



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

Office 365 (Exchange Online)

Exchange ActiveSyncでのクライアント証明書認証

Ver.1.1

2018年6月

- ・ 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。

プライベート認証局 Gléas ホワイトペーパー
Office 365 Exchange OnlineにおけるExchange ActiveSyncでのクライアント証明書認証

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. 電子証明書発行時の留意事項	5
2. Azure Active Directory のテナントの設定	5
3. Gléas の管理者設定	6
4. クライアント操作	8
4.1. Gléas の UA より証明書取得	8
4.2. OTA エンロールメントを利用した証明書発行	10
4.3. Exchange Online へのアクセス	11
5. 証明書の失効	11
6. 問い合わせ	12

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」で発行したクライアント証明書を利用して、Microsoft Corporationのクラウドサービス Office 365（Exchange Online）でサポートされている Exchange ActiveSync（EAS）においてクライアント証明書認証をおこなう環境の設定例を記載します。

本書は以下URLの内容を参考にしています。

<https://azure.microsoft.com/ja-jp/documentation/articles/active-directory-certificate-based-authentication-ios/>

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

本書における手順は、以下の環境で動作確認を行っています。

- SaaSサービス：Office 365 Enterprise E3（Exchange Online） / Azure Active Directory（Azure AD）※以後、「Exchange Online」と記載します
- JS3 プライベート認証局Gléas（バージョン1.13.103）
※以後、「Gléas」と記載します
- クライアント：iPhone6（iOS 10.0.1）
※以後、「iPhone」と記載します
※iOSの標準メールアプリを利用します

以下については、本書では説明を割愛します。

- Office 365 / Exchange Onlineの基本設定
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定
- iPhoneでのネットワーク設定等の基本設定

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. 電子証明書発行時の留意事項

Gléasで電子証明書を発行する際に以下の属性を含める必要があります。

- ✓ サブジェクトの別名：証明書利用ユーザのActive Directoryにおけるユーザプリンシパル名
- ✓ CRL配布ポイント（Exchange Onlineからアクセス可能なところに失効リスト（CRL）を配置する）
- 本書の手順をおこなった後にもパスワードによるExchange Onlineへのログインは可能です。（本書の内容はユーザが自身のOffice365のログインパスワードを知らない場合に有効）

2. Azure Active Directoryのテナントの設定

事前に Gléas よりルート証明書ファイルをダウンロードしておきます。

デフォルトのルート証明書ダウンロード URL は以下の通りです。

<http://example.com/crl/ia1.pem>

Powershell を管理者権限で起動し、Azure AD モジュールをインストールします。

```
Install-Module -Name AzureAD
```

Azure AD に接続します。

以下のコマンドを利用し、管理者 ID でログインします。

```
Connect-AzureAD
```



以下コマンドで Azure AD テナントに信頼するルート認証局を設定します。

```
$cert=Get-Content -Encoding byte "[ルート証明書ファイルのパス]"  
$new_ca=New-Object -TypeName `   
    Microsoft.Open.AzureAD.Model.CertificateAuthorityInformation  
$new_ca.AuthorityType=0  
$new_ca.crlDistributionPoint="[CRL 配布ポイントの URL]"
```


[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UAを利用する]をチェックします。



構成プロファイル生成に必要な情報を入力する画面が展開されるので、以下設定を行います。

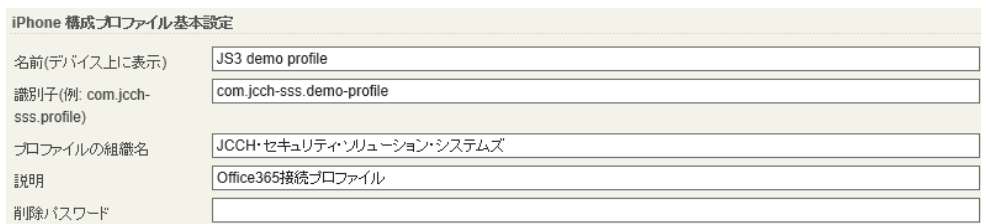
画面レイアウト

- [iPhone用レイアウトを利用する]をチェック
- [ログインパスワードで証明書を保護]をチェック



iPhone構成プロファイル基本設定

- [名前]、[識別子]に任意の文字を入力 (必須項目)
- [削除パスワード]を設定すると、iPhoneユーザが設定プロファイルを削除する際に管理者が定めたパスワードが必要となります (iPhoneユーザの誤操作等による構成プロファイルの削除を防止できます)



Microsoft Exchange(Active Sync)の設定

- [Exchange ホスト名] : outlook.office365.com
- [パスワードの入力方法] : パスワードを保存しない
- [iOS4 互換のフォーマットを使用しない] : チェック



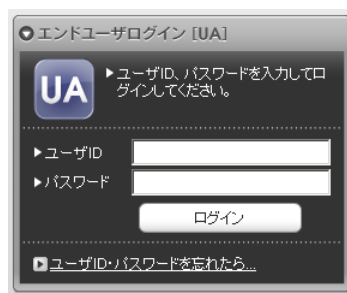
各項目の入力が終わったら、[保存]をクリックします。

4. クライアント操作

4.1. GléasのUAより証明書取得

iPhoneのブラウザ（Safari）でGléasのUAサイトにアクセスします。

ログイン画面が表示されるので、ユーザIDとパスワードを入力しログインします。



ログインすると、そのユーザ専用ページが表示されるので、[ダウンロード]をタップし、構成プロファイルのダウンロードを開始します。

※インポートロックを有効にしている場合は、この時点からカウントが開始されます



自動的にプロファイル画面に遷移するので、[インストール]をタップします。

なお、[詳細]をタップすると、インストールされる証明書情報を見ることが可能ですので、必要に応じ確認してください。

プライベート認証局 Gléas ホワイトペーパー
Office 365 Exchange OnlineにおけるExchange ActiveSyncでのクライアント証明書認証



以下のようなルート証明書のインストール確認画面が現れますので、内容を確認し[インストール]をクリックしてください。

※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります。



Exchange アカウントに対するパスワード入力を求められますが、何も入力せずに[次へ]をタップします。



インストール完了画面になりますので、[完了]をタップします。



元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトします。

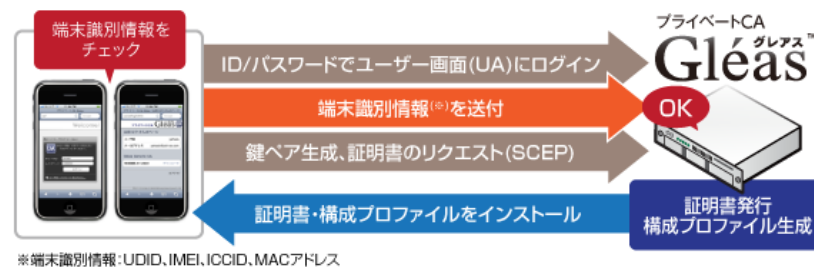
以上で、iPhoneでの構成プロファイルのインストールは終了です。

なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可となります。



4.2. OTAエンロールメントを利用した証明書発行

Gléasでは、iOSデバイスに対するOver The Air (OTA) エンロールメントを利用した証明書の発行・構成プロファイルの配布も可能です。OTAを利用すると事前に指定した端末識別番号を持つ端末だけに証明書の発行を限定することも可能になります。



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。

4.3. Exchange Onlineへのアクセス

構成プロファイルのインポート完了後にメールアプリを開くと、Exchange Online にアクセス可能な状態になっています。

5. 証明書の失効

Azure AD では指定した URL より取得した失効リスト (CRL) をキャッシュします。そのため Gléas で失効処理をした証明書が実際に Azure AD に反映されるのは、キャッシュされた CRL が更新されたあととなります。

端末の紛失などで早急に失効反映が必要な場合は、以下の StsRefreshTokenValidFrom 属性の変更 (認証トークンの更新) をおこなうことで対応可能です。

1) Powershell を開き、以下の操作をおこないます。

```
connect-msolservice
```

※管理者アカウントでログイン

StsRefreshTokenValidFrom を変更します。

```
Set-MsolUser -UserPrincipalName username@domain.com -StsRefreshTokensValidFrom ("09/30/2016")
```

※指定する StsRefreshTokenValidFrom 属性の値は、現在より後の日付にする必要があります

StsRefreshTokenValidFrom は以下で確認することができます。

```
$user = Get-MsolUser -UserPrincipalName username@domain.com  
$user.StsRefreshTokensValidFrom
```

2) Gléas で対象の証明書を失効し、CRL の手動更新 (更新予約) をおこないます (CRL の自動更新機能が有効になっていない場合)。

6. 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