Living with FreeBSD

1 FreeBSDについて

2 FreeBSD 4.10-R のインストール

3 インターネット常時接続について

4 基本的な操作方法

5 DNSの設定

6 Web Serverの設定

7 FTP Serverの設定

8 Mail Serverの設定

9 セキュリティについて

10 参考資料

1 FreeBSD について

1.1 FreeBSDとは

386BSDから派生し、AT&TのUNIXライセンスからフリーなBSD[注1] 系のUNIX系OS。intel x86系(32ビット)、DEC alpha系(64ビット)システムで稼動し、安定性を重視している。同じBSD系には幅広いプラットホームで動き、先進的な機能を持つNetBSD[注2] 、セキュリティー技術に優れたOpenBSD[注3] などがある。

1.1.1 FreeBSDの歴史

http://www.ua.freebsd.org/ja/handbook/handbook.html#HISTORY

1.1.2 FreeBSDのVersionについて

CURRENT, STABLE, RELEASE の違い。最新のRELEASEは5.3と4.10。

注1 BSD [Berkeley System Distribution]

注2 NetBSD <http://www.netbsd.org/>

注3 OpenBSD <http://www.openbsd.org/>

2 FreeBSD 4.10-Rのインストール

2.1 インストール

2.1.1 BIOSでCD-ROMからの起動を設定し、インストールCD-ROMを入れ電源を入れる。自動的に"Kernel Configuration Menu"が開く。3つの選択肢の中から"Start kernel configuration in full-screen visual mode"をカーソルキーを使い選択し、リターンキーを押す。

2.1.2 この"visual mode"で明らかに不要なデバイスを外す。手動で外せるものはほとんどがISAやPCMCIA関連のものなので神経質になる必要はない。PCIやAGPのデバイスは自動的に検出される。

2.1.3 Storageからは"ATA/ATAPI compatible disk controller", "Floppy disk controller"以外を全てBackSpaceキーを使い削除する。Networkからは全て外す。Communications、Input、Multimediaはそのまま。Miscellaneousからは"PC-card controller"を外す。qを押し、その後yを押してvisual modeを保存終了する。

2.1.4 その後"/stand/sysinstall Main Menu"になる。

2.1.5 英語キーボードを使うのならば必要ないが日本語キーボードを使うにはまず"Keymap"を選択し、Japanese 106を選択する(カーソルキーで下がり、スペースキーで選択する)。

2.1.6 "Standard"を選び進むと"Message"が出るので、読んでOKを押す。

2.1.7 ここからFDISKでハードディスクのパーティションを設定する。今回はディスク全てをFreeBSDに使うので"A"で全てのディスクを選択し、"Q"で次のメニューに進む。

2.1.8 "BootManager"のメニューから"Standard"を選択する。

2.1.9 ここでディスクにパーティションを作れとメッセージが出る、OKで進む。次に"FreeBSD Disklabel Editor"でスライスを作成する。今回は下記のような設定で行う。

```
swap          300MB
/             300MB
/usr        5,000MB
/var        3,000MB
/tmp          500MB
/home        残り全て
```

2.1.10 "c"を押すとサイズを聞かれるので"300M"などとサイズを記入し進み、"partition type"はswap以外は全て"FS"を選択し進む。FSの場合、次にマウントポイントの指定をする。"/", "/home"などと記入し進む。ここまででは設定はまだハードディスクに書きこまれていないので"U"を押すことにより、元に戻すことが可能。

2.1.11 設定を終了するには"Q"を押す。

2.1.12 "Choose Distributions"では"Developer"を選択し、進む。Portsをインストールするかと出るが"No"とし、その後"Exit"で進む。"Choose Installation Media"ではCD/DVDを選択し、進む。

2.1.13 "User Confirmation Requested"から"Last Chance!"と出てくるので、"Yes"で進む。ハードディスクの設定がしばらくかかる。"ALT-F2"で進行状況を見ることが出来る、元に戻すには"ALT-F1"を押す。

2.1.14 終了と出て、ネットワークの設定をするかと出てからネットワークの設定になる。"Intel EtherExpress Pro/100"を選択し進む。IPv6が必要かと聞かれるので"No"を選択する。次にDHCPが必要かと聞かれるが、ここも"No"とする。

2.1.15 "Network Configuration"を記入する。Host:に"yebisu.beer.jp"と記入する、Domain:は自動的に"beer.jp"となる。IPv4 Gateway:は"192.168.0.1"、Name server:は"192.168.0.□"、IP Address:もは"192.168.0.□"とし、Netmask:は"255.255.255.0"とする。(□内は参加者番号を入れる)

>> 実際の設定の際はIPv4 Gatewayにはルータのアドレス、Name serverにはプロバイダーなどから指定されるDNSのアドレス、IP Addressには専用のグローバルまたはローカルアドレスを指定する。これらは/etc/rc.conf, /etc/resolv.confなどを直接編集して変更する事も可能。

2.1.16 次に"fxp0"を有効にするかと聞かれるので"Yes"とし進む。次にこのマシンを"network gateway"にするかと聞かれるので"No"で進む。

2.1.17 "inetd"と"simple internet services"を設定するかと出るので"Yes"とする。"inetd"を稼動させるかと出るので"No"とする。

2.1.18 "anonymous FTP"にするかと出るので"No"とする。"NFS server", "NFS client"はどちらも"No"とする。

2.1.19 "default security profile"を選択するために"Yes"とする。"system security profile"から"Medium"を選択する。その後、必要ならば"/etc/rc.conf"を修正するようにと表示される。

```
>> Security Profile

Medium
nfs_server              *
sendmail                YES
sshd                    YES
securelevel             NO

Extreme
nfs_server              NO
sendmail                NO
sshd                    NO
securelevel             YES (2)
```

2.1.20 "system console setting"は"No"で進む。"time zone"は"Yes"とし、次に"UTC(世界標準時)"に合わせるかと出るので"No"とする。"Asia"から"Japan"を選び、"JST"でいいかと出るので"Yes"を選ぶ。

2.1.21 "Linux binary compatibility"は"No"とする。"USB Mouse"が接続されているかには"No"とする。

2.1.22 "FreeBSD package collection"を見ますかと出たら"No"として進む。

2.1.23 "initial user accounts"を設定しますかで"Yes"とする。まず"Group"を選びGroup name:を"hotei"にし"OK"とする。次に"User"を選びLogin ID:に使用したいID、Group:は"user"、Password:は任意のパスワード、Full Name:には英語で名前、Member groups:には管理者になる必要があるので"wheel"、Home directory:には"/home/あなたのID"としOKする。"exit"で"User Account"から抜けられる。

2.1.24 次に"system manager's password"の設定を促される。6文字以上の同じパスワードを2回続けて入力する。このパスワードを忘れると何の設定も出来なくなるので注意が必要。

2.1.23 "Last option"の確認をするかで"Yes"としもう一度確認する。

2.1.24 "Exit"を選択する。"X Exit Install"を選択しインストールを終了する、確認のメニューが出るので"Yes"を選択する。BIOSの画面が出たらCD-ROMのイジェクトボタンを押しCD-ROMを抜いおく、そうしないとまたインストーラが立ち上がってしまう。

2.1.25 ログインメニューになればインストールは成功。

2.2 基本設定

2.2.1 ユーザ登録

```
# /stand/sysinstall
```

Configure -> User Management を選択しグループ、ユーザを作成する。作成したユーザ名でログイン可能か確認する。

2.2.2 rootへの変更

一般ユーザからsuコマンドを利用し、rootに変更することができる。ただしwheelグループに所属している必要がある。

```
% /usr/bin/su -
```

パスワード入力

```
#    ←スーパーユーザになるとプロンプトの記号"$"が"#"になることを確認する。
```

2.2.3 /etc/resolv.confの設定

/etc/resolv.confを設定し、ドメイン引きが出来るようにする。現在設定されている自己アドレスを一時使用停止し外部のDNSを設定する。DNSは最大3登録できる。

```
# vi /etc/resolv.conf
```

```
#nameserver 192.168.0.□
nameserver xxx.xxx.xxx.xxx
nameserver xxx.xxx.xxx.xxx
```

修正後、hostコマンドなどを利用しDNSにアクセスできることを確認する。

```
# host www.freebsd.org
```

2.2.4 viの設定

viの利用状態を分かりやすく表示する様に初期設定を行う。

```
# vi ~/.exrc
```

```
set showmode
set showmatch
```

3 インターネット常時接続について

3.1 フレッツ ISDN

ISDN回線のBチャンネル1つを利用して64kbpsで接続する。初期投資が安く、月々の利用料金も安い。プロバイダーによってはグローバルIPを利用できる。常時接続というよりは固定料金での接続利用となる。

3.2 ADSL[注4]

一般の銅線電話回線を利用し、数Mbpsまでの高速なインターネット接続が可能。上りと下りの回線速度が違うのが特徴。値段は安く、広く使われている。

3.3 CATV

CATV用の同軸ケーブルを利用し、数Mbpsまでの高速なインターネット接続が可能。サービス地域が限定されている。値段に関しては業者次第で複数のPCからの接続を認めない、法人は別契約などあり割高になる場合もある。

3.5 FTTH[注5]

郵政省とNTTが主導して90年代初めから計画されている次世代通信ネットワークで一般家庭にも光ファイバー網を引く計画。サービスが提供されている地域は広がりつつある。

注4 ADSL [Asymmetric Digital Subscriber Line]

注5 FTTH [Fiber To The Home]

4 基本的な操作方法

4.1 基本情報

■ WindowsやMacintosh(Mac OS 9まで)とUNIXの違い
■ GUIとCUIの違い
■ /(ルート)について
■ /とrootの違い
■ ディレクトリとファイル
■ /etc, /usr, /var, /home, /tmp
■ ホームディレクトリ
■ 起動状況 dmesg, ifconfig
■ マウントポイント /mnt
>> CD-ROMのマウント
```
# mount /cdrom
```
>> CD-ROMのアンマウント
```
# umount /cdrom
```
>> フロッピーディスクの使い方
/mntポイントにfloppyディレクトリを作る。
```
# mkdir /mnt/floppy
```
読み込むためにマウントする。
```
# mount -t msdos /dev/fd0 /mnt/floppy
```
/etc/fstabに下記の様に記入する事によりmount /mnt/floppyでのマウントが可となる。

```
/dev/fd0    /mnt/floppy     msdos   rw,noauto     0 0
```

■ shellについて echo $SHELL sh, csh, tcsh, bash
■ PATHについて echo $PATH /bin, /usr/bin, /usr/local/bin rootと一般ユーザのPATHの違い。
■ ユーザとグループの追加
```
# /stand/sysinstall
```
"Configure"より"User Management"を選択する。
他にもuseraddコマンドを使う、vipwを使うなどいくつかの方法がある。
■ rc.conf、/etc/rc.confと/etc/defaults/rc.conf

4.2 基本的なコマンド

4.2.1 コマンド

ls ディレクトリ内のファイルを一覧表示する

```
% ls        通常の一覧
% ls -l     詳細な一覧
% ls -a     隠しファイルを含むすべての一覧
% ls -F     ファイルタイプを表示しながらの一覧
            ls -laなど組み合わせての使用も可
```

pwd カレントディレクトリの絶対パスを表示する。

cd ディレクトリを移動する

```
% cd /etc   /etcに移動する
% cd ..     ひとつ上のディレクトリに移動する
% cd ~      ホームディレクトリに移動する
% cd -      直前のディレクトリに移動する
```

less ファイルを閲覧する。

```
% less apple.txt
            apple.txtを開く、qで終了する。
            カーソルキーまたはj、kで上下スクロール。
            スペースキーまたはctrl-fで1画面先へ、ctrl-bで1画面戻る。
            /apple (enter): appleという文字を下に向かって検索する
            ?apple (enter): appleという文字を上に向かって検索する。
```

cp コピーする

```
% cp melon.txt lemon.txt
            ファイルmelon.txtをlemon.txtという名前でカレントディレクトリにコピーする。
% cp melon.txt /tmp/lemon.txt
            ファイルmelon.txtをlemon.txtという名前で/tmpにコピーする。
% cp /tmp/melon.txt ./
            /tmpにあるファイルmelon.txtをカレントディレクトリにコピーする。
% cp melon.txt ../lemon.txt
            ファイルmelon.txtをlemon.txtという名前でひとつ上のディレクトリにコピーする。
% cp -r mango/ /tmp/mango
カレントディレクトリにあるmangoというディレクトリを/tmpにディレクトリごとコピーする。
```

mv 移動する

```
% mv melon.txt /tmp/
            カレントディレクトリにあるファイルmelon.txtを/tmpディレクトリに移動する。
% mv melon.txt lemon.txt
            melon.txtというファイル名をlemon.txtという名に変更する。
% mv mango/ /tmp/
            カレントディレクトリにあるmangoというディレクトリと/tmpに移動する。
```

mkdir ディレクトリを作成する
```
% mkdir mango
```
カレントディレクトリにmangoというディレクトリを作る。
```
% mkdir /tmp/mango
```
/tmpの中にmangoというディレクトリを作る。

rm 削除する。
```
% rm melon.txt
```
ファイルmelon.txtを削除する。
```
% rm -i aaa.txt
```
確認後、ファイルaaa.txtを削除する。
```
% rm -r mango
```
ディレクトリmangoを削除する。

chown 所有者を変更する。
```
% chown apple melon.txt
```
ファイルmelon.txtの所有者をappleに変更する。
```
% chown apple *
```
カレントディレクトリ内のすべての所有者をappleに変更する。
```
% chown apple mango
```
ディレクトリmangoの所有者をappleに変更する。
```
% chown -R apple mango
```
mangoディレクトリとその中のすべてのファイルの所有者をappleに変更する。
```
% chown apple:kobe melon.txt
```
melon.txtのユーザをapple、グループをkobeに変更する。

chgrp グループを変更する。
```
% chgrp kobe melon.txt
```
ファイルmelon.txtのグループをkobeに変更する。
```
% chgrp kobe *
```
カレントディレクトリ内のすべてのグループをkobeに変更する。
```
% chgrp kobe mango
```
ディレクトリmangoのグループをkobeに変更する。

chmod ファイルモードを設定する。

ファイルへのアクセス権を設定。オーナー、グループ、その他のユーザという3つに対しそれぞれ設定する。読む(r)を4、書く(w)を2、実行する(x)を1で表し、その合計数を使い設定する。
```
% chmod 444 apple.txt
```
-r--r--r--となりすべての人がこのapple.txtを読む事ができる。
```
% chmod 440 apple.txt
```
-r--r-----となり所有者と同じグループのユーザのみがこのapple.txtを読む事ができる。
```
% chmod 400 apple.txt
```
-r--------となり所有者のみがこのapple.txtを読む事ができる。
```
% chmod 644 apple.txt
```
-rw-r--r--となり所有者はapple.txtを読み、書く事ができるが、それ意外のユーザは読む事のみできる。
```
% chmod 755 orange.pl
```
-rwxr-xr-xとなり所有者はorange.plを読み、書き、実行事ができるが、それ意外のユーザは読んで実行はできるが内容を変更する事はできない。

history 使ったコマンドの履歴を表示する。

```
% history 10
```
直近使った10のコマンドを表示する。!の後に番号を打てば同じコマンドを実行できる。

```
% history | grep vi
```
ヒストリーの結果より"vi"を含む行のみを表示させる。

find ファイルを検索する。

```
% find /tmp/mango/ -name apple.txt -print
```
ディレクトリ/tmp/mango内でapple.txtを検索し表示する。

```
% find /tmp/mango/ -name "*.txt" -print
```
ディレクトリ/tmp/mango内で.txtで終わるファイルを検索し表示する。

date 日付けを表示する。

```
% date
```
現在の日時を表示する。

```
# date 200012231210
```
日付けを2000年12月23日12時10分に設定する(rootのみ)。

cal カレンダーを表示する。

```
% cal 1998
```
1998年のカレンダーを表示する。

```
% cal 8 2001
```
2001年8月のカレンダーを表示する。

ps 実行中のプロセスを表示する。

```
% ps ax
```
全プロセスを表示する。

```
% ps ax | grep sshd
```
inetdのプロセスのみ表示する。

kill プロセスを停止させる。

```
% kill 239
```
プロセスID239を強制的に終了させる。

```
% kill -HUP 3988
```
プロセスID3988をハングアップさせる。

top 実行中のプロセスをリアルタイムで表示する。

```
q
```
終了させる

man オンラインマニュアルを表示する。

```
% man less
```
lessのマニュアルを表示する。

head, tail ファイルの最初や最後だけを表示する。

```
% head apple.txt
```
apple.txtの最初の10行のみを表示する。

```
% tail -n5 apple.txt
```
apple.txtの最後の5行のみ表示する。

su 管理モードに入る。super user, substitute userの略。

```
% /usr/bin/su -
```
rootの環境でsuになる。"su"コマンドを使用する時にフルパスで指定しないとトロイの木馬などが仕掛けられている場合にrootのパスワードがそのまま取られる可能性があるので常に/usr/bin/suと利用した方が良い。

mount CD-ROMやフロッピーをマウントする(rootのみ)。

```
# mount -t cd9660 /dev/cd0a /cdrom
```
CD-ROMをマウントする。

```
# mount /cdrom
```
/etc/fstabにcdromの設定がある場合。

umount CD-ROMやフロッピーをアンマウントする(rootのみ)。

```
# umount /cdrom
```
/etc/fstabにcdromの設定がある場合。

gzip/gunzip ファイルを圧縮/解凍する。

```
% gunzip yebisu.tar.gz
```
yebisu.tar.gzを解凍する。

tar ファイルをまとめる、展開する。

```
% tar xvf yebisu.tar
```
yebisu.tarからすべてのファイルを取り出す。

```
% tar xvfz yebisu.tar.gz
```
yebisu.tar.gzからすべてのファイルを取り出す。

fetch 指定のアドレスからファイルをダウンロードする。

```
% fetch ftp://ftp.sample.org/pub/latest/sample.tar.gz
```
ftp.sample.orgよりsample.tar.gzをダウンロードする。

ping ネットワークの応答を確認する。

```
% ping 192.168.0.1
```
IPアドレスを指定しての確認。ネットワーク機能の確認を確認するにはまずローカル(127.0.0.1)、次に自分に割り当てられているIP(192.168.0.□)、最後にルータへとpingを利用すると分かりやすい。

reboot リスタートする(rootのみ)。

shutdown システムを停止する(rootのみ)。

```
# shutdown -h now
```
今すぐシステムを停止する。

```
# shutdonw -h +5
```
5分後にシステムを停止する。

```
# shutdown -r +7
```
7分後にシステムを再起動する。

crontab cronの設定、表示。

```
% crontab -l
```
cronの設定を表示する。

```
% crontab -e
```
cronを設定する。

4.2.2 crontabの書式

分(0-59) 時(0-23) 日(1-31) 月(1-12) 曜日(0-7，0が日曜) 実行するファイル
で指定する。

例)`5 0 * * * /home/script/sample.sh`
毎日、0時5分に/home/scriptにあるsample.shを実行する。

例)`*/5 * * * * /home/script/sample.sh`
5分毎に/home/scriptにあるsample.shを実行する。

4.2.3 ftpコマンドの使い方

ftp.freebsd.orgに接続する場合。

```
% ftp ftp.freebsd.org
```

接続されるとユーザ名の入力を促される。

```
Connected to ftp.freebsd.org.
Name (ftp.freebsd.org:user):
```

anonymousサーバの場合、ここで"ftp"または"anonymous"でログインをする。

anonymousサーバの場合、パスワードに自分のメールアドレスを入力する。

```
Guest login ok, send your complete e-mail address as password.
Password:
```

うまくログインできると"welcome"などが表示され、失敗すると"Login failed."などと表示される。"ls"コマンドでファイルの一覧が表示され、"cd"コマンドで必要なディレクトリに移動できる。

テキストデータをダウンロードする場合には"ascii"モードで、それ以外のファイルは"binary"モードで行う必要がある。このファイル転送タイプは"ascii(asc)"と"binary(bin)"と打つことにより変更でき、一度変更したら再度ファイルごとに設定する必要はない。

```
ftp > bin
200 Type set to I.

ftp > asc
200 Type set to A.
```

希望のファイルが"ls"で確認できたら、"get"コマンドでダウンロードを行う。apache-1.3.20.tar.gzがファイル名の場合は下記のようにする。

```
ftp > get apache-1.3.20.tar.gz
```

ファイルはローカルのカレントディレクトリに保存される。

ftpコマンドを終了するには"quit"または"bye"とする。プロンプトが"ftp >"になっているのがftpコマンド状態となる。

4.2.5　パッケージの利用

パッケージを利用することでプログラムを簡単に導入することができる。下記サイトなどからダウンロードできる。

```
ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-stable/
```

現在インストールされているパッケージの一覧表示。

```
# pkg_info
linux_base-7.1_7    The base set of packages needed in Linux mode
pgp-6.5.8_1         Public-Key encryption for the masses
```

インストールされているパッケージの詳細表示。

```
# pkg_info pgp-6.5.8_1
```

パッケージのインストール。

```
# pkg_add pgp-6.5.8_1.tgz
```

パッケージの削除。

```
# pkg_delete pgp-6.5.8_1.tgz
```

4.2.5　pgpコマンドの使い方

pgpコマンドは下記サイトなどのパッケージなどを利用し、インストールする。

```
ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-stable/security/
```

鍵のインポート

```
# pgp -ka public_key.asc
```

鍵の検証

```
# pgp FreeBSD-SA-04:05.openssl.asc
```

鍵の確認

```
# pgp -kv
```

4.2.6　UNIXコマンドの参考サイト

UNIXの部屋 <http://x68000.startshop.co.jp/~68user/unix/>
UNIX1年生 <http://www.tokaido.co.jp/syoko/>

4.3 viの使い方

% vi apple.txt　　apple.txtをエディターviで開く。

■ escでコマンドモードへ移行する。

l	カーソル前進
h	カーソル後進
k	カーソル上へ
j	カーソル下へ
3l	3文字前進
5h	5文字後退
G	最終行に移動
1G	先頭行に移動
23G	23行目へ移動
^	行頭へ移動
$	行末へ移動
ctrl-f	次ページへ移動
ctrl-b	前ページへ移動
i	カーソルの前へ文字挿入
a	カーソルの後ろへ文字挿入
A	行の終わりに文字を挿入
x	カーソル上の文字削除
4x	カーソルから右4つの文字削除
dd	現在行を削除
4dd	4行削除
/apple(enter)	appleという文字を下に向かって検索する。
?apple(enter)	appleという文字を上に向かって検索する。
:%s/apple/orange/g	appleをorangeに置き換える。
:%s/apple/orange/c	appleをorangeに確認しながら置き換える。置き換える時はyにリターン、しない時はnにリターン。
:q	終了する
:q!	強制終了する
:w	保存する
:wq	保存して終了
ZZ	保存して終了
:set showmode	動作モードを表示する
:set nu	行番号を表示する
:set nonu	行番号を表示しない

5 DNSの設定

5.1 BIND注6<http://www.isc.org/products/BIND/>

5.1.1 BINDのインストール

インストールされているものは古いもののため、新しいものをインストールする。
>> BINDはセキュリティホールとなる場合が高いので常に最新版を入れる様に心掛ける。

/usr/localにsrcディレクトリを作成しダウンロードしたBINDのソースを復元する。

```
# mkdir /usr/local/src
# cd /usr/local/src/
# tar xvfz /tmp/bind-9.2.4.tar.gz
```

コンパイルする。

```
# cd bind-9.2.4/
# ./configure
# make
# make install
```

5.1.2 named.confの設定

設定ファイルnamed.confは/etcに、それ以外は/etc/namedb内に作成する。named.confで指定したlocalhost.zone(localhostの正引き)、localhost.rev(localhostの逆引き)、beer.zone(beer.jpの正引き)、beer.rev(beer.jpの逆引き)ファイルを/etc/namedbに作成する。

```
# cd /etc/namedb
# mv named.conf named.conf.default
```

/etc/namedbのオーナーとグループを起動ユーザであるbindに変更する。

```
# chown bind:bind /etc/namedb
```

注6 BIND [Berkeley Internet Name Daemon]

```
# vi /etc/named.conf
```

```
options  {
        directory "/etc/namedb";
        pid-file "/etc/namedb/named.pid";
        allow-transfer { none; };
        recursion yes;
};
zone "."  {
        type hint;
        file "named.root";
};
zone "localhost"  {
        type master;
        file "localhost.zone";
};
zone "0.0.127.IN-ADDR.ARPA"  {
        type master;
        file "localhost.rev";
};
zone "beer.jp"  {
        type master;
        file "beer.zone";
};
zone "0.168.192.IN-ADDR.ARPA"  {
        type master;
        file "beer.rev";
};
```

作成後、下記コマンドで書式を確認する。何も表示されなければ問題なしとなる。

```
# /usr/local/sbin/named-checkconf
```

5.1.3 localhost.zoneの設定

```
# vi /etc/namedb/localhost.zone
```

```
;localhost.zone
$TTL 604800 ;Minimum 7 days
@            IN    SOA   ns.beer.jp. root.beer.jp. (
                         20041201   ;Serial
                         28800      ;Refresh 8 hours
                         1800       ;Retry 30 minutes
                         2592000    ;Expire 30 days
                         3600 )     ;Minimum 1 hour
;
             IN    NS    ns.beer.jp.
;
localhost.   IN    A     127.0.0.1
```

下記コマンドで書式を確認する。

```
# /usr/local/sbin/named-checkzone localhost /etc/namedb/localhost.zone
zone localhost/IN: loaded serial 20041201
OK
```

5.1.4 localhost.revの設定

```
# vi /etc/namedb/localhost.rev
```

```
;localhost.rev
$TTL 604800 ;Minimum 7 days
@       IN    SOA      ns.beer.jp. root.beer.jp. (
                       20041201     ;Serial
                       28800        ;Refresh 8 hours
                       1800         ;Retry 30 minutes
                       2592000      ;Expire 30 days
                       3600 )       ;Minimum 1 hour
;
        IN    NS       ns.beer.jp.
;
1       IN    PTR      localhost.
```

5.1.5 beer.zoneの設定

```
# vi /etc/namedb/beer.zone
```

```
;beer.zone
$TTL 604800 ;Minimum 7 days
@           IN    SOA      ns.beer.jp. root.beer.jp. (
                           20041201     ;Serial
                           28800        ;Refresh 8 hours
                           1800         ;Retry 30 minutes
                           2592000      ;Expire 30 days
                           3600 )       ;Minimum 1 hour
;
            IN    NS       ns.beer.jp.
;
            IN    MX 10    ns
;
ns          IN    A        192.168.0.□
ftp         IN    CNAME    ns
www         IN    CNAME    ns
mail        IN    CNAME    ns
tempest     IN    A        192.168.0.31
```

5.1.6 beer.revの設定

```
# vi /etc/namedb/beer.rev
```

```
;beer.rev
$TTL 604800 ;Minimum 7 days
@       IN    SOA      ns.beer.jp.  root.beer.jp. (
                       20041201     ;Serial
                       28800        ;Refresh 8 hours
                       1800         ;Retry 30 minutes
                       2592000      ;Expire 30 days
                       3600 )       ;Minimum 1 hour
;
        IN    NS       ns.beer.jp.
;
        IN    PTR      beer.jp.
        IN    A        255.255.255.0
;
□       IN    PTR      ns.beer.jp.
31      IN    PTR      tempest.beer.jp.
```

5.1.7 named.root

ルートサーバの一覧表ファイル、named.rootは必要に応じて下記よりダウンロードし、/etc/namedb内に置く。

```
ftp://rs.internic.net/domain/named.root
```

5.1.8 rndc.keyの作成

rndcコマンドを利用できるようにするため、/etc/rndc.keyを作成する。作成した鍵のオーナーを起動ユーザnamedに変更する。乱数のエントロピーを発生させてから実行を行う。

```
# rndcontrol -s 1 -s 2 -s 3 -s 4 -s 5 -s 6 -s 7 -s 8 -s 9 -s 10
# /usr/local/sbin/rndc-confgen -a -k rndckey
# chown bind /etc/rndc.key
# chmod 400 /etc/rndc.key
```

5.1.9 named.confの修正

rndcコマンドをローカルでのみ使用できるようにし、rndc.keyを読み込む設定する。下記4行を追加する。

```
# vi /etc/named.conf
```

```
controls {
      inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};
include "/etc/rndc.key";
```

5.1.10 起動確認

namedをテストモードで起動する。起動状況のログが画面に表示される。エラーがあった場合はファイルを適宜修正する。

```
# /usr/local/sbin/named -u bind -g
```

5.1.11 自動起動

/etc/rc.confに次の3行を加える(オリジナルは/etc/default/rc.conf)。

```
# vi /etc/rc.conf
```

```
named_program="/usr/local/sbin/named"
named_enable="YES"
named_flags="-u bind"
```

5.1.12 手動での起動

専用のbindユーザで立ち上げる。

```
# /usr/local/sbin/named -u bind
```

5.1.13 resolvの設定

ここで/etc/resolv.confで自IPアドレスから#を取り、有効にする。

```
# vi /etc/resolv.conf
```

```
#nameserver 192.168.0.□  ←を
nameserver 192.168.0.□  ←にする。
```

5.1.14 動作確認

hostコマンドで動作を確認する。

localhostの正引き(localhost.zone)

```
# host localhost.  ←実行
localhost has address 127.0.0.1  ←結果
```

localhostの逆引き(localhost.rev)

```
# host 127.0.0.1  ←実行
1.0.0.127.IN-ADDR.ARPA domain name pointer localhost.  ←結果
```

beer.jpの正引き(beer.zone)

```
# host www.beer.jp.  ←実行
www.beer.jp has address 192.168.0.□  ←結果
```

beer.jpの逆引き(beer.rev)

```
# host 192.168.0.□  ←実行
□.0.168.192.IN-ADDR.ARPA domain name pointer ns.beer.jp  ←結果
```

mxの確認(beer.zone)

```
# host -t mx beer.jp  ←実行
beer.jp mail is handled by 10 ns.beer.jp.  ←結果
```

ゾーン転送の確認(named.conf)

```
# host -l beer.jp  ←実行
Host beer.jp not found: 5(REFUSED)  ←結果
; Transfer failed.
```

最後にwww.freebsd.orgなどの一般サイトもhostコマンドで引けることを確認する。

5.1.15 設定の再読み込み

```
# /usr/local/sbin/rndc reload
```

5.1.16 BINDの稼動状況確認

```
# /usr/local/sbin/rndc status
```

5.1.17 用語説明

$TTL　Time To Liveの略、キャッシュ時間をここで指定する、これを設定しないと起動時にエラーが出る(起動はする)。

SOA　SOA(Start Of Authority)はホスト名や管理者のメールアドレスを定義する。

NS　NS(Name Server)はネームサーバを定義する。

A　A(Address)はIPアドレスを定義する。

CNAME　CNAME(Canonical Name)はホストに別名をつける場合に使用する。

PTR　PTR(Domain Name Pointer)はIPアドレスに対応するホスト名を定義する。

MX　MX(Mail Exchanger)はメールの配送先を指定する。

Serial　シリアル番号、設定した日付を入力することが多い。セカンダリサーバはここが新しくなったときにデータの更新を求めるので、修正したときはここも変更すること。

Refresh　セカンダリサーバに対して、プライマリサーバへのデータの更新を行う頻度を決定する。

Retry　Refreshで指定した時間経過後、プライマリがダウンしていたなどの事情で接続できなかった場合にこの間隔をあけて再度確認を行う。

Expire　この間隔の間でセカンダリがプライマリからの応答を得られない場合、保持しているデータを削除する。

Min　ネガティブキャッシュの有効期限を設定する。

6 Web Serverの設定

6.1 Apache <http://www.apache.org/>

6.1.1 Apacheのインストール

/usr/local/srcにソースを展開する。

```
# cd /usr/local/src/
# tar xvfz /tmp/httpd-2.0.52.tar.gz
```

コンパイルする。

```
# cd httpd-2.0.52/
# ./configure
# make
# make install
```

6.1.2 設定

```
# cd /usr/local/apache2/conf/
```

httpd.confが設定をするためのファイル。あらかじめ設定されている専用のwwwユーザ、グループを利用して起動する。

```
# vi httpd.conf
```

```
#ServerName www.example.com:80  ←を
ServerName www.beer.jp:80  ←に変更する

User nobody  ←ここと
Group #-1  ←ここを

User www  ←このように
Group www  ←変更する

AddDefaultCharset ISO-8859-1  ←ここを
AddDefaultCharset off  ←に変更する
```

6.1.3 テスト

httpd.confの修正内容を確認する。

```
# /usr/local/apache2/bin/apachectl configtest
Syntax OK  ←と出ればOK
```

6.1.4 手動での起動

```
# /usr/local/apache2/bin/apachectl start
```

でスタートする。IPアドレスを指定してページが表示されるのを確認する。http://ip address/manualでマニュアルページを見る事ができる。

6.1.5 HTMLファイル

/usr/local/apache2/htdocsに一般のhtmlファイルを置く。必要に応じてhttpd.conf内のDocumentRootを変更することにより、このディレクトリを変更することができる。

6.1.6 CGI

CGIプログラムは専用のディレクトリ(/usr/local/apache2/cgi-bin/)に設置する。予め用意されているサンプルCGIプログラムを使いCGIの実行を確認することができる。

```
# cd /usr/local/apache2/cgi-bin/
# chmod +x test-cgi
```

でtest-cgiに実行権をつける。

```
http://IP address/cgi-bin/test-cgi
```

で動作を確認する。

>> cgi-binディレクトリにあるprintenvとtest-cgiはセキュリティホールとなる可能性があるので、cgi動作確認後は削除した方がよい。

6.1.7 自動起動

存在しない場合、/usr/localにetcディレクトリを作り、その中にrc.dディレクトリを作る。

```
# mkdir -p /usr/local/etc/rc.d
```

起動スクリプトを/usr/local/etc/rc.dにコピーする、これにより次回起動時よりapacheが自動起動するようになる。

```
# cp /usr/local/apache2/bin/apachectl  /usr/local/etc/rc.d/apache.sh
```

6.1.8 再起動

httpd.confを修正した場合には再起動が必要になる。

```
# /usr/local/apache2/bin/apachectl restart
```

6.1.9 停止

```
# /usr/local/apache2/bin/apachectl stop
```

6.1.10 manの設定

.cshrcに一行追加する、これによりapacheのmanを呼び出せるようになる。

```
# vi ~/.cshrc
```

```
# apache man path
if ($?MANPATH) then
     setenv MANPATH "$MANPATH":/usr/local/apache2/man
else
     setenv MANPATH /usr/local/apache2/man
endif
```

下記コマンドで設定を反影できる。

```
# source ~/.cshrc
```

6.1.11 MD5値の確認

ダウンロードしたファイルのMD5値を確認することで改竄されたファイルの利用を防ぐことができる。

```
# md5 /tmp/httpd-2.0.52.tar.gz
MD5 (/tmp/httpd-2.0.52.tar.gz) = eba528fa8613dc5bfb0615a69c11f053
```

6.1.12 参考サイト

Japanized Apache <http://www.apache.or.jp/>

7 FTP Serverの設定

7.1 ProFTPD[注7] <http://www.proftpd.org/>

7.1.1 インストール

ダウンロードしたソースファイルを展開する。

```
# cd /usr/local/src/
# tar xvfz /tmp/proftpd-1.2.10.tar.gz
# cd proftpd-1.2.10/
```

コンパイルする。

```
# ./configure
# make
# make install
```

proftpd実行専用のユーザとグループを作る。

```
# pw groupadd -n proftpd
# pw useradd -n proftpd -g proftpd -s /sbin/nologin -d /nonexistent
```

7.1.2 設定

初期設定ではanonymousでのログイン設定がしてあるので無効にする。

```
# cd /usr/local/etc/
# cp proftpd.conf proftpd.conf.default
# vi proftpd.conf
```

```
ServerName                      "YEBISU FTP SERVER"  ←ここを修正

# Set the user and group that the server normally runs at.
User                            proftpd  ←ここを修正
Group                           proftpd  ←ここを修正

# Bar use of SITE CHMOD by default
<Limit SITE_CHMOD>
Allow from 127.0.0.1, 192.168.0.  ←この行を加える
#  DenyAll  ←ここを修正
</Limit>

<Anonymous ~ftp>  ←ここから

</Anonymous>  ←ここまでのすべての行の先頭に#を付ける、または削除。
```

7.1.3 テスト

proftpd.confの修正内容を確認する。

```
# /usr/local/sbin/proftpd -t
Checking syntax of configuration file
Syntax check complete.  ←と出ればOK
```

注7 FTP [File Transfer Protocol]

7.1.4 自動起動

/usr/local/etc/rc.dに起動スクリプトを書く。

```
# cd /usr/local/etc/rc.d/
# vi proftpd.sh
```

```
#!/bin/sh
echo -n 'proftpd starting.'
/usr/local/sbin/proftpd &
```

実行権を付ける。

```
# chmod +x proftpd.sh
```

7.1.5 PAMの設定

ユーザ認証時に使われるプログラムであるPAMの設定ファイルに下記3行を追加する。

```
# vi /etc/pam.conf
```

```
ftp   auth      required    pam_unix.so      try_first_pass
ftp   account   required    pam_unix.so      try_first_pass
ftp   session   required    pam_permit.so
```

7.1.6 手動での起動

作成したスクリプトを利用して起動する。

```
# /usr/local/etc/rc.d/proftpd.sh
```

7.1.7 動作確認

```
# ftp 127.0.0.1
```

ローカルからftpにアクセスしてみる。問題なければWindowsなどのクライアントマシンからFTPクライアントで接続してみる。

FFFTPを利用する際はホストの設定より高度、LISTコマンドでファイル一覧を取得を選択する。

7.1.8 chroot

この設定ではユーザで入ればどのディレクトリにも移動でき危険なため、ユーザのディレクトリより上に行けないようにする。記述後proftpdを再起動し、ユーザでログインしてホームディレクトリより上には行けないことを確認する。

```
# vi /usr/local/etc/proftpd.conf
```

```
#DefaultRoot    ~  ←#を取り有効化する
```

7.1.9 FTP利用者の設定

/etc/ftpusersの中に使用させないユーザ名を記入することにより、そのユーザはFTPの使用が不可となる。下記コマンドによりユーザ全員が登録されるので、FTPを利用させるユーザのみをリストから削除する。

```
# awk -F: '{ print $1 }' /etc/passwd | sort > /etc/ftpusers
```

7.1.10 Windows用FTPクライアント

FFFTPは下記よりダウンロード可能。

```
http://www.vector.co.jp/soft/win95/net/se061839.html
```

8 Mail Serverの設定

8.1 qmail <http://cr.yp.to/qmail.html>

8.1.1 qmailのインストール

qmailのディレクトリを作る

```
# mkdir /var/qmail
```

下記のコマンドを実行して必要なユーザとグループを作る。

```
# pw groupadd nofiles
# pw useradd alias  -g nofiles -d /var/qmail/alias -s /sbin/nologin
# pw useradd qmaild -g nofiles -d /var/qmail -s /sbin/nologin
# pw useradd qmaill -g nofiles -d /var/qmail -s /sbin/nologin
# pw useradd qmailp -g nofiles -d /var/qmail -s /sbin/nologin
# pw groupadd qmail
# pw useradd qmailq -g qmail -d /var/qmail -s /sbin/nologin
# pw useradd qmailr -g qmail -d /var/qmail -s /sbin/nologin
# pw useradd qmails -g qmail -d /var/qmail -s /sbin/nologin
```

ダウンロードしたソースファイルを展開する。

```
# cd /usr/local/src/
# tar xvfz /tmp/qmail-1.03.tar.gz
# cd qmail-1.03/
```

インストールする。

```
# make setup check
# ./config-fast yebisu.beer.jp
```

>> **"yebisu.beer.jp"は登録するホスト、ドメイン名により適宜変更すること。**

8.1.2 設定

qmailが必要とする最低限のaliasを登録する。

```
# touch ~alias/.qmail-postmaster
# touch ~alias/.qmail-mailer-daemon
# touch ~alias/.qmail-root
# chmod 644 ~alias/.qmail-*
```

起動スクリプトのコピー

```
# cp /var/qmail/boot/home /var/qmail/rc
```

起動スクリプトの設定をする。

```
# vi /var/qmail/rc
```

```
exec env - PATH="/var/qmail/bin:$PATH" \
qmail-start ./Mailbox splogger qmail  ←この行を
qmail-start ./Maildir/ splogger qmail  ←とする
```

8.1.3 root宛メールの転送設定

root宛てのメールは全て管理するユーザに届く様に転送を設定する。

```
# vi ~alias/.qmail-root
```

```
melon  ←ユーザ名がmelonの場合
```

8.1.4 各ユーザの設定

それぞれのユーザに設定する。

```
% /var/qmail/bin/maildirmake ~/Maildir
```

としメールを受け取るディレクトリを作成する。/usr/bin/su -でrootに戻り以下の作業を続ける。

rootユーザは

```
# su - ユーザ名
```

とすることで一般ユーザに変更でき、exitでrootユーザに戻る。

8.1.5 skelの設定

skelディレクトリにMaildirを作成する。これにより新規ユーザに自動的にMaildirが作成されるようになる。

```
# /var/qmail/bin/maildirmake /usr/share/skel/Maildir
```

8.1.6 sendmailの変更

sendmailが自動起動しない様にする。

```
# vi /etc/rc.conf
```

```
sendmail_enable="YES"  を
sendmail_enable="NONE"  に変更する。
```

sendmailを止める。

```
# ps ax | grep sendmail
# kill PID
```

sendmailを起動出来ない様にする。

```
# rm /usr/sbin/sendmail
# chmod 0 /usr/sbin/mailwrapper
# chmod 0 /usr/libexec/mail.local
# chmod 0 /usr/libexec/sendmail/sendmail
```

```
# vi /etc/mail/mailer.conf
```

```
#sendmail       /usr/libexec/sendmail/sendmail
#send-mail      /usr/libexec/sendmail/sendmail
#mailq          /usr/libexec/sendmail/sendmail
#newaliases     /usr/libexec/sendmail/sendmail
#hoststat       /usr/libexec/sendmail/sendmail
#purgestat      /usr/libexec/sendmail/sendmail  ←ここまでをコメント化

sendmail        /var/qmail/bin/sendmail  ←3行追加する
send-mail       /var/qmail/bin/sendmail
mailq           /var/qmail/bin/qmail-qread
```

8.1.6 自動起動

/usr/local/etc/rc.dにqmail.shというファイルを作り、下記の様に記述する。

```
#!/bin/csh
echo -n 'qmail starting.'
csh -cf '/var/qmail/rc &'
```

```
# chmod +x qmail.sh
```

で実行権を与える。これで次回からは起動時にqmailが自動的に立ち上がるようになる。

8.1.7 手動での起動

```
# /usr/local/etc/rc.d/qmail.sh
```

で起動する。

```
# ps ax | grep qmail
```

とし下記の様な表示がされるか確認する。

```
   2233  p0  S      0:00.02 qmail-send
   2234  p0  S      0:00.00 splogger qmail
   2235  p0  S      0:00.00 qmail-lspawn ./Maildir/
   2236  p0  S      0:00.00 qmail-rspawn
   2237  p0  S      0:00.00 qmail-clean
```

8.1.8 sendmailとの互換

qmailをsendmailとの互換性を持たせるための"sendmail wrapper"を使えるようにする。これによりmailコマンドなどがqmailで実行される様になる。

```
# ln -s /var/qmail/bin/sendmail /usr/sbin/sendmail
```

mailコマンドの確認。

```
# mail user
Subject: test  ←件名を書く
test mail  ←内容を書く
```

"."を打ち、リターンキーを押すとメールが送信される。

/home/*user*/Maildir/newの中のファイルを確認する。確認したらroot宛にもメールを出し、自分宛に転送されるか確認する。

8.1.9 manを使えるようにする

.cshrcに追加する、これによりqmailのmanを呼び出せるようになる。

```
# vi ~/.cshrc
```

```
if ($?MANPATH) then
     setenv MANPATH "$MANPATH":/var/qmail/man
else
     setenv MANPATH /var/qmail/man
endif
```

```
# source ~/.cshrc  ←これで設定が反映される
```

8.1.11 Localtime Patch

必要ならばmake setup checkを実行する前にqmailの日付をローカルタイムに修正するパッチをあてる。これによりタイムスタンプは+9 JST(日本標準時)となる。

```
ftp://ftp.nlc.net.au/pub/unix/mail/qmail/qmail-date-localtime.patch

# patch < /tmp/qmail-date-localtime.patch
```

8.1.12 参考サイト

qmail japan <http://www.jp.qmail.org/>

8.2 SMTP[注8]

8.2.1 tcpserverのインストール

qmail-smtpdをtcpserverより起動する、入手先
http://cr.yp.to/ucspi-tcp.html

ソースファイルを展開し、コンパイルを実行する。
```
# cd /usr/local/src/
# tar xvfz /tmp/ucspi-tcp-0.88.tar.gz
# cd ucspi-tcp-0.88/
# make
# make setup check
```

設定ファイルを置く専用のディレクトリを作る。
```
# mkdir /etc/tcpserver
```

8.2.2 SMTPの設定

接続のルールを定義するファイルsmtpd_rulesを作成する。ここではクラアントマシン"192.168.0."からのみの接続を受付けるという設定にする。リレーを許可するアドレスはここに記入すればよい。
```
# cd /etc/tcpserver
# vi smtpd_rules
```

```
127.0.0.1:allow,RELAYCLIENT=""
192.168.0.:allow,RELAYCLIENT=""  ←リレー接続を許可するアドレス
:allow
```

複数のマシンからの接続を受付ける場合の設定は下記を参考。また、IPアドレスだけでなくドメイン名での指定も可能。

192.168.0.5からのみ。
```
127.0.0.1:allow,RELAYCLIENT=""
192.168.0.5:allow,RELAYCLIENT=""
:allow
```

192.168.0.5と192.168.0.8から。
```
127.0.0.1:allow,RELAYCLIENT=""
192.168.0.5:allow,RELAYCLIENT=""
192.168.0.8:allow,RELAYCLIENT=""
:allow
```

192.168.0.5から192.168.0.10までのすべてのマシンから。
```
127.0.0.1:allow,RELAYCLIENT=""
192.168.0.5-10:allow,RELAYCLIENT=""
:allow
```

192.168.0.上のすべてのマシンから。
```
127.0.0.1:allow,RELAYCLIENT=""
192.168.0.:allow,RELAYCLIENT=""
:allow
```

注8 SMTP [Simple Mail Transfer Protocol]

8.2.3 CDB形式への変換

次のコマンドでこのファイルをtcpserver用に作り変える。

```
# /usr/local/bin/tcprules smtpd_rules.cdb smtpd_rules.tmp < smtpd_rules
```

8.2.3 自動起動

/usr/local/etc/rc.dにtcpserver_smtpd.shというファイルを作り、下記のように記述すると起動時に自動的起動する。UIDとGIDにはそれぞれ調べた番号を記述、またこのコマンドは一行で記述すること。

qmaildのUIDとnofilesのGIDを調べる。

```
# cat /etc/passwd  ←UIDを確認
# cat /etc/group  ←GIDを確認
```

```
# vi /usr/local/etc/rc.d/tcpserver_smtpd.sh
```

```
#!/bin/sh
echo -n 'qmail-smtpd starting.'
/usr/local/bin/tcpserver -x  ←ここから
/etc/tcpserver/smtpd_rules.cdb -v -u UID -g GID 0 smtp
/var/qmail/bin/qmail-smtpd 2>&1 |
/var/qmail/bin/splogger smtpd 3 &  ←ここまで一行
```

これに実行権をつける。

```
# chmod +x /usr/local/etc/rc.d/tcpserver_smtpd.sh
```

8.2.4 手動で起動

```
# /usr/local/etc/rc.d/tcpserver_smtpd.sh
```

で起動する。

8.3 POP[注9]

8.3.1 POPの設定

checkpasswordを使用する。

<http://cr.yp.to/checkpwd.html>

8.3.2 checkpasswordのインストール

ソースファイルを展開する。

```
# cd /usr/local/src/
# tar xvfz /tmp/checkpassword-0.90.tar.gz
```

コンパイルを実行する。

```
# cd checkpassword-0.90/
# make
# make setup check
```

8.3.3 checkpasswordの設定

tcpserverを使いqmail-popupを起動する。

```
# cd /etc/tcpserver/
# vi pop3d_rules
```

```
127.0.0.1:allow
192.168.0.:allow  ←POP接続を許可するアドレス
:deny
```

8.3.4 CDB形式への変換

次のコマンドでこのファイルをtcpserver用に作り変える。

```
# /usr/local/bin/tcprules pop3d_rules.cdb pop3d_rules.tmp < pop3d_rules
```

8.3.5 自動起動

/usr/local/etc/rc.dにtcpserver_pop3d.shというファイルを作り、下記のように記述すると起動時に自動的起動する。"yebisu.beer.jp"は自分のドメインに合わせること。

```
# vi /usr/local/etc/rc.d/tcpserver_pop3d.sh
```

```
#!/bin/sh
echo -n 'qmail-pop3d starting.'
/usr/local/bin/tcpserver -x  ←ここから
/etc/tcpserver/pop3d_rules.cdb 0 pop3 /var/qmail/bin/qmail-popup
yebisu.beer.jp /bin/checkpassword /var/qmail/bin/qmail-pop3d
Maildir 2>&1 | /var/qmail/bin/splogger pop3d 3 &  ←ここまで一行
```

これに実行権をつける。

```
# chmod +x /usr/local/etc/rc.d/tcpserver_pop3d.sh
```

8.3.6 手動での起動

ウィンドウズなどのメールクライアントでsmtpとpopサーバの設定を行い、送受信できるか確認してみる。qmailの動作確認には /var/log/maillogを見る。

```
# /usr/local/etc/rc.d/tcpserver_pop3d.sh
```

[注9] POP [Post Office Protocol]

8.4 APOP[注10]

8.4.1 APOPの設定

checkpwを使用する。

<http://checkpw.sourceforge.net/checkpw/>

8.4.2 checkpwのインストール

ソースファイルを展開し、コンパイルを実行する。/binにcheckpwとcheckapoppwがインストールされる。

```
# cd /usr/local/src/
# tar xvfz /tmp/checkpw-1.01.tar.gz
# cd chckpw-1.01/
# make
# make setup check
```

8.4.3 checkpwの設定

各ユーザごとにパスワードは~/Maildir/.passwordに記述する。作成後、他人に見られないように記入後属性を変更する。

```
% vi ~/Maildir/.password
```

```
password
```

```
% chmod 600 ~/Maildir/.password
```

8.4.4 自動起動

/usr/local/etc/rc.dにtcpserver_apop3d.shというファイルを作り、下記の様に記述すると起動時に自動的起動する。長いが、一行で行う。"yebisu.beer.jp"は自分のホスト、ドメインに合わせる。

```
# vi /usr/local/etc/rc.d/tcpserver_apop3d.sh
```

```
#!/bin/sh
echo -n 'qmail-apop starting.'
/usr/local/bin/tcpserver -x ←ここから
/etc/tcpserver/pop3d_rules.cdb 0 pop3
/var/qmail/bin/qmail-popup yebisu.beer.jp /bin/checkapoppw
/var/qmail/bin/qmail-pop3d Maildir 2>&1 |
/var/qmail/bin/splogger apop 3 &  ←ここまで一行
```

これに実行権をつける。

```
# chmod +x /usr/local/etc/rc.d/tcpserver_apop3d.sh
```

8.4.5 手動での起動

起動、pop3dが起動している場合はそちらを先に終了しておく。メールクライアントの設定でAPOPを確認し、受信ができることを確認する。

```
# /usr/local/etc/rc.d/tcpserver_apop3d.sh
```

8.4.6 POPとAPOPの選択

このままでは起動時にpopとapopの両方が立ち上がってしまうため、使わない方を下記の様にファイル名の前に"_"を付け実行されない様にする。

```
# cd /usr/local/etc/rc.d/
# mv tcpserver_apop3d.sh _tcpserver_apop3d.sh
```

注10 APOP [Authenticated POP]

9 セキュリティについて

9.1 現状

またもや偽シティバンクからメール，今度は件名が“至急”に

先日，シティバンクをかたり個人情報を入力させるフィッシングのメールが筆者に送信されてきたことを報告したが，26日にシティバンクになりすましたメールがまた送られてきた。前回のメールから4日しかたっていない。

2通目の件名は「ただちに注意が必要」（ATTN: Immediate attention required (Citi.com)。1通目は「シティバンクのお客様に秘密のお知らせ」（ATTN: Confidentialy For Citibank Customers!）だった。緊急度が増したことを強調している。件名などで判断し，スパム・メールを削除するフィルタリングへの対策という側面もあるだろう。

本文の内容は先日のメールと全く同じだった。また，フィッシング用にポップアップするウインドウも同様だ。ちなみにそのウインドウのアドレスは同じhttp://xxx.xxx.34.242/confirm/で指定されている（xxxは伏字）。

このように，フィッシング・メールの送信者はさまざまな手段で攻撃してくる。シティバンクなど金融業やポータル・サイトでは，日本語のフィッシング・メールの報告が出始めている。ユーザー側で警戒するだけでなく，なりすまされた企業も性急に顧客に対する注意喚起が必要ではないだろうか。

（市嶋　洋平＝日経コミュニケーション）

ITPro 2004.08.27
<http://itpro.nikkeibp.co.jp/>

9.2 基礎知識

9.2.1 シュレッダー
初めに必要なものは何か?

9.2.2 ハッカーとクラッカー
ハッカーはコンピュータで犯罪を犯す人という定義をしている人、マスコミが多いいが本来はコンピュータに精通した人を指す。悪意を持ち攻撃などを行う人をクラッカーと呼ぶように一部では呼び掛けているが、あまり一般には知られていない。

9.2.3 内部の人間、辞めた人
外部からの攻撃よりも内部からの攻撃の方が簡単である。内部からの攻撃は全体の60-80%を占めるとも言われ、大きな問題となっている。

9.2.4 オープンソースは安心か?
LinuxやFreeBSDなどオープンソースが人気である、その理由としてソース(プログラムそのもの)が公開されていると点がある。直接ソースを見る事ができるので安心して使えるという面があるが、また穴を探してそこを攻撃できるという一面も合わせ持つ。

9.2.5 セキュリティの方針
どれだけ強力な暗号を設定しても、利用する人が使わなければ意味がない。ファイアウォールをいくら導入したところでサーバルームに清掃員が自由に出入りできたとしたらそこにセキュリティがあるとは言えない。

9.2.6 何が重要か?
書類やコンピュータデータだけが守るべきものではない。社員の健康、プライバシー、顧客の信用、社会的な評価、システムの構成なども重要であり注意が必要となる。

9.2.7 費用対効果
社内向けのファイルサーバが一日止まったらどれだけの損失になるか、社外向けのウェッブサーバが一日止まったらどれだけの損失になるかなど計算してみる。

9.2.8 様々な攻撃
DoS (Denial of Service)、DDoS (Distributed Denial of Service)
なりすまし
改竄
盗聴
スニッファリング
IPアドレス偽造

9.2.9 ウィルスなど
裏口　　不正アクセスに使用。
ウィルス　　自分のコピーを送り、コンピュータ上の自分以外のプログラムを書き換える
ワーム　　ネットワーク上を渡り歩くもの。
トロイの木馬　見た目とは違った働きをするもの。

9.2.10 ログ

ログを定期的に確認する。
随時ログをプリントする様にすると、内部を荒らされても証拠は残る。
外からは入れないマシンにログをコピーする。
マシンごとにノートを作り、気がついた事などを書き込むのも有効。

9.2.11 物理的セキュリティ

サーバの保管場所、バックアップメディアの保管場所など。
火、煙、ほこり、地震、温度、湿度、雷
プリンタ、ファクス
ログインしたまま端末を離れる、、、
ビルに入る、部屋に入る時、

9.2.12 人事

管理者は適切な人に任せる。
一人の人間に全てを任せると、、、

9.3 セキュリティの方針

9.3.1 担当責任者を決める

責任者がいない → 管理が曖昧になる → そして、、、
セキュリティに関する担当者を決める、小規模以外の組織では複数の担当者を用意しないと、担当者が必要な時に休暇や病気などで対応できない事がある。

9.3.2 利用者を考える

一般的にセキュリティを厳しくするという事は利用者にとっては負担が増えるといえる。あまり複雑なパスワードを要求すると覚える事が出来ず、メモ帳に書いてモニタに貼るといった事がおこる。

9.3.3 何を、何から守るのか?

何を　プライバシー
　　パスワード(root, user)
　　システム構成
　　業務能力
　　データなど

何から　管理者がいなくなる(病気や事故など)
　　停電
　　ネットワーク障害
　　ハードウェア、リムーバブルメディアなどの盗難
　　ノートPCの盗難
　　ウィルス
　　ソフトウェアメーカの倒産
　　社員、元社員による攻撃など

所属する組織での必要な事柄を上げそれぞれに対策をたてる。

9.3.4 守るべき価値は高いのか?

場合によってはネットワークに侵入するよりも、管理者を買収する方がはるかに安く上がる。

9.3.5 パスワードの発行

ユーザに新しいパスワードを発行するときはそれぞれに新規のパスワードを割り当てる。

9.3.6 パスワードを作る

>> 悪いパスワード

簡単に推測できるもの。

自分、家族の名前	apple1, orange, KimuraTakuyaなど
自分、家族の誕生日	0228, 19620422など
短い文字	abc, xyz, funなど
単語	Computer, NASA, Dreamなど
ゲームの登場人物	Toro, Momoなど
電話番号、車のナンバー	0312345678など

>> 良いパスワード

8文字以上で英字の大文字と小文字を含み、数字や特殊記号も含むものが理想。

単語の組み合わせ	IBM33Compaq（IBMでは散々な思いをしたのでCompaqに変えてみた）
詩や歌を元に作る	Abnskna-（"あれから僕達は何かを信じて来れたかなぁ", "Arekara Bokutachiwa Nanikawo Shinjite Koretaka NA-"）

9.3.7 教育

入力しているところをじっと見られては意味がない。
パスワードをメールで送ってはいけない。
メモに書いて貼ってはいけない。
など、利用者に徹底する。

9.3.8 パスワードの更新

ユーザが定期的にパスワードを変更することを期待してはいけない。定期的に強制的に変更させるようにする、ただし余り頻繁に行うと反感を買う。

9.3.9 グループ共有のパスワードは避ける

利用者は自分のみの物には管理意識を持つが、共有して所有するものに対する意識は著しく低くなる。そのためグループで共有のパスワードはグループ外の利用者ににも簡単に知られるという事を認識する。

9.3.10 ユーザ名

単純なユーザ名よりは複雑なユーザ名の方がよい、クラッカーはパスワードと共にユーザ名も推測しなければならなくなる。

9.4 暗号

9.4.1 暗号化する

例えクラッカーがシステムを乗っ取たとしてもデータが暗号化されていればまだ安全性は保てる。またファイルを転送する際にも暗号化されていれば途中での盗聴、盗難から守る事ができる。

9.4.2 秘密鍵暗号方式と公開鍵暗号方式

秘密鍵暗号方式では文書の暗号化と複合化に同一の鍵を使用する。
公開鍵暗号方式では公開鍵を使い文書を暗号化し、秘密鍵を使って復号化する。

9.4.3 PGP注11

UNIX, Windows, Macなどに対応していて、フリーウェア版と商用版がある。

9.4.4 PGPの仕組み

送信者の秘密鍵、公開鍵と受信者の秘密鍵、公開鍵がある。それぞれの秘密鍵は本人のみが持ち公開鍵は鍵サーバなどに置き必要な人が使えるようにする。

受信者の公開鍵で文書を暗号化すれば、それを開けられるのは受信者が受信者の秘密鍵を使う時のみである。

送信者の秘密鍵で署名し、受信者が送信者の公開鍵でそれを開けばその文書が送信者本人の物であると受信者は確認できる。これをデジタル署名という。

上記の二つを組み合わせ、送信者の秘密鍵で文書に署名し、受信者の公開鍵で暗号化して送信する。受信者は受信者の秘密鍵で暗号を復号化し、送信者の公開鍵で署名を確認するという使い方をする。

9.5 バックアップ

9.5.1 バックアップの必要性

定期的にバックアップを取る事の重要性。

9.5.2 ユーザによるミス

初心者の誤操作によりデータを失う事がある。そして経験を積んでいるユーザ(管理者権限を持っている場合もある)による致命的なミスもよくある。

9.5.3 ハードウェアの故障

信頼性は以前よりは高いが、ハードディスクはいつか必ず壊れる。

9.5.4 ソフトウェアのバグ

今迄見つからなかったということは、今後見つからないという事にはならない。

9.5.5 クラッキング

悪意のあるものに侵入されて破壊される可能性がある。

注11 PGP [Pretty Good Privacy] http://www.pgpi.org/

9.5.6 盗難
コンピュータは換金しやすいため、盗難にあう可能性が高い。

9.5.7 自然災害
地震、火事、雷などにより被害を受ける可能性がある。

9.5.8 その他の災害
ネズミにケーブルをかじられる。酔っぱらい運転の車が飛び込んでくるなど。

9.5.9 バックアップの種類
>> 初期バックアップ
OSをインストールし設定後、ユーザが使い始める前に取る。不正侵入後の普及、OSの再インストールが楽になる。

>> フルバックアップ
すべてのファイルを全てコピーする、定期的に行う。

>> インクリメンタルバックアップ
ファイル内でフルバックを取った後に変更があったものだけをコピーする、これによりフルバックアップと比べ短い時間ですむ。

フルバックアップとインクリメンタルバックアップを組み合わせて通常は使用する。

9.5.10 バックアップメディア
バックアップ先はリムーバブルメディア(MO, DAT, CD-R/RWなど)が良い、同じハードディスクの別のパーティションにバックアップを取ってもあまり意味がない。メディアは複数組用意し交互に利用する、これによりメディア自身の故障などからデータロスを防ぐ事ができる。また定期的にバックアップされたデータを検証する必要がある、一見問題なくコピー出来ていてもそれが読み出せるという保証はない。

9.5.11 バックアップメディアの保管
メディアをハードディスクのある部屋などにおいて置いては意味がない、必ず物理的に離れた場所に置く必要がある。また温度や湿度、直射日光によりメディアがダメージを受ける事がある事を理解しておく必要がある。メディアは書き込み禁止の状態にしておかないと、過って別の物を上書きしてしまう可能がある。

9.6 参考サイト 書籍

9.6.1 サイト

CERT/CC
http://www.cert.org/
CERT/CC (Computer Emergency Response Team, Coordination Center)は1988年12月にDARPA (the Defense Advanced Research Projects Agency, part of the U.S. Department of Defense)がインターネット上にある10%ものコンピュータが被害を受けたワーム事件の後に出来た組織であり、コンピュータセキュリティに関する多くの情報がまとめられている。

JPCERT/CC
http://www.jpcert.or.jp/

@police
http://www.cyberpolice.go.jp/

CERT Advisory (邦訳版)
http://www.lac.co.jp/security/information/CERT/

IPA セキュリティセンター
http://www.ipa.go.jp/security/

ATTRITION Web Page Hack Mirror
http://www.attrition.org/mirror/
ハッキングされたサイトの一覧。

マイクロソフト セキュリティ情報
http://www.microsoft.com/japan/technet/security/current.asp

FreeBSD Security Information 日本語版
http://www.freebsd.org/ja/security/

Linux バグ・セキュリティ情報
http://www.linux.or.jp/security/

Sun Microsystems Sunsolve
http://sunsolve.sun.com/

9.6.2 Windows用SSHクライアント

WindowsからSSHを利用してアクセスするにはPuTTYを利用する。下記サイトより"putty.exe"をダウンロードすればよい。特にインストールの作業は必要無く、そのまま起動できる。
http://www.chiark.greenend.org.uk/~sgtatham/putty/

9.6.3 Macintosh用SSHクライアント

MacintoshからSSHを利用してアクセスするにはMacSSHを利用する。下記サイトよりダウンロードすればよい。
http://www.macssh.com/

10 FreeBSD参考資料

10.1 参考URL

FreeBSD <http://www.freebsd.org/>
FreeBSD Japan <http://www.jp.freebsd.org/>

FreeBSDの入手
FTP <ftp://ftp.jp.FreeBSD.org/pub/FreeBSD/>
パッケージ　ぷらっとホーム <http://www.plathome.co.jp/>

11.2 参考書籍

「FreeBSD パーフェクトネットワーク」著者 曽田眞史、花井浩之、濱本雄二、前田幸範
　　株式会社毎日コミュニケーションズ　ISBN4-8399-0223-2
「新インターネットサーバ構築術」著者 石橋勇人
　　ソフトバンク パブリッシング株式会社　ISBN4-7973-0552-5
「qmail メールサーバの構築」著者 Richard Blum, 翻訳 コスモプラネット
　　株式会社アスキー　ISBN4-7561-4001-7
「UNIXコマンドポケットリファレンス」著者 中西 隆
　　株式会社技術評論社　ISBN4-7741-0508-2

11.3 参考雑誌 ムック

「FreeBSD Express」株式会社毎日コミュニケーションズ
「FreeBSD PRESS」株式会社毎日コミュニケーションズ
「BSD magazine」株式会社アスキー　http://www.ascii.co.jp/BSDmag/