なりすましの手口とその正しい対策

~DKIM第三者認証問題とDMARCの普及に向けて~

2016.10.04-05

第14, 15回 迷惑メール対策カンファレンス

IAjapan (Internet Association Japan)

講演者紹介

- 加瀬 正樹　ニフティ株式会社
- 北川 直哉　東京農工大学
- 櫻庭 秀次　株式会社インターネットイニシアティブ

Agenda

- なりすましメールとは
- なりすましメール対策としての送信ドメイン認証技術
- 送信ドメイン認証技術の普及状況
- 送信ドメイン認証技術の課題
  - なりすましの手口 (加瀬)
  - DKIMの抱える問題点とその対策 (北川)
- 送信ドメイン認証技術の応用
  - DKIM署名の信頼性検証システム (北川)
  - 個人でできるDMARC検証システム (北川)
  - 認証結果を活用できる事例 (加瀬)
  - DMARC + FBL + Reputation
- DMARCをより普及させていくために

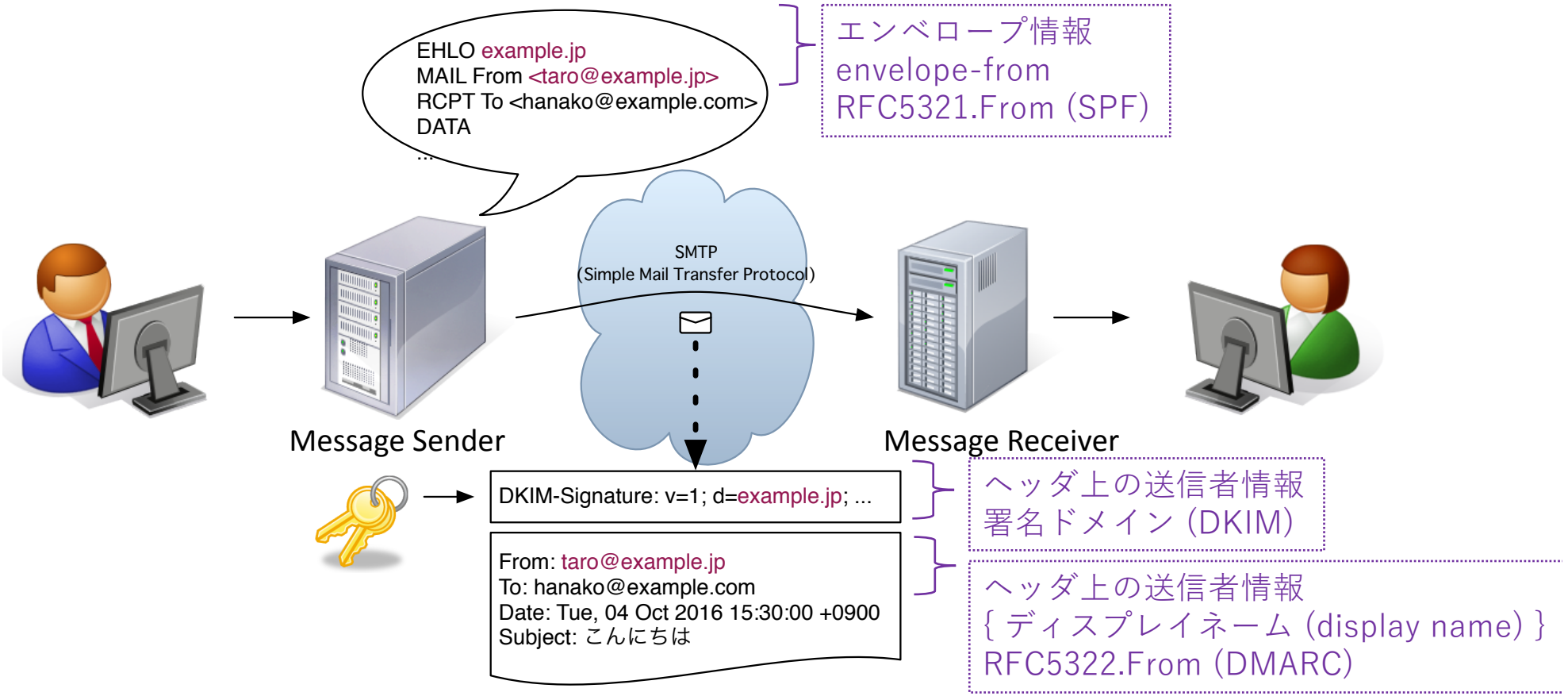
なりすましメールとは

概略

- 送信者情報を偽って送信されるメール
- 送信者情報とは
  - メールの送り手，書き手を示す情報
  - 技術的には
    - エンベロープ情報
    - メールヘッダ上の情報
- メールの運用上考慮が必要なパターン
  - メーリングリスト
  - メール配送代行
  - メール転送
  - 複数のメールアドレスを有する利用者

なりすましメールとは

送信者情報



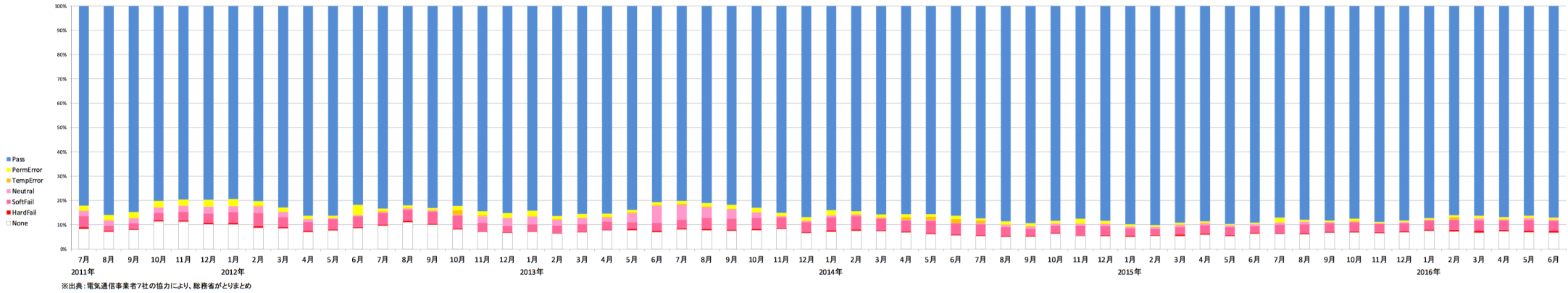
なりすましメールとは
メールの運用上考慮が必要なパターン

- 問題がないパターン
  - 全ての送信者情報が一致している
    RFC5321.From = RFC5322.From = DKIMドメイン
    (但し display name には注意が必要)
- 正当なメールが不一致となるパターン
  - メーリングリストサーバからの配送
    - RFC5321.From = メーリングリスト運営ドメイン
  - 送信代行事業者からのメール (全てが当てはまるとは限らない)
    - RFC5321.From = 送信代行事業者 (配送状況を管理するため)
    - DKIM ドメイン =送信代行事業者 (多くの場合，鍵管理の都合上)
  - 自動転送されたメール
    - RFC5321.From = 転送元ドメイン
  - 複数のメールアドレスを所有しているユーザ
    - 送信ドメインが変更可能なメールサービス (ex. gmail.com)
    - 提供形態により様々 (ex. Gmail は RFC5321.From, DKIM ドメインが送信元)

→ 本セッションではこれらの対策 (なりすましと思われないための) にはあまり触れません

送信ドメイン認証技術の普及状況
総務省とりまとめ (SPF)

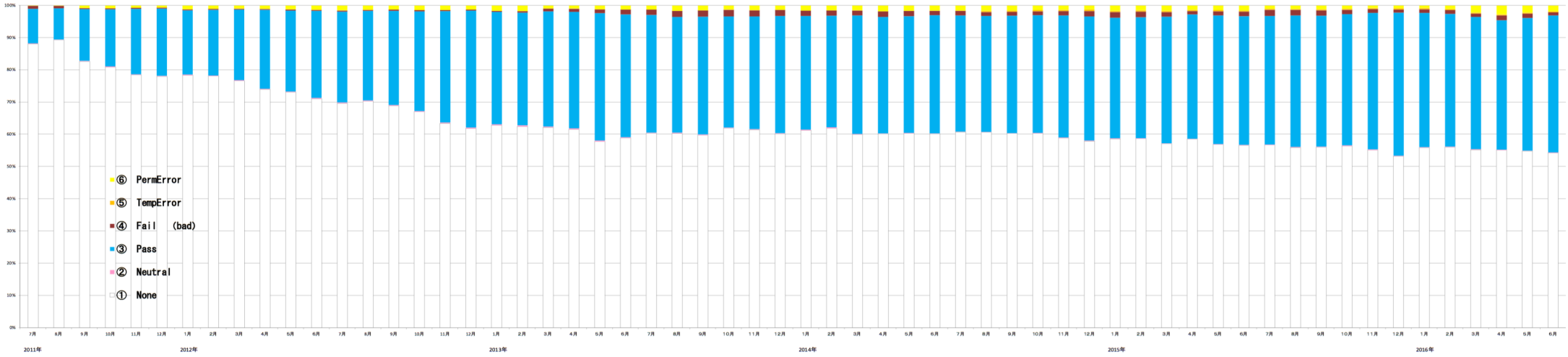
- 対象: 電気通信事業者7社
- 期間: 2011.07～2016.06
- 最新データ
  - Pass: 87.01%
  - Hard/Soft Fail & Neutral: 5.26%
  - None: 6.86%



送信ドメイン認証技術の普及状況

総務省とりまとめ (DKIM)

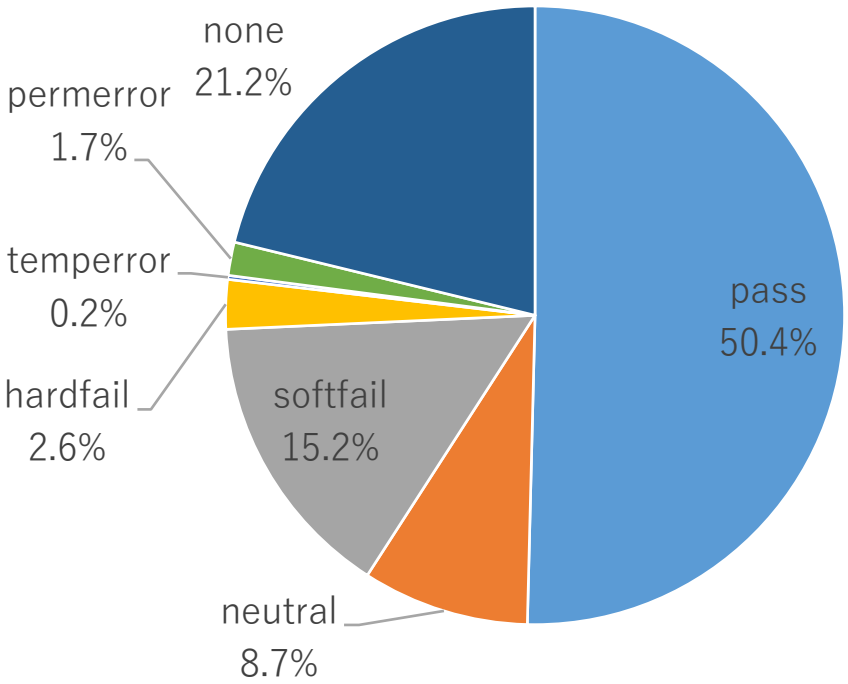
- 対象:電気通信事業者4社
- 最新データ (2016.06)
  - Pass: 42.62%
  - Fail: 0.88%
  - None: 54.21%



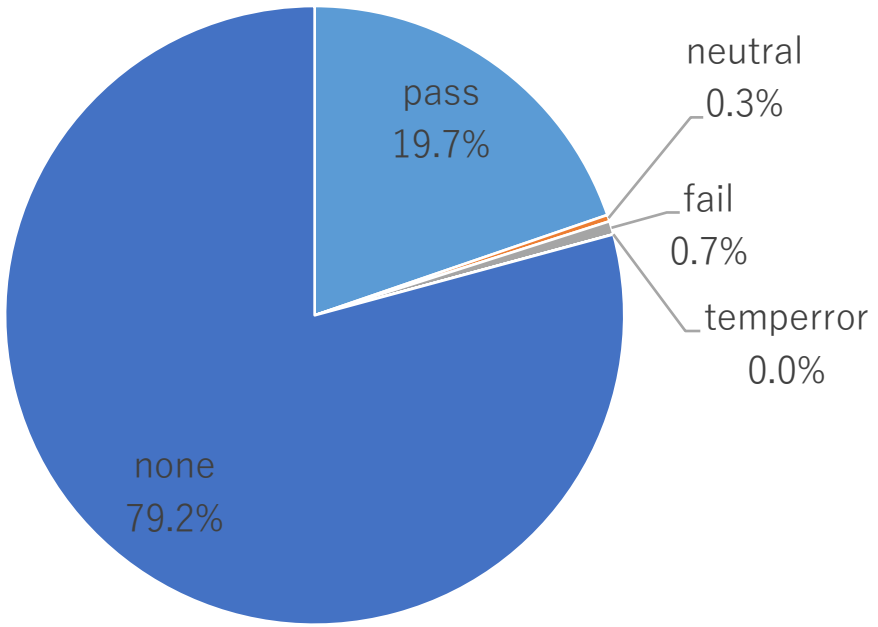
※出典:電気通信事業者4社の協力により、総務省がとりまとめ

送信ドメイン認証技術の普及状況
IIJ 調査 (SPF, DKIM)

- 対象: 2016.09 (流量ベース)



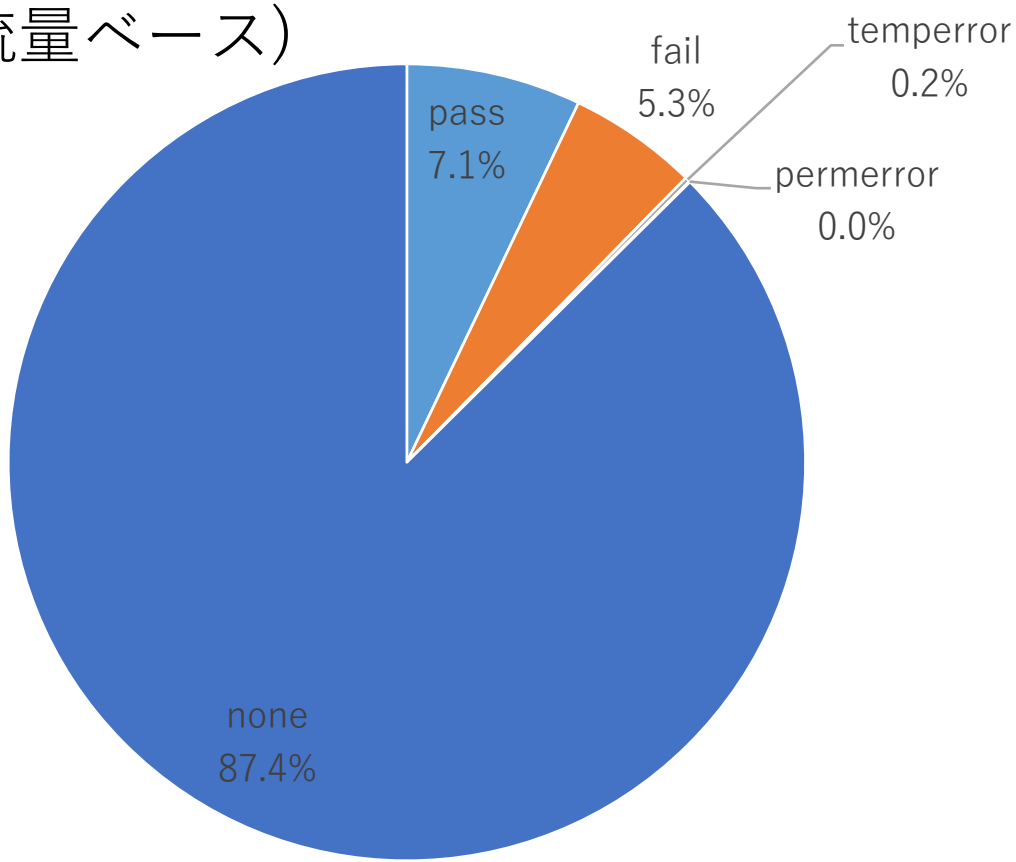
SPF



DKIM

送信ドメイン認証技術の普及状況
IIJ 調査 (DMARC)

- 対象: 2016.09 (流量ベース)



送信ドメイン認証技術の課題
送信ドメイン認証技術の応用

- 別資料

DMARC + FBL + Domain Reputation

DMARCの概要

- DMARC
  - Domain-based Message Authentication, Reporting & Conformance
  - 仕様は RFC7489 で公開
- DMARC の目的
  - 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
- DMARC の特徴
  - 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

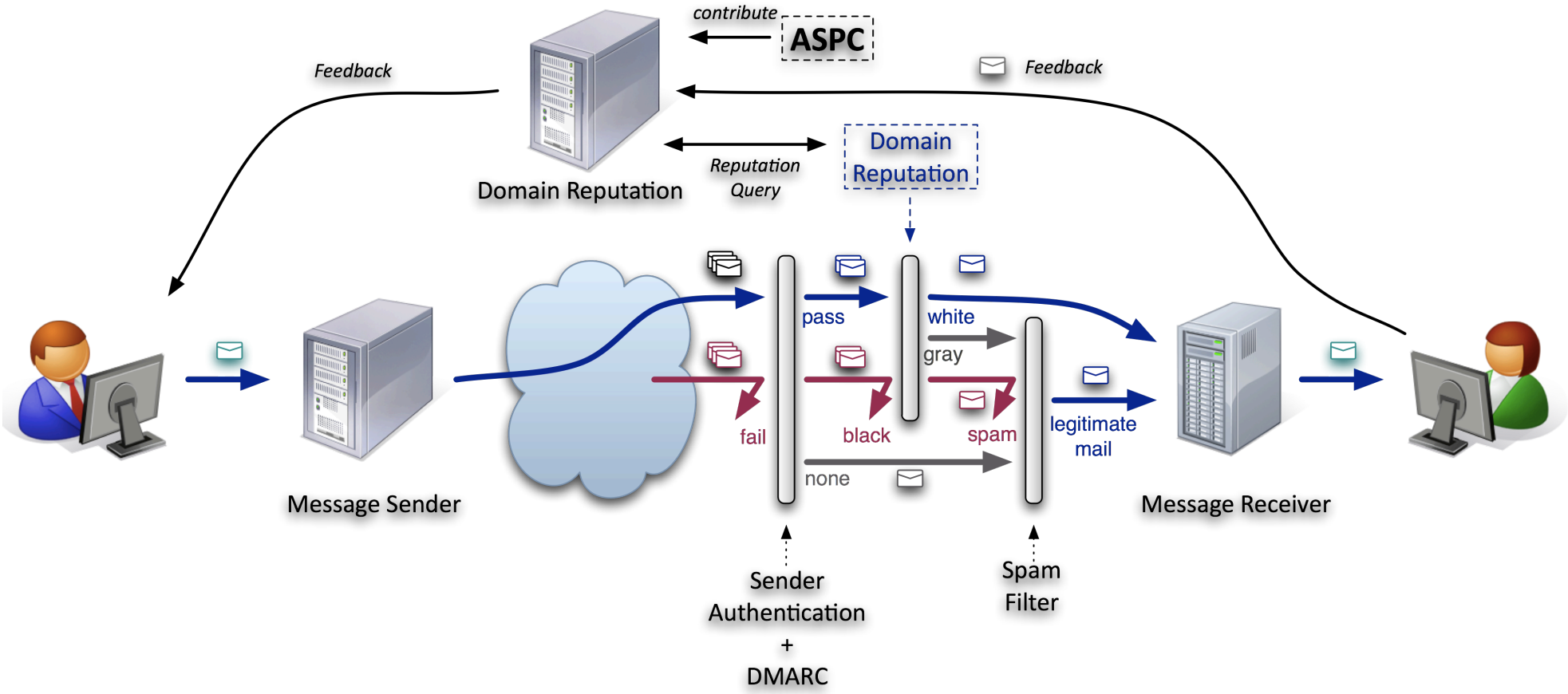
FBL: Feedback Loop

DMARC + FBL + Domain Reputation
目的と概要

- 目的
  - 正しく送信者情報を設定した、受け取るべきメールを確実に受信者に届ける
  - 判断する情報 (送信者情報) を更新するために Feedback の仕組みを組み込む
- 実現手法
  - 送信ドメイン認証技術 (SPF, DKIM) の認証結果と、受信者が参照できる送信者情報 (RFC5322.From) を元に送信者をドメイン単位で確認 (認証) する
    → DMARC (RFC7489)
  - 認証されたドメインを評価して受け取るべきメールを判断する
    → Domain Reputation
  - 迷惑メールを受け取った場合に通知する仕組みを用意する
    → Feedback Loop

DMARC + FBL + Domain Reputation

概略



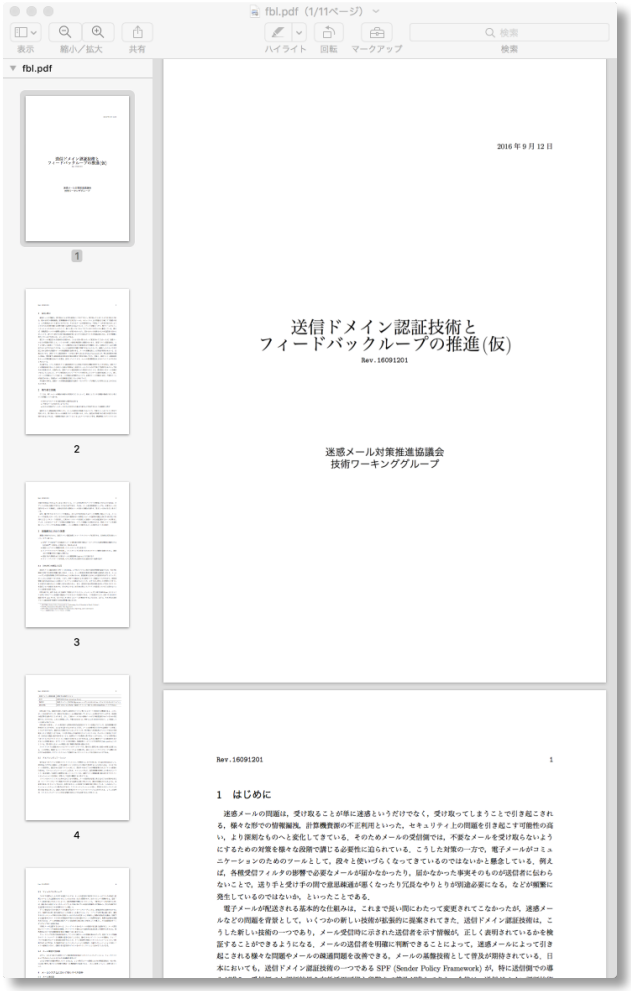
DMARC + FBL + Domain Reputation
効果

- 受信側が期待できる効果
  - 認証された送信者情報を元に判断するのでメールの内容に依存しない判断を行う
  - 配送すべきメールを送信者情報で判断 (WhiteList) することで迅速に受信側に届けることが可能
  - WhiteList があることにより迷惑メール判断の閾値を下げることが可能
- 送信側が期待できる効果
  - WhiteList に登録
    - 迅速にメールが届く
    - きちんと管理されていれば Outbound Filter が不要 (かもしれない)
  - Feedback の仕組み
    - 不要と思われたメールとその受信者を判断できる (メールコンテンツの評価, Opt-out)
    - 踏み台にされた場合にそのメールの送信者を特定できる (SMTP-AUTH で認証している場合など) ので対策がしやすい

DMARC + FBL + Domain Reputation

効果

- 詳細
  - 迷惑メール対策推進協議会 技術 WG で検討
  - 迷惑メール対策推進協議会として公開 (予定)
- 概要
  - 実現することによるメリット
    - なりすましメール対策
    - 正当なメールがきちんと届く環境
  - 各構成要素が果たすべき役割や要件
    - 送信側
    - 受信側
    - 受信者
    - ドメインレピュテーション



DMARCをより普及させていくために

- DMARCの導入 (送信側)
  - サブドメインも含めたドメイン全体でポリシー等を検討
  - SPF, DKIM を導入していれば DMARC レコードを公開するだけ
  - DMARC レポートを受信し SPF, DKIM の設定を確認可能
  - DMARC レポートからなりすましの程度を確認可能
  - ドメインの価値を守るための必須要件
- DMARCの導入 (受信側)
  - SPF, DKIM の認証機能を導入していれば比較的容易
  - 認証結果を利用したなりすまし対策の導入へ
  - DMARC レポート機能の実装は要検討 (次のセッションで)