Apache(mod_ssl)編

改版履歴			
版数	日付	内容	担当
V.1.1	2014/12/22	初版	NII
V.1.2	2015/5/15	中間CA証明書のファイル名を修正	NII
V.1.3	2015/12/11	サーバ証明書設定について注釈を追加	NII
V.2.0	2018/2/26	SHA1の記載内容の削除	NII
V.2.1	2018/3/26	CT対応版の中間CA証明書について説明を追加	NII
V.2.2	2018/4/27	Apache(mod_ssl)2.4.8以降における手順を追加	NII
V.2.3	2018/7/9	ECDSA対応版の中間CA証明書についての説明を追加	NII
V.2.4	2019/4/22	ECC認証局 中間CA証明書の名称を変更	NII
V.2.5	2020/4/13	中間CA証明書のファイル名を修正	NII
V.2.6	2020/8/25	中間CA証明書の記載内容を修正	NII
V.2.7	2020/12/22	中間CA証明書を修正	NII

目次

1. Apache (mod_ssl) によるサーバ証明書の利用

1-1. 前提条件

Apache（mod_ssl）でサーバ証明書を利用する場合の前提条件について記載します。適宜、サーバ証明書をインストールする利用管理者様の環境により、読み替えをお願いします。
（本マニュアルでは、Red Hat Enterprise Linux Server release 6.3 (Santiago)、OpenSSL 1.0.1e-fips 11 Feb 2013、Apache/2.2.15 (Unix) または Apache/2.4.9 (Unix)での実行例を記載しております）

前提条件

1. OpenSSLがインストールされていること
2. Apacheがインストールされていること
3. 使用されているApacheシステムに適当なmod_sslがインストールされていること
4. ssl.confファイルまでの絶対パス：/etc/httpd/conf.d/ssl.conf
5. httpd.confファイルまでの絶対パス：/etc/httpd/conf/httpd.conf
6. ssl.confファイルの設定
   a. SSLCertificateFile: /etc/httpd/conf/ssl.crt/server.crt （サーバ証明書を配置）
   b. SSLCertificateKeyFile: /etc/httpd/conf/ssl.key/server.key （秘密鍵を配置）
   c. SSLCertificateChainFile: /etc/httpd/conf/ssl.crt/nii-odca3sha2ct.cer （SHA-2認証局 中間CA証明書を配置）
   または
   /etc/httpd/conf/ssl.crt/nii-odca3ecdsa.cer （ECC認証局 中間CA証明書を配置）

Apache2.4.8以降をご利用の場合

a. SSLCertificateFile: /etc/httpd/conf/ssl.crt/server.crt (サーバ証明書と中間CA証明書を連結した証明書を配置)
b. SSLCertificateKeyFile: /etc/httpd/conf/ssl.key/server.key (秘密鍵を配置)

CSR作成時は既存の鍵ペアは使わずに、必ず新たにCSR作成用に生成した鍵ペアを利用してください。
更新時も同様に、鍵ペアおよびCSRを新たに作成してください。
鍵ペアの鍵長は、RSAの場合は2048bit、ECDSAの場合は384bitにしてください。
※Apache2.2(mod_ssl)はECDSA鍵について非対応となっております。

1-2. 証明書のインストール

Apache(mod_ssl)への証明書のインストール方法について記述します。

1-2-1. 事前準備

事前準備として、サーバ証明書、中間CA証明書を取得してください。

事前準備

別ページ記載の手順(※)にて取得したサーバ証明書をserver.crtという名前で任意の場所に保存してください。
※「サーバー証明書インストールマニュアル / Apache・IIS・Nginx編 / 事前準備 〜 証明書の申請から取得まで」 - 「3.証明書の申請から取得まで」を参照

1. 中間CA証明書を準備します。
2. 次のURLにアクセスすることでリポジトリにアクセスすることが可能です。

●リポジトリ（証明書の発行日時が2020年12月25日0時以降の場合）：https://repo1.secomtrust.net/sppca/nii/odca4/index.html
サーバー証明書 RSA認証局　中間CA証明書
「NII Open Domain CA - G7 RSA(SC Organization Validation CA) CA証明書(nii-odca4g7rsa.cer)」
サーバー証明書 ECC認証局　中間CA証明書
「NII Open Domain CA - G7 ECC(SC Organization Validation CA) CA証明書(nii-odca4g7ecc.cer)」

●リポジトリ（証明書の発行日時が2020年12月25日0時以前の場合）：https://repo1.secomtrust.net/sppca/nii/odca3/index.html
SHA-2認証局CT対応版サーバ証明書
「国立情報学研究所 オープンドメイン SHA-2認証局 CT対応版 CA証明書(nii-odca3sha2ct.cer)」
ECC認証局サーバ証明書
「国立情報学研究所 オープンドメイン ECC認証局 CA証明書(nii-odca3ecdsa201903.cer)」

【SHA-2認証局 CT対応版 CA証明書(nii-odca3sha2ct.cer)をインストールする場合】
SHA-2認証局 CT対応版 CA証明書をnii-odca3sha2ct.cerという名前で保存したと仮定して以降記載します。

【サーバー証明書(ecdsa-with-SHA384)をインストールする場合】
ECC認証局 中間CA証明書 をnii-odca3ecdsa.cerという名前で保存したと仮定して以降記載します。

1-2-2. 中間CA証明書のインストール

以下の手続きに従って、中間CA証明書のインストールを行ってください。

中間CA証明書のインストール

中間CA証明書は「1-1.前提条件」条件6.で記述した**ssl.conf**ファイルの「**SSLCertificateChainFile**」で指定します。
「1-2-1. 事前準備」で取得した中間CA証明書を「1-1. 前提条件」条件6.c.で記述したパスへ移動してください。

SHA-2認証局 中間CA証明書の場合

```
$ mv nii-odca3sha2ct.cer /etc/httpd/conf/ssl.crt/nii-odca3sha2ct.cer
```

ECC認証局 中間CA証明書の場合

```
$ mv nii-odca3ecdsa.cer /etc/httpd/conf/ssl.crt/nii-odca3ecdsa.cer
```

Apache2.4.8以降をご利用の場合

後述の「1-2-3. サーバ証明書のインストール」手順にて記載します。
(Apache2.4.8以降では設定ファイルで中間CA証明書を指定する**SSLCertificateChainFile**ディレクティブが廃止されました)

1-2-3. サーバ証明書のインストール

新規でサーバ証明書をインストールする場合は以下の手続きによりサーバ証明書のインストールを実施してください。

サーバ証明書のインストール

サーバ証明書は「1-1. 前提条件」条件6.で記述した**ssl.conf**ファイルの「**SSLCertificateFile**」で指定します。

「1-2-1. 事前準備」で取得したサーバ証明書を「1-1. 前提条件」条件6.a.で記述したパスへ移動してください。

```
$ mv server.crt    /etc/httpd/conf/ssl.crt/server.crt
```

Apache2.4.8以降をご利用の場合

「1-2-1. 事前準備」で取得したサーバ証明書と中間CA証明書を連結して保存します。

SHA-2認証局 中間CA証明書の場合

```
$ cat server.crt nii-odca3sha2.cer > server.crt
```

ECC認証局 中間CA証明書の場合

```
$ cat server.crt nii-odca3ecdsa.cer > server.crt
```

※ 上記コマンドの前提
・連結前の証明書は同ディレクトリに存在する
・連結前のサーバ証明書は、連結後の内容で上書保存する

連結した証明書は「1-1. 前提条件」条件6.a.で記述したパスへ移動してください。

1-3. Apacheの設定変更

Apacheに証明書を適用するための設定方法について記述します。

Apacheの設定変更

証明書のインストール終了後、「1-1. 前提条件」で記述したssl.confファイルの編集を行ってください。
（既に「1-1. 前提条件」の通りにssl.confファイル設定済である場合は、当手順は不要です）

証明書の更新を行った場合は新たに作成した秘密鍵を**SSLCertificateKeyFile**に、新たに作成したサーバ証明書を**SSLCertificateFile**に、新たに取得した中間ＣＡ証明書を**SSLCertificateChainFile**に設定してください。

```
・・・
SSLCertificateFile:
←デフォルトでは/etc/httpd/conf/ssl.crt/server.crt （サーバ証明書を配置）
SSLCertificateKeyFile:
←デフォルトでは/etc/httpd/conf/ssl.key/server.key （秘密鍵を配置）
SSLCertificateChainFile:
←デフォルトでは/etc/httpd/conf/ssl.crt/server-chain.crt（中間CA証明書を配置）
・・・
```

Apacheを再起動し、変更した設定を反映させます。

```
$ /etc/init.d/httpd stop ←Apacheの停止

$ /etc/init.d/httpd start ←Apacheの起動
```

Apache2.4.8以降をご利用の場合

証明書の更新を行った場合は新たに作成した秘密鍵を**SSLCertificateKeyFile**に、新たに作成したサーバ証明書と中間CA証明書を連結した証明書を**SSLCertificateFile**に設定してください。

```
・・・
SSLCertificateFile:
←デフォルトでは/etc/httpd/conf/ssl.crt/server.crt （連結した証明書を配置）
SSLCertificateKeyFile:
←デフォルトでは/etc/httpd/conf/ssl.key/server.key （秘密鍵を配置）
・・・
```

Apacheを再起動し、変更した設定を反映させます。

```
$ /etc/init.d/httpd stop ←Apacheの停止

$ /etc/init.d/httpd start ←Apacheの起動
```

1-4. サーバ証明書の置き換えインストール

更新したサーバ証明書をインストールする場合は以下の手続きによりサーバ証明書のインストールを実施してください。

サーバ証明書の置き換えインストール

1. 旧サーバ証明書の鍵ペアをコピーしてください。

```
$ cd /etc/httpd/conf/ssl.key/
$ cp server.key server.key.old
```

2. 更新対象のサーバ証明書をコピーして、保管してください。

```
$ cd /etc/httpd/conf/ssl.crt/
$ cp server.crt  server.crt.old
```

3. 更新対象の中間CA証明書をコピーして、保管してください
SHA-2認証局 中間CA証明書の場合

```
$ cd /etc/httpd/conf/ssl.crt/
$ cp nii-odca3sha2ct.cer  nii-odca3sha2ct.cer.old
```

ECC認証局 中間CA証明書の場合

```
$ cd /etc/httpd/conf/ssl.crt/
$ cp nii-odca3ecdsa.cer  nii-odca3ecdsa.cer.old
```

4. 別ページ記載の手順「支援システム操作手順書 / 利用管理者用」 - 「2-2. サーバ証明書更新申請手続き概要」に従い、証明書の更新申請を実施してください。

5. 「1-2-1. 事前準備」で取得したサーバ証明書を、「1-1. 前提条件」条件6.a.で記述したパスへ移動してください。

```
$ mv server.crt  /etc/httpd/conf/ssl.crt/server.crt
```

6. 「1-2-1. 事前準備」で取得した中間CA証明書を、「1-1. 前提条件」条件6.c.で記述したパスへ移動してください。

SHA-2認証局 中間CA証明書の場合

```
$ mv nii-odca3sha2ct.cer  /etc/httpd/conf/ssl.crt/nii-odca3sha2ct.cer
```

ECC認証局 中間CA証明書の場合

```
$ mv nii-odca3ecdsa.cer  /etc/httpd/conf/ssl.crt/nii-odca3ecdsa.cer
```

Apache2.4.8以降をご利用の場合

1. 旧サーバ証明書の鍵ペアをコピーしてください。

```
$ cd /etc/httpd/conf/ssl.key/
$ cp server.key server.key.old
```

2. 更新対象のサーバ証明書をコピーして、保管してください。

```
$ cd /etc/httpd/conf/ssl.crt/
$ cp server.crt  server.crt.old
```

3. 別ページ記載の手順「支援システム操作手順書 / 利用管理者用」 - 「2-2. サーバ証明書更新申請手続き概要」に従い、証明書の更新申請を実施してください。

4. 「1-2-1. 事前準備」で取得したサーバ証明書、中間CA証明書を用いて「1-2-3. サーバ証明書のインストール」の手順を実施し、連結してください。

1-5. 起動確認

インストールした証明書によるSSL通信に問題がないか確認する方法を記述します。

証明書の反映・確認
1. Apacheを再起動し、変更した設定を反映させます。 $ /etc/init.d/httpd stop ←Apacheの停止 $ /etc/init.d/httpd start ←Apacheの起動 2. ブラウザ経由で、該当のサーバへアクセスし、SSL通信に問題がないことを確認してください。