迷惑メールへの根本的な対策

山本和彦
(株)インターネット・イニシアティブ
kazu@iij.ad.jp

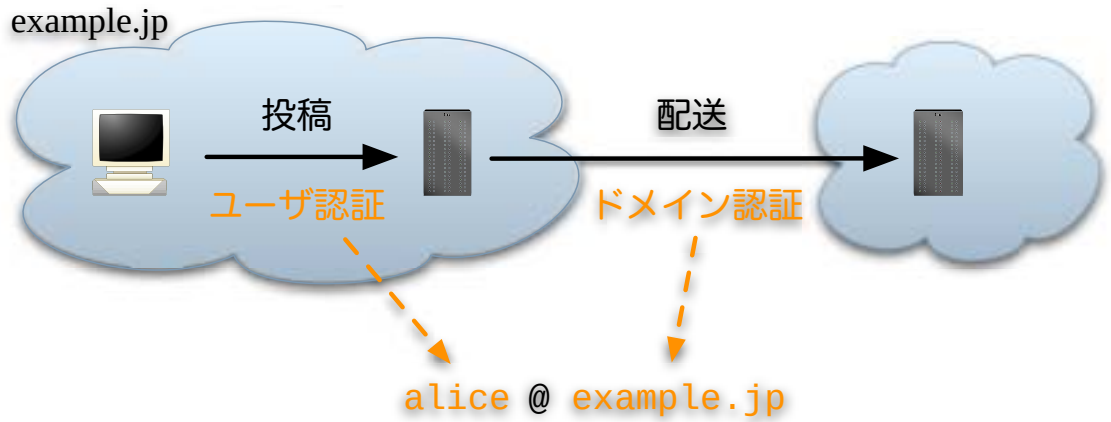
内容

- メールを追跡可能に
- 代替ポートとポート25番のブロック
- ドメイン認証
- 格付け
- ドメイン認証の詳細

メールを追跡可能に

2つの認証

- ゾンビからの配送の禁止
- 配送と投稿の分離
- 投稿に対するユーザ認証
- 配送に対するドメイン認証

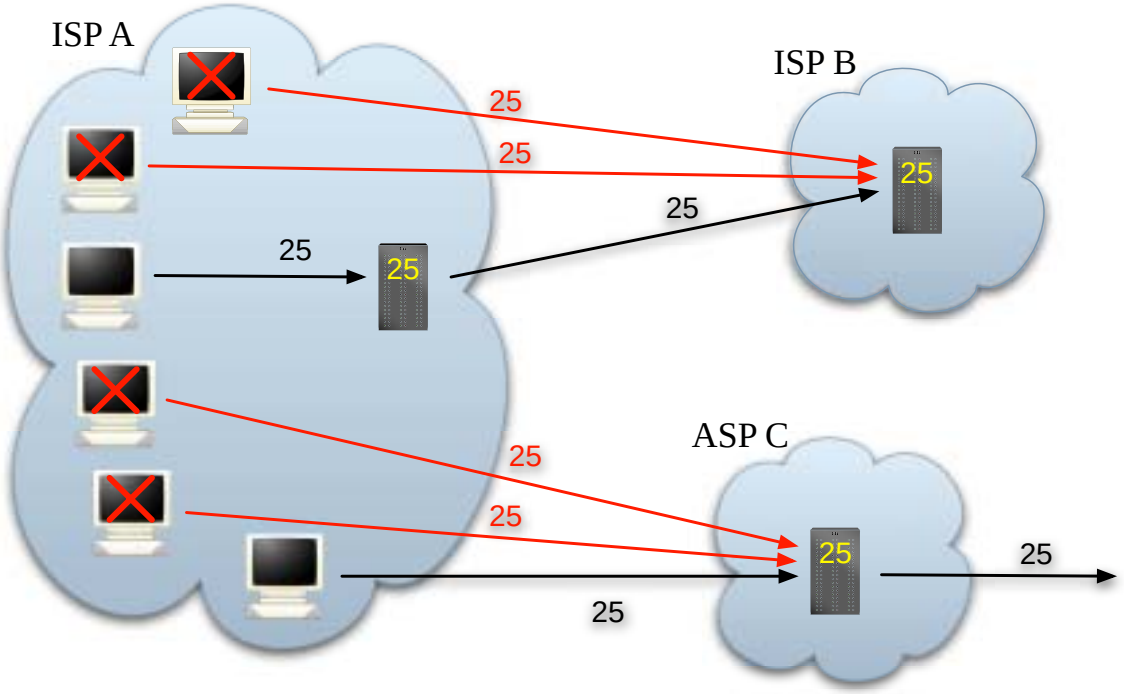


- メールアドレスを詐称できない世界
  - 迷惑メールを受け取ったら、そのドメインの管理者へ文句を言えばよい

注意

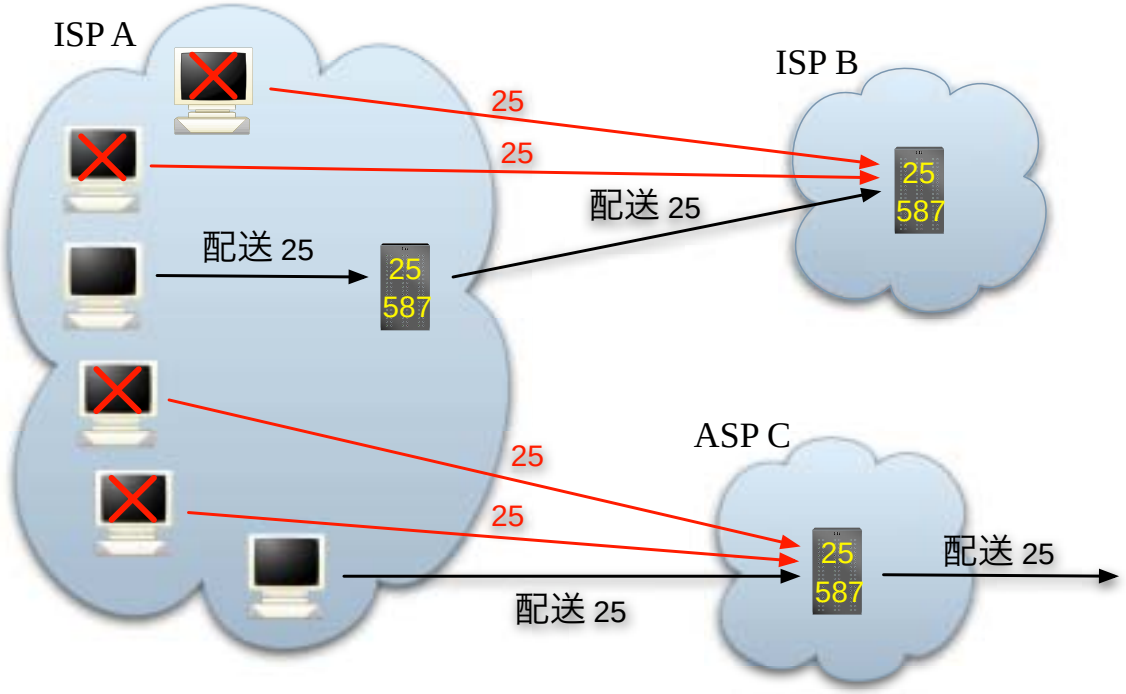
- ISP/ASP のメール管理者の「共通理解」
- 内容はあくまで理想論
  - すべての ISP/ASP が、すべてを実現できる訳ではない
    - 政治的な理由
    - 技術的な理由
    - 経済的な理由
- インターネットのあるべき姿は？
  - ユーザに自由を与えるが、責任も課す？
  - ユーザの自由を制限するが、安全なサービスを提供する?

問題点



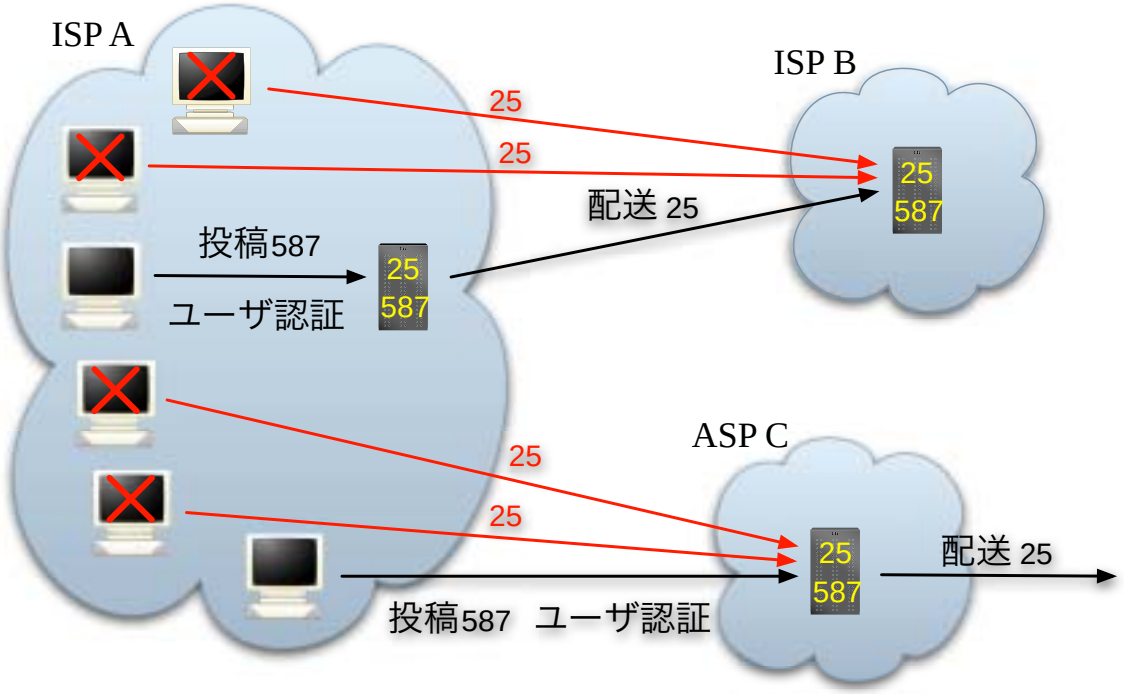
- ゾンビ(bot)による迷惑メールの大量送信
- メールアドレスの詐称
  - メールの追跡が困難、フィッシング

投稿ポートの提供



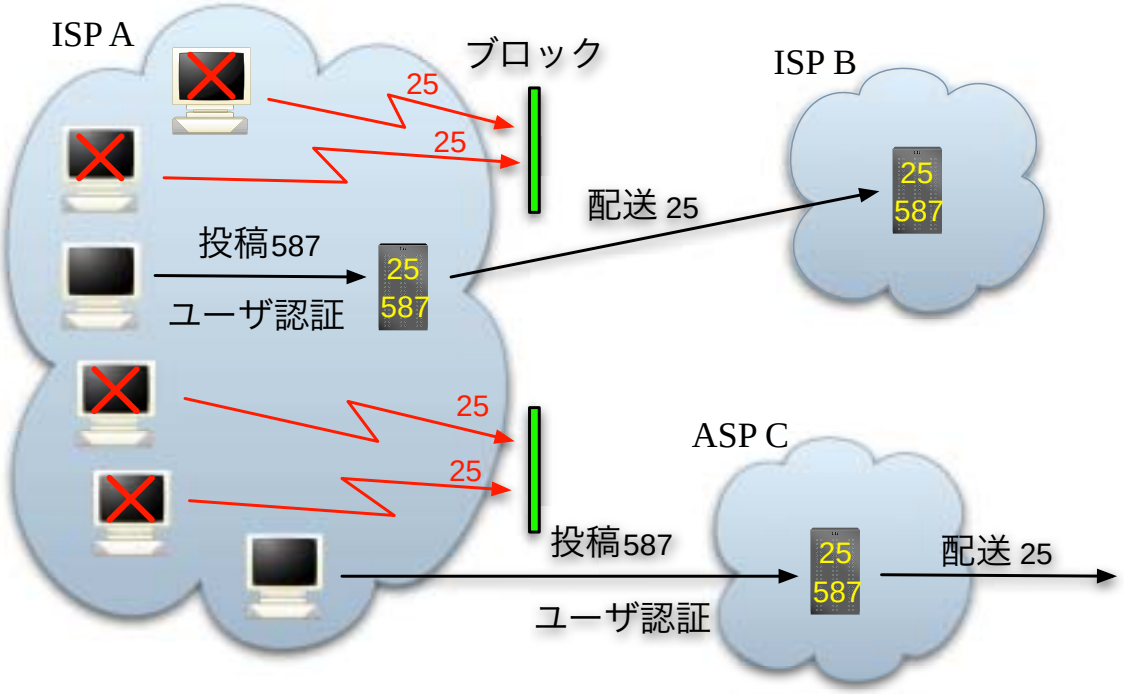
- **配送** = **サーバ間の通信 (ポート** 25 **番)**
- **投稿** = **メールリーダとサーバの通信 (ポート** 587 **番)**
  - Submission：**プロトコル自体は** SMTP

投稿ポートへの移行



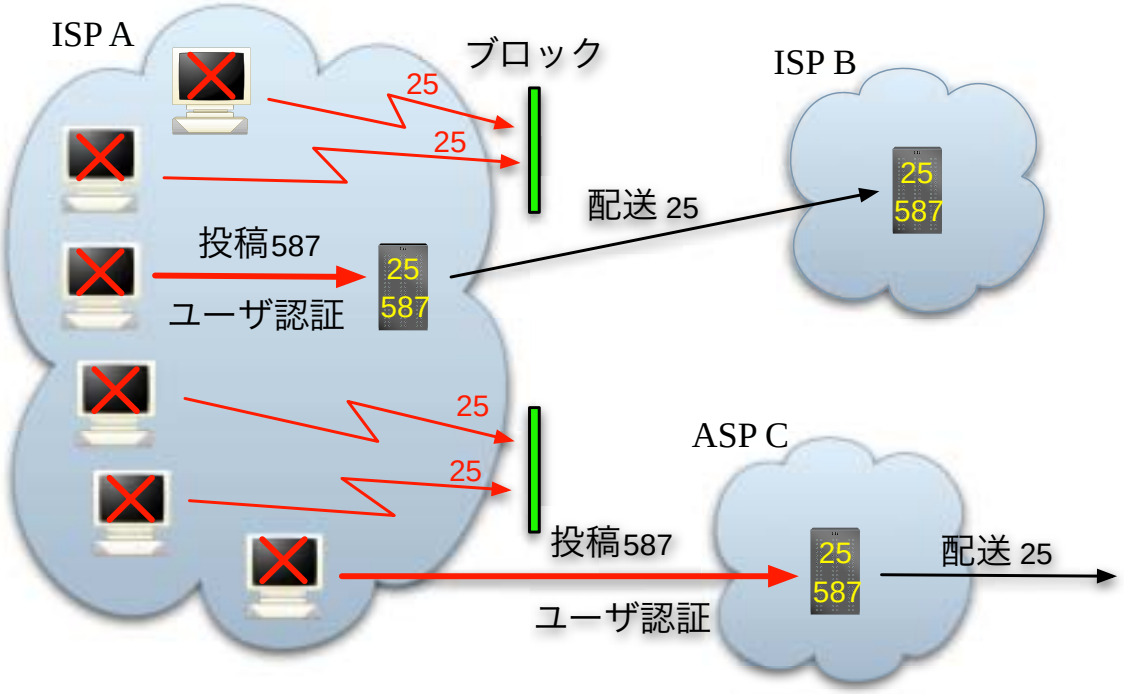
- **投稿ポートにはユーザ認証が必須**
  - POP before SMTP では不十分
- **理想的には、ポート 25 番への投稿を禁止する**

25番ポートのブロック



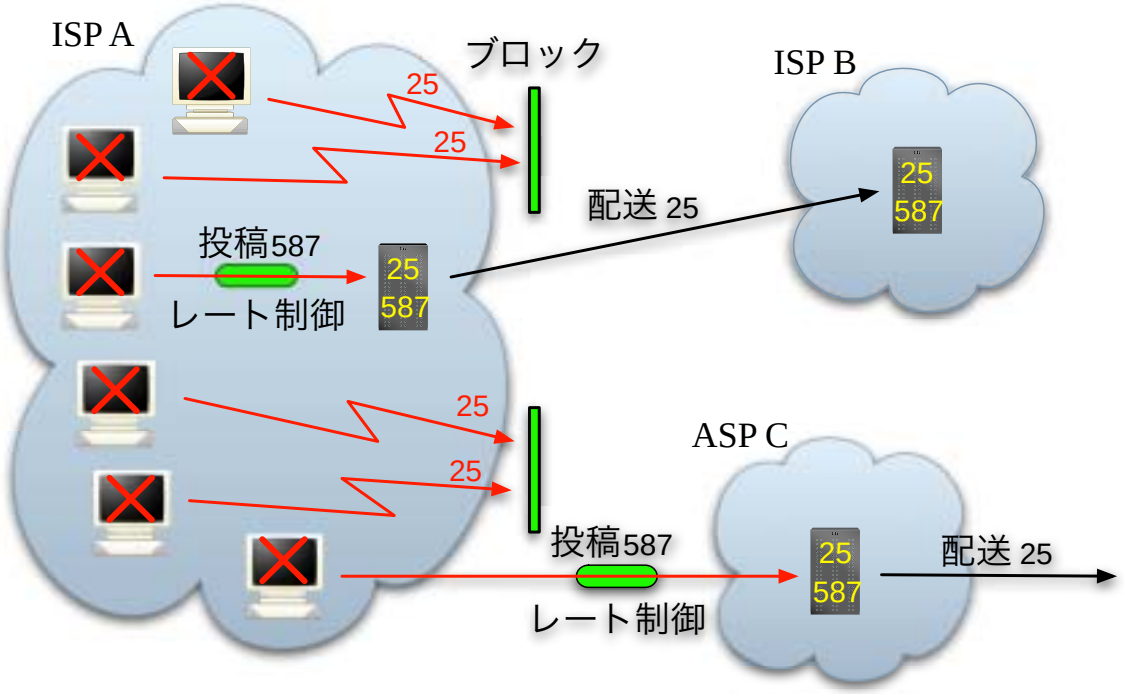
- **ポート 25 番をブロックする**
  - **追跡しにくい動的 IP からのみ**
  - **独自にメールサーバを運用したい人は、固定 IP へ**

予想される新しい攻撃



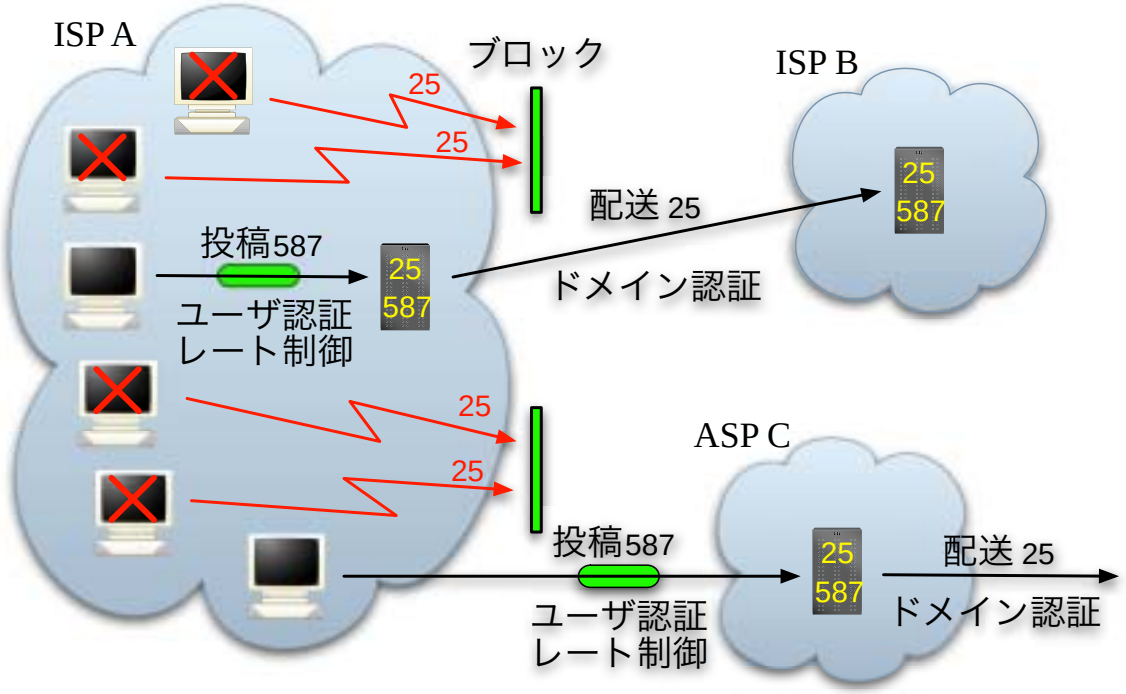
- パスワードを盗むゾンビが出現？
- 堂々と迷惑メールを投稿する配送業者

レート制御



- 投稿にレート制御をかける
  - 短時間にたくさんの迷惑メールを送られることを禁止

ドメイン認証



- 配送にはドメイン認証を必須にする
  - 本当にそのドメインの送信サーバから送られているか検査

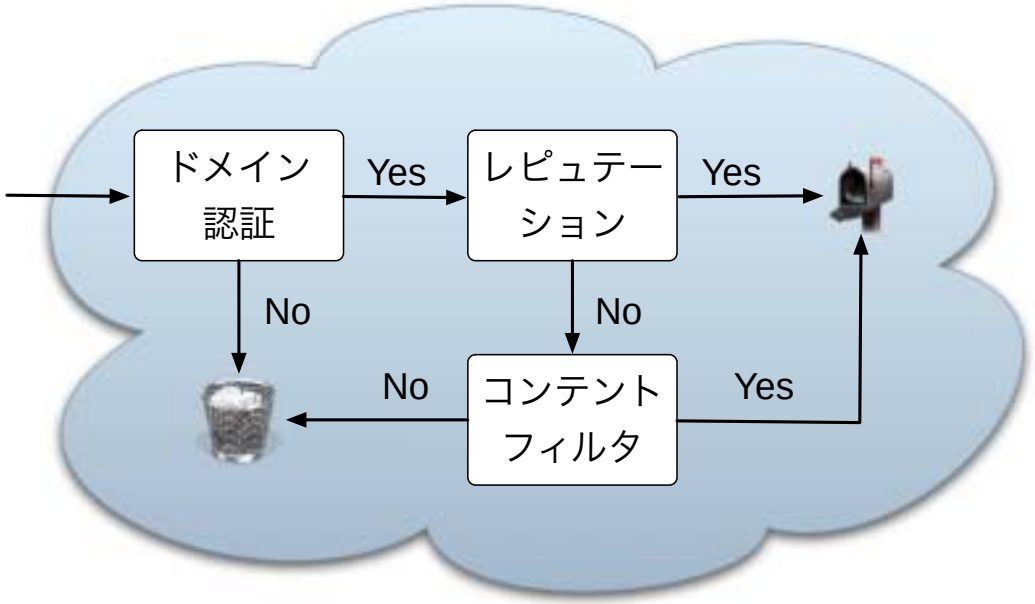
格付け

- メールが追跡可能になった後、
  迷惑メール配送業者は
  - 独自のドメインを取る (日替わりドメイン)
  - ドメイン認証に対応する
  - 堂々と迷惑メールを送る
- 配送元を格付けするシステムが必要
  - レピュテーション (reputation) と呼ばれる
  - IP アドレス、ドメイン
  - ドメインの格付けの例：cloudmark.com

```
% dig iij.ad.jp.rating.cloudmark.com txt
iij.ad.jp.rating.cloudmark.com.  1M IN TXT  "Status: Good"
iij.ad.jp.rating.cloudmark.com.  1M IN TXT  "Rating: 100"
```

ISP/ASP の将来像

一例



代替ポートと
ポート25番のブロック

投稿ポートへの移行

- 理想的には
  - 投稿ポート(587)＋ユーザ認証のみを提供
  - ポート 25 番は投稿目的では利用不可にする
- メールリーダの対応状況
  - ほとんどすべてのメールリーダは、
    ユーザ認証を実装済みで、ポートも変更可能
  - 機械的に送られるメールが問題
    - 自動的にレポートを送るプログラム
    - ネット家電
- 現実的には
  - 同じドメイン内からはポート 25 番での投稿を受け付ける
  - ドメイン外からは投稿ポート(587)のみを受け付ける

代替ポート

- **代替ポートとしての** SMTP over SSL
- SSL
  - SMTP **には変更が不要**
  - **別ポートが必要**
- TLS
  - SMTP **に変更が必要**
  - **同じポート**
- SMTP over SSL **の問題**
  - **ポート** 465 **番は、以前** SMTP over SSL **に割り当てられていた**
  - **現在、**Cisco **のあるプロトコルに割り当てられている**
  - IETF **は** SMTP over SSL **には、二度とポート番号を割り当てない**
  - **国内の** ISP/ASP **は、ポート** 465 **番を使っている**

SMTP/Submission over SSL/TLS

- **推奨**
  - Submission over TLS (**ポート**587**番**)
    - **投稿用には、これが一番**
  - SMTP over SSL (**ポート** 465 **番**)
    - **投稿用にこのサービスを提供しているところは、止める必要はない**
  - SMTP over TLS (**ポート**25**番**)
    - **配送に暗号化が必要であれば**
- **日本の** ISP/ASP **の対応状況**

  http://www.wakwak.com/info/spec/port25/mail_group.html

25番ポートのブロックの導入実績

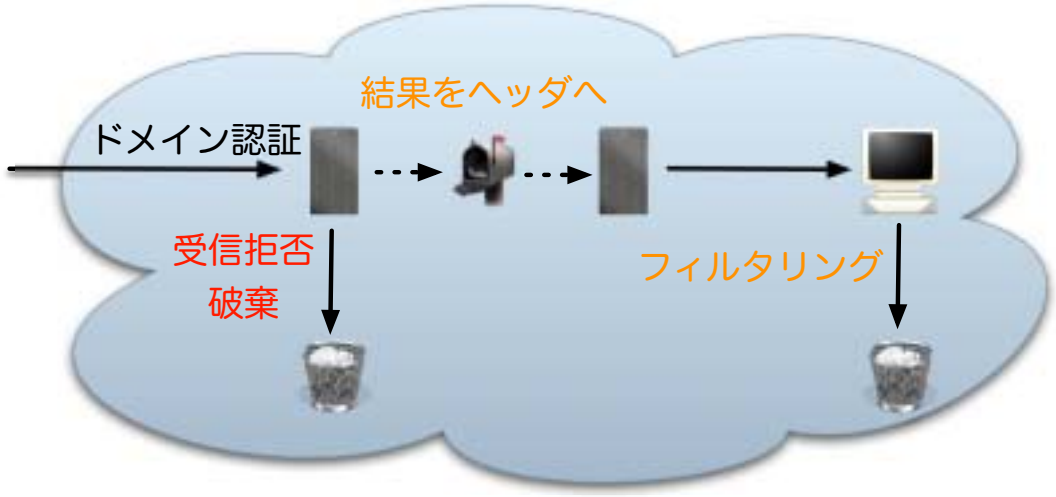
- **アメリカ**
  - AT&T、Bell CA、Bell South、Comcast
  - Earthlink、MSN、Verizon
  - **詳しくは**
    - http://www.postcastserver.com/help/Port_25_Blocking.aspx
- **日本**
  - **ぷららネットワークス**
    - http://www.plala.or.jp/access/living/releases/nr05_jan/0050127.html
    - **携帯事業社向け**
  - WAKWAK(NTT-ME)
    - http://www.wakwak.com/info/news/2005/port25blocking0107.html
    - **全面**
  - SANNET
    - http://www.sannet.ne.jp/news/20050331-1.html
    - **全面**

ドメイン認証

ドメイン認証の候補

- IP アドレス型
  - SPF、Sender ID (MFROM)
    - 封筒の送り主 (SMTP MAIL FROM)
  - Sender ID (PRA)
    - 便箋の送り主 (メールのヘッダ)
- 電子署名型
  - DKIM
    - 便箋の署名
    - Yahoo! DomainKeys と Cisco IIM を統合
- これらは共存できる
- ヘッダを保護できればフィッシング対策となる
  - Sender ID (PRA)
  - DKIM

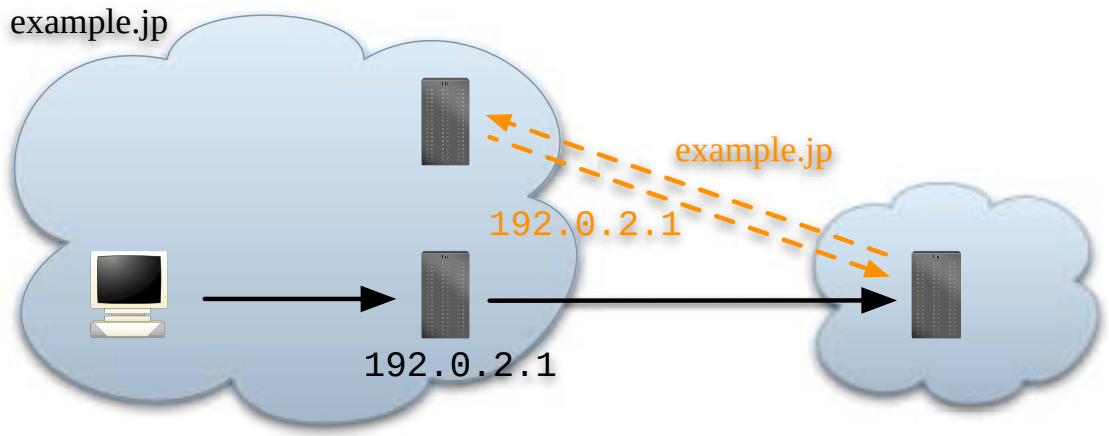
普及のストーリー



- 移行前期
  - 受信サーバは認証結果をメールのヘッダへ

    Authentication-Results: mx.example.jp
    from=bob@example.jp; sender-id=pass; spf=pass
  - メールリーダは認証結果を元にフィルタリング
- 移行後期
  - 受信サーバは認証に失敗したら受信拒否

IPアドレス型



- **受信側**
  1) SMTP コネクションから相手の IP アドレスを得る
  2) 保護対象となるドメイン名を取り出す
     - SMTP MAIL FROM
     - メールのヘッダ
  3) そのドメイン名で DNS を索き、
     送信サーバの IP アドレスを得る
  4) 1. と 3. の IP アドレスを比較

SMTP の動作例

S: 220 mail.example.com ESMTP Sendmail 8.8.5
C: EHLO host.example.jp **＃ あいさつ (セルフループの検出)**
S: 250 Hello host.example.jp, pleased to meet you
C: MAIL FROM:<alice@example.jp> **＃ 送信者を指定**
S: 250 <alice@example.jp>... Sender ok
C: RCPT TO:<bob@example.com> **＃ 受信者を指定**
S: 250 <bob@example.com>... Recipient ok
C: DATA **＃ メール本体をこれから渡す**
S: 354 Enter mail, end with "." on a line by itself
C: Subject: A test message
C: From: alice@example.jp
C: To: bob@example.com
C:
C: This is a body.
C: --Alice
C: .
S: 250 Message accepted for delivery
C: QUIT **＃ 通信終わり**

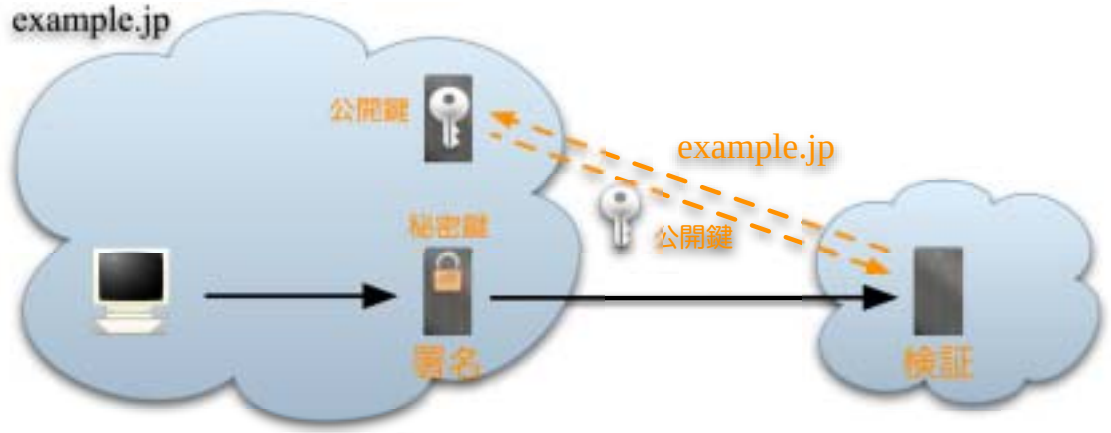
SPF (Sender Policy Framework)

- POBOX **が提唱**
- **送信サーバの宣言**
  - exmaple.com IN TXT "v=spf1 +a +mx -all"
    - A RR **か** MX RR **の** IP **アドレスのみ送信可能**
  - "+" → pass
    - **受信許可**
  - "?" → neutral
    - SPF RR **がないことと同等**
  - "~" → softfail
    - **一時エラーを返す**
  - "-" → fail
    - **受信拒否**
  - Web **サービスのみのドメインの例**
    - exmaple.jp IN TXT "v=spf1 -all"
- **保護対象となるドメイン名は、**SMTP MAIL FROM

Sender ID

- IETF で SPF と Caller ID を統合
- 送信サーバの宣言は SPF と同様
  - example.com IN SPF "spf2.0/mfrom,pra +a +mx -all"
  - "v=spf1" は "spf2.0/mfrom,pra" と読み替える
- 保護対象となるドメイン名は
  - SMTP MAIL FROM (MFROM)
  - メールのヘッダ (PRA)
  - 受信者が選択する
- PRA =「責任があるとされるアドレス」
  - PRA(Purported Responsible Address) と呼ぶ
  - Resent-Sender:, Resent-From:, Sender:, From:

電子署名型



- 送信側
  - 秘密鍵を使って署名
- 受信側
  - 保護対象となるドメイン名を取り出す
  - そのドメイン名で DNS を索き、公開鍵を得る
  - 公開鍵を使って署名を検証

DKIM

- **メールの電子署名**

```
DKIM-Signature: a=rsa-sha1; d=example.net; s=brisbane
 c=simple; q=dns; i=@eng.example.net; t=1117574938; x=1118006938;
 h=from:to:subject:date;
 z=From:foo@eng.example.net|To:joe@example.com|
   Subject:demo%20run|
   Date:July%205,%202005%203:44:08%20PM%20-0700
 b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4z
   GeeruD00lszZVoG4ZHRNiYzR
```

- DNS **での公開鍵の宣言**

```
% dig omgo._domainkey.iij.ad.jp txt
omgo._domainkey.iij.ad.jp. 86400 IN     TXT     "g=; k=rsa; t=y;
p=MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAM3STVzQy4
dy3cSb7rseAtdXmSmjGCNWQy8ttVs8Nord0487PiQS9kWYOgX
djXfJE3PLyi0WcnvxofzDasm+4zUCAwEAAQ=="
```

- **公開鍵は自分で作る**
  - **認証局とはまったく関係ない**

格付け

ブラックリスト

- **さまざまなブラックリスト**
  - SMAPCOP
    - http://www.spamcop.net/
  - SBL
    - http://www.spamhaus.org/sbl/
  - CBL
    - http://cbl.abuseat.org/
  - DSBL
    - http://dsbl.org/
  - BOPM
    - http://opm.blitzed.org/
- **問題**
  - **信用できるか？**
  - 0 or 1 **でいいのか？**

ホワイトリスト

- **認定**(accreditation)**サービス**
  - **責任あるホワイトリスト**

- Bonded Sender Program (BSP)
  - IronPort **による認定サービス**
    - http://www.bondedsender.com/
  - **参加企業は迷惑メールを出さないと誓約し供託金を積む**
  - **だれでもホワイトリストに入っているか検索可能**

    % dig 1.2.0.192.query.bondedsender.org

    入っていれば → 127.0.0.10

    入ってなければ → 空
  - **ユーザから迷惑メールだと言われたら、第三者機関が判定**
    - AOL **のユーザインターフェイスには、迷惑メールのレポート機能がある**
  - **迷惑メールであれば、供託金が差し引かれる**
    - **差し引かれた供託金は慈善団体へ寄付**
    - **供託金がなくなれば、ホワイトリストから削除**

レピュテーション

- 種々の情報から配送元を格付けする
  - IP アドレスのブラックリスト
  - IP アドレスのホワイトリスト、認定サービス
  - メールの流量 (BSP など)
  - 独自の情報
- 配送元の識別子
  - IP アドレス
  - ドメイン
- レピュテーションの例
  - Cloudmark の rating
    - ドメイン・ベース
    - フリー
  - IronPort の SenderBase
    - IP アドレス・ベース
    - IronPort の製品からしか参照できない
  - CipherTrust の TrustedSource

ドメイン認証の詳細

普及率の測定

- DNS の宣言から普及率を推し量る
- JPRS と WIDE プロジェクトの共同研究
  - .jp 以下のすべてのドメインを調査
    http://jpinfo.jp/stats/
- SPF/Sender ID
  - v=spf1、spf2.0 の合計
  - 送信側の対応状況は分かる
  - 受信側の対応状況は分からない
- DKIM
  - 公開鍵の場所は、メールのヘッダからしか判断できない
  - 場所の分かるポリシーを調査
    - _domainkey.example.jp
  - ポリシーなしでも DK は使用可能
  - 送信側は氷山の一角の数
  - 受信側の対応状況は分からない

普及率の測定

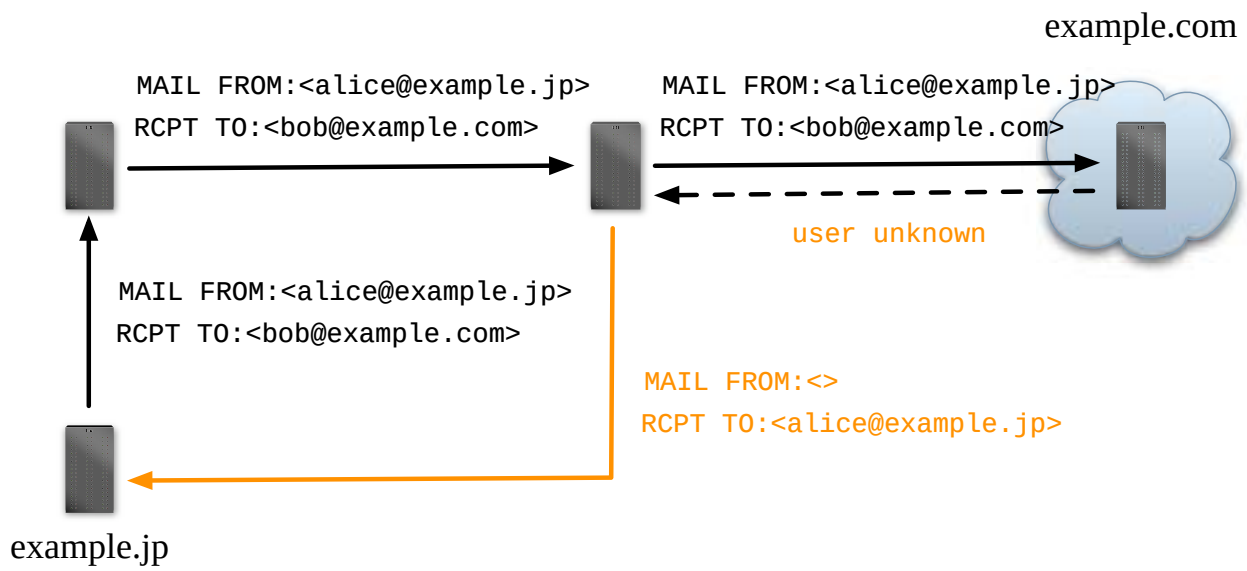
- 2005年7月
  - http://member.wide.ad.jp/wg/antispam/

ゾーン	総数	MX	SPF	DK	誤 DK
汎用	397161	255087	489	1	25
AC	3192	3003	10	0	0
AD	299	257	10	1	1
CO	275219	255199	236	3	14
ED	4327	3916	0	0	0
GO	839	722	1	0	0
GR	9149	7762	14	0	0
LG	2673	982	0	0	0
NE	17299	13178	68	1	7
OR	20352	18971	20	1	1
地域	4010	3445	8	0	0
合計	734520	562522	856	7	48

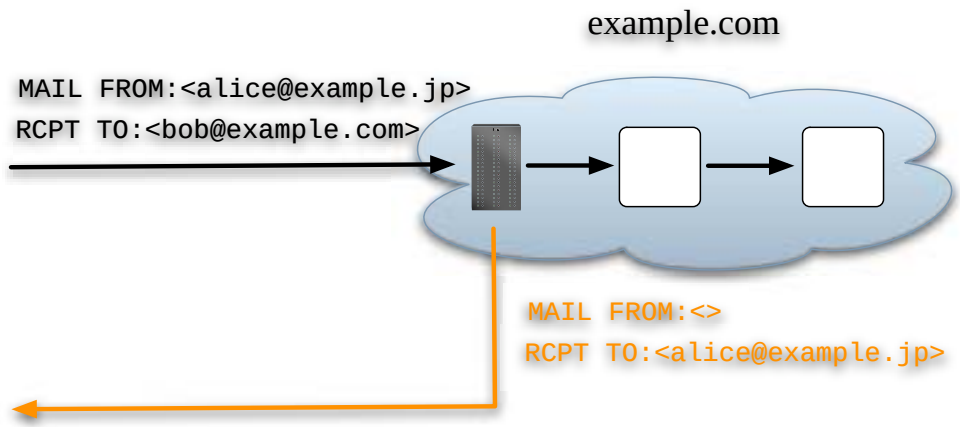
SPF とエラーメール

- SPF RR を書くと受け取るエラーメールが減る？
  - SPF RR を書く強い動機になる
- IIJ では、"?all" と宣言したが減らなかった
  - 認証に失敗すれば、SPF の宣言はないのと同等
- "-all" と宣言すると減るのか？
  - 認証に失敗すれば、受信拒否

エラーメール


example.com
MAIL FROM:<alice@example.jp>
RCPT TO:<bob@example.com>
MAIL FROM:<alice@example.jp>
RCPT TO:<bob@example.com>
user unknown
MAIL FROM:<alice@example.jp>
RCPT TO:<bob@example.com>
MAIL FROM:<>
RCPT TO:<alice@example.jp>
example.jp

ISP での受信の仕組み



- ISP はハーベスティング攻撃を防ぐため、すべてのメールを受け取る
  - ハーベスティング攻撃 = メールアドレスを収集する方法
    - Web から収集
    - ランダムなユーザ名のメールアドレスへメールを送りつける
- 内側で多段の検査
  - 最初に SPF を検査し、認証失敗ならメールを捨てる？
  - AOL で採用？

エラーメールの測定

- Mew.org に SPF RR を書いた
  - 2005年4月20日
  - v=spf1 +mx -all

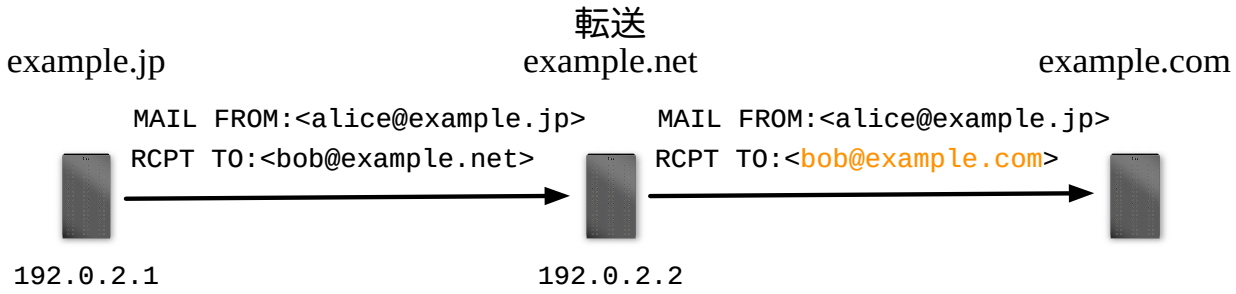
日付	全体	AOL
2005/04/15	539	1
2005/04/16	510	1
2005/04/17	446	4
2005/04/18	534	5
2005/04/19	628	3
2005/04/20	606	2
2005/04/21	509	4
2005/04/22	720	2
2005/04/23	597	1
2005/04/24	510	3
2005/04/25	755	3

- 根拠のない噂だった...
  - しかしながら SPF RR はレピュテーションに影響する

ドメイン認証の問題点

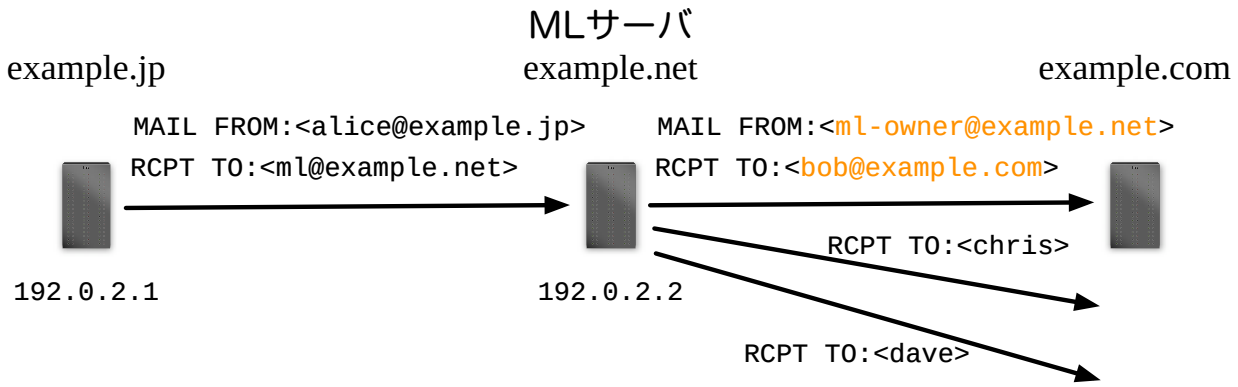
- **特許**
  - Microsoft **は、**Sender ID **の** PRA **に特許を持つ**
  - **防御目的**
- SMTP **レベルでの転送**
- **メーリングリスト**
- **第三者サーバ**
  - **会社のメールアドレスを使って、自宅で契約している** ISP **からメールを送る**

SMTP レベルでの転送



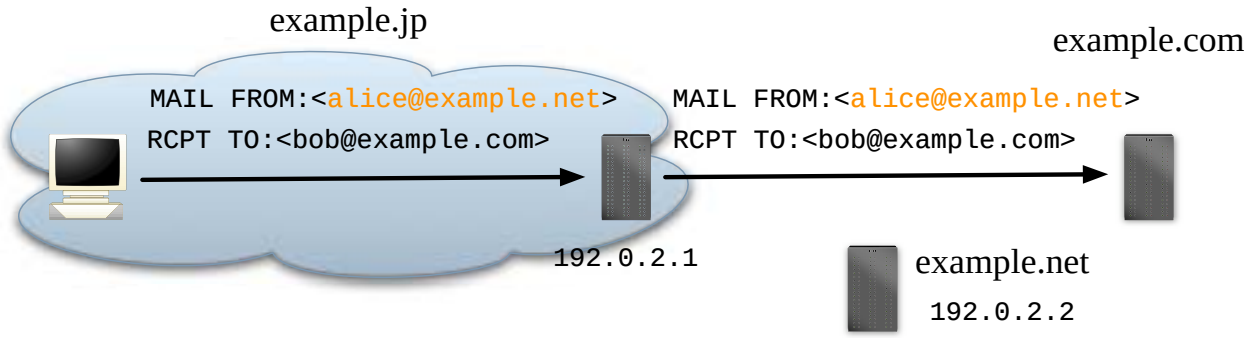
- SPF、Sender ID (MFROM)
  - IP アドレスが変わるので認証に失敗する
  - SMTP MAIL FROM の SUBMITTER を使えば解決できる
    - MAIL FROM: <alice@example.jp> SUBMITTER=bob@example.net
- Sender ID (PRA)
  - IP アドレスが変わるので認証に失敗する
  - Resent-Sender: を付けることが推奨されている
    - Resent-Sender: bob@example.net
- DKIM
  - IP アドレスに依存しないので問題ない

メーリングリスト



- SPF、Sender ID (MFROM)
  - **問題はない**
- Sender ID (PRA)
  - Resent-Sender: **を付けることが推奨されている**
    - Resent-Sender: ml-owner@example.net
  - **実際の** ML **サーバは、**Sender: **を付けることが多い**
- DKIM
  - **メールの書き換えにより、検証が失敗することがある**

第三者サーバ



- SPF、Sender ID (MFROM)
  - **認証に失敗する**
  - SMTP MAIL FROM **の** SUBMITTER **を使えば解決できる**
    - MAIL FROM:<alice@example.net> SUBMITTER=alice@example.jp
- Sender ID (PRA)
  - Sender: **を付けることが奨励されている**
    - Sender: alice@example.jp
  - **ユーザ認証をしていないと、**Sender: **を付加できない**
- DKIM
  - **サーバが異なるので意図した秘密鍵では署名できない**

署名の検証が失敗する原因

- DKIM の署名はヘッダと本文が対象
- これまでに見つけた原因
  - Content-Transfer-Encoding: を変換するメールサーバ
    - → 変換しないように設定
  - Subject: を変更する ML サーバ
    - 通し番号を入れるため
    - → 署名対象から除外
  - Received: を削除する ML サーバ
    - ホップ数を稼ぐため
    - → 署名対象から除外
  - フィールドの順番を変える ML サーバ
- 対症療法
  - Subject: と Received: を署名の対象から外す
  - ほとんどの場合、うまくいく

問題点と解決案

- **使わない**
  - SMTP MAIL FROM の SUBMITTER
    - SMTP の変更は難しい
  - PRA
    - 特許問題
- SPF
  - 転送に弱い
  - メーリングリストに強い
- DKIM
  - 転送に強い
  - メーリングリストに弱い
- **両者を組み合わせる**
  - どちらか一方の検証が成功すれば OK
  - どちらとも失敗なら
    - コンテンツ・フィルタへ
    - ゴミ箱へ