迷惑メールを低減するための技術と法的な位置づけ

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

- 最近の迷惑メール事情
- 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
- まとめ

最近の迷惑メール事情

迷惑メールの種類

- 未承諾広告
- 出会い系サイトへの誘導
- フィッシング
- なりすまし

未承諾広告

- あの手この手で注意を引こうとする

  Q. どうやってキリンを冷蔵庫に入れますか？

  A. 正解は「冷蔵庫の扉を開け、キリンをいれ、扉を閉じる」です。この質問ではあなたが単純なことを複雑な方法でしていないかどうかをテストしました。

  では次に

  Q. どうやって象を冷蔵庫に入れますか？

  A. 間違った答は「冷蔵庫の扉を開け、象を入れ、扉を閉じる」です。正解は「冷蔵庫の扉を開け、キリンを取り出し、象を入れ、扉を閉じる」です。
  この質問はあなたの記憶力を試しました。

  こんなたのしいことが沢山☆登録してからのお楽しみ☆
  http://www.meguriai-max.net/?j92

  拒否はこちら
  pp_info_0001@yahoo.ca

出会い系サイトへの誘導

- 日常会話から始まる

  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？

- 返答

  誰が送ったのかわからないのですが、
  そちらが何らかの悪意で送ったのではない、
  知人のいたずらとも思えない、
  ということで、何だか安心しました。
  実際のところ、どうして届いたのかは判明してないのですが。
  わざわざご返信ありがとうございました。

フィッシング・メール

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。

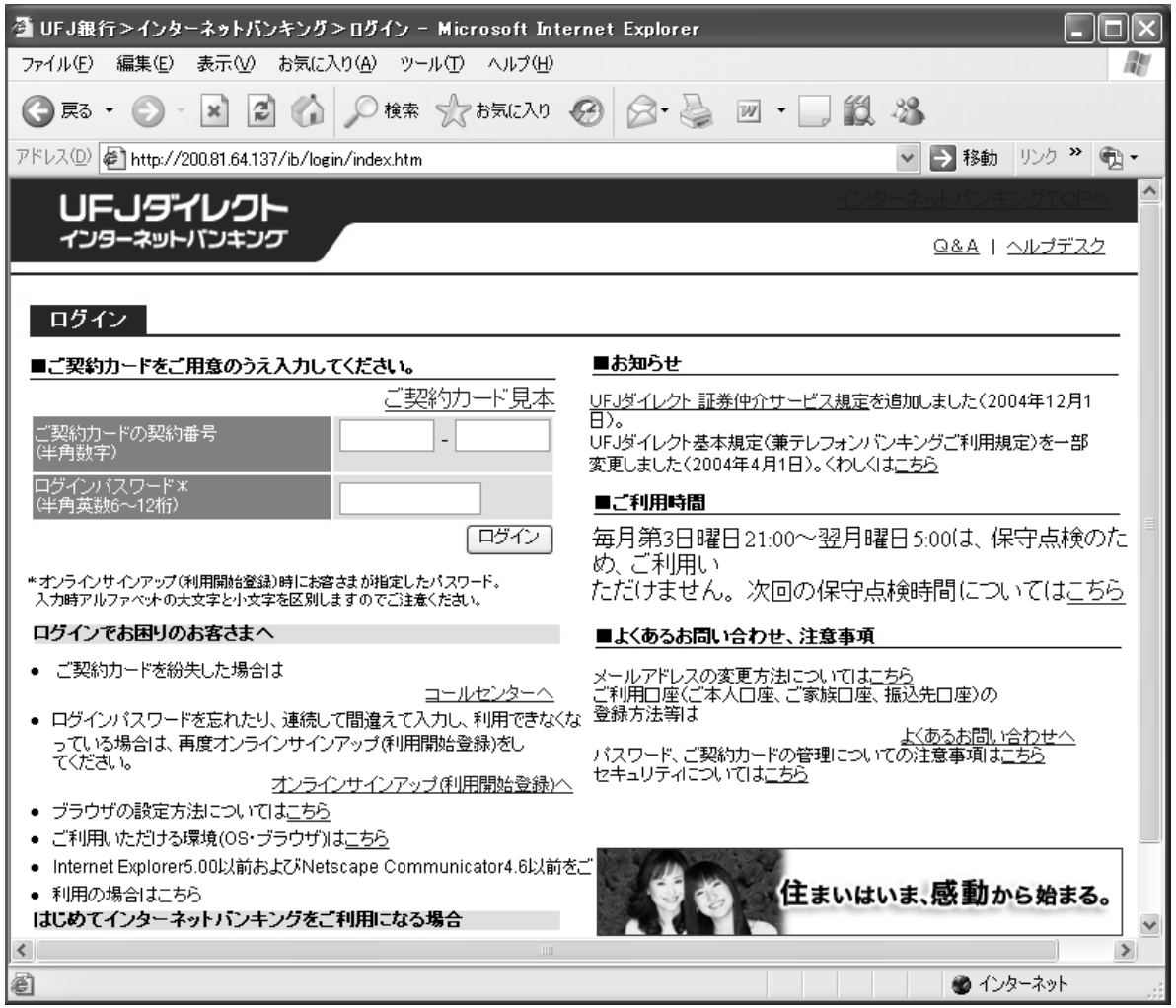
https://www.ufjbank.co.jp/ib/login/index2.html

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


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

フィッシングのページ


UFJ - 最新情報 - Microsoft Internet Explorer - [オフライン作業]
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 メディア
アドレス(D) http://61.38.30.55/ib/login/update.htm
移動 リンク
Google ウェブ検索 サイト検索 オプション
UFJダイレクト
インターネットバンキング
最新情報
姓
名
ご契約カードの契約番号
ログインパスワード※
クレジットカード番号
有効期限
Month
Year
桁の暗証番号
最新情報
(C)Copyright 2005, UFJ Bank Limited
UFJ銀行

フィッシングやなりすましの被害

- 直接的な被害の事例
  - UFJ クレジットカード
    - 2004年9～10月
    - カードの偽造 33 件
    - 8件の不正使用 (ルーマニア)
    - 被害総額 150 万円
- 間接的な被害
  - 信用の低下
  - ドメインに対するブランドイメージの低下

フィッシングへの対処

- フィッシングを見つけたら？
  - フィッシング対策協議会
    - http://www.antiphishing.jp/
  - 事例一覧
    - http://www.antiphishing.jp/db/list.html
- フィッシングで被害にあったら？
  - フィッシング110
    - 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

特定電子メール法

- 特定電子メール送信適正化法
- 2002年7月施行
  - ルールを守らない未承諾広告を出す人を取り締まる
    - Subject: 未承諾広告※
  - 総務省から警告メールの送信 → 措置命令の発出
  - 措置命令の発出は、3年間で 3 件
  - 問題点
    - 対象は SMTP → SMS は対象外
    - 個人宛 → 業務用 ML は対象外
    - 未承諾広告のみ → 本文が空のメールは対象外
- 2005年5月改正、11月施行
  - 問題点の改善
  - 直罰化
    - 差出人の詐称
    - 詐称の定義は限定的に公開

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！！

携帯電話と迷惑メール

- 携帯電話への迷惑メールは減少傾向にある
- DoCoMo の発表
  - 2003年7月　一日一ユーザ辺り 1.8 通
  - 2005年6月　一日一ユーザ辺り 0.02 通　(99% 減少)
- レート制御
  - KDDI では効果絶大
- 約款の行使
  - DoCoMo では 6,674 件
  - 迷惑メール配送事業者の特定が容易
- 政府の支援

迷惑メール追放支援プロジェクト

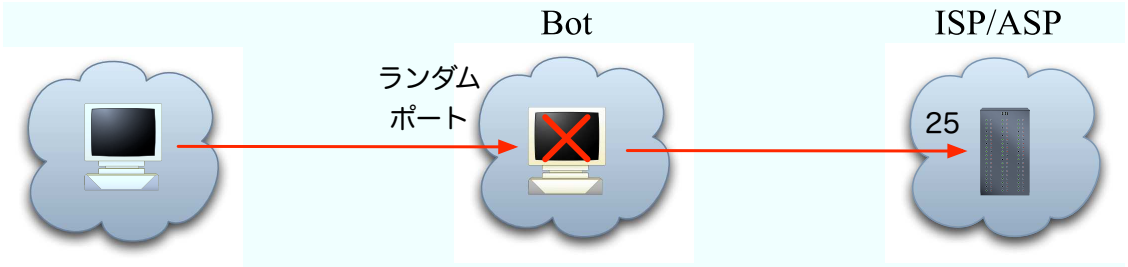
- 政府が迷惑メールだと認定してくれる
  - 総務省と経済産業省の共同プロジェクト
  - オトリを用意し、メールを集め、迷惑メールと判定
  - 2005年2月開始
    - http://www.meti.go.jp/press/20050121003/20050121003.html
- 実施する機関
  - 日本データ通信協会
    - http://www.dekyo.or.jp/
  - 日本産業協会
    - http://www.nissankyo.or.jp/
- 総務省の役割
  - 悪用されているメールアドレスを ISP/携帯電話事業者へ通知
  - 約款の行使を後押し
- 経済産業省の役割
  - 悪用されている口座を銀行へ通知

迷惑メールの問題点

インターネットと迷惑メール

- 大量の迷惑メール
  - ISP/ASP の「渡り」
  - Bot (ゾンビ)
    - Robot の短縮形
- 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/なりすまし

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？

コンテンツ・フィルタ

- ヒューリスティック・フィルタ
  - 経験に基づいたルール
    - Subject: 未承諾広告※
- ベイジアン・フィルタ
  - 単語の統計情報
    - ユーザが迷惑メールだと判定すると、学習する
- URL フィルタ
  - URL のホワイトリスト/ブラックリスト
- シグニチャ・フィルタ
  - 迷惑メールのチェックサムと照合

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
- 迷惑メールのフィルタリングは通信の秘密を侵す
  - 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
- ウイルスのフィルタリングは正当業務行為
  - だれも受け取りたくない

ブラックリスト

- IP アドレスに基づくブラックリスト
  - SPAMCOP
    - http://www.spamcop.net/
  - SBL
    - http://www.spamhaus.org/sbl/
  - CBL
    - http://cbl.abuseat.org/
  - DSBL
    - http://dsbl.org/
  - BOPM
    - http://opm.blitzed.org/
- 弊害
  - 間違った情報を登録可能
  - いつまでも情報が残っていることがある
  - 登録されたサイトへ通知がない場合が多い
- ホワイトリストとの併用が望ましい
  - 例) 携帯事業者の送信メールサーバの IP アドレスは、ホワイトリスへ
  - ブラックリストの結果だけから受信を拒否しないこと

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

グレーリスト

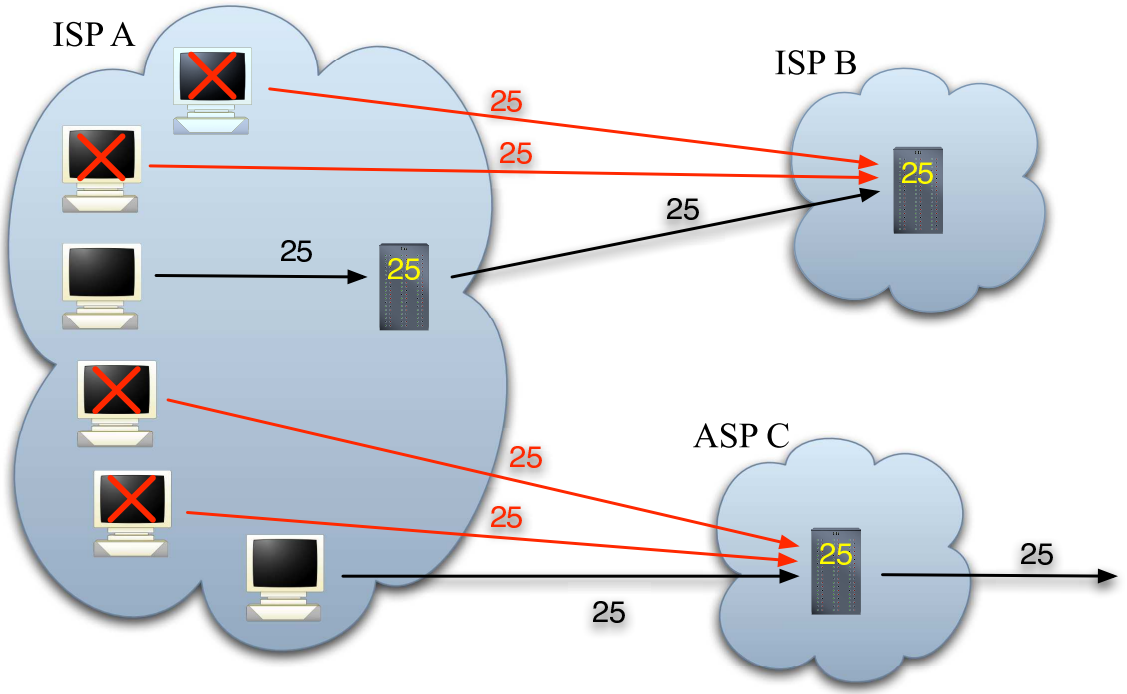
- ある IP アドレスからの送信要求に「一時エラー」を返す
- 再送、およびそれ以降の送信は、受理する
- 一時エラーを受け取ったときの挙動
  - 通常のサーバは、一定時間後、再送
  - Bot は、二度とそのサーバにメールを送らない
    - Bot は、迷惑メールの送信にコストをかけたくないから
- 注意点
  - サービスの質を低下させている
  - 通常のサーバが、正しく再送するとは限らない
  - ホワイトリストとの併用が望ましい
  - Bot が再送するようになれば無意味
    - サービスの質を低下させるだけ

Greet Pause

- 接続時に「あいさつ」の送信を遅らせる
  - 60 秒程度
  - Bot はあいさつを待たずに、迷惑メールの送信をあきらめる
- 注意点
  - サービスの質を低下させている
  - Bot が待つようになれば無意味
    - サービスの質を低下させるだけ

根本的な対策

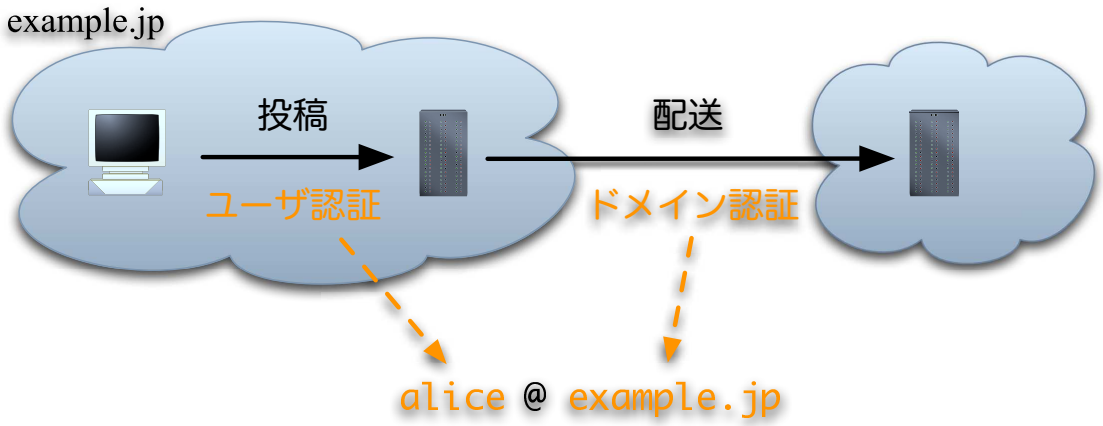
迷惑メールの問題点



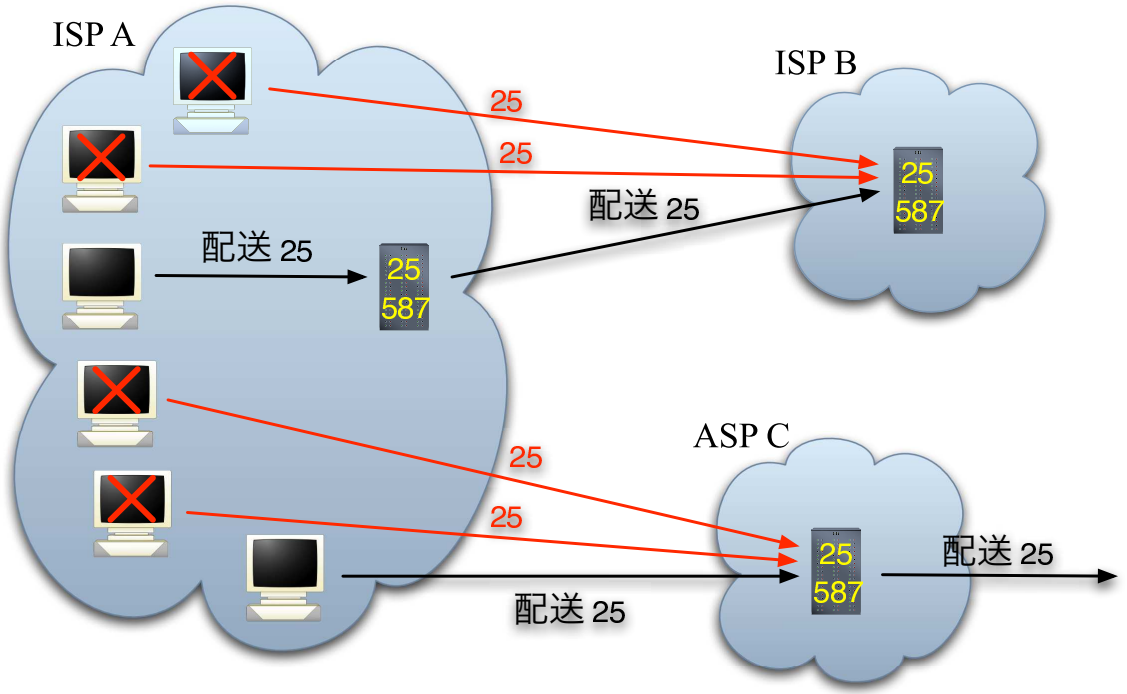
- 迷惑メールの大量送信
  - 渡り、Bot
- メールアドレスの詐称
  - 迷惑メール配送業者の特定が困難、フィッシング、なりすまし

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

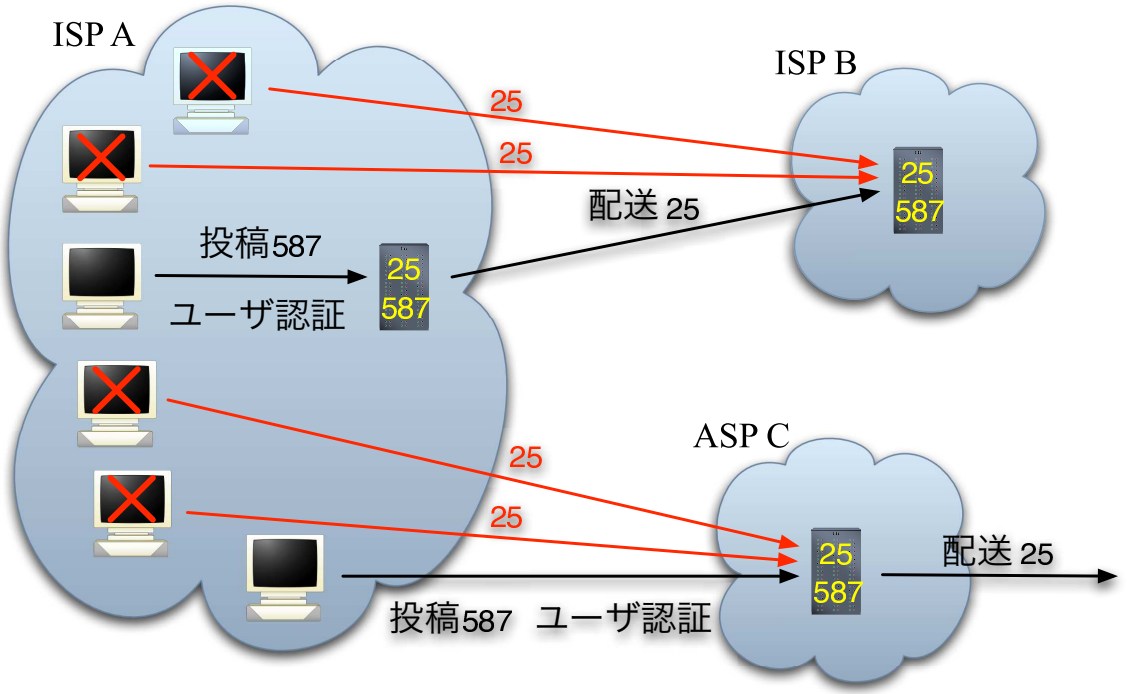


投稿ポートの提供



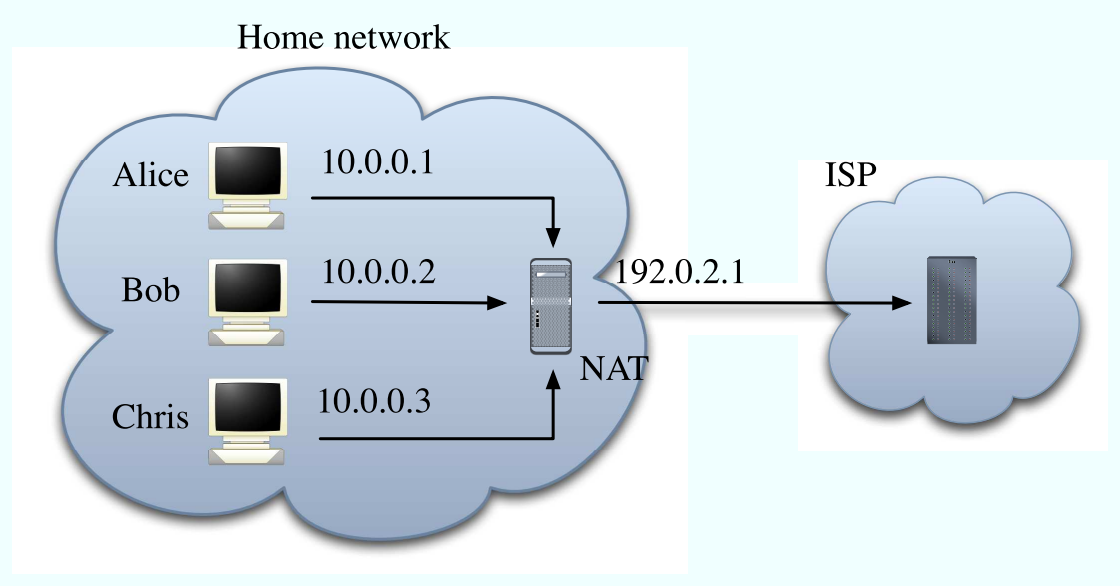
- 配送 = サーバ間の通信 (ポート 25 番)
- 投稿 = メールリーダとサーバの通信 (ポート 587 番)
  - Submission：プロトコル自体は SMTP

ユーザ認証



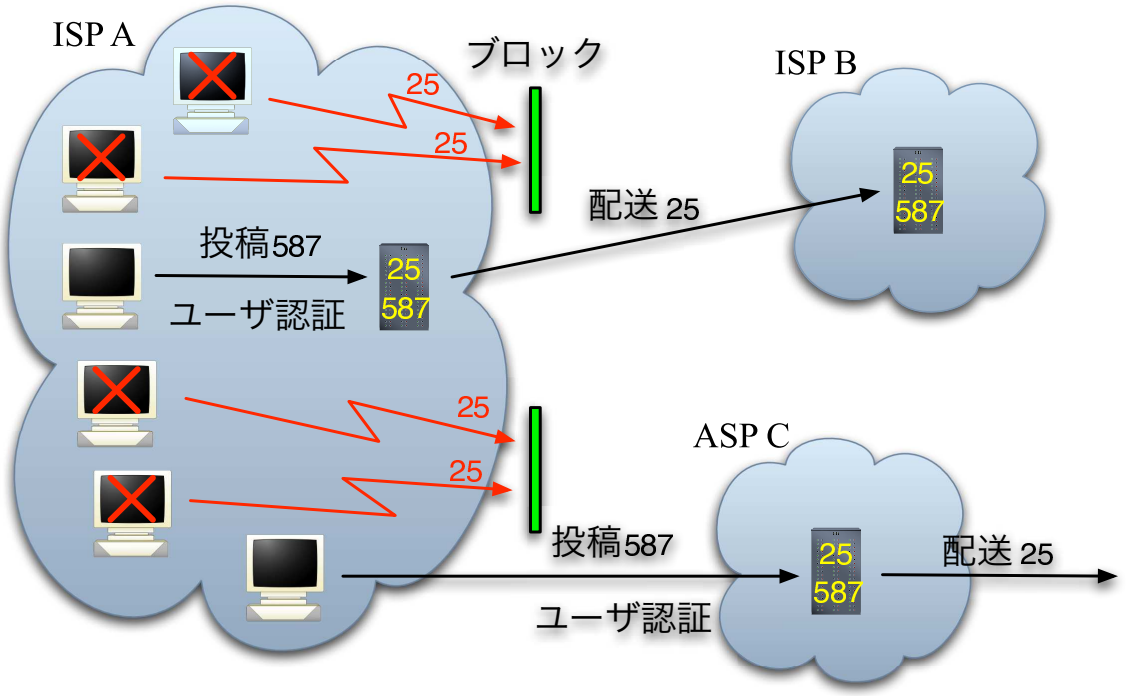
- 投稿ポートにはユーザ認証(SMTP AUTH)が必須
  - POP before SMTP では不十分

POP before SMTP



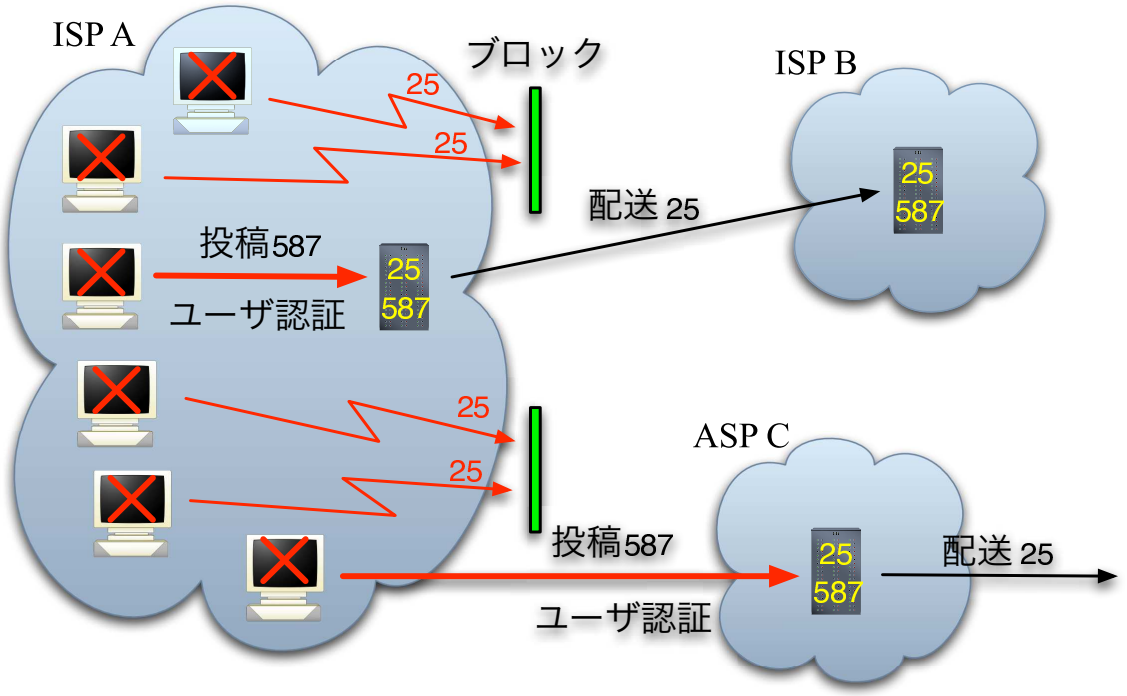
- POP before SMTP は IP アドレスを認証するだけ
- ユーザ認証ではない
- SMTP AUTH の代わりにはならない

OP25B



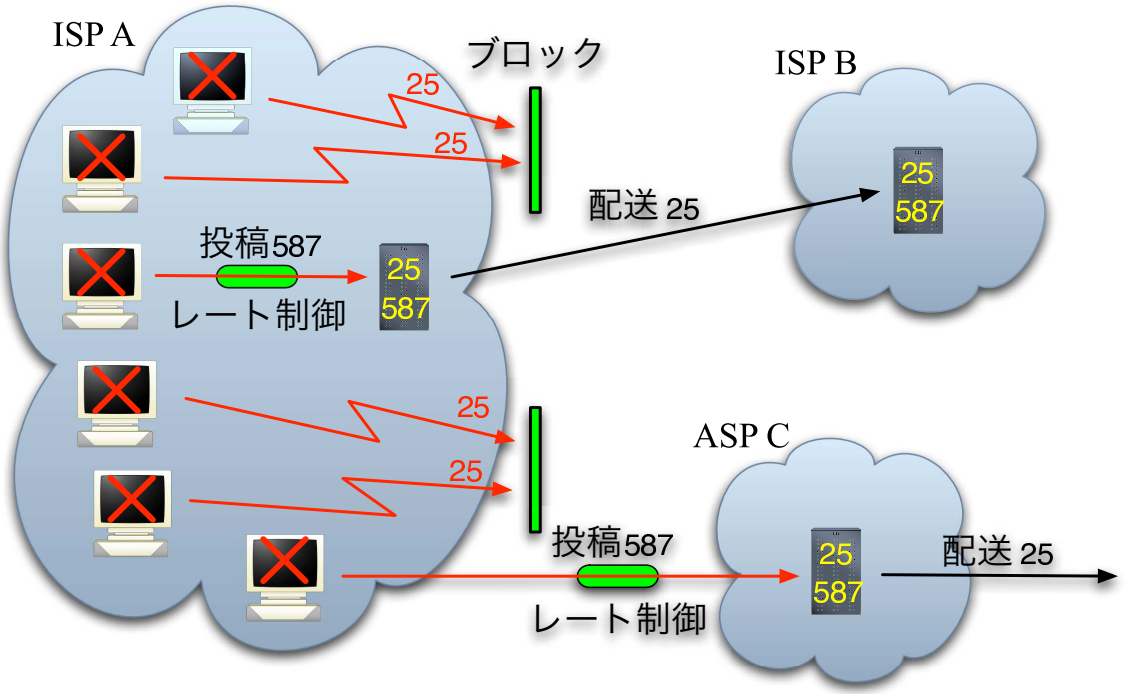
- ポート 25 番をブロックする
  - 追跡しにくい動的 IP からのみ
  - 独自にメールサーバを運用したい人は、固定 IP へ

予想される新しい攻撃



- パスワードを盗む Bot
- 堂々と迷惑メールを投稿する配送業者

レート制御

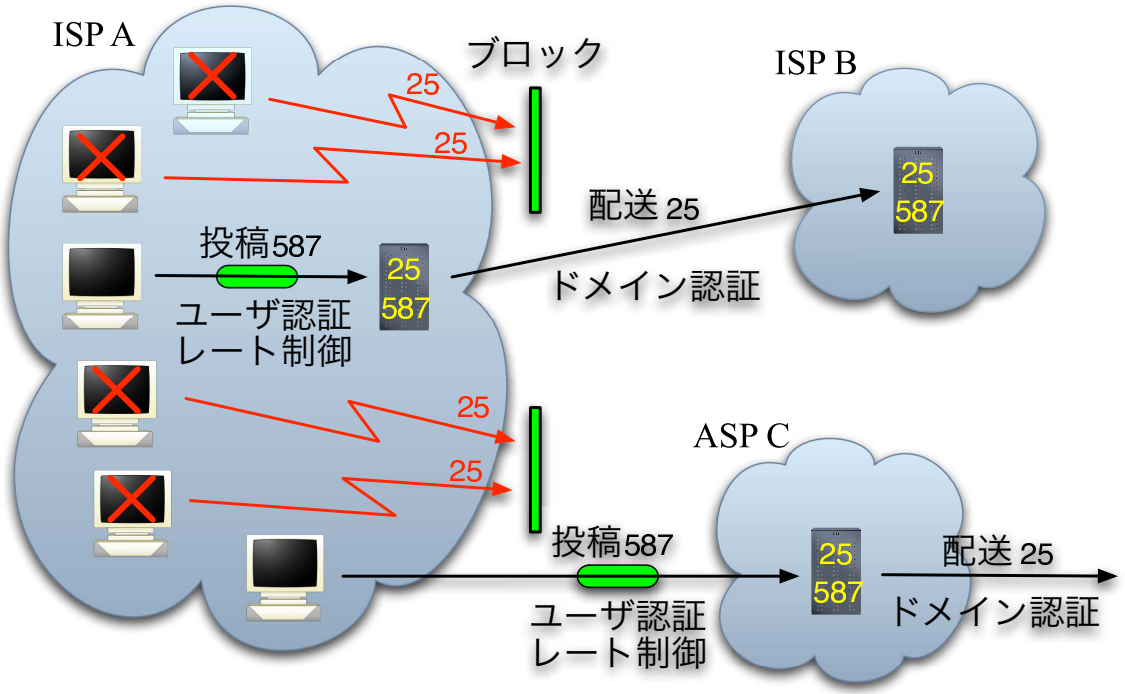


- 投稿にレート制御をかける
  - 短時間にたくさんの迷惑メールを送られることを禁止

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
  - エラー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

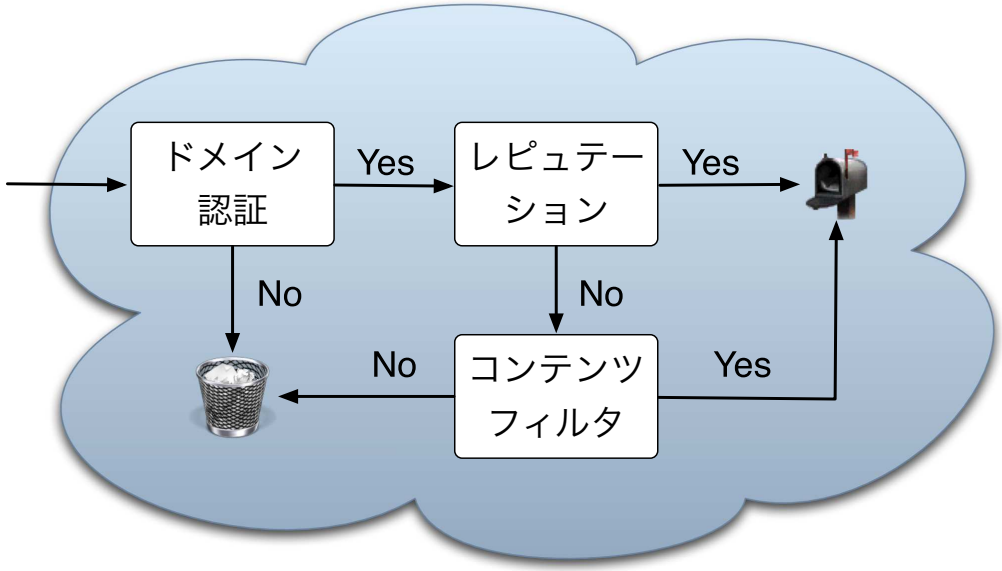
格付け

- 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

一例

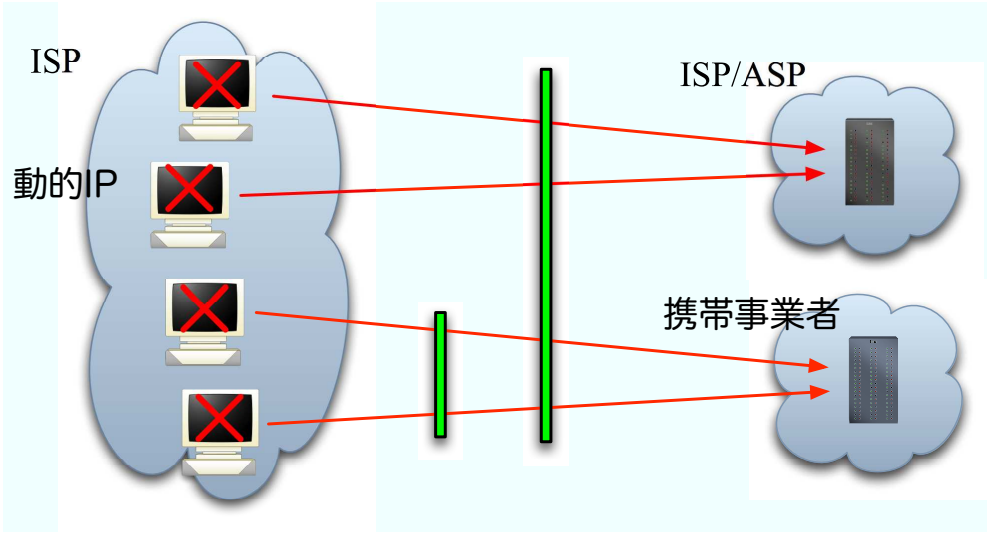


JEAG 勧告

- ISP/ASP へ勧告されているスケジュール
  - 投稿ポート+ユーザ認証の用意
    - 2006年5月 SHOULD
  - 投稿ポート+ユーザ認証への完全移行
    - 2007年3月 SHOULD
    - 2008年3月 MUST
  - OP25B の実施
    - 2006年12月 SHOULD
  - ドメイン認証(SPF)の送信側の設定
    - 2006年3月 SHOULD

OP25B と投稿ポート

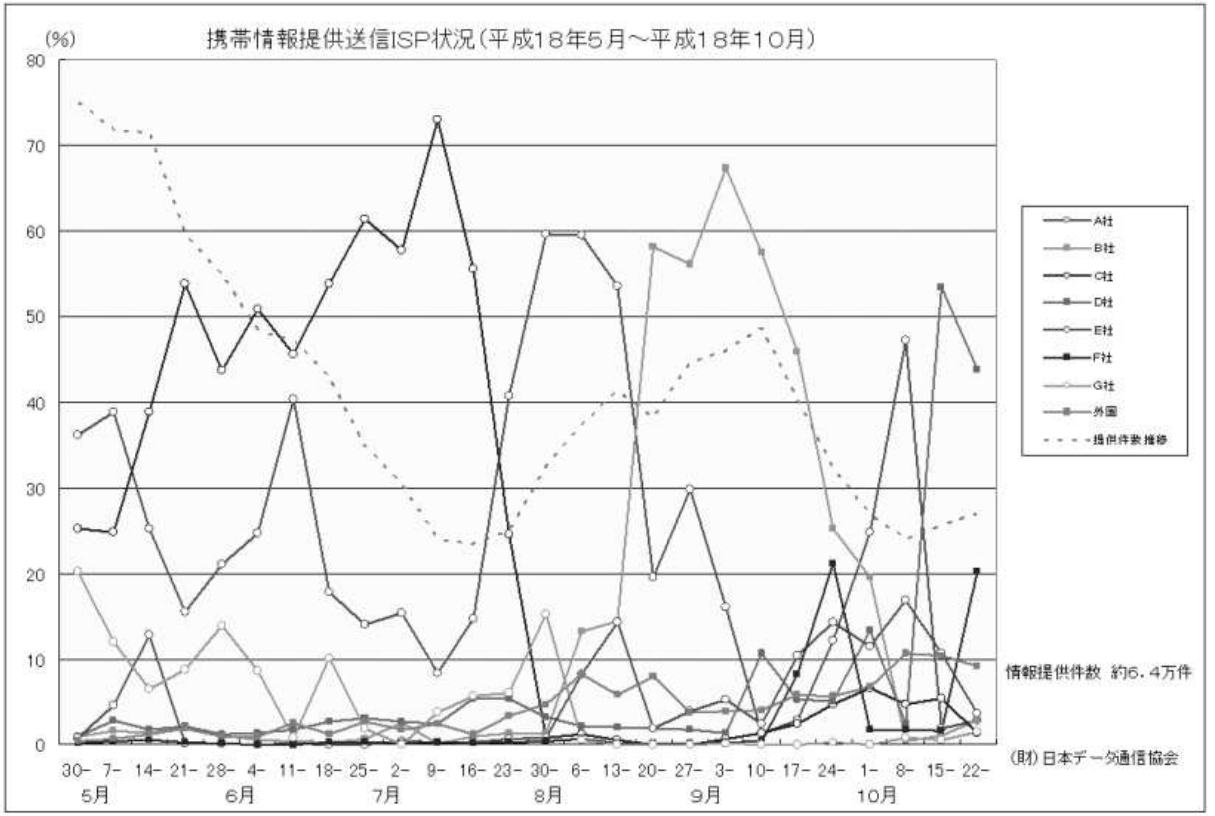
OP25B の導入実績



- 実施ISP一覧
  - http://www.dekyo.or.jp/soudan/taisaku/i2.html#isplist
- 総務省は OP25B を正当業務行為と認定

OP25B の効果

- 国内 PC から携帯向けの迷惑メールの推移



http://www.dekyo.or.jp/soudan/taisaku/i2-1.html#result3

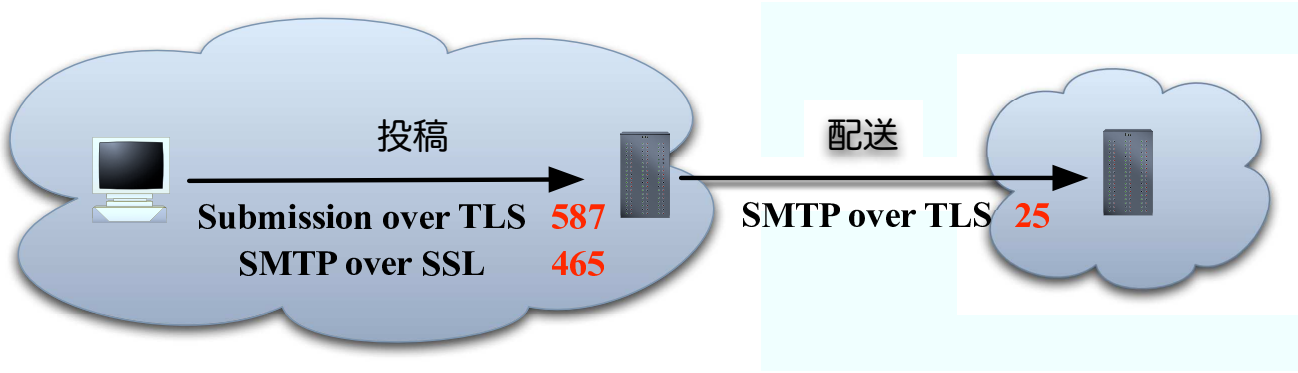
投稿ポートへの移行

- 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

Outlook Express と投稿ポート

- 送信のためのポート
  - デフォルトは 25 番ポート
  - 投稿ポート 587 番ポートも設定可能
- SMTP でのユーザ認証
  - 生パスワード(SASL PLAIN/LOGIN) には対応している
  - 使い捨てパスワード(SASL CRAM-MD5) には対応していない
- TLS/SSL
  - 25 番ポートなら TLS
  - それ以外のポートは SSL
- 一見よさそうだが、パスワードは守れない
  - 使い捨てパスワードに対応していない
  - 587/TLS に対応していない
  - SMTP over SSL はあるが、465 番ポートは IETF 標準ではない

Outlook Express と投稿ポート

- MS にお願いしてきましたが、
  OE を改善してもらえません

```
if (SSL) {
    if (ポート == 25) /* "|| ポート == 587" */
        TLS;
    else
        SSL; /* 465 はこのケース */
} else
    生SMTP;
```

- OE は受信側も脆弱
  - POP の使い捨てパスワード(APOP)もサポートしていない

Thunderbird の自動設定機能

- Thunderbird の特徴
  - Windows, Mac, Unix のすべてをサポート
  - セキュリティの機能に優れる
- 自動設定機能
  - 「拡張機能」による自動設定
    - サーバ名 + ポート番号
    - ユーザ認証を必須化
    - SSL/TLS を利用
  - ユーザは、名前とアカウント名を打ち込むだけ
  - IIJ での利用例
    - https://www.iij4u.or.jp/guide/basic/mail/thunderbird/?i=0u00b060830cb

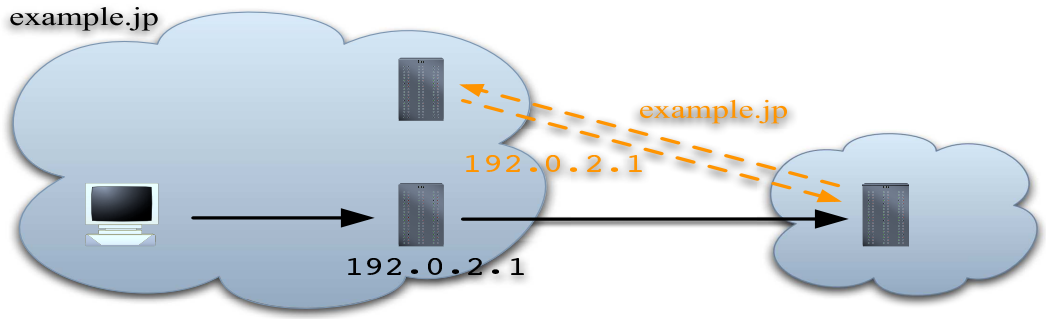
ドメイン認証

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"
  - example.jp IN TXT "v=spf1 +a +mx ~all"
    - 間接参照
  - example.jp IN TXT "v=spf1 -all"
    - Web のみ

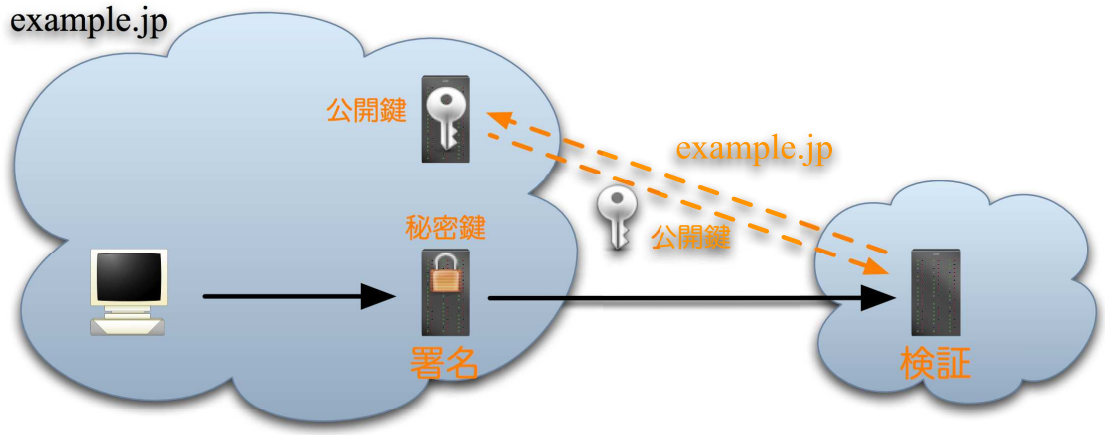
DKIM の署名

- 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=
```

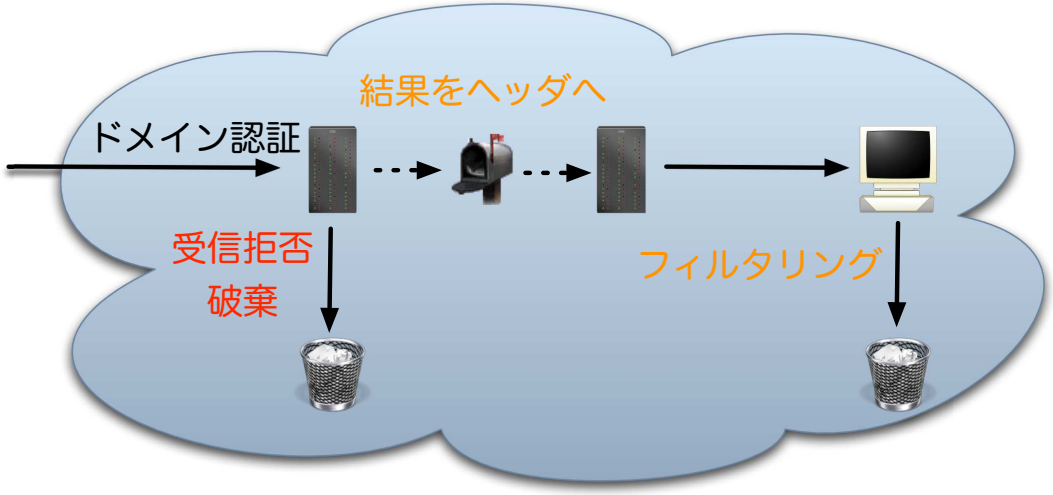
- DNS を利用
  - 公開鍵を DNS で配布
  - 認証局(CA)は不要

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

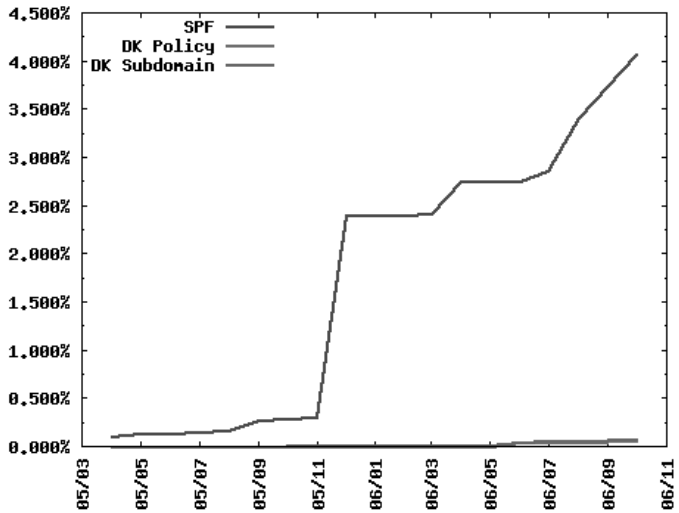
普及のストーリー



- 普及前期
  - 受信サーバは認証結果をメールのヘッダへ「ラベリング」
    Authentication-Results: mx.example.com
    from=alice@example.jp; spf=fail
  - 総務省は、ラベリングを正当業務行為と認定
  - メールリーダは認証結果を元にフィルタリング
  - フィルタリングは、ユーザの同意が必要
- 普及後期
  - 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10月現在
  - SPF = 4.08%
  - DKIM = 0.06 %



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

SPF

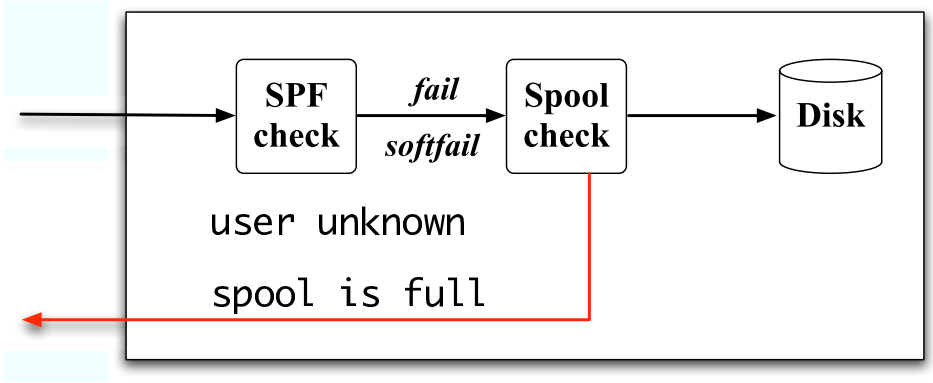
SPF の普及に関する問題

- 普及の初期
  - 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)
- 送信側の提案
  - 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

SPF によるエラーメールの低減



- 受信側の提案
  - 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
- Sendmail 用のパッチ
  - http://member.wide.ad.jp/wg/antispam/sm-dsn-supr/

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ラベリングしましょう
  - SPF の検証結果が fail/softfail で、
    unknown 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ラベリングしましょう

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/