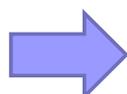


セキュリティインシデント分析コース の概要

公益社団法人 私立大学情報教育協会

本コースの概要

- 1. 標的型サイバー攻撃
標的型メールを用いたサイバー攻撃の実態や仕組みを確認する
- 2. サイバー攻撃のインシデント対応
サイバー攻撃の痕跡調査と対応について理解する
- 3. サイバー攻撃への対策
事前対策を理解し、自校の現状と比較する



総合演習(24日午後)に向けた技術的知識の習得

公益社団法人 私立大学情報教育協会

本コースのプログラム

A-1 標的型メールによるサイバー攻撃

A-2 痕跡調査のための事前対策

＜昼食＞

A-3 サイバー攻撃の痕跡調査

A-4 サイバー攻撃への対策

A-1 標的型メールによるサイバー攻撃

- 標的型攻撃メールの中身とマルウェア感染の影響
 - 「どこで」「どうやって」感染するのか？
 - 感染すると何が起きるのか？
- サイバー攻撃の実例（ストーリー）
 - 内部調査→感染拡大→目的達成



マルウェアに感染したときの影響をいち早く想像できる

A-2 痕跡調査のための事前対策

- PCでやるべき監視強化のポイント
 - マルウェア感染の事実や、アクセスされたファイルを特定するために、事前にPCで行うべき監視強化とは？
- イベントログの調べ方



PCの監視を強化し、サイバー攻撃を受けた時の痕跡調査に備えることができる。

A-3 サイバー攻撃の痕跡調査

- 感染拡大の手法
 - 攻撃者が、目的とする情報を入手するまでのストーリー
- 痕跡調査演習
 - イベントログによる攻撃ツールの痕跡調査



サイバー攻撃の痕跡を調査し、その結果をインシデント報告書として作成できる。

A-4 サイバー攻撃への対策

- サイバー攻撃への事前対策
 - 多層防御
- 法律と実施すべき対策
 - 個人情報保護法、GDPR、etc.



サイバー攻撃への一般的な事前対策を理解し、
自校におけるサイバー攻撃対策の改善点を提案できる。