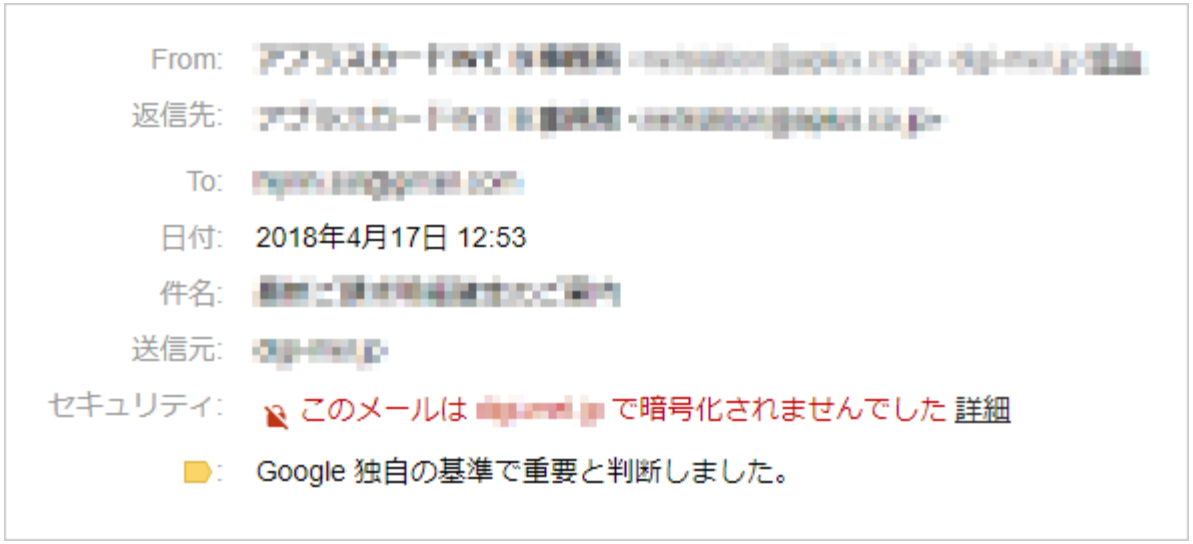
ENOG50

メールの話をしよう

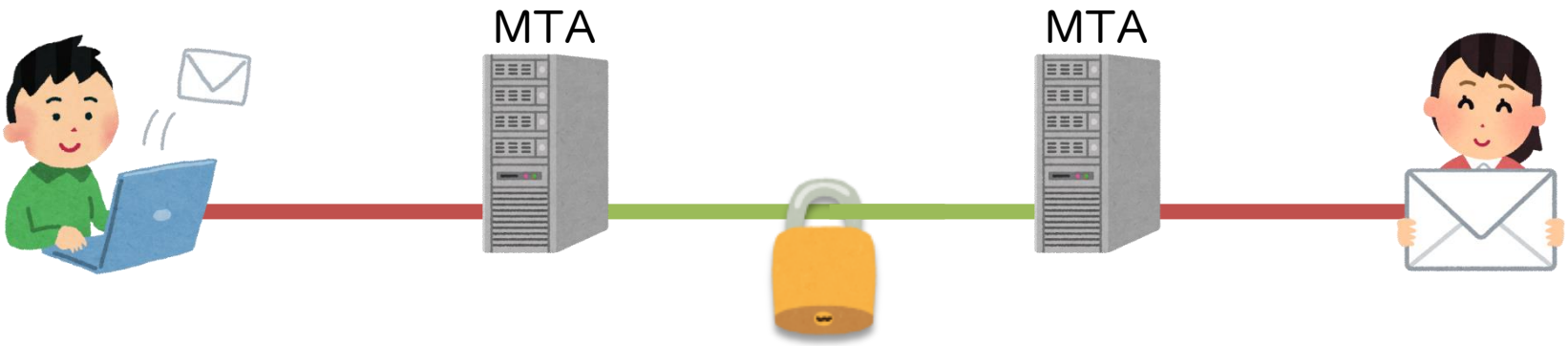
株式会社 新潟通信サービス
櫻井 佑樹


暗号化なし


From:
To:
Cc:
日付: 2016年5月17日 23:11
件名:
セキュリティ: 暗号化なし 詳細


From:
返信先:
To:
日付: 2018年4月17日 12:53
件名:
送信元:
セキュリティ: このメールは で暗号化されませんでした 詳細
: Google 独自の基準で重要と判断しました。


MTA
MTA

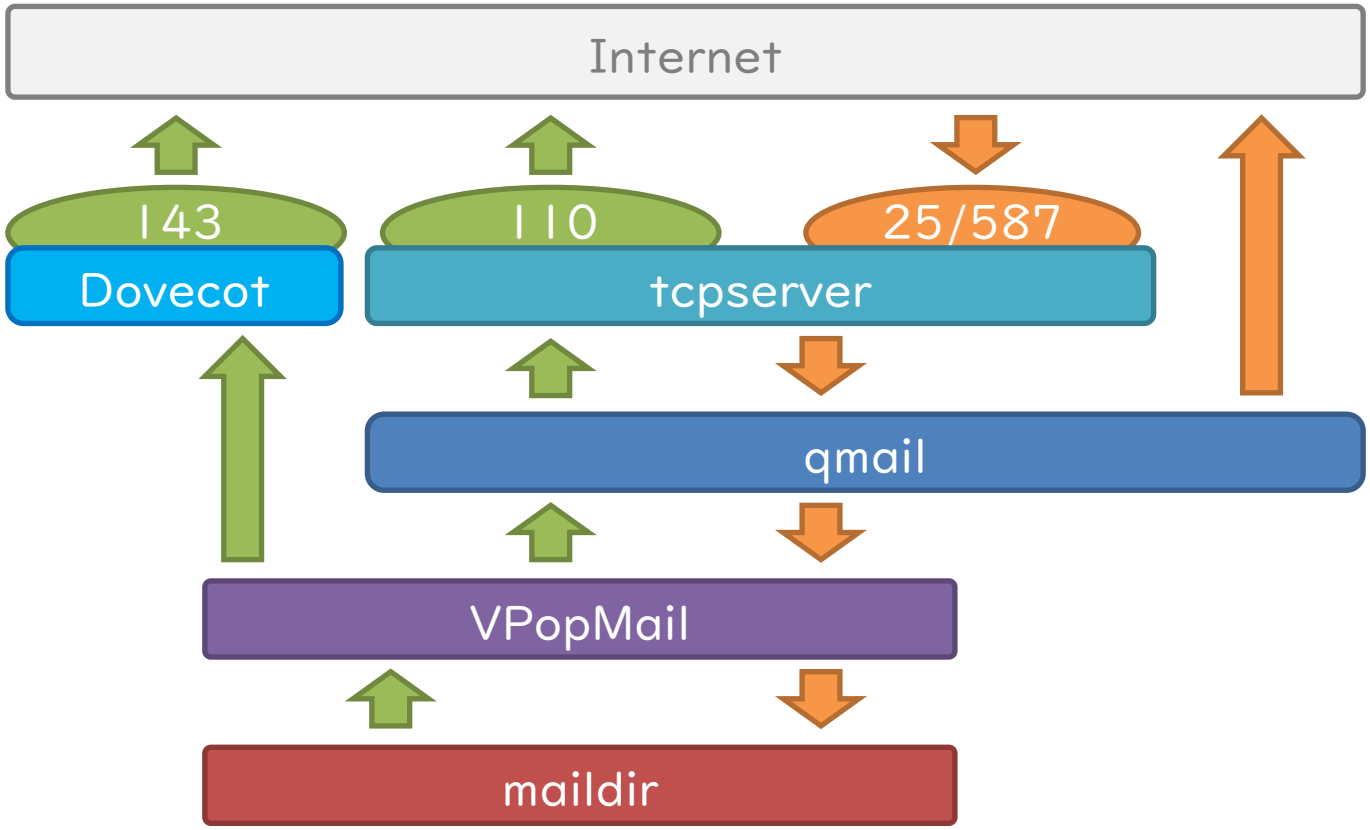

MTA
MTA

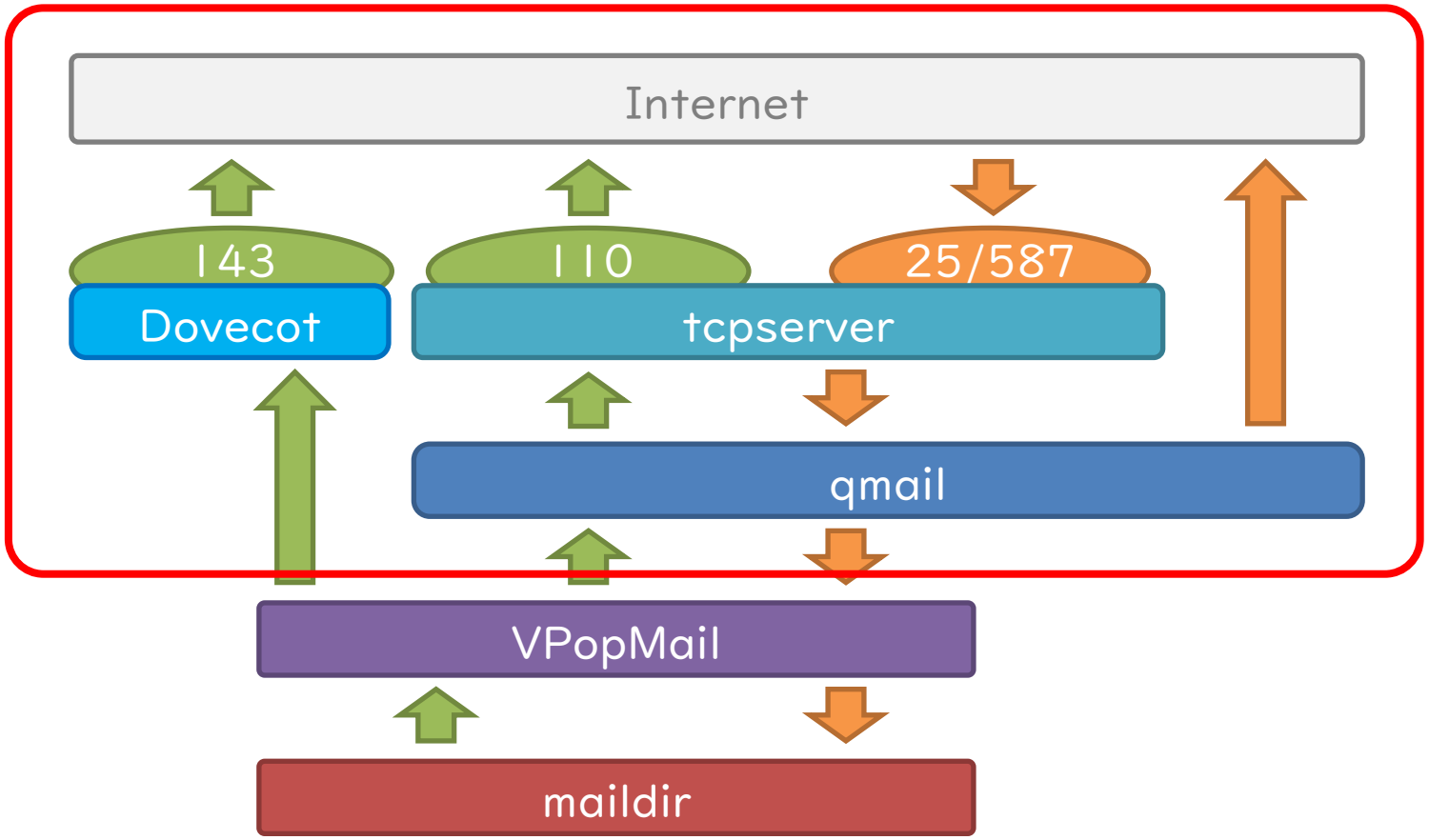
SMTP(25)
SUBMISSION(587)
↓
SMTP over SSL(465)

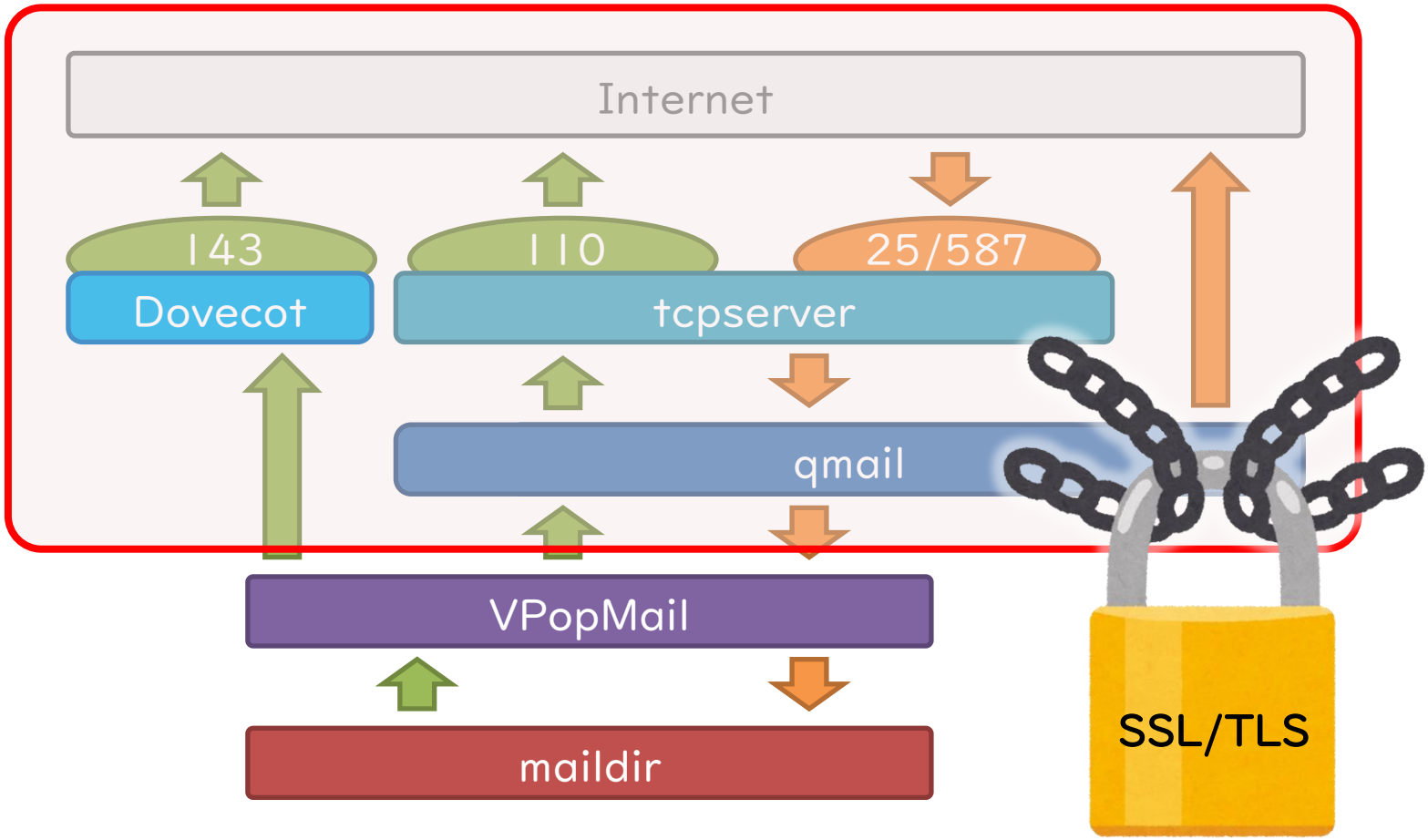
SMTP(25)
↓
SMTP over SSL(465)

POP3(110)
↓
POP3 over SSL(995)

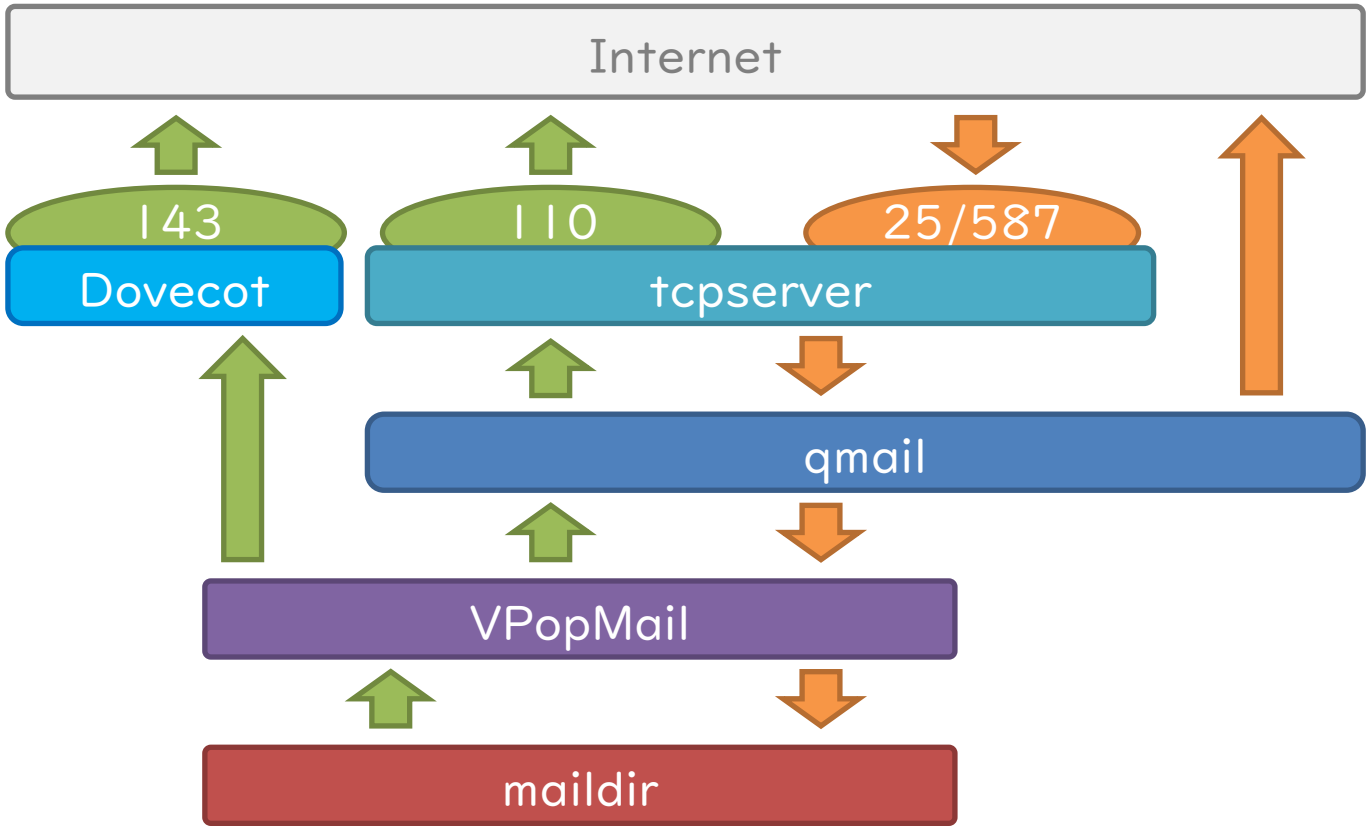
IMAP(143)
↓
IMAP over SSL(993)


Internet
143
110
25/587
Dovecot
tcpserver
qmail
VPopMail
maildir

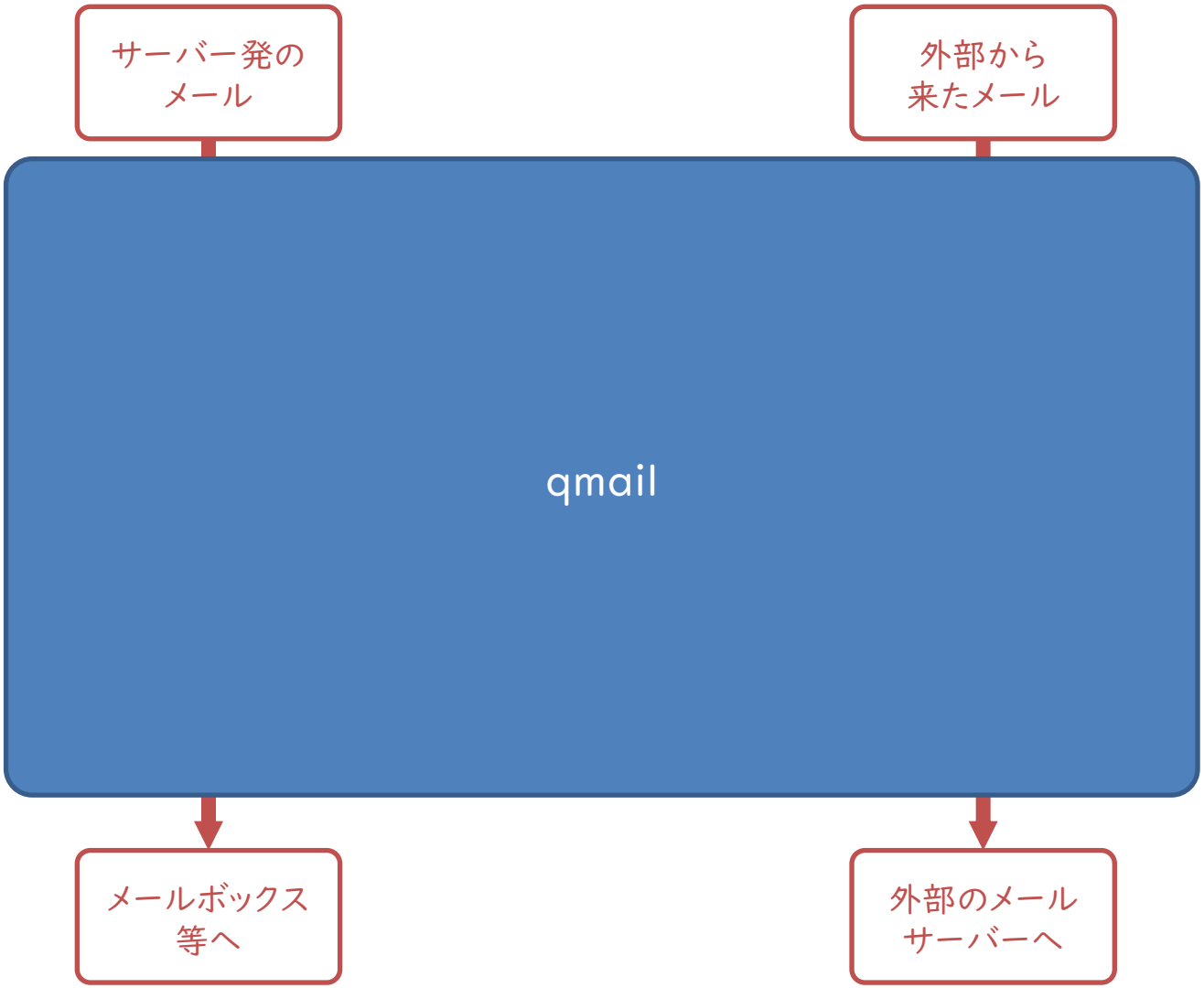

Internet
143
110
25/587
Dovecot
tcpserver
qmail
VPopMail
maildir


Internet
143
110
25/587
Dovecot
tcpserver
qmail
VPopMail
maildir
SSL/TLS

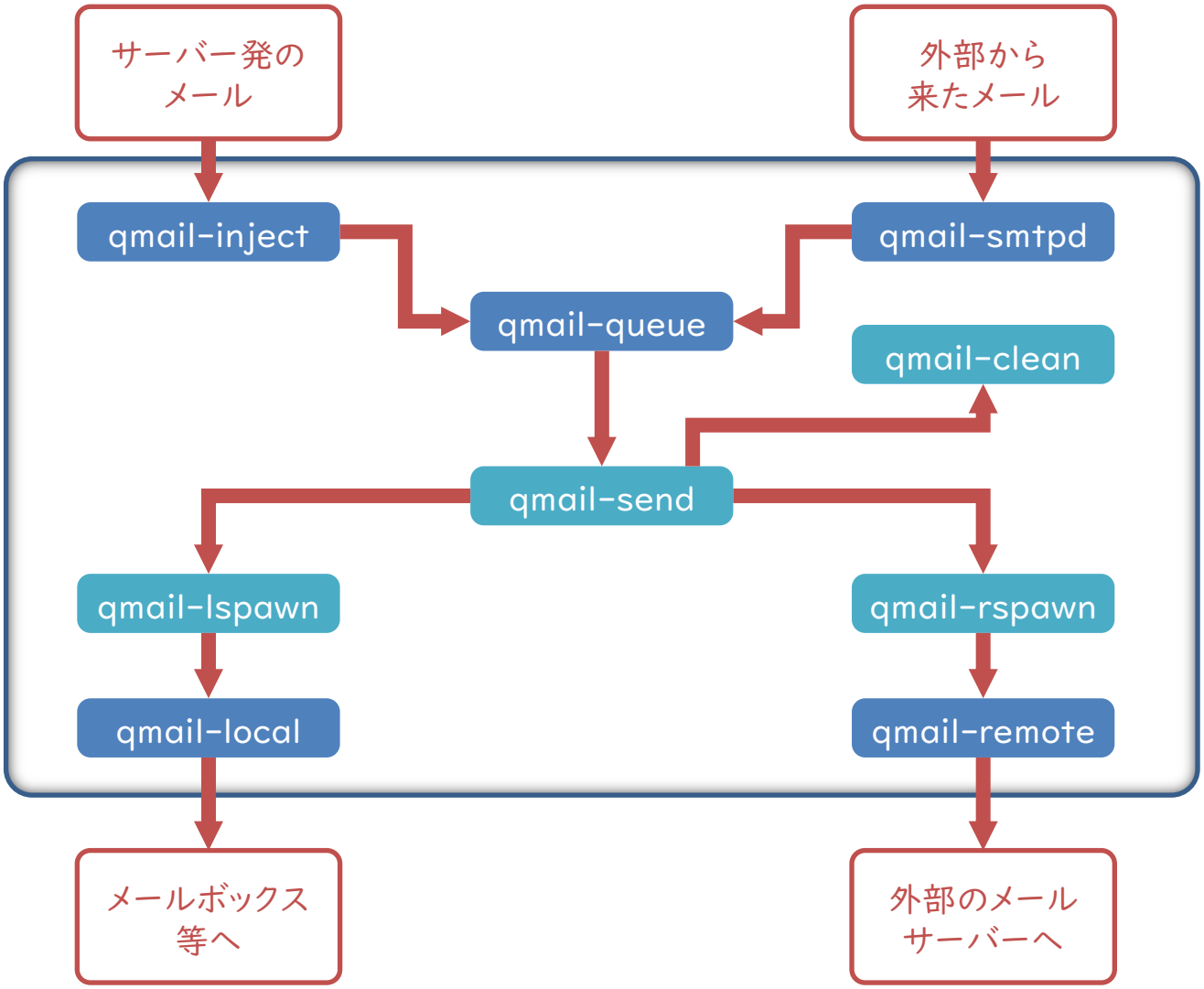
①現在の構成のSSL化・・・の前に



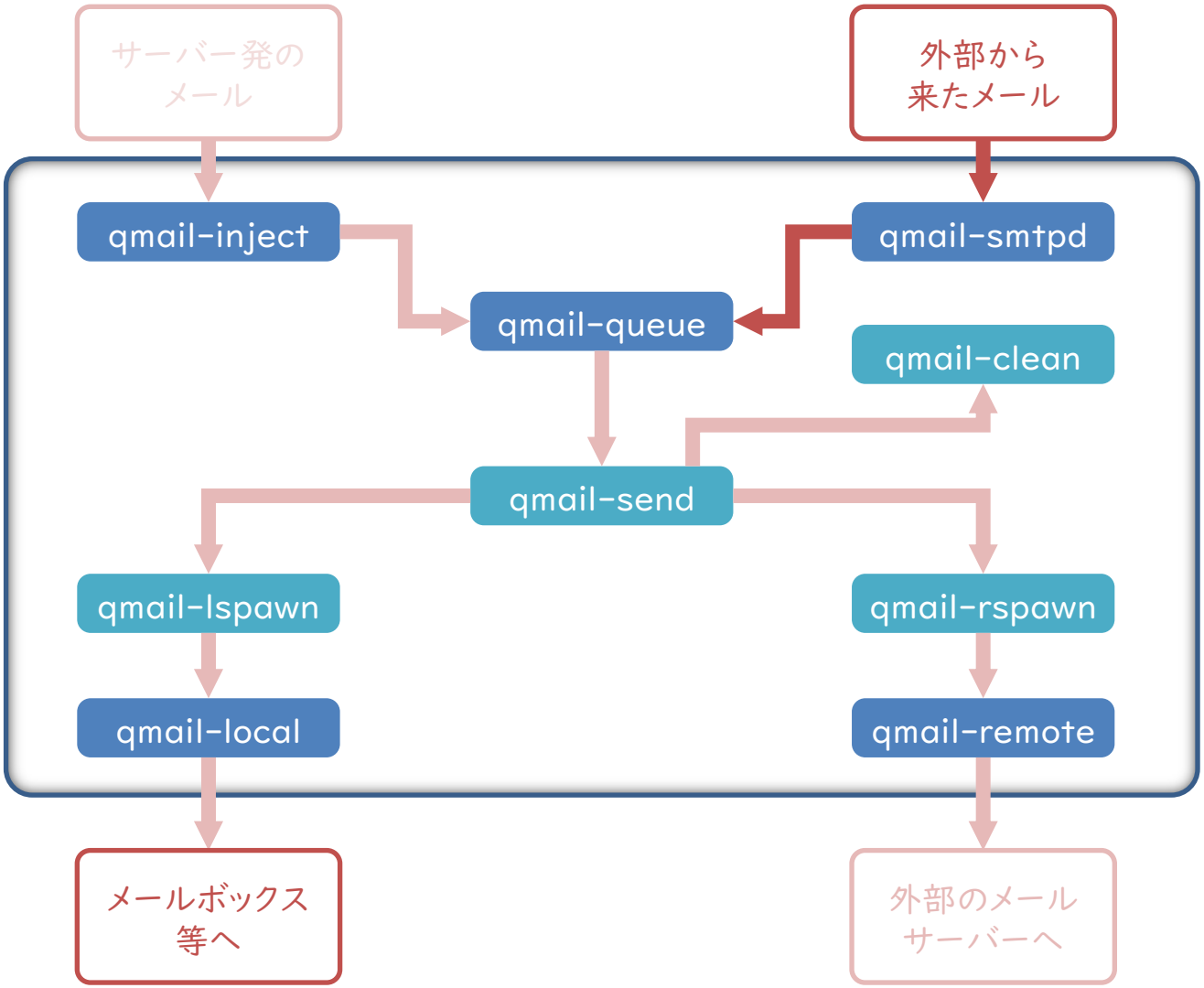
qmailのしくみ



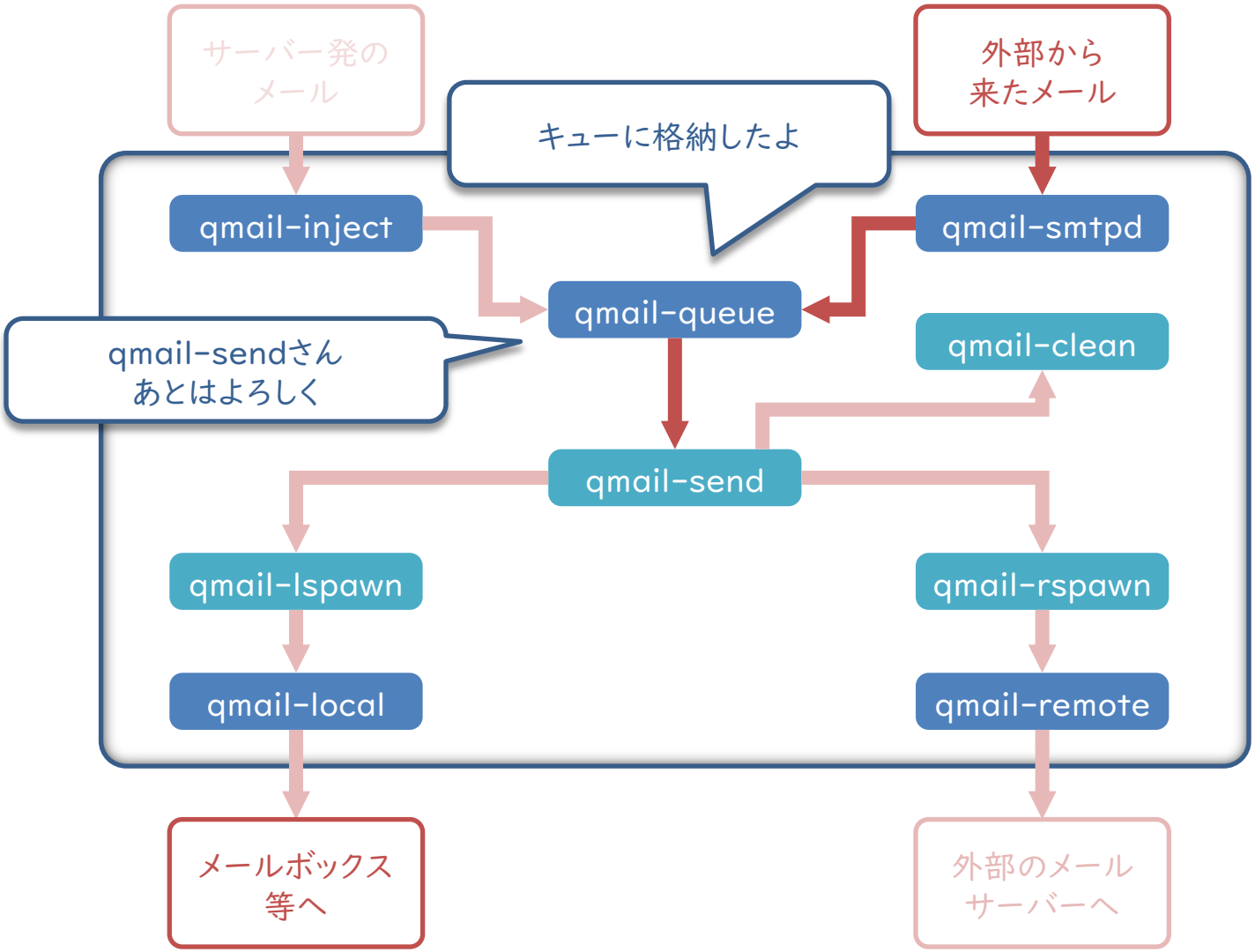
qmailのしくみ


サーバー発の
メール
外部から
来たメール
qmail-inject
qmail-smtpd
qmail-queue
qmail-clean
qmail-send
qmail-lspawn
qmail-rspawn
qmail-local
qmail-remote
メールボックス
等へ
外部のメール
サーバーへ

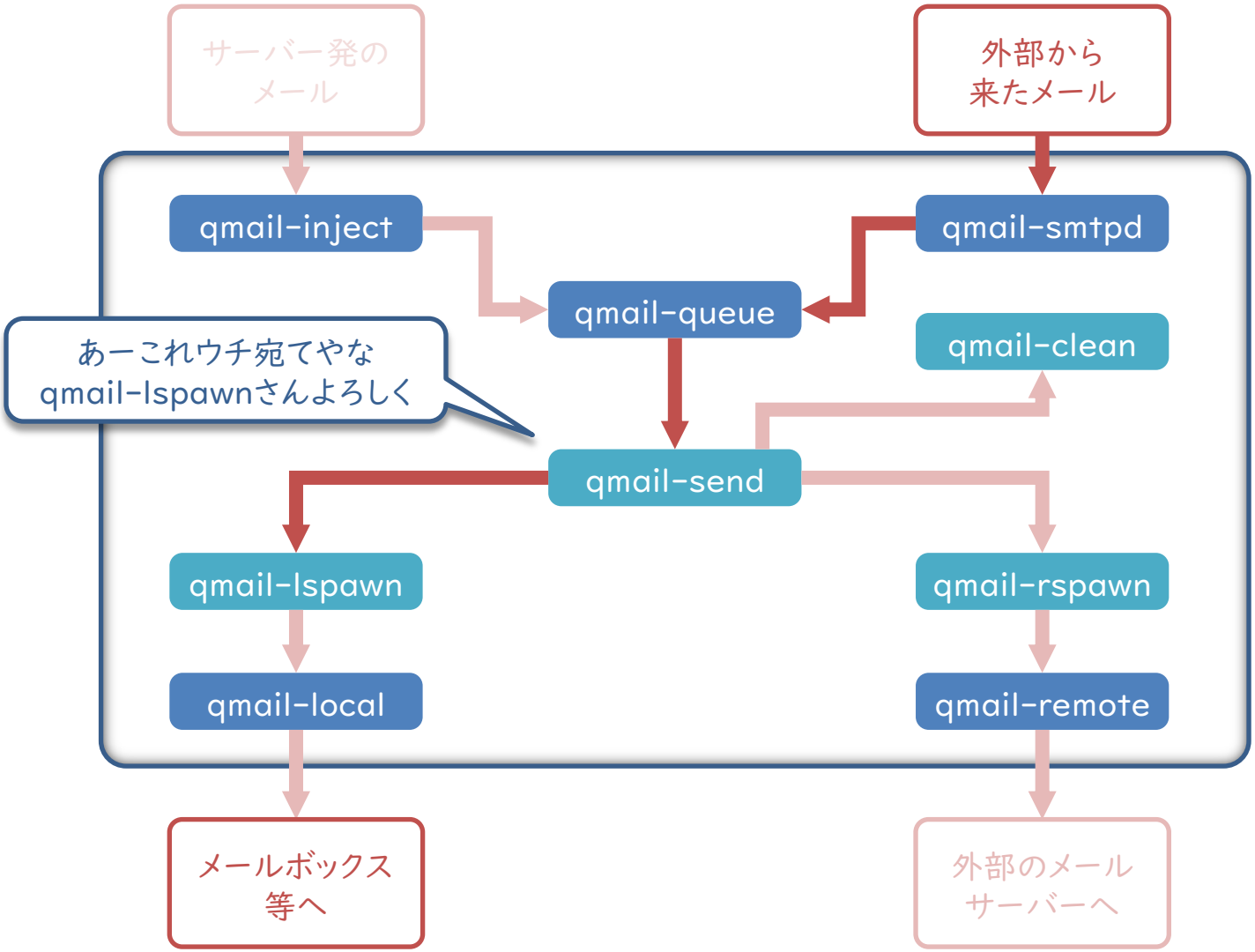
qmailのしくみ


サーバー発の
メール
外部から
来たメール
qmail-inject
qmail-smtpd
qmail-queue
qmail-clean
qmail-send
qmail-lspawn
qmail-rspawn
qmail-local
qmail-remote
メールボックス
等へ
外部のメール
サーバーへ

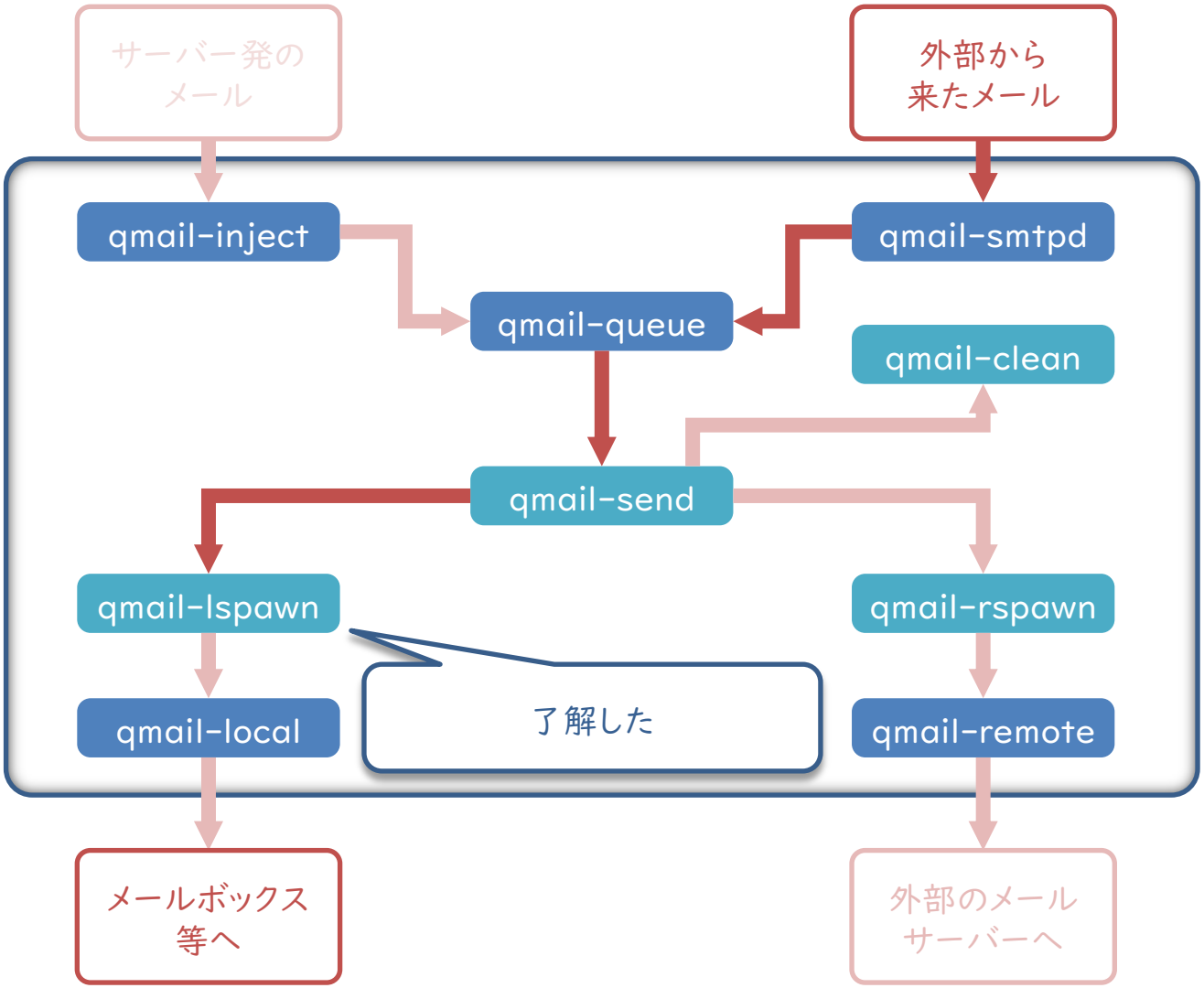
qmailのしくみ


サーバー発の
メール
外部から
来たメール
キューに格納したよ
qmail-inject
qmail-smtpd
qmail-queue
qmail-sendさん
あとはよろしく
qmail-clean
qmail-send
qmail-lspawn
qmail-rspawn
qmail-local
qmail-remote
メールボックス
等へ
外部のメール
サーバーへ

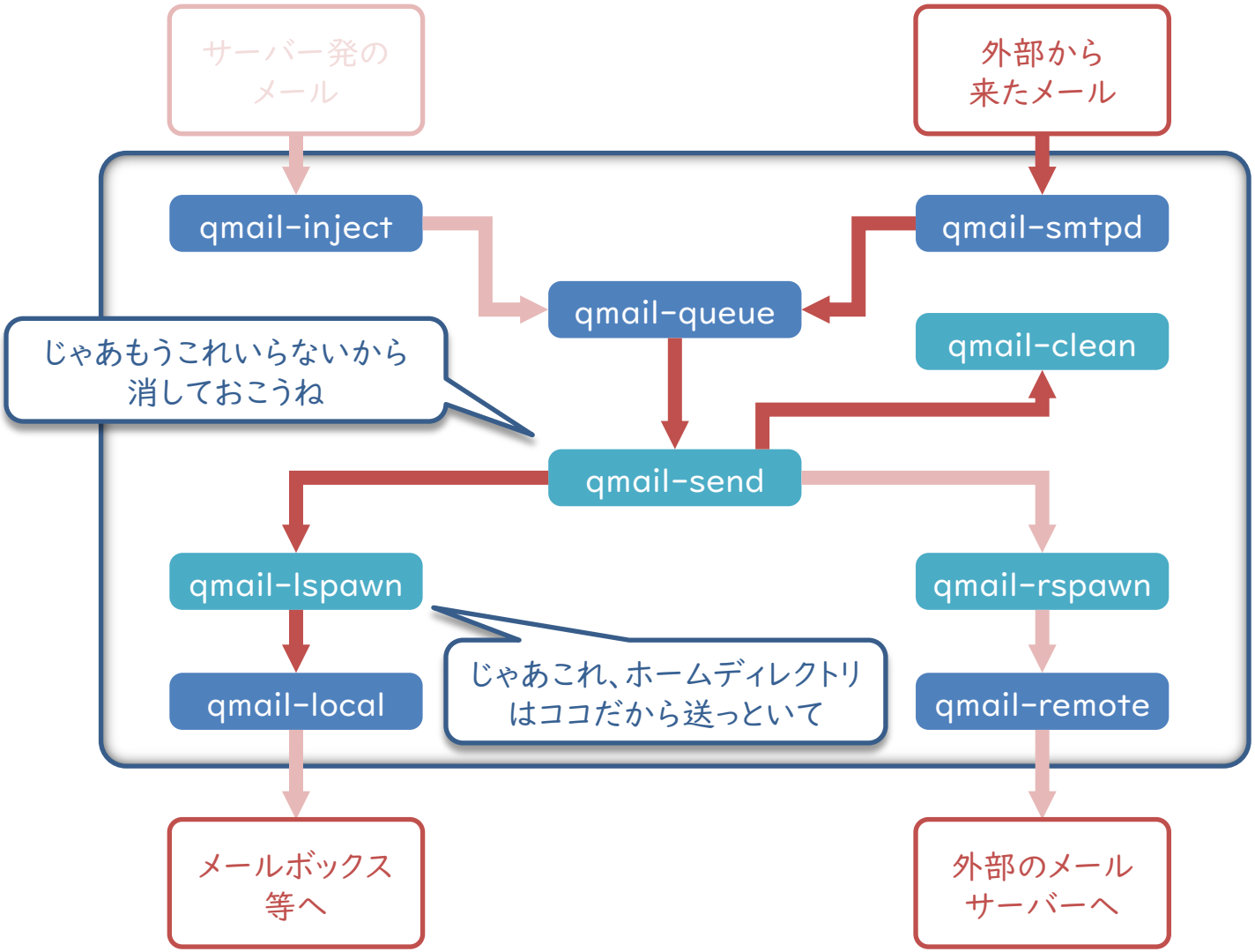
qmailのしくみ


サーバー発の
メール
外部から
来たメール
qmail-inject
qmail-smtpd
qmail-queue
qmail-clean
あーこれウチ宛てやな
qmail-lspawnさんよろしく
qmail-send
qmail-lspawn
qmail-rspawn
qmail-local
qmail-remote
メールボックス
等へ
外部のメール
サーバーへ

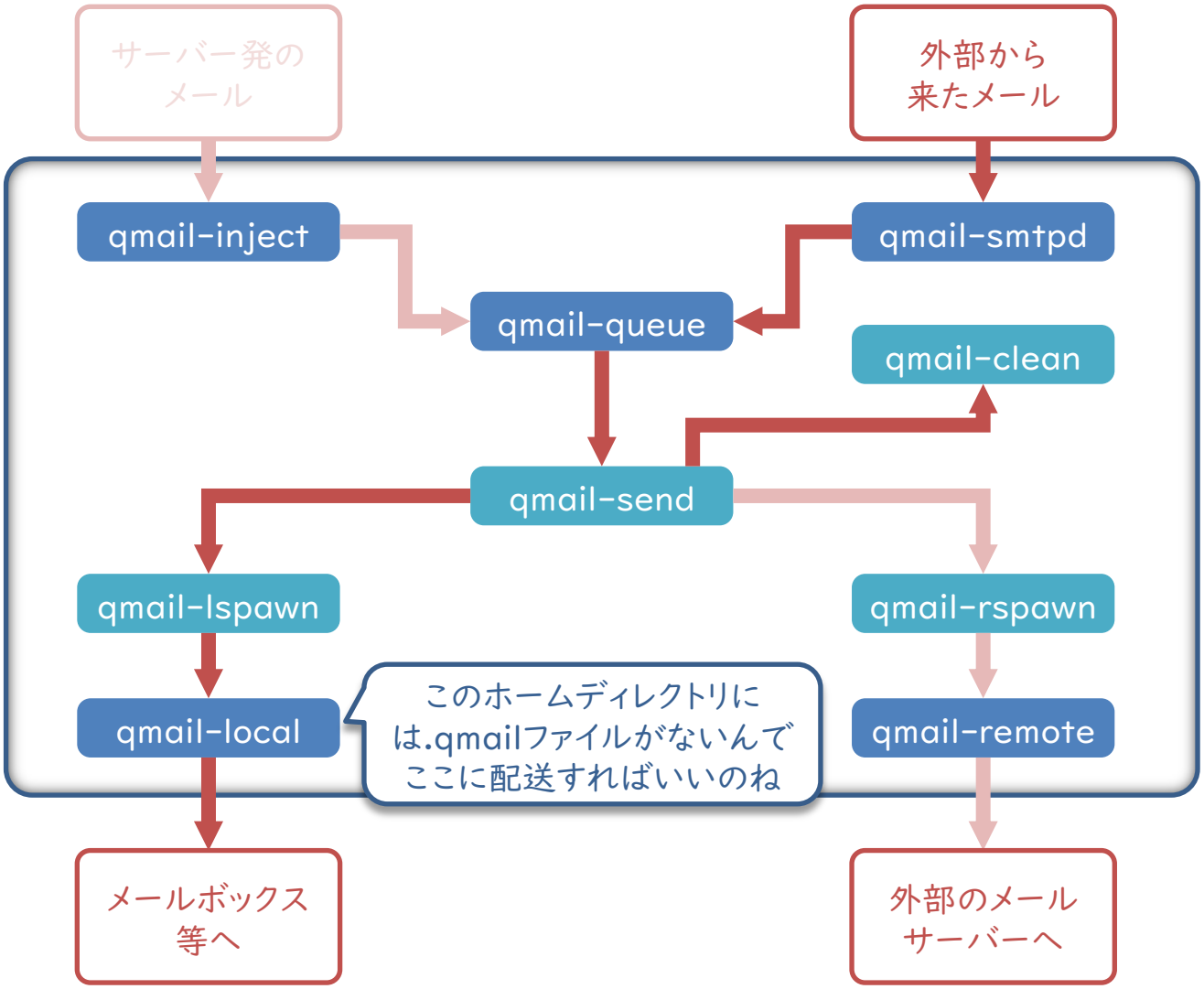
qmailのしくみ


サーバー発の
メール
外部から
来たメール
qmail-inject
qmail-smtpd
qmail-queue
qmail-clean
qmail-send
qmail-lspawn
qmail-rspawn
了解した
qmail-local
qmail-remote
メールボックス
等へ
外部のメール
サーバーへ

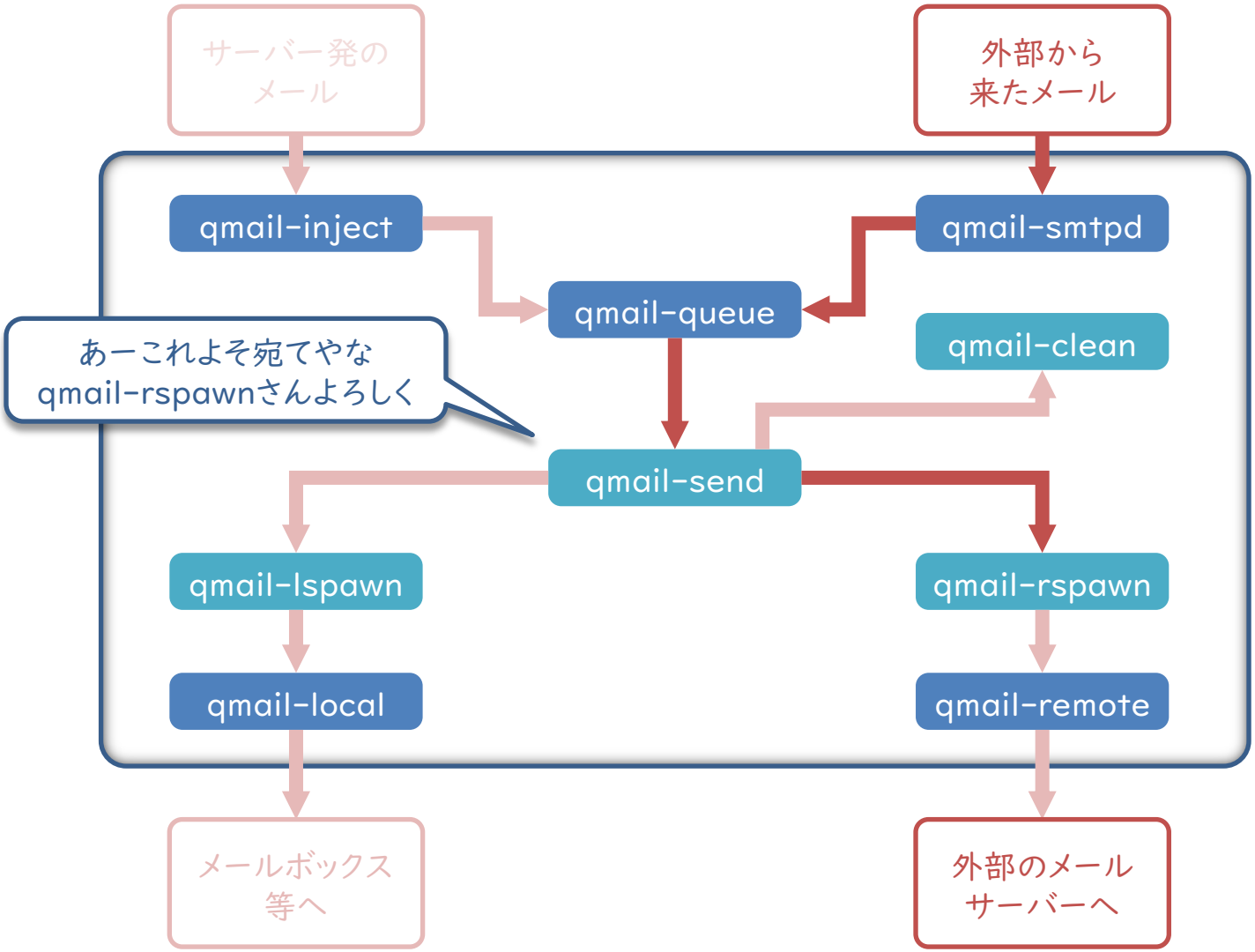
qmailのしくみ


サーバー発の
メール
外部から
来たメール
qmail-inject
qmail-smtpd
qmail-queue
qmail-clean
じゃあもうこれいらないから
消しておこうね
qmail-send
qmail-lspawn
qmail-rspawn
じゃあこれ、ホームディレクトリ
はココだから送っといて
qmail-local
qmail-remote
メールボックス
等へ
外部のメール
サーバーへ

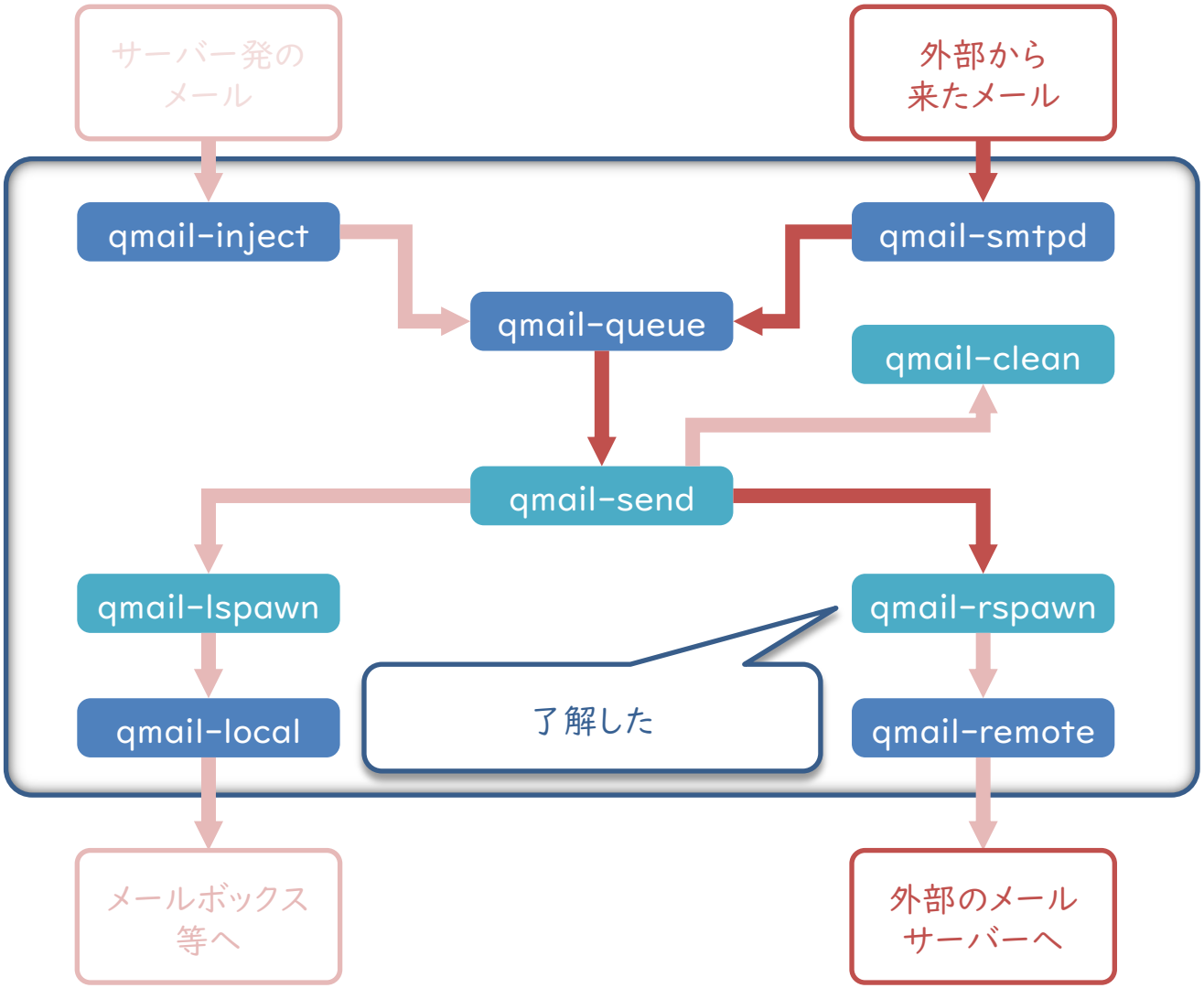
qmailのしくみ


サーバー発の
メール
外部から
来たメール
qmail-inject
qmail-smtpd
qmail-queue
qmail-clean
qmail-send
qmail-lspawn
qmail-rspawn
qmail-local
qmail-remote
このホームディレクトリに
は.qmailファイルがないんで
ここに配送すればいいのね
メールボックス
等へ
外部のメール
サーバーへ

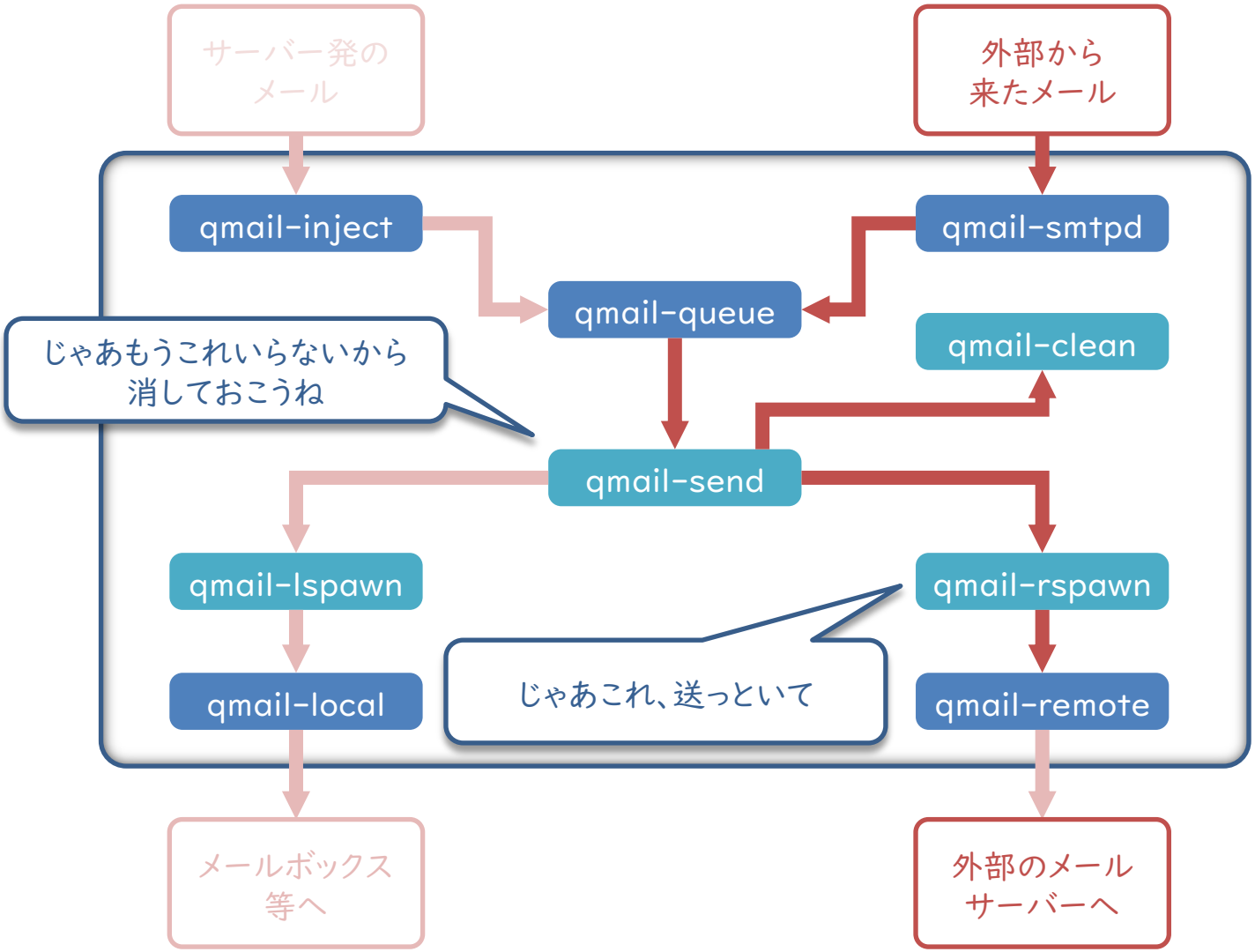
qmailのしくみ


サーバー発の
メール
外部から
来たメール
qmail-inject
qmail-smtpd
qmail-queue
qmail-clean
あーこれよそ宛てやな
qmail-rspawnさんよろしく
qmail-send
qmail-lspawn
qmail-rspawn
qmail-local
qmail-remote
メールボックス
等へ
外部のメール
サーバーへ

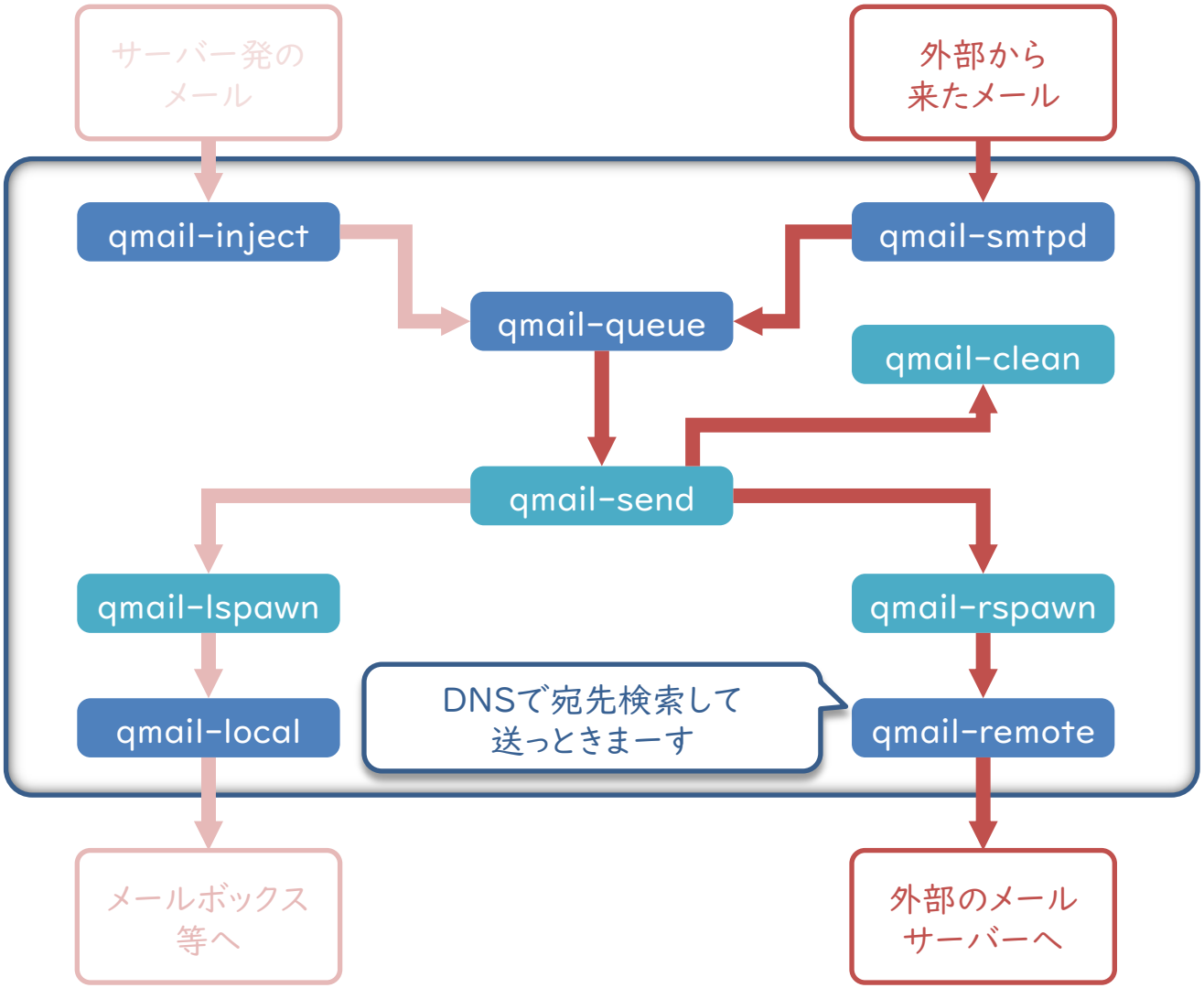
qmailのしくみ


サーバー発の
メール
外部から
来たメール
qmail-inject
qmail-smtpd
qmail-queue
qmail-clean
qmail-send
qmail-lspawn
qmail-rspawn
了解した
qmail-local
qmail-remote
メールボックス
等へ
外部のメール
サーバーへ

qmailのしくみ


サーバー発の
メール
外部から
来たメール
qmail-inject
qmail-smtpd
qmail-queue
qmail-clean
じゃあもうこれいらないから
消しておこうね
qmail-send
qmail-lspawn
qmail-rspawn
じゃあこれ、送っといて
qmail-local
qmail-remote
メールボックス
等へ
外部のメール
サーバーへ

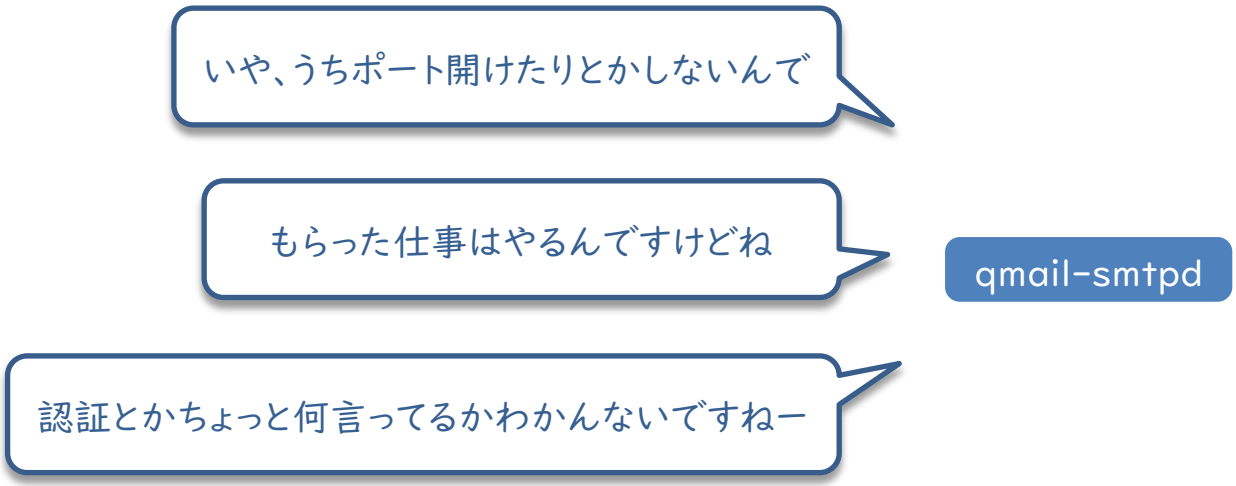
qmailのしくみ


サーバー発の
メール
外部から
来たメール
qmail-inject
qmail-smtpd
qmail-queue
qmail-clean
qmail-send
qmail-lspawn
qmail-rspawn
DNSで宛先検索して
送っときまーす
qmail-local
qmail-remote
メールボックス
等へ
外部のメール
サーバーへ

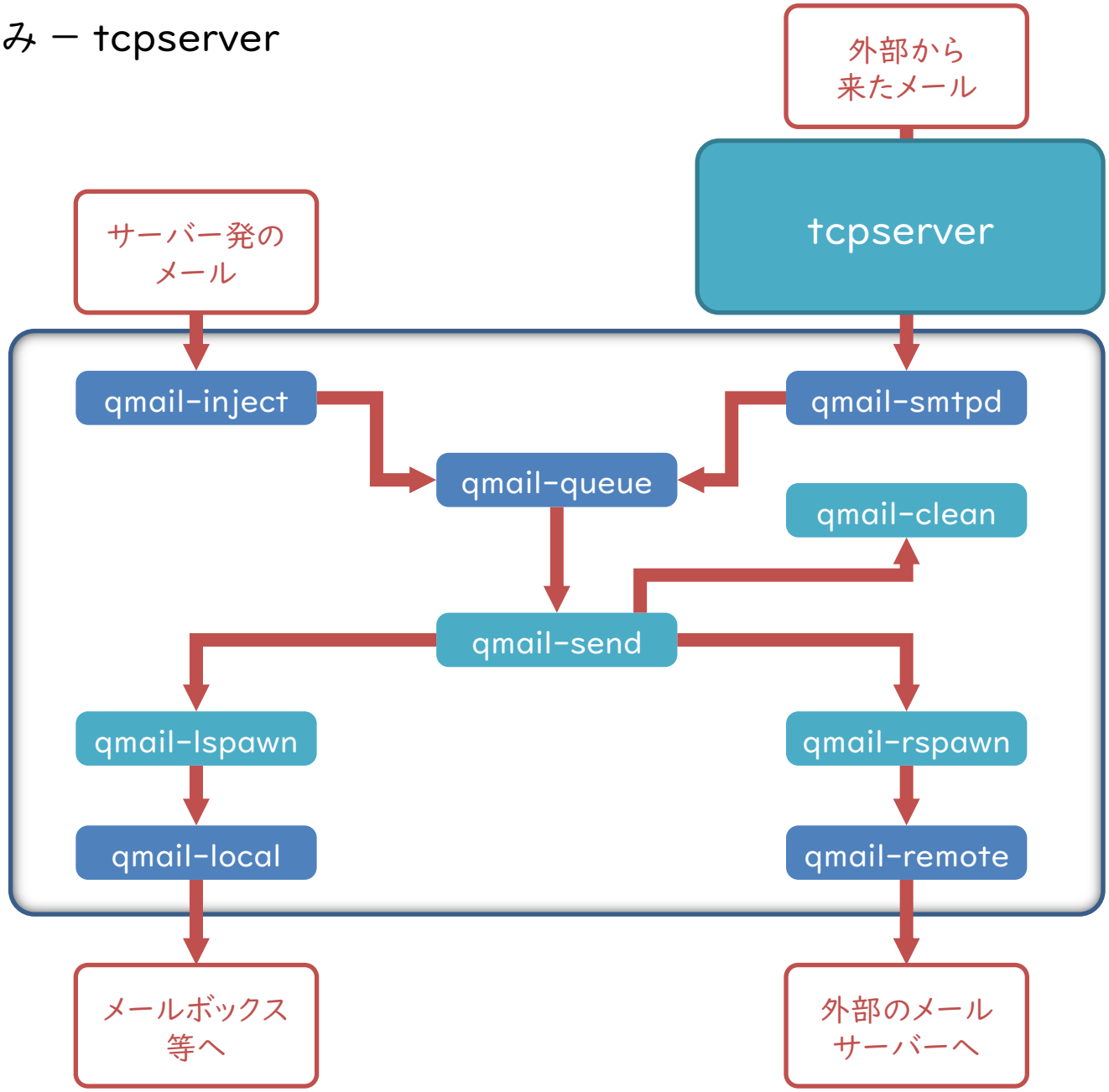
qmailのしくみ

qmail-smtpd

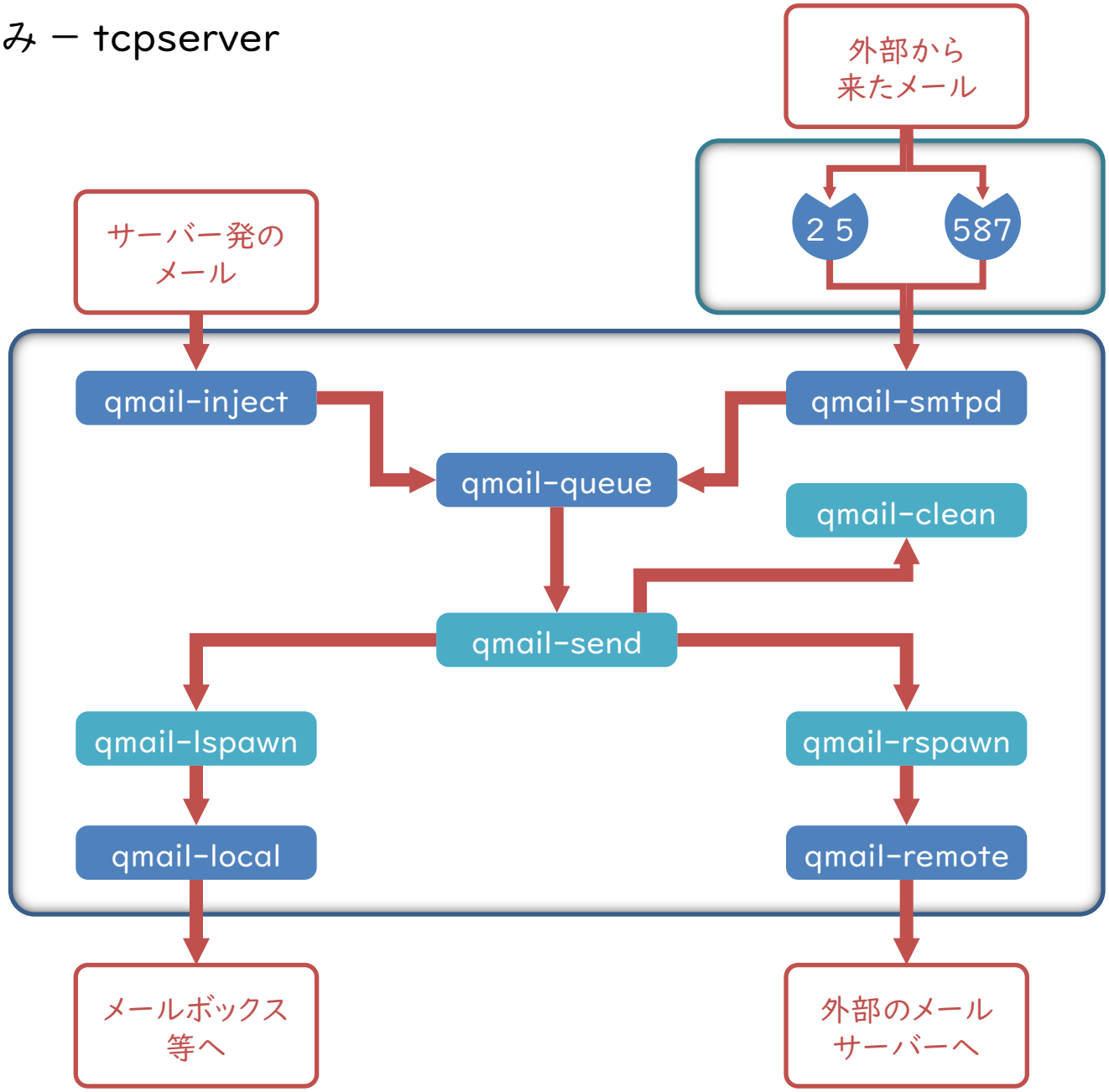
qmailのしくみ


いや、うちポート開けたりとかしないんで
もらった仕事はやるんですけどね
認証とかちょっと何言ってるかわかんないですねー
qmail-smtpd

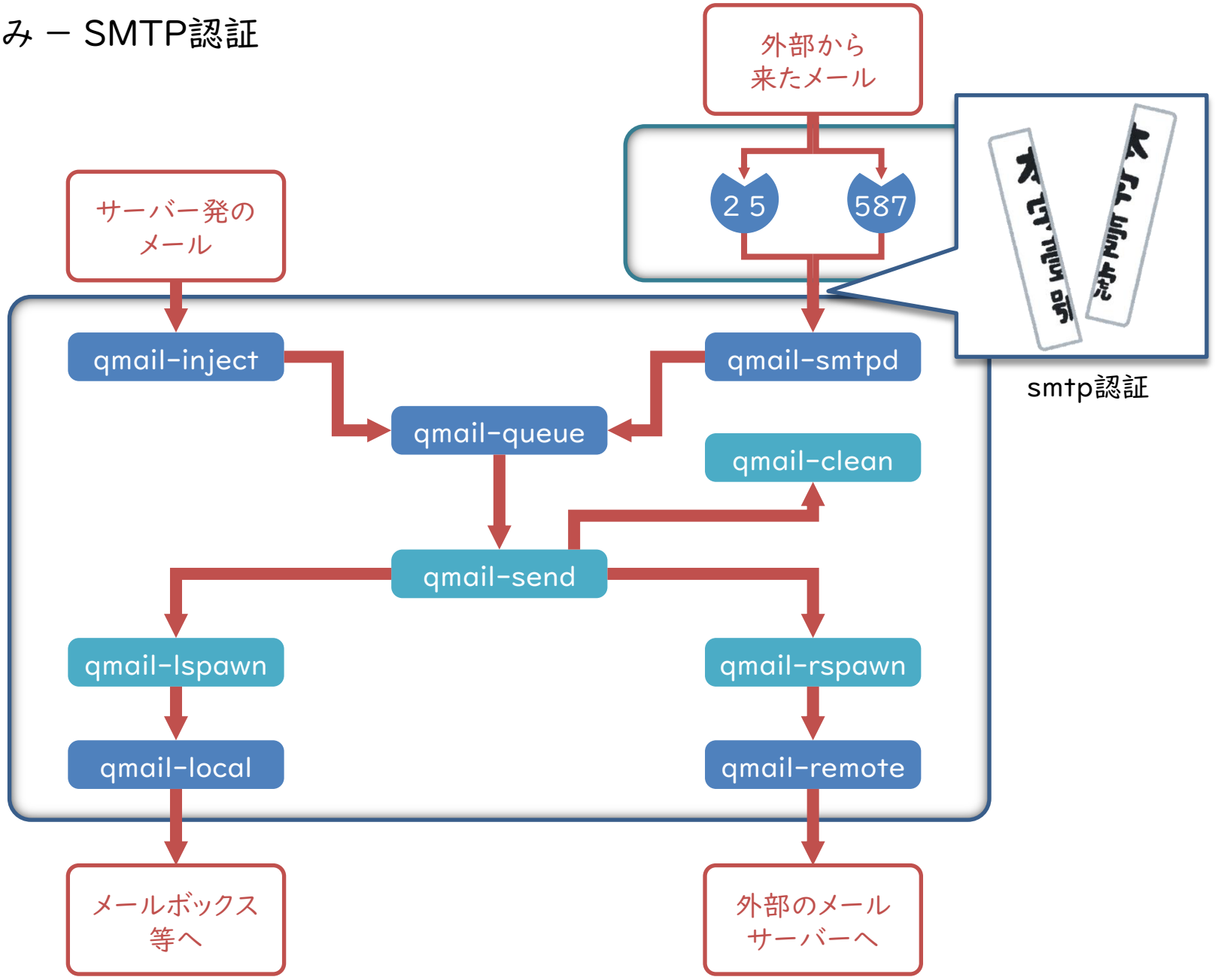
qmailのしくみ ー tcpserver



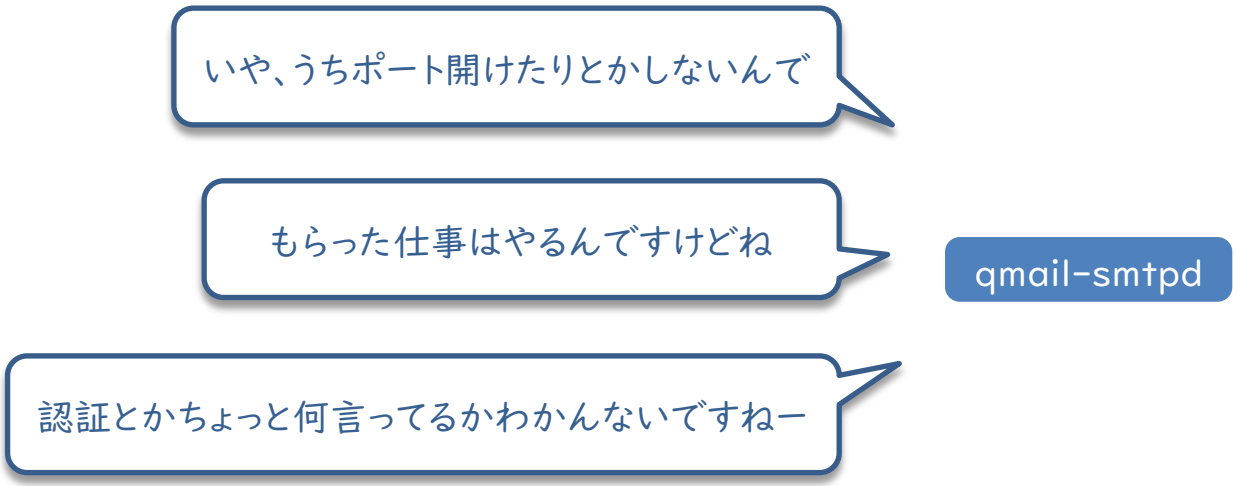
qmailのしくみ － tcpserver



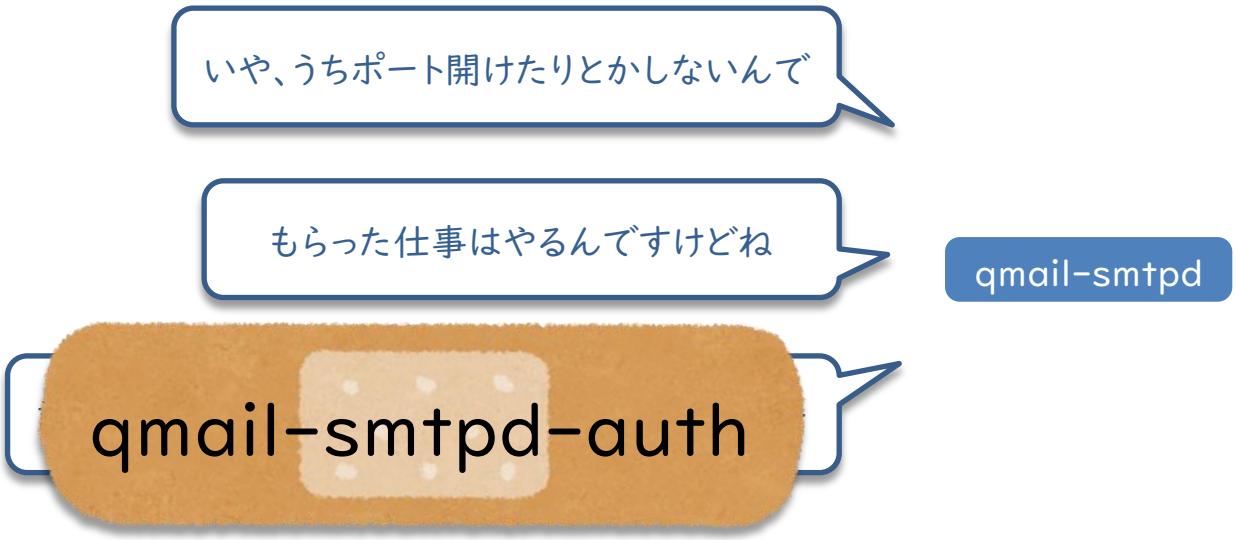
qmailのしくみ － SMTP認証



qmailのしくみ ー SMTP認証



qmailのしくみ － SMTP認証



qmailのしくみ － SMTP認証

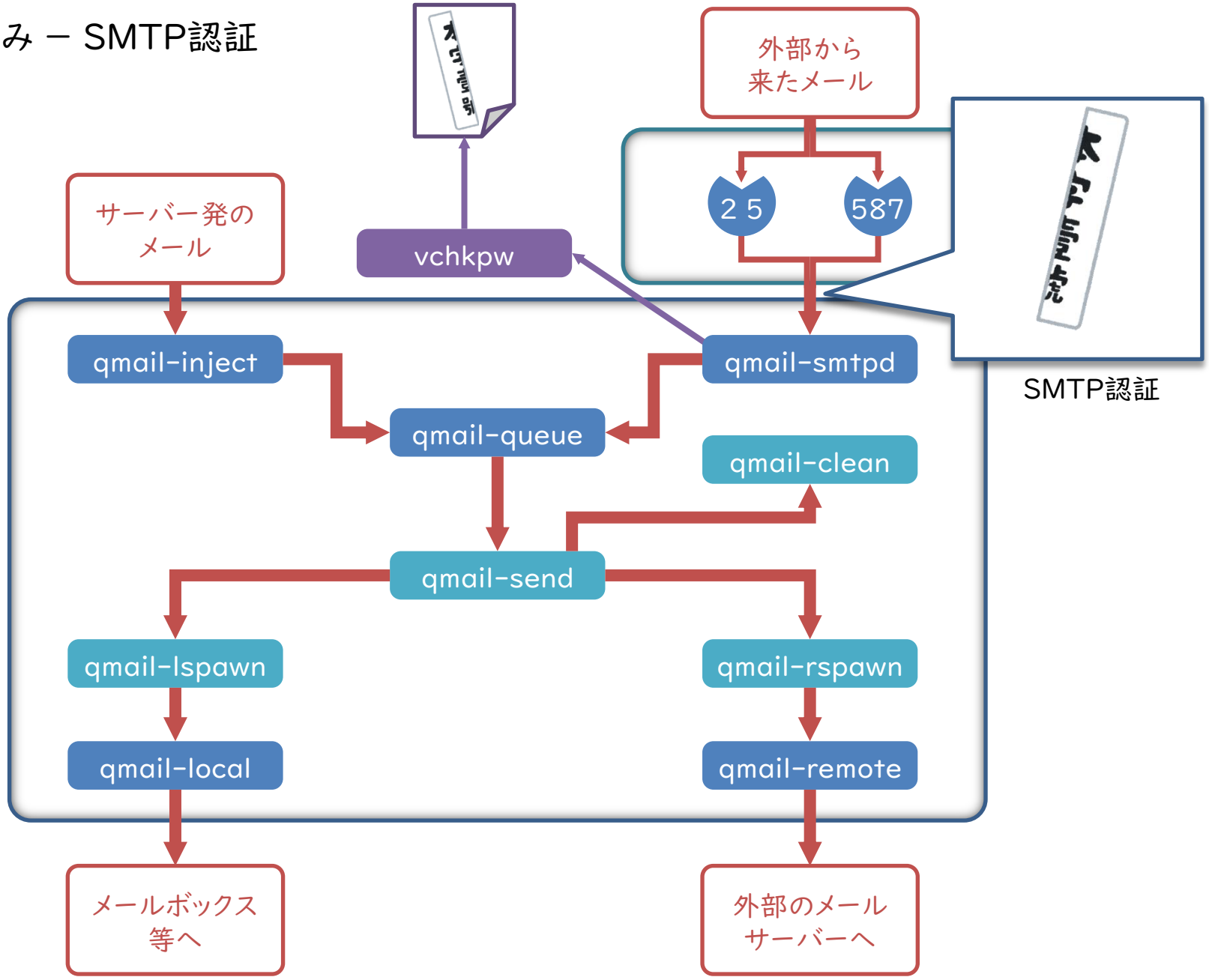
いや、うちポート開けたりとかしないんで

もらった仕事はやるんですけどね

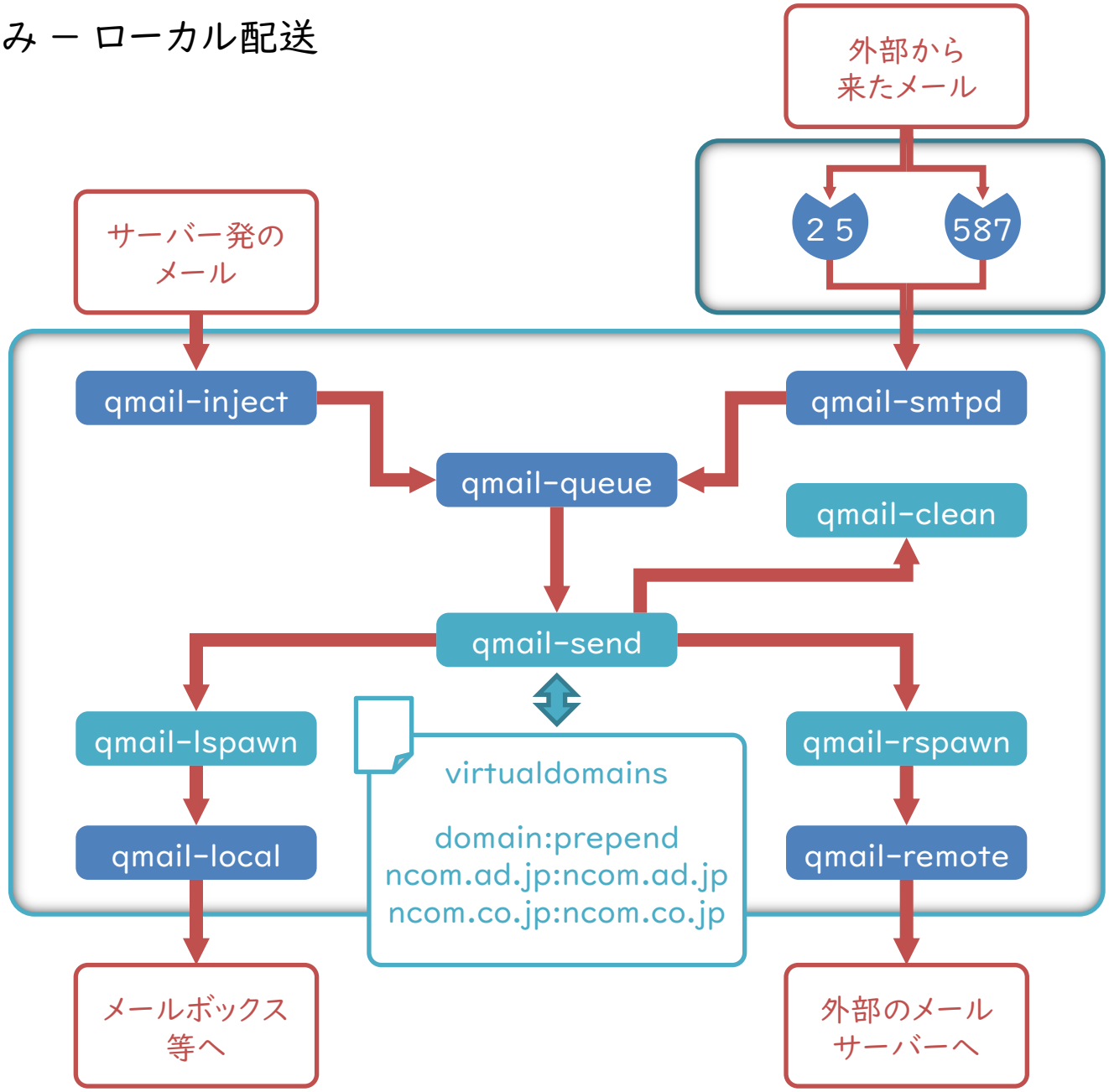
qmail-smtpd

あ、認証はできますんで認証に使う
プログラムとか指定してくださいねー

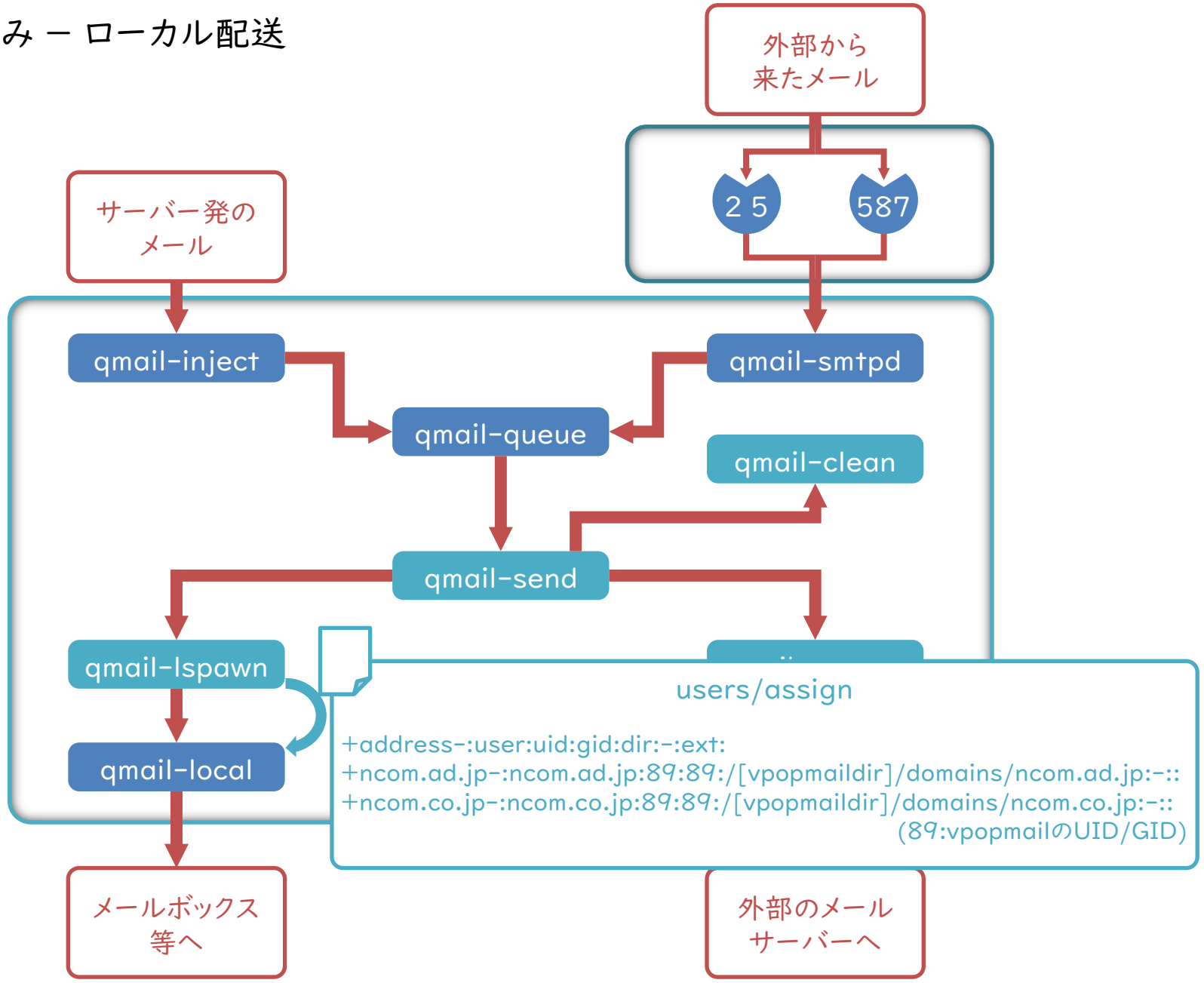
qmailのしくみ － SMTP認証



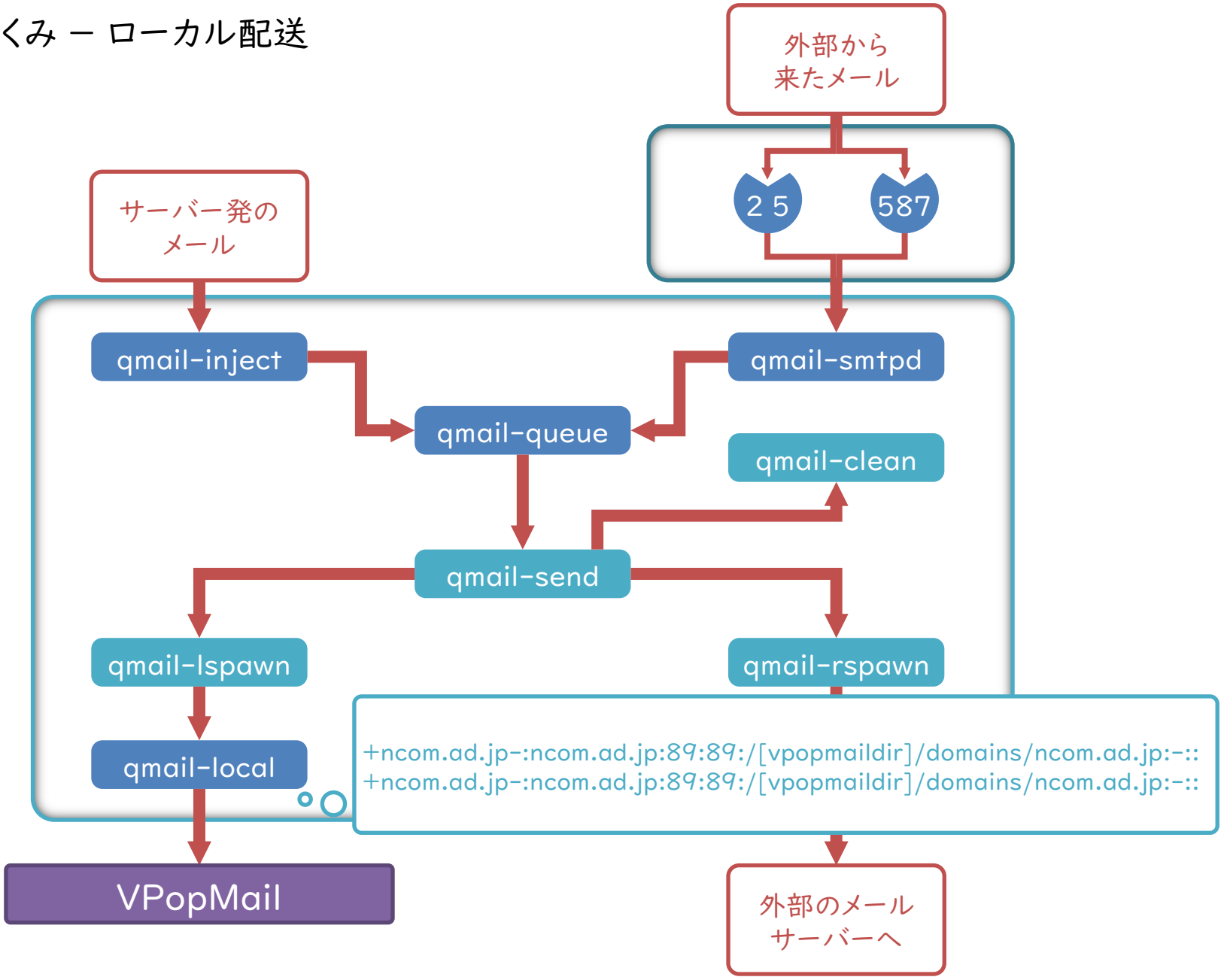
qmailのしくみ ー ローカル配送



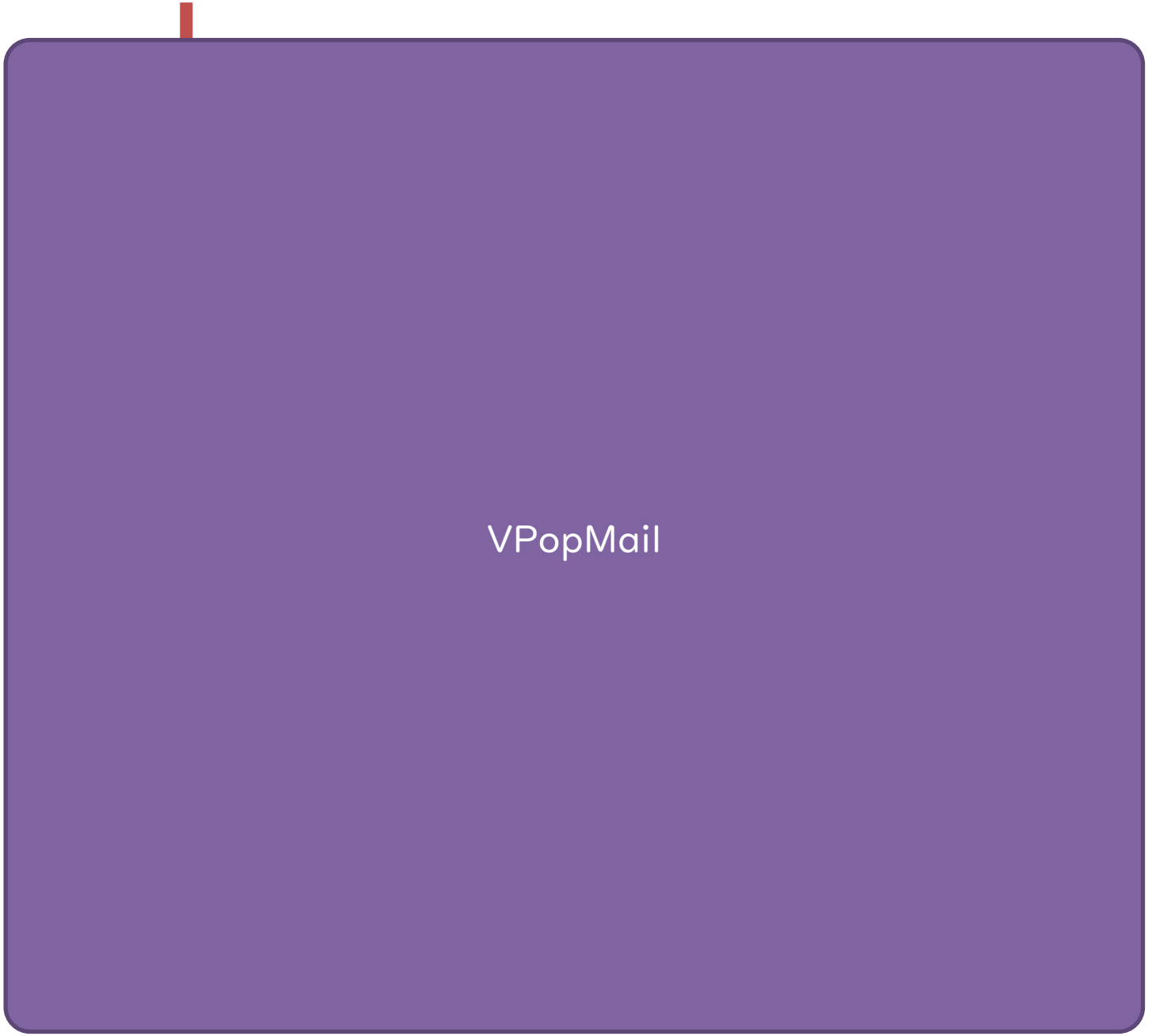
qmailのしくみ ー ローカル配送



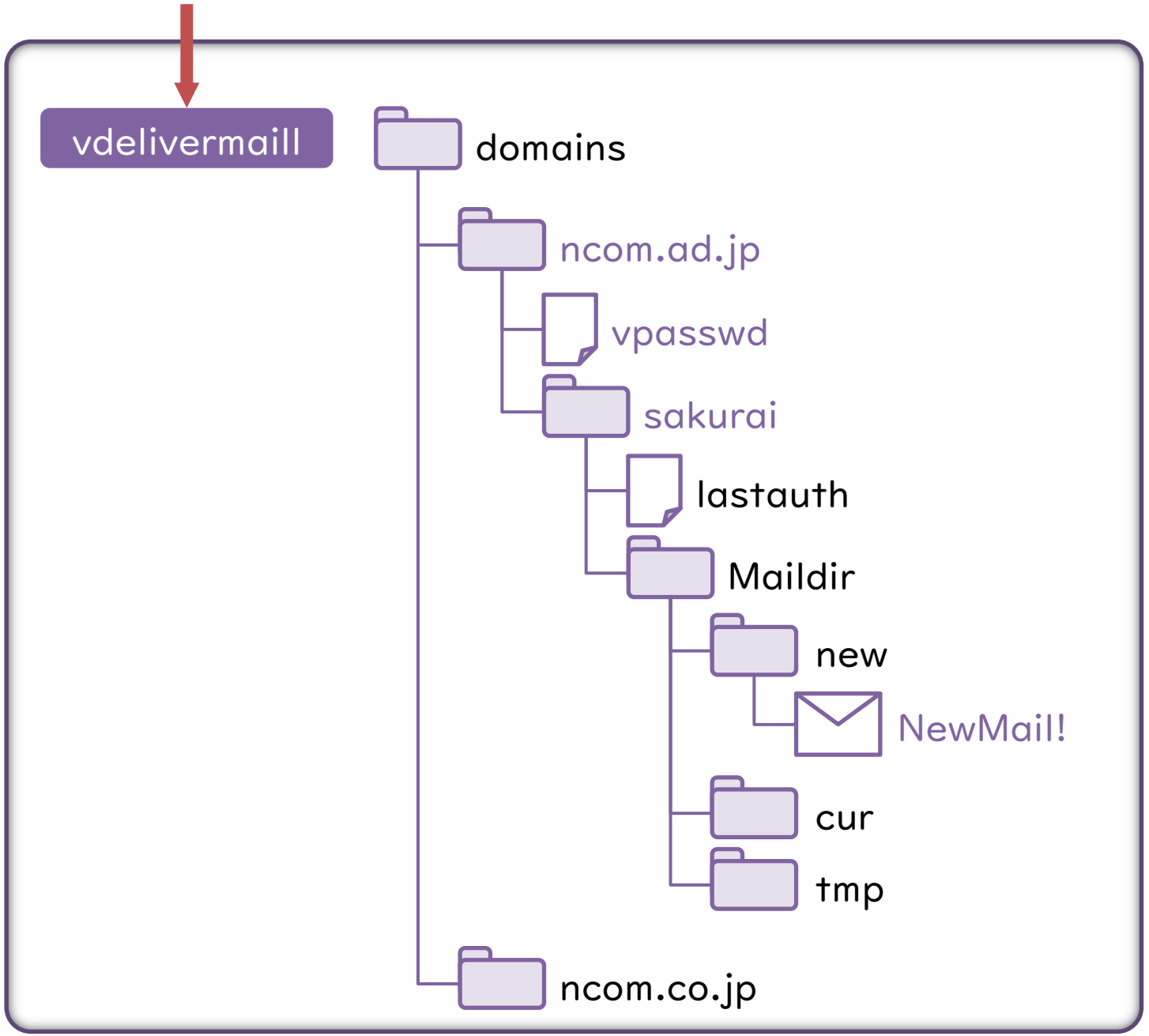
qmailのしくみ ー ローカル配送



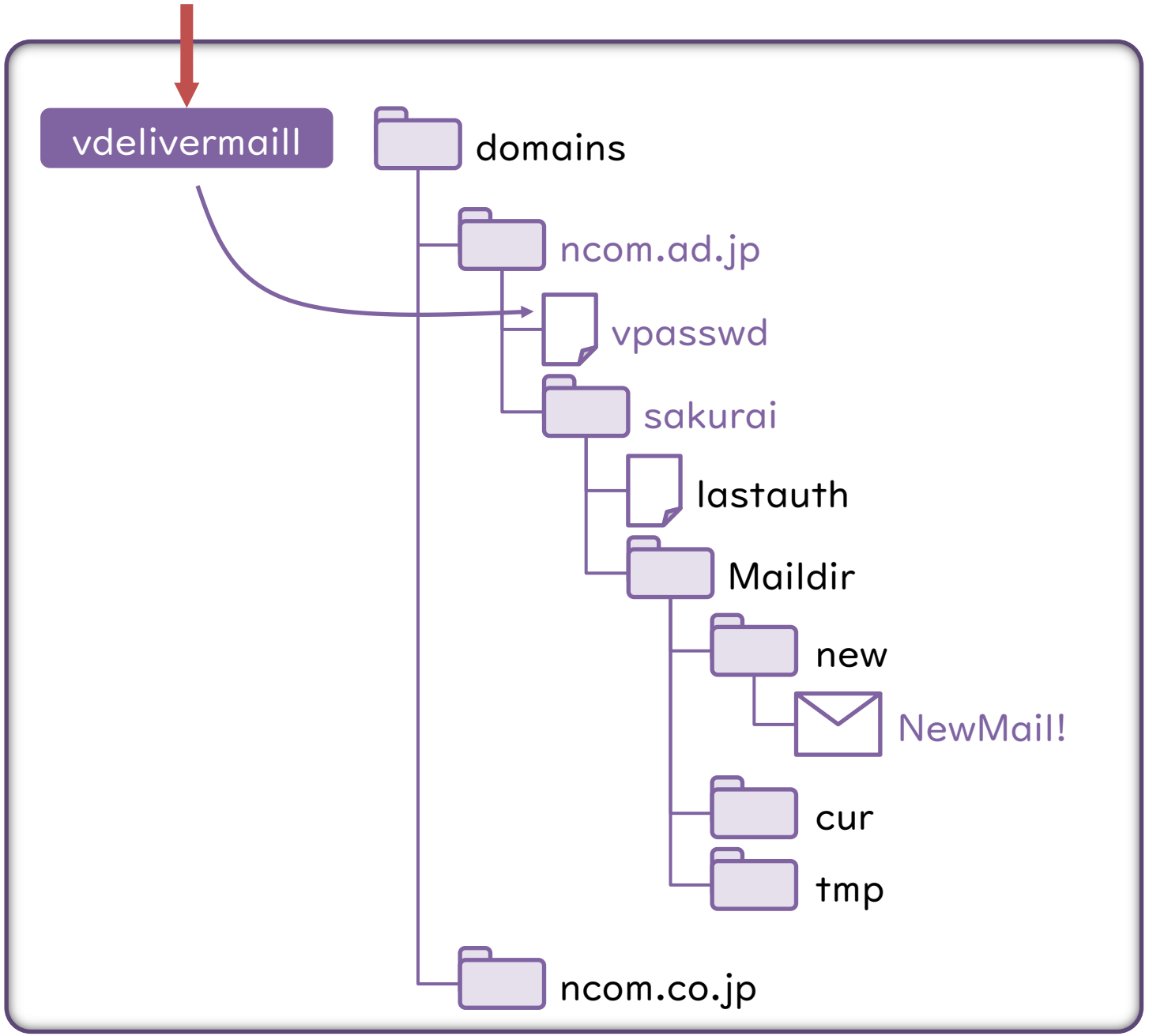
qmailのしくみ ー ローカル配送



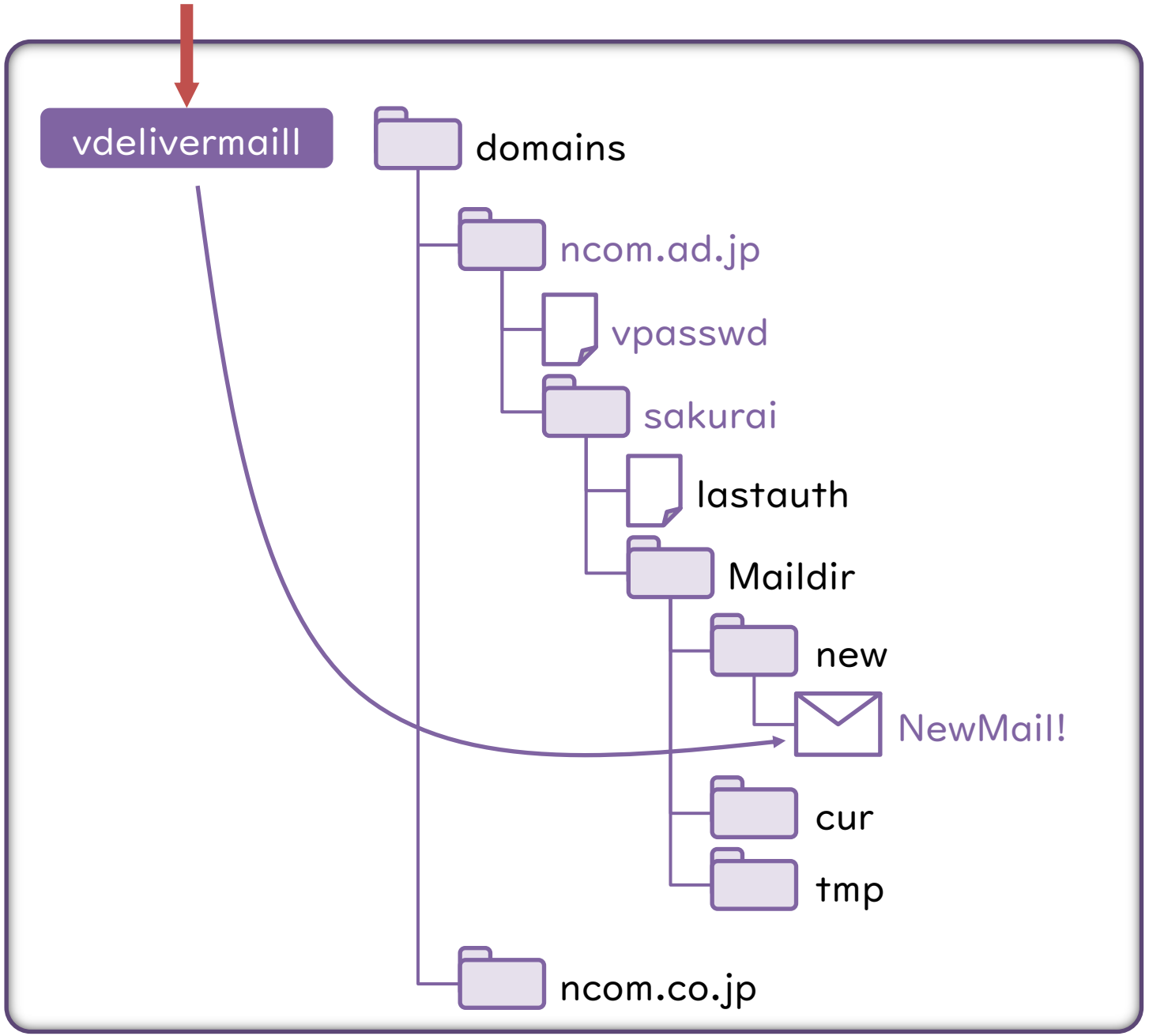
qmailのしくみ ー ローカル配送



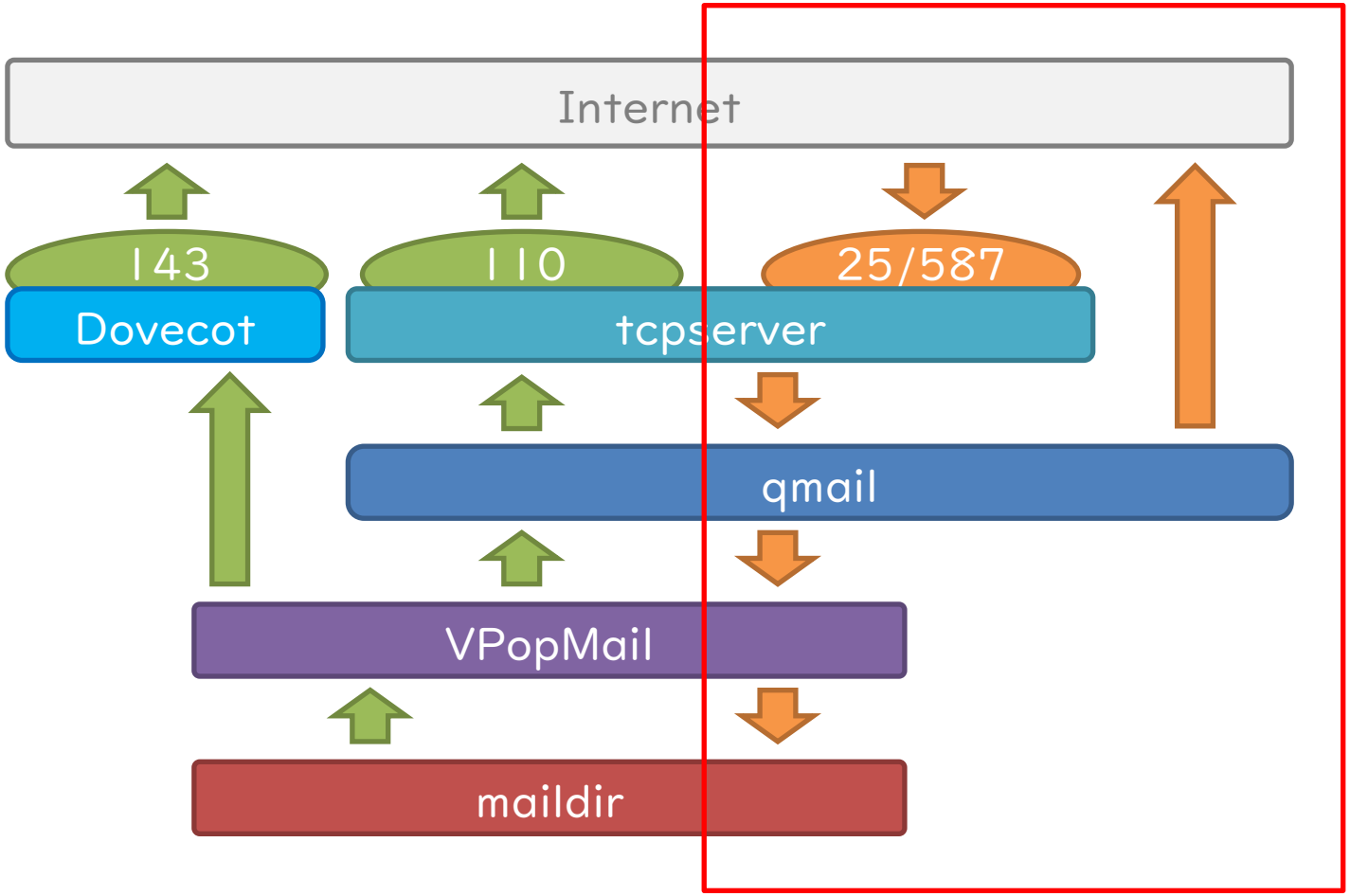
qmailのしくみ ー ローカル配送



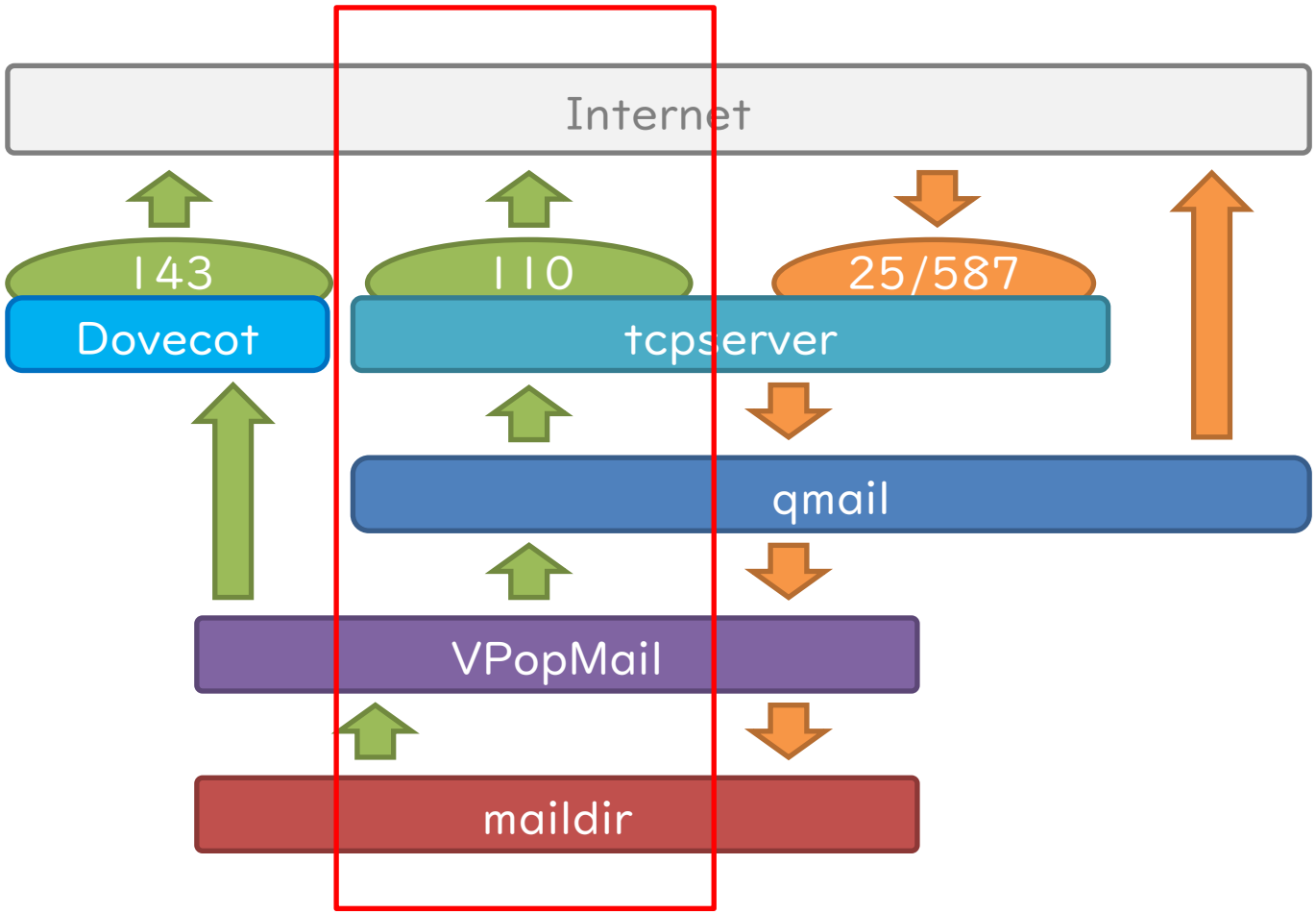
qmailのしくみ ー ローカル配送



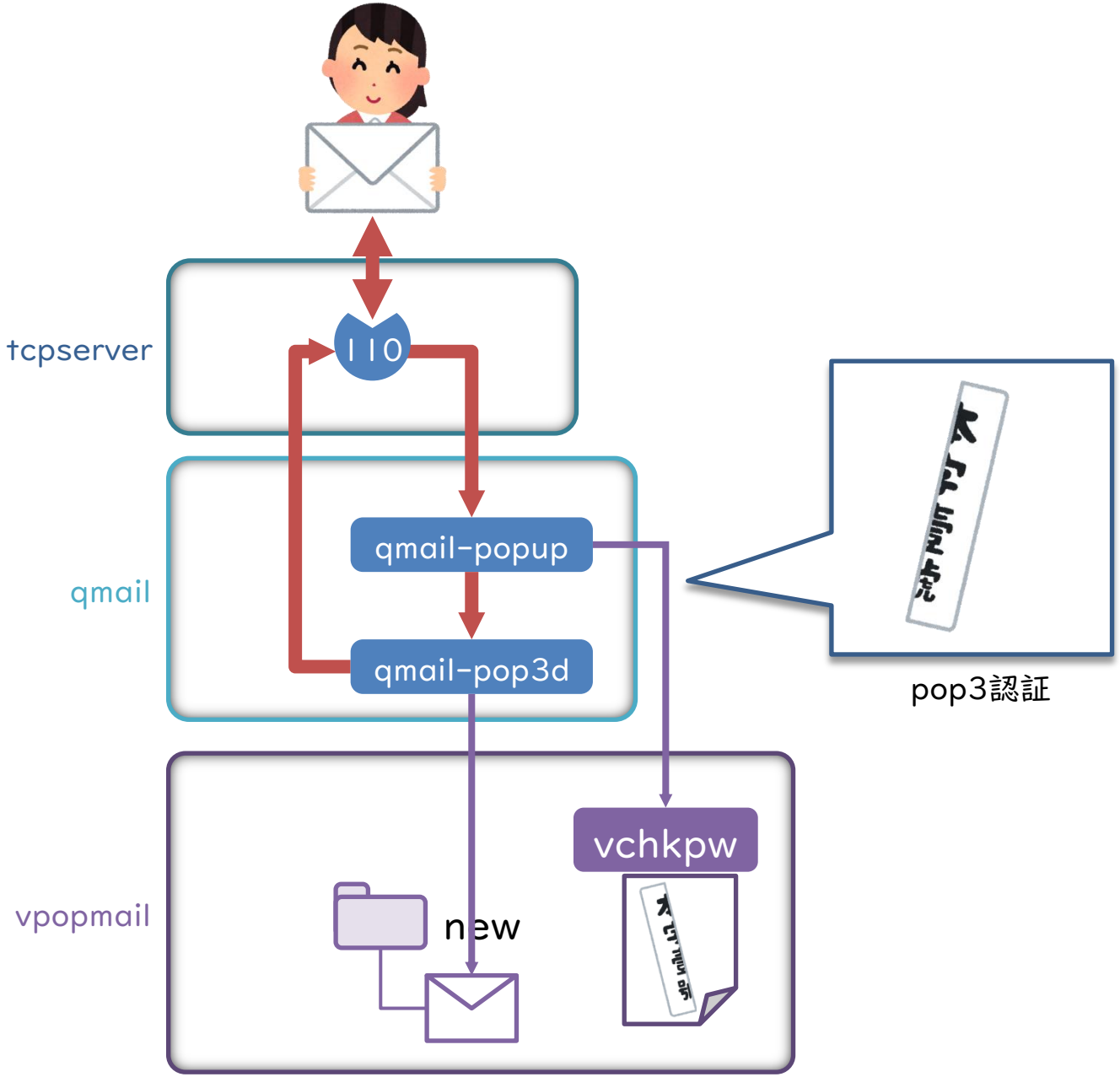
ここについてお話しました



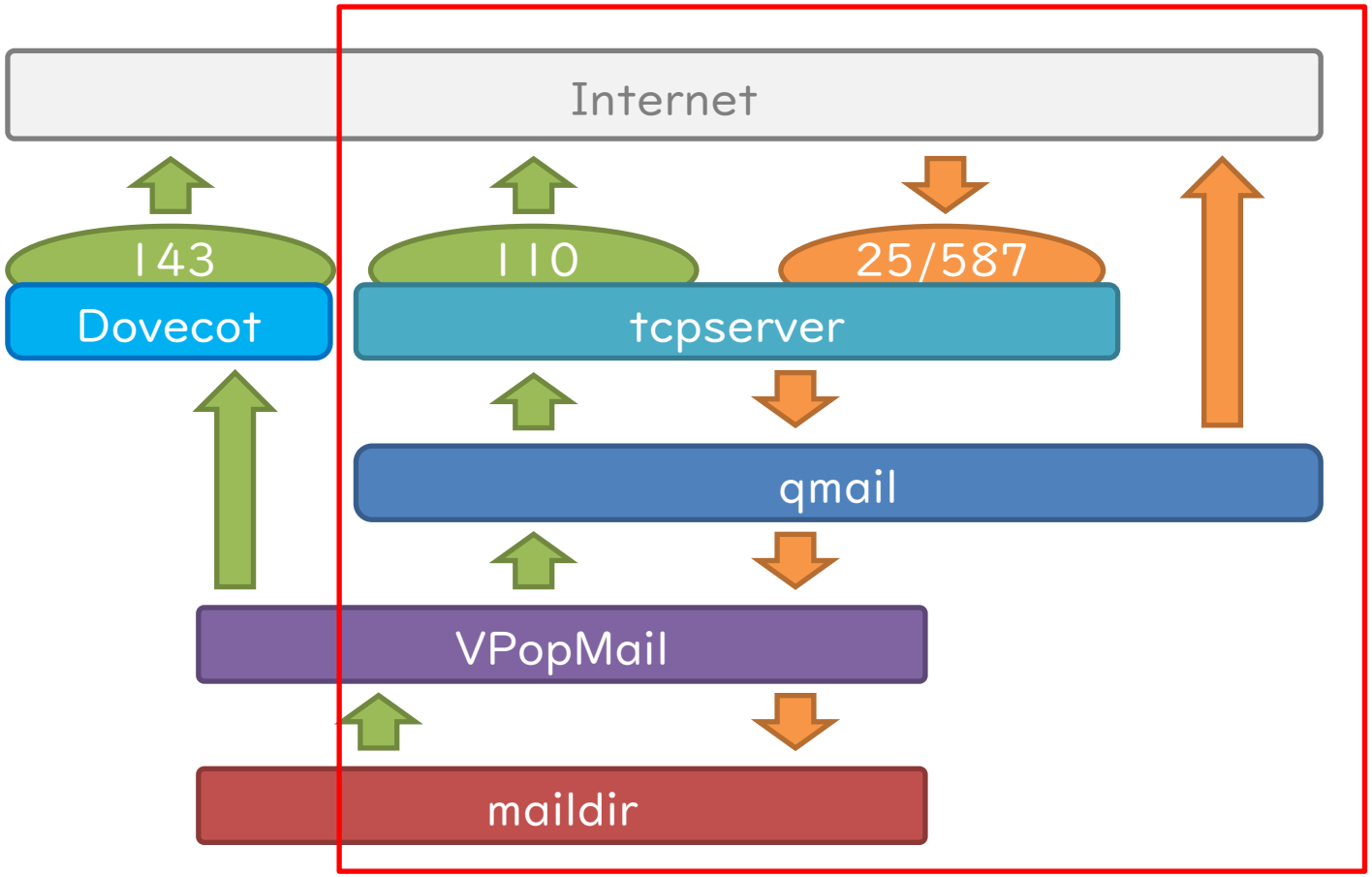
次にここ

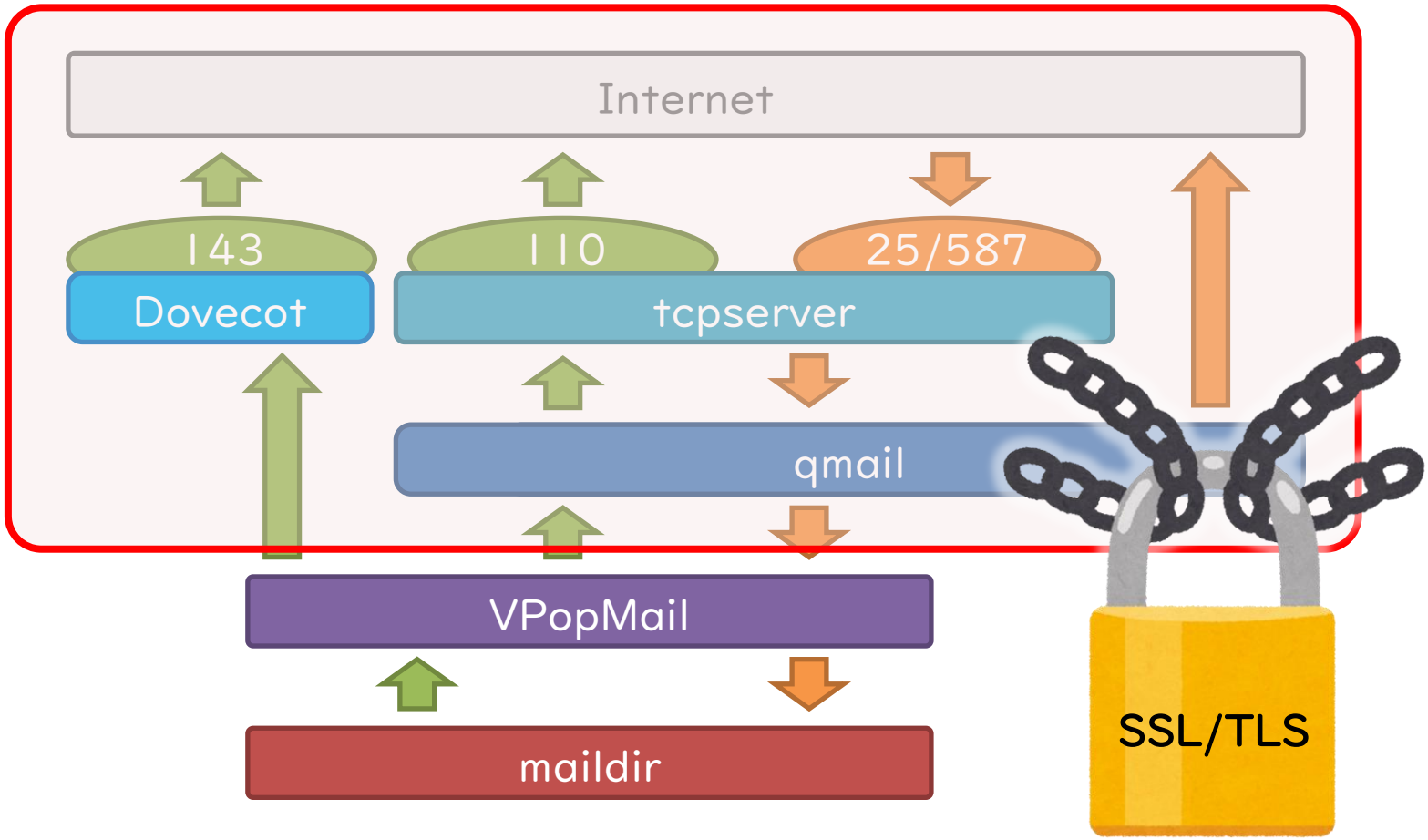

Internet
143
110
25/587
Dovecot
tcpserver
qmail
VPopMail
maildir

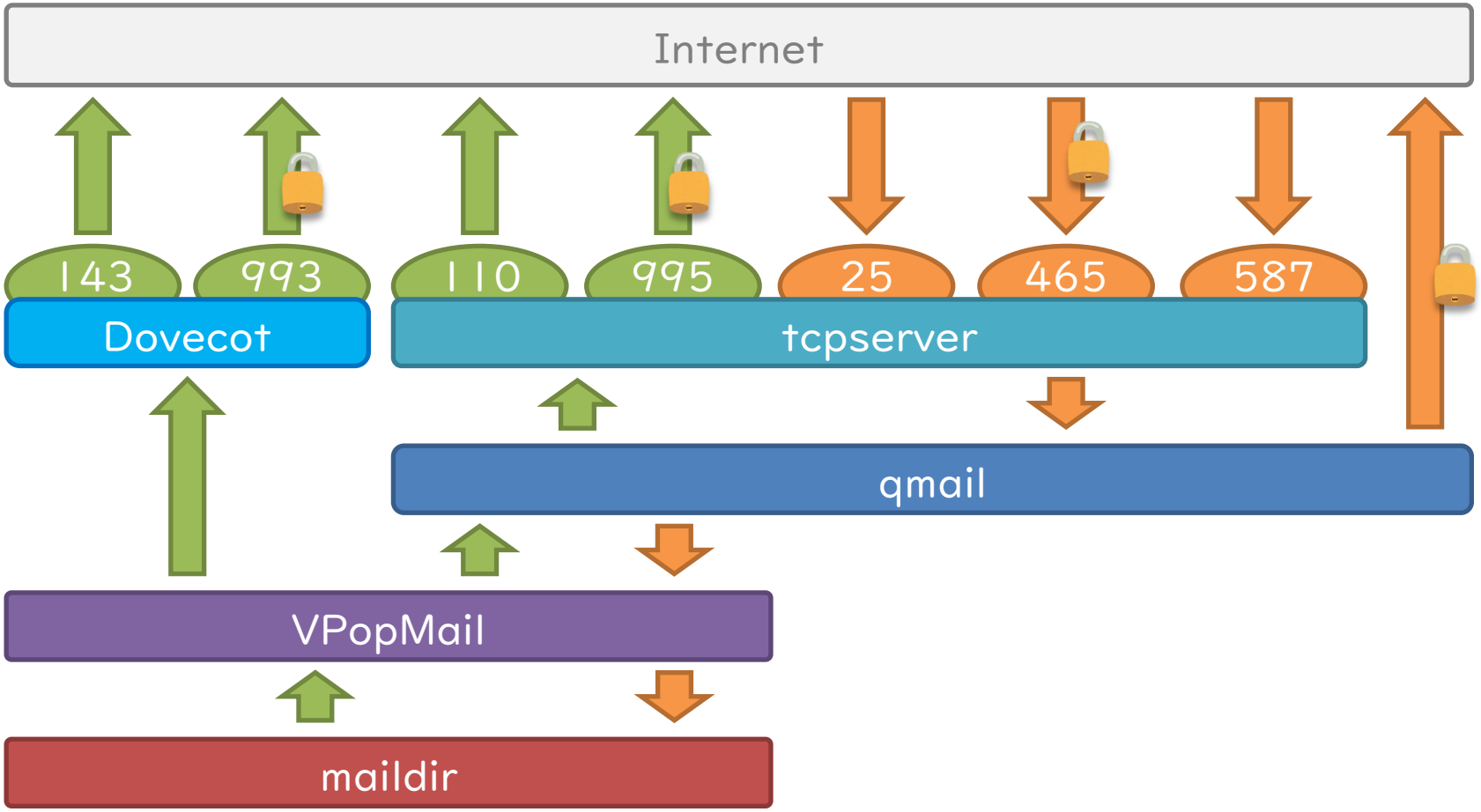
メールの受信プロセス

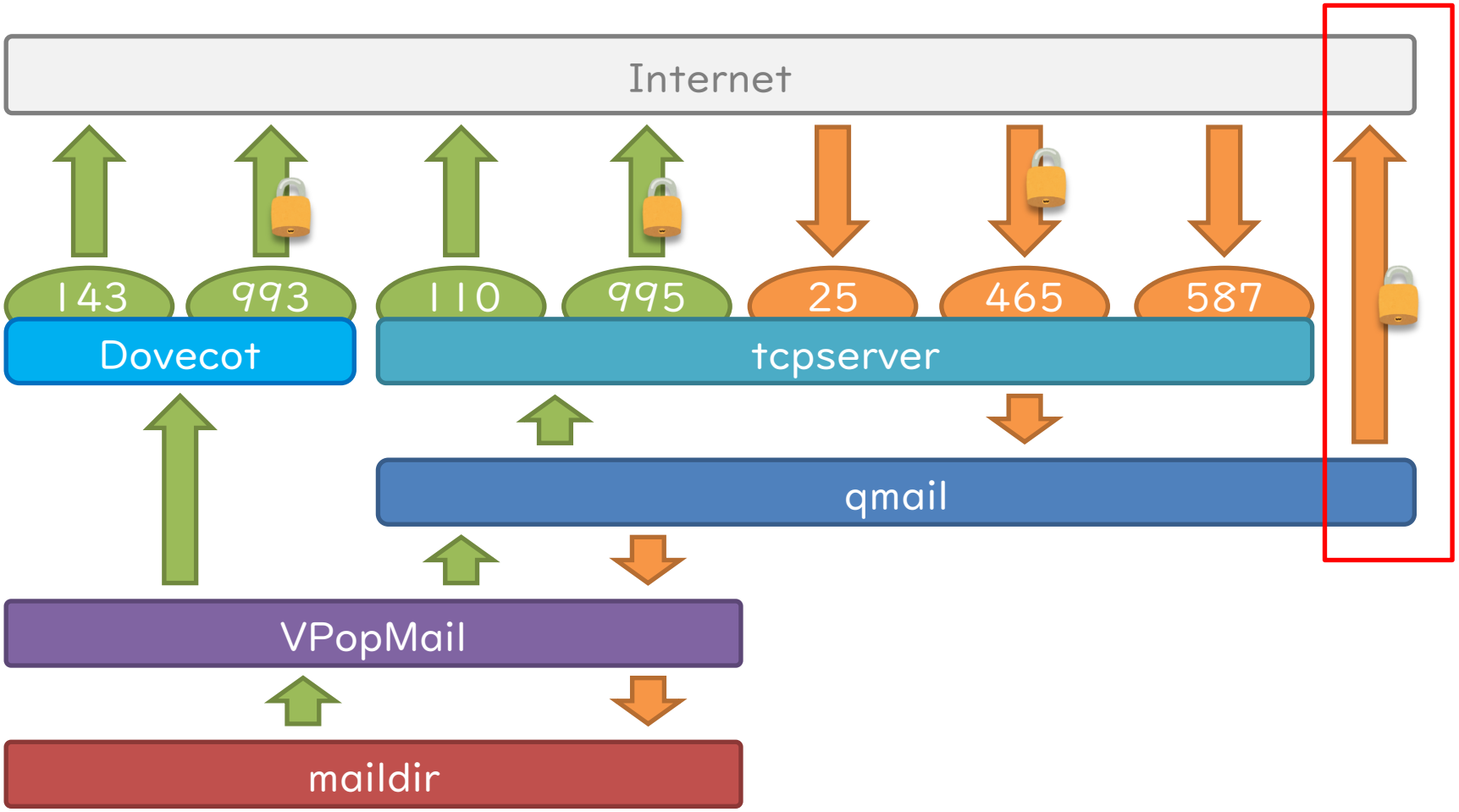

tcpserver
110
qmail
qmail-popup
qmail-pop3d
pop3認証
vpopmail
vchkpw
new

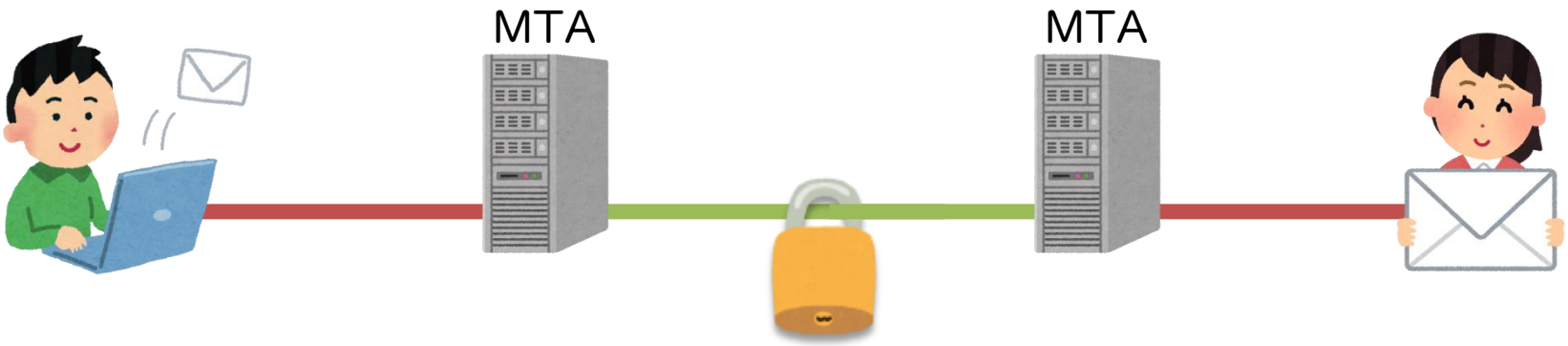
今ここ


Internet
143
110
25/587
Dovecot
tcpserver
qmail
VPopMail
maildir


Internet
143
110
25/587
Dovecot
tcpserver
qmail
VPopMail
maildir
SSL/TLS


Internet
143
993
110
995
25
465
587
Dovecot
tcpserver
qmail
VPopMail
maildir


Internet
143
993
110
995
25
465
587
Dovecot
tcpserver
qmail
VPopMail
maildir


MTA
MTA

qmailにおけるMTA間接続のSSL化

用意するもの

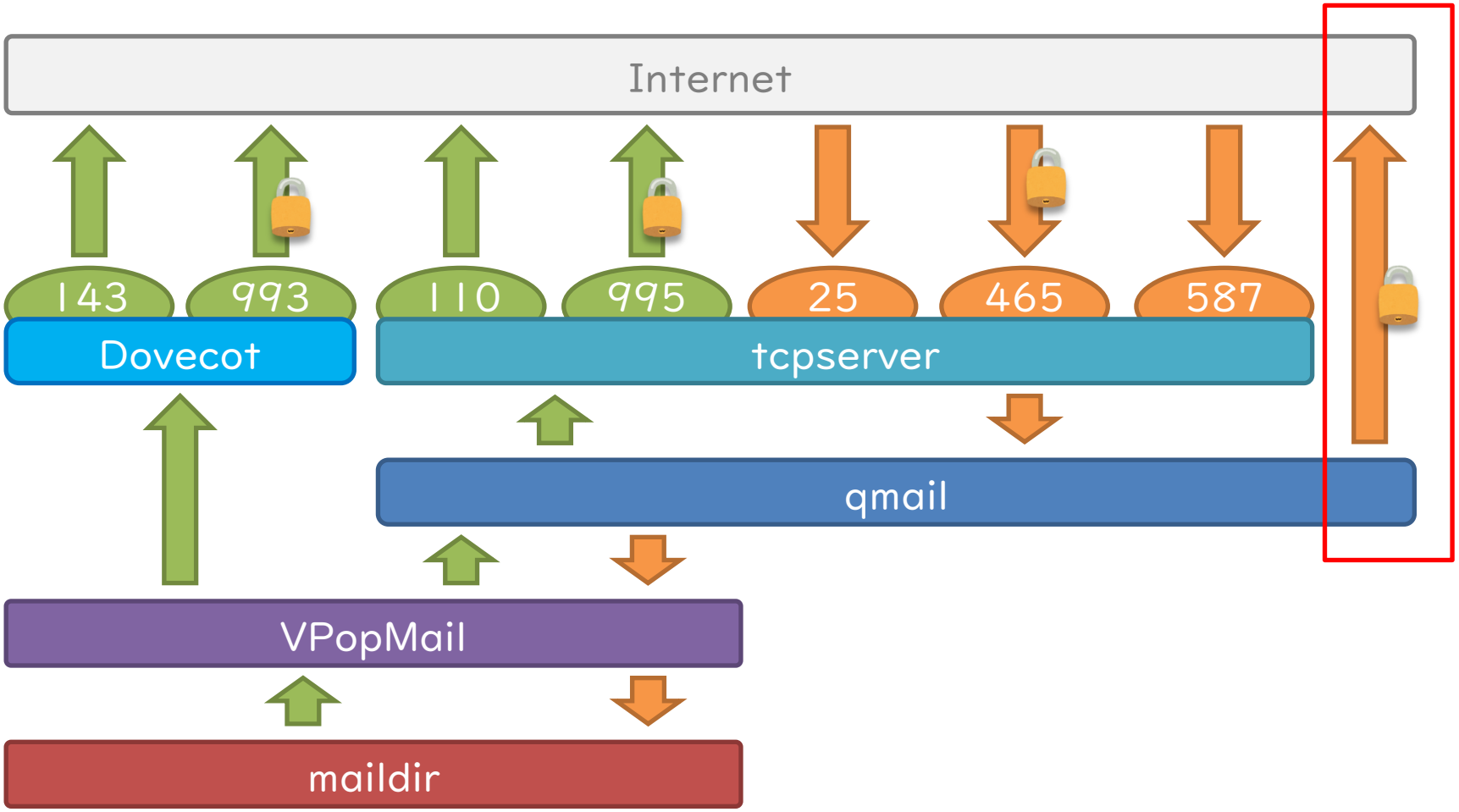
> SSLの一部のライブラリ(ssl.h)
> netqmail-1.06-tls-20160918.patch

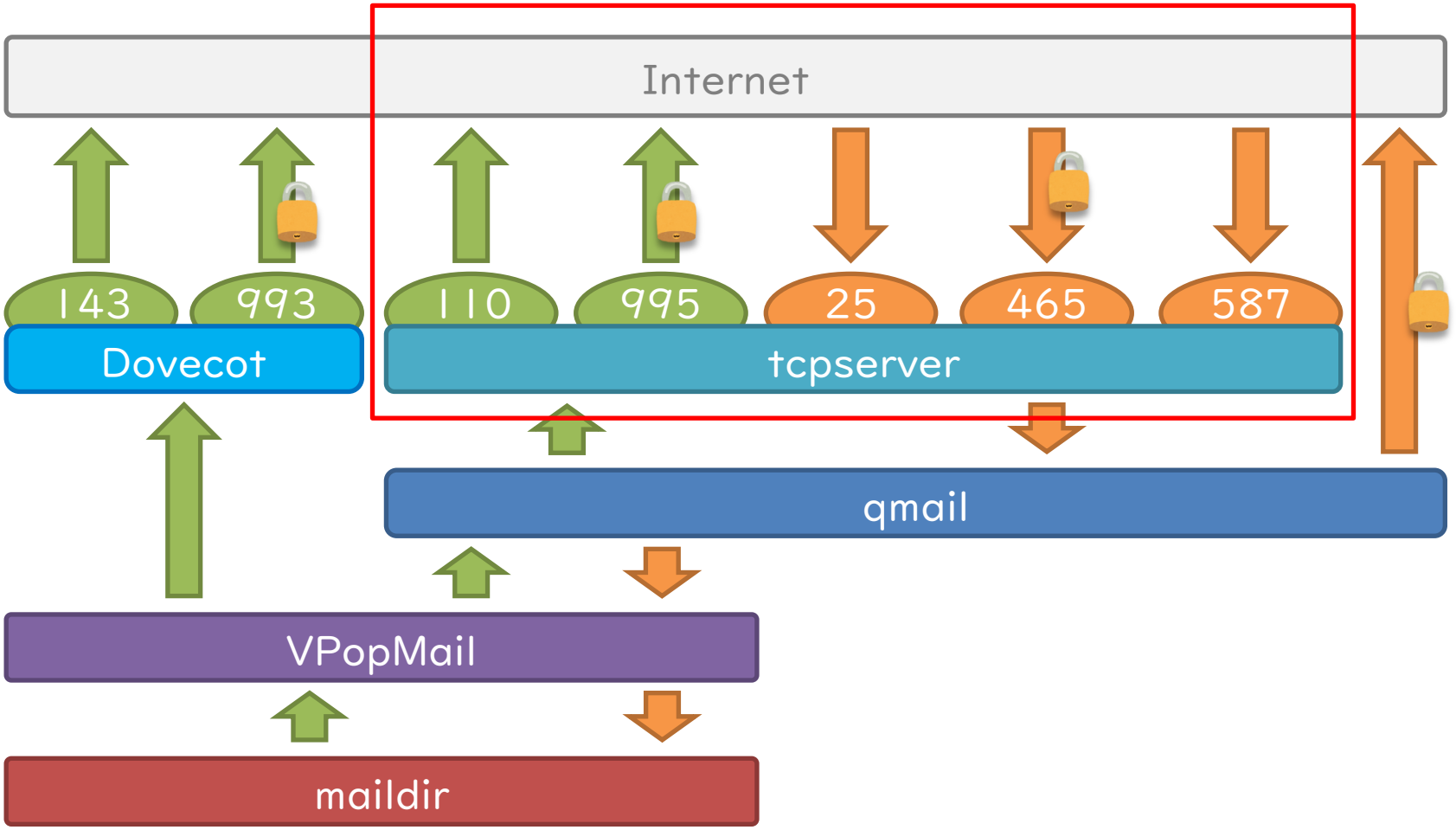
手順

1. libssl-dev(Debian/Ubuntu)やopenssl-devel(Redhat/CentOS)を入れてssl.hを使えるようにしておく
2. netqmail-1.06-tls-20160918.patchをnetqmailのソースディレクトリにダウンロード
3. patchを当て、一旦qmailを停止して再コンパイル&インストール
4. qmailを再度起動

結果

From: [redacted]
To: [redacted]
日付: 2018年5月17日 11:32
件名: [redacted]
セキュリティ: 標準的な暗号化(TLS) 詳細


Internet
143
993
110
995
25
465
587
Dovecot
tcpserver
qmail
VPopMail
maildir


Internet
143
993
110
995
25
465
587
Dovecot
tcpserver
qmail
VPopMail
maildir

SMTP(25)
↓
SMTP over SSL(465)

POP3(110)
↓
POP3 over SSL(995)

IMAP(143)
↓
IMAP over SSL(993)

tcpserverのSSL対応

用意するもの

> SSLサーバー証明書
> tcpserver SSL/TLS patch

手順

1. 適当なディレクトリにSSLサーバー証明書を保存
2. tcpserverのソースディレクトリにtcpserver SSL/TLS patch を
   ダウンロード
3. patchを当て、コンパイルし直す
4. 作成されたバイナリファイル「tcpserver」はssl接続のみに対応
   インストールで置き換えてしまうと非SSL接続での送受信ができなくなるので
   既存の「tcpserver」と並行して利用するため、「tcpserver」と同じディレクトリに
   「tcpserver-ssl」として保存
5. 起動スクリプトの変更
6. qmailを再起動

起動スクリプトの変更

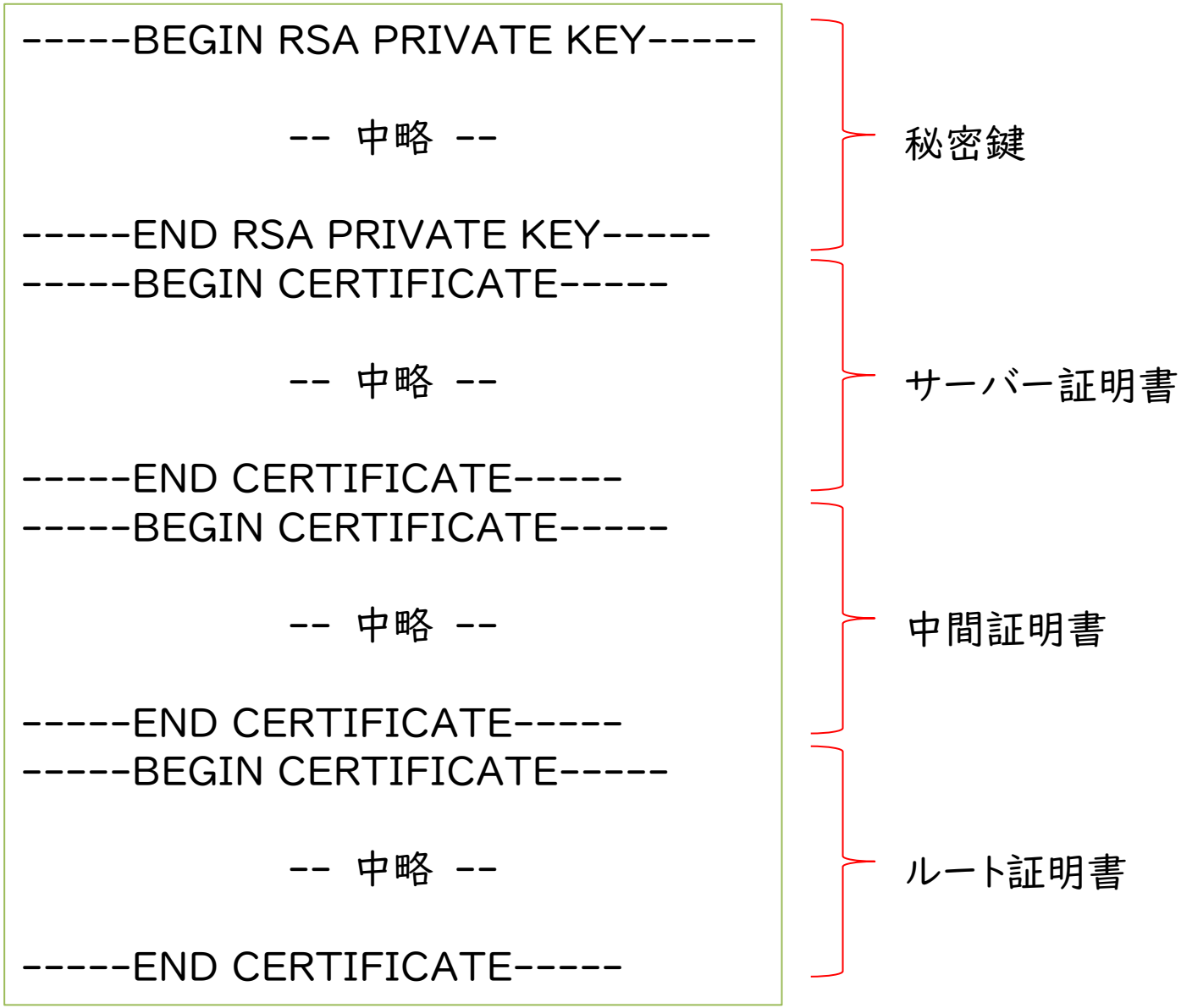
```
# SMTP
    tcpserver -qv -l0 -HR -u `id -u vpopmail` -g `id -g vpopmail` ¥
    -x /home/vpopmail/etc/tcp.smtp.cdb 0 smtp ¥
    qmail-smtpd `hostname` /home/vpopmail/bin/vchkpw /bin/true 2>&1 |¥
    splogger smtp &

# SUBMISSION
    tcpserver -qv -l0 -HR -u `id -u vpopmail` -g `id -g vpopmail` ¥
    -x /home/vpopmail/etc/tcp.smtp.cdb 0 submission ¥
    qmail-smtpd `hostname` /home/vpopmail/bin/vchkpw /bin/true 2>&1 |¥
    splogger submission &

# POP3
    tcpserver -qvRH -u `id -u vpopmail` -g `id -g vpopmail` ¥
    0 pop3 qmail-popup `hostname` /home/vpopmail/bin/vchkpw ¥
    qmail-pop3d Maildir 2>&1 | ¥
    splogger pop3 &
```

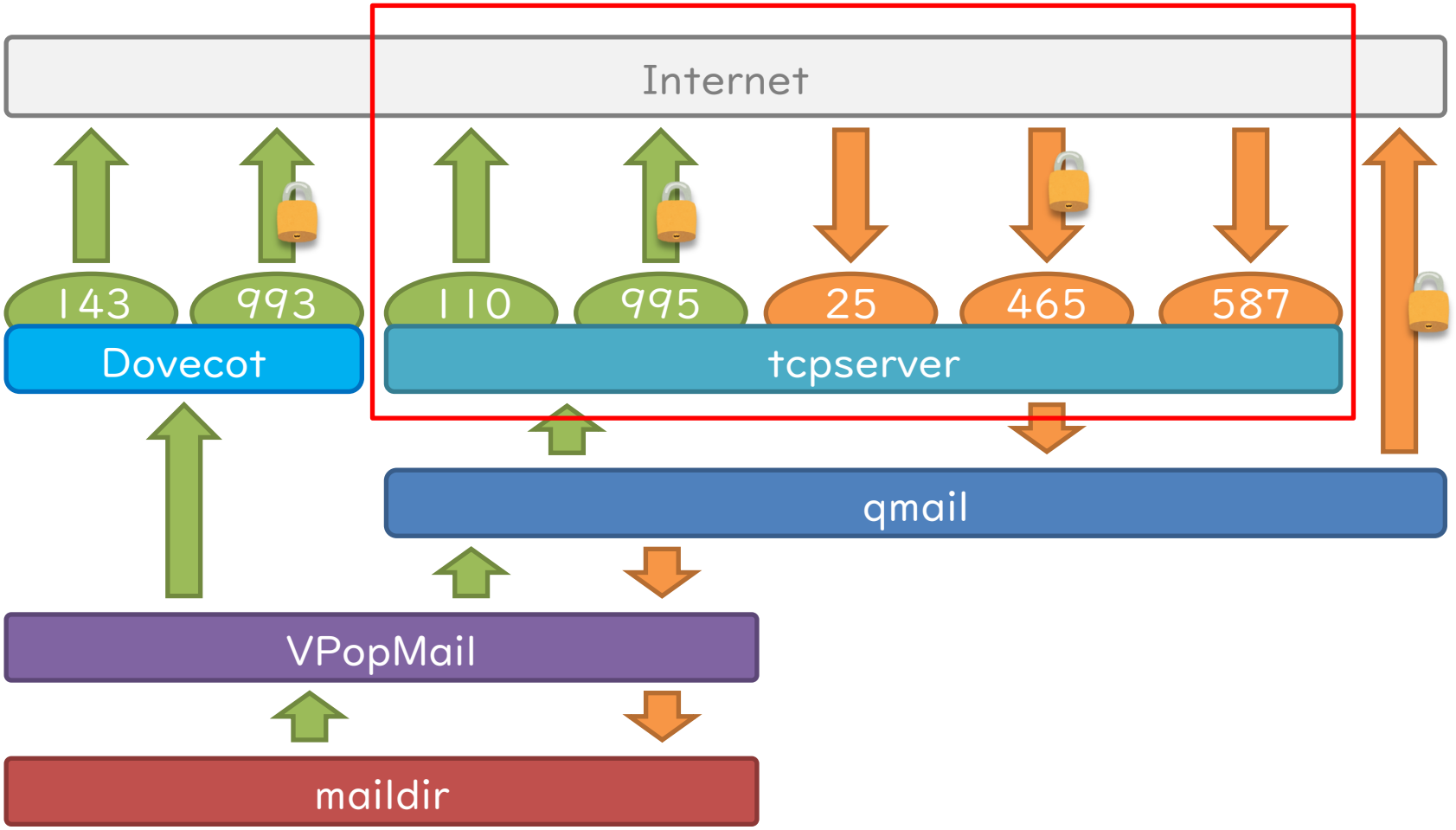
起動スクリプトの変更

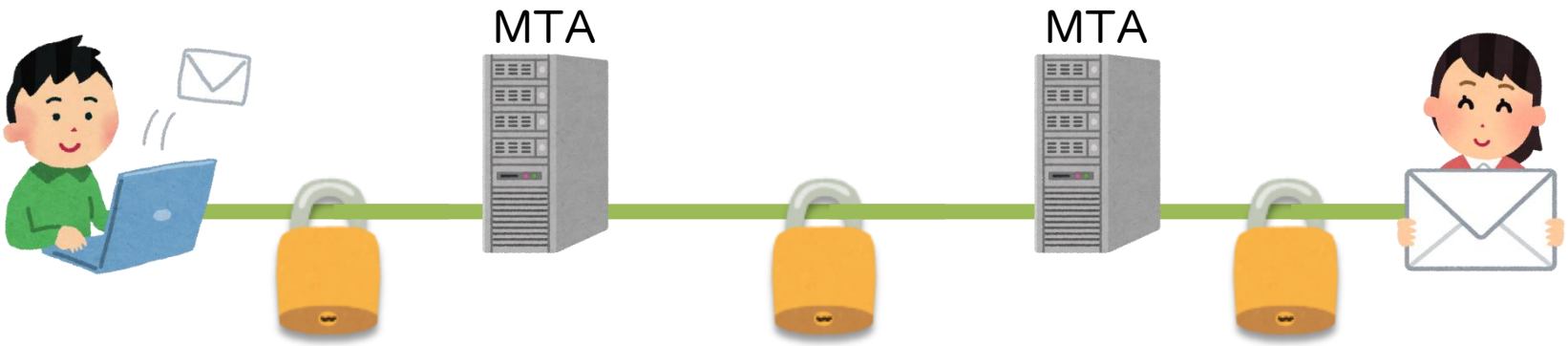
```
# SMTPS
    tcpserver-ssl -qv -l0 -sHR -u `id -u vpopmail` -g `id -g vpopmail` ¥
    -s -n /etc/ssl/private/qmail.pem ¥
    -x /home/vpopmail/etc/tcp.smtp.cdb 0 465 ¥
    qmail-smtpd `hostname` /home/vpopmail/bin/vchkpw /bin/true 2>&1 |¥
    splogger smtps &


 #POP3S
    tcpserver-ssl -qvsRH -u `id -u vpopmail` -g `id -g vpopmail` ¥
    -s -n /etc/ssl/private/qmail.pem ¥
    0 995 qmail-popup `hostname` /home/vpopmail/bin/vchkpw ¥
    qmail-pop3d Maildir 2>&1 |¥
    splogger pop3s &
```

SSLサーバー証明書

qmail.pem




Internet
143
993
110
995
25
465
587
Dovecot
tcpserver
qmail
VPopMail
maildir



SMTP(25)
↓
SMTP over SSL(465)

POP3(110)
↓
POP3 over SSL(995)

IMAP(143)
↓
IMAP over SSL(993)

Mozilla Thunderbird

まとめ

MTA間のSSL通信の必要増
qmailの対応は簡単

MTA-MUA間のSSL化もね

課題
S/MIMEで緑にしたい

おまけ

道①
tcpserverのSSL対応
＋
qmailのSSL対応

道②
Postfixにしてみる

②Postfixにしてみる

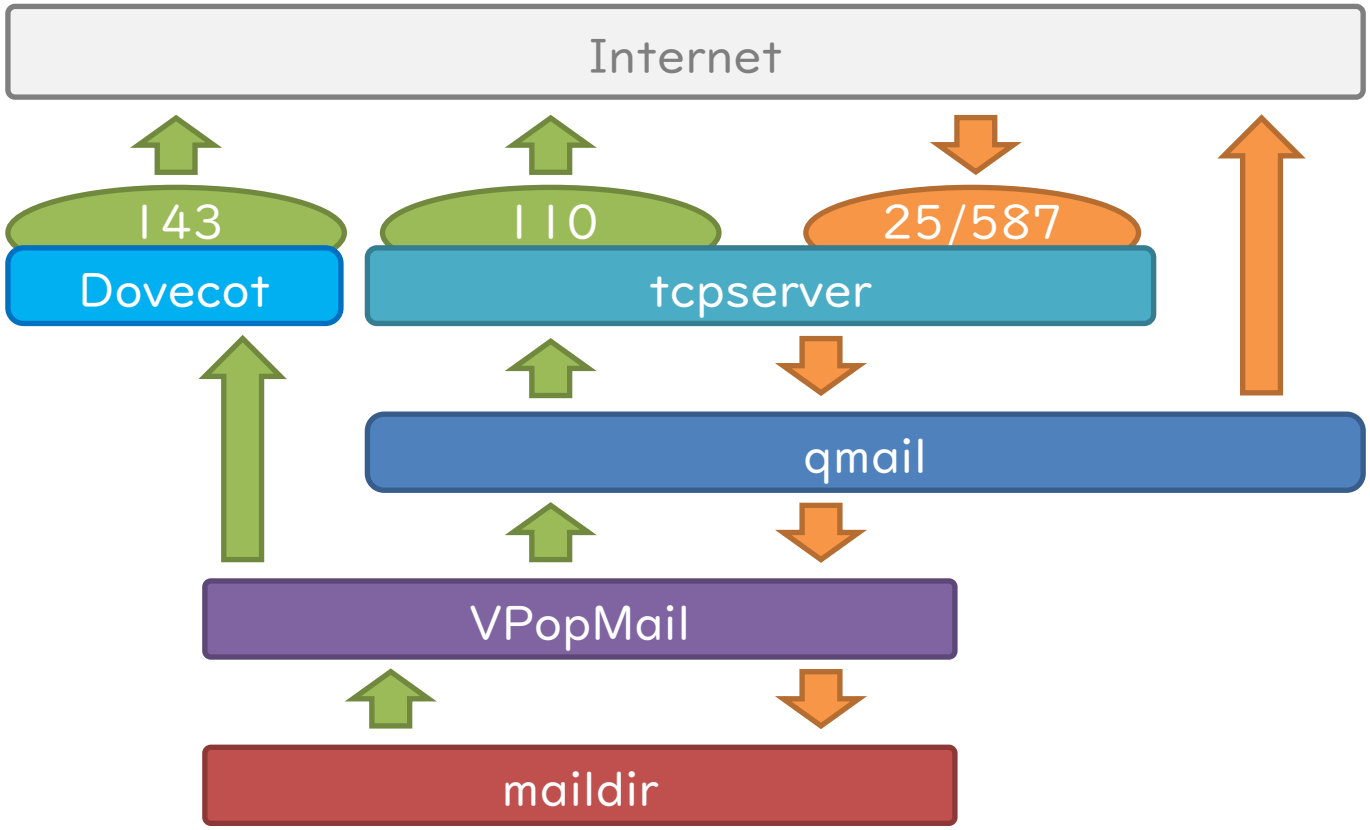
概要

・MTAをまるっとPostfixに替える
・MTA間送信にSSLを利用するための設定が容易

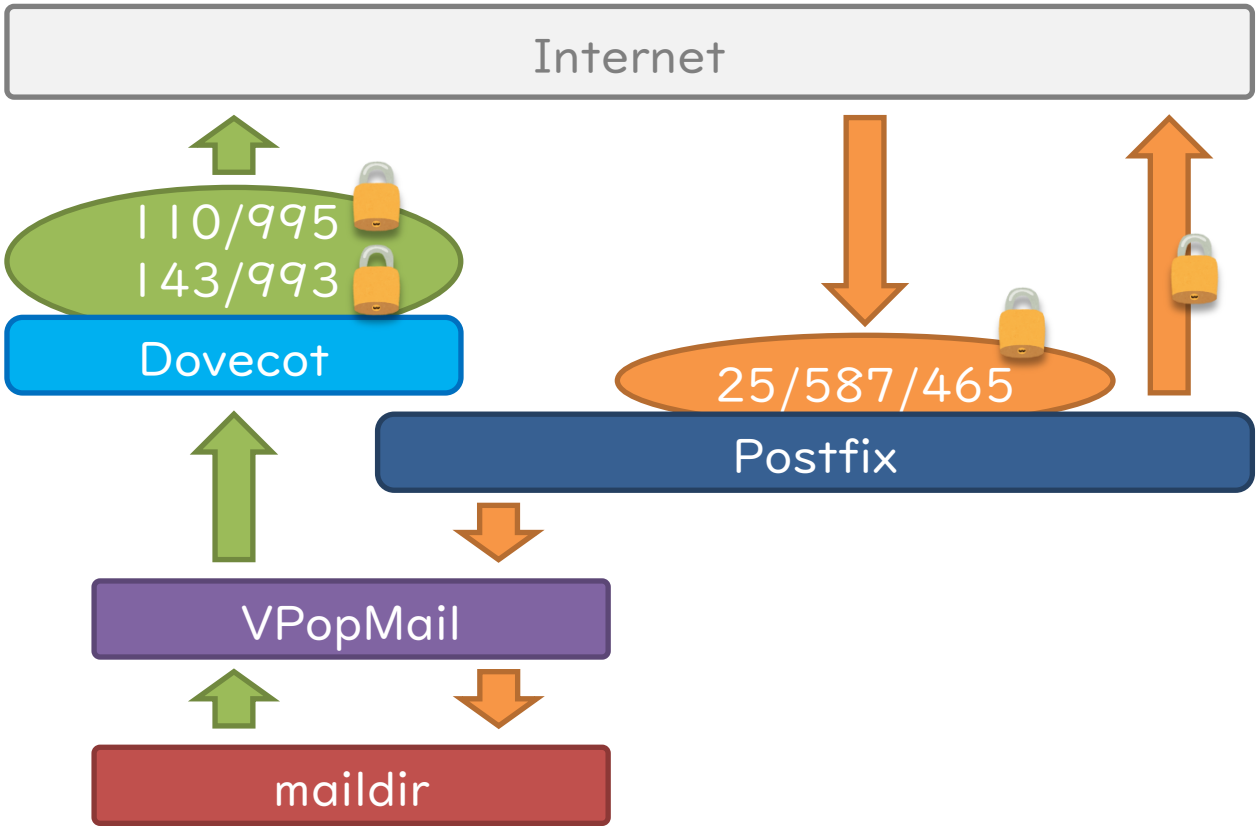
・サーバーへの変更大
・ぶっちゃけPostfixは使いたくない
・バーチャルサーバーでのユーザー管理に不慣れ
・Postfix admin + Mailman があんまり好きじゃない

・じゃあユーザー管理は VPopMail + QmailAdmin +ezmlm のままで
送受信だけPostfixにすればいいじゃん

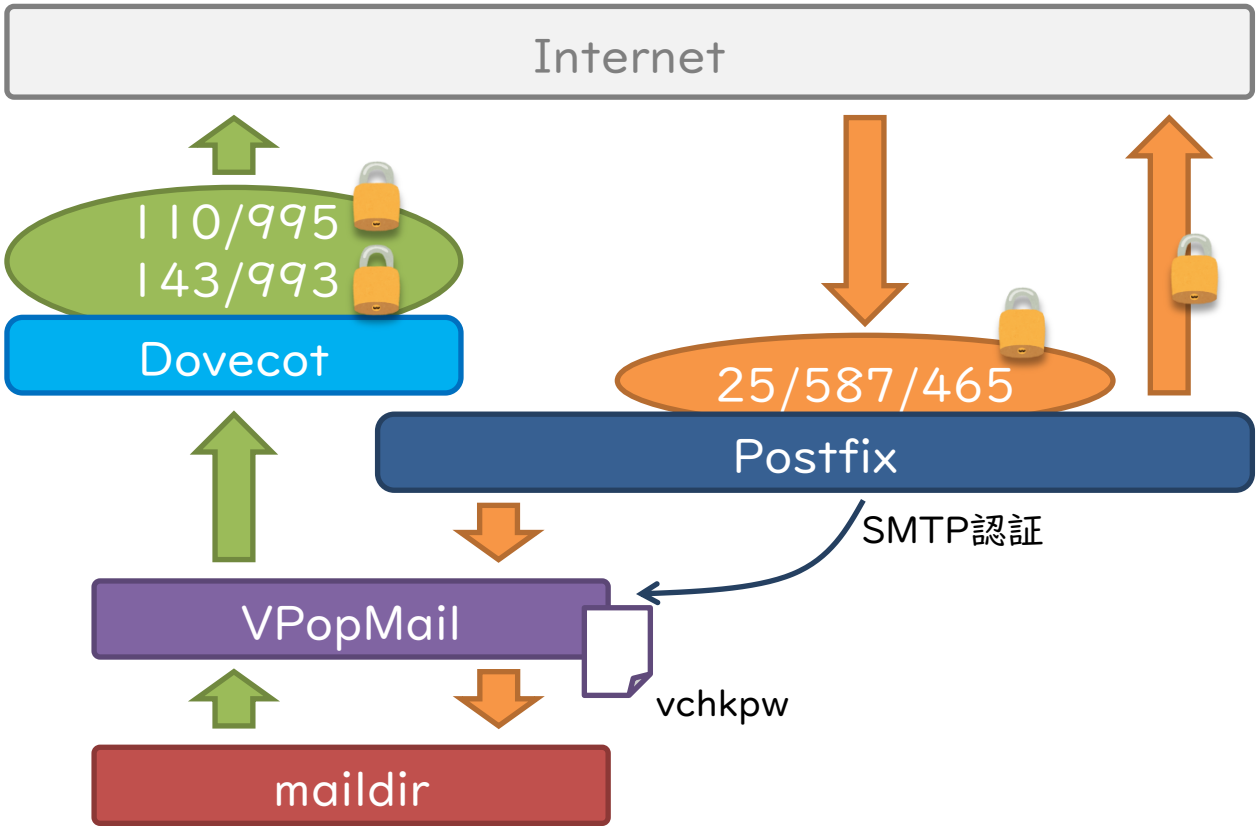
これを


Internet
143
110
25/587
Dovecot
tcpserver
qmail
VPopMail
maildir

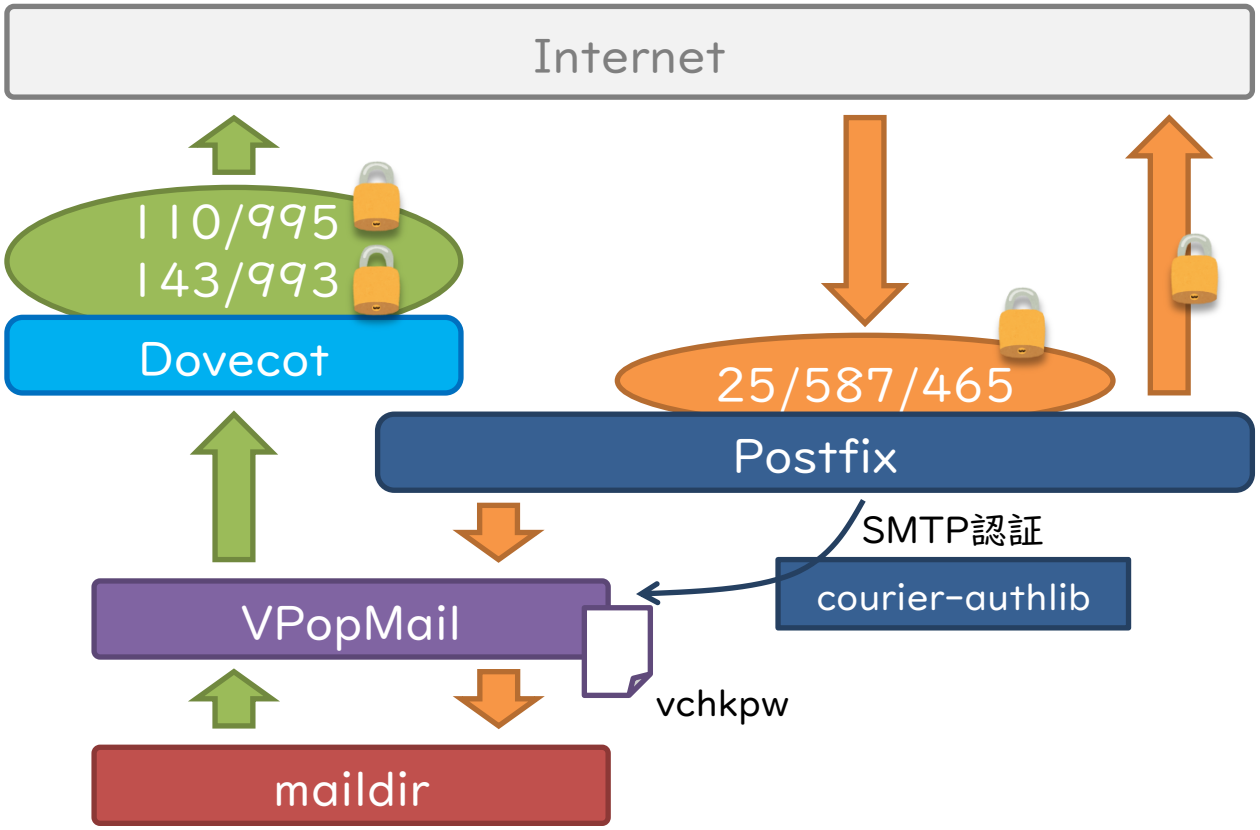
こうしてみよう


Internet
110/995
143/993
Dovecot
25/587/465
Postfix
VPopMail
maildir

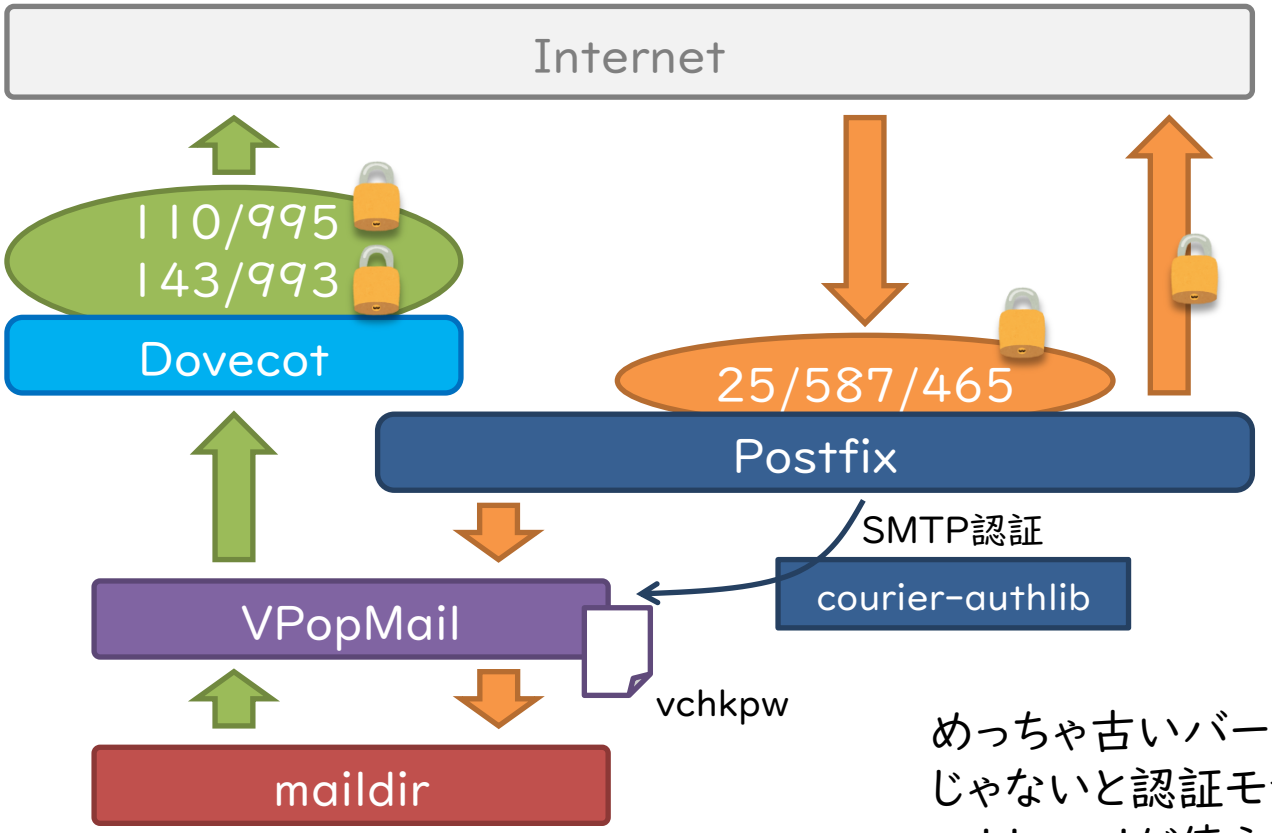
罠


Internet
110/995
143/993
Dovecot
25/587/465
Postfix
SMTP認証
VPopMail
vchkpw
maildir

罠

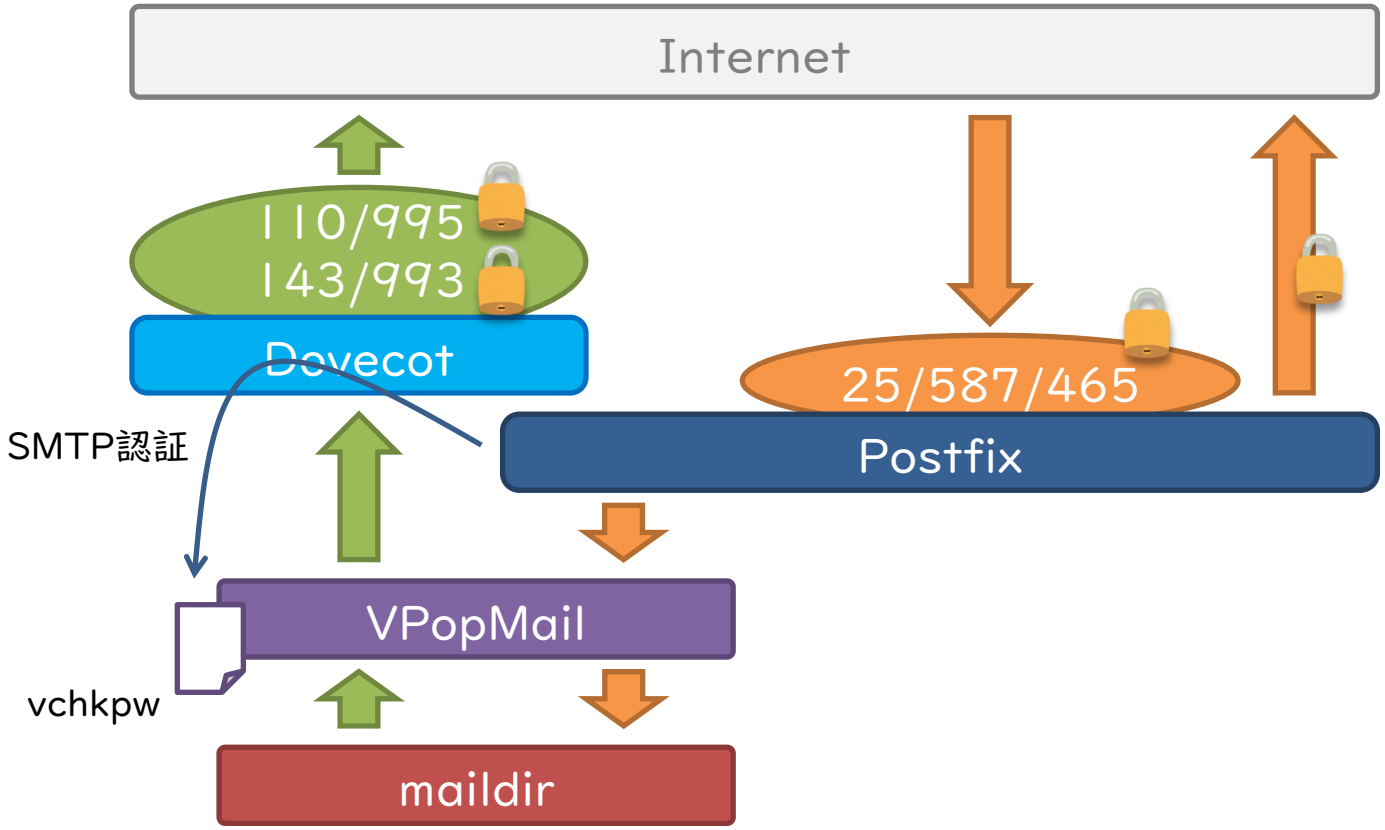

Internet
110/995
143/993
Dovecot
25/587/465
Postfix
SMTP認証
courier-authlib
VPopMail
vchkpw
maildir

罠



めっちゃ古いバージョン
じゃないと認証モジュールに
vchkpwdが使えない！

実は


Internet
110/995
143/993
Dovecot
25/587/465
Postfix
SMTP認証
VPopMail
vchkpw
maildir

構築手順

1.qmailのインストール
 (1)qmail用のユーザー・グループの作成
 (2)qmailのインストール
 (3)tcpserverのインストール

2.VPopMailのインストール
 (1)VPopMail用のユーザー・グループの作成
 (2)VPopMailの設定

3.Postfixのインストール
 (1)Postfixのインストール
 (2)Postfixの設定
 (3)Postfixのvpopmail対応
 (4)courier-authlibのインストール
 (5)courier-authlibのvpopmail対応

4.Dovecotのインストール
 (1)Dovecotのインストール
 (2)Dovecotの設定

5.SSL/TLS対応化
 (1)SSL証明書の準備
 (2)各種SSL/TLS化

できた！

```
[root@enog50 conf.d]# netstat -antlp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:587             0.0.0.0:*               LISTEN      5737/master
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN      5236/tcpserver
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN      6045/dovecot
tcp        0      0 0.0.0.0:465             0.0.0.0:*               LISTEN      5737/master
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      5737/master
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN      6045/dovecot
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN      5238/tcpserver-ssl
tcp6       0      0 :::587                  :::*                    LISTEN      5737/master
tcp6       0      0 :::143                  :::*                    LISTEN      6045/dovecot
tcp6       0      0 :::465                  :::*                    LISTEN      5737/master
tcp6       0      0 :::25                   :::*                    LISTEN      5737/master
tcp6       0      0 :::993                  :::*                    LISTEN      6045/dovecot
[root@enog50 conf.d]#
```

できた！

```
[root@enog50 conf.d]# netstat -antlp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:587             0.0.0.0:*               LISTEN      5737/master
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN      5236/tcpserver
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN      6045/dovecot
tcp        0      0 0.0.0.0:465             0.0.0.0:*               LISTEN      5737/master
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      5737/master
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN      6045/dovecot
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN      5238/tcpserver-ssl
tcp6       0      0 :::587                  :::*                    LISTEN      5737/master
tcp6       0      0 :::143                  :::*                    LISTEN      6045/dovecot
tcp6       0      0 :::465                  :::*                    LISTEN      5737/master
tcp6       0      0 :::25                   :::*                    LISTEN      5737/master
tcp6       0      0 :::993                  :::*                    LISTEN      6045/dovecot
[root@enog50 conf.d]#
```

submission
pop3
imap
smtps
smtp
imaps
pop3s

と思ったら間違えた！