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CA Gléas ホワイトペーパー

Pulse Secureでのクライアント証明書認証設定

（Office 365 先進認証）

Ver. 1.0
2017 年 4 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CA Gléas」で発行したクライアント証明書を利用して、Pulse Secure社のSSL-VPN装置「Connect Secure」経由でMicrosoft Corporationのクラウドサービス「Office 365」の認証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

本書における手順は、以下の環境で動作確認を行っています。

- SAML IDP：Pulse Connect Secure 8.2R5 (build 49363)
  ※以後、「Pulse Secure」と記載します
  ※本書のスクリーンショットはClassic UIをベースとしたものとなります
- SaaSサービス：Office 365 Enterprise E3
  ※以後、「Office 365」と記載します
  ※Office 365をサービスプロバイダとして利用するには、ビジネスプランのサブスクリプションが必要になります
- ドメインコントローラ： Microsoft Windows Server 2012 R2 Standard
  ※以後、「AD」と記載します
  ※以下のツールをインストールしています
  - ✧ Microsoft Online Services サインイン アシスタント
  - ✧ Windows PowerShell用 Microsoft Azure Active Directory モジュール
  - ✧ Azure AD Connect （IDプロビジョニング用）
- JS3 プライベートCA Gléas （バージョン1.14.6）
  ※以後、「Gléas」と記載します
- クライアント：Windows 10 Pro / Internet Explorer 11 / Excel 2016
  ※以後、「PC」と記載します
- クライアント：iPhone 5c（iOS 10.3.1）/

Outlook 2.20.0 / Microsoft Authenticator 5.2.5

※以後、「iPhone」と記載します

※iOSでは、Microsoft Authenticatorが必要になるので事前にインストールしておきます

以下については、本書では説明を割愛します。

- Pulse Secureの基本的な設定

  ※本書の手順は、以下URLで公開しているホワイトペーパー「Pulse Connect Secureクライアント証明書による認証設定」の手順がおこなわれていることを前提に記述しています

  https://www.gleas.jp/news/whitepaper/pulse-connect-secure
- Gléasでのアカウント登録や各種証明書発行

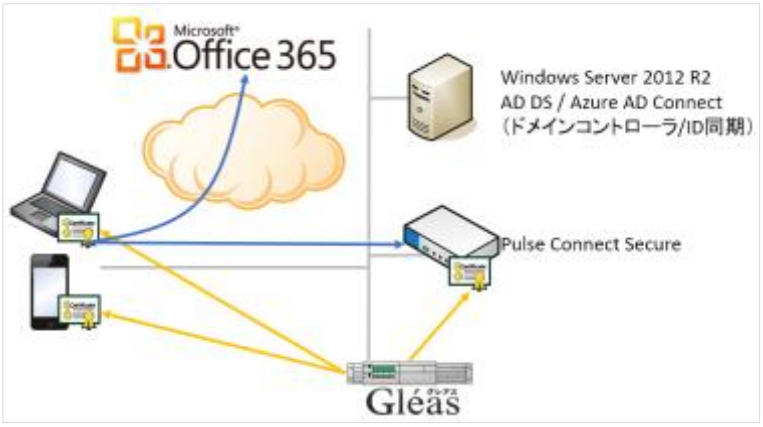
  本書記載の内容では、以下の証明書を発行する前提です

  - SSLサーバ証明書　（兼 アサーション署名用証明書）
  - クライアント証明書
- Windows ServerやWindowsドメインのセットアップ
- Azure AD Connectを用いたOffice 365のユーザプロビジョニング
- PC、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. 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. Gléasでは、Pulse Secure用にSSLサーバ証明書を、PC・iPadの利用者にクライアント証明書を発行する
2. PC：クライアントはブラウザやOfficeアプリケーション（本書ではExcel 2016を利用）でOffice 365にアクセスすると、認証先としてPulse Secureにリダ

イレクトされる
3. iOS：Officeモバイルアプリ（本書ではOutlookを利用）でOffice 365にアクセスすると、認証先としてPulse Secureにリダイレクトされる
4. Pulse Secureではクライアント証明書とパスワードによる二要素認証をおこなう。この時に、ログインIDは証明書のサブジェクトのCN（Gléasでのアカウント名）より抽出する。認証完了後にPulse SecureはADより情報を取得し、Office 365に送信しログインする。

1.4. 電子証明書の発行時における留意事項

本書の設定内容において、Gléasで電子証明書の発行操作をする際には以下の点に留意する必要があります。

- サーバ証明書
  サブジェクトの代替名（Subject Alt Name）に、Pulse Secureのサーバホスト名と、本書でSAML用の代替ホスト名（Alternate Host FQDN for SAML）の両方のホスト名が記載されている必要があります。

2. Pulse Secureの設定

Pulse Secure の管理 Web 画面にログインし、以下の設定をおこないます。

2.1. 事前設定内容の確認

PulseSecure 本体の Office 365 連携設定にはあらかじめ以下の設定が必須となります。

1. ホスト名設定
System > Network 画面内の Network Identity 項目で、Hostname が入力されていること。

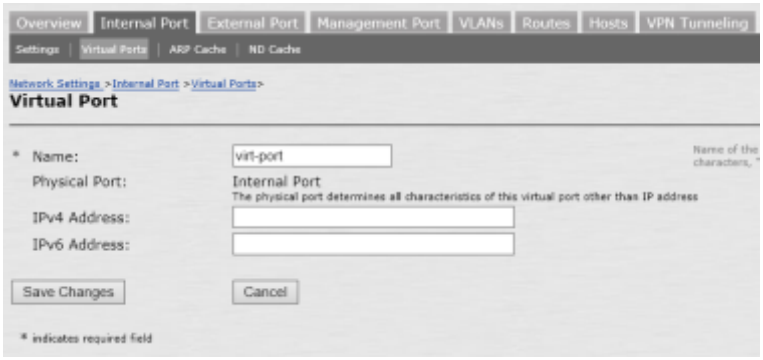
2. DNS サーバ設定
同画面上の「DNS name resolution」項目にて DNS サーバおよび DNS ドメインが入力されていること。

3. 時刻同期設定
System > Status > Overview 画面内の「System Date & Time」項目の「Edit」ボタ

ンをクリックし、正しい「Time Zone」および正しい「System Time」にて動作していること。

2.2. バーチャルポート設定

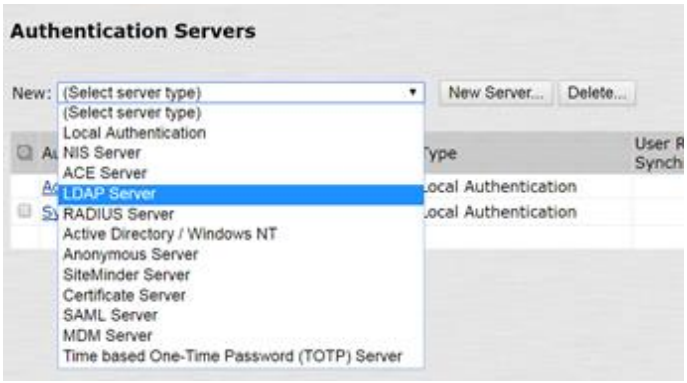
Office 365 連携時に使用される代替 URL の名前解決先アドレスとなるバーチャルポートを設定します。
Network > Internal Port > Virtual Port をクリックし、物理 NIC の IP アドレスとは異なる IP アドレスをアサインします。



設定後、[Save Changes]をクリックして保存します。

2.3. 認証サーバの登録

二要素認証をおこなうため、Office 365 連携時に使用されるドメインコントローラを認証サーバとして設定します。
Authentication > Auth. Server をクリックし、プルダウンメニューから“LDAP Server”を選択して［New Server...］をクリックします。



以下の項目を設定します。

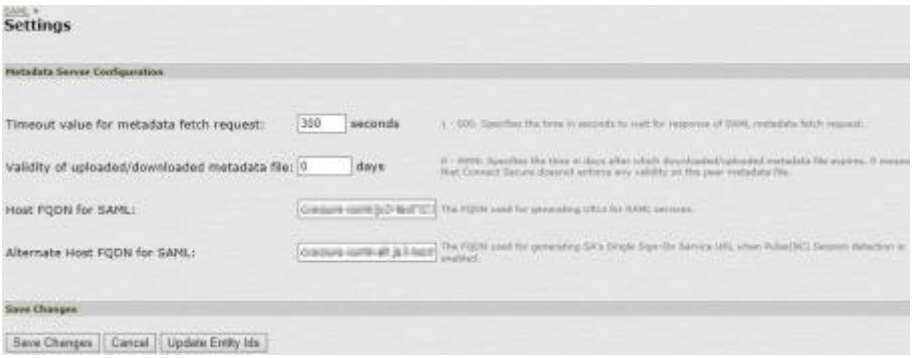
- Name：　　任意の名称（識別名）を入力
- LDAP Server：　ドメインコントローラのホスト名か IP アドレスを入力
- LDAP Port：　　ドメインコントローラの LDAP(S)ポートを入力
- LDAP Server Type：「Active Directory」を選択
- Authentication Required 項目
  「Authentication Required to Search LDAP」にチェック
  Admin DN に、適切な DN とパスワードを入力
  例）　cn=Administrator,cn=Users,dc=example,dc=local
- Find User entries 項目
  Base DN に、ユーザ情報の検索ベースになる DN を入力
  例）　cn=Users,dc=example,dc=local
  Filter は、ログイン ID を持つ AD の属性を指定　（LDAP Server Type に「Active Directory」を選択すると、「samaccountname=<USER>」が自動的に入ります）
- その他の設定項目はデフォルトのまま（利用環境に応じて設定）

設定後、[Save Changes]をクリックして保存します。

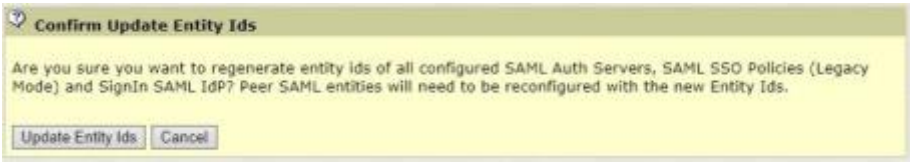
2.4. SAML 基本設定

System > Configuration > SAMLと進みます。[Settings]をクリックし以下を設定します。

- Host FQDN for SAML：　Pulse Secure のホスト名を入力
- Alternate Host FQDN for SAML：　代替ホスト名を入力
  代替ホスト名は、2.2 項でバーチャルポートに割り当てた IP アドレスに名前解決されるようにします



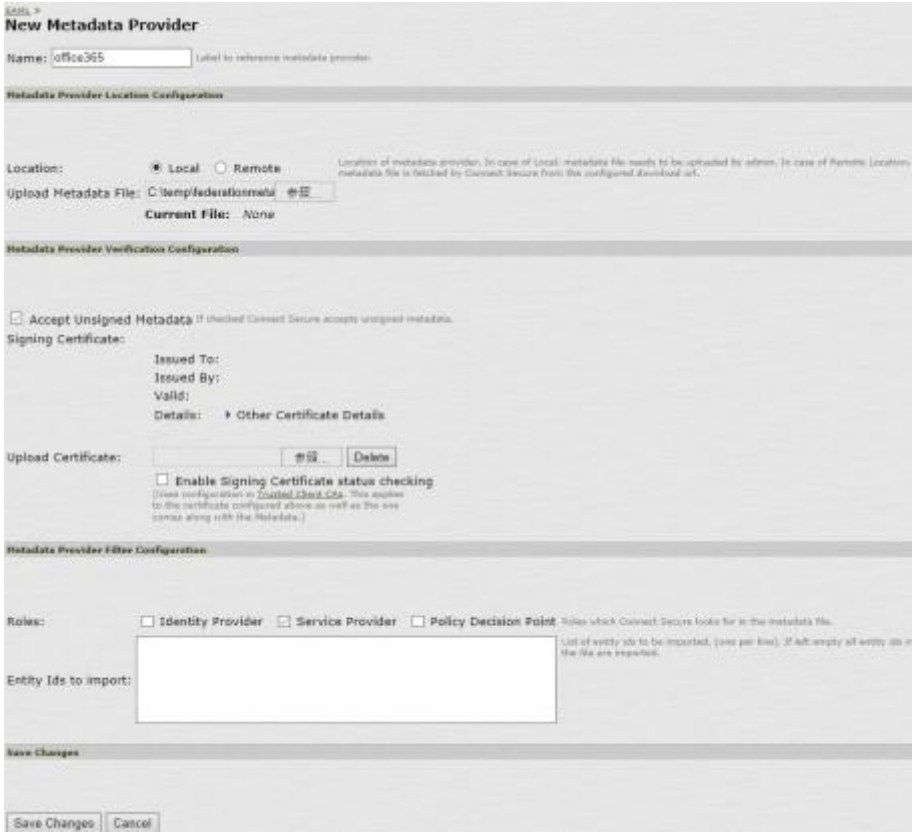
設定終了後、[Save Changes]をクリックし保存します。
その後に、[Update Entity Ids]をクリックし、以下の確認画面にて同じボタンをクリックします。



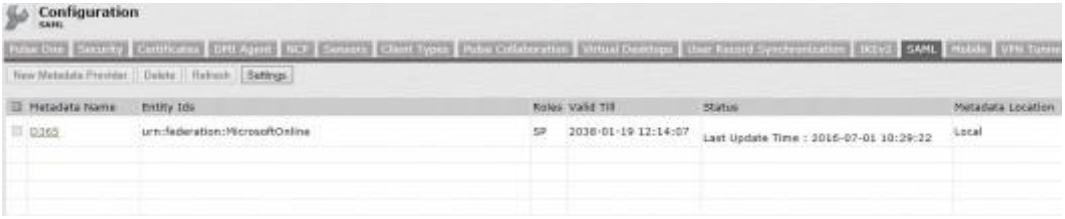
2.5. Office 365 メタデータのインポート

System > Configuration > SAMLと進みます。
[New Metadata Provider]をクリックし以下を設定します。

- Name：　任意の名称を入力
- Upload Metadata：以下 URL より Office 365 の設定情報（メタデータ）をローカル PC にダウンロードし、Pulse Secure へアップロード
  ※ダウンロード URL（2017 年 3 月現在）
  https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml
- Accept Unsigned Metadata：チェック
- Role：　「Service Provider」にチェック



設定終了後、[Save Changes]をクリックし保存します。
正常にインポートされると以下のように表示されます。



2.6. IDP 動作モードの設定

Authentication > Signing In > Sign-in SAML > Identity Provider と進み、以下の設定をおこないます。

- Protocol Binding to use for SAML Response：
  「Post」及び「Artifact」の両方にチェック
- Signing Certificate：
  導入済みの SSL サーバ証明書をプルダウンメニューから選択
- Other Configuration：
  「Reuse Existing NC（Pulse）Session」および「Accept unsigned

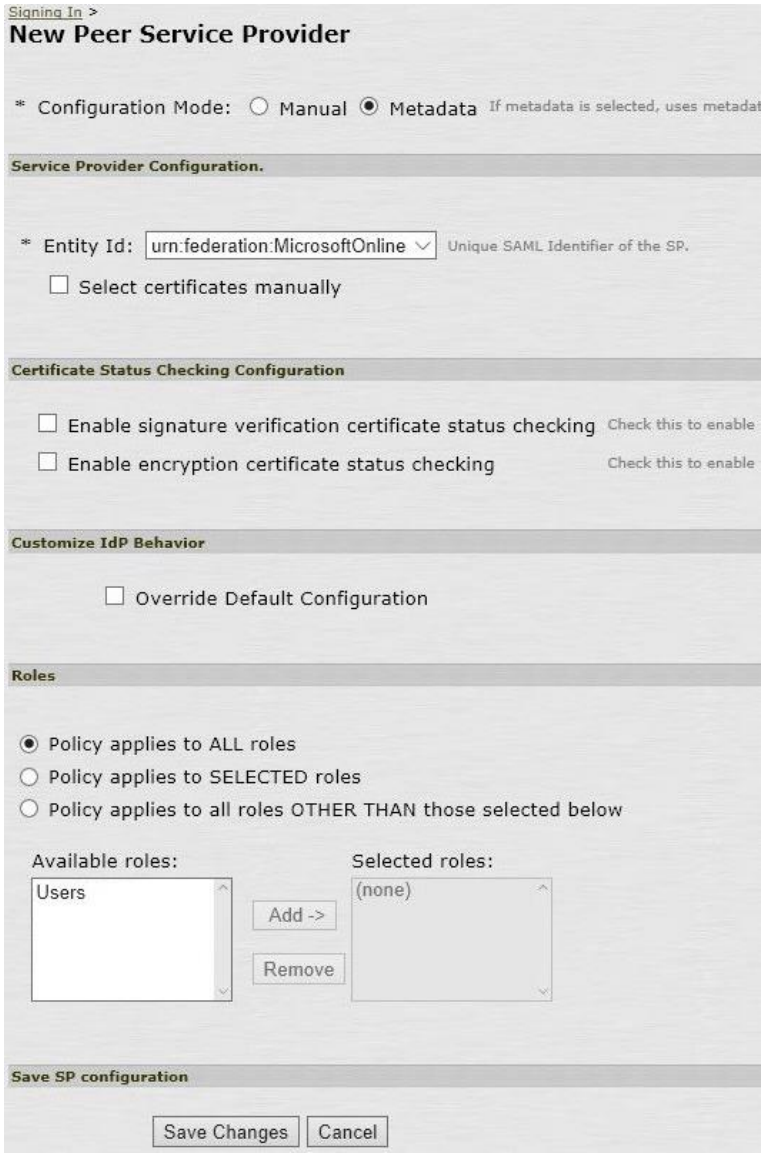
AuthnRequest」の両方にチェック

- SignIn Policy：「*/」をプルダウンメニューから選択
  ※異なるログイン URL を設定している場合などは適宜変更
- Subject Name Format：「Persistent」をプルダウンメニューから選択
- Subject Name：「<OBJECTGUID>」という Pulse Secure 内部の変数名を入力（「<」「>」も含めて）

- Directory server based Configuration
  Directory Server：2.3 項で設定したドメインコントローラを選択
  Username for Lookup：デフォルト値の「<USERNAME>」を設定
  Attribute Name 及び Friendly Name：それぞれ「ObjectGUID」と入力し[Add]をクリック

ここまで設定して、[Save Changes]をクリックします。
その後、同画面最下部の Configuration の[Add SP]をクリックし、以下の設定をおこないます。

- Entity ID:　「urn:federation:MicrosoftOnline」を選択
- Role:　「Policy applies to ALL roles」か、個別に割り当てるロールを選択

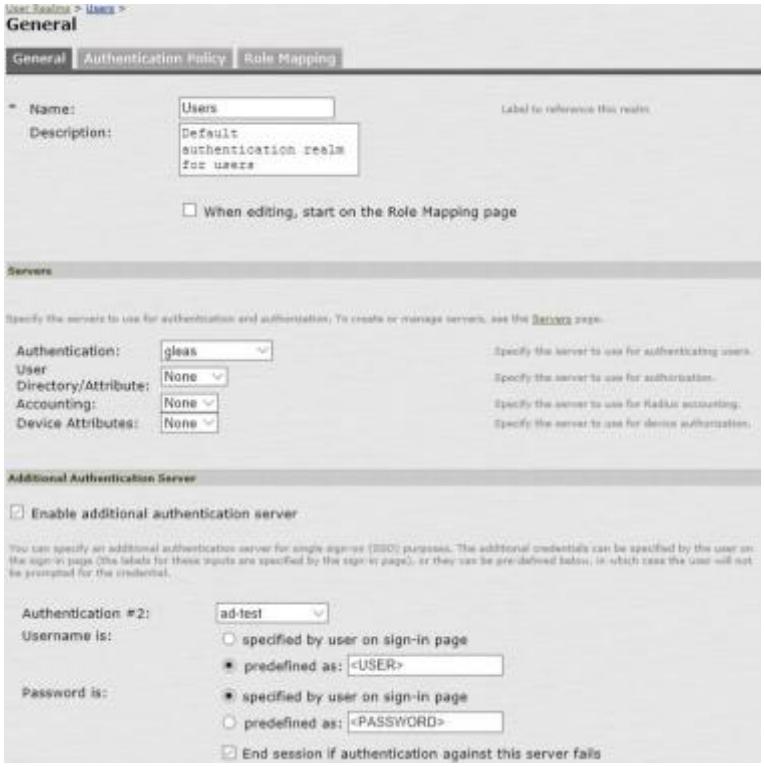


2.7. レルムの設定

User Realms > [2.6項のSignIn Policyで設定されたログインURLに紐づくレルム]と進み、以下の設定をおこないます

※Serversの各項目　（クライアント証明書認証の設定）はすでにおこなわれているものとします

- 「Enable additional authentication server」にチェック
- Authentication Server #2 は、2.3項で設定した認証サーバ（AD）を選択
- Username is は、「predefined as:」を選択し、そのあとに「<USERS>」を入力
- Password is は、「specified by user on sign-in page」を選択



設定終了後、[Save Changes]をクリックし保存します。

以上で Connect Secure の設定は完了です。

3. Office 365（Azure AD）の設定

Office 365 の認証をおこなう Azure Active Directory の設定変更のため、「Windows PowerShell 用 Windows Azure Active Directory モジュール」を起動します。

以下のコマンド入力し、Office 365 の管理者権限を持つアカウントでログインします。

```
Connect-MsolService
```

ログイン後に以下を入力し、対象ドメインをフェデレーションドメインに変更します。

```
#入力例
$dom = <Federated Domain_Name>
$fedBrandName = "PulseSecure"
$url = "https://<Alternate Host FQDN for SAML>/dana-na/auth/saml-sso.cgi"
$logouturl = "https://<Alternate Host FQDN for SAML>/dana-na/auth/logout.cgi"
$issuer = "https://<Host FQDN>/dana-na/auth/saml-endpoint.cgi"
$ecpUrl = "https://<Host FQDN>/dana-ws/saml20.ws"
$certData = "<2.6 項で設定した Signing Certificate（テキスト形式）>"
Set-MsolDomainAuthentication -DomainName $dom `
-FederationBrandName $fedBrandName -Authentication Federated `
-PassiveLogOnUri $url -SigningCertificate $certData -IssuerUri $issuer `
-ActiveLogOnUri $ecpUrl -LogOffUri $logouturl  `
-PreferredAuthenticationProtocol SAMLP
```

以下のコマンドを実行することで設定内容の確認が可能です。

```
Get-MsolDomainFederationSettings -DomainName <DomainName>
```

※Exchange Online で先進認証を有効にするためには、以下の操作が必要です。
https://support.office.com/en-us/article/Enable-Exchange-Online-for-modern-authentication-58018196-f918-49cd-8238-56f57f38d662

4. Gléasの管理者設定（PC）

GléasのUA（申込局）より発行済み証明書をPCにインポートできるよう設定します。
※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RA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA（申込局）をクリックします。

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用す

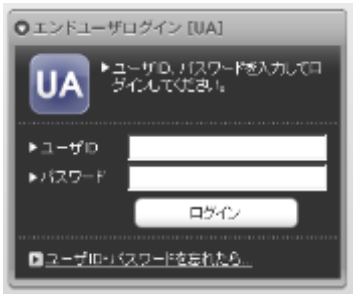
る]にチェック

設定終了後、[保存]をクリックし設定を保存します。
各項目の入力が終わったら、 [保存]をクリックします。

5. クライアント操作（PC）

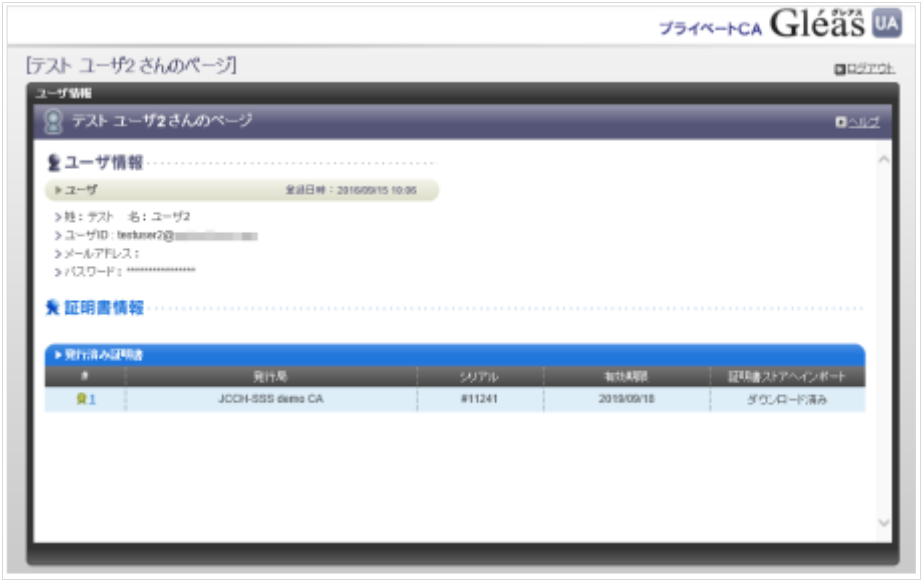
5.1. クライアント証明書のインポート

Internet Explorer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、Gléasでのユーザ 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、ユーザ専用ページが表示されます。
[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。
※初回ログインの際は、ActiveXコントロールのインストールを求められるので、画面の指示に従いインストールを完了してください。

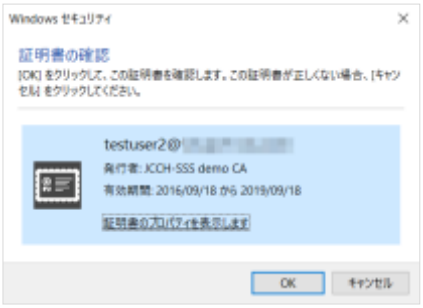
「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません。



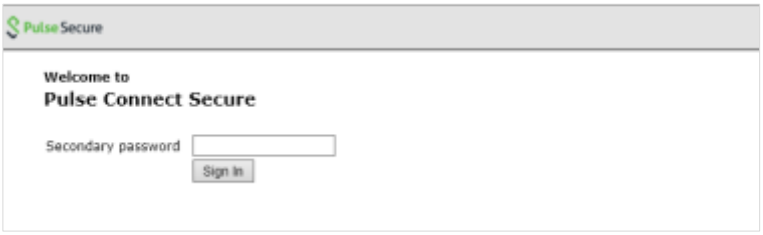
5.2. Office 365 へのアクセス（ブラウザ）

Internet ExplorerでOffice 365へアクセスし、ドメイン名を含むユーザIDを入力します。その後、Pulse Secureに転送されクライアント証明書を求められます。

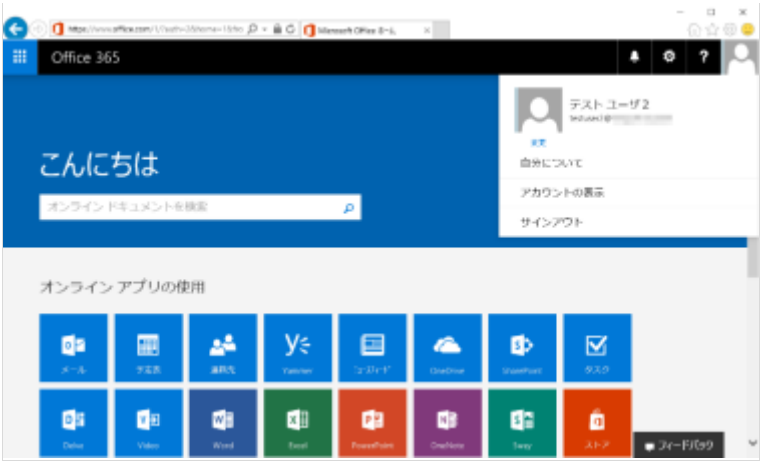
※Pulse SecureのログインURLがローカルイントラネットゾーンに設定されている場合など、IEの設定によっては以下の「Windows セキュリティ」画面は表示されない場合もあります



証明書認証が完了すると、Pulse Secureのログイン画面が表示されるのでWindowsドメインのパスワードを入力します。



パスワード認証成功後に、Office365のポータル画面が表示されます。

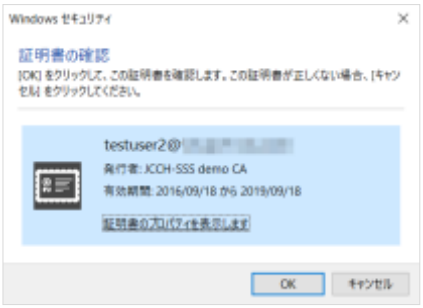


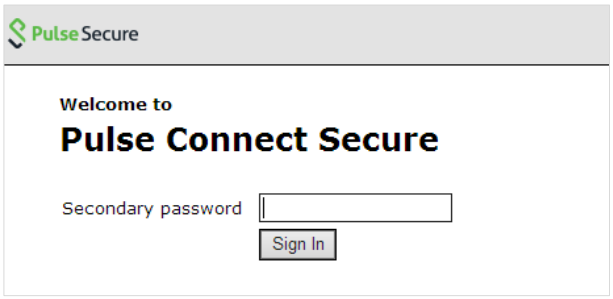
5.3. Office 365 へのアクセス（Office アプリ）

Excel 2016をひらきタイトルバーにある[サインイン]をクリックします。

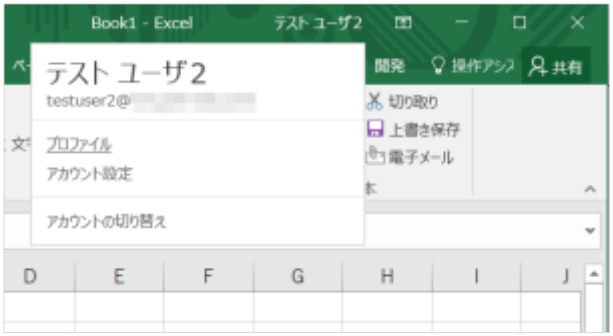
Office 365ログイン用のユーザIDを入力します。

その後、ブラウザでのアクセスと同様にクライアント証明書とパスワードによる認証をおこないます。





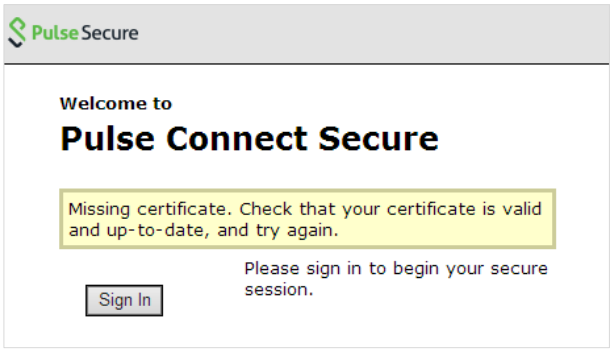
認証に成功するとログインユーザが表示されるようになります。



同時にOneDriveやSharePoint Onlineにもログインするので、オンラインストレージを透過的に利用することが可能です。

また一度ログインした情報はキャッシュされるので、他のOfficeアプリケーションを開いてもログインした状態になります。

証明書を提示しない場合は以下のメッセージが表示されます。



失効された証明書でアクセスすると、ログインに失敗します。

6. Gléas の管理者設定（iPhone）

Gléas で、発行済みのクライアント証明書を iPhone にインポートするための設定を記載します。

※　下記設定は、Gléas の納品時に弊社で設定を既にしている場合があります

GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA（申込局）をクリックします。
[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック
  この設定を行うと、GléasのUAからインポートから指定した時間（分）を経過した後は、構成プロファイルのダウンロードが不可能になります（インポートロック機能）。これにより複数台のデバイスへの構成プロファイルのインストールを制限することができます。

設定終了後、[保存]をクリックし設定を保存します。

[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。

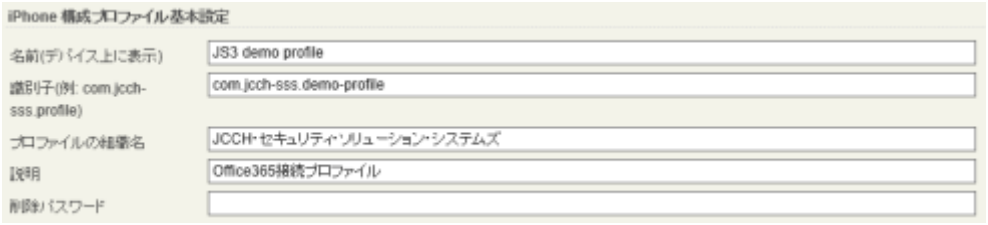
構成プロファイル生成に必要となる情報を入力する画面が展開されるので、以下設定を行います。

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）



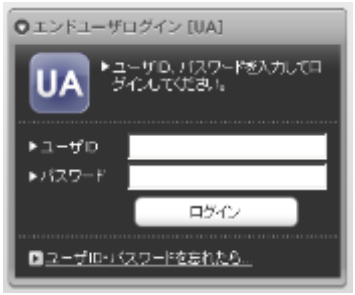
各項目の入力が終わったら、 [保存]をクリックします。

以上でGléasの設定は終了です。

7. クライアント操作（iPhone）

7.1. クライアント証明書のインポート

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。

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]をクリックして続行してください。
※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。

インストール完了画面になりますので、[完了]をタップしてください。

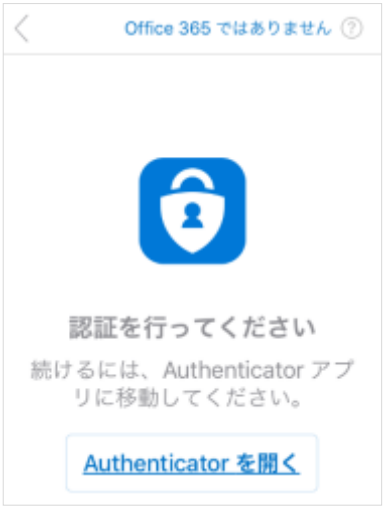
元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトします。

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。

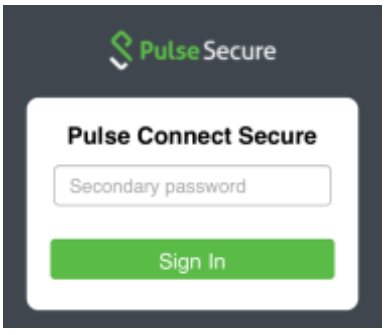
7.2. Office 365へのアクセス

Outlook アプリを起動してアカウントの追加をおこないます。

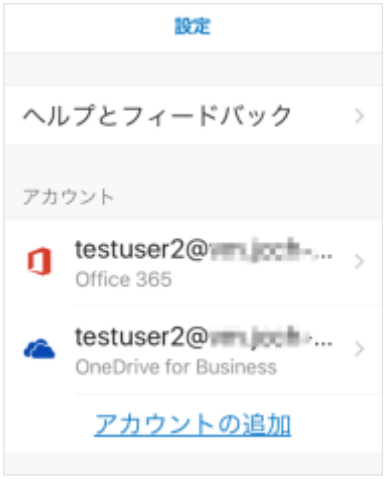
画面の指示にしたがい、Microsoft Authenticator を開きます。



その後、クライアント証明書認証がバックグラウンドでおこなわれ、成功するとパスワード認証の画面が表示されます。



AD 認証が完了すると、メール閲覧が可能となります。
この状態で Outlook アプリの[設定]をタップすると、Office 365 や OneDrive にログインしていることがわかります。



有効な証明書を提示できない場合は、以下のようになります。

また Microsoft Authenticator を見ると、Azure AD にログインできたことが記録されています。
（Microsoft Authenticator を認証に使う他 Office モバイルアプリもこの認証結果情報を参照します）

8. 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。

■Pulse Connect Secureに関するお問い合わせ先
マクニカネットワークス株式会社
Pulse Secure 製品担当
TEL:　045-476-1980

Mail：　pulsesecure-sales@cs.macnica.net

■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
営業本部
Tel:　050-3821-2195
Mail:　sales@jcch-sss.com