abmailの迷惑メール判定

株式会社あいはら 研究開発チーム

山田 泰司

abmailにとっての迷惑メールとは

- EHLO/HELOを偽装しているメール！
  - スパムの痕跡を残してくれてありがとう！
- 逆引き不能なMTAからのメール！
  - 稀に逆引きがタイムアウトするときがあるけど…
- 許可していないMTAからのメール！
  - 正当なMTAはすべて登録しなきゃいけないの？
- 元々のメールが迷惑メールであるようなMAILER-DAEMONからのメール
  - 偽のバウンスメールも迷惑メールです

EHLO/HELOを偽装しているメール

- 実はスパムの３から４分の１程度が、自らを信頼させようと宛先ドメインや宛先アドレスを騙っている。
  - 一部のスパム判定ソフトには効果があるらしい
  - 明らかに偽装と判るので、誤判定がありえない
  - スパマー固有のパターンを正直に名乗るものや、やたら出鱈目なパターンを記すもの等、なぜか特有の痕跡を残すものが少なからずある

逆引き不能なMTA

- 正当なMTAのほとんどは正当な逆引きが返る
  - ホスティングサービスで、稀に逆引き不能
- DNS応答遅延で、逆引き不能なときがあり得る
  - 一部のMTAにて３ヶ月から１年に１回という頻度
  - 偽陽性の場合、IPアドレスをホワイトリストに登録
  - もしくは、時間をおいて改めて逆引きを試みて救済

許可していないMTA

- 世界中のすべてのMTAについて、許可・不許可を設定するのは不可能なので、
- 逆引き名から正当なMTAか否かを類推
  - エンドユーザ空間等、スパムの巣窟との相関が高い
- 類推が外れる逆引き名のみを管理すればよい
  - ホスティングサービスで類推が外れやすい傾向
  - 偽陽性の場合、所有IPアドレスをホワイトリストへ
  - 偽陰性の場合、逆引き名をブラックリストへ
    - スパム業者なら、所有IPアドレスをブラックリストへ
  - 既存のRBLを併用することも可能（多少効果あり）

偽のバウンスメール

宛先不明で差出人である自分に差し戻された…

- バウンスメールには、自分が送ったはずのメールが添付されているはず
  - メールのヘッダだけでも添付されていれば判別可能
  - 一部、それさえも添付しないMTAもありますが…
- 添付されているメールのヘッダ情報から、前述と同様な迷惑メール判定方法を適用！
  - なので、なんら特別な設定は不要
- 真に自分が送った（宛先を間違えた）メールを迷惑メールと誤判定しません

abmailがやらないこと

- 本文は走査しません
  - イタチごっこになるし、必要ない
- 差出人はチェックしません
  - どうせ詐称されてます
- ヘッダ情報は信頼できる箇所しか見ません
  - Receivedヘッダも偽装されてます
- 受信拒否、再送要求、応答遅延など
  - スパマーに気付かれるようなことはしません
  - 正当なMTAに迷惑をかけることはしません

abmailは

- 単純！高速！簡単！
- bsfilterやSpamAssassin等とは全く違います
  - イタチごっこになりません、画像スパムとも無縁！
- greylisting, tarpittingとは全く違います
  - 正当なMTAに迷惑を掛けません
- S25R系とも違います
  - 偽のバウンスメールを迷惑メール判定できます
- MTA、スパマーのアドレス管理に徹する潔さ！

abmailを攻略するには

- スパマーは費用を掛けてドメインを所有・管理
- 正当なMTAを設営して、そこからスパム送信
  - ブラックリストに載るまでは効果有り
- ドメイン名を頻繁に変更する
  - IPアドレスのブラックリストに載るまでは効果有り
- IPアドレス空間を転々とする
  - コストが掛かるので、それに見合った収益が必要
- 巧妙に偽装したバウンスとしてスパムを送信
  - それは、そもそもスパムとして機能する？

abmailのある未来

- スパマーはサイト誘導、詐欺、国際犯罪などのメールを、懸命に送り続ける
- しかし、利用者はスパムを気に留めないので、
  - スパマーは収益が思うように上げられず、
  - スパムを維持するコストの方が高くなっていく
- スパマーはメール以外で暗躍するしかない！
  - アドウェア、スパイウェア、マルウェア、
  - トラックバック、コメントスパムなど

迷惑メール対策はこれでお終いにしよう！