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

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　名古屋大学 大学院情報科学研究科博士課程後期課程

1 序論

1-1 背景

我が国におけるユビキタス社会の進展に伴い，より多くのネットワーク管理者の育成が求められている．大学や専門学校あるいは企業においては，ネットワーク管理者育成を目的とした教育が進められているが，それらの多くは座学によるものであり，演習を伴うものも指定されたネットワークトポロジーについての体験に限られているのが実情である．一方，ネットワーク仮想環境を構築するソフトウェアの発展に加えて，パーソナルコンピュータ（PC）の性能向上のため，1 台の PC 上で複数の仮想ネットワーク機器を動作させることが可能になってきた．

我々は，2003 年後半より，仮想環境ソフトウェア User-mode Linux（UML）[1]を活用することで 1 台の PC 上に仮想的なネットワークを実現し，これをネットワーク管理者教育へ応用するための基礎研究を行ってきた[2]．現在，この研究成果に基づき，ネットワーク管理演習のための環境を提供するためのシステムとして LiNeS（Linux Network Simulator）を開発している．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．Linux サーバを中心としたネットワークを構築する演習[3]，そのネットワーク動作のアニメーション表示閲覧によるネットワーク構築技能と TCP/IP との関連性についての学習を行える[4].

1-2 目的

本研究では，LiNeS に以下の機能を追加することを目的とする．

外部ネットワークの存在を考慮したネットワーク構築演習環境提供機能：これまでの LiNeS にはネットワーク管理者が考慮すべき他者の管理するネットワーク（以下，外部ネットワークとする）が存在せず，そういった要素が影響する学習項目を効果的に演習できなかった．そこで，外部ネットワークの存在を演習に取り入れるために，学習者や指導者が各々の PC 上に構築した仮想ネットワークを相互に接続するための機能を開発する．

ネットワークトラブルシューティング演習環境提供機能：大学や専門学校でのネットワーク管理者育成の一環として，初歩的なネットワークトラブルシューティングの演習を行うことも大切である．演習により，トラブルの原因の絞り込み方法や，ネットワーク診断ツールの使い方を学習できる．また，修復には LAN 構築技能や TCP/IP の応用を必要とするため，これら知識の理解強化や復習においても有効である．

ネットワークセキュリティ演習環境提供機能：ネットワークセキュリティを教科書や講義で概念として学ぶだけではなく，体験によって学ぶことも極めて有意義である．本機能は，学習者が 1 台の PC 上に実現した仮想ネットワークの運営において遭遇したネットワークインシデントに対処する演習を行うための環境を提供する．仮想ネットワーク内で完結する形での演習であるため，手軽かつ安全に行え，授業カリキュラムへの導入が容易に進められる．

1-3 関連事例

精巧なネットワークシミュレーションを行えるシステムとして OPNET[5], ns2[6], MAADNET[7], GNS3[8]

が有名である．これらは，サーバオブジェクトやケーブルの配置を行って，ネットワークを仮想的に構築することができる．また，ネットワークのトポロジー構築の学習に対象を特化したシステムとして，早川らのシステム[9]や精廬らのシステム[10]がある．これらは，GUI 上でネットワークトポロジーの構築，および各機器の TCP/IP の設定を学習させることを目的としている．しかしながら，以上のシステムでは本研究の演習対象とする Linux サーバをシミュレーションできないという問題があるため，本研究の目的を満足できない．

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[11]．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．後野は，1 台の PC 上に UML 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ことで，各学習者に個別のサーバ構築演習環境を提供するシステムを開発した[12]．これらのシステムは，サーバ構築演習に有用であるが，ネットワーク構築演習を行うための機能を有していない．加えて，Anisetti ら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本研究の目的を満たすことができない．

中川らは，VMware Workstation[13]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[14]．このシステムは，「外部ネットワークの存在を考慮したネットワーク構築演習」に対して有効であるが，「ネットワークトラブルシューティング演習」と「ネットワークセキュリティ演習」に対して有効な機能を有していない．また，VMware Workstation と高性能機器による大規模計算機演習室での演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，従来の演習室設備での手軽な実施を目指す本研究の目的を満たすことができない．

上田らは，UML と Quagga により擬似的な仮想 Cisco ルータを実現し，1 台の PC で複数の仮想ルータによる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[15]．このシステムは，Cisco Systems のシスコネットワーキングアカデミーの講義[16]の支援を目的とするものであり，ルータやスイッチといったトランスポート層・ネットワーク層を中心とした学習を対象としている．しかし，本研究の「外部ネットワークの存在を考慮したネットワーク構築演習」は，サーバソフトウェアやファイアウォールの設定などアプリケーション層を中心とした学習を目的としており，研究対象が異なっている．

Tele-Lab[17]は，仮想環境ソフトウェア UML を使うことで，ネットワークセキュリティの概念とツールの使用方法の学習環境を実現するためのシステムである．本研究では，ネットワークセキュリティ技術の個々の学習ではなく，仮想サーバ運用を通してネットワークセキュリティを体験的に演習するシステムを目指す．

Walden らは"Capture the Flag"（二陣営に分けた旗取りゲーム）のような方式によって，セキュリティ演習を行った[18]．この演習では学習者にグループを作らせ，攻撃側と守備側に分かれたセキュリティ演習を行う．しかし，セキュリティツールの入手や環境の構築を学習者に任せているため，学習者のレベルが相応に高くなければ実施できず，また多くの手間を必要とする．

Azadegan らはセキュリティ演習の最後のコースとして，実践的なケーススタディを行った[19]．この試みの目的は，実践的・体験的なセキュリティ演習であり，本研究の「ネットワークセキュリティ演習」に非常に近いものである．しかしながら，前述の Walden らの試みと同様に，演習の質については学習者に依存することになる．このような形の演習を実施するには，本研究で対象とするような入門者のレベルを大きく超えた知識が必要となる．こうした形式の学習は，本研究で取り扱う学習方式の次のステップの学習に当たるものである．

以上のように，ネットワーク管理者教育に役立つ可能性を有する研究やシステムを取り上げてきたが，これらは機能不足であったり，学習項目が異なっていたり，特殊な設備を必要としていたりするため，我々の目的に優れた効果を期待できない．

2 外部ネットワークの存在を考慮したネットワーク構築演習環境提供機能

2-1 システム実装

図 1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[20]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．

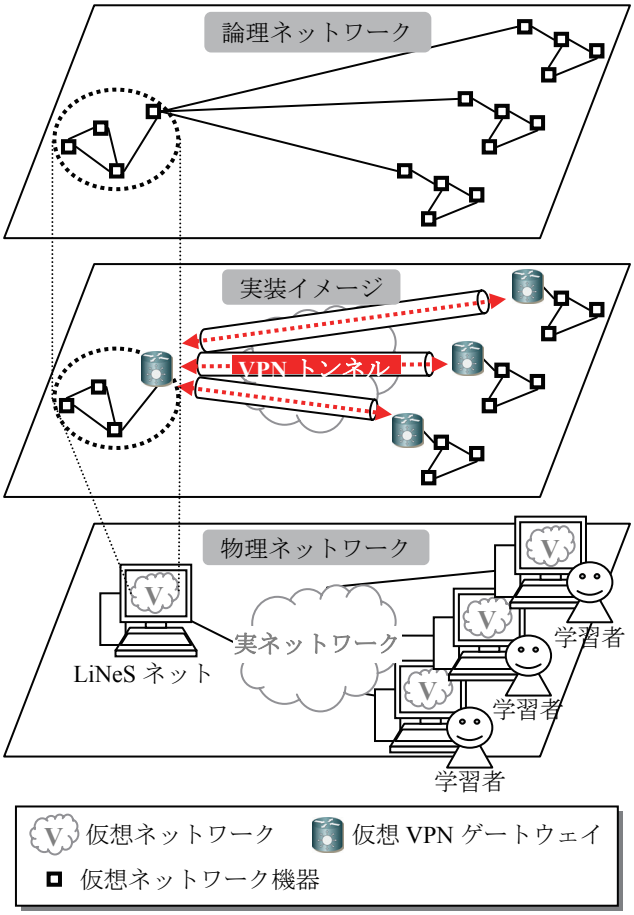


図 1 VPN 技術による LiNeS ネットと学習者の仮想ネットワークとの接続

2-2 実行例

図 2は，LiNeS ネットへの接続作業を支援するセットアップウィザードである．VPN 接続に必要なパラメータを効率的に管理し，複雑な操作が必要となる UML への VPN 用ファイルのセットなどを学習者の代わりに行う．

図 3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．

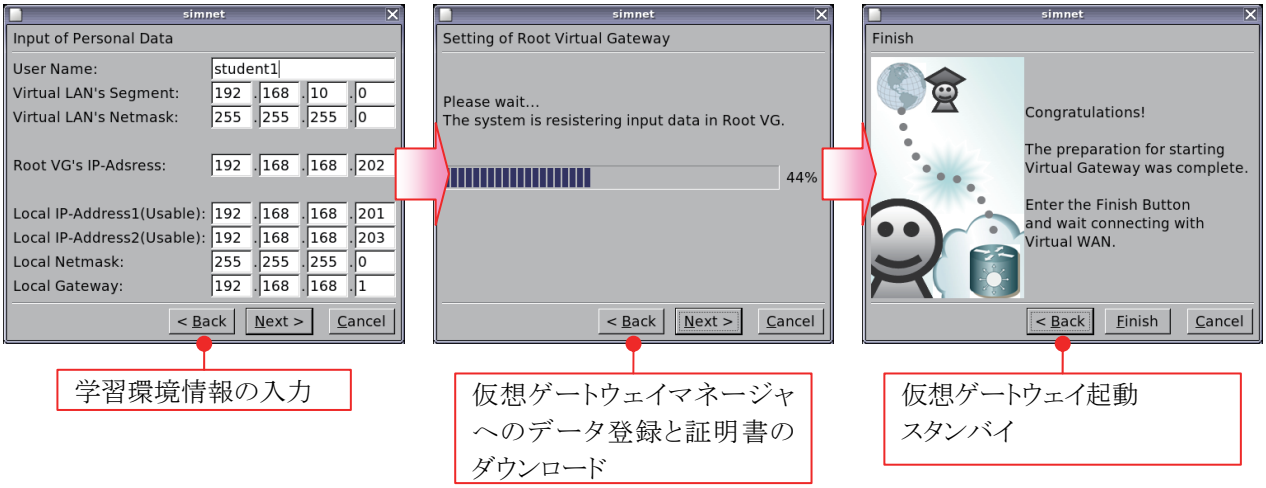


図 2 セットアップウィザードの流れ

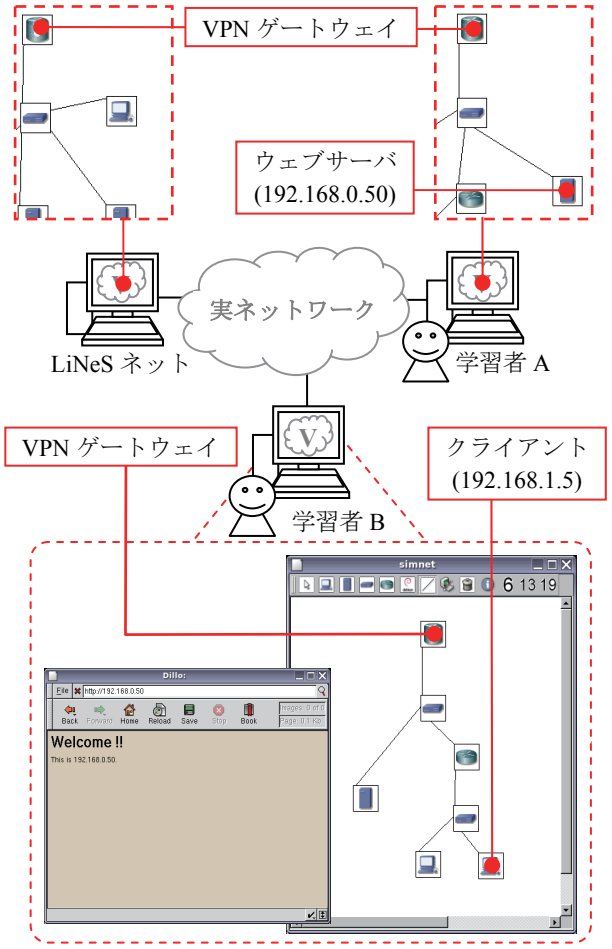


図 3 VPN 技術による仮想ネットワーク間通信

3 ネットワークトラブルシューティング演習環境提供機能

3-1 機能要件

本研究の想定するネットワークトラブルシューティング演習は，大学生や専門学校生が LAN 構築演習や TCP/IP 講義を終えた後で行うものである．この演習により，学習者がネットワークトラブルシューティングの基礎的な手順と，ネットワーク診断ツールの使い方を習得することが，期待する効果である．対象となる診断ツールは，Linux のトラブルシューティング用の代表的なツールである ping, traceroute, ifconfig, route, ps,

netstat, telnet, arp, nslookup, tcpdump である．これらのツールはネットワーク管理において重要で基本的なものである．

このような演習を効率的に行うには，LAN 構築の演習と TCP/IP 理論の講義で学習した知識に基づいて行えることが重要である．したがって，以下のようなシステム要件となる．

要件 A. LAN 構築演習後に使用するシステムであるので，LAN 構築の演習において使用したネットワークが望ましい．したがって，ネットワーク機器としては，クライアント，サーバ，スイッチ，ルータ，ネットワークケーブルを使用し，ネットワーク規模は，15 台程度のものまでを提供できるようにする．

要件 B. 学習者に提示するネットワークトラブルの原因は，「不調な機器」，「設定ミス」，および「接続ミス」とする．「不調な機器」は要件 A で述べたネットワーク機器の不調で，パケットロスや通信データ配送遅延といったトラブルを引き起こす原因となる．「設定ミス」は IP アドレスなどの TCP/IP 設定やウェブサーバ Apache などのサーバソフトウェア設定のミスである．これらにより，「ウェブページが閲覧できない」，「メールを受信できない」といったトラブルが引き起こされる．「接続ミス」はネットワークケーブルの接続ミスで，初学者がよく遭遇するミスの 1 つである．例えば，接続ポートを間違えて接続してしまったり，コネクタが外れていたりするものである．これにより，「目標外のサーバへ接続されてしまったり」，「まったく通信できなかったりする」といったトラブルが引き起こされる．これらの原因を複数組み合わせることで，トラブルのあるネットワークの種類を増やし，難易度も上げることができる．

要件 C. 学習者に提示するネットワークは，学習者の管理する領域と，学習者の管理していない領域から構成されるものとする．この概念は，実際のネットワーク形態を抽象化したものであり，様々な難易度のネットワークトラブルの提供に有用である．すべてのネットワーク機器が管理領域内に設置されたケースと，一部のネットワーク機器が管理領域外に設置されたケースとでは難易度が大きく異なる．例えば，後者のケースにおいて，管理内のネットワークにトラブルの原因がないことを証明することは非常に難易度が高い演習となる．

要件 D. 演習毎の準備の手間と機器への投資が現実的な範囲内であることが，実際に演習を行おうとする場合には必須の要件となる．各学習者に対してトラブルのあるネットワークを課題毎に教師が準備する手間は大変なものである．不調な機器や設定ミスのあるネットワーク機器を実現し，それらを自由に組み合わせたネットワークを手軽に実現できるようにしなければならない．

3-2 機能実装

本機能の構成を図 15に示す．LiNeS は UML により実現した仮想機器で仮想ネットワークを構成する機能を有している（要件 A）．これらの機器を実現している UML のソースコードを改造することにより，トラブルのあるネットワークを実現している（要件 B）．学習者は UML を直接制御するのではなく，アイコンによって提示されたインタフェースを通して，ネットワーク機器を配置したり，プログラムを実行したりすることができる（要件 C）．学習者に提示されるトラブルのあるネットワークは，あらかじめ教師がネットワーク定義ファイルに記述しておいたデータを基に構築される（要件 D）．

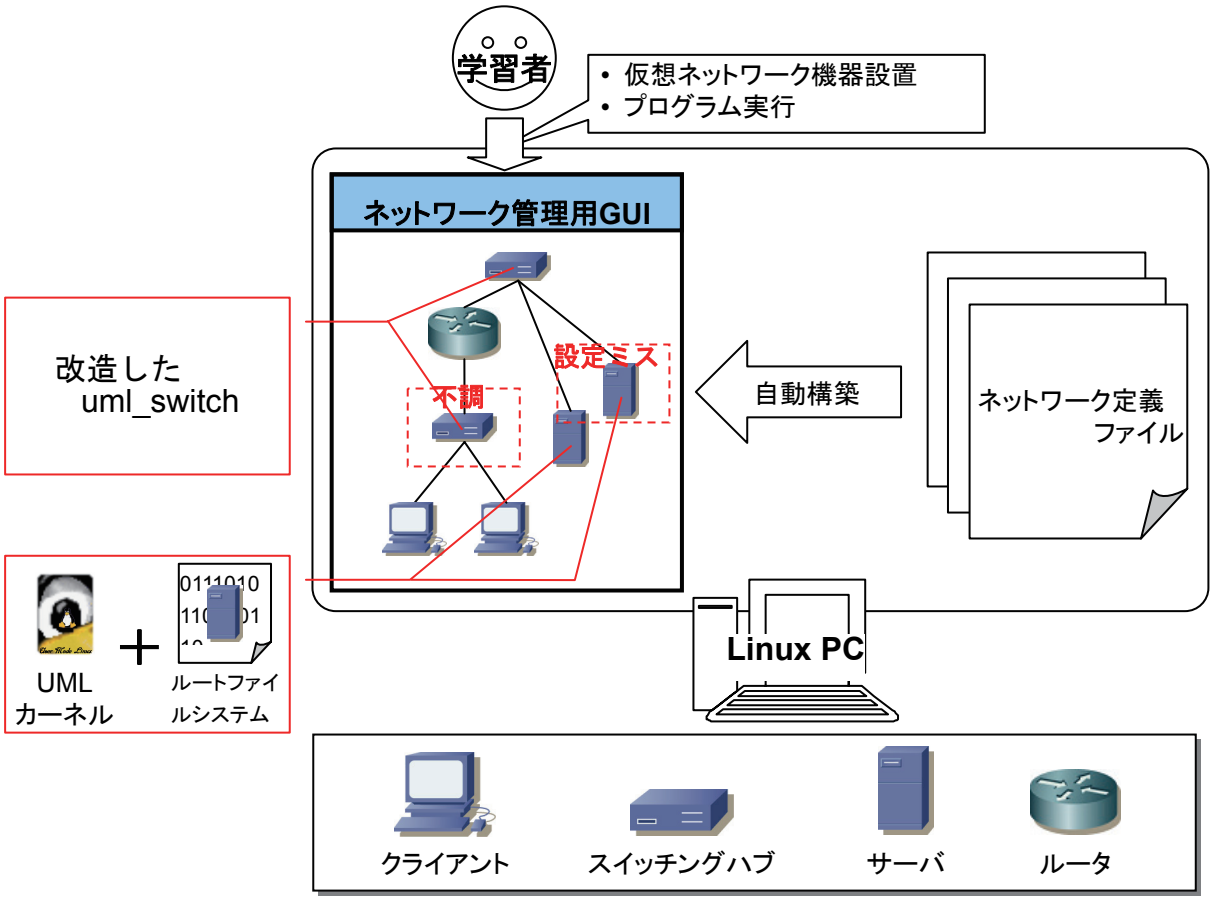


図 4 本機能の構成図

（1）XML によるトラブルのあるネットワークの設定

教師は，表 1に定義した XML タグでトラブルのあるネットワークの情報をネットワーク定義ファイルに定義することで，手間なく自由にネットワークを学習者に提示することができる．各仮想機器は記述された通りの初期化設定で起動し，トラブルのある仮想ネットワークとして学習者に提示される．

表 1 トラブルのある仮想ネットワーク構築用 XML タグの一部

タグ	説明
client	クライアントを示すタグ
init	client, router, server の初期化用シェルスクリプトを指定するタグ
gift	client, router, server に渡すファイルを指定するタグ
conf	switchinghub の初期化設定を指定するタグ
属性	説明
area	管理領域を示す属性
x	x 方向の設置座標を示す属性
srcid	cable の接続先機材 1
srdport	cable の接続先ポート 1
guestpath	<gift> で指定されたファイルの仮想機器内におけるファイル名

（2）ソースコード追加による不調な機器の実現

通常の UML には不調な機器を実現する機能はないため，UML にソースコードを追加することで，不調な機器を実現した．図 5に不調な機器の実装の一例として，不調なスイッチングハブの実装方法を示す．UML のスイッチングハブプログラム uml_switch にソースコードを追加することにより実現している．この機器をネットワーク定義ファイルに「switchinghub」タグで記述することで，仮想ネットワークに組み込むことがで

きる．

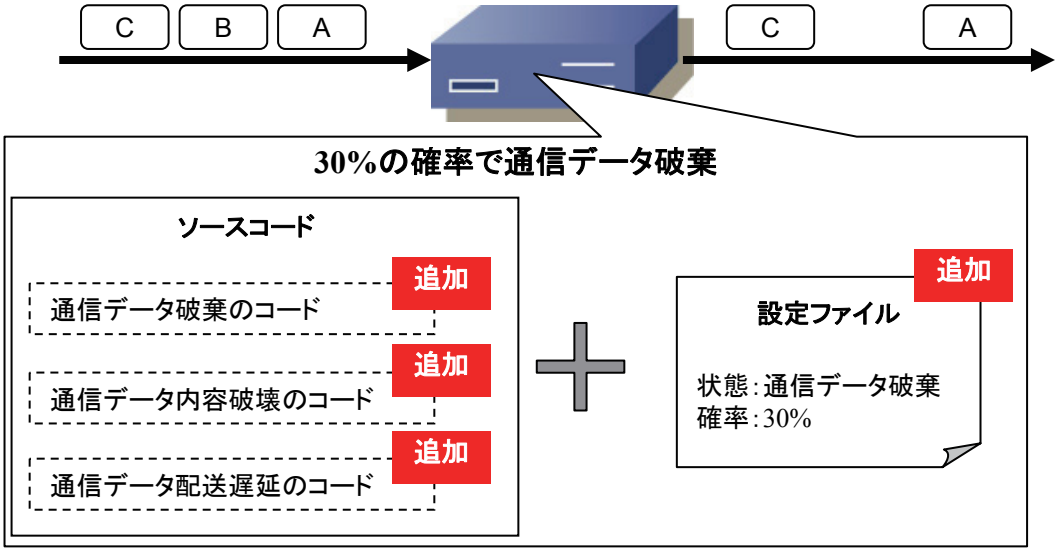


図 5 不調なスイッチングハブの実現

（３）UML の改造による設定ミスのある機器の実現

3-2（１）にて述べたクライアント，サーバ，およびルータを対象としたタグ init により定義された初期設定を，自動的にこれらの機器に適用するための機能を実現した．これはトラブルのあるネットワークを学習者に提示するために必要な機能である．この機能により，ネットワーク機器に特殊な設定を施した状態や，新たな設定ファイルを追加した状態で学習者に提示することができる．

この機能を図 6に示すような仕組みによって実装した．本システムのクライアント，サーバ，およびルータは UML により実装されているので，UML の従来の初期設定処理に追加する形で，UML がネットワーク定義ファイルにある初期設定を自身に適用すればよい．したがって，UML の改造により，UML が init 処理の最後に hostfs にあるファイルを読み，その内容を自身に適用するようにした．また，そのファイルにはネットワーク定義ファイルから抽出された UML 用の設定情報が記述されているようにした．

この仕組みでは UML が init 処理の最後で, 追加の設定を自身に適用している．UML は hostfs を経由して，教師により定義された設定情報を得ている．ゲスト OS である UML とホスト OS のデータ空間は，隔離されているためお互いのファイルを直接参照することができない．そこで，両者の間に共有のデータ空間を構築するための UML の機能の 1 つである hostfs 機能を利用した．システムがネットワーク定義ファイルから初期設定を抽出し，それを hostfs 上のファイルに記述する．そのファイルを UML が参照することで，ネットワーク定義ファイルに定義されていた初期設定を適用できる．

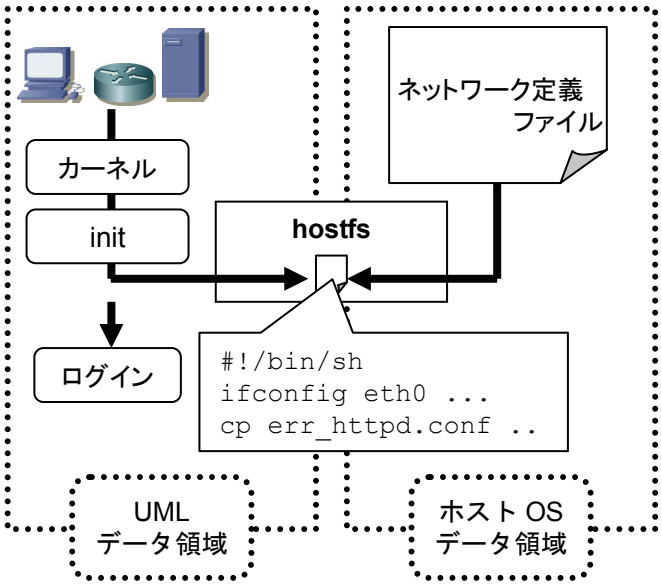


図 6 初期設定の自動的な適用の仕組み

（4）管理領域とケーブルの接続性の表現

学習者の制御可能な管理内領域と，制御できない管理外領域をユーザインタフェースの工夫によって実装した．制御可能な管理内領域では，学習者がすべてのネットワーク機器を確認でき，それらを自由に操作・設置・撤去できる必要がある．制御できない管理外領域では，学習者がネットワーク機器を見ることができず，機器の操作・設置・撤去ができてはならない必要がある．そこで，図 7に示すように，ネットワークを表示する画面の背景により管理内および管理外の領域を表現し，管理内の機器はアイコンを表示しておき，管理外の機器は基本的にアイコンを表示しないようにした．しかし，トラブルシューティングの作業の便宜を考慮し，管理外の領域の機器であっても，設定記述によってはアイコンを表示可能にもしてある．

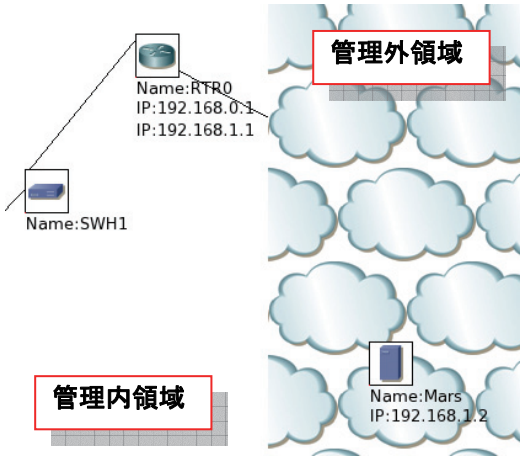


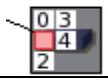
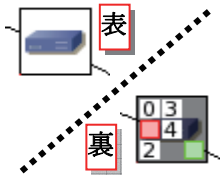
図 7 管理内領域と管理外領域の表現

ケーブルの接続性の表現もユーザインタフェースの工夫によって実装した．ケーブルの接続性の表現は，ケーブルの一端が，

・機器 X のポート Y に接続されている
・機器 X に接続されていると錯覚する
・どの機器にも明らかに接続されていない

を表現することである．そこで，表 2に示すように，ポートを表すアイコンを作成し，各機器の裏にそれらを配置し，ケーブルの両端に接続状態を示すアイコンを表示することによって実装した．これにより，「一見接続されているように見えるが，実際には未接続となっているケーブル」などをトラブルの原因として使用できるようになる．

表 2 ケーブルの接続性の表現

表現項目	アイコン
仮想機器表面(スイッチングハブの例)	
仮想機器裏面(スイッチングハブの例)	
未接続状態のコネクタ	
仮想機器へ接続された状態のコネクタ	
接続されていると錯覚するケーブル配線 (スイッチングハブの例)	

3-3 本機能のメリットと実行例

（１）本機能のメリット

本機能の主なメリットは以下の 2 つである．

第 1 は，教師が簡単にトラブルのあるネットワークを学習者に提供できることである．実機を使用して，トラブルのあるネットワークを提供するのは大変である．故障した機器の実現や，学習者毎に課題毎のネットワークを構築し，個々の機器に必要な設定を施すことは，教師にとって大きな負担となる．しかし，本機能では，教師は XML ファイルに提供したいネットワーク情報を記述することで容易に提供可能である．

第 2 は，学習者が安心して自由な発想で，ネットワークトラブルシューティングの作業を行えることである．試行錯誤を伴うトラブルシューティングの作業は，各機器のシステム設定を破壊してしまう可能性がある．最悪の場合，再インストールをしなければならなくなるため，演習にとって相応しい環境ではない．本機能では，仮想環境ソフトウェアによる仮想機器を使用することで，LiNeS を再起動するだけで各機器をリカバリーできるため，実機より効率よく演習できる．例えば，Apache の設定ファイルなどを再起不能にしてしまった場合や，最初からトラブルシューティングを手早くやり直したい場合などに有効である．

（２）本機能の実行例

まず，学習者が演習したいネットワークトラブルを選択する．そうすると，システムが該当するネットワークを構築し図 8のように学習者へ提示する．その後，学習者は症状の確認やネットワーク診断ツールの実行を行い，トラブルシューティング作業を行う（図 9～図 12）．

図 8 に提示されたネットワークは，「クライアント Sun からサーバ Mars のウェブページ(http://www.mars.com/)の閲覧ができない」というトラブルを持つものである．このトラブルは，サーバソフトウェア Apache の設定とルータのファイアウォールの設定が適切でないことに起因する．

トラブルシューティング作業において，まず，学習者は web ブラウザを使用しサーバ Mars のウェブページが閲覧できないことを確認する（図 9）．次に，ps によりサーバソフトウェア Apache が稼働していることを確認し（図 10 (1)），netstat によりサーバソフトウェア Apache の不適切な動作を発見し（図 10 (2)），Apache の設定ファイル httpd.conf をエディタで編集し，Apache を再起動して設定の変更を有効にする．この作業を行った結果，クライアント Venus からは閲覧できるが，依然としてクライアント Sun や Saturn から閲覧することができない．そこで，ルータ RTR0 の設定を調査しファイアウォールの設定が不適切であることを突き止め（図 11 (1)），これを修正する．以上の作業によってクライアント Sun からサーバ Mars のウェブページを閲覧できるようになり（図 12），トラブルを解決できたことになる．

学習者はこのような作業を通じて，ネットワーク診断ツールの演習や，Apache の設定などの LAN 構築技能の復習，ファイアウォールに設定したポート番号の役割などの TCP/IP 理論の復習を行える．また，様々な機器からアプローチすることによって原因を絞り込むという，基本的なトラブルシューティングの手順を学習できるのである．

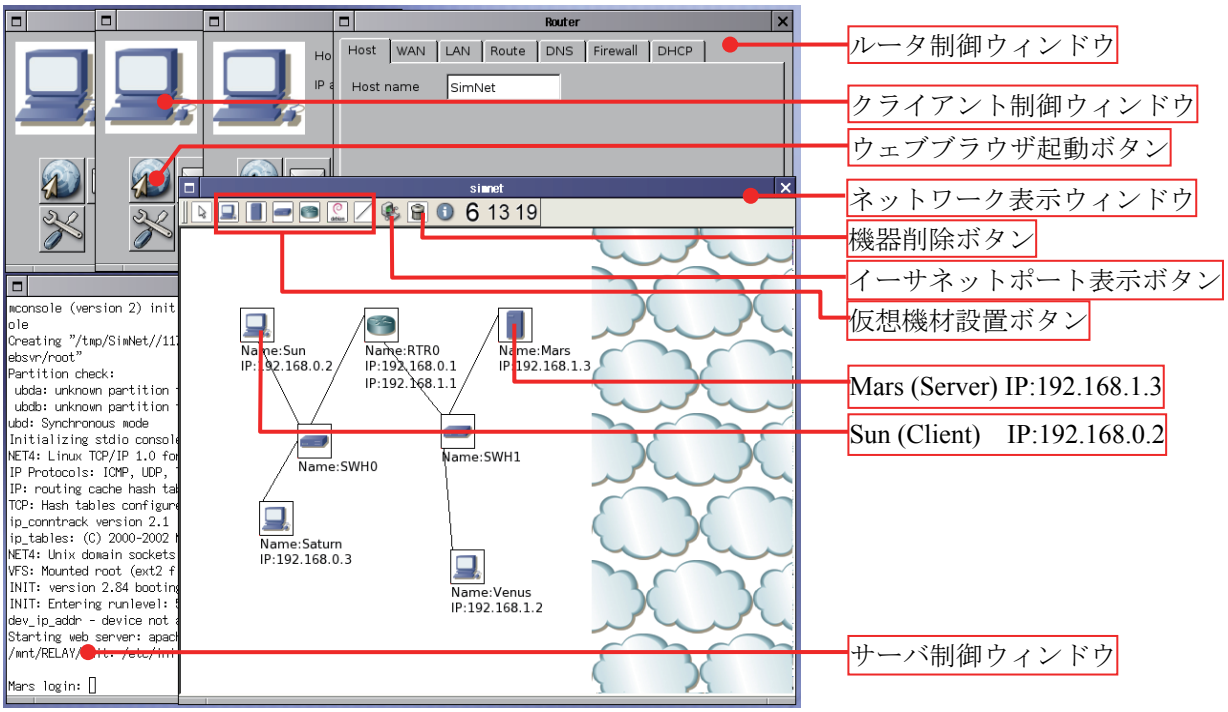


図 8 トラブルのあるネットワーク

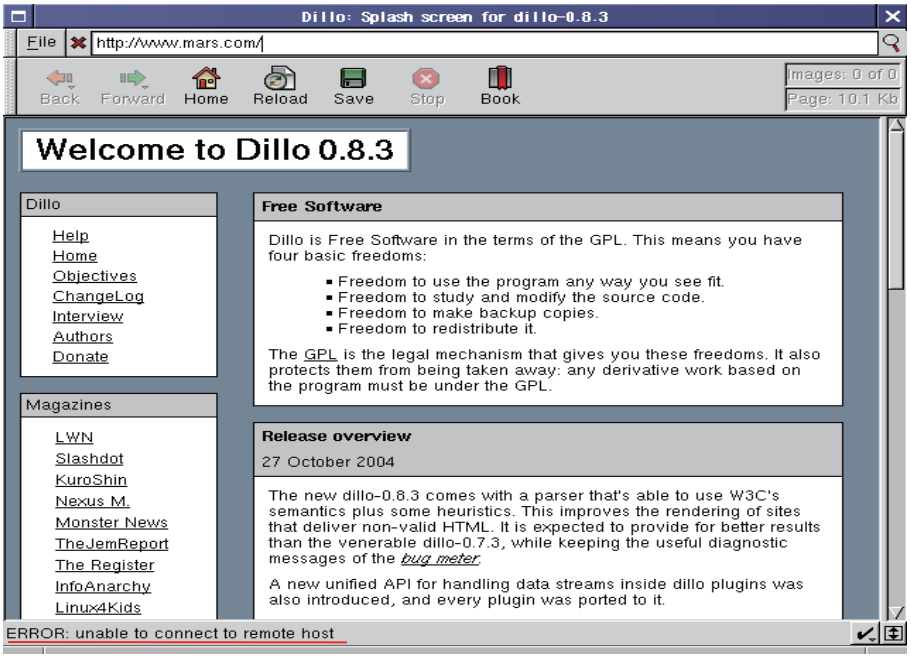


図 9 Mars 上のウェブページを取得失敗

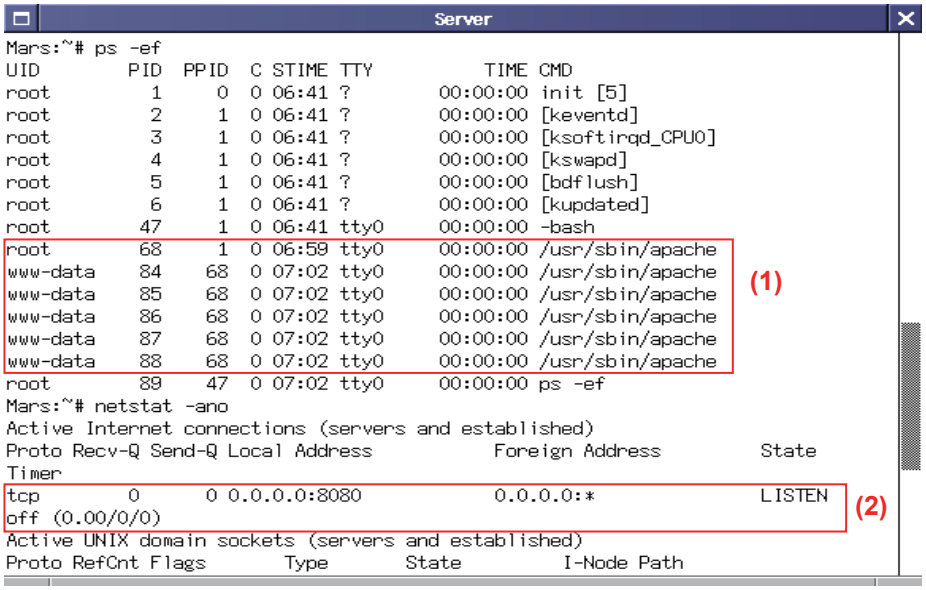


図 10 サーバでのネットワーク診断ツール ps, netstat の実行結果

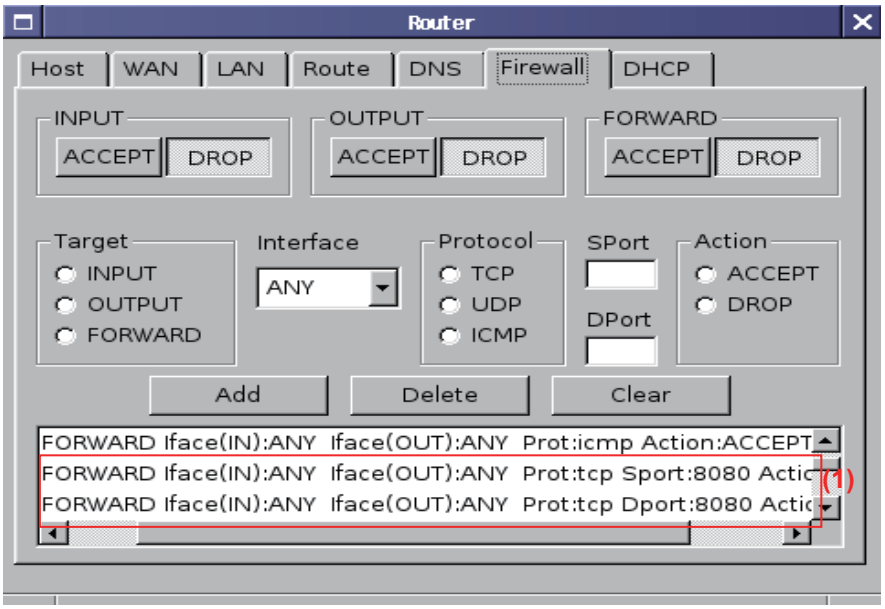


図 11 ルータのファイアウォールの設定

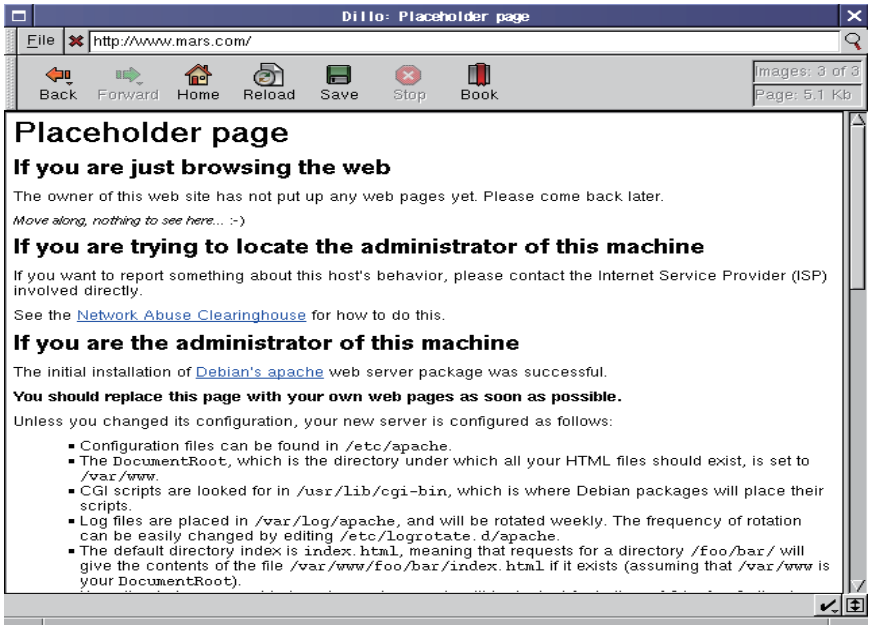


図 12 Mars 上のウェブページを取得成功

3-4 実証実験

本機能の性能評価とアンケートを行った．実験は，教育現場での使用を考慮した性能の PC（CPU：PentiumM1.6GHz，メモリ：512MB）を使用した．この PC で動作すれば，教育現場においても十分に本機能を使用できると考えられる．

（１）機能の性能評価

トラブルのある 2 つのネットワークにおいて，CPU 負荷計測による性能評価を行った．一方は本研究が想定している平均的な規模である 6 台構成のネットワークであり（以下 Network A と呼ぶ），他方は本研究が想定している最大の規模である 15 台構成のネットワーク（以下 Network B と呼ぶ）である．

図 13，図 14にネットワークトラブルシューティングの作業過程の CPU 使用率を示す．図中(1)は，本機能が各機器を起動し設定を施している期間で，Network A は 33 秒，Network B は 98 秒であった．その後のトラブルシューティングの作業の期間は図中(2)である．Network A では ping による原因の特定や故障機器の交換などを行った．ping 実行のための端末の起動には約 1 秒であった．Network B ではウェブ閲覧（ブラウザの起動時間は約 3 秒，Web ページ取得時間は約 1 秒）や web サーバ Apache の再起動（再起動時間は約 2 秒）などを行った．

ネットワークの準備時間，各アプリケーションの起動時間・実行時間，加えて作業中の CPU 使用率から考えると，システムのレスポンスにおいて学習者がストレスを感じることは少ないと思われる．15 台と機器の台数が増えるとシステム負荷も大きくなるが，学習者は作業を 1 つずつ個別に実行するので，大きな問題ではないと考えている．

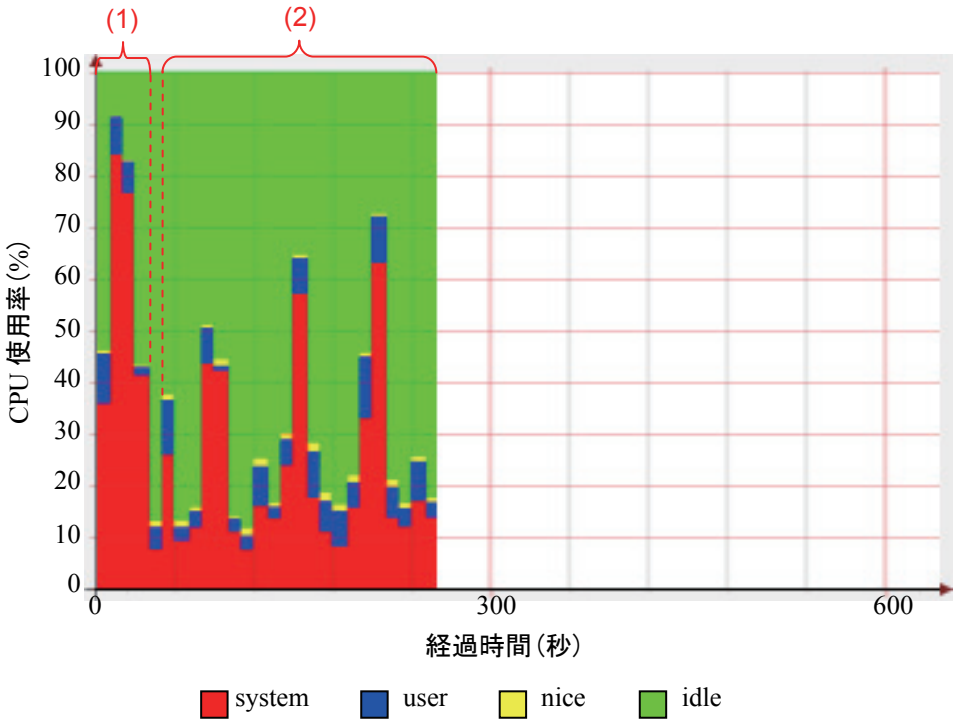


図 13 Network A におけるトラブルシューティング作業の CPU 使用率

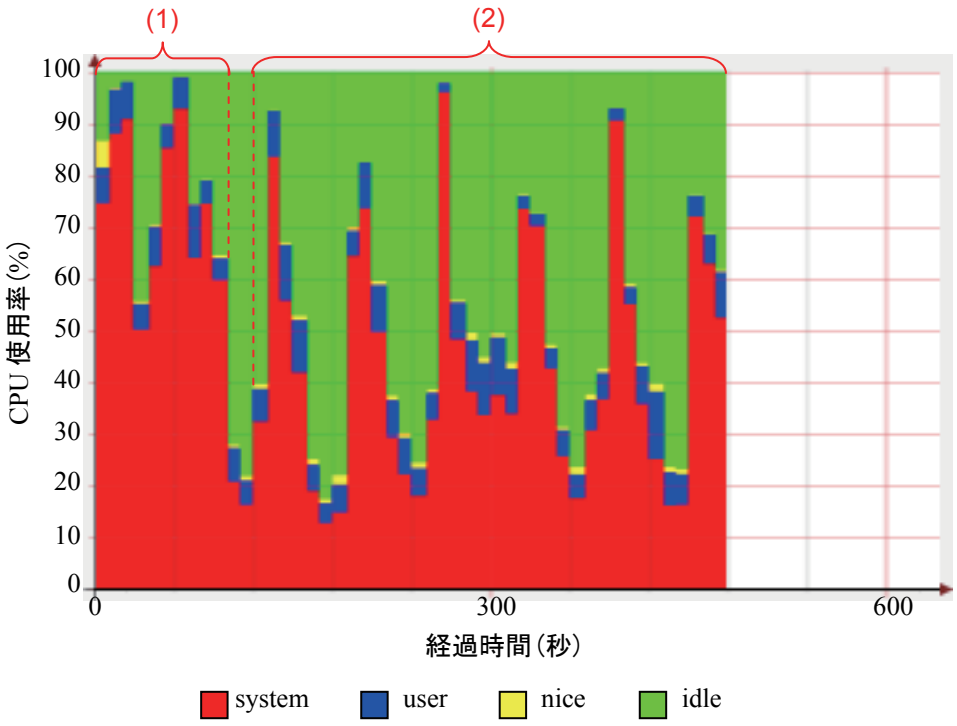


図 14 Network B におけるトラブルシューティング作業の CPU 使用率

（2）アンケート結果

表 3 に示すような質問項目，および自由記述欄から構成されるアンケートを行った．アンケート項目に対して{5 そう思う | 4 どちらかと言えばそう思う | 3 どちらとも言えない | 2 あまりそう思わない | 1 そうは思わない}の 5 段階評価と自由記述で評価を実施した．被験者は，情報系大学生・大学院生 13 名で，TCP/IP を学んだことがあり，10 台程度の小規模な LAN を構築できる者である．彼らは，本研究で想定している対象者とほぼ同じステータスである．

表 3質問項目とその平均点，および自由記述（一部要約）

質問	平均値
【1】ネットワークトラブルシューティングの演習に役立ちましたか？	4.5
【2】診断ツールの演習に役立ちましたか？	4.5
【3】TCP/IP 理論の復習に役立ちましたか？	4.4
【4】LAN 構築技能の復習に役立ちましたか？	4.5
【5】ユーザインタフェースは使いやすかったですか？	3.6
【6】トラブルのあるネットワークの準備時間(自動構築)は許容範囲内でしたか？	4.1
【7】システムの反応は許容範囲内でありましたか？	4.1
【8】操作ミスが致命傷にならないことは，演習に役立ちましたか？	4.9
自由記述	
【ア】トラブルの可能性を示したりわからない場合に怪しいポイントを点滅したりといった拡張をすると良い 【イ】操作に慣れが必要だと思う 【ウ】ウィンドウの数が増えてくると扱いにくくなる 【エ】仮想機器は壊してしまっても問題ないので，良いと思う	

アンケート結果より，学習に関する評価は概ね良好であったが，操作感に関する評価は芳しくなかった．特に，ユーザインタフェースに関して課題が残っている．

学習に関する評価は，質問【1】～【4】および自由記述【ア】である．質問【1】,【2】が本機能の主目的であるトラブルシューティングの演習に関する評価で,質問【3】,【4】が副目的であるLAN構築技能とTCP/IPの復習に関する評価である．これらの評価結果が概ね良好であることにより，本機能を講義に取り込んで使用した場合でも，高い学習効果を期待できると推定できる．また，自由記述【ア】に述べられているヒント機能の実現は，学習効率の向上になると考えられる．

操作に関する評価は，質問【5】～【8】および自由記述【イ】,【ウ】,【エ】である．質問【5】および自由記述【イ】,【ウ】から，操作手順を考慮したユーザインタフェースの設計，ウィンドウの管理機能の追加，インタフェースデザインの工夫により，本機能の使いやすさを改善できると考えられる．システム反応に関する評価(質問【6】,【7】)は，平均的な評価であった．3-4（１）で示した結果と併せて考察すると，本機能は実用に耐えうるものであると考えられる．質問【8】の評価が非常に高かったことと自由記述【エ】により，トラブルシューティングのような試行錯誤を伴う作業の演習において，仮想機器を使用することの優位性が示された．

4 ネットワークセキュリティ演習環境提供機能

4-1 機能実装

本機能は，①サーバ，②ユーザエージェント，および③アタックエージェントから成り立つ（図 15）．学習者はユーザエージェントの要求に応え，かつアタックエージェントの攻撃からサーバとネットワークを守りながらサービス運営を行う．このようなプロセスを通して，学習者は情報セキュリティの知識を実践的・体験的に身につけていくことになる．

我々はそれぞれの部品が果たすべき役割に合わせ，必要となるアプリケーションを UML 上に搭載した．これらの仮想的に作られたマシンはすべて LiNeS 内にあり，外のネットワークから孤立した UML ネットワークを作っている．

①のサーバには Apache など，演習において学習者が管理することになるサービスを提供するためのアプリケーションを搭載した．セキュリティ学習のために，このサーバはあえてセキュリティホールを抱えた設定となっている．学習者は教師の指示を受けて，このサーバ上で動くサービスの管理，あるいは複数のマシンからなるネットワークの管理を行うことになる.学習者はターミナルによって,このサーバにアクセスし，正しい設定を施していく．

②のユーザエージェントは学習者が運営するサービスを利用し，運営状態を評価するエージェント・プログラムである．掲示板サービスであればフォームへの書き込みを行うなど，サービス形態に合わせた利用を行う．また,サービスへのアクセスが不可能になった場合など,サービスの利用において不都合が生じた際,メールによって学習者へと連絡を行う．

③のアタックエージェントは攻撃ツールを活用することで，学習者の管理するサービスの妨害を試みるエージェント・プログラムである．ネットワーク上のアクティブなマシンの探査，ポートスキャンによるサー

ビスの判定を行うなど，汎用的なものとなる開発を試みている．学習者はアタックエージェントの攻撃からサービス運営を守り，必要に応じて設定を変化させながらセキュリティについて学習する．

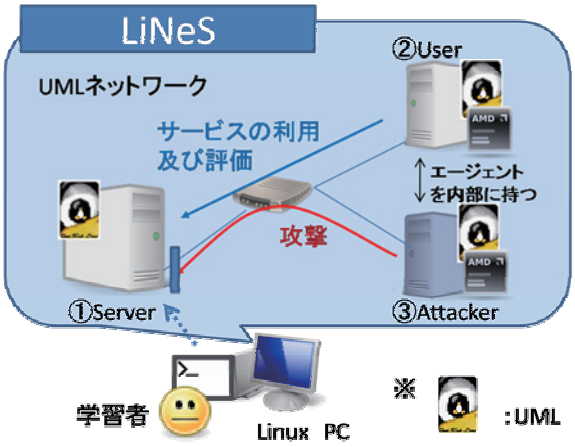


図 15　本機能の構成図

4-2 実行例

次に本機能の実行例と学習過程の一例を紹介する．この例では，学習者が 1 台の Web サーバを管理し，登録制掲示板サービスを運営するという状況を想定した（図 16）．

学習者は教師から UML ネットワーク上の Web サーバを 1 台割り当てられる．学習者はサーバに対して適切と思われる設定をほどこし，サービスの提供を開始する．サービス稼働後，UML ネットワーク内のマシン上で動作するユーザエージェントプログラムは，学習者の運営する掲示板サービスを利用するようになる（図中(Ⅰ)）．さらに一定時間後，同様にアタックエージェントプログラムが行動を開始する．アタックエージェントプログラムによる学習者の管理するサーバに対する攻撃がはじまると，学習者にはユーザからメールが届けられる（図中（Ⅱ））．メールには「サイトに接続できません」などのサービス運営状態の評価が書かれており，学習者はこの内容とサーバの状態を判断することによって，セキュリティトラブルの解決を目指す．このケースでは，ユーザの報告にあるようにサイト閲覧ができなくなっており（図中（Ⅲ）），netstat コマンドによってネットワーク接続状態を確認すると，大量の SYN パケットが届けられていることがわかる（図中(Ⅳ)）．この結果から，学習者は行われている攻撃が接続要求を繰り返し行う SYN flood 攻撃，すなわち DoS 攻撃（サービス妨害攻撃）であると判断する．そして，サーバの/proc エントリ変更によって，SYN/ACK のタイムアウト時間を短くし、tcp_max_syn_backlog の値を増やすことによって，SYN flood 攻撃への対策を行う．

本機能ではこのようなサービス運営体験の中で，より実践的・体験的なセキュリティ演習を手軽に行うことが可能になる．

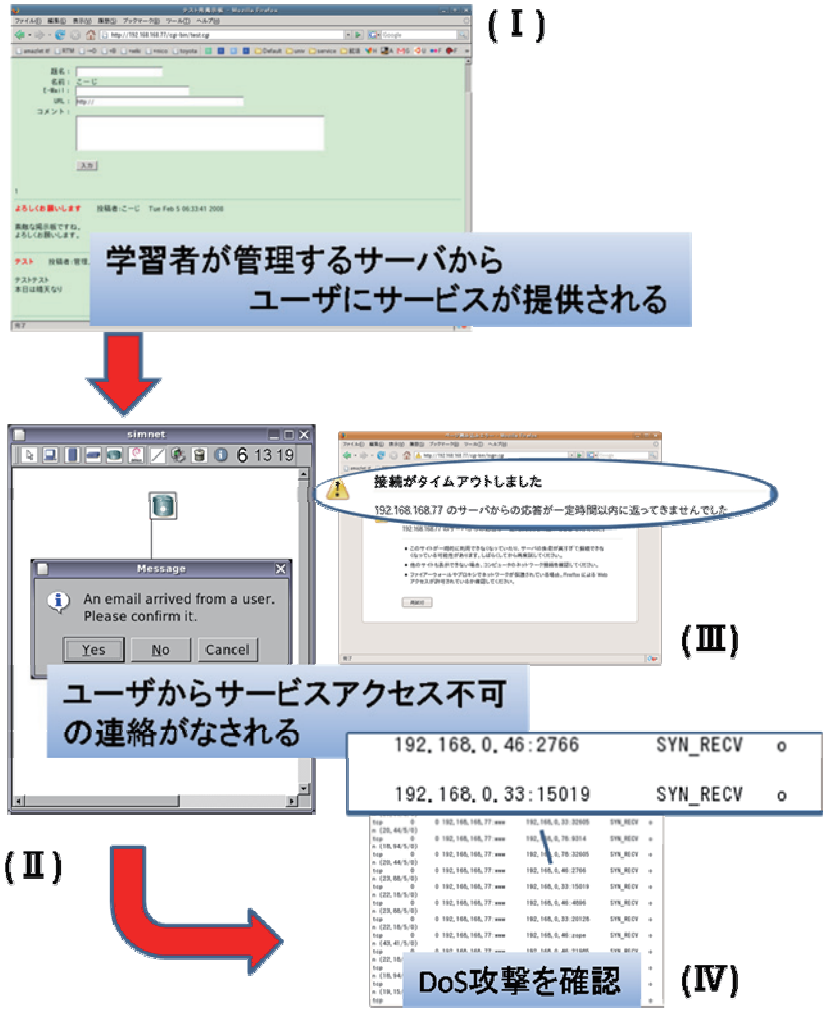


図 16 演習の流れ

5 結論

本研究では，大学や専門学校におけるネットワーク管理者教育におけるネットワーク演習環境提供システム LiNeS において，「外部ネットワークの存在を考慮したネットワーク構築演習環境提供機能」，「ネットワークトラブルシューティング演習環境提供機能」，「ネットワークセキュリティ演習環境提供機能」の開発を行った．

「外部ネットワークの存在を考慮したネットワーク構築演習環境提供機能」は，VPN 技術の活用その操作支援用 GUI の開発により実現し，これまで個々の PC 上で独立して構築していた仮想ネットワーク同士を通信可能にした．これにより，各学習者は他の学習者の管理するネットワークに配慮したネットワーク構築演習を行えるようになった．この機能の今後の課題は，性能を確認するために通信実験を行うことである．

「ネットワークトラブルシューティング演習環境提供機能」は，User-mode Linux のソースコード改造や UML-OS の改造などにより実現した．これにより，ネットワークトラブルを含む仮想ネットワークを学習者に提示できるようになった．評価実験では，トラブルシューティングの演習，TCP/IP 理論および LAN 構築技能の復習に高い効果を期待できることがわかった．一方で，ユーザインタフェースに改善の余地があることもわかった．この機能の今後の課題は，教育現場導入を考慮し，使いやすさを念頭においた改善と，教育コースの構築である．

「ネットワークセキュリティ演習環境提供機能」は，主に，擬似的なユーザと擬似的なクラッカーをユーザエージェントプログラムとアタッカーエージェントプログラムの実装により実現した．これによりセキュリティリスクのある仮想ネットワークを学習者に管理させる演習の基盤技術を確立できた．今後は，スタンドアロンな設計から，サーバ・クライアント方式へと設計を移行させ，時間の概念を導入することで，より

多くのネットワーク管理者の業務を演習できるようにすることである.

【参考文献】

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

[2] 立岩佑一郎, 安田孝美, 横井茂樹:TCP/IP 学習のための可視化シミュレータの研究, 第 3 回情報科学技術フォーラム, 情報科学技術レターズ pp.355-357, 2004 年 9 月.

[3] Tateiwa, Y., et al., "A System for Providing A Training Environment for Linux Networks using Virtual Environment Software" ,International Journal of Computer Science and Network Security, VOL.6 No.8A pp. 166-173, August 2006.

[4] 立岩佑一郎, 安田孝美, 横井茂樹:仮想環境ソフトウェアに基づく LAN 構築技能と TCP/IP 理論の関連付け学習のためのネットワーク動作可視化システムの開発, 情報処理学会論文誌, Vol.48, No.4, pp.1684-1694(2007).

[5] OPNET: http://www.opnet.com/.

[6] The Network Simulator-ns2: http://www.isi.edu/nsnam/ns/.

[7] MAADNET: http://www.maadnet.net/.

[8] Graphical Network Simulator: http://www.gns3.net/.

[9] 早川正昭, 丹野克彦, 山本洋雄, 中山実, 清水康敬:LAN 構築シミュレータの開発と教育手法の改善, 教育システム情報学会26回全国大会講演論文集, E5-4, pp.367-368(2001).

[10] 精廬幹人, 木村昌史:教育向けネットワークシミュレータの開発, 情報処理学会65回全国大会講演論文集, 2D-2, pp.273-274(2003).

[11] Anisetti, M. et al., "Learning Computer Networking on Open Paravirtual Laboratories," IEEE Transactions on Education, Vol.50, No.4, pp.302-311 (2007).

[12] 後野隆:仮想環境を利用した「サーバ構築実習」環境の構築--仮想 OS の UML(User Mode Linux)活用報告, 技能と技術, Vol.2004, 雇用問題研究会, pp.34-39(2004).

[13] VMware - Virtualization Software: http://www.vmware.com/.

[14] 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, Vol24, 教育システム情報学会, pp.126-136(2007).

[15] 上田拓実, 井口信和:仮想 Linux 環境を用いたネットワーク教育システムのための仮想ルータと GUI の実装, 第 6 回情報科学技術フォーラム講演論文集, J-026, pp.447-448(2007).

[16] Cisco Networking Academy: http://www.cisco.com/web/learning/netacad/.

[17] Hu, J., et al., "Tele-Lab IT Security: An Architecture for Interactive Lessons for Security," Computer security, Volume36, Issue1, pp.412-416, ACM, New York (2004).

[18] Walden, J., et al., "A real-time information warfare exercise on a virtual network," Capstone projects, pp. 86 – 90, ACM, New York (2005).

[19] Azadegan, S., "A dedicated undergraduate track in computer security education," Security education and critical infrastructures, pp.319-331, Kluwer Academic Publishers, Norwell (2003).

[20] OpenVPN-An Open Source SSL VPN Solution by James Yonan: http://openvpn.net/.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
仮想環境ソフトウェアに基づくネットワークトラブルシューティング実習環境提供システムの評価	第 6 回情報科学技術フォーラム 情報科学技術レターズ, pp. 469−470	2007 年 9 月
マルチユーザ型 LAN 構築実習環境提供システムについての研究 -VPN を用いた仮想ネットワーク間相互接続機能の開発-	教育システム情報学会第 32 回全国大会 講演論文集, pp.340-341	2007 年 9 月
仮想環境ソフトウェアに基づく Linux ネットワークトラブルシューティング実習環境提供システムの開発	情報処理学会コンピュータと教育研究会 第 92 回研究会情報処理学会研究報告	2007 年 12 月

	2007-CE-92，pp.37-44	
LAN 構築実習システムにおける仮想 WAN の VPN による構築とその支援機能の開発	情報処理学会コンピュータと教育研究会 第 92 回研究会情報処理学会研究報告 2007-CE-92，pp.45-50	2007 年 12 月
DEVELOPMENT OF A SYSTEM FOR PROVIDING A TRAINING ENVIRONMENT FOR NETWORK TROUBLESHOOTING BASED ON VIRTUAL ENVIRONMENT SOFTWARE	Advances in Computer Science and Engineering, Vol.1, No.3, pp.223-248	2008 年 1 月
仮想化技術に基づくネットワーク管理者育成支援システム LiNeS におけるセキュリティ演習機能の開発	JSiSE 第２回 学生･院生研究発表会，講演論文集	2008 年 3 月