DMARCとフィードバックによる新しいメールの枠組み

~ 第12回迷惑メール対策カンファレンス ~

Email Security Conference 2015

2015.10.09

櫻庭 秀次

(株)インターネットイニシアティブ

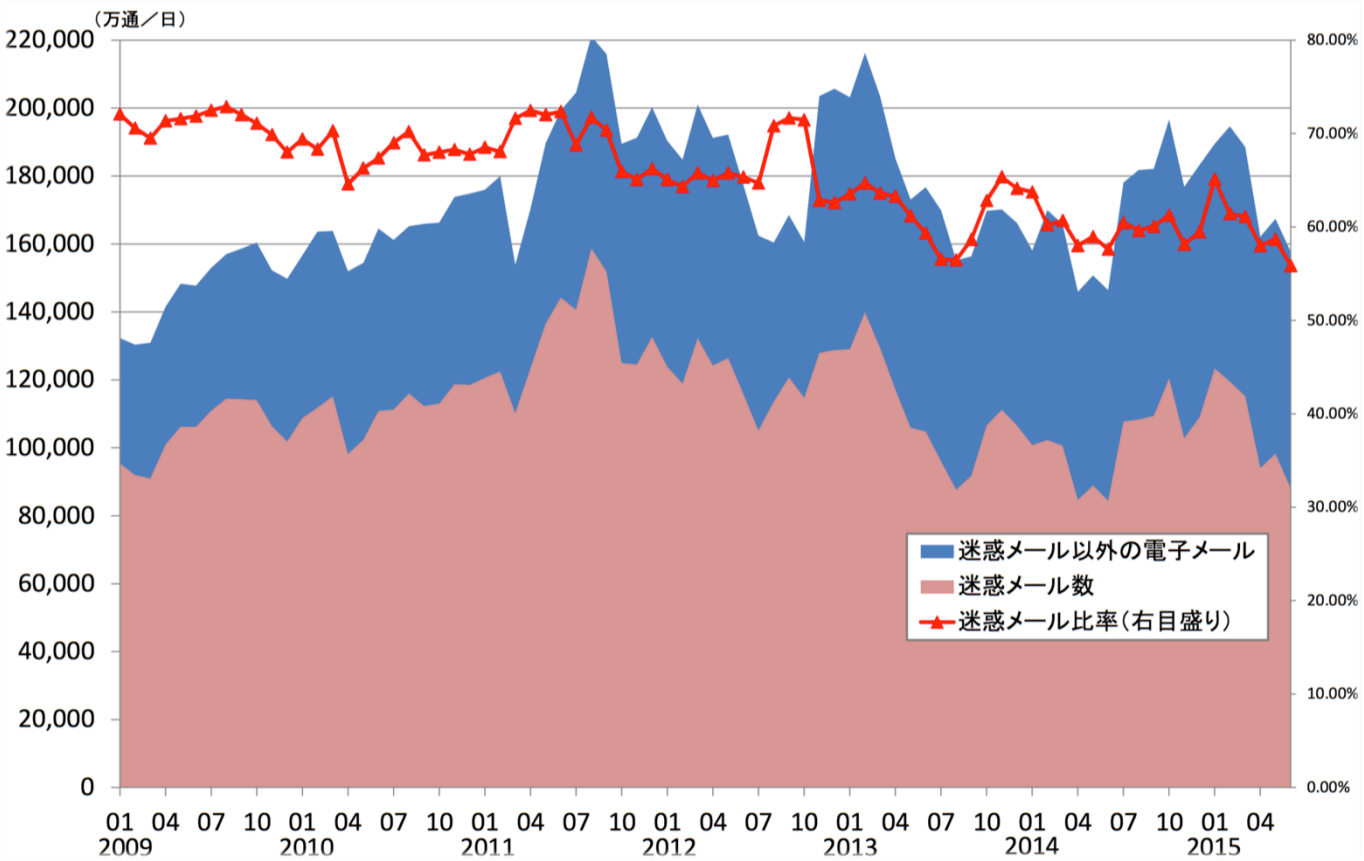
Agenda

- 迷惑メールの状況
- メールシステムの課題と対策
- DMARCの概要
- 新しいメールの枠組み

  DMARC + レピュテーション + フィードバック
- フィードバックの役割

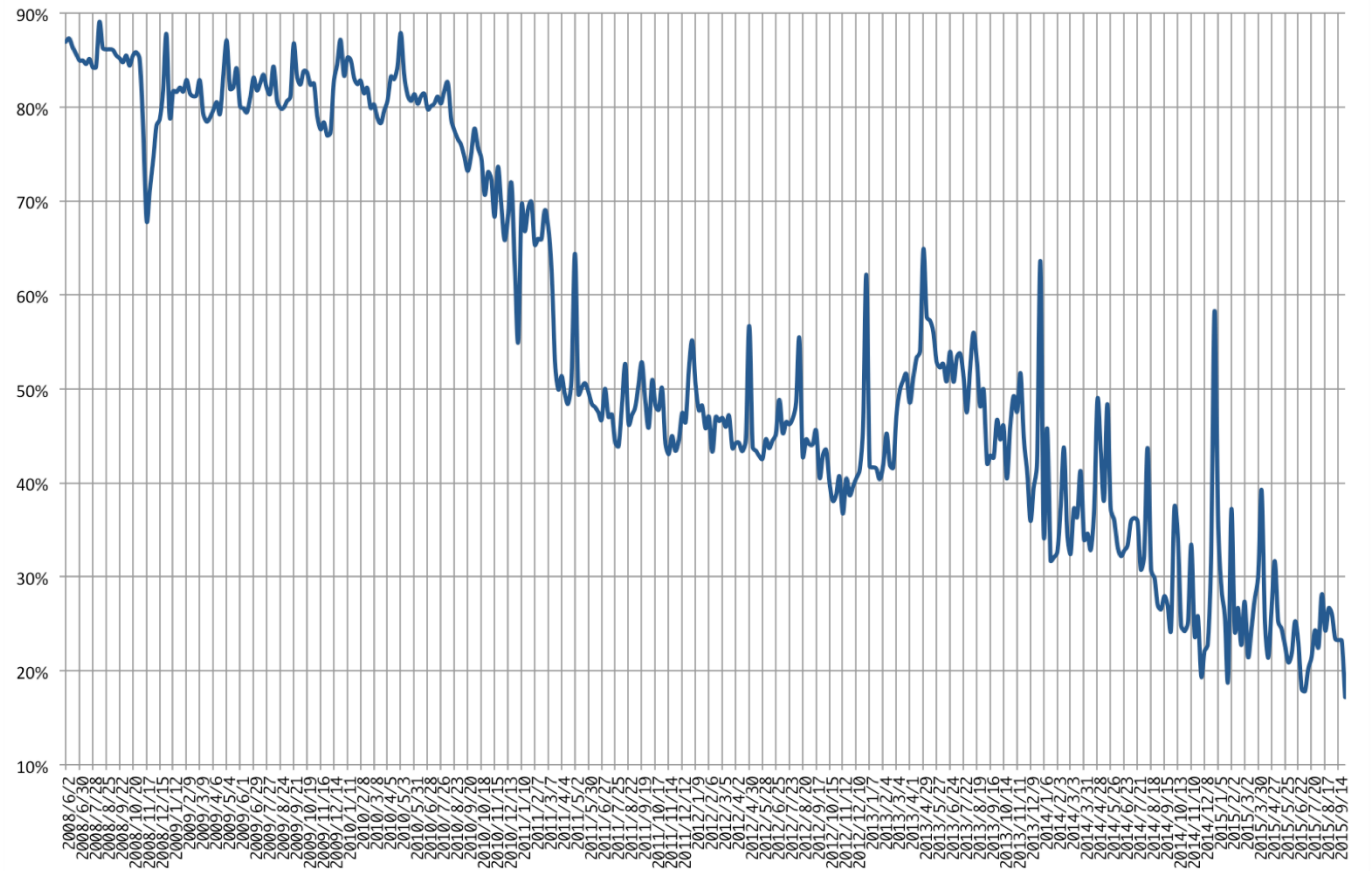
迷惑メールの動向

- 迷惑メールの動向
  - 電気通信事業者10社の協力により、総務省とりまとめ
  - 55.8% (2015.06, 迷惑メール割合)



迷惑メールの動向

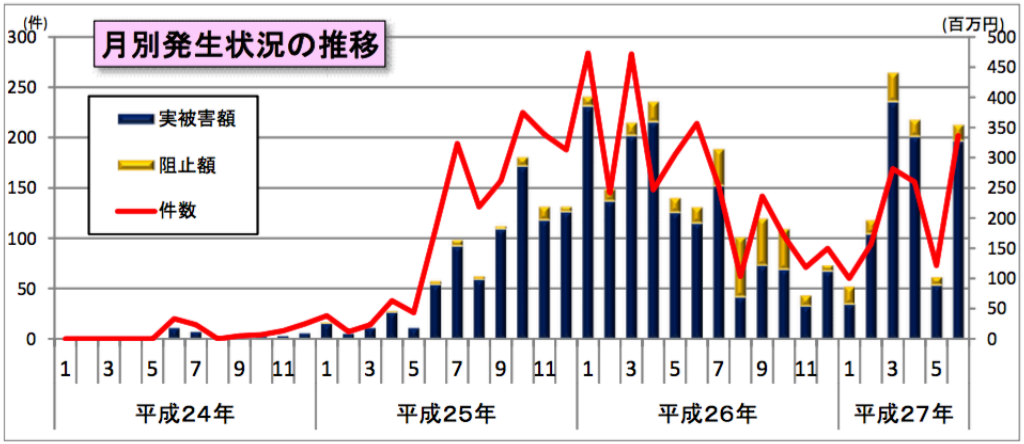
- 迷惑メールフィルタによる検知率の推移
  - IIJが提供するメールサービスで利用 (2008.06.02～2015.10.04)
  - 22.72% (2015.09 の平均値)



迷惑メールの動向

- 平成27年上半期のインターネットバンキングに係る不正送金事犯の発生状況等について (平成27年9月3日、警察庁広報資料)
  - 754件, 約15億4400万円と昨年下半期に比べて増加
  - 犯行等の状況
    - 信用金庫, 信用組合, 農業協同組合, 労働金庫に被害が拡大 (件数は多いが被害額は都銀)
    - 法人口座の被害が急増 (被害額はまだ個人口座)

期間	被害件数	被害額
平成27年上	754件	15億4,400万円
平成26年下	619件	10億5,800万円
平成26年上	1,257件	18億5,100万円
平成25年	1,315件	14億6,000万円



メールシステムの課題

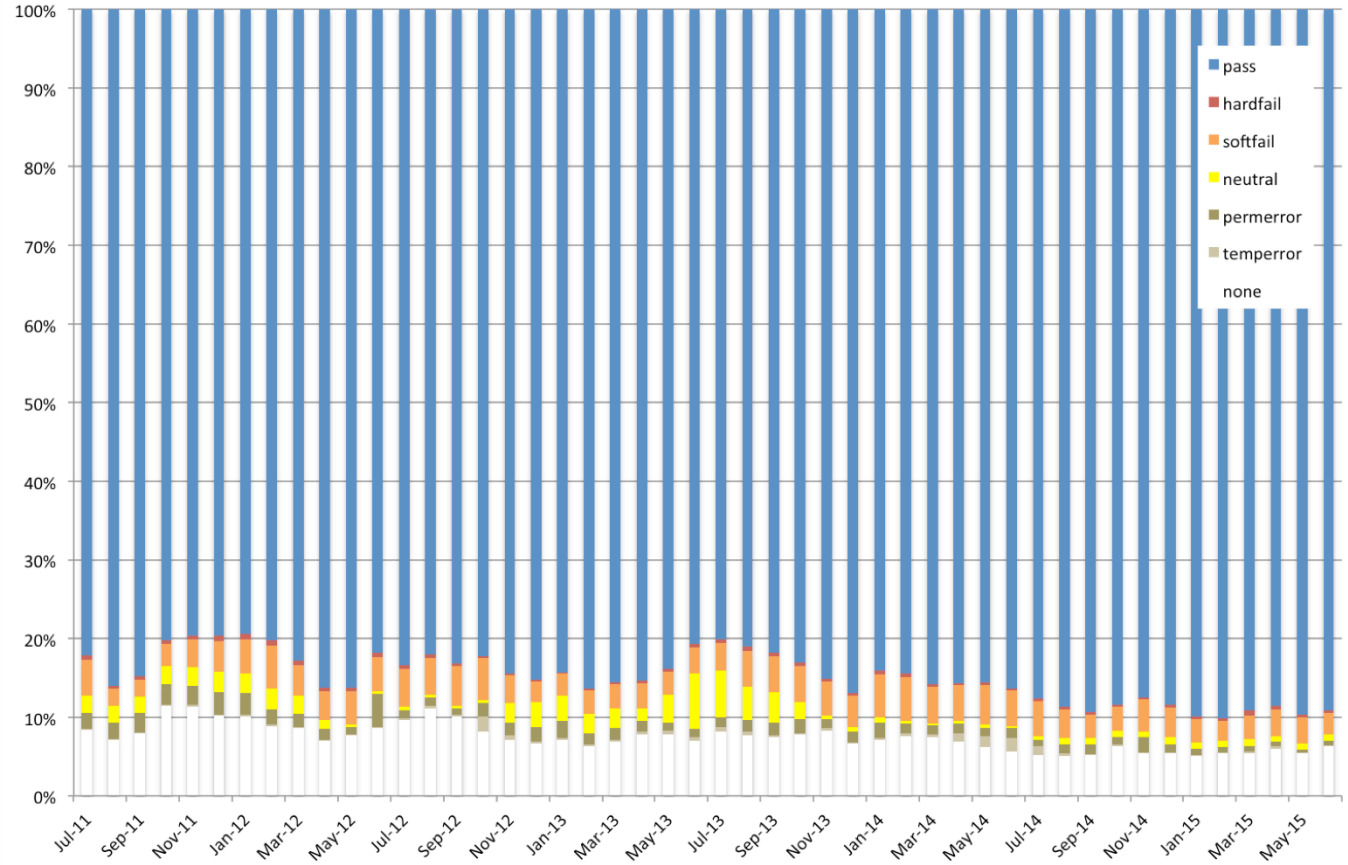
- 迷惑メール量は増大していないがセキュリティ的脅威は深刻
  - 各種情報漏洩が継続して発生
  - インターネットバンキングの悪用による金銭的被害が高レベルで推移
  - メールによるマルウェア(添付ファイル)の混入
  - メールによる危険なWebサイトへの誘導でマルウェアのダウンロードや各種脆弱性をついた攻撃による感染
- メール送受信環境改善の必要性
  - 受信側は対策強化をせざる終えず必要なメールが届きにくい状況に
  - メールはコミュニケーション基盤でありビジネスや防災連絡などにも利用
- 迷惑メール送信対策強化の必要性
  - 日本がspam送信国として上位
    - Sophos 社 Dirty Dozen (11位, 2015Q1:1月-3月)
    - Spamhaus による The World's Worst Spam Enabling Countries (5位, 2015.10.08)

課題に向けた対策

- 受け取るべきメールを判断
  - 普及した送信ドメイン認証技術 (SPF/DKIM) を利用し，統一的な認証技術を利用して受け取るべき送信者を判断 → DMARC
  - 受け取るべきメールが事前に明らかになれば，それ以外を spam filter の判断基準を引き上げて対策することも可能 → レピュテーション(ホワイトリスト)
- 迷惑メール送信対策
  - 認証 (SMTP-AUTH) してメールサーバを利用してもPCがマルウエアに感染して乗っ取られている場合を検知したい → フィードバック
  - 悪意を持った利用者 (認証IDの不正入手，悪用者) のメールサーバ利用対策 (緊急避難的なものを含む) → フィードバック
  - 迷惑メール送信が明らかになれば緊急的にメールサーバ利用の停止や送信依頼元の判断が可能 (送信代行事業) → フィードバック
- メール利用環境の改善
  - 受信したメールが不要であることを安全に通知 (opt-out) → フィードバック (safe unsubscribe)
  - Opt-out に対応しない送信元からのメールは受け取らない → レピュテーション，フィードバック

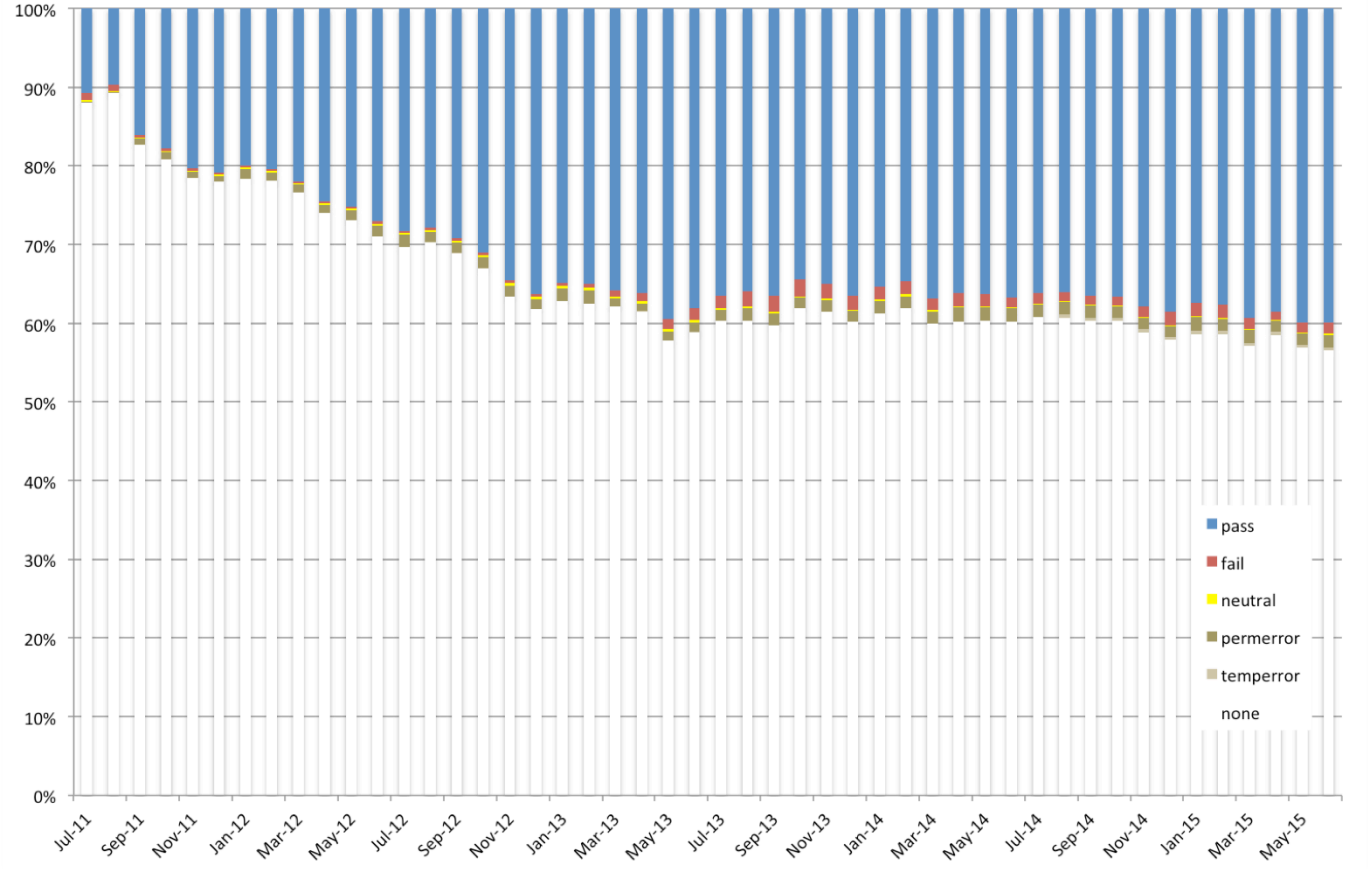
SPF の普及状況

- 認証結果の推移
  - 電気通信事業者7社による総務省とりまとめ
  - 93.67% (2015.06, none 以外の割合)



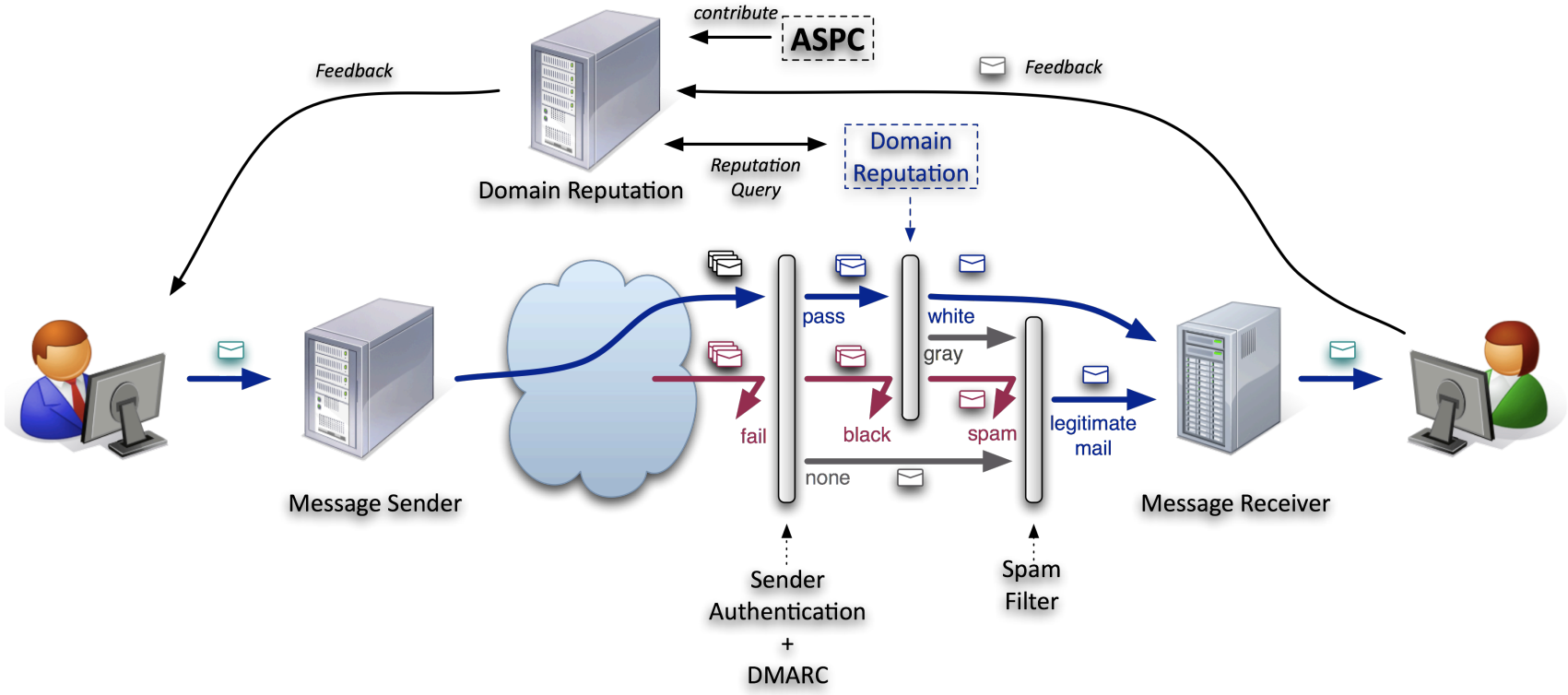
DKIM の普及状況

- 認証結果の推移
  - 電気通信事業者4社による総務省とりまとめ
  - 43.44% (2015.06, none 以外の割合)



DMARC+レピュテーション+フィードバック

全体構成



DMARC+レピュテーション+フィードバック
各構成要素の役割

- メール送信側
  - SPF/DKIM の導入
  - DMARC レコードの宣言
  - フィードバックの受信と対応 (opt-out, 一時利用停止, 各種対策)
- メール受信側 (事業者)
  - SPF/DKIM の導入 (受信側認証)
  - DMARC の認証
  - ドメインレピュテーション利用による配送判断 (各社それぞれが利用を判断)
  - フィードバック機能の提供 (Webメールのspamボタン，購読解除ボタン等)
- メール受信者 (個人)
  - 不要なメールの報告 (フィードバック)
- ドメインレピュテーション (フィードバック受け元)
  - 受信側の要求に応じてドメインに対するレピュテーションを提示
  - メール受信者からのフィードバックを受信
  - 必要に応じて送信側にフィードバックを行う

DMARC

Domain-based Message Authentication, Reporting & Conformance

- 目的
  - ドメイン詐称を防ぐために既にある個別の仕組みをオープン化
  - 認証識別子の標準的な利用方法の確立
  - 認証の運用上の各種問題解決に役立てる
  - SPF & DKIM のより広い導入の動機付け
  - より積極的な認証方針 (policy) への奨励

- 特徴
  - 複数の認証技術 (SPF, DKIM) を利用
  - 信頼関係を築きより強い方針 (policy) を導入できるように受信側から送信側へフィードバックを行う
  - 認証の対象は、メールヘッダ上 (From: ヘッダ) のドメイン

DMARC

- 送信側としての準備
  - DKIM と SPF の導入 (and/or)
  - 利用する識別子の整理 (Identifier Alignment)
  - フィードバック受信の準備 (メールアドレスの用意)
  - DMARC policy (DMARC record) の宣言
    - 対象となるドメインの “_dmarc” サブドメインの TXT RR
    - 最初は “p=none” から

```
_dmarc.example.jp TXT "v=DMARC1; p=none; rua=mailto:dmarc-feedback@example.jp"
```

  - 送信ドメイン認証の結果確認と調整 (feedback を利用)
  - DMARC policy の調整 (“pct=” と “p=“ による段階的な強化)
    - 次の段階として “p=quarantine” と “pct=小さい値”
    - さらに次の段階として “pct=100” に
    - さらに “p=reject” と “pct=小さい値”
    - 段階的に p と pct を引き上げて行く

DMARC

- 受信側の手順
  - ヘッダ From (RFC5322.From) からドメインを取り出す
    - 取り出すドメインは一つだけ
  - DMARC policy レコードを取り出す
    - DMARC TXT レコードが存在しない場合 Organizational Domain に問い合わせを行う
  - DKIM 署名の検証と SPF 認証を行う
    - 認証が成功 (pass) したドメインを利用する
  - 認証された識別子 (ドメイン) と Identifier Alignment をチェック
  - DMARC 方針 (policy) を適用して処理する
  - DMARC Feedback
    - “rua=”: 集約レポート (aggregate reports), XML 形式
    - “ruf=”: 失敗レポート (failure reports, forensic reports), ARF を利用

フィードバック

- 仕組み
  - メール受信者は不要なメールを申告 (ex. [spam] ボタン)
  - 購読解除 (opt-out) は別途申告手段を用意
  - フィードバックを一旦受け取るレピュテーション事業者は送信者を確認して適切な処理を行う
    - 正当な送信者 (Whitelist Domain) への通知
    - それ以外はレピュテーション情報に活用
- 利用技術
  - フィードバックは ARF (Abuse Reporting Format, RFC5965) で理由とメール内容を申告

注: DMARCのレポーティング (Failure, Aggregate) とは別の通知システムを想定

フィードバック

- フィードバックを受ける送信側がすべきこと
  - 送信者を明確に判断 (認証) できるような設定を実施
    - SPF/DKIM の導入, DMARC レコードを宣言
  - DMARC が fail しないようなヘッダを設定
    - RFC5321.From と署名ドメインを RFC5322.From と一致させる
    - もしくは　Identifier Alignment となるドメインを利用
  - 送信メールの発信者及び宛先を管理できること
    - SMTP-AUTH や 送信依頼元による発信者管理
    - ログ等による宛先と日時情報の一定期間保持
  - フィードバックを受けた場合に適切に管理できること
    - opt-in メールの送信で不要と申告された場合には opt-out 手続きを行う
    - 迷惑メール (spam) と申告された場合には送信者を特定し，一時的に認証 (SMTP-AUTH) を不許可とし，迷惑メールが送信されないような対応を行うこと (PC の cleanup 等)
    - 悪質な送信者である場合 (故意に大量送信を行っている場合等) には契約者情報を共有し他事業者で利用できないような対応について検討 (別途)

フィードバックの役割

- 必要なメールの流通促進
  - 最終メール受信者から情報を直接入手 ← 送信メールに対する評価
  - 購読したメルマガ等を簡便に opt-out できることの利点
    - Opt-in がしやすい環境づくり → 送信側の利点
    - 受け取ってもらうための様々な (≒無用な) 工夫の軽減 → コンテンツに集中
- メール環境の改善
  - いち早くフィードバックに対応することで
    - 不要なメールの大量送信を早い段階で抑制 → 被害の最小化
    - 他の RBL (Real-time Black-List) への登録抑制 → メールが届きやすい環境
  - 悪意を持った利用者の特定と情報共有 → 迷惑メールが送信しづらい環境づくり
- セキュリティ対策
  - メール送信者のPC改善: 利用者が意図せず送信している場合はマルウェア感染が疑われる
  - 対応を迅速に行うことにより被害の拡大が防げる

まとめ

- メールは組織内部に侵入する窓口
  - 様々な情報がディジタル化され内部に蓄積されている
  - 組織を各種防御システムで守ることも大事，メールは内部に侵入できる残された手段なので常に対策が必要
  - 攻撃者はメールを利用して組織内部への侵入を絶えず考えている (social engineering)
- メールはコミュニケーション基盤
  - SNS や各種メッセンジャーアプリが普及しているが，それぞれで閉じているシステム
  - 認証手段や最後の連絡手段としてメールが利用され続けている現実
- 健全なメール環境維持のために
  - 送信したメールが届いているかを気にしなければならない時代
  - 誰でも利用できるシステムであるからこそ，皆で守っていく必要がある