milter managerによる柔軟なメールフィルタリング

須藤功平

株式会社クリアコード

2010/02/03

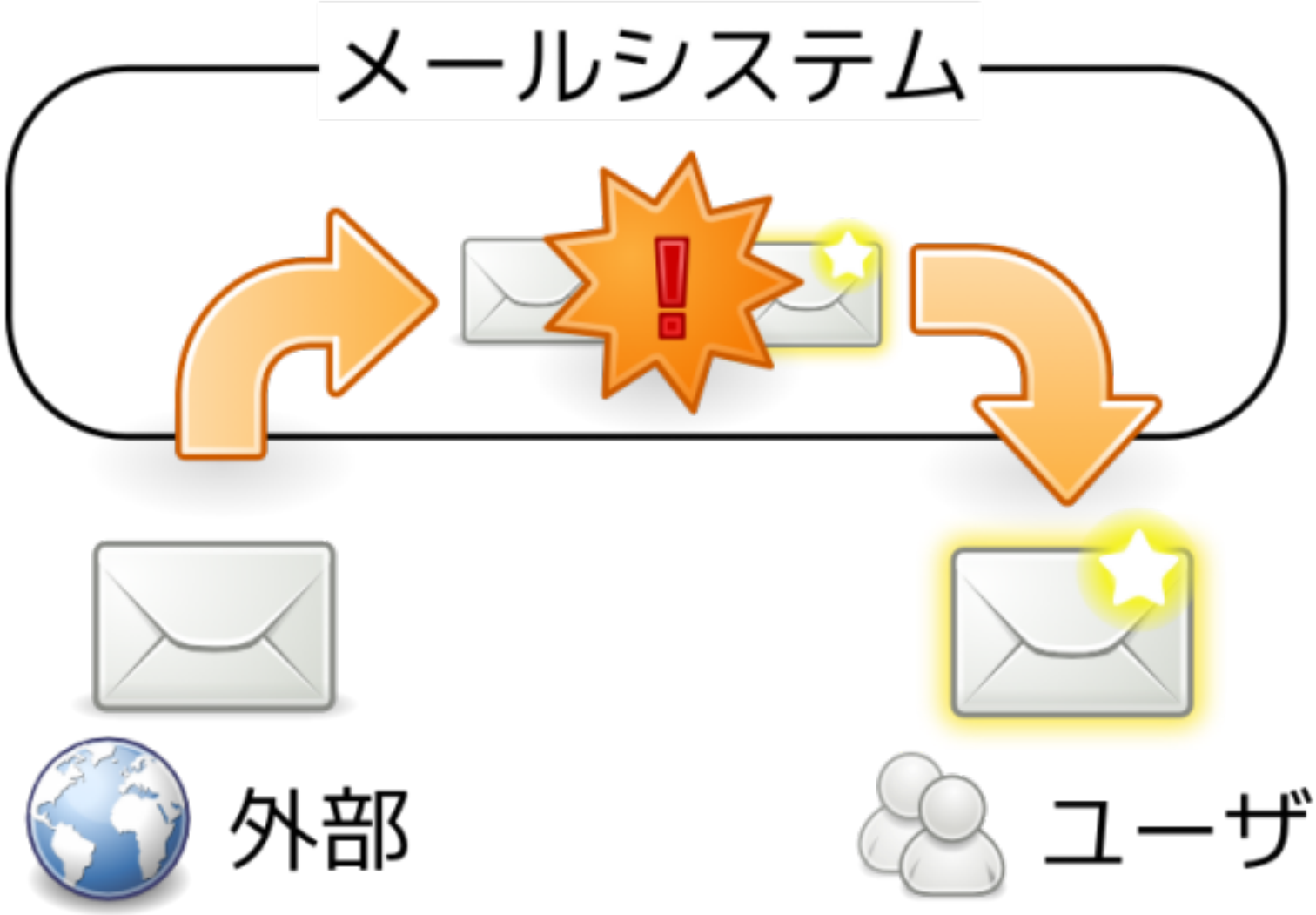
話すこと

- ✓ メールフィルタのこと
- ✓ milterのこと
- ✓ milterの使い方のこと

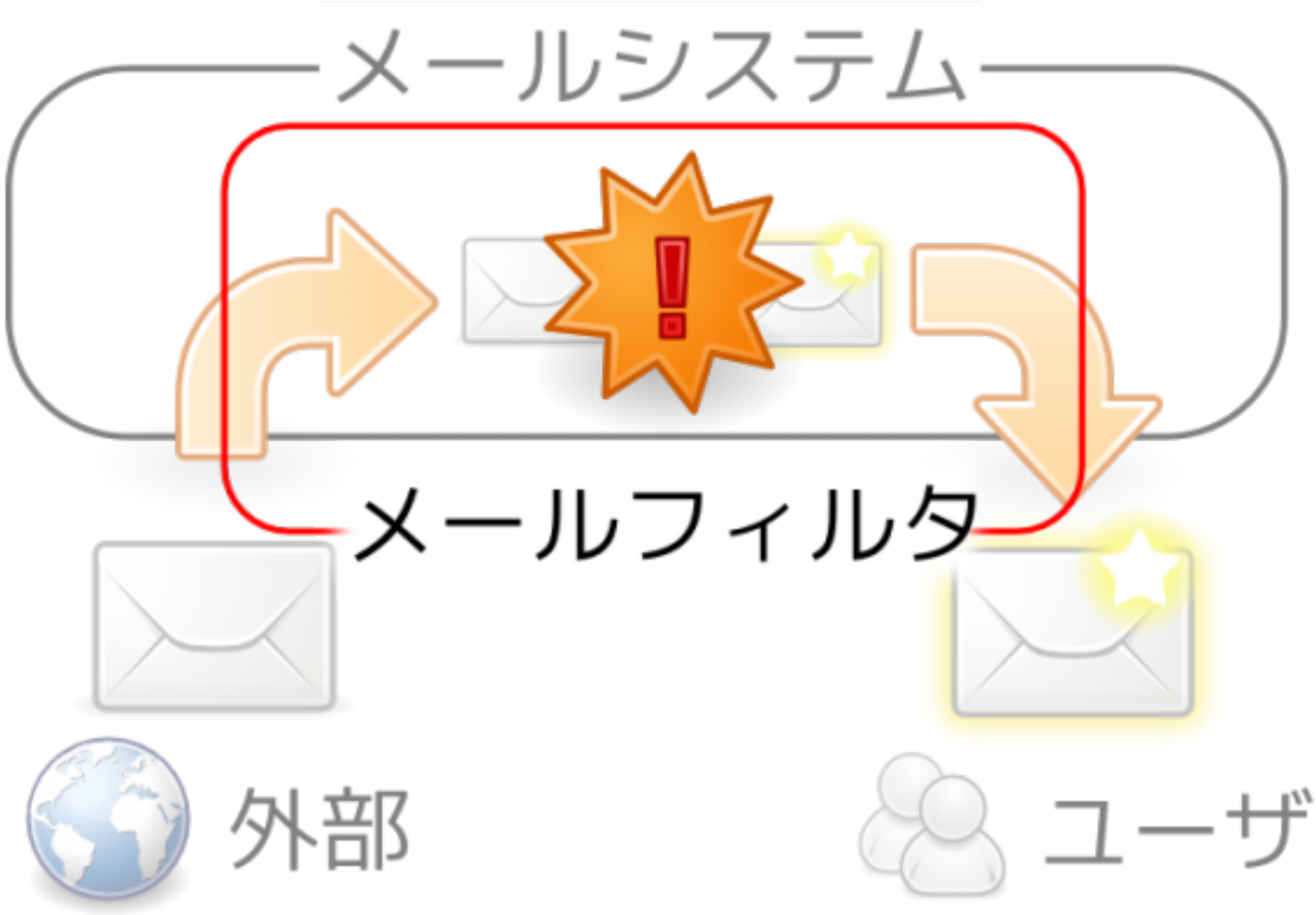
3行でわかるmilter

- ✓ メールフィルタ: mail filter
- ✓ 迷惑メール対策に使える
- ✓ Sendmail/Postfixなどで使える

メールシステム



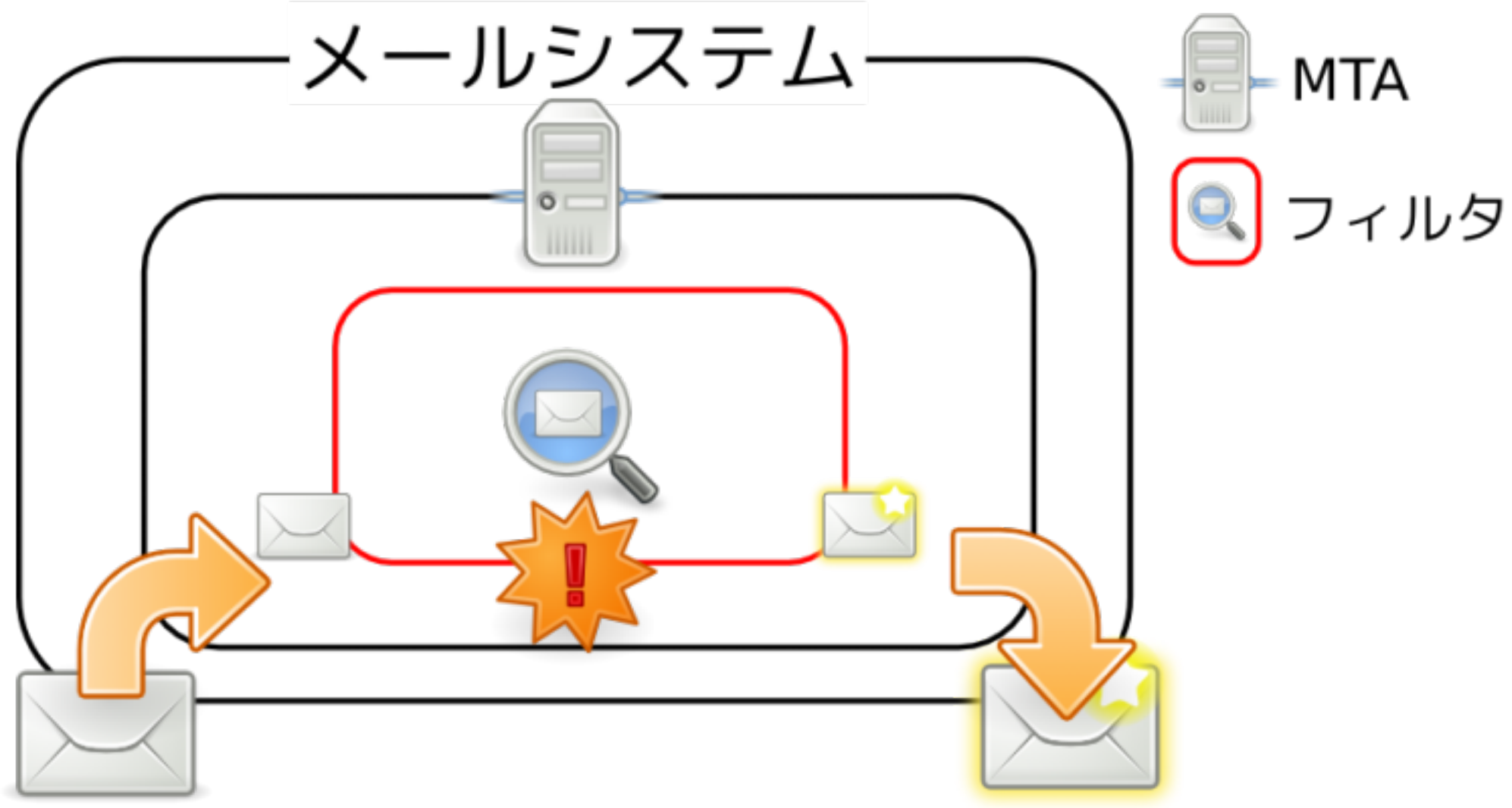
メールフィルタ



フィルタの仕組み

- ✓ MTA組み込み
- ✓ MTAにプラグイン
- ✓ フィルタMTAを挿入

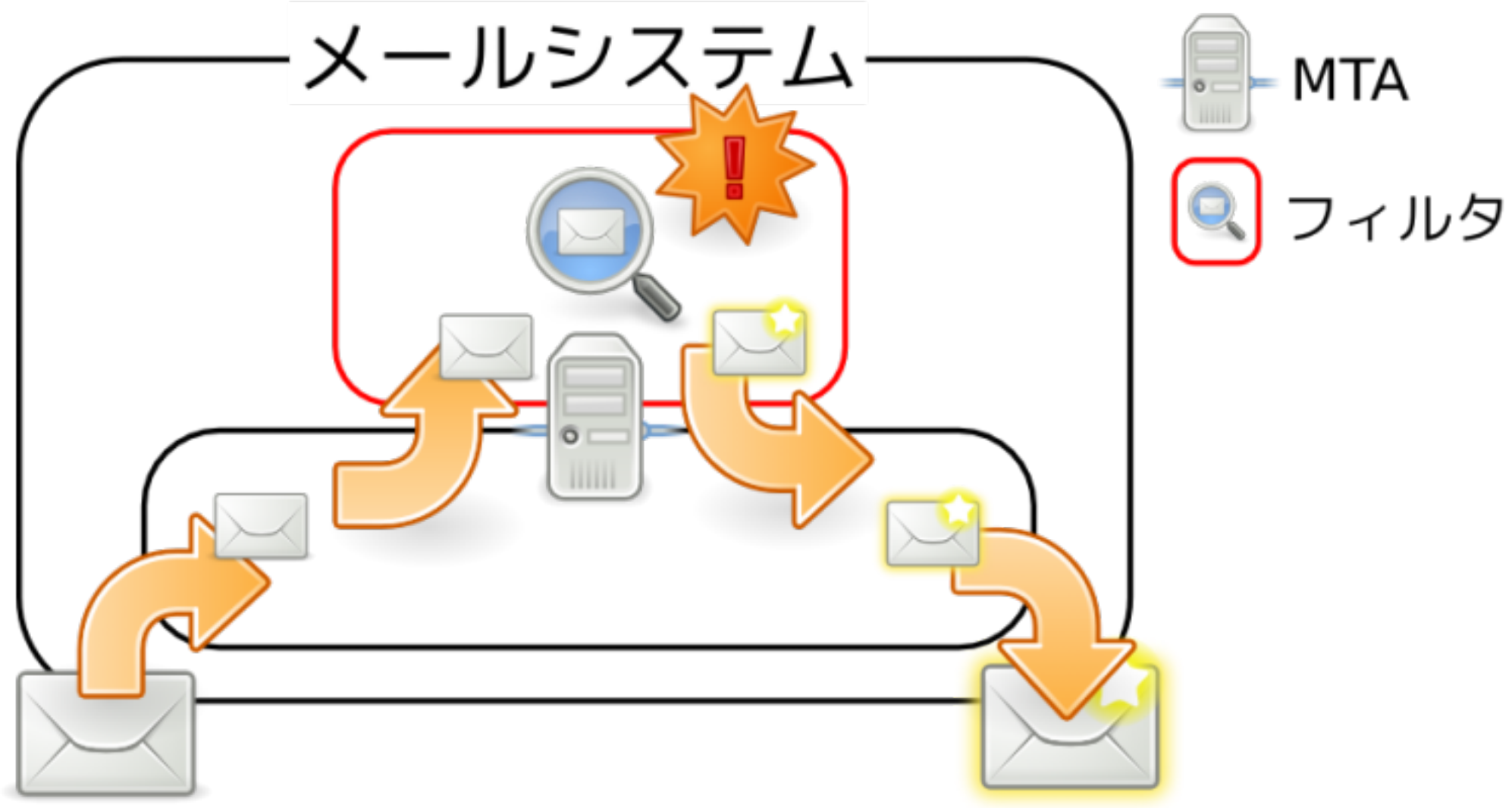
MTA組み込み



MTA組み込み: 例

- Postfix:
  - access(5)/cidr_table(5)
  - reject_rbl_client
- Sendmail: ...
- qmail: ...

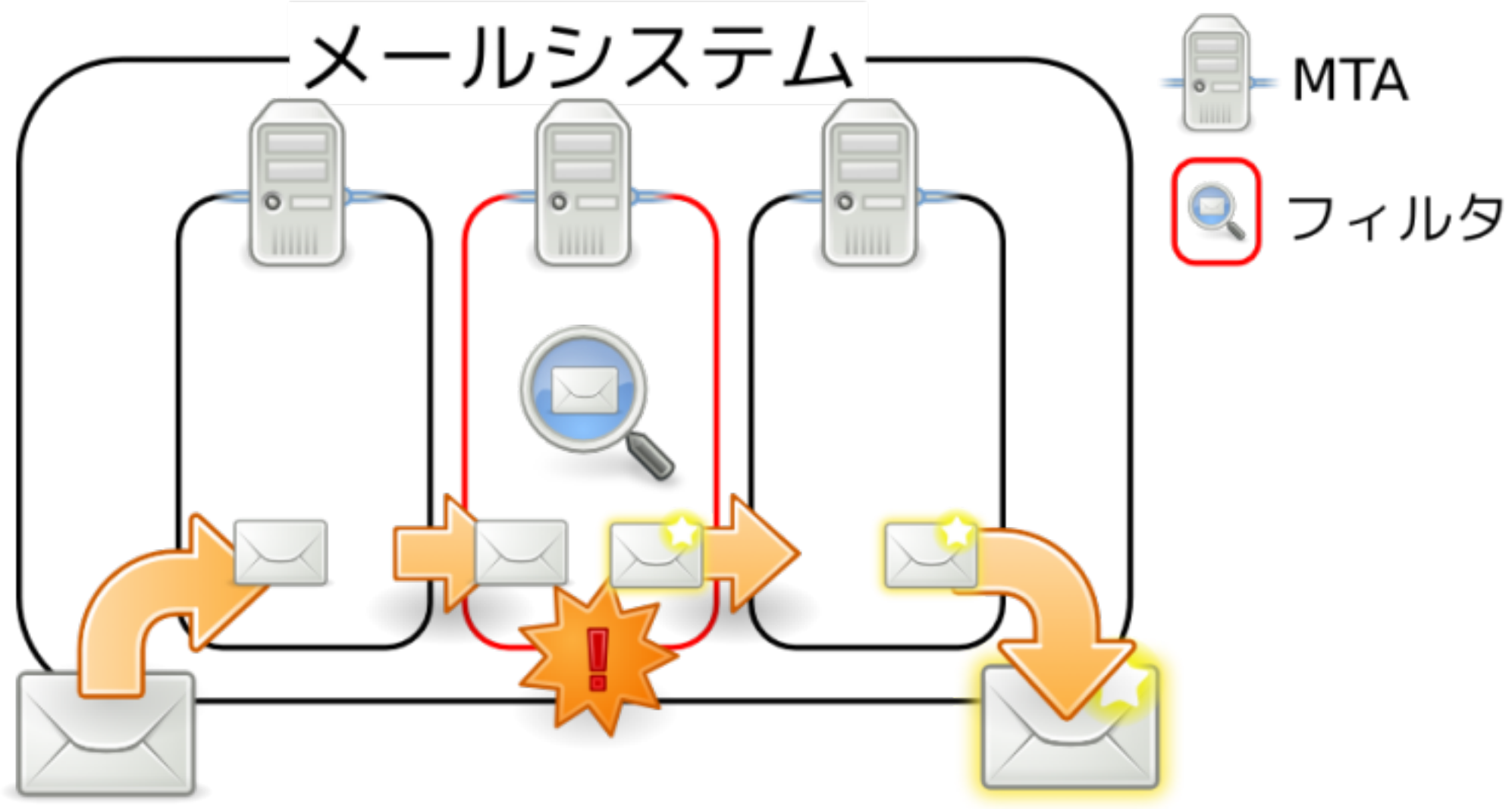
MTAにプラグイン



MTAにプラグイン: 例

- ✓ Postfix: ポリシーサーバ
- ✓ milter
- ✓ …

フィルタMTAを挿入



フィルタMTAを挿入: 例

- ✓ Postfix: コンテントフィルタ
- ✓ amavisd-new
- ✓ Dr.Web
- ✓ …

違いは？

- ✓ 組み込み: お手軽
- ✓ プラグイン: 柔軟
- ✓ フィルタMTA: 汎用的

機能

- 組み込み: お手軽
  - MTA毎にできることが違う
- プラグイン: 柔軟
  - なんでもできる
- フィルタMTA: 汎用的
  - なんでもできる（rejectできないこともある）

導入

- ✓ 組み込み: お手軽
  - ✓ MTAを設定
- ✓ プラグイン: 柔軟
  - ✓ MTAとプラグインを設定
- ✓ フィルタMTA: 汎用的
  - ✓ MTAとフィルタMTAを設定
    （DNSも変更するかもしれない）

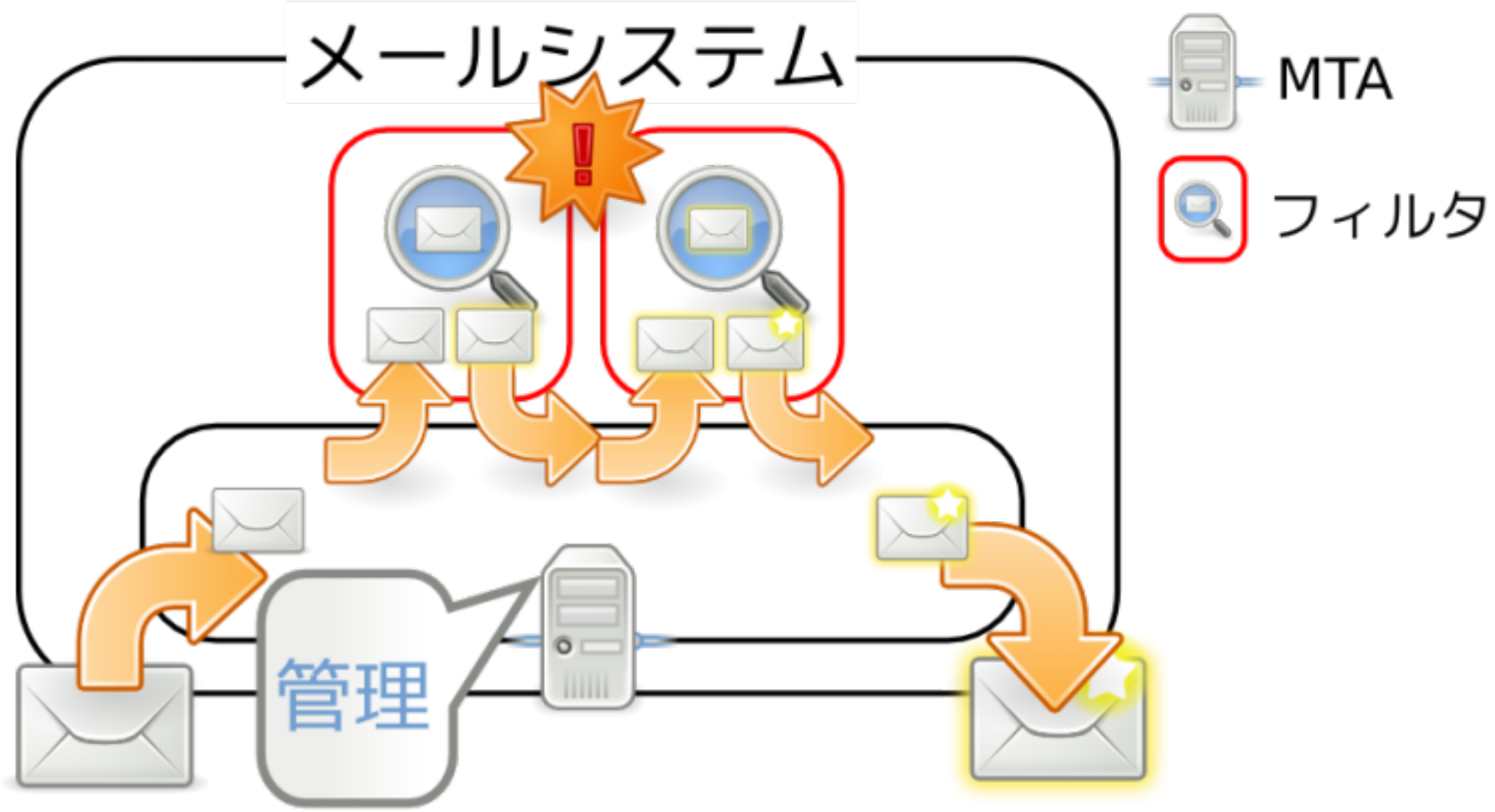
機能追加

- 組み込み: ~~お手軽~~
  - MTAを再ビルド/バージョンアップ
- プラグイン: 柔軟
  - 新しいプラグインの導入
- フィルタMTA: 汎用的
  - 新しいフィルタMTAの導入

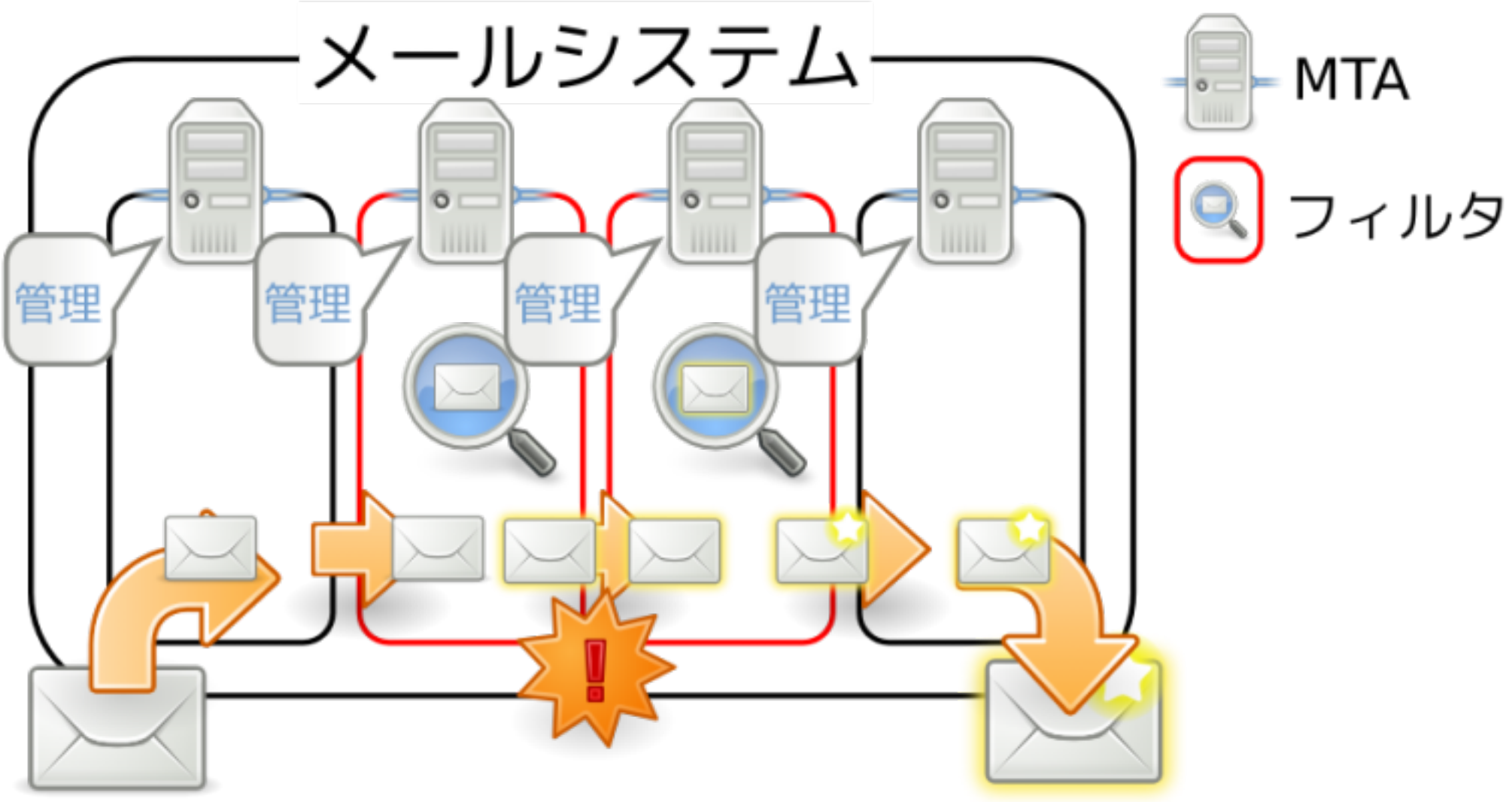
管理場所

- 組み込み: お手軽
  - MTA
- プラグイン: 柔軟
  - MTA
- フィルタMTA: 汎用的
  - それぞれのMTA

管理場所: プラグイン



管理場所: フィルタMTA



メールフィルタのまとめ

- ✓ 迷惑メール対策に使える仕組み
- ✓ 大きく分けて3タイプ
- ✓ それぞれ特徴がある
- ✓ 環境に合った仕組みを選ぶこと

選び方

- 組み込み: お手軽
  - 機能が十分ならこれ
- プラグイン: 柔軟
  - 複数の機能を組み合わせるならこれ
- フィルタMTA: 汎用的
  - 1つのフィルタMTAで済むならこれ

迷惑メール対策

- 今: 1つの手法では対応できない
  - 複数の手法を組み合わせ
  - all in oneのものを1つ使う
- これから: より手法が多様化
  - 新しい対策が必要

望まれる迷惑メール対策

- ✓ 複数の手法を組み合わせられる
- ✓ 新しい手法を追加できる
- ✓ でも管理は容易なままに

今日のオススメ

milter
（プラグイン）

milterのこと

- ✓ メールフィルタのこと
- ✓ milterのこと
- ✓ milterの使い方のこと

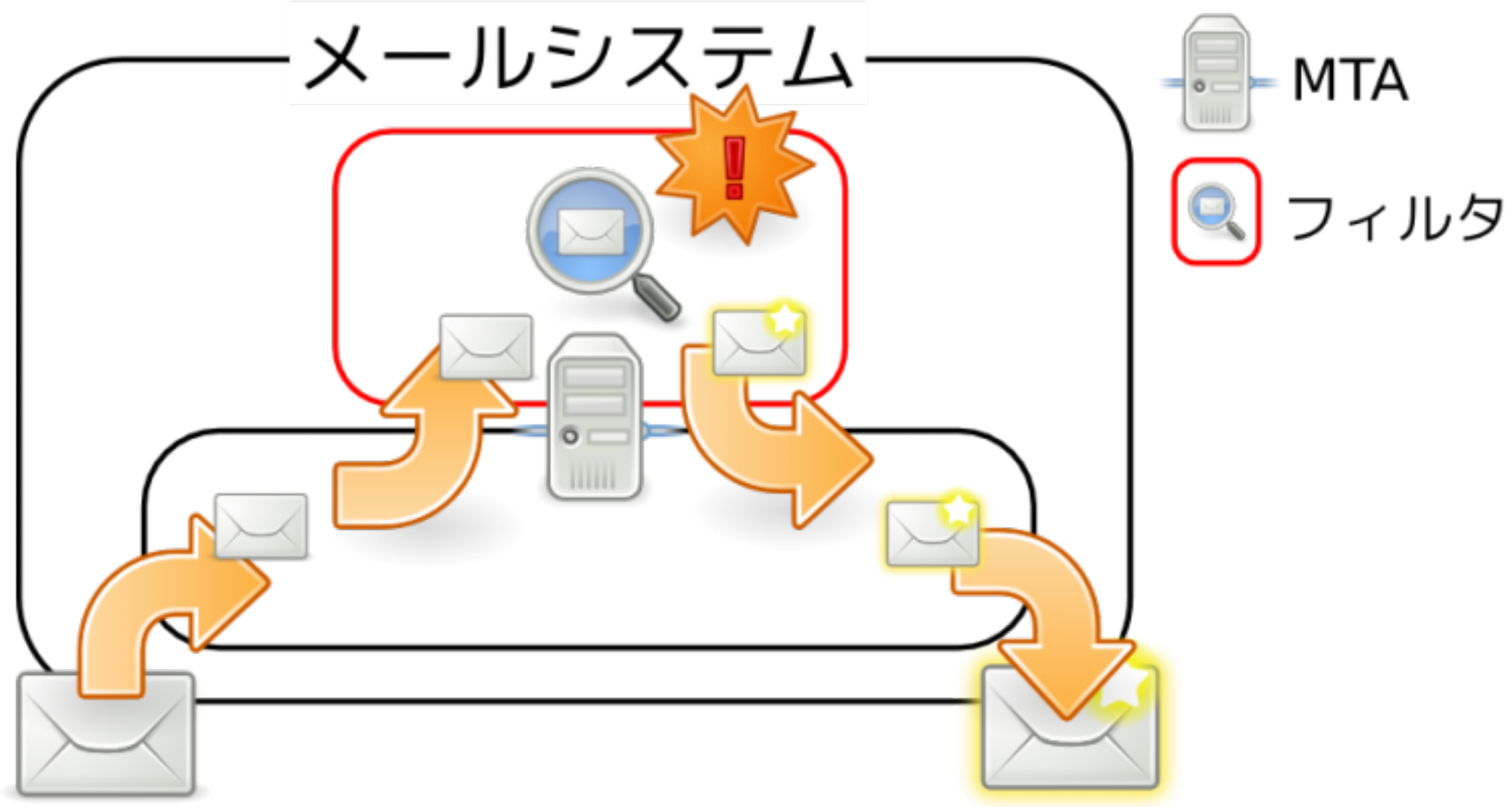
milter?

1. 仕組み:
   milterシステム
2. プロトコルの名前:
   milterプロトコル
3. ↑に準拠したフィルタ:
   milter

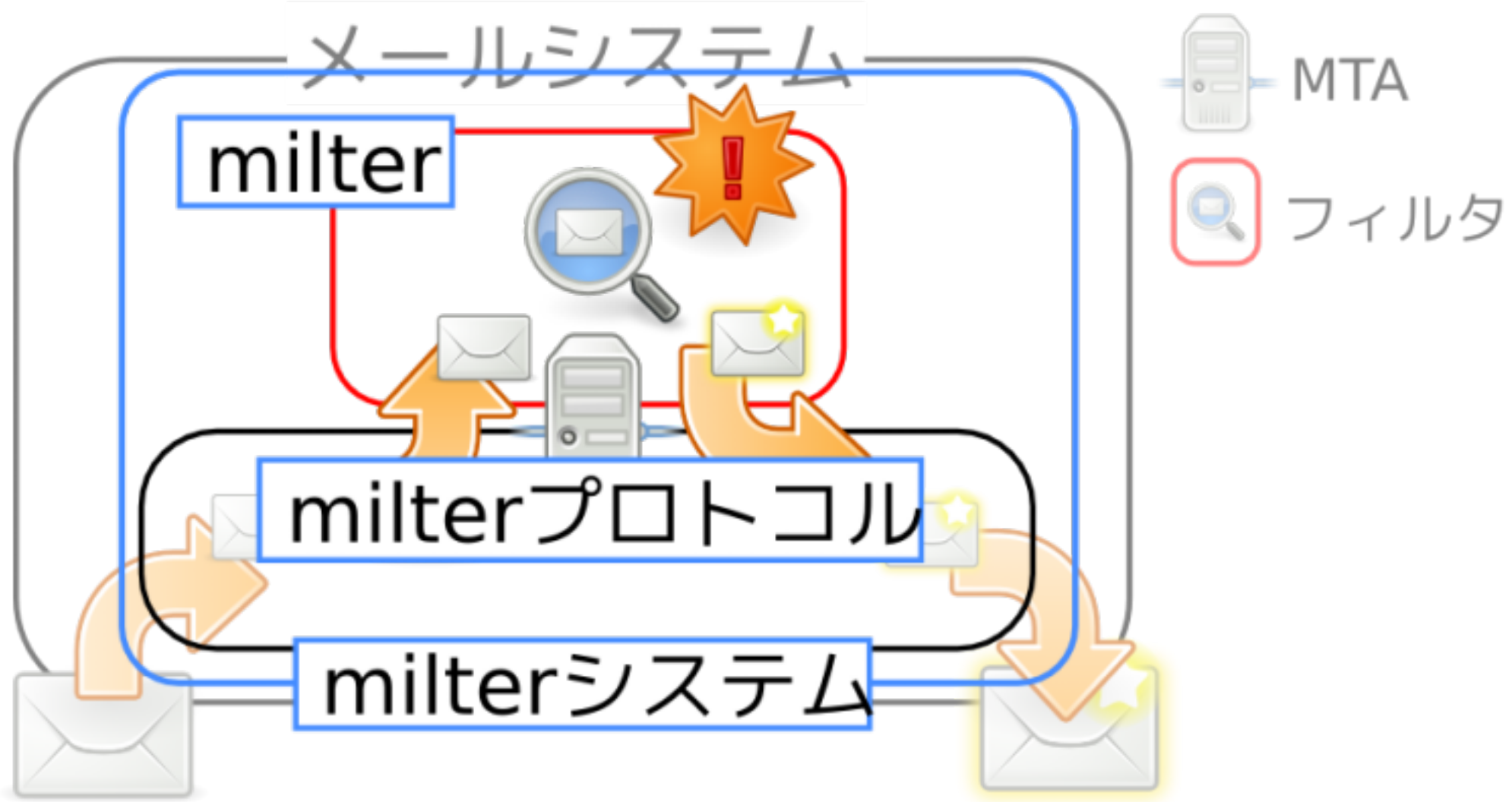
milterの仕組み

- MTAにプラグインタイプ
  - MTAとフィルタは別プロセス
- MTAとフィルタのやりとり:
  - 専用プロトコル == milterプロトコル
- フィルタ == milter

プラグインタイプ



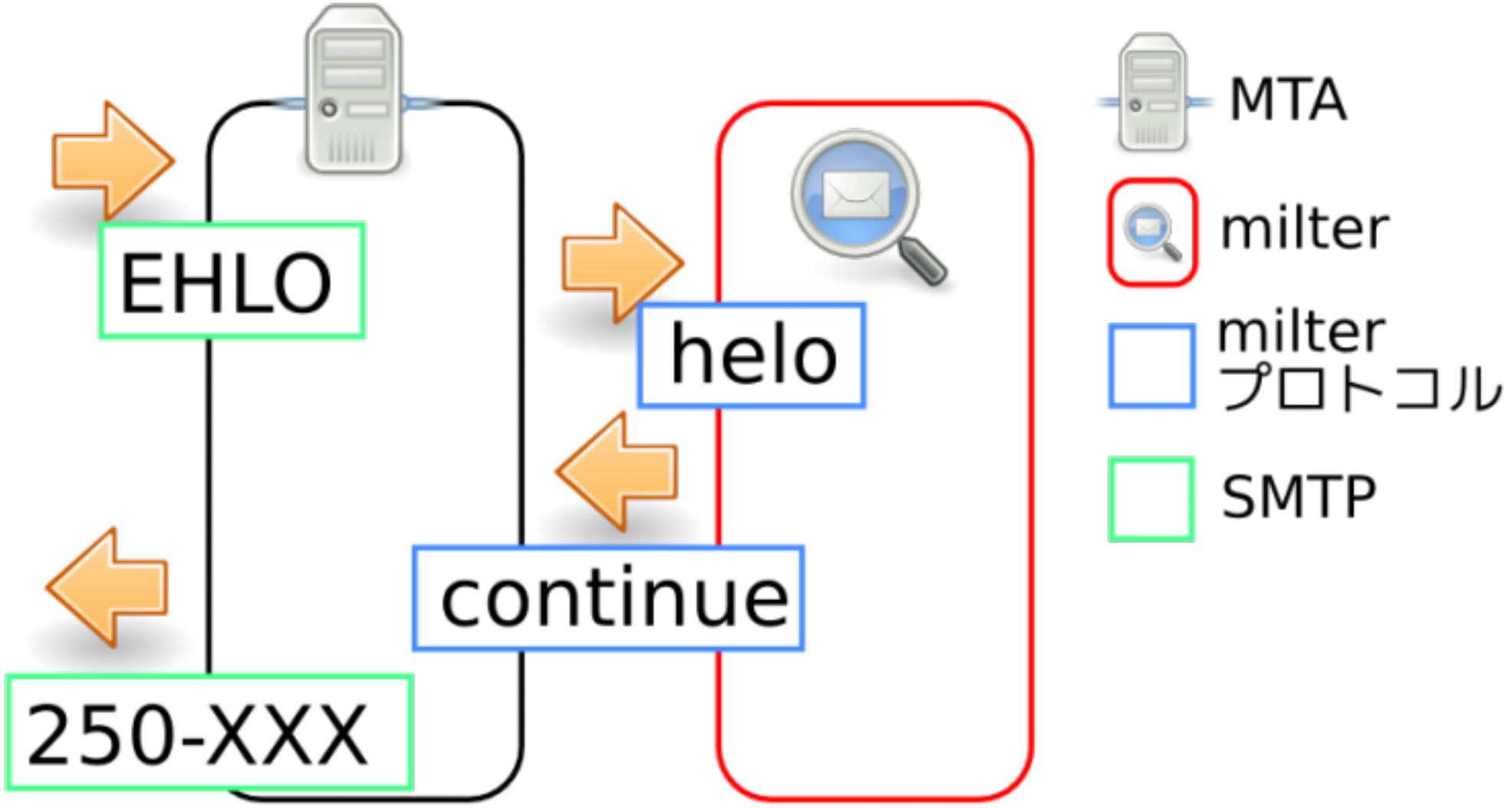
milterシステム



milterプロトコル

- バージョン: 2, 3, 4, 6
  - Postfix 2.6までは2がデフォルト
  - Postfix 2.6以降は6がデフォルト
- SMTPセッションと密接
- UNIXソケット/IPv4/IPv6対応

SMTPとmilterプロトコル



milterプロトコル

- SMTPと平行動作
- SMTPセッション == milterセッション
- セッション毎に情報を持つ
  - 利用例: 差出人が○○で宛先が××のとき△△をする
  - 参考: ポリシーサーバはコマンド毎

milter

- 1プロセス
- 同時に複数セッション
  - 参考: Postfixは1smtpdで1セッション
- 多くの手法が実装済み
  - Greylisting, taRgrey, SPF, DKIM, ...

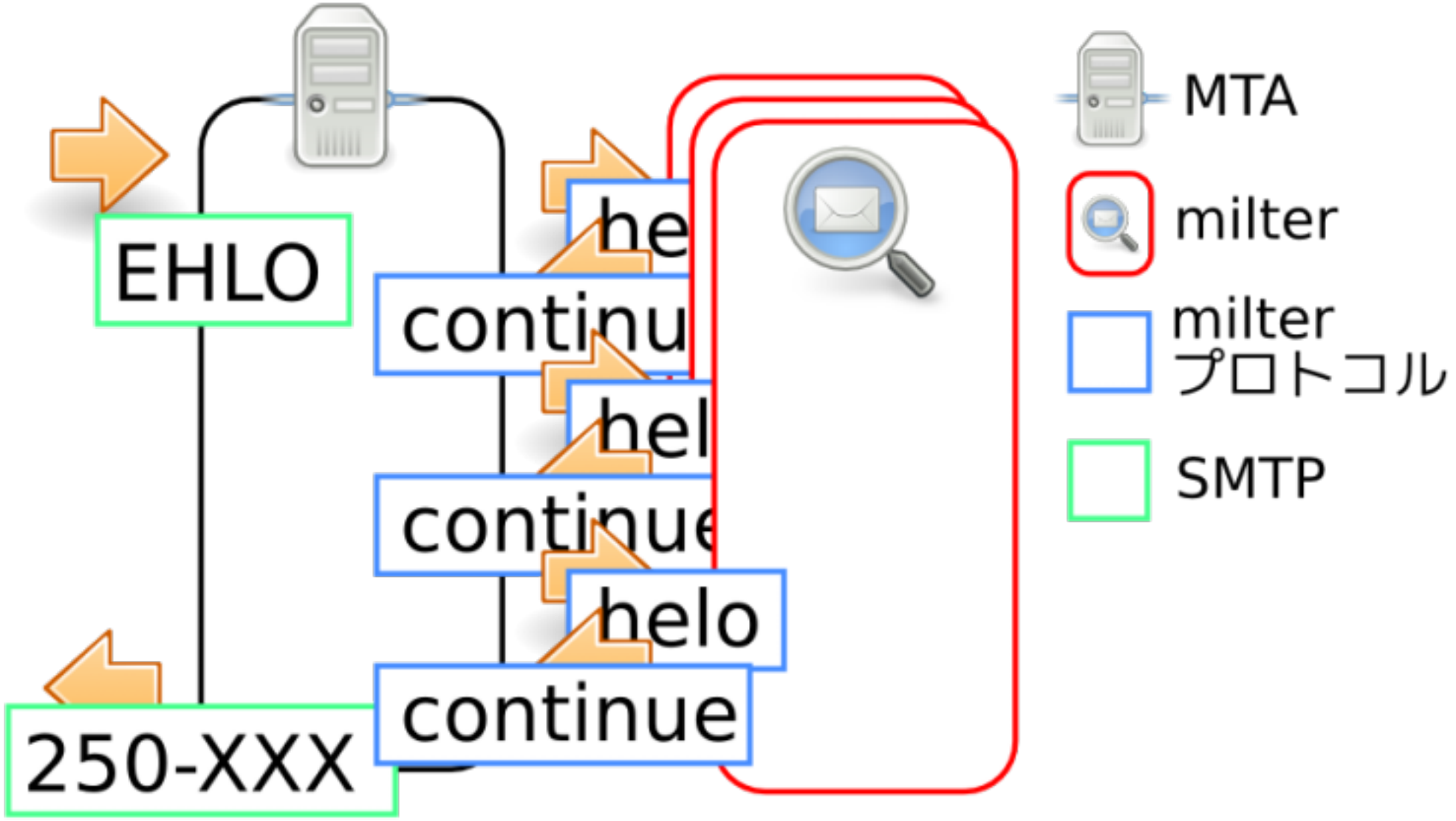
機能の組み合わせ

1. milterをインストール
2. MTAにmilterを登録

複数のmilter

- SMTPと平行動作
- 1SMTPセッション毎に複数のmilterセッション
- コマンド毎に直列
  - 前のmilterの影響を受ける
  - DKIM使用時は順序に注意

複数milter利用時の動作



milterのまとめ

- MTAにプラグインタイプ
- セッション内の情報を利用可能
  - 柔軟な処理が可能
- 複数のmilterを同時利用可能
- 多くの既存のmilterを利用可能

milterの使い方のこと

- ✓ 自分のこと
- ✓ milterのこと
  - ✓ メールフィルタのこと
- ✓ milterの使い方のこと

気になるところ

- milterが増えると管理が面倒
- すべてのセッションに適用
  - ×: ユーザ・ドメイン毎に適用on/off
  - smtpdを分けて対応可能→
    フィルタMTAタイプ
- 情報が少ない

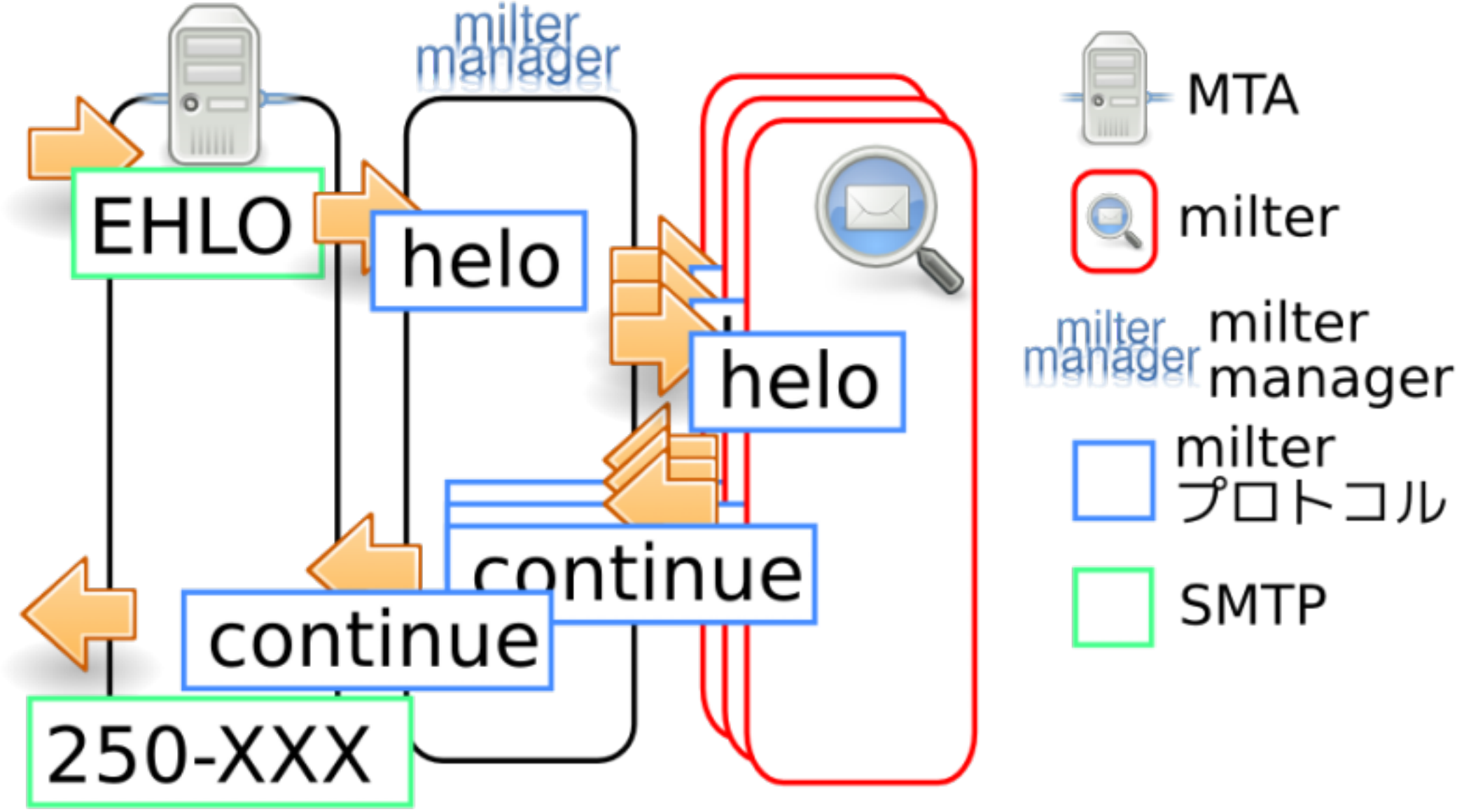
解決案

milter manager

milter manager

- milterをより使いやすくする
  - MTA側に足りない機能を補う
- MTA・milterどちらも変更なし
  - 既存の環境に導入しやすい
- オープンソースソフトウェア

milter manager: 構成



気になるところ: 管理

- milterが増えると管理が面倒
- すべてのセッションに適用
  - ×: ユーザ・ドメイン毎に適用on/off
  - smtpdを分けて対応可能→
    フィルタMTAタイプ
- 情報が少ない

milter管理

- MTA:
  - milterのソケットを指定
- Postfix: 設定項目の影響範囲:
  - milter全体（milter毎ではない）
- milter:
  - 設定はそれぞれで
  - 死活管理はそれぞれで

milter管理: milter

- MTA:
  - milterのソケットを指定
- Postfix: 設定項目の影響範囲:
  - milter全体（milter毎ではない）
- milter:
  - 設定はそれぞれで
  - 死活管理はそれぞれで

milter検出

- milterを自動検出
  - /etc/以下を走査
  - milterインストール→自動で反映
  - milter無効→自動で反映
- milterの設定を自動検出
  - 例: tarpit利用→タイムアウト時間延長

milter管理: Postfix

- MTA:
  - milterのソケットを指定
- Postfix: 設定項目の影響範囲:
  - milter全体（milter毎ではない）
- milter:
  - 設定はそれぞれで
  - 死活管理はそれぞれで

互換性向上: Postfix

Sendmailとの互換性向上

- ✓ マクロ（メタデータ）の違い
- ✓ v2とv6の混在
  パッチは作成済み
  動作確認・修正後Postfix本体にフィードバック予定
- ✓ milter毎の設定
- ✓ ソケット指定の書式

milter管理: 死活管理

- MTA:
  - milterのソケットを指定
- Postfix: 設定項目の影響範囲:
  - milter全体（milter毎ではない）
- milter:
  - 設定はそれぞれで
  - 死活管理はそれぞれで

milter自動起動

- 接続失敗→milter起動
  - プロセス起動用のサブプロセス（root権限）
- milterの起動方法
  - 自動検出: 通常は/etc/init.d/XXX start
- milterの実行権限
  - 指定可能

milter管理のまとめ

milter manager導入→
milter管理が容易に

- ✓ milter関連の設定を自動検出
- ✓ MTAの違いを吸収
- ✓ milterの死活管理

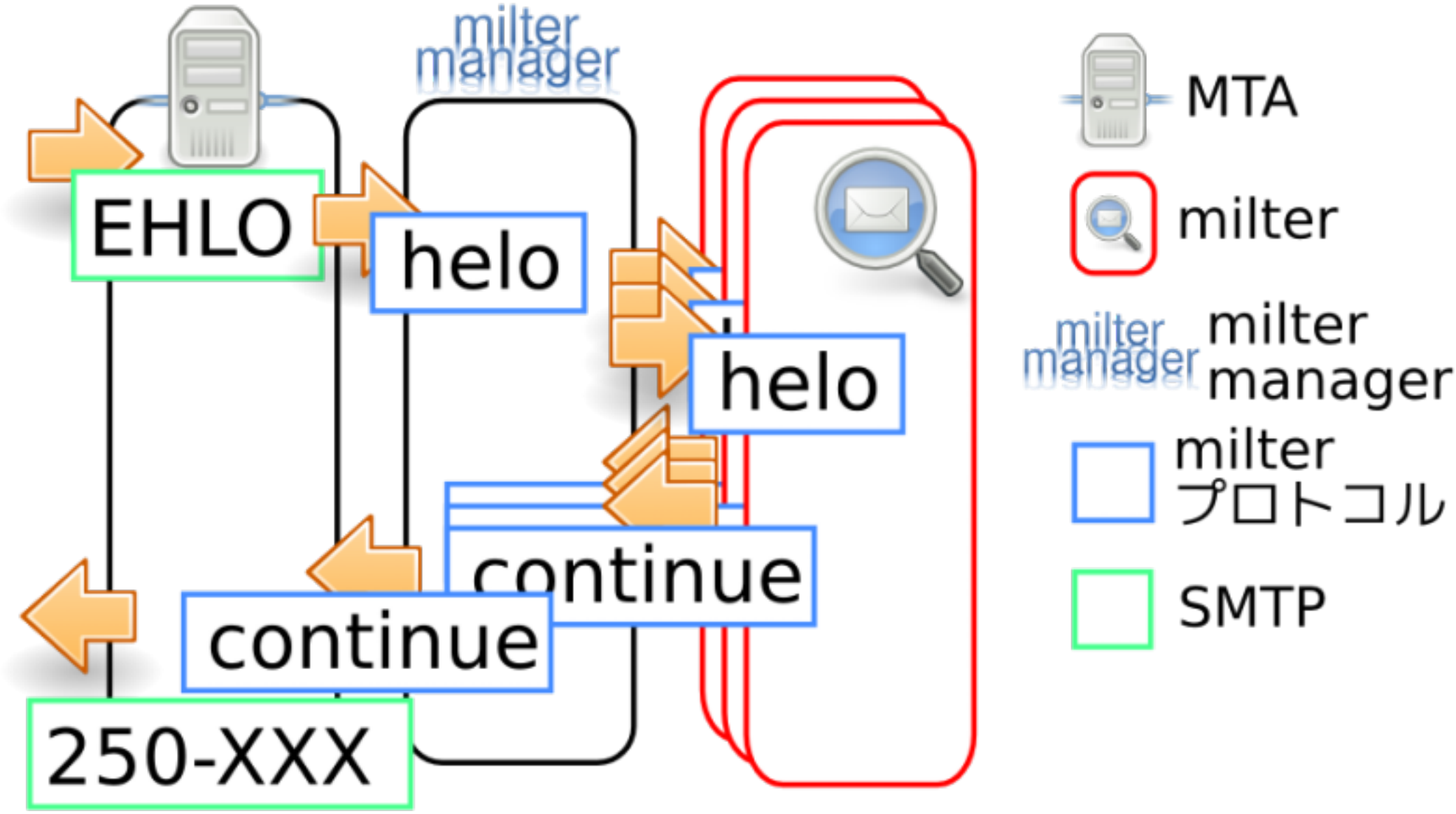
気になるところ: 柔軟性

- milterが増えると管理が面倒
- すべてのセッションに適用
  - ×: ユーザ・ドメイン毎に適用on/off
  - smtpdを分けて対応可能→
    フィルタMTAタイプ
- 情報が少ない

柔軟性: ユーザ毎の設定

- ユーザ毎に使用milter変更:
  - milter毎に適用ユーザを指定
  - milter毎に設定方法が異なる
- ↑をmilter managerレベルで実現
  - ポリシーを一括管理
  - メンテナンスが容易に

milter manager: 構成



柔軟性: 細かい適用指定

- ユーザ毎の設定方法
  - LDAP, RDB, Postfixの設定ファイル, ...
  - スクリプト言語処理系を内臓→
既存の大量のライブラリを使用可能
- 複数の情報を組み合わせて利用可
  - 接続元はローカル？
  - SMTP AUTH済み？

柔軟性のまとめ

- milterのon/offを一括管理
- 外部との連携機能が強力:
  - 例: LDAP, RDB, access(5), ...
- 条件判断に必要な情報:
  - セッション情報を複合的に利用可

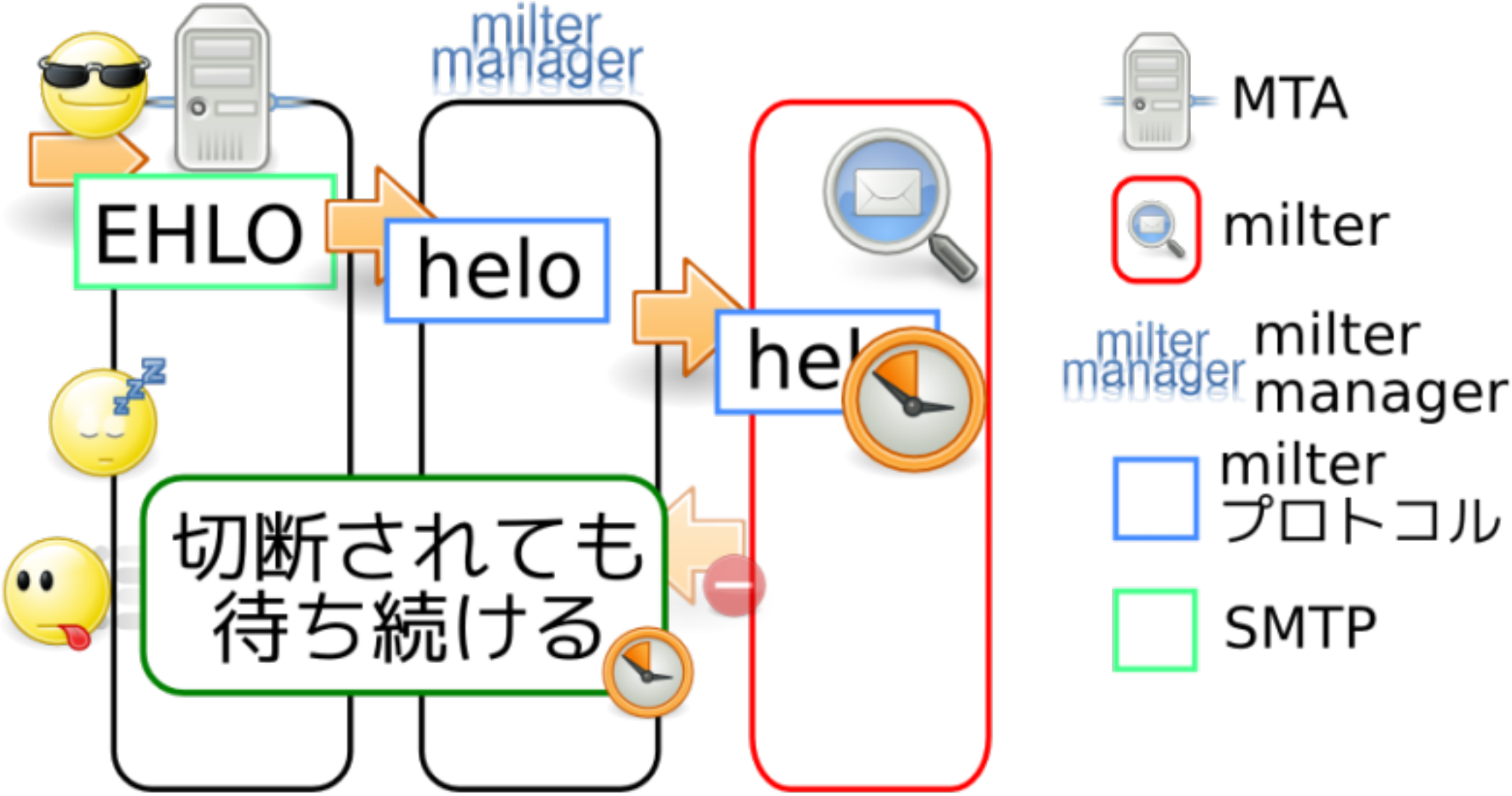
もっとmilter manager

- ✓ tarpit問題の解決
- ✓ …

tarpit問題

- tarpit→smtpdプロセス増加
  - 1セッション == 1smtpdプロセス
- smtpdプロセス増加→
  リソース使用量増加
- 解決法:
  - クライアントからの切断を検出

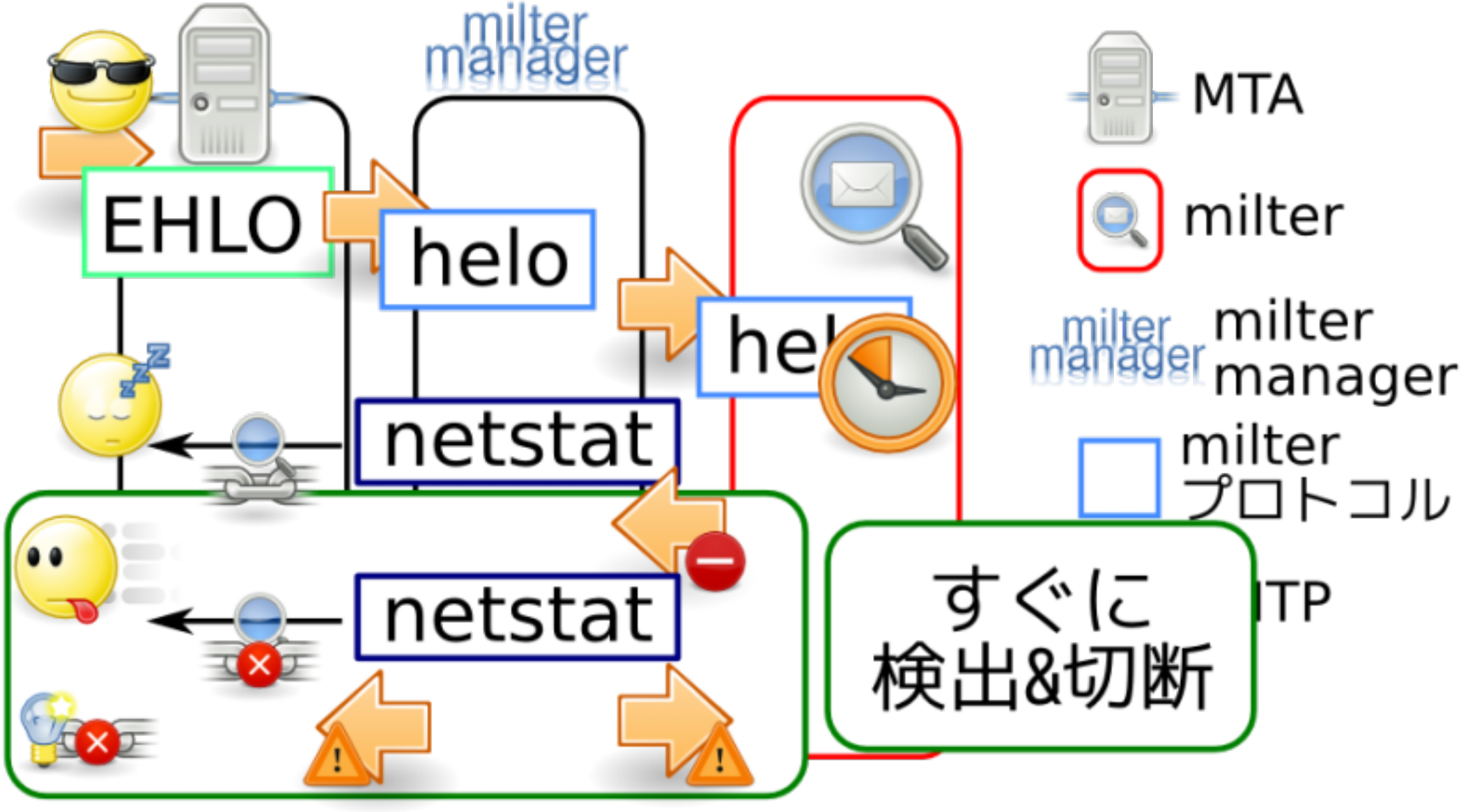
tarpit問題: ケース例



解決法1: MTA改造

- ✓ Postfix: さとうさんパッチ

解決法2: milter manager



まとめ: メールフィルタ

- ✓ 組み込み: お手軽
- ✓ プラグイン: 柔軟
- ✓ フィルタMTA: 汎用的

まとめ: milter

- ✓ MTAにプラグインタイプ
- ✓ 同時利用が楽
- ✓ 既に多くの実装あり

まとめ: milter manager

- 既存の技術をより活かす
  - MTAのmilterサポートを強化
  - milterを自動検出
  - ユーザ毎にmilterをon/off
  - 外部アカウントシステムとの連携
- tarpit問題の解決

柔軟な迷惑メール対策

milter manager

http://milter-manager.sf.net/

須藤功平（クリアコード）http://www.clear-code.com/