システム情報科学研究院情報理学部門の計算機管理とセキュリティ対策

石野, 明

森, 雅生

https://doi.org/10.15017/1470679

出版情報：九州大学情報基盤センター広報 : 学内共同利用版. 4 (3), pp.139-145, 2004-12. 九州大学情報基盤センター
バージョン：
権利関係：

システム情報科学研究院情報理学部門の計算機管理とセキュリティ対策

石野 明　　森 雅生

1 はじめに

情報理学部門では計算機の利用が研究と直接結び付いており，多数の計算機を部門内に有しています．しかし，個々の研究室単位でのサーバ計算機の管理は行わず，専攻全体の共通サーバを設け管理の対象を集約することで管理の手間を簡約化しています．一つのLANに複数の管理者がいることが望ましいですが，当部門で仕事を完全に分担していません．理由は，各サービスのトラブルにいつでも対応できるようにするためです．情報理学部門は筑紫地区と箱崎地区に分かれており，現在，箱崎地区のネットワークにすべてのサービスを集中させて管理しています．主な管理者は4人おりますが，仕事は分担するのでなく，できる限り全員同じ仕事ができるような体制をとっています．また，管理の範囲ですが，規模としては一つのネットワークセグメントにつき一つの管理グループを割り当てるのがちょうどよいと思われます．研究室単位で行っている部署もあるようですが，これくらい規模で以下に述べるネットワークサービスのみを行い，個々に研究などで必要なサービスは研究室単位で行うなどきっちりとした分担をしておいた方がよいと思われます．次の節から共通サーバの管理とセキュリティ対策について，また，用いられているツールの紹介などを行います．

2 共通サーバ群とネットワーク

情報理学部門箱崎地区のネットワーク構成の概略を図1に示します．情報基盤センターからの1Gbpsのラインを，まずL3スイッチを用いてルーティングおよびフィルタリングしています．ネットワークは大きくワークステーション群と一般PC群に分けられ，ワークステーションを用いた大規模な実験と，一般PCによる作業が互いに干渉しないようになっています．また，対外向けのサービスを提供している2台のワークステーションをL3スイッチに直接接続しています．

九州大学情報基盤センター広報
Vol. 4 No. 3 2004

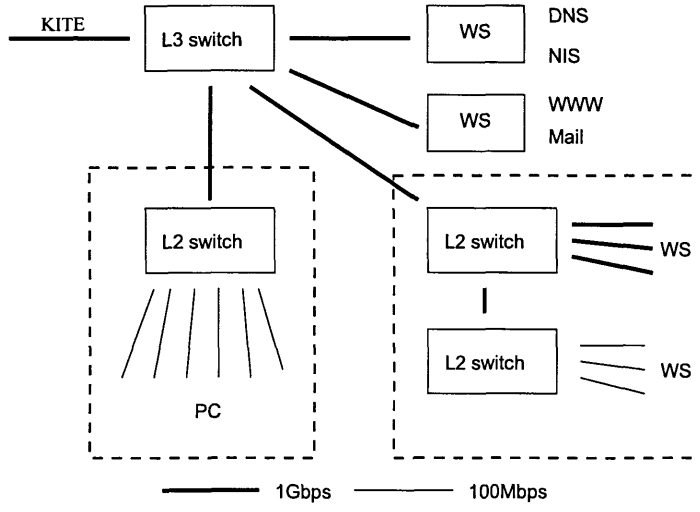

図 1: 情報理学部門のネットワーク構成

3　センタースイッチ

図 1 において，L3 switch と記述されている部門の出入口となっている L3 スイッチによって，ルーティングとパケットフィルタリングを行っています．L3 スイッチによるルーティングとパケットフィルタリングは非常に高速であり，過負荷によるトラブルは現在のところ発生していません．当部門ではパケットフィルタリングの設定として，「内部からのアクセスか，外部からのアクセスかに関わらず，必要のないポートはすべて閉じる」という厳しいポリシーを採用しています．これは，多くのファイアーウォールで採用されている「内部からのアクセスは許可する」というポリシーでは，トロイの木馬型のウィルスや，予期しない P2P サーバの稼働などを防ぐことができないためです．具体的には，外部から内部に関しては，登録されたサーバへの特定のポートに対するアクセス (DNS, WWW, Mail, ftp, ssh など) のみを許可しています．内部から外部に対しても同じく，よく知られたサービス (WWW, Mail, ftp, ssh) のみを許可しています．

このような厳しいポリシーを採用した結果，外部からの侵入はもちろん，Blaster や Welchia などのウィルスにネットワークを通じて感染するという被害も受けていません．Welchia に関しては，出張中に外部のネットワークに接続し感染した PC が持ち込まれたことがありましたが，上記のパケットフィルターの設定により部門外への感染拡大が起きることはなく，また各 PC にインストールされていたファイアーウォールソフトの働きにより，1 台も感染することなく駆除されています．

最近のアプリケーションは通信には HTTP を使用するなどファイアーウォー

ルが設置されていることを考慮したものが多く，上記のような厳しい設定でも問題なく使用できるものが多いです．しかし，FTP では passive モードで通信しないと使用できないという問題が発生しています．これに関しては FTP proxy を用意するといった対策が必要であると考えています．

4 ネームサービス

LAN で一番最初に行うべきサービスはネームサービス (DNS) でしょう．いわゆるドメイン名とサーバの名前に対応する IP アドレス情報をサービスする仕事です．このサービスは LAN の外側と内側でやり方が異なることがあります．LAN の外側からのホスト名の問い合わせに関しては bind をはじめとする DNS サーバを，内側から LAN 内のホスト名の問い合わせに対しては NIS サーバを使うなどです．以下にその違いを表にまとめてみました．

	問い合わせ元	問い合わせるホストの位置	サービス
1.	LAN の外側	LAN の外側	※通常はサービスしない
2.	LAN の外側	LAN の内側	BIND, tinydns(djbdns)
3.	LAN の内側	LAN の外側	BIND, dnscashe(djbdns)
4.	LAN の内側	LAN の内側	NIS, NISPLUS

bind は非常に多く普及している DNS サーバですが，セキュリティバグなどが頻繁に発見されるのと運用時に問題点があるため，情報理学では **djbdns** を使っています．この場合，上の表の 2 と 3 の仕事には別のサーバ (異なる IP アドレス) を割り振ることになります．詳しくは djbdns のサイト[1]をご覧ください．NIS および NISPLUS は Sun Microsystems の製品ですが，ワークステーションの利用が少なくなりつつある今，需要は減っています．NIS と NISPLUS の利点は個人ユーザのアカウント情報の利用が考えられますが，これもクライアントソフトのサポート状況から見て LDAP などに移行するほうがよいでしょう．

5 WWW サーバ

WWW サーバとしては Apache [2]を用いています．部門のホームページのみならず，スタッフや学生は自由にホームページを設置することができますが，CGI に関しては管理グループに申請をしてもらうことにしています．

[1] http://dns.qmail.jp/
[2] http://httpd.apache.org/

6　メールサーバ

近年の電子メールの普及状況を鑑みると，メールサーバの設置運営は大変重要なものとなっています．常に駆動していなければならないサーバとしてはウェブサーバよりもリアルタイム性と重要性は高いと考えられます．よって，サーバの設置・ソフトの選択には細心の注意を払う必要があります．情報理学部門ではメールサーバの基本ソフトウエア (MTA) として **qmail** を使っています．このソフトウエアの利点としての特徴を以下にあげておきます．

1. 堅牢で役割ごとに細かいコマンドが用意されていること．メールサーバ内の各ユーザへのメール配送や SMTP 接続によるサーバ間メール配信などは，すべて個別のコマンドによって駆動されます．これにより個々の作業のチェックが容易に行えて，サーバ管理が簡潔になります．**sendmail** のように一つのデーモンプロセスがいろいろな機能を持つようになっていると，一部の機能に不備が出た場合，プロセス自体が停止してしまいすべての機能が動かなくなってしまうのと対照的で，qmail の堅牢性はここにあるといえます．

2. 各ユーザのメールボックスは一つのメールにつき一つのファイルで保存され，ファイル名はメールが配信されたタイムスタンプで管理されること．これを **Maildir** 形式とよび，すべてのメールを一つのファイルで保存するよりも安全です．

3. エイリアス (代理メールアドレス) の管理が容易であること (**dot-qmail**)．エイリアスデータを保存しているファイル名がメールアドレスとなり，一つのエイリアスにつき一つのファイルを管理すれば良く，sendmail のような `/etc/aliases` のファイルに一括して管理する必要はありません．たとえば，学生の学年ごとのエイリアスは年度更新時にファイル名を変えるだけでよいなど管理が楽です．

4. メーリングリストが個人で運用でき，また多機能なメーリングリストのソフトウエア (**ezmlm**) との連係が容易なこと．

ユーザからみたメールサーバの役割を大別すると，　個人へのメール配送 (POP,IMAP) と　メールの配信 (SMTP) となります．

POP, IMAP メールサーバのディスク領域が潤沢にある場合とクライアントのメールリーダソフトがサポートしている場合は IMAP をお薦めします．IMAP であれば異なるクライアント (異なるパソコン端末) でメールをダウンロードしたときに重複してメールを読むことにならないからです．ユーザのメール履歴はすべてサーバに保存され，メールの内容自体も実際に読むときにダウンロードされるなど大変重宝します．情報理学部門では **courier-imap** を使っています．POP を使わなくてはなら

ない場合は，暗号化したパスワードを交換する APOP を利用するようにしましょう．先に紹介した courier-imap には IMAP のほかに POP および APOP がサポートされています．また qmail にも POP サーバが用意されていますが，パスワードの暗号化などは一工夫必要になります．

SMTP メールの配送を行うには不正中継されないように工夫する必要があります．qmail に付属する qmail-smtpd では中継されないようにする設定が簡単に行えます．注意するべきは LAN の外側から外側への中継を悪用されないようにすることです．しかし LAN の内側からの中継は，メールクライアント (MUA) がメールを送信する際に利用するので初期設定で認証なしに中継するという設定でもよいですが，最近のメールウィルスなどの傾向を見るとすべての中継に認証を行うようにすることが必要でしょう．基本的に SMTP サーバは認証をせずに中継しますが，**POP before SMTP** や **IMAP before SMTP** などの機能を使って SMTP に鍵をかけることができます．これらはメールクライアントが一度メールをダウンロードするときの認証を利用して一定時間内にそのクライアントの IP アドレスからの SMTP 接続を許可するものです．具体的には，qmail-smtpd と courier-imap を **relay-ctrl** というソフトを使って連係させることができます．

7 迷惑メール撃退

迷惑メールが急増しています．perl で駆動する **SpamAssassin**[3] というソフトウェアを使えば，各ユーザのアカウントに配送されたメールを迷惑メールかどうか判断して，そうであれば破棄してくれます．しかしながら，これを利用していてもかなりの迷惑メールが届いていることも事実です．有償ですが，迷惑メール撃退を請け負う業者もいます．これは，SpamAssassin と同じようなソフトで判断するためのデータベースを購入するものです．当部門ではこれは試したことがないのでどれくらいの成果が出るかは分かりません．

8 FTP サーバ

FTP サーバとして，設定が容易にできるのが特徴である ProFTPD [4] を使用しています．また，このサーバで提供されている FTP は対外向けのものであり，一般ユーザーのホームディレクトリーにはアクセスできないようになっています．

[3] http://spamassasin.apache.org
[4] http://www.proftpd.org/

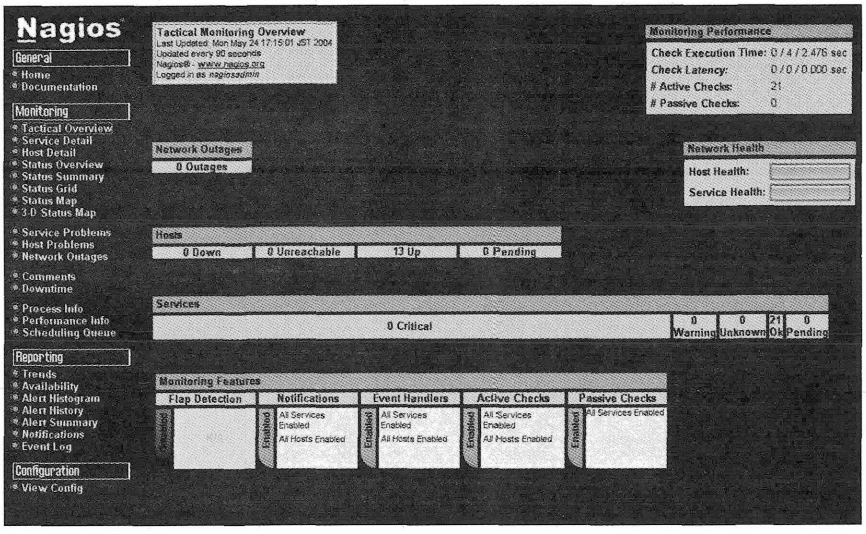

図 2: Nagios

9　そのほか

以上のサーバは対外向けのものであり，管理グループしかログインできないようになっていますが，スタッフと学生が自由に使用できるサーバも別に用意されています．また，対外向けサーバが Solaris であったのに対して，内部向けサーバは Debian GNU/Linux を用いており，使用したいソフトウェアのリクエストなどに柔軟に応えることができています．このサーバ上では内部向け WWW, FTP, ssh, CVS などのサービスが稼働しています．また，このサーバ上ではサーバ群の稼働状況を Nagios [5]を用いて監視しており（図 2），サーバに問題が発生したときは管理グループへとメールが届くようになっています．

10　おわりに

システム情報科学研究院情報理学部門の計算機とネットワークの概要とその管理について説明しました．最後に，機器の購入と選定について述べておきます．ネットワークはガス・水道・電気と同様，大学のライフラインとなっています．機器の選定は慎重に先を見据えた判断を行うことをお薦めします．また，主幹ネットワーク機器は高価なので購入するタイミングなども考慮しなければなりません．当部門ではシステム情報で一括して教育用システムを 5 年間のレンタルするというちょうどよい予算がありました．このときに研究

[5] http://www.nagios.org/

室単位での機器購入要望は遠慮していただき，予算の部門分配分の使い道について部門全体で「必要」なネットワーク機器をレンタルすることを許可していただきました．共用する機器なので，その点を強調すると協力を得やすいでしょう．また，予算の規模が大きいと入札ということになりますが，このときに作成する仕様書についても十分な注意が必要です．たとえば，L3 スイッチなどはネットワークインターフェースを 2 つ以上持つ DOS/V パソコンに Linux などをインストールしファイアーウォールのソフトを入れれば同じ機能を持つ機器を作ることができます．転送速度など詳細な調査を行い，しっかりとした製品で落札させるとよいでしょう．