# 送信ドメイン認証技術について

株式会社インターネットイニシアティブ
三膳 孝通

# なぜ送信『ドメイン』認証か



- 一般的呼称：送信『者』認証
  - 『者』＝ユーザ名@ドメイン名
- 現在の枠組：主にドメインが対象
  - ドメイン単位での認証技術
  - ユーザの正当性の確認は別の枠組が必要
- より正確な表現を使うことの意味
  - 利点・欠点等を正確に把握してもらうことができる
  - 「過剰な期待」⇒「残念感」を懸念
  - 適切な技術を適切な用途で適用することが重要

# 送信ドメイン認証技術の概略



## 登場の背景

- 迷惑メール (spam等) の爆発的な増大
  - インターネット上に流通しているメールのほとんどに
- Phishing等悪質な迷惑メールの登場
  - 詐欺等の悪質な犯罪行為に利用される
- 事態の深刻化
  - 「変なメールが届いた」だけでは済まなくなってきた

- 電子メールが再び普通に使えるための仕組み作り
  - 法制度の整備
  - Anti-spam filter
  - 送信ドメイン認証

# 送信ドメイン認証技術の概略


## 技術の概略

- 「メールの送信元が確認できる技術」
  - 現在の迷惑メールが不適切な発信者を名乗ったり、踏み台など適切ではないサーバから発信されていることに対しての対応策
  - メールの発信を防ぐ技術ではなく、メールを受け取る側での対応に関する技術
  - メールの発信者情報から得られる発信元情報（サーバの情報等）を、受信側で確認できる認証の枠組

- 受信側でメールの信頼性に応じて処理が可能
  - 少なくとも発信ドメインは正しいことが確認できる
  - 「信頼できるメール」と確認できたもののみ受け取るなどの対応が可能となる

# 送信ドメイン認証技術の概略
## 枠組の種類



- 現状：複数の種類が提案・実装
  - SPF (Sender Policy Framework) / Sender ID
  - DomainKeys
- それぞれに独立した技術
  - 対立する（選択しなければいけない）技術ではない
  - 相互に補完可能
  - どちらから始めても構わない
  - 両方使っても構わない
- 提供者や利用者が柔軟に技術を選択可能
  - 利用形態等に応じた柔軟な運用ができる

# 送信ドメイン認証技術の概要



## SPF (Sender Policy Framework)

- Pobox社が開発、AOLが早くから支持
- 既に20万ドメイン以上で利用されている
  - http://spftools.net/register.php
- DNSにより「メールをInternetに送信するサーバの情報」を確認する方法
  - Envelope From (ヘッダに現れる送信者ではなくメール配送プロトコルSMTPで指定される送信者情報)と、接続元メールサーバ情報にて確認
  - 接続時点での確認が可能、処理の負荷が軽い
  - メールの転送やMLへの対応が難しい

# 送信ドメイン認証技術の概要



## Sender ID

- IETF MARID-WGで検討
  - Pobox社のSPFとMicrosoft社のCaller ID for E-mailを統合
- SPF同様、DNSにより「メールをInternetに送信するサーバの情報」を確認する方法
- 二種類のチェック方法
  - Envelope From (MAIL FROM)
  - PRA (Purported Responsible Address)
- MFROMチェック
  - SPFv1と同じ
- PRAチェック
  - ヘッダ情報と、接続元メールサーバ情報で確認
  - 転送の問題等が解決されたもの

# 送信ドメイン認証技術の概要



## DomainKeys

- Yahoo!が提唱
- DNSを用いて「メール自体の認証」をドメイン単位で行う
  - ヘッダ情報・ボディ情報に対してデジタル署名を行う
  - デジタル署名に関する情報を、ヘッダに含め送信
    - Domainkey-Signature
  - 受信者はDNSにて公開鍵を取得し、ヘッダの情報と照合
- 発信者情報だけではなく、本文についても確認が可能
- ML等で問題が起きる可能性
  - 構造的にPGP等と同様の問題がある

# 送信ドメイン認証技術の概要



## 技術の特徴

- 迷惑メール対策技術の一つ
  - 送信ドメイン認証技術がすべて解決するわけではない
  - 「送信ドメインは正しいことが確認できる」環境の確立
- シンプルな技術の組み合わせによって解決
  - 個々の特徴に特化してシンプルな対応策を実装
  - 柔軟に状況に応じた対応が可能に
- 他の要素技術との組み合わせ
  - 送信ドメイン認証技術によるフィルタリング
  - Reputationサービスによるフィルタリング
  - Anti-spam filterによるフィルタリング、等

# 送信ドメイン認証技術の動向



## MAAWG (Messaging Anti-Abuse Working Group)

- 電子メールの悪用に対して総合的な対策を検討するWG
  - 世界の通信会社、ISPが参加
  - 2004年1月に発足
- 施策･技術･協調の三本を柱に活動


(MAAWGホームページより)

# 送信ドメイン認証技術の動向

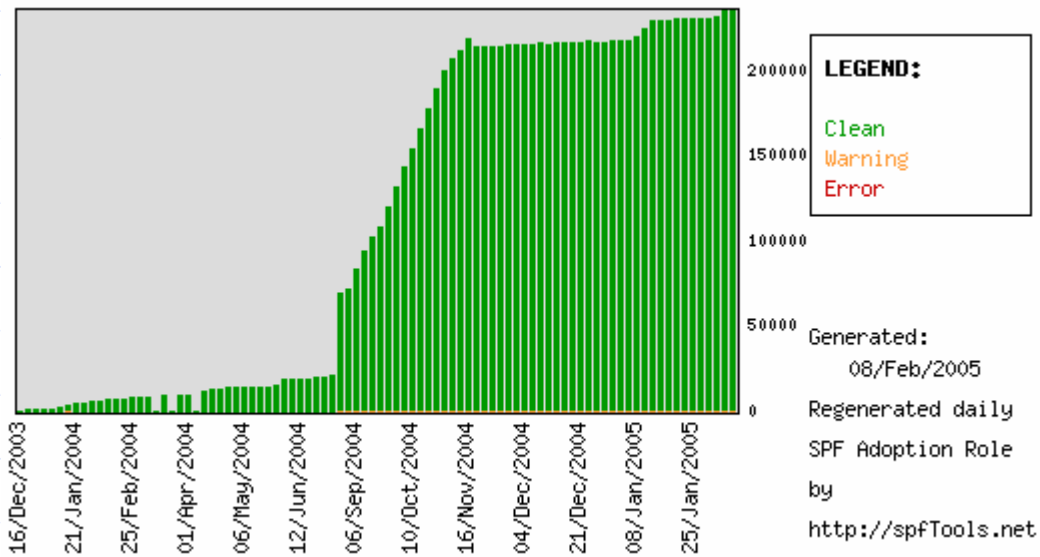


## MARID (MTA Authorization Records in DNS)

- DNSを使った送信者認証技術の議論が活発化
- IETF 59 (2004年3月) にMARID BoF開催、WGに
  - SPF、Caller ID、DomainKeysなどさまざまな方式を議論
  - Sender IDとしてCaller IDを軸に策定することに
  - DNS側の仕様策定・認証技術の標準化
- 知的所有権問題により、議論が停止
  - Sender IDに対する反対意見・懸念等が表明される
- MARID-WGの解散 (2004年9月)
- Sender IDの修正案が提出 (2004年10月)
  - 知的所有権の問題への対応等

# 送信ドメイン認証技術の動向
## 海外の動向

- 電子メールの機能不全に対する危機意識
  - 迷惑メールの比率が大半に
  - Phishing等の被害も深刻化
- 業界以外でも企業が対応策を講じ始める
  - 送信ドメイン認証技術も急速に普及
  - FTCに電子メール認証技術普及の公開簡書
- 認証技術利用を前提とした環境に急速に展開



# 送信ドメイン認証技術の動向
## 国内の動向



- 被害の深刻化が確認される
  - 欧米に遅れて国内でも急速に被害が拡大
- 欧米での動向に同期する必要性
  - Internet全体で対応していくことの重要性
  - 対応していないと「信頼できないメール」に
- 事業者などで対策の検討が開始
  - ISPやベンダーなど十数社が参加
  - 海外の動きと連動
- 国内でも活動が活発に

# 事業者の取り組み
## ISPの取り組み



- 電子メール環境の改善に関する取り組みの活発化
  - Anti-spam filterを始め、各種要素技術の提供及び検討
  - 送信ドメイン認証技術についても検討
- 電子メール環境の広がり：広範囲なサービスへの影響
  - 送信ドメイン認証技術：DNSやメールサーバでの対応
  - メール送信ポリシーの確立：メールの出口の整理
  - 受信メール取扱いポリシーの確立
  - 転送・ML等電子メールアプリケーションの取扱い
  - メールマガジンなどのメール送信代行サービス
  - モバイル等のメール送受信環境、等
- 電子メール利用環境の新たな標準の確立へ

# 事業者の取り組み
# ユーザへの展開



- 個人・法人ともに使い方に影響を及ぼす
  - 送信：使用するメールアドレスのドメインで指定されたサーバからのみメールがInternetに出るようにする、など
  - 受信：受信メールの対応ポリシーに従って、自身のメール環境の設定の見直しを行う、など
- Internet全体での取り組みの重要性
  - 誰もが『信頼できるメール』を送受信できるように
- 普及に協力頂けるための活動から
  - ISP・ベンダーを超えた展開
- 技術の確立から普及段階へ

# 事業者の取り組み
# 業界での連携

- 新しい電子メール利用環境が当たり前の世界へ
  - 送信ドメイン認証技術への対応
  - 電子メール送受信ポリシーの確立･対応
  - 新しい利用環境への移行モデルの確立
- 業界全体での連携の重要性
  - 要素技術･サービスモデル･利用形態
  - 移行に関する技術やスケジュール
- ユーザとInternetの両方に対する責任
  - 情報インフラとしての信頼性を取り戻すため
- 業界での連携体制の確立

# 今後の展開
# 全体像の展望

- 電子メール利用環境全体としての信頼性の確保
  - 研究会での整理を元に
- 他の技術要素の展開
  - 他の『ドメイン間』認証技術の展開
  - 『ドメイン内』での認証技術の展開
  - クライアント側での選択技術の確立
- 技術要素以外の展開
  - 法的根拠の確立
- 対応体制の確立
  - 業界での連携
  - 業界を超えた連携

# 今後の展開

## 認証技術の普及･推進

- 新たな『常識』の確立
  - 『認証されていて当然』
  - 『選択が適切に行えて当然』
- スムーズな移行モデルの重要性
  - 失敗を許容できること
  - 現状の問題に対応できること
  - 将来の変化に追従できること
  - 移行の効果が確認できること
- 利用の増加：最も重要な普及策
  - 率先して技術の採用を
  - 移行の問題もクリアに

# 今後の展開
# 展望の確立



- 必要な要素はほぼ出揃っている状況
  - 技術、制度、サービス等
- 実行すれば効果は確実に確認できる状況
- 適切な技術を適切な範囲に順次適用
- 電子メールが再びコミュニケーションの道具に

# 参考



- Sender Policy Framework (SPF)
  - http://spf.pobox.com/
- Sender ID
  - http://www.microsoft.com/senderid
- DomainKeys
  - http://antispam.yahoo.com/domainkeys
- MAAWG (Messaging Anti-Abuse Working Group)
  - http://www.maawg.org/
- MARID (MTA Authorization Records in DNS)
  - http://www.ietf.org/html.charters/OLD/marid-charter.html
- IIJ
  - http://www.iij.ad.jp/