

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

Copyright by JCCH Security Solution Systems Co., Ltd., All Rights reserved

- 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.	はじょ	りに	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
	1.4.	証明書発行時における留意事項	5
2.	BIG-I	P の設定	6
	2.1.	サーバ証明書の登録	6
	2.2.	ルート証明書の登録	9
	2.3.	失効リスト (CRL) の登録	10
	2.4.	SSL プロファイルの作成	12
	2.5.	SSL プロファイルの適用	13
3.	Gléas	の管理者設定	14
4.	PC か	らの接続操作	15
	4.1.	クライアント証明書のインポート	15
	4.2.	Web システムへのアクセス	16
5.	問いる	うわせ	17

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。
- 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

System » File 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-sss						
Locality							
State Or Province							
Country	Japan						
E-mail Address							
Subject Alternative Name							
Challenge Password							
Confirm Password							
Key Properties							
Кеу Туре	RSA V						
Size	2048 🗸 bits						
Cancel Finished							

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 » File Management : SSL Certificate List » Certificate Signing Request						
Certificate Signing Request						
Request Text	di0LPS5/KhyEMkWsycAXMAEZxeXFBZQ1 ZebbJeza7cl2GDDX68+RHczqlArLP1Tp; l4xUWZmWQ01M/qHtP2yYyYK8kNPbubU bTW6uIGeV2DmMcqPMpKrOT2742SxEa+Vi UesmIueg514FcIPBr10qBuxvkXX9CCxK, END CERTIFICATE REQUEST					
Request File	Download ServerCert_by_Gleas.csr					
Certificate Authorities	ldenTrust Entrust GlobalSign VeriSign					
Finished						

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。

アカワント」>詳細		■認証局 ■ <u>ログ</u> ■ 管	理者 ヘルブ ログアウト	● サイドバー
アカウント Account	アカウント		▶ <u>一覧に戻る</u>	▶ クイックナビ
の グループ	Itm-test.jcch-sss.local		<u>►±≥2</u>	2 ユーザ証明書
Group	9 アカウント情報	ち グループ情報	^	■ マンン血の者
★ 証明書 Certificate	▶サーバ 会議日時・2015/10/26 20:01	▶ フーザグループ	日参加	☆認証局証明書
応証デバイス Device	▶ ステータス:有効	>ral	- 30A	
テンプレート	▶サーバ属性 最終更新:2015/10/26 20:01 編集	▶ロールグループ	四参加	
Template	》ホスト名:Itm-test.jcch-sss.local	> サーバ証明書		保存
アカウント操作				
アカウントー覧	★ 証明書発行の履歴・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・			▶ ドック 素 アカウント (0)
登録申請者一覧	Þ1			★証明書 (0)
アカウント新規作成	# シリアル 開始 有効期限 スラ	アータス 失効日 暗号相	別 トークン	
▶証明書発行	証明書は発行さ	きれていません。		
▶アカウント削除	▶ テンプレート情報			
▶ドックに入れる	+ # # 5 % a / h			

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。

 O 作業名: <u>LTMテスト</u> O 管理者: <u>サンブル管理</u> 	K.	プライベートCA	Gléå 🕏 🎮
[アカウント]>証明書	8 行	◎認証局 ◎ログ ◎管理者 ◎ヘルブ ◎ログアウト	O#⊀F/(- □
🌔 アカウント 🛛 🔽	カウント	▶一覧に戻る	▶クイックナビ
Account	🔲 ltm-test.jcch-sss.local	■詳細に戻る	8 ユーザ証明書
Group		^	星マシン証明書
🐞 証明書	★ 証明書発行		■ <u>サーハ証明書</u>
Certificate	この画面では証明書要求の作成を行います。 左側の「サブジェクト」と「属性」の内容で証明書要求を作成します。		THE REALPHONE OF ST
Sevice Bevice	右側のテンプレートの中から必要なものを選択して「発行」を押してください	•	
テンプレート	▶証明書発行	■上級者向け設定	
Template	> 下記の内容で証明書を発行します。よろしければ「発行」を押してくださ	ίμ.,	保存
●アカウント操作	 ・		► Km/2
アカウント一覧	▶ 証明書要求(CSR)ファイルをアップロードする: 参照 servercer	t_by_gleas.csr	アカウント (0)
登録申請者一覧	CSRファイルの内容を確認する		★ 註明書 (0)
アカウント新規作成	発行		
▶証明書発行			
	▶サブジェクト	択されているテンプレート ■全て解除	
	> CN=Itm-test.jcch-sss.local > 必	須デフォルト設定	
	> DC=JCCH-SSS, COM	須サーハ証明書	
操作履歴 ブライベート CA Gléas		Copyright (C)2010-2014 JCCH Security Solution Syst	ems Co.,Ltd. All rights reserved.

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。

アカウント」>発行		証局 国ログ 国管理者 国ヘルブ 国ログアウト	● サイドバー
6 アカウント		<u>一覧に戻る</u>	▶ クイックナピ
Account	ltm-test.icch-sss.local 証明書要求(CSR) の確認	■キャンセル ■この内容で発行する	॑ ユーザ証明書
シグループ			
Group	tificate Request:	^	= ++. (CTOP+
13 RH SR	Data:		<u>9 7 7 18 99 18</u>
Certificate	Version: 0 (0x0)		⑦ 認証局証明書
	Subject: C=JP, O=jcch-sss, CN=ltm-test.jcch-sss.loc	al	
2 認証デバイス	Subject Public Key Info:		
Device	Public Key Algorithm: rsaEncryption		
	RSA Public Key: (2048 bit)		
テンプレート	Modulus (2048 bit):		
Template	UU:DD:DE:D/:0D:99:DU:E8:24:80:32:U4:II: Ad:07:50:b2:05:50:c4:00:01:2d:00:05:b2:	02:50	保友
	f5-a1-24-70-04-a2-51-1a-01-70-67-aa-a2-	54-b1-	PH-13
アカウント操作	68:97:70:92:df:0d:aa:03:42:8b:48:fa:6c:	10:71:	
25026-8	f2:3a:31:1b:0b:d7:fd:6e:8a:4c:d6:32:b6:	57:54:	▶ ドック
77551-頁	b9:a2:fe:Od:fc:47:52:2e:Ob:81:e7:ad:39:	ad:6d:	2 アカウント (0)
1錄申請者一覧	09:9c:d3:48:d3:d8:55:9c:4b:3c:ad:ce:34:	cd:91:	
	97:e2:cd:70:ec:57:10:89:70:85:45:ed:68:	ea:bb:	★ 1104 EF (0)
Pカウント新規作成	5f:20:bf:65:ab:c2:ce:68:06:1c:d6:73:28:	ab:62:	
	cf:1b:4e:85:25:12:29:8f:ca:a7:89:d2:df:	5b:de:	
	b7:0b:1d:d6:e0:50:1d:00:63:a1:2b:87:55:	4f:66:	
	lb:5b:df:8b:78:d5:fa:5a:61:cf:4d:16:68:	98:b9:	
	91:0b:89:83:d2:61:7f:19:83:42:a7:b5:35:	8a:73:	
	82:70:f3:64:f2:1b:4e:a4:d8:e8:89:81:48:	8f:10:	
	la:aa:80:7a:cb:c9:4b:92:63:8f:ee:ed:1b:	ed:19:	
	61:da:8C:Cd:78:30:7T:80:C8:21:42:ea:59:	ZI:ca:	
	ZD:01:80;09:08;Z0;DD:50:00;8C:83:9D:19;	02:14:	

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:<u>あり</u>」をクリ ックし、発行された証明書をダウンロードします。

正明書]>詳細		2 認証局 2 ログ 2 管理者 2 ヘルプ 2 ログアウト	O サイドバー
アカウント	証明書		▶ クイックナビ
Account	JCCH-SSS demo CA#11161	■ <u>E≥Ż</u>	2 ユーザ証明書
グループ Group			■ マシン証明書
EX DE SER	▶證明書情報		● サーバ証明書
Certificate	> 認証局: <u>JCCH-SSS demo CA</u>		愈 認証局証明書
認証デバイス	> 暗号アルゴリズム:rsa		
Device	> メインエストアルコリスム: Sna206 > 説を : 2049		
テンプレート	> 建設:2000 > 建田途: 電子要点 離の暗号化		
Template	▶ 就張健用途: SSLサーバ認証 SSLクライアント認証		保存
E明書操作	> 别名: DNS名:itm-test.jcch-sss.local		
明書一覧			▶ Fック
失效処理	▶証明書ファイル		
事止始理	> 証明書要求: <u>あり</u>		X LOUI (0)
シックに入れる	作成日時 2015/10/26 20:09		
771071110	> 証明書: あり 作成日時 2015/10/26 20:11		
	1 秋田時 201010120 2011		
	· NUMPE · ···		
	▶ テンプレート情報 ······		
	トテンプレート情報		

8/18

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。

System » File Management : SSL Certificate List » ServerCert_by_Gleas							
⇔ -	Certificate	Key		Certificate Signing Request			
General Properties							
Name			ServerCert_by_Gleas				
Certificate Subject(s)			No certificate				
Import							

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。

System » File Management : SSL Certificate List » /Common/ServerCert_by_Gleas					
SSL Certificate/Key Source					
Import Type	Certificate				
Certificate Name	/Common/ServerCert_by_Gleas				
Certificate Source	● Upload File ○ Paste Text 参照 download.crt				
Free Space on Disk	226 MB				
Cancel Import					

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。

System » File Management : SSL Certificate List								
🟚 🚽 Data Group File List iFile List External Monitor Program File List SSL Certificate List Apache Certificate List								
					Evairation			
	• Contents			• Organization	Expiration			

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。

System » File Management : SSL Certificate List » Import SSL Certificates and Keys				
SSL Certificate/Key Source				
Import Type	Certificate			
Certificate Name	Create New O Overwrite Existing GleasRoot			
Certificate Source	● Upload File 〇 Paste Text 参照 ia1.cer			
Free Space on Disk	226 MB			
Cancel Import				

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。

System » File Management : SSL Certificate List								
🔅 🗸 Data Group File List iFile List External Monitor Program File List SSL Certificate List Apache Certificate List								
* Search								
Name	Contents		≑ Co	mmon Name	Organization	Expiration		
GleasRoot I	RSA Certificate		JCCH	I-SSS demo CA		Jan 7, 2030		

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。

System » File Management : S	SL Certificate List » Import SSL Certificates and Keys
SSL Certificate/Key Source	
Import Type	Certificate Revocation List 🗸
Certificate Revocation List Name	Create New O Overwrite Existing gleascr1
Certificate Revocation List Source	● Upload File ○ Paste Text 参照 ja1.cri
Free Space on Disk	226 MB
Cancel Import	

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。

Syst	System » File Management : SSL Certificate List							
\$	 Data Group File List 	t iFile List	iFile List External Monitor Program File List SSL Certificate List					
k.								
r		Sea	ircn				I	
	 Name 	Contents		≑ Co	mmon Name	Organization	\Rightarrow Expiration	
	GleasRoot	RSA Certificate		JCCH	I-SSS demo CA		Jan 7, 2030	
	ServerCert_by_Gleas	RSA Certificate, Key	& Certificate Signing Request	Itm-te	st.jcch-sss.local	jcch-sss	Oct 26, 2018	
	gleascrl	Certificate Revocatio	n List					

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。

General Properties Name js3test Parent Profile clientssi configuration: Basic Custom Certificate ServerCert_by_Gleas Custom Certificate Key Chain Correct_by_Gleas Chain Passphrase OCSP Stapling Parameters None Common/ServerCert_by_Gleas.set Certificate Key Chain Add Replace Common/ServerCert_by_Gleas.set Common/ServerCert_by_Gleas.key Delete Delete Continues of the set of th	Local Traffic » Profiles : SSL : C	Client » New Client SSL Prof	ile		
General Properties Name js3test Parent Profile clientssi Configuration: Basic Custom Key ServerCert_by_Gleas Custom Chain None Chain Chain Passphrase OCSP Stapling Parameters None Common/ServerCert_by_Gleas.v Chain Add Replace // Common/ServerCert_by_Gleas.ct //Common/ServerCert_by_Gleas.key Common/ServerCert_by_Gleas.key C					
Name js3test Parent Profile clientssi Configuration: Basic Custom Certificate ServerCert_by_Gleas Custom Certificate Key Chain Certificate ServerCert_by_Gleas Chain Passphrase OCSP Stapling Parameters None Common/ServerCert_by_Gleas.key Chain Octions Add Replace Replace Common/ServerCert_by_Gleas.key <	General Properties				
Parent Profile clientssi Configuration: Basic Custom Certificate ServerCert_by_Gleas Custom Certificate Key Chain Certificate ServerCert_by_Gleas Chain Passphrase OCSP Stapling Parameters None Common/ServerCert_by_Gleas.key Chain Octomon/ServerCert_by_Gleas.cri/Common/ServerCert_by_Gleas.key Common/ServerCert_by_Gleas.cri/Common/ServerCert_by_Gleas.key Common/ServerCert_by_Gleas.key Common/ServerCert_by_Gleas.key Options List Enabled Options Cont insert empty fragments Cont insert empty fragments Cont insert empty fragments Proxy SSL Imable Cont Did SLV2 RSA padding Cont Did SLV2 RSA padding	Name	js3test			
Configuration: Basic Custom Certificate ServerCert_by_Gleas Custom Key ServerCert_by_Gleas Chain Passphrase Chain None Chain OcsP Stapling Parameters None Common/ServerCert_by_Gleas.cust Custom Add Replace //Common/ServerCert_by_Gleas.cust Custom Delete Don't insert empty fragments Custom Disable Xailable Options Custom Norespective coher change bug workaroi Microsofte big SSLV2 Buffer Microsofte big SSLV2 Buffer Microsofte big SSLV2 Buffer Proxy SSL Imable Imable	Parent Profile	clientssl	\checkmark		
Certificate ServerCert_by_Gleas ✓ Key ServerCert_by_Gleas ✓ Chain None ✓ Passphrase ✓ ✓ OCSP Stapling Parameters None ✓ ✓ Add Replace ✓ I/Common/ServerCert_by_Gleas.ct //Common/ServerCert_by_Gleas.key ✓ Delete ✓ Options List Enabled Options I/Contine tempty fragments ✓ I/Sable ✓ Available Options ✓ Netscape@reuse cipher change bug workaro Microsofte big SSLV2 BMFer Microsofte big SSLV2 BMFer Proxy SSL Proxy SSL	Configuration: Basic 🗸				Custom 🗌
Key ServerCert_by_Gleas Chain None Passphrase OCSP Stapling Parameters OCSP Stapling Parameters None Add Replace /Common/ServerCert_by_Gleas.ct /Common/ServerCert_by_Gleas.key Delete Delete Image: Delete Options List Pisable Available Options Netscaped reuse cipher change bug workaro Microsofte big SSLv2 Notifer Microsofte big SSLv2 Notifer Microsofte big SSLv2 Notifer Proxy SSL Proxy SSL		Certificate	ServerCert_by_Gleas 🗸		
Chain None Passphrase OCSP Stapling Parameters OcSP Stapling Parameters None Add Replace // Common/ServerCert_by_Gleas.ct //Common/ServerCert_by_Gleas.key Delete Delete Disable Available Options None None Options List Proxy SSL Proxy SSL		Key	ServerCert_by_Gleas 🗸		
Certificate Key Chain Passphrase Add Replace //Common/ServerCert_by_Gleas.ct //Common/ServerCert_by_Gleas.key Delete Enabled Options Dont insert empty fragments V Disable Available Options Netscape@reuse cipher change bug workarol Microsofte big SSLv2 RSA padding SSLever SSL Proxy SSL Proxy SSL		Chain	None		
Certificate Key Chain OCSP Stapling Parameters None Add Replace //Common/ServerCert_by_Gleas.crt //Common/ServerCert_by_Gleas.key Delete Delete Options List Enabled Options Disable Available Options Isable Proxy SSL Proxy SSL		Passphrase		-	
Certificate Key Chain Add Replace //Common/ServerCert_by_Gleas.ct //Common/ServerCert_by_Gleas.key Delete Doptions List Enabled Options Options List Disable Available Options Netscape@reuse cipher change bug workarol Microsoft® big SSLV2 BAMer Microsoft® big SSLV2 BAMer Proxy SSL Proxy SSL		OCSP Stapling Parameters	None 🗸		
Image: Proxy SSL Image: Proxy SSL Proxy	Certificate Key Chain	Add Replace			
Options List Enabled Options Options List Disable Available Options - Nicrosoft® big SSLv2 Notifer Nicrosoft® big SSLv2 Notifer Microsoft® big SSLv2 RSA padding SSLeavy 000 client DH bug workaround Proxy SSL - Proxy SSL -		/Common/ServerCert_by_G	ileas.ctt /Common/ServerCert_by_Glea	as.key	
Options List Disable Available Options Available Options Netscape@reuse cipher change bug workaro Microsoft@ big SSLv3 buffer Microsoft@ big SSLv3 Buffer Microsoft@ big SSLv3 Buffer Microsoft@ big SSLv3 Buffer Proxy SSL Proxy SSL Proxy SSL		Enabled Options			
Options List Disable Available Options Netscape@reuse cipher change bug workaro Microsoft@ big SSLv3 buffer Microsoft@ ESSLv3 RSA padding SSLeav 000 cilent DH bug workaround TLS D5 bug workaround Proxy SSL Proxy SSL Proxy SSL		Don't insert empty fragment	is		
Options List Available Options Netscape@reuse cipher change bug workarol ^ Microsoft@ big SSLv2 Notifer Microsoft@ E SSLv2 RSA padding SSLEavy 080 citent DH bug workaround TLS D5 bug workaround Enable		Disable			
Proxy SSL Proxy SSL Proxy SSL Passthrough	Options List	Available Options			
Proxy SSL Passthrough		Netscape® reuse cipher ch Microsoft® big SSLv3 buffer Microsoft® IE SSLv2 RSA pa SSLeay 080 client DH bug v TLS D5 bug workaround	ange bug workarol A adding vorkaround		
Proxy SSL Proxy SSL Passthrough		Enable			
Proxy SSL Passthrough	Proxy SSL				
	Proxy SSL Passthrough				

Client Authentication		Custom 🗆
Client Certificate	require 🗸	
Frequency	once 🗸	
Retain Certificate	Enabled	
Certificate Chain Traversal Depth	9	
Trusted Certificate Authorities	GleasRoot	
Advertised Certificate Authorities	GleasRoot	
Certificate Revocation List (CRL)	gleascri.cri 🗸	
Allow Expired CRL		

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。

Local Traffic » Virtual Servers	Local Traffic » Virtual Servers : Virtual Server List » vs-web01				
🗱 👻 Properties Res	ources Statistics 🗵				
General Properties					
Name	vs-web01				
Partition / Path	Common				
Description	1				
Туре	Standard				
Source Address	0.0.0.0/0				
Destination Address/Mask	192.168.20.242				
Service Port	443 HTTPS V				
Notify Status to Virtual Address					
Availability	Available (Enabled) - The virtual server is available				
Syncookie Status	Off				
State	Enabled 🗸				

Configuration: Basic 🗸	
Protocol	TCP
Protocol Profile (Client)	tcp 🗸
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	None
FTP Profile	None 🗸
RTSP Profile	None 🗸
SSL Profile (Client)	Selected Available /Common js3test /Common clentssl clentssl-inecure-compatible clentssl-secure crypto-server-default-clientssl v
SSL Profile (Server)	Selected Available Crypto-client-default-serverssl serverssi serverss-insecure-compatible wom-default-serverssl v

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。

UA	申込局		
	▶ <u>Gleas Generic UA</u>	Gleas デフォルト申込局	

[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ポート	証明書ストアの種類	ユーザストア	-
□ ダウンロードを許可	🗹 インポートワンスを利用す	5	

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。

●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 ラインしてください。
▶ユーザ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。

			JJAK-FCA Gle	éås UA
[サンプル ユーザ さんのページ]				■ <u>ログアウト</u>
ユーザ情報	_	_		
🙎 サンプル ユーザ さんのペー	-ジ			<u>∿וז</u>
▶ユーザ情報 ······				~
▶ ユーザ 登録日時 : 20	11/07/19 13:48			
>姓:サンブル 名:ユーザ >ユーザD:user01 >メールアドレス:sales@joch-sss.co >パスワード:************************************	m			
▶ 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ボート	
<u> <u> </u> </u>	#11158	2018/10/24	証明書のインポート	
				V
プライベートCA Gléas	c	Copyright (C)2010-2014	JCCH Security Solution Systems Co., Ltc	. All rights reserved.

			プラ	an-eca Gléäs ua
サンプル ユ	ーザ さんのページ]			<u>□</u> ログアウト
ユーザ情報				
	パル ユーザ さんのページ			<u>∿וול</u>
2 ユーザ	情報			^
▶ ユーザ > 姓 : サン > ユーザID > メールア > パスワー	登録日 Web ページがe Web ページがe Web ページがe Web ページがe ドレス:sales@jcc ド:::::::::::::::::::::::::::::::::::	5のメッセージ 5のメッセージ ーザの証明書ストアへ1	× インポートしました。	
★ 証明書	情報 · · · · · ·		OK	
▶ 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ボート
<u>\$1</u>	JCCH-SSS demo CA	#11158	2018/10/24	証明書のインポート
	_	_	_	Ŷ
プライベートCA Gléi	85	Copyrig	ht (C)2010-2014 JCCH Se	curity Solution Systems Co., Ltd. All rights reserved

「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。

			プライイ	K-FCA Gléäš	UA
[サンプル ニ	Lーザ さんのページ]			■ <u>ログアウ</u>	<u>うト</u>
ユーザ情報					
2 サン	プル ユーザ さんのページ				2
2-サ	"情報				\sim
▶ ユーザ	登録日時 : 2011/07/19	13:48			
> 姓 : サ > ユーザII > メールア > パスワー	ンブル 名:ユーザ):user01 7ドレス: sales@jcch-sss.com -ド: ********				
★ 証明書	ቔ情報······				
▶ 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	
槃1	JCCH-SSS demo CA	#11158	2018/10/24	ダウンロード済み	

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