milter manager

須藤功平

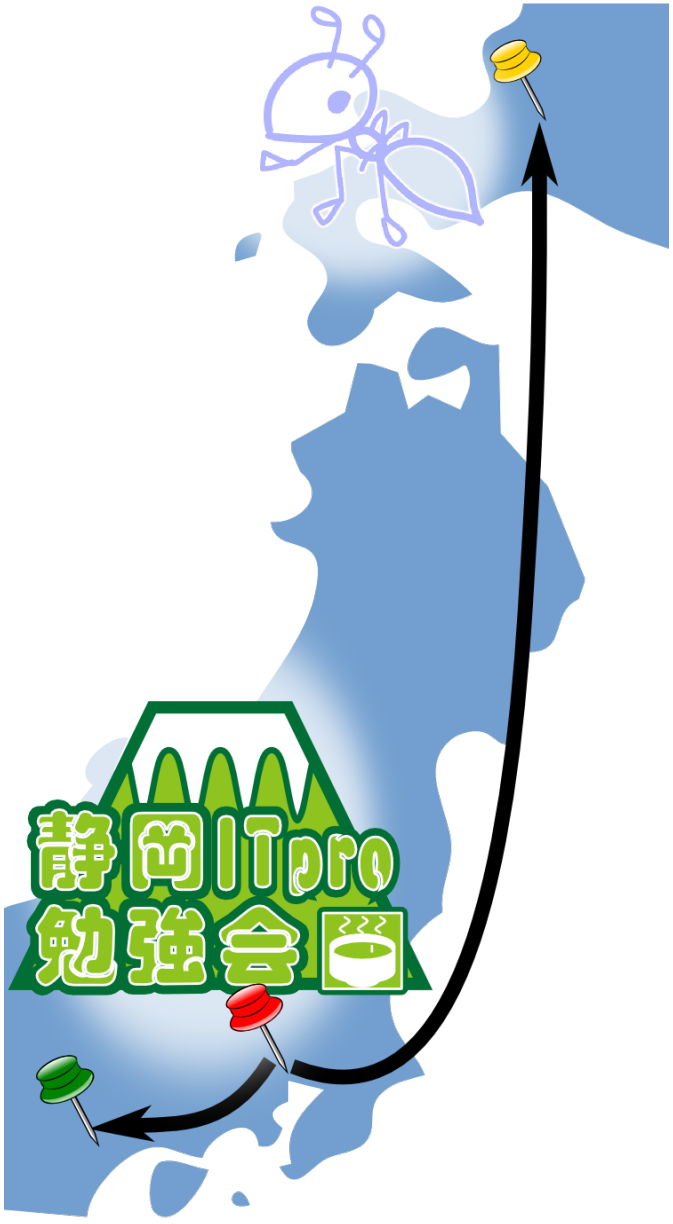
株式会社クリアコード

2009/06/20

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


静岡ITpro
勉強会

milter manager

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

話すこと

- ✓ 迷惑メールの現状
- ✓ 迷惑メール対策手法
- ✓ milter managerで対策
- ✓ milter manager情報

迷惑メールの現状

- 迷惑メールの現状
  - さとうさん感謝
- 迷惑メール対策手法
- milter managerで対策
- milter manager情報

現状概観

情報源: さとうさん、第7回迷惑メール対策カンファレンス

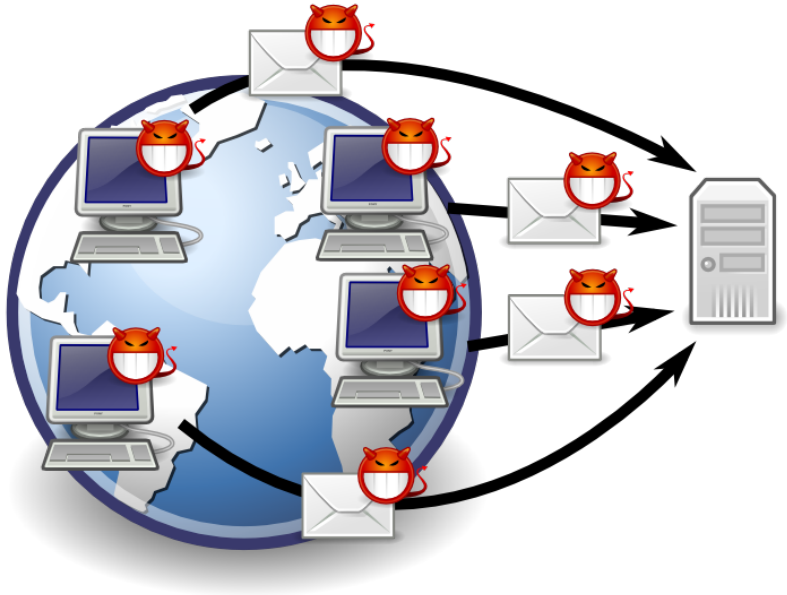
- ✓ 80%〜90%が迷惑メール
- ✓ 大規模ボットネットから送信
- ✓ 日本発は少ない

迷惑メール数

- 80%〜90%が迷惑メール
- 大規模な専門業者がいくつか
  - 2008/11: ある業者の通信を遮断
  - 迷惑メール激減: 数10%減

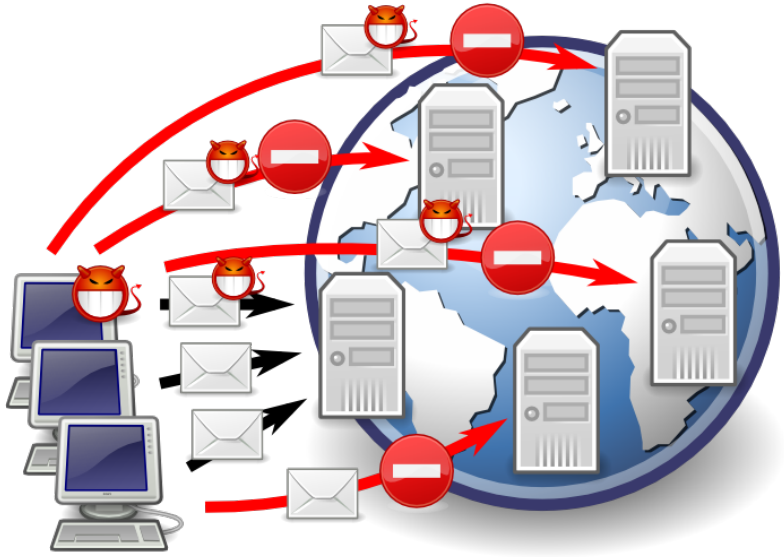
ボットネット

- 大規模ボットネットから送信
  - ボット: 乗っ取られた一般PC



日本発は少ない

- 一般PCからの送信を制限
  - 日本のISPの多くが実施



現状概観まとめ

情報源: さとうさん、第7回迷惑メール対策カンファレンス

- ✓ 80%〜90%が迷惑メール
- ✓ 大規模ボットネットから送信
  - ✓ ボット: 乗っ取られた一般PC
- ✓ 日本発は少ない
  - ✓ 一般PCからのメール送信を制限

迷惑メール対策手法

- 迷惑メールの現状
- 迷惑メール対策手法
  - さとうさん感謝
- milter managerで対策
- milter manager情報

前置き

情報源: さとうさん他

- 一長一短
  - 1つで完璧な対策はない
- 送信側も頑張っている
  - しばらくすると対抗策
  - まだ有効なものを紹介

ブラックリスト

- 送信ホストのIPアドレス
  - ボットが多くて対応できない
- 禁止ワード
  - 変形に弱い: 未承諾 → 未承認

送信ホストベース

- ブラックリストを共有
  - DNSベース
  - 検出率がまちまち・誤検出あり
- 一般PCっぽいものは怪しい
  - ボットが多いから
  - 検出率は高い・誤検出あり

禁止ワードベース

画像化に弱い

- ベイジアンフィルタ
  - 学習すれば効果が高い
  - 重い・言語依存
- 怪しいURLを共有
  - 重い・検出率はよい

ブラックリスト

- そのまま使うのは危険
- 救済措置と組み合わせ
  - Greylisting
- スコアとして利用
  - 統合型

Greylisting

- まともな送信者っぽいとOK
  - グレイ→ホワイト
  - ホワイトリスト作成が自動化
- 効果はある・誤検出もある
  - 落とし所: 怪しいときだけ実施

統合型

- 怪しさをスコア付け
  - 様々な手法を利用
- 効果・誤検出: トレードオフ
  - スコアの閾値次第: 無理はしない
- 重くなりがち
  - 利用する手法を選択して回避

おすすめのシステム

効果は高く

対策は多数

一長一短

優先するのは
こっち

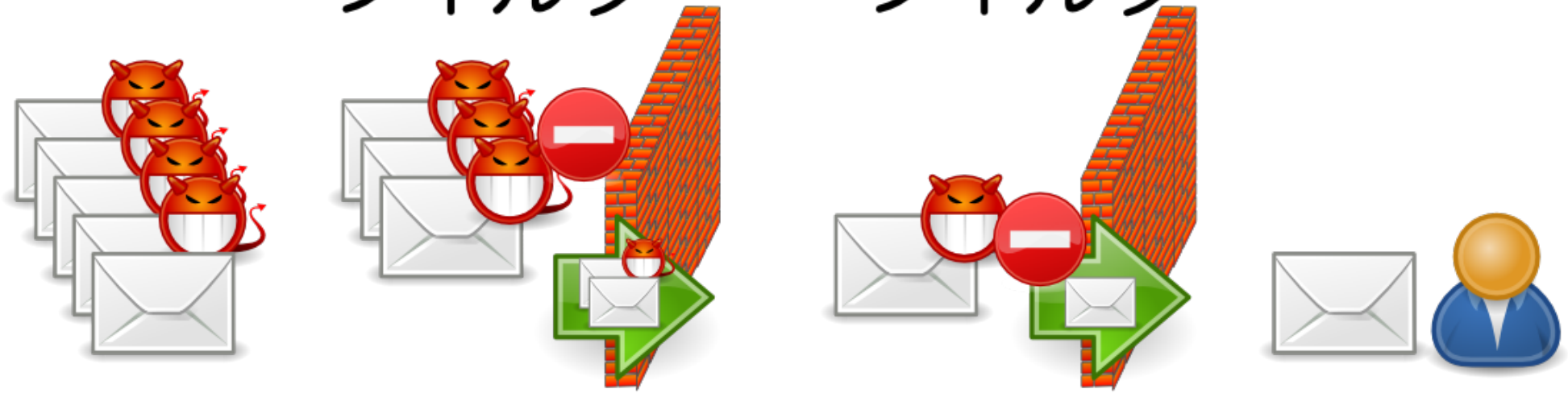
対策を連携

副作用は抑える

対策を連携

接続情報で フィルタ

内容まで見て フィルタ



80〜90%: 接続情報で検出

残りのさらに80〜90%: 内容で検出

対策手法のまとめ

- 手法はたくさんある
- 手法は組み合わせる
  - 1つで100%は無理
- 無理はしない
  - 検出率↑より誤検出↓

対策の実施

- ✓ 迷惑メールの現状
- ✓ 迷惑メール対策手法
- ✓ milter managerで対策
- ✓ milter manager情報

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とは？

1. メールフィルタの仕組み
2. メールフィルタの実装

特長:

- ✓ 汎用的: Sendmail/Postfix
- ✓ たくさんの実装

milter

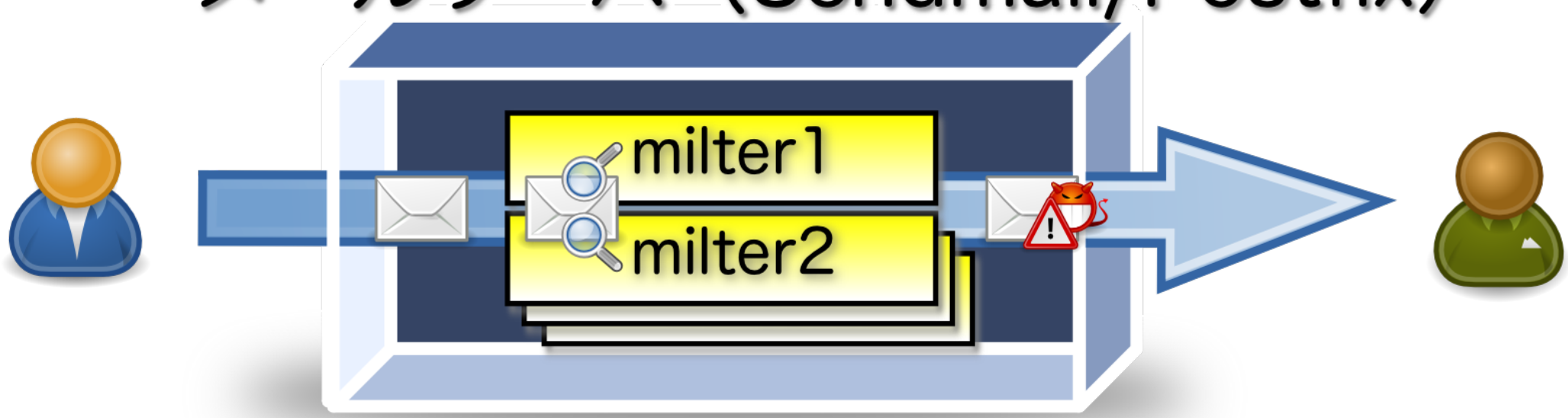
メールサーバ（Sendmail/Postfix）

milter: メールフィルタ

mail filter

プラグイン形式

メールサーバ（Sendmail/Postfix）

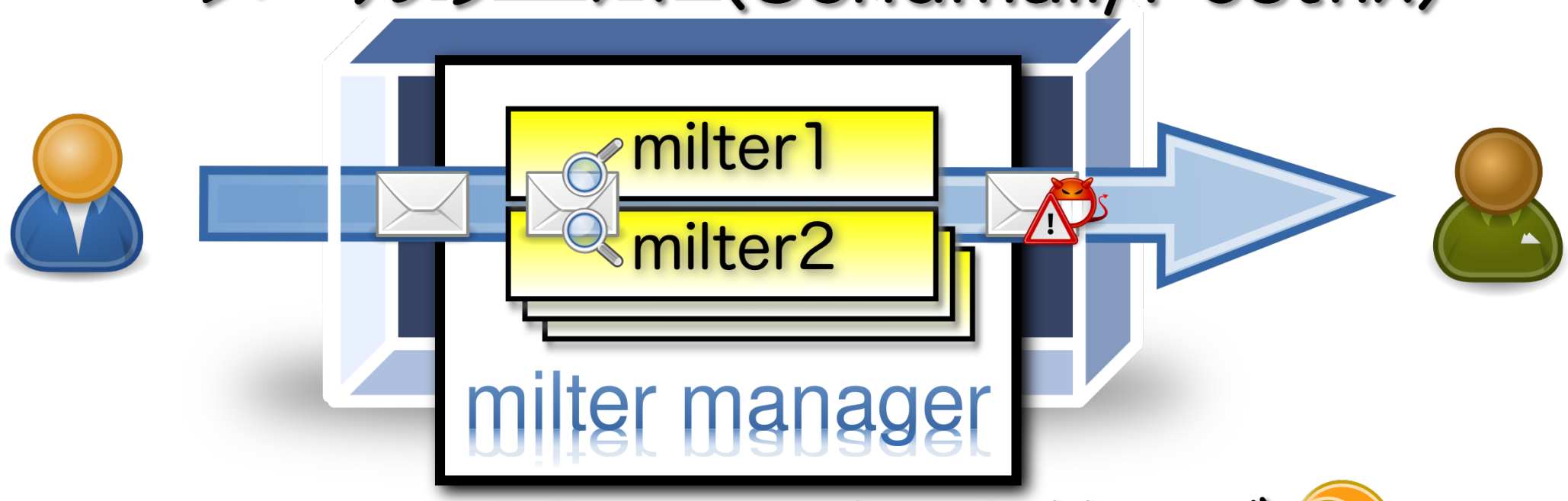


milter: プラグイン形式

対策の組み合わせが可能

milter manager

メールサーバ（Sendmail/Postfix）



milter管理: メールサーバ

milter manager

効果的にmilterを組合せ

強力なmilter管理

milter manager

- ✓ 強力なmilter管理機能
- ✓ システム管理支援機能

設定例

- おすすめ設定付き
  インストールマニュアル
- 対応環境
  - Ubuntu, CentOS, FreeBSD

システム管理支援

milter manager

- ✓ 強力なmilter管理機能
- ✓ システム管理支援機能

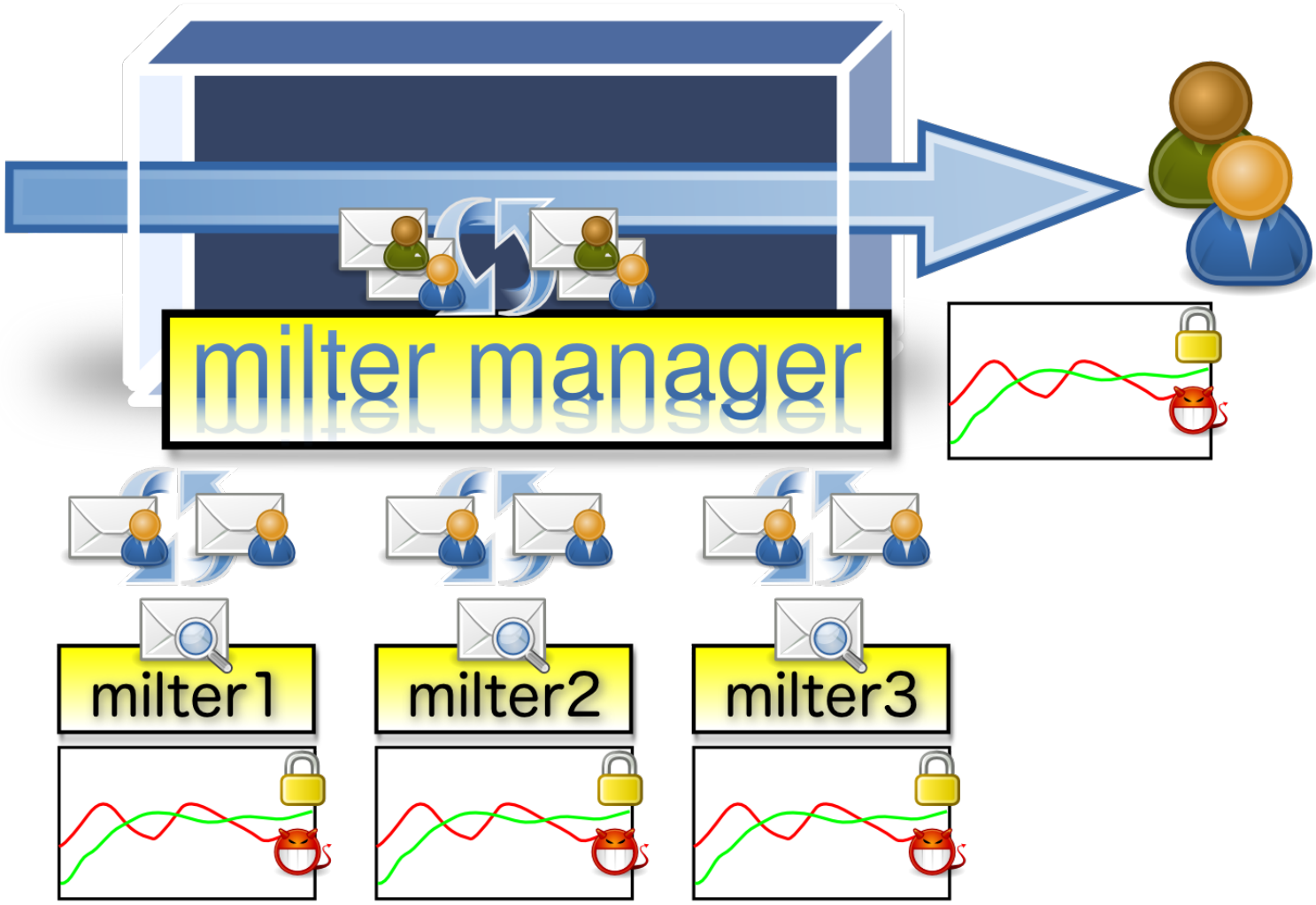
管理支援

- 導入
  - 試験導入支援
  - 導入効果測定
- 運用
  - 対策効果測定
  - 新対策の検証支援

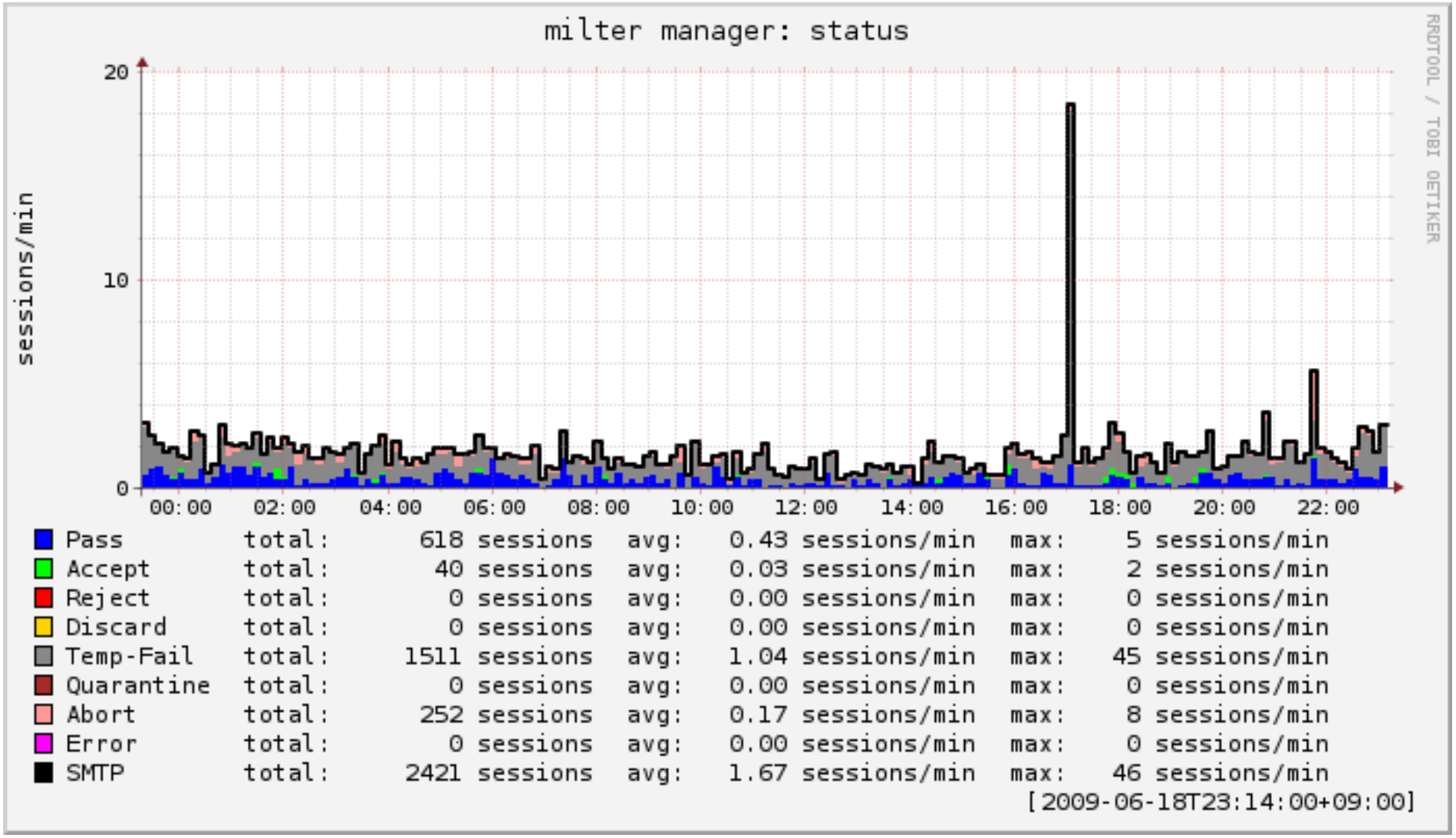
導入

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

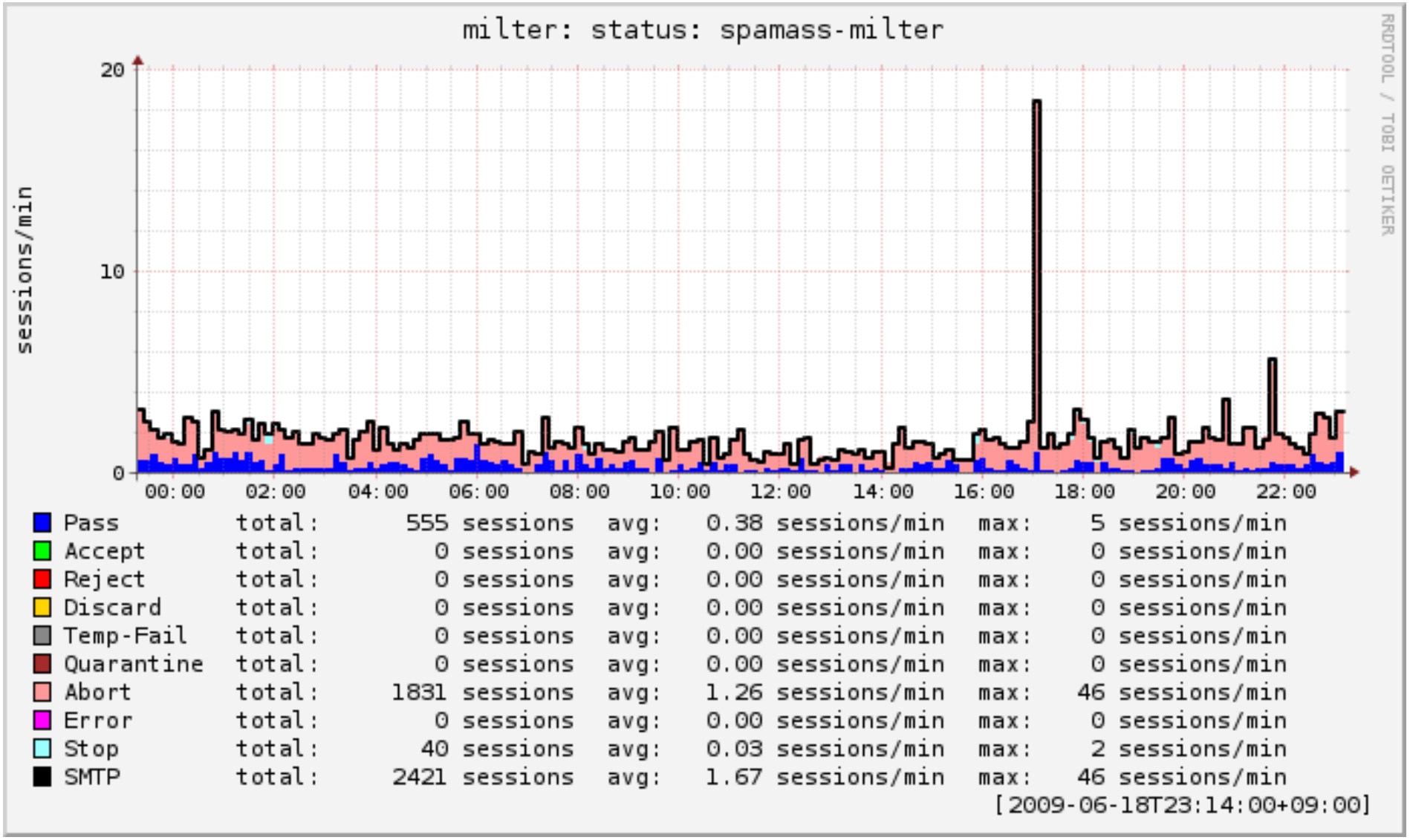
導入支援



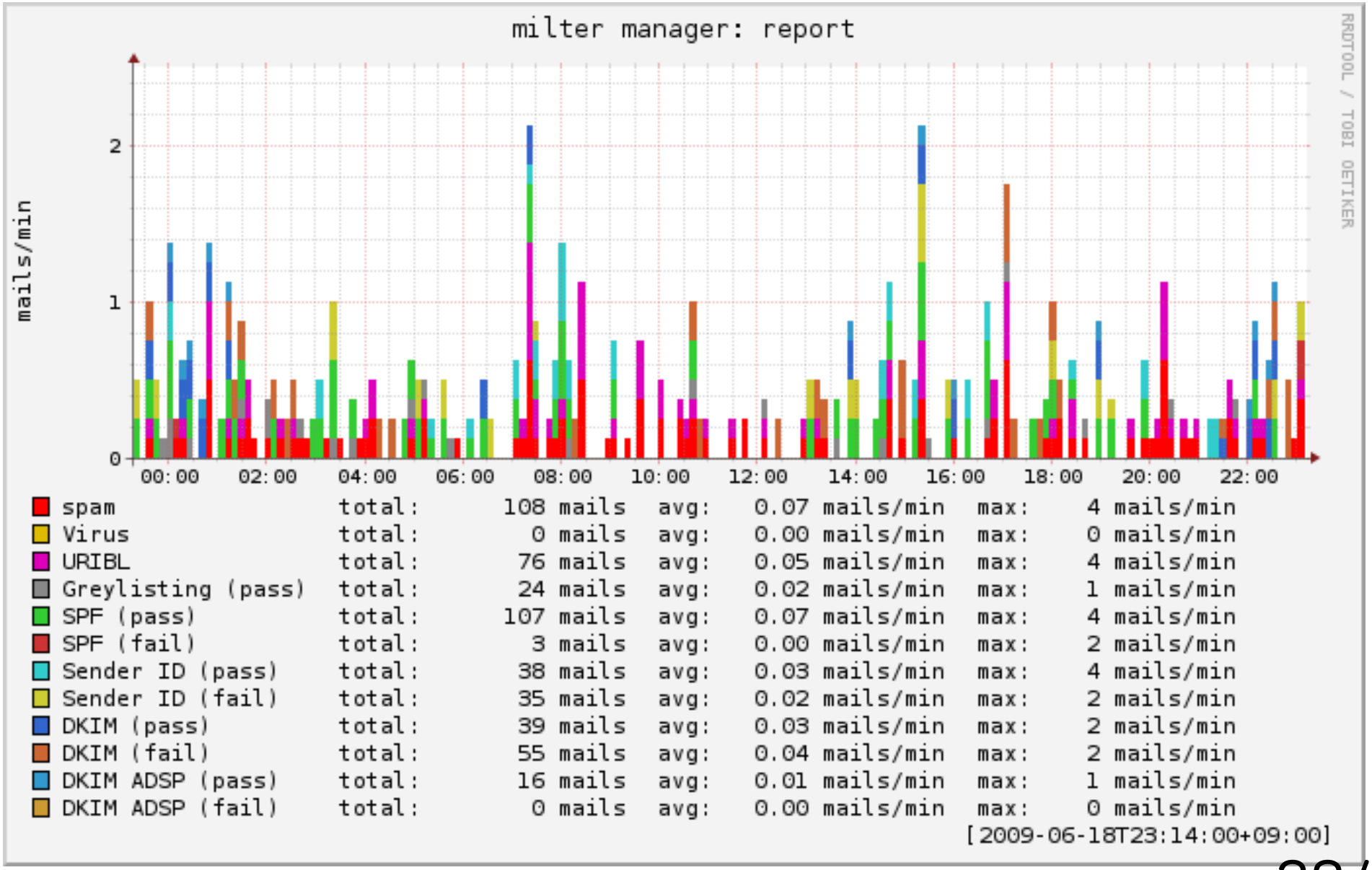
グラフ: 全体の結果


milter manager: status
sessions/min
20
10
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
RRDTOOL / TOBI OETIKER
Pass total: 618 sessions avg: 0.43 sessions/min max: 5 sessions/min
Accept total: 40 sessions avg: 0.03 sessions/min max: 2 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: 1511 sessions avg: 1.04 sessions/min max: 45 sessions/min
Quarantine total: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
Abort total: 252 sessions avg: 0.17 sessions/min max: 8 sessions/min
Error total: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
SMTP total: 2421 sessions avg: 1.67 sessions/min max: 46 sessions/min
[2009-06-18T23:14:00+09:00]

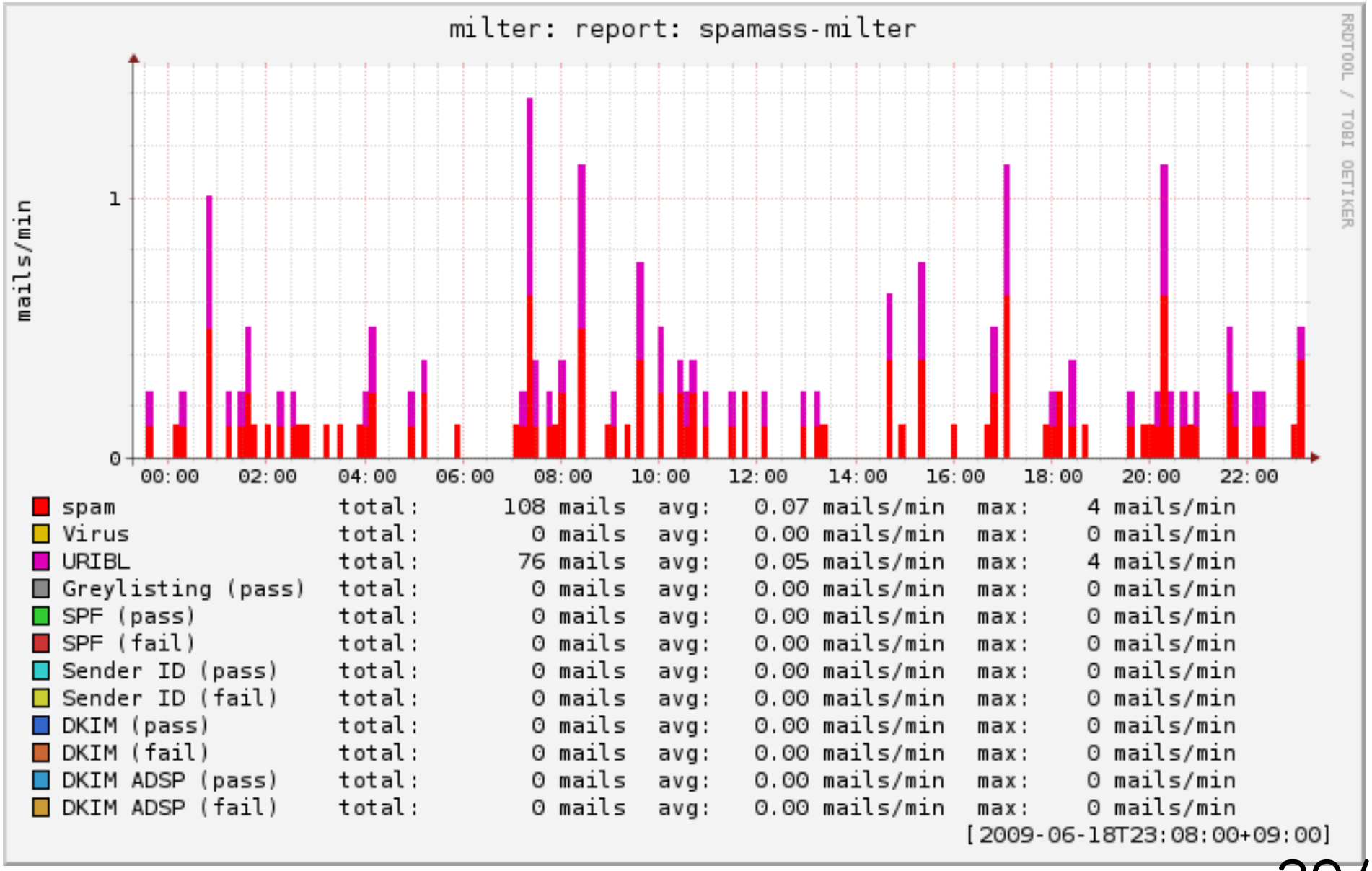
グラフ: 個々の結果


milter: status: spamass-milter
RRDTOOL / TOBI OETIKER
sessions/min
20
10
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
Pass total: 555 sessions avg: 0.38 sessions/min max: 5 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: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
Quarantine total: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
Abort total: 1831 sessions avg: 1.26 sessions/min max: 46 sessions/min
Error total: 0 sessions avg: 0.00 sessions/min max: 0 sessions/min
Stop total: 40 sessions avg: 0.03 sessions/min max: 2 sessions/min
SMTP total: 2421 sessions avg: 1.67 sessions/min max: 46 sessions/min
[2009-06-18T23:14:00+09:00]

グラフ: 対策結果


milter manager: report
mails/min
RRDTOOL / TOBI OETIKER
0
1
2
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
spam total: 108 mails avg: 0.07 mails/min max: 4 mails/min
Virus total: 0 mails avg: 0.00 mails/min max: 0 mails/min
URIBL total: 76 mails avg: 0.05 mails/min max: 4 mails/min
Greylisting (pass) total: 24 mails avg: 0.02 mails/min max: 1 mails/min
SPF (pass) total: 107 mails avg: 0.07 mails/min max: 4 mails/min
SPF (fail) total: 3 mails avg: 0.00 mails/min max: 2 mails/min
Sender ID (pass) total: 38 mails avg: 0.03 mails/min max: 4 mails/min
Sender ID (fail) total: 35 mails avg: 0.02 mails/min max: 2 mails/min
DKIM (pass) total: 39 mails avg: 0.03 mails/min max: 2 mails/min
DKIM (fail) total: 55 mails avg: 0.04 mails/min max: 2 mails/min
DKIM ADSP (pass) total: 16 mails avg: 0.01 mails/min max: 1 mails/min
DKIM ADSP (fail) total: 0 mails avg: 0.00 mails/min max: 0 mails/min
[2009-06-18T23:14:00+09:00]

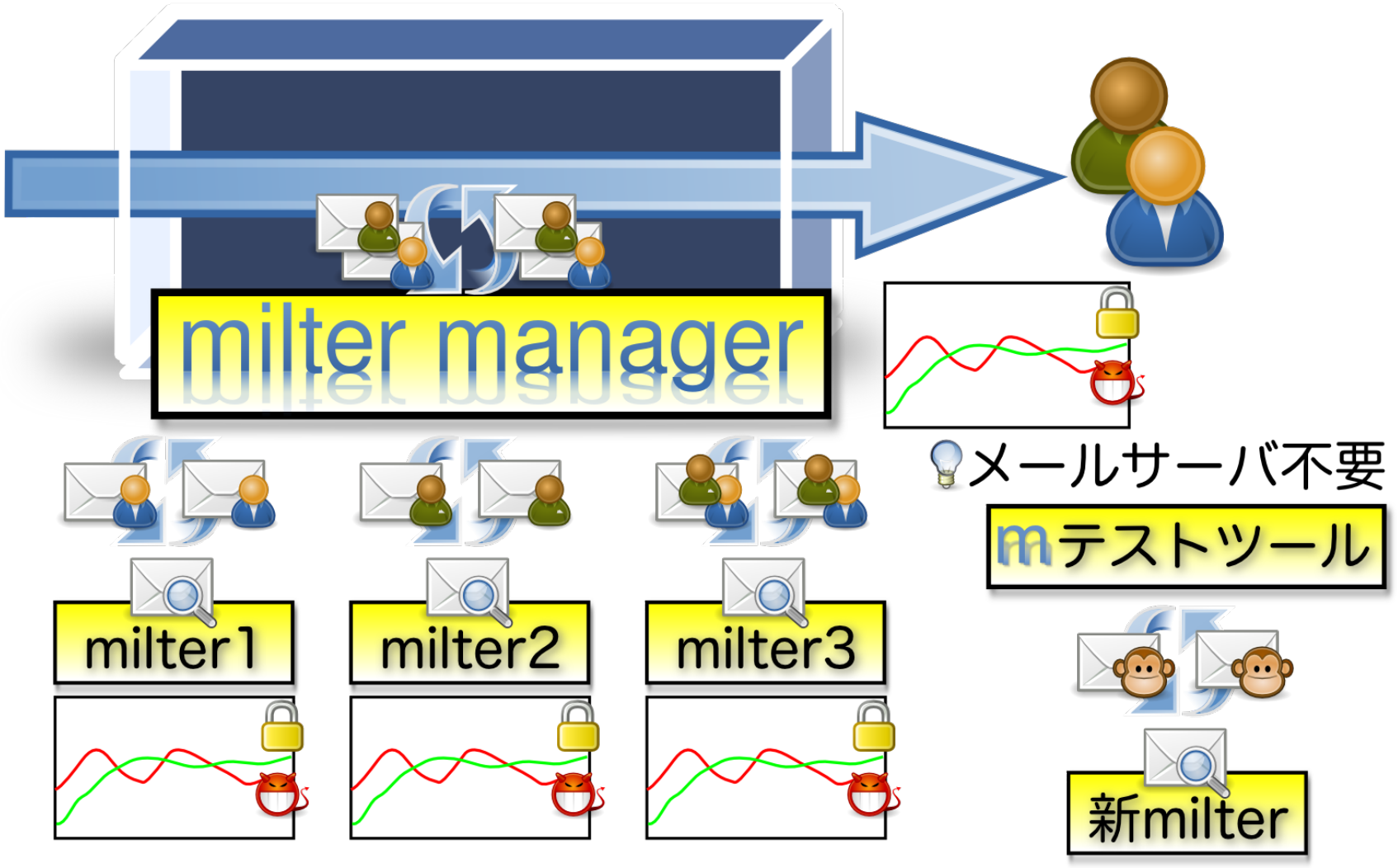
グラフ: 対策別結果


milter: report: spamass-milter
mails/min
1
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
RRDTOOL / TOBI OETIKER
spam total: 108 mails avg: 0.07 mails/min max: 4 mails/min
Virus total: 0 mails avg: 0.00 mails/min max: 0 mails/min
URIBL total: 76 mails avg: 0.05 mails/min max: 4 mails/min
Greylisting (pass) total: 0 mails avg: 0.00 mails/min max: 0 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
[2009-06-18T23:08:00+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

- ユーザ毎の対策ON/OFF
- 効果を視覚化
- → 段階的な導入を支援
- → 運用時の負担を削減

milter manager情報

- ✓ 迷惑メールの現状
- ✓ 迷惑メール対策手法
- ✓ milter managerで対策
- ✓ milter manager情報

費用対効果

- ✓ 低費用
  - ✓ ライセンス料なし
  - ✓ アカウント数に比例しない
- ✓ 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

有償サポート

安心が欲しい企業向け

- ✓ 導入支援
- ✓ サポート
  - ✓ 定期的な情報提供
  - ✓ 問い合わせ対応

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
- 北海道で2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/