Internet Initiative Japan

Japan Email Anti-Abuse Group

Internet Initiative Japan Inc.

JEAG Recommendation (送信ドメイン認証)

～第3回 迷惑メール対策カンファレンス～

櫻庭 秀次

(株)インターネットイニシアティブ / JEAG

Copyright © 2006 Internet Initiative Japan Inc.

迷惑メールの問題点

- 不要なメールを受信するコスト
  - ハードウェアおよびネットワーク設備 (メール受信および保管)
  - 内容確認と削除のための時間
- 直接的な被害
  - 従来の 広告メール→商品購入 といった間接的なビジネスモデルからより犯罪性の高いビジネスモデルへの転換
  - phishing や spyware による個人情報の取得
  - これらのトリガとしてのメールの悪用
- 不快・公序良俗に反するような内容
  - 送信者の目的の第一歩はまず読んでもらうこと，そのため内容を工夫したり画像を添付するなどより過激に
  - メールは多様な人が利用する社会基盤の一部
- メール経由によるウイルス感染でのボット化
  - 被害者から知らない間に加害者側に
- 送信者を詐称されることによる実害
  - イメージダウン
  - エラーメール (bounce mail) による被害

Copyright © 2006 Internet Initiative Japan Inc.

迷惑メールの特徴

- 送信者情報を詐称している
- 送信元が固定的でなくなっている (ボットネット経由が主流)
- 画像の利用，内容の巧妙化によるフィルタの回避

→ 単純なブラックリストやフィルタでは対応が難しくなっている

Copyright © 2006 Internet Initiative Japan Inc.

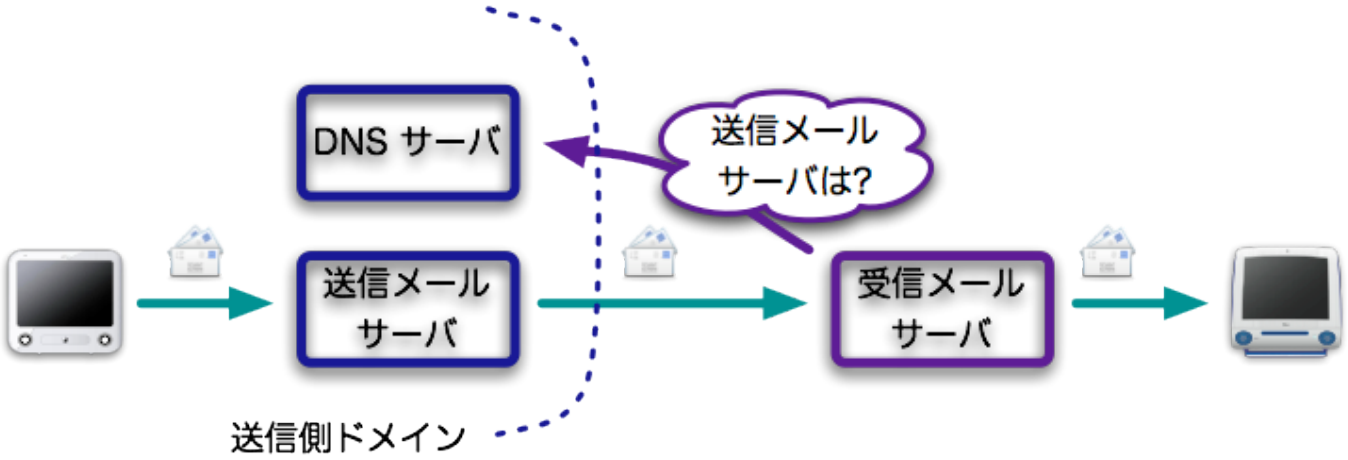
迷惑メール対策のために

- 送信者情報を詐称できないような仕組みをまず導入すべき
  → 送信ドメイン認証技術
- 送り元が明確になれば対策し易くなる
  - 送信者の管理元 (ISP, 企業等) への連絡
  - 特定の送信元を受信拒否
- 正規の送信元からのメールを正しく受信できる
  - 迷惑メールにまぎれた正規メールの取りこぼしを防止
  - 正規のものはフィルタ処理を軽減し優先受信等も可能

Copyright © 2006 Internet Initiative Japan Inc.

送信ドメイン認証の概要

- 送り手側は送信元情報を明確にする
- 受け手側は送信元によって峻別する
  - 不確かなものは詳しくフィルタリング処理
  - 明確なものはさらに信頼できる送り手かを判断 (reputation)
- 送信ドメイン認証技術の特徴
  - 既存のメール配送の仕組みを変えることなく上位互換的に実現
  - 送信元情報はドメイン名単位で判断 (DNS との連携)



Copyright © 2006 Internet Initiative Japan Inc.

送信ドメイン認証技術

- 二つの代表的な方式
  - 送信元をネットワーク的に判断 (SPF: Sender Policy Framework)
  - 送信時に電子署名をメールに付加 (DKIM: DomainKeys Identified Mail)

- 特徴
  - 取り出す送信者情報の種類，認証の方式に違いがある
  - 導入のコスト (特に送信者側) に大きな差がある
  - それぞれ長所と短所を持ち相互補完的に利用可能
  - 既存の電子署名技術 (S/MIME, PGP/MIME) との違い
    - 利用者個人 (MUA) での対応が主流 → メールサーバ (MTA) での対応
    - 公開鍵利用の信用モデルの問題 → ドメインを管理する DNS を利用

Copyright © 2006 Internet Initiative Japan Inc.

普及にむけて

- メール送信側でまず導入すべき
  送信側の導入増 → 受信側の判断が容易 → 導入しない送信元は不利
  → 送信側の導入増
- 送信側の SPF の導入は容易
  - DNS への SPF レコード追加で済む
- 利用局面に応じて導入技術を判断
  - それぞれの長所，短所を把握し判断
  - ビジネスとして連絡，情報提供に使うメールは DKIM で
- 既に利用は進みつつある
  - 既に多くの ISP では送信側の対応が済んでいる (ex. JEAG member 企業)
  - 受信側の対応も今後増えるだろう

Copyright © 2006 Internet Initiative Japan Inc.

JEAG Recommend 1

- 送信側ドメインでは以下のいずれかの技術を導入すべき
  - SPF Classic の DNS 宣言
  - DKIM (DomainKeys) の電子署名作成および DNS での宣言

- 解説
  - 全ての送信者が何らかの技術は導入すべき
  - それぞれ長所短所があるためどれか一つだけを推奨できない
  - 単一の技術で送受信側それぞれ揃うことが望ましいが，今後の技術動向等を考慮し長期的に判断することが必要
  - まず今できることから始めるべき

Copyright © 2006 Internet Initiative Japan Inc.

JEAG Recommend 2

- SPF Classic の DNS 宣言
  - SPF レコードの末尾 (正規のメールサーバ以外から送信された場合)

    “~all” もしくは “-all” と宣言すべき
  - メールを送信しないドメインについて

    “v=spf1 -all” と宣言すべき
- 解説
  - “?all” では詐称されていても認証結果が neutral で SPF 宣言していない場合と区別ができない
  - Recommend 5 で softfail (“~all” 時の認証結果) 時に受信拒否を禁止しているので，仮に転送時に softfail となっても捨てられることは無い

Copyright © 2006 Internet Initiative Japan Inc.

JEAG Recommend 3

- SPF の転送問題解決後
  - すみやかに “~all” から “-all” へ移行すべき
- 解説
  - SPF の転送問題は技術的解決の可能性がある
  - 転送の多くはメールボックスの集約等，受信者本人が設定している場合が多く，その場合転送者と受信者が同一 (何らかの設定で回避可能)
  - SPF は本文を受け取る前に認証可能なことが利点 → そもそも不要なメールは受け取りたくない

Copyright © 2006 Internet Initiative Japan Inc.

JEAG Recommend 4

- DKIM の移行時期
  - DomainKeys を利用している場合，DKIM が規格化され次第，速やかに DKIM (DomainKeys Identified Mail) へ移行すべき
- 解説
  - DKIM は DomainKeys と IIM の統合技術で，現在 IETF の DKIM Working Group で標準化作業が行われている
  - 同じような技術が併存するような状況は好ましくないので，運用上も標準技術で統一されることが望ましい

Copyright © 2006 Internet Initiative Japan Inc.

JEAG Recommend 5

- 送信ドメイン認証の結果について
  - 単一の技術での結果が fail (送信元ドメインが詐称された疑いがある) した場合でも受信を拒否すべきではない
  - SPF Classic の Softfail で受信を拒否すべきではない
- 解説
  - 現段階では，それぞれ長所と短所が相互補完の関係にある
  - 単一技術では誤認証が起こりうる
  - SPF Classic の softfail は，利用状況によっては避けられない
  - SPF Classic の softfail を避ける設定には問題がある (Recommend 2)

Copyright © 2006 Internet Initiative Japan Inc.

JEAG Recommend 6

- メーリングリストの運用について
  - メーリングリストサーバは送信ドメイン認証を実施し，投稿者の管理をすべきである
  - メーリングリストサーバは SPF Classic 認証及び DKIM 認証の両方を採用すべきである

- 解説
  - 安易に迷惑メールを大量配信させないためにも，投稿者の認証はきちんと行うべき
  - サービスとして提供しているような場合は，なおさら厳密な仕組みが必要であろう

Copyright © 2006 Internet Initiative Japan Inc.

JEAG Recommend 7

- メーリングリストにおける SPF Classic の利用
  - メーリングリストサーバから参加者へ配送する際の送信元 (envelope From) はメーリングリスト管理者とすべき
  - メーリングリストサーバは，参加者からの投稿時に認証処理を実施すべき

- 解説
  - SPF の転送問題はメーリングリストでは解決可能
  - 送信ドメイン認証以外にも，envelope From を管理者としないと既に問題がある

Copyright © 2006 Internet Initiative Japan Inc.

JEAG Recommend 8

- メーリングリストにおける DKIM の利用
  - メールヘッダ情報や本文を改変する場合は再署名すべき
- 解説
  - DKIM の問題点は，メーリングリスト等による署名対象情報の途中改変でこれを解決することが重要
  - 署名対象情報であるヘッダ情報 (特に Subject: など) や本文を改変 (フッタ等) する場合は再署名すべき

Copyright © 2006 Internet Initiative Japan Inc.

JEAG Recommend 9

- メールマガジンにおける SPF Classic の利用
  - 配送上の送信元 (envelope From) はメールマガジン管理者用アドレスとすべき
- 解説
  - メールマガジン等の多くは，既にその送り方が問題となる場合が多い
  - サービスとして委託をうけて配送する場合も含め，SPF の認証が失敗しないような運用をすべき
  - 宛先不明とならないために，購読者管理をきちんと行うべきで，そのためにも bounce mail の処理は適切にすべき

Copyright © 2006 Internet Initiative Japan Inc.

JEAG Recommend 10

- 第三者サーバの利用
  - 投稿時に SMTP 認証 (SMTP-AUTH) を実施し，投稿ポート (port 587) を利用すべき
  - 配送上の送信元 (envelope From) は自ドメインのアドレスを利用すべき

- 解説
  - メールサーバが踏み台にされないためにも送信者の個別管理を行える SMTP-AUTH を導入すべき
  - 複数のメールアドレスを利用する場合，本来はその都度適切なメールサーバを利用すべき

Copyright © 2006 Internet Initiative Japan Inc.

参考情報 1

- エラーメールについて
  - SPF Classic で Softfail, Fail になったメールで宛先不明なものはエラーメール (bounce mail) を送信しない
- 解説
  - 詐称された側に bounce mail が返る，という問題が発生している
  - SPF の問題点として転送問題があるが，この場合宛先不明となることは考えにくい (転送者と受信者が同一管理者)
  - 今後の実験等による検証が必要

Copyright © 2006 Internet Initiative Japan Inc.

参考情報 2

- メール転送時の envelope From について
  - メール転送時に envelope From を書き換える
  - 転送メールに対するエラーメール (bounce mail) については以下のいずれかで対処する
    - Bounce mail は転送元に保存し，再転送は行わない
    - Bounce mail だけは envelope From を書き換えずに転送する
- 解説
  - SPF 普及のためには転送問題が解決されることが望ましい
  - 全ての転送メールの envelope From を単純に書き換える処理では loop が発生する
  - 通常 bounce mail は envelope From が無い (<>) ので，配送情報から判別することは可能 → 転送処理の挙動を変える
  - 今後の実験等による検証が必要

Copyright © 2006 Internet Initiative Japan Inc.

まとめ

- メールは重要なコミュニケーション基盤
  - 連絡，報告，議論の場，宣伝，情報取得，本人確認手順の一部 (web サービスとの連携)
  - 非同期的な連絡手段
  - 瞬時に相手に届く (携帯電話等モバイル環境で何時でも何所でも)
- 迷惑メールは公害，犯罪の手段としても悪用されている
  - 業界全体で取り組むべき重要な課題
  - 国際的な協調，標準の技術で対策すべき
- ドメイン名はインターネットにおけるブランド
  - 悪用されると評判 (reputation) が下がる
  - 対策は急務 → 送信側で詐称されない対応を実施すべき
- 送信ドメイン認証技術
  - まず DNS に SPF レコードを宣言
  - ビジネスとしてのメール送信には DKIM の導入を

Copyright © 2006 Internet Initiative Japan Inc.