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 と

Active Directory フェデレーションサービス（AD FS）での

クライアント証明書認証設定

（ブラウザ および Officeアプリ）

Ver.2.0
2020 年 1 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利用して、Microsoft Corporationのクラウドサービス Office 365 と Windows Serverに含まれる Active Directory フェデレーションサービスで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。

- ドメインコントローラ：Microsoft Windows Server 2012 R2 Standard
  ※　以後、「ドメインコントローラ」と記載します
- フェデレーションサーバ：
  Windows Server 2016 Datacenter
  / Active Directory フェデレーション サービス 4.0
  ※　以後、「ADFSサーバ」と記載します
- AD FSプロキシサーバ：
  Windows Server 2016 Datacenter
  / リモート管理（Web Application Proxy）
  ※　以後、「WAPサーバ」と記載します
- JS3 プライベート認証局 Gléas （バージョン2.1.4）
  ※　以後、「Gléas」と記載します
- SaaSサービス：Office 365 Enterprise E3
  ※　以後、「Office 365」と記載します
- クライアント：Windows 10 Pro / Internet Explorer 11 / Excel バージョン1902
  ※　以後、「PC」と記載します
- クライアント：iPhone （iOS 13.3）/
  Outlook 4.21.0 / Microsoft Authenticator 6.3.27

※　以後、「iPhone」と記載します
※　iOSでは、Microsoft Authenticatorアプリ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。

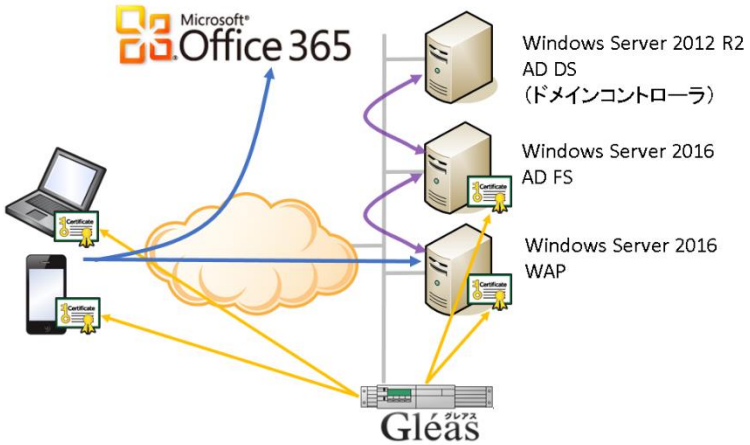
- Windows ServerやWindowsドメインのセットアップ
- ADFSサーバや、WAPサーバのセットアップ
- Office 365の基本設定、ADFSとのフェデレーション設定
  本書では、Office 365とADFS/WAPとのフェデレーション設定が完了していることを前提にしています。
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定
- PC、iPhoneでのネットワーク設定等の基本設定

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。

ADFSではクライアント証明書認証にポート番号49443を利用します。このため、クライアントデバイスからWAP向けのTCPポート49443の通信ができる必要があります。
Gléasでサーバアカウントを作成する際に、ホスト名に追加記述をすることでポート443での通信をすることもWindows Server 2016のADFSでは可能です。(代替ホスト名バインド。1.4項参照)

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ADFSとWAPにSSL用サーバ証明書を、PC、iPhoneの利用者にク

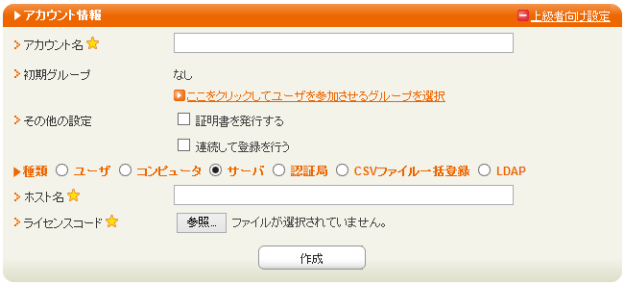
ライアント証明書を発行する

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を利用）でOffice 365にアクセスすると、認証先としてWAPにリダイレクトされる
3. iPhone：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WAPにリダイレクトされる
4. ADFSでは二要素認証をおこなう（フォーム認証＋クライアント証明書認証）。
   認証情報はOffice 365に連携される（フェデレーション）。
   有効な証明書を持つクライアントデバイスのみOffice 365に接続してOfficeアプリを利用することができる。

1.4. 電子証明書の発行時における留意事項

Gléasで電子証明書を発行する際に以下の点に留意する必要があります。

- 本書では、ADFSサーバ・WAPサーバのSSLサーバ証明書を入れ替える手順を記述しますが、その場合ADFSの[フェデレーションサービス名]と、Gléasでのサーバアカウントを作成する際の[ホスト名]が一致している必要があります。



フェデレーションサービス名は、[ADFSの管理]より左ペインの[サービス]を右クリックし、[フェデレーションサービスのプロパティの編集(E)]をクリックすると表示される[フェデレーションサービスのプロパティ]画面で確認できます。

また1.2項で触れた通り、Windows Server 2016 以降では［ホスト名］に、”certauth.[フェデレーション サービス名]”も加えておくことで、ポート49443の通信をしないようにできまです。
その場合の[ホスト名]欄の入力は以下の例のようにします。
例）sts.example.com;certauth.sts.example.com

- iOS 13以降より、サーバ証明書に対する要件が変更されており、証明書有効期間は825日未満である必要があります。

- クライアント証明書には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（UPN）
  - ✓ CRL配布ポイント

2. ドメインコントローラでの設定

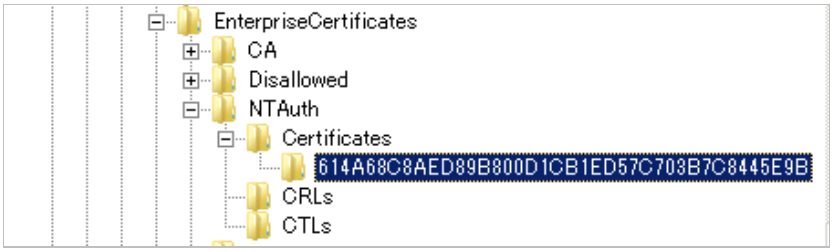
2.1. ルート証明書の NTauth ストアへのインポート

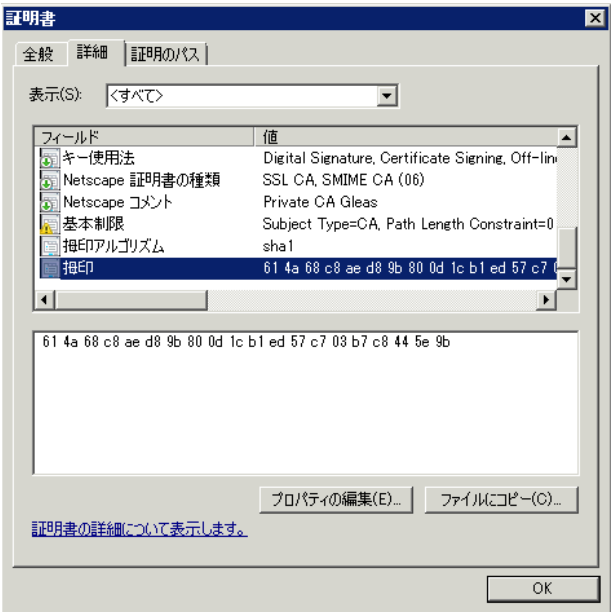
ルート証明書を Gléas よりダウンロードし、Windows ドメインの NTauth ストアと呼ばれる格納領域にインポートします。
コマンドプロンプトを開き、以下のコマンドを入力します。

```
certutil -dspublish -f [filename] NTAuthCA
```

※ [filename]には、エクスポートしたルート証明書を指定します

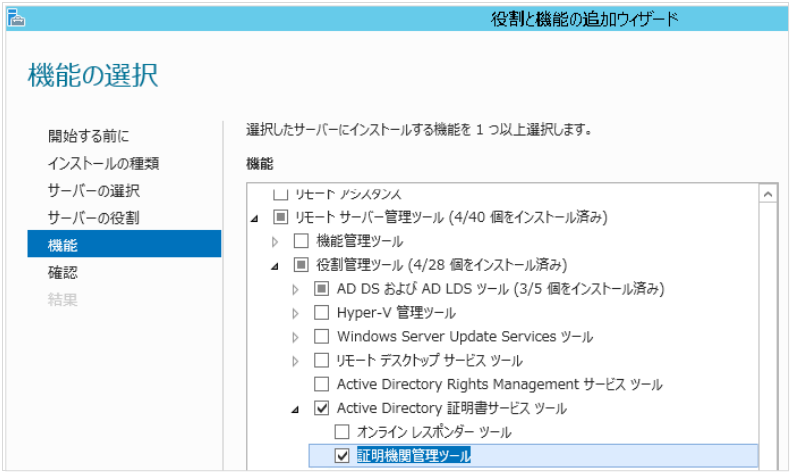
コマンド実行後、以下のレジストリにルート証明書の拇印と同じ名前のレジストリキーが追加されます。
HKLM¥SOFTWARE¥Microsoft¥EnterpriseCertificates¥NTAuth¥Certificates
※ 追加されない場合は、gpupdate コマンドでポリシーの更新を行ってください



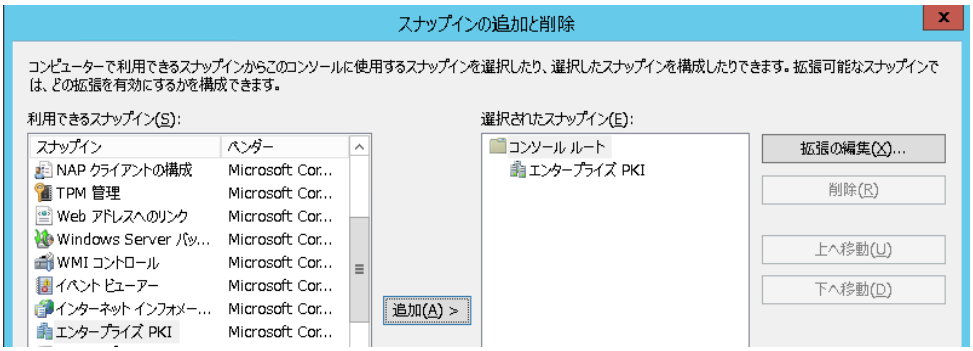


ADFS サーバでも同様にレジストリエントリに追加されているか確認します。
※ 追加されない場合は、gpupdate コマンドでポリシーの更新をします

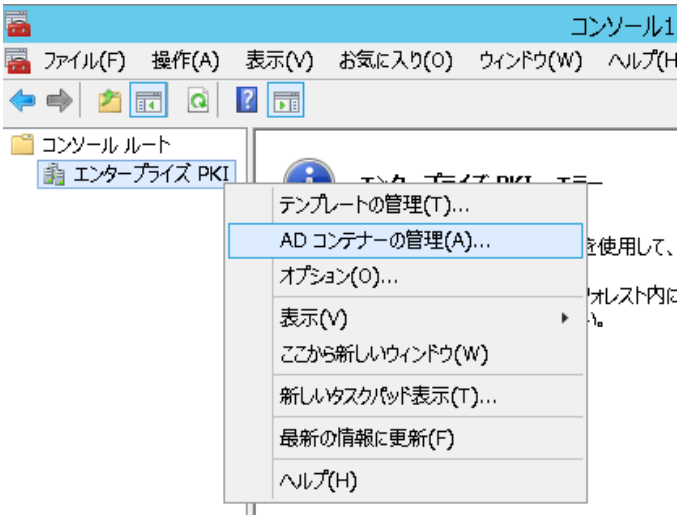
なお、NTauth ストアへの証明書インポートは、GUI でおこなうことも可能です。サーバーマネージャで、[役割と機能の追加]をおこない、[証明機関管理ツール]を追加します。



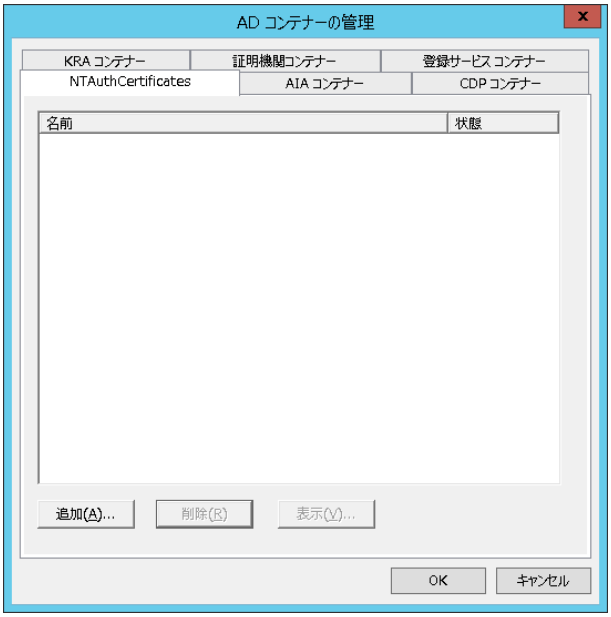
その後、MMC（マイクロソフト管理コンソール）を開き、[エンタープライズ PKI]スナップインを追加します。



エンタープライズ PKI 上で右クリックをし、[AD コンテナーの管理(A)…]を選択します。



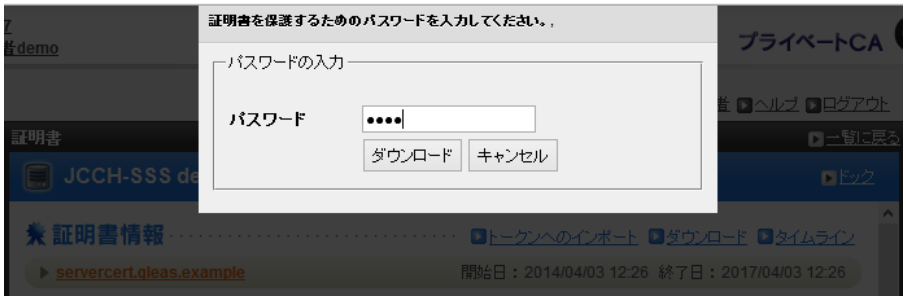
[NTAuthCetificates]タブで[追加(A)…]をクリックし、ルート証明書ファイルを選択することで NTauth ストアにルート証明書を追加します。



3. ADFSサーバでの設定

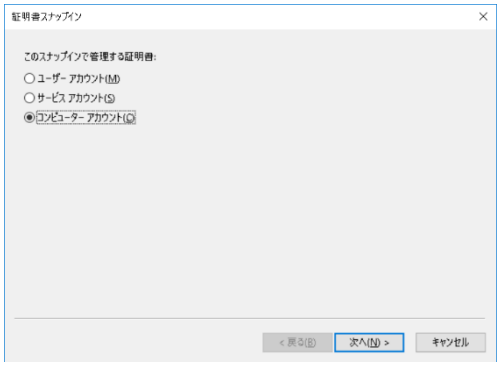
3.1. SSL サーバ証明書のインポート

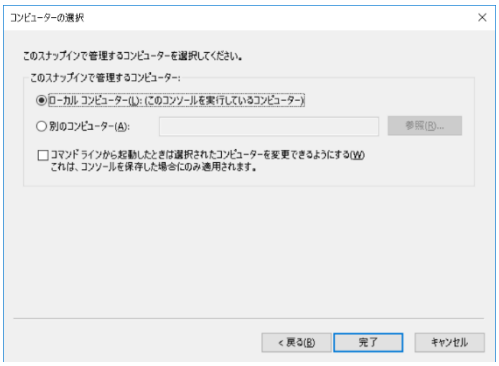
本手順開始前に、Gléas の管理者画面よりサーバ証明書ファイル（PKCS#12 ファイル）をダウンロードします。
ダウンロードする際に保護パスワードの入力を求められますので、入力してからダウンロードし、ADFS サーバにそのファイルをコピーします。



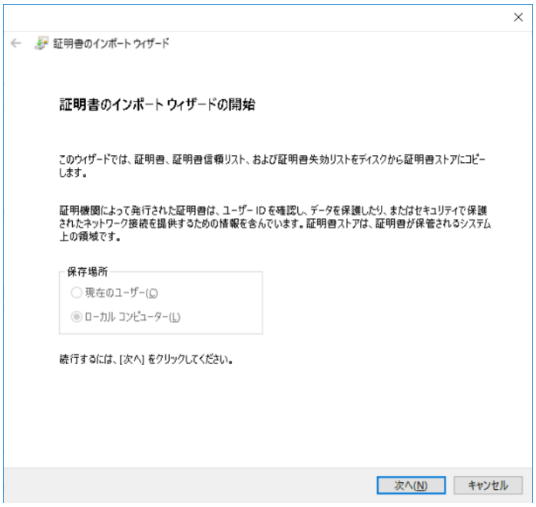
MMC を開き、メニューの[ファイル(F)] > [スナップインの追加と削除(N)]より[証明書]を追加します。

「証明書のスナップイン」では、[コンピューター アカウント(C)]を選択し、次の「コンピューターの選択」では、[ローカルコンピューター(L)]を選択し、[完了]をクリックします。





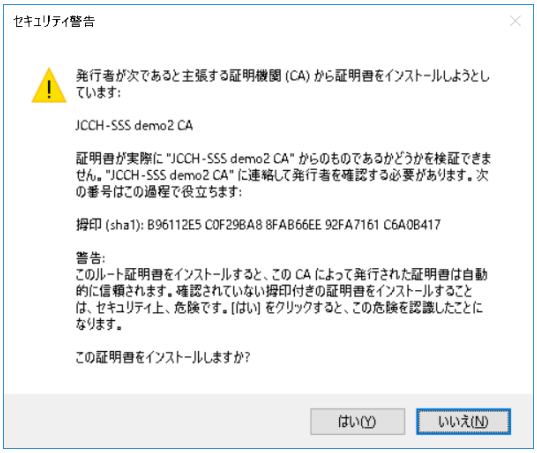
スナップインが追加されたら左側のペインより[証明書] > [個人]と展開し、右側のペインで右クリックして、[すべてのタスク(K)] > [インポート(I)]をクリックします。「証明書のインポートウィザード」が開始されるので、サーバ証明書をインポートします。



ページ	設定
証明書のインポートウィザードの開始	[次へ(N)]をクリック
インポートする証明書ファイル	Gléas よりダウンロードした PKCS#12 ファイル（拡張子：p12）を指定して、[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

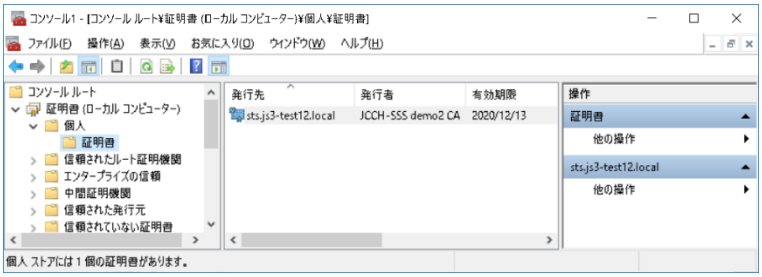
証明書インポートウィザードの終了	[完了]をクリック

ルート証明書も同時にインポートされるため、Windows OS が警告を表示します。正しい拇印を持った証明書であることを確認し、[はい]をクリックします。

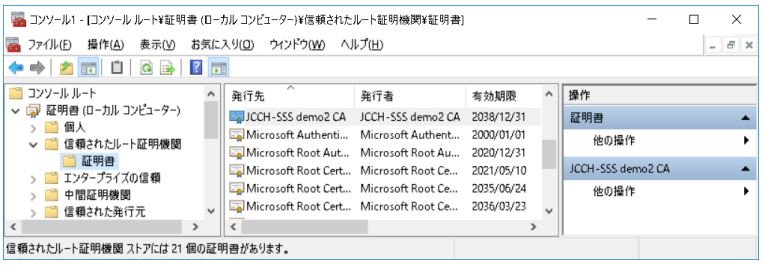


なお、Gléas 上でルート証明書の拇印を確認するには、管理画面右上の[▶認証局]から該当する発行局情報をクリックし、拇印の欄を参照します。

完了後、サーバ証明書がインポートされていることを確認します。



またルート証明書も同時にインポートされていることを確認します。



※ ルート証明書については、以下のグループポリシ（GPO）により複数マシンに対して同様の設定を一括しておこなうことが可能です。
[コンピューターの構成] > [ポリシー] > [Windows の設定] > [セキュリティの設定] > [公開キーのポリシー] > [信頼されたルート証明機関]

3.2. SSL サーバ証明書の適用

Windows Powershell を起動して、以下のコマンドを入力します。

```
Set-AdfsSslCertificate  -Thumbprint [証明書の拇印]
```

代替ホスト名バインドを使う場合は、Set-AdfsSslCertificate の代わりに以下コマンドを入力します。

```
Set-AdfsAlternateTlsClientBinding -Thumbprint [証明書の拇印]
```

なお、3.1 項でインポートした証明書の拇印は以下のコマンドで確認できます。

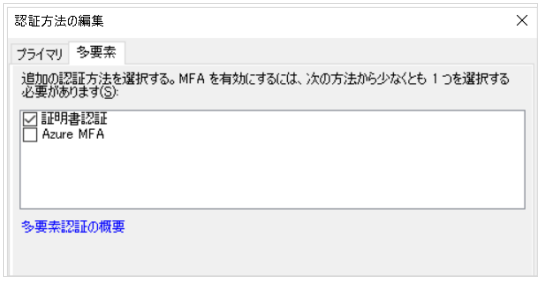
```
Get-ChildItem Cert:¥LocalMachine¥My
```

なお、適用されたサーバ証明書は以下で確認できます。

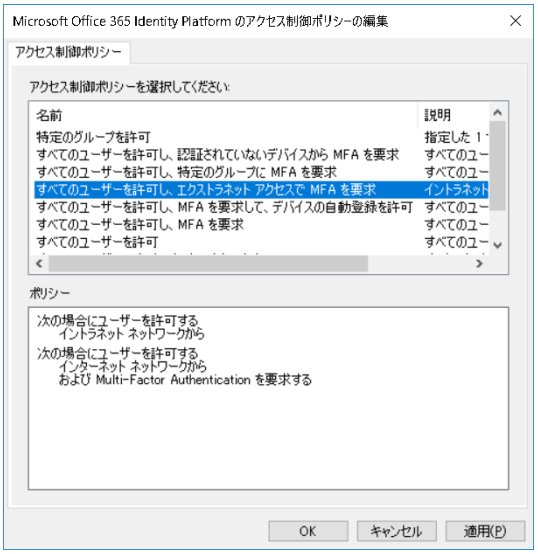
```
Get-AdfsSslCertificate
```

3.3. 多要素認証（MFA）の設定

スタートメニューより[AD FS の管理]を起動し、左側ペインの[サービス] > [認証方法]を選択し、中央ペインの[多要素認証方法]の[編集]をクリックします。
[認証方法編集]ウィンドウが開くので、[多要素]タブで[証明書認証]をチェックします。



次に、左ペインで[証明書利用者信頼]を選択し、中央ペインで”Microsoft Office 365 Identity Platform”を選択、右ペインよりアクセス制御ポリシーの編集をクリックします。
アクセス制御ポリシーの編集ウィンドウで、[すべてのユーザーを許可し、エクストラネット アクセスで MFA を要求]を選択し、[適用(P)]ボタンをクリックします。



4. WAPサーバでの設定

4.1. SSL サーバ証明書のインポート

3.1 項と同じ手順でサーバ証明書とルート証明書を WAP サーバにインポートします。

4.2. SSL サーバ証明書の適用

Windows Powershell を起動して、以下のコマンドを入力します。

```
Set-WebApplicationProxySslCertificate  -Thumbprint [証明書の拇印]
```

なお、4.1 項でインポートした証明書の拇印は以下のコマンドで確認できます。

```
Get-ChildItem Cert:¥LocalMachine¥My
```

設定された証明書は以下のコマンドで確認できます。

```
Get-WebApplicationProxySslCertificate
```

5. 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。

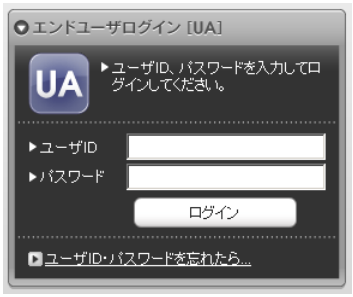
- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

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。

6. クライアント操作（PC）

6.1. 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。



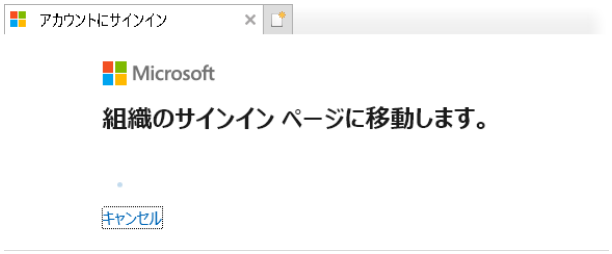
ログインすると、ユーザ専用ページが表示されます。
[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。

※ 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。

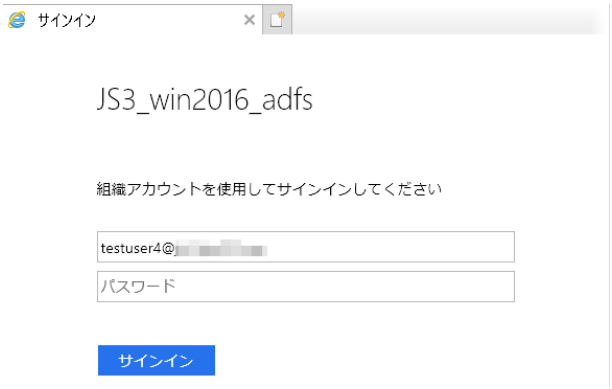
「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません。

6.2. Office 365 へのアクセス（ブラウザ）

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



ADFSのサインイン画面でパスワードを入力します。

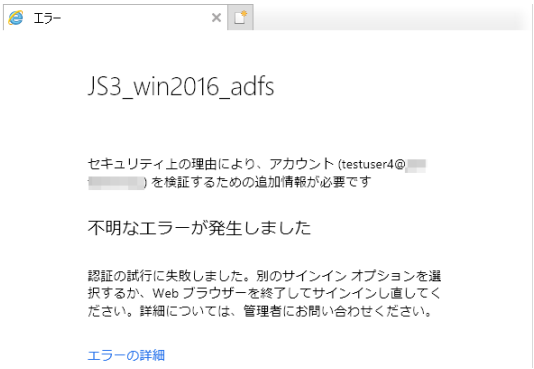


その後、クライアント証明書を提示するよう求められます。

※ WAPサーバ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

認証が完了すると、Office 365のポータル画面が表示されます。

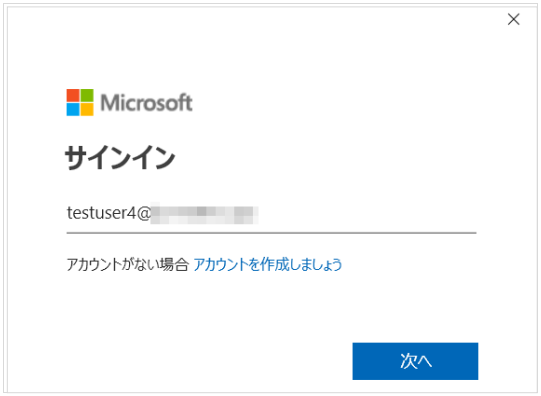
なお、失効した証明書でアクセスをすると、エラー表示となります。



6.3. Office 365 へのアクセス（Office アプリ）

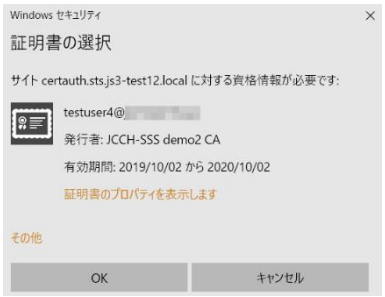
Excelを起動しタイトルバーにある[サインイン]をクリックします。

Office 365ログイン用のユーザIDを入力します。

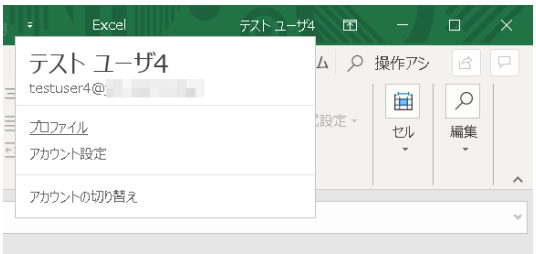


ADFSのログイン画面でパスワードを入力します。

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の提示を求められます。



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できます。

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。

7. 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。

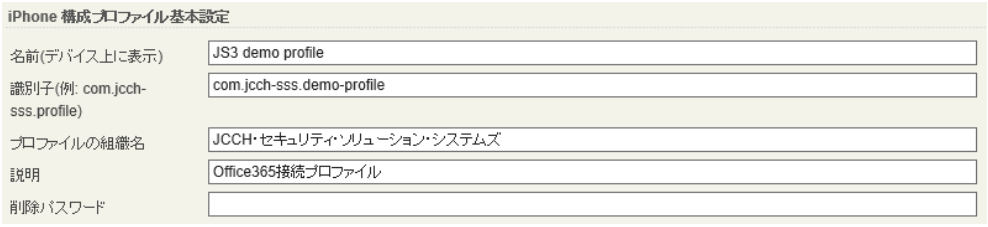
構成プロファイル生成に必要となる情報を入力する画面が展開されるので、以下設定を行います。

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）



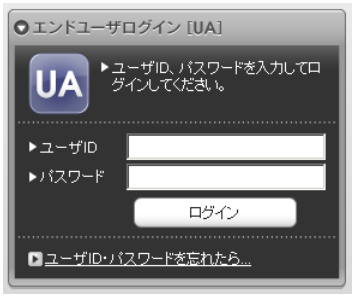
各項目の入力が終わったら、 [保存]をクリックします。

以上でGléasの設定は終了です。

8. クライアント操作（iPhone）

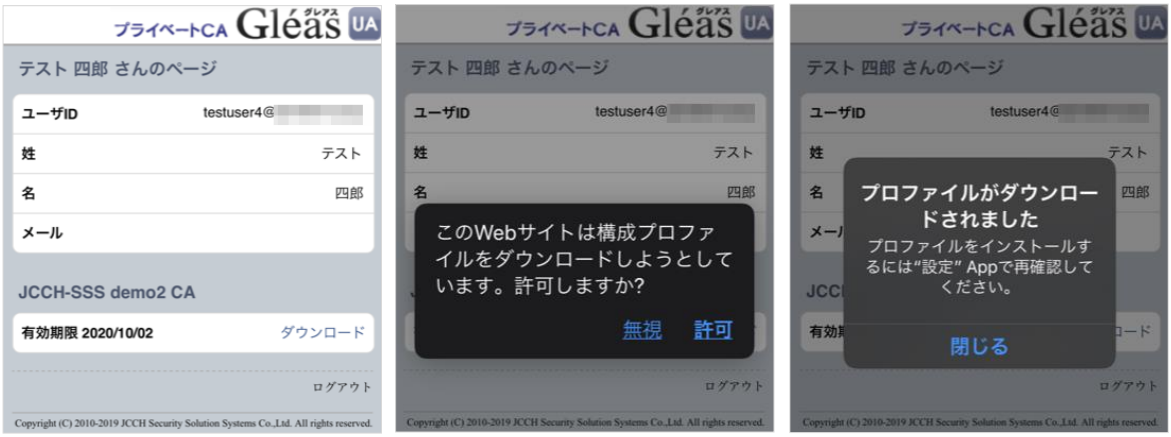
8.1. クライアント証明書のインポート

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。

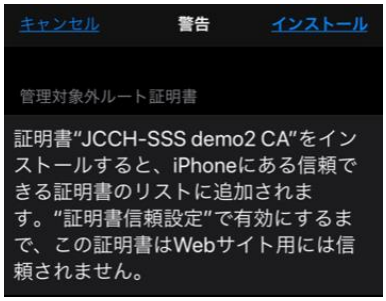
※インポートロックを有効にしている場合は、この時点からカウントが開始されます



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。

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]をタップして終了します。

その後、設定より[情報] > [証明書信頼設定] と進み、インポートしたルート証明書を信頼するよう設定をおこないます。

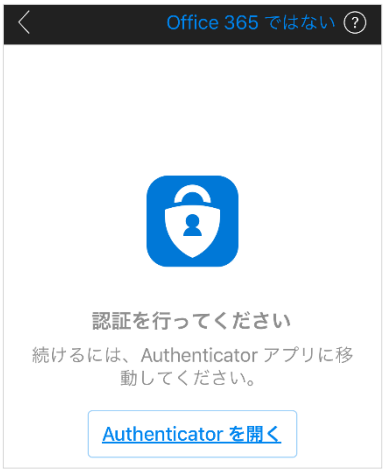
Safariに戻り、[ログアウト]をタップしてUAからログアウトします。
以上で、iPhoneでの構成プロファイルのインストールは終了です。

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。

8.2. Office 365へのアクセス

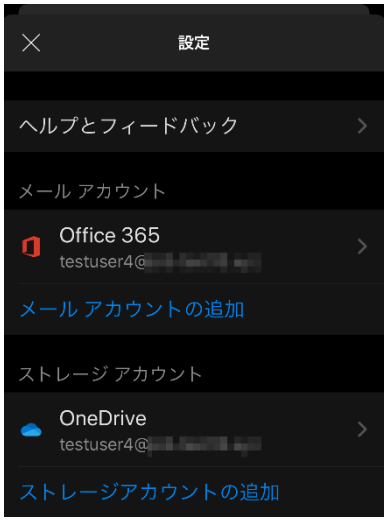
Outlook アプリを起動してアカウントの追加をおこないます。

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

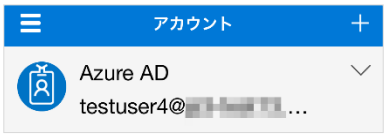


ADFSのログイン画面に遷移するので、パスワードを入力します。

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や、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。

9. 失効について

証明書失効によるアクセス拒否時には、ADFSサーバのadminログに以下のログエ

ントリが発生します。

> 説明:
> トークンの検証に失敗しました。
>
> 追加データ
>
> トークンの種類:
> http://schemas.microsoft.com/ws/2006/05/identitymodel/tokens/X509Certificate
> %エラー メッセージ:
> ID4070: X.509 証明書 'CN=testuser4@example.com' チェーンの構築に失敗しました。使用された証明書には、検証できない信頼チェーンが存在します。証明書を交換するか、certificateValidationMode を変更してください。' 証明書が失効しています。
> '

Windows Serverは失効リスト（CRL）を取得するとその有効期限までキャッシュします。以下コマンドをADFSを動かしているサーバ上で実行することで、CRLのキャッシュ終了時間を即時にクリアできます。

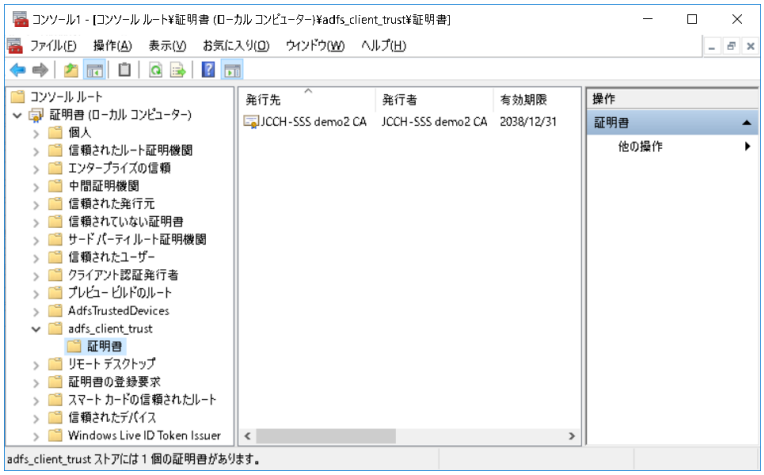
```
certutil -urlcache crl delete
certutil -setreg chain¥ChainCacheResyncFiletime “@now”
net stop cryptsvc
net start cryptsvc
```

10. CTL（Certificate Trust List）について

CTLを使うことで、Gléasから発行したクライアント証明書だけをクライアントに提示させることが可能となります。
CTLの設定は、今回の環境ではWAPサーバにて以下の手順でおこないます。

- CTLを作成する

certutil -f -addstore [**証明書ストア名**] [**ルート証明書ファイル**]
MMC**で証明書ストアを見ると**（certlm.msc）**、ストアが作成されているのが分かります。**
例）certutil -f -addstore adfs_client_trust ia1.cer



この画面で信頼するルート証明書を追加インポートすることも可能です。

- ポート49443（証明書認証サイト）のSSLバインドを解除する

netshコマンドを使って設定します。

```
> netsh
netsh>http
netsh http>delete sslcert hostnameport=[フェデレーションサービス名]:49443
```

※ 代替ホスト名バインドの利用時は、「hostnameport=certauth.[フェデレーションサービス名]:443」とします(以下同じ)

正常に終了すると、「SSL 証明書を正常に削除しました」と表示されます

- 作成したCTLを指定し、ポート49443に対してSSLバインドを再度設定する

```
netsh http>add sslcert hostnameport=[フェデレーションサービス名]:49443
certhash=[サーバ証明書の拇印] appid={5d89a20c-beab-4389-9447-324788eb944a}
certstorename=MY sslctlstorename=[証明書ストア名]
```

正常に終了すると、「SSL 証明書を正常に追加しました」と表示されます

- 実施した結果を確認

```
netsh http>show sslcert
```

```
SSL 証明書のバインド:
-------------------------

    ホスト名:ポート                : [フェデレーションサービス名]:49443
    証明書ハッシュ                 : e98585ee1f032b7fd7f94f2bb57de2bc7d6e9e0f
    アプリケーション ID            : {5d89a20c-beab-4389-9447-324788eb944a}
    証明書ストア名                 : MY
    クライアント証明書の失効状態の検証: Enabled
    キャッシュされたクライアント証明書のみを使用した失効状態の検証: Disabled
    使用法のチェック               : Enabled
    失効リストの更新を確認する間隔: 0
    URL 取得のタイムアウト         : 0
    Ctl 識別子                     : (null)
    Ctl ストア名                   : adfs_client_trust
    DS マッパーの使用法            : Disabled
    クライアント証明書のネゴシエート: Disabled
```

11. お問い合わせ

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