仮想マシンを用いた 攻防戦型ネットワークセキュリティ学習支援システムにおける ネットワーク型 IDS を用いた不正侵入シナリオの実装

湯川誠人[†1]　井口信和[†2]

概要：不足するセキュリティ技術者の養成を目的として，ネットワークセキュリティ教育が広く実施されている．ネットワークセキュリティ教育において，防御の視点のみでなく攻撃の視点を加えた学習を行い，防御手法の理解をより促すことが望まれている．そのため，攻防戦型演習などの両側の視点を学べる演習が有効とされている．しかし，この演習を行う際，安全面に問題がある場合がある．そこで，我々は仮想マシンを用いることにより安全に両側の視点を学べる演習を行えるシステムを開発してきた．本稿では，本システムで行える演習をより充実させるために，不正侵入シナリオを実装した．また，不正侵入に気づく手段としてネットワーク型 IDS を実装した．性能評価実験の結果，本システムにこれらを実装した場合においても問題なく演習を行えることを確認した．また，動作検証の結果，不正侵入シナリオとネットワーク型 IDS が正しく動作することを確認した．さらに，利用評価実験の結果，ネットワーク型 IDS の有用性を確認した．

キーワード：ネットワークセキュリティ，仮想マシン，学習支援，ネットワーク型 IDS

Implementation of Fraudulent Access Scenario Using Network-based Intrusion Detection System on Virtual Machine-based Network Security Learning System Enabling Offensive and Defensive Battle Exercise

MAKOTO YUKAWA[†1]　NOBUKAZU IGUCHI[†2]

Abstract: Network security education is widely practiced for the purpose of training missing security engineers. In network security education, it is desired to promote understanding of defense methods by conducting learning with not only defensive viewpoint but also attack viewpoint. Therefore, exercises to learn the viewpoints of both sides such as battlefield exercises are considered effective. However, for this exercise, some problems of safety are pointed out. Therefore, we have developed a system that can conduct exercises that can safely learn viewpoints of both sides by using virtual machines. In this paper, we implemented fraudulent access scenario to further improve the exercises that can be done with this system. In addition, we implemented network-based IDS as a method of noticing fraudulent access. Through the performance evaluation experiment, we confirmed that exercises with this system can be done without problems. Also, through operation verification, we confirmed that fraudulent access scenario and network-based IDS operate correctly. Further through utilization evaluation experiment, we confirmed the usefulness of network-based IDS.

Keywords: Network security, Virtual machine, Learning support, Network-based IDS

1. はじめに

警察庁が 620 の組織を対象に行った調査によると，不正アクセス行為に対する脆弱性調査を実施していない組織は約 58%と，5 割を上回っている[1]．その原因として，予算やセキュリティ技術者の不足などが挙げられる．セキュリティ技術者の不足に関して，2020 年にはセキュリティ技術者の不足数が 20 万人弱に拡大すると予測されている[2]．また，日本におけるセキュリティ技術者約 26.5 万人の内，約 16 万人がスキル不足とされており，高いスキルを身につけた技術者の育成が求められている[3][4]．この現状の改善には，不正アクセス対策などのネットワークセキュリティ教育を各組織が実施し，セキュリティ技術者を育成する必要がある．

さらに総務省の報告によると，1 年間で観測されたサイバー攻撃回数が 3 年で約 10 倍に増えている[5]．このように，サイバー攻撃の増加やその複雑さ[5]から，従来の学習のみでは実際に攻撃を防ぐことが難しくなっている．その解決には，防御の視点のみでなく，攻撃の視点から攻撃の性質などを学び，それを防御に活かすことが必要である[6]．両側の視点でセキュリティを学べる演習として，攻防戦型の演習である Capture The Flag[7][8]がある．しかし，このような攻防戦型の演習を実環境で行う場合，運用しているネットワークに支障をきたすおそれがある．また，実機を新たに用意して演習を行う場合においても，実機のソフト

†1 近畿大学大学院　総合理工学研究科
Graduate School of Science and Engineering Research, Kindai University
†2 近畿大学　理工学部　情報学科
Department of Informatic, Faculty of Science and Engineering, Kindai University

ウェアや内部の情報に支障をきたすおそれがある．

そこで，我々はこれまでに 1 対 1 で行う攻防戦型演習を可能とする仮想マシンを用いたネットワークセキュリティ学習支援システム（以下，本システム）を開発してきた[9]．本システムは実機の代わりに仮想マシンを用いることで，安全に攻防戦型の演習を行える環境を提供する．これにより，従来の学習に攻撃の視点を加えた学習が可能なセキュリティ技術者教育の支援を可能とした．

本稿では，本システムで行える演習をより充実させるため，不正侵入に関する演習を行えるようにした．JPCERT/CC の報告によると，報告を受けたインシデントの中で，未遂に終わった不正侵入に関する行為が含まれるスキャンの件数が 1164 件と，フィッシングサイトの次に多い[10]．また，その他には実際に不正侵入が成功した件数も含まれている[10]．これらから，未だ不正侵入に関する脅威は存在する．よって，不正侵入に関する演習を行うことは有意義である．不正侵入に関する演習を行うことで，学習者は不正侵入に関する理解を深めることが可能となる．

不正侵入に関する演習において，不正侵入に気づく手段は必要である．現状，本システムを用いてこの演習を行う場合，防御側は tcpdump を用いてパケットを常に監視し，防御側自身で不審なパケットを検知する方法が挙げられる．しかし，本システムの利用対象者は IT 分野の学生および新入社員など，セキュリティに関する知識が不足している学習者であるため，不審なパケットとそうでないパケットを見分けられない場合がある．この問題に対して，我々は Network-based Intrusion Detection System（以下，NIDS）を新たに実装した．NIDS は，通過するパケットを監視し，その解析を行う．解析の結果，不審だと判断した場合，そのパケットに関する情報を記録し，管理者に通知を行う．NIDS により，防御側は不審なパケットが仮想ネットワーク内に流れたことを知ることが可能となる．また，tcpdump を用いて検知できなかった不審なパケットも検知可能となる．さらに，防御側は NIDS が記録した不審なパケットに関する情報と tcpdump の出力結果を見比べることで，どのようなパケットが検知対象になるか知ることが可能となる．

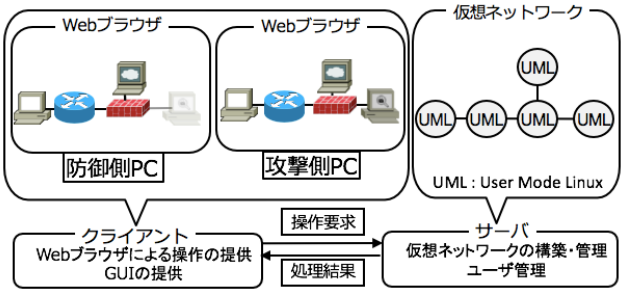

図 1　本システムの構成図

Figure 1　System configuration diagram

以上より，NIDS を用いて不正侵入に関する演習を行うことで，防御側は NIDS の性質や不正侵入に対する防御方法の学習などが可能となる．

本稿は，以下の構成の通りである．まず，2 章で本研究に関連する研究について述べる．そして，3 章でこれまでに開発してきた本システムについて述べる．4 章で本システムを用いた演習の流れについて述べる．5 章では，本稿で新たに実装した NIDS と不正侵入シナリオについて述べる．6 章で本システムの性能評価実験と本稿で新たに実装した NIDS と不正侵入シナリオの動作検証，NIDS の利用評価実験について述べる．最後に，7 章でまとめについて述べる．

2. 関連研究

本システムに関連した研究として，立岩らがセキュリティ人材の育成を目的として開発した仮想化技術を用いたセキュリティ演習システムがある[11]．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を利用することで，防御方法を効率的に学べる演習を実現している．また，演習で利用するネットワークトポロジはあらかじめ決められている．これに対して，本システムは攻撃の視点から得た攻撃の性質などを防御に活かすために，防御方法のみでなく，攻撃方法も学習対象とする．また，ネットワークトポロジをあらかじめ決めて行う演習のみでなく，自在に仮想ネットワークを構築して行う演習も可能なため，演習のバリエーションが豊富となる．

また，Walden らも，セキュリティの概念と技術に関して理論的および実践的な理解の習得を目的に仮想化技術を用いてセキュリティ演習環境を提供している[12]．これは，Capture The Flag 形式となっており，防御方法と攻撃方法を学習対象としている．また，演習時に使用するツールの入手は学習者に委ねている．そのため，利用対象者は安全なツールの取捨選択が可能な，セキュリティに関する知識を一定以上持つ学習者となっている．これに対して，本システムの利用対象者は IT 分野の学生および新入社員など，セキュリティに関する知識が不足している学習者を対象としている．そのため，本システムは安全なツールをあらかじめ仮想マシンに導入している．これにより，学習者は安全なツールの取捨選択を行う必要はなくなり，安全にセキュリティ演習の実施が可能となる．

3. 仮想マシンを用いた攻防戦型ネットワークセキュリティ学習支援システム

本章では，我々がこれまでに開発してきた本システムについて述べる．はじめに，本システムの概要について述べる．次に，本システムの既存機能について述べ，最後に実施可能な演習項目について述べる．

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，ネットワーク構築演習支援システム[13][14]を基盤技術として活用し，仮想的なネットワークの構築・管理やユーザの管理などを行うサーバと，ユーザインタフェースを提供するクライアントから構成される．サーバは，User Mode Linux（以下，UML）[15]と呼ばれる仮想化技術を用いて複数の仮想マシンを作成する．作成した仮想マシンは，Host またはネットワーク機器（以下，総称して仮想機器）として動作させる．そして，複数の仮想機器を相互に接続し，通信させることで，仮想的にネットワークの構築を可能とする．学習者は，PC 端末上にある Flash Player[16]を導入した Web ブラウザを用いてクライアントを操作する．クライアントは，学習者が操作した内容を操作要求としてサーバに送信する．サーバは，受信した操作要求の処理を行い，その結果をクライアントに送信する．クライアントは，受信した処理結果を Web ブラウザに表示する．

本システムのクライアントが提供している攻防戦型ネットワークセキュリティ演習画面を図 2 に示す．ネットワーク図表示部は，構築しているネットワークのトポロジを表示する．また，機器追加パネルから，対象の仮想機器のアイコンをネットワーク図表示部にドラッグ&ドロップすることで，そのアイコンがネットワーク図表示部に表示される．表示されると同時に仮想機器が起動し，その起動のログがコンソール部に表示される．また，ネットワーク図表示部に表示されている仮想機器間にある直線は，結線を表している．コンソール部は，仮想機器のターミナルと接続されており，その仮想機器に対してコマンドの発行を可能とする．また，発行したコマンドやその発行結果の確認も可能とする．チャット欄は，演習を行っているもう一方の学習者とのチャットを可能とする．演習補助パネルは，ヒントの表示と攻撃開始や仮想ネットワーク構築完了の通知を可能とする．また，制限時間の設定・表示を可能とする．ヒントの表示の詳細については，3.3 節で述べる．

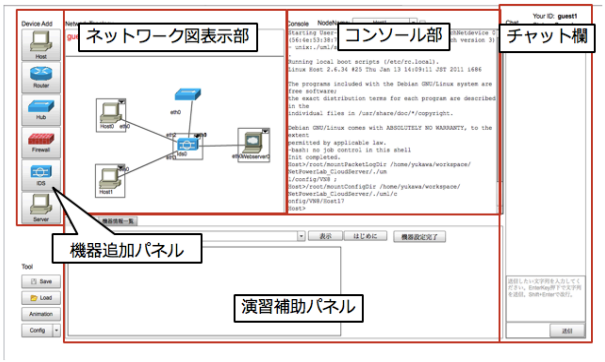

図 2　ネットワークセキュリティ演習画面（防御側）
Figure 2　Network security exercise GUI (defending side)

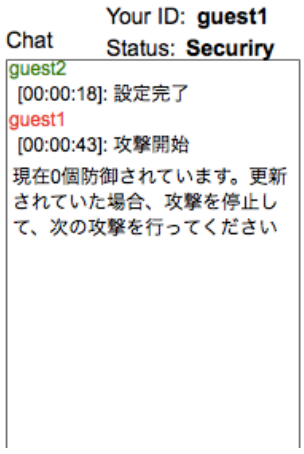

図 3　演習状況（攻撃側）
Figure 3　Exercise situation (attacking side)

3.2 攻防戦型セキュリティ演習機能

攻防戦型セキュリティ演習機能は，2 人の学習者が攻撃側と防御側に分かれて演習を行うことを可能とする機能である．防御側が演習を行う目的は，攻撃における性質の理解である．また，攻撃に対してどのような対応を取るべきかの理解と理解した上で各仮想機器に導入しているツールなどを用いて，仮想機器に適切な防御コマンドを発行できるようになることも目的としている．これらを通じて，使用する仮想機器における性質の理解も目的としている．攻撃側は，攻撃における性質の理解を目的としている．

防御側は，仮想機器を用いて仮想ネットワークを構築する．また，仮想機器を用いてリアルタイムで行われる攻撃側からの攻撃に対応する．攻撃側は，防御側が仮想ネットワークを構築した後に攻撃ツールを備えた仮想機器(以下，攻撃用ホスト）を配置し，これを用いて攻撃を行う．攻撃と防御は交互に行われ，攻撃側が行える攻撃は 3 回までとしている．演習を行う際，本システムの利用対象者が防御側のネットワークトポロジが何も見えない状態で攻撃の演習を行うのは難しい．そのため，攻撃側は防御側のネットワークトポロジの把握を可能としている．また，実践的な演習に近づけるため，防御側では攻撃用ホストの配置位置が見えないようにしている．

演習には制限時間を設けている．制限時間は，学習者同士で相談して決める．学習者は，制限時間内にできる限り多くの攻防戦を行う．演習の終了条件として，防御側が制限時間内に 3 つの攻撃を防げた時と，制限時間が経過した時がある．防御側が制限時間内に 3 つの攻撃を防げた時，防御側の勝利となる．制限時間が経過した場合，攻撃側が行った全ての攻撃を防御側が防げていた時，防御側の勝利となる．防げていなかった時，攻撃側の勝利となる．演習状況として，攻撃側は現在いくつ防御されているか，防御

側は現在いくつ防御できているかについては，図 2 にあるチャット欄に適時表示される．演習状況の表示例を図 3 に示す．勝敗結果についても図 2 にあるチャット欄に表示される．

3.3 演習補助機能

演習補助機能は，演習を行う際，学習者にヒントの表示を行う機能である．演習補助機能は，図 2 にある演習補助パネルにある．演習補助パネルを図 4 に示す．学習者は，質問選択部から知りたい項目を選択し，表示ボタンを押下することで，攻撃側ではどのような攻撃方法があるか，防御側では現在どこが攻撃されているかなどがヒント表示部に表示される．なお，ヒントは階層式となっており，表示ボタンを押下するごとに，より詳細なヒントがヒント表示部に表示される．

3.4 実施可能な演習項目

本システムで実施可能な演習項目について述べる．新たに実装した不正侵入シナリオについては, 5.2 節で述べる．

図 4　演習補助パネル（防御側）
Figure 4　Exercise assistance panel (defending side)

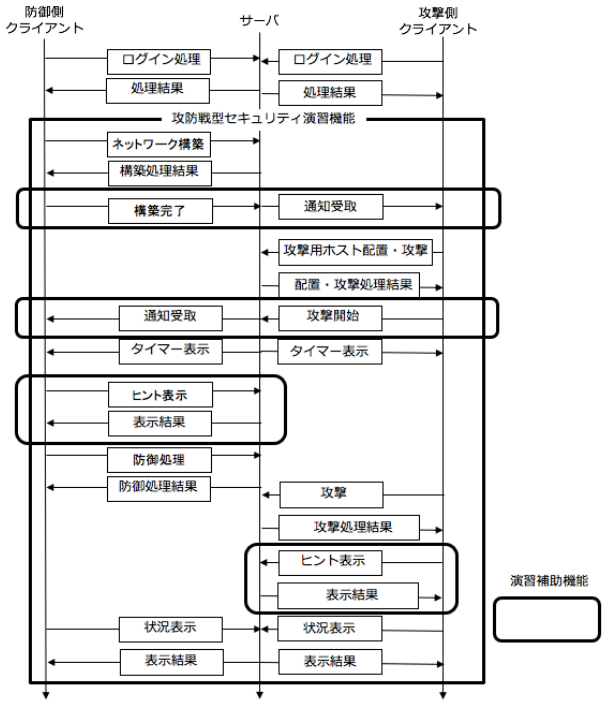

図 5　本システムを用いた演習の流れ
Figure 5　Flow of the exercise using this system

- DoS 攻撃

DoS 攻撃は，Web サービスを稼働しているサーバやエンドホストなどに意図的に過剰な負荷をかけることでサービスを妨害する攻撃である．攻撃側は，攻撃用ホストを用いて攻撃対象の仮想機器に SYN Flood 攻撃を行うことが可能である．防御側は，仮想ネットワーク内にあるいずれかの仮想機器に対して tcpdump を実行し，攻撃対象の仮想機器に SYN パケットが多く流れていることを確認する. 確認した場合，アクセスリストや iptables の設定が行える仮想機器に対して防御コマンドを発行し, DoS 攻撃の対応を行う．

- ARP Spoofing 攻撃

ARP Spoofing 攻撃は，正規のエンドホストから送られる ARP 要求に対して，攻撃側が不正な ARP 応答を何度も流すことで，正規のエンドホストの LAN 上にある通信機器になりすます攻撃である．攻撃側は，攻撃用ホストを用いて攻撃対象の仮想機器に ARP Spoofing 攻撃を行うことが可能である．防御側は，仮想ネットワーク内にあるいずれかの仮想機器に対して ARP テーブルの確認を行い，IP アドレスと MAC アドレスの対応付けが正しくないものを見つける．見つけた場合，対応付けが正しくない仮想機器の ARP キャッシュに対して静的エントリを登録し，ARP Spoofing 攻撃の対応を行う．

4. 本システムを用いた演習の流れ

本システムを用いた演習の流れを図 5 に示す. はじめに，両側の学習者が本システムにログイン処理を行う．両側の学習者がログインを完了すると，防御側は，仮想機器である Host，Router，Hub，Web Server，Firewall を用いて仮想ネットワークの構築を行う．この時，防御コマンドを発行することも可能である．しかし，今回はある攻撃とそれに対応する防御コマンドを適切に発行できるか確認するため，構築に関するコマンドのみを発行し，防御に関するコマンドは発行しないものとする．

構築が完了すると，防御側は図 4 にある機器設定完了ボタンを押下する．押下すると，構築が完了した旨が攻撃側に伝わる．防御側が仮想ネットワークを構築したことを知ると，攻撃側は攻撃用ホストを配置して攻撃を行う．はじめの攻撃を行うと，攻撃側は攻撃側の演習補助パネルにある攻撃開始ボタンを押下する．押下すると，制限時間の設定画面が表示される．攻撃側は，制限時間の設定を行った後，制限時間の設定画面にある完了ボタンを押下する．押下すると，攻撃側がはじめの攻撃を行った旨が防御側に伝わる．また，設定した制限時間を持つタイマーが両側の演習補助パネルに表示される．攻撃側がはじめの攻撃を行ったことを知ると，防御側はヒントなどを用いて攻撃箇所や攻撃の種類を特定し，その対応を行う．この対応の判定結果については，両側のクライアントが演習状況の表示に関する要求をサーバに適時送信することで，両側のチャット

欄に表示されるようにしている．表示内容は，3.2 節で述べた通りである．

防御側が行った対応が正しかった場合，防御側のチャット欄では防御できている数が増え，1 と表示される．その時，攻撃側のチャット欄では防御されている数が 1 と表示されるため，攻撃側は攻撃が防がれたと判断し，新たに攻撃を行う．防御側が行った対応が正しくなかった場合，防御側のチャット欄で表示されている，防御できている数は増えず，0 のままとなる．その時，防御側は対応が正しくなかったと判断し，改めてその攻撃の対応を行う．このように，攻撃と防御が交互に行われる．以上が，本システムを用いた演習の流れとなる．

5. 追加実装

本章では，新たに実装した NIDS と不正侵入シナリオについて述べる．

5.1 NIDS

NIDS は，通過するパケットを監視して解析を行い，そのパケットが不審だと判断した場合，そのパケットに関する情報を記録し，管理者に通知を行う機器である．本稿では，仮想マシンを用いて NIDS を実装した．NIDS の実装にあたって，パケットの監視と解析，ログの記録が可能な Snort[17]を仮想マシンに導入し，NIDS として動作させている．また，解析には不審なパケット情報をあらかじめ定義し，それに一致するパケットが流れた場合に不審だと判断するシグネチャ型を用いた．

NIDS は仮想機器の一つである．そのため，防御側は NIDS を含んだ仮想ネットワークを構築可能である．防御側が NIDS を含んだ仮想ネットワークを構築した時，攻撃を検知する方法は 2 種類となる．1 つ目は，tcpdump を用いる方法である．防御側は tcpdump を用いて不審なパケットが送られてこないか常に監視を行って防御側自身で検知する．2 つ目は NIDS を用いる方法である．NIDS は通過するパケットを監視し，不審なパケットの検知を行う．NIDS が不審なパケットを検知した場合，NIDS はそのパケットに関する情報を記録する．

NIDS が記録した不審なパケットに関する情報を防御側が確認するまでの流れを説明する．サーバは，攻撃用ホストからコマンドが発行される度に NIDS にある不審なパケットに関する情報が記録されるファイルの内容を確認する．ファイルの内容に変化があった場合，サーバは防御側のクライアントに NIDS が不審なパケットを検知した旨を通知する．通知画面を図 6 に示す．防御側は通知を受け取ることで，不審なパケットが仮想ネットワーク内に流れたことを知ることが可能となる．通知を受け取った後，防御側は図 7 にある検出ログを押下する．検出ログがあるドロップダウンリストは，NIDS として動作する仮想機器にある右上の▼印を押下すると表示される．押下すると，NIDS にある不審なパケットに関する情報が記録されるファイルの内容が図 4 にあるヒント表示部に表示される．表示例を図 8 に示す．表示することで，防御側は不審なパケットに関する情報を確認することが可能となる．以上が，NIDS が記録した不審なパケットに関する情報を防御側が確認するまでの流れとなる．NIDS により，防御側は tcpdump を用いて検知できなかった不審なパケットも検知可能となる．さらに，防御側は NIDS が記録した不審なパケットに関する情報と tcpdump の出力結果を見比べることで，どのようなパケットが検知対象になるか知ることが可能となる．

5.2 不正侵入シナリオ

不正侵入は，悪意ある第三者が個人・企業の PC やサービスに不正に侵入する行為である．本稿では，攻撃側が攻撃対象の仮想機器に対してポートスキャンを行い，23 番ポートが開いていた場合に不正侵入を行えるように実装した．攻撃側は，攻撃対象となる仮想機器の 23 番ポートが開いて

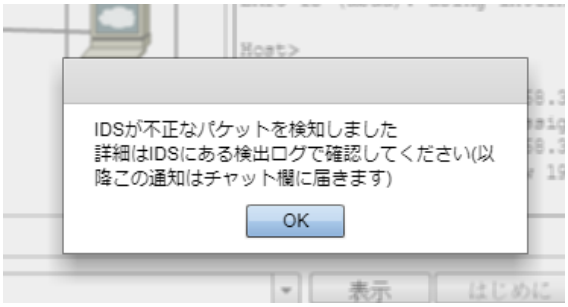

図 6 検知した際の通知画面

Figure 6 Notification GUI when detecting

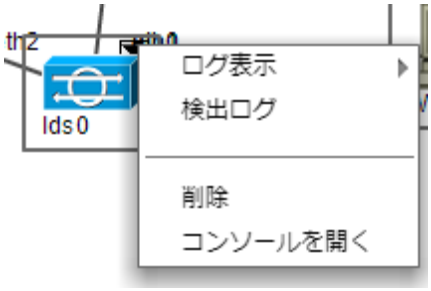

図 7 検出ログ項目

Figure 7 Detection log item

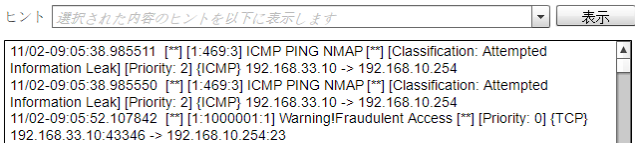

図 8 検出ログ

Figure 8 Detection log

いることをポートスキャンで確認すると，Telnet を用いてその仮想機器に接続する．Telnet 接続時に聞かれるユーザ名とパスワードに関しては，脆弱なものを設定している．Telnet 接続が成功した場合，攻撃側はその仮想機器内にあるファイルの閲覧や改竄などが可能となっている．

不正侵入を攻撃側が行っていた時において，防御側が仮想ネットワーク構築時に NIDS を配置していた場合，不審なパケットを検知した旨が防御側に通知される．そして，防御側は不審なパケットに関する情報を確認して不審な Telnet 接続が行われたことを知ると，不審な Telnet 接続が行われないよう，Firewall に対してポートフィルタリングの設定などを行う．また，防御側が仮想ネットワーク構築時に NIDS を配置しなかった場合，各仮想機器に対して tcpdump を実行し，23 番ポートに関するパケットを常に監視する．常に監視することで，不審な Telnet 接続が行われたことを検知する．不正侵入に関する演習を行うことで，学習者は不正侵入に関する理解を深めることが可能となる．また, NIDS を用いて不正侵入に関する演習を行うことで，防御側は NIDS の性質や不正侵入に対する防御方法の学習などが可能となる．

6. 実験

本章では，本システムの性能評価実験と，本稿で新たに実装した NIDS と不正侵入シナリオの動作検証, NIDS の利用評価実験について述べる．実験で用いたサーバのスペックを表 1 に示す.

6.1 性能評価実験

本稿で新たに実装した NIDS を本システムに導入した場合においても，想定する演習のネットワーク規模に本システムが対応可能であり，学習者が本システムを円滑に実施可能か確認する. 想定する演習のネットワーク規模は, Web Server と攻撃用ホストがそれぞれ 1 台，その他の仮想機器はそれぞれ 1 台以上 10 台以下とする．演習は，1 台の攻撃用ホスト，1 台の Hub，1~2 台の Router，2~4 台の Host 程度で実施可能となるが，実運用されているネットワーク規模に近づけるため，このような想定規模とした.

はじめに，想定する最大規模のネットワークを構築し，その時の CPU 使用率とメモリ使用量をそれぞれ 20 回計測した．CPU 使用率の計測には，Linux の vmstat コマンドを用いた．CPU 使用率は，構築時の最大 CPU 使用率を値とした．メモリ使用量の計測には，Linux の free コマンドを用いた．この時のメモリ使用量は，構築後と構築前のメモリ使用量の差分を値とした．計測の結果，最大 CPU 使用率は平均 33.5%，標準偏差 2.1 であった．また，メモリ使用量は平均 1.59GB，標準偏差 0.017 であった．以上より，想定する演習のネットワーク規模に本システムが対応可能であることを確認した.

次に, 各仮想機器の起動に要するメモリ使用量と時間(以下，起動時間)，結線に要する時間（以下，結線時間)，サーバの起動に要するメモリ使用量をそれぞれ 20 回計測した．メモリ使用量の計測には，Linux の free コマンドを用いた．仮想機器の起動に要するメモリ使用量は，対象の仮想機器の起動後と起動前のメモリ使用量の差分を値とした．サーバの起動に要するメモリ使用量は，サーバ起動後と起動前のメモリ使用量の差分を値とした．起動時間と結線の計測には，クライアントの開発に使用している Action Script[18]の getTimer()関数を用いた．起動時間は，図 2 にある機器追加パネルから対象の仮想機器のアイコンをネットワーク図表示部にドラッグ&ドロップしてから，対象の仮想機器のアイコンが図 2 にあるネットワーク図表示部に表示され，図 2 にあるコンソール部においてコマンドの発行が可能となるまでの時間を値とした．結線時間に関しては，あらかじめ 2 台の仮想機器を起動し，その仮想機器間で結線を行う．結線の要求を送信してから，図 2 にあるネットワーク図表示部にある仮想機器の間に直線が表示されるまでの時間を結線時間の値とした.

各仮想機器の起動に要するメモリ使用量と起動時間の計測結果を表 2 に示す．Web Server を除く全ての仮想機器は約 60MB 以下のメモリ使用量で起動することを確認した．また, 全ての仮想機器が約 20 秒以下で起動することを確認した．Hub のメモリ使用量が，システム上で計測可能な範囲内にならなかった理由については，Hub のみが UML を使用しておらず，uml_switch を用いていることが考えられ

表 1　実験で使用したサーバ用 PC のスペック
Table 1　Specification of server PC used in experiment

OS	Ubuntu 14.04 LTS
CPU	Intel(R)Core(TM)i7-3770@3.4GHz
MM	16GB

表 2　仮想機器の計測結果
Table 2　Measuring result of virtual machine

	メモリ使用量（MB）		起動時間（秒）	
	平均	標準偏差	平均	標準偏差
Host	13.8	0.8	3.45	0.03
Router	25.1	1.1	8.85	3.21
Firewall	25.3	1.1	8.73	2.58
Web Server	211.3	9.1	10.16	0.77
Attacker Host	19.7	1.7	18.52	2.55
Hub	0	0		
NIDS	54.5	4.3	10.04	0.19

る．また，Hub は図 2 にあるコンソール部を使用しないため起動時間は計測不能としている．なお，Hub のアイコンは 1 秒も満たずに表示される．結線時間は，平均 0.32 秒，標準偏差 0.01 であった．さらに，本システムにおけるサーバの起動に要するメモリ使用量は平均 29.6MB，標準偏差 3.7 であった．以上より，演習に必要な仮想機器が十分設置可能であることと，学習者が本システムを円滑に実施可能であることを確認した．また，各仮想機器の起動に要するメモリ使用量の計測結果から，想定を超えた規模のネットワーク構築も問題ないと考える．

6.2 動作検証

実装した NIDS と不正侵入シナリオが正しく動作するか確認する．本検証では，NIDS を配置した仮想ネットワーク内にある，23 番ポートが開いている Web Server に，攻撃側が攻撃用ホストを用いて不正侵入シナリオを行う．その時，NIDS が反応し，不審なパケットに関する情報の記録を行う．次に，攻撃用ホストから何らかのコマンドが発行された時，サーバが NIDS にある不審なパケットに関する情報が記録されるファイルの内容を確認しているかを確認する．ファイルの内容に変化があるため，サーバは NIDS が不審なパケットを検知した旨を防御側のクライアントに通知を行う．防御側は，通知を受け取った後不審なパケットに関する情報を確認する．その後，防御側が Firewall を用いてポートフィルタリングの設定などを行い，不審な Telnet 接続が行われないようにする．防御側は，不審な Telnet 接続に対して適切な対応をした後，しばらくしてチャット欄に表示される演習状況に表示される数が更新されていることを確認する．攻撃側は，演習状況が更新されていることを確認すると，攻撃用 Host から Web Server に Telnet 接続を改めて行う．この時，Telnet 接続が行えなくなっていることを確認する．検証の結果，想定した動作を確認することができた．

6.3 利用評価実験

実装した NIDS の有用性を確認するため，本学で開講しているシスコネットワーキングアカデミー[19]受講経験者 6 名（以下，被験者）を対象に利用評価実験を実施した．

実験内容として，NIDS を用いずに構築した仮想ネットワークに対して不正侵入シナリオを行った場合と，NIDS を用いて構築した仮想ネットワークに対して不正侵入シナリオを行った場合において，被験者が不審なパケットを検知できたか否かと，検知できた場合には検知を確認するまでの時間（以下，検知時間）を計測した．NIDS を用いない場合は，不正侵入シナリオの開始から tcpdump を用いて不審なパケットを 1 つ見つけてもらうまでの時間を検知時間とした．NIDS を用いる場合も tcpdump を実行してもらい，不正侵入シナリオの開始から NIDS にある不審なパケットに関する情報が記録されるファイル内容のいずれかと合致するパケットを tcpdump の出力結果から 1 つ見つけてもらうまでの時間を検知時間とした．なお，被験者には事前に不審なパケットの例を示しており，それを参考に検知してもらっている．

実験結果を表 1 に示す．NIDS を用いない場合と用いる場合のいずれにおいても，被験者が不審なパケットを検知できたことから，検知の差は見られないことを確認した．しかし，その検知時間に差が出ており，6 名中 5 名が NIDS を用いる場合の方が早く検知できていることを確認した．これに関しては，NIDS を用いる場合，不審なパケットに関する情報が記録されるファイル内容を確認することで，流れてきたパケットがどのように不審なのか把握でき，それを元に tcpdump の出力結果から探すことで早く検知できたと考えられる．一方，NIDS を用いても検知時間が長かった被験者もいた．この原因として，NIDS と tcpdump を実施した仮想機器におけるシステム時刻の不一致が挙げられる．システム時刻の不一致により，不審なパケットに関する情報が記録されるファイル内容にあるタイムスタンプと tcpdump の出力結果にあるタイムスタンプに大きな違いが生じた．そのため，時刻の対応付けを被験者自身で行う必要が出てしまい，合致するパケットを探すのに時間を要したと考える．改善策として，全ての仮想機器のシステム時刻を一致させることが挙げられる．

そして，被験者の中には事前に示した不審なパケットの例以外の不審なパケットを，NIDS が記録した不審なパケットに関する情報を参考にして検知した者もいた．このことから，NIDS を用いる演習では，不審かどうか今まで学習者が見分けられなかったパケットを不審なパケットであると見分けられるようになる機会が存在すると言える．以上より，NIDS の有用性を確認した．

7. まとめ

本稿では，本システムで行える演習をより充実させるため，不正侵入に関する演習を行えるようにした．不正侵入に関する演習を行うことで，学習者は不正侵入に関する理解を深めることが可能となる．また，不正侵入に関する演

表 3　利用評価実験の結果

Table 3　Results of utilization evaluation experiment

	NIDS を用いない場合		NIDS を用いる場合	
被験者	検知	検知時間	検知	検知時間
A	○	9 分	○	3 分
B	○	9 分 40 秒	○	7 分 10 秒
C	○	3 分 20 秒	○	5 分
D	○	8 分	○	1 分 40 秒
E	○	4 分 40 秒	○	2 分 10 秒
F	○	5 分 56 秒	○	2 分 52 秒

習において，不正侵入に気づく手段の一つとして，新たにNIDS を実装した．NIDS により，防御側は tcpdump を用いて検知できなかった不審なパケットも検知可能となる．さらに，防御側は NIDS が記録した情報と tcpdump の出力結果を見比べることで，どのようなパケットが検知対象になるか知ることが可能となる．以上より，NIDS を用いて不正侵入に関する演習を行うことで，防御側は NIDS の性質や不正侵入に対する防御方法の学習などが可能となる．

性能評価実験により，新たに実装した NIDS として動作する仮想機器を本システムに導入した場合においても，想定する演習のネットワーク規模に本システムが対応可能であり，円滑な演習の実施が可能であることを確認した．また，想定を超えた規模のネットワーク構築も問題ないと考える．そして，動作検証により，NIDS と不正侵入シナリオが想定した動作を確認することができた．さらに，利用評価実験により，NIDS の有用性を確認した．

今後は，Web アプリケーション攻撃などの新たなシナリオの実装を行う予定である．これにより，学習者は，より多くの演習項目を持つネットワークセキュリティ演習を行うことが可能となる．また，現状一度に 2 人の学習者が演習を行えるようにしているが，一度に 2 人以上の学習者が演習を行えるよう開発を進める予定である．これにより，より実践的な演習を行えると考える．

謝辞 本研究は JSPS 科研費 18K11592 の助成を受けたものです.

参考文献

[1] 警察庁サイバー犯罪対策:平成 29 年度不正アクセス行為対策等の実態調査，入手先 <https://www.npa.go.jp/cyber/research/h29/h29countermeasures.pdf>（参照 2018-11-11）.
[2] 経済産業省 : IT 人材の最新動向と将来推計に関する調査結果, 入手先 <http://www.meti.go.jp/press/2016/06/20160610002/20160610002.pdf>（参照 2018-11-11）.
[3] 情報処理推進機構：情報セキュリティ人材の育成に関する基礎調査−調査報告書−，入手先 <https://www.ipa.go.jp/files/000014184.pdf>（参照 2018-11-11）.
[4] 情報処理推進機構：情報セキュリティ人材不足数等に関する追加分析について，入手先 <https://www.ipa.go.jp/files/000040646.pdf>（参照 2018-11-11）.
[5] 総務省事務局：サイバーセキュリティの現状と総務省の対応について，入手先 <http://www.soumu.go.jp/main_content/000467154.pdf>（参照 2018-11-11）.
[6] Uma, M. and Padmavathi, G.: A Survey on Various Cyber Attacks and Their Classification, *IJNS*, Vol.15, No.5, pp.390-396(2013).
[7] DEF CON Communications Inc：DEFCON CTF, available from <https://www.defcon.org/html/links/dc-ctf.html>(accessed 2018-11-11).
[8] SECCON2018 運営事務局：SECCON，入手先 <https://2018.seccon.jp/>（参照 2018-11-11）.
[9] 湯川誠人，井口信和：1 対 1 で行う攻防戦型演習を可能とする仮想マシンを用いたネットワークセキュリティ学習支援システム，電子情報通信学会関西支部第 23 回講演論文集，Vol.2018，pp.15 (2018).
[10] JPCERT/CC：JPCERT/CC インシデント報告対応レポート [2018 年 7 月 1 日〜2018 年 9 月 30 日]，入手先 <https://www.jpcert.or.jp/pr/2018/IR_Report20181016.pdf>（参照 2018-11-11）.
[11] 立岩祐一郎，岩崎智弘，安田考美：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.96，No.7，pp.1585-1594（2013）.
[12] Walden, James: A Real-time information Warfare Exercise on a Virtual Network, *SIGCSE Bull*, Vol.37, No.1, pp.86-90(2005).
[13] 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.1412-1423（2011）.
[14] Nobukazu, Iguchi: Development of a self-study and testing function for NetPowerLab, an IP networking practice system, *Int. J. Space-Based and Situated Computing*, Vol.4, No.3/4, pp.175-183(2014).
[15] Dike, J.: User Mode Linux, Pearson Education, 2006.
[16] Adobe Systems：Flash Player，入手先 <http://www.adobe.com/jp/products/flashplayer.html>（参照 2018-11-11）.
[17] Cisco Systems Inc:Snort, available from<https://www.snort.org>(accessed 2018-11-11).
[18] Adobe Systems：Action Script，入手先 <https://help.adobe.com/jaJP/FlashPlatform/reference/actionscript/3/index.html>（参照 2018-11-11）.
[19] Cisco Systems Inc:イントロダクション-シスコネットワーキングアカデミー- Cisco Systems，入手先 <http://www.cisco.com/jp/go/academy/>（参照 2018-11-11）.