

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

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

目次

1.	はじぬ	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	5の事前設定	7
3.	AirWa	atch 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.	AirWa	acth からのクライアント証明書配信	17
5.	問いる	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
- 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
- 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。

◎ 🍠 証明書のインポート ウィザード	x
証明書のインボート ウィザードの開始	
このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。	
証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保 護されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシス テム上の領域です。	
保存場所 ○ 現在のユーザー(<u>C</u>) ● ローカルコンピューター(L)	
続行するには、[次へ]をクリックしてください。	
愛次へ(N) キャンセル	

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:<u>あり</u>]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。

▶記書ファイル	
> 証明書要求: <u>あり</u> 作成日時 2016/11/21 19:14	
> 証明書: <u>あり</u> 作成日時 2016/11/21 19:15	
> 秘密鍵:あり 作成日時 2016/11/21 19:14	

その後、画面上部の[▶<u>管理者</u>]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。

🖢 管理者設定	
▶管理者情報	
>管理者	web-service管理者
> 証明書	参照 登録 Evaluation CA#146
	CN=ws_admin
	O=JCCH Security Solution Systems
>管理するトークン	Gemalto社製デバイス

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[▶<u>ダ</u>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。

券 証明書情報	 ■トーケノへのインポート	■ダウンロード

※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

証明書を保護するため	のバスワードを入力してください。,
バスワードの入力	
パスワード	[ダウンロード] キャンセル

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。

◎ 🭜 証明書のインポート ウィザード
証明書のインボート ウィザードの開始
このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。
証明機関によって発行された証明書は、ユーザー ID を確認し、デーダを保護したり、またはセキュリティで保 護されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシス テム上の領域です。
保存場所
○ 現在のユーサー(<u>し</u>) ● □ーカル コンピューター(<u>L)</u>
続行するには、[次へ]をクリックしてください。
愛次へ(N) キャンセル

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

認証局 - 追加/編集			8
名前 *	gleas		
説8月			
認証局の種類 *	JCCH Gleas	5 *	
サーバURL *	https://hos	tname.example.com/ra/ws/GleasOr (i)	
証明書 *	タイプ	P fx (i)	
	発行先 CN=ws_adn	O=JCCH Security Solution Systems, nin	
	発行者	CN=Evaluation CA	
	有効期限開 始日	2016/11/21	
	有効期限終 了日	2017/03/31	
	サムプリント 684C775E10	C426DBF6D440F92D22F3C3B0087E4D2	
	置換す	る 消去	
保存	保存して	別のテンブレートを追加 接続のテスト キャンセル	

[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。

認証局 - 追加/編集		
名前 *	gleas	0

[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

証明書テンプレートの	追加/編集	8
名前 *	gleas_template	
説明		
認証局 *	gleas ×	
プロファイル ID *	0	
ブロダクトコード *	0	
有効期間 (年) *	3 ~	
サブジェクト名	CN={EnrollmentUser}	
証明書の自動更新		
証明書の取り消しを有効 化		
	保存して別のテンプレートを追加 キャンセル	

[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

資格情報		
資格情報ソース	定義済み認証局	*
認証局 *	gleas	*
証明書テンプレート *	gleas_template	*

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

資格情報 #2						
資格情報ソース	<i>アッ</i> ブロード ・					
資格情報名 *	DC=JCCH-SSS, DC=COM, CN=JCCH-SSS demo C					
証明書 *	証明書アップロード 変更					
タイプ	Cert					
発行先	DC=JCCH-SSS, DC=COM, CN=JCCH-SSS demo CA					
発行者	DC=JCCH-SSS, DC=COM, CN=JCCH-SSS demo CA					
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					

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。

Exchange ActiveSync				
メールクライアント	ネイティブ メールクライアント			
アカウント名 *	Exchange ActiveSync]		
Exchange ActiveSync ホスト *	exchange.example.com]		
SSL 使用				
S/MIME を使用する				
ログイン情報 ―――				
ドメイン	{EmailDomain}	+		
ユーザー名	{EmailUserName}	+		
Eメール アドレス	{EmailAddress}	+		
バスワード		+		
ベイロード証明書	証明書 #1 、			

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

資格情報		
資格情報ソース	定義済み認証局	~
認証局 *	gleas	~
証明書テンプレート *	gleas_template	*

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

資格情報 #2	
資格情報ソース	アップロード・
資格情報名 *	DC=JCCH-SSS, DC=COM, CN=JCCH-SSS demo C
証明書 *	証明書アップロード変更
タイプ	Cert
発行先	DC=JCCH-SSS, DC=COM, CN=JCCH-SSS demo CA
発行者	DC=JCCH-SSS, DC=COM, CN=JCCH-SSS demo CA
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

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。

VPN	
接続情報 ————————————————————————————————————	
接続タイブ *	IPSec Xauth RSA 🗸
接続名 *	VPN Configuration
サーバ・	vpn.example.com
認証 ————————————————————————————————————	
ユーザー名	sample-user +
ID 証明書	証明書 #1

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

資格情報				
資格情報ソース	定義済み認証局	*		
認証局 *	gleas	*		
証明書テンプレート *	gleas_template	~		
キーの位置	ソフトウェア	*		
証明書ストア	個人	~		

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。

	デバイス > リスト表示 > testuser Androic google Nexus 9 7.1.1	I Android 7.1.1 所有形態: 企業 - 専用	1036		クエリ	◆ 送信 ▲ ロック ◆	1 / 2 > 最近のリスト ▼ その他のアクション
概	要 順守 プロファイル	, アプリ コンテンツ	/ ロケーション	ユーザー	証明書 🗸		
最終ス	キャン: 2017年1月23日 19:40					リストを検索	C 🖻
ID	名前	▲ 発行者	プロファイル	失効ま	での期間	状態	
1	CN=testuser,O=JCCH Securit	CN=Evaluation CA	android_test	67 日間	3	インストール済み	\odot \odot

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

イベントログ(全 149件中 1-50件目)					
フィルタ Webサービス管理者 ▼ Q タスク名で検索					
日時	種類	タスク名	メッセージ		
2017/12/	<u>Webサービス管理者</u>	GleasOrderService	OrderPkcs12(82) success. (issuer_id:4 serial:76)		
2017/12/	<u>Webサービス管理者</u>	GleasOrderService	Revoke(75) success. (issuer_id:4 serial:69)		
2017/12/	<u>Webサービス管理者</u>	GleasOrderService	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