ISSN 1346-650X

九州大学 情報基盤センター

広報

学内共同利用版
2003年 Vol. 3 No. 1

目次

特　集

ネットワークアウトソーシング事例の紹介 …… 池田大輔　1

メールサーバのアウトソーシング事例
－大学院言語文化研究院の場合－ …… 鈴木敦典　3

セキュリティ対策のアウトソーシング事例 …… 北祐一郎　8

附属図書館におけるコンピュータ関連の
アウトソーシングの実際 …… 小川　稔　14

システム情報科学研究院情報工学部門における
支線LAN管理作業について …… 乃村能成　17

解　説

キャンパス間接続のギガビット化および対外接続の
高速化について ……岡村耕二　24

九州大学の学内LANにおけるウェブサーバの分布と
傾向について …… 笠原義晃　27

報　告

平成14年度教育用システム統計…… 38

リモートアクセスサービス利用統計 …… 39

人事異動 …… 40

編集後記 …… 41

Computing and Communications Center
Kyushu University

www.cc.kyushu-u.ac.jp

情報基盤センターサービス機器一覧

■ 教育用システム

ホスト計算機	ah.cse.ec.kyushu-u.ac.jp
WWW サーバ	www.cse.ec.kyushu-u.ac.jp
ウェブメーラー (GraceMail)	https://mailserv.cse.ec.kyushu-u.ac.jp/

■ KITE 関連機器

教職員向けメールサーバ	mbox.nc.kyushu-u.ac.jp

■ リモートアクセスサービス

電話番号	制御手順	種別	通信速度	回線数
092-642-7341	PPP	モデム	最高 56Kbps	64 回線
		ISDN	同期 64Kbps	92 回線
		PSH(PIAFS)	32/64Kbps	32 回線

特集「ネットワークアウトソーシング事例の紹介」

池田 大輔*

インターネット利用者の急速な増加とともに、ワームやクラッキング等の件数も増加しています。最近では、今年1月末に、Microsoft SQL サーバに感染するワーム Slammer により、学内のネットワークが一時不通となりました。また、一般に公開はしていませんが、学内の支線 LAN の中には攻撃を受けたり、あるいは、その結果として他のコンピュータに攻撃をしかけているコンピュータもあります[1]。

このような状況を受け、九州大学でも学内の情報やコンピュータなどを守るために、九州大学セキュリティポリシーが策定されました。具体的な手続きを定める実施手順書も策定に向け準備中です。これらは、学内の構成員の方々が安全かつ確実にネットワークやコンピュータ、あるいはコンピュータ上の情報を利用するために作成されたものですが、保守や整備に関しては負担を強いる面もあります。コンピュータやネットワーク機器の保守等を行なう専門の職員がいるわけではない場合がほとんどで、そのため、厳格にセキュリティポリシーを実施するには人員が足りないという根強い意見があります。

このような状況に対応する解決策の一つにネットワーク管理のアウトソーシングがあります。情報基盤センター(以下、センターと呼ぶ。)では、昨年11月に学内の支線 LAN 管理者やネットワーク管理者を対象に、メールと Web のホスティングサービスについてアンケートを行ないました。費用にもよりますが、総じてホスティングサービスに高い関心があることがわかりました。しかし、アンケートはセンターが検討しているサービスについてであり、他の企業ではどのようなサービスがあるのか、また、具体的にどのくらいの値段なのかという疑問もあるかと思います。そこで、一足先にネットワーク関連のいくつかのサービスを外部の企業に委託している部局の事例をまとめて紹介する本特集を企画しました。各記事は、部局の利用形態やサービスの内容等の紹介していただいています。

メールサーバのアウトソーシング事例–大学院言語文化研究院の場合–

本特集の企画発案のきっかけとなったのは、大学院言語文化研究院でメールサーバの外注をするという話しを聞いたからです。その時は、研究院の鈴木敦典先生からセンターへ、アウトソーシングをしたいと思っているが構わないか、と問い合わせがありました。このとき、鈴木先生にアウトソーシング契約の経緯やサービスを実際に利用した感想などを寄稿してもらえないかと依頼し、快諾していただきました。

メールサーバだけの外注ですが、打ち合せの時の様子からサービスの値段まで細かに紹介していただいています。また、実際に利用しているサービスは、単にメールの送受信だけではなく、セキュリティ強化も考えたものを利用されています。

セキュリティ対策のアウトソーシング事例

次に、薬学研究院におけるアウトソーシング事例を紹介します。著者はセンターネットワーク運用掛の北技官となっていますが、著者が薬学研究院の担当者である安田事務官に話しを聞いてまとめたものです。言語文化研究院の事例ではメールサーバだけでしたが、他に Web サーバなども含め広い範囲のサービスを受けています。

*情報基盤センター研究部　mailto:daisuke@cc.kyushu-u.ac.jp

[1]もちろん、そのような事例が発覚すると同時に、当該支線 LAN 管理者を通じて対応をお願いしています。

附属図書館におけるコンピュータ関連のアウトソーシングの実際

附属図書館の事例は、ネットワークのみの外注ではなく、図書館の業務に関連したシステムの一部としてネットワーク関連機器の保守を担当の企業が行なっているものです。したがって、予算としては上述の2事例と異なりシステムの借料にネットワーク保守も含まれていると考えてよいでしょう。その意味では、あまり他部局の参考にはなりませんが、サービスの内容や対応など、どの程度期待してよいのか、という参考にはなると思います。執筆者は、センター電子図書館掛の小川掛長です。

システム情報科学研究院情報工学部門における支線LAN管理作業について

最後に、システム情報科学研究院情報工学部門における支線LAN管理作業について、乃村能成先生に紹介していただきます。ここは、管理業務を外注しているわけではなく、主に助手の方々により管理されています。システム情報という、コンピュータに非常に関連のある部局の事例で、自前でしっかり管理するにはどの程度のことをやらないといけないのかが分かると思います。

メールサーバのアウトソーシング事例 ― 大学院言語文化研究院の場合 ―

鈴木敦典*

1 はじめに

学術研究・教育のための基本的な情報インフラとして、電子メールはもはや欠かすことのできないものになっているが、同時にこれを介したウイルスの感染や、迷惑メール（いわゆるSPAM）の横行など、システム悪用による被害も増えている。メールサーバを責任もって運用するためには、常に最新情報に目を配り、絶えずメンテナンスを行うことが必要で、管理者にかかる負担は一層重くなってきている。

ところが、サーバ管理を専門に行うスタッフがいる部局はまれで、所属教官のうち誰かがボランティア的に業務を引き受けているのが一般的であろう。大学であるからにはメールサーバぐらい自前で管理できて当然、という考え方もあるだろうが、その負担が長期にわたって特定個人に集中する状況は、部局全体にとっても決して望ましいものではない。

また、万一メールサーバへの不正侵入があった場合、被害は学外の広い範囲に及ぶ可能性があり、大学としての管理責任を問われる。しかし、その責任をボランティア管理者個人が負うことはきわめて困難であると思われる。

言語文化研究院では今回、学外業者のホスティングサービスを利用することで、管理者負担の軽減とセキュリティ強化という両課題の一挙解決をはかった。ここでは、メールサーバのアウトソーシングを決めた経緯、また導入過程で生じた問題点、導入後の運用状況について報告する。

2 導入決定に至る経緯

六本松地区には大学院言語文化研究院の他、大学教育研究センター、大学院比較社会文化研究院など複数の組織が存在する。地区全体のDNSサーバはrcsvrで、多くの部局がこれをメールサーバとして利用している。その運営は長年、数名のボランティア教官によって担われてきた。日常的な登録・更新・監視業務に加え、トラブルがあると直ちに駆けつけ徹夜で復旧に尽力する管理者の姿を見るにつけ、いつも頭の下がる思いがする。

こうした運営がいよいよ限界に近づいたという理由で、六本松地区各部局に対し、自前のメー

*大学院言語文化研究院 文化情報学部門　E-mail：asuzuki@flc.kyushu-u.ac.jp

ルサーバを準備してほしいとの意向が示されたのが、今から2年ほど前のことである。また、現在のキャンパスが福岡市西区元岡・桑原地区に移転すると、rc(= ropponmatsu campus) ドメイン自体が消滅するので、従来のメールアドレス（*@rc.kyushu-u.ac.jp）はいずれにせよ使えなくなる。遅かれ早かれ自前のメールサーバを立ち上げる必要があるとわかった。

こうした状況を受け、言語文化研究院では自前のサーバ（OS は Linux) を購入し、まずウェブサーバとして運用を開始 (2001 年 8 月）し、さらにこれをメールサーバとしても利用する計画を立てた。

しかし、その際問題になったのが、想定されるさまざまなトラブル、外部からの攻撃に対し、十分な保守体制を取れるかという点であった。管理すべてを部局内スタッフだけで行うのはやはり不安である。そこで、サーバ保守を業務とするいくつかの会社に対し、メールサーバ監視を委託できないか、問い合わせてみた。

が、得られた回答は、部局として支出可能な金額とは遠くかけ離れたもの（月額数十万円）で、実現の可能性はなかった。これは要するに「管理者一人を常時張りつける」というやり方であり、これでは人件費が嵩むのも無理はない。また、週 1 回の巡回管理方式を提案する業者もあったが、安価なのはよいとしても、緊急時の対応を考えると、十分とは思えなかった。こちらの状況をよく把握したサービススタッフがいる間はよいが、その人が転勤等でいなくなった場合、責任ある保守が望めるかという問題もあった。

2001 年秋から 2002 年前半にかけて、続けざまにメールを介したウイルス (かなり悪質なワーム) 感染が部局内で発生し、安全なメール環境を望む声が高まった。

こうした中、いろいろ情報を集めるうち、ようやく見つけたのが、今回導入を決めた NTT コミュニケーションズ社による OCN メールホスティングサービス「PowerMail[1]」である。

こちらは、先の管理者張りつけ型とはまったく逆の「各顧客のサーバを一箇所に置いて集中管理する」方式で、大幅なコストダウンがはかられている。サーバの設置場所は東京大手町にある同社ビル内。24 時間体制で監視される機材は、電話交換機並みの頑丈な耐震環境に置かれているとのことである。

サーバが学外にあっても、メールアドレスは kyushu-u.ac.jp ドメインが使えること、またメール送受信に際し、自動的にトレンドマイクロ社のウイルスチェック（オプション）が行われることなど、我々の求める基本条件にかなうものであった。

3　導入準備

【2002 年 3 月末】

NTT コミュニケーションズ社と第 1 回目の交渉を行った。「PowerMail」についての説明を受ける。この日、同社からは「メール&ウェブ[2]」というウェブサーバ委託も含めたホスティングサービスの提案もなされた。管理者の負担を考えると、ウェブサーバも一括して任せた方が楽には違いないが、これは断念せざるを得なかった。基本的なディスク領域があまりに少なく (50 ユーザに対し 100MB)、研究・教育情報の発信を行う基盤としては明らかに不足だったからで

[1] http://www.ocn.ne.jp/hosting/service/index03.html
[2] http://www.ocn.ne.jp/hosting/service/index06.html

ある。このため、ウェブサーバは、引き続き自前のサーバ (flcsvr) を使用することに決まる。

【2002 年 4 月】
第 2 回目の交渉。「PowerMail」については、サーバが遠方にあることで、レスポンスの低下が起きるのではと心配されたが、この日、学内のマシンから東京のサーバを利用した送受信実験を行い、数 MB 程度のファイルを添付しても、特に問題ないことを確認した。この段階で「PowerMail」導入の方針を言語文化研究院広報メディア委員会に報告。

【2002 年 5 月】
第 3 回目の交渉。情報基盤センターからネットワーク管理掛の方に出席していただき、技術的打ち合わせを行った。九大の DNS サーバを利用し、OCN 回線上の IP アドレスとサーバホスト名を対応させる方法（A レコードによる指定）について検討。

また今回の導入が国立大学では初めての事例ということで、事務局から用度・経理・工営各掛に立ち会ってもらい、必要な問い合わせ、契約に向けての予備的検討をお願いした。物品購入を含まない業務委託に対して校費を支払うわけで、当初難しい面もあるかと予測されたが、最終的には約款上に載っているサービスということで一般の電話代等と同じ扱いでの支払いが可能になった。

【2002 年 6 月】
情報基盤センターの通信委員会で、言語文化研究院メールサーバのアウトソーシングが了承される。

【2002 年 7 月】
言語文化研究院教授会でこの件が最終的に認められる。NTT コミュニケーションズ社に正式申し込み。情報基盤センターへ、flc.kyushu-u.ac.jp という新ドメインを仮想的な支線として申請。九大のトップ DNS に、使用する 3 つのサーバ (pop.flc.kyushu-u.ac.jp, smtp.flc.kyushu-u.ac.jp, vcsmtp.flc.kyushu-u.ac.jp[3]) の IP アドレスを記述してもらう。

【2002 年 8 月末】
新メールサーバの準備が整い、利用する 50 人分のメールアドレスを登録[4]。POP サーバ上に割り当てられるディスク領域 250MB を各 5MB ずつ割り当てた[5] 。

【2002 年 9〜10 月】
正式稼動を開始し、各利用者の端末のメールクライアントソフトの設定変更ならびに旧メールサーバ（rcsvr）からの転送設定を順次行う。中には非常に古いソフトを使っている人がいて、POP サーバの指定に戸惑う場面もあったが、的確な電話サポートを受け、無事全員の分を完了。

[3]ウイルスチェックを利用する場合の送信用サーバ。
[4]csv ファイルからの一括登録が可能。パスワードは各ユーザ側でブラウザ画面から随時変更できる。
[5]一部のユーザがメールを溜め込み過ぎて、全体が受信不能に陥ったりしないよう、このような設定にした。なお、各ユーザのディスク領域使用状況は Postmaster 権限で一括調査できるので、満杯になりそうなユーザに対しては、事前に警告することが可能。

4　利用サービスの概要

以下、今回導入したサービスの概要を示す。

サービス名：	NTT コミュニケーションズ株式会社 OCN ホスティングサービス「PowerMail」
利用方法：	新設の flc.kyushu-u.ac.jp ドメインを用い、NTT コミュニケーションズ社のメールサーバ（設置場所は東京大手町）を利用し、メールの送受信を行う
DNS：	九州大学情報基盤センター内のサーバを利用
利用メールアドレス数：	50 （10〜最大 10 万アドレスまで 10 個単位で増設可能）
利用ディスクサイズ：	250MB
送信時認証方式：	セキュリティ強化のため、POP before SMTP を採用
ウイルスチェック機能：	利用する（メール送受信の際、全メッセージを自動検査）

また、同社の提供する「Mail ON[6]」サービスを用いて、到着メール確認、クイックメール（Web メール）送信、メール転送機能（2 件まで）、アドレス及び件名指定による迷惑メール自動削除機能（最大 20 件まで）などが利用できる。i モードにも対応。

トレンドマイクロ社「ウイルスバスター On-Line Scan」を利用してローカルディスクに侵入したウイルスを検出・除去する機能は、マシン数の制約なく使用できる。

以上の契約内容全体（50 アドレス）で、月々の利用料金が 25,000 円となっている。うち、ウイルスチェック・サービスが 15,000 円で、相当の部分を占めるが、各教官が個別にウイルスチェックソフトを購入する必要がなくなる分、かえって安くつくと思われる。

5　導入後の状況と問題点

導入後、約 4ヶ月が過ぎ、ようやく新しいメール環境に慣れてきたところである。以下、この間に気づいた点を述べる。

当初、POP before SMTP という認証方式にとまどう人が多かった。不正なメール送信を防止するため、メール送信を受け付ける前に POP 認証を要求する機能であるが、受信後 30 分間以上経つと、前回の認証が無効となり、送信ボタンを押しても拒否されることがある。クライアントソフト側で定期的に新着メールを読みにいく設定を行えば解決するはずの問題だが、現在でも、ときどき送信に失敗するという声を聞く[7]。

また、部局内の同僚宛てにメールを発信する場合、従来であれば、相手のユーザ名のみ記入しホスト名は省略できたのに、新サーバでは省略できない点が不便であるとの苦情もあった。

速度的にはあまり不満がない。通常であれば、自分宛てにメールを送ると、送信ボタンを押した 1〜2 秒後には届いている。福岡－東京間往復していることをほとんど意識させないスピードである。ただ、六本松地区の学生が一斉にコンピュータを使う時間帯では、いくらかレスポ

[6] http://www.ocn.ne.jp/hosting/service/mailon.html

[7] 2002 年 12 月から、固定 IP アドレスの OCN 常時接続回線サービスと PowerMail を併用し PowerMail の DNS 機能を利用している場合、その併用回線からは POP before SMTP なしでメール送信が可能になったとアナウンスされている。ただし、今回の言語文化研究院のように学内の DNS を使う場合には、該当しない。

ンスが低下するようである。また、これまで数回だが、おそらくメールサーバ側の問題と思われる極端な速度低下が見られた(20～30分間)。サーバ機材を共用している他機関・他社等で、大きな負荷のかかる使い方をしているのが原因らしい[8]。

ウイルスチェックが功を奏して、メールを介したウイルスの感染は、当方の把握している限り、この4ヶ月間1件も発生していない。ウイルスの含まれた添付ファイル等を自動削除したというメッセージは、数度ならず現れた。

ただ、増える一方の迷惑メールに対して、20件の事前登録ではとても対処しきれない。数十通の迷惑メールがいっぺんに届いた、という人もある。が、少なくとも部局のメールサーバを踏み台に多量のSPAMを撒かれる恐れがないだけでも安心していられる。

会議報告のために作った教授会構成員メーリングリストが、活用されるようになってきた。ただ、メーリングリスト作成件数が5件までと限られているため、各講座、各委員会ごとに必要な数を設定できないのが残念である。

「Mail ON」サービスのうち、クイックメール（Webメール）に関しては、かなり不満が残る。出先のコンピュータを使って気軽にメールチェックできるのはありがたいが、受信したメールに対して直接返信できない(新規メッセージとして作成するしかない)こと、添付ファイルを受け取れないことの2点は、ぜひとも改善を望みたいところである[9]。

6　おわりに

サーバ管理、とりわけメールサーバ管理というのは、その苦労の割に報われることの少ない仕事だと思う。管理がきちんと行われていればいるほど、一般ユーザはその存在を意識することがなくなるからである。

今回紹介した事例は、ボランティア管理者をその苦労から解放するとともに、比較的少額で安定したメール環境を手に入れるための選択肢の一つである。もし、同じような悩みをお持ちの部局があれば、ぜひこうした方法も検討してみていただきたいと思う。

ホスティングサービス業界には、各社次々参入しているようであるし、九州大学情報基盤センターでも有料サービスを検討中であると聞く。競い合うことによって、より使いやすく、安全でしかも安価なサービスが現れることを期待する。

[8]この問題をなくすため、NTTコミュニケーションズ社では、料金を上乗せするかわりに、機材を1顧客専用にするサービスを検討しているようである。

[9]この点について、NTTコミュニケーションズ社に問い合わせたところ、他のユーザからも多く要望されている点であり、平成15年春以降、検討していく予定であるとの返答を得た。

セキュリティ対策のアウトソーシング事例

北　祐一郎*

1　はじめに

近年ネットワークは高速化されており、九州大学のネットワークも平成12年度の補正予算により新ネットワーク（ギガビット級ネットワーク）が構築されました。基幹ネットワークは1Gbpsへ、支線ネットワークは各建屋の各階までは1Gbps、その配下は100Mbpsへ生まれ変わりました。非常に高速なネットワークへ変わったわけですが、同時に悪質なウィルスメールやサーバに対するクラッカーの攻撃による被害が年々増加しているという現実も考慮しなければなりません。ウィルスに感染したりサーバをクラックされれば、被害は自分だけでなく九大内の他の部局、或いは他大学や企業、一般の方へも及びます。

これらの被害を防ぐためには利用者や管理者の意識改革が必要で、今後はインターネットを使用するにはコンピュータをネットワークに接続するだけでよいという認識から、セキュリティ対策を行っていなければコンピュータをネットワークに接続してはいけないという認識へと変えていかなければなりません。

とはいえ、サーバ等のセキュリティ対策は支線LAN管理者やサーバ管理者にとって、本来の仕事ではなくボランティアで行っている方が殆どなので、頭の痛い問題だと思います。

情報基盤センターで支線LAN管理者に対してアウトソーシングに関するアンケートを行いましたが、回答者の約半数の方々は「料金によってはアウトソーシングを利用したい」、約３割の方々は「アウトソーシングを利用したい」ということで、回答者の約８割の方々がアウトソーシングを希望しています。特にソフトウェアのバージョンアップやセキュリティ対策の面で管理者に負担がかかっているようなので、アウトソーシングを行えば管理者の負担はかなり軽減されるのではないかと思います。

情報基盤センターはアウトソーシングを行っている部局を把握しているわけではありませんが、ネットワーク障害等で各部局を訪問した際に支線LAN管理者から伺った情報ではアウトソーシングを行っている部局は少ないようです。

そこで本稿ではサーバのセキュリティ対策として、ファイアーウォールやサーバ類のアウトソーシングを行っている大学院薬学研究院へインタビューした結果をもとに、その状況や契約内容を紹介していきたいと思います。

*情報基盤センター ネットワーク管理掛
E-mail:kita@cc.kyushu-u.ac.jp

2　導入前・導入後の状況

今回、サーバ類のアウトソーシングを行っている大学院薬学研究院へ導入前と導入後の状況を簡単にインタビューしました。

本章では、そのインタビューの内容を紹介します。

2.1　導入前の状況

・端末状況

Mac、WindowsPC、ワークステーションを使用しており、Macはメールやワープロ及び実験データの処理が主で、WindowsPCは上記用途の他に計測機器の制御に使用されている。

また、ワークステーションは各講座保有のメールサーバの他に、機器制御用及びデータ解析用に使用されている。

・導入前のサーバ類の管理状況

メールサーバ等を分散して保有管理しており、講座によっては管理者の不足で管理が困難な状況であり、老朽化や容量不足によりトラブルの頻度も高かった。

また、セキュリティホールの情報等は殆ど入らず修正プログラム適用作業も殆ど行われていなかった。

・運用状況

各講座保有のメールサーバにトラブルが高い頻度で起こっていたが、それがアタックによるものかの判別はつかなかった。

しかし、ファイアーウォール導入後のフィルタリング[1]されたパケットの件数によりアタックはかなりあったのではないかと推測される。なお、改竄等の実被害は受けていない。

メールサーバのトラブルの際は各講座の管理者が対処していたが、手に負えない場合は支線LAN管理者が対処していた。

この際、学部内にメールサーバが非常に多数存在していたため、支線LAN管理者の負担は大きかったと思われる。

[1] ここではパケットフィルタリングのことをいい、ネットワーク上のデータを選別し、そのパケットの通過を許可したり拒否したりすること。

2．2　導入後の状況

・導入後のサーバ類の管理状況

メールアカウントの設定、廃止、フォワーディング先の変更、ホームページ作成等の簡単な作業は部局のサーバ管理者が行っている。

一方、セキュリティ情報の提供や修正プログラム適用作業などは部局の担当者が行うには非常に負担がかかるため、契約業者の担当者が来学あるいはリモートにより行っている。

・ファイアーウォールの管理状況

基本的にはファイアーウォールで出口を厳しく制限し、運用を見ながら必要な通信を通過させている。

今までに図書館のデータベースを使用する際や、外部からのPOP3へのアクセス許可などでポートの開放の要望があったが、POP3へのアクセスに関しては出来る限り外部へのメールアドレスの転送により対処してもらうようにした。

なお、ファイアーウォールのポートの開閉は支線LAN管理者と希望者との話し合いで決定し、管理は契約業者が行っている。

下記はファイアーウォールを運用するにあたっての基本ポリシーである。

① 内部から内部へ（133.5.226,227,228）は全て許可
② 内部から外部へは殆ど許可
③ 外部から内部へはホスト指定で最小限のサービスポートのみ許可

・運用状況

フィルタリングされたパケットの件数は導入直後に比べ減少しており、アタックによる実際の被害は起こっていない。

しかし、メールウィルスの被害はファイアーウォールでは防御できないため[2]現在も稀にみられる。

3　契約内容

大学院薬学研究院よりファイアーウォールおよびサーバ類の管理に関する契約内容と保守に関するデータを頂きました。

本章ではその内容を紹介します。

---

[2] ファイアーウォールは一般的にポート番号（メールの送信はSMTP:tcp/25、メールの受信はPOP:tcp/110）あるいはアプリケーションごとに制御するので、例えばtcp/25を閉じてしまうとメールの送信ができなくなるためファイアーウォールでウィルスを防ぐことはできません。

3.1 契約内容

大学院薬学研究院の請負業者は「千代田興産株式会社[3]」で保守契約内容は表1のようになっており、毎月システムのログや障害状況を報告してくれることになっている。

現在大学院薬学研究院が保守契約しているサーバ数は5台である。

表1 薬学研究院の契約内容

請負業者	千代田興産株式会社
請負事項	九州大学大学院薬学研究院メールサーバ等運用支援業務
請負場所	九州大学大学院薬学研究院
対象システム	Mail・DNS・POP3・Firewall・WWWサーバ
請負期間	平成14年4月1日～平成15年3月31日（単年度契約）
業務内容	（1）日々の以下の稼働情報監視と、緊急時の対応 ・システムログ（障害発生メッセージ） ・ディスク使用状況 ・Webサーバへのアクセスログ ・Webサーバでのエラーログ ・メール送受信でのエラーログ ・ルータ、ファイアーウォールでのエラーログ （2）稼働状況をまとめた月次の報告書の提出 （3）電話及びメールでの相談対応 （4）OS設定等のリモートメンテナンス

3.2 保守データ

保守データの報告は月単位で行われており、その作業内容やファイアーウォールのログ等をまとめて報告してくれるようになっている。

以下は平成13年5月の報告例である。

[3]保守契約の金額は規模や契約内容等によってかわりますので、詳細は「千代田興産株式会社」にお尋ねください。
担当者 末金・吉田
TEL 092-533-2983
FAX 092-533-2999

報告例（平成13年5月）

① 全体の運営状況

５月度はsadmind/IISというワーム（ウィルス）が猛威を振るい、国内に設置されているSolaris, WindowsのServerで多数の被害が発生しています。

貴部門のServerの安全な運営を図る上で、主要なSoftwareの更新を実施しました。

② サーバの運営状況

サーバの運営上で、大きな問題はありませんでした。

③ 作業内容

5/23	bind-8.2.4 への更新（ Rigel, Vega ）
	apache-1.3.20 への更新（ HomePage ）
	ntpd-4.0.99k23 への更新（ HomePage ）
	Firewallのフィルタリング定義変更
5/28	Firewallのフィルタリング定義変更（ PHS関連のMailトラブル対応 ）

＊ソフトウェアのバージョンアップはCERTやCERT-JP、ディストリビュータ、各オープンソフトプロジェクトからの情報をもとに契約業者が実施しています。

情報が公開されて数日以内に契約業者から大学院薬学研究院へアップデートの許可申請があり、許可が下りると契約業者がアップデートを行います。

ただし、緊急性かつ重要性の高いものについてはアップデート後に報告がくることもあります。

④ ファイアーウォールによるフィルタリング状況

５月度にFirewallでフィルタリングされたパケットのレコード件数は、2,469,174件でした。

４月度と比較して1,900,000件ほど大幅増加（約４倍）しています。

上記フィルタリングされたパケットの内訳は下記の通りです。

TCPパケット	62,944 件
UDPパケット	2,396,590 件
ICMPパケット	9,640 件

4　おわりに

今回、サーバのアウトソーシングを紹介しましたが、これでセキュリティが完全に守られるわけではありません。例えばウィルスメールはファイアーウォールを導入したり、サーバのセキュリティを向上しても防御することはできないため、別途ウィルスチェックソフトが必要で、さらに毎日ウィルスパターンファイルのアップデートが必要になります。

このように今やセキュリティの問題はネットワークを使用する上で切っても切り離せない問題となっています。

しかしながら、クラッカーによる攻撃等は基本的に弱点がありそうなコンピュータを探し出してそのコンピュータへ攻撃するわけですから、サーバのアウトソーシングを行うことでセキュリティが強化されれば、攻撃やクラックされる可能性は少なくなると思います。

セキュリティ強化を行うと、それに比例してコストが上がり使い勝手も悪くなるためどこまでセキュリティを強化すればよいかというのは判断が難しいところではありますが、今後の管理の選択肢のひとつとして本稿で紹介したアウトソーシングを考えて頂ければと思います。

最後に、本稿を執筆するに当たってご協力頂いた大学院薬学研究院の方々に感謝致します。

附属図書館におけるコンピュータ関連のアウトソーシングの実際

小川　稔[1]

1．はじめに

附属図書館では，図書／雑誌の貸出や返却，所蔵検索，文献検索，情報検索，情報発信などのサービスを提供しています。それらの図書館サービスの根幹をなすのは，図書館電子計算機システム（以下，「システム」と略します）です。附属図書館では，システム納入業者である日本電気株式会社（以下，「NEC」と略します）の関連会社がシステムの保守を行っています。

それでは，システムの概要とアウトソーシングの現状について述べてみます。

2．システムの概要

九州大学附属図書館は，全国に先駆けて，昭和56年１月にシステムを導入し，図書館業務全般のシステム化を実現させました。その後，学術情報センター（現国立情報学研究所）における全国総合目録データベース形成事業への参加，学内LANからのOPAC（オンライン蔵書検索）提供開始を実施し，平成８年４月にオープンシステム化したシステムに更新しました。

平成12年12月に更新・導入したシステムは，NEC製の大学図書館情報システムであるLICSU-LXをベースとしたものです。本システムは，図書・雑誌の発注・受入・支払・登録・目録，閲覧，図書館間での相互利用などの図書館業務を効率的に処理しています。また，学内LANを利用した学外への文献複写／図書借用申込など，利用者サービス機能の充実・強化が図られています。

ちなみに，システムは単年度毎の借入れであり，契約上，NECが保守を行うことになっています。

3．システムの構成内訳

データベースサーバ	１台
検索／WWWサーバ	１台
メールサーバ	１台
セキュリティ／ネームサーバ	１台
目録情報中継サーバ	１台（買い取り）
多言語目録サーバ	１台（買い取り）
業務サーバ（ワークステーション）	25台（買い取り１台含む）
業務用端末	134台（買い取り28台含む）
プリンタ	30台（買い取り４台）

4．システムの役割

システムは，利用者への図書館サービスやそのサービスを行う図書館職員の日常業務を支えています。システムは，上述の図書館業務のほかに，近年，電子図書館といわれるWeb上での図書館サービスの基盤をなしています。特に，検索／WWWサーバは，附属図書館のWWWサーバの役目を果たし，OPACや利用案内だけでなく，全文検索システムや画像提供システムを取り込み，また，各種データベースシステムの入り口となっており，図書館の情報発信機能を担っています。

5．アウトソーシングの実状

保守については，サーバ類はスポットで対応し，業務用端末は年２回保守を行うことになっています。システム，特にサーバに障害が発生すると，図書館利用者及び図書館職員に多大な迷惑をかけることになります。このため，NEC側ではシステム構成機器に何らかの障害が発生した場合，図書館業務の速やかな回復を図るべく，迅速に対応しています。また，システムに障害が発生しないよう事前に対応することもあります。

サーバに関する主な障害及び対応を表１にまとめてみました。

1　情報基盤センター電子図書館掛　E-mail: ogawa@cc.kyushu-u.ac.jp

表　1　障害対応一覧

時期	内　　容	対　　応
H12.12	検索／WWWサーバのWWWサーバソフトのバーチャルホスト動作不正	Apacheの設定ファイル(httpd.conf)の修正
H12.12	データベースサーバのハードウェア障害	調査の結果，CPU障害と判明し．CPU交換
H13.1	検索／WWWサーバのハードウェア障害	同上
H13.2	ネームサーバ用ソフトのバージョンアップ	BINDをバージョンアップ
H13.2	セキュリティ／ネームサーバのセキュリティ強化	ipfilter設定変更
H13.5	検索／WWWサーバの復電時自動起動不可	「ACリンク」スイッチ設定不正のため，設定を変更
H13.6	メールサーバのメーリングリスト用ソフト(majordomo)動作不正	内部コマンド実行時に動作不正が発生しているため，設定ファイルを変更
H13.6	データベースサーバのバックアップ障害及びOracle起動不正	バックアップ所要時間増により，バックアップ及びOracleが起動に失敗していた。リブート前に終了するようブロックサイズを修正
H13.8	セキュリティ／ネームサーバのハードウェア障害	ハードディスクを交換
H13.9	データベースサーバの復電時自動起動不可	後日，UPSを交換
H13.11	WWWサーバソフトのバージョンアップ	Apacheをバージョンアップ
H14.3	データベースサーバの復電時自動起動不可	UPS障害のため，UPSを交換
H14.6	メールサーバのハードウェア障害	ハードウェア交換後，システム復旧作業を実施
H14.6	WWWサーバソフトのバージョンアップ	Apacheをバージョンアップ
H14.7	検索／WWWサーバの起動時PORT診断画面で停止	手動再起動，同日，マザーボード予測交換
H14.7	検索／WWWサーバのマザーボード予測交換後，外付けDAT装置電源連動せず	外付けDAT装置UPSコンセントへ差し替え，起動させた
H14.7	検索／WWWサーバの外付けDAT装置電源が連動しない	マザーボード交換
H14.7	検索／WWWサーバの温度異常感知によるシャットダウン	マザーボード交換
H14.8	データベースサーバの停電時にスレーブUPSが切れない　復電後のUPSが動作しない	マルチUPSボード交換，ただし，現象変化せず→後日，UPS設定情報の更新，動作確認を行う予定
H14.11	ネームサーバ用ソフトのバージョンアップ	BINDをバージョンアップ
H15.1	WWWサーバソフトのログが肥大化している	定期的に，ログファイルのバックアップを取り，別のディレクトリに移動させるようスクリプトを作成した

障害の種別に応じて，以下のとおり，対応業者は異なっています。

・図書館業務ソフトウェア
　NECシステムテクノロジー株式会社によるリモート対応
・オペレーティングシステム，ネットワーク関係
　株式会社ビーシーシーによる現地またはリモート対応
・ハードウェア
　NECフィールディング株式会社による現地対応

システムに障害が発生した場合，システム管理者（附属図書館情報システム課電子情報掛及び情報基盤センター電子図書館掛）が図書館業務ソフトウェア，オペレーティングシステム，ネットワーク関係，ハードウェアのいずれに問題があるのか判断し，各会社の担当者に障害への対応を依頼します。

サーバに障害が発生すれば，上記３社の担当者が，リモートまたは現地で迅速に対応し，適切な処置を行います。ただし，データベースサーバ復電時の自動起動に関する障害だけは，解消されたわけではありません。この件に関して，先日，NECより対応策（UPS設定情報の更新及び動作確認）が実施されました。慎重を期して，３月実施予定の中央図書館での計画停電の際，データベースサーバが復電時に自動起動できるか確認する予定となっております。

なお，ネットワーク関連では，一昨年秋以降のネットワークのギガビット移行に関して，図書館とNECで相談を行い，中央図書館及び工学部のネットワーク設定変更作業を行いました。ところが，その後，ネーム／セキュリティサーバが新ネットワークに接続できないという障害が発生しました。情報基盤センターの調査により，学内基幹LAN変更期間中は，本サーバ接続セグメントを新ネットワーク側で使用できないことが判明しました。この障害については，本サーバを旧ネットワーク環境に戻すことにより，対応することができました。後日，情報基盤センターと共同でネットワーク環境変更を実施し，新ネットワークで稼働させています。

以上のことから判断して，NEC側の障害対応には満足しています。

6．セキュリティ対策

各種サーバは，情報基盤センターによって，ファイアウォールの配下に置かれています。また，NEC側でもサーバのセキュリティ確保を重視していますので，外部から侵入を受けたことはありません。

7．おわりに

今回，附属図書館におけるアウトソーシングの実例を紹介しました。本稿を作成したのは私ですが，実際に，システムを管理しているのは，附属図書館情報システム課電子情報掛です。電子情報掛とNEC側の迅速かつ的確な対応により，システムは障害が発生しても速やかに復旧し，図書館利用者及び図書館職員に不利益を被らせるのを短時間に抑えています。

以上のとおり，附属図書館では図書館サービスの維持及び安定化を図っていることを述べました。このことにより，皆様の知らない図書館の一面をお伝えできたのではないでしょうか。附属図書館では図書館サービスの向上も図っていきますので，今後とも図書館をご利用ください。

システム情報科学研究院情報工学部門における支線LAN管理作業について

システム情報科学研究院情報工学部門
乃村能成
nom@csce.kyushu-u.ac.jp

1 はじめに

システム情報科学研究院情報工学部門における支線LAN管理作業の概要について説明する．他の支線LANに比べて，管理すべき事柄は大きく違わないと思われるが，その手法や道具については幾分違うかもしれない．また，情報工学部門は，ネットワークそのものを研究している研究室を擁しているため，ネットワークの構成にやや特徴がある点も多くの他学科と違う点であるといえる．

そこで，まず，当部門のネットワーク構成について簡単に説明する．次に，支線LAN管理作業の手法やツールについて説明したい．当部門では，サーバ計算機の多くをUNIX機で構成しており，いわゆる伝統的な管理手法をとっている．つまり，UNIXサーバにキャラクタベース端末で遠隔ログインして管理作業を行っている．昨今のマウス1つでできる管理作業スタイルと比べると，逆に新鮮な部分もあるのではないかと思い，作業に実際利用している道具立てを中心に紹介することにしたい．紺屋の白袴という部分もあるかもしれないが，参考になる部分があれば幸いである．

最後に，運用上抱えている問題点や課題を説明する．

2 ネットワーク構成の概要

まず，情報工学部門に関わるネットワーク構成の概要について説明する．当部門は知能システム学部門と関係が深く，ネットワーク利用やその管理において互いに連携している．そのため，知能システム学部門のネットワークについても説明の都合で一部言及している．

情報工学部門に関わるネットワークには，以下の6支線LANがある．

(1) KITEネットワーク用
(2) 情報工学部門用/管理用
(3) 情報工学部門用
(4) 知能システム学部門用
(5) 教育用システム端末用

九州大学情報基盤センター広報
Vol. 3 No. 1 2003

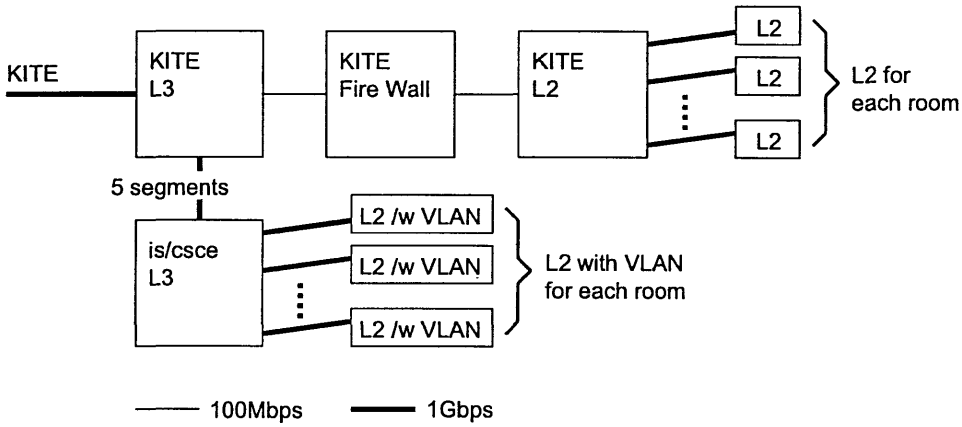


図 1: 知能システム・情報工学部門のネットワーク構成概略図

(6) 無線ネットワーク用

図 1 に各支線 LAN を収容しているネットワーク機器構成を示して，具体的に説明する．

支線 LAN (1) は，情報基盤センター設置の KITE L3，Fire Wall，KITE L2 を経由して各部屋に配線されている．通常の運用ネットワークとして利用している．Fire Wall によって外部との通信を制限することができる反面，それによる速度低下がある．

支線 LAN (2)-(6) は，情報基盤センター設置の KITE L3 を系由し，is/csce L3 に収容されている．is/csce L3 から，建物内の各部屋に設置されている L2 スイッチには 1000Base-SX で接続しており，知能システム学・情報工学部門独自のネットワークを構成している．各部屋の L2 は全て VLAN に対応しているので，目的に応じて，ポート単位で 5 つの支線 LAN のいずれかを自由に割当てることができる．この特徴は，運用の自由度を上げるだけでなく，研究のための一時的なネットワークの構成変更や，実験ネットワークを柔軟に構成することにも役立つ．

管理のための各種サーバは，支線 LAN (2)-(6) の側に配置されている．サーバ用の OS として，Solaris, FreeBSD をはじめとした UNIX 系 OS を多く採用している．

3　支線 LAN 管理の業務

支線 LAN 管理の業務は，IP アドレスの管理とネットワークの接続性確保が作業の中心となるが，付帯的なネットワークサービスについても管理業務の一端を担っている．関係の大小はあるが，おおよそ以下の項目がある．ここでは，項目を挙げるのみにする．

(1) 計算機のメンテナンス

セキュリティ勧告に基づくソフトウェアのバージョンアップ，バックアップ，停電作業

(2) 情報管理

IPアドレス，DNS情報，電子メールアドレス，メーリングリスト，Webページ，アカウント情報

(3) ネットワーク管理

ルーティング，各種サーバ (Mail, DNS, Web, Cache) 運用

(4) 監視・障害対策

ネットワークトラフィックの監視，障害対策

(5) 情報提供

統計情報，需要予測，技術情報，ウィルス情報，管理者育成，機器購入に関する情報提供

(6) 実験・検証

新しい技術の実験と検証，装置導入前の検証

4 管理作業の道具とその利用例

管理作業を行う上で，様々なソフトウェアツールを利用している．その中でもよく利用する定番ツールを紹介する．

ssh[1]

sshとは，telnetに代わる遠隔端末ツールである．ネットワーク上に配置された各種サーバを管理するために，管理者は，遠隔の計算機からサーバにログインして作業を行うことが多い．そのような場合，かつてはtelnetクライアントを利用していた．しかし，telnetではパスワードの送信を含めて，全ての通信が暗号化されずに行われるため，悪意のある第三者が通信内容を容易に傍受してしまう危険性があった．そのため，近年ではtelnetクライアントに代わりsshクライアントを利用することが多い．sshは，通信を暗号化することによって安全性を確保している．代表的なものに，各種UNIXに対応したOpenSSH，Windows上の実装として，ttsshなどがある．詳細については，過去の広報[2]に詳しい解説があるので，それを参照していただきたい．

sshは，セキュリティ向上を第一の目的としているが，それ以外に多くの便利な機能を持つ．そのため，telnetからの移行が急速に進んだ．例えば，sshを利用したport forwarding，中でもX画面の安全な転送は利用する機会が多い．通常，セキュリティの向上 = 利便性の低下という図式が一般的であるが，sshに限っては，そうともいえない．導入をおすすめする．

rsync[3]

日常的なデータのバックアップが必要であることはいうまでもない．多くのユーザのホームディレクトリを抱えるサーバなどは，日頃からバックアップ体制を整え，高価なテープドライブに毎日バックアップを取ることを考慮されている場合が多い．しかし，小規模の，管理者以

外のユーザを持たないようなネットワークサーバの場合，少量であるが重要な設定ファイルを持っている．管理者はそのようなサーバが持つデータのバックアップを怠りがちである．

このような場合，我々は rsync を利用してバックアップを取ることが多い．rsync は，遠隔の計算機と手元の計算機のファイルの同期を取るツールである．これによって例えば 2 台の計算機の /etc ディレクトリ以下を相互に保存しあうことで，安価にバックアップを取ることができる．

rsync は，2 台の計算機にインストールさえすればすぐに利用できるため，導入が簡単で，バックエンドとして ssh を利用することができるので，安全性も高い．また，同期アルゴリズムが高速であるため，数 GB 単位のバックアップをそれほど高速でない回線を利用して毎晩同期することも可能である．

RCS[4] と CVS[5]

支線 LAN 管理作業では，各種設定ファイルや Web ページ等の文書の更新作業が多く発生する．複数の管理者が連携して作業することも多い．そのため，ある管理者による文書更新作業の内容が，他の管理者の作業内容と矛盾しないようにすること，また，作業の履歴を残しておいて，ロールバックできるようにすることは大事なことである．

そこで，RCS, CVS といったバージョンコントロールのためのツールを利用している．RCS や CVS は以下の作業を支援してくれる．

(1) 更新履歴の管理

(2) 更新内容が衝突した場合の調整作業

(3) 異なるバージョン間の比較

(4) 過去のバージョンへのロールバック

これによって，操作ミスによる事故を防ぐだけでなく，共同作業を円滑に進めることができる．

Perl[6], Ruby[7] と Make[8]

退屈な管理作業を少し楽しくするために，プログラミングは必要な行為である．Perl や Ruby は，プログラミング言語処理系である．どちらもテキスト処理を得意としており，小さなプログラムを書くことで，退屈な設定ファイルの編集に要する労力を軽減してくれる．たまに管理者の作業量を劇的に低減するようなプログラムを書き上げると，カタルシスが得られるものである．よく利用している自家製プログラムを下記に挙げる．(一般には配布していない)

makerev	DNS の正引き情報から，逆引き DB を生成する．
dhcp_check	DHCP サーバによる IP アドレス動的割当の状況をレポートする．
sdb2x	教職員の名簿ファイルから，各種メーリングリストのメンバと，部門の Web ページを自動生成する．

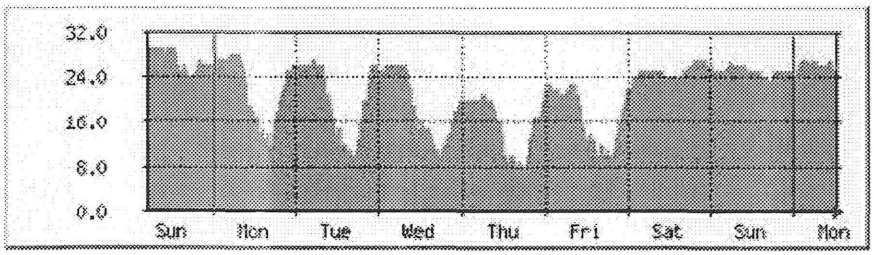


図 2: MRTG

Perl や Ruby の他に，UNIX 標準の sh, sed, awk もよく用いる．Make はプログラミング言語処理系ではないが，管理作業において一連のバッチ処理を効率よく行うためによく用いるため，ここに含めて名前を挙げておいた．

MRTG[9]

管理に必要な各種統計情報を視覚化することは，ネットワークやサーバの監視をしたり，現状の問題点を明らかにしたり，今後の管理方針を立てることに役立つ．そのような目的に，MRTG を用いている．

MRTG は，SNMP (Simple Network Management Protocol) によって取得できる情報を視覚化するツールである．例えば，ルータを通過するトラフィック量の推移やサーバマシンの負荷を日，週，月，年単位でグラフ化し，Web ブラウザで見られるような HTML を生成する．また，MRTG は，SNMP だけではなく，各種時系列データをグラフ化するインタフェースを備えているため，様々な応用が可能である．例えば，計算機ログインログを視覚化することで，計算機利用動向を知ることができる．

MRTG の出力例を，図 2 に示す．図 2 は，MRTG が出力した Web ページの抜粋である．図は，DHCP による動的 IP アドレスを取得している計算機の数を時系列で示している．前述の自家製プログラム dhcp_check が出力したデータを MRTG に与えることで実現している．このグラフは，動的割当て用に用意すべき IP アドレスの最適数を見極めるのに役立っている．

その他，ネットワークでライセンス鍵を配布してユーザ数を管理しているソフトウェア (例えば Wnn 仮名漢字変換サーバ) の利用状況を視覚化して，ライセンス追加購入の必要がないかどうかの判断材料に利用したりしている．

TCPDUMP[10] と Ethereal[11]

ネットワーク障害の際に，ネットワークを流れるパケットを覗いてみることで解決の糸口を得ることができる．TCPDUMP と Ethereal は，ネットワークに流れるパケットを解析するためのツールである．ここでは，名前の紹介にとどめ，詳細は省略する．

5　運用における問題点と課題

支線 LAN 管理において，現在抱えている問題には，以下がある．

ウィルスの増加

最近のウィルスはメールや特定プログラムに仕込まれたトロイの木馬によって感染することが多い．そのため，ネットワークの特定ポートを塞ぐといった対策によっては解決しない．クライアント PC のこまめなソフトウェアアップデート，ウィルス対策ソフトの導入の奨励等を行う必要がある．当部門では，ウィルス対策ソフトを一括導入した．これによる効果を期待しているが，それ以上に，身元のはっきりしないソフトウェアを実行しない，添付ファイル付きのメールを安易に開封しない等のユーザ教育が必要である．

ネットワーク構成の柔軟性向上に伴う複雑化

昨今は，VLAN 技術によって，物理的な 1 本の線に 2 つ以上の支線 LAN を混在させることが可能となった．そのため，各部屋にあるスイッチの特定のポートのみを違う支線 LAN に割当てることができるので，柔軟なネットワーク構成が設定一つで可能になった．また NAT や NAPT と呼ばれるネットワークアドレス変換技術によって，プライベートネットワークを構成することも容易になっている．しかし一方で，そのためにネットワーク構成は複雑さを増し，矛盾なくルーティングの設定をしたり，それらの設定内容に関する理解を管理者全員で共有することが難しくなりつつある．

省電力

ネットワーク機器が増えるにつれ，常時稼働する機器が増えてきた．そのため，それによる消費電力も馬鹿にならなくなってきた．加えて，P2P に代表されるような技術によって，端末とサーバの区別が希薄になってきている．そのため，PC であっても常時電源を入れていることが多くなってきている．

IP アドレスの枯渇

ネットワークに PC を接続するのは非常に簡単になっている．PC を買ってきて HUB につなぐだけでネットワークサービスが受けられるようになっているのは，DHCP に代表される

ネットワーク設定の自動化技術のおかげである．これによって多くの PC が管理者の手を煩わせることなくネットワークに接続している．また，今やプリンタも IP アドレスを持つのがあたりまえになりつつあるし，全ての機器が IP アドレスを欲しがっている．そのため，電力の問題と同時に IP アドレス不足が現実的になってきた．多くの PC は DHCP によって動的に IP アドレスを取得する．そのため，固定的に割当てるためのアドレスと，DHCP 用のアドレスの配分についても考慮する必要がある．

6 おわりに

情報工学部門における，支線LAN 管理作業の概要と，管理のための道具について説明した．種々の道具を利用することによって，管理作業が楽になる．しかし，やはり重要なのは，管理や運用に直接的，間接的たずさわる方々の協力体制である．当部門でも，日頃の実作業を行っているのは，主に教官 3 名，修士の学生 4 名程度であるが，それ以外にも，各研究室の方々や学生の皆さん，情報通信のためのワーキンググループ，各委員会の方々，知能システム学部門の皆さんによって，ネットワークが維持されていることを最後に明記したい．

参考文献

[1] OpenSSH: http://www.openssh.com/

[2] 伊東栄典，井上仁: SSH による遠隔接続，九州大学情報基盤センター広報 Vol.2, No.1, pp.32–40, (2002)，http://www.cc.kyushu-u.ac.jp/koho/genkoVol2No1/inoue-ssh.pdf

[3] rsync: http://samba.anu.edu.au/rsync/

[4] RCS: http://www.gnu.org/software/rcs/

[5] CVS: http://www.cvshome.org/

[6] Perl: http://www.perl.com/

[7] Ruby: http://www.ruby-lang.org/

[8] Make: http://www.gnu.org/software/make/

[9] MRTG: http://people.ee.ethz.ch/ oetiker/webtools/mrtg/

[10] TCPDUMP: http://www.tcpdump.org/

[11] Ethereal: http://www.ethereal.com/

キャンパス間接続のギガビット化および対外接続の高速化について

岡村耕二†

1　はじめに

平成12年度の補正予算によって、平成13年度に九州大学の学内ネットワーク基幹部分のギガビット化が完了しました。しかし、これに対して、対外接続であるSINETとの接続部分の回線速度は40Mbps、また、箱崎から病院、筑紫、六本松キャンパスへの回線速度は30Mbpsでしたので、インターネットへの接続およびキャンパス全体で見るとキャンパス内のギガビット化を十分に活用できる状況ではありませんでした。一方、平成14年度には九州大学にもスーパーSINETが伸び、また、キャンパス間ネットワーク用に通信事業者から光ファイバを直接借りることができるようになったため、インターネットへの接続ならびにキャンパス間の回線速度もキャンパス内と同様にギガビット級となりました。本稿は、このキャンパス間のギガビット化および対外接続の高速化について紹介します。

2　キャンパス間のギガビット化について

以前のキャンパス間接続は、箱崎キャンパスを中心として、病院、筑紫、六本松を30Mbpsの回線速度のATMで接続していました。しかし、30Mbpsという速度がキャンパス内のギガビットネットワークに比べ非常に低速であることに加えて、キャンパス内で用いられているイーサネットというネットワークの種類とATMの相性が悪く、キャンパス全体で見ると効率的なネットワーク構成ができないという問題がありました。ATMは、2つのホスト間を接続するネットワークメディアであるのに対して、イーサネットは同一のネットワークメディアで複数のホスト間の通信が行えるものであり、そのため、例えば経路制御を考えても、キャンパス内とキャンパス間での経路制御方式も複雑になりがちでした。

さて、箱崎キャンパスから他のキャンパスまでは10Kmから20Kmくらいの距離があるため、九州大学が間にケーブルを敷設してゆくのはほぼ不可能です。そこで、キャンパス間のネットワークは通信業者のサービスに頼らざるを得ないのですが、キャンパス間をイーサネットで接続するためには、いくつかの選択肢がありました。一つは、通信業者がサービスとして提供しているイーサネットサービスを購入すること、もう一つは通信業者から直接光ファイバを借りてその上でイーサネットを利用すること。最初のイーサネットサービスの購入は比較的安価で手軽なのですが、回線速度が高々100Mbpsであること、福岡市外となる筑紫キャンパスへのサービスは間にスイッチが

†九州大学情報基盤センター
Email: oka@cc.kyushu-u.ac.jp

余計にはいるため、法外に高価になること、それからこれが比較的決定的な要因でもありましたが、キャンパス間の通信の一部に内線電話が用いられていて、これがATMを使っていることなどにより、イーサネットサービスの購入は見送り、光ファイバを借りることに決まりました。

多くの方は光ファイバを借りるメリットとして、高速ネットワークが実現できることをまず考えられると思います。それは確かに正しいのですが、キャンパス間ネットワークで光ファイバを直接利用できる他の長所は、WDM (光多重装置) によって、複数の種類のネットワークメディアが利用できることです。そのため、通信業者から借りた1本の光ファイバで、ギガビットイーサとATM二つのネットワークメディアを箱崎から各キャンパス間で利用できるようになりました。前者は研究用ネットワークとして、後者は事務用LANおよび 内線用にそれぞれ活用されています。なお、平成15年10月に統合が予定されている九州芸術工科大学 (統合後は大橋キャンパス) との接続も同様に通信業者から光ファイバを借りて接続する計画がすでに進められています。

キャンパス間のネットワークとして、通信業者から光ファイバを借りる案は、新キャンパス計画専門委員会の情報通信基盤 ワーキンググループで、将来元岡キャンパスと箱崎キャンパスなどを高速に接続するために必要であるという提言にも基づいています。本当のことをいうと、情報通信基盤 ワーキンググループではこんなに早くキャンパス間で光ファイバを利用できるようになるとは考えていませんでした。当初は、元岡キャンパスと箱崎キャンパスがギガビットで接続できればいいという案でしたので、これがかなり早く前倒しになったことになります。現在の通信技術に基づいて考えると、元岡キャンパスと箱崎キャンパスは 40Gbps のイーサネットで接続されると予想されます。しかし、技術の進歩はもっと早いので、実際にはもっと高速なネットワークで接続されることになると思います。

3 対外接続の高速化

国立情報学研究所が運用しているSINETの超高速版であるスーパーSINETが2002年10月から九大でも利用できるようになりました。これによって、従来40Mbps程度でSINETに接続していたのが、ギガビット級の回線速度に更新されました。SINET内部では全ての組織とギガビット級の速度で通信できるわけではありませんが、ネットワークを利用した研究が活発に行われている研究組織とはギガビットの速度で通信が可能となりました。また、スーパーSINETは、電子メールやWebアクセスなどのいわゆるコモデティ用のネットワークが大容量になっただけではなく、スーパーSINETを構成するラムダネットワークをネットワーク研究者に直接提供したり、スーパーSINETの中でMPLSという技術を用いて高速なVPNを提供したりしています。九州大学でもこれらの研究者向けのネットワークサービスをグリッド研究、高エネルギー研究、核融合研究、宇宙・天文研究、日韓高速ネットワーク研究などで利用してます。この際に、キャンパス間ネットワークがギガビットイーサになっているため、イーサネットのVLAN機能を用いて、例えば箱崎キャンパスと六本松キャンパスに分散している天文研究チームに一つの広大なネットワークセグメントを提供したりすることが可能となりました。なお、これらのスーパーSINET上の研究にキャンパス内の各研究室から参加するためにはスーパーSINETと直接接続している情報基盤センターとの高速な接続が必要になります。キャンパスのギガビット級ネットワークを利用するというのは

いい案ですが、キャンパス内の通常のトラフィックと共存しないといけないという問題があります。そのため宇宙研究などは専用の光ファイバを独自で敷設し情報基盤センターとの接続に利用しています。

4　おわりに

現在、九州大学から SINET に向けて定常的に 100Mbps 以上のトラフィックがあります。先の 1 月 25 日に発生したマイクロソフト社製の SQL Server に関するワームの事件の時には 200Mbps 以上のトラフィックが記録されましたが、実は、別の日でこれ以上のトラフィックが発生した日もありました。1Gbps が埋まるのはまだ先と考えていたこともありましたが、それは予想よりも早く来そうです。今後も、地区間の高速化について世の中の技術情報また動向に注意して常に最善の環境を提供できるようにするチャレンジ精神を忘れないようにしなければなりません。

九州大学の学内LANにおける ウェブサーバの分布と傾向について

笠原 義晃*

1 はじめに

近年，インターネットはますます普及し，インターネットの利用法としてのワールドワイドウェブ (以下ウェブ) も完全に定着したように思います。今のところ，ウェブとインターネットは切っても切れない関係にあると言っても過言ではないでしょう。ウェブを閲覧するためのウェブブラウザは，インターネットにつながるパソコンやワークステーション用の OS のみならず，個人情報端末 (PDA) や携帯電話，ゲーム機にも組み込まれています。インターネットでの情報収集にウェブブラウザは必須と言えます。

逆に言うと，インターネットで情報発信をする場合にもウェブを利用するのがよいことになります。九州大学では，今の所学内 LAN で個人が自由にウェブサーバを用意して情報発信できるため，学内に数多くのウェブサーバが稼働しており，研究や趣味の情報を発信していると思います。加えて，ウェブブラウザが一般に普及し，利用者もその操作に慣れているため，プリンタやルータといったネットワークに接続しているさまざまな機器の設定や状態確認にもウェブの仕組みが使われるようになっています。組み込み用のウェブサーバが稼働し，PC 上のウェブブラウザで接続して設定変更などをできる機器が増えているわけです。サーバが動いているのに気づかずに使っている人もいるでしょう。つまり，現在学内のネットワーク上では多数のウェブサーバが稼働し，内外からの接続を待ち続けているということになります。

ウェブサーバが稼働していると，問題になる可能性があります。ウェブサーバに限りませんが，サーバはクライアントからの要求を受け取り，サーバ側で何らかの処理をしてクライアントに応答を返します。通常，クライアントから悪意のある行為 (パスワードファイルを見るとか，機器をクラッシュさせるなど) はできないように，サーバには防御手段が構じてあるのですが，人間が作る物ですから見落しや勘違いなどがある場合もあります。その結果，クライアントから特殊な要求をサーバに送ってサーバを乗っとったり，動作を停止させたりする方法が見つかる場合があります。このような問題点をセキュリティホールと呼びます。もちろん，一般的にそのような問題点は随時修正され，修正されたプログラムが公開されます。しかし，もし利用者が自分の所有する機器でサーバが動いているという事実を知らなければ，新しいプログラムを入れ直すこともなく，セキュリティホールは残ったままになります。

*九州大学情報基盤センター
E-mail : kasahara@nc.kyushu-u.ac.jp

2001 年夏に大発生した CodeRed[1] と呼ばれるプログラムも，このようなセキュリティホールが原因でした。CodeRed は，Windows 2000 (Professional 含む) などに標準で付属している Microsoft Internet Information Server (IIS) というウェブサーバのセキュリティホールを利用し，自身を他の同じ問題を持つサーバに感染させて自己増殖するという機能を持っています。このようにネットワーク上で自己増殖するプログラムをワームと呼びます。このワームがネットワークに放たれた時，インターネット上にはセキュリティホールのある IIS を稼働させている PC が多数あり，ワームはまたたく間に世界中に蔓延しました。このワームは感染するとその PC の力を振り絞って他のホストに攻撃をかけるため，攻撃のためのデータ転送量も大変大きくなります。九州大学でもこのワームが原因で学内 LAN が停止するほどでした。Windows 2000 を標準インストールしても IIS はインストールされませんが，フルインストールしたり，その Windows に特定のソフトウェアをインストールすると，IIS が自動的にインストールされて起動されてしまいます。このため，自分ではサーバを稼働しているつもりがなくても，実は CodeRed が感染する状態になっている PC がたくさんあったのです。IIS 側の問題は既に修正され，修正用のファイルも公開されていますが，発生から 1 年以上経った今でも CodeRed は根絶されておらず，攻撃は少なくなったとは言え日々続いています。また学内でも時々感染するホストが出ています。

CodeRed はほぼ鎮静化しましたが，今後また同じような問題が別のサーバプログラムに対して発生しないとも限りません。このような問題に対策を構じるには，学内でどれくらいどのようなウェブサーバが活動しているかをまず調査する必要があります。情報基盤センターでは，2002 年の 7 月と 8 月に 1 回ずつ，試験的にこの調査を行ないました。本稿では，その結果の概略と，発見された主なウェブサーバに関する情報を提供します。

2　経緯

2002 年 6 月，特に UNIX 系の OS で最も利用されている Apache というウェブサーバに，重大と思われるセキュリティホール[2]が発見されました。発見された時には，このセキュリティホールを利用してそのサーバを乗っ取られる可能性が示唆されました。最終的に，そのセキュリティホールは CodeRed の時ほど簡単には利用できないことがわかりましたが，発見された時には CodeRed の再来になるのではないかと言われた程のインパクトがありました。少なくとも特定の OS(FreeBSD の特定のバージョン) に対して，自己増殖するワームが作成され，インターネット上で活動していることが確認されていました。

Apache は学内でも多数利用されているため，CodeRed の二の舞になる恐れがあり

[1] http://www.microsoft.com/japan/technet/security/virus/default.asp
[2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0392

ました。しかし，学内でどれくらいApacheが利用されているかは把握されていませんでした。そこで，ウェブサーバに接続した時にサーバから帰ってくる応答を収集し，学内LANにおけるウェブサーバの稼働数やその種類の分布を調査することになりました。

調査は7月15日と8月23日の2回実施されました。また，7月の調査後，問題があると思われるApacheウェブサーバが稼働している支線の支線LAN管理者にそのことを通知しました。

調査には，scanssh[3]というソフトウェアを使用しました。このソフトウェアは元々SSHのバージョン文字列を収集するために開発されたのですが，-p 80というオプションでポート80(ウェブサービスに利用されるポート番号)を指定するとウェブサーバのバージョンを収集するという機能があります。そこで，簡単のため今回はこのソフトウェアを利用しました。このソフトウェアによるサーバのスキャン結果は図1のようになります[4]。

図 1: スキャンの出力

```
   :
133.5.***.110 <refused>
133.5.***.111 <refused>
133.5.***.112 HTTP/1.0 501 Not implemented
133.5.***.113 <refused>
133.5.***.114 <timeout>
133.5.***.115 Server: JC-HTTPD/1.3.7
133.5.***.116 HTTP/1.0 501 Not implemented
133.5.***.117 <timeout>
133.5.***.118 <timeout>
133.5.***.119 <refused>
133.5.***.12 <timeout>
133.5.***.120 <closed>
133.5.***.121 Server: JC-HTTPD/1.3.7
133.5.***.122 Server: JC-HTTPD/1.3.7
133.5.***.123 Server: Microsoft-IIS/4.0
133.5.***.124 Server: Apache/1.3.26 (Unix)
133.5.***.125 <refused>
   :
```

[3] http://www.monkey.org/~provos/
[4] 支線のアドレスは隠しています。

Server: で始まる文字列が，サーバが返したサーバの種類を示しています。サーバが自分の種類を返さなかった場合には，HTTP で既定されているステータスコードが表示されます。また，<refused> は「そのアドレスで機器は稼働しているがウェブサーバは動いていない」，<timeout> は「そのアドレスで機器が稼働していない」，<closed> は「そのアドレスで機器は稼働していてサーバも動いているが，接続直後に切断された」という意味になっています。途中にファイアウォールなどがあると，機器があるのに見えない場合もあります。今回の調査ではファイアウォールの存在は考慮せず，結果を返してきたホストだけを対象としました。

3　結果

3.1　総計

まず，センターからのスキャンに対して応答したホストやウェブサーバの総数を表1に示します。

表 1: ホストとサーバの数

日付	サーバなし	サーバあり	合計	サーバ種別判明	種別不明	合計
7月 15 日	6177	893	7070	788	105	893
8月 23 日	5312	835	6147	731	104	835

九州大学は約 6 万 5 千台の機器が接続可能なアドレス空間を持っており，調査ではそのアドレス全てに対し接続要求が出されました。その結果，7 月には約 7 千台，8 月には約 6 千台の機器が (ウェブサーバの有無にかかわらず) 何らかの応答を返しました。これは実際にセンターに登録されているホストの数よりもかなり少ない結果になっています。ファイアウォール等に保護されている機器は見えませんし，8 月は夏休みだったため電源が落とされている機器も多かったと思います。いずれにしても，これくらいの機器が九大の外からも見えているわけです。

ちなみに，九州大学の全アドレス空間をスキャンするのに要した時間は 12 分程度でした。学外からスキャンする場合はもうちょっと時間がかかると思われますが，いずれにしても非常に短時間でスキャンできるわけです。「誰にも言わずにこっそりサーバを動かしているから見つかる心配はないだろう」という考えは全く間違っていると言えます。ネットワークの高速化は，利便性を高めると同時に，危険性を増す原因にもなっていると言えるでしょう。

3.2 Apacheのバージョン

次に，本来の目的であった「Apacheのバージョン」について見てみます。

まず7月の調査です。7月15日当時，正式に公開されているApacheの最新版は1.3.26と2.0.39でした[5]。これらの最新版で，この調査の時に問題になっていたセキュリティホールが修正されました。これより古いバージョンのサーバにはセキュリティホールが残っていました。

調査の結果，発見された893台のサーバのうち，462台がApacheを名乗り，そのうち最新版を名乗ったサーバは168台でした。つまり，残りの294台はそれより古いバージョンでした。これは95の支線に渡って存在していました。そこで，対応する各支線LAN管理者に対しバージョンアップを勧めるメールを送りました。この時，調査の主眼は古いApacheの駆逐にあったため，その他のサーバについては特に連絡等はされませんでした。

続いて8月の調査です。8月23日当時の最新版は1.3.26と2.0.40でした。調査の結果，発見された835台のサーバのうち，409台がApacheを名乗り，そのうち最新版を名乗ったサーバは250台でした。つまり，残りの159台はそれより古いバージョンでした。以上をまとめると表2のようになります。

表2: Apacheのバージョン

日付	全サーバ数	Apache総数	最新版	それ以外
7月15日	893	462	168	294
8月23日	835 (-58)	409 (-53)	250 (+82)	159 (-135)

2回目での最新版とそれ以外の数の変化を見ると，1回目の調査後の指摘によって古いバージョンがある程度駆逐され，最新版に置き換わった様子がわかります。連絡した結果，不要であるとして停止されたサーバもあったようです。つまり，管理者への連絡は効果があったと言えると思います。しかし，完全に駆逐するには至っておらず，やはりメールで支線LAN管理者に連絡するだけでは完全に古いバージョンを駆逐するのは難しいとも言えます。

3.3 調査の問題点

1回目の調査で見つかった古い(と思われる)Apacheに関して，各支線LAN管理者へ個別に連絡した結果，一部の管理者の方々から返事をいただきました。それらのメールのやりとりを通してこの調査での問題点がわかってきました。

それは，「サーバの返すバージョン文字列だけではセキュリティホールがあるかどう

[5]Apacheは1.x系と2.x系の2つの系統で開発が進められています

か判断できない」ということです。サーバが返すバージョン文字列は，単にサーバがそう主張しているだけですから，管理者がその気になれば任意の文字列を返せます。また，管理者はそこまで手を出していなくても，OS に Apache ウェブサーバが付属しており，かつ OS の開発元がこのバージョン文字列に手を入れている場合が多いのです。

ウェブサーバは OS の管理などに利用される場面が増えており，もともとのプログラムに OS の開発元によって改変が加えられている場合があります。また，Apache の開発元によるバージョンアップに伴う機能拡張により，その OS に付属している設定ファイルが使えなくなる等，機能拡張が邪魔になる場面もあります。このような場合，あるバージョンでセキュリティホールが発見されると，その OS の開発元は Apache のバージョンアップで対応せず，古いバージョンにセキュリティ修正のみを適用します。

今回の調査では，例えば Vine Linux においてバージョンは 1.3.23 のまま修正が施されたサーバ，RedHat Linux において 1.3.22 を修正したサーバ，また古い Debian Linux では 1.3.6 というようなかなり古いサーバを独自に修正し続けていることがわかりました。また，セキュリティ修正が適用される前と後で，ウェブサーバが返すバージョン文字列には変化が無いサーバが多く，スキャンをかけてバージョン文字列を集めても対処済みかどうかがわからないサーバがかなりありました。

このように通常のサーバ応答だけで判断がつかない場合，セキュリティホールがあるかどうかを調べるには，実際に攻撃をかけてみるしかありません。今回の調査では，たまたま手元に疑似攻撃をかけてセキュリティホールの有無を判別できるプログラムがあったため，これを希望する部局のサーバにだけ使用して，本当にセキュリティホールの対策が行われているかどうかを調べることができました。しかし，常にこのような疑似攻撃ツールが手に入るとは限りませんし，疑似といってもセキュリティホールを突くことには変わりがないため，思わぬ障害が出るかもしれません。

この問題は Apache に限った話ではありません。例えば Microsoft IIS でも同様で，先に述べた CodeRed 対策がされたかどうかもバージョン文字列では判別ができません。セキュリティ対策がなされているかを外部から調べる監査ツールを利用して，ある程度は情報収集できます。とは言え，最も正確にそのホストの状況を把握できるのはそのホストの管理者です。各ホストの管理者が，責任と自覚を持ってホストを管理するのが最良の対策と言えるでしょう。

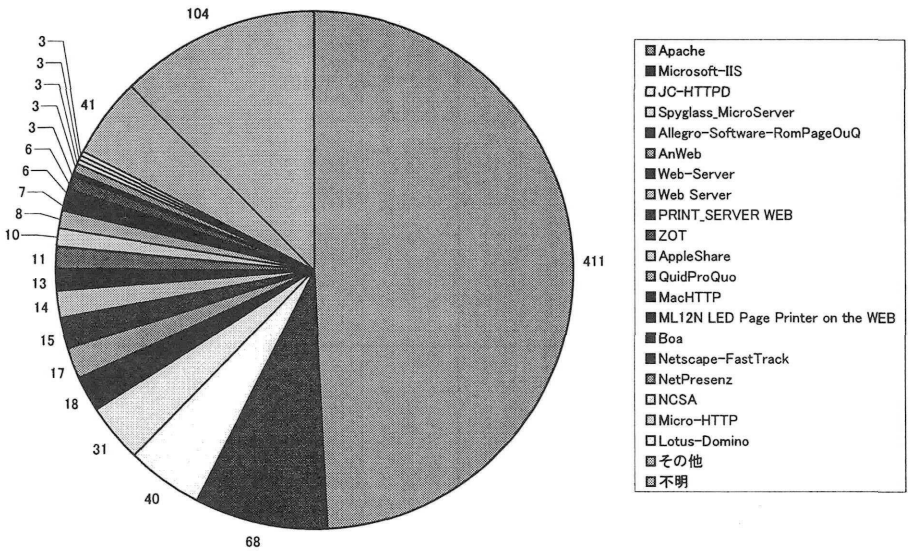
4　Apache 以外のサーバについて

4.1　サーバの種類

当初この調査では Apache のバージョン調査を主眼に置いていたわけですが，収集した情報には他のサーバからの応答も含まれています。そこで，Apache 以外にどの

ようなサーバが発見できたかを集計してみました。集計は，8月23日分の調査結果を元に行いました。サーバの返したバージョン文字列から単純に集計した結果を図2に示します。

図 2: 発見されたサーバの種類



これを見ると，お馴染みのApacheやMicrosoft IISといったサーバ以外に，あまり聞かない名前がたくさんあるのに気づくと思います。JC-HTTPD 40台とか，Spyglass Microserver 31台などです。これだけ見ても正体がわからないため，ひとつひとつ実際にウェブブラウザで接続し，どんなページが表示されるか調べてみました。

その結果，これら見慣れないサーバ名は，プリンタなどの機器に組み込まれたサーバであることが判明しました。学外から接続してみたわけではないため，学外からのアクセスが制限されているかははっきりしませんが，少なくとも他の支線から見えるようになっている機器が多数ありました。プリンタの設定がまるみえなだけでなく，中には設定の変更が可能そうな機器もありました。[6]

見つかったサーバの中で数が多かった物をいくつか紹介します。

- Apache
  - Apache Software Foundation開発のウェブサーバ
  - `http://httpd.apache.org/`
- Microsoft-IIS

[6]大きな声では言えませんが「再起動」のリンクをクリックしてみたらなんの確認もなくいきなり再起動がかかってしまった機器もありました。

  - Microsoft Internet Information Server
  - `http://www.microsoft.com/japan/products/iis/`
- JC-HTTPD
  - silex technology 社のプリンタサーバに内臓される組み込み用ウェブサーバ
  - `http://www.jci.co.jp/japan/support/index.html`
  - プリンタ外付け用，プリンタ内蔵用 (Canon・EPSON) 各種
- Spyglass_Microserver
  - Spyglass 社の小型軽量組み込み用ウェブサーバ
  - `http://www.spyglass.com/`
  - NEC Multiwriter，XEROX Phaser 等のプリンタ
- Allegro-Software-RomPager
  - Allegro Software 社の組み込み用ウェブサーバ
  - `http://www.allegrosoft.com/rpproduct.html`
  - Extreme Summit(ネットワークスイッチ)，EPSON プリンタ，APC(インテリジェント電源) 等
- AnWeb
  - フリーの Windows 用ウェブサーバ
  - `http://www.st.rim.or.jp/~nakata/`
- Web-Server・Web Server
  - 素性不明 (RICOH 製?)
  - RICOH プリンタに組み込み
- PRINT_SERVER_WEB
  - 素性不明
  - CANON LASER SHOT 専用プリントサーバ NetHawk に組み込み
- ZOT
  - Zero One Technology 社のプリントサーバ組み込み
  - `http://www.01tech.com/index1.htm`
  - Planex などに OEM されている
- Microsoft-PWS
  - Microsoft 社のウェブサーバ (Personal Web Server・Peer Web Service)
  - IIS の前身? サポートは既に無し
  - Windows 95 などで動いている
- AppleShare

- Apple MacOS 用商用インターネットサーバソフトウェア群
- http://www.apple.co.jp/applesshareip/

学内 LAN ではこれ以外にもさまざまな種類のサーバが稼働していました。どちらかというと，PC やワークステーションで動作するサーバの方が種類が多く，管理者の趣味・嗜好によってソフトウェアが選択されているのがわかります。それに対し組み込み用サーバは導入した機器に入っているソフトウェアがそのまま使われるため，それほどバリエーションは多くありませんでした。

4.2 サーバの内容

8月 23 日に発見された全てのサーバ 825 台に対して，実際にウェブブラウザでアクセスし，その内容を目視で確認しました。確認時期が最初の調査からだいぶ遅れてしまったため，接続できない機器が 87 台ありました。連休中だったため，プリンタなどは停止していたと思われます。残りも目視による判断のため分類は大雑把ですが，だいたい以下のような内容になっていました。

- 九大関係公開用: 約 300 台
- プリンタ関係: 168 台応答・約 40 台電源断 (サーバ名から判断)
- 初期ページ放置: 83 台
- その他
  - ユーザ認証要求のみ
  - 内輪向け (ウェブメールなど)
  - ファイル一覧が出る
  - 空

この中で「初期ページ放置」というのは，IIS での「工事中」ページや，Apache の「It worked!」など，サーバをインストールした時に自動で設定されるトップページが表示されたサーバを表しています。これらのページを返すサーバは，入れて動かしただけで放置されている場合が多く，セキュリティ上危険な可能性が高いと考えています。

4.3 セキュリティについて

今回，サーバの種類を調査した時に，セキュリティホールに関する情報が出ていないかも調べました。しかし，Apache や IIS のようなメジャーなサーバ以外では，そ

れほど多くの情報は得られませんでした。今の所，プリンタなどの組み込み系サーバの動作を乗っとって悪さをするような人はあまりいないか，見つかっていないようです。組み込み機器はCPUの種類もまちまちで開発環境も一般的で無く，そのような攻撃ツールを開発するのは難しいのかもしれません。

しかし，プリンタなどでサーバが動いているためにプリンタを利用したユーザのユーザ名が漏れていたり，またパスワードの設定がされていないために外部からの設定変更を許している機器がかなりあります。たぶん，利用者は自分が使っているプリンタでウェブサーバが動いている事実すら知らない場合が多いのではないでしょうか。あるIPアドレスがついた機器でウェブサーバが動いているかどうかは，URLにIPアドレスを指定してウェブブラウザでアクセスすればすぐわかるので，確かめてみた方がよいと思います。もしその機器でウェブサーバが動いているとわかり，誰もそれを必要としていないなら，安全のためサーバの機能は止めてしまった方がよいでしょう。

もっと悪い例としては，ウェブブラウザ経由で管理者権限でアクセスできるネットワーク機器が数台見つかっています。すなわち，学外からそのネットワーク機器を操作して，その機器に接続しているネットワークを遮断したり，パケットを操作できるおそれがあります。

よほどのことがない限り，プリンタなどの機器の情報を支線の外から見る必要はないはずです。必要のないサービスは止める，というのは何もワークステーションやPCに限った話ではなく，プリンタなどの機器にも必要な考え方であると言えるでしょう。

5　おわりに

本稿では，2002年7月と8月に行なわれた学内ウェブサーバ全数調査の結果を元に，学内LAN上で稼働しているウェブサーバの種類とその内容について紹介しました。

今回の調査で，学内で利用されているサーバはApacheが大多数を占めており，Microsoft IISは予想よりかなり少ないことがわかりました。CodeRedやNimdaによる大攻勢によってIISの利用を諦めた管理者がかなり多かったのではないかと考えています。Apacheについては，支線LAN管理者へのメール連絡によってある程度最新版への更新をしていただけましたが，やはりそれだけでは不十分で，古いままのサーバも依然として残っています。サーバの返すバージョン文字列を収集するだけでは，セキュリティホールの調査としては不十分であることもわかりました。

また，同時にウェブブラウザでアクセス可能なプリンタ等の機器がかなりの数発見されました。これらの機器は直接セキュリティホールになるという訳ではありませんが，トラブルを未然に防ぐという意味ではあまりよい状況ではないように思います。ウェブに関してだけ言えば，ウェブブラウザを使って簡単にサーバの存在を調べられますので，不審に思ったら試してみるのがよいと思います。たまにはプリンタなどの

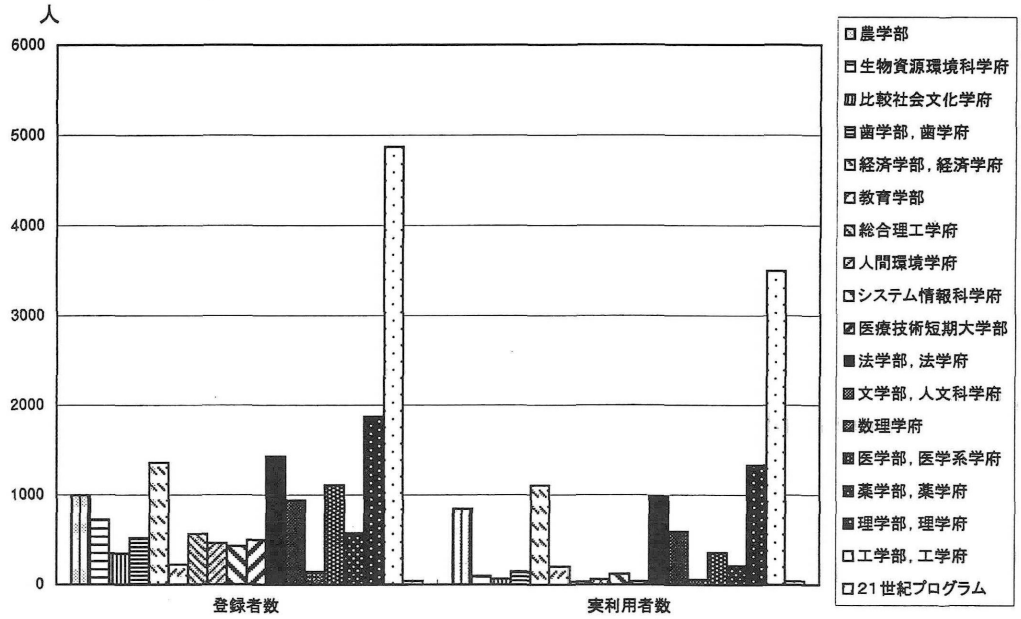
取扱説明書に目を通してみるのもよいでしょう。

センターではこれ以降全数スキャンによる調査は行なっていませんが，効果が限定的であるとしても，対策を進めるためには定期的な調査が必要だろうと考えています。ただ，今回はかなりの部分を手作業で行なったため効率が悪かったという問題もあります。自動化を進めれば，定期的な調査により傾向の変化を掴むこともできるようになるでしょう。また，ウェブサーバ以外のサーバ (メールサーバ，DNS サーバ等) についても，同様な調査をする仕組みを用意する必要があると考えています。

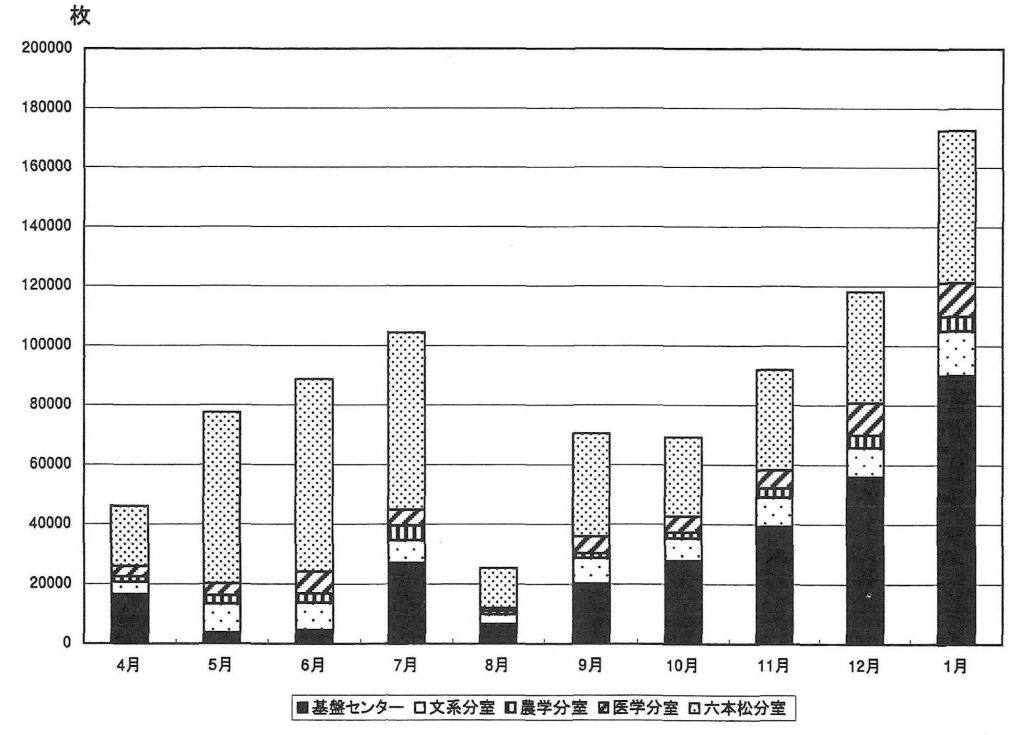
調査によって問題点が発見されたとしても，これを解決するには各支線 LAN 管理者，および利用者の協力が不可欠です。センターとしても，電子メールやウェブ，講習会などを通じて，ユーザや管理者への情報提供，啓蒙活動を進めて行きたいと考えています。安全で快適にネットワークを利用できるようにするため，今後とも御協力をお願いします。

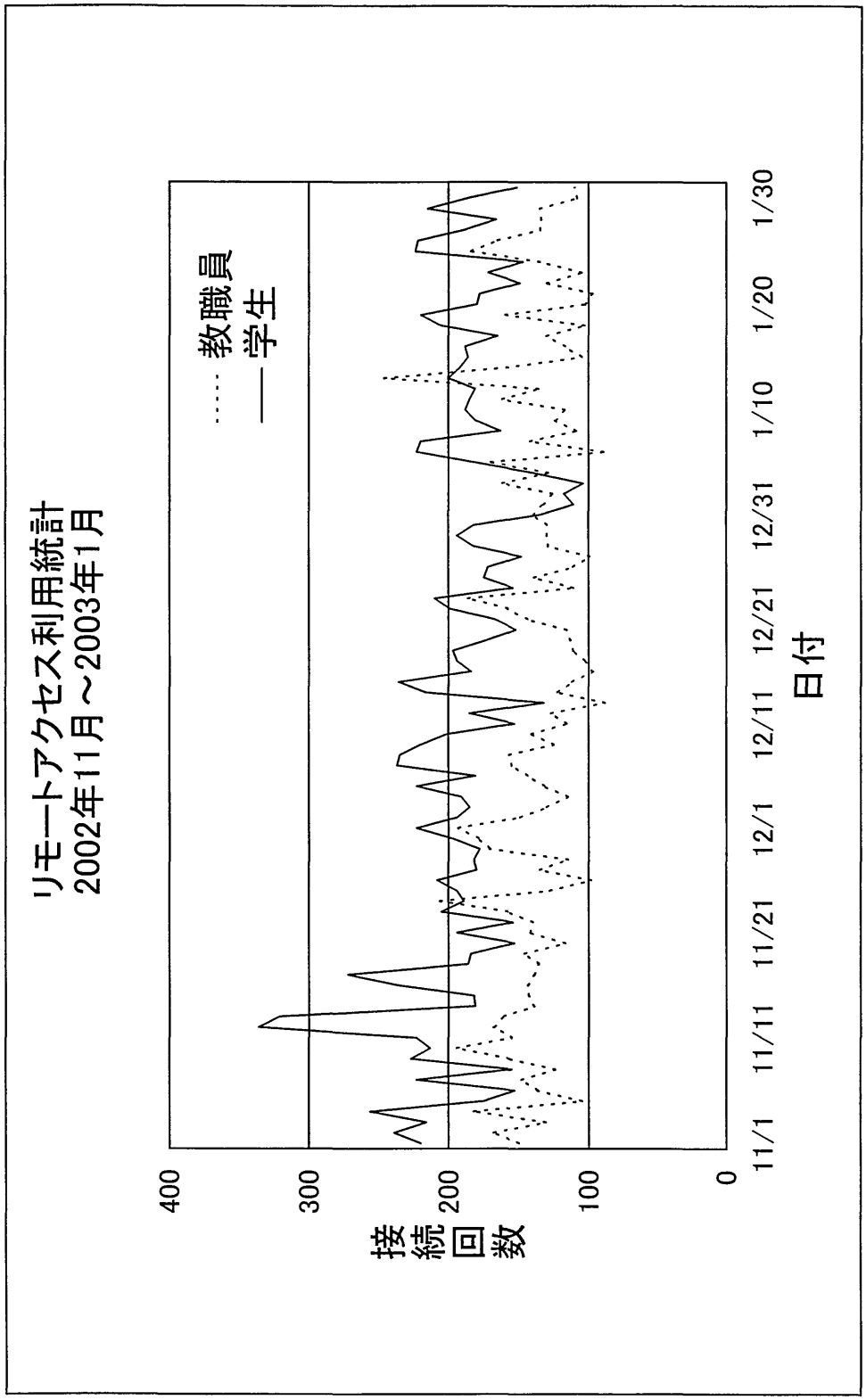
平成14年度教育用システム統計

1．学部等別登録者数および実利用者数（平成14年4月～平成15年1月）



2．月毎分室別のプリンタ出力状況（平成14年4月～平成15年1月）




リモートアクセス利用統計
2002年11月～2003年1月
教職員
学生
接続回数
400
300
200
100
0
11/1
11/11
11/21
12/1
12/11
12/21
12/31
1/10
1/20
1/30
日付

人　事　異　動

○平成１４年１２月３１日限り退職

研究部　技術補佐員　　渡　邊　礼　子

○平成１５年１月１日付け採用

研究部　技術補佐員（パート）上　村　利　香

○平成１５年２月１日付け教官の部門換

研究部　助教授　伊　東　栄　典　　学術情報メディア研究部門から

ﾈｯﾄﾜｰｸｺﾝﾋﾟｭｰﾃｨﾝｸﾞ研究部門へ

編　集　後　記

博多湾の人工島計画が進められています。将来は、ここに港湾施設、住宅、研究・開発施設などを建設するそうです。雁ノ巣レクレーションセンターと箱崎ふ頭の間を知人の車で何度か通り抜けたことがありますが、それなりに眺めがよく、短い時間で往復することができます。健康の為か、ジョギングをしている人や散歩をしている人を見かけます。走るにしても、歩くにしても、いい場所なのかもしれません。

しかし、博多湾は東奥部にある和白干潟が渡り鳥の中継地になっており、これらの野鳥を支える底生動物・魚類・植物が豊富であること。また、百万都市に残された貴重な環境教育の場、市民の憩いの場、水質を浄化する自然の浄化槽との声もあり、人工島計画は工事前から干潟とその周辺の環境に悪影響を及ぼすと指摘されていました。

さらに、最近ではケヤキと庭石の購入を巡って市議会で委員会が開かれるなど何かと問題は多いようですが、それは頭の片隅に置き、時間がある方は一歩足を踏み入れてはいかがですか。ひとときの安らぎになるかも。　(Y.I.)

現在、あるホームページの更新作業に取り組んでいて、その一環として、「文献検索のフローチャート」なるものを試行的に作成しました。この「文献検索のフローチャート」の元は紙媒体（A３のものをA４でプリントアウト）ですけど、これをこのまま html 化または PDF 化したら、一画面での表示字数が多く、利用者の方には見づらいものになりそうです。このような理由により、今回、「フローチャート」はシンプルなものになっています。実際、公開する際には、見栄えが変わることはありえますが、今のシンプルさは保ちたいと思っています。

この「フローチャート」の特長は、ある個所をクリックすれば、別のウィンドウが開き、そのウィンドウに各種文献検索データベースへのリンク機能を持たせたことです。つまり、「フローチャート」は、データベースへのナビゲート機能を果たすことができます。

いずれ、「フローチャート」を使った方が、データベースを使って必要な文献を探し出し、レポートや論文の作成に役立てていただくようになればありがたいです。

話は変わって、先日『学内版向け広報』に原稿を書きました。この原稿を書くように言われたのは 11 月ですけど、そのときは、共著で書くようになっていた『大学〇〇〇研究』（雑誌）の原稿が仕上がってませんでした。この原稿は数度も書き直しを余儀なくされ、最終的には数ページも削減されました。また、原稿を書くのかと思うと、気が重くなりましたが、なんとか書き上げました。幸いなことに、今回は書き損じが少なく、修正個所が少ないようなので、ほっとしました。この原稿は某社のワープロソフトで作成し、その中に表を入れていました。原稿をチェックされたところ、表のフォントを変更するよう指示があったので、フォントを変更したら、ページが１ページ減りました。私が書く文章は、ページが減るようになっているようです。

ちなみに、この『大学〇〇〇研究』の同じ号には、私と同じ職場の方も原稿を書いています。内容はともかく、文章のレベルを比較されるとどうでしょう？　(M.O.)

九州大学情報基盤センター広報
Vol. 3,　No. 1
平成 15 年 3 月　発行
編集　九州大学情報基盤センター
広報委員会
印刷　松隈印刷株式会社