メールサーバ構築

～運用コストへの挑戦～

安藤一憲
ando@bbsec.co.jp

このチュートリアルの構成

- スパマーの手口の進化と対策
  - botnetへの対策
  - OP25Bだけで十分か?
- 管理コストを最小化する選択
  - スパムフィルタの選択
  - ゲートウェイ型の配置に潜む盲点
  - 自分の管理範囲からスパムを発信させないためには
  - 新たなスパム配信を受けないためには
  - スパムが来た場合の処理の法的問題は？

スパマーの手口（アドレス収集）

- スパム送信には送信先アドレスの一覧が必要
  - アドレスの漏洩はどこから?
    - アドレスハーベスティング
      - ディレクトリハーベスティングアタック（DHA()）
      - WWWサイト巡回ロボット
    - ワーム／ウイルス
      - 個人のPCのハードディスクから
    - ボット／バックドア／キーロガー
      - 実質何をされるかわからない

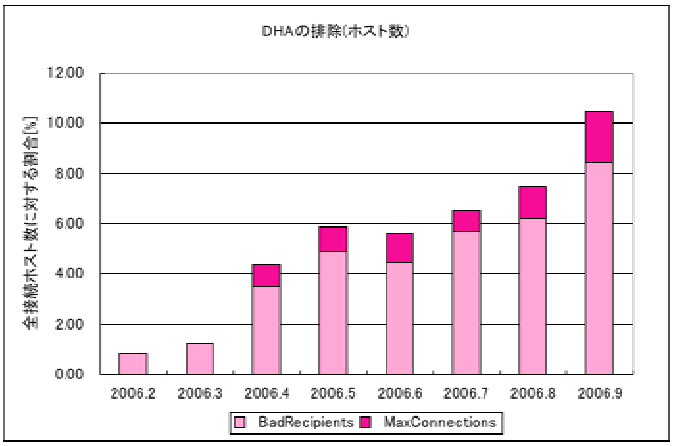
アドレス収集攻撃への対策

アドレス収集攻撃の検知

- DHAによるアドレス収集はどのように見えるか?
  - ログにUser Unknownが大量に記録される
    - DATAコマンドを実行しない（本文を送信しない）アタックも
  - 本文なしのメールが送られてくる
    - エンドユーザにはこのように見える
  - 場合によってはエラーメールが大量に滞留する
    - 「エラーメールを返さない」のは本当に有効な対策なのか?

アドレス収集攻撃への対策

アドレス収集攻撃の実態



アドレス収集攻撃への対策

究極の姿は水際作戦

- 有効なのは「水際作戦」
  - エラーメールを返さないと
    - メルマガ、ML等でも無効なアドレスを検知できない
    - スパマーにとってはアドレスが有効に見える
      - 逆にUser Unknownなメールがどんどん増加する結果になる
  - エラーメールを生成させないためには
    - 対外セグメントでメールを受信するサーバで対策
      - User Unknownを頻発させる送信元に対してtempfailで応答
        - 法的には「受信拒否ではない」ことがポイント
      - ということは、そのサーバでUser Unknownがわからないとダメ
      - 「MXを向けるだけ」のサーバではこの対策はできない！

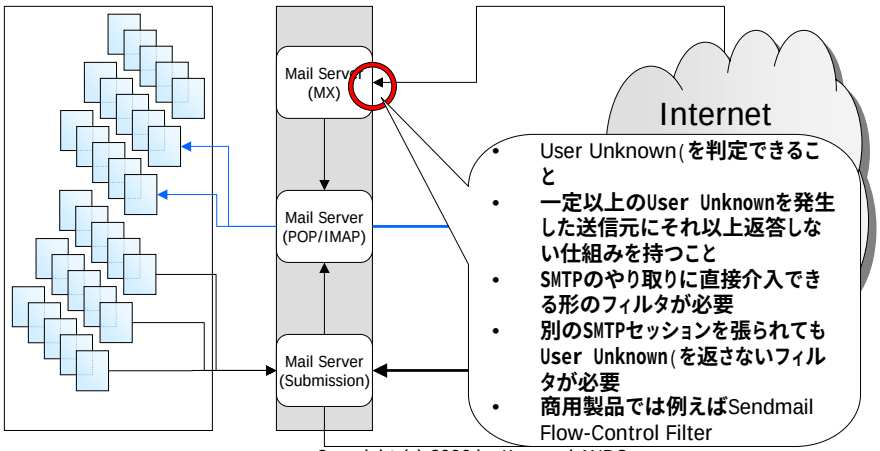
アドレス収集攻撃への対策

究極の姿は水際作戦

- オープンソースでの対策は?
  - SMTP接続の範囲内での対策が必要
    - SMTP接続の中に対策を埋め込めるのは Sendmail(のMilterの枠組みくらいしかない
- ISPクラスの大きさのサイトでは対策必須
  - 個人情報漏洩対策の一環とみなせる
  - 問題化は時間の問題
  - 「User unknownを一定以上の割合で含む場合にメール送信を拒否」だけでは不十分

アドレス収集攻撃への対策

究極の姿は水際作戦



アドレス収集攻撃への対策

RBL等IPアドレスでのブロック?

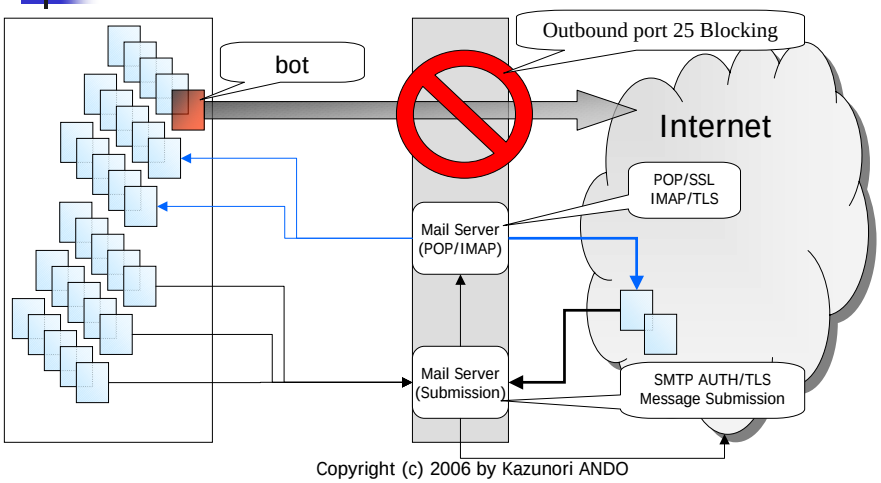
- RBL等での接続拒否は対策たり得るか?
  - 相手のbotはどこにでも発生
    - IPアドレスベースの対策はもはや現実的でない
    - そのIPアドレス経由のユーザが大量にいるケースでは弊害の方が大きくなる
  - ISPでは法的に黒に非常に近いグレー
    - メール受信の拒否には最低でもエンドユーザの承諾が必要だが、この方法だとそもそもエンドユーザ（受信側）が特定できない段階でフィルタすることになる

アドレス収集攻撃への対策

ISPによるOP25B

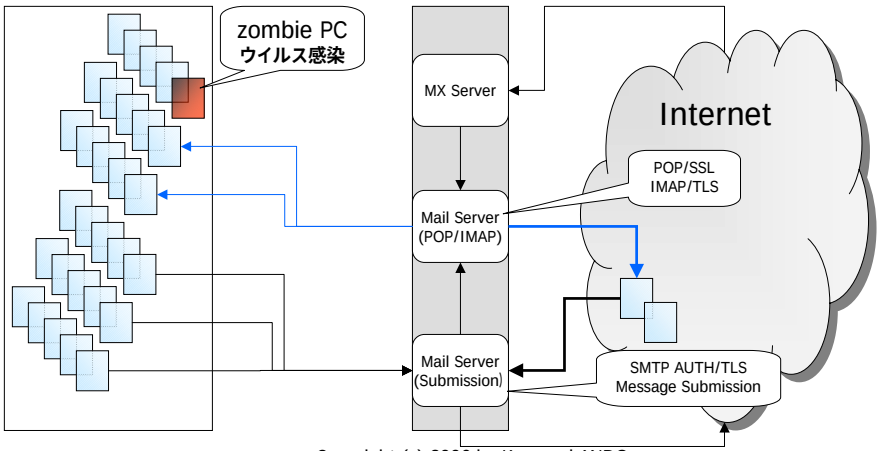
- 2005年の迷惑メール対策を象徴する大きな動き
  - ユーザに対して対外的なport25への通信を遮断
    - botによる迷惑メール送信が全メール流量の半数以上を占める状況にあって、何も知らないPC所有者を保護するために必要だった。
    - 代替送信手段（ISPのサーバやport 587等）が確保される。
    - 総務省により、違法性阻却事由あり（つまり遵法）と認められた対策
  - ISP内部のbotからISPのサーバへの攻撃は阻止できないが…
    - 問題をISPの内部に閉じ込める効果はある
      - 自ISPのユーザに寄生するbotだけを相手にすれば良い

ISPによるOP25B



IW2006 11

企業での基本構成



IW2006 12

スパマーの手口（認証破り）

- スパムの送信には送信元のパスワードも必要
  - スパマーはSMTP認証をクリアしてメールを送信したい
    - MUAの「パスワードを記憶」ダイアログでYESと答えると
      - どこかにパスワードが記録されているはず！
        - 記録される形式は安全なのか?
    - ボット／バックドア／キーロガー
      - 通信をモニタしてそこからパスワードを奪取
        - APOPが守れるのは、この部分
      - キーロガーなんて
        - 暗号化する前の生パスワードを盗聴

認証破りへの対策

POP before SMTPの限界

- bot
  - ユーザの気がつかないうちに乗っ取られる
- ワーム／ウイルス
  - 力任せに送信するとすぐに発見できるが…
- POP before SMTP
  - ユーザが1度メールをPOPで取得すると一定時間、そのマシンから使える認証なしリレーサーバを提供する仕組み

認証破りへの対策

POP before SMTPの限界

- 気づかれずに感染している場合
  - POP before SMTPは危険
  - メールサーバから見えるIPアドレスを共用している場合はさらに危険
    - FW経由であるとか、PROXY(経由であるとか
- 既に前世代のテクノロジ
  - 「なにもないよりはマシ」というレベル
  - パスワードもメール本文も平文で通信?
  - 早急にSMTP AUTHと経路暗号化を導入すべき

認証破りへの対策

APOPの神話

- 「APOPを使用するとセキュリティは安心」?
  - POPパスワードだけがChallenge/Response型に
  - サーバとMUA間でメールアドレスが漏れる時点で失格
  - むしろ「パスワードしか守れない」が正解
  - 経路暗号化に移行すべき
- 「APOPじゃダメなんですか?」
  - 通信経路が怪しい場合はダメです
  - 「あの電話局に行ってその後は…」ならまだ良いが
  - 「どの基地局が電波拾ってるんだこれ?」が現実

認証破りへの対策

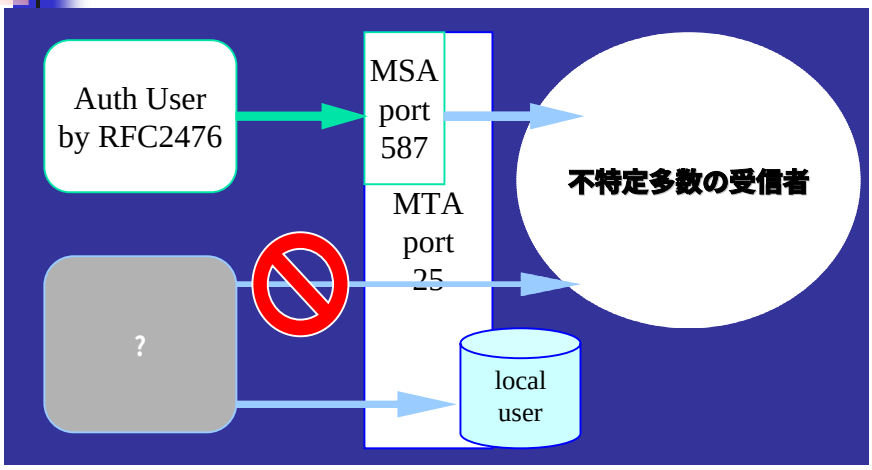
SMTP認証の完全利用

- POP before SMTPは過去の捨て去るべき技術
  - botはPOP before SMTPをクリアしてくる
  - そのSMTPコネクションがどのユーザのものかを確実に認識することができる
- OP25B対策としてのMessage SubmissionでもSMTP認証を必須にすること
- 仮にbotがパスワードを盗用してSMTP認証を突破してスパム送信した場合、不正アクセス禁止法で禁止された違法行為になる→スパム発信を法律で追い込むことに相当

Message Submission (RFC2476)

- MSA (Message Submission Agent)
  - メールを「送信MTAに渡す」枠組み
    - Relayと区別することでspam不正中継を防止
      - SMTPではlocal宛のメールしか受けない
      - Submissionによる発信は自分のサイトからの接続だけを許可してさらに認証をかける
    - port 587
      - sendmail-8.11以降はdefaultでMSAになる
      - MSP (MessageSubmissionProgram/クライアント) からの接続を受け付ける

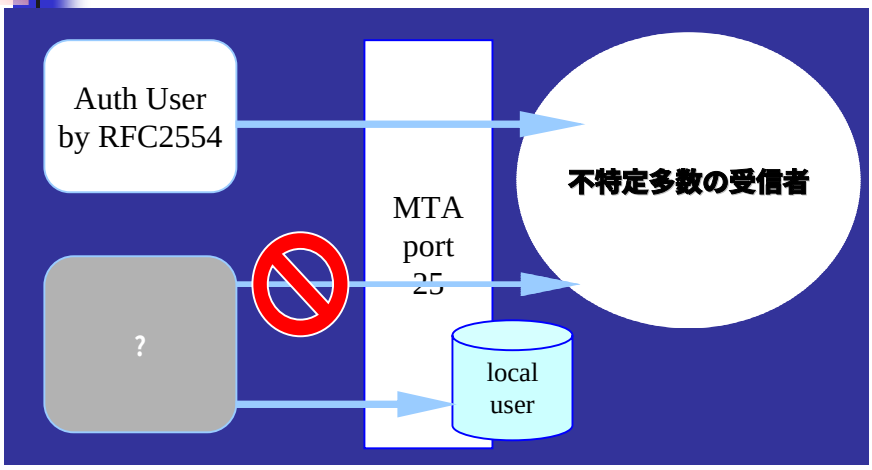
Message Submission (RFC2476)



SMTP Authentication (RFC2554)

- SASL (RFC2222) を利用したRelay認証
  - sendmail-8.13では
    - 必要な作業
      - cyrus SASLライブラリをインストール
      - SASLを利用するようにsendmailをコンパイル
      - /usr/local/lib/sasl/Sendmail.confの準備 (必要なら)
      - /etc/sasldb.dbの準備 (saslpasswdコマンドでユーザ登録)
      - sendmail.cfの設定追加
    - 認証を通るとそのサーバ経由のRelay配送を許可
    - SMTP/TLSを併用しましょう
      - PLAINとLOGINでパスワードが平文で飛ぶ認証形式しかサポートしていないOutl**k(のために...

SMTP Authentication (RFC2554)



IW2006 21

認証破りへの対策

経路暗号化の励行

- 認証の行われる通信を全て経路暗号化
  - POP/SSL(Port995)
  - IMAP/TLS(Port 443)
  - SMTP/TLS(Port 25,587)
- パスワード盗聴の危険度を軽減する
- SSL/TLSが持つ認証機構を利用するとなお良い
  - 鍵の管理が面倒というのはあるかも知れない

IW2006 22

認証破りへの対策

POP/SSLの利用

- SSL (Secure Socket Layer)
  - POPを経路暗号化
  - MUAとメールサーバ (POP) 間の通信からアドレスやメールの内容が漏れるのを防ぐ
  - 例えばqpopperでもこのTLSの枠組みを用いてPOPの接続を暗号化することが可能
    - OpenSSLの利用が前提
    - 商用版では使えるようになっている製品もある

認証破りへの対策

SMTP/TLSの利用

- TLS (Transport Layer Security)
  - 乱暴に言うと、ポートを変えずにSSL接続へ移行できる枠組みのこと
  - SMTPを経路暗号化
  - sendmailでもこのTLSの枠組みを用いてSMTPの接続を暗号化することが可能
    - OpenSSLの利用が前提
    - 商用版では使えるようになっている製品もある

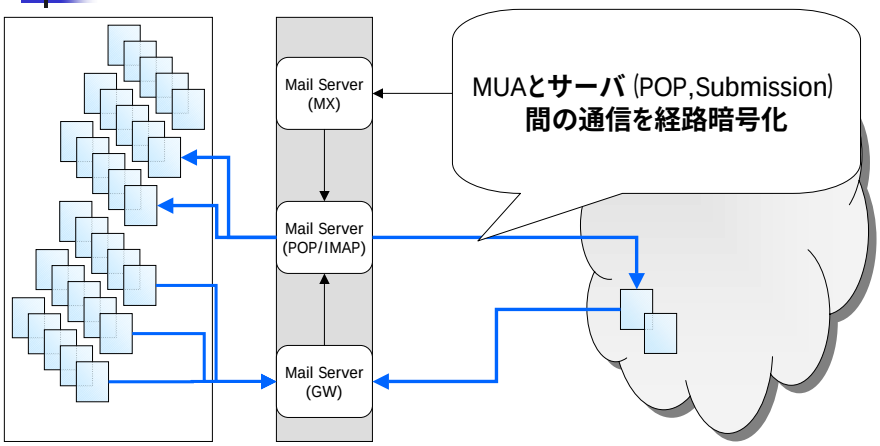
認証破りへの対策

鍵の準備

- TLS (SSL) には鍵 (証明書) が必要
  - CA (認証局) から購入
    - ユーザに対しサーバが「本物である」という証明が必要なら第三者の認証局で認証できる鍵を使う
  - 経路暗号化だけが目的なら自前の鍵で
    - オレオレ証明書と言われるかも知れないが…
    - 鍵の配布範囲にTLSでの認証の利用が限定される
    - ユーザ認証はSMTP AUTHでやる

認証破りへの対策

POP/SSL,SMTP/TLS



認証破りへの対策

ソフトウェア脆弱性への対策

- エンドユーザが使うPCのbot化を阻止
- ウイルスやbotはソフトウェアの脆弱性を突いて感染し拡散する
- 対象はOS、SSLパッケージ、圧縮ライブラリ、画像処理ライブラリ、WWWブラウザ、SSH、MUAなど多岐にわたる
- 脆弱性情報の収集が大事

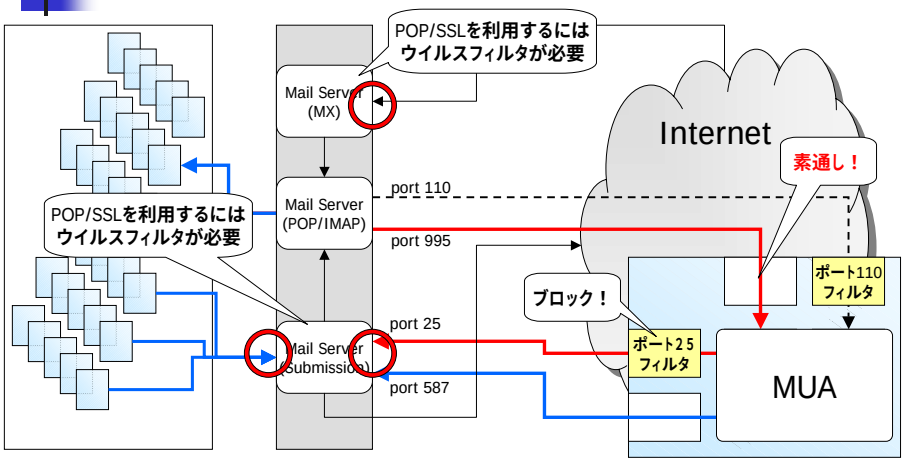
認証破りへの対策

ウイルスフィルタと経路暗号化

- MUAとメールサーバ間を経路暗号化
  - その経路上で動作するウイルスフィルタ
    - ユーザのPC上にあるProxy型のフィルタはそもそもPOP/SSLの通信をチェックしない
    - SMTP/TLS(の通信をブロックするものがある
      - 使い物にならない
  - 端点で動作するウイルスフィルタが必要
    - サーバ側かMUAが暗号化を解いた後か
    - 現実解はサーバ側のフィルタ

認証破りへの対策

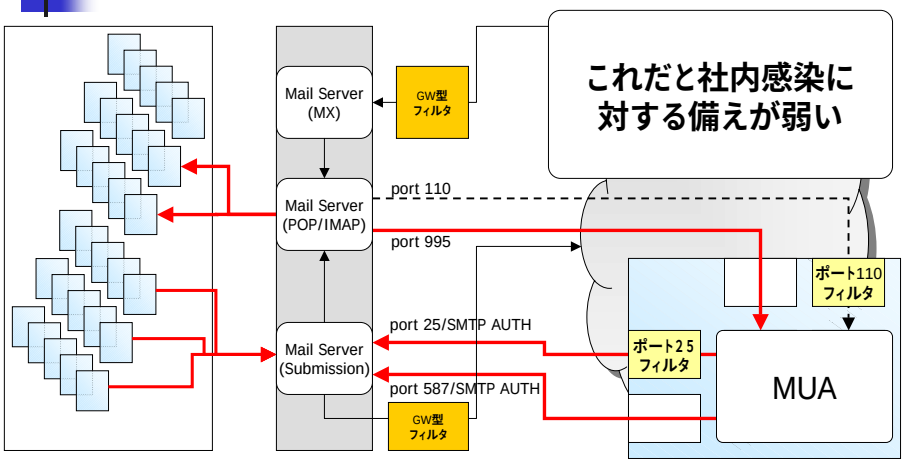
ウイルスフィルタと経路暗号化



IW2006 29

認証破りへの対策

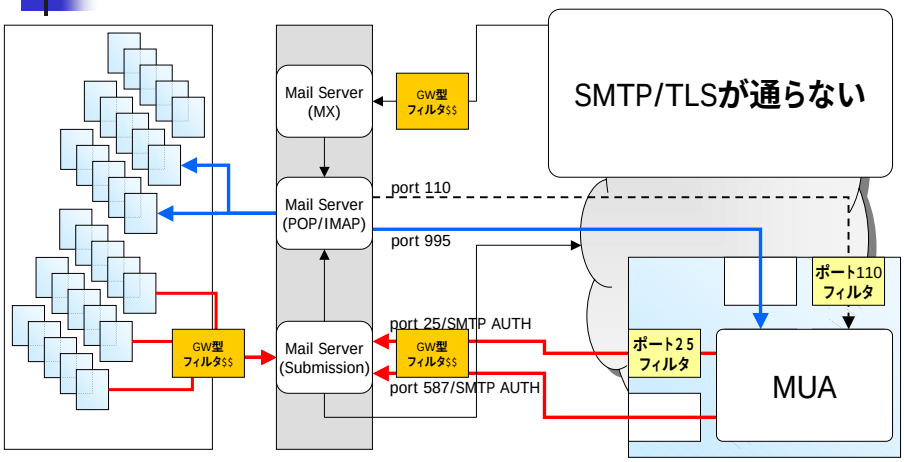
フィルタの配置（1）



IW2006 30

認証破りへの対策

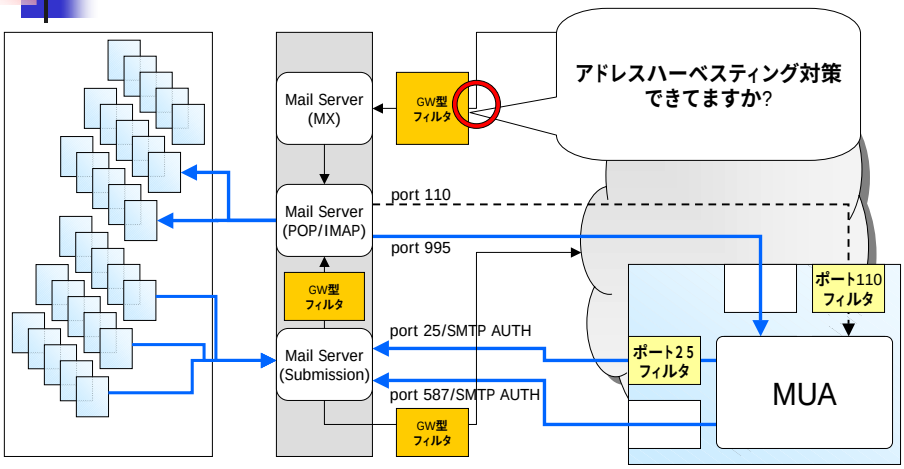
フィルタの配置 (2)



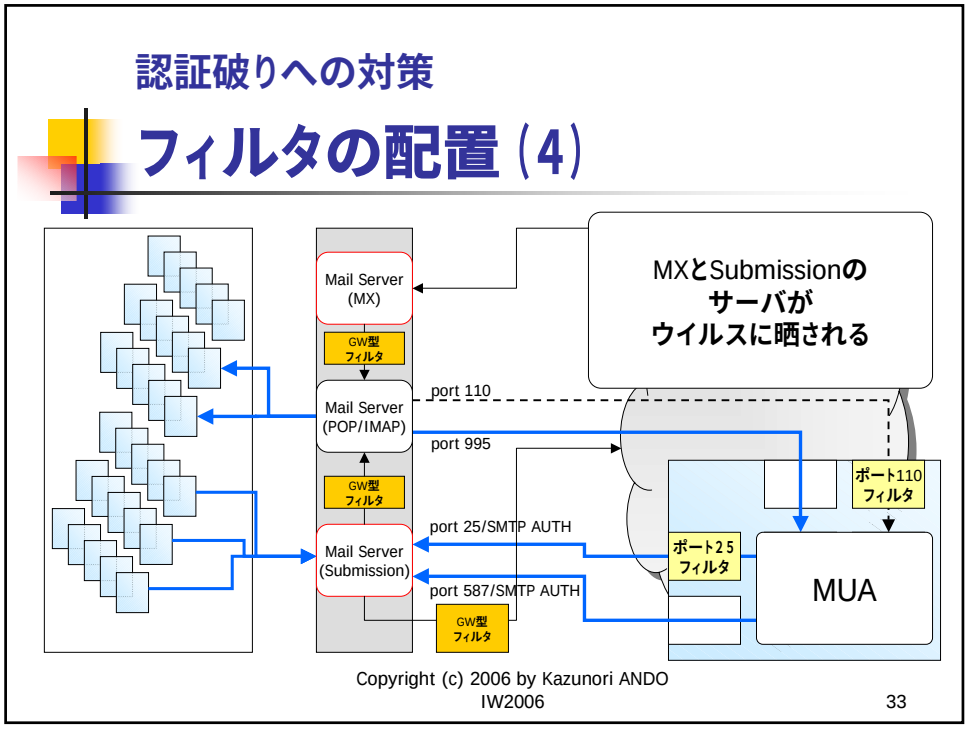
IW2006 31

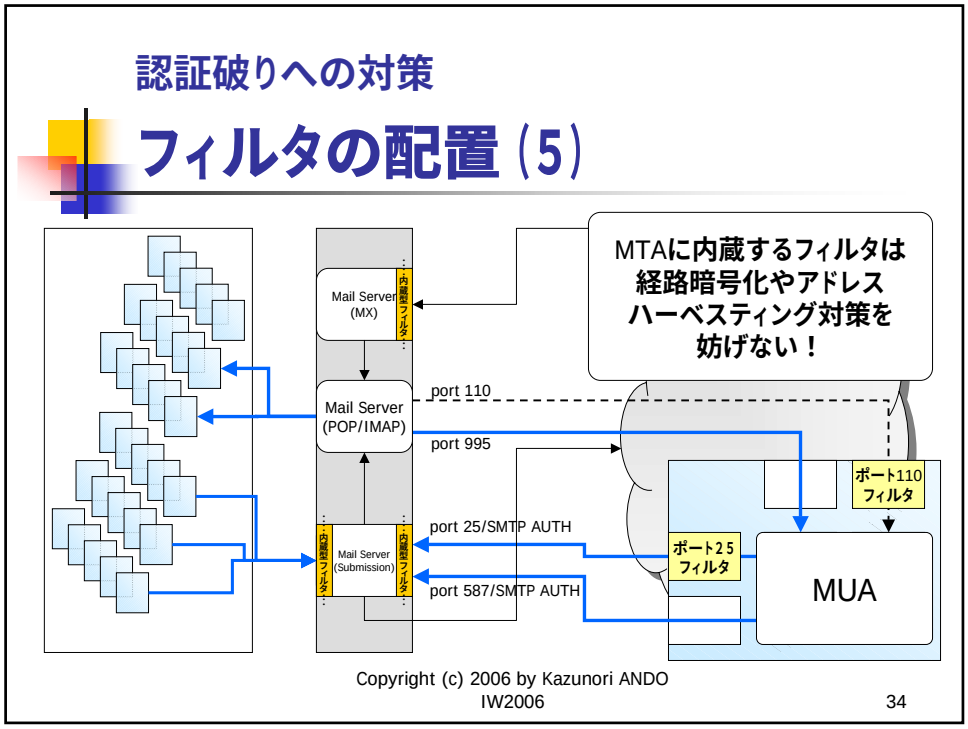
認証破りへの対策

フィルタの配置 (3)



IW2006 32


認証破りへの対策
フィルタの配置（4）
Mail Server (MX)
GW型フィルタ
Mail Server (POP/IMAP)
GW型フィルタ
Mail Server (Submission)
GW型フィルタ
MXとSubmissionのサーバがウイルスに晒される
port 110
port 995
port 25/SMTP AUTH
port 587/SMTP AUTH
ポート110フィルタ
ポート25フィルタ
MUA
Copyright (c) 2006 by Kazunori ANDO
IW2006
33


認証破りへの対策
フィルタの配置（5）
Mail Server (MX)
内蔵型フィルタ
Mail Server (POP/IMAP)
Mail Server (Submission)
内蔵型フィルタ
内蔵型フィルタ
MTAに内蔵するフィルタは経路暗号化やアドレスハーベスティング対策を妨げない！
port 110
port 995
port 25/SMTP AUTH
port 587/SMTP AUTH
ポート110フィルタ
ポート25フィルタ
MUA
Copyright (c) 2006 by Kazunori ANDO
IW2006
34

認証破りへの対策

他のフィルタの効果

- スパムを判定して応答遅延時間を増やす
  - 大量発信に対して有効
    - 1カ所からの大量送信は防げる
  - 多数のボットからゆっくり送信された場合は?
    - 多数の送信元からの送信数をモニタできるか?
  - アドレスハーベスティングには?
    - 多数の送信元からのUser Unknown数をある程度の時間モニタし続けないとbotに対しては効果がない

スパマーの手口（送信手段）

- 送信に使うのはbotnet
  - 乗っ取られ、かつクラスタとして動作するPC群
    - SMTP proxyだったり、送信エンジンを装備していたり
    - コントロールするPCから命令送信サーバを経由して指令を受け取って動作
    - 全世界に分布
  - PCの所有者も気づかないケースが多い
    - 知らない間にスパム発信元になっている

スパム送信手段への対策

メール経由のウイルス (1)

- 添付ファイルが感染源であることが多い
  - マクロウイルス (Excel、Word、PowerPoint)
    - 中に忍ばせてあるOfficeオブジェクトが曲者
  - 実行形式ファイル
    - 不用意に実行してはいけない
  - JPEG画像
    - 実行ファイルを仕込むことが可能
    - HTMLメールの画像表示 (リンク) だけで危険

スパム送信手段への対策

メール経由のウイルス (2)

- 自動的に実行されてしまう添付ファイル
  - .wav (nimda) とか.pif(Sircam)とか.scr(bugbear)とか
- 感染スピードの爆発的上昇
  - メール、HTTP、JavaScript、ファイル共有など複数経路で感染するワームの登場
  - 市販のウイルス対策プログラムのupdateが追いつかず、防ぎきれない例も多発
  - ウイルス除去プログラムが影響を除去し切れない例もある模様。
  - こまめにWindows updateを!

スパム送信手段への対策

メール経由のウイルス（3）

- 添付ファイル
  - 元凶はMIME-multipart（便利さの代償?）
    - 入れ子構造でファイルを添付できる
      - 2段目にファイルを添付した後の1段目にウイルス添付（nimda）
      - 1通に3種類のウイルスを貼付してくる例もある
      - 使われるContent-Typeも多様化している
  - 無限段まで入れ子をチェック
    - DoS対象になってしまうかも….

スパム送信手段への対策

ウイルス・ワーム対策体制の例

- ウイルス対策プログラムを過信しない
  - ウイルスの感染の方が速い場合がある
- できるだけ速い情報の収集
  - ワームによるアクセスを監視（WWWサーバやIDSで）
  - 感染経路情報を示して警戒呼びかけ
    - なにもやらないのと比較して格段の防御になる
- 大量感染源になり得る部分での対策
  - メーリングリスト・ドライバで添付ファイルの拡張子チェック＋削除（メーリングリストでの添付ファイル使用の禁止）
  - Windowsのsecurity-updateに常に注意を払う

スパマーの手口（目的の多様化）

- スパムはどんなことを目的としているか?
  - メールアドレスの死活
    - 例えば、MUAが画像リンクを辿って画像を表示すると、誰がどのIPアドレスでそのメールが読んでいるかが判明する
  - 詐欺サイトへの誘導
    - リンクは不用意にクリックしないように
    - アドレスとパスワード、カード番号の詐取に注意
  - bot配布
    - 画像の中に仕込んである場合がある
    - OS／ブラウザの脆弱性を放置してある場合にはとても危険

知っておくべきメールアドレス

- MAILBOX NAMES FOR COMMON SERVICES, ROLES AND FUNCTIONS (RFC2142) で挙げられているもの
- 例えば、
  - abuse@example.gr.jp
    - いざという場合の問い合わせ先
  - postmaster@example.gr.jp
    - メール配送についての問い合わせ先
  - hostmaster@example.gr.jp
    - DNSについての問い合わせ先

MLの周辺アドレス

- 周辺アドレスの例
  - owner-hoe@example.gr.jp
    - sendmail的にちょっと考慮されたMLの発信者アドレス
  - hoe-admin@example.gr.jp
    - 管理者のaliasとして使われることがある
  - hoe-request@example.gr.jp
    - RFC2142的管理者アドレス
  - hoe-errorsto@example.gr.jp
    - エラーメールの専用受信アドレスを用意している場合

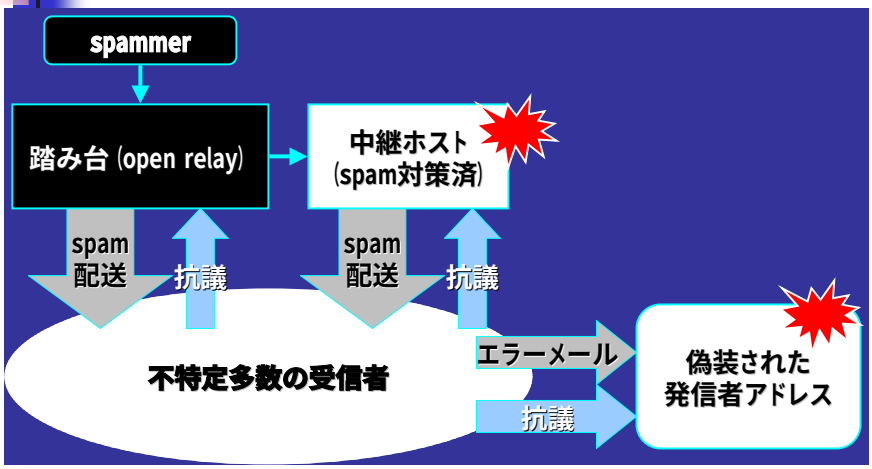
エラーメールの基礎

- エラーメール配信の枠組み
  - DSN (Delivery Status Notification)
    - Envelope From は null address (<>)
      - エラーメールに返信アドレスはない
- トラブルの種類を判定する手段
  - RFC1893 (Status Code) ：RFC2821に統合
    - Status: 5.1.1
      - 5.X.X　Permanent Failure
      - X.1.1　Bad destination mailbox address

エラーハンドリング問題

- 配送エラーコード (status code) の実装
  - 実際にRFCを守っているか？
    - sendmailやPostfix、SIMS等守っているものも多い
    - その他の対応はいまいち
      - MTAの数だけエラーハンドリングのプログラムが必要
      - 標準を守ろうとしないMTAは大迷惑なんだけど…
    - 大量にメールを配るところでは頭痛のタネ
    - 最近はウイルス通知メールの嵐
      - エラーメールの通知形式に準拠してくれないかなぁ….

spam中継の被害の構図



エラーメールによるRDDoS

- envelope-fromを詐称されてしまった場合
- 非常に多数のサイトから大量のエラーメール
- メインの1stMXが潰れそうになったら、1stMXをDNSから削除、TTLの短い2ndMXのみにする
  - RDDoSのエラーメールはDNSを新たに引いて2ndMXへ
  - 普段から良くメールの来る相手はDNSのcacheがあるので1stMXにメールが来る
  - DNSのcacheの生存時間を利用したエラーメールの振り分け
    - 岡山大学の山井先生の考えられた手法です（JANOG12）
      - RDDoS＝Reflected Distributed Denial of Service

大量のDoubleBounce

- エラーメールの配送エラー
  - 通常、エラーメールのエラーは消失する
    - エラーメールのsenderはnull-address
    - 例外がDoubleBounceの機能
    - DefaultではPostmaster宛になっている
  - envelope-fromの詐称による絨毯爆撃型spamの副作用として発生
  - DoubleBounceをOFFにする
    - ログをチェックすることが条件

必須の技術へ

- spam対策技術
  - 「来たときの対策」と「出させない対策」
    - SMTP Authentication (RFC2554)
    - Message Submission (RFC2476)
    - SMTP over TLS (RFC2487)
    - DHA対策フィルタ
    - 動的流量制限フィルタ
    - 各種のコンテンツフィルタ
  - メーリングリストではアドレス一覧を出さないこと
    - 一般参加者のwho/membersコマンドに対して
    - 過去のメールアーカイブをWWWで公開する場合、アドレスハーベスティング対策を！

最近の傾向 (1)

- 大規模化に伴う相対的な管理レベルの低下
  - ISP等では大規模化する一方
    - ユーザ管理の省力化を目的にサービスの簡単化を指向するケースがあるのはわかるが...
  - 携帯電話メールのトラフィックの増加
    - 容量は小さいが通数はものすごい
  - MIME-multipartによる添付文書
    - 容量が大きいのでspool容量の再考が必要なケースも

最近の傾向 (2)

- spam送信側が高度に組織化されてきている
  - botを束ねて送信してくる
    - ワームやトロイの木馬を利用してbotを増やす
    - botは世界中に分散している
    - USに持っていかれたアドレスに世界中のbotからspam
      - CAN-SPAM法対策か? (US国内法の範疇外になる)
  - 日本語のspamもそのような送信法で送られてくるようになった
    - 1つの国での対策はもはや限界

最近の傾向 (3)

- ISPが動き始めた
  - ユーザに対するspam対策手法の提供
    - 商用スパムフィルタの提供
      - ユーザが自分でON/OFFできることが必要
  - ISPは「発信させない対策」を実施
    - アドレスハーベスティング対策はまだまだ
    - SMTP AUTHとTLSの併用で発信者認証
    - ダイアルアップのセグメントはOP25B
  - 「特定電子メールの送信等に関する法律」の改正
    - 直罰規定が盛り込まれ警察の捜査が可能になった

最近の傾向 (4)

- 常時接続の問題 (bot対策)
  - botとそうでないPCの区別をどこで付けるのか?
  - SPFはドメイン内の送信ポリシーを記述できる
    - spammerもSPFのエントリーを書いてきている
  - 予防はウイルス対策と同等の扱いが必要
  - 本気でやるならOP25BとISPの中継サーバのSMTP認証の併用で送信制限するしかない
    - 住みづらい世の中になったものだ. . .
    - ISPにその余裕ある?

最近の傾向 (5)

- ISPはデフォルトでport 25をフィルタする!
  - 固定IPユーザだけport 25を通す
    - サーバ・マシン管理で自己責任を果たせることが必要
    - ISPのメールサーバを利用→サーバ側で頑張る
    - 自前メールサーバを利用→bot対策が必須
  - それだけ厳しい状況になりつつある
    - 快適な環境を得るために我慢しなければならない部分
    - Phishing等の犯罪の発生
    - spamの国際化
      - botは数百万台と言われている

最近の傾向 (6)

- 家電製品/コピー機にIP接続するものが出現
  - 一部製品はLinuxやWindowsベース
  - 管理者権限でパスワードなしでアクセスできるものが!
    - botにするには持ってこいの素材
    - ベンダーの方は是非製品のセキュリティチェックを
    - telnetは開いてるわ、FTPもsambaも．．．
    - リモートからrebootできてしまう．．．
    - オンメモリ動作（メモリ上にファイルシステム）しているものは電源OFFで一切の証拠が消滅．．．

最近の傾向 (7)

- 総務省の動き（2006年）
  - 改正特電法の施行
  - 各国とスパム対策に関する協定の締結
  - ISPのスパム対策技術に対する見解の発表
    - OP25B/IP25B
      - 違法性阻却事由あり（つまり遵法）
    - コンテンツフィルタ
      - サービスに後付けする場合、エンドユーザの意思でON/OFFできることが必要
    - 送信ドメイン認証によるフィルタ
      - ラベリング…違法性阻却事由あり
      - フィルタリング…コンテンツフィルタと同等にエンドユーザの意思でON/OFFできることが必要

最近の傾向 (8)

- 通信手段としてのメールの社会的な認知が進む
  - 直接的には犯罪の発生が契機になった
    - フィッシング
    - ワンクリック詐欺
  - 改正特電法で迷惑メールの発信に対して警察の捜査が可能に
  - 2006年は検閲の禁止（憲法に規定された基本的人権、国民の義務）とISPにおける迷惑メール対策の是非が問われた1年
    - どんなフィルタをどのように入れれば法的に問題がないのか?
    - エンベロープの情報も基本的に「通信の秘密」の保護の範囲内
    - 「何でも好きなように対策をすれば良い」という時代の終焉

アドレス詐称・隠蔽問題 (1)

- bombing等では発信者アドレスが偽装される
  - spam発信者を偽装して発信者をbombing
  - 発信者の偽装は特電法で規制されている
- MLに他人のアドレスを登録する
  - 自動登録でConfirmなしだとアウト
- 無料メールアドレスの転送機能
  - 誰に届くかわからないという意味で曲者

アドレス詐称・隠蔽問題 (2)

- Phishingが問題化
  - メールアドレスの詐称とWWWサイトの作りこみで個人情報を詐取する
  - 画像、バナーまで本物を使用
    - ページは本物でもID入力ウインドウが偽者の場合も
  - SSLでも証明書の中身まで確認しないとダメかも
    - 自己署名証明書とか、会社の存在までは証明できない証明書とか、問題がありそうなケースはいろいろある
  - メールでは詐称を防ぐ対策が必要に
    - アドレスは詐称できても発信サイトは隠しにくい
    - 発信者認証した後、その証拠をメールにどう残すか?

spam対策技術 (1)

- RBL (Realtime Blackhole List)
- SBL (Spam Blocking List)
  - spamの発信元を登録する闇魔帳
    - DNSと同じ枠組みで作られている
      - MTAがメール送信元のIPアドレスを照会
    - 自分のサーバが登録された場合
      - メールを受け取らない所が出てくる
  - botnet (botの大群) によりほぼ破綻
  - ISPでは接続を拒否した場合、「検閲の禁止」に抵触する可能性がある
    - エンドユーザがON/OFFできる仕組みの実装が困難

spam対策技術 (2)

- SPAMLIST (access_db)
  - 発信元についていずれかを指定して排除
    - メールアドレス (envelope from)
    - ドメイン
    - IPアドレス
  - リスト管理コストの増大が問題
- POP before SMTP
  - ISPで取り入れられている手法
    - POPアクセスの発信元に対してSMTP接続を許可する
    - 例えばqpopperにパッチを当てて実現する
  - 同じIPアドレスからbotと一般ユーザのメールが送信された場合、対策として無力。

spam対策技術 (3)

- Sender Base
  - spamを発信したことを記録している一種の信用 (reputation) サービス。
    - IPアドレス、IPブロックのオーナー、ドメイン、ドメインのオーナー等でグルーピングしている。
    - RBLの発展型とみることができる。
  - botからの発信でもIPアドレスブロックの信用度は下がってしまうのか?
    - 信用を供託金で買うBonded Sender Programが存在
      - そこってお金で解決する問題?

spam対策技術 (4)

- ベイズ推定を用いたフィルタ
  - 狙いはspamに登場する語句の出現傾向
    - 語句の出現傾向からspamかどうかを判定する
    - 辞書が比較的大きくなる
    - 言語依存 (現状で英語、日本語くらいならOK)
  - 弱い相手
    - 画像1枚、リンク1つだけのspam
    - 大量の一般的な文書に埋め込まれた広告
    - 縦書きの日本語文書！
    - あの手この手の偽装手段
  - 各個人のspamの定義の違いを吸収する手段としてMUA(への実装が定着しつつある
    - 負荷的には大規模サーバでの実装には向かない

spam対策技術 (5)

- パターンマッチ
  - 例えば正規表現でパターンを指定
    - 個人で使ってもあまり効果はない
    - サーバで使用すると効果的
    - 誤判定リスクはパターン次第
    - 言語への依存性は実装次第
  - パターンの管理コストが問題になる

spam対策技術 (6)

- ヒューリスティック・フィルタ
  - 各部のパターンを抽出して確率で引っ掛ける
    - Fromヘッダの特徴
    - Subjectの特徴
    - Toの特徴
    - Receivedの特徴
    - Content-Typeの特徴
    - . . . と積み上げて判定する手法
  - ベイジアンフィルタと融合して普及?

spam対策技術 (7)

- URLをベースにしたspam排除
  - URLのパターンマッチ的な手法はよくある
    - 誤判定リスクは排除すべきURLの確認に依存
    - userinfoとquery部分を宛先ごとに改変している例
    - 言語依存性なし
  - 携帯電話のスパム対策で使用されている

spam対策技術 (8)

- デジタルシグネチャ (d-sig) のDB化
  - spamの各パートのd-sigを検知する
    - MIME multipart解析
    - d-sigが一致する (同一の内容の) partがあればspamと判定する
    - spamの内容も (ランダム文字列等で) その都度改変されるので、データの共有と更新が効果を上げる鍵になろう
    - ウイルスフィルタは基本的にはこのタイプだが、ウイルスと比較して変化の速いスパムに対してはこの方式単独ではあまり有効性を確保できない

spam対策技術 (9)

- Channelled Address
  - 宛先に応じて自分のアドレスを変える
    - この宛先には自分のアドレスはこれで. . . と決めうち。
  - 返信先がその宛先用のアドレスかどうかでspam判定
  - USではAT&Tの特許があって使用許諾が必要。
    - WebMail形式のサービスとしてZoEmailというのがある。
    - 日本では講演者の特許検索の範囲では見つからず

spam対策技術 (10)

- 自動確認付きホワイトリスト
  - メールを出してきた相手に、「ほんとに送りたいならこのメールに返答してね」と返信し、そのメールに返答のあった送信者をホワイトリストに登録する。
  - MLの登録認証のしくみに似ている。
  - 相手が自動応答アドレスであった場合、そのメールはどこへ行くかわからない。

spam対策技術 (11)

- 流量制限
  - しきい値を超えるとtempfailを返す実装が現実的
  - BruteForce型spam等への対策
  - 同一送信元IPアドレスからのメールの受信数を制限
    - 動的に受信拒否動作をするものもある。
  - 同一送信元IPアドレスからのSMTP接続数を制限
    - Sendmailでも実装
  - 同一送信元IPアドレスからのUser Unknown(数を制限
    - アドレスハーベスティング対策

Phishing対策技術 (1)

- SPF
  - AOLが採用している送信ドメイン認証
  - 自ドメインのメール発信ホスト/ポリシーをDNSに登録
  - 受信側はSMTP Senderから、登録された送信ホストからの発信かどうかをチェックする。
  - http://spf.pobox.com/

```
example.jp.  IN TXT "v=spf1 ip4:218.223.0.0/22 ip4:210.164.161.64/27
 mx a:accele.ope.example.jp a:sv04.example.jp a:jasmine.example.jp
 include:example.com -all"
```


Phishing対策技術 (2)

- Sender-ID (MS Caller-ID + SPF)
  - SPFとCaller-IDの融合規格として出てきたもの
  - MSの未公開特許が含まれ、無償提供ながらライセンスに対する警戒感からかいままでの普及はイマイチ
  - Microsoftは**Sender-IDの仕様に関してライセンスフリーで提供**することを発表 (2006.10.23)
    - 今後の普及動向が注目される
    - sid-filter (http://www.sendmail.net/)

Phishing対策技術 (3)

- DKIM (Yahoo! DomainKeys + CISCO Identified Mail)
  - 公開鍵暗号を利用した送信ドメイン認証の仕組み
  - 公開鍵をDNSに掲載し、送信サーバでは正規に登録されたユーザからの送信メールに秘密鍵でサインして送信する。
  - ヘッダに記載された送信アドレスとDNSから得られる公開鍵を用いて、サインの正当性を検証する。
  - Yahoo!,Google (Gmail) ,Sendmail等
    - dk-milter (SourceForge.net)

spam対策の傾向 (1)

- アドレス偽装の問題化
  - Phishing (個人情報の詐取目的のメール) の横行
  - 送信ドメイン認証はPhishing対策の色合いが濃い
  - 特電法の直罰規定の効果は? (改正法は17年11月1日施行)
- ベイジアンフィルタはMUA側に実装
  - メールの振り分けをするため、POPサーバではアカウントが2つ必要になってしまう。IMAPならいいかも。
  - ISP側で一律にスパムをフィルタすることは困難
    - spamの定義は人それぞれ (ユーザ個々に辞書を持たなければいけない)
    - 通信の秘密 (検閲の禁止) に引っかからないためにはユーザが自分でフィルタのON/OFFを選択できることが必要
  - ナイーブなベイジアンフィルタはspammerの対抗策のためほぼ終焉。

spam対策の傾向 (2)

- spam発信側の技術の高度化
  - フィルタはアルゴリズムがわかると突破される
    - ベイジアンフィルタに対するWord-Salad等
  - botの存在
    - 持ち主の知らない間に発信サイトになっているPC
    - 常時接続ゆえの怖さ
  - WWWサイトに載せてあるアドレスにspamが来る
    - 実験済
    - 米国内のあるサイトに持っていかれたアドレスに世界中のbotからspamが届く

spam対策の傾向 (3)

- サーバに対するアドレスハーベスティングの激化
  - 大規模サイトはアドレスハーベスティング対策が必須条件になりつつある
    - エンドユーザから見たキーワードは「本文のないスパム」
      - 何のために送ってくるのか?
      - User Unknown(が返るかどうかでアドレスの存在を確認
        - 大量に繰り返すと存在するアドレスがリストになる
        - リストが流通するとスパムが増加する
    - サーバ管理者から見たキーワードは大量のUser Unknown
      - アングラでツールが流通しているっぽい
        - と思ったら、spamでそういうツールを売り込んでいるでは…

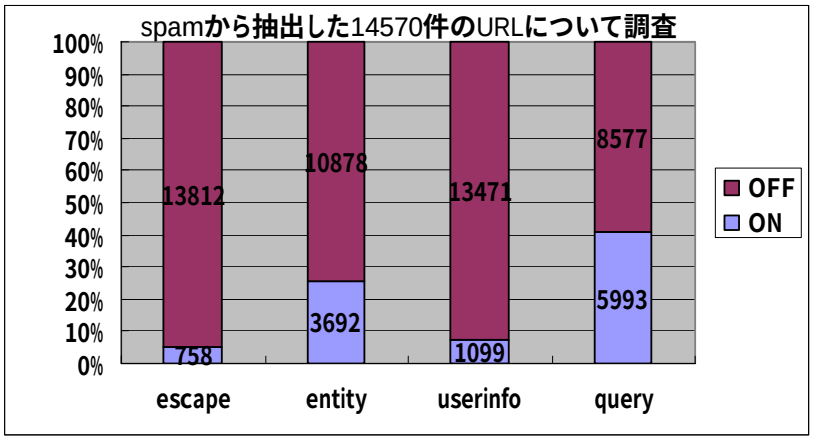
spam対策の傾向 (4)

- 受信対策から出させない対策へ
  - 大規模サイトはまずアドレスハーベスティング対策を
  - 発信者認証 (SMTP AUTH) の積極的な採用を
  - 認証結果を記録
    - 認証アドレスをSenderヘッダに記録
      - Senderヘッダは配送に影響しない→控えめな対応
    - 認証アドレスをSMTP senderにして発信
      - 完全に普及するとエラーメールRDDoSへの対策になる
  - 認証を通らないメール送信の遮断
    - OP25B
    - IPアドレスブロックの管理責任

spam対策の傾向 (5)

- メール中のURLの詐称
  - 2004年の講演の時点でURLの隠蔽状況をまとめていたが、Phishingの横行で心配は現実のものとなった。
  - MUAの持つ脆弱性にはこまめなアップデートで対応
  - セキュリティ情報に常に関心を持つこと
    - 重大なものは社内にアナウンスすることも必要

URLの改変可能要素



spam対策の傾向 (6)

- JPEG画像にbot(やワームやスパイウェアを仕込む
  - 2004年から問題化
    - HTMLメールでリンクが張られているJPEG画像を読み込んだだけで感染
    - 根本はOSの画像表示用ライブラリの問題なので、そこを対策しないと、ブラウザもMUAも危ない。
    - 単純なspamかどうかの判定も難しくなってきた
    - ウイルス対策→ bot対策→ spam対策という構図が発生

Spam対策の傾向 (7)

- シマンテック社の動き
  - 米国Security Focus (脆弱性情報サイト) を買収
  - 米国BrightMail (商用スパムフィルタベンダー) を買収
- マカフィー社 (ネットワークアソシエイツ) の動き
  - DeerSoft (SpamAssassinの母体) を買収
    - Apache SpamAssassin ProjectでOpensource版も継続
- 被害をもたらしている主なウイルスもspamとして配信されてくる
  - ウイルスフィルタで排除すべき対象
  - ウイルス対策ベンダーがspam対策に動き出しているが…

法律の整備

- 不正アクセス禁止法
  - 他人のパスワードの盗用を禁止している
    - 送信にSMTP認証→パスワード盗用での送信は黒
- 特定電子メールの送信の適正化等に関する法律 (特電法)
  - 基本的にopt-outで良いとする考え方
  - 架空メールアドレスへのメール送信も規制 (DHAも一部規制されている)
  - 直罰規定が盛り込まれて実効性が少し増した
    - 国内法なので送信元が国内ならなんとかなる
  - 合法スパムの条件を規定
    - 送信者アドレスを偽装してはいけない
    - 送信者を文面で表示しなくてはいけない
    - Subjectにも表示義務
- 個人情報保護法/通信の秘密
  - ログやユーザアカウントデータ、メールアーカイブ等が対象になりそう
  - 通信事業者向けには個人情報保護のための社内規定作り等が総務省のガイドラインで示されている

業界動向分析(1)

- 国内大手ISP(のスパムフィルタはほぼ二極化
  - Cloudmark(Sendmail,Openwave,OCN,Biglobe,So-net,αWeb…)
    - 協調型フィルタ
    - DNAパターン検索技術の応用
    - 170万人超のレポータからの情報がベース
      - レポートからデータのアップデートまでが極めて高速
  - Brightmail系(@NIFTY,Hi-Ho,IRONPORT…)
    - 複合型フィルタ
    - 多数のアルゴリズムの併用で精度を確保
    - ハニーポットからの情報がベース

業界動向分析(2)

- 国内ISP(のメールサービスもほぼ二極化
  - コストをかけてでもガチンコで対策して高機能化
    - アドレスハーベスティング対策
    - 商用ウイルスフィルタの追加
    - 商用スパムフィルタの追加
    - 経路暗号化のサービス実装
      - 必ずサーバ側ウイルスフィルタとペアで提供すべき
    - OP25Bに対応してMessage Submission/SMTP AUTH対応
    - 送信ドメイン認証に対応
  - コストに負けて従来仕様でそのまま運用
    - アドレスハーベスティング対策なし
    - とりあえずゲートウェイ型のウイルスフィルタを採用
      - 経路暗号化に対応した配置で採用してくれればいいが
    - スパムフィルタなし
    - 経路暗号化対応せず
    - OP25B対応せず、POP before SMTP(で運用
    - spamの温床にならなければ良いが…

管理コストの最小化 (1)

- 管理コストの最小化を狙うシステム作り
  - サーバ管理者が管理すべき内容
    - アドレスハーベスティング攻撃 (DHA) 対策
    - DoS対策
    - ウイルスフィルタの定常稼働 (データ更新)
    - スパムフィルタの定常稼働 (データ更新)
    - 不正侵入/ソフトウェア脆弱性対策
    - ログの取り扱い
    - アドレスの新規作成/削除
  - エンドユーザに管理を任せるべき内容
    - 転送先の設定
    - エンドユーザ別のブラックリスト／ホワイトリストの設定
    - スパムフィルタのON/OFF (特にISPの場合は必須)
    - パスワードの変更

管理コストの最小化 (2)

- DHA/DoS対策ソフトの選定ポイント
  - 多数の送信元に対して単位時間あたりのUser Unknown数/送信通数/接続数を把握できること
    - 対外セグメントのサーバでUser Unknownがわからないとダメ
    - 結局何らかのDBと連携動作しないといけない
  - 閾値を超えた送信元に対して自動的に一定時間だけtempfailを返す設定ができること
    - tempfailは受信拒否ではないことがポイント
  - 一定時間後には初期状態に復帰すること
    - この最後の条件が管理コストを著しく下げる

管理コストの最小化 (3)

- 商用ウイルスフィルタ/スパムフィルタの選定
  - 高負荷に強いものを選択
    - 動作が軽くマシン負荷の小さいものが良い
  - パターンデータの自動更新機能は必須
    - 学習型、パターン手動設定の必要なものは却下
  - 高検知率と同時に低誤検知率のものが良い
  - ISPではスパムフィルタはエンドユーザの設定で完全に素通しできる配置をすること
    - 検閲の禁止（憲法、電気通信事業法、有線電気通信法）に配慮した構成にしましょう！（訴訟リスクの回避）

管理コストの最小化 (4)

- 対外セグメントに配置するサーバは最低2台の複数サーバ構成にすること
  - メール受信は極端な変動もあり得る
    - DoS以外にメルマガ配信等で高負荷を生むケースがある
  - 脆弱性対策/不正侵入対策でのサーバ全停止は管理コストを増大させる
  - 後方サーバへのメールがQueueingできること
  - POP/IMAPサーバは出来ればローカルセグメントに配置したい

管理コストの最小化 (5)

- 複数サーバ構成でもログは一元管理すべき
  - ログを調べるために複数サーバを渡り歩くのは管理コストの増大と調査時間の無駄に繋がる
  - 検索システムがあればベスト
- アカウント管理
  - CSVデータの流し込みに対応できるか?
  - GUIで特定アカウントだけの設定が変更できるか?

付録 (devtools/Site/siteconfig.m4)

```
APPENDDEF(`conf_sendmail_ENVDEF', `-DMILTER')
APPENDDEF(`conf_sendmail_ENVDEF', `-DSASL')
APPENDDEF(`conf_sendmail_LIBS', `-lsasl')
APPENDDEF(`confINCDIRS', `-I/usr/local/include/sasl1')
APPENDDEF(`confLIBDIRS', `-L/usr/local/lib')
APPENDDEF(`conf_sendmail_ENVDEF', `-DSTARTTLS')
APPENDDEF(`conf_sendmail_LIBS', `-lssl -lcrypto')
```

付録（社内ホスト設定例）

```
VERSIONID(`$Id: config.mc,v 1.8 2006/12/05 12:27:36 ando Exp ando $')
OSTYPE(bsd4.4)dnl
DOMAIN(generic)dnl
MASQUERADE_AS(`example.jp')dnl
MASQUERADE_DOMAIN(`accele.example.jp')dnl
FEATURE(`limited_masquerade')dnl
FEATURE(`masquerade_envelope')dnl
EXPOSED_USER(`root postmaster')dnl
FEATURE(`mailertable')dnl
FEATURE(`nocanonify')dnl
FEATURE(`access_db')dnl
FEATURE(`blacklist_recipients')dnl
FEATURE(`accept_unresolvable_domains')dnl
FEATURE(`no_default_msa')dnl
MODIFY_MAILER_FLAGS(`LOCAL', `+S')
MAILER(local)dnl
MAILER(smtp)dnl
Dmexample.jp
Dwaccele
define(`confDOMAIN_NAME', `$w.$m')dnl
define(`confTO_IDENT', `0s')dnl
define(`confCF_VERSION', `IW2006 Sample')dnl
define(`confMAX_QUEUE_CHILDREN', `100')dnl
define(`confMIN_QUEUE_AGE', `1m')dnl
define(`confAUTH_MECHANISM', `[LOGIN PLAIN DIGEST-MD5 CRAM-MD5]')dnl
TRUST_AUTH_MECH(`LOGIN PLAIN CRAM-MD5 DIGEST-MD5')
dnl INPUT_MAIL_FILTER(`sid-filter', `S=inet:8891@localhost')
INPUT_MAIL_FILTER(`dk-filter', `S=inet:8892@localhost')
define(`confCACERT_PATH', `/etc/ssl/CA/certs/')
define(`confCACERT', `/etc/ssl/CA/ca.crt')
define(`confSERVER_CERT', `/etc/ssl/CA/certs/server-ca.crt')
define(`confSERVER_KEY', `/etc/ssl/CA/private/server.key')
```