これまでの迷惑メール対策のおさらい

山井 成良（東京農工大学）

第12回迷惑メール対策カンファレンス【東京】

October 9, 2015

迷惑メールの動向

迷惑メール

- 受信者が望まない電子メール
  - ウィルスメール
  - 架空請求メール
  - フィッシング(phishing)詐欺メール
  - 広告メール
  - エラーメール

    など

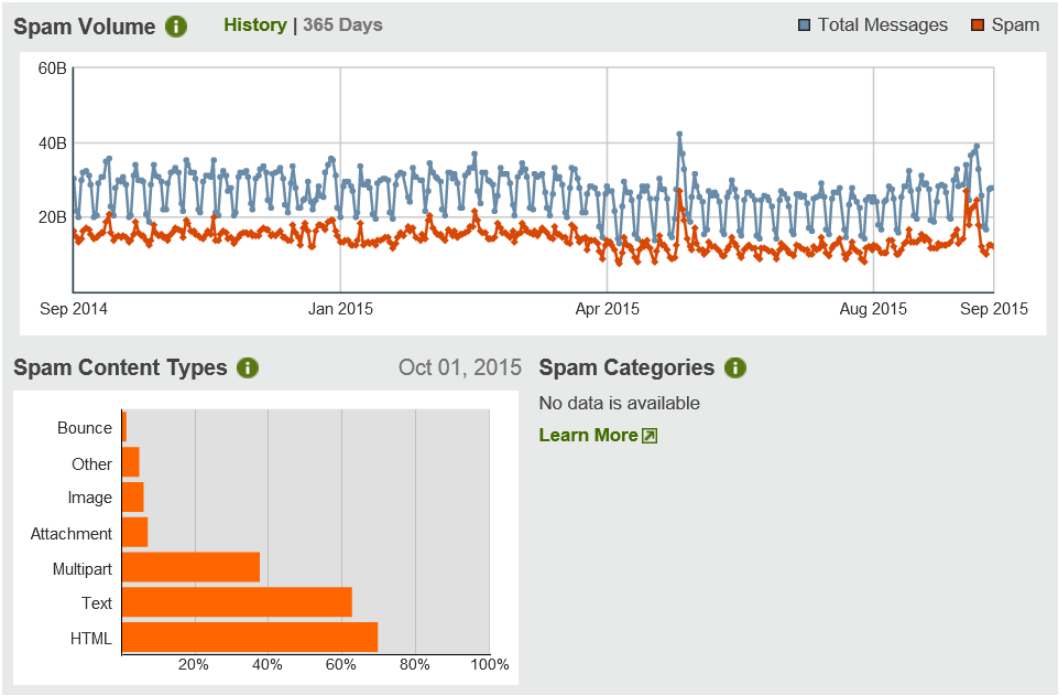
Spamメール

- SPAM（全て大文字）
  - 米Hormel Foods社の商品&登録商標
    - http://www.spam.com参照
  - “Monty Python’s Flying Circus”の寸劇に登場
- spam（全て小文字）
  - 一方的かつ大量に送られる電子メール
  - Hormel Foods社も公認
  - UCE (Unsolicited Commercial E-mail)
  - UBE (Unsolicited Bulk E-mail)

Spamメールの現状

- Spamメールの流量
  - 最近は減少傾向だがそれでも50%以上

（シマンテックSecurity Responseより）



標的型攻撃（1）

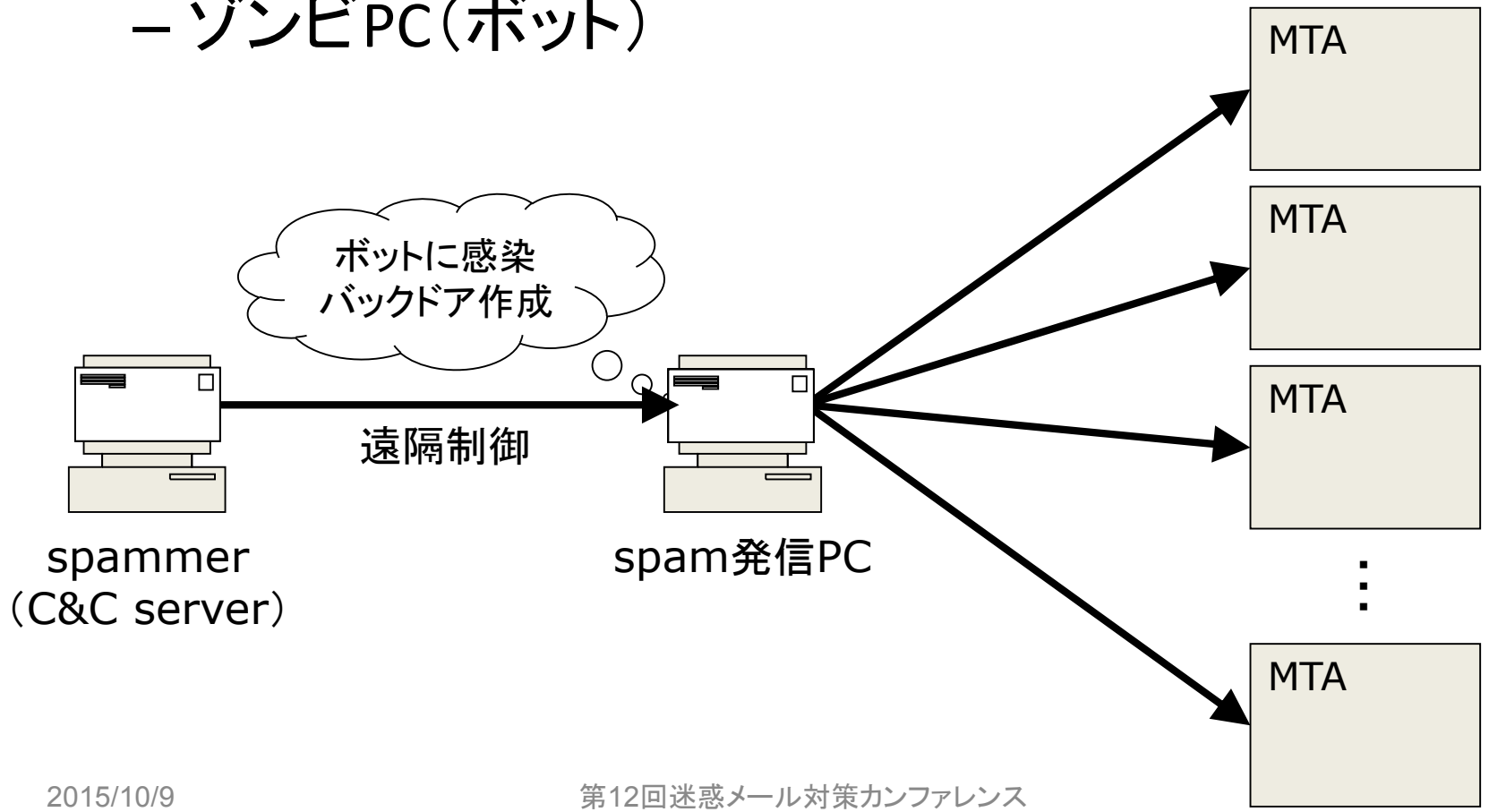
- 衆議院への攻撃
  - 2011年7月発生，8月発覚，10月報道
  - 感染サーバ・端末: 32台，ID・パスワード: 1142人分
  - 差出人：週刊誌の記者名を騙ったもの
  - 件名：お願い事
  - 本文：最新号の週刊誌にあなたの顔写真を掲載することになりますがよろしいですか
  - 添付ファイル：Photo.zip
    - 開くとキーロガー，リモート操作などの不正プログラムを実行（トロイの木馬）
- 参議院への攻撃
  - サーバ・端末: ３１台
  - 2011年8月発生，11月発覚・報道
  - 差出人：未公表（jpドメイン）
  - 件名：「『内部資料』中国権力継承の動き」，「資料送付のお知らせ」

標的型攻撃(2)

- 日本年金機構への攻撃
  - 2015年5月発生・発覚，6月報道
  - 感染端末: 31台
  - 流出個人情報: 約125万件分(約101万人分)
  - 4回にわたり攻撃
    - 1回目(5/8):「厚生年金基金制度の見直しについて(試案)に関する意見」×2通
      - 1台感染→4時間後LANケーブル抜線
    - 2回目(5/18):「給付研究委員会オープンセミナーのご案内」×98通
      - 3台感染→実害なし(C&Cサーバへの通信失敗)
    - 3回目(5/18-19):「厚生年金徴収関係研修資料」×20通
      - 未感染
    - 4回目(5/20):「【医療費通知】」×3通
      - 計21台感染→国内サーバへ個人情報流出

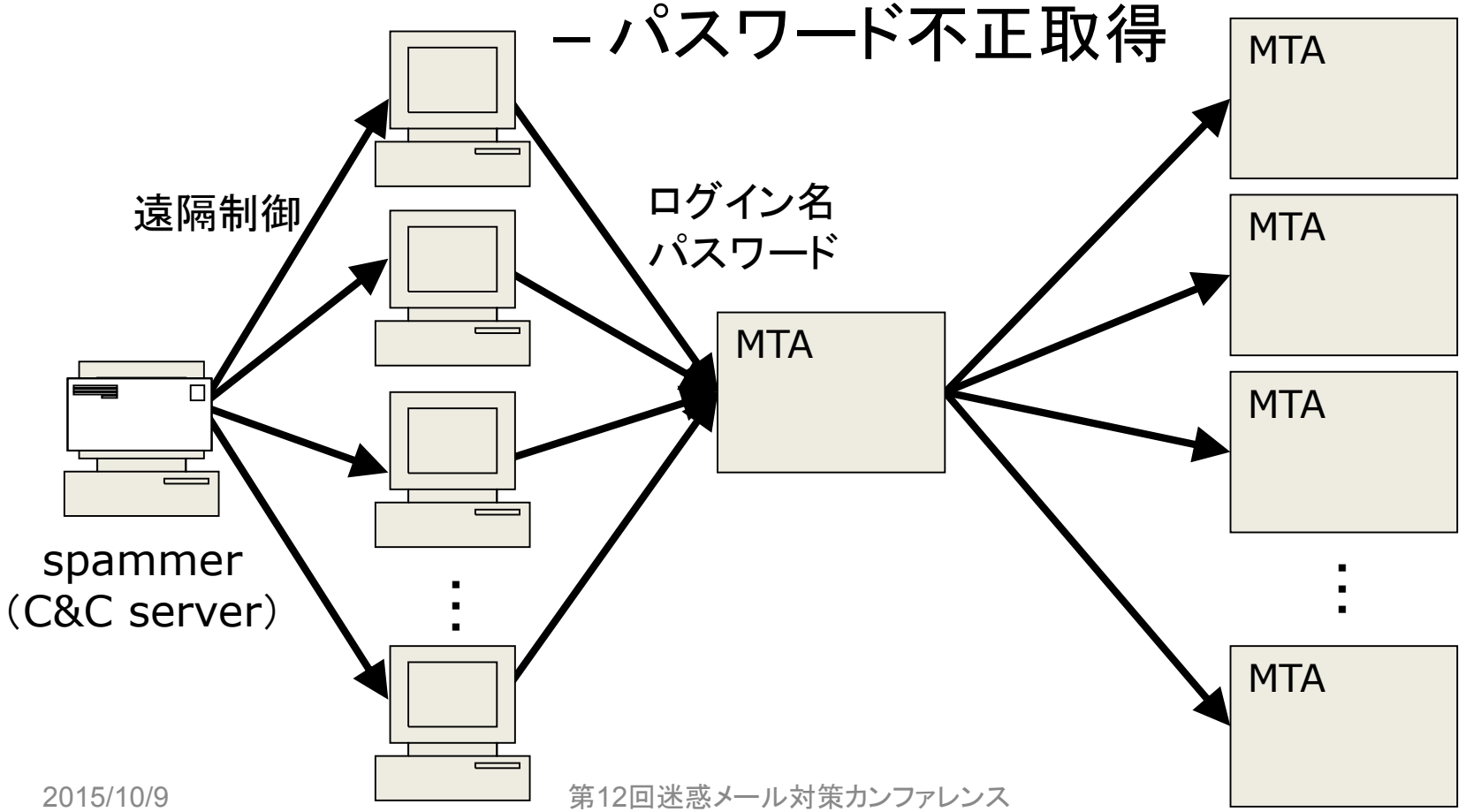
Spammerの手口(1)

- Spamメールの配送(1)
  - ゾンビPC（ボット）



Spammerの手口(2)

- Spamメールの配送(2)
  - パスワード不正取得



Spammerの手口(3)

- メール対策団体への攻撃
  - 攻撃対象：Spamhaus.org
    - イギリスの非営利spam対策団体
  - 攻撃期間：2013年3月18日より10日間ほど
  - 攻撃方法：DDoS（分散型サービス不能攻撃）
    - DNS Amp攻撃
      - オープンリゾルバに対して送信元IPアドレスを偽装したパケットを送出
      - 大きなパケットが偽装送信元（spamhaus.org）に返送
      - 全体で300Gbpsほどの通信量

受信対策手法

受信対策の性能評価基準

- 代表的な2つの評価基準
  - 見逃し率(FNR: false negative rate)
    - 迷惑メールを通常メールと判断する割合
    - 検出率（迷惑メールを正しく判断する割合）と等価
  - 誤検出率(FPR: false positive rate)
    - 通常メールを迷惑メールと判断する割合

- 重要なのは誤検出率
  - 見逃した迷惑メールは単に削除すればよい
  - 重要なメールが迷惑メールと判定されると影響大

代表的な受信対策

- ブロッキング・スロットリング
  - Spamメールの受信を拒否
- フィルタリング
  - Spamメール受信後に内容により判断
- 送信ドメイン認証
  - 送信者（ドメイン）の詐称を受信側で判別

ブロッキング(1)

- 定義
  - 送信側IPアドレス，エンベロープFromアドレス等に基づいて迷惑メールかどうかを判定し，迷惑メールの本文を受信せず拒否する方法
- 代表的なブロッキング技法
  - ブラックリスト
  - Tempfailing

ブロッキング(2)

- ブラックリスト(DNSBL: DNS Black List)
  - 迷惑メール発信ホスト，不正侵入ホスト等を登録
  - 代表例
    - Spamhaus ZEN (http://www.spamhaus.org/zen)
    - SpamCop SCBL (http://www.spamcop.net/bl.shtml)
    - SORBS (http://www.us.sorbs.net/)
    - ORDB (http://ordb.org/) ※2006年12月サービス中止
  - 使用例(Spamhaus ZENの場合)
    - IPアドレスがA.B.C.DのMTAからSMTP接続
    - D.C.B.A.zen.spamhaus.orgのAレコードを検索
    - Aレコード(127.0.0.x)が得られれば，接続を拒否

ブロッキング(3)

- ブラックリスト（続き）
  - トラブルも多い
    - 登録ホストからは通常メールも（ある日突然）拒否
    - 対策完了後も復旧に時間を要するものもある
    - 一部は訴訟にまで発展
  - 効果も疑問（CEAS 2006の論文†における調査）
    - 登録ホストはbot感染ホストの6%程度
    - 検出後に直ちに登録されるホストは少ない

† A. Ramachandran, *et al.*: Can DNS-Based Blacklists Keep Up with Bots? http://www.ceas.cc/2006/14.pdf

ブロッキング(4)

- Tempfailing
  - 「迷惑メール発信MTAは再送をしない」との仮説に基づく方法
    - 通常MTAは信頼性重視
    - 迷惑メール発信MTAは配送効率重視
  - 一時的に受信を拒否
    - 再送されれば正当なMTAと判断して受信
  - 代表例
    - お馴染みさん方式（IPアドレスのみで判定）
    - Greylisting（IPアドレス，差出人，宛先の3つ組で判定）

ブロッキング(5)

- Tempfailing(続き)
  - 利点
    - かなり効果的（80%程度排除）
      - 海外からの（外国語）迷惑メールはほとんど排除
  - 欠点
    - 配送遅延が結構大きい
      - 再送まで1時間のものもある
      - 別MTAからの再送も一時拒否
      - 再送間隔が短すぎるものは再送と見なされないことも
    - 誤検出（再送しない通常MTA）も多い
      - 一部のファイアウォール・オンライン予約システムなど
    - ホワイトリスト（除外MTAリスト）の管理が必須

スロットリング(1)

- 定義
  - 通信速度などを意図的に低下させることにより，迷惑メールの大量送信を妨害する方法
- 代表的なスロットリング技法
  - 同時接続数・確立頻度・帯域の制限
  - 配送不能宛先数の制限
  - Tarpitting

スロットリング(2)

- 同時接続数・接続頻度・帯域の制限
  - サービス不能(DoS)攻撃に対する防御
  - Bot等からの大量配送の防止
- 配送不能宛先数の制限
  - 一部の迷惑メールに対して効果的
  - アドレス収集の防止

※いずれも一部の正常メール配送（特にメーリングリスト）に影響

スロットリング(3)

- Tarpitting
  - 直訳は「タールの落とし穴」
  - 意図的に応答を遅延
    - 迷惑メール送信側でのタイムアウトを誘発
    - あるいは配送効率を抑制
  - ブラックリスト/ホワイトリストとの併用が多い
    - ブラックリスト登録MTAに対して遅延挿入など
  - 代表的な技法
    - Greet pause

スロットリング(4)

- Greet pause
  - コネクション確立時の応答(220 …)を遅延
    - RFC5321では送信側は5分間待つべきと規定
    - 多くの迷惑メール送信MTAは15秒程度で切断
  - MAIL/RCPTの応答を遅延する方法も
    - 例: 宛先不明の場合には遅延挿入
  - 応答を待たずに送信するMTAも拒否
    - 本来はPIPELININGが指定されている場合のみ可

スロットリング(5)

- Greet pause（続き）
  - 長所
    - Tempfailingより設定が簡単
      - 再送判定が不要
    - 配送遅延が小さい
    - 誤判定が少ない
  - 短所
    - サービス不能攻撃に弱い
      - コネクションテーブルオーバーフローが発生

フィルタリング(1)

- 基本方針
  - メール受信後に迷惑メールかどうかを判断
  - 迷惑メールは削除あるいは別に格納
- 代表的な方法
  - ルールベースフィルタ
  - ベイジアンフィルタ
  - 分散協調フィルタ(シグネチャベースフィルタ)

フィルタリング(2)

- ルールベースフィルタ
  - 迷惑メールの特徴をルールとして記述
    - 単純なパターンマッチング
      - 本文中に「$」「Viagra」など特定のキーワードを含む
    - ヒューリスティック
      - 長い英単語がある，FromとToが同じアドレスなど
  - マッチした場合，ルールに対応したスコアを加算
  - 一定のスコア以上のものを迷惑メールと判定
  - 欠点=柔軟性の欠如
    - スコアの調整は可能だが限界が存在
    - 新たな手口には新たなルールが必要
    - 誤検出が比較的多い

フィルタリング(3)

- ベイジアンフィルタ(Bayesian filter)
  - キーワード(単語，3字組等)の出現率を学習
  - キーワードの種類に応じて迷惑メールを判定
  - ベイズ則 P(A|B)= P(A)P(B|A)/P(B)を利用
    - 事象A・・・メッセージが迷惑メールである
    - 事象B・・・メッセージがキーワードを含む
  - 有効なキーワードの例
    - ff0000 … HTMLメールにおける赤色指定
  - 新しい手口にもある程度対応可能
    - 但し，正当なメールと併せて学習が必要
    - いろいろな回避策の存在が確認
  - ルールベースフィルタのスコア調整にも適用可能

フィルタリング(4)

- 分散協調フィルタ(シグネチャベースフィルタ)
  - 最近の主流
  - 判定済みの迷惑メールの再受信を排除
    - 同一内容の迷惑メールが大量配送される点を逆利用
    - 誤検出が非常に小さい
  - 利用者が迷惑メールをデータベースに登録
    - おとりアドレスに届いたメールの自動登録も有効
  - メール受信時に同一メッセージの存在を問合せ
    - 一定数以上の登録があれば迷惑メールと判定
  - 大量の迷惑メールが必要
    - 大手のMSPやspam対策製品メーカーなら可能
  - 内容の一部変更に弱い ⇒ URIブラックリストの活用

フィルタリング(5)

- Spammer側のフィルタリング回避策
  - 十分にフィルタリング技法を研究
    - 単語の加工/挿入
    - 背景と同じ色での単語埋込み
    - 一部のWebサイトが提供するredirect機能の利用
    - サーチエンジン検索URLの埋込み
      - 検索結果の先頭に誘導先URLが表示されるようなリンク
    - ファイルへの埋込み（PDF, MS Word等）
    - 画像ファイルの添付+宛先毎の変形
    - URIの一部をランダマイズ（ブラックリスト逃れ）

送信ドメイン認証(1)

- 発信者ドメインの詐称を識別する手段
  - ローカルパートの詐称は対象外
    - 必要なら発信者認証（S/MIME）を活用
  - メッセージの中身も対象外
    - Spamメールを受け取ることもあり得る
- 詐称なしならドメイン名の信頼度を判定可能
  - 認定(accreditation)サービス
    - 信頼のある機関に公的に認定してもらう
  - 評価(reputation)サービス
    - Spamメールを大量に発信すると評価が下がる

送信ドメイン認証(2)

- 2種類の方法
  - IPアドレスに基づく認証
    - SPF (Sender Policy Framework)
  - デジタル署名を利用した認証
    - DKIM (DomainKeys Identified Mail)

送信ドメイン認証(3)

- SPF(1)
  - 3種類の要素により構成
    - ヘッダ内の送信者の認証(PRA)・・・SPF2.0のみ
    - エンベロープFromの認証(MFROM)
    - 送信側ドメインのポリシー定義(SPFレコード)
  - 受信側での認証動作
    1. 送信者アドレスを取得（MFROMあるいはPRA）
    2. 送信ドメインのポリシー（送信用IPアドレス）を取得
    3. 送信元IPアドレスと照合
    4. ポリシーに合致すれば認証成功

送信ドメイン認証(4)

- SPF(2)
  - SPFレコード
    - DNSのTXT (SPF)レコードで送信サーバを宣言
      - \+　　pass (受信許可)
      - ?　　neutral (宣言なしと同様)
      - ~　　softfail (neutralとfailの中間)
      - \-　　fail (受信拒否)
    - 例：AレコードかMXレコードに対応するIPアドレスを持つMTAからのみ送信可能な場合
      - example.jp　IN TXT　“v=spf1 +a +mx –all”
      - example.jp　IN SPF　“spf2.0/mfrom,pra +a +mx -all”

送信ドメイン認証(5)

- DKIM (1)
  - 公開鍵暗号方式を利用
    - 送信側
      - 秘密鍵を使って署名
    - 受信側
      - DNSを用いて公開鍵を取得
      - 公開鍵を使って署名を検証

送信ドメイン認証(6)

- DKIM (2)
  - 署名ヘッダの例

```
DKIM-Signature: v=1; a=rsa-sha256; s=brisbane; d=example.com;
                                  ↑アルゴリズム ↑セレクタ   ↑ドメイン
      c=simple/simple; q=dns/txt; i=joe@football.example.com;
          ↑正規化方法       ↑公開鍵入手法  ↑ユーザ名
      h=Received : From : To : Subject : Date : Message-ID;
          ↑ 署名対象に含めるヘッダフィールド ↓本文のハッシュ値
      bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
          ↓署名
      b=AuUoFEfDxTDkHlLXSZEpZj79LICEps6eda7W3deTVFOk4yAUoqOB
        4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+NahM6L/LbvaHut
        KVdkLLkpVaVVQPzeRDI009SO2Il5Lu7rDNH6mZckBdrIx0orEtZV
```

送信ドメイン認証(7)

- DKIM (3)
  - DNSの設定例

```
brisbane._domainkey.example.com.      IN TXT  (
 1セレクタ  "v=DKIM1; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQ"
           "KBgQDwIRP/UC3SBsEmGqZ9ZJW3/DkMoGeLnQg1fWn7/zYt"
           "IxN2SnFCjxOCKG9v3b4jYfcTNh5ijSsq631uBItLa7od+v"
           "/RtdC2UzJ1lWT947qR+Rcac2gbto/NMqJ0fzfVjH4OuKhi"
           "tdY9tf6mcwGjaNBcWToIMmPSPDdQPNUYckcQ2QIDAQAB"
           )
```

送信ドメイン認証(8)

- 2つの認証方式の選択
  - IPアドレスに基づく認証
    - ヘッダや本文の書換えに強い
    - 転送に弱い
      - PRA，MFROMが維持できるかどうかが問題
  - デジタル署名を利用した認証
    - 転送に強い
    - ヘッダや本文の書換えに弱い

⇒相補的に利用することが重要（DMARC）

送信ドメイン認証(9)

- DMARC
  - Domain-based Message Authentication, Reporting and Conformance
  - 2つの機能
    - SPF/DKIMの結果を送信ドメイン側に通知
    - いずれの認証にも失敗するとポリシーに基づいて処理
      - ポリシー: 通過，隔離，拒否のいずれか
  - 詳しくはTF-4/OD-4参照

送信対策手法

代表的な送信対策

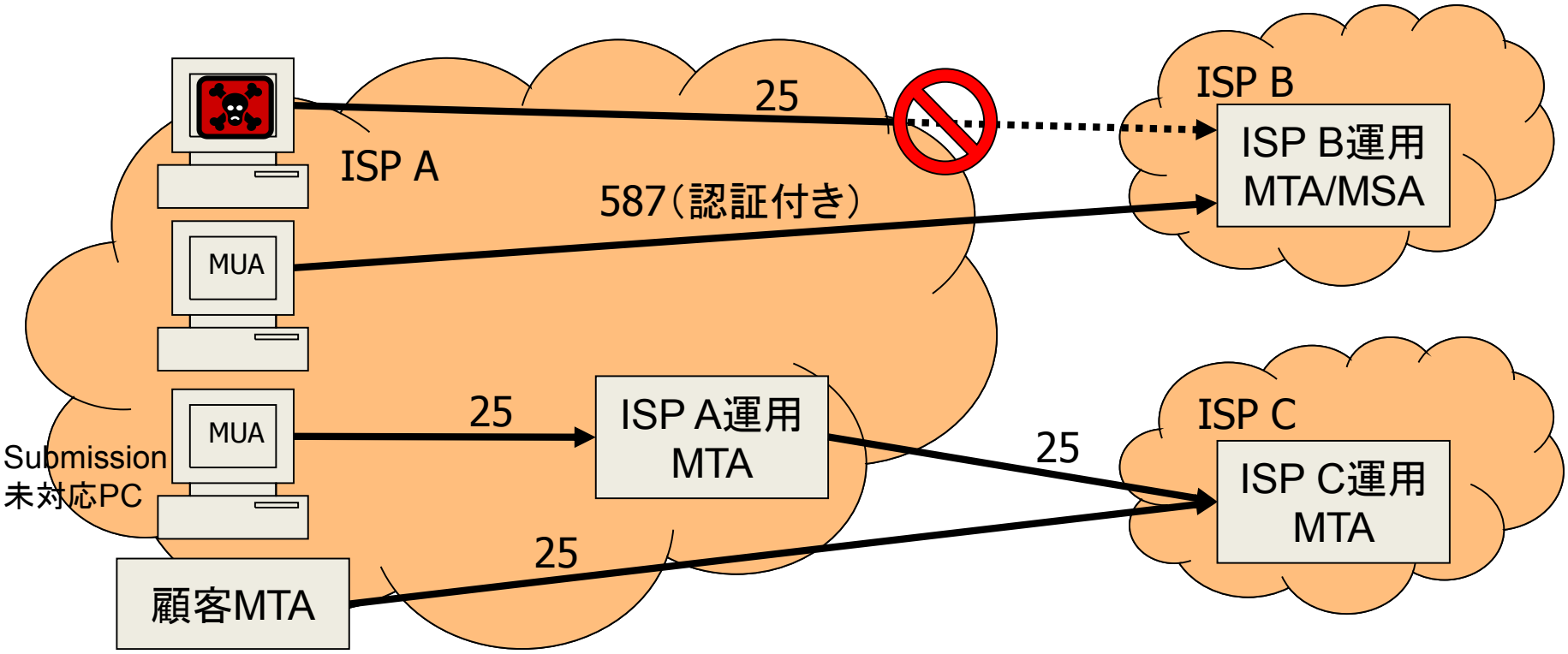
- ISPでのブロッキング
  - 迷惑メールに限らず送信を原則的に禁止
- ISPでのスロットリング
  - 迷惑メールに限らず大量送信を抑制
- （法的対策）
  - 今回は割愛

ISPでのブロッキング(1)

- Outbound Port 25 Blocking (OP25B)
  - 自網からの迷惑メール送信防止が目的
    - 迷惑メール配送業者やbotが対象
    - 普通の電子メール発信は対象外
  - 方法
    - 自網→外部MTAへのSMTP(25番)をブロック
    - 他社MTAの利用者には発信ポートの利用を推奨
      - Submission(587番), SMTP/SSL(465番)
    - 一般利用者は自社ISP運用のMTAを利用
    - 自網内の顧客MTAは固定IPアドレスで対応
      - 当該IPアドレスのみブロックを解除

ISPでのブロッキング(2)

- Outbound Port 25 Blocking (続き)



ISPでのブロッキング(3)

- Outbound Port 25 Blocking (続き)
  - 既にほとんどのISPが導入
  - 十分な効果
    - 国内宛迷惑メールの送信拠点が国外に移行
  - 問題点
    - 発信ポートを提供していない組織もまだ多い
      - 特に大学，中小企業が問題かも

ISPでのスロットリング

- 外部MTAに対するメール発信を制限
  - 同時送信数・送信頻度・帯域などを制限
    - 基本的には受信対策の場合と同じ
  - OP25Bとの併用
    - 自網内からのメールの大量送信を直接的にも間接的にも防止

おわりに(1)

- いたちごっこはまだまだ続く. . .
  - 標的型攻撃の増加
  - パスワード不正取得による送信の増加
  - SMS (Short Message Service)でのフィッシング(smishing)の増加
  - SNSでの誘導

おわりに(2)

- 根絶は可能か
  - 巧妙な手口への対処には膨大な資源が必要
    - 過去の例
      - 画像spam → 画像のOCR解析
      - 添付ファイルspam→ ファイルの解析

    ⇒ 根絶は非現実的
  - spammer側も資源が必要
    - 巧妙な手口は非効率
      - 画像spam：’07Q3以降急速に減少

⇒「採算割れ」への誘導が重要

  - 送信コストの押し上げ
  - 被害者の減少
- 外国国家機関のspam発信に注意

Wikipedia（英語版）”Image spam”より