インターネットセキュリティ対策技術の研究

Guideline for Internet security

坂本佳則

Yoshinori SAKAMOTO

ADSL、FTTHと、世の中ブロードバンドインターネット接続が身近なものとなってきた。ダイヤルアップによるインターネット接続が主流であった時代は終わりを告げようとしている。中小企業のインターネット接続環境において、接続速度はもとより、通信費用が通信時間によらない、月額定額制のインターネット接続は非常に魅力があり、インターネットの醍醐味の常時接続も身近になった。

一方で、接続時間が長くなればなるほど、また常時接続の利点を生かして、対外的なインターネットサービスを始めるなどすると、インターネット外部からのセキュリティ対策が必要不可欠となってくる。

そこで中小企業のインターネットセキュリティ対策として、既存のフリーネットワークOSを活用して、安価に簡易的なファイヤウォール装置を構築するパッケージを試作した。

1．インターネットとセキュリティ

インターネットはそもそもの「生い立ち」が、ネットワークのネットワークを作り上げることであり、異なる組織間のネットワークが相互に協力しあいながら巨大な世界的ネットワークを形成してきたものである。

いわば、インターネットの基本設計の上で最重要視されてきたのは相互につながれること、遠隔地であってもデータを失わずに送受信できることであり、そのための基本設計が随所に盛り込まれている。

広域分散情報処理環境の実験的なネットワークとして広がりを見せたインターネットであるが、当初は「とにかく使えるネットワーク」を作るために相互補助運営の精神で構築されてきた仕組みが多い。地球規模に成長を見せたインターネットは、一般社会に解放され様々な活用方法にさらされるとともに、セキュリティを考慮した運営方法が必要な時代になってきているのが現状である。

インターネットに接続されたコンピュータのセキュリティに関する問題は、上記の根本的な設計方針のほかに、プログラムミスによるものや、管理ミスによるもの、それらの弱点をついた悪意のプログラム（ウイルスやワームと呼ばれるもの）によるものなどが存在する。

ここでは、主に管理上の知識不足またはミスによるセキュリティー対処不足を補うための簡易設定パッケージの作成を目指した。

2．利便性とセキュリティ

組織がインターネットに接続する場合、一番利便性が高いのは、組織内のコンピュータ類をすべて外部と直接通信可能にしてしまうことである。インターネット上のすべてのサービスが利用できる。しかしながら現在の状況では次の2点で考慮すべき問題が発生する。

1点目は、セキュリティの問題である。個々のコンピュータ等からインターネットに直接アクセスできるということは、逆もあり得るということも考慮しなければならない。つまり組織内の全コンピュータに対して、インターネットから身を守るべく対処を施す必要が出てくる。

2点目は、IPアドレスの問題である。ここ10年来、世界的にIPアドレスの枯渇が問題となってきており、旧来の枠組みであるIPv4(Version 4)の範囲内では一般ユーザが要求する数だけ潤沢にIPアドレスを用意するというわけにはいかなくなってきている。

2.1 ファイヤウォール

1点目の問題について、組織内のユーザー全員が常に自らのパソコンのセキュリティ設定に留意し、セキュリティアップデートを施すことへの期待はできない。　そこで、

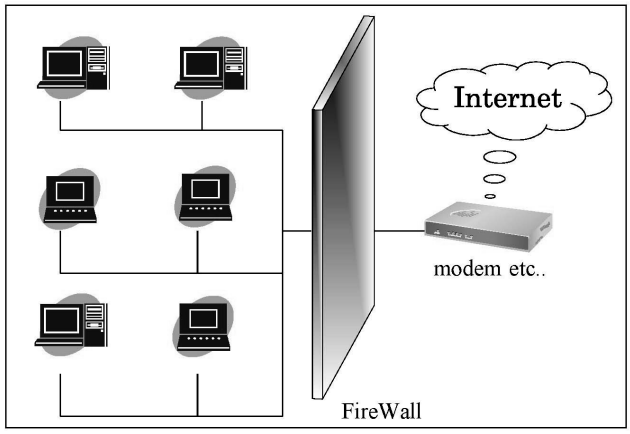

Fig.1　Firewall

システム技術チーム（現在、電子・情報・デザイン技術チーム）

組織内ネットワークからインターネット外部への出入り口を通過するパケットを制限し、危険な通信から組織内ＬＡＮを防御する。

Fig.1に示すように、インターネットと組織との境界線にあらゆる対外的な通信を監視または制御・制限する仕組みをもうける。

こうしたネットワークとネットワークの接続点で、接点を通過するパケットを監視することによって不要な不安をなくそうとする装置をファイヤウォールと呼ぶ。

2.2 IPマスカレード

もう一点はIPアドレスの問題である。インターネット上で潤沢にIPアドレスを配布できない現状において、組織内で利用する端末の数だけのIPアドレスが入手できることはまず無い。

この件の解決策としては、根本的にはIPv6の普及を待たなければならないが、ここでは現状の枠組み、すなわちIPv4の中での対策を考える。

インターネットでは「世界に１つしかないアドレス体系」、すなわち「グローバルアドレス」が相互接続の大前提である。IPアドレスは世界的に統一管理され、重複割り当ての無いように配布されてきた。これは世界中が通信するためには必要なルールであるが、昨今ではアドレスの枯渇が問題となっている。そのため、インターネットに直接接続していない組織内でローカルなIPネットワークを構成する場合に自由に使ってよいアドレスの範囲を「プライベートアドレス」として定めている。

プライベートアドレスの範囲をTable 1に示す、このアドレス範囲は、直接外部と通信する必要がない組織内ネットワークの構築に大いに活用され、アドレスの節約に役立った。

プライベートIPとして使用可能なアドレス	
Class A	10.0.0.0～10.255.255.255
Class B	72.16.0.0～172.31.255.255
Class C	92.168.0.0～192.168.255.255

Table 1　Private IP address.

このプライベートアドレスで構築された組織内ネットワークとインターネットを通信可能にする仕組みとして、NAT(Network Address Translator)がある。

「プライベートアドレス」は、その定義により、たとえ直接接続されたとしてもインターネット上でルーティングされたないため外部のいかなるホストとも通信ができない。そこで、グローバルIPアドレスを持ち外部と接続されている通信装置が、組織内からの通信をリアルタイムで変換し仲介することによって外部との通信を可能とするのがNATである。

さらに、単純なアドレス置き換えだけのNATでは、直接外部と通信できるホスト数は、その組織に割り当てられたグローバルIPの数に制限されてしまう。そこでIPマスカレードという手法を使い、通信ポートも同時に変換してしまうことで、複数のプライベートアドレスを一つのグローバルアドレスでまかなう手法も開発されており、現状のブロードバンドルータではこちらの手法をよく見かける。Fig. 2に両者の違いを示す。

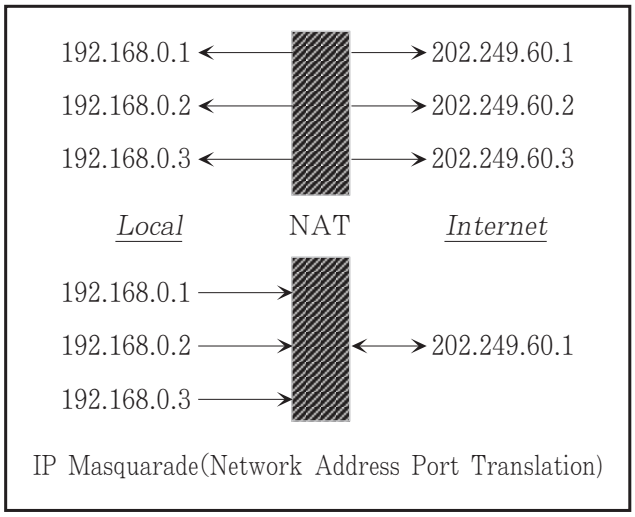

Fig.2　NAT and IP masquarade

ほかにもダイナミックNATという、プライベートIP側からの接続に応じて、同時接続数分のグローバルIPを割り当てる仕組みもある。

１対１対応のNAT以外は、グローバルアドレス側から組織内アドレスへの通信は、基本的にできない。つまり結果的に組織内ＬＡＮに対して外部からの通信をブロックしていることになり、ファイヤウォールと同時に論じられることが多い。

3．Linuxを用いたファイヤウォール

ファイヤウォールは、ルータで実現するものである。データが経由するネットワークが複数ある場合に、データを仲介して「経路(route)」を制御し、相互通信を実現するための装置であるので、ルータという。

ルータ装置は今では比較的安価に購入可能な専用機器も存在するが、ネットワークOSがあればPCで実現可能である。その場合のメリットは、使い古したパソコンを流用することによる経費削減効果と、ケースバイケースに応じた柔軟なカスタマイズ性である。

3.1 ハードウェア

ここでは、フリーソフトであり、ここのところインターネットサーバとしてはシェアを伸ばし続けているLinuxを用いて、一般のパーソナルコンピュータに導入し、前述のセキュリティ機能を実現させる。

利用パーソナルコンピュータとしては、128kbps から

8 Mbps程度の対外接続の帯域であれば、Pentium 200Mhz に64Mのメモリの数年前のパーソナルコンピュータの能力で対応可能である。

3.2 基本設計

ファイヤウォールを実現するために、複数のネットワークとの通信、データパケットの転送、特定の通信をブロックする機能、加えてIPマスカレードまで実現する。

設計の大前提として、組織内のコンピュータは信頼できることを条件とした。組織内からの情報の漏洩などについての考慮は運営ポリシーの問題の方が大きい。

組織内ＬＡＮはローカルIPで構成することとし、IPドレスは自動配布させる。このことにより、根本的に外ネットワークから内部ネットワークへの通信が発生するとはなくなる。

組織内ＬＡＮの利便性を損なわないように、内部から部に対する通信リクエストは、すべて許可した。

ここで問題となるのは、今回作成するLinux PC そもののセキュリティである。OSを最新の状態に保つの当然として、本来であれば、Linuxにインストールされいる様々なネットワークサービスについて、組織内ＬＡからはアクセス可能にし、インターネットからのリクエトに対しては制限する設定がおのおの必要である。

この作業は大変な作業量となる上に、設定ミスも起きすく、また変更が必要となったときに混乱を招く。しかも、プログラムレベルで判定を行うため、CPU負荷が高く、DoS攻撃への配慮も必要となる。

そこで、ここでは、ipchainsを用いて、カーネルレベルでパケットそのものを拒否する設定を行う。カーネルレベルの受信拒否は、CPUの負荷も少ない。

Linux PC の初期サービスとしては、インターネットに接続する場合の最低限のサービス、DNS, mail(postfix), NTPサービスのみとした。WWWについては、将来公開する場合にはリクエストを受け付けるように設定変更することとし、初期状態では禁止してある。

また、全体として「デフォルト拒否」の方針で設計し、外部からの接続についてはすべて拒否の設定を行い、その例外として必要サービスのみ許可している。

4．基本インストール

ネットワークカード2枚を装着したPC/AT互換機をセットアップの対象とする。

また、Ethernetで外部ネットワークと接続可能な状態を構築していることを前提とする。INSやADSL, FTTHなどとの接続デバイスをLinuxで直接サポートすることは今回の自動設定の対象外とする。具体的には高速モデム装置などを介して、Ethernet経由でインターネットと接続でき、Linux PCにグローバルアドレスが１つ割り当てられている環境である。Fig.3に前提とするネットワーク構成を示す。

Linuxのディストリビューション(配布キット)として、Vine Linuxを利用する。Linuxのディストリビューションの中でも広く利用されているRed Hatベースの日本語化ディストリビューションである。

インターネットに直接接続するOSは、こまめなアップデートが必須である。Vine Linux では、Debianのaptを用いたRPMパッケージアップデート機能をサポートしており、管理が容易である。

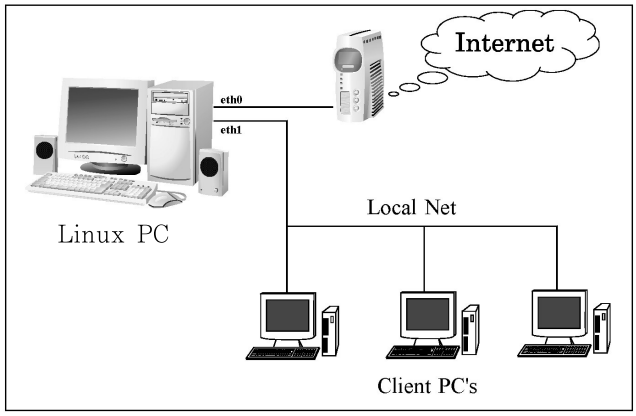

Fig.3　Precondition for installing linux

以下の3点を今回の前提条件とする。今回の手順による場合、必要ハードディスク容量は2G程度で収まる。

1．ネットワークカードは2枚差し、一方をインターネットアクセスが可能なセグメントに接続し、もう一方を組織内ＬＡＮに接続する。
2．インストール時にインターネット側のインタフェースがeth0、組織内ＬＡＮに接続する側がeth1となるようにする。
3．基本的にハードディスクを全域フォーマットしてLinuxだけをインストールする。

インストール手順について、CDROMまたは、ブートFDからCDROMを使ってインストールする例を示す。

最近のVine Linuxのインストーラでは、グラフィカルなインストールができるようになっている。グラフィックモードはVGAなのでたいていの環境で動作するが、マウスが必要である。もし、マウスが接続されていないなら、最初の起動時にtextと入力すればテキストモードでインストールが始まる。

1995年程度以降のパーソナルコンピュータならば、GUIでの利用が前提であったはずなので、ここでは、マウスが利用できるものとして、グラフィカルインストールを選択したものと仮定する。(text インストールであっても、表示されるメッセージに留意すれば手順は大きく変わらない)

グラフィカルインストールの場合はFig.4に示す初期画面でそのままリターンキーをたたき次の画面にすすめる。

最初に現在接続されているキーボードとマウスの設定の選択が必要となる。Vineではデフォルトのキーボードは日本語配列となっている。たいていの環境ではそのままでよいとおもわれる。Fig.5は、オープニング画面とキーボード・マウスの設定とすすみ、ようこそ画面までの様子を示している。

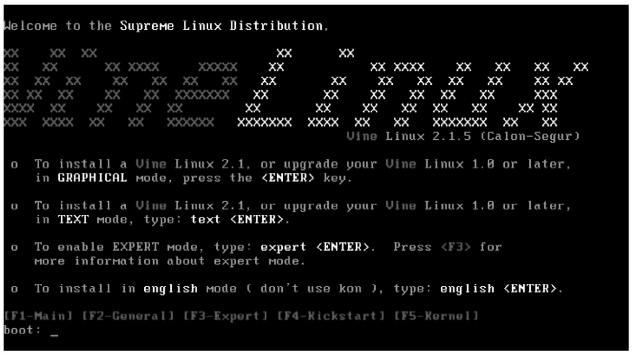

Fig.4　Initial screen for install

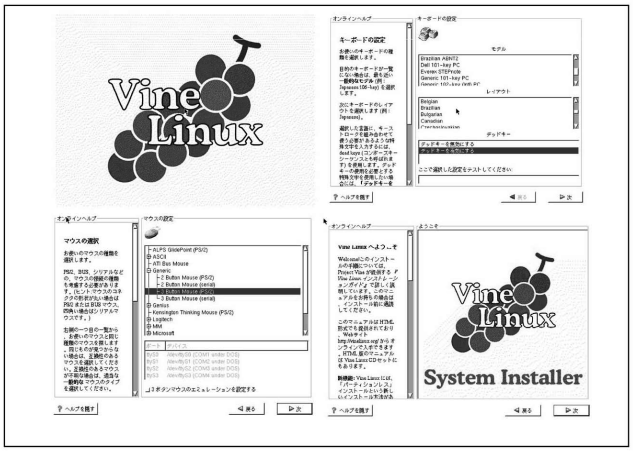

Fig.5　Keyboard and mouse setting

ウェルカムメッセージが表示され、そのまますすむと、インストールの種類を選択する画面になる。ハードディスクのパーティションや、UNIXシステムにおけるマウントの仕組みを理解しているユーザーはカスタムインストールを選択して、細かい指定をすることができる。

不明な場合「サーバ」インストールを選択すればよい。ハードディスクが消去されるが自動的に領域確保が行われる。Fig.6がその様子である。

次に、ネットワーク・タイムゾーン・root(管理者)パスワードの設定がある。Fig.7がそれらの画面である。

ネットワークの設定では、eth0 と eth1 の二つのタブがきちんとでていれば問題なく認識されている。ここでネットワークの設定が出てこないか、または一つしかタブがない場合には、個別対応が必要となる。Linux対応と明記されたネットワークカードであれば問題が発生しにくい。ここでは、eth0とeth1 の認識は問題ないものとする。

なお、eth1 側の設定は、後ほど自動セキュリティ強化スクリプトで自動設定するので、ここではeth0 の設定だけを行う。インターネット接続プロバイダから割り当てられたサーバ用のグローバルアドレスを１つ、ここに設定する。ゲートウェイの設定を追加し、インターネットに通信パケットが確実に出て行けるように設定する。

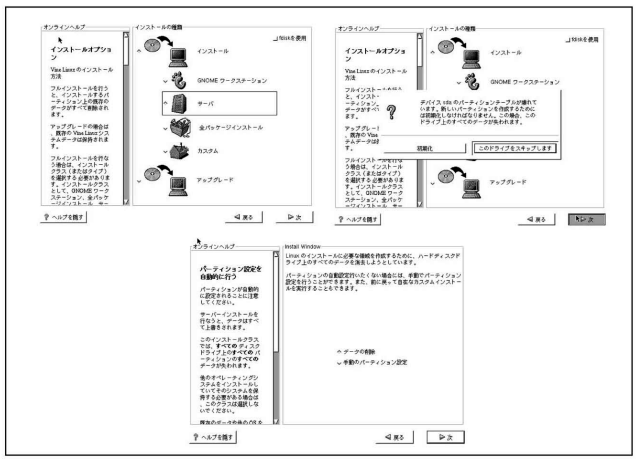

Fig.6　Select install type

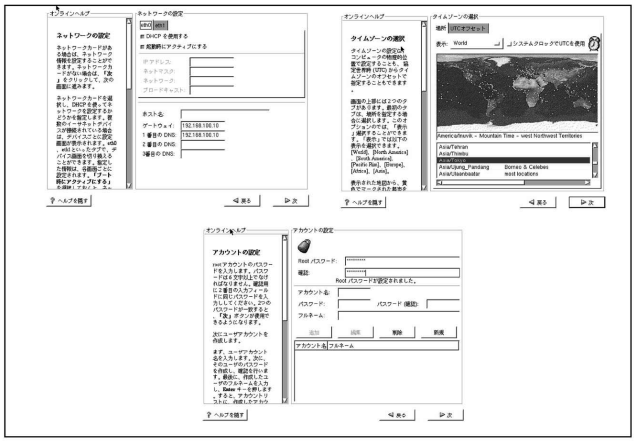

Fig.7　Network,time and root password configuration

rootパスワードの設定はセキュリティの要となるので、知人の名前や辞書に載っている単語など、第３者に類推しやすいパスワードを使わないように留意しながら、英文字と数字記号を組み合わせて推定しにくいパスワード文字列を用いる。

次に、X-Windowの設定画面となるが、今回はネットワークサーバで利用する前提なのでここで設定は行わない。ディスプレイの種類は選択しないと次に進めないので適当なものを選択すればよいが、正しいものを選択する必要はない。「Xの設定を行わない」を選択すれば、インストールの準備は完了である。Fig.8に示すように、ディスクのフォーマット後、パッケージのインストールが開始される。

パッケージのインストール後、緊急用のブートフロッピーを作成する。ハードディスクからブートしなくなった場合に備えて、この手順を省略してはならない。Fig.9にその

様子を示す。

リブートし、無事動作することを確認する。インターネットに通信できることが前提なので、rootでログインし、ping コマンドなどを使って到達性も確認する。

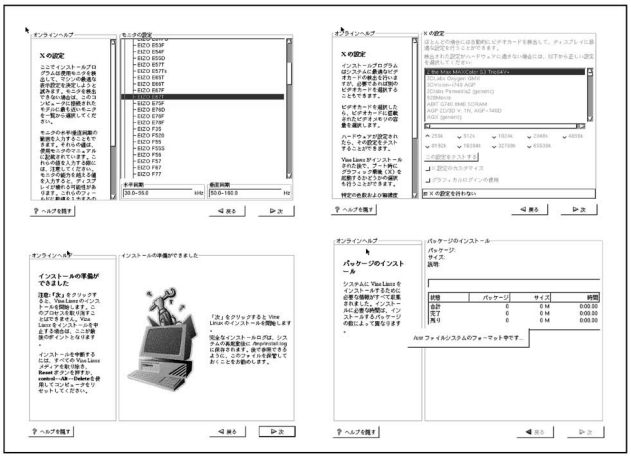

Fig.8　Skipping the X-Window configuration then start disk format

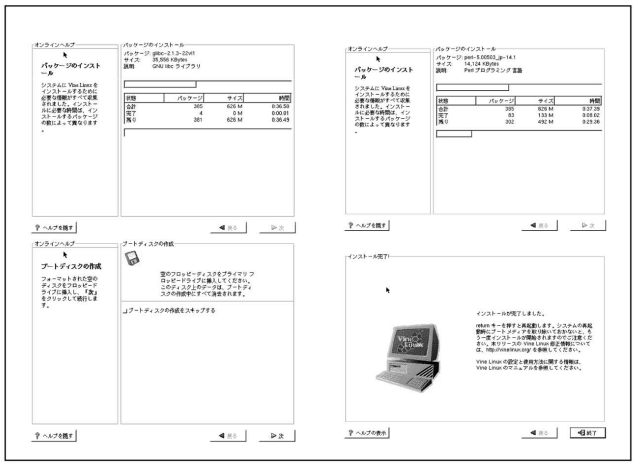

Fig.9　Packages install and making boot floppy

5．セキュリティ強化

今回試作したのは、インストール済みのLinuxシステムを組織のファイヤウォールとして自動設定するためのパッケージCDROMである。

これまで説明してきたインストール方法、機器構成が前提条件であるが、本CDに格納されたスクリプトを用いることによって、以下の作業が自動的に実行できる。

①インストール済みのVine Linux 全パッケージを最新版にアップデートすると同時に、DHCP・メール・DNS・NTPサービスについては確実にインストールする。
②インターネット外部に対しDNS,メールサービスを実施
③Linuxマシンの時刻を常時インターネット上の標準時刻に同期させるNTPの設定。
④インターネットからの不必要なネットワーク接続要求をすべて拒否する設定
⑤組織内ＬＡＮ(eth1)側のDHCPサーバ機能
⑥組織内からの通信をIPマスカレードでインターネットに中継

CD-ROMには、Vine Linux の最新アップデートパッケージがすべて格納されており、パッケージ全体のアップデートを行うための自動設定スクリプト「update」と、ネットワーク周りの設定を一気に行う「netsetup」の２本立てで自動設定を行う。なおCDROMのマウントは、通常はrootでコマンドラインから mount /mnt/cdrom とすれば/mnt/cdromというディレクトリ下にマウントされる。

updateはshスクリプトで記述し、netsetupではLinuxの各種パラメータを自動変更したり、自動生成したりする処理が多く、その処理中に文字列処理が必要となるためperlのスクリプトを採用している。

5.1 update

セキュリティ対策において、ネットワークOSそのものの最新版へのアップデートは最優先事項である。昨今の状況下では、メンテナンスリリースの大半はセキュリティ関連の対応が目的であるといってもよいほどである。

updateスクリプトでは、aptの機能を用いて、今回インストールされたソフトウェアの中からCDに格納された最新パッケージにアップデートが必要なものだけを自動的にアップデートする。最初からインストールされていないものについては、アップデートパッケージの中に格納されていてもインストールされない。

ただし、今回の前提であるファイヤウォールサービスに必要な、xntp,dhcpd,bindのパッケージについては、インストールされていなくても強制的にインストールするようになっている。

ユーザがカーネルの変更を行っていた場合、むやみにパッケージが提供する最新版に入れ替えるとブートすらしないという状況もあり得るため、安全を見越してaptを用いたシステムのアップグレードでは、Linuxのカーネルそのもののアップグレードは行われない。

今回、Linuxの用途をファイヤウォールマシンと限定し、機器構成についてもある程度限定した前提条件をおき、かつ初期インストール直後のアップデートという限定条件下で、この部分も全自動で行うスクリプトにした。

CPUに合った最新版のカーネルを自動インストールし、初期化RAMDISKを作成して、ブートセレクタであるliloの設定ファイルを書き換えた後に、ブートストラップへの登録を行う。

カーネルの入れ替えには万全を期し、updateスクリプトは、初期インストール時のカーネルを残し、起動時のブー

トセレクタ画面でlinux-oldというメニューで初期カーネルが選択可能な状況を作成して終了する。

5.2 netsetup

updateが終了すると、いったん再起動して無事動作することを確認する。eth0側が確実にインターネットにつながっているかの確認である。(pingなどを用いる。)

eth1側にローカルLANを接続し、再びCDROMから、netsetupを実行すれば、インターネット側の不必要なパケットをすべて遮断、ローカル側にはローカルIPを自動配布(DHCPサーバ)の上、IPマスカレードでローカルＬＡＮをインターネットに接続するLinuxルータが完成する。

ローカル側の設定はプライベートアドレスの192.168.100.1決めうちで設定し、ＬＡＮ内のクライアントは192.168.100.128から192.168.100.254の番号を自動配布する。

UNIX系OSのネットワークセキュリティ手法には、TCP wrapperを用いたものなど、複数の手法が考えられる。今回、netsetupを作成するに当たり、Linuxのipchains の機能を使い、プログラムのレベルのセキュリティ強化より前にカーネルレベルで不要なパケットを水際で遮断する手法を取った。

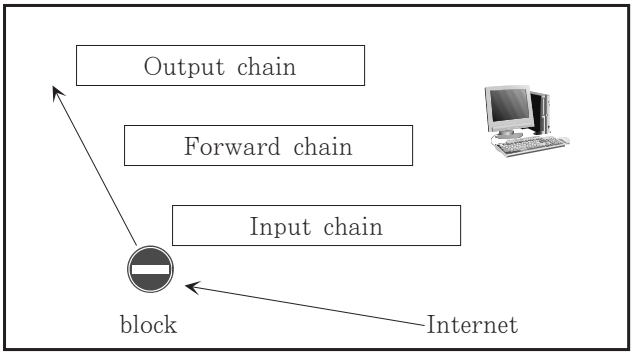

Fig.10　Blocking input datas

必要なサービス以外のTCP,UDPパケットには、 この設定をしたLinuxホストは全く反応しない。ipchainsによるパケットの制御では、データパケットの入り口に当たるinput チェーン、受け取ったパケットの扱いを決めるforwardチェーン、出力先の制御をするforwardチェーンが存在するが、入り口のinputチェーンにおいて不要なパケットをすべて落としている状態になる。Fig.10にその概念図を示す。

今回留意したのは、内側からの通信はできるだけ制限したくないということから、組織内からの通信リクエストの返信パケットに関しては受信可能としている。

カーネルレベルのパケット制御を活用しているので、コンピュータの資源を浪費せず、数年前の使い古したパソコンを活用できるというメリットがある。

今回試作したスクリプトでは、組織内ＬＡＮで通常サービスをしておけば便利だと思われる、組織内用DHCPサーバ、ローカル向けのDNSサーバ(外部への問い合わせキャッシュ付き)、インターネット上にある標準時刻サーバとの同期機能(NTP)を自動設定する機能も内蔵した。

DHCPに関して、ＬＡＮカードを2枚差した場合、ディストリビューション標準の状態では、たとえDHCPサーバをインストールしたとしても、eth0側でサーバーが稼働してしまう。この部分はそもそも変更可能パラメータとして用意されていないので、eth1側でDHCPサーバを稼働させるために起動スクリプト変更する必要がある。これはエディタを用いた編集作業であるため、UNIX系サーバの管理が不慣れな人には難しい。今回、netsetupスクリプトでは、ローカルLANがeth1側であるという前提で起動スクリプトを自動修正し、パラメータ変更可能なスクリプトに変更した上で確実にeth1側でDHCPのサービスが行えるようにした。

同時に、ローカルＬＡＮ側のDHCPクライアントに関して、配布IPアドレス範囲にクライアントの名前を自動生成してファイヤウォール装置で名前解決ができるようにした。ローカルＬＡＮ側に内部サーバをもうける必要がある場合には、netsetupの実行後、192.168.100.2から192.168.100.127の範囲内でIPアドレスを割り振って運営する。

6．おわりに

広く無料で入手可能なLinux OSを用いたファイヤウォール構築のためのパッケージ制作に挑戦した。入手しやすく、かつ継続してアップグレードメンテナンスが行われているものを活用するという手法を用いた。

本手法のメリットは、アクティブなメンテナンス活動を行っているディストリビューションを活用しているので、経常的なアップデートが行えるという点にある。

設定の簡便性と一括設定を目指した。ユーザに不要な入力を促さずに設定が完了するところを目的としたので、自分なりの設定をするための項目設定は省略している。この点に関しては議論の余地があると思われる。

また、インターネット接続が前提なので、インターネットを使った恒常的な自動アップデート機能を仕込むことも可能であるが、本格稼働中のシステムをアップデートするタイミングは組織それぞれであり、判断が難しいので今回は省略した。設定中ユーザの入力を促すようにすれば対処可能な部分なので、今後の課題としたい。

参考文献

1）久米原栄, Linux Networkファイヤウォール管理者ガイド, ソフトバンクパブリッシング, 2000.2.25

2）Project Vine, Vine Linux Home Page, http://www.vinelinux.org/, 2002