快適なメール環境を維持するための メールサーバ構築

安藤一憲
ando@iri-com.co.jp

このチュートリアルの構成

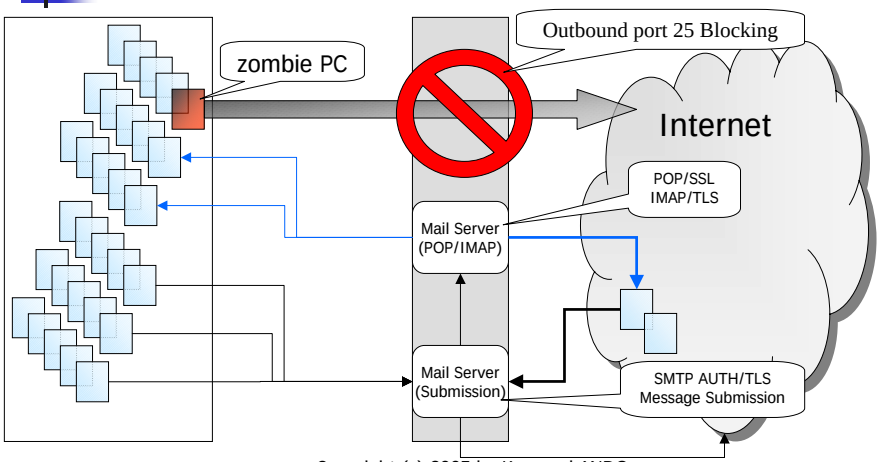
- Outbound Port 25 Blocking(
  - Message Submission(Port 587)も同時に普及
  - 問題はそれだけか?
- 知れば知るほど厳しいメール環境
  - User unknownのパラドックス
  - POP before SMTPの限界
  - ゲートウェイ型フィルタの盲点
  - 経路暗号化の落とし穴

Outbound Port 25 Blocking (OP25B)

- 足回り回線を提供するISPがPort 25をブロック
  - ゾンビPC対策
  - 動的にIPアドレス付与する接続に対して適用
  - メール送信はMessage Submission(Port 587)を使用するようにユーザに案内
  - 国内でも大手ISPが徐々に導入してきている

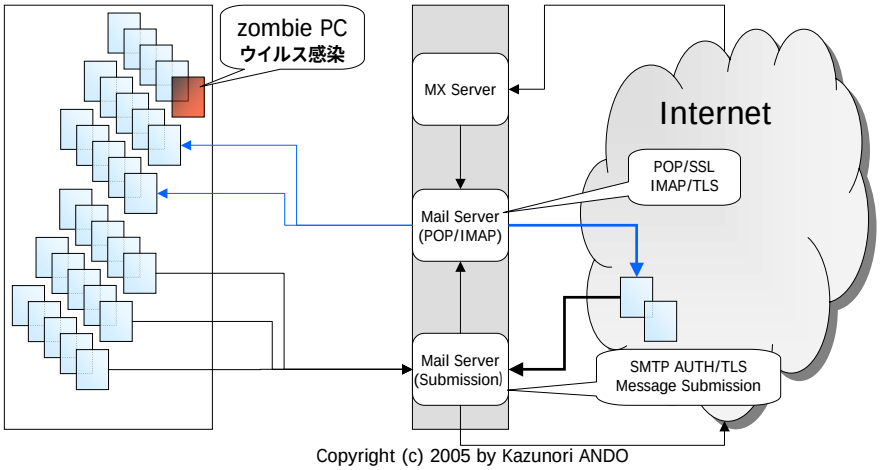
IW2005 3

ISPでの基本構成



IW2005 4

企業での基本構成



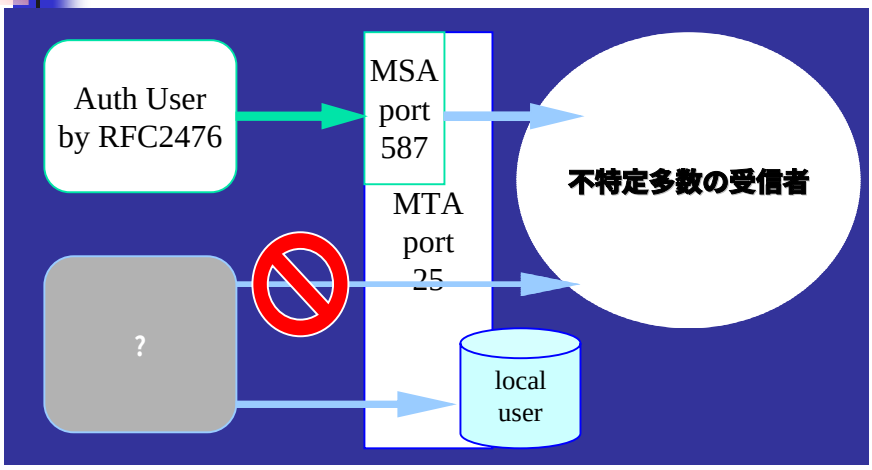
IW2005 5

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**

IW2005 6

Message Submission (RFC2476)



User unknownのパラドックス

- エラーメールの滞留するメールサーバ
  - エラーメール滞留で高負荷
    - 配送が遅延
  - 原因はエラーメールを受け取らない送信元からの大量のメール送信
    - Spam送信なのか?
    - ログを見るとそうとは限らない
      - DATAコマンドを打っていない例もある

User unknownのパラドックス

- 実は大半がアドレスハーベスティング
  - 辞書引きでRcpt Toをめくら撃ち
  - User unknown(をチェック
  - ならなかったものはアドレスが存在
  - 多数のユーザを抱えるサイトほど被害甚大
  - アングラでツールが出回っている模様

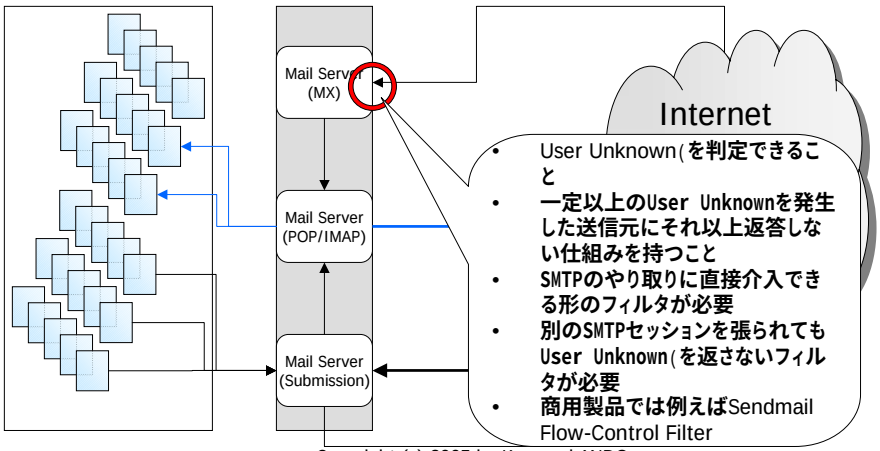
User unknownのパラドックス

- User unknownを返すな!?
  - ブラックホール型サーバは実現可能だが
    - ML等で無効なアドレスが検知できなくなる
      - 結果、無駄なメール送信が増加
      - MXサーバへのアドレスハーベスティングと同じ状態になり得る
  - 一見さんお断り方式だと
    - 通常のメール配信にも一定の遅延が発生する
      - 送信側メールサーバの負荷が増加
  - User unknown(を頻発する送信元を判別
    - 辞書引きだけに本当に頻発
      - 判別したらそこからのSMTP接続はfailさせる

User unknownのパラドックス

- 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

アドレスハーベスティング対策



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?
    - だめかも
  - アドレスハーベスティングには?
    - ボット併用されるとだめかも

POP before SMTPの限界

- ゾンビPC
  - 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されるが…
- 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

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

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
  - 通信そのものを暗号化するPOP/TLS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

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

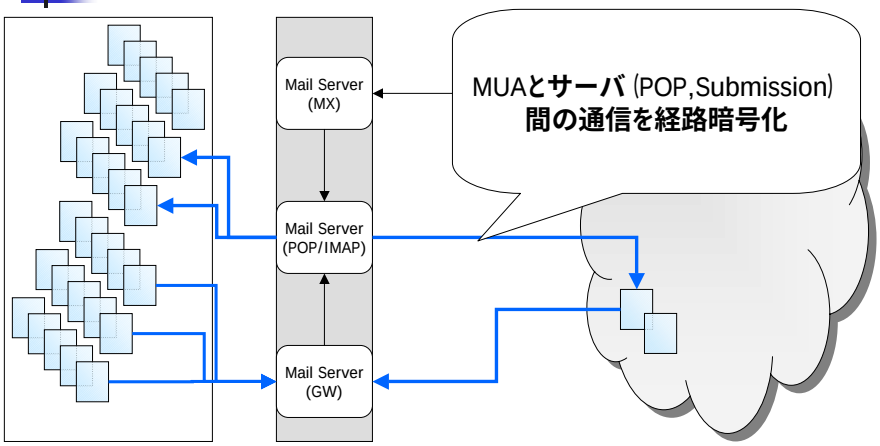
SMTP/TLSの利用

- 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

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

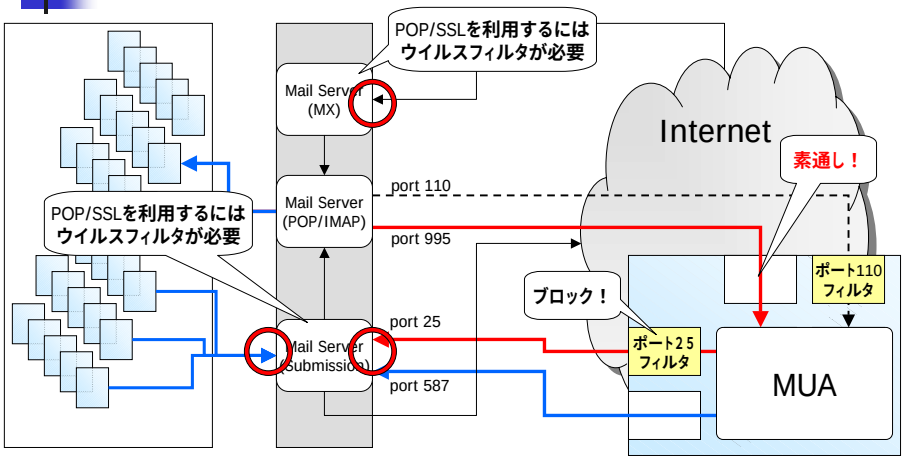
POP/SSL,SMTP/TLS

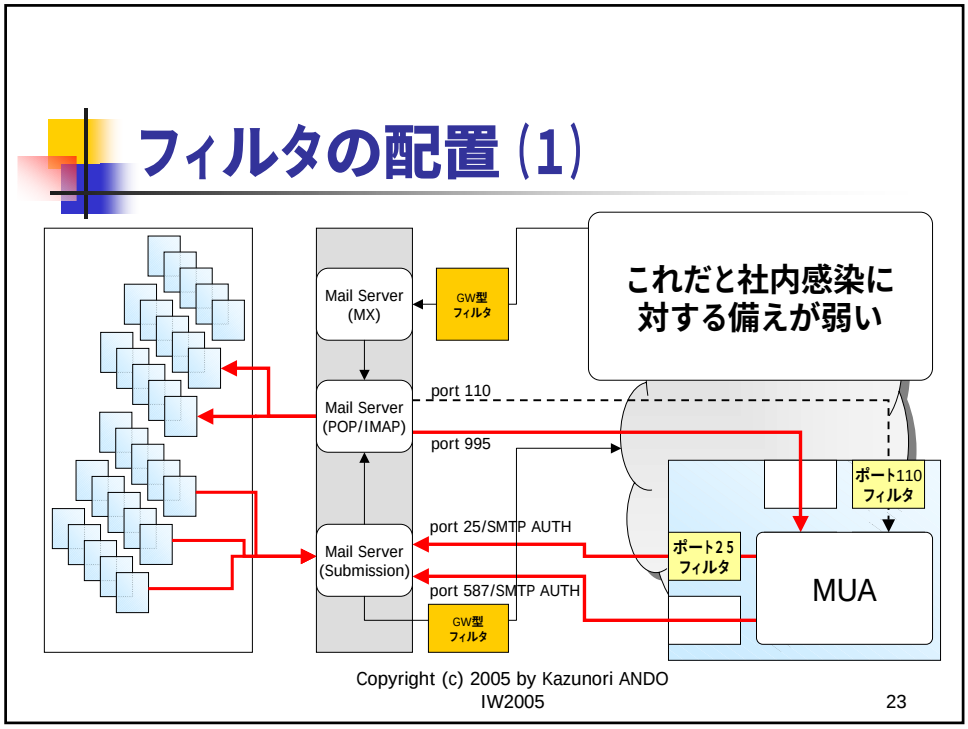


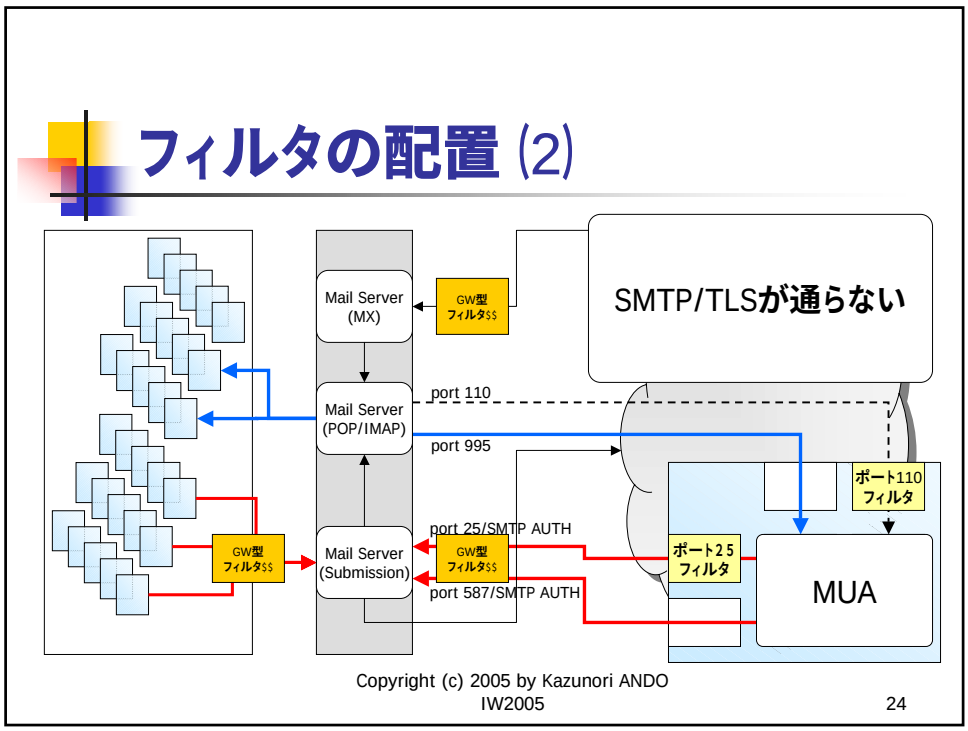
ウイルスフィルタと経路暗号化

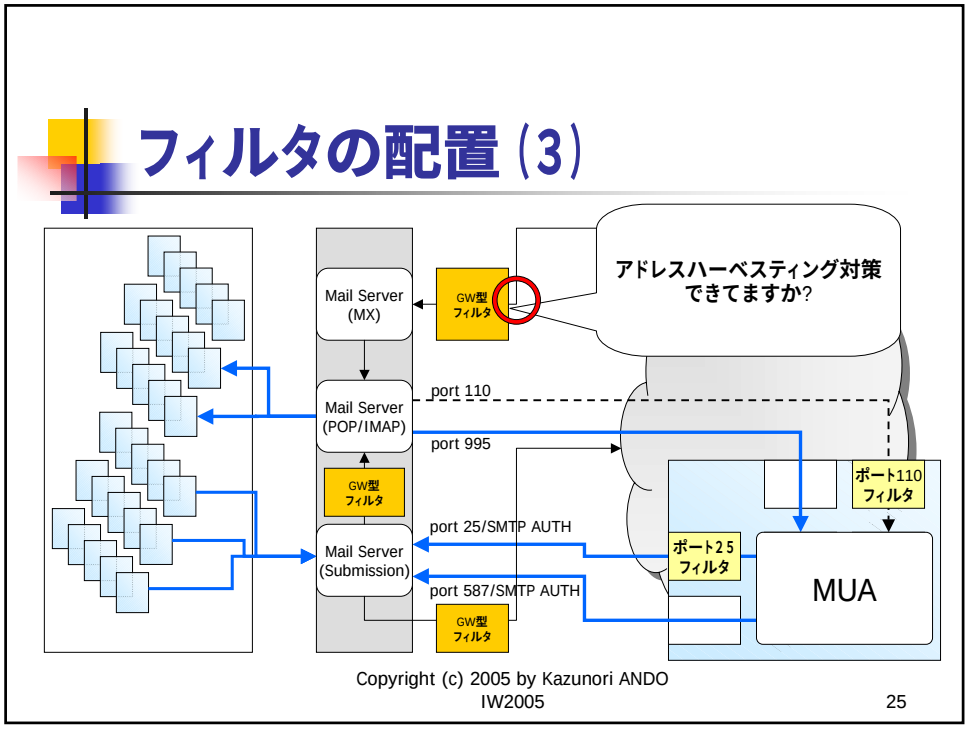
- MUAとメールサーバ間を経路暗号化
  - その経路上で動作するウイルスフィルタ
    - ユーザのPC上にあるProxy型のフィルタはそもそもPOP/SSLの通信をチェックしない
    - SMTP/TLSの通信をブロックするものがある
      - 使い物にならない
  - 端点で動作するウイルスフィルタが必要
    - サーバ側かMUAが暗号化を解いた後か
    - 現実解はサーバ側のフィルタ

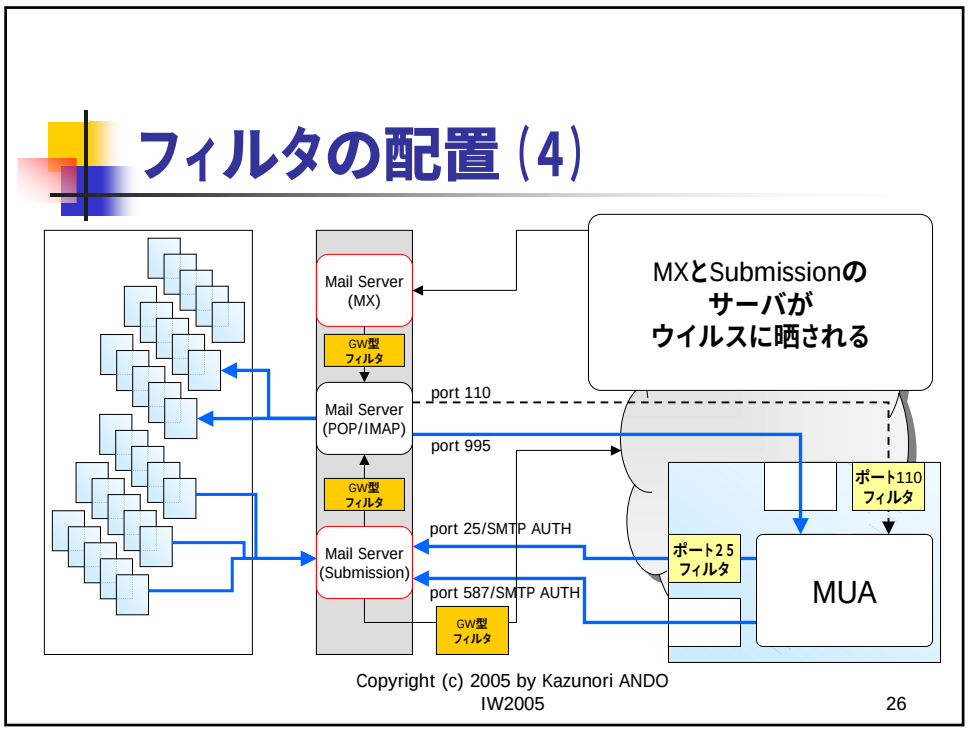
ウイルスフィルタと経路暗号化



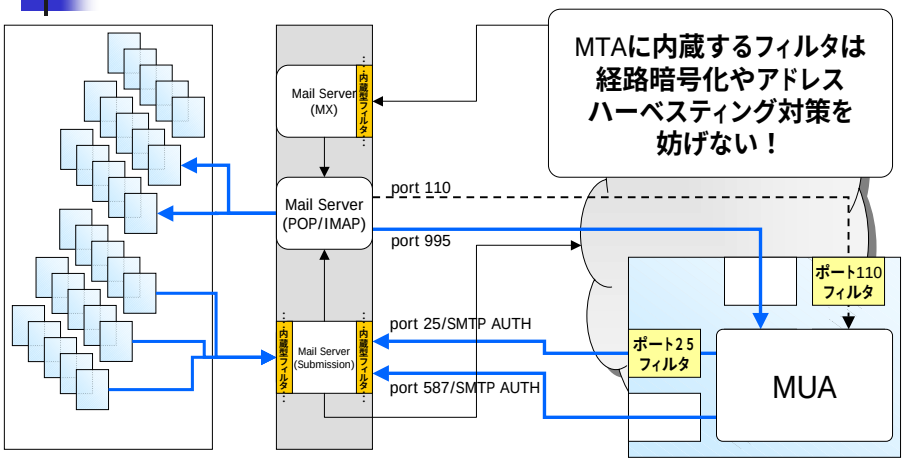

フィルタの配置 (1)
Mail Server (MX)
GW型 フィルタ
これだと社内感染に 対する備えが弱い
Mail Server (POP/IMAP)
port 110
port 995
ポート110 フィルタ
port 25/SMTP AUTH
Mail Server (Submission)
ポート25 フィルタ
MUA
port 587/SMTP AUTH
GW型 フィルタ
Copyright (c) 2005 by Kazunori ANDO
IW2005
23


フィルタの配置 (2)
Mail Server (MX)
GW型 フィルタ$$
SMTP/TLSが通らない
Mail Server (POP/IMAP)
port 110
port 995
ポート110 フィルタ
GW型 フィルタ$$
port 25/SMTP AUTH
Mail Server (Submission)
GW型 フィルタ$$
ポート25 フィルタ
MUA
port 587/SMTP AUTH
Copyright (c) 2005 by Kazunori ANDO
IW2005
24


フィルタの配置（3）
アドレスハーベスティング対策
できてますか?
Mail Server
(MX)
GW型
フィルタ
port 110
Mail Server
(POP/IMAP)
port 995
GW型
フィルタ
ポート110
フィルタ
port 25/SMTP AUTH
Mail Server
(Submission)
ポート25
フィルタ
MUA
port 587/SMTP AUTH
GW型
フィルタ
Copyright (c) 2005 by Kazunori ANDO
IW2005
25


フィルタの配置（4）
MXとSubmissionの
サーバが
ウイルスに晒される
Mail Server
(MX)
GW型
フィルタ
port 110
Mail Server
(POP/IMAP)
port 995
GW型
フィルタ
ポート110
フィルタ
port 25/SMTP AUTH
Mail Server
(Submission)
ポート25
フィルタ
MUA
port 587/SMTP AUTH
GW型
フィルタ
Copyright (c) 2005 by Kazunori ANDO
IW2005
26

フィルタの配置 (5)



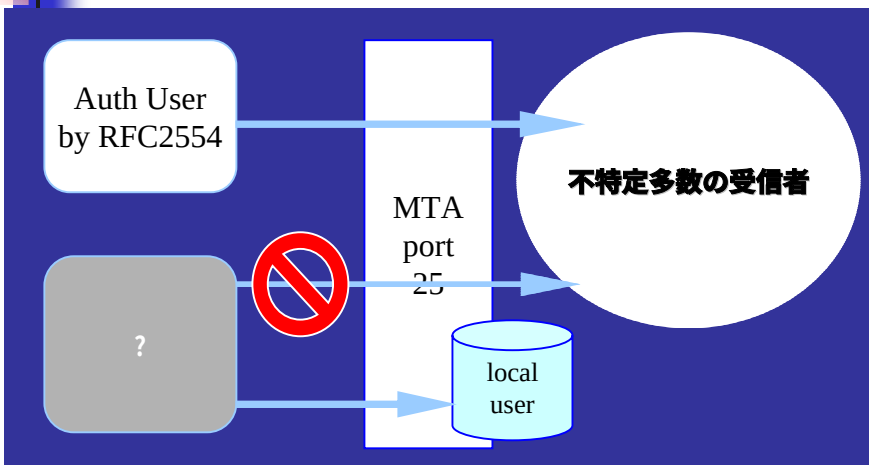
IW2005 27

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...

IW2005 28

SMTP Authentication (RFC2554)



IW2005 29

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

IW2005 30

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!

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)
      - たまにデリミタの使い方を間違っているワームもある (Sircam)
      - 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....

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

チェインメール

- 善意の協力依頼を装う（あるいは本物）
  - 「このメールを転載して下さい」が曲者
    - 無制限の転載を意図している場合には無視
    - 本来の目的を達成するには、期間や範囲を限定して一定数しか転載されない工夫を
- 不幸･幸福のメール
  - 「このメールを5人に転送しないと．．．」
    - 初心者の多い環境で流行りやすい

メール爆撃 (Bombing)

- 2種類ある
  - 巨大なサイズのメールを送付
  - 膨大な数のメールを送付
    - どちらもspoolを膨らませる結果になる
    - loopと見分けがつきにくい場合がある
- サイズ制限、通数制限等の防御
  - メーリングリストではさらに深刻な問題に
  - O MaxMessageSize=500000

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

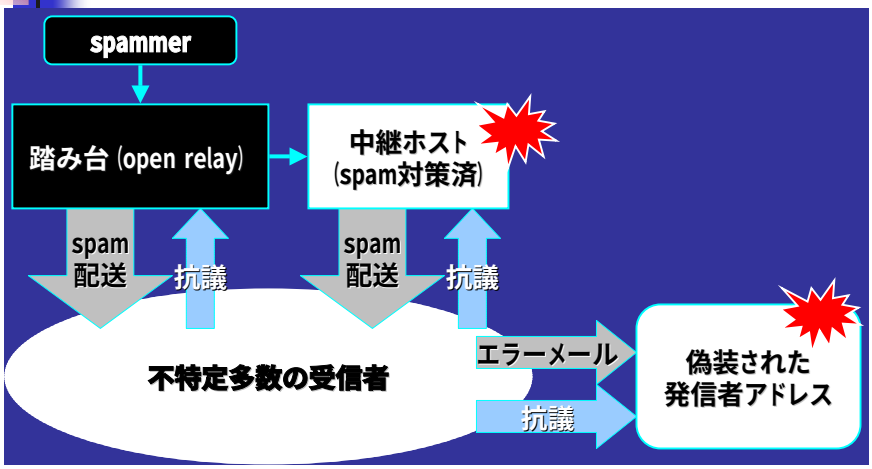
エラーメールの基礎

- 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)
    - RBL/SBL
    - Bayesian filter
    - URL filter
  - 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
  - ゾンビPC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ゾンビPCを増やす
    - ゾンビPC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ゾンビPC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らしい
    - 1つの国での対策はもはや限界

最近の傾向 (3)

- ようやくISPが動き始めたらしい
  - 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
    - ベイジアンフィルタの提供
    - 逆引きエントリの存在しないサーバからの受信拒否
      - ビジネスユーザを抱えていると危険ではあるが....
  - ISPでは「発信させない対策」をして欲しい
    - アドレスハーベスティング対策
    - SMTP AUTHとTLSの併用で発信者認証を
      - 正式ユーザのspam発信は約款で禁止し明示的に罰則を
      - ダイアルアップのセグメントはOP25B

最近の傾向 (4)

- 常時接続の問題 (ゾンビPC対策)
  - ゾンビPC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→ゾンビPC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
      - ゾンビPCは数百万台と言われている

最近の傾向 (6)

- 家電製品にIP接続するものが出現
  - 一部製品はLinux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!
    - ゾンビPC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．．．

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
- 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
    - 残念ながら訴訟対策のためかどんどん有料化
      - ORDBでも寄付を募っている
    - 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 (ゾンビPCの大群) によりほぼ破綻

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アドレスからゾンビPC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。
  - ゾンビPCからの発信でもIPアドレスブロックの信用度って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
    - 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

spam対策技術 (9)

- 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"
```

spam対策技術 (10)

- Sender-ID (MS Caller-ID + SPF)
  - SPFとCaller-IDの融合規格として出てきたもの
  - IETF->IRTF->ASRG->MARIDでRFC化を目指した
  - 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普及はイマイチ (送信者とみなされるべきヘッダの選択方法が特許になっている)
    - sid-filter (http://www.sendmail.net/)

spam対策技術 (11)

- 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対策技術 (12)

- 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 (13)

- 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 (14)

- 流量制限
  - 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

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
- 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
  - ゾンビPC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ゾンビPC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…

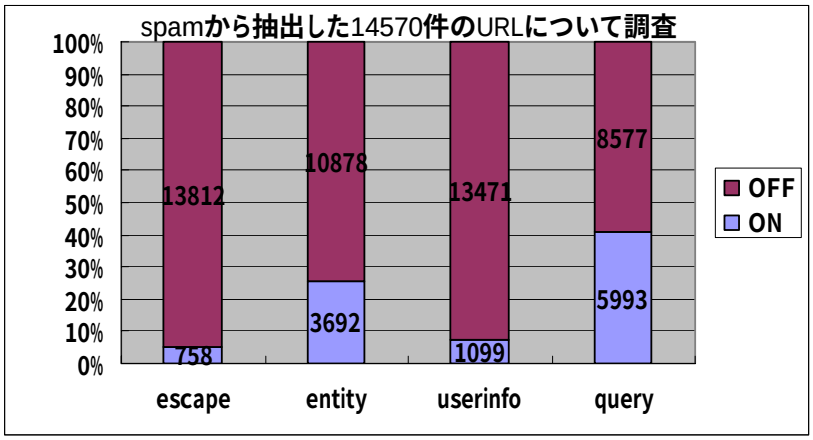
spam対策の傾向 (4)

- 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
  - 昨年の講演の時点で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
  - 昨年問題化した新種
    - 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Windowsの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→ ゾンビPC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を買収
  - 米国BrightMail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

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
    - 170万人のレポータからの情報
      - 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 (IIJ,@NIFTY,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

業界動向分析(2)

- 国内ISP(のメールサービスはほぼ二極化
  - コストをかけてでも対策して高機能化
    - アドレスハーベスティング対策
    - ウイルスフィルタオプションの追加
    - スパムフィルタオプションの追加
    - 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
    - 送信ドメイン認証への対応
    - OP25Bに対応してMessage Submission/SMTP AUTH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...

まとめ(1)

- メールサーバの管理は難しくなってきている
- spamを発信させないのは社会的要請
  - 不用意なメール中継をしないのは当然
  - アドレス漏洩を阻止せよ！
  - ユーザの利便性を確保するため発信者認証を利用
  - 認証パスワードの漏洩を防ぐためにTLS/SSLを利用
  - 無知なユーザをも守る施策を!
    - 言うばっかしで行動しないのもアレなので、私も今年はとりあえずISP向け対策全部入りMailASPを立ち上げてみました。

まとめ (2)

- 受信したspamへの対策はMUAの機能が鍵
  - 例えばMozilla Thunderbirdの場合
    - ベイジアンフィルタ装備
    - アドレス帳にあるかどうかでフィルタ設定が可能
      - ホワイトリストとして利用できる
    - spamフィルタにはヘッダ情報を付加するものが多い
      - 任意のヘッダ情報を見るようにフィルタ設定が可能
  - ユーザの教育も欠かせない
    - ウイルス対策のないメールサーバにPOP/SSLすると自分のPCのウイルス対策ソフトが効かずにウイルスに感染する危険があることをどれだけのユーザが知っているだろうか?

まとめ (3)

- POP/IMAPサーバについても
  - 企業の場合、出先 (モバイル環境) からの使用を考えなければならない
  - POP/SSL、IMAP/TLSといった技術を利用すること
    - サーバ側でのウイルス対策が必須になります
    - 平文パスワードの飛ぶ状態での使用は絶対に避けること
    - APOPなら良いか?
      - APOPはCHAPと似ていて、サーバから渡される文字列とshared passwordの文字列を合わせて、サーバ側とクライアント側でMD5ハッシュ値を計算し、クライアントの計算結果をサーバ側で検証することで正当性を認証する仕組み. ユーザ名はばれる。

その他注意すべき話題

- MD5 (128bit) が破られると...
  - 以下のような認証が破綻
    - APOP
    - SMTP AUTH/SASL (CRAM-MD5、Digest-MD5)
    - PAP/CHAP (ダイアルアップの認証)
    - 被害甚大だが既にハッシュ値の衝突が起きるデータの生成方法が論文発表されたりしている模様
- SHA1 (160bit) が破られると...
  - SET (電子決済) が破綻
    - 考えたくない事態に...

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 1.6 2005/12/04 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', `IW2005 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')
```