

プライベートCA Gléas ホワイトペーパー

Thunder ADC (ロードバランサー) における

クライアント証明書認証の設定手順

Ver.1.0 2015 年 9 月

- JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
- ・その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

プライベート CA Gléas ホワイトペーパー Thunder ADCにおけるクライアント証明書認証の設定手順

目次

1. はじる	めに4
1.1.	本書について4
1.2.	本書における環境4
1.3.	本書における構成
2. Thun	der ADC での設定5
2.1.	サーバ証明書の設定5
2.2.	ルート証明書のインポート7
2.3.	失効リスト(CRL)のインポート8
2.4.	SSL テンプレートの設定9
2.5.	バーチャルサービスへのテンプレートの適用11
3. Gléa	s の管理者設定(PC)12
3.1.	UA(ユーザ申込局)設定12
4. PC カ	ヽらの接続操作12
4.1.	クライアント証明書のインポート12
4.2.	Web サーバへの接続14
5. 問い	合わせ14

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベートCA Gléas」で発行したクライアント証明書を 用いて、A10ネットワークス株式会社製のアプリケーション配信コントローラ 「Thunder ADC」でWeb負荷分散におけるクライアント証明書認証をおこなう環 境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あら ゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構 築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な 場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- レードバランサー: A10 Thunder ADC (AX vThunder 4.0.1 build214)
 ※以後、「Thunder ADC」と記載します
- JS3 プライベートCA Gléas (バージョン1.12)
 ※以後、「Gléas」と記載します
- ➤ Webサーバ: Ubuntu 14.04.2 LTS / Apache/2.4.7
- クライアント: Windows 8.1 Pro / Internet Explorer 11
 ※以後、「PC」と記載します

以下については、本書では説明を割愛します。

- Thunder ADCのセットアップ、ロードバランス設定
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定
- Webサーバのセットアップや設定、クライアントPCの各種設定など

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています



- Gléasでは、Thunder ADCにサーバ証明書を、PCにクライアント証明書を発行する
- PCはThunder ADC経由で冗長化されたWebサーバにhttpsでアクセスする。 Thunder ADCはTLS通信を終端し、またクライアント証明書を要求する。 PCは有効なクライアント証明書がないと負荷分散されたWebサーバに接続 することができない

2. Thunder ADC での設定

2.1. サーバ証明書の設定

本手順の前に、Gléas の管理者画面よりサーバ証明書ファイル(PKCS#12 ファイル)をダウンロードします。

ダウンロードする際に保護パスワードの入力を求められますが、Thunder ADC にインポートする際にこのパスワードが必要となります。

7	証明書を保護するため	のバスワードを入力してくたさい。,	プライベートCA
<u>#demo</u>			
証明書 JCCH-SSS de	729-1	••••• ダウンロード キャンセル	D <u>一覧に戻る</u> D <u>ビック</u>
業証明書情報···· ▶ <u>servercert.gleas.ex</u>	ample	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	▲ <u> レロード</u> ■ <u> タイムライン</u> 1:2017/04/03 12:26

Thnuder ADC の管理画面にログインし、画面上部のメニューより[ADC] > [SSL Management] とクリックし SSL Certificates の画面を表示させ、[Import]をクリックします。

Importの画面より以下の通りにして、[Import]をクリックします。

- [File Name]: このサーバ証明書の任意の名称を入力
 [Import]: [Certificate]を選択
 [Import Certificate from]: [Local]を選択
 [SSL or CA Certificate]: [SSL Certificate]を選択
 [Certificate Format]: [PFX]を選択
 [PFX Password]: サーバ証明書ファイルをGléas からダウンロードするときに設定したパスワードを入力
- [Certificate Source] :

トリるとさに設定したハスリートを入力	
Gléas よりダウンロードしたファイルを指定	2

AB	Dashboard 👻	ADC 👻	GSLB 🔻	WAF 👻	AAM 👻	CGN -	Network 👻	System -	Integration -	Partition: share	ed 🗸 😧 🗸 🤅) 🖺 🚢 🕩
SSL Certificates	Cert Revocatio	on List	Expiration	Email							AXvThunder 4	1.0.1 build 214
ADC >> SSL Ma	anagement >>	SSL Ce	rtificates	>> Impo	ort							Help
SSL Certifi	cates											
File Name *			server	cert-gleas								
Import *			Certi	ficate (CKey (Certific	ate and Key					
Import Certifica	ate from *		Loca		mote C	Text						
SSL or CA Cer	tificate *		• SSL	Certificat	e Oca	Certifica	te					
CSR Generate												
Certificate For	mat		PFX									\checkmark
PFX Password												
Certificate Sou	rce *		C:\Tem	np\server	cert.gleas	; 参照						
											取り消し	Import

インポートが終了すると、以下のように表示されます。 正しくインポートされているか確認します。

AIE	Dashboard	★ <u>ADC</u> ★	GSLB ▾ WAF ▾ AAM ▾	CGN - Net	work 👻 System 👻 Inte	egration -	Partition: shared	·~ @ ~ (0 🖹 🛔 🕩		
SSL Certificates	Cert Revo	ocation List	Expiration Email					AXvThunder 4	4.0.1 build 214		
ADC >> SSL M	anagement	>> SSL Cer	tificates						Help		
Certificate Name - Search Search Reset											
SSL Ce Na	ertificate ime	Туре	Common Name	Organization	Expiration		Issuer				
servercert-	gleas	certificate/key	/ servercert.gleas.example		Jul 6 14:20:45 2018 GMT	/CN=JCCH SSS	I-SSS demo CA/[)C=COM/DC	=JCCH-		
First Prev	vious 1	Next Las	st Page 1 of	1 Go			Total 1 it	em, Items pe	r page: 25		

2.2. ルート証明書のインポート

本手順前に、Gléas のよりルート証明書(PEM フォーマット)をダウンロードします。

※デフォルトのルート証明書は以下 URL よりダウンロード可能です。

http://hostname/crl/ia1.pem

2.1 項と同じく SSL Certificates の画面を表示させ、[Import]をクリックします。 Import の画面より以下の通りにして、[Import]をクリックします。

- [File Name]: このルート証明書の任意の名称を入力
- [Import] : [Certificate]を選択
- [Import Certificate from]: [Local]を選択
- [SSL or CA Certificate]: [CA Certificate]を選択
- [Certificate Format]: [PEM]を選択
- [Certificate Source]: Gléas よりダウンロードしたファイルを指定

All	Dashboard ▼ <u>ADC</u> ▼	GSLB → WAF → AAM → CGN →	Network - System	 Integration - 	Partition: shared 🗸 🤪 🔪	 • • • • • • • • • • • • • • • • • • •
SSL Certificates	Cert Revocation List	Expiration Email			AXvThund	ler 4.0.1 build 214
ADC >> SSLM	anagement >> SSL C	rtificates >> Import				Help
SSL Certif	icates					
File Name *		gleas				
Import *		Certificate O Key O Certific				
Import Certific	ate from *	● Local O Remote O Text				
SSL or CA Cer	rtificate *	O SSL Certificate				
CSR Generate						
Certificate For	mat	PEM				\checkmark
Certificate Sou	Irce *	C:\Temp\ia1.cer 参照				
					取り消し	Import
					取り消し	miport

インポートが終了すると、以下のように表示されます。 正しくインポートされているか確認します。

AIR	Dashboard	d ▼ <u>ADC</u> ▼ 0	GSLB → WAF → AAM →	CGN 👻 Net	work 👻 System 👻 Integ	ration -	Partition: share	ed 🗸 🔇 🗸	O 🖹 🛔 🕩
SL Certificates	Cert Rev	ocation List E	Expiration Email					AXvThunder	4.0.1 build 214
DC >> SSL Ma	anagement	t >> SSL Cert	ificates						Help
Certificate Na	me 👻	Search	Search	Reset	C Refresh	💼 Delete	+ Create	≝ Import	
SSL Cer Nar	rtificate me	Туре	Common Name	Organization	Expiration		Iss	uer	
servercert-g	gleas	certificate/key	servercert.gleas.example		Jul 6 14:20:45 2018 GMT	/CN=JCCH SSS	I-SSS demo CA	VDC=COM/D	C=JCCH-
☐ gleas		CA- Certificate	JCCH-SSS demo CA		Jan 6 15:46:45 2030 GMT	/CN=JCCH SSS	I-SSS demo CA	VDC=COM/D	C=JCCH-
First Prev	ious 1	Next Last	t Page 1 of 1	Go			Total 2 i	tems, Items p	er page: 25

2.3. 失効リスト(CRL)のインポート

• [Source] :

本手順前に、Gléas より CRL(PEM フォーマット)をダウンロードします。 ※デフォルトの CRL は以下 URL よりダウンロード可能です。 http://hostname/crl/crl_ia1.pem

2.2 項と同じく SSL Management の画面を表示させ上部メニューより[Cert Revocation List]をクリックし、[Import]をクリックします。
 Import の画面より以下の通りにして、[Import]をクリックします。

- [Local or Remote]: [Local]を選択
- [Name]: 任意の識別名を入力
 - Gléas よりダウンロードしたファイルを指定

AI	Dashboard 👻	<u>ADC</u> -	GSLB 🗸	WAF -	AAM 🗸	CGN 🗸	Network 👻	System 👻	Integration -	Partition: shared 🗸 🤪 🗸 🖨 🖺	•		
SSL Certificates	Cert Revocat	ion List	Expiration	Email						AXvThunder 4.0.1 build	214		
DC >> SSL Management >> Cert Revocation List >> Import													
Cert Revoo	ation List												
Local or Remo	te *		• Loca		mote								
Name *			gleas_crl										
Source *			C:\Tem	np\crl_ia1	.cer	参照							
										取り消し Import			

インポートが終了すると、以下のように表示されます。 正しくインポートされているか確認します。

AIB	Dashboard ▼ <u>ADC</u> ▼	GSLB → WAF → AAM → CG	N 👻 Network 👻 System 👻	Integration -	Partition: shared 🗸 🤮 🗸	• 🗘 🖺 🖀 🗭
SSL Certificates	Cert Revocation List	Expiration Email			AXvThund	er 4.0.1 build 214
ADC >> SSL M	anagement >> Cert R	evocation List				Help
File Name -	Search	Search Reset		C Refresh	n 💼 Delete 🖆 Import	
	Cert Revocation		ŀ	ssuer		
gleas_c	rl	/CN=JCCH-SSS demo CA	/DC=COM/DC=JCCH-SSS			
First Prev	rious 1 Next L	ast Page 1 of 1 G	D		Total 1 item, Items	per page: 25

CRL は Thunder ADC 側で自動的に更新されるわけではないので、Gléas で CRL が 更新されたらインポート及びテンプレートへの適用操作を再度おこなう必要があり ます。

※CRLの有効期限を過ぎてしまうと、証明書認証をすべて停止するので注意が必要です

また Thunder ADC の仕様では、OCSP(Online Certificate Status Protocol)をサポ ートしております(弊社未検証)。

2.4. SSL テンプレートの設定

[ADC] > [Templates] > [SSL]をクリックし SSL テンプレートの画面に進み、[Create] > [Client SSL]をクリックします。

以下の通り設定します。

•	[Name] :	任意の識別名を入力
•	[CA Certs] > Name :	2.2 項でインポートしたルート証明書名を選択
•	[CA Certs] > Client OCSP :	[Disable]を選択
	その後、[Add]をクリック	
•	[Server Certificate] :	2.1 項でインポートしたサーバ証明書名を選択
•	[Server Private Key] :	2.1 項でインポートしたサーバ証明書名を選択
•	[Client Certificate] :	[Require]を選択
•	[Close Notify] :	チェック
•	[Cert-Revocation List] :	2.3 項でインポートした CRL 名を選択

プライベート CA Gléas ホワイトペーパー Thunder ADCにおけるクライアント証明書認証の設定手順

		General Fields			
Name *	clientcert auth				
Auth Username					
	subject-alt-name	-email			
	□ subject-alt-name	othername			
CA Certs	✓	Enable 🗸	~		Add
			011 (0.000	017 (0000	
	Name	Client OCSP	Service Group	Server	
	dloac	Disable			
	gieas	Disable			
Chain Certificate					\checkmark
Server Certificate	servercert-gleas				\checkmark
Server Private Key	servercert-gleas				
Server Private Key					
Password Phrase					
Server Name List		servercert-gleas 🗸	servercert-gleas		Add
				11 ⁰	
	Name	Cert	Private Key	ハスリード	
Cipher Selection	Individual Ciphers	Cipher Template			
Cipher without Priority List					
		2_0003_011X		•	Add
	Cipher without Price	ority			
		-			
Client Certificate	Require				\checkmark
Close Notify	\checkmark				
Cert-Revocation List	gleas_crl				\checkmark
Forward Proxy CA Cert					\checkmark
Forward Proxy CA Private Key					\checkmark
Forward Proxy CA Private Key Pass Phrase					
Forward Proxy Enable					
Session Cache Size					
session Cache Timeout seconds)					
Session Ticket Lifetime seconds)					
SSL False Start					
Reject Client Requests for SSLv3					
Service Group Bypass SSLv2					\checkmark
EC Name X9_62_prime256v1					
EC Name secp384r1					
	Fo	rward Proxy Bypass			G
	Forward	Proxy Bypass Client	Auth		8
		OCSP			6

Cancel OK

設定後、[OK]をクリックします。以下のように表示されます。

ŀ	AID.) Da	ashboard 👻	<u>ADC</u> ▼	GSLB	▼ W.	AF 👻	AAM 👻	CGN 👻	Network 👻	System 👻	Integration -	Partition: s	hared 🗸	@ ~	• 🤀 [2 🔒 🗭
SLB	Appl	ication	Persistence	L4 Pro	tocols	L7 Pr	rotocols	SSL	Genera	I				AXv	Thund	er 4.0.	1 build 214
ADO	; >> T	emplates	>> SSL														Help
	Name -	•											C Refresh	a Del	lete	+ Ci	reate 🕶
	Search	h													Sear	ch	Reset
			Name				Ту	ре		Total Configured Items Actions						IS	
		clientcert_	auth			Client	SSL							0		Edit	
	First	Previous	5 1 N	lext La	ast Pa	ige	1	of 1	Go				Tot	al 1 item,	Items	per pa	ige: 25

2.5. バーチャルサービスへのテンプレートの適用

[ADC] > [SLB] > [Virtual Service]をクリックし、クライアント証明書認証を適用する バーチャルサーバのポートの[Edit]をクリックします。

Update Virtual Service 画面の Template を展開し、以下を設定します。

● [Template Client SSL]: 2.4 項で設定したテンプレート名を選択

	Templates	
Template Virtual Port		✓ Add+
Template Policy		V Add+
Template Scaleout		~
Template Connection Reuse		V Add+
Template Client SSL	clientcert_auth	V Add+
Template Cache		V Add+
Template TCP Proxy Client		V Add+
Template HTTP		V Add+
Template WAF		\checkmark
Template TCP Proxy Server		V Add+
Template External Service		V Add+
Template HTTP Policy		\checkmark
Template Server Ssl		V Add+
Template TCP Proxy		V Add+
Persist Type	O Destination IP O Source IP O Cookie	
	取り消し	Update

設定後、[Update]をクリックします。

以上で、Thunder ADC の設定は終了です。必要に応じて、 ^{四 森}をクリックして設 定を保存します。 プライベート CA Gléas ホワイトペーパー Thunder ADCにおけるクライアント証明書認証の設定手順

3. Gléas の管理者設定 (PC)

GléasのUA(申込局)より発行済み証明書をiPadにインポートできるよう設定します。

※下記設定は、Gléas納品時などに弊社で設定をおこなっている場合があります

3.1. UA (ユーザ申込局) 設定

GléasのRA(登録局)にログインし、画面上部より[認証局]をクリックし[認証局一 覧]画面に移動し、設定を行うUA(申込局)をクリックします。



[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

▶ 証明書ストアへのインボート	証明書ストアの種類	ユーザストア	•
□ ダウンロードを許可	🗹 インボートワンスを利用す	ta	

設定終了後、[保存]をクリックし設定を保存します。 各項目の入力が終わったら、 [保存]をクリックします。

4. PC からの接続操作

4.1. クライアント証明書のインポート

Internet Explorer で Gléas の UA サイトにアクセスします。 ログイン画面が表示されるので、ユーザ ID とパスワードを入力しログインします。

●エンドユーザログイン [UA]
● ユーザID、パスワードを入力して口 ダインしてください。
▶ユ-ザID
▶パスワード
ログイン
□ <u>ユーザID・バスワードを忘れたら…</u>

ログインすると、ユーザ専用ページが表示されます。

[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポート が行われます。

※初回ログインの際は、ActiveX コントロールのインストールを求められるので、画面の指示に 従いインストールを完了してください。

ユーザ情報				
2 ユーザ	01 さんのページ	_	_	_
2ユーザ情	≣幸 ₩ · · · · · · · · · · · · · · · · · · ·			~
▶ユーザ	登録日時:2011/07/	19 13:48		
> ユーザID : user01 > パスワード:**********				
証明書情	5 幸 尼 · · · · · · · · · · · · · · · · · · ·			
▶発行済み証	明書			
#	発行局	シリアル	有効期限	証明書ストアヘインポート
<u>\$</u>1	JCCH-SSS demo CA	#10865	2017/04/21	証明書のインポート

「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログ アウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、 再度のインポートを行うことはできません。

ーザ情報				
🤰 ユーザ (D1 さんのページ			
	**			
ユーサ情	「辛饭 · · · · · · · · · · · · · · · · · · ·			
▶ユーザ	登録日時:2011/07/19	13:48		
>ユーザID:u >バスワード:	ser01			
、証明書情	報			
▶発行済み訂	明 妻			
#	発行局	ジリアル	有効期限	証明書ストアヘインポート
<u>\$1</u>	JCCH-SSS demo CA	#10865	2017/04/21	ダウンロード済み

4.2. Web サーバへの接続

Thunder ADCのバーチャルサーバにWebブラウザで接続します。

クライアント証明書の提示を求められるので提示をするとWebページが表示されます。



証明書を持っていない場合や、失効済みの証明書の場合はエラー表示となります。 以下は失効された証明書を提示した場合の表示となります。

8	この Web サイトのセキュリティ証明書には問題があります。
	この組織の証明書は失効しています。
	セキュリティ証明書の問題によって、詐欺や、お使いのコンピューターからサーバーに送信される情報 を盗み取る意図が示唆されている場合があります。
	このページを閉じて、この Web サイトの閲覧を続行しないことを推奨します。
	🥺 ここをクリックしてこの Web ページを閉じる。
	● 詳細情報

5. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Thunder ADCに関するお問い合わせ

A10ネットワークス株式会社 Tel: 03-5777-1995 Mail: jinfo@a10networks.com

■Gléasや検証用の証明書に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ

- Tel: 03-5615-1020
- Mail: sales@jcch-sss.com