【令和3年度教育改革推進事業経費】　b.教育課程改善・試行プロジェクト

情報セキュリティ教育コンテンツの整備

和歌山大学 学術情報センター

川橋　裕，風間　一洋，
内尾　文隆，藤本　章宏

リカレント・（情報）リテラシ演習

- 新しい演習形式・演習方法の開発
  - 社会人向け、情報セキュリティ入門
  - 演習と座学の相互で理解を深める
- 情報セキュリティに関する新たな試み
  - インシデントを起こす・修復することで学ぶ
  - なぜインシデントが起こるか、で対策を実践する
- 例：標的型メールによる攻撃など
  - 標的型メールの作成・送信・受信
  - 標的型メールの解析による見分け方
- 当該環境を容易に構築し運営する必要がある

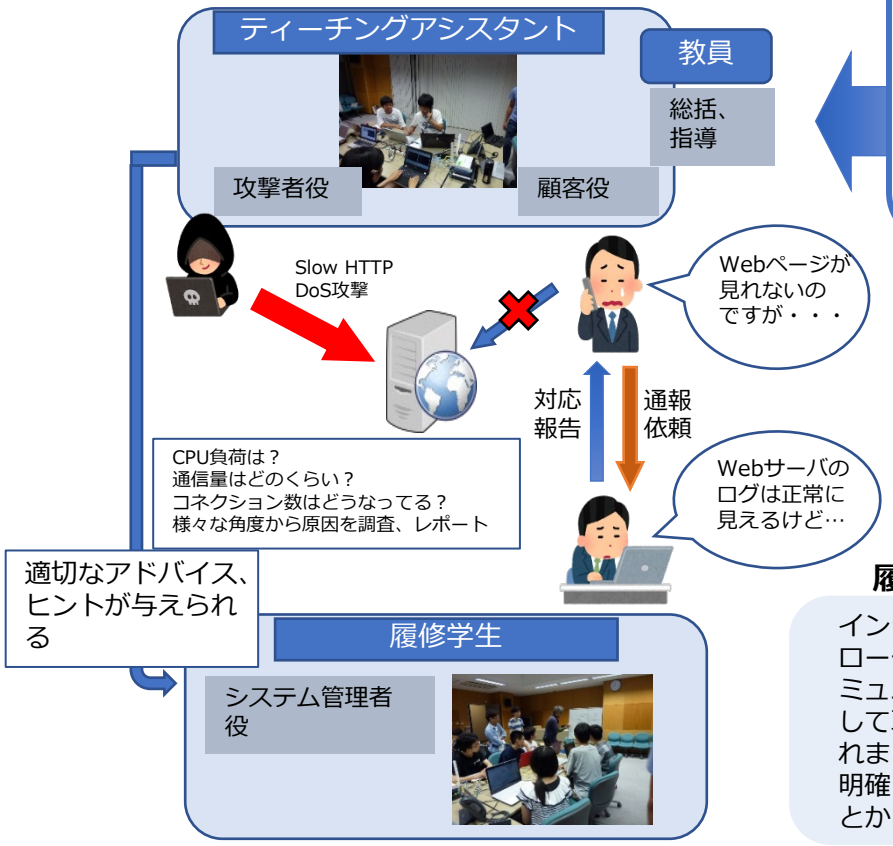
PBL演習授業「インシデントレスポンス演習」

Basic SecCap × 国立大学法人 和歌山大学

毎年白浜で開催されている「情報危機管理コンテスト」で実施したシナリオを実際に体験できます。

ネットワークおよびサーバで発生するトラブルの事例と環境をもとに、なぜトラブルが発生するのか、その発生原因は何か、あわせてその仕組みについてを理解します。
セキュリティ事案はその延長にあり、発生原因の切り分けと封じ込め、および解析方法について学びます。

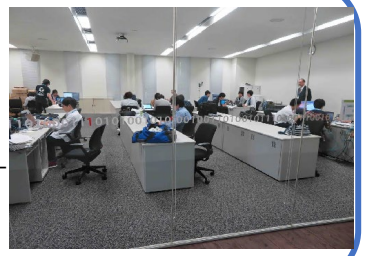
演習の内容



「情報危機管理コンテスト」で実施したシナリオ、環境構築のノウハウをこの演習に還元します。

コンテスト運営スタッフとして参画した学生が本演習のティーチングアシスタント（指導補助スタッフ）として参画し再び活躍します

➡運営側、受講生側双方の人材育成に貢献



1日目	2日目	3日目	4日目
・演習環境構築 ・Linux演習 ・インシデント対応（不審ファイル） ・インシデント対応（Webの遅延）	・演習環境構築 ・インシデント対応（リダイレクト） ・インシデント対応（Web改ざん）	・演習環境構築 ・インシデント対応（DoS攻撃） ・インシデント対応（Webの遅延 2）	・演習環境構築 ・インシデント対応（DoS攻撃の復習） ・インシデント対応（NW不通） ・振り返り

履修者の声

インシデントを対処する様々なアプローチの仕方を先生方や先輩方とコミュニケーションを取りながら協力して取り組むことで、協調性が生まれました。また出題問題毎の目的が明確になり、質問が気軽に出来ることから理解が深まりました。

実践的な形式のトラブルシューティングを行えたと思います。演習の中でもこういった形式のものは珍しく、対応力を高めることができました。

今後のネット社会に必要な知識を、実践を交えて身に付けることができました。

受講・修了者数

平成29年度　29名，平成30年度　23名（近畿大7名）
令和元年度　24名（近畿大3名，北京郵電大11名），令和2年度　37名（近畿大8名，東北大1名）

国立大学法人 和歌山大学

川橋研の行ってきたプラクティス

- 情報危機管理コンテスト （2006年～）
  - サイバー犯罪に関する白浜シンポジウム
  - 経済産業大臣賞，文部科学大臣賞，JPCERT/CC賞
- SecCap， IT危機管理演習（2007年～）
  - 先導的ITスペシャリスト育成推進事業（旧IT-KEYS）
  - 奈良先端科学技術大学院大学
- enPiT Pro Security（ProSec）（2019年～）
  - 社会人向けインシデントレスポンス実践コース
  - 民間企業，県警サイバーポリス向け研修など
- サイバーセキュリティ人材育成事業（KSEC）（2018年～）
  - 高専機構KSEC拠点校への情報危機管理演習

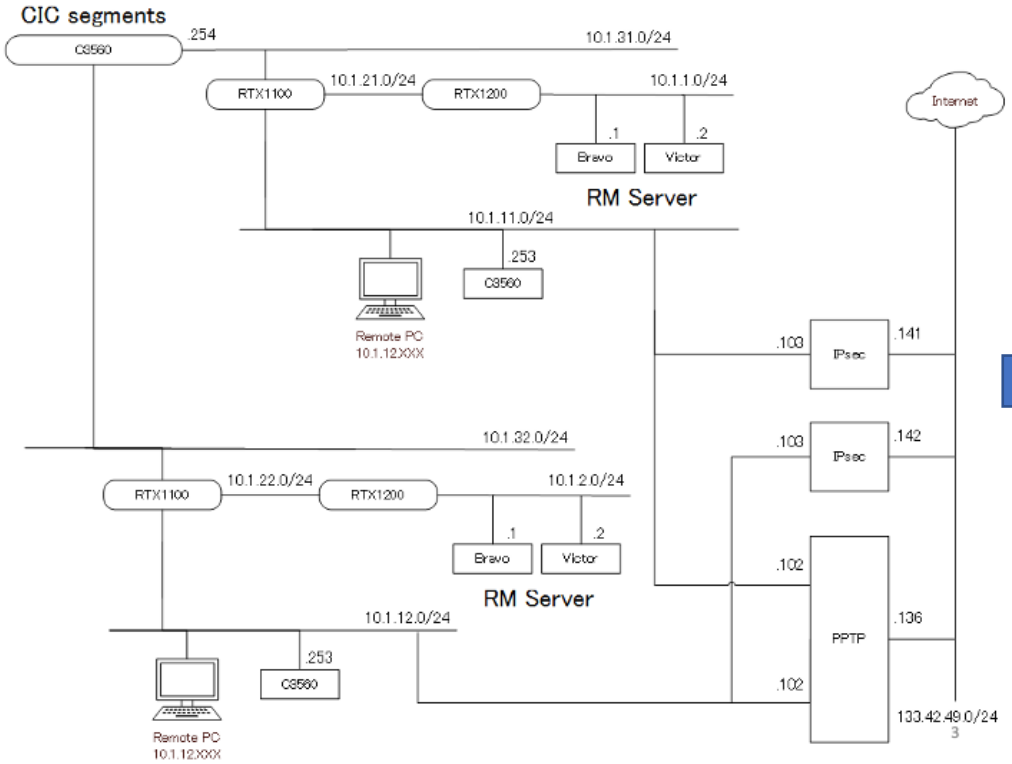
プラクティスで得たノウハウ

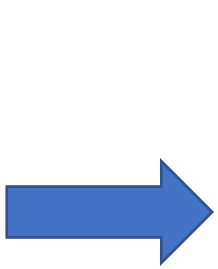
- 攻撃を実施するための環境づくり
  - 攻撃プログラムを作成する技術
  - インターネットに被害を及ぼさない局所化の技術
- 攻撃を成功させるための環境づくり
  - 攻撃される側の脆弱性を作成する技術
  - 決められた条件で100％攻撃を成功させる技術
  - 決められた範囲と規模で被害を発生させる技術
- 演習（コンテスト）として運営すること
  - 履修者の手が止まればヒントを出す
  - どのような反応をするかあらかじめ念入りに訓練

これまでの問題点

- 環境を構築するためのハードとソフトの維持
  - 環境のため様々なものを揃えないといけない
    - サーバ、ネットワーク、ファイアウォール、etc
    - OS、アプリ、脆弱性
    - 精密機器は数年で交換する必要も
- 仮想化によってソフト面の負荷は軽減
  - 同じインシデントを再現しやすい
- だがハードと運営については解決していない
  - 教育改革プロジェクトによって改善させる
  - ハードウェアの仮想化を運営のマニュアル化

開発

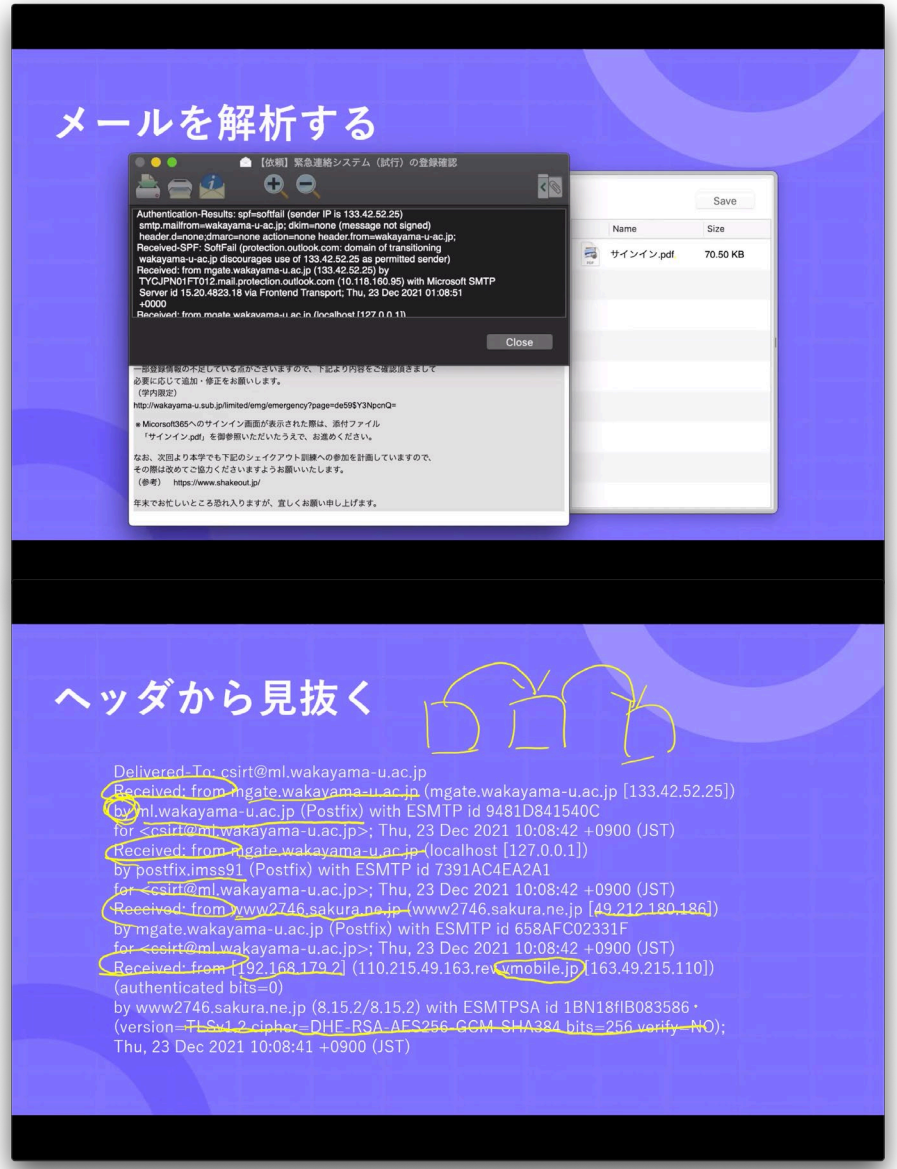




AWS（Amazon Web Swevice）で構築
- サーバ・ネットワークも仮想化
- ハード・ソフトの維持管理が容易
- 状況の高い再現性、再利用が容易
- 規模の拡張が容易

オンプレミス
- 物理的なサーバ、ネットワーク機器
- 機器の維持管理が必要
- 物理的制約（実際には最大５ブース）

試行（標的型メール攻撃）

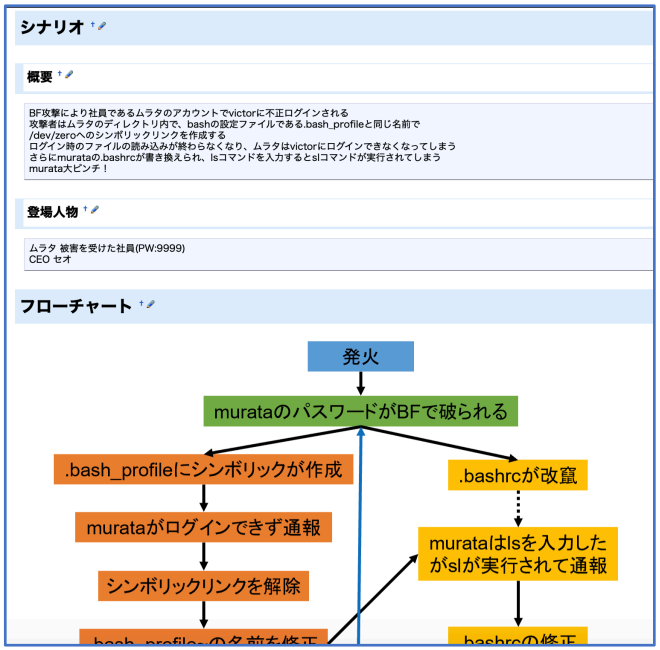


田辺産業技術専門学院（非常勤）
- 遠隔にて演習を実施
- AWS内で標的型メールを送受信
- メールの不自然な点を解説
- メールヘッダの解析と原理の説明
- 自組織で標的型にしやすい文面の作成

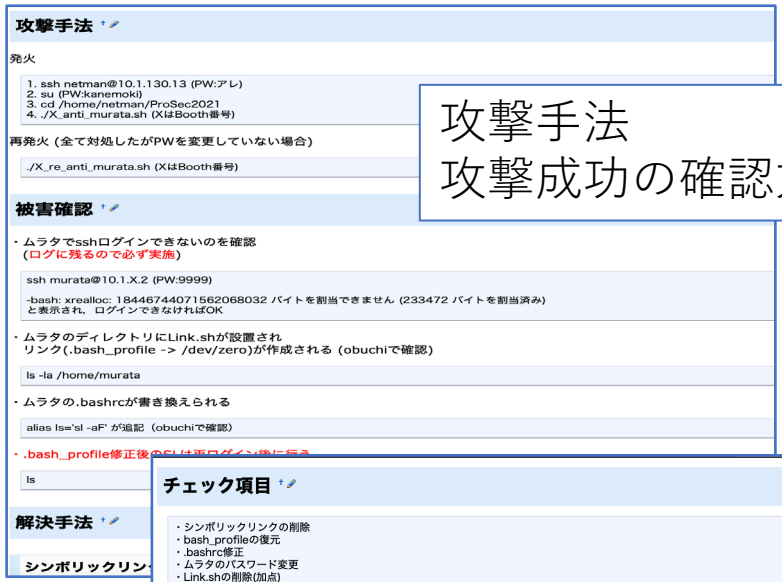
得られる効果と課題

- リテラシ教育における効果
  - 「情報倫理」を知識のみでなくどう使うか理解する
  - 悪意がどのような不自然さで現出するか理解する
- リカレント教育における効果
  - 手間暇をかけて演習を構築していると実感
  - 社会人と短い時間で信頼関係を構築しやすい
  - 自分の立場に置き換えて想像しやすい
- 運営するための体制づくりは課題
  - 簡単なインシデントのみAWSで再現
  - オペレータは必須
  - 業務の段取りをマニュアル化したが訓練は必須

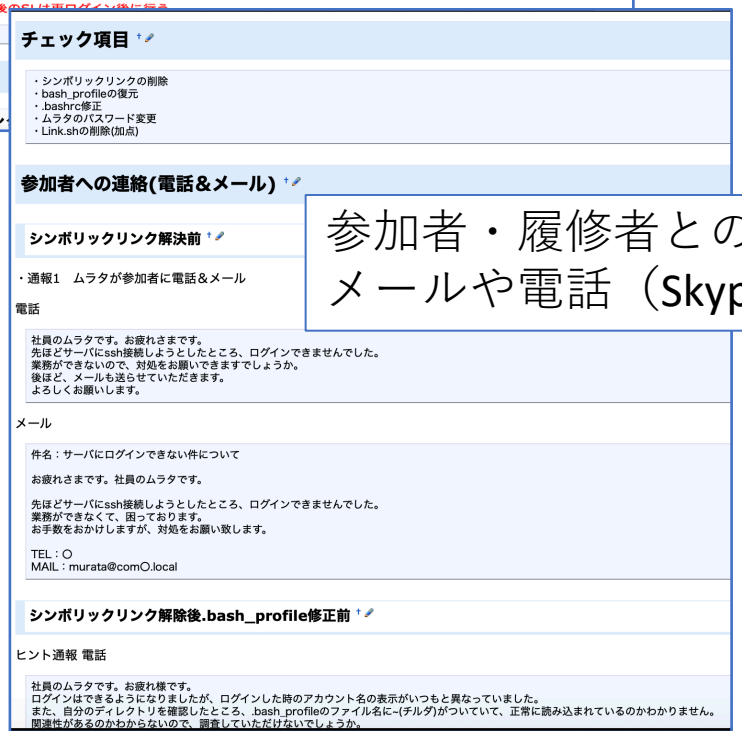
運営のマニュアル化



インシデントの概要
インシデントにおける登場人物
解決に至るまでの必要なステップ



攻撃手法
攻撃成功の確認方法



参加者・履修者との問答集
メールや電話（Skypeなど）

川橋研のこれまでのプラクティスを全面マニュアル化

さらなる課題と予算の内訳

- 運営側の体制を整える必要がある
  - AICスタッフと研究室学生（現在は川橋研で）
  - 学生を指導しつつ活用する
    - 謝金だけで動ける内容ではなく何らかのインセンティブ
    - 現在はリカレントを通じた企業とのふれあい・就活など
- 複雑なインシデントをAWS上で再現する
  - プライベートに押し込んだまま可能か検証
  - 発生するAWS利用料のマネージメント（制御）
- 予算
  - AWSでの環境構築・マニュアル化作業
  - AWS利用料はクーポンとアンケートでほぼ賄う
  - 運用開始すればランニングコストは要検討

学術情報センターの講義・演習の将来構想

「インシデントレスポンス演習」などの学術情報センターが提供してきた講義・演習を再構成して，受講者のレベルと要求に合わせて内容を容易に再構成可能にします。

高校生・企業の専門家，一般人などの様々な受講者に向けた教育コンテンツを提供可能にします。
担当教員の負荷を低減・分散化します。

現在の講義・演習を再構成

- 情報危機管理コンテスト
- インシデントレスポンス演習
- 高専向け講義

段階的な学習

「情報セキュリティエキスパートコース（仮称）」
IT実務の現場での業務遂行とセキュリティ対策及びインシデントレスポンスの運用設計ができるリーダーを目指す者を対象とし、内容としてはenPiT-Pro Securityで得られたノウハウを基にサーバやネットワークの構築・運用術等について取り扱う。

「情報セキュリティ基礎コース（仮称）」
ITスキルの習得を目指す社会人を対象とし、内容としてはTCP/IP基礎、ネットワークトラブルシューティング方法等を取り扱う。

「情報セキュリティ入門コース（仮称）」
一般のITユーザーを対象とし、内容としては情報倫理、情報セキュリティ基礎、関連法規等を取り扱う。