WEB ARCH LABO

WEBシステム開発のノウハウを蓄積・共有するエンジニア向けサイト

- Ruby
- PHP
- Java
- Apache httpd
- MySQL
- Vagrant
- Python
- その他

- トップページ
- › Let's Encrypt

CentOS 7 + Apache 2.4 に Let’s Encrypt の証明書を導入する手順

投稿者：OSCA

関東地方の美しい夜景を観にいこう。 夜景サイト「夜景散歩」で夜景スポットを検索

本稿では、CentOS 7 上で Let’s Encrypt の無償のSSL/TLSサーバー証明書を発行して Apache 2.4 で利用する手順について解説します。

手順と事前知識

まずは **Let’s Encrypt** で SSL/TLS サーバー証明書を発行するにあたり知っておくべき手順と事前知識について解説します。

Let’s Encrypt サーバーと Certbot クライアント

Let’s Encrypt における証明書発行の手順は、そのほとんどが自動化されています。 その自動化を担っているのが Let’s Encrypt のサーバーと、Certbot クライアントというソフトウェアです。 Let’s Encrypt を利用するのに最初にすべきことは、証明書を設定しようとしているマシンに Certbot クライアントをインストールすることです。 インストールした Certbot クライアントが、 Let’s Encrypt のサーバーとやり取りすることで証明書の発行と設定を自動的におこなってくれます。

事前に設定しておくべきこと (前提条件)

Let’s Encrypt で発行される証明書は、いわゆる「DV証明書」という種類の証明書です。 Let’s Encrypt サーバーは、発行する証明書の対象のドメインの所有者自身が発行要求をしてきたことを確認した上で、SSL/TLSサーバー証明書を発行します。 具体的にどのような確認が行われるのかというと、証明書の発行を要求された Let’s Encrypt サーバーは、発行しようとしている証明書のドメインの80番ポートにアクセスし、特定の内容のファイルが存在していることを確認します。 問題なくファイルが取得できればドメインの所有者が発行要求を出していることを確認できますので、これをもって証明書の発行を行うというわけです。 よって本稿の手順では、次のことを前提として解説を進めます。

- Apache httpd 2.4 がすでにインストールされている。
- インターネットから HTTP で 80 番ポートで公開しているホームページにアクセスできること。

Apache httpd 2.4 の導入が済んでいない方は、別稿「Apache httpd 2.4 を CentOS 7 に yum でインストールする手順」を参考の上でインストールしてください。 それでは事前の説明はこれくらいにしておいて、それではさっそく Let’s Encrypt での証明書の発行手順を説明します。

Certbot クライアントをインストールする

CentOS 7 用の Certbot クライアントは、EPELリポジトリからインストールすることができます。 次のように epel リポジトリをインストールした上で、certbot と python-certbot-apache をインストールします。

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

SSL/TLS証明書の作成

それでは Let's Encrypt クライアントを実行して証明書を作成しましょう。 ここでは、Apache httpd の DocumentRoot が /var/www/www.mywebsite.jp に設定されていると仮定して話を進めます。 実際の DocumentRoot の設定に合わせて読み替えてください。

次のようにオプションを指定して certbot コマンドを実行します。 -d オプションには、証明書を発行するサーバーのドメインを、-w には DocumentRoot のパスを指定します。

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

すると、まずは次のようにメールアドレスを入力するように求められます。 このメールアドレスは、後に証明書の有効期限が近づいた際にお知らせしてくれたりすることなどに利用されます。 有効なメールアドレスを入力しましょう。

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): メールアドレスを入力
```

次に規約に同意するかを問われます。 同意するために A と入力します。

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

-------------------------------------------------------------------------------
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.1.1-August-1-2016.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
```

次に Electronic Frontier Foundation にメールアドレスを共有するかを問われます。 メールアドレスを共有すると、 EFF や証明書のことなどについてのメールを送ると書かれています。 メーリングリストのようなものです。 メールを受け取りたければ Y を、受け取りたくなければ N と入力します。

```
-------------------------------------------------------------------------------
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
```

これで証明書の作成が開始されます。 正しく証明書の作成が行われた場合は、次のように出力されます。

```
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for www.mywebsite.jp
Using the webroot path /var/www/www.mywebsite.jp for all unmatched domains.
Waiting for verification...
Cleaning up challenges
Generating key (2048 bits): /etc/letsencrypt/keys/0000_key-certbot.pem
Creating CSR: /etc/letsencrypt/csr/0000_csr-certbot.pem

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at
/etc/letsencrypt/live/www.mywebsite.jp/fullchain.pem. Your cert
will expire on 2017-07-16. 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
```

これにて証明書の発行は終了です。 作成されたサーバー証明書は、次のように /etc/letsencrypt/live/[発行したサーバーのドメイン]/ 内に作成されました。

```
# ls -l /etc/letsencrypt/live/www.mywebsite.jp/
total 4
-rw-r--r-- 1 root root 543 Apr 17 17:23 README
lrwxrwxrwx 1 root root 44 Apr 17 17:23 cert.pem -> ../../archive/www.mywebsite.jp/cert1.pem
lrwxrwxrwx 1 root root 45 Apr 17 17:23 chain.pem -> ../../archive/www.mywebsite.jp/chain1.pem
lrwxrwxrwx 1 root root 49 Apr 17 17:23 fullchain.pem ->
../../archive/www.mywebsite.jp/fullchain1.pem
lrwxrwxrwx 1 root root 47 Apr 17 17:23 privkey.pem -> ../../archive/www.mywebsite.jp/privkey1.pem
```

Apache 2.4 への設定

SSL/TLSサーバー証明書が作成できましたので、Apache 2.4 に設定を追加します。 ssl.conf の SSLCertificateFile SSLCertificateKeyFile SSLCertificateChainFile にそれぞれ設定します。

```
[/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
...
```

これで Apache httpd を再起動して完了です。

```
# systemctl start httpd
```

それではさっそく https://[サーバーのドメイン]/ にアクセスしてみましょう。 アクセスすることができましたでしょうか？ もし接続できない場合は、SELinux や firewalld などによりアクセスが遮断されていないかを確認してください。 firewalld によってアクセスが遮断されてしまっている場合は、次のようなコマンドで HTTPS (443) ポートを開放することができます。

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

ブラウザで証明書の情報を確認してみると Let's Encrypt で発行したものだということがわかると思います。

これで Let's Encrypt での証明書の設定は終了です。

証明書の更新

Let's Encrypt で発行した証明書は、有効期限が3ヶ月となっています。 証明書の有効期限が近づくと、証明書の発行時に入力したメールアドレスに「まもなく証明書の有効期限が切れる」と

いう旨のメールが届きます。 その際には、証明書の有効期限が切れる前に certbot renew というコマンドを実行するだけで、証明書の有効期限を延長することができます。

```
# certbot renew
```

証明書の有効期限が近づくたびに手動で証明書の有効期限を延長しても良いですが、cron などで certbot renew コマンドを毎月1回実行するようにしておくと手間が省けて良いでしょう。 自動的に証明書を更新することができます。 なおその際には、Apache も再起動して更新された証明書を読み込むようにすることを忘れないようにしましょう。 自動的に証明書を更新する詳しい手順については、別稿をご覧ください。

Let’s Encrypt の証明書の更新を自動化する手順 (cron)

Let’s Encrypt の証明書の更新を cron で自動化する手順について解説します。

weblabo.oscasierra.net

おわりに

本稿では、CentOS 7 で Let’s Encrypt で発行されたSSL/TLS証明書を Apache 2.4 に設定する手順について解説しました。 個人でも手軽にSSL/TLS証明書が手に入れられるようになったのは、とても革新的だと思います。 是非積極的に利用したいものです。

更新履歴

- 2015年12月09日 – Let’s Encrypt の Open Beta 版に合わせた初稿を公開しました。
- 2017年04月17日 – Certbot を利用した最新の利用方法に合わせて記事を改変しました。

著者：OSCA

Java, PHP 系のWEBエンジニア。 WEBエンジニア向けコミュニティ「WEBエンジニア勉強会」を主催。
個人として何か一つでも世の中の多くの人に使ってもらえるものを作ろうと日々奮闘中。
@engineer_osca

WEBエンジニア勉強会 最新情報

- WEBエンジニア勉強会 #13 を開催しました
- WEBエンジニア勉強会 #13, 05月24日開催！
- WEBエンジニア勉強会 #12 を開催しました
- WEBエンジニア勉強会 #12, 03月29日開催！
- WEBエンジニア勉強会 #11 を開催しました
- WEBエンジニア勉強会 #11, 02月01日開催！

- Ruby
- PHP
- Python
- Java
- Swift
- Apache Maven
- Apache Tomcat
- Vagrant
- Subversion
- Apache httpd

- MySQL
- Redis
- ownCloud
- OpenSSL
- OpenSSH
- CentOS 6

About Us

- WEB ARCH LABO について
- 広告掲載のご案内