送信ドメイン認証技術の利用について

第10回迷惑メール対策カンファレンス

2014.02.14

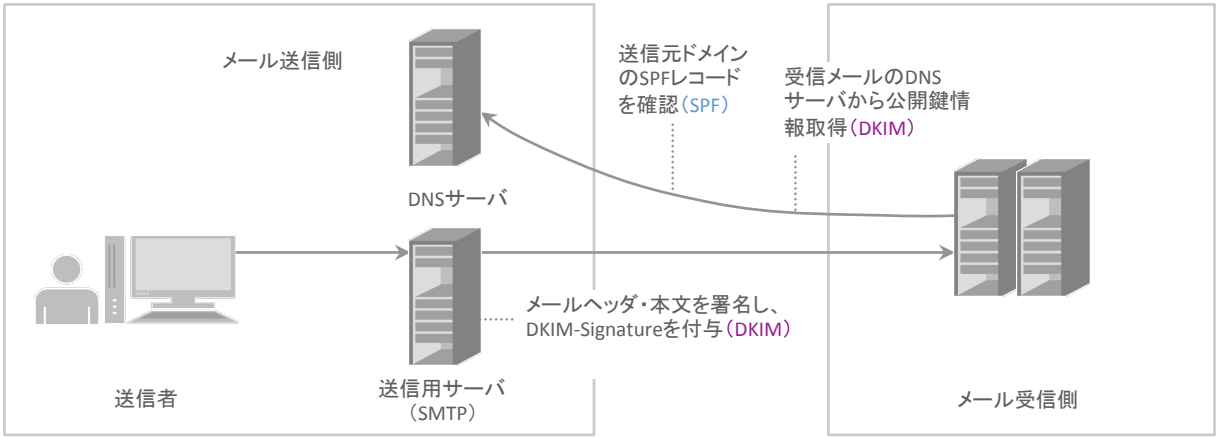
櫻庭 秀次
(株)インターネットイニシアティブ

Agenda

- 送信ドメイン認証技術
  - 迷惑メールの動向
  - SPF
  - DKIM
- 送信ドメイン認証技術の利用
  - DMARC
- 課題

送信ドメイン認証技術 (1)

- 基本的な仕組み
  - 送り手は送信元を明確に表明 (ごまかしがきかない情報を利用)
  - 受け手は送信元情報が正しく表明されているか確認 (認証)
  - DNS を利用することにより外部の認証機関が不要



SPF: Sender Policy Framework (RFC4408)
DKIM: DomainKeys Identified Mail (RFC6376, STD76)

送信ドメイン認証技術 (2)

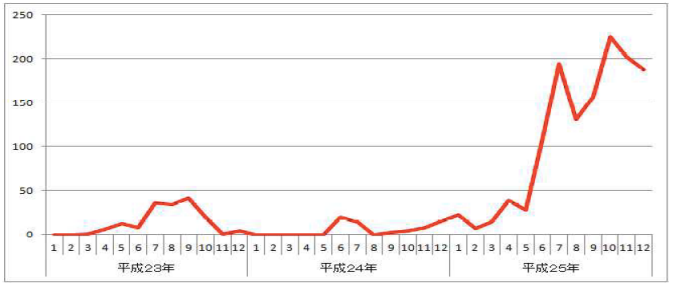
- 期待される効果
  - 信頼できる送信者からのメールを識別 → 優先受信等
  - 巧妙化する不正行為を事前に見破る
    - 有名サイトを騙ったフィッシング → 偽のサイトへ誘導し ID やパスワードを搾取
    - 信頼性が高そうな送信者を騙った不正プログラムの実行 (添付ファイルや不正サイトへの誘導) → botnet の拡散、spyware の混入
    - 情報搾取を目的とした標的型攻撃 → 内部情報の外部への漏洩等
    - etc…
  - 迷惑メールを判定するのではなく送信者情報を認証する技術

→ メールに関連する種々の問題を解決するための基盤技術

迷惑メールの動向 (1)

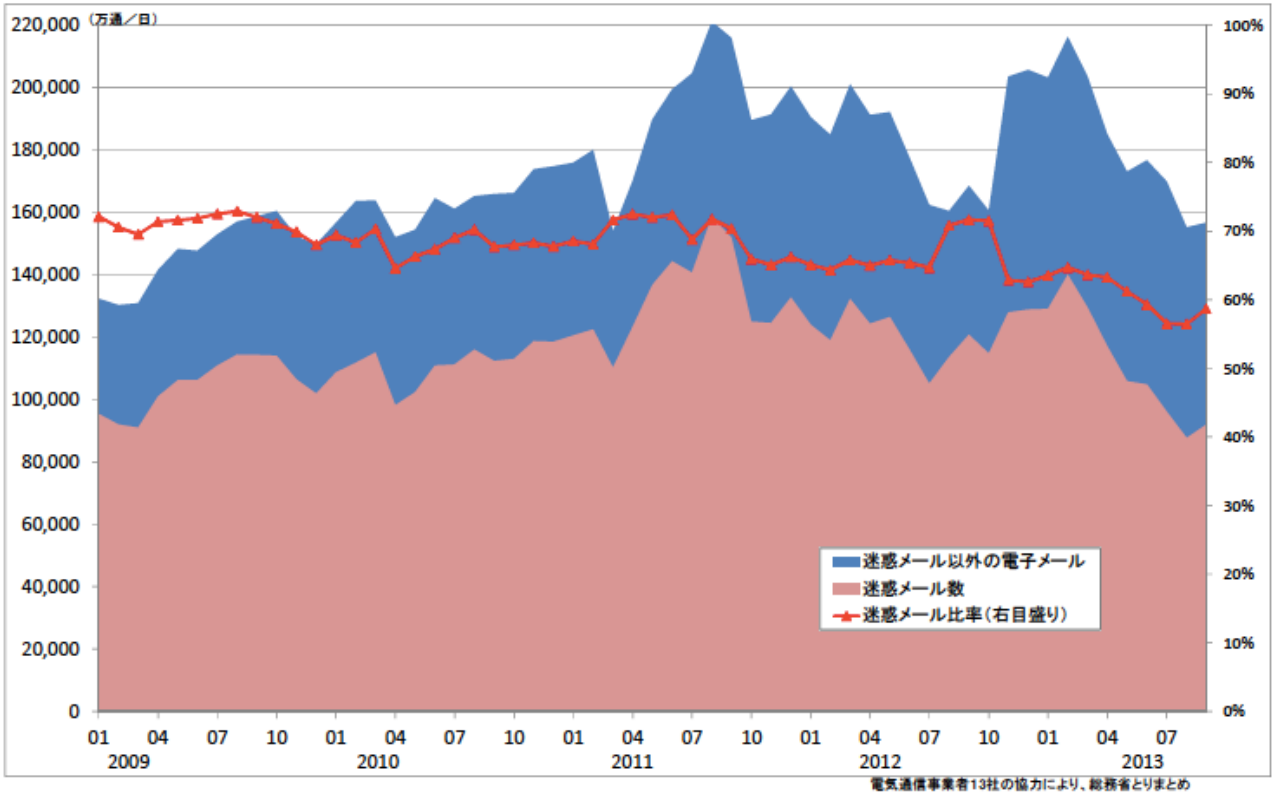
- 平成25年中のインターネットバンキングに係る不正送金事犯の発生状況等について (平成26年1月30日、警察庁広報資料)
  - 1,315件, 約約14億600万円と過去最大の被害。特に6月以降、急増
  - 犯行等の状況
    - 被害口座は個人名義がほとんどである
    - 被害口座に係るパスワード等を入手する方法は、コンピュータウイルスで表示した不正画面に入力を求めるものが主。ただし、11月以降、メールでフィッシングサイトに誘導するものが多発
    - 不正送金等の態様
      - 不法に売買された口座を用いて送金し、出金役がATMで引き出すもの～約5割
      - 真正な名義の口座を用いるものの、資金移動業者を介して不法に国外送金するもの～約2割
    - 金融機関等の対策により被害状況が変化。対策を講じたことにより、夏以降、ほぼ発生がない金融機関もある

被害件数, 被害額		
平成25年	1,315件	14億600万円
平成24年	64件	4,800万円
平成23年	165件	3億800万円



迷惑メールの動向 (2)

- 迷惑メールの動向
  - 電気通信事業者13社の協力により、総務省とりまとめ
  - 58.67% (2013.09, 迷惑メール割合)



SPF の動向 (1)

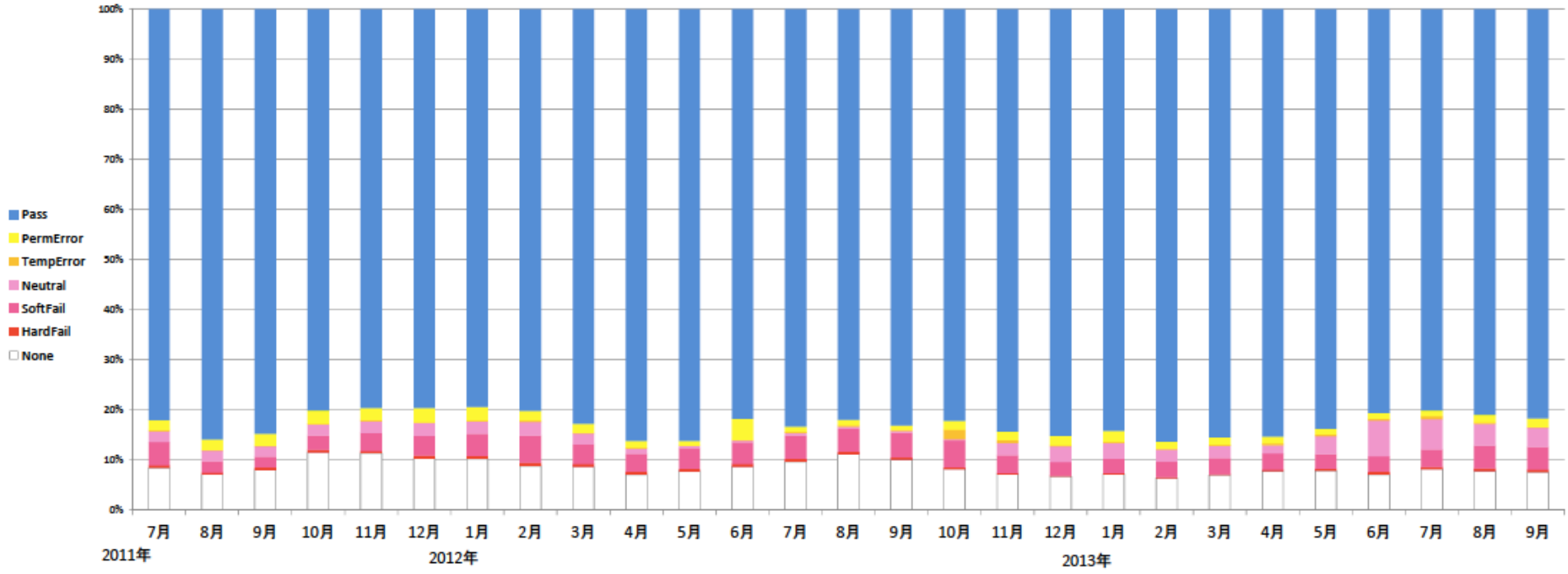
- IETF spfbis (SPF Update) WG (2011.11〜)
  - MARID WG (2004-2006), Experimental RFC4405〜RFC4408 (April, 2006)
  - その後 SPF が広く導入されたことを背景にこれまでの経験を集約し仕様の改訂を目指す
  - Standard Track 状態に持って行く
  - 議論の前提
    - SPF は成功したが Sender-ID はそうではない
    - SPF の仕様改訂は、間違いの訂正、利用していない機能の削除、既に広く使われ手いる拡張の追加など
    - SPF の拡張や使われている機能の削除はしない

SPF の動向 (2)

- Internet Draft の概要
  - draft-ietf-spfbis-4408bis-21
  - DNS RR Type
    - SPF RR type (99) ではなく TXT RR を利用
  - 認証失敗時の扱いについて
    - Local policy で判断
  - マクロ機能
    - とりあえず残す方向
  - 認証結果の記録
    - `Received-SPF:` ヘッダと `Authentication-Results:` ヘッダの併用
  - 転送とメーリングリストとの関係
    - それほど議論にはならなかった模様 (RFC5321.From の書き換えや受け側での whitelist による対応)

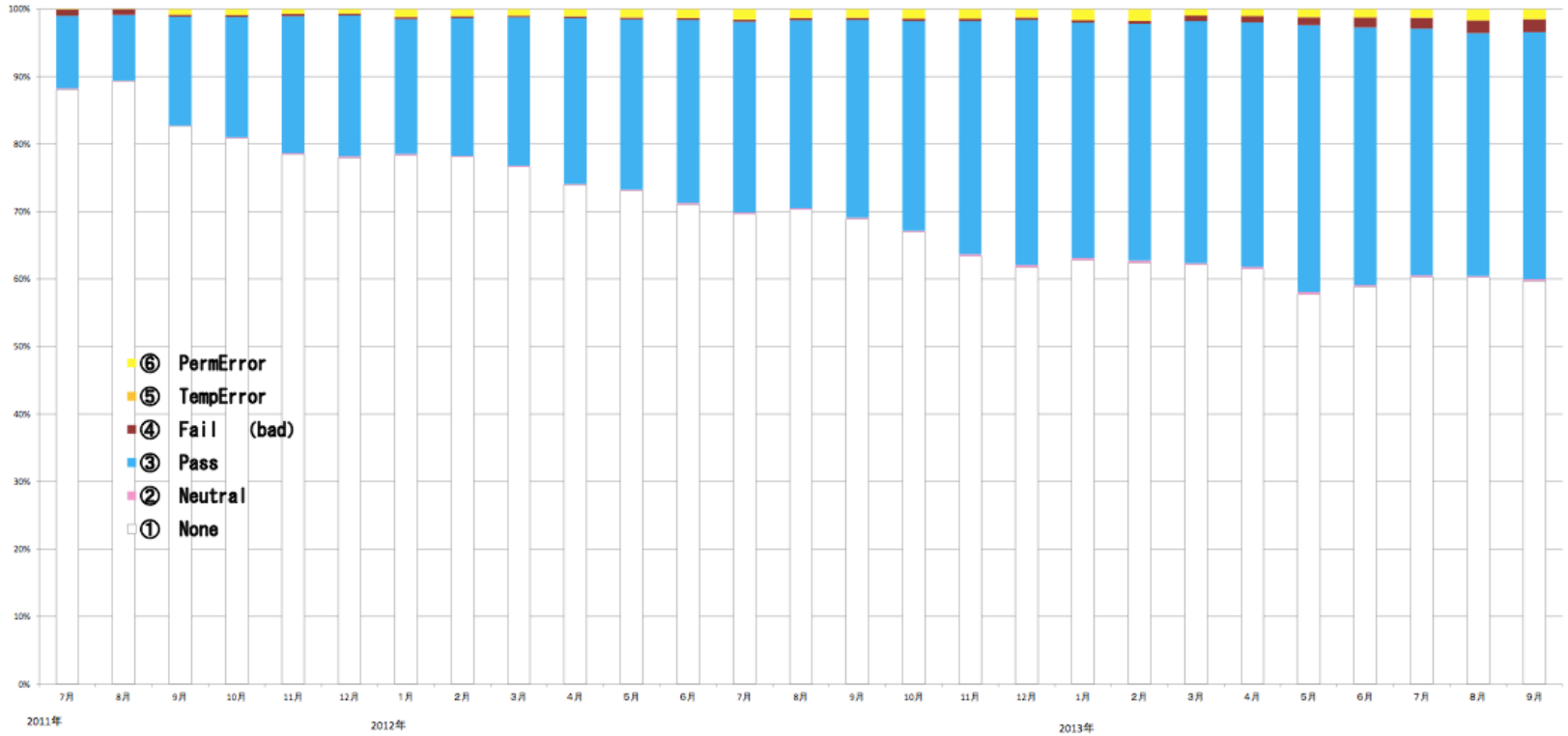
SPF の動向 (3)

- SPF の導入状況
  - 電気通信事業者7者の協力により、総務省のとりまとめ
  - 92.47% (2013.09、認証結果none以外の割合)



DKIM の動向 (1)

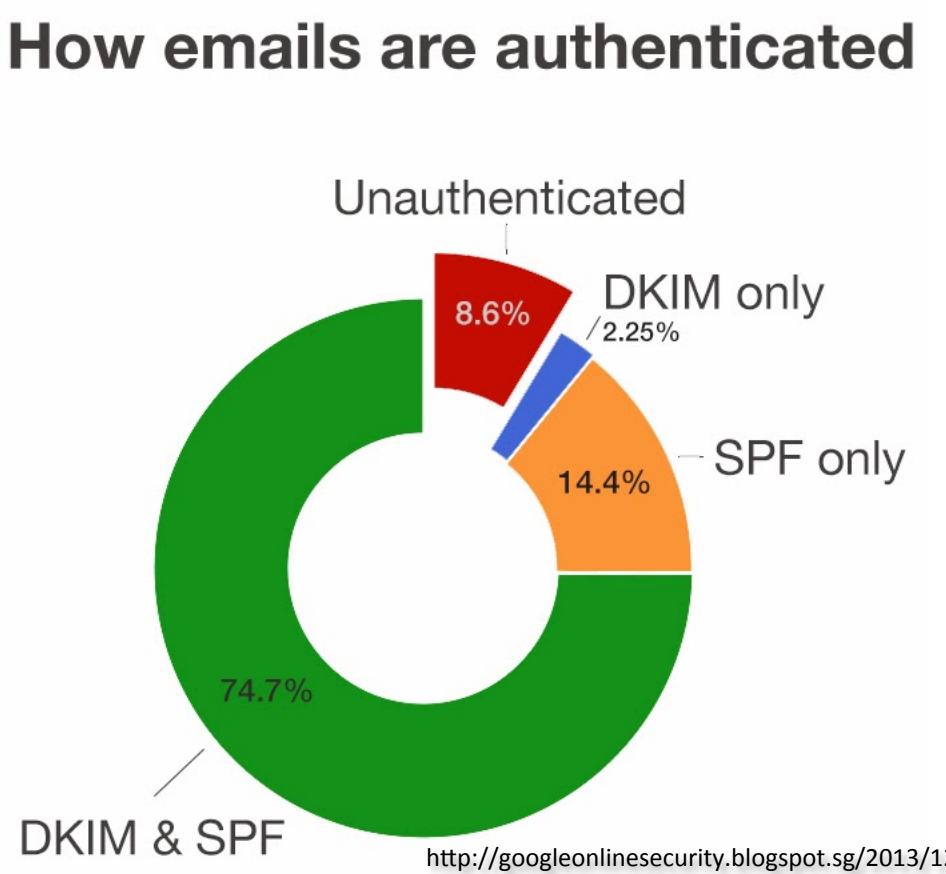
- DKIM の導入状況
  - 電気通信事業社4社の協力により総務省がとりまとめ
  - 40.26% (2013.09, 認証結果 none 以外の割合)



※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

SPFとDKIMの動向

- Gmail (Google) の調査結果



http://googleonlinesecurity.blogspot.sg/2013/12/internet-wide-efforts-to-fight-email.html

source: Gmail 2013

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 (2)

- 動機と経緯
  - eBay, PayPal と Yahoo!, Google (Gmail) が DKIM を利用したフィッシング対策を開始
    - eBayとPayPal, フィッシング対策でGmailと協力 (2008.07.09, 日経BP ITpro News)
  - 初期のテスト結果は比較的良好
    - しかしながら認証が失敗するケースも多少あった
    - 単一の認証技術だけでなく複数の認証技術を利用すことに
    - 認証失敗の原因を究明できるよう Feedback が行えるような仕組みも必要
  - さらに他の送受信事業者を含めてより広いグループに拡張
  - グループで初期ドラフトを作成し、2011年の MAAWG で提示、2012.01.30 DMARC.org として発足 (dmarc-discuss ML)
  - 2012.11 85th IETF @ Atlanta で dmarc WG を提案、その後 IETF へ (dmarc-ietf ML)

DMARC
(3)

- 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

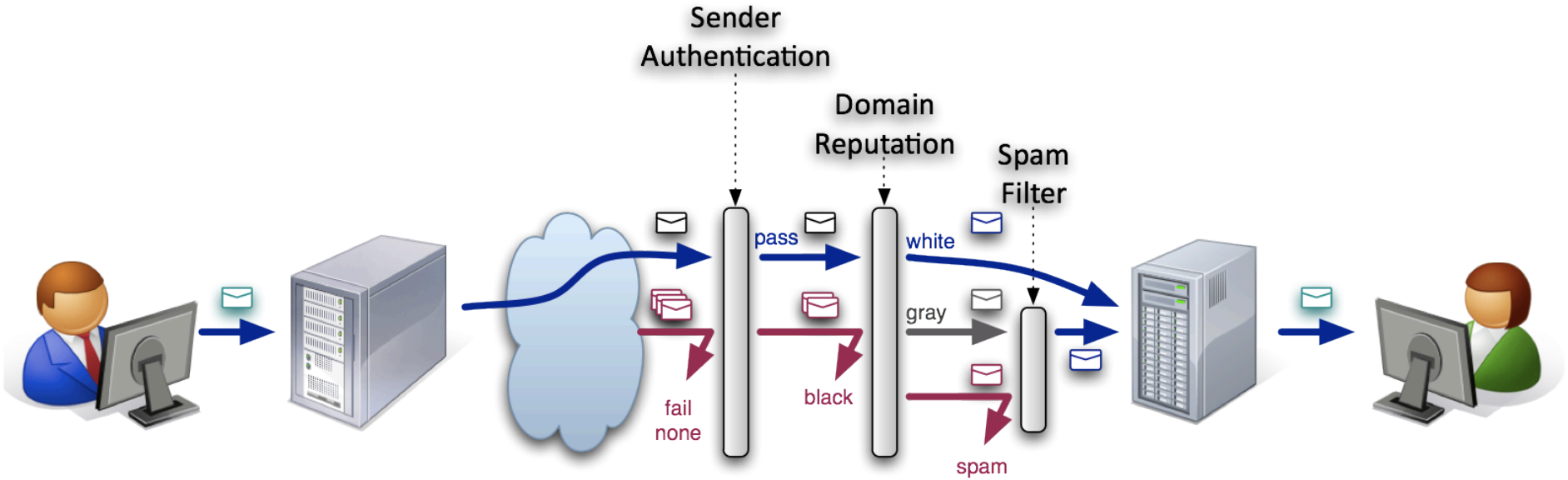
```
_dmarc.example.jp TXT "v=DMARC1; p=none; rua=mailto:dmarc-feedback@example.jp"
```

  - 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 (4)

- 受信側の導入
  - 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

送信ドメイン認証技術の利用



- Sender Authentication & DMARC
  - 正当なメールの送信元がほとんど対応していることを前提に pass 以外は詐称と判断して reject (**最終形**)
  - 認証結果 none のメールを柔軟に対応 (**移行期**)
- Domain Reputation
  - 認証された送信者情報 (詐称されていない) を評価して受け取るべきメールだけを受け取る (Domain White List の利用)
- Spam Filter
  - ドメインレピュテーションで判定ができなかった送信元のメールを内容などを基に spam 判定 → 結果はレピュテーションへ feedback

課題

- メール配送形態による認証の失敗
  - メール転送による SPF の認証失敗
    - 転送元での RFC5321.From の書き換え → 転送先で SPF は pass → DMARC では RFC5322.From と不一致 (fail)
    - DKIM の導入 or 転送先でのホワイトリスト (転送者≒転送受信者なので) で対応
  - メーリングリスト機能
    - Mailman などでは RFC5321.From はメーリングリスト管理アドレス → SPF は pass → DMARC では RFC5322.From と不一致 (fail)
    - Subject: ヘッダの書き換え ([dmarc-ietf] の付与等) → DKIM の認証失敗 → コンテンツの改変を止める
    - Mailman の次バージョンでは From: ヘッダを書き換える機能が追加されるとの情報もあり
- 日本におけるDKIMの普及

普及に向けて

- 向かうべき方向性
  - SPF, DKIM 双方の良いところをうまく活用
  - メールの責任の所在を明確に

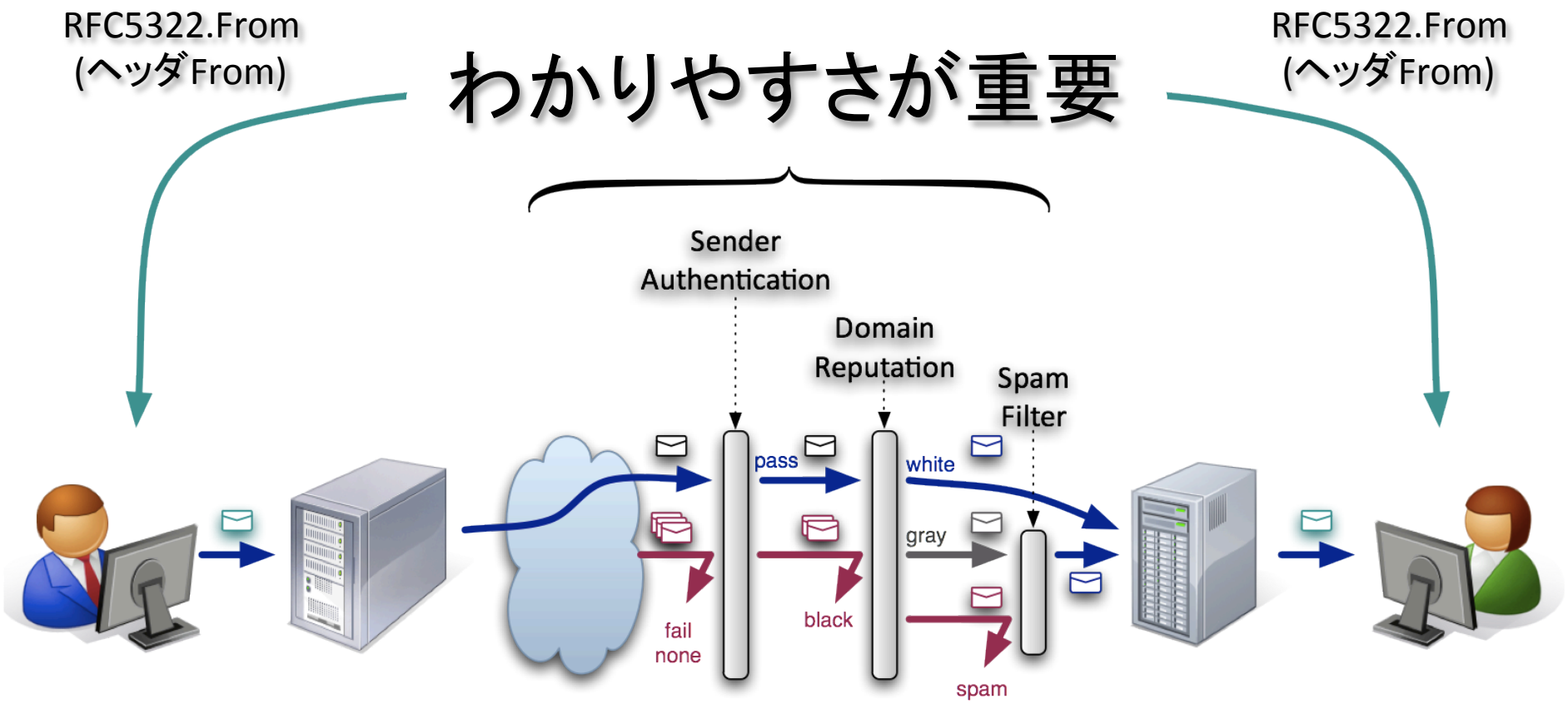
    → RFC5322.From (ヘッダ From) を基軸に
  - 認証がうまくいかないケースが見つけ出せる仕組み & 対策の検討 → feedback の仕組み

↓

DMARC

(Domain-based Message Authentication, Reporting & Conformance)

普及に向けて


RFC5322.From
(ヘッダFrom)
わかりやすさが重要
RFC5322.From
(ヘッダFrom)
Sender
Authentication
Domain
Reputation
Spam
Filter
pass
white
gray
fail
none
black
spam