迷惑メールの低減に向けて

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

- 迷惑メールあれこれ
- ゾンビ対策
- メールを追跡可能に

携帯電話と迷惑メール

宣伝メール配信にもっとも強力な新製品が出ました！！

携帯による携帯メール自動送信システム発売！！

ドメイン指定拒否されていても届きます。(悪用厳禁！)

AU by KDDI(CDMA)携帯電話1〜20台接続型
通常価格2,300,000円を 特別価格898,000円
内容:送信システムインストール済PC1本体(モニタ別)+携帯接続ケーブル10本(追加ケーブル1本3980円)

AU by KDDI(CDMA)携帯電話1〜5台接続型
通常価格1,800,000円を 特別価格498,000円
内容:送信システムインストール済PC1本体(モニタ別)、携帯接続ケーブル5本¥50000別売)

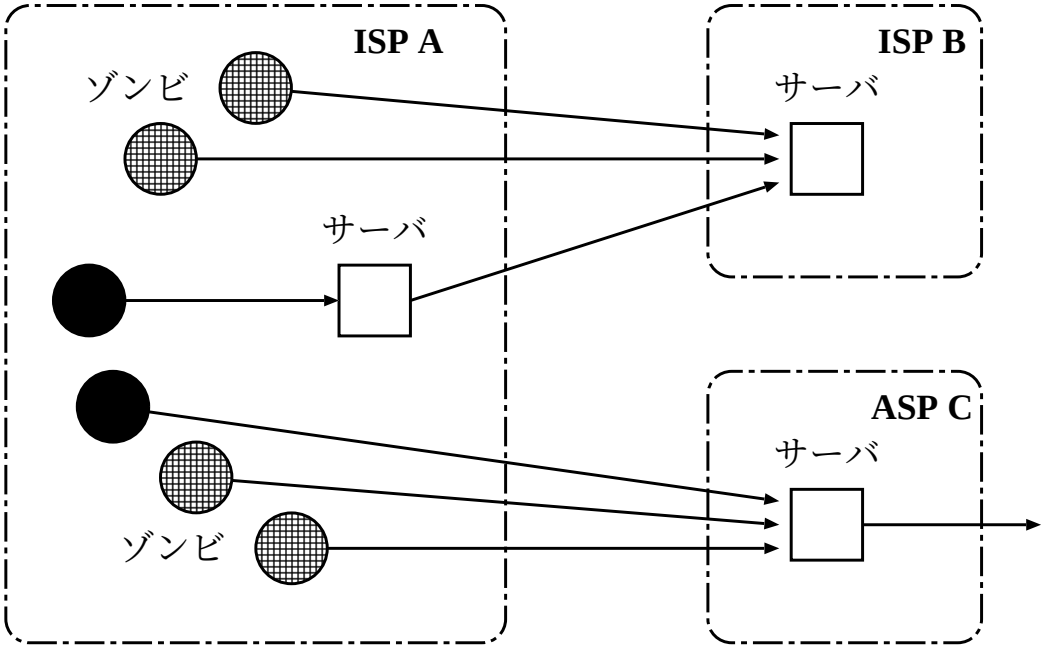
※お届けは入金後1~2週間程度になります。
他社AUシステムよりかなり安くて最も高速なメール配信システム！ ここでしか買えません！！
お電話はいますぐ！ 0909-5656-588 へどうぞ！！
メールなら info@hitbitweb.com
New! パケット定額WIN端末対応型完成！↓

インターネットと迷惑メール

- 携帯電話への迷惑メールは減少傾向にある
  - レート制御
  - 迷惑メール配送事業者の特定が容易
  - 迷惑メール追放支援プロジェクト
    - 総務省 ＋ 経済産業相
    - オトリを用意し、迷惑メールと判定
    - 約款の行使を後押し
- インターネットの迷惑メールは急増加
  - 昨年の夏に 10 倍になった
  - メールサーバを圧迫
- 問題点
  - 迷惑メール配送事業者の特定が困難
  - ゾンビによる大量のメール配信
  - メールアドレスの詐称によるフィッシング

ゾンビ

- **乗っ取られた PC を「ゾンビ」と呼ぶ**
  - **あるいは「Bot」**
  - **迷惑メール配送業者は、世界最大の分散コンピューティング環境を持っている**



フィッシング・メール (1)

UFJ銀行　こたえていくチカラ。

UFJ銀行ご利用のお客様へ

UFJ銀行のご利用ありがとうございます。
このお知らせは、UFJ銀行をご利用のお客様に発送しております。

この度、UFJ銀行のセキュリティーの向上に伴いまして、
オンライン上でのご本人確認が必要となります。

この手続きを怠ると今後のオンライン上での操作に支障をきたす恐れがありますので、一刻も素早いお手続きをお願いします。

https://www.ufjbank.co.jp/ib/login/index.html

また、今回のアップデートには多数のお客様からのアクセスが予想されサーバーに負荷がかかるため、下記のミラーサイトを用意しております。上記のリンクが一時期不可能になっている場合は、下記をご利用ください。

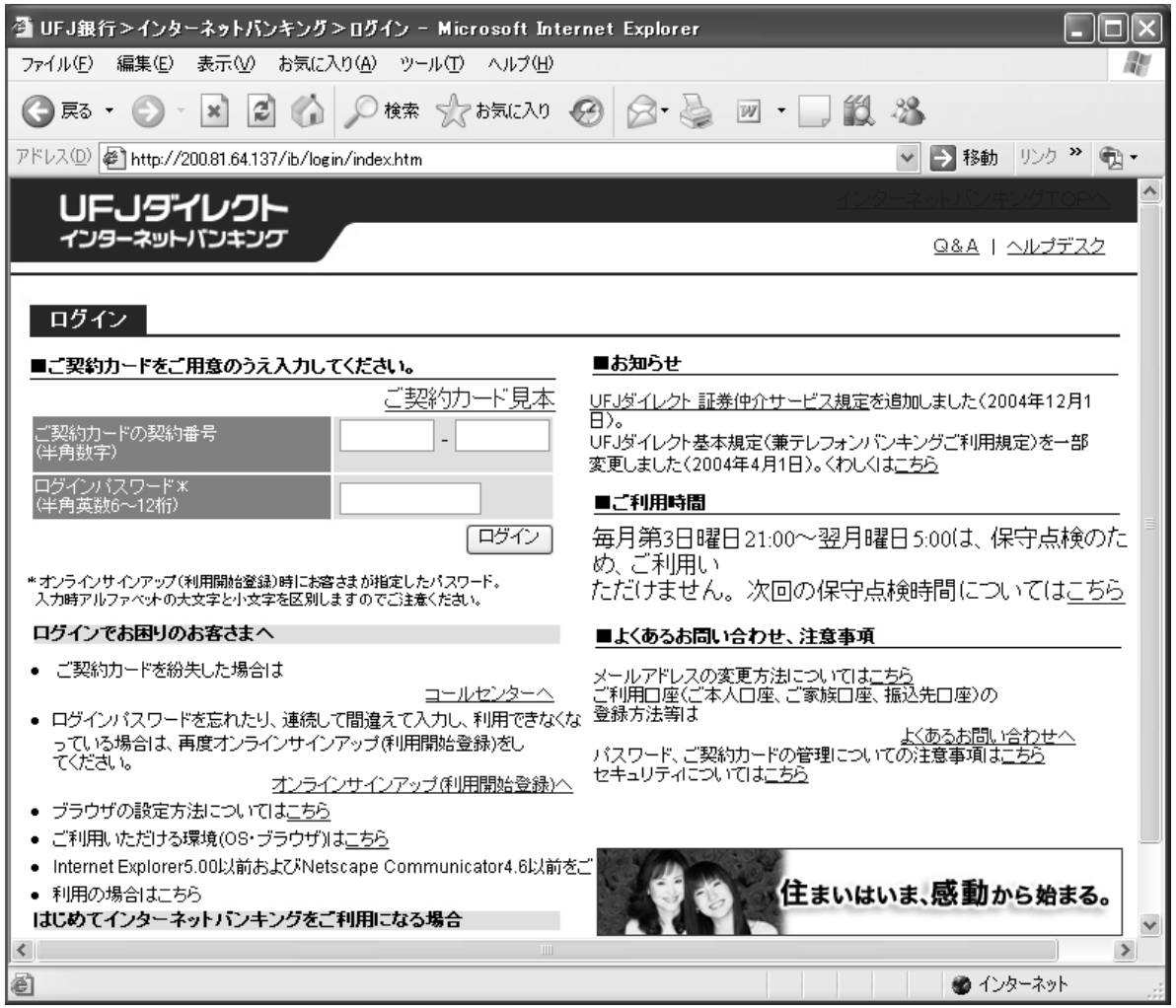
https://www.ufjbank.co.jp/ib/login/index2.html

https://www.ufjbank.co.jp/ib/login/index3.html

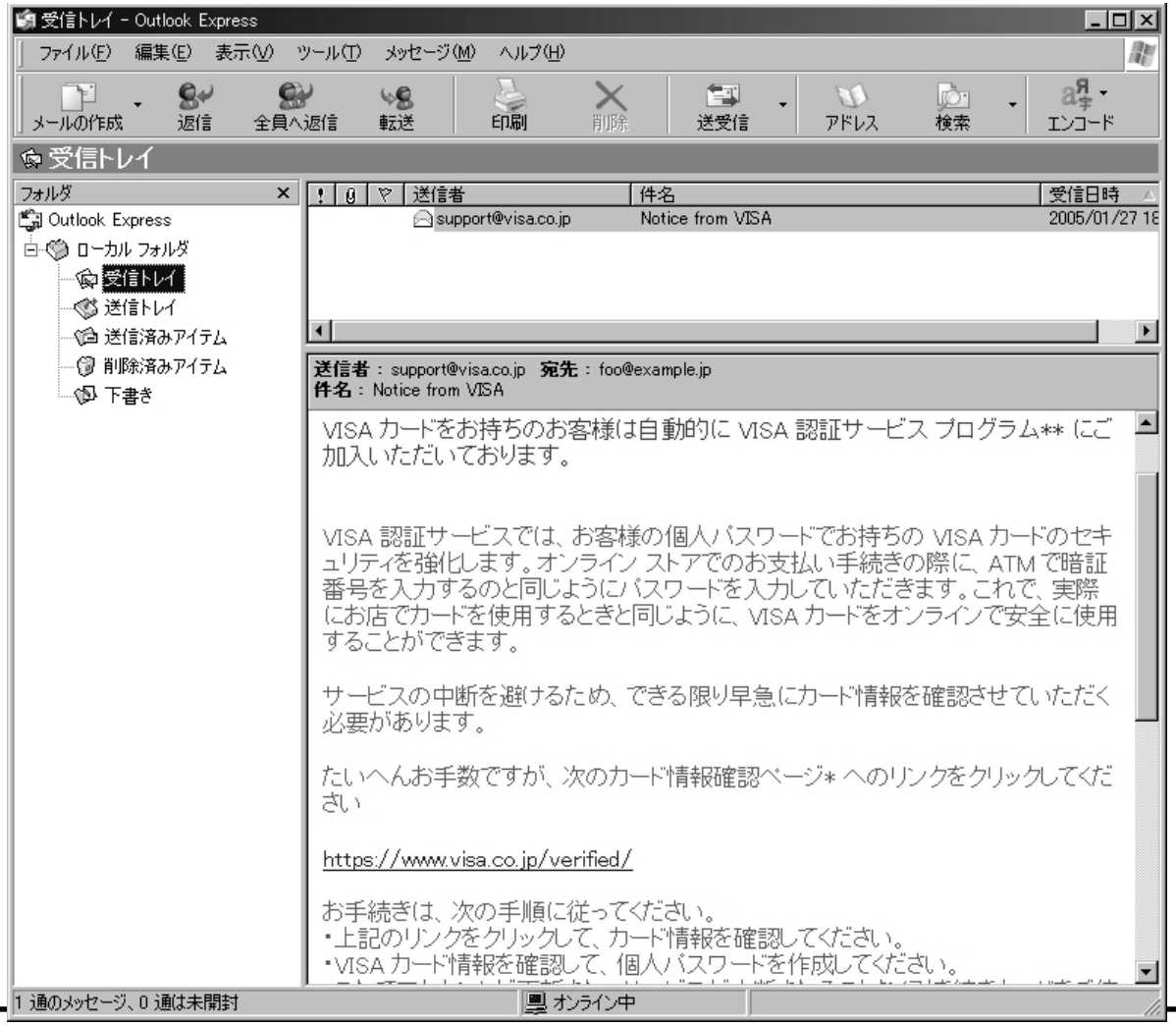
お客様のご協力とご理解をお願いいたします。

UFJ銀行

フィッシング・サイト (1)


UFJ銀行＞インターネットバンキング＞ログイン - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り
アドレス(D) http://200.81.64.137/ib/login/index.htm
移動 リンク
UFJダイレクト
インターネットバンキング
インターネットバンキングTOPへ
Q&A | ヘルプデスク
ログイン
■ご契約カードをご用意のうえ入力してください。
ご契約カード見本
ご契約カードの契約番号
(半角数字)
ログインパスワード*
(半角英数6～12桁)
ログイン
*オンラインサインアップ(利用開始登録)時にお客さまが指定したパスワード。
入力時アルファベットの大文字と小文字を区別しますのでご注意ください。
ログインでお困りのお客さまへ
ご契約カードを紛失した場合は
コールセンターへ
ログインパスワードを忘れたり、連続して間違えて入力し、利用できなくなっている場合は、再度オンラインサインアップ(利用開始登録)をしてください。
オンラインサインアップ(利用開始登録)へ
ブラウザの設定方法についてはこちら
ご利用いただける環境(OS・ブラウザ)はこちら
Internet Explorer5.00以前およびNetscape Communicator4.6以前をご
利用の場合はこちら
はじめてインターネットバンキングをご利用になる場合
■お知らせ
UFJダイレクト 証券仲介サービス規定を追加しました(2004年12月1日)。
UFJダイレクト基本規定(兼テレフォンバンキングご利用規定)を一部変更しました(2004年4月1日)。くわしくはこちら
■ご利用時間
毎月第3日曜日21:00～翌月曜日5:00は、保守点検のため、ご利用いただけません。次回の保守点検時間についてはこちら
■よくあるお問い合わせ、注意事項
メールアドレスの変更方法についてはこちら
ご利用口座(ご本人口座、ご家族口座、振込先口座)の登録方法等は
よくあるお問い合わせへ
パスワード、ご契約カードの管理についての注意事項はこちら
セキュリティについてはこちら
住まいはいま、感動から始まる。
インターネット

フィッシング・メール (2)


受信トレイ - Outlook Express
ファイル(F) 編集(E) 表示(V) ツール(T) メッセージ(M) ヘルプ(H)
メールの作成 返信 全員へ返信 転送 印刷 削除 送受信 アドレス 検索 エンコード
受信トレイ
フォルダ
Outlook Express
ローカル フォルダ
受信トレイ
送信トレイ
送信済みアイテム
削除済みアイテム
下書き
送信者 件名 受信日時
support@visa.co.jp Notice from VISA 2005/01/27 18
送信者 : support@visa.co.jp 宛先 : foo@example.jp
件名 : Notice from VISA
VISA カードをお持ちのお客様は自動的に VISA 認証サービス プログラム** にご加入いただいております。
VISA 認証サービスでは、お客様の個人パスワードでお持ちの VISA カードのセキュリティを強化します。オンライン ストアでのお支払い手続きの際に、ATM で暗証番号を入力するのと同じようにパスワードを入力していただきます。これで、実際にお店でカードを使用するときと同じように、VISA カードをオンラインで安全に使用することができます。
サービスの中断を避けるため、できる限り早急にカード情報を確認させていただく必要があります。
たいへんお手数ですが、次のカード情報確認ページ* へのリンクをクリックしてください
https://www.visa.co.jp/verified/
お手続きは、次の手順に従ってください。
・上記のリンクをクリックして、カード情報を確認してください。
・VISA カード情報を確認して、個人パスワードを作成してください。
1 通のメッセージ、0 通は未開封
オンライン中

フィッシング・サイト(2)


「VISA認証サービス」 - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り
アドレス(D) http://62.231.95.161/verified/
移動 リンク
https://www.visa.co.jp/verified/
日本 Japan
検索
安全なオンラインショッピング
VISA
VISAさえあれば
安全なオンラインショッピング／ホーム
VISAカード会員の方へ
VISA加盟店の方へ
ホーム
カードのお申し込み
お得なキャンペーン <VISA e-mailclub>
安全なオンライン ショッピング
プラチナカードの特典・サービス
カードの紛失・盗難
カードご利用のヒント
プレス・センター
VISAについて
VISA TV コマーシャル
VISA法人カード
VISAのICカードへの取り組み
AIS について
このサイトは、高度な SSL (Secure Socket Layer) 暗号化技術を利用しており、個人情報が閲覧、傍受または改ざんされることはありません。
VERIFIED by VISA
VISA認証サービス
VISA 認証サービス Web サイトで入力されたカード番号情報は、本サービスを開始することを目的として、お客様の VISA カードの発行元金融機関および処理機関に通知する場合を除き、使用または開示されることはありません。
以下のフォームに記入し、カードを登録してください。
カード番号:
カードの有効期限:
月 / 年
カード認証番号 (CVV):
ページが表示されました
インターネット

フィッシング 110 番

- フィッシングの相談窓口
  http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm
- すぐに警察が動ける
  - 業務妨害罪
  - 著作権法違反
- 特定電子メール送信適正化法では？
  - 警告メールの送信 → 措置命令の発出
  - 措置命令の発出は、3年間で 3 件
  - 2005年5月 問題点を改訂
    - SMTP のみ → SMS も含む
    - 未承諾広告のみ → 空メールも含む
    - 個人宛のみ → 業務用 ML も含む
    - 措置命令 → 送信者を偽造した場合の直罰
  - 2005年6月 初の業務停止命令 (2件)

コンテンツ・フィルタ

- メールの内容から迷惑メールか判断
  - 単語の統計を取る
    - アダルト関連の用語
    - 強壮剤関連の用語
    - サイトへのリンク

Subject: **白姫女子校保健室からのおしらせ**
From: **県立白姫女子校保険室**

この前の妊娠検査について
県立白姫女子高校保健室からのお知らせです。

間違って受け取った方は、
お手数ですが、破棄してください。
お詫び致します。

該当する人は
下記リンクより入ってお知らせを確認して下さい。

http://just-feed.net/shirahime/?m9xDi8OM2U18v6troZOMN8xluEhWd4BwN7

法律

- **日本国憲法** (21**条**2**項**)
  検閲は　これをしてはならない
  通信の秘密は、これを侵してはならない
- **電気通信事業法**
  3**条：電気通信事業者の取扱中に係る通信は、**
  検閲してはならない
  4**条：電気通信事業者の取扱中に係る通信の秘密は、**
  侵してはならない
- **フィルタリングは検閲**
  - ISP **にとって、標準でフィルタリング・サービスを**
    提供するのは違反
  - **ユーザの同意が必要**

コンテンツ・フィルタの限界

- **出会い系サイトへの誘導**

  Subject: **あのぉ・・・**
  From: **黒川京子**

  黒川ですけど、
  何も書いてないメールくださいましたよね？
  念のために返信しますが、どちらさまでしょうか？
  知人のいたずらですか？

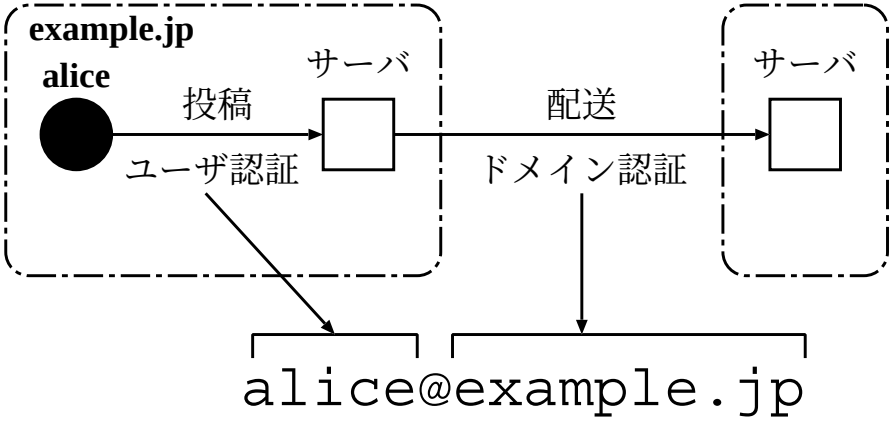
  Subject: **あの～**
  From: **井上知美**

  メールくれましたよね？
  最初は迷惑メールかと思ってたんだけど
  よく見たらそんな変なアドレスじゃないので
  メール返してみたんですが、
  以前どちらかのチャットか何かでお話したかたですか？？

- **コンテンツ・フィルタは対症療法**

メールを追跡可能に

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

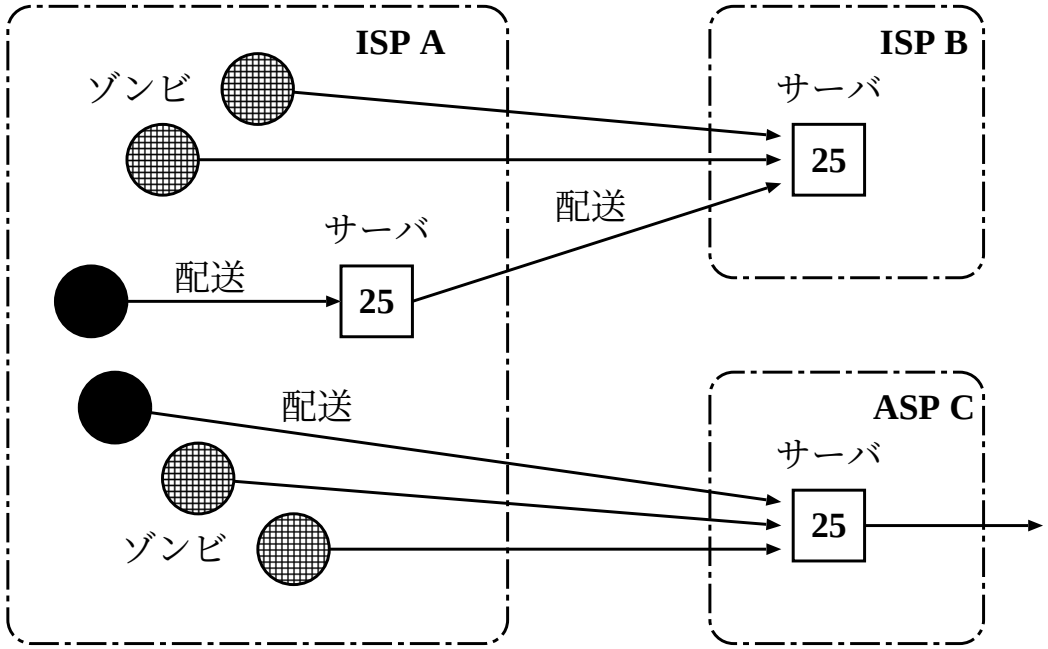


- メールアドレスを詐称できない世界
  - 迷惑メールを受け取ったら、そのドメインの管理者へ文句を言えばよい

注意

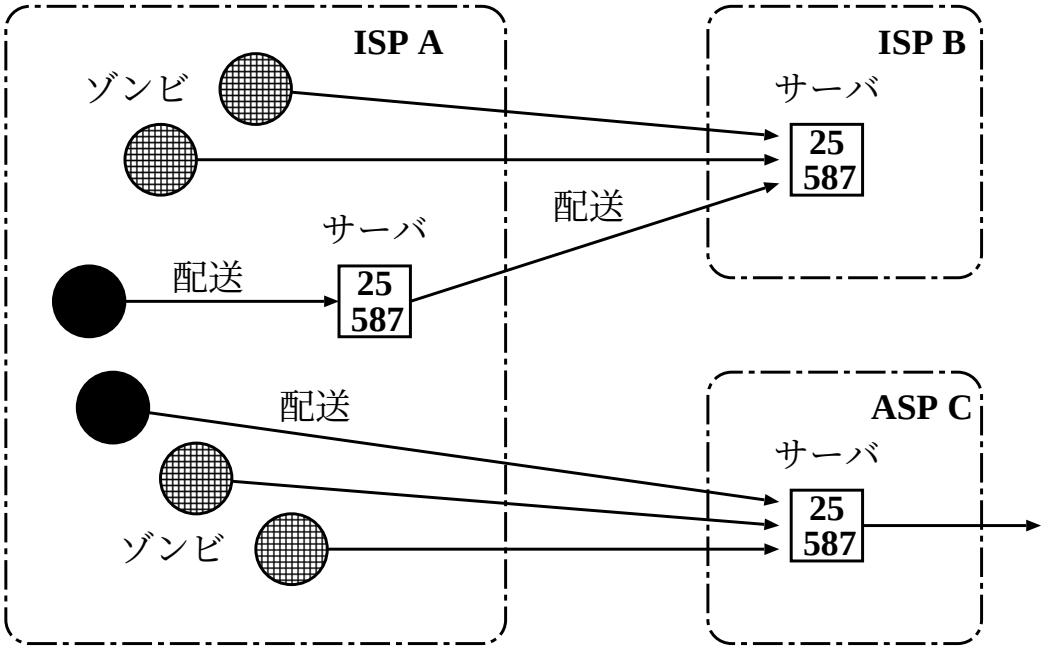
- ISP/ASP のメール管理者の「共通理解」
- 内容はあくまで理想論
  - すべての ISP/ASP が、すべてを実現できる訳ではない
    - 政治的な理由
    - 技術的な理由
    - 経済的な理由
- インターネットのあるべき姿は？
  - ユーザに自由を与えるが、責任も課す？
  - ユーザの自由を制限するが、安全なサービスを提供する?

問題点



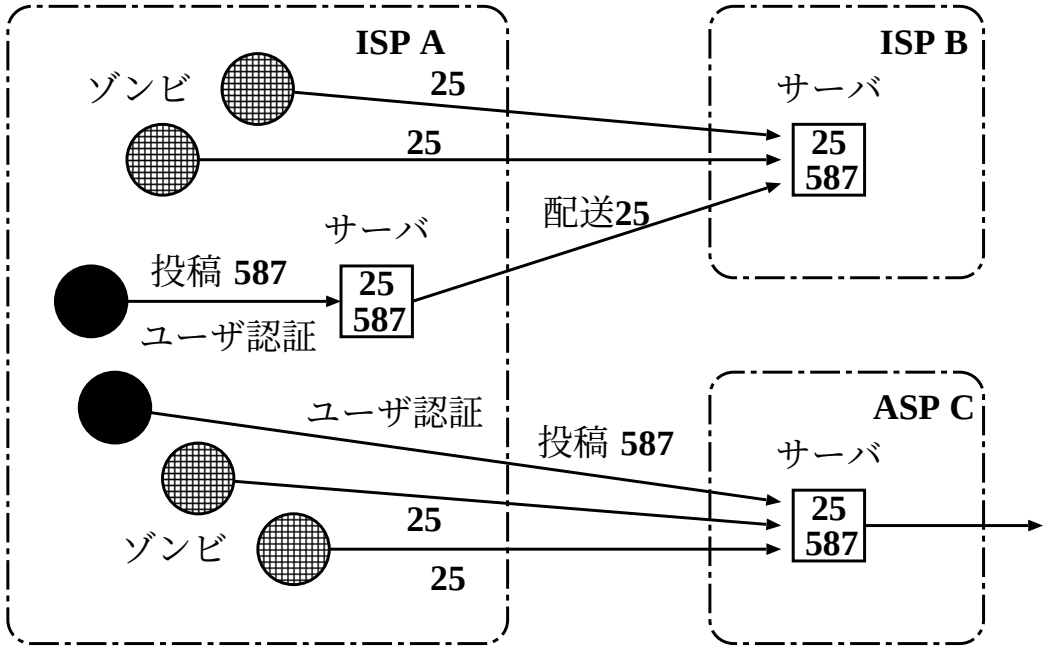
- ゾンビ(bot)による迷惑メールの大量送信
- メールアドレスの詐称
  - メールの追跡が困難
  - フィッシング

投稿ポートの提供



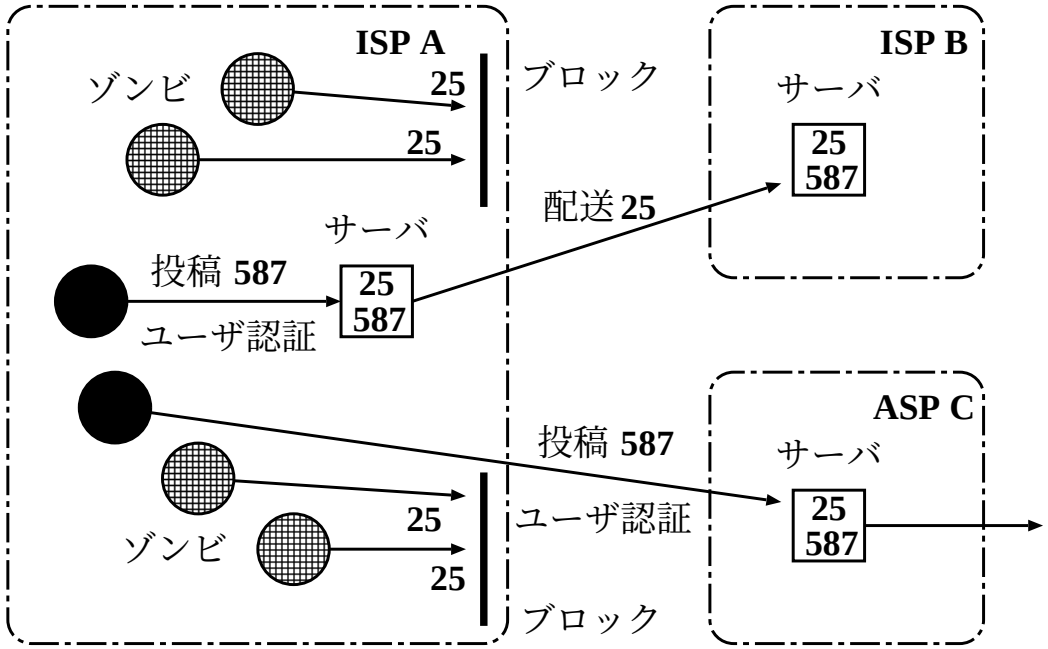
- **配送**
  - **ドメイン間の通信 (ポート** 25 **番)**
- **投稿**
  - **ユーザとそのドメイン間の通信 (ポート** 587 **番、**RFC 2476)
  - **プロトコル自体は** SMTP

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**
  - **現実的には、ドメイン内からのポート 25 番への配送も許可**
  - **ドメイン外からは、ポート 587 番のみ投稿を許可**

25番ポートのブロック

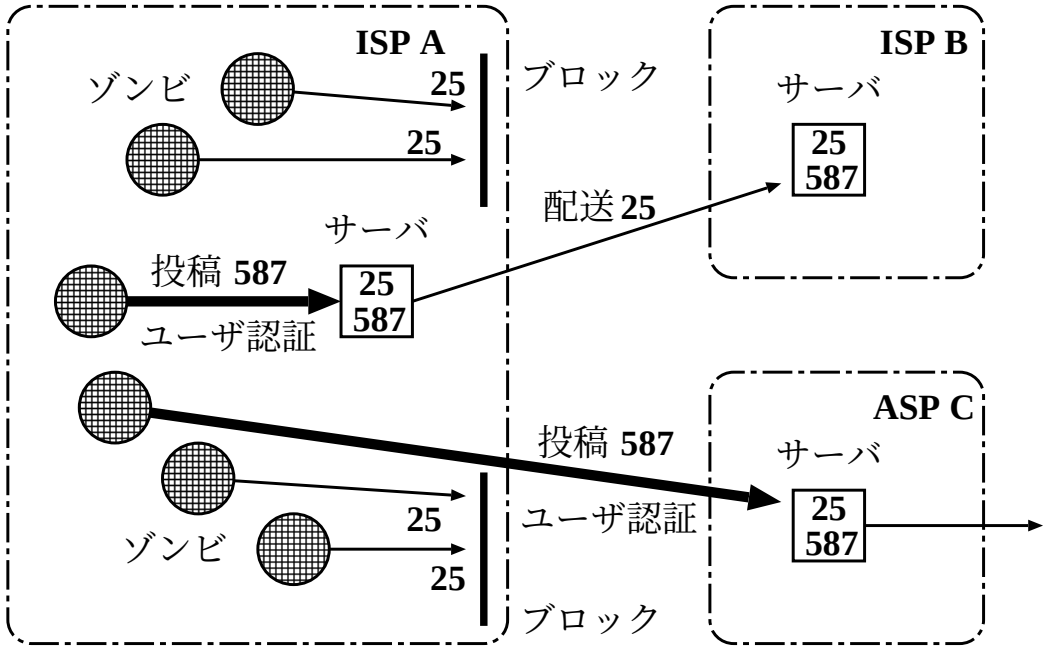


- ポート 25 番をブロックする
  - 追跡しにくい動的 IP からのみ
  - 固定 IP は受信側でブラックリストを作成できる
  - 独自にメールサーバを運用したい人は、固定 IP へ

25番ポートのブロックの導入実績

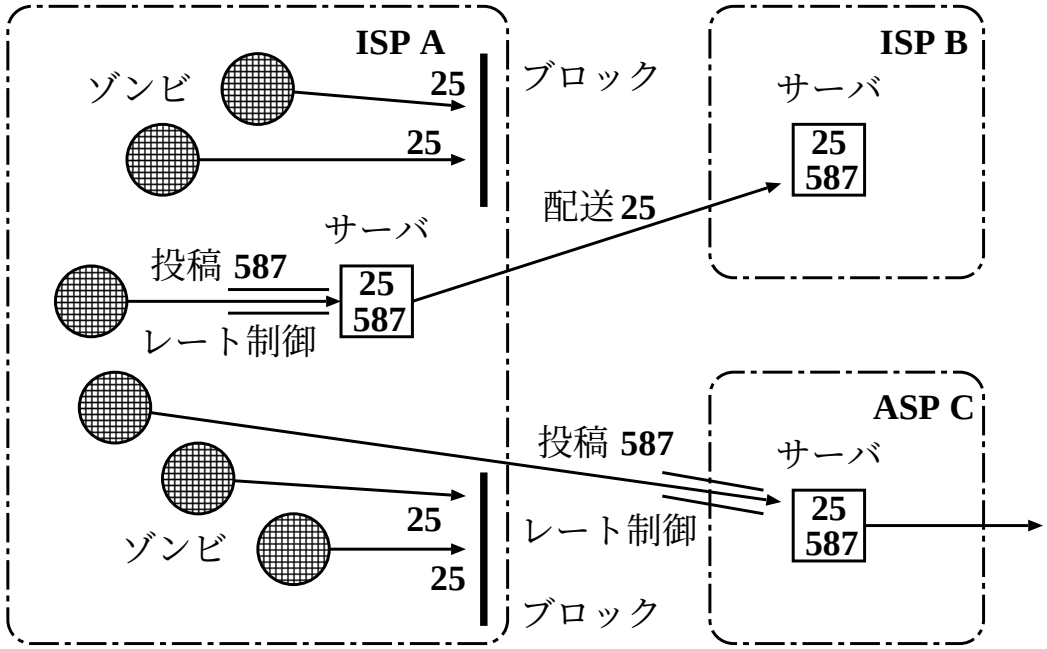
- **アメリカ**
  - AT&T、Bell CA、Bell South、Comcast
  - Earthlink、MSN、Verizon
  - **詳しくは**
    - http://www.postcastserver.com/help/Port_25_Blocking.aspx
- **日本**
  - **ぷららネットワークス**
    - http://www.plala.or.jp/access/living/releases/nr05_jan/0050127.html
    - **携帯事業社向け**
  - WAKWAK(NTT-ME)
    - http://www.wakwak.com/info/news/2005/port25blocking0107.html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

予想される新しい攻撃



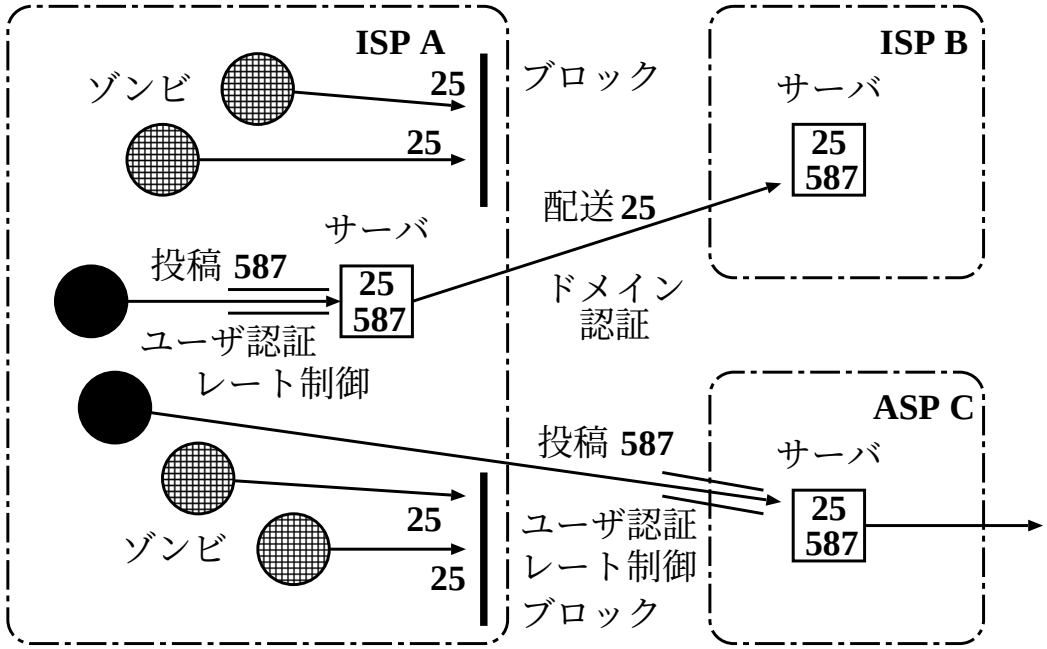
- パスワードを盗むゾンビが出現？
- 堂々と迷惑メールを投稿する配送業者

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

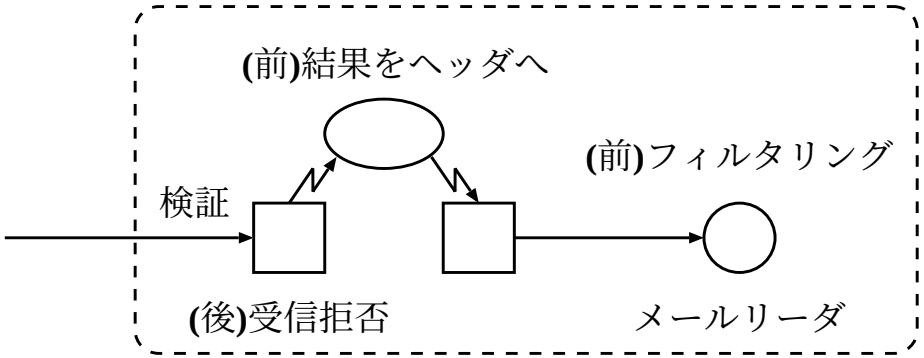


- 配送にはドメイン認証を必須にする
  - 本当にそのドメインの送信サーバから送られているか検査

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
    - DomainKeys と IIM は統合された
- 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

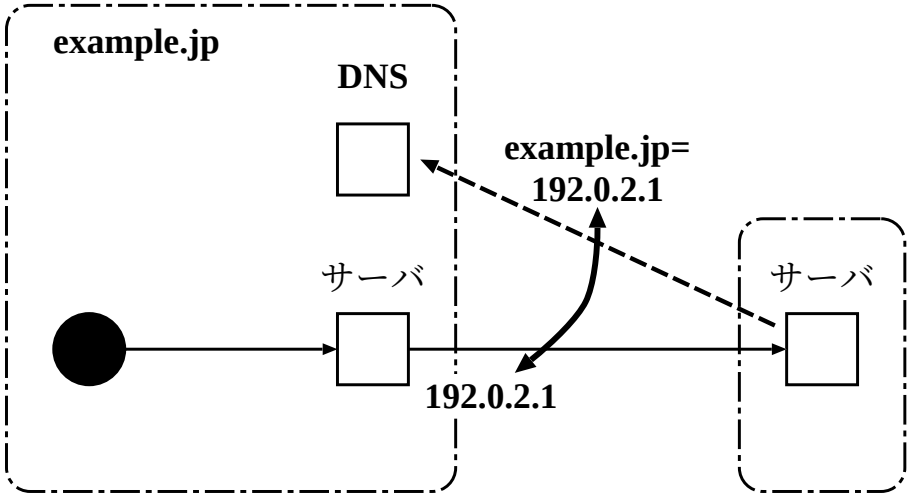
普及のストーリー



- 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**

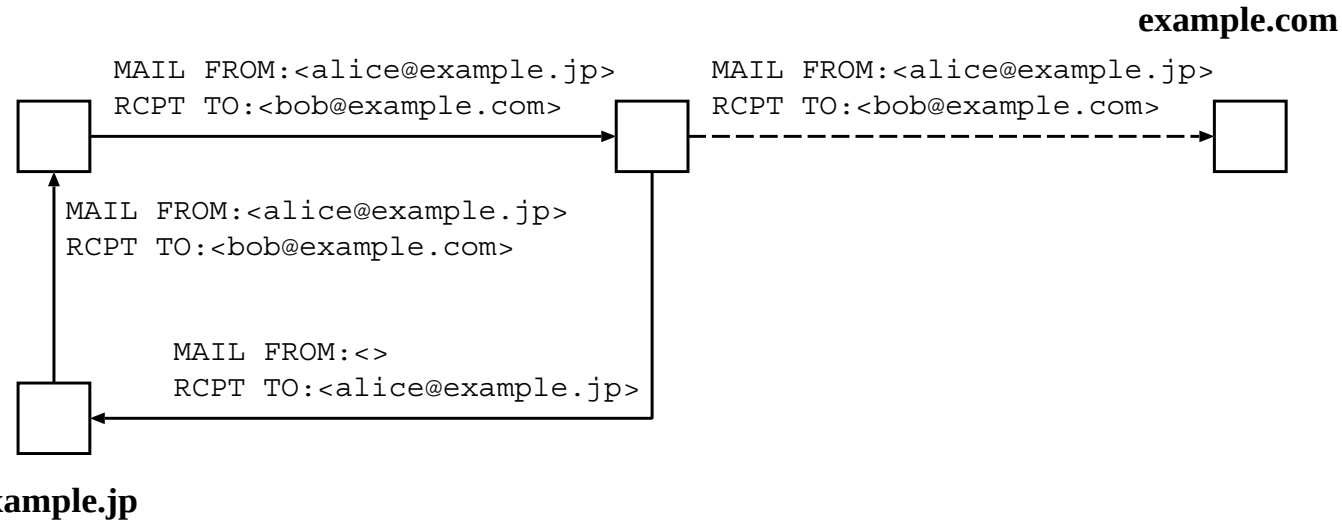
SPF (Sender Policy Framework)

- 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
  - "?" → neutral
  - "~" → softfail
  - "-" → fail
- **保護対象となるドメイン名は、**SMTP MAIL FROM

Sender ID

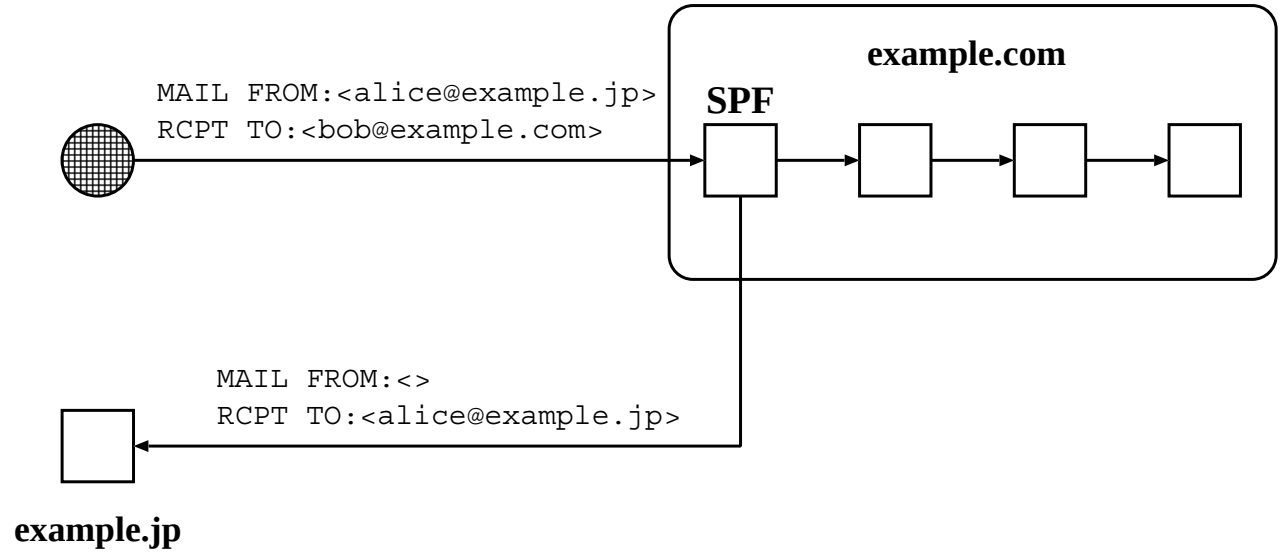
- IETF で SPF と Caller ID を統合
- 送信サーバの宣言は SPF と同様
  - example.com IN SPF "spf2.0/mfrom,pra +a +mx -all"
  - "v=spf1" は "spf2.0/mfrom,pra" と読み替える
- 保護対象となるドメイン名は
  - SMTP MAIL FROM (MFROM)
  - メールのヘッダ (PRA)
  - 受信者が選択する
- PRA =「責任があるとされるアドレス」
  - PRA(Purported Responsible Address) と呼ぶ
  - Resent-Sender:,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

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

SPF とエラーメール

- 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
- 内側で多段の検査
  - SPF の検査をし、検証失敗ならメールを捨てる

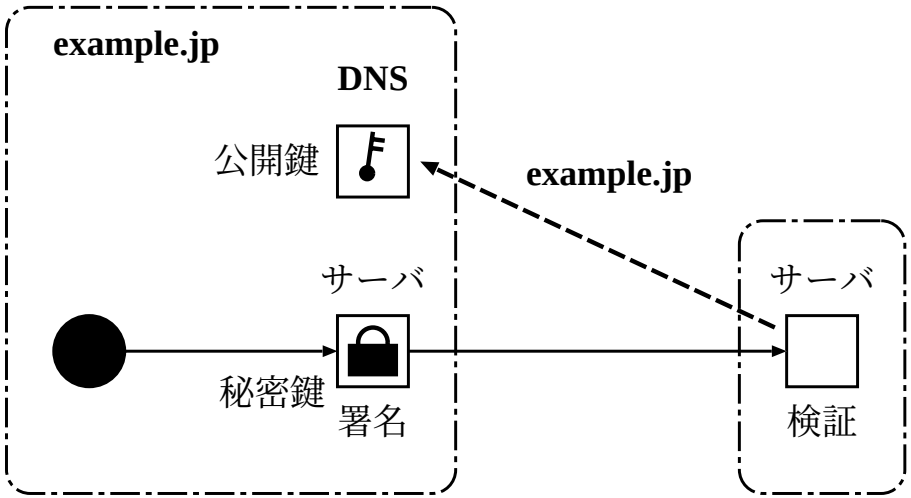


エラーメールの測定

- 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

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

署名の検証が失敗する原因

- DomainKeys 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 MTA
    - → 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

普及率の測定

- JPRS と WIDE プロジェクトの共同研究
- 2005年5月

http://jpinfo.jp/stats/

ゾーン	総数	MX	SPF	DK
汎用	361104	234123	389	23
AC	3166	2986	10	0
AD	299	255	6	1
CO	272223	252860	204	16
ED	4315	3894	0	0
GO	835	726	0	0
GR	9203	7832	13	0
LG	27223	1016	0	0
NE	17318	13222	66	8
OR	20088	18758	18	2
地域	4084	3381	8	2
合計	719858	539053	714	52

問題点と解決案

- 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、レピュテーションへ
  - どちらとも失敗なら、コンテンツ・フィルタへ

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り、ドメイン認証に対応して、迷惑メールを送る
- ドメインを評価するシステムが必要
  - レピュテーション (reputation) と呼ばれる
  - (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
  - 追跡可能なメールシステム
  - レピュテーション
  - コンテンツ・フィルタ