Firewall 導入奮闘記

松元 隆二
情報工学部 知能情報工学科

平成 13 年 3 月 21 日
改訂平成 13 年 5 月 22 日

1 はじめに

インターネット上には、他人の計算機をダウンさせたり、他人のデータを改竄してまわるのを楽しみとしている Cracker が多数存在する。日本国内でも平成 12 年 1 月頃に中央省庁の Web ページが改竄される事件が多発した。最近では、平成 13 年 1 月下旬から、「UNIX のネットワークツール (bind) のセキュリティホールを使った不正侵入」、「Windows の Web サーバのセキュリティホールを使った Web ページ改竄」が多数報告されている。

Cracker からの攻撃を防ぐためには、絶えずセキュリティ情報を収集し、セキュリティホールを塞ぐ事が大切である。だが、受動的な対策だけではなく、能動的な対策も提案されている。 Cracker の攻撃を未然に防ぐ手段である。その一つとしてインターネット **Firewall(防火壁)** という技術がある。 (以降 Firewall と書く) インターネットと内部ネットワークの境界に様々な技術を使って強固な壁を作り、 Cracker の侵入を困難にし、内部ネットワークの計算機のセキュリティホールを攻撃されないようにする技術である。非常に効果が高い技術の一つである。

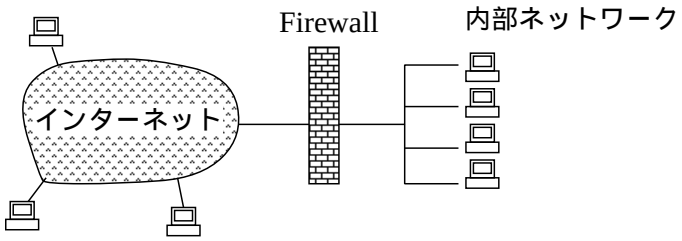


図 1: Firewall イメージ図

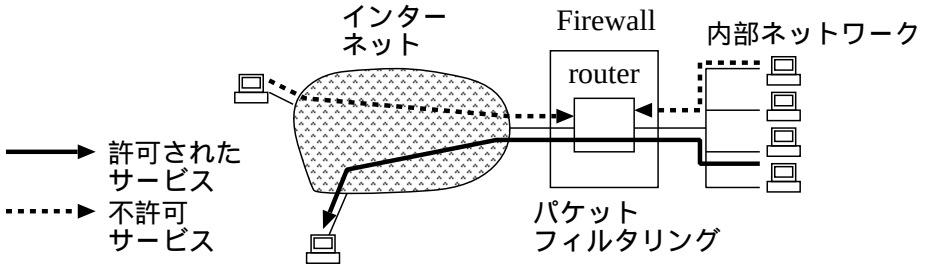
中央省庁の Web ページ改竄事件後、企業だけではなく公共機関でも Firewall の必要性が問われはじめている。今回、私の所属する講座で Firewall を構築し、それを紹介する。

2 Firewall で使われる技術

Firewall で使われる代表的技術を紹介する。

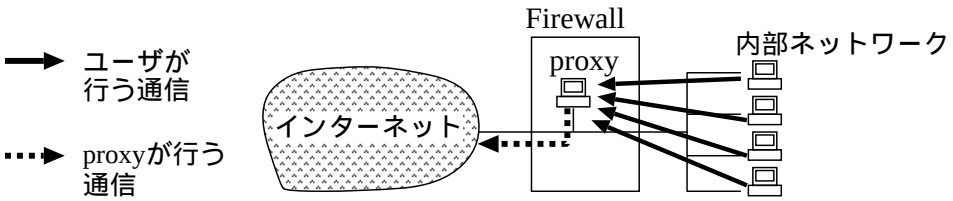
2.1 パケットフィルタリング

近年の最新サーバ OS では標準でを使い router を構成すると、設定により許可された発信・受信 IP アドレスと、許可されたサービス (telnet/http/ メール) のみを通過させ、許可されない発・受信 IP アドレスお



許可されたサービスは router を通過出来る。
不許可サービスは router で遮断される。

図 2: パケットフィルタリング



内部ネットワークの全員が、インターネットのサービスに
アクセスできるが、インターネットからは一台のみが見える。

図 3: proxy サーバ

よびサービスを遮断する事ができる。このような技術をパケットフィルタリング [1]という。例えばセキュリティ上好ましくない通信 (遠隔地への telnet、 pop3 等) を遮断したり、協同研究などで、特定の大学のみ通信許可を与え、それ以外からは通信を遮断するという設定が可能である。

2.2 proxy サーバ

内部ネットワークのユーザにインターネットへの直接通信を許可すると、不必要な情報が洩れたり、 router の設定が複雑になる。直接通信を防ぐために **proxy**(代理) サーバという技術がある。サービスを中継出来る。代表的なサービスは proxy がすでに開発されている[2]。

代表的な使い方を挙げると、 http(Web ページ) の proxy がある。内部ネットワークのユーザが Web ブラウザ (Netscape 等) で http proxy サーバの設定を行うとユーザは proxy サーバとしか通信を行わないが、インターネットのどのマシンへも間接的に通信可能である。インターネット側から見ると、 proxy サーバ一台のみが通信しているように見える。

また、パケットフィルタリングの弱点として、限定されたサービスのみを通過させるという設定ができるが、サービスの偽造が可能である。例えば Web サーバへの通信のふりをして、 telnet が可能。そのため、通信内容の検査も必要である。 proxy サーバでは検査が可能である。

2.3 強度の強いユーザ認証

インターネットのほとんどのサービスは通信内容が暗号化されない。だがインターネットは router で通信内容の盗聴が可能。実例を挙げると「知能情報工学科内 ↔ 学科外」の通信は、知能情報工学科の計算機

[1] FreeBSD・ NetBSD・ OpenBSD・ Linux などでは標準で提供されている機能。 Solaris・ SunOS4 等では提供されていないが、 ip-filter などのフリーソフトを使う事により可能。

[2] http の proxy としては squid が有名。汎用 proxy サーバとしては fwtk が有名

室の router で全て盗聴可能。「学内 ↔ 学外」の通信は情報科学センターの router で盗聴が可能である。

Cracker により不正に通信の盗聴されると、ユーザ認証の情報を盗まれる。例えば、あるマシンへ login するために telnet でパスワードを入力したり、メールを受信するために pop3 サーバにパスワードを送信すると、パスワードを盗まれる。

この問題を回避するために、いくつかの方法が提案されている。

- 常に暗号化

  システムとしては容易に見えるが、結局の所、暗号化された通信経路を確立するためのパスワードが必要。そのパスワードを交換するのに「公開 / 秘密鍵」等難しい技術が使われるので詳細は省略する。実装例として login の認証を行う **ssh**[3] がある。

- パスワードを使い捨てにする

  システムとしては、パスワードの種となるパスワード (パスフレーズ) を事前にサーバに設定する。ユーザ認証する時に、パスフレーズから一定の規則に基づきパスワードを生成する。このパスワードは使い捨てであり、次回のユーザ認証には使えない。したがって Cracker にパスワードを盗聴されても不正侵入には使えない。実際の実装では、アプリケーションが使い捨てパスワードを自動生成する場合が多いので、ユーザは使い捨てである事を認識できない事が多い。実装例として login や ftp の認証を行う **s/key, otp**, メールの受信の認証を行う **apop** がある。

3 事のはじまり

平成 12 年 3 月頃、所属講座の教授より、近年 Internet 上で Cracking 行為が多発しているので、 Firewall を設置するように指示された。

私自身も、近年の Cracking 行為の多さを見兼ねていた事もあり、当講座でも SPAM 攻撃 (メールサーバの不正利用) の被害にあった事もあり、喜んで引き受けた。

4 設計段階

4.1 ネットワーク構成

旧来のネットワークは図 4の通りである。ネットワーク的にはインターネットへは直接接続を行っていた。Firewall 導入にあたり図 5のように変更する計画を立てた。

変更にあたり「Firewall 専用ネットワーク」と計算機 2 台が (proxy サーバと新 router) 新たに必要になった。旧 router は 8 年前の機種のため、能力的に不満があり、新たな計算機に交換する事にした。ネットワークについては公共の資源のために、学科の計算機管理室の許可なく使用出来ない。新たに割り当てをもらえないかと何回か担当教授と話合いを行った。当初は、学科では使ってないネットワークが幾つかあったので、すぐに割り当ててもらえると考えていた。また詳細な Firewall 計画書を作成し、提出していた。しかし割り当てにはかなり時間が必要だった。

今回の設計では、「Firewall 専用ネットワーク」が必要な設計を行なったが、可能なら必要でない設計の方が短時間で導入出来ると思う。その代わり、 router の設定が複雑怪奇になり、 Firewall の強度が劣る。

4.2 通信規制について

次のような方針にした。

- 講座内からインターネットへの通信: 制限は極力緩めにする。

  Proxy の使用を推奨するが、未使用でも直接インターネットへの通信を許可する。

[3] ssh は、バージョンが二つある (Ver.1.*, Ver.2.*)。互いに互換性無し。センターで使っているのは Ver.2.* である。しかし Windows で使われている ssh のツールは Ver.1 にしか対応してない場合が多い。どちらを使うかは、十分検討の必要あり。

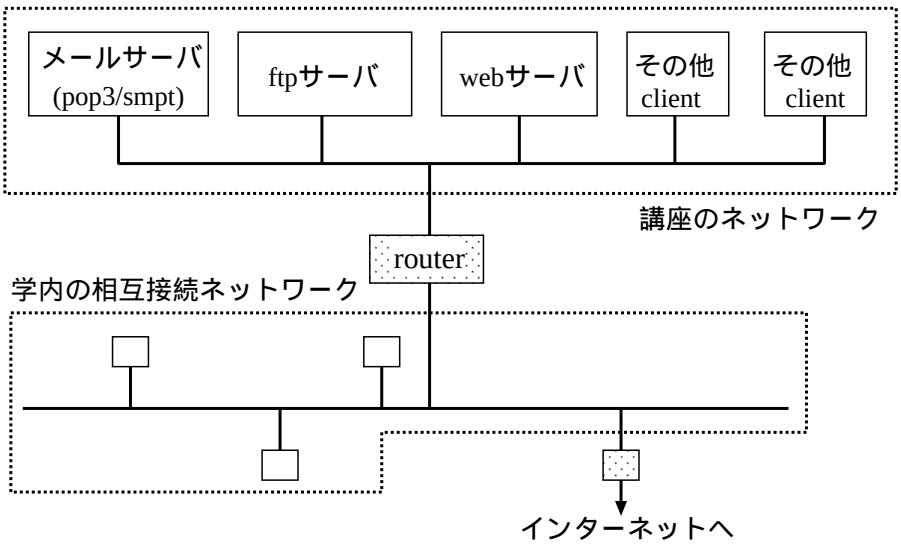


図 4: 旧来のネットワーク構成

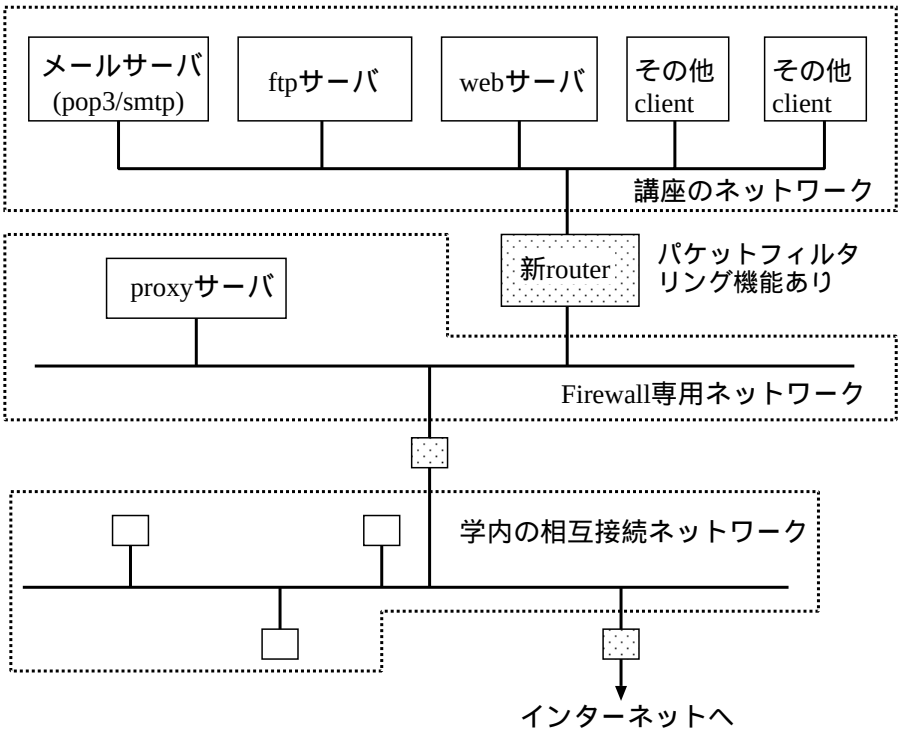


図 5: 新しいネットワーク構成

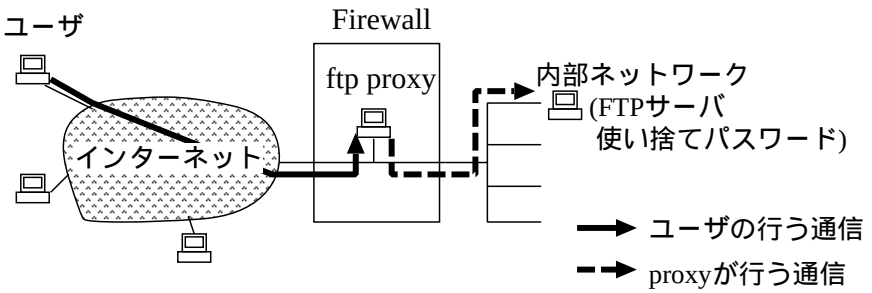


図 6: ftp proxy サーバ

- インターネットから講座内への通信: 厳しく制限する。

  学内学外の区別なし。現状の他学科、他講座のネットワーク管理体制を見ると、学内を無条件に信用すべきではないと判断した。

  特定の通信のみ許可。例えば、メールについては、メールサーバでメールの通信のみ許可。

4.3 設計で苦労した点

ユーザからインターネットから ftp を使えるようにして欲しいという意見が出た。 ftp というのはファイル転送を行うだけなので簡単な通信に見えるが、複雑な通信を行うため、簡単に Firewall を通過させる事ができない。数種類を試した結果、図 6のように proxy サーバで ftp を受け付け待機させ、受け付けた ftp を proxy で講座内に転送させ、ユーザ認証は使い捨てパスワード[4]で実現した。通常の proxy サーバとは逆の設定である。認証方法を増やすのは極力避けたかったのだが、仕方がない。参考書等でよく紹介される「ssh を使った port forwarding」は技術的問題で使用出来なかった。

次に、メール関係で、メールの取り込みを行う pop3 サーバとメールの送信を行う smtp サーバの提供を求められた。 pop3 サーバはそのままだとパスワードが盗聴される。それを防ぐために使い捨てパスワードを使う apop 等が提案されているが、対応メールリーダの問題[5]があり apop 採用は断念した。試行錯誤した結果、ユーザに pop3 専用のパスワードをつけてもらう事にした[6]。このパスワードは UNIX の login パスワードと同じにされるとセキュリティが劣るので、検査機能を付けた。

5 移行段階 1

ネットワーク構成を次の段階で変更した。

旧来の router を設置したまま、新 router を設置した。つまり 2 台ルータを設置した。旧 router が受け取った通信を全て新 router に投げるようにした[7]。そして、新 router の動作テストをしばらく行った。

6 構成変更

新 router のテスト中に、教授に、 Web サーバは Firewall の外にあるべきだと指示された。その通りである。一般的にも Web サーバは外に置くべきである。

Web サーバは Cracker からの攻撃対象になる事が多い。はじめに挙げた中央省庁の Web ページ改竄事件もしかり。危険な物は内部ネットワークの外に出して危険を最小限に抑えるという考えである。万が一 Web サーバが Cracking されても被害は Web ページだけで、ユーザの研究データなどは守られる。

---

[4] ftp サーバとして wu-ftpd、使い捨てパスワードのツールとして opie を使用。

[5] Microsoft OutlookExpress は、 Mac 版は apop 対応だが、 Windows 版は apop 未対応。

[6] qpopper-3.1 をベースに独自に改造した pop3 サーバを使用。改造パッチが必要でしたら御連絡ください。

[7] 旧 router でルーティングデーモンを停止後、 default router を手動で設定すればよい。

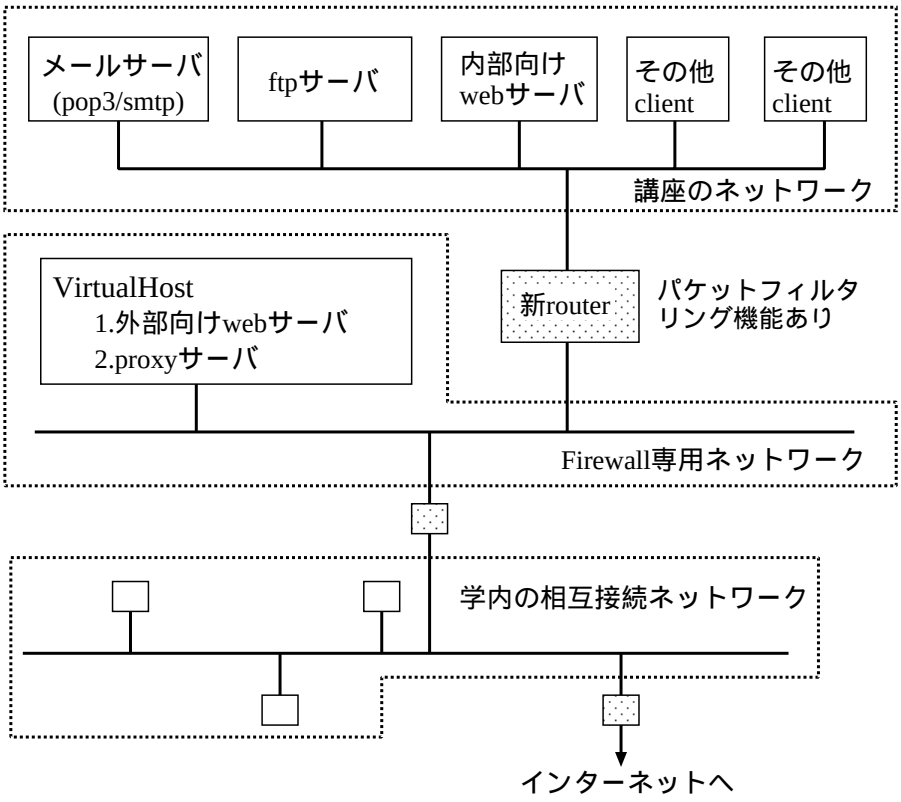


図 7: 新しいネットワーク構成 (改)

次に、新 router でパケットを監視していると、学内からも Cracking と思われる通信が行われていた。発信元に調査を依頼すると、学生がネットワークを検査するツールを走らせていたようである。また、最近、講座内でウイルスが蔓延していた。ウイルスの中にはインターネットと通信するものもある。

その事をふまえて、図 7のように変更した。

- インターネット向け情報提供用 Web サーバを講座外へ新設

  インターネット向け Web サーバへの login は ssh でのみ可能とした。

- 講座内からインターネットへの通信

  直接通信は一部を除いて禁止。基本的に proxy を使ってインターネットと通信する。そして通信記録を残すようにする。

この変更によって新たに Web サーバ用計算機が必要となった。新たに計算機購入を考えたが、 FreeBSD-4.0R 以降を使うと、 Virtual Host を容易に設置出来る事がわかり、 VirtualHost で proxy サーバと兼用する事にした。

7 移行段階 2

次の段階として、旧 router を取り外し、新 router のみでの運用にする事にした。この段階では通信規制を行なっていない。当講座では、土日問わず学生教官が研究活動を行っているので、移行作業時期決定は難しいかった。作業時間も長時間が予想される。そのため、文化祭期間中に移行作業を行った。

移行作業後、 VirtualHost 上に Web サーバと proxy サーバを仮設置し、 Firewall の準備はほぼ整った。次の段階として、通信制限を行った。通信制限を行うに当たって Web ページに Firewall の詳細なマニュアルを作成した。

通信制限にあたり、猶予期間を 5 日間とって、 Web ブラウザ等で直接通信を停止し proxy サーバを使うよう設定変更を指示を出した。 5 日間はとても短時間に思われるが、猶予期間は長めに設定しても無駄。以前講座のメールサーバ移動作業を行った時、猶予期間を 2 週間とした。ほとんどのユーザは 2-3 日中に変更を行ったが、少数のユーザは、いつまでも変更を行わななかった。 1 週間過ぎても同様。結局〆切前日に口頭で変更するよう注意して回った。移行期間は長くしても無駄。

通信制限開始後も、 proxy を経由せず、直接通信を試みているユーザが多数存在しましたが、情報工学部の学生なので、ほっといても自力解決するはずである。というのはダメかもしれない。

8 Firewall 設置後

設置後様々なトラブルが発生した。主なトラブルについて述べる。

proxy サーバ過負荷 夜間のみ proxy サーバの LAN カードがエラーを起こす。原因を調べると、夜間巨大ファイルを download しているユーザが居た。カーネルパラメータを調整する事によりエラー発生を回避出来た。

ログを見る限り、極少数のユーザが proxy サーバの資源の大部分を使っている。負荷のかけ方にもよるが、ユーザの需要に合わせて proxy サーバを増強するより、帯域制限をかけた方がいいのではと思う。学外へのネットワーク帯域は大学共通の資源である。

LAN カード相性 proxy サーバを経由しての通信速度が内部ネットワークの OS により通信速度が異なる。原因を探ると router の LAN カードの相性問題だった。 100BASE-Tx の LAN カードから 10BASE-T の LAN カードに変更すると、通信速度が改善された。 router には Pentim 75[MHz] の低速マシンを使っていたので、 100[MBPS] の帯域はさばき切れなかったのではないかと考えられる。後日 router の増強を行った。 Pentium Pro 200[MHz] に変更した所、 100[MBPS] の帯域を十分さばききれるようになった。

教務情報システム 平成 12 年度後学期から情報工学部では Java による教務情報システムでの成績報告が行われるようになった。当然ながら講座内からも使いたいという要望が出た。 proxy を経由した通信で対応したかったが、教務情報システムは仕様が公開されたサービスではなく、 proxy にも未対応のため、不可能だった。だが、教務情報システムは、特定のマシンのみと通信を行うため、パケットフィルタリングで特定マシンとの通信を解放するという設定変更で対処した。

ftp proxy 苦労して設置した ftp proxy だが、設置後一ヶ月程度全くユーザが使用していなかった。ある日助教授が質問に来て、マニュアルに不備がある事が判明した。使い捨てパスワードの生成コマンド (otp-md5) は、 remote login での実行が認められていない事実を記入していなかったために、使い捨てパスワードの生成が出来なかったためだった。私はその事を知っていたために無意識に remote login を回避していたので気がつかなかった。マニュアルを書くのは難しい。

9 おわりに

どうにか Firewall を完成できた。経費として 20 万程度使用し、ユーザに様々な不自由を強要した。教授の発案だったからこそ完成可能だったのではないだろうか？。技官からの発案だとかなり困難を極めただろう。また完成までに、 9ヶ月近くかかり、教授の叱咤を受けた。しかし Howto ができたので、次回 Firewall を構築する機会を与えられたら、短期間で構築可能であろう。ユーザの協力が得られればだが。

最後に Firewall はネットワークの全ての脅威に対して万全ではないことに注意してほしい。 Cracker は新たな攻撃手段を探して虎視眈々としている。例えば router のセキュリティホールを使ってパケットフィルタリングを無効にするかもしれない。ウイルスに Cracker の仕掛けた罠が含まれるかもしれない。内部ユーザが Web ページから誤ってウイルスを取り込んでも Firewall は無力である。検査は不可能。またメー

ルに含まれるウイルスが蔓延しているが、同様に Firewall はメールにウイルスが含まれるか含まれないか検査は不可能[8]。

謝辞

Firewall の設計構築という、技術的に興味がある事をやらせてくれた岡田教授、査読に協力していただいた井本技官、文献 [1] を貸してくれた本田技官に感謝いたします。

参考文献

[1] D.Brent Cbapman, Elizabeth D.Zwicky, 「Building Internet Firewalls(2nd Edition)」, O'Reilly, ISBN1565928717. (第 1 版の邦訳: 鈴木充彦訳, 「ファイヤウォール構築 インターネットセキュリティ」, オライリー・ジャパン, 1996 年, 5200 円, ISBN-4-900900-03-06)

[2] 一條博, 「ファイヤウォール構築ガイド (第 2 版)」, テクノプレス, 2000 年, 2500 円, ISBN-4-924998-41-9.

参考データ

Firewall 機器のスペックについて。

- VirtualHost のサーバ
  - CPU:「PentiumIII 550Mhz/Mem256M」、 NIC:「3Com 3c905B」、 OS:「FreeBSD-4.2R」。
  - OS の提供している VirtualHost(jail) 環境を使い proxy と Web サーバを構築
- 新 router
  - CPU:「Pentium75Mhz/Mem24M」、 OS:「FreeBSD-4.2R」。
  - NIC(内側ネットワーク側): 「PCMCIA: IO-DATA PCETTX」
    (相性問題が出るので「PCMCIA: IO-DATA PCLA/T」に変更した。)
  - NIC(インターネット側): 「PCMCIA: IO-DATA PCLA/TE」。
  - ノートパソコンなので、 UPS 附属:-)
- 新 router(増強後)
  - CPU:「Pentium Pro 200Mhz/Mem128M」、 OS:「FreeBSD-4.2R」。
  - NIC(内側ネットワーク側): 「Intel Ether ExpressPro100」。
  - NIC(インターネット側): 「DEC 21140 Fast Ethernet」。

使用したソフトウエアについて。

- squid: 高性能 http キャッシュサーバ
  `http://www.squid-cache.org/`
- ip-filter: 汎用 OS パケットフィルタリングツール
  `http://coombs.anu.edu.au/~avalon/ip-filter.html`
  64bit CPU 環境の Solaris7,8 では gcc でコンパイル不可。バイナリを所有していますので、相談してください。

[8] 商用ソフトを買えば対応可能。

- fwtk: 汎用 proxy サーバ
  http://www.fwtk.org/
- otpi: 使い捨てパスワード
  ftp://ftp.st.ryukoku.ac.jp/pub/security/tool/opie/
  一次サイト不明。
- wu-ftpd: ftp サーバ
  http://www.wu-ftpd.org/
- qpopper: pop3 サーバ
  http://www.eudora.com/qpopper/
- ssh: Secure shell
  http://www.ssh.com/
  商用ソフト。
- openssh: ssh の Free 版。
  http://www.openssh.org/
  商用の ssh とは一部互換性で問題あり。