| | | | | |
|---|---|---|---|---|
| コース名 | 専門人材特化型コース | | | |
| 講座名 | 社会人向けサイバーセキュリティ人材育成講座(九州大学SECKUN)（共同事業） | | | |
| 科目名 | フォレンジック演習 | | | |
| 必修・選択 | ― | 単位 | ― | |
| 概要・目的 | 前半のデジタルフォレンジックの概要と証拠保全およびデジタルフォレンジック解析基礎演習パートではサイバーインシデントや不正調査、犯罪捜査等で活用されるデジタルフォレンジックの基礎を習得する。あらゆる事象にデジタル機器が関係する社会において、過去に発生した事象を把握するためには、デジタルフォレンジックの活用が欠かせない状況である。<br>講義では、デジタルフォレンジックの概要を学び、デジタルフォレンジックがどのようなプロセスで実施され、どのようにデジタル証拠を保全するのかを習得する。演習では、架空のインシデントで被害を受けた端末のディスクイメージから、侵害の原因や攻撃者活動の特定に有用ないくつかの証跡（レジストリ、ファイルシステム情報、イベントログ等）について、その分析方法を学び、実際に分析する。<br><br>後半の動的マルウェア解析パートでは、マルウェア感染によるインシデント発生時において、マルウェアがシステム上でどのように動作し、どのような痕跡を残し、最終的にどのような被害をもたらすのかを迅速かつ正確に調査・分析できる基礎的な動的解析技術を習得する。 | | | |
| 到達目標 | まず、デジタルフォレンジックの概要を理解する。サンプルの証拠の分析を通じて、デジタルフォレンジック調査の一端を経験する。<br>次に、実際のインシデント対応において、マルウェアの挙動を理解し、適切な封じ込め、駆除、復旧策を立案・実施するための実践的な知識とスキルを身につけることを目指す。 | | | |
| 授業方法 | 講義 | 実施形態 | 対面＋遠隔同期 | |
| 評価方法 | 演習の進捗状況により総合的に評価する。 | | | 開講日 |
| 授業項目 1 | デジタルフォレンジックの概要と証拠保全　（杉山/赤松） | | | 12/13 |
| 授業項目 2 | デジタルフォレンジック解析基礎演習①　（杉山/赤松） | | | |
| 授業項目 3 | デジタルフォレンジック解析基礎演習②　（杉山/赤松） | | | |
| 授業項目 4 | デジタルフォレンジック解析基礎演習③　（杉山/赤松） | | | |
| 授業項目 5 | 動的マルウェア解析1（折田） | | | 12/20 |
| 授業項目 6 | 動的マルウェア解析2（折田） | | | |
| 授業項目 7 | 動的マルウェア解析3（折田） | | | |
| 授業項目 8 | | | | |
| 授業項目 9 | | | | |
| 授業項目 10 | | | | |
| 授業項目 11 | | | | |
| 授業項目 12 | | | | |
| 授業項目 13 | | | | |
| 授業項目 14 | | | | |
| 授業項目 15 | | | | |
| 使用教材 | [授業項目5～7]<br>スライド、解析用仮想環境、マルウェア検体、解析ソフトウェア | | | |
| 特記事項 | [授業項目1～4]<br>解析基礎演習で取り扱う内容（現時点での想定であり、一部変更の可能性があります。）<br>1. フォレンジックイメージの取り扱い方法<br>2.ウェブアクセス履歴の分析<br>3.ファイルシステムに関する証跡の分析<br>4.プログラムの実行痕跡の分析<br>5.イベントログの分析<br>6.データ窃取に係る痕跡の分析<br>7.その他（Windows端末以外のフォレンジック概要等説明）<br>※当日受講不可の場合、録画した講義動画視聴による後日の受講可能。<br><br>[授業項目5～7]<br>講座内で使用するマルウェア検体の実行と解析を行うため、Windows の仮想マシン環境を各自でご準備ください。準備方法については、別途手順をご連絡します。 | | | |