6. sendmailシステム管理

Contents

- メールボックス
- 受信の一時拒否
- メールのサイズ
- 配信処理効率
- mqueue管理
- Ident プロトコル
- エラー通知
- Return-Receipt
- プライバシー
- MIME
- 統計
- その他の落とし穴
- 日常管理
- セキュリティ

メールボックス (cont.)

- ローカル配信用プログラム
  - binmail, mail.local
  - OS 添付の sendmail.cf を参考にする
    - local mailer 定義 (Mlocal 行)
  - 最新の mail.local を利用するのが安全
- ディスクの溢れ
  - TEMPFAIL(75)が返ること
  - /tmp/ の溢れも検出できること (使うなら)

メールボックス (cont'd)

- quota 制限時の注意
  - 複数同時配信の抑制
    - 一人が制限を越えると他人に何通も届く
    - 誰宛の配信がエラーになったのかが不明なため
      - LMTP (RFC2033(I)) へ
  - mailer flag F=...m... の m をはずす
    - local mailer (Mlocal の行)
    - 一人ごとに mailer を起動

受信の一時拒否

- 高負荷時
  - O RefuseLA=12
- mqueue の空きが少ないとき
  - O MinFreeBlocks=100
- 従来の非応答処理
  - accept せずにほったらかし(従来)
    - 遅延の原因になり、よくない
  - socket を close
    - connection refused、すぐに次の MX へ

メールのサイズ制限

- O MaxMessageSize=1000000
  - ESMTP で受信前にチェック
    - RFC1870(S)
    - MAIL FROM:<addr> *SIZE=1234*
- mailer 定義の M=式
  - Msmtp,... M=1000000
  - sendmail 8.8.5 (古い!) はうまく機能しない

配信処理効率の向上 (cont.)

- コネクション・キャッシュ
  - O ConnectionCacheSize=2
  - – 連続配信の際にSMTPコネクションを再利用
  - – run-queue (sendmail -q) に効果的
- 配信状況情報の活用
  - O PersistentHostStatus=.hoststat
  - – mqueue に情報を保存
    - # mkdir /var/spool/mqueue/.hoststat
    - .hoststat/jp./ac./kyoto-u./… に情報を保存

配信処理効率の向上 (cont'd)

- Timeout.hoststatus=30m
  - 配信失敗から30分以内は再試行しない

- 相手ホストに対する考慮
  - SingleThreadDelivery
  - 同時に複数のコネクションを張らない

mqueue 管理 (cont.)

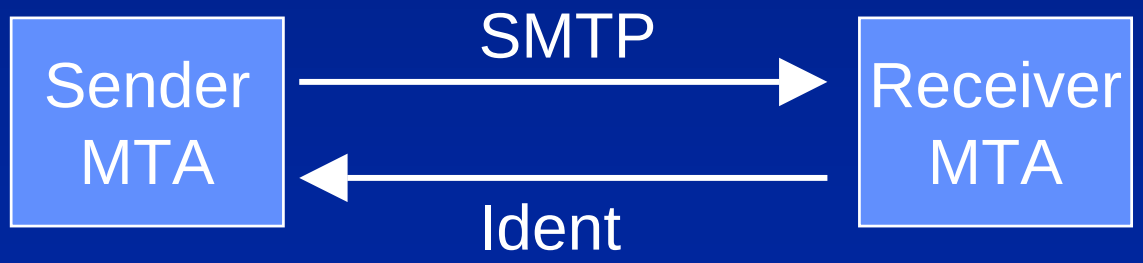
- 頻繁な処理の抑制
  - O MinQueueAge=30m
- 指定したメッセージだけ配信
  - sendmail -qI*qid*
  - sendmail -qS*sender-substr*
  - sendmail -qR*rceiver-substr*
- ETRN (リモートから sendmail -q)
  - RFC1985(PS): Remote Message Queue Starting

mqueue 管理 (cont'd)

- 処理の順序
  - 停電復旧後に届くメールの順序を時間順に
  - O QueueSortOrder=time
    - デフォルトは priority
      - サイズ、受信者数、Precedence: などから算出
- mqueue の集約
  - O FallbackMXhost=fall.back.host
  - 指定した fall.back.host に転送
    - DNS から得られた MX に送れなかったとき

Identとfirewall (cont.)

- Ident (識別)プロトコル (133/TCP)
  - RFC1413(PS)
  - 発信者の識別情報の問い合わせ
    - ユーザID (login name)
    - 完全に信頼できる情報ではない



Identとfirewall (cont'd)

- フィルタが Ident に対して host unreach
  - SMTP も一緒に切れてしまう

  → メールが送れない

→ 静かに捨てる
  - タイムアウト待ちが発生するが、届く

→ port unreach を返す

エラー通知 (cont.)

mqueue に入ってからの経過時間に基づく

- 返送するまでの時間
  - O Timeout.queuereturn=5d
  - – 長期休業の際に注意
    - Lower-MX での設定
  - – Preference: が負なら本文を返さない
  - – エラー通知(発信者が<>)に返送しない

エラー通知 (cont'd)

- 未配信(まだ届いていないこと)を通知
  - O Timeout.queuewarn=4h
  - – Preference: が負なら通知しない
  - – エラー通知(発信者が<>)に通知しない
- 負の Preference:
  - – list, bulk, junk
  - – sendmail.cf の P 行で定義
    - Plist = -30

エラーのモニタ

- エラー発生時に postmaster にも通知
  - O PostMasterCopy=postmaster
  - – ヘッダ部分のみ
    - Subject: は見えてしまうので注意
- ダブル・エラー
  - – 発信者への返送不能
  - O DoubleBounceAddress=postmaster
  - – 本文を含めて通知
    - オプションにすべき(?)

Return-Receipt-To:の現在

- RFC1891(PS): DSN (Delivery Status Notification)
  - sendmail 8.7 以降
  - 古い sendmail が途中にあるとダメ
- Return-Receipt-To: ヘッダの廃止
- エンベロープで指定
  - RCPT TO:<*addr*> NOTIFY=*success*
- エンベロープの発信者に通知
- sendmail -N *success*

プライバシーを守る

- O PrivacyOptions= (, で区切って複数指定)
  - authwarnings
    - 不審な挙動に X-Authentication-Warnings: を付与
  - noexpn, novrfy
    - EXPN (転送先の確認) の禁止
  - restrictmailq
    - 一般ユーザの mailq コマンド利用規制
  - noreceipts
    - Return-Receipt の抑制

MIME形式の利用

- MIME 形式のエラー通知
  - O SendMimeErrors=True
- 7Bit しか通らないところへの配信のため
  - O SevenBitInput=False
  - O EightBitMode=pass8
    - 8Bit → 7Bit (base64/quoted-printable encode)
    - Content-Type: unknown-8bit がついてしまう
- 7Bit → 8Bit デコード
  - mailer flag F=9 の指定の場合

配信統計

- syslog から収集
- mailstats コマンド
  - O StatusFile=/var/log/sendmail.st

M	msgsfr	bytes_from	msgsto	bytes_to	Mailer
3	1308	6475K	4072	14975K	local
4	3450	15797K	1819	5681K	smtp
T	4758	22272K	5891	20656K	

- 情報のクリア
  - cp /dev/null sendmail.st

ありがちな落とし穴 (cont.)

- 2行greetingに対応していない相手
  - sendmail 8.6までの問題

    220-mail.x.co.jp Sendmail 8.6.13 …

    220 ESMPT spoken here
- SMTPコネクションを再利用できない
  - コネクションキャッシュサイズを 0 に

    O ConnectionCacheSize=0

ありがちな落とし穴 (cont'd)

- アドレスにコメントがついていると受け取れない
  - mailer flag に F=C を足す
- 同時に2人以上の宛先で受信できない
  - mailer flag から F=m を削除
- 古い(?) TIS FWTK の smapd
  - 5xx のエラーコードなのにキューに保存する
    - エラーメールが何通もくる
  - アドレスに / が使えない (X.400 アドレス)

日常管理

- アドレスの廃止
- NFS関連
- 停電からの回復
- システムリプレース

アドレスの廃止

- 異動/転勤/卒業/除籍
  - 単に削除
  - アドレス変更通知

    oldaddr: newaddr.redirect (/etc/aliases)

    エラーメッセージ：User has moved; please try <*newaddr*>
  - 新アドレスに転送
  - 通知つき転送

    oldaddr: newaddr.forward, newaddr

    エラーメッセージ：User has moved; your mail has been forwarded; next time please try to <*newaddr*>

NFS はトラブルのもと (cont.)

- メールボックス
  - lock の不完全問題
    - メールを失う可能性
- ホーム・ディレクトリ
  - mount に時間がかかる (automount)
  - .forward の無視 (マウントに失敗したとき)
    - .forward の置き場所をローカルに

      O ForwardPath=$z/.forward:/var/forward/$u/.forward

NFS はトラブルのもと (cont'd)

- プログラム共有
  - プログラムが見つからずエラーで返送
    - マウントに失敗したとき
      - 停電後の起動の順序問題
    - vacation, slocal,...
- 設定ファイル
  - セキュリティチェック
  - ファイルの所有者の権限で実行されない
    - :include:

停電からの回復

- NFS マウントの順番
- ネームサーバを先に
  - メールサーバは後
  - メールサーバで named を動かす
    - Secondary にする
  - 自分の FQDN が引けない
    - アドレスの認識を誤る恐れがある
    - sendmail が常駐しない (メールが届かない)

システムリプレース (OSのバージョンアップ)

- 未設定のsendmailが動くとひさん
  - 回復後に届いたメールがエラーになる！
  - 使っていた sendmail.cf を残しておく
  - 未処理メールの確認 (mqueue)
    - run-queue プロセスが動くとまずい
  - ネットワークをはずしておく
  - sendmail を殺してから接続
    - リブートの場合は /etc/rc から起動されないように

メールサーバとセキュリティ (1)

- CERT report をチェック (www.cert.org)
- 最新の sendmail にする
- パッケージの PGP シグネチャの確認
  - トロイの木馬対策
- 各種ファイルのパーミッション
- SafeFileEnvironment option の活用
- smrsh の利用

メールサーバとセキュリティ (2)

- 発信者認証
  - POP サーバアクセス権による確認
  - XTND XMIT (POP) を利用したメールの発信
  - identd
- ヘッダから internal address を隠す
- 無用な転送の防止
  - メール爆撃、スパムの踏み台