

SCS評価制度に必要なインシデント対応体制とは？初動対応から報告まで

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）への対応では、攻撃を防ぐ対策だけでなく、異常を検知した後に被害を抑え、必要な相手へ報告し、事業を復旧できる体制が重要になる。結論から言えば、必要なのは「連絡網を作ること」ではない。判断権限、初動手順、証拠保全、社内外への報告、復旧判断、再発防止までを一つの業務プロセスとして整え、訓練で実効性を確認することである。

本記事では、従業員100～1,000名程度の企業を想定し、経営者と実務担当者が準備すべき内容を、初動対応から最終報告まで具体的に解説する。なお、SCS評価制度は制度設計や運用準備が進行中であり、申請時には経済産業省が公開する最新版の要求事項・評価基準を確認する必要がある。

この記事で分かること

- SCS評価制度を見据えたインシデント対応体制の全体像
- 発見直後から封じ込め、報告、復旧、再発防止までの実務手順
- 経営層、情報システム部門、現場部門、外部専門家の役割分担
- 報告先・報告期限を判断するための基準と、訓練・証跡の残し方
- 見積依頼や支援会社選定で確認すべきポイント

SCS評価制度とインシデント対応体制の関係

SCS評価制度は、企業のサプライチェーン上の立ち位置や影響度に応じて、必要なセキュリティ対策を段階的に示し、取引先が対策状況を確認しやすくするための制度である。経済産業省の公表資料では、☆3・☆4・☆5の水準が想定され、☆3と☆4は2026年度末頃の制度開始が予定されている。制度への対応は、認証取得そのものを目的にするのではなく、取引先から求められる説明責任と、事故発生時の事業継続力を高める取り組みとして捉えることが大切だ。

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）](#)

インシデント対応に関して重要なのは、方針や連絡先の存在だけではない。異常を検知できること、対応責任者が判断できること、影響範囲を把握できること、関係者へ適時に報告できること、そして

訓練や点検を継続することが問われる。IPAの2026年版資料も、対応を「検知・初動対応」「報告・公表」「復旧・再発防止」の三段階で整理している。

出典: [IPA: 中小企業のためのセキュリティインシデント対応の手引き\(2026年6月\)](#)

なぜ今、インシデント対応体制が必要なのか

サプライチェーンでは自社の事故が取引先の事業停止につながる

製造、物流、IT、人材、専門サービスなどでは、取引先から預かったデータ、接続用アカウント、共有システムを日常的に扱う。攻撃者が自社を踏み台にして取引先へ侵入すれば、自社の復旧だけで問題は終わらない。受発注停止、納期遅延、接続遮断、監査対応、契約見直しへ波及する可能性がある。このため、対応体制には「取引先への通知条件」と「接続を止める判断権限」をあらかじめ組み込む必要がある。

100～1,000名規模では、責任の空白が生まれやすい

この規模の企業では、専任CSIRTがない一方、拠点、クラウド、委託先、子会社が増えていることが多い。情報システム部門が技術対応、総務が個人情報、広報が公表、営業が顧客説明を担当していても、全体を指揮する人が決まっていないケースは珍しくない。事故発生後に会議を開いて役割を決めるのでは遅い。平時に指揮命令系統と代行順位を決めておくことが重要となる。

法令・契約・業界ルールで報告が必要になる

個人データの漏えい等で個人の権利利益を害するおそれがある場合、個人情報保護委員会への報告と本人通知が必要となる。委員会は速報を概ね3～5日以内と案内している。業種によっては所管省庁への報告、犯罪性がある場合は警察への相談、契約に基づく委託元への通知も検討しなければならない。重要なのは、法務・個人情報担当を初動から参加させ、報告要否の判断を後回しにしないことである。

出典: [個人情報保護委員会: 漏えい等報告・本人への通知の義務化について](#)

対応しなかった場合に起こり得る問題

初動が遅れると、感染端末から認証情報が窃取され、管理者権限の奪取やバックアップ破壊へ進むことがある。反対に、慌てて端末の電源を切ったり初期化したりすれば、メモリやログに残る調査材

料を失い、侵入経路や漏えい範囲を説明できなくなる。技術的な失敗は、顧客対応や法的判断の遅れに直結する。

報告の遅れや不正確な公表は、事故そのもの以上に信用を損なう場合がある。第一報で原因や漏えい件数を断定し、その後訂正を重ねれば、取引先は管理能力に疑問を持つ。第一報では確認済み事実、未確認事項、実施済み措置、次回更新予定を分けて示すべきだ。

経営面では、復旧費、フォレンジック調査費、法律相談費、通知・問い合わせ対応費に加え、受注停止や契約解除による逸失利益が発生し得る。インシデント対応体制はIT部門の作業手順ではなく、事業継続と取引維持の仕組みである。

対象となる企業・システム・場面

対象は、SCS評価制度への申請を直接予定する企業だけではない。主要顧客からセキュリティ調査票を受ける企業、委託元の情報やシステムを扱う企業、M&A・IPO・大手企業との新規取引を控える企業にも有効である。対象システムは、基幹系だけに限定しない。Webアプリケーション、クラウド、VPN、メール、ID管理、工場・倉庫の設備、委託先が運用する環境まで、事故が取引先や事業継続に与える影響で優先順位を決める。

例えば、顧客向け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にはプラットフォーム診断が有効である。さらに、攻撃者が複数の弱点を組み合わせることで目的を達成できるかを検証するにはペネトレーションテストが役立つ。ただし、これらは予防・検証策であり、インシデント対応体制の代替ではない。診断結果を監視ルール、対応手順、復旧計画へ反映して初めて、一連の管理になる。

SCS評価制度を見据えたインシデント対応の実施手順

1. 経営層が対応方針と判断権限を決める

最初に、何を守るか、どの程度の停止を許容するか、誰が緊急停止や外部公表を決めるかを定める。経営層は、重要業務ごとの最大許容停止時間、顧客・社会への影響、法令・契約上の報告義務を確認し、対応責任者と代行者を任命する。現場に丸投げせず、事業停止と復旧の優先順位を判断する役割を担う。

2. 対象範囲と重要資産を可視化する

資産台帳、ネットワーク構成図、クラウド一覧、データフロー、委託先一覧、取引先との接続関係を整える。すべてを同時に詳細化する必要はない。まず、停止すれば売上・生産・出荷に影響するシステム、機密情報を保有する環境、取引先へ接続する経路を優先する。資産の所有部門と技術的な管理者を分けて記録すると、事故時の連絡が速くなる。

3. 検知・連絡受付を一本化する

従業員が「怪しいメールを開いた」「端末が暗号化された」「取引先から不審な通信を指摘された」と気づいたとき、迷わず連絡できる窓口を設ける。電話、チャット、専用メールなど複数経路を用意し、夜間・休日の受付方法も決める。連絡内容は、発見日時、端末・アカウント、現象、直前の操作、業務影響、連絡者を基本項目とする。

4. 深刻度を分類し、対応体制を立ち上げる

深刻度は、技術的な派手さではなく、情報の機密性、影響人数、重要業務の停止、取引先への波及、攻撃継続の可能性、法令・契約報告の要否で判断する。重大事案では、インシデント責任者の下に、技術、法務・個人情報、事業部門、広報・顧客対応、経営判断の各担当を配置する。外部のフォレンジック会社、保守ベンダー、弁護士、保険会社への連絡条件も決めておく。

5. 封じ込めと証拠保全を両立する

感染端末やサーバーはネットワークから隔離し、不正アカウントの停止、侵害された認証情報の変更、外部公開の一時停止などを行う。ただし、電源断、再起動、初期化、ログ削除は証拠を失うおそれがある。操作前に、実施者、日時、対象、目的、結果を記録し、必要に応じてメモリ、ディスク、ログ、クラウド監査証跡を保全する。証拠はアクセス権を限定し、取得者と受渡履歴を残す。

6. 影響範囲を調査し、報告要否を判断する

発生日時、侵入経路、影響したアカウント・端末・データ、外部送信の有無、業務停止範囲を時系列で整理する。調査中で断定できない事項は「未確認」と明記する。報告先は、経営者、取締役会、委託元、顧客、個人情報保護委員会、所管省庁、警察、IPA、JPCERT/CCなどから、法令、契約、被害拡大防止の必要性に基づいて選ぶ。

7. 第一報、続報、最終報を使い分ける

第一報の目的は、早期に事実と対応状況を共有し、相手が被害拡大防止策を取れるようにすることだ。発覚日時、確認済みの事象、現時点の影響、実施済み措置、顧客側に依頼する行動、問い合わせ先、次回更新予定を記載する。続報では調査の進展と影響範囲を更新し、最終報では根本原因、被害、対応経過、復旧確認、再発防止策、実施期限と責任者を示す。

8. 安全を確認して復旧し、再発防止を管理する

復旧は、単にシステムが起動することではない。侵入経路の閉鎖、認証情報の再設定、マルウェア除去、バックアップの健全性、監視強化を確認したうえで段階的に行う。再発防止策は、緊急・短期・中長期に分け、重大度、悪用可能性、事業影響、実施難易度で優先順位を付ける。経営会議等で期限と担当を追跡し、完了後に再診断やペネトレーションテストで有効性を確かめる。

報告先と報告内容を平時に整理する

主な報告先	判断の根拠	第一報で重視する内容
経営層・取締役会	事業・財務・信用への影響	業務停止、顧客影響、判断が必要な事項
委託元・主要取引先	契約、接続関係、被害波及防止	影響可能性、遮断措置、相手に依頼する対応
個人情報保護委員会	個人情報保護法上の報告対象	概要、漏えい項目、原因、二次被害防止策
警察・IPA・JPCERT/CC等	犯罪性、届出、技術支援・情報共有	攻撃手口、痕跡、被害状況、支援依頼
顧客・本人・社会	法令、被害防止、説明責任	確認済み事実、注意事項、問い合わせ窓口

出典: [参考:IPAのインシデント対応手引き・報告先一覧](#)

平時に準備すべき資料と成果物

実効性を示すには、規程だけでなく、使える資料と運用記録が必要になる。準備すべき主な資料は、インシデント対応方針、対応手順書、緊急連絡網、役割分担表、深刻度基準、資産台帳、ネットワーク・データフロー図、委託先・取引先一覧、法令・契約上の報告要件一覧、証拠保全手順、第一報・最終報のひな形、復旧判定チェックリストである。

成果物には、文書の制定日・承認者・版数を含める。訓練では、参加者、想定シナリオ、判断内容、所要時間、発見した課題、改善担当、期限を記録する。SCS評価制度への説明では、「文書がある」

だけでなく、「誰がいつ点検し、訓練で何を改善したか」を示せる状態が望ましい。個人情報や機密情報を含む記録は、保管場所、閲覧権限、保存期間、廃棄方法を定める。

実施期間と費用を左右する要因

期間の目安は、現状把握から基本体制・手順の整備まで2～4か月、机上演習と改善まで含めると3～6か月程度で考えると計画しやすい。これは一般的な目安であり、対象拠点、システム数、委託先数、既存規程の成熟度、経営会議の承認サイクルによって変わる。SCS評価制度の最新要件とのギャップが大きい場合や、SOC・ログ管理・バックアップなど技術対策を同時に整備する場合は、より長い期間が必要になる。

費用は、対象範囲、インタビュー対象部門、規程や台帳の整備量、演習の規模、技術検証、24時間対応の有無、フォレンジックやインシデントレスポンスの待機契約を含むかで変動する。社内稟議では、制度対応費だけでなく、取引継続、顧客監査への回答力、事故時の停止時間短縮、報告遅延リスクの低減という効果を説明すると判断しやすい。

支援会社の選び方とRFP・見積依頼時の確認項目

支援会社は、制度文書を作成できるだけでなく、実際のインシデント対応、デジタルフォレンジック、診断、復旧支援まで理解しているかを確認したい。紙上の手順が技術的に実行できなければ、緊急時には機能しない。経営層への説明、現場ヒアリング、委託先との責任分界整理を一貫して支援できることも重要である。

RFPや見積依頼では、①参照するSCS評価制度資料の版、②対象組織・拠点・システム、③現状調査の方法、④作成・改訂する成果物、⑤演習シナリオと参加部門、⑥技術検証の範囲、⑦課題の優先順位付け方法、⑧機密情報の保管・再委託条件、⑨支援終了後のフォロー、⑩実際の事故発生時の支援可否を確認する。価格だけでなく、社内で運用を継続できる状態まで移管されるかを比較すべきだ。

よくある失敗と注意点

連絡網を作って終わる

担当者名が並んでいても、誰が重大度を判定し、誰が停止・公表を決めるか不明では動けない。権限、代行順位、判断期限まで定める。

IT部門だけで手順を作る

報告・公表、顧客補償、事業停止はIT部門だけでは決められない。法務、個人情報、広報、営業、事業責任者、経営層を設計段階から参加させる。

委託先と責任分界が曖昧

クラウドや保守を委託していても、顧客・当局への説明責任まで移転するとは限らない。ログ取得、初動、報告、証拠保全の担当と時間条件を契約・運用手順で確認する。

訓練が台本の読み合わせになる

実効性を見るには、情報が不足した状態で判断する訓練が必要だ。ランサムウェア、Webアプリケーション侵害、委託先からの漏えいなど、自社の事業に近いシナリオを使い、連絡速度と意思決定を測る。

復旧を急ぎ、根本原因を残す

バックアップから戻しても、侵入経路や窃取された認証情報が残れば再侵入される。復旧条件を明文化し、脆弱性診断、プラットフォーム診断、ペネトレーションテスト、監視強化を適切に組み合わせる。

Librus株式会社が提供できる支援

Librus株式会社は、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)にかかるコンサルティングとして、現状評価、対象範囲の整理、要求事項とのギャップ分析、規程・手順・証跡の整備、経営層向け説明、机上演習、改善計画の策定を支援する。企業ごとの事業、組織、取引関係、既存システムを踏まえて個別に設計するため、既成の規程を導入するだけの対応にはしない。

また、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、インシデントレスポンス、デジタルフォレンジックまで一気通貫で対応できる。制度対応で見つかった課題を、技術面と経営面の双方から整理し、改善・運用までつなげられる点が強みである。大企業から中堅・中小企業まで、M&A、IPO、取引先監査など重要局面にも対応している。

よくある質問

Q1. SCS評価制度への対応では、CSIRTの設置が必須ですか？

名称としてのCSIRTより、責任者、役割、連絡経路、判断権限、外部支援先が明確で、実際に機能することが重要である。専任組織が難しい企業では、既存部門を横断する仮想チームとして設計できる。最終的には申請時点の評価基準を確認する必要がある。

Q2. 情報システム担当者が数名でも体制を作れますか？

可能である。社内は意思決定と事業影響の把握に集中し、24時間監視、フォレンジック、法的助言など専門性が必要な機能を外部と分担する設計が現実的だ。外部委託しても責任者と連絡手順は社内に残す。

Q3. インシデント対応手順はどの頻度で見直すべきですか？

少なくとも年1回を基本とし、組織変更、システム更改、主要委託先の変更、重大インシデントや訓練後にも見直す。連絡先だけは人事異動の都度更新し、夜間連絡が通じるかも確認する。

Q4. 机上演習では何を確認しますか？

検知から責任者への連絡時間、重大度判定、隔離・停止判断、取引先や当局への報告、公表文の承認、復旧判断を確認する。正解を当てる場ではなく、手順と責任の空白を見つける場として実施する。

Q5. 事故時に端末の電源を切ってはいけないのですか？

常に禁止という意味ではない。被害拡大防止を優先しつつ、電源断で揮発性データやログを失う可能性を考慮する。可能ならネットワーク隔離を先に行い、専門家の指示を受ける。人命や設備安全に関わる場合は、安全確保を最優先する。

Q6. 取引先への報告は、事実が確定してからでよいですか？

契約上の期限や被害拡大のおそれによっては、確定前の第一報が必要になる。確認済み事実と未確認事項を分け、次回更新時刻を示す。自社だけで判断せず、法務・契約担当を交えて決める。

Q7. 診断やペネトレーションテストだけで十分ですか？

十分とは限らない。診断は弱点発見、ペネトレーションテストは攻撃経路の検証に有効だが、検知、報告、復旧、再発防止の組織運用は別途必要である。両者を連携させることで対応力が高まる。

Q8. まだ対象範囲が決まっていなくても相談できますか？

相談できる。主要取引、重要業務、保有情報、システム構成、委託関係を確認し、優先順位の高い範囲から段階的に決める方法がある。最初から全社一律で始める必要はない。

まとめ:SCS評価制度対応は、動ける体制まで整備する

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)を見据えたインシデント対応では、方針、責任者、初動手順、証拠保全、報告先、復旧条件、再発防止を一つの流れとして整備する必要がある。重要な結論は、「誰が、何を根拠に、いつまでに判断するか」を平時に決め、訓練で確認することだ。

制度対応を取引先への説明資料づくりで終わらせず、事業停止時間の短縮、顧客との信頼維持、法令・契約対応の迅速化につなげることが望ましい。制度の最新版を確認しながら、自社の重要業務とサプライチェーン上の責任に合う体制を構築したい。

SCS評価制度への対応方針を、現状整理から相談できます

Librus株式会社では、SCS評価制度の対象範囲や進め方が決まっていない段階から相談を受け付けている。現状の規程・体制・システムを整理し、優先すべき課題、必要な成果物、想定期間、技術対策の可否を可視化することで、経営会議や社内稟議に必要な判断材料を整えられる。インシデント対応手順の策定、机上演習、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、改善・運用まで、必要な範囲を組み合わせた支援が可能だ。まずは、取引先から求められている水準や現在の悩みを共有いただきたい。

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](tel:03-6772-8015)

お問い合わせフォーム: <https://librus.co.jp/contact>