請・一次請けから取引先へ取得要請が波及する構造を整理し、中堅・中小企業が何を、どの順番で準備すべきかを解説します。制度開始前の現段階で重要なのは、製品を急いで買うことではありません。対象範囲を定め、現状と要求事項の差を把握し、経営判断を伴う改善計画を作ることです。

この記事で分かること

この記事を読むと、SCS評価制度が中堅・中小企業にも関係する理由、★3と★4の基本的な違い、取引先から要請を受ける前に整えておくべき資料、Webアプリケーション診断やプラットフォーム診断、ペネトレーションテストの位置づけ、準備期間と費用を左右する要因が分かります。さらに、社内稟議、ベンダー選定、改善後の運用まで、実務上の進め方を把握できます。

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セキュリティ対策状況を共通基準で評価し、可視化する仕組みです。経済産業省と内閣官房国家サイバー統括室が制度構築を進め、独立行政法人情報処理推進機構（IPA）が運営します。★3と★4は2027年3月頃の運用開始が予定されています。制度の詳細や様式は今後も更新され得るため、実際の申請時にはIPAの最新版を確認する必要があります。

背景には、委託元が取引先の対策状況を外部から判断しにくい一方、委託先は顧客ごとに異なるチェックシートへの回答を繰り返しているという双方の負担があります。共通の基準で対策状況を示せれば、発注側は取引リスクを判断しやすくなり、受注側も説明を標準化しやすくなります。

制度の直接的な対象は、クラウド環境を含む企業のIT基盤です。一般にIT基盤に該当しない製造設備などの制御システム（OT）や、取引先へ提供する製品自体は直接の対象外とされています。ただし、それらに関するリスク対策が不要になるわけではありません。OTや製品については、該当する別の制度やガイドラインと組み合わせて管理することが必要です。

★3と★4の違いをどう理解するか

★3は、SCS評価制度の要求事項・評価基準に基づいて企業が自己評価を行い、所定の研修を受けたセキュリティ専門家の確認を経て申請する仕組みです。経営層による自己適合宣誓も求められる予定であり、情報システム部門だけで完結するチェック作業ではありません。

★4は、★3より広い範囲と高度な対策を対象とし、登録された第三者評価機関による評価を受ける仕組みです。技術検証を伴うため、規程があるかだけでなく、設定や運用が実際に機能しているかを示す証拠が重要になります。どの★を目指すかは、会社の規模だけでなく、委託業務の重要性、扱う情報、システム接続、停止時の影響、発注者の要求によって判断します。

なお、SCS評価制度は企業の優劣を競う格付け制度ではなく、対策の実施状況を可視化する制度です。また、特定のEDRや資産管理製品の購入が一律に必須となるわけでもありません。自社の環境とリスクに照らし、要求事項を満たす手段を選ぶことが基本です。

なぜ中堅・中小企業にも対応が求められるのか

最も大きな理由は、攻撃者が企業規模ではなく、サプライチェーン上の到達経路を見ているからです。大企業の防御が強固でも、保守会社、開発委託先、物流会社、会計・人事業務の受託先などが持つ認証情報や接続経路が侵害されれば、そこから委託元へ影響が及ぶ可能性があります。

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、8年連続で選出されています。また警察庁によれば、2025年に報告されたランサムウェア被害226件のうち143件は中小企業でした。これらはSCS評価制度の取得義務を示す数字ではありませんが、企業規模にかかわらず、侵害と事業停止のリスクが現実に存在することを示しています。

発注企業にとって、委託先の事故は『他社の問題』で終わりません。サービス停止、納期遅延、個人情報や営業秘密の漏えい、顧客への説明、代替調達、復旧費用などが自社へ波及します。経済産業省のサイバーセキュリティ経営ガイドライン Ver.3.0も、経営者が認識すべき原則としてサプライチェーン全体への目配りを示し、委託先との契約で役割と責任範囲を明確にすることを求めています。発注企業がSCS評価制度を取引先管理に使う流れは、この経営責任と整合します。

元請・一次請けから取得要請が波及する構造

要請は、発注元からすべての取引先へ一斉に広がるとは限りません。まず、重要データを扱う企業、発注元のネットワークへ接続する企業、停止すると供給継続に大きな影響が出る企業などに、一定の★や同等水準の対策が示されると考えられます。一次請けが業務の一部を再委託している場合、一次請け自身も再委託先のリスクを管理しなければなりません。このため、要求は二次請け、三次請けへ連鎖します。

例えば、大手メーカーが生産管理システムの運用をA社へ委託し、A社が監視や保守の一部をB社へ再委託しているとします。B社の端末からA社の環境へリモート接続できるなら、B社の認証管理や端末管理は大手メーカーの事業継続にも関係します。大手メーカーがA社に★4相当を求め、A社がB社に★3または同等の対策を求める構造は十分に想定できます。

また、★取得そのものを契約条件にしない場合でも、SCS評価制度の要求事項を委託先チェックシートやRFPに取り込む運用が考えられます。したがって、自社が直接大企業と契約していない、あるいは現時点で取得要請を受けていないという理由だけで、影響がないとは判断できません。主要顧客の業界、再委託関係、接続権限、保有データを確認する必要があります。

一方、発注者が一方的に過大な費用負担を押し付けてよいわけではありません。経済産業省は、★取得の契約上の扱いは当事者間で合意し、独占禁止法や中小受託取引適正化法（取適法）上、適切に制度を活用する必要があると説明しています。受注側は、要求範囲、期限、費用分担、契約価格への反映、再委託先に求める水準を具体的に協議することが重要です。

対応しない場合に起こり得る問題

SCS評価制度を取得していないだけで、直ちに取引が停止するわけではありません。しかし、発注者が合理的な理由から一定水準を契約条件や選定基準に定めた場合、未対応は新規入札での不利、追加質問や監査の増加、契約更新の遅延、取り扱える情報や接続権限の制限につながる可能性があります。重要なのは『★がないこと』だけでなく、対策状況と改善計画を説明できないことです。

インシデントが発生すれば、売上の減少だけでなく、復旧・調査費用、顧客通知、代替業務、法務対応、再発防止、保険対応が同時に発生します。受託業務が止まれば委託元の生産やサービスにも影響し、信用毀損や損害賠償の論点に発展することもあります。SCS対応は、認証マークを取るための費用ではなく、重要顧客との取引継続と事業継続を支える投資として稟議に載せるべきです。

どの企業・システムから優先して考えるべきか

優先度が高いのは、大企業や重要インフラ企業から業務を受託している企業、顧客の個人情報・設計情報・営業秘密を保有する企業、顧客環境へリモート接続する企業、SaaSやシステム開発・運用を提供する企業、停止時に代替が難しい部品やサービスを供給する企業です。IPO、M&A、金融機関からの審査、重要な取引先監査を控える企業も、対策状況を説明できるようにしておく価値があります。

対象範囲を決める際は、法人全体を機械的に一括評価するのではなく、組織、拠点、ネットワーク、クラウド、端末、委託業務、データの流れを整理します。ただし、都合のよい狭い範囲だけを切り出すと、共通ID基盤、管理端末、バックアップ、委託先接続などの重要な依存関係を見落とします。『どこが侵害されると対象業務へ影響するか』を基準に境界を設定します。

SCS評価制度への具体的な対応手順

最初に経営層が、対応目的と責任者を決めます。目的は、主要顧客の要請への対応、取引継続、新規受注、事業継続、監査対応など、経営課題の言葉で定義します。同時に、★3と★4のどちらを想定するか、対象業務と拠点、予算、期限、許容できるリスクを仮決定します。顧客の要求が不明な場合は、調達部門や取引窓口を通じて、想定する★、適用時期、対象契約を確認します。

次に、情報システム部門と関係部門が証拠資料を集めます。最低限、組織図、情報セキュリティ規程、資産台帳、ネットワーク構成図、クラウド・SaaS一覧、アカウントと権限の管理手順、ログ管理、脆弱性・パッチ管理、バックアップと復旧手順、インシデント対応計画、教育記録、委託先一覧・契約、過去の診断結果と改善記録を準備します。規程だけでなく、申請、承認、設定画面、チケット、訓練記録など、運用の実態を示す証跡が必要です。

その後、要求事項とのギャップ分析を行います。各項目を『対応済み』『一部対応』『未対応』『非該当』に分け、根拠と責任者を明記します。非該当とする場合は理由を残します。未対応項目は、攻撃の起こりやすさ、影響の大きさ、顧客要求、是正に必要な期間を踏まえて優先順位を付けます。

技術面では、設定確認だけでなく、外部から到達できるWebサイトやAPIにはWebアプリケーション診断、サーバー・ネットワーク機器・クラウド設定にはプラットフォーム診断を検討します。Webアプリケーション診断は認証や入力処理などアプリ固有の弱点を、プラットフォーム診断はOS、ミドルウェア、ネットワーク、クラウド構成の弱点を確認するものです。

さらに、重要システムについて攻撃経路全体の実効性を確認したい場合は、ペネトレーションテストが有効です。これは、許可された範囲で攻撃者と同様の手法を用い、侵入や権限拡大、重要情報への到達可能性を検証する試験です。ただし、診断やペネトレーションテストを一度実施するだけでSCS対応が完了するわけではありません。制度は、ガバナンス、教育、委託先管理、検知、対応、復旧なども含む総合的な管理を扱います。

改善計画では、短期、中期、継続運用に分けます。初期設定の是正、多要素認証、不要アカウントの削除などは短期で進めやすい一方、ネットワーク分離、ログ基盤、バックアップ再設計、規程改定、委託先契約の見直しには時間がかかります。各施策に責任者、期限、予算、完了条件、確認方法を設定し、経営会議で残存リスクを承認します。最後に、想定する評価方式に合わせて自己評価、専門家確認または第三者評価へ進みます。

実施期間と費用を左右する要因

準備期間は企業ごとの差が大きく、一律の標準期間を示すことは適切ではありません。すでにISMSや顧客監査を運用し、資産台帳や証跡が整っている企業と、規程や担当者が未整備の企業では必要な作業が異なります。制度開始から逆算するなら、まず数週間程度で対象範囲と現状を把握し、その結果に基づいて改善工程を見積もる進め方が現実的です。システム改修や調達、規程承認を伴う場合は、半期または年度の予算策定を待たず、段階的に着手する必要があります。

費用を左右する主な要因は、対象拠点・システム・アカウント数、目指す★、既存規程と運用の成熟度、クラウドや海外拠点の有無、技術検証の範囲、診断対象の画面数・IP数、改善実装を外部へ委託する範囲です。見積りでは、評価支援費だけでなく、規程整備、技術対策、教育、診断、再確認、継続運用の費用を分けて示してもらうと、社内説明がしやすくなります。

社内稟議では、制度対応費を単独で示すのではなく、守るべき売上、主要顧客との契約更新時期、事故時の停止影響、既存施策との重複、翌年度以降の運用費を記載します。『なぜ今か』に対しては、制度開始直前に人材や評価枠が集中する可能性、改善に調達・承認期間を要すること、顧客からの要請後では期限を選びにくいことを説明するとよいでしょう。

成果物と改善の優先順位

支援会社から受け取る成果物には、対象範囲、前提条件、要求事項ごとの評価、根拠資料、発見事項、リスク、改善案、優先順位、責任部署、期限、概算負荷を含めるべきです。経営層向けには、取引・財務・事業継続への影響を要約した資料が必要です。現場向けには、具体的な設定変更や運用手順まで落とし込まれていることが望まれます。

優先順位は、単純に未対応項目の数で決めません。外部公開されている、特権権限がある、顧客環境に接続する、機密情報を大量に扱う、バックアップから復旧できない、といった重大な経路を先に是正します。診断で見つかった脆弱性も、深刻度スコアだけでなく、実際の攻撃可能性、情報価値、代替策、事業影響を合わせて判断します。改善後は再診断または設定再確認を行い、残存リスクを記録します。

SCS対応を支援する会社の選び方

支援会社を選ぶ際は、制度資料を説明できるだけでなく、要求事項を実際の規程、運用、技術対策へ落とし込めるかを確認します。RFPや見積依頼には、想定する★、対象組織、対象システム、希望時期、既存認証、顧客要求、必要な成果物、改善実装の要否、診断の要否を記載します。分からない項目は未定とし、スコーピング支援を依頼して構いません。

確認したい点は、SCS評価制度に関する支援範囲、担当者の資格と実務経験、評価と改善支援の役割分担、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の対応能力、再診断、緊急時支援、機密情報の保管と削除、再委託、報告書のサンプル、追加費用の条件です。★4の評価を依頼する場合は、IPAが公表する登録状況と、評価の独立性に関する条件も確認します。

秘密保持契約だけで安心せず、資料の受渡方法、アクセス権、保存場所、保存期間、作業端末、作業ログ、廃棄証明、事故時の連絡期限を合意します。特に構成図、脆弱性情報、認証方式は攻撃に悪用され得るため、閲覧者を必要最小限に限定します。

よくある失敗と注意点

第一の失敗は、チェックリストを埋めること自体を目的にすることです。規程上は実施することになっていても、退職者アカウントが残り、バックアップ復旧を試したことがなければ、実効性は十分とはいえません。担当者へのヒアリング、証跡確認、技術検証を組み合わせる必要があります。

第二の失敗は、情報システム部門へ丸投げすることです。予算、人員、取引条件、リスク受容、委託先契約は経営判断を伴います。経営層、情報システム部門、法務・調達、事業部門が責任を分担しなければ、申請直前に承認が止まります。

第三の失敗は、認証取得後の運用を設計しないことです。人事異動、クラウド追加、システム更新、脆弱性の公表によりリスクは変化します。資産台帳、権限棚卸し、教育、パッチ、ログ監視、バックアップ試験、インシデント訓練、委託先確認を年間計画に組み込みます。

第四の失敗は、制度開始前の不確かな説明をうのみにすることです。IPAは不適切な勧誘への注意喚起も行っています。現時点で評価機関やSCSセキュリティ専門家の公表は今後予定されているため、『必ず取得できる』『指定済み』といった説明は、公的情報で確認してください。

Librus株式会社が提供できる支援

Librus株式会社は、SCS評価制度への対応方針の整理から、対象範囲の設定、要求事項とのギャップ分析、規程・運用の整備、技術的な検証、改善計画、継続運用まで一気通貫で支援します。経営層には取引・財務・事業継続の観点で、情報システム部門には具体的な証跡と実装の観点で説明し、社内の合意形成を進めます。

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、SOC／CSIRT構築・運用支援、インシデントレスポンス、デジタルフォレンジック、教育・訓練などを組み合わせます。診断結果を報告して終えるのではなく、企業ごとのシステム、予算、人員、顧客要求に応じて改善の優先順位を設計し、運用へ定着させることを重視しています。

大企業向けの高負荷な仕組みをそのまま導入するのではなく、必要な水準を保ちながら、既存の規程、ツール、委託サービスをできるだけ活用します。SCS評価制度への対応だけでなく、M&A、IPO、取引先監査などの重要局面も見据え、技術と経営の両面から整理できる点がLibrus株式会社の強みです。

よくある質問

SCS評価制度は中小企業にも義務ですか？

国がすべての中小企業へ取得を義務付ける制度ではなく、任意制度です。ただし、発注者が取引契約、入札、委託先審査などで一定の★または同等水準を求める可能性があります。主要顧客の方針を早めに確認してください。

取得しないと取引を停止されますか？

未取得だけで自動的に取引停止になる制度ではありません。契約上の扱いは当事者間で合意されます。要請を受けた場合は、必要性、期限、費用負担、代替的な確認方法を協議し、改善計画を提示することが重要です。

★3と★4のどちらを選ぶべきですか？

会社規模だけでは決まりません。扱う情報、顧客環境への接続、停止時の影響、委託業務の重要性、顧客要求を基に判断します。顧客指定がなければ、リスク分析とギャップ分析を行って適切な段階を選びます。

ISMSを取得していればSCS対応は不要ですか？

不要とは限りません。ISMSとSCS評価制度は相互補完的に位置づけられています。既存のISMS文書や運用証跡は活用できますが、SCSの要求事項・評価基準との差分確認が必要です。

SCS対応には特定のセキュリティ製品が必要ですか？

制度は特定製品の導入を一律には求めていません。既存の仕組みで要求事項を満たせる場合もあります。製品選定より先に、対象範囲とリスク、現状の運用を確認してください。

脆弱性診断を受ければ取得できますか？

診断だけで完了するものではありません。診断は技術的な弱点を確認する重要な手段ですが、ガバナンス、資産管理、権限管理、教育、委託先管理、インシデント対応、復旧なども整える必要があります。

準備はいつから始めるべきですか？

顧客から正式要請を受ける前が望ましい時期です。まず対象範囲と現状を短期間で把握し、予算やシステム改修が必要な項目を早期に特定します。2027年3月頃の運用開始予定から逆算して計画してください。

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。業務、取引関係、データ、システム接続、停止影響を整理し、合理的な対象範囲と想定する★を決める段階から専門家の支援を利用できます。

まとめ｜SCS評価制度は取引継続の共通言語になる

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、大企業だけの制度ではありません。任意制度であっても、元請・一次請けが契約や委託先審査で活用すれば、要求は二次請け以降へ波及します。中堅・中小企業に必要な

のは、要請を待って製品を買うことではなく、主要顧客との関係、重要業務、データ、接続経路を把握し、要求事項とのギャップを計画的に埋めることです。

経営層は取引継続と事業継続の観点から目的、責任者、予算を決め、情報システム部門は資産・規程・運用証跡を整えます。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を使い分け、改善後も再確認と継続監視を行います。早めの準備は、顧客からの照会に答える力を高めるとともに、自社の事故リスクを下げる機会になります。

Librus株式会社へのご相談

SCS評価制度の準備状況を一度整理しませんか

取引先から具体的な要請が届く前に、対象業務、システム、現状の対策、必要な改善を整理しておくと、予算化と顧客説明を進めやすくなります。Librus株式会社では、想定する★や対象範囲が決まっていない段階から、スコーピングとギャップ分析をご相談いただけます。

取引先からの要請に、実行可能な計画で応えるために

SCS対応では、短期間にすべてを入れ替えるのではなく、重要なリスクから優先して改善することが大切です。Librus株式会社は、顧客要求の読み解き、社内稟議、規程整備、技術対策、診断、改善後の確認まで支援し、説明可能なロードマップづくりをお手伝いします。

制度対応と実効性のあるセキュリティを両立

★の取得だけを目的にすると、運用負荷や形骸化が残りかねません。Librus株式会社は、既存の規程やツールを活かしながら、事業継続と取引先の信頼につながる対策を個別に設計します。まずは現状確認だけ、診断の要否だけといったご相談にも対応します。

参考資料・出典

制度の詳細は更新される可能性があります。公開・申請時には、以下の公的機関による最新版をご確認ください。

- 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）
- IPA：SCS評価制度 公式サイト
- IPA：SCS評価制度の詳細情報
- IPA：要求事項・評価基準
- IPA：SCS評価制度 よくある質問
- 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：情報セキュリティ10大脅威 2026
- 警察庁：令和7年におけるサイバー空間をめぐる脅威の情勢等について

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