マルチトラスト設定ガイド

（nginx1.20.0 編）

2024 年 09 月 24 日

Ver. 1.10

改訂履歴

版	日　付	内　容	備　考
Ver. 1.00	--	初版作成	
Ver. 1.10	2024/09/24	CA3G2 の失効リスト配布ポイントの変更	

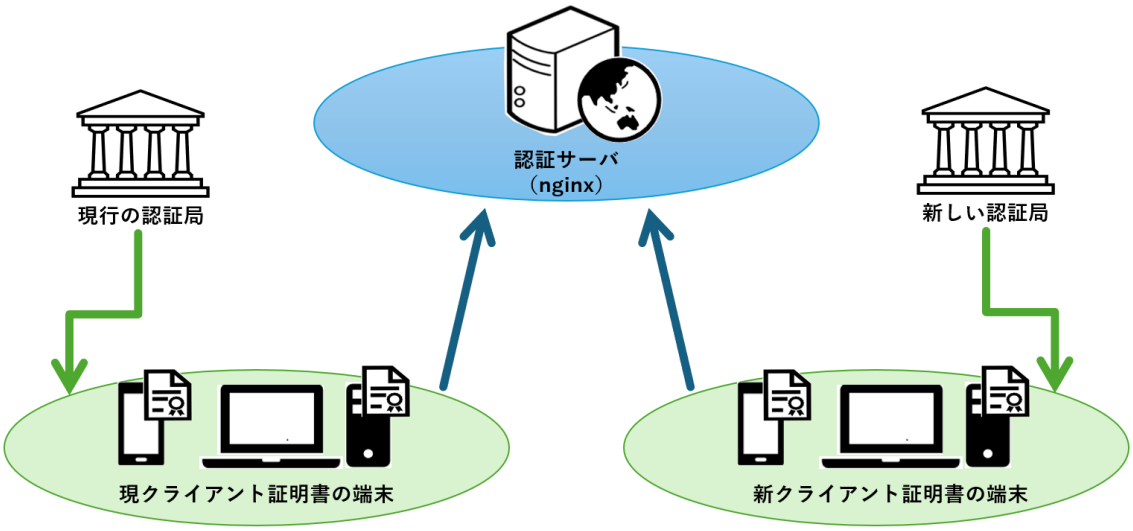
<目　次>

1. 概要

1.1. はじめに

本書は、NRA-PKI クライアント証明書の認証局（表 1）の世代交代（※1）に伴い、現行の認証局から発行したクライアント証明書と、新しい認証局から発行したクライアント証明書の両方を従来と同様にご利用頂くための nginx におけるマルチトラスト設定の手順を記載したものです。

【構成図】



【表 1 NRA-PKI の認証局】

	現行の認証局	新しい認証局
ルート認証局	Nippon RA Root Certification Authority	Nippon RA Root Certification Authority G2
中間認証局CA3	Nippon RA Certification Authority 3	Nippon RA Certification Authority 3 G2
中間認証局CA4	Nippon RA Certification Authority 4	Nippon RA Certification Authority 4 G2
中間認証局CA5	Nippon RA Certification Authority 5	Nippon RA Certification Authority 5 G2

※1 現行のルート認証局および中間認証局の有効期限により新しい認証局への移行

1.2. 本書における注意事項

本書は既存のクライアント証明書認証に追加して、新しい認証局のクライアント証明書を認証する設定手順を記載しております。
詳しいクライアント証明書認証の設定手順については、Web サーバ設定ガイドをご参照ください。

また、中間認証局 CA3 以外をご利用の場合は、本書における「Nippon RA Certification Authority 3」および「CA3」という記載をご利用の中間認証局に置き換えてください。
ご利用の中間認証局の確認方法については、後記の Appendix1 をご参照ください。

2. マルチトラストの設定手順

nginx における認証局世代交代に伴うマルチトラスト設定は以下の手順で行います。

2.1. 認証局証明書の設定変更

新しい認証局の証明書をインストールし、既存の CA 証明書に追加します。

2.2. 失効リスト（CRL）の設定変更

新しい認証局から発行されるクライアント証明書の失効リスト（CRL）を設定します。

2.3. 失効リスト（CRL） の自動取得&更新

cron を使用して失効リストの自動取得と更新を行うスクリプトを作成します。

2.4. クライアント証明書認証の設定変更

クライアント認証で許可する条件を設定します。

2.1. 認証局証明書の設定変更

クライアント証明書を発行した認証局を指定するファイルに、新しい認証局の証明書を追加登録します。

(1) 新しい認証局のルート証明書および中間証明書を取得してください。

ルート認証局 G2 の証明書とご利用の中間認証局の証明書を以下の URL よりダウンロードしてください。

ご利用の中間認証局の確認方法については、Appendix1 をご参照ください。

【新しい認証局の証明書】

■ルート認証局 G２（Nippon RA Root Certification Authority G2）

https://www.nrapki.jp/nrawp/cert/NipponRARootCertificationAuthorityG2.crt

■中間認証局 CA３ G２（Nippon RA Certification Authority 3 G2）

https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority3G2.crt

■中間認証局 CA４ G２（Nippon RA Certification Authority 4 G2）

https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority4G2.crt

■中間認証局 CA５ G２（Nippon RA Certification Authority 5 G2）

https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority5G2.crt

(2) 新しい認証局のルート証明書および中間証明書を追加します。

nginx.conf ファイルの server セクション「ssl_client_certificate」で指定しているファイルに、新しい認証局の証明書（PEM 形式）の記載を追加します。

■nginx.conf ファイルの設定例

ssl_client_certificate “配置 PATH”/nra.crt

■複数認証局の証明書の記述例

```
-----BEGIN CERTIFICATE-----
MIIDazCCAlOgAwIBAgIBATANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluYy4xLzAtBgNVBAMTJk5pcHBvbiBSQSBSb290
IENIcnRpZmljYXRpb24gQXVOaG9yaXR5MB4XDTExMDgxNTAyMzAyNloXDTMxMDgx
NTAyMjg1NlowVzELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJbmMu
MS8wLQYDVQQDEyZOaXBwb24gUkEgUm9vdCBDZXJOaWZpY2FOaW9uIEF1dGhvcml0
eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPRqqsUWzgB38ZMi7aeT
ThqijKzqBaNOUWL9Czhb3Ob/Li5KEQrAz2PegOwZns6b+F/4QE2H2gl9k4qBe8dh
Arlns9tSIH6N6/rDg625rCGKj9cAiOizis2gyTptmcgMffENQI6dcDxviuCY98dG
8ITMWxKucza/rCVt5KBC5Uh17AgPA1j5vPgXnDn9vnwVO4sYqoXXa7ZRgYFc+g/h
pM/lqWFze1gtGLBvEnYIgyd3cbVEOmMwc15NNaCcSFJbr2p/P/KA9xEmot768M5f
5NTlW/Cg6LJ/bm/byu8H2jhjpQEdY35rDSOip2OmqEJy51nWbUMqMV2SesPouVjv
x5UCAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAcYwHQYD
VR0OBBYEFBmZpk3iL3keWO5k2YDn98mwn3IOMAOGCSqGSIb3DQEBCwUAA4IBAQCX
Meqx614XO8HFK/XWmzBmnXbU1OXGigNK5CCmVXVM5tdVGSySW8br9c+ZUGRcq4cd
6cUA/4pIUlLTqUb5TOwO8+pw+egehYWeeVqoF7T5EWLps2HBv8+LolPnXY/Btp88
teacCIQS5tiSbfuR3UDuCfGWtAUdmyG5jH6Ose9k/k+zLCvChOhXGaQXAeOAnEIM
n+oKqSQeSTbo7+7KxiqtjyZ2WerBqPgAFpJNu+PCpG1rXaPU87//PKqP9lYqkO5h
VGMOs8QNnWXVbVTOeJV79Ef5ZfbtWS8x2OJYRALzbLKtu9wuFdlocL5dWeVL6QxS
uWKlNqU/oyG9yDKuoG5l
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID7TCCAtWgAwIBAgIBITANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluYy4xLzAtBgNVBAMTJk5pcHBvbiBSQSBSb290
IENIcnRpZmljYXRpb24gQXVOaG9yaXR5MB4XDTEOMDcxNzA3MTI1NVoXDTMxMDgx
NTAyMjg1NlowVDELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJbmMu
MSwwKgYDVQQDEyNOaXBwb24gUkEgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgMzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIyaWX8RUMgPmjUFOtO8GkxR
Xt/kEoaUHt81dPO1r4nLth6LKcBQ8ao6CajTv7un5OkZ+olOMeLRVvamXqrgCbZw
PMO91e9Dpkdl2Ojdwm4OPEUgLQeb/4hfQyQaSIN/VtnMvyRtjSdZhNigyaKYRiKS
2lOCTbdn3hpWIHgot5rD5sh5wJ96EHmeTaIOOp8BAlmaejEantMR3KhZZfhxC2kK
a2LIRtsXCHRXB15shFD8yMiS5KBlXEkpKAKyp8Zat8fgm58d1UXdLotRC91biH5W
96JL22fnbuz3WsFoaQMjdLDa9Q9fC7GewSF3OaYljPkcEXkAQcw36mjRmaQUFxUC
AwEAAaOBxjCBwzAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBxjAfBgNV
HSMEGDAWgBQZmaZN4i95HltOZNmA5/fJsJ9yDjBgBgNVHR8EWTBXMFWgU6BRhk9o
dHRwOi8vbXBraWNybC5tYW5hZ2VkcGtpLm5lLmpwL21wa2kvTmlwcG9uUkFSb290
Q2VydGlmaWNhdGlvbkF1dGhvcmlOeS9jZHAuY3JsMBOGA1UdDgQWBBRbOO113m4V
nZU8OO/XPyhMvhBfgDANBgkqhkiG9w0BAQsFAAOCAQEAqpAvO3zpxGAF5R7pZtde
k3eHH1JVnhr+gWHty2OjGBmr2RBzWpBu1tXWZjKilaPjU14mMD5L/rA/OtwnTk7x
ep+bFEHdJzJ+bcTf/LOFETRfu/i9ctKQiDRqrpI5nuJDyg8/+j/EaawiOY3bs6qj
q/r7MNfQGDghg6dMIlzOmETLVjisSfDI1EPQOwfxV2TvfQDNaE39OVqSb4GOYfuP
Pyb44omkQmbQOemlZDF5YkmncVHE4dI/stVeue8YArnO6BYvhRpHveIBtkG8phWD
th6MVyMzsnn4FCEtmRN687uukbfsnQ/mlmEpzPXDEYlAvxrH4u3zUccQRhhiq5ub
3A==
-----END CERTIFICATE-----
```

新しい認証局の証明書の PEM 形式を追加します。

後記の Appendix2 で弊社のルートおよび中間証明書を PEM 形式でマージした内容を記載しております。

2.2. 失効リスト（CRL）の設定変更

新しい認証局の失効リストは、現行の認証局の失効リストとは別となる為、失効リスト参照の追加設定が必要となります。クライアント証明書を発行した認証局の失効リストを指定するファイルに、新しい認証局の失効リストを追加登録します。

なお、失効リストの参照設定を行っていない場合は、本設定は必要ありません。

(1) 新しい認証局の失効リスト（CRL）を取得してください。

以下の配布ポイントからルート認証局 G2 とご利用の中間認証局の失効リストをダウンロードします。

【新しい認証局の失効リスト（CRL）の配布ポイント】

■ルート認証局 G２（Nippon RA Root Certification Authority G2）の失効リスト
http://mpkicrl.managedpki.ne.jp/mpki/NipponRARootCertificationAuthorityG2/cdp.crl

■中間認証局 CA３ G２（Nippon RA Certification Authority 3 G2）の失効リスト
http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3G2/cdp.crl

■中間認証局 CA４ G２（Nippon RA Certification Authority 4 G2）の失効リスト
http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4G2/cdp.crl

■中間認証局 CA５ G２（Nippon RA Certification Authority ５ G2）の失効リスト
http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority5G2/cdp.crl

(2) 新しい認証局の失効リスト（CRL）を追加します。

nginx.conf ファイルの server セクション「ssl_crl」で指定しているファイルに、新しい認証局の失効リスト（PEM 形式）の記載を追加します。

nginx 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 形式に変換してください。後記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。

■nginx.conf ファイルの設定例

ssl_crl "配置 PATH"/crl.pem

■複数 CRL の記述例

```
-----BEGIN X509 CRL-----
MIIE5jCCA84CAQEwDQYJKoZIhvcNAQELBQAwVDELMAkGA1UEBhMCSlAxFzAVBgNV
BAoTDk5pcHBvbiBSQSBJbmMuMSwwKgYDVQQDEyNOaXBwb24gUkEgQ2VydGlmaWNh
dGlvbiBBdXRob3JpdHkgNRcNMjQwNDIyMDA1MTM0WhcNMjQwNDI5MDA1MTM0WjCC
AqowPAIDHoW3FwOyMjA2MDkwNDI2MjdaMCYwGAYDVR0YBBEYDzIwMjIwNjA5MDQy
NjAwWjAKBgNVHRUEAwoBBTA8AgMehhMXDTIyMDYwOTA0NTY0M1owJjAYBgNVHRgE
ERgPMjAyMjA2MDkwNDU2MDBaMAoGA1UdFQQDCgEFMDwCAx6GexcNMjIwNjEwMDcw
OTQ5WjAmMBgGA1UdGAQRGA8yMDIyMDYxMDA3MDkwMFowCgYDVR0VBAMKAQUwPAID
HobbFwOyMjA2MTQwMzU3MDNaMCYwGAYDVR0YBBEYDzIwMjIwNjEOMDM1NzAwWjAK
BgNVHRUEAwoBBTA8AgMehhUXDTIyMDYwOTA1NTQ0N1owJjAYBgNVHRgEERgPMjAy
MjA2MDkwNTUOMDBaMAoGA1UdFQQDCgEFMDwCAx6GFhcNMjIwNjEwMDcwNDI5WjAm
MBgGA1UdGAQRGA8yMDIyMDYxMDA3MDQwMFowCgYDVR0VBAMKAQUwPAIDHoaAFwOy
MjA2MTMwMTQyNTlaMCYwGAYDVR0YBBEYDzIwMjIwNjEzMDE0MjAwWjAKBgNVHRUE
AwoBBTA8AgMehbgXDTIyMDYwOTA0MjgOOVowJjAYBgNVHRgEERgPMjAyMjA2MDkw
NDI4MDBaMAoGA1UdFQQDCgEFMDwCAx6GfhcNMjIwNjEzMDE0MTU1WjAmMBgGA1Ud
GAQRGA8yMDIyMDYxMzAxNDEwMFowCgYDVR0VBAMKAQUwPAIDHoYUFwOyMjA2MDkw
NTAxMzVaMCYwGAYDVR0YBBEYDzIwMjIwNjA5MDUwMTAwWjAKBgNVHRUEAwoBBTA8
AgMehn0XDTIyMDYxMzAxMzMwOVowJjAYBgNVHRgEERgPMjAyMjA2MTMwMTMzMDBa
MAoGA1UdFQQDCgEFoIGXMIGUMB8GA1UdIwQYMBaAFLndgfenx88LZvRcK3T6PzcS
INUaMAwGA1UdFAQFAgMAxdAwYwYDVR0cAQH/BFkwV6BSoFCGTmh0dHA6Ly9tcGtp
Y3JsLm1hbmFnZWRwa2kubmUuanAvbXBraS9oaXBwb25SQUNlcnRpZmljYXRpb25B
dXRob3JpdHk1L2NkcDAyLmNybIEB/zANBgkqhkiG9w0BAQsFAAOCAQEAeo1yscNh
gFOqk7OSQZf9iRAaWxtQb7xGYc4oXOrVi5hakxWMbe/luilbhXvjsykfLrwlJxz1
y7MG4XTYeqK8BOXH7SS4+OMEaoC2b5MFVL4zVKRk+yxlloCc2fK1837JSmJhv1qM
tk4Kl/EfdlRWJwZog6fyQCVIStUN7Gk966Gbg1bXTKrrLbzWFpY2UlqSsncmmCT+
yOC1JNOnMGwgJS6WnIA3r7OLP2bDY8/Ma6TVwv8lU5zzVRp66OKJiGWBVeKC4YkM
1H4lcpgUpLEfwEEem5/O9xPOzY7jlDMK10bMqau2hREcrSfEsjXlha5JBSVl+/x2
LL3lROBXTwUByw==
-----END X509 CRL-----
-----BEGIN X509 CRL-----
MIICtjCCAZ4CAQEwDQYJKoZIhvcNAQELBQAwVDELMAkGA1UEBhMCSlAxFzAVBgNV
BAoTDk5pcHBvbiBSQSBJbmMuMSwwKgYDVQQDEyNOaXBwb24gUkEgQ2VydGlmaWNh
dGlvbiBBdXRob3JpdHkgNRcNMjQwNDIyMDAzMTI0WhcNMjQwNDI5MDAzMTI0WjB8
MDwCAx9gPRcNMjMwMTA1MDg1NjA5WjAmMBgGA1UdGAQRGA8yMDIzMDEwNTA4NTYw
MFowCgYDVR0VBAMKAQUwPAIDH2A7FwOyMzAxMTAwNTM4MzNaMCYwGAYDVR0YBBEY
DzIwMjMwMTEwMDUzODAwWjAKBgNVHRUEAwoBBaCBlzCBlDAfBgNVHSMEGDAWgBS5
3YH3p8fPC2bOXCtO+j83EpTVGjAMBgNVHRQEBQIDAMXPMGMGA1UdHAEB/wRZMFeg
UqBQhk5odHRwOi8vbXBraWNybC5tYW5hZ2VkcGtpLm5lLmpwL21wa2kvTmlwcG9u
UkFDZXJOaWZpY2FOaW9uQXVOaG9yaXR5NS9jZHAwNC5jcmyBAf8wDQYJKoZIhvcN
AQELBQADggEBAHbmVWqK7z5dVJPbFVjpLRCD8+jipYzbPliFiN4NjBRfWsGw1Qkb
y6jVZgo/dYChFrj5SxYFS92zCPb5LifFYG9i4rXeUJeVSwgoOLu1UofJ5tlEJAbj
aEibcWHpF2aaz8auzxxhkuuwuu4QVEQ4JD1k9kaLuMp+JNHTOaYHKASigD/vRENo
HfHAca8uSiJaS+TS7oPOsjFtbc/F2X+FUhxCbp7Ey39e0Qg273YZDjksh2+fqYOo
mEQFLtXkX1gLQfcbSKw7qfsJsQsfqei8G6t8O4ja5Xcq6VZ9+eEsGOSWDibdHUlO
RFCGBGuUASMc4Cu9sTQEGaoQakD2FaP3PS8=
-----END X509 CRL-----
```

新しい認証局の失効リストの PEM 形式を追加します。

2.3. 失効リスト（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。

■サンプルスクリプト

配布ポイントから取得した DER 形式の失効リスト（CRL）を PEM 形式に変換し、現認証局の失効リストと新認証局の失効リストをマージしたファイルを作成し、任意のディレクトリに配置します。

```
#!/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/NipponRARootCertificationAuthority/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl_root.pem
rm -f cdp.crl

wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl_ca3.pem
rm -f cdp.crl

wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRARootCertificationAuthorityG2/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl_rootG2.pem
rm -f cdp.crl

wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3G2/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl_ca3G2.pem
rm -f cdp.crl

cat crl_root.pem crl_ca3.pem crl_rootG2.pem crl_ca3G2.pem > 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 ./
systemctl reload nginx
```

【補足】

具体的な値を用いた設定は、後記の Appendix3 をご参照ください。

2.4. クライアント証明書認証の設定変更

クライアント認証において、新しい認証局の証明書を許可する条件の設定手順を以下に記載します。なお、クライアント認証の条件に発行局（認証局）を指定していない場合は、本設定は必要ありません。

(1) nginx.conf ファイルの server セクションを確認します。

■nginx.conf ファイルの設定例（変更前）

・発行局が CA3

且つ、クライアント証明書の「O」の値が合致した証明書のみを受け付ける設定

```
server {
listen          443 ssl;

      ～省略（ホスト名、SSL サーバ証明書 等のディレクティブ）～

ssl_verify_client on;
ssl_client_certificate 配置 PATH/nra.crt;
ssl_verify_depth 3;

<Location>

if ($ssl_client_i_dn !~ "CN=Nippon RA Certification Authority 3") {
            return 403;
        }
        if ($ssl_client_s_dn !~ "O="<条件値>" ") {
            return 403;
            }
</Location>
            ~~~~（以下省略）
  }
```

(2) 新しい認証局の証明書を許可する条件に変更します。

現発行局（CA3）または新発行局（CA3 G2）を受け付けるよう OR で指定します。

■nginx.conf ファイルの設定例（変更後）

・発行局が CA3 または CA3 G2

且つ、クライアント証明書の「O」の値が合致した証明書のみを受け付ける設定

```
server {
listen          443 ssl;

      ～省略（ホスト名、SSL サーバ証明書 等のディレクティブ）～

ssl_verify_client on;
ssl_client_certificate 配置 PATH/nra.crt;
ssl_verify_depth 3;

<Location>

if ($ssl_client_i_dn !~ "CN=(Nippon RA Certification Authority 3|Nippon RA Certification Authority 3 G2)"){
                return 403;
        }
        if ($ssl_client_s_dn !~ "O="<条件値>" ") {
            return 403;
            }
</Location>
            ~~~~（以下省略）
  }
```

※設定を有効にする場合は、「systemctl reload nginx」コマンドを実行して nginx を再起動（設定をリロード）してください。

具体的な値を用いた設定は、後記の Appendix4 をご参照ください。

3. Appendix1（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。サービス名の後の（CA4）等の表記がご利用いただいている中間認証局です。表記がなければ CA3 をご利用いただいております。

4. Appendix2（PEM 形式のルート・中間証明書）

弊社のレポジトリで公開しているルートおよび中間証明書を PEM 形式にした内容です。
既存の CA 証明書（現行のルート証明書と中間証明書）に新ルート証明書と新中間証明書を追加しております。

(1) 下記の内容をテキストファイルへコピー＆ペーストし、CA 証明書を作成し配置します。（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/nginx/temp

■nginx.conf ファイルの設定例

```
ssl_client_certificate /etc/nginx/temp/nra.crt
```

【注意事項】
下記の内容をコピー＆ペーストした際に改行が入らない場合があります。その際は 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 nginx に正しく認識されません）。

【レポジトリ】

■新認証局レポジトリ
https://www.nrapki.jp/client-certificate/repository/

■現認証局レポジトリ
https://www.nrapki.jp/client-certificate/repo/

■中間認証局 CA3 をご利用の場合

（現行のルート証明書、中間証明書（CA3）と新しいルート証明書（G2）、中間証明書（CA3 G2）をマージしたものです）。

```
-----BEGIN CERTIFICATE-----
MIIDazCCAlOgAwIBAgIBATANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluYy4xLzAtBgNVBAMTJk5pcHBvbiBSQSBSb290
IENlcnRpZmljYXRpb24gQXVoaG9yaXR5MB4XDTExMDgxNTAyMzAyNloXDTMxMDgx
NTAyMjg1NlowVzELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJbmMu
MS8wLQYDVQQDEyZOaXBwb24gUkEgUm9vdCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0
eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPRqqsUWzgB38ZMi7aeT
ThqijKzqBaNOUWL9Czhb3Ob/Li5KEQrAz2Peg0wZns6b+F/4QE2H2gl9k4qBe8dh
Arlns9tSIH6N6/rDg625rCGKj9cAiOizisZgyTptmcgMffENQI6dcDxviuCY98dG
8lTMWxKucza/rCVt5KBC5Uh17AgPAIj5vPgXnDn9vnwVO4sYqoXXa7ZRgYFc+g/h
pM/lqWFzeIgtGLBvEnYIgyd3cbVEOmMwc15NNaCcSFJbr2p/P/KA9xEmot768M5f
5NTlW/Cg6LJ/bm/byu8H2jhjpQEdY35rDSOip2OmqEJy51nWbUMqMV2SesPouVjv
x5UCAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAcYwHQYD
VR0OBBYEFBmZpk3iL3keWO5k2YDn98mwn3IOMAOGCSqGSIb3DQEBCwUAA4IBAQCX
Meqx614XO8HFK/XWmzBmnXbU1OXGigNK5CmVXVM5tdVGSySW8br9c+ZUGRcq4cd
6cUA/4pIUlLTqUb5TOwO8+pw+egehYWeeVqoF7T5EWLps2HBv8+LolPnXY/Btp88
teacCIQS5tiSbfuR3UDuCfGWtAUdmyG5jH6Ose9k/k+zLCvChOhXGaQXAe0AnEIM
n+oKqSQeSTbo7+7KxiqtjyZ2WerBqPgAFpJNu+PCpG1rXaPU87//PKqP9lYqkO5h
VGMOs8QNnWXVbVTOeJV79Ef5ZfbtWS8x2OJYRALzbLKtu9wuFdlocL5dWeVL6QxS
uWKlNqU/oyG9yDKuoG5l
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID7TCCAtWgAwIBAgIBITANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluYy4xLzAtBgNVBAMTJk5pcHBvbiBSQSBSb290
IENlcnRpZmljYXRpb24gQXVoaG9yaXR5MB4XDTE0MDcxNzA3MTl1NVoXDTMxMDgx
NTAyMjg1NlowVDELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJbmMu
MSwwKgYDVQQDEyNOaXBwb24gUkEgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgMzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIyaWX8RUMgPmjUFOtO8GkxR
Xt/kEoaUHt81dPO1r4nLth6LKcBQ8ao6CajTv7un5OkZ+olOMeLRVvamXqrgCbZw
PMO91e9Dpkdl2Ojdwm4OPEUgLQeb/4hfQyQaSIN/VtnMvyRtjSdZhNigyaKYRiKS
2lOCTbdn3hpWIHgot5rD5sh5wJ96EHmeTalOOp8BAlmaejEantMR3KhZZfhxC2kK
a2LIRtsXCHRXB15shFD8yMiS5KBlXEkpKAKyp8Zat8fgm58d1UXdLotRC91biH5W
96JL22fnbuz3WsFoaQMjdLDa9Q9fC7GewSF3OaYlpKcEXkAQcw36mjRmaQUFxUC
AwEAAaOBxjCBwzAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBxjAfBgNV
HSMEGDAWgBQZmaZN4i95HItOZNmA5/fJsJ9yDjBgBgNVHR8EWTBXMFWgU6BRhk9o
dHRwOi8vbXBraWNybC5tYW5hZ2VkcGtpLm5lLmpwL21wa2kvTmlwcG9uUkFSb290
Q2VydGlmaWNhdGlvbkF1dGhvcml0eS9jZHAuY3JsMBOGA1UdDgQWBBRbOO113m4V
nZU8OO/XPyhMvhBfgDANBgkqhkiG9w0BAQsFAAOCAQEAqpAvO3zpxGAF5R7pZtde
k3eHH1JVnhr+gWHty2OjGBmr2RBzWpBu1tXWZjKiIaPjU14mMD5L/rA/OtwnTk7x
ep+bFEHdJzJ+bcTf/LOFETRfu/i9ctKQiDRqrpI5nuJDyg8/+j/EaawiOY3bs6qj
q/r7MNfQGDghg6dMIlzOmETLVjisSfDI1EPQOwfxV2TvfQDNaE390VqSb4GOYfuP
Pyb44omkQmbQOemlZDF5YkmncVHE4dl/stVeue8YArnO6BYvhRpHvelBtkG8phWD
th6MVyMzsnn4FCEtmRN687uukbfsnQ/mlmEpzPXDEYlAvxrH4u3zUccQRhhiq5ub
3A==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFcTCCA1mgAwIBAgIBATANBgkqhkiG9w0BAQsFADBaMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluYy4xMjAwBgNVBAMTKU5pcHBvbiBSQSBSb290
IENlcnRpZmljYXRpb24gQXVoaG9yaXR5IEcyMB4XDTIOMDgwMjAyMzMzOFoXDTQO
MDkwMjAyMzMzOFowWjELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJ
bmMuMTIwMAYDVQQDEylOaXBwb24gUkEgUm9vdCBDZXJOaWZpY2F0aW9uIEF1dGhv
cmlOeSBHMjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALh9x9q92LDN
WhqWCqPtTgNLWgCWbOEnZXt4YY9oMBbxzKU6lpMixuHxdCv5Fcct+gNWE98VmRVz
7NjBzlOpUyzasjzWZLCIxacSJpxKKn3lIQorHsFKdEgYoelEbom/duj81c7r2ftP
9S3LpX776DQI6FeEvWfNkqdCcUBm79Geounn8mIH5Ub1JtBLRRHFiVcvKoq8UQQk
pdrRY22Nh3pOXqkOMRt/sVCLA9seZyaRm/aSALTK3OGMyN782H7dWHyhaZOed/cw
qKd5yBzWzCeBKLEz8xkoF3oztMArPdGpQr+tzlSpOeRuNuQP9POpxgPD3egbX+D/
GXQaQsaa+54yxjCIr/kAUi7273DooyAFGXnheRG7EsRu8mX5vRiJZPt1YZw2lCXu
sQmyWqOFch6Ve2jD9kc4IdoLezIz1/nwJu4jZaiWIyk7plsT9jyL99kQhCfOQjAQ
wr+oxVafpAt7ejZcwOM8IH7KDQ32iCUCMWnFiaiyyhbRkuqEjtoOIXNN6dOBKmBx
bWOJJH2FBKHt6XhfDaGeDDiiE/iCnpSIfIUDjXkJvOI+rLWgg1PrpuOTgyJj7Rn7
X2RNRr2WE9bt1Db68RvMEzwWBEfJxZaQwYtaOWOf6iG+Ssr5deefoppyfhOOesrx
Bei2nkhIUG//TqkcBMMaFuox3ROJPwRFAgMBAAGjQjBAMA8GA1UdEwEB/wQFMAMB
Af8wDgYDVR0PAQH/BAQDAgHGMBOGA1UdDgQWBBQTrjzkvfDAcNazgpqjawHolkx2
fjANBgkqhkiG9w0BAQsFAAOCAgEAQithspZyjJ6jS8tZbVEQtMxS9dx8tHUfKb3l
N+P2D2KkLgF+lVKX2MY/+8/VhzYAIO/4kvHNbXFMco70btw37bumkCeCT4B8pZZe
Ao7ixh9m4OXBYWn7APvwXiBFOG4YEwmhS98jNxzOMj6GhuCOGeKbkUWbZxbNH9av
WGPHgFPQ5lqPBqW5glaOmLDPd+alnciJCtfNiB+cVqhrCs3OOuMsBPsLQeaoVFSc
6Apk1vOAjWArg1PFtvRfFalEzGLzdsxT/PYtX/5elxAlYbeBUF7GLyOSXtTG+P8V
DbpF7b9OKmvEx42b7ocOppWiIgZG76XtWuWFQ3Zo8Jzvt7plsPd0432EJSa+QmHB
xtph2Qv7L6jhM5ChVxifsLYu4F6n9Oij/ivwN5s+eo5okIeI5CITUOgsd+mkiPdD
5eQgSExJpJ8F9kdtBXzozG9sczaSktr2xVYOsvgtMjIBdqyMU2bGwUp1rKn8IUwW
NphrJaTxAuQKF9qiFOvXTU/4igBHfkxOKO5JosJlvC1pkODOqAm9c34wV2bskOIx
tRyxgrZa4ley7y1Qa8eg5wwKbUik5Yj9rIEZ8/32nE7JBIOHSpOevXFA4cmg9oUX
Dzj3RXMYtDaemGZ6gTCxdV7Hi4L/OP+Zop99zY9aNAzQW2MsvizjZBrJTs7LpOKw
Vw8mcPU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIF9TCCA92gAwIBAgIBAzANBgkqhkiG9w0BAQsFADBaMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluYy4xMjAwBgNVBAMTKU5pcHBvbiBSQSBSb290
IENlcnRpZmljYXRpb24gQXVoaG9yaXR5IEcyMB4XDTIOMDgwMjA2NTMwOVoXDTM4
MDEwMjA2NTMwOVowVzELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJ
bmMuMS8wLQYDVQQDEyZOaXBwb24gUkEgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkg
MyBHMjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJjG/HVHyb339r4T
DfEIAyXxDfsgCvXXABPYujfBPGEr0nXYGKdLiJgtyEDAR8h8dfhOKEGhInwl5xef
V6tpuzmUZojAeO/uCNKdytj28TMIT67cu4SwOND6ZO9GCiPOcs2zQPeo2e8Zdt1c
v6C2dbp1J3ybIALKJWmI81FGaRYHWG73Raqi8SZQnz5UrIGlYCNLl3kOgzO8JEKs
kIccOHG4yrZywPQzOsIkM7or8Uy4TVpb6BDMxAtjLLZPgShuLToTq+PO4pgT9kbD
TrklVee/A8qwZXU4/4a3alzttq1rZe23HIlusTIJ1mHERJDFftcyR78gW3OyOv/f
pIdeTNtvEDh5oHrlXkEn6+YsSviaFyLuZqo7L5I2/1cwXfLstT/ToDUNd+1ZQnGa
rbhwFqBhwi1bY1pPuUgLQ19iA4eQyI8NIjk+k2dynk8LMcRKZDLeGeU7yiiEXJgW
McVBbZETRXDWrGTQSvdVrDlBG9ZTOseYM4bQX6mNhszNsXzbT196s6PysqTEF2qF
56vjoBAjNsAe52kuOXQffAdvkPL7CNRn2HT5OwADEYUDezrmK1yJw2c03ZDnPN6Q
35rkKEpVNo2cEATIwZfRpn3SnkPQrsw8fnIeI+e+RQyNoyXsEzz5hsEvu9LvzMrG
GQgKxLPiCfkZAQ9Vi03roOeDgAr5AgMBAAGjgcgwgcUwDwYDVR0TAQH/BAUwAwEB
/zAOBgNVHQ8BAf8EBAMCAcYwHwYDVR0jBBgwFoAUE6485L3wwHDWs4Kao2sB6JZM
dn4wYgYDVR0fBFswWTBXoFWgU4ZRaHR0cDovL2lwa2ljcmwubWFuYWdlZHBraS5u
ZS5qcC9tcGtpL05pcHBvbiJBUm9vdENlcnRpZmljYXRpb25BdXRob3JpdHlHMi9j
ZHAuY3JsMBOGA1UdDgQWBBQZNBBw468fpt8yyjOE+7psCL/PzTANBgkqhkiG9w0B
AQsFAAOCAgEAfJ9hFvgNhdHYJNU9y/Zzrc/JOtNZP4aytmsm2i+HdUm/ppjL9JzO
unGltQd5f2nklhrFGcl+No3Y8pvGOVJ87+AEMsRGzehs134JetMUP9KbkV+T9eJZ
e5szbzAOJ1uG1JETITWViMAeriA/2Xk7ie2whhyIeb4Xscey7VouT32ZCjj/aOS
OZO+s0qhJZoSgDEGBCLpDW+yefyKG8O8eRVOpwPZYI+G6kNuf0yxflw+6sedg9uF
hg2wERywRRCXmb4r0UshWW1Dmh8qQvBCKZvgWmZHCogCWNO2ahsMdNuMOv9DZ3fl
e3Q+SlOYHKiA3wJGMkHE4bBVDbdr13i2QKFOu95rEYc7ulqjWFTWIu6GHlSVKoAv
L2DVnwDtxeTdXOKdTct3FcYjU9//vd5nUAnqCMYniuVGxtOpt8EN9TN9xzmV7TVV
RIw7OSTavnTv7ovMbJR+2pAkeO3iIFNTd9IGlXnAe8m4iP6NbRD+ubiHd8tYgSri
zE4C+lXBuo5vR747OCSBxWTr2R+LbArQDPjlkLgbw+FraeRtnH4wPyJk/s8WRgK
Y/YpMZc5C2W7SpC6gNv6P8tllbzFcD4x3dOIodsI2SXbUS++jXcW8DAFgD2xREBp
O7mSMHZaCciW/P1PPEmrmkZy4v3tC8nRu+ZkfOEu8GRgODsQE/Obqbk=
-----END CERTIFICATE-----
```

現ルート証明書

中間（CA3）証明書

新ルート証明書（G2）

新中間（CA3 G2）証明書

■中間認証局 CA4 をご利用の場合

（現行のルート証明書、中間証明書（CA4）と新しいルート証明書（G2）、中間証明書（CA4 G2）をマージしたものです）。

現ルート証明書

中間（CA4）証明書

新ルート証明書（G2）

新中間（CA4 G2）証明書

5. Appendix3（失効リスト（CRL）の設定：具体例）

「2.2. 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/nginx/temp

(2) nginx.conf ファイルの server セクションにて以下のディレクティブで設定します。

■ nginx.conf ファイルの設定例

```
server {
listen 443 ssl;

server_name   xxxx;    #環境に応じて設定

ssl_certificate           /etc/nginx/temp/server.crt;
ssl_certificate_key    /etc/nginx/temp/server.key;

ssl_verify_client on;
ssl_verify_depth 3;
ssl_client_certificate /etc/nginx/temp/nra.crt;

<Location>   #環境に応じて設定

if ($ssl_client_i_dn !~ "CN=(Nippon RA Certification Authority 3|Nippon RA Certification Authority 3 G2)"){
                return 403;
        }
        if ($ssl_client_s_dn !~ "O=REIWA CERTIFICATES SERVICES"){
                return 403;
        }

</Location>

ssl_crl /etc/nginx/temp/crl.pem;

    location / {
            root    /usr/share/nginx/html;
            index   index.html index.htm;
            }

~~~~（以下省略）

}
```

(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

現ルートおよび中間認証局の失効リストと新ルートおよび中間認証局の失効リストを取得し PEM 形式に変換後、各失効リストをマージし crl.pem ファイルを作成します。

作成した crl.pem ファイルを保存先ディレクトリ「/etc/nginx/temp」に配置します。

【中間認証局 CA3 をご利用の場合】

```
#!/bin/sh
cd /etc/nginx/temp/download

wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRARootCertificationAuthority/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl_root.pem
rm -f cdp.crl

wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl_ca3.pem
rm -f cdp.crl

wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRARootCertificationAuthorityG2/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl_rootG2.pem
rm -f cdp.crl

wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3G2/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl_ca3G2.pem
rm -f cdp.crl

cat crl_root.pem crl_ca3.pem crl_rootG2.pem crl_ca3G2.pem > crl.pem

cd /etc/nginx/temp
rm -f crl.pem
cp -p /etc/nginx/temp/download/crl.pem ./
systemctl reload nginx
```

【中間認証局 CA4 をご利用の場合】

```
#!/bin/sh
cd /etc/nginx/temp/download

wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRARootCertificationAuthority/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl_root.pem
rm -f cdp.crl

wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl_ca4.pem
rm -f cdp.crl

wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRARootCertificationAuthorityG2/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl_rootG2.pem
rm -f cdp.crl

wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4G2/cdp.crl'
openssl crl -inform der -in cdp.crl -outform pem -out crl_ca4G2.pem
rm -f cdp.crl

cat crl_root.pem crl_ca4.pem crl_rootG2.pem crl_ca4G2.pem > crl.pem

cd /etc/nginx/temp
rm -f crl.pem
cp -p /etc/nginx/temp/download/crl.pem ./
systemctl reload nginx
```

【補足】

・/etc/nginx/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。

6. Appendix4（クライアント証明書認証の設定：具体例）

「2.4.クライアント証明書認証の設定変更」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/nginx/temp （A）

(2) nginx.conf ファイルの server セクションにて、クライアント認証で許可する条件を設定します。

NRA-PKI 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（B）

① NRA-PKI の発行局（CA3 または CA3 G2 で発行された証明書のみ受け付けます）

CN=Nippon RA Certification Authority 3

CN=Nippon RA Certification Authority 3 G2

※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

CN=Nippon RA Certification Authority 4 G2

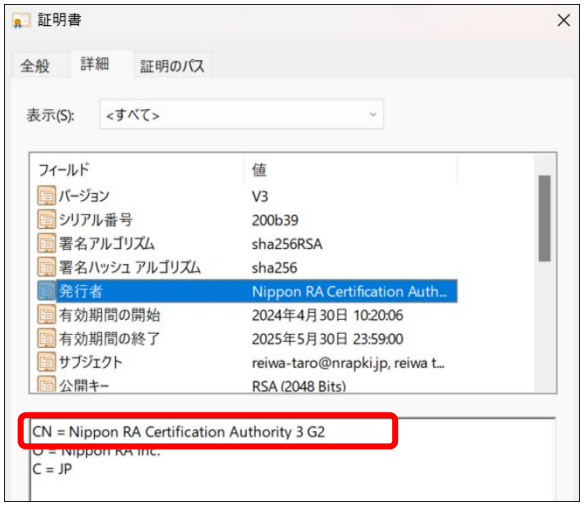
② 条件に合致した証明書（ここでは「レイワ証明書サービス」社が管理する証明書のみ受け付けます）

O=REIWA CERTIFICATES SERVICES

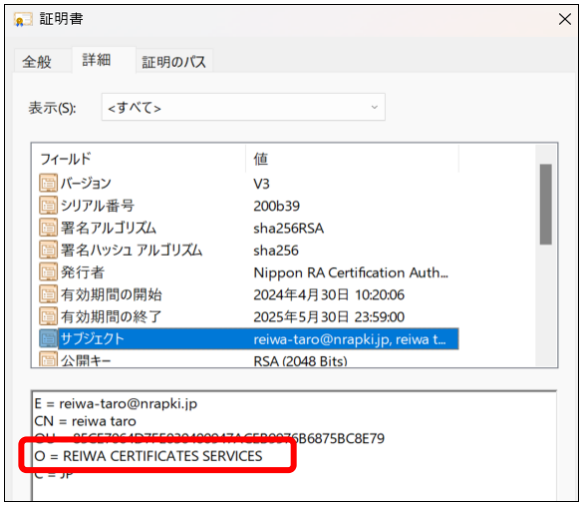
【補足】

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。

(1) NRA-PKI の発行局



(2) サブジェクト O の値



■nginx.conf ファイル設定例

```
server {
listen 443 ssl;

server_name   xxxx;    #環境に応じて設定

ssl_certificate           /etc/nginx/temp/server.crt;
ssl_certificate_key       /etc/nginx/temp/server.key;

ssl_verify_client on;
ssl_verify_depth 3;
ssl_client_certificate /etc/nginx/temp/nra.crt;          ―― (A)

<Location>   #環境に応じて設定

if ($ssl_client_i_dn !~ "CN=(Nippon RA Certification Authority 3|Nippon RA Certification Authority 3 G2)"){
                return 403;
        }
        if ($ssl_client_s_dn !~ "O=REIWA CERTIFICATES SERVICES"){
                return 403;
        }                                                                    } (B)

</Location>

    location / {
            root    /usr/share/nginx/html;
            index   index.html index.htm;
    }
~~~~（以下省略）
}
```

【補足】

・Location は環境に応じて設定してください。

・設定を有効にする場合は、「systemctl reload nginx」コマンドを実行して nginx を再起動（設定をリロード）してください。

以上