JPAAWG | Japan Anti-Abuse Working Group

DMARCガイドライン解説

作成者によるRPKI/DNSSEC/DMARCガイドライン要点解説

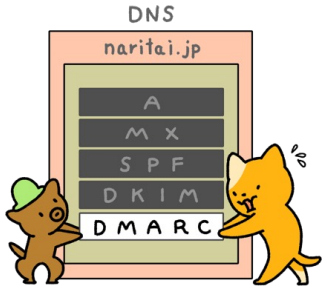
2024.11.21

Messaging Research Institute (MRI)
Japan Anti-Abuse Working Group (JPAAWG)

SAKURABA Shuji, Ph.D.

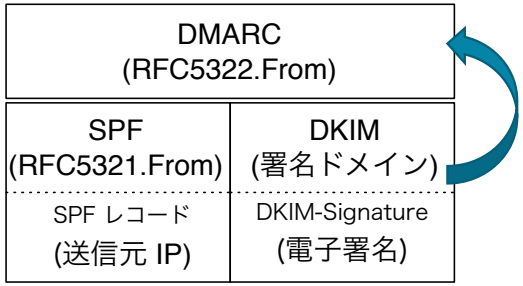
送信ドメイン認証技術

- 送信者をドメイン名単位で認証 (詐称されていないことを確認) する仕組み
- 認証の仕組みの違いで 2つの認証方式と 3つの認証ドメイン
  - SPF (Sender Policy Framework): 送信元 IP + RFC5321.From ドメイン
  - DKIM (DomainKeys Identified Mail): 電子署名 + 署名ドメイン
  - DMARC (Domain-based Message Authentication, Reporting, and Conformance): SPF and/or DKIM + RFC5322.From ドメイン
- 認証結果は `Authentication-Results` ヘッダに記載



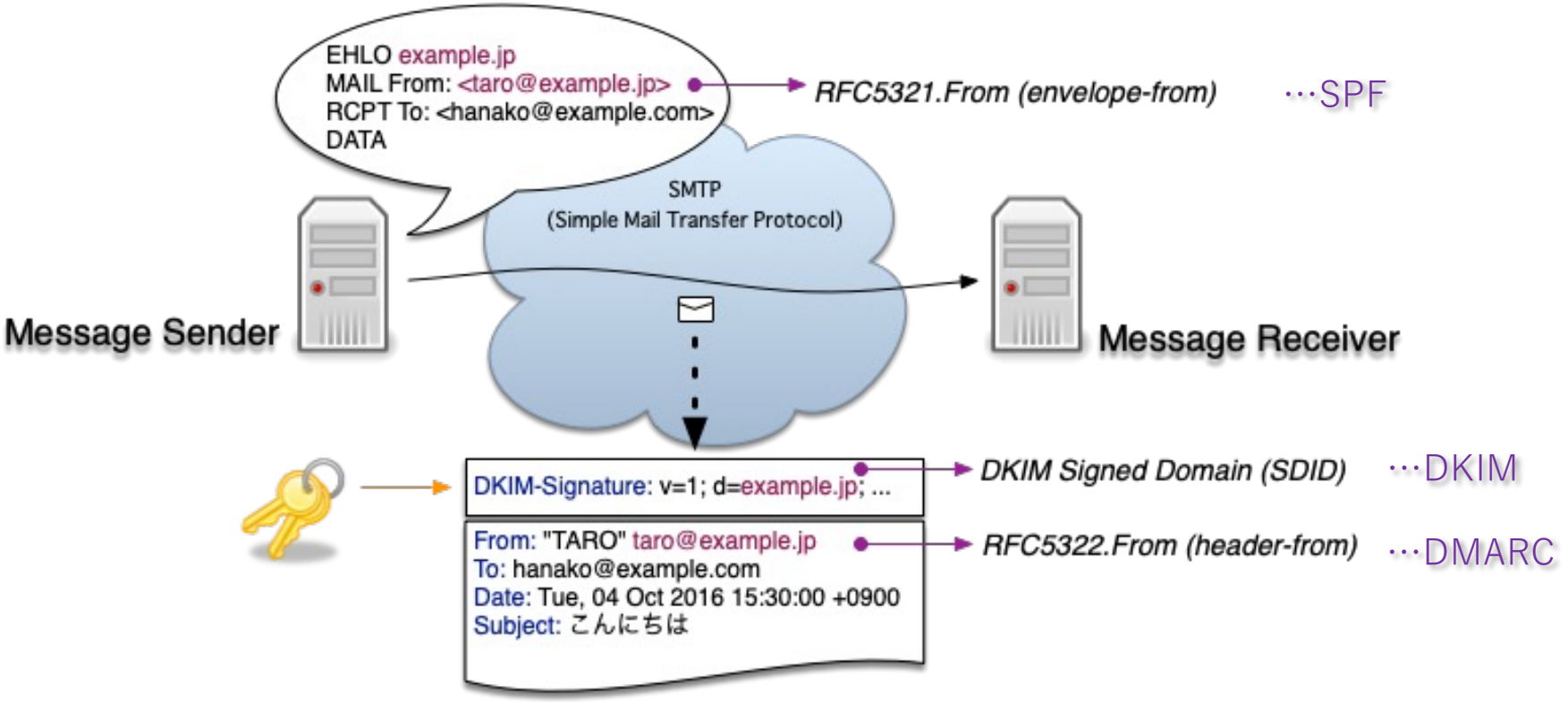
ナリタイ <naritai.jp>

	SPF	DKIM	DMARC
名称	Sender Policy Framework RFC 7208	DomainKeys Identified Mail STD 76, RFC 6376	Domain-based Message Authentication, Reporting, and Conformance RFC 7489
特徴	送信元をネットワーク的に判断 （送信元のIPアドレスにより確認）	送信時に電子署名をメールに付加 （電子署名の検証により判断）	SPFあるいはDKIMの認証結果を利用 （送信側でポリシーを設定、認証結果のレポート機能）
導入コスト	送信側はほぼ皆無（DNSの記述のみで1通ずつの処理は不要） 受信側では一定の処理が必要	送信側は相対的に高め （1通ずつ署名作成・付加が必要） 受信側では一定の処理が必要	既にSPF, DKIMを導入していれば送信側はほぼ皆無 （DNSの記述のみ） 受信側では一定の処理が必要
長所	送信側の導入の容易さ（特にコスト面） 普及が進んでいる	メール本文の改ざんも検知 メールの配送経路に影響されない	送信側の導入の容易さ 認証失敗時のふるまいをポリシー指定可能
短所	メール転送時に認証失敗する場合がある	配送経路上でメール内容が変更されると認証失敗 第三者署名ではDMARC認証に失敗する場合がある（DNS設定の工夫で回避できる場合がある）	SPFとDKIM双方が失敗する場合には認証が失敗する



JPAAWG

送信ドメイン認証技術 SPF,DKIM,DMARC



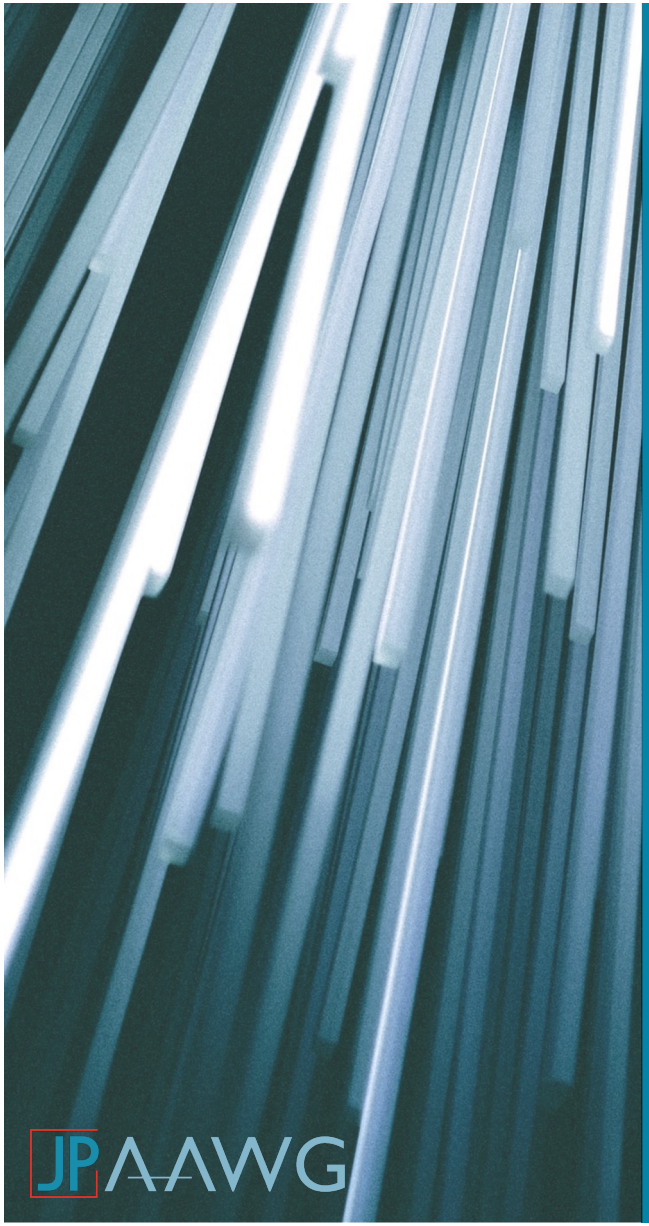
DMARC導入ガイドラインの概要 I

- 導入に際してのレベルを3段階で設定
  - Must: するべきである，最低限守らなければならない基準
  - Should: した方が良い，実現可能な場合に取り組むべき基準
  - May: 勧める，現時点では任意だが実現できればより効果が得られる基準
- メール送受信に関わる立場毎に設定
  - 送信側 (ドメイン管理者): メール送信側およびドメイン名を管理している側
  - 配送事業者: メール作成者に代わって多くのメール受信者に届ける立場
  - 再配送時: メール転送やメーリングリストなど受け取ったメールを再配送する立場
  - 受信側: 送られてきたメールを受け取り，最終的な受信者に届ける側
- 位置付け
  - 全体で 19 pages
  - 設定の詳細や解説は「送信ドメイン認証技術導入マニュアル」の参照を想定

JP AAWG

DMARC導入ガイドラインの概要 II

- ガイドライン項目数 (全36)
  - 送信側 (15): Must (4), Should (8), May (3)
  - 配送事業者 (4): Must (2), Should (2), May (0)
  - 再配送時 (7): Must (5), Should (0), May (2)
  - 受信側 (10): Must (4), Should (4), May (2)
- ガイドラインの管理
  - 今後の技術標準や運用方法の変化などに応じてレベルや項目は見直し予定
  - 既に DMARC や関連する技術の仕様の改訂作業が行われている
  - DMARC導入ガイドラインの管理移管先 (迷惑メール対策推進協議会 技術WG) にて内容および改善のタイミングと議論予定



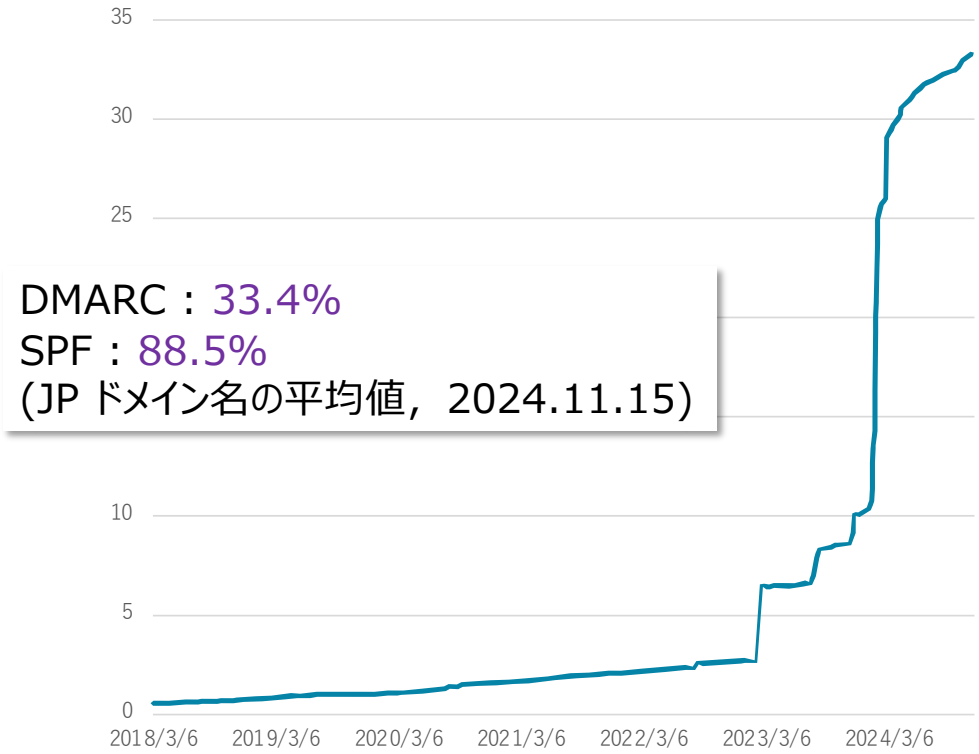
送信ドメイン認証技術
DMARC導入ガイドライン

JPAAWG

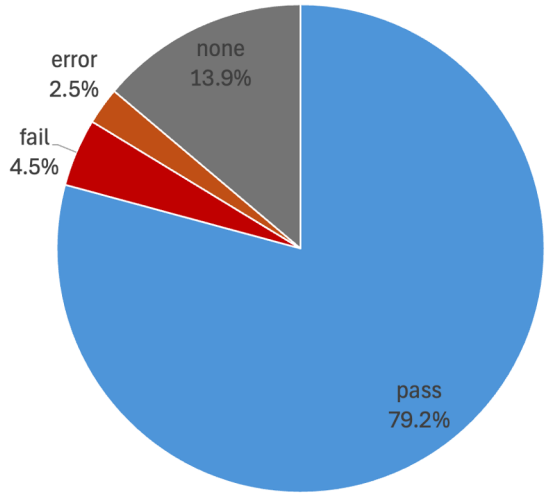
メール送信側 I

- DMARC導入に際しては SPF, DKIM のいずれか (Must) あるいは両方 (Should) を導入 [1][2]
- DMARCのポリシー (p=) は，none から始め (Should) 認証結果をDMARCレポートを利用 (May) して強度を上げる [3][4]
- SPF レコードの設定内容を事前に確認 (May) し，他のドメイン名のSPF レコードを取り込む場合は定期的に確認 (Should) [5][6]
- DKIM の署名が再利用されないよう署名対象を適切に (Must) [7]
- 組織ドメインにはDMARCレコードを設定し (Must), サブドメインに対するポリシーも設定 (Should)，メールに利用するドメイン名は個別に設定 (Should) [8][9][10]

DMARCの普及率



DMARC：33.4%
SPF：88.5%
(JP ドメイン名の平均値，2024.11.15)



電気通信事業者4社の総務省の統計 (2024.03)

JPAAWG

DMARC, SPF レコードの設定

- JP ドメイン名の DMARC レコードの policy 設定間違い: 0.06%
- JP ドメイン名の SPF レコードの設定間違い (permerror): 1.70%
  - SPF レコードを複数設定: 31.2%
  - include 先に SPF レコードが無い: 20.1%
  - DNS の lookup 回数超過: 18.5%
  - mechanism の間違い: 9.2%
  - include が再帰: 6.7%
  - IP address の指定間違い: 6.3%
  - 引けないドメイン名が制限 (2回) を越える: 2.5%

2024.11.01 調査

メール送信側 II

- メールに利用しないドメイン名にも適切に設定 (Should) [11]
- DMARCレポート (aggregate) を受信 (Should) し，DMARC のポリシーを reject まで設定 (Should) [12][13]
- DMARCレポートの受信および分析について (May)，外部ドメイン名でレポートを受ける場合の移譲設定 (Must) [14][15]

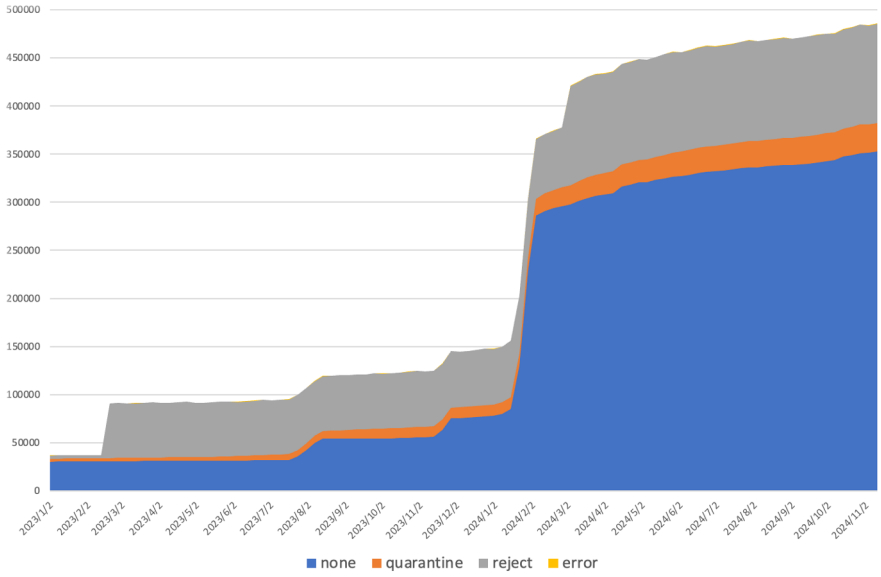
メールに利用しないドメイン名の設定

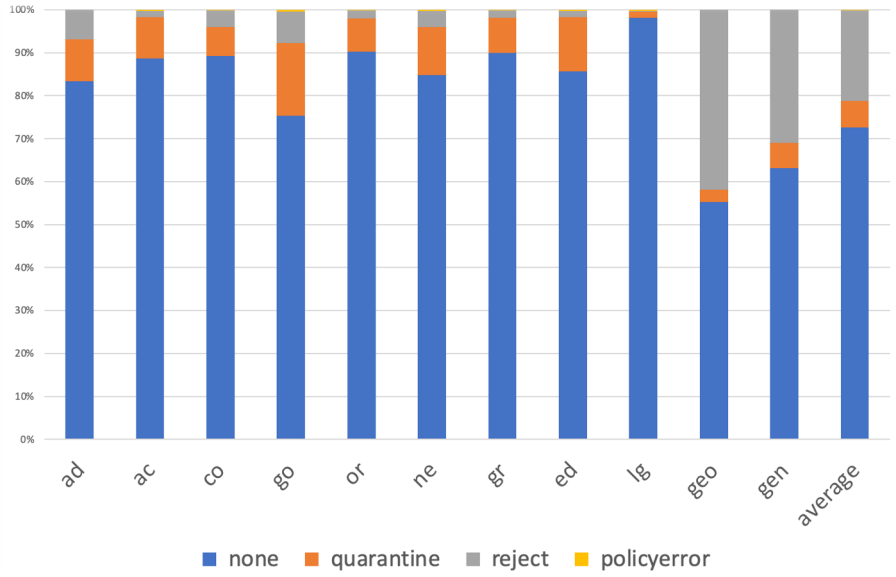
- メールに利用しないドメイン名の設定
  - ドメイン名が DNS で参照できるだけで悪用される恐れあり (親ドメイン等)
  - メールに利用しないドメイン名ことを示す設定方法 (Null MX および SPF, DMARC)

```
example.com.          IN MX 0 .
example.com.          IN TXT "v=spf1 -all"
_dmarc.example.com.IN TXT "v=DMARC1; p=reject"
```

  - jp ドメイン名で設定されているMXレコードの 6.6% が Null MX
  - Null MX の 99.2% のSPFレコードが “v=spf1 –all” ← ドメイン名の詐称防御
  - Null MX & fail SPF の 99.6% の DMARC レコードが “v=DMARC1; p=reject” ← 受信拒否可

DMARC policy の設定状況





JPAAWG

配送事業者

- SPF, DKIM, DMARC の設定 (Must) [1]
- include 用の SPF レコードの提供 (Should) [2]
- 配送依頼元に対する DKIM 鍵レコードの適切な提供 (Should) [3]
- DMARC 認証対象であるヘッダ From の適切な設定 (Must) [4]

再配送時

- 送信メールが転送される場合はDKIMに対応 (Must) [1]
- 転送先で受け取り判断を SPF で行う場合，RFC5321.From を転送元とし (May), エラーメールがループしないよう処理 (Must) [2][3]
- メーリングリストでは RFC5321.From と RFC5322.From のドメイン名をメーリングリストのドメイン名とし，SPF, DKIM, DMARC に適切に対応する (Must) [4][5][6]
- メーリングリストの再配送先が ARC に対応している場合，ARC 導入を勧める (May) [7]

受信側

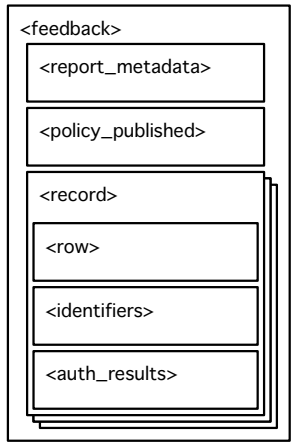
- メール受信時に SPF, DKIM, DMARC 認証を行い (Must)，SPF レコードの内容確認や DKIM の署名対象も確認 (May) [1][2][3]
- 認証結果だけではなく認証ドメイン名も確認 (Must)，ドメイン名の評価 (レピュテーション) も行う (Should) [4][5]
- DMARCレポートの送信は移譲関係を確認 (Must) [6]
- DMARCレポートの failure report 送信は含まれる情報に注意が必要 (Must)，aggregate report は送信 (Should) [7][8]
- 送信ドメイン認証の結果をわかりやすく提示 (Should)，BIMI への対応 (Should) [9][10]

DMARC レポート

- failure report
  - 認証失敗の都度送信
  - ARF (Abuse Reporting Format) 形式
  - いわゆる bounce mail と同様だが送信先が ruf= で示されたアドレス

- aggregate report
  - 定期的なフィードバック
  - XML フォーマットのデータ
  - 圧縮データ(gzip)
  - MIME 形式によるメール送信
  - データ例 (右図→)
  - 送信元 (IP) と各認証結果情報

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>…</ report_metadata>
<policy_published>
    <domain>iij.ad.jp</domain>
    <adkim>…</adkim><aspf>…</aspf>
    <p>none</p><sp>none</sp><pct>100</pct>
</policy_published>
  <record>
    <row>
      <source_ip>…</source_ip>
      <count>319</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>pass</dkim><spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
      <header_from>iij.ad.jp</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>iij.ad.jp</domain>
        <result>pass</result><selector>…</selector>
      </dkim>
      <spf>
        <domain>iij.ad.jp</domain><result>pass</result>
      </spf>
    </auth_results>
  </record>
….
</feedback>
```



Aggregate Report Format

まとめ

- 送信側でのDMARC導入 (SPF, DKIM 含めて) は必須
- なりすまし対策のためには p=reject まで設定
- SPF や DKIM の設定内容の確認を (DMARC aggregate report の利用などを検討)
- メール再配送時の対応 (できれば DKIM 再署名と RFC5322.From ドメイン名の書き換え) を
- メール受信者に対して適切な認証結果の提示を，BIMI への対応も検討していくべき (幾つかのメール受信サービスでは既に BIMI に対応してきている)
- DMARC の受信側の認証および policy に対応した処理については法的な整理がなされている → 通信の秘密に関しての課題は解決済み

Thank you