情報処理学会論文誌 Vol.57 No.3 931–935 (Mar. 2016)

テクニカルノート

# 仮想マシンを活用したネットワークセキュリティ学習支援システムの実装と評価

福山 和生[1,a)] 谷口 義明[2] 井口 信和[2]

受付日 2015年5月8日, 採録日 2015年10月2日

**概要**：不正アクセスによる被害の増加，ネットワークセキュリティに関する知識，技能を持つ技術者の不足などを背景に，ネットワークセキュリティ教育の重要性および緊急性が高まっている．実践的なネットワークセキュリティ教育のためには演習が不可欠であるが，独立した演習環境を構築するための機材の準備コストなどが障壁となる．本研究では，仮想マシンを用いて1台のコンピュータ上に不正アクセス対策機器を導入した仮想ネットワークを構築することにより，安全かつ低コストにネットワークセキュリティに関する演習を実施できるシステムを実装した．評価実験の結果，本システムで実践的なネットワークセキュリティの学習環境を提供できることが分かった．

**キーワード**：仮想化技術，ネットワークセキュリティ，e ラーニング，ファイアウォール，Web アプリケーションファイアウォール

# Implementation and Evaluation of Virtual Machine-based System to Support Network Security Learning

Kazuki Fukuyama[1,a)] Yoshiaki Taniguchi[2] Nobukazu Iguchi[2]

Received: May 8, 2015, Accepted: October 2, 2015

***Abstract:*** Education of network security has attracted a lot of attentions due to increasing unauthorized access, lack of engineers who have network security skills, and so on. Although practice using computer networks is highly important for network security education, it requires costs to prepare a computer network for practice. In this paper, we develop a low-cost, easy and safe learning support system for network security by utilizing virtual machine technologies. In our system, a virtual network is constructed on one PC. By using firewall and web application firewall functions in our system, a user can learn countermeasures against unauthorized access. Through evaluations, we show that our system can provide practical environment for learning network security.

***Keywords:*** virtualization technology, network security, e-learning, firewall, web application firewall

## 1. はじめに

インターネットの普及にともない，不正アクセスによる被害が多発している．ところが警察庁の調査によると，不正アクセス対策を実施し，システムの脆弱性を検証している組織は3分の1程度となっている [1]．その理由として，ネットワークセキュリティに関する知識を有したエンジニアの不足や，外部委託するための予算がないといった問題が指摘されている．そのため，各組織は独自に不正アクセス対策などのネットワークセキュリティに関する教育を実施しなければならない場合がある．ネットワークセキュリティに関する教育は，知識の習得を目的とした机上学習に加えて，実践的スキルの習得を目的とした演習が必要不可欠である．演習は，実運用されているネットワークやサーバに影響を及ぼさないよう，独立した演習環境を用いて行うことが望ましい．しかし，演習環境を構築するには，機

[1] 近畿大学大学院総合理工学研究科
Graduate School of Science and Engineering Research, Kinki University, Higashiosaka, Osaka 577–8502, Japan
[2] 近畿大学理工学部情報学科
Department of Informatics, Faculty of Science and Engineering, Kinki University, Higashiosaka, Osaka 577–8502, Japan
[a)] fukuyama0083@gmail.com

材やその機材設定に準備コストが発生する．また，実機を用いた演習では，演習自体に要する時間も長くなり，限られた時間の中で学習できる演習項目が制限される．このような問題点から，現状の多くの組織では，セキュリティ教育として教材を用いた机上学習のみしか実施されていない．

これらの問題を解決するため，本研究では，仮想マシンを活用し，1台のコンピュータ上にルータやWebサーバなどを仮想的に配置した仮想ネットワークを構築することにより，安全，低コストにネットワークセキュリティの演習を実施できるシステム（以下，本システム）を開発した．本システムは，仮想ネットワーク上で実際に攻撃を行い，ファイアウォール（以下，FW）やWebアプリケーションファイアウォール（以下，WAF）でのフィルタリングや，ログを観察する演習が可能である．本システムを用いることで，各組織が独自にネットワークセキュリティに関する実践的な教育を実施できる．

## 2. 関連研究

ネットワーク技術に関する認定資格であるCCNA（Cisco Certificated Network Associate）やネットワークセキュリティ技術に関する資格であるCCNA Securityなどの取得を目的としたCisco Networking Academy [2]（以下，CNA）が世界中の教育機関で行われている．CNAにおいては，Packet Tracerと呼ばれるパケットレベルのネットワークシミュレーションソフトウェアが提供されており，ネットワーク技術やネットワークセキュリティ技術に関する演習を行える．しかし，Packet Tracerはシミュレーションソフトウェアであり，特定のOSやアプリケーションの挙動を再現できない．本システムでは，仮想マシンを活用することにより，任意のOSおよびアプリケーションを用いた演習を実施できる．

立岩らは，本システムと同様に仮想マシンを用いた，セキュリティ人材の育成のためのシステムを提案，開発している [3]．このシステムは遠隔演習環境の実現と，攻撃を自動的に行う仮想クラッカとサービスを自動的に利用する仮想ユーザの開発を行うことで，防御方法のみを効率的に学べる演習環境を実現している．また，演習問題で利用するトポロジは自動生成される．これに対して，本システムは，防御手法の理解度向上のために，防御手法に加えて攻撃手法の学習も対象としている．また，あらかじめ用意されたトポロジを用いるだけでなく，対策機器を自由に配置したネットワーク構築も実施可能である．

## 3. 仮想マシンを活用したネットワークセキュリティ学習支援システム

### 3.1 システム概要

本システムは，仮想ネットワークの構築に，これまで当研究室で開発してきたIPネットワーク構築演習支援システムを利用した [4]．本システムでは，これを基にFWやWAFなどを用いた不正アクセス対策に関する演習支援機能を実現している．

本システムの構成を**図1**に示す．本システムでは，User Mode Linux [5] を用いて作成した仮想マシンを仮想的なネットワーク機器（以下，仮想機器）として動作させる．そして，ホストやルータなどの機器どうしを仮想的に相互接続することで，1台のPC上に実機を用いた場合と同様のネットワーク演習環境を構築する．構築したネットワーク上で，FWやWAFといった仮想的な不正アクセス対策機器を動作させることにより，ネットワーク上で実施される攻撃のフィルタリングやログの収集ができる．さらに，仮想ネットワークの定義ファイルを作成することにより，ネットワーク構築作業の中断・再開を可能とする．

本システムのGUIを**図2**に示す．図中，『ネットワーク図表示部』は，仮想ネットワークの物理トポロジを表している．所望の仮想機器を，『機器追加パネル』からドラッグ&ドロップすることで自由に生成，配置できる．現状のシステムでは，仮想機器として，ホスト，ルータ，ハブ，FW，Webサーバを選択できる．なお，WAFはWebサーバ中で設定される．『コンソール部』は，生成した仮想マシ

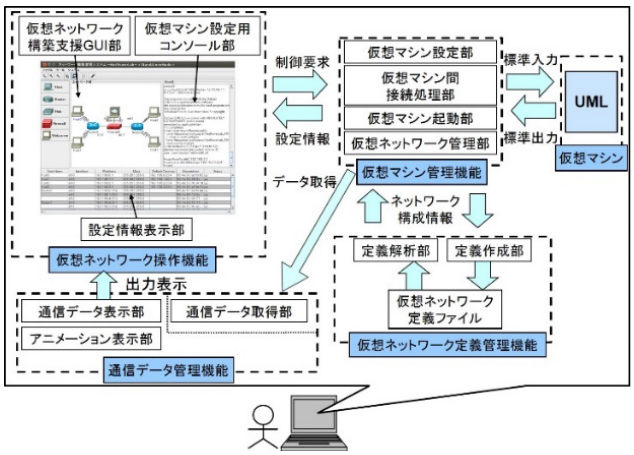


図1 システム構成
**Fig. 1** System overview.

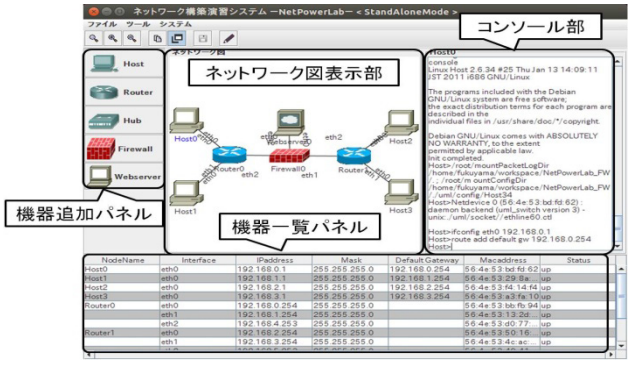


図2 ネットワーク構築支援GUI
**Fig. 2** Network construction support GUI.

ンのターミナルと接続しており，コマンドの入力とその結果が確認できる．『機器一覧パネル』では，各機器の簡易的な設定情報の確認ができる．

このように本システムは GUI による仮想機器の表示，操作が可能であり，本システムを用いずに 1 台の PC 上で複数の仮想マシンを動作させる演習を実施する場合と比べ，手軽な仮想ネットワーク構築や効率的な演習が可能である．以下，仮想機器のうち FW および Web サーバの詳細について述べる．

### 3.2 仮想ファイアウォール

FW は，受信したパケットのフィルタリングやログの収集が可能である．FW を設定したネットワークへの攻撃には，仮想ホストから hping [6] を用いて任意のパケットを自動生成させることで実施する．以下にネットワークセキュリティ学習支援のために実装した FW の機能を説明する．

- 基本設定機能

GUI を用いて，FW のルーティング方法および各インタフェースの IP アドレス，サブネットマスクの設定を行える．

- パケットフィルタリング機能

GUI を用いて，FW のパケットフィルタリングルールを設定できる．設定可能なフィルタリング方式には，静的フィルタリングと動的フィルタリングの 2 種類がある．静的フィルタリングでは，パケットの通過を拒否あるいは許可するための条件を設定する．フィルタリング条件として，ネットワークデバイス，パケットの通過する方向，送信元/宛先ネットワーク，プロトコルの情報を設定できる．動的フィルタリングでは，フィルタリング条件として，構築済みネットワークの中から内部ネットワークとする範囲を設定する．動的フィルタリング適用時，FW は外部ネットワークから受信するパケットのうち，内部ネットワークからの送信パケットに対する応答以外のパケットを拒否する．なお，静的フィルタリングと動的フィルタリングが同時に設定されている場合，静的フィルタリングの設定を優先して処理する．設定したフィルタリング情報は，設定確認用の GUI を用いて適宜確認できる．

- ログ収集・確認機能

FW は受信したパケットの情報を収集し，ログとして保存する．ログは**図 3** に示す GUI により FW のインタフェースごとに確認できる．FW で破棄されたパケットは赤色で強調表示される．また，収集したログはパケットのヘッダ情報をプロトコルのフォーマットに合わせて表示できる．表示形式は簡易表示，詳細表示，16 進数表示の 3 種類がある．16 進数表示は，レイヤ別とフィールド別で色分け表示が可能である．

### 3.3 仮想 Web サーバ

Web サーバは，**図 4** に示す Web 攻撃体験ページを公開


**図 3** ログ表示 GUI
**Fig. 3** Log display GUI.


**図 4** Web 攻撃学習ページ
**Fig. 4** Web pages for learning web attack.

しており，学習者はこのページ内で，SQL インジェクションやクロスサイトスクリプティング（以下，XSS）といった Web 攻撃の体験や，WAF を用いた Web 攻撃のフィルタリング，ログの確認を行える．Web サーバへのアクセスは，Java 用の GUI ツールキットである Standard Widget ToolKit（SWT）[7] を用いて作成したブラウジング機能を利用する．これにより，学習者が利用しているブラウザに依存せず，Web 攻撃体験ページを利用できる．以下に学習支援のために実装した Web サーバの機能を説明する．

- 一般機能

一般機能として，ユーザ登録ページ，ログインページ，パスワード変更ページが用意されている．それぞれ対応するページで，新規ユーザの登録や，登録したユーザ情報を用いた，ログイン認証，パスワードの変更ができる．

- Web 攻撃体験機能

ページ内の脆弱性を利用することで，Web 攻撃を実施する．SQL インジェクションを実施した場合，データベースを不正に参照，改竄，破壊する．また，XSS を実施した場合，不正にセッション情報の確認ができる．

- Web 攻撃フィルタリング機能

Web 攻撃のフィルタリングには，Web サーバ上で動作している WAF を利用する．フィルタリング設定ページで，Web 攻撃を検知した際の処理方法や，フィルタリングしたい Web 攻撃の種類を選択する．選択された攻撃を WAF

が検知した際，そのアクセスを拒否する．

- ログ収集・確認機能

Web 攻撃が実施された際，WAF はログを保存する．学習者は，ログから，攻撃の発生日時や，種類，発生ページなどの詳細情報を確認できる．

## 4. 評価

### 4.1 メモリ使用量と起動時間の評価

まず，本システムで，複数台の仮想機器を用いたネットワークの構築を実施できるか確認するために，メモリ使用量を計測する実験を行った．実験には，一般的な性能の PC（OS：Ubuntu 14.04 64 bit，CPU：Intel（R）Core（TM）i7-3770 CPU @ 3.400 GHz，メモリ：16.00 GB）を用いた．メモリ使用量は，メインシステム起動前と起動後，各仮想機器追加前と追加後のメモリ使用量の差分を，free コマンドを用いて 20 回ずつ計測した．また，手軽に利用できることを示すため，学習用トポロジの作成にかかる時間を計測した．トポロジとしては，ホスト 4 台，ルータ 2 台，FW 1 台，Web サーバ 1 台からなる演習を想定したトポロジ（図 2 ネットワーク図表示部を参照）を用いた．1 台ずつ仮想機器を作成しそれぞれ結線してトポロジを構築した場合と，あらかじめ定義ファイルを作成しておき再現機能を用いてトポロジを構築した場合それぞれのトポロジ作成時間を 10 回ずつ計測した．仮想マシンの起動から仮想マシン設定用コンソール部が表示されるまでの時間をストップウォッチを用いて計測し，トポロジ作成時間とした．

それぞれの計測結果を**表 1**，**表 2** に示す．この結果から，学習に必要な仮想機器を十分な台数を起動でき，定義ファイルの有無によらず，手軽に学習用ネットワークを構築できるといえる．

### 4.2 アンケートによる評価

次に，従来の学習方法に加えて本システムを利用する場合の，学習効果に関する評価を目的として，本学で開講している CNA 修了生 10 名に本システムを利用してもらい，アンケート評価を実施した．アンケートは，各質問項目に対し，1 が最も悪く，5 が最も良いとした 5 段階評価で答えていただき，加えて自由記述形式による回答項目を追加した．質問項目と各項目に対する評点結果を**表 3** に示す．また，自由記述への回答は，次のとおりであった．

- 仮想環境なので自由に攻撃できる．
- アニメーションとログから視覚的にフィルタリング結果が分かりやすい．
- GUI を用いて設定できるため，ベンダ独自の CLI に依存せず学習が可能である．
- 座学だけでは分かりにくかった内容も理解できた．

アンケート結果から，ネットワークセキュリティの学習を行ううえで良好な学習効果を得られると評価できる．また，仮想環境を用いて自由に学習できるといえる．しかし，学習できる攻撃の種類が少ないことや，自身で攻撃した場合，防御箇所の特定が容易で実践的でないという指摘があった．

**表 1** メモリ使用量（単位：MB）
**Table 1** Memory usage.

| 名称 | 平均 | 標準偏差 |
|---|---|---|
| メインシステム | 77.02 | 3.58 |
| ホスト | 23.24 | 7.83 |
| ルータ | 30.50 | 5.45 |
| FW | 29.38 | 7.16 |
| Web サーバ | 225.61 | 28.15 |

**表 2** トポロジ作成時間（単位：秒）
**Table 2** Measurement time for constructing the topology.

| トポロジ構築方法 | 平均 | 標準偏差 |
|---|---|---|
| 1 台ずつ機器を生成し結線 | 25.32 | 1.20 |
| 定義ファイルによる再現 | 18.26 | 1.11 |

**表 3** 評価項目と評点（単位：点）
**Table 3** Evaluation items and scores.

| 評価項目 | 平均 | 標準偏差 |
|---|---|---|
| 攻撃手法の学習に役立つか？ | 3.7 | 1.00 |
| 防衛手法の学習に役立つか？ | 4.2 | 0.60 |
| 実践的スキルの修得に役立つか？ | 3.6 | 0.66 |

## 5. おわりに

本研究では，1 台の PC 上で FW や WAF を動作させた仮想ネットワークを構築するネットワークセキュリティ学習支援システムを開発した．評価の結果，ネットワークセキュリティを学習するうえで良好な学習効果を得られることが分かった．しかし，実践的な学習を行ううえで課題が残されていることが分かった．

今後の課題として，実施可能なネットワークセキュリティ演習の追加，また，より実践的な学習の支援のために，本システムに，決まったパターンの攻撃を自動的に実施する攻撃者エージェントを組み込むことを考えている．

### 参考文献

[1] 平成 26 年度不正アクセス行為対策等の実態調査，入手先 ⟨http://www.npa.go.jp/cyber/research/h26/h26countermeasures.pdf⟩ (Jan. 2015).
[2] Cisco Networking Academy, available from ⟨http://www.netacad.com/⟩ (Oct. 2015).
[3] 立岩佑一郎，岩崎智弘，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システム，電子情報通信学会論文誌，Vol.J96-D, No.7, pp.1585–1594 (2013).
[4] 井口信和：仮想ルータを活用したネットワーク構築演習支援システムの開発，情報処理学会論文誌，Vol.52, No.3,

pp.1412–1413 (2011).
[5] User-Mode-Linux, available from ⟨http://user-mode-linux.sourceforge.net/⟩.
[6] Hping, available from ⟨http://www.hping.org/⟩.
[7] SWT, available from ⟨https://www.eclipse.org/swt/⟩.

**福山 和生** （学生会員）

2014 年近畿大学理工学部卒業．同年同大学大学院総合理工学研究科博士前期課程入学，現在に至る．ネットワークセキュリティの学習支援に関する研究に従事．

**谷口 義明** （正会員）

2008 年大阪大学大学院情報科学研究科博士後期課程修了，博士（情報科学）．2014 年より近畿大学理工学部講師となり現在に至る．センサネットワーク，無線ネットワークに関する研究に従事．電子情報通信学会，画像電子学会，IEEE 各会員．

**井口 信和** （正会員）

1988 年三重大学大学院修士課程修了．同年（株）豊田自動織機製作所入社．1992 年和歌山工業技術センター研究員．2001 年大阪大学大学院基礎工学研究科博士後期課程修了，博士（工学）．2002 年近畿大学理工学部情報学科助教授．2008 年同大学教授となり，現在に至る．近畿大学総合情報基盤センター長を兼務．情報ネットワーク応用，教育システム開発，農業 ICT に関する研究に従事．電子情報通信学会，農業情報学会，教育システム情報学会，IEEE 各会員．