FreeBSD 4.6.2-RELEASE で行こう

龍谷大学理工学部　小島 肇
kjm@rins.ryukoku.ac.jp
http://www.st.ryukoku.ac.jp/~kjm/

FreeBSD って何ですか?

- Linux と人気を二分する、free に利用できる UNIX 系 OS
  - 少なくとも、日本では「 Linux と人気を二分する」と思う…
    - 雑誌まであるくらいだし…
  - ISP などの「裏方」で活躍している事例がかなりある模様
    - Yahoo! とか…

私が FreeBSD を使っている理由

- 安定して動作する
  - OS 全体として維持されている
    - 個別モジュール毎の Linux とは違う
  - 4.6.x-RELEASE はちょっと混乱があったが
- 豊富なドキュメント
  - OS 全体として維持されている
    - ドキュメントと実際の中身とでけっこう違和感がある Linux とは違う
  - 活発なユーザコミュニティ

私が FreeBSD を使っている理由

- source がある
  - source が基本
- make 一発
  - source tree
  - ports
- 慣れ :-)

注意点

- 早い（早すぎる）OS リリース
  - 3 カ月おきに新リリースが登場
  - 古いリリースには security fix がされない
    - 現状、4.4-RELEASE 以降のみ
    - ずいぶん長くサポートされる Red Hat Linux とは違う
- 追いかけるための仕掛けはあるにはある
  - しかし、それなりの手間は必要
  - source が基本、binary only では追いかけられない。fix package を rpm などでインストールすればよい Linux 方面とは違う

インストール

- 「FreeBSD 徹底入門 [改訂版] 」を読んでください
- X Window はインストールすべきか?
  - 安全性を優先するならインストールすべきではない（特にサーバ機）
  - X Window を必要とする packages/ports をインストールする時点で一部が自動的にインストールされる可能性あり

インストールした後のチューニング

- kernel つくりなおし
  - 手順:
    - cd /usr/src/sys/i386/conf
    - cp GENERIC MyConf
    - vi MyConf
    - config MyConf
    - cd ../../compile/MyConf
    - make depend
    - make
    - make install
- さまざまなパラメータ設定(/etc/rc.conf など)

kernel つくりなおし

- 設定ファイルから不要なデバイスを削る
  - CPU
  - network device
  - SCSI device
  - RAID device
- 不要な機能を削る
  - IPv6
  - BPF
- なぜつくりなおす?
  - サイズが小さくなるのでリソースを有効利用できる
  - 使わない機能を侵入者に悪用されないために
  - 標準(GENERIC)カーネルには存在しない機能を追加する場合

削るものの例（あくまで例）

- CPU
  cpu I366_CPU
  cpu I486_CPU
  cpu I586_CPU
- options
  options MATH_EMULATE
  options INET6

- device
  device fd1
  device atapist
  device ahb
  device adv0 at isa?
  device asr
  device sio2
  device ppc0
  device de
- pseudo-device
  pseudo-device bpf
  pseudo-device sl 1

さまざまなパラメータ設定

- /etc/rc.conf ファイルに記述
  - /etc/default/rc.conf ファイルにデフォルト設定が記載されているので、これを参考にして、変更すべき場所だけを記載する
  - /etc/rc.conf にはサイト内で共通する要素を記述し、/etc/rc.conf.local にホスト独自の内容を記載してもよい
- /etc/sysctl.conf ファイルに記述
  - カーネル設定ファイルでは設定しきれない、カーネルパラメータの細かい調整
- 各種 daemon（サーバプログラム）の設定ファイルに記述
  - daemon 毎に設定

/etc/rc.conf ファイル記述例

- セキュリティ関連

	説明
tcp_drop_synfin="YES"	SYN+FIN を破棄
icmp_drop_redirect="NO"	ICMP redirect を破棄
icmp_log_redirect="NO"	ICMP redirect を記録
ipfilter_enable="YES"	ip filter を有効化
ipmon_enable="YES"	ipmon を有効化
firewall_enable="YES"	ipfwを有効化
firewall_type="simple"	ipfw を「simple」で初期化

- ロギング

accounting_enable="NO"	アカウンティングを有効化
inetd_flags="-wWl"	デフォルトは -wW

- kernel securelevel 機能

kernel_securelevel_enable="YES"	kernel securelevelを有効化
kern_securelevel=1	デフォルトは -1

/etc/sysctl.conf 設定例

- 高負荷サーバ
  kernel.ipc.somaxconn=1024
  kern.ipc.maxsockets=16384
  kern.ipc.nmbclusters=65535
- blackhole(4)（副作用に注意! traceroute に反応しなくなる）
  0: RST を返す　1: SYN には何も返さない　2: 何も返さない
  net.inet.tcp.blackhole=2
  net.inet.tcp.blackhole=1
- squid みたいな特殊なもの用（？）
  kern.maxfiles=32767
  kern.maxfilesperproc=16424
  net.inet.ip.portrange.first=8192
  net.inet.ip.portrange.last=65535

各種 daemon の設定ファイル

- ssh (/etc/ssh/sshd_config)
  - UsePrivilegeSeparation yes
- inetd (/etc/inetd.conf)
  - ftpd –l –l
- login (/etc/login.conf)
  - :minpasswordlen=12:

パケットフィルタで設定すべき事

- あり得ない（はずの）パケットを取り除く
  - http://www.sans.org/dosstep/index.htm
- 危険なパケットを取り除く（IP option つき、パケット長が異常、など）：ip filter での例

```
block in log quick from any to any with ipopts
block in log quick proto tcp from any to any with short
block in log quick proto icmp from any to any icmp-type redir
block in log quick proto icmp from any to any icmp-type routerad
block in log quick proto icmp from any to any icmp-type routersol
```

- その他、サイト毎の設定
  - /etc/rc.firewall（ipfw 設定ファイル）は参考になる
    さきほどの「simple」もここに記載されている

IP filter v.s. IP firewall (ipfw)

- IP filter – いろんなプラットホームで使える
- IP firewall – FreeBSD 標準
- 最近の標準状況
  - FreeBSD – ipfw
  - NetBSD – ip filter
  - OpenBSD – pf (packet filter)
  - BSD/OS - ?
  - Mac OS X – ipfw
  - Linux – ipchains / iptables
  - HP-UX – ip filter (?)
- FreeBSD の場合、ふつうの人は、ipfw の simple をベースにしてカスタマイズするのがよいような気がする。

OS を最新状態に

- CVSup で最新のソースを入手
  - cvsup –g supfile
  - supfile の中身
    *default host=cvsup.jp.freebsd.org
    *default base=/usr
    *default prefix=/usr
    *default release=cvs tag=RELENG_4_6
    *default delete use-rel-suffix compress
    src-all
- 複数の FreeBSD を維持する場合はローカルの CVSup ミラーを構築し、そこから CVSup した方がよい
  - ports の net/cvsup-mirror を利用すると簡単に構築できる
- 変更点にあわせて再構築
  - 部分的でいい場合が多いが、make buildworld; make installworld が必要な場合もたまにある。事例: DNS resolver 脆弱性

更新情報を得る

- FreeBSD 友の会主催の FreeBSD-announce-jp ML に加入しておこう
  - http://www.jp.freebsd.org/
- 更新情報: 主にセキュリティ情報
  - 情報をよく読んだ上で CVSup して source 更新し再構築
- 体力があれば FreeBSD-users-jp ML にも参加
  - 特に新リリース登場時などでは、トラブル報告はまず ML に現れる
  - かなりの流量があるので覚悟する

ports/packages 活用

- ports - /usr/ports/*
  - 3rd party ソフトウェアを有志が移植（port）したものが、一定の手順に従って大量に集積されている
  - 他のソフトウェアに対する依存情報も含まれており、依存するソフトウェアがインストールされていなければ、そのソフトウェアもあわせて自動的にインストールされる
  - つくりかた: security/sudo の例
    - cd /usr/ports/security/sudo
    - make
    - make install
  - OS リリース時点での ports の内容を元に作成されたバイナリ「パッケージ」が OS に添付されている

最新の ports

- 最新の ports（ports-current）は CVSup すれば入手できる
- supfile の中身
  *default host=cvsup.jp.freebsd.org
  *default base=/usr
  *default prefix=/usr
  *default release=cvs tag=.
  *default delete use-rel-suffix compress
  ports-all
- ports-current は FreeBSD 開発版（-current）と安定版（-stable）でしか試されていないので注意。
  - ある時点の安定版を取り出し、さらに検証を行ったものが RELEASE 版として登場する
  - ports-current は、たいていは RELEASE 版でもちゃんと動くが、…

ports みてあるき

- net/
  - bsdproxy – 汎用 proxy サーバ
    - stone
  - ethereal – ネットワークアナライザ★
  - honeyd – for honeyports
  - iplog – TCP/IP ロガー★
  - netcat – 強力ツール★
  - ngrep – ネットワーク grep
  - ntop – ネットワーク top
  - socks5 – NEC socks5
    - dante

ports みてあるき

- security/
  - snort – ネットワーク IDS
    - acid, snort-snarf
  - amavis-perl – アンチウィルス メールフィルタ
    - amavisd, amavisd-new, inflex
  - arirang – web スキャナ
    - nessus, saint, whisker
  - bcwipe – ファイル / ディスク消去ソフト
  - ca-roots – CA ルートファイル (old!)
  - chkrootkit – rootkit チェッカ ★
  - dsniff – パスワード盗聴ソフト★

ports みてあるき

- security/
  - fragrouter – IDS テストツール
    - hping
  - gnupg – GNU OpenPGP
    - pgp5, pgp6
  - john – パスワード解読ソフト★
    - crack
  - nmap – ポートスキャナ★
    - portscanner, strobe
  - portsentry – ポートスキャン検知ソフト
  - pscan – ソースコード検査ソフト
    - its4, rats

ports みてあるき

- security/
  - openssh – OpenSSH
    - openssh-portable, ssh2, lsh
  - sudo ★
    - super
  - swatch – simple watcher
    - logcheck
  - tripwire – ファイル整合性検査ソフト★
    - aide, integrit
- www/
  - squid – www proxy
    - tinyproxy, transproxy

その他

- 情報源
  - 本家 - http://www.freebsd.org
  - FreeBSD 友の会 - http://www.jp.freebsd.org
  - 各種 ML
  - 雑誌
    - FreeBSD Press
    - BSD magazine
    - その他、ネットワーク系・セキュリティ系雑誌など