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

IIJ ID サービスでのクライアント証明書認証

（Office 365 連携）

Ver.1.0
2021 年 10 月

目次

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベート認証局 Gléas」で発行したクライアント証明書を使って、株式会社インターネットイニシアティブが運営するクラウド型認証管理サービス「IIJ IDサービス」でMicrosoft CorporationのOffice 365の認証を行う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： IIJ IDサービス
  ※以後「IIJ ID」と記載します
- SaaS (SAML SP)： Office 365 Enterprise E3
  ※以後「Office 365」と記載します
- 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
  - Azure AD Connect バージョン 1.4.18.0 (Office 365/Azure ADへのID同期)
  - IIJ ID Service Directory Sync バージョン 3.0.1 (IIJ IDへのID同期)
- JS3 プライベート認証局 Gléas（バージョン 2.2.8）
  ※以後「Gléas」と記載します
- クライアント：Windows 10 Pro (21H1) / Microsoft Edge 94.0.992.47 / Microsoft Excel for Microsoft 365 MSO バージョン2109
  ※以後「Windows」と記載します
- クライアント：iPhone 12 Pro (iOS 15.0.2) / Microsoft Authenticator 6.5.84 / Microsoft Outlook 4.2139.0
  ※以後「iPhone」と記載します

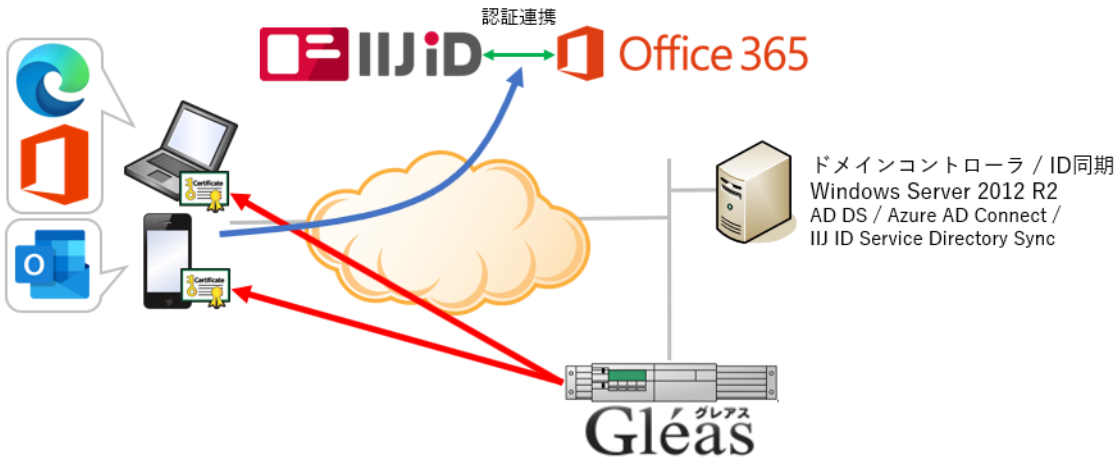
以下については、本書では説明を割愛します。

- IIJ IDの基本設定、およびADとのID同期方法
- IIJ IDとOffice 365とのフェデレーション設定
- Azure AD Connectを用いたOffice 365のユーザプロビジョニング
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作
- Windows、iPhoneでのネットワーク設定やアプリインストール方法

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. WindowsとiPhoneは、GléasのUAから証明書をインポートする
2. Windowsでは、ブラウザおよびOfficeデスクトップアプリケーションからOffice 365へアクセス試行する
3. 認証連携先のIIJ IDのログイン画面に画面遷移し、IIJ IDはパスワードとクライアント証明書を要求し、認証成功するとOffice 365にログインした状態になる
4. iPhoneは、Outlookアプリ でOffice 365へアクセス試行する
5. Microsoft Authenticatorアプリが呼びだされ、IIJ IDでのパスワードとクライアント証明書認証を経て、Exchange Onlineに接続する

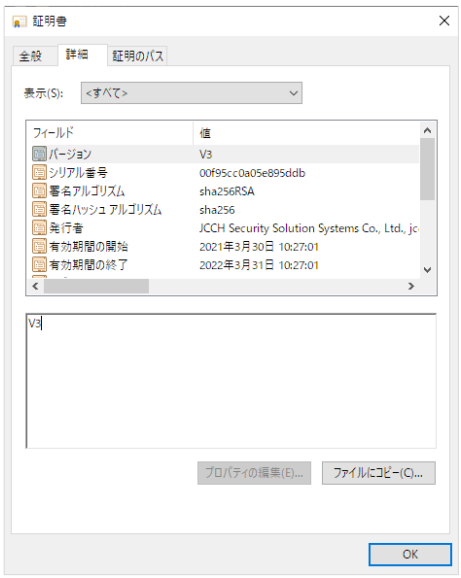
2. IIJ ID の設定

2.1. Gléas のルート証明書の信頼設定

Gléas より発行したクライアント証明書を IIJ ID で認証できるようにするため、Gléas の認証局証明書を IIJ ID に設定します。

Gléas の管理画面（RA）の画面上部の[認証局]リンクをクリックし、発行局（IA）にあるルート認証局名をクリックします。証明書ダウンロードで[CA 証明書:PEM 形式]をクリックし、認証局証明書をダウンロードします。

ダウンロードした証明書ファイルは拡張子が“.pem”となり、それを“.cer”（或いは“.crt”）に変更するとダブルクリックで証明書ウィンドウが開きます。開いたら[詳細]タブをクリックし、ウィンドウ下部の[ファイルにコピー]をクリックすると、証明書のエクスポートウィザードが開始されます。

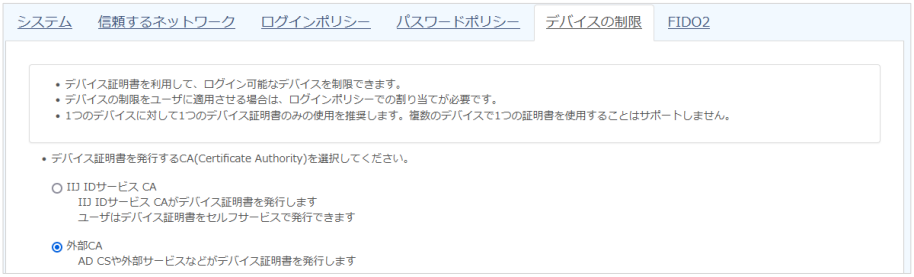


ウィザードを進めエクスポート形式では[Cryptographic ～]を選択し、エクスポートされる PKCS#7 証明書ファイルに名前を付けて保存します。

※ OpenSSL コマンドが利用できる環境では、以下コマンドで PKCS#7 形式に変換可能で

```
openssl crl2pkcs7 -nocrl -certfile ./ia1.pem -out ./ia1.p7b
```

IIJ ID の管理者画面の上部メニュー［システム］>［セキュリティの設定］>［デバイスの制限］と進み、[外部 CA]を選択します。



その下の外部 CA の設定で、[CA 証明書チェーンを登録する]をクリックし、エクスポートした PKCS#7 形式の認証局証明書をアップロードします。

登録成功すると認証局の情報が表示されます。次に、[証明書の失効設定]をクリックします。

OCSP 設定で以下設定を行います。

- [OCSP を有効にする]にチェック
- OCSP サーバ URL に、Gléas の OCSP レスポンダーの URL を入力
  通常は右のような URL 形式になります：http://gleas.example.com:2560/ia1
- [Nonce を有効にする]にチェック

最新の検証ステータスの[OCSP サーバ接続の検証]を行うと、テスト接続をおこないます。その際に HTTP ステータスが 200 で、OCSP ステータスが revoked（あるいは good）になっていれば OCSP レスポンダーとの通信に成功していると判断できます。

次に同じ画面の下部にある CRL 設定をおこないます。

- [CRL を有効にする]にチェック
- [CRL 配布ポイント URL]に、Gléas の CRL 配布ポイント URL を入力
  通常は右のような URL 形式になります：http://gleas.example.com/crl/ia1.crl
- [変更を適用する]をクリック(同時に CRL を取得します)
- [CRL を再取得する]をクリックすると、再度 CRL を取得します(失効の緊急反映時などに利用可能)

なお、OCSP と CRL を両方設定した場合は、OCSP での検証確認が優先され、OCSP レスポンダーに正常に接続できない場合に CRL が利用されます(弊社未検証)。

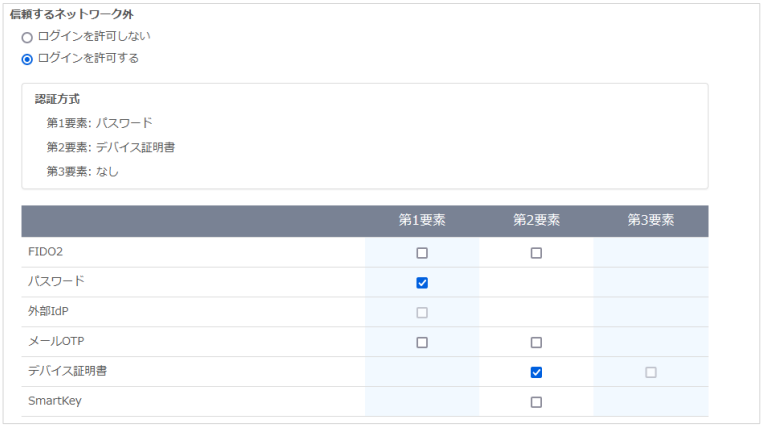
2.2. ログインポリシーの設定

[システム] > [セキュリティの設定] > [ログインポリシー]と進みます。

※　本検証ではデフォルト(Default）ポリシーを編集します

別途設定された信頼されたネットワーク(例：社内ネットワークセグメント)以外からのアクセスにクライアント証明書を要求するよう設定します。
【信頼するネットワーク外】

- [ログインを許可する]を選択
- 第 1 要素に[パスワード]、第 2 要素[デバイス証明書]を選択



設定後、[更新]をクリックして保存します。
これで信頼されたネットワーク以外からの IIJ ID へのアクセスには Gléas より発行された有効なクライアント証明書が必須になります。

3. Gléas UAの管理者設定（Windows向け）

GléasのUA（申込局）より発行済み証明書をWindowsクライアント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おこな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。

※　実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

申込局詳細画面が開くので、基本設定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

設定完了後、[保存]をクリックし保存します。また、認証デバイス設定の以下項目にチェックがないことを確認します。

- iPhone/iPad の設定の、[iPhone / iPad 用 UA を利用する]
- Android/Windows Phone の設定の、[Android / Windows Phone 用 UA を利用する]
- 証明書インポートアプリ連携の設定の、[証明書インポートアプリを利用する]

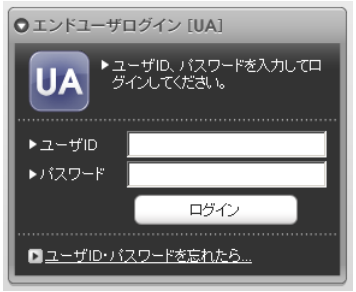
以上でGléasの設定は終了です。

4. クライアントからのアクセス（Windows）

4.1. クライアント証明書のインポート

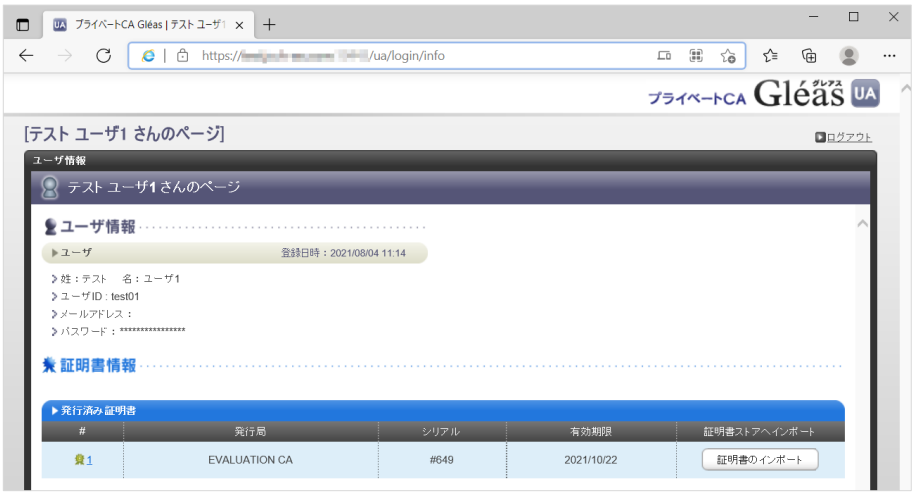
IEモードが設定されたEdge、あるいはInternet ExplorerでGléasのUAサイトにアクセスします。ログイン画面が表示されるので、Gléasでのユーザ IDとパスワードを入力しログインします。

※　UAのログイン認証をActive Directoryで行うことも可能です。詳細は最終項のお問い合わせ先までご連絡ください



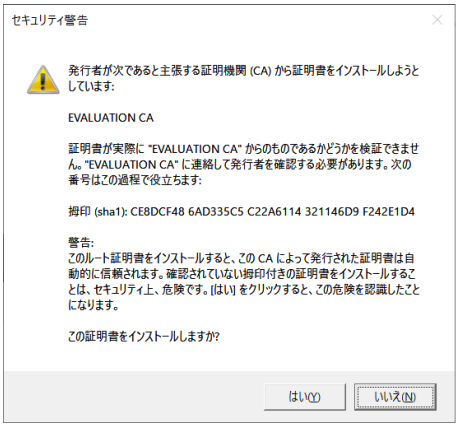
ログインすると、ユーザ専用ページが表示されます。
[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行

われます。

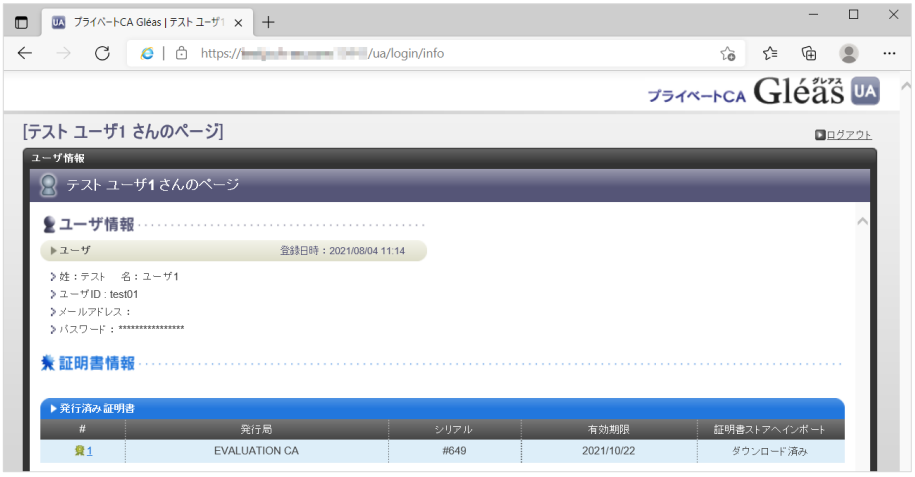


※　初回ログイン時にはActiveXコントロールのインストールを求められるので、画面の指示に従いインストールを完了します

※　証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印を確認するなど正当性を確認してから[はい]をクリックします
(IIJ ID利用においては必須ではないので［いいえ]を選択しても問題ありません)

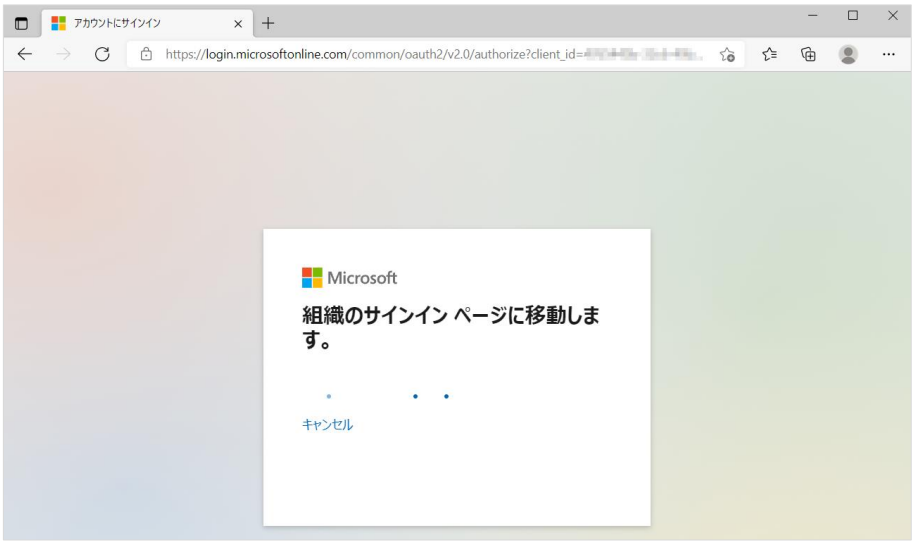


インポートワンス機能を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ログインしてインポートをおこなうことはできません。



4.2. Office 365 への接続(ブラウザ)

ブラウザでOffice 365のログインURLへアクセスし、ドメイン名を含むユーザIDを入力すると、IIJ IDのログオン画面にリダイレクトされます。

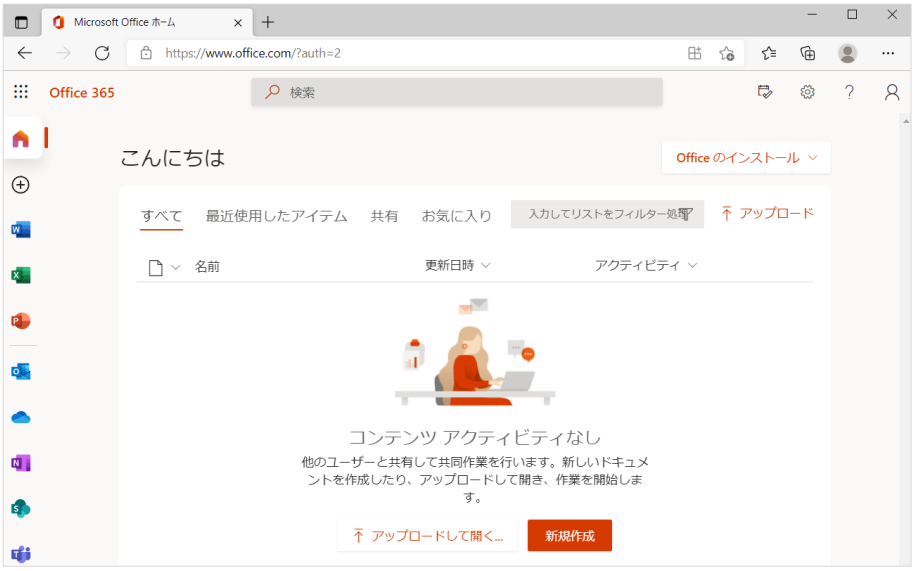


IIJ IDのサインイン画面でログインIDを入力します。

次にパスワードを入力します。

その後、クライアント証明書を提示するよう求められます。

認証が完了すると、Office 365のポータル画面が表示されます。



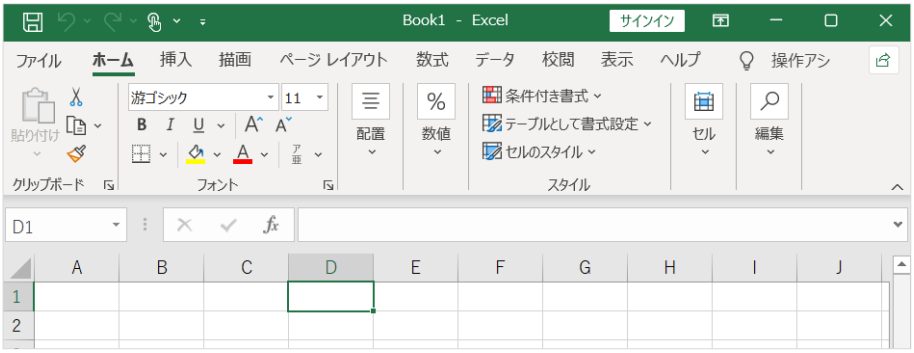
IIJ ID管理画面の上部メニュー[レポート] > [ログイン履歴]を見ると、二要素(パスワード・クライアント証明書)によるログインに成功したことが分かります。

なお、クライアント証明書がない状態でアクセスをすると、「登録されていないデバイスからのアクセス」と表示されます。

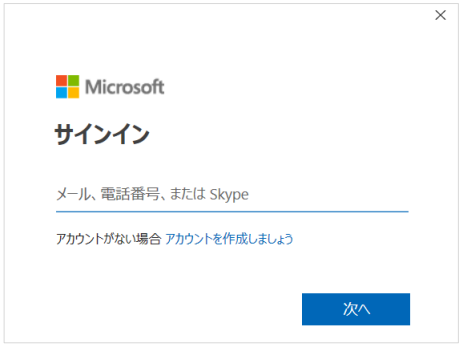
失効された証明書でアクセスしても同様の表示に加え、提示した証明書情報が表示されます。

4.3. Office 365 への接続(Office デスクトップアプリ)

Officeデスクトップアプリ（ここではExcelを使用）を起動して、画面上部の[サインイン]をクリックします。

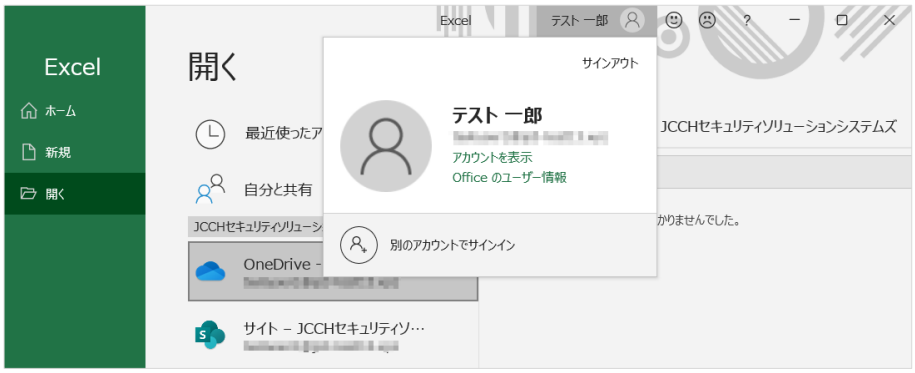


サインイン画面でドメイン名を含むユーザIDを入力すると、IIJ IDのログオン画面にリダイレクトされます。



ユーザIDとパスワードを入力します。

証明書認証がバックグラウンドでおこなわれ（証明書が複数ある場合は選択ダイアログが出現します）、ログインに成功するとOfficeデスクトップアプリケーションにログインした状態になり、そのユーザに割り当てられたOfficeライセンスやファイル共有システム（OneDrive、SharePoint）が利用可能な状態になっています。



証明書がない場合、失効された証明書でアクセスした場合の表示はブラウザのものと同じになります。

5. Gléas の管理者設定（iPhone 向け）

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。

構成プロファイルに必要となる情報の入力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】

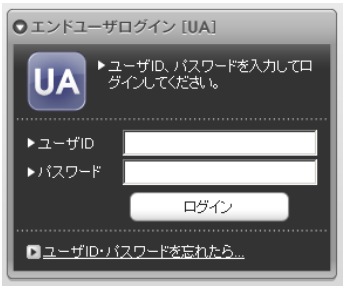
- [名前]、[識別子]に任意の文字を入力（必須項目）

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。

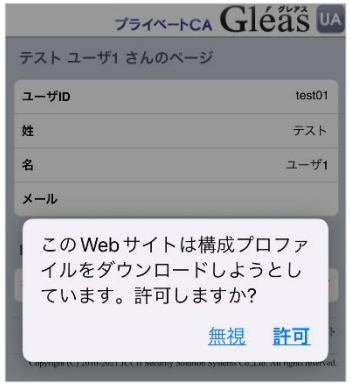
6. クライアントからのアクセス（iPhone）

6.1. 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おこないます。



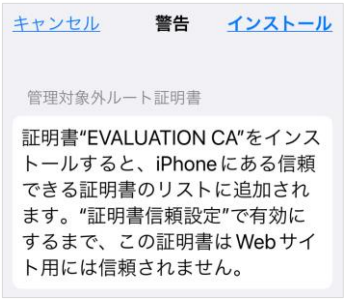
※　インポートロックを有効にしている場合は、この時点からカウントが開始されます

画面の表示にしたがい設定を開くと、プロファイルがダウンロードされた旨が表示されるので、インストールをおこないます。

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できます。必要に応じて確認してください。

インストール中にルート証明書のインストール確認画面が現れるので、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]をタップして終了します。

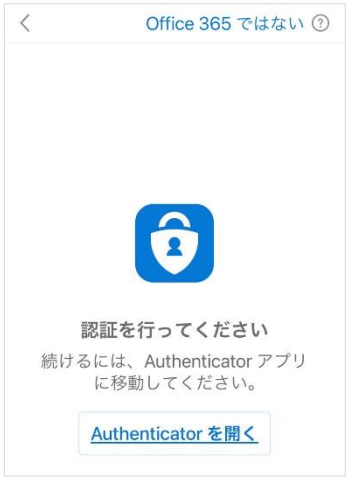
Safariに戻り、[ログアウト]をタップしてUAからログアウトします。
以上で、iPhoneでの構成プロファイルのインストールは終了です。

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。

6.2. Office 365へのアクセス

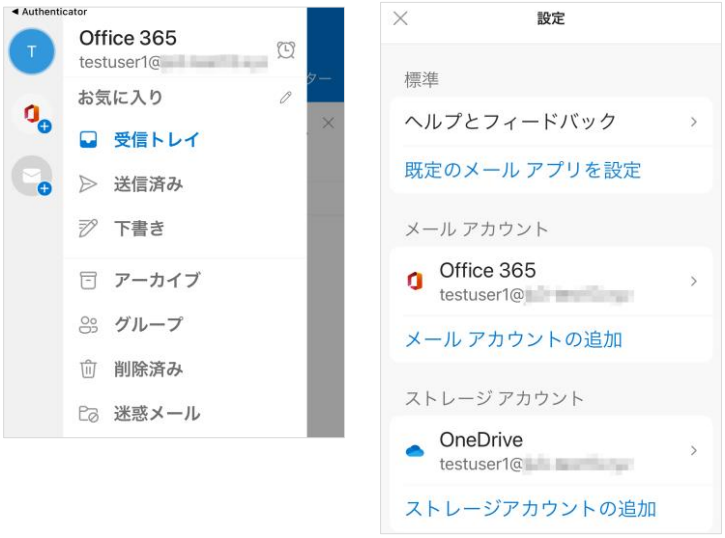
Outlook アプリを起動してアカウントの追加をおこないます。

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

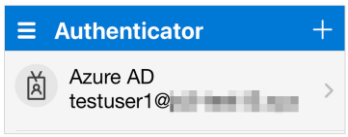


IIJ IDのログイン画面に遷移するので、IDとパスワードを入力します。

その後、証明書認証がバックグラウンドでおこなわれ（提示できる証明書が複数ある場合は選択ダイアログが出現します）、ログインが完了しメール閲覧が可能となります。この状態で[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。



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）



なお、有効な証明書がない場合はログインに失敗します。

また、失効した証明書でログインを試行するとログインに失敗します。

7. 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。

■IIJ ID に関するお問い合わせ

株式会社インターネットイニシアティブ
担当営業までお問い合わせいただくか、以下よりご連絡をお願いいたします。
お問い合わせURL：https://biz.iij.jp/public/application/add/33

■Gléasや本検証内容、テスト用証明書の提供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