IA japan

あらためて
送信ドメイン認証技術を考える

2011年11月25日

(財)インターネット協会

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/dkim.jp/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

送信ドメイン認証技術の目的

IA japan

- 迷惑メールフィルタ技術は・・・
  - 受信したメールの本文(テキスト)を分析して迷惑メールフォルダに振り分ける
  - 受信する迷惑メールの数そのものを減らすものでは無い
  - できれば、迷惑メールを元から絶ちたい
- 送信ドメイン認証技術で元から絶てるのか？
  - もともとの英語ではSender Authentication
    - Senderを送信者と訳して、送信者認証と呼ばれていたこともあった
    - Senderが意味するものは、送信元のMTA
    - 送信元のドメインを認証するものなので、2005年の迷惑メール対策カンファレンスで、用語としては送信ドメイン認証を使うように呼びかけ
- ボットネットの遮断
  - 迷惑メールを元から絶つのに即効的な手段と言えるが、いたちごっこかも

•SPF/Sender IDとDKIM

IA japan

- **SPF/Sender ID**
  - 送信MTAのIPアドレスを認証
  - 送信側ドメインのDNSレコードにSPFレコードを記述
    - JPドメインでの普及率は42%くらい
  - 受信側ではDNSを用いてSPFレコードを参照
- **DKIM**
  - 送信MTAで送信メールに電子署名を付与
    - 技術的な敷居が高そうに見えるためか、JPドメインでの普及率は低い
  - 受信側ではDNSを用いて公開鍵を参照
- **SPF/Sender ID vs DKIM？**
  - 両者は共存可能、補完し合う技術

認証の次は評価(reputation)

IA japan

- IETF
  - DKIM WGは活動完了
  - Reputation WGが活動中
    - ドメイン評価の標準化を議論
- Reputation
  - 送信ドメイン認証技術で、送信元ドメインが確定できたとしても、送信元ドメインの評価は単純に〇か×かというわけにはいかない
    - 一般企業などは〇でいいかもしれない
    - ISPの場合、〇のユーザーが大半だが、×のユーザー(スパマー)が入り込む可能性もある
    - 大学などでも学生の中には×なケースもあるかも
  - IPv4アドレス枯渇→IPv6利用増加
    - IPv6ベースではDNSBLの運用に疑問
    - Reputationの役割に期待

送信ドメイン認証技術の目的

IA japan

- 電子メールの送信元を追跡可能にし、なりすましメールをなくす
- 発信元を認証できた電子メールは、認証できないメールよりも評価を高くする
  - たとえばGmailのプライオリティinboxのように
  - 迷惑メールに埋もれて重要なメールを見失わないようにできる

財団法人インターネット協会

http://www.iajapan.org/