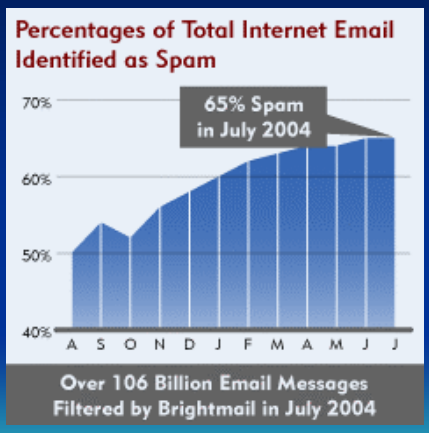
コミュニケーションにおける発信者認証

中村　素典@京都大学 / WIDE

IP Meeting 2004

spamの増加



- 半数以上がspamで増加を続けているという観測結果もある(Brightmaillによる)
- 国内の調査
  - http://www.web110.com/spam/ (SPAM WATCH)

スパムに狙われるネットワーク上のコミュニケーションメディア

- Mail
- NetNews
- IM [SPIM: spam over Instant Messaging]
- IRC (Internet Relay Chat)
- VoIP [SPIT: spam over Internet Telephony]
- Blog — comment spam

スパムによってメディアの価値が下がる

なぜスパムに狙われるのか

- 宣伝
  - URLが伝われば良い
  - 同じメディアでの返事は不要
  - 多様なメディアの活用
  - 費用対効果
- 詐欺、フィッシング(phishing)
- いたずら、いやがらせ
- ウィルスの感染経路

電子メールにおけるスパム対策

- ドメインによるAuthorization
  - MTAとMSA (Message Submission Agent)の分離
    - port 587 (RFC 2476) で明示的に分離することも可能

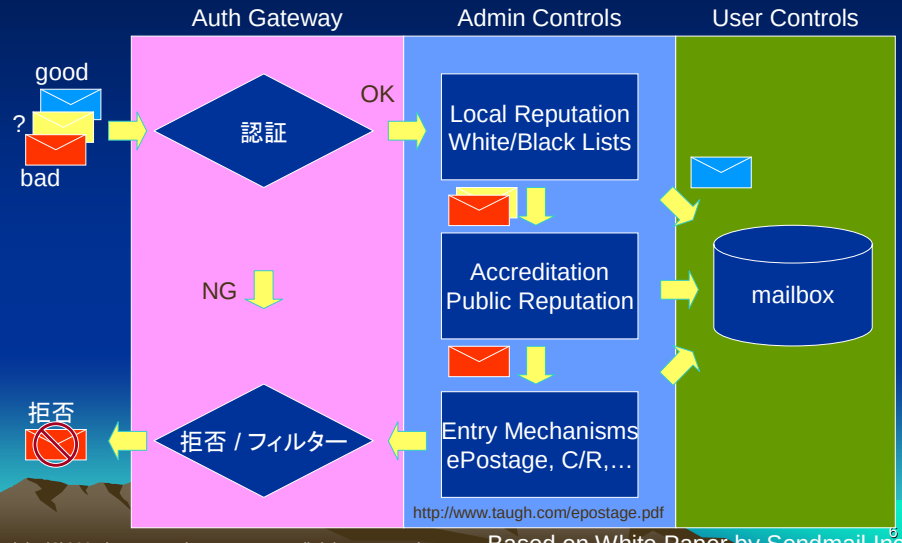
＋

- 発信者認証によるドメイン詐称検出
  発信サイト認証

＋

- 発信者ごとの評価機構
  (Reputation, Accreditation)

spam対策を考慮したメールシステム設計



Based on White Paper by Sendmail Inc.

電子メールにおける発信者認証

- メールアドレスとIPアドレスの関係による認証
  - SPF, Caller-ID, Sender-ID, CSV など
  - メールアドレスのドメイン名をキーにしてDNSを検索し、接続元のIPアドレスとの一致を確認
    - DNSの信頼性が前提
- メールアドレスと署名との関係による認証
  - DomainKeys など
  - 本文とヘッダに対する署名を検証し、鍵に示されるメールアドレスとの一致を確認

電子メールにおける発信者認証の問題点

- 中継サーバの存在
  - ファイアウォールやウィルスチェッカの導入でも
  - IPアドレスが変化する
    - サーバに対する発信認証？　認証がとれたものを中継？
  - MSA の導入(zombie host等の撲滅)
- 転送、メーリングリスト
  - アドレスのつけかえ
  - 署名方式との相性
- モバイル、ローミング
- ヘッダ、本文の改変
  - エンコーディングの変更

Reputation/Accreditation DB

- IPアドレスに対するもの
  - DNSBL
    (一覧の例 http://www.dnsbl.info/dnsbllist.asp)
  - Bonded Sender Program (BSP) by IronPort
    - http://www.bondedsender.org/
- メールアドレス(ドメイン名)に対するもの
  - DNA (Domain Name Accreditation)
    - CSV (Client SMTP Validation) の枠組みでの提案

特定を困難にさせるもの

- メッセージの改変
  - Mail Relay Server
  - Mailing List
- Relay Server
- NAT
- Proxy
- Mobile Networking
- Ubiquitous Networking

何を特定・評価したいのか

- IPアドレス？
- ドメイン名・ホスト名？
- ユーザ単位？

統合できるのか

- 識別子の統一の可能性
  - IP Address
  - Mail Address
  - Signature
- Reputation/Accreditation
  - 効果
  - 信頼性
  - スケーラビリティ
- DomainによるAuthorization?