NTT DATA
Trusted Global Innovator

注目されているセキュリティ事故・事件に関する情報 ＜2020年9月版 (第34号)＞(選り抜き版)

2020年9月25日
ＮＴＴデータ先端技術株式会社
セキュリティ事業本部

今回のサマリー

セキュリティインシデント対応訓練の効果的な実施方法
現状の組織力、対応力を確認・強化する目的で、セキュリティインシデントを想定した訓練が注目されています。本記事では、机上訓練の効果的な実施方法を中心に解説します。

セキュリティインシデント対応訓練の効果的な実施方法

1. はじめに

　現状の組織力、対応力を確認・強化する目的で、セキュリティインシデントを想定した**インシデント対応訓練**が注目されています。

　注目される背景の一つとして、内閣サイバーセキュリティセンター(NISC)が重要インフラ事業者向けに実施する**分野横断的演習**があります。参加者は年々増加しており、2019年には4,967名(717組織)が参加しました。(※1)
　分野横断的演習では机上訓練などの手法が採用されています。

　本記事では、CSIRTが自組織に実施する際に効果的な机上訓練方法を中心に解説します。

※1:2019年度分野横断的演習について https://www.nisc.go.jp/conference/cs/ciip/dai21/pdf/21shiryou03.pdf

2. インシデント対応に必要なCSIRTのミッションと必要な要素

CSIRTは、いつ発生するかわからないインシデントに備えるべく常に以下の要素の維持向上が必要です。

①ハンドリングに必要な手順やルールの整備

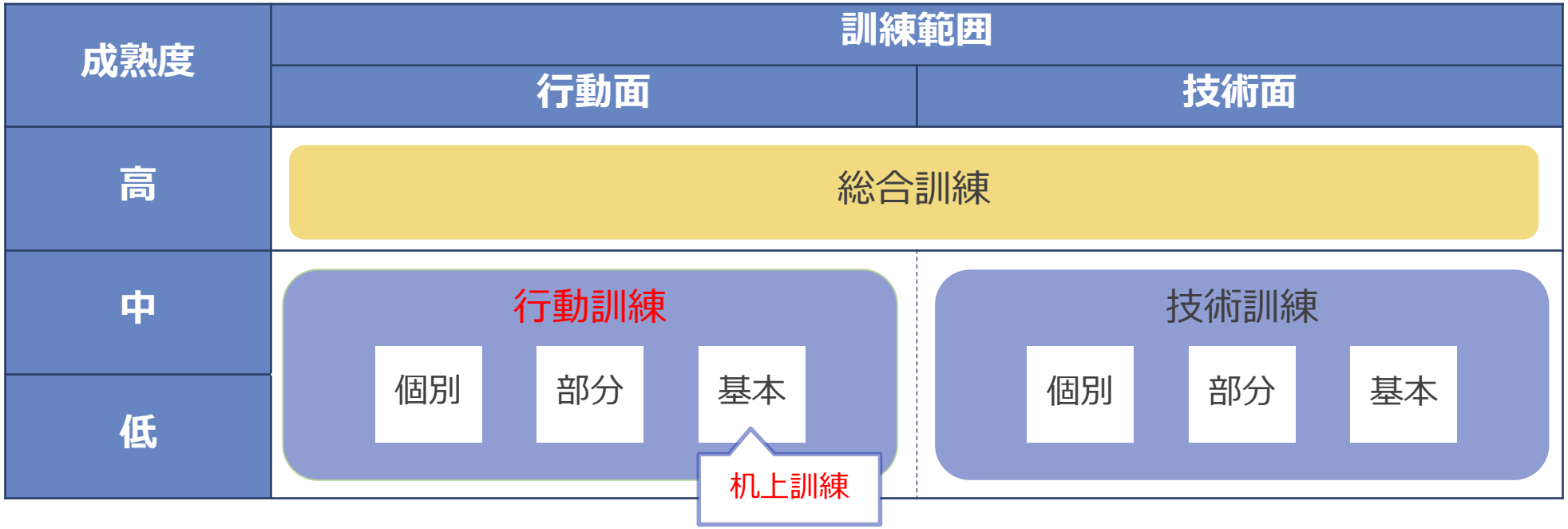
インシデント対応を迅速に行い、被害拡大を防ぐために、手順やルールの整備が必要になります。模擬的なインシデントを机上で想定して行う机上訓練が効果的です。
内閣サイバーセキュリティセンター(NISC)が実施している重要インフラ企業向けの**分野別横断的演習**は①に該当します。

②調査に必要な技術力

インシデントの原因調査にはログ分析や保全、フォレンジックなどの技術が必要になります。調査に必要な技術力の維持向上には、仮想環境を用意し、実際に技術的な対応を学習できるCyberRangeなどの技術訓練が効果的です。
国立研究開発法人情報通信研究機構(NICT)が実施している**CYDER**は②に該当します。

3. 目標・目的に合わせた訓練実施

インシデント対応訓練は目標・目的に合わせて訓練を実施する必要があります。「①ハンドリングに必要な手順やルールの整備」を維持向上するために効果的な訓練手法として**机上訓練**が広く採用されています。



次ページ以降では、インシデント対応訓練を実施するために必要な工程を解説します。

4. インシデント対応訓練に必要な工程

インシデント対応訓練の実施には、以下のような工程が必要となります。状況設定の複雑さ、実施規模により必要な期間は大きく変わります。

No	分類	内容	
1	体制構築	訓練事務局立ち上げ	・基本方針の確認する。
2	準備(方針)	目標、目的の設定 評価項目の設定 演習形式の設定 対象組織の決定	・訓練目標、目標、訓練タイプなど、訓練の基礎となる事項を決定する。
	準備(詳細)	シナリオ設計 参加者調整 会場確保	・訓練シナリオのインシデントの種類、状況付与ポイント、ディスカッションのイメージなど、シナリオの基礎となる事項を決定する。 ・シナリオ案、演習当日資料を作成する。
3	実施	参加者説明会 シナリオ解説	・訓練を実施する。
4	結果分析	評価内容分析 報告	・訓練結果の振り返りを行う。

5. 準備(方針)：強化したい項目に合わせた訓練の選択

インシデント対応訓練の種類を以下に示します。自組織で強化したい項目に合わせて訓練を選択します。

分類	概要	メリット	デメリット
総合訓練	行動訓練と技術訓練を掛け合わせたもので、最も実践に近い訓練である。	・実践に近い形でインシデント対応の行動面と技術面を評価できる。	・費用がかかる。 ・訓練期間中に広範囲に業務を中断したり、縮退する必要がある。
行動訓練	机上でインシデント対応をシミュレーションする。	・インシデント内容・対応をイメージし、インシデントの全体像を捉えることができる。 ・他の訓練と比較して準備が容易である。	・机上であるため、高度で複雑なインシデントでの訓練には限界がある。 ・リアリティに欠ける。
技術訓練	仮想環境を用意し、実際に技術的な対応を行う。攻撃チームと防御チームを用意し、実践的な訓練を行うことができる。	・実際に技術的な対応を行い、技術力を身につけることができる。	・難易度の高い訓練は、準備の観点から実施が困難になる。 ・大規模な訓練になるとインシデントの全体像の把握が難しくなる。

机上訓練は行動訓練に該当します。

6. 準備(方針)：成熟度を考慮した訓練方法の選択

次にCSIRT組織やメンバの成熟度を考慮して訓練方法を選択します。
以下に成熟度別に実施すべき訓練を示します。

分類	成熟度	種類	概要
総合訓練	高	総合訓練	インシデント対応における各部署の連携を習得する。実際のインシデントに近い状況を想定した実践的なインシデント対応を習得する。
行動訓練/技術訓練		基本訓練	CSIRTとしてのインシデント対応、自身の役割や各部署間での役割を明確にする。
		部分訓練	CSIRTメンバとしての基本的な行動スキル、対応方法などを習得する。 CSIRTメンバに限定して行うことが多い。
	低	個別訓練	インシデント対応の基礎であり、基本的な考え方など個人スキルを習得する。

多くの組織では、基本訓練として**机上訓練**が実施されてます。

7. 準備(方針)：目的・環境に合わせた訓練形式の選択

成熟度に合わせた訓練の決定後は**訓練の目的、環境に合わせて訓練形式を選択する**必要があります。以下に訓練形式の例を示します。

分類	種類(※2)	訓練形式(例)	概要
総合訓練	総合訓練	総合訓練	インシデント対応における各部署の連携を習得する。実際のインシデントに近い状況を想定した実践的なインシデント対応を習得する。
行動訓練	基本訓練	机上訓練	手順書の確認やルールの整備に効果的です。事前にインシデント対応手順書を用意する必要がある。
	部分訓練	ワークショップ型	手順書の作成や課題解決のために、ポイントを絞り議論を行う訓練である。
	部分訓練 個別訓練	ボードゲーム型	予め用意された訓練キットを活用します。各組織に合わせたものではなく汎用的シナリオが多いため、訓練の入門編になる。
	個別訓練	セミナー型	座学の訓練になる。個別訓練としてセミナー型を実施することで後続の訓練の理解度が深まる。

※2:成熟度別の訓練は参考であり、必ずしも記載の内容として分類されるわけではありません。

8. 準備(詳細)：シナリオ設計

　机上訓練では、手順書やルールによって定められているインシデント対応を検証のテーマとして設定します。選択したテーマに沿ったインシデント対応が発生するようにシナリオを設計します。複数のテーマを同時にシナリオに組み込むことも可能です。訓練に参加する組織や人も決定します。

分類		テーマ(例)
組織	連携	インシデント対応時の連絡ルートの確認
		インシデント対応時のCSIRTと他部署(広報、SOCなど)連携
	対応	脆弱性が確認された場合の対応
		マルウェア検知時の対応
		自社サイトが改ざんされた場合の対応
	報告	監督省庁などへの報告
		インシデントの対外公表
個人		CSIRTメンバとしての基本的な行動スキル、対応方法を習得
		インシデント対応中の自分の役割を理解

9. 準備：効果的な実施方法

机上訓練をより効果的に実施する方法の例を以下に示します。

準備(方針)

- CSIRT組織やメンバの成熟度に合わせた進め方
  成熟度が低いCSIRTの場合、矢継ぎ早にシナリオを提示して負荷をかけるような訓練を実施すると、理解も深まらないどころかインシデント対応に苦手意識を持ち逆効果になる可能性もあります。**シナリオをインシデント対応のフェーズごとに分けて作成することで状況把握が容易になり、議論が活発になる**などの効果が見込めます。事前にセキュリティに関する勉強会を実施することも有効です。

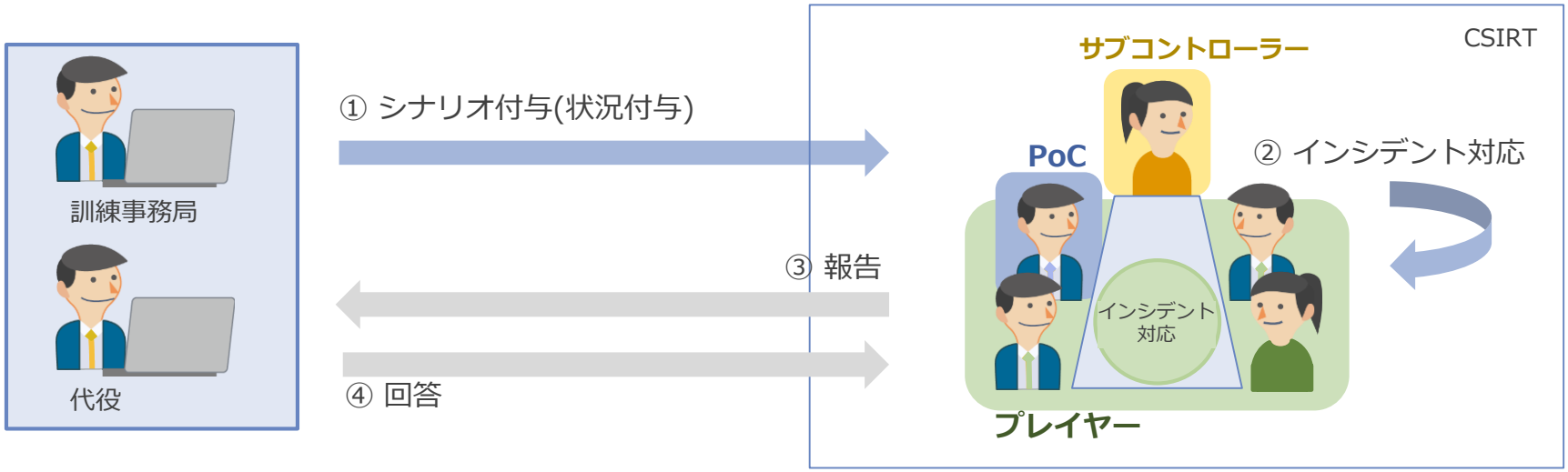
準備(詳細)

- 状況付与のポイント
  シナリオには、手順書の課題などを抽出するためのポイントを設定します。また、プレイヤーに**期待する行動を促すような状況付与**を意識するとよいです。成熟度の高いCSIRTには**期待する行動を妨げる状況付与**を行うと教育効果が見込めます。

- 参加する組織や人が多い場合
  状況付与がCSIRTなどのインシデント対応を主担当で行う組織に偏りがちとなります。そのため、他組織(広報、SOCなど)が主担当として対応を行うサブシナリオを作成する方法もあります。

10. 実施：机上訓練の流れ

机上訓練は以下のように実施します。



ステップ	主担当	詳細
① シナリオ付与(状況付与)	訓練事務局	事前に決められたタイミングでPoC、プレイヤーに状況付与を行う。
② インシデント対応	PoC(Point of contact) プレイヤー	①で付与されたシナリオに基づき、CSIRT内で対応方法を検討する。シナリオが付与するたびに繰り返す。**サブコントローラー**は原則ファシリテーターとして行動し、インシデント対応は行わない。
③報告	PoC(Point of contact)	**PoC**が監督省庁への報告や他のチームへの問い合わせに対する回答を行う。
④回答	代役	③の報告を受けてSOC/監督省庁/マスコミ役として回答を行う。 訓練参加者のインシデント対応に直接影響を与えない役に限る。

11. 実施・結果分析：効果的な実施方法

机上訓練をより効果的に実施する方法の例を以下に示します。

実施

- ファシリテートで意識すること

発言者に偏りがある場合には、個人の作業時間を確保するのも有効です。シナリオ付与された後に、まずは個人での検討時間を設けます。その後、一人ずつ検討結果を説明します。発言の偏りは改善されますが、単なる多数決にならないように注意する必要があります。

- 訓練の行動記録

事前に行動記録シートを用意しておくと、当日の記録がスムーズに行えます。シナリオ作成時に設定した手順書の課題などを抽出するためのポイントでの記録を忘れずに行う必要があります。

結果分析

- 振り返りで実施すること

可能であれば、訓練当日の振り返りをお勧めします。事前に設定した評価項目に対して、振り返りを行います。改善点だけでなく、評価点をフィードバックします。

- 抽出された課題に対して

「手順書やルールどおりに対応したが、不備があった点」を抽出します。抽出後は理由別にグルーピングし、原因分析します。手順書やルールの整備が必要な場合には、ワークショップ型の行動訓練を実施して意見を集めるのも有効です。

12. まとめ

本記事では、「インシデント対応訓練」の効果的な実施方法を解説しました。

机上訓練を実施することで、**個人・組織のインシデント対応における課題を可視化**できます。特に「効果的な実施方法」で解説したように**定めていた手順やフレームワークなどの課題などを抽出する**際に効果を発揮します。

訓練は、CSIRT組織やメンバの成熟度に合わせて計画することが重要です。まずはCSIRT内部でのミニマムスタートをお勧めします。成熟度が高まったら他部署と連携し訓練規模を拡大すると良いでしょう。繰り返すことで**組織の強靭化**に繋がります。

訓練準備や運営については自組織で内製する他に、最初はノウハウのある事業者が実施する外部のサービスを利用する方法も有効です。**良い訓練を実施するために成熟度の高いCSIRTリーダを訓練事務局にアサインすると、プレイヤーとして参加できないため、本来のインシデント対応とは異なるものになります。**こうした場合も外部のサービスを利用を検討すると良いでしょう。

13. 参考URL

- 2019年度分野横断的演習について
  https://www.nisc.go.jp/conference/cs/ciip/dai21/pdf/21shiryou03.pdf
- 実践的サイバー防御演習「CYDER」
  http://cyder.nict.go.jp/

NTT DATA

Trusted Global Innovator