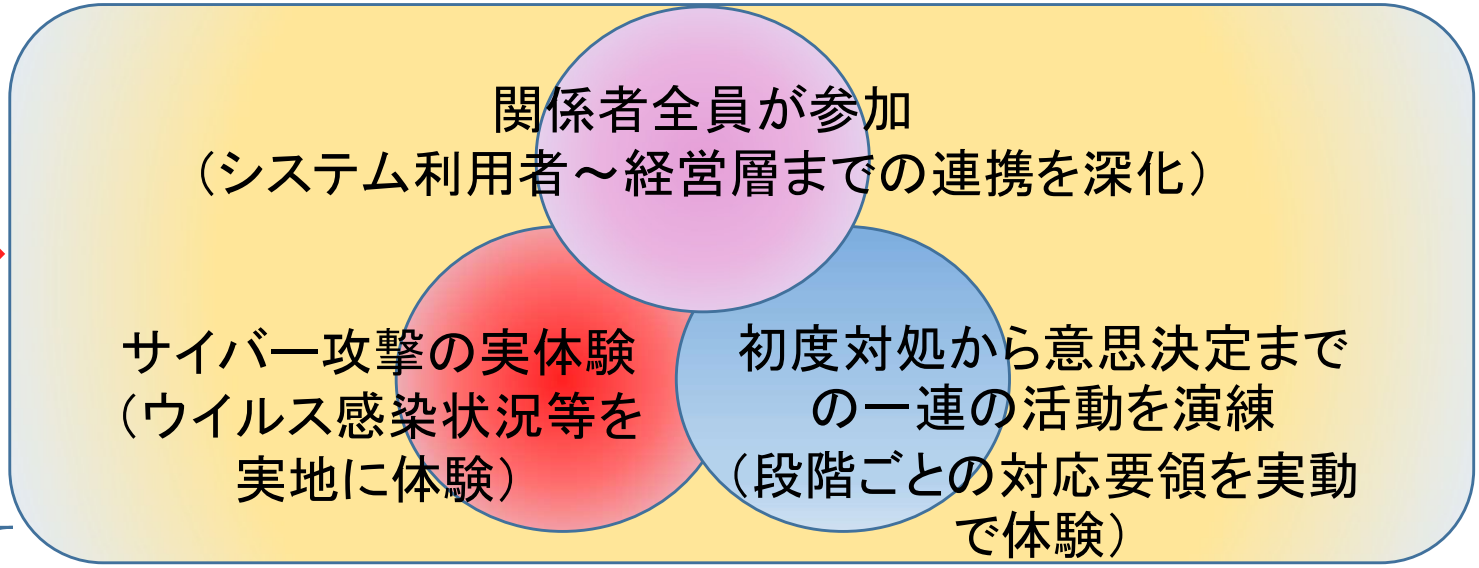
サイバー攻撃に対する組織的な対処演習
【情報インシデント発生時の対応訓練】

サイバー攻撃対処計画や事故発生時の処理体制を整備しているものの、実際に検証したことのない又は計画の有効性に不安をお持ちのお客様へ

座学教育の知識を実践に反映できるか確認！



演習実施の必要性

- 近年サイバー攻撃は、件数が増加、手口が多様化・巧妙化して誰でもが狙われる身近な脅威に
- IT依存度の高まりに伴いサイバー空間の重要性が増し、空間で発生する事象の影響が増大
- 巧妙かつ頻発するサイバー攻撃には、予防策だけでは対応しきれず、侵入に備えた対応が必須
- インシデント発生時の企業ダメージを防止するために、迅速かつ適切な対処が重要

今後発生が予想されるサイバー攻撃に備え実践的な対処能力を向上させることが必須

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訓練の実施

演習参加者等の構成及び効果

訓練指導員

攻撃者

演習参加者

システム管理者

システム利用者

対処責任者

対策本部

経営者

報告先

被訓練者

演習指導部

効　果

○　組織対応の有用性評価

　組織で定めた対応手順が、実際にインシデントが発生した時に十分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はなく組織としての対応能力を含め）を検証できる

○　参加者の意識向上

　関係者が実際の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出来、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

　実際に活動することで対応手順の見落としや不備を確認するとともに第三者による評価を活用して組織の対処力を総合的に向上させる

サイバー攻撃対処演習のイメージ

参加者の対応、役割

【演習指導員】
・演習統制
・評価実施

【攻撃者】
・疑似サイバー攻撃
・証拠の現示

【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

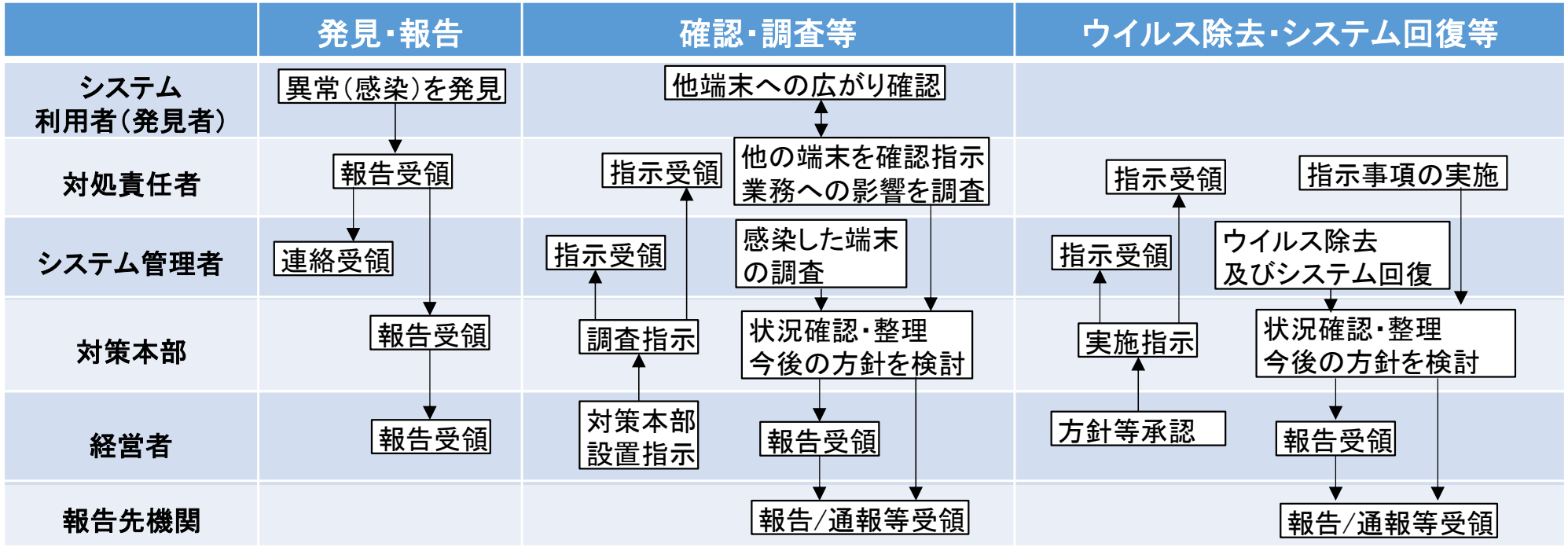
【対処責任者】
・現場確認、初度対処
・経営陣等への報告
・関係者への通知
・システム管理者への通報

【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

【経営陣】
・報告受け
・対応判断
・対策案承認

【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、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を会場に持ち込みます。
○　演習実施費は、基本料金を100万円（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。

連絡先

【担当部署】
（公財）防衛基盤整備協会
情報セキュリティ部　情報セキュリティ支援課

【担当者】
部長代理兼情報セキュリティ支援課長：小島
情報セキュリティ支援課員：加納、朝田

電話：03-3358-8704
Mail：infor-secu@bsk-z.or.jp