メールサーバ管理者のみ知る話

野々垣裕司

JPAAWG 7th LT

自己紹介

KEYTEC合同会社

野々垣 裕司（ののがき ひろし）

サーバ管理者:1996年から
IPv6運用:　2001年から
SMTP認証:　2001年から
SPF運用:　2012年から
DKIM運用:　2019年から
DMARC運用:　2019年から
MTA-STS運用: 2021年から

SPF

- 送信元のIPアドレスで判断する
- MAIL FROMのホスト名、HELOのホスト名

```
keytec.jp.    86400   IN    TXT    “v=spf1 include:spf.keytec.jp -all”
spf.keytec.jp. 86400   IN    TXT    "v=spf1 ip6:2001:f58:2003:1::/126 ip6:2001:f58:2003:1::a
ip4:202.124.214.192/30 ip4:202.124.214.202 ~all"
```

- -all Fail　　一致していないとREJECT
- ~all Softfail　　信頼できないが受信する
- DNS参照は最大10回まで。
- 設定したら必ず確認しましょう。

大企業でも間違えるSPF

```
@       IN A TXT  “v=spf1 ip4:192.0.2.10/24 ~all”
@       IN A TXT  “v=spf1 ip6:2001:db8::/32 ~all”
```

SPF Permanent Errorとなっていた
全て私が世界中で一番最初に発見したらしい(Xにて)

2021年6月 某グローバル企業A

2021年9月 某通信会社B

2022年6月 某グローバル企業C

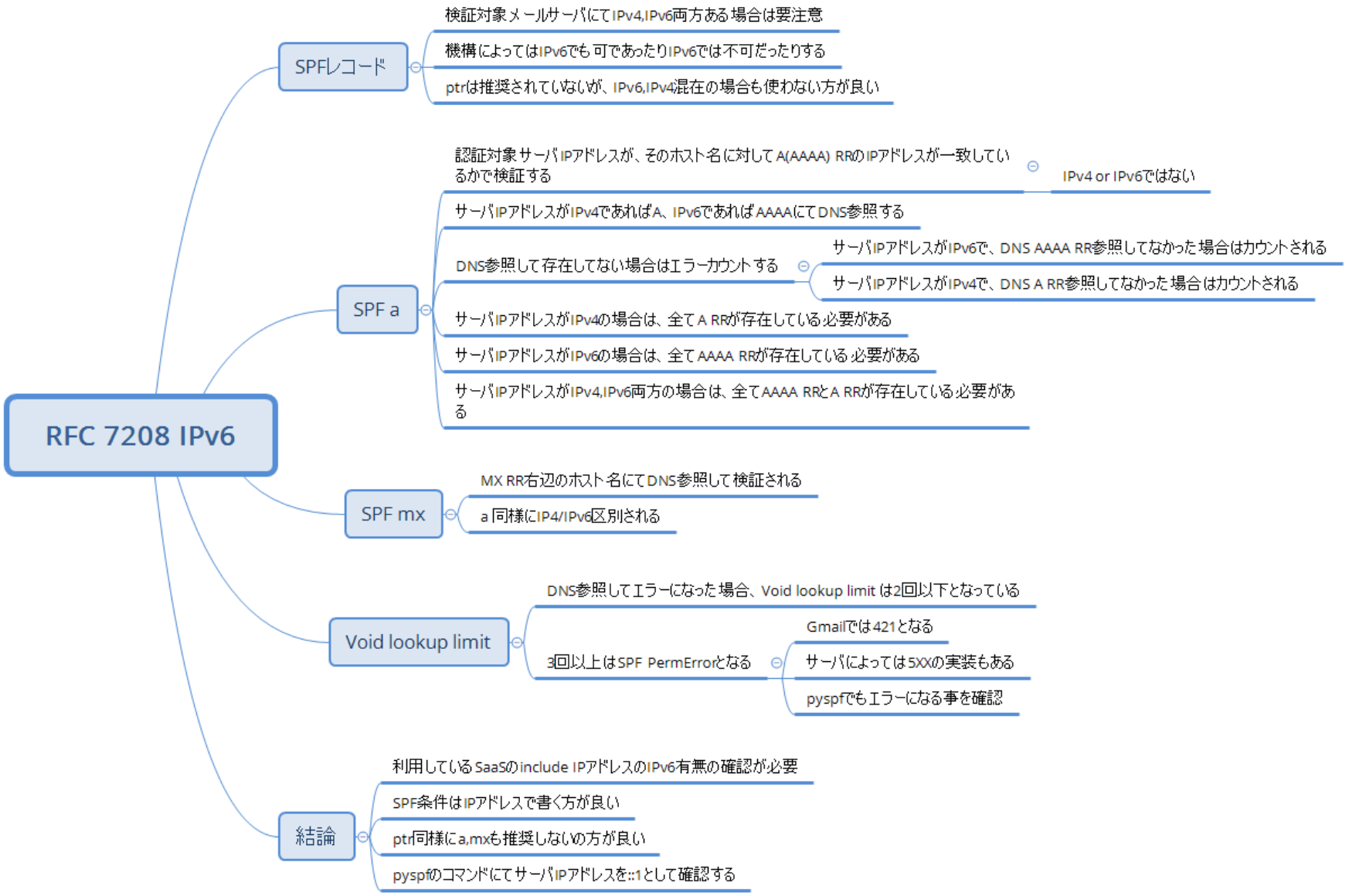
2024年8月 某通信会社D

SPF IPv6,IPv4混ぜるな

ドメイン名 example.jp

```
@       IN MX 300 mx.example.jp.
        IN A TXT  “v=spf1 a:m41.example.jp a:m42.example.jp a:m43.example.jp ”
         “a:m61.example.jp a:m62.example.jp a:m63.example.jp a:mx.example.jp -all”
m41     IN A 192.0.2.1
m42     IN A 192.0.2.2
m43     IN A 192.0.2.3
m61     IN AAAA 2001:db8::1
m62     IN AAAA 2001:db8::2
m63     IN AAAA 2001:db8::3
mx      IN A 192.0.2.10
        IN AAAA 2001:db8::10
```

これでは正しく機能しませんよ!!!


RFC 7208 IPv6
SPFレコード
検証対象メールサーバにてIPv4,IPv6両方ある場合は要注意
機構によってはIPv6でも可であったりIPv6では不可だったりする
ptrは推奨されていないが、IPv6,IPv4混在の場合も使わない方が良い
SPF a
認証対象サーバIPアドレスが、そのホスト名に対してA(AAAA) RRのIPアドレスが一致しているかで検証する
IPv4 or IPv6ではない
サーバIPアドレスがIPv4であればA、IPv6であればAAAAにてDNS参照する
DNS参照して存在してない場合はエラーカウントする
サーバIPアドレスがIPv6で、DNS AAAA RR参照してなかった場合はカウントされる
サーバIPアドレスがIPv4で、DNS A RR参照してなかった場合はカウントされる
サーバIPアドレスがIPv4の場合は、全てA RRが存在している必要がある
サーバIPアドレスがIPv6の場合は、全てAAAA RRが存在している必要がある
サーバIPアドレスがIPv4,IPv6両方の場合は、全てAAAA RRとA RRが存在している必要がある
SPF mx
MX RR右辺のホスト名にてDNS参照して検証される
a同様にIP4/IPv6区別される
Void lookup limit
DNS参照してエラーになった場合、Void lookup limitは2回以下となっている
3回以上はSPF PermErrorとなる
Gmailでは421となる
サーバによっては5XXの実装もある
pyspfでもエラーになる事を確認
結論
利用しているSaaSのinclude IPアドレスのIPv6有無の確認が必要
SPF条件はIPアドレスで書く方が良い
ptr同様にa,mxも推奨しないの方が良い
pyspfのコマンドにてサーバIPアドレスを::1として確認する

DMARC

- SPFとDKIMの結果で判断する
  - TXTレコード v=DMARC1 記述する (Fromヘッダのメールアドレス)
    - p=none なにもしない(実態)
    - p=quarantine 隔離
    - p=reject 拒否
- DMARCレポート
  - 受信先からDMARC認証結果レポートを送ってくれる(受信報告書)
  - rua=メールアドレス にて記述する

```
_dmarc.keytec.jp.    3600  IN    TXT    "v=DMARC1; fo=1; p=reject; aspf=s;
rua=mailto:postmaster_rua@keytec.jp"
```

DMARC

DMARCレポート

受信先からDMARC認証結果レポートを送ってくれる

- 正しく動作しているか確認できる
- 詐称や改ざんされたメールがどこから発信されているかわかる


```
<?xml version="1.0" encoding="UTF-8"?>
<feedback>
  <report_metadata>
    <org_name>kits.ne.jp</org_name>
    <email>postmaster_rua@manage.kits.ne.jp</email>
    <report_id>keytec.jp:1567467023</report_id>
    <date_range>
      <begin>1567380623</begin>
      <end>1567467023</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>keytec.jp</domain>
    <adkim>r</adkim>
    <aspf>s</aspf>
    <p>reject</p>
    <sp>reject</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
    <identifiers>
      <header_from>keytec.jp</header_from>
    </identifiers>
    <auth_results>
      <spf>
        <domain>keytec.jp</domain>
        <result>pass</result>
      </spf>
      <dkim>
        <domain>keytec.jp</domain>
        <result>pass</result>
      </dkim>
    </auth_results>
  </record>
```

困ったDMARCレポート受信

- DMARCレポートがSPF=Noneにて送られてくる。
- DMARC導入しているであれば、DMARC=Passで送るべきですよね。

困ったDMARCレポート送信1

- 溢れちゃった

```
                    The mail system

net>: cannot update mailbox /home/.mail for user
      error writing message: File too large

-------------------------------------------------------

Reporting-MTA: dns; .net
X-Postfix-Queue-ID: 185A22C1FBA
X-Postfix-Sender: rfc822; postmaster rua@manage.kits.ne.jp
Arrival-Date: Sat, 24 Aug 2019 05:19:01 +0600 (BDT)

Final-Recipient: rfc822; net
Original-Recipient: rfc822; net
Action: failed
Status: 5.2.2
```

困ったDMARCレポート送信2

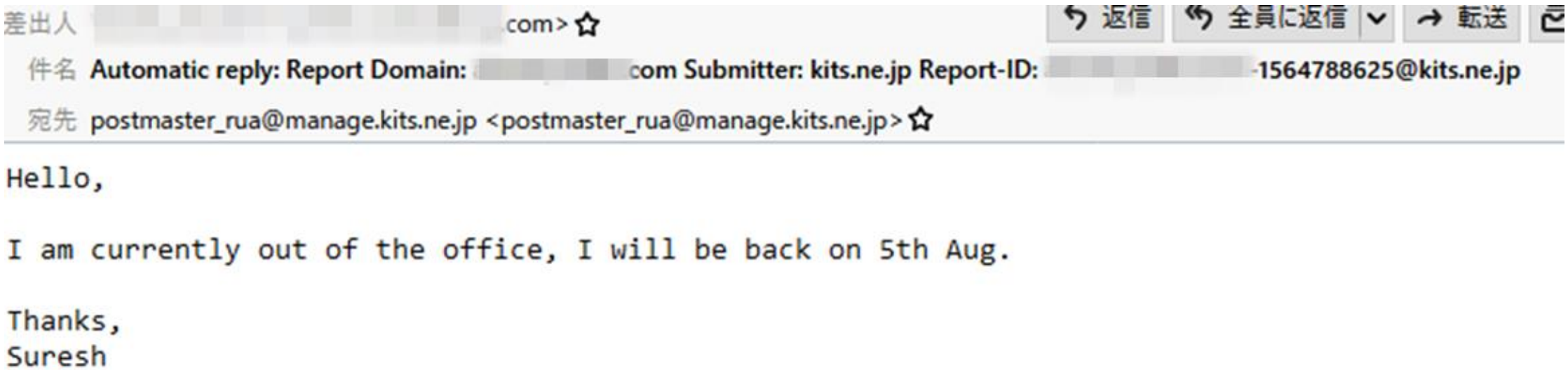
- あんた誰?

@ IN TXT
"v=DMARC1; p=quarantine; rua=mailto:postmaster@example.com"

```
[redacted]: host aspmx.l.google.com[74.125.203.27] said: 550-5.1.1 The
email account that you tried to reach does not exist. Please try 550-5.1.1
double-checking the recipient's email address for typos or 550-5.1.1
unnecessary spaces. Learn more at 550 5.1.1
https://support.google.com/mail/?p=NoSuchUser a190si16264461pge.88 - gsmtp
(in reply to RCPT TO command)
```

困ったDMARCレポート送信3

- 長期休暇中です


差出人 [redacted]com> ☆
返信 全員に返信 転送
件名 Automatic reply: Report Domain: [redacted]com Submitter: kits.ne.jp Report-ID: [redacted]-1564788625@kits.ne.jp
宛先 postmaster_rua@manage.kits.ne.jp <postmaster_rua@manage.kits.ne.jp> ☆

Hello,

I am currently out of the office, I will be back on 5th Aug.

Thanks,
Suresh

基本に振り返りましょう

- 設定変更したらちゃんと動作確認しましょう。
- DNSが正しく設定できていないと、送信ドメイン認証も正しく設定できる訳がない。間違いに気づかない。
- DNSもMTAもSPFもDKIMも全て正しく設定できないと、DMARCの運用なんてとても無理。
- RFC逸脱も意外と多いので確認しましょう。

ありがとうございました