第 12 部

Fire Wall 構築技術

第 1 章

ファイアウォールに優しい FTP

ファイル転送を行うプロトコル FTP では、データ転送の中止や流量制限を行うために、制御コネクションに加えて、データコネクションを用いる。制御コネクションは、クライアントからサーバに向かって (外向きに) 張られるが、データコネクションは通常サーバからクライアントに向かって (内向き) に張られる。このため、サーバからコネクションを張る場合は、安全にサーバ側のポート番号を固定することができる。実際に、ftp-data ポートとして 20 番が予約されており、統計情報を取るために役立っている。

インターネットが成長し危険性が増した今日では、ファイアフォールを構築し、なるべく労力をかけずにローカルネットワーク全体の安全性を高めることが多くなった。高度なセキュリティレベルを要求しない組織では、IP の到達性を損ねないフィルターを用いたファイアフォールを構築することが多い。フィルターの高度な設定として、コネクションの確立を一方向にする方法がある。つまり、外向きのコネクションは張れるが、内向きにコネクションは確立できないように設定できる。

このように方向性を有するフィルターは、従来の FTP クライアントと親和性が低い。組織内の FTP クライアントから、インターネットにあるサーバへアクセスする場合、制御コネクションは張れるが、データコネクションはその組織からみて内向きであるので確立できない。

幸いなことに RFC1579[90] で方向性を有するフィルターに親和性の高い「ファイアウォールに優しい FTP」について考察されている。要約すると、従来の FTP クライアントは PORT コマンドによってクライアント側のポートをサーバに指示し、コネクションを張るように要請するが、PASV コマンドを使えばサーバにデータコネクションを受動的に受け取るように指示することができる。また、現在使われている多くのサーバで、この PASV コマンドはサポートされているので、サーバ側は問題ない。

そこで、PASV コマンドをサポートするクライアントを作成すれば、方向性を有するフィルターを用いてファイアフォールを構築していても、インターネットとローカルネットワーク間で不自由なくファイルを転送できる。PASV コマンドをサポートするクライアントには、NcFTP があるが、BSD の ftp と互換性がないため ange-ftp.el などでは利用できない。そこで、BSD ftp に PASV コマンドを組み込んだ FFF(Firewall-Friendly FTP) を作成した。また、xarchie にも、PASV コマンドをサポートさせた。

このように UNIX のクライアントの改造は問題ないが、頭の痛いのは PC や Mac の FTP クライアントである。現在では、anarchie などを除いて、PASV コマンドをサポートしている PC や Mac 上のクライアントは少ない。

また、URL に ftp が指定されている場合、WWW クライアントが PASV コマンドをサポートしていなければ、うまく通信ができないという問題がある。しかし、proxy をサポートしている WWW クライアントでは、次のようにしてこの問題を解決できる。つまり、proxy サーバをファイアウォールの外側に置きインターネットとの通信を自由に行えるようにする。そして、URL が ftp で始まる場合、WWW クライアントと proxy サーバ間では HTTP を用いて通信し、proxy サーバと FTP サーバ間のみで FTP を使うようにする。こうすることによって、WWW クライアントに何ら改造を加えずにファイアウォールとの親和性を高めることができる。たとえば、xmosaic や netscap などでは、ftp_proxy という環境変数を設定するだけでよい (例、`ftp_proxy=http://pr.aist-nara.ac.jp/`)。

自組織が情報を提供するための FTP サーバは、ファイアウォールの外側に置かなければならない。例えば、組織 A が、一方向のフィルターを用いたファイアウォールの内側に FTP サーバを設置した場合を考えてみる。一方向のフィルターは、例外として FTP ポート 21 番は組織 A からみて内向きにコネクションを確立することを許しているとする。

組織 B から通常の FTP クライアントを用いてサーバにアクセスすると、制御コネクションは A にとって内向きであるが、21 番ポートであるのでコネクションが確立できる。また、データコネクションは A にとって外向きであるので確立でき、ファイルを問題無く転送できる。しかしながら、組織 C からファイアフォールに優しい FTP クライアントを用いてアクセスした場合には、問題が発生する。なぜなら、データコネクションをクライアントからサーバに張るため、組織 A にとっては内向きのコネクションとなる。しかも、このコネクションの終点ポート番号は、あらかじめ予想できないので、フィルターに穴をあけておくことができない。そこで、データコネクションは確立できないことになる。

このように、一方向のファイルターを用いる場合には、通信のパターンをきちんと分類し、問題のないように設定に気を配る必要がある。

第 2 章

ファイアウォールの役割 RFC1597 でのインターネットアーキテクチャについて

RFC1597[36] によりインターネットのアーキテクチャが大きく変わろうとしている。プライベートインターネットがインターネットの一部に認められつつある。ファイアウォールはインターネットとプライベートインターネットとの境界を作るものでもある。ここでは従来のアーキテクチャでのファイアウォールの与える影響、および RFC1597 でのアーキテクチャについての考察を行う。まず、従来のアーキテクチャについて紹介し、次に RFC1597 でのアーキテクチャについて説明する。　ファイアウォールについても概要を紹介する。次に、ファイアウォールが従来のインターネットアーキテクチャに与える影響を述べる。この考察を元に RFC1597 でのインターネットアーキテクチャについて考察する。

2.1　インターネットアーキテクチャ

インターネットアーキテクチャは次の 3 点から成り立つ。

- Catnet Model
- Addressing
- Layering

それぞれについて説明する。

2.1.1　Catnet Model

計算機のネットワークアダプタ、電話番号などの固有なアドレスだけで通信できる範囲のネットワークを物理ネットワークと呼ぶことにする。インターネットアーキテクチャではこの物理ネットワークがルータでつながったものをインターネットとする。　ルータは複数の物理ネットワークにつながっており、一つの物理ネットワーク上のパケットを別の物理ネットワークに転送する。この転送はパケットの送り先アドレスと経路 表とにしたがっ

て行う。インターネットアーキテクチャではインターネットにつながっている計算機は IP アドレスで識別される。ルータでのパケットの転送はネットワーク単位で制御する。このために物理ネットワーク上の計算機の IP アドレスはネットワーク部が同一のものを使う。物理ネットワークの IP アドレスはすべて異なってなければならない。　物理ネットワーク上の計算機の IP アドレスも異なっていなければならない。

2.1.2 Addressing

Address とは通信のために自分または通信の相手を指定する方法である。インターネットアーキテクチャではネットワーク層、トランスポート層、アプリケーション層での Address がある。ネットワーク層では Catnet Model での IP アドレスを使う。トランスポート層でのアドレスはネットワーク層のアドレスに何かを付け加えたものとなる。これは Layering によるもので下の層のアドレスにその層でのアドレスを付け加える。インターネットでポピュラーな TCP, UDP のトランスポートプロトコルではポートを使う。つまりトランスポートでの端点の指定は (IP アドレス, ポート) の組みとなる。アプリケーション層での Addressing の書式はプロトコル毎にさまざまであるが還元していくとトランスポートアドレスに何かを加えたものとなる。トランスポートに TCP,UDP を使う場合は (IP アドレス, ポート、アプリケーションでの付け加えたもの) となる。

2.1.3 Layering

2 点で通信を行うときに通信の一方の点で、ある層は下の層に送るデータを渡す。このとき、その層は下の層でのデータが相手にどのような方法で渡るかについては気にしない。通信の反対側では対応する下の層から送ったのと同じデータが対応する層に受け渡される。インターネットアーキテクチャでは (下位から順に) 物理層、データリンク層、ネットワーク層、トランスポート層、アプリケーション層を使う。

2.2 RFC1597 でのインターネットアーキテクチャ

RFC1597 でのインターネットアーキテクチャでは、Catnet Model と Addressing に関して変更がある。

2.2.1 Catnet Model

物理ネットワークがルータでつながっているけれども、ルータの中にはネットワーク層でパケットの転送しないものもある。IP Forwarding をしない型の Firewall でプライベートインターネットとインターネットとが接続している場合だ。パケットはトランスポート層、アプリケーション層で中継しなければ物理ネットワーク間で転送されない。

2.2.2 Addressing

プライベートインターネットのネットワークアドレスを使ってインターネット内でアドレス付けされないのでプライベートインターネットのアドレスはインターネットでのアドレスと異なってなくてもいい。プライベートインターネット用のアドレスとしてあるレンジのアドレスが予約された。複数のプライベートインターネットで直接通信しないので、複数のプライベートインターネット のネットワークアドレスも互いに異なっていなくてもよく、上の予約されたレンジのアドレスを使ってもよくなった。

2.3 ファイアウォール

ファイアウォールは管理方針の違いなどによりネットワーク上の計算機へのアクセスに違いを設けるための仕組みである。アクセス元計算機、アクセス先計算機、アクセスするサービス (TCP,UDP ではポート)、それにアクセスしている人などによって違いを出す。例えばネットワーク X 上の計算機からしかネットワーク Y 上の計算機へは Login できないとかである。ネットワーク A とネットワーク B との間にアクセスの差を設けたいときはネットワーク A,B 間にファイアウォールを設置する。ファイアウォールの実装としては次の 2 つの方法がよく使われる。

- パケットフィルタ
- IP forwarding を止めてトランスポート層、アプリケーション層で中継する。

2.4 パケットフィルタによるインターネットアーキテクチャへの影響

パケットフィルタによるインターネットアーキテクチャへの影響としては、次の 2 点がある。

- CatnetModel の部分的崩壊
- CatnetModel にはない方向の出現

2.4.1 CatnetModel の部分的崩壊

パケットフィルタではルータがパケットを選択的に転送する。選択の基準はあて先 IP アドレス、送り元 IP アドレス、トランスポートプロトコル、トランスポートプロトコルのフラグなどである。ネットワーク A,B,C が相互につながっているとする。ネットワーク A はネットワーク B と、ネットワーク B はネットワーク C と通信できるようにネットワーク

A,B 間のパケットフィルタ、ネットワーク B,C 間のパケットフィルタでそれぞれ設定してあるとする。ネットワーク B からみるとネットワーク A,C とは通信できるが、この時ネットワーク A,C 間は通信できない。したがってネットワーク B からみると Catnet Model は成り立っているように見えるが、ネットワーク A,C ではネットワーク C,A とはそれぞれ通信できなく Catnet Model は崩れている。パケットフィルタでは部分的に Catnet Model を崩している。

2.4.2 CatnetModel にはない方向の出現

パケットフィルタでは TCP のフラグを見て、パケットを選択的に転送できる。したがってネットワーク A,B 間でネットワーク A からネットワーク B へは TCP のコネクションを開設できるが、ネットワーク B からネットワーク A へは TCP のコネクションを開設できないということがある。Catnet Model では方向という概念はなかったがパケットフィルタにより方向が出現した。

2.5 パケットフィルタと RFC1597 で拡張されたインターネットアーキテクチャとの関係

パケットフィルタは部分的にパケット転送を行うのでパケットフィルタの両側のネットワークの IP アドレスは固有でなければならない。そのためプライベートインターネットとインターネットとの接点にパケットフィルタを持ちいるとプライベート IP アドレスを使えない。すなわち、RFC1597 で拡張されたインターネットアーキテクチャでのインターネットとプライベートインターネットとの接点には IP Forwarding を止めてトランスポート、アプリケーション層で中継する方式か、NAT(Network address Transformation) を用いなければならない。

2.6 IP Forwaring を止めてトランスポート、アプリケーション層で中継する方式のインターネットアーキテクチャへの影響

Catnet Model をネットワーク層での中継を指すとすると IP forwarding をしないルータから外側は Catnet Model ではないということになる。ネットワーク A,B との間に IP Forwarding をしないルータがある場合はネットワーク A,B 間の通信はトランスポート層、アプリケーションで中継されるがネットワーク A,B それぞれの内部の通信はネットワーク層、物理ネットワークで行われる。これら内部では Catnet Model が成り立っている。トランスポート層、アプリケーション層での中継それぞれについての影響を述べる。

2.6.1　トランスポート層での中継

通信の相手先がネットワーク層で通信できない場合トランスポート層はネットワーク層にデータを渡す前にネットワーク層で通信出来る場合には行わない次の過程を踏まえなければならない。

- 通信の相手先とのトランスポート層での中継を行う計算機の IP アドレスを知る。
- トランスポートゲートウェイに対して本当の通信の相手先を指定する。

トランスポート層での中継をする場合はトランスポートでの経路制御 (トランスポートゲートウェイを使うか (使うときはその IP アドレス) ネットワークに渡すかの判断) が各計算機で必要となる。

2.6.2　アプリケーション層での中継

通信の相手先がネットワーク層で通信できない場合アプリケーション層はネットワーク層にデータを渡す前にネットワーク層で通信出来る場合には行わない次の過程を踏まえなければならない。

- 通信の相手先とのアプリケーション層での中継を行う計算機の IP アドレスを知る。
- アプリケーションゲートウェイに対して本当の通信の相手先を指定する。

アプリケーション層での中継をする場合はアプリケーションでの経路制御 (アプリケーションゲートウェイを使うか (使うときはその IP アドレス) ネットワークに渡すかの判断) が各計算機で必要となる。

トランスポート、アプリケーション層で中継する場合はそれぞれの層での経路制御が必要となる。ネットワーク層で中継している場合にはネットワーク層での経路制御が必要なことからも中継する層での経路制御は必要となる。トランスポートゲートウェイのよく使われる TCP ゲートウェイ Socks では socks のトランスポートゲートウェイを決めうちないしは通常のネットワーク層でのコネクション開設に失敗した場合トランスポートゲートウェイを使う。経路制御は使用者まかせまたはネットワーク層を試しその後、決められたゲートウェイを使うという貧弱なものだ。アプリケーションゲートウェイもメール、ニュース、Telnet などすべて使用者がゲートウェイを選択するか設定ファイルでゲートウェイとどういうものをゲートウェイをとおすかを選択する。メールの sendmail に関しては UUCP 時代の名残りで複数のゲートウェイの使い分けができる。どのゲートウェイを使うかについては DNS の MX レコードで制御する。

2.7 RFC1597 で拡張されたインターネットアーキテクチャへの考察

プライベートインターネットにプライベートインターネット IP アドレスを使うためにはインターネットとプライベートインターネットとの接点には IP forwarding を行わないトランスポート、アプリケーションゲートウェイを置くか、NAT を置かねばならない。ここでは IP forwarding を行わないトランスポート、アプリケーションゲートウェイを使う場合について次の 2 点についての考察を行う。

- トランスポート、アプリケーション層での経路制御
- IP アドレスを端点の指定につかえない

2.7.1 トランスポート、アプリケーション層での経路制御

RFC1597 ではプライベートインターネットとインターネットとのトポロジーについての規定はない。図 2.1に示すように、インターネット、プライベートインターネット A、プライベートインターネット B が直線的につながっている場合ありえる。ネットワークXとネットワークYとのゲートウェイをG_{xy}で表す。インターネットは I と表す。ネットワークX上の計算機をH_{x1}，H_{x2}.. と表す。メール (SMTP) の場合はH_{i1}からH_{b1}にメールを送る場合、ネットワークBのドメイン名よりインターネットからネットワークB当てのメールのゲートウェイはG_{ia}であることをH_{i1}は知り、H_{i1}はG_{ia}にメールを送る。G_{ia}は同様にゲートウェイはG_{ba}であることを知り、メールを送る。H_{a1}からH_{a2}にメールを送る場合は直接送ればいい。

トランスポート、アプリケーションゲートウェイのどちらの場合でも中継するプロトコルに関して、ゲートウェイを使って到達するのかネットワーク層で到達するのかの判断とゲートウェイのアドレスとをプライベートインターネットも含むインターネット上の全ての計算機は相手先ごとに知る必要がある。ゲートウェイのアドレスはネットワークのトポロジー、相手先の計算機によって変わるのでゲートウェイをまたがる毎に変わってくる。これは RFC1597 以前のインターネットでのネットワーク層の経路制御と同じことである。従って RFC1597 でのインターネットアーキテクチャではトランスポート、アプリケーションゲートウェイので中継されるプロトコルの数だけの経路制御が必要となる。

2.7.2 IP アドレスを端点の指定につかえない

RFC1597 でのインターネットアーキテクチャではプライベートインターネットでの IP アドレスが固有でない。先の例のネットワークトポロジーでネットワークA、ネットワークBがプライベートインターネット IP アドレスとして同じネットワークアドレスを使っていることもありえる。これを NP1 と表すことにする。H_{a1}とH_{b1}とがG_{ab}上のトランスポー

トゲートウェイを介して通信を行う場合を考える。H_{a1}は何らかの方法でトランスポートゲートウェイのアドレスG_{ab}を知り、G_{ab}に対してＨｂ１とＴＣＰで通信を行いたいと伝える。この時に、RFC1597 以前のインターネットアーキテクチャでは IP アドレスはネットワークＡ，Ｂでことなっていたのでトランスポート（ＴＣＰ）アドレスとして（ＩＰアドレス、ポート）の組みで通信の相手を指定できた。RFC1597 でのインターネットアーキテクチャでは IP アドレスは固有でなく、この例のようにネットワークＡ，Ｂで共通のもの使えるので、（ＩＰアドレス、ポート）の組みでは通信の相手を指定できない。ゲートウェイでのプライベートアドレスはコネクションの相手の反対側のアドレスを指すということにしたとしても、先の例のトポロジーでH_{i1}からH_{b1}と通信するときにG_{ia}に（ＩＰアドレス、ポート）の組みを与えてもネットワークＡを指すのかその先のネットワークＢを指すのか判断できない。以上の議論はアプリケーションゲートウェイでも同様に成り立つ。従って RFC1597 でのインターネットアーキテクチャでトランスポート、アプリケーションゲートウェイを介して通信する場合、通信の端点は IP アドレス以外の別のものを使って指定しなければならない。現実的にはドメイン名付きのホスト名などになるであろう。

2.8　まとめ

RFC1597 でのインターネットアーキテクチャではネットワーク層より上のトランスポート、アプリケーション層での経路制御が必要になり、かつ、通信の端点の指定に IP アドレスが使えないという重大な影響を及ぼすであろう。ネットワークトポロジの制限やトランスポート、アプリケーションゲートウェイの設置点の制限を設けネットワーク層以外での経路制御を不必要にしなければネットワーク層での経路制御の意味がなくあるであろう。

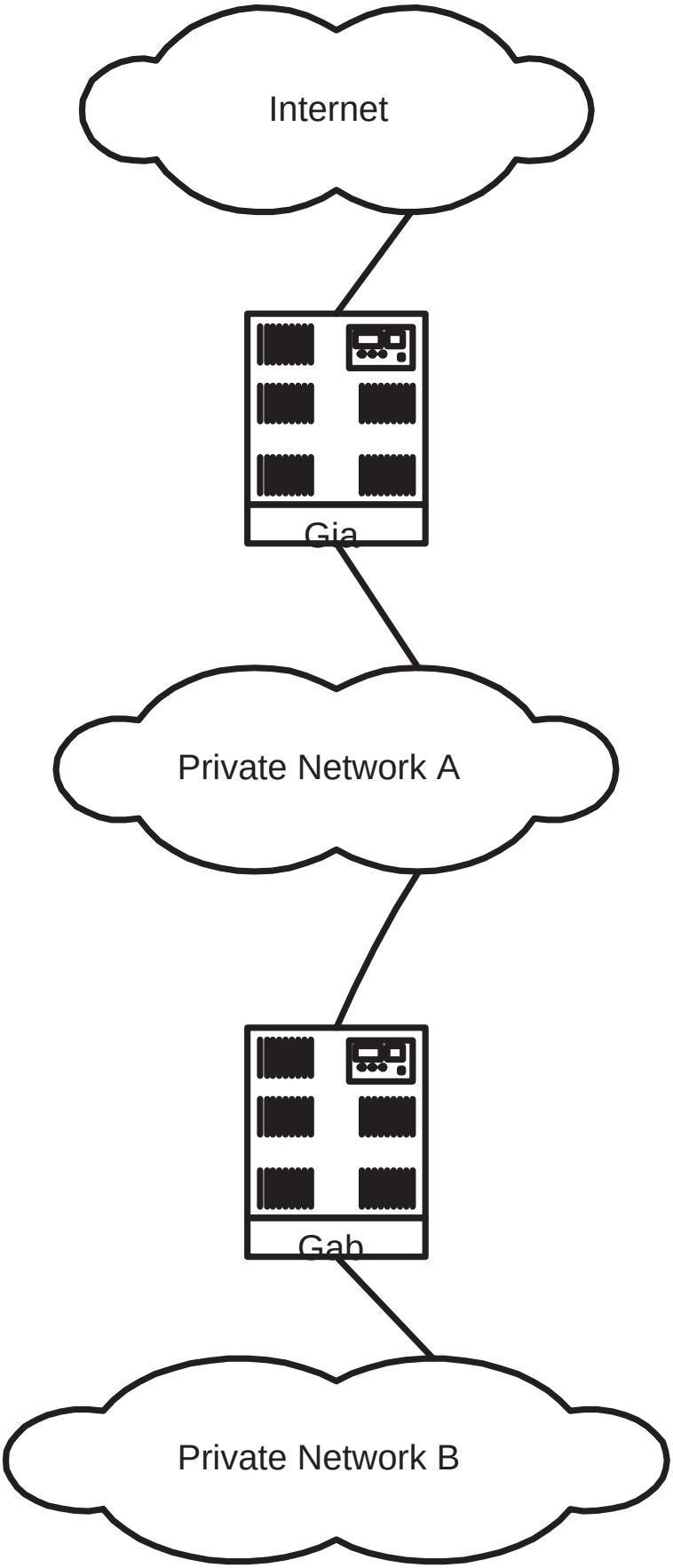

図 2.1: RFC1597 でのプライベートインターネットも含むインターネットの例

第 3 章

おわりに

本年度はファイアウォールでインターネットと接続している組織でも使いやすい FTP とアーキテクチャの中でのファイアウォールの位置付けを議論しファイアウォールを含んだアーキテクチャを模索した。これは RFC1597 でのアーキテクチャとも密接に絡んでいる。この活動は来年度以降も続ける方針である。

インターネット上のセキュリティに関して One Time Password の使用が積極的になってきている。ファイアウォールワーキンググループでは来年度では One Time Password についてやトランスポートゲートウェイの効率と仕様について議論と実装を行なう予定である。