JP AAWG JAPAN ANTI-ABUSE WORKING GROUP

# SPF/DKIM/DMARCの基本

株式会社インターネットイニシアティブ

大木 一輝

# 目次

1. 送信ドメイン認証とは
2. SPFの仕組み
3. DKIMの仕組み
4. DMARCの仕組み
5. まとめ

# 1. 送信ドメイン認証とは

- 送信元IPアドレスや、電子署名の仕組みを利用してなりすましメールを判断する仕組み
- なりすましメールは送信元の情報が記載されるFromアドレス（エンベロープFromまたはヘッダーFrom）を偽装することができるので対策が必要
- SPF/DKIM/DMARCといった仕組みを利用する
- 今後の説明では2種類のFromに関する情報が出てくるので注意
  - エンベロープFrom：メールの配送で使われる差出人
  - ヘッダーFrom：実際に受信した人が見る差出人

# 2-1. SPFの仕組み

## SPF（Sender Policy Framework）とは

- IPアドレスを利用して受信したメールが正しい差出人から送られていることを確認する仕組み
- 送信側は、送信に利用するサーバのIPアドレスをDNSに「SPFレコード」として登録する必要がある
- メールの受信サーバは、エンベロープFromのドメインからSPFレコードを取得し、送信元IPアドレスと照合する
- ただし、転送されると送信元のIPアドレスが変わるため、認証に失敗する場合がある
  - DKIMを併用することで補うことができる場合がある
- SPFが確認するのはエンベロープFromのみのため、表示上のヘッダーFromの偽装は判断できない（DMARCで補完）

# 2-2. SPFの仕組み

SPFレコードについて

## SPFレコードの例（DNSのTXTレコード）

```
v=spf1 ip4:192.0.2.0/24 include:_spf.example.net -all
```

| | |
|---|---|
| **どのドメイン** | エンベロープFrom（MAIL FROM）のドメイン |
| **構成** | ドメイン名そのもの（例:example.com） |
| **参照するレコード** | example.com のTXT（v=spf1で始まるもの） |

# 2-3. SPFの仕組み

**SPFレコードの主要な属性（抜粋）**

| 記述 | 意味 | 主な使い方 |
|---|---|---|
| **v=spf1** | SPFレコードのバージョン | 必ず先頭に1つ記述する |
| **ip4** | 送信を許可するIPアドレス・範囲 | 自社メールサーバのIPを指定　例）ip4:192.0.2.0/24 |
| **include** | 他ドメインのSPFレコードを取り込む | クラウドメールや配信サービスの利用時<br>例）　include:_spf.example.net |
| **-all** | 上記以外は拒否（ハードフェイル） | 厳格に拒否したい場合（導入初期は~allで様子見も可） |

※ include などはDNS参照が最大10回まで。SPFレコードは1ドメインにつき1つだけ登録する
※ 上記は主な属性のみ。他にも複数の属性がある（詳細はRFC 7208参照）

# 2-4. SPFの仕組み

**正規メールと差出人偽装メールを比較**

| | 接続元IP | MAIL FROM | DNSの許可IP | 判定 |
|---|---|---|---|---|
| 正 正規 | 192.0.2.10<br>許可済み | bounce@example.com | 192.0.2.10<br>許可IP | **SPF pass**<br>配信 |
| 偽 偽装 | 198.51.100.66<br>未許可 | bounce@example.com | 192.0.2.10<br>許可IP | **SPF fail**<br>受信拒否 |

**192.0.2.10 ＝ 許可IP → pass　｜　198.51.100.66 ≠ 許可IP → fail**

※ MAIL FROMにexample.comを使い、未許可IPから送った偽装メールはSPF fail。
ヘッダーFromだけの偽装はDMARCで確認する。

例示用：RFC 2606 / RFC 5737

# 3-1. DKIMの仕組み

**DKIM（DomainKeys Identified Mail）とは**

- 電子署名を利用してメールが改ざんされていないかを確認する仕組み
- 送信側は、メールに電子署名を付与し、検証用の公開鍵を「DKIMレコード」としてDNSに登録する必要がある
- メールの受信サーバは、署名に記載されたドメインとセレクタをもとにDNSからDKIMレコードを取得し、公開鍵で署名を検証する
- 転送されても、メールが改変されなければ署名は保たれるため、SPFの転送時の弱点を補える場合がある
- 一方で、メーリングリスト（ML）などで件名や本文が書き換えられると、署名が一致せず検証に失敗する場合がある
- DKIMが確認するのは署名ドメイン（d=）による署名の正当性であり、表示上のヘッダーFromとは一致しない場合がある（DMARCで補完）

# 3-2. DKIMの仕組み

DKIMレコードについて

## DKIMレコードの例（DNSのTXTレコード）

```
selector1._domainkey.example.com. IN TXT
v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEB...
```

| | |
|---|---|
| **どのドメイン** | 署名のd=（署名ドメイン）とs=（セレクタ） |
| **構成** | s=の値 + ._domainkey. + d=のドメイン |
| **参照するレコード** | selector1._domainkey.example.com のTXT |

# 3-3. DKIMの仕組み

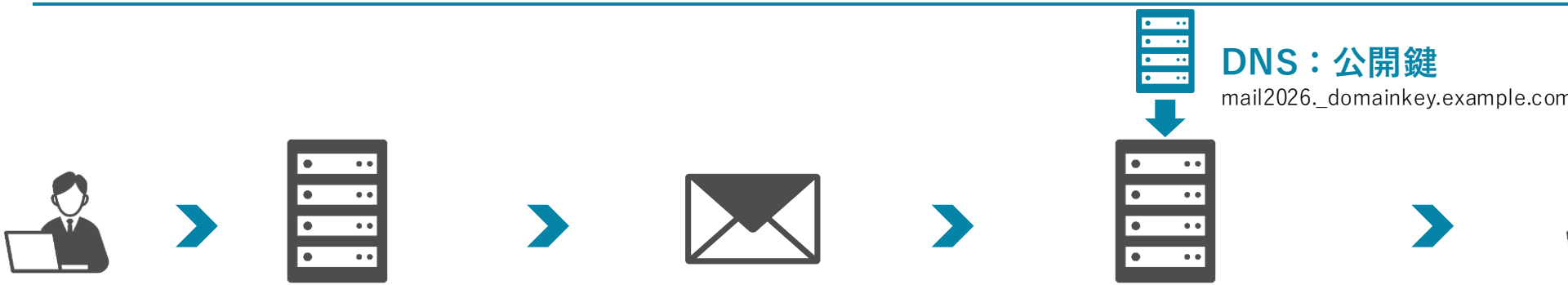
**DKIMレコードの主要な属性（抜粋）**

| 記述 | 意味 | 主な使い方 |
|---|---|---|
| **v=DKIM1** | DKIMレコードのバージョン | 先頭に記述する |
| **k=rsa** | 署名に使う鍵の種類（RSA） | 省略するとrsaとして扱われる |
| **p=** | 署名の検証に使う公開鍵 | 受信サーバがこの公開鍵で署名を検証する |

※ 鍵を更新するときは、新しいセレクタで公開鍵を追加登録してから切り替える
※ 上記は主な属性のみ。他にも複数の属性がある（詳細はRFC 6376参照）

# 3-4. DKIMの仕組み

## メール配送で見るDKIM認証




## 検証結果の2パターン

| | | | | | |
|---|---|---|---|---|---|
| 正 | 改変なし | 署名付きメール<br>署名対象が同じ | → | 公開鍵で検証<br>署名が一致 | → DKIM pass<br>検証後に配信 |
| 改 | 改変あり | 配送中に改変<br>本文・署名対象が変化 | → | 公開鍵で検証<br>署名が不一致 | → DKIM fail<br>改変・署名不正を検知 |

※ DKIM fail時の最終的な扱いは受信側ポリシーやDMARC判断による。

出典：RFC 6376

# 4-1. DMARCの仕組み

**DMARC（Domain-based Message Authentication, Reporting and Conformance）とは**

- SPF/DKIMの認証結果を使い、なりすましメールへの対応を決めるための仕組み
- SPF/DKIMで認証されたドメインが、表示上のヘッダーFromのドメインと一致するか（アライメント）を確認し、SPFかDKIMのどちらかがpassし、かつドメインが一致すれば認証成功とする
- 認証失敗時の扱い（ポリシー）を、ドメイン所有者がDNSで宣言する
- 認証結果の集計レポートを、受信側から受け取れる

# 4-2. DMARCの仕組み

**DMARC導入のメリット**

- 差出人側（ドメイン所有者）
  - ポリシー（p=）で、fail時の扱いを受信者に宣言できる
  - 集計レポート（rua=）で、認証状況や把握できていない送信元、対策の効果を確認できる
  - p=none から始め、影響を見ながら少しずつ強められる
  - 最終的には p=reject に強め、認証に失敗したなりすましメールを受信側で拒否してもらえる
- 受信者側
  - ヘッダーFromとのドメイン一致で、SPF/DKIMがpassでもヘッダーFromの偽装を判断できる
  - 公開されたポリシーを参考に、差出人の意図に沿って隔離・拒否を判断できる

# 4-3. DMARCの仕組み

DMARCレコードについて

## DMARCレコードの例（DNSのTXTレコード）

```
_dmarc.example.com. IN TXT
v=DMARC1; p=quarantine; rua=mailto:dmarc@example.com
```

| | |
|---|---|
| **どのドメイン** | ヘッダーFromのドメイン |
| **構成** | _dmarc. + ヘッダーFromのドメイン |
| **参照するレコード** | _dmarc.example.com のTXT（なければ上位ドメイン） |

# 4-4. DMARCの仕組み

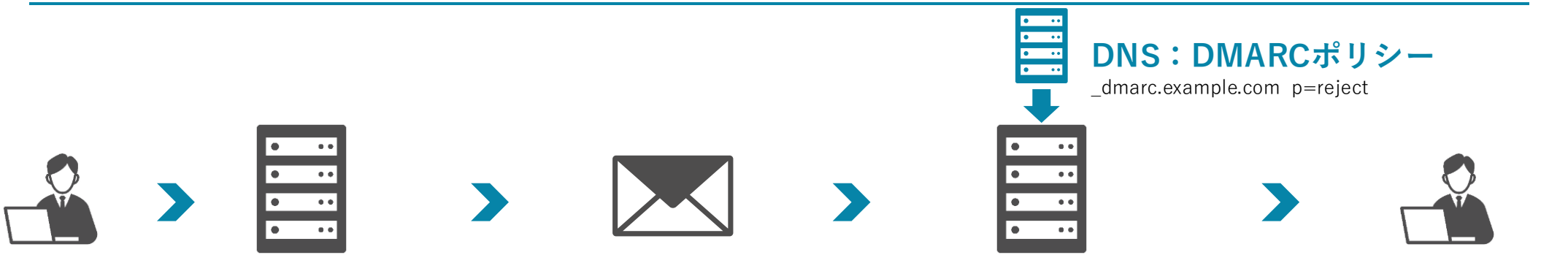
**DMARCレコードの主要な記述（抜粋）**

| 記述 | 意味 | 主な使い方 |
|---|---|---|
| **v=DMARC1** | DMARCレコードのバージョン | 必ず先頭に記述する |
| **p=** | 認証失敗時のポリシー（none / quarantine / reject） | none:何もしない、quarantine:隔離、reject:受信拒否 |
| **rua=** | 集計レポートの送信先 | mailto:形式で指定。受信側から認証結果の集計が届く |

※ 導入時は p=none で集計レポートを確認し、quarantine → reject と段階的に強める
※ 上記は主な属性のみ。sp= / adkim= など、他にも複数の属性がある（詳細はRFC 9989参照）

# 4-5. DMARCの仕組み

## メール配送で見るDMARC判断




## 判定結果の2パターン

| | | | | | | |
|---|---|---|---|---|---|---|
| 正 | 正規 | SPFまたはDKIM<br>どちらかがpass | → | Fromと照合<br>ドメインが一致 | → | DMARC pass<br>検証後に配信 |
| 偽 | 偽装 | SPF・DKIMともfail<br>またはFromと不一致 | → | Fromと照合<br>ドメインが不一致 | → | DMARC fail<br>ポリシー（p=）に従い処理 |

※ DMARC fail時は、公開ポリシー（none / quarantine / reject）を参考に受信側が隔離・拒否などを判断する。

出典：RFC 9989

# 5. まとめ

SPF・DKIM・DMARCの比較

- **SPF：送信元サーバの正当性を確認する**
  - メールを送ったサーバのIPアドレスが、許可されたものか確認する
  - エンベロープFromのドメインについて、なりすまし送信を見分ける
- **DKIM：メールが改ざんされていないことを確認する**
  - 電子署名を検証して、送信ドメインの正当性と内容の一致を確認する
  - 転送されても署名が保たれるため、SPFの弱点を補える場合がある
- **DMARC：認証結果の扱いを決め、なりすましを判断する**
  - SPF/DKIMの結果とヘッダーFromの一致を確認し、失敗時の扱いを宣言する
  - 最終的には認証に失敗したメールは受信拒否できる状態にする
  - レポートで、認証の状況を把握できる

※ 3つを組み合わせることで、なりすましメール対策を強化できる

# Thank you

