迷惑メールを低減するための根本的な技術対策

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

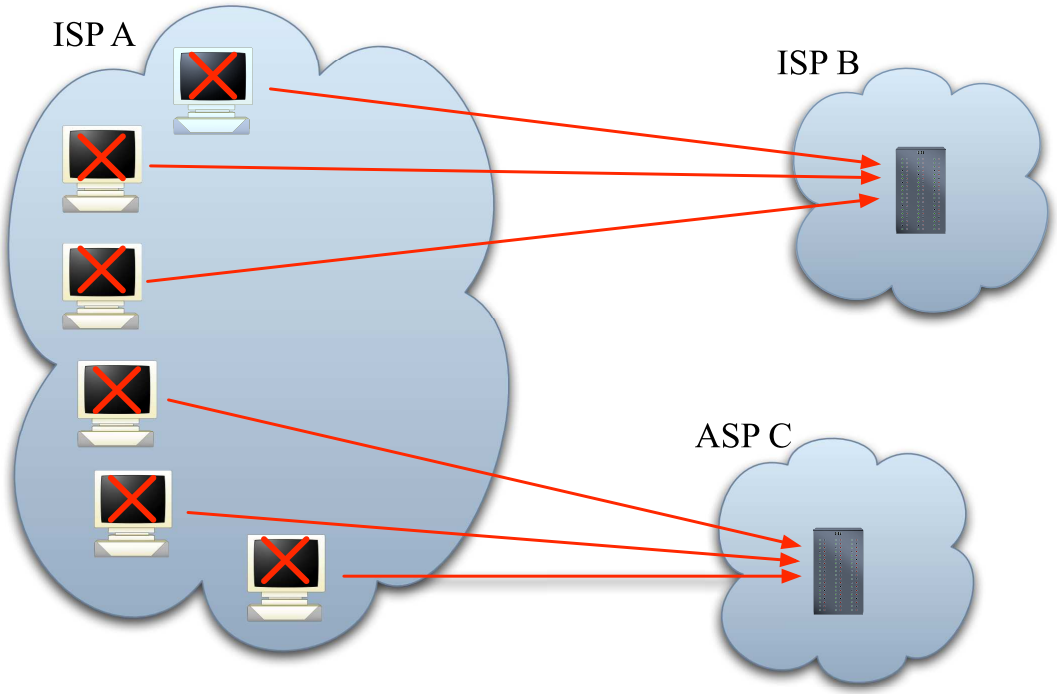
- 迷惑メールの問題点
  - Bot と渡り
- 根本的な対策
  - Outbound port 25 blocking (OP25B)
  - ユーザ認証
  - ドメイン認証
  - 格付け
- OP25B と投稿ポート
- ドメイン認証
  - DKIM
  - SPF
- SPF
  - SPF のメリット
  - 転送との相性問題の解決
- まとめ

迷惑メールの問題点

インターネットと迷惑メール

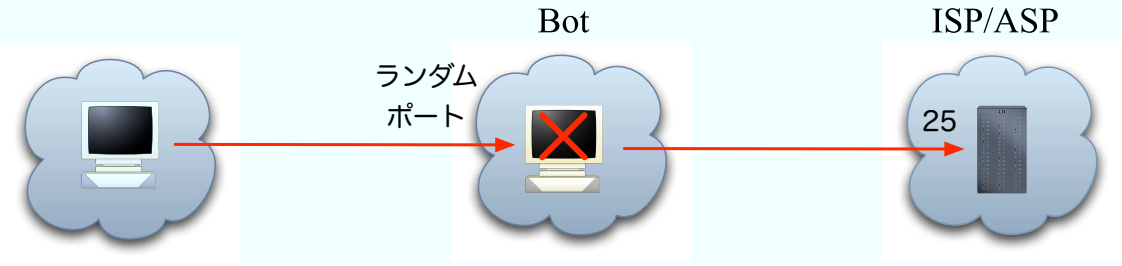
- インターネットの迷惑メールは急増加
  - 2004年の夏、一時的にそれまでの 10 倍になった
    - 迷惑メール配送業者が Bot を利用？
  - メールサーバを圧迫
- 大量の迷惑メール
  - ISP/ASP の「渡り」
  - Bot (ゾンビ)
- メールアドレスの詐称
  - 迷惑メール配送事業者の特定が困難
  - フィッシング

Bot (ゾンビ)



- 乗っ取られた PC を Bot (ゾンビ)と呼ぶ
  - Robot の短縮形

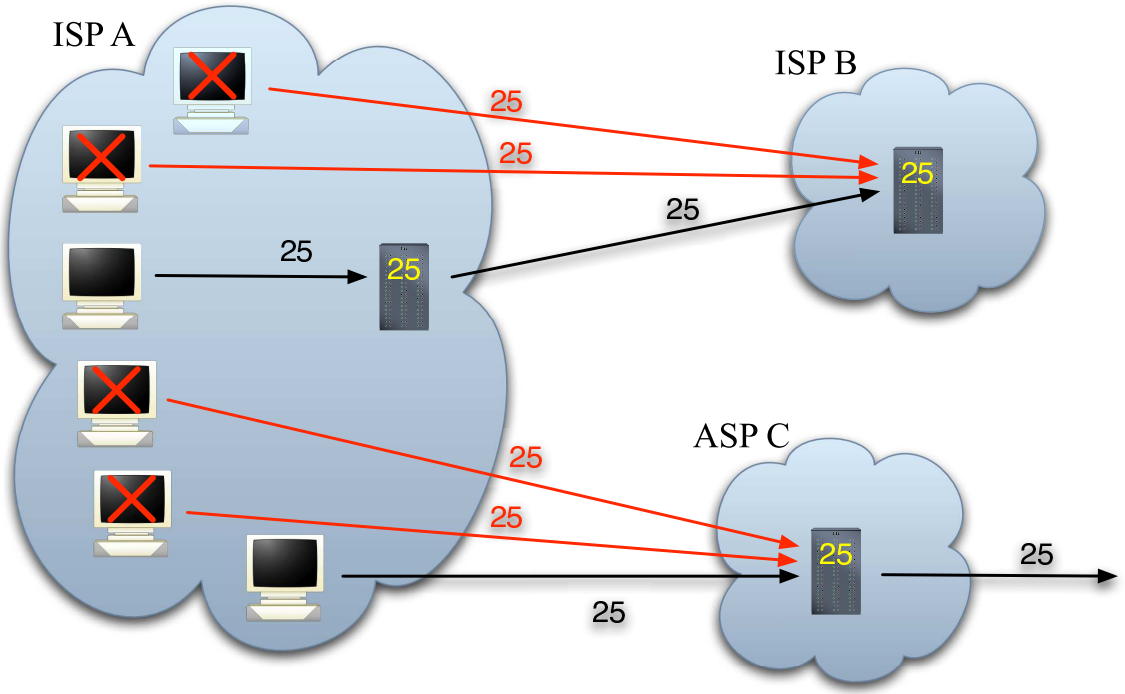
Bot の仕組み



- 身を潜めて PC を悪用
  - 愉快犯から闇のビジネスへ
- 特徴
  - ウイルスなどで PC に感染し、Bot をダウンロード
    - 素の Windows をグローバル IP でつなぐと、4 分程度で感染
    - 毎日数十種類の亜種が発生
  - コントローラへアクセスして、どう振る舞うか決める
  - 極めて高機能
- SMTP のオープンリレー
  - 最近ではランダムポートをポート 25 番へリレー
  - レンタルのため？

根本的な対策

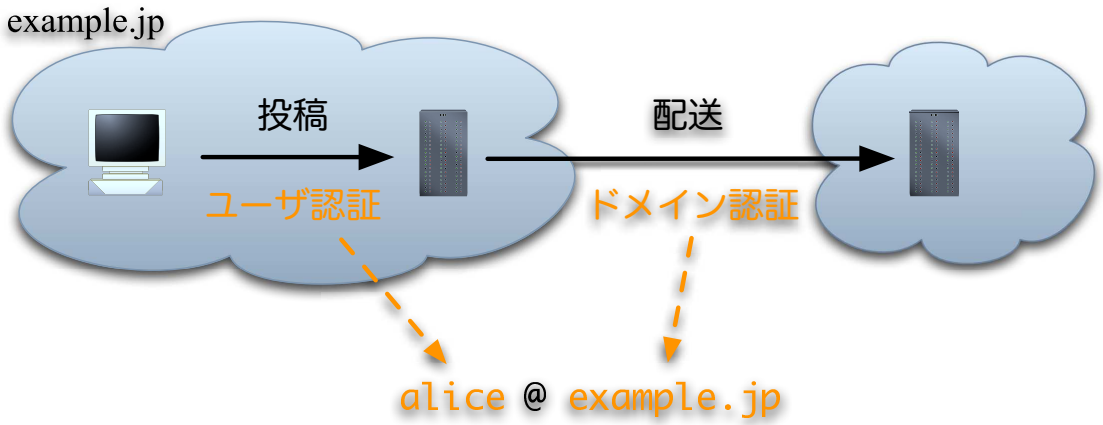
迷惑メールの問題点



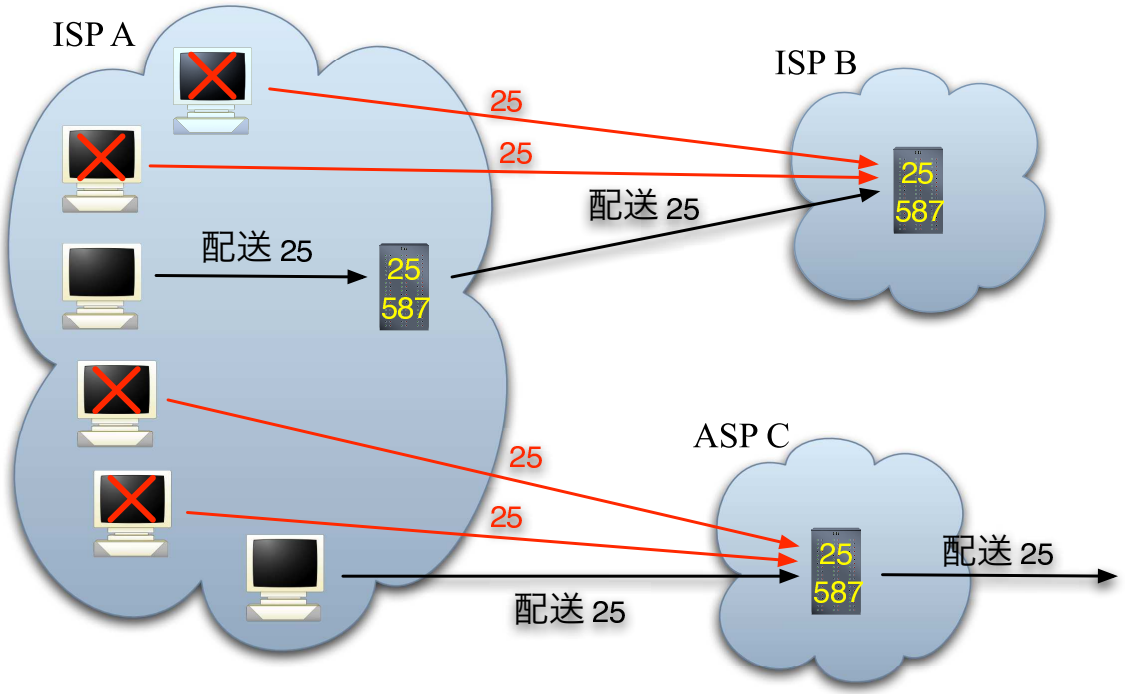
- 迷惑メールの大量送信
  - 渡り、Bot
- メールアドレスの詐称
  - 迷惑メール配送業者の特定が困難、フィッシング

根本的な対策

- Outbound port 25 blocking (OP25B)
  - Bot からの迷惑メールをブロック
  - 投稿と配送の分離
- 2つの認証
  - 投稿に対するユーザ認証 (SMTP AUTH)
  - 配送に対するドメイン認証 (SPF + DKIM)
  - メールアドレスの詐称を防止

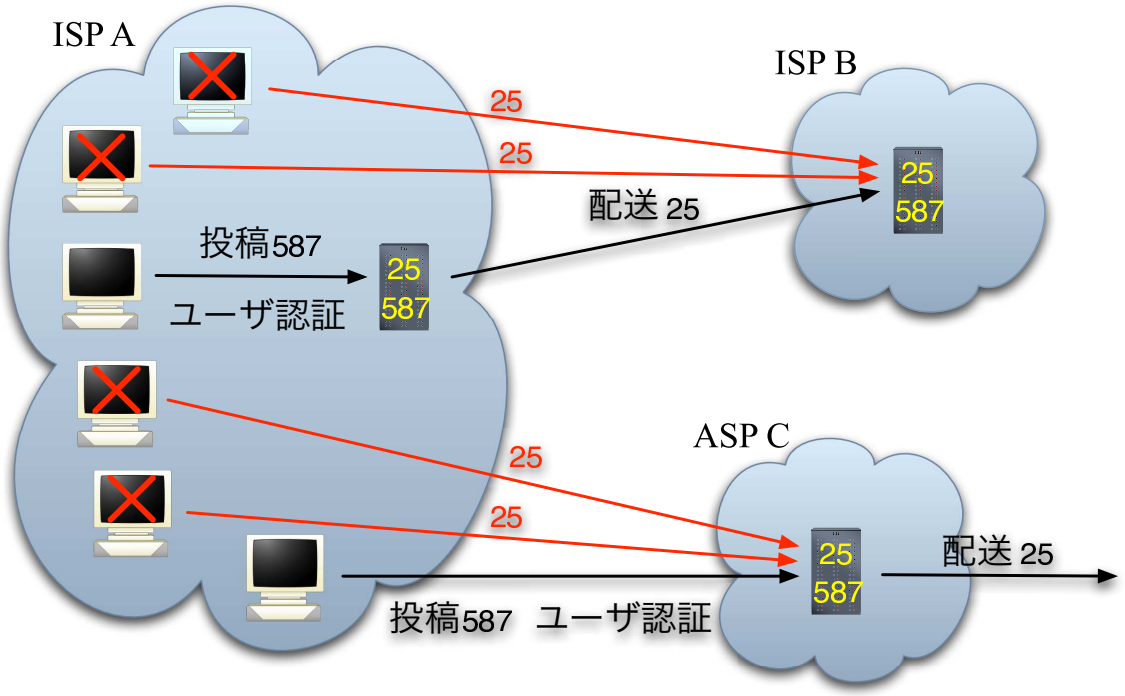


投稿ポートの提供



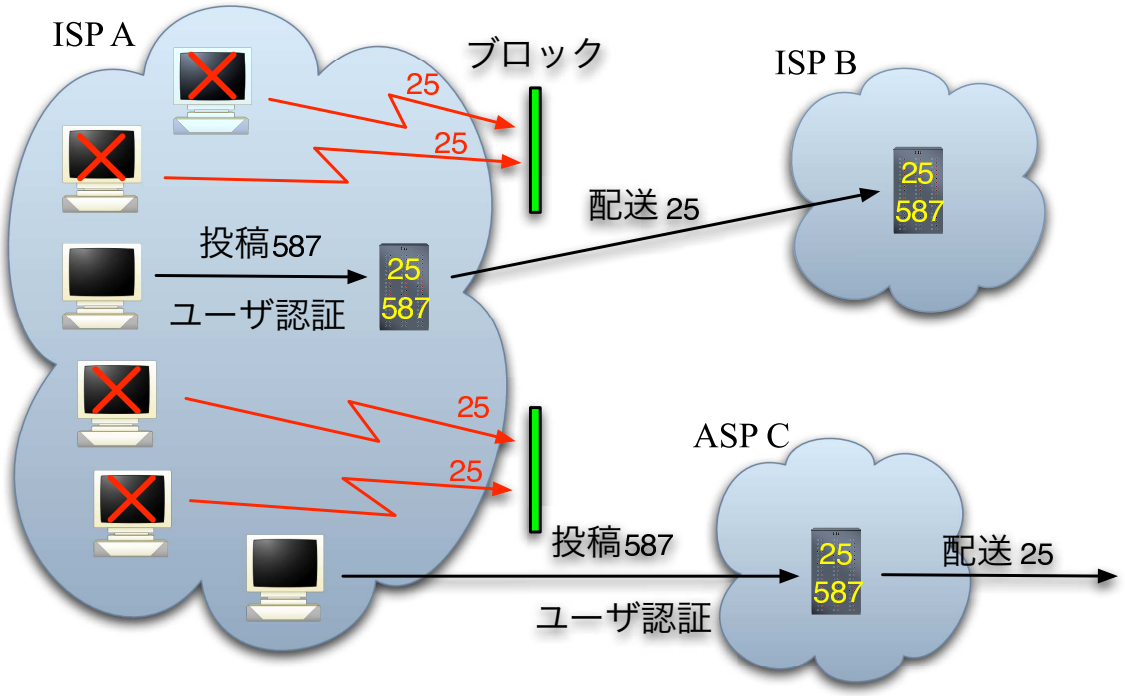
- 配送 = サーバ間の通信 (ポート 25 番)
- 投稿 = メールリーダとサーバの通信 (ポート 587 番)
  - Submission：プロトコル自体は SMTP

投稿ポートへの移行



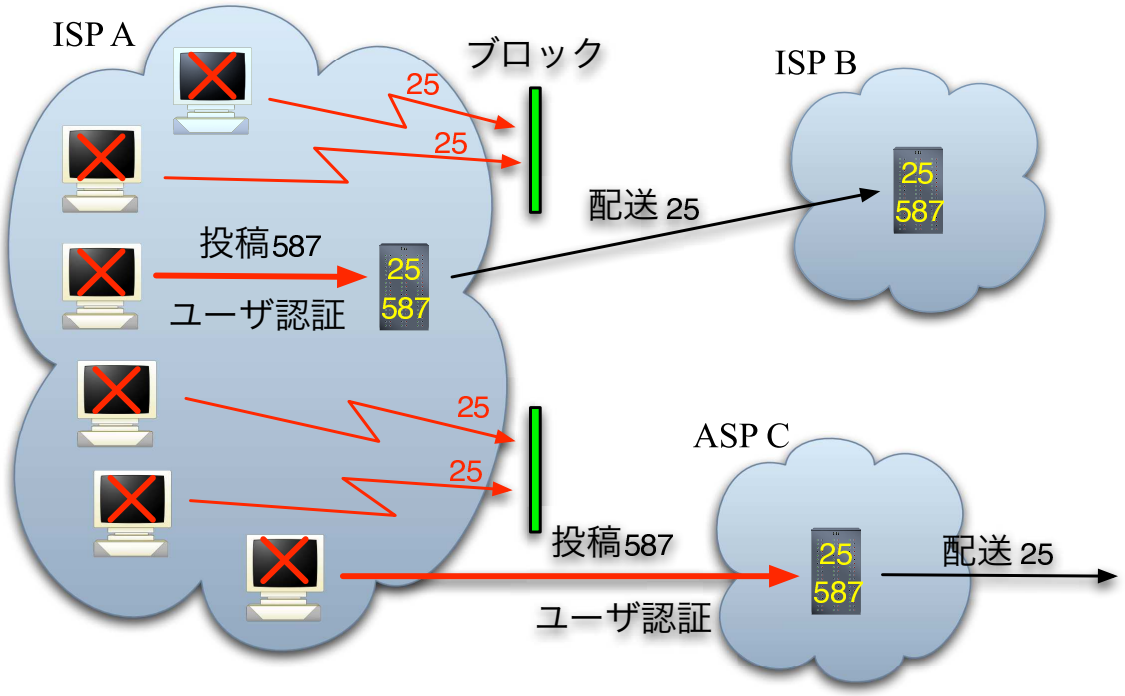
- 投稿ポートにはユーザ認証が必須
  - POP before SMTP では不十分

OP25B



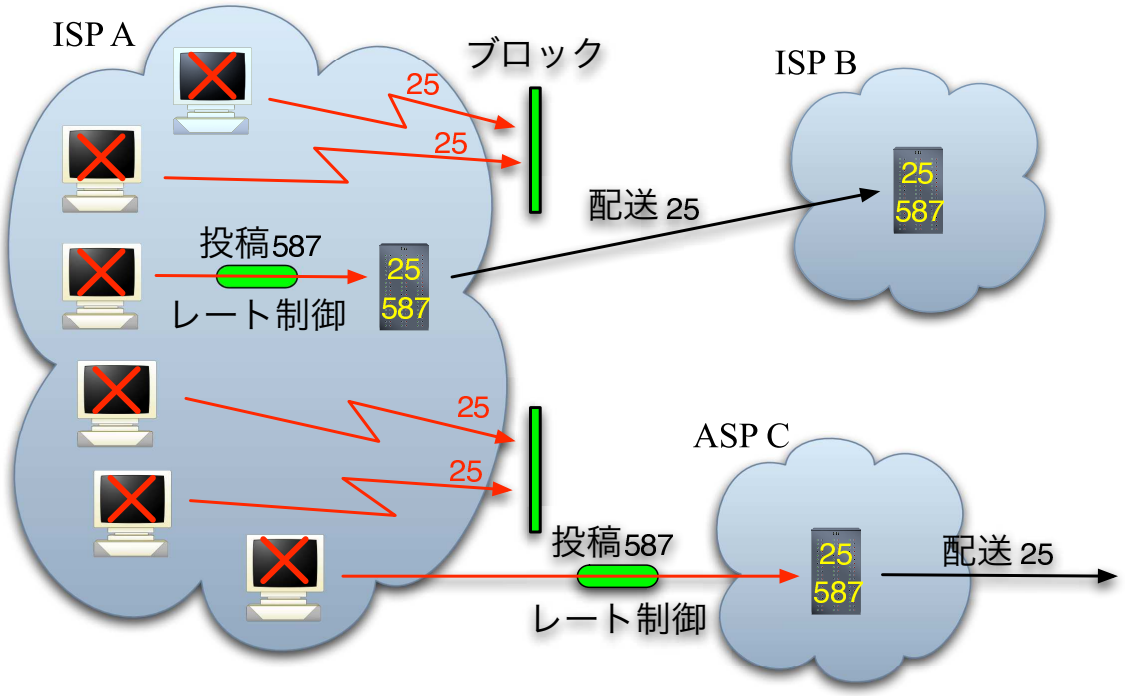
- ポート 25 番をブロックする
  - 追跡しにくい動的 IP からのみ
  - 独自にメールサーバを運用したい人は、固定 IP へ

予想される新しい攻撃



- パスワードを盗む Bot 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

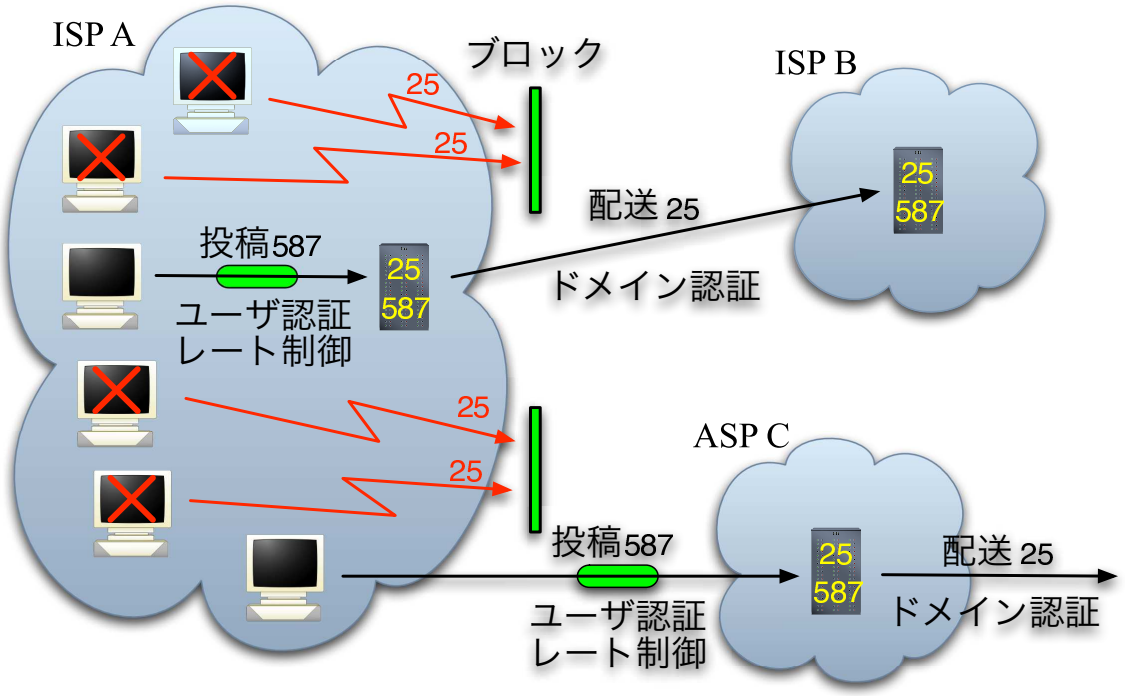


- 投稿にレート制御をかける
  - 短時間にたくさんの迷惑メールを送られることを禁止

レート制御

- 両方向
  - 受信(配送)と送信(投稿)
- 制限
  - メールの大きさ
  - 同時に受け付ける SMTP コネクションの数
  - ある IP アドレスから同時に受け付ける SMTP コネクションの数
  - ある IP アドレスから受け付ける SMTP コネクションの頻度
  - user unknown などを起こした通信相手に対し、次のコネクションを受け付けるまでの時間を長くする

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証

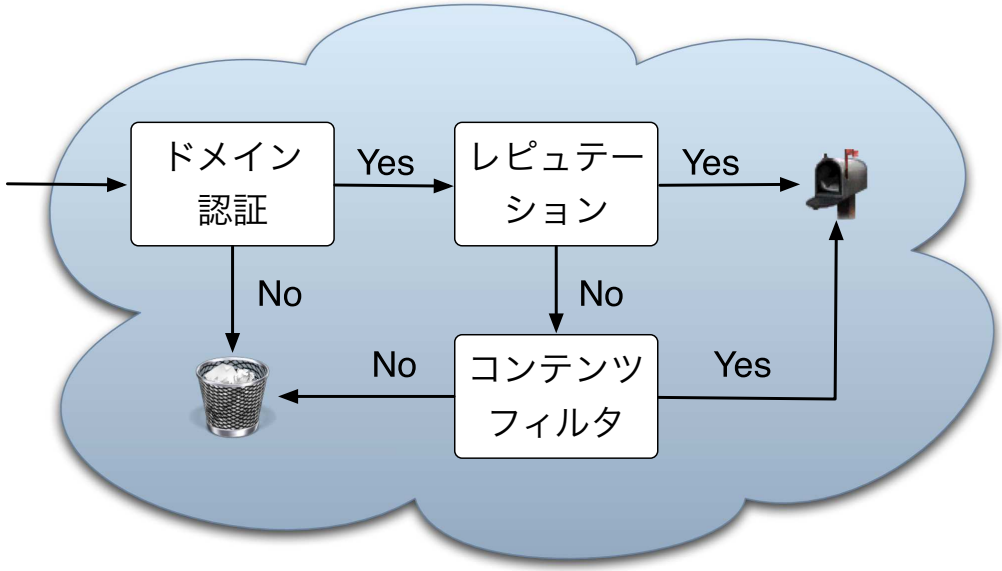
格付け

- 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"
```

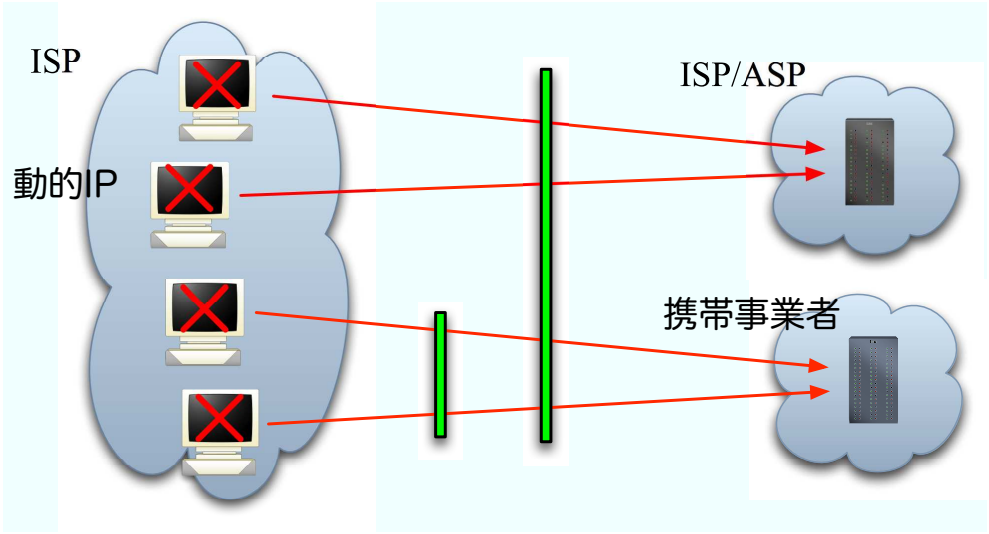
ISP/ASP の将来像

—例



OP25B と投稿ポート

OP25B の導入実績



- 携帯事業者のみ
  - ぷららネットワークス、hi-ho、NTTPC、KDDI、IIJ
- 全面
  - WAKWAK(NTT-ME)、SANNET、Nifty
- アメリカ
  - AT&T、Bell CA、Bell South、Comcast、Earthlink、MSN、...
    - http://www.postcastserver.com/help/Port_25_Blocking.aspx

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
- 注意
  - 知らない間に、ユーザ認証なしで投稿ポートを提供している
    サイトが多い！

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

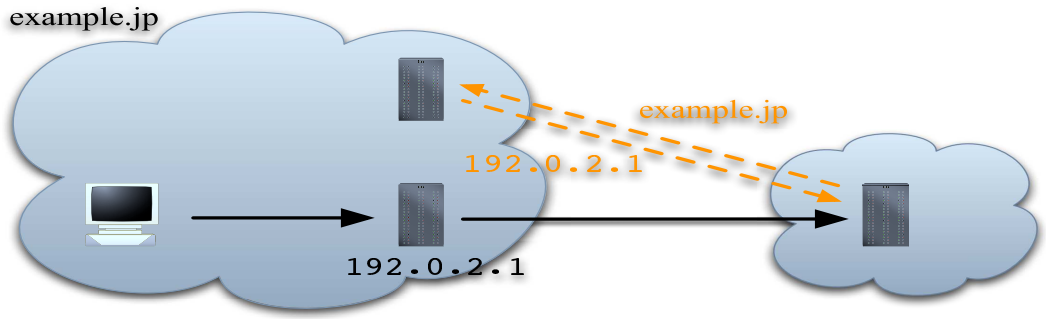
ドメイン認証

ドメイン認証の候補

- IP アドレス型
  - SPF (Sender Policy Framework)
    - SMTP MAIL FROM
- 電子署名型
  - DKIM (DomainKeys Identified Mail)
    - ヘッダ (From:) + 本文
- これらは共存できる
  - まず、IP アドレス型
  - 次に、電子署名型
- ヘッダを保護できればフィッシング対策となる
  - DKIM

SPF (Sender Policy Framework)

- 送信サーバの宣言 (SPF RR, TXT RR)
  - example.jp IN TXT "v=spf1 +ip4:192.0.2.1 -all"
  - 送信サーバの IP アドレスは 192.0.2.1



- 受信サーバで SPF 認証
  1) SMTP コネクションから相手の IP アドレスを得る
  2) SMTP MAIL FROM からドメイン名を取り出す
  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

SPF の宣言

- 限定子
  - "+" → pass
    - 受信許可
- "all" の限定子
  - "?" → neutral
    - SPF RR がないことと同等
  - "~" → softfail
    - neutral と fail の中間
  - "-" → fail
    - 受信拒否
- 宣言の例
  - example.jp IN TXT "v=spf1 +ip4:192.0.2.1 -all"
  - exmaple.jp IN TXT "v=spf1 +a +mx ~all"
    - 間接参照
  - exmaple.jp IN TXT "v=spf1 -all"
    - Web のみ

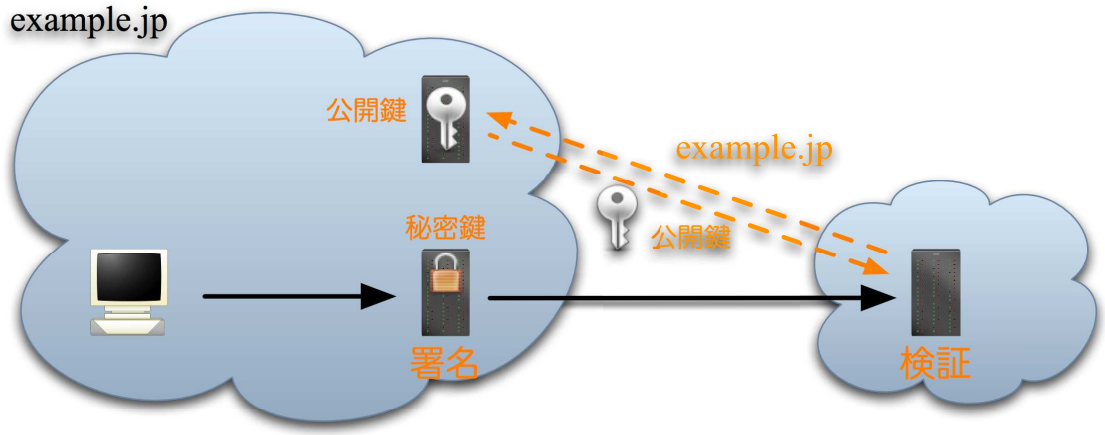
DKIM の署名

- Yahoo! と Cisco が提唱
  - 2つのプロトコルをマージ
    - Yahoo! DomainKeys
    - Cisco Identified Internet Mail (IIM)
- 署名の対象はヘッダと本文
  - 署名はヘッダに挿入される

```
DKIM-Signature: a=rsa-sha1; c=simple; d=example.jp; s=test;
 t=1137157317; x=1137762117; i=alice@example.jp; q=dns;
 h=DomainKey-Signature:Received:DKIM-Signature:
 DomainKey-Signature:Received:Message-ID:Date:From:Organization:
 User-Agent:MIME-Version:To:Subject:References:In-Reply-To:
 Content-Type:Content-Transfer-Encoding:Reply-To;
 b=ktdmQPIrkLGajBALhScj7I+Mx+h6uPBRxrcWm4pcW6bc8OwJTFdl9
 4LddNDq+iDGfT3m3Awe6j+Um2LIxpc0ET1dny0ut42H98I40C5QnjTo9
 8AahlUYkKeKXQZhTwU2PraJMBXFm8=
```

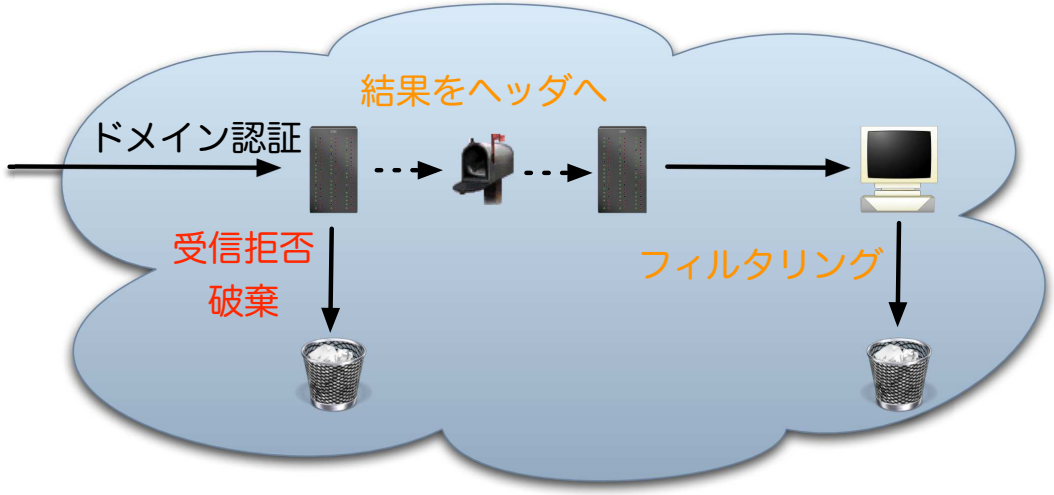
- DNS を利用
  - 公開鍵を DNS で配布
  - 認証局(CA)は不要

DKIM の動作



- 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

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.com
    from=alice@example.jp; spf=fail
  - 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
  - 受信サーバは認証結果が「詐称」なら受信拒否

ドメイン認証の普及率の測定

- WIDE プロジェクトと JPRS の共同研究
  - 2006年2月現在
  - SPF = 2.4%
  - DKIM = 0.0 %

登録型	登録数	MX	SPF	DK
AD(JPNIC会員)	297	251	18	1(3)
AC(大学系教育機関)	3254	3048	89	0(1)
CO(一般企業)	284729	264201	10149	6(12)
GO(政府機関)	836	718	24	0(1)
OR(会社以外の団体)	21151	19694	726	3(6)
NE(ネットワークサービス)	17291	13248	342	2(5)
GR(任意団体)	8908	7523	372	2(4)
ED(小・中・高校など主に18歳未満を対象とする各種学校)	4394	3967	71	0(0)
地域型(都道府県名、政令指定都市名、市町村名)	3768	3194	48	1(2)
汎用JPドメイン	445526	296777	2919	8(55)
合計	792622	613587	14760	23(89)

  - http://member.wide.ad.jp/wg/antispam/stats/

SPF

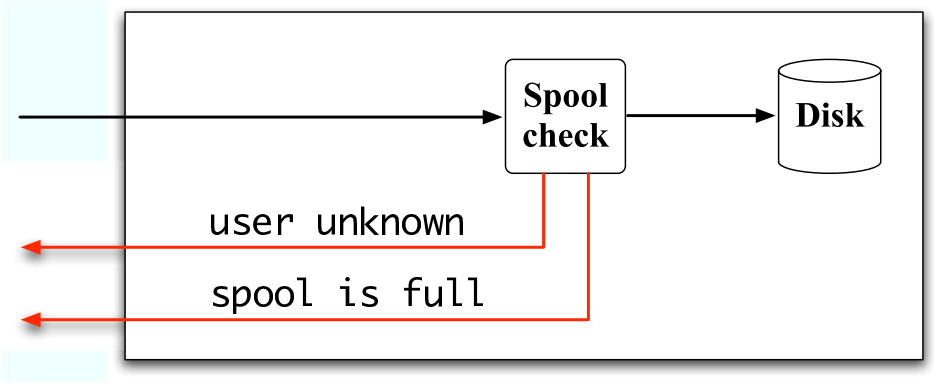
SPF の普及に関する問題

- 移行の初期
  - 導入のメリットが少ない
  - 宣言を失敗するとメールを受け取ってもらえなくなる？
  - 心理的な障壁がある
- 悪循環
  - 普及していないと導入できない
  - 導入するドメインが増えないので普及しない
- 好循環へ
  - 導入のメリットを出す必要がある

エラーメールと SPF

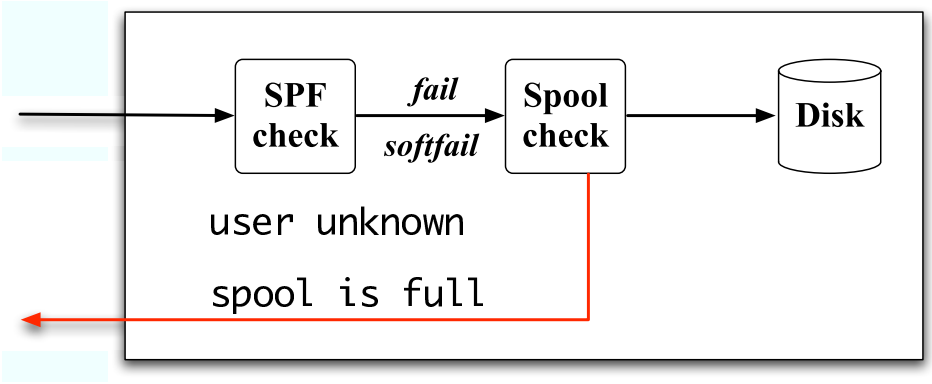
- SPF をエラーメールの低減に活用
- ほとんどのエラーメールは無駄
  - ハーベスティング攻撃
  - ウイルス
  - アンチウイルス製品
- 以下の条件のときは、エラーメールを返さない
  - 宛先不明 (user unknown)
  - SPF 認証の結果、送信元が「詐称」 (fail / softfail)
- 提案 (1a)
  - softfail の意味を
    「受信はするがエラーメールは返さなくてよい」
    とする
  - 送信側は "~all" (softfail) と宣言する

エラーメール



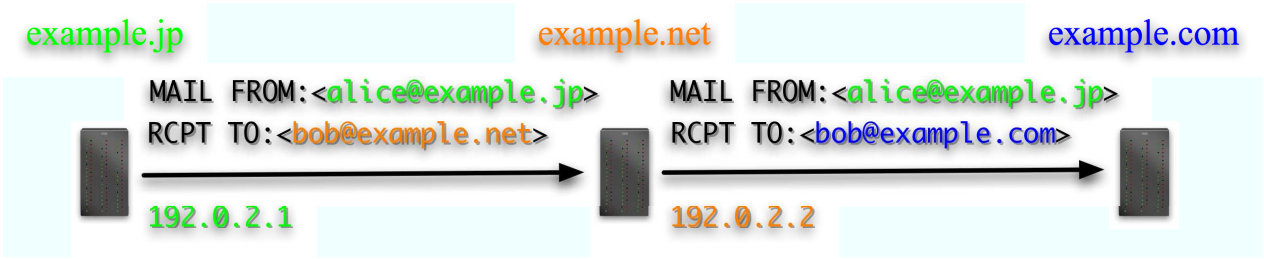
- 自分自身でエラーメールを返すサーバ
  - 多くの ISP の受信サーバ
  - ハーベスティング攻撃を防止するため

SPF によるエラーメールの低減



- 提案 (1b)
  - 以下の両方を満たす場合、エラーメールを生成しない
  - SPF 認証が fail または softfail
  - user unknown
- 好循環へ
  - SPF RR で "~all" と宣言すれば、
    受け取る不要なエラーメールが減る

SPF と転送

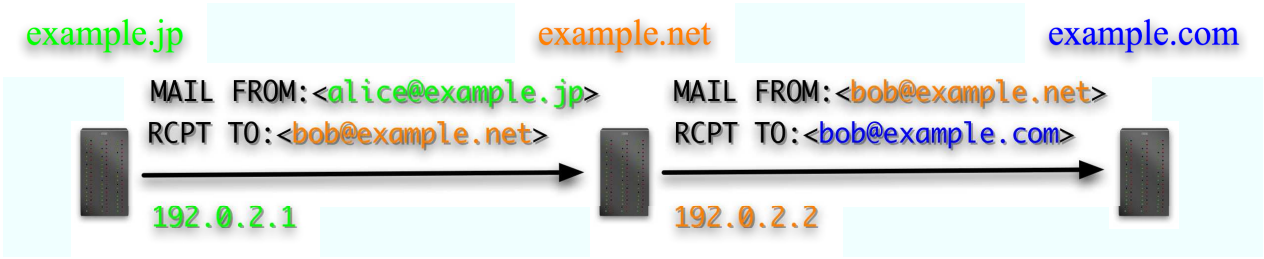


- 転送によって、IP アドレスが変わる
- SPF 認証の結果は、常に「詐称」
  - "~all" なら softfail
  - "-all" なら fail

解決方法への要求

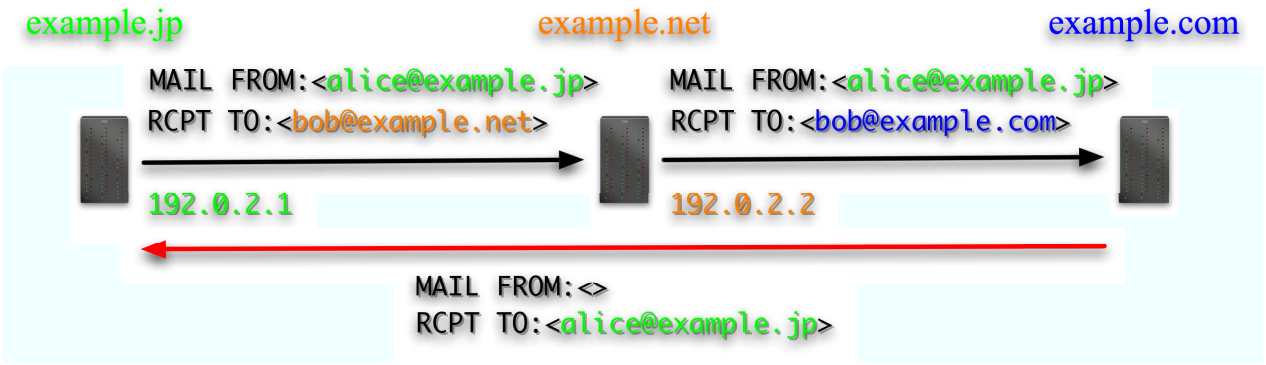
- これまで提案された解決方法
  - SUBMITTER
    - MAIL FROM: <alice@example.jp> SUBMITTER=bob@example.net
  - SRS
    - MAIL FROM: <alice#example.jp@example.net>
- SMTP の書式を変更する必要があると普及しない
  - 転送元だけでなく転送先も対応する必要がある
- 解決方法への要求
  - SMTP の書式を変更してはならない

MAIL FROM の上書き



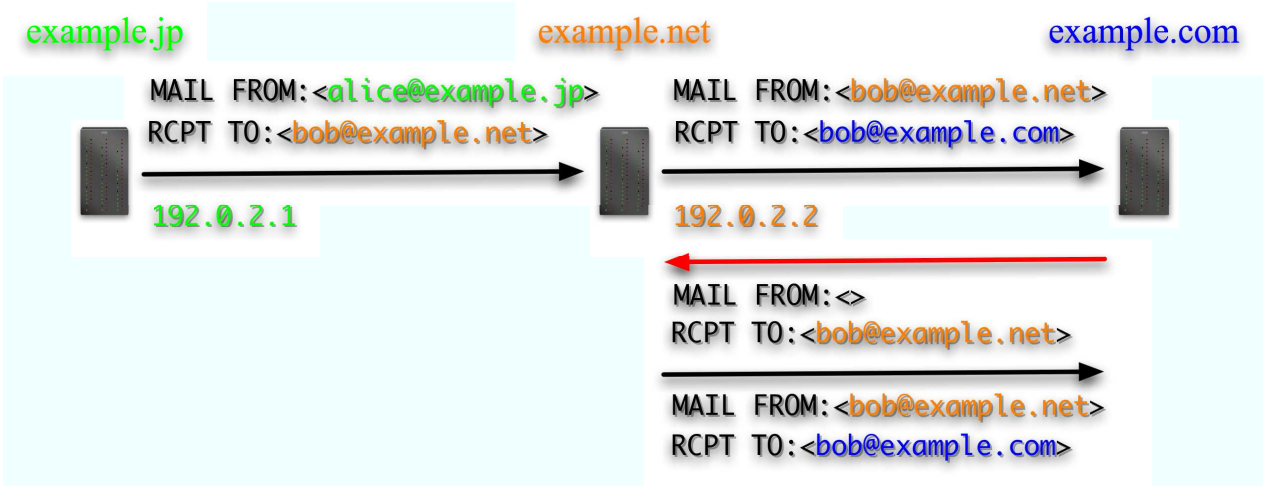
- 提案 (2)
  - MAIL FROM を書き換える
- 利点
  - SPF 認証の結果は「本物」(pass)になる
  - SMTP の書式に変更はない
  - 転送元だけが対応すればよい

転送とエラー



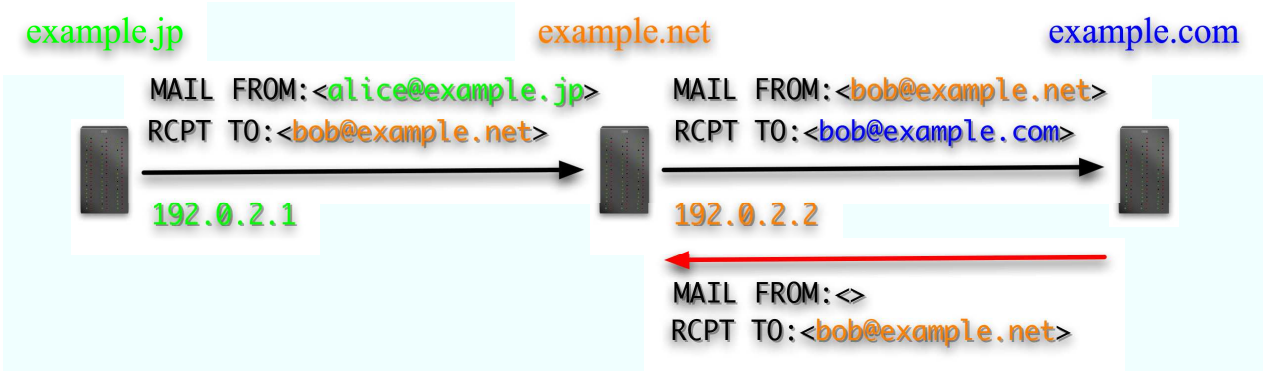
- 今までは(提案 (2) に未対応なら)
  エラーメールは送信者へ返る

エラーメールのループ



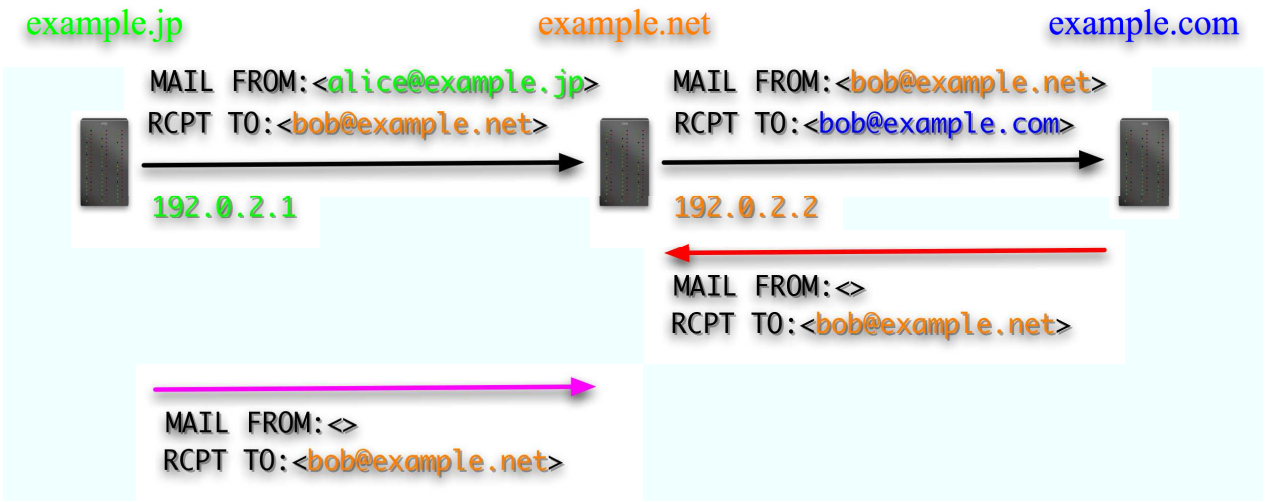
- 提案 (2) により、エラーメールの意味が変わる
  - エラーメールは、送信者ではなく、転送者へ戻る
- エラーメールがループする
  - SPF の仕様書 9.3 章では、考察がここまで

ループの防止案(2a)



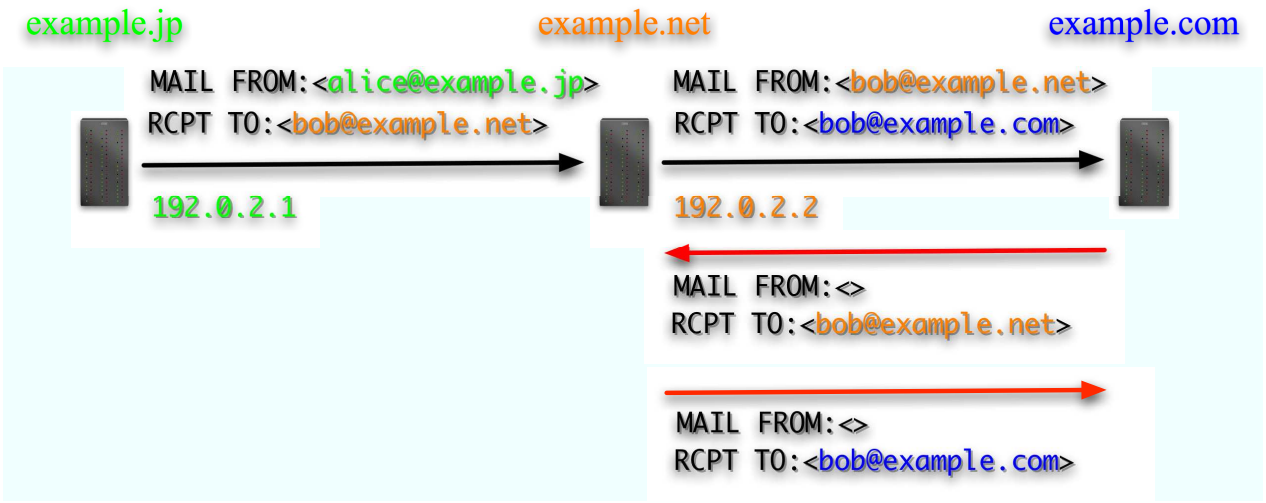
- 提案 (2a)
  - 転送元は、エラーメールをローカルスプールへ
  - 転送によるエラーメールがループしなくなる

ループの防止案(2a)の副作用



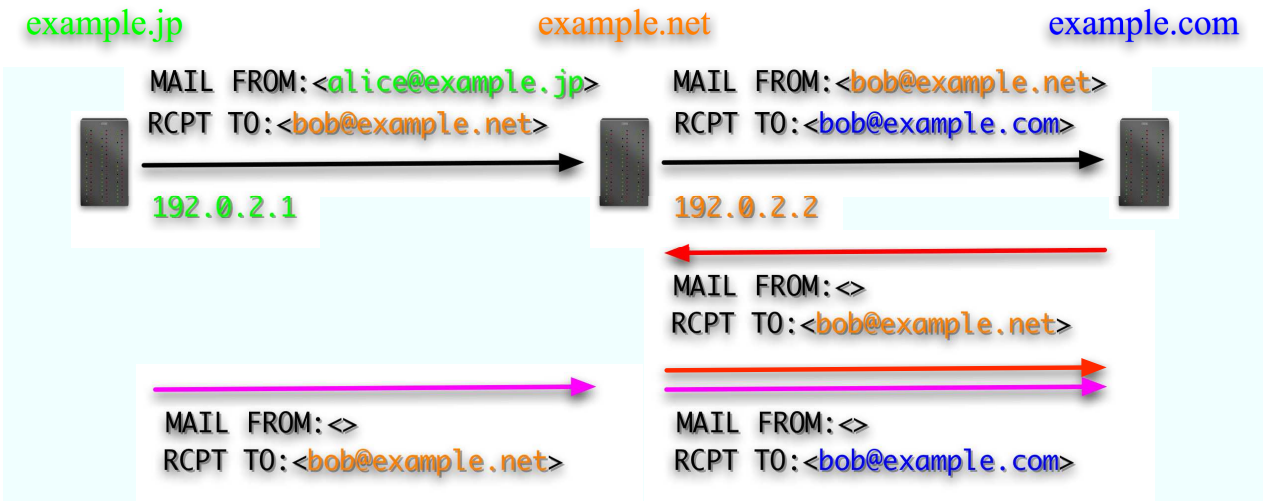
- すべてのエラーメールが影響を受ける
  - 長所) エラーメールは確実に残る
  - 短所) ユーザへの周知が必要
    ユーザの利便性を損なう

ループの防止案(2b)



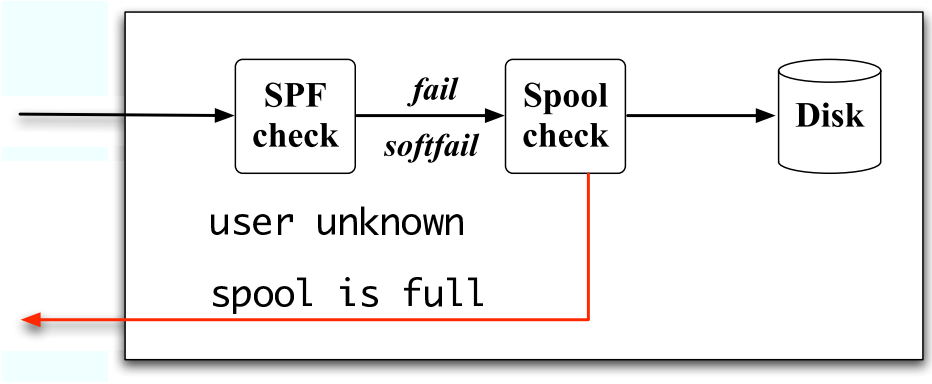
- 提案 (2b)
  - 転送元は MAIL FROM を "<>" のまま転送
  - 転送先でさらなるエラーメールは発生しない

ループの防止案(2b)の副作用



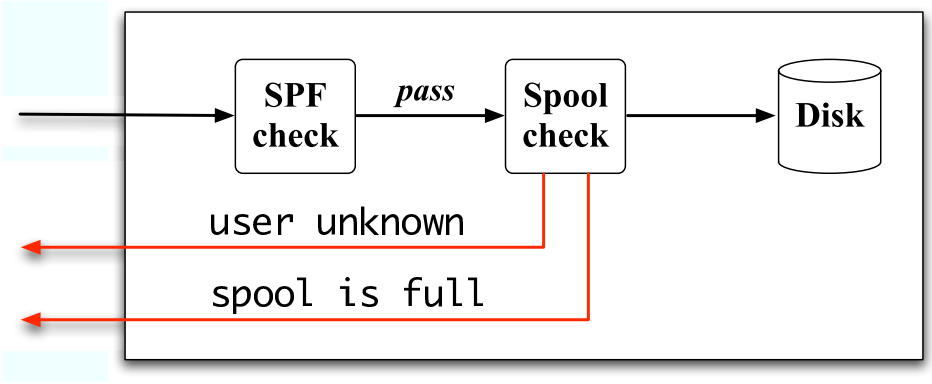
- すべてのエラーメールは、転送される
  - 長所) ユーザの利便性を維持
  - 短所) 転送先が受け取った後、エラーが発生すると、
    すべてのエラーメールがなくなる
    エラーの発生を送信者も転送者も知ることができない

転送とエラーメール(1)



- 転送元が提案 (2) に未対応
  - SPF 認証の結果は「詐称」
  - スプール溢れの場合は、エラーメールが返る
  - 宛先不明の場合は、返らない
    - 転送の設定自体が誤り

転送とエラーメール(2)



- 転送元が提案 (2) に対応
  - SPF 認証の結果は「本物」
  - スプール溢れの場合は、エラーメールが返る
    - 転送元が (2a) を採用しているなら、エラーメールは転送元のスプールへ
    - 転送元が (2b) を採用しているなら、エラーメールはなくなる
      エラーメールを犠牲にする
  - 宛先不明の場合は、エラーメールが返る
    - 転送元が (2a) を採用しているなら、エラーメールは転送元のスプールへ
    - 転送元が (2b) を採用しているなら、エラーメールはなくなる
      転送の設定自体が誤り

SFP の普及のストーリー

- 普及前期
  - 受信側：SPF 認証の結果をヘッダに残す
    - メールは必ず受信
  - 送信側：SPF RR で "~all" を宣言 (提案1a)
  - 受信側：Softfail/fail ならエラーメールを返さない (提案1b)
    - エラーメールが減るというメリットが出る
  - 転送元：MAIL FROM を書き換える方法へ移行 (提案2)
    - SPF と転送の相性問題を解決 (提案 2a, 2b)
    - ユーザごとに選択可能
- 普及前期
  - 受信側：SPF 認証の結果を受信に反映
    - "Fail" なら受信拒否
    - "Softfail" なら受信
  - 送信側："~" → "-"

まとめ

検討項目

- Submission と OP25B
  - 投稿ポートとユーザ認証(SMTP AUTH)を用意しましょう
  - OP25B の導入を検討しましょう
- SPF
  - 送信側として SPF RR を宣言しましょう
    - 最初は "~all"
  - 受信側では、SPF の検証結果をヘッダに残すようにしましょう
  - SPF の検証結果が fail/softfail で、
    uknown user のメールには、
    エラーメールを返さないようにしましょう
- DKIM
  - DKIM の導入を考えましょう
  - 受信側では、DKIM の検証結果をヘッダに残すようにしましょう

参考サイト

- IAjapan ポータルサイト
  - http://www.iajapan.org/anti_spam/portal/
- JEAG
  - http://www.jeag.jp/
- WIDE antispam WG
  - http://member.wide.ad.jp/wg/antispam/