2007－CE－92 (7)
2007／12／7

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

倉地 宏輔† 立岩 佑一郎† 安田 孝美† 横井 茂樹†
†名古屋大学大学院情報科学研究科

抄録：近年，インターネットの普及に伴うネットワーク管理者教育の必要性が叫ばれている．これに対し，我々はUser-mode Linuxを用いたLAN構築実習システムの開発を行ってきた．今回，仮想WAN（Wide Area Network）という実際のネットワーク社会に近い環境を作り出しての実習を実現したので報告する．学習者や指導者が各々のPC内に構築した仮想ネットワーク（仮想LAN）同士をVPN技術によって接続することで仮想WANを構築できる．接続に伴うシステムへの情報入力のなど学習上の負担は，セットアップウィザードやVPN接続申請自動化システムなどのユーザ支援システムにより軽減している．これにより，仮想WANの手軽かつ柔軟な構築が可能となった．

Development of the function for supporting construction of the virtual WAN based on VPN in the training system for LAN construction

Kosuke KURACHI† Yuichiro TATEIWA† Takami YASUDA† Shigeki YOKOI†
†Graduate School of Information Science , Nagoya University

Abstract: Recently, the necessity of the network administrator promotion is insisted because of spread of the Internet. Therefore, we have developed a training system for LAN construction based on User-mode Linux. This time, we realized a practice by producing environment near actual network society that is called the virtual WAN. To construct the virtual WAN, the system we developed can connect two or more virtual LANs students or their teacher constructed. The connection is based on the VPN technology. When the system connects virtual LANs mutually, students or their teacher will feel a burden. Because they should execute the operation unrelated to LAN construction. We have reduced this burden by the function for supporting construction of the virtual WAN. The function consists of setup wizard and an automation system for VPN connection. Consequently, easy and flexible construction of Virtual WAN became possible.

1. はじめに

近年，インターネットの普及に伴うネットワーク管理者育成の必要性が叫ばれている．しかし，将来のネットワーク管理者を育成すべき専門学校や大学のネットワーク実習では，コスト等の問題から生徒個々人に十分なネットワーク機器を用意できず，グループ実習などによる個人の理解度の低下を招いている．

こうした現状を解決するため，我々は仮想環境ソフトウェアUser-mode Linux[1]（以下UML）を用いたLAN構築実習システムLiNeS（Linux Network Simulator）の開発を行ってきた[2]．UMLを用いることでネットワーク機器を仮想環境に実現し，直感的なGUI（Graphical User Interface）による仮想ネットワークの構築，管理を行うことができる．また非常に動作が軽快であるというUMLの特性から，1台の標準的なPC上に20台程度まで仮想機器を立ち上げることができ，柔軟なネットワークの構築が可能である．本システムによって，1台のPC上での手軽なネットワーク実習環境が実現され，Linuxサーバを中心としたLAN構築実習を行うことが可能になった．

LiNeSには，従来非現実的であった実習を実現できるという利点がある．例えば，UMLの設定により故障したネットワーク機器を作り出し，トラブルシューティング実習に利用することなどが可能である．しかしその一方で，LiNeSを用いた実習にはネットワーク管理者が考慮すべき「管理外のネットワーク」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実習することができないという問題も存在している．

本研究では，LAN構築実習システムLiNeSへの「管理外のネットワーク」を目的として，仮想WANという実際のネットワーク社会に近い環境を作り出しての実習を実現した．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（以下仮想LAN）をVPN技術によって接続し，仮想WANを構築できる．学習対象が，従来のシステムでは1台のPC上での個々のネットワーク管理（仮想LAN）だったことに対し，本システムでは「他者の仮想LAN」を含むネットワーク社会全体（仮想WAN）になる．これにより，従来リアリティが欠如していた学習項目に対す

る効果的な実習が可能になった[3]．また，VPN接続に伴うデータの入力など学習上の負担は，セットアップウィザードやVPN接続申請自動化システムなどのユーザ支援システムにより軽減している．これにより，仮想WANの手軽かつ柔軟な構築が可能になった．

表1　実習項目の比較

	仮想LAN	仮想WAN
ネットワーク設定	自分の管理できるネットワーク内だけで完結	他の学習者が管理する仮想LANへの影響を考慮
ネットワークサービス実験	学習者自身でWebサーバ，メールサーバ等の設置，動作確認	他の学習者の仮想LANからサービスを受けられるか確認可能
セキュリティ実験	学習者自身でセキュリティの設定，安全性確認	他の学習者の仮想LANからの攻撃，不正アクセス実験による安全性の確認が可能
トラブルシューティング演習	学習内容が小規模トラブルに限定	WAN規模のトラブルシューティング演習が可能
学習者間のコミュニケーション	1つの問題に関する解決法を同じ視点で相談	1つの問題に関する解決法を異なる視点で相談

2. 関連システム

本研究と同様に仮想環境を用いてネットワーク管理者教育を実現したシステムを例に挙げ，本研究で開発したシステムの研究目的に対する有効性を示す．

VMUML[4]はXMLベースの記述言語によって，UMLによる仮想ネットワーク構築を支援するシステムである．IPv6の実験用ネットワーク構築という目的で開発され，サーバアプリケーションのテスト等への利用が想定されている．UMLを利用している点では本研究と似ているが，教育ではなくシミュレーション目的であることや，システムにGUIを採用しておらず教育に不向きである点が異なっている．

後野はUMLを利用したサーバ構築実習環境を構築している[5]．実習室に元々ある機器とUMLのみを用いて，学習者1人に対する2台以上のサーバ提供（仮想OSを含む）とネットワーク間通信が実現される．UMLを利用している点やコストダウンを目的としている点，ネットワーク間通信の実現を目指している点など，本研究と類似する部分も多い．しかし，サーバ構築に関する実習に重点をおいているため，ネットワークの構築やルーティングの設定を自由に行うことはできず，ネットワーク全体の構築・管理を学習することができない．

中川らはVMWare[6]を利用し，集団学習を目的とした学習用LAN構築支援システムを開発した[7]．Windows上で自由に仮想ネットワークを構築できるという利点があるが，演習室内での利用を前提とした設計がなされており，高価な実機が多数必要になるなど導入への敷居が高い．ネットワーク実習導入の敷居を下げるという，我々の研究の発端となった目的とは異なる方向性を持ったシステムであるといえる．

上田らは，我々と同様にUMLを利用し，ネットワーク教育システムを開発した[8]．しかし，このシステムはシスコネットワーキングアカデミー[9]の支援を目的としたものであり，ルータやスイッチングハブ設定など，下位層プロトコルの学習を対象としている．これに対し，我々のシステムはサーバアプリケーションなどの上位層プロトコルを中心とした学習を対象としており，目的とする学習分野が異なっている．

以上4件の仮想環境ソフトウェアに基づくシステムと本研究で開発したシステムの比較を行ったが，導入の手軽さと自由なネットワーク構築，仮想環境におけるリアリティの全てを追及したシステムは未だ存在しないといえる．これにより，我々の開発したシステムの研究目的に対する有効性が示された．

3. システムの要件

ここでは，LiNeSへ「管理外ネットワーク」を導入するために求められるシステムの要件を述べる．

「管理外ネットワーク」を実現するためには，学習者が管理できないブラックボックスになっているネットワークを，何らかの方法で従来LiNeSの仮想LANに参加させなければならない．もっとも単純な解決策として，このブラックボックス部分をあらかじめ開発者側で構築，ユーザが操作できないようにプロテクトしておき，LiNeSに組み込んで配布する方法が考えられる．この機能は既に，「擬似インターネット」としてシステムに実装されている．しかし，「管理外ネットワーク」が影響する学習項目では，ネットワーク管理者同士のオフラインでのコミュニケーションも重要であり，このようなコミュニケーションのシステムによる実現は非常に困難である．

そこで我々は，学習者や指導者が構築した仮想LAN同士を接続することによって「管理外ネットワーク」を導入する方法を考案した．他者が構築・管理する仮想LANは，自分から見れば「管理外ネットワーク」に他ならない．また，実習室でのシステム利用においては，接続先の仮想LAN管理者とコミュニケーションをとって問題解決を行うことも可能である．

異なるホストマシン上に構築された仮想 LAN 同士の接続を実現するためには，ホストマシン同士が実環境ネットワークによって接続されていることが必須である．加えて，UML の機能により仮想 LAN とホストマシンを TUN/TAP 接続することで初めて，仮想 LAN 同士が接続された状態になる．しかし，この接続方式のままでは仮想 LAN と実環境ネットワークが混在する状態になってしまい，学習者の混乱を招く恐れがある．よって，仮想 LAN と実環境ネットワークを切り分けた状態で，実環境の部分がどのような状態でも接続先の仮想 LAN と通信できるような手段を選択しなければならない．

また，これと並行して，学習者や講師を含むユーザへの負担を考慮する必要もある．従来の LiNeS における「手軽さ」を維持したまま，学習効率を損なうことのないシステムを実現する．

最後に，従来 LiNeS が想定している利用環境をそのまま維持することを目指す．インターネットに接続しているという条件が加わるが，PC が 1 台あれば，特殊なネットワーク設定をすることなく導入可能なシステムの設計を行う．

4. システムの実現方法

図 1 に，本研究で開発したシステムの構成図を示す．本システムは，大きく分けると仮想ゲートウェイとユーザ支援システムの 2 つから成り，指導者用と学習者用で異なったものになる．このため，LiNeS も指導者用と学習者用の 2 つのバージョンに拡張した．仮想 WAN を構築するときに必須となる VPN は，仮想機器である仮想ゲートウェイと，指導者用 LiNeS における仮想ゲートウェイである仮想ゲートウェイマネージャを起点として構築される．

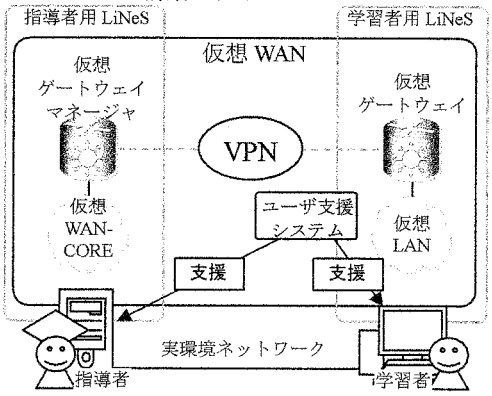

図 1　システムの構成図

4.1. 仮想 LAN 間接続の実現

本システムでは，仮想 LAN 同士の接続に VPN 技術を利用している．VPN（Virtual Private Network）とは，インターネット上に仮想的な専用ネットワークを構築して異なるセグメントに属したネットワーク同士の直接的な通信を実現する技術であり，このとき構築された専用ネットワーク自体も VPN と呼ぶ．有効な接続先を指定し，接続先からの承認が得られれば，中間のネットワーク構成に左右されることなく VPN が構築されるという特徴がある．

この技術を仮想環境に適応することで，ホストマシン間の実環境ネットワークの設定を無視して仮想 LAN 同士を接続することが可能になった．学習者や講師がホストマシン間の実環境ネットワークに特殊な設定を施す必要はない．また，仮想 LAN のインターネットを介した接続も可能になるため実習時間外のシステム利用や自宅からの利用にも応用可能である．さらに，VPN 内では通信が暗号化されるため，外部からの影響，外部への影響を考慮する必要がなく，処理のすべてが仮想環境内で完結するシステムを構築することができる．今回は，開発のしやすさなどを考慮して，オープンソースである OpenVPN[10]というソフトウェアを採用した．

図 2 に本システムにおける仮想 WAN の構築方法を示す．OpenVPN には OpenVPN サーバ，OpenVPN クライアントという 2 種類のモードがあり，OpenVPN サーバをインストールした機器 1 台と，OpenVPN クライアントをインストールした機器複数台の間で VPN が構築される．これはそのまま，指導者が 1 人で学習者が複数という実習の人員構成と類似している．そこで，指導者の LiNeS には OpenVPN サーバを，学習者の LiNeS には OpenVPN クライアントを導入し，指導者が構築した仮想 LAN の周辺に学習者が構築した仮想 LAN が繋って仮想 WAN を構築する方法を考案した．なお本稿では便宜上，指導者が構築した仮想 LAN を仮想 LAN-CORE と呼ぶことにする．

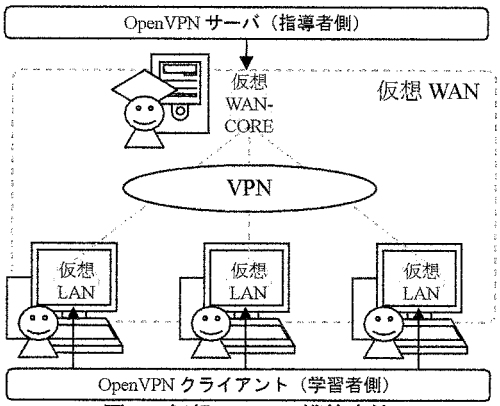

図 2　仮想 WAN の構築方法

4.2. 仮想ゲートウェイの構築

従来のLiNeSにOpenVPNを導入するためには，いくつかの問題が存在する．

まず解決しなければならないのが，LiNeSインタフェースからのVPNの起動である．学習者が他の仮想機器と同様の感覚でVPNを起動し，仮想WANに参加できる必要がある．また，学習者の混乱を避けるため，VPNが使用されていることを極力表に出さないようなインタフェース設計にしなければならない．そこで，我々は仮想ゲートウェイという新たな仮想機器を作成しLiNeSのインタフェースに配置した．

LiNeSにおける仮想機器の数々はUMLカーネルにカスタマイズしたルートファイルシステムを読み込ませることで実装されている．仮想ゲートウェイも同様に，UMLカーネルにOpenVPNインストール済みのルートファイルシステムを読み込ませることで実装した．指導者用LiNeSの仮想ゲートウェイ（以下，仮想ゲートウェイマネージャと呼ぶ）にはOpenVPNサーバが，学習者用LiNeSの仮想ゲートウェイにはOpenVPNクライアントが組み込まれている．

仮想ゲートウェイは3つのポートを持ち，1つは学習者が構築した仮想LANに，2つ目はホストマシンのある実習環境のLANに，3つ目はVPNに接続される．実際は仮想LANと実環境LANの間でデータをやり取りしているが，VPNにより学習者には仮想LANと仮想WAN-COREの間でデータのやりとりが行われているように見える．なお，ルータとしての性質も持ち，コンソールからの制御も可能なため，こちらに直接ファイアーウォールの設定を行うことも可能である．この構造は，仮想ゲートウェイマネージャにおいても同様である．

仮想ゲートウェイマネージャは接続待ちのため常時起動，仮想ゲートウェイは実習に応じて適宜起動させることを想定している．

4.3. セットアップウィザードの構築

OpenVPNを用いてVPNを構築するためには，自分の実習環境を示すパラメータやOpenVPNサーバが発行した証明書が必要であり，これらを仮想ゲートウェイに転送しなければならない．パラメータとは，例えば実習用ホストマシンのIPアドレスなどであり，このような動的な情報をあらかじめLiNeSに組み込んでおくのは不可能である．さらに，仮想ゲートウェイへのパラメータ，証明書ファイルの直接的な転送は，高度なLinux操作技術やUML特有の操作が必要になるため，学習者にとってシステムのハードルを上げてしまう恐れがある．

この問題を解決するための機能が，UMLのホストファイルシステムという機能を利用したセットアップウィザードである．図3にセットアップウィザードを用いたデータ転送の概念図を示す．ホストファイルシステムとは，UMLとホストマシンの両方がアクセスできる共有スペースを作り，そこを経由して仮想機器とホストマシンの間でファイル転送を行う機能である．セットアップウィザードは仮想ゲートウェイ起動時に立ち上がり，ユーザは必要な項目を入力するだけでよい．セットアップウィザードが終了すると，プログラムに入力したデータを元に設定ファイルが生成され，仮想ゲートウェイへのファイル転送が行われる．

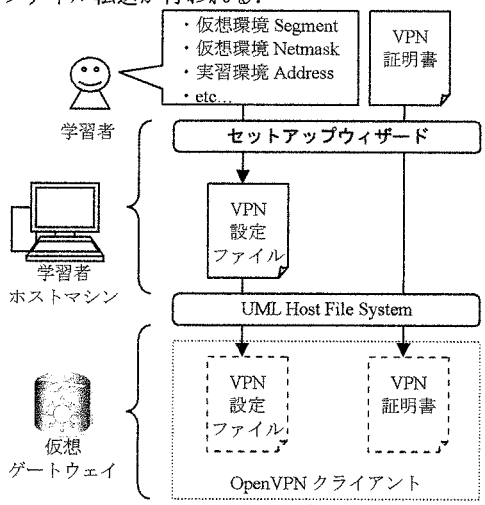

図3 セットアップウィザードを用いたOpenVPNへのデータ転送

4.4. VPN接続申請の自動化

指導者も学習者と同様に，接続してくる仮想LANの情報を仮想ゲートウェイマネージャに追記しなければならない．加えて，学習者の認証と識別のため，学習者ごとに異なる証明書を発行する必要がある． 指導者が学習者に一人ひとり対しこれらの処理を行うことは，指導者にかかる負担を考えれば非現実的である．

このような指導者の負担は，VPN接続申請自動化システムにより解決した．図4は，プログラムとの会話を自動化するプログラムであるexpect[11]を用いた，VPN接続申請の自動化を説明している．仮想ゲートウェイマネージャに記述するデータは，学習者側仮想LANのパラメータがほとんどである．よって，学習者が仮想ゲートウェイ起動時にセットアップウィザードに記入するデータを流用することが可能である．仮想ゲートウェイマネージャが接続待ちのために常時起動なのを利用して，学習者側ホストマシンからSSHでリモートアクセスし，直接デー

タの追記，証明書の発行申請を行う．その後 FTP を用いた証明書のダウンロードを行えば，講師の負担をなくすことができる．システムはセットアップウィザードに入力されたデータのうち，必要なものだけを組み合わせて SSH や FTP セッション用のスクリプトを生成する．このスクリプトを expect に読ませることで VPN 構築手続き自動化することができ，学習者の負担にはならない．

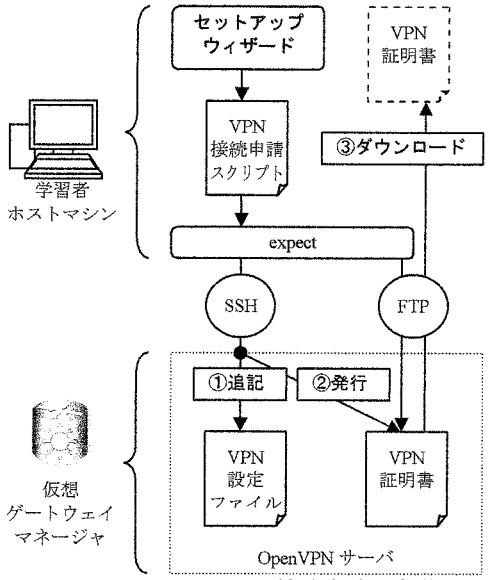

図 4　expect による VPN 接続申請の自動化

5.　システムの実行例

仮想 WAN を構築している様子を図 5 に示す．左が指導者，右が学習者の見ている画面である．まず，学習者は，従来 LiNeS と同様にインタフェース上で自由に仮想ネットワークを構築する．指導者から仮想 WAN に接続する指示があると，学生は仮想ゲートウェイアイコンをクリックし，セットアップウィザードを起動する．続いて学習者はセットアップウィザードに自己の学習環境を入力し（図 6-a），仮想ゲートウェイマネージャへのデータ登録，証明書のダウンロードを行い（図 6-b），仮想ゲートウェイを起動する（図 6-c）．以上の操作で仮想ゲートウェイマネージャと学習者側 LiNeS 内の仮想ゲートウェイの間に VPN が構築され，仮想 WAN-CORE と仮想 LAN の間で通信が可能になり，学習者の仮想 LAN は仮想 WAN に加わったことになる．

次に，構築した仮想 WAN を用いた実習の例を紹介する．先ほどの仮想 WAN 構築例に，さらに学習者を 1 人追加した，仮想 WAN-CORE1 つ，仮想 LAN2 つからなる仮想 WAN を構築する．学習者 A は図 7 のように，自分で構築した仮想 WAN の Web サーバに HTML によるテストページをアップロードしておく．学習者 B は，構築した仮想 LAN のクライアントから，仮想 WAN-CORE を経由してこの Web サーバにアクセスし，テストページを取得できるかを確認する．クライアントの Web ブラウザに Web ページが正常に表示されれば，ネットワークの設定が正しいことがわかる．もし正常に表示されなければ，自分（学習者 B）が管理する範囲内に設定ミスがないか，相手（学習者 A）の設定は本当に正しいかを学習者同士でとコミュニケーションをとりながら確認し，設定を改善していく．

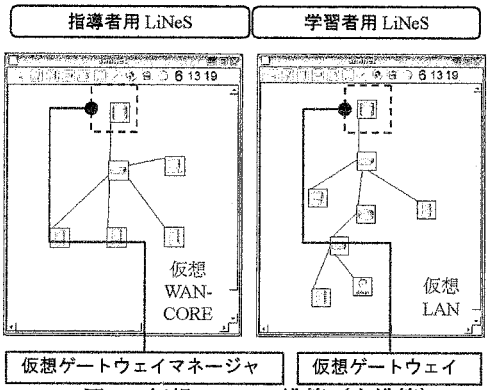

図 5　仮想 WAN の構築（未構築）

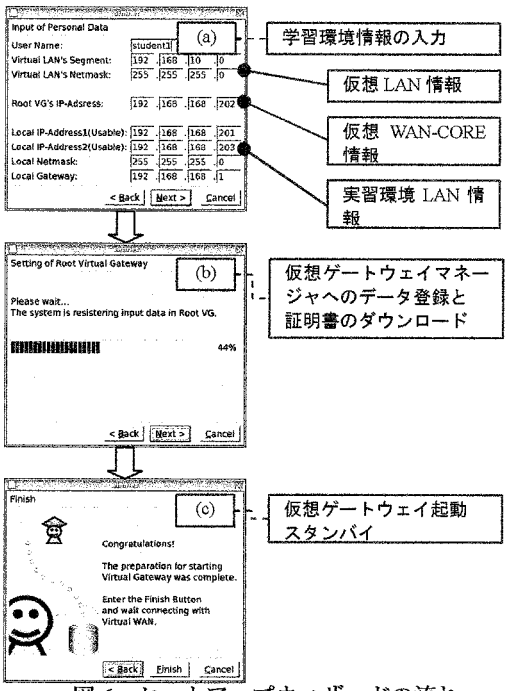

図 6　セットアップウィザードの流れ

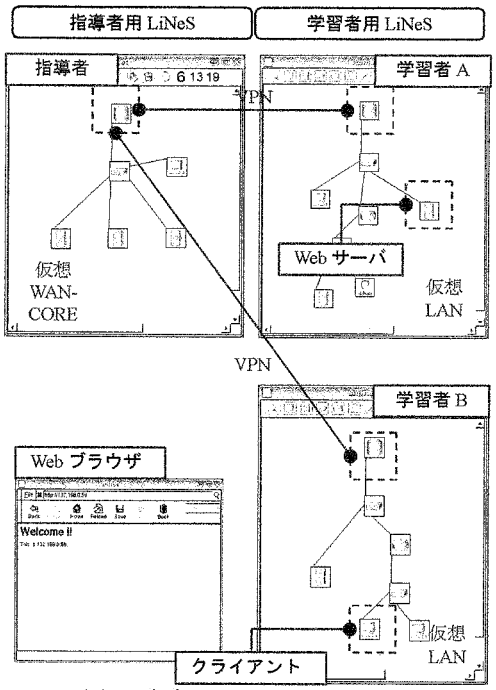

図 7　仮想 WAN を用いた実習例

6. おわりに

本研究では，LAN 構築実習システム LiNeS に仮想 LAN 接続機能を組み込むことで，仮想 WAN という実際のネットワーク社会に近い環境を作り出して実習を行うことができるシステムを開発した．

仮想 WAN は仮想 LAN 同士の接続に VPN 技術を活用することにより実現された．また，VPN 構築時のデータ転送や対話的手続きなどの手間を，セットアップウィザードと VPN 接続申請自動化システムにより解消し，ユーザの負担軽減に成功した．

小規模ネットワークを用いた通信実験の結果，システムによる仮想 WAN の構築が確認されたが，仮想 WAN への接続者が増加した場合のシステムの挙動やスループットなど検討する必要のある部分は多い．

今後は，システムの有効性を測る評価方法を検討し，その方法を用いての評価実験を行う予定である．

謝辞：本研究の一部は，科研費および（財）電気通信普及財団の研究助成による．

7. 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：“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におけるトラブルの拡充とユーザインタフェースの拡張”，情報処理学会第 69 回全国大会，講演論文集 6G-8 pp.4-319--320（2007）

[3] 倉地宏輔，立岩佑一郎，安田茂樹，横井茂樹：“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）

[4]Virtual Network User Mode Linux (VNUML): http://www.dit.upm.es/vnumlwiki/index.php/Main_Page

[5]後野隆：“仮想環境を利用した「サーバ構築自習」環境の構築　-仮想 OS の UML（User Mode Linux）活用報告-”，技能と技術 Vol.2004, No.5 (2004/9) (通号 228) pp. 34--39

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

[7] 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”，教育システム情報学会誌，Vol.24, No.2，pp.126-136（2007）

[8] 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開発”，電子情報通信学会関西支部第 12 回学生研究発表講演会，講演論文集 D2-5　pp.77（2007）

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

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

[11] The Expect Home Page: http://expect.nist.gov/