攻防戦型演習を可能とするネットワークセキュリティ学習システムの評価

Evaluation of a Network Security Learning System that enables Offensive and Defensive Battle Exercise

寺西 弘登[*1], 井口 信和[*2*3]
Hiroto TERANISHI[*1], Nobukazu IGUCHI[*2]
[*1] 近畿大学大学院総合理工学研究科
[*1]Graduate School of Science and Engineering, Kindai University
[*2] 近畿大学情報学部
[*2] Faculty of Informatics, Kindai University
[*3] 近畿大学情報学研究所
[*3] Cyber Informatics Research Institute, Kindai University
Email: iguchi@kindai.ac.jp

あらまし：年々サイバー攻撃の報告件数は増加しており，対策の難易度も上昇している．本研究では，サイバー攻撃に関して攻撃側と防御側の両視点からセキュリティ演習が実施可能な環境の提供を目的に，攻防戦型演習を可能とするネットワークセキュリティ学習システムを開発している．本稿では，本システムを用いて演習を円滑に取り組めるかについて確認することを目的に，性能評価実験を実施した．また，本システムを用いた場合に，座学と比較してネットワークセキュリティ学習を支援できるかについて確認することを目的に，利用評価実験を実施した．
キーワード：ネットワークセキュリティ，学習システム，攻防戦

1. はじめに

令和 4 年に警察庁が実施した 372 社の民間企業，行政機関等における調査結果によると，ペネトレーションテストを導入していないと回答した組織は 50%であった[1]．原因としてセキュリティ技術者不足がある．この原因の解消には，各組織がネットワークセキュリティ教育を実施し，セキュリティ技術者の早期養成が必要とされる．

年々サイバー攻撃が増加し，手口も巧妙化することで対策の難易度が上昇している．こうした現状を改善するために，サイバー攻撃に対して防御視点だけでなく，攻撃視点からも攻撃の性質やプロセスを学習し，対策に活かすことが重要である[2].

そこで本研究では，サイバー攻撃に対して攻撃側と防御側の両視点からネットワークセキュリティ演習が実施可能な環境の提供を目的に，攻防戦型演習を可能とするネットワークセキュリティ学習システムを開発してきた[3]．本システムでは，学習者は 2 人 1 組になり，攻防戦形式で，DoS 攻撃，ARP Spoofing 攻撃，不正侵入攻撃及び SQL インジェクション攻撃のセキュリティ演習を仮想ネットワーク上の仮想機器を用いて取り組む．仮想ネットワークを活用するため，実運用されているネットワークに影響を与えず，実践的な演習を実施可能である．本稿では，本システムを用いて演習を円滑に取り組めるかを確認した．また，本システムを利用した学習と座学による学習のグループに分け，事前・事後テストの点数差を比較し，システムを利用した場合の学習効果を評価した．

2. 先行研究

本システムの先行研究として，湯川らの研究がある[2]．この研究では，Web ブラウザ上で攻防戦型ネットワークセキュリティ演習が可能となっている．しかし，Web ブラウザ上の GUI の描画に Flash を用いており，このシステムは 2020 年末に Flash のサービスが終了したことで利用ができなくなった．また，全ての機能を 1 つのサーバで管理しており，保守や開発のハードルが高くなる問題があった．本研究ではこれらの問題を解決するために，新たな設計で開発した[3]．まず，GUI の描画に PixiJS を用いた．そして，コンポーネント設計を採用することで，機能の追加や再利用を容易にした．加えて通信サーバを実装し，負荷分散によって多数のユーザの演習に対応可能とした．

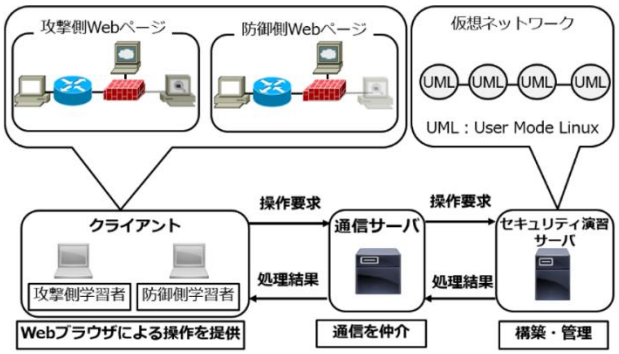

図 1 システム構成図

3. 研究内容

3.1 システム概要

本システムのシステム構成を図 1 に示す．本シス

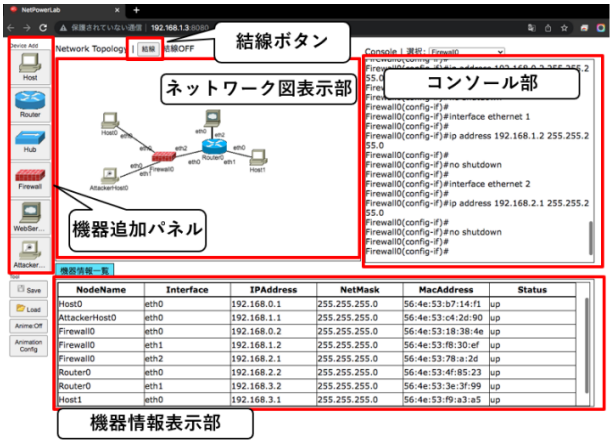

図 2 ネットワークセキュリティ演習画面

テムは，セキュリティ演習サーバ，通信サーバ及びクライアントから構成されている．セキュリティ演習サーバは，アクセスしているユーザの管理と，学習者が User Mode Linux を用いて複数の仮想マシンの作成を可能とする機能を提供する．作成した仮想マシンはホストやネットワーク機器(以下，仮想機器)として動作させる．複数の仮想機器を相互接続させることで，仮想的にネットワークの構築を可能とする．通信サーバは，セキュリティ演習サーバとクライアント間の通信を仲介する．クライアントは，学習者が Web ブラウザ上で GUI によって仮想機器の配置や設定が可能となる機能を提供する．

3.2 攻防戦型ネットワークセキュリティ演習機能

本システムの演習画面を図 2 に示す．本システムでは，学習者が 2 人 1 組で攻撃側と防御側に分かれ，DoS 攻撃演習，ARP Spoofing 攻撃演習，不正侵入攻撃演習及び SQL インジェクション攻撃演習が実施可能である．それぞれの演習実施前に，事前学習ページで本システムの利用方法と攻撃方法及び防御方法を学習する．その後で防御側が仮想ネットワークを構築する．利用可能な機器は Host，Router，Hub，Firewall 及び WebServer である．次に攻撃側は，攻撃用ホストを用いて攻撃を開始する．防御側は，攻撃に対して対策を施す．2 人 1 組でのネットワークセキュリティ演習は，防御側がランダムに実施される攻撃の種類を特定して対策するため，実践的なネットワークセキュリティ学習が可能である．また攻撃側は，実際に攻撃を体験することで攻撃の性質やプロセスを学習することが可能となる．

4. 実験

4.1 性能評価実験

想定する演習のネットワーク規模に対応可能であることを確認するために，想定する演習の最大規模のネットワーク構築時における最大 CPU 使用率とメモリの使用量を 10 回計測した．想定する最大規模は，Host，Router，Firewall，Hub をそれぞれ 10 台，攻撃用ホスト，WebServer をそれぞれ 1 台とした．通信サーバとセキュリティ演習サーバは VirtualBox 上の仮想マシンで起動する．仮想マシンのスペックは CPU(2 コア) : AMD Ryzen5 4600G with Radeon Graphics 3.70GHz, Mem : 10GB, OS : Ubuntu 20.04 LTS である．計測結果を表 1 に示す．本システムが想定する最大のネットワーク規模に対応可能であることが確認できた．

表 1 計測項目とその結果

計測項目	平均	標準偏差
最大 CPU 使用率	40.1%	2.8%
メモリ使用量	1.78GB	0.06GB

表 2 事前・事後テストの結果

	事前テスト		事後テスト	
	平均	標準偏差	平均	標準偏差
本システム	11.2	2.39	14.4	0.89
座学	10.4	2.40	11.4	1.14

4.2 利用評価実験

本システムを用いた場合の学習効果を確認するために，情報学を専攻する学生 10 名を対象として利用評価実験をした．実験対象者は，本システムで学ぶグループと座学で学ぶグループに分割し，学習に取り組んでもらった．それぞれの学習の前後にテストを設けた．2 グループにおけるテストの点数差から学習効果を評価した．

事前・事後テストは，基本・応用情報技術者試験を基に作成した．事後テストは，事前テストと同レベルの別の問題を用いた．問題数は 15 問であり，1 問 1 点として点数をつけた．また，事前テストの解答を知らせずに，事後テストを実施した．実験結果を表 2 に示す．本システムを用いたグループは平均点が 3.2 点上昇し，座学のグループは平均点が 1 点上昇した．したがって，本システムを用いて学習した場合に点数の上昇幅が大きくなることを確認した．

5. おわりに

本研究では，攻撃側と防御側の両視点からネットワークセキュリティ演習が実施可能な環境の提供を目的として，攻防戦型演習を可能とするネットワークセキュリティ学習システムを開発した．そして，本システムを利用した場合の学習効果を評価した．

参考文献

(1) 警察庁サイバー警察局サイバー企画課 : 不正アクセス行為対策等の実態調査，入手先 <https://www.npa.go.jp/bureau/cyber/pdf/R4countermeasures.pdf>(参照 2023-05-26).
(2) 湯川誠人，谷口義明，井口信和 : “攻防戦型ネットワークセキュリティ学習支援システム”，電子情報通信学会論文誌，Vol.J103-D，No.8，pp.591-602(2020).
(3) 寺西弘登，井口信和:“攻防戦型演習を可能とするネットワークセキュリティ学習システムにおける SQL インジェクション攻撃演習機能の追加”,情報処理学会第 85 回全国大会講演論文集,No 4, pp.903-904(2023).