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
2016 年 2 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

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）でロードバランシング（Web負荷分散）でのクライアント証明書による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。

- BIG-IP Local Traffic Manager （BIG-IP 12.0.0 Build 0.0.606）
  以後、「LTM」と記載します
- JS3 プライベートCA Gléas（バージョン1.12.96）
  以後、「Gléas」と記載します
- Webサーバ：Ubuntu 14.04.2 LTS / Apache/2.4.7(Ubuntu)
- Windows10 Pro / Internet Explorer 11
  以後、「PC」と記載します

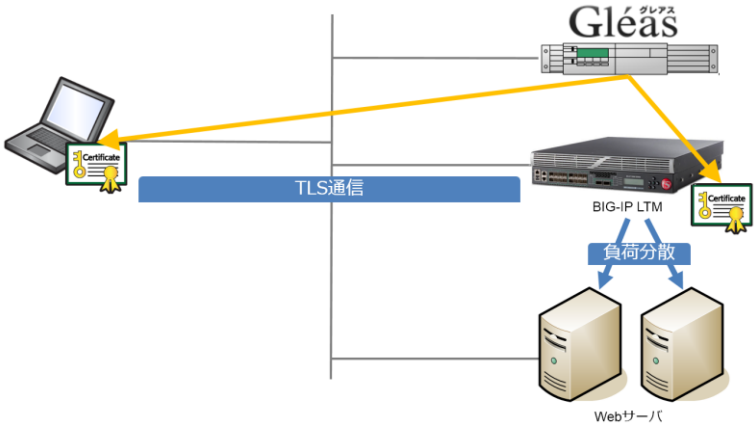
以下については、本書では説明を割愛します。

- 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）
  ※F5ネットワークス社では、以下URLでLTMの操作ガイドを公開しています。
  http://www.f5networks.co.jp/depot/
  「BIG-IP 800 LTM かんたんセットアップガイド」
- 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
- 各種サーバ・クライアント端末におけるネットワーク設定など

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、LTM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通信を終端氏、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。

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2.2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、[サーバ証明書]ロールグループに参加しておく必要があります。

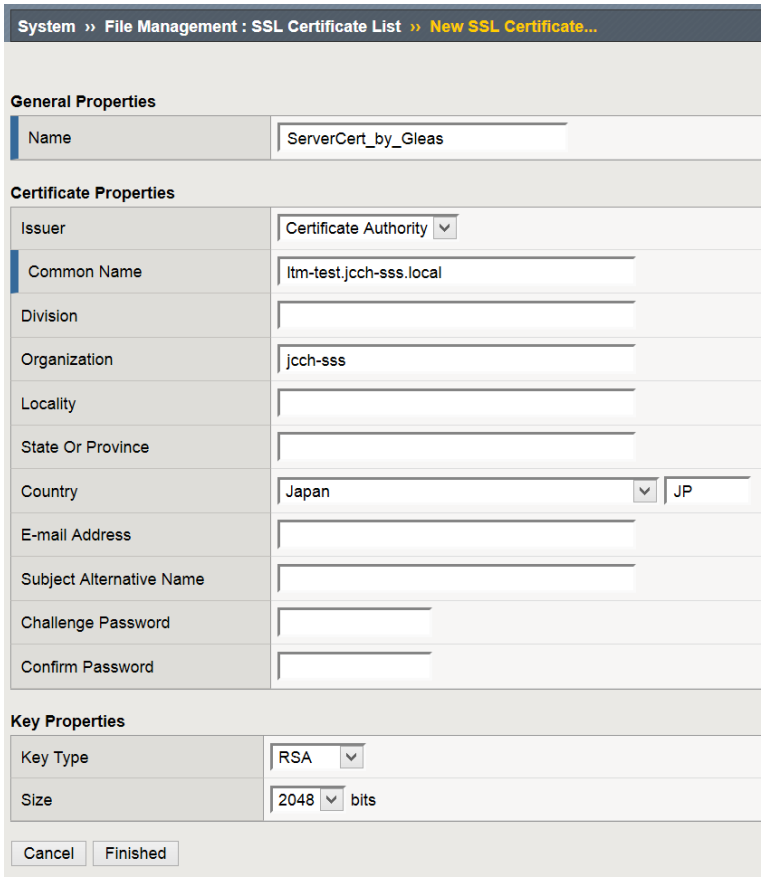
2. BIG-IPの設定

2.1. サーバ証明書の登録

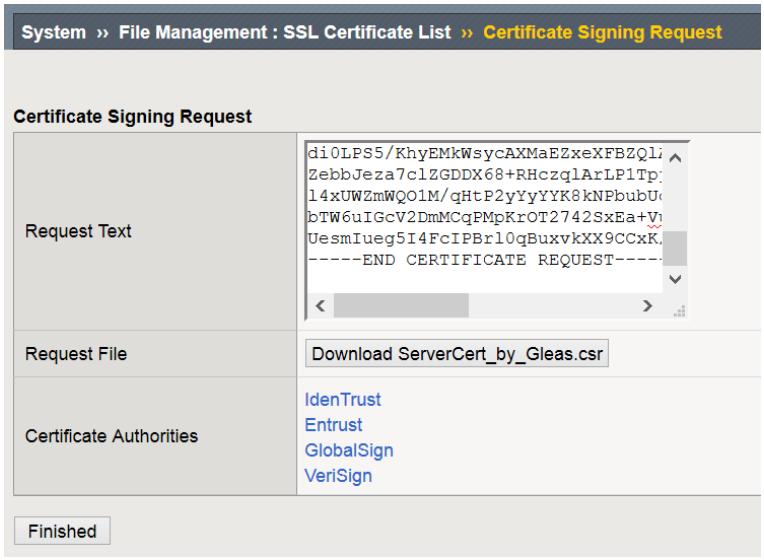
LTMのバーチャルサーバに適用するサーバ証明書を発行します。
※本手順では、Gléasで事前にサーバアカウントを作成してあることが前提です
※本手順では、LTMで証明書発行リクエスト（CSR）を発行していますが、Gléas側でこれらを一括しておこなうことも可能です

左側メニューから System ›› File Management : SSL Certificate List と進み、右上にある[Create…]ボタンをクリックします。
Name や Common Name などの証明書情報や Key Properties に必要事項を入力し、[Finished]ボタンをクリックします。

以下は Key Properties に RSA 2048bit 鍵長を選択した例です。
※Subject Alternative Name はここで設定しても、Gléas が証明書を発行するときにテンプレートに基づき上書きされます



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。



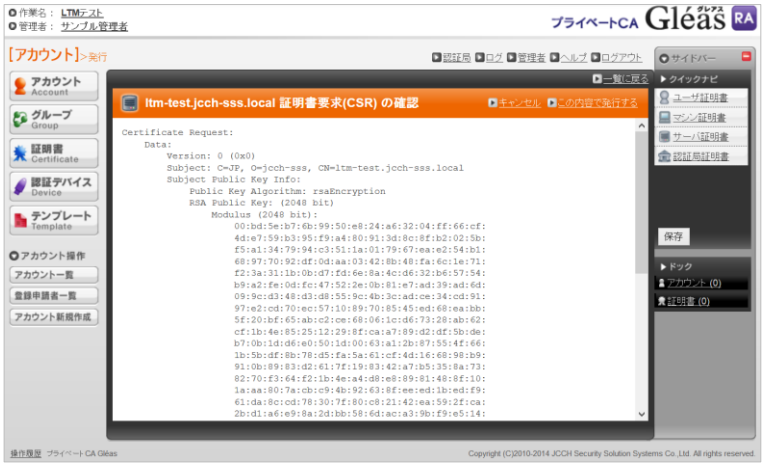
Gléas（RA）にログインし、該当のサーバアカウントのページへ移動します。
小メニューの[証明書発行]をクリックします。

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をチェック

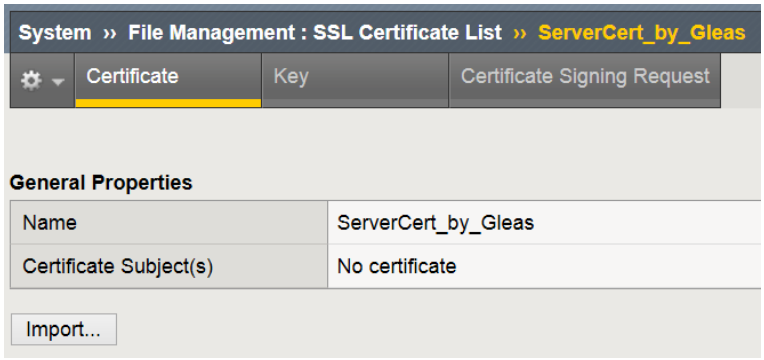
その後、[発行]ボタンをクリックします。

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。

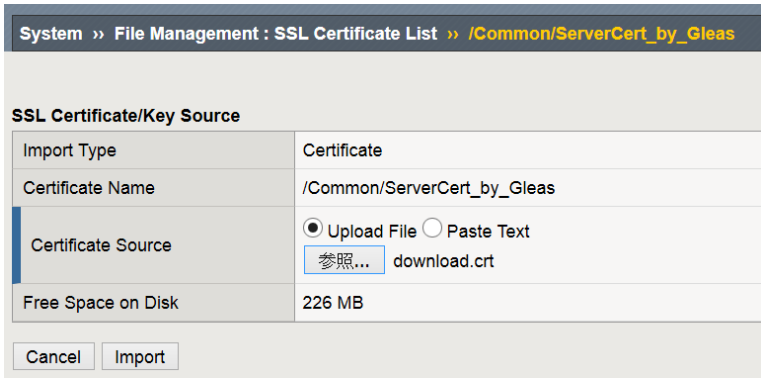


証明書発行完了後、証明書詳細画面の証明書ファイル欄の「証明書：あり」をクリックし、発行された証明書をダウンロードします。

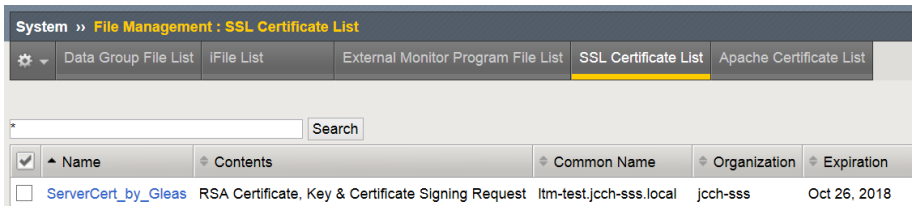
LTM の管理画面で、System ›› File Management : SSL Certificate List にて先ほど作成した CSR の詳細画面で、[Import…]ボタンをクリックします。



Gléas からダウンロードした証明書ファイルを選択し、[Import…]ボタンをクリックします。



以上でサーバ証明書の登録が完了です。
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PCから提示されるクライアント証明書が正しいこと

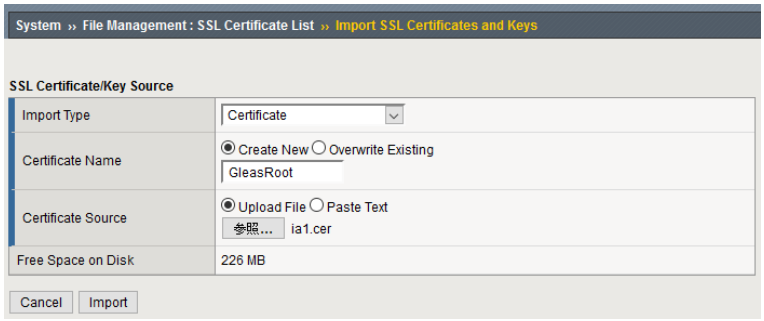
を検証する際に利用するためです。

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のダウンロードURLは以下となります。
http://hostname/crl/ia1.der

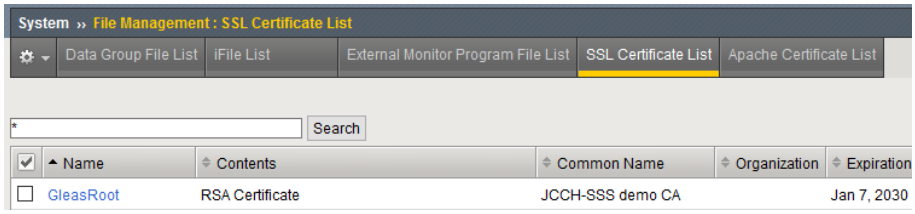
左側メニューから System ›› File Management : SSL Certificate List と進み、右上にある[Import…]ボタンをクリックします。
以下の操作をおこないます。

- Import Type は、[Certificate]を選択
- Certificate Name は、[Create New]を選択し任意の名称を入力
- Certificate Source は、[Upload File]を選択し[参照…]よりダウンロードしたファイルを選択

その後、[Import]をクリックします。



以上でルート証明書の登録が完了です。
Contents 欄に、RSA Certificate と表示されます。



2.3. 失効リスト（CRL）の登録

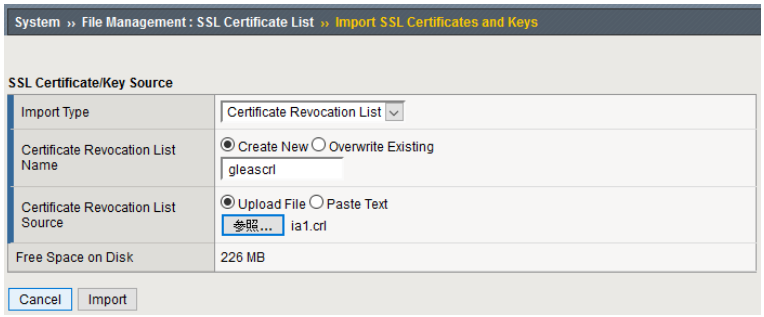
失効済みのクライアント証明書でのアクセスを防ぐために、CRLの登録をします。
あらかじめGléasよりCRLをダウンロードしておき、以下の操作をおこないます。

※ Gléas の初期設定での CRL ファイルの公開場所は以下のとおりです
http://hostname/crl/ia1.crl

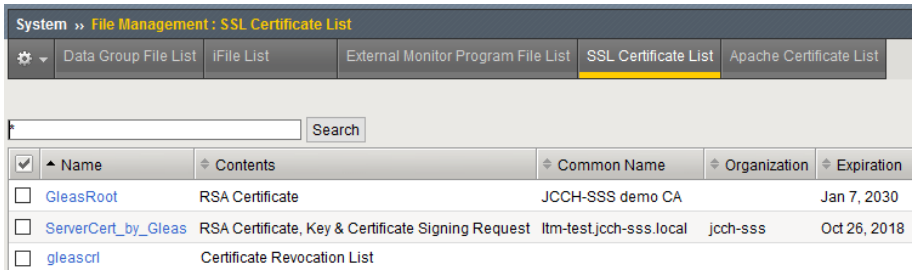
左側メニューから System ›› File Management : SSL Certificate List と進み、右上にある[Import…]ボタンをクリックします。
以下の操作をおこないます。

- Import Type は、[Certificate Revocation List]を選択
- Certificate Name は、[Create New]を選択し任意の名称を入力
- Certificate Source は、[Upload File]を選択し[参照…]よりダウンロードしたファイルを選択

その後、[Import]をクリックします。



以上で CRL の登録が完了です。
Contents 欄に、Certificate Revocation List と表示されます。



CRLを更新する場合は、Certificate Revocation List 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。

また、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。
tmsh modify /sys file ssl-crl *gleascrl.crl* source-path *http://hostname/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
tmsh list /sys file ssl-crl *gleascrl.crl*

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プロファイルの作成

クライアント証明書による認証を実施するプロファイルを作成します。
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（或いは既存のプロファイルの設定変更をおこないます）。

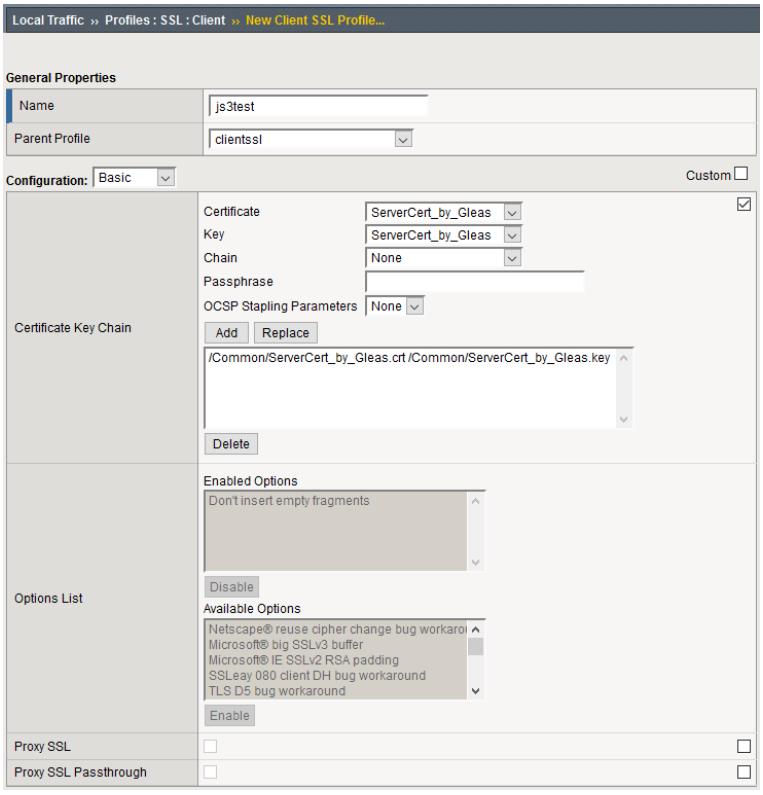
以下の設定変更をおこないます。
【Configuration】

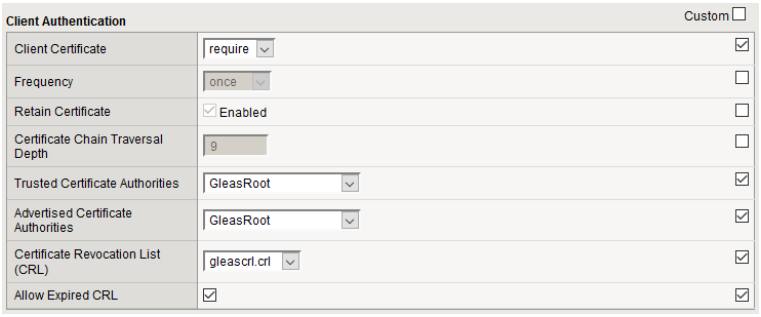
- Certificate Key Chain：Certificate と Key に 2.2 で設定したサーバ証明書を選択し、[Add]で追加

【Client Authentication】

- Client Certificate： require を選択
- Trusted Certificate Authorities：2.3 で設定したルート証明書を選択
- Advertised Certificate Authorities：2.3 で設定したルート証明書を選択
- Certificate Revocation List（CRL）：2.4 で設定した CRL を選択
- Allow Expired CRL：必要に応じチェック（弊社未検証）

設定後に[Finished]（或いは、[Update]）をクリックし、保存します。





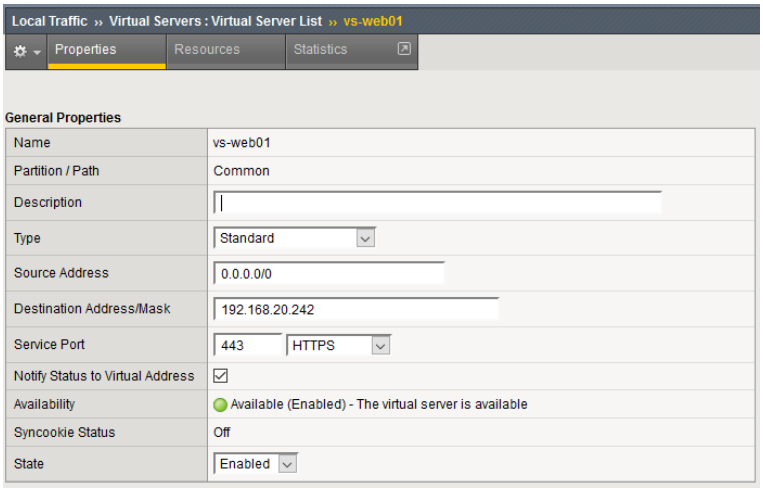
2.5. SSLプロファイルの適用

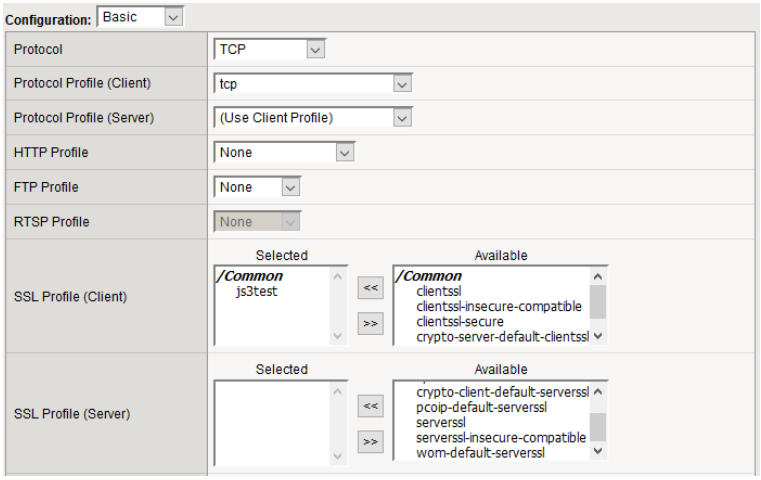
2.5 で作成したプロファイルを対象のバーチャルサーバに適用します。

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。
そのバーチャルサーバの以下を変更します。

- Service Port を HTTPS（443）に変更
- SSL Profile (Client)を 2.4 で作成した SSL プロファイルに変更

設定後、[Update]をクリックし保存します。





以上でBIG-IPの設定は終了です。

3. Gléas の管理者設定

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設定します。
※下記設定は、Gléasの納品時に弊社で設定をおこなっている場合があります

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。

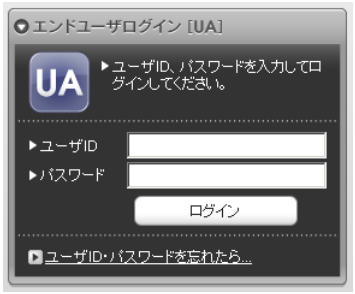
- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

設定終了後、[保存]をクリックし設定を保存します。

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 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。

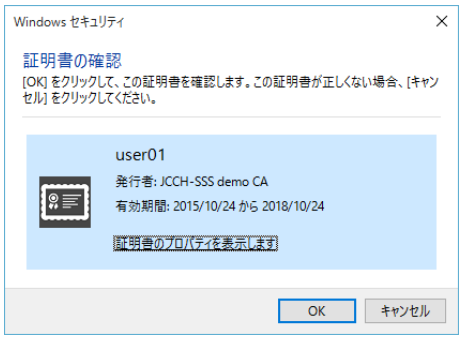


ログインすると、ユーザ専用ページが表示されます。
[証明書のインポート]ボタンをクリックすると、クライアント証明書が証明書ストアにインポートされます。
※初回ログインの際は、ActiveX コントロールのインストールを求められるので、画面の指示に従いインストールを完了してください。

「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システムへのアクセス

LTM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。



適切な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エラーとなり、LTMの /var/log/ltm に以下のログが出力されます。

証明書を持っていない場合のログ例：

```
Oct 01 00:00:00 hostname warning tmm[30155]: 01260009:4: Connection error:
ssl_shim_vfycerterr:4401: application verification failure (46)
```

証明書が失効している場合のログ例：

```
Oct 01 00:00:00 hostname warning tmm[30155]: 01260003:4: Certificate with serial xxxx
revoked per CRL from issuer /CN=JCCH-SSS demo CA/DC=COM/DC=JCCH-SSS
Oct 01 00:00:00 hostname warning tmm[30155]: 01260006:4: Peer cert verify error:
certificate revoked (depth 0; cert /CN=user01/DC=COM/DC=JCCH-SSS)
Oct 01 00:00:00 hostname warning tmm [30155]: 01260009:4: Connection error:
ssl_shim_vfycerterr:4401: certificate revoked (44)
```

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。

■BIG-IP LTMに関するお問い合わせ先
F5ネットワークスジャパン株式会社
Tel: 03-5114-3210
URL: https://f5.com/jp/fc/
（上記URLのお問い合わせフォームよりご連絡ください）

■Gléasに関するお問い合わせ先

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