



JCCH・セキュリティ・ソリューション・システムズ

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。

目次

1. はじめに	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	5
2. Thunder 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. Gléas の管理者設定 (PC)	12
3.1. UA (ユーザ申込局) 設定	12
4. PC からの接続操作	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。

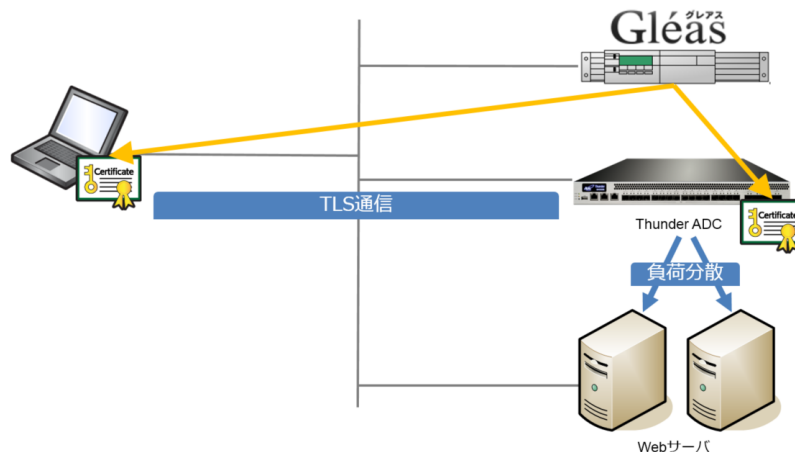
- ロードバランサー：A10 Thunder ADC (AX vThunder 4.0.1 build214)
※以後、「Thunder ADC」と記載します
- JS3 プライベートCA Gléas (バージョン1.12)
※以後、「Gléas」と記載します
- Webサーバ：Ubuntu 14.04.2 LTS / Apache/2.4.7
- クライアント：Windows 8.1 Pro / Internet Explorer 11
※以後、「PC」と記載します

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



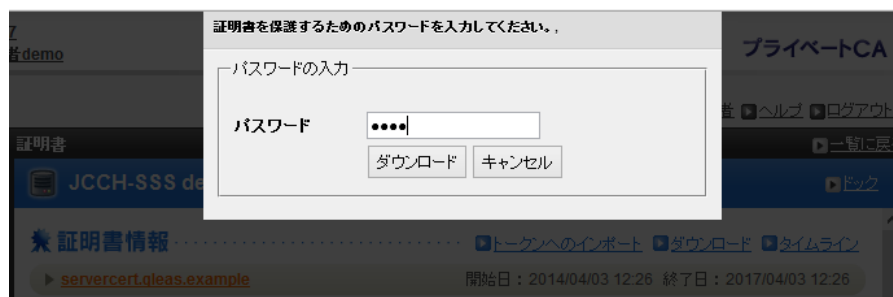
1. Gléasでは、Thunder ADCにサーバ証明書を、PCにクライアント証明書を発行する
2. PCはThunder ADC経由で冗長化されたWebサーバにhttpsでアクセスする。Thunder ADCはTLS通信を終端し、またクライアント証明書を要求する。PCは有効なクライアント証明書がないと負荷分散されたWebサーバに接続することができない

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。



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

Thunder 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] : Gléas よりダウンロードしたファイルを指定

SSL Certificates

File Name * servercert-gleas

Import * Certificate Key Certificate and Key

Import Certificate from * Local Remote Text

SSL or CA Certificate * SSL Certificate CA Certificate

CSR Generate

Certificate Format PFX

PFX Password

Certificate Source * C:\Temp\servercert.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。

SSL Certificates

ADC >> SSL Management >> SSL Certificates

Certificate Name Search Search Reset Refresh Delete Create Import Export

<input type="checkbox"/>	SSL Certificate Name	Type	Common Name	Organization	Expiration	Issuer
<input type="checkbox"/>	servercert-gleas	certificate/key	servercert.gleas.example		Jul 6 14:20:45 2018 GMT	/CN=JCCH-SSS demo CA/DC=COM/DC=JCCH-SSS

First Previous 1 Next Last Page 1 of 1 Go Total 1 item, Items per 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

File Name *

Import * Certificate Key Certificate and Key

Import Certificate from * Local Remote Text

SSL or CA Certificate * SSL Certificate CA Certificate

CSR Generate

Certificate Format

Certificate Source *

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。

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

SSL Certificate Name	Type	Common Name	Organization	Expiration	Issuer
servercert-gleas	certificate/key	servercert.gleas.example		Jul 6 14:20:45 2018 GMT	/CN=JCCH-SSS demo CA/DC=COM/DC=JCCH-SSS
gleas	CA-Certificate	JCCH-SSS demo CA		Jan 6 15:46:45 2030 GMT	/CN=JCCH-SSS demo CA/DC=COM/DC=JCCH-SSS

2.3. 失効リスト（CRL）のインポート

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
- [Source] : Gléas よりダウンロードしたファイルを指定

Local or Remote * Local Remote

Name *

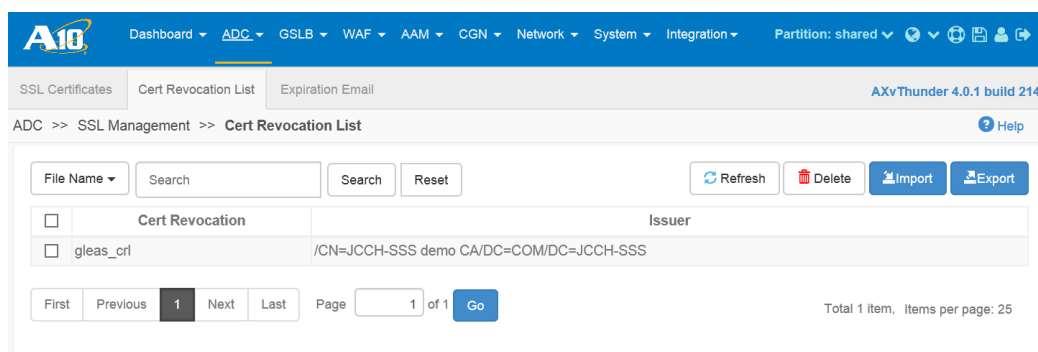
Source * 参照...

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。

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



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

Create Client SSL Template

General Fields -

Name *

Auth Username
 common-name
 subject-alt-name-email
 subject-alt-name-othername

CA Certs
 Enable Add

Name	Client OCSP	Client OCSP Service Group	Client OCSP Server	
gleas	Disable			✎ ✕

Chain Certificate

Server Certificate

Server Private Key

Server Private Key Password Phrase

Server Name List
 Add

Name	Cert	Private Key	パスワード	

Cipher Selection
 Individual Ciphers Cipher Template

Cipher without Priority List
 Add

Cipher without Priority	

Client Certificate

Close Notify

Cert-Revocation List

Forward Proxy CA Cert

Forward Proxy CA Private Key

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

EC Name X9_62_prime256v1

EC Name secp384r1

Forward Proxy Bypass +

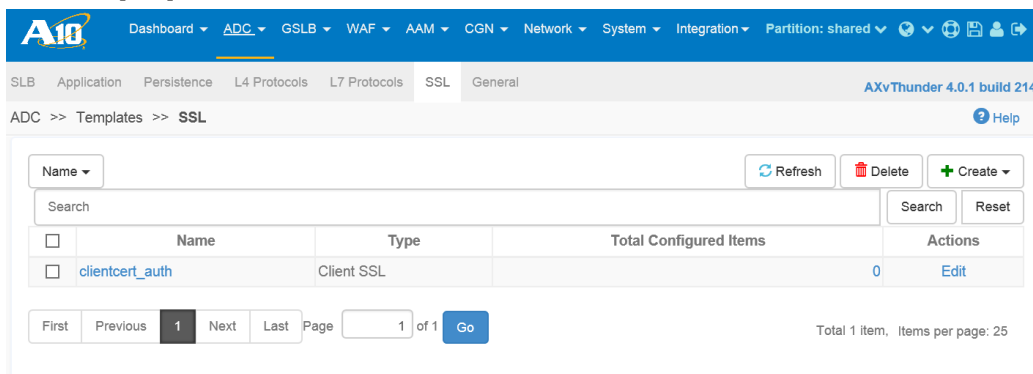
Forward Proxy Bypass Client Auth +

OCSP +

LDAP +

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

設定後、[OK]をクリックします。以下のように表示されます。

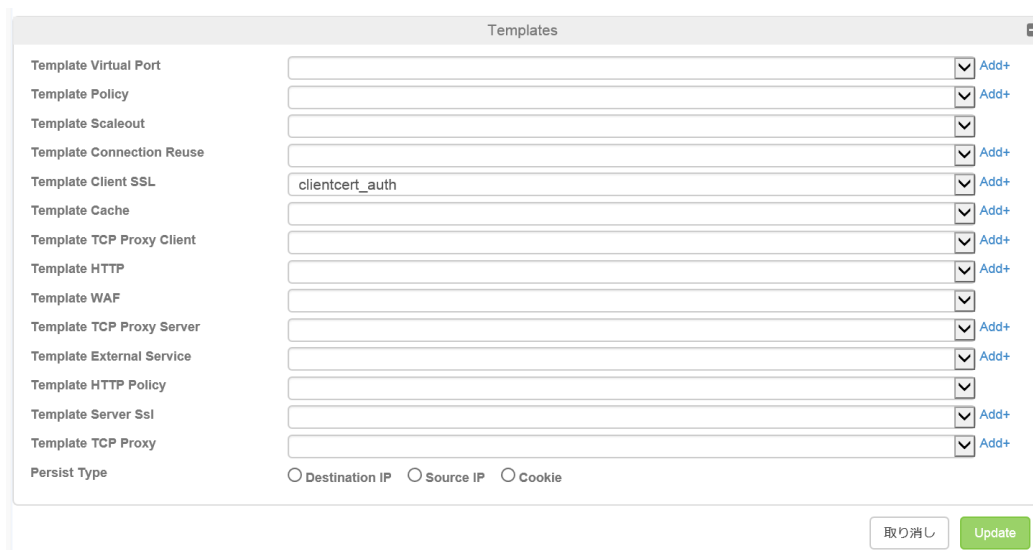


2.5. バーチャルサービスへのテンプレートの適用


[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ビスのポートの[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



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、 をクリックして設定を保存します。

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に設定します。

※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



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。

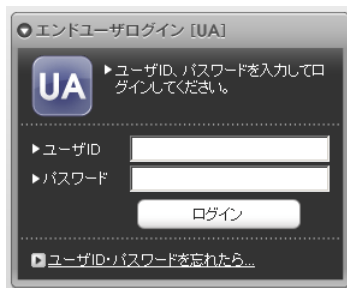
4. PC からの接続操作

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。

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



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。

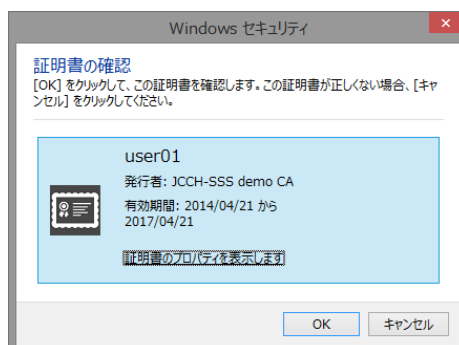


「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません。

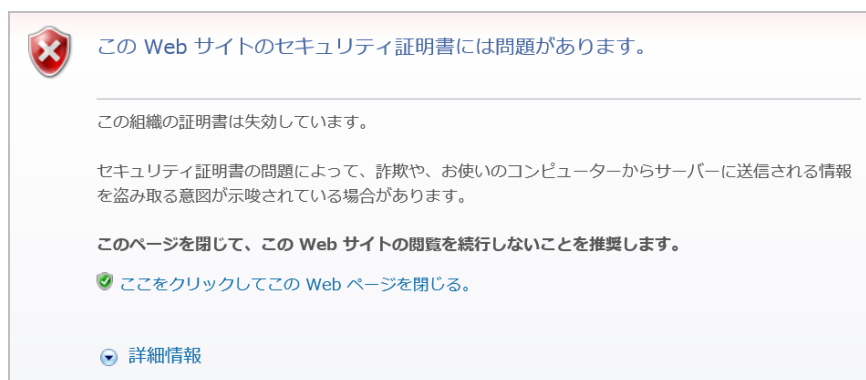


4.2. Web サーバへの接続

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。



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

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

■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