# SCS評価制度で必要となるインシデント対応体制とは？CSIRT構築のポイント

SCS評価制度への対応では、サイバー攻撃を防ぐための対策だけでなく、インシデントが発生した後に被害を抑え、事業を復旧させる体制も重要です。特に★4では、システム防御・検知に加え、インシデント対応や復旧までを含む包括的な対策が求められます。結論から言えば、SCS評価制度への対応にあたり「CSIRTという名称の専任組織」を必ず新設しなければならないわけではありません。重要なのは、誰が何を判断し、誰へ報告し、どのように封じ込め・復旧・対外説明を行うかが明確で、実際に機能することです。本記事では、SCS評価制度とインシデント対応体制の関係、CSIRT構築の考え方、必要な規程・証跡、演習や外部連携まで、経営者や情報システム部門が準備すべき事項を実務的に解説します。

## この記事で分かること

- SCS評価制度でインシデント対応が重視される理由
- ★3・★4に向けて準備したいインシデント対応体制の基本
- 専任CSIRTを設置できない企業でも実効性を確保する方法
- インシデント対応規程、連絡網、判断基準、演習記録などの証跡
- SOC、脆弱性診断、ペネトレーションテストとCSIRTの役割分担
- 外部ベンダーを活用する場合の選定ポイントと予算の考え方

## SCS評価制度とは

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、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し、取引時の確認をしやすくすることを目的とした制度です。IPAが制度を運営し、★3は一般的なサイバー攻撃への最低限の対策、★4は供給停止や重要情報の漏えいなど、より大きな影響を及ぼす攻撃への標準的な対策を想定しています。

IPAによると、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」の7分類で構成されています。つまり、SCS評価制度は予防だけでなく、発生後の対応と復旧まで含めて評価する制度です。

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

## なぜSCS評価制度ではインシデント対応体制が重要なのか

### 攻撃を完全に防ぐ前提ではなく、発生後の被害最小化まで考える必要がある

ランサムウェア、認証情報の窃取、Webサイトの改ざん、クラウドアカウントの不正利用などは、境界防御やウイルス対策だけで完全に防ぐことは困難です。攻撃を受けた際に、感染端末を切り離す、漏えい範囲を調査する、顧客や取引先への連絡要否を判断する、復旧優先順位を決めるといった行動が遅れるほど、事業影響が拡大しやすくなります。

IPAのサイバーセキュリティ経営ガイドラインの実践情報でも、インシデント時には検知、報告、封じ込め、復旧という流れを整理し、CSIRT等の緊急対応体制を平時から整備することが示されています。

出典：IPA「インシデント発生時の緊急対応体制の整備」 https://www.ipa.go.jp/security/economics/practices_navi/practice226.html

### 取引先への影響が大きい企業ほど、対応力そのものが信用になる

SCS評価制度は、2社間の取引契約などで委託元が委託先に必要な★の段階を示し、対策状況を確認することを想定しています。受託企業がインシデントを起こした場合、自社だけでなく委託元のシステム停止、情報漏えい、納期遅延、顧客対応にも影響する可能性があります。そのため、発注側から見ると「事故を起こさない会社」だけでなく「事故が起きても適切に対応できる会社」であることが重要です。

出典：IPA「SCS評価制度」 https://www.ipa.go.jp/security/scs/index.html

## SCS評価制度で整備したいインシデント対応体制の基本

実務上は、専任のCSIRTを置けるかどうかよりも、以下の機能が組織として成立しているかを確認することが重要です。

| 機能 | 実務上のポイント |
| --- | --- |
| 検知・受付 | SOC、EDR、ログ監視、従業員や取引先からの通報など、異常を把握する経路を定める。 |
| 初動判断 | 何をインシデントとして扱うか、重大度を誰が判断するかを決める。 |
| 報告・エスカレーション | 経営層、情報システム、法務、広報、営業、取引先への報告基準と連絡先を整理する。 |

| 機能 | 実務上のポイント |
| --- | --- |
| 封じ込め | 端末隔離、ネットワーク遮断、アカウント停止、アクセス制限などの権限と手順を定める。 |
| 調査・原因分析 | ログ保全、フォレンジック、侵入経路や影響範囲の調査を行えるようにする。 |
| 復旧 | バックアップ、代替手段、優先システム、復旧条件を定める。 |
| 対外対応 | 法令・契約に基づく報告、顧客・取引先への説明、公表判断を行う。 |
| 再発防止 | 原因に応じて脆弱性修正、設定変更、教育、規程改定などを実施する。 |

## CSIRTは必ず専任組織でなければならないのか

従業員100〜1,000名規模の企業では、専任CSIRTを新設する余力がない場合もあります。その場合でも、情報システム部門、セキュリティ担当、法務・総務、広報、営業、経営層などの既存メンバーを横断的に組み合わせ、インシデント発生時にCSIRT機能を発動する体制を設計できます。常設の「組織」より、役割・権限・連絡経路・対応手順が明確であることが重要です。

JPCERT/CCは、組織内CSIRTの構築について、役割や位置づけ、活動内容を定義し、インシデントの分類、優先度判断、技術対応者への連絡調整、被害局限化、原因排除などを行う考え方を示しています。企業規模に応じて、社内要員と外部専門家を組み合わせる方法も現実的です。

出典：JPCERT/CC「CSIRTマテリアル」 https://www.jpcert.or.jp/csirt_material/

## SCS評価制度対応で準備したい規程・証跡

### インシデント対応規程・手順書

規程には、インシデントの定義、重大度区分、初動責任者、連絡先、エスカレーション条件、証拠保全、外部通報、復旧判断などを明記します。実務では「担当者が不在でも動けるか」「休日・夜間に誰へ連絡するか」まで決めておくことが重要です。

### 連絡網・責任分担表

CSIRT責任者、システム担当、経営層、法務、広報、個人情報保護担当、委託先、保守ベンダー、フォレンジック事業者などの連絡先を整理します。RACI表などで、判断者・実行者・報告先を分けると、緊急時の混乱を抑えやすくなります。

### ログ・チケット・会議記録などの運用証跡

規程があるだけでは、実効性を示しにくい場合があります。過去のインシデント対応記録、アラート確認記録、対応チケット、訓練議事録、改善計画、バックアップ復旧テスト結果などを残しておくと、運用実態を説明しやすくなります。★4では文書確認に加えて実地審査が行われるため、記録や画面等を示せる状態にしておくことが重要です。

## 具体的なCSIRT構築の進め方

#### 1. 対象範囲と重要資産を整理する

どの事業、システム、拠点、クラウド環境を対象にするかを決めます。売上への影響、顧客情報、機密情報、停止時の代替可否などから優先順位をつけます。

#### 2. 想定するインシデントを決める

ランサムウェア、標的型メール、Web改ざん、不正アクセス、情報漏えい、クラウドアカウント侵害、委託先起因の事故など、自社で現実的に起こり得るシナリオを設定します。

#### 3. 役割と意思決定権限を定める

システム停止やアカウント停止を誰が承認できるか、取引先への報告を誰が判断するか、経営層へのエスカレーション条件を明文化します。

#### 4. 手順書と連絡網を整備する

検知から復旧までのフローと、社内外の連絡先を一つの手順としてまとめます。緊急時に検索しなくても使える状態にすることが大切です。

#### 5. 監視・検知と技術対応を接続する

SOCやEDRのアラートを誰が確認し、どの条件でCSIRTへ上げるかを定めます。脆弱性診断やペネトレーションテストで見つかった問題も、重大度に応じてCSIRTや経営層へ共有する仕組みが有効です。

#### 6. 演習を行い、改善する

机上演習や模擬インシデント対応を行い、連絡遅延、権限不足、連絡先の不備、バックアップ復旧の課題などを確認します。演習後は改善計画を作成し、規程・連絡網・技術対策を更新します。

## SOC・脆弱性診断・ペネトレーションテストとの関係

CSIRTは「事故対応の司令塔」であり、SOCや脆弱性診断とは役割が異なります。ただし、これらを分断せず連携させることで、SCS評価制度への対応力を高めやすくなります。

| 施策 | 主な役割 | **CSIRT**との接点 |
|---|---|---|
| SOC／ログ監視 | 不正通信や異常挙動を検知する | 重大アラートをCSIRTへエスカレーションする |
| Webアプリケーション診断 | Webアプリの脆弱性を確認する | 高リスク脆弱性を是正し、悪用時の対応手順へ反映する |
| プラットフォーム診断 | OS・ミドルウェア・ネットワーク機器等を確認する | 侵入経路になり得る設定不備や既知脆弱性を減らす |
| ペネトレーションテスト | 攻撃者視点で侵入・横展開・権限昇格等の成立性を検証する | 実際の攻撃シナリオを演習や対応計画へ反映する |
| DFIR | インシデント発生後の調査・証拠保全・原因分析を行う | CSIRTの調査機能を外部から補完する |

## 対応しなかった場合に起こり得る問題

インシデント対応体制が曖昧なままだと、技術的な被害そのものより、意思決定の遅れによって損失が拡大することがあります。たとえば、感染端末を止める権限者が分からず横展開を許す、契約上の報告期限を見落とす、ログを消して原因調査ができなくなる、復旧優先順位が決まっておらず重要業務の再開が遅れる、といった問題です。

また、取引先からSCS評価制度の★取得や同等水準の対応を求められた際に、体制や証跡を説明できなければ、新規取引の審査や契約更新で追加対応を求められる可能性があります。SCS評価制度への準備は、単なる認証取得ではなく、事業継続と取引先対応を含めた経営課題として進めることが重要です。

## 費用や期間を左右する要因

CSIRT構築の費用は、専任組織を置くか、既存部門で兼務するか、SOCやDFIRを外部委託するかによって大きく異なります。特に費用を左右するのは、対象拠点数、監視対象、既存ログ基盤の有無、24時間365日の対応要否、外部通報やフォレンジック支援の契約範囲、演習の頻度などです。

期間も一律ではありません。既にISMSや情報セキュリティ規程が整備され、連絡体制やSOC運用がある企業は既存資産を活用できます。一方、規程・ログ管理・バックアップ・責任分担が未整備の場合は、SCS評価制度の申請前に複数の改善を並行して進める必要があります。稟議では「CSIRT構築費」だけでなく、監視、診断、演習、外部専門家、復旧対策を含めた年間運用費として説明すると実態に合いやすくなります。

## サービス提供会社を選ぶときのチェックポイント

外部支援を利用する場合は、規程作成だけでなく、実際のインシデント対応、DFIR、SOC、脆弱性診断、ペネトレーションテストまで理解しているかを確認するとよいでしょう。文書だけを整えても、実際の事故時に動けなければ意味がありません。

RFPや見積依頼では、SCS評価制度のどの要求事項を支援対象とするか、成果物、演習の有無、緊急時の連絡可能時間、フォレンジック対応、再委託、機密情報の扱い、改善後の再評価まで確認します。特に「誰がインシデント時の実行責任を負うのか」は曖昧にしないことが重要です。

## よくある失敗と注意点

### CSIRTを組織図に載せただけで終わる

名称や体制図だけでは実効性は高まりません。連絡先、重大度、報告基準、停止権限、復旧判断、外部連携まで具体化する必要があります。

### 情報システム部門だけで完結させる

重大インシデントでは、法務、広報、営業、人事、経営層などの判断が必要です。顧客説明や個人情報漏えい対応、事業停止判断はIT部門だけでは決められないため、平時から役割を整理します。

### 演習をしない

手順書は、実際に使って初めて不備が見つかります。連絡先が古い、承認者に連絡がつかない、バックアップから戻せない、といった問題は演習で発見できます。年1回など自社に合った頻度で訓練し、改善履歴を残すことが有効です。

## Librus株式会社が支援できること

Librus株式会社では、SCS評価制度への対応に向けて、現状評価から要求事項とのギャップ整理、規程・体制整備、技術対策、改善・運用まで一気通貫で支援できます。

- SCS評価制度の要求事項に基づく現状評価・ギャップ分析
- CSIRT／インシデント対応体制の設計、役割分担、連絡網の整備
- インシデント対応規程、手順書、エスカレーション基準の作成支援
- 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
- 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
- インシデント対応演習、教育・訓練、改善計画の策定
- 経営層・情報システム部門・現場部門をまたぐ推進体制の整理

企業ごとに既存のISMS、社内規程、SOC、委託先管理の状況は異なります。必要な対策だけを切り出すのではなく、既存資産を活かしながらSCS評価制度への適合と実際のインシデント対応力の両方を高めることが重要です。

## よくある質問

**Q1. SCS**評価制度を取得するには**CSIRT**の設置が必須ですか？

特定の名称の専任組織を置くことより、インシデント発生時の責任者、連絡、判断、封じ込め、復旧などの機能が実効的に整備されていることが重要です。企業規模に応じて兼務体制や外部専門家の活用も検討できます。

**Q2. ★3**でもインシデント対応体制は必要ですか？

SCS評価制度は★3・★4ともに「インシデントへの対応」「インシデントからの復旧」を含む要求事項体系です。★4はより包括的な対策を想定しているため、取得を目指す段階に応じて要求事項・評価基準を確認する必要があります。

**Q3. SOC**と**CSIRT**は同じものですか？

同じではありません。SOCは監視・検知を中心とする機能、CSIRTはインシデント対応の司令塔として、判断、関係者調整、封じ込め、復旧、外部連携などを担います。両者の連携が重要です。

**Q4.** インシデント対応規程があれば十分ですか？

規程だけでなく、連絡網、対応記録、演習記録、復旧テスト、教育記録など、実際に運用されていることを示す証跡を残すことが重要です。

**Q5.** 外部の**CSIRT**／**DFIR**サービスを使ってもよいですか？

自社だけで専門人材を確保できない場合、外部支援を活用する方法は有効です。ただし、経営判断や顧客への報告など自社でしか行えない役割は残るため、社内外の責任分界を明確にします。

**Q6.** ペネトレーションテストは**CSIRT**構築に必要ですか？

必ずしもCSIRT構築そのものの必須条件ではありませんが、攻撃シナリオや侵入後の影響を具体化し、対応手順や優先順位を見直す材料になります。

**Q7.** どのような演習を行えばよいですか？

最初は机上演習でも構いません。ランサムウェア、情報漏えい、クラウドアカウント侵害などを想定し、誰が何分以内に誰へ連絡し、どの判断をするかを確認します。その後、技術担当を含む実践的な訓練へ段階的に広げます。

**Q8. SCS**評価制度の申請受付はいつからですか？

IPAは★3・★4の登録申請について2027年3月の受付開始を予定しています。準備に時間がかかる規程・体制・技術対策は、申請直前ではなく早めに着手することが重要です。

## まとめ｜SCS評価制度では「事故後に動ける体制」まで整備する

SCS評価制度への対応では、防御策だけでなく、インシデントを検知し、適切に報告し、被害を封じ込め、事業を復旧させる体制が重要です。CSIRTはその司令塔となる機能ですが、専任組織の新設そのものが目的ではありません。自社の規模とリスクに応じて、既存部門と外部専門家を組み合わせ、実際に動ける仕組みを作ることが重要です。

特に従業員100～1,000名規模の企業では、SCS評価制度対応をきっかけに、規程、連絡網、SOC、ログ管理、DFIR、脆弱性診断、演習をばらばらに整備するのではなく、ひとつのインシデント対応プロセスとしてつなげることで、取引先への説明力と事業継続力を同時に高めやすくなります。

## SCS評価制度への対応やCSIRT構築でお困りの場合はご相談ください

Librus株式会社では、「どこまでCSIRTを整備すべきか分からない」「既存の情報セキュリティ体制をSCS評価制度にどうつなげるべきか」「規程はあるが運用証跡が不足している」「SOCやDFIRまで内製するのは難しい」といった段階からご相談いただけます。

対象範囲や実施方法がまだ決まっていない場合でも、現在の体制・契約・システム構成を確認し、SCS評価制度の要求事項とのギャップと優先順位を整理することで、必要以上に対策範囲を広げず、経営・取引・事業継続の観点から現実的な対応計画を検討できます。

## 公的情報の確認先

IPA「SCS評価制度」: https://www.ipa.go.jp/security/scs/index.html

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

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

IPA「SCS評価制度の評価用ガイド等を公開」: https://www.ipa.go.jp/pressrelease/2026/press20261028.html

IPA「インシデント発生時の緊急対応体制の整備」: https://www.ipa.go.jp/security/economics/practices_navi/practice226.html

JPCERT/CC「CSIRTマテリアル」: https://www.jpcert.or.jp/csirt_material/

## 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