共通計算機システムのファイアウォール化

名古屋大学 工学部・工学研究科 技術部
○鬼頭 良彦、高田 昇治、藤原 文治、福森 勉

１．はじめに

インターネットの発達と普及に伴い、名古屋大学においても不正アクセスの報告、セキュリティ対策の通知等が頻繁に行われるようになってきた。電気系教室には専攻関係者が自由に利用できる共通計算機システムがあり、日々セキュリティ対策に追われている。しかし、設置台数が６０数台と多いため、通知されたセキュリティ対策への対応が遅れがちとなってきた。また、計算機の中には学生実験で利用する外部接続用ボードの関係上ＯＳのバージョンアップ自体ができないものもあり、セキュリティ上危険なものが存在した。

そこで、共通計算機システム運営委員会で検討した結果、これまでの共通計算機システムでは、ユーザーの利便性を優先してきたが、近年の情勢を考慮するとセキュリティ対策は不可欠な要素であるため、今回ファイアウォール化することによってセキュリティの向上を図ることとなった。ファイアウォール化によってセキュリティ対策を行う計算機を集中化するとともに共通計算機システムですでにファイアウォール化されているドメインとの統合化を行ったので報告する。

２．ファイアウォール化への方針

図１にファイアウォール化前の電気系ドメイン nuee.nagoya-u.ac.jp（以下、nuee）の状況を示す。nuee には約 290 台の計算機が接続され、研究室によっては独自にドメインやファイアウォールを立ち上げている所もある。また、共通計算機システムは nuee 内のどの計算機からもアクセスが可能である。nuee の共通計算機システムは大規模集積システム設計教育研究センター中部支部（以下、VDEC）の計算機システムドメイン vdec-nagoya.nuee.nagoya-u.ac.jp（以下、vdec-nagoya.nuee）と学生実験及び研究用計算機システムドメイン echo.nuee.nagoya-u.ac.jp（以下、echo.nuee）の二つが存在する。vdec-nagoya.nuee は東海地区の VDEC ユーザーのライセンスサーバで、すでにファイアウォール化されている。今回ファイアウォール化を予定している echo.nuee は nuee のサーバーである nuee server のアカウント情報やファイルサーバを利用している為、nueeserver も一緒にファイアウォール下に置く必要があった。しかし、nuee server は電気系教室約 1400 人のメールや www サーバとなっている為、単にドメインのファイアウォール化でなく、nuee 全体の影響も検討する必要があった。そこで以上のことを考慮し、次の方針を立てた。

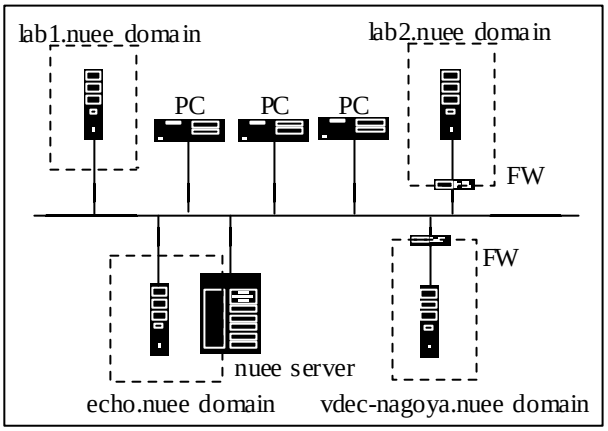

図１．電気系ドメイン(nuee)

- メール利用者に負担をかけないため DNS, SMTP,POP 利用時のサーバー名を変更しない。
- セキュリティ対策計算機集中化のため、FTP, TELNET の利用計算機を限定する。
- echo.nuee, vdec-nagoya.nuee クライアントではアカウント、ホームディレクトリを共通にする。
- WWW はファイアウォール内で www.nuee.nagoya-u.ac.jp,www.echo.nuee.nagoya-u.ac.jp の二つを立ち上げる。
- vdec-nagoya.nuee サーバは学外 VDEC 利用者のライセンスサーバの為、IP 等の変更をしない。

３．ファイアウォールの構成

図２に共通計算機システムのファイアウォール化の構成を示す。ファイアウォールは nueeserver で行い、

vdec-nagoya.nuee クライアントの利用者もこの計算機から共通計算機を利用することとし、vdec-nagoya server は VDEC 利用者のライセンスサーバーと vdec-nagoya.nuee の DNS サーバーのみとした。また、nuee の DNS は nuee server が応答する。echo.nuee server は nuee のメール、nuee、echo.nuee の WWW サーバー、echo.nuee の DNS サーバー及び echo.nuee、vdec-nagoya.nuee クライアントを共通利用するための NIS、NFS サーバーとした。access server は echo.nuee、vdec-nagoya.nuee クライアント利用者が共通計算機を利用するため nuee server に接続時の応答計算機として TELNET、FTP サーバーとした。共通計算機利用者は accessserver に接続後、利用したい計算機に telnet で移動する。サーバーに使用した計算機は nueeserver が Sun Blade100、OS は Solaris8、echo.nuee server、vdec-nagoya.nuee が Sun Blade1000、OS は Solaris8 である。accessserver は Sun SparcSS-5、OS は Solaris2.6 である。

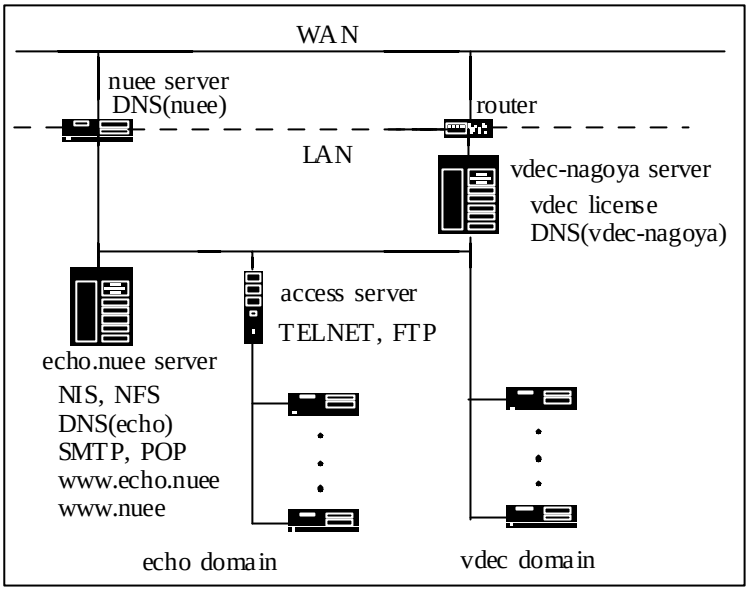

図２．共通計算機システムのファイアウォール構成

４．ファイアーウォール化の為のアプリケーション

図３にファイアウォール化の為にインストールしたアプリケーション[1] [2]とパケットの流れを示す。アプリケーションの詳細についてはインターネットや雑誌等を参照して頂くこととし、主に基本部分と苦労した点を中心に報告する。

4.1 IPFilter

図中の nuee server がファイアウォールの計算機にあたり、WAN net が外向き、LAN net が内向きのネットワークボードである。ファイアウォールに使用した計算機は 64bit カーネルで動作するため、IPFlter をインストールする際にこれまでのように gcc でコンパイルして使用するということができなかった。現在でもまだ 64bit 用 gcc はまだ出回っていないようであるが、幸いにも IPFilte は 64bit 用バイナリファイルを公開しているサイトがあったためそれを利用した。

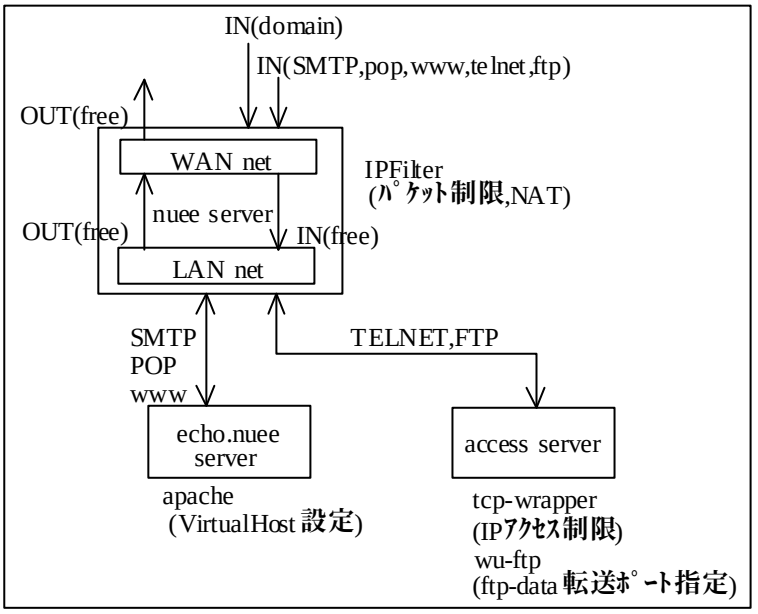

図３．ファイアウォール時のパケットの流れ

IPFilter は ipf.conf でパケットの制限、ipnat.conf で WAN と LAN とのアドレス整合及び通過したパケットの応答計算機の設定ができる。今回のシステムでは LAN から WAN へは全てフリーとし、WAN から LAN へは SMTP,POP,WWW,TELNET,FTP のみ通過させ、nuee ドメインの DNS の問い合わせには WAN 側で応答するようにした。LAN 側の応答計算機はアクセス時の危険度に応じて分散するのが理想であるが、現時点では echo.nuee server と accessserver の２台で対応している。

IPFilter 以外の設定で Sun Blade に関してはハードウェアチェックサムと IPFilter の NAT との間で不具合

が生じるようなので/etc/system に setip:dohwcksum=0 の１行を追加した。

4.2 apache

WWW に関しては図中の echo.nuee　server が応答する。旧システムでは nuee ドメインと echo.nuee ドメインの二つのホームページを公開していた。今回この二つのサーバーをファイアウォール下に置いたことによってファイアウォール内で二つのホームページを表示しなくてはならなくなった。しかし、IPFilter を通過する際は 80 番のポート番号だけで識別され、nuee ドメインか echo.nuee ドメインかの区別ができない。その為、ホームページに関しては nuee ドメイン、echo.nuee ドメインの問い合わせを１台の計算機で応答させるため、apache のバーチャルホストを利用して二つのホームページを表示させることにした。設定としては apache の httpd.conf ファイルに二つの WWW サーバ名とそのデータディレクトリの記述を行った。

4.3 tcp-wrapper

telnet や ftp は図中の access　server が応答する。telnet や ftp でのアクセスは危険度が高いため、tcp-wrapper で IP アドレスによるアクセス制限を行った。設定としては/etc/hosts.deny に全ての IP アドレスをブロックするよう記述をし、/etc/hosts.allow に接続を許可する IP アドレスを記述する。

4.4 wu-ftp

FTP は通常 20、21 番ポートを使って行われるが、ファイアウォールを立ち上げている研究室やパソコンの FTP ソフトではデータ転送にパッシブモード(PASV)が使われていたりする。パッシブモードは FTP 接続時にサーバーが任意のポートを割り振ってデータ転送を行おうとするため、途中にファイアウォールが存在する場合は接続ができない。これに対応するには FTP サーバーにパッシブモード対応のソフトをインストールし、そのソフトでポート番号の制限を行い、IPFilter に記述する必要がある。ポート番号の制限を設定するには ftpaccess ファイルに使用するマシンとポート番号を記述する。今回のシステムでは 10001 ～ 10010 番ポートを使用した。

例：
```
passive   address    133.6.xxx.xxx    0.0.0.0/0
passive   ports      0.0.0.0/0        10001 10010
```

５．まとめ

共通計算機システムのファイアウォール化への移行にあたり、電気系教室のサーバー移行が付随してきたため、一般ユーザーへの影響を最小限に抑えることが移行時の重要課題であった。特にメールは長期間停止させることはできないため、ファイアウォール化を行うと共にサーバーも利用可能な状態にし、その後 echo.nuee ドメイン、vdec-nagoya.nuee の統合等の作業を順次行った。今回のファイアウォール化は一システムのファイアウォール化と違い、やや変則的な条件であったが無事乗り越えることができた。

まだ課題はいろいろ残っているが、セキュリティ面では対策をする計算機が集中化できたことによって安全性も上がり、また、懸念されていた OS のバージョンアップ等の問題もクリアされた。

６．今後の課題

現段階では最低限の移行が済んだばかりなので、今後は WWW サーバーの分離、スレーブマシンの設定、ログの整備、バックアップの整備等を検討し、より安心で安全、安定したシステムにする必要がある。

参考文献

[1] 内田 法道 ”はじめてのファイアウォール” 技術評論社

[2] 技術評論社第 2 編集部編 ”ファイアウォール＆ネットワークセキュリティ” 技術評論社