「迷惑メール」時代のメールシステム

2005年7月28日 JANOG16@福岡
株式会社インターネットイニシアティブ
山本　功司
koji@iij.ad.jp

本日の内容

- メールシステムから見た迷惑メールとは
- 迷惑メール対策の現状
- 「迷惑メール」時代のメールシステムにもとめられるもの

メールシステムから見た迷惑メールとは

迷惑メールとは

- 受信者が受け取りたくないと思っているメール
  - 主に受信者の同意を得ずに送られるメール
  - 究極的には、定義は受信者毎に異なる
  - 一般的には spam やフィッシング
  - マスメール型ウイルスやその残骸も含む

メールシステムから見た迷惑メール

- 受信者と同じ判断基準というわけにはいかない
  - 受信者のメールボックスに配送してみないと迷惑メールかどうかわからない可能性も
- あきらかに迷惑メールとシステムで判断してもよいものもある
- メールシステムに負荷をかけるメール
- メールシステム、ドメインのレピュテーションを下げるメール
  - 自ドメイン/設備から出て行く迷惑メール

迷惑メール対策の現状

迷惑メール対策の基本

- 迷惑メールをなるべく受け取らない
  - ユーザのメールボックスへ届けない
  - ユーザが判断できる情報を受信時に付加する
  - メールシステムを守る
- 迷惑メールを送信させない
  - 自社設備から
    - 社会的な責任
    - 利用者の認証、送信制限
  - 自社設備外から
    - ドメインのレピュテーション
    - 自ドメインのメール「到達性」の確保
    - 送信ドメイン認証

迷惑メール対策の構成要素

- 送信ドメイン認証
  - あるドメインが自社のメールの出口のサーバを宣言する（IPアドレス型）
  - あるドメインが自社から出て行くメールに署名する（署名型）
  - いずれも、送信元の「ドメイン」を認証する
    - ドメインというぐらいなので、DNSを使う
  - 送信ドメイン認証の先に、レピュテーション等がある
    - ドメインの「評判」 - spam をよく送ってくるドメインかそうでないか
- 送信制限
  - 動的IPアドレスからの直接のメール配送を禁止する(OP25B)
  - 送信SMTPサーバで一定の制限をかける（流量制限など）
- コンテンツフィルタ
  - いわゆる anti spam 製品と言われるようなものが該当
  - ヒューリスティック、ベイジアン、キーワード等

迷惑メール対策の現状 update - 送信ドメイン認証

- 送信ドメイン認証プロトコルの標準化動向
- SPF と SenderID がそれぞれ Experimental RFC へ
  - IESG が承認、RFC Editor の queue で処理待ち
    - draft-schlitt-spf-classic-02
    - draft-lyon-senderid-core-01
    - draft-lyon-senderid-pra-01
    - draft-katz-submitter-01
- DomainKeys と IIM の仕様をマージ、DKIMへ
  - DomainKeys Identified MailとしてI-D公開
    - draft-allman-dkim-base-00
    - draft-allman-dkim-ssp-00
  - IETFでMASS WGを作りそこで議論していく模様

迷惑メール対策の現状 update - 送信ドメイン認証

- 送信ドメイン認証の採用状況

- US では、SPFを中心に対応が進む
  - Bank of America 顧客の62%の利用ISPで送信ドメイン認証に対応済み
  - http://www.emailauthentication.org/summit2005/02_BoA_EJohnson.pdf
  - MSN/hotmail では、送信ドメイン検証結果をwebmailにて表示
  - 送信側でSPF/SenderIDを書くのは当たり前、「ホリデーシーズン前に受信側の対応も」
- DomainKeys / DKIMは一部の採用にとどまる
  - DKIM の標準化、実装待ち
  - 早いところで今年中、本格的には来年か

- 日本のISPでは、まだごく一部
  - 企業を中心に進んでいくだろう
  - ISPは今年度中にそれなりに出てくるか

迷惑メール対策の現状 update - OP25

- Outbound Port 25 Blocking
  - 以前も報告したように、USでは多くのコンシューマ向けISPで行なわれている
  - 日本での実施も少しづつだが増えている
    - 実施にまで至っていないが、検討が進んでいるところは多い
    - JEAG OP25B sub working group
  - BIGLOBEでは完全な block でなく、throttlingを実施
  - 携帯向けは今年のうちにそれなりの数のISPが追従すると思われる

IIJ
Internet Initiative Japan

Network Initiative

「迷惑メール」時代のメールシステムに求められるもの

現在/これからのメールシステムに求められるもの

- 送信系、受信系の独立したシステム
  - システムの構成要素はどんどん増えていく
  - 複雑な構成のシステムは、設計、運用、トラブルシューティング、チューニングが難しい
  - メールの流れをシンプルに保つ
- 構成要素を柔軟に追加、変更できるシステム
  - 2年前に現在のような迷惑メールの状況を予想できた人は？
  - 去年の今頃現在の送信ドメイン認証の標準化状況を予想できた人は？
- 「メール」を扱わない要素も重要
  - 認証サーバ
  - 各種データベース/ディレクトリ
  - L3/L4 ネットワーク機器

現在/これからのメールシステムに求められるもの - 送信系

- 主な目的は、「迷惑メールをその設備から送信させないこと」
  - アカウントの使い捨てが横行しているので、あとから止めるのでは駄目
  - リアルタイムでの制限が必要
  - サインアップ直後は厳しい制限を課す（1日10通まで送信等）
- その設備から送信されるメールの「到達性」を確保する
  - 世の中の迷惑メール対策（流量制限、送信ドメイン認証）にひっかからないようにする
- 必要と思われる機能
  - 送信時の利用者認証
  - ウイルスチェック等の各種フィルタリング
  - レートコントロール
  - Outbound サーバでのコントロール

送信系 - ユーザ向けSMTPサーバ

- 送信時の利用者認証
  - SMTP AUTH のみとすることが必須
  - IPアドレス制限や、POP before SMTP は廃止へ（詳細は後述）
- 送信ポート
  - Submission port (587番ポート）への対応
    - Outbound Port 25 blocking の普及
    - SMTP over SSL でもよいが、暗号化したいなら今後はSubmission+TLS
- 利用者認証にもとづく、レートコントロール
  - 表玄関から堂々と迷惑メールを送られないように
  - 1ユーザの単位時間あたりの送信可能通数を制限
    - 「通常」のユーザは大量配信は行なわない
    - 大量配信を行なうユーザは、バウンスハンドリングをきちんとしたサービスへ誘導

SMTP AUTH 必須化

- なぜIPアドレスでの制限やPOP before SMTPではいけないのか
  - SMTP セッション内では利用者の識別が不可能
    - わかるのはIPアドレスのみ、「誰」が送ってるかわからない
    - 単一IPアドレスからの送信通数を制限すると困るケースがある
      - NATの裏に大量のユーザ
    - 毎回IPアドレスを変更して送信すると、大量送信が可能
      - 自動化ツールを使えば簡単
      - そういうbotが登場したら…
    - サインアップして上記の手法を使い、止められるまで送りまくる
  - 利用者毎の送信履歴を管理し、送信時に参照する
    - SMTP AUTH で SMTP セッション自体を認証する必要がある
  - OP25Bが普及してくると、上記のようなシナリオは現実化する

SMTP AUTH 必須化

- 送信ドメイン認証への対応
  - 複数ドメインでの共有設備の場合、他ドメインへのなりすまし問題
    - example.com と example.jp が同じシェアドホスティングにいる場合
    - foo@example.com として POP して、foo@example.jp で送信
    - SMTP時には「誰」としてPOPしたかわからないので、禁止しようがない
    - 送信ドメイン認証に対応していると、正しい送信元サーバから迷惑メールが送られることになる
    - ドメインのレピュテーションが下がる
    - SMTP AUTHのIDとMAIL FROMの一致を強制する必要がある
  - 単一ドメインでもISPドメインの場合同様の問題が
    - foo@isp.example.com として POP して bar@isp.example.com で送信
    - 苦情が bar に行く、ISPでの調査に時間がかかる
    - ドメインのレピュテーションが下がる

Outbound SMTP サーバ

- 特定のサーバへ過剰にメールを送りつけないよう注意
  - 主に携帯キャリア向け等
  - 送信レートコントロールができること
- 送信ドメイン認証への対応
  - SPF/SenderID レコードへのリストアップ
  - DKIMの署名

現在/これからのメールシステムに求められるもの - 受信系

- MXサーバでしか取れない情報とそれを利用しての後段でのフィルタリング
  - 送信元の挙動
  - 送信ドメイン認証
- 受信系は過負荷になりがちなので、容易に増強可能であること
- 自ドメインの存在しないユーザ宛のメールへの対応
  - ドメイン詐称
  - マスメール型ウイルスの残骸
  - ハーベスティング

受信系 - MXサーバ

- MXサーバ
  - 「おかしな」「はげしい」送り方をしてくるサーバからシステム後段を守る
    - 流量制限
    - 送信側は手を変え品を変えやってくる
    - きめの細かいコントロールができることが必要
  - 送信ドメイン認証チェック
    - 受信拒否をしないとしても、この段階でのチェックが必要
    - チェック結果をヘッダ等に残す
  - 場合によっては、ここでユーザの存在確認
    - ハーベスティングにあう危険性と諸刃の剣
    - 多数の宛先不明メールを送ってくる送信元への制限
  - MXサーバでもバックエンドの各種DB/ディレクトリと連携可能であること
    - ドメイン指定受信/拒否、アドレス指定受信/拒否のようなものをユーザ毎に

受信系 - フィルタリングエンジン

- ウイルスチェックや anti spam フィルタ等
  - 各種商用製品が多数
  - MTA/アプライアンスにプラグインで組み込む形式のものも
  - ここはビジネスの領域なので深く立ち入りません
- スプールと一体でない場合、後段のスプールで最終的な振り分けができるようなタグ付け/スコアリングが必要なケースも
- ただし、性能は重要
  - 受信系ではここがボトルネックになりやすい
- 近年、ウイルスでは残骸を送らない事が強く求められている
  - 悪意のないメールが感染していた過去のケースと、マスメール型ウイルス/ワームが主流である現状の違い

まとめ

- 迷惑メール送信者の手法や、それに対する対策手段は日々進化していく
- メールシステムを構成しているパーツを個別にアップデート/強化していけるような仕組みが必要
  - 迷惑メール対策はISPや企業にとってお金を生むわけではないので、巨大な投資は難しい
- エンドユーザの利用方法を変化させるには時間がかかる
  - 先を見越したシステム更新のロードマップを作成する必要
- 新規機能への対応の遅いベンダ、機能追加に莫大な費用がかかるベンダの製品をつかまないように
  - キーコンポーネントはオープンソースを利用し、自社でがんばるのも一つの方法

参考URL

- MAAWG
  - http://www.maawg.org/
- JEAG
  - http://jeag.jp/ (coming soon)
- 迷惑メール対策カンファレンス
  - http://www.iajapan.org/anti_spam/event/2005/conf0510/
- 迷惑メール対策に関する技術交流会
  - http://www.antiabuse.jp/zilwan/
- 総務省
  - http://www.soumu.go.jp/joho_tsusin/d_syohi/m_mail.html
- Email Authentication Implementation Summit
  - http://www.emailauthentication.org/summit2005/