JPCERT CC®

CSIRTマテリアル付録
インシデント対応演習プログラム

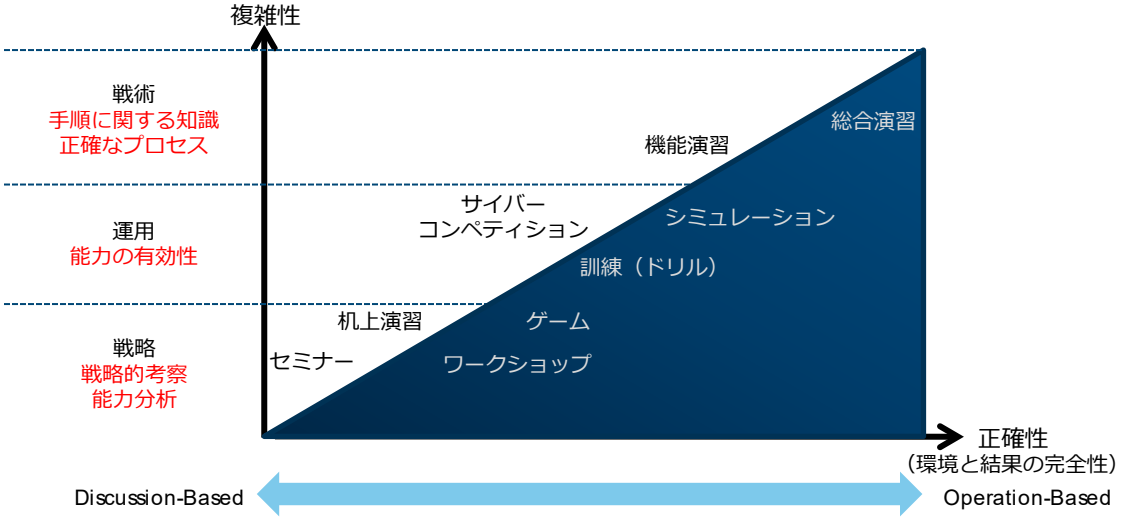
一般社団法人
JPCERTコーディネーションセンター

本資料の目的

- 組織のインシデント対応力向上、CSIRTの活動の認知と理解の促進の目的で利用するための演習プログラムの概要、方法論、実施例について紹介する

教育、訓練、演習

- さまざまな種類があり、目的やスコープに応じて使い分ける
  - 討論を中心としたもの：机上演習、セミナー、ワークショップ、ゲーム
  - オペレーション中心のもの：訓練（ドリル）、機能演習、総合演習
    - 複雑性（シナリオの詳細さ、正確さ）、および、正確性（環境やプレーヤーの対応を現実に近づける度合い）のレベルが異なる
    - 一般に、右上に行くほど実施のコストは大きくなる



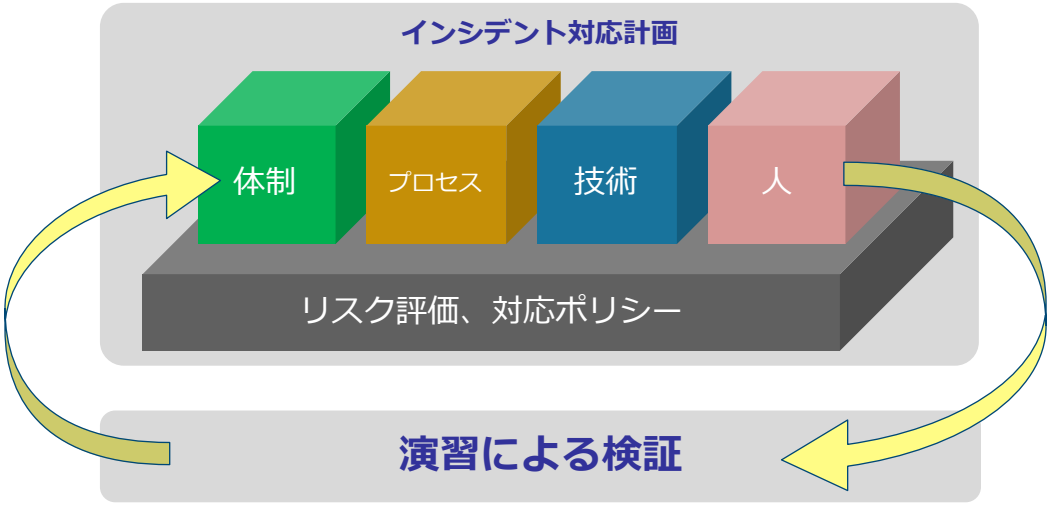
インシデント対応演習

- インシデントの発生とその対応を擬似的に再現する
- 演習の実施によって
  - 現在の対応能力を確認する
  - あるべき姿とのギャップを特定し、対策につなげる
  - 練度を向上し、対応時間を早め、適切で効果的な対応を可能にする
  - 参加者の相互理解を深め、連携を促進する

- CSIRTだけでなくインシデント対応に関与するさまざまな部署を参加させて行うことによって、組織全体としての対応能力を検証することができる
  - 組織にとっての最重要リスクは何か、守るべきものは特定されているか
  - インシデント対応の手順、体制、技術は、有効に機能するか
  - インシデント対応について、組織内の関係者間での共通理解があるか
  - 技術的、機能的に十分な対応能力を備えているか、常に活用できるよう準備が整っているか

組織の対応力の改善サイクルをまわす

- 演習によって検証することで、インシデント対応計画における課題を洗い出し改善につなげることができる
- さまざまなインシデントを想定したシナリオを用い、繰り返し実施することによって、計画を継続的に改善するとともに、計画を確実に遂行できるようにする



演習プログラムの策定と運用に利用可能なリソース

- 組織の演習プログラムの運用に関するフレームワーク
  - Homeland Security Exercise and Evaluation Program（HSEEP）
    https://www.fema.gov/hseep
  - ISO 22398:2013 - Societal security -- Guidelines for exercises
    JIS Q 22398:2014 社会セキュリティ－演習の指針

演習計画の策定、個別の演習の企画実施、評価と改善までの一連のプロセスについて説明している。HSEEPではそれぞれの作業フェーズで作成する文書の雛型も提供されている。

組織の対応力向上に演習を活用する

- CSIRT要員を対象とする演習
  - CSIRT内オペレーション、組織内外のステークホルダーとの連携の確認
  - インシデントハンドリング
  - テクニカルスキル
  - CSIRT要員の育成

- 組織内ステークホルダーを対象とする演習
  - インシデント発生時における、CSIRTとの連携を含む対応手順を確認する
  - 組織内の連携と情報共有
  - 危機管理、業務継続、顧客やメディアへの対応、法的対応
  - CSIRTの活動に関する理解の促進
  - サイバーインシデントに対する理解の促進

演習サンプル事例

サンプル事例

- ここで紹介する事例は、JPCERT/CCがいくつかの企業に対して実施した、サイバーインシデント発生時における組織の対応を検証するための机上演習の概要を紹介するものです。

サンプル事例：演習の目的とスコープ

- 演習の目的
  - インシデント発生時の組織の対応を検証する
    - いつ誰が何をするか
    - CSIRTを含む、組織内の関係部署がどのように連携するか
  - インシデントが組織にもたらすリスクの全体像についての理解を促進する
    - 特にCSIRTや情報システム部門以外の部門・部署に対して、情報資産や事業継続性に対するリスクと、リスク緩和における各部門・部署の責任を明確にする
- 演習のスコープ
  - 参加者：経営層やシニアマネージャーを含む、インシデント対応に関与するすべての部門が対象
    - ビジネスオペレーション、顧客対応、広報、法務リスク管理、情報システム、CSIRTなど
  - 形式：討論主体の机上演習
    - 2～3時間程度で実施
    - プレーヤーは数名～十数名程度が適当
  - シナリオ：サイバー攻撃活動による組織への侵害が疑われる状況への対応を検証

サンプル事例：演習の形式

- 討論主体の机上演習
  - インシデントが自組織で発生した時に観測される事象を時系列に分けて示す
    （例）
    - シーン1：インシデントの認知と初動対応
    - シーン2：悪化する状況への対応、業務影響の緩和と封じ込め
    - シーン3：インシデントの収束、再発防止と中長期的な対策
  - 各シーンにおける対応を参加者全員で議論する
    - 誰が、何を根拠にどのように判断し、何をするか
    - どのような対応ポリシー、規定、手順にもとづいて行動するか
    - 現在のポリシーや手順、体制は十分であるか
    - 足りない機能や手順、課題は何か

    など
  - 終了後のHot Wash（振り返り）で、演習中に明らかになった課題を再確認する
- 特長
  - 低コストで実施可能
  - シナリオに技術的な正確さや詳細さをそれほど必要としない
- チャレンジ
  - インシデント対応のさまざまな局面における意思決定が可能な、上級管理職を含むプレーヤーを組織横断的に集めること
  - それらのプレーヤーに対し中立的に振る舞うことができるファシリテータを用意すること

サンプル事例：参加者の役割

- ファシリテータ
  - 演習の進行役。演習のペースと流れをコントロールする
  - 演習の目的と基本ルールをプレーヤーに説明する
  - プレーヤーに状況を提示し、議論を促し、回答と解決策を引き出す（プレーヤーに対し回答や解決策を与えるのではない）
- プレーヤー
  - ファシリテータから示される状況に対し、プレーヤー全員で議論し対応を決定する
- 記録係
  - 演習およびHotwashにおけるプレーヤーの議論と対応を記録する
- 評価者
  - 演習を観察し、事前に定められた評価クライテリアに従いプレーヤーの対応を評価する
  - ファシリテータや記録係、場合によってはプレーヤー自身が評価者を兼ねてもよい
- オブザーバー
  - 演習を観察する
  - 演習進行における役割は持たない

サンプル事例：作業項目

① 演習の準備（２週間～1カ月）
- 目的、スコープ、実施内容、スケジュールについて社内の承認を得る
- 参加者のスケジュールを調整し実施日を決定する
- シナリオを作成しファシリテーションの準備をする
- 会場、設備を手配する

② 演習の実施
- ファシリテータの進行のもと演習を実施する

③ 評価と報告
- 演習の実施結果を収集し報告書を作成する（演習実施後　1～2週間以内）
- プレーヤーおよび他の関係者に向けた報告会を実施する、または報告書を回覧する

④ 改善
- 演習結果からインシデント対応計画における課題を特定し、改善点を洗い出す
- 演習の改善点を洗い出し、次回の演習企画に反映する

サンプル事例：作業項目 – ①演習の準備

- 目的、スコープ、実施内容、スケジュールについて社内の承認を得る
  - 上級管理職を含む幅広い部門からの参加者を集めるためには、経営層の承認とサポートによるトップダウンのアプローチが有効
- 参加者のスケジュールを調整し実施日を決定する
  - 演習の企画準備における最重要事項であり、おそらく最も困難なタスク
  - 重要なキーパーソン（演習の目的達成に欠かせない人物）の参加を確実に取り付ける
- シナリオを作成しファシリテーションの準備をする
  - 状況付与：プレーヤーに提示される状況の記述
  - 質問リスト：ファシリテータが議論の活性化のために使用する質問集
- 会場、設備を手配する
  - 会場：一般的な会議室。プレーヤー全員が 1 つのテーブルに着席するよう配置する
  - 設備：PCとプロジェクター（ファシリテータのスライド投影用）、ホワイトボード（プレーヤーの行動記録用）など

サンプル事例：作業項目 – ②演習の実施

- TimeTable（例）
  - ブリーフィング　15min
    - 演習の趣旨と目的、進行ルール、その他の手順について説明する
  - 演習　1.5h～2h
  - Hot Wash（振り返り）　30min～45min
  - デブリーフィング　30min
- ファシリテーション
  - 演習における議論はプレーヤーが主体となって行うものであり、ファシリテータは議論をガイドしてプレーヤーを演習の目的達成に導くためのサポートを行う。状況と論点を示し、必要に応じて議論を活性化するために質問を投げかける。議論の時間進行を管理し、限られた時間の中で重要な論点を網羅するようコントロールする。
- Hot Wash（振り返り）
  - 演習終了の直後に実施する。ファシリテータの司会で、以下のアジェンダで進行する
    - シナリオ解説
    - 議論の要点の確認
    - 演習中に十分に議論されなかった点の確認
    - プレーヤーの気付きや感想を共有する
- アンケート
  - プレーヤーはHot Washの後にアンケートを記入し提出する
- デブリーフィング
  - すべての予定を終了しプレーヤーが解散した後、ファシリテータ、記録係、評価者が集まり、それぞれの観察内容を収集する

サンプル事例：作業項目 – ③評価と報告

- 記録係と評価者のメモ、Hotwashや参加者アンケートでのプレーヤーのコメントを集め、次の点を整理する
  - インシデントを回避、防止、対応するためにどのような計画、ポリシー、手順を実行したか
  - 各部署の役割と責任は明確に定義されたか
  - 誰が決定権限を持ち、どのように決定が下されたか
  - 組織のリスクに関してどのような情報が集められ、どのように対処されたか
  - 組織内外のステークホルダーとの情報共有はどのようになされたか。どのような情報が共有されたか
  - 改善のための推奨事項は何か
  - 未解決またはフォローアップが必要な課題は何か、それらに対するアクションプランは何か
- これらの内容をもとに、次の点について分析する
  - 演習の目的は達成されたか
  - 各シーンの中での鍵となる判断は何か
  - 状況への対処に必要な活動やタスクを遂行する能力を備えていることが示されたか
  - インシデント対応の遂行を阻害する要素は特定されたか
  - 計画、ポリシー、手順は活動をサポートするものとなっているか。プレーヤーはそれらに精通しているか
  - 他組織との連携をサポートすることのできる合意や関係はあるか
  - 各シーンでどのような強みが確認されたか、どのような改善点が特定されたか
- これらの結果を踏まえ、以下の内容を含む報告書をまとめる
  - 演習の目的、シナリオ
  - 演習の中で見られたベストプラクティスと強み
  - 改善点と、それらを解決するための提言

サンプル事例：作業項目 – ④改善

- 演習結果からインシデント対応計画における課題を特定し、改善点を洗い出す
  - After-Action Meeting
    - 演習参加部署の意思決定者、評価者、演習計画チームが集まり開催する。演習を振り返り改善計画を精緻化する。
  - 改善計画
    - 修正措置を特定し、実施責任者を任命し、実施期限を設定する。演習参加組織の代表者によりAfter-Action Meetingの中で作成される。
- 演習の改善点を洗い出し、次回の演習企画に反映する
  - 上述の活動の中で演習の企画運営における課題と改善点を明確にし、組織の演習プログラムに反映させる

サンプル事例：シナリオ作成

- シナリオの作成
  - 状況付与（演習中にプレーヤーに開示される情報）
    - インシデントの認知から始まり、事態が進展するとともに現れる状況を、いくつかのシーンに分けて記述する
    - それぞれのシーンにおいて、議論すべき論点を設定する
      ※ プレーヤーに論点を提示することでスムースな進行の助けになるが、熟練したプレーヤーに対しては論点を開示せずに実施してもよい
  - 質問リスト（議論を促すためにファシリテータが使用する）
    - それぞれのシーンにおいて、議論の進行を助けるための質問リストを作成する
- シナリオ作成の注意点
  - 現実を反映したストーリー
    - 組織の事業環境、組織構造、提供／利用するサービスや保有するデータ等に根差したシナリオ
    - 現実に存在し得る脅威を想定する。荒唐無稽にならないように注意する
      - 技術的な妥当性
      - 脅威、攻撃活動、インシデント事例等の一般的な傾向
  - 観測可能な事実を記述する
    - インシデント報告、検知情報、ユーザーからの問い合わせ、分析結果、メディア報道、社内外のステークホルダーの反応、など
  - プレーヤーが理解しやすい記述を心掛ける
    - 解釈のブレが生じないよう明確に記述する
    - プレーヤーの前提知識レベルにあわせて用語や表現を調節する

サンプルシナリオ

サンプルシナリオ

- APTによる自組織に対する侵害への対応について、リーダーシップ、マネージメント、上級テクニカルスタッフとのディスカッションを行うことを想定したシナリオ。いくつかの状況を提示し、リスク（守るべき資産と情報についての理解、脅威の性質、システムや事業活動における脆弱性、重要なビジネスプロセスへのインパクト、などを含む）を評価し、組織が取りうる対応策についてディスカッションを行う。
- シナリオは以下の３つのシーンで構成される
  - シーン1：インシデントの認知と初動対応について議論する
  - シーン2：組織の危機管理、業務影響の緩和について議論する
  - シーン3：再発防止と中長期的な対策について議論する
- 想定するプレーヤー
  - 経営層やシニアマネージャーを含む、インシデント対応に関与するすべての部門が対象
    - ビジネスオペレーション、顧客対応、広報、法務リスク管理、情報システム、CSIRTなど
- このサンプルはシナリオの骨組みを提示するものであり、実際の演習に使用するためには、組織の実情にあわせて、シナリオ中に登場する業務、サービス、データ、人物などの記述を変更したり、追加の状況を加筆するなどした上で使用することを推奨する

サンプルシナリオ：Scene 1

プレーヤーへの状況付与

20yy年mm月dd日

警察から当社の代表窓口へ、次の内容の連絡があった。

「2日前、警察はあるサイバー犯罪捜査の一環でハードディスクとサーバーを押収した。それらを分析した結果、国内の複数の企業から窃取されたと思われる情報があり、その中に貴社とA社との間で交換されたと思われる情報を発見した。また、サーバーの通信ログに、貴社が管理するIPアドレスからの通信が6カ月前からあったことを示す記録があった。」

警察が示した「当社とA社との間で交換された情報」の内容は、1週間前に営業部門がA社と取り交わした文書と一致するものであった。

警察は当社に対し、捜査への協力を求めている。

主な論点

- インシデントの通知を受けた際の調整とコミュニケーション
- テクニカル／セキュリティスタッフの初動対応
- 侵害範囲を特定するためのアクション
- 攻撃活動の全体像についての検討
- 長期間にわたる侵害への対応
- 捜査機関との連携、捜査協力に伴う業務影響やリスクの検討

など

サンプルシナリオ：Scene 2

プレーヤーへの状況付与

20yy年mm月dd+5日

警察から通知された情報をもとに調査した結果、これまでに次の点が確認された。

- 社内ネットワークで、不審な通信を行うPCが複数確認された。
- それらのPCで、共通するマルウェアの活動の痕跡が確認された。セキュリティベンダーの情報によれば、同じマルウェアを使った活動が国内外で広く行われているとのこと。
- ファイルサーバーに、管理台帳にないユーザー名での継続的なアクセスが記録されていた。ファイルサーバーにはA社を含む多数の顧客企業に関する情報が格納されている。不審なユーザーアカウントはファイルサーバーの管理者権限が付与されサーバー内のすべての情報にアクセス可能であるが、実際にどのデータにアクセスしたかは特定できていない。

20yy年mm月dd+10日

あるニュースメディアの記者から広報部門へ次の内容の問い合わせがあった。

「貴社で発生したサイバー攻撃被害について教えて欲しい。」

主な論点

- 重要なシステムやデータへの侵害が確認されたときの対応
- 侵害範囲が特定できない状況での対応
- システムやネットワークを停止するか否か、業務影響を最小限に抑える方法
- 組織全体の緊急対応体制や危機管理体制を設置する判断と手順
- 顧客や他の外部ステークホルダーへの説明
- メディア対応ポリシー、社内の情報統制

など

サンプルシナリオ：Scene 3

プレーヤーへの状況付与

6カ月後のある日のこと

CSIRTの連絡窓口へJPCERT/CCから次の内容が通知された。
「各国の政府機関や企業を標的とした数多くのサイバー攻撃に関与していた大規模な攻撃者ネットワークが先日摘発された。JPCERT/CCではこの攻撃者ネットワークに関連する日本国内の感染ノードを調査している。分析によれば、貴社が管理するIPアドレスから攻撃者のC2サーバーへの通信が発生していた可能性がある。現時点で判っているC2サーバーのIPアドレスは次のとおりである。確認をお願いしたい。」

通信ログの調査の結果、JPCERT/CCから開示されたIPアドレスへの通信が、社内の複数のPCから発生していたことが確認された。それらの通信のうち最初のものは2カ月前に発生し、時間の経過とともに複数のPCで観測されている。

経営陣は、6カ月前のインシデントから続く一連の事象について企業全体の防御能力を改善するため、どうすれば最初の侵入とその後の拡大を防ぐことができたのか、そしてこのような攻撃によるリスクを緩和するための戦略やポリシーはどうあるべきかについて明らかにするよう指示した。

主な論点

- **未発見の感染端末の存在や再侵入を前提とした行動計画**
- **侵入、感染拡大、機密情報への不正アクセスについての再発防止策**
- **今後の新たな感染に備えた継続的な監視体制**
- **感染発生時の根絶プラン**

など

サンプルシナリオ：質問リストの例

- ファシリテータは、プレーヤーを各シーンの論点へ誘導し議論を促すために、質問リストをあらかじめ作成し必要に応じて使用する。以下はこのサンプルシナリオにおける質問リストの例である。
  - 提示された状況から、自社にどのような事態が起きていると考えられるか
  - 外部から侵害の可能性を指摘された場合、その情報は社内でどのように扱われるか
  - 顧客やビジネスパートナーとの間でのセキュリティインシデントに関する会話は、誰が窓口となり、誰が責任を持つか
  - 対応を進めるために足りない情報は何か、それはどのようにして入手するか
  - ビジネスへの影響を最小限に抑えるために、CSIRTは何をするべきか。他の部署は何をするべきか
  - 経営層へのエスカレーションは、誰がどのような判断基準で行うか
  - 被害当事者の顧客と、他の顧客に対するアクションは何か
  - メディア対応に備え、何を準備するか
  - 実施すべき対応は何か、実施すべきでない対応は何か
  - 全社的な危機管理体制を敷くタイミングを誰がどのように判断するか
  - 重要情報へのアクセスに対する防御手段はあるか
  - 重要情報への侵害が確認された場合の対応計画はあるか
  - インターネットの遮断や、重要なシステムの遮断は誰がどのような基準に基づいて判断するか
  - 停止したシステムやネットワークの復旧は誰がどのような基準に基づいて判断するか
  - 情報連携すべき社外のステークホルダーは誰か、誰の判断で、どのようなタイミングと手順で情報連携するか
  - 技術支援を求めるべき外部組織は誰か、どのような判断と手続きによって支援を要請するか
  - 被害または加害に関連する法的対応についてどのように考えるか
  - 経営陣をどのように説得し、対策強化への協力を引き出すか