# SCS評価制度で求められるリスクアセスメントとは？実施手順と評価のポイント

SCS評価制度への対応を進める際、リスクアセスメントは「自社にどのような危険があり、何を優先して対策するか」を決めるための土台です。特に★4では、大分類「リスクの特定」の中に「リスクアセスメント」が位置付けられ、脆弱性情報・脅威情報の収集、対応要否の判断、残存する脆弱性の把握、対応履歴の点検までを継続的な管理プロセスとして実施することが求められます。

一方、リスクアセスメントは単に脆弱性診断を一度実施することではありません。重要なシステムや情報を把握し、想定される脅威と脆弱性、事業への影響を整理したうえで、優先順位を付けて対策し、その結果を継続的に見直す活動です。従業員100〜1,000名規模の企業では、情報システム部門だけで完結させず、経営層、事業部門、総務・法務、調達・購買などを巻き込むことが実効性を高めるポイントになります。

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

出典：IPA「★3・★4 要求事項・評価基準 解説書」 https://www.ipa.go.jp/security/scs/rcu1hd0000007a2i-att/SCS-620-handbook-v1.0.pdf

## この記事で分かること

- SCS評価制度におけるリスクアセスメントの位置づけ
- リスクアセスメントを実施する具体的な手順
- 経営層と情報システム部門がそれぞれ判断・準備すべき事項
- 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との違いと使い分け
- 評価で確認される証跡と、よくある失敗
- SCS評価制度対応を外部へ依頼する際の選定ポイント

## SCS評価制度におけるリスクアセスメントとは

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の基準で可視化する制度です。2026年11月時点では★3と★4の要求事項・評価基準、自己評価ガイド、★4第三者評価ガイド、技術検証ガイドなどが公開されており、★3・★4の登録申請は2027年3月からの受付開始が予定されています。

要求事項は「ガバナンスの整備」「取引先管理」「リスクの特定」「攻撃等の防御」「攻撃等の検知」「インシデントへの対応」「インシデントからの復旧」という7つの大分類で構成されています。このうち「リスクの特定」には資産管理とリスクアセスメントが含まれます。

出典：IPA「要求事項・評価基準」 https://www.ipa.go.jp/security/scs/requirements-criteria.html

重要なのは、SCS評価制度が特定の製品導入だけを求める制度ではない点です。自社の取得単位・適用範囲を定め、対象となるシステムや情報資産を把握し、要求事項を満たす運用と証跡を整える必要があります。したがって、リスクアセスメントは「何を守るか」「どの危険を先に減らすか」を決める実務プロセスとして捉えるのが適切です。

## ★3と★4でリスクアセスメントの扱いはどう違うか

SCS評価制度では、★3は一般的なサイバー攻撃に対処するため、すべてのサプライチェーン企業が最低限実装すべき水準とされています。要求事項は26件で、評価はSCSセキュリティ専門家による確認付きの自己評価です。

★4は、供給停止や機密情報漏えいなど、サプライチェーンに大きな影響を与える事態を想定した標準的な水準です。要求事項は43件で、第三者評価に加え、実地審査と技術検証が行われます。

ここで注意したいのが、IPAの「★3・★4 要求事項・評価基準 解説書」における「No.3-2 リスクアセスメント」です。2026年10月28日版では、脆弱性の管理体制・管理プロセスを定め、それに基づいて管理する要求事項No.3-2-1は★4の評価項目として示されています。具体的には、脆弱性情報・脅威情報を収集する情報源・ツール・頻度、対応要否の判断基準と対応手順、脆弱性の残存状況を把握する仕組み、対応履歴の記録と月次点検などが評価基準として示されています。

そのため、「★3取得のために正式なリスクアセスメント要求が必ず同じ粒度で課される」と一括りにするのは正確ではありません。ただし、★3でも資産管理や脆弱性への基本的な対策、インシデントへの備えが求められます。将来的に★4を目指す企業や、取引先から高い管理水準を求められる企業は、★3準備の段階からリスクベースで管理する仕組みを整えておくと、後工程の手戻りを減らせます。

出典：IPA「★3・★4 要求事項・評価基準 解説書」No.3-2 https://www.ipa.go.jp/security/scs/rcu1hd0000007a2i-att/SCS-620-handbook-v1.0.pdf

## なぜ今、SCS評価制度を見据えたリスクアセスメントが必要なのか

理由は、サイバーリスクが自社だけで完結しないためです。委託先やクラウドサービス、保守会社、ソフトウェア、リモート接続環境などを経由した侵害は、自社の事業停止や情報漏えいだけでなく、取引先へ波及する可能性があります。SCS評価制度は、こうしたサプライチェーン上のリスクに対して、企業が一定の対策水準を満たしていることを可視化する仕組みです。

経営の観点では、リスクアセスメントにより「どのシステムが止まると売上・生産・顧客対応に影響するか」「どの情報が漏えいすると契約・法務・信用面の損失が大きいか」を明らかにできます。セキュリティ予算を単なるIT費用として扱うのではなく、事業継続や取引維持に必要な投資として説明しやすくなる点も重要です。

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

## リスクアセスメントを行わない場合に起こり得る問題

リスクアセスメントが不十分な企業では、セキュリティ対策が「導入しやすい製品」や「直近で指摘された項目」に偏りやすくなります。その結果、重要なサーバーの脆弱性が放置される一方で、影響の小さい端末対策に予算を集中させる、といった優先順位の逆転が生じます。

また、取引先からSCS評価制度への対応状況を確認されたときに、規程はあるものの実際の対象資産が分からない、脆弱性情報の収集担当が決まっていない、パッチ適用履歴を説明できない、といった状況も起こり得ます。これは評価対応の遅れだけでなく、監査対応の長期化、追加作業の発生、場合によっては取引先との条件調整にも影響します。

## リスクアセスメントの対象範囲はどう決めるか

最初に決めるべきなのは、SCS評価制度の取得単位と適用範囲です。会社全体を一律に対象とするのか、特定事業・拠点・サービスを単位とするのかによって、調査量も必要な対策も変わります。対象範囲を曖昧にしたまま診断や資料作成を始めると、後から対象機器や委託先が追加され、工数と費用が膨らみやすくなります。

実務では、業務プロセス、顧客・取引先との接続関係、重要情報、サーバー・ネットワーク機器、クラウド、SaaS、PC、モバイル端末、委託先、リモートアクセス経路などを整理します。特に「止まると事業に大きな影響を与えるもの」「外部からアクセス可能なもの」「機密情報を扱うもの」「取引先のネットワークやデータに接続するもの」は優先的に把握すべき対象です。

## SCS評価制度を見据えたリスクアセスメントの実施手順

### 1. 経営上の重要業務と評価範囲を決める

売上・生産・顧客対応・法令対応など、停止時の影響が大きい業務を整理します。経営層は、どの事業やサービスを守るべき対象とするか、許容できる停止時間や損失の考え方を示す必要があります。

## 2. 情報資産とIT資産を棚卸しする

サーバー、PC、ネットワーク機器、クラウド、SaaS、業務アプリケーション、データ、アカウント、委託先接続などを一覧化します。資産台帳が古い場合は、実機・管理画面・契約情報と突合し、実態との差分を解消します。

## 3. 脅威と脆弱性を把握する

ランサムウェア、不正アクセス、認証情報の窃取、設定不備、既知脆弱性、誤操作、委託先経由の侵害などを想定します。★4を見据える場合は、JVN iPedia、IPAの重要なセキュリティ情報、JPCERT/CC、CISA KEV Catalog、ベンダー情報など、情報源と確認頻度を定めることが重要です。

## 4. 発生可能性と事業影響を評価する

単にCVSSなどの技術的な深刻度だけで順位を決めず、インターネット公開の有無、攻撃実績、重要情報の取扱い、停止時の影響、代替手段の有無、取引先への波及を踏まえて評価します。

## 5. 対応要否と優先順位を決める

「即時対応」「短期是正」「計画対応」「受容」などの区分を定め、責任者と期限を設定します。重大度が高く、かつ事業影響が大きいものから優先するのが基本です。

## 6. 是正後の残存リスクを確認する

対策を実施してもリスクがゼロになるとは限りません。パッチ適用後の再診断、設定変更後の確認、アクセス権の棚卸しなどにより、残ったリスクを把握します。

## 7. 継続的に見直す

新たな脆弱性やシステム変更、取引先変更、組織変更があればリスクも変化します。脆弱性情報の収集履歴、対応履歴、残存状況を記録し、定期的に未対応項目がないか確認します。

リスク評価の記録は、次のような項目を最低限そろえておくと、経営報告・是正管理・SCS評価対応で再利用しやすくなります。

| 管理項目 | 記録する内容 | 判断 | 証跡例 |
|---|---|---|---|
| 対象資産 | システム名、用途、管理部署、重要度 | 重要度 | 資産台帳、構成図 |
| 脅威・脆弱性 | 既知脆弱性、設定不備、攻撃経路 | 発生可能性 | 診断結果、脅威情報 |
| 事業影響 | 停止、漏えい、取引先影響、復旧負荷 | 影響度 | BIA、業務ヒアリング |

| | | | |
|---|---|---|---|
| 対応計画 | 対策内容、責任者、期限、残存リスク | 優先度 | 是正計画、チケット履歴 |

## 脆弱性診断・ペネトレーションテストはどこで使うか

リスクアセスメントと技術診断は同じものではありません。リスクアセスメントは、資産・脅威・脆弱性・事業影響を総合して優先順位を決める活動です。一方、Webアプリケーション診断やプラットフォーム診断は、実際のシステムに存在する脆弱性や設定不備を技術的に確認する手段です。

Webアプリケーション診断は、認証・認可、入力値処理、セッション管理など、Webアプリ固有の問題を確認するのに適しています。プラットフォーム診断は、OS、ミドルウェア、ネットワーク機器、公開ポート、既知脆弱性などを確認します。ペネトレーションテストは、複数の弱点を組み合わせた侵入経路や実際の影響を検証するために有効です。

SCS評価制度の★3では制度上の技術検証は実施されません。★4では、評価機関・技術検証事業者による技術検証として、適用範囲内のIT基盤等に対する脆弱性検査が行われます。そのため★4を目指す企業は、正式評価の前に自社で診断・是正を行い、重大な問題を減らしておくことが実務上有効です。

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

## 評価で確認されやすい資料・証跡

制度対応では「対策をしている」だけではなく、第三者が確認できる証跡が重要です。たとえば、情報資産台帳、ネットワーク構成図、脆弱性管理規程、脅威情報の収集記録、パッチ適用履歴、診断報告書、是正管理票、アクセス権台帳、バックアップ結果、インシデント対応手順、委託先管理資料などが挙げられます。

特に★4では、文書確認だけでなく実地審査と技術検証があります。規程上は「月次点検」と書いていても、実際の記録が残っていなければ運用実態を説明しにくくなります。規程・実運用・証跡の三つを一致させることが重要です。

## 経営層と情報システム部門が準備すべきこと

### 経営層が判断すべき事項

経営層は、どの事業・サービスをSCS評価制度の対象として優先するか、どこまでのリスクを許容するか、対策予算と人員をどこまで確保するかを判断します。取引先から★の取得を求められる可能性がある場合は、受注・契約更新への影響も含めて投資判断する必要があります。

### 情報システム部門が準備すべき事項

情報システム部門は、資産台帳の最新化、脆弱性・脅威情報の収集経路、パッチ管理、アカウント管理、ログ・監視、バックアップ、診断結果、インシデント対応などを整理します。SaaSやクラウドが各部門で個別導入されている場合は、事業部門や総務・購買と連携してシャドーITを含めた実態把握を進めることも重要です。

## 実施期間と費用を左右する要因

リスクアセスメントの期間や費用は、従業員数だけでは決まりません。対象拠点数、システム数、クラウド利用数、資産台帳の整備状況、委託先数、既存規程の成熟度、技術診断の有無、★3・★4のどちらを目指すかによって大きく変わります。

現状把握から始める企業では、まず数週間程度で対象範囲と主要なギャップを把握し、その後に優先度の高い是正へ進む方法が現実的です。ただし、これは一般的な進め方であり、正式な評価や取得に必要な期間を示すものではありません。評価前に規程整備、システム改修、再診断などが必要になれば、数か月単位の計画になる場合もあります。

社内稟議では、「SCS取得そのものの費用」だけでなく、ギャップ分析、規程整備、技術診断、ツール導入、設定変更、教育、再診断、外部専門家支援などを分けて整理すると、予算の根拠を説明しやすくなります。

## SCS評価制度対応を支援する会社の選び方

支援会社を選ぶ際は、制度文書を説明できるだけでなく、要求事項を実際のシステム・運用・証跡に落とし込めるかを確認することが重要です。SCS評価制度は、経営・規程・取引先管理・技術対策・インシデント対応が横断するため、コンサルティングだけ、あるいは診断だけでは対応が分断されることがあります。

RFPや見積依頼では、対象とする★、対象範囲の決め方、ギャップ分析の方法、成果物、技術診断の範囲、是正支援、再確認、機密情報の取扱い、再委託の有無、評価機関との役割分担を確認するとよいでしょう。正式な★4評価を受ける場合は、IPAが指定する評価機関・技術検証事業者の公表状況も最新情報で確認する必要があります。2026年11月時点では、評価機関・技術検証事業者等は2026年12月下旬の公表予定とされています。

出典：IPA「評価機関・技術検証事業者・研修事業者・SCSセキュリティ専門家」 https://www.ipa.go.jp/security/scs/security-experts-organization/index.html

## リスクアセスメントでよくある失敗と注意点

### 資産台帳を作るだけで終わる

一覧化は出発点です。重要度、脅威、脆弱性、事業影響、対策状況まで結び付けなければ、優先順位を判断できません。

### 技術的な深刻度だけで順位を決める

CVSSが高い脆弱性でも、外部から到達できない環境と、インターネット公開された重要システムでは実際のリスクが異なります。技術指標と事業影響を併せて判断する必要があります。

### 規程と実運用が一致していない

「毎月確認する」と規程に書かれていても、記録がなければ継続運用を示しにくくなります。実施可能なルールを定め、担当者・頻度・証跡の保存先まで設計しましょう。

### 一度評価したら終わりにする

新しい脆弱性やクラウド導入、組織変更、委託先変更によりリスクは変化します。定期見直しと変更時レビューを組み合わせることが重要です。

## 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評価制度への対応を、要求事項の読み合わせだけでなく、現状診断から改善・運用まで一気通貫で支援します。企業ごとの事業環境や取引関係を踏まえて適用範囲を整理し、ギャップ分析、リスクアセスメント、規程・運用の整備、技術対策の優先順位付けまで個別に設計します。

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、セキュリティ教育などを組み合わせることも可能です。診断結果を指摘一覧で終わらせず、経営上の影響と改善優先度を整理し、実装・運用へつなげることを重視しています。

特に、経営層・情報システム部門・現場部門の認識がずれている企業では、技術リスクを経営リスクへ翻訳し、稟議・予算化・取引先説明に使える形へ整理することで、対応を進めやすくできます。

# よくある質問

## Q1. SCS評価制度ではリスクアセスメントは必須ですか？

A.「リスクの特定」は制度の大分類の一つです。2026年10月28日版の解説書では、No.3-2「リスクアセスメント」における脆弱性管理体制・管理プロセスの要求事項は★4として示されています。★3と★4では要求事項が異なるため、目指す段階に応じて最新の要求事項・評価基準を確認する必要があります。

## Q2. リスクアセスメントと脆弱性診断は同じですか？

A. 異なります。脆弱性診断は技術的な弱点を確認する手段で、リスクアセスメントは資産、脅威、脆弱性、事業影響を総合して優先順位を判断する活動です。

## Q3. ★3でも脆弱性診断を受けた方がよいですか？

A. ★3の制度評価として技術検証は実施されません。ただし、実際の脆弱性を把握し、評価前に是正する目的で診断を利用することは有効です。

## Q4. ★4ではペネトレーションテストが必須ですか？

A. ★4では技術検証として脆弱性検査が実施されますが、一般的な意味でのペネトレーションテストと完全に同義ではありません。実施内容はIPAの技術検証ガイドや指定事業者の評価計画に基づいて確認する必要があります。

## Q5. どの部署がリスクアセスメントを担当すべきですか？

A. 情報システム部門が中心になるケースは多いものの、事業影響の評価には業務部門、取引先管理には購買・調達、規程・契約には管理部門などの協力が必要です。経営層はリスク受容と優先投資を判断します。

## Q6. 既にISMSを取得していればSCS評価制度の対応は不要ですか？

A. 不要とは限りません。IPAはSCS評価制度とISMSを相互補完的な制度と位置付けています。既存のISMS資料を活用できる場合はありますが、SCS固有の要求事項・評価基準との対応関係を確認する必要があります。

## Q7. リスクアセスメントはどのくらいの頻度で見直すべきですか？

A. 年1回などの定期レビューに加え、重大な脆弱性の公表、システム変更、新規クラウド導入、M&A、委託先変更など、リスクが変化するタイミングで見直す方法が実務的です。★4の脆弱性管理では、対応履歴の記録と対応漏れがないかの月次点検も評価基準に示されています。

## まとめ｜SCS評価制度対応では「評価する仕組み」を作ることが重要

SCS評価制度への対応で重要なのは、リスクアセスメントを一度きりの調査にしないことです。対象資産を把握し、脅威・脆弱性情報を収集し、事業影響を踏まえて優先順位を決め、是正後の残存リスクを確認し、継続的に見直す仕組みを作る必要があります。

特に★4では、リスクアセスメントの中で脆弱性の管理体制と管理プロセスが具体的に評価されます。SCS評価制度への対応を検討している企業は、申請直前に資料を整えるのではなく、早い段階から資産・運用・証跡を整理し、実際に回る管理プロセスへ落とし込むことが重要です。

## SCS評価制度のリスクアセスメントから相談したい企業へ

「自社が★3と★4のどちらを目指すべきか分からない」「どこまでを評価対象にすべきか決まっていない」「資産台帳や規程はあるが、SCS評価制度との差分が分からない」といった段階でもご相談いただけます。

Librus株式会社では、現状診断・ギャップ分析から、リスクアセスメント、規程整備、脆弱性診断、ペネトレーションテスト、是正計画、運用体制の構築まで、企業ごとの状況に応じて支援範囲を設計します。最初に対象範囲と優先課題を整理することで、不要な対策投資や手戻りを抑えながら、取引先への説明や将来の評価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