迷惑メールに対する包括的な技術対策

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

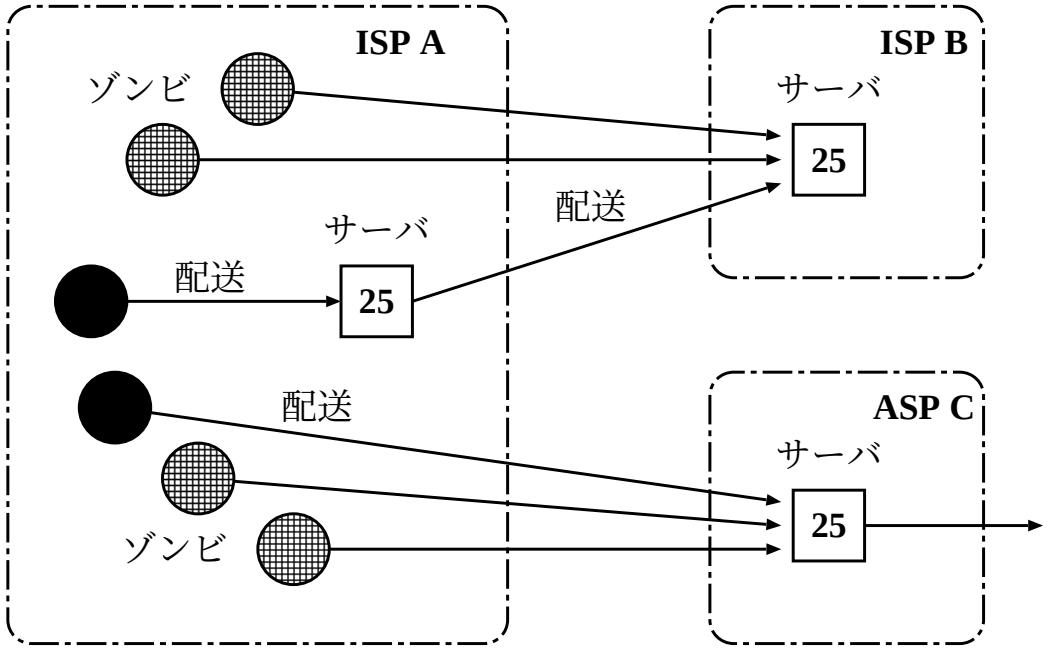
内容

- メールを追跡可能にするには
  - 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
  - 投稿に対するレート制御
  - 配送に対するドメイン認証
- メールが追跡可能になった後は
  - リピュテーション

注意

- ISP/ASP のメール管理者の「共通理解」
- 発表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?

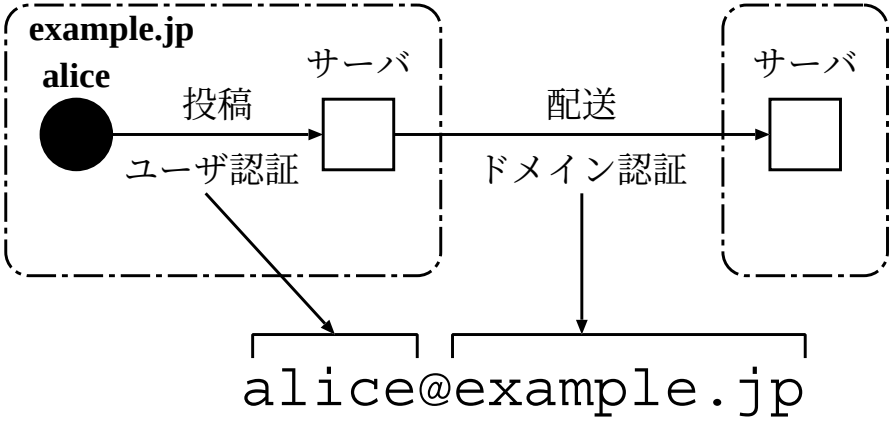
現状の問題点



- ゾンビ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

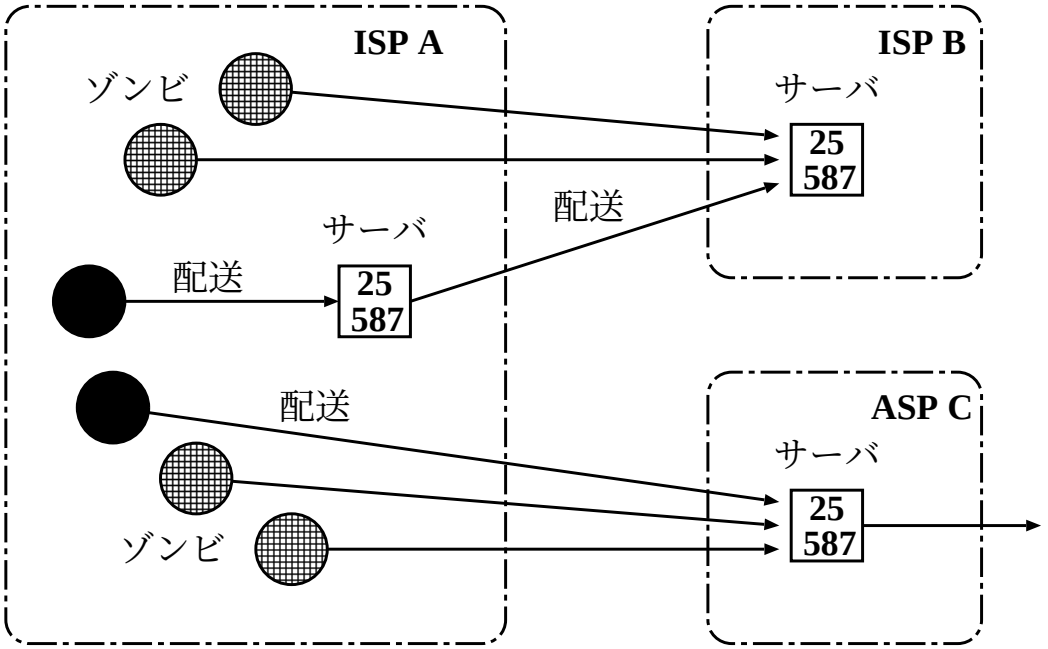
メールを追跡可能に

- 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

投稿ポートの提供



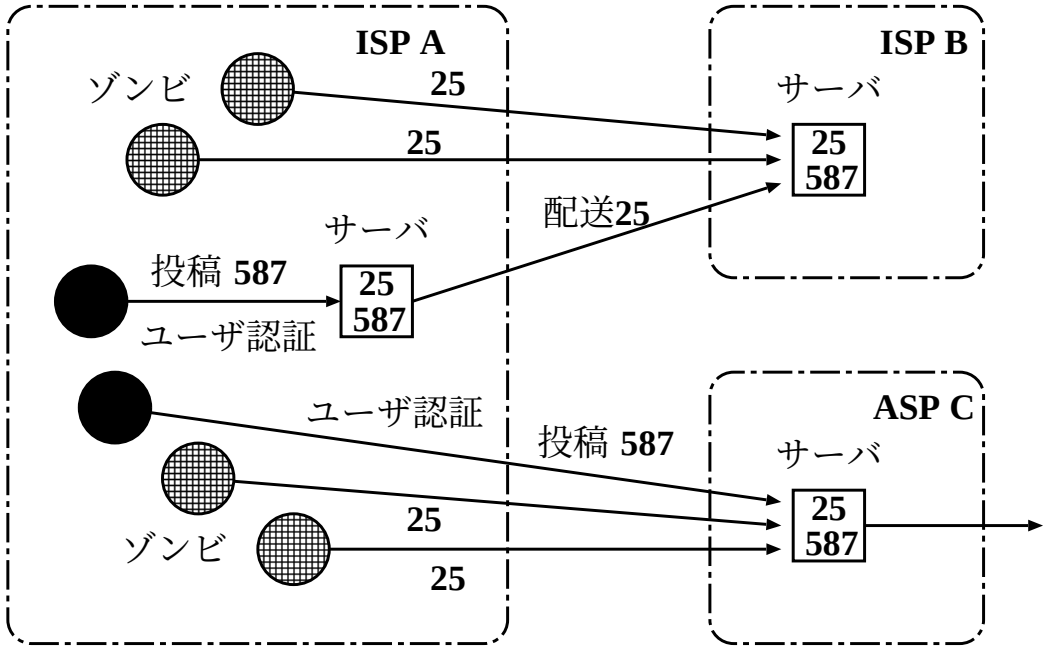
- **配送**
  - **ドメイン間の通信 (ポート** 25 **番)**
- **投稿**
  - **ユーザとそのドメイン間の通信 (ポート** 587 **番、**RFC 2476)
  - **プロトコル自体は** SMTP

SMTP/Submission over SSL/TLS

- SMTP over SSL **も一案**
  - **ポート** 465 **番**
  - **ポート** 25 **番の代替ポートという意味**
- IETF **は** SSL **より** TLS **を推奨**
  - TLS **は同一ポートを使う**
- **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**

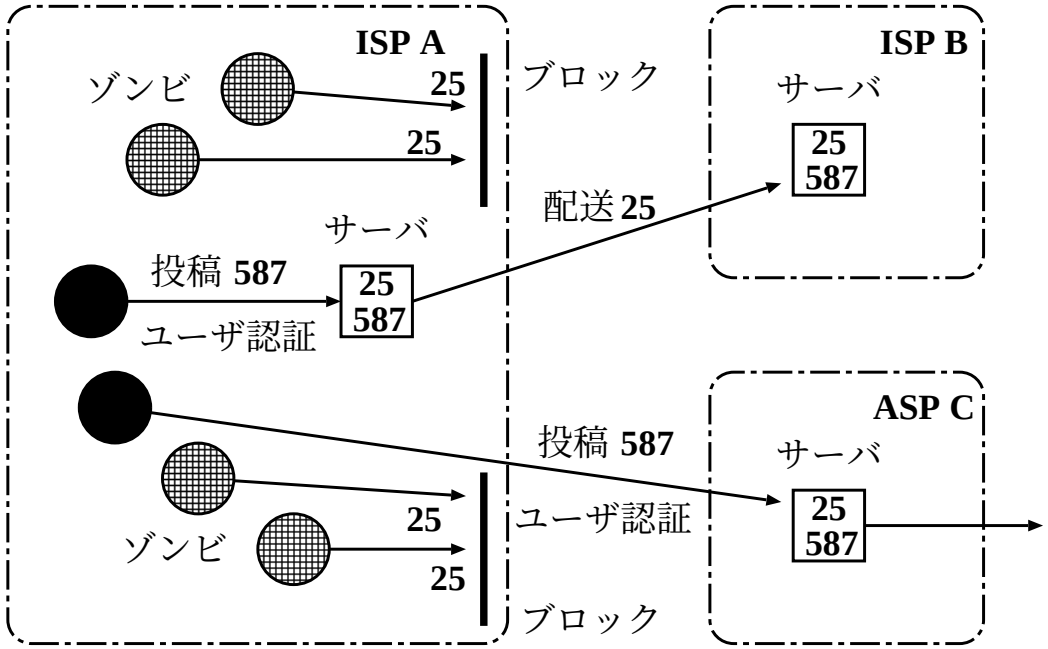
  http://www.wakwak.com/info/spec/port25/mail_group.html

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「投稿」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

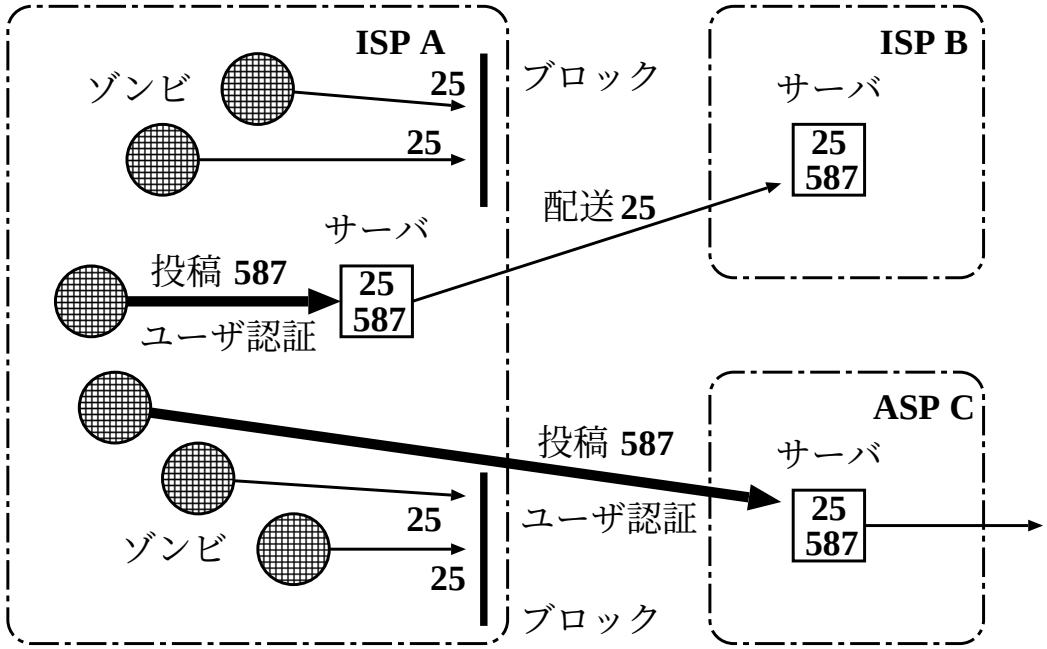


- **ポート 25 番をブロックする**
  - **追跡しにくい動的 IP からのみ**
  - **固定 IP は受信側でブラックリストを作成できる**
  - **独自にメールサーバを運用したい人は、固定 IP へ**

25番ポートのブロックの導入実績

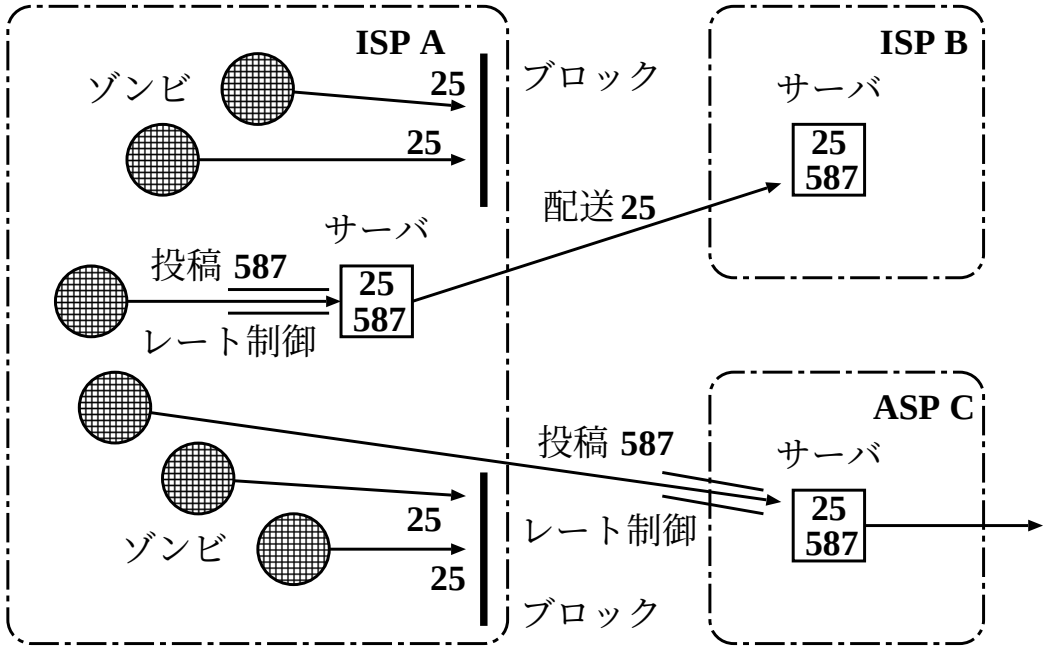
- **アメリカ**
  - AT&T、Bell CA、Bell South、Comcast
  - Earthlink、MSN、Verizon
  - **詳しくは**
    - http://www.postcastserver.com/help/Port_25_Blocking.aspx
- **日本**
  - **ぷららネットワークス**
    - http://www.plala.or.jp/access/living/releases/nr05_jan/0050127.html
    - **携帯事業社向け**
  - WAKWAK(NTT-ME)
    - http://www.wakwak.com/info/news/2005/port25blocking0107.html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

予想される新しい攻撃



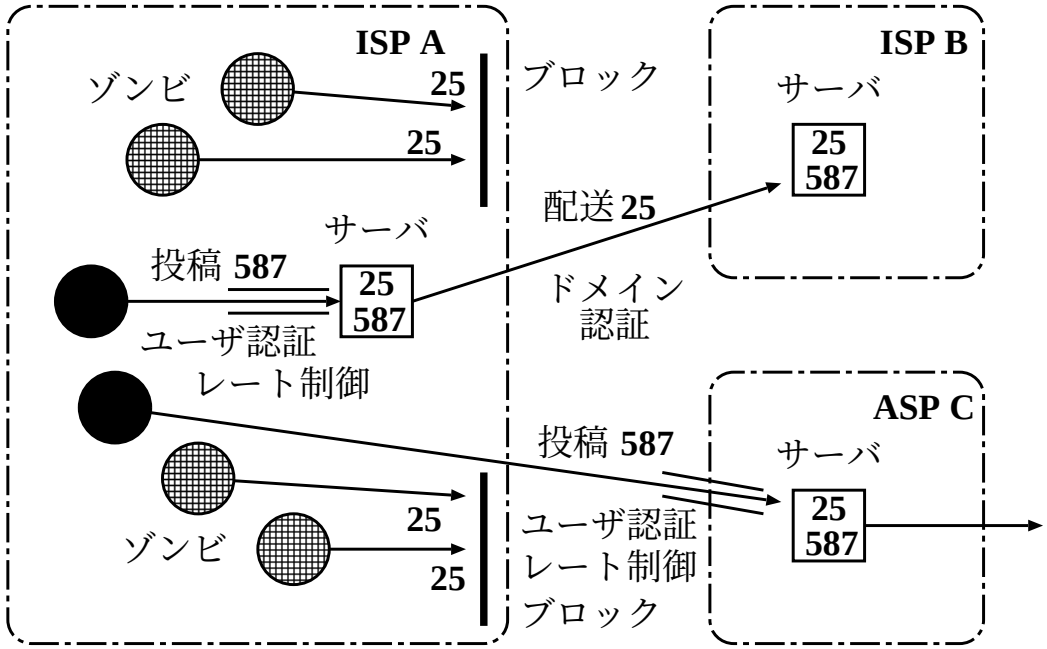
- パスワードを盗むゾンビが出現？
- 堂々と迷惑メールを投稿する配送業者

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

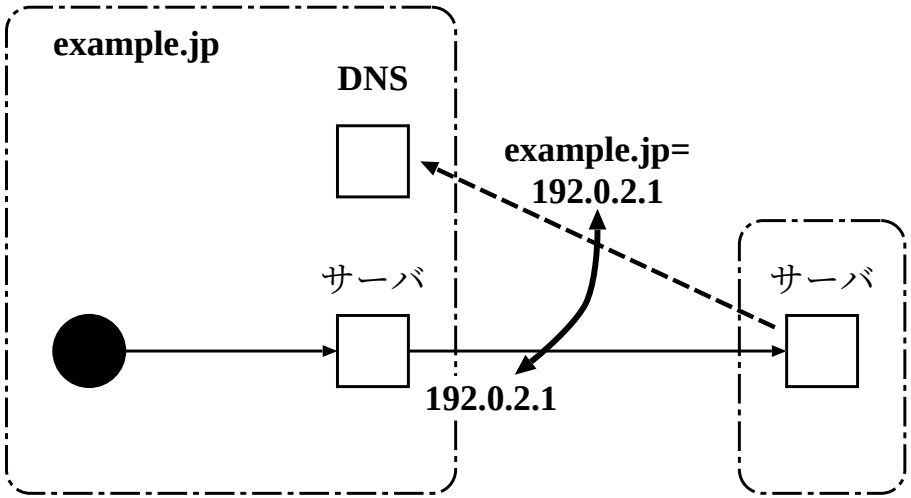
ドメイン認証



- 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

- **共存できる三つのプロトコル**
  - SPF、Sender ID (MFROM)
    - **封筒の送り主**
  - Sender ID (PRA)
    - **便箋の送り主**
  - DomainKeys
    - **便箋の署名**



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
  - ドメインを使い捨てる？
- ドメインを評価するシステムが必要
  - リピュテーション (reputation) と呼ばれる
- ISP/ASP の将来像
  - 追跡可能なメールシステム
  - リピュテーション
  - コンテンツ・フィルタ

詳しくは

- **ポート25番ブロッキング**
  - **小野里 佳和、エヌ・ティ・ティ エムイー**
- **ドメイン認証**
  - **池田 武、パナソニック ネットワークサービシズ**
- **ドメインの評価**
  - **脇山 弘敏、**IronPort Systems, Inc.