A-1.
テクニカルコースの概要

文京学院大学
浜　正樹

実習概要

- 1．標的型サイバー攻撃などが疑われる場合の診断と初動対応の演習
  - 疑わしい「メールの添付ファイル」の開封や「リンク先」の接続を想定し、仮想環境などを用いて診断して、安全確認する方法を演習
- 2．インシデント発生時の対応フローチャートに基づく演習
  - 標的型サイバー攻撃の疑いが強い場合を想定して、インシデント対応フローチャートに基づく緊急遮断の判断、システムのログ解析、被害の全容把握、関係者への報告書作成などを演習

プログラム

- A-1　イントロダクション
- A-2　標的型攻撃などが疑われる場合の診断と初動対応の演習
- A-3　インシデント発生時の対応フローチャートに基づく演習
  - A-3-1 「内部侵入・調査」実習
  - A-3-2 「インシデント被害予想」演習

環境

- 私立「SJK 大学」
- 学生数4000人・教職員数400人
- 年金機構や大学からの情報流出事件が相次ぎ、情報センターも学内への啓蒙（情報共有）に注力している
- また、大学ガバナンス側も、セキュリティ運用体制の整備を行って、学内外の情報共有にも積極的に参加しようという機運が高まっている

実習のロールの違い

	ロール	環境	目的
A-2	情セ スタッフ	エンド ユーザー 端末	マルウェア 検知
A-3-1	攻撃者	侵入した 端末	内部侵入・ 調査
A-3-2	情セ スタッフ	SJK大学	被害予想

A-2　標的型攻撃などが疑われる場合の診断と初動対応の演習

A-2 の概要

1. 標的型攻撃の定義
2. 標的型攻撃に使われるメールの事例
3. 標的型攻撃への対策
4. 【実習】怪しいメールを受け取ったら

A-3　インシデント発生時の対応フローチャートに基づく演習

A-3 の概要

A-3-1

1. 攻撃者側が内部侵入に使う手法を学ぶ
2. 【実習】攻撃者側の侵入プロセスを体験

A-3-2

1. SJK大学のネットワーク・システム構成の把握
2. 【実習】SJK大学にマルウェアが感染・拡散した場合の被害予想

A-3-2 実習の概要

インシデント対応フローチャートに沿った対応

1. 外部からの指摘＆マルウェアの検出
2. 既に感染しているPCは無いかどうか、確認
3. ネットワーク・システムの把握
4. 被害範囲の予想
5. 報告・連絡・協議
6. 感染拡大防止・緊急対応
7. 警察への連絡・セキュリティベンダーへの依頼

各セッションの成果物

- A-2 マルウェア挙動調査報告書
  - マルウェアの検出や通信状況などの調査結果の報告
- A-3-2 被害範囲予想報告書
  - SJK大学のネットワークにマルウェアが拡散した場合に予想される脅威の報告