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

AirWatchと連携したクライアント証明書発行配布

Ver.2.1
2018 年 3 月

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
1.4. 留意事項 6
2. Gléas の事前設定 7
3. AirWatch の管理者設定 9
3.1. ACC を利用する場合の設定 9
3.2. 認証局の設定 10
3.3. プロファイル設定（iOS） 12
3.4. プロファイル設定（Android） 14
3.5. プロファイルの設定（Windows） 16
4. AirWacth からのクライアント証明書配信 17
5. 問い合わせ 18

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、VMware のモバイルデバイス管理サービスである AirWacth とを連携させてクライアント証明書の発行およびクライアント端末への自動配布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。

- モバイルデバイス管理：VMware AirWatch 9.2.2.1
  ※以後、「AirWatch」と記載します
- 中継用サーバ：Windows Server 2012 R2 /
  VMware Enterprise System Connector 9.2.1.0
  ※本ソフトウェアに含まれるAirWatch Cloud ConnectorをAirWatchとGléasの中継用に利用します。以後、「ACC」と記載します
- 認証局：JS3 プライベート認証局Gléas（バージョン1.14.6）
  ※以後、「Gléas」と記載します
- クライアント：iPad Air2（iOS 11.0）
  ※以後、「iPad」と記載します
- クライアント：Nexus 9（Android 7.1.1）/ AirWatch MDM Agent 8.0.0.101
  ※以後、「Android」と記載します
- クライアント：Windows10 Pro / VMware AirWatch Agent 1.2.6.0
  ※以後、「Windows」と記載します

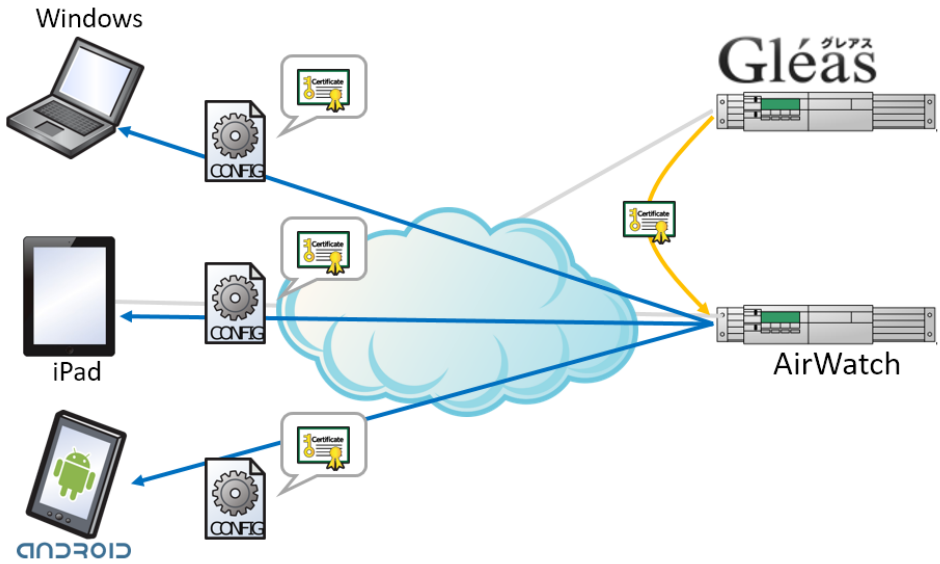
以下については、本書では説明を割愛します。

- AirWatchの基本操作、ACCのインストール方法
- 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

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。

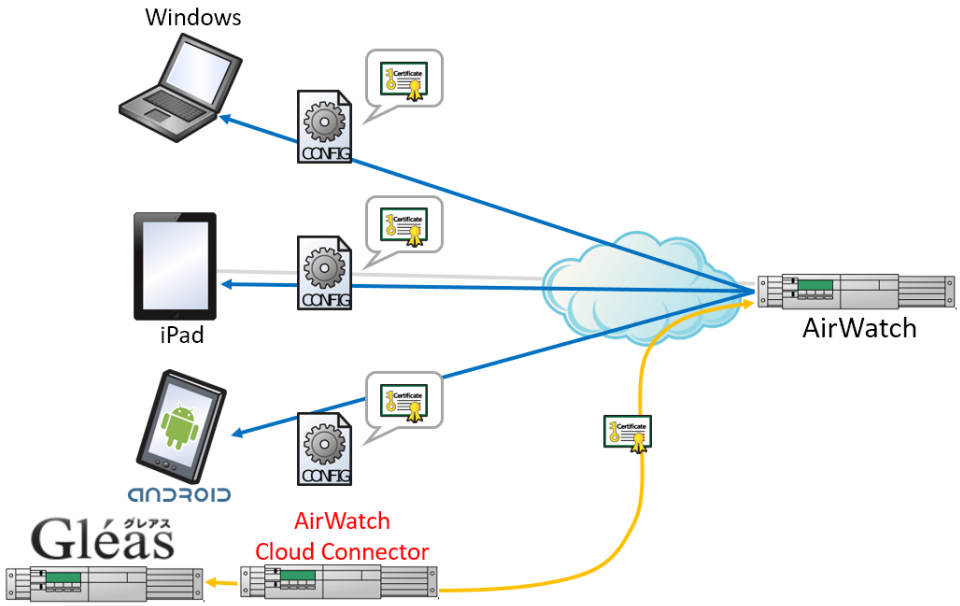
1.3. 本書における構成

本書では、以下の構成で検証を行っています。



1. 事前にAirWatchの管理画面上でクライアント証明書を発行する認証局を設定し、プロファイル（資格情報）に指定する
2. 各クライアントがAirWatchの管理下になり、証明書の配布設定が含まれるプロファイルが適用される
3. AirWatchよりGléasのAPI経由で証明書発行リクエストが送信されると、Gléasはクライアント証明書を発行しAirWatchにレスポンス送信する
4. AirWatchは発行されたクライアント証明書（および、その証明書を認証に利用するVPN、Wi-Fi、Exchange ActiveSyncなど）を含むプロファイルをクライアントに自動インストールする

また、Gléasが宅内にありインターネット上のAirWatchからの直接通信を許可することが難しい場合は、ACCを設置し中継サーバとすることでインターネット側からの通信をしないよう構成することも可能です。

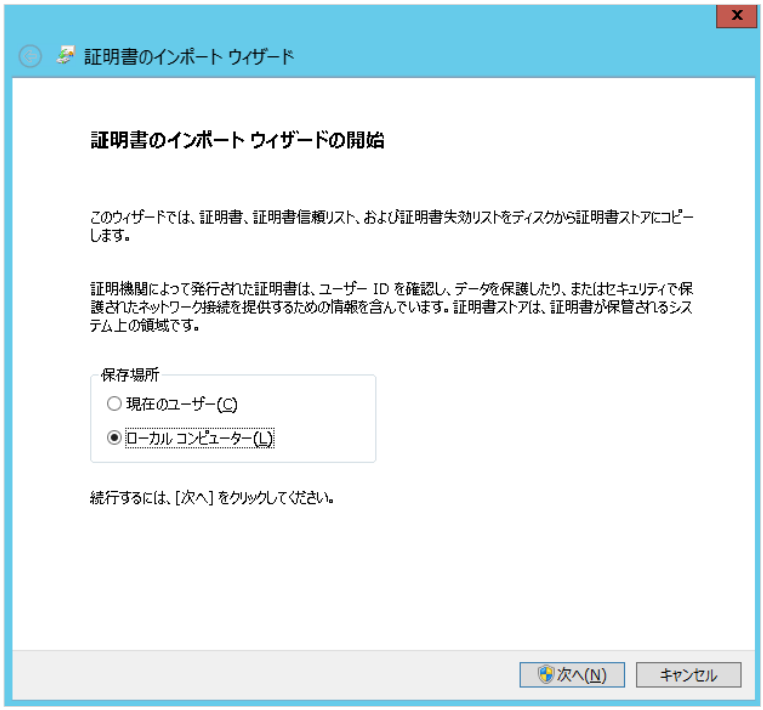


1.4. 留意事項

AirWatchよりAPI経由でGléasにアクセスする場合は、GléasのRA/IA用のSSLサーバ証明書には公的な証明書を利用する必要があります。
詳細は最終項のお問い合わせ先までお問い合わせください。

なお、ACCを利用する場合はこの必要はありません。
代わりにGléasの管理用認証局のルート証明書を、ACCを動かしているWindows Serverの証明書ストアにインポートする必要があります。
Gléasの管理用認証局のルート証明書は以下よりダウンロード可能です。
http://hostname.example.com/crl/ia2.der

※以下の操作は管理者権限が必要です
ACCを動かしているWindows Server上にダウンロードしたファイルを配置し、そのファイルを右クリックし［証明書のインストール(I)］を選択します。
証明書のインポートウィザードが起動しますので、以下の通りにします。



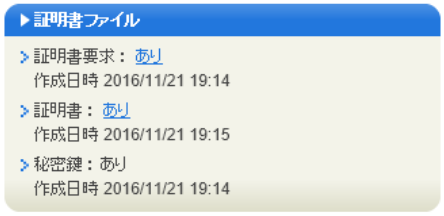
ページ	設定
証明書のインポートウィザードの開始	[ローカルコンピューター(L)]を選択し、[次へ(N)]をクリック
証明書ストア	[証明書をすべて次のストアに配置する(P)]を選び、証明書ストアに[信頼されたルート証明機関]を選択。 [次へ(N)]をクリック
証明書インポートウィザードの終了	[完了]をクリック

2. Gléas の事前設定

Gléas に対し API アクセスをするためには、事前に API 管理者アクセス用の証明書を設定する必要があります。

※ 下記設定は、Gléas 納品時等に弊社で設定を既に行っている場合があります

Gléasの管理者画面RAにログインし、API管理ユーザアカウントの証明書詳細画面に移動し、[証明書：あり]のリンクより証明書ファイル（crtファイル）をダウンロードします。



その後、画面上部の[▶管理者]リンクより管理者一覧 ＞ API管理者の詳細画面に移動します。
次に、[参照]ボタンをクリックし、さきほどダウンロードした証明書をアップロード（登録）します。

またAirWatchへの登録用にAPI管理者ユーザアカウントの証明書詳細画面の[▶ダウンロード]リンクより証明書ファイル（.p12ファイル）をダウンロードしておきます。

※ダウンロード時に入力を要求されるファイルの保護パスワードはAirWatch登録時に必要です

以上でGléasの設定は終了です。

3. AirWatch の管理者設定

3.1. ACCを利用する場合の設定

※ACCを利用していない場合は本項目の設定は不要です

AirWatch 管理コンソールにログインし、[グループと設定] > [すべての設定] > [エンタープライズ統合] > [VMware Enterprise Systems Connector] > [高度な設定] と進みます。

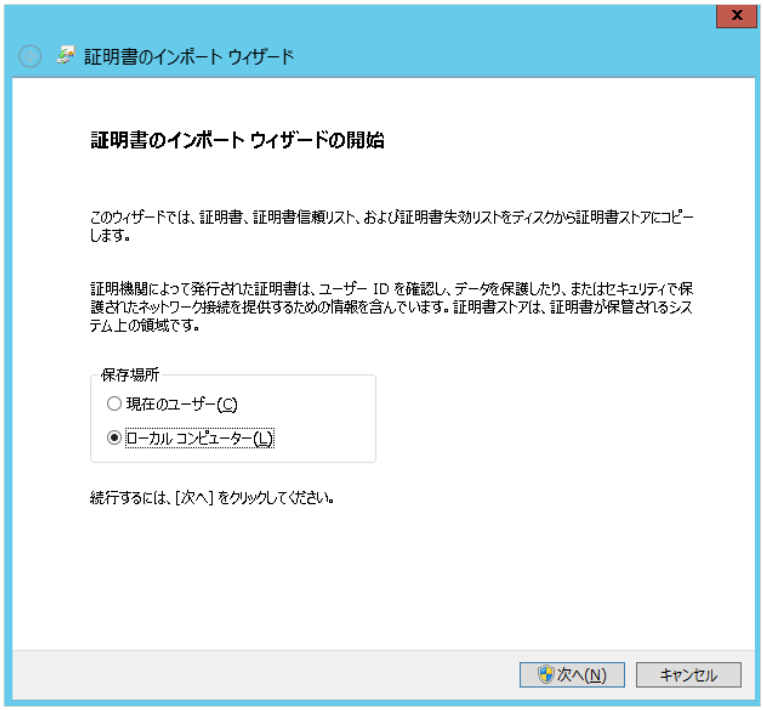
[エンタープライズサービス] > [認証局] > [JCCH Gleas]を有効にすることで、Gléas への通信を ACC 経由にすることができます。

また2項でダウンロードしたp12ファイルを、ACCを動作させているWindows Server にインポートします。

※以下の操作は管理者権限が必要です

Windows Server上にp12ファイルを配置し、そのファイルを右クリックし［PFX のインストール(I)]を選択します。

証明書のインポートウィザードが起動しますので、以下の通りにします。

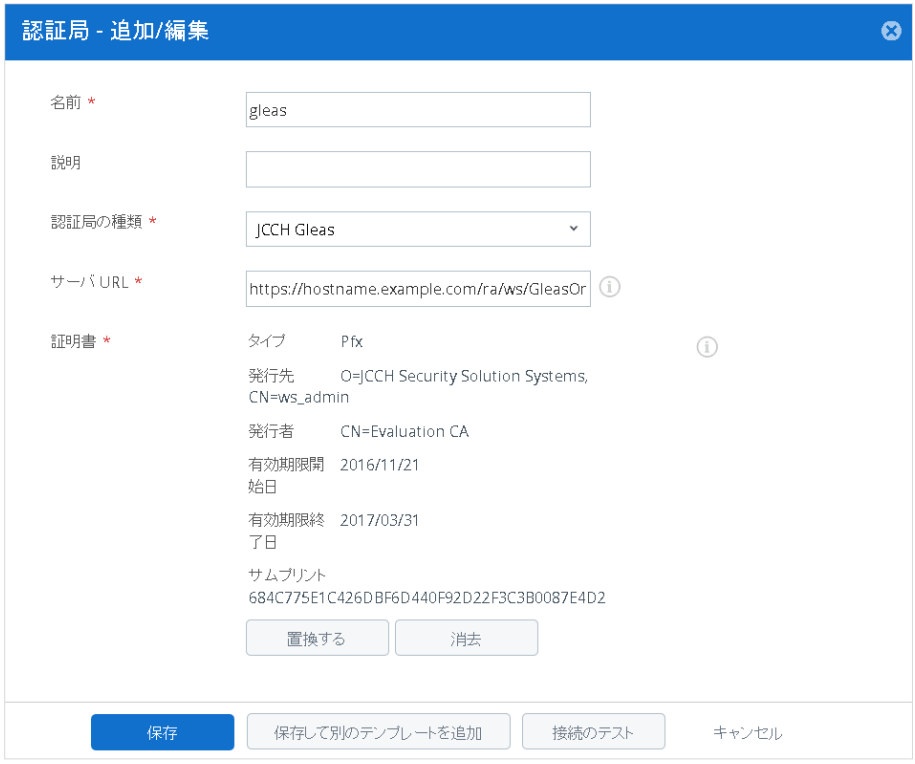


ページ	設定
証明書のインポートウィザードの開始	[ローカルコンピューター(L)]を選択し、[次へ(N)]をクリック
インポートする証明書ファイル	[次へ(N)]をクリック
パスワード	Gléas から PKCS#12 ファイルをダウンロードする際に設定したパスワードを入力して、[次へ(N)]をクリック
証明書ストア	[証明書の種類に基づいて、自動的に証明書ストアを選択する(U)]を選択し、[次へ(N)]をクリック
証明書インポートウィザードの終了	[完了]をクリック

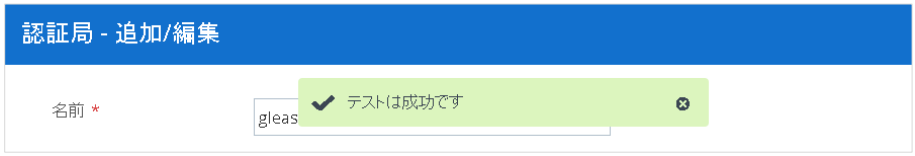
3.2. 認証局の設定

AirWatch 管理コンソールにログインし、[デバイス] > [証明書] > [認証局]と進みます。[追加]をクリックし、以下を設定します。

- 名前：任意の名称を入力
- 認証局の種類：[JCCH Gleas]を選択
- サーバ URL：https://*hostname.example.com*/ra/ws/GleasOrderService
  ※ホスト名部分（hostname.example.com）は、環境に応じて変更
  ※AirWatch から Gléas への https の疎通が必要
- 証明書：2 項でダウンロードした p12 ファイルをアップロード



[接続のテスト]をクリックすると、Gléas に対しテスト接続をおこない、その結果が表示されます。

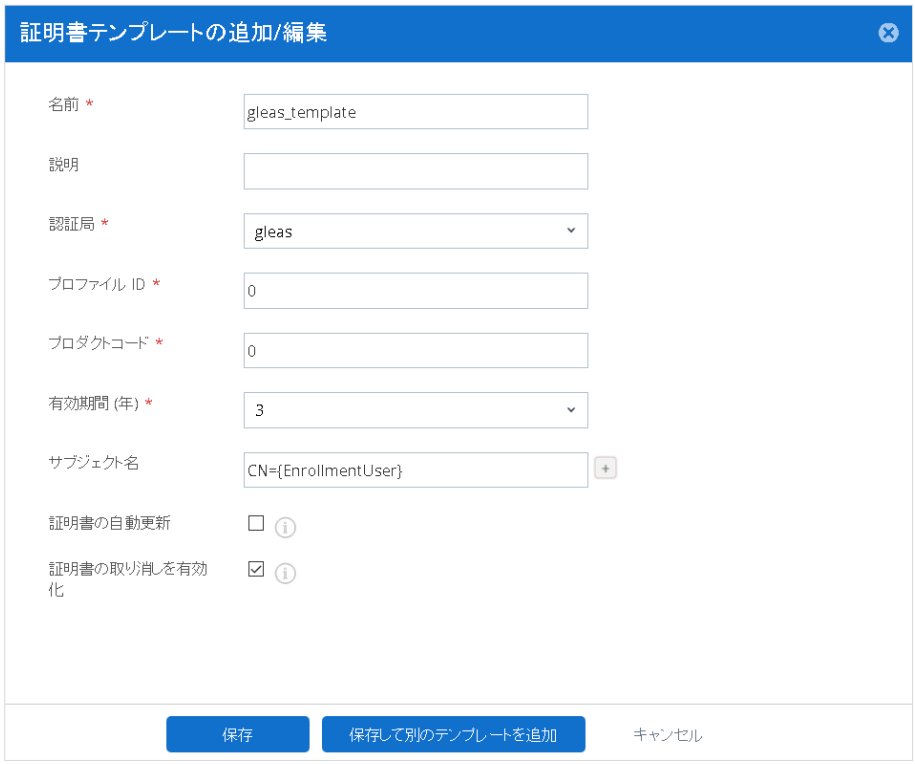


[保存して別のテンプレートを追加]をクリックし、以下の設定をおこないます。

- 名前：任意の名称を入力
- 認証局：認証局の追加で設定した名称を選択
- プロファイル ID：Gléas にあらかじめ作成してあるグループ ID を指定
  Gléas ではそのグループに設定されたテンプレートを用いて証明書を発行（カンマ区切りで複数のグループを指定可能）。
  デフォルトグループの場合は、実在しないグループ ID を設定
- プロダクトコード：0 を入力（未使用）
- 有効期間（年）：発行する証明書の有効期間を選択（1 年・2 年・3 年）
- サブジェクト名：証明書のサブジェクト名を指定（AirWatch にあらかじめ定義されている変数の利用が可能）
  ここに設定された値が Gléas のアカウントに紐づきます。Gléas に対応するア

カウントがない場合は、自動的にアカウントが作成されます。

- 証明書の自動更新：自動更新をする場合にチェック（弊社未検証）
  ※証明書を自動的に更新するには、関連するプロファイルの割り当てタイプが「自動」に設定されている必要があります
- 証明書の取り消しを有効化：デバイスの加入解除、特定プロファイルの削除、または AirWatch からデバイスを削除したとき等の証明書自動失効を有効にする場合にチェック



[保存]をクリックします。

3.3. プロファイル設定（iOS）

AirWatch 管理コンソールより、 [デバイス] > [プロファイルとリソース] > [プロファイル]と進みます。[追加] > [プロファイルを追加] > [Apple iOS]をクリックし、以下を設定します。
※プロファイルの各項目の設定については、設定項目が多岐にわたることや本書の主旨と異なるので割愛します

[資格情報] > [構成]をクリックし、以下を設定します。

- 資格情報ソース：定義済み認証局を選択

- 認証局：3.1 項で設定した認証局を選択
- 証明書テンプレート：3.1 項で設定した証明書テンプレートを選択

またプライベート認証局のルート証明書なども配布したい場合は、[+]をクリックすることで追加することが可能です。

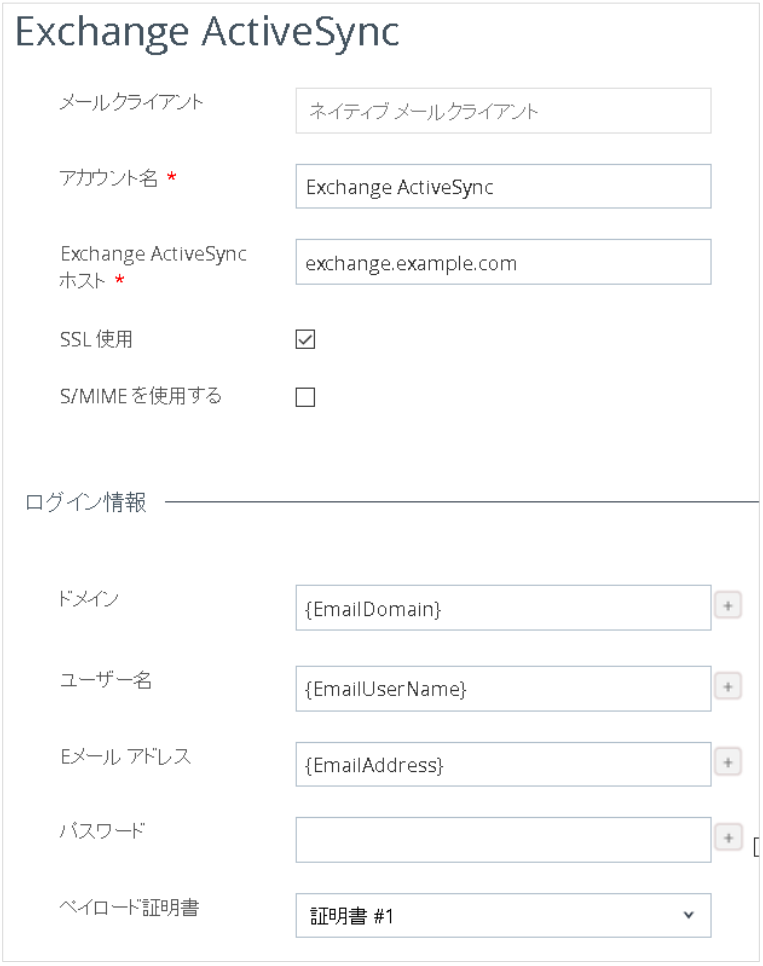
- 資格情報ソース：アップロードを選択
- 証明書：証明書ファイルをアップロード

証明書の発行および配布設定は以上です。
ここで設定したクライアント証明書は、以下のプロファイル項目で利用することが可能です。

- Wi-Fi （EAP-TLS 選択時）
- VPN
- Exchange ActiveSync

以下はクライアント証明書を Exchange ActiveSync で利用する設定例です。

[ペイロード証明書]に事前に設定した資格情報（証明書#1）を選択します。



3.4. プロファイル設定（Android）

AirWatch 管理コンソールより、 [デバイス] > [プロファイルとリソース] > [プロファイル]と進みます。[追加] > [プロファイルを追加] > [Android]をクリックし、以下を設定します。

※プロファイルの各項目の設定については、設定項目が多岐にわたることや本書の主旨と異なるので割愛します

[資格情報] > [構成]をクリックし、以下を設定します。

- 資格情報ソース：定義済み認証局を選択
- 認証局：3.1 項で設定した認証局を選択
- 証明書テンプレート：3.1 項で設定した証明書テンプレートを選択

またプライベート認証局のルート証明書なども配布したい場合は、[+]をクリックすることで追加することが可能です。

- 資格情報ソース：アップロードを選択
- 証明書：証明書ファイルをアップロード

証明書の発行および配布設定は以上です。
ここで設定したクライアント証明書は、以下のプロファイル項目で利用することが可能です。

- Wi-Fi （EAP-TLS 選択時）
- VPN
- Exchange ActiveSync

以下はクライアント証明書を VPN の認証で利用する設定例です。
[ID 証明書]に 3.1 項で設定した資格情報（証明書#1）を選択します。

3.5. プロファイルの設定（Windows）

AirWatch 管理コンソールより、 [デバイス] > [プロファイルとリソース] > [プロファイル]と進みます。[追加] > [プロファイルを追加] > [Windows] > [Windows デスクトップ] > [ユーザープロファイル]をクリックし、以下を設定します。

※プロファイルの各項目の設定については、設定項目が多岐にわたることや本書の主旨と異なるので割愛します

[資格情報] > [構成]をクリックし、以下を設定します。

- 資格情報ソース：定義済み認証局を選択
- 認証局：3.1 項で設定した認証局を選択
- 証明書テンプレート：3.1 項で設定した証明書テンプレートを選択
- キーの位置：ソフトウェアを選択（TPM やパスポートは弊社未検証）
- 証明書ストア：個人を選択

証明書の発行および配布設定は以上です。

4. AirWacth からのクライアント証明書配信

AirWatchの管理下になり3項で設定したプロファイルが適用された端末にはAirWacthより自動的に証明書および各種設定がプッシュ配信されます。

※Androidの場合は、証明書のインストールを促されますので画面の指示にしたがい操作をおこないます

証明書の格納状況は、AirWatch管理コンソールより[デバイス] > [リスト表示]から対象のデバイスを選択し、[さらに] > [証明書]で確認することが可能です。

なお、AirWatchからGléasへの各種アクセスの際に、Gléasのイベントログには以下エントリが出力されます。

- 証明書発行の成功メッセージ：
  OrderPkcs12(x) success (issuer_id x serial x)
- 証明書失効の成功メッセージ：
  Revoke(x) success (issuer_id x serial x)
- テスト接続の成功メッセージ：
  GetProfiles success

5. 問い合わせ

■Airwatch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

■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