# A-1.
# セキュリティインシデント分析コースの概要

明治大学
服部　裕之





## 本コースの概要

- 1．マルウェアを用いたサイバー攻撃

  マルウェアを用いたサイバー攻撃の実態や仕組みを確認する
  - ランサムウェアによる攻撃
  - 標的型サイバー攻撃

- 2．サイバー攻撃のインシデントレスポンス

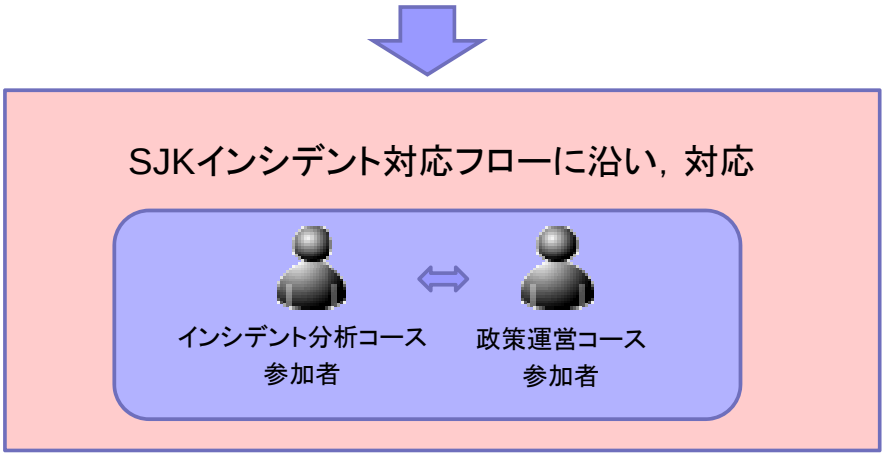
  不正通信や情報流出の痕跡調査について理解する

→ 総合演習1（25日）に向けた技術的知識の習得

# 総合演習1　インシデント対応模擬体験

想定：　SJK大学の教員のPCがランサムウェアに感染

教員のPCがランサムウェアに感染しファイルが暗号化され、
この情報（相談）が情報センターに届いた。








# 本コースのプログラム

A-1　セキュリティインシデント分析コースの概要
A-2　マルウェアの脅威と事例
A-3　ランサムウェアへの感染と対策
　　＜休憩＞
A-4　標的型サイバー攻撃
　　＜休憩＞
A-5　サイバー攻撃に対する調査と対応

# A-2　マルウェアの脅威と事例

- マルウェアの分類と動作
  - マルウェアのタイプや振る舞いの違い
- サイバー攻撃の実例

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-3　ランサムウェアへの感染と対策

- ランサムウェアの感染実習
  - 被害の範囲
- 事後対応
- 事前対策

ランサムウェアに感染したときの被害状況の把握、事後対応が行え、さらに、事前対策を講じることができる

# A-4　標的型サイバー攻撃

- 標的型サイバー攻撃の流れ
  - 攻撃者が、目的とする情報を入手するまでの手順
- 標的型サイバー攻撃で用いるマルウェア及び各種侵入拡大ツールの動作検証

標的型サイバー攻撃を受けた時の被害や
影響範囲について、的確な想定ができる





# A-5　サイバー攻撃に対する調査と対応

- 状況の把握と痕跡調査
  - プロセス、通信、ログ
- 証拠保全
  - 外部機関との連携

サイバー攻撃を受けた時に、状況の把握や痕跡調査の
一次対応ができる