Nginx編

改版履歴			
版数	日付	内容	担当
V.1.0	2018/2/26	初版	NII
V.1.1	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.1.2	2018/7/9	ECDSA対応版の中間CA証明書について説明を追加	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. Nginxによるサーバ証明書の利用

1-1. 前提条件

Nginxでサーバ証明書を使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OpenSSL 1.0.1e、Nginx1.2.0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. Nginxがインストールされていること 3. nginx.confファイルまでの絶対パス：/etc/nginx/conf/nginx.conf a. ssl_certificate: /etc/nginx/conf/cert.pem（サーバ証明書を配置） b. ssl_certificate_key: /etc/nginx/conf/cert.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鍵の場合、2048bit
ECDA鍵の場合、384bit
にしてください。

1-2. 証明書のインストール

本章ではNginx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

「証明書の受領」で受領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。

●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証明書の配置

以下の手続きに従って、中間CA証明書を指定したパスへ配置してください。

中間CA証明書の配置

「1-2-1.事前準備」で取得した中間CA証明書を下記のパスへ配置してください。

SHA-2認証局 中間CA証明書の場合

```
$ mv nii-odca3sha2ct.cer /etc/nginx/conf/nii-odca3sha2ct.cer
```

ECC認証局 中間CA証明書の場合

```
$ mv nii-odca3ecdsa.cer /etc/nginx/conf/nii-odca3ecdsa.cer
```

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3で記述したnginx.confファイルの「ssl_certificate」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」3.a.で記述したパスへ移動してください。

```
$ mv server.crt　/etc/nginx/conf/
```

「1-2-2.中間CA証明書の配置」で取得した中間CA証明書とサーバ証明書を連結します。

SHA-2認証局 中間CA証明書の場合

```
$ cat server.crt nii-odca3sha2ct.cer > cert.pem
```

ECC認証局 中間CA証明書の場合

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

1-3. Nginxの設定変更

本章ではNginx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。

Nginx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nginx.confファイルの編集を行ってください。

証明書の更新を行った場合は新たに作成した秘密鍵を**ssl_certificate_key**に、新たに作成した証明書を**ssl_certificate**に設定してください。

（1-1 前提条件のとおりである場合は、設定の変更は必要ございません）

```
 ・・・
ssl_certificate:
←デフォルトではcert.pem（サーバ証明書を配置）
ssl_certificate_key:
←デフォルトではcert.key（秘密鍵を配置）
```

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/nginx/conf/
$ cp cert.key cert.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。

```
$ cp cert.pem cert.pem.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

```
$ cp nii-odca3sha2ct.cer　nii-odca3sha2ct.cer.old
```

   ECC認証局 中間CA証明書の場合

```
$ cp nii-odca3ecdsa.cer　nii-odca3ecdsa.cer.old
```

4. 本マニュアルに従い、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」3.a.で記述したパスへ移動してください。

```
$ mv server.crt　/etc/nginx/conf/server.crt
```

6. 「1-2-1.事前準備」で取得した中間CA証明書を「1-2-2.中間CA証明書の配置」に従って指定の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/nginx/conf/nii-odca3sha2ct.cer
```

   ECC認証局 中間CA証明書の場合

```
$ mv nii-odca3ecdsa.cer　/etc/nginx/conf/nii-odca3ecdsa.cer
```

7. 「1-2-2.中間CA証明書の配置」で取得した中間CA証明書とサーバ証明書を連結します。

   SHA-2認証局 中間CA証明書の場合

```
$ cat server.crt nii-odca3sha2ct.cer > cert.pem
```

   ECC認証局 中間CA証明書の場合

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

1-5. 起動確認

本章では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. Nginxを再起動し、変更した設定を反映させます。

```
$ /sbin/nginx -s stop ←Nginxの停止

$ /sbin/nginx ←Nginx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。