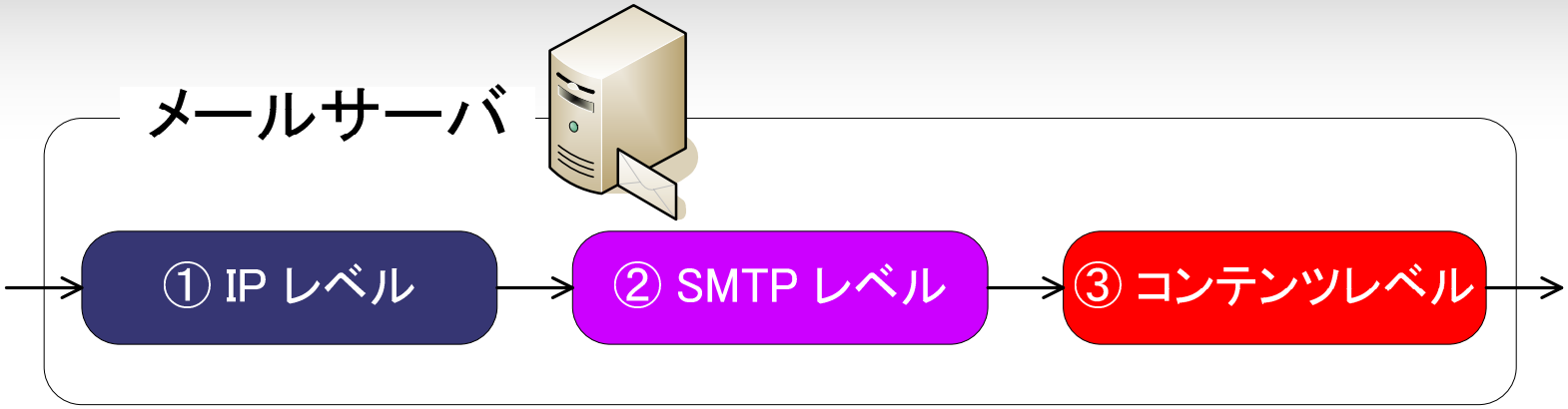
Rgrey 他によるスパム対策事例

株式会社 ネットフォレスト
植田　裕之<ueda@drweb.jp>

アジェンダ

- スパム対策の基礎(メールサーバ)
- Greylist と S25R、その問題点
- Rgrey
- HELO チェック
- コンテンツフィルタ

スパム対策の基礎（@メールサーバ）



① IP レベル

… IP blacklist, RBL, **S25R**, **Greylisting** etc.

② SMTP レベル

… HELO/Sender blacklist, Sender Check etc.

③ コンテンツレベル

… **Dr.WEB**, SpamAssassin etc.

負荷：低

負荷：高

IP レベルでの制御 – S25R(Selective SMTP Rejection)

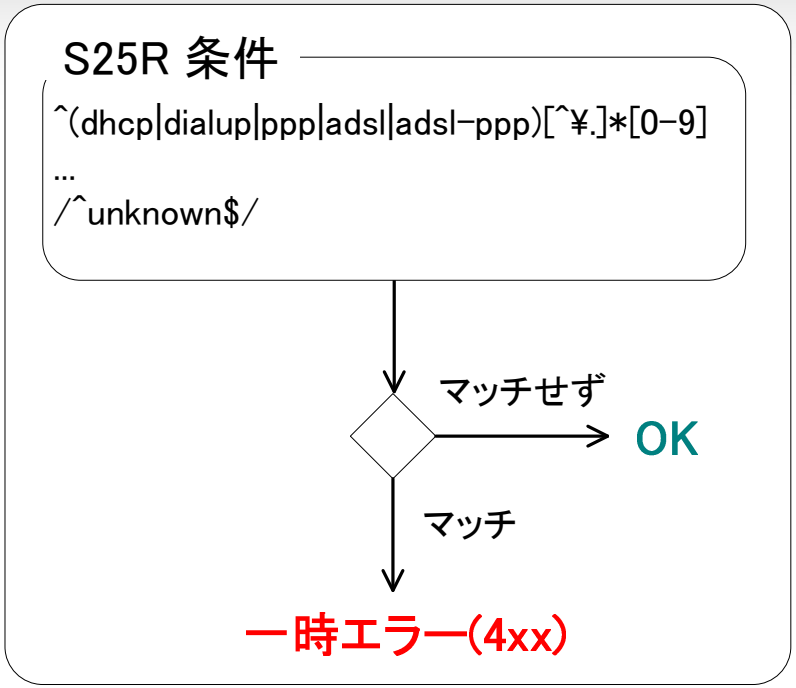
Net forest
Network × People

1. 逆引きできないクライアントを応答コード「450」（「後で再試行せよ」の意味）で拒否
2. 逆引き名からメールサーバでないと推定されるクライアントを応答コード「450」で拒否
3. 応答コード「450」による拒否に対して規則的に再試行する正当なメールサーバをホワイトリストで救済

http://www.gabacho-net.jp/anti-spam/

『正当なメールサーバは逆引き設定されている』、『動的 IP アドレスから送られるメールはスパム』という仮定に基づいている

S25R の動作イメージ



1. 接続元 IP アドレスを逆引き
2. 得られたホスト名をチェック
3. 条件にマッチしたら一時エラーで拒否

DNS の逆引き結果のみを判断材料とするため、コンテンツフィルタよりも低い負荷でスパムホストを排除可能

S25R の問題点

- 逆引きが設定されていないメールサーバが結構ある（セキュリティポリシー？）
- 真っ当なところでも S25R 条件にマッチしてしまうホストが結構ある（フレッツの逆引きサービスを提供しないISPは多い）

ログを定期的にチェックして正常なホストを救済するためにホワイトリストの管理が必須（やらないと一時エラーから永遠に救済されない＝拒否と同じ）

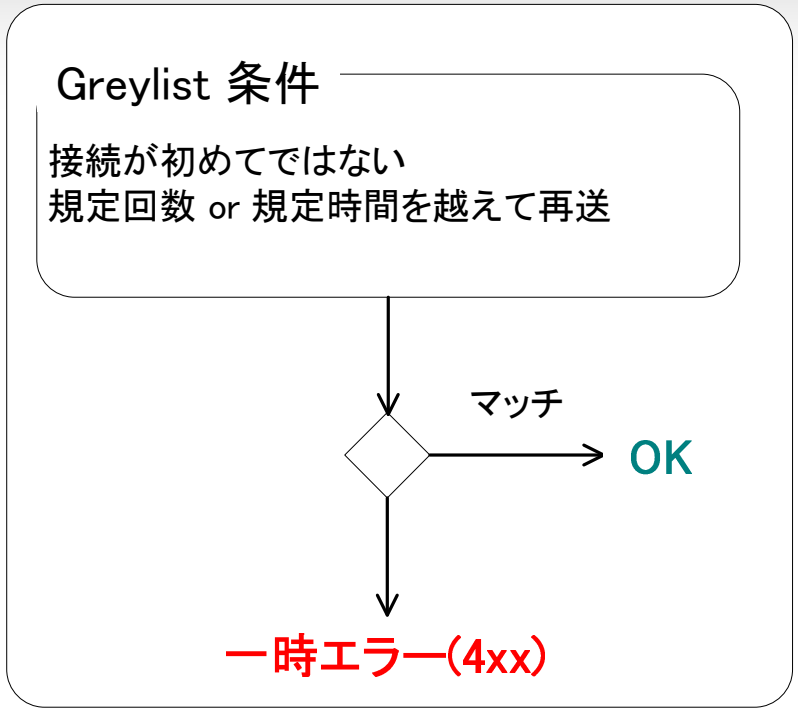
IP レベルでの制御 - Greylisting（一見さんお断り方式）

Net forest
Network × People

1. 接続してきた相手の IP アドレスを確認し、初めての相手であれば一時エラー（4xx）を返す
2. 規定回数 and/or 規定時間になるまで一時エラーを繰り返す
3. クリアしたら接続を受け付けて処理を行い、一時リストに IP アドレスを登録
4. 規定時間経過後、一時リストから削除

『ボットネットはあまり再送してこない』、『正常な MTA は一定回数の再送信を試みる』という特徴を利用している

Greylisting の動作イメージ

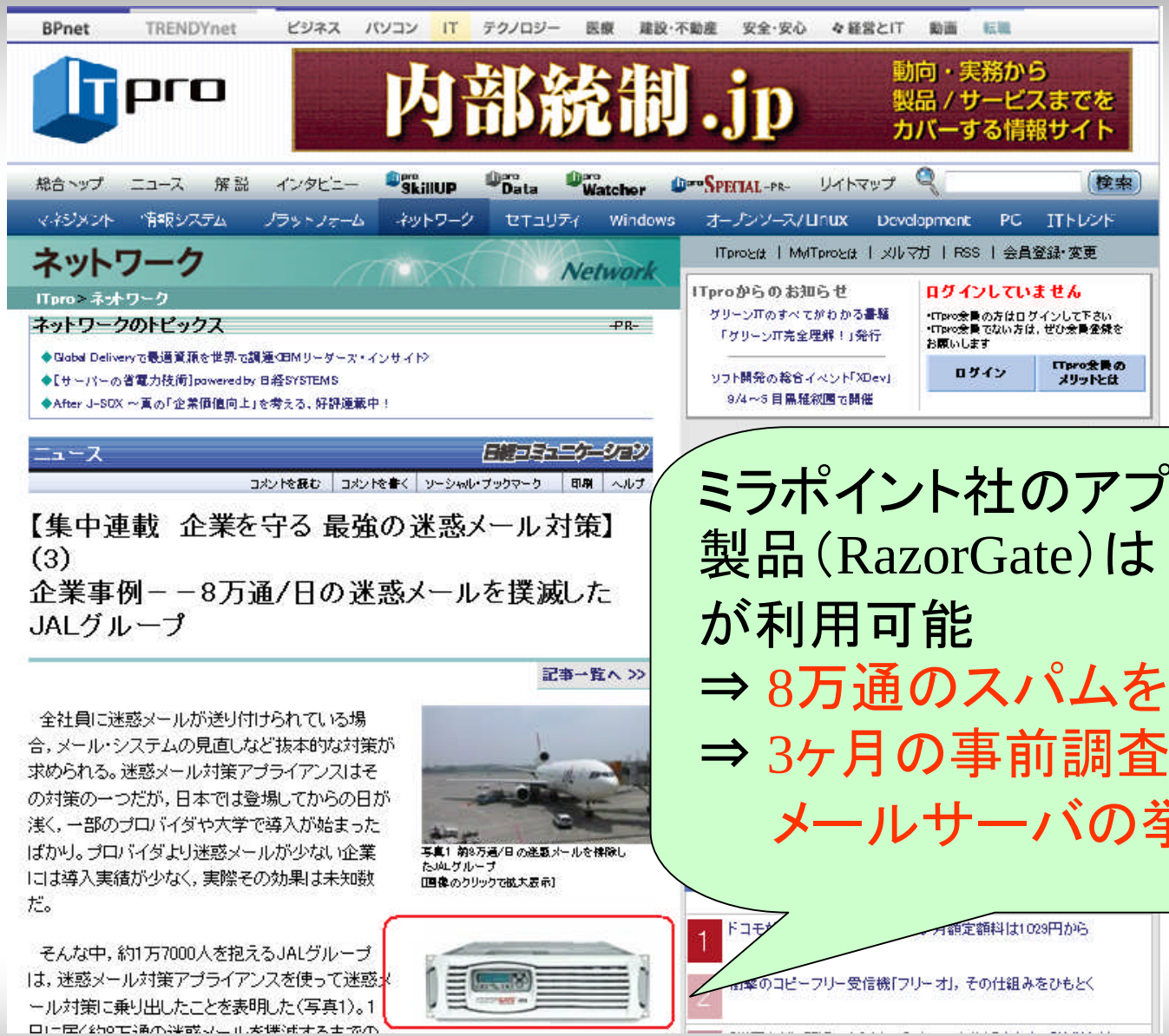


1. 接続元 IP アドレスがデータベースにあるかチェック
2. あれば処理を継続
3. なければデータベースに登録した後、一時エラーで拒否

送信元 IP アドレスとその接続試行時期・回数などを判断材料とするため、コンテンツフィルタよりも低い負荷でスパムホストを排除可能

Greylisting の導入事例 – JAL グループ

Net forest
Network × People



ミラポイント社のアプライアンス製品（RazorGate）は Greylisting が利用可能

⇒ 8万通のスパムを半減

⇒ 3ヶ月の事前調査（取引先メールサーバの挙動確認）

http://itpro.nikkeibp.co.jp/article/NEWS/20051115/224650/

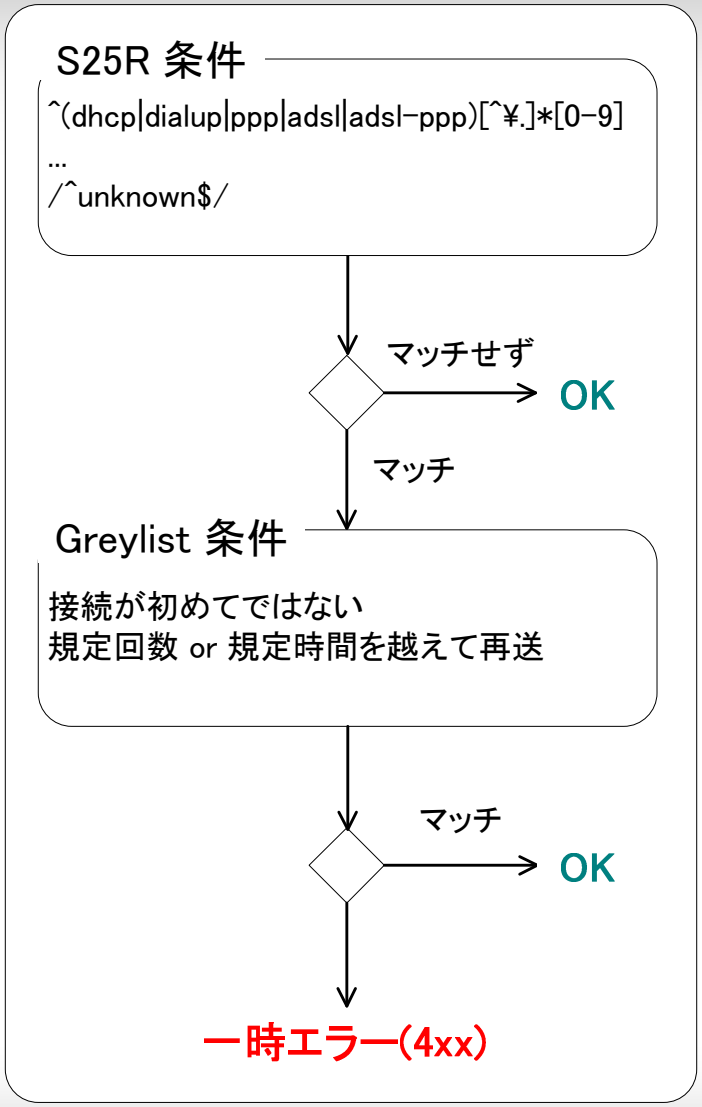
Greylisting の問題点

Net forest
Network × People

- 初めてメールを送ってきたホストの場合、必ずメールが遅延する
- ホワイトリスト未登録のホストの場合、一定時間経つと一からやり直しになる

ログを定期的にチェックし、誤って greylisting されているホストを救済するためにもホワイトリストの管理が必須（やらないと配送遅延が発生する可能性が高い）

IP レベルでの制御 – Rgrey(S25R + Greylisting)



1. 接続元 IP アドレスを逆引きし、得られたホスト名をチェック（S25R 条件）
2. S25R 条件にマッチした場合、Greylist 条件をチェック

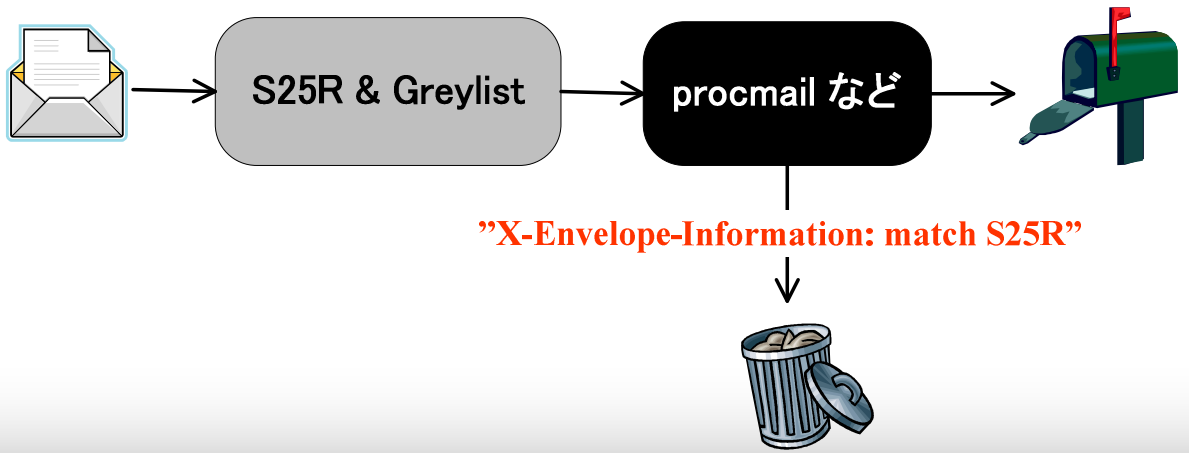
二つの条件を満たした場合のみ一時エラーで拒否する（AND 条件のため誤判定が少ない）

http://k2net.hakuba.jp/rgrey/

IP レベルでの制御 – Rgrey(S25R + Greylisting) つづき

S25R にマッチ && Greylisting を通過したメールには X- ヘッダを付加すれば、後段プログラム（procmail や MUA）の機能でフィルタ可能

X-Envelope-Information: match S25R
Received: from webservicefeature.info (**unknown** [216.151.155.63])
by foo.drweb.jp (Postfix) with SMTP id A5B7CEF8049
for <Ueda@drweb.jp>; Tue, 26 Aug 2008 12:02:32 +0900 (JST)



Rgrey の実装

Net forest
Network × People

Postfix + Postgrey が最もメジャー

FreeBSD なら両方とも ports にある

- mail/postfix
- mail/postgrey

cf. postfix 以外での Rgrey 実装例

sendmail … scam-grey（`http://www.elandsys.com/scam/scam-grey/`）

qmail … Qgrey（`http://k2net.hakuba.jp/qgrey/`）

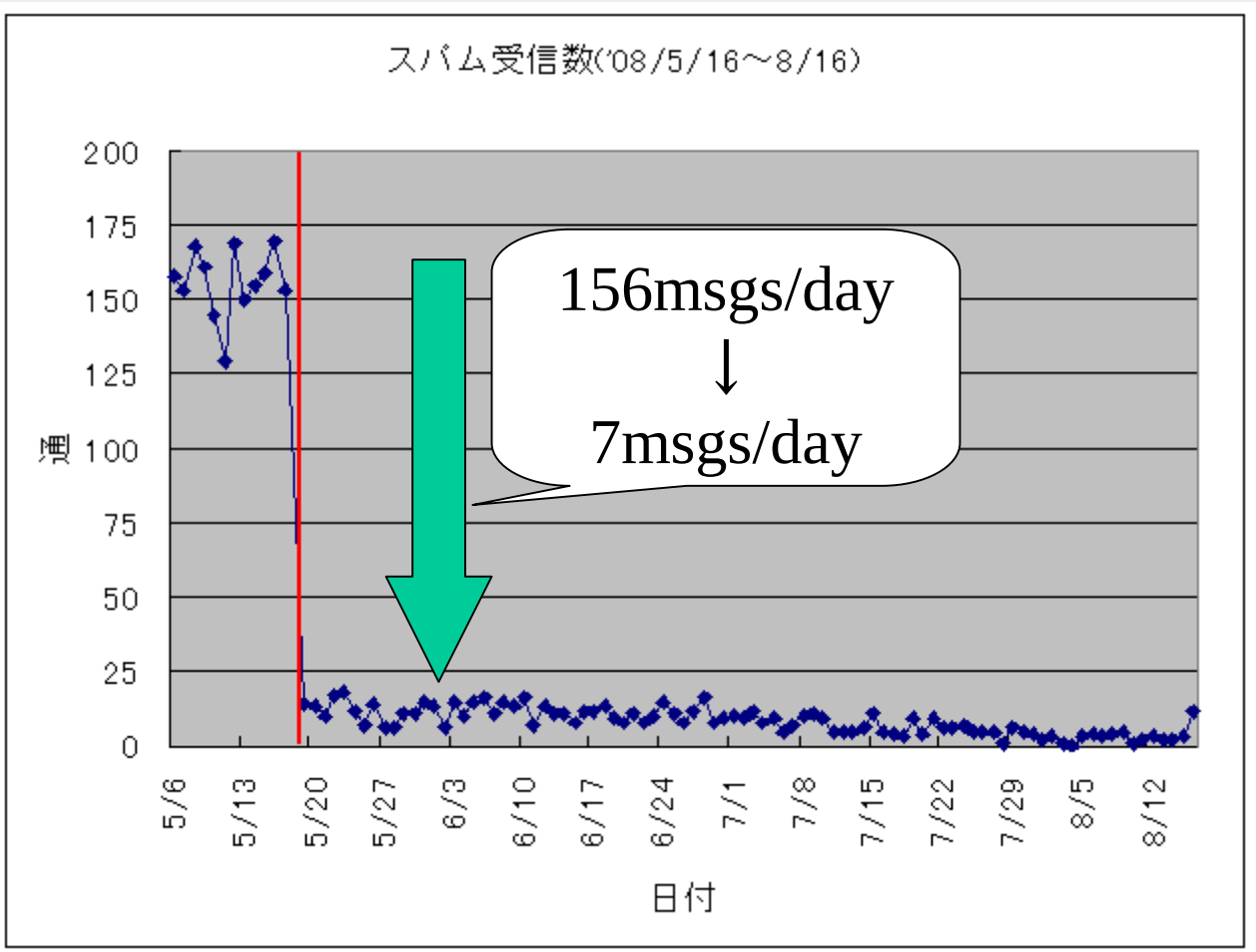
※ Qgrey はコードを見る限り、実運用はちょっと微妙…

Rgrey の実装（検証環境）

最もメジャーな構成の某サーバで実運用中

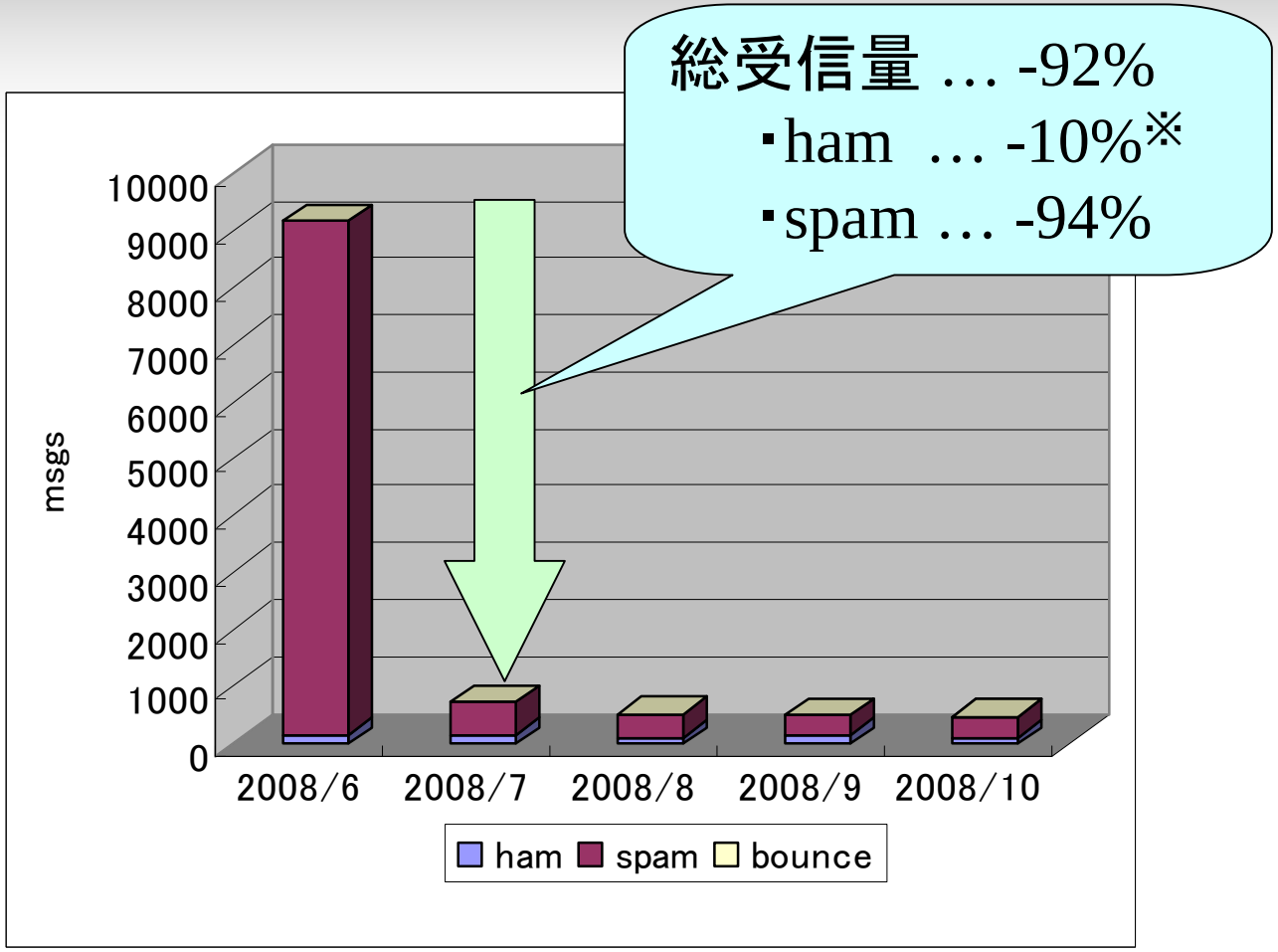
- OS　　… CentOS 5.2
- MTA　　… **Postfix**（2.3.3-2.1.el5_2）
- Greylist　… **Postgrey**（1.31-1.el5.rf）
- 評価対象 … 個人ドメイン（’98年取得）の以下のアドレス
  - ✓ webmaster 他 3個（ ほぼスパム受信専用アドレス）
  - ✓ 担当者アドレス（10年以上使用しており、かなりのスパム被害）

Rgrey の効果（webmaster@... など宛）



95%強のスパムを排除することに成功！

Rgrey の効果 つづき（担当者のアドレス）



メールボックスに入るメールの総量が大幅減（選別容易に）

※ ML の流量が少ないなどの理由（誤排除ではない）

ホワイトリスト・ブラックリストのメンテナンス

Net forest
Network × People

ホワイトリスト …チケットぴあ（pia.jp）、google の 2回対応

- チケットぴあは遅配
- google（Google Apps?）は別ルールにマッチして拒否 orz

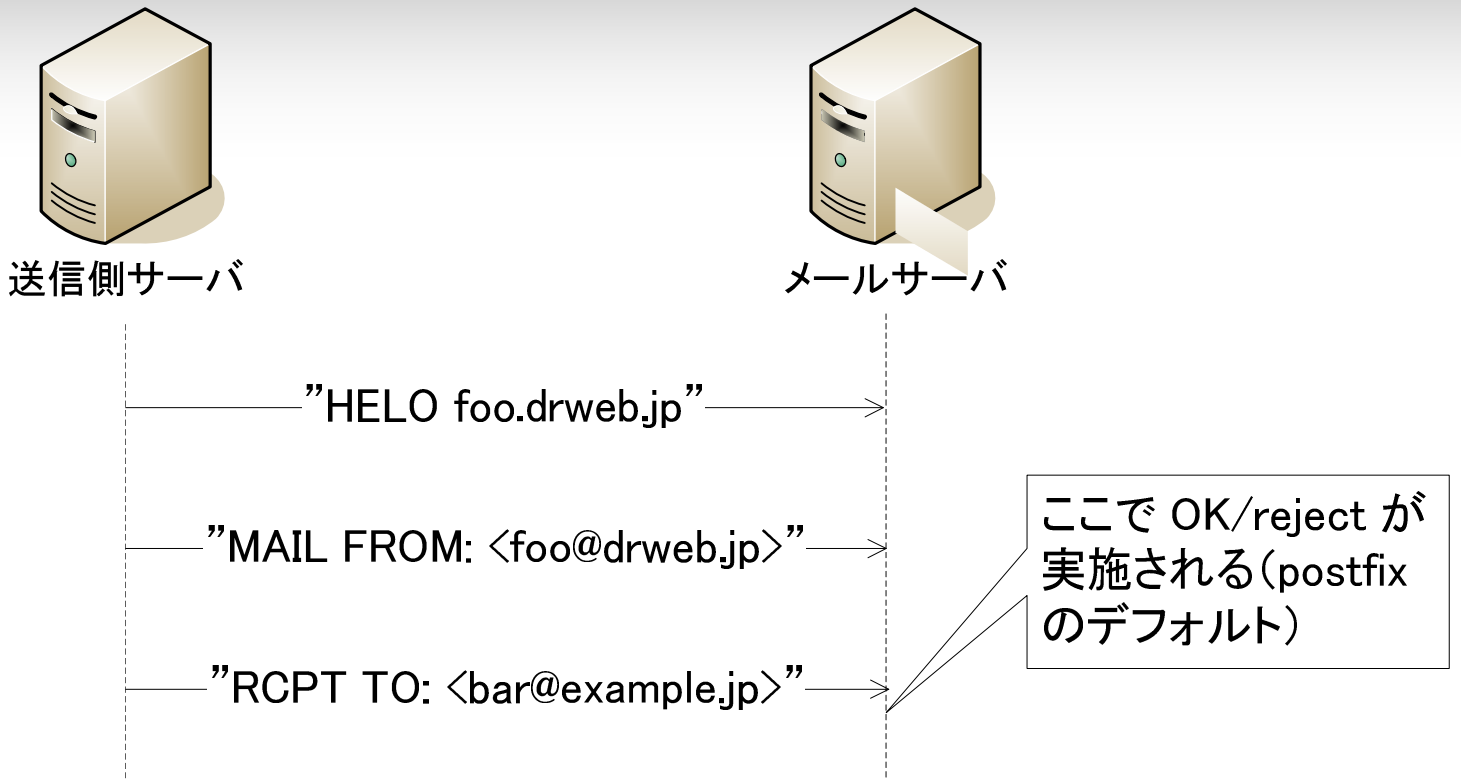
ブラックリスト … 最初の1ヶ月で数回程度

- 後はたまに追加する程度
- 細かく詰めてもあまり意味が無い

ほぼメンテナンスの必要なし

柔軟な設定が可能（Rgrey on Postfix の場合）

Net forest
Network × People



送信者の IP アドレスだけではなく、送・受信者のアドレスもホワイトリストで利用可能（= 個別 on/off 可）

※ smtpd_delay_reject = yes の場合の挙動

※ Qgrey だと接続段階で処理するため、送受信者情報が取れない

柔軟な設定が可能（Rgrey on Postfix の場合）つづき 1

Net forest
Network × People

```
Aug 27 09:51:13 test postfix/smtpd[8164]: NOQUEUE:
reject: RCPT from unknown[121.33.213.253]: 450 4.2.0 <
ueda@drweb.jp >: Recipient address rejected:
Greylisted, see
http://postgrey.schweikert.ch/help/drweb.jp.html;
from=<xxxxxx@veriserve.co.jp> to=<ueda@drweb.jp>
proto=ESMTP helo=<[121.33.213.252]>
```

/var/log/maillog

```
% geoiplookup 121.33.213.253
GeoIP Country Edition: CN, China — 中国の IP アドレス
% host veriserve.co.jp
veriserve.co.jp has address 210.150.254.86
% geoiplookup 210.150.254.86
GeoIP Country Edition: JP, Japan — 日本の IP アドレス
```

cf. net/GeoIP

事後対応に必要な全情報の記録後に切断

柔軟な設定が可能（Rgrey on Postfix の場合）つづき 2

Net forest
Network × People

language: english | spanish

Postgrey Help

You came here probably after seeing a mail of yours being rejected with a message like this:

```
Greylisted for 300 seconds (see http://postgrey.schweikert.ch/help)
```

The mail server generating this error message is using a system called *Greylisting* to filter spam and viruses. It relies on Mail Servers behaving according to the standards and usually doesn't require any action by the user. Your mails should only possibly be delayed.

If you see this error message while sending a mail, it probably means that you did something wrong: the configured mail server should trust your machine and thus not apply greylisting at all.

Make sure that you did turn on encryption and authentication for the SMTP server in your mail client. Ask your system administrator if you are not sure about how to configure it.

See this page for a description about how Greylisting works.

Who to contact in case of problems

By the URL (web address) that you used, it can be deducted that you had problems when sending a mail to *somebody@dnweb.jp*. The right contact-address for problems with the *dnweb.jp* domain is **postmaster@drweb.jp**.

Return to the Postgrey homepage.

http://postgrey.schweikert.ch/help/drweb.jp.html

Rgrey の問題点

Net forest
Network × People

- 真っ当な逆引き設定のあるホストはフィルタできない

  「95% の残り 5% をどこまで IP/SMTP レベルで弾くのか？」

- IPv6 になったらどうなる？

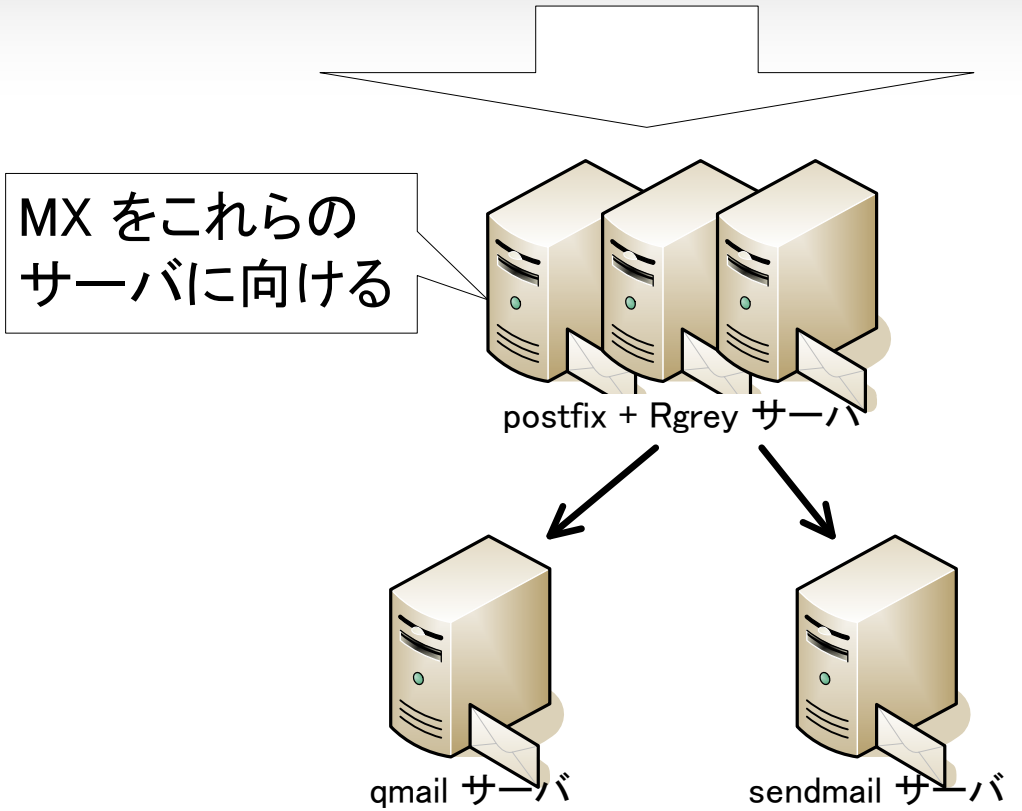
  「逆引き設定が IPv4 より面倒になるので、サーバ以外は全部 unknown」とかだとベストだけど

- 一度しか送信してこない S25R なホストは救えない

  Web フォームからの送信メールなど（筋が悪すぎ…？）

複合的なスパム対策で更に弾く・検出することは可能

提案：postfix 以外のメールサーバを使っているなら…



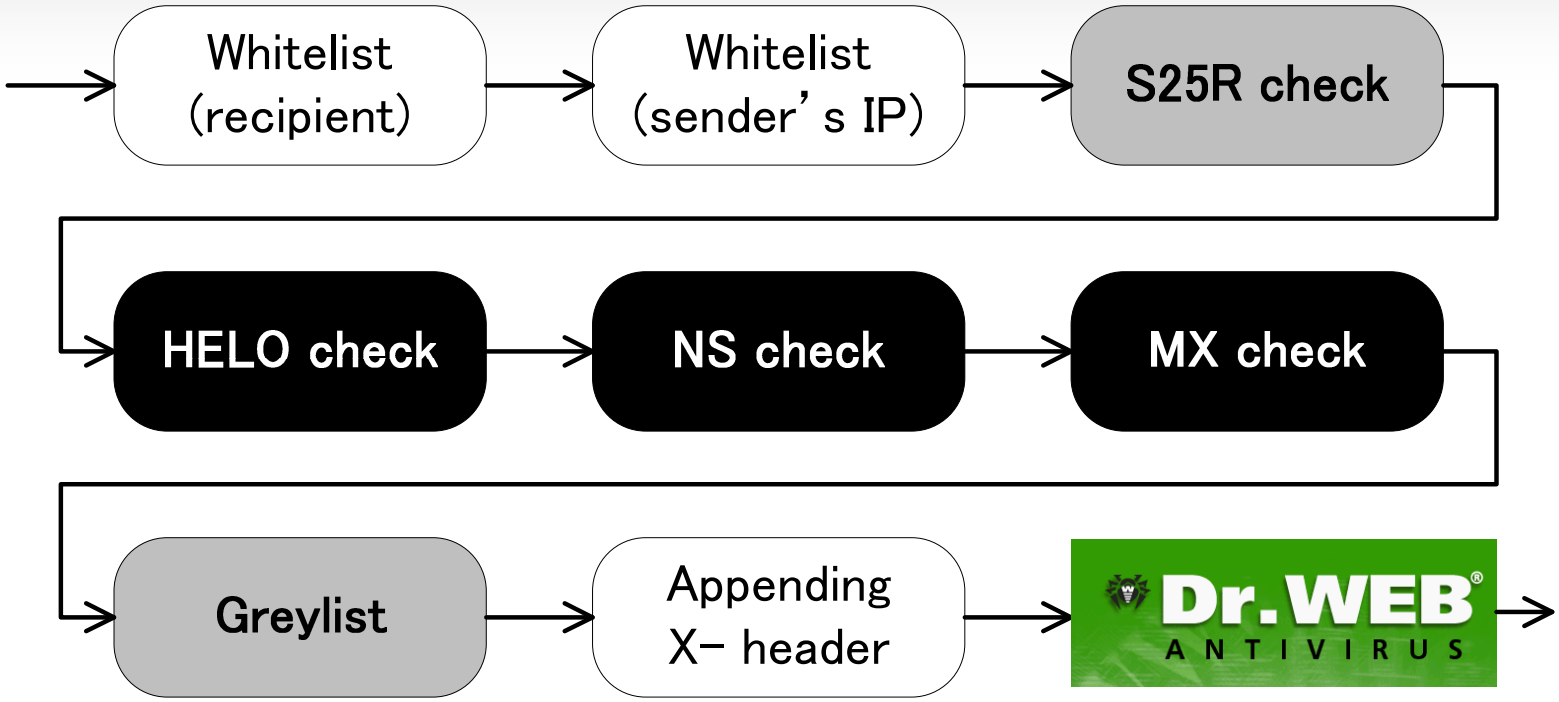
Tips: 後段 MTA が sendmail などであれば

```
smtpd_recipient_restrictions =
        …
        reject_unverified_recipient
```

すると存在しないアドレス宛のメールも Rgrey サーバでブロック可能

『2nd MX としてテスト導入 ⇒ 全 MX に適応』など、
上手くやればスムーズに導入可能と思われる

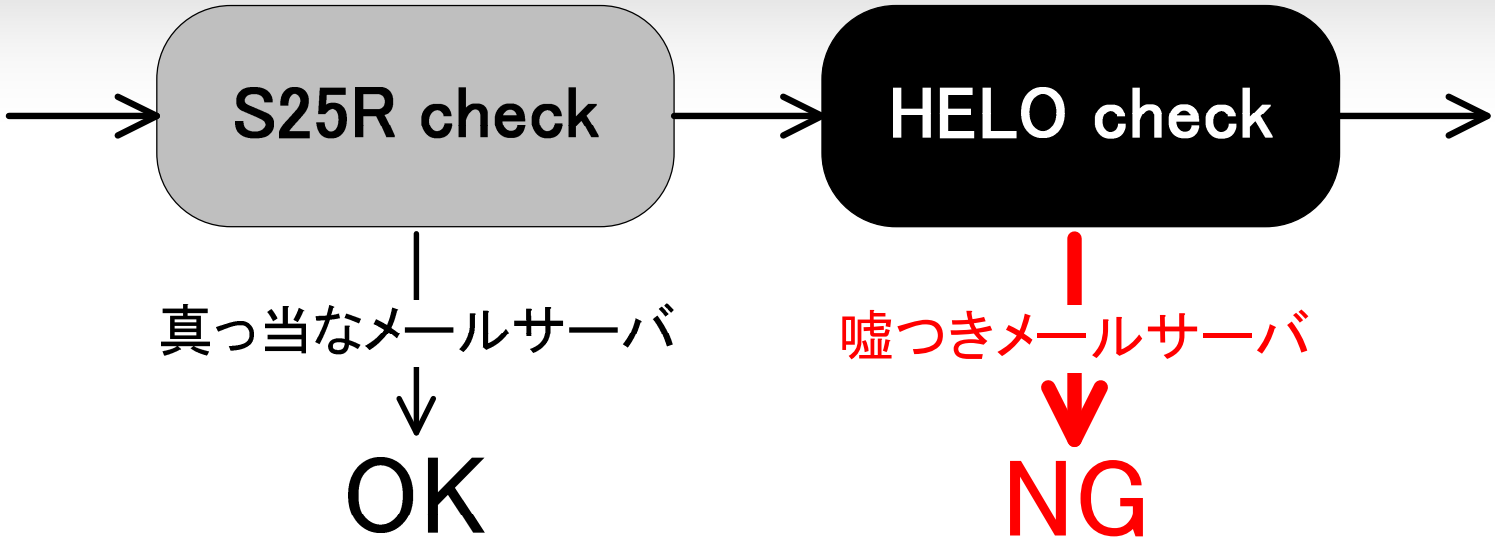
実際のスパム対策



最終段で初めてコンテンツフィルタ(Dr.WEB Antivirus + Antispam)が処理するため、負荷が最低限で済む

※ DNS の頑張り重要 ー dnscache(djbdns) が good

SMTP レベル - HELO check はかなり効く – 1/2

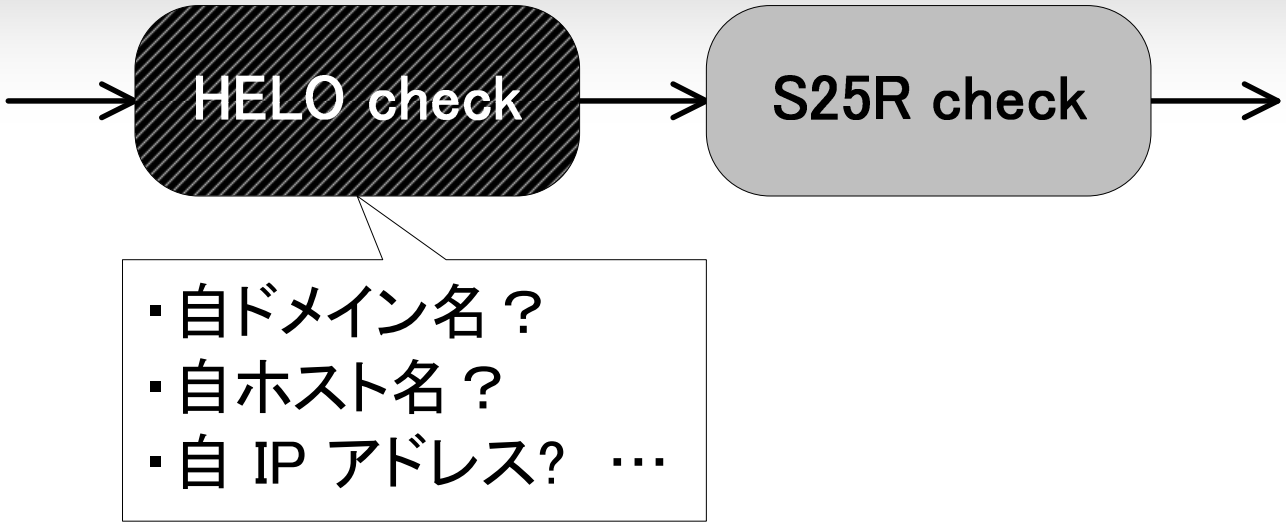


大手 xSP を HELO/EHLO で騙る S25R なホストは一網打尽

〇例：8/3～8/10 の間の拒絶数

yahoo.co.jp	… 53回
a-net.ne.jp	… 26回
mail.goo.ne.jp	… 22回
infoseek.jp	… 16回

SMTP レベル - HELO check はかなり効く – 2/2



自ドメイン名や自ホスト IP アドレスを名乗るホストは一網打尽

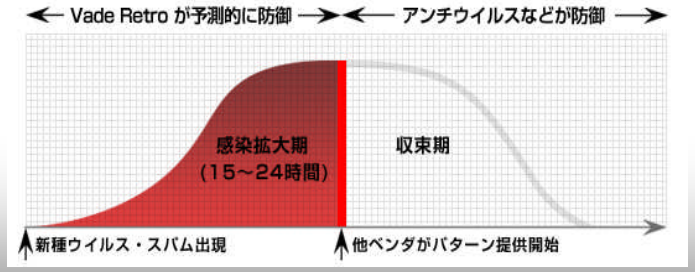
〇例 : 8/3～8/10 の間の拒絶数

ドメイン名	… 13 回
ホスト名	… 0 回
MX 名	… 26 回
IP アドレス	**… 142 回**

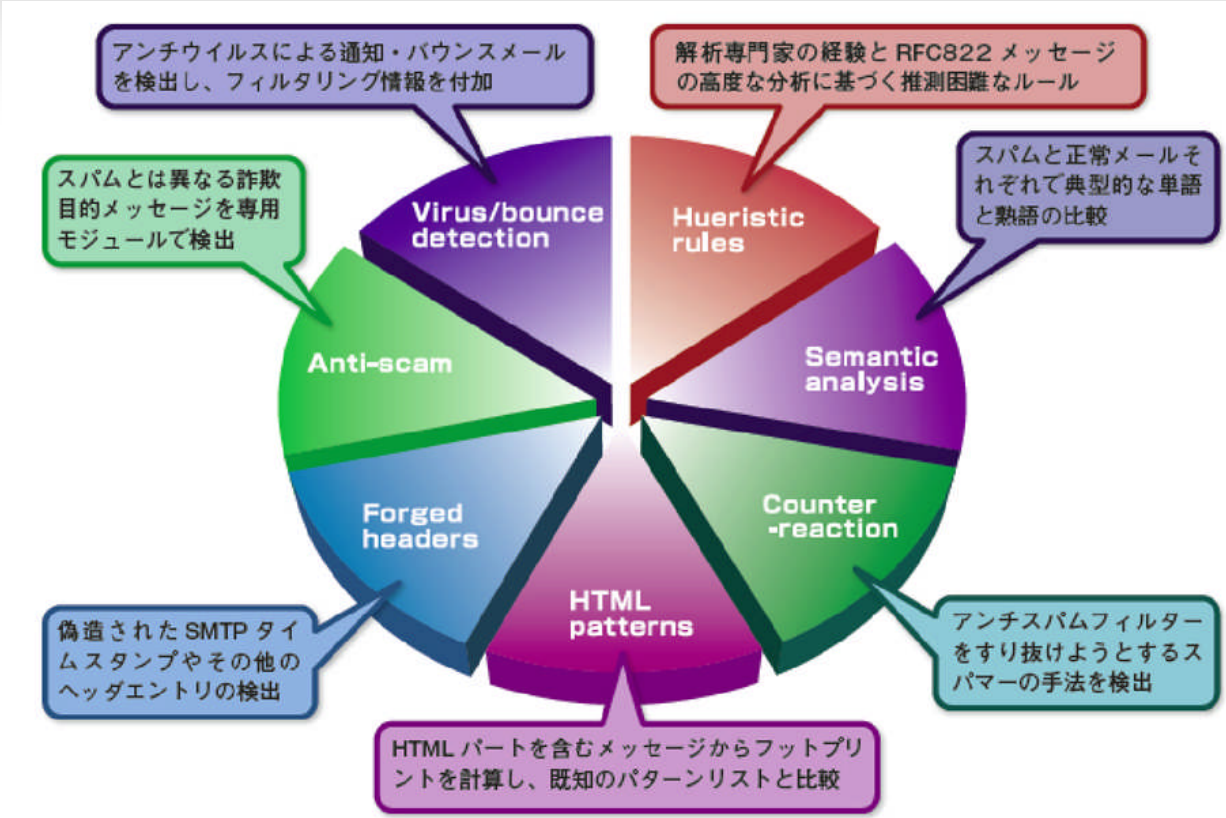
コンテンツレベル - Dr.WEB メールデーモン ー 1/4

高速・軽量アンチスパムエンジン『Vade Retro』を搭載

- ■検知ルール・データを2MBytes 強のアンチスパムエンジンに内蔵
  - ■メモリ、ディスク消費量が他社製品と比較してごくわずか
  - ■外部データベース・パターン参照が不要なため高速・軽量
  - ■ルール・データの更新はエンジンごとアップデート（HTTP 経由）
- ■学習不要、導入直後から 90% 以上の高い検出率を実現
  - ■日本語は 90% 以上、非日本語は 98% 以上の検出率（誤検出は 0.3% 未満）
  - ■複数のスパム検出テクノロジーを採用
- ■新種ウイルス、スパムも予測的ヒューリスティック技術で即座に検出・遮断
  - ■最も危険な“感染拡大期”に有効な防御技術
  - ■エンジン更新無しで対応可能

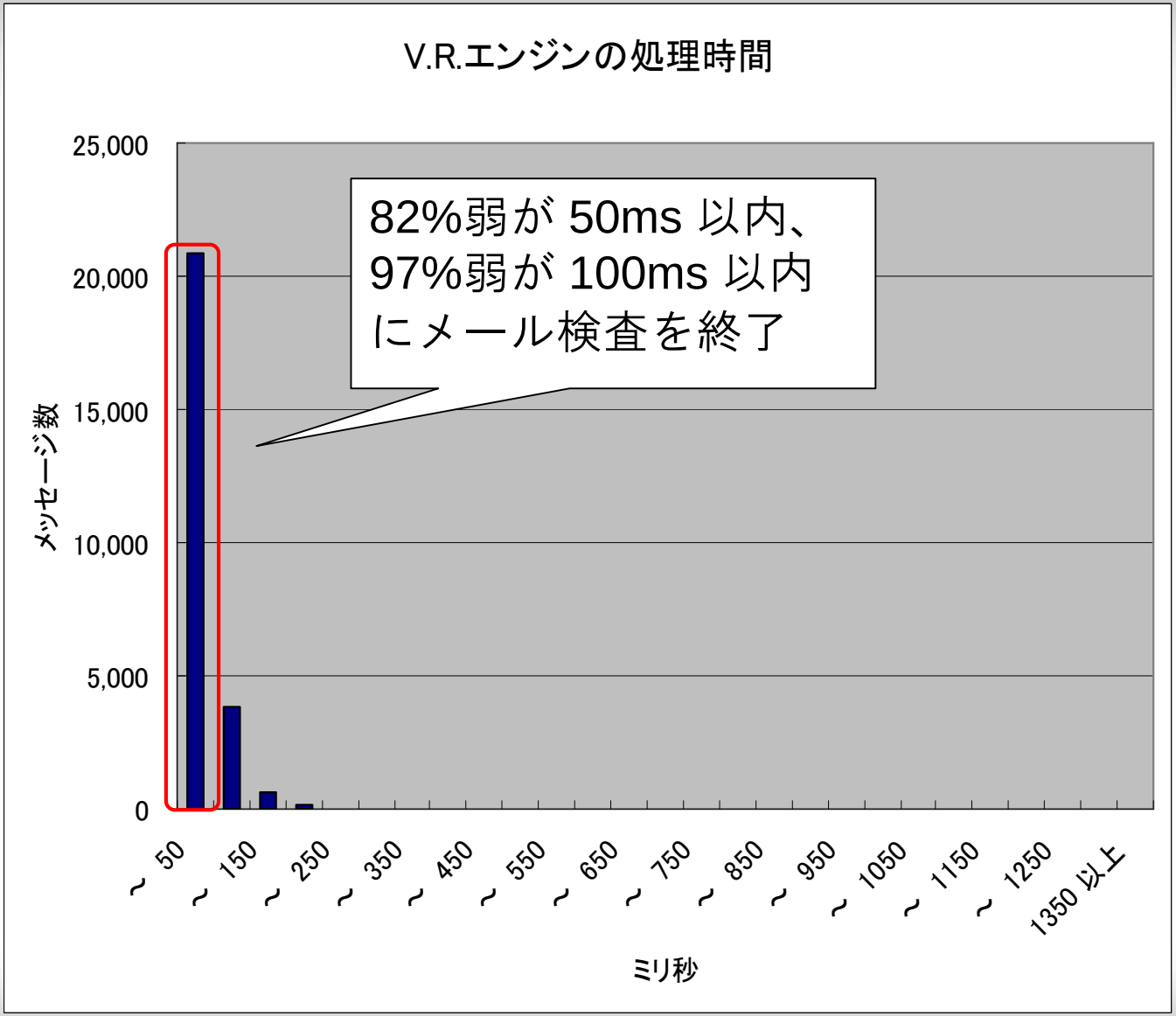


コンテンツレベル - Dr.WEB メールデーモン ー 2/4



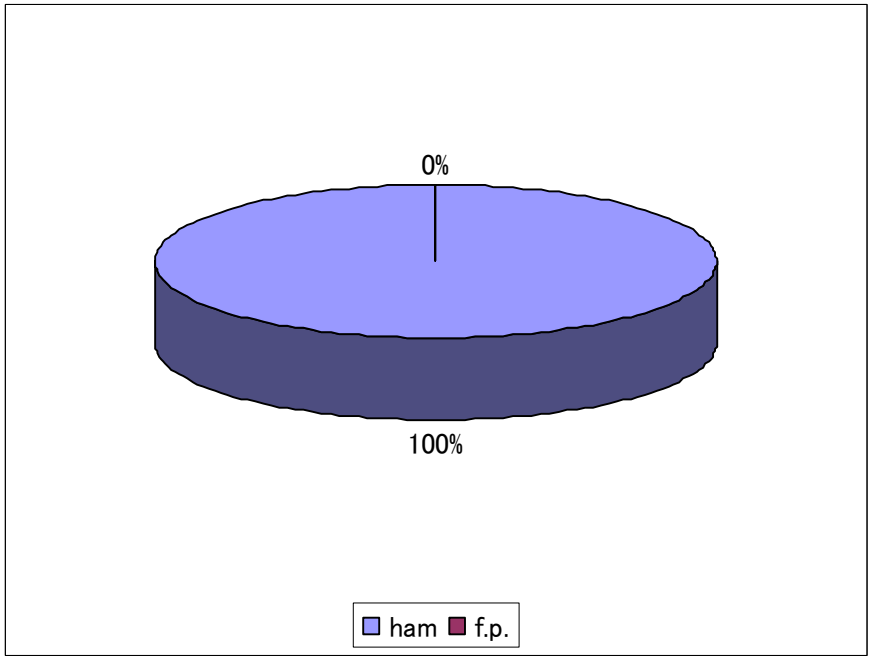
ほぼ毎日エンジンをアップデートし、常に最新技術による効果的なスパム検出を実現

コンテンツレベル - Dr.WEB メールデーモン ー 3/4

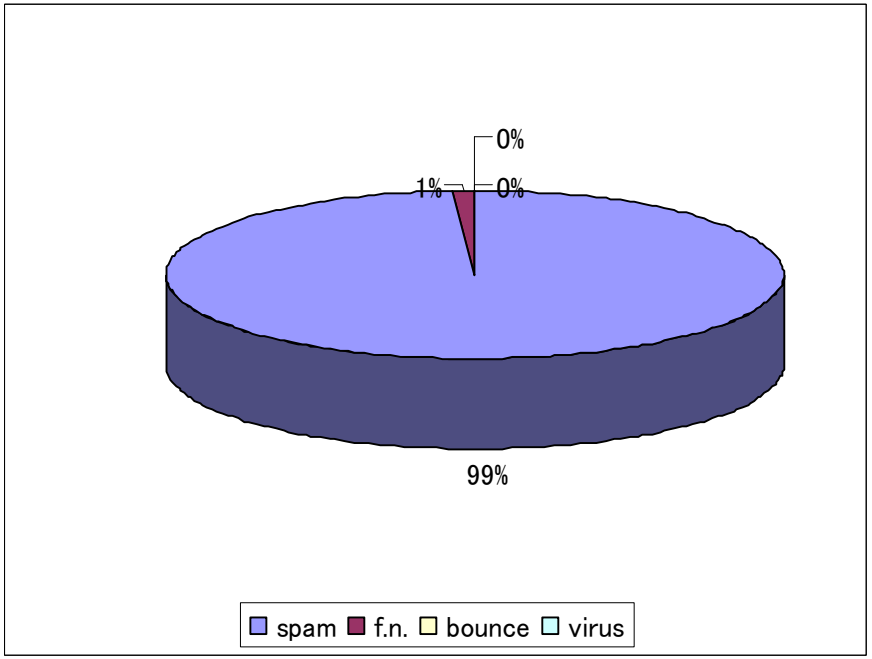


コンテンツレベル - Dr.WEB メールデーモン ー 4/4

正常メール処理

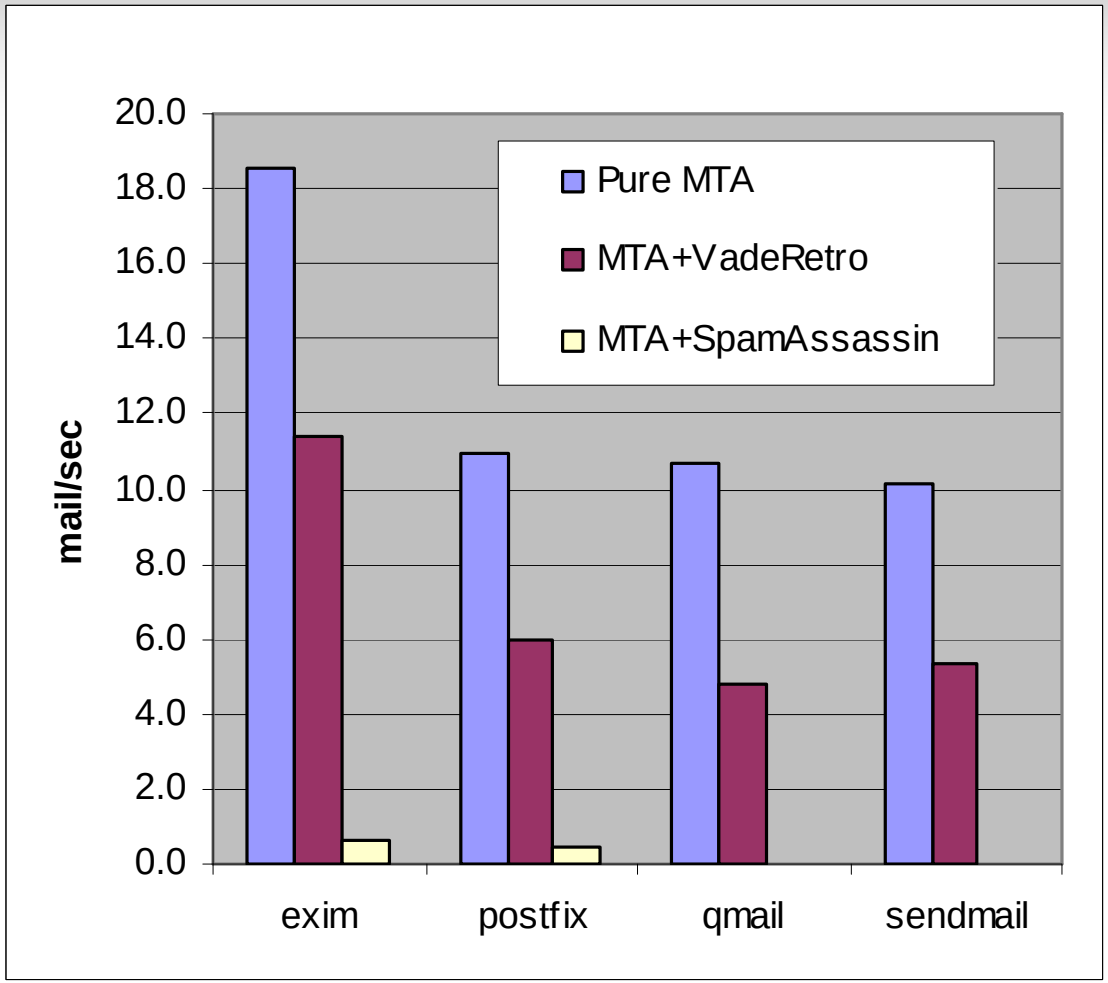


スパムメール処理



2008年6月のメインアドレスでのデータ

参考データ：SpamAssassin との比較



VR/SA = 12 ~ 17倍のスループット

まとめ

Net forest
Network × People

- 小規模サイトで Rgrey を導入
  - 95% 程度のスパムを排除
  - 誤排除は今のところ無し
  - ほとんどメンテナンス不要（精度上げるなら必要）
  - postfix 以外でもゲートウェイとしての使用が可能
- 残り 5% も色々やれば排除可能
  - HELO チェック はかなり効く
  - 最後はコンテンツフィルタがやっぱり必要