# SCS評価制度とSOC・ログ監視の関係｜検知・監視体制を整備する方法

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、攻撃を防ぐ対策だけでなく、異常を早く見つけ、適切に対応へつなげる「検知」の仕組みが重要です。結論から言えば、SCS評価制度のために必ずしも自社内に大規模なSOC（Security Operation Center）を新設する必要はありません。重要なのは、必要なログを取得し、継続的に監視・分析し、異常を検知した際に誰が判断し、どのようにインシデント対応へ移るかを、実際に運用できる形で整えることです。特に従業員100〜1,000名規模の企業では、情報システム部門だけで24時間365日の監視を担うことが難しいケースも多く、外部SOCやマネージドサービスを活用しながら、自社側の責任分界とエスカレーションルールを明確にすることが現実的です。

重要な結論：**SCS**評価制度で評価されるのは「**SOC**という名称の組織があるか」ではなく、必要な監視対象を定め、ログを収集・分析し、異常を検知して対応に結び付ける仕組みが実効的に運用されているかです。

## この記事で分かること

- SCS評価制度における「攻撃等の検知」とSOC・ログ監視の関係
- ★3・★4対応で確認すべきログ、監視対象、運用証跡
- SIEM・EDR・UTM・SOCをどこまで導入すべきかの判断軸
- 社内SOCと外部SOCの使い分け、RFP・見積依頼時の確認事項
- 脆弱性診断・ペネトレーションテスト・CSIRTとのつなぎ方
- SCS評価制度対応を単発の審査対策で終わらせない運用方法

## SCS評価制度とは｜「防御」だけでなく「検知・対応・復旧」まで評価する

SCS評価制度は、経済産業省と内閣官房国家サイバー統括室が示した制度構築方針に基づき、IPAが運営する制度です。2026年11月時点では、★3と★4について2027年3月の登録申請受付開始が予定されています。★3は一般的なサイバー脅威に対処しうる水準、★4は初期侵入の防御に加えて被害拡大防止や取引先のデータ・システム保護まで意識した、より高い水準として設計されています。

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。つまり、ファイアウォールやウイルス対策ソフトを導入するだけではなく、攻撃を見つけ、初動を判断し、事業を復旧させる一連の能力まで含めて考える必要があります。

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

## SCS評価制度とSOC・ログ監視はどう関係するのか

### 「攻撃等の検知」では、異常を見つける仕組みが求められる

IPAの制度概要資料では、「攻撃等の検知」の具体例として、情報機器等の状態・挙動の監視、ネットワーク接続やデータの監視が示されています。また、攻撃等の防御に関連する項目として、ログの収集と定期的な分析も挙げられています。したがって、SCS評価制度への対応では「ログを取っている」ことだけでなく、どのログを、誰が、どの頻度で確認し、異常時にどのような行動を取るのかまで説明できる状態が重要です。

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」概要資料：https://www.ipa.go.jp/security/scs/rcu1hd0000007ajp-att/20260327001-br.pdf

### SOCは手段であり、制度上の目的そのものではない

SOCは、システムやネットワークを監視し、ログ・通信・イベント情報を分析して、サイバー攻撃や不審な挙動を検知するための運用機能です。SIEM（Security Information and Event Management）は、複数の機器・システムからログを集約し、相関分析によって異常を見つけやすくする仕組みを指します。

SCS評価制度では、特定製品の導入や「SOC」という名称の部署設置が一律に必須とされているわけではありません。小規模な環境であればUTM、EDR、クラウドサービスの標準監査ログなどを組み合わせて運用する場合もあります。一方、複数拠点・多数のクラウドサービス・大量の端末を抱える企業では、SIEMや外部SOCを活用しなければ、実質的な監視が追い付かないことがあります。重要なのは、自社のリスクとシステム構成に対して監視方式が十分かどうかです。

参考：**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」：https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0.pdf

## SCS対応で整理したい監視対象とログ

ログ監視の範囲は、取得できるものをすべて集めるのではなく、重要な情報資産・外部接続点・認証経路・管理者操作など、攻撃の兆候や被害状況の把握に有効なログから優先順位を付けることが重要です。

| 監視対象 | 主なログ・イベント例 | 確認したい異常の例 |
|---|---|---|
| 認証・アカウント | ログイン成功／失敗、MFA、特権ID、アカウント作成・削除 | 短時間の大量失敗、国外・通常外拠点からのアクセス、特権IDの不審利用 |
| 端末・サーバー | EDR／アンチウイルス、OSイベント、プロセス起動、管理者操作 | マルウェア検知、権限昇格、不審プロセス、セキュリティ機能停止 |
| ネットワーク | FW、UTM、VPN、DNS、プロキシ、IDS/IPS | 不審な外部通信、C2通信兆候、通常と異なる大量通信、未知の接続先 |
| クラウド・SaaS | 管理者操作、認証、設定変更、データアクセス、API利用 | 設定改変、異常なダウンロード、管理権限変更、不審なAPI利用 |
| Web・アプリケーション | Webアクセス、WAF、アプリケーション、DB監査ログ | SQLインジェクション等の攻撃兆候、異常な大量アクセス、機密データへの不審アクセス |

### ログは「保存」より「検知・判断・対応につなげる運用」が重要

ログを長期間保存していても、異常を誰も見ていなければ検知能力は高まりません。逆に、すべてのアラートを人手で確認すると担当者が疲弊し、本当に重要な兆候を見落とす可能性があります。実務では、重要度の高いイベントを定義し、一次判定、追加調査、インシデント判定、CSIRTや経営層へのエスカレーションという流れを設計する必要があります。

## SCS評価制度を見据えた検知・監視体制の整備方法

### 1. 重要な事業・システムと監視対象を決める

まず「何を守るか」を明確にします。取引先データを扱うシステム、基幹システム、インターネット公開サーバー、VPN、クラウド管理者アカウントなど、停止や漏えいが取引継続に直結する対象を優先します。SCS評価制度の適用範囲とログ監視の対象範囲がずれていると、評価時に説明が難しくなるため、資産台帳・ネットワーク構成図・クラウド利用一覧と合わせて整理します。

### 2. 取得できているログと不足を棚卸しする

各システムについて「取得しているログ」「保存期間」「保管場所」「時刻同期」「閲覧権限」「監視の有無」を確認します。特に、管理者操作ログや認証ログ、ネットワーク境界の通信ログは、インシデント発生時の調査にも重要です。

### 3. 検知ルールと優先度を決める

すべてのアラートを同じ扱いにせず、緊急度と影響度で分類します。例えば、マルウェア検知、特権アカウントの異常利用、外部への大量通信、公開サーバーへの攻撃兆候などは、通常の情報通知より高い優先度で扱います。

### 4. 誰が監視し、誰が判断するかを決める

SOCが一次監視を担っても、業務停止や顧客報告を決めるのは自社です。SOC、情報システム部門、CSIRT、事業部門、経営層、広報・法務などの責任分界を定め、連絡先と判断基準を文書化します。休日・夜間の連絡方法も確認しておきます。

### 5. SOC・SIEM・EDRなどの手段を選定する

製品導入を先に決めるのではなく、監視対象、必要な対応時間、社内人員、予算から逆算します。少数拠点ならマネージドEDRやUTM監視で足りる場合もあります。複数システムを横断して相関分析する必要があればSIEMが有効です。24時間の初動が必要なら外部SOCの活用も選択肢になります。

### 6. アラートからインシデント対応までを訓練する

検知した後に担当者が迷えば、実効性は十分とは言えません。模擬アラートや机上演習を使い、「どの情報を確認するか」「端末隔離や通信遮断を誰が判断するか」「取引先へいつ報告するか」を確認します。訓練結果と改善内容は、運用証跡としても有用です。

### 7. 定期的に検知ルール・対象ログを見直す

システム構成や攻撃手法は変化します。クラウド導入、新規拠点、M&A、委託先変更などがあればログ取得や監視対象も見直します。誤検知が多いルールは調整し、見逃しにつながる監視空白がないか定期的に確認します。

## 自社SOCと外部SOCはどう使い分けるべきか

従業員100～1,000名規模の企業では、専門人材を24時間配置して自社SOCをゼロから構築するより、監視・一次分析を外部サービスへ委託し、自社はインシデント判断と事業影響の判断に集中する構成が現実的なことがあります。ただし、外部委託すれば責任まで移るわけではありません。

外部SOCを選定する際は、監視時間、対象機器・クラウド、ログの保存期間、検知ルール、重大アラートの通知時間、一次調査の範囲、インシデント時の支援範囲、レポート内容、証跡の提供可否、個人情報・機密情報の取扱いを確認します。SCS評価制度を見据える場合、評価時に「何をどのように監視しているか」を説明できるレポートやチケット履歴が残ることも重要です。

### RFP・見積依頼時に確認したいポイント

- 24時間365日監視か、営業時間内監視か。重大アラートの初動目標時間は何分・何時間か
- EDR、FW、UTM、クラウド、認証基盤、Web/WAFなど、どのログを取り込めるか
- ログ保管期間と、調査時に生ログを取得できるか
- 重大インシデント時に、分析・封じ込め助言・DFIRへどこまで連携できるか
- 月次報告書に、アラート件数だけでなく原因・傾向・改善提案が含まれるか
- SCS評価制度の証跡として提示できる運用記録やレポートを提供できるか
- 委託先・再委託先で扱うログや機密情報の管理方法が明確か

## SOC・ログ監視と脆弱性診断は代替関係ではない

SOCやログ監視は「攻撃や異常を見つける」役割を担います。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、攻撃される前に弱点を発見し、侵入経路を減らすための施策です。ペネトレーションテストは、複数の脆弱性や設定不備を組み合わせた場合に、どこまで侵入・権限拡大・情報到達が可能かを攻撃者視点で検証します。

これらは競合する施策ではありません。診断で弱点を減らし、SOCで残存リスクや新たな攻撃を検知し、CSIRTでインシデントに対応するという役割分担が基本です。SCS評価制度への対応でも、単一製品の導入ではなく、防御・検知・対応・復旧をつなげて設計することが重要になります。

## 検知・監視体制が不十分な場合に起こり得る問題

攻撃を受けても異常に気付くまで時間がかかれば、認証情報の窃取、端末間の横展開、バックアップの破壊、機密情報の外部送信など、被害が拡大する可能性があります。さらに、取引先から「いつ侵入されたのか」「どのデータにアクセスされたのか」を問われた際、必要なログがなければ事実関係を説明できません。これは復旧の遅れだけでなく、信用毀損や取引継続判断にも影響します。

そのため経営層は、SOC導入の有無だけでなく、重要システムの監視空白、夜間・休日の初動、重大インシデント時の意思決定、フォレンジック調査に必要なログ保存などを、事業継続リスクとして確認する必要があります。

## 費用・期間を左右する要因

監視体制の費用は、単純な「従業員数」よりも、監視する端末数、サーバー数、クラウドサービス数、ログ量、24時間監視の要否、分析レベル、インシデント対応支援の範囲などに左右されます。SIEMでは取り込むログ量が料金に影響するサービスもあるため、必要性の低いログまで無制限に収集するとコストだけが増えることがあります。

期間についても、既にEDRやクラウド監査ログが整備されている企業と、資産台帳やネットワーク構成の棚卸しから必要な企業では大きく異なります。SCS評価制度の取得時期から逆算し、最初にギャップ分析を行い、短期で整えられる設定変更と、中長期のSOC・SIEM導入を分けてロードマップ化すると稟議を進めやすくなります。

## SCS評価制度を見据えた支援会社の選び方

支援会社を選ぶ際は、SOC製品の導入だけではなく、SCS評価制度の要求事項、ログ設計、インシデント対応、脆弱性診断まで横断して整理できるかを確認するとよいでしょう。監視対象が不明確なままSIEMを導入しても、有効な検知ルールを設計できないケースがあります。

また、評価前のギャップ分析、規程整備、アセスメントシート作成、監視設計、技術対策、診断、是正、運用証跡の整理を複数の会社へ分断して依頼すると、責任分界の調整に時間がかかる場合があります。自社の体制や既存ツールを活かしながら、必要な範囲だけ補完できるかも重要な判断軸です。

## よくある失敗と注意点

### SIEMを導入しただけで監視体制が完成したと考える

SIEMはログを集約・分析する手段です。検知ルール、誤検知の調整、アラート対応者、エスカレーション先が定まっていなければ、十分に活用できません。

### ログを集めすぎて重要なアラートが埋もれる

ログ量が増えるほど安心とは限りません。重要資産と想定脅威を起点に、監視優先度を設計することが必要です。

### 外部SOCに委託した後、自社側の役割を決めていない

SOCから重大通知が来ても、端末隔離やサービス停止を誰が決めるか不明では初動が遅れます。委託前に責任分界と緊急連絡網を決めておく必要があります。

### 評価直前にログや証跡を揃えようとする

ログ監視は日常運用の積み重ねです。月次レポート、アラート対応記録、チケット、ルール変更履歴、訓練記録などを平常時から残しておくことで、評価時の説明が容易になります。

## Librus株式会社が提供できる支援

Librus株式会社では、SCS評価制度対応を単なる書類作成としてではなく、実際のセキュリティ運用と結び付けて支援します。現状のログ取得・監視体制のギャップ分析、重要資産と監視対象の整理、SOC／CSIRT構築・運用支援、インシデント対応手順の整備、脆弱性診断・ペネトレーションテスト、改善計画の策定まで、一気通貫で対応可能です。

既にEDR、UTM、クラウド監査ログ、SIEM等を導入している企業では、既存投資を前提に不足部分を整理します。新たな製品導入が必要か、運用ルールの見直しで対応できるかを切り分けることで、過剰投資を避けながら、SCS評価制度と実際のリスク低減の両方を目指します。

## よくある質問

### Q1. SCS評価制度を取得するにはSOCの設置が必須ですか？

必ずしも自社SOCの設置が必須という制度ではありません。重要なのは、必要な監視対象を定め、ログや状態を継続的に確認・分析し、異常を検知した際に対応へつなげられることです。外部SOCやマネージドサービスを活用する方法も考えられます。

### Q2. ★3でもログ監視は必要ですか？

★3でも一般的なサイバー脅威への対応を想定しており、ログ収集・分析や機器・ネットワークの監視は重要です。自社の適用範囲と要求事項に照らして、必要な証跡と運用を整理する必要があります。

### Q3. ログは何年間保存すればよいですか？

一律の期間だけで判断せず、制度要求、契約、法令、インシデント調査の必要性、ストレージ費用を踏まえて決めます。重要なのは、保存期間をルール化し、実際にその期間保存されていることです。

### Q4. SIEMを導入すればSCS評価制度の検知要件を満たせますか？

SIEM導入だけで自動的に要件を満たすわけではありません。監視対象、検知ルール、アラート分析、責任者、対応手順、改善履歴などの運用が必要です。

### Q5. 外部SOCを利用していても自社でCSIRTは必要ですか？

正式な名称としてのCSIRTが必須とは限りませんが、SOCからの通知を受けて事業影響を判断し、封じ込め・顧客連絡・復旧を指揮する自社側の役割は必要です。

### Q6. Webアプリケーション診断とSOCはどちらを優先すべきですか？

役割が異なるため、単純な二者択一ではありません。診断は弱点を事前に減らし、SOCは攻撃や異常を検知します。公開Webシステムなど重要度が高い対象では、両方を組み合わせることが有効です。

### Q7. SCS評価制度のために24時間365日監視が必要ですか？

すべての企業に一律で24時間365日監視が必要というわけではありません。事業停止の影響、顧客要求、システム重要度、攻撃リスクを踏まえて監視時間と初動体制を決めます。

### Q8. SOCの月次レポートはSCS評価制度の証跡になりますか？

監視内容、検知結果、対応履歴、改善状況が分かるレポートは有用な証跡となり得ます。ただし、評価基準との対応関係を確認し、必要に応じてチケット履歴や設定画面、手順書など他の証跡も組み合わせます。

## まとめ｜SCS評価制度の検知対策は「ログを取る」から「異常を見つけて動ける」へ

SCS評価制度では、防御策だけでなく「攻撃等の検知」が独立した大分類として位置付けられています。SOCやSIEMは、その実現手段の一つです。重要なのは、重要資産に必要なログを取得し、適切な頻度で監視・分析し、異常を見つけたらCSIRTや経営層へ確実に連携できることです。

従業員100～1,000名規模の企業では、既存のEDR、UTM、クラウド機能、外部SOCなどを組み合わせれば、必ずしも大規模な監視基盤を自社構築する必要はありません。SCS評価制度をきっかけに、自社の「見えていない領域」と「検知後に動けない領域」を洗い出し、事業継続と取引先からの信頼につながる監視体制へ改善することが重要です。

## SCS評価制度とSOC・ログ監視を一体で整理したい企業へ

「SCS評価制度のどの要求事項に、現在のSOCやログ監視が対応しているのか分からない」「SIEMを追加すべきか、既存のEDRやUTMで足りるのか判断できない」「評価に向けて、どのログや運用記録を証跡として残せばよいか整理したい」といった段階でもご相談いただけます。

Librus株式会社では、制度要求と現在のシステム・運用を突き合わせ、監視対象の優先順位、SOC／CSIRTの役割分担、必要な技術対策、脆弱性診断、証跡整備まで整理します。対象範囲や実施方法が固まっていない段階から検討することで、不要な製品導入を避けながら、評価対応と実際のリスク低減を同じロードマップで進めやすくなります。

## 参考情報

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

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

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

**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」:https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0.pdf

## 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