—論　文—

高岡短期大学紀要　第10巻　平成9年10月
Bull.Takaoka National College,Vol.10,October 1997

内部情報の保護と外部への公開を統合したネットワークの設計と構築

近藤　潔

（平成9年5月28日受理）

要　旨

外部から内部ネットワークへのアクセスに対するセキュリティを確保しつつ，内部情報の外部への公開を可能にするネットワークを設計・構築した。ファイアウォールによりネットワークを内部と境界に分離し，内部と境界でそれぞれ個別のネームサーバ，メールサーバ，WWWサーバを稼働させて独立性を保ちながら，これらのサーバを統合することで内部および外部のユーザにファイアウォールの存在を意識させない透過な環境を構築できた。また，ファイアウォール導入の前後において，ユーザの利用環境の変化を最小限に抑えるとともに，既存のサーバおよびクライアント機器やネットワーク機器の設定変更をきわめて少なくすることができた。

キーワード

ファイアウォール，ネットワーク設計，境界ネットワーク，セキュリティ，WWWサーバ，DeleGate，Sendmail

1　はじめに

インターネットを本格的に業務に使用するためにはセキュリティの確保が重要である。このため，最近になってファイアウォールを導入する事例が増えてきた。ファイアウォールの構成は種々多様であり[1)2)]，目的に応じた設計が必要である。

ファイアウォールは情報のアクセスを監視してセキュリティ確保に必要なアクセス制御を行なうので，利用者の側から見ると利用制限を課せられるような印象をうけ，マイナスのイメージが強くなりがちである。しかし，ファイアウォールのようなセキュリティ確保の手段が確立できないと，情報の保護を必要とする業務への適用ができないなど，すぐにネットワーク利用の範囲拡大に限界が来てしまう。また，ネットワークの資源を外部に開放したくても，それを利用して非公開の情報にアクセスされるなどの恐れがあると思い切った実施ができない。

最近のファイアウォール製品は，利用者による外部アクセスについては実用上十分な手段を提供しているが，内部情報の外部への公開について一貫した機能を提供しているものはほとんどない。「地域へ開かれた大学」を大きな特色とする本学では，内部情報の保護と同時に特定情報を外部へ公開するための機

産業情報学科

能が重要である。そこで，ネットワークの内部をファイアウォールによって保護しつつ，公開したい特定情報や機能を外部へ開放することを可能とするネットワークを設計し，本学ネットワーク上に構築して機能を検証した。

また，ファイアウォールの導入によりネットワーク構成を変更する場合，コンピュータやネットワーク機器の設定変更が大量に発生する可能性がある。このような設定変更を少なくする方法についても設計目標に含めてネットワークの設計を行なった。

2 ファイアウォールの設計

設計対象とするネットワークに要求される主な仕様について述べる。

2.1 設計の目標および条件

ファイアウォールの導入に際しては，インターネットへのアクセスの制限や多大な設定変更作業の発生が懸念される。そこで，設計の目標と条件を以下のように設定した：

（設計目標）ファイアウォールによりネットワーク内部のセキュリティを確保しつつ外部の利用者にできるだけ多くのコンピュータ資源を開放する。

（設計条件1）ファイアウォールの導入前後でインターネットへのアクセス方法がほとんど変わらない。

（設計条件2）既存のサーバおよびクライアント機器の設定変更作業がほとんど発生しない。

（設計条件3）ファイアウォールのセキュリティレベルが最高水準の方式を採用する。

2.2 ネットワークの分割

セキュリティの観点から，ファイアウォールを境として内部ネットワークと境界ネットワークに分割し，外部の利用者は内部ネットワークには入れないが，境界ネットワークには自由にアクセスできる構成とする。

2.3 ファイアウォールの方式

ファイアウォールの方式は，ゲートウェイ機能により次の3つに分類される[1]：

1．パケット・フィルタリング・ゲートウェイ
ゲートウェイの前後でＩＰ転送機能が作動しており，パケットに関する一般的なルールを記述することでフィルタリングを行なうもの

2．サーキット・ゲートウェイ
ゲートウェイの前後でのＩＰ転送機能は停止しているが，ＴＣＰレベルでの一般的なチェックを行なって転送するもの

3．アプリケーション・ゲートウェイ
ＩＰ及びＴＣＰレベルでの一般的な転送機能を停止し，アプリケーションごとにチェックしてデータを通過させるもの

ファイアウォールの選択基準としては，

1．セキュリティの強さ

2．維持管理の容易さ

3．ユーザから見たファイアウォールの透過性

4．種々のプロトコルに対応できる柔軟性

を選ぶ。アプリケーション・プロトコルごとに個別のプログラムによってデータの通過を制御するアプリケーション・ゲートウェイの方式は，一般的なメカニズムで制御する他の方式に比べてセキュリティの強さと維持管理の容易さで優れている。ただし，ユーザにファイアウォールを意識させない透過性および様々なプロトコルに対応できる柔軟性については疑問がある。

透過性について

透過性はパケットフィルタリングが最も優れている。ゲートウェイにルーティングされてきたパケットは単にルールに従って処理さ

れ，ゲートウェイを通過するだけなので，ユーザは何も考慮する必要がない。アプリケーション・ゲートウェイ方式では，使用するアプリケーションごとにゲートウェイのアドレスを設定したり（PROXYの場合），まずゲートウェイにログインするなどの操作が必要となることが多い。

最近のファイアウォール製品は，ＩＰレベルでのパケット・フィルタリング機能とアプリケーション・レベルでの個別処理機能を兼ねたものが多く，ＩＰレベルでの一般的なルールを記述するのではなく，あらかじめ組み込まれているアプリケーション・レベルの処理プログラムに対して条件を設定するようになっている。この場合には，ルーティングされてきたＩＰパケットをファイアウォールが自分で識別して適切な処理プログラムへ渡すので，ユーザはアプリケーションごとにホストアドレスやポート番号を設定する必要がない。そこで，このような機能を備えたファイアウォール製品を採用する。

柔軟性について

ファイアウォール製品を用いる場合，製品がサポートしていないプロトコルに対処することが不可能となる。そこで，種々のプロトコルに対応したアプリケーション・ゲートウェイの機能を持つDeleGate[3]を併用する。DeleGateでも対応できない場合は，ファイアウォール製品が持つパケットレベルの制御機能を直接操作することが考えられるが，セキュリティの問題と維持管理の問題があるのでこれは最小限に抑える。

2．4　ドメイン名，ＩＰアドレス

設計条件２（設定変更の最小化）を満足するために，ドメイン名は内部ネットワークと境界ネットワークとで同じ名前（takaoka-nc.ac.jp）を用い，ＩＰアドレスはネットワーク分割の前後で最小限の変更に抑える。

2．5　ネットワーク資源の外部への開放

外部へ開放する主な目的は，以下の通りである：

1．公開講座等の地域と関連した活動
例えば，ホームページ作成講座の開講中にＷＷＷサーバを受講生に開放するなど。

2．外部との共同研究
学外との共同研究で境界ネットワーク上のコンピュータを利用する。

3．学外からの教職員，学生，卒業生等の利用
自宅や出張先から利用する。

上記，１及び３を実現するために，境界ネットワーク上の１台のコンピュータをＰＰＰのサーバとして設定し，電話回線を介した利用を可能とする。２は境界ネットワークを外部から自由にアクセスさせることで可能となる。

3　サーバ及びネットワーク機器の配置と役割り

設計条件の１と２を満足させるため，旧来のネットワーク関連サーバおよびネットワーク機器の配置はできるだけ変更せずに，ファイアウォール装置と境界ネットワークを付け足すことにした。図１に本学のネットワークにおけるサーバ及び機器の配置を示す。図中，バックボーンルータを含む内部ネットワークが旧来の部分にほぼ相当する。なお，ネットワーク系サーバのＯＳは性能及び安定性の点でUNIXを使用する。

3．1　ネームサーバ（ＤＮＳ）

内部ネットワークと境界ネットワークで異なるＤＮＳサーバを持つことにより，内部ネットワークのホスト情報等が外部へ洩れないようにする。ただし，ユーザにファイアウォールを意識させない観点から，内部に独

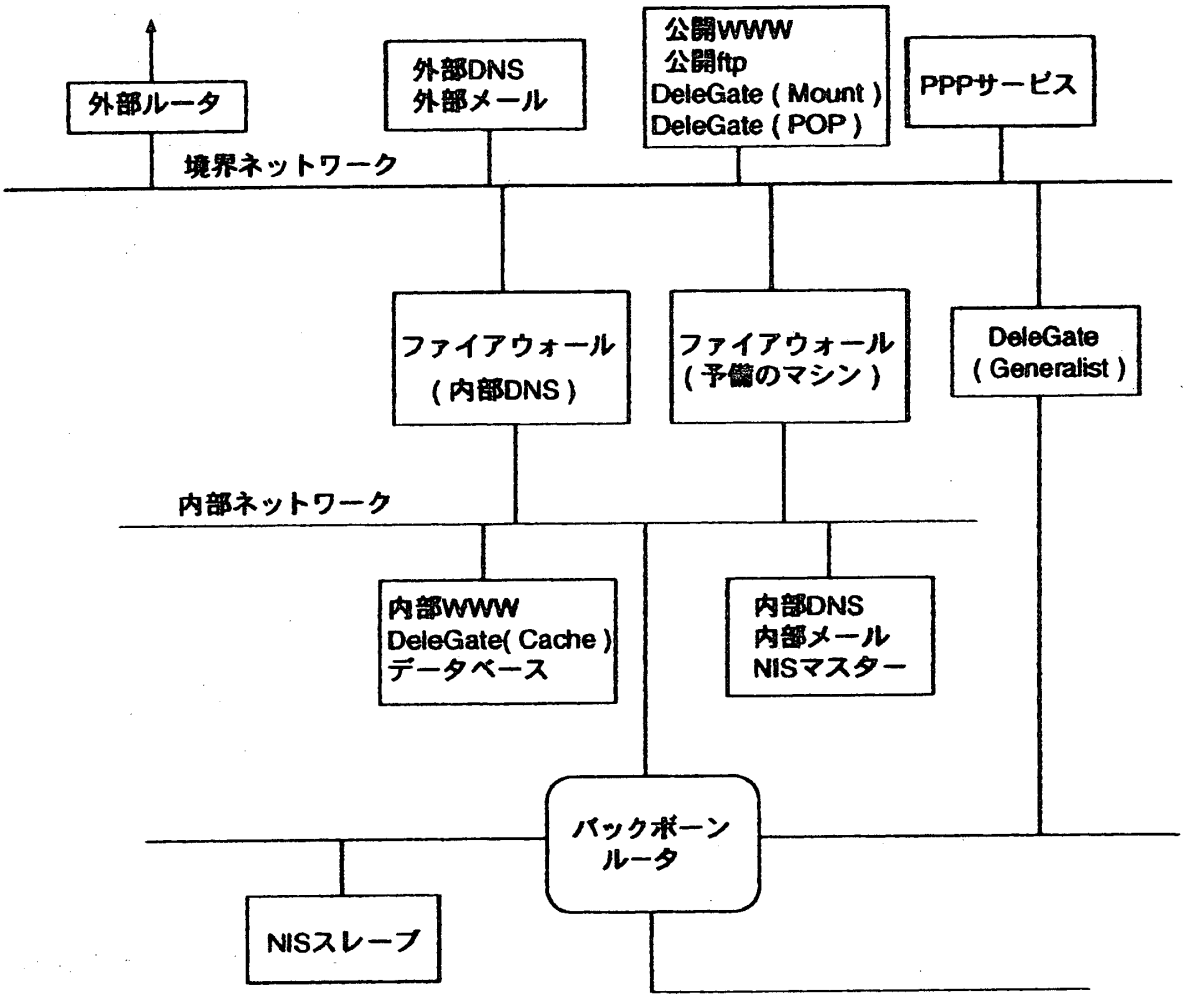

図1 サーバ／機器の配置

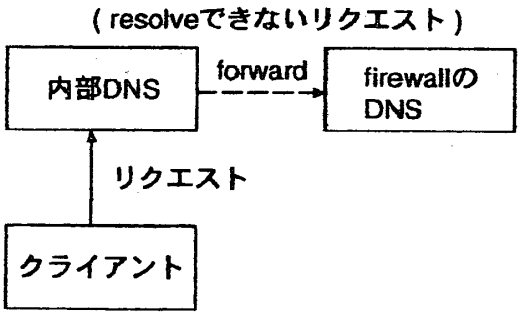

図2 内部ＤＮＳサーバ

立のルートサーバを持つ方式ではなく，ファイアウォールのＤＮＳ機能を利用する方法をとる（図2を参照)。つまり，内部ＤＮＳは自分でresolveできないリクエストのみをファイアウォールへ送る。また，外部ＤＮＳは外部及び境界ネットワークからのresolve要求に応えるドメインの正式ネームサーバであるが，内部ネットワークの情報は持たない。

このように，ＤＮＳの機能を，外部，ファイアウォール，内部の3つに分割することで以下のメリットが生じる：

1．各ＤＮＳを独立に維持管理できる。例えば，内部ネットワークに新しい機器を追加しても，内部ＤＮＳのデータのみを変更すれば良い。
2．内部のresolve要求は内部のみで迅速に処理される。
3．ファイアウォールのＤＮＳへの依存が小さいので，ＤＮＳソフトのバージョンアップ等への対応が容易。

3．2　メールサーバ

メール機能は，内部，外部，及び内部と外部を中継するファイアウォールの3つに分割する。最近のファイアウォール製品はほとんどがメールサーバ機能を持っているが，以下の理由で独自の内部メールサーバを持つことにし，ファイアウォールにはメール中継のみを行なわせる：

1．内部メールサーバはメール・ハブとして全ユーザのメールスプールを管理するので，ユーザ管理等の汎用的な機能が必要。
2．添付メール等が集中すると一時的に処理の負荷が増大することがあるので役割を分散して負荷の分散を図る。
3．メールサーバ・ソフトのバージョンアップが容易。
4．従来と同じサーバマシンを使うことで設定変更を最小にできる。

なお，外部に独自のメールサーバを持つ理由の1つは，負荷の集中しやすいファイアウォールの負荷を軽減するためである。また，通常のメール送受信以外にメールサーバのエイリアス機能からプログラム等を起動する利用法がある。例えば，本学で用いている電子掲示板は電子メール機能を利用してメールサーバからプログラムを駆動している[4]。境界ネットワークでこのような利用法を行なう場合にはファイアウォールと別にメールサーバが必要となる。

境界ネットワークを利用するユーザのメールスプールは機密保護の観点から内部メールサーバを利用する。

3．3　WWWサーバ

WWWサーバは公開用のデータと非公開のデータを保持しており，公開用のデータを外部（境界ネットワーク上）に置き，非公開のデータを内部に置くという考え方もあるが，以下の点からできるだけ多くのデータを内部ネットワークに置くことが望ましい：

1．ユーザ管理の簡素化
境界ネットワーク上のWWWサーバに各ユーザのコンテンツを置くと，全ユーザのアカウントを境界ネットワーク上のコンピュータに設けることになり，セキュリティ及び維持管理の面から好ましくない。
2．内部データベースとの連動
公開するデータの中に内部データベースを利用するものがあると，境界ネットワークにデータを持つことができない。
3．データ・バックアップ等の維持管理
公開データを内部に持つ方が維持管理が容易である。

このため，WWWサーバを内部ネットワーク上の内部WWWサーバと，境界ネットワーク上の公開WWWサーバに分離し，公開WWWサーバには全体のホームページの表紙にあたる部分と，ＰＰＰ等によって主に境界ネットワーク上でコンピュータを利用するユーザのデータのみを置く。内部WWWサーバと公開WWWサーバはDeleGateを利用して統合する。

3．4　DeleGateの利用

DeleGateは電子総合研究所の佐藤豊氏が開発したインターネットのソフトウェアで，ファイアウォールで分離されたネットワーク間を中継するための様々な機能を提供する[3]。DeleGateを利用する上での問題は，DeleGateを稼働させるホストが内部ネットワークと境界ネットワークの両方に接続する必要があるのでセキュリティを確保しなければならないことである。このため，DeleGateのホストはIP forwardingをオフにしたゲートウェイとして作動させ，さらに以下の条件をつける：

1．一般のユーザアカウントは一切設けない。
2．DeleGate以外のアプリケーションは

原則として稼働させない。

3．ユーザが直接アクセスしないGeneralistのみを稼働させ，かつ，Generalistにアクセスできるホストを限定する。

次に，DeleGateの役割について述べる。

WWWサーバの統合

DeleGateのマウント機能は，サーバの特定のディレクトリにアクセスしてきたリクエストを別のサーバへのリクエストに書き換える機能である。図3に示すように，ホストAの特定のディレクトリ（例えば／public）の下にあるファイルにアクセスするリクエストを，ホストBのどこかのディレクトリの下のファイルへのリクエストに書き換え，リクエストとそのリプライをGeneralistのDeleGateが中継することにより，実際にはホストBにあるファイルがホストAにあるかのように見せかける。

ホストAが境界ネットワーク上，ホストBが内部ネットワーク上にあるとすれば，ホストAにアクセスしたユーザはすべてのデータがホストA上にあるのと全く同様に操作することができ，内部WWWサーバと公開WWWサーバを統合することができる。

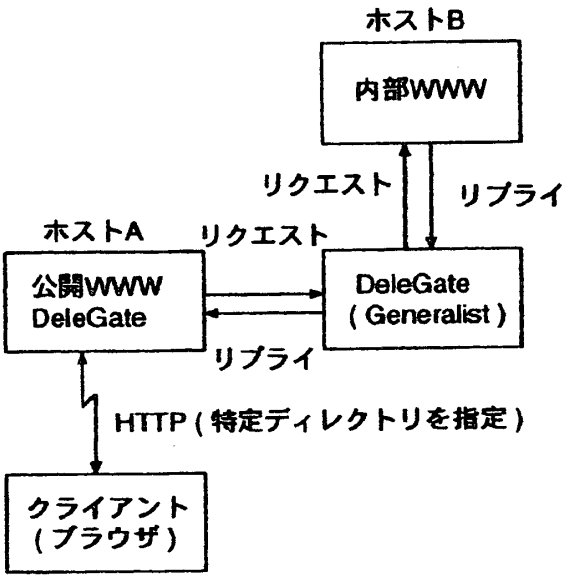

図3 DeleGateのマウント機能

WWWデータのキャッシュ

授業等で複数人が一斉にWWWブラウザを使用するような場合には，外部への回線に一時に大きな負荷がかかるためキャッシュサーバが必要である。内部ネットワークで稼働するDeleGateをプロキシに指定し，そのキャッシュ機能を利用する。

4 ネットワークの構築

2章及び3章で述べた仕様と構成に基づいてネットワークを構築した。構築における基本的な問題と移行の注意点について述べる。なお，表1に構築に用いたサーバソフトの一覧を示す。

表1 サーバソフトの一覧

種 類	名 称
ネームサーバ	named（OSに附属）
メールサーバ	sendmail（V8.8.5）
WWWサーバ	httpd (NCSA, Apache)
中継用サーバ	DeleGate（V3.0.30）
ファイアウォールサーバ	BorderWare (Secure Computing社)

4.1 ドメイン名の保持

ファイアウォール導入の前後でドメイン名が変わると，種々の設定変更が生じ，管理者及びユーザの負担となる。外部及び内部のドメイン名を同じtakaoka-nc.ac.jpとすると，内部ネットワークから境界ネットワークへアクセスができないという問題が起こる。つまり，内部ネットワークのネームサーバは，

hostname.takaoka-nc.ac.jp

の形式のネームに対するリゾルブ要求がくると，自分のデータベースを検索して名前が見つからないとfowarderに渡さずにエラーを返してしまう。これを防ぐためには，内部ネットワークからアクセスする可能性のある

境界ネットワーク上のホスト名も内部ＤＮＳのデータベースに加えておく必要がある。

４．２　メールの設定

メールの設定はネットワークが複雑になってくると注意が必要である。メールソフトとしては，インターネット上で最も広く使われているSendmailの新しいバージョンであるＶ8.8.5を使用した。メールは，内部と外部及びファイアウォール上のメールサーバ等で構成されるサーバ群によって処理される。図４に全体の処理の流れを示す。

sendmail.cfの記述

Sendmail Version 8.8の設定については，文献５）に詳しく記述されている。Sendmailの設定には豊富なマクロが用意されており，単純なメールサーバの構成であれば数行のマクロで設定できるが，図４のような構成ではマクロで作成したsendmail.cfに手を加える必要がある。

図４のメールの流れを以下に説明する：

●外部→内部への流れ

1．takaoka-nc.ac.jpのドメインへ向けたメールはＭＸレコードに従って外部メールサーバへ送られる。
2．外部メールサーバのエイリアス機能を利用するもの以外を全てファイアウォールへ送る。
3．ファイアウォールは全てのメールを内部メールサーバへ送る。
4．内部メールサーバはメール・ハブとして，宛先に誤りのあるメール以外の全メールをローカルに配信する。

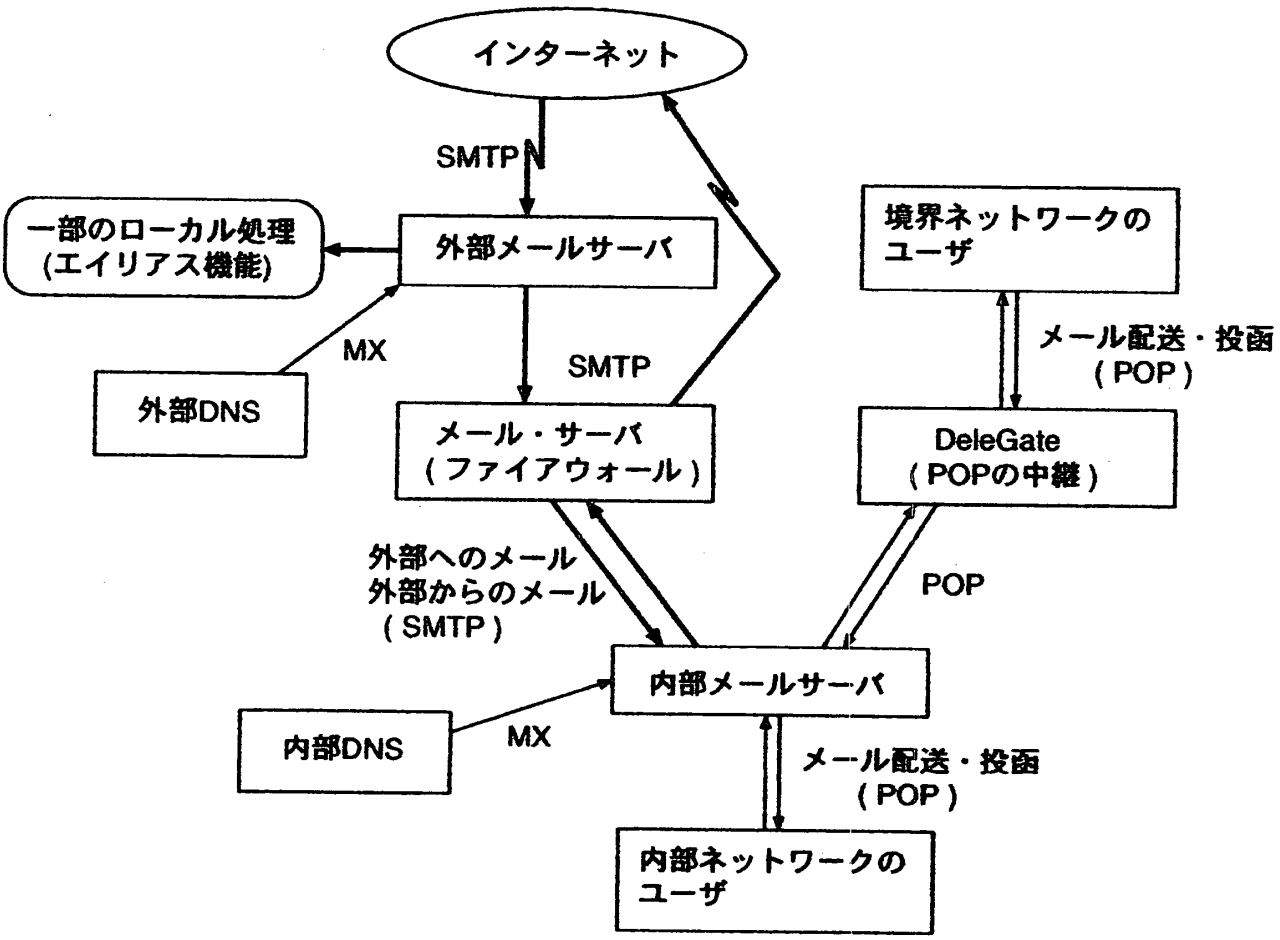

図４　メール処理の流れ

●内部→外部への流れ

1．内部及び境界ネットワーク上のユーザは全て内部メールサーバにメールを送る。

2．内部メールサーバは外部へ向けたメールをファイアウォールへ送り，それ以外はローカルに配信する。

3．ファイアウォールは外部へ直接送信する。

●境界→外部メールサーバ（図4には記述してない）

これは，外部メールサーバのエイリアス機能を境界ネットワーク上で使用する場合に限定する。

以上の構成に対して作成したsendmail. cfの概要を述べる。まず，内部サーバのためのマクロファイルの例を示す（ファイル名をinner. mcとする）：

```
include（'../m4/cf. m4'）
OSTYPE（'os-type'）
DOMAIN（'generic'）
MASQUERADE-AS（takaoka-nc. ac. jp）
MAILER（local）
MAILER（smtp）

LOCAL-CONFIG
# Japan local time
OtJST-9
# Firewall definition
D（FW）firewall. takaoka-nc. ac. jp
D（IP）firewall-IP-address
# Local host names
Cw hostname1 hostname2...
```

ここで，イタリック体は適切な文字に置き換えることを意味する。また，*firewall-IP-address*はファイアウォールの内部ネットワークにおけるＩＰアドレスの意味である。

ここでは，ファイアウォールの名前とＩＰアドレスを格納するマクロとしてＦＷとＩＰを与えている他は普通のメールサーバの設定と変わりがない。このinner. mcファイルはm4マクロを使っているので，m4コマンドで展開し，得られたファイルの名前をinner. cfとする。

inner. cfのルールセット０はメール配送エージェントを決定する部分であるが，リモート・ホストに関する部分は次のようになっている（ルールのlhsとrhsの間は本来はタブで区切るが，表示の都合上，ここでは改行している）：

```
# handle numeric address spec
R$* < @ [ $+ ] > $*
  $#esmtp $@ [ $2] $: $1 < @ [$2] > $3

# deal with other remote names
R$* < @$* > $*
  $#esmtp $@ $2 $:$1 < @ $2 > $3
```

これらはメール受取人のホストに直接メールを送るための記述である。このメールをファイアウォールに中継させるためには，送り先のホストを示す$2を次のようにファイアウォールへと書き換えればよい：

```
# handle numeric address spec
R$* < @ [ $+ ] > $*
  $#esmtp $@ [${IP}] $: $1 < @ [$2] > $3

# deal with other remote names
R$* < @$* > $*
  $#esmtp $@ ${FW} $: $1 < @ $2 > $3
```

次に，外部メールサーバのmcファイルの例を以下に示す（ファイル名はouter. mcとする）：

```
include（'../m4/cf. m4'）
```

```
OSTYPE（'os-type'）
DOMAIN（'generic'）
MAILER（local）
MAILER（smtp）

LOCAL-CONFIG
# Japan local time
OtJST-9
# Firewall definition
D（FW）firewall. takaoka-nc. ac. jp
# Define local user names
CL root name1 name2...
# Local host names
Cw hostname1 hostname2...
```

ここで，イタリック体は，適切な文字に置き換えることを意味する。なお，クラスLには，外部メールサーバ上でローカルに配信したいユーザ名（つまり，エイリアス機能を起動させるための名前）を記述する。

outer. mcファイルをm4コマンドで展開して得られたファイルをouter. cfとする。outer. cfの変更の要点は以下の通り：

- クラスwで定義したローカル・ホスト名に一致した宛先にはローカルのメーラで配信せず，SMTPでファイアウォールへ送る。

outer. mcのルールセット0でクラスwとの一致などからローカル配信を決定している部分を以下に示す：

```
# short circuit local delivery so for-
# warded mail works
R$+ < @ $=w . >      $#local $: $1

# handle locally delivered names
R$+      $#local $: $1
```

これを，ファイアウォールへ送るように変更する：

```
# short circuit local delivery so for-
# warded mail works
R$+ < @ $=w . >
  $#esmtp $@ ${FW} $: $1 < @ $m . >

# handle locally delivered names
R$+
  $#esmtp $@ ${FW} $: $1 < @ $m . >
```

4．3　DeleGateの設定

図1で境界ネットワーク上のDeleGate SpecialistはDeleGate Generalistを経由してMountによるHTTPの中継とPOPの中継を行なう。この関係を図5に示す：

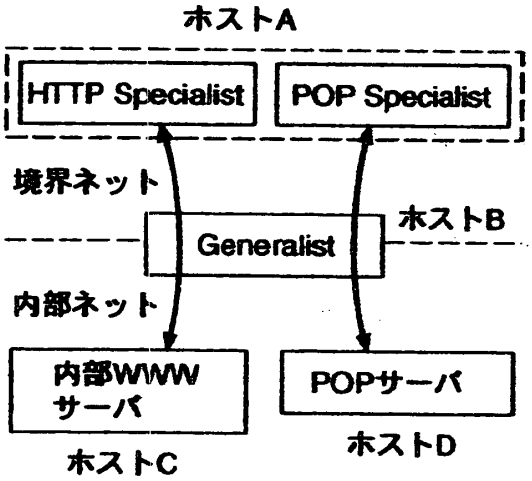

図5　DeleGateによる中継

ここで，Specialistは特定のプロトコルでクライアントと接続し，クライアントとサーバ間でリクエスト／レスポンスを中継するDeleGateであり，Generalistは任意のSpecialistとDeleGate固有のプロトコルで接続し，リクエスト／レスポンスを中継するDeleGateを意味する[6]。

ホストBのGeneralistの起動は以下のように行なう：

```
(Generalist)
delegated -Pportnumber \
RELIABLE=hostA
```

ここで，RELIABLEの指定はホストAからのリクエストのみ受けつけることを表わす。

次に，ホストAのHTTP Specialist及びPOP Specialistの起動方法は以下の通りである：

```
（HTTP Specialist）
delegated -Pportnumber \
SERVER=http://hostA:portnumber \
MASTER=hostB:portnumber \
MOUNT="/dir1/* http://hostC/dir2/*" \
          （マウントする数だけ記述する）
PERMIT=*:*:*

（POP Specialist）
delegated -Pportnumber \
SERVER=pop://hostD:110 \
MASTER=hostB:portnumber \
PERMIT=*:*:*
```

4．4 移行に関する問題

ファイアウォール導入の前後で，設定変更が必要となる主な要因は次の通りである：

1．ドメイン名の変更
2．ＩＰアドレスの変更
3．サーバの変更
4．ルーティングの変更
5．ＤＮＳの切替え

このうち，ユーザ側に影響を与えるものは1～3であり，ネットワークの設計・構築に際してできるだけ変更が少なくなるように努めた。それでも，変更せざるを得なかった項目は，

1．境界ネットワークのＩＰアドレス
2．WWWサーバへのアクセス方法

である。

境界ネットワークのＩＰアドレス

境界ネットワークのアドレスは外部から参照されるので，既に本学に割り当てられているアドレスを利用する必要がある。内部ネットワークのアドレスはプライベートＩＰアドレス[7]を採用することも可能であるが，その場合は種々の設定変更が必要となるので今回の構築では見合わせた。

境界ネットワークのアドレスは，従来のネットワークの1つを2分割してサブネット化し，その一方を割り当てた。このため，サブネット化したネットワーク上のホストについてネットマスクの変更等の作業が発生した。今後，境界ネットワーク上のホストが増加する場合は内部のネットワークにプライベートＩＰアドレスを割り当て，その分を境界ネットワークに振り向ける予定である。

WWWサーバへのアクセス方法

外部接続回線の速度不足を補うために必要なＨＴＴＰのキャッシュ用DeleGateは利用頻度が高いので，内部ネットワークにおく必要がある。WWWサーバの統合により，公式のWWWサーバは境界ネットワーク上に移り，WWWサーバのホスト名であるwww.takaoka-nc.ac.jpを引き継ぐことになった。このため，ブラウザのHTTPプロキシの設定をDeleGateが稼働する内部WWWサーバのホスト名に変更する必要が生じた。

ＤＮＳの切替え

ＤＮＳホストの変更はJPNICに届ける必要があり，かつ，上流サイトの設定変更を依頼する必要があるので，瞬間的に切替えることはできない。ある期間，既存のサーバと新しいサーバを平行して稼働させ，外部の切替が終った時点で完全に切替えることで，ネットワークの停止を回避できた。

5 結　言

ファイアウォールを導入して内部情報を外部から保護すると同時に，ネットワーク資源を外部へ公開するための機能をもつネットワークの設計と構築が完了した。今後は，内部での本格的な業務活動への利用と，外部とのより密着した活動の両面で積極的に利用していきたい。以下に，今後の課題として検討すべき事項を掲げる：

- DeleGateホストのセキュリティ
  境界ネットワークと内部ネットワークの両方に接続するDeleGate用のホストは，WWWサーバの統合とPOPによるメールの中継という重要な役割を担っている。ここでは，DeleGate以外のサーバを稼働させないようにしてセキュリティの確保を図っているが，さらにいっそうセキュリティ強化を検討する必要がある。
- Sendmailの設定
  Sendmailの設定は複雑で，現在の設定がベストとは言い難い。本論文の設定はcfファイルを直接編集する必要があるが，維持管理等の面からmcファイルレベルでの設定のみとすることが望ましい。

最後に，ネットワークの構築に際し多大の協力をいただいた高岡短期大学産業情報学科の米川覚助手に厚く謝意を表する。

文　献

1）W. R. Cheswick, S. M. Bellovin：Firewalls and Internet Security, Addison－Wesley（1994）
2）D. B. Chapman, E. D. Zwicky：ファイアウォール構築，オライリー・ジャパン（1996）
3）佐藤：インターネット防火壁の基礎技術と応用－DeleGateの仕組み－，コンピュータソフトウェア，Vol. 14, No. 1, pp. 55－63（1997）
4）米川：WWWと電子メールによる「学内情報システム」の枠組み，高岡短期大学紀要，第9巻，pp. 25－39（1997）
5）B. Costales, E. Allman：sendmail（2nd Edition), O'Reilley&Associates, Inc.（1997）
6）DeleGateの配布モジュールに附属のドキュメント（Manual. txt）を参照。DeleGateは次のＵＲＬで配布されている：
ftp：//ftp. etl. go. jp/pub/DeleGate/
7）Y. Rekhter et al.：Address Allocation for Private Internets, RFC1918（1996）

Design and implementation of a network which integrates the ability of protecting and providing inner information to the outside

Kiyoshi KONDO

(Received May 28, 1997)

ABSTRACT

A network which can provide inner information to the outside while maintaining secure access from outer networks was designed and implemented. The network was divided by a firewall into the inside and the perimeter, each having their own name server, mail server and WWW server. By intergating these servers, a transparent envitonment which allows users to access outer networks almost without noticing the firewall could be built. The change of the user environment as well as the re-configuration of servers, client PCs and network instruments after the introduction of the firewall was minimized.

KEY WORDS

firewall, network design, perimeter network, security, WWW server, DeleGate, Sendmail