# SCS評価制度の★3と★4の違いとは？要求事項・評価方法・選び方を徹底比較

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）では、★3と★4で求められるセキュリティ水準だけでなく、評価方法や準備負担も大きく異なります。結論から言えば、★3は一般的なサイバー攻撃に対処するための基礎的な組織対策・システム防御を整え、セキュリティ専門家の確認を受けて自己評価する水準です。一方の★4は、供給停止や機密情報漏えいがサプライチェーン全体へ大きな影響を及ぼす企業・資産を想定し、ガバナンス、取引先管理、検知、インシデント対応まで含む包括的な対策を、第三者評価・実地審査・技術検証によって確認する水準です。

したがって、「★3と★4のどちらが上か」だけで選ぶのではなく、自社がサプライチェーンで担う役割、停止時の影響、扱う情報の重要性、取引先から求められる水準を基準に選ぶことが重要です。なお、★3を先に取得しなければ★4を取得できないという制度設計ではありません。

SCS評価制度は2026年3月に経済産業省と内閣官房国家サイバー統括室が公表した制度構築方針に基づき、IPAが運営する制度です。★3・★4は2027年3月頃の運用開始が予定されています。
出典：IPA「SCS評価制度の詳細情報」 https://www.ipa.go.jp/security/scs/details.html

## この記事で分かること

- SCS評価制度における★3と★4の目的・対象・要求水準の違い
- ★3の「専門家確認付き自己評価」と★4の「第三者評価」の違い
- ★4で実施される実地審査・技術検証と脆弱性診断の関係
- 従業員100～1,000名規模の企業が★3・★4を選ぶ際の判断基準
- 取得準備で必要になる資料、期間、費用、社内稟議、ベンダー選定のポイント

## SCS評価制度とは

SCS評価制度は、企業が自社のセキュリティ対策の実施状況を共通の基準で評価し、その結果を登録・公表することで、サプライチェーン上の取引先同士が必要な対策水準を確認しやすくする仕組みです。委託元にとっては取引先の対策状況を判断しやすくなり、委託先にとっては取引先ごとに異なるチェックシートへ何度も回答する負担を軽減することが期待されています。

制度上、★3や★4の取得そのものは一律の法的義務ではありません。ただし、IPAは2社間の取引契約等で委託元が委託先に適切な段階を提示し、対策を求める利用方法を想定しています。つまり制度が任意でも、実務上は取引条件、調達条件、監査要件として特定の★取得を求められる可能性があります。
出典：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」
https://www.ipa.go.jp/security/scs/index.html

## SCS評価制度の★3と★4の違いを一覧で比較

| 比較項目 | ★3 | ★4 |
|---|---|---|
| 想定する脅威 | 広く認知された脆弱性等を悪用する一般的なサイバー攻撃 | 供給停止などによりサプライチェーンへ大きな影響を与える攻撃、重要な機密情報等を狙う攻撃 |

| | | |
|---|---|---|
| 対策の考え方 | 全てのサプライチェーン企業が最低限実装すべき基礎的な組織対策・システム防御 | ガバナンス、取引先管理、システム防御・検知、インシデント対応等を含む包括的な対策 |
| 評価方式 | セキュリティ専門家の確認を受けた自己評価 | 指定された評価機関による第三者評価 |
| 文書確認 | あり | あり |
| 実地審査 | 原則なし | あり。規程、運用、操作画面、証跡等を確認 |
| 技術検証 | 制度上の評価プロセスとしては実施なし | あり。対象機器に対する脆弱性検査等を実施 |
| 主な想定企業 | 一般的なサプライチェーン企業。まず共通の基礎水準を整えたい企業 | 停止や情報漏えいが取引先・社会へ大きく波及する企業、重要資産を扱う企業 |
| 上位関係 | ★3取得後でなければ★4に進めないわけではない | ★3を事前取得せず直接★4を目指すことも可能 |

経済産業省は★3を「全てのサプライチェーン企業が最低限実装すべきセキュリティ対策」、★4を「サプライチェーン企業等が標準的に目指すべきセキュリティ対策」と整理しています。単純にチェック項目が増えるというより、★4では「組織として機能しているか」「攻撃を検知し、侵入後の被害拡大を抑えられるか」「取引先を含めたサプライチェーンの強靭化に取り組んでいるか」まで確認範囲が広がる点が重要です。

出典：経済産業省「SCS評価制度の実現」
https://www.meti.go.jp/press/2026/04/20260403003/20260403003-b.pdf

## ★3とは？一般的なサイバー攻撃に備える基礎水準

★3は、広く知られた脆弱性や一般的な攻撃手法を悪用したサイバー攻撃に対処し得る水準を想定しています。経営者の承認を伴う体制整備、IT資産やアカウントの管理、脆弱性への対応、バックアップ、インシデント時の連絡・対応など、企業として最低限欠かせない対策を「実施していると言える状態」にすることが重要です。

### ★3の評価方法は「専門家確認付き自己評価」

★3では、取得希望企業が要求事項・評価基準に基づいて自己評価を行い、その内容をSCS評価制度に登録されたセキュリティ専門家が確認します。専門家は記載内容や評価基準との整合性を確認し、必要に応じて修正・助言を行います。最終的には、経営層による自己適合宣誓を含めて事務局へ提出する流れです。

「自己評価だから簡単」という意味ではありません。IPAのFAQでは、★3・★4とも定められたすべての要求事項・評価基準を満たす必要があるとされています。不適合がある場合は、是正して専門家の了承を得るプロセスが必要です。

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

### ★3で企業が準備しておきたい証跡

自己評価では「規程に書いてある」だけでなく、実際に運用されていることを説明できる資料をそろえることが重要です。例えば、情報セキュリティ方針、組織図・責任分担表、IT資産台帳、アカウント一覧、脆弱性・パッチ管理記録、バックアップ結果、教育実施記録、インシデント対応手順、取引先管理ルールなどが候補になります。

従業員100～1,000名規模では、情シスだけで資料を集めきれないケースが少なくありません。人事、総務、法務、購買、事業部、開発部門などが保有する証跡を横断的に整理し、「誰が、何を、どの頻度で実施しているか」まで明確にすると評価準備が進みやすくなります。

## ★4とは？停止・漏えいの影響が大きい企業向けの包括的水準

★4は、初期侵入を防ぐだけでなく、侵入された後の被害拡大防止、検知、インシデント対応、復旧、取引先管理まで含めて、より包括的にサイバーリスクを管理する水準です。供給停止が大きな影響を及ぼす事業、重要な顧客データや機密情報を扱う事業、サプライチェーンの中核を担う企業では、★4が現実的な目標となる可能性があります。

### ★4は第三者評価・実地審査・技術検証が必要

★4では、取得希望企業の自己評価だけでは完結しません。指定された評価機関が文書確認に加えて実地審査を行い、さらに技術検証事業者による技術検証が実施されます。IPAの制度構築方針では、実地審査で脆弱性管理体制、インシデント対応手順、事業継続要件に沿った復旧準備などを確認する例が示されています。

技術検証では、インターネットに公開している機器のうち、脆弱性を悪用された場合に組織内部へ侵入されるリスクが高い機器を対象に、既知脆弱性の悪用等を想定した検査を行う方針が示されています。制度文書ではVPN装置やルータが例示されています。
出典：経済産業省・IPA「制度構築方針」
https://www.ipa.go.jp/security/scs/rcu1hd0000007ajp-att/20260327001-br.pdf

### 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関係

SCS評価制度への対応と、脆弱性診断やペネトレーションテストは同じものではありません。特に★3では、制度上の評価プロセスとして技術検証は求められていません。一方で、実際に脆弱性管理やシステム防御が十分かを確認し、不適合の原因となる問題を早期に把握するために、Webアプリケーション診断やプラットフォーム診断を事前に実施することは有効です。

★4では技術検証が評価プロセスに組み込まれます。ただし、通常の脆弱性診断やペネトレーションテストを受けているだけで★4を取得できるわけではありません。文書・運用・ガバナンス・インシデント対応など、制度全体の要求事項への適合が必要です。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可能性や攻撃経路を確認するために有効ですが、SCS評価制度の技術検証との目的・範囲をRFP段階で区別する必要があります。

## ★3と★4、どちらを目指すべきか

判断の基本は「自社の規模」ではなく、「自社が止まった場合、または侵害された場合にサプライチェーンへどの程度影響するか」です。従業員数が同じ500名でも、一般的なバックオフィス業務を担う企業と、複数の大手企業の基幹システムを運用する企業では、求められる水準が異なります。

### ★3を優先しやすい企業

まず共通の基礎対策を整備し、一般的なサイバー攻撃への耐性を説明できる状態を作りたい企業は★3が候補です。取引先から具体的な★4指定がなく、自社の停止や情報漏えいが直ちに広範な供給停止へつながる立場ではない場合、★3を基準にギャップ分析を始めることは合理的です。

### ★4を検討すべき企業

一方、重要インフラに近い事業、製造・物流・金融・ITサービス等で多くの取引先の業務継続を支える企業、大量の機密情報・個人情報を扱う企業、取引先から高いセキュリティ保証を求められる企業は★4を検討する価値が高まります。M&A、IPO、大規模な新規取引など、セキュリティ管理水準を外部に説明する必要性が高い局面でも、★4を見据えた体制整備が有効です。

### 経営層が判断すべき4つのポイント

- 自社サービスが停止した場合、顧客や取引先の事業がどの程度止まるか
- 漏えいした場合に影響が大きい機密情報・個人情報・設計情報等を保有しているか
- 主要顧客・業界の調達基準としてどの★が求められそうか
- ★取得だけでなく、取得後の運用・継続改善に必要な予算と人員を確保できるか

## ★3・★4取得に向けた実務的な進め方

### 1. 適用範囲を決める

最初に、自社のどの組織・拠点・IT基盤・サービスを評価対象にするかを決めます。適用範囲が曖昧なままでは、資産台帳や規程、診断対象、証跡が膨らみ、見積もりも不安定になります。取引先との契約や重要サービスとの関係から、守るべき範囲を明確にすることが出発点です。

### 2. 要求事項とのギャップ分析を行う

現行の規程・運用・技術対策を要求事項と照合し、「適合」「一部適合」「未対応」「証跡不足」に分類します。ここでは、単に対策製品の有無を見るのではなく、責任者、手順、実施頻度、例外時の承認、記録保存まで確認します。

### 3. 優先順位を付けて是正する

不備をすべて同時に直すのではなく、外部公開システムの既知脆弱性、特権ID、MFA、バックアップ、インシデント連絡体制など、侵害時の影響が大きい項目から優先します。技術的な弱点が疑われる場合は、Webアプリケーション診断やプラットフォーム診断を組み合わせ、設定・実装上の問題を把握します。

### 4. 証跡を整え、評価に備える

評価では「実施している」という説明だけでは不十分になり得ます。ログ、チケット、教育記録、バックアップ確認結果、脆弱性対応記録、取引先評価記録など、運用の実態を裏付ける証跡を継続的に残します。★4では実地審査も想定されるため、担当者へのヒアリングに耐えられる状態まで運用を定着させることが重要です。

## 実施期間と費用を左右する要因

制度構築方針では、評価そのものの所要期間として文書確認や実地審査、技術検証についてそれぞれ1～2日程度の想定が示されていますが、これは事前準備や是正、報告書作成を除いた目安です。実際の取得準備は、ギャップの大きさや適用範囲によって大きく変わります。特に、規程未整備、資産管理未整備、MFA未導入、バックアップ復旧テスト未実施、インシデント対応体制未整備などが重なると、評価前の改善に時間がかかります。

費用は、制度運営機関への登録料だけでなく、専門家確認、第三者評価、技術検証、コンサルティング、必要なセキュリティ製品・運用改善などを含めて考える必要があります。IPAが2026年9月18日に公表した料金では、登録希望組織の登録料は、2028年3月31日まで★3が年1万円、★4が3年6万円、2028年4月1日以降は★3が年2万円、★4が3年6万円とされています。評価機関や専門家への費用は別途発生し得ます。

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

## 社内稟議では「認証取得費」だけで説明しない

社内稟議では「SCSのマークを取るための費用」とだけ説明すると、単なる認証コストと見られやすくなります。経営層には、①主要取引先との取引継続、②サプライチェーン上の信用維持、③インシデントによる事業停止・復旧費用の低減、④取引先ごとの個別監査対応の効率化、⑤M&A・IPO・大手企業との新規取引における説明力向上、といった経営上の目的を併せて示すべきです。

また、一度の評価取得で終わる施策ではありません。人事異動、新システム導入、クラウド移行、M&A、委託先変更などでリスクは変化します。取得後の運用費、継続監視、教育、再診断まで含めた複数年度の予算として計画すると、対策が形骸化しにくくなります。

## サービス提供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、「チェックシートを埋められるか」だけでなく、制度、技術、運用、経営の4つを横断して支援できるかを確認することが重要です。

- ★3・★4の要求事項と評価プロセスを区別して説明できるか
- 適用範囲の設計からギャップ分析、規程整備、証跡作成まで支援できるか
- 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も対応できるか
- 不適合を単に指摘するだけでなく、費用・優先度を踏まえた改善計画を提示できるか
- 個人情報・機密情報の取扱い、データ保管、再委託の有無を明確にできるか
- 経営層向け報告と現場向けの具体的な改善指示の両方を提供できるか

★4では評価機関の中立性・公平性も重要になるため、取得支援を行う事業者と実際の第三者評価を担う評価機関の役割を整理してRFP・見積依頼を行う必要があります。

## よくある失敗と注意点

### ★3を「簡易版の★4」とだけ考える

★3は単なる項目数の少ない評価ではありません。一般的な脅威に対する共通の基礎水準として位置づけられています。まず★3で基礎を固める企業もあれば、取引先要件や事業影響を踏まえて最初から★4を目指す企業もあります。

### ツール導入だけで適合すると考える

EDR、MFA、SIEM、バックアップ製品などは重要ですが、制度では組織体制や運用手順、証跡も確認されます。製品を購入しただけでは、誰がアラートを確認し、異常時に誰へ連絡し、どの基準で復旧判断するかという運用上の課題は解決しません。

### 評価直前に証跡を集め始める

証跡は後から作るほど、実態との整合性を説明しづらくなります。脆弱性対応、アクセス権レビュー、バックアップ確認、教育、インシデント訓練などは日常運用として記録を残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評価制度への対応を「評価取得のための書類作成」に限定せず、実際のセキュリティ水準を高めるプロジェクトとして支援します。要求事項とのギャップ分析、適用範囲の整理、規程・運用ルールの整備、証跡設計、経営層向けの説明、改善ロードマップ策定まで一気通貫で対応可能です。

技術面では、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などを組み合わせ、制度対応と実際のサイバーリスク低減を同時に進められます。

また、企業ごとの事業特性、予算、既存のISMSや社内規程、取引先からの要求を踏まえて、★3を優先するのか、★4を見据えて整備するのかを個別に設計します。M&A、IPO、取引先監査など、経営上の重要局面に合わせてセキュリティ課題を整理できる点もLibrus株式会社の特徴です。

## よくある質問

### Q1. ★3を取得してからでないと★4は取得できませんか？

いいえ。IPAは、上位段階が下位段階の要求を包括するものの、★3を事前に取得していなければ★4を取得できない関係ではないと説明しています。事業上の必要性があれば、直接★4を目指すことも可能です。

### Q2. ★3と★4はどちらも全項目を満たす必要がありますか？

はい。IPAのFAQでは、★3・★4とも、それぞれに定められたすべての要求事項・評価基準を満たす必要があるとされています。

### Q3. ★3でも脆弱性診断は必須ですか？

制度上の評価プロセスとして、★3には★4のような技術検証は設定されていません。ただし、脆弱性管理やシステム防御の実効性を確認し、取得前に問題を是正する目的で診断を実施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？

制度上は技術検証が必要ですが、一般的なペネトレーションテストと完全に同義ではありません。評価範囲や検証方法は制度文書・評価機関の指示に従う必要があります。

### Q5. SCS評価制度は中小企業だけが対象ですか？

いいえ。IPAは全てのサプライチェーン企業を対象としています。特に中小企業で活用効果が大きいとされていますが、業種や企業規模を問わず対象となり得ます。

### Q6. 取得すれば取引先のセキュリティチェックシートは不要になりますか？

必ず不要になるとは限りません。SCS評価制度は共通化・可視化によって負担軽減を目指す制度ですが、取引先が独自に追加確認を行う可能性はあります。

### Q7. ★3・★4の取得準備はいつ始めるべきですか？

取引先から正式に要請されてからではなく、早めにギャップ分析を始めることが望まれます。規程整備やMFA導入、脆弱性対応、バックアップ・復旧訓練などは、短期間で形式的に整えるより、一定期間運用して証跡を蓄積した方が評価に備えやすいためです。

### Q8. どちらを選ぶべきか判断できない場合はどうすればよいですか？

自社のサプライチェーン上の役割、停止時の影響、保有情報、主要取引先の要求、現状の対策成熟度を整理し、★3・★4それぞれのギャップと費用を比較すると判断しやすくなります。

## まとめ｜★3と★4の違いは「対策範囲」と「評価の客観性」

SCS評価制度の★3と★4の最大の違いは、求められる対策の広さと評価方法です。★3は一般的なサイバー攻撃に対処するための基礎的な対策を、専門家確認付き自己評価で確認します。★4は、供給停止や重要情報の漏えいによる影響が大きい企業を想定し、ガバナンス、取引先管理、検知、インシデント対応まで含む包括的な対策を第三者評価・実地審査・技術検証によって確認します。

重要なのは、「★4の方が上だから★4を取る」「まず★3を取らなければならない」と機械的に決めないことです。自社の事業影響と取引先要件を基準に必要な水準を選び、現状とのギャップを把握した上で、規程・運用・技術対策を計画的に改善することがSCS評価制度への実務的な対応となります。

## SCS評価制度の★3・★4選定から取得準備までご相談いただけます

「取引先からどの★を求められる可能性があるのか分からない」「★3と★4のどちらを目標にすべきか判断できない」「現状の規程やシステムで何が不足しているのか把握したい」といった段階でもご相談いただけます。

Librus株式会社では、事業・取引関係・IT環境を整理した上で、SCS評価制度の要求事項とのギャップ、優先して改善すべき項目、必要な技術検証、取得までのロードマップを具体化します。対象範囲や実施方法が決まっていない段階から整理することで、不要な対策や重複投資を避けながら、取引継続と実際のセキュリティ向上の双方を見据えた計画を立てやすくなります。

## 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