不要になったものが放出された．人手は筆者自身で，持ち合わせたスキルは数年前にやった技術職員研修で FreeBSD をノートパソコンにインストールして見た程度．つまり，今から考えるとこれで安全が買えたのかという問いには，明確な回答はきない．

4．ネットワークの設計

1）パソコンの１台にネットワークカードを増設し，Linux のカーネルに標準装備されている NAT（Network Address Translation：IP masquerade）を利用して，ファイアウォールとする．さらに DHCP サーバとする．プライベート IP はパソコン，WS，ネットワークプリンタで必要数+αの IP を用意．

2）いま１台は外部向け各種サービス（DNS，FTP，WWW，Mail）サーバとする．

3）パソコン用のファイルサーバとプリンタサーバの機能を samba サーバとして１のパソコンに持たせる．

4）外部に置くサーバへの攻撃を想定し，各種サービス（DNS，FTP，WWW，Mail）サーバのバックアップのマシンを用意する．

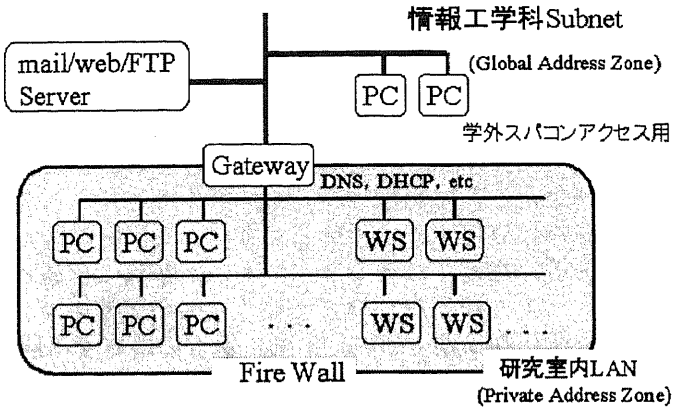

Fig. 1 研究室新ネットワークの構想

5．実際の作業

5-1　OS の選定．

情報収集の段階では，セキュリティに強いのは，FreeBSD と SlackWare という事だった．FreeBSD は試験インストールでどうしても VGA 以上の画面設定が出来ず断念し，SlackWare は関係資料の少なさで諦めた．結局書店で今回の作業の 80％を網羅するような解説本を発見して RedHat Linux を用いた．しかしこのことが後に問題を起こすことになった．その後バックアップマシンの立ち上げに Mac を使用することになり，ここには同系統の Vine Linux for PPC を用いた．

5-2　UNIX のインストール

PC-UNIX は潰してもいいパソコンとやる気さえあれば，最近は日本語のインストーラも整備されインストール自身は易しい．ネットワークの設定も指示通りで問題ない．追加するネットワークカード（以下 NIC）も自動認識された．インストール時に各種サーバ，ワークステーション，カスタムインストールの選択肢があるが新しいバージョンなら各種サーバでシステムを構築し，不必要なサービスを後で切った方が簡単である．

5-3　UNIX の環境設定

新設サーバは外部に接続する通信端末としても使うので，X-Window をはじめ日本語表示やソースやバイナリの取得のための Netscape，ftp の専用ツールなど，一通りの環境設定を行った．学生全員にアカウントを発行した．これらとの接続は SSH（Secure Shell）を用いている．

5-4　ネットワークサービス詳細

各マシンに実装したアプリケーションは以下のようである．

NAT	各カーネルに標準で付属する機能である IP Maquarade を使用．プライベート IP による独自ドメインを設定．プライベート IP を持つ研究室内のパソコンからの要求を自分の IP に変換して外部に発信し，要求に対する返信をプライベート IP に変換する．外部からは研究室内のパソコンは見えない．
DHCP	研究室内のパソコンに接続順に自動でプライベート IP を配布する．
MTA	当初 sendmail を立ち上げたが，その後 postfix に変更した．設定ファイルの簡便性には驚いた．
DNS	従来の SunWS から引き継ぐ．不必要な IP をデータベースから削除．
http	apache を使用した．パスワードによる閲覧制限のためとアクセスカウンタのために CGI と SSI の使用を許した．
ftp	wu-ftpd を当初採用した．その後セキュリティホールが確認されたので proftpd に変更．今回を機に anonymouseFTP を廃止した

6．ネットワーク改編の経過

2000年12月

パソコンの準備，PC-UNIXの試験インストール．

2001年1月～3月

各アプリケーションインストール，動作確認．研究室Web移設，DNSの書き換えが順次行われ新設のwebサーバが外部から見えるようになる．

2001年4月　ファイアウォール，DHCPサーバ稼働．sambaも稼働させる．同時期に学部で情報コンセントの増設工事があり，この際各研究室の各コンセントのうち，特定のものをグローバルIPから切り離して，相互に接続してもらった．このためファイアウォール下で部屋を跨いだ接続が簡単かつスマートに出来た．

実際に使用してみると，windowsマシン相互でファイル共有するのに時間がかかることが判明．ほとんど通常の立ち上げでは接続できない状態が続いた．プリンタサーバとしてもうまく動かなかった．調査の結果，windowsマシンのファイルサーバを従来やっていたwindows2000マシンの機能とぶつかっているらしかった．このマシンは常時立ち上げしており，やや古い機種なので，使い潰す方針でプリンタサーバともにこのマシンをファイルサーバとし，結局sambaを停止した．

Macのファイルサーバ機能のnetatalkは問題なく稼働している．また，Macはまったく設定なしでプリンタも共有できた．

2001年5~6月　メールサーバの更新を計画するが，学生の就職活動時期と重なり，夏以降に延期する．

2001年8月　試用中の外向けサーバと囲い込みが遅れたWS（？）が外部の通信の踏み台にされる事件が起こる．新潟大学情報処理センターで運用されているトラフィック監視ツール(MRTG)によれば，当日は図2のようであった．学部のネットワーク管理者からは3Mbyte/secのトラフィックは異常であり，

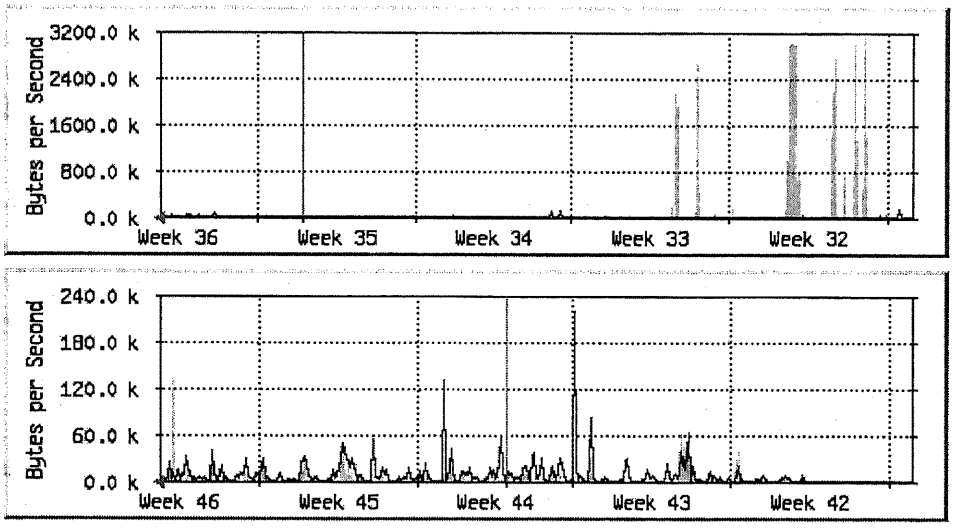

Fig. 2
新潟大学情報処理センターのMRTGの記録
灰色：IN
実線：OUT

上段は7/1から7/14に異常なパケットが流れている．
下段は10週間後，ほぼ通常の状態．

パケットのほとんどが京都の商用プロバイダ向けであった．調査の上当研究室のマシンを特定し，当日は休日だったので，シャットダウンできずネットワークから切り離し（ケーブルを抜いた）したと連絡を受けた．特定されたIPの1台は今回新設したLinuxマシン，もうひとつはAIXが稼働するIBMのWSが使用していた．

2001年9月　8月の事件でネットワーク管理者から踏み台にされたマシンの状態の報告を求められた．しかしながら/var/messagesなどの調査では痕跡は確認できなかった．そこでマシンの脆弱性を知るためネットワーク点検ツール Saint-3.0（http://www.wwdsi.com/saint）をインストールした．うまく動いたので早速被害を受けたマシンを点検した．結果を図3に示した．

2001年/10，11月

やや古いWSをファイアウォール下で使用する際にIPの動的配布が不可能なことが判明する．さらに調査の結果SUN以外のWSは導入当時業者によって環境設定が行われ，必要のないサービスのデーモンが稼働していることが判明．関連情報が少ないIBMやHPのWSはスーパーユーザ（学生）の世

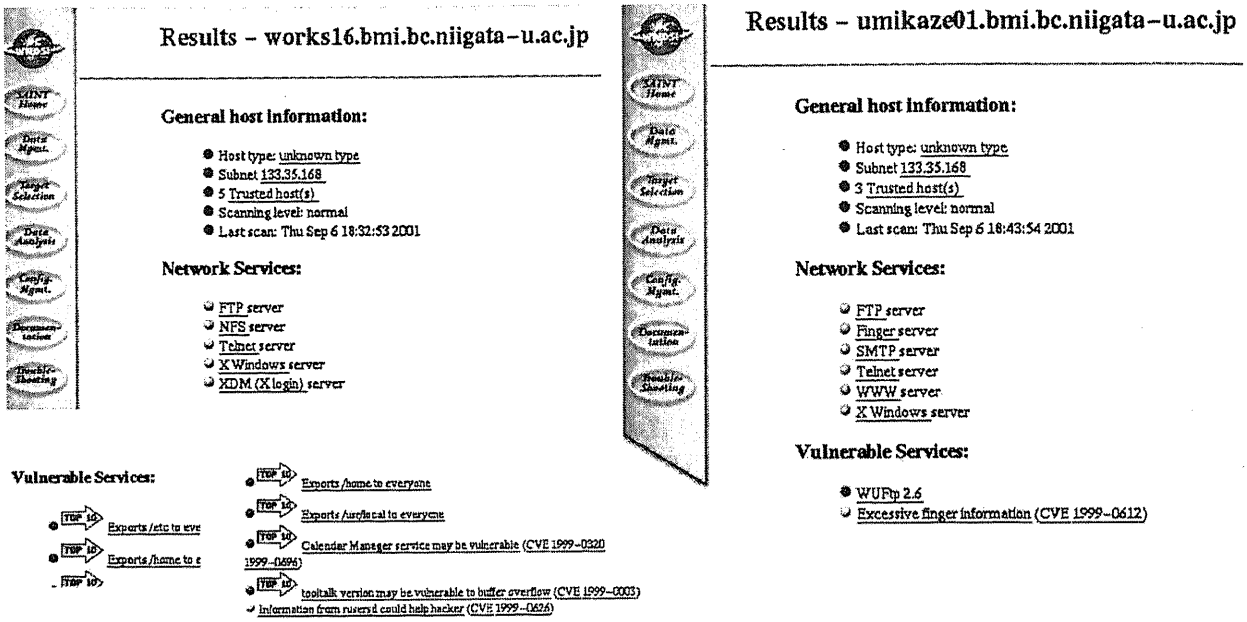

Fig. 3　2001年7月，踏み台にされたマシンの saint による点検結果．Vulnerable Services 以下の項目が問題の項目で濃い色がより脆弱性が高い．左がやや古い IBM の WS，右は今度新設したマシン．このバージョンの wu-ftp は後にセキュリティホールの存在が指摘された．

代交代の中で管理が放置されたようだ．sendmail や apache を停止し，さらに停電後などによる再起動時に立ち上がらないように設定する．ドメイン名や IP アドレスの変更は NIC の名前さえ分かれば比較的簡単だが，過去の研究上のプログラム資産を持つ WS の設定変更は最悪のケース（起動しなくなる）を想定して，バックアップを慎重に行う必要がある．今回から従来の DAT テープへの保存から Windows パソコンを介して CD-R へ変更した．特に問題はないようだ．今後 PC-UNIX 上で使える CD-R の登場を待ちたい（もうあるか？）．

2001年/12月

メールサーバを稼働させる．DNS の書き換え後2週間程度待つが外部からのメールが届かない．外部の DNS で mailhost.bmi.bc.niigata-u.ac.jp として名前解決できない．調査の結果，当研究室の所属するサブネットのルータの設定で，新設したメールサーバの IP アドレスがメールサーバ用に許可されていないことが判明．許可された IP アドレスに変更して稼働．起動後不正中継チェックサイト等を使って点検している．

2002年/1月

教官の間で学生がインターネットを資料検索以外の用途に無制限に使用することの是非が問題になり，コアタイム？（9時から17時）のインターネット接続マシンの制限の検討を依頼される．telnet, ftp や windows のファイルサーバやプリンタへのアクセスを残し，firewall 内のマシンに対して 80 ポートへのアクセスを制限することとし，以下の設定をした．具体的には NAT サーバに squid（プロキシーサーバ）を立て，透過プロキシとして外部の http サーバへのアクセスを禁止し，Linux のコマンド ipchains（あるいは iptable）で 80 ポートへのパケットを squid へフォワードさせている．時間の設定は crontab でコントロール，時間の正確さを確保するために NTP（Network Time Protocol）をインストールした．学生には非常に評判は悪いが初期の目的は達している．

2003年/1月

ほぼ一年を経過するが，特に問題は起きていない．この間，apache にパッチを当てた．サーバに用いている RedHat Unix のバージョンは Ver.8 となったので，更新が必要である．

7．この報告をめぐる現在の評価

現在，一般家庭に ADSL などの高速インターネット回線が急速に普及している．このことは各家庭で複数台のパソコンを回線に常時接続する状況という点で今回報告した内容と類似している．いわゆるブロードバンドルータをいわれる商品は，今回立ち上げたサーバのうち，NAT と DHCP サーバのことである．このブロードバンドルータは機種にもよるが価格は1万円を切っており，設定も web 上で行うことができる．したがってこうした使い方では，今回の報告のアドバンテージは時間を費やすだけマイナ

スである．ただ，UNIX ベースでたとえばログインシェルを使って外部のスーパーコンピュータ等と長時間接続する，あるいは数十 MB におよぶ巨大なファイルを FTP で授受するということであれば意味がある．なぜなら家庭向けのブロードバンドルータにおける NAT の IP 変換テーブルは通常 10 分程度で消滅してしまうからである．さらに言えば，処理速度（多くは感覚的）の問題だけで廃棄されるやや古いパソコンの再利用という地球資源の有効活用という面もある．

8．まとめと今後の課題

ネットワーク保守管理は常にセキュリティホール等の情報を集めて必要なら，プログラムの更新が必要である．今回のように場合によっては研究室外への悪影響がある以上，ネットワーク管理は学生任せには最早できない．また，ネットワーク自体基本的に問題がないのが当たり前で，問題があれば時間が取られ苦労の多い割には，冷や汗の出る仕事である．技術職員個人としてはこの関係のスキルも重要だと考えるが，こうした事を研究室単位で維持管理するのは非効率である．学科単位，学部単位で専門家を配置するべきかも知れない．

参考文献
1） サーバ構築研究会：“Red Hat Linux ネットワークサーバ構築ガイド” 秀和システム
2） “Software Design Linux Issue すみからすみまで linux ～テクニカル編” 技術評論社
3） 山口和紀他：“The Unix Super Text（上），（下）” 技術評論社

＊しかし，むしろオンラインで http://www.linux.or.jp からインストールする項目に従って資料を集めるのが効果的である．強力な検索システムがあり，過去の ML，FAQ の記録も検索できる．マニュアルも翻訳されていれば日本語で手に入れる事が出来る．