「特設実習(セキュリティ実践Ⅰ)及び特設実習(セキュリティ実践Ⅱ)」実践演習モジュール(SecCap I-04:社会科学系)

「インシデント対応と CSIRT 基礎演習」詳細

■日程: 9/8(木), 9/9(金), 9/12(月), 9/13(火)
■時間帯: 9:00～16:10
■担当: 種茂 文之（情報セキュリティ大学院大学 客員教授）他
■場所: 情報セキュリティ大学院大学 3F 303･304 教室

1. 演習のねらい

インシデント発生を前提として、問題発生時の迅速な対応と復旧を行い、被害を最小限に抑える CSIRT 活動が重要性を増している。本演習では、セキュリティインシデント対応の基本的なプロセスとして、計画の立案から対応、振り返りまでの一連の活動を解説と演習を通して習得する。また、CSIRT に求められる役割の一つであるインシデント対応教育を計画するための演習シナリオ策定についてデザイン思考の基本的な手法であるジャーニーマップを用いて検討する。

2. 演習計画

以下のテーマをもとに、講義と事例から課題解決をはかる演習を組み合わせた形式で行う。

1. **オリエンテーション**
   本演習の趣旨、進め方などを説明した後で、セキュリティ活動におけるセキュリティインシデント対応の位置づけおよび事故対応・管理の基本概念を解説する。
2. **セキュリティインシデント対応のフレームワーク**
   インシデント対応のフレームワーク（準備、検知・分析、封じ込め・復旧、改善・見直し）といった段階毎に要求される事項を解説する。
3. **演習(1) リスク評価とセキュリティ対策**
   リスク評価とセキュリティ対策の関係性、事前のセキュリティ対策と事後対応の関係性を考察する。
4. **演習(2) インシデントの影響と優先度評価**
   インシデントの事例から影響の大きさや緊急度判断と優先度評価について考察する。
5. **演習(3) インシデントハンドリングプロセスの理解**
   フレームワークをベースに平常時、非常時の対応について考察する。
6. **演習(4) インシデント対応の事例研究とコスト試算**
   セキュリティインシデント対応費用の費用項目と算出を試みる。
7. **演習(5) インシデント対応研修のデザイン**
   学習した内容をもとに、模擬的組織、環境をモデルとしたインシデント対応演習計画の立て方と効果測定を考察する。
8. **まとめ**
   講義および演習の結果を共有し、インシデント対応の基本的な概念の習得状況を確認する。

3. 教科書

適宜紹介する。

4. 参考書

適宜紹介する。

以上