デジタル・フォレンジックのカリキュラム

立命館大学
情報理工学部
上原哲太郎

RITSUMEIKAN

大学でセキュリティやフォレンジックを教える難しさ

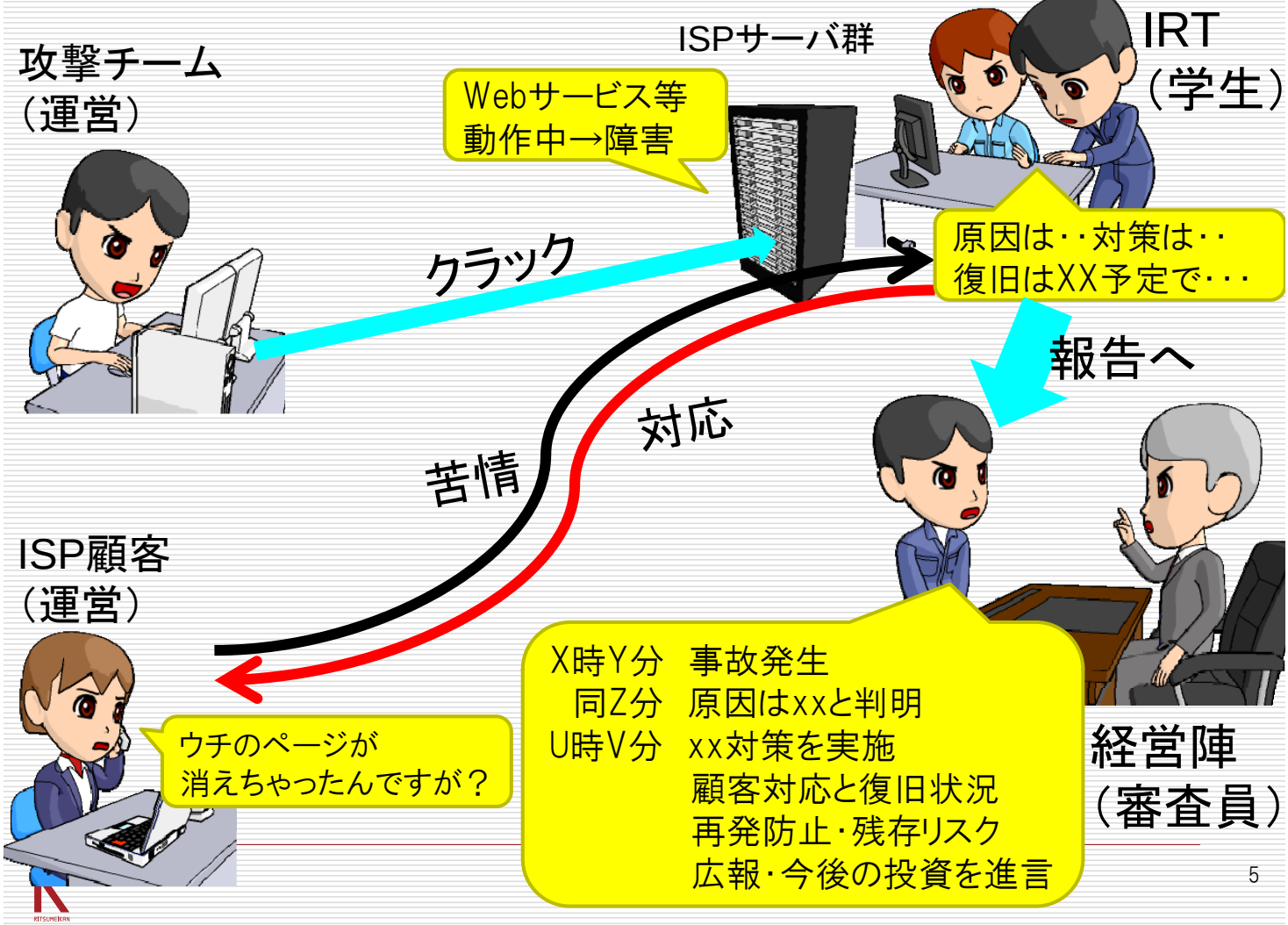
- 大学のミッションは「将来も変わらない基礎技術」
- しかしセキュリティ問題は多くが現在進行形
  - 特にシステムセキュリティ
- フォレンジックは具体的製品や規格に特化した話が多い
  - 例えば削除ファイル復活法はファイルシステム固有
  - レジストリやキャッシュファイルはWindows固有
- 学生は「実システム」を学ぶ機会に乏しい
  - 大学教員側が意外と価値を見いだしていない
    （大学は職業訓練の場ではないという意識が強い）

いきなり実践をさせて自学自習を誘う

大学対抗情報危機管理コンテストとは

- サイバー犯罪に関する白浜シンポジウム
  第10回記念として2006年に開始
- 3～4名のチームを学生で編成
  サーバ管理を委託されたという想定で
  発生するインシデントへの対応力を競う
  - 評価はIRTから提出された報告書をベースとする
- 現在はネットワークでの2段階予選を経て本選
  - 第1次予選は課題に対するレポートを評価
    - 昨年は「オンラインゲーム会社からの依頼」へのコンサル
  - 第2次予選はネットワーク越しに本選と同じ形式
  - 本選は白浜シンポジウムと同会場で実施

情報危機管理コンテスト本選の様子



情報危機管理コンテストの展開

- 教材化へ
  - 先導的ITスペシャリスト育成推進プログラム
    IT－Keysへの応用
  - 現在はenPIT SecurityのSecCapで演習へ
- ただし運営は（教材となる事故シナリオ含め）
  ノウハウの塊であり、外部移転が困難
  - 結果として白浜シンポジウムのスタッフが
    そのまま演習を提供する形になっている

カリキュラムに演習を入れる利点と欠点

- フォレンジックの現場は結局ノウハウの塊
  - 実応用の経験を積み重ねた者が
    一般化に至ることができれば教育として成功だが
    そのためには最低限の知識が必要→座学との連携
- 一種のゲーミフィケーションとなる
- 基礎が疎かとならない配慮が必要
  - 基礎知識があれば知らない事例でも対応可能
- なにより演習実施側の負担が大変！！
  - シナリオ作成から予行演習まで綿密な準備
  - 演習実施では臨機応変さも求められる（特に難度）