spam対策の現状

ディープソフト株式会社

北野利治

kitano@DEEPSoft.co.jp

韓国のspam事情

- 韓国はspam王国
  - 海苔店とか会員制エロペグサイトとか・・・
  - メールトラフィックの70%がspamとの統計
- 何でこんなにspamが多いのか
  - 韓国のISPはメールアドレスを配らない
  - メールサービスはMSPが提供する
  - MSPの収益モデルはWebMail画面の広告収入
  - ページビューを稼ぐためにたくさんアドレスを配る
  - 一見メールに関係ない会社もバンバン配る配る
  - メールサービスはサイトへの集客ツール

韓国のspam事情

- メールアドレスの氾濫
  - 一人あたり5～6個のメールアドレスを使い分け
- メールサーバの負荷が増大
  - サーバ増強に際限なくお金がかかる
- 法律で規制してみた
  - 誰も守らないので無法地帯
- spam遮断製品もspam発送ツールもスゴイ
  - マッチポンプする会社も現れた！

あるメールサーバの一日

- ソウルのとあるデータセンタで、韓国で3本の指に

구분	전체메일		정상메일		스팸메일		바이러스메일	
	메일 수	비율	메일 수	비율	메일 수	비율	메일 수	비율
합계	1851564	100	656188	35.439	1194148	64.494	1228	0.066
송신	0	0	0	0	0	0	0	0
수신	1851564	99.999	656188	35.439	1194148	64.494	1228	0.066

- Pentium III 1G x 2, 1024M, Linux

↑ ↑ ↑

総メール受信数　普通メール受信数　spam**受信数**

(注) 何かの間違いではありません

韓国のspam対策の歴史

- 大量のspamのためDoS状態
  - メールサーバ保護のソリューションが必要
- ゲートウェイ対策 vs メールストア対策
  - ゲートウェイなら一カ所でまとめて遮断
  - メールストアで個人ごとにきめ細かく
  - 間違ってドロップしたらどうする？
- それぞれメリットデメリットはあるが・・・
  - spamは受け取った時点で負け

韓国のspam対策の歴史

- そこで・・・
  - 両方式のいいとこ取りをゲートウェイで
  - ゲートウェイソリューションでメールサーバを保護
  - 個人ごとにきめ細かなフィルタ設定も可能に
  - 間違ってドロップしてもリカバリー可能に
- 遮断方法は？
  - ブラックリスト、ホワイトリスト
  - 接続回数、送信数などで自動的にブラックリストへ
  - フィルタリングルールによるパターンマッチ

spammerとの戦い

- 敵もさるもの、いろいろと考えてきやがる
  - こちらも進化しないと負けてしまう
- たくさんの踏み台から一斉に
  - 同じメールボディのメールを認識・検出し、複数のIPアドレスからのコネクションを遮断
- メールボディに画像がひとつ
  - ウェブページへの誘導を追跡、遮断
- パターンマッチでは限界
  - ベイジアンフィルタ（統計的手法）の導入

- **果てしなく続くspammerとの戦い**

つづく・・・