

プライベートCA Gléas ホワイトペーパー

∼ BIG-IP Edge Gateway & VMware View ∼

クライアント証明書を用いたVPNおよび、

仮想デスクトップへのシングルサインオン設定

(PC/シンクライアント)

Ver.1.0 2012 年 10 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. はじる	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
1.4.	電子証明書の発行時における留意事項	6
2. View	接続サーバの設定	6
2.1.	サーバ証明書のインポート	6
3. BIG-I	IP の管理設定	7
3.1.	Active Directory の登録	7
3.2.	アクセスプロファイルの作成	7
4. Gléa	s の管理者設定(PC)	10
5. クラ・	イアント証明書を用いた VPN 接続	10
5.1.	Gléas の UA からのクライアント証明書インストール	
5.2.	VPN アクセス、および仮想デスクトップの利用	11
6. シン	クライアントでの接続設定	13
7. 問い	合わせ	

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 F5 ネットワークス社製 SSL-VPN 装置「BIG-IP Edge Gateway」で VPN を 張り、その認証情報を用いてヴイエムウェア社製仮想デスクトップインフラストラ クチャー「VMware View」に対し、シングルサインオン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。

- 【VPN機器】BIG-IP Edge Gateway (バージョン11.1.0 build 1943.0)
 ※以後、「BIG-IP」と記載します
- 【仮想デスクトップ インフラストラクチャ】VMware View 5
 ※以後、「VMware」と記載します
 ※構成コンポーネントは以下の通りです
 ハイパーバイザー: VMware ESXi 5.0.0
 vCenterサーバ: Windows Server 2008 R2 Standard / vCenter Server 5.0
 View接続サーバ: Windows Server 2008 R2 Standard / View Connection Server 5.0
- 【ドメインコントローラ】Windows Server 2008 R2 Standard
 ※以後、「ドメインコントローラ」と記載します
- > 【認証局】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
- 【クライアントPC】
 Windows 7 Professional SP1 / VMware View Client 5.2.0 build-848202
 ※以後、「PC」と記載します
- ▶ 【シンクライアント】日本HP 6360t Mobile Thin Client

Windows Embedded Standard 7 SP1 / VMware View Client 4.6.0 build366101 ※以後、「シンクライアント」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のVPN接続設定・クライアント証明書による認証設定
 ※弊社のWEBサイトでは、BIG-IPでのクライアント証明書認証をおこなうための環境構築のホワイトペーパーを公開しておりますので、構築時の参考にしてください
 参考URL: http://www.jcch-sss.com/service/support/2011/02/big-ip-ssl-client-auth
- VMware Viewでの仮想デスクトップインフラ環境の構築
 ※WindowsドメインでのユーザID/パスワードを用いてView接続サーバにログインし、仮 想デスクトップを利用できる状態になっていることを前提としています
- 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
- PC・シンクライアント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。

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。



 ViewクライアントはすでにPC・シンクライアントにインストールされている ものとする。またBIG-IPに対するSSLサーバ証明書もすでにインストールさ れているものとする。

- 2. View接続サーバにサーバ証明書をインストールする
- PC・シンクライアントには、Gléasより発行されたクライアント証明書をインポートする
- PC・シンクライアントはBIG-IPに接続する。BIG-IPではクライアント証明書 認証をおこない、さらに二因子認証として、Windowsドメインでのユーザ認 証(パスワード認証)をおこなうが、この時のユーザIDはクライアント証明 書のサブジェクトcn(一般名)から抽出する
- 5. 認証成功後SSL-VPNセッションが確立される。その後、Viewクライアントが 自動的に起動しView接続サーバへの認証がおこなわれ仮想デスクトップが 起動する

1.4. 電子証明書の発行時における留意事項

本環境で利用するクライアント証明書をGléasで発行する際には、以下の点に留意 する必要があります。

 Gléasでのユーザアカウント(=証明書サブジェクトのcn)と、Active Directoryでのユーザ名は同一にする必要があります ※Gléasでは、Active Directoryからアカウント情報をインポートさせることも可能です。 詳細は弊社までお問い合わせください。

2. View接続サーバの設定

2.1. サーバ証明書のインポート

Gléasよりサーバ証明書ファイルをダウンロードします。 そのファイル(*.p12)をView接続サーバの以下のフォルダに配置します。 C:¥Program Files¥VMware¥VMware View¥Server¥sslgateway¥conf¥ (インストール先をデフォルトの場所より変えている場合は、適宜変更してください)

同フォルダにある locked.properties ファイルに以下を記述します。

(locked.properties が存在しない場合は、メモ帳などで新規作成します)

keyfile=[サーバ証明書ファイルのファイル名(*.p12)]

keypass=[Gléasから上記ファイルをダウンロードした時に設定したパスワード]

VMware View Connection Server サービスを再起動すると、設定が反映されます。 この時、ログファイルに以下のようなログが記録されます。 ※ログファイルは以下にあります(デフォルトインストール時)

C:¥ProgramData¥VMware¥VDM¥logs

INFO <Thread-1> [q] The Secure Gateway Server is using SSL certificate store
filename.p12 with password of x characters
INFO <Thread-1> [q] The Secure Gateway Server is listening on https://*:443

3. BIG-IPの管理設定

3.1. Active Directory の登録

左ペインで[Access Policy] > [Access Profile] > [AAA Server] > [Active Directory]を 選択し、右画面で[Create...]をクリックします。

General Properties			
Name	dc01		
Туре	Active Directory		
Configuration			
Domain Controller	10.0.0.1		
Domain Name	jcch-sss-vmware.local		
Admin Name	administrator		
Admin Password	•••••		
Verify Admin Password	•••••		
Timeout	15 seconds		

ドメインコントローラに認証アクセスするための情報を設定します。

3.2. アクセスプロファイルの作成

左ペインで[Access Policy] > [Access Profile]と進み、右側画面で設定をおこなうア クセスプロファイルの[Edit...]をクリックし(あるいは[Create...]ボタンをクリック し新規作成)、ビジュアルポリシーエディター(VPE)を開きます。 ※許可するクライアントなどのその他の接続条件は、必要に応じて追加してください

VPE でアクセスポリシーを設定します。以下は今回の設定例となります。 ※VPE の操作方法については、本書では省略します ※許可するクライアントなどその他の接続条件は、必要に応じて追加してください

Access Policy: /Common/tw	o_factor_auth Edit Endings (Endings: Deny [default], Allow)
Start	Successful + Extract Username Albuck + Logon Page Albuck + AD Auth Albuck + Eul Resource Assign Albuck + ConfigureVewSSO Albuck + Albure Assign Albuck + ConfigureVewSSO Albuck +

Client Cert Inspection	Branch Rule で、クライアント SSL プロファイルで設定さ		
	れたクライアント証明書認証の結果をチェックします(デ		
	フォルトのまま)。		
Variable Assign	カスタム変数 session.logon.last.username に証明書サブジ		
※上図では"Extract Username"という名	ェクト cn 値を代入するように設定します。		
前に設定	※下図ではクライアント証明書のサブジェクトが dc=com,		
	dc=example, ou=sales, cn=username のように cn が 4 番目(固定)		
	であることを想定。この並び順により Custom Expression の 3 行		
	目の"lindex \$f2 3"の右側の"3"を変更する必要があります		
Custom Variable - Unsecure	- Eustom Expression -		
	ext ft foreset (excise of ext whice) 1		
session.logon.last.username	set f2 [split \$f1","]		
	set f3 [lindex \$f2 3] set f4 [split \$f3 "="]		
4	4		
Logon Page	ユーザ ID はすでに取得しているので、Read Only を[Yes]		
	に変更し変更不可に設定して、パスワードのみを入力させ		
	るよう設定します。		
Logon Page Agent	I		
Split domain from full Username			
Type Post var	Table Name Session Variable Name Read Only		
1 text v username	username Yes 🗸		
2 password 🖌 password	password No 🗸		
AD Auth	[Server]には 3.1 項で設定した Active Directory を設定しま		
	す。		
	Branch Rule では、認証結果をチェックします(デフォルト		
	のまま)		
Full Resource Assign	設定済みのネットワークアクセスリソースと、Webtop を指		
	定します。		
Variable Assign	PC にインストールされた View クライアントを起動させま		

プライベート CA Gléas ホワイトペーパー

∼ BIG-IP Edge Gateway & VMware View ~

クライアント証明書を用いたVPNおよび、仮想デスクトップへのシングルサインオン設定

(PC/シンクライアント)

※上図では"configureViewSSO"という	す。
名前に設定	1 行目は、アプリケーション起動時の警告を出現させない設
	定です。2 行目は、View クライアントの起動設定になりま
	す。
Yariable Assign	'
Add new entry	Insert Before: 1 💌
	Assignment
1 [5] 'warn_before_application_launch' prope 1 {0} change	<pre>sty of '/Common/js3-vpn_na_res' (type 'Network Access') = expr</pre>
2 [S] 'application_launch' property of '/Comm { " <application_launch><item><path>C:\\ View\\Client\\bin\\wswc.exe</path><paran password [mcget -secure {session.logon.la - "} change</paran </item></application_launch>	on/js3-vpn_na_res' (type 'Network Access') = expr Progra m Files\WMware heter>-use rname [mcget {session.logon.last.username}] - st.password}] -domainName <os_type>WI NDOWS</os_type>
(1 行目)	
Configuration Variable 👻 Secure	
Type: Network Access 👻	expr {0}
Name: /Common/js3-vpn_na_res -	
Property: warn_before_application_launch	▼
(2 行目)	
Configuration Variable 🔻 Secure	Eustom Expression
Type: Network Access 👻	expr { " <application_launch><item><path>C:WProgram</path></item></application_launch>
Name: /Common/js3-vpn_na_res -	Files\WMware\WMware View\VClient\bin\wswc.exe <parameter>-username</parameter>
	[mcget {session.logon.last.username}] -password [mcget - secure {session.logon.last.password}] -domainName icch-
上図右側の内容は以下の通りです。	
expr {	
" <application_launch><item><pat< td=""><td>th>C:¥¥Program Files¥¥VMware¥¥VMware</td></pat<></item></application_launch>	th>C:¥¥Program Files¥¥VMware¥¥VMware
View¥¥Client¥¥bin¥¥wswc.exe <td>ath><parameter>-username [mcget</parameter></td>	ath> <parameter>-username [mcget</parameter>
{session.logon.last.username}]	-password [mcget -secure
{session.logon.last.password}]	-domainName [ドメイン名] -serverURL [View 接続サーバの
FQDN]	
-unattended <os_type< td=""><td>>WINDOWS" }</td></os_type<>	>WINDOWS" }

```
プライベート CA Gléas ホワイトペーパー
~ BIG-IP Edge Gateway & VMware View ~
クライアント証明書を用いたVPNおよび、仮想デスクトップへのシングルサインオン設定
(PC/シンクライアント)
※View クライアントがカスタムロケーションにインストールされている場合は、正しいパス設定する必要が
あります
※パラメータ「-unattended」を外すと、View クライアントでのログイン後に仮想デスクトップ選択画面が表
示されるようになります
```

4. Gléasの管理者設定 (PC)

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、設定をおこなうUA(申込局)をクリックします。

> UA 申込局 ▶ Gleas Generic UA 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ボート	証明書ストアの種類	ユーザストア	-
🔲 ダウンロードを許可	🗹 インボートワンスを利用す	13	

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。

以上でGléasの設定は終了です。

5. クライアント証明書を用いた VPN 接続

5.1. Gléas の UA からのクライアント証明書インストール

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。



ログインすると、ユーザ専用ページが表示されます。

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。

その後、 [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。

ユーザ情報				
🙎 テスト ユーザ さん	んのページ		_	∎⊴uzi
2ユーザ情報の確認	₨•変更			<u></u>
▶ ユーザ 登録	日時:2010/07/13 09:49			
 >姓:テスト 名:ユーt >ユーザID:testuser >メールアドレス: >パスワード:************************************	f			
# 発	行局 シリアル	有効期限	証明書ストアヘインポート	
<u>₿1</u> JCCH-SS	S demo CA #9235	2013/11/25	証明書のインポート	
		_		T

※「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

5.2. VPN アクセス、および仮想デスクトップの利用

Internet ExplorerでBIG-IPへアクセスします。

PCにインポートされたクライアント証明書による認証(端末認証)と、Active Directory認証(ユーザ認証)を経て、Viewクライアントによる仮想デスクトップへ

の自動接続がおこなわれます。

認証から仮想デスクトップへの流れは以下のとおりです。



クライアント証明書認証(証明書選択ダイアログ)

F5 Networks セキュアログオン
ユーザー名 vmtest01
ログオン

BIG-IPでのユーザ認証画面(ユーザー名は証明書より抽出されているのでグレーアウトされています)

🕐 初期化中です				
トラフィック タイプ	送信	圧縮	受信	圧縮
ネットワークアクセス				
-ネットワークトンネル	0 B	0%	0 B	0%
- 最適化されたアプリケー	0 B	0%	0 B	0%
ション				
合計	0 B	0%	0 B	⁵ 0%

VPNトンネリング(Edge Clientコンポーネント)起動中画面



Viewクライアントの自動起動、及び仮想デスクトップへの自動接続

※3.2項のconfigureViewSSOの2行目のViewクライアントの起動パラメータの設定で、-unattended を付加すると自動的に仮想デスクトップへの接続までおこなわれます(ユーザに割り当てられた 仮想デスクトップが複数ある場合の挙動は弊社未検証)。

※BIG-IPのFQDNがInternet Explorerでの[信頼するサイト]に登録されていない場合(下図)や、 UAC(ユーザのアクセス制御)がオンになっている場合などは、自動起動時にセキュリティ確認 画面が出現します

Security Alert		
Webサイト は信頼できるサイトリストに登録されてい ないためローカルアプリケーションの起動ができません。		
この操作を統行しますか?		
Yes(Y) No(N)		

6. シンクライアントでの接続設定

シンクライアントでは、AdministratorでログインしEWF(Enhanced Write Filter) をオフにしてから以下の設定をおこないます。 (以下は、Userでログイン(デフォルト)しての操作です)

- クライアント証明書のインストール(Userでログイン)
 5.1項のとおりUAからインポートするか、RAよりダウンロードした証明書ファイル(*.p12)
 をダブルクリックすると起動するウィザードでインポートする方法があります
- BIG-IP Edge Client Components (VPNクライアントモジュール)のインストー

BIG-IPへの初回アクセス時にインストールを促されるので、インストールします

 [信頼するサイト]への登録や、必要に応じUACの設定変更(Administratorでのロ グインが必要)をします

以上の設定が終わったら、EWFを有効にして5.2項のとおり接続をおこないます。

7. 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。)

■VMware Viewに関するお問い合わせ先

ヴイエムウェア株式会社 URL:http://www.vmware.com/jp/company/contact.html

■シンクライアントに関するお問い合わせ先

日本ヒューレット・パッカード株式会社 プリンティング&パーソナルシステムズ事業統括 クライアントソリューション本部 製品部 Mail:thinclient.jpn@hp.com

■Gléasや検証用の証明書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