SpamAssassin

滝澤 隆史
日本SpamAssassinユーザー会
株式会社　サードウェア

私は誰？

氏名　滝澤隆史
所属　株式会社サードウェア

オープンソース関連
- http://www.emaillab.org/ の中の人
- 昔はqmail関連（qmail-vidaの作者）
- Muttの日本語／国際化対応関連
- SpamAssassinの日本語対応パッチ
- DNSキャッシュサーバUnboundの紹介

物書き
- 日経Linux
- Software Design

今日の内容

10分でわかる SpamAssassin （概要編）

5分でできる SpamAssassin （導入編）

5分で役に立つ
かもしれない
SpamAssassin
（実践編）

10分でわかる SpamAssassin （概要編）

SpamAssassin とは何ぞや

様々な試験を行い
スパムらしさを判定する
総合的なメールフィルタ

様々な試験の結果をスパムらしさのスコアとして加算する

0.1 + 0.5 + 1.0 + 3.0 + 2.0 + 1.0 = 6.6

→スパムっぽいよ

正常なメールを
スパムと誤判定する
ことを少なくする

SpamAssassinが提供するもの

- スパムらしさを判定するPerlモジュールライブラリ
- ツール
- 標準のプラグイン
- 標準のルールファイル

動作環境（日本語パッチ対応）

Perl 5.8.5以降が
インストールされた
UNIX系OS（Linux/*BSDも含む）

Windows環境でも動作する

SpamAssassinでできること

メールの解析

- 様々な試験の実施
- スパムらしさのスコアの計算および判定

判定結果に対する処理

- 協調型データベースへの報告
- ベイジアンフィルタの自動学習

メールの書き換え

- ヘッダの書き換え
- スコアや判定結果のヘッダへの追加
- スパムメールのカプセル化（message/rfc822形式）

スコアや判定結果のヘッダへの追加

- X-Spam-Flag: YES
- X-Spam-Level: ********
- X-Spam-Status: Yes, score=7.3, ...

SpamAssassinでできないこと

SpamAssassin単体では

- スパムを除去できない
- スパムを振り分けできない
- バウンスメールを送れない

スパムの除去とか
振り分けをしたい

他のソフトウェアと
組み合わせてください。
→実践編へ

日本語メールの判定はできるの？

日本語対応パッチ
あります

http://spamassassin.jp/download/sa3.2/

日本語でテストルールが書けます

body　HOGOHOGE　/ほごほげ/

ベイジアンフィルタが
日本語対応になります

日本語は単語毎に
区切られていない言語。

「私の名前は中野です」

ベイズ解析を行うためには、
分かち書きが必要。

「私　の　名前　は　中野　です」

分かち書き処理はSpamAssassinのプラグインとして実装。

プラグインを
2つ用意している。

Tokenizer::MeCab

- 形態素解析エンジンMeCabの利用
- 分かち書きの結果
  - 私の名前は中野です
  - 私　の　名前　は　中野　です

Tokenizer::SimpleJA

- 文字種による区別
  - ひらがなによる切り出し
- 他のソフトウェアは不要
- 分かち書きの結果
  - 私の名前は中野です
  - 私　名前　中野

SpamAssassinの機能をみてみよう！

Perlモジュール

```
use Mail::SpamAssassin;

my $sa = Mail::SpamAssassin->new();
my $mail = $sa->parse($message);
my $status = $sa->check($mail);
if ($status->is_spam()) {
   $message = $status->rewrite_mail();
   ....
}
$status->finish();
$mail->finish();
```

Perlのプログラムに
SpamAssassinを
組み込むことができる。

ツール

SpamAssassinのツール

ツール	説明
spamassassin	メールがスパムであるかどうかを判定する。
spamc	メールがスパムであるかどうかを判定する。 spamdのクライアントとして動く。
spamd	メールがスパムであるかどうかを判定するデーモン。spamcをクライアントとして接続を受け付ける。
sa-learn	ベイジアンフィルタの学習を行わせる。
sa-update	最新のルールファイルをダウンロードしてきて更新する。
sa-comple	BODYルールのコンパイル

spamassassin

- スタンドアローンのスパム判定プログラム
- 標準入力からメールを渡して、標準出力に結果のヘッダを付けて出力する。
- Perlのプログラムであるため、起動のオーバーヘッドがある。

ヘッダの出力例

```
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on
  star-destroyer.in.emaillab.org
X-Spam-Level: *******
X-Spam-Status: Yes, score=7.6 required=5.0 tests=BODY_JA_AERU,BODY_JA_AITE,
  BODY_JA_ANATA,BODY_JA_DANSEI,BODY_JA_HOSHI,BODY_JA_JOSEI,BODY_JA_KINJO,
  BODY_JA_KONOKAN,BODY_JA_KYOHI,BODY_JA_SHUJIN,HS_INDEX_PARAM,MISSING_MID,
  MISSING_MSGID,NO_RECEIVED,NO_RELAYS,TEXT_NOCHARSET,URIBL_WS_SURBL,URI_QUERY
  autolearn=no version=3.2.5
X-Spam-Report:
  *  0.0 MISSING_MID Missing Message-Id: header
  *  1.0 TEXT_NOCHARSET Content-Type: text/(plain|html) with no charset
  * -0.0 NO_RELAYS Informational: message was not relayed via SMTP
  *  0.6 BODY_JA_KYOHI BODY: KYOHI
  *  0.3 BODY_JA_AERU BODY: AERU
  *  0.5 BODY_JA_DANSEI BODY: DANSEI
  *  0.3 BODY_JA_KINJO BODY: KINJO
  *  0.6 BODY_JA_ANATA BODY: ANATA
  *  0.3 BODY_JA_SHUJIN BODY: SHUJIN
  *  0.3 BODY_JA_AITE BODY: AITE
  *  0.6 BODY_JA_JOSEI BODY: JOSEI
  *  0.3 BODY_JA_HOSHI BODY: HOSHI
  *  0.3 BODY_JA_KONOKAN BODY: KONOKAN
  *  0.5 URI_QUERY URI: query
  *  0.0 HS_INDEX_PARAM URI: Link contains a common tracker pattern.
  *  1.0 URIBL_WS_SURBL Contains an URL listed in the WS SURBL blocklist
  *      [URIs: melkko.net]
  *  1.0 MISSING_MSGID Missing Message-Id: header
  * -0.0 NO_RECEIVED Informational: message has no Received headers
```

特に重要なヘッダ

```
X-Spam-Flag: YES
X-Spam-Level: *******
X-Spam-Status: Yes, score=7.6 required=5.0
 tests=BODY_JA_AERU,BODY_JA_AITE,
 BODY_JA_ANATA,BODY_JA_DANSEI,BODY_JA_HOSHI,
 BODY_JA_JOSEI,BODY_JA_KINJO,
  BODY_JA_KONOKAN,BODY_JA_KYOHI,
 BODY_JA_SHUJIN,HS_INDEX_PARAM,MISSING_MID,
 MISSING_MSGID,NO_RECEIVED,NO_RELAYS,
 TEXT_NOCHARSET,URIBL_WS_SURBL,URI_QUERY
  autolearn=no version=3.2.5
```

spamcとspamd

- クライアント/サーバ型のスパム判定プログラム
- spamdがデーモンとして常駐する。
- spamcはクライアントとして動作し、spamdにメールを渡してスパムの判定を依頼する。
- spamcはC言語で書かれているため、起動のオーバーヘッドが小さい。

sa-learn

- ベイジアンフィルタに手動で学習させるプログラム。

sa-update

- ルールファイルを最新のものに更新するプログラム
- スパムの手法は常に変化するため、対応する新しいルールが作られる。
- →最新のルールへの更新が必要

sa-compile

- BODYルールをコンパイルする。
- BODYルールの正規表現をC言語のプログラムに変換して、コンパイルする。
- ルール判定の高速化
- 残念ながら日本語には対応していない。

試験

- パターンテスト
  - ヘッダ
  - ボディのテキストパート
  - URI
  - メッセージ全体
  - ホワイトリスト・ブラックリスト

- 国、言語のテスト
  - メールが中継された国の一覧
  - テキストから言語の判断

- ネットワークテスト
  - IPアドレスやホスト名
  - DNSブラックリスト
  - URIDNSブラックリスト
  - 協調型データベース
  - 送信者認証
    （SPF, DomainKeys, DKIM）

- ベイジアンフィルタのテスト
- 特殊（プラグイン）
  - AS番号
  - URI
  - 画像情報
  - バウンスメール
- METAテスト

各試験は
プラグインとルールにより
実行される。

5分でできる SpamAssassin （導入編）

日本語対応パッチがあるので
適応してインストールする。
http://spamassassin.jp/download/sa3.2/

設定ファイル
/etc/mail/spamassassin/local.cf

必要最小限の設定

- 日本語パッチの機能を使う場合
  - normalize_charset　1
- 判定スコアの設定
  - required_score　5
  - 運用当初は高めに設定し、精度が上がってきたら徐々に下げる。
  - 最適な閾値が5になるように各ルールのスコアは調整されている。

必要最小限の設定

- ネットワークの設定
  - trusted_networks 192.168/24
- レポートオプションの設定
  - report_safe 0
  - これを設定しないとスパム判定されたメールはmessage/rfc822形式のレポートメール形式になる。

利用するプラグインを選び、有効にする。

/etc/mail/spamassassin/*.pre

- init.pre
- v310.pre
- v312.pre
- v320.pre

Mail::SpamAssassin::Plugin

- ASN.pm
- AWL.pm
- AccessDB.pm
- AntiVirus.pm
- AutoLearnThreshold.pm
- Bayes.pm
- BodyEval.pm
- BodyRuleBaseExtractor.pm
- Check.pm
- DCC.pm
- DKIM.pm
- DNSEval.pm
- DomainKeys.pm
- HTMLEval.pm
- HTTPSMismatch.pm
- Hashcash.pm
- HeaderEval.pm
- ImageInfo.pm
- MIMEEval.pm
- MIMEHeader.pm
- OneLineBodyRuleType.pm
- Pyzor.pm
- Razor2.pm
- RelayCountry.pm
- RelayEval.pm
- ReplaceTags.pm
- Rule2XSBody.pm
- SPF.pm
- Shortcircuit.pm
- SpamCop.pm
- Test.pm
- TextCat.pm
- URIDNSBL.pm
- URIDetail.pm
- URIEval.pm
- VBounce.pm
- WLBLEval.pm
- WhiteListSubject.pm

プラグイン

- 自動学習関連
  - AutoLearnThreshold、AWL
- パターンテスト関連
  - WhitelistSubject、MIMEHeader、ReplaceTags、HTTPMismatch、URIDetail
- 国、言語関連
  - RelayCountry、TextCat

プラグイン

- ネットワークテスト関連
  - DCC、Pyzor、Razor2、SpamCop、URIDNSBLI
- 送信者認証関連
  - SPF、DKIM、HashCash
- その他（AccessDB、AntiVirus）

例:DKIMを有効にする

/etc/mail/spamassassin/v312.preを
編集し、次の行を有効にする。

loadplugin Mail::SpamAssassin::Plugin::DKIM

必要に応じてルールを記述する。
local.cfに記述するのではなく、
別ファイルに記述し、
includeするのがおすすめ。

include site/bodytest.cf

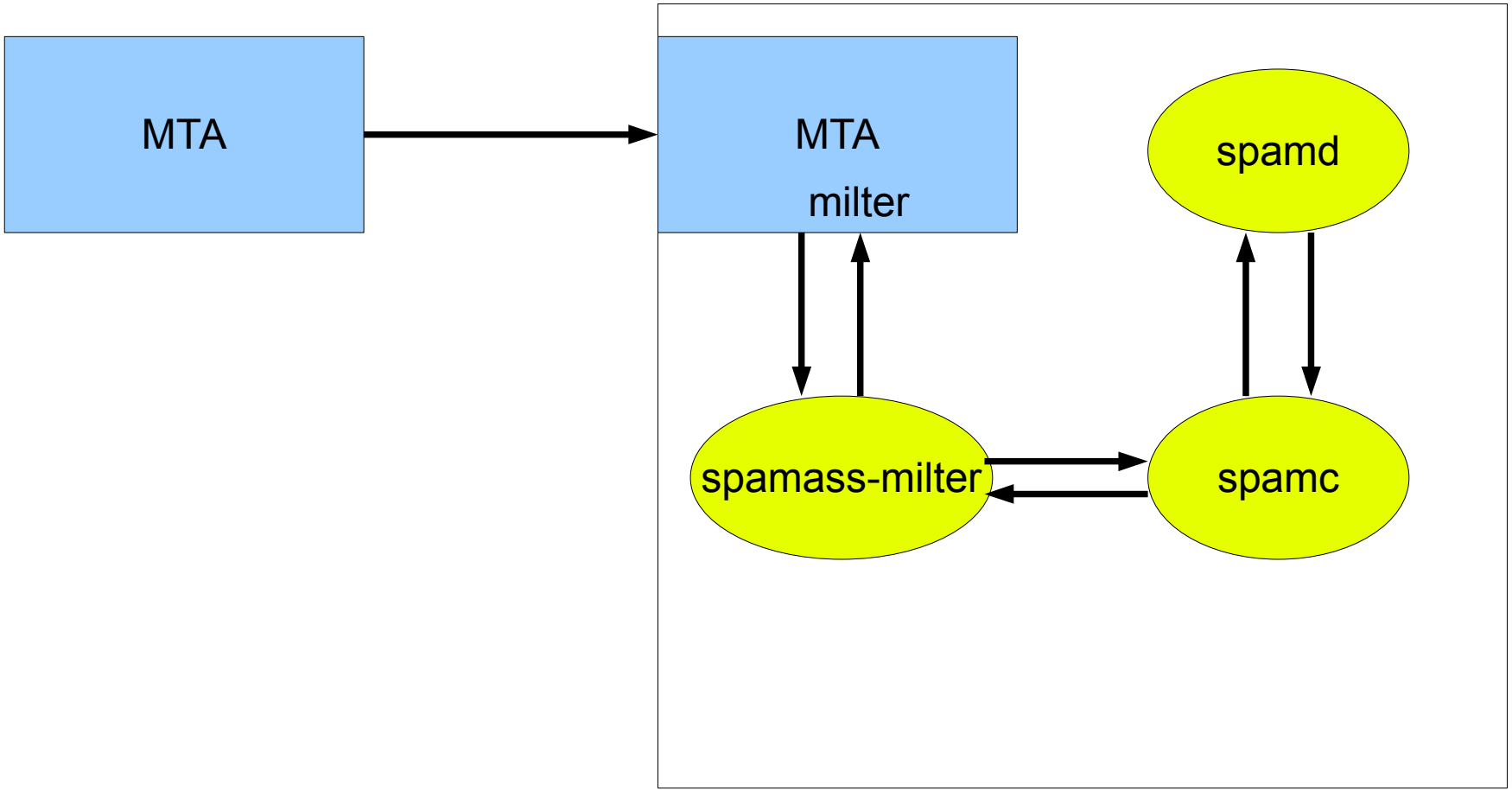
設定ファイルの記述を
変えたら必ず
spamassassin --lint
を実行すること

5分で役に立つ
かもしれない
SpamAssassin
（実践編）

MTAでの利用

spamass-milter

- SpamAssassin専用のmilterプログラム
- できること
  - SpamAssassinの判定結果のヘッダを付与する。
  - 指定したスコア以上のものを拒否することもできる。

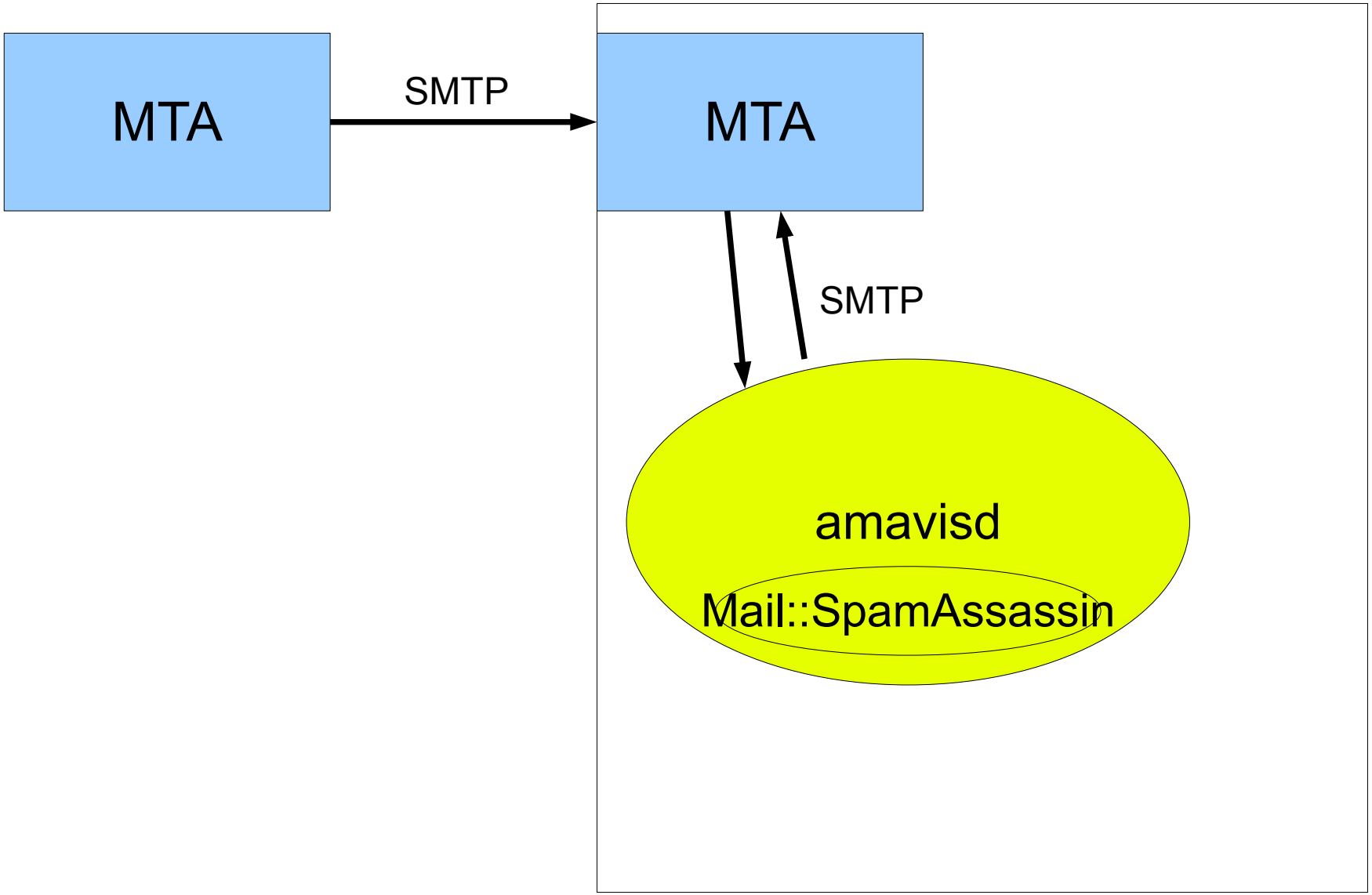

MTA
MTA
milter
spamd
spamass-milter
spamc

amavisd-new

- SpamAssassinを組み込んだ総合メールフィルタ
  - 不正なヘッダチェック
  - 添付ファイルの形式や拡張しのチェック
  - ウイルスチェック
  - スパムチェック（SpamAssassin）
  - ホワイトリスト/ブラックリスト

amavisd-new

- smtpサーバとして動作する。
- MTAと組み合わせて使用することもできる。
  - Postfixのcontents_filterなど

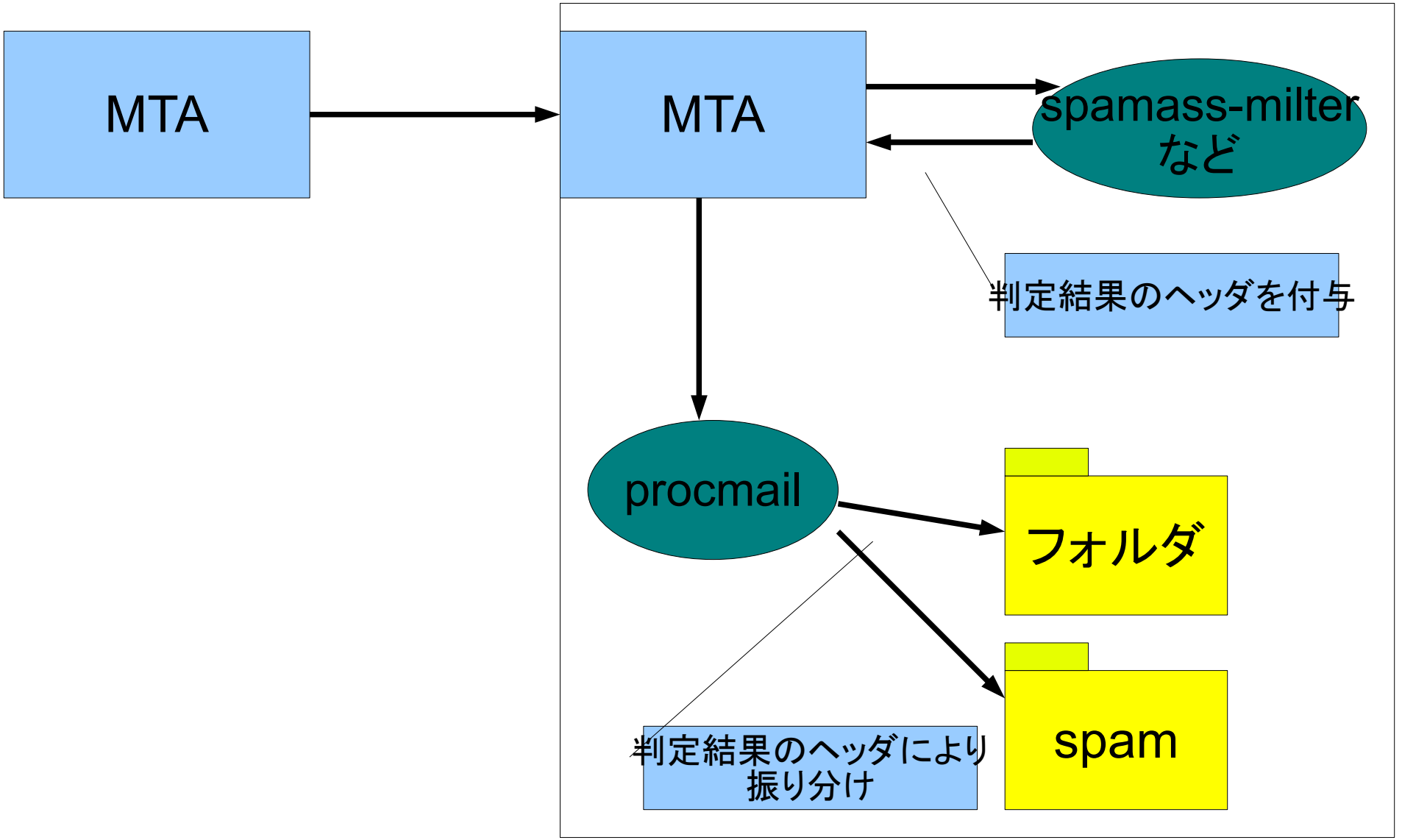

MTA
SMTP
MTA
SMTP
amavisd
Mail::SpamAssassin

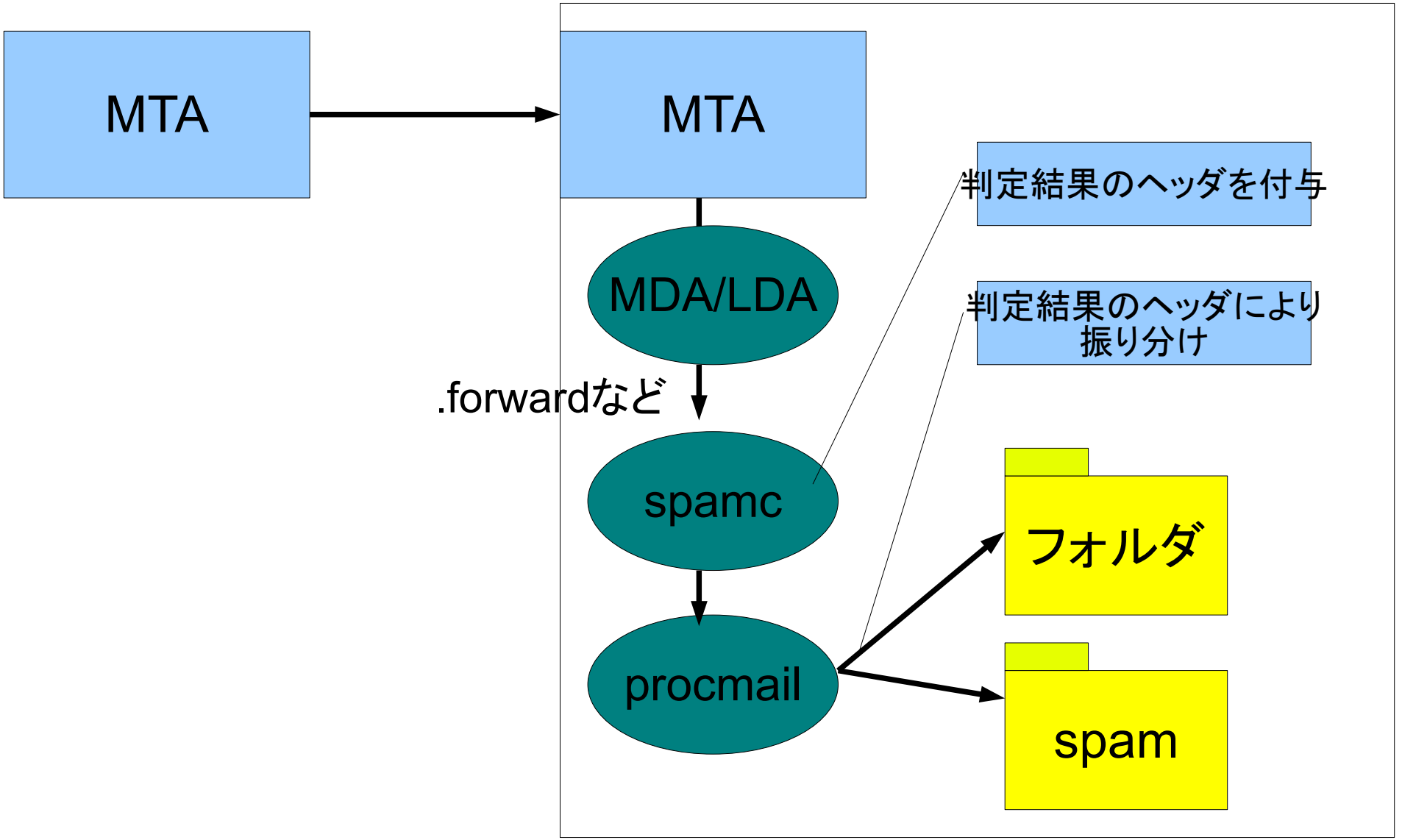
MDA/LDAでの利用

MDA/LDA

- MDA
  - Message Delivery Agent
- LDA
  - Local Delivery Agent
- 振り分けできるMDA/LDA
  - procmail
  - maildrop
  - sieve機能（dovecotのdeliver+sieveプラグインなど）

- 上流で付与したSpamAssassinの判定結果のヘッダによりMDA/LDAで振り分けする。
- 上流
  - MTAレベル（spamass-milter）
  - メールボックスレベル.forwardなどでspamcやspamassassinコマンドを呼び出す
- 判断するヘッダ
  - X-Spam-Flag: YES
  - X-Spam-Level: *******

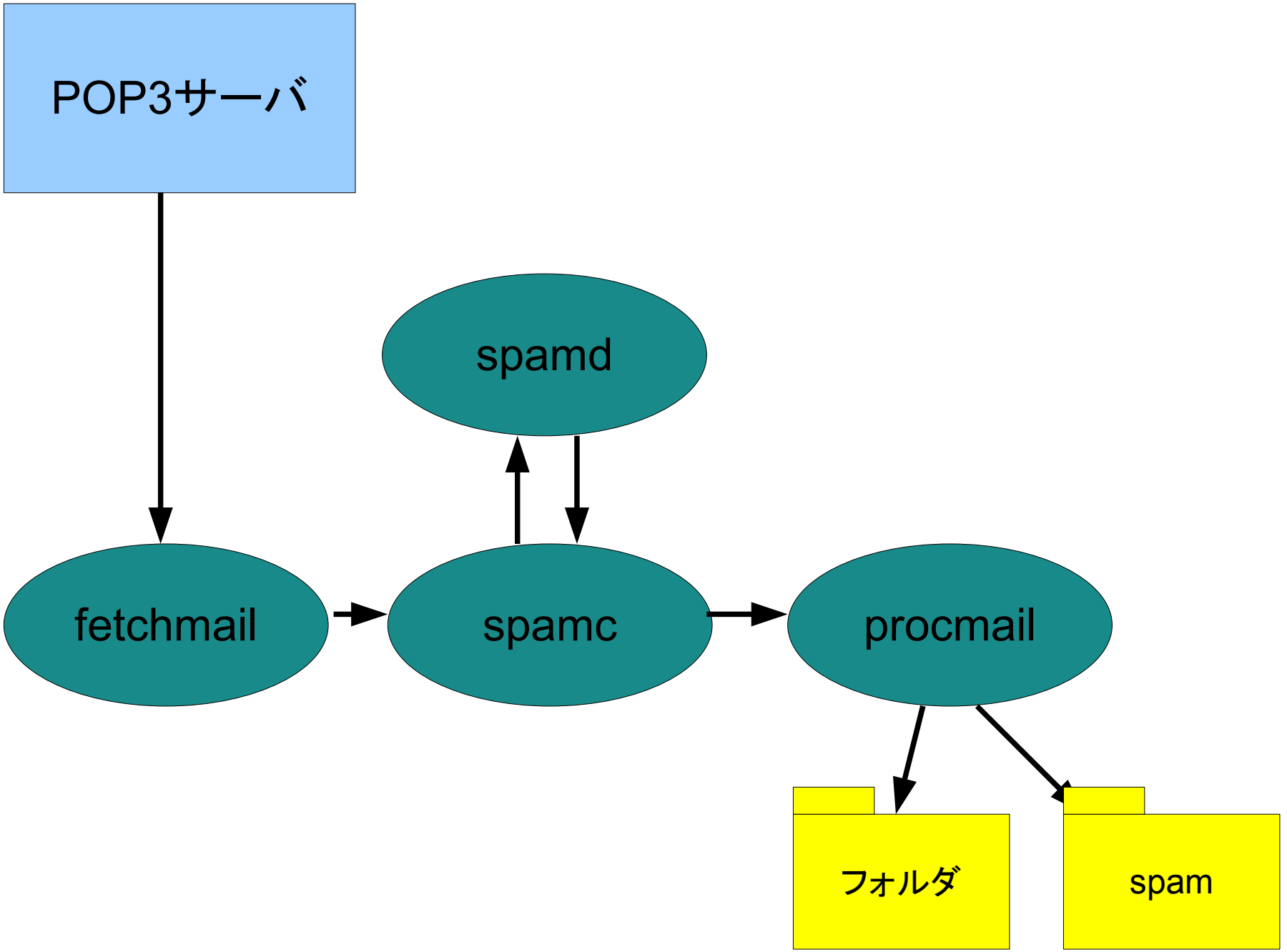

MTA
MTA
spamass-milter
など
判定結果のヘッダを付与
procmail
フォルダ
spam
判定結果のヘッダにより
振り分け


MTA
MTA
判定結果のヘッダを付与
MDA/LDA
判定結果のヘッダにより
振り分け
.forwardなど
spamc
フォルダ
procmail
spam

クライアント側での利用

fetchmail（UNIX系環境）

- POP3/IMAPサーバからメールを取得して、配送するプログラム
- spamc/spamdにより判定させて、procmailなどでメールボックスに配送させる。
- procmailなどで振り分けを行うことができる。


POP3サーバ
spamd
fetchmail
spamc
procmail
フォルダ
spam

メーラーでの振り分け

- Thunderbird
  - SpamAssassinのフラグを信用するオプションあり
  - MTAやMDA/LDAなどで付与したSpamAssassinの判定結果を利用する。

迷惑メールフィルタの設定

学習フィルタを使う場合、どのようなメッセージが迷惑メールなのか学ばせる必要があります。迷惑メールを受信したらツールバーの [迷惑メール] ボタンを押してください。間違って迷惑メールと判断されてしまったメールがあれば、[非迷惑メール] ボタンで訂正してください。

☐ このアカウントで迷惑メールの学習フィルタを有効にする(E)

送信者が以下に含まれる場合はメッセージが迷惑メールであるとマークしない(D):

☑ 個人用アドレス帳
☐ 記録用アドレス帳

☑ 次の迷惑メールヘッダを信用する(T): SpamAssassin

☑ 迷惑メールと判断された受信メッセージを次のフォルダに移動する(M):

◉ [迷惑メール] フォルダ(J): taki@cyber.email.ne.jp

○ その他(O): Local Folders の Junk

☐ このフォルダの迷惑メールのうち(U) 14 日以上前のものは自動的に削除する

判定するスコア

私の経験上ですが……

- ～5未満
  - ham
- 5以上6未満
  - hamあるいはspammy
- 6以上12未満
  - spammy
- 12以上20未満
  - spam
- 20以上
  - trash

おまけ

日本語ルール作成スクリプト

- http://spamassassin.jp/download/experimental/taki/
- sa-tokenizer.pl　　--- トークナイザー
- sa-ja-testmaker.pl --- テスト生成スクリプト

こんなルールを自動作成

```
# BODY_JA_HITOZUMA: 人妻 spam=2583/1325054, ham=1/1841092, ratio=0.00194
body     BODY_JA_HITOZUMA       /人妻/
describe BODY_JA_HITOZUMA       HITOZUMA
score    BODY_JA_HITOZUMA       0.6

# BODY_JA_ANATA: 貴方 spam=2645/1325054, ham=11/1841092, ratio=0.00193
body     BODY_JA_ANATA          /貴方/
describe BODY_JA_ANATA          ANATA
score    BODY_JA_ANATA          0.6

# BODY_JA_ICHIHACHIMIMAN: １８未満 spam=2446/1325054, ham=0/1841092, ratio=0.00184
body     BODY_JA_ICHIHACHIMIMAN     /１８未満/
describe BODY_JA_ICHIHACHIMIMAN     ICHIHACHIMIMAN
score    BODY_JA_ICHIHACHIMIMAN     0.6

# BODY_JA_ADARUTO: アダルト spam=2426/1325054, ham=0/1841092, ratio=0.00183
body     BODY_JA_ADARUTO        /アダルト/
describe BODY_JA_ADARUTO        ADARUTO
score    BODY_JA_ADARUTO        0.5

# BODY_JA_DEAI: 出会い spam=2444/1325054, ham=9/1841092, ratio=0.00179
body     BODY_JA_DEAI           /出会い/
describe BODY_JA_DEAI           DEAI
score    BODY_JA_DEAI           0.5
```

自動生成されたルール

- テスト名称(ローマ字)を自動生成
- 出現頻度によりスコアの割り付け

```
# BODY_JA_DEAI: 出会い spam=2444/1325054,
#    ham=9/1841092, ratio=0.00179
body      BODY_JA_DEAI          /出会い/
describe BODY_JA_DEAI          DEAI
score     BODY_JA_DEAI          0.5
```