試行錯誤を可能とするセキュリティ演習システムの提案

Proposal of a Security Exercise System Enabling Trial and Error

- はじめに
- 特徴
- 設計
- 演習方法
- 関連研究
- おわりに

竹原一駿 石塚美伶 喜田弘司 最所圭三

香川大学

s20g470@stu.kagawa-u.ac.jp

はじめに

目的

知識と経験を持つ**セキュリティ人材**が**不足**している.

防御演習を**試行錯誤**することで，**セキュリティ人材の育成**を目指す.

セキュリティ教育 + 試行錯誤 = ?
セキュリティ人材の育成

サイバー攻撃から防御する
- 防御手法の調査 (調査)
- 防御手法の選別 (選別)
- 防御手法の試行錯誤 (試行)

サイバー防御の演習を試行錯誤
"ぷろてっくん"

セキュリティ人材の不足

より，日本では**サイバーセキュリティ人材**が圧倒的に**不足**

- ログを監視・分析して危険な兆候をいち早く察知できる
- セキュリティインシデントへの対応・指揮ができる

教育機関では

サイバー攻撃の予防，攻撃の発見，的確な対処の
知識と技術と持ったセキュリティ技術者の育成

IPA Better Life with IT
情報処理推進機構

より，「今後身につける必要のある知識」の調査では

「情報セキュリティ」の回答が最多である
情報処理技術者試験では，セキュリティの出題を拡充

試験にて

試験の合格がセキュリティに関する能力の指標

●総務省 , “ 総務省 ― 令和元年版情報通信白書 ― サイバーセキュリティに関する現状と新たな脅威 ”. https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd113310.html, 2021/05/04.
●IPA 独立行政法人 情報処理推進機構 , “ プレス発表 i パス（ IT パスポート試験）をはじめとする情報処理技術者試験の出題構成の見直しについて ”. https://www.ipa.go.jp/about/press/20131029.html, 2021/05/09.

セキュリティ人材の育成

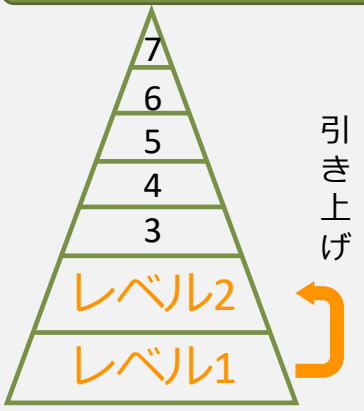
知識
- 学習することで一定の範囲で身につく
- ある程度の経験を補足

スキル
- 知識を活用して成果を生み出す能力
- **知識と経験**を重ねることで体得

即座に成果が発揮されるものではない

知識と経験を持つセキュリティ人材が不足している → スキルの向上を目指すことで十分な知識と経験を得る → **セキュリティ人材の育成**

受講者のスキルレベル



「i コンピテンシ ディクショナリ」に当てはめる
(旧: 共通キャリア・スキルフレームワーク)

現在の受講者
- 技術内容について講義を受講し知識がある
- ITパスポート合格程度

目指す受講者
- 指示があると活用できる
- 実装経験がある
- 基本情報技合格程度

● IPA , “ 共通キャリア・スキルフレーム (第一版・追補版)”.独立行政法人情報処理推進機構 IT 人材育成本部 IT スキル標準センター， pp.7 ， 2012/06/17.
● IPA , “i コンピテンシディクショナリ解説書”.独立行政法人 情報処理推進機構IT人材育成本部ＨＲＤイニシアティブセンター，
https://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/， pp.36， 2015/06/30.

スキルレベルの向上のための実践

セキュリティ人材を目指した，スキルレベルの向上

調査

防御手法の知識の習得
- サイバー攻撃に対する自発的な調査
- 機器の設定を基に，攻撃の**原因や影響を調査**
- Webや過去の事例を活用

選別

習得した知識の活用
- 防御手法の有効性はその時々で異なる
- 知識を選別し，現状に**最適な手法を選択**
- OSやミドルウェアに応じた手法

試行

様々な環境で試行錯誤し，今後を見据えた防御
- 攻撃に合わせた防御手法を試行
- 指示された作業(スキルレベル2)は環境毎に異なる
- 異なる環境を多く経験
- 防御の成功や失敗を検証し，経験を重ねる

“ぷろてっくん”の提案

試行錯誤を促す

サイバー攻撃に対する防御演習を
試行錯誤できるシステム
”ぷろてっくん”

**知識の習得と活用を行い，試行錯誤で経験を重ねる
スキルレベルが向上する**

セキュリティ人材の育成に寄与

“ぷろてっくん”を用いた演習

宿題型の**コンテスト形式**で防御スコアを**一定時間毎に比較**する

受講者は，調査や選別に長い時間を掛けた熟考を可能とする	**宿題型** 1週間程度の演習を想定する 自宅でも演習ができる
ゲーム感覚のイベントで参加でき，成績向上の目的意識を明確にする	**コンテスト形式** ISUCONやAtCoderのように成績によって，実力が明確にわかる
受講者に演習への積極的な取り組みや多く試行を誘導する	**一定時間毎に比較** スコアを受講者間で共有し，対抗意識による学習効果の向上を目指す

●富永浩之 , 太田翔也 , “ 実行テスト系列を取り入れた小コンテスト形式の初級 c プログラミング演習における段階的実装を誘導する得点ルール ”. 情報教育シンポジウム論文集 , 2017(33), pp.206–211, 2017.
●ICPC, “ 国際大学対抗プログラミングコンテスト ”.https://icpc.iisf.or.jp/, 2021/05/09.
●AtCoder, “ 競技プログラミングコンテストを開催する国内最大のサイト ”. https://atcoder.jp/, 2021/05/09.
●ISUCON, “ 公 式 Blog”. https://isucon.net/,2021/05/09.

演習の流れ

事前説明

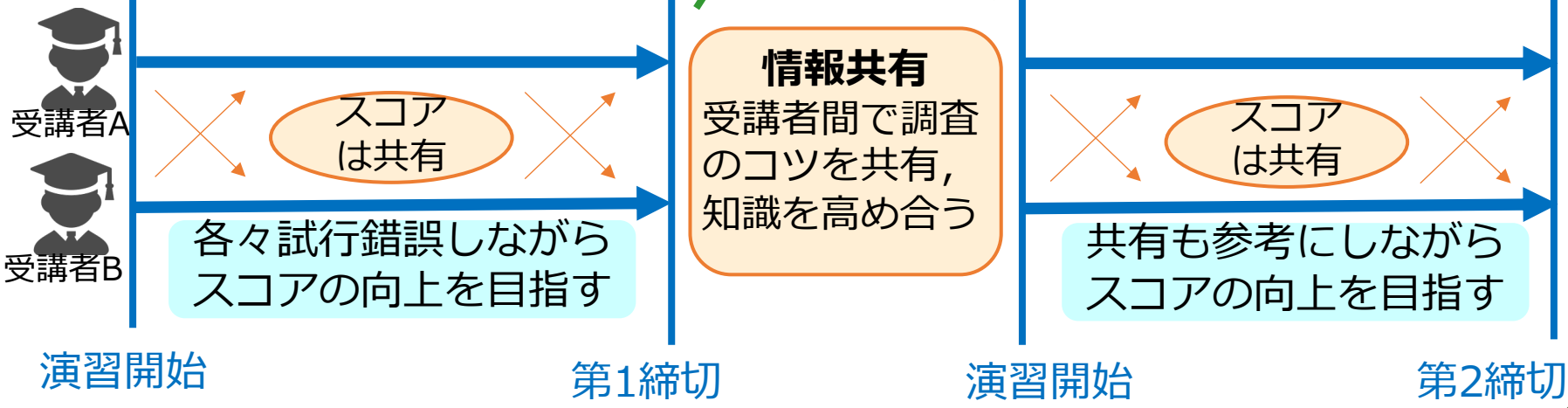
●機能説明
サービスが明確に攻撃されており，受講者が対応する必要がある
●調査方法
攻撃を受け防御する例示する
●使用方法
自宅からアクセスする方法や試行錯誤の手法

環境を変更

OS(Windows/Linux)やアプリケーション(Apache/Nginx)を変更

評価

●防御スコア
知識や経験の習得度を計測



“ぷろてっくん”の特徴

防御スコア

- 成功度合い
- 他の受講者と共有
- 対抗意識を促す

試行錯誤

- セーブ&リストア
- 防御手法を何度も実践
- 最適な防御手法を検討

単独演習

- 個人で機器を操作
- 手を動かせる
- 独力で作業の遂行

機器操作

- 受講者は機器を操作
- ログの調査
- 防御の実行

環境変更

- 異なる環境で防御
- osやアプリケーション
- 環境に合う選別

自宅演習

- 自宅で長期間
- オンライン対応

防御スコアを試行錯誤

防御スコア

- 防御が効果的か判断できる
- 通常状態か異常か判断できる
- 受講者間で共有し対抗意識を促す
- ECサイトなら防御中の売上である

スキルレベルが向上した指標 → 完璧な防御を行ったときの **6割程度**

攻撃に対する防御の操作を「要求された作業」 → 基本情報技術者の合格点の **60点程度**

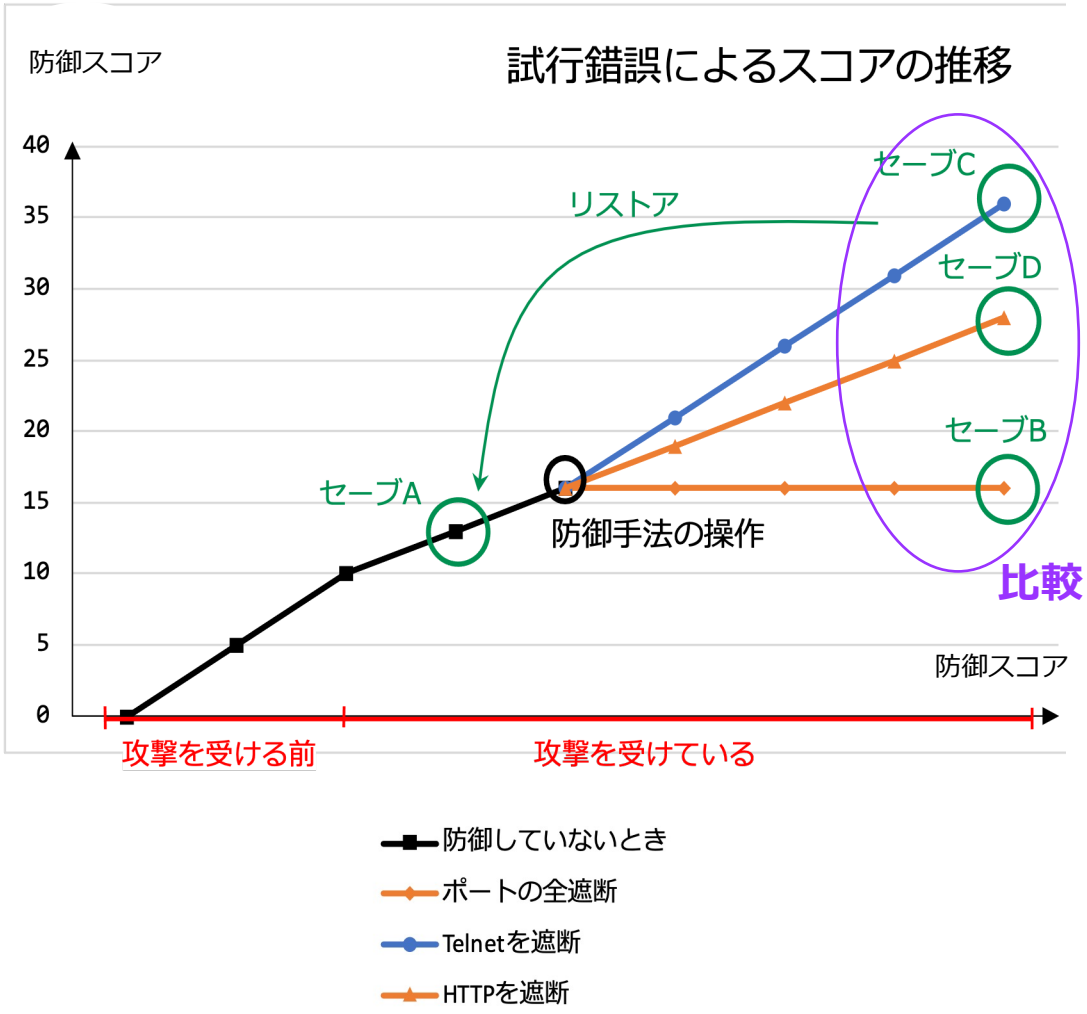
試行錯誤

- 演習システムをセーブ&リストア
- 任意の箇所で行える
- リストアし，異なる防御手法を実践できる
- 最適手法を試行錯誤で取得できる

攻撃を受けた直後にセーブ → 防御する手法を実践

セーブした箇所にリストア → **異なる** 防御手法を実践

試行錯誤によるスコアの推移



攻撃を受けたことに気づき，セーブAする

とりあえずポートの全遮断で防御し，セーブBする

攻撃を受けた当初(セーブA)にリストアする

セーブB,C,Dのスコアを比較し，この環境ではセーブCの防御が最適だとわかる

異なる環境にも対応する機器の操作

機器操作

- 受講者は攻撃を受ける機器を操作してサービスを防御する
- 機器のログなど調査をする
- コマンドなどで防御手法を実行

サービスの防御のための現状調査 → **自発的に調査する**

調査した手法の実行 → **攻撃へ対応**

環境変更

- 防御するサービスを異なる環境で提供する
  - Linux/WindowsやApache/Nginx
- 環境に合う防御手法を選別する

異なる環境での操作 → **知識の活用**

環境に合った手法の選別 → **攻撃への的確な対処**

単独での自宅学習

単独演習

- 受講者が個人で機器を操作する
- グループワークだと，スキルレベルの高い受講者が演習を独占
- 受講者の全員がスキルを習得

防御のために機器を操作する → **レベル2の指示に従って活用できる**

個々人で演習する → **スキルレベルの全体的な引き上げ**

自宅演習

- 自宅で長期間取り組める
- SSHなどで遠隔ログイン
- オンラインに対応している
  - 会場の設営が不要

長期間の演習 → **手法を多く試行錯誤できる**

オンライン対応 → **COVIT-19下でも安定してレベルを向上**

“ぷろてっくん”の設計

特徴の実現のために以下の機能を有する

標的機能

受講者が防御すべきサービスを提供
例: ECサイト，ファイル共有

環境変更機能

サービスを様々な環境で提供する
e.g. Linux / Windows, Apache / Nginx

攻撃機能

標的機能を攻撃する
バックドアを仕掛けたり，脆弱性を狙う

状態管理機能

任意のタイミングでセーブ&リストア
Snapshotを用い，木構造で管理する

防御スコア機能

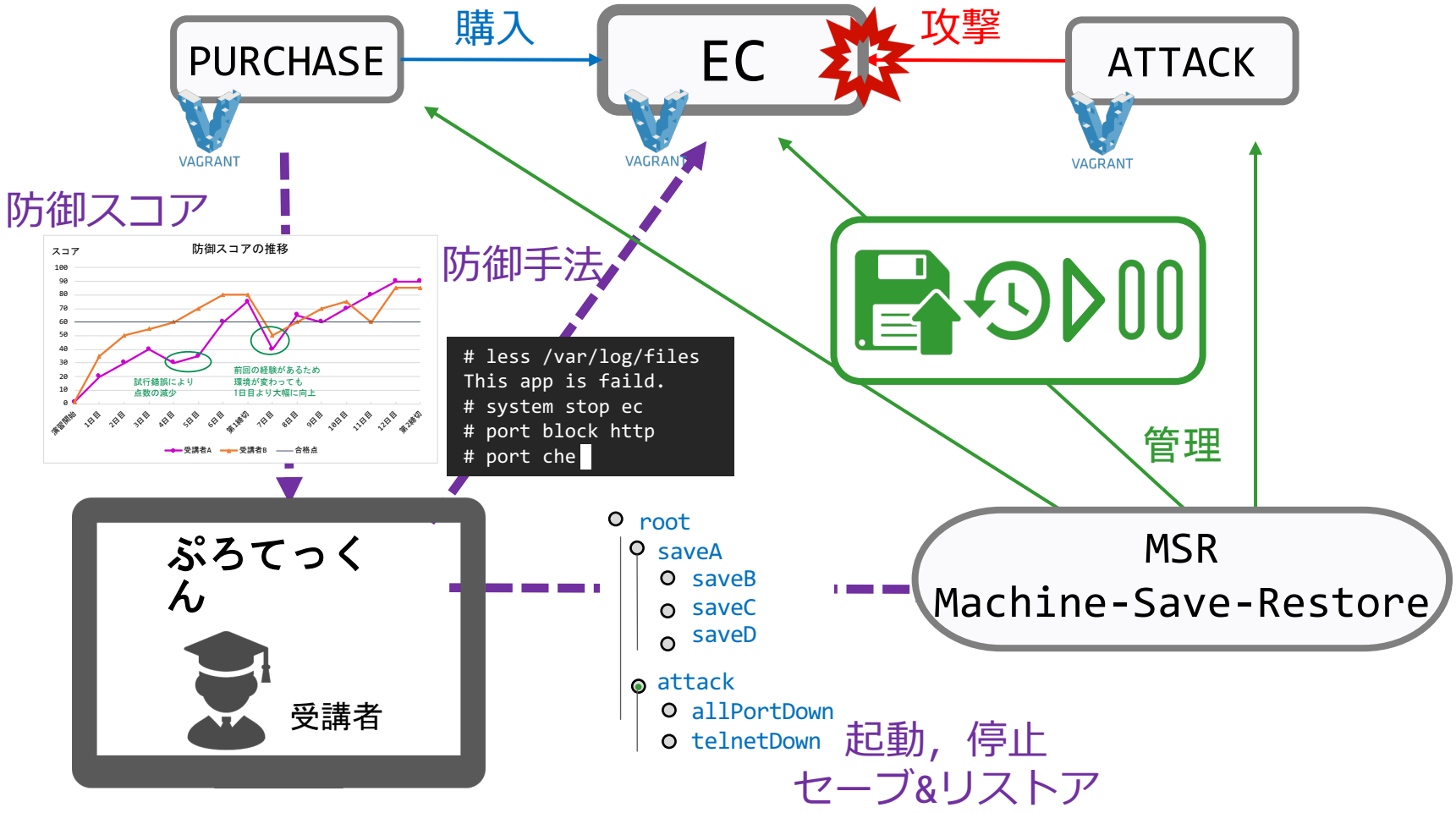
どの程度システムを防御するか
受講者間でスコアを共有する

単独演習機能

自宅からでも遠隔ログインできる
SSHなどで機器を操作できる.

香川大学
KAGAWA UNIVERSITY

“ぷろてっくん”のシステム構成



関連研究

インシデントの仕組み学習と体験を可能とするセキュリティ訓練システム
- セキュリティインシデントの再発防止を目指す
- インシデントを再現し，個人が端末を操作し，攻撃の結果を体験する

→ **演習環境内で攻撃を体験することで知識を増やせる**

体験型サイバーセキュリティ学習システム
- 自習形式のセキュリティの体験型学習のシステムを提案
- LinuxやWindowsを操作し，ログの参照や検索の演習を行う

→ **自習形式でも体験型学習が実現でき，学習効果が確認できる**

Micro Hardening
- クラウド上に構築したECサイトを攻撃から守る競技を行う
- 情報共有や記録収集など技術外の対応も演習する

→ **スキルの高いメンバーのみが機器の操作や調査を全て行う**

●清時耀 , 福田洋治 , 井口信和 , “ インシデントの仕組みの体験学習を可能とするセキュリティ訓練システムの開発 -情報収集作業を支援する訓練シナリオ作成機能の検討 -”.2019 年度 情報処理学会関西支部 支部大会 講演論文集 ,G-08, 2019.
●清時耀 , 福田洋治 , 井口信和 , “ インシデントの仕組み学習と体験を可能とするセキュリティ訓練システムの開発-Web を介した誘導型攻撃の訓練の評価と確認テストの機能の検討 -”. 第 81 回全国大会講演論文集 pp.411–412.2019.
●八代哲 , 高橋和司 , 渡辺亮平 , 角田裕太 , 田邉一寿 , 横山雅展 , 齋藤祐太 , 齋藤孝道 , “ 体験型サイバーセキュリティ学習システムの提案と構築 ”. コンピュータセキュリティシンポジウム 2017 論文集 , pp.1453–1460, 2017.
●八代哲 , 田邉一寿 , 齋藤祐太 , 齋藤孝道 , “ 体験型サイバーセキュリティ学習システムの提案と再評価 ”. マルチメディア , 分散協調とモバイルシンポジウム 2018 論文集 ,pp.1809–1816, 2018.
●株式会社 川口設計 , “MicroHardening”. https://www.sec-k.co.jp/mh, 2021/05/09.

おわりに

セキュリティ人材の不足

サイバー攻撃の予防，攻撃の発見，的確な対処の**知識と技術と持ったセキュリティ技術者の育成**

サイバー攻撃から防御する
- 防御手法の調査 (調査)
- 防御手法の選別 (選別)
- 防御手法の試行錯誤 (試行)

知識の習得と活用を行い，試行錯誤で経験を重ねるスキルレベルが向上する

サイバー防御の演習を試行錯誤
"ぷろてっくん"

セキュリティ人材の育成に寄与