

メールサーバ構築と周辺技術動向



安藤一憲
ando@wni.co.jp

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
- ◆ メールの基礎知識
 - 普段目にするメールについての解説
- ◆ メール配送のモデル
 - MX配送、static配送の使い分け
 - 設定のまとめ

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

3

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

4

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
 - sendmailではオプションになった
- ◆ DNSのMXには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が知っているが良い

Copyright (c) 2001 by Kazunori ANDO
IW2001

5

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い

と書いてあったりする

Copyright (c) 2001 by Kazunori ANDO
IW2001

6

メール本体とエンベロープ

Mail From: ando@wni.co.jp
Rcpt To: motonori@media.kyoto-u.ac.jp

エンベロープ
SMTP的配送情報

From: Kazunori ANDO <ando@wni.co.jp>
To: Motonori NAKAMURA <motonori@media.kyoto-u.ac.jp>
Subject: Re: smtpfeed-1.16
Message-Id: <ANDO.SB10224@axis.wni.co.jp>

(空行のあとが本文)

メール本体
ヘッダは基本的に配送とは関係ない

Copyright (c) 2001 by Kazunori ANDO
IW2001

7

メール本体とエンベロープ(2)

Mail From: motonori@media.kyoto-u.ac.jp
Rcpt To: ando@wni.co.jp

配送経路情報が記録される

Received: from query.media.kyoto-u.ac.jp
by wni.co.jp with ESMTTP
for <ando@wni.co.jp>; 15 Dec 1999 14:00:01 +0900
Return-Path: motonori@media.kyoto-u.ac.jp
From: Motonori NAKAMURA <motonori@media.kyoto-u.ac.jp>
To: Kazunori ANDO <ando@wni.co.jp>
Subject: Re: smtpfeed-1.07
Message-Id: <ANDO.SB10224@axis.wni.co.jp>

(空行のあとが本文)

Return-Path: にSMTPのMail From:が
保存される(設定による)

Copyright (c) 2001 by Kazunori ANDO
IW2001

8

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

9

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

10

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(メールを再送信する場合の)

- 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: 再送信日時

Copyright (c) 2001 by Kazunori ANDO
IW2001

11

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等

Copyright (c) 2001 by Kazunori ANDO
IW2001

12

文字の話

- ◆ 機種依存文字を使ってはいけない
 - ①②③④⑤⑥⑦⑧⑨⑩
 - I II III IV V VI VII VIII IX X
 - トウゼンハンカクカクナモダメ
- ◆ 漢字コードはISO-2022-JPを使用する
 - SJISだめ、EUCだめ、UNICODEだめ

Copyright (c) 2001 by Kazunori ANDO
IW2001

13

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20へ

Copyright (c) 2001 by Kazunori ANDO
IW2001

14

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
```

additional information

Copyright (c) 2001 by Kazunori ANDO
IW2001

15

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

16

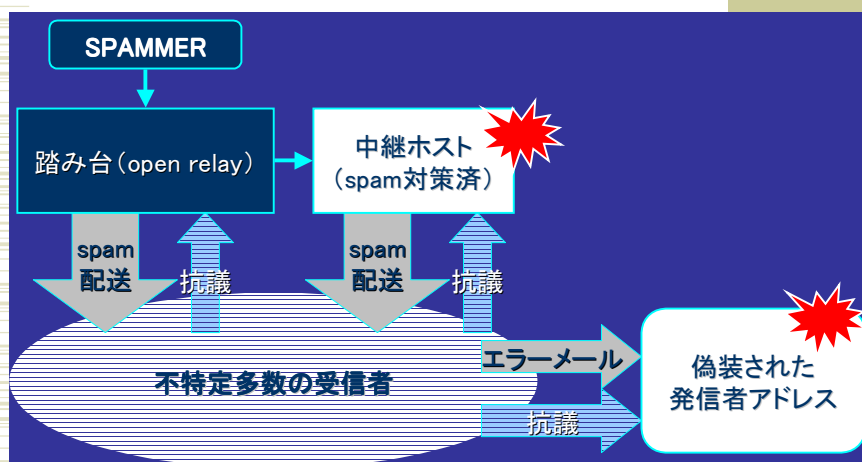
配送トラフィック

- ◆ 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

Copyright (c) 2001 by Kazunori ANDO
IW2001

17

SPAM中継の被害の構図



Copyright (c) 2001 by Kazunori ANDO
IW2001

18

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、RSS、DUL、RBL+、ORDB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
 - MTAによってはRBLが落ちると「全てのIPアドレスはクロ」判定
 - ◆ 全部受け取り拒否して全然メールが来なくなる

Copyright (c) 2001 by Kazunori ANDO
IW2001

19

SPAM対策(2)

- ◆ SPAMLIST(access_dbに進化)
 - 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

Copyright (c) 2001 by Kazunori ANDO
IW2001

20

SMTP Authentication (RFC2554)

◆ SASL (RFC2222) を利用した Relay 認証

■ sendmail-8.12 では

● 必要な作業

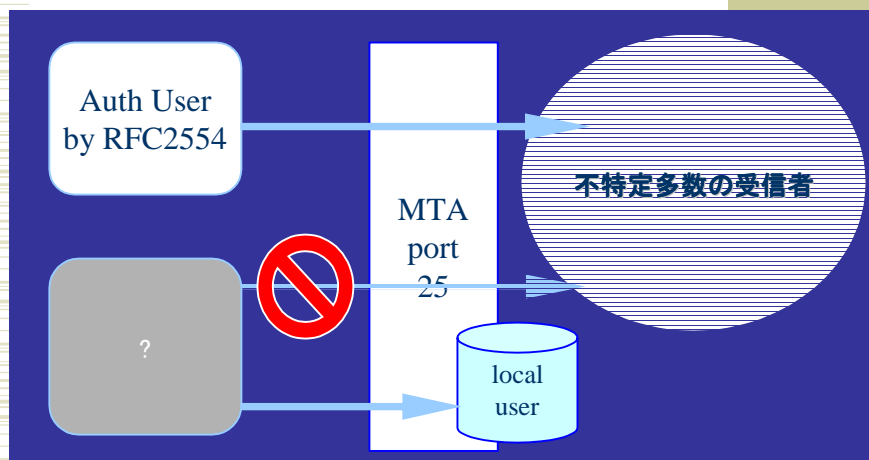
- ◆ cyrus SASL ライブラリをインストール
- ◆ SASL を利用するように sendmail をコンパイル
- ◆ /usr/local/lib/sasl/Sendmail.conf の準備 (必要なら)
- ◆ /etc/sasldb.db の準備 (saslpasswd コマンドでユーザ登録)
- ◆ sendmail.cf の設定追加

● 認証を通るとそのサーバ経由の Relay 配送を許可

Copyright (c) 2001 by Kazunori ANDO
IW2001

21

SMTP Authentication (RFC2554)



Copyright (c) 2001 by Kazunori ANDO
IW2001

22

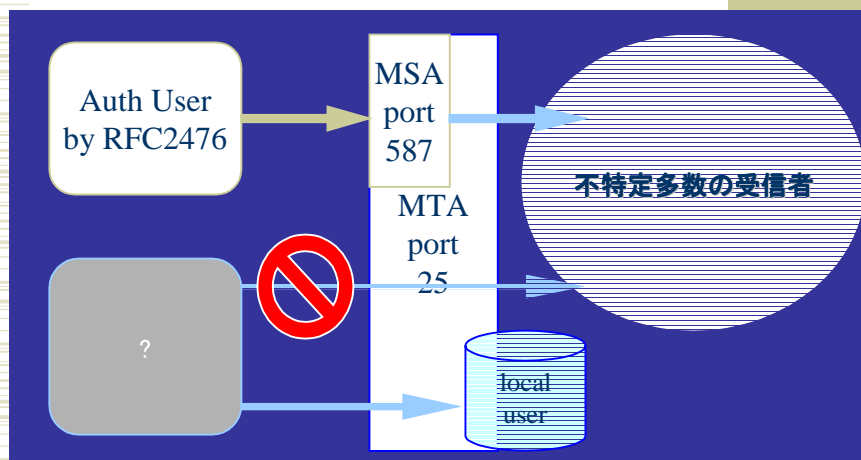
Message Submission (RFC2476)

- ◆ 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不正中継を防止
 - ◆ 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-8.11以降はdefaultでMSAになる

Copyright (c) 2001 by Kazunori ANDO
IW2001

23

Message Submission (RFC2476)



Copyright (c) 2001 by Kazunori ANDO
IW2001

24

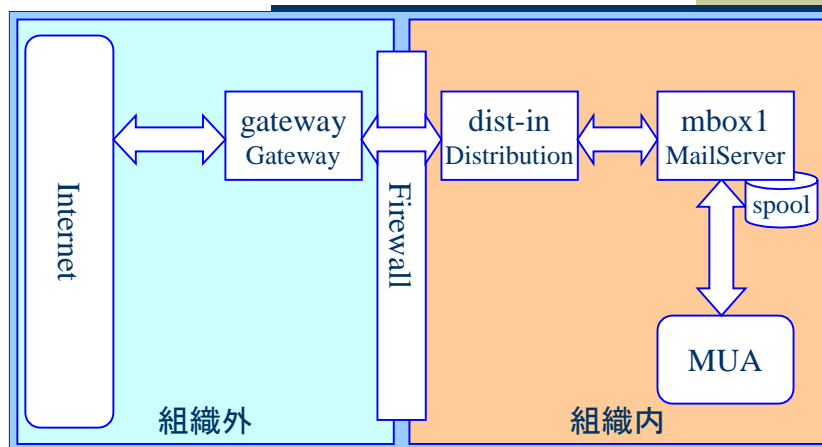
配送設定の基本要素

- ◆ 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(mailertable)でもいける
 - resolv.confで参照するDNSサーバを指定

Copyright (c) 2001 by Kazunori ANDO
IW2001

25

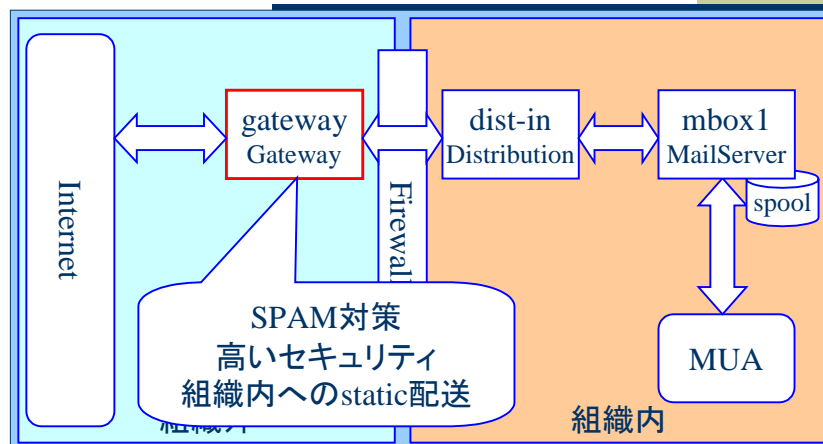
メール配送モデル



Copyright (c) 2001 by Kazunori ANDO
IW2001

26

メール配送モデル: Gateway



Copyright (c) 2001 by Kazunori ANDO
IW2001

27

Gateway

◆ 特別に必要な機能

- 内側サーバへのstatic配送
 - FEATURE(`mailtable`)
- スпам不正中継の防止対策
 - FEATURE(`access_db`)
 - FEATURE(`blacklist_recipients`)
 - FEATURE(`dnsbl`)
 - FEATURE(`enhdnsbl`, `dnsbl.example.com`, `t`, `127.0.0.2`, `RBL BLOCK`)

Copyright (c) 2001 by Kazunori ANDO
IW2001

28

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

29

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
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

Copyright (c) 2001 by Kazunori ANDO
IW2001

30

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

31

Gateway: dnsbl , enhdnsbl

- いわゆるRBLの設定と、その拡張版
- RBLはDNSの仕組みを利用している
- デフォルトはMAPS RBLを参照するが変更も可能
 - <http://www.mail-abuse.org/>
- RBLへのqueryが失敗した場合にはtmpfailになる
 - 再送処理がおこなわれる

```
FEATURE(`dnsbl')
FEATURE(`enhdnsbl',`dnsbl.example.com',`,`t',`127.0.0.2.',`RBL BLOCK')
```

Copyright (c) 2001 by Kazunori ANDO
IW2001

32

Gateway: config.mcファイル

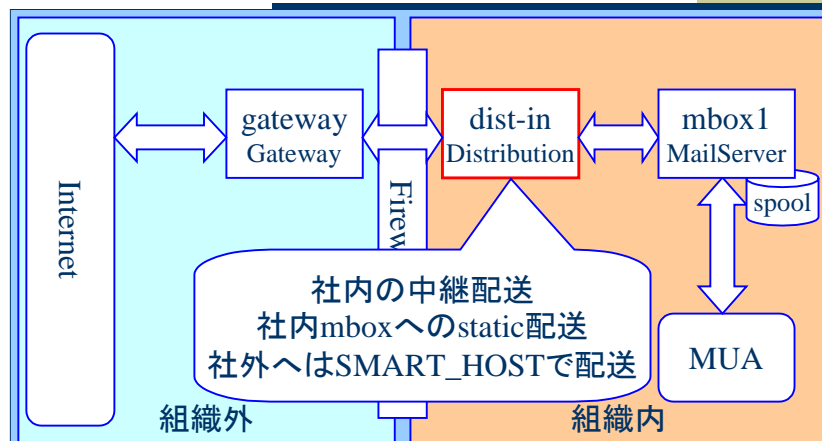
```
divert(0)dnl
VERSIONID(`$Id: config.mc,v 1.1 2001/12/4 13:48:05 ando Exp $')
OSTYPE(bsd4.4)dnl
DOMAIN(generic)dnl
FEATURE(`nocanonify')dnl
FEATURE(`mailetable')dnl
FEATURE(`access_db')dnl
FEATURE(`blacklist_recipients')dnl
FEATURE(`dnsbl')dnl
MAILER(local)dnl
MAILER(smtp)dnl
define(`confDOMAIN_NAME',`$w.$m')dnl

cd ${SENDMAIL_SRC}/cf/cf
make config.cf
make install-cf CF=config
```

Copyright (c) 2001 by Kazunori ANDO
IW2001

33

メール配送モデル: 社内中継サーバ



Copyright (c) 2001 by Kazunori ANDO
IW2001

34

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(`mailtable`)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

Copyright (c) 2001 by Kazunori ANDO
IW2001

35

社内中継サーバ: mailtable

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

/etc/mail/mailtable

```
sub1.example.gr.jp      smtp:[mbox1.example.gr.jp]
sub2.example.gr.jp      smtp:[mbox2.example.ad.jp]
sub1.example.ad.jp      smtp:[192.168.10.25]
```

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

このコマンドでmailtable.dbが生成され本設定が完了

Copyright (c) 2001 by Kazunori ANDO
IW2001

36

社内中継サーバ: config.mcファイル

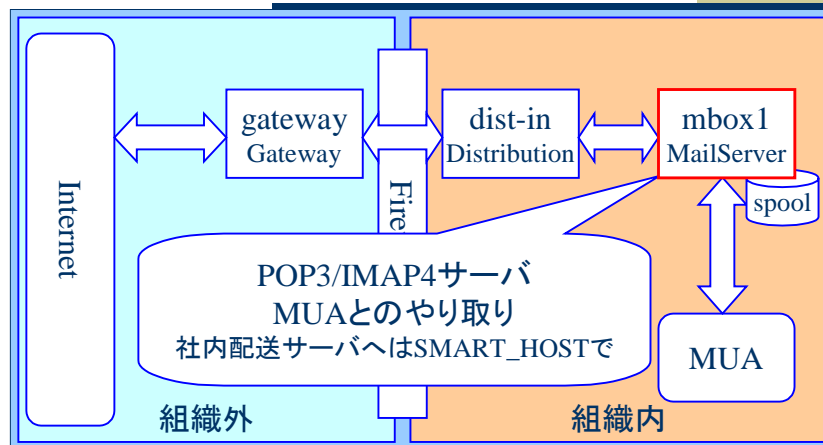
```
divert(0)dnl
VERSIONID(`$Id: config.mc,v 1.1 2000/12/17 22:48:05 ando Exp $')
OSTYPE(linux)dnl
DOMAIN(generic)dnl
FEATURE(`mailtable')dnl
MAILER(local)dnl
MAILER(smtp)dnl
define(`SMART_HOST',`gateway.example.gr.jp')dnl

cd ${SENDMAIL_SRC}/cf/cf
make config.cf
make install-cf CF=config
```

Copyright (c) 2001 by Kazunori ANDO
IW2001

37

メール配送モデル: 社内メールサーバ



Copyright (c) 2001 by Kazunori ANDO
IW2001

38

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

39

社内メールサーバ: config.mcファイル

```
divert(0)dnl
VERSIONID(`$Id: config.mc,v 1.1 2000/12/17 22:48:05 ando Exp $')
OSTYPE(linux)dnl
DOMAIN(generic)dnl
FEATURE(`nocanonicalize')dnl
MASQUERADE_AS(`example.gr.jp')dnl
MASQUERADE_DOMAIN(`myhost.example.gr.jp')dnl
FEATURE(`limited_masquerade')dnl
FEATURE(`masquerade_envelope')
FEATURE(always_add_domain)dnl
MAILER(local)dnl
MAILER(smtp)dnl
Dmexample.gr.jp
define(`SMART_HOST',`dist-in.example.gr.jp')dnl
```

マスカレードするドメインの範囲を指定。

```
MASQUERADE_DOMAIN(`example.gr.jp')dnl
FEATURE(masquerade_entire_domain)dnl
```

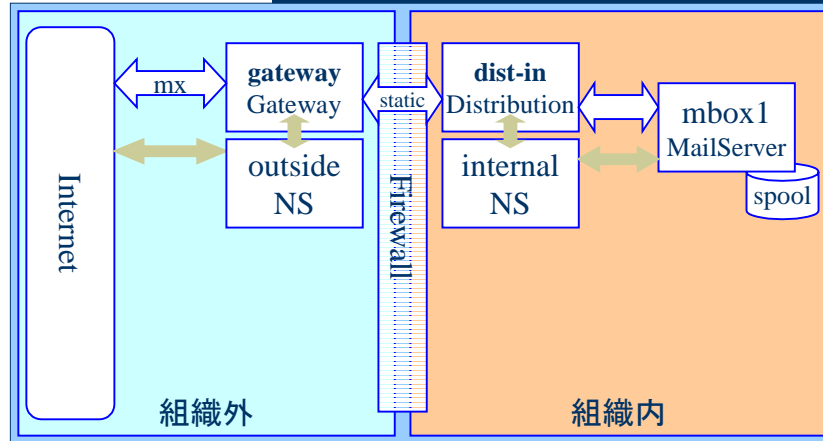
とするとそのドメイン以下全部のマシン名をマスカレード

```
cd ${SENDMAIL_SRC}/cf/cf
make config.cf
make install-cf CF=config
```

Copyright (c) 2001 by Kazunori ANDO
IW2001

40

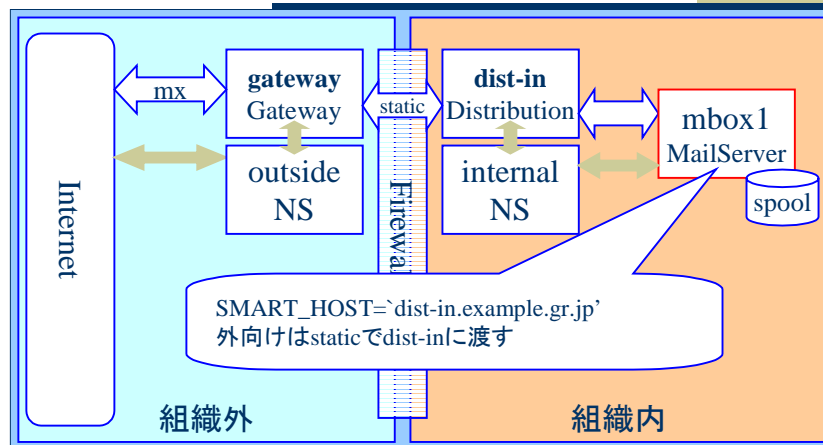
メール配送モデル(社内DNS利用)



Copyright (c) 2001 by Kazunori ANDO
IW2001

41

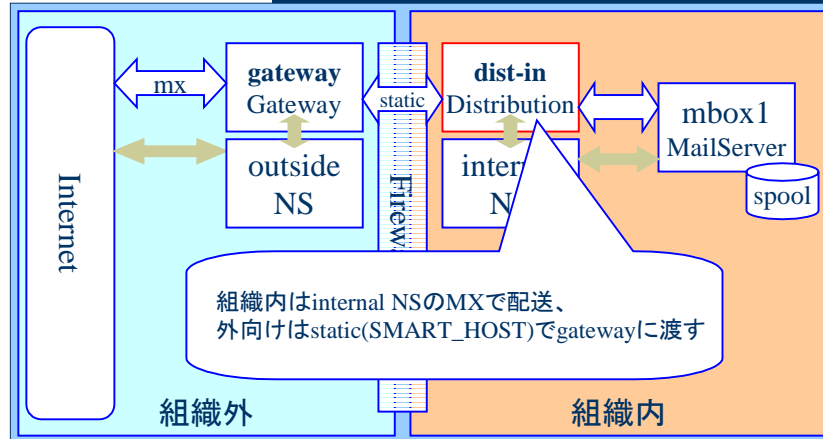
内部MSの設定



Copyright (c) 2001 by Kazunori ANDO
IW2001

42

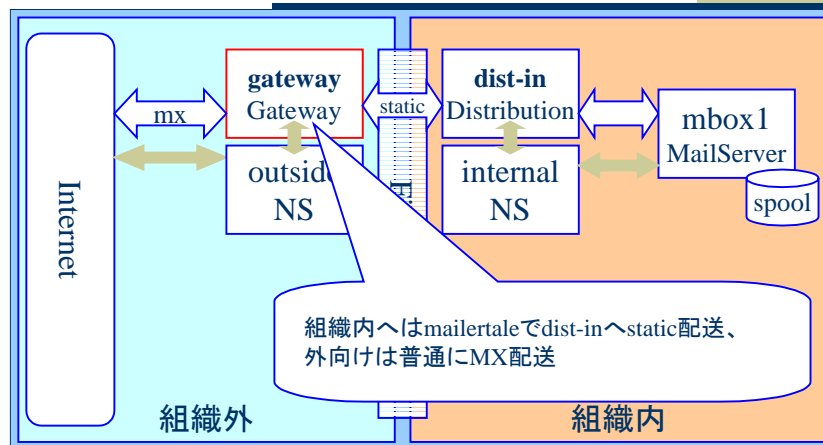
内側distributionサーバの設定



Copyright (c) 2001 by Kazunori ANDO
IW2001

43

外側サーバの設定



Copyright (c) 2001 by Kazunori ANDO
IW2001

44

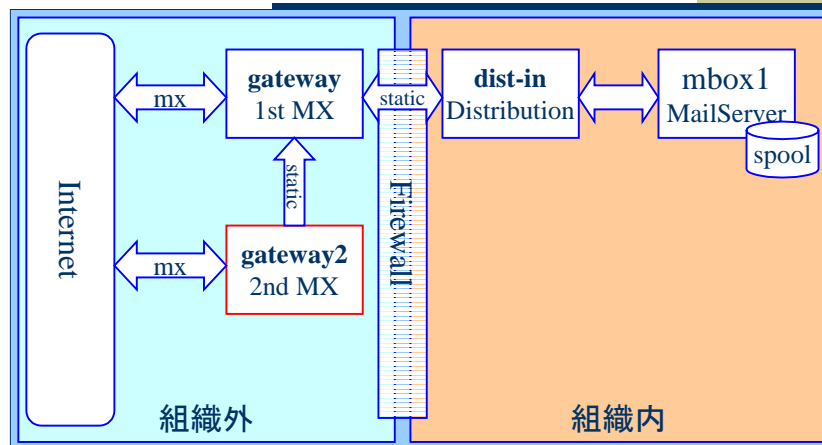
対外受信ホストの多重化

- ◆ 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

Copyright (c) 2001 by Kazunori ANDO
IW2001

45

2nd MXのあるメール配送モデル



Copyright (c) 2001 by Kazunori ANDO
IW2001

46

FallbackMX

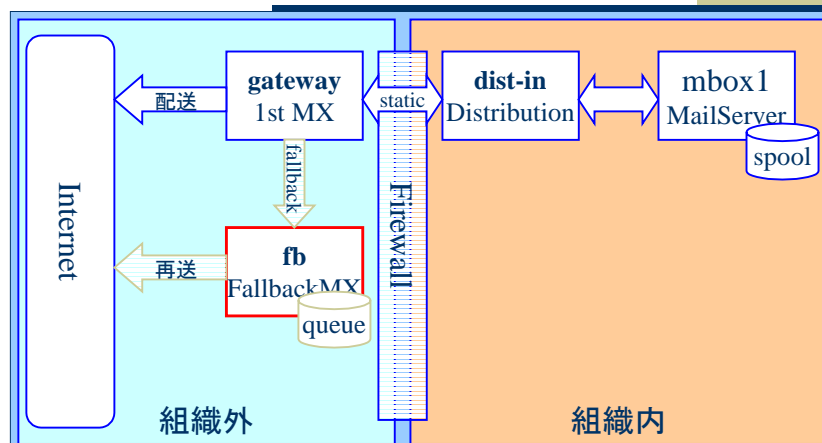
◆ 再送専用ホスト

- 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`

Copyright (c) 2001 by Kazunori ANDO
IW2001

47

FallbackMXのある配送モデル



Copyright (c) 2001 by Kazunori ANDO
IW2001

48

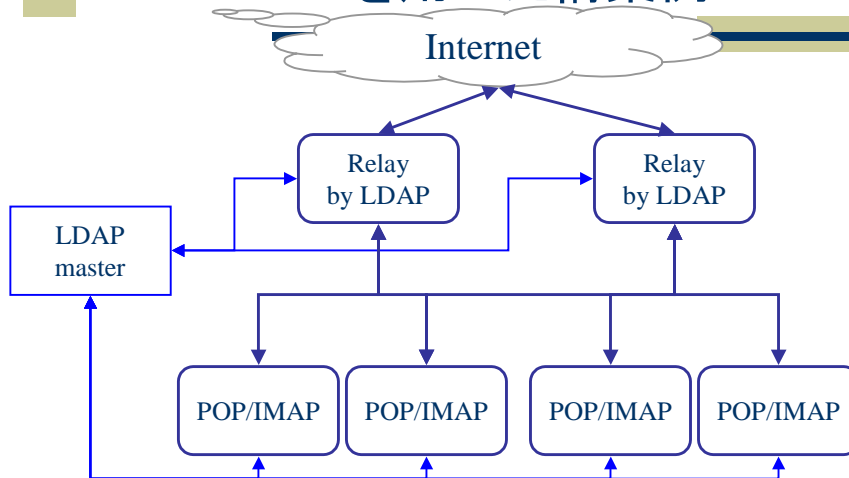
LDAPの利用

- ◆ 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
 - 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

Copyright (c) 2001 by Kazunori ANDO
IW2001

49

LDAPを用いた構築例



Copyright (c) 2001 by Kazunori ANDO
IW2001

50

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
 - 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

Copyright (c) 2001 by Kazunori ANDO
IW2001

51

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

52

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
 - setuid rootの廃止 (8.12.0~)
 - 地道にパフォーマンスを改善
 - 不要なファイルI/Oを減らした
 - 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

Copyright (c) 2001 by Kazunori ANDO
IW2001

53

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無い
 - ◆ 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
 - エラーメッセージの不備、DSNに対応していない
 - ◆ 敢えて言えば作者の姿勢の問題

Copyright (c) 2001 by Kazunori ANDO
IW2001

54

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
- これも機能を分割したプログラムの集合
 - qmailほどばらばらではない

Copyright (c) 2001 by Kazunori ANDO
IW2001

55

MTAの種類(4)

◆ その他商用製品

- Sendmail Server
- Netscape Messaging Server/SIMS
- InterMail/Post.Office
- その他アプライアンスサーバも多数
 - 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。そんなにパフォーマンスが出ないものもある

Copyright (c) 2001 by Kazunori ANDO
IW2001

56

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popよりはサーバのリソースを食う
 - パフォーマンスもリスクもサーバに依存

Copyright (c) 2001 by Kazunori ANDO
IW2001

57

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

58

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点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
 - セキュリティ情報を早期に得る努力を
 - ◆ 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/>

Copyright (c) 2001 by Kazunori ANDO
IW2001

59

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

60

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は大迷惑なんだけど...
 - 大量にメールを配るところでは頭痛のタネ

Copyright (c) 2001 by Kazunori ANDO
IW2001

61

メール経由のウイルス(1)

- ◆ 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
 - 実行形式ファイル
 - 不用意に実行してはいけない
 - Happy99、SirCam、Nimda

Copyright (c) 2001 by Kazunori ANDO
IW2001

62

メール経由のウイルス(2)

- ◆ 自動的に実行されてしまう添付ファイル
 - .wav (nimda) とか.pif(Sircam)とか
- ◆ 感染スピードの爆発的上昇
 - メール、HTTP、JavaScript、ファイル共有など複数経路で感染するワームの登場 (nimda)
 - 市販のウイルス対策プログラムのupdateが追いつかず、防ぎきれない例も多発
 - こまめにWindows updateを！（徹底が難しい）

Copyright (c) 2001 by Kazunori ANDO
IW2001

63

メール経由のウイルス(3)

- ◆ 添付ファイル
 - 元凶はMIME-multipart(便利さの代償?)
 - 入れ子構造でファイルを添付できる
 - ◆ 2段目にファイルを添付した後の1段目にウイルス添付 (nimda)
 - たまにデリミタの使い方を間違っているワームもある (Sircam)
 - 無限段まで入れ子をチェック
 - DoS対象になってしまうかも....

Copyright (c) 2001 by Kazunori ANDO
IW2001

64

ウイルス・ワーム対策体制の例

- ◆ ウイルス対策プログラムを過信しない
 - ウイルスの感染の方が速い場合がある
- ◆ できるだけ速い情報の収集
 - nimdaの第1報はntbugtraq@securityfocus.orgだった
 - ワームによるアクセスを監視(WWWサーバやIDSで)
 - 感染経路情報を示して警戒呼びかけ
 - なにもやらないのと比較して格段の防御になる
- ◆ 大量感染源になり得る部分での対策
 - メーリングリスト・ドライバで添付ファイルの拡張子チェック+削除(メーリングリストでの添付ファイル使用の禁止)
 - Windowsのsecurity-updateに常に注意を払う

Copyright (c) 2001 by Kazunori ANDO
IW2001

65

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」が曲者
 - 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

Copyright (c) 2001 by Kazunori ANDO
IW2001

66

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
 - メールングリストではさらに深刻な問題に
 - O MaxMessageSize=500000

Copyright (c) 2001 by Kazunori ANDO
IW2001

67

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

68

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

69

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

70

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)
- メール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

Copyright (c) 2001 by Kazunori ANDO
IW2001

71

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

72

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?

Copyright (c) 2001 by Kazunori ANDO
IW2001

73

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

Copyright (c) 2001 by Kazunori ANDO
IW2001

74

懸案事項(3)

- ◆ 管理者不足
 - sendmailを設定できる人間が不足?
 - 真っ先にSPAM対策で困るケースが多発
 - 付属のcfでも設定する項目はそれほど多くない
 - READMEが英語なのが障壁?
 - ◆ 日本語訳したcf/READMEくらいならネットワーク上にはある
 - 凝ったことをしようと思ったらコウモリ本もある

Copyright (c) 2001 by Kazunori ANDO
IW2001

75

設定の勘所(1)

- ◆ まずはstatic配送 = mailertable
 - sendmailは配送先の判定で真っ先にmailertableを見る
 - 全丸投げstatic = LOCALRELAY
 - spool(localuser)がない→LOCALRELAY
- ◆ ドラえもんstatic = SMART_HOST
 - localとstaticで配送先がわからなかったら→SMART_HOST
- ◆ SmartHost設定がない = MX配送
 - MXもAも引けない→エラー

Copyright (c) 2001 by Kazunori ANDO
IW2001

76

設定の勘所(2)

- ◆ SPAM対策はaccess_dbに集約
 - 身内のrelay配送の可否
 - SPAMLIST的設定
 - blacklist-recipient設定
- ◆ dnsbl(RBL)ももちろん使える
 - デフォルトはMAPS RBL
 - もちろん他にも指定可能

Copyright (c) 2001 by Kazunori ANDO
IW2001

77

設定の勘所(3)

- ◆ ドメイン名の書き換え
 - MASQUERADE_ASで書き換え後のドメイン指定
- ◆ 範囲指定
 - FEATURE(`limited_masquerade`)だと
 - MASQUERADE_DOMAINに指定したドメインだけ書き換え
 - FEATURE(`masquerade_entire_domain`)だと
 - MASQUERADE_DOMAINに指定したドメイン以下の全ドメインを書き換え

Copyright (c) 2001 by Kazunori ANDO
IW2001

78

まとめ

- ◆ メールを安全なメディアにするには?
 - 携帯電話でメールを使う人も爆発的に増加
 - デバイスを選ばないユビキタス・メディア
 - 大規模サーバの安定性にまだ課題がある
 - 便利な一方でワーム/ウイルスの伝達手段にもなる
 - 情報漏洩の可能性もあちこちに
 - ちゃんと管理すべきものだが....

Copyright (c) 2001 by Kazunori ANDO
IW2001

79

付録(社内ホスト設定例)

```
VERSIONID(' $Id: config.mc,v 1.5 2001/12/04 12:27:36 ando Exp ando $')
OSTYPE(bsd4.4)dnl
DOMAIN(generic)dnl
MASQUERADE_AS('example.gr.jp')dnl
MASQUERADE_DOMAIN('iw2001.example.gr.jp')dnl
FEATURE('limited_masquerade')dnl
FEATURE('masquerade_envelope')dnl
EXPOSED_USER('root postmaster')dnl
FEATURE('mailertable')dnl
FEATURE('nocanonify')dnl
FEATURE('access_db')dnl
FEATURE('blacklist_recipients')dnl
FEATURE('accept_unresolvable_domains')dnl
MAILER(local)dnl
MAILER(smtp)dnl
Dmexample.gr.jp
Dwiw2001
define('confDOMAIN_NAME','Sw.Sm')dnl
define('SMART_HOST','smtp:[192.168.0.3]')dnl
define('confCF_VERSION','IW2001')dnl
```

Copyright (c) 2001 by Kazunori ANDO
IW2001

80