参考

https://weblabo.oscasierra.net/letsencrypt-2/

Certbot を使う

Certbot クライアントのインストール

EPEL からインストールできる。

```
# yum install certbot python-certbot-apache
```

SSL/TLS 証明書の作成

Let ’s Encrypt が指定したドメインのドキュメントルートのファイルを確認し、正当性を確認した上で証明書が発行される仕組みのようです。

```
# certbot certonly --webroot -w /var/www/html -d hoge.jp
```

次にメールアドレスの入力を求められる。証明書の有効期限が近づいたりしたときのお知らせの通知さきです。

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator webroot, Installer None
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): メールアドレスを入力
```

次に規約への同意を問われる。

```
Starting new HTTPS connection (1): acme-v01.api.letsencrypt.org

-------------------------------------------------------------------------------
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v01.api.letsencrypt.org/directory
-------------------------------------------------------------------------------
(A)gree/(C)ancel: A
```

Electronic Frontier Foundation にメールアドレスを登録するかを問われる。いろいろな情報が飛んでくるらしい。とりあえず N で。

```
-------------------------------------------------------------------------------
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about EFF and
our work to encrypt the web, protect its users and defend digital rights.
-------------------------------------------------------------------------------
(Y)es/(N)o: N
```

証明書が完成。

```
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for hoge.jp
Using the webroot path /var/www/html for all unmatched domains.
Waiting for verification...
Cleaning up challenges
```

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/hoge.jp/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/hoge.jp/privkey.pem
   Your cert will expire on 2018-04-13. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

Apache に証明書を設定

SSL を設定している箇所を編集

```
vim /etc/httpd/conf.d/ssl.conf
```

```
SSLCertificateFile /etc/letsencrypt/live/[サーバーのドメイン]/cert.pem
SSLCertificateKeyFile /etc/letsencrypt/live/[サーバーのドメイン]/privkey.pem
SSLCertificateChainFile /etc/letsencrypt/live/[サーバーのドメイン]/chain.pem
```

apache 再起動

```
systemctl restart httpd
```

ファイヤーウォール設定

```
firewall-cmd --add-service=https --zone=public --permanent
firewall-cmd --reload
```

証明書の更新

```
 certbot renew
```

で更新できる。3ヶ月で証明書の期限が切れるので cron 等で毎月更新されるようにしておくとよい。

```
certbot renew --post-hook "service httpd restart"
```

で更新された際に Apache を再起動する。更新が不要だった場合は、Apache の再起動はされない。

```
crontab -e
00 03 1 * * certbot renew --post-hook "service httpd restart"
```