「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・時間帯: 8/20(火), 8/21(水), 8/22(木), 8/23(金), 8/27(火), 8/29(木) :18:20～21:30
8/28(水) 学外演習: 13:00～17:50 (予定)
■担当教員: 星 智恵 (情報セキュリティ大学院大学 客員講師) 他
■場所: 情報セキュリティ大学院大学 2F 201 教室 ~~(火曜日は 3F 303 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のシナリオ策定についてデザイン思考の基本的な手法を用いて学習する。

2. 演習計画

以下のテーマをもとに、講義と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**
   組織内の様々な情報に対する価値を評価する手法とセキュリティ対策の種類を考察することで事前のセキュリティ対策と事後対応の位置づけを理解する。
4. **演習(2) インシデントの影響と優先度評価**
   様々なインシデント報告の事例から影響の大きさや緊急度を判断し、対応の優先度の評価を行う。
5. **演習(3) インシデントハンドリングプロセスの整備**
   インシデント発生時に、中心となり対応を行う組織として CSIRT（Computer Security Incident Response Team）や SOC (Security Operation Center)の役割像と業務概要を解説し、インシデント対応ポリシー、マニュアル例をもとに、インシデント対応のプロセスフローを作成し、作成プロセスの妥当性を評価する。
6. **演習(4) インシデント対応のロールプレイとコスト試算**
   インシデントの特徴からインシデント被害の大きさと対応コストの試算を行い、セキュリティインシデント対応費用の算出を行う。
7. **インシデント対応の実態**
   企業や国家へのサイバー攻撃の脅威と対策について、実際に企業でインシデント対応に携わる実務家の視点から講演をいただく。
8. **演習(5) インシデント対応研修のデザイン**
   これまで学習した内容を元に模擬的組織、環境をモデルとしたインシデント対応演習をデザインし、演習計画の立て方と効果測定を試みる。
9. **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。

■学外演習： 8/28(水) 富士通研究所(JR 南武線 武蔵中原駅前)
13:00～17:50(予定) ※詳細は演習初日にご連絡します。

3. 教科書

適宜紹介する。

4. 参考書

適宜紹介する。

以上