楽をしたい管理者のためのサーバ構築法

- **第I部 作るもの**
  - 1. 発端
    - 突然サーバ壊れちゃった
    - 新規購入決定
    - やるなら，新規インストール
  - 2. 今までの機械は...
    - (Pentium!!! 1GHz の 1U サーバ，IDE 40G HDD) x 2
    - Mail, DNS サーバ（今回壊れた方）
      - NetBSD 1.6 系で運用
      - qmail は apop 用のパッチを手で当てて作成
      - imap サーバは pkgsrc を使わずにインストール
    - Web, squid サーバ
      - Debian woody
      - バッケージの apache
      - squid は自前でコンパイル
    - 1日1回，互いのデータを rsync でコピー
    - どちらかが壊れたらすぐに復旧できるように，ほぼ同じアプリケーションをインストール
  - 3. 今回の計画
    - 2台の機能を1台に統合する.
    - 旧サーバのうち動いている方は，バックアップ&テスト用環境とする.
  - 4. メールサーバ
    - メール利用者は 20〜30人位.
    - SMTP（内部からの中継含む）
    - POP（APOP 認証のみ）
    - IMAP over SSL
    - IMAP（lo0 のみ．ssh 経由で利用）
  - 5. DNS サーバ
    - 7個のドメインとその逆引きのプライマリ
    - 9個のドメインとその逆引きのスレーブ
    - もちろんキャッシュサーバ
  - 6. Web サーバ
    - 外部向け
    - とりあえず cgi は必要ない.
    - CVS でコンテンツを管理しているらしい.
  - 7. squid
    - wpad で自動設定.
- **第II部 楽をするための下地作り**
  - 1. ハードウェア選び
    - Pentium4 3GHz
    - SCSI HDD で RAID1
  - 2. OS 選び

- SA が出たときにパッチをあててコンパイル，なんて手間のかかることはしたくない．
  - FreeBSD
    - OS 本体 ... 最近バイナリアップデートを提供している人がいるらしい．
    - ports ... portupgrade は ports からコンパイルが主．サービス停止時間が長い．
  - NetBSD
    - OS 本体 ... ソースにパッチをあててコンパイル
    - pkgsrc ... make update / pkg_chk -i 等，アップデートの際の依存関係の解決は，「依存するものを全部アンインストールしてインストールし直す」が基本．
- 必要なもの以外インストールしたくない．
- 頻繁にバージョンアップしない．
- 結論：Debian しかない（ちょうど sarge でたばかりだし）

- 3. インストールの方針
  - できるだけパッケージを使う
    今の所必要なものはすべてパッケージでインストールできている．
  - できるだけデフォルトは変更しない
    設定ファイルの変更点は最小限に抑える．
  - 自分が手で編集する場合，設定ファイルのコピーを残す
  - デフォルトでインストールされる物でも，必要ないパッケージは積極的に消す
  - 悩みどころ
    - カーネルのカスタマイズ
      必要ないものは入れないという方針からすれば，不要なドライバは削った方が良い．楽にアップデートするという点からみれば，いじらない方が良い．→ 今はパッケージのまま．
    - パーティション
      今どきは1つでもいいのかもしれない．けど... 結局こうなりました．

/dev/sda1 /	512M	ext3
/dev/sda6 /usr	2G	ext3
/dev/sda7 /var	2G	ext3
/dev/sda8 /cache	20G	ext2
/dev/sda9 /u	40G	ext3

    - MTA
      qmail? postfix? sendmail?
      今までのサーバとの整合性を考えて qmail を選択．
      APOP は solid-pop3d を使用．
      IMAP は courier imapd を使用．

- **第III部 管理を楽にするために**
  - 1. 方針
    - 1回しかやらなくていいことは素直に手作業する
      スクリプトでやろうとすると，凝り始めて，いろんなことができて，いろんなエラーにも対応できるけど，1回しか使わないスクリプトが出来上がり，何倍も時間を浪費する．
    - 何度もやらないといけない作業は「特定の人だけが使うための」「単機能」スクリプトを作る
      誰でも使えようとしたり，いろんな状況に対応できるなんてことを考えると，自分も毎回使い方を調べるはめになる．
      最小限の引数のみとるようにする．オプションは付けない．

楽をしたい管理者のためのサーバ構築法

- がんばって作業手順をドキュメント化する
  誰かにやってもらう時のために必要.
  「誰か」をできるだけ少数に絞り込んで，その誰かにだけ分かるように書く.
  読めば誰でも出来るように作ろうなんていう無駄な努力はしない.
- できない人には触らせない
  やり方を聞いてくる人にやり方を説明するより，こちらでやった方が早いことが多い.
  （できる人は聞かない）

- 2. 発生する作業
  - ログの管理
  - SA のチェックとアップデート
  - ホストやドメインの登録
  - メールアカウントの追加/削除
  - エイリアスやメーリングリストの追加/削除
- 3. ログのチェック
  - /var/log にあるもの

apcupsd.events	aptitude	auth.log	btmp
daemon.log	debug	dmesg	kern.log
lastlog	lpr.log	mail.err	mail.info
mail.log	mail.warn	messages	syslog
upsstat.log	user.log	uucp.log	wtmp

  - メールでレボートを送るようにしたい（未実装）
- 4. SA のチェックとアップデート
  - Debian のセキュリティーチームを信じる.
  - アップデートのチェック
    1日1回次のコマンドを動かして，結果をメールで送る.
    --

```
apt-get update -qq        # パッケージリストの取得
apt-get upgrade -sqq      # バッケージアップグレードを dry-run
```

    --
    dry-run しているのは，どのパッケージがアップグレードされるのか確認するため．アップデートしなければいけないが場合だけメールが届くので，ログインして手作業で apt-get upgrade する.
    apt-get upgrade のオプションを変更すれば，アップグレードも自動化できるが，そこまではやっていない.
- 5. ホストやドメインの登録
  - bind のファイルの形式は複雑
    ホストの情報，プライマリネームサーバのアドレス等が複数のファイルにある.
  - 実際に必要なのは，マスター，スレーブとなるドメインの情報と，マスターの /etc/hosts ファイル程度で十分.
  - 簡単で見通しの良い形式のファイルを bind9 用の形式に変換するようなスクリプトを作成
    /etc/hosts みたいなファイルと，ドメイン情報が入ったファイルから，正逆用データベースと named.conf を生成するスクリプトを作成.
- 6. メールアカウントの追加/削除
  - この環境では，メールアカウント = ログインアカウント
    メールしか使わない人用に，POP しかできないアカウントを作った方が良いかもしれない.
    利用者の顔をすべて知っているのでそのまま運用している.
    shell は通常 false か rbash になっている．（パスワード変更，フォワード設定ができるように）

- 追加スクリプトの作成
  ユーザとグループの登録，ホームディレクトリの作成，Maildir と .qmail の作成，APOP パスワードの設定をする1つのスクリプトを作成.
- 7. エイリアスやメーリングリストの追加/削除
  - エイリアスのみで運用
    qmail の場合は，/var/qmail/alias/.qmail-アドレス というファイルを作成し，そこにアドレスを列挙するだけ.
    以前は fastforward で /etc/alias ファイルを使っていたが今は .qmail-* に統一.
  - ML サーバは使っていない
    自動登録やヘッダの書き換えは必要とされない．Reply-To が付く ML サーバを使ったら，おばかなメールが蔓延するだけ.
    ML 上で議論する，といった発想がないらしい．議論したい場合は「今メール送ったんだけど...」という電話がかかってきたり，本人が来たりする．（そのメールを読むよりも，電話や本人がくる方が早い場合が多い）
- 8. これからの課題
  - 人に作業を委譲する
  - バックアップサーバのインストール
  - メールバックアップ方法の改善
- 9. （付録）今回のトラブルで分かったこと
  - IMAP の ID 重複問題