「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-02:技術系)

「デジタルフォレンジック演習」詳細

■日程: 9/14(土),15(日),21(土),22(日)
■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

インシデント発生後の対処に必要となるデジタルフォレンジック技術の基礎技術を修得することをねらいとする。まず、デジタルフォレンジックの基礎知識や技術、解析の考え方を解説するとともに、予備演習を通してファイル操作とその痕跡の関係を理解する。さらに、模擬的なインシデントを想定した解析演習を通して、インシデントの原因や影響範囲の解明までのプロセスを一通り経験する。

本演習の受講には、「情報セキュリティ技術演習Ⅰ」を受講していること、または同等の知識を有すること。特に、Windows のファイルシステム（NTFS）やレジストリに関する基礎知識を有することが望ましい。

2. 演習計画

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
(2) デジタルフォレンジックとは
(3) デジタルフォレンジックに必要な知識と作業の流れ
(4) 各種オープンソース解析ツールの使い方（Autopsy、Registry Decoder、等）
(5) 予備演習：Windows パソコン利用者が行った操作を知り、その痕跡を調査
- ファイルシステムのタイムスタンプ
- レジストリ
- イベントログ
- Web アクセス履歴
- USB デバイス接続履歴、等

(6) 解析演習：ある企業からの情報漏えいの原因、影響範囲等を解析
- 情報漏えい経路の解析
- 情報漏えいの原因となった不正アクセス等の解析
- 不正アクセスに伴う影響範囲の解析、等

(7) 検査結果報告書作成と発表
(8) まとめ

3. 教科書

特に指定しない

4. 参考書

演習実施時に指定

５．演習に必要な環境

- 演習環境は、本学利用のデータセンター内にある仮想環境を利用する。
  - 端末は各自で持参する。
  - 端末に VPN ソフトウェアその他をインストールして仮想環境にアクセスする。インストール等の手順は、後日配布する。また、必要があれば、オンラインで演習環境構築のサポートを行う。

以上