



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

～F5 BIG-IP Edge Gateway連携～

iPhone版 BIG-IP Edge Clientによる

BIG-IPへのSSL-VPNトンネリング接続

Ver.2.0

2013年1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
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続

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
2. BIG-IP の設定	5
2.1. Network Access の設定	5
2.2. ルート証明書の登録	8
2.3. 失効リスト (CRL) の登録	9
2.4. SSL プロファイルの作成	10
2.5. SSL プロファイルの適用	11
2.6. アクセスポリシーの設定	11
3. Gléas の管理者設定	12
3.1. UA (ユーザ申込局) 設定	12
4. Gléas を利用したクライアント証明書の配布	15
4.1. Edge Client のインストール	15
4.2. Gléas の UA から配布	15
4.3. OTA エンロールメントを利用した証明書発行について	18
5. Edge Client の利用	18
6. 問い合わせ	20

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・iPhone用の構成プロファイルを利用して、iPhone用VPNクライアントである「BIG-IP Edge Client」からF5 Networks社製「BIG-IP Edge Gateway」とiPhone用VPNクライアントソフトウェアである「BIG-IP Edge Client」を利用してのトンネリング接続を行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、6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、以下の環境で作成しています。

- BIG-IP Edge Gateway (BIG-IP 11.1.0 Build 1943.0 Final)
以後、「BIG-IP」と記載します
- JS3 プライベートCA Gléas (バージョン1.10)
以後、「Gléas」と記載します
- iPhone 5 (iOS 6.0.2)
以後、「iPhone」と記載します
- BIG-IP Edge Client (バージョン1.0.4 7060.2012.0629.1)
以後、「Edge Client」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。

- BIG-IPでのネットワーク設定やサーバ証明書設定等の基本設定
- 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
- iPhoneでのネットワーク設定等の基本設定

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。

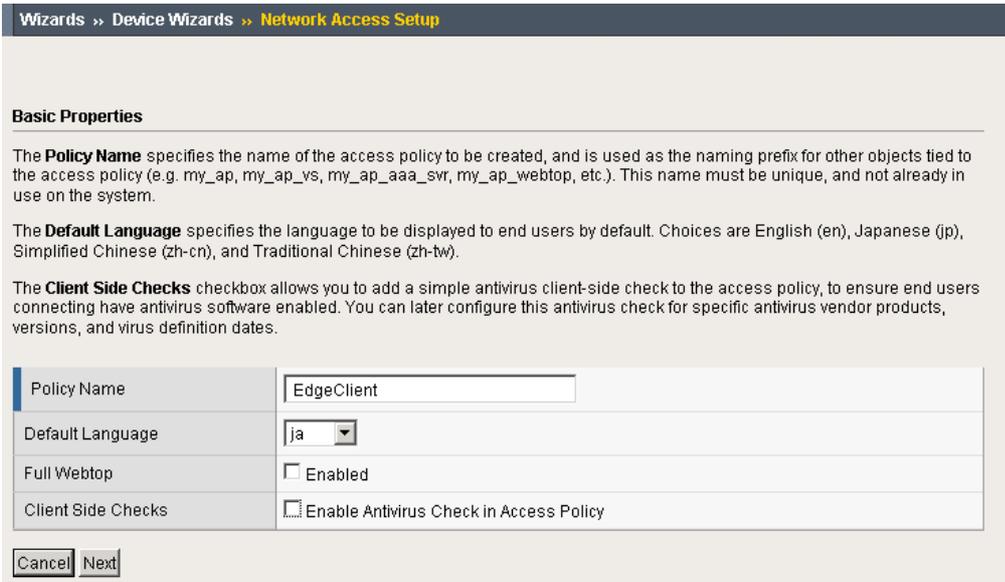
2. BIG-IPの設定

2.1. Network Access の設定

本書ではウィザードを使用して Virtual Server や Network Access をセットアップします。既に作成していれば、本項は実施する必要はありません。2.2 に進んでください。

管理画面にログインし、メニューから Wizards→Device Wizards の順にクリックして、ウィザードの一覧を表示します。Network Access Setup Wizard for Remote Access を利用して、環境に合わせて Network Access をセットアップしてください。

以下は設定例となります。



The screenshot shows the 'Network Access Setup' wizard interface. At the top, the breadcrumb navigation reads 'Wizards >> Device Wizards >> Network Access Setup'. Below this is the 'Basic Properties' section, which contains explanatory text for the 'Policy Name', 'Default Language', and 'Client Side Checks' fields. The configuration table below shows the following values:

Policy Name	EdgeClient
Default Language	ja
Full Webtop	<input type="checkbox"/> Enabled
Client Side Checks	<input type="checkbox"/> Enable Antivirus Check in Access Policy

At the bottom of the form, there are 'Cancel' and 'Next' buttons.

プライベート CA Gléas ホワイトペーパー
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続

Wizards » Device Wizards » Network Access Setup

Select Authentication

Please select the type of authentication you would like to configure for your access policy. When end users access the virtual server they will be shown a logon page to enter credentials. These credentials are checked against a preconfigured external authentication server.

If you would like to test a basic access policy without authentication, you are not authenticating users at all, or you will configure authentication later, you can select No Authentication. To add authentication later, create a new AAA server, then edit your access policy and add an authentication action.

Authentication Options	<input checked="" type="radio"/> Create New <input type="radio"/> Use Existing
Select Authentication	<input type="radio"/> RADIUS <input type="radio"/> LDAP <input type="radio"/> Active Directory <input type="radio"/> SecurID <input type="radio"/> HTTP <input type="radio"/> OCSP Responder <input type="radio"/> CRLDP <input type="radio"/> TACACS+ <input checked="" type="radio"/> No Authentication

Cancel Previous Next

- ※ 本書では、クライアント証明書のみによる認証の設定を記載します。ID/パスワードを併用する 2 因子認証を実施する場合は、ここで No Authentication 以外の認証を選んでください。
- ※ Gléas の UA で構成プロファイルをダウンロードする場合、UA にログインする時のパスワードが Edge Client に保存され、VPN 接続時に利用されます。

Wizards » Device Wizards » Network Access Setup

Configure Lease Pool

Lease pools are collections of IP addresses that the system assigns to users who make network access connections (client PPP addresses). A lease pool IP address is assigned to each client when the network access connection is established.

Create a lease pool that contains enough IP addresses to support your total number of expected concurrent connections. You must also ensure that there is no overlap between the IP addresses you define, and other networks within your organization.

By default these IP addresses are treated as a SNAT auto map pool and translated to the configured Self IP address when traffic is sent to your internal network. With this configuration, a return route to the lease pool from your internal network is not required. For more information on configuring SNAT and routing options, see the **Configuration Guide for BIG-IP® Access Policy Manager**.

Supported IP Version	IPV4
IPv4 Member List	Type: <input type="radio"/> IP Address <input checked="" type="radio"/> IP Address Range
	Start IP Address: 172.16.1.1
	End IP Address: 172.16.1.254
	Add
	172.16.1.1 - 172.16.1.254
	Edit Delete

Cancel Previous Next

プライベート CA Gléas ホワイトペーパー
 ~F5 BIG-IP Edge Gateway 連携~
 iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続

Wizards >> Device Wizards >> Network Access Setup

Configure Network Access

Configure the network access resource. For a basic network access connection, use the default values. For more information on these configuration options, click the Help tab in the navigation pane.

The lease pool you defined previously is assigned to this network access resource.

Compression	No Compression ▾
-------------	------------------

Client Settings

Traffic Options	<input checked="" type="radio"/> Force all traffic through tunnel <input type="radio"/> Use split tunneling for traffic
Allow Local Subnet	<input type="checkbox"/> Enable
Client Side Security	<input type="checkbox"/> Prohibit routing table changes during Network Access connection
DTLS	<input type="checkbox"/>

Cancel Previous Next

Wizards >> Device Wizards >> Network Access Setup

Configure DNS Hosts for Network Access

Specify DNS name servers, WINS servers, and a DNS default domain suffix. These servers and settings are assigned to end user client machines as part of the network access connection process, and are used by the client when performing name resolution for internal network resources.

These settings may be different than the BIG-IP system settings configured under **System : Configuration : Device : DNS**. For more information on these configuration options, click the Help tab on the navigation pane.

IPv4 Primary Name Server	172.16.1.100
IPv4 Secondary Name Server	172.16.1.101
Primary WINS Server	
Secondary WINS Server	
DNS Default Domain Suffix	jcch-sss.local
Static Hosts	Host Name <input type="text"/>
	IP Address <input type="text"/>
	Add
	<input type="text"/>
	Edit Delete

Cancel Previous Next

プライベート CA Gléas ホワイトペーパー
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続

Wizards » Device Wizards » Network Access Setup

Virtual Server (HTTPS connection)

Specify an IP address to create a local traffic virtual server that is correctly configured for network access. Your end users connect to a DNS name representing this destination address to start a network access connection.

Check the option **Create Redirect Virtual Server (HTTP to HTTPS)** to create a local traffic virtual server that automatically redirects users who connect using **http://** instead of **https://** with their web browser.

For information on installing a valid SSL server certificate and using this destination address behind a firewall, please see the **Configuration Guide for BIG-IP® Access Policy Manager**.

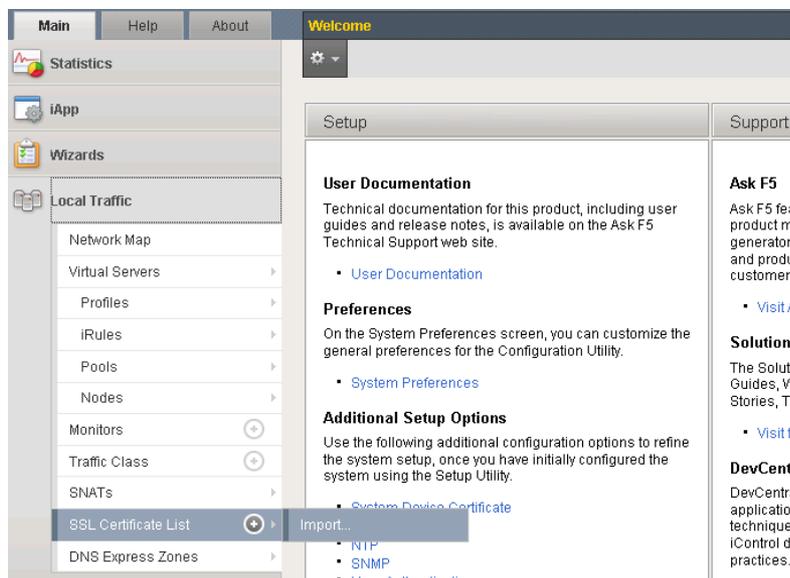
Virtual Server IP Address	172.16.1.99
Redirect Server	<input checked="" type="checkbox"/> Create Redirect Virtual Server (HTTP to HTTPS)

Cancel Previous Next

2.2. ルート証明書の登録

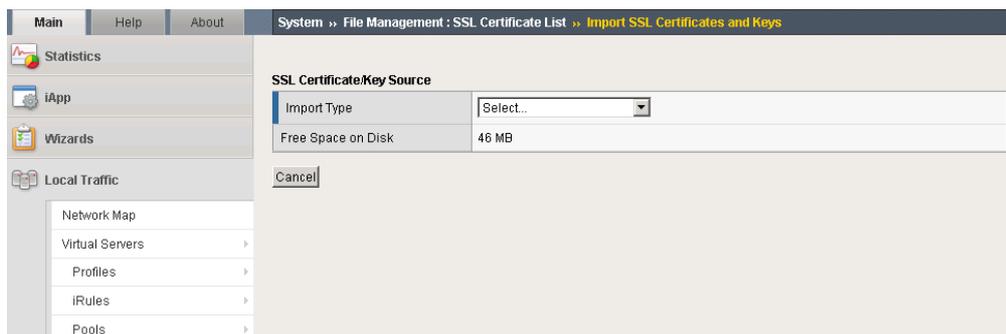
クライアント証明書によるSSL認証を利用するためには、ルート証明書の登録が必要です。これは、クライアントPCから提示されるクライアント証明書が正しいことを検証する際に利用するためです。

1. Local Traffic→SSL Certificate List→import の順にクリックする。



2. Import Type にて、Certificate を選択する。

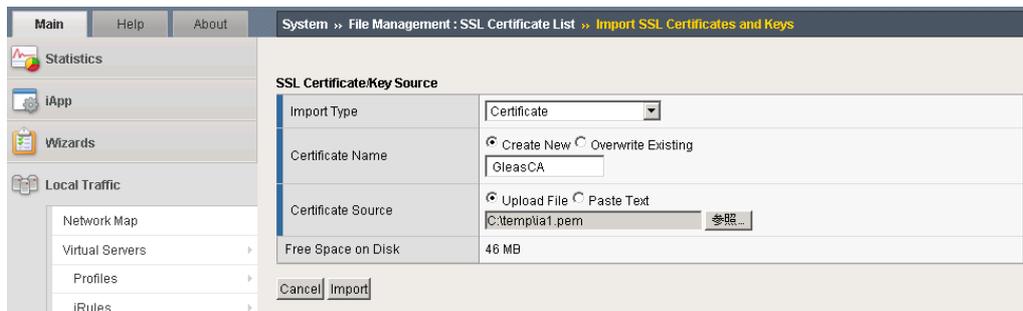
プライベート CA Gléas ホワイトペーパー
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続



3. ルート証明書を指定する。

Certificate Nameには、任意の名前を入力します。Certificate Sourceには、ルート証明書ファイルの場所を指定します。

入力が完了したら、Import ボタンをクリックします。



2.3. 失効リスト（CRL）の登録

Gléasで失効した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.example.local/crl/ia1.crl`

1. Local Traffic→SSL Certificate List→import の順にクリックする。

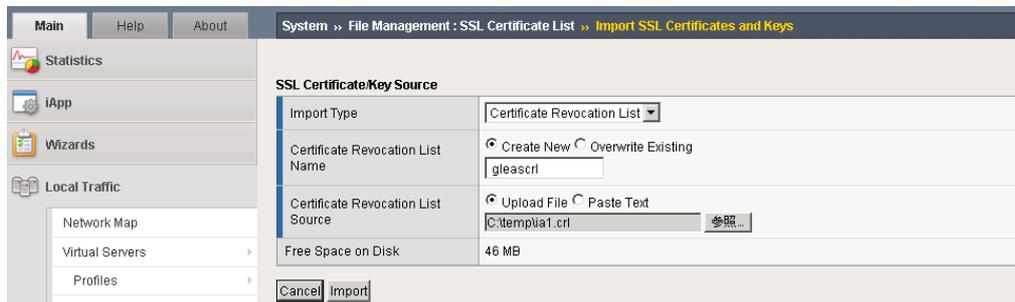
2. Import Type にて、Certificate Revocation List を選択する。

3. CRLを指定する。

Certificate Revocation List Nameには、任意の名前を入力します。Certificate Revocation List Sourceには、CRLファイルの場所を指定します。

プライベート CA Gléas ホワイトペーパー
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続

入力が完了したら、Import ボタンをクリックします。



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。

コマンドライン (tmsh。BIG-IPの管理用シェル) からCRL更新を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://host.example.local/crl/ial.crl
```

※ crontab で動かすことで定期取得の設定も可能です

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。

1. Local Traffic → Virtual Servers → Profiles → SSL → Client の順にクリックします。
2. Client Authentication の各項目を設定します。
 - Client Certification を request に変更
 - ※ require とすると、Edge Client がトンネリング接続に失敗します。認証時は、Access Policy にてクライアント証明書の正当性を検証します。
 - Trusted Certificate Authorities を 2.2 で登録したルート証明書に変更
 - Advertised Certificate Authorities を 2.2 で登録したルート証明書に変更
 - Certificate Revocation List (CRL)を 2.3 で登録した CRL に変更
3. Update 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
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続

Client Authentication	
Client Certificate	request
Frequency	once
Certificate Chain Traversal Depth	1
Trusted Certificate Authorities	gleas
Advertised Certificate Authorities	gleas
Certificate Revocation List (CRL)	gleascrl.crl
<input type="button" value="Update"/>	

2.5. SSL プロファイルの適用

2.4 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。

1. Local Traffic → Virtual Servers → Virtual Server List の順にクリックします。
2. 2.1 のウィザードで作成された Virtual Server をクリックします。
3. SSL Profile (Client)を 2.4 で作成した Profile に変更します。

Configuration: Basic					
Protocol	TCP				
OneConnect Profile	None				
NTLM Conn Pool	None				
HTTP Profile	http				
HTTP Compression Profile	None				
Web Acceleration Profile	None				
FTP Profile	None				
SSL Profile (Client)	<table border="1"><thead><tr><th>Selected</th><th>Available</th></tr></thead><tbody><tr><td>/Common SSLClientAuth</td><td>/Common clientsssl-insecure-compatible wom-default-clientsssl clientsssl</td></tr></tbody></table>	Selected	Available	/Common SSLClientAuth	/Common clientsssl-insecure-compatible wom-default-clientsssl clientsssl
Selected	Available				
/Common SSLClientAuth	/Common clientsssl-insecure-compatible wom-default-clientsssl clientsssl				
SSL Profile (Server)	<table border="1"><thead><tr><th>Selected</th><th>Available</th></tr></thead><tbody><tr><td></td><td>/Common serverssl serversssl-insecure-compatible test wom-default-serverssl</td></tr></tbody></table>	Selected	Available		/Common serverssl serversssl-insecure-compatible test wom-default-serverssl
Selected	Available				
	/Common serverssl serversssl-insecure-compatible test wom-default-serverssl				
VLAN and Tunnel Traffic	All VLANs and Tunnels				
SNAT Pool	None				

4. Update ボタンをクリックします。

2.6. アクセスポリシーの設定

Access Policy を変更します。

プライベート CA Gléas ホワイトペーパー
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続

1. Access Policy→Access Profiles の順にクリックし、Access Profile List を表示します。
2. 2.1 のウィザードで作成された Access Profile を編集するため、Access Policy の Edit をクリックします。
3. Logon Page の×をクリックして、削除します。
4. Resource Assign の左側の+をクリックして、Authentication 内の Client Cert Inspection を選び、Add Item ボタンをクリックします。
5. Save ボタンをクリックします。



上記のようになったら、Apply Access Policy をクリックします。

- ※ 上記は 2.1 のウィザードで No Authentication を選んだ場合の手順になります。クライアント証明書のみによる認証ではなく、ID/PW 認証も同時に行う 2 因子認証を実施する場合は、Logon Page は削除せず、Logon Page と Resource Assign の間に RADIUS Authなどを追加してください。

以上でBIG-IPの設定は終了です。

3. Gléas の管理者設定

Gléas で、発行済みのクライアント証明書を含む Edge Client 設定（構成プロファイル）を iPhone 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
- ※ Edge Client 用の構成プロファイル作成機能はオプションとなります。詳細は弊社営業までお問い合わせください。

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

プライベート CA Gléas ホワイトペーパー
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続

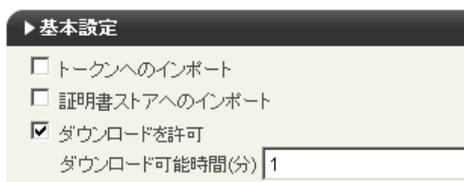
覧]画面に移動し、設定を行うUA（申込局）をクリックします。



[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。

- [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

この設定を行うと、GléasのUAからダウンロードしてから、指定した時間（分）を経過した後に、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）。このインポートロックにより複数台のiPhone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。



[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。



構成プロファイル生成に必要な情報を入力する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）
- [削除パスワード]を設定すると、iPhoneユーザが設定プロファイルを削除する際に管理者が定めたパスワードが必要となります（iPhoneユーザの誤操作等によ

プライベート CA Gléas ホワイトペーパー
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続

る構成プロファイルの削除を防止できます)

iPhone 構成プロファイル基本設定	
名前(デバイス上に表示)	プライベートCA Gleas
識別子(例: com.jcch-sss.profile)	com.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	EAS構成プロファイル
削除パスワード	

F5 SSL-VPNの設定

- [SSL-VPN接続名]に任意の名前を入力 (Edge Client上ではDescriptionに対応)
- [F5 SSL-VPN ホスト名]にBIG-IPのホスト名を入力 (Edge Client上ではServerに対応)
- [オンデマンド接続先]にオンデマンド接続に利用するドメイン名を入力 (Edge Client上ではDomain ListのAlways Connectに対応)

F5 SSL-VPNの設定	
SSL-VPN 接続名	js3_by_ua
F5 SSL-VPN ホスト名	big-ip.example.com
オンデマンド接続先	example.local
<input checked="" type="checkbox"/> 接続設定にユーザID/パスワードの情報を入れる	

各項目の入力が終わったら、[保存]をクリックします。

今回の設定ではパスワード認証なしでVPN接続が可能となるので、デバイスパスコードを設定しておくことが推奨されますが、構成プロファイルでパスコードを強制させることも可能です。

パスコードの設定	
<input checked="" type="checkbox"/> デバイスのパスコードが必要	<input type="checkbox"/> 英数字の値が必要
<input type="checkbox"/> 単純値を許可	

以上でGléasの設定は終了です。

4. Gléas を利用したクライアント証明書の配布

4.1. Edge Client のインストール

iPhoneでEdge Clientを利用する場合は、クライアントソフトウェアのダウンロードが必要です。App Store より事前にインストールを行ってください。
本書ではEdge Clientのインストール方法については割愛します。

4.2. Gléas の UA から配布

iPhoneのブラウザ（Safari）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。



ログインすると、そのユーザ専用ページが表示されるので、[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開始します。

※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

プライベート CA Gléas ホワイトペーパー
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続



自動的にプロファイル画面に遷移するので、[インストール]をタップします。
なお、[詳細]をタップすると、インストールされる証明書情報を見ることが可能です
ので、必要に応じ確認してください。



以下のようなルート証明書のインストール確認画面が現れますので、[インストール]
をクリック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。

プライベート CA Gleas ホワイトペーパー
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続



デバイスパスコードを設定している場合は、入力を求められます。
パスコード強制が構成プロファイルに含まれていて、デバイスにパスコードを設定していない場合は、以下の画面が出現しパスコードの設定を求められます。



インストール完了画面になりますので、[完了]をタップしてください。



元のUA画面に戻りますので、[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。

プライベート CA Gléas ホワイトペーパー
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続

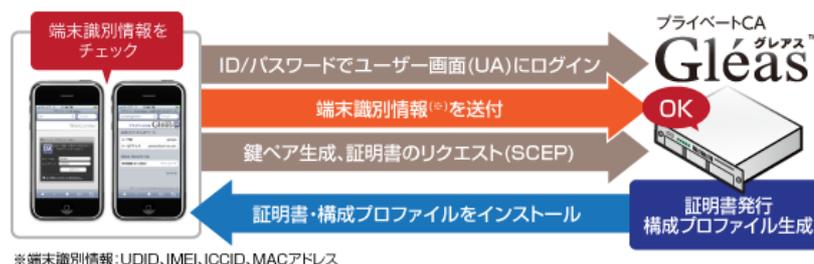
なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可となります。



4.3. OTA エンロールメントを利用した証明書発行について

Gléasでは、iOSデバイスに対するOver The Air (OTA) エンロールメントを利用した証明書の発行・構成プロファイルの配布も可能です。

OTAを利用すると事前に指定した端末識別番号を持つ端末だけに証明書の発行を限定することも可能になります。



詳細は最終項のお問い合わせ先までお問い合わせください。

5. Edge Client の利用

インストールした構成プロファイルにより、Edge Clientに認証に利用するクライアント

プライベート CA Gléas ホワイトペーパー
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続

ント証明書やユーザID、オンデマンド接続用のドメインが設定されています。
Edge Clientを起動し[接続]ボタンをタップ、或いは構成プロファイルでオンデマ
ンド接続が設定されている場合は、Safariなど対応アプリのアドレスバーに指定された
アドレスを入力すると、クライアント証明書を利用した認証を行いVPNの接続がお
こなわれます。

クライアント証明書によるセキュアな接続をお試してください。

以下はEdge Clientから接続した画面です。

(接続すると、iPhoneの通知エリアに **VPN** アイコンが表示されます)。



なお、失効した証明書でアクセスすると以下のようになり接続することができませ
ん。

※失効情報を含むCRLがBIG-IPに伝搬されている必要があります



プライベート CA Gléas ホワイトペーパー
～F5 BIG-IP Edge Gateway 連携～
iPhone 版 BIG-IP Edge Client による BIG-IP への SSL-VPN トンネリング接続

失効された証明書でアクセスした場合には、BIG-IPに以下のログが記録されます
(`/var/log/ltm`)。

※ファシリティSSLのログレベルをdebugにしておく必要があります

```
debug tmm[xxxx]: 01260003:7: Certificate with serial xxxx revoked per CRL
from issuer Issuer_DN
debug tmm[xxxx]: 01260006:7: Peer cert verify error: certificate revoked
(depth X; cert Subject_DN)
debug tmm[xxxx]: 01260009:7: Connection error: ssl_shim_vfycert:2462:
certificate revoked (44)
```

6. 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: <http://www.f5networks.co.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