JCCH・セキュリティ・ソリューション・システムズ

プライベート認証局Gléas ホワイトペーパー

Pulse Connect Secure / MobileIronでのPer-App VPN

Ver. 1.0

2019 年 3 月

目次

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、MobileIron社のMDM/EMM「MobileIron Cloud」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

- MobileIron Cloud（Platinum バージョン R59）

※以後、「MobileIron」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、「イントラサーバ」と記載します。ApacheはOSのパッケージを利用

- クライアント：Apple iPad (iOS 12.1.1)

Pulse Secure (バージョン 7.1.1 78493) / Web@Work (バージョン 2.6.0)

※以後、「iOS」「Pulse Secureアプリ」「Web@Work」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

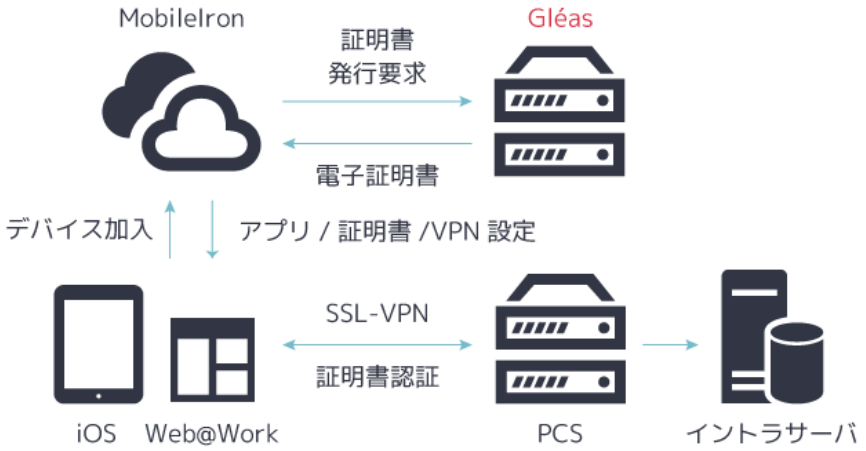
Per-App VPN接続時にはパスワードなどのユーザ入力待ちが発生してはならないので、本書ではクライアント証明書認証のみを前提とします

● MobileIronの基本設定およびGléasとの証明書発行連携の設定
※MobileIronとGléasの証明書発行連携の設定について、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/mobileiron
事前にMobileIronで、Connectorの設置、外部認証機関の設定、ID証明書（動的生成）の設定をしておきます
● iOSのネットワーク設定
● Gléasの基本設定

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. iOSでMobileIronへの加入操作をおこなう
2. MobileIron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、Pulse Secureアプリ、Web@WorkをiOSに配布する
3. iOSでWeb@Workを起動すると、自動的にPCSへのVPN接続がおこなわれ、イントラサーバにアクセス可能となる。

2. MobileIron での設定

2.1. Per-App VPN設定

MobileIron の管理画面で、[構成]→[+追加]→[Per-App VPN]と進みます。

- [名前]に任意の名前を入力します。

- [接続の種類]に[PulseSecure]を選択
- [サーバー]に PCS の URL を入力
- [ユーザー認証]に[証明書]を選択
- [認証情報]には Gléas から発行するように設定された ID 証明書（動的生成）の構成設定名を選択
- [オンデマンド VPN を有効化]にチェック

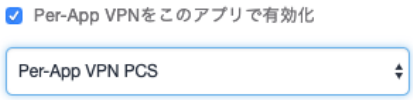
上記の設定をしたら[次へ]をクリックし、構成を有効化するデバイスを選択し、[完了]をクリックします。

2.2. アプリケーションの配布設定

MobileIron の管理画面で[アプリ]→[+追加]と進み、iOS 用の[Pulse Secure]を検索、追加します。

続いて[アプリ]→[+追加]と進み、[Web@Work]を選択して[次へ→]をクリックします。

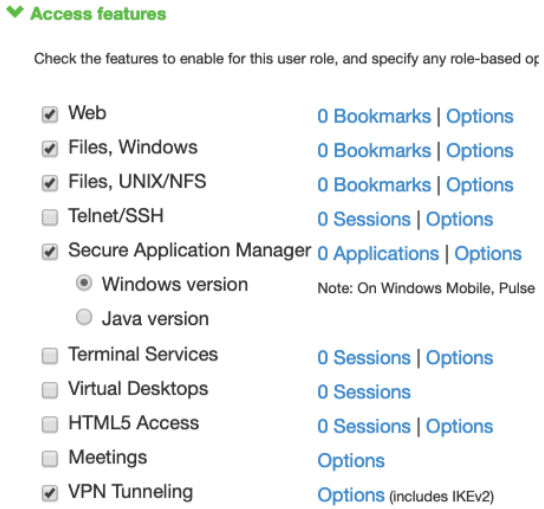
[アプリ委譲]と[配布]の項目は任意で設定します。[アプリ構成]では[デバイスにインストール]を[on]にし、[Per-App VPN]で、 [名前]に任意の名前を入力します。
[Per-App VPN をこのアプリで有効化]にチェックを入れ、[Per-App VPN 構成を選択]で、2.1.項で設定した Per-App VPN 設定を指定し、[次へ→]、[完了]をクリックします。



3. PCS での設定

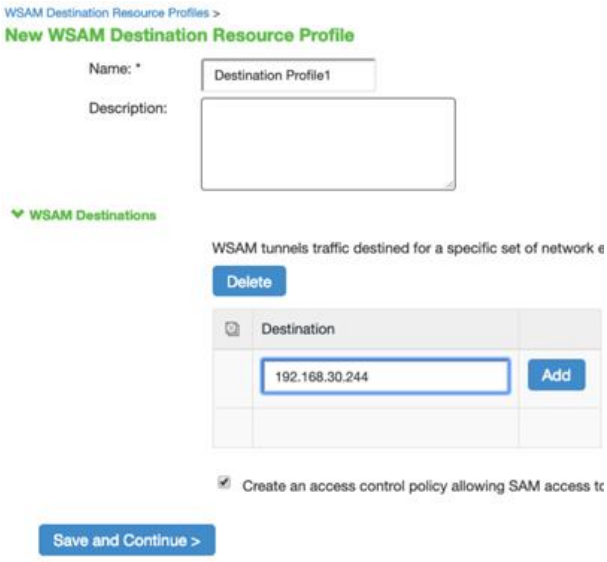
3.1. User Rollの設定

[Users] → [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] → [Secure Applycation Manager] で[Windows version]を選択して[Save Changes]をクリックします。



3.2. WSAM Destinationの設定

[Users] → [Resource Profiles] → [WSAM Destinations]と進み、[New Profile]をクリックします。[Name]に任意の名前を、[Destination]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入力して、[Add]をクリックします。



[Save and Continue]をクリックし、[Available Roles]から使用する Role を選択して[Add ->]をクリックし、[Save Changes]をクリックします。

4. iOS での操作

4.1. MobileIronへの加入

iOS で MobileIron に加入すると、MobileIron は 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 PCS への VPN 接続設定やクライアント証明書を含むプロファイルと、2.2.項で設定したアプリが自動インストールされます。

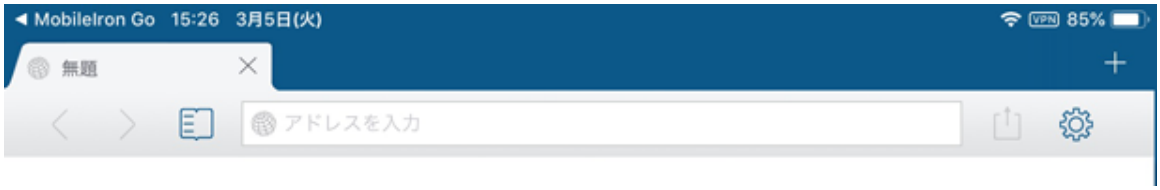
※ID 証明書（動的生成）の設定で、主体者[CN=]に該当するアカウントが Gléas に存在しない場合はクライアント証明書の発行が行われません

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。

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。

4.2. Per-App VPNの動作確認

iOS で Web@Work 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 iOS 画面の右上に VPN マークが表示されます。



イントラサーバへアクセスできるようになっています。

Web@Work 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。

5. 問い合わせ

■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