様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月　 ２ 日現在

機関番号：３４４１９
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ１１５９２

研究課題名（和文）攻防戦型演習を可能とする仮想マシンによるネットワークセキュリティ演習支援システム

研究課題名（英文）A Network Security Exercise Support System Using Virtual Machines to Enable Offensive and Defensive Exercises

研究代表者
井口　信和（IGUCHI, Nobukazu）

近畿大学・理工学部・教授

研究者番号：５０３５１５６５

交付決定額（研究期間全体）：（直接経費）　　2,100,000円

研究成果の概要（和文）：　本研究課題では，攻防戦型ネットワークセキュリティ演習を実施できるシステムを開発した．本システムでは，2人の学習者が攻撃側と防御側に分かれて演習を行う．仮想化ソフトウェアを利用しているため，既存のネットワークに対して攻撃を行わない安全な演習が実施可能である．また，ブラウザを通して機器を操作するため，学習者は自身の保有するPC等を使って手軽に演習を実施可能である．
　必要な機能を実装し，システムの性能評価を実施した結果，想定する演習のネットワークの規模に本システムが対応可能であること，学習者が仮想ネットワークの構築を円滑に実施できることを確認した．さらに，利用評価から本システムの有用性を確認した．

研究成果の学術的意義や社会的意義
　本研究成果の学術的意義は，ソフトウェアによって実装する演習支援システムが、今後ますます必要となるネットワークセキュリティ技術者の早期の養成に有用であることを明らかにした事，さらに、協同演習の利点である観察学習やリフレクションがネットワークセキュリティの学習においても有用であることを明らかにした事である．
　社会的意義は，本課題で開発した演習支援システムを活用することで，ネットワークセキュリティ技術者の早期の養成の一助となり，セキュリティ対策に精通したネットワーク技術者の慢性的な不足の解決に貢献できる事である．

研究成果の概要（英文）：In this research, we developed a system for supporting learning of network security through offensive and defensive battle exercise. In this system, two learners are divided into an attacker and a defender. This system utilizes free software and virtual machine technologies so that low-cost and safe exercise is possible. In addition, since the user interface is a browser, learners can easily conduct exercise.
Through experimental evaluations, we confirmed that our system can support learning of network security.

研究分野：ネットワーク応用

キーワード：ネットワークセキュリティ　演習支援システム　攻防戦演習　仮想マシン

１．研究開始当初の背景

情報システムに対する不正アクセスや情報漏えいの事故は社会問題の一つになっている．その一方で，組織における脆弱性診断などの実施は十分にされていない現状がある．その原因の一つとして，セキュリティ対策に精通したネットワーク技術者の慢性的な不足があげられる．そこで，本課題において，ソフトウェアによるセキュリティ対策演習支援システムを開発することで，ネットワークセキュリティ技術者の早期の養成を目的とした学習支援環境を構築する．さらに、その有用性を利用評価実験から明らかにする．

２．研究の目的

本研究課題の目的は，仮想 Linux 環境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を用いて，疑似学習者を含む複数の学習者による攻防戦型セキュリティ演習を実現する機能と演習支援システムを開発することである．本システムによって，学習者は安全かつ手軽にセキュリティ対策の演習が実施できる．さらに，疑似学習者との協同演習を可能とすることで，共同学習者が身近にいない環境，たとえば学習者が自宅で演習を行う場合でも，協同演習を可能とする．

３．研究の方法

本研究課題では，仮想 Linux 環境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を用いて，疑似学習者を含む複数の学習者による攻防戦型セキュリティ演習を実現する機能の開発した．開発したシステムの性能評価実験および利用評価実験から，本システムの有用性を明らかにした．開発した具体的な機能は以下の通りである．

(1) 攻防戦型セキュリティ演習機能
(2) 攻撃側の疑似学習者として動作する攻撃側疑似学習者エージェント機能
(3) 協同演習の結果を自動的に採点する演習結果自動採点機能

本研究課題では，これまでに開発した IP ネットワーク構築演習支援システムを基盤技術として活用した．また、一人の学習者の演習結果を自動採点する機能を発展させ、疑似学習者を含む複数の学習者の演習結果を自動採点する機能を開発した．さらに、ネットワークセキュリティの対策学習を実行できる演習支援システムで開発した攻撃用仮想サーバや仮想マシンによるネットワーク機器のログ確認機能等を活用した．本システムは、これらの基盤・基本機能に加えて，今回，開発を計画した攻防戦型セキュリティ演習機能，攻撃側疑似学習者エージェント機能，および演習結果自動採点機能から構成されている．

本システムにおいて実施可能な演習シナリオを提案し，実際に利用評価実験を実施した．本システムで実施可能なネットワークセキュリティ演習の実施例は，以下の 4 つである．

(1) DoS 攻撃とその対策
(2) ARP Spoofing 攻撃とその対策
(3) 不正侵入攻撃とその対策
(4) SQL インジェクション攻撃とその対策

さらに，本システムの性能評価実験を実施し，本システムの有用性を確認した．

図 1 に開発した本システムの構成図，図 2 にサーバクライアントの構成を示す．

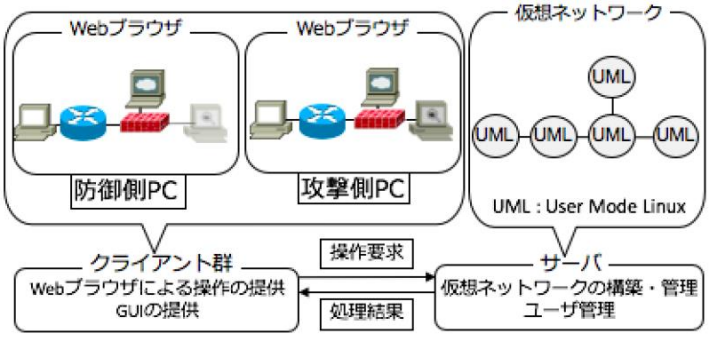

図 1 システム構成

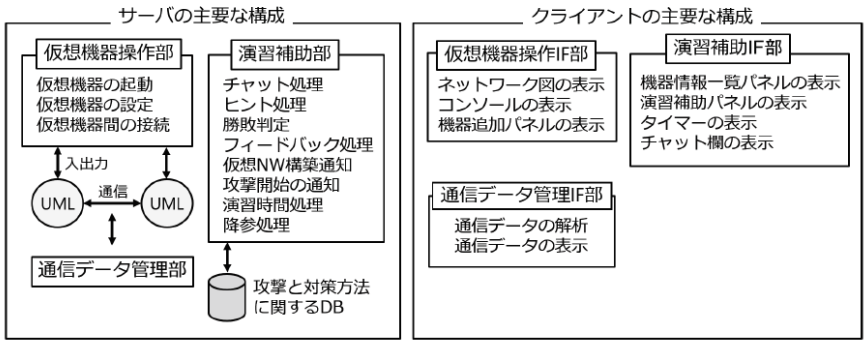

図 2 サーバクライアントの構成

４．研究成果

研究の成果として，開発システムの性能評価結果と利用評価結果について述べる．

性能評価実験においては，サーバとして CPU が Core i7 @3.4GHz，メモリが 16GB，OS が Ubuntu 14.04 LTS の PC を用いた．

(1) 仮想ネットワーク構築の負荷の評価

まず，演習で想定するネットワークの規模に本システムが対応可能であることを確認するために，想定する最大規模の仮想ネットワークを構築した時の最大 CPU 使用率とメモリ使用量を計測した．本課題では，攻防戦演習で想定するネットワークとして，Web サーバと攻撃用ホスト，NIDS がそれぞれ 1 台，その他の仮想機器が 10 台以下程度の規模のネットワークを想定している．そこで，Web サーバ 1 台，攻撃用ホスト 1 台，NIDS 1 台，ホスト 10 台，ルータ 10 台，ファイアウォール 10 台，ハブ 10 台からなる仮想ネットワークを最大規模の仮想ネットワークとし，このネットワークを構築した場合の負荷を評価する．

まず，各仮想機器の起動に要するメモリ使用量を計測した．起動に要するメモリ使用量は，仮想機器の生成前後のメモリ使用量を free コマンドによって取得し，その差分とした．20 回の計測実験により得られた，各仮想機器の起動に要するメモリ使用量を表 1 に示す．なお，計測の際は，1 回の計測毎にサーバを再起動した．ここで，表 1 に示されるようにハブの起動に要するメモリ使用量は小さいことがわかる．これは，ハブは UML ではなく uml_switch を用いて実現しているためである．表 1 で得られたメモリ使用量を最大規模の仮想ネットワークにおける各機器の台数分足し合わせると，合計のメモリ使用量は 2.02 GB となる．

続いて，実際に最大規模の仮想ネットワークを構築した場合のメモリ使用量と CPU 使用率を計測した．CPU 使用率は，vmstat を用いて，ネットワーク構築時の最大 CPU 使用率を取得した．20 回の計測実験の結果，最大規模の仮想ネットワークを構築した場合のメモリ使用量は平均 1.42 GB，標準偏差 0.008 GB であった．前述した見積値である 2.02 GB と比べて小さいのは，キャッシュが理由と考える．また，CPU 使用率は平均 33.4%，標準偏差 2.5%であった．したがって，本システムは標準的な PC をサーバとして利用可能であると考える．また，以上より，想定する演習のネットワークの規模に本システムが対応可能であることを確認した．

表 1 仮想機器の実行に要するメモリ使用量（単位：MB）

仮想機器	平均	標準偏差	最大	最小
ホスト	51.9	2.3	57	48
ルータ	52.4	2.5	60	48
ハブ	0	0	0	0
ファイアウォール	50.5	2.8	59	47
攻撃用ホスト	35.6	3.8	46	32
Web サーバ	389.6	7.8	404	374
NIDS	95.1	3.1	101	89

(2) 攻撃対象となった仮想機器の負荷の評価

次に，学習者が本システムを円滑に利用できるかを確認するために，攻撃が実施されている仮想機器の応答時間，CPU 使用率，メモリ使用量を計測した．応答時間は，コンソールに対して入力を施してからその結果が出力されるまでの時間とした．CPU 使用率は攻撃が実施されている間の最大 CPU 使用率とした．メモリ使用量は，攻撃後と攻撃前のメモリ使用量の差分を用いた．実験では，全ての仮想機器が 1 台ずつある仮想ネットワークを構築し，各仮想機器に対して攻撃用ホストから一定時間継続して DoS 攻撃（SYN Flood 攻撃）ないしは ARP Spoofing 攻撃

を実施した．それぞれの仮想機器のスペックを表 2 に示す．DoS 攻撃の対象となる仮想機器はホスト，ルータ，ファイアウォール，Web サーバ，NIDS とした．ARP Spoofing 攻撃の対象となる仮想機器はホストのみとした．応答時間，CPU 使用率，メモリ使用量いずれも仮想機器ごとに 20 回の計測を行った．また，1 回の計測ごとにサーバを再起動した．

表 2 仮想機器のスペック

仮想機器	メモリ	OS
ホスト	32 MB	Debian GNU/Linux 5.0.1
ルータ	32 MB	Debian GNU/Linux 5.0.7
ファイアウォール	32 MB	Debian GNU/Linux 5.0.7
Web サーバ	512 MB	CentOS release 6.10
NIDS	256 MB	Debian GNU/Linux 5.0.7

実験の結果，DoS 攻撃の対象となった Web サーバのみ CPU 使用率が 1〜2%上昇し，メモリ使用量も約 3MB 上昇した．一方，他の仮想機器の CPU 使用率，メモリ使用量には変化が見られなかった．DoS 攻撃を実施する前と，攻撃を実施中の各仮想機器の応答時間の計測結果を表 3 に示す．表に示されるように，応答時間にはわずかな差がみられた．また，ARP Spoofing 攻撃を実施した後のホストの応答時間は平均 0.38 秒，標準偏差 0.01 秒であり，これもわずかに差が見られた．しかし，応答時間の差は最大でも 0.2 秒程度であり学習者がわずらわしさを感じる長さでないと考える．以上から，学習者が本システムを円滑に利用できることを確認した．

表 3 DoS 攻撃実施前，攻撃中の平均応答時間（単位：秒）

仮想機器	攻撃前（標準偏差）	攻撃中（標準偏差）
ホスト	0.29 (0.01)	0.30 (0.01)
ルータ	0.26 (0.04)	0.35 (0.04)
ファイアウォール	0.27 (0.04)	0.34 (0.06)
Web サーバ	0.41 (0.01)	0.60 (0.01)
NIDS	0.43 (0.06)	0.55 (0.13)

(3) 最後に，本システム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受講経験者 10 名（以下，学習者）を対象に利用評価実験を実施した．いずれの学習者もネットワークに関する基本的な知識を持っている．実験では，学習者 2 人ずつでペアになってもらい，5 グループに分かれてもらった．次に，事前学習ページを閲覧し，システムの使い方や各攻撃手法の理解をしてもらった．その後，攻撃側と防御側に分かれ演習を実施してもらった．また，両側の立場で本システムを利用してもらうため，攻撃側と防御側の立場を入れ替えた演習も実施してもらった．自由度を持たせることでモチベーションが変わると考え，どのような攻撃を行うか，また，制限時間をどうするかは学習者に一任した．また，立場が入れ替わっても同じ制限時間で演習を実施してもらった．学習者が実際にどのようにクライアントを操作しているかを確認するため，クライアントのスクリーン画面の記録もあわせて実施した．演習終了後に，本システムに関するアンケートに回答してもらった．アンケートには操作性に関する内容が含まれるため，別途，全ての学習者に全ての仮想機器を一度以上起動し，操作してもらった．アンケートは，5 段階評価となっており，1 が強く思わない，5 が強く思う，となっている．また，アンケート用紙には自由記述欄も用意した．

事前学習ページに関する評価項目，本システムに関する評価項目，本システムの操作性に関する評価項目とそれらの項目に対する評点結果を表 4，表 5，表 6 に示す．

自由記述欄からは「わからない点はヒントを使ったが，できるだけ自分の知識で演習できた」，「使い方を説明する動画や，使い方をもう一度見直せる機能があればいいと思った」，「システムの操作方法が独特で慣れが必要であった．説明を見ても操作方法がわからない点があった」，「実際の機器と同じように機器を操作できるのでよかった」，「事前にセキュリティの知識が多少必要だと感じた」などの意見を得た．

表 4，表 5 に示すように，全ての項目で概ね良好な評価を得られた．また，スクリーン画面の記録を解析した結果，学習者がヒント機能を用いて防御を実施している場合が多かった．

アンケートの自由記述欄でヒントの有効性に関する記述もあり，ヒント機能の有用性を確認することができた．加えて，表 7 から，学習者は仮想機器の起動にわずらわしさをほぼ感じないことを確認した．また，本システムの操作性についてもこれらの結果から問題ないと考える．

以上の結果から，本システムの有用性を確認した．

(4) 研究課題では，攻撃側と防御側両方の視点を取り入れたネットワークセキュリティの演習を低コストかつ安全，手軽に実施できる環境の提供を目的に，仮想マシンを活用して攻防戦型

の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を開発した．性能評価の結果，想定する演習のネットワークの規模に開発システムが対応可能であること，また，学習者が仮想ネットワークの構築を円滑に実施できることを確認した．さらに，利用評価を行い，開発システムの有用性を確認した．

表 4 事前学習ページに関する評価項目とその結果

評価項目	平均	標準偏差
システムの使い方の説明は理解できたか	3.8	0.60
演習のルールの説明は理解できたか	4.2	0.87
DoS 攻撃の説明は理解できたか	4.4	0.48
ARP Spoofing 攻撃の説明は理解できたか	4.4	0.48
不正侵入攻撃の説明は理解できたか	4.3	0.45
SQL インジェクション攻撃の説明は理解できたか	4.0	0.89

表 5 本システムに関する評価項目とその結果

評価項目	平均	標準偏差
攻撃を実施したことにより攻撃に対する理解度は向上したと思うか	4.2	0.40
攻防戦型演習により防御手法の習得はできたと思うか	4.1	0.53
攻防戦型演習によりセキュリティに関する関心は高まったか	4.3	0.9
本システムで実施可能な演習の難易度は適切であったか	3.9	0.53
本システムで実施可能な演習の種類は適切であったか	4.4	0.66
ヒントの数は適切であったか	4.4	0.48
ヒントの内容は適切であったか	4.4	0.80
フィードバックの内容は適切であったか	3.8	1.07
また本システムを使ってみたいと思うか	4.8	0.4

表 6 操作性に関する評価項目とその結果

評価項目	平均	標準偏差
ホストが起動するまでの時間は長く感じなかったか	4.6	0.66
ルータが起動するまでの時間は長く感じなかったか	4.6	0.66
ファイアウォールが起動するまでの時間は長く感じなかったか	4.6	0.66
攻撃用ホストが起動するまでの時間は長く感じなかったか	4.7	0.45
Web サーバが起動するまでの時間は長く感じなかったか	4.5	0.67
NIDS が起動するまでの時間は長く感じなかったか	4.6	0.66
構築フェーズの操作に問題はなかったか	4.4	0.48
防御フェーズの操作に問題はなかったか	4.4	0.48
攻撃フェーズの操作に問題はなかったか	4.4	0.48

＜引用文献＞

① 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.3，2011， 1412-1423

② Nobukazu Iguchi， Development of a self-study and testing function for NetPowerLab, an IP networking practice system, International Journal of Space-Based and Situated Computing, Vol.4, 2014, Nos.3/4

③ 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の実装と評価，情報処理学会論文誌，Vol.57，No.3，2016，931-935

④ 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 D，Vol.J103-D，No.8，2020，591-602

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 湯川 誠人、谷口 義明、井口 信和	４．巻 J103-D
２．論文標題 攻防戦型ネットワークセキュリティ学習支援システム	５．発行年 2020年
３．雑誌名 電子情報通信学会論文誌D 情報・システム	６．最初と最後の頁 591～602
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transinfj.2020JDP7011	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 湯川 誠人、 井口 信和
２．発表標題 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
３．学会等名 2019年度情報処理学会関西支部 支部大会
４．発表年 2019年

１．発表者名 岸本和理、井口信和
２．発表標題 仮想マシンを活用した クロスサイトスクリプティングの実践的学習環境の開発
３．学会等名 2019年度情報処理学会関西支部 支部大会
４．発表年 2019年

１．発表者名 湯川 誠人、 井口 信和
２．発表標題 仮想マシンを活用し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性能評価実験の検討
３．学会等名 情報処理学会インターネットと運用技術シンポジウム
４．発表年 2019年

１．発表者名
湯川 誠人、 井口 信和

２．発表標題
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の開発

３．学会等名
電気関係学会関西連合大会

４．発表年
2019年

１．発表者名
岸本和理、井口信和

２．発表標題
仮想マシンを活用した クロスサイトスクリプティングの実践的演習システム

３．学会等名
情報処理学会全国大会

４．発表年
2020年

１．発表者名
湯川誠人、井口信和

２．発表標題
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 不正侵入シナリオ時に使用するネットワーク型IDSの実装

３．学会等名
平成30年度電気関係学会関西支部連合大会

４．発表年
2018年

１．発表者名
湯川誠人、井口信和

２．発表標題
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

３．学会等名
情報処理学会インターネットと運用技術シンポジウム2018

４．発表年
2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関