reputation

曽田 哲之

2005年12月7日

格付け

どの格付けサービスを信用して使うべきか

偽陽性をどれくらい許容できるか

格付け対象 (1/2)

- IP アドレス
  - 迷惑メール源: spamhaus SBL…
  - オープンリレー等: list.dsbl.org…
  - ウィルス感染: virus.rbl.jp…
  - 動的 IP アドレス
  - 地理情報

格付け対象 (2/2)

- ドメイン (RHS)
  - ブラックリスト
  - ホワイトリスト
- コンテンツ (URL ホスト部)

ブラックリスト サービス (1/2)

- DNS & RHS Blackhole lists

  `http://spamlinks.net/filter-dnsbl-lists.htm`

- 日本国内主体のサービス

  `http://www.rbl.jp/`

ブラックリスト サービス (2/2)

登録のしくみ

- おとりアドレス
- 利用者からの報告
- 正当なメールの流量を監視
- 有償ホワイトリスト
- 他の格付けサービスの参照

問題点 (1/3)

- 動的 IP アドレス

  ブロックして良いか? データベースが不正確。
- 国全体をブロック
- コンテンツフィルタ

  偽陽性が避けられない。

問題点 (2/3)

- ブラックリストへの誤登録
  - 連絡なしの登録
  - 迷惑メール業者と同じ ISP を利用
    迷惑メールの打ち逃げ (増加中)
  - backscatter

問題点 (3/3)

- ホワイトリスト

  無名なサイトと迷惑メール源が同じ扱い

- SPF, DKIM はいつ利用可能になるか？

IPブラックリストの評価 (海外アドレスが主)

	偽陽性	info@ 検知	その他検知
逆引き不能なIPアドレス	2.71%	85%	57.2%
dul.dnsbl.sorbs.net	3.41%	7%	49.6%
bl.spamcop.net	0.62%	14%	7.3%
list.dsbl.org	0.31%	0%	29.2%
sbl-xbl.spamhaus.org	0.16%	83%	23.5%
short.rbl.jp	0.00%	42%	0.2%
サンプル数 (IPアドレス)	1290	2929	12203

※ bl.spamcop.net のブラックリストには gmail.com も

できること？

- 格付けサービスへのネットワークリソースの提供
- 動的 IP アドレスのような情報はサイトが自ら提供？
- 偽陽性のより少ないブラックリスト？
  - 連絡後の登録？
  - 打ち逃げの危険のあるホストを自身で表明する？
  - 各種ブラックリストの共有？
    RHS の NS/MX, HELO

協力が可能な方は

reputation@iajapan.org

へ御連絡を