

サイバー攻撃対処演習

【「防衛産業サイバーセキュリティ基準」で求められる事故等対処テストに適合する訓練】

情報セキュリティ事故等対処計画や事故発生時の対処体制を整備しているものの、実際に検証する機会がない又は計画の有効性に不安をお持ちのお客様へ

計画の有効性を検証、潜在的な弱点又は欠陥を発見!!

演習実施の必要性

事故等の発見及び検知時の報告・連絡要領

事故等の監視(システム監視を含む。)及び分析

事故等による被害及び影響の抑制並びに局限

事故等に係る証拠の保存及び原因の究明

事故等からの復旧(復旧に要する時間の目標を含む。)

情報セキュリティ事故等対処計画で規定する各段階の対処の有効性は演習の一連の対処活動の中で検証することが必要

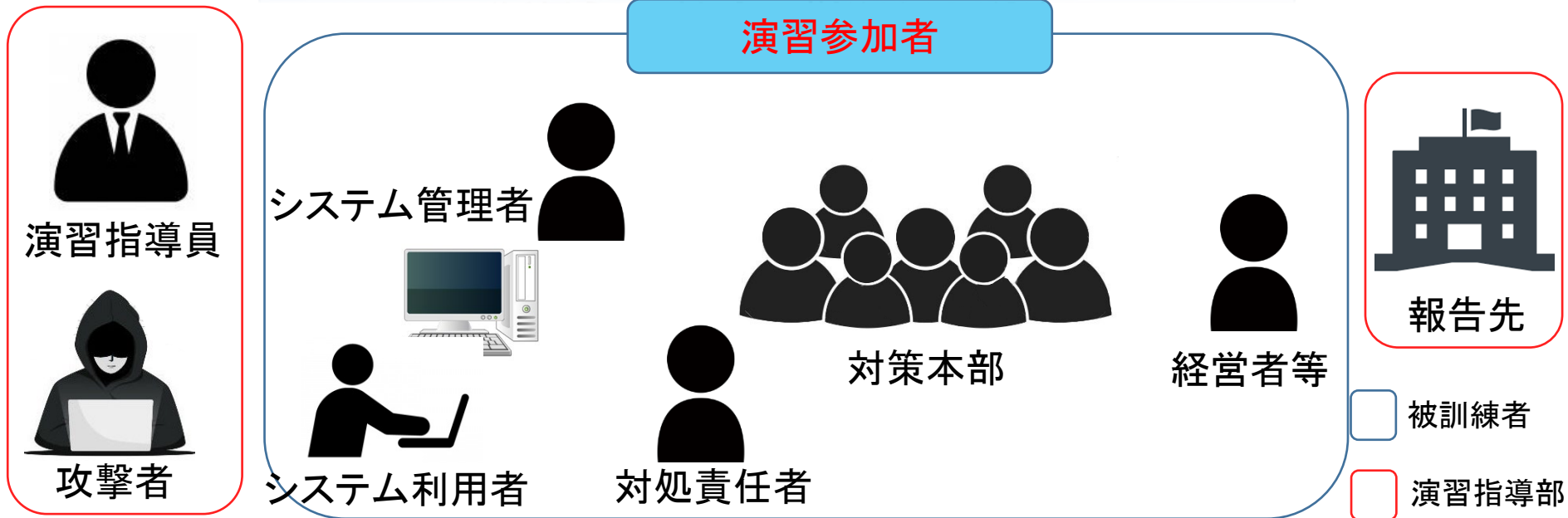
演習形式による関係者全員が参加するサイバー攻撃対処演習の実施

関係者全員が参加
(システム利用者～経営者等までの連携を深化)

サイバー攻撃の実体験
(ウイルス感染状況等を
実地に体験)

初度対処から意思決定までの一連の活動を演練
(各段階ごとの対応要領を実動で体験)

演習参加者等の構成及び効果



効果

○ 組織対応の有効性評価

組織で定めた対処手順が、実際に情報セキュリティ事故が発生した時に有効的に機能するかどうか(システム管理者の技術的対応能力だけでなく組織としての対応能力を含め)が検証できる。

○ 参加者の意識向上

関係者が実動演習に参加することにより、脅威の現状認識や各人の果たすべき役割を実地に演練することができ、対応手順の理解と意識向上が図れる。

○ 課題や改善点の抽出

実動により実地に活動することにより定めた対処手順の潜在的な弱点や欠陥を自らの検証及び第三者による評価を活用して発見・改善を図ることができる。

参加者の責任、対応

【演習指導員】

- ・演習統制
- ・評価実施

【攻撃者】

- ・実際のウイルスを使った攻撃の現示

【システム利用者】

- ・発見・報告
- ・現場保存

【システム管理者】

- ・状況確認、拡大防止
- ・原因究明(ログ解析)
- ・封じ込め、証拠保全
- ・復旧措置

【対処責任者】

- ・現場確認、初度対処
- ・経営陣等への報告
- ・関係者への通知
- ・システム管理者への通報

【経営者等】

- ・報告受け
- ・対応判断
- ・対策案承認

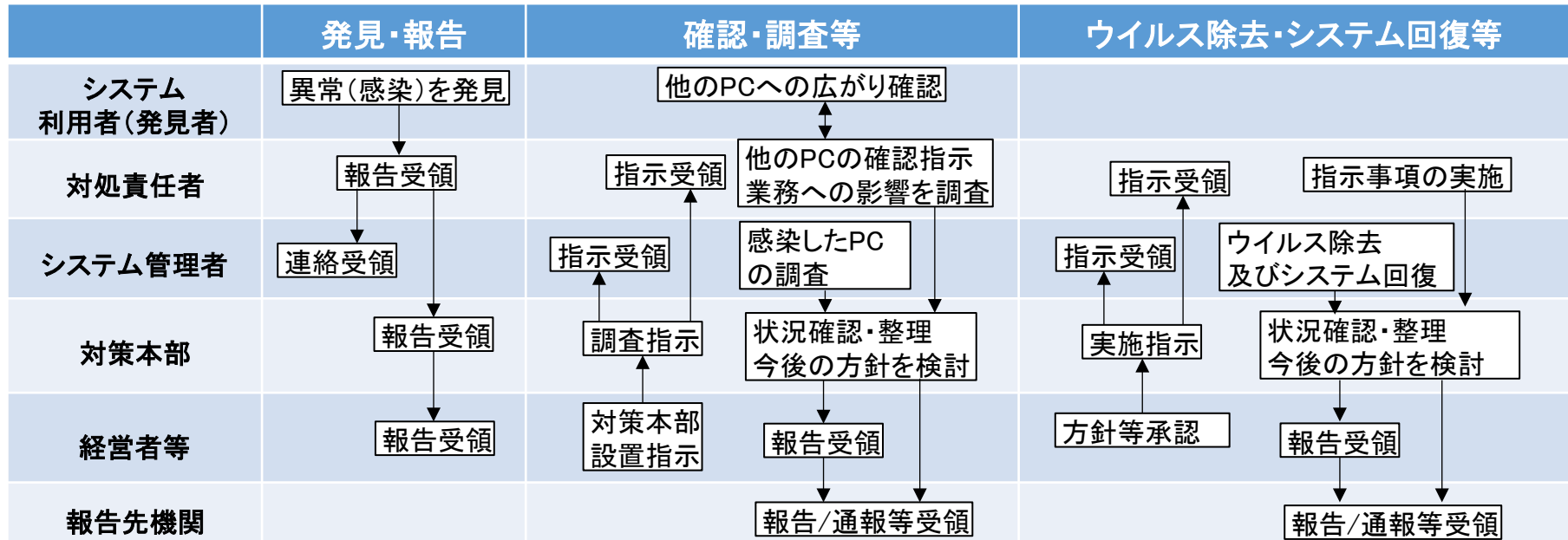
【対策本部】

- ・関係者の招集、対策本部設置
- ・状況の掌握・対応検討
- ・再発防止策、復旧案の検討
- ・報告・公表

【報告先機関】

- ・報告受け

対応の流れ



サイバー攻撃対処演習実施要領

- 演習は、演習指導員を現地に派遣し、演習受講側が準備した会場で実施します。
- 演習指導員は、3～4名を基準とします。
- 演習時間は、講評を含め3時間程度とします。
- 演習参加者の認識の共有化や手順の確認のため、事前の教育を希望される場合はお申し出下さい。
- 検証を効果的に実施するために情報セキュリティ事故等対処計画をお借りすることがあります。
- 演習時のウイルス感染等の現示は、リアルウイルスを使用するため演習実施側で準備したPCを演習会場に持ち込みます。
- 演習実施費は、基本料金を200万円(税抜き、旅費を除く)とし、実施規模に応じて加算する場合があります。