ClearCode

milter manager

須藤功平

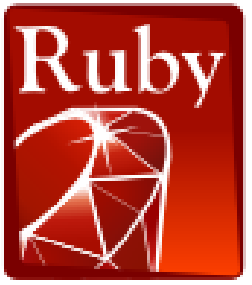
株式会社クリアコード

2009/06/13

自己紹介

- クリアコード代表取締役
- milter manager開発者
- よく使う言語: RubyとC

Rabbit



milter manager

開発のきっかけ

IPA平成20年度オープンソフトウェア利用促進事業

> *迷惑メール対策を柔軟に*
> *実現するためのmilterの開発*

milter manager

新しい迷惑メール対策手法

既存の手法を活用する基盤

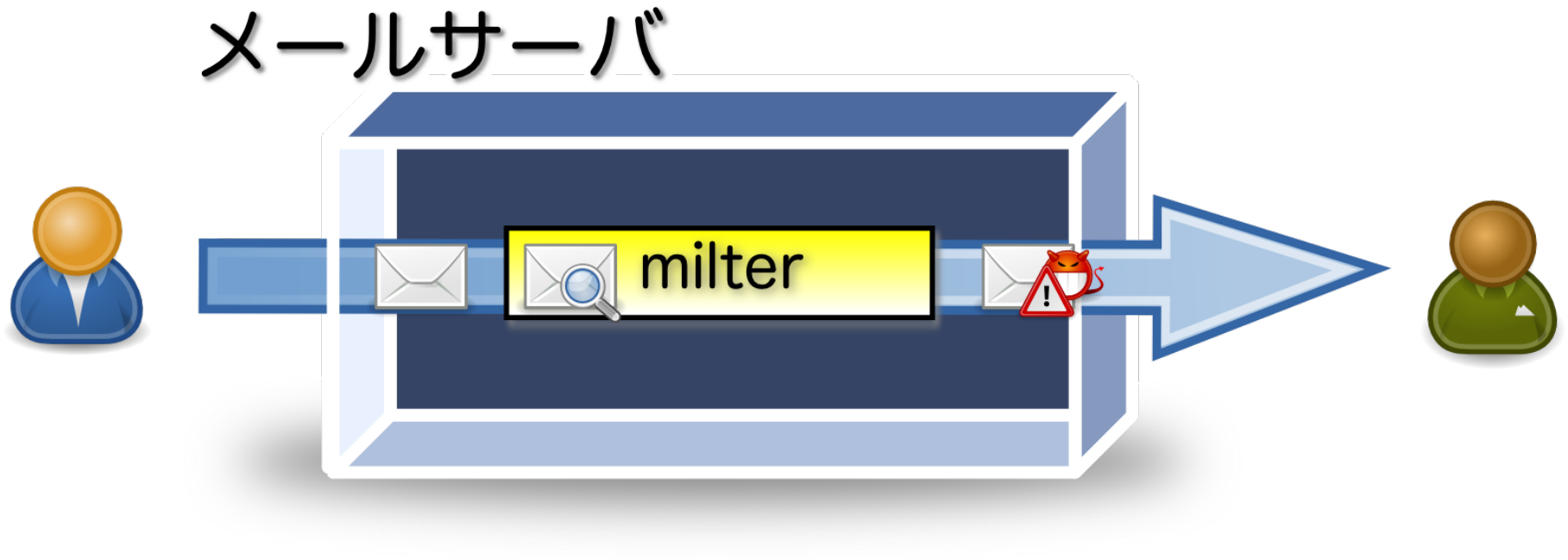
milter manager

- 多くの対策を使える
- 状況に応じた対策の適用
- 管理コストを削減
- 統計情報

話すこと

- milterとmilter manager
- 対策の連携例
- milter manager
プラットフォーム
- milter manager情報

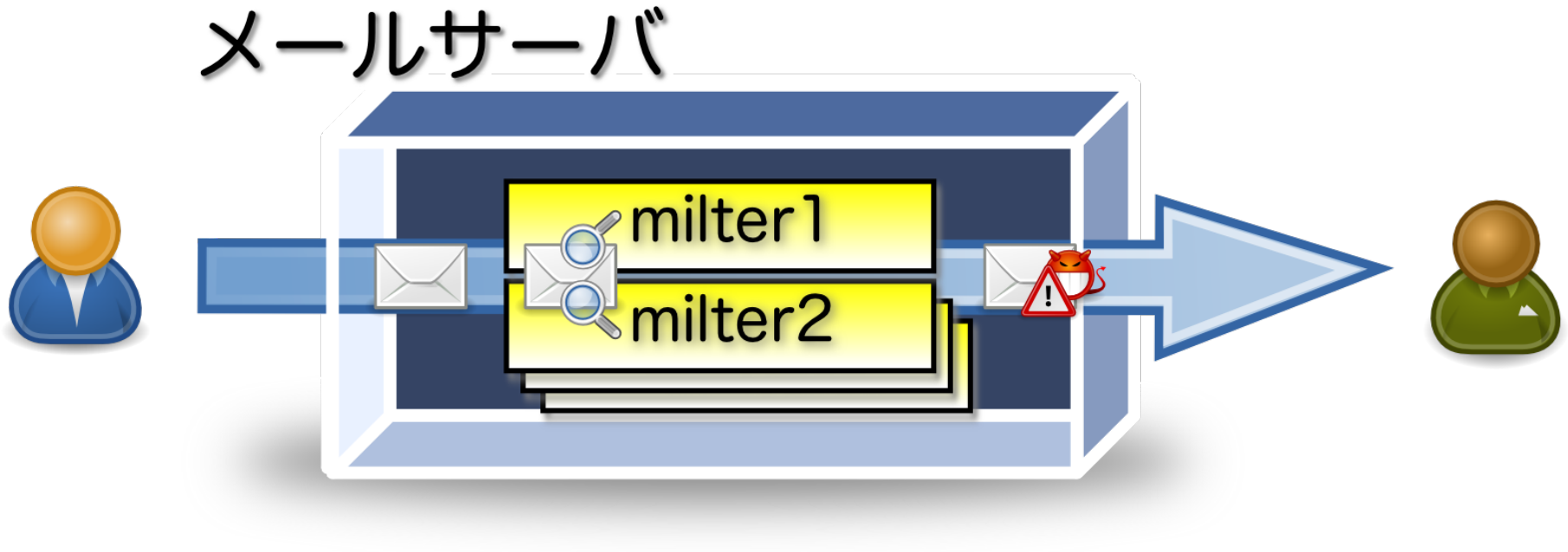
milter



milter: メールフィルタ

mail filter

プラグイン形式



milter: プラグイン形式

対策の組み合わせが可能

多数のmilter

接続情報を利用

S25R
p0f
国

- milter-regex
- milter-greylist
- milter-p0f
- など

差出人・宛先情報を利用

Greylisting
DNSBL
SPF

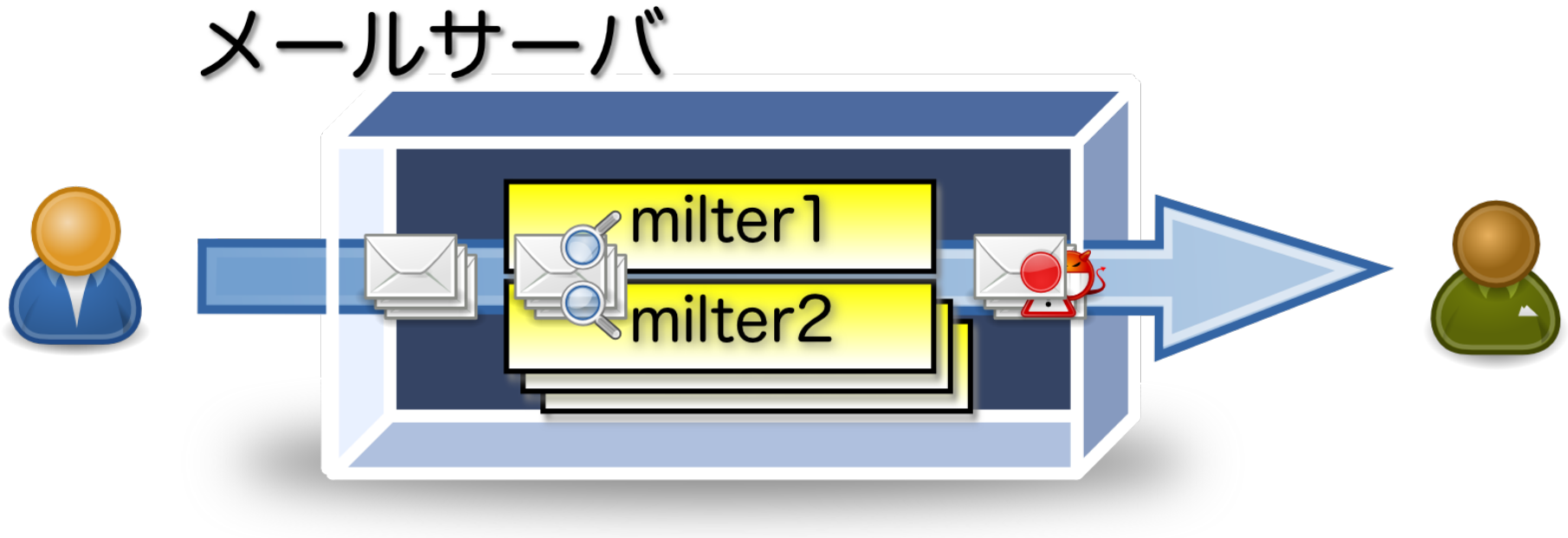
- milter-greylist
- milter-dnsbl
- sid-milter
- ENMA
- など

内容を利用

ベイジアンフィルタ
Razor/Pyzor
URIBL
国
DKIM/Sender ID

- spamass-milter
- dkim-milter
- sid-milter
- ENMA
- など

問題点



milter: 全メールに適用
それぞれが独立

効果的な対策

解決方法

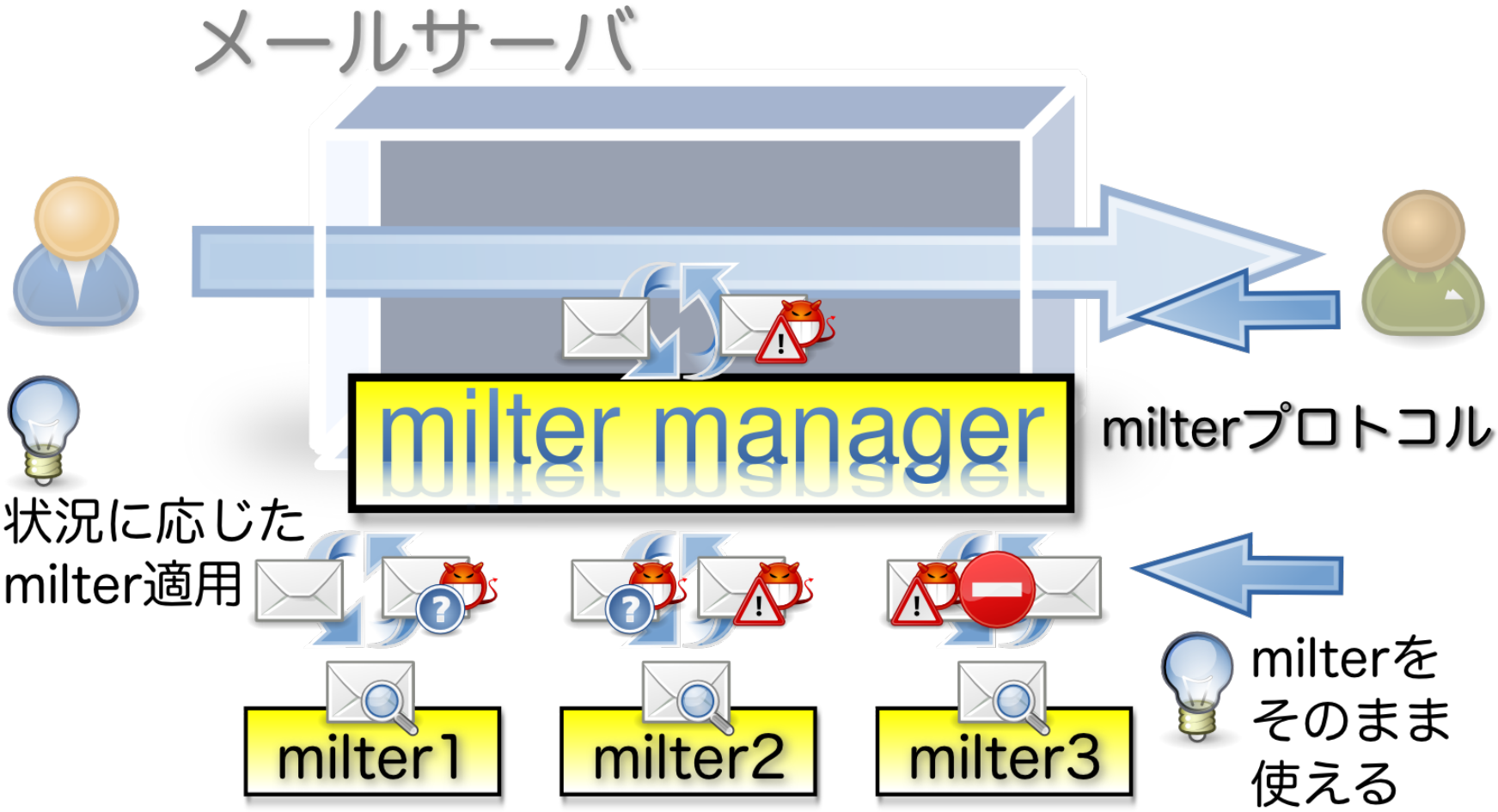
milter manager

メールサーバ  milter

メールサーバ

milterプロトコル

メールサーバ ⇄ milter manager ⇄ milter



milter manager

- ✓ milterを使える
- ✓ 状況に応じたmilterの適用

→ milterを活かすmilter

対策の連携例

- milterとmilter manager
- 対策の連携例
- milter manager
プラットフォーム
- milter manager情報

有効な対策システム


効果は高く



対策は多数

一長一短


副作用は抑える


対策を連携

効果は高く

対策は多数

一長一短

対策を連携

副作用は抑える

連携例

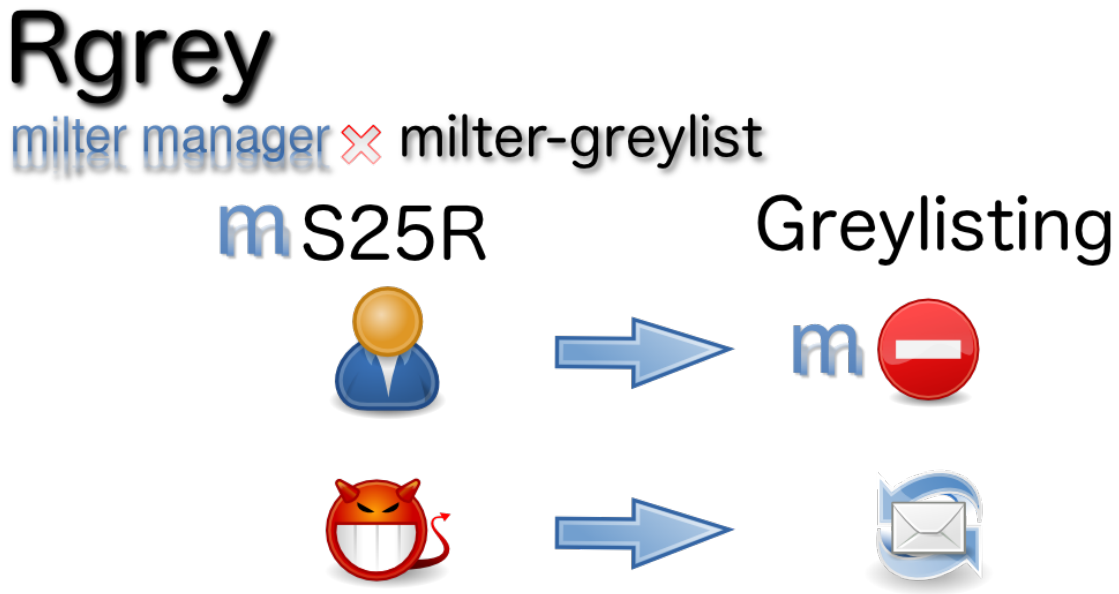
Greylistingをベースにした場合

- ✓ Rgrey
- ✓ taRgrey
- ✓ Rgrey + SPF/DKIM
- ✓ Rgrey + SpamAssassin

実現例: Rgrey

- ✓ milter-manager: S25R
- ✓ milter-greylist: Greylisting

実現図: Rgrey



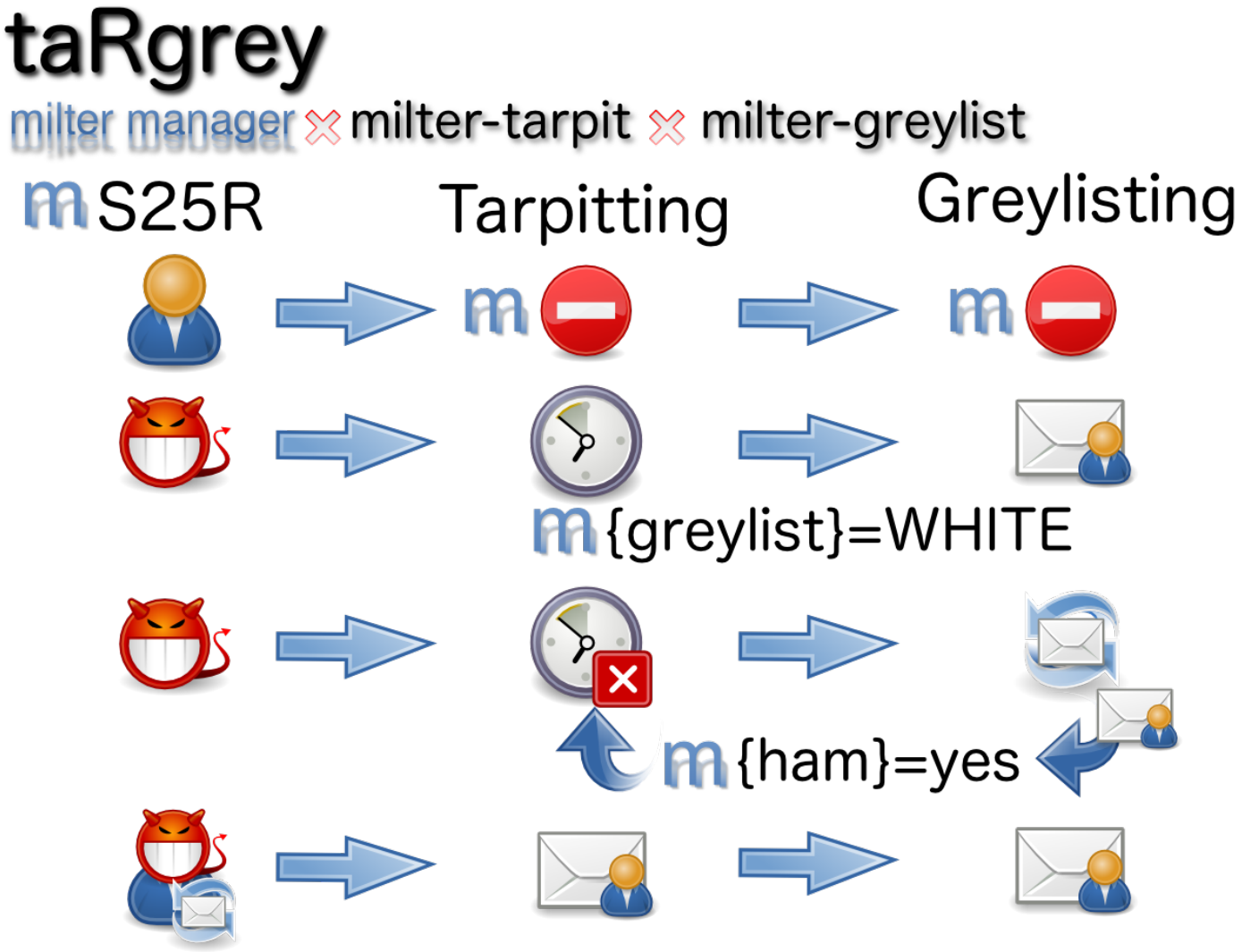
連携例: taRgrey

- ✓ S25R
- ✓ Tarpitting
- ✓ Greylisting

実現例: taRgrey

- ✓ milter-manager: S25R
- ✓ milter-tarpit: Tarpitting
- ✓ milter-greylist: Greylisting

実現図: taRgrey


taRgrey
milter manager × milter-tarpit × milter-greylist
S25R
Tarpitting
Greylisting
{greylist}=WHITE
{ham}=yes

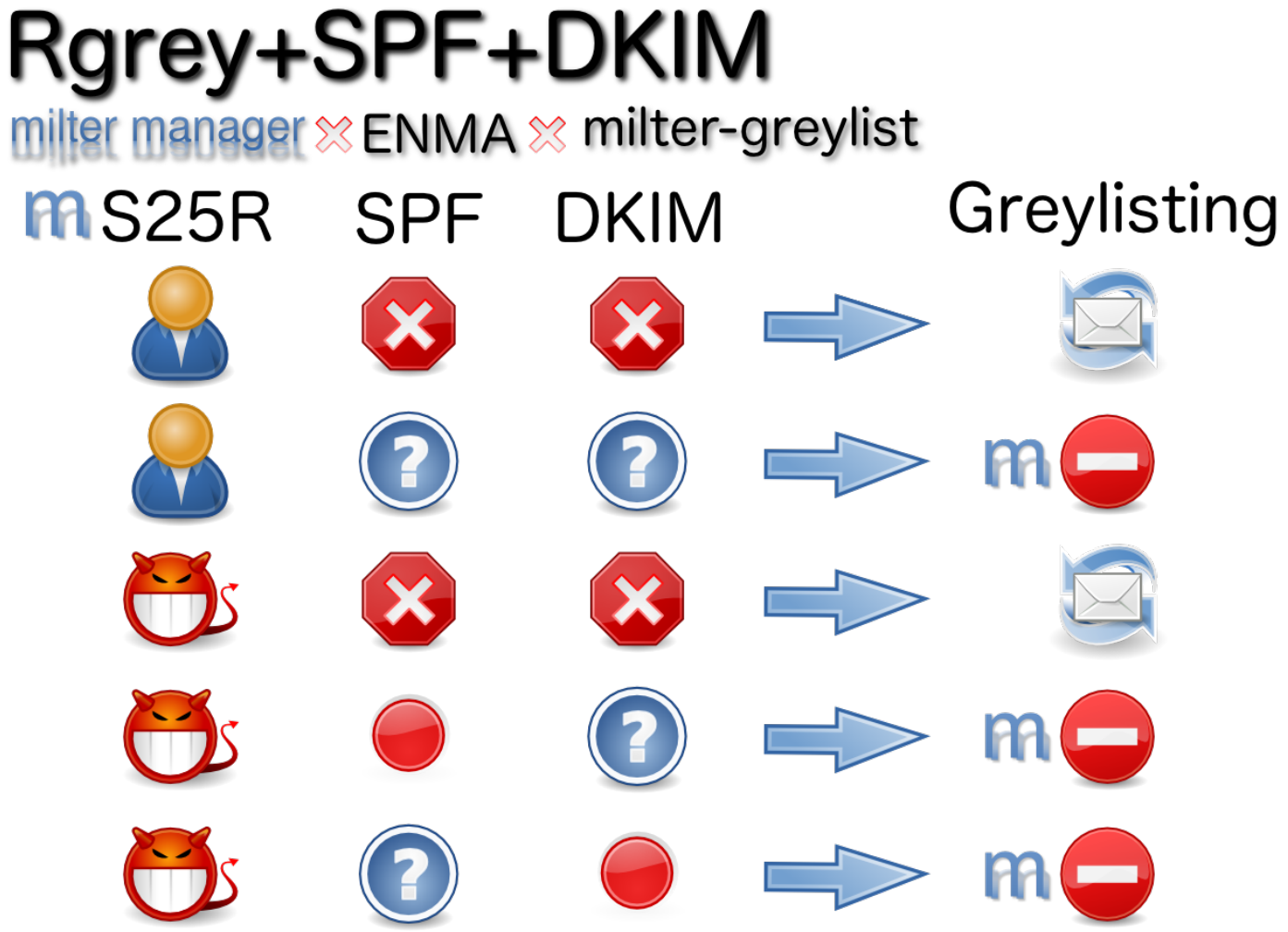
連携例: +SPF/DKIM

- S25R
- 送信ドメイン認証
  - SPF
  - DKIM
- Greylisting

実現例: +SPF/DKIM

- ✓ milter-manager: S25R
- ✓ ENMA: SPF/DKIM
- ✓ milter-greylist: Greylisting

実現図: +SPF/DKIM


Rgrey+SPF+DKIM
milter manager × ENMA × milter-greylist
S25R
SPF
DKIM
Greylisting

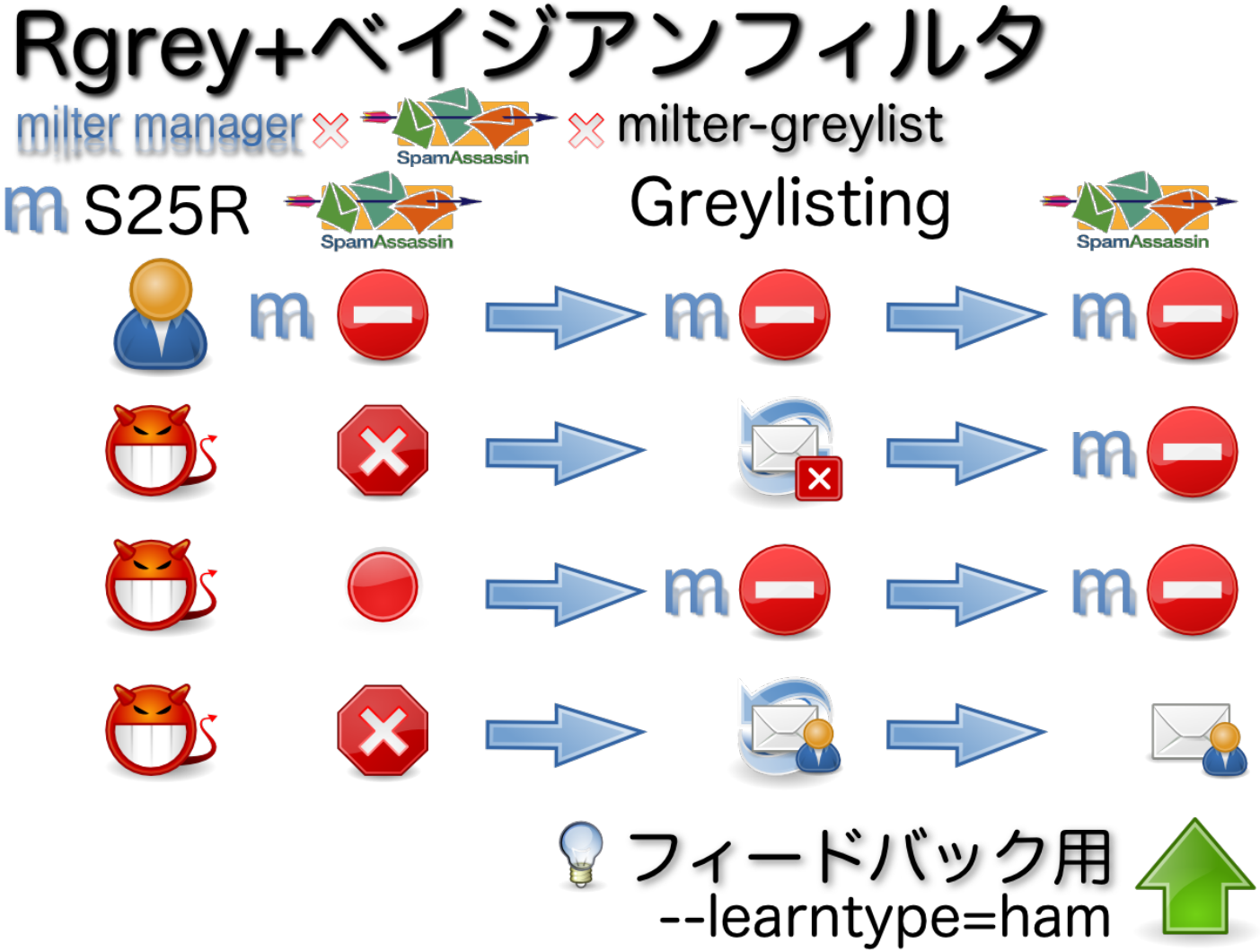
連携例: +内容ベース

- ✓ S25R
- ✓ SpamAssassin
- ✓ Greylisting

実現例: +内容ベース

- milter-manager: S25R
- spamass-milter: SpamAssassin
- milter-greylist: Greylisting

実現図: +内容ベース


Rgrey+ベイジアンフィルタ
milter manager
SpamAssassin
milter-greylist
S25R
SpamAssassin
Greylisting
SpamAssassin
フィードバック用
--learntype=ham

有効な対策


効果は高く



対策は多数

一長一短

対策を連携


副作用は抑える


mmで有効な対策


効果は高く



milterは多数

一長一短


milterを連携
milter manager


副作用は抑える


milter-greylist

- milterとmilter manager
- 対策の組み合わせ例
- milter-greylist: おまけ
- milter manager
  プラットフォーム
- milter manager情報

高機能

単体で実現可能

- ✓ Rgrey
- ✓ + SPF/DKIM
- ✓ + SpamAssassin

Rgrey

```
extendedregex
racl greylist domain /^\[.+\]$/ msg "S25R rule 0"
racl greylist domain /^[^.]*[0-9][^0-9.]+[0-9].*\./ msg "S25R rule 1"
racl greylist domain /^[^.]*[0-9][0-9][0-9][0-9][0-9]/ msg "S25R rule 2"
racl greylist domain /^([^.]+\.)?[0-9][^.]*\.[^.]+\..+\.[a-z]/ msg "S25R rule 3"
racl greylist domain /^[^.]*[0-9]\.[^.]*[0-9]-[0-9]/ msg "S25R rule 4"
racl greylist domain /^[^.]*[0-9]\.[^.]*[0-9]\.[^.]+\..+\./ msg "S25R rule 5"
racl greylist domain /^(dhcp|dialup|ppp|[achrsvx]?dsl)[^.]*[0-9]/ msg "S25R rule 6"
```

+SPF

```
racl whitelist spf pass
# ↑デフォルト
racl greylist spf fail msg "SPF fail"
```

+DKIM

```
racl whitelist default
dacl whitelist dkim pass
dacl greylist dkim fail msg "DKIM fail"
```

+SpamAssassin

```
racl whitelist default

spamdsock inet "localhost:783"
dacl greylist spamd msg "SpamAssassin"
# または
dacl greylist header "X-Spam-Flag: YES" msg "SpamAssassinn"
```

あれ？

プラットフォーム

- milterとmilter manager
- 対策の組み合わせ例
- milter manager
プラットフォーム
- milter manager情報

milter manager

- 多くの対策を使える
- 状況に応じた対策の適用
- 管理コストを削減
- 統計情報

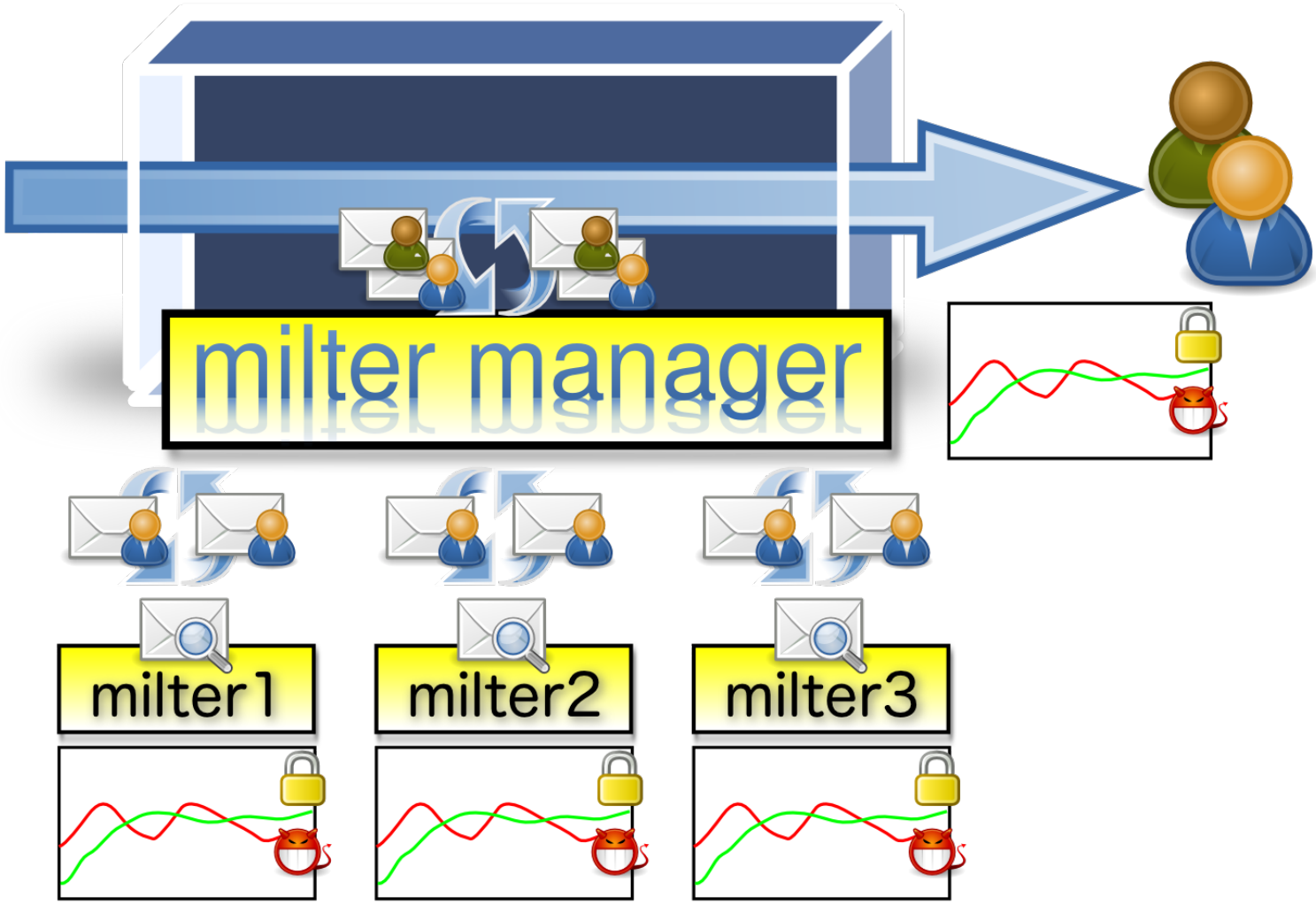
管理

導入
運用

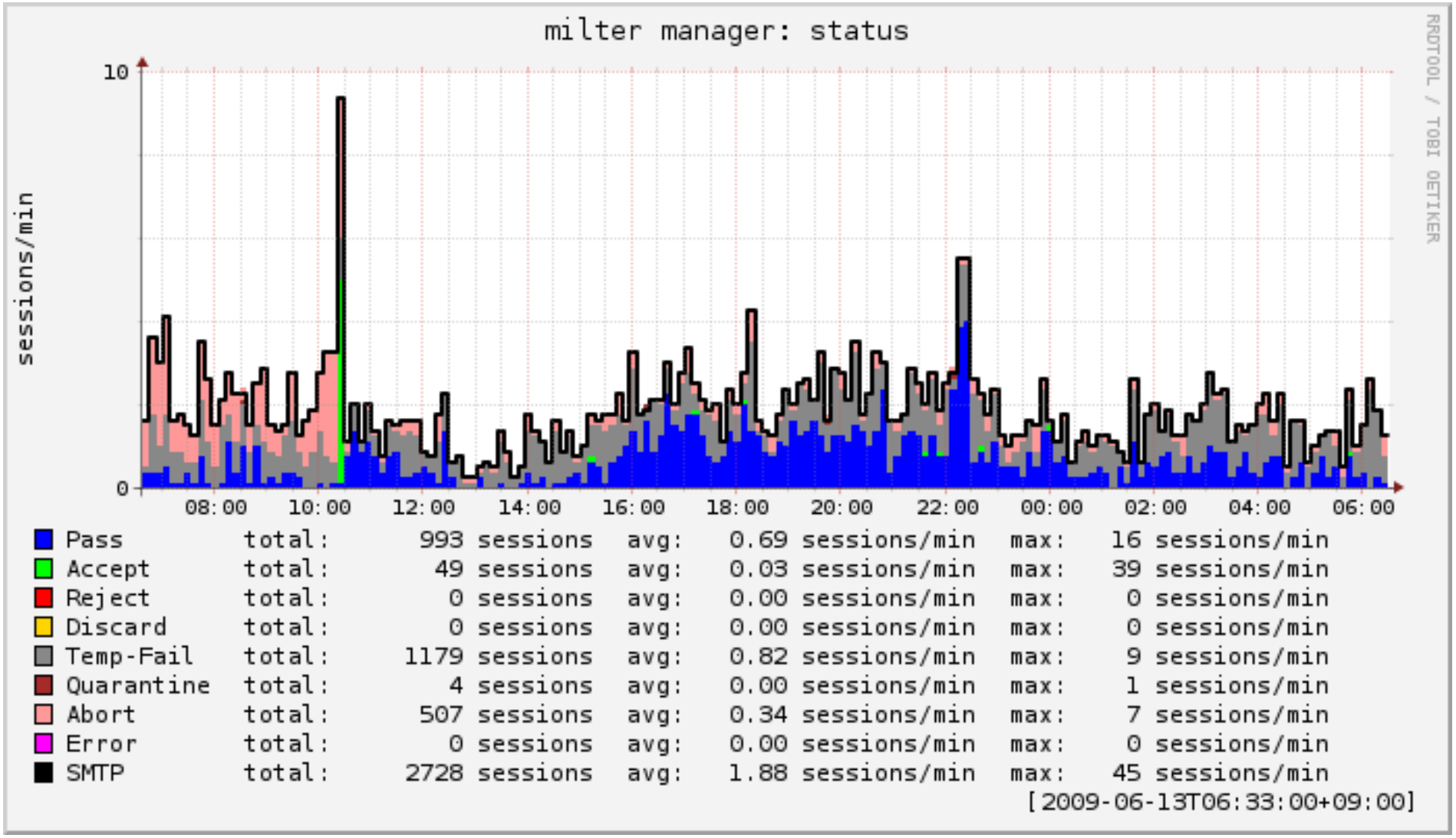
導入

- ✓ 特定ユーザのみ試験導入
- ✓ 効果の確認・報告
- ✓ 導入範囲の拡大
  - ✓ 例: 特定ドメインに拡大

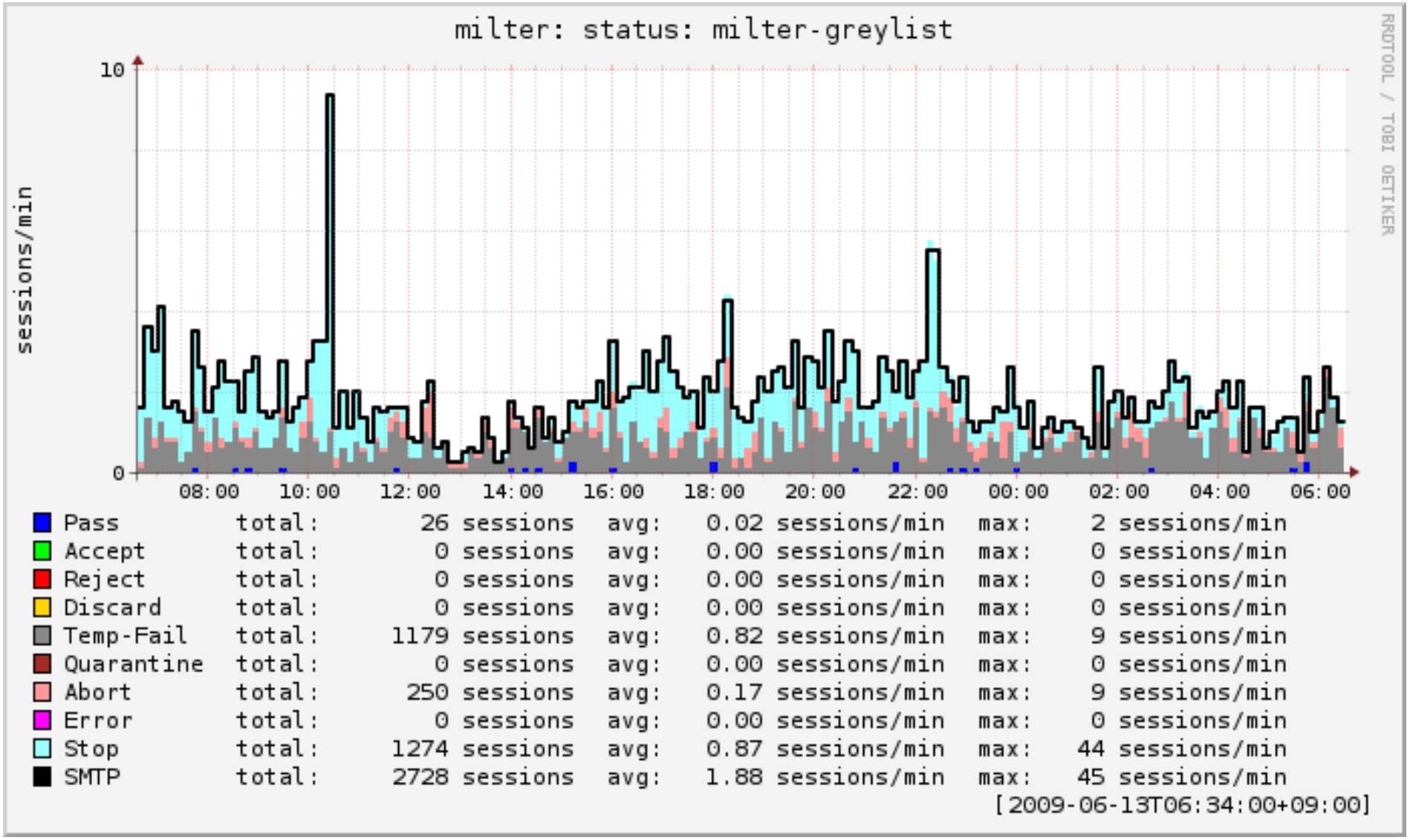
導入支援



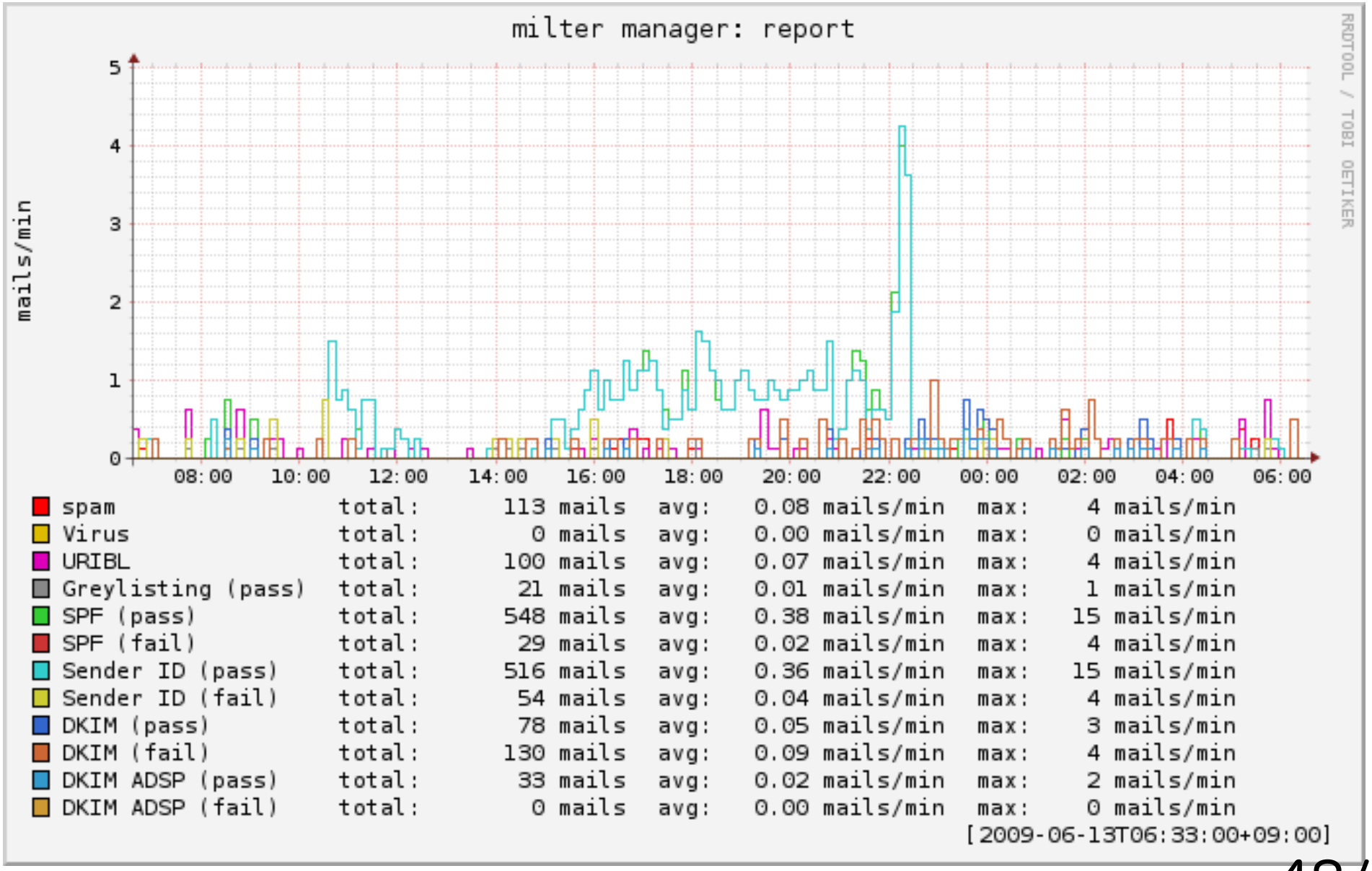
グラフ: 全体の結果


milter manager: status
sessions/min
10
0
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
RRDTOOL / TOBI OETIKER
Pass total: 993 sessions avg: 0.69 sessions/min max: 16 sessions/min
Accept total: 49 sessions avg: 0.03 sessions/min max: 39 sessions/min
Reject total: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
Discard total: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
Temp-Fail total: 1179 sessions avg: 0.82 sessions/min max: 9 sessions/min
Quarantine total: 4 sessions avg: 0.00 sessions/min max: 1 sessions/min
Abort total: 507 sessions avg: 0.34 sessions/min max: 7 sessions/min
Error total: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
SMTP total: 2728 sessions avg: 1.88 sessions/min max: 45 sessions/min
[2009-06-13T06:33:00+09:00]

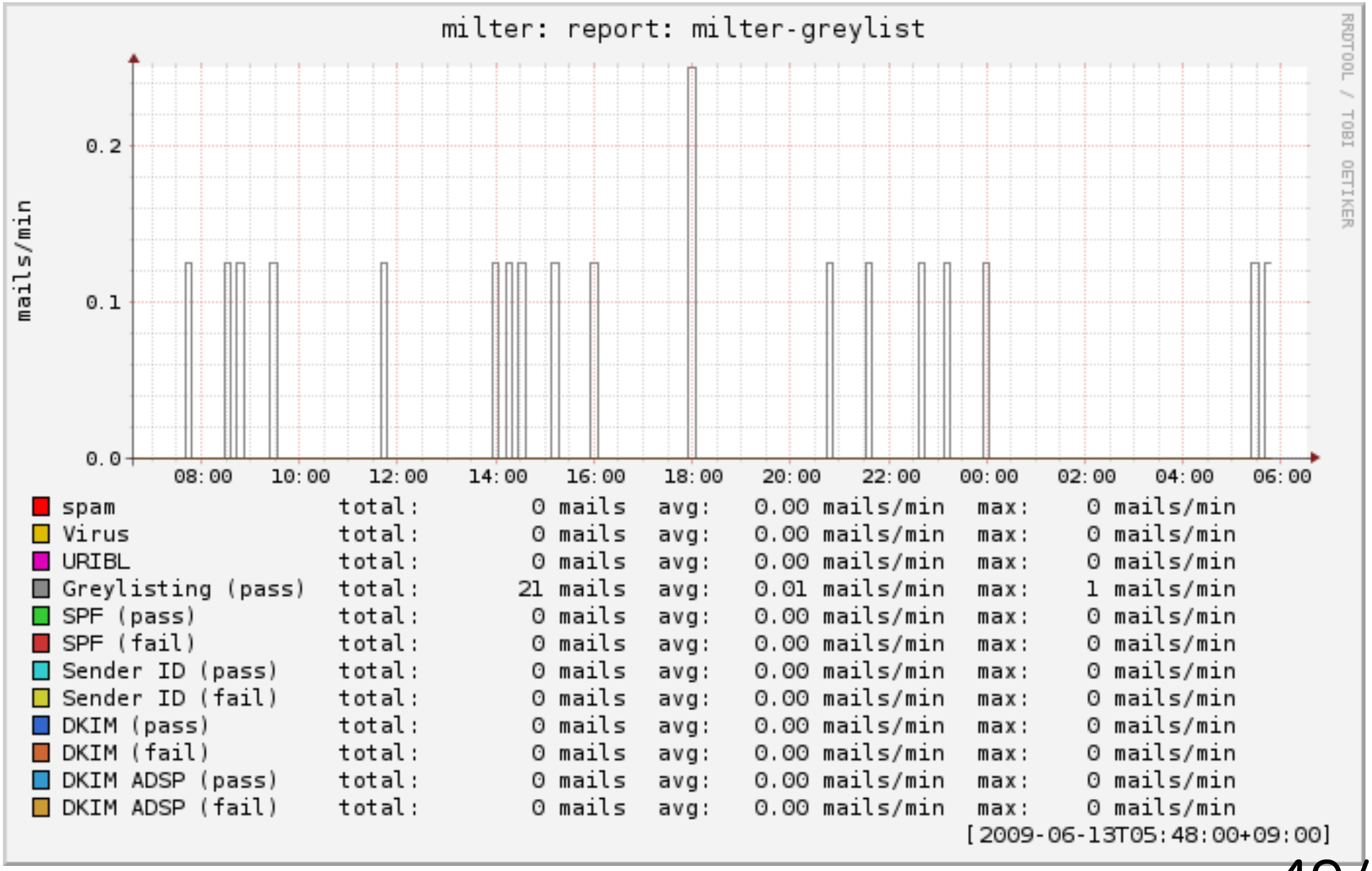
グラフ: 個々の結果


milter: status: milter-greylist
sessions/min
10
0
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
RRDTOOL / TOBI OETIKER
Pass total: 26 sessions avg: 0.02 sessions/min max: 2 sessions/min
Accept total: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
Reject total: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
Discard total: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
Temp-Fail total: 1179 sessions avg: 0.82 sessions/min max: 9 sessions/min
Quarantine total: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
Abort total: 250 sessions avg: 0.17 sessions/min max: 9 sessions/min
Error total: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
Stop total: 1274 sessions avg: 0.87 sessions/min max: 44 sessions/min
SMTP total: 2728 sessions avg: 1.88 sessions/min max: 45 sessions/min
[2009-06-13T06:34:00+09:00]

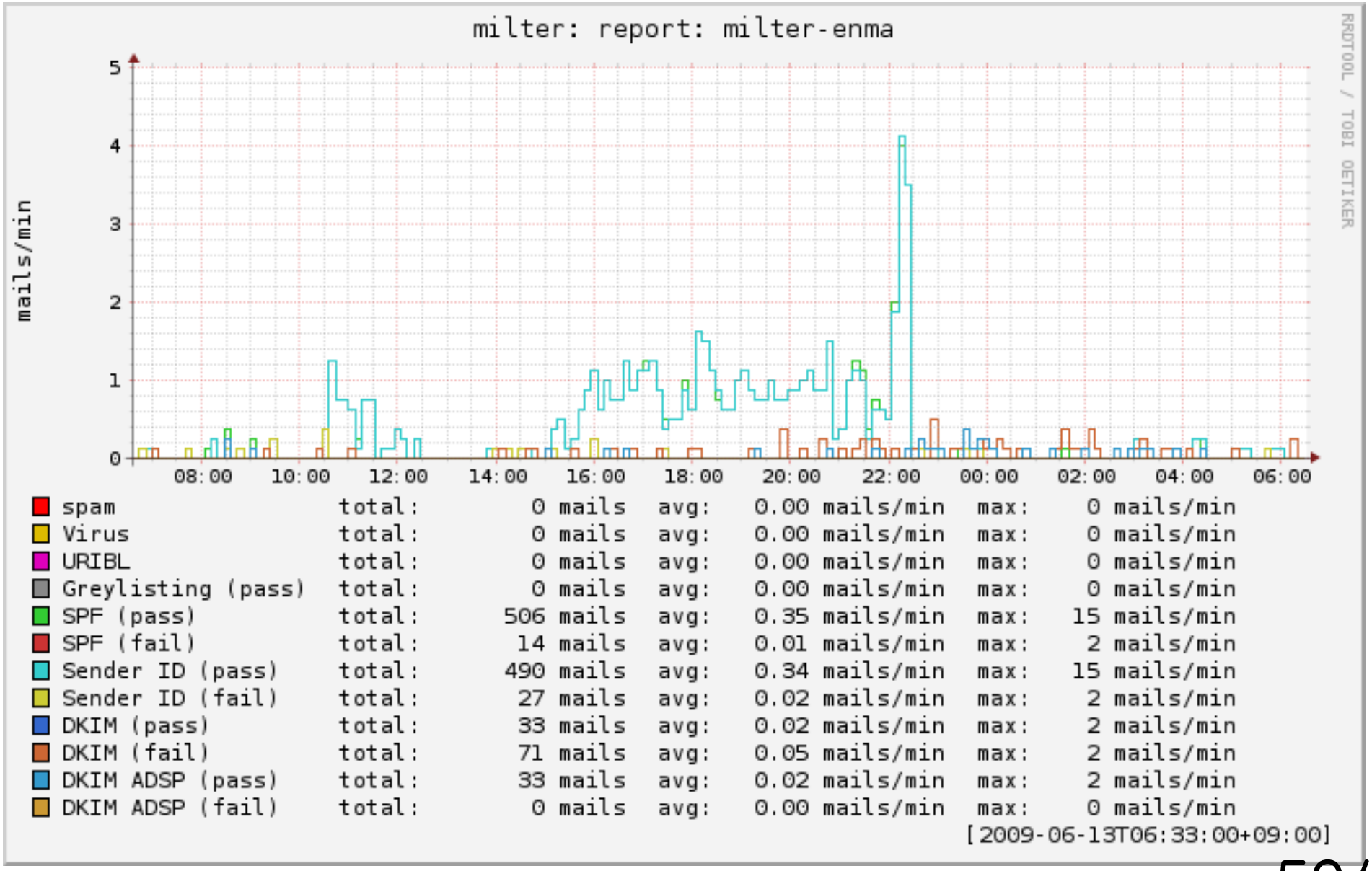
グラフ: 対策結果


milter manager: report
mails/min
RRDTOOL / TOBI OETIKER
0
1
2
3
4
5
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
spam total: 113 mails avg: 0.08 mails/min max: 4 mails/min
Virus total: 0 mails avg: 0.00 mails/min max: 0 mails/min
URIBL total: 100 mails avg: 0.07 mails/min max: 4 mails/min
Greylisting (pass) total: 21 mails avg: 0.01 mails/min max: 1 mails/min
SPF (pass) total: 548 mails avg: 0.38 mails/min max: 15 mails/min
SPF (fail) total: 29 mails avg: 0.02 mails/min max: 4 mails/min
Sender ID (pass) total: 516 mails avg: 0.36 mails/min max: 15 mails/min
Sender ID (fail) total: 54 mails avg: 0.04 mails/min max: 4 mails/min
DKIM (pass) total: 78 mails avg: 0.05 mails/min max: 3 mails/min
DKIM (fail) total: 130 mails avg: 0.09 mails/min max: 4 mails/min
DKIM ADSP (pass) total: 33 mails avg: 0.02 mails/min max: 2 mails/min
DKIM ADSP (fail) total: 0 mails avg: 0.00 mails/min max: 0 mails/min
[2009-06-13T06:33:00+09:00]

グラフ: 対策別結果


milter: report: milter-greylist
mails/min
0.2
0.1
0.0
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
RRDTOOL / TOBI OETIKER
spam total: 0 mails avg: 0.00 mails/min max: 0 mails/min
Virus total: 0 mails avg: 0.00 mails/min max: 0 mails/min
URIBL total: 0 mails avg: 0.00 mails/min max: 0 mails/min
Greylisting (pass) total: 21 mails avg: 0.01 mails/min max: 1 mails/min
SPF (pass) total: 0 mails avg: 0.00 mails/min max: 0 mails/min
SPF (fail) total: 0 mails avg: 0.00 mails/min max: 0 mails/min
Sender ID (pass) total: 0 mails avg: 0.00 mails/min max: 0 mails/min
Sender ID (fail) total: 0 mails avg: 0.00 mails/min max: 0 mails/min
DKIM (pass) total: 0 mails avg: 0.00 mails/min max: 0 mails/min
DKIM (fail) total: 0 mails avg: 0.00 mails/min max: 0 mails/min
DKIM ADSP (pass) total: 0 mails avg: 0.00 mails/min max: 0 mails/min
DKIM ADSP (fail) total: 0 mails avg: 0.00 mails/min max: 0 mails/min
[2009-06-13T05:48:00+09:00]

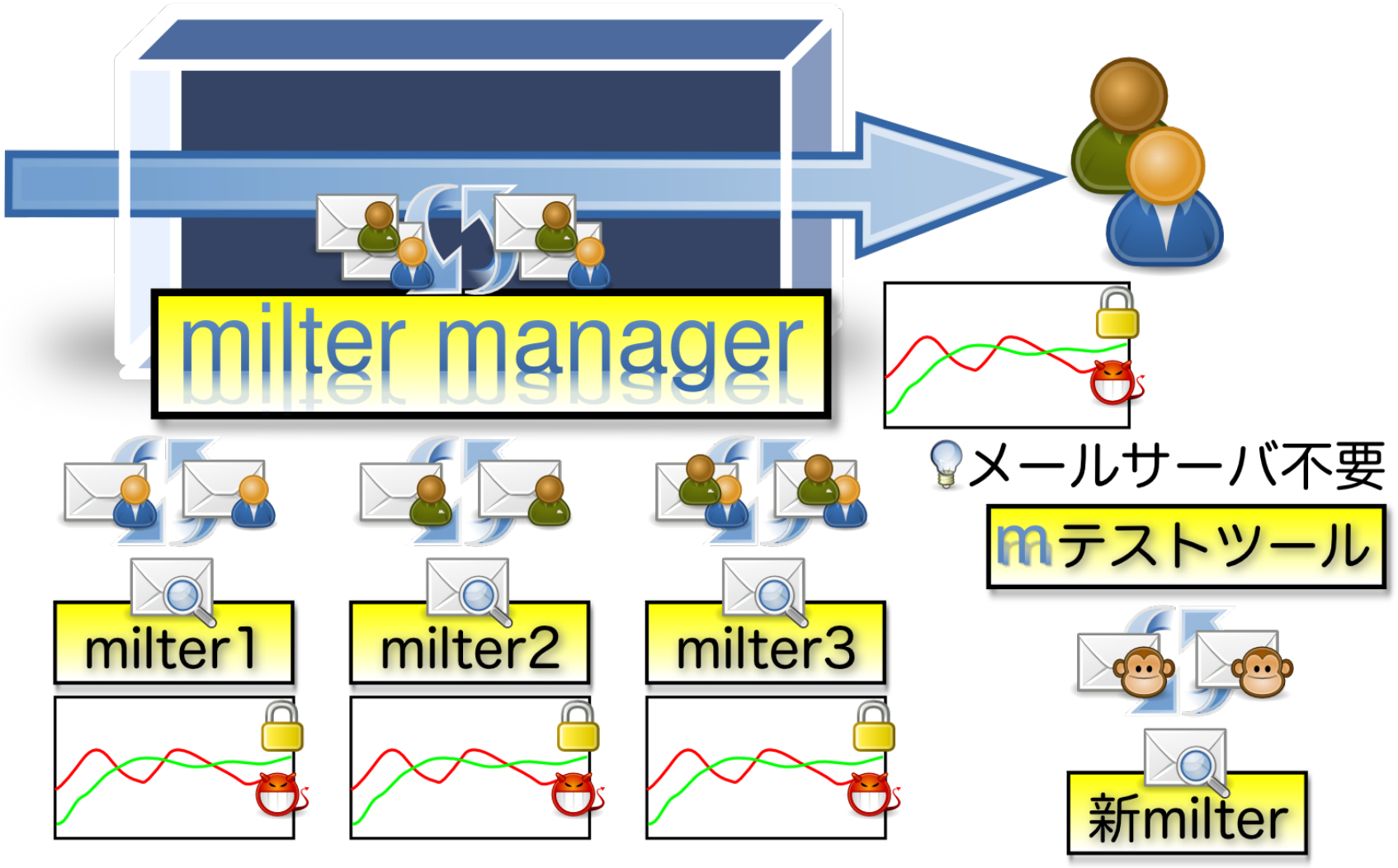
グラフ: 対策別結果


milter: report: milter-enma
mails/min
RRDTOOL / TOBI OETIKER
0
1
2
3
4
5
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
spam total: 0 mails avg: 0.00 mails/min max: 0 mails/min
Virus total: 0 mails avg: 0.00 mails/min max: 0 mails/min
URIBL total: 0 mails avg: 0.00 mails/min max: 0 mails/min
Greylisting (pass) total: 0 mails avg: 0.00 mails/min max: 0 mails/min
SPF (pass) total: 506 mails avg: 0.35 mails/min max: 15 mails/min
SPF (fail) total: 14 mails avg: 0.01 mails/min max: 2 mails/min
Sender ID (pass) total: 490 mails avg: 0.34 mails/min max: 15 mails/min
Sender ID (fail) total: 27 mails avg: 0.02 mails/min max: 2 mails/min
DKIM (pass) total: 33 mails avg: 0.02 mails/min max: 2 mails/min
DKIM (fail) total: 71 mails avg: 0.05 mails/min max: 2 mails/min
DKIM ADSP (pass) total: 33 mails avg: 0.02 mails/min max: 2 mails/min
DKIM ADSP (fail) total: 0 mails avg: 0.00 mails/min max: 0 mails/min
[2009-06-13T06:33:00+09:00]

運用

- ✓ 効果の確認・報告
- ✓ ユーザ毎に違う方法
- ✓ 新しいmilterの試験導入

運用支援


milter manager
メールサーバ不要
mテストツール
milter1
milter2
milter3
新milter

ポイント

- ✓ 段階的な導入を支援
- ✓ 効果を視覚化
- ✓ ユーザ毎の対策ON/OFF

そうか！

milter manager情報

- milterとmilter manager
- 対策の組み合わせ例
- milter manager
プラットフォーム
- milter manager情報

費用対効果

- 低費用
  - 500人×100通 = 50,000通/日
  - エントリクラスのサーバで十分
  - ライセンス料なし
- 検出率 > 90%
  - 既存の有効な方法を利用可能

インストール方法

- 情報:
  - http://milter-manager.sf.net/
  - milter-manager-users-ja@
- 対応環境
  - Ubuntu, CentOS, FreeBSD
  - おすすめ設定付き
    インストールマニュアル

モニター募集

- 無料提供:
  - 導入支援・サポート
- 協力してもらうもの:
  - アンケート・グラフ
- 静岡・北海道で10〜20社

クリアコード

低コストの迷惑メール対策は

http://www.clear-code.com/