

プライベート認証局Gléas ホワイトペーパー

MobileIron Cloudと連携したクライアント証明書配布

Ver.1.2 2019 年 6 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

MobileIron Cloud と連携したクライアント証明書配布

目次

1. はし	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. Gléa	as の設定	5
2.1	SCEP サーバの利用開始設定	5
3. Mob	bileIron の設定	6
3.1.	認証機関の追加	6
3.2.	ID 証明書の構成を作成	7
4. Mob	bileIron へのデバイス加入	8
5. 問い	い合わせ	9

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、MobileIron Cloudに加入したデバイスに、自動的にGléasのクライア ント証明書を配布する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、 ご参照いただけますようお願いいたします。

弊社では試験用証明書の提供も行っております。検証などで必要な場合は、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

本書における手順は、以下の環境で動作確認を行っています。

- MobileIron Cloud (Platinum バージョンR54)
 ※以下「MobileIron」と記載します
- 中継用サーバ MobileIron Cloud Connector (バージョン54.0.0.69)
 ※以下「Connector」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)
 ※以下「Gléas」と記載します
- ▶ クライアント: Dell XPS 12 (Windows 10 Pro)
 - : iPhone 6S+ (iOS 11.4)
 - : mac mini Late 2012 (macOS High Sierra)
 - : Nexus 9 (Android 7.1.1)

※それぞれ以下「Windows」「iOS」「macOS」「Android」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。

- MobileIronの基本設定
- Connectorの基本設定
- Gléasの基本設定
- クライアントの基本設定

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. クライアントがMobileIronへデバイス加入をすると、MobileIronはConnectorを経由し て連携設定をされたGléasへSCEPによる証明書発行要求をする。
- 2. GléasはMobileIron (Connector) からのSCEP要求に対し、クライアント証明書を発行し、証明書はMobileIronからクライアントへプッシュ配信される。

2. Gléasの設定

2.1. SCEP サーバの利用開始設定

SCEP 通信には専用の電子署名用証明書が必要になるので、事前に Gléas より SCEP サーバ に利用する証明書を発行し、ファイルダウンロードしておきます。 RA で上部の[認証局] > [デフォルト登録局]をクリックします。

認証局一覧
💿 test.jcch-sss.com の認証局
RA 登録局
▶ <u>Gleas Generic RA</u> Gleas デフォルト登録局
14 発行局
► Evaluation CA Evaluation CA

登録局詳細の「▶SCEP の設定」で、以下設定をおこないます。

- SCEP 用の証明書をアップロードする
- [静的チャレンジを利用する]にチェックを入れ、チャレンジ値を入力する ※チャレンジ値は MobileIron にも設定します
- [接続を許可するネットワーク]に、"ネットワークアドレス/ネットマスク"の形式で、 Connectorのネットワーク情報を入力します

プライベート認証局 Gléas ホワイトペーパー MobileIron Cloud と連携したクライアント証明書配布

※未入力の場合は、全てのアドレスからのアクセスを許可します

▶ SCEPの設定	
> SCEPサーバを利用中です。	
> SCEP用証明書 : 🌟 🗾 🖻 <u>削除</u>	
》有効期限 : 2019/03/29 01:44	
🗦 🔽 静的チャレンジを利用する	
>静的チャレンジ	
> 接続を許可するネットワーク	/32
	保存

設定が完了したら[保存]をクリックすることで SCEP サーバ機能が利用可能になります。

3. MobileIronの設定

3.1. 認証機関の追加

管理画面上部のメニューより[管理]をクリックし、左側メニューの[インフラ]にある[認証 機関]をクリックします。

画面中央にある[+追加]をクリックし、[外部認証機関を追加]にある[続行]をクリックします。[認証機関]のプルダウンメニューで、[汎用 SCEP サーバー]を選択し、[名前]に任意の名称を入力、[SCEP URL]に Gléas の SCEP 用 URL を入力します
※https://[Gléas UA ホスト名]/scep/[認証局番号]
例:デフォルトの認証局で発行する場合: https://ua.example.com/scep/1

2.1 項で設定したチャレンジ値を[チャレンジパスワード]に入力し、[完了]をクリックします。

! 外部認証機関を追	自加	×
名前	[必須]	
認証機関	汎用SCEPサーバー ◆	
	✓ MobileIron Cloud上のキャッシュID 毎回生成することなく、完全IDをMobileIron Clo に保管します	bud.L
SCEP URL	[必須]	
チャレンジパスワード		
← 戻る		完了

3.2. ID 証明書の構成を作成

管理画面上部のメニューより[構成]をクリックし、画面左上の[+追加]をクリックします。

	ダッシュボード ユーザー	デバイス アプリ コンテンツ	構成 ポリシー 管理	
構成を追加 取り消し				
フィルター 🗙	構成を検索			
OS ~ ~	プ ライバシー プライパシー設定を定義します。	 証明書 証明書を追加して、デバイスにサ ーパーとネットワークの信頼を確 立させます。 	D証明書 ID証明書 IFI書を追加して、デバイスにサ -バーとネットワーク上のリソー スへの信頼を確立させます。	8880 パスコード デバイスのパスコード要件を定義 します。
OSバージョン 〜	108 👘 🔳 mac	1005 🏟 🌐 mac	108 📻 🔳 mac	108 🔿 🔳 mac
 IOS 9+ IOS 8+ IOS 7+ Android 6+ 	 Windowsの制約 どの機能をWindowsデバイスで有効にするかを定義します。 	アプリ 制御 アプリの許可ルールと禁止ルール を作成します。	 ソフトウェア更新 ソフトウェア更新のルールを作成 します。 	iOSの制約 どの機能をiOSデバイスで有効にす るかを定義します。

[ID 証明書]をクリックし、[構成設定] > [証明書の配布]のプルダウンメニューから[動的生成]を選択し、[ソース]は 3.1 項で設定した Gléas を選択します。

[主体者]には MobileIron が用意するシステム属性の他に、固定値を入力もできます。

Gléas が SCEP 要求によって証明書を発行するためには、CN として指定されたアカウン トが Gléas 内に存在する必要があります。

[テスト証明書の発行なしで構成を作成]にチェックを入れ、[続行]をクリックします。 ※MobileIron からテスト証明書の発行をする場合は、事前に Gléas に test_user_id のアカウントを作成 しておく必要があります。

Scloud	ダッシュボード ユー	ザー デパイス	アプリコン	ンテンツ 🕴	貫成 ポリシー	管理
 構成を追加 取り消し ① 設定を作成 ② 配布する 	ID証明書の ユーザー、デバイ ネントなどのリン 行い、認証にID副 ん。	構成を作成 、スまたはグループべ・ ノースへのアクセスを E明書を使用できます。	ースの証明書は、\ 認証するために使 。iOSでは、証明書	Webサイト、メ 甲できます。証 FをWebサイト・	- ールサーバー、お。 E明書を手動でアッ へのアクセス認証に	よびVPNまた プロードする こ使用する場
	-1 มัม + 説明を追加					
	構成設定 証明書の配布 動的生成					•
	ソース CSR Signature Algorithm	Gleas		¢ \$		
	主体者 主体者別名タイプ	CN=\${userUIDLocalPart} X.500名の表示	,OU=staffs,DC=\${devic	eS		
		 デジタル署名として使 キー暗号化として使用 	用			
	✓ テスト証明書の発行なし	しで構成を作成 - ックすることで、私はこの	D構成がテスト証明書の	D発行なしで保存さ	されることを理解してい	ます。
	← 戻る				(続行 →

プライベート認証局 Gléas ホワイトペーパー MobileIron Cloud と連携したクライアント証明書配布

構成を当てはめるデバイスグループを選択し、[完了]をクリックします。

4. MobileIron へのデバイス加入

クライアントからMobileIronへデバイス加入すると、MDMプロファイルがインストールさ れます。続いてGléasが発行したクライアント証明書が自動でクライアントに配布されます。

🕻 Safari 📶 🗢	10:27	• •		
	インストール完了	完了		
	COOT MDM Profile CCH Security Solution Systems Co	., Ltd.(…		
署名者	*.mobileiron.com 検証済み ✔			
説明 The top-level MDM payload containing the MDM profile, the identities and the trust certificates necessary to MDM-manage this device.				
内容	モバイルデバイス管理 デバイスID証明書			
詳細		>		
SでのMDN	/ プロファイルインストール	完了時画面		
🖬 docomo 奈	12:01	@ Ö 🔳		
くプロファ	イルとデバイス管理 プロファイ ル	L		
	coot MDM Profile CCH Security Solution Systems Co	., Ltd.(…		

Sector Secturity Solution Systems Co., Ltd.(**)
#名者 *:mobileiron.com 検証済み ✓
助明 The top-level MDM payload containing the MDM profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage this device.
profile, the identities and the trust certificates necessary to MDM-manage the identities and the trust certificates necessary to MDM-manage the identities and the trust certificates necessary to MDM-manage the identities and the trust certificates necessary to MDM-manage the identities and the trust certificates necessary to MDM-manage the identities and the trust certificates necessary to MDM-manage the identities and the identities and the trust certificates necessary t

iOSでのMobileIronからクライアント証明書のインストール完了後画面

プライベート認証局 Gléas ホワイトペーパー MobileIron Cloud と連携したクライアント証明書配布

5. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Gléasや検証用の証明書に関するお問い合わせ

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