

シミュレーション演習： サイバー攻撃の インシデント対応



所要時間
2時間



参加人数
最大30名

🎯 対象

インシデント対応計画 (IRP) の策定に携わる従業員 (※技術職の方だけでなく、専門知識のない他部署のメンバーもご参加いただけます)

📋 概要

この演習は、参加者が特定の役割を担い、架空のシナリオに沿って行動するロールプレイ型のシミュレーションです。単なる知識の習得にとどまらず、不測の事態に不可欠なチーム連携や状況判断力の養成に重点を置いています。この演習を通じて、社内のインシデント対応マニュアルの課題を浮き彫りにし、組織全体の対応力を高めることを目的とします。

🎯 目標

この演習を通じて、以下の3点の習得を目指します。

- 重要性の理解：インシデント対応計画の必要性を説明できる
- 役割の明確化：インシデント発生時における各部署・各自の責任範囲を正確に把握する
- 対応力の向上：緊迫した状況下での適切な判断・意思決定を実践できる

🛠️ 準備するもの

- インシデント対応リスト
- タイマー・ストップウォッチ
- 役割カード (インシデントコマンダー、ITセキュリティ責任者、広報、法務、人事、部門などの責任者)
- シナリオカード
- ホワイトボード・フリップチャート
- ホワイトボードマーカー
- 筆記用具・ノート

👤 役割分担

《**進行役**》：演習全体のまとめ役です。全員が発言しやすい環境を整えつつ、議論をリードします。また、状況に応じた課題 (追加シナリオ) を投入し、現場の緊張感をコントロールします。

《**参加者**》 割り当てられた役割 (IT、広報、法務など) の担当者として、事態収束に向けて主体的に行動します。情報の集約、他部門との連携、意思決定の実践が主な任務です。

《**評価者**》 第三者の視点で演習を評価します。組織の強みや改善が必要な箇所を特定し、訓練後の振り返りや、マニュアルのアップデートに向けたフィードバックを行います。

《**アドバイザー**》 直接的な議論には加わず、専門的な観点から適宜ヒントや助言を行います。客観的な観察を通じて、参加者の気づきを促し、訓練の質を向上させるサポーターです。

《**記録係**》 「いつ・誰が・何を判断したか」を記録します。特に既存のマニュアルと実際の動きのズレや議論になった重要ポイントを漏らさずメモします。

はじめに

🕒 所要時間：10分

サイバー攻撃が起きたとき、技術だけで解決することは不可能です。現場での迅速な情報共有、意思決定の明確化、そして状況に合わせた柔軟な動きこそが、組織の命運を分けます。この演習では、リアルティのあるシナリオを通じて、チームワークと判断力を鍛えます。実際の役割になりきり、組織を守るための実戦力を身につけましょう。

アクティビティ① 並べ替え演習：インシデント発生時の手順

🕒 所要時間：30分

【準備するもの】

- ・ タイマー・ストップウォッチ
- ・ 筆記用具・ノート
- ・ インシデント対応リスト(アクティビティ①添付資料参照)

【アクティビティの目的】

このアクティビティでは、実際にトラブルが起きた場面を想定して、「まず何をすべきか」「誰にどう連絡するか」「判断の基準は何か」といった一連の流れを確認します。

【アクティビティで使うシナリオの説明】

「社内の主要サーバーがランサムウェアに感染。データが使えなくなっただけでなく、攻撃者から『元に戻してほしければ大金を支払え』と脅迫が届きました」

【アクティビティの流れ】

1. 参加者全員にインシデント対応リストを配布します。リストの項目は順不同になっています。
2. まずは10分間、どの順番で動くべきか、自分なりに順番を並べ替えます。
3. つぎに10分間、3～4人のグループに分かれます。なぜその順番を選んだのか理由を話し合いながら、グループとしての答えをひとつにまとめます。
4. 最後に10分間、全員で答え合わせをします。正しい順番や手順を確認して、推奨される手順を確認することで、実際の現場で使える知識を身につけます。

【推奨される対応手順のポイント】

業界標準の「最も効率的なインシデント対応」にもとづいた、重要な項目は次のとおりです。

1. 社内規定にもとづき、状況をすぐに報告する
2. インシデント対応チームを招集する
3. 被害に遭ったシステムをネットワークから切り離す
4. インシデントの経緯を時系列で細かく記録する
5. バックアップからデータを復元できるか確認する
6. 社内外の関係者へ情報を周知する
7. 法令や規制に従い、必要な報告・通知の手続きを行う
8. 弁護士などの専門家に相談する
9. 社内規定にもとづき、ランサムウェア攻撃の対応計画を実行する
10. 社内規定にもとづき、必要に応じて捜査機関へ通報する

アクティビティ② ロールプレイ演習：インシデント発生時の対応

🕒 所要時間：35～60分

【準備するもの】

- ・ 役割カード(アクティビティ②添付資料参照)
- ・ 追加シナリオ(アクティビティ②添付資料参照)
- ・ タイマー・ストップウォッチ
- ・ ホワイトボード・フリップチャート
- ・ ホワイトボードマーカー
- ・ 筆記用具・ノート
- ・ 社内のインシデント対応マニュアル

【アクティビティの目的】

このアクティビティでは、部門を超えた連携が必要なトラブルを想定し、実際の役職や役割になりきって、社内外への情報の伝え方や決断を下すまでの流れをシミュレーションします。

グループごとにインシデント対応チームを作り、自分自身の実際の役割、または配布されたカードに書かれた役割を演じながらアクティビティを行います。

【アクティビティの流れ】

1. 各グループにシナリオカードを配ります。複雑なトラブルが発生した場面を想定した、具体的な状況が書かれています。
2. まずは20分間、それぞれの役割や社内規定に従って、グループで対応方針を話し合い、計画を立てます。
3. つぎに各グループ5分間ずつ、それぞれが立てた計画を発表します。
4. ここで、さらに状況を悪化させるシナリオを追加します(例：「マスコミに情報が漏れた」などの新しいトラブルが発生し、事態が深刻化する)。
5. 新たなトラブルに対して、さらに10分間、グループで先ほどの計画を練り直します。
6. 最後に、見直した計画と社内規定に従ってどこをどう調整したかを発表します。

【アクティビティのヒント】

- ・ グループで話し合うときは、社内のインシデント対応計画を参照する
- ・ 判断までの過程を共有するために、頭の中にある考えを積極的に声に出して伝える
- ・ 実際の役割や役職にもとづき、参加者全員がそれぞれの責任を果たせるように協力し合う
- ・ 実際にインシデントが発生したとき、自分の役割で具体的にどう行動するかを考える

ディスカッション:振り返りと改善

🕒 所要時間:15分

【質問事項】

- アクティビティ①で確認した優先すべき行動は、どのように役立ちましたか？
- 社内のインシデント対応マニュアルの中で、「実際に行うのは難しい」と感じた部分はありましたか？
- 今の対応手順の中に、現在の組織体制や実務の流れと「ズレている」と感じる部分はありましたか？
- 部署を越えた情報の共有や担当者同士の連携はスムーズに行えましたか？
- もし実際にインシデントが起きたとき、自分の役割をしっかりと果たすために、どのようなトレーニングやサポートが必要だと感じましたか？

【想定される回答・意見の例】

- 直面した課題:部署間の細かな調整や正しい連絡先の把握、「誰がどこまで決めていいのか」という権限のあいまいさ
- 改善が必要な点:報告手順が不明確、連絡先情報が古い、誰が最終判断を下すかが不明確、すぐに使える通知用のテンプレートがない
- 今後の改善策:定期的な部門合同トレーニングの実施、連絡先情報の更新、意思決定ツリーの可視化、すぐに参照できる「役割別クイックガイド」の作成
- 必要なサポート:役割ごとの具体的な行動マニュアル、実際のメンバーとの顔合わせを兼ねた演習、最新のインシデント対応計画に関するトレーニング

まとめ

🕒 所要時間:5分

【アクティビティ①～②のまとめ】

- アクティビティ①の並べ替え演習で組織の対応手順を理解し、アクティビティ②のロールプレイ演習で「実際に起こりうるリアルな課題」を浮き彫りにしました。
- 実際の役割や役職にもとづき、個人や部門がどう動くべきかを事前に確認しておくことは、迅速で効果的なインシデント対応に欠かせません。
- いかなる事態においても、社内規定にもとづきながら、状況に合わせて柔軟に判断・対応することが重要です。

さらなる改善に向けて

- 演習で見つかった課題を反映し、インシデント対応計画をアップデートする
- いざという時に迷わないよう、連絡先情報や連絡手段を最新の状態に更新する
- 役割分担や意思決定の権限におけるあいまいさをなくし、部門間でのスムーズな連携を図る
- 実際のメンバーとの演習を定期的に行い、組織全体の対応力を磨き続ける

アクティビティ①添付資料：インシデント対応リスト

参加者6名につき、このページを1枚印刷して線にそって切り取ってください。1名につき1枚ずつカードを配布します。（厚紙への印刷をおすすめします）



《インシデント対応リスト》 ☐ 被害に遭ったシステムをネットワークから切り離す ☐ 社内規定にもとづき、状況をすぐに報告する ☐ バックアップからデータを復元できるか確認する ☐ 社内規定にもとづき、必要に応じて捜査機関へ通報する ☐ 弁護士などの専門家に相談する ☐ 社内規定にもとづき、ランサムウェア攻撃の対応計画を実行する（要相談） ☐ 社内外の関係者へ情報を周知する ☐ インシデントの経緯を時系列で細かく記録する ☐ 法令や規制に従い、必要な報告・通知の手続きを行う ☐ インシデント対応チームを招集する	《インシデント対応リスト》 ☐ 被害に遭ったシステムをネットワークから切り離す ☐ 社内規定にもとづき、状況をすぐに報告する ☐ バックアップからデータを復元できるか確認する ☐ 社内規定にもとづき、必要に応じて捜査機関へ通報する ☐ 弁護士などの専門家に相談する ☐ 社内規定にもとづき、ランサムウェア攻撃の対応計画を実行する（要相談） ☐ 社内外の関係者へ情報を周知する ☐ インシデントの経緯を時系列で細かく記録する ☐ 法令や規制に従い、必要な報告・通知の手続きを行う ☐ インシデント対応チームを招集する	《インシデント対応リスト》 ☐ 被害に遭ったシステムをネットワークから切り離す ☐ 社内規定にもとづき、状況をすぐに報告する ☐ バックアップからデータを復元できるか確認する ☐ 社内規定にもとづき、必要に応じて捜査機関へ通報する ☐ 弁護士などの専門家に相談する ☐ 社内規定にもとづき、ランサムウェア攻撃の対応計画を実行する（要相談） ☐ 社内外の関係者へ情報を周知する ☐ インシデントの経緯を時系列で細かく記録する ☐ 法令や規制に従い、必要な報告・通知の手続きを行う ☐ インシデント対応チームを招集する
《インシデント対応リスト》 ☐ 被害に遭ったシステムをネットワークから切り離す ☐ 社内規定にもとづき、状況をすぐに報告する ☐ バックアップからデータを復元できるか確認する ☐ 社内規定にもとづき、必要に応じて捜査機関へ通報する ☐ 弁護士などの専門家に相談する ☐ 社内規定にもとづき、ランサムウェア攻撃の対応計画を実行する（要相談） ☐ 社内外の関係者へ情報を周知する ☐ インシデントの経緯を時系列で細かく記録する ☐ 法令や規制に従い、必要な報告・通知の手続きを行う ☐ インシデント対応チームを招集する	《インシデント対応リスト》 ☐ 被害に遭ったシステムをネットワークから切り離す ☐ 社内規定にもとづき、状況をすぐに報告する ☐ バックアップからデータを復元できるか確認する ☐ 社内規定にもとづき、必要に応じて捜査機関へ通報する ☐ 弁護士などの専門家に相談する ☐ 社内規定にもとづき、ランサムウェア攻撃の対応計画を実行する（要相談） ☐ 社内外の関係者へ情報を周知する ☐ インシデントの経緯を時系列で細かく記録する ☐ 法令や規制に従い、必要な報告・通知の手続きを行う ☐ インシデント対応チームを招集する	《インシデント対応リスト》 ☐ 被害に遭ったシステムをネットワークから切り離す ☐ 社内規定にもとづき、状況をすぐに報告する ☐ バックアップからデータを復元できるか確認する ☐ 社内規定にもとづき、必要に応じて捜査機関へ通報する ☐ 弁護士などの専門家に相談する ☐ 社内規定にもとづき、ランサムウェア攻撃の対応計画を実行する（要相談） ☐ 社内外の関係者へ情報を周知する ☐ インシデントの経緯を時系列で細かく記録する ☐ 法令や規制に従い、必要な報告・通知の手続きを行う ☐ インシデント対応チームを招集する

アクティビティ②添付資料：役割カードとシナリオカード

このページを1枚印刷して線にそって切り取ってください。

(厚紙への印刷をおすすめします)



役割カード

【ITセキュリティ責任者】

技術的な封じ込めと原因究明

セキュリティ侵害の範囲と性質を特定・評価する

被害拡大を防ぐための封じ込め（隔離など）を行う

原因究明のためのフォレンジック調査（事実関係の調査）を指揮する

外部のセキュリティ専門会社と連携する



役割カード

【インシデントコマンダー】

インシデント対応チームの総責任者

インシデント対応チーム全体の活動を統括し、指示を出す

組織としての重要な戦略的判断を下す

経営陣へ状況の報告を行う

必要なリソースの割り当てと優先順位を決定する



役割カード

【広報責任者】

社内外へのメッセージ管理と
対外コミュニケーションを管理する

既存のコミュニケーションプランを
実行する

ステークホルダー向けの通知を作成する

メディア対応やPRチームと連携する

SNSやニュース報道などの反応を監視する



役割カード

【法務顧問】

インシデントによる法的影響や規制遵守
について助言する

情報漏えい通知法などの法令にもとづき、正しく報告が行われるよう監督する

証拠保全の手順についてアドバイスする
外部向けのコミュニケーションの内容を
チェックする

必要に応じて警察などの捜査機関と
連携する



役割カード

【人事担当者】

インシデントに伴う従業員関連の諸問題
に対応する

社内向けのコミュニケーションを
管理する

内部不正が疑われる場合の調査を
サポートする

影響を受けた従業員のケアやサポートを
調整する

業務継続に必要な人員確保や労務上の
課題に対処する



役割カード

【部門の責任者】

被害を受けた部署を代表する
業務への影響範囲を評価する

事業継続計画の実施

他部門の責任者と連携する

業務の稼働状況をインシデント
コマンダーへ報告する



シナリオ

ランサムウェア攻撃による データ窃取

“社内のファイルがランサムウェアにより暗号化されました。攻撃者は顧客の財務データも盗み出しており、『24時間以内に身代金を支払わなければ、すべての機密情報を一般公開する』と脅迫しています。[さらなる難題] さらに調査の結果、バックアップデータにもすでに2週間前から不正アクセスの形跡があったことが判明しました”



シナリオ

ビジネスメール詐欺

“最高財務責任者（CFO）のメールアカウントが乗っ取られ、偽の口座に約5,000万円を振り込むよう指示するメールが送信されました。振込処理は今朝すでに完了しています。[さらなる難題] さらに、大口の取引先3社に対しても、支払い先情報の変更を求める詐欺メールが送信されていたことが判明しました”



シナリオ

内部不正によるデータ窃盗

“すでに退職が決まっているIT部門の従業員が、顧客の機密データを個人のUSBメモリにコピーし、社外へ持ち出そうとしているところを警備員が制止しました。従業員は『個人的なファイルだ』と主張しています。[さらなる難題] ところが、この従業員のSNSには『これまでの貴重な経験を丸ごと新しい職場へ持っていく』という含みを持たせた投稿がありました”

アクティビティ②添付資料：シナリオと追加シナリオ

このページを1枚印刷して線にそって切り取ってください。

(厚紙への印刷をおすすめします)



シナリオ

サプライチェーン攻撃

“取引先のソフトウェア会社から、アップデートサーバーが攻撃を受け、顧客にマルウェアが拡散された可能性があるとの報告がありました。自社のシステムも昨日、そのアップデートを完了してしまっています。[さらなる難題]ソフトウェア会社は『現在調査中』として、詳細な技術情報の提供を拒んでいます”



シナリオ

物理的なセキュリティ侵害

“夜間のサーバールームで、ネットワークに接続されたパソコンを操作している不審な人物が発見されました。警備員が制止したところ、その人物は『ITチームの従業員だ』と主張しています。[さらなる難題]複数の従業員から『身に覚えのない時間帯にアカウントが利用された形跡がある』との報告が相次いでいます”



シナリオ

クラウドサービス侵害

“利用中のクラウドサービス運営会社から、顧客情報や企業秘密などの機密情報が保管されているサーバーに不正アクセスがあったとの報告を受けました。この侵害はすでに数週間前から続いていた可能性があります。[さらなる難題]運営会社からの初期報告は、発生時期や被害範囲に関する説明に矛盾が多く、正確な状況が掴めていません”



追加シナリオ

“メディアによる暴露：テック系のブログで、自社のインシデントに関する詳細な記事が公開されました。そこには、まだ公表していない内部情報まで含まれています”



追加シナリオ

“監督機関からの報告要求：業界の監督機関から、今回のインシデントに関する詳細と対応状況について、至急報告を求める通達が届きました”



追加シナリオ

“取引先との関係悪化：大口の取引先から『自社への影響を説明せよ』と緊急会議を要求されました。契約の即時解除も辞さないという、極めて厳しい姿勢を示しています”



追加シナリオ

“内部での誤情報拡散：社内のチャットツールで、従業員たちが今回のインシデントについて議論をはじめており、不正確な情報が飛び交っています”



追加シナリオ

“対応措置による二次被害：封じ込め措置を行った結果、その弊害で業務に不可欠な基幹システムまで遮断されてしまいました”



追加シナリオ

“法的措置の警告：被害を受けた顧客側の弁護士から、情報漏えいの経緯とセキュリティ対策の実態について、詳細な開示を求める書面が届きました”