DNSBL でスパム対策 とりあえずやってみよう編

Echigo BSD Users group 14th meeting
at Suncross of Tokamachi city.
21st, May, 2005
INOUE Mikio <mikio@ebug.jp>

おしながき

- DNSBL って何
- 導入の問題点
- sendmail で使ってみる
- 開き直る
- その他

※ Spam® は、Hormel 社製品の登録商標です。spam は、インターネットコミュニティにおける伝統的な用語で、受信者の意図に反して大量に送信される迷惑メールを指し示します。本稿で扱うスパムは、後者についてのものであり、Hormel 社の製品について記述されたものではありません。

DNSBL

- DNS based Blackhole List
  - RBL (Realtime Blackhole List) や SBL (Static Blocking List) なんかがあります。
- 怪しいホスト一覧
  - IP アドレスとかドメイン名とか。
  - リストを参照することで怪しいホストとの通信を拒否ったりできる。
- 照会は DNS の検索と同じ方法

検索手順

- リストに対象ホストの IP アドレスを逆順にして付加したホストの存在を調べる
  - リスト `sbl-xbl.spamhaus.org`
  - 対象 IP アドレス `A.B.C.D`
  - `dig D.C.B.A.sbl-xbl.spamhaus.org`
  - 検索できなければ、登録されてない。
  - 検索できたら、登録されてる。

検索してみる 1/2

```
% dig 137.172.63.66.sbl-xbl.spamhaus.org

; <<>> DiG 8.3 <<>> 137.172.63.66.sbl-xbl.spamhaus.org
;; res options: init primry(unimpl) recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12898
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 15,
   ADDITIONAL: 12
;; QUERY SECTION:
;;      137.172.63.66.sbl-xbl.spamhaus.org, type = A, class =
   IN

;; ANSWER SECTION:
137.172.63.66.sbl-xbl.spamhaus.org.  1h59m45s IN A  127.0.0.2
```

検索してみる 2/2

```
% dig 206.136.239.210.sbl-xbl.spamhaus.org

; <<>> DiG 8.3 <<>> 206.136.239.210.sbl-xbl.spamhaus.org
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 23880
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
   ADDITIONAL: 0
;; QUERY SECTION:
;;      206.136.239.210.sbl-xbl.spamhaus.org, type = A, class
   = IN
```

怪しいホスト

- メール関係
  - Open Relay、spam source、一時的な spam source、バグのある form mail、spam 支援者、rfc 違反。
- その他
  - virus source、DDoS source、 Open Proxy 、ダイアルアップ、その他。
- ポリシーはリスト作成者によって様々。

導入の問題点 1/2

- 伝統的な通信の常識に反する
  - 自由な通信を防げる。
  - 通信の秘密を守らない。
    - サーバベースのウィルススキャナも同じ。
- リストの正当性を検証し難い
  - リストのポリシーが不適切なものが存在する。
  - リストへの誤登録の可能性が常にある。

導入の問題点 2/2

- どこで適用するか
  - サーバ全体でするか、アカウント毎に勝手にやるか。
- /etc/mail/freebsd.mc
  - 一時期 'recommended!' って書いてあった。
- いくつかの ISP が導入してるらしい
- スパムいや度との兼ね合い
  - サーバのポリシーとして開き直る?

リストを選ぶポイント

- それぞれのポリシーを確認する
  - 複数のリストを提供してる場合がある。
  - 目的に合ったリストを探す。
- リスト自体が怪しいことも
  - ポリシーがない。
  - ポリシーが不適切。
  - 但し、程度問題。

有名なリスト作成元 1/2

- SpamCop.net (登録量が多い)
  - http://www.spamcop.net/
- The Spamhaus Project
  - http://www.spamhaus.org/
- Distributed Sender Blackhole
  - http://dsbl.org/
- Open Relay Database (老舗)
  - http://www.ordb.dk/

有名なリスト作成元 2/2

- RBL.JP (数少ない国産)
  - http://www.rbl.jp/
- SORBS
  - http://www.au.sorbs.net/
- SURBL
  - http://www.surbl.org/

sendmail で使ってみる 1/2

- sendmail.mc を変更する
  - DNSBL 毎に 1 行追加するだけ。
  - `FEATURE(‘dnsbl’, ‘リスト’, `メッセージ’)dnl`

例) bl.spamcop.net を使う場合

```
FEATURE(`dnsbl’, `bl.spamcop.net’ ,¥
 `"550 Email from " $&{client_addr} " ¥
rejected using DNS-based Blocking List - ¥
 see: http://spamcop.net/’)dnl
```

sendmail で使ってみる 2/2

- sendmail.cf を更新
- sendmail を再起動する
- 導入完了
  - 指定したメッセージは maillog に出ます。
  - postmaster へのレポートとかはありません。
  - FreeBSD 4.x の場合は、daily run output に rejected mail hosts: としてリストされます。

スパムは減ったか 1/2

- 結構拒否ってると思います
  - 2005 年 3 月 22 日〜3 月 31 日

bl.spamcop.net	57.2%
sbl-xbl.spamhaus.org	19.3%
all.rbl.jp	5.6%
list.dsbl.org	2.3%
拒否しなかったメール	15.7%

スパムは減ったか 2/2

- リストの分布はかなり変化するようです
  - 2005 年 4 月 1 日〜4 月 30 日

bl.spamcop.net	23.0%
sbl-xbl.spamhaus.org	28.2%
all.rbl.jp	3.1%
list.dsbl.org	28.9%
拒否しなかったメール	16.8%

気になること

- 負荷の状況
  - 導入前と比較して、CPU もトラフィックも負荷が増えた実感は全くありません。
- 誤認識がないか
  - maillog を眺めてる範囲では、気になる拒否はほどんどありません。極稀にありました。
- メンテナンス
  - 今のところ何もしてません。

自サイトのポリシー変更

- サイト全体に適用する場合
  - リストのポリシーに対応せざるをえない。
- アカウント毎に適用する場合
  - 利用者が勝手にやる分には、個人の趣味の問題。

問題になりやすい拒否

- DSL 系サービスの固定されていない IP アドレスからの SMTP
  - スパムを撒き散らしては切断する。
  - ひろえ～が被害にあいました。
- spam source が大量にある IP アドレスブロックに巻き込まれる
  - OCN がごっそり巻き込まれる。
  - 5hed 氏が被害にあったらしい。

誤拒否の言い訳

- 固定してない IP アドレスは公衆便所。
  - 誰がどう使ったかわからへん。
- SMTP は、スパマーを制限してるか、減らす努力をしてる IP アドレスから張ってね。
- 感染症予防と思ってあきらめろ。
  - 不特定多数が相手なのでコンドーム。

他のスパム拒否技術

- SpamAssassin
  - 拒否の対象が広い
    - 経由してきたサーバも拒否の対象にできる。
    - メール本文内の URL なども拒否の対象にできる。
  - ユーザ毎に設定できる
    - サイトのポリシーを変更する必要がない。
    - サイトの規模が大きくなると運用が難しい。
- Bayesian Filtering
- レピュテーション
  - 送信者評価 (Sender Reputation)

スパム発信の制限技術 1/2

- Outbound port 25/tcp のブロック
  - ISP を含む多くのサイトが導入済みか検討中。
- ユーザ認証
  - SMTP-AUTH、POP befor SMTP
- レート制御 (Rate Control)
  - SMTP のセッション数を制御。
- 投稿ポート

スパム発信の制限技術 2/2

- ドメイン認証
  - IP アドレスベースの送信ホスト認証
    - SPF (Sender Policy Framework)、Sender ID、
    - DNS の TXT レコードに送信 MTA の IP アドレス
  - 電子署名による送信ホスト認証
    - DomainKeys
    - DNS の TXT レコードに公開鍵
  - 期待の星らしい (おもしろそうだ)

まとめ

- 導入と運用はメチャ簡単
- 効果は大きい
- 誤拒否への注意は求められる
- ポリシーの設定と確認が重要
  - サイトの運用ポリシー
  - リストの構成･作成ポリシー