NRA

Akamai EAA クライアント証明書認証

設定手順書

2025年01月22日

Ver. 2.00

改訂履歴

版	日付	内容	備考
Ver.	7022/2/7	初版作成	
1.00	2022/3/7		
Ver.	2025/1/22	ルート、中間証明書を新認証局(G2)に変更	
2.00	2023/1/22		

<目 次>

1. 概要	. 3
2. 事前準備	.4
3. 設定手順	. 5
3.1. ルート・中間証明書のアップロード	.6
3.2. OCSP レスポンダの登録	.7
3.3. Idp の設定変更	.8
3.4. 変更内容の反映1	10
4. Appendix (PEM 形式のルート証明書・中間証明書)1	12

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. Appendix (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。

3.1. ルート・中間証明書のアップロード6
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。
3.2. OCSP レスポンダの登録7
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。
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。
3.4. 変更内容の反映
ここまでで設定した内容を反映させます。

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。

Akamai	Dashboard	Applications	Connectors	Identity 🗸	Clients	Reports 🗸	System 🗸	
NRAROC	DT CA4							
Certificat	e info							
	(1 Name N	IRARoot CA4				()	
	2 Add	d certificate O	Manually					
		0	√ia file upload					
		0	Certificate auth	ority (CA)				
	3	Select file	Choose file	NRARoot+CA4.crt				
			ave changes	Cancel				

【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。

Applications Dashboard Applications	Connectors	Identity 🗸	Clients	Reports 🗸	System 👻	
NRAOCSP						
OCSP info						
1 Name	NRAOCSP					
2 Туре	External					
3 Validation URL	http://mpkiocsp.ma	anagedpki.ne.jp/m	npkiocsp		()	
(Save changes	Cancel				

【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。

Akamai Dashboard Applications	Connectors Identity - Client	ts Reports - Systen	1 -
SAMPLE GENERAL DIRECTOR	es 🖌 customization 🔒 M		
Certificate Validation Settings			
Certificate validation 🗃			
2 Enforcement	Required		
3 CA certificate issuer	NRARoot CA4		
Certificate Identity Attribute	CN		
Certificate identity is username 🗖			
5 Certificate validation method	OCSP		
6 OCSP Responder	NRAOCSP		
Allow Request 🗖	OCSP responder returns Unknown		
٥	OCSP responder is Unreachable		
Certificate attribute validation 🗖			
Certificate onboard URL			
Misc			
Help desk email	Help desk email		
Session settings			
	120	minutes	
Limit session life 🔄			
Discard Changes and exit 🗙 Save and exit	+)		

【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。

	Certificate attribute validation 🛃				١	
	Certificate Attribute Client cert subje	3 ct DN 🗸	Operator 4	Regular Expression		
	Add Attribute					
Micc	Certificate onboard URL				6	

①Certificate attribute validation $\cdot \cdot \cdot f$ 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。

🐖 証明書		×
全般詳細証明のパス		
表示(S): <すべて>	~	
	1-4-	•
	值	
	V3	
シリアル番号	13e59b	
割割割割割割割割割割割割割割割割割割割割割割割割割割割割割割割割割割割割	sha256RSA	
書名ハッシュ アルコリズム データー・シュー	sha256	
● 発行者	Nippon RA Certification Auth	
目有効期间の開始	2022年1月6日 11:25:40	
目の期间の終」	2027年2月6日 11:25:00	
	Sample-taro@nrapki.jp, sam	~
E = sample-taro@nrapki.jp		
CN = sample taro	410000007010493000	
O = NRA	41C9C5D9D751CA0590E	
C = JP		
1		
	プロパティの編集(E) ファイ	(ルにコピー(C)
		ОК

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。

Click "Deploy identity provider" to deploy the IDP. It typically take three to five minutes for the idp's configuration to propagate.	Identity Provider status: READY FOR DEPLOYMENT
	Click "Deploy Identity provider" to deploy the IDP. It typically take three to five minutes for the idp's configuration to propagate. Deploy identity provider

以下図の画面が表示されれば完了です。

Identity Provider status: IDP SUCCESSFULLY DI	EPLOYED	
		V

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。

Application status: READY FOR DEPLOYMENT	
Click "Deploy Application" to deploy the application. It typically takes three to five minutes for the application's configuration to propagate.	
Deploy application	

以下図の画面が表示されれば完了です。

Application status: APPLICATION SU	JCCESSFULLY DEPLOYED		
		· · · · · · · · · · · · · · · · · · ·	

「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。

web-app01	💎 Health	🛃 Control Traffic	🛅 Delete 🛛 🛱 Settings
https://			

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(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(<u>https://www.nrapki.jp/client-certificate/repository/</u>)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。テキストファイルヘコピー&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 (G2)、中段が中間認証局 CA3 G2、下段が中間認証局 CA4 G2 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。



※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。

Ж2

【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 G2、なければ CA3 G2 をご利用いただいております。

NRA	統合認	証基	盟システ.	4			
令相証明書サービス 令和 三郎 私 ログイン中	利用者メンテナンス	_					
◎ サービス情報メンテナンス	利用法人組織の選択	利用者の	メンテナンス				
利用法人 詳細設定							
利用者 メンテナンス	令和徒崩書サービス 加入組織情報						
利用者 耐除							
○ へルプ	以下のサービスを選択してい	ます。					
NRA-PKIシステム サポートサイト	テストサービス (CA4)	∽					
💿 このサイトの実在証明							
	組織名	部門		住所	電話冊号		
	本社		東京都 千代田区 〇〇町1-2-3 ムムビル 2階		123-4567-890		