DNS&Mail

ウェザーニューズ（株）システムコンテンツ開発事業本部
安藤一憲
ando@wni.co.jp

1

このチュートリアルの構成

- DNSの重要性
  - 階層構造を持った分散データベース
  - 多国語対応
- メール配送のモデル
  - MX配送、static配送の使い分け
- メールの抱える問題
  - SPAM対策、ウイルス、チェーンメール

2

DNSの重要性

- あるドメインのリソース情報へ到達する鍵
  - 順次NSを手繰ってデータを引きに来る仕組み
    - 手繰れないと破綻
  - IPアドレス付け替え時、ドメイン変更時に注意
  - ほぼ全てのサービスに影響
    - FQDNを用いるもの全て
  - NSを死守すべし
    - 全ての基礎となるサービスのひとつという位置付け

3

DNS多国語ドメインとメール

- RACE（ASCII互換）、UTF8方式等
  - いまのところWWW用に留まっている?
  - MUAが頑張るのかMTAが頑張るのか?
  - まだ考えられていない部分が多いのでは?
    - USの人間は日本語のアドレスを扱える?
    - アラビア語ドメインのアドレスは入力できる?
    - 問題は単純ではないと思われる

4

DNSとメール

- user@example.gr.jp
  - ここから配送先をどう見つけるか?
  - 手がかりはドメイン名の部分
- example.gr.jpのMXレコードを調べる
  - 配送にはMXとサーバのAレコードが必要
    - 最も効率が良いのは、 MXを聞いたらMXだけではなくAが同時に返ってくる場合
    - 答えるnamedがMXとAを両方知っているのがベスト

MXはCNAMEではいけない

- O DontExpandCnames=False
  - RFC822,1123的にはたぐるのが正しい
  - IETFはCNAMEをたぐらない方向に動いている
  - というわけでsendmailはオプションにする模様
- DNSのMXはCNAMEを指定してはいけない
  - RHSにはAを書く
  - そのAはMXを答えるnamedが知っていると良い

ワイルドカードMXは使わない

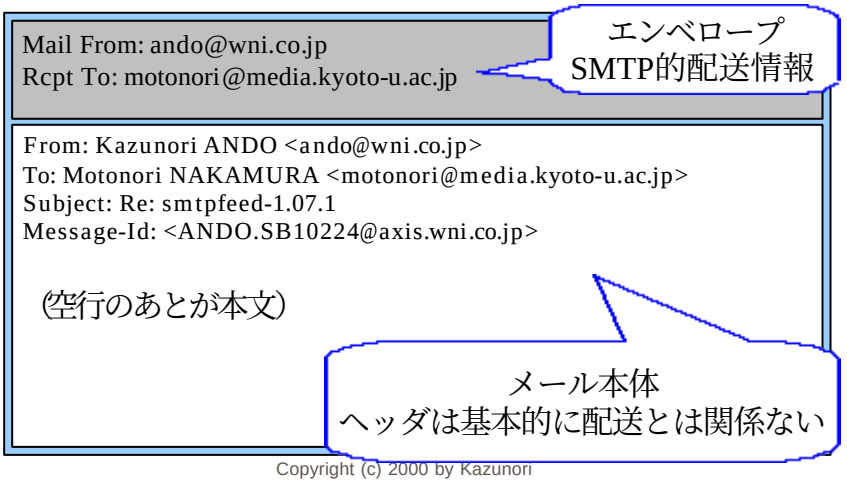
- 手抜きはいけません
  - sendmailのREADMEには…
    - ワイルドカードが自分のドメインを含まない特殊なDB
    - 指している先がfirewall

  という状況でしかうまく動かない
  これ以外だと頭痛のタネにしかならない

  と書いてあったりする

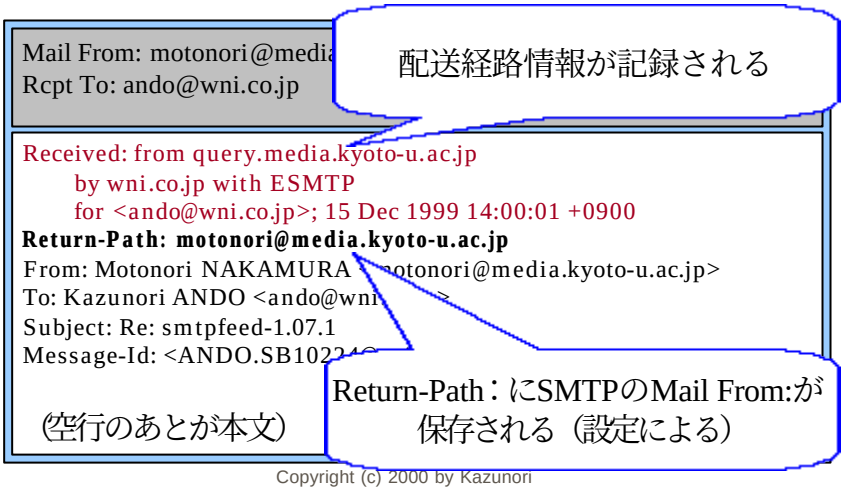
7

メール本体とエンベロープ



8

メール本体とエンベロープ (2)



メール本体とエンベロープ (3)

- え？ To: に書くとそこに送られるじゃん...
  - それはMUAの仕業
  - To: ヘッダに書いたアドレスをSMTP的な配送先情報としてMTAに渡しているだけ
  - 例えば、To:ヘッダがメーリングリストのアドレスなのに自分にメールが届くのはこのため

ヘッダの話 (1)

- Field-name: Field-body (standard)
  - From: 差出人アドレス
  - Sender: 差出人アドレスが不明確な場合に差出人を明示
  - To: 宛先アドレス
  - Cc: カーボンコピー
  - Reply-To: 返信先アドレス
  - Message-Id: ５年間固有のID
  - Subject: タイトル
  - Date: 差出時間
  - Return-Path: エラー返信先アドレス

ヘッダの話 (2)

- Field-name: Field-body (standard)
  - Received: 配送経路
  - In-Reply-To: どのメールに返信したかを示す
  - References: どのメールに返信したかを示す
- Resent系（メールを再配信する場合の）
  - Resent-From: 差出人アドレス
  - Resent-Sender: 差出人アドレスが不明確な場合に明示
  - Resent-Reply-To: 返信先アドレス
  - Resent-Message-Id: ５年間固有のID
  - Resent-Date: 再配信日時

ヘッダの話 (3)

- Field-name: Field-body
  - Precedence: 配送優先度
  - X-Authentication-Warning: アドレス詐称（?）
- (おまけ) MLドライバ等の付けるヘッダ
  - X-MLServer: fml
  - X-ML-System : ppml
  - X-Ml-Version: kkml
  - X-Distribute: distribute
  - Delivered-To: qmail

13

文字の話

- 機種依存文字を使ってはいけない
  - ①②③④⑤⑥⑦⑧⑨⑩
  - Ⅰ ⅡⅢⅣ Ⅴ ⅥⅦⅧⅨ Ⅹ
  - ﾄｳｾﾞﾝﾊﾝｶｸｶﾀｶﾅﾓﾀﾞﾒ
- 漢字コードはISO-2022-JPを使用する
  - SJISだめ、EUCだめ、UNICODEだめ

14

配送の実際 (1)

- 宛先アドレスのMXを引いてみる
  - MX 10 mail-g1.example.gr.jp
  - MX 10 mail-g2.example.gr.jp
    - この場合はランダムでどちらかに配送
  - MX 10 mail-g1.example.gr.jp
  - MX 20 mail-g2.example.gr.jp
    - この場合は10の方に配送して駄目だったら

配送の実際 (2)

- MX RRの他にも答がいっぱい返ってくる

```
example.gr.jp   MX  10   mail-g1.example.gr.jp
example.gr.jp   MX  20   mail-g2.example.gr.jp
```

MX RR

```
example.gr.jp   NS   ns1.example.gr.jp
example.gr.jp   NS   ns2.example.gr.jp
mail-g1.example.gr.jp   A   202.250.31.150
mail-g2.example.gr.jp   A   202.250.31.151
ns1.example.gr.jp    A  202.250.31.148
ns2.example.gr.jp    A  202.250.31.149
```

additinal information

実際の配送 (3)

- Additional Information
  - MXを聞かれたNSがMXのAも知っている
    - MXとAがわかれば実際に接続しにいける
    - １回のqueryで済むので効率が良い
    - MX RRを保持しているNSがAも保持することが重要
  - Additional InformationとMTA
    - 例えばSMTPfeedはAdditional Informationを利用
    - MTAが利用しなくても手元のnamedがcache
      - Aを聞きに行くとそこが答えるので速い

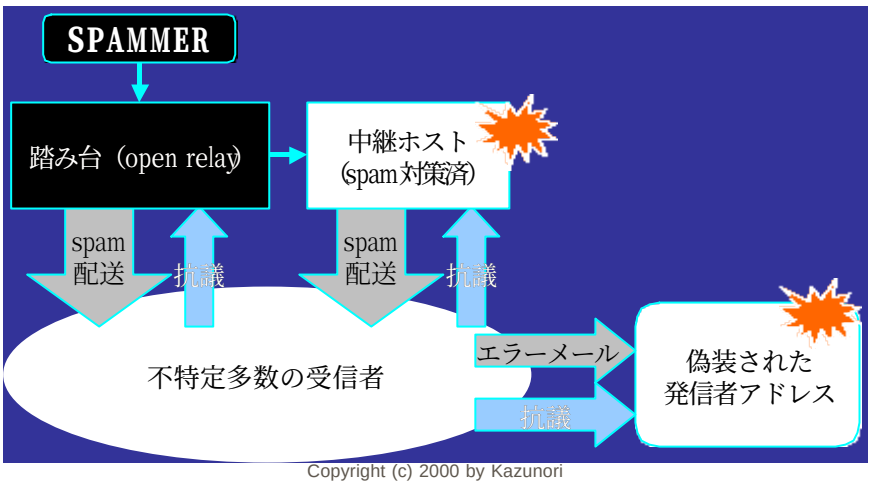
17

配送トラフィック

- 回線帯域を示さないベンチマークは無意味
  - 「n万通しか配送できない」？
    - 多くは対外回線の帯域がボトルネック
    - 例えばsendmailは1.5Mbpsの回線を埋められる
  - 機能まで考慮しない比較は無意味
    - 総合性能を評価する場合そろえるべき条件
      - 実現している機能（binary-codeはMIME-encodeとか）
      - 計算機リソース・OS
      - 使用回線帯域

18

SPAM中継の被害の構図



19

SPAM対策（1）

- RBL（Realtime Blackhole List）
  - SPAMの発信源を登録する閻魔帳
    - DNSと同じ枠組みで作られている
      - MTAがメール送信元のIPアドレスを照会
    - 類似のものが何種類もある
      - MAPS RBL、MAPS RSS、MAPS DUL、ORBS、IMRSS等
    - 自分のサーバが登録された場合
      - メールを受け取らない所が出てくる
    - RBLのサーバが落ちると「**全てのIPアドレスはクロ**」
      - 全部受け取り拒否して全然メールが来なくなる

20

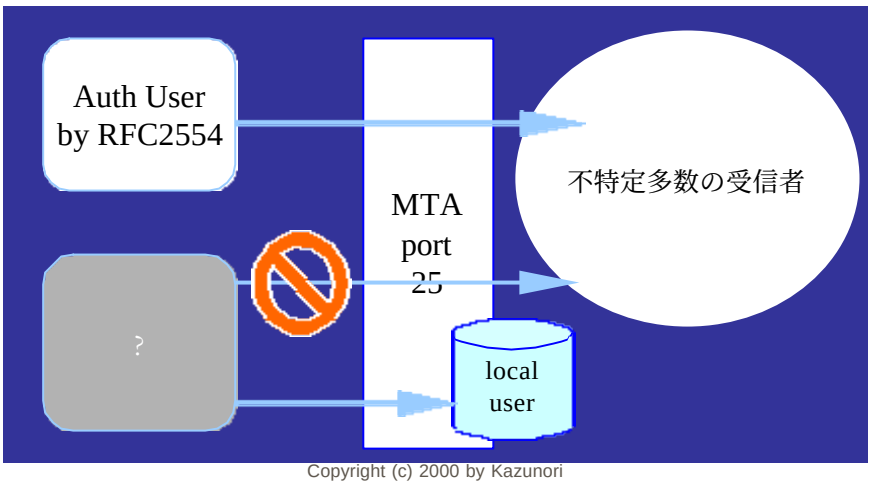
SPAM対策 (2)

- SPAMLIST
  - 発信元についていずれかを指定して排除
    - メールアドレス（envelope from)
    - ドメイン
    - IPアドレス
- POP before SMTP
  - ISPで取り入れられている手法
    - POPアクセスするとSMTP接続を許可する
    - 例えばqpopperにパッチを当てて実現する

SMTP Authentication（RFC2554)

- SASL（RFC2222）を利用したRelay認証
  - sendmail-8.11では
    - 例えばcyrus SASLライブラリを利用
    - SASLのデフォールトは/etc/passwdを利用した認証
    - 認証を通るとそのサーバ経由のRelay配送を許可
  - POP before SMTPの置き換え
    - MUAの対応が条件ではある

SMTP Authentication（RFC2554）



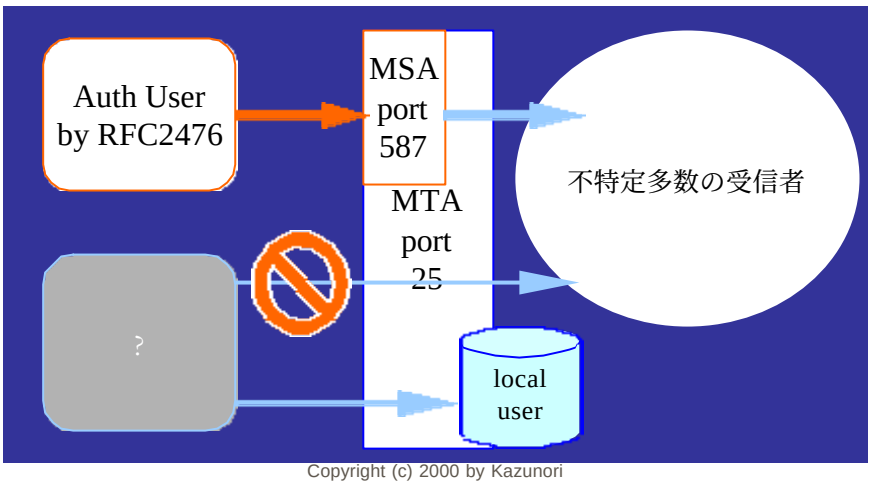
23

Message Submission（RFC2476）

- MSA（Message Submission Agent）
  - メールを「出す」新たな枠組み
    - Relayと区別することでSPAMを防止
      - SMTPではlocal宛のメールしか受けない
      - Submissionによる発信は自分のサイトからの接続だけを許可してさらに認証をかける
    - port 587
      - sendmail-8.10はMSAになれる

24

Message Submission (RFC2476)



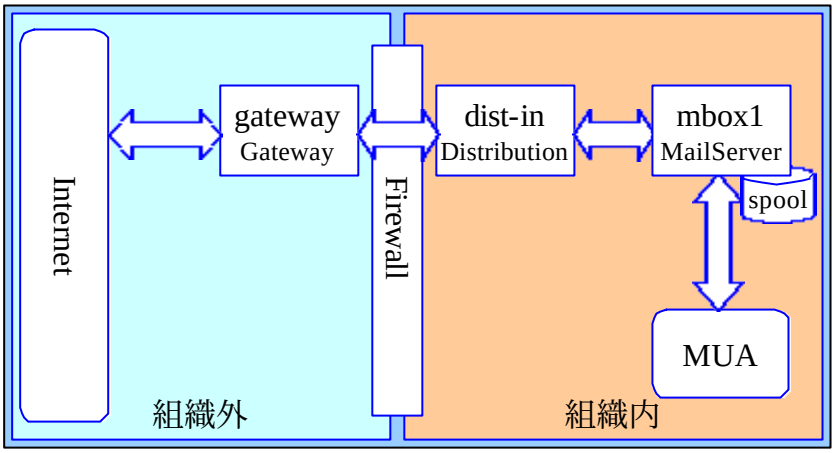
25

配送設定の基本要素

- MX配送かstatic（静的）配送か?
  - 対外配送はMX配送
  - 組織内部の配送はどちらか選択
    - 組織内部で独自のDNSの定義をしている場合
    - 集中サーバならstaticでもいける
  - resolv.confで参照するDNSサーバを指定

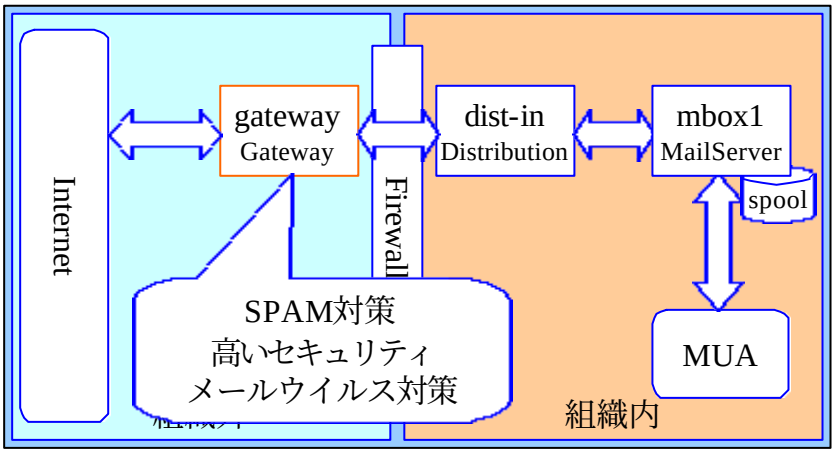
26

メール配送モデル



27

メール配送モデル:Gateway



28

Gateway

- 特別に必要な機能
  - 内側サーバへのstatic配送
    - FEATURE(`mailertable‘)
  - スパム不正中継の防止対策
    - FEATURE(`access_db’)
    - FEATURE(`blacklist_recipients')
    - FEATURE(`dnsbl')

29

Gateway: `mailertable`

- static配送ルールを書く
- 設定ファイル名は/etc/mail/mailertable

/etc/mail/mailertable

```
.example.gr.jp     smtp:[dist-in.example.gr.jp]
.example.ad.jp     smtp:[non-mx.example.ad.jp]
.example.com       esmtp:mx.example.co.jp
```

```
# makemap hash /etc/mail/mailertable < /etc/mail/mailertable
```

このコマンドでmailertable.dbが生成され本設定が完了

30

Gateway: access_db

- 拡張されたspamlistの設定
- 設定ファイル名は/etc/mail/access

/etc/mail/access

```
spammers.net                    REJECT
spammer@ube.com                 ERROR:5.7.1:551 Relay denied
spam@uce.uce.com                DISCARD
localhost.example.gr.jp         RELAY
localhost                       RELAY
127.0.0.1                       RELAY
```

```
# makemap hash /etc/mail/access < /etc/mail/access
```

このコマンドでaccess.dbが生成され本設定が完了

31

Gateway: blacklist_recipient

- 自ドメインのあるアドレスが狙われた場合の措置手段
- /etc/mail/accessに設定を付加できるようになる

/etc/mail/access

```
bogus_user@                 REJECT
bogus.example.gr.jp         ERROR:550 Bogus host
junk@other.example.gr.jp    ERROR:550 Mailbox unavailable
```

```
# makemap hash /etc/mail/access < /etc/mail/access
```

このコマンドでaccess.dbが生成され本設定が完了

32

Gateway: dnsbl

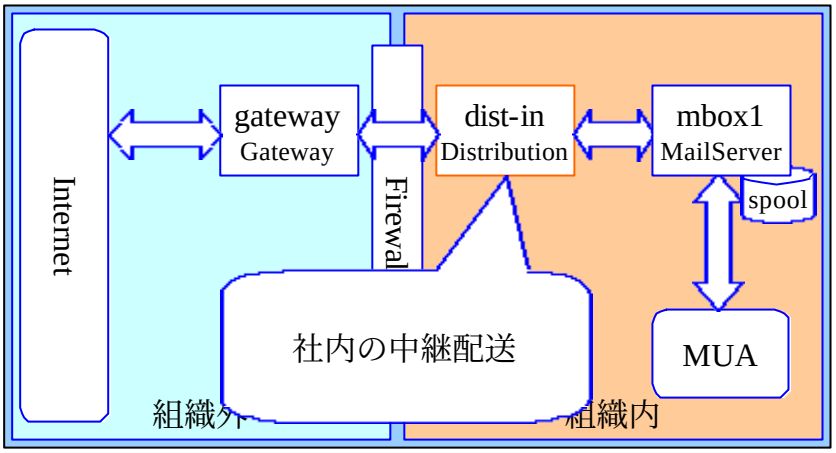
- いわゆるRBLの設定
- RBLはDNSの仕組みを利用している
- デフォルトはMAPS RBLを参照するが他のRBLも利用可能

Gateway: config.mcファイル

```
divert(0)dnl
VERSIONID(`$Id: generic-linux.mc,v 8.1 1999/09/24 22:48:05 ando Exp $')
OSTYPE(linux)dnl
DOMAIN(generic)dnl
MAILER(local)dnl
MAILER(smtp)dnl
FEATURE(`mailertable')dnl
FEATURE(`access_db')dnl
FEATURE(`blacklist_recipients')dnl
FEATURE(`dnsbl')dnl
```

```
cd ${SENDMAIL_SRC}/cf/cf
make config.cf
```

メール配送モデル: 社内中継サーバ



社内中継サーバ

- 特別に必要な機能
  - 社内メールサーバへのstatic配送
    - FEATURE(`mailertable')の利用
  - 自ドメイン以外へのメールをGatewayへ
    - クラス SMART_HOST にGatewayを設定

社内中継サーバ: mailertable

- 社内でのstatic配送ルールを書く
- 設定ファイル名は/etc/mail/mailertable

/etc/mail/mailertable

```
sub1.example.gr.jp      smtp:[mbox1.example.gr.jp]
sub2.example.gr.jp      smtp:[mbox2.example.ad.jp]
sub1.example.ad.jp      smtp:[mbox3.example.co.jp]
```

```
# makemap hash /etc/mail/mailertable < /etc/mail/mailertable
```

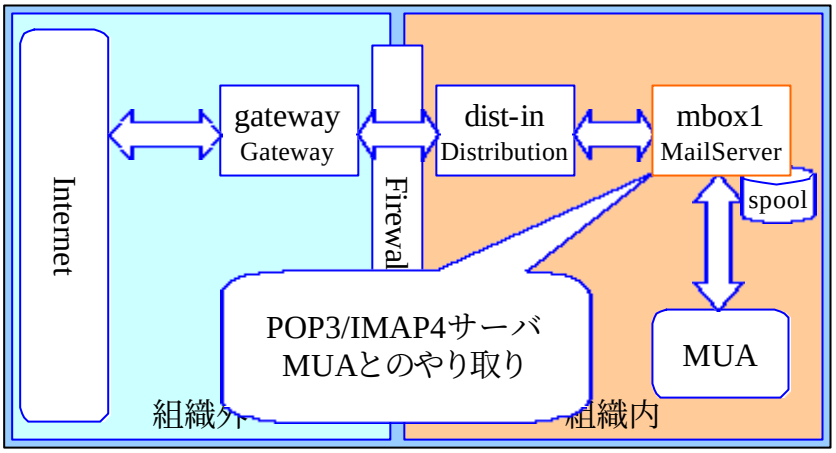
このコマンドでmailertable.dbが生成され本設定が完了

社内中継サーバ: config.mcファイル

```
divert(0)dnl
VERSIONID(`$Id: generic-linux.mc,v 8.1 1999/09/24 22:48:05 ando Exp $')
OSTYPE(linux)dnl
DOMAIN(generic)dnl
MAILER(local)dnl
MAILER(smtp)dnl
FEATURE(`mailertable')dnl
define(`SMART_HOST',`gateway.example.gr.jp')dnl
```

```
cd ${SENDMAIL_SRC}/cf/cf
make config.cf
```

メール配送モデル: 社内メールサーバ



39

社内メールサーバ

- 特別に必要な機能
  - 社内中継サーバへのstatic配送
    - クラスSMART_HOST の利用
  - 知らないドメインでもそのまま中継に渡す
    - 自分のドメインを付加しない
  - ドメイン名のマスカレード
    - マシン名だけ含まないアドレスでメールを出したい

40

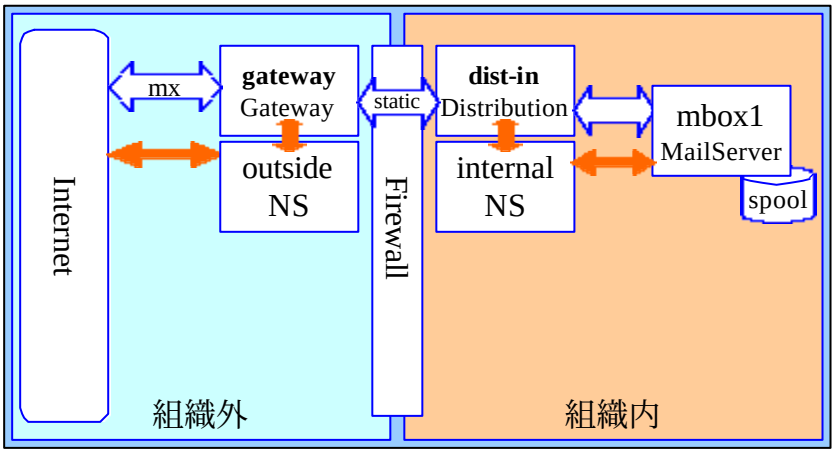
社内メールサーバ: config.mcファイル

```
divert(0)dnl
VERSIONID(`$Id: generic-linux.mc,v 8.1 1999/09/24 22:48:05 ando Exp $')
OSTYPE(linux)dnl
DOMAIN(generic)dnl
MAILER(local)dnl
MAILER(smtp)dnl
Dmexample.gr.jp
FEATURE(`nocanonify')dnl
define(`SMART_HOST',`dist-in.example.gr.jp')dnl
MASQUERADE_AS(`example.gr.jp')dnl
MASQUERADE_DOMAIN(`myhost.example.gr.jp')dnl
FEATURE(`limited_masquerade')dnl
FEATURE(`masquerade_envelope')
```

```
cd ${SENDMAIL_SRC}/cf/cf
make config.cf
```

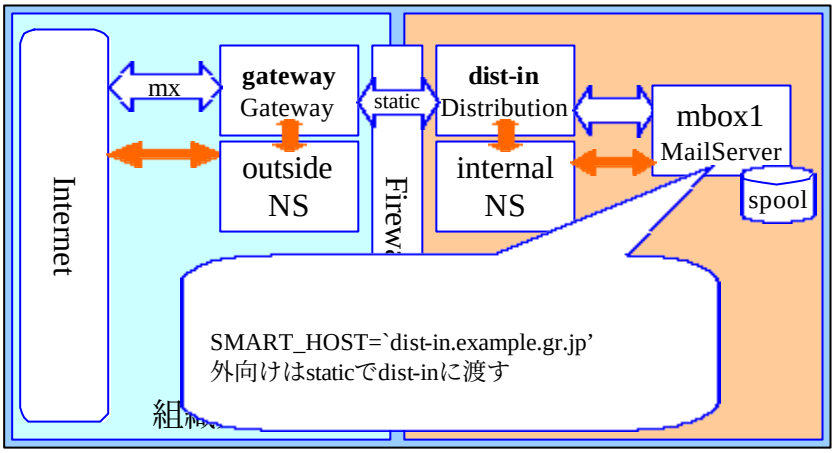

41

メール配送モデル（社内DNS利用）



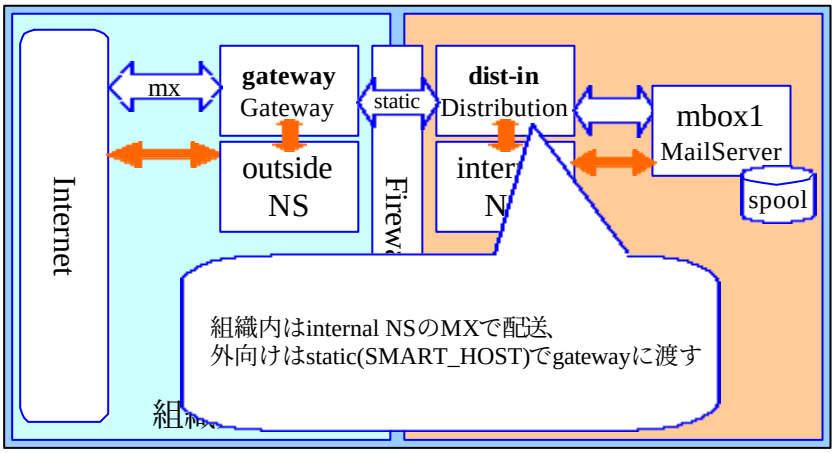
42

内部MSの設定



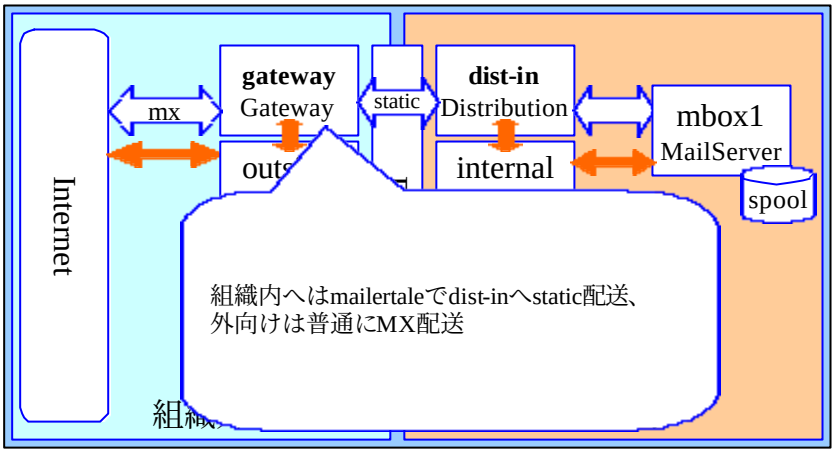
43

内側distributionサーバの設定



44

外側サーバの設定



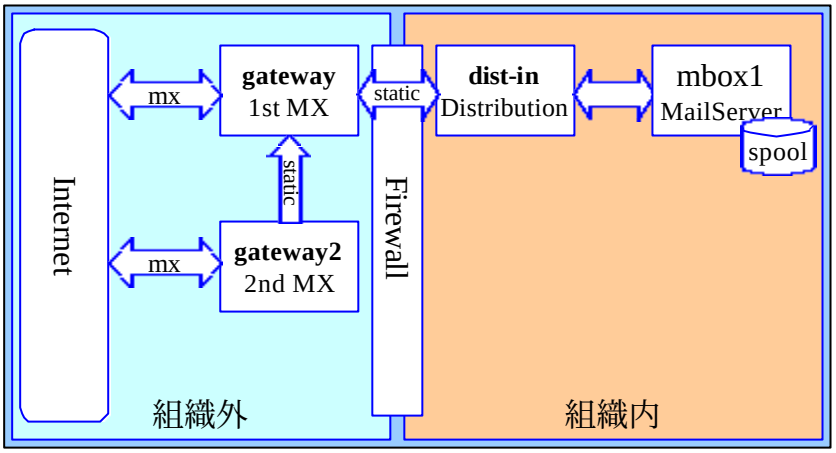
45

対外受信ホストの多重化

- MXを複数にする理由
  - メールが集中して負荷が高い場合
    - 一時的にため込む
    - 可能なら2nd MXは1st MXとは独立に配信
  - メンテナンス用
    - 片方が停止しても受け取りに支障を出さない

46

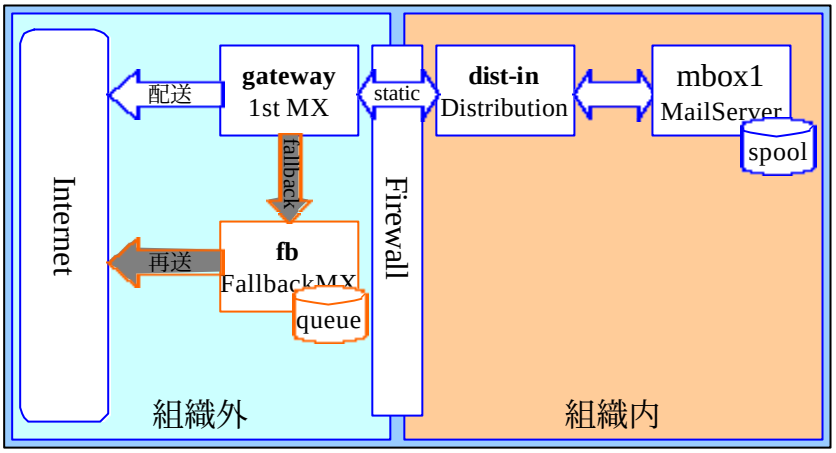
2nd MXのあるメール配送モデル



FallbackMX

- 再送専用ホスト
  - 再送queueを特定のホストに集める
    - DNSが引けなかった場合
    - 全MXに対してメールが送れなかった場合
  - ネットワーク的なトラブルがすぐわかる
  - 再送を試みる期間の調整
  - `define(`confFALLBACK_MX',`fb.example.gr.jp')dnl`

FallbackMXのある配送モデル



LDAPの利用

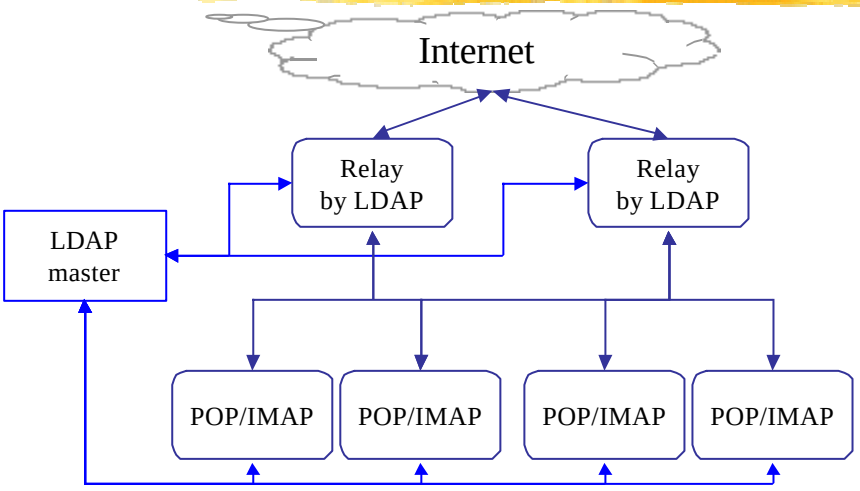
- LDAP（Lightweight Directory Access Protocol）
  - ローカルの配送先を記録してあるディレクトリへのアクセスに利用
  - できればshadowサーバも用意して多重化
  - Netscape製品のディレクトリサーバでの配送先を示すエントリ名はIETFのドラフトに則ったものではないため、他の製品で利用する際にはエントリ名の変更が必要かもしれない

LDAPを使用するメリット

- ユーザごとに使用するmboxを指定できる
  - 全社で導入すると
    - 部署が変わってもメールアドレスの変更が不要
    - 同じドメインのmboxサーバを複数に増やして運用することが可能
    - つまりは大規模化が可能

51

LDAPを用いた構築例



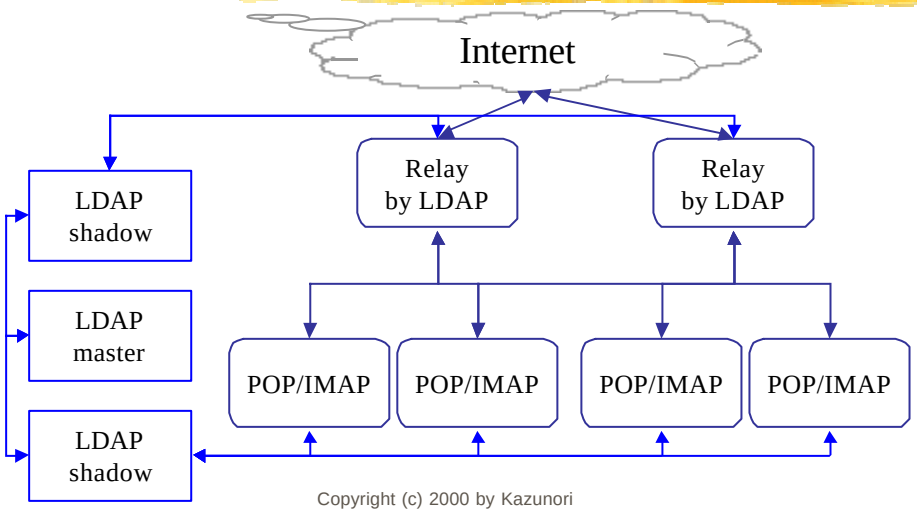
52

Shadow

- 複製ディレクトリサーバ
  - DAP（X.500）を用いた複製
- DB検索の負荷を分散
  - さらなる大規模化には必須の技術
  - 信頼性を求めるなら商用製品か?

53

LDAP（shadow）を用いた構築例



54

SMTP/TLSの利用

- TLS（Transport Layer Security）
  - 乱暴に言うと、SSL接続への移行を視野に入れた接続の枠組みのこと
  - サーバ間SMTPを経路暗号化
  - sendmailでもこのTLSの枠組みを用いてSMTPの接続をSSLへ移行することが可能になっている
    - OpenSSLの利用が前提
    - 商用版では使えるようになっている製品もある

鍵の準備

- TLS（SSL）には認証用の鍵が必要
  - CA（認証局）から購入
    - 他社からの接続でもTLS利用が可能に
  - 自前で準備
    - 鍵の配布範囲にTLSの利用が限定される

MTAの種類（1）

- Sendmail（商用版：Sendmail SWITCH）
  - さまざまな意味で最も手堅い選択
  - 地道にパフォーマンスを改善
    - Multiple-queue-directory等
  - 大規模MLの配送ではsmtpfeedを併用
    - 外部メーラへの受け渡しでLMTPを話せる
  - CFのupdateは止まってしまいました
    - m4で頑張る
    - GUIで設定ができる商用版

57

MTAの種類（2）

- qmail
  - 単機能の小さいプログラムの集合体
    - 比較的パフォーマンスは良い
    - 個々の機能を見ると必ずしもベストを尽くしていない
      - 同一MX宛てのメールのまとめ送りがない
      - ひらたく言えば配送戦略は「力任せ」
  - トラブルが発生しても原因がさっぱりわからない
    - ログ情報の不足、エラーメッセージの不備

58

MTAの種類（3）

- Postfix
  - Sendmailの置き換えを目指したMTA
    - 設定が比較的簡単
    - UUCPメーラーまで実装されている
    - インターネット標準への準拠もまじめにやっている
    - 移行も比較的容易
  - もともとはIBM社内グループの作品

59

MTAの種類（4）

- その他商用製品
  - Sendmail Server
  - Netscape Messaging Server/SIMS
  - InterMail
    - オールインワンサーバ（MTA＋POP/IMAPサーバ）
    - ユーザ数ベースの課金形態
      - データベースを併用しているから？
    - ユーザ数の上限を拡大しているのが売りだがそんなにパフォーマンスが出ないものもある

60

MTA選び（1）

- アカウント管理
  - OSに依存
    - 規模に限界がある
  - LDAPを利用
    - サーバ分散が可能
- 仲介サーバはpopかimapか？
  - popはメールをクライアントが保持する
    - リスク分散と見ることができる
  - imapは便利だがサーバがメールを保持
    - パフォーマンスもリスクもサーバに依存

MTA選び（2）

- サーバの実際の収容数は...
  - 定期メールチェックのアクセス頻度に依存
    - ネットワーク接続の同時接続数上限はOS依存
      - メールチェックはネットワークとファイルI/Oのリソースを消費
    - 100Mbpsのリソースも１００００人で使えば１０kbps
      - リソースの上限近くでは急激にパフォーマンスが悪化する
    - セールストークにありがちなごまかし
      - × 少数ユーザでテストして大人数の場合を推測する
      - × ストライピング（RAID0)を利用したストレージの利用
        - 製品の性能ではなくストレージの性能が高い

MTA選び（3）

- セキュリティホール
  - そもそも「あると仮定しておくべきもの」である
    - 一般にシェアの大きい方が発見が早い
    - ＯＳ自体のセキュリティホールの方が圧倒的に多い
      - 商用製品なら安心かというと必ずしもそうではない
      - MTA自体が完璧なら安心というものでもない
    - セキュリティが心配ならそういう情報を得る努力を
      - 実際、セキュリティホールは呆れるほど多い
      - 例えば、http://www.securityfocus.com/

エラーメールの基礎

- エラーメール配信の枠組み
  - DSN（Delivery Status Notification）
    - Envelope From は null address（<>）
      - エラーメールに返信アドレスはない
- トラブルの種類を判定する手段
  - RFC1893（Status Code）
    - Status: 5.1.1
      - 5.X.X　Permanent Failure
      - X.1.1　Bad destination mailbox address

エラーハンドリング問題

- 配送エラーコード（status code）の実装
  - 実際にRFCを守っているか？
    - sendmailやPostfix、SIMS等守っているものも多い
    - その他の対応はいまいち
      - MTAの数だけエラーハンドリングのプログラムが必要
      - 標準を守ろうとしないMTAは迷惑なんだけど...
    - 大量にメールを配るところでは頭痛のタネ

メール経由のウイルス

- 添付ファイルが感染源であることが多い
  - マクロウイルス（Excel、Word、PowerPoint）
    - 中に忍ばせてあるOfficeオブジェクトが曲者
    - 代表は勝手にウイルスメールをばら撒くI Love You
    - 大規模MLでは添付ファイルは許可しない
  - 実行形式ファイル
    - 不用意に実行してはいけない
    - 代表はメール発信するとそのあて先にもう１通ウイルスメールを送付するHappy99とかTROJ_NAVIDAD.A

チェインメール

- 善意の協力依頼を装う（あるいは本物）
  - 「このメールを転載して下さい」が典型
    - 無制限の転載を意図している場合には無視
    - 本来の目的を達成するには、期間や範囲を限定して一定数しか転載されない工夫を
- 不幸・幸福のメール
  - 「このメールを５人に転送しないと．．．」
    - 初心者の多い環境で流行りやすい

メール爆撃（Bombing）

- ２種類ある
  - 巨大なサイズのメールを送付
  - 膨大な数のメールを送付
    - どちらもspoolを膨らませる結果になる
    - loopと見分けがつきにくい場合がある
- サイズ制限、通数制限等の防御
  - メーリングリストではさらに深刻な問題に
  - O MaxMessageSize=500000

知っておくべきメールアドレス

- MAILBOX NAMES FOR COMMON SERVICES, ROLES AND FUNCTIONS（RFC2142)で挙げられているもの
- 例えば、
  - abuse@example.gr.jp
    - いざという場合の問い合わせ先
  - postmaster@example.gr.jp
    - メール配送についての問い合わせ先
  - hostmaster@example.gr.jp
    - DNSについての問い合わせ先

MLの周辺アドレス

- 周辺アドレスの例
  - owner-hoe@example.gr.jp
    - sendmail的にちょっと考慮されたMLの発信者アドレス
  - hoe-admin@example.gr.jp
    - 管理者のaliasとして使われることがある
  - hoe-request@example.gr.jp
    - RFC2142的管理者アドレス
  - hoe-errorsto@example.gr.jp
    - エラーメールの専用受信アドレスを用意している場合

アドレス詐称・隠蔽問題

- bombing等では発信者アドレスが偽装される
  - SPAM発信者を偽装して発信者をbombing
- MLに他人のアドレスを登録する
  - 自動登録でConfirmなしだとアウト
- 無料メールアドレスの転送機能
  - 誰に届くかわからないという意味で曲者

71

運用上の留意点

- SPAM対策
  - 「来たときの対策」から「出させない対策」へ
    - SMTP Authentication (RFC2554)
    - Message Submission (RFC2476)
    - SMTP over TLS (RFC2487)
  - メーリングリストではアドレス一覧を出さないこと
    - 例えばPPMLは一般参加者のwhoコマンドに対して GECOSの一覧を出す

72

最近の傾向

- 大規模化に伴う相対的な管理レベルの低下
  - ISP等では大規模化する一方
    - ユーザ管理の省力化を目的にLDAP/ディレクトリサーバを利用するケースも珍しくなくなってきている
  - 携帯電話メールのトラフィックの増加
    - 容量は小さいが通数はものすごい
  - MIME-multipartによる添付文書
    - 容量が大きいのでspool容量の再考が必要なケースも出てきている

懸案事項 (1)

- メールが媒介するウイルスの多様化
  - 次から次へ新種
  - ちょっと昔のやつも根強く繁殖
  - ウイルス対策ソフトが売れる理由
    - 大量繁殖を防ぐにはMTAかMLドライバのレベルで添付ファイルのチェックを
- MailとWWW、死守すべきはどっち？

懸案事項 (2)

- 大規模サイトのサーバの受信能力不足
  - 再送が再送を呼んで昼間は常に輻輳しているとしか思えないサイトもある
  - ある程度のメール流量のあるメールゲートウェイやFallbackMXサーバの残存queueの観察でいらないことがいろいろわかってしまう
    - いやでもわかってしまう

75