防火壁によるネットワークセキュリティ確保における サービス水準の確保

江尻博信　川合英俊
いわき明星大学

概要

インターネットユーザーが爆発的に増えつつあることから、IP接続に伴うネットワークセキュリティの確保が重要になる。その対策として防火壁マシン(FireWall Machine)を介在させて、LANをサブネットに分断すると、内外のユーザに対して、十分なネットワークサービスの水準を維持できなくなる。そこで、不特定の外部ユーザに提供する匿名サービスについては、サーバを片方のサブネットに集中し、もう片方のサブネットが提供するサービスについては、サービスプログラムが防火壁マシンを通してサービスの転送を行うこととした。ここでは、防火壁マシンを実験的に実現し、サービス限定やサーバの再配置を試み、各種設定ファイルの取り扱いを検証したので、その結果を報告する。

1. はじめに

LANを外部ネットワークと接続すると、リソースを共有できるという利点が生ずるかわりに、ネットワークを介して様々な機能を使い[1]、予期しない外部の他人が、LAN内コンピュータのリソースを読んだり書いたり実行する可能性も生じる[2]。ネットワークがインターネットのように広域大規模な場合には、不特定者のアクセスを拒む必要がある。

しかしその一方、不特定者のアクセスをただ機械的に拒むためにLANをネットワークから隔離するだけでは、匿名サービスのようなネットワークサービスを提供できなくなるばかりでなく、LAN内ユーザも外部に関するメール、ニュース、匿名サービス等のネットワークサービスの利用に障害を生じる。そこで、次の2つの視点からセキュリティを確保しながら、ネットワークサービスの種類ごとにサービス水準を設定したりサーバの配置を工夫して実験的に効果を上げたのでここに報告する。

1）サービスの質をほんのわずか低下させる。例えば紹介情報は、斬新性を半日ほど犠牲にしたり、遠隔ログインを二度手間にしたりした。

2）紹介情報のサーバを、LAN内の某所に無造作に配置せずに、経済性を犠牲にしてLANの前置部分に局在させた。

匿名サービスに関するデータベースの保守更新のためは、新しく設けた開発者ディレクトリの定期的複写機構を使った。

上記の方針に基づいて、メール、ニュース、WWW、匿名FTP、遠隔ログイン等のネットワークサービスの実装を試みた。このことから、防火壁マシンを設

"Service level keeping for insuring network security by the LAN Fire wall."
Hironobu EJIRI and Hidetoshi KAWAI　(Iwaki Meisei University)

けたことにより、実際に外部からの侵入を防ぐだけでなく、各サーバの配置とも関連させることができ、セキュリティが向上すると共にユーザに対するネットワークサービスの水準を確保できることが明らかになった。この結果は、ネットワークの更新時に応用できることが分かった。

2 種類別ネットワークサービスの維持

2．1 ネットワークサービスの形態

インターネットの拡大に伴ってネットワークサービスの種類も増加してきている、この実験では特に現在重要と思われる表1に示す8種類のサービスを取り扱った。

表1 ネットワークサービスの種類

種類	サービス内容	サービスの向き local Internet
メール	送信	→
	受信	←
ニュース	投稿	→
	購読	←
WWW	情報収集	→
WWW	情報提供	←
FTP	転送	→
FTP	資源提供	←
ログイン	外部マシンへ	→
ログイン	外部マシンから	←

これら8種類のサービスはセキュリティ上の理由で、次の3つに大きく分けることができる。

1）外部ユーザには提供しないサービス
．メール、ニュースのように外部ユーザが直接使えないサービス
．WWW、ＦＴＰ、rloginを内部から外部へ向かって使う場合。

2）外部ユーザに対する匿名サービス
紹介情報を発信するもので、WWW、ＦＴＰがある。

3）外部からLAN内マシンに対する遠隔ログイン
外部のユーザが、内部のマシンにログインし、LANのコンピュータ資源を使用する場合。

それぞれについて以下のような対策をとることとした。

1）外部のユーザが関わってはこないために、セキュリティ上は問題があまりない。そこで、従来と同じネットワークサービスの水準をユーザに提供する。

2）設定を誤った場合パスワードのファイルが見えてしまう等、セキュリティを低下させる恐れがある。そこで、LAN内ユーザの使用するコンピュータ資源から切り離されたコンピュータが独占的に、サービスを提供するものとした。

3）ユーザの認証という現在セキュリティ上重大な問題となっているところである。そこで、防火壁マシンには、ユーザの登録を行わないようにし、サービスを必要とする場合には、限られた期間だけ、事前に登録された必要最少人数に、サービスを行うこととした。

2．2 防火壁に伴うサービス水準の維持

IP forwardingを停止させるように防火壁マシンをLAN内に介在させることによって、このLANのセキュリティを向上させることができる。しかし単にLANを二つに隔離してしまうことになるために、内部のユーザだけではなく、サービスを受けていた外部のユーザにも、

ネットワークサービスを提供できなくなってしまう。

そこで、サーバの配置の変更をしたり、防火壁マシンに、サービスの内容にもとづいて、必要なときだけ、パケットのリレーを行わせることで、ネットワークサービスの水準を維持する。このときネットワークサービスのリレーを伴う種類のサーバは、外部と通信できなければならないため、防火壁マシン上に置く。

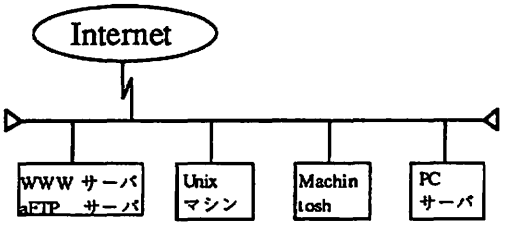

図1 従来のLANの形態

いわき明星大学の教育研究ネットワークであるIMU-NETでは、従来、図1のように、全てのマシンが一つのLAN上にあるフラットなネットワークであった。しかし、IP接続や、システムの入れ替えに伴って、セキュリティへの要求が高まったことから、防火壁を設けることとなった。防火壁は、一台のマシンによってネットワーク全てのマシンのセキュリティを確保できるものである[3]。

しかし、防火壁をただ単に設置した場合、内外のユーザにネットワークサービスを提供することができなくなってしまうために、図2のように、このLANを防火壁マシンで前置網とローカルネットの二つに分断する構成にし、内外のユーザへサービスを提供できるものとした。

内部のLANユーザは、ローカールネットの中で作業を行う。前置網は、外部ユーザへの紹介情報の提供のみを行い、ローカルネットのユーザはこれを使用しないものとした。

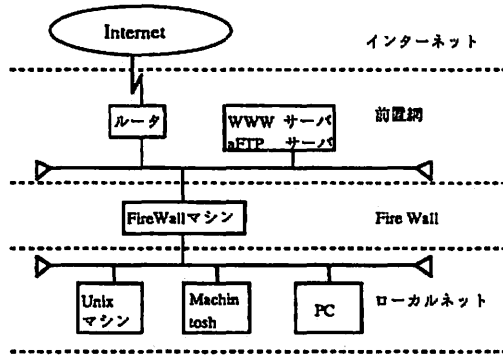

図2 防火壁を伴うネットワーク

防火壁マシンは、外部へのサービスを行うこともできる。しかし防火壁マシンは、セキュリティ上特に重要なマシンなので、問題を起こし得るものはここに置くべきではない。また、防火壁マシンへの負荷の増大を防ぎたいなどの理由から、WWW、FTP、など外部へのサービスは、前置網に設けられたサーバで提供することとした。

メール、ニュースなどの、ローカルネットワーク内のユーザに対するサービスは、防火壁マシンが、サービスを限定して、必要に応じてデータを内外にリレーすることとした[4]。

以上のことを念頭に置き、システムの入れ替えの事前に、防火壁マシンの有効性を調べる実験をした。

3 防火壁の実現

3．1 防火壁の実現とリレー設定の内容

防火壁には、ネットワークカードを2つ持つSUN のSparc Station 20を使用し、2つのネットワークカード間でIP Forwardingを行わないカーネルを作製し、防火壁マシンとした。この防火壁マシンによってLANは、前置網とローカ

ルネットワークに分割されたことになる。この時に、紹介情報のサーバは、前置網に置くべきものであるが、今回は、防火壁マシンの中に設置した。従来のネットワーク上に、防火壁マシンを作り、別のネットワークカードに新たにサブネットを接続する形で実験を行った。この場合、論理的に、従来のネットワークを、外部ネットと前置網、新しいサブネットを、ローカルネットと見ることができ、防火壁を通した外部への接続実験などは、従来のネットワークと新しいサブネットの間で行った。

図3に実験時のネットワーク配置を示す。

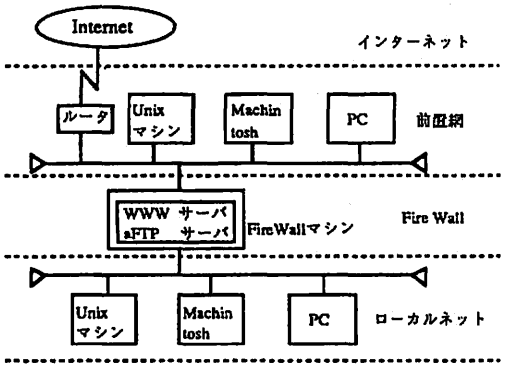

図3　実験時のネットワーク

メールとニュースについては、防火壁マシン上にサーバを配置した。

メールについては、外部からのメールは、一度防火壁マシンが受けて、ローカルネット内のそれぞれのユーザのホームマシンに配送する。内部からのメールは、防火壁マシンに集められ、そこから外部のネットワークに配送される。

ニュースは、防火壁マシンのニュースプールに記事が集まる。内部ユーザは、nntpを使って防火壁マシンのスプールからニュースの購読と、投稿を行うことができる。

ユーザは、従来ホームマシンに転送されてきたメールを読み、nntpを使ってニュースサーバからニュースの購読、投稿を行っていた。このため、防火壁ができても、もし必要ならばこれらのサーバが割り当てられているホスト名の変更に伴う設定を変更するだけで、従来と同じ操作でこれらのネットワークサービスを受けることができる。今回の実験では、メール、ニュースサーバであったマシンを防火壁マシンとしたために、ユーザは、サーバ名の設定の変更等はなにも必要としなかった。

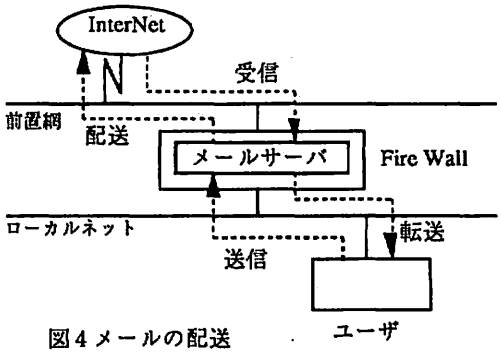

図4 メールの配送

WWW、FTP、rloginなどの内部から外部への要求については、その処理に伴うパケットの転送を代行するアプリケーションであるPROXYを防火壁マシン上に置き、それぞれのサービスごとにPROXYが内外両方向のIPデータグラムのリレーを行うこととした。（図5）。したがって、ユーザは、アプリケーションによっては、自動的に行ってくれるものもあるが、操作に先立って、防火壁マシンのPROXYを動作させてから、サービスを受けなければならないこととなり、手間が増えることになる。

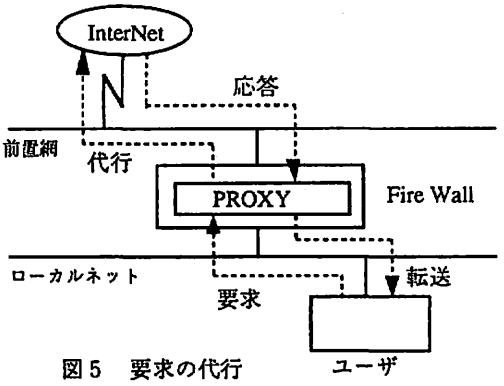

図5　要求の代行

ローカルネット内のマシンへの外部からのログインは、ログインを希望する人が、希望期間を、防火壁マシンの管理者に申告し、管理者は、その一定の期間だけ、防火壁マシンにそのユーザのアカウントが使える状態にしておく。またこの時に使うパスワードは、ユーザにあらかじめ登録しておいてもらった物を使うという方法によって、ユーザへ成り代わってアカウントの申請をすることを防ぐことができる。

外部から、ローカルネット内のマシンを使用する場合、使用者は、まず防火壁マシンにログインし、そこから目的のマシンに再度ログインすることで、ローカルネット内の各マシンを使用できることとなる（図6）。

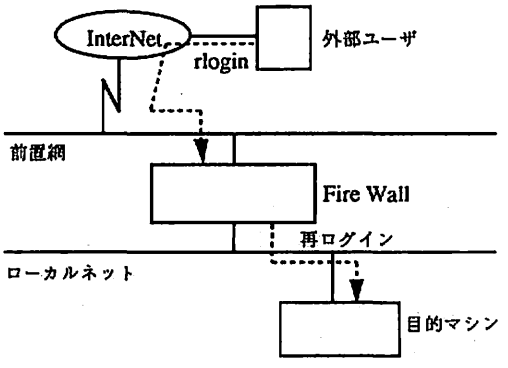

図6　ローカルネット内への外部ユーザのログイン

3．2　各サーバの配置と実現

実験時に、各サーバは、図7に示すように配置した。

1）　防火壁マシンの設置

二つのネットワークカード間で、IP Forwardingを行わないように、カーネルを再構築したに防火壁マシンを用意した。実際に、外部から内部が、内部から外部が見えないことを確認した。

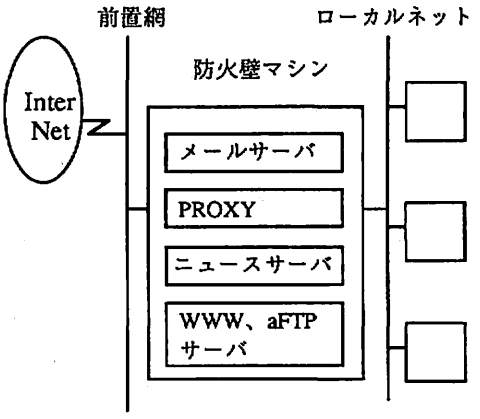

図7　サーバのLAN内配置

2）　メールサーバの設置

メールサーバは、防火壁マシンの中にsendmailを入れ、ローカルネットのメールサーバとし、外部からのメールをローカルネットに転送するように設定した。実際に問題なく外部とのメールの送受信ができることを確認した。

3）　ニュースサーバの設置

ニュースサーバーは、防火壁マシン上にインストールした。従来からニュースはnntpを使ってユーザが購読や、投稿をしていたために、ニュ

ースサーバのインストール時に、特に設定の変更を必要としなかった。実際にニュースリーダを使いローカルネットの中からニュースの購読と投稿ができることを確かめた。

4） PROXYの設置

PROXYについては、WWW、FTP、rloginのPROXY機能が含まれているDelegateを防火壁マシンにインストールした。実際にPROXYを使いネットワークサービスが受けられることを確認した。また、ネットワークを使う授業に対応するために必要となるPROXYのキャッシュ機能の有効性を確かめた

5） 防火壁マシンでのユーザの制限

防火壁マシンのユーザの制限は、調査の結果IMU-NETでは、20%以上の人が簡単に他人から憶測されるパスワードを使っていることが確かめられた。このため、ユーザが簡単なパスワードを使う傾向があり、ユーザ登録が、防火壁マシンにとっていかに危険であるかが再認識された。そこで、今回の外部からのログインの制限が有効であり、さらに今後防火壁マシンにユーザを作製する際、ユーザに推測されにくいパスワードを薦め、定期的にパスワードチェックプログラムを動かす、盗聴にも対応できるなど、安全性が高いユーザ認証法である、ワンタイムパスワードの導入等が必要になる。

4 前置網サーバの保守

4．1 グループによる紹介情報の保守

紹介情報の保守にあたっては、紹介情報サーバの管理者のもとに、情報提供を希望するユーザが、グループを作る。グループの各自が、紹介情報サーバにある、各自あてディレクトリの内容を間接的にでも更新できればよい。

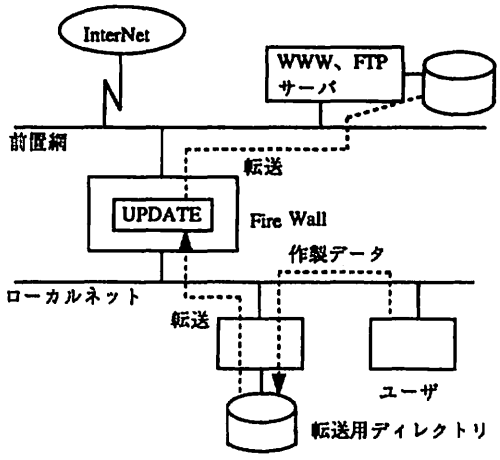

図8 紹介情報複写機能

前置網にWWW、aFTPなどの紹介情報のサーバを配置して外部ユーザに提供する場合、ローカルネット内のユーザは、防火壁マシンがあるために、紹介情報の作成や、更新を行えなくなってしまう。そこで、ローカルネットからユーザが紹介情報の保守を行えるようにするために、ローカルネット内に特定の転送用ディレクトリを設る。各自は、そこに紹介情報をおくだけとし、新しい情報を自動的に、前置網内にあるサーバの所定の位置に複写する機能を設けた（図8）。

紹介情報複写機能は次のようなものである。紹介情報の管理者が、特定のマシンに、紹介情報転送用のディレクトリを用意しておく。ユーザは作成した紹介情報を、そのマシンの転送用のディレクトリに置く。その更新された紹介情報は、防火壁マシン内にある、UPDATEスクリプトによって、前置網内にある紹介情報

サーバーマシンの所定のディレクトリに、転送用ディレクトリから転送される。転送を行うこの UPDATE スクリプトは、cron によって一日二回実行され情報の更新を行うものとした。更新の頻度は、各 LAN ごとに状況に合わせて変更が必要となるだろう。

転送用ディレクトリを持つマシンに WWW サーバをインストールしておけば、ユーザは、そのマシンにインストールされているサーバを使って HTML の試験を行うことができ、前置網の紹介情報サーバには、完成したデータを載せることができる。前置網の情報を見る時には、PROXY を介して見る。

4．2　前置網でのサービスに関する議論

紹介情報以外に必要になるであろう前置網でのサービスとして次のものが考えられる。

FTP 等でネットワーク資源の提供を受ける者は、アプリケーション、データなどの資源の情報として、名前だけ、もしくは、短いドキュメントだけしか入手できないのでは、実際に資源を持っていって使ってみないことには、その資源が、どの様な物なのかを判断することが難しい。そこで、資源の提供者が、提供資源のテストベッドを作製し、公開することが考えられる。これは、主な資源の、実際に動作する物とそのテストデータとを、前置網のマシンの中にインストールしておき、匿名でマシンにログインしてもらい、資源の試用を行ってもらう物である。ただし、この時匿名でログインしたシステムを使用できる。このため、最悪の場合には、マシンの資源を破壊される恐れもある。この恐れから、紹介情報サーバ等の他のサービスを守るために、このマシンは専用のものであるべきである。

紹介情報の提供を受けるユーザは、多くの情報があるために、そのサーバの中のどこに自分が望んでいる紹介情報が入っているかがわかりにくい。そこで、紹介情報の検索機能を設けることができれば、ユーザにとって必要な情報が、どこに配置されているかが解りやすいものとなる。検索されるデータの更新は、紹介情報の更新時に同時に自動的に行うようにしておくと、事実データベースと、それを紹介する情報との一致を図ることができる。また、他のネットワークのサーバにもこの検索機能をリンクさせるようにすると、いっそう便利なものとなるだろう。

5　おわりに

LAN をインターネットに IP 接続するに伴い、 LAN 外部インターネットユーザが LAN 内のコンピュータ資源に無断でアクセスすることを拒むために、防火壁マシンを介在させて LAN を二分した。防火壁によって、パケットがリレーされなくなるので、 LAN のネットワークセキュリティは向上するが、LAN 内の資源を利用するネットワークサービスを外部ユーザに提供できないばかりでなく、LAN 内部ユーザもインターネットサービスが受けられなくなる。

そこでほんの少しだけ質的に低下したネットワークサービスの水準を維持しながら、パケットのリレーをする機能を、防火壁マシンに設けることをネットワークサービスごとに試みて、良い成績を収めたことを報告した。

この報告の結論は、

1）　LAN を防火壁で、前置網とローカルネットに分割し、インターネッ

トを利用しようとするLAN内部ユーザをローカルネットに局在化したので、使用中のLAN内コンピュータ資源を外部からの恐怖から守ることができ、ネットワークセキュリティを向上できた。

2） 外部ユーザに提供する匿名サービスは、 LANの前置網に局在化したサーバに集中する。サーバのデータベースの開発保守にあたっては、定期的複写機能を設けた。

これらのことにより、運用方針としては、外部からのログインに対して、ユーザ数の削減、期限の限定を行うこととなる。また介在する防火壁マシンをくぐり抜けるために、内部からの匿名サービスの利用要求と遠隔ログインはPROXY経由となり、外部からの遠隔ログイン要求は、防火壁へのログインを経るため、二度手間となった。

今後の課題として、次の点があげられる。

1） LAN内のマシンに遠隔ログインできる外部ユーザのパスワードの有効期限を短くするとともに、遠隔ログイン手続きを暗号化するなど、ユーザ認証の強化。

2） 紹介情報の編集者が参照すべきサーバの管理用資料、および、LAN管理者などが参考にすべきユーザ登録用の資料などを自動収集すること。

参考文献

[1] C.E.Landuhr et al: A Taxonomy of Computer Program Security Flaws, ACM Computing Surveys, Vol.26, NO.3,September 1994

[2] N.D.Arnold:UNIX SECURITY A Practical Tutrial,マグロウヒル出版株式会社,1993

[3] S.Garfinkel, G.Spafford: Practical UNIX Security, 株式会社アスキー、p367-385,1993

[4] W.R.Cheswick,S.M.Bellovin: Firewalls and Internet Security、ソフトバンク株式会社、p 51-119、1995