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

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

インターネットを始めとするネットワークの発展に伴い，セキュリティの知識を持ったネットワーク管理者の必要性が高まっている．そのため，ネットワーク管理者に向けたセキュリティ演習環境のあり方について見直す必要が出てきている．現在行われているネットワークセキュリティ演習では，実験室に演習用のネットワークを構築し，攻撃側と防衛側に分かれて攻撃・防衛実験を行ったり，攻撃・防衛ツールの使用実験によりその結果を考察したりする．このような演習方法は，授業時間内において実験室で行うため，演習のための時間と場所を大きく制限してしまう．また，学習者に攻撃方法を教えることになるため，倫理上の問題が指摘されている[1]．

近年では，ネットワーク管理演習環境の構築に仮想化技術が利用されることが多い．仮想化技術とは，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技術のことである．その代表的なソフトウェアに VMware や Xen があげられる．これらは，主に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．そのような仮想化技術がネットワーク管理演習環境の開発に利用されるのには，実機で演習を行う場合と比較し，次の 2 つの利点があるからである．まず，1 つ目は，費用や手間がかからず，演習を行いやすいことである．実機で演習を行う場合，高価なネットワーク機器を多数準備する必要があり，経済的負担が大きい．また，それらのネットワーク機器の準備や後片付けを行うためにかかる手間も大きい．2 つ目は，学習効果が上がることである．実機で演習を行う場合，前述の 1 つ目の理由から，学習者一人一人に実機を与えることが難しく，演習がグループ活動によって行われる傾向にある．その結果，グループ内の数少ない学習者が多くの作業を行うなど，一人一人の演習時間が不足し，学習効果が下がっている．一人一人に十分な演習時間を与えることができるようにするために，仮想化技術が利用される．

そこで本研究では，1）時間と場所の制限を改善するために仮想マシンによる遠隔演習環境の構築を行い，2）攻撃検知・防衛方法に絞った演習のために，自動攻撃機能の開発を行う．学習者はインターネットに接続した計算機から演習環境サーバにアクセスすることで，自動攻撃機能が自動的に攻撃する仮想マシンネットワークにおいて，検知・防衛方法を演習する．

2 関連研究

Ji Hu は，ブラウザと VNC アプレットを用いて，遠隔地からシステム内の仮想マシンにアクセスし，ネットワークセキュリティの概念とツールの使用方法を学習するためのシステム Tele-lab IT security を開発している[2]．SEED も，仮想マシンによるネットワークセキュリティ演習システムである[3]．学習者はパートナーのネットワークを攻撃したり，パートナーからの攻撃を防いだりする．学習者は Tele-lab よりテクニカルなスキルを学習できる．しかし，これら 2 つのシステムは，実施は倫理上の問題を解決していない．

仲間は，セキュリティ対策を行える人材を育成するため，攻撃を直接受ける安全でないネットワーク環境を実現した[4]．しかし，初心者がいきなり外部に完全に開放された環境で実習を行えば侵入されてしまう危険性が高いので，学習者のスキルをどのようにスキルアップするか，それぞれのレベルでどのような環境を利用すべきかを検討した．その結果として，外部から侵入される危険性がほとんど無い安全なネットワーク環境から，段階的に侵入の危険性を徐々に増した環境へと実習環境を移行していくネットワークセキュリティ教育の必要性を主張した．また，手順や合格基準などの具体的な教育方法を提案し，１つの例として，実際にそれを実現できる環境を構築した．しかし，「セキュアでない環境を構築し，外部からの攻撃を期待したが，実際には攻撃・侵入までいたらなかった」という報告もあり，本研究で開発したシステムのような安定した演習環境は実現できていない．

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[5]．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．

3 本研究での攻撃検知・防衛演習

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．

4 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）[6]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）[7]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．また，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 スイッチによって，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．

5 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 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 1）．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．

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．

本研究では，この LiNeS を基盤としてシステムを構築する．そのために，前述した LiNeS の機能に加えて，LiNeS の以下の機能を活用する．

・UML 内のファイルをホスト OS から取得する機能（ファイル取得機能）

・設計データに基づいた仮想マシンネットワークの自動構築を行う機能（仮想マシンネットワーク管理機能）．

・起動時に設計データに指定されたホスト OS 上のファイルを UML 内に自動的に取り込んだり，設計データで指定されたシェルコマンドを UML 内で実行したりする機能（UML 自動初期化機能）

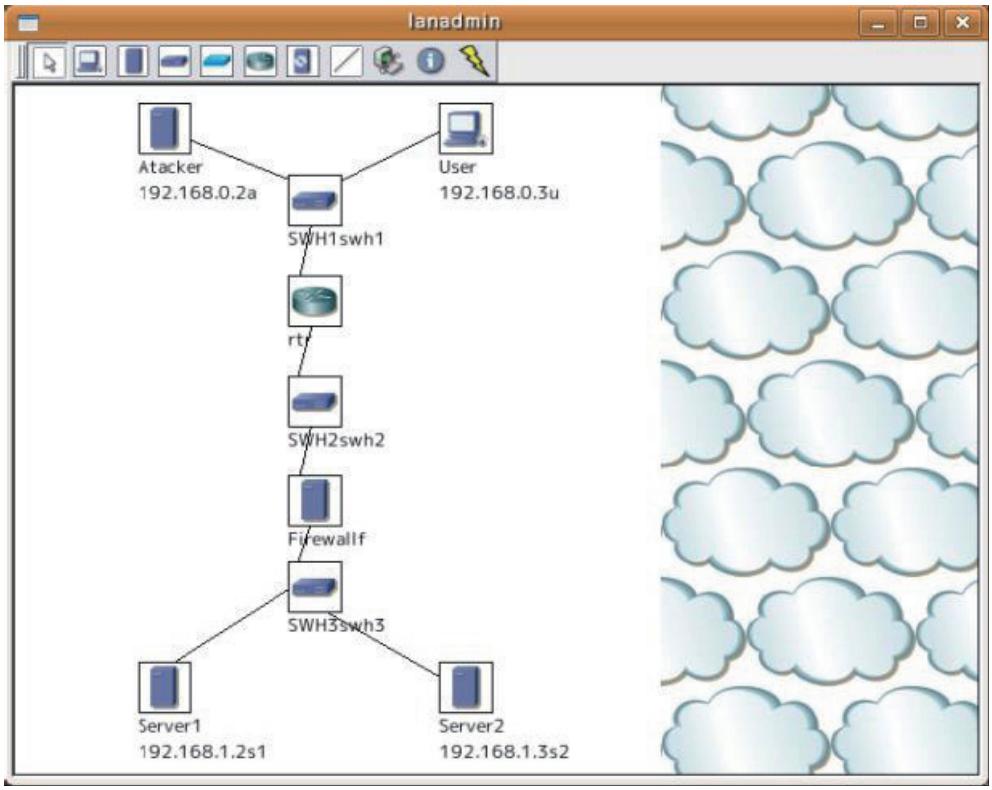

図 1：LiNeS ネットワーク構築用 GUI

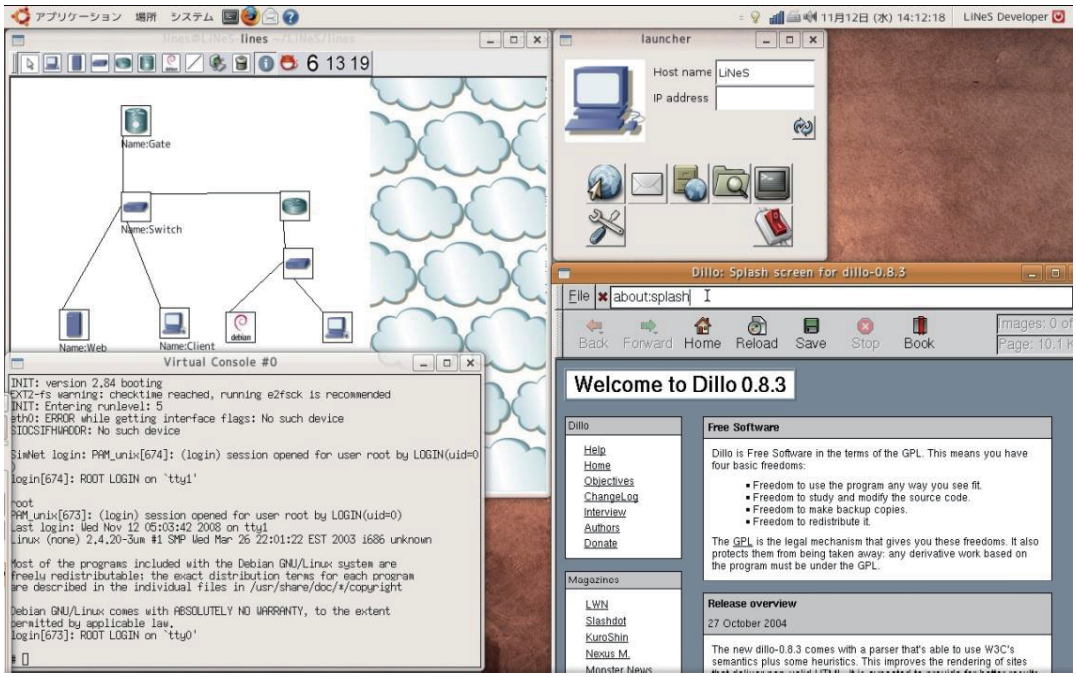

図 2：LiNeS の実行例

6 システムの実装

図 3 に本システムの構成図を示す．本システムは学習者用の PC と，遠隔学習環境提供用のサーバから構成される．学習者用 PC と演習用サーバはインターネットに接続され，TCP/IP 通信が可能である．

我々がこれまでに開発してきたシステム LiNeS は，仮想マシンネットワークを実現し制御する機能を有する（仮想マシンネットワーク管理機能）．しかしながら，スタンドアローンで利用することを想定したシステムであるため，遠隔操作のための機能を有していない．本研究では，LiNeS に基づいた仮想マシンネットワーク管理の遠隔演習環境の構築を行う（演習用サーバ，VNC サーバ，VNC ビューア）．

攻撃検知演習の前に，攻撃に対して実感を持たせることが大切であると考える．そのため，攻撃によるログとシステム状態との変化をわかりやすく見せることが役に立つ．しかし，これらのシステム情報は膨大であり時間とともに変化するものもあるため，攻撃の理解に必要な情報を効率的に示すことは難しい．そこで，各攻撃に対するシステム情報の変化を抽出し表示するためのシステム情報抽出表示機能を開発した．

学習者に攻撃作業を行わせるのは倫理上の問題を伴う．学習者の演習内容を攻撃検知・防衛方法に限定するために，教師の指定したタイミングで，指定した種類の攻撃を行う自動攻撃機能を開発する．

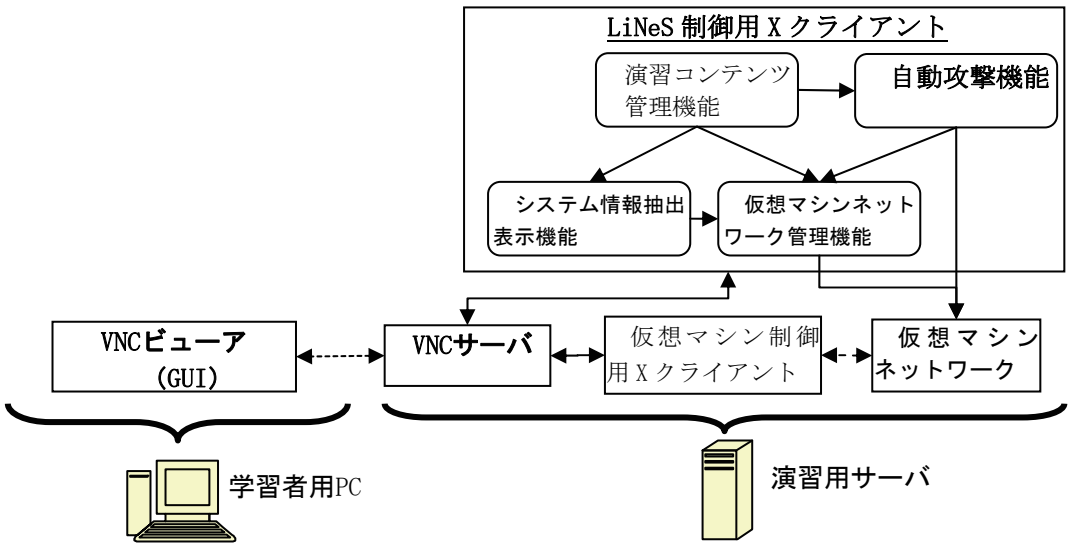

図 3：システム構成図

6-1 仮想マシンネットワーク管理の遠隔演習環境の構築

１台の演習用サーバに学習者の演習環境を集め，その演習用サーバから学習者のコンピュータに学習者用の演習画面を転送することで環境を実現する．

サーバ上に学習者用の仮想マシンネットワークを構築し,学習者用 PC からはサーバの仮想マシンネットワークを操作することになる．仮想マシンネットワークの操作は GUI を通して行われるため，サーバ上の GUI をクライアントから操作できる必要がある．本研究では，VNC サーバ・VNC ビューア[8]を利用して，演習用サーバから学習者のコンピュータへ演習画面を転送することにした．

VNC サーバ・VNC ビューアは，他のコンピュータの画面をネットワーク経由で転送できるフリーソフトウェアのことである．操作される側に VNC サーバ，操作する側に VNC ビューアをインストールすることで，ネットワークを通して，物理的に離れたコンピュータを操作することができる．X クライアントが X プロトコルを利用して VNC サーバと通信し，その描画命令を VNC ビューアに転送する． しかし，VNC サーバと VNC ビューアの間の通信は，前述の X Window System とは異なり，X プロトコルではなく，VNC プロトコルを利用して行われる．また，VNC はクロスプラットフォームなソフトウェアとして開発されているため，OS などのプラットフォームの種類に依存することなく，通信を行うことができる．つまり，VNC サーバも VNC ビューアも Windows に対応しているため,Windows であることが多いと考えられる学習者のコンピュータにも画面転送を行うことができる．

6-2 システム情報抽出表示機能

クラッキング対象となった仮想マシンのシステムファイル，システムログ，システム状態，Snort[9]ログを材料とする．このデータ膨大であるため，クラッキングの理解に必要なデータにキーワードで絞り込み，クラッキング行為中のデータの変化のリアルタイム表示(log モード)と，クラッキング前と後の差分表示(diff モード)を行う．diff モードは，攻撃前と攻撃後それぞれのタイミングで一度だけデータを保存・取得する．設定ファイルの指定に合わせ，ファイルのコピー又はコマンドの出力から，擬似端末を利用し共有ディレクトリにファイルを作成する．そして，前後のデータと diff によって得られたデータを解析＆可視化機能へと引き渡す．この際，diff には--unified オプションを指定した．本システムにおいては時間による前後が明確に存在するため,”--“と”++“によって差分を示す形式が適当と考えた．教師の設定に基づいて，攻撃前後の差分データおよびキーワードを含む行を抽出し，色付けなどの見やすい形で表示する．

6-3 自動攻撃機能の開発

現実世界のクラッカーは，ネットワークに接続した計算機から攻撃対象に攻撃を行う．本研究でも，仮想マシンネットワークに接続した仮想マシンから攻撃対象の仮想マシンに攻撃を行うようにする．具体的には以下の要件となる．

要件 1）既存の攻撃ツールを攻撃に使用できること

要件 2）攻撃対象の仮想マシンネットワークが学習者に自動的に提示されること

要件 3）攻撃ツールと攻撃発生のタイミングを教師が指定できること

要件 1）のために，既存の攻撃ツールがインストールされている攻撃用仮想マシンを構築した．要件 2）の

ために，仮想マシンネットワーク管理機能を拡張し，攻撃用仮想マシンを含んだ仮想マシンネットワークを構築できるようにした．要件 3）のために，UML 自動初期化機能に基づいたシナリオ記述方式を考案した．教師が指定した時間通りに攻撃を発生させるために，攻撃用仮想マシンに atd を導入した．また，既存の攻撃ツールには，シェルコマンドとして実行できるツールだけでなく，対話型のツールも存在する．これによる攻撃を行えるようにするために，定型処理の自動化が可能である expect[10]を利用する．

7 実行例

実行環境を図 4 に示す．演習環境サーバ用の計算機は，Dell PowerEdge（CPU：IntelR XeonR CPU E5420 @2.50GHz，メモリ：2.0GB，ギガビットネットワークインタフェース）を使用した．学習者用 PC は，Dell Studio（CPU:IntelR Core2 Duo P8400 @2.26GHz，メモリ：4GB，ギガビットイーサネットネットワークインタフェース）を使用した．

図 5 では，VNC ビューワにより学習者用 PC から演習環境サーバのデスクトップ画面の LiNeS を操作している．表示されているウィンドウは，演習メニューである．演習メニューを選択すると図 6 が表示される．メニューで選択した攻撃に必要な仮想マシンネットワークが自動的に構築されており，学習者は丸で囲んだボタンをクリックすることで，システムに攻撃を開始させる．システム情報抽出機能により，攻撃対象マシンのシステム情報を抽出して表示している（図 7，図 8）．図 7 は，IDS ツールの Snort のログをリアルタイムに整形して表示している．図 8 は，攻撃前後のシステム状態を整形して表示している．学習者は，攻撃の検知の演習の前に，検知対象となる攻撃の影響を理解することができる．

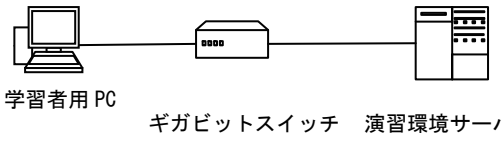

図 4：実行環境

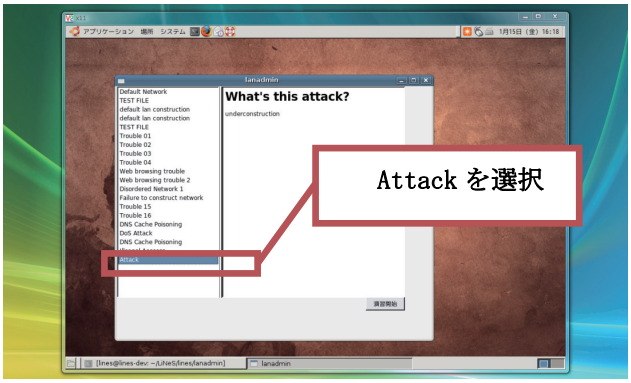

図 5. VNC ビューワによる遠隔演習画面

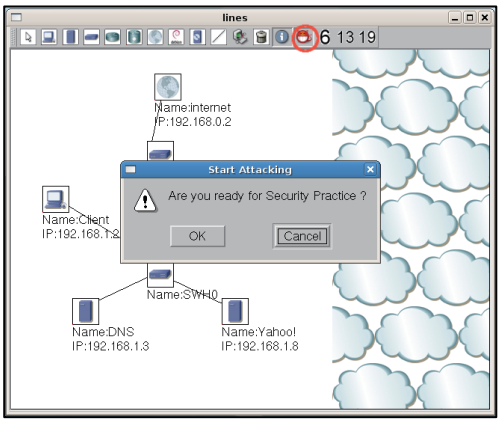

図 6：仮想マシンネットワークでの攻撃

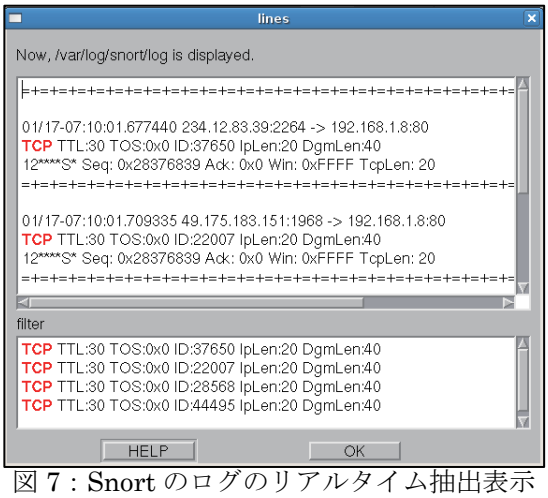

図 7：Snort のログのリアルタイム抽出表示

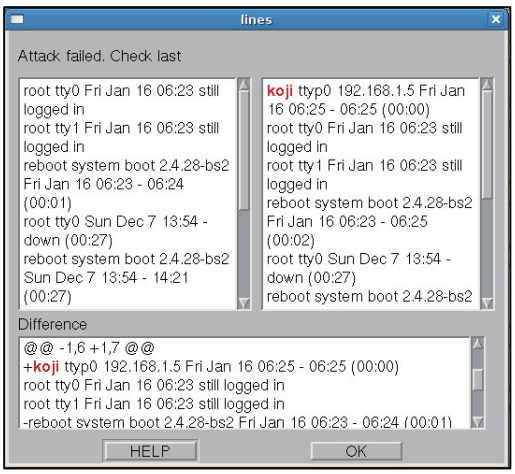

図 8：攻撃前後のシステム情報差分表示

8 評価実験

開発したシステムの評価実験を行い表 1，2，3 に示す結果を得た．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｝である．被験者は，サーバ構築などの経験がある情報系の大学生・大学院生 10 名で，攻撃の概念と防衛方法を書籍により理解した者である．使用した学習者用 PC，演習環境サーバは第 5 章で述べたもので，学習者用 PC は名古屋工業大学に，演習環境サーバは名古屋大学に設置した．学習者用の PC から演習環境サーバまでのネットワークスループットは 94.9Mbps（nttcp[11]により計測）であった．

表 1 は，本演習環境における画面転送方式として VNC サーバ・ビューワが適当であるかの評価である．Q1～Q3 により本演習において VNC サーバ・ビューワは十分な性能であることが示された．表 2 は，システム情報抽出表示機能についての評価結果である．Q1～Q3 より表示内容の効果が高いことが示された．一方，アニメーション表示の要望（コメント 1）は，この機能の効果の改善に重要であると考えられるため，今後の課題とする．表 3 は，自動攻撃機能よる演習の効果の評価である．この評価実験では，攻撃発生と種別を被験者に知らせた場合と知らせない場合の各々において，検知と防衛の作業を行わせた．自動攻撃は，攻撃発生の検知および攻撃の種別の特定に役に立つという評価より，本研究の目的を達成できたと言える．また，コメント 1, 2, 3 はネットワークセキュリティ演習の e-learning システムとして重要な要素であると考えられる．これらの機能の開発は今後の課題としたい．

表 1：遠隔演習環境における VNC サーバ・ビューアの演習での使用感

アンケート項目	平均値
Q1. ネットワーク機器を起動したりそのウィンドウを動かしたりするとき，描画速度は演習にとって許容範囲内でしたか？	5.0
Q2. キーボード入力に対する画面表示にラグがありますが，それは演習にとって許容範囲内でしたか？	4.7
Q3. マウス操作に対する画面表示にラグがありますが，それは演習にとって許容範囲内でしたか？	4.9

表 2：システム情報抽出表示機能についての評価結果

アンケート項目	平均値
Q1. システム情報のリアルタイム表示が，攻撃の効果の理解に役立ったと思いますか？	4.7
Q2. 攻撃前後のデータ比較は，動作の理解に役だったと思いますか？	4.8
Q3. キーワードを色付けなどによって目立たせることがわかりやすさに繋がったと感じましたか？	4.6
コメント 1. アニメーションで状況を把握できるとよい.	

表 3：自動攻撃機能による自動攻撃の演習に及ぼす効果

アンケート項目	平均値
Q1. 任意のタイミングで攻撃されることは，正常な状態と異常な状態を見極めることができ，攻撃の検知方法を学ぶ学習に役立つと思いますか？	4.7
Q2. 任意の種類の攻撃が行われることは，何の攻撃が行われているかを考えることができ，攻撃の検知方法を学ぶ学習に役立つと思いますか？	4.5
コメント 1. ある程度時間が経ったら，どのような攻撃が行われているのかというヒントの表示があると良いと思う. コメント 2. 自分で構築したネットワークに対して様々な攻撃がされるようになると，より体験的な学習ができると思う. コメント 3. より高性能な演習管理機能があると，受講者は授業時間外でも演習できてよいと思う.	

9 おわりに

本研究では，高性能サーバに LiNeS による仮想マシンネットワークを構築し，VNC サーバ・クライアントにより画面転送を行うことで，ネットワークセキュリティの遠隔演習環境を構築した．また，攻撃の効果を表示して学習者の理解を促進するシステム情報抽出機能や，攻撃方法を学んでしまう倫理的な問題を解決するために，自動攻撃機能による攻撃を実現した．評価アンケートの結果，本システムについて高評価を得られた．

今後の課題は，自動攻撃機能の知的化および学習者への演習支援機能の開発である．高度な自動攻撃エージェントは，学習者の演習行動に応じて攻撃行動を決め，より人間のクラッカーに近い存在となる．現状では，誰がどこで何をするかを記述したシナリオに基づいているが，学習者の状況を把握する機能の開発と，シナリオの柔軟な記述形式を開発することで，高度なエージェントを開発する．演習支援機能は，学習者が構築したネットワークの情報を取得し，躓いている学習者の救済をしたり，演習の進捗を管理したりする．これらは，学習者の行動履歴の取得や学習者の仮想ネットワークの状態の分析機能を開発し，それに基づいてヒントを検索し学習者に提示する機能を開発することで実現する．

【参考文献】

[1] James Harris,"Maintaining ethical standards for a computer security curriculum," Proceedings of the 1st annual conference on Information security curriculum development, pp.46-48 (2004).
[2] 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)
[3] 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)
[4] 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", 琉球大学教育学部紀要, Vol. 59, pp.213-219(2001).
[5] 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).
[6] 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)
[7] The User-mode Linux Kernel Home Page. http://user-mode-linux.sourceforge.net/index.html. Accessed 19 February 2010.
[8] RealVNC - RealVNC remote control software:http://www.realvnc.com/. Accessed 19 February 2010.
[9] Snort :: Home Page: http://www.snort.org/. Accessed 19 February 2010.
[10] Expect - Home Page : http://expect.nist.gov/. Accessed 19 February 2010.
[11] nttcp.c: http://sd.wareonearth.com/~phil/net/ttcp/nttcp.c. Accessed 19 February 2010.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
仮想化技術によるネットワーク管理者育成支援システムにおけるサーバ OS インストール演習環境の開発	電子情報通信学会技術研究報告. ET, 教育工学, pp.27-32	2009 年 6 月
Multiuser Network Administration Training in LiNeS: Connection Function between Virtual Networks	Proc. of KES-IIMSS 2009, SCI 226, pp. 535-544	2009 年 7 月
異種・分散型仮想マシンネットワーク構成機能に基づくネットワーク協同管理演習システムの開発	電子情報通信学会技術研究報告. ET, 教育工学, pp.83-88	2010 年 3 月
Evaluation of network construction exercise system LiNeS on the basis of heterogeneous and distributed virtual machine network composition function	International Journal of Knowledge and Web Intelligence (IJKWI), Volume 1, Number 3/4	採録決定（発行待ち）