



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

BIG-IP Local Traffic Manager (LTM) での

ロードバランシングにおけるクライアント証明書認証

Ver.1.0

2023年3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	5
1.1. 本書について	5
1.2. 本書における環境	6
1.3. 本書における構成	8
1.4. 証明書発行時における留意事項	9
2. BIG-IP の設定	10
2.1. サーバ証明書の発行と登録	10
2.2. ルート証明書の登録	17
2.3. 失効リスト (CRL) の登録	19
2.4. SSL プロファイルの登録	22
2.5. バーチャルサーバの設定	25
2.6. リクエストヘッダにクライアント証明書情報を挿入	27
3. Gléas の管理者設定 (Windows 向け)	31
4. クライアントの設定 (Windows)	33
4.1. クライアント証明書のインポート	33
4.2. サーバアクセス	35

5. Gléas の管理者設定 (iPhone 向け)	37
6. クライアントの設定 (iPhone)	40
6.1. クライアント証明書のインポート	40
6.2. サーバアクセス	43
7. Web サーバでクライアント証明書情報を取得	45
8. 問い合わせ	47

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利用して、F5ネットワークス株式会社の BIG-IP Local Traffic Manager (LTM) で SSLオフレードしたロードバランシング (Web負荷分散) 構成で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

本書は、以下の環境で検証をおこなっております。

➤ SSLロードバランサー

BIG-IP Local Traffic Manager (BIG-IP Virtual Edition 16.1.3.2 Build 0.0.4)

※以後、「LTM」と記載します

➤ 認証局 : JS3 プライベートCA Gléas (バージョン2.5.1)

※以後、「Gléas」と記載します

➤ Webサーバ : CentOS7.5.1804 / Apache 2.4.6

※以後、「Webサーバ」と記載します

➤ クライアント : Windows10 Pro 22H2 / Microsoft Edge 108.0.1462.46

※以後、「Windows」と記載します

➤ クライアント : iPhone8 (iOS 15.3.1) / Safari

※以後、「iPhone」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。

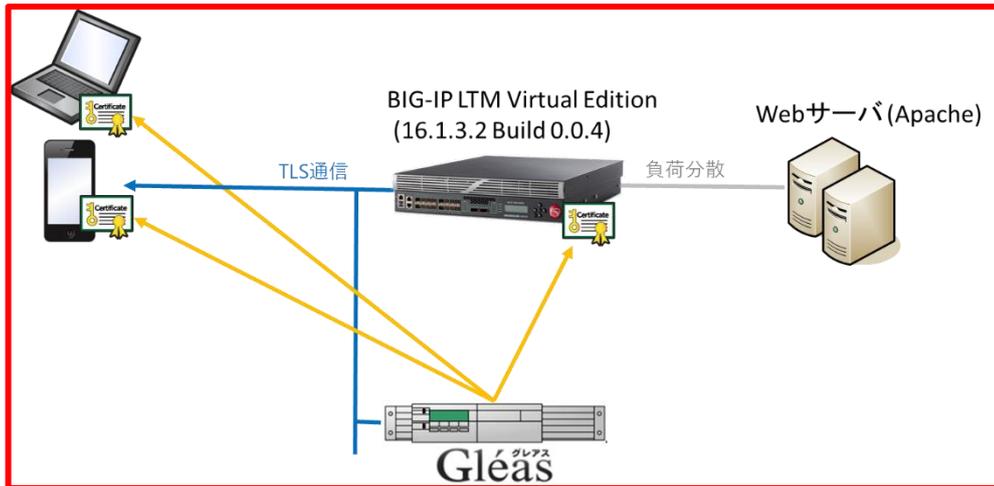
- LTMの基本設定 (ネットワークや基本的な負荷分散に関する設定)
- Webサーバの基本設定 (ネットワークや基本的なWebページ公開設定)
- Gléasでのユーザ登録やクライアント証明書発行などの基本操作

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、LTMにサーバ証明書を、PCとiPhoneにクライアント証明書を発行する。
2. PCとiPhoneはGléasより証明書をインポートする。
3. PCではEdgeブラウザ、iPhoneではSafariブラウザよりLTM経由で冗長化されたWebサーバにHTTPSでアクセスする。

LTMはTLS通信を終端し、クライアント証明書認証を行う。

証明書認証後にロードバランスしているWebページをクライアントに表示。

証明書を提示しない、期限切れ、または失効している、端末はクライアント証明書認証に失敗。

1.4. 証明書発行時における留意事項

Gléasで電子証明書を発行する際に以下の点に留意する必要があります。

- 本書2.1の方法でサーバ証明書を発行する場合は、事前にサーバアカウントを作成しておき、[SSLサーバ証明書]ロールグループに参加させる必要があります。

2. BIG-IP の設定

2.1. サーバ証明書の発行と登録

バーチャルサーバで使用するサーバ証明書をGléasから発行し、LTM に登録します。

LTM管理画面の左側メニューから [System] > [Certificate Management] > [Traffic Certificate Management] > [SSL Certificate List] と進み、右上にある [Create...] ボタンをクリックします。

その画面で以下を入力し、鍵ペアを生成します。

- General Properties欄の[Name]には、任意の識別名を入力
- Certificate Properties欄の[Issuer]には、[Certificate Authority]を指定
- Certificate Properties欄の[Common Name] には、バーチャルサーバのFQDNを入力
- Key Properties欄の[Key Type]には、[RSA]を指定
- Key Properties欄の[Size]には、[2048]を指定
- 他の項目は、環境に応じて設定

※以下は、2048bitのRSA秘密鍵で証明書発行リクエスト(CSR)を生成する例。

System » Certificate Management : Traffic Certificate Management : SSL Certificate List » New SSL Certificate...

General Properties

Name: ServerCert_by_Gleas

Certificate Properties

Issuer: Certificate Authority

Common Name: itm-test.jcch-sss.local

Division:

Organization: JCCH Security Solution Systems

Locality:

State Or Province:

Country: Japan JP

E-mail Address:

Subject Alternative Name:

Basic Constraints: CA, pathlen:

Key Usage:

Selected:

Available:

- nonRepudiation
- keyAgreement
- decipherOnly
- cRLSign
- digitalSignature
- keyEncipherment
- keyCertSign
- dataEncipherment
- encipherOnly

Certificate Signing Request Attributes

Administrator E-mail Address:

Challenge Password:

Confirm Password:

Key Properties

Key Type: RSA

Size: 2048 bits

Certificate Order Properties

Certificate Order Manager: None

Cancel Finished

入力後、[Finished]ボタンをクリックします。

CSR が発行されるので、Request File 欄にある[Download...]ボタンより CSR ファイルをダウンロードします。

System » Certificate Management : Traffic Certificate Management : SSL Certificate List » Certificate Signing Request	
Certificate Signing Request	
Request Text	-----BEGIN CERTIFICATE REQUEST----- MIICnTCCAAYUCAQAwwDELMAkGA1UEBhMC! dHkgU29sdXRpb24gU31zdGVtczEgMB4G! bG91YWVwggE1MA0GCsgGSIB3DQEBAAQU! IaC+AHN6ovpJd+ZIFbOa/64Az1mS2J66! BOH00FgN4zN07W0T1+Rm/QA4acLi13J1! aRBLHITOWdAA7cYQZgWZq3zRoaG/VtgB: -----
Request File	Download ServerCert_by_Gleas
Certificate Authorities	IdenTrust Entrust GlobalSign VeriSign
Finished	

ダウンロードが完了したら、[Finished...]ボタンをクリックします。

Gléas (RA) にログインし、該当のサーバアカウントのページへ移動します。

サーバ属性の[編集] をクリックし、ホスト名に公開するバーチャルサーバの FQDN を
入力します。

小メニューの[証明書発行]をクリックします。



上級者向け設定を展開し、以下の操作をおこないます。

- 証明書要求 (CSR) ファイルをアップロードする : の[参照...]ボタンよりダウンロードした CSR ファイルを選択
 - [CSR ファイルの内容を確認する]にチェック
- その後、[発行]ボタンをクリックします。

プライベート CA Gléas ホワイトペーパー BIG-IP LTM でのクライアント証明書認証



証明書の要求内容が表示されるので確認し、**[この内容で発行する]**をクリックし、証明書の発行をおこないます。



証明書発行完了後、証明書詳細画面の証明書ファイル欄の「証明書：あり」をクリックし、発行された証明書をダウンロードします。

プライベート CA Gléas ホワイトペーパー
BIG-IP LTM でのクライアント証明書認証

The screenshot displays the Gléas RA web interface for a private CA. The main content area shows details for a certificate issued by 'JCCH-SSS demo CA#156' to the subject 'ns.js3.test.xen.local'. The interface is organized into several sections:

- 証明書情報 (Certificate Information):** Displays the subject 'ns.js3.test.xen.local' and the start/end dates: '開始日: 2016/10/24 17:27' and '終了日: 2019/10/24 17:27'.
- サブジェクト (Subject):** Lists attributes: '国: JP', '都道府県: Tokyo', '組織: JS3', and '一般名: ns.js3-test-xen.local'.
- 基本情報 (Basic Information):** Lists: '作成日: 2016/10/24 17:26', '有効日数: 1095', '失効日:', '失効理由:', '期限終了日:', '状態: 有効な証明書', '処理の状態: 有効な証明書', 'トークン必要:', and 'バージョン: 4'.
- 証明書情報 (Certificate Details):** Lists: '認証局: JCCH-SSS demo CA', '暗号アルゴリズム: rsa', 'ダイジェストアルゴリズム: sha256', '鍵長: 2048', '鍵用途: 電子署名 鍵の暗号化', and '拡張鍵用途: SSLサーバ認証 SSLクライアント認証'.
- 証明書別名 (Certificate Aliases):** Lists the alias: 'DNS名 ns.js3-test-xen.local'.
- 証明書ファイル (Certificate File):** Lists: '証明書要求: あり', '作成日時: 2016/10/24 17:26', '証明書: あり', '作成日時: 2016/10/24 17:28', and '秘密鍵: なし'.

The interface includes a left sidebar with navigation options like 'アカウント', 'グループ', '証明書', '認証デバイス', and 'テンプレート'. The top right shows the user is logged in as 'サイドバー' and provides navigation links for '認証局', 'ログ', '管理者', 'ヘルプ', and 'ログアウト'. The footer contains the text '著作権 © 2010-2016 JCCH Security Solution Systems Co., Ltd. All rights reserved.'

LTM の管理画面に戻ります。

System >> Certificate Management : Traffic Certificate Management : SSL Certificate List >> ServerCert_by_Gleas	
⚙	Certificate
Key	Certificate Signing Request
Instances	

General Properties

Name	ServerCert_by_Gleas
Partition / Path	Common
Certificate Subject(s)	No certificate

Import... Create...

[Import...]ボタンをクリックします。

その画面で以下を入力します。

- [Certificate Source]の[Upload File]を選択
- [Certificate Source]の[ファイルを選択]をクリックし、ダウンロードしたCSRファイルを選択

System >> Certificate Management : Traffic Certificate Management : SSL Certificate List >> /Common/ServerCert_by_Gleas

SSL Certificate/Key Source

Import Type	Certificate
Certificate Name	/Common/ServerCert_by_Gleas
Certificate Source	<input checked="" type="radio"/> Upload File <input type="radio"/> Paste Text ファイルの選択 download.crt
Free Space on Disk	1974 MB

Cancel Import

入力後、[Import]ボタンをクリックするとサーバ証明書が登録されます。

Status	Name	Contents	Key Security	Common Name	Organization	Expiration	Partition / Path
<input checked="" type="checkbox"/>	ServerCert_by_Gleas	RSA Certificate, Key & Certificate Signing Request	Normal	ltn-test.jcch-sss.local	JCCH Security Solution ...	2015-01-01	Common
<input type="checkbox"/>	ServerCert_by_Gleas	RSA Certificate, Key & Certificate Signing Request	Normal	ltn-test.jcch-sss.local	JCCH Security Solution ...	2015-01-01	Common
<input type="checkbox"/>	ServerCert_by_Gleas	RSA Certificate, Key & Certificate Signing Request	Normal	ltn-test.jcch-sss.local	JCCH Security Solution ...	2015-01-01	Common
<input type="checkbox"/>	ServerCert_by_Gleas	RSA Certificate, Key & Certificate Signing Request	Normal	ltn-test.jcch-sss.local	JCCH Security Solution ...	2015-01-01	Common
<input type="checkbox"/>	ServerCert_by_Gleas	RSA Certificate, Key & Certificate Signing Request	Normal	ltn-test.jcch-sss.local	JCCH Security Solution ...	2015-01-01	Common

Archive... View Certificate Order Status... Delete OCSP Cache... Delete...

※Contents 欄に、RSA Certificate, Key and Certificate Signing Request と表示されます。

2.2. ルート証明書の登録

クライアント証明書によるSSL認証を利用するためには、ルート証明書の登録が必要です。これは、クライアントから提示される証明書が正しいことを検証する際に利用するためです。

本手順の前にGléasよりルート証明書をダウンロードします。

※GléasのデフォルトCAのルート証明書 (PEM形式) のダウンロードURLは以下となります
`http://[GléasのFQDN]/crl/ia1.pem`

LTM 管理画面の左側メニューから [System] > [Certificate Management] > [Traffic Certificate Management] > [SSL Certificate List] と進み、右上にある [Import...] ボタン をクリックします。

次の画面で 以下を設定します。

- [Import Type]には、[Certificate]を選択
- [Certificate Name]には、任意の識別名を入力
- [Certificate Source]の[Upload File]を選択
- [Certificate Source]の[ファイルを選択]をクリックし、ルート証明書ファイルを選択

プライベート CA Gléas ホワイトペーパー
BIG-IP LTM でのクライアント証明書認証

System » Certificate Management : Traffic Certificate Management : SSL Certificate List » Import SSL Certificates and Keys

SSL Certificate/Key Source

Import Type: Certificate

Certificate Name: New Overwrite Existing
gleasCA

Certificate Source: Upload File Paste Text
ファイルの選択: ia1.pem

Free Space on Disk: 1974 MB

Cancel Import

入力後、[Import]ボタンをクリックするとルート証明書が登録されます。

Status	Name	Contents	Key Security	Common Name	Organization	Expiration	Partition / Path
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input checked="" type="checkbox"/>	gleasCA	RSA Certificate	...	JCCH-SSS demo2 CA	JCCH Security Solution	Common

※Contents 欄に、RSA Certificate と表示されます。

2.3. 失効リスト (CRL) の登録

クライアント証明書によるSSL認証を利用するためには、失効リストの登録が必要です。

これは、クライアントから提示される証明書が失効されていないことを検証する際に利用するためです。

本手順の前にGléasよりルート証明書をダウンロードします。

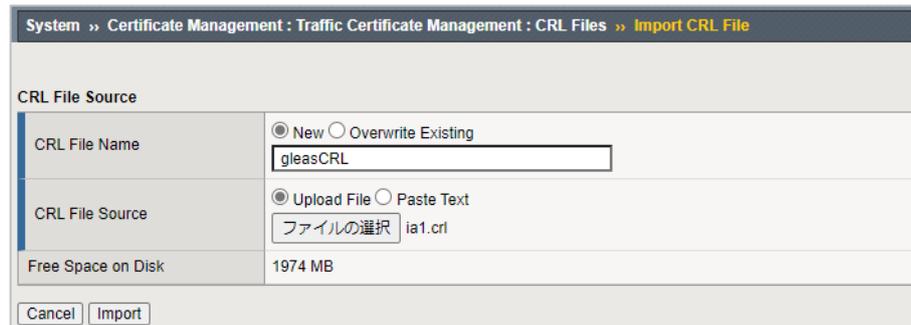
※GléasのデフォルトCAのCRLのダウンロードURLは以下となります。

`http://[GléasのFQDN]/crl/ia1.crl`

LTM 管理画面の左側メニューから [System] > [Certificate Management] > [Traffic Certificate Management] > [CRL Files] と進み、右上にある [Import...] ボタン をクリックします。

次の画面で以下を設定します。

- [CRL File Name]には、任意の識別名を入力
- [CRL File Source]の[Upload File]を選択
- [CRL File Source]の[ファイルを選択]をクリックし、CRLファイルを選択



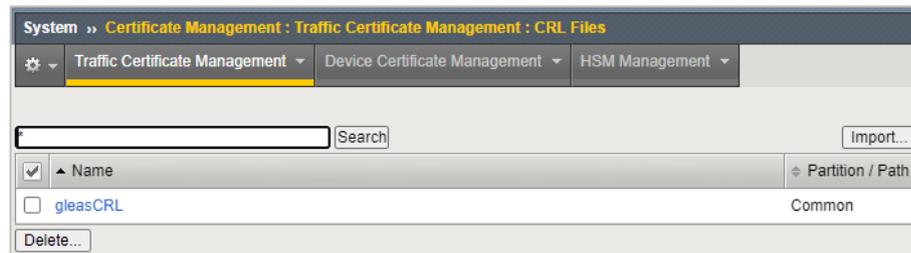
System » Certificate Management : Traffic Certificate Management : CRL Files » Import CRL File

CRL File Source

CRL File Name	<input checked="" type="radio"/> New <input type="radio"/> Overwrite Existing gleasCRL
CRL File Source	<input checked="" type="radio"/> Upload File <input type="radio"/> Paste Text ファイルの選択 ia1.crl
Free Space on Disk	1974 MB

Cancel Import

入力後、[Import]ボタンをクリックするとCRLが登録されます。



System » Certificate Management : Traffic Certificate Management : CRL Files

Traffic Certificate Management Device Certificate Management HSM Management

Search Import...

<input checked="" type="checkbox"/> Name	Partition / Path
<input type="checkbox"/> gleasCRL	Common

Delete...

CRL を更新する場合は、[CRL File Name]で [Overwrite Existing]を選択し、更新された CRL ファイルをアップロードします。

CRL 更新は BIG-IP の管理用シェル (tmsh) からおこなうことも可能です。

以下はコマンド例です。

```
/bin/tmsh modify /sys file ssl-crl gleasCRL source-path http://[Gléas の FQDN]/crl/ia1.crl
```

※crontab で上記を実行することで、CRL の定期取得をおこなう設定をすることも可能です

※利用中の CRL は、以下コマンドで確認することが可能です

```
/bin/tmsh list /sys file ssl-crl gleasCRL
```

また失効確認には、LDAP (Lightweight Directory Access Protocol) や OCSP

(Online Certificate Status Protocol) を利用する方法もあります。

2.4. SSLプロファイルの登録

バーチャルサーバでクライアント証明書認証を行うためのSSLプロファイルを作成します。

LTM 管理画面の左側メニューから [Local Traffic] > [Virtual Servers] > [Profiles] >

[SSL] > [Client] と進み、右上にある [Create...] ボタン をクリックします。

次の画面で以下を設定します。

- General Properties 欄の[Name]には、任意の識別名称を入力
- General Properties 欄の[Parent Profile]には、[clientssl]を選択
- Configuration 欄の[Custom]をチェック
- Configuration 欄の[Certificate Key Chain]の[Add]ボタンをクリック

- ダイアログで以下を入力

Certificate : 2.1 項で登録したサーバ証明書

Key : 2.1 項で登録したサーバ証明書

Chain : 2.2 項で登録したルート証明書



Add SSL Certificate Key Chain	
Certificate	ServerCert_by_Gleas
Key	ServerCert_by_Gleas
Chain	gleasCA
Passphrase	

[Add]ボタンをクリック

- Client Authentication 欄の[Custom]をチェック
- Client Authentication 欄の[Client Certificate] には、[require]を選択
- Client Authentication 欄の[Trusted Certificate Authorities] には、2.2 項で登録したルート証明書を選択
- Client Authentication 欄の[Advertised Certificate Authorities] には、2.2 項で登録したルート証明書を選択
- Client Authentication 欄の[CRL File] には、2.3 項で登録した CRL を選択
- Client Authentication 欄の[Allow Expired CRL]を必要に応じチェック (弊社未検証)

プライベート CA Gleas ホワイトペーパー
BIG-IP LTM でのクライアント証明書認証

Local Traffic » Profiles : SSL : Client » New Client SSL Profile...

General Properties

Name: js3-test-clientssl
Parent Profile: clientssl

Configuration: Basic Custom

Certificate Key Chain: /Common/ServerCert_by_Gleas /Common/ServerCert_by_Gleas /Common/gleasCA

OCSP Stapling:
Notify Certificate Status to Virtual Server:
Proxy SSL:
Proxy SSL Passthrough:

Client Authentication Custom

Client Certificate: require
Frequency: once
Retain Certificate: Enabled
Certificate Chain Traversal Depth: 9
Trusted Certificate Authorities: gleasCA
Advertised Certificate Authorities: gleasCA
CRL: None
CRL File: gleasCRL
Allow Expired CRL File:

入力後に、[Finished] (或いは、[Update]) ボタンをクリックすると SSL プロファイル
が登録されます。

Local Traffic » Profiles : SSL : Client

Services Content Persistence Protocol SSL
Authentication Message Routing Other

Search Create...

Name	Application	Parent Profile	Partition / Path
...
...
...
...
js3-test-clientssl	clientssl	clientssl	Common
...
...

Delete...

2.5. バーチャルサーバの設定

バーチャルサーバにSSLプロファイルを適用してクライアント証明書認証を行うように設定します。

本手順の前にWebサーバにロードバランスするバーチャルサーバを作成しておきます。

LTM 管理画面の左側メニューから [Local Traffic] > [Virtual Servers] > [Virtual Server List] と進み、クライアント証明書認証を適用するバーチャルサーバをクリックします。

選択したバーチャルサーバの以下を変更します。

- General Properties 欄の[Service Port]を HTTPS (443) に設定
- Configuration 欄の[SSL Profile (Client)]に 2.4 項で登録した SSL プロファイルを選択

プライベート CA Gléas ホワイトペーパー
BIG-IP LTM でのクライアント証明書認証

The screenshot shows the 'General Properties' configuration for a virtual server named 'js3-test-vs'. The configuration includes:

Name	js3-test-vs
Partition / Path	Common
Description	テスト用
Type	Standard
Source Address	Host <input type="radio"/> Address List <input type="radio"/> <input type="text" value="0.0.0.0"/>
Destination Address/Mask	Host <input type="radio"/> Address List <input type="radio"/> <input type="text"/>
Service Port	Port <input type="radio"/> Port List <input type="radio"/> <input type="text" value="443"/> <input type="text" value="HTTPS"/>
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
Availability	<input checked="" type="radio"/> Available (Enabled) - The virtual server is available
Synccookie Status	Inactive
State	Enabled

The screenshot shows the 'Configuration' tab for the virtual server, with the 'Basic' configuration selected. The settings are as follows:

DoH Profile Type	None
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	http
HTTP Profile (Server)	(Use Client Profile)
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
PPTP Profile	None
SSL Profile (Client)	Selected: /Common js3-test-clientssl Available: /Common clientssl, clientssl-insecure-compatible, clientssl-quick, clientssl-secure, crypto-server-default-clientssl, splitssession-default-clientssl
SSL Profile (Server)	Selected: (empty) Available: /Common apm-default-serverssl, cloud-service-default-ssl, crypto-client-default-serverssl, do-not-remove-without-replacement, f5aas-default-ssl, pcoip-default-serverssl
SMTSP Profile	None
POP3 Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
Service Profile	None
SMTP Profile	None
TDR Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

入力後、[Update]ボタンをクリックして設定を保存します。

2.6. リクエストヘッダにクライアント証明書情報を挿入

バーチャルサーバでSSLオフロードした場合、ロードバランスしているサーバはクライアント証明書の情報を受け取ることができないため、LTM の iRule 機能を使ってリクエストヘッダを書き換え、サーバにクライアント証明書の情報を送信するように設定します。

まず、iRuleを設定します。

LTM 管理画面の左側メニューから [Local Traffic] > [Virtual Servers] > [iRules] > [SSL] > [Client] と進み、右上にある [Create...] ボタン をクリックします。

次の画面で以下を設定します。

- [Name] には、任意の識別名を設定
- [Definition] に iRule を定義

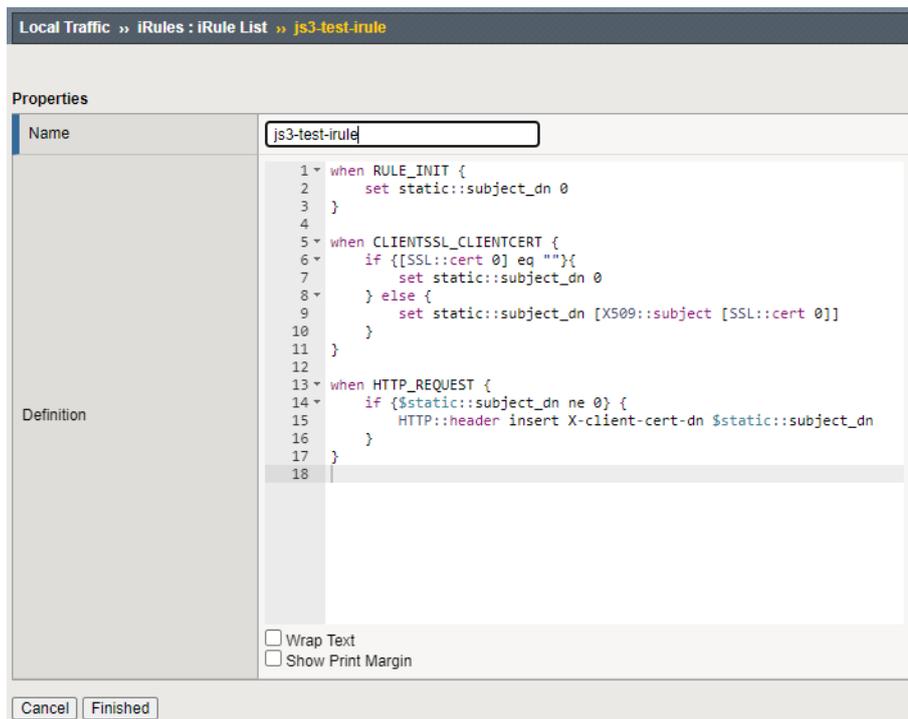
※以下は、Web サーバへのリクエストにクライアント証明書のサブジェクト DN を X-client-cert-dn ヘッダとして挿入する例

```
when RULE_INIT {
    set static::subject_dn 0
}

when CLIENTSSL_CLIENTCERT {
    if {[SSL::cert 0] eq ""} {
        set static::subject_dn 0
    } else {
        set static::subject_dn [X509::subject [SSL::cert 0]]
    }
}

when HTTP_REQUEST {
    if {$static::subject_dn ne 0} {
        HTTP::header insert X-client-cert-dn $static::subject_dn
    }
}
```

プライベート CA Gléas ホワイトペーパー
BIG-IP LTM でのクライアント証明書認証



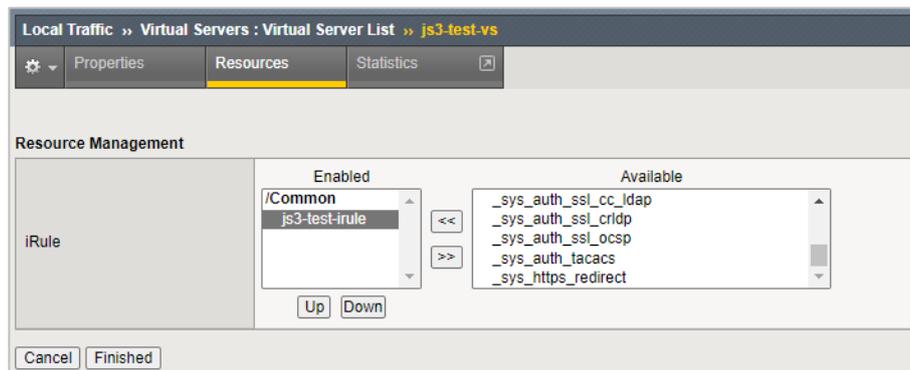
入力後に、[Finished]ボタンをクリックすると iRule が登録されます。

次に、バーチャルサーバにiRuleを適用します。

LTM 管理画面の左側メニューから [Local Traffic] > [Virtual Servers] > [Virtual Server List] と進み、クライアント証明書認証を適用するバーチャルサーバをクリックします。

選択したバーチャルサーバで[Resources] タブを選択し、以下を設定します。

- iRules 欄の[Manage]ボタンをクリック
- Resource Management 欄の[iRule]に登録した iRule を選択



- [Finished]ボタンをクリック

プライベート CA Gléas ホワイトペーパー
BIG-IP LTM でのクライアント証明書認証

Local Traffic » Virtual Servers : Virtual Server List » js3-test-vs

⚙ Properties Resources Security Statistics

Load Balancing

Default Pool	js3-test-pool
Default Persistence Profile	None
Fallback Persistence Profile	None

Update

iRules Manage...

Name
/Common/js3-test-irule

Policies Manage...

Name
No records to display.

入力後、[Update]ボタンをクリックして設定を保存します。

以上でサーバへのWebサーバへのリクエストヘッダにクライアント証明書情報が挿入

されるようにする設定が完了です。

3. Gléas の管理者設定 (Windows 向け)

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

※下記設定は、Gléas納品時等に弊社で設定を既に行っている場合があります

GléasのRA (登録局) にログインします。

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。

※実際はデフォルト申込局ではなく、その他の申込局の設定を編集します



申込局詳細画面が開くので、基本設定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



設定完了後、[保存]をクリックし保存します。

また、認証デバイス設定の以下項目にチェックがないことを確認します。

- iPhone/iPad の設定の、[iPhone / iPad 用 UA を利用する]
- Android の設定の、[Android 用 UA を利用する]

以上でGléasの設定は終了です。

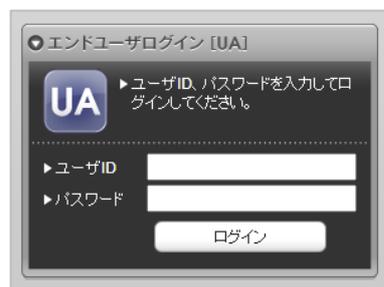
4. クライアントの設定 (Windows)

4.1. クライアント証明書のインポート

PC のブラウザ (Edge) で、UA にアクセスします。

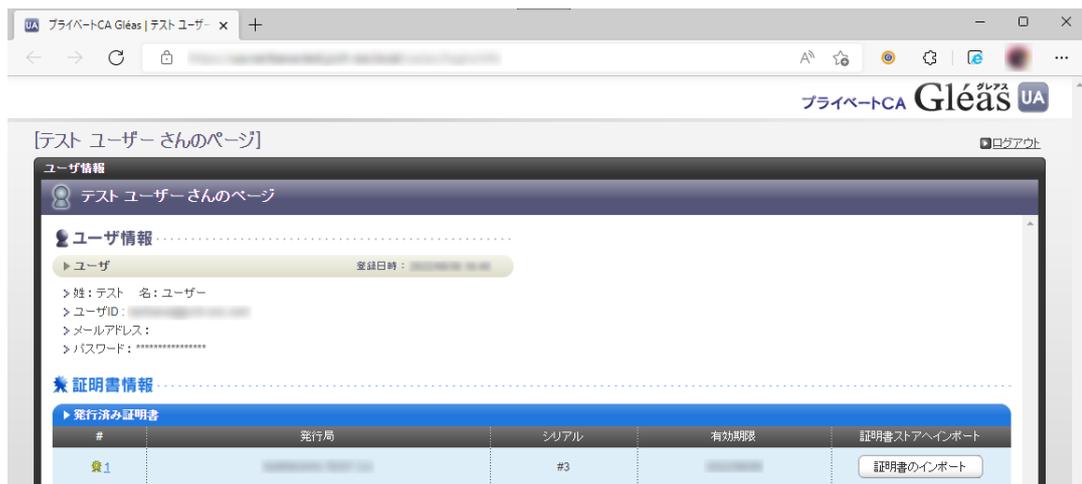
※URL `https://[UA の FQDN]/[UA の名前]/ua`

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。

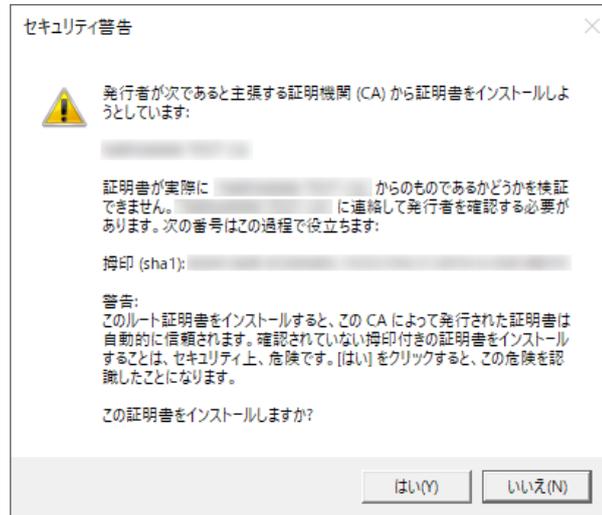


ログインすると、ユーザ専用ページが表示されます。

[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。



※証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印を確認するなど正当性を確認してから[はい]をクリックします

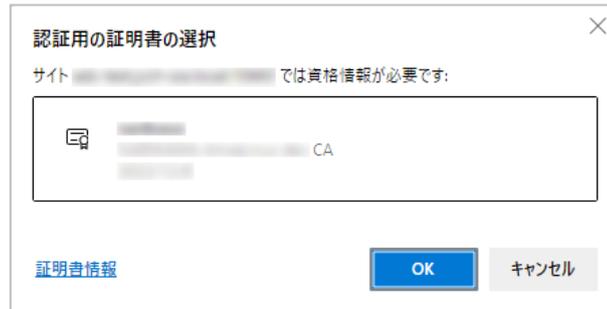


インポートワンス機能を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ログインしてインポートを行うことはできません。



4.2. サーバアクセス

PCのブラウザ (Edge) でLTMのバーチャルサーバのURLにアクセスすると、クライアント証明書の提示を求められます。



[OK]ボタンをクリックし、クライアント証明書認証がおこなわれるとページが表示されます

※以下は7項のCGIを実行するWebページにアクセスしている例



証明書を持っていない場合や、失効された証明書を提示した場合はアクセスに失敗します。

※以下は失効されたクライアント証明書でアクセスした例



5. Gléas の管理者設定 (iPhone 向け)

Gléas で、発行済みのクライアント証明書を iOS にインポートするための設定を本書では記載します。

※下記設定は、Gléas 納品時等に弊社で設定を既に行っている場合があります

GléasのRA (登録局) にログインします。

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。

※実際はデフォルト申込局ではなく、その他の申込局の設定を編集します



[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。

- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック

この設定を行うと、GléasのUAからインポートから指定した時間 (分) を経過した後は、構成プロファイルのダウンロードが不可能になります (インポートロック機能)。これにより複数台のデバイスへの構成プロファイルのインストールを制限することができます。



設定完了後、[保存]をクリックし保存します。

[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UAを利用する]をチェックします。



構成プロファイルに必要なとなる情報の入力画面が展開されるので、以下設定を行います。

【画面レイアウト】

- [iPhone用レイアウトを利用する]をチェック
- [ログインパスワードで証明書を保護]をチェック

【iPhone構成プロファイル基本設定】

- [名前]、[識別子]に任意の文字を入力（必須項目）



認証デバイス情報

iPhone / iPadの設定

iPhone/iPad 用 UA を利用する

画面レイアウト

iPhone 用レイアウトを使用する ログインパスワードで証明書を保護

Mac OS X 10.7以降の接続を許可

OTA(Over-the-air)

OTAエンロールメントを利用する 接続する iOS デバイスを認証する

OTA用SCEP URL

OTA用認証局 デフォルトを利用

iPhone 構成プロファイル基本設定

名前(デバイス上に表示) サンプルプロファイル

識別子(例: com.jcch-sss.profile) local.jcch-sss.profile

プロファイルの組織名 JCCHセキュリティソリューション・システムズ

説明 サンプル構成プロファイル

各項目の入力が終わったら、[保存]をクリックします。

以上でGléasの設定は終了です。

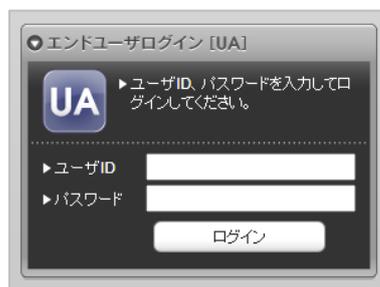
6. クライアントの設定 (iPhone)

6.1. クライアント証明書のインポート

iPhoneのブラウザ (Safari) で、UAにアクセスします。

※URL https://[UA の FQDN]/[UA の名前]/ua

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。



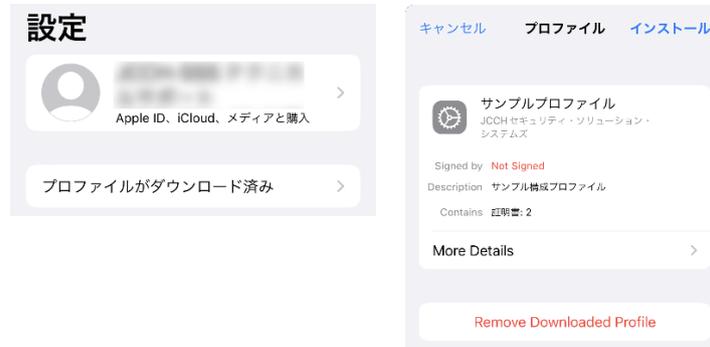
ログインすると、ユーザ専用ページが表示されます。

[ダウンロード]をタップし、構成プロファイルのダウンロードをおこないます。



※ インポートロックを有効にしている場合は、この時点からカウントが開始されます

画面の表示にしたい設定を開くと、プロフィールがダウンロードされた旨が表示されるので、インストールをおこないます。



[インストール]をタップして続行してください。

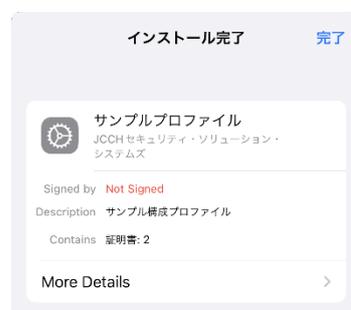
インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[インストール]をタップして続行してください。

※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります



インストール完了画面になりますので、[完了]をタップして終了します。



なお [More Details]をタップすると、インストールされた証明書情報を見ることが
できます。必要に応じて確認してください。



Safariに戻り、[ログアウト]をタップしてUAからログアウトします。

以上で、iPhoneでの構成プロファイルのインストールは終了です。

なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より
管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウン
ロード済み」という表記に変わり、以後のダウンロードは一切不可となります。



6.2. サーバアクセス

iPhoneのブラウザ (Safari) でLTMのバーチャルサーバのURLにアクセスすると、構成プロファイルにあるクライアント証明書が自動的に提示されます。

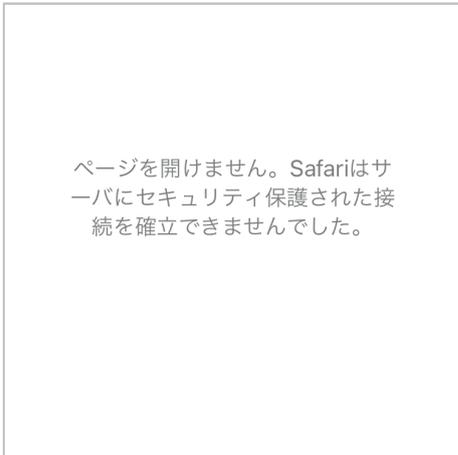
クライアント証明書認証がおこなわれるとページが表示されます。

※以下は7項のCGIを実行するWebページにアクセスしている例

```
Welcome Server
HTTP_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_ENCODING = gzip, deflate, br
HTTP_ACCEPT_LANGUAGE = ja
HTTP_CONNECTION = keep-alive
HTTP_HOST = [redacted]
HTTP_USER_AGENT = Mozilla/5.0 (iPhone; CPU iPhone OS 15_3_1 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.3 Mobile/15E148 Safari/604.1
HTTP_X_CLIENT_CERT_DN = CN=[redacted]
```

証明書を持っていない場合や、失効された証明書を提示した場合はアクセスに失敗します。

※以下はクライアント証明書を持っていない状態でアクセスした例



ページを開けません。Safariはサーバにセキュリティ保護された接続を確立できませんでした。

プライベート CA Gléas ホワイトペーパー
BIG-IP LTM でのクライアント証明書認証

7. Web サーバでクライアント証明書情報を取得

LTM の ReWrite 機能によってHTTPリクエストヘッダに挿入されたクライアント証明書情報をWebサーバが受信していることを確認します。

※以下は、Python で作成した CGI を Apache で公開する例

- http.conf に以下を追加

```
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options +ExecCGI
    Require all granted
    AddHandler cgi-script .py
</Directory>
```

- CGI を作成

```
vi /var/www/cgi-bin/test.py
chmod 755 /var/www/cgi-bin/test.py
```

※スクリプトの内容は以下。環境変数からリクエストヘッダを取得して出力

```
#!/usr/bin/env python

import os
print "Content-Type: text/html"
print "Cache-Control: no-cache"
print

print "<html><body>"
print "<h1>Welcome Server</h1>"

for headername, headervalue in sorted(os.environ.iteritems()):
    if headername.startswith("HTTP_"):
        print "{0} = {1}<br>".format(headername, headervalue)
print "</html></body>"
```

- Apache を再起動

```
systemctl restart httpd
```

Web ブラウザから CGI にアクセスすると、環境変数 HTTP_X_CLIENT_CERT_CN にクライアント証明書のサブジェクト一般名(CommonName)が取得できていることが確認できます。

※以下はPCからEdgeブラウザでアクセスした場合の例

```
Welcome Server

HTTP_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
HTTP_ACCEPT_ENCODING = gzip, deflate, br
HTTP_ACCEPT_LANGUAGE = ja,en;q=0.9,en-GB;q=0.8,en-US;q=0.7
HTTP_CONNECTION = keep-alive
HTTP_HOST = ██████████
HTTP_SEC_CH-UA = "Not?A_Brand";v="8", "Chromium";v="108", "Microsoft Edge";v="108"
HTTP_SEC_CH-UA_MOBILE = ?0
HTTP_SEC_CH-UA_PLATFORM = "Windows"
HTTP_SEC_FETCH_DEST = document
HTTP_SEC_FETCH_MODE = navigate
HTTP_SEC_FETCH_SITE = none
HTTP_SEC_FETCH_USER = ?1
HTTP_UPGRADE_INSECURE_REQUESTS = 1
HTTP_USER_AGENT = Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.46
HTTP_X_CLIENT_CERT_DN = CN=██████████, OU=██████████, O="JCCH Security Solution Systems Co., Ltd.", DC=jcch-sss, DC=com
```

8. 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。

■Gléasや本検証内容、テスト用証明書の提供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: 050-3821-2195

Mail: sales@jcch-sss.com