DMARCによる新しいメール認証と導入の留意点

~DMARCのおさらい~

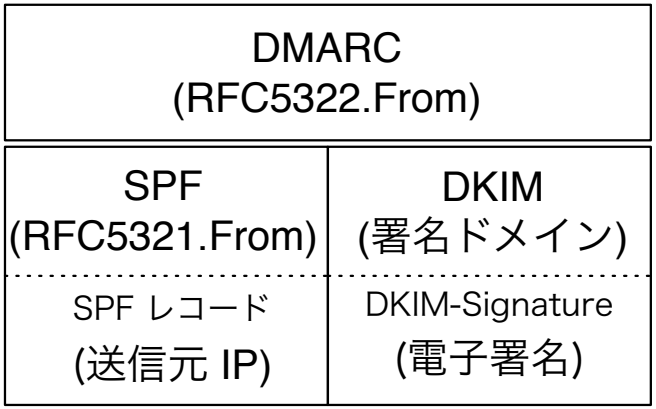
2016.10.05

第15回 迷惑メール対策カンファレンス

IAjapan (Internet Association Japan)

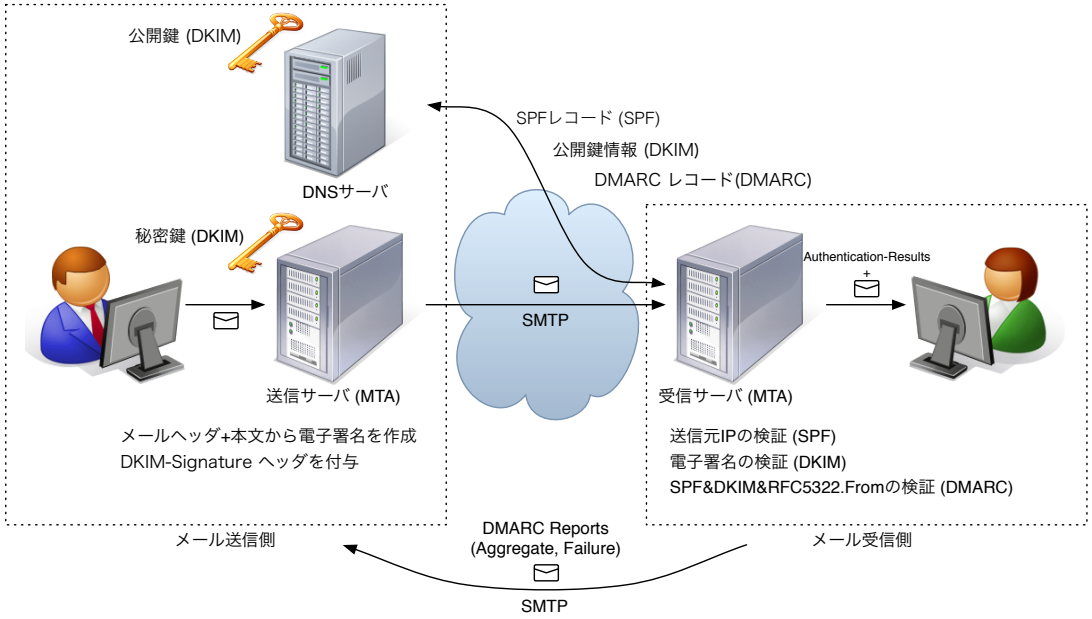
DMARCとは

- 特徴
  - SPFとDKIMの認証結果を利用（どちらか pass したドメイン）
  - 送信側が認証失敗したメールの取り扱いを表明可能（ポリシー）
    → 受信側の判断が容易に
  - 送信側が認証状況を DMARC レポートとして受け取る
    → レポートは受信側が作成し送信する
  - DMARC レポートから SPF, DKIM の設定確認が可能



DMARCとは

- 規格
  - SPF: RFC7208, Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1
  - DKIM: STD76, RFC6376, DomainKeys Identified Mail (DKIM) Signatures
  - DMARC: RFC7489, Domain-based Message Authentication, Reporting, and Conformance (DMARC)



DMARCの導入
メール送信側

- 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 (最終的には “p=reject” へ)

DMARCとは
ポリシー

- 送信側のポリシーを表明
  - 受信側に認証が失敗したメールの取り扱いを表明 (ポリシー)
  - DMARCレコードの “p=“ で記述

none	何もしない
quarantine	不要なメールとして認識させる (隔離)
reject	受信拒否

- 他の送信ドメイン認証技術との比較
  - SPF: SPF レコードの末尾で強度を表明 (neutral, softfail, hardfail)
  - DKIM: DKIM-ADSP で署名の有無を表明

DMARCの導入
メール受信側

- 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 (上位ドメイン) 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

Aggregate Report

- 方法等
  - DMARC レコードの “rua=” で示された URI (mailto: は必須) に送信
  - XML フォーマット (must) で GZIP (should) 圧縮されたファイル
  - mailto: 宛の場合は MIME 形式
    - 圧縮された場合の Content-Type は application/gzip
    - 非圧縮の場合は application/xml
  - ファイル名の規則

```
receiver"!"policy-domain"!"begin-timestamp"!"end-timestamp[!uniq-id]"."extension
```

実例:

```
mail.receiver.example!example.com!1013662812!1013749130.gz
```

Aggregate Report

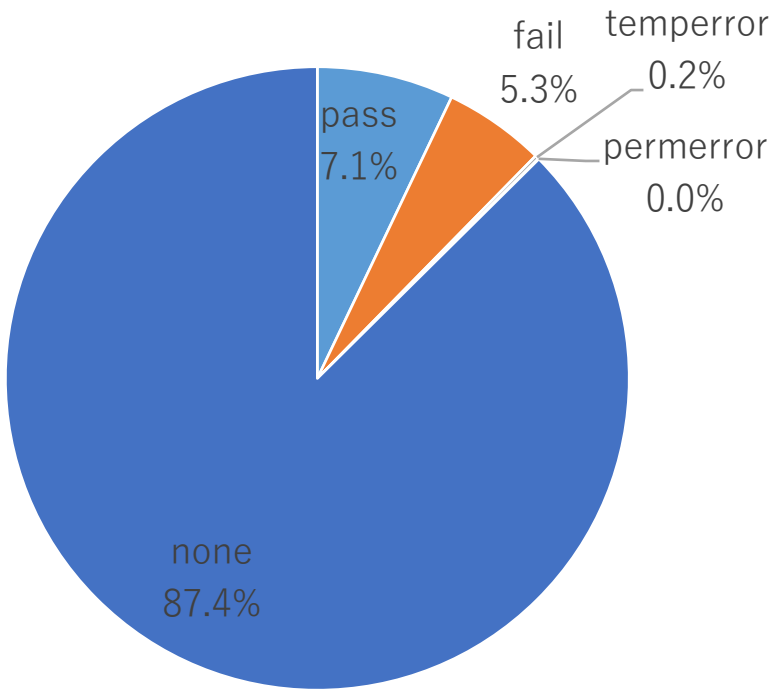
```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
    <org_name>acme.com</org_name>
    <email>noreply-dmarc-support@acme.com</email>

<extra_contact_info>http://acme.com/dmarc/support</extra_contact_
info>
    <report_id>9391651994964116463</report_id>
    <date_range>
      <begin>1335571200</begin>
      <end>1335657599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>example.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>none</p>
    <sp>none</sp>
    <pct>100</pct>
  </policy_published>
```

```
<record>
    <row>
      <source_ip>72.150.241.94</source_ip>
      <count>2</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
      <header_from>example.com</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>example.com</domain>
        <result>fail</result>
        <human_result></human_result>
      </dkim>
      <spf>
        <domain>example.com</domain>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
</feedback>
```

DMARCの導入状況

DMARCの認証結果

- 期間: 2016.09 (流量ベース)
- 対象: IIJ のメールサービス
- DMARC認証結果
  - 導入割合は 12.6% (fail を含む) と低め
  - 認証失敗 (fail) 割合が高めで 5.3%



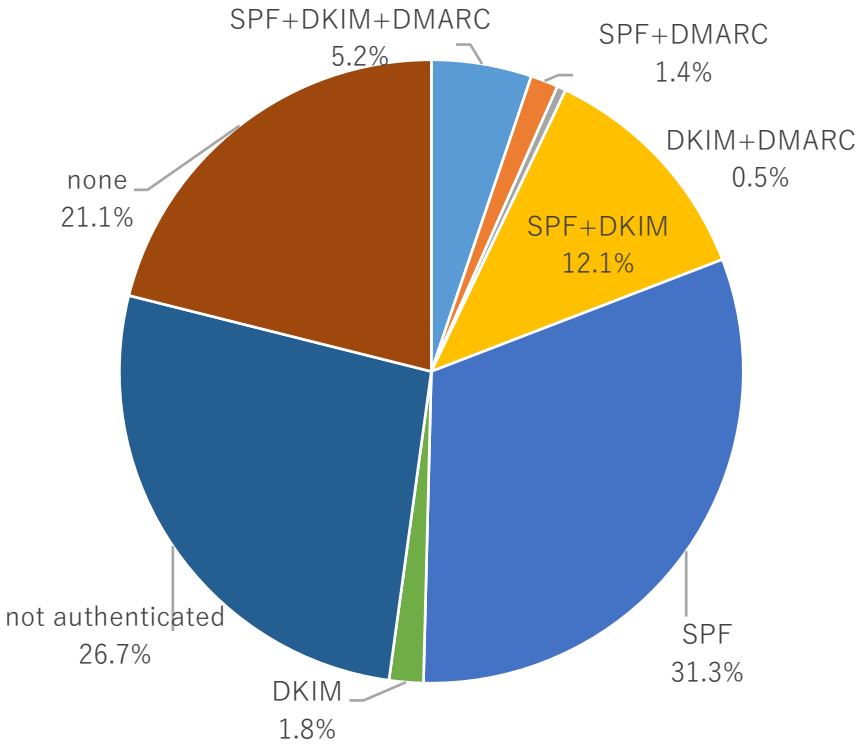
DMARCの導入状況

認証成功の組み合わせ

- DMARC認証 pass の要因
  - 最も多い組み合わせは SPFとDKIMともに “pass” 5.2%
  - DKIM による pass 割合 5.7%
  - SPF による pass 割合 6.6%
- DMARC認証に非対応
  - SPF 普及率の高さ 31.3%
  - SPF と DKIM ともに pass している割合も高い 12.1%

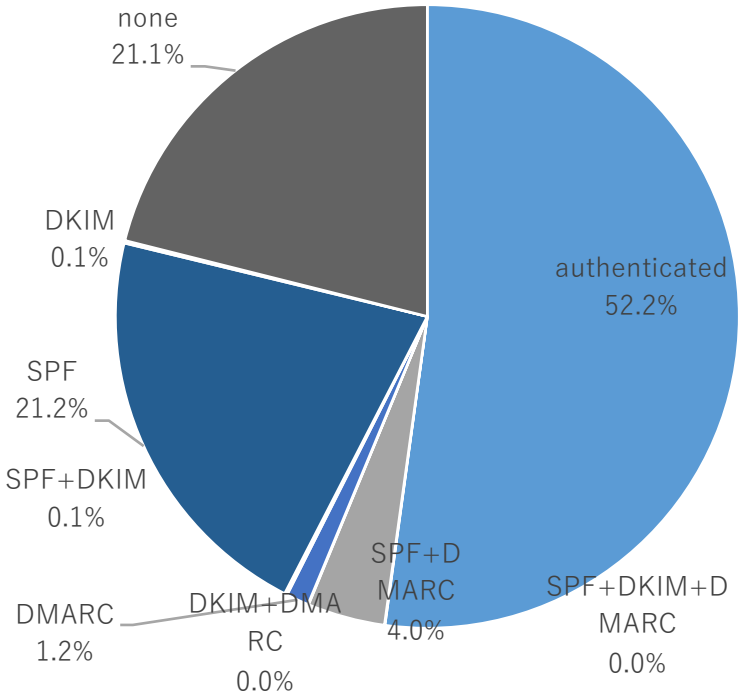
  → DMARC レコードを記述するだけ (とも言い切れないが)
- 認証できない割合
  - いずれの送信ドメイン認証技術でも認証できなかったのは 21.1%
  - 認証失敗の割合も高い (26.7%)

    → 要因分析が必要



DMARCの導入状況
認証失敗の組み合わせ

- 認証失敗の要因
  - SPF 単体時の認証失敗が高い
    - DMARC 無し 21.2%
    - DMARC あり 4.0%
  - DKIM に対応している場合の失敗割合は低い
    - DMARC 無し 0.1%
    - DMARC あり 合計 0.1%
  - SPFにもDKIMにも対応していないのにDMARCが fail (1.2%)
    → 別途検討が必要



DMARC認証結果からの考察

- 普及率
  - DMARCの認知率はまだ低い (fail も含めて 12% 程度)
  - DMARCの導入方法は DMARC レコード (TXT RR) を記述するだけ
    → 送信側は SPF (8割程度) と同等の作業
- DMARC導入の注意
  - DMARC単体での認証失敗
    - RFC5322.From の詐称メール (SPF, DKIM 非対応)
    - 上位ドメインが DMARC レコードを記述
      - SPF と DKIM を導入していないサブドメイン
      - 上位ドメインは Organizational Domain の仕組みにも注意
  - SPF の認証失敗割合は高い
    - 詐称メールが正しく認証失敗しているかもしれないが…
    - 転送問題も…
  - DMARCをpassさせるには
    - DKIMの導入が効果的 ← DKIMの認証失敗割合は少ない