Free PC - UNIXを用いたゲートウェイの構築

Free PC - UNIXを用いたゲートウェイの構築

その他（別言語等）のタイトル	Construction of a Gateway by utilizing a Free PC - UNIX
著者	寺崎　仁司, 畑中　雅彦
雑誌名	室蘭工業大学研究報告. 理工編
巻	45
ページ	117-128
発行年	1995-11-10
URL	http://hdl.handle.net/10258/614

Free PC－UNIXを用いたゲートウェイの構築

寺崎仁司，　畑中雅彦

Construction of a Gateway by utilizing a Free PC－UNIX

Hitoshi TERASAKI and Masahiko HATANAKA

Abstract

To connect our laboratory computer network to the INTERNET via a LAN in this institute, we try constructing a low-cost and high-reliability gateway. Because the cost-performance of personal computers are getting much higher recently, we utilize an IBM-PC clone machine and Free PC-UNIX(Linux) for it. The constructed gateway shows acceptable performance(its transfer speed is 80 % of a commercial -gateway machine) and reliability.

1．はじめに

今や世界中に張りめぐらされたコンピュータネットワークは，人間の情報活動の基礎的基盤となっている，といっても過言ではないだろう。コンピュータネットワークによってもたらされるサービスは人々の生活に様々な変化を与えてきた。資源共有による資源の有効利用，遠隔操作による資源分散，それらがもたらす快適な作業環境，またコミュニケーションの手段としても用いることができる。

現在，室蘭工業大学にも学内ネットワークが張られ，少しづつだが研究の環境も変わりつつある。ネットワークを通じて電子メールや，ネットニュースでの情報交換もはかれるようになった。また，学内ネットワークはインターネットに接続しているので，学内に限らず学外のインターネットに接続しているあらゆる研究機関から情報を入手したり，意見を交換することも可能となっている。

当研究室では研究テーマとして MRI画像の処理，気象レーダーエコー像の解析による降雨・降雪量の測定，衛星回線の降雨・降雪による減衰量の測定などを行なっている。これらにおいて，データの処理や解析は，すべてコンピュータを用いて行なわれる。当然，データは磁気ディ

スク等の記憶装置に蓄えられる。常に1台のコンピュータを用いて作業するのであれば，それほどでもないのだろうが，複数のコンピュータを選択して使うことができるのなら，それぞれの環境をできるだけ同じにできれば便利である。それを実現させるためには，ネットワークを構築するのがもっとも良い手段であると思われる[1]。さらに，研究室に構築されたコンピュータネットワークを，学内のコンピュータネットワークに接続することによって，研究室のコンピュータから学外のコンピュータ(もちろん国内，国外を問わず)にもアクセスできるようになり，ネットワーク上の様々なサービスが利用できるようになる。

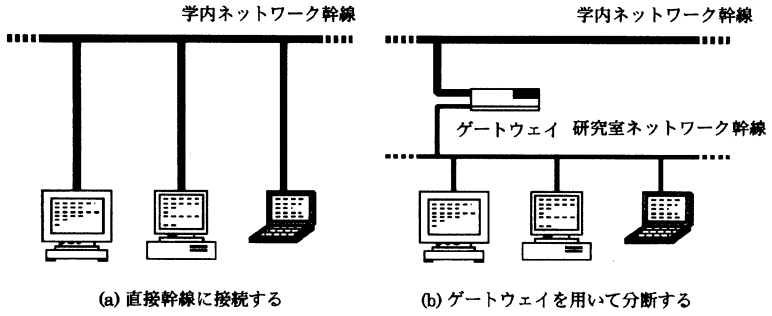
本報告では当研究室のコンピュータネットワークを学内のコンピュータネットワークへ接続するために行なった，フリーソフトウェアのPC-UNIXを用いたネットワークゲートウェイの構築について，いくつか実験したので報告する。

2．PC-UNIXによるゲートウェイの構築

2．1　学内ネットワークへの接続法

学内ネットワークを利用する場合，次のようなことを考慮して接続する方法を決める必要がある。

・ネットワークのトラヒック
・保守性
・ネットワーク資源



図－1　ネットワークの接続方法

トラヒックはネットワークの通信量のことだが，幹線に直接数十台のコンピュータを接続するような図－1(a)の場合は，コンピュータに対する送受信パケットがすべて学内ネットワーク幹線に流れ込むので通信量が増えネットワークの反応が遅くなることがある。一方，図－1(b)の様なゲートウェイを用いた構成にすると，ゲートウェイが研究室のコンピュータ間通信用のパケットは学内幹線に流さず，幹線を流れている研究室内のコンピュータに関連のないパケットを研究室幹線に流さないので，両幹線の通信量を減らすことができる。保守性については何か故障が発生した場合の回復のしやすさを考えれば良い。例えば図－1(b)のような場合はゲートウェイが故障してしまうと，外部へは一切通信ができなくなってしまうが，図－1(a)の場合は数台が故障しても外部へ通信できるコンピュータは残る。そして，ネットワーク資源として，TCP/IPを用いて通信を行なっている場合は，IPアドレス(ネットワーク上でホストを識別するためのユニークなアドレス)のことも考えておかねばならない。本学では 日本ネットワークインフォメーションセンター(JPNIC)より公式にIPアドレスを取得している(上位2バイト 157.19)。このアドレスの場合65534台のコンピュータを接続することが可能である。なお，実際の運用ではこれをサブネット[4] という概念を用いて，254台のコンピュータを接続することができるネットワーク254個に分割している。つまり図－1(b)の様な場合はその254個のうちの1つを割り当ててもらう必要がある。

当研究室の場合は，トラヒックについては，なるべく少なくしたいので関係のないパケットは研究室ネットワークに流したくない。保守については，ゲートウェイが故障することよりも，何らかの原因で研究室のコンピュータから不正なパケットが学内ネットワークに流れた場合(もしくは逆)，ゲートウェイを学内幹線から外すだけでとりあえず難を逃れることができるということを考慮して，研究室ネットワークは独立させて学内ネットワークに接続したい。ネットワークアドレスについては大学側に申請したところ当研究室独自のネットワークアドレスを割り当ててもらえた。これによってゲートウェイを用いての学内ネットワークへの接続を行なうことが可能となった。

2．2　ゲートウェイの構成

学内のコンピュータネットワークはUNIXマシンが中心となって構築されているので通信プロトコルとしてTCP/IPを用いている。TCP/IPゲートウェイには専用のものとUNIXマシンに複数のインターフェースを実装したものがある。前者は専用機なのでゲートウェイ以外には使えないが，TCP/IP以外にもAppleTalk(Macintoshで用いられている) 等の多種のプロトコルを扱えるものもある。また，後者はそのままUNIXマシンとしても使える。当研究室としてはなるべく安価で安定したゲートウェイを入手したい。安定性の面ではゲートウェイ専用機が良いのだが，それほど安価ではない。UNIXマシンをゲートウェイにするためにワークステーションを用いる場合はさらに高価である。検討を重ねた結果，IBM-PCとその互換機で動作するUNIX-

like-OS(通称PC-UNIXと呼ばれる[2])を用いてゲートウェイが構築できないかと考えた。ゲートウェイとして動作させることができる最低限のハードウエアとソフトウエアを用意すれば，安価にゲートウェイを構築することができる。最近のパーソナルコンピュータはかなり高性能であるので，PC-UNIXを用いたゲートウェイ構築については問題ないと判断した[10]。安定性はゲートウェイとして専用に使用することで確保する。ゲートウェイ兼用でUNIXマシンを使用すると，膨大にメモリを使用するプログラムやシステムの拡張作業よってシステムダウンを招く恐れがある。システムダウンのたびにリセットしていたのでは外部との通信が滞ってしまう。そのため，ゲートウェイが稼働を始めたあとは専用に使用した方が安全である。

現在までに，PC-UNIXとして様々なものが作成されている。大別すると商品としてのPC-UNIXと，フリーソフトウェア(著作権は放棄しないが，使用や配布に関しては無償で自由なもの)のPC-UNIXがある。商品の方はベンダーが製品に関して責任を持っているが，フリーソフトウエアは使用する側の責任において動作させることになっている。なるべく安価にゲートウェイを構築したいと考えていたので，フリーソフトウェアのPC-UNIXを用いることにした。候補としてはBSD UNIXの派生であるFreeBSD[5]，NetBSD[6]そしてPosix仕様のLinux[7]を考えていた。各々の最低限の動作環境は大体同じでCPU(中央処理装置)がi386SX以上，メインメモリ4MB以上(X Window Systemを使用する場合は8MB以上が望ましい)，ハードディスク容量60MB以上である[3]。

以上の値を参考にして，それよりも少し余裕のあるシステムを構築しようと考え，表－1のコンピュータを用意した。CPUについてはi386SXより上位のi486SXを，メインメモリは少し大きめに16MB，そして，ネットワークカードは3COM社のものを2枚用意した。ゲートウェイはネットワークを結ぶ役目を担うのでインターフェースが2つ必要となる。ところが，FreeBSD，NetBSDではこのイーサネットカードのサポートが遅れており，結局この時点でこのカードをサポートしていたLinuxをゲートウェイのOSとして使用することになった。

Linuxのインストールには Slackware 2.0.1 というパッケージを用いた。基本的にLinuxはカーネル(OSの核となる部分)とカーネル回りの基礎的なソフトウェアだけなので，その他のシステムに必要なコマンドやネットワークデーモンなど(もちろんすべてがフリーソフトウェアである)は，こうしたパッケージによって別途，提供されている。Linuxカーネルには安定性を重視した1.0シリーズと先進性を重視した1.1シリーズがある。最初，安定性を考慮して1.0シリーズを用いたが，ゲートウェイとして動作させると，パニックを起こしてしまった。どうやら，このシリーズではゲートウェイとしての使用は考慮されていないようだ。したがって1.1シリーズを使用することになったのだが，このシリーズでは試験的に様々なことが行なわれている。使用しないデバイスドライバや機能をすべて排除し，システム構成をゲートウェイとして動く最低限の設定にした。カーネルはバージョン1.1.59のものを用いた。これはその時の1.1シリーズの最

表－1　コンピュータの構成

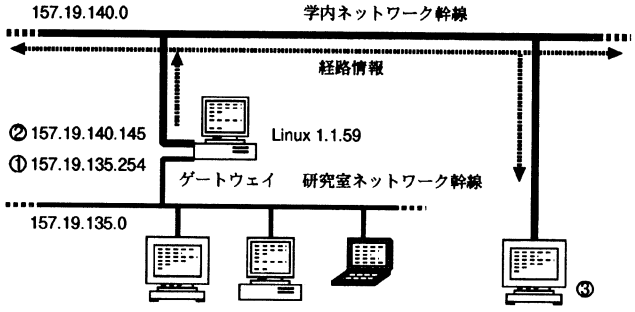
		備考
機種名	東芝J3100PV2 433	
CPU	i486SX	数値演算プロセッサなし
動作周波数	33MHz	
主記憶容量	16MB	
バス	ISA	
拡張バス	ISA×3	その内VL×1
ハードディスク容量	80MB×2	IDE
ファレキシブルディスク	3.5inch×1	1.44MB または1.2MB
イーサネットカード	3COM 3C509×2	ゲートウェイにするためは2枚必要

新版である(現在はその後のバージョンアップによりSlackware 2.1，カーネル 1.2.8 を用いている。カーネル 1.2シリーズは 1.1シリーズを安定化させたものである)。その他については，スワップエリアとして24MB確保したので，仮想メモリ全体で40MBになった。

ここまでの状態を図－2に示す。当研究室に割り当てられたネットワークアドレスは 157.19.135.0 である。研究室内のコンピュータは157.19.135.1～157.19.135.254の範囲のアドレスをつけることになる。構築したゲートウェイには157.19.135.254を割り当てた(図－2 ①)。学内幹線のアドレスは157.19.140.0である。同様に254個のアドレスのうち当研究室に割り当てられた範囲の中から構築したゲートウェイにアドレスを割り当てた(図－2 ②)。

TCP/IPネットワークでは経路制御はRIP(Routing Infomation Protocol)を使用して動的に行うのが一般的である[8]。RIPを使用しないで静的に制御する方法もあるのだが，静的な制御ではシステム管理者が経路情報テーブルを管理しなければならず，手間がかかる割に柔軟な制御ができない。一方，動的な制御ではパケットの通り道を場合に応じてRIPが最適化するので，回線の故障などがあっても他に回避できる回線があれば自動的にそれを選択できる柔軟性がある。

経路制御における我々の方針としては，研究室内では外側へ通じる箇所がこのゲートウェイだけであり経路情報は固定されていてるので，研究室内に経路情報を流すのは冗長であり無駄なトラヒックである。そのため研究室内では静的な経路制御にしたい。反対に，学内幹線は動的な経路制御がなされているため，それに対応して研究室外では動的な経路制御にしておく必要がある。この方針を満足させることができる経路制御プログラム(gated。バージョンは 3.5alpha7。フリーソフトウェア)があるので，それを使用することにした[9]。



図－2　ネットワークの構成

3. 動作確認実験

動作確認実験として，次のことを行なった。

・gatedのトレース

・経路情報が外部に正しく送信されているかの確認

3．1　gatedのトレース

gatedのトレースは起動時にトレースモードを指定すると行なうことができる。トレース情報を用いて確認することは，外から流れてきた経路情報がシステム内に正しく反映されているか，当研究室の経路情報が正しく外側へ流れているか，の２点である。トレース情報から目的の部分を抜粋したものを図－3に示す。

図－3 ①のtask_send_packetを含む行が，外側のネットワーク(この場合はネットワークアドレス157.19.140.0のブロードキャストアドレス157.19.140.255)に対して経路情報を送信していることを示している。length24という記述があるので24バイトの大きさのパケットを送信していることがわかる。同様な情報をgatedのメモリダンプを得ることによっても得られる。図－4にメモリダンプの送信部分を示す。こちらの方がもっと具体的である。ゲートウェイの外側の

```
Apr 7 16:52:31 task_set_option: task RIP.0.0.0.0+520 socket 6 option TTL(18) value 1
Apr 7 16:52:31 task_send_packet: task RIP.0.0.0.0+520 socket 6 length 24 flags MSG_DONTROUTE(4) to 157.19.140.255+520
                                                                                    ①
                                        .
                                        .
                                        .
Apr 7 16:52:32 task_receive_packet: task RIP.0.0.0.0+520 from 157.19.140.130+520 socket 6 length 504
Apr 7 16:52:32 adv_destmask_match: no match for 202.31.224/255.255.255 found
CHANGE 202.31.224 255.255.255 gw 157.19.140.254 Kernel pref 254/0 metric 0/0 eth0 <NoAdvise Int HoldDown Gateway>
ADD 202.31.224 255.255.255 gw 157.19.140.130 RIP pref 100/0 metric 10/0 eth0 <Int Active Gateway>
                                                                                    ②
Apr 7 16:52:32 adv_destmask_match: no match for 202.25.192/255.255.255 found
CHANGE 202.25.192 255.255.255 gw 157.19.140.254 Kernel pref 254/0 metric 0/0 eth0 <NoAdvise Int HoldDown Gateway>
```

図－3　gatedのトレース情報（一部抜粋）

インターフェース（アドレス157. 19. 140. 145)からそのブロードキャストアドレスに内側(ネットワークアドレス157. 19. 135. 0)の経路情報を送信していることを示している。

```
157.19.140.145    ->    157.19.140.255        Interface:    157.19.140.145 (eth0)
                        Flags: <Poll Broadcast Supply Policy>
                        Bit: 4
                        Routes:
                                157.19.135/255.255.255 metric 1
```

図－4　gatedのメモリダンプ（一部抜粋）

そして，図－3 ②のtask_receive_packetを含む行が，外側のゲートウェイ(アドレスは157.19.140.130)から情報を受けとったことを示している。後に続く部分は受けとった情報を基に経路情報テーブルを変更している部分である。外部の経路情報がシステム内に結果的に正しく反映されているかを調べるのにシステムが持っている経路情報テーブルを見るという方法がある。これはnetstatというコマンドを用いると見ることができる。図－5に構築したゲートウェイの経路情報テーブルの一部を示す。図中の実線より下の部分が外側から流れてきた経路情報である。上の部分はそれぞれ上からループバック，外側のネットワーク(図－2 ②)，内側のネットワーク(図－2 ①)を示している。

Kernel routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
loopback	*	255.0.0.0	U	0	0	1455366	lo
157.19.140.0	*	255.255.255.0	U	0	0	233762	eth0
157.19.135.0	*	255.255.255.0	U	0	0	238101	eth1
157.19.143.0	157.19.140.130	255.255.255.0	UG	0	0	0	eth0
157.19.134.0	157.19.140.254	255.255.255.0	UG	0	0	21	eth0
157.19.144.0	157.19.140.254	255.255.255.0	UG	0	0	0	eth0
202.26.147.0	157.19.140.254	255.255.255.0	UG	0	0	0	eth0
202.26.146.0	157.19.140.254	255.255.255.0	UG	0	0	0	eth0
202.252.67.0	157.19.140.254	255.255.255.0	UG	0	0	0	eth0

図－5　ゲートウェイの経路情報テーブル（一部抜粋）

3．2　外部への経路情報の伝達確認

構築したゲートウェイから送信された経路情報が正しいか調べるために，UNIXマシンを当研究室が接続している幹線に接続し経路情報を受信させた(図－2 ③)。このコンピュータで受信できればその他のコンピュータやゲートウェイでも受信できていると判断できる。そのUNIXマシンの経路情報テーブルを図－6に示す。図中，枠で囲まれた部分がこのゲートウェイから送信された経路情報を示している。当研究室のネットワークアドレス157.19.135.0が登録されているの

がわかる。その後，このUNIXマシンと研究室のコンピュータの間で，telnet，ftp等のネットワークアプリケーションを使用してみたが問題はなかった。以上のことから，Linuxがゲートウェイとして正しく動作していることが確認できた。

Routing tables

Destination	Gateway	Flags	Refcnt	Use	Interface
localhost	localhost	UH	0	19144	lo0
192.244.160.0	157.19.140.254	UG	0	0	le0
192.218.136.0	157.19.140.254	UG	0	0	le0
192.50.8.0	157.19.140.254	UG	0	0	le0
163.48.0.0	157.19.140.254	UG	0	0	le0
157.19.135.0	157.19.140.145	UG	0	562	le0
202.250.208.0	157.19.140.254	UG	0	0	le0
202.32.8.0	157.19.140.254	UG	0	0	le0
202.26.48.0	157.19.140.254	UG	0	0	le0
202.24.48.0	157.19.140.254	UG	0	0	le0

図－6　経路情報テーブル（一部抜粋）

4．構築したゲートウェイの性能評価

構築したゲートウェイの性能評価としてftp(File Transfer Protocol)のデータ伝送時間を調べてみた。実験におけるワークステーション，ゲートウェイの位置関係を図－7に示す。転送に使用したのは441603バイトの画像データである。これを数回転送しその転送時間を測定した。測定値はftpコマンドの出力を用いた。ワークステーションの負荷，ネットワークトラヒックを考慮して，測定した中から最も良かったものを測定値とした。実験結果を表－2に示す。

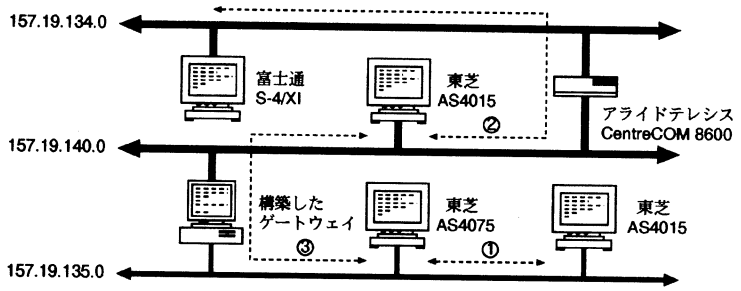
同じ幹線に接続されているワークステーション間で行なった場合(図－7 ①の場合)はおよそ1200K byte/sの転送速度が得られた。間にゲートウェイ専用機(アライドテレシス製

表－2　転送実験結果

	ケース①	ケース②	ケース③
通信速度（K byte/s）	1200	1000	790

CentreCOM 8600[12]）を介しての場合（図－7 ②の場合）はおよそ1000K byte/s，このゲートウェイを介した場合（図－7 ③の場合）は790K byte/sだった。我々が構築したゲートウェイの転送速度はゲートウェイ専用機のおよそ8割の通信速度である。

さらに，構築したゲートウェイのコンピュータ資源の消費状況を調べてみた。調査にあたりyamm(Yet Another Micro Monitor)というフリーソフトウェアを用いた。このソフトウェアではメモリの使用状況，ロードアベレージ，アイドル時間(何も処理しない時間)，デーモンの状態をモニターすることができる。結果として，メモリ空間40 MB(その内実メモリ16 MB)のうちの36%(約14 MB)が常に使用されていた。この消費量だと常に実メモリに余裕がある。アイドル時間は平均して約95%であった。



図－7　転送速度測定実験

5．まとめ

今回行なったゲートウェイの構築では，我々の方針を満足させるだけのものができたといえる。動作に問題がないことが実験によって確認できたし，性能，安定性も十分である。

今回表－1のコンピュータとLinux用いてゲートウェイを構築したのだが，この構成でのコン

ピュータ資源の消費状況がメモリについては35.6%と低い数字で，実メモリにも少し余裕がある。実メモリは16MB用意したのだがこれでちょうど良いといえる。アイドル時間も約95%であった。この状況だと，まだ全体的に余力があると考えられる。ゲートウェイのOSにLinuxを用いたことについては，その動作を保障してくれるものがなく(特にネットワーク関連)，最初は不安であったが，実際使用してみると商用のUNIXと比べてもそれほど遜色なく，快適な作業環境を与えてくれた。

通信速度については，ゲートウェイ専用機の8割程度の通信速度であった。この数値に関しては，それほど問題があるとは感じない。World Wide Webのクライアント(Mosaic，Netscape等）やftp等のネットワークアプリケーションを使用してみたが，学内のサーバにアクセスする分については特に遅いと感じたことはない。ゲートウェイの性能はデバイスドライバやCPUの性能に依存している部分があるのでもう少し改善できる可能性がある。また，今回使用できなかったFreeBSD，NetBSDの方でも我々が使用したイーサネットカードがサポートされたようなので，OSをこちらに変更して性能の比較を行なうことも可能となってきた。

そして，安定性についてであるが，当研究室にはネットワークに接続されているコンピュータが10数台ある。研究室外にアクセスするのは多くても同時に5台程度であり，また，電子メールに関しては，常時受け付けているがそれほど頻繁にメールが送られてくるわけではない。全体的に見ても構築したゲートウェイを通るトラヒックはそれほど多くない。このような環境において，1994年9月から1995年5月までのおそよ9カ月間様子を見てみたが，このゲートウェイがパニックを起こしたことはなく，このゲートウェイを介して転送したデータやプログラムが壊れたこともない。安定性は十分であるといえる。

構築したゲートウェイの性能を調べてみて思っていたよりも余裕があったので，最初のゲートウェイとして専用に使用するという方針を変えてネットワーク・プリントサーバの機能も追加した。ゲートウェイのシリアルポートとパラレルポートにそれぞれレーザ・プリンタ，シリアル・プリンタを接続して設定を行なった。この機能を追加したあとでもメモリの使用量，アイドル時間が占める割合はほとんど変わらなかった。

今後の計画として，研究室外からのアクセスを拡張するという意味で，電話回線から研究室のコンピュータにアクセスできるように，今回構築したゲートウェイをダイヤルアップPPP[11]のサーバに再設定することを考えている。PPPというプロトコルを用いることによって電話回線を介してTCP/IPで通信を行なうことができるのである。これによって大学に登校してこなくても電子メールやネットニュースを利用できるし，演習・実験の課題なども大学のコンピュータを好きな時間に利用して行なうことが可能となる。

また，学内ネットワークに接続した以上（これはインターネットに接続したことと等価である），ネットワークセキュリティについても考慮する必要があると考えている。研究室外から研

究室内のコンピュータにアクセスするためには，ゲートウェイを通らなければならない。研究室ネットワークのセキュリティを高めるにはゲートウェイに何らかの機能を付加して，例えば，パケットフィルタリングゲートウェイ，アプリケーションゲートウェイなどのファイアウォールにする方法がある[13]。セキュリティ強化と作業環境の快適さは表裏一体でありそのバランスが難しい。「保護すべき資源は何か？」，「コンピュータシステムを誰から守るのか？」，「セキュリティにどれだけの代償を払えるか？」といったことを十分検討してセキュリティ対策を立てる必要があると思われる。

謝　辞

学内ネットワークへの接続に関して協力して下さいました本学CRDセンターの黒島 利一技官に深謝します。

参 考 文 献

1） 寺崎仁司：平成5年度室蘭工業大学卒業論文, 35-55(1994)
2） 宮川 晋：はやわかりPC-UNIX, 43-50(共立出版社, 1994)
3） 宮川 晋：はやわかりPC-UNIX, 52-97(共立出版社, 1994)
4） 石橋 勇人：UNIX USER, 2, (8), 125-127(ソフトバンク社, 1993)
5） 胡桃：UNIX USER, 3, (1), 48-55(ソフトバンク社, 1994)
6） 鵜飼 文敏：UNIX USER, 3, (1), 56-62(ソフトバンク社, 1994)
7） 山田 圭：UNIX USER, 3, (7), 37-44(ソフトバンク社, 1994)
8） 山口 英：UNIX MAGAZINE, 8, (3), 25-37(アスキー社, 1993)
9） 山口 英：UNIX MAGAZINE, 8, (4), 47-61(アスキー社, 1993)
10） 宮川 晋：UNIX MAGAZINE, 9, (8), 71-78(アスキー社, 1994)
11） 大野 俊治：UNIX MAGAZINE, 10, (2), 33-44(アスキー社, 1995)
12） アライドテレシス株式会社：CentreCOM 8600 マネージメントガイド, 2.1-2.5(1994)
13） William R. Cheswick, Steven M. BellovinZ, 監訳 川副 博, 訳 田和 勝, 鎌形 久美子：ファイアウォール, 51-118(ソフトバンク社, 1995)