電子メールの仕組みと迷惑メール対策の基礎知識

岡山大学 総合情報基盤センター
山井 成良
<yamai@cc.okayama-u.ac.jp>

2005/12/6
Internet Week 2005

Contents

- 迷惑メール(spamメール)の現状
- 電子メールの仕組み
- Spamメール対策の基礎知識
  - Spammerの手口
  - Spamメールへの対策
    - アドレス収集対策
    - Spamメール受信対策
    - Spamメール発信対策

迷惑メール(spamメール)の現状

迷惑メール

- 受信者が望まない電子メール
  - ウィルスメール
  - 架空請求メール
  - フィッシング(phishing)詐欺メール
  - 広告メール
  - エラーメール

  など

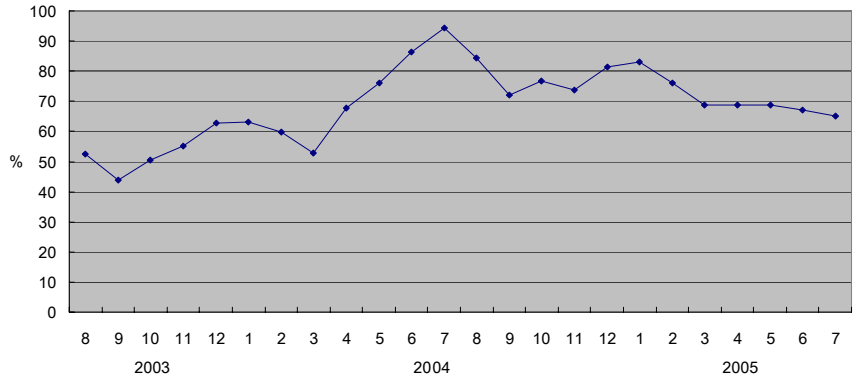
Spamメール

- SPAM (全て大文字)
  - 米Hormel Foods Corporationの商品&登録商標
    - http://www.spam.com参照
  - “Monty Python’s Flying Circus”のスキットに登場
- spam (全て小文字)
  - 一方的かつ大量に送られる電子メール
  - Hormel Foods社も公認
  - UCE (Unsolicited Commercial E-mail)
  - UBE (Unsolicited Bulk E-mail)

Spamメールの現状(1)

- Spam比率 - MessageLabs社のデータより

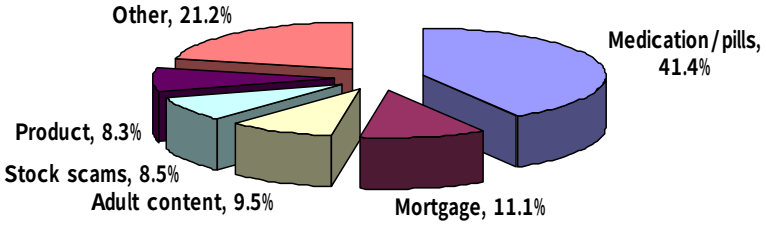
http://www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_en/threat_statistics/spam_intercepts/DA_114633.chp.html



Spamメールの現状(2)

- **種類と割合**(2005年1月～6月)
  - Sophos社のデータより

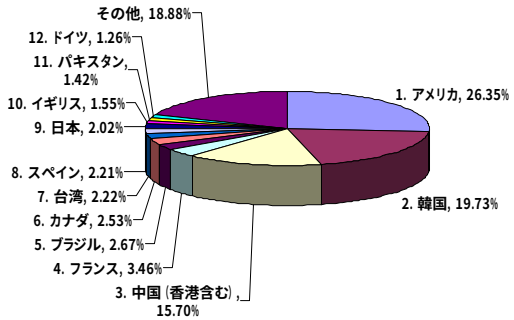
http://www.sophos.com/pressoffice/news/articles/2005/08/pr_us_20050803topfive-cats.html



Spamメールの現状(3)

- **発信国**(2005年4月～9月)
  - Sophos社のデータより

http://www.sophos.com/pressoffice/news/articles/2005/10/pr_us_dirtydozoct05.html



Spamメールによる被害(1)

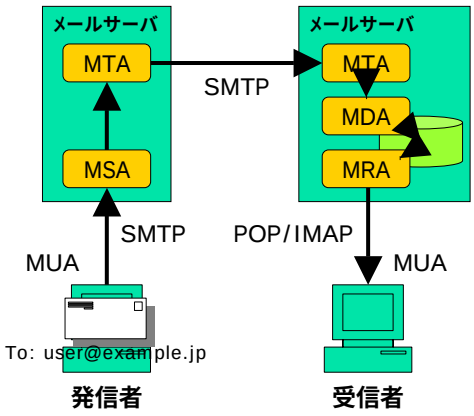
- CPU・ディスク・ネットワーク資源の浪費
  - メール全体の70%程度
  - 特に携帯電話利用者には深刻
    - メールの受信に時間（＝通信費用）がかかる
    - メールボックスがすぐに一杯
- メールの分類・削除
  - メール受信後も時間がかかる
  - 重要なメールの見落としも問題
    - spamフィルタを用いても起こりえる

Spamメールによる被害(2)

- 発信者詐称による間接的な被害
  - spamメール発信者との誤解
    - 苦情メールへの対処
    - 信頼性の低下
      - 通常メールの受信拒否も
- エラーメールの集中
  - 発生頻度小（自組織アドレスに詐称された場合）
  - 被害は甚大
    - 事実上のサービス不能(DoS)攻撃

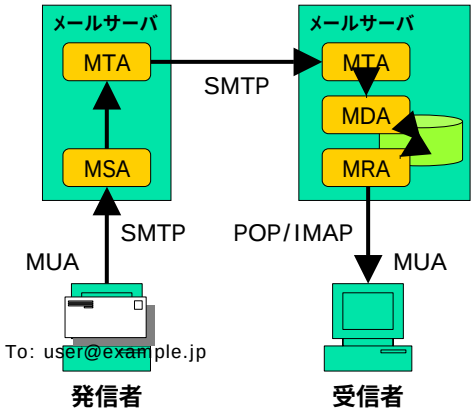
電子メールの仕組み

電子メールシステムの構成(1)



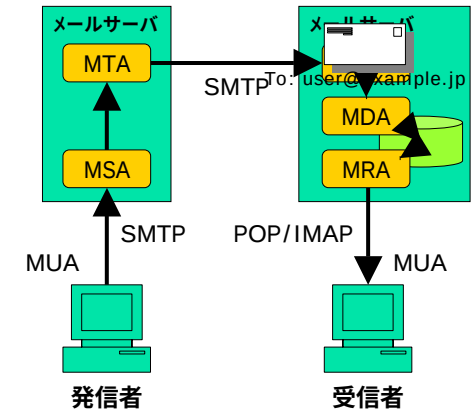
- MUA (Mail User Agent)
  - メールクライアント，メーラなど，いろいろな呼び方がある
  - ユーザインタフェースを担当
  - メールの送信･受信処理を行う
  - 例：Outlook, Eudora
  - 通常は1台のメールサーバのみと通信

電子メールシステムの構成(2)



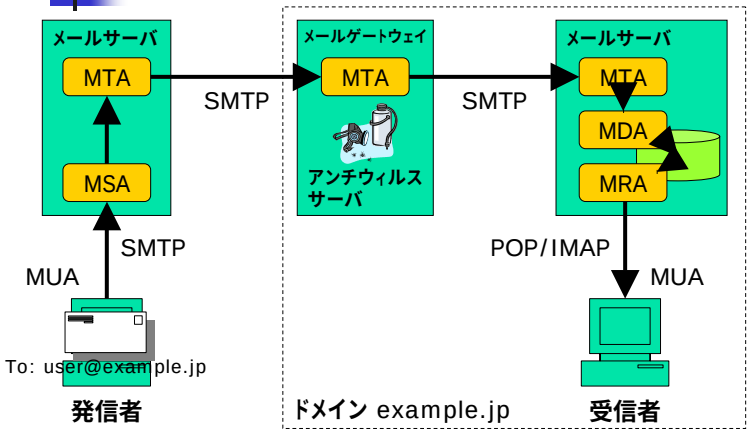
- MSA (Message Submission Agent)
  - MUAに対するSMTPサーバ
  - メールの発信受付を担当
  - MTAから分離・独立
  - 有資格者からの発信のみ受理
- MTA (Mail Transfer Agent)
  - メールの中継配送を担当
  - ドメイン部に従って中継
  - 例：sendmail, qmail, Postfix

電子メールシステムの構成(3)



- MDA (Mail Delivery Agent)
  - メールの格納を担当
  - ローカルパート(@より左側)に従ってメールボックスに格納
  - 転送処理も担当範囲
  - 例：mail.local, procmail
- MRA (Mail Retrieval Agent)
  - メールボックスからのメール取出しを担当
  - POP/IMAPサーバに相当

電子メールシステムの構成(4)



- 多段中継の場合

電子メールのプロトコル(1)

- SMTP (Simple Mail Transfer Protocol)
  - 電子メールの発信･配送用プロトコル
    - MUAからMSA (MTA)への発信
    - MTAからMTAへの配送
  - 標準ではTCP 25番ポートを利用
  - MSA専用としてTCP 587番ポートを利用可

電子メールのプロトコル(2)

- **主なコマンド**
  - HELO/EHLO (Hello/Extended Hello)
    - ･･･ MTA名の通知･オプションの選択
  - MAIL (Mail) ･･･ **発信者の指定**
  - RCPT (Recipient) ･･･ **受信者の指定**
  - DATA (Data) ･･･ **本文の送付**
  - QUIT (Quit) ･･･ **セッションの終了**
  - RSET (Reset) ･･･ **発信者指定状態に復帰**

電子メールのプロトコル(2)

1. `S: 220 mail.example.jp ESMTP Ready`
2. `C: HELO mta.example.com`
   `S: 250 Hello mta.example.com`
3. `C: MAIL FROM: <alice@example.com>`
   `S: 250 <alice@example.com> ... OK`
4. `C: RCPT TO: <bob@example.jp>`
   `S: 250 <bob@example.jp> ... OK`
5. `C: DATA`
   `S: 354 Go ahead`
   `C: From: alice@example.com`
   `C: To: bob@example.jp`
   `C: Subject: test`
   `C:`
   `C: This is a test message.`
   `C: .`
   `S: 250 Message accepted`
6. `C: QUIT`
   `S: 221 Closing connection`

1. **セッションの開始**
2. **送信の準備**
3. **発信者の指定**
4. **受信者の指定**
   - **複数指定も可能**
5. **本文の送付**
6. **セッションの終了**

電子メールのプロトコル(3)

- サーバの応答コード
  - 3桁の数字+説明
    - 200番台　肯定完了応答
    - 300番台　肯定中間応答
    - 400番台　一時的否定完了応答
    - 500番台　恒久的否定完了応答
  - 400番台と500番台の違いが重要
    - 400番台の場合には「再送」
    - 500番台の場合には「返送」

電子メールのプロトコル(4)

- エラーの例

```
S:     220 mail.example.jp ESMTP Ready
C:     HELO mta.example.com
S:     250 Hello mta.example.com
C:     MAIL FROM: <alice@example.com>
S:     250 <alice@example.com> ... OK
C:     RCPT TO: <bob@example.jp>
S:     550 <bob@example.jp>... User Unknown
C:     QUIT
S:     221 Closing connection
```

電子メールのプロトコル(5)

- POP (Post Office Protocol)
- IMAP (Internet Message Access Protocol)
  - **電子メールの読込み用プロトコル**
  - **メッセージの操作･管理方法が異なる**
    - **POPではMUAにメッセージを取り込んで操作･管理**
    - **IMAPではMRAにメッセージを置いたまま操作･管理**
  - **ポート番号**
    - **POP3ではTCP 110番ポートを利用**
    - **IMAPではTCP 143番ポートを利用**

電子メールのプロトコル(6)

- **POP3の代表的なコマンド**
  - USER　**ユーザ名の通知**
  - PASS　**パスワードの通知**
  - APOP　**ユーザ名と認証情報の通知**
  - STAT, LIST, RETR, DELE
    メールボックス操作
  - QUIT　**セッションの終了**

電子メールのプロトコル(7)

- POP3の使用例(RFC1939の例を一部修正)

```
S:    +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C:    APOP mrose c4c9334bac560ecc979e58001b3e22fb
S:    +OK mrose's maildrop has 1 message (120 octets)
C:    LIST
S:    +OK 1 message (120 octets)
S:    1 120
S:    .
C:    RETR 1
S:    +OK 120 octets
S:    <メッセージ1の内容が入る>
S:    .
C:    DELE 1
S:    +OK message 1 deleted
C:    QUIT
S:    +OK dewey POP3 server signing off (maildrop empty)
```


エンベロープとヘッダ(1)

- エンベロープ(envelope)
  - 封筒に書かれた情報
  - MAILコマンド, RCPTのコマンドの引数
- ヘッダ(header)
  - 本文（便箋の先頭部分）に書かれた情報
  - DATAコマンドの後に送られる
  - 空白行までの範囲

エンベロープとヘッダ(2)

```
S:      220 mail.example.jp ESMTP Ready
C:      HELO mta.example.com
S:      250 Hello mta.example.com
C:      MAIL FROM: <alice@example.com> ← エンベロープFrom
S:      250 <alice@example.com> ... OK
C:      RCPT TO: <bob@example.jp> ← エンベロープTo
S:      250 <bob@example.jp> ... OK
C:      DATA
S:      354 Go ahead
C:      From: alice@example.com ← ヘッダFrom
C:      To: bob@example.jp ← ヘッダTo
C:      Subject: test
C:
C:      This is a test message.
C:      .
S:      250 Message accepted
C:      QUIT
```


エンベロープとヘッダ(3)

- ヘッダのフォーマット
  - 基本は「フィールド名：値」
  - 継続行が許される場合もある
- 代表的なヘッダ
  - 差出人関係
    - From: 本来の差出人
    - Sender: 実際の送信者
    - Reply-To: 返信先
    - Return-Path: エラー時の返送先 (エンベロープFrom)

エンベロープとヘッダ(4)

- 代表的なヘッダ（続き）
  - 受取人関係
    - To: 正受取人
    - Cc: 副受取人(Carbon Copy)
    - Bcc: 副受取人(Blind Cc, 配送時に消去)
  - 転送関係
    - Resent-From: 再送元の本来の差出人
    - Resent-Sender: 再送した実際の差出人
    - Resent-To: 再送先

エンベロープとヘッダ(5)

- 代表的なヘッダ（続き）
  - その他
    - Date: 発信日時
    - Subject: タイトル
    - Message-Id: メッセージ固有のID
    - Received: 配送記録（上に追加）

エンベロープとヘッダ(5)

```
Return-Path: <owner-anti-spam@cc.okayama-u.ac.jp> ← エンベロープFromと同じ
Received: from unknown (HELO ccsrv2.cc.okayama-u.ac.jp) ([150.46.xx.xx])
    (envelope-sender <owner-anti-spam@cc.okayama-u.ac.jp>) ← エンベロープFrom
    by xxx.xxx.xxx.xxx with SMTP
    for <user@example.co.jp>; 13 Oct 2005 00:22:33 +0900 ← エンベロープTo
Received: from ccsrv1.cc.okayama-u.ac.jp (ccsrv.cc.okayama-u.ac.jp [150.46.xx.xx])
    by ccsrv2.cc.okayama-u.ac.jp with ESMTP id AAA26964
    for <user@example.co.jp>; Thu, 13 Oct 2005 00:22:29 +0900 ← エンベロープTo
Received: (from majordom@localhost)
    by ccsrv.cc.okayama-u.ac.jp id AAA29022
    for anti-spam-outgoing; Thu, 13 Oct 2005 00:20:02 +0900 (JST) ← エンベロープTo
Date: Thu, 13 Oct 2005 00:20:01 +0900 (JST)
From: Nariyoshi Yamai <yamai@cc.okayama-u.ac.jp> ← 本来の差出人(投稿者)
Message-Id: <200510121520.AAA29014@ccsrv.cc.okayama-u.ac.jp>
To: anti-spam@cc.okayama-u.ac.jp ← 本来の宛先
Subject: [anti-spam: 638] anti-spam articles (September 19 - September 25)
Sender: owner-anti-spam@cc.okayama-u.ac.jp ← 実際の送信者
Precedence: bulk
Reply-To: anti-spam@cc.okayama-u.ac.jp ← 返信先アドレス
```


エンベロープとヘッダ(6)

- エンベロープとヘッダの関係
  - もともと役割が異なる
    - エンベロープFrom・Toは配送用(MTAが利用)
    - ヘッダFrom・Toは記録用(受信者・MUAが利用)
  - 両者が一致しなくてもよい
    - Bccで指定したアドレス
    - メーリングリストの宛先・差出人アドレス
  - 特にspamメールでは一致しないことが多い

DNSとの連携(1)

- ドメイン名と資源レコード(RR)を対応付け
- 電子メールの配送に深く関与
  - 配送先の決定に利用
    - MXレコード
    - Aレコード, AAAAレコード
  - 発信元の確認・記録に利用
    - PTRレコード
  - 最近ではspam対策にも利用
    - DNSBL(DNS Black List), 送信ドメイン認証, etc.

DNSとの連携(2)

- MX (Mail eXchange) レコード
  - 複数のレコードを優先度つきで指定可
    - 小さい番号が優先

```
okayama-u.ac.jp.    IN MX   10 mta1.okayama-u.ac.jp.
                    IN MX   20 mta2.okayama-u.ac.jp.
```

      - まずmta1への配送を試み, 失敗すればmta2へ
    - 同じ番号の場合にはランダム

```
okayama-u.ac.jp.    IN MX   10 mta1.okayama-u.ac.jp.
                    IN MX   10 mta2.okayama-u.ac.jp.
```

      - まずどちらかへの配送を試み, 失敗すればもう一方へ

DNSとの連携(3)

- PTR (PoinTeR) レコード
  - 逆引き (IPアドレス⇒ホスト名) に利用
    - IPアドレスがAAA.BBB.CCC.DDDのホスト名

DDD.CCC.BBB.AAA.in-addr.arpa. IN PTR client.okayama-u.ac.jp.

⇒ client.okayama-u.ac.jpを取得

  - 正引き (ホスト名⇒IPアドレス) で整合性検証
    - パラノイド検査

client.okayama-u.ac.jp. IN A AAA.BBB.CCC.DDD

⇒ 最初のIPアドレスと一致するため，正当と判断

発信者認証(1)

- 目的
  - 第三者による不正発信の拒否
  - 問題発生時の発信者特定
- 発信者アドレスの正当性は対象外
  - 他のISPから発信する場合などを考慮
  - 利用者レベルでデジタル署名を利用可能
    - PGP (Pretty Good Privacy)，S/MIMEなど
  - 発信者アドレスの正当性保証も可能
    - 強制的にSender:ヘッダを挿入/置換するなど

発信者認証(2)

- POP before SMTP
  - 前提条件
    - POPサーバと発信用MTAが同じ
  - 方法
    - 受信時に先立ってPOPで認証
    - 認証に成功したIPアドレスを一定時間 (例えば10分) 登録
    - 登録IPアドレスからは任意の宛先への配送を許可
  - 利点･欠点
    - MUAを選ばない
    - IPアドレスが同じMUA/MTAから他の利用者も発信可能
      - 特にNATを利用するISPから発信する場合に問題

発信者認証(3)

- SMTP-AUTH
  - SMTPの拡張(RFC2554)
    - 新しいコマンドAUTHの追加
    - メール発信時に利用者を認証
    - いくつかの認証方法がサポート
      - CRAM-MD5, MD5-DIGEST, PLAIN, LOGIN
  - 対応したMUAが必要
    - 最近は殆どのMUAがどれかの認証方式に対応

暗号化(1)

- 基本的には平文で通信
  - 少なくとも本文は盗聴可能
    - SMTP-AUTHでは一部の認証方法のみ暗号化
    - POPではAPOP利用時のパスワードのみ暗号化
- TLS，SSLによる通信暗号化
  (TLS: Transport Layer Security, SSL: Secure Socket Layer)
  - MUA･MTA間，MUA･MRA間での盗聴を防止
  - MTA･MTA間での盗聴およびサーバ管理者の覗き見には無力
- メール全体の暗号化
  - PGP (Pretty Good Privacy)，S/MIMEなど

暗号化(2)

- ポート番号
  - TLSでは通常と同じ
    - SMTP/TLS: 25番，587番
    - POP/TLS: 110番
    - IMAP/TLS: 143番
    ※ セッションの途中で「STARTTLS」コマンドを使用
  - SSLでは異なる
    - SMTP/SSL: 465番(非公認)
    - POP/SSL: 995番
    - IMAP/SSL: 993番

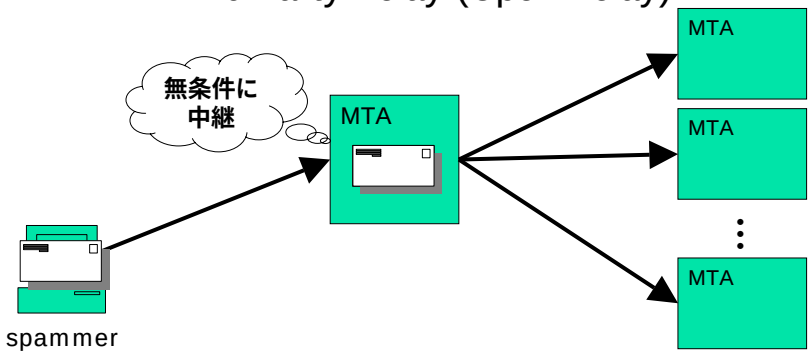
Spamメール対策の基礎知識

Spammerの手口(1)

- アドレスの収集
  - 辞書攻撃 (架空アドレスの生成)
    - 使われそうなアドレスに片っ端からメールを送る
      - 人名データ, 英数字の適当な組合せなど
    - 有効なアドレスだけリストに登録
      - 宛先不明エラーになれば, リストから削除
      - HTMLメールを開けば, リストに登録(web bug)
    - MTAへの負荷が非常に大きな問題 (特に携帯電話メール)
  - ハーベスティング (実在アドレスの自動収集)
    - Webページやネットニュースの記事から@を含むものを検索
  - 業者間での売買
    - アドレスを売るspamメールも存在

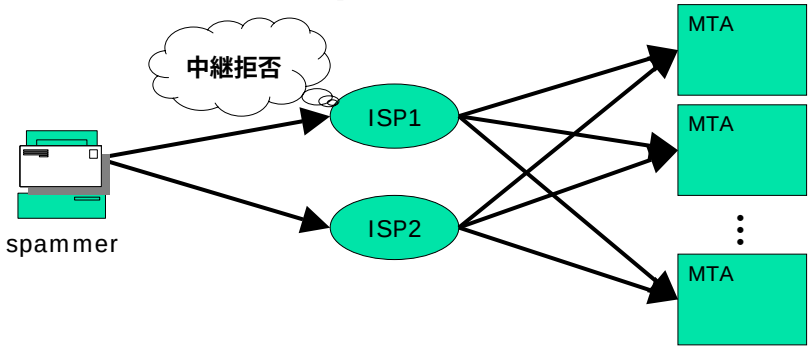
Spammerの手口(2)

- Spamメールの配送(1)
  - Third Party Relay (Open Relay)



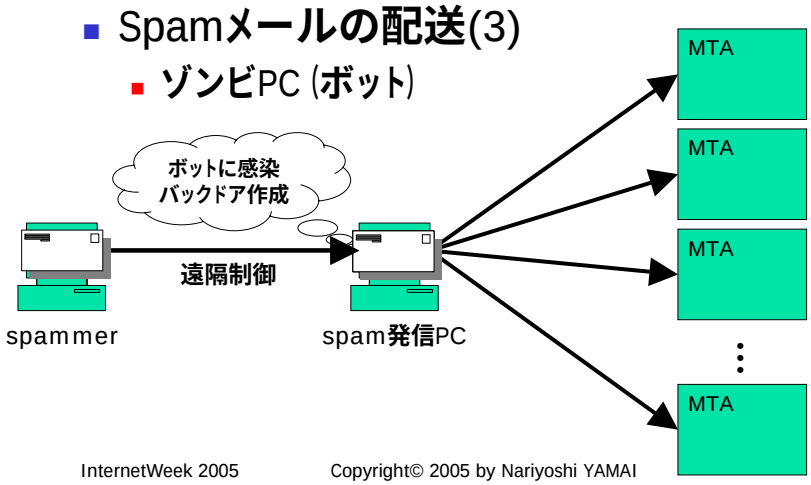
Spammerの手口(3)

- Spamメールの配送(2)
  - ISPの「渡り」



Spammerの手口(4)

- Spamメールの配送(3)
  - ゾンビPC（ボット）



Spammerの手口(5)

- ゾンビPC・ボットに関する話題
  - Spamの60%はゾンビPCから配信
    - Sophos社COO=Steve Munford氏(2005/9/15)
  - 国内のゾンビPCは最低でも40〜50万台
    - JPCERT/CC, Telecom-ISAC Japan(2005/9/8)
  - ボットネットのレンタル価格は1時間で300ドル
    - MX Logic社CTO=Scott Chasin氏(2005/7/13)
  - ボットネットではDNS問合せとspam配送が分業化
    - APCAUSE Chair=James Lick氏(2005/2/24)

Spamメールへの対策

- アドレス収集対策
  - 辞書攻撃対策
  - ハーベスティング対策
  - 法的対策
- Spamメール受信対策
  - ブロッキング・スロットリング
  - フィルタリング
  - バウンスメール対策
  - 送信ドメイン認証
- Spamメール発信対策
  - 課金
  - ISPでのブロッキング
  - 法的対策

アドレス収集対策(1)

- 辞書攻撃への対策
  - 攻撃元を遮断
  - バウンスメール(エラーメール)を返さない
  - 最近は携帯電話メールで実施
- ハーベスティングへの対策
  - Webページにアドレスを掲載しない
  - 掲載する場合には検索されないよう工夫する
    - 画像として表現
    - @をatなどで表現(例：yamai at okayama-u.ac.jp)

アドレス収集対策(2)

- 法的対策
  - CAN-SPAM法(米国，2004年1月施行)
    Controlling the Assault of Non-Solicited Pornography and Marketing Act
    - 自動的なアドレス収集･発信用アドレスの取得を禁止
    - 罰則規定あり
  - 特定電子メール法(日本，平成14年7月施行)
    - 辞書攻撃を禁止
    - 罰則規定あり
      - 違反者には総務大臣による措置（是正）命令
      - 措置命令に従わないときには50万円以下の罰金

Spamメール受信対策

- ブロッキング･スロットリング
  - Spamメールの受信を拒否
- フィルタリング
  - Spamメール受信後に内容により判断
- バウンスメール対策
  - 発信者詐称spamメールによるDoS攻撃を防御
- 送信ドメイン認証
  - 送信者（ドメイン）の詐称を受信側で判別

受信対策の性能評価基準

- 代表的な2つの評価基準
  - 見逃し率 (false negative rate)
    - spamメールを通常(ham)メールと判断する割合
    - 検出率 (spamメールを正しく判断する割合) と等価
  - 誤検出率 (false positive rate)
    - 通常(ham)メールをspamメールと判断する割合
- 重要なのはfalse positive rate
  - 見逃したspamメールは単に削除すればよい
  - 重要なメールがspamと判定されると影響大

ブロッキング(1)

- 発信者アドレスの存在確認
  - DNSを用いて発信者ドメインの存在を確認
  - 実在するドメイン名に詐称されると効果なし
    - 通常メールでも発信ホストと発信者アドレスが不一致の場合あり
  - 本来であれば不要な通信が発生
  - ネットワークが不安定だと，通常メールでも受信を拒否する場合あり

ブロッキング(2)

- IPアドレスの逆引き
  - 失敗すれば受信拒否
  - 成功すれば別の検査を実施
    - 例えば，IPアドレスを含むようなホスト名なら拒否
  - 本来であれば不要な通信が発生
    - 場合によってはパラノイド検査が必要
  - ネットワークが不安定だと，通常メールでも受信を拒否する場合あり
  - PTRレコードがないMTAもかなり多い

ブロッキング(3)

- ブラックリストサービス
  - 代表例
    - Spamhaus SBL, XBL (http://www.spamhaus.org)
    - SpamCop SCBL (http://www.spamcop.net/bl.shtml)
    - ORDB (http://ordb.org/)
    - DSBL (http://dsbl.org/main)
  - DNSを利用 (DNSBL: DNS Black List)
    - spamメール発信ホスト，open relayホストなどを登録
    - 登録ホストからのメールは無条件で受信拒否するようにMTAを設定

ブロッキング(4)

- ブラックリストサービス（続き）
  - 使用例(Spamhaus SBL, XBLの場合)
    - IPアドレスがA.B.C.DのMTAからSMTP接続
    - D.C.B.A.sbl-xbl.spamhaus.orgのAレコードを検索
    - Aレコード(127.0.0.x)が得られれば，接続を拒否
  - トラブルも多い
    - 登録ホストからは通常メールも（ある日突然）拒否
    - 対策完了後も復旧に時間を要するものもある
    - 一部は訴訟にまで発展

ブロッキング(5)

- Tempfailing
  - 「Spam発信MTAは再送をしない」との仮説に基づく方法
    - 一時的に受信を拒否
    - 再送されれば受信
    - 殆どのspam発信MTAは仮説どおりに動作
  - 代表例
    - お馴染みさん方式
    - Greylisting

ブロッキング(6)

- Tempfailing(続き)
  - かなり効果的
  - 欠点も多少ある
    - 配送遅延が結構大きい
      - 再送まで1時間のものもある
    - 再送しないMTAがある
      - 一部のファイアウォール
      - 一部のオンライン予約システムなど
    - ホワイトリスト(信頼するMTAリスト)の管理が必要

ブロッキング(7)

- 自動認識つきホワイトリスト
  - プログラムがspamメールを送信する点を利用
    - 初めての相手には再送要求メッセージを返送
    - 再送されればホワイトリストに登録して配送
  - 長所
    - 人間相手には非常に効果的
  - 短所
    - 送信元が正当なプログラムな場合には適用不可
      - オンライン予約システムなど
    - 第三者(詐称された送信者)に再送要求メッセージを配送
      - バウンスメール（エラーメール）による攻撃と同じ

スロットリング(1)

- 「spam発信MTAはtimeoutが短い」との仮説に基づく方法
  - コネクション確立後の最初の応答 (220 greeting message) を遅延
    - sendmailでは8.13より対応
    - RFC2821では送信側は5分間待つべきと規定
  - 応答を待たずに送信するMTAも拒否
    - 時間は15秒程度でもかなりの効果あり

スロットリング(2)

- Tempfailとの比較
  - 性能はtempfailのほうがよい(?)
    - 少なくともスロットリングで拒否できず greylistingでは拒否できるものがかなりある
    - 遅延時間にも影響
  - 設定が簡単
    - 再送かどうかの判定が不要
  - 適用範囲が広い
  - 配送遅延が小さい

フィルタリング(1)

- 基本方針
  - メール受信後にspamメールかどうかを判断
  - spamメールは削除あるいは別に格納
- 代表的な方法
  - ルールベースフィルタリング
  - ベイジアンフィルタリング
  - 協調分散型spamデータベース

フィルタリング(2)

- ルールベースフィルタ
  - spamメールの特徴をルールとして記述
    - 単純なパターンマッチング
      - 本文中に「$」「Viagra」など特定のキーワードを含む
    - ヒューリスティック
      - 長い英単語がある，FromとToが同じアドレスなど
  - マッチした場合，ルールに対応したスコアを加算
  - 一定のスコア以上のものをspamと判定
  - 欠点=柔軟性の欠如
    - スコアの調整は可能だが限界が存在
    - 新たな手口には新たなルールが必要

フィルタリング(3)

- ベイジアンフィルタ(Bayesian filter)
  - キーワード(単語，3字組等)の出現率を学習
  - キーワードの種類に応じてspamメールを判定
  - ベイズ則 P(A|B)= P(A)P(B|A)/P(B)を利用
    - 事象A･･･メッセージがspamメールである
    - 事象B･･･メッセージがキーワードを含む
  - 有効なキーワードの例
    - ff0000 … HTMLメールにおける赤色指定
  - 新しい手口にもある程度対応可能
    - 但し，学習が必要
    - 最近は対応できないような回避策がいろいろ使われている

フィルタリング(4)

- 分散協調型spamデータベース
  - 既に判定済みのspamメールの再受信を排除
    - 同一メッセージが多数の利用者に(何回も)配送されることを逆利用
  - 利用者がspamメールをデータベースに登録
  - メール受信時に同一メッセージの存在を問合せ
    - 一定数以上の登録があればspamメールと判定
  - spamメールの認識率が低い点が問題
    - 登録までのタイムラグあり
    - 内容の一部変更に弱い ⇒ fuzzy checksum

フィルタリング(5)

- Spammer側のフィルタリング回避策
  - 十分にフィルタリング技法を研究
    - 単語を分割
    - ランダムな単語の挿入
    - 背景と同じ色での単語埋込み
    - 普通のニュース記事への誘導先URLの挿入
    - バウンスメールへの擬装
    - サーチエンジン検索URLの埋込み
      - 検索結果の先頭に誘導先URLが表示されるようなリンク

フィルタリング(6)

- フィルタリング側での対策
  - 複数の技法の組合せ
    - 多いものでは10種類の技法を利用
  - フィルタリング技法の秘匿化
    - Spammerに回避策のヒントを与えない
  - ハニーポットの活用
    - おとりのアドレスにspamメールを誘導
    - ゾンビPCのハニーポットを仕掛けることも

バウンスメール対策(1)

- バウンスメールの集中
  1. Spamメールが大量に配送
  2. そのうちの相当数の宛先不明
  3. エンベロープFrom宛にバウンスメールが返送
  4. 特定のアドレスが発信者として使われると…
  5. バウンスメールが特定のMTAに集中
  6. MTAが過負荷となり通常メールの配送に影響

バウンスメール対策(2)

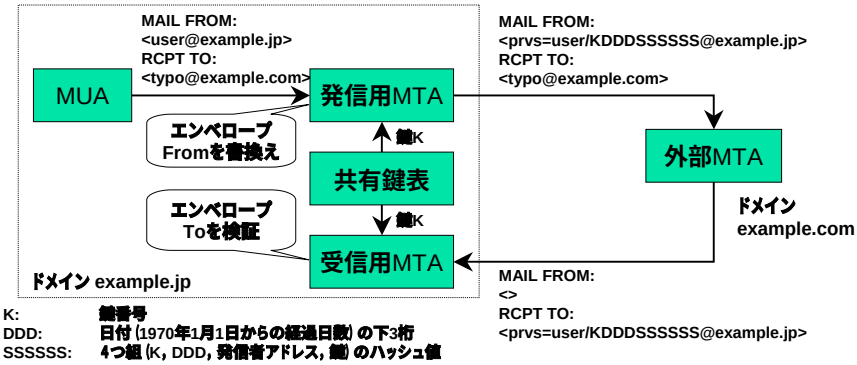
- 発生頻度と影響
  - 発生頻度小
    - 詐称アドレスが自組織ドメインの場合のみ発生
  - 発生時の影響大
    - MTA・ネットワークの過負荷
    - ディスクの大量消費(詐称アドレス実在の場合)
    - Spam発信者との嫌疑を受ける
    - 苦情への対処も必要
  - 事実上のサービス不能(DoS)攻撃
    - “Joe job”とも呼ばれる

バウンスメール対策(3)

- 2002年11月に国内ISPで発生した事例
  - 30万通以上のエラーメールが集中
  - 通常メールの配送遅延は最大15時間
  - 復旧に約2.5日間
    - 11/5 9:30am 〜 11/7 11:00pm
  - 恐らく実在アドレス
    - アドレスリスト中に含まれるものと推察

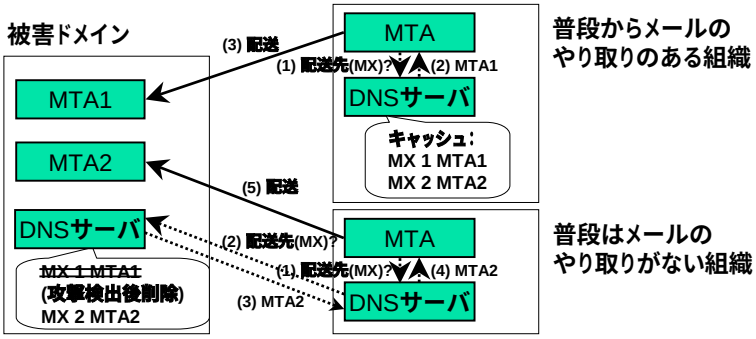
バウンスメール対策(4)

- バウンスメールの正当性検証
  - BATV (Bounce Address Tag Validation)



バウンスメール対策(5)

- DNSを利用した負荷分散
  - MXレコードのキャッシュ有無を利用



送信ドメイン認証(1)

- 発信者ドメインの詐称を識別する手段
  - ローカルパートの詐称は対象外
    - 必要なら発信者認証を活用
  - メッセージの中身も対象外
    - Spamメールを受け取ることもあり得る
- 問題発生時の追跡が目的
  - Spamメールを受け取ったときの苦情先
  - フィッシング詐欺の抑止

送信ドメイン認証(2)

- 2種類の方法
  - IPアドレスに基づく認証
    - Sender ID = SPF + Caller ID
      - SPF (Sender Policy Framework) ･･･ POBOX
      - Caller ID ･･･ Microsoft
  - デジタル署名を利用した認証
    - DKIM = DomainKeys + IIM
      - DomainKeys ･･･ Yahoo!
      - IIM (Identified Internet Mail) ･･･ Cisco Systems

送信ドメイン認証(3)

- Sender ID(1)
  - 3種類の要素により構成
    - ヘッダ内の送信者の認証(PRA)
    - エンベロープFromの認証(MFROM)
    - 送信側ドメインのポリシー定義(SPFレコード)

送信ドメイン認証(3)

- Sender ID(2)
  - PRA (Purported Responsible Address)
    - 責任があるとされるアドレス
      - Resent-Sender:, Resent-From:, Sender:, From:の順
      - 転送する場合には, Resent-From:などを追加
    - MAILコマンドのSUBMITTERオプションも利用可能
      - 本文を受け取る前に判定するため

例:
```
MAIL FROM: <alice@example.com> SUBMITTER=<alice@example.jp>
```


送信ドメイン認証(4)

- Sender ID(3)
  - SPFレコード
    - DNSのTXT (SPF)レコードで送信サーバを宣言
      - \+ pass (受信許可)
      - ? neutral (宣言なしと同様)
      - ~ softfail (neutralとfailの中間)
      - \- fail (受信拒否)
    - 例: AレコードかMXレコードに対応するIPアドレスを持つMTAからのみ送信可能な場合

```
example.jp  IN TXT  "v=spf1 +a +mx -all"
example.jp  IN SPF  "spf2.0/mfrom,pra +a +mx -all"
```


送信ドメイン認証(5)

- Sender ID(4)
  - Sender IDに関する話題
    - MicrosoftがPRAに対して知的所有権を主張
      - 特許料は取らないがライセンス契約が必要など
    - IETFでのワーキンググループが余波を受け解散
      - MARID (MTA Authorization Records in DNS) WG
    - RFCにも影響
      - 強制力のあるStandardではなくExperimentalに

送信ドメイン認証(6)

- DKIM (DomainKeys Identified Mail)
  - 公開鍵暗号方式を利用
    - 送信側
      - 秘密鍵を使って署名
    - 受信側
      - DNSを用いて公開鍵を取得
      - 公開鍵を使って署名を検証

送信ドメイン認証(7)

- DKIM (続き)
  - 署名つきヘッダの例

```
DKIM-Signature: a=rsa-sha1; s=brisbane; d=example.com;
                    ↑アルゴリズム    ↑セレクタ       ↑ドメイン
   c=simple; q=dns; i=joe@football.example.com;
    ↑正規化方法 ↑公開鍵入手法      ↑ユーザ名
   h=Received : From : To : Subject : Date : Message-ID;
    ↑ 署名対象に含めるヘッダフィールド ↓署名
   b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR;
```

  - DNSの設定例

```
brisbane._dkim.example.com.       IN TXT   "g=¥; k=rsa¥; t=y¥; p=MIGfMA
0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC69TURXN3oNfz+G/m3g5rt4P6nsKmVgU1D6cw2X
6BnxKJNlQKm10f8tMx6P6bN7juTR1BeD8ubaGqtzm2rWK4LiMJqhoQcwQziGbK1zp/MkdXZ
EWMCflLY6oUITrivK7JNOLXtZbdxJG2y/RAHGswKKyVhSP9niRsZF/IBr5p8uQIDAQAB"
```


送信ドメイン認証(8)

- 2つの認証方式の選択
  - IPアドレスに基づく認証
    - ヘッダや本文の書換えに強い
    - 転送に弱い
      - PRA, MFROMが維持できるかどうかが問題
  - デジタル署名を利用した認証
    - 転送に強い
    - ヘッダや本文の書換えに弱い

⇒相補的に利用することが重要

送信ドメイン認証(9)

- 普及後の問題点
  - 既にspammerは送信ドメイン認証に対応
    - 単に認証するだけでは問題
  - 認証後の判定が重要に
    - 認定(accreditation)サービス
      - 信頼のある機関に公的に認定してもらう
    - 評価(reputation)サービス
      - Spamメールを大量に発信すると評価が下がる

Spamメール発信対策

- Spamメール発信対策
  - 課金
    - 送信者に対するコスト負担
  - ISPでのブロッキング
    - ISP利用者からのspamメール発信抑制
  - 法的対策
    - Spamメール発信者への罰則

課金(1)

- 送信者にコスト負担をさせる仕組み
  - 普通の利用者には負担を軽くする必要あり
    - メーリングリスト運用者が問題
  - 効果は未知数
    - 宣伝効果が高ければコストを多少負担しても送信
    - 例：携帯電話メールからのspamメール発信

課金(2)

- 電子切手(E-Postage)
  - いくつかの方式が提案
  - 送信時には電子切手を添付
  - 受信時には電子切手を検証
  - 受信後に換金・返金できるものも存在

課金(3)

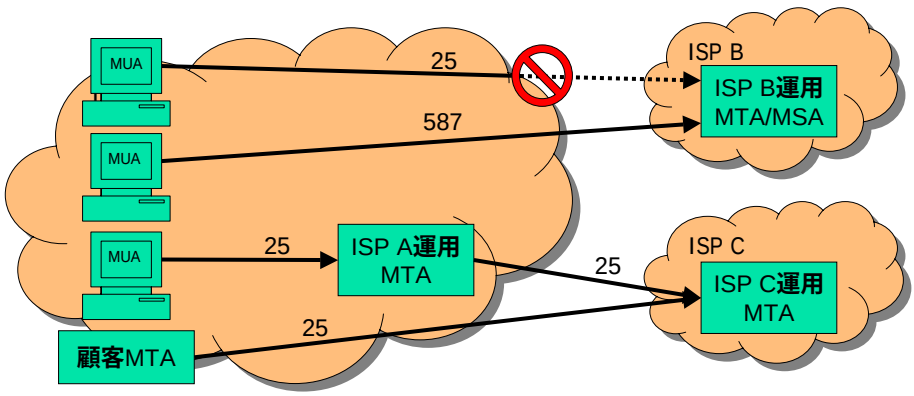
- 供託金制度
  - 例：Bonded Sender Program (BSP)
    - IronPort Systems社が実施
  - 仕組み
    - 送信者がBSPに供託金を拠出
    - 受信者はBSP登録MTAからのメールは信用
    - Spamメールの受信者はBSPに苦情
    - 苦情があれば供託金から引き落とし
    - さらに悪化すれば登録抹消

ISPでのブロッキング(1)

- Outbound Port 25 Blocking (OP25B)
  - 自網からのspamメール発信防止が目的
    - Spammerやゾンビ PCが対象
    - 普通の電子メール発信は対象外
  - 方法
    - 自網→外部MTAへのSMTP(25番)をブロック
    - 他社MTAの利用者には代替ポートの利用を推奨
      - Submission(587番), SMTP/SSL(465番)
    - 一般利用者は自社ISP運用のMTAを利用
    - 自網内の顧客MTAは固定IPアドレスで対応
      - 当該IPアドレスのみブロックを解除

ISPでのブロッキング(2)

- Outbound Port 25 Blocking (2)



ISPでのブロッキング(3)

- Outbound Port 25 Blocking (3)
  - 最近ではISP各社が連携して導入を検討
    - 「渡り」防止のため
  - 問題点
    - 自社ISP以外のMTA(25番ポート)が利用できない
    - 代替ポートが利用可能なら大丈夫
      - 但し，設定変更が必要
    - 代替ポートが利用不可能なところが多い
      - 特に大学，中小企業が問題かも

ISPでのブロッキング(4)

- ISPでのスロットリング
  - 外部MTAに対するメール発信を制限
    - 帯域を制限
    - 応答を遅延
    - 同時送信数を制限
    - 単位時間当たりの発信件数を制限
      - 特に携帯電話メールで採用
  - SMTP通信量や宛先不明メール数に応じた制限も可能
  - Outbound Port 25 Blockingとの併用も有効

法的対策(1)

- 技術的なspamメール対策の限界
  - ブロッキング・フィルタリングでは spamメール発信者は不利益を被らない

  ⇒何らかの法的な対策が必要
- 法的なspamメール対策の実施国
  - 日本
  - アメリカ合衆国
  - EU
  - オーストラリア
  - 韓国など

法的対策(2)

- 日本における法律
  - 迷惑メール対策法(2002年7月施行)
    - 特定商取引に関する法律の一部を改正する法律
      (特定商取引法)
    - 特定電子メールの送信の適正化に関する法律
      (特定電子メール法)

  ※ 広告メールを全面的に禁止するものではない
  (オプトアウト方式)
    - 広告は企業活動にとって必要
    - CM, ダイレクトメールとの比較

法的対策(3)

- 迷惑メール対策法の比較

法律名	改正特定商取引法	特定電子メール法
担当官庁	経済産業省	総務省
規制対象	事業者	メール発信者
表示義務	1. メールアドレス 2. 未承諾広告※ 3. オプトアウト方法	1. 未承諾広告※ 2. 氏名・住所 3. 発信アドレス 4. 受信アドレス
禁止事項	拒否者への送信	・拒否者への送信 ・架空アドレスへの送信
罰則	・2年以下の懲役 ・300万円(法人は2億円)以下の罰金	50万円以下の罰金

法的対策(4)

- 迷惑メール対策法の効果 ⇒ 殆どなし
  - 殆どの広告メールは表示義務に違反
    - 違反者の調査が困難
      - 発信者情報の欠落
      - 多くの場合，ゾンビPCから発信 ⇒ 追跡が困難
    - 違反しても直ちには処罰されない
      - 措置命令に違反した場合に初めて罰金･懲役
  - 平成15年10月9日に初めて2社が行政処分
    - 件名に「未承諾広告※」「※未詳諾広告※」などと表示
    - 平成14年8月頃から平成15年9月頃まで発信
    - 平成15年6月以降は送信者情報表示義務にも違反

法的対策(5)

- 迷惑メール対策法の効果(続き)
  - 総務省･経済産業省の合計で10件程度
    - Spamメール発信で初の逮捕者(2005/5/16)
      - 容疑は「有線電気通信法」
      - メールサーバに過負荷を与えたため
    - Spamメール発信で初の業務停止命令(2005/6/14)
      - 同一人物が運営する2社
      - 特定商取引法違反（表示義務違反）
  - 罰金･懲役刑は適用例なし

法的対策(6)

- 迷惑メール対策法の効果（続き）
  - 多数の抜け道が存在
    - 登録者への送信は規制の対象外
      - 登録会員への送信を装う
    - 広告メールが対象
      - 友人からの情報交換メールを装い，URLのみ表記

⇒「優良」迷惑メールしか効果なし

- 「正直者が馬鹿を見る」状態

法的対策(7)

- 特定電子メール法の改正(平成17年11月1日施行)
  - 改正のポイント
    - 特定電子メールの範囲の拡大
      - 個人用⇒企業等の事業用メールアドレスも含む
    - 架空アドレス宛メール送信を禁止する範囲の拡大
      - 空メール，友人を装ったメール等も含む
      - 措置命令違反に対する罰則も強化
        - 罰金(～50万円)⇒懲役(～1年)または罰金(～100万円)
    - 発信者詐称は直罰の対象⇒追跡が可能
      - 表示義務違反は措置命令のみ
    - 電気通信事業者による役務提供拒否事由の拡大
      - 設備に著しい障害⇒メール配信が大幅に遅延する恐れも含む

法的対策(8)

- 米国での迷惑メール対策法
  - CAN-SPAM法(2004年1月施行)
    - 表示義務
      - オプトアウト方法の提示
      - 有効な返信アドレス
      - 広告メールの表示
    - 禁止事項
      - 発信元詐称
      - 偽の件名の表示
      - 自動的なアドレス収集・発信用アドレスの取得
      - ラベルを含まない「性的内容が中心の素材」の発信
    - 罰則あり

法的対策(9)

- 米国での迷惑メール対策法(続き)
  - 条件を満たすspamメール発信は合法
    - spam業者にとってはクリスマスプレゼント
  - 州法に優先
    - カリフォルニア州(2004年1月施行)など36州で制定
      - より強力なオプトイン（事前登録）方式が事実上無効に
      - 但し，オプトイン方式は合衆国憲法に反するとの指摘あり
  - CAN-SPAMは事実上 “You CAN SPAM”
    - 本当はControlling the Assault of Non-Solicited Pornography and Marketing Act

法的対策(10)

- EUでの迷惑メール対策法
  - 2003年10月31日発効
  - 原則的にはオプトイン方式
    - 国内法も遵守する必要あり
  - マーケティング業者やプロバイダが対処に苦慮
  - 効果は不明

法的対策(11)

- まとめ
  - オプトアウトとオプトイン
    - 「表現の自由」「検閲の禁止」との兼ね合い
    - ユーザあるいは優良業者のいずれかが苦慮
  - 国外から来るspamメールへの効果
    - 国際法なし
    - 国により規制がばらばら
  - 効果は疑問だが，規制は必要
    - 現在は「正直者が馬鹿を見る」状態
    - 特定電子メール法の改正の効果に期待

おわりに(1)

- 手口の巧妙化
  - ウィルス作者とのspammerとの結託
  - 多くのゾンビPCから少量のspamメール
- 内容の悪質化
  - 単なる宣伝からフィッシング，スパイウェアなど
- 多方面からの取組みが必要
  - ブロッキング，フィルタリング，法律
  - 計算機におけるセキュリティ対策･ウィルス対策
- 国際的な枠組みが必要
  - 国外からのspamメールへの対処

おわりに(2)

- 今後はアジア(特にCJK)が問題か
  - 現在のフィルタリングは殆ど英語が対象
  - 現実に中国･台湾からのspamメールは多い
  - 韓国は既にspam大国
    - ISPが自衛のためフィルタリング

⇒ 皆さんの活躍に期待

おわりに(3)

- Anti-spamメーリングリスト
  - 主にspam関連のニュース記事を報告
  - 現在のところ週に1通程度
  - anti-spam-request@cc.okayama-u.ac.jp 宛に以下の内容のメールを送信

    subscribe
    end