

MTA の確認

```
alternatives --config mta
```

で利用する MTA の確認と選択ができる。

```
  選択      コマンド
-----
*+ 1      /usr/sbin/sendmail.sendmail
   2      /usr/sbin/sendmail.postfix
Enter を押して現在の選択 [+] を保持するか、選択番号を入力します：
```

「+」が付いている MTA が選択されているもの。

メール送信に外部の SMTP サーバを使う

gmail のパスワード

2 段階承認プロセスで認証を行なっている場合、
smtp や pop を利用した認証を行う手順

1. ブラウザ google へログイン
2. アカウント情報の画面を開く
3. ログインとセキュリティを選択
4. google へのログインを選択
5. アプリパスワードを選択
6. 新しいパスワードを発行
7. 発行したパスワードを smtp や pop のパスワードとして設定する

postfix の場合

postfix がインストールされていない場合

```
yum install postfix
```

サービスの起動と自動起動の設定をする

```
systemctl start postfix.service
systemctl enable postfix.service
```

とか

認証なしの場合 (ocn とか)

```
vi /etc/postfix/main.cf
```

```
myhostname = xxx.ddo.jp
relayhost = [xxx.ocn.ne.jp]
```

テスト

```
sendmail hoge hoge@aa.bb.cc
```

```
test
```

```
.
```

SASL 認証の場合 (gmail) とか

<http://www.uetvi.mydns.jp/wordpress/postfix-setting/entry-456.html>

<http://memo.xight.org/2009-05-24-3>

sasl plain 認証を使うので

```
cyrus-sasl-plain
```

が必要。なければ

```
yum install cyrus-sasl-plain
```

```
vi /etc/postfix/main.cf
```

```
relayhost = [smtp.gmail.com]:587
smtp_use_tls = yes

smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_tls_security_options = noanonymous
smtp_sasl_mechanism_filter = plain

smtp_tls_CApath = /etc/pki/tls/certs/ca-bundle.crt
```

証明書(/etc/pki/tls/certs/ca-bundle.crt)のパスはディストリビューションにより異なることがある。

認証するためのユーザとパスワードを設定

```
vi /etc/postfix/sasl_passwd
```

```
[smtp.gmail.com]:587 foo@gmail.com: パスワード
```

パスワードは google の 2 段階認証設定後のアプリパスワードを指定する

```
# chown root:root /etc/postfix/sasl_passwd
# chmod 600 /etc/postfix/sasl_passwd
# postmap /etc/postfix/sasl_passwd
```

/etc/postfix/sasl_passwd.db が作成されたのを確認

aws ses の場合

<https://dev.classmethod.jp/articles/sendmail-from-ses-smtpendpoint/>

テスト

```
sendmail hoge@aa.bb.cc
```

```
test
```

```
.
```

送れない場合は、google が怪しいアクセスとみなしている可能性がある。

<https://accounts.google.com/DisplayUnlockCaptcha>

へアクセスし、怪しくないことを伝える。

sendmail の場合

<http://www.sios.com/product/rhel/usersite/faq/faq3-98.html>

<http://d.hatena.ne.jp/adsaria/20080331/1207021853>

設定ファイルの変更

/etc/mail/submit.mc を編集する

```
FEATURE(`msp', `[127.0.0.1']')dnI
```

を

```
FEATURE(`msp', `[192.168.1.1']')dnI
```

などのように編集。192.168.1.1 は外部のメールサーバ。

submit.mc ファイルを submit.cf に変換

sendmail-cf パッケージが必要なので、もしなければ

```
yum install sendmail-cf
```

でインストール。

```
# make -C /etc/mail
```

で、submit.cf を作成する

sendmail サービスを再起動

```
/etc/init.d/sendmail restart
```

外部からのメールを受信する

必要なもの

ドメイン名

25 ポートの使用許可

DNS に mx レコードを指定する環境

準備

[Dynamic DNS.jp - ダイナミック DNS -](#) を例に設定。

- 1.DDO の mx レコードを確認、設定
 1. 指定先はメールを受信するサーバ
2. ポート 25 を開ける
 - 1.aws の場合以下を確認

1. セキュリティグループ
2. firewalld などのファイヤーウォール
3. aws の 25 ポートの制限
4. <https://aws.amazon.com/forms/ec2-email-limit-rdns-request>

postfix の場合

設定

```
myhostname = xxx.ddo.jp
mydomain = xxx.ddo.jp
myorigin = $mydomain
inet_interfaces = all
```

リレーサーバとして動作させる設定

注意

設定を間違えたりするとスパムメールの踏み台にされるので注意。
最悪の場合、メールサーバがブラックリストとして登録されて受信拒否される。

postfix の場合

mynetworks と relay_domains の設定でリレーの設定をする。

mynetworks

指定されたホストからのメールを受信すると、宛先が mydestination で指定されたもの以外の場合、DNS サーバを使用して宛先の名前解決を行い、自分自身以外の MTA への転送を行います。

relay_domains

mynetworks で設定されていない MTA から届いたメールをリレーするドメインを指定する。

イメージ的に mynetworks はリレー元の設定、relay_domains はリレー先の設定。

設定	mynetworks	relay_domains
デフォルト (リレーなし)	ローカル	mydestination(ローカル)
192.168.1.0/24 からのリレー許可	mynetworks=127.0.0.0/8 192.168.1.0/24	mydestination(ローカル)