岡山大学公開講座

セキュリティ演習講座

本講座では、組織のネットワーク環境を模した演習環境（サイバーレンジ）を利用し、仮想環境で模擬的に発生させたサイバー攻撃を体験することで、インシデントレスポンスの知識やスキルを学びます。実機を用いたハンズオンを中心とした演習により、業務に活かせる実践的な講座となっています。

定員各回 5名

講座の学習目標

攻撃者の立場で疑似マルウェアや攻撃ツールを操作する体験や、防御側の立場でログから侵害の痕跡を分析する体験を通じて、実践で活かせるインシデント対応の知識やスキルが身につきます。

POINT 01
サイバー攻撃が発生した際のインシデントレスポンスの流れを理解する。

POINT 02
インシデントレスポンスにおける技術的な調査や分析を体験する。

POINT 03
攻守の両方の視点から、セキュリティ上の問題点や対策を考えるスキルを磨く。

参加対象者

下記の条件をすべて満たす方

- ✓ 岡山県内に本社又は製造事業所がある企業（自営を含む）に勤務する方
- ✓ セキュリティ関連の実務を担当する方
- ✓ 基本的なセキュリティやネットワーク関連の知識を有する方（基本情報処理技術者レベル）

本講座は、ログ解析やフォレンジクスの内容が含まれますので、コンピュータとネットワークに関する基礎知識をお持ちの方のご参加を想定しています。

第1回	2024 12/19（木） 13:00 – 18:00
第2回	2024 12/20（金） 13:00 – 18:00
会場	岡山大学 グリーンイノベーションセンター（津島キャンパス）
持ち物	無線 LAN に接続可能なパソコン
受講料	100,000円 (税込) / 人

申込

＜申込方法＞
岡山大学公開講座 URL より、お申込みください。
https://www.okayama-u.ac.jp/tp/society/koukaikouza.html

＜申込期間＞
11/19（火） ～ 12/3（火）

備考

- 第1回、第2回ともにプログラムの内容は同じです。ご都合の良い日をお選びください。
- 岡山県内以外の方も応募可能ですが、定員を超えた場合は岡山県内の方が優先されます。
- 領収書の発行は可能です（申込み時に通信欄でご依頼ください。但し請求書の発行は対応しておりません）

問い合わせ
岡山大学
自然系研究科等総務課総務グループ
TEL 086-251-8005
E-MAIL kikaku@adm.okayama-u.ac.jp

実践で活かせるスキルを身に着ける

サイバー演習では、机上での演習と比較した場合に、端末を実際に操作してハンズオンを取り入れることで、高い学習効果が実現できます。サイバー攻撃やインシデントレスポンスの理解、技術的なスキルの向上に関しても、実機を用いたサイバー演習は不可欠です。本講座では、組織のネットワーク環境を模した演習環境（サイバーレンジ）を利用します。仮想環境で模擬的に発生させたサイバー攻撃を体験することで、実践で活かせるインシデントレスポンスの知識やスキルが身につきます。

講座の内容

講義

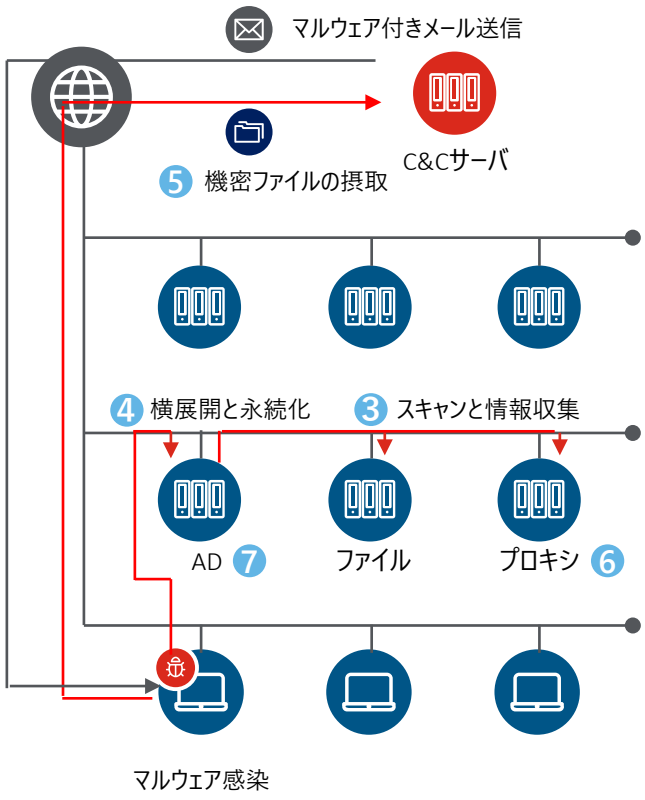
1. 代表的なサイバー攻撃の概要と標的型攻撃における攻撃者の戦略・戦術、攻撃で使用されるツールやサービスを学ぶ。
2. インシデントレスポンスの全体の流れと各フェーズにおけるポイント、早期復旧するためのTIPSを学ぶ。

攻撃側ハンズオン

3. スキャンを実行し、侵入先の情報を収集する。ホストに対してポートスキャンを行いサービスやOSの情報を収集する。
4. 脆弱性を悪用した攻撃により、ADへの横展開と権限昇格をする。
5. バックドアを作成し、侵害を永続化する。環境内の認証情報や機密ファイルを窃取する。

防御側ハンズオン

6. プロキシログをSIEMで分析し、攻撃者に悪用された端末や被害が発生した日時を特定する。
7. SIEMでWindowsイベントログを調査し、攻撃者が端末上で実行した操作を調査・分析する。
8. フレームワークを用いて発生したセキュリティインシデントを分析する。



01 組織のネットワーク環境を模した演習環境を利用

攻撃者の立場で疑似マルウェアや攻撃ツールを操作する体験や、業者の立場でログから侵害の痕跡を分析する体験を通じて、実践で活かせるインシデント対応の知識やスキルが身につきます。

02 経験豊富な講師・チューターのサポート

セミナーでは複数のチューターが皆様の演習をサポートします。質問や分からないことは適宜確認しながら進めることもできます。

03 短期集中型の集合演習

短期集中型の演習により、セキュリティインシデントに迅速・適切に対応できるテクニカルなスキル、およびノンテクニカルスキルも学びます。