

メールサーバとメールの配送の仕組み と 不正アクセスからサーバを守る仕組み

神戸大学 理学部 惑星学科
流体地球物理学教育研究分野 B4

岩谷菜々子

岡田和真

目次

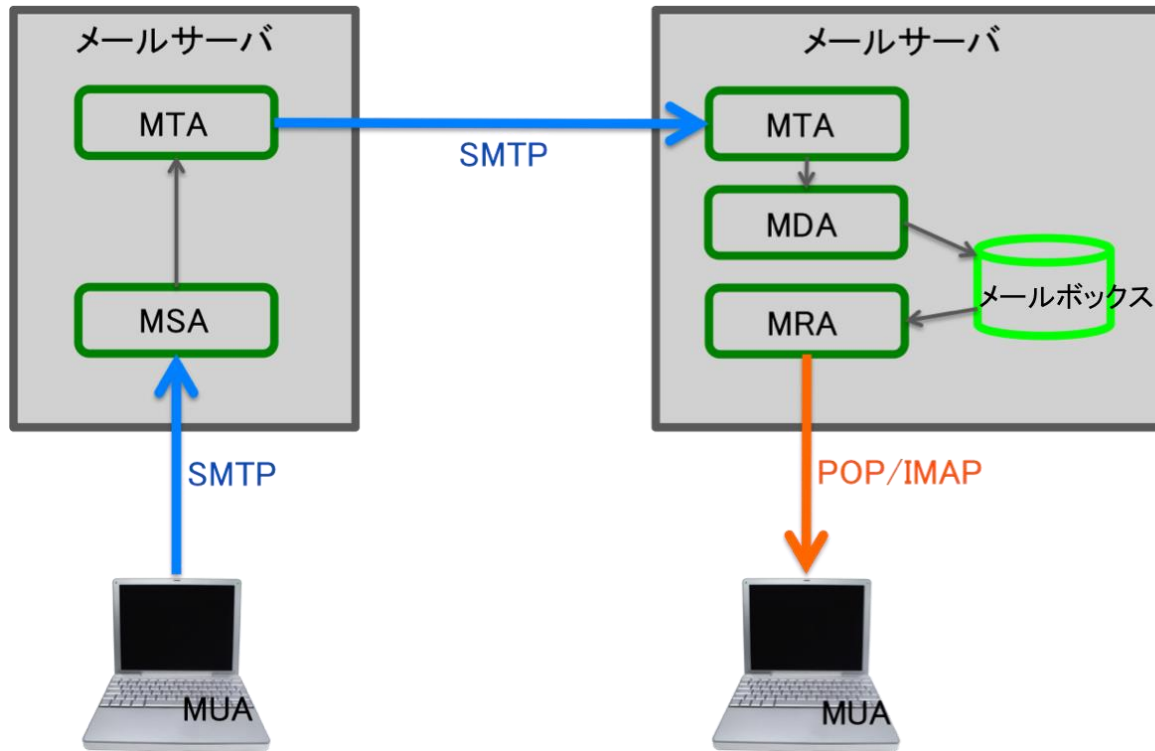
1. メール送受信の大まかな流れ
 - i. MUA, MSA, MTA, MDA, MRA
 - ii. メールの送受信とプロトコル
 - SMTP
 - POP
 - IMAP
2. 不正な攻撃からサーバを守る仕組み
 - fail2ban
3. まとめ

メール送受信の大まかな流れ

手紙の大まかな流れ

1. 自分が手紙を書きます
2. ポストへ投函します
3. 投函されたものは地元の郵便局へ集められます
4. 地元の郵便局から、宛先の地域の郵便局へ配達されます
5. そこで私書箱へ割り振られます
6. 相手が取りにきます

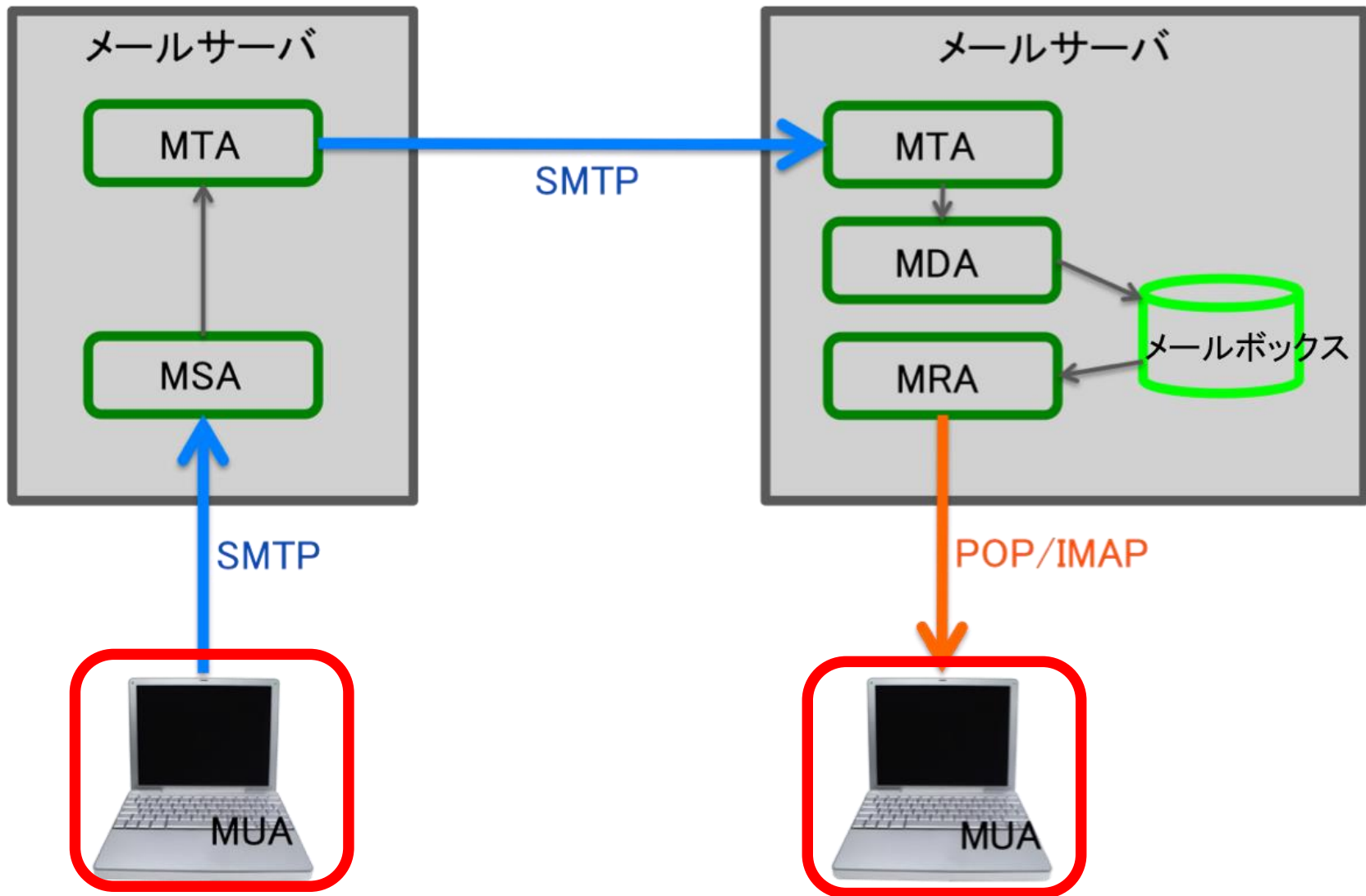
メール送受信の大まかな流れ



- 送信者はメールソフトを使ってメールをメールサーバに送る
- 宛先アドレスを管理するメールサーバへメールを転送する
- 受信者は自分のメールサーバに受信メールの有無を問い合わせる
- 受信メールがあれば, そのメールを受信する

MUA, MSA, MTA, MDA, MRA

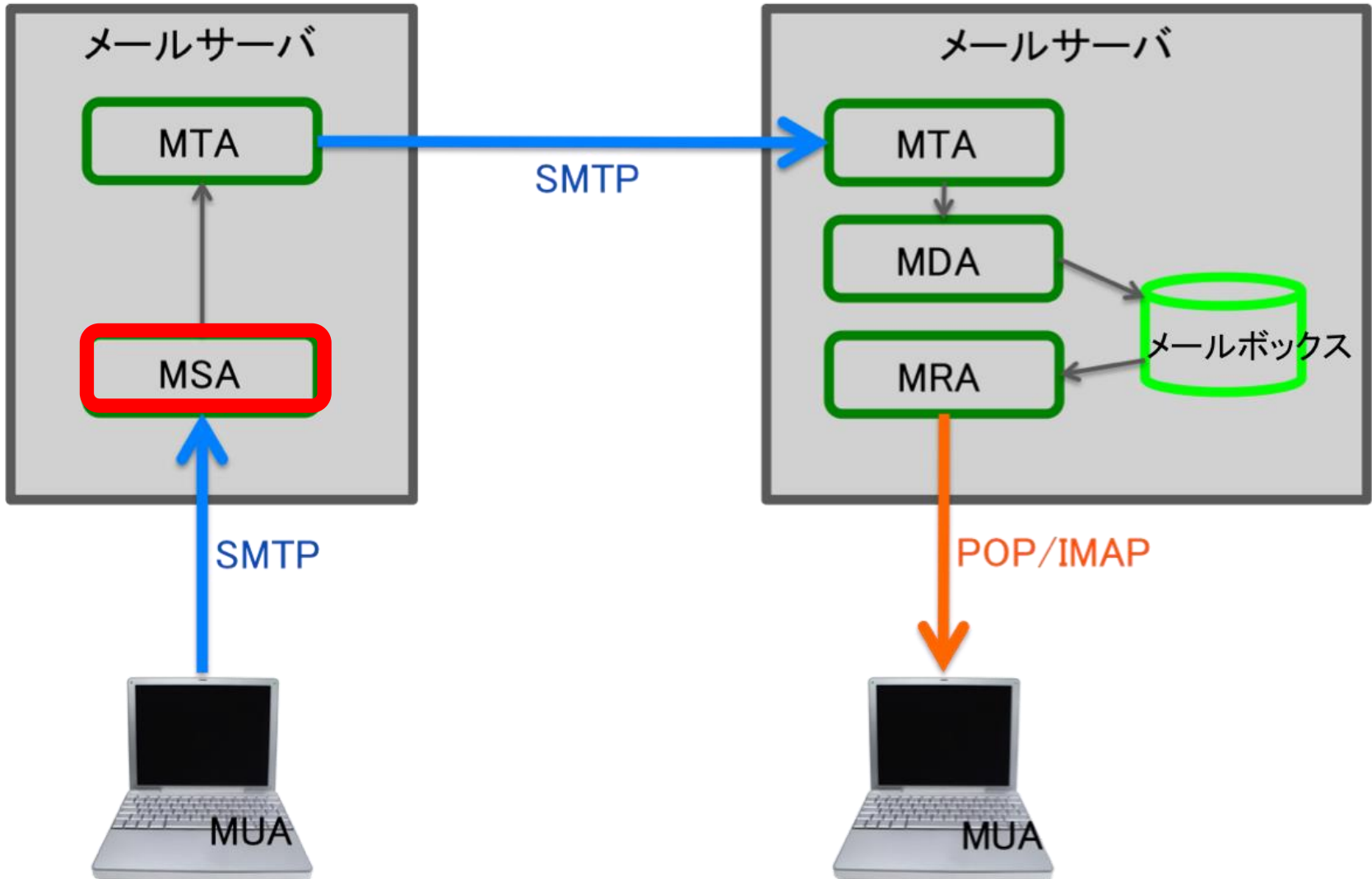
MUA とは



MUA とは

- MUA (Mail User Agent)
 - 電子メールを扱うためのプログラム
 - メールの閲覧, 作成
 - メールの送受信
 - ファイルの添付
 - 例
 - Mozilla の Thunderbird
 - Windows Mail , Windows Live Mail...etc.
 - 手紙を送る場合で考えると
 - 手紙を書いたり, 受け取った手紙を管理したりする役割
 - 書いた手紙を郵便局のポストに投函する役割
 - 郵便局から手紙を取ってくる役割

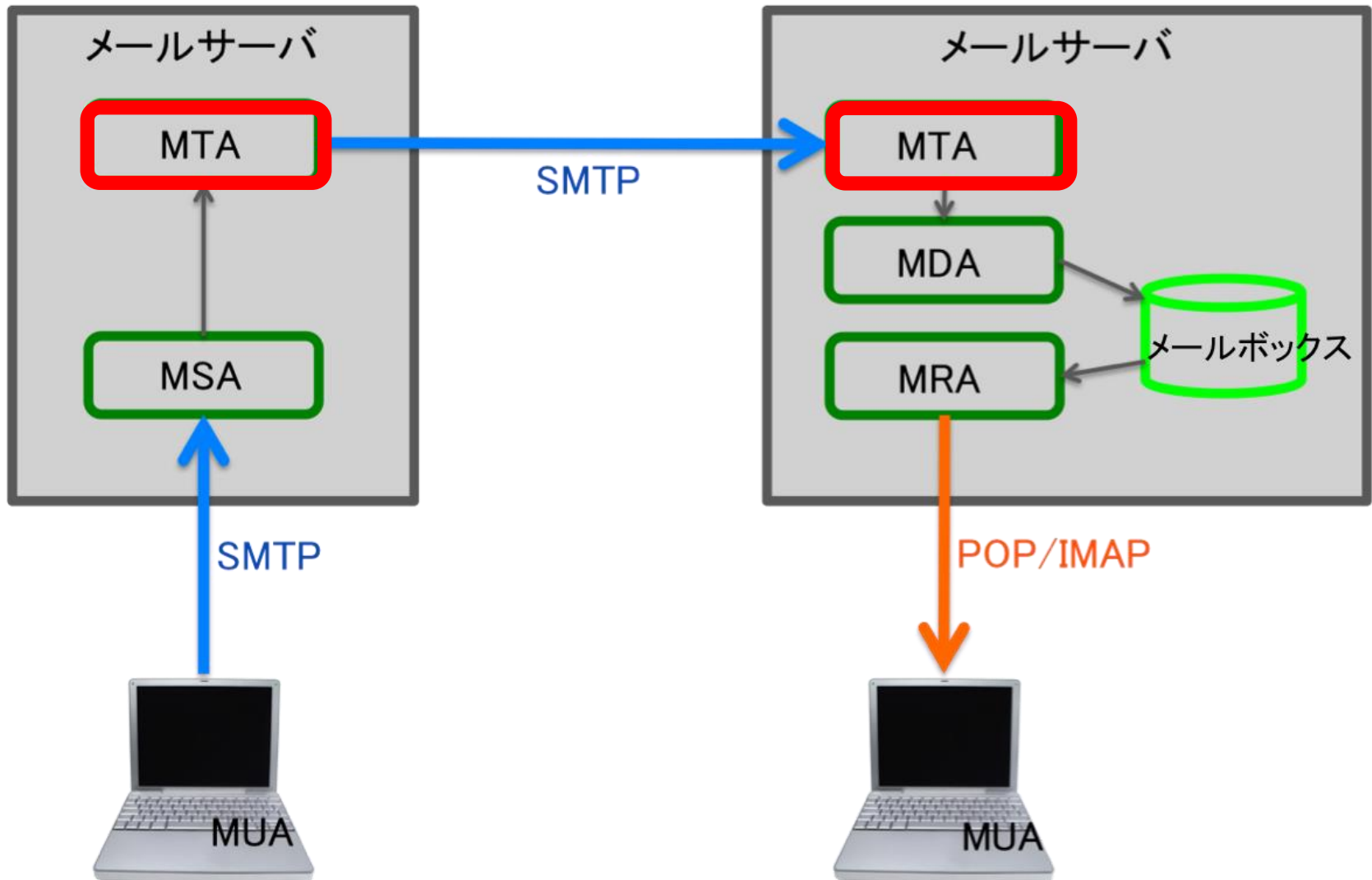
MSA とは



MSA とは

- MSA (Message Submission Agent)
 - MUA がメールを送信する際に接続するシステム
 - ユーザ認証
 - スパムメール対策
 - 昔は, MUA が直接 MTA (後述) に接続しメールを送信していた
 - どのコンピュータからでも, 認証無しで電子メールの送信が可能であった
 - スパムメールを多くばらまかれた

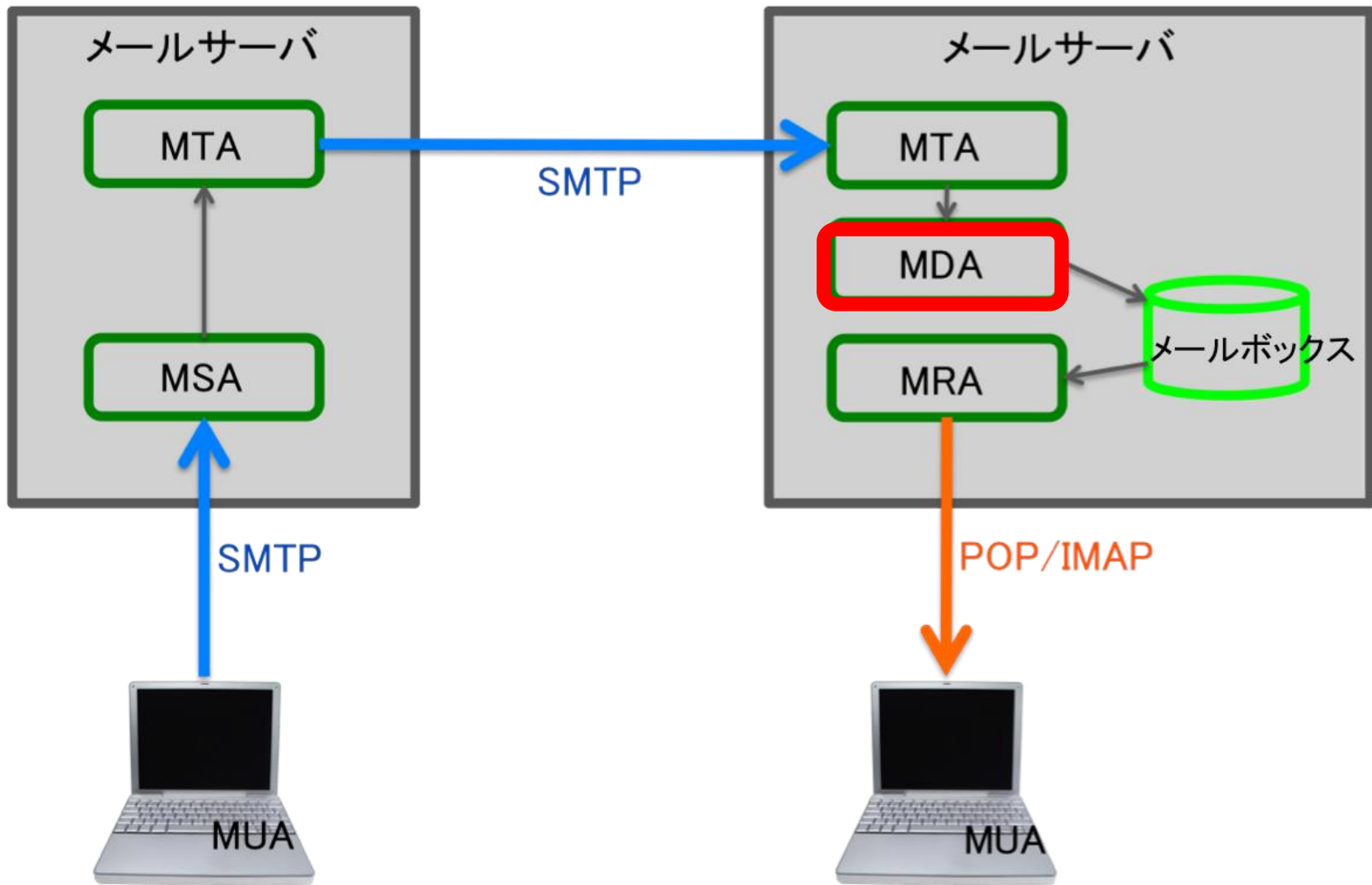
MTA とは



MTA とは

- MTA (Mail Transfer Agent)
 - メールを配送するプログラム
 - ① MUA からメールを受け取り, 適切な配送経路を決定する
 - ② 送信側のサーバから受信側のサーバへメールを転送
 - ③ (別のメールサーバから送られてきた) メールを受け取り, MDA (後述) へ振り分ける
 - 例
 - sendmail, qmail, Postfix ...etc.
 - ITPASS サーバでは qmail を使用
 - 手紙を送る場合で考えると
 - 手紙を郵便局間で郵送する役割

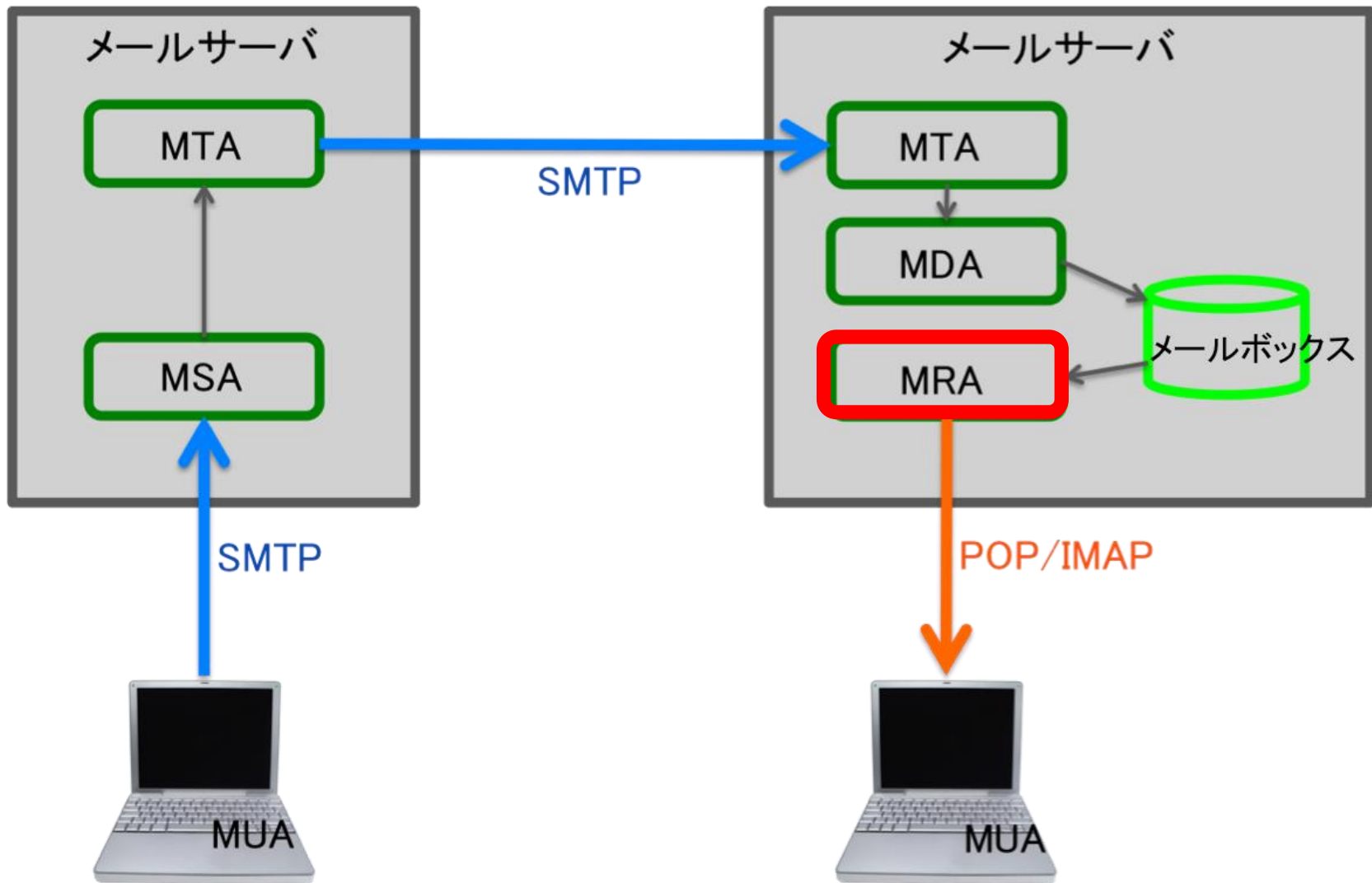
MDA とは



MDA とは

- MDA (Mail Delivery Agent)
 - メールをメールボックスに格納するプログラム
 - 例
 - mail.local, qpopper, procmail など
 - ITPASS サーバでは qpopper を使用
 - 手紙を送る場合で考えると
 - 手紙を私書箱に振り分ける役割

MRA とは



MRA とは

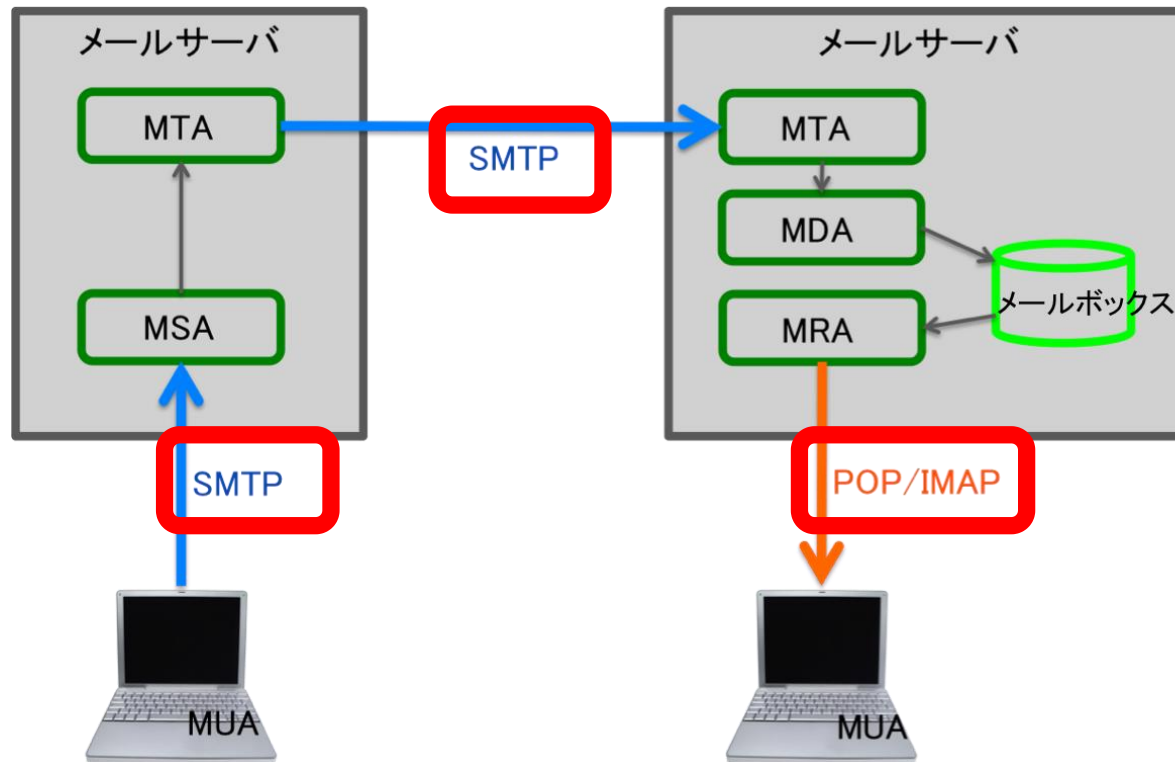
- MRA (Mail Retrieval Agent)
 - メールボックスからメールを取り出す (retrieve) プログラム
 - サーバから MUA へメールデータを転送・同期
 - MUA との間でのプロトコルは主に POP や IMAP を利用

 - 手紙を送る場合で考えると
 - 私書箱から手紙を取り出す役割

メールの送受信とプロトコル

プロトコルとは

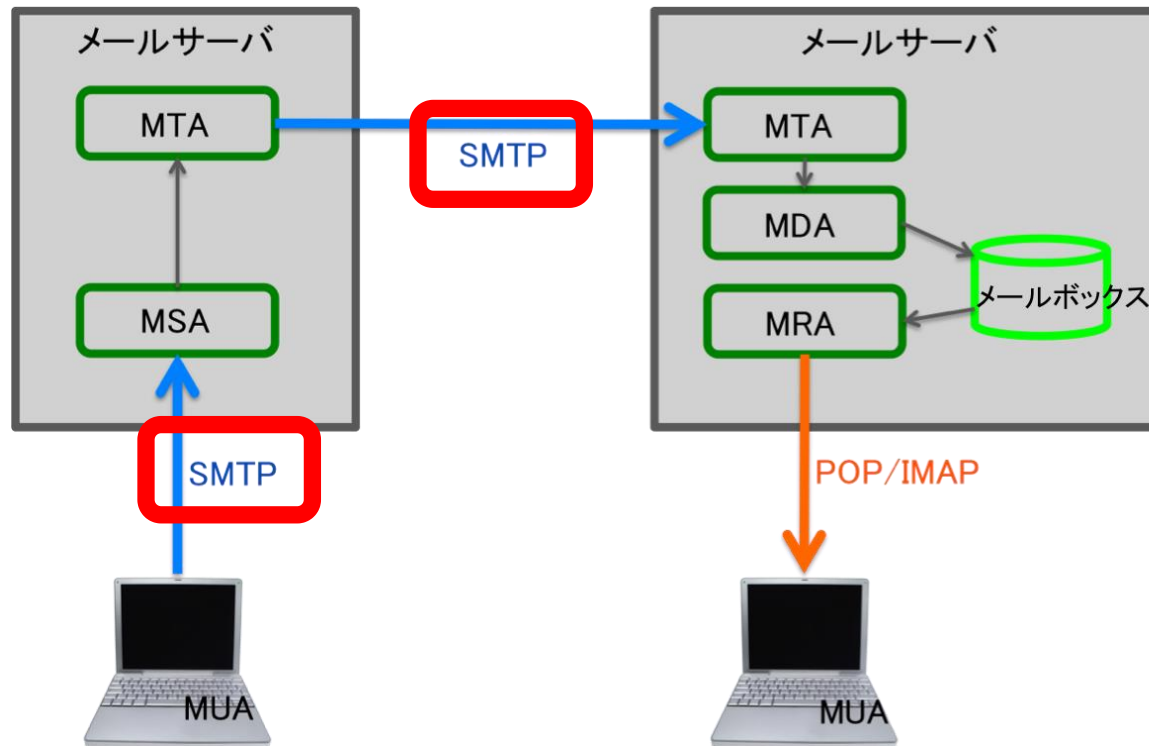
- ネットワークを介して通信する際の約束事
 - メールを送受信では SMTP, POP, IMAP



SMTP とは

- SMTP (Simple Mail Transfer Protocol)

- MUA からメールサーバへ, またメールサーバ間でメールを転送する際に使われるプロトコル
- メール転送手段を決めている



SMTP 通信で転送されるメールの構造

- SMTP エンベロープ

- 宛先と送信者の情報

- MTA によるメール転送に使用されている
 - 通常, MUA で見ることにはできない

- メール転送のため, 以下の SMTP コマンドが交わされる

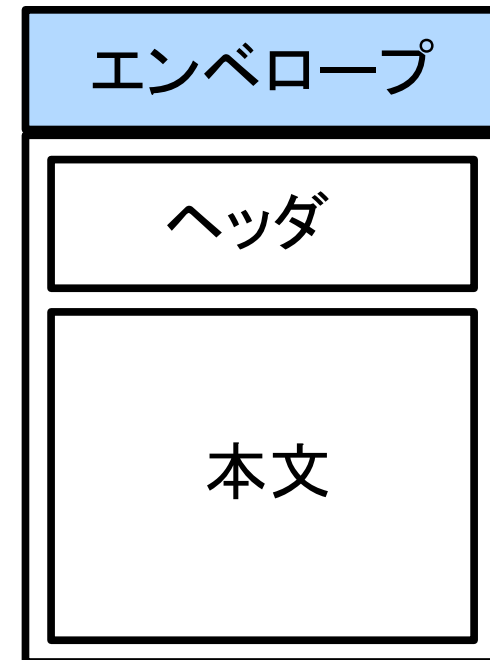
- MAIL FROM: メッセージの送信者を指定
 - RCPT TO: メッセージの受信者を指定

- SMTP コンテンツ (メール本体)

- ヘッダ

- 送信者や受信者, 送信日時などの情報
 - メール転送には使用されず, MUA で表示するため
に使用される

- 本文 (body)



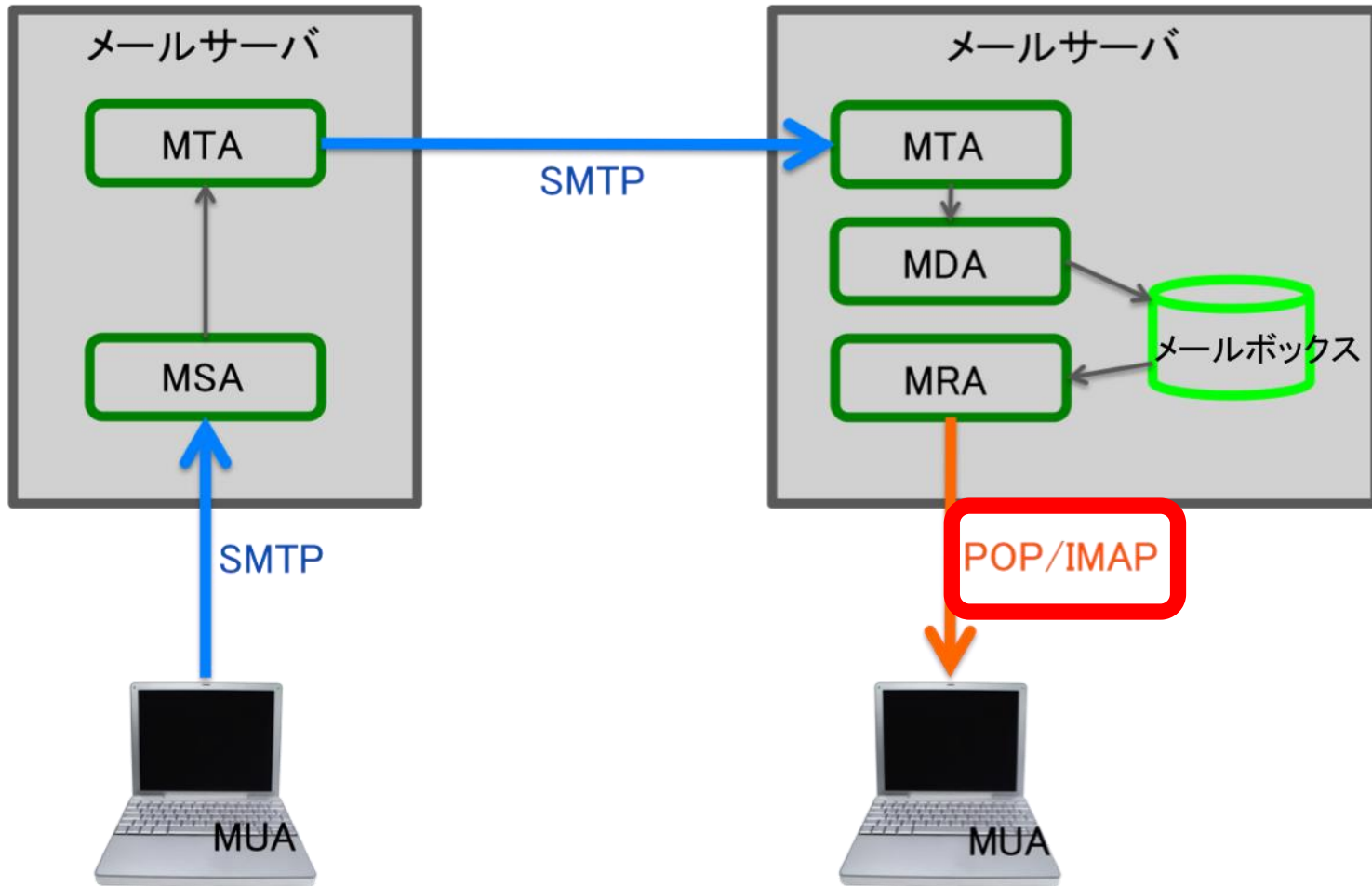
SMTP 通信の内容

- クライアントのコマンドとメールサーバーからのレスポンスで通信が行われる



	クライアント(hoge.com)	サーバ(mail.hoge.jp)
送信先サーバに接続		220 mail.hoge.jp ESMTP
接続を確認	HELO hoge.com	250 mail.hoge.jp
送信者アドレス指定	MAIL FROM: (送信元)	250 OK
宛先アドレス指定	RCPT TO: (宛先)	250 OK
メール本体の開始	DATA	354 go ahead
	(ヘッダ)	
改行		
	(メール本文)	
本文終了は「.」	.	250 OK
処理の終了	QUIT	221 mail.hoge.jp

POP / IMAP とは



POP とは

- POP (Post Office Protocol)
 - メールサーバからメールをダウンロードするためのプロトコル
- POP の特徴
 - メールの移動, 削除などを素早く処理できる
 - 端末の容量が許す限り, メールの保存が可能
 - 受信したメールはサーバから削除される
 - 残すように設定することも可能
 - 複数の端末での管理が困難
 - パスワードを平文で送る
 - POP over SSL などで認証を暗号化することができる

POPによるメールの受信

- クライアントのコマンドとメールサーバからのレスポンスで通信が行われる

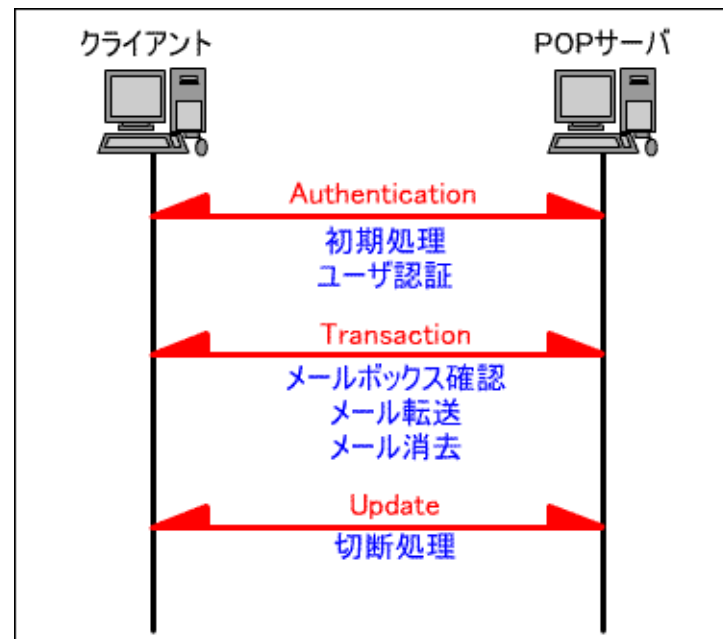
① 認証

- ユーザ名とパスワードをサーバに送信

② トランザクション

- メールの情報取得や受信など
- QUIT コマンド
 - サーバ上のメールを削除し、アップデート状態に

③ アップデート (切断)



IMAP とは

- IMAP (Internet Message Access Protocol)
 - サーバ上でメールを管理
- IMAP の特徴
 - メールの一部のみの受信が可能
 - ヘッダのみ, 添付ファイル以外など
 - メールの作成, 移動, 検索, 削除などを, 全てサーバ上で行うことができる
 - サーバに複数のメールボックスを作成できる
 - 複数の端末で管理できる
 - サーバの容量制限に達すると, 新しいメールを閲覧できない

不正な攻撃からサーバを守る仕組み

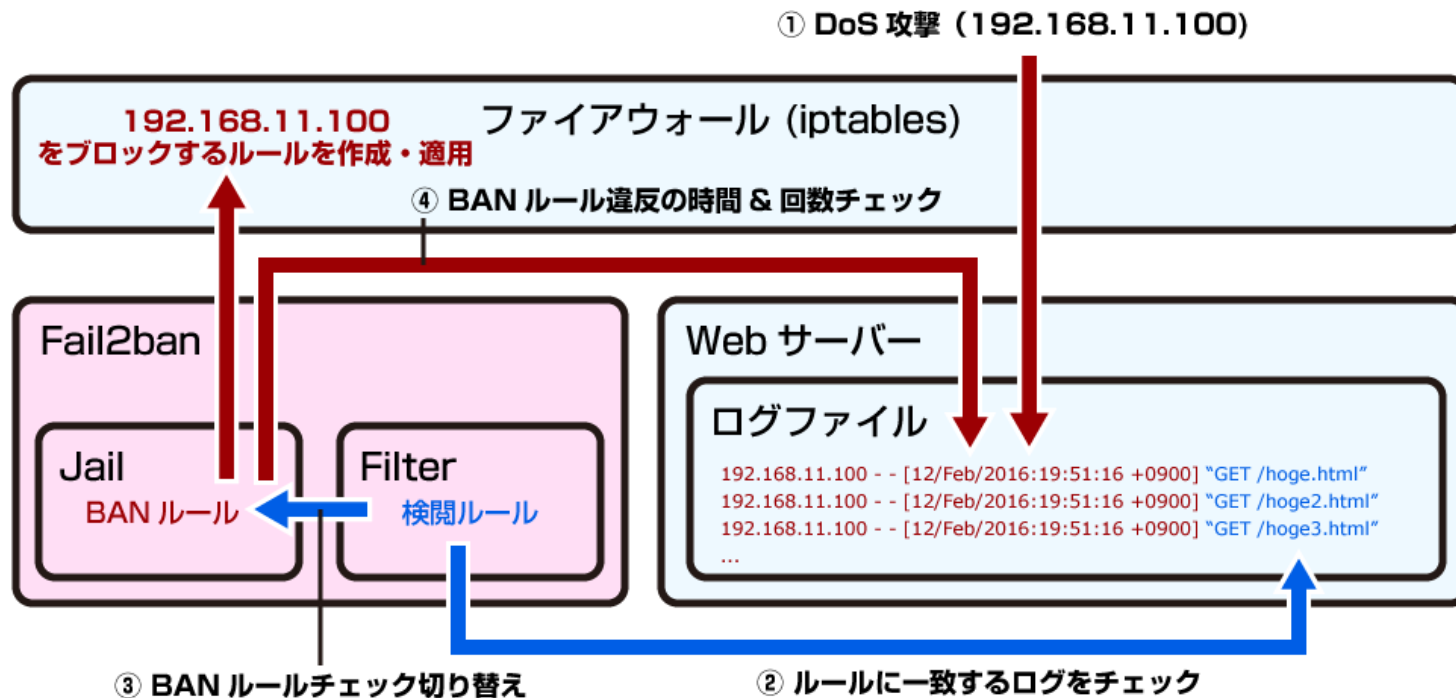
不正攻撃からサーバを守るために

- サーバを外部に公開していると, 様々な攻撃を受けダウンしてしまう可能性がある
 - DoS 攻撃 (Denial of Service attack)
 - 標的のサーバに対して大量のデータを送り付ける
 - DDoS 攻撃 (Distributed Denial of Service attack)
 - 複数のコンピュータを乗っ取り, そこから一つのサーバに大量のデータを送り付ける
- ITPASS サーバでは fail2ban を用いて対処

fail2ban

fail2ban とは

- サーバのログファイルをチェックし、設定した時間と回数を超えるアクセスをした IP アドレスを任意の時間ブロックするよう、ファイアウォール (iptables) に指示する



fail2ban とは

- サーバのログファイルに対して, filter と jail を設定
 - filter: 「どのようなアクセスを違反とみなすか」を定義
 - jail: 「どれくらいの時間」で「何回違反があった」ら「どれくらいの時間ブロックする」かを定義
- iptables の設定
 - iptables: Linux に実装されているファイアウォール機能
 - パケットフィルタリングの機能を持つ
 - 外部から受信したデータをあらかじめ設定した条件と比較して, 通過させるか破棄するかを判断

まとめ

まとめ

- メール送受信に関するプログラム
 - MUA: ユーザがメールの作成や送受信などを行うためのプログラム
 - MSA: ユーザの認証を行なうためのプログラム
 - MTA: メール配信経路を決定するためのプログラム
 - MDA: メールをメールボックスに格納するためのプログラム
 - MRA: メールボックスからメールを取り出すためのプログラム
- メール送受信に関するプロトコル
 - SMTP: メール送信に関わるプロトコル
 - POP, IMAP: メール受信に関わるプロトコル
 - IMAP はメールサーバ上でメールを一元管理

まとめ

- ITPASS サーバでは
 - MSA: なし
 - MTA: qmail を使用
 - MDA: qpopper を使用

まとめ

- サーバが様々な攻撃でダウンすることを防ぐ必要がある
- ITPASS サーバでは
 - fail2ban
 - ログファイルをチェックし, 設定したルールに違反した IP アドレスのアクセスを拒否する

参考文献

- 2018 年度 ITPASS セミナー勉強会資料「メールサーバとメール配送の仕組み」
 - <https://itpass.scitec.kobe-u.ac.jp/seminar/lecture/fy2018/181109/pub/>
- IT 用語辞典
 - <http://e-words.jp>
- メール配送の仕組み
 - [http://www2.it-shikaku.jp/top30.php?hidari=102-04-03.php&migi=km102-04.php&title=108.3%20メール転送エージェント\(MTA\)の基本](http://www2.it-shikaku.jp/top30.php?hidari=102-04-03.php&migi=km102-04.php&title=108.3%20メール転送エージェント(MTA)の基本)
- **メールの仕組み**
 - <http://docs.olab.org/XXX/netmemo/mailemailsystem.html>
- 通信用語の基礎知識「メッセージサブミッション」
 - <https://www.wdic.org/w/WDIC/メッセージサブミッション>
- 通信用語の基礎知識「SMTP」
 - <https://www.wdic.org/w/WDIC/SMTP>

参考文献

- Linuxexpert 「SMTP 配送の仕組みと sendmail」
 - <http://linuxexpert.ne.jp/modules/pukiwiki/46.html>
- **トレンドマイクロ Q&A ページ「SMTP: エンベロープとヘッダについて」**
 - <http://esupport.trendmicro.com/solution/ja-jp/1306779.aspx?print=true>
- Cuenote 「SMTP 通信の流れ」
 - <https://www.cuenote.jp/documents/smtp/000193.html>
- 通信用語の基礎知識「IMAP」
 - <https://www.wdic.org/w/WDIC/IMAP>
- メールサービス
 - <http://fctv.mitene.jp/mail/which.html>
- DoS 攻撃・DDoS 攻撃とは？
 - <https://cybersecurity-jp.com/security-measures/18262>
- DoS 攻撃 / DDoS 攻撃からサーバーを守る方法 (fail2ban のススメ)
 - <https://colo-ri.jp/develop/2016/02/fail2ban.html>

参考文献

- Linux の iptables によるパケットフィルタリング入門
 - <http://eno0514.hatenadiary.jp/entry/20150617/1434525167>
- 実用 qmail サーバ運用・管理術 (1): qmail による SMTP サーバの構築
 - <http://www.atmarkit.co.jp/ait/articles/0109/04/news002.html>
- 実用 qmail サーバ運用・管理術 (4): メールングリストの構築と運用 (前編)
 - <http://www.atmarkit.co.jp/ait/articles/0112/11/news002.html>

補足 . SMTPコマンド

- EHLO...サーバーがサポートしている ESMTP コマンドを、サーバー自体が認識できるようにする
- MAIL FROM...メッセージの送信者を指定
- RCPT TO...メッセージの受信者を指定
- DATA...メッセージの内容の送信を開始
- QUIT...セッションを終了

補足 . SMTPレスポンス一覧その1

- 211 ... システムのステータス , システムヘルプ応答
- 214 ... ヘルプメッセージ , コマンド使用方法
- 220 ... パラメータに指定されるドメイン名のサーバを準備
- 221 ... コネクションのクローズ (QUIT への応答)
- 250 ... リクエストされたコマンドの終了
- 251 ... 宛先として指定されたアドレスがローカルに存在しないことを示す
- 252 ... VRFY コマンドでユーザーが確認できないことを示す
 - ユーザーがローカルに存在しない
 - メールの送信は可能である
- 354 ... メールデータの入力を促す
 - 最後は <CR> <LF> <CR> <LF> で終了すること

補足 . SMTPレスポンス一覧その2

- 412 ... ホストのメールサービスが起動していないことを示す
- TCP コネクションを切断
 - メール転送中のサーバのシャットダウン時にもこのレスポンス
- 450 ... メールボックスがビジーであるため、リクエストされたコマンドが実行されない
- 451 ... ローカルエラーのため、指定コマンドが実行されない
- 452 ... リクエストされたコマンドは実行されない
- 500 ... コマンドの文法エラー
- 501 ... 指定コマンドのパラメータエラー

補足 . POPでのコマンド&レスポンスその1

- コマンド一覧

- Authentication : クライアントの確認

- USER ... ユーザー名
 - PASS ... パスワード
 - APOP ... USER と PASS の代わりに用いるユーザーの認証のためのコマンド

- Transaction : メッセージに対する操作

- STAT ... 受信メール数とそのサイズの表示要求
 - LIST ... 受信メールの一覧と各メールのサイズの表示要求
 - RETR ... 指定した受信メールの転送要求

補足 . POPでのコマンド&レスポンスその2

- コマンド一覧

- Update

- QUIT … 接続を切断して終了

- ※ DERE で指定したメールがあれば消去

- レスポンス

- + OK 状態表示 … 肯定反応

- - ERR 状態表示 … 否定反応