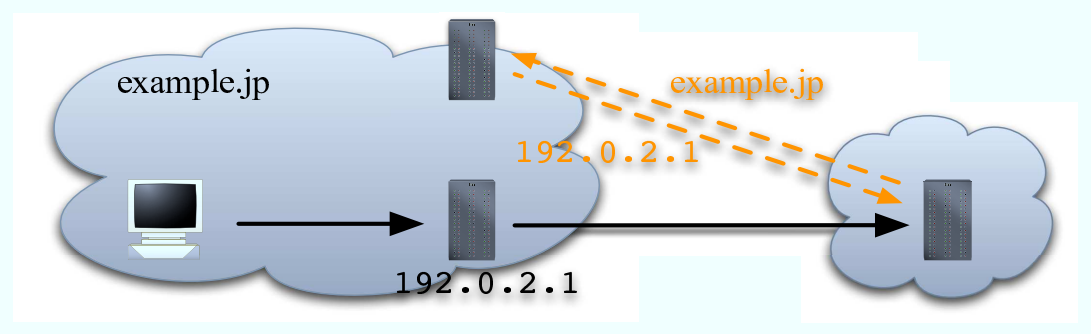
SPF と Sender ID

山本和彦
(株)インターネットイニシアティブ
kazu@iij.ad.jp

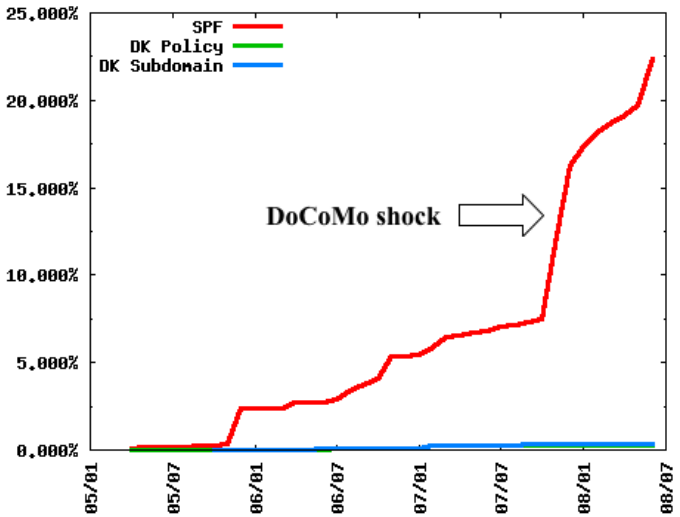
SPF の動作原理



- 送信側
  - DNS で送信サーバの IP アドレスを宣言 (MX の逆)
- 受信側
  1) SMTP コネクションから相手の IP アドレスを得る
  2) SMTP MAIL FROM からドメイン名を得る
     - エラーメッセージの場合は、SMTP EHLO からドメインを得る
  3) ドメイン名から SPF RR を検索して IP アドレスを得る
  4) 1) と 3) を比較
     - 合致すればドメイン名は正当
     - 合致しなければドメイン名は不正

SPF の送信側の普及状況

- .JP 以下での2008年6月現在の普及率は 22.38%
  - # SPF RR ÷ # MX RR × 100
    - http://member.wide.ad.jp/wg/antispam/stats/index.html.ja
    - WIDE と JPRS の共同研究



DoCoMo ショック

- 2007年9月11日のプレスリリース
  - http://www.nttdocomo.co.jp/info/news_release/page/070911_00.html
- 2007年11月1日より開始

  お客様が、「全て拒否する」と設定された場合には、
  DNSサーバに必要な対処を行っていないISP事業者様や
  企業様などからのメールは認証ができないため
  受信できません。

  - http://www.nttdocomo.co.jp/service/mail/imode_mail/notice/sender_id/
- 2007年11月の計測で急増
  - 10月末に慌てて SPF RR を設定した？

SPF RR の例

- example.jp ゾーン

```
@ IN SOA   ns.example.jp. root.example.jp. ( ... )
  IN MX 10 mx.example.jp.
  IN TXT   "v=spf1 +ip4:192.0.2.1 -all"
```

- SPF RR は普及していないので、
  今は TXT RR で代用
  - `v=spf1` で他の TXT RR と区別

SPF RR の書式

- 送信サーバを列挙

```
"v=spf1 +ip4:192.0.2.1 ~all"
"v=spf1 +ip4:192.0.2.1 +ip4:192.0.2.2 ~all"
"v=spf1 +ip4:192.0.2.0/24 -all"
"v=spf1 +a +mx -all"
"v=spf1 -all"
```

- 送信サーバの限定子
  - "+" -- pass (ドメイン名は正当)
  - 省略したら "+" になる
- `all` の限定子
  - `"-all"` -- fail (ドメイン名は不正)
  - `"~all"` -- softfail
    - いきなり `"-all"` だと怖い人は `"~all"`
    - http://www.iajapan.org/anti_spam/portal/Operation/Suggestion/sugg_a01_01.html
  - `"?all"` -- SPF RR は無いものとして扱う
    - JEAG (Japan Email Anti-Abuse Group) は推奨していない
  - `"+all"` と書くと受信側で不正とみなされるかも...

IP アドレスの直書き

- IPv4 アドレス
  `"v=spf1 +ip4:192.0.2.1 +ip4:192.0.2.2 ~all"`
  - `ipv4` ではありません！
- IPv6 アドレス
  `"v=spf1 +ip6:2001:DB8::1 +ip6:2001:DB8::2 -all"`
  - `ipv6` ではありません！
- IPv4 アドレスのブロック
  `"v=spf1 +ip4:192.0.2.0/24 -all"`
  - `.0` は省略できません！
- IPv6 アドレスのブロック
  `"v=spf1 +ip6:2001:DB8::/64 -all"`
- 間違いや DNS の負荷を減らすために、
  この範囲で設定しましょう

間接参照

- A RR の向いている IP アドレス
  ```
  "v=spf1 +a:example.jp -all"
  ```
- MX RR の向いている IP アドレス
  ```
  "v=spf1 +mx:example.jp ~all"
  "v=spf1 +a +mx -all"
  ```
- 他のゾーンの設定を使う
  ```
  "v=spf1 include:example.com include:example.org -all"
  ```
  - 参照先の pass のみ使われる
  - include ではなく、if-pass という名前にするべきだった
- 他のゾーンへ向け直す
  ```
  "v=spf1 redirect:example.com"
  ```
  - `all` がないことに注意
- 参照先が存在することを確かめましょう
  - include, redirect をループさせないようにしましょう

ワイルドカード

- ワイルドカード SPF RR は非推奨
- 書く場合は、2回書く

```
example.jp.        MX   10        sub.example.jp
example.jp.        TXT  "v=spf1 a:sub.example.jp -all"

*.example.jp.      MX   10        sub.example.jp
*.example.jp.      TXT  "v=spf1 a:sub.example.jp -all"

sub.example.jp.    A    192.0.2.1
sub.example.jp.    MX   10        sub.example.jp
sub.example.jp.    TXT  "v=spf1 a:sub.example.jp -all"

*.sub.example.jp.  MX   10        sub.example.jp
*.sub.example.jp.  TXT  "v=spf1 a:sub.example.jp -all"
```

  - sub.example.jp には *.example.jp の設定が適応されない

メールを出さないドメイン

- メールを出さないドメインこそ
  SPF RR を書きましょう！

```
"v=spf1 -all"
```

確認！確認！確認！

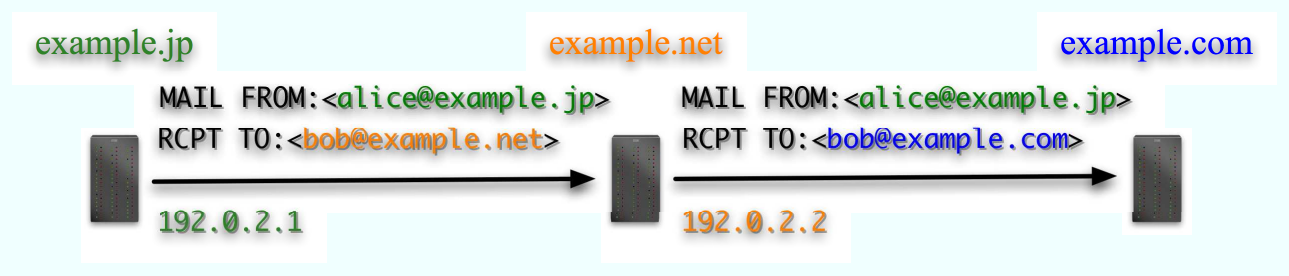
- SPF RR の書式の生成
  - http://www.openspf.org/
- SPF RR の書式の確認
  - http://www.kitterman.com/spf/validate.html
- spfquery で動作確認
  - http://search.cpan.org/dist/Mail-SPF/bin/spfquery
  - ドメイン名と IP アドレスを与えて、どう評価されるかを検査

```
% spfquery --id user@example.jp --ip 192.0.2.1
Received-SPF: pass
```

  - 参照先がないなどのエラーが見つかることもある
- メールで動作確認
  - `spf-test@openspf.org`
  - エラーメールとして SPF 検査の結果を返してくれる

SPF の受信側

- 受信側には、SPF は普及していない
- 転送問題



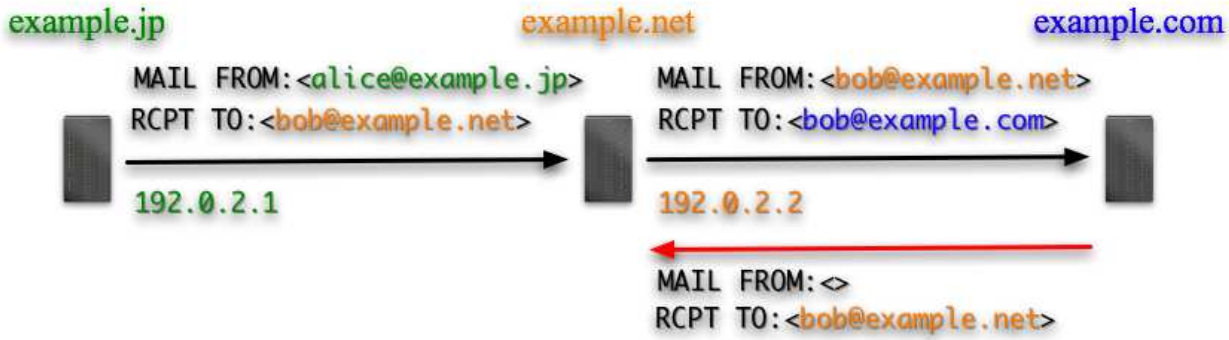
  - SMTP MAIL FROM は変わらない
  - IP アドレスは変わる
  - SPF による認証結果は、softfail や fail になる

転送問題の解決

1) ホワイト・リスト

- DoCoMo 方式
- 受信側のみで対応可能

2) SMTP MAIL FROM の書き換え



- http://www.iajapan.org/anti_spam/portal/Operation/Suggestion/sugg_a02_01.html

3) Sender ID

- 転送の際に Resent-From: フィールドをヘッダに付加
  - Resent-From: bob@example.net

Sender ID、覚えていますか？

- Sender ID は SPF のスーパーセット
  - SMTP MAIL FROM からドメイン名 (mfrom)
  - メールのヘッダからドメイン名 (pra)
- Purported Responsible Address (PRA)
  - Resent-Sender:
  - Resent-From:
  - Sender:
  - From:
- DNS の書式
  - 送信サーバの宣言方法は SPF と同じ
  - spf2.0/mfrom,pra
    - mfrom でチェックしても、PRA でチェックしても OK
  - v=spf1 は spf2.0/mfrom,pra と解釈される

Sender ID と特許問題

- 2004 年当時の MS の声明

  ライセンスが、Sender ID Framework の PRA チェック手段を使用して電子メールを確認する組織 (ISP、大企業) に関連する場合だけ、ライセンスを取得する必要があることに注意することが重要です。

  - http://download.microsoft.com/download/d/c/5/dc59cbef-72c4-4f64-8830-81d1c01dfc56/senderid_faq.pdf

- 2006年12月から OSP(Open Specification Promise)

  No one needs to sign anything or even reference anything.

  - http://www.microsoft.com/interop/osp/default.mspx

  - RFC 4406 - Sender ID: Authenticating E-Mail
  - RFC 4407 - Purported Responsible Address in E-Mail Messages
  - RFC 4408 - Sender Policy Framework: Authorizing Use of Domains in "Mail From"

設定間違いの例

- 見たことのある間違い
  - × v=spf
  - × v=spf2
  - × v=spf2.0
- 正しくは
  - ○ v=spf1
  - ○ spf2.0/mfrom,pra
- 一般的な注意
  - TXT RR の最大の長さは 255
    - 255 を越える場合は、文字列の連結を使う
  - DNS query の結果は 512 バイトに収まらないといけない

まとめ

- SPF RR を書きましょう
- v=spf1 のみで十分です
- "all" の限定詞は、できれば "-all"、
  せめて "~all" にしましょう
  - "?all" は止めましょう
- Web だけのドメインは、"-all" にしましょう