UML(User-mode Linux)による仮想ネットワーク環境でのネットワーク管理者育成支援システムの開発（継続）

代表研究者　安　田　孝　美　名古屋大学大学院情報科学研究科教授
共同研究者　立　岩　佑一郎　名古屋工業大学大学院情工学研究科助教

1 はじめに

申請者らは，仮想マシンソフトウェア User-mode Linux [1]（以下 UML）の活用により，大学におけるネットワーク管理者育成環境の強化を視野に入れ，仮想ネットワークに基づく新しい形のネットワーク実習環境を提供するためのシステム LiNeS（Linux Network Simulator）を開発してきた．LiNeS は，従来の PC 演習室設備でネットワーク管理演習を行えるようにすることを目的としたシステムである．標準的な性能の Linux PC 上で動作し，20 台程度の仮想ネットワーク機器から構成される仮想ネットワークを実現できる．仮想ネットワーク機器は Linux サーバ，ルータ，クライアント，スイッチングハブである．従って，1 台の Linux PC で 1 人の生徒に仮想 Linux ネットワークを管理する演習を行わせることが手軽にできる．図 1 は，大学でのネットワーク管理者育成に重要な知識とその学習順序である．(1) ～ (4) は多くのネットワーク機器が必要となるため，実施困難な大学も多い．これまでの LiNeS は，(1) ～ (3) の演習環境を，既存の PC 演習室にて提供する機能を有している．

本研究では，「クラッキング可視化機能」，「仮想ネットワーク間接続機能」，「仮想ネットワーク統括機能」を開発した．クラッキング可視化機能は図 1(4)の演習のためのもので，図 2(a)における学習者の理解を支援するものである．仮想ネットワーク間接続機能は，本研究で対象とする学習分野全体に影響するもので，図 2(b)にあたる．仮想ネットワーク統括機能は，本研究で対象とする学習分野全体に影響するもので，図 2(a)における教師による学習者の進捗把握を支援するものである．

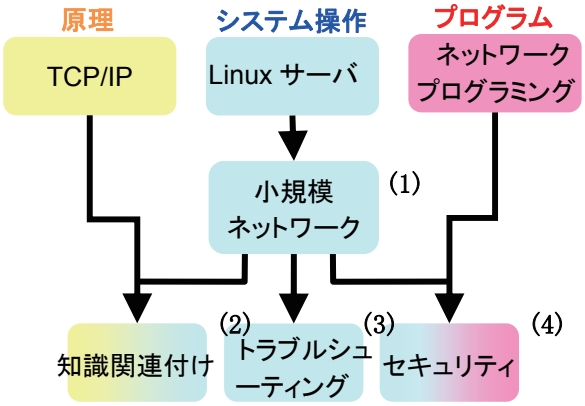

図 1：本研究の学習対象分野

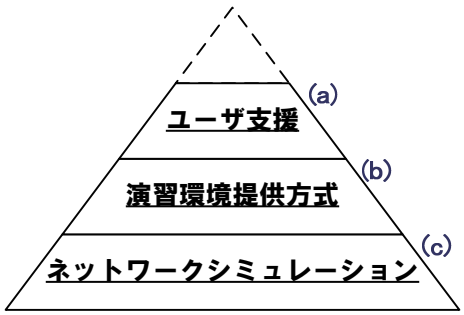

図2：LiNeSの機能構成

2 クラッキング可視化機能の開発

本研究の目的は，クラッキングがシステム内部に引き起こす変化を可視化することによって，学習者にとってより印象の強い演習体験を提供できる環境を実現することと，多様なクラッキング手法を仮想環境上で実現するための柔軟な仕組みを作り上げることにある．前者は，クラッキング手法とその攻撃がシステムに引き起こす変化を一覧できるようにすることで，普段セキュリティに関心を持たない Linux 利用者に，クラッキングに対する危機感を与え，学習者がセキュリティについて学ぶ足がかりとなる情報を提供できる環境を開発するためのものである．後者では，新たな攻撃手法が次々と生まれるセキュリティ分野のシステムとして，特定のクラッキング手法の表現に偏ったものではなく，様々なクラッキング手法に対応可能な柔軟なシステムを目指す．

2-1 関連研究

Tele-lab 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，セキュリティ教育を行うためのシステムである[2]．仮想マシンを利用したセキュリティ教育，という点においては本研究と同様だが，Tele-lab のシステムではネットワークを組むことができないため，ネットワークセキュリティ演習を実施できない．ネットワークセキュリティ演習を志向する本研究とは取り扱う題材が異なる．

Wenliang Du らの研究は，仮想マシンを利用したセキュリティ教育カリキュラムを組み，学生らを対象に実施し，評価をとった実践報告の形をとるものである[3]．仮想マシンを利用したセキュリティ教育という観点で本研究と同一であり，またこの研究ではネットワークセキュリティ演習を行っている点でも本研究と類似しているといえる．しかしながら，この研究では教育用のシステムを開発することなく，仮想マシンをそのまま利用している．仮想マシンを複数台立ち上げ，ネットワークを構築する作業は，初学者にとっては敷居の高い作業であり，初学者にとってもわかりやすいシステムを目指す本研究とは対象とする人物像が異なる．また，評価アンケートでは，仮想マシンを利用したセキュリティ教育の効果の高さについて賛同する声が多くある一方で，およそ 9 割の学生から演習内容の難しさについて賛同する声も出ている．そして「困難」と感じる者の多くは，「教材の不足」をその理由として挙げている．本研究とは対象が異なっているが，以上の結果から，仮想環境を利用したセキュリティ教育の有用性の証明と，セキュリティ教育をサポートする環境の需要があるという事実を示す一例としてとらえることも可能であろう．

2-2 実現法

以下の技術と機能を組み合わせ，プログラムによって制御することでシステムの構築を行う．本システムの構成を図 3 に示す．

（１）攻撃マシンおよびターゲットマシン

攻撃マシンには，セキュリティ実験で多用されるツールとして，ポートスキャンツールである nmap，脆弱性スキャンツールである Nessus，またセキュリティ検証用フレームワークである Metasploit を攻撃ツールとして組み込む．さらに，基本的なクラッキング演習のために，辞書攻撃型のパスワードクラッキングと辞書ファイル,及び DoS 攻撃用のツールも導入する.これらのツールを利用したセキュリティ演習を行う場合，シェルコマンドの expect を利用したスクリプトを攻撃マシンに引き渡し実行する．

攻撃のターゲットとなるネットワークに関する詳細なデータを収集するために，IDS&IPS としてデファクトスタンダードである Snort を導入したマシンの追加も行う．Snort を利用することで，通常得られないクラッキングの兆候についてもデータとして取得することが可能になる．

（２）セキュリティ演習管理機能

XML によって作成した設定ファイルから，攻撃を実行するマシン，状態を監視するマシン，監視するデータなどのセキュリティ演習に必要な各種データのシステムへの引き渡しを行う．演習項目作成者は，基本的にはこの設定ファイルを書きかえることでシステムへの演習追加を行う．設定を読み込み，仮想ネットワーク内のマシンを統括管理することでセキュリティ演習全体を管理する機能については新たに開発を行う．

（３）データ解析＆可視化機能

設定ファイルから引き渡されたデータと，攻撃前後または攻撃時に取得した指定マシンの出力データを利用し，わかりやすい形で提示するための機能を開発する．攻撃が終了しているかどうか，などのマシン状態の調査，取得したデータへの色付けなどの見やすい形への加工，攻撃前後の差分データの取得，指定キーワードを含む行抽出などの作業を行う．

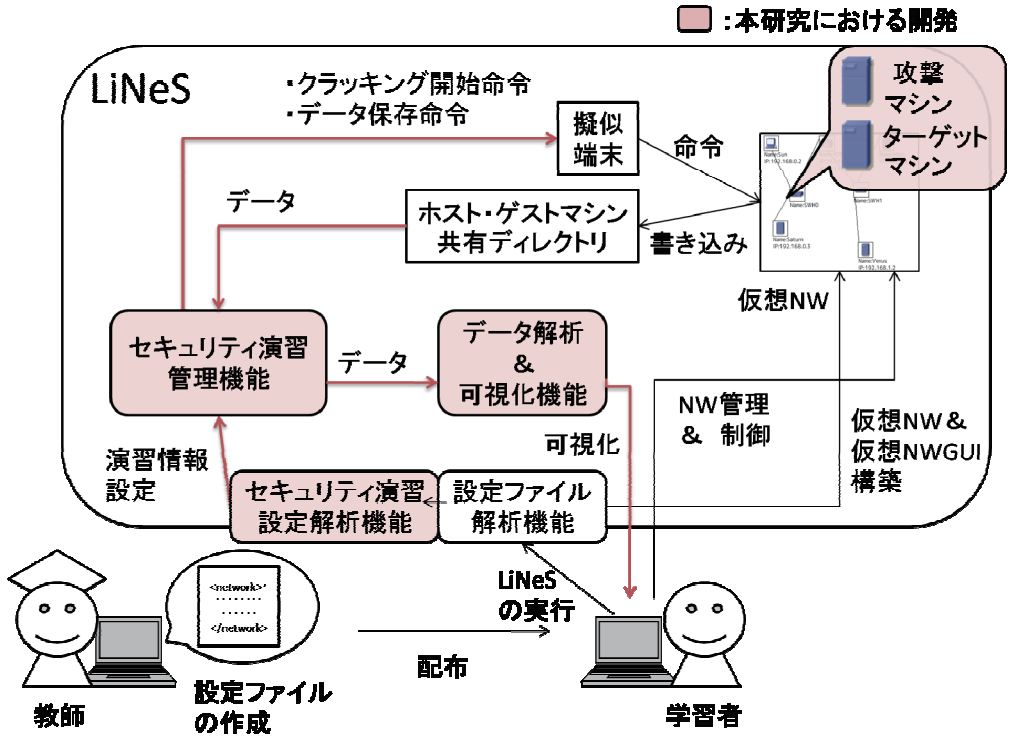

図 3：システム構成

2-3 実行例

実際の操作画面を提示し，本研究によって開発したシステムの学習利用の流れを示す．LiNeS を利用した演習では，学習者は GUI から簡単にネットワークを構築できる ．セキュリティ演習についても，アイコンをクリックするだけの簡単な操作によって攻撃が実行される仕組みになっているため，学習者は攻撃ツールの細かな使用法を覚えずとも，クラッキングの体験を得ることができる．

本システムを利用した学習を行う場合，学習者は以下の手順でシステムを操作することになる．

(1)　LiNeS を起動する

(2)　演習項目を選択する(図 4)．演習の説明があるため，内容を確認する

(3)　初期状態では，各マシンは起動されていない状態にある．GUI から各機器を起動する(図 5)

(4)　必要に応じて各マシンの環境設定を行う(ネットワーク設定,ユーザの追加,パスワードの設定など)．環境については教師が指示したものに従うことになる

(5)　環境が整ったことを確認後,メニューからセキュリティ演習用のアイコンを選択し,演習を開始する．攻撃マシンからのクラッキングがはじまる(図 6)

以下，教師の設定した可視化表示モードによって，流れが分岐する

(6)-1（リアルタイム表示モードの場合）演習開始とともに，ウィンドウが表示される．教師によって指定されたファイル又はコマンド出力が更新表示される．攻撃のプロセスを確認する(図 7)

(6)-2（比較・差分表示モードの場合）攻撃の終了後，攻撃前と攻撃後の比較と差分データがウィンドウ内に表示される．攻撃の結果，システム内部に起きた変化を確認する(図 8)

(7)　ブラウザなどから実際の被害を確認する,ヘルプドキュメントのコメントを元にシステムにアクセスし，クラッキングへの対策について検討する(図 9)

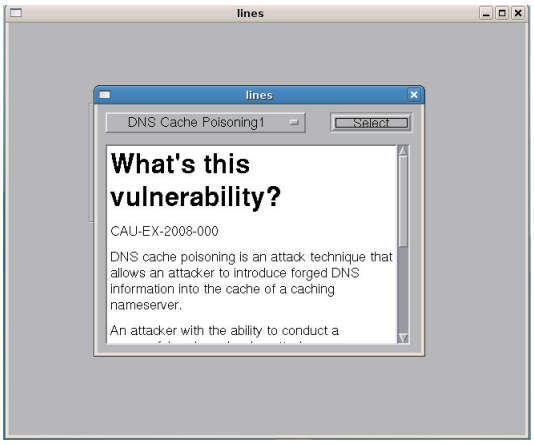

図 4：演習項目選択画面

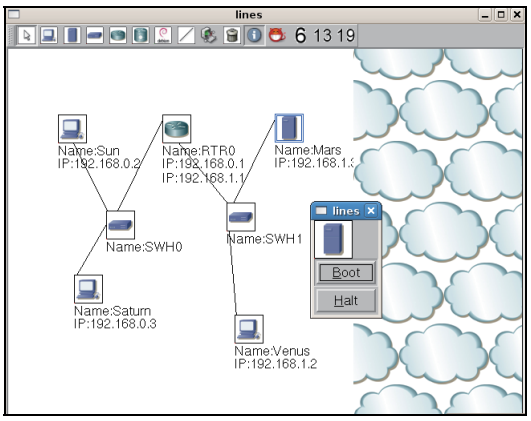

図 5：各機器の起動

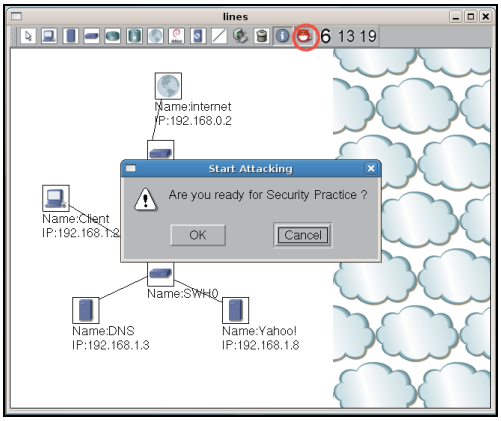

図 6：メニューから選択し，演習開始

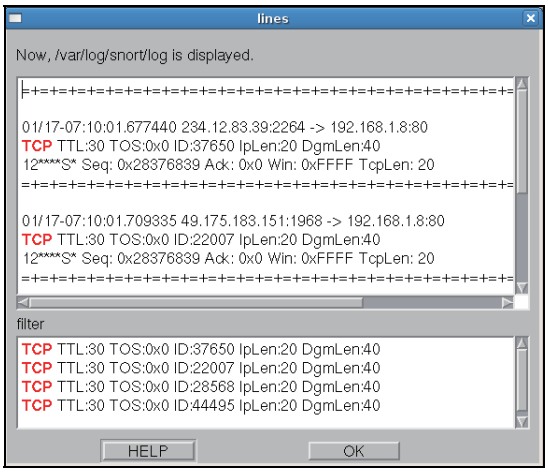

図 7：リアルタイム表示機能

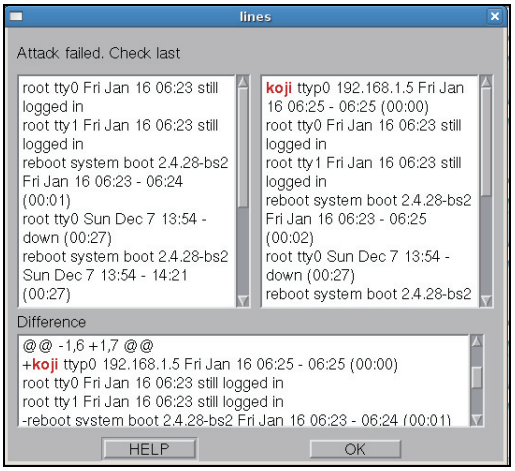

図 8：比較・差分表示機能

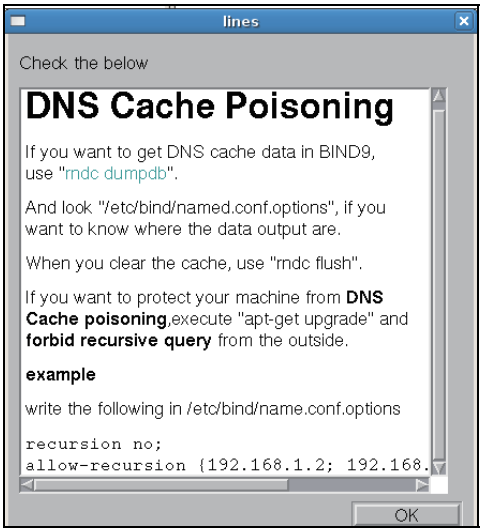

図 9：ヘルプドキュメントの表示

3 仮想ネットワーク間接続機能の開発と実用可能性の検討

本研究の目的は，LiNeS を拡張し，これまでは各 PC 上に孤立して構築していた仮想ネットワークを外部ネットワークに接続可能にすることによって，外部ネットワークの存在を考慮した以下のようなネットワーク演習を新たに行えるようにすることである．

・外部ネットワークを考慮した TCP/IP の設定
・外部ネットワークとのアクセス制御
・外部ネットワークのネットワーク資源の利用
・外部ネットワークへのサービスの提供

この機能によって，LiNeS において，実社会でのネットワーク形態により近いネットワーク演習環境を提供できるようになるため，より実践的なネットワーク管理者育成を行うことができるようになる．

3-1 関連システム

仮想マシン技術によるサーバ構築演習，およびネットワーク構築演習のためのシステムを取り上げ，本研究との違いを述べる．

Anisetti らは，高性能なサーバ上に仮想マシン技術 Xen により実現した複数の Linux 仮想マシンを，個々の学習者に割り当てるシステムを開発した[4]．学習者は，遠隔地からサーバにログインし，割り当てられた Linux 仮想マシンにおいてサーバソフトウェアの導入やネットワークプログラミングの演習を行うことができる．このシステムでは高性能なサーバ設備が新たに必要になるため，従来の演習室設備での手軽な実施を目指す LiNeS の目的を満たすことができない．

中川らは，VMware Workstation により 1 台の PC 上に数台の仮想ネットワーク機器を実現し，その PC 複数台を VLAN 機能を有している実ネットワークによって接続することで，各仮想ネットワーク機器を自由に組み合わせた仮想ネットワークを構築できる演習環境を提供するシステムを開発した[5]．しかし，VMware Workstation と高性能機器による大規模計算機演習室での実習環境構築であるため，多大な導入コストが必要となってしまい，LiNeS の目的を満たすことができない．

以上の関連研究は，ネットワーク構築演習を行うための機能を有していなかったり，特別な設備を必要としたりするため，LiNeS の目的を達成できない．

3-2 システム実装

（１）VPN 技術による仮想ネットワークと外部ネットワークの接続

図１０は，学習者の仮想ネットワークを外部ネットワークに接続するための手法について示している．

「物理ネットワーク」は実際に使用するネットワーク環境を示している．学習者各々の PC 上に構築される仮想ネットワークは,LAN やインターネットなどの実ネットワークを介して LiNeS ネットに接続される.LiNeS ネットは，擬似的なインターネットという位置づけのネットワークであり，ネットワーク資源として DNS ルートネームサーバやパッケージサーバを保持している．

「実装イメージ」は本手法による通信イメージと実装手法を示す．本研究では LiNeS ネットと学習者の仮想ネットワークを VPN 技術によって接続している．大学の PC 演習室内限定であれば，経路制御の工夫により対応することも可能であるが，LiNeS が自宅での自習利用のほか，将来的に遠隔教育への展開を想定しているので，インターネットを介した接続に対応している必要があるためである．VPN ゲートウェイは VPN ソフトウェア OpenVPN[6]により実装されている．LiNeS ネットの VPN ゲートウェイと学習者の VPN ゲートウェイとの VPN 接続の確立によって，学習者のネットワークは LiNeS ネットおよび，他の学習者のネットワークと通信できるようになる．

以上により，学習者の仮想ネットワークと LiNeS ネットは，「論理ネットワーク」に示されるような実ネットワーク上に独立したネットワークを構成する．このような形態は，既存のネットワークへの悪影響を防ぐだけでなく，学習者の混乱を防げるため，効率的・効果的に学習を進めることを可能にする．

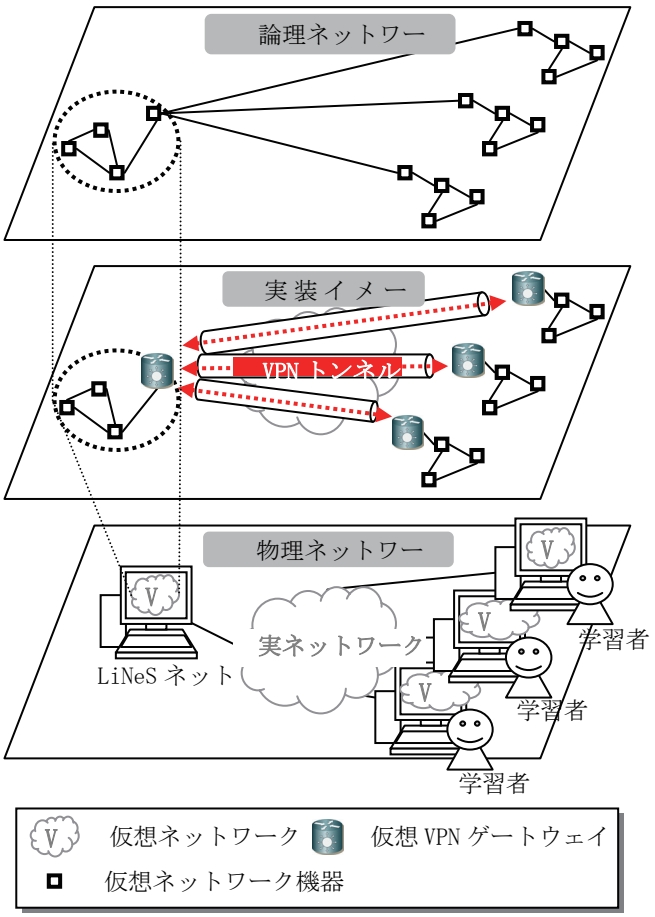

図 10：VPN 技術による LiNeS ネットと学習者の仮想ネットワークとの接続

（２）NAT 技術による仮想 VPN ゲートウェイの公開

LiNeS ネットにインターネット上の PC から参加するためには，VPN ゲートウェイをインターネットに公開する必要がある．LiNeS の VPN ゲートウェイは，Linux 実機の上で UML の仮想機器として動作している．実機ではなく，実機上の仮想機器において VPN サービスを公開するためには，通常，実機と仮想機器にグローバル IP アドレスが各々必要になる．本研究ではグローバル IP アドレスの浪費を防ぐため，NAT 技術によりグローバル IP アドレス 1 つで運用可能にした．具体的には，図 11 に示す設定を LiNeS ネットの稼働している PC に施している．実機の IP アドレスがグローバル IP アドレスの 133.X.Y.Z であり，TCP ポート 1194 番に来た VPN のための通信データを UML の VPN サーバのプライベート IP アドレス 172.0.0.2 に転送するための設定である．

```
# iptables -t nat -A PREROUTING -d 133.X.Y.Z ¥
                    -p tcp --dport 1194 -j DNAT --to 172.0.0.2
```

図 11：NAT 技術によるグローバル IP アドレスの節約

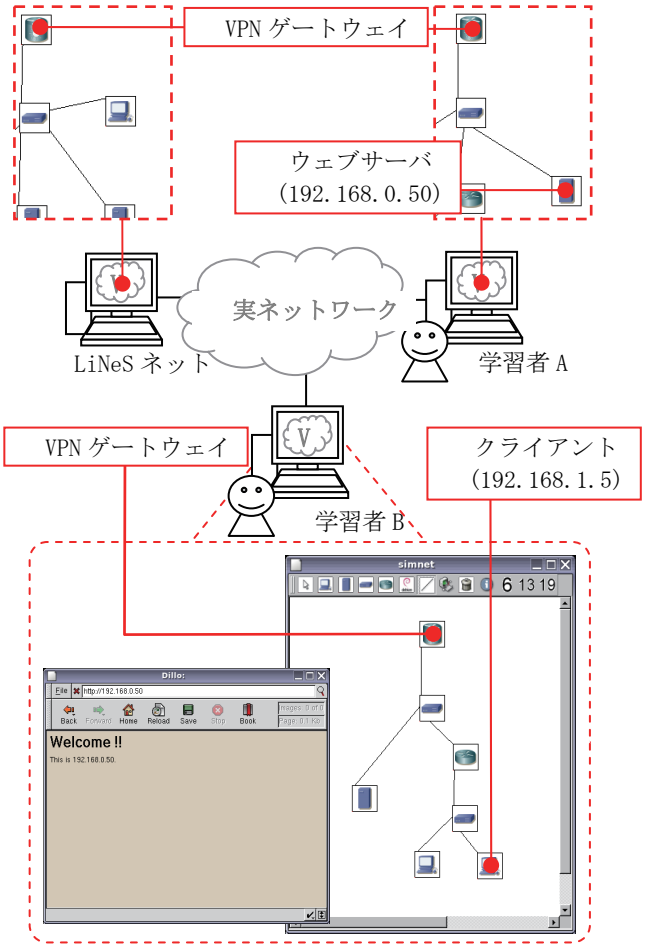

図 12：VPN 技術による仮想ネットワーク間通信

3-3 実行例

図 12 は LiNeS ネットと学習者 2 人によって構築されたネットワークである．学習者 A および学習者 B の仮想ネットワークは，LiNeS ネットとの VPN 接続を各々の VPN ゲートウェイを通じて確立している．学習者 A と学習者 B の仮想ネットワークは LiNeS ネットを経由してお互いに通信可能である．

学習者 A が自身のネットワーク内のウェブサーバに公開したテスト用ウェブページを，学習者 B が自身のネットワークの仮想クライアントから閲覧できるか確認している．もし，学習者 B が図に示すようにテストページを閲覧できれば，学習者 A と学習者 B が各々のネットワークを正確に構築し外部に公開できていることになる．そうでなければ，学習者 A または学習者 B がネットワークを正しく構築できていないことになるため，2 人は協力してミスを探し修正していくことになる．

3-4 予備的評価実験

本手法において，ボトルネックとなりうるのは LiNeS ネットの VPN ゲートウェイである．学習者の外部ネットワークへの通信は，すべてこの VPN ゲートウェイを経由する．従って，多数の通信データが VPN ゲートウェイを同時に経由する場合のネットワークパフォーマンスを測定することで，本手法の性能の下限を明らかにし，その結果をもとにシステムの実用可能性について考察する．

図 13 に測定環境を示す．測定するネットワークは，2 台，8 台，14 台の学習者用 PC にそれぞれ 1 台の LiNeS ネット用 PC を加えたもので，3 パターンである．各パターンのうち 1 台をインターネット上に設置し，その他を LiNeS ネット用 PC と同じ LAN 内に設置した．LiNeS ネット用 PC の性能は Pentium4 2.8GHz，メモリ 512MB であり，学習者用 PC は同程度かやや低い性能である．

測定にはネットワークパフォーマンスの測定ソフトウェア ttcp[7]を用いた．2 つの PC でペアを組み，両方の PC から通信データを同時に送受信する．これは，学習者同士がお互いに相手のネットワークからデータをダウンロードしている状態と考えることができる．この通信を各々のパターンにおいてすべてのペアで同時に行うことで，VPN ゲートウェイに最も負荷のかかっている時のネットワークパフォーマンスを測定できる．

測定結果として，LiNeS ネット用 PC の CPU 使用率を図 14 に，学習者用 PC の通信速度の平均を図 15 に示す．通信中の CPU 使用率はすべてのパターンにおいて 100%で，通信速度はネットワーク規模に反比例している．従って，ボトルネックとなっているのは LiNeS ネット用 PC の CPU 性能であると言え，通信データが LiNeS ネット用 PC において転送処理を待っていることが原因であると考えられる．2 台のパターンと比べて，8 台のパターンは 1/3 程度，14 台のパターンは 1/5～1/6 の速度となっており，台数に反比例している．これを基に，本システムの想定する使用条件である 30 台（学習者 30 人）での結果を推定すると，およそ 13KByte/sec となる．

本機能を使用する演習では，最大で 5MByte 程度のデータを送受信する．このデータを 13KByte/sec で送信あるいは受信するには約 384 秒かかる計算となる．しかし，演習内容を考慮すると，このような負荷のかかった状態（学習者 30 人が同時かつ双方向に送受信するケース）になる可能性は低い．従って，本手法は本システムの使用目的において大きな問題とならないと考える．また，LAN 上の PC 同士，インターネット上の PC と LAN 上の PC との通信速度はほぼ同じであることから，インターネットを経由した学習も，本手法で大きな問題なく行えると言える．

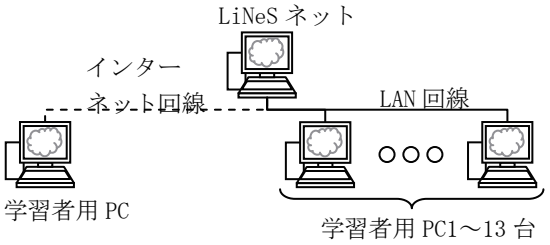

図 13：測定環境

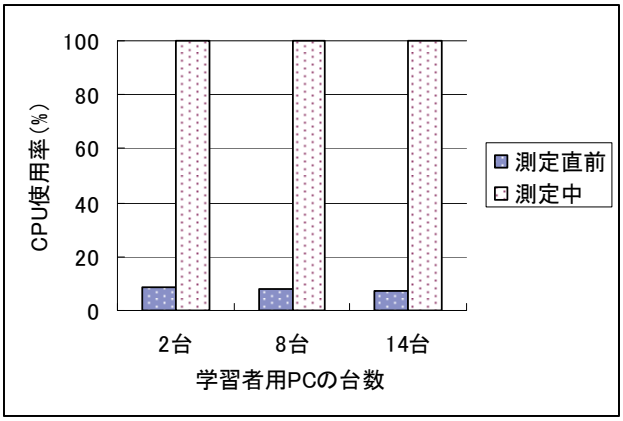

図 14：CPU 使用率測定結果

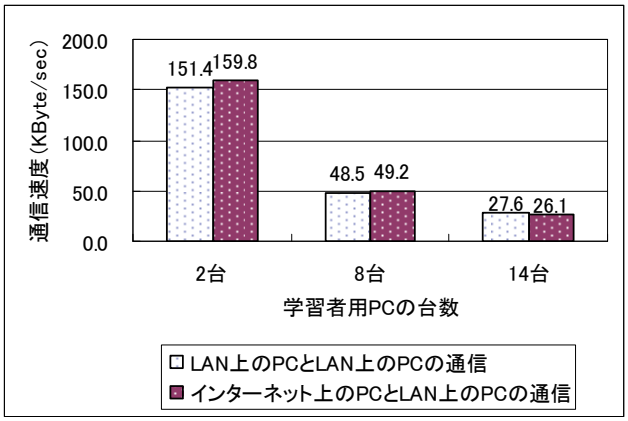

図 15：通信速度測定結果

4 仮想ネットワーク統括機能の開発

LiNeS（Linux Network Simulator）は，各学習者の PC 上に孤立して構築された仮想ネットワーク（LiNeS-LAN）

を，インターネットを通じ，教師の構築した仮想ネットワーク（LiNeS-Net Core）に VPN 接続することで，オーバレイネットワーク（LiNeS-Net）を構成する機能を有している．本研究では，教師の定義した LiNeS-Net の設計データに基づき，各学習者の PC 上に仮想ネットワークを自動構築する機能，および学習者の仮想ネットワークの状態を取得し教師に提示する機能の開発を行う．これにより，教師の設計した大規模な仮想ネットワークを各学習者がセグメント別に分担して管理する演習や，教師が学習者の演習の進捗を容易に把握することなどが可能となる．

4-1 関連研究

ネットワーク機器の状態を取得する方法として，SNMP（Simple Network Management Protocol）は良く知られた方法である．しかし，SNMP による方法では，ネットワークに参加していない機器や，電源が入っていない機器など，学習者のネットワーク構築未完了時における状態を取得できない．

VNUML[8]は，利用者の記述したネットワーク設計データに基づいて，仮想マシンソフトウェア User-mode Linux（以下，UML）による仮想ネットワークを自動的に構築するシステムである．この機能は，これまでの LiNeS の機能 － 設計データに基づき PC 内に UML の仮想ネットワークを自動的に構築する － に類するものである．しかし，VNUML では，ネットワーク上に分散した PC によるオーバレイネットワークの自動構築を行うことはできない．

4-2 LiNeS

LiNeS の仮想ネットワーク機器（以下，仮想機器）は，UML により実現されている．仮想機器同士を接続することで，一般的な性能の Linux PC 上に仮想ネットワークを構築できる．学習者は，仮想 Linux サーバや仮想ルータによる仮想ネットワーク（LiNeS-LAN）を構築できる．教師は，それらに加えて，ルートネームサーバを模擬する DNS や，擬似的なパッケージ配布サーバを含む仮想ネットワーク（LiNeS-Net Core）を構築できる．LiNeS-LAN と LiNeS-Net Core の接続によりできた LiNeS-Net は，複数の学習者が連携してネットワーク管理を行う演習のためのネットワークである（図 16）．

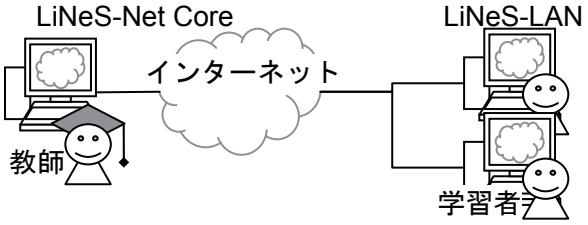

図 16：本研究で想定する演習環境

4-3 システム実装

図 17 にシステム構造を示す．LiNeS による仮想ネットワークを管理するための仕組み LNMP（LiNeS Network Management Protocol）を定義した．教師側に常駐する LNMP Manager と学習者側の LNMP Agent が表 1 に示す通信を行う．また，NAT 環境の可能性を考慮し，トランスポート層には TCP を使用した．LNMP Agent から LNMP Manager に TCP セッションを張り続けることで，継続して双方向のデータ交換を可能にする．

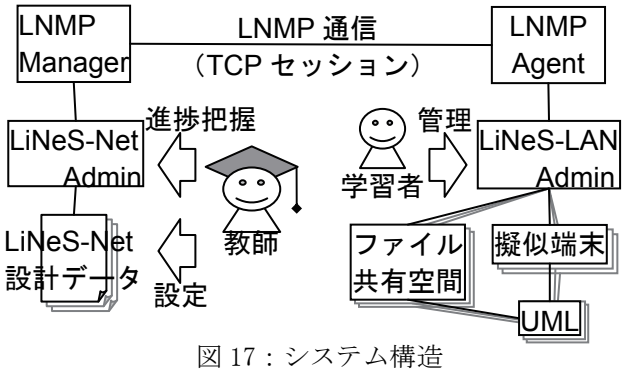

図 17：システム構造

表 1：要求および応答一覧

要求および応答名	要求側
ログイン要求／応答	LNMP Agent
初期ネットワークデータ取得要求／応答	LNMP Agent
ネットワーク状態取得要求／応答	LNMP Manager

表 2 に示す XML のタグおよび属性は，LiNeS-Net の設計を記述するために，新たに必要となったものである．これまでの LiNeS における仮想ネットワークの記述は，LiNeS-LAN の構成要素についてのものであり，LiNeS-Net の記述のためには，それらを教師および学習者毎の仮想ネットワークに分けて記述する必要がある．このため，「network」と「userid」を定義した．また，LiNeS-Net への参加は VPN を持つ仮想ゲートウェイを必要とするため，「gateway」を定義した．そして，LiNeS-Net Admin の分析した設計データを LNMP 通信で各 LiNeS-LAN Admin へ伝達する機能を実装した．LiNeS-LAN Admin は受け取ったデータに基づき，仮想ネットワークを構築する．

表 2：新規追加したタグおよび属性

タグ・属性	説明
network	仮想ネットワークを示すタグ．
userid	network タグの属性．仮想ネットワークのユーザ割り当て指定用．
gateway	LiNeS-Net へ参加するための仮想ゲートウェイを示すタグ．

LiNeS における学習者の仮想ネットワーク構築の進捗は，表 3 に示すデータにより推定できる．

LiNeS における仮想ネットワーク構築では，学習者は LiNeS-LAN Admin を通して，仮想ネットワークを設計し，仮想機器の起動を行う．起動後の仮想機器の操作は，UML の提供するユーザインタフェースを通じてを行われる．従って，表の（1），（2）を LNMP Agent が取得するには，LiNeS-LAN Admin に問い合わせれば良い．一方，表の（3）～（7）を LNMP Agent が取得するためには，LiNeS-LAN Admin が UML から取得する必要がある．そこで，UML の制御端末の 1 つを擬似端末と結びつけること，およびファイル共有空間の利用により，LiNeS-LAN Admin が Linux コマンドの実行結果，およびファイルデータを取得できるようにした．

表 3：仮想ネットワーク構築の進捗推定用データ

データ	保管元
（1）仮想ネットワークのトポロジー	LiNeS-LAN Admin
（2）仮想機器の ON/OFF 状態	LiNeS-LAN Admin
（3）仮想機器中のプロセス一覧	UML
（4）仮想機器中のネットワークインタフェースの状態	UML
（5）仮想機器中のルーティングテーブル	UML
（6）仮想機器中の ARP テーブル	UML
（7）仮想機器中の各サーバ設定ファイル	UML

2-4 実行例

図 18，図 19 は LiNeS-Net 管理用 GUI である．図 18 における人型のアイコンが学習者を意味し，クリックをすると図 19 のウィンドウ（1）が表示される．図 19（2）は LiNeS-Net への接続を意味している．図 19（3）は，サーバ A の状態を表示するウィンドウであり，現在のタブでは動作プロセス一覧を表示している．

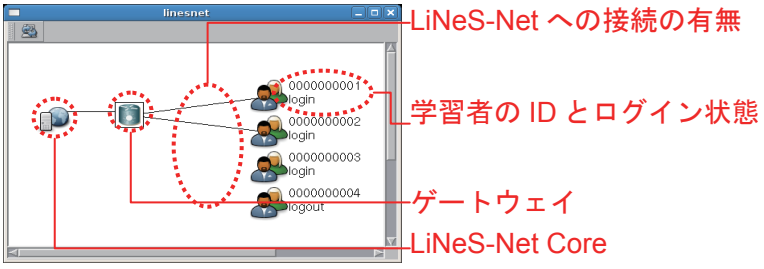

図 18：LNMP サービスを利用している学習者一覧

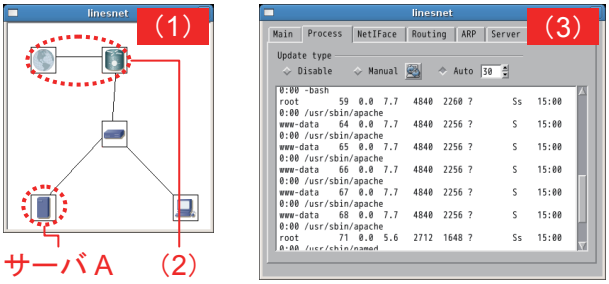

図 19：学習者の仮想ネットワークの状態

5 おわりに

本研究におけるクラッキング可視化機能と仮想ネットワーク間接続機能の開発により，LiNeS は大学におけるネットワーク管理者育成のための学習対象分野をすべてカバーできるようになった．今後は，全ての分野を演習できる点に着目した，総合システムとしての機能の開発を中心に研究をすすめることで，個々の学習対象分野に特化しているシステムとの一層の差別化を図りたい．例えば，図 1（1）～（4）は各々関係が深いため，学習者の学習状況に応じた演習課題の振り分けのための教育コースおよび学習状況分析機能の開発などが考えられる．本研究にて開発した，仮想ネットワーク統括機能は，そのための予備的研究と捉えることができる．

【参考文献】

[1] The User-mode Linux Kernel Home Page: http://user-mode-linux.sourceforge.net/index.html
[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] Anisetti, M.; Bellandi, V.; Colombo, A.; Cremonini, M.; Damiani, E.; Frati, F.; Hounsou, J.T.; Rebeccani, D.; Learning Computer Networking on Open Paravirtual Laboratories, IEEE Transactions on Education, Vol.50, No.4, pp.302-311 (2007).
[5] 中川泰宏, 須田宇宙, 三井田惇郎, 浮貝雅裕:VMware を利用した学習用 LAN 構築支援システムの開発, 教育システム学会誌, Vol.24, 教育システム情報学会, pp.126-136(2007).
[6] OpenVPN-An Open Source SSL VPN Solution by James Yonan: http://openvpn.net/.
[7] ttcp.c : http://www.netcordia.com/files/ttcp.c.
[8] Main Page - VNUML-WIKI: http://www.dit.upm.es/vnumlwiki/index.php/Main_Page.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
LiNeS: Virtual Network Environment for Network Administrator Education	Proceedings CD of the Third International Conference on Innovative Computing, Information and Control (ICICIC-2008)	June 18-20, 2008
LiNeS における仮想ネットワーク間接続機能の開発と実用可能性の検討	FIT2008（第 7 回情報科学技術フォーラム），講演論文集 第 4 分冊，pp. 75-78	2008 年 9 月
LiNeS における仮想ネットワーク統括機能の開発	情報処理学会第 71 回全国大会，講演論文集，pp. 3-3-3-4	2009 年 3 月