

ケーススタディ(qmail)

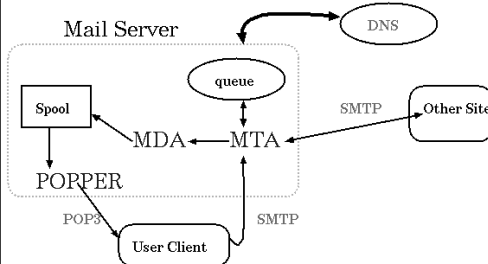
NAIST用メールサーバ構築
sendmailからqmailへの移行
荒木靖宏
IIJ/(NAIST)
ar@ij.ad.jp

メールサーバの要件

- 1.信頼性/安全性:きちんと届く
 - 2.利便性:運用上の要求への対応
 - 3.高速性:十分な速さで動作
高速性は、あくまでおまけ。
- 結局のところ..
プログラム(の組みあわせ)と運用で評価される

メールサーバ概観

おおざっぱな話



このそれぞれがきちんと動作する必要がある

メールサーバの構成要素

MTA

- ホスト間メール転送:sendmailなど

MDA

- ローカル配送:/bin/mailなど

POP/IMAP

- ホストからユーザクライアントへの転送

DNS/リゾルバ

- ホスト間メール配送にはDNSが欠かせません

その他のソフト

- ML、biff、filterなど

qmail

<ftp://koobera.math.uic.edu/www/djb.html>

特徴

- 宛先毎(MX相乗り無し)に一連の配送プロセスが起動する
- 機能別に分かれた9つのメインプログラムと補助プログラム
- qmail-queueだけがsetuidされている
- 典型例:

qmail-smtpd, qmail-queue, qmail-send, qmail-rspawn, qmail-remoteと5

つのプログラムを経る

機能一覧については <http://www.jp.qmail.org/q103/jblurb/blurb3.html>

安全性

- アドレス(&)、ファイル、プログラム(!)をはっきりと区別
- setuidされたコードはひとつ qmail-queue
- root権限で実行されるコードも必要最小
(qmail-start, qmail-lspawn)

受信サービス qmail-smtpd

- 8-bit透過
- 中継の制限 --- 外部からの不法な中継利用を禁止 (control/rcpthosts)
- 中継機能と転送機能の独立設定
- tcpdなど
- ローカルIPアドレスは自動認識
- ホップカウント機能

キューの管理 qmail-send

- キュー登録後、直ちに処理開始
- 並列度の限定 (control/concurrencyremote, control/concurrencylocal)
- 分割されたキューディレクトリ --- キューが大きくなっても遅くならない
- キューの掃除/表示 qmail-clean qmail-qread

転送とメイリングリスト qmail-local

- アドレスワイルドカード (.qmail-default, .qmail-foo-default, etc.)
- sendmailのforward互換機能(dot-forwardパッケージによる)
- 高速転送のためのデータベース(fastforwardパッケージによる)
- sendmailの/etc/aliases互換機能(fastforward/newaliases)
- VERP --- メイリングリストでのバウンス時、宛先を特定する
- Delivered-To --- ループの検出、ホストを跨いでも可能

ローカル配送 qmail-local

- アドレス階層 --- fredがfred-xxxのアドレスを管理
- mbox / maildir への配送
- 利用者が指定できるプログラム実行: procmailなど (qmail-command)
- 新着メールの通知 (qbiff)

メールサーバの規模と用途@NAIST

規模

- 2000人ほど(8つのdomain,重複usernameは無し)
- LAN内部
- 約600個のML

用途

- 通常の学内外とのメール
- ML(全学教職員への連絡等はほぼMLで行われる)

要件

要件

- メール転送設定、procmail等の使用を許容
- ユーザはPOP/RPOPでメールを読む
- ユーザはそのままの設定で使えること

ユーザ層

- 研究者(手元に環境持つことが多い) or 事務員(とにかくユードラ)
- forward設定している人が多数

条件

- firewall下。*.aist-nara.ac.jp のMXはすべてこのホスト
- しかし他のマシンへSMTP配送は行う
- 学内マシンは全ていくつかのfileサーバにhomeを持つ
- ユーザ管理はNIS
- MLはdistribute/majordomo/素のaliases/fmlなど
- メールサーバには一般ユーザはloginできない

sendmailでの運用設定

変更前夜…

- 学内配送時MXを無視するlocalhackする以外は、wide patchあてただけ
- 8つのドメインがついたメールを受けとる
- .forwardは/var/forward/domain/USERNAME
- mbox形式。/bin/mailで /usr/mail/USERNAMEに配送
- ユーザのhomeはNFSサーバ上(procmail,RPOP等が使用)
- popperはdaemonに改造したqpopper1.8

運用状況

- 全ユーザ(約2000)への配送は平常時6時間程
- procmailを利用するユーザが多いMLは普段から配送が遅れ気味だった
- ML等でprocmail等が失敗するユーザ(30人=1.5%程)がいると配送が大幅に遅れる
- UNIXでのユーザはほとんどRPOPを利用するためNFSと一蓮托生

ローカル配送の遅さが問題
NFSが悪者

新サーバの設計と概要

目標

- 遅い一部のユーザに足をひっぱられないシステム
- とにかくローカル配送の高速化をはかる
- 将来のドメイン毎に移行できるようなシステム

概要

- ハードウェアはUltraEnterprise3000 RAID-0,1
- NFSは追放する
- qmailの利用
 - IPベースのバーチャルホスト(設定、バイナリ、キューも独立)
 - スプール位置のhash化
 - スプール配送時にgetpw()を使用しない
- POPはRPOP/POPを使えるようなqpopper

運用の工夫

Bindも動かす

互換性のためsendmailマシン設置

- NFSが必要な場合はここを使う
- procmailを使うユーザ
- sendmail依存のML
 - ML宛てメールはメールサーバから転送される

メールスプール

localhost名は /var/qmail/control/local

- ローカル配送にDNSは使わない

メールサーバ上のユーザディレクトリを作成

- Maibox(mbox形式)に配送 (popperとの関係)
- .forward, .rhostsをおく
- このディレクトリ位置はhash化
- /mailid/HASHLETTER/USERNAME
 - getpw()と一致するようにリンクを作成
 - ex. /mail/c/yasuhi-a -> ~/yasuhi-a
- qmailはcdb化されたデータベースを使って位置特定して配送
 - /var/qmail/control/assign.cdb

メールスプールの階層化あれこれ

qpopper & procmailでのサポート

- /var/spool/mail/u/s/username
 - NAISTではk-chinnenのように“-”と組んだ名前が多く効果が薄い?
- /var/spool/mail/HASHLETTER/username
 - 位置が直感的にわからないのが欠点。4文字目までのhash

Spool/キューの信頼性

fsync()

- きちんとinodeが反映される必要がある
- 一般にはmountはsyncで

/usr/mail/\$USER or mbox形式

- ひとりのメールは一つのファイル
- 一般的にサポートされている
- MDAがsetuidされるorディレクトリモードが666
- アクセスするプログラムにロック機構が必須且つ厳重に管理する必要有
- NFSでは特に注意が必要

Maildir形式

特徴

cur/ tmp/ new/ に分けた構造
1メール1ファイルのためロックが不要

対応状況

- MDA: qmail/postfix/deliver/maildrop等がサポート
- MUA: pine/mutt/im
- POP: qmail-pop3d/UW ipopd(patch)
- IMAP: UW imap4(patch)
- xbiff: xbuffy/gbuffy

qmailの配送制御

me

- hostnameを指定する(最低限これだけは必要)

smtproutes

- 配送経路を指定する
 - 例えば is.aist-nara.ac.jp:ismailgate.aist-nara.ac.jp

concurrencylocal / concurrencyremote

- ローカル / リモート配送の並列配送度
- 最大で255並列まで。プロセス制限に注意

SPAM対策

受信制御

- locals
 - ローカルメールとして処理すべきアドレス
 - ▶ 例えば is.aist-nara.ac.jp とする
- rcpthosts
 - RCPTに対応
 - ▶ 例えば .aist-nara.ac.jp とするとNAISTドメイン全てを受信
- badmailfrom
 - 拒否するアドレス
 - ▶ friend@pubic.com : メールアドレスで拒否
 - ▶ @doki-doki.com : ドメインまるごと
- databytes
 - 許可する最大メールサイズ

SPAM対策(2)

abuse@DOMAINNAMEを用意する

- spamが起きたときの対応窓口
- 自動返送スクリプト
- RFC2142にあるサービスは設置する
 - メールならpostmaster
 - DNSはhostmaster などなど

ブラックホールリストの利用

- 使うデータベースをよく考える
 - rblsmtpd → データベースサーバ名 qmail-smtpd

そのほかNAISTで困った例

- Message-IDをつけないMUA
- RCPT TO: address の処理がおかしいMUA
- Message-Loop?