

送信サイドからみた DMARC

使っていないドメインから設定してもいいんじゃない？

株式会社クオリティア
平野善隆 <hirano@qualitia.co.jp>

名前 平野 善隆

所属 株式会社クオリティア
メール好きの方募集中！！

主な活動 M3AAWG
JPAAWG
IA Japan 迷惑メール対策委員会
迷惑メール対策推進協議会
MRI
Audax Randonneurs Nihonbashi



1. 自社のドメインをなりすましたメールが到達しないようにできる
2. SPFやDKIMが正しくないメールを追跡できる

自社のドメインをなりすましたメールを到達させない

example.jpからのメールは全部
DKIMかSPFがPASSするはずなので、
そうではない場合は拒否してくださいね



`_dmarc.example.jp TXT "v=DMARC1; p=reject"`

※ DMARC登場以前はスパムフィルタ業者にお願いするしかなかった

SPF範囲外からの送信や
DKIM署名が正しくないメールを追跡できる

example.jpからのメールは全部
DKIMかSPFがPASSするはずなので、
そうではない場合は**教えてください**ね



`_dmarc.example.jp` TXT

`"v=DMARC1; rua=mailto:rua@example.jp"`

設定方法

- 利用中のドメイン
- 利用していないドメイン
- 新規のドメイン

利用中のドメイン


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

レポートを受け取って様子を見る

➡ SPFやDKIMが正しく設定されていなければレポートが来る

本物のなりすましのレポートも混ざります

```
example.jp TXT "v=spf1 ip4:192.0.2.1 -all"
```

```
example.jp TXT "v=spf1  
ip4:192.0.2.1 ip4:10.0.1.0/24 -all"
```

```
example.jp TXT "v=spf1  
ip4:192.0.2.1 include:_spf.example.com -all"
```

- RFC8301: Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail (DKIM) (2018/1月)
- 署名も検証もrsa-sha256を使いましょう(MUST)
- rsa-sha1はやめましょう(MUST)
- 署名は1024bit以上(MUST)、2048bit以上(SHOULD)
- 検証は1024bit~4096bit(MUST)

※ しかし、2048bitはDNSに書けるサイズ255バイトを超えてしまう

- RFC8463: A New Cryptographic Signature Method for DomainKeys Identified Mail (DKIM) (2018/9月)

Ed25519-SHA256を使いましょう

BASE64後のサイズが44バイトしかないのでDNSの問題もない

- 署名側は実装しましょう(SHOULD)
- 検証側は実装必須(MUST)
- 後方互換性のために署名はEd25519-SHA256とRSA-SHA256(1024bit以上)を2つ記述する

rsa-20181108._domainkey.example.jp TXT

"v=DKIM1; k=rsa; p=11qYAYKCrFVS/7..."

ed25519-20181108._domainkey.example.jp TXT

"v=DKIM1; k=ed25519; p=MIGfMA0GCsGSIb..." "

※ RSA-SHA256とEd25519-SHA256の
両方の署名を登録する

```
DKIM-Signature: v=1; a=ed25519-sha256; c=relaxed/relaxed;  
d=example.jp; s=ed25519-20181108; t=1528637909;  
h=from : to : subject : date : message-id : from : subject : date;  
bh=2jUSOH9NhtVGCQWNR9BrIAPreKQjO6Sn7XIkfJVOzv8=;  
b=/gCrinpcQOoIfuHNQIbq4pgh9kyIK3AQUdt9OdqQehSwhEIug4D...  
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=example.jp; s=rsa-20181108; t=1528637909;  
h=from : to : subject : date : message-id : from : subject : date;  
bh=2jUSOH9NhtVGCQWNR9BrIAPreKQjO6Sn7XIkfJVOzv8=;  
b=F45dVWDfMbQDGHJFIXUNB2HKfbCeLRyhDXgFpEL8Gw...  
From: Alice <alice@example.jp>
```

- ※ ed25519とrsaの両方の署名をヘッダに付ける
- ※ Fromのドメインとd=は同じにする

ここまで来ると必要なメールのレポートは
来なくなっているはず

➡ p=rejectに変更!

```
_dmarc.example.jp TXT "v=DMARC1; p=reject;  
  rua=mailto:rua@example.jp;  
  ruf=mailto:ruf@example.jp"
```

利用中してないドメイン


メールの送信に利用していないドメイン

今日はこの意味で使います！

- 他社に取得されないように保持しているだけのドメイン
- 終了したサービスやキャンペーンで使い終わったドメイン
- 社名変更前のドメイン
- メール受信はするけど、送信しないドメイン
- Webサーバでのみ使用しているドメイン
- 意識したこともない、サブドメイン

送信に使っていないなら

躊躇なく $p=reject$ できるはず！

- メール送信なし / 受信あり
→ 受信専用ドメイン
- メール送信なし / 受信なし / Aレコードあり
→ メール以外の用途で使用されるドメイン
- メール送信なし / 受信なし / Aレコードなし
→ 使用されていないドメイン
- メール送信あり / 受信なし  これは取り扱いません
→ スパマー用ドメイン

送信がある場合

```
example.jp TXT "v=spf1 ip4:192.0.2.1 -all"
```

送信がない場合

```
example.jp TXT "v=spf1 -all"
```

送信がない場合(サブドメイン)

```
*.example.jp TXT "v=spf1 -all"
```


送信がある場合

```
selector1._domainkey.example.jp TXT "v=DKIM1;  
p=1234567890ABCD..."
```

送信がない場合

```
*._domainkey.example.jp TXT "v=DKIM1; p="
```

=で止めます



サブドメインからの送信がない場合

```
*._domainkey.*.example.jp TXT "v=DKIM1; p="
```

とは書けない！



```
*.example.jp TXT "v=DKIM1; p="
```

```
_dmarc.example.jp TXT "v=DMARC1; p=reject;  
rua=mailto:rua@example.jp;  
ruf=mailto:ruf@example.jp"
```

※ 同じ

組織ドメインの場合サブドメインも含む

a.b.c.d.example.jpの場合

`_dmarc.a.b.c.d.example.jp`を参照し、なければ、
`_dmarc.example.jp`を参照する

```
_dmarc.example.jp TXT "v=DMARC1; p=reject;  
  rua=mailto:rua@example.com;  
  ruf=mailto:ruf@example.com"
```

```
example.jp._report._dmarc.example.com TXT "v=DMARC1"
```


メール受信がなく
AやAAAAAレコードがある
ドメインの場合

MXレコードがない場合のメール配送の動きについて

RFC5321 5.1

The lookup first attempts to locate an MX record associated with the name.

....

If an empty list of MXs is returned, the address is treated as if it was associated with an implicit MX RR, with a preference of 0, pointing to that host.

拙訳)

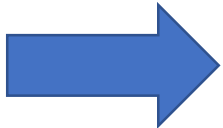
まず、(メールアドレスのドメイン)名に対応したMXレコードを参照する。

...

MXが空だった場合、そのアドレスは暗黙的にそのホストを指す preference値0のMXレコードとして扱われる

MXレコードがない場合のメール配送の動きについて

つまり、MXレコードがない場合
Aレコードを参照して配送する

 webサーバ等にメールが来る

RFC 7505 A "Null MX" No Service Resource Record for Domains That Accept No Mail (2015/6月)

```
example.jp  MX  0  .
```



サブドメインでの受信がない場合

```
*.example.jp  MX  0  .
```

SOAにもメールアドレスがあるので、届くアドレスを書きましょう

```
example.jp SOA ns.example.jp  
hostmaster.example.com  
2018110801 900 600 86400 3600
```

M³AAWG Protecting Parked Domains Best Common Practices (Updated December 2015)

https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bp-2015-12.pdf

新規のドメイン

```
example.jp    TXT "v=spf1 -all"  
*.example.jp TXT "v=spf1 -all"  
  
*.example.jp TXT "v=DKIM1; p=" "  
  
_dmarc.example.jp TXT "v=DMARC1; p=reject;  
    rua=mailto:rua@example.com;  
    ruf=mailto:ruf@example.com"  
example.jp._report._dmarc.example.com TXT "v=DMARC1"  
  
example.jp.  MX 0 .  
*.example.jp.  MX 0 .
```

パークドメインと同様に設定。TTLは短めにして必要に応じて変更。

できるところだけでも、
p=rejectにしましょう。

レポート編

 **TransWARE**



 **DEEPSoft**



今は使われていない
transware.co.jp ドメインで
DMARCを設定してみました

送信には使われていないし、
スパムは毎日のように届いているので
transware.co.jpをなりすましたメールが
あちこちで拒否されている様子が
DMARCレポートでわかるだろう。

レポートから判明した送信元

- 社内から
- 誤送信防止サービスのデモ環境から
- 監視システムから

えっ！

送信には使用されていないはずなのに・・・

```
<feedback>
```

```
<record>
```

```
<row>
```

```
<source_ip>202.241.206.5</source_ip>
```

```
<count>54</count>
```

```
<policy_evaluated>
```

```
<disposition>none</disposition>
```

```
<dkim>fail</dkim>
```

```
<spf>fail</spf>
```

```
</policy_evaluated>
```

```
</row>
```

```
<identifiers>
```

```
<header_from>support.transware.co.jp</header_from>
```

```
</identifiers>
```

```
<auth_results>
```

```
<spf>
```

```
<domain>delivery.qualitia.co.jp</domain>
```

```
<result>none</result>
```

```
</spf>
```

```
</auth_results>
```

```
</record>
```

```
</feedback>
```

送信元IPアドレス

= 社内から送信する全メールが
経由するメールサーバ

ヘッダのFROMドメイン

ヘッダFROMのドメインが
support.transware.co.jp
のメールを
社内からgoogleに
送信または転送しているらしい

※ メールアドレスがわかるわけではない

➡ rufレポートがあればわかる