spam対策

吉田（大分大）* 笠原（九大）
長谷川（中京大）
*リーダー

SS研セキュリティマネージメントWG
spamグループ

背景

- 大量の迷惑メールとバックスキャッタ
- メールが届くのは幻想？
  - SMTPもbest effort
- 仕事に使えなくなるメール
  - ゴミに埋もれて見落とす
  - ゴミで細るネットワーク
- メールが必ず届くという思い込み
  - 重要な連絡は電子メール以外で！

spam対策の基本

- spamに対するポリシーの明確化
  - メール運用の方針の議論と確立
  - 対策手段はポリシー決定後
  - ポリシーと手段をごっちゃに議論しない！
- システム運用者が苦情に埋もれないこと
  - false positive問題
  - アプライアンスによる運用（責任の移転）
  - アウトソース

spam対策ポリシー(1)

- 社会的責任
  - spam受け入れはspamを助長する行為？
    - spam受信者がいなくなればspamはなくなる？
  - spamの発信源とならないこと。
    - 組織の社会的信用の失墜

spam対策ポリシー(2)

- 対策しない場合のコスト
  - ハードウェア・ソフトウェア資源
    - 対策をしないとサーバ等に過大な投資が必要
  - 人的資源の無駄（spamメール削除等）
- 対策する場合のコスト要因
  - 機器等への投資や人的投資コスト
  - false positive問題
- 現場に責任を押し付けない方針が必要

spam対策の基本選択肢

- 対策をとらない
- 自前で実現
  - ソフトウェア実装で実現
    - 現場の負担と金銭コストのトレードオフ
  - アプライアンスの導入
    - ユーザごとにオプションが選べるものがいい
- メールサービスを外部委託
  - 機密漏洩の不安

発信者確認とspam発信防止

- 発信者の身元証明
  - SPFやDKIM
    - 証明書は取得容易
  - SMTP-AUTH
- 送受信のポート制限
  - OP25B+Submission port
  - IP25B
    - 動的割り当てアドレスからの発信拒否

バックスキャッタ対策

- メールアドレスのガバナンス
  - メールアドレスをすべて把握
  - 学生証等のIC化やポータル導入がチャンス
  - 受け取ってからuser unknownは問題
    - バックスキャッタ
- 受信拒否？　受け取ってゴミ箱行き？
  - アドレスのハーベスティング防止
  - ただし、トラフィックは減らせない

メールアドレスの管理

- アドレスの一元管理
  - メールアドレスのLDAP認証
    - 認証サーバに多大の負荷？
  - 受信サーバの一元化
    - ポータルで一括（メールサーバは1台）
    - 中継サーバで管理
      - DB,LDAP等との連携
      - サブドメイン連携（受信前のアドレス存在確認）
        - » VRFYやLMTP(例　舛田、落合:FIT2007 LL-003)

受信側対策

- ●ホワイトリスト・ブラックリスト
- ●コンテンツフィルタ
- ●実装の差異を利用した判定
- ●遅延・流量制限
- ●経験則による判定

ホワイトリスト・ブラックリスト

- 送信者・送信元に○×をつける
  - 仕組み自体は単純でわかりやすい
- 問題点
  - 送信者詐称・ヘッダ改ざんに弱い
    - →発信者確認の必要性
  - 手動ではリストの管理が煩雑
  - 公開 Realtime Black List (RBL) の利用
    - DNSクエリを利用したサービスが一般的
      - 多くのMTAで設定が容易に可能
    - リストの信頼性に疑問
      - spamhaus.org と ISP の対立など

コンテンツフィルタ

- メールヘッダ・本文の内容で判断
  - NGキーワードによる単純なフィルタ
  - 単語の生起確率による学習型フィルタ
    - ベイジアンフィルタ
  - URIBL（spam本文に含まれるURIのリスト）
  - 利用者の報告に基づく公開データベース
- 問題点
  - spamかどうかの判断が100%信頼できない
    - 誤判定によるメール紛失問題
  - 画像spamなどの回避策が増加

コンテンツフィルタ/実装

- Spamassassin : http://spamassassin.apache.org/
  - キーワード・学習フィルタ・公開データベース等多数の手法からspamらしさを点数で判定
- Bogofilter : http://bogofilter.sourceforge.net/
  - ベイジアンフィルタ実装
- Bsfilter : http://bsfilter.org/
  - Ruby によるベイジアンフィルタ実装（日本語対応）
- Vipul's Razor : http://razor.sourceforge.net/
  - 公開データベース
- その他多数ある

実装の差異を利用した判定

- spam送信ソフトウェアと通常のMTAとの実装の差異を利用
  - 再送処理
  - MXレコード処理
  - その他のプロトコル違反
- 実装が甘い正当なサーバをはじく恐れ
  - ホワイトリストの管理が必要

再送処理

- 仮定: spam送信ソフトウェアは再送しない
- 初接続のMTAには一旦tempfailを応答
  - 「一時的な障害なので後で再送せよ」
- 再送してきたら受け取り、ホワイトリストに登録する
  - IPアドレスによるもの、エンベロープも利用するものなどいくつかバリエーションがある
- 単純だが効果は大きい
- 問題点
  - 再送が起こると配送遅延がかなり大きい
  - 適切に再送しない既知の実装・サービスがある
  - 適切に再送するspam実装が存在する

再送処理/実装

- greylisting: http://www.greylisting.org/
  - ポータルサイト
  - 各種MTAの実装がまとめられている
- 「お馴染さん」方式:
  http://moin.qmail.jp/_a4_aa_c6_eb_c0_f7_a4_b5_a4_f3_ca_fd_bc_b0
  - 初接続ホストは遅延通信後tempfailする
- S25R: http://www.gabacho-net.jp/anti-spam/
  - 逆引きしたホスト名を経験則で分類しtempfail 対象とする
  - Starpit・Rgrey・taRgrey等のバリエーションがある

MXレコード処理

- MXレコードの優先順位処理の差異を利用
- ダミーMX・SMTPリセット
  - 優先度最高のMXでメールを受け取らない
  - 通常は次のMXへ即時再送する
  - MXを正しく処理しないspam送信ソフトは次のMXに再送できない

MXレコード処理/実装

- MXフォールバック判定:
  http://moin.qmail.jp/MX_20fallback_20_c8_bd_c4_ea
  - 最優先MXでは接続を受け付けず、接続履歴だけ取る
  - 次のMXでは最優先MXに接続履歴があるホストからだけメールを受け取る
- Unlisting: http://unlisting.org/
  - MXフォールバック判定とほぼ同様
- Nolisting: http://nolisting.org/
  - 接続履歴の検証を省略したもの
- GION: http://www.reflection.co.jp/spam/
  - 次MXでtempfailや遅延応答・逆引きチェックも実施

受信側対策

その他のプロトコル違反

- greet pause
  - sendmail 8.13 の設定項目名に由来
  - 接続時の最初の応答（greeting）を一定時間遅らせる
    - 正しい実装はgreetingを待つ
    - 待たずにメールを流し込むspammerを拒否
- プロトコルの検査
  - HELOの形式チェック
  - EHLOからHELOへのフォールバック

受信側対策

遅延・流量制限

- spammerからの通信を遅延させたり流量を絞る
  - 時間当たりの総送信量を減らす
  - 他の判定方法でspammerと判定されたホストに対して実行
  - spamの流量を減らし下流のサーバ負荷低減
  - spammerの作業効率を低下
- tarpitting・トラフィックシェーパ等

受信側対策

遅延・流量制限/実装

- OpenBSD spamd: http://www.openbsd.org/spamd/
  - 遅延通信とgreylisting機能
  - pf（OpenBSD/FreeeBSD のパケットフィルタ）と組み合わせて使用
- Symantec Mail Security 8100 シリーズ: http://www.symantec.com/ja/jp/enterprise/products/overview.jsp?pcid=1011&pvid=852_1
  - メールの通過パスを元にspam判定
  - spamは流量制限（最大50%減）

受信側対策

経験則による判定

- 逆引きのできないサーバを拒否・制限
- 逆引きしたホスト名が特定のルールに合致するものを拒否・制限
  - 動的アドレスらしいものを判定など
- 問題点
  - 経験則なので必ず例外がある

受信側対策

アプライアンス・ソリューション

- 個々の対策には異なる特徴がある
  - それぞれの利点と欠点
- 現場の管理者が組織のサーバに対し自力で対策した場合、欠点や設定ミスによるメール紛失等の責任問題が発生する
- 既存の製品を導入することでこれを回避する方が得策かもしれない
  - 採用している技術が異なる
  - 可能なら複数の製品を試用して比較するべき
  - コストとの兼ね合い

受信側対策

代表的な製品（網羅的でない）

- Barracuda SPAM Firewall
  - http://www.barracudanetworks.com/ns/index.php?L=jp
- IronPort Mail Security Appliance
  - http://www.ironport.com/jp/
- McAfee SpamKiller for WebShield
  - http://www.mcafee.com/japan/products/mcafee/spamkiller_ws.asp
- Symantec Mail Security 8200
  - http://www.symantec.com/ja/jp/enterprise/products/overview.jsp?pcid=1008&pvid=849_1
- Trend Micro Spam Prevention Solution
  - http://jp.trendmicro.com/jp/products/enterprise/sps/index.html

送信側対策

- OP25B(Outbound Port 25 Blocking)
  - Bot(ゾンビ)等からのspam送信をブロックする
- 送信者メールアドレスの詐称防止
  - 送信ユーザの認証
    - SMTP AUTH
  - ドメイン認証
    - SPF (Sender Policy Framework)
    - DKIM (DomainKeys Identified Mail)

OP25BとSMTP AUTH(1)

- Outbound port 25 blocking
- 受信側での対策はたいへん(法的・技術的)
- 送信側のルータで止めることが効果的
- 「spamを送らない」
  - Bot(ゾンビ)や、無線LAN不正使用によるspam送信を止めることができる

OP25BとSMTP AUTH(2)

- 配送ポート(25)と投稿ポート(587)との分離
- 投稿ポートでは、smtp authによるユーザ認証
- 利用者には、ユーザ認証が必要な投稿ポート(587)のみを提供する
- 配送ポート(25)は、投稿目的での利用は不可
- 現実的には、
  - 同一ドメイン内: 配送ポートでの投稿もOK
  - ドメイン外から: 投稿ポートからのみ受け付ける

OP25BとSMTP AUTH(3)

- MTA(Mail Transfer Agent)のみが配送ポートを使って外部へメールを配送する
- 一般端末から配送ポート(25)で、直接外部へのメール配送は禁止
- レート制御
  - 同一送信者、同一IPから

レート制御

- 同一送信者、同一IPから短時間に大量のメール(spam)が送られることを禁止する
- OP25Bにより配送サーバを限定することで、そのサーバの中で対応できる。

SPF

- POBOX.COMが提唱
- 送信サーバをDNSに登録

  [例] - example.jp IN TXT “v=spf1 +ip4:10.1.2.3 –all”
  - example.jp IN TXT “v=spf1 +mx ~all”
  - 「+」pass, 「?」neutral, 「~」softfail, 「-」fail
  - 「ip4:」ipv4アドレス, 「mx」mxレコード
- 受信側
  - SMTPコネクションから送信元MTAのIPアドレスを得る
  - 送信者メールアドレスを取り出す(envelope from:)
  - そのドメイン部をDNSで検索し、SPFレコードを得る
  - 送信元MTAのIPアドレスとSPFレコードを比較する

送信側対策

DKIM

- YahooとCiscoが提唱
- 送信者は、公開鍵をDNSに登録
  - 認証局(CA)は不要
- 秘密鍵を使ってメールに署名
  - 署名はヘッダに挿入される
- 受信側
  - メールを受信する
  - 送信元アドレスを取り出す
  - そのドメイン部からDNSを検索し公開鍵を得る
  - 公開鍵を使って署名を検証する

送信側対策

メールの転送

- SPF
  - 送信MTAが変わるので認証に失敗する
- DKIM
  - 送信MTAのIPアドレスに依存しないので問題なし

送信側対策

メーリングリスト

- SPF
  - MLサーバにSPFのための機能追加をする必要なし
- DKIM
  - メールの書き換え等のため、署名を作り直す必要あり（MLサーバに機能追加）

送信側対策

SenderID

- SPF＋CallerID(Microsoft)
- DNSへ登録するSPFレコードは、共通
- 送信元アドレスとしてエンベロープFROMではなく、ヘッダ中からPRA(purported responsible address)を抽出し、用いる。