IPv6時代の迷惑メール対策

2011年5月27日

迷惑メール対策委員会委員長
IPv6ディプロイメント委員会委員
樋口貴章

インターネット協会 迷惑メール対策委員会

- インターネット協会は2001年に設立された財団法人。
  - 賛助会員88社(2011年4月25日現在)
- 迷惑メール対策委員会
  - 2004年に設立
  - メンバーはISPの他、大学、企業関係者、それらにサービスを提供するSIerなど。
  - 2005年以降、毎年迷惑メールカンファレンスを主催、地方セミナーも開催
  - 迷惑メール対策ポータルサイトを提供
  - オーストラリアや中国のインターネット協会とも交流、提携、国際的な迷惑メール対策の活動にも参加

カンファレンス/セミナー活動

- 迷惑メール対策カンファレンス
  - 年に1回、東京にて開催
- 地方セミナー
  - 年に2回程度
- 迷惑メール対策技術や法対策に関する最新動向・情報提供中心
  - 技術: OP25Bや送信ドメイン認証技術の普及推進
    - JEAG/JAIPA/日本データ通信協会など関連団体と協力
  - 法対策: 法改正のポイント解説など
    - 総務省/経済産業省/消費者庁などの協力

迷惑メール対策ポータル

- 有害情報対策ポータルサイト 迷惑メール対策編
  - http://salt.iajapan.org/wpmu/anti_spam/
  - メール管理者向け
    - 技術情報
      - 送信ドメイン認証解説
      - 関連RFCの翻訳
    - 運用情報
    - 法令情報
  - 一般利用者向け
    - メールリーダー設定方法など

国際活動

- 主にアジア太平洋地域での国際交流活動
  - APCAUCE(Asia Pacific Coalition Against Unsolicited Commercial Email)
  - 中国インターネット協会
  - APRICOT(Asia Pacific Regional Internet Conference on Operational Technologies)

IPv6

- IPv4アドレス枯渇に伴い、2011年からIPv6の普及が見込まれる
  - 現時点ではIPv6を利用した迷惑メール送信は観測されていない
  - 今後、IPv6を利用した迷惑メール送信が増加してくる場合、どのような対応が考えられるか？
- IPv6上で問題無い迷惑メール対策技術
  - OP25B(outbound port 25 block)
  - SPF: IPv6オプションがあり、規格上、既に対応済
  - DKIM: 電子署名なので、IPとは直接関係しない
  - 上記技術はIPv6上でも普及推進を継続

IPv6

- 迷惑メール対策技術との関係で問題ありそうなこと
  - 逆引き
    - 逆引きできないメールの受信拒否は可能か？
      - IPv6ディプロイメント委員会の見解
        - メールサーバーに関しては、IPv4と同様、逆引きを設定することが多いと想定
      - 迷惑メール対策委員会としての推奨
        - IPv6移行の際には**メールサーバーの逆引き設定を必須**と考えていただきたい
    - 総務省/消費者庁のモニターアカウントで受信した迷惑メールの分析
      - IPアドレスを用いて分析しているがIPv4アドレスが前提
      - IPv6ではブロック単位でISPを特定できるので、処理プログラムの更改は必要となるが、分析は引き続き可能

IPv6

- 迷惑メール対策技術との関係で問題ありそうなこと
  - IPv6普及における一般的な問題点が関連する技術
    - IPv4アドレスを前提としたプログラムでは対応できない
      - データ長(32bitを前提)
      - データ形式(192.168.1.1などの形式を前提)
    - 例えば
      - DNSBL
      - Greylisting

IPv6とDNSBL

- DNSBL
  - 迷惑メール送信システムのIPアドレスをブラックリストデータベース登録し、DNSを利用して参照するサービス
  - これまでIPv4アドレスを前提とした運用が行われている。
- IPv6に対する問題点
  - IPアドレスが128bitに拡張されるため、
    - データベースに登録するIPアドレスのデータ長がIPv4(32bit)と比べて4倍になる
    - データベースに登録するIPアドレスのデータ空間はIPv4と比べて膨大になる
    - IPv6アドレスを登録することに意味があるのか。
      - IPv6アドレスは通常上位64bitをプロバイダーから割り当てられる運用を想定している。この場合、下位64bitを一秒に一個ずつ変更しながら迷惑メールを送信すると、全部のアドレスを使い切るのに5800億年くらいかかる

IPv6とDNSBL

- IPv6に対応したDNSBLはあるか、どう対処しているか
  - Spamhaus
    - ホワイトリストで対応
      - SBL: IPv4アドレスとIPv6アドレスの両方をサポート
      - DBL: DKIMを使用しているドメインのリスト
      - ホワイトリストはどの程度有用か？

IPv6とDNSBL

- IPv6に対応したDNSBLはあるか、どう対処しているか
  - Virbl
    - http://virbl.bit.nl/
      - 2010年1月15日からIPv6対応
      - ポリシー
        - ホスト単位で登録
        - 同じ/64を持つアドレス5つを確認した場合、その/64全体もBL登録する
        - IPv6ホスティングサービスなどで「お隣さん問題」が起きる可能性
      - 今のところの統計情報では(2011/5/20)
        - IPv6 hosts on virbl: **0**

Greylisting

- Greylisting
  - Botからの迷惑メールは再送されないと言う前提
    - 初めてメールを受けるホストからの受信を一度拒否。IPアドレスをグレイリストに登録。
    - 再送してきた場合には、正規のメールサーバーとして受信。IPアドレスをホワイトリストに登録。
  - IPアドレスに依存した処理なので、プログラム側のIPv6対応が必要
    - 対応済みのものは存在している
      - milter grey-list home page
        - http://hcpnet.free.fr/milter-greylist/
      - Greylisting for qmail with IPv6 support
        - http://gurubert.de/greylisting
  - IPv6に対応したGreylisting処理の有効性は今後の検証待ち

現時点では

- IPv6上の迷惑メール対策のディレンマ
  - IPv6経由の迷惑メールはほとんど無い
  - 今後の増加は必然
  - 増えて来てからでないと対策の有効性を検証できない
- できれば増えて欲しくない
  - IPv6でも有効な技術の積極的な導入を
    - OP25B
    - メールサーバーの逆引き設定
    - 送信ドメイン認証(SPF/DKIM)