ネットワークセキュリティー教育のためのネットワーク教育環境の構築と実習

ネットワークセキュリティー教育のためのネットワーク教育環境の構築と実習

仲 間 正 浩*

Development of Network Environment and Training for Network Security Education

Masahiro NAKAMA

1．はじめに

従来、コンピュータのインターネット環境は、コンピュータ資源がボランティアで提供される平和的な環境であった。その環境では、インストールの容易さと操作の簡便さを重点的に追及するようなコンピュータ及びソフトウェアの開発が行われてきたため、新規に購入したOSを初心者がインストールすれば、様々な標準的なサーバーソフトがデフォルトで実行され、すぐに使えるようになっていた。そのような状況下でのコンピュータ設置、管理の教育指導は、ネットワークセキュリティーを考慮する必要は無く、単純にOSのインストールを行わせた後で、利用方法や、管理方法を教授するだけで十分であり、また、何の問題も生じなかった。

しかしながら、近年、不正侵入のためのソフトウェアツールが大量に、コピー、配布されたため、不正侵入されるコンピュータの数は急速な勢いで増加しつづけるような状況になってしまった[1]。

現在では、従来の指導方法でOSのインストールを行わせ、それに、セキュリティー的な対策を何も施さなければ、間違いなく一週間以内に不正侵入されるような状況になっている。事実、本コースでもそのような状況はたびたび発生していた。また、本学部でも、6台以上のコンピュータが不正に利用されて、システムを停止した。本稿執筆時点でも、不正侵入された状態で稼動しつづけているコンピュータが本学部内に存在しつづけている。

不正侵入されたコンピュータをそのまま放置すれば、それが、悪用されて、内外に多大な悪影響を与える危険性があるため、多くの大学で、コンピュータネットワークを管理する担当教官が、本来の教育・研究を行うことにも支障が出る程の状態に陥っている。

このような状況を回避するため、コンピュータのセキュリティー管理をアウトソーシング（外注）する必要があるとの意見も多く聞かれるようになり始めている。しかしながら、セキュリティー的に完全に安全な環境では、セキュリティー対策を行える人材を育成することは困難であり、また、そのような人材を早急に育成する必要であることも、確かである。

この状況を早急に改善する必要があると考え昨年度一年間に、まず、緊急措置的に3台の使い古したコンピュータを投入し、さらに、2台のネットワークコンピュータを購入した。そして、コンピュータセキュリティー教育方法を検討し、それを実施するためのネットワーク環境を整備してきた。本稿は、その検討の結果を報告する。

* Department of Computer Science、 Faculty of Education、University of the Ryukyus. Nishihara、 Okinawa、 903-0213.

2．安全でないネットワーク教育環境の必要性

単純に、インターネット上のホームページを閲覧したり、ホームページを制作して公開するのみならば､セキュリティー的に安全に管理されたセキュアーなネットワーク環境を構築すればよい。そのような環境下に設置されたコンピュータ端末は、コンピュータウィルスに対する脅威を警戒するのみでよく、インターネット上から､直接的な攻撃を仕掛けられても被害を受けることが無いので安心してコンピュータの設置と管理を行うことができる。しかし、このような環境はその安全性ゆえに、頻繁に起こっているインターネット上のサーバーに対する攻撃の脅威を認識することができない、従って、ネットワークシステムを安全に管理できるような人材を育成するためには、ネットワーク上からの攻撃を直接受ける安全でないネットワーク環境を保有しておく必要があると考える。

2．1．ファイアーウォールで実現できるセキュリティーレベル

今日、様々なファイアーウォール製品が開発され、出荷されるようになってきているがその代表例として、以下が挙げられる。

・パケットフィルタリング
・アプリケーションゲートウェイ

前者と後者を比較した場合、ファイアーウォール管理の負担が少ないのが前者である。従って、本研究では、前者のファイアーウォールを使ってシステムを構築することにした。

インターネット上を流れる主な代表的なデータ通信プロトコルとして、ＴＣＰとＵＤＰがあげられる。前者は、サーバーとクライアントの種別に応じてのアクセスコントロールが可能であるが、後者は、それができない。従って、学習の初期段階では、前者にかかわるサーバーを実習の対象とし、後者を利用するサーバーについてはある程度の、セキュリティー管理能力が備わった後で実習の対象にすることが望ましいと考えた。

データ通信プロトコルをＴＣＰに限定して考えた場合、ほとんどの個々のインターネットサービスにおいて以下のような性質を持つネットワーク環境をパケットフィルタリングのファイアーウォールで実現することが可能である[3]。

Lan-a．インターネットに接続されていない環境
Lan-ｂ．クライアント端末は安全に守られ、外部にサーバーを公開できないネットワーク：インターネットに接続されていて、外部のサーバーにクライアント接続はできるが、外部に対してサービスを提供できないネットワーク
Lan-ｃ．サーバー設置環境としてのみ機能するネットワーク：インターネットに接続されていて外部のクライアントに対してサービスを提供できるが、他のサーバーにクライアント接続できないネットワーク
Lan-ｄ．セキュリティー制限をまったく受けないネットワーク：インターネットに接続されていて、外部に対してクライアント接続も、サービスの提供も何でもできるネットワーク

このような、環境を適切に利用すれば､学習者のスキルにあわせた適切な実習指導が行えるものと考えた。

2．2．サーバーのプロトコルと他サーバーへのアクセス

表２．１．に、主なインターネットサーバーで、使用するプロトコルとそのサーバーが、インターネットパケットの視点で見て、クライアントとして、他サーバーへ常にアクセスするかどうかを示す。

もっともポピュラーなWWWサーバーは、特別な機能を実装しなければ、基本的には、サーバーとしてのみ機能する。FTPサーバーは、クライアントで、用意したポートに対して、サーバーの方

表2.1　主なサーバーのプロトコルと他サーバーへのアクセス

サービス種別	プロトコル	他サーバーへのアクセス
WWW	TCP	なし
FTP	TCP	あり
mail	TCP	あり
dns	TCP+UDP	あり

から、アクセスを開始する。そのため、ここでは、他サーバへのアクセスありとした。FTPは、その性質上、不正侵入を試みようとするものが、あるクライアントへFTPサーバーからの返事を装えば、外部へのFTPアクセスを可能にしているネットワークエリアにファイアーウォールを越えて不正パケットを送りつけることが可能になる。実際、多くの不正行為を行う者が、この性質を利用して、不正侵入のためのネットワークスキャンを行っている。

このことから,初心者のインターネットサーバー設置導入は、WWWサーバーなどの性質のものを２．１．で示したLan-c等の環境で実施するのが望ましいものと考えた。

以下では、２．１．と２．２．の事実を基礎にして、学習者のスキルをどのようにレベルアップしていき、また、それぞれのレベルで,どのような環境を利用していくかということを議論する。

３．ネットワークセキュリティー教育の段階と、実習環境

ネットワークセキュリティー教育の教育目標を簡単に言えば、

インターネット上で外部に開放されたサーバーやLANの設定及び安全な運用ができるようにすること

であるが、いきなり、外部に完全に開放された環境で実習を行えば、未熟な学習者が設置したシステムは、いきなり侵入されてしまう危険性が非常に高くなる。

前に述べたように、完全に安全に管理された環境で実習を行った場合には、インターネット上の危険性を認識することは困難であり、完全に安全なサーバーやＬＡＮを実現できたとしても、どれ程安全であるかを確認するのは不可能である。従って、ある程度の危険性を残した上での実習環境も実現しておくのが望ましいものと考える。その環境を利用した実習を体験することによって、油断をすれば、外部から、簡単に侵入されてしまうという危機意識をもってもらうことも重要な教育の一環になると考える。実際のインターネット上でも、セキュリティー意識を持たない管理者が運営しているサーバーやLANのほとんどが、容易に侵入されていることからもその重要性は、明らかであると考える。

これと同じような考え方の教育は、一般的にも行われている。例えば、自動車教習では、

・自動車シミュレーター
・教習所構内
・公道（教官付き添い）
・公道（免許取得後、教官付き添い無）

の順に実習環境を学習者のスキルに合わせて変化させている。

以下では、これと同じような実習のあり方を、コンピュータネットワークではどのような環境でどのように行っていくのが適切であるかを論じる。

３．１．サーバー用、クライアント用OSの設置と、ネットワークプロトコルの理解

〔ネットワーク実習第１段階〕
クライアント端末は安全に守られ、外部にサーバーを公開できないネットワーク（Lan-b）上でのクライアント端末の設置

この段階の実習は、Lan-bの環境で行う。この環境は、メールやWebを閲覧することによって、コンピュータウィルスに感染する危険性は残るが、コンピュータを長時間動かしても外部ネットワークから不正に侵入される危険性は無い比較的安全な環境である。

＜合格基準＞
・コンピュータのOSをインストールできること
・コンピュータをインターネットに接続できること

〔ネットワーク実習第２段階〕
クライアント端末は安全に守られ、外部にサーバーを公開できないネットワーク（Lan-b）上でのインターネットサーバーの設置

外部には公開していないネットワーク上で、イ

ンターネットサーバーの設置の実習を行う。このエリアにサーバーを設置しても、外部ネットワークからそれを参照することはできないが、Lan-b内部のネットワークからの、参照、利用は可能である。この環境にサーバーを設置しても、ネットワーク外部から不正に侵入される心配は無い。この環境では、WWW、NFS、SAMBA、Netatalk、Telnet、FTP、データベースサーバー等の各種インターネット、イントラネットサービスを設置する実習を行う。

＜合格基準＞
・各種インターネットサーバーをインストールできること
・設置したサーバーを適切に管理できること

〔ネットワーク実習第３段階〕
インターネットに接続されていない環境（Lan－a）でのローカルネットワークの構築

インターネットとは完全に遮断された環境で、ネットワークを構築する。この段階では、２つ以上のローカルネットワークをルーターによって相互に接続する実習を行う。インターネット全体が、基本的にルータによるネットワーク間接続によって実現できることをこの実習によって理解してもらう。次いで、この環境において、dns、DHCP、mail、等の、設定方法を誤ると、他のシステムに影響を与えるようなサーバー設置の実習を行う。

＜合格基準＞
・簡単なLANを構築できること
・LAN上で必要な基礎的なサーバーの設置運用ができること

〔ネットワーク実習第４段階〕
クライアント端末は安全に守られ、外部にサーバーを公開できないネットワーク（Lan-b）での、ネットワークセキュリティー情報の取得、及びインターネットに接続されていない環境（Lan-a）でのネットワークセキュリティー対策の演習

Lan-bで、セキュリティー対策が施されたサーバーパッケージを、インターネットサイトから取得する。同時に、ネット上の様々なサイトから、インターネットセキュリティーに関する情報を得て、学習を行う。この活動を通じて得られた、情報やパッケージを基礎に、Lan-a上にセキュリティーを施されたサーバーやLANを設置する実習を行う。その実習は、まず、はじめに、
・サーバーのログの検査方法
・サーバー改竄検知ツールの使用方法
・不正パケット検知ツールの使用方法
・ポートスキャンツールの使用方法
等の実習を通して基本的なネットワークセキュリティーツール類の使用方法を学び、それらの使い方を熟知した上で、
・外部から侵入されないセキュリティー対策の実地方法
・ネットワークサーバーの基本的な管理方法
・設置したサーバーのセキュリティー強度の検査方法
・外部ネットワークからの侵入の検出方法
・侵入を受けた場合の、対処方法

等の具体的なネットワークセキュリティー管理の方法を、インターネットから完全に遮断された環境で実習する。

＜合格基準＞
・各種ネットワークセキュリティーツールを取得、利用できること
・セキュリティーホールのあるプログラムを安全な最新のものに更新できること
・不正侵入を阻止する方法を身につけること
・不正侵入を検出できること
・不正侵入された場合に適切な処置ができること

〔ネットワーク実習第5段階〕
サーバー設置環境としてのみ機能するネットワーク（Lan-c）に、サーバー及びLANを設置する。

上記の第４段階で基本的な、ネットワークセキュリティー設置や管理の方法をトレーニングした上で、不正侵入されても、他に影響を与えない用に、設定、管理されたネットワーク上にサーバー

やLANを設置する。ここで扱うサーバーは、学生が、設置したサーバーが、何らかの不手際で、不正侵入されたとしても、他のネットワーク上のサーバーに悪い影響を与えないWWWサーバー等を実習の対象にする。
ネットワーク侵入された場合に起こりうる主な危険性は、

a．他のコンピュータに侵入する為の踏み台にされる
b．ネットワーク上に流れる情報を盗聴される
c．侵入されたコンピュータ上のデータを改竄される
d．侵入されたコンピュータの計算機資源を不正に利用される

等が挙げられるが、Lan-cの環境での実習を行うことによって、a. の危険性を回避することができる。但し、依然としてb.の危険性は存在するので、盗聴されて困るような情報は、このネットワーク上に流さないような注意が必要である。

この段階での、実習は、外部に公開するサーバーや、LANを設置し、数日間稼動して、放置した後に、学習者が設置したサーバーが、外部から侵入されて無いかどうかを確認する。セキュリティーの設定が不適切であれば、ほぼ、確実に侵入されることになる。

＜合格基準＞

・可能なセキュリティー対策を確実に行えること
・不正侵入を確実に検出できること
・不正侵入された場合に、確実にかつ迅速に適切な処置が取れること
・不正侵入を確実に阻止できること

〔ネットワーク実習第6段階〕

セキュリティー制限をまったく受けないネットワーク（Lan-d）上での、サーバーの公開及び、LANの構築

上記の実習第5段階までの実習を行った後で、最終段階の、セキュリティー制限を受けないネットワークでのLANや、サーバーの設置を行う。この段階で、侵入を受けなければ、ネットワークセキュリティー対策の基本は、ほぼ、身につけたことになる。

3．2．ネットワークセキュリティー教育用ネットワーク環境の構築例

上に述べたような、教育段階を実施するために構築したネットワーク環境を図3．2．に示す。このネットワークは、全て、同じ教室内に設置してあるものである。図でわかるように、まず、Lan-aは、ネットワークに接続しない完全に孤立したネットワークとして実現した、Lan-bは、2段のファイアーウォールを通じて、インターネットに接続しており、2段目のファイアーウォール2は、IPパケットフィルタリングと、IPマスカレードを利用したプライベートネットワークとして実現した。これによって、Lan-bに外部の者がネットワークを通じて侵入するのは非常に困難になる。このネットワーク内は、通常のコンピュータリテラシー教育にも利用するため、インターネット上に公開しない、各種のイントラネット用ファイルサーバーを複数設置してある。

Lan-cは、インターネット上にサーバーを公開することはできるが、ネットワーク外部のサーバーに対してクライアントとして接続できないような設定をファイアーウォール1で行う。また、このファイアーウォールでは、ファイアーウォール2に対するセキュリティー制限及び、ファイアーウォール1および、ファイアーウォール2の間に設置してある公開サーバー群のためのセキュリティー制限も同時に行っている。

Lan-dは、セキュリティー制限をまったく受けないネットワークである。通常のインターネット接続方法を行うだけで実現できる。

3．3．ネットワークセキュリティー教育を行う上での教官の役割

これまでの、活動を通じて、実用上十分な安全性をもったネットワークセキュリティー教育環境を整備できたと考えている。しかし、その安全性も永続的なものではなく、ひとたび、セキュリティーホール等が発見されると、たちまち、環境全体が脅威にさらされてしまう。従って、教官の役割としては、日々のセキュリティー情報[5),6),7)]の収

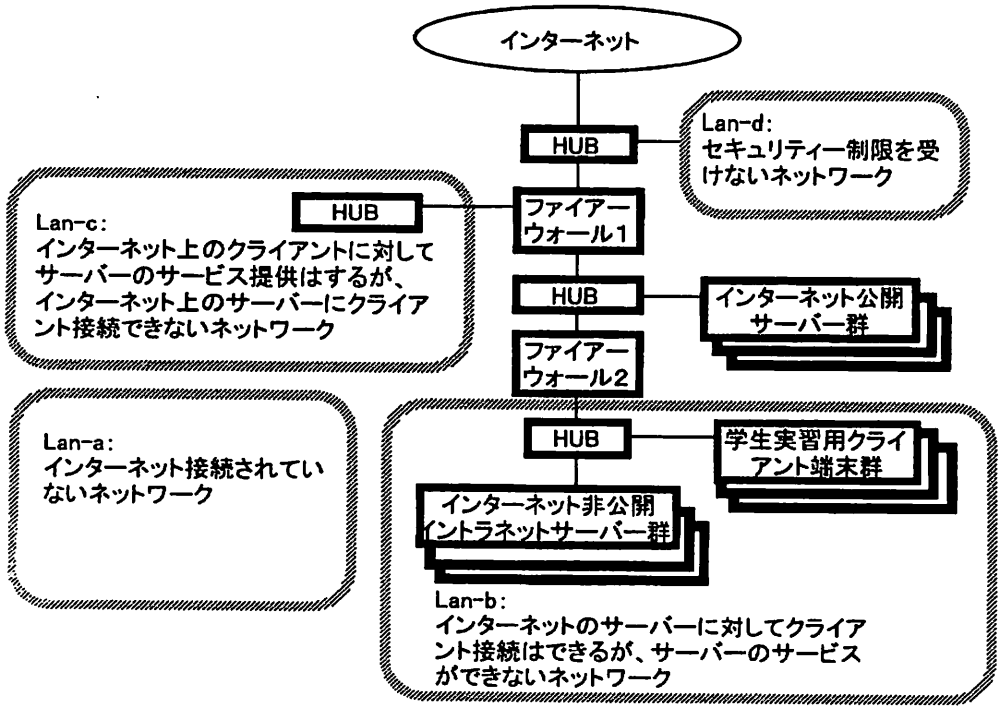

図3.2. ネットワークセキュリティー教育用に構築したコンピュータネットワーク環境

集と、ネットワーク環境構築に利用しているサーバー機器のメンテナンスを常に実施する必要がある。

学習途中の者が構築するサーバーや、ネットワークは、彼らのスキルの未熟さゆえに、常に悪用される危険性を持っているので、損害を外部に与えないように、実習の際には、十分な監視を怠らないようにすることが重要である。

4．ネットワークセキュリティー教育用ネットワーク環境を利用した実習の経過

本稿で示した、ネットワーク環境を構築する前は、コンピュータサーバーの設置の実習は、Lan-dのような、セキュリティー制限を行っていない環境で実習を行っていた、その環境では、学習者が設置したサーバーを、長期間稼動させたために、3台のコンピュータが外部から、ネットワーク侵入を受けて乗っ取られた。しかし、その後、図3．2．で示すようなネットワーク環境を構築して、Lan-aおよび、Lan-bで、実習を行うようになってからは、本稿執筆時点までの半年間一度も、外部から侵入されることはなくなった。現在、一日に2～3回のネットワークスキャンをネットワーク外部から受けつづけている。従って、現在のところ、実用上十分なセキュリティー強度を確保できていると考えられる。

なお、図に示した2つのファイアーウォールと、インターネットに公開しているサーバー群は、1週間に一回のセキュリティー検査を行いつづけている。

これまで、上で示した第3段階までの実習を行った。Lan-cのエリアを使った実習は、現在のところ、まだ、一度も行っていない。今後、実際に実習を行ってみて、その有用性や弱点を確認する予定である。

5．おわりに

本稿では、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ー教育環境の必要性と、そこでの実習の手順と合格の基準及びその環境の構築例を示した。
この環境は、まずネットワーク機器として
・ネットワークコンピュータ　4台
・ネットワークHUB　5台
で構成した。また、学生実習用の機器として
・ネットワークコンピュータ　5台、
・ネットワークHUB　4台
を整備した。

これまで、Lan-aとLan-bの環境と上で述べた実習機器を利用して、（上記第3段階の）安全にセキュリティー管理された環境での、基本的なサーバー、LANの構築の実習までを行った。その結果、ほぼ、安全に実習が行えることを確認できた.今後は、Lan-c、Lan-dの環境も利用して本題であるセキュリティーに関する実習を行うとともに、これまで、構築した環境の有用性や弱点を確認していく予定である。

この環境がセキュリティー的に危険な状況になるのを防ぐため、本稿では、ファイアーウォールのルール等の詳細の記述は行わなかった。しかしながら、本稿の内容を通じて、基本的な考え方と構築方法及び、授業での活用方法等は十分に理解できるものと考える。システムの詳細な設定方法等に関してはネットワークセキュリティー関連の文献[1),2),3),4)]等によって十分に推測できるものと考える。

謝　辞

緊急対策的にセキュリティー教育環境を整備するにあたって、サーバー用ハードディスク機器の提供と、OSの購入をしていただいた、中村功氏と2台のサーバー機器を購入する為に共通予算を使用することを了承していただいたコース主任の加藤満生氏に心より感謝いたします。

参考文献

1）山口英、鈴木裕信：“bit別冊　情報セキュリティ”、共立出版、2000.
2）Anonymous：“Linux版　クラッカー撃退完全ガイド”、インプレス、2000.
3）久米原栄：“Linux Network　ファイアウォール管理者ガイド”、ソフトバンク、2000.
4）久米原栄：“TCP/IPセキュリティ”、ソフトバンク、2000.
5）http：//www.jpcert.or.jp/
6）http：//itpro.nikkeibp.co.jp/members/security/
7）http：//www.zdnet.co.jp/news/virusinfo/index.html