

プライベート認証局Gléas ホワイトペーパー

Pulse Connect Secure / Workspace ONE UEMでの Per-App VPN

Ver. 1.0 2019 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

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

プライベート認証局Gléasホワイトペーパー Pulse Connect Secure / Workspace ONE UEMでのPer-App VPN

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	UEM での Per-App VPN 設定	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	.8
2.3.	Workspace ONE Web の設定	.9
3. PCS	での設定	9
3.1.	User Roll の設定	.9
3.2.	SAM Access Control の設定1	.2
4. iPad	での Per-App VPN の実行1	.1
4.1.	WS1 UEM への加入と Workspace ONE Web のインストール1	.1
4.2.	Per-App VPN の動作確認1	.2
5. 問い	合わせ1	.3

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、Pulse Secure社の「Pulse Connect Secure」 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。

- Pulse Secure Pulse Connect Secure (バージョン 9.0R2 Build 63965)
 ※以後、「PCS」と記載します
- VMware Workspace ONE UEM (バージョン 18.11.0.4)
 ※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: CentOS 7.6.1810 / Apache 2.4.6
 ※以後、「Webサーバ」と記載します。ApacheはOSのパッケージを利用
- ➤ Apple iPad (iOS 12.1.1) Pulse Secure (バージョン 7.1.1 78493) / Workspace ONE Web (バージョン 7.2.1) ※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。

PCSのVPN設定およびクライアント証明書認証の設定
 ※PCS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/pulse-connect-secure
 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

- 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
- iPadのネットワーク設定
- 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。



- 1. 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 ァイルをiPadに配布する
- 3. iPadで、Workspace ONE Webを起動すると自動的にPCSへのVPN接続がおこな われ、社内サーバにアクセス可能となる。

2. WS1 UEM での Per-App VPN 設定

2.1. プロファイル設定

WS1 UEM の管理画面で、[デバイス]→[プロファイルとリソース]→[プロファイル]と進み、[追加]のドロップダウンリストから[プロファイルを追加]をクリックします。

🕲 Workspace ONE UEM			JCCH Security Solution Syste 🗸	
(注) はじめに	ダッシュボード		デバイス 🕨 プロファイルとリソース	
\sim	リスト表示		プロファイル	
10 E	プロファイルとリソース	ý	フィルタ ≫ 🔝加 🗸	
म इत्य	プロファイル		プロファイル詳細 管理元	割り当てタイプ
答	リソース (新)		adds-test Apple IOS ICCH Security Solution Systems Co. Ltd.	オブション
アカウント	パッチの状態		・ 資格情報	17727
詳 アプリとブック	プロファイル設定 順守ポリシー	> >	 EASテスト Apple IOS 資格情報, Exchange JCCH Security Solution Systems Co.,Ltd. 	オプション

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	アップロード	
資格情報名 *	ia1test.der	
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	2018/03/28	
有効期限終了日	2019/03/31	
サムプリント	BE34BB900CA887378D00DD1	
	消去	
資格情報 #2		
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 *	testca-pulse-devComp	

VPN の項目で、以下を設定します。

- [接続名]に任意の接続名称を入力
- [接続タイプ]は[Pulse Secure(Legacy)]を選択
- [サーバ]に 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
- [プロバイダタイプ]は[AppProxy]を選択
- [ユーザー認証]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は、資格情報の2番目にクライアント証明書を設定した場合の例です
- [オンデマンド VPN を有効化]をチェック

iOS 新しい Apple iOS フ	ロファイルを追加			×
◎ 全般				
Φ ₆ バスコード	VPN			
◎ 制限	接続情報			
🗇 Wi-Fi	接続名 *	PCS		
A VPN				
≜ E×−ル	接続タイプ *	Pulse Secure (Legacy) v		
53 Exchange ActiveSync	サーバ・	pcs.jcch-sss.local		
111 通知				
LDAP	アカウント		*	
CalDAV	アイドル状態で切断(秒)			
豆 定期配信カレンダー				
I CardDAV	レルム			
≫ Web クリップ	役割			
🖤 資格情報 🛛 🔞		-		
<→ SCEP	アプリ ベース VPN 規則			IOS7
◎ グローバルHTTPプロキ シ	自動接続	2		IOS7
	プロバイダ タイプ	AppProxy ~		
		Səfəriドメイン		
		0		
	認証			
	art, rank	Read do		
	ユーザー認証	証明書 。		位結左切探するための道線運転
	ID 証明書	Certificate #2 ~] *	接続を設置するための具管用権
	オンデマンド VPN を有効化	0		
	新しいオンデマンド キーを使用 する	0		
	オンデマンド VPN	ドメインまたはホストがー オンデマンド アクション		
		常に確立 ~ (2	
	プロキシ			
				⊕ ⊖
				保存して公開 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。

2.2. アプリケーション配布設定

WS1の管理画面で[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、[Workspace ONE Web]を検索、追加します。

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して[保存して割り当て]をクリックします。
 ※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。Workspace ONE Web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

0	アブ	ク o 状	- ションの編集 - Web - Wor 創 育務 管理売: JCCH Security Solution Systems Co	kspace ONE
詳細	利用规约	SDK		
SDK 7	ロファイル		iOS Default Settings @ Global	* ()
アプリ	のプロファイル		選択	× ()

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、2.1 項で設定した VPN 項目を含むプロファイ ルを選択

1

Web - Workspace (Veb - Workspace ONE - 割り当ての追加						
	イプに対して	「制限事項」ブ	ロファイルを作成しま	95	構成する		
管理アクセス	有効	無効	0				
加入解除時に削除	有効	無効	0				
アプリケーションのバッ クアップを防ぐ	有効	無効	0				
ユーザーがインストール したアプリを MDM 管理 対象にする	有効	無効	0				
アプリトンネル	有効	無効	0		iOS 7+		
アブリ ベース VPN ブロフ ァイル*	PCS-IOS @ JCCH	Security Soluti	on Systems Co. 👻 🤇	D			
アプリケーション構成	有効	無効	0				
					_		
					追加 キャンセル		

8 / 13

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. Workspace ONE Webの設定

WS1 の管理画面で[グループと設定]→[すべての設定]→[アプリ]→[Workspace ONE Web]と進みます。

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。

> システム	アプリ	
> デバイスとユーザー	Workspace ONF Web	D @
✓ アプリ	Workspace one we	
> アプリスキャン	Workspace ONE Web の設定	ブックマーク 通知
・アフリケーション統合 Workspace ONE Web ・Workspace ONE Container Inbox	現在の設定 Workspace ONE Web で事前定義さ	○ 継承 ○ オーバーライド れたブックマークの URL ①
> 設定とポリシー	名前	URL
Microsoft Intune® アプリ保護ポリシ ー	testWeb	http://192.168.30.244
> コンテンツ	● ブックマークを追加	
> Eメール		
> テレコム	サブグループの権限 *	○ 龍承のみ ○ オーバーライドのみ ○ 継承またはオーバーライド
 Adv THE ALC 		

※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

設定完了後、[保存]をクリックして設定を保存します。

3. PCS での設定

3.1. User Rollの設定

[Users] \rightarrow [User Roles] で今回使用する User Role をクリックして設定を開きます。 [Access features] \rightarrow [Secure Applycation Manager] で[Windows version]を選択し て[Save Changes]をクリックします。

プライベート認証局Gléasホワイトペーパー Pulse Connect Secure / Workspace ONE UEMでのPer-App VPN

✓ Access features	
Check the features to enable for this user	role, and specify any role-based of
Web	0 Bookmarks Options
 Files, Windows 	0 Bookmarks Options
Files, UNIX/NFS	0 Bookmarks Options
Telnet/SSH	0 Sessions Options
Secure Application Manager	0 Applications Options
Windows version	Note: On Windows Mobile, Pulse
Java version	

3.2. SAM Access Controlの設定

[Users] → [Resource Policies] → [SAM] → [Access Control]と進み、[New Policy] をクリックします。[Name]に任意の名前を、[Resources]にイントラサーバのドメイン 名あるいは IP アドレスと使用ポートを、[Roles]では[Policy apply to SELECTED roles] を選択し、適用させる Role を[Selected roles]に加え、[Actions]で[Allow ~]を選択し、 [Save Changes]をクリックします。

💲 Pu	<mark>lse</mark> Secure	System	Authentication	Admin
General	Detailed Rules			
* Name: Description:	Policy1			
✓ Resources				
* Resources:	Specify the resources for which this po NOTE: This does not support IPv6. 192.168.30.244:80	Exa U U U U U U U U U U U U U U U U U U U	ver line. ampiles: SER>.domain.com:22,23 shange*.domain.com:* 10.10.10/255.255.255.0/8 10.10.10/24:8000-9000	0,443,8080
♥ Roles				
	 Policy applies to ALL roles Policy applies to SELECTED Policy applies to all roles OTI 	roles HER THAN thos	e selected below	
	Available roles:	Selec	cted roles:	
	(none) Ad Re	d ->	13	
Y Actions				
(Allow socket access Deny socket access Use Detailed Rules(see Detail	iled Rules page))	
[Save Changes Save as C	бору		

4. iPad での Per-App VPN の実行

4.1. WS1 UEMへの加入とWorkspace ONE Web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 接続設定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、2.2 項で設定した通り Workspace ONE Web 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。

Appのイ	ンストール
"techp-ds.awmd	Im.com"によりApp
StoreからApp "VM	ware Browser"がイン
ストールされ、	管理されます。
お使いのiTunesアカ	ウントにはこのAnnの
お使いのiTunesアカ	ウントにはこのAppの
料金は課金	されません。

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。

く プロファイ	イルとデバイス管理 プロファイル
	デバイス マネージャ
署名者	*.awmdm.com 検証済み ✓
說明	デパ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、 デパイス管理プロファイルです。
内容	モパイルデバイス管理 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 Pulse Secure アプリを起動すると、[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。・

要求時に接続	
要求時に接続 タップして詳細を表示	
アプリ VPN 毎	
アプリ VPN 毎 タップして詳細を非表示	
VPN は特定のアプリケーション用にのみ指定されています	
com.air-watch.secure.browser	(i) >

4.2. Per-App VPNの動作確認

iPad で Workspace ONE Web 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。



ブックマーク設定してあるイントラ Web サーバヘアクセスできるようになっています。

Workspace ONE Web 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しても、VPN に接続できないため、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 Pulse Connect Secure / Workspace ONE UEMでのPer-App VPN

5. 問い合わせ

■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

■Pulse Connect Secureに関するお問い合わせ先

パルスセキュアジャパン株式会社

Tel: 03-6809-6836

Mail: info_jp@pulsesecure.net

■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