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における攻撃者エージェントの実装と評価

福山和生[†1]　谷口義明[†2]　井口信和[†2]

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等を背景に，ネットワークセキュリティ教育の重要性及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等が障壁となる．我々の研究グループでは，これまでに，仮想マシンを活用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学習を行えるシステムを提案してきた．本報告では，防御手法に関する実践的な学習を実施できるよう，本システムに，仮想ネットワーク上で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実装した．評価実験の結果，本システムを用いることにより，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．

Implementation and Evaluation of Attacker Agent in Virtual Machine-based Network Security Learning System

KAZUKI FUKUYAMA[†1]
YOSHIAKI TANIGUCHI[†2]　NOBUKAZU IGUCHI[†2]

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 computer networks for practice. We have developed a low-cost, easy and safe learning support system for network security by utilizing virtual machine technologies. In this report, we implement an attacker agent that automatically attacks virtual network devices in a fixed pattern for practical learning of defense techniques. Through evaluations, we show that our system can provide practical environment for learning network security.

1. はじめに

インターネットの普及に伴い，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知識，実践的スキルを有する技術者を育成することを目的として，種々の大学が連携してセキュリティ技術者を育てる教育プログラムである SecCap [2]や，ネットワークセキュリティに関するコンテストである SecCon [3]など，さまざまな試みが行われている．このように，ネットワークセキュリティに関する実践的スキルを取得するためには，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．ネットワークセキュリティに関する演習は，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，独立した演習用ネットワークを用いて行うことが望ましい．しかし，演習用環境を構築するためには，ルータ，サーバ等の機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るため，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，我々は，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 サーバ等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，安全かつ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）を検討してきた [4]．これまでに，不正アクセス対策機器であるファイアウォール（以下，FW）に関する演習を行える機能や Web アプリケーションファイアウォール（以下，WAF）に関する演習を行える機能を開発し，その有効性を示してきた．本システムを用いることにより，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可能である．

本報告では，本システムを用いることにより実施可能な

†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
†2 近畿大学理工学部情報学科
Department of Informatics，Faculty of Science and Engineering，Kinki University

ネットワークセキュリティ演習の整理を行う．また，攻撃手法の学習および，防御手法の実践的かつ効率的な学習を実現するために，決まったパターンの悪意ある攻撃を実施する攻撃者エージェントを本システムに実装する．また，実装したシステムを，負荷や学習効果の観点から評価する．

本報告の構成は以下の通りである．まず，2 章で関連研究の紹介を行い，3 章でこれまで開発してきたシステムについて述べる．4 章で今回実装した攻撃者エージェントについて述べ，5 章で開発したシステムの性能評価およびアンケートによる評価結果を示す．最後に 6 章で本報告のまとめを述べる．

2. 関連研究

セキュリティ人材の育成を目的とした学習環境や，仮想マシンを利用した学習システムが開発されている．

IPA（情報処理推進機構）は，ウェブアプリケーションや，サーバ・デスクトップアプリケーションの脆弱性について学習できる，脆弱性体験学者ツール APPGoat [5]を提供している．このツールは，学習に Web ブラウザを利用する．学習者は，ツール内の教材から攻撃のテーマに合わせた概要や，原理について学習した後，実際にツール内で攻撃演習を実施する．攻撃演習完了後，その攻撃の影響や，対策方法についてさらに教材で学習する．最後に，Web ページのソースプログラムを修正することで，脆弱性を無くし，それに対応した解答を確認する．これに対して本システムは，Web 攻撃だけでなく，さまざまなネットワーク攻撃を学習の対象としている．また，脆弱性対策に関しては，ページ内のソースプログラムの修正による対策ではなく，不正アクセス対策機器を活用したフィルタリングによる対策や，機器内のログによる確認を学習の対象としている．

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 等の取得を目的とした Cisco Networking Academy [6]（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 [7]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，任意の OS やアプリケーションの挙動を再現できない．これに対して本システムでは，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 [8]．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ーおよび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．

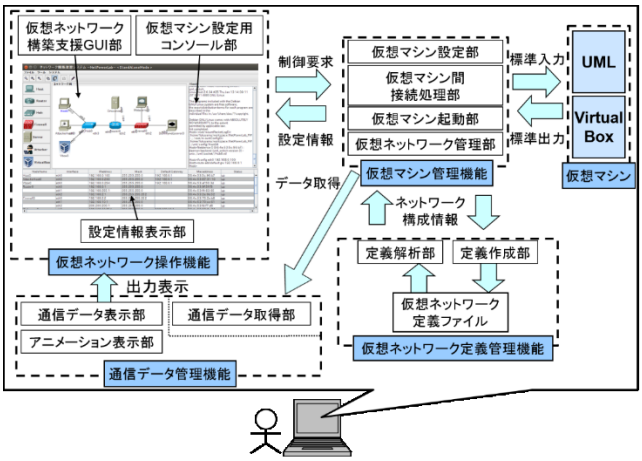

図 1　システム構成
Figure 1　System overview.

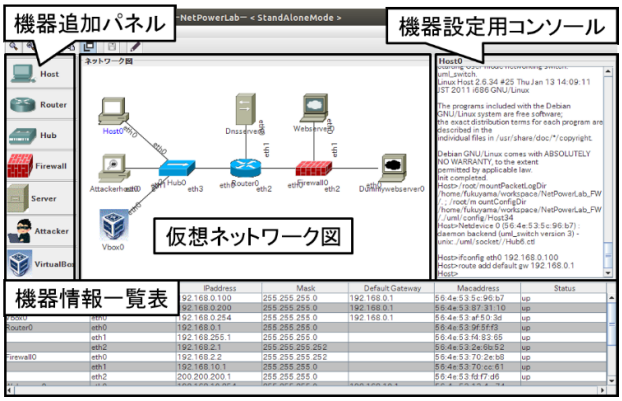

図 2　ネットワーク構築支援 GUI
Figure 2　Network construction support GUI.

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

我々がこれまでに開発してきたシステムの概要および本システムを用いることにより実施可能な演習項目を述べる．

3.1 システム概要

本システムの構成を図 1 に示す．本システムは，Java をベースに開発している．本システムでは，User Mode Linux [9]（以下，UML）と Oracle VM VirtualBox [10]（以下，VirtualBox）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同士を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仮想的な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 といった仮想的な対策機器を動作させることで，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，ネットワークの定義ファイルを作成することで,ネットワーク構築作業の中断･再開を可能とする．

本システムはネットワークの構築作業に図 2 の GUI を用いる．画像中,『仮想ネットワーク図』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，仮想ネットワークに仮想機器を自由に追加，配置できる．現状のシステムでは，UML を用いた仮想機器として，ホスト，ルータ，ハブ，FW，Web サーバ，ダミーWeb サーバ，DNS サーバ，攻撃用ホストを選択できる．さらに，VirtualBox を用いて任意の OS で動作させた仮想機器を利用できる．なお，WAF は Web サーバ中で設定される．『機器設定用コンソール』は，生成した仮想機器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.『機器情報一覧表』では,各機器の簡易的な設定情報の確認ができる．

上述の通り本システムは UML と VirtualBox の 2 つの仮想化技術を利用している．これらの違いをまとめたものを表 1 に示す. UML は VirtualBox に比べてリソース消費量が少ない．しかし，利用できる OS は LINUX ベースのもののみと限られている．さらに，GUI が提供されておらず操作は CLI のみとなっている．これに対して，VirtualBox はリソースの消費量は UML よりも多いが,利用できる OS に制限はなく，GUI を用いた操作も可能である．そこで本システムでは，それぞれの利点を生かすことで，リソースの消費量を最低限に抑えつつ， 任意の OS およびアプリケーションを用いた演習の実施を可能にしている．

3.2 実施可能なネットワークセキュリティ演習

本システムを用いることにより実施可能なネットワークセキュリティ演習を述べる．IPA 情報セキュリティスペシャリスト試験 [11]，SecCap プログラム演習等を参考に，コンピュータネットワークを用いた演習を必要とするネットワークセキュリティに関する演習項目を表 2 に整理した．本システムによって演習を実施できる項目を◎，現状演習を実施できないが実装が容易な項目には○を記している．なお，ネットワークセキュリティの学習においては，マルウェアや無線 LAN に関するセキュリティも重要である．しかし，マルウェアは，ウイルス定義ファイルや OS，ソフトウェアを最新の状態にアップデートすることが基本的な対策となるため学習に不向きである．また，仮想化技術の仕様上，仮想機器間で無線 LAN を利用した通信の実現が困難であるため,これらの学習項目を演習の対象外とした．以下，各演習項目に関する説明を行う．なお，文中の FW や WAF の持つ機能に関しては,参考文献 [4]を参照されたい．

表 1　仮想化技術の比較

Table 1　Comparison of virtualization technologies

	仮想化技術名	
対象項目	UML	VirtualBox
リソース消費量	少ない	多い
GUI の有無	なし	あり
利用できる OS	LINUX のみ	制限なし

表 2　演習が必要な項目

Table 2　Necessary exercises

演習内容	実施の可否
ポートスキャン	◎
DoS 攻撃	◎
ARP スプーフィング	◎
DNS スプーフィング	◎
Web アプリケーション攻撃	◎
セッションハイジャック	○
バッファオーバーフロー攻撃	○

- ポートスキャン

仮想攻撃用ホストからポートスキャンを実施可能である．また，仮想 FW を動作させ，専用の GUI を用いて不要なポートへのアクセスを遮断することにより，ポートスキャンによる対策を行う演習を実施できる．また，ログによりフィルタリングの結果を確認できる．

- Web アプリケーション攻撃

本システムにおける仮想 Web サーバは, Web 攻撃体験ページを公開している．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といった攻撃の演習や, WAF を用いたフィルタリング，ログの確認ができる．

- DoS 攻撃

仮想攻撃用ホストから別の仮想ホストに対して DoS 攻撃の一つである SYN Flood 攻撃を行った場合に，経路上にある仮想ルータ等で TCP SYN パケットが流れる様子をアニメーションで確認できる．また，エンドホストでの iptables の設定や，仮想 FW 上でフィルタリングの設定等の対策を実施できる．

- ARP スプーフィング

攻撃対象となった機器宛のパケットが攻撃用ホストに転送されるよう偽の ARP 応答を流すことにより, 通信パケットを盗聴する演習を実施可能である．また，ARP テーブルを静的に設定することにより，ARP テーブルのエントリの上書きを禁止することによる盗聴対策を実施できる．

- DNS スプーフィング

上述の ARP スプーフィングにより，仮想 DNS サーバを経

由することなく偽の名前解決を行い，攻撃者が事前に用意した仮想ダミーWeb サーバへアクセスさせる演習を実施できる．また，攻撃実施前と実施時における同一ドメイン名の名前解決の変化を確認できる．

- セッションハイジャック

仮想 Web サーバと仮想ホスト間のセッションにおいて，URL，クッキー，hidden フィールドなどのセットされたセッション管理情報を，仮想攻撃用ホストからネットワークツールを用いて盗聴できる．この結果から，仮想攻撃用ホストで偽装パケットを生成し，正規の仮想 Web サーバと仮想ホスト間のセッションをハイジャックする演習を実施できる．また，仮想 Web サーバでセッション ID の複雑化や，暗号化，WAF の設定を行うなどによるセッションハイジャック対策を実施，確認できる．

- バッファオーバーフロー攻撃

仮想 Web サーバや仮想 DNS サーバ上で稼働するプログラムの脆弱性を利用することで，仮想攻撃用ホストで root 権限を奪取する，といった演習を実施可能である．この対策のため，プログラム上でバッファオーバーフローが起こらないようソースコードを修正するなどの学習も実施できる．

以上より，本システムを用いることで，多くのネットワークセキュリティに関する演習を実施可能であることが分かる．これは，本システムでホストやルータ等の機器を実現するために仮想化技術を用いており，任意の OS やアプリケーションを導入可能なためである．

4. 攻撃者エージェントの検討と導入

本システムでは，実装済みの学習支援機能を利用し，学習者が防御手法の実施前後のネットワークに対して自身で攻撃を行うことにより，攻撃手法と防御手法の学習が可能である．しかし，その場合想定された攻撃しか発生しないため，実践的な防御手法の学習が行えない．また，防御手法の学習項目毎に毎回攻撃を実施しなければならないため，学習の効率が悪いなどの問題がある．そこで，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，本システムで作成した仮想ネットワーク上で動作させることで，　実践的で効率的な防御手法の学習環境を提供する．

攻撃者エージェントは，本システムにおける仮想攻撃用ホスト上で動作する．攻撃者エージェントを用いた演習イメージを図 3 に示す．図 3 では，FW の内側の『LAN』，外側『外部ネットワーク』，またその間にどちらにも含まれない『DMZ』から構成された仮想ネットワークを利用している．最初に学習者は，自身で仮想機器を設置・結線する，あるいは指導者から与えられた仮想ネットワーク設定ファイルを読み込むことにより，ホストやルータ，FW，サーバ，攻撃用ホスト等から構成される仮想ネットワークを生成する（図 3（a））．この時，攻撃用ホストは FW の内部と外部のどちらに配置しても良い．なお，図 3 の例では攻撃用ホストは外部ネットワークに配置されている．次に，攻撃者エージェントを動作させることで仮想ネットワーク上の各機器へ自動的に攻撃を実施する（図 3（b））．この時，学習者は，攻撃前後における各機器の設定情報の変化や，FW や WAF 等の仮想機器のログを確認することで，攻撃者エージェントにより攻撃された箇所や，攻撃の種類，生成した仮想ネットワークの脆弱性，問題点などを特定する（図 3（c））．最後に，これらの特定した脆弱性，問題点等に基づいて，学習者は，ホストやルータの設定内容や FW や WAF のフィルタリングルールの修正等など各攻撃に適した対策を施す（図 3（d））．そして，ログを再び確認することで，正しく対策が行えているか，対策手法の正当性を確認する．全ての対策が完了すると，対策完了を示すアラートが表示され，演習が終了される．

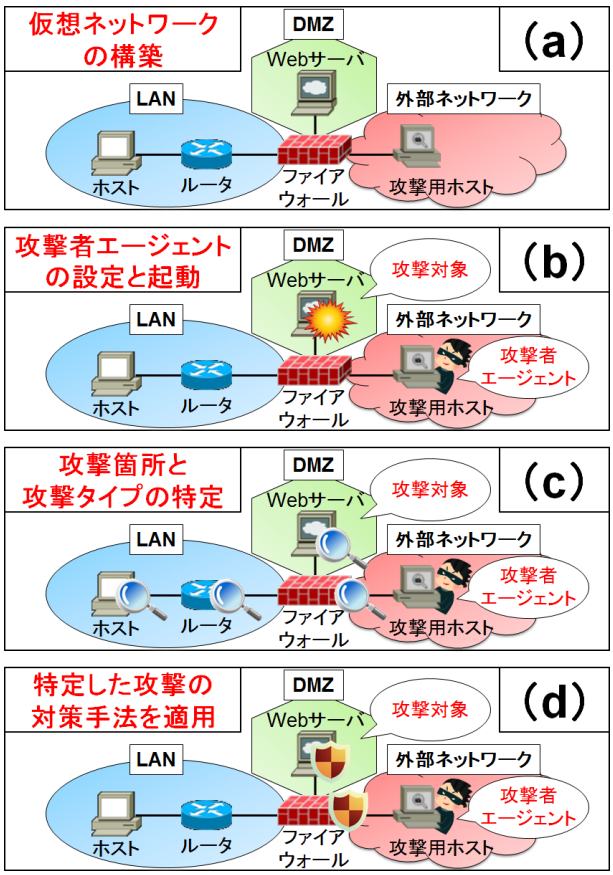

図 3　攻撃者エージェントを用いた演習イメージ

Figure 3　Exercise image by our system with attacker agent.

仮想攻撃用ホストには攻撃に必要なツールがあらかじめ複数備わっており，攻撃者エージェントはこれらのツールを攻撃に利用する．学習者は，仮想ネットワーク上に設置した仮想攻撃用ホストを右クリックして図 4 の GUI を表示，設定する等により，攻撃者エージェントから発生させる攻撃の種類を選択できる．また，GUI より学習者が自動攻撃機能を有効にすることで，指導者があらかじめ用意したスクリプトファイルが読み込まれ攻撃が開始される．攻撃は

選択された攻撃の中からランダムに順次実行される．

実際に攻撃を行う際，理論上のセキュリティホールがあっても，情報無しに特定のネットワークやホストに攻撃を成功させるには情報の収集に時間がかかる．これを回避するため，攻撃者エージェントに学習者が設定したインターフェースやデフォルトゲートウェイなどの情報を盗み見る機能を設けている．これにより，無駄の少ない効率的な攻撃が可能である．

全ての学習者が容易に攻撃の特定や対策，ログの確認ができるわけではない．これを解決するため，本システムでは，ヒントを提供する機能を用意している．ヒントの形式は 2 種類ある．1 つは現状実施されている攻撃の種類に基づいて，対策方法を提示する形式である．ヒントは攻撃毎に 3 段階ずつ用意されており，被害を受けている箇所の情報，実施されている攻撃の種類の情報，対策に必要な設定手順の情報の順番で 1 つずつ表示される．学習者は必要な最低限のヒントを活用することで，演習を達成できる．もう 1 つは，攻撃を終了したかどうかをログやツールから判断できない場合に利用する形式である．この形式のヒントでは，現状対策が完了している攻撃の一覧が表示される．これにより，学習者は自身の対策の正当性を確認できる．

攻撃者エージェントを用いた演習では，防御手法の学習における理解度向上のため，学習する上で必要な禁止事項をいくつか設けている．例えば，攻撃を受けている機器のネットワークを孤立させることも攻撃を回避する一つの方法であるが，対策機器などを用いた防御手法の学習を重要としているため，演習においては禁止行為とみなす．勿論，攻撃者エージェントが実行される仮想攻撃用ホストを削除することも禁止行為である．もし，こういった禁止行為に該当した場合，設定を無効化し，アラートを表示させる．

5. 評価

5.1 メモリ使用量と起動時間の評価

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：

図 4　攻撃タイプ選択 GUI
Figure 4　Attack type selected GUI

表 3　計測結果
Table 3　Measuring result.

対象名	メモリ使用量（MB） 平均	メモリ使用量（MB） 標準偏差	起動時間（秒） 平均	起動時間（秒） 標準偏差
メインプログラム	78.88	4.50	1.01	0.11
ホスト	25.38	4.61	4.37	0.12
ルータ	35.02	2.14	6.54	0.12
ハブ	9.77	2.19	0.14	0.02
FW	35.07	2.67	6.67	0.14
Web サーバ	235.92	24.11	25.25	0.70
ダミーWeb サーバ	257.29	16.87	25.86	0.70
DNS サーバ	123.49	20.03	12.45	0.34
攻撃用ホスト	22.94	2.77	17.79	0.28

Ubuntu 14.04 64bit，CPU：Intel（R）Core（TM）i7-3770 CPU@ 3.400GHz，メモリ：16.00GB）を用いた．メモリ使用量は，メインプログラム起動前と起動後，各仮想機器生成前と生成後のメモリ使用量の差分を，Linux の free コマンドを用いて 10 回ずつ計測した．また，本システムが手軽に利用できる事を示すため，VirtualBox を除く各仮想機器生成後から，コンソール部の入力が可能になるまでの時間をストップウォッチで計測した．VirtualBox を用いた仮想機器は，起動させる OS の種類によって必要なメモリ消費量や起動時間が大きく変動するため，実験の対象外としている．

それぞれの計測結果を表 3 に示す．各サーバの仮想機器は，他の仮想機器と比べてメモリ使用量が比較的多い．しかし，本システムでは，各サーバの同時起動台数は 1 台までと想定しており，演習では，ホストやルータ，ハブなどのメモリ使用量が少ない仮想機器を中心にネットワークを構築することになる．そのため，演習に必要な仮想機器を充分な台数起動できると考えられる．また，いずれの仮想機器も起動時間が 30 秒に満たなかった．さらに，本システムは演習終了時に片付けに時間を要しない．これに対して実機を用いてネットワークを構築する場合，箱に収納されている各機器の準備と片付けに 1 台当たり約 5 分程度の時間を要してしまう．この結果から，本システムは準備や片付けにかかる時間を削減し手軽に学習用ネットワークを構築できると言える．

5.2 アンケートによる評価

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った．実験では，ホスト，ルータ，FW，Web サーバ，ダミーWeb サーバ，DNS サーバ，攻撃用ホスト，VirtualBox の仮想機器各 1 台ずつから構成されるネットワーク（図 2 上の仮想ネットワークと同様）を用いて，3.2

節で説明した実施可能なネットワークセキュリティ演習をそれぞれ行った．また，VirtualBox の仮想機器上で動作させる OS には，ペネトレーションテストに特化した Linux ディストリビューションである Kali Linux を用いた．

今回の実験では，最初に，実装済みの機能やツールを用いて手動で攻撃を行ってもらい，攻撃の原理を確認してもらった．次に，攻撃者エージェントによる自動攻撃を開始させ，防衛演習を行った．演習では，自身で攻撃の特定や対策，およびログの確認をすることで，被害の影響や，対策後の変化を確認してもらった．最後に，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 段階評価で答えて頂き，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 4 に示す．(1) ~ (3) までの全ての項目でおおむね良好な評価が得られた．中でも，(3) の項目で高い評価を得られことから，本システムは実践的な学習に対応できていることが分かった．

また，自由記述への回答は，本システムで実施可能な攻撃手法と防御手法の演習について，

- 攻撃に必要な時間を，対策のために使えて効率が良い．
- 自分で攻撃を行うことで，防御手法の理解に繋がった．
- 任意のタイミングで攻撃の開始や停止が出来るため，対策状況別の攻撃の影響を把握できた．
- さまざまな攻撃が次々と行われるため，総合的な防衛演習ができた．

などの意見が得られた．以上より，攻撃者エージェントを用いることで，実践的かつ効率的な学習に対応でき，また攻撃手法を体験する演習を取り入れたことで，防御手法の理解に繋けることができたと言える．

しかし，実施できる演習のバリエーションが少ないという指摘があった．これに関しては，現状実装予定の演習，および実装済みの演習でも現状とは異なる攻撃手法，防御手法の追加が必要となる．また，攻撃の演習の難易度を学習者が選択できた方が良いという指摘があった．本システムでは，攻撃者エージェントによる自動攻撃を実施する際，学習者が選択した攻撃の種類にのみ応じて，あらかじめ用意したスクリプトファイルを動作させている．そのため，学習者の理解度に関わらず，同一レベルの演習が開始される．このため，慣れてくると物足りなくなるという意見が得られた．そこで，自動攻撃開始時に，演習の難易度を変更できる機能の追加が必要である．

6. おわりに

本研究では，我々が開発している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において，防御手法の実践的な学習を実現するため，決まったパターンの悪意のある攻撃を自動的に実施する，攻撃者エージェントを検討し，実装した．評価の結果，攻撃者エージェントを用いることにより，防御手法に関する実践的，効率的な学習を行えることが分かった．しかし，実践的な学習を行う上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や，学習者の理解度に応じて難易度を変更できる機能の追加を予定している．さらに，当研究室でこれまで開発してきた，クラウド環境を利用することで複数の学習者が協調してネットワークの構築演習を実施できるシステムに本システムを移行することを検討している [13]．これにより，複数の学習者が同時に 1 つのネットワーク上でネットワークセキュリティの攻防戦を実施することや，攻撃者エージェントを動作させた環境において他の学習者と協力したトラブルシューティングが可能となり，より実践的な演習に対応できると考えている．

表 4　評価項目と評点（単位：点）

Table 4　Evaluation items and scores.

評価項目	平均	標準偏差
(1) 攻撃手法の学習に役立つか	3.7	0.90
(2) 防衛手法の学習に役立つか	3.9	0.83
(3) 実践的スキルの修得に役立つか	4.0	1.10

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: http://www.npa.go.jp/cyber/research/h26/h26countermeasures.pdf, Jan. 2015.
2) SecCap: http://www.seccap.jp/
3) SecCon: http://www.seccon.jp/
4) 福山和生,谷口義明,井口信和,“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における攻撃者エージェントの検討”，信学技報, vol. 114, no. 305, ET2014-67, pp. 37-42, Oct. 2014.
5) 脆弱性体験学習ツール AppGoat: http://www.ipa.go.jp/security/vuln/appgoat/
6) Cisco Networking Academy: http://www.netacad.com/
7) Packet Tracer: https://www.netacad.com/about-networking-academy/packet-tracer
8) 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, July 2013.
9) User-mode Linux: http://user-mode-linux.sourceforge.net/
10) Oracle VM VirtualBox: http://www.oracle.com/technetwork/jp/server-storage/virtualbox/overview/index.html
11) 情報セキュリティスペシャリスト試験(SC): https://www.jitec.ipa.go.jp/1_11seido/sc.html/
12) Kali Linux: https://www.kali.org/
13) 北澤友基,越智洋司,溝渕昭二,井口信和,“クラウド環境を利用した協調演習を可能とする IP ネットワーク構築演習支援システムの検討”，信学技報, vol. 112, no. 66, ET2012-4, pp. 19-24, May 2012