NRA

Web サーバ設定ガイド

（Apache2.4.6 クライアント証明書認証編）

2020 年 11 月 06 日

Ver. 2.02

改訂履歴

版	日　付	内　容	備　考
Ver. 1.00	--	初版作成	Apache2.4 で刷新
Ver. 1.01	2017/12	失効リスト設定の追記修正	
Ver. 2.00	2019/5/24	設定例を Appendix に追記	
Ver. 2.01	2020/9/8	「server.cer」⇒「server.crt」に変更	
Ver. 2.02	2020/11/6	CA4 に対する記載を修正 Appendix5（中間認証局の確認方法）を追記	

<目　次>

1. Apache のクライアント証明書認証の設定について

Apache2.4.6 でクライアント証明書を使った認証を行う場合の設定は以下の 3 ステップで行います。

1.サーバ証明書（SSL 証明書）をインストールして、SSL 通信を有効にする
　※サーバ証明書（SSL 証明書）は別途ご用意してください
2.クライアント証明書を発行した認証局の証明書（CA 証明書）をインストールしたのち、Apache が
　クライアント証明書を要求するように設定する
3.クライアント証明書の失効リスト（CRL）を設定する

【本資料における注意事項】
中間認証局 CA4 を使用する場合は、本資料における「Nippon RA Certification Authority 3」および「CA3」という記載を「Nippon RA Certification Authority 4」および「CA4」と置き換えてください。使用する中間認証局の確認方法については、Appendix5 を参照ください。

2. SSL サーバ証明書のインストール

クライアント証明書認証を行うにあたって、まず Apache の設定にて SSL サーバ証明書をインストールし通信の暗号化（SSL 化）を有効にしている必要があります。

※SSL サーバ証明書は別途ご用意ください。

※本資料では SSL サーバ証明書は「サーバ証明書」と「中間 CA 証明書」を順番で連結して 1 つにしたファイルを想定して説明しています。「サーバ証明書」と「中間 CA 証明書」が別の場合は、以下にある【参考資料】を参照ください。

①SSL サーバ証明書と秘密鍵をサーバに保存します。

②ssl.conf にて、以下のディレクティブで設定します。

・SSL サーバ証明書の指定→SSLCertificateFile ディレクティブ

（例）

SSLCertificateFile　　"配置 PATH"/server.cer

・SSL サーバ証明書の秘密鍵の指定→SSLCertificateKeyFile ディレクティブ

（例）

SSLCertificateKeyFile　"配置 PATH"/server.key

③SSL 通信（443 ポート）の有効化します

・SSL 通信の有効化

（例）

SSLEngine on

※mod_ssl のインストール・設定は、割愛します。

※具体的な値を用いた設定は、後記の「Appendix1」をご参照ください。

④Apache 再起動

Web サーバで以下のコマンドを実行し Apache の再起動（設定のリロード）を実行します。

service httpd restart

ここまでで SSL サーバ証明書がインストールされ、SSL 通信（https）が行えるようになります。

【参考資料】

サイバートラスト・SSL サーバ証明書サポート

サーバ証明書の設定に関する資料を多数掲載しておりますので、ご参照ください。

https://www.cybertrust.ne.jp/sureserver/support/tec_download.html#01

3. クライアント証明書認証

3.1. CA 証明書の配置

日本 RA のルート証明書および中間証明書をリポジトリより取得します。
（後記 Appendix4 のルート・中間証明書で準備いただけます。）
これらの証明書は弊社のクライアント証明書の認証を行う場合に必要となります。

■NRA リポジトリ
https://www.nrapki.jp/client-certificate/repo/

・ルート証明書　　Nippon RA Root Certification Authority
・中間 CA3 証明書　　Nippon RA Certification Authority 3
・中間 CA4 証明書　　Nippon RA Certification Authority 4

※後記 Appendix4 の CA 証明書（nra.crt）は、弊社のルート証明書、中間証明書（CA3）、中間証明書（CA4）を結合して 1 ファイルとしたものです。

CA 証明書（nra.crt）はテキストファイルです。テキストエディター等で内容をご確認いただけます。
CA 証明書（nra.crt）をサーバに配置します。

3.2. CA 証明書の設定

ssl.conf に、以下のディレクティブで CA 証明書のパスを指定します。

(例)
SSLCACertificateFile　　"配置 PATH"/nra.crt

3.3. クライアント証明書要求を有効化

ssl.conf に、以下のディレクティブで設定します。

(例)

- クライアント証明書による認証を有効にする
- ロケーションが複数ある場合は以下の例のように OR で指定する
- NRA の発行局（例では CA３）、且つ条件に合致した証明書のみを受け付けるように設定する

```
<Location /仮想ディレクトリ/(パス 1|パス 2|パス 3)>
SSLVerifyClient require
SSLVerifyDepth 10
SSLRequire ( ¥
              %{SSL_CLIENT_S_DN_サブジェクト値} eq "<条件値>" ¥  ←O:の値の場合は、"SSL_CLIENT_S_DN_O"
        and (%{SSL_CLIENT_I_DN_CN} eq "Nippon RA Certification Authority 3" ¥
            )
</Location>
```

※証明書の条件は、SSL_CLIENT_S_DN_<サブジェクト値> で指定します。

サブジェクト値：C、O、OU、CN、Email などがあります。

参考 URL：https://httpd.apache.org/docs/2.4/mod/mod_ssl.html

※具体的な値を用いた設定は、後記の「Appendix2」をご参照ください。

※設定を有効にする場合は、Web サーバで「service httpd restart」コマンドを実行して Apache を再起動（設定をリロード）してください。

4. 失効リスト（CRL）の設定

4.1. CRL の取得

失効リスト（CRL）を以下の配布ポイントから取得します。
Apache の場合、配布ポイントから取得した DER 形式の失効リスト（CRL）ファイルでは読み込めないため OpenSSL コマンドにて PEM 形式に変換して、任意のディレクトリに配置します。後述のサンプルプログラム内で PEM 変換のコマンド例を記載します。

【失効リスト（CRL）の配布ポイント】

・中間認証局 CA３（Nippon RA Certification Authority 3）の失効リスト
http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3/cdp.crl

・中間認証局 CA４（Nippon RA Certification Authority 4）の失効リスト
http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4/cdp.crl

配布ポイントから取得した失効リストファイル（DER 形式）を PEM 形式に変換したものを Apache に設定する失効リスト（CRL）ファイル（crl.pem）としてください。

4.2. CRL ファイルの設定

ssl.conf にて、以下の２つのディレクティブで設定します。

（例）

```
SSLCARevocationCheck leaf
SSLCARevocationFile "配置 PATH”/crl.pem
```

※具体的な値を用いた設定は、後記の「Appendix3」をご参照ください。

4.3. CRL の自動取得＆更新

以下のサンプルスクリプトを適宜修正し、cron 等で自動実行するよう設定します。

```
#!/bin/sh
cd <<失効リストファイルダウンロードディレクトリ>>
wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl.pem
cd <<失効リストファイル配置ディレクトリ>>
rm -f crl.pem
cp -p /<<失効リストファイルダウンロードディレクトリ>>/crl.pem ./
service httpd restart
```

【補足】

中間認証局 CA4 を使用する場合は、上記スクリプト 3 行目を以下の通りにしてください。

```
wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4/cdp.crl'
```

以上

5. Appendix1（SSL サーバ証明書のインストール：具体例）

「２．SSL サーバ証明書のインストール」について、具体的な値を用いた説明は以下のとおりです。

① SSL サーバ証明書と秘密鍵を Web サーバに保存します（ここでは以下のとおりとします）。

・SSL サーバ証明書ファイル：server.cer

・SSL サーバ証明書の秘密鍵ファイル：server.key

・Web サーバでの保存先ディレクトリ：/etc/httpd/temp

② ssl.conf ファイルにて SSL 通信（443 ポート）の有効化、及び以下のディレクティブで設定します。

・SSL 通信の有効化**（A）**

・SSL サーバ証明書の指定→SSLCertificateFile ディレクティブ**（B）**

・SSL サーバ証明書の秘密鍵の指定→SSLCertificateKeyFile ディレクティブ**（C）**

■ssl.conf ファイル設定例

```
#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on                                    ―― （A）※70 行目付近

~~~~（省略）

#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/httpd/temp/server.cer   ―― （B）※100 行目付近

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/httpd/temp/server.key   ―― （C）※109 行目付近

~~~~（以下省略）
```

6. Appendix2（クライアント証明書認証：設定の具体例）

「３．クライアント証明書認証」について、具体的な値を用いた設定の説明は以下のとおりです。

① CA 証明書を取得し Web サーバに保存します（ここでは以下のとおりとします）。

- CA 証明書ファイル：nra.crt
- Web サーバでの保存先ディレクトリ：/etc/httpd/temp

② ssl.conf ファイルにて、以下のディレクティブで設定します。

- クライアント証明書による認証を有効にする（**A**）
- ロケーションが複数ある場合は以下の例のように OR で指定する（**B**）
- NRA の発行局、且つ条件に合致した証明書のみを受け付けるように設定する（**C**）

（１） NRA の発行局（CA3 で発行された証明書のみ受け付けます）

CN=Nippon RA Certification Authority 3

CA4 を使用している場合は以下の通りとなります。

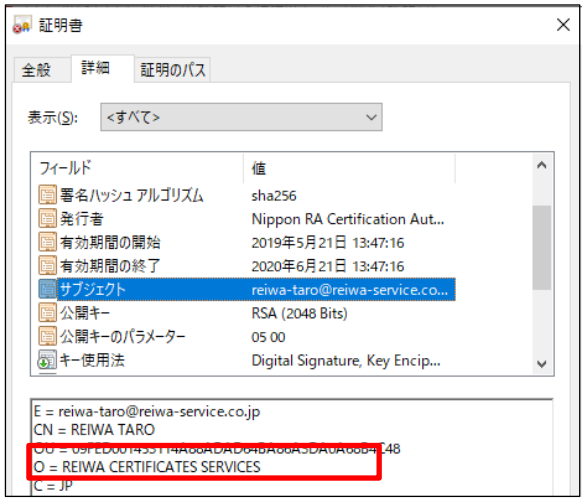
CN=Nippon RA Certification Authority 4

（２） 条件に合致した証明書（ここでは「レイワ証明書サービス」社が管理する証明書のみ受け付けます）

O=REIWA CERTIFICATES SERVICES

【補足】

これらのレコードはクライアント証明書の下図の情報になります。



■ssl.conf ファイルの設定例

```
#   Certificate Authority (CA):
#   Set the CA certificate verification path where to find CA
#   certificates for client authentication or alternatively one
#   huge file containing all of them (file must be PEM encoded)
SSLCACertificateFile /etc/httpd/temp/nra.crt
```

―― （A）※120 行目付近

```
#   Client Authentication (Type):
#   Client certificate verification type and depth.  Types are
#   none, optional, require and optional_no_ca.  Depth is a
#   number which specifies how deeply to verify the certificate
#   issuer chain before deciding the certificate is not valid.
SSLVerifyClient require
SSLVerifyDepth  10
```

―― （A）※130 行目付近

```
#   Access Control:
#   With SSLRequire you can do per-directory access control based
#   on arbitrary complex boolean expressions containing server
#   variable checks and other lookup directives.  The syntax is a
#   mixture between C and Perl.  See the mod_ssl documentation
#   for more details.
<Location />   #環境に応じて設定
SSLRequire ( ¥
        %{SSL_CLIENT_I_DN_CN} eq "Nippon RA Certification Authority 3" ¥
    and %{SSL_CLIENT_S_DN_O} eq "REIWA CERTIFICATES SERVICES" ¥
    )
</Location>

~~~~（以下省略）
```

―― （B）※140 行目付近

―― （C）

【補足】

・Location は環境に応じて設定してください。

7. Appendix3（失効リスト（CRL）の設定：具体例）

「４．　失効リスト（CRL）の設定」について、具体的な値を用いた設定の説明は以下のとおりです。

① 配布ポイントから取得した DER 形式の失効リストを PEM 形式に変換しマージしたファイルを Web サーバに保存します（ここでは以下のとおりとします）。

・失効リストファイル：crl.pem

・Web サーバでの保存先ディレクトリ：/etc/httpd/temp

② ssl.conf ファイルにて以下のディレクティブで設定します。

■ssl.conf ファイルの設定例

```
#    Access Control:
#    With SSLRequire you can do per-directory access control based
#    on arbitrary complex boolean expressions containing server
#    variable checks and other lookup directives.  The syntax is a
#    mixture between C and Perl.  See the mod_ssl documentation
#    for more details.
<Location />   #環境に応じて設定
SSLRequire ( ¥
          %{SSL_CLIENT_I_DN_CN} eq "Nippon RA Certification Authority 3" ¥
     and %{SSL_CLIENT_S_DN_O} eq "REIWA CERTIFICATES SERVICES" ¥
     )
</Location>

SSLCARevocationCheck leaf
SSLCARevocationFile /etc/httpd/temp/crl.pem

~~~~（以下省略）
```

【補足】

・「SSLCARevocationCheck」「SSLCARevocationFile」設定は、デフォルトの ssl.conf ファイルには用意されておりませんので、クライアント証明書認証設定に続けて記載ください。

・SSLCARevocationCheck には「leaf」を設定ください。

③ 配布ポイントの失効リストは適宜更新されますので、以下のとおりスクリプトを作成し Web サーバの失効リスト（crl.pem）も cron 等で定期的に自動取得＆更新するように設定します。

■スクリプト例

```
#!/bin/sh
cd /etc/httpd/temp/download
wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl.pem
cd /etc/httpd/temp
rm -f crl.pem
cp -p /etc/httpd/temp/download/crl.pem ./
service httpd restart
```

【補足】

・/etc/httpd/temp/download は、配布ポイントの失効リストファイルをダウンロードするディレクトリになります。スクリプトを実行する前にあらかじめ作成ください。

8. Appendix4（PEM 形式のルート・中間証明書）

以下、リポジトリで公開するルート・中間証明書を PEM 形式にした内容です。

※上段がルート、中段が中間（CA3）、下段が中間（CA4）の証明書の内容となります。

ルートと許可する証明書の発行局のみ中間証明書として設定ください。

テキストファイルへコピー＆ペーストし、本手順を例に、”nra.crt”というファイル名で、

"配置 PATH”/nra.crt に配置します。

ルート証明書

```
-----BEGIN CERTIFICATE-----
MIIDazCCAlOgAwIBAgIBATANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluY4xLzAtBgNVBAMTJk5pcHBvbiBSQSBSb29O
IENlcnRpZmljYXRpb24gQXVOaG9yaXR5MB4XDTExMDgxNTAyMzAyNloXDTMxMDgx
NTAyMjg1NlowVzELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJbmMu
MS8wLQYDVQQDEyZOaXBwb24gUkEgUm9vdCBDZXJOaWZpY2F0aW9uIEF1dGhvcmlO
eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPRqqsUWzgB38ZMi7aeT
ThqijKzqBaNOUWL9Czhb30b/Li5KEQrAz2PegOwZns6b+F/4QE2H2gl9k4qBe8dh
Arlns9tSIH6N6/rDg625rCGKj9cAiOizis2gyTptmcgMffENQI6dcDxviuCY98dG
8ITMWxKucza/rCVt5KBC5Uh17AgPA1j5vPgXnDn9vnwVO4sYqoXXa7ZRgYFc+g/h
pM/lqWFze1gtGLBvEnYIgyd3cbVEOmMwc15NNaCcSFJbr2p/P/KA9xEmot768M5f
5NTlW/Cg6LJ/bm/byu8H2jhjpQEdY35rDSOip2OmqEJy51nWbUMqMV2SesPouVjv
x5UCAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAcYwHQYD
VR0OBBYEFBmZpk3iL3keWO5k2YDn98mwn3IOMAOGCSqGSIb3DQEBCwUAA4IBAQCX
Meqx614XO8HFK/XWmzBmrXbU1OXGigNK5CCmVXVM5tdVGSySW8br9c+ZUGRcq4cd
6cUA/4pIUlLTqUb5TOwO8+pw+egehYWeeVqoF7T5EWLps2HBv8+LolPnXY/Btp88
teacC1QS5tiSbfuR3UDuCfGWtAUdmyG5jH6Ose9k/k+zLCvChOhXGaQXAeOAnEIM
n+oKqSQeSTbo7+7KxiqtjyZ2WerBqPgAFpJNu+PCpG1rXaPU87//PKqP9lYqkO5h
VGMOs8QNnWXVbVTOeJV79Ef5ZfbtWS8x2OJYRALzbLKtu9wuFdlocL5dWeVL6QxS
uWKlNqU/oyG9yDKuoG5l
-----END CERTIFICATE-----
```

中間（CA3）証明書

```
-----BEGIN CERTIFICATE-----
MIID7TCCAtWgAwIBAgIBITANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluY4xLzAtBgNVBAMTJk5pcHBvbiBSQSBSb29O
IENlcnRpZmljYXRpb24gQXVOaG9yaXR5MB4XDTEOMDcxNzA3MTI1NVoXDTMxMDgx
NTAyMjg1NlowVDELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJbmMu
MSwwKgYDVQQDEyNOaXBwb24gUkEgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgMzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIyaWX8RUMgPmjUFOtO8GkxR
Xt/kEoaUHt81dPO1r4nLth6LKcBQ8ao6CajTv7un5OkZ+olOMeLRVvamXqrgCbZw
PMO91e9Dpkdl2Ojdwm4OPEUgLQeb/4hfQyQaSIN/VtnMvyRtjSdZhNigyaKYRiKS
2lOCTbdn3hpWIHgot5rD5sh5wJ96EHmeTaIOOp8BAlmaejEantMR3KhZZfhxC2kK
a2LIRtsXCHRXB15shFD8yMiS5KBlXEkpKAKyp8Zat8fgm58d1UXdLotRC91biH5W
96JL22fnbuz3WsFoaQMjdLDa9Q9fC7GewSF3OaYljPkcEXkAQcw36mjRmaQUFxUC
AwEAAaOBxjCBwzAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBxjAfBgNV
HSMEGDAWgBQZmaZN4i95HltOZNmA5/fJsJ9yDjBgBgNVHR8EWTBXMFWgU6BRhk9o
dHRwOi8vbXBraWNybC5tYW5hZ2VkcGtpLm5lLmpwL21wa2kvTmlwcG9uUkFSb29O
Q2VydGlmaWNhdGlvbkF1dGhvcmlOeS9jZHAuY3JsMBOGA1UdDgQWBBRbOO113m4V
nZU8OO/XPyhMvhBfgDANBgkqhkiG9w0BAQsFAAOCAQEAqpAvO3zpxGAF5R7pZtde
k3eHH1JVnhr+gWHty2OjGBmr2RBzWpBu1tXWZjKilaPjU14mMD5L/rA/OtwnTk7x
ep+bFEHdJzJ+bcTf/LOFETRfu/i9ctKQiDRqrp15nuJDyg8/+j/EaawiOY3bs6qj
q/r7MNfQGDghg6dMIlzOmETLVjisSfDI1EPQOwfxV2TvfQDNaE39OVqSb4GOYfuP
Pyb44omkQmbQOemlZDF5YkmncVHE4dI/stVeue8YArnO6BYvhRpHveIBtkG8phWD
th6MVyMzsnn4FCEtmRN687uukbfsnQ/mlmEpzPXDEYIAvxrH4u3zUccQRhhiq5ub
3A==
-----END CERTIFICATE-----
```

中間（CA4）証明書

```
-----BEGIN CERTIFICATE-----
MIID7TCCAtWgAwIBAgIBIjANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluY4xLzAtBgNVBAMTJk5pcHBvbiBSQSBSb29O
IENlcnRpZmljYXRpb24gQXVOaG9yaXR5MB4XDTEOMDcxNzA3MTgzM1oXDTMxMDgx
NTAyMjg1NlowVDELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJbmMu
MSwwKgYDVQQDEyNOaXBwb24gUkEgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgNDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALNvx9mQLWZdSvJf/8PmGW3A
178UL2MHWqFbiIJCaZ5oVXSPG//6PO+dCpjD/Hm3/9KpxqICc7l6HdHsZXSKbCFi
kHlJhqZ+jQL5q511z8bAbtQff2VyMSNQeOtzLayxdCMfckxMYjS2nsX84stQ3mEC
5E2Cf+ovZM96RpTEAjrOb2DcOuUxnZCVgJiy1OoryrICMVfNnfTpFmkuATXRmeko
yx9DVMi9fegGYwFhfl+zNFSBAKuBBsqf9l4yfk9CBouGfOOiQrF/DkrpoLmEPS1b
tbcB7agTkaeSKTbqCXZj9AMDFMaNYzun24KHXhJUbt2efJRbLHYmAPZC7pnAE3MC
AwEAAaOBxjCBwzAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBxjAfBgNV
HSMEGDAWgBQZmaZN4i95HltOZNmA5/fJsJ9yDjBgBgNVHR8EWTBXMFWgU6BRhk9o
dHRwOi8vbXBraWNybC5tYW5hZ2VkcGtpLm5lLmpwL21wa2kvTmlwcG9uUkFSb29O
Q2VydGlmaWNhdGlvbkF1dGhvcmlOeS9jZHAuY3JsMBOGA1UdDgQWBBSeu4RjR78m
fX37XfMNpsxb2ay3qzANBgkqhkiG9w0BAQsFAAOCAQEAjc80OeZsNeLg5cZIO56R
CgXVGe1+XwadaRfodzsQBFDNYD+y5iTpndw45XGsuH2rHSdWZuCluju9YPqGKnHr
oae5uxTutw8MrIKKcERHIac4SpqsEWEHRHBgnqpnV/45FJqxhEVOanyxQlEEmeXW
cPdZOXlWLhWcxOVPC8OxaoDw/VF/P+9SYioENvY1Oix8VEKb7yui9SALdIx1VmZg
mMHxUDZixsEs4CLL+NXlSIg+KSI3Wqd6FFIep3UOEAm8cNC4FQoO9M6WSp8moL4R
zahrIvBCWCAc4SflBggLDAbf4eXc49UQ5xjLKH3iRDSiMNOVpbt6PtY/WTVK7UYU
Mw==
-----END CERTIFICATE-----
```

【注意事項】

上記データをコピー＆ペーストしたとき改行が入らない場合があります。その時は PDF 資料を別のエディタ（Adobe 等）でオープンしてコピー＆ペーストしてください（改行が入らないと CA 証明書が Apache

に正しく認識されません)。

9. Appendix5（中間認証局の確認方法）

下図の NRA-PKI システム管理画面にて、[利用者メンテナンス]をクリックしていただくと、適用されているサービス名が表示されます。サービス名の後に**（CA4）**という表記があれば CA4、なければ CA3 をご利用いただいております。

以上