SMTP セッションでのスパム対策と taRgrey

有限会社ジーワークス

佐藤 潔

自己紹介

- taRgrey/Rgrey/Starpit
- 有限会社ジーワークス
- 長野県白馬村
- スキーしたかったから :)

今やってる仕事

- 8 年ほど前から地方 ISP 様から外注
- サーバの管理やユーザサポート業務
- 小規模ですが自社のサーバサービスも
- スパム対策についての要望が非常に多い

こんなことを話します

- SMTP セッションでの対策手法紹介
- 特にSMTPクライアントの振る舞いや特徴を利用するもの
- スパムbotの振る舞いは通常のMTAとは違うため
- taRgrey という手法の説明

greylisting

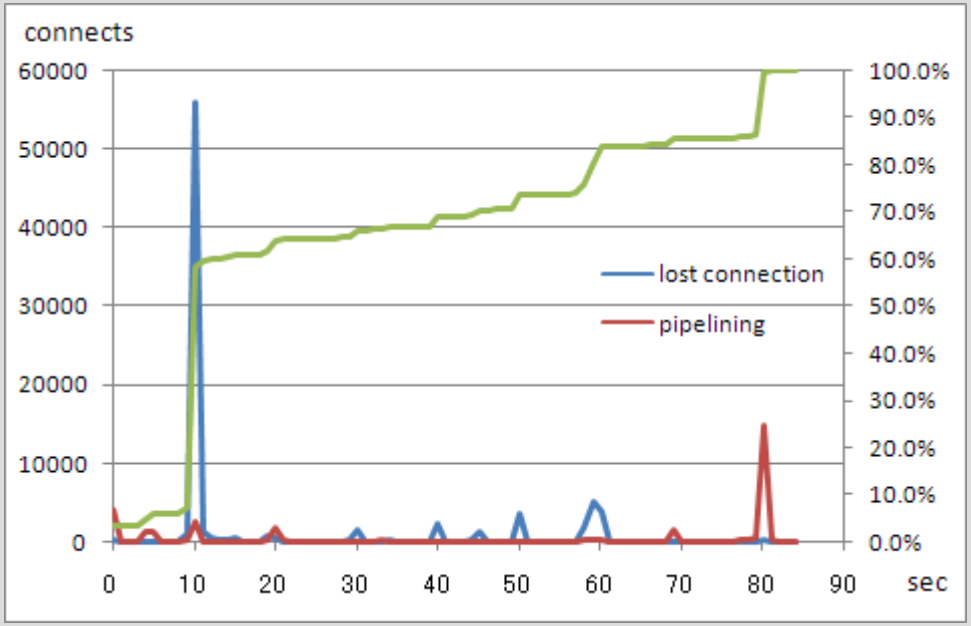
- 一時拒否して再送してきたら受け取る
- 一時拒否(4xx)で返すと正しいMTAは30分後とかに再送
- スパムbotは再送しない
- とても強力でこの種の中では一番メジャーな手法
- 95%以上のスパムを排除できる

nolisting

- プライマリmxや優先順位の低いmxにダミーのIPを指定
- セカンダリmxなどで受け取る
- スパムbotはプライマリmxにしか送らないものが多い
- DNSの設定だけでできるためとてもお手軽
- リソースも食わない
- 80%くらいのスパムが正しいMXへ接続すらできない

tarpitting

- SMTPセッションの返答を何10秒か待たせる
- スパムbotは応答時間を少ししか待たない
- 向こうから接続を切ってくる
- greylistingのように再送までの遅延がなくて済む
- postfixやsendmailなら設定だけで簡単に利用できる
- 90%強のスパムを排除できる



pregreet detection

- 正しくない偽の応答を返して反応を見る
- スパムbotは応答内容をちゃんと確認せず送ろうとしてくる
- tarpittingのように「待つ」必要がなくすぐに判定できる
- 排除率は不明(夏休みの宿題だったのに… 間に合わず)

passive OS fingerprinting (p0f)

- TCP/IPのパケットから接続元のOS種を判定する
- スパムbotはWindowsのPCなので接続元がWindowsか見る
- スパムの98%くらいはWindowsのbotから出ている
- Windowsからの接続によるスパム比率は99%強くらい

国コード(GeoIP)

- IPアドレスから国コードを識別
- メール発信国毎でスパムとハムの送信数に偏りがあるため
- 日本宛て中国からのメールは99.5%くらいの比率でスパム

これら手法の良いところ

- 基本的にどれも軽い
- 判定の「揺れ」が無い
- スパム排除率は80～98%程度と軽いわりに結構良い

良いとこばかりではない

- p0fとGeoIPの例がわかりやすい
- Windowsだったら必ずスパム？中国からなら必ずスパム？
- いくら確率が高くてもそれだけではスパム判定できない
- つまり誤検出
- 副作用の問題

greylistingの問題点

- メールの遅延
- 再送しない「正しい」サーバや違うIPから再送される場合
- ユーザ登録の確認メールなどで直接SMTPしゃべる場合
- DBのクリーンアップが意外に重かったり

tarpittingの問題点

- 待ち時間を極端に短くしている「正しい」サーバがある
- メールマガジンなどの大量メール配信サービスに多い
- FireWallが無通信時間を監視してて切ってしまう場合
- プロセス数の増大

nolistingの問題点

- ログが残せないので誤検出を後から調べられない
- 最初からセカンダリmx送ってくるスパムが意外に多い
- プライマリmxにしか送らない「正しい」MTAも多そう

誤検出が無いことを重視すべき

- 検出率に目が行くが運用上重要なるのは誤検出率
- 重大な誤検出が起こるとユーザは使ってくれない
- 逆に仕事が増える
- 人が判定する場合より誤検出が少なくなるのが最低ライン

誤検出や副作用が少なくなるように組み合わせる

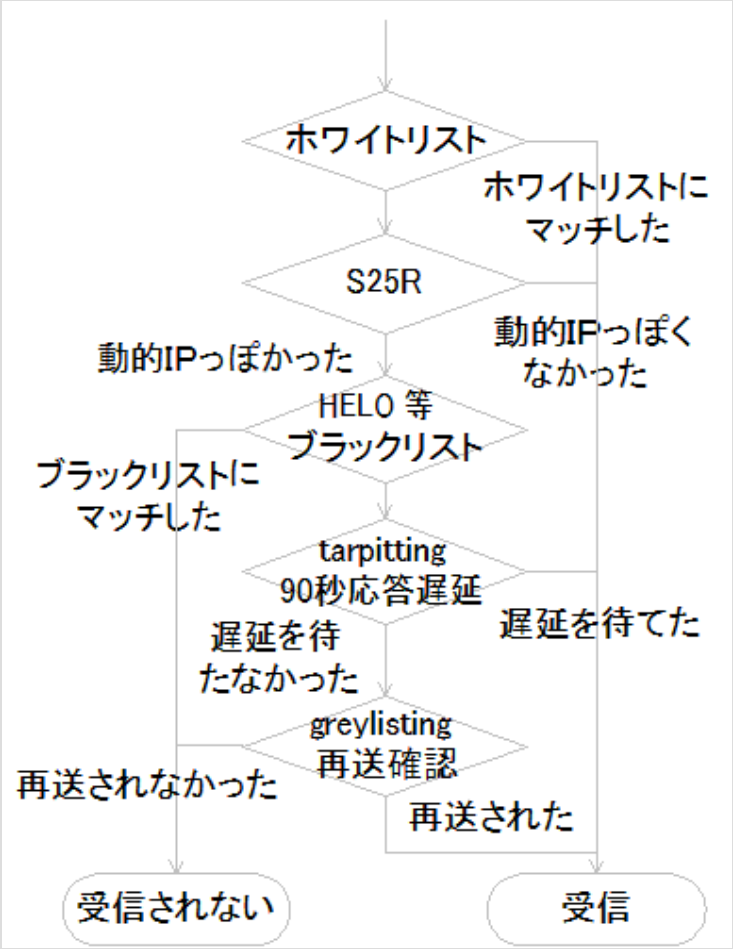
- 多重に重ね合わせるのではなく条件を絞ることに使う
- postfixだとアクセスポリシーを多段で利用
- sendmailでは？milter managerを使おう！
- 一つの仕組みでシンプルなシステムにこだわると誤検出や負荷の問題がおこりやすい

Rgrey

- S25R+greylisting
- 怪しい接続に対してのみgreylistingを掛ける
- selective greylistingという名で手法として一般化
- S25R(の補集合)は汎用ホワイトリストという考え方
- S25RはDNSBLと比べ結果が揺れないという利点が大きい
- 95%弱のスパムが排除

taRgrey

- S25R+tarpitting+greylisting
- 怪しい接続に対してのみtarpitting掛け再送で救済する
- S25Rに引っかかってしまった場合の遅延が無くなる
- ほぼ誤検出はない
- p0fやSPFでさらに絞っても良い
- 90%強のスパムが向こうから去る



誤検出が無いと90%でも有用

- スパムが1/10になれば十分なユーザは多い
- 2次フィルタへ回るメール数が1/5になる
- 「ゴミ箱」のスパムが1/10になり確認が楽

まとめ

- スパム対策はすでにセキュリティ対策の一環
- 誤検出が無いことを重視
- 各手法を組み合わせて弱点をカバー

- taRgrey 試してみてください
  - 特に教育機関での導入が多い
    - 大東文化大学
    - 和歌山大学システム情報学センター
    - 佐世保高専
    - 尚絅学院大学
    - 宇部工業高等専門学校
    - 一橋大学　情報基盤センター
    - 中央大学
    - HDE Anti-spam