平成12年度　第3回情報ネットワーク担当職員研修
－ネットワーク管理Ⅱ－

センター系（情報メディア教育センター）　佐藤　之紀

1．研修期間・場所

期　間　2000年12月4日（月）～7日（木）

場　所　国立情報学研究所（1日目）

東芝OAコンサルタント（2日目～4日目）

2．研修目的

大学等において、ネットワーク管理業務に従事している職員で、ネットワークに関する基本的な知識を有する者を対象に、ネットワーク管理業務に係わる最新かつ専門的な知識と技術を修得する。

3．研修内容

ネットワーク管理の概説、WWWサービス環境の構築、Proxyサーバの設定、ルータの設定、ファイアウォールの構築、TCPWrapperの実装について、国立情報学研究所と東芝OAコンサルタントの講師による講義と実習を行った。

3．1 ネットワーク管理概説

国立情報学研究所で実際にネットワークを管理している方から、インターネットの接続管理およびLAN（Local Area Network）管理の概要と、その障害対応の実例が紹介された。実際の障害を仮定した対応法が演習の形で紹介されたため、具体的かつ実践的な方策が介された。

また、キュリティに関する研修では、SINET（Science Information Network：学術情報ネットワーク）の加入機関で実際に起きたDoS（Denial of Service）攻撃について、その対処法が紹介された。

3．2 WWWサービス環境構築

WWW(World Wide Web)とは、ハイパーテキストを基本構造とする広域情報提供システムであり、その情報を提供するホストをWWWサーバと言う。そしてWWWサーバに要求を出し、その後提供された情報を表示するWWWクライアント側のソフトウェアをWWWブラウザと言う。本研修では、WWWサーバの仕組み、インストール方法、環境設定について研修した。

3．3 Proxyサーバ設定

自サイトのネットワーク上の資源を保護するために、またキャッシュ機能を使い同じURLへの検索を減らしネットワーク負荷を軽減させるために、このProxyサーバを設定する。

本研修ではフリーソフトウェアである「Squid2.2」を使用して研修を行った。その手順は、まずソースをインターネット上のAnonymousFTPサーバから入手するが、実際に外部へ接続して入手すると、ダウンロードに余計な時間を費やし、またネットワークに余計な負荷をかけてしまうため、講師が事前に用意したソースを使用した。入手したソースはGNUのgcc.2.7.2.1でコンパイルし、GNUのgunzipコマンドにより解凍、その後configureにより環境構築しインストール(makeおよびmake install)した。

インストール完了の後、実際にSquidを起動し、実際に設定を行った。

3．4 ルータ設定

インターネットの通信において、ネットワーク層の役割は、目的のホストまでインターネット上の最適な経路を選択することである。ルータはパケットを受け取った時に、ルーティングテーブルの経路情報にもとづいて目的のホストまでの経路を選択し、パケットを転送する。

ルーティングテーブルを作成するための手段は大きく二つに分かれており、一つは「スタティックルーティング」といい、管理者が手動でルータ情報を設定する方法である。この利点としては、管理者があらかじめ経路を予測できる、またルータやネットワークに負荷がかからない等がある。しかし、ネットワークが大規模になると経路の選択が複雑になり、また構成の変化に対してその都度管理者が更新作業を行う手間がかかる欠点がある。

もう一つの方法は「ダイナミックルーティング」といい、ルーティングプロトコルにもとづいたプログラムがデータの作成、追加、変更を自動で行う方法である。管理者はプログラムを起動するだけであり、経路を自動で選択するので人的負担が少ない。また大規模ネットワークにも対応でき、ネットワーク障害が起こっても自動で迂回ルートを選択できる利点がある。この方法の欠点としては、実装したプロトコルのルールのもとづいた経路しか選択できない（応用性に乏しい）、ルータ同士がルーティングに関する情報交換をするためネットワークやルータに負荷がかかるなどがある。

そこで、ひとつのネットワーク環境において、スタティックルーティングとダイナミックルーティングの両方を使用する「ハイブリッドルーティング」という方法がある。ハイブリッドルーティングを使用する場合の例は次のような場合である。

- ネットワークの末端部でスタティックルーティングを使用し、他の部分でダイナミックルーティングを使用する。
- 各部門の高速LANでダイナミックルーティングを使用し、部門間を接続するWANでのみスタティックルーティングを使用する。

本研修ではCisco社製のルータを用い、その構成、起動法、操作法、各種設定法につい

て研修した。しかし、ルータは１台のみだったため、個別に実習することはできなかった。

３．５ ファイアウォール構築

ネットワークのセキュリティを確保するために、まず個々のホストのセキュリティを考えた場合、アカウント及びパスワードの管理、アクセス権の管理、セキュリティホール対策などがあるが、それだけで組織内の全てのホストのセキュリティを均一に高レベルに設定することは困難である。そこで、インターネットから組織内への入り口を一つに絞り、その一箇所に集中して高セキュリティを設定することが考えられる。この環境のことをファイアウォール(Fire Wall：防火壁)と言い、外部からのアクセスに対して強固なセキュリティを構築できる。しかし、部内者からの攻撃、迂回経路からの攻撃には防御できず、単体ではウィルスに対する防御もできない点に注意を要する。

本研修では Solstice FireWall-1 を使って、実際にファイアウォールを構築し、動作テストを行った。

３．６ TCPWrapper 実装

セキュアなネットワーク構築のために、一般的にファイアウォールを構築することにより、ファイアウォールの内側の安全はある程度保証される。しかし、ファイアウォールの外側はまだ危険にさらされたままにある。WWW サーバ、FTP サーバなど外部からの接続が無ければ意味を為さないサーバについては、DMZ(De-Militarized Zone：非武装地帯)に配置しなくてはならない。なお、この DMZ はファイアウォールの外側にある。

これらのサーバの中で常駐プロセスとなっているデーモンは、一般的にサーバプログラム数が多いので要求頻度の低いサービスについては inetd というデーモンが受け付け、inetd から各デーモンを起動する設定になっている。そこで、inetd と各デーモンの間にプログラムを介在させ、アクセスの限定を行うことにより、これら DMZ にあるサーバについての安全を保つのである。この機能を実現する代表的なプログラムが「TCPWrapper」である。TCPWrapper をインストールすることで、特定のホストからの特定の要求に対してのみ、inetd 経由でデーモンを起動することができる。

本研修では実際に TCPWrapper をソースから解凍しインストールを行い、設定後実際にテストを行った。これについてはこれまでに何度か他の研修にて実習を行っており、また業務においても行っているので、私的には復習となった。

４．所感

本研修は、初日のネットワーク管理の講義に始まり、Proxy サーバ、WWW サーバ、ルータ、ファイアウォール、TCPWrapper と、全てに安全対策の方法が盛り込まれていたので、セキュア・ネットワークの重要性の意識が高まった。そして行った実習は、その際の資料と共に業務に直接役立つものであった。