

# プライベート認証局Gléas ホワイトペーパー

Per-App VPN

(BIG-IP APM / Workspace ONE UEM)

Ver. 1.0 2018 年 10 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

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

# 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
1.3.	本書における構成	5
2. WS1	LUEM での Per-App VPN 設定(iOS 向け)	6
2.1.	プロファイル設定	6
2.2.	アプリケーション配布設定	9
2.3.	VMware Browser の設定	11
3. iPad	I での Per-App VPN の実行	12
3.1.	WS1 UEM への加入と VMware Browser のインストール	12
3.2.	Per-App VPN の動作確認	14
4. WS1	LUEM での Per-App VPN 設定(Windows 向け)	15
4.1.	プロファイル設定	15
5. Wind	dows での Per-App VPN の実行	
5.1.	WS1 UEM への加入	
5.2.	Per-App VPN の動作確認	
6. 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「プライベート認証局 Gléas」と、ヴイエムウェア社のデジタル ワークスペース・プラットフォーム「VMware Workspace ONE UEM」(AirWatchの後 継サービス)を連携させ、デバイスにプッシュ配信した電子証明書を利用して、F5ネ ットワークス社の「BIG-IP Access Policy Manager」(APM)をゲートウェイとした Per-App VPN(アプリケーション単位でのVPN接続)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。

- F5ネットワークス BIG-IP Access Policy Manager (バージョン 13.1.1 Build 0.0.4)
   ※以後、「APM」と記載します
- VMware Workspace ONE UEM (バージョン 9.6.0.7)
   ※以後、「WS1 UEM」と記載します
- JS3 プライベート認証局Gléas (バージョン1.16.9)
   ※以後、「Gléas」と記載します
- Webサーバ: Ubuntu 16.04.4 / Apache 2.4.18
   ※以後、「Webサーバ」と記載します。ApacheはOSのパッケージを利用
- ➤ Microsoft Windows 10 Pro
   F5 Access (バージョン 1.2.8.0 Build 51.0) / AirWatch Agent (バージョン 9.7.0.0)
   ※以後、「Windows」と記載します
   ※デスクトップアプリ BIG-IP Edge Client は使いません
- ▶ Apple iPad Air 2 (iOS 12.0)
   F5 Access (バージョン 3.0.2) / VMware Browser (バージョン 6.16.1)
   ※以後、「iPad」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。

APMのVPN設定やクライアント証明書認証の設定
 ※APMでの証明書認証設定について、弊社では以下のURLでドキュメントを公開しています。
 https://www.gleas.jp/news/whitepaper/big-ip-apm
 Per-App VPN接続時にはパスワードなどのユーザ入力待ちが発生してはならないので、本書で
 はクライアント証明書認証のみを前提とします
 以下はAPMでのアクセスポリシーの設定例です



- WS1 UEMの基本操作、およびGléasとの証明書発行連携の設定
   ※WS1 UEM (AirWatch)とGléasの証明書発行連携の設定について、弊社では以下のURLでドキュメントを公開しています
   https://www.gleas.jp/news/whitepaper/airwatch
   事前にWS1 UEMで認証局と証明書発行テンプレートの設定をしておきます
- WindowsやiPadのネットワーク設定や操作方法
   ※F5 Accessはそれぞれのストアからあらかじめインストールしておきます
   ※本検証では、WindowsではFirefoxをVPN接続アプリケーションとします
   FirefoxはあらかじめMozilla CorporationのWebサイトからインストールしておき、実行ファイル (firefox.exe)のパスを調べておきます
- Gléasの基本操作

以上については、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。

プライベート認証局Gléasホワイトペーパー

#### Per-App VPN

#### (BIG-IP APM / Workspace ONE UEM)



- 1. WindowsとiPadで、WS1 UEMへの加入操作をおこなう
- WS1 UEMはGléasと連携して発行した証明書と、Per-App VPN設定を含むプロフ アイルを加入済みのWindowsとiPadに配布する またiPadに対しては、VMware Browserアプリも配布する
- 3. Windowsでは、Firefoxを起動すると自動的にAPMへのVPN接続がおこなわれ、イントラネットWebにアクセス可能となる。
- 4. iPadでは、VMware Browserを起動すると自動的にAPMへのVPN接続がおこなわれ、イントラネットWebにアクセス可能となる。
- 5. Windows、iPadともに他のブラウザではイントラネットWebに接続することはで きない

# 2. WS1 UEM での Per-App VPN 設定(iOS 向け)

### 2.1. プロファイル設定

WS1 UEM の Web 管理コンソールにログインし、[デバイス] > [プロファイルとリソース] > [プロファイル]よりプロファイルを新規に追加します。

iOS 新しい Apple iOS プロファイルを追加 メ				
<ul> <li>◆ 全般</li> <li>ヘ パスコード</li> </ul>	全般			
◎ 制限	名前 *	f5 per-app-vpn test		
<ul><li>WI-Fi</li><li>⑥ VPN</li></ul>	バージョン	1	\$	
💩 Eメール	説明	F5 Per-App VPN検証		
🔀 Exchange ActiveSync		between a sufficiency of the		
通知	展開	管埋对源	v	
LDAP	割り当てタイプ	自動	×	
聞 CalDAV 営 定期配信カレンダー	削除を許可	いつでも	~	
E CardDAV	管理元	JCCH Security Solution Systems Co.,Ltd.		
℅ Web クリップ				
♥ 資格情報	割り当てるグループ	👥 CA01_group	×	
↔ SCEP		ここに入力してグループを追加	Q,	
◎ グローバ↓HTTPプロキ シ	除外	HIN HIN		
◎ シングルアプリモード 🗸				
				保存して公開 キャンセル

資格情報の項目で、クライアント証明書の発行・配布設定と、ルート証明書の配布設定 をおこないます。

※設定内容の詳細は 1.2 項に記載の弊社ホワイトペーパーを参照

資格情報#1				
資格情報ソース	定義済み認証局	~		
認証局 *	Test CA	~		
証明書テンプレート *	vpn-template	~		

### プライベート認証局Gléasホワイトペーパー Per-App VPN

(BIG-IP APM / Workspace ONE UEM)

資格情報#2	
資格情報ソース	アップロード・
資格情報名 *	gleas.cer
証明書 *	証明書アップロード 変更
タイプ	Cert
有効期限開始日	2010/01/11
有効期限終了日	2030/01/06
サムプリント	614A68C8AED89B800D1CB1ED57C703B7C8445E9B

VPN の項目で、以下を設定します。

- [接続名]には、任意の接続名称を入力
- [接続タイプ]は、"カスタム"を選択
- [識別子]には、"com.f5.access.ios"を入力
- [サーバ]には、VPN の接続先ホスト名を入力
- [アプリベース VPN 規則]をチェック
- [自動接続]をチェック
- [プロバイダタイプ]は、"PacketTunnel"を選択
- [ユーザー認証]には、"証明書"を選択
- [ID 証明書]には、資格情報プロファイルで設定したクライアント証明書を選択 ※以下のスクリーンショットでは、資格情報の1番目にクライアント証明書を設定した場合の例と なります
- [オンデマンド VPN を有効化]をチェック

VPN	
接続情報	
接続名 *	f5 new client
接続タイプ *	לאקע 🗸
識別子	com.f5.access.ios
* パーゼ	apm.js3-test12.local
アカウント	+
アイドル状態で切断 (秒)	٢
カスタムデータ	キ- 値 ●追加
アプリ ベース VPN 規則	V
自動接続	$\checkmark$
プロバイダ タイプ	PacketTunnel v
	Safariドメイン
	0
認許	
ユーザー認証	証明書 、
ID 証明書	証明書 #1
オンデマンド VPN を有効化	$\checkmark$
新しいオンデマンド キーを 使用する	
オンデマンド VPN	ドメインまたはホスト オンデマンド アクシ
	常に確立 🗸 🔮

設定完了後、[保存して公開]をクリックし対象デバイスへの割り当てをおこないます。

### 2.2. アプリケーション配布設定

Web 管理コンソールで[アプリとブック] > [ネイティブ] > [パブリック]と進み、[アプ リケーションの追加]をクリックし、VMware Browser を検索、追加します。

検索			
		vmware browser	
	VMware Browser	VMware Browser は、Safari に代わる、安全なインターネット閲覧を提供する iOS デバイス向けオプ ションです。今歳 IT 管理専が各社後间のエンド ユーザーのニーズに応じてカスタマイズおよび構成で	
Ø	com al-watch.secure.browser フリー カテゴリ: Business 現在のバージョン: 6.16.1	きます。またすべてのインターネット騒気をセキュア化し、抽定Web かくからかに増減を制限するこ とにより、貸仕さビイル・テクノロシーの意思を受けながら、セキュリティノンなを組成できます。 注 Whate Browset & 理想コンシールと違い。コンシールで増えされるシステムな安全後して 置見されます。Whate Browset の使用には、ArWatch インフラストラクチャが多差でき、Whate Decome Are 0.2 に、メオイビー、使力に変更がなかかか、の人がない、Marcon	
		Browserをインストールする用に、異在!! 管理者までお問い包ひてください。WWware Browserの注 更極能セキュリティ・ArWatch Tunnel およびFS デバイスと達成し、企業ファイアウォール内の Web サイトが閲覧可能に・加入資格情報で、指定 Web サイトに目動的に認証・VMware Secure Cont	

追加したのちに、[編集]タブをクリックし以下の設定をおこないます。

 SDK タブの[SDK プロファイル]で、作成した SDK プロファイルを選択 ※SDK プロファイルは、[グループと設定] > [すべての設定] > [アプリ] > [設定とポリシー] > [プ ロファイル]で作成できます。VMware Browser の機能制限など各種設定をおこなうことが可能で すが、本書の主旨から外れるので説明は省きます

また[割り当て]をクリックして、[割り当ての追加]、或いは既に割り当ててあるグループ を選択し、以下の設定をおこないます。

- [管理アクセス]で、"有効"を選択
- [アプリトンネル]で、"有効"を選択
- [アプリベース VPN プロファイル]で、3.1 項で設定した VPN 項目を含むプロファイ ルを選択



VMware Browser - 割り当ての追加	×
割り当てグループを選 択 ここに入力してグループを追加 Q	
アプリ配信方法* 自動 オンデマンド	
ポリシー	
柔軟な管理レベル: <b>管理アクセス</b>	
デバイスの管理に基いて、ユーザーにアプリへのアクセスを与えるポリシ を適用します。	/
データ漏洩防止 (DLP) を有効化しますか? DLP ポリシーにより、デバイス上の管理アプリケーションおよび非管 理アプリケーション間データ交換を制御できます。 このアプリのデータ損失を防止するには、「管理アクセス」にし、目 的のデバイスタイプに対して「制限事項」プロファイルを作成します。	
管理アクセス 有効 <u>急効</u> ()	•
加入解除時に削除 有効 無効	
アプリケーションの 有効 <u>無効</u> () バックアップを防ぐ	
ユーザーがインストー 有効 気効 ① ルしたアプリを MDM 管理対象にする	
アプリトンネル 有効 無効 (i) iOS	7+
アプリベース VPN プ f5 per-app-vpn test @ JCCH Security So ヾ () ロファイル *	
アプリケーション構成 有効 無効 ①	
<u>送加</u> =	キャンセル

設定完了後、[保存して公開]をクリックし対象デバイスへの割り当てをおこないます。

### 2.3. VMware Browserの設定

Web 管理コンソールで[グループと設定] > [すべての設定] > [アプリ] > [Browser]と進 むと、VMware Browser の各種設定がおこなえます。 本書の主旨から外れるので詳細設定は省きますが、テスト用 Web サイトの URL をブッ クマークに追加しておきます。

#### プライベート認証局Gléasホワイトペーパー

#### Per-App VPN

(BIG-IP APM / Workspace ONE UEM)

Browser 🕐				
ブラウザ設定	ブックマーク	通知		
現在の設定	○ 継承	● オーバーライド		
ブラウザに事前定義	するブックマークのUR	XL (j)		
名前		URL		
testWeb http://10.10.11.10				
● ブックマークを追加				

※上のスクリーンショットのようにサーバ URL に IP アドレスを使う場合は、[ブラウザ設定]タブの[IP 閲覧を許可する]を有効にし、[許可された IP アドレス]に Web サーバの IP アドレスを指定する必要が あります

IP 閲覧を許可する	有効	無効	
許可された IP アドレス	10.10.11.10		
	それぞれの IP ア さい。それぞれの リストするには、 使用します。IP 7 IPv4 形式で入力す	ドレスを改行また )オクテットにあ アステリスク (* ?ドレスは、有効 する必要がありま	-はコンマで区切ってくだ るすべての値をホワイト )をワイルドカードとして な値とピリオド使った す。例 さらに表示

設定完了後、[保存]をクリックして設定を保存します。

# 3. iPad での Per-App VPN の実行

### 3.1. WS1 UEMへの加入とVMware Browserのインストール

iPad で WS1 UEM に加入すると、WS1 UEM と Gléas との間で証明書発行がおこなわ れ、少しの時間が経つと SSL-VPN やクライアント証明書を含むプロファイルが自動イ ンストールされます。

また WS1 UEM 加入後に、3.2 項で設定した通り VMware Browser をインストールする旨のメッセージが表示されるのでそれに従いインストールをおこないます。



プロファイルは iPad の[設定]アプリで[一般] > [プロファイルとデバイス管理]と進み、 [デバイスマネージャ]という名前でインストールされ、タップすることで内容を確認で きます。

<b>く</b> プロファイ	ルとデバイス管理 <b>プロファイル</b>
	デバイス マネージャ
署名者	*awmdm.com 検証済み ✓
説明	デバイス上の仕事用アプリケーションおよびサービスを管理およびアクティブ化する際に使用する、 デバイス管理プロファイルです。
内容	モバイルデバイス管理 管理対象App AppレイヤーVPN設定 Webクリップ:1 証明書:4
詳細	>
Арр	1 >
	削除

またその状態で F5 Access を起動すると、[アプリごとの]欄で Per-App VPN が追加されていることがわかります。

	F5 Ac	cess	
2	エンタープライズVPN		
	接続先設定	新規追加 >	
	状況	切断されました	
	アプリごとの		
	f5 new client apm.js3-test12.local		

# 3.2. Per-App VPNの動作確認

この状態で VMware Browser を起動すると、自動的に VPN 接続がおこなわれます。 接続時には iPad 画面の右上に VPN マークが表示されます。

TOTA SIMPRIM				
<	>	G	ブックマーク	
		$\mathbf{\overline{\cdot}}$	1	
		Catalog	testWeb	

ブックマーク設定してある APM の内部セグメントに接続されている Web サーバヘア クセスすると閲覧可能となります。

100	10.0		🗢 VPN 🕫 82% 🔳,
<	> 6	10.10.11.10	
	(O) ubunt	Apache2 Ubuntu Default Page	
		It works!	

ホームボタンを押下して VMware Browser を閉じると VPN マークの表示は消えます。 同じ URL に対して safari などの他のブラウザでアクセスすると、Web サーバに接続で きないためエラーとなります。

1000	100						(÷	82% 🔳
<		$\square$		10.10.11.10	Ç	Ê	+	
			ページを開けません。	サーバが応答を停止してい	ます。			

# 4. WS1 UEM での Per-App VPN 設定(Windows 向け)

## 4.1. プロファイル設定

WS1 UEM の Web 管理コンソールにログインし、[デバイス] > [プロファイルとリソース] > [プロファイル]よりプロファイルを新規に追加します。

【 新しい Windows デス	マクトップ プロファイ	ルを追加			×
● 全版 A VPN	全般				
♥ 資格情報	名前 *	win10-perapp-vpn			
<ul> <li>シングルアプリモード</li> </ul>	バージョン	1	<b>.</b>		
※ Web クリップ 窓 Exchange ActiveSync	説明				
<-> SCEP	展開	管理対象	*		
☆ カスタム設定	割り当てタイプ	自動	×		
	削除を許可	いつでも	~		
	管理元	JCCH Security Solution Systems Co.,Ltd.			
	割り当てるグループ	ま CA01_group ここに入力してグループを追加	<b>×</b>		
	除外				
				保存して公開	キャンセル

資格情報の項目で、クライアント証明書の発行・配布設定をおこないます。

資格情報#1		
資格情報ソース	定義済み認証局	*
認証局 *	Test CA	*
証明書テンプレート *	vpn-template	*
キーの位置	ソフトウェア	*
証明書ストア	個人	~

※設定内容の詳細は 1.2 項に記載の弊社ホワイトペーパーを参照

VPN の項目で、以下を設定します。

- [接続名]には、任意の接続名称を入力
- [接続タイプ]は、"F5 Edge VPN"を選択
- [サーバ]には、VPN の接続先ホスト名を入力
- [カスタム構成 XML]に以下を入力

<f5-vpn-conf><client-certificate><issuer>ISSUER\_CA\_NAME</issuer></client-certificate><prompt-for-credentials>false</prompt-for-credentials></f5-vpn-conf>

※上記の"*ISSUER\_CA\_NAME*"の部分は、資格情報プロファイルで指定したクライアント証明書を 発行する CA の名前(クライアント証明書の発行者 CN)に変更します

- [アプリ識別子]は、"デスクトップアプリ"を選択し、その下には Per-App VPN の対象 アプリケーションの実行ファイルのパスを入力 例: C:¥Program Files (x86)¥Mozilla Firefox¥firefox.exe
- [VPN オンデマンド]をチェック
- [ルーティングポリシー]には、"外部リソースにダイレクトアクセスを許可"を選択 (スプリットトンネリングを許可)

VPN	
接続情報	
接続名 *	APMtest2
接続タイプ *	F5 Edge VPN 👻
サーバ*	apm.js3-test12.local
高度な接続設定	
カスタム構成	
カスタム構成 XML	<f5-vpn-conf><client-certificate> ^ <issuer>Evaluation CA</issuer></client-certificate></f5-vpn-conf>
VPN トラフィック規則	
アプリベース VPN 規則	
アプリ識別子	デスクトップアプリ
	C:\Program Files (x86)\Mozilla Firefox\firefox.e
VPN オンデマンド	
ルーティングポリシー	外部リソースにダイレクトアクセスを許可 、
VPN トラフィックフィ ルタ	
● 新しいアプリペース VPN	接動を注加する
デバイス全体の VPN ルー ル	D
<ul> <li>デバイス全体の新しい VPN</li> </ul>	リルールを追加する
ポリシー	
資格情報を保存	有効化 無効化
常にオン	有效化 無效化 ①
ローカル接続ではバイパス	有効化 無効化
信頼されたネットワークを 検出する	

設定完了後、[保存して公開]をクリックし対象デバイスへの割り当てをおこないます。

# 5. Windows での Per-App VPN の実行

5.1. WS1 UEMへの加入

Windows で WS1 UEM に加入すると、WS1 UEM と Gléas との間で証明書発行がおこ なわれ、少しの時間が経つと SSL-VPN 設定やクライアント証明書が自動インストール されます。

追加された VPN 設定は、Windows の[設定] > [ネットワークとインターネット] > [VPN] (ms-settings:network-vpn) と進むと確認できます。

步定	
俞 木-ム	VPN
設定の検索の	VPN
ネットワークとインターネット	+ VPN 接続を追加する
多 状態	APMtest2
n Wi-Fi	0,00
🗟 ダイヤルアップ	詳細オプション
8° VPN	従量制課金接続経由での VPN を許可

また、インストールされたクライアント証明書は、インターネットオプション (inetcpl.cpl)の[コンテンツ]タブ > [証明書(C)] > [個人]タブの中で確認できます。

### 5.2. Per-App VPNの動作確認

この状態で Firefox を起動すると、自動的に VPN 接続がおこなわれます。 VPN の設定を見ると"接続済み"と表示され、APM の内部セグメントに接続されている Web サーバへアクセス可能となります。

← 設定		- 🗆 ×	ファイルロ 編集(E) 表示(M) 履歴(S) ブックマーク(B) ツール(D) ヘルプ(H) ー ロ ×
ŵ ホ−ム	VPN		$\begin{array}{c c} Apache2 Uburut Default Page II: = X & + & & \\ \hline & & & \\ \hline \\ \hline$
設定の検索の	VPN		な よ 見 る ベージ ● Firefox を使い こ な そう へ
ネットワークとインターネット	+ VPN 接続を追加する		🧿 Apache2 Ubuntu Default Page
● 状態	APMtest2		ubuntu
// Wi-Fi	接続済み		It works!
ダイヤルアップ	詳細オプション	切断	This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed this site is working properly. You should replace <b>this</b> file (located at /var/we/ht1/index.hta) before
98º VPN			continuing to operate your HTTP server.

接続された状態で、同じ URL に対して Edge などの他のブラウザでアクセスすると、 Web サーバに接続できずエラーとなります。 プライベート認証局Gléasホワイトペーパー Per-App VPN

(BIG-IP APM / Workspace ONE UEM)

← 設定		- 🗆 X		Can't reach this page	× + ~			-	□ ×
命 ホーム	VPN		$\leftarrow  \rightarrow$	0 ଲି <sup>()</sup>	10.10.11.10/	□ ☆	墙	h	ē
設定の検索・パーク	VPN								
ネットワークとインターネット	VPN 接続を追加する			$\bigcirc$	このページを表示できませ	th			
● 状態	T				対処方法				
<i>i</i> ∕‰ Wi-Fi	APMtest2 接続済み				<ul> <li>Web アドレスが正しいことを確認してください http://10.10.11.10</li> </ul>	:			
☺ ダイヤルアップ		詳細オプション 切断			<ul> <li>Bing で "http://10.10.11.10" を検索してく</li> </ul>	ťż			
% VPN					<ul> <li>パージを最新の情報に更新</li> </ul>				

# 6. 問い合わせ

#### ■BIG-IP APM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 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)

#### ■Workspace ONEに関するお問い合わせ先

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

#### ■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