外部接続用インターネットサーバの構築

佐藤　悦教*・大西　孝臣**・松尾　征夫***

Constructing the Internet server for external connections

Yoshinori SATO, Takaomi OHNISHI and Yukio MATSUO

要　旨

これまでの苫小牧高専校内LANシステムにおけるインターネット接続は、1台のインターネットサーバによって行ってきた。しかし、インターネットの爆発的な普及により、既存のインターネットサーバのみではトラフィックを十分に処理仕切れない状態となった。そこで我々は、セキュリティを十分に考慮したインターネットサーバを新しく構築し、2重化を実現することを通じて、負荷の分散処理を行った。これにより高速化、高信頼性化、高安定化を図ることが可能になった。

Abstract

The campus LAN (Local Area Network) system of Tomakomai National College of Technology owed external connections to an Internet server. But it did not deal with the heavy communication traffic because of access increase in proportion to the Internet boom. To cope with this statue, we employed and constructed another Internet server so as to implement the load distribution by means of the dual connections. This leads to reliability and stability of the network system at high speed.

1．緒　　言

1996年（平成8年）3月にATM(Asynchronous Transfer Mode)を幹線とした、苫小牧高専校内LANシステム（以下、校内LANと略記）を導入し運用を行ってきた。本システム導入当初より、教職員、学生に対して有効利用を促した結果、教育、研究等の業務で欠かせないものとなっている。

しかし、年月が経過するにつれて、教職員、学生の利用率の上昇に伴い、各サーバの負荷やネットワークトラフィックも爆発的に増大してきている。特に外部ネットワークと接続することが可能な唯一のサーバであるインターネットサーバは、学内全体からのリクエストによる負荷の増大に対応出来ず、処理の遅延が発生するといった過負荷状態が続いている。結果、本サーバは、ネットワークの利用効率を妨げるボトルネックとなっている。また、本サーバは冗長性を持つ構成をしていないため、障害発生時や保守時における外部ネットワークとの接続が不可能となり、教育、研究等の業務において大きく支障をきたしている。

そこで我々は、この既存のサーバのボトルネックを解消するために、新規のサーバの導入を通じて、既存のサーバとの間において各アプリケーションが行う処理の分散化を図ることを考えた。また、既存のサーバにおいて、障害が発生した際においてもネットワークが正常に運用できるよう、既存のサーバが提供している全てのアプリケーションについて、新規のサーバがバックアップとして動作する対応が取れるような構成を考えた。

導入するインターネットサーバは、内部と外部との接続を受け持ち、校内の全ユーザは新規のサーバに搭載されている様々なアプリケーションを利用することを考慮し、我々は、以下の点を特に重視して、新規のサーバの導入、構築を行った。

(i) セキュリティ
(ii) フェイルセーフ
(iii) フェイルオーバ

＊ 技　官　情報処理センター
＊＊ 助　手　情報工学科
＊＊＊ 教　授　機械工学科

2．ネットワークの構成

2-1　既存のネットワーク構成

既存のネットワーク構成においては、唯一であるインターネットサーバを通じて、外部ネットワークとの接続を行っている。既存の構成は、図1の通りである。

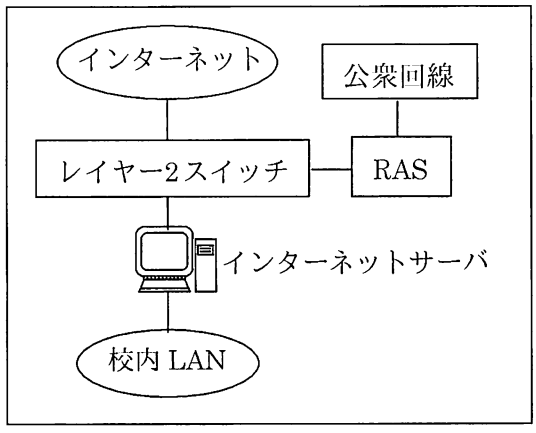

図1　既存のネットワーク構成

2-2　新規のネットワーク構成

既存のネットワーク構成においては、図1の通り冗長性が無く、耐障害性が低いことがわかる。そこで、新規に導入するサーバと既存のサーバを用いて、冗長性を有することが可能となるよう構成し、ネットワークの耐障害性を高める。構成としては、図2の通りである。

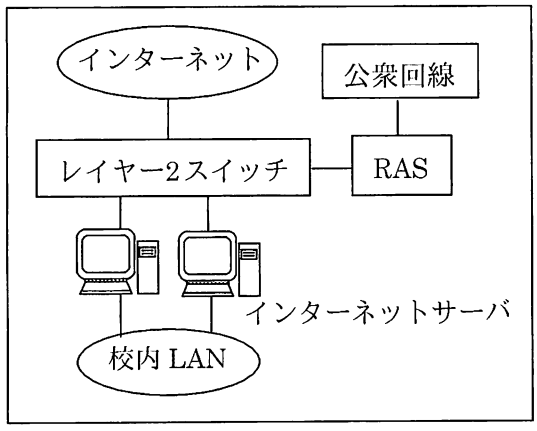

図2　新規のネットワーク構成

3．ハードウェア

新しくインターネットサーバを導入するにあたり、信頼性、耐障害性を考慮し、以下に示すハードウェアを導入した。

3-1　中央処理装置

校内全体で利用するため、できる限り高速なCPUを採用し、ディスクスワップによるアクセスの低下を避けるため、以下の中央処理装置及び物理メモリを導入した。

(1) CPU
　PentiumⅢ Xeon 1GHz×2
　マルチプロセッサ
(2) キャッシュ
　32Kbyte/256Kbyte（1CPU）
(3) メインメモリ
　133MHz 4Gbyte ECC SDRAM

3-2　磁気ディスク装置

高速であることは勿論のこと、ディスク装置単体での信頼性、冗長性を向上させるため、以下の機器を導入した。

(1) ハードディスクドライブ
　10Krpm　実効144Gbyte以上
(2) ディスク構成
　RAID5、ホットスタンバイが可能
(3) ディスクコントローラ
　Ultra3(Ultra 160)SCSIコントローラ

3-3　補助記憶装置

インストールやバックアップ等の様々な事例で補助記憶装置は利用される。特に利用する機器として、以下の機器を導入した。

(1) FDD
　3.5inch1.44Mbyteディスクドライブ
(2) CD-ROM
　40倍速CD-ROM
(3) DLT
　非圧縮時40Gbyteのデータ容量

3-4　その他の装置

その他、ネットワークの管理、運用上必要な機器を以下の通り導入した。

(1) ネットワークコントローラ
　10/100Base-TX自動認識
(2) グラフィックスコントローラ
　65,000色時の最大解像度1,600×1,200
　VRAM SGRAM 4M

(3) ディスプレイ装置
21inchカラーフラットディスプレイトリニトロン
(4) 電源ユニット
冗長構成をもつ。
(5) 無停電電源装置
・ サーバの最大消費電力以上の電源容量
・ 最大5分間以上の電源供給
・ 停電による、シャットダウン制御

4. ソフトウェア

4-1 利用するソフトウェア

ソフトウェアは、既存のインターネットサーバで利用されているアプリケーション相当以上のものと既存のサーバ以上のセキュリティを持つことが必要である。導入したサーバでは次表に示すアプリケーションを用いて、構築を行った。

表1 アプリケーション

項　目	ソフトウェア
カーネル	2.4.2-2smp
ファイアウォール	FWTK-2.1
電子メール	Sendmail-8.9.3
ネームサービス	bind-8.2.4
WWWサーバ	apache-1.3.20
プロキシサーバ	squid-2.4
電源管理ソフトウェア	Power Chute Plus-4.5.3
ログ解析	Analog-5.0
sendmail.cf	CF-3.7
Perl	Perl-5.6.0
Ssh	Open ssh-2.5.2
NTP	ntpd-4.0.99
MRTG	Mrtg-2.9.7

これらのソフトウェアを利用し、新規のサーバの構築を行った。以降ではこれらのソフトウェアについて、セキュリティに関する部分について簡単に解説するが、本校のセキュリティ情報に大きく関る部分については、本稿における掲載を差し控える。

4-2 OS（カーネル）

利用するOSとして、以下の事項に対応していることが必須であった。

1）BSD由来のUNIXまたはSYSVR4由来のUNIX OSであること。
2）X-Window相当のWindowシステムが使用可能であること。
3）shadowパスワードが利用できること。
4）xinetd相当のデーモン制御プログラムを持ち、各々のアプリケーションについてアクセス制限を付加することが可能であること。
5）パケットフィルタリングソフトウェアが利用可能であること。
6）大容量のメモリに対応していること。
7）ソフトウェアの信頼性が高いこと。
8）セキュリティに関するバグフィックス等が頻繁に行われること。
9）前述したハードウェアが全て問題なく動作すること。

以上の条件を満たすOSとして、普及が目覚しく、アプリケーションの開発やバグフィックス等も頻繁に行われているRed Hat LINUX7.1J（カーネル：2.4.2-2smp）を新規のサーバにおいて採用した。Red Hat LINUX7.1Jを採用することにより、従来ソフトウェアをインストール際に使用していたmakeやconfigureを利用せずに、rpmパッケージを利用することで、様々なアプリケーションのバージョン管理が容易となる。

構築したインターネットサーバは、外部接続で使用されるため、特にセキュリティに対して注意する必要があるが、デーモン制御プログラムとしてxinetdを採用することにより、従来のデーモン制御プログラムであるinetdとinetdのアクセス制御を行うTCP Wrappersを組み合わせた構成に比べ、より細かなアクセス制限を設けることが可能なうえ、各サービスの動作状況について、細かなログを記録することができ、従来以上のセキュリティを確保することが可能となる。

今回の構築では、xinetdを利用して運用上必要なサービスのみをユーザからのリクエストに応じて起動し、IPアドレスを用いたアクセス制限を行っている。リクエストが想定されるIPアドレスの種別は以下の表2があげられる。

表2 アドレスの種類

種　別	クラス	サブネットマスク
グローバルアドレス	Cクラス(学内)	255.255.255.0
グローバルアドレス	全てのクラス	255.255.255.255
プライベートアドレス	Bクラス(学内)	255.255.0.0

xinetdでは、サービスの利用を許可するIPアドレスについて、クラス単位、サブネット単位、IP

アドレス単位でアクセス制限を行っている。
ユーザが利用可能なサービスについても、アプリケーション単体でIPアドレスを用いたアクセス制限を設けるとともに、DNSと連動させ表3に示すドメイン名やホスト名を用いてアクセス制限を設けることで、更にセキュリティを向上させることが可能である。

表3　ドメインの種類

ドメイン名	DNSサーバ	クラス
tomakomai-ct.ac.jp	学内のDNS	Cクラス
*.tomakomai-ct.ac.jp	学科ごとのDNS	Bクラス
*	学外のDNS	全てのクラス
単一のホスト	学科ごとのDNS	Bクラス

更に、アプリケーションゲートウェイで起動できるアプリケーションについてもxinetdと連携させ、2重のアクセス制限を設けることにより、強固なセキュリティを持つことが可能である。

4-3　基本サービスソフトウェア

既存のサーバでエンドユーザに対して行っている基本的なサービスである電子メール、DNS、WWW、HTTP等のサービスを従来どおり提供することを可能とした上で各サービスの負荷分散を新規のサーバとの間において行った。また、既存のサーバに障害が発生した際も、ネットワークの運用が継続して行われるように一部のサービスを既存のサーバのslaveとして動作するよう構築を行っている。

各サービスについて、セキュリティの観点から以下の点に特に注意して構築を行った。

(1) 電子メール（SMTP）
　電子メールを利用する上で必要なSMTPを利用したrelayメールやメール爆弾等の外部からの不正利用からシステムを保護するため、セキュリティを重視したsendmail.cfの作成。

(2) DNS
　DoSを防ぐために、zone転送を行うホストのアクセス制限。

(3) WWW
　CGIプログラムを用いた不正アクセスやDoSからホストを保護するためにIPアドレスを用いたアクセス制限、厳密なアクセス権の設定およびプロセス数の制限。

(4) HTTP
　HTTPサーバへの接続を許可していないホストのアクセス制限。IPアドレスを不正使用しているホストからのアクセスを制するためにFQDN（Fully Qualified Domain Name）を用いたアクセス制限。

これらのサービスの内、SMTP、DNS、WWWは学内のユーザのみならず、学外の不特定多数のユーザが利用することになるため、サービスを提供する際のセキュリティについて特に注意しなければならない。

また、これらのサービスに関するログを全て記録することで、障害時に備えるとともに、利用度を算出するため、各アプリケーションのログを利用し、analog等の統計プログラムを用いて統計情報を得られるよう設定を行っている。

4-4　パケットフィルタリング

ネットワーク内部のホストからのアクセスに対しては、ネットワーク外部からのアクセスに比べて低いセキュリティにより、実現されている。このため、ネットワーク外部のユーザがネットワーク内部からのアクセスと見せかける不正アクセス（IP Spoofing）が行われる可能性がある。IP Spoofingからシステムを保護するために、ネットワークインタフェースに流れるパケットの情報についてのポリシーを設定することにより、高度なセキュリティを実現している。

ポリシーの基本的な作成については以下の手順で行った。

(1) 全てのパケットの通過を不許可にする。
(2) 必要なパケットの通過のみ許可する。
　このようにポリシーの概念そのものは非常に簡単なものとなる。
　今回、構築したサーバではipchainsを用いてパケットフィルタリングの設定を次のように行った。
(1) 全てのパケットを遮断。
(2) 始点アドレスが本校のDNSが管理しているIPアドレスである場合のみパケットのフォワーディングを許可する。
(3) 外部インタフェースに入ってくるパケットの内、始点アドレスがプライベートアドレスであった場合、パケットを破棄する。
(4) ICMPはエラーメッセージを送信する際利用するため、エラーに関するICMPのパケットを許可する。

4-5 アプリケーションゲートウェイ

既存のサーバでの外部へのTELNETやFTPを用いた接続はアプリケーションゲートウェイにより実現し、利用されている。今回、構築したサーバも同様にアプリケーションゲートウェイを必要とするためフリーウェアのファイアウォールであるFWTKを用いて構築を行った。

FWTKで起動可能なアプリケーションゲートウェイにはrlogin、finger、smap等様々なアプリケーションがあるが、本校で現在必要とされているアプリケーションゲートウェイのアプリケーションはTELNET、FTPの2種類である。この2種類について、一般ユーザが利用できるアプリケーションゲートウェイを構築した。

本校で利用していないアプリケーションは全て利用できないよう設定を行い、利用するアプリケーションのTELNET、FTPについては以下のように設定を行った。

(1) アプリケーションゲートウェイの利用が必要なホストについて許可する。
(2) 全てのホストについてアプリケーションゲートウェイの利用を不許可とする。

先程のパケットフィルタリングと全く逆のポリシーの概念で設定することとなる。パケットフィルタリングでは、設定ファイル内で後述された設定が有効になるのに対して、アプリケーションゲートウェイでは設定ファイル内で前述した設定が有効となるためこのようなポリシーの概念で設定することとなった。

また、アプリケーションゲートウェイのセキュリティをより高めるためにアプリケーション毎にパスワードを設定することも可能であるが、今回の構築ではアプリケーションゲートウェイにパスワードを設定することはユーザの利便性を大きく損なう点と既存のサーバでもパスワードを設定しなくともセキュリティに関る大きな問題が起こっていないことから、ホストによるアクセス制限により、アプリケーションゲートウェイの構築を行っている。

5 結　言

既存のサーバと同等の利便性、アプリケーションを持ち、外部に対してより強固なセキュリティを持つインターネットサーバの構築をおこなった。新規のインターネットサーバは、校内LANの核となり、最もセキュリティが求められる部分であるため、OS及びアプリケーションそれぞれが堅牢なセキュリティをもち、ユーザの利便性を損なわないことが必要であった。しかし、ユーザの利便性とセキュリティという、求められる2つの性質の双方を同時に確保することは困難であり、ユーザが利便性を損なう点とセキュリティを高めることの線引きが重要課題であった。この点については、今後策定する本校のセキュリティポリシーにも大きく関る部分であり、ネットワークを運用する上で特に重要な点となるため、学校全体でこれらに取り組む必要がある。

セキュリティを単独で考えた場合でも、未知の不正アクセスが行われることが考えられ、OSや各アプリケーションのバグなどについて特に注意しなければならない。

今後は各アプリケーションのバグや不正アクセスに注意するとともに、最近被害が大きく増加しているコンピュータウィルスへの対策を取り入れたシステム構成について考慮することが必要である。

参考文献

1) Eleen Frisch著,榊正憲訳,Essential System Administration,アスキー出版局,1996
2) Hal Stern著,倉骨彰,砂原秀樹訳,Managing NFS and NIS,アスキー出版局,1995
3) Bryan Costales,Eric Allman著,中村素典,鈴木克彦訳,sendmailシステム管理,O'REILLY JAPAN,1997
4) Bryan Costales,Eric Allman著,中村素典訳 sendmailデスクトップリファレンス, O'REILLY JAPAN, 1997
5) 高町健一郎著,UNIXネットワークセキュリティ導入・運用ガイド,秀和システム,2001
6) Digital,Digital UNIXオペレーティングシステムシステム管理ガイド,1997
7) Digital,Digital UNIXオペレーティングシステムネットワーク管理ガイド,1997

(平成13年11月30日受理)