仮想マシン技術に基づくネットワークセキュリティ演習環境提供システムの開発とその評価（継続）

代表研究者　立岩 佑一郎　名古屋工業大学・大学院工学研究科・助教
共同研究者　高橋 直久　名古屋工業大学・大学院工学研究科・教授

1 はじめに

いまやITは重要な社会基盤となり，経済活動から日常の社会生活にわたり様々な場面で利用されている．特に，インターネットをはじめとするコンピュータネットワークの発展は目覚ましく，社会の重要なインフラとなっている．ネットワーク環境の充実により，ネットワークを介して不特定多数のコンピュータが相互に接続されることで，社会生活上の利便性が向上したと言える．World Wide Web(www)のように，ネットワークを介して，遠隔のコンピュータに保存された情報を閲覧し，様々な情報を収集できるようになっていることがその代表例であると言える．近年では，ネットワークを活用したサービスも多数行われている．

しかし，その一方で，重要なインフラであるコンピュータネットワークの仕組みを悪用し，不正に利益を得ようと試みたり，社会に大きな被害をもたらそうとしたりする行為が増加するなど，情報セキュリティ問題が深刻化している状況にある． このような中で，セキュリティに関する専門知識を持った人材が不足している．情報セキュリティ白書2010によると，「貴社の情報セキュリティ対策で課題と思われる事項は何ですか」というアンケート(図 1)において，第一位「対策ソフトウェア・ハードウェア導入にコストがかかる」(25%)に続いて，「セキュリティに関する専門知識を持つ人材がいない」(20%)が挙げられている[1]．また，「今後10年間に重要となるスキルのアンケート結果」(図 2)において，「セキュリティに関する技術力」を挙げたIT企業は54.6%とトップの，「分野を横断する幅広い技術力」に次ぐ高い数値となっている[2]．これらの調査結果から,セキュリティに関する専門的知識を持った人材育成が強く求められていることが分かる．

セキュリティ人材育成のために，大学や専門学校などの教育機関において様々な形でセキュリティ学習が行われている．それらは，主に書籍などを用いて攻撃の概念について体系的に学ぶ座学型講義，実機などを用い，実際に攻撃を体験する演習から構成される．演習においては，実機を用いて実際に攻撃を体験することができる．しかし，実機を用いて演習を行う際には，学習者の演習用ネットワークの構築に要する準備や後片付けの手間が問題となる（問題点1)．

また,攻撃を発生させる際にも問題が生じる(問題点2)．本来,教師が攻撃者の役割を担うべきであるが,人員不足により，このような演習の実現は困難である．そこで，攻撃を発生させる方法として，学習者同士で攻撃を行うといった演習方法があげられる．しかし，この方法においては，学習者が攻撃方法まで学んでしまう倫理的問題が生じる[1]．次に実際のネットワーク上に，演習用ネットワークを構築し，外部から攻撃を受け，それに対する防衛を行うという演習方法があげられる．しかし，この方法では，外部から攻撃を受けない可能性もあり，攻撃に対する防衛演習を安定的に行うことが困難である．

我々はネットワークセキュリティの演習のための遠隔アクセス可能な環境を開発した[2].この環境はユーザに仮想マシンにより構成されるネットワークをインターネットを通じて提供する．ユーザは，自宅の PC からこのネットワークを管理することができる．このため，問題点1を解決できる．また，システムは仮想マシンネットワークを構築し，そのネットワークを攻撃する機能を有する．しかし，この機能は仮想ネットワークの初期化において，各ネットワーク機器で攻撃ツールを実行するものであるため，学習者の管理によって変化したネットワークを攻略できない．

そこで本稿では，問題点2の解決のために，仮想クラッカー機能を有する遠隔ネットワークセキュリティ演習システムを提案する．仮想クラッカーは，ネットワークの状態を調査・分析し，分析結果に応じた攻撃を行う．本演習での学習目標は，検知ツールやログ解析により攻撃の発生と種類を特定できるようになること，およびシステム設定や防御ツールにより攻撃を失敗させられるようになることである．学習者は，与えられたネットワークにおいて，サーバやファイアウォールなどのネットワーク機器を操作する．使用するネットワーク機器は,Linuxサーバ,ルータ,スイッチングハブ,リピータハブ,Linuxクライアント,iptablesファイアウォールである．また，ネットワーク内で発生する攻撃は，パケットの盗聴，SSH ブルートフォー

スアタック，ARP スプーフィング，バックドア，SYN flood アタック，DNS キャッシュポイズニングである．

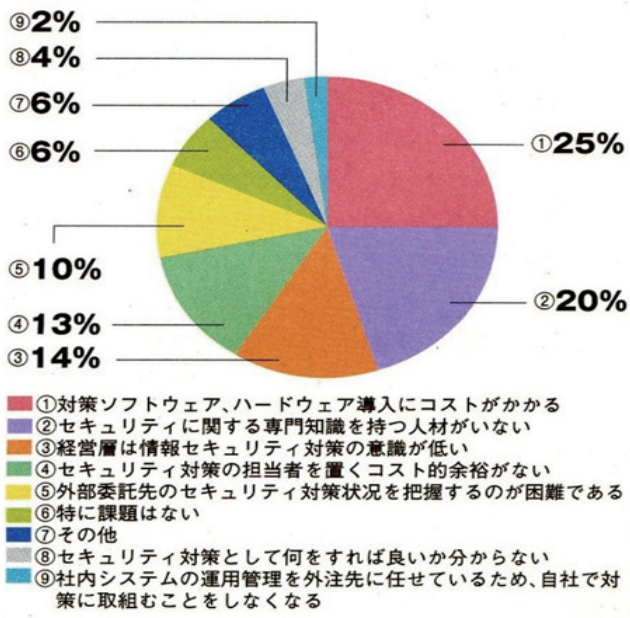

図 1：貴社の情報セキュリティ対策で課題と思われる事項は何ですか
(出典：情報セキュリティ白書 2010[1])

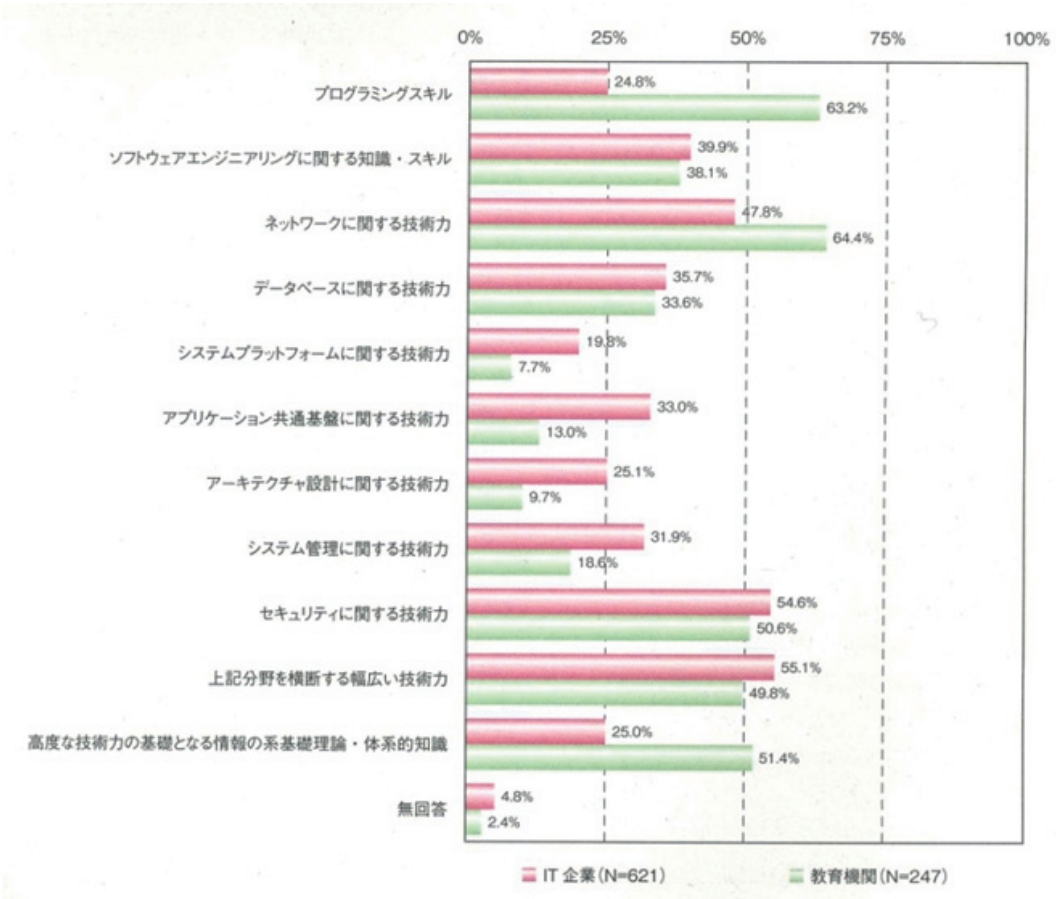

図 2：今後 10 年間に重要となるスキルのアンケート結果
(出典：情報セキュリティ白書 2010[2])

2. 関連研究

仲間は，ネットワークセキュリティに関する教育カリキュラムを作成し，実際に実習を行い，その結果報告を行った[3]．実習は，グループ単位で実機を用い，完全に安全なネットワーク環境から，段階的に侵入の危険性が増すネットワーク環境へと移行することで行われた.実習を行った結果,「余裕をもった計画を立てながらも想定外のトラブルが起こり，時間が足りず，全ての実習ができなかった」,「外部からのポートスキャンは行われたが，攻撃・侵入には至らなかった」という報告がされている．本研究においては，学習者のネットワークに対して攻撃を自動的に発生させる機能を開発することで，安定的に攻撃を受ける演習環境を実現する．

Tele-lab は,ネットワークセキュリティツールの使用を学ぶ仮想的な演習環境である[4]．この環境では，学習者は，遠隔地から VNC アプレットを使うことで，演習環境にアクセスし，演習環境サーバ上で稼働している仮想マシン群において攻撃・防衛ツールを使う．SEED[5]は，学習者のための仮想マシンネットワークの実現のための演習コースである．学習者は二人一組となり，相手のネットワークを攻撃したり，自身のネットワークを相手の攻撃から防衛したりする．Tele-lab より SEED は学習者により高度なスキルを習得できる．しかしながら，これらの手法は問題点 2 の倫理問題を解決するものではない.

内田は，ネットワークセキュリティを中心とした，技術者・管理者の情報セキュリティ教育の考察を行った[6]．物理的側面での情報セキュリティは比較的古くから検討されてきたが,インターネットを中心としたネットワークセキュリティは新しくて進歩が激しいため，専門家が不足しており，専門家の育成が大きな課題となっている．また，情報セキュリティの教育方法を，講義形式や事例による講義，実習・実技，ケーススタディ・プレゼンテーション形式に分類した．また，情報セキュリティ教育の内容を，情報セキュリティの基礎，情報セキュリティ技術，ネットワーク技術，Windows セキュリティ，UNIX セキュリティ，情報セキュリティ管理などに分類した．我々は，このような有用な研究成果を取り込み，実践的に学べる環境の構築を目指す．また，今後，本研究の目的にあるような，ネットワークを継続的に管理する演習を可能にすることで,「実習・実技」と「ケーススタディ・プレゼンテーション形式」の両方の要素を更に深く絡み合わせたような演習が可能になるのではないかと考えた.

川橋は情報危機管理における演習を行うための環境を実現した[7].仮想企業の情報セキュリティ担当を演じる参加者と，攻撃役，被害者役を演じる運営者側に分かれ，演習を行う．演習参加者には，演習用ネットワークとして，VMwareServer[8] による仮想 OS 環境を接続した仮想マシンネットワークが与えられる．参加者は 5～6 人の 1 グループで VMware Server Console を用いて遠隔の演習環境にアクセスすることで演習に参加する．参加者のネットワークに対しての攻撃は，運営者側で行う．川橋の研究においては，攻撃を行うのは運営者側であり，攻撃を行うために大きな負担がかかることが問題であると言える．本システムでは，攻撃を行う仮想クラッカー機能を開発することで，この問題を解決する．

3 仮想マシン技術

本システムは，我々がこれまでに開発してきたネットワーク管理者育成支援システム Linux Network Simulator (以下LiNeS)[9]を基盤技術として利用する.LiNeS では,仮想マシンソフトウェア User-mode Linux（以下 UML）[10]を活用して仮想マシンネットワークによるネットワーク管理演習環境を実現している．仮想マシンソフトウェアは，1 台のコンピュータの資源で，複数の OS を同時に動作させることのできるソフトウェアのことである．一般的には，サーバ統合や開発したソフトウェアのテスト環境の実現などに利用される．一台のコンピュータ上で，仮想環境ソフトウェアによって仮想マシン上で動作する OS をゲスト OS，ゲスト OS を動作させる土台の OS をホスト OS という．代表的な仮想環境ソフトウェアとしては，UML の他に，VMware などが挙げられる.

UML は，Linux 上で動作する特殊な Linux であり，複数の Linux を同時に動作させることができる．仮想的に動作させた Linux においては，Linux アプリケーションを動作させることが可能である．例えば，UML カーネルと Red Hat Linux のルートファイルシステムを組み合わせることで，Linux 上で仮想的な Red Hat Linux を動作させることができる．このように，UML によって仮想的に作り出された環境上で Linux を動作させることができる.UML は仮想的なネットワークデバイスを持っており， UML 付属ツールである uml_switch によって，仮想 Linux 間のネットワーク通信を行うことができる．UML スイッチによって接続された仮想ネットワークは,外部のネットワークとは独立したネットワークを構成する．そのため,この仮想ネットワークは,外部から攻撃を受ける可能性や，外部ネットワークに悪影響を及ぼす可能性がない．これにより，予定外の

事態が起こらず，安定したシステムで演習を行えるというメリットがある．また，安全性の確保や，演習を行う際の教師の負担を軽減することにも繋がる．

4 仮想マシンネットワーク制御システム LiNeS

我々が開発してきたシステム LiNeS[9]は 1 台の Linux 計算機上で動作し，学習者に UML による仮想マシンネットワークを提供する．学習者は，LiNeS 制御用 X クライアントから仮想マシンネットワークのトポロジーを仮想ネットワーク機器のアイコンのマウス操作により作成する（図 3）．また，各仮想ネットワーク機器の制御ウィンドウにより仮想ネットワーク機器を設定する（図 4）．

LiNeS における仮想ネットワーク機器は,UML カーネルとルートファイルシステムを組み合わせることで実現されており，その起動は GUI からマウス操作で行う．また，それぞれの仮想ネットワーク機器を UML の付属ツールで接続することで，１台のコンピュータ上で仮想的なネットワークを構築することができる． UML はメモリ消費が少ないため，1 台のコンピュータ上でより多くの仮想ネットワーク機器を同時に起動できる．このため，多数の機器が必要なネットワーク構築・管理演習において，十分な仮想機器を用いて演習を行える．また,UML の起動は,UML カーネルとルートファイルシステムのイメージファイルで行われる．そのため，障害が起きても，ルートファイルシステムのイメージを交換するだけで問題を解決することができる．このことから，試行錯誤を伴うネットワーク構築・管理演習に適している．

UML 付属ツールである uml_switch によって実現される仮想ネットワークは，外部ネットワークからは独立したネットワークを構成する．そのため，このネットワークは，外部から攻撃を受ける可能性や外部ネットワークに悪影響を及ぼす可能性がない．これにより，予定外の事態が起こらず，安定したシステムで演習を行えるというメリットがある．これに加え，安全性の確保や，演習を行う際の教師の負担を軽減することにも繋がる．

LiNeS は，1）仮想マシンネットワークのトポロジーの編集のための API，および 2）各仮想ネットワーク機器の制御のための API を提供する．前者は，例えば，新たに仮想ネットワーク機器を追加したり，既存の機器の接続先を変更したりすることを可能にする．後者は,仮想 Linux サーバ,仮想 Linux ルータ,仮想 Linux クライアントに対して，起動状態の変更と Linux コマンドの実行を可能にする．仮想スイッチングハブに対して，起動状態の変更を可能にする．

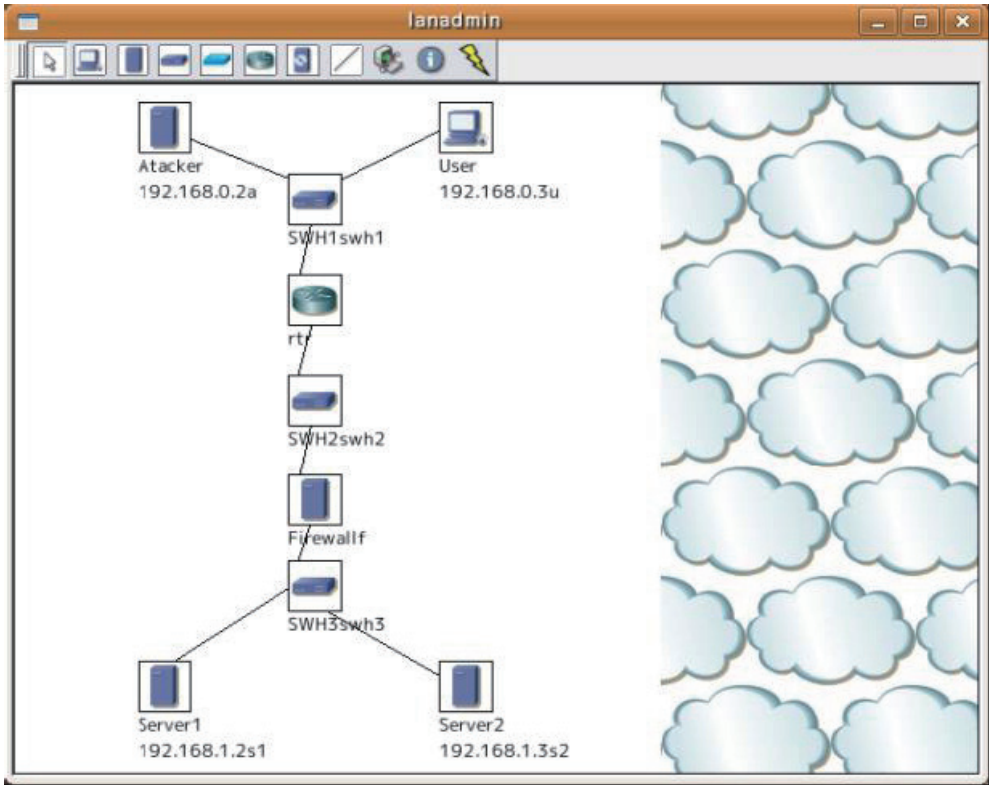

図 3：LiNeS ネットワーク構築用 GUI

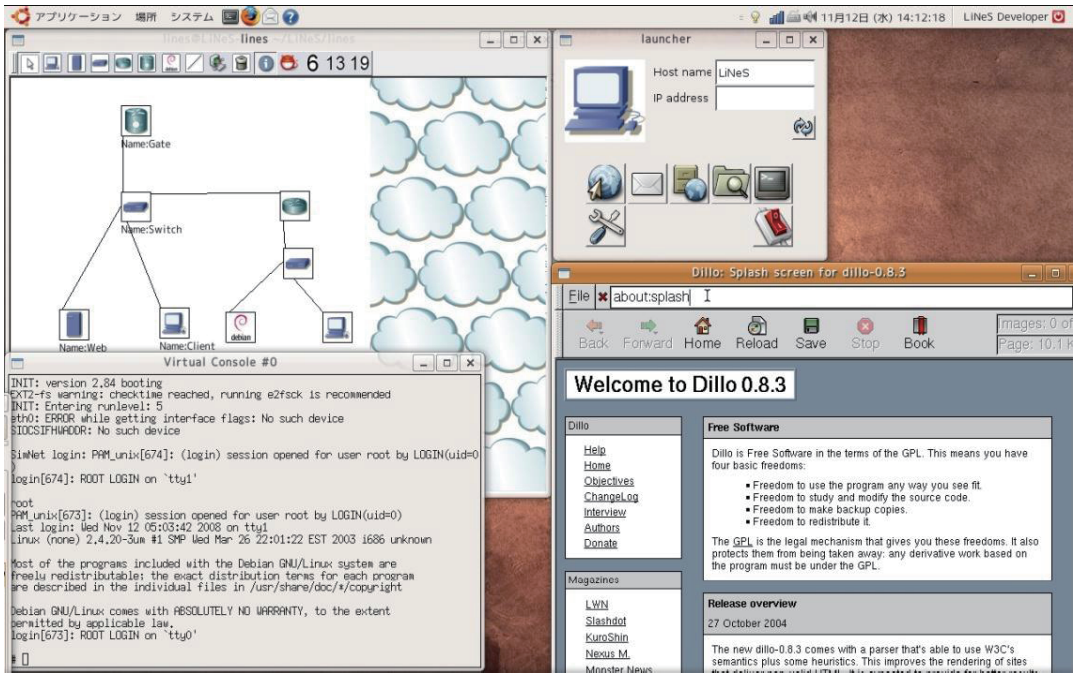

図 4：LiNeS の実行例

5 システムの実現法

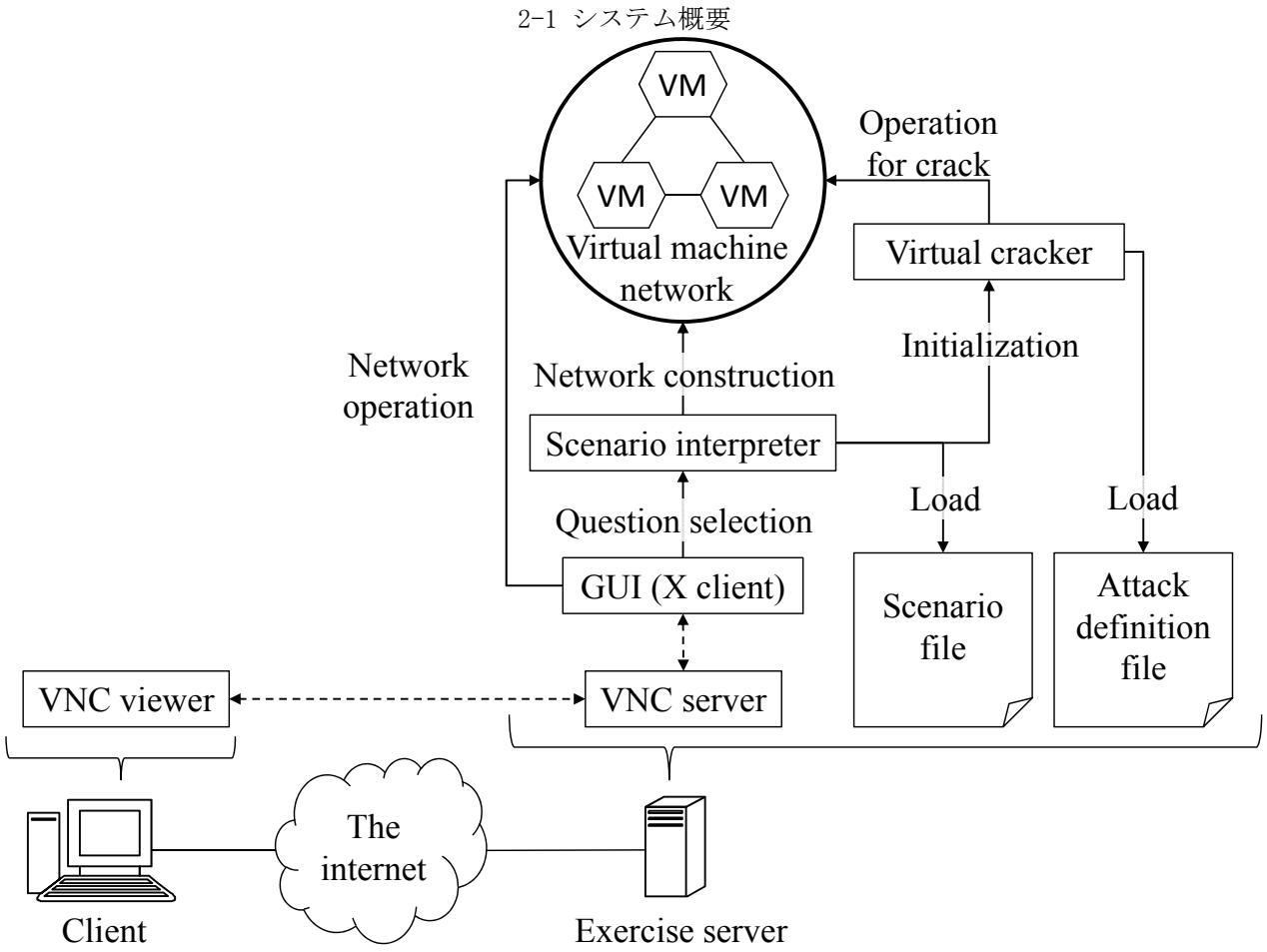

図 5：システム構成図

図 5 に本システムの構成図を示す．本システムは，学習者の仮想マシンネットワークが動作している演習

用サーバと学習者のクライアントから構成される．演習用サーバ（Exercise server）と学習者のクライアント（Client）は，インターネットに接続され，演習用サーバから学習者のコンピュータに演習用の画面が転送される．仮想クラッカー（Virtual cracker）は，攻撃定義ファイル（Attack definition file）から読み込んだクラッキング情報に従い，学習者の仮想マシンネットワーク（Virtual machine network）への攻撃を行う（第 5-2 節）．

演習の準備として，教師は演習シナリオファイル（Scenario file）に演習用ネットワークの構成情報を，攻撃定義ファイルに演習用ネットワーク内でのクラッカーの行動を記述しておく．学習者はインターネットに接続されたクライアントコンピュータから遠隔の演習用サーバにログインし，仮想マシンネットワークを一定期間に渡り管理する.学習者の仮想マシンネットワークは,演習シナリオファイルの演習情報に基づき，演習シナリオファイル解釈機能（Scenario interpreter）により構築される．

5-1 ネットワークセキュリティ遠隔演習システム

我々は，仮想マシン User-mode Linux(以下 UML)[10]から構成される仮想マシンネットワークを用いた，Linux ネットワーク管理者育成支援システム LiNeS(Linux Network Simulator)の開発を行ってきた[9]．UML は Linux エミュレータであり，Linux-OS 上で動作する．仮想マシンネットワークは，仮想 Linux サーバ，仮想 Linux ルータ，仮想 Linux クライアント，および仮想スイッチングハブである．

また，LiNeS を遠隔 PC から操作可能にするために，LiNeS を稼働させ，VNC[11]による遠隔操作を受け付けるサーバを構築した．これにより，一人の学習者が演習に用意する機材は，ネットワークに接続されており，VNC のインストールされた PC1 台である．本研究では，図 5 の演習サーバにこのサーバを用いている．

学習者は，LiNeS の提供するネットワークトポロジー設計用 GUI を用いて，マウス操作でネットワークのトポロジーを作成する．また，仮想 Linux サーバ，仮想 Linux ルータをコンソールにより設定し，仮想 Linux クライアントを GUI により設定する．また，LiNeS はネットワーク定義データに基づき，仮想マシンネットワークを自動的に構築する．教師は，ネットワーク定義ファイルに，ネットワークトポロジー，および仮想ネットワーク機器の初期設定を記述できる．教師がこの仮想マシンの初期設定に，攻撃ツールの実行を設定することで，システムは攻撃発生のあるネットワークを学習者に提供する．

しかし，この方法は仮想ネットワークの初期化時に，各ネットワーク機器でツールを実行するものであるため，学習者の管理によって変化したネットワークを攻略できない．そこで，我々は仮想クラッカーを提案する．

5-2 仮想クラッカーの実現法

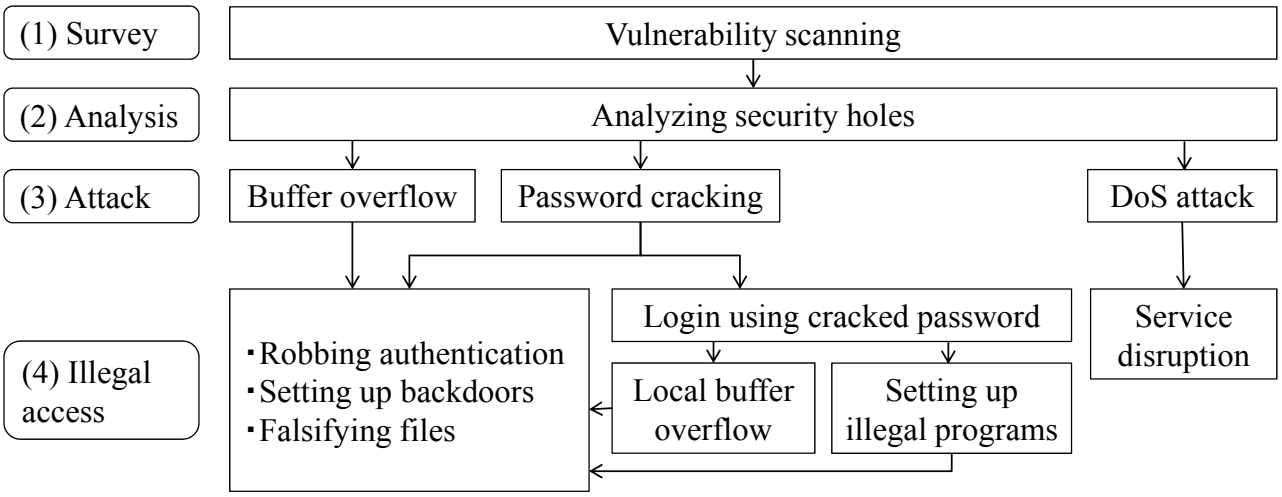

図 6：クラッカーの動作フロー

図 6 は本システムにて実行される攻撃の流れである．

仮想クラッカーは各々のフェーズにおいて，A）時刻に基づく動作，B）攻撃ツールの実行結果に基づく動作，および C）仮想ネットワークの状態に基づく動作を行う．A）の時刻は絶対時刻と相対時刻である．絶対時刻は GMT であり，相対時刻は演習開始時刻からの経過時間および，仮想クラッカーの任意の動作からの経過時間である．B）は，ポートスキャン結果（nmap[12]），および攻撃の成否（THC-Hydra[13]，Metasploit[14]）である．C）では，仮想ネットワーク機器の保持している情報（例えば，稼働プロセスやサーバソフトウェア設定）を分析する．これらの機能は，第 4 章で述べた 1）の API により仮想ネットワーク機器を検索し，2）の API によりその仮想ネットワーク機器の情報を取得し，それを分析することで実現する．

クラッカーは，図 5 の攻撃定義ファイルの記述に基づき行動する．このファイルは表 1 に示す XML タグを用いたプロダクションルールにより構成される．イベントタグは図 6 の(1)～(4)におけるクラッカーの行動を定義する．属性は各イベントの実行条件を定義する．

表 1：攻撃定義のための XML タグの一部

属性	説明
id	イベントの ID
time	イベントを実行する時刻
wait	イベントの実行前の待機時間
success	イベントが成功した後で実行するイベントの ID
failure	イベントが失敗した後で実行するイベントの ID
タグ	説明
netscan	ネットワークスキャン
search	仮想ネットワーク機器のファイルを検索する
passwordattack	THC-Hydra によるパスワードアタック
metasploit	Metasploit による攻撃
ssh	ssh によるリモートアクセス．子ノードに command タグを持つことができる．
command	ssh によるリモートログイン後に実行する Linux コマンド

6 システム実行例

学習者はインターネットに接続されたクライアントコンピュータを利用して,演習用サーバへ VPN 接続し，演習用画面を操作する．図 7 は，演習の画面の一例である．学生は Windows PC を使用しており，VNC ビューワの中で LiNeS の仮想マシンネットワークを操作している．

この演習の流れは以下の通りである．学習者がシステムに提示された課題を選択すると，システムが学習者の管理する仮想ネットワークを自動構築し，それを学習者に提示する．一定時間が経過すると，攻撃定義ファイルに基づき仮想クラッカーが動作を開始する．本実行例では学習者の管理するネットワーク内のサーバに対して SSH ブルートフォースアタックを行い，図 8 のようなログが残る．この仮想クラッカーは root ユーザのパスワードの取得に成功した後，バックドアを作成する．

次の仮想クラッカーの行動分岐は，バックドアの有無により分岐される．学習者は，演習用クラッカーの攻撃に気が付き，サーバ上でバックドアを発見・削除した場合，バックドアの発見・アクセス制限を行った場合には，ターゲットとなるマシンに対して DoS 攻撃を行う．学習者は，ブラウザで web サーバへ接続し，web ページを表示しようとするが，失敗する．これにより異常に気がつき，ログを確認し，攻撃への対策を行うこととなる．

学習者が仮想クラッカーの攻撃に全く気がつかなかった場合,上述で挙げた以外の対策を行った場合には，仮想クラッカーが作成したバックドアから再度アクセス可能なままとなっている．そこで，仮想クラッカーは，再度バックドアから不正アクセスを行い，web ページの html ファイルを削除する攻撃を行う．クライアントのブラウザを起動し，web ページにアクセスすると，ページが表示されない．学習者は，ここから異常に気がつくこととなる．その後，異常なログを探し出し，攻撃への対策を行うこととなる．

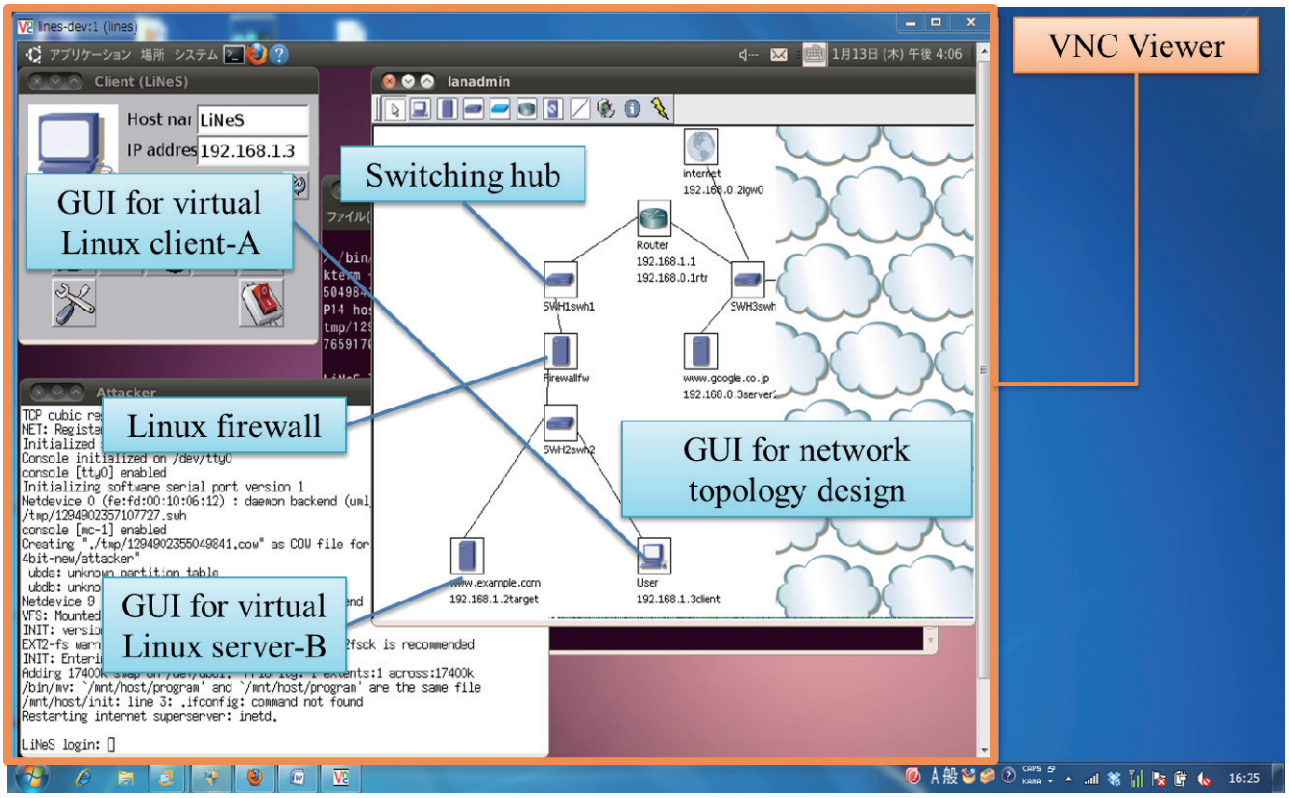

図 7. 演習用サーバへのアクセス

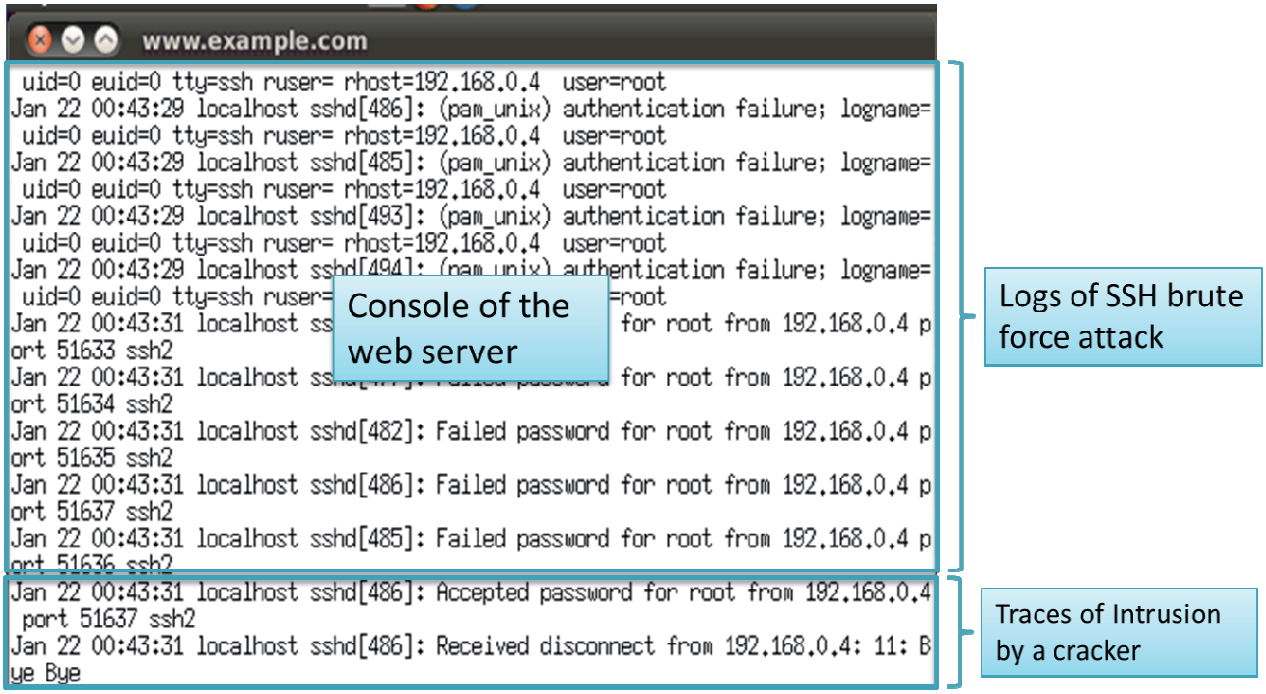

図 8：仮想クラッカーによるサーバへの SSH ブルートフォース攻撃と検知ログ

7 評価実験

7-1 評価実験の目的

評価実験の目的は 2 つある．一つ目は，演習内容と学習者の知識・スキルとの妥当性を明らかにすることである．このシステムは，ネットワーク構築とネットワークセキュリティ基礎に関するスキル/知識を持った人々を対象にしている．そこで，演習中の学習者の行動を分析する．もう一つは，このような演習の必要性

と有効性を明らかにすることである．座学による学習の後で，本システムによる演習を実施し，ユーザの意見をアンケートにより収集する．

7-2 評価実験の概要

被験者は，ネットワーク構築経験のある情報系大学生・大学院生の 12 名で，実験者は申請者らである．実験手順は以下の通りである．

1. 被験者は DoS 攻撃，ブルートフォースアタック，バックドア，バッファオーバフローといったクラッキングに関する記事を読む．また，実験者は必要に応じてレクチャーを行う．

2. システムを利用しネットワーク管理演習を行う(約 20 分程度)．実験者は演習中の行動を観察し，クラッカーの行動を分岐させる行為があったかを記録する．被験者は演習中に行った設定変更についてメモをとる．

3. 被験者は本システムの評価アンケートを記入する

被験者は我々のシステムで仮想マシンネットワークを安全に管理するという課題に取り組む．仮想マシンネットワークは図 7 に示したネットワークトポロジーである．このネットワークは以下の要件を満たさなければならない．サーバは，ウェブページの公開を目的としたもので，ウェブサービス，FTP サービス，SSH サービス，TELNET サービスを稼働している．クライアントのユーザはサーバに対して，ウェブページを FTP でアップロードし,SSH と TELNET のパスワード認証で遠隔ログインし,WWW サーバソフトウェアを設定する．

さらに，被験者は行動ルールと呼ぶ以下のルールに従わなければならない．

・あなたがサーバに対しできることは，ログの閲覧，/etc 以下の設定ファイルの閲覧，/etc 以下の設定ファイルの書き換え（/etc/apache/以下を除く），および各サービスの再起動だけである．

・あなたがファイアウォールに対してできることは，iptables を利用して外部ホストからの通信の遮断である．

・あなたはネットワークトポロジー，およびその他の機器の編集をしてはならない．

また，被験者へはサーバの脆弱性を知らせない．脆弱性は，管理者権限での遠隔ログインの許可，脆弱なパスワード，およびバッファオーバフローのプロセスの稼働である．

7-3 システムの妥当性の評価

実験時に用いた演習用クラッカーの動作フローを図 9 に示す．本評価実験で用いた仮想クラッカーは，前半の 10 分間および後半の 10 分間における被験者の行動により，その後の行動を選択する．評価実験中の被験者の行動を観察し，想定された仮想クラッカーの動作と，実際に仮想クラッカーがどのように動作したかを比較した結果を表 2 に示す．仮想クラッカーが攻撃できないような完璧なセキュリティ対策をした学習者は存在しなかった．また，セキュリティ対策を何もしていない学習者も存在しなかった．このことより，対象者と演習内容の整合性は妥当であると言える．

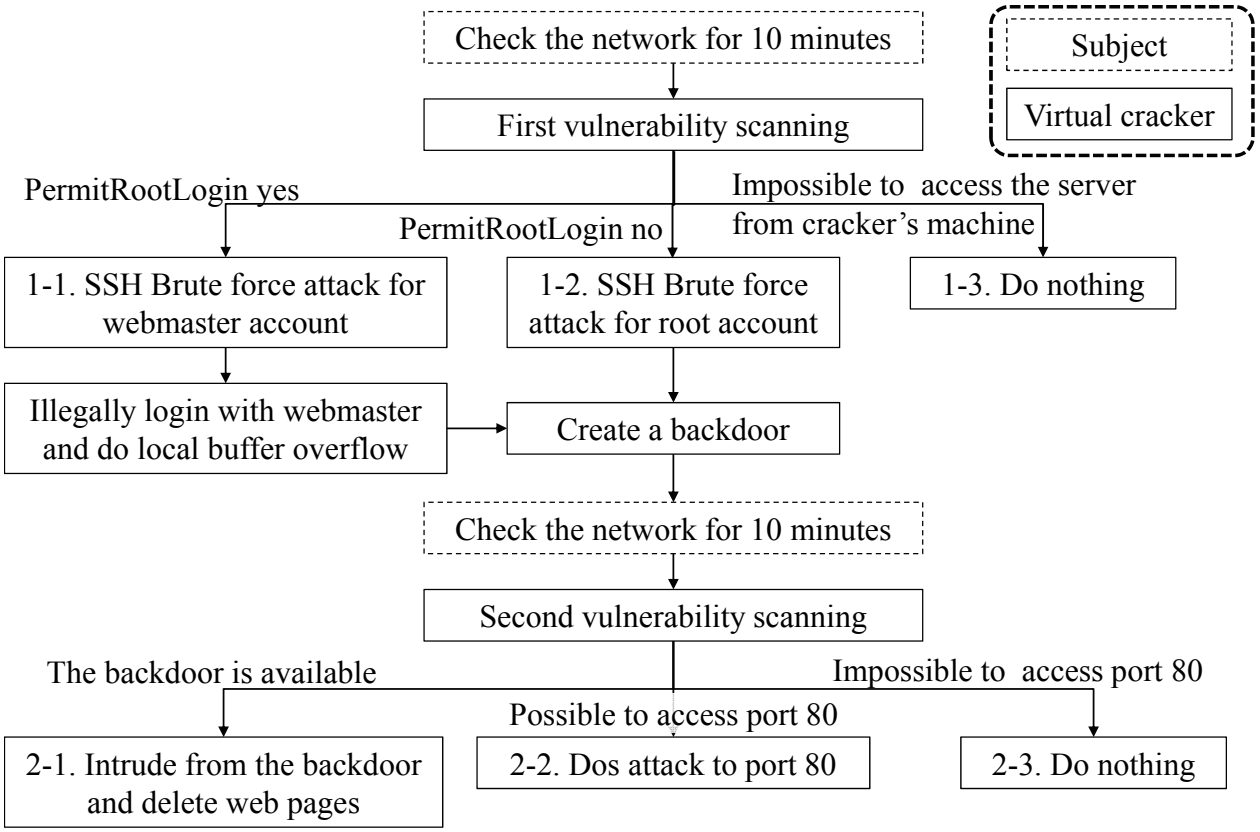

図 9：仮想クラッカーの動作フロー

表 2 被験者の行動と演習用クラッカーの動作比較

クラッカーの動作	被験者の行動から想定された人数	実際の人数
図 9 中 1-1 の動作	1	1
図 9 中 1-2 の動作	11	11
図 9 中 1-3 の動作	0	0
図 9 中 2-1 の動作	6	6
図 9 中 2-2 の動作	2	2
図 9 中 2-3 の動作	4	4

7-4 システムの必要性と有効性に関する評価

システム利用に関する評価アンケートの項目と結果を表 3 に示す．評価アンケートの回答は，5 段階評価｛5. そう思う｜4. どちらかといえばそう思う｜3. どちらともいえない｜2. どちらかといえばそう思わない｜1. そう思わない｝とした．

質問 1 と質問 2 は，実際のツールを用いて実践的に行う演習が，ネットワークを安全に管理するために必要であり有効であることを示している．自由記述[B]は，本演習システムの課題であると言える．この問題は，教師が予め学習者に対して禁止する行動を記述し，学習者がその中の行動を行おうとした際に，システム上で抑止する仕組みを実装することで解決を図る．

表 3 評価アンケートの項目と結果

アンケート項目	平均値
[質問 1] 動的に攻撃の行われるネットワーク上での演習により，クラッキングへの対策の必要性を感じることはできましたか？	4.91
[質問 2]本演習システムを利用することで，クラッキング防衛方法に対する理解が深まりましたか？	4.66
自由記述	
[A]個々の攻撃方法・対策方法を知っていても，それをどのように利用したらいいのか分からないので，今回のような実践的な演習を行うことは印象に残るし，重要であると感じた. [B]遠隔演習環境となっているので，実際に運用する際には，教師がいない場で生徒が想定外の行動をしてしまわないようにする方法について検討が必要.	

8 おわりに

本研究では，演習用サーバを用いた遠隔セキュリティ演習環境に，自動的に攻撃を起こす仮想クラッカーを導入することで，攻撃の検知と防衛方法のみを手軽に学ぶことのできるネットワークセキュリティ演習システムを実現した．評価実験により，本システムによる演習の必要性，有効性，および妥当性を評価した．学習者の行動および評価アンケートの分析結果より，本研究の目的を達成できたといえる．今後の課題は，学習者の行動ルールの厳守をサポートするためのユーザインタフェースを開発すること，より複雑な攻撃を行うための仮想クラッカーの改良などがあげられる．

【参考文献】

[1] 独立行政法人情報処理推進機構,『情報セキュリティ白書 2010』, 独立行政法人情報処理推進機構, p.27 (2010).

[2] 独立行政法人情報処理推進機構,『情報セキュリティ白書 2010』, 独立行政法人情報処理推進機構, p.58 (2010).

[3] 仲間正浩:“ネットワークセキュリティ教育のためのネットワーク教育環境の構築と実習”, 琉球大学紀要, pp.213-219 (2001).

[4] Ji Hu, Christoph Meinel, Michael Schmitt : “Tele-lab IT security: an architecture for interactive lessons for security education”, ACM SIGCSE Bulletin, Volume 36 , Issue 1 SESSION: Computer security, pp.412 - 416 (2004).

[5] Wenliang Du, Ronghua Wang : “SEED: A Suite of Instructional Laboratories for Computer Security Education”, Journal on Educational Resources in Computing (JERIC) , Volume 8 , Issue 1, Article No. 3 (2008).

[6] 内田勝也, “技術者・管理者向け情報セキュリティ教育試案”, 日本セキュリティマネジメント学会第 16 回全国大会(2002).

[7] 川橋裕:“情報危機管理における演習環境の構築と運用”, 情報知識学会誌, Vol. 20, No. 3, pp.239-248 (2010).

[8] VMware Server - 無償のサーバ仮想化製品: http://www.vmware.com/jp/products/server/.

[9] Yuichiro TATEIWA and Takami YASUDA, ″Multiuser Network Administration Training in LiNeS: Connection Function between Virtual Networks,″ Proc. of KES-IIMSS 2009, SCI 226, pp. 535-544, Italy. (July15-17, 2009)

[10] The User-mode Linux Kernel Home Page. http://user-mode-linux.sourceforge.net/index.html.

[11] RealVNC - RealVNC remote control software:http://www.realvnc.com/.

[12] Nmap - Free Security Scanner For Network Exploration & Security Audits.:http://nmap.org/.

[13] THC-HYDRA - fast and flexible network login hacker: http://freeworld.thc.org/thc-hydra/.

[14] Penetration Testing | The Metasploit Project: http://metasploit.com/.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Remotely Accessible Exercise Environment for Intrusion Detection/Defense Exercises Based on Virtual Machine Networks	Proceedings of the Second KES International Symposium IDT 2010	2010 年 7 月
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環境の開発	電子情報通信学会技術研究報告	2011 年 3 月
仮想マシンネットワークを用いた初学者向け IP ネットワーク構築演習の自動評価システムの実現	電子情報通信学会技術研究報告	2011 年 3 月
仮想マシンを用いたネットワーク構築演習のための演習履歴データベースシステムの実現	2011 年度春 JSiSE 学生研究発表会	2011 年 3 月
高機能仮想ハブによる異種構成・分散配置型仮想マシンネットワークの実現とネットワーク構築演習への応用	電子情報通信学会論文誌	2011 年 5 月