

SCS評価制度対応チェックリスト | 自社のセキュリティ対策を簡易診断

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）への対応を検討していても、「自社は何ができていて、何が足りないのか分からない」という企業は少なくありません。特に従業員100～1,000名規模では、情報システム部門が日常運用を担いながら、経営層への説明、取引先からのセキュリティチェック、規程整備、脆弱性対応まで並行して進めているケースも多くあります。

結論からいえば、SCS評価制度への準備は、申請書を作り始めることからではなく、「適用範囲を決める」「現状を棚卸しする」「不足を優先順位付けする」「証跡を残せる運用にする」という順番で進めるのが実務的です。本記事では、制度の7つの主要領域を踏まえ、経営層・情報システム部門が自社の状態を簡易診断できるチェックリストとして整理します。

この記事で分かること

- SCS評価制度と★3の基本的な位置付け
- 自社の現状を短時間で把握するための簡易チェック項目
- 不足が見つかった場合の優先順位の付け方と改善手順
- 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どこで活用するか
- 社内稟議、費用、期間、外部支援会社選定で確認すべきポイント

SCS評価制度とは | サプライチェーンの対策水準を共通化する制度

SCS評価制度は、取引先を含むサプライチェーン全体のセキュリティ水準を可視化し、委託元と委託先の間で求める対策水準を分かりやすく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2026年3月に制度構築方針を公表し、独立行政法人情報処理推進機構（IPA）が制度を運営します。IPAは★3・★4について2027年3月頃の運用開始を予定しています。

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

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>

★3は、一般的なサイバー脅威に対処し得る水準として位置付けられています。取得希望組織が自己評価を行い、SCSセキュリティ専門家による確認を受けたうえで、経営層による自己適合宣誓を含めて申請する「専門家確認付き自己評価」です。★4のような第三者評価・技術検証とは仕組みが異なります。なお、★3・★4の取得には、それぞれで定められた要求事項・評価基準をすべて満たす必要があるとIPAが公表しています。

出典：IPA「よくある質問」<https://www.ipa.go.jp/security/scs/faq.html>

なぜ今、自社のセキュリティ対策をチェックしておくべきなのか

SCS評価制度は法令上すべての企業に取得を義務付ける制度ではありません。しかし、制度は2社間の取引契約等で、委託元が委託先に必要な★の水準を示し、対策実施状況を確認することを想定しています。つまり、自社が制度対応を先送りしていても、主要顧客の調達基準や委託先管理方針の変更によって、短期間で対応を求められる可能性があります。

取引先から回答期限付きで対応状況の提出を求められた後に、端末台帳、ネットワーク構成、アクセス権限、バックアップ、委託先管理、インシデント対応手順を一から確認すると、複数部門との調整が必要になります。セキュリ

ティ対策は製品を購入すれば終わるものではなく、規程、責任者、実施記録、教育、例外管理まで含めて運用として定着させる必要があるためです。

SCS評価制度対応チェックリスト | まず自社を簡易診断

以下は、SCS評価制度の公表資料に示されている主要領域を踏まえ、準備状況を把握するためにLibrus株式会社が実務向けに整理した簡易チェックリストです。正式な要求事項・評価基準そのものではなく、★取得の適合判定を保証するものでもありません。正式な評価ではIPAが公表する最新の要求事項・評価基準を確認してください。

1. ガバナンスの整備

観点	簡易チェック項目	確認
経営責任	情報セキュリティに関する経営責任者と実務責任者が明確になっている	☐
方針	情報セキュリティ基本方針や主要ルールが文書化され、社内に周知されている	☐
報告	重大な脆弱性やインシデント、主要リスクが経営層に報告される仕組みがある	☐
証跡	会議記録、承認記録、改定履歴など、実施したことを説明できる証跡が残っている	☐

2. 取引先管理

観点	簡易チェック項目	確認
接続関係	顧客、委託先、クラウド事業者等とのシステム接続や情報授受を把握している	☐
契約	機密情報の取り扱い、事故時の報告、責任分担などを契約・規程で定めている	☐
連絡体制	インシデント発生時に連絡すべき取引先と社内責任者が分かる	☐
終了時	契約終了・委託終了時のアカウント削除やデータ返却・消去の手順がある	☐

3. リスクの特定

観点	簡易チェック項目	確認
資産台帳	PC、サーバー、ネットワーク機器、クラウドサービスなどの台帳が更新されている	☐
情報資産	機密情報・個人情報・顧客データがどこに保存されているか把握している	☐
構成把握	ネットワーク構成やインターネット公開システムを一覧化している	☐
リスク評価	重要資産について、脅威・脆弱性・事業影響を踏まえたリスク評価を行っている	☐

4. 攻撃等の防御

観点	簡易チェック項目	確認
ID管理	入社・異動・退職に応じてIDの発行、変更、削除が行われる	☐
認証	管理者アカウントや重要クラウドサービスで多要素認証を活用している	☐
権限	最小権限を原則とし、不要な管理者権限や共有IDを定期的に見直している	☐
脆弱性・更新管理	OS、ミドルウェア、ネットワーク機器等の脆弱性情報を収集し、優先度に応じて更新している	☐
マルウェア対策	端末のマルウェア対策、EDR等の検知・防御機能を運用している	☐
境界防御	VPN、ファイアウォール、公開ポート、管理画面など外部境界の設定を把握している	☐
バックアップ	重要データのバックアップを取得し、復元できることを確認している	☐
教育	標的型メール、認証情報詐取、情報持ち出し等を想定した教育を継続している	☐

5. 攻撃等の検知

観点	簡易チェック項目	確認
監視	重要システム、認証、ネットワーク等の異常を検知できる仕組みがある	☐
ログ	必要なログを取得・保管し、事故時に調査できる状態になっている	☐
判断	アラート発生時に誰が確認し、何を基準にエスカレーションするか決まっている	☐

6. インシデントへの対応

観点	簡易チェック項目	確認
初動	感染端末の隔離、アカウント停止、ネットワーク遮断などの初動手順がある	☐
役割	経営、情シス、法務、広報、営業などの役割と意思決定者が決まっている	☐
連絡	顧客、委託元、関係機関等への報告判断と連絡先が整理されている	☐
訓練	机上演習や連絡訓練を行い、手順が実際に機能するか確認している	☐

7. インシデントからの復旧

観点	簡易チェック項目	確認
復旧優先度	停止した場合に事業影響が大きいシステムを特定し、復旧優先順位を決めている	☐
復元確認	バックアップからの復元テストや代替手段の確認を行っている	☐

観点	簡易チェック項目	確認
改善	事故・障害・訓練後の振り返りを行い、規程や設定を更新している	□

チェック結果の読み方 | 点数化より「未対応の理由」を確認する

この簡易診断では、チェック数の多さだけで成熟度を判断しないことが重要です。同じ「未対応」でも、①ルールがない、②ツールはあるが運用されていない、③運用しているが証跡がない、④対象範囲が不明確、では対応方法が異なります。まず未対応項目ごとに原因を分け、事業影響と攻撃可能性を踏まえて優先順位を付けます。

優先度を高くすべき典型例は、インターネット公開システムの重大な脆弱性、管理者アカウントの多要素認証未導入、退職者IDの残存、バックアップから復元できるか未確認、重要取引先への事故連絡手順が不明確、といった項目です。これらは一つの不備が侵入、権限拡大、被害拡大、復旧遅延につながる可能性があるため、規程整備だけではなく技術対策と運用確認をセットで進めます。

具体的な対応手順 | 簡易診断から改善計画まで

Step 1 適用範囲を決める

対象会社、拠点、部門、クラウド、ネットワーク、端末、インターネット公開システムを整理します。最初に対象範囲を曖昧にすると、後から「このSaaSは誰が管理しているのか」「子会社の端末は対象か」といった手戻りが起きます。

Step 2 資料と証跡を集める

規程、資産台帳、アカウント一覧、ネットワーク構成図、クラウド一覧、バックアップ設定、教育記録、インシデント対応手順、委託先契約などを集めます。情報システム部門だけで揃わない資料は、総務、人事、法務、購買、営業にも協力を依頼します。

Step 3 要求事項とのギャップを整理する

「適合」「一部対応」「未対応」「要確認」などの状態に分け、根拠資料と担当部署を紐付けます。チェックリストを埋めること自体を目的にせず、実際の運用と文書の内容が一致しているかを確認します。

Step 4 技術的な弱点を確認する

公開WebシステムにはWebアプリケーション診断、サーバーやネットワーク機器にはプラットフォーム診断を活用すると、設定不備や既知脆弱性を具体的に把握できます。複数システムを横断した侵入経路や攻撃成立性まで確認したい場合は、ペネトレーションテストを検討します。★3の取得手続そのものが一律にこれらの診断を必須とする、という意味ではありません。自社の実装状況を確認し、優先順位を付けるための手段として活用します。

Step 5 改善ロードマップを経営判断につなげる

改善項目を「直ちに実施」「3か月以内」「次期予算で対応」などに分け、費用、担当、期限、取引先への影響を明確にします。経営層には技術用語だけでなく、取引継続、業務停止、顧客データ、信用、復旧コストへの影響として説明すると意思決定しやすくなります。

実施期間と費用を左右する要因

SCS評価制度対応に必要な期間は、従業員数だけでは決まりません。拠点数、対象システム数、クラウド利用数、規程の整備状況、資産台帳の精度、未対応事項の多さ、経営承認のリードタイム、外部ベンダーとの調整有無によって大きく変わります。簡易診断だけであれば短期間でも可能ですが、規程の改定、MFA展開、ネットワーク変更、パッチ運用の再設計、バックアップ方式の見直しなどが必要になると、複数月単位で計画することが現実的です。

費用も同様に、申請・登録費だけではなく、ギャップ分析、専門家確認、規程整備、ツール導入、設定変更、脆弱性診断、教育、再確認などの対応範囲で変動します。IPAが2026年9月18日に公表した料金設定では、★3登録希望組織の登録料は2028年3月31日まで1年分10,000円、2028年4月1日以降は1年分20,000円です。ただし、これは登録料であり、外部支援や改善施策に必要な費用とは別です。

出典：IPA「SCS評価制度 料金設定のお知らせ」

<https://www.ipa.go.jp/security/scs/rcu1hd00000075om-att/pricelist.pdf>

社内稟議で説明すべきポイント

稟議では「SCS評価制度に対応したい」という制度名だけで説明するより、なぜ今着手するのかを経営課題に置き換えることが重要です。主要顧客から将来取得を求められる可能性、取引先セキュリティチェックへの回答負荷、事故時の事業停止・信用毀損、M&AやIPO、重要顧客との契約更新でセキュリティ状況の説明が必要になる可能性などを整理します。

そのうえで、「現状診断→優先改善→専門家確認→申請準備」という段階に分けて予算化すると、最初から大規模投資を求めるよりも社内合意を得やすくなります。経営層が判断すべき事項は、目指す★の水準、対象範囲、期限、許容できるリスク、対策予算、社内責任者です。情報システム部門は、それを実現するための資産・設定・運用・証跡を整理します。

サービス提供会社の選び方 | チェックリスト作成だけで判断しない

- 制度の要求事項と評価スキームを最新情報で理解しているか
- 規程・ガバナンスだけでなく、ネットワーク、クラウド、認証、脆弱性まで技術面を確認できるか
- 指摘事項を重要度・事業影響・対応コストで優先順位付けできるか
- 改善策の設計、実装、再確認まで支援範囲を明確にできるか
- 個人情報や機密情報の受領方法、保管、削除、再委託条件が明確か
- RFPや見積書で対象範囲、成果物、前提条件、追加費用、スケジュールを明示できるか

成果物についても確認が必要です。少なくとも、現状評価、根拠資料、ギャップ一覧、リスク・優先度、改善案、担当部門、目安時期が整理されていれば、その後の社内説明や予算化に利用しやすくなります。脆弱性診断を実施する場合は、検出内容だけでなく、再現条件、影響、推奨対策、再診断結果まで確認できる報告形式が望まれます。

よくある失敗と注意点

チェックリストを担当者一人で埋める

SCS評価制度の領域は経営、人事、法務、購買、情報システム、現場運用にまたがります。担当者の認識だけで「できている」と判断すると、証跡や実運用との不一致が残ります。

ツール導入を適合と同一視する

MFA、EDR、資産管理ツールなどは有効ですが、特定製品を導入しただけで制度対応が完了するわけではありません。経済産業省も、評価基準達成に特定のセキュリティ対策製品の導入を必須としていないと説明しています。

規程だけ整えて設定を確認しない

ルール上はパッチ適用、アクセス制御、バックアップを実施することになっていても、実際の設定が異なっているケースがあります。文書と技術の両方を確認することが必要です。

証跡を後から集めようとする

正式な確認時に、教育記録、アカウントレビュー、承認履歴、バックアップテストなどが残っていなければ、実施状況を説明しにくくなります。日常運用の中で証跡が自然に残る仕組みにしておくことが重要です。

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評価制度に向けた現状整理から改善・運用まで、一気通貫で支援します。企業ごとのシステム構成、取引先要件、社内体制、予算に応じて対象範囲を設計し、経営面と技術面を分けずに課題を整理できる点が特徴です。

具体的には、要求事項とのギャップ分析、規程・体制・証跡の整備支援、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、セキュリティ教育、SOC／CSIRT構築・運用支援などを組み合わせられます。診断で問題を発見するだけでなく、改善方針、優先順位、運用への落とし込みまで支援することで、「評価対応用の資料」と「実際に機能するセキュリティ対策」が乖離しない状態を目指します。

よくある質問

Q1. このチェックリストで全て「はい」なら★3を取得できますか？

いいえ。本記事のチェックリストは準備状況を把握するための簡易診断です。正式な★3取得では、IPAが公表する要求事項・評価基準を満たし、所定の評価・申請プロセスを経る必要があります。

Q2. SCS評価制度への対応は義務ですか？

制度自体は任意です。ただし、実際の取引では委託元・取引先が契約条件や調達条件として一定の★取得を求める可能性があります。

Q3. ISMSを取得していればSCS評価制度への追加対応は不要ですか？

自動的に不要になるとは限りません。SCS評価制度は代表的な脅威を踏まえたベースライン型の評価で、ISMSとは相互補完的な位置付けです。既存のISMS規程や運用を活用できる部分を確認したうえで、SCS固有の要求事項との差分を整理することが必要です。

Q4. ★3に脆弱性診断やペネトレーションテストは必須ですか？

★3の評価スキームは専門家確認付き自己評価であり、★4のように制度上の技術検証を必須とする仕組みではありません。ただし、自社の技術的な弱点を把握し、対策の実効性を確認する方法として脆弱性診断やペネトレーションテストは有効です。

Q5. まず何から着手すべきですか？

適用範囲とIT資産の把握から始めることを推奨します。対象が分からなければ、アカウント、パッチ、バックアップ、ログなどの確認対象も決められないためです。

Q6. 情報システム部門だけで対応できますか？

技術面は中心的に担当できますが、経営責任、教育、人事手続、契約、委託先管理、事故時の対外連絡などは他部門との連携が必要です。

Q7. 申請までどれくらいかかりますか？

企業の現状によって異なります。規程・資産台帳・認証・バックアップ等が整っている企業と、棚卸しから必要な企業では期間が大きく変わります。取引先から期限を示される前にギャップ分析だけでも実施しておく、必要期間を見積もりやすくなります。

Q8. 外部支援を依頼するタイミングはいつが良いですか？

対象範囲が未確定の段階でも相談可能です。むしろ、最初の適用範囲や優先順位を誤ると手戻りが生じるため、社内だけで判断が難しい場合は初期段階で専門家を交える方法が有効です。

まとめ | SCS評価制度対応は「現状の見える化」から始める

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）への準備では、いきなり申請を目指すのではなく、自社の対策状況をガバナンス、取引先管理、リスク特定、防御、検知、対応、復旧の観点で見える化することが第一歩です。

簡易チェックで未対応が多くても、すべてを同時に改善する必要はありません。重要資産や外部公開システム、管理者アカウント、バックアップ、インシデント対応など、事業継続や取引先への影響が大きい項目から着手します。制度対応をきっかけに、規程・技術・運用を一体で見直すことで、取引先への説明力と実際のセキュリティ水準の両方を高めやすくなります。

SCS評価制度対応の現状整理からご相談いただけます

「どの範囲を対象にすべきか決まっていない」「自社が★3水準にどの程度近いかわかりたい」「取引先から求められる前に不足を把握したい」といった段階でも、Librus株式会社へご相談いただけます。要求事項とのギャップ整理だけでなく、規程・体制、脆弱性、認証、ネットワーク、バックアップ、教育、インシデント対応まで横断して確認することで、優先して投資すべき項目と、既存運用を活用できる項目を切り分けやすくなります。

対象範囲や実施方法が固まっていない場合も、現状を確認しながら進め方を整理できます。限られた予算と社内リソースの中で、取引先対応と実効性のあるセキュリティ対策を両立させたい場合はご相談ください。

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>