G-30

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フィードバック機能の実装

Implementation of Feedback Function in a System for Supporting Learning of Network Security Enabling Offensive and Defensive Battle Exercise

湯川 誠人†　井口 信和‡
Makoto Yukawa　Nobukazu Iguchi

1. 序論

警察庁が企業や教育機関など，630 の組織を対象に実施した調査によると，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 割を上回っていた[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ている．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[2]．このように，サイバー攻撃の増加やその複雑さ[2]から，対策難易度が向上している．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，そこから実際の対策に活かすことが必要である[3]．両側の視点でセキュリティを学べる演習として，攻防戦型の演習が存在する Capture The Flag[4][5]がある．しかし，このような攻防戦型の演習を，運用しているネットワーク上で実施する場合，ネットワークに障害が発生し，利用者に影響を与える可能性がある．さらに，実機を新たに用意して演習を実施する場合，実機の OS 等の動作に支障をきたすおそれがある．

この問題に対して，実環境・実機に影響を与えることなくサイバー演習を実施できる Cyber Range といったシステム[6]が開発されている．しかし，このようなシステムを導入・運用するには金銭，時間，人員といったコストがかかるため，学習者が手軽に，繰り返し利用することは難しい．

これまでに，我々は攻撃視点を取り入れたネットワークセキュリティの演習が安全・手軽に実施できる環境の提供を目的に，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[7]．本システムは，2 人の学習者が攻撃側と防御側に分かれてネットワークセキュリティの演習を実施することを可能とする．本システムにより，学習者は実環境・実機に影響を与えることなく，安全に攻防戦型の演習を実施でき，ネットワークセキュリティに関する知識とスキルの向上を図ることが可能となる．また，システムの利用の手軽さから，学習者が繰り返し演習できるため，各攻撃に対してより早く正確に対応できるようになり，理解度と定着度を高めることが期待できる．

本稿では，防御側の学習者が各攻撃に対する理解度と定着度をより高めるため，演習終了時までに防御側の学習者が対応できなかった攻撃に対して適切な対応策を提示する機能を実装した．

† 近畿大学大学院総合理工学研究科, Graduate School of Science and Engineering Research, Kindai University

‡ 近畿大学理工学部,Faculty of Science and Engineering, Kindai University

2. 研究内容

本章では，本システムについて述べる．最初に，本システムの概要を説明する．次に，我々がこれまでに開発してきた本システムの実装内容について述べる．最後に，フィードバック機能の実装を報告する．

2.1. システム概要

本システムは，ネットワーク構築演習支援システム[8][9]を基盤技術として活用している．実装技術として，Linux マシン上で別の仮想 Linux マシンを動作させることが可能なオープンソースの仮想化ソフトウェアである User Mode Linux[10]を用いている．本システムでは，作成した仮想 Linux マシンを，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．User Mode Linux はホスト型であるため，仮想 Linux マシンはホスト OS 上で一つのアプリケーションとして扱われる．

仮想 Linux マシンは GUI 操作がなく，CLI 操作のみ可能である．そのため，起動時のメモリ使用量が少なく，複数の仮想 Linux マシンを起動することが可能となる．また，ゲスト OS で発生した障害はホスト OS に影響しないため，セキュリティ的に堅牢である．

本システムの構成を図 1 に示す．本システムは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 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，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[11]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

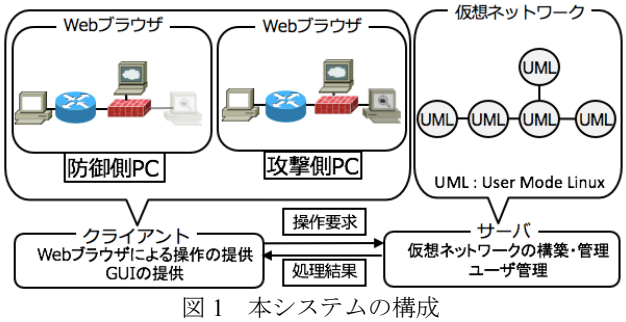

図 1　本システムの構成

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．

2.2. 攻防戦型ネットワークセキュリティ演習

攻防戦型ネットワークセキュリティ演習は，2 人の学習者が攻撃側と防御側に分かれて演習を実施することを可能とする．本システムの利用対象者は，セキュリティ分野に携わる学生および新入社員などの中で，ネットワークセキュリティに関する知識が不足している初級の学習者である．演習を実施する際，学習者には役割を与えている．攻撃側には攻撃者の役割を与えており，攻撃を継続的に実施してもらう．防御側にはネットワーク管理者の役割を与えており，ネットワークの監視や攻撃の対応などを実施してもらう．学習者が発行した攻撃・防御コマンドについては，本システムが記録し，それを基に正誤を判断して勝敗を決めている．

2.2.1. 攻防戦型ネットワークセキュリティ演習の流れ

攻防戦型ネットワークセキュリティ演習の流れを図 2 に示す．以下に詳細を述べる．

① 両側の学習者は提案システムにログイン処理を実施する．

② 防御側は仮想機器である Host，Router，Hub，Web Server，Firewall，NIDS を用いて仮想ネットワークを構築する．
この時，攻撃側が実施した攻撃に対して防御側が適切に防御コマンドを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．

③ 防御側は構築を完了すると図 3 にある機器設定完了ボタンを押下し，構築が完了した旨を攻撃側クライアントに伝える．

④ 攻撃側は攻撃ツールを備えた仮想機器（以下，攻撃用ホスト）を仮想ネットワークに配置する．攻撃用ホストの配置に関して，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を実施することは本システムの利用対象者にとって難しい．そのため，攻撃側は防御側が構築した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を非表示にしてある．

⑤ 攻撃側は攻撃を実施する．

⑥ 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し，タイマーの設定を実施する．設定すると，はじめの攻撃を実施した旨が防御側に伝わると同時に攻撃側が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．

⑦ 防御側は攻撃がされた箇所とその攻撃の種類を特定し，対応する．

⑧ 攻撃側は自身が実施した攻撃が失敗したことに気づくと，次の攻撃を実施する．

以上のように，攻撃と防御を交互に繰り返す．

2.2.2. 演習の終了条件

この演習の終了条件は，次の 2 つである．1 つ目は制限時間が経過した時である．経過した際，攻撃側が実施した攻撃を防御側が防いでいた状態で終了した場合は防御側の勝利となる．攻撃を防いでいない状態で終了した場合は攻撃側の勝利となる．2 つ目は演習補助パネルにある降参ボタンをどちらかが押下した時である．降参ボタンを押下した学習者は敗北となり，もう一方の学習者の勝利となる．なお，勝敗結果はチャット欄に表示される．

2.2.3. 学習項目

学習者がこの演習を通して学ぶ項目は以下の通りである．攻撃側は，攻撃コマンドとその動きを学ぶ．これにより，攻撃の性質を理解してもらう．また，攻撃されるおそれがある箇所を推測するスキルの向上を図る．そして，ツールやコマンドは使い方次第で攻撃となり得るおそれがあることを理解してもらう．防御側は，攻撃の確認方法とその防御コマンドを学ぶ．これにより，攻撃の性質を理解してもらう．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適切な防御コマンドを仮想機器に発行できるようにしてもらう．

2.2.4. 演習補助機能

演習補助機能は，学習者にヒントの提示を可能とする機能である．図 3 の演習補助パネルを通して利用可能である．演習補助パネルは攻撃側と防御側の両方に存在している．学習者は，演習補助パネルにある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．押下されると，サーバは，その項目に関するヒントをヒント表示部に表示する．質問選択部には，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等を用意した．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毎に，より詳細なヒントがヒント表示部に表示される．

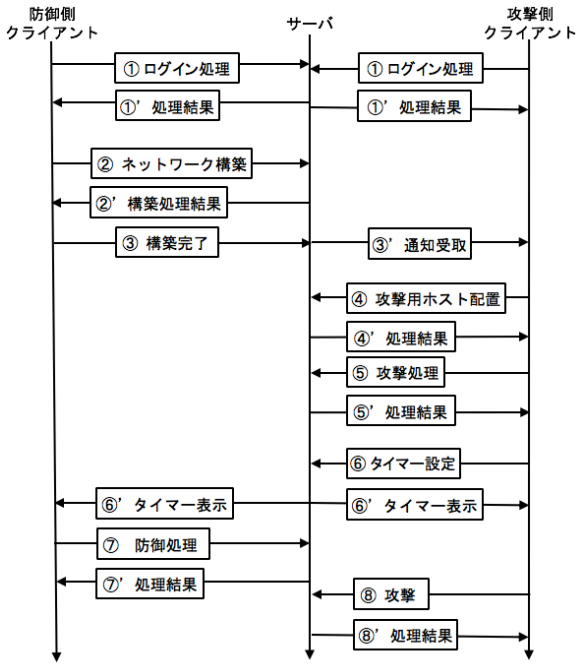

図 2　本システムを用いた演習の流れ

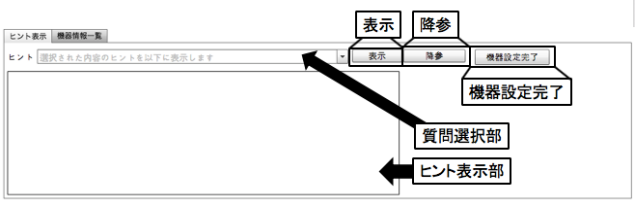

図 3　演習補助パネル（防御側）

2.3. フィードバック機能

フィードバック機能は，演習終了時までに防御側の学習者が対応できなかった攻撃に対して適切な対応策を提示する機能である．本機能の流れを図 4 に示す．制限時間が経過した，もしくは降参ボタンをどちらかの学習者が押下した時，本機能ははじめに，本システムが記録している，攻撃側の学習者が発行した攻撃コマンドから攻撃の種類を特定する．次に，その攻撃を防いでいるかを防御側の学習者が発行した防御コマンドから判断する．全ての攻撃を防いでいた場合，何もしない．防いでいない攻撃があった場合，攻撃名とその攻撃に対する対応策の説明を格納しているデータベース（以下，対応管理 DB）を使用する．防いでいない攻撃に対応した対応策の説明を対応管理 DB から取得し，その情報を図 3 にあるヒント表示部に表示する．本機能により，防御側の学習者が各攻撃に対する理解度と定着度をより高めることが期待できる．

3. 実験

動作検証として，実装したフィードバック機能が正しく動作するかを確認した．実験の手順は次の通りである．最初に，防御側が Web サーバを含む仮想ネットワークを構築する．次に，攻撃側の学習者が攻撃用ホストを配置し，攻撃を開始する．なお，今回の実験の対象となる攻撃は本システムで実施可能な DoS 攻撃，Arp Spoofing 攻撃，不正侵入攻撃，SQL インジェクション攻撃の 4 つである．最後に，防御側の学習者は何もせずに制限時間が経過するのを待つ．この時，防御側の学習者は適切な対応をしていないため，フィードバック機能が実施されることになる．その結果，その攻撃に対する対応策の説明が表示されることを確認する．防御側の学習者が降参ボタンを押下した場合においても同様の結果になることを確認する．また，防御側の学習者が攻撃を防いでいた場合は特定の攻撃に対する対応策が表示されないことを確認する．実験の結果，目的通り正しく動作していることを確認した．

4. 結論

これまでに，我々は攻撃視点を取り入れたネットワークセキュリティの演習が安全・手軽に実施できる環境の提供を目的に，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を開発してきた．本稿では，防御側の学習者が各攻撃に対する理解度と定着度をより高めるため，演習終了時までに防御側の学習者が対応できなかった攻撃に対して適切な対応策を提示する機能を実装した．今後の予定として，本システムに有用性があるか確認するため，本システムの利用評価実験を実施する予定である．

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 2019-7-18）．

[2] 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 2019-7-18）．

[3] Uma, M. and Padmavathi, G.: A Survey on Various Cyber Attacks and Their Classification, *IJNS*, Vol.15, No.5, pp.390-396(2013).

[4] DEF CON Communications Inc：DEFCON CTF, available from <https://www.defcon.org/html/links/dc-ctf.html>(accessed 2019-7-18).

[5] SECCON2018 運営事務局：SECCON，入手先 <https://2018.seccon.jp/>（参照 2019-7-18）．

[6] サイバー演習システム「ADI Cyber Range」（旧名称「Sypris Cyber Range」）：NTT データ先端技術株式会社，入手先 <http://www.intellilink.co.jp/security/services/cyberrange.html>（参照 2019-07-03）．

[7] 湯川誠人，井口信和：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，インターネットと運用技術シンポジウム論文集，Vol.2018，pp.92-99（2018）．

[8] 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）．

[9] 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).

[10] Dike, J.: User Mode Linux, Pearson Education, 2006.

[11] Adobe Systems：Flash Player，入手先 <http://www.adobe.com/jp/products/flashplayer.html>（参照 2019-7-18）．

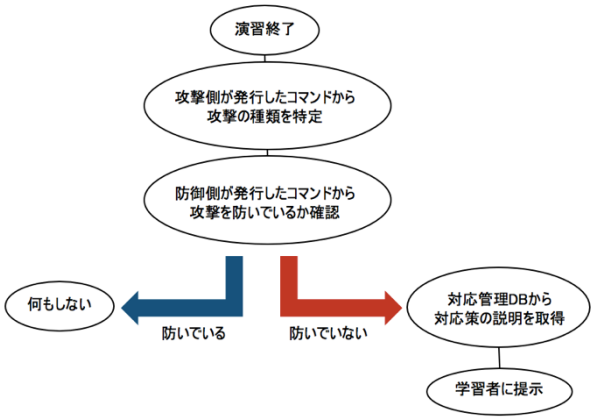

図 4　フィードバック機能の流れ