OpenLDAP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	誤記修正 DNのルールの修正	NII
V.1.3	2018/8/21	ECC非対応の記載を追加	NII
V.2.5	2019/6/10	DNのルール(Locality Name)の修正	NII
V.2.6	2020/4/13	DNのルール(State or Province Name、Locality Name)の修正	NII
V.2.7	2020/7/15	DNのルール、TSVファイル形式のSTおよびLの値の説明、リンクの変更	NII
V.2.8	2020/8/25	中間CA証明書の記載内容を修正	NII
V.2.9	2020/12/22	中間CA証明書を修正 サーバー証明書L、STを必須に修正 サーバー証明書OUの利用条件を修正	NII
V.2.10	2022/08/02	CSR作成からOUを削除	NII

目次

1. OpenLDAP2.4 によるサーバ証明書の利用

1-1. 前提条件

OpenLDAP2.4 (以下OpenLDAP)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。適時、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 7.2 (Maipo)、OpenSSL1.0.1eでCSRを作成し、OpenLDAP2.4.44へインストールする方法での実行例を記載しております）

前提条件

1. 鍵ペア及びCSRを生成する端末にOpenSSLがインストールされていること。
2. 証明書をインストールする端末にOpenLDAP 2.4がインストールされていること。
   ※ LDAP server及びLDAP clientを含みます
3. OpenLDAPの証明書参照先について本マニュアルでは以下ディレクトリとします。
   「/etc/openldap/certs」
4. 発行されたサーバ証明書について本マニュアルでは以下ファイル名とします。
   「server.crt」

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2048bitにしてください。

※ OpenLDAPではECC 証明書 はサポートされていません。

1-2. 事前準備

鍵ペア・CSRを生成する前に、事前に以下の項目の準備をしてください。

事前準備

1. 乱数生成用ファイルの準備(200KB程度のファイルであればどんなものでもかまいません) 本マニュアルではファイル名を**randfile1.txt、randfile2.txt、randfile3.txt**とします。
2. サーバ鍵ペア用私有鍵パスフレーズ***<PassPhrase>***([**1-3-1**、**1-3-2**で使用])
3. サーバ DN（※サーバDNについては、本サービス証明書ポリシまたは、下記DNのルールをご確認ください）

CSRに記述するDNのルールは以下のとおりとなります。

DNのルール			
項目	指定内容の説明と注意	必須	文字数および注意点
Country (C)	本認証局では必ず「JP」と設定してください。 例）C=JP	○	JP固定
State or Province Name (ST)	「都道府県」（ST）は利用管理者及び利用者が所属する組織の所在地の都道府県名としサービス窓口に事前に届出したとおりの所在地の都道府県名をローマ字表記で指定してください。この情報は各所属機関の登録担当者にお問い合わせください。 例）ST=Tokyo	○	STとして指定できる値は下記リンクを参照してください。機関ごとに固定となります。 UPKI証明書 主体者DNにおける ST および L の値一覧 ※STおよびLが必須。（2020年12月22日以降）
Locality Name(L)	「場所」（L）は利用管理者及び利用者が所属する組織の所在地の市区町村名とし、サービス窓口に事前に届出したとおりの所在地の市区町村名をローマ字表記で指定してください。この情報は各所属機関の登録担当者にお問い合わせください。 例)L=Chiyoda-ku	○	Lとして指定できる値は下記リンクを参照してください。機関ごとに固定となります。 UPKI証明書 主体者DNにおける ST および L の値一覧 ※STおよびLが必須。（2020年12月22日以降）
Organization Name(O)	サービス参加申請時の機関名英語表記を設定してください。この情報は各所属機関の登録担当者にお問い合わせください。 例)O=National Institute of Informatics	○	半角の英数字64文字以内 (記号は「'(),-./:=」と半角スペースのみ使用可能)
Common Name (CN)	サーバ証明書URLに表示されるウェブ・サーバの名前をFQDNで設定してください。例えばSSL/TLSを行うサイトが https://www.nii.ac.jpの場合には、「www.nii.ac.jp」となります。 FQDNにはサービス参加申請時に登録いただいた対象ドメイン名を含むFQDNのみ、証明書発行が可能となります。 例)www.nii.ac.jp	○	証明書をインストールする対象サーバのFQDNで64文字以内 半角英数字、”．“、“-”のみ使用可能。また、先頭と末尾に“.”と“-”は使用不可
Email	本認証局では使用しないでください。	×	
鍵長			
RSA 2048bit			

○・・・必須　×・・・入力不可　△・・・省略可

注意：証明書の更新を行う場合は、先に1-6をご確認ください。

1-3. 鍵ペアの生成とCSRの作成

1-3-1. 鍵ペアの生成

以下に鍵ペアの生成方法を記述します。

鍵ペアの作成

1. 鍵ペアを生成するため、「1-2.事前準備」の手続き1で用意したファイル (200 KB 程度) を3つ選んでください。
   この手続きでは、 選択したファイルの名前を「randfile1.txt」、「randfile2.txt」、「randfile3.txt」として表記します。

2. 用意したファイルを、作業ディレクトリに移動してください。

   ```
   $mv <randfile1.txt> <randfile2.txt> <randfile3.txt> /etc/httpd/conf/ssl.key/
   ```

3. 鍵ペアの作成を行うため、次のコマンドを入力してください。
   今回のコマンド例では、 作業ディレクトリに移動し、2048 bitの RSA 鍵ペアを生成し、「servername.key」という名前で保存することを示しています。

   ※OpenLDAPではパスフレーズ付きの私有鍵を利用することが出来ないため、 <PassPhrase> には何も入力せずEnterを押下してください。

   ```
   $cd /etc/httpd/conf/ssl.key/ ←作業ディレクトリへ移動してください
   $openssl genrsa -des3 -rand <randfile1.txt>:<randfile2.txt>:<randfile3.txt> 2048 > servername.key
   Generating RSA private key, 2048 bit long modulus
   ..............................++++++
   ..............++++++
   unable to write 'random state'
   e is 65537 (0x10001)
   Enter pass phrase: <PassPhrase>                    ←私有鍵パスフレーズ入力
   Verifying - Enter pass phrase: <PassPhrase>        ←私有鍵パスフレーズ再入力
   ```

   重要： この鍵ペア用私有鍵は、証明書のインストール時に必要となるファイルです。
   OpenLDAPではパスフレーズ付きの私有鍵を利用することが出来ないため、情報が他人に漏れることがないよう、安全な方法で管理してください。

4. 作成した鍵ペアのファイルを保存します。バックアップは外部媒体ディスク等に保存し、安全な場所に保存してください。
   鍵ペアの中の私有鍵を利用すれば、お使いのウェブ・サーバがSSL/TLS で保護して送受信したデータを、解読することができてしまいます。
   従って保存する鍵ペアファイルへのアクセス権は利用管理者自身とSSL/TLS サーバのプロセス等必要最小限になるよう設定してください。
   またバックアップを保存した外部媒体ディスク等も利用管理者のみまたは同じ権限のある方のみ利用できる場所へ保管してください。
   また、鍵ペア用私有鍵パスフレーズの管理も、確実に行ってください。鍵ペアファイルの紛失、鍵ペア用私有鍵パスフレーズ忘れ等が発生した場合、証明書のインストールが行えなくなります。
   この場合、新たに証明書を申請しなおしていただくことになりますので、ご注意ください。

1-3-2. CSRの生成

鍵ペアが作成されたことを確認後、CSRを生成します。

CSRの作成

1. 次のコマンドを入力し、CSRの作成を開始してください。パスフレーズの入力が求められますので、「1-3-1 鍵ペアの生成」の手続き3で作成した私有鍵のパスフレーズを入力してください。

   コマンドでは、署名アルゴリズムSHA2でCSRを作成し、「servername.csr」（ファイル名は任意）というファイル名で保存することを示しています。

   ```
   $openssl req -new -key servername.key -sha256 -out servername.csr ←CSRファイル名
   Enter pass phrase for servername.key: <PassPhrase> ←私有鍵パスフレーズ入力
   ```

   「**-sha256**」:署名アルゴリズムを示すオプション。
   署名アルゴリズムSHA1でCSRを作成する場合は、「**-sha1**」に置き換えてください。

2. コマンドでは、署名アルゴリズムでCSRを作成し、「servername.csr」（ファイル名は任意）というファイル名で保存することを示しています。

3. パスフレーズの入力に成功するとDN情報の問い合わせが行われますので、「1-2. 事前準備」の「DNルール」に従い、DN情報を入力してください。
OpenSSLでは必要ない項目を「.」ドットを入力することにより、省略することができます。

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

 Country Name (2 letter code) [AU]:JP ←"JP"を入力
 State or Province Name (full name) []:Tokyo ←都道府県名の入力
 Locality Name (eg, city) []:Chiyoda-ku ←市区町村名を入力
 Organization Name (eg, company) [Default Company Ltd]:National Institute of Informatics ← 組織名を入力
 Organizational Unit Name (eg, section) []:. ← 「.」ドットを入力
 Common Name (eg, your name or your server's hostname) []:www.nii.ac.jp ← サーバ名FQDN を入力
 Email Address []:. ← 「.」ドットを入力
 Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:.← 「.」ドットを入力
 An optional company name []:.← 「.」ドットを入力
```

要求された情報の入力が完了すると CSR が生成され、servername.csrに保存されます。なお、このファイルも、バックアップをとって、証明書を受領するまでは別途保管することをお勧めします。

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBhDCB7gIBADBFMQswCQYDVQQGEwJKUDEQMA4GA1UEBxMHQWNhZGVtZTEMMAo
G
例
Um0E3vq8Ajg=
-----END CERTIFICATE REQUEST-----
```

以下のコマンドを入力することにより、CSRの内容を確認することができます。

```
$ openssl req -noout -text -in servername.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=JP, ST=Tokyo, L=Chiyoda-ku, O=National Institute of Informatics, O=Cyber Science Infrastructure
Development Department,CN=www.nii.ac.jp←CSR生成時に入力したDNと一致していることを確認してください。
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public Key: (2048 bit)←鍵長が2048bitであることを確認してください。
                Modulus:
                00:c9:0e:99:5c:8a:4a:e3:b2:e2:0d:3d:60:4d:30:
                                :
                               例
                                :
                ca:2e:56:f7:66:bd:01:44:ea:f3:ca:d2:f6:e0:5e:
                6c:57:4b:65:e4:e7:f7:ca:dd
            Exponent: 65537 (0x10001)
    Attributes:
        a0:00
    Signature Algorithm: sha256WithRSAEncryption← CSR生成時に指定した署名アルゴリズムであることを確認してください。署名アルゴリズムにsha1を指定した場合は「sha1WithRSAEncryption」と表示されます。

    88:44:e5:27:06:02:ec:85:6c:29:6a:0f:a3:92:87:4e:e2:f1:
                           :
                          例
                           :
    9c:3c:0b:7e:1c:55:3d:c3:b3:7a:3a:36:d1:f6:3a:97:78:1a:
    c1:cc
```

1-4. 証明書の申請から取得まで

CSRを作成しましたら、登録担当者へ送付する証明書発行申請TSVファイルを作成し申請します。発行申請TSVファイルの作成方法、申請方法等につきましては、「**証明書自動発行支援システム操作手順書（利用管理者用）**」をご確認ください。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください
証明書の発行が完了すると、本システムより以下のメールが送信されます。メール本文に記載された証明書取得URLにアクセスし、証明書の取得を実施してください。

証明書取得URLの通知

【件名】
Webサーバ証明書発行受付通知

・・・・・

#以下に証明書の取得先が記述されています。
貴機関の登録担当者経由で発行申請をいただきましたサーバ証明書を配付いたします。
本日から1ヶ月以内に以下の証明書取得URLへアクセスし、サーバ証明書の取得を行ってください。
証明書取得URL：

https://scia.secomtrust.net/ **←左記URLにアクセスし証明書の取得を行ってください。**

～

・・・・・

1-5. 証明書のインストール

本章ではOpenLDAPへのサーバ証明書のインストール方法について記述します。

1-5-1. 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

1. 「1-4.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。
   中間CA証明書を準備します。
   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)」

   ●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)」
   SHA-2認証局 CA証明書 (CT対応版)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。

1-5-2. 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

「1-5-1.事前準備」で取得した中間CA証明書を「1-1.前提条件」3.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/openldap/certs/nii-odca3sha2ct.cer
```

1-5-3. 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

「1-3-1. 鍵ペアの生成」で作成した私有鍵を「1-1.前提条件」3.で記述したパスへ移動してください。

```
$ mv servername.key /etc/openldap/certs/servername.key
```

重要：OpenLDAPではパスフレーズ付き秘密鍵ファイルを利用できません。当ファイルは「1-3-1. 鍵ペア生成」でパスフレーズなしで作成した私有鍵となります。
適切にディレクトリ・ファイルのアクセス権限を設定する。運用をイントラ環境のみなどの、閉じられた環境のみにする。
フロントに別サーバを介し直接OpenLDAPサーバにアクセスさせない。等十分なセキュリティ対策を利用者様にて施した上保管してください。
OpenLDAPにおける、私有鍵のパスフレーズ利用について詳しくは以下URLを参照下さい。

参照：https://www.openldap.org/doc/admin24/tls.html#Server%20Certificates
「16.2.1.4. TLSCertificateKeyFile <filename>」項

「1-4-1.証明書の申請から取得まで」で受け取ったサーバ証明書を「1-1.前提条件」3.で記述したパスへ移動してください。

```
$mv server.crt /etc/openldap/certs/server.crt
```

1-6. OpenLDAPの設定変更

配置した証明書を読み込むための設定と、LDAPSを有効にするための設定を追加する必要があります。

OpenLDAPの設定変更

１．配置した中間CA証明書と、サーバ証明書を読み込む設定を追加します。
1-1. 以下に示すldapmodifyによる設定変更ファイルを作成します。

```
$vi ./enable-ldaps.ldif
dn:cn=config
changetype:modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/openldap/certs/nii-odca3sha2ct.cer ←中間CA証明書

replace:olcTLSCertificateFile
olcTLSCertificateFile: /etc/openldap/certs/server.crt ←サーバ証明書

replace:olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/openldap/certs/servername.key ←私有鍵
```

1-2. 以下コマンドにて作成したldifファイルを反映します。

```
$ldapmodify -Y EXTERNAL -H ldapi:/// -f enable-ldaps.ldif
```

1-3. 反映結果を確認します。

```
$ldapsearch -LLL -Y EXTERNAL -H ldapi:// -b cn=config
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,
cn=auth
SASL SSF: 0
dn: cn=config
objectClass: olcGlobal
cn: config
olcArgsFile: /var/run/openldap/slapd.args
olcPidFile: /var/run/openldap/slapd.pid
olcTLSCACert
olcTLSCACertificateFile: /etc/openldap/certs/nii-odca3sha2ct.cer
olcTLSCertificateFile: /etc/openldap/certs/server.crt
olcTLSCertificateKeyFile: /etc/openldap/certs/servername.key

dn: cn=schema,cn=config
objectClass: olcSchemaConfig
.
.
.
（省略）
```

2. LDAPS通信を有効化します。
2-1. LDAPサーバがldaps通信を受け入れられるよう、SLAPD_URLSにldaps通信の記載を追加します。

```
$vi /etc/sysconfig/slapd



# see 'man slapd' for additional information
#Where the server will run (-h option)

#- ldapi:/// is required for on-the-fly configuration using client tools

# (use SASL with EXTERNAL mechanism for authentication)

#- default: ldapi:/// ldap:///

#- example: ldapi:/// ldap://127.0.0.1/ ldap://10.0.0.1:1389/ ldaps:///

# SLAPD_URLS="ldapi:/// ldap:/// ldaps:///"    ←右記記載を追記



# Any custom options

#SLAPD_OPTIONS=""



#Keytab location for GSSAPI Kerberos authentication

#KRB5_KTNAME="FILE:/etc/openldap/ldap.keytab"|
```

1-7. 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/openldap/servername.key
$ cp servername.key servername.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 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

```
$cp nii-odca3sha2ct.cer nii-odca3sha2ct.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. 「1-5-2.中間CA証明書の配置」で取得した中間CA証明書を移動してください。

   SHA-2認証局 中間CA証明書の場合

```
$ mv nii-odca3sha2ct.cer /etc/openldap/certs/nii-odca3sha2ct.cer
```

6. 「1-3-1. 鍵ペアの生成」で作成した私有鍵を移動します。

```
$ mv servername.key /etc/openldap/certs/servername.key
```

7. 「1-4-1.証明書の申請から取得まで」で受け取ったサーバ証明書を移動します。

```
$mv server.crt /etc/openldap/certs/server.crt
```

1-8. 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. OpenLDAPを再起動は不要です。
2. OpenLDAPクライアント経由で、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。