L-026

サイバー・セキュリティ教育を目的としたシリアスゲームの構築法の提案
A proposal of serious game development method for cyber security education

伊藤 達哉 † Tatsuya Ito
古市 昌一 ‡ Masakazu Furuichi

1. はじめに

IT 技術の進化とともにサイバー空間における脅威は日々進化し続けている. コストパフォーマンスの関係から, 国家間の戦争がサイバー空間へと変わってきている. しかしサイバー空間を守るための人材が不足している. それらの対策として, 従来は CTF(Capture The Flag)[1] と呼ばれるセキュリティの技術を競うための大会を開催することで情報セキュリティの人材育成を行っていた. しかし CTF に出場するためには, 一定水準の技術力を身につけていなければならないという欠点がある. そこで本研究では, アドベンチャーゲームと仮想環境を用いてセキュリティ技術の学習支援を行うシリアスゲームの構築方法を提案する.

2. 既存研究

ネットワークセキュリティの教育を目的とした研究として, 金井はユーザを攻撃プレイヤー, 防御プレイヤー, 観戦者の 3 つの立場に分け, ネットワーク上の脅威や対策の効果を体験できるシリアスゲームの構築を行った [2]. この研究はセキュリティ意識の向上を目的としているが, 技術についての演習を行うことが出来ない. また岩崎らはサイバー演習のシナリオをファイルによって定義し仮想マシンネットワークを再現することで演習環境の準備の自動化を行った [3].

3. 提案方式

3.1. システムの概要

先述した岩崎らの研究においては, ネットワーク機器の接続状態を定義することは出来るがミドルウェアやアプリケーションの定義を行うことが出来ない. 本研究においては Vagrant[4] を用いることによる仮想環境構築の自動化を行うことで上記の問題を解決した. またサイバー演習 [5] に代表されるシナリオを用いたサイバー攻撃の対策・対処を訓練するための演習方法を採用し, 本システムではアドベンチャーゲームを用いることにより,1 人でも演習が実施可能な形態とした. 図 1 に提案システムの構成を示す.

本提案システムは,Web サーバと仮想マシンを起動する命令を送受信する python のアプリケーション (以下仮想マシン管理サーバ, 仮想マシンハンドラ), データベースを LAN 内に設置する. 演習者は Web サーバへ接続し問題文を読む.Web サーバは問題の内容に従って仮想マシン管理サーバへ仮想マシンの識別子と起動命令を送信する. 続いて仮想マシン管理ハンドラが仮想マシンの起動を行う. そして仮想環境での演習によって得られたキーワードを Web サーバへ送信する事によって問題の解答を行う.

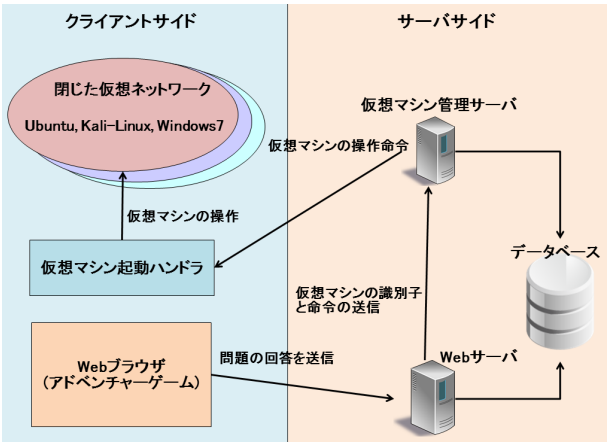

図 1: システムの構成

図 2: システムのユーザインターフェース

4. 試作システムの実装

4.1. ゲームシナリオの定義

演習はアドベンチャーゲームを用いて進める. 本システムではアドベンチャーゲーム内に登場するキャラクターの台詞, キャラクターの画像や背景をスクリプトを用いて容易に記述することができるように TyranoScript[6] を用いた. さらにゲームの進行に合わせて TyranoScript から仮想マシンを起動するためのインターフェースを PHP を用いて実装した. これらのスクリプトをシナリオ定義ファイルと呼ぶ.

4.2. 演習用仮想マシンの作成

本システムでは, 繰り返し同じ演習環境を再利用することを考えて, スナップショット機能を用いる. 仮想化ソフトウェアは VirtualBox を用いた. また演習者が仮想マシン内で用いるツールは表 1 の通りである. 演習者が使用する仮想マシンへ自動的に攻撃を行う仮想マシン上で実行される攻撃ツールは表 2 の通りである. 演習者が利用する仮想マシンと自動的に攻撃を行う仮想

†日本大学生産工学研究科
‡日本大学生産工学部

マシンはシナリオ定義ファイルによって起動される．またログ解析やマルウェア解析は初心者には難易度が高いためそれぞれ通信の可視化ツール [7] とサンドボックス解析ツール [8] を用いた．

表 1: 演習環境で使用するツール

ツール名	利用目的
wireshark	パケット解析
regripper[9]	プログラム実行履歴の解析
Cuckoo Sandbox	マルウェアの動作解析
firefox	HTML ソースの確認

表 2: 攻撃サーバが実行するツール

ツール名	利用目的
metasploit-framework	C&C サーバの起動
xssf[10]	XXS 攻撃の実行

4.3. 演習の流れ

演習の流れは図 3 に示す通りである．はじめに各演習者の PC 端末に仮想マシンのイメージファイルをコピーする．次に演習で利用するツールと Web ユーザーインターフェースの使い方を動画によって説明 (以下動画説明) し, アドベンチャーゲームでの演習を行なう．演習者がツールの使い方を忘れてしまった場合には演習を中断しもう一度動画説明を受けてから演習を再開することが出来る．演習のデータはヒント表示回数, 動画の再生回数, 正答数, 誤答数の 4 つを記録する．

4.4. ユーザインターフェース

演習者の Web ブラウザーから演習用のサーバへアクセスすると図 2 のような画面が表示される．演習者はこの画面を利用してセキュリティ演習を行う．はじめに演習者はメイン画面に表示されるアドベンチャーゲームから提示された課題を指示に従って仮想マシン上で解く．続いて得られた答えを,Web ページのフォーム画面へ入力して送信を行うことによって問題の解答を行う. 解答結果が正しい場合には画面下にある下部のプログレスバーが減少する. 解答結果が正しくない場合には画面下の青いプログレスバーが減少する. 画面下にある上部のプログレスバーの値が 0 %となった場合はゲームオーバーメッセージを表示し, はじめから演習をやり直す．また動画説明は, 画面右側の動画リストから説明内容を選択すると, メイン画面がアドベンチャゲームから動画の再生画面へと遷移する. アドベンチャーゲームへ戻る場合はブラウザの戻るボタンを使用する．

5. 評価方法

本システムの評価は基本情報技術者試験資格取得者を対象に一定時間行い, 理解度のテスト, アンケート, 演習データの計測の 3 つの手法を用いて行う．理解度のテストによる評価ではゲーム中で使用したツール名や使い方, 使用理由を問う問題を出題し演習目的を達成出来たかどうかを確認する．アンケートによる評価ではユーザーインターフェースの使いやすさや演習の難易度, 面白さなどのゲームの質についてのアンケートを実施する．また, 演習データの計測による評価は上記 2 つの評価と演習のデータとの関係性を示す．

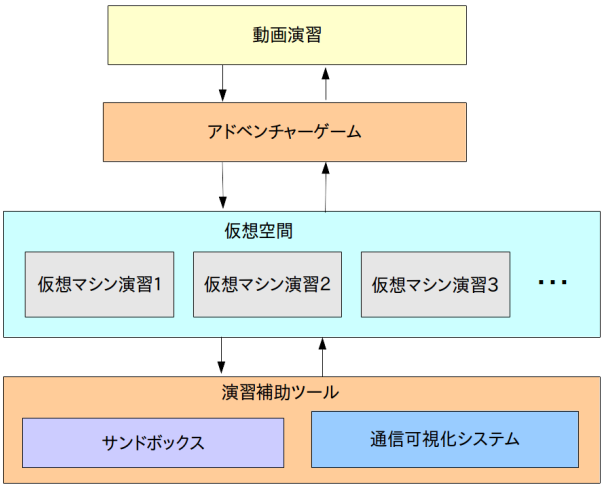

図 3: 演習の概要

6. おわりに

本稿ではセキュリティ技術教育を目的としたシリアスゲーム構築方法について概要を説明した後, 本研究の評価方法を述べた. 今後上記の評価方法に基づき実験を実施し本研究の有効性を評価することが課題である. 提案方式の有効性を確認した後, 仮想環境での学習範囲の拡大を検討したいと考えている．

参考文献

[1] DEFCON CTF, http://www.defcon.org/html/links/dc-ctf.html (2014.6 参照)

[2] 金井 正和, “3DCG を用いたネットワークセキュリティの教育支援ゲーム”, 大学院研究年報　理工学研究科篇 第 41 号, pp.2-5, 2011.

[3] 岩崎 智弘, 立岩 佑一郎, 安田 孝美,“仮想マシンネットワークによる継続的なクラッキング防衛演習環境の開発”, 電子情報通信学会技術研究報告. ET, 教育工学 110(453), 175-180, 2011.

[4] Vagrant, http://www.vagrantup.com/ (2014.6 参照)

[5] サイバー演習 (サイバーディフェンス研究所), http://www.cyberdefense.jp/services/lab.html (2014.6 参照)

[6] TyranoScript, http://tyrano.jp/ (2014.6 参照)

[7] CyberGlobe, https://github.com/tatsui/cyberglobe/ (2014.6 参照)

[8] Cuckoo-Sandbox, http://www.cuckoosandbox.org/ (2014.6 参照)

[9] regripper, http://regripper.wordpress.com/ (2014.6 参照)

[10] xssf, https://code.google.com/p/xssf/ (2014.6 参照)