NRA

Akamai EAA
クライアント証明書認証
設定手順書

2022 年 3 月 7 日

Ver. 1.00

改訂履歴

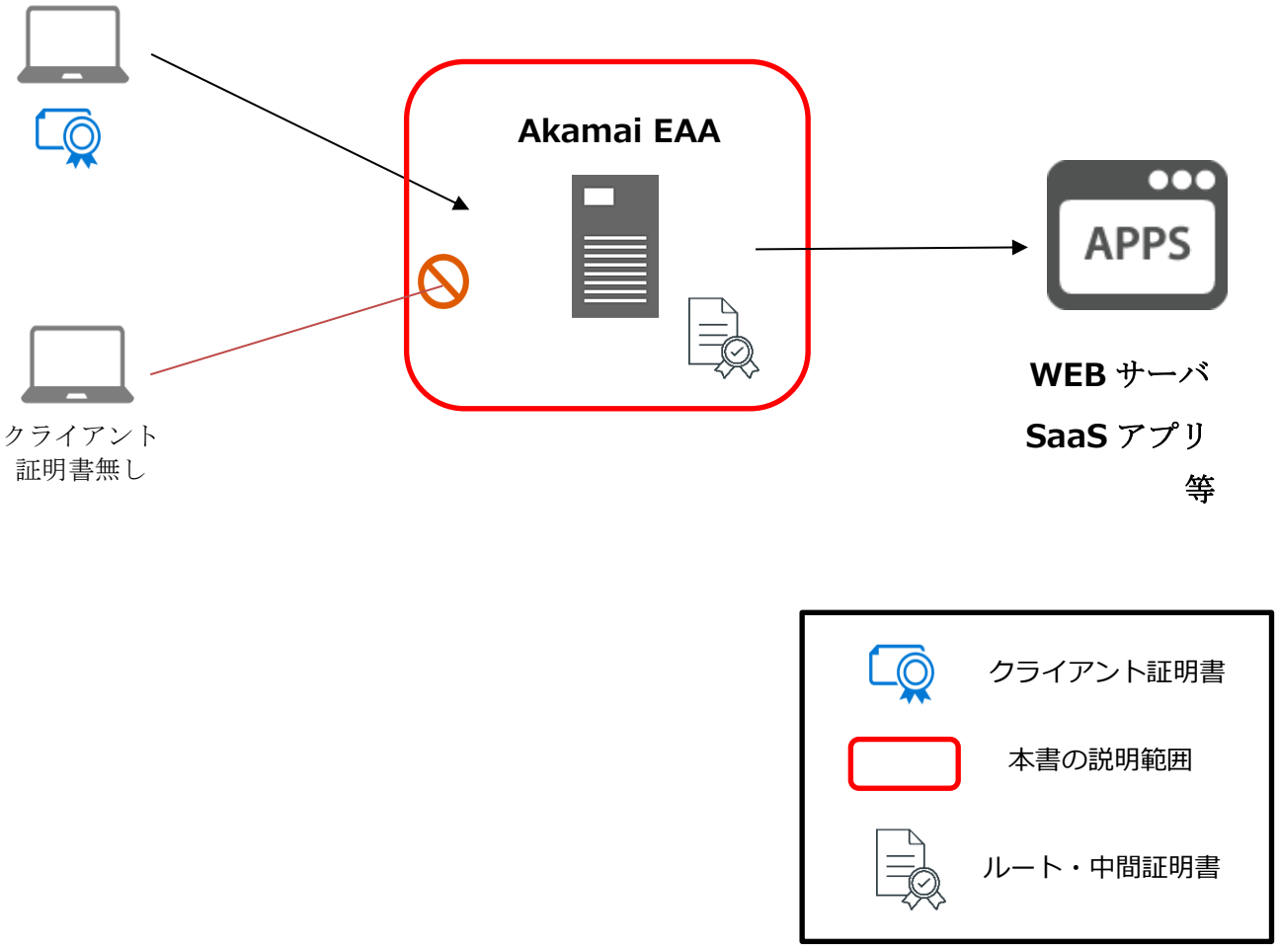
版	日　付	内　容	備　考
Ver. 1.00	2022/3/7	初版作成	

<目　次>

1. 概要

本書では Akamai 社が提供するサービス「Akamai EAA」において弊社クライアント証明書を用いた証明書認証を有効にする手順を説明いたします。

【構成イメージ】



2. 事前準備

■ルート証明書と中間証明書

PEM 形式のルート証明書とご利用中の中間認証局の証明書が必要です。

※PEM 化については、p12「4.1. PEM 形式のルート証明書・中間証明書」をご確認ください。

■クライアント証明書

ご利用する端末にインストールしてください。

3. 設定手順

本項から詳細な設定手順に関する説明になります。

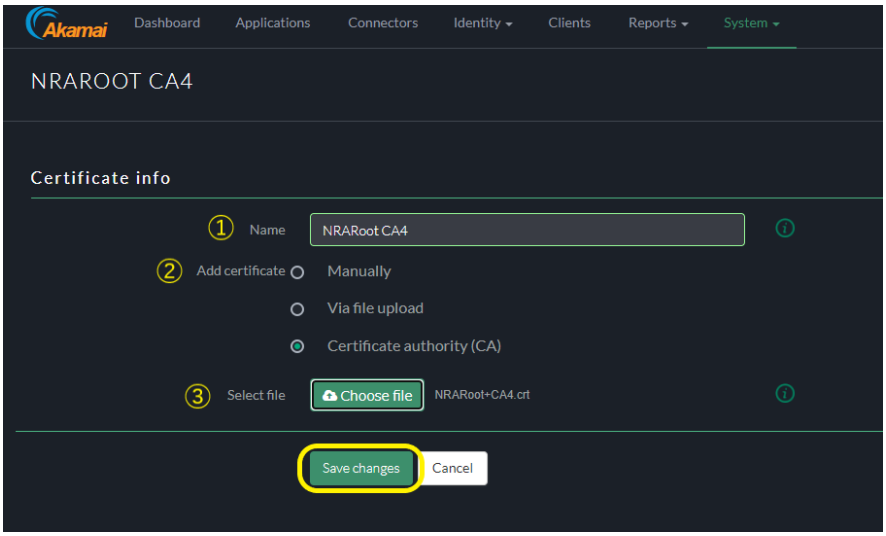
流れは次の通りです。

項目は以上です。次ページから各項目の説明の記載になります。

3.1. ルート・中間証明書のアップロード

PEM 形式のルート証明書と中間証明書をアップロードします。

Akamai EAA の管理コンソールから[System]⇒[Certificates]と選択し、右上の【Add certificate】をクリックします。
以下図の画面が表示されるので【設定内容】を参考に設定してください。



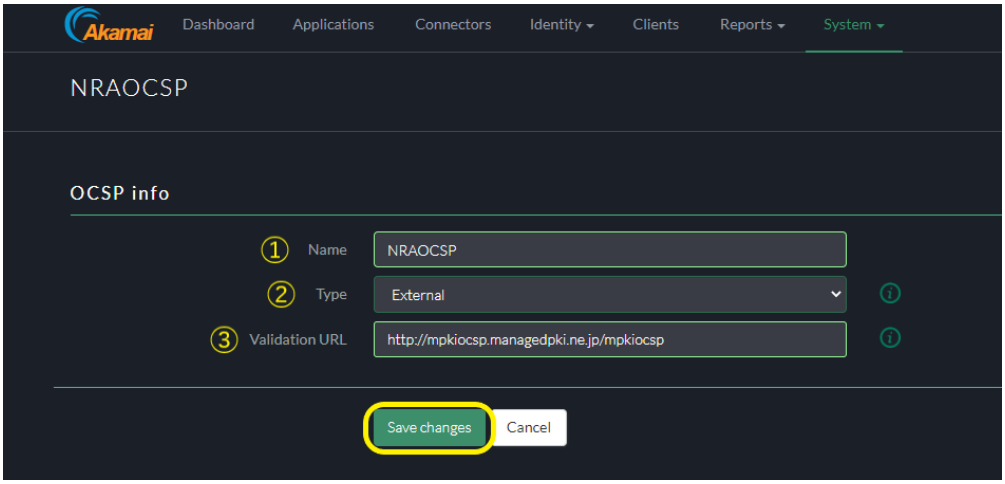
【設定内容】
①Name・・・・・・・・・任意の値を入力（本書では NRARoot CA4 とします）
②Add certificate・・・・「Certificate authority (CA)」にチェック
③Select file・・・・・・「Choose file」から PEM 形式のルート・中間証明書ファイルを選択

「Save changes」をクリックして設定完了です。

3.2. OCSP レスポンダの登録

証明書の失効確認をする為の OCSP レスポンダの登録をします。

[System]⇒[OCSP]と選択し、右上の「Add OCSP」をクリックします。
以下図の画面が表示されるので【設定内容】を参考に設定してください。



【設定内容】

①Name・・・・・・・・・・任意の値を入力（本書では NRAOCSP とします）

②Type・・・・・・・・・・[External]を選択

③Validation URL・・・・・以下 OCSP レスポンダ URL を入力

OCSP レスポンダ URL» http://mpkiocsp.managedpki.ne.jp/mpkiocsp

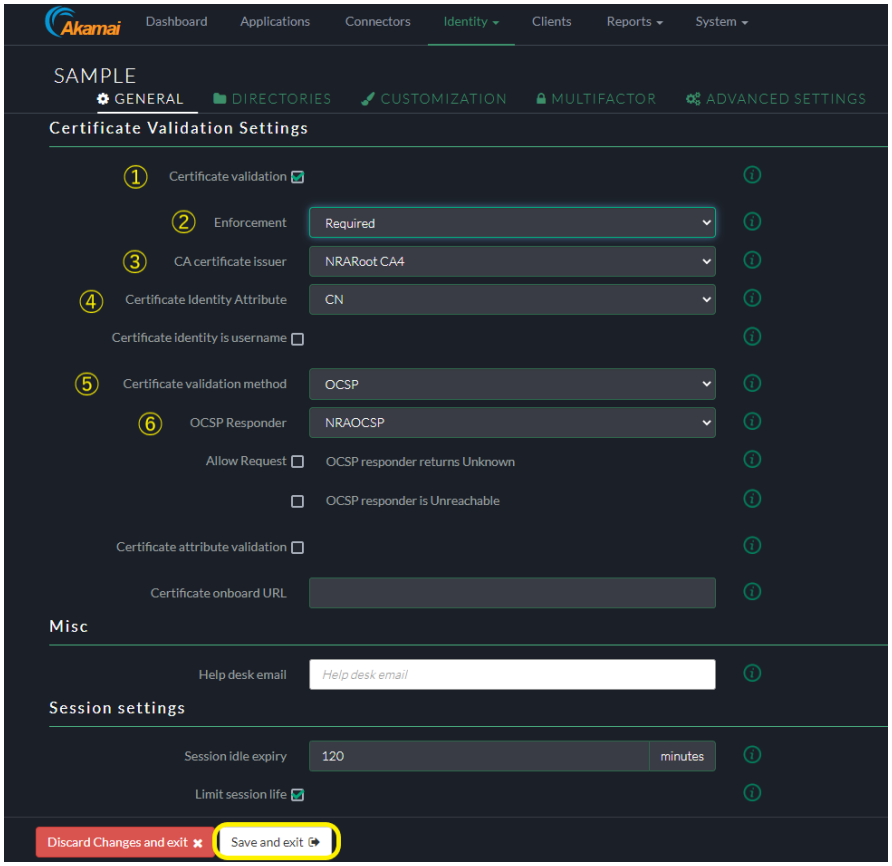
「Save changes」をクリックし設定完了です。

3.3. Idp の設定変更

対象の Idp の証明書認証を有効にします。

[Identity]⇒[Identity providers]と選択し、対象の Idp の設定画面を開きます。

以下図の画面が表示されるので「Certificate Validation Settings」の項目を設定します。



【設定内容】

①Certificate validation・・・・・・・チェック

②Enforcement・・・・・・・・・・[Required]を選択

③CA certificate issuer・・・・・・・項目 3.1 でアップロードしたルート・中間証明書を選択

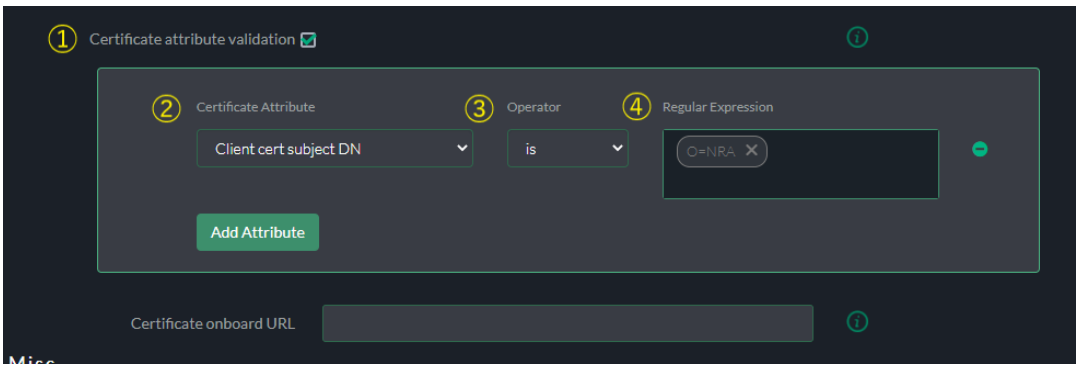
④Certificate Identity Attribute・・・[CN]を選択

⑤Certificate validation method・・・[OCSP]を選択

⑥OCSP Responder・・・・・・・・項目 3.2 で登録した OCSP レスポンダを選択

「Save and exit」をクリックし設定完了です。

【補足】ここまでの設定で、ご利用中の中間認証局から発行された証明書のみ認証可能となりますが、証明書のサブジェクト O(会社名英字表記)で制限したい場合は追加で以下を設定してください。



①Certificate attribute validation・・・チェック

②Certificate attribute・・・・・・・・「Client cert subject DN」を選択

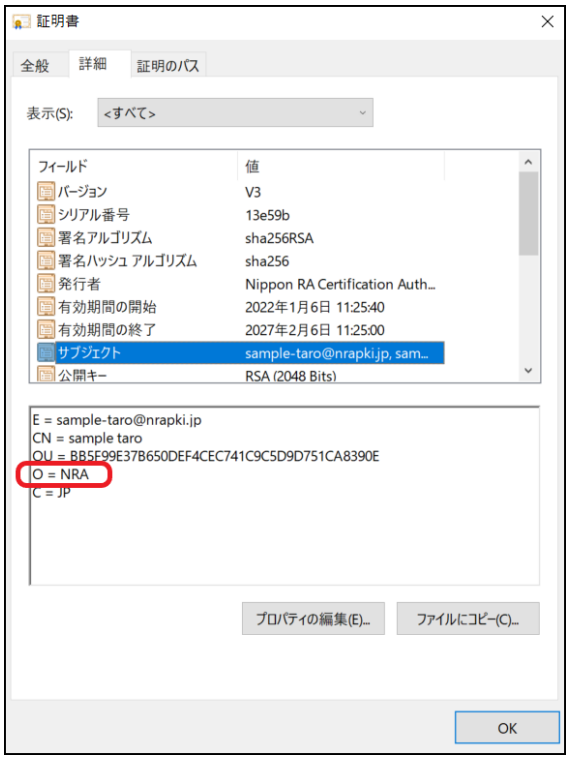
③Operator・・・・・・・・・・・・・・「is」を選択

④Regular Expression・・・・・・・・「O=会社名英字表記」の形式で入力

【O(会社名英字表記)の値の確認方法(WindowsPC の場合)】

「certmgr.msc」を実行し、「個人」-「証明書」にて対象の証明書を選択します。

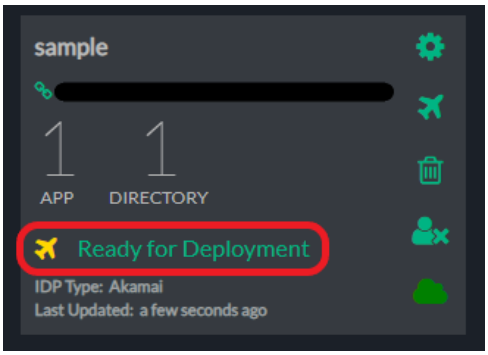
証明書をダブルクリックで開き、詳細タブのサブジェクト欄をご確認ください。



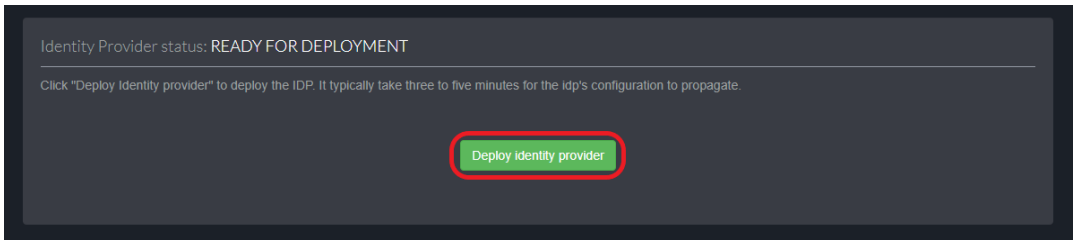
3.4. 変更内容の反映

設定した内容を反映させます。

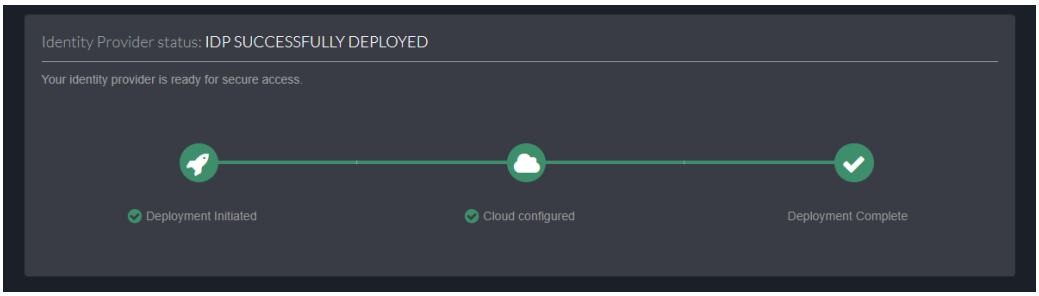
[Identity]⇒[Identity providers]の画面で設定変更を実施した Idp にて、「Ready for Deployment」をクリックします。



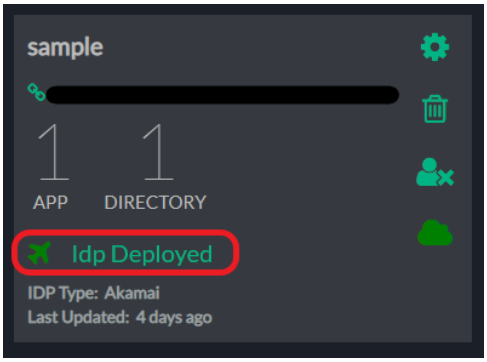
「Deploy identity provider」をクリックします。



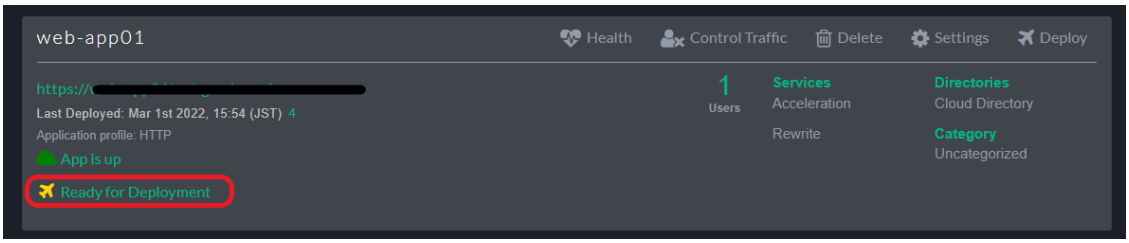
以下図の画面が表示されれば完了です。



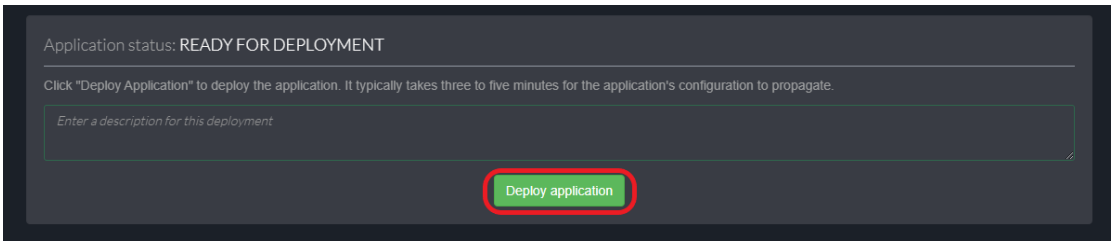
完了後は、「Ready for Deployment」の部分が「Idp Deployed」になっている事を確認してください。



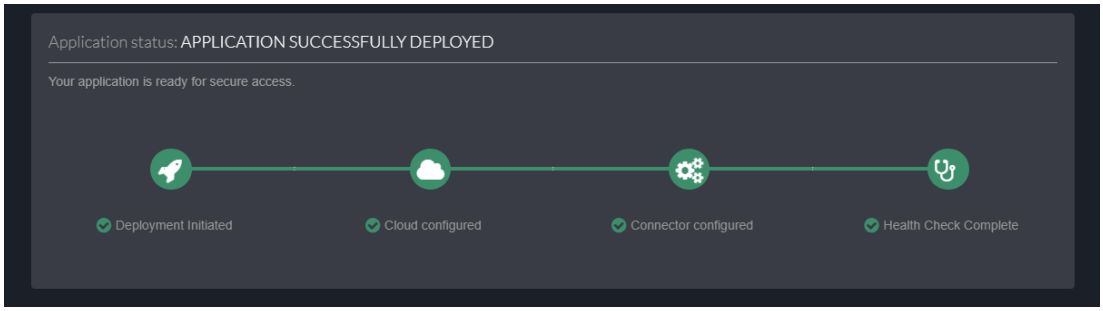
次に[Applications]を開き、対象の Idp が紐づくアプリにて「Ready for Deployment」をクリックします。



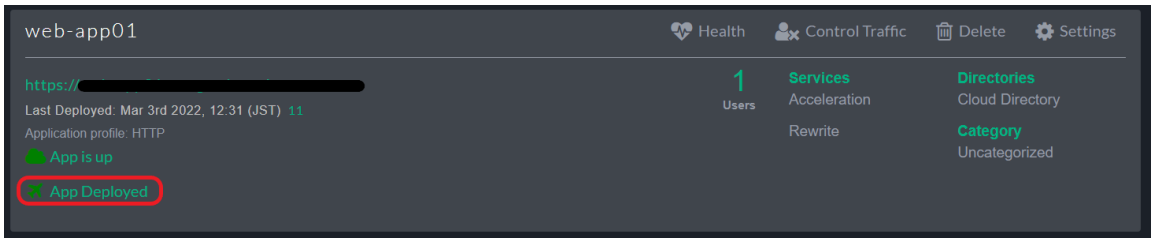
「Deploy application」をクリックします。



以下図の画面が表示されれば完了です。



「Ready for Deployment」の部分が「App Deployed」になっていることを確認してください。



以上で Akamai EAA でクライアント証明書認証をするための設定は完了です。

4. appendix

4.1. PEM 形式のルート証明書・中間証明書

以下、弊社 HP のレポジトリ(https://www.nrapki.jp/client-certificate/repo/)で公開するルート証明書・中間証明書を PEM 形式にした内容です。テキストファイルへコピー＆ペースト(※1)し、任意のファイル名(拡張子は.crt)で保存してください。

上段がルート認証局、中段が中間認証局 CA3、下段が中間認証局 CA4 の証明書の内容となります。ルート証明書とご利用中の中間認証局(※2)の証明書のみコピーしてください。


```
-----BEGIN CERTIFICATE-----
MIIDazCCAlOgAwIBAgIBATANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluY4xLzAtBgNVBAMTJk5pcHBvbiBSQSBSb29O
IENlcnRpZmljYXRpb24gQXVOaG9yaXR5MB4XDTExMDgxNTAyMzAyNloXDTMxMDgx
NTAyMjg1NlowVzELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJbmMu
MS8wLQYDVQQDEyZOaXBwb24gUkEgUm9vdCBDZXJOaWZpY2FOaW9uIEF1dGhvcmlO
eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPRqqsUWzgB38ZMi7aeT
ThqiJKzqBaNOUWL9Czhb3Ob/Li5KEQrAz2PegOwZns6b+F/4QE2H2gl9k4qBe8dh
Arlns9tSIH6N6/rDg625rCGKj9cAiOizis2gyTptmcgMffENQI6dcDxviuCY98dG
8ITMWxKucza/rCVt5KBC5Uh17AgPA1j5vPgXnDn9vnwVO4sYqoXXa7ZRgYFc+g/h
pM/lqWFze1gtGLBvEnYIgyd3cbVEOmMwc15NNaCcSFJbr2p/P/KA9xEmot768M5f
5NTIW/Cg6LJ/bm/byu8H2jhjpQEdY35rDSOip2OmqEJy51nWbUMqMV2SesPouVjv
x5UCAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAcYwHQYD
VR0OBBYEFBmZpk3iL3keW05k2YDn98mwn3IOMAOGCSqGSIb3DQEBCwUAA4IBAQCX
Meqx614XO8HFK/XWmzBmnXbU1OXGigNK5CGmVXVM5tdVGSySW8br9c+ZUGRcq4cd
6cUA/4pIUILTqUb5TOwO8+pw+egehYWeeVqoF7T5EWLps2HBv8+LolPnXY/Btp88
teacCIQSS5tiSbfuR3UDuCfGWtAUdmyG5jH6Ose9k/k+zLCvChOhXGaQXAe0AnEIM
n+oKqSQeSTbo7+7KxiqtjyZ2WerBqPgAFpJNu+PCpG1rXaPU87//PKqP9lYqkO5h
VGMOs8QNnWXVbVTOeJV79Ef5ZfbtWS8x2OJYRALzbLKtu9wuFdlocL5dWeVL6QxS
uWKlNqU/oyG9yDKuoG5l
-----END CERTIFICATE-----
```


ルート証明書


```
-----BEGIN CERTIFICATE-----
MIID7TCCAtWgAwIBAgIBITANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluY4xLzAtBgNVBAMTJk5pcHBvbiBSQSBSb29O
IENlcnRpZmljYXRpb24gQXVOaG9yaXR5MB4XDTE0MDcxNzA3MTI1NVoXDTMxMDgx
NTAyMjg1NlowVDELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJbmMu
MSwwKgYDVQQDEyNOaXBwb24gUkEgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgMzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIyaWX8RUMgPmjUFOtO8GkxR
Xt/kEoaUHt81dPO1r4nLth6LKcBQ8ao6CajTv7un5OkZ+olOMeLRVvamXqrgCbZw
PMO9le9Dpkdl2Ojdwm4OPEUgLQeb/4hfQyQaSIN/VtnMvyRtjSdZhNigyaKYRiKS
2lOCTbdn3hpWlHgot5rD5sh5wJ96EHmeTalOOp8BAlmaejEantMR3KhZZfhxC2kK
a2LIRtsXCHRXB15shFD8yMiS5KBlXEkpKAKyp8Zat8fgm58d1UXdLotRC91biH5W
96JL22fnbuz3WsFoaQMjdLDa9Q9fC7GewSF3OaYljPkcEXkAQcw36mjRmaQUFxUC
AwEAAaOBxjCBwzAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBxjAfBgNV
HSMEGDAWgBQZmaZN4i95HltOZNmA5/fJsJ9yDjBgBgNVHR8EWTBXMFWgU6BRhk9o
dHRwOi8vbXBraWNybC5tYW5hZ2VkcGtpLm5lLmpwL21wa2kvTmlwcG9uUkFSb290
Q2VydGlmaWNhdGlvbkF1dGhvcml0eS9jZHAuY3JsMBOGA1UdDgQWBBRbOO113m4V
nZU8OO/XPyhMvhBfgDANBgkqhkiG9w0BAQsFAAOCAQEAqpAvO3zpxGAF5R7pZtde
k3eHH1JVnhr+gWHty2OjGBmr2RBzWpBu1tXWZjKilaPjU14mMD5L/rA/OtwnTk7x
ep+bFEHdJzJ+bcTf/LOFETRfu/i9ctKQiDRqrp15nuJDyg8/+j/EaawiOY3bs6qj
q/r7MNfQGDghg6dMIlzOmETLVjisSfDI1EPQOwfxV2TvfQDNaE39OVqSb4GOYfuP
Pyb44omkQmbQOemlZDF5YkmncVHE4dI/stVeue8YArnO6BYvhRpHveIBtkG8phWD
th6MVyMzsnn4FCEtmRN687uukbfsnQ/mlmEpzPXDEYlAvxrH4u3zUccQRhhiq5ub
3A==
-----END CERTIFICATE-----
```


中間（CA3）証明書


```
-----BEGIN CERTIFICATE-----
MIID7TCCAtWgAwIBAgIBIjANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluY4xLzAtBgNVBAMTJk5pcHBvbiBSQSBSb29O
IENlcnRpZmljYXRpb24gQXVOaG9yaXR5MB4XDTEOMDcxNzA3MTgzM1oXDTMxMDgx
NTAyMjg1NlowVDELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJbmMu
MSwwKgYDVQQDEyNOaXBwb24gUkEgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgNDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALNvx9mQLWZdSvJf/8PmGW3A
178UL2MHWqFbilJCaZ5oVXSPG//6PO+dCpjD/Hm3/9KpxqICc7l6HdHsZXSKbCFi
kHlJhqZ+jQL5q511z8bAbtQff2VyMSNQe0tzLayxdCMfckxMYjS2nsX84stQ3mEC
5E2Cf+ovZM96RpTEAjrOb2DcOuUxnZCVgJiy1OoryrICMVfNnfTpFmkuATXRmeko
yx9DVMi9fegGYwFhfl+zNFSBAKuBBsqf9l4yfk9CBouGfO0iQrF/DkrpoLmEPS1b
tbcB7agTkaeSKTbqCXZj9AMDFMaNYzun24KHXhJUbt2efJRbLHYmAPZC7pnAE3MC
AwEAAaOBxjCBwzAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBxjAfBgNV
HSMEGDAWgBQZmaZN4i95HltOZNmA5/fJsJ9yDjBgBgNVHR8EWTBXMFWgU6BRhk9o
dHRwOi8vbXBraWNybC5tYW5hZ2VkcGtpLm5lLmpwL21wa2kvTmlwcG9uUkFSb290
Q2VydGlmaWNhdGlvbiBBdXRob3JpdHkvY3JsMBOGA1UdDgQWBBSeu4RjR78m
fX37XfMNpsxb2ay3qzANBgkqhkiG9w0BAQsFAAOCAQEAjc8OOeZsNeLg5cZIO56R
CgXVGe1+XwadaRfodzsQBFDNYD+y5iTpndw45XGsuH2rHSdWZuCluju9YPqGKnHr
oae5uxTutw8MrIKKcERHIac4SpqsEWEHRHBgnqpnV/45FJqxhEVOanyxQlEEmeXW
cPdZOXlWLhWcxOVPC8OxaoDw/VF/P+9SYioENvY1Oix8VEKb7yui9SALdIx1VmZg
mMHxUDZixsEs4CLL+NXISIg+KSI3Wqd6FFIep3UOEAm8cNC4FQoO9M6WSp8moL4R
zahrIvBCWCAc4SflBggLDAbf4eXc49UQ5xjLKH3iRDSiMNOVpbt6PtY/WTVK7UYU
Mw==
-----END CERTIFICATE-----
```


中間（CA4）証明書

※1

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。

※2

【ご利用中の中間認証局の確認方法】

以下画像の 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。