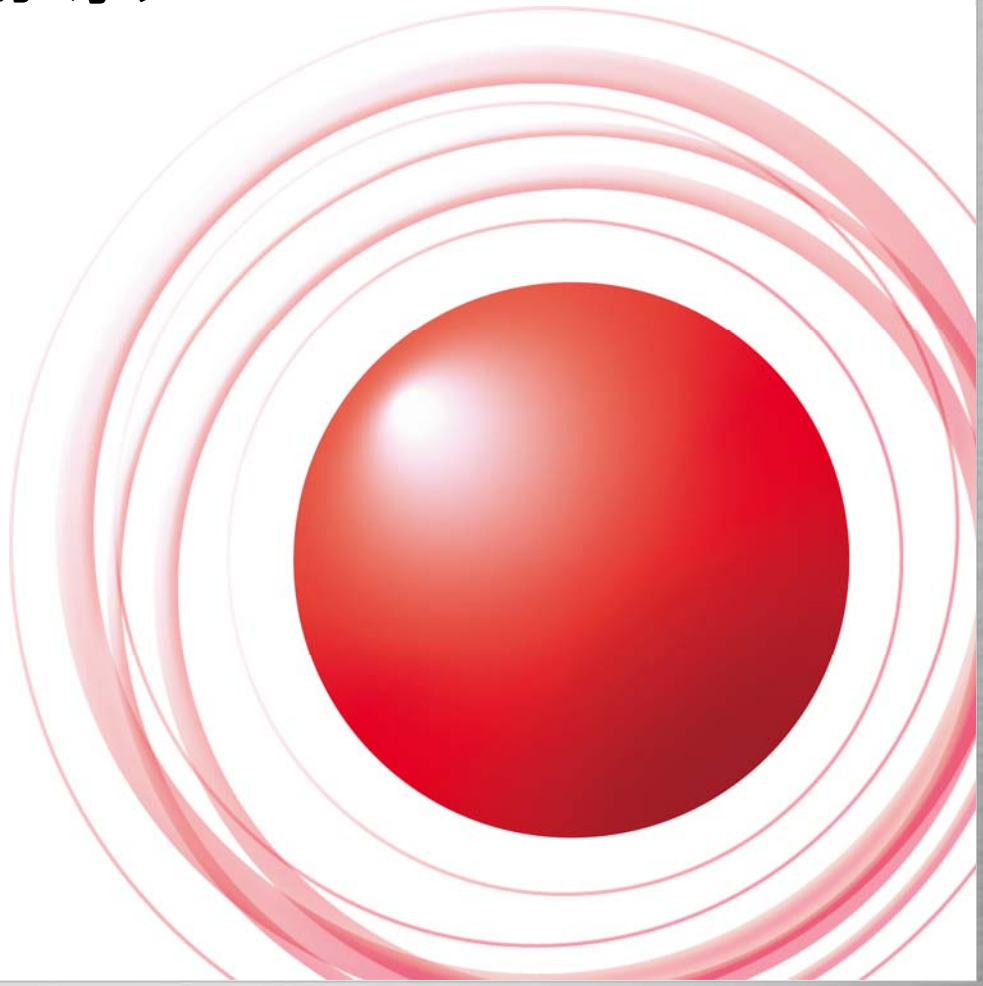
Internet Week 2011

送信ドメイン認証 ENMA による受信側導入

IIJ Internet Initiative Japan



2011/11/30

株式会社インターネットイニシアティブ
鈴木高彦

Ongoing Innovation

ENMA とは

- 送信ドメイン認証の検証をおこなう milter
  - MTA (Sendmail, Postfix, その他) と連携するモジュール
- 受信したメールに対して認証処理をおこない、結果をヘッダとして挿入
  - その他のアクションはとらない

認証結果ヘッダの例

```
Authentication-Results: mx.example.jp;
    spf=pass smtp.mailfrom=username@example.com;
    sender-id=pass header.From=username@example.com;
    dkim=pass header.i=@example.com;
    dkim-adsp=pass header.From=username@example.com
```

Agenda

- ENMA の紹介
- ENMA の導入
- 送信ドメイン認証と DNS
- おまけ
- まとめ

ENMA の紹介

ENMA のコンセプト

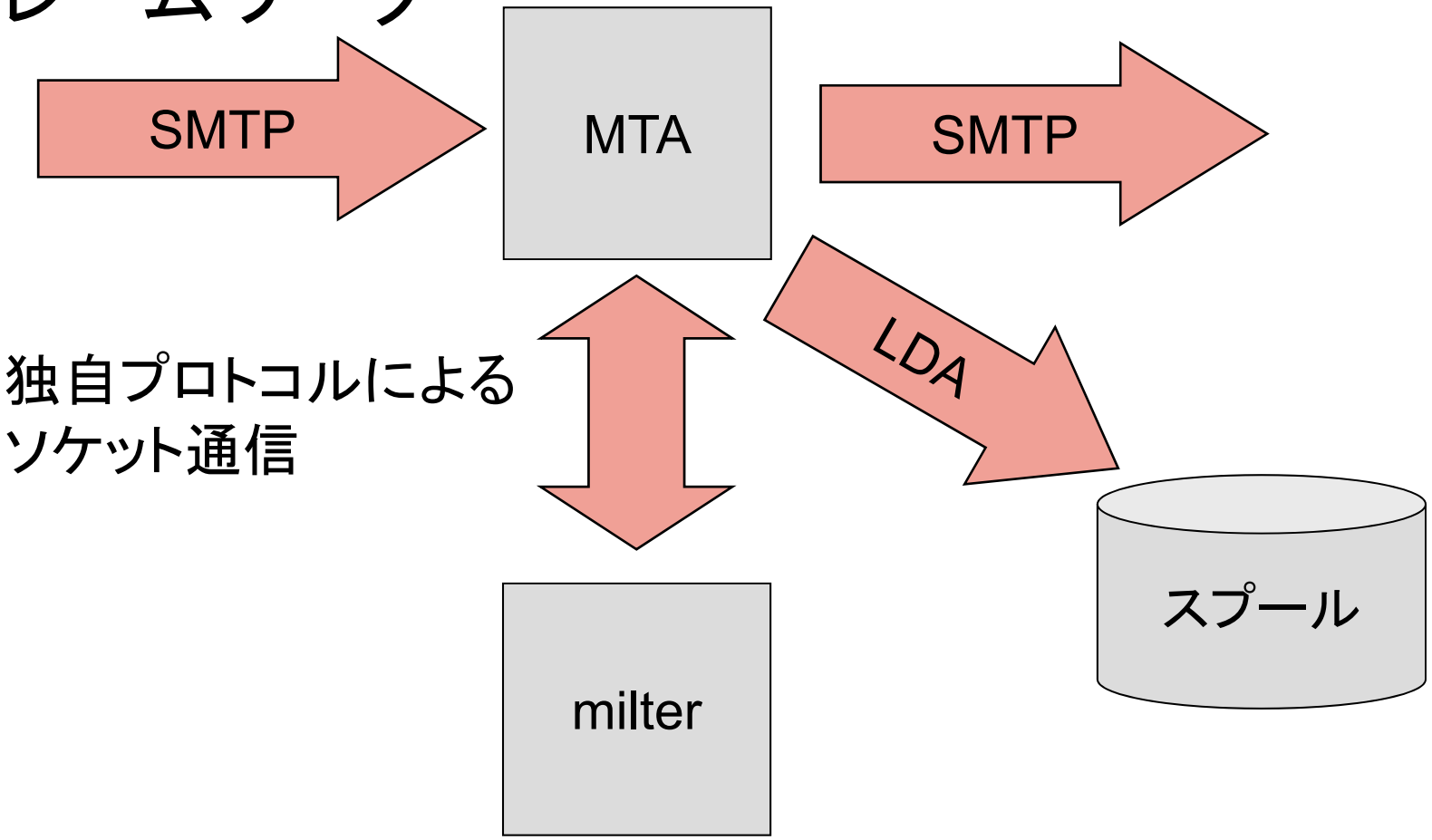
- 手軽
  - 導入手順がシンプル
  - 入れるだけで主要な送信ドメイン認証技術に一通り対応
  - 導入してからも手間がかからない
- 安定動作
  - 最も過酷なエッジでの動作に耐えうる堅牢性
    - 対大量のコネクション
    - 対汚いコネクション

ENMA がオススメな理由

- オールインワン
- 豊富な使用実績
  - 安定稼働
- SPF　検証処理をおこなうオープンソースソフトウエアは少ない
  - 実は他の選択肢は多くない
- BSD ライセンス

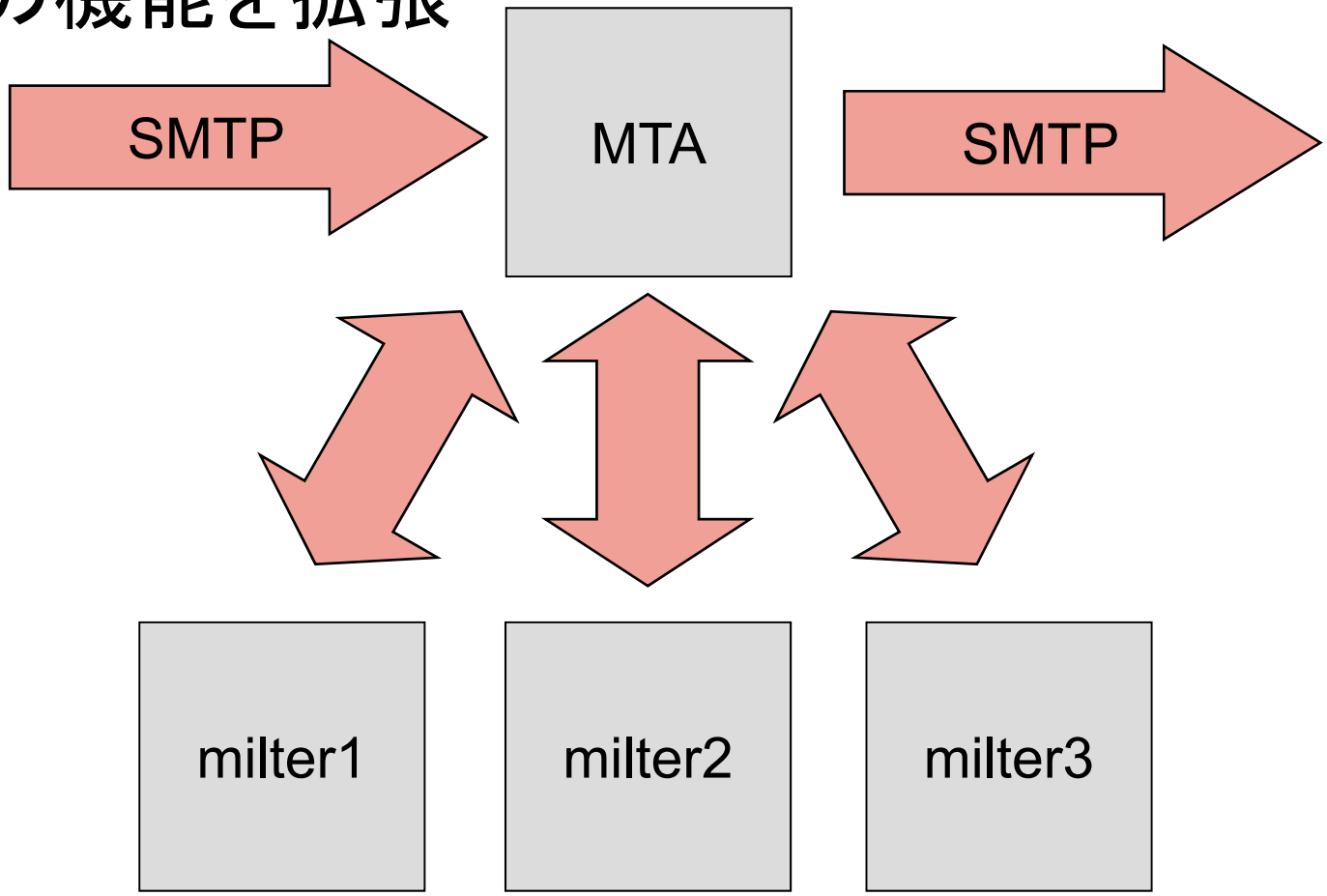
milter 概要

- MTA の機能を自在に拡張できる強力なフレームワーク



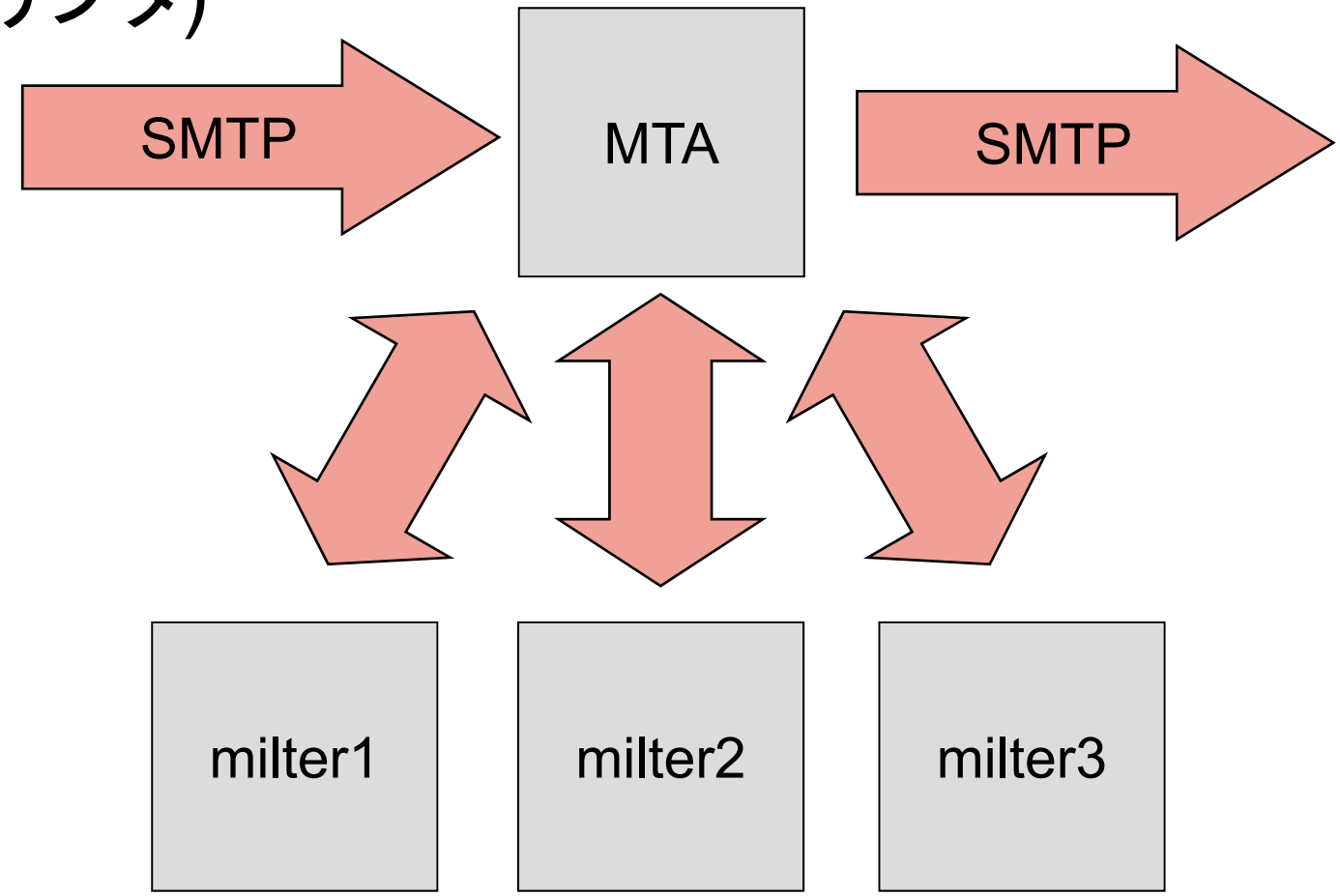
milter の特長

- 既存の系に milter を追加するだけで MTA の機能を拡張



milter の注意点

- milter が増えると MTA は辛い (I/O, ディスクリプタ)



オールインワンのメリット

- milter インスタンスの数を最小限に抑制
  - エッジの MTA にとって無視できない問題
- 導入が容易
  - 1回の作業で複数の送信ドメイン認証技術を導入できる
- Authentication-Results ヘッダをまとめられる
- (将来的に) SPF+DKIM など複数の認証結果を参照したアクションをとりやすい

使用実績

- 2008年夏頃から IIJ の各種メールサービスで稼働
  - 膨大、かつ汚い SMTP トラフィックで鍛錬
  - 最初から安定していたわけではない
  - 運用環境と開発者の距離が近いので不具合の対応がしやすい
- いくつかの国内大手 ISP や地方 ISP で使用しているという報告も頂いています

ENMA 1.2.0

- 2年ぶりのバージョンアップ
- 変更点
  - DKIM の RFC の更新 (4871, 5672 → 6376) に追従
  - デフォルトのリゾルバを変更
  - Bug fix いくつか
  - 内部構造を整理

DKIM RFC の更新

- 2011年9月 RFC6376 が発行
  - RFC4871, 5672 のマージ
  - 公開鍵レコードの “g=” タグが廃止
- デフォルトでは RFC6376 に従って “g=” タグを評価しないよう変更
  - 設定項目 “dkim.rfc4871_compatible” を “true” にすることで RFC4871 に従って “g=” タグを評価するよう設定可能

リゾルバ

- ENMA 1.2.0 では configure 時にリゾルバを選択可能
  - libbind (1.1.0 までのデフォルト)
  - libresolv (実は使用可能)
  - ldns (1.2.0 からのデフォルト)
- 送信ドメイン認証は DNS に大きく依存
- DNS ルックアップの機会は多く、リゾルバはとても重要なコンポーネント

リゾルバ

- libbind
  - bind に付属 (現在は分離) の定番リゾルバライブラリ
    - http://www.isc.org/software/libbind
  - libresolv と元は同じ
  - 幅広い OS で利用可能
  - 動作は非常に安定
  - 良くも悪くも枯れている
  - libbind9 と勘違いする人が続出
    - libbind9 は bind9 用の全く別のライブラリ

リゾルバ

- libresolv
  - いくつかの OS で libc に取り込まれている、ある意味標準のリゾルバライブラリ
  - OS によって仕様が独自に拡張されていたり、挙動が異なったりする
    - これまで libbind を採用していた最大の理由
  - ENMA での利用は非推奨
    - OS 毎の仕様・挙動の差を正確に把握しきれないため
    - 腕に覚えのある人が自己責任で使えるようにはしてある
      - ./configure --with-resolver=libresolv
      - ドキュメント中でも使用可能な旨にはわざと触れていない
      - サポートはしない

リゾルバ

- ldns
  - NSD/unbound でおなじみの NLnet Labs 製
  - NSD/unbound にも組み込まれている
  - 整理された使いやすいプログラミング I/F
  - 機能が豊富
  - DNSSEC 対応
  - BSD ライセンス
  - アクティブにメンテナンスされている

ENMA の導入

ENMA 導入のポイント

- ENMA のビルド
- ENMA の導入・設定
- MTA の設定

ENMA のビルド

- 依存するライブラリ
  - OpenSSL (libcrypto)
  - ldns (or libbind)
  - libmilter (sendmail に同梱)
- 大規模に使うのでなければバイナリパッケージで十分
  - CentOS 用の RPM パッケージを用意

libmilter ビルドのポイント

- confENVDEF に以下を追加:
  - MTA が受けた IPv6 接続を扱う
    -DNETINET6=1
  - 1024 本以上の接続を同時に受ける
    -DSM_CONF_POLL=1
  - libmilter に libbind を使わせる際に指定
    -DNEEDSGETIPNODE=0
- ENMA のパッケージにサンプルを同梱したので参考にしてください

ENMA の設定

- enma.conf
  - MTA からの接続を受けるソケット
    milter.socket: inet:10025@127.0.0.1
  - Authentication-Results ヘッダで使用する識別子
    authresult.identifier: mx.example.jp
  - 認証処理を除外するアドレスレンジ
    common.exclusion_addresses: 192.0.2.0/24
    - 送受信を1つの MTA で処理するシステムで、イントラネットからインターネットに出て行くメールを認証処理の対象外とする (Authentication-Results ヘッダを付けないようにする)

ENMA の設定

- PID ファイル用ディレクトリの作成

  $ mkdir /var/run/enma
  $ chown daemon:daemon /var/run/enma
  (パスやユーザー/グループなどは要件に応じて変更)

- リゾルバの設定
  - /etc/resolv.conf (ldns, libbind とも)
    - “nameserver” を DNS キャッシュサーバに向けておく

MTA 設定のポイント

- Sendmail の場合
  - sendmail.mc

```
INPUT_MAIL_FILTER(`enma', `S=inet:10025@127.0.0.1')
```

  - enma.conf (Sendmail 8.13 以前の場合のみ)

```
milter.sendmail813: true
```

MTA 設定のポイント

- Postfix の場合
  - main.cf

    smtpd_milters = inet:127.0.0.1:10025
    milter_protocol を調整 (うまく動かない場合)

  - enma.conf

    milter.postfix: true

どの MTA で検証するか

- 多段構成のメールシステムの場合はエッジ
  - 最もインターネット側の MTA
  - 最も負荷が高く、最も汚れた接続を受け付ける MTA

送信ドメイン認証と DNS

送信ドメイン認証の DNS への依存

- 大事なことはみんな DNS に書いてある
  - SPF レコード
  - DKIM 公開鍵
  - DKIM-ADSP レコード
- DNS が信頼できない環境下では送信ドメイン認証も信頼できない
- 送信ドメイン認証における DNS ルックアップでは、DNSSEC は必須

送信ドメイン認証における DNS ルックアップの考察

- 検証処理は DNS ルックアップの回数が多い
- SPF/SIDF
  - 最大 111 query/message
- DKIM
  - 1 query/signature
  - 最大 10 signature/message
    - 最大値は設定で変更可
- DKIM ADSP
  - 1 query/message

送信ドメイン認証における DNS ルックアップの考察

- ENMA で1通検証する際に発生する最大 DNS ルックアップ数
  - 233 query/message
    - SPF, SIDF, DKIM, DKIM-ADSP 全て ON
    - DKIM-Signature を10個まで検証
    - 最大限の悪意を持ったメール
- 悪意を持ったメールを作成すると大量の DNS クエリを発生させられる

送信ドメイン認証における DNS ルックアップの考察

- DNSSEC
  - “信頼の連鎖” を構築するために上位階層へのクエリが発生する
  - 署名の検証処理による CPU 負荷

送信ドメイン認証における DNS ルックアップの考察

- EDNS0
  - 512byte を超える DNS メッセージを扱う拡張
  - 送信ドメイン認証や DNSSEC では利用される機会が増える
  - 場合によっては TCP による通信が発生する
    - 一般に UDP よりは負荷が大きい

送信ドメイン認証における DNS ルックアップの考察

- 送信ドメイン認証の検証処理においては大量の DNS クエリが発生する可能性がある
  - SPF/SIDF
  - DNSSEC
  - EDNS0

送信ドメイン認証における DNS ルックアップの考察

- 同一レコードが繰り返し参照されるケースが多い
  - ほとんどの場合、ある送信元ドメインに対して、発生する一連の DNS クエリは同一
  - spam の場合、少数の有名ドメインが騙られる傾向にある

送信ドメイン認証における DNS ルックアップの考察

- DNS キャッシュの導入を強く推奨
  - いずれの観点から見ても非常に有効
    - 導入しない場合の負荷が大きすぎる
  - ENMA に libunbound を組み込もうかと考えたくらい

EDNS0

- 512byte を超える DNS メッセージを扱う拡張
- 送信ドメイン認証では欠かせない機能
  - DKIM 公開鍵の鍵長に 2048 bit のものを使うと公開鍵レコードの長さが 512byte を超える
  - 512byte を超える SPF レコードは推奨されていないが、禁止されてもいない
  - EDNS0 が使用不能だと DNSSEC やその他の障害※1の原因にもなる

※1 http://jprs.jp/tech/notice/2011-03-03-inappropriate-handling-for-long-dns-packet.html

EDNS0

- 典型的な EDNS0 の敵
  - 旧型の FW
  - 家庭用ルータ
    - 簡易 FW 機能
  - 大昔に設定して以来全く触っていない FW
- 送信ドメイン認証の導入に際しては EDNS0 が正常に機能するか一度確認を

おまけ

sidfquery

- SPF/SIDFの評価をおこなうテストツール
- 引数
  - メールアドレス
  - IP アドレス (IPv6 対応)
- モード
  - SPF (デフォルト)
  - Sender ID - mfrom
  - Sender ID - PRA

sidfquery の使用例

```
$ sidfquery username@iij.ad.jp 192.168.1.1 ::1
username@iij.ad.jp 192.168.1.1 hardfail
username@iij.ad.jp ::1 hardfail

$ sidfquery username@iij.ad.jp www.iij.ad.jp
username@iij.ad.jp 210.130.137.80 hardfail
username@iij.ad.jp 2001:240:bb42:b000::1:80 hardfail
```

- メール受信時と同一の検証処理をおこなう
- トラブルシューティングのお供に

まとめ

- 受信時の検証は ENMA を入れるだけで OK
- ENMA の導入は簡単
- DNSSEC を有効にした DNS キャッシュサーバを挟む

リソース

- Web サイト

  http://enma.sf.net/

- 要望・提案・質問・バグ報告

  enma-users-jp@lists.sourceforge.net