

今 おさえておきたい
ドメイン認証技術

Hirohisa Yamaguchi

ネットエージェント株式会社

2009-06-13

発表者について



- ネットエージェント株式会社

- <http://www.netagent.co.jp>

- 研究開発部



- 関西 *BSD ユーザ会 (K*BUG)

- <http://www.kbug.gr.jp>

発表者について

- ✧ FreeBSD のパッケージメンテナ ([not commiter](#))
 - ✧ mail/dkim-milter
 - ✧ mail/enma
 - ✧ mail/milter-manager (申請中)
 - ✧ mail/batv-milter (申請中)

はじめに

Q. 送信ドメイン認証で迷惑
メールはなくなりますか？

A. いいえ

Q. じゃあ、
送信ドメイン認証は
いらない子？

A. いいえ

ドメイン認証は
受信側より
送信側の方に
導入効果がみこめます

送信ドメイン認証のしくみ

あやしいメールが
多し

せめて、自サイト
から出る分ぐらいい
しっかりさせよう

今日のキーワード

☛ SPF / Sender ID

☛ DKIM / ADSP

☛ Authentication-Results

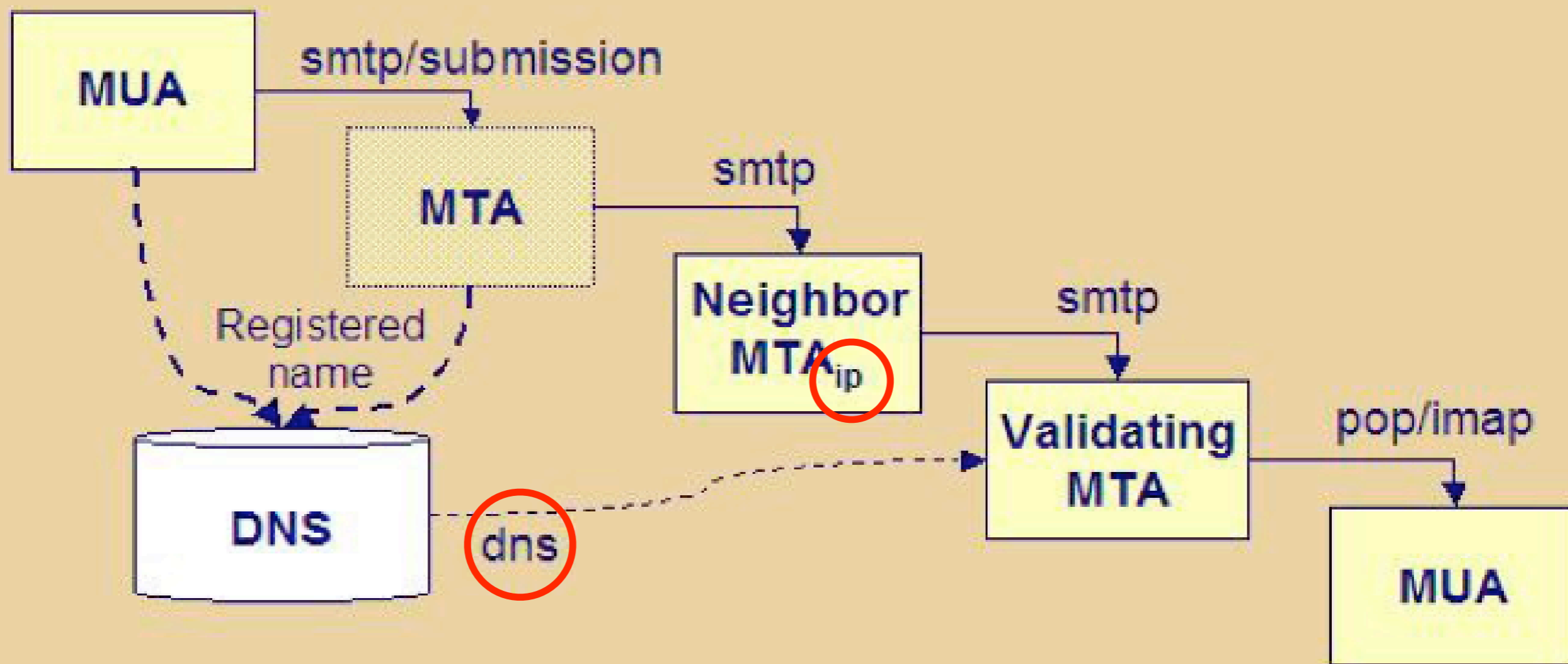
SPF / SIDF

- ☛ Sender Policy Framework (SPF)

 - ☛ rfc 4408

- ☛ Sender ID Framework (SIDF)

 - ☛ rfc 4406



経路による認証

Sender ID

と

SPF

の違いは？

- ♪ SPF は、From (not From:) または HELO/EHLO のドメインから
- ♪ Sender ID は、謂わば上位互換
さらに Purported Responsible Address (PRA: rfc4407) で判断することもできる
 - ♪ Resent-Sender: → Resent-From: →
Sender: → From:

SPF/SIDF 導入

- ☛ DNS RR を追加する

```
example.jp      TXT  "v=spf1 +mx +ip4:192.0.2.3 -all"  
example.jp      MX   mx.example.jp  
mx.example.jp  A    192.0.2.2
```

- ☛ 左から評価する、ホワイトリスト的構文
- ☛ 明記していないアドレスを、-all, ~allで表す

SPF の弱点

♡ 転送に弱い

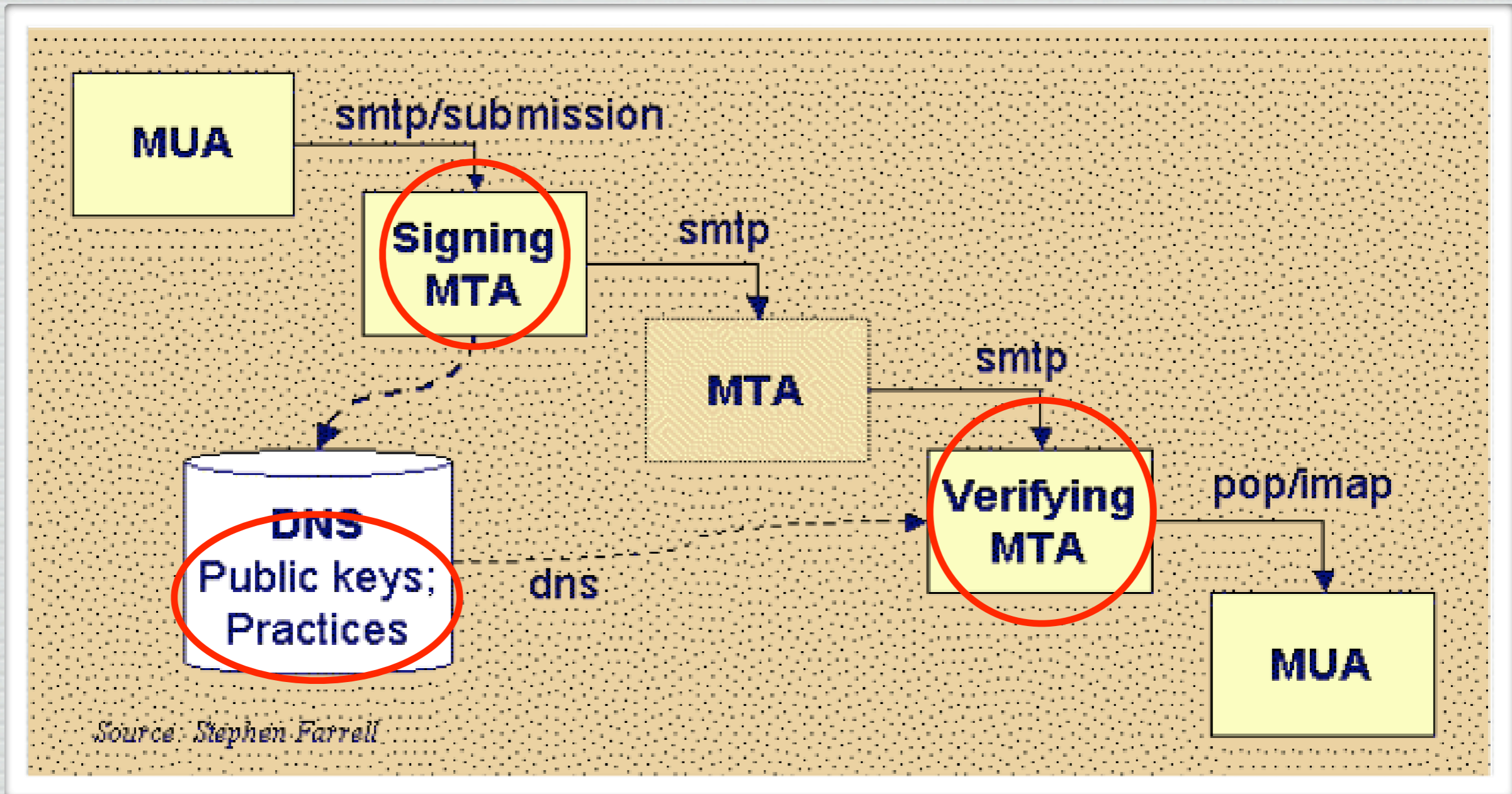
♡ たとえば ~/.forward

転送対策

- ☛ SMTP の SUBMITTER (rfc4405) を使う
- ☛ HELO/EHLO を使う(無視されるかも)
- ☛ PRA の活用(Sender ID)
- ☛ 転送時にアドレスを書き換える
 - ☛ SRS, VERP, BATV
- ☛ DKIMを併用する

DKIM / ADSP

- Domain Keys Identified Mail (rfc4871)
- Author Domain Signing Practices
(draft-ietf-dkim-ssp)
- 他にも rfc4871-update, overview,
deployment, reporting などが作業中



デジタル署名による認証

DKIM の特徴

- ✧ 主要ヘッダやボディが変更されなければ、経路は気にしない
 - 転送に強い
 - メイリングリストなど、ヘッダなどに変更の加わるものには弱い

DKIM 導入

- ✧ 署名機構 (signer) を MSA(もしくは自サイトないのいずれかのMTA)に設置し、署名要件を決める
- ✧ 鍵ペアを作成し、DNS サーバに公開鍵を登録する (複数登録可)
- ✧ 署名をテストする
 - ✧ <http://testing.dkim.org/reflector.html>

ADSP 導入

- ✧ DKIM 署名機構が実装できたら送信するメッセージに付与する署名について扱いを決める

 - ✧ discardable → all → unknown

- ✧ 決めたら

 - `_adsp._domainkey.example.jp TXT "dkim=all"`

 - のように登録する

DKIM 全然聞かない？

- ♪ rfc4871 以外、全部 draft なので様子見気配
 - ♪ とはいえ SPF / Sender ID は experimental のまま放置のような気も
- ♪ ここ半年ぐらいで急速に固まってきているので、そろそろ検討してもいいのでは

Authentication-Results:

- ✧ rfc5451 (April 2009)
- ✧ 各種認証の結果を示す

**Authentication-Results: mx.example.jp
spf=pass smtp.mailfrom=trusted@example.com**

- ✧ どこでついたかが重要 && 自サイトでつけたものしか信用できない (Received:と同様)
- ✧ Received-SPF: (rfc4408)はだんだん使われなくなるかも

まとめ

- ❧ SPF / Sender IDは送出ホストを宣言
- ❧ DKIM は自サイトから出たことを証明
- ❧ 送信ドメイン認証への対応は送出側から