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

Microsoft Entra CBAによる高アフィニティな認証バインド設定

Ver.1.0

2025 年 5 月

目次

1. はじめに 5

1.1. 本書について 5

1.2. 本書における環境 6

1.3. 本書における構成 7

2. Gléas の設定 8

2.1. 証明書テンプレートの設定 8

2.2. アカウント作成と証明書発行 9

2.3. 証明書の配布設定 11

3. Entra ID の設定 13

3.1. 認証局を登録 13

3.2. グループの作成 15

3.3. 証明書ベース認証の有効化 17

3.3.1. 認証強度を構成 18

3.3.2. 証明書とユーザーの紐づけを構成 20

3.4. ユーザー情報の更新 21

3.4.1. 証明書の属性値を取得 21

3.4.2. 証明書ユーザーID を設定 23

4. クライアントの設定 25

4.1. クライアント証明書をインポート 25

4.2. 証明書ベース認証 27

5. その他 30

5.1. 証明書ユーザーID を用いた認証制御について 30

5.2. 証明書ユーザ ID の取得について 33

6. 問い合わせ 34

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、Entra ID ユーザーと高い親和性（高アフィニティ）をもった認証バインドによる証明書ベース認証 (CBA)を行う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。

- 認証基盤： Microsoft Entra ID

  ※以後「Entra ID」と記載します

- アプリケーション： マイ アプリ ポータル

  ※以後「マイ アプリ」と記載します

- 認証局： JS3 プライベート認証局 Gléas (バージョン 2.7.1)

  ※以後「Gléas」と記載します

- クライアント：Windows 10 Pro (22H2) / Microsoft Edge 136.0.3240.50

  ※以後「Windows」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。

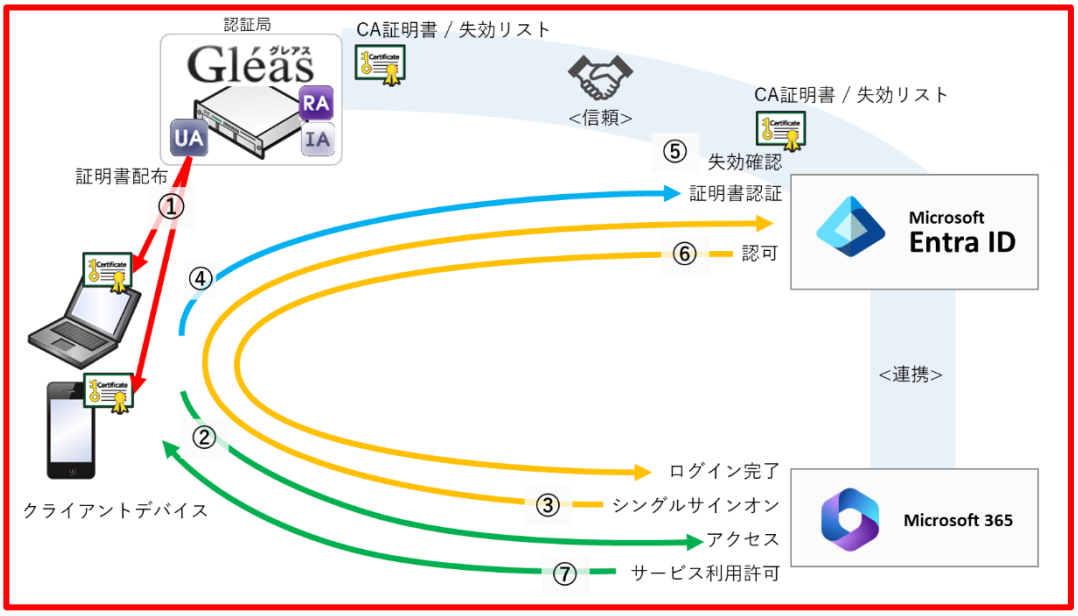
- Entra ID の基本設定
- Gléas のアカウント登録やクライアント証明書発行等の基本操作

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 は、クライアントデバイス向けにクライアント証明書を発行する。
2. Entra ID に、Gléas の CA 証明書を登録して証明書の発行元を信頼する。
3. Entra ID に、m365 のログインに証明書認証を強制するように設定。
4. クライアントデバイスは、Gléas より証明書をインポートする。①
5. 利用者は、PC より マイ アプリ にアクセスする。②
6. マイ アプリ は、Entra ID にシングルサインオン。③
7. クライアントデバイスは、Entra ID にクライアント証明書認証を行う。④、⑤
   このとき、証明書ベース認証（Entra CBA）は、証明書の「サブジェクトキー識別子（SKI）」属性と Entra ID の「ユーザ証明書 ID（UserCertificateIDs）」属性を用いて認証を行う。
8. 認証成功すると、Entra ID は認可して マイ アプリ にログイン完了。⑥
9. 利用者は、 マイ アプリ を利用可能となる。⑦

2. Gléas の設定

2.1. 証明書テンプレートの設定

Entra ID 証明書ベース認証の要件を満たすように Gléas のデフォルトテンプレートを以下のように設定します。

※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

証明書の属性	データベースの項目
発行局	[発行局名]
暗号アルゴリズム	RSA暗号
鍵長	2048bit
ダイジェストアルゴリズム	SHA256
有効日数	1年
鍵用途	電子署名、鍵の暗号化
拡張鍵用途	SSLクライアント認証

2.2. アカウント作成と証明書発行

クライアント証明書の発行対象となる Gléas アカウントを作成し、証明書を発行します。

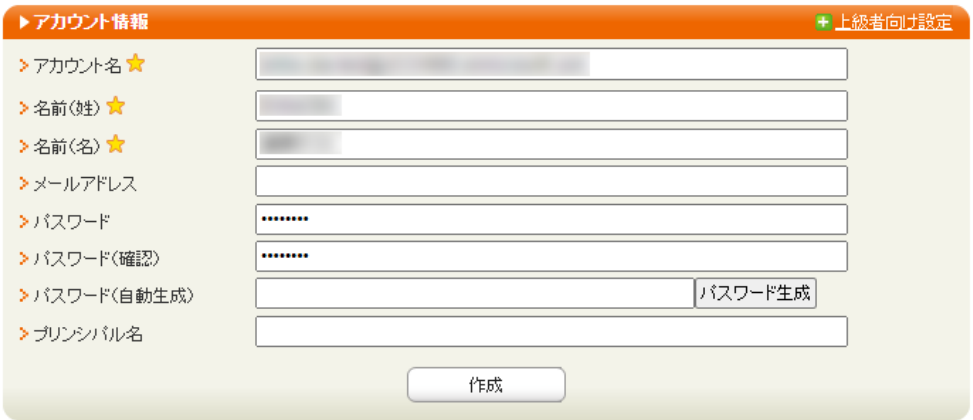
Gléas RA（登録局）にログインします。

[アカウント]>[アカウント新規作成]メニューをクリックします。

- [その他の設定]の[証明書を発行する]をチェック
- [▸種類]から[CSV ファイル一括]を選択
- アカウント情報に以下を入力

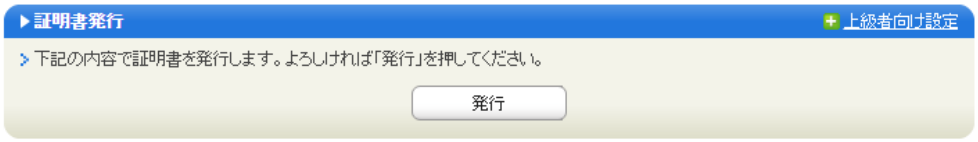
項目	意味
アカウント名	証明書のサブジェクト一般名となります
名前（姓）	UA に表示される名前（姓）となります
名前（名）	UA に表示される名前（名）となります
パスワード	UA のログインパスワードとなります

- [作成]をクリック



- [アカウント] > 詳細画面で [証明書発行] メニューをクリック

- 内容を確認し [発行] をクリック



※しばらくするとアカウントに対してクライアント証明書に発行されます

2.3. 証明書の配布設定

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おこなっている場合があります

Gléas RA（登録局）にログインします。

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

各項目の入力が終わったら、 [保存]をクリックします。

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 の設定の、[Android 用 UA を利用する]

3. Entra ID の設定

3.1. 認証局を登録

証明書ベース認証と連携する認証局を登録します。

本手順の前にGléasよりルート証明書をダウンロードします。

※GléasのデフォルトCAのルート証明書（PEM形式）のダウンロードURLは以下となります
http://[GléasのFQDN]/crl/ia1.pem

Microsoft Entra 管理センター にログインします。

メニュー [保護] > [セキュリティセンター] を選択します。

[認証局] を選択し、[アップロード] をクリックします。

- [証明書] に Gléas のルート証明書を指定

  ※拡張子が .cer でないとアップロードできないので、.pem を .cer に変更して指定
- [ルートCA証明書である] に [はい] を選択
- [証明書失効リストのURL] にCRL配布点のURLを入力

  ※GléasのデフォルトCRL配布点のURLは以下となります
  http://[GléasのFQDN]/crl/ia1.crl
- [デルタ証明書失効リストの URL] は指定しない
- [追加] をクリック

認証局が登録されました。

3.2. グループの作成

証明書ベース認証を行う対象となるセキュリティグループを作成します。

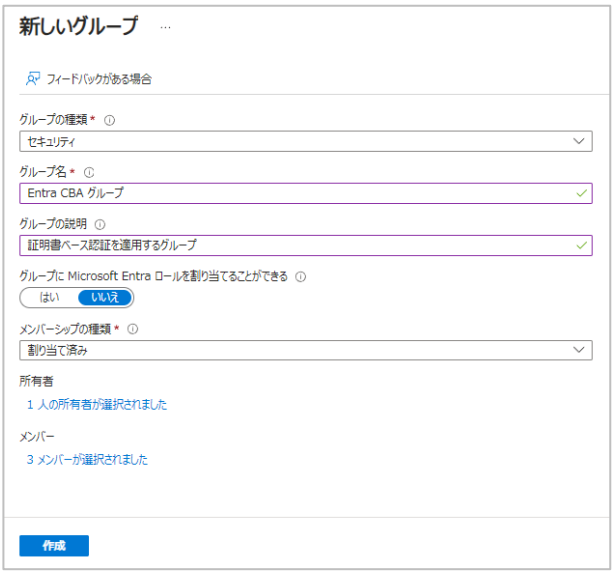
メニュー [グループ] > [すべてのグループ]を選択します。

[新しいグループ] をクリックします。

- [グループの種類] に [セキュリティ] を選択
- [グループの名] に任意の名前を入力

  ※例) "Entra CBA グループ"
- [グループの説明] に任意の説明を入力

  ※例) "証明書ベース認証を適用するグループ"
- [メンバーシップの種類] に [割り当て済み] を選択
- [所有者] の [所有者が選択されていません] をクリックして、セキュリティグループの所有者となるユーザーを選択
- [メンバー] の [メンバーが選択されていません] をクリックして、セキュリティグループの所属メンバーとなるユーザーを選択
- [作成] をクリック



セキュリティグループが作成されました。

3.3. 証明書ベース認証の有効化

作成したセキュリティグループに対して証明書ベース認証を有効化します。

メニュー [保護] > [認証方法]を選択します。

[ポリシー] を選択し、[証明書ベースの認証] をクリックします。

[有効化およびターゲット] タブを選択します。

- [有効にする] を ON
- [含める] タブの [ターゲット] の [グループの選択] を選択
- [グループの追加] をクリックして作成したセキュリティグループを選択
- [保存] をクリック

3.3.1. 認証強度を構成

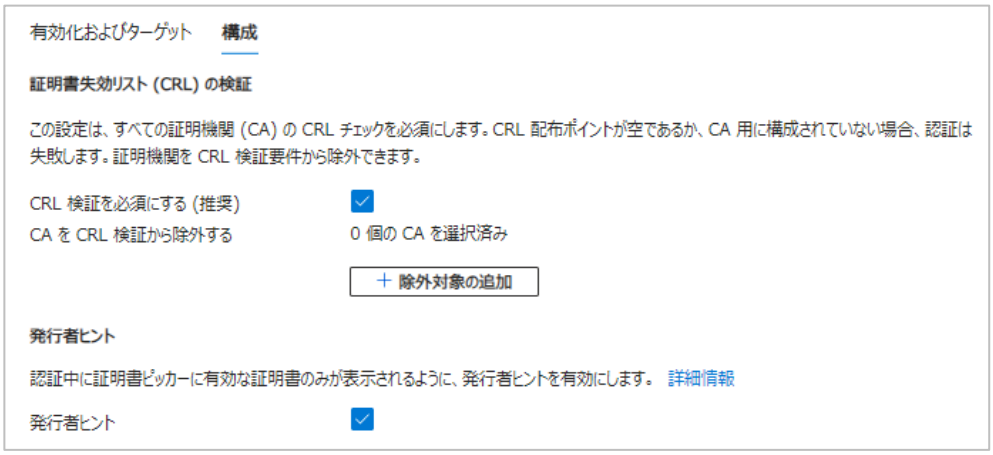
証明書ベース認証の認証強度を設定するポリシーを構成します。

メニュー [保護] > [認証方法]を選択します。

[ポリシー] を選択し、[証明書ベースの認証] をクリックします。

[構成] タブを選択します。

- [CRL検証を必須にする] をチェック
- [発行者ヒント] をチェック



- 認証バインド [保護レベル] に [多要素認証] を選択

  認証バインド [必須のアフィニティバインド] に [高] を選択

- 認証バインド [＋規則の追加] をクリック
- 証明書の属性 で [証明書の発行者] を選択

- [証明書の発行者] に先に登録した認証局を選択
- [認証強度] に [多要素認証] を選択

  ※本書では証明書を用いた認証を多要素認証として扱うように設定しています。
- [アフィニティ バインド] に [高] を選択
- [追加] をクリック

- [保存] をクリック

3.3.2.証明書とユーザーの紐づけを構成

証明書ベース認証でクライアント証明書と Entra ID ユーザーを紐づけるポリシーを構成します。

メニュー [保護] > [認証方法]を選択します。

[ポリシー] を選択し、[証明書ベースの認証] をクリックします。

[構成] タブを選択します。

- ユーザー名バインド [+規則の追加] をクリック
- [証明書フィールド] に [SKI] を選択
- [ユーザー属性] に [CertificateUserIDs] を選択

  ※証明書のSKI（サブジェクト キー識別子）が Entra ID ユーザーの CertificateUserIDs 属性の内容と一致するかをチェックして認証する設定とします。
- [追加] をクリック

3.4. ユーザー情報の更新

配布した証明書で認証が行えるように Entra ID ユーザーの証明書ユーザーID (CertificateUserIDs) 属性に証明書を特定するための情報を設定します。

3.4.1. 証明書の属性値を取得

本書では発行した証明書を特定するための固有値として、「サブジェクト キー識別子 (SKI)」を使用します。

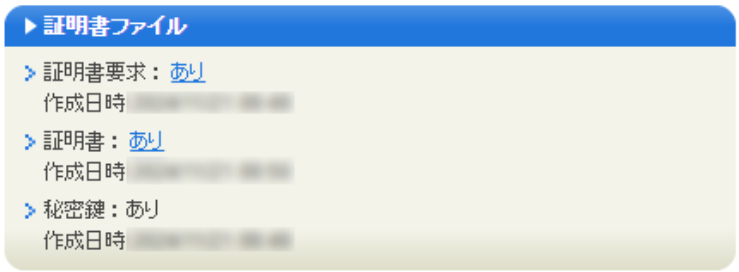
Gléas RA（登録局）にログインします。

[アカウント]>[アカウント一覧]メニューをクリックします。

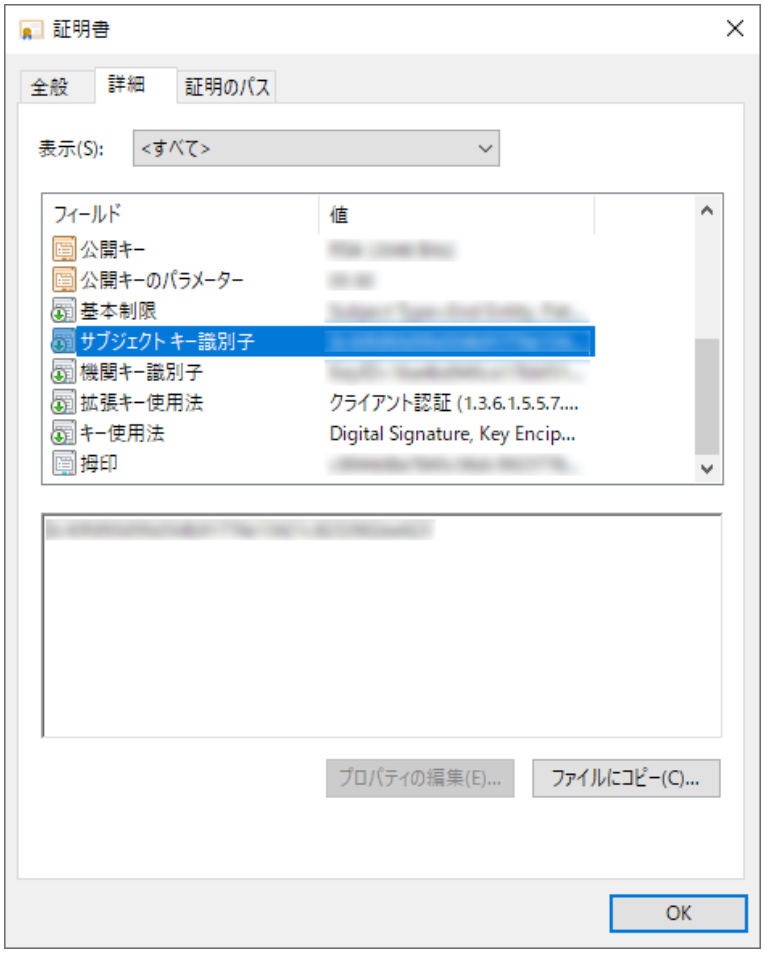
[アカウント] > アカウント一覧 画面から2.2項で作成したアカウントを検索し、

[アカウント] > 詳細 画面に遷移します。

- 証明書発行の履歴 から発行した証明書の行をクリック
- [証明書] > 詳細 画面の証明書ファイルのリンクから証明書をダウンロード



- ダウンロードした証明書ファイルを開き、[詳細]タブを選択
- [サブジェクト キー識別子] フィールドの値をコピーして控えておく



3.4.2. 証明書ユーザーID を設定

対象の Entra ID ユーザーに証明書ユーザーID（CertificateUserIDs）を追加します。

メニュー [ID] > [ユーザー]を選択します。

[すべてのユーザー] から対象のユーザーを選択し、[概要] 画面を表示します。

- [プロパティの編集] をクリック
- 認可情報 の [＋証明書ユーザIDの編集] をクリック
- 入力欄に3.4.1項で取得した証明書の固有値を入力

```
X509:<SKI>1433506CD38FA413DF86BC27B8C650949E247ADC
```

※<SKI>の後に 証明書の[サブジェクト キー識別子] を入力
※入力値は Entra CBA の仕様に準じた形式で入力してください。
※証明書ユーザIDは最大10個登録可能

- [保存] をクリック

- [保存] をクリックしてプロパティを保存

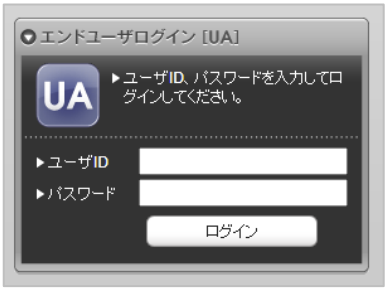
4. クライアントの設定

4.1. クライアント証明書をインポート

Edgeブラウザから UAにアクセスします。

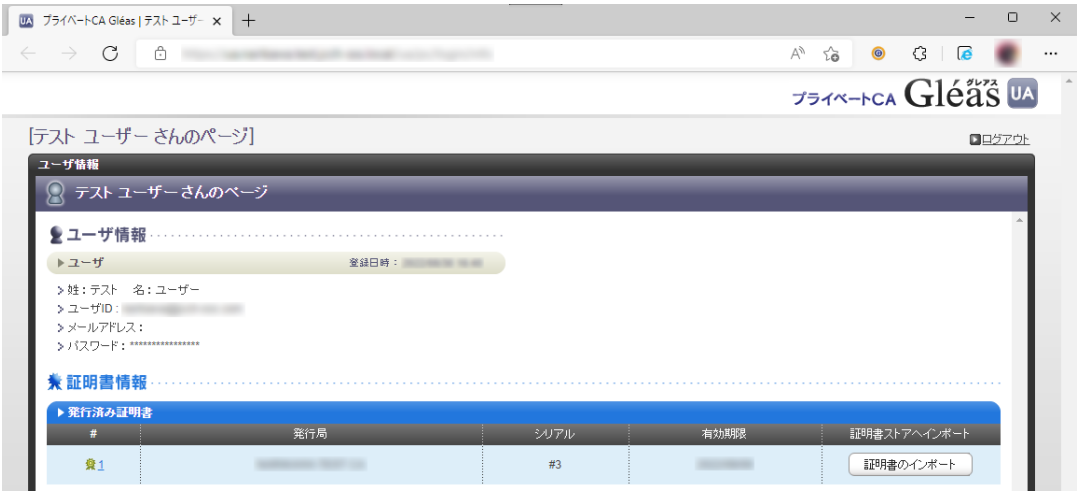
※URL https://[UAのFQDN]/[UAの名前]/ua

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。

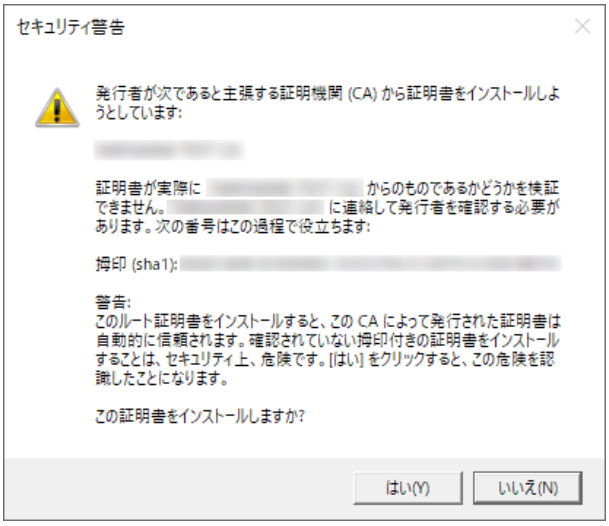


ログインすると、ユーザ専用ページが表示されます。

[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。



※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



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行うことはできません。

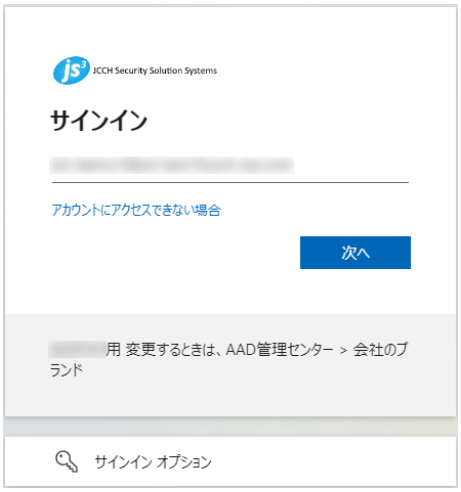
4.2. 証明書ベース認証

Edgeブラウザから マイ アプリ ポータル にサインインを試みます

※https://myapps.microsoft.com/

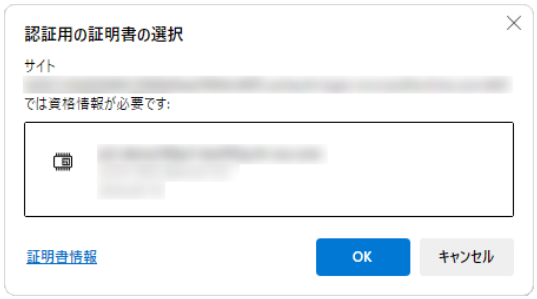
Entra ID のサインイン画面に遷移します。

ユーザー名を入力して次へをクリックします。

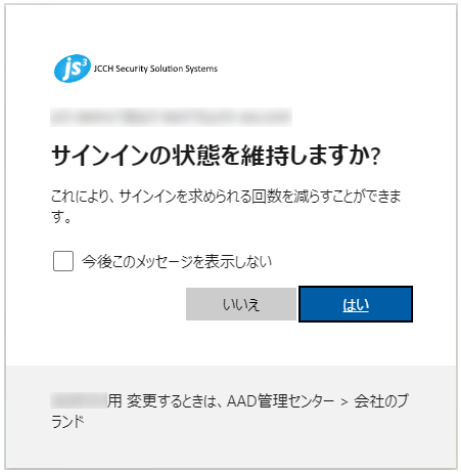


[証明書またはスマートカードを使用する]をクリックします。

クライアント証明書を選択して[OK]ボタンをクリックします。



[はい]または[いいえ]をクリックすると、サインインできます。

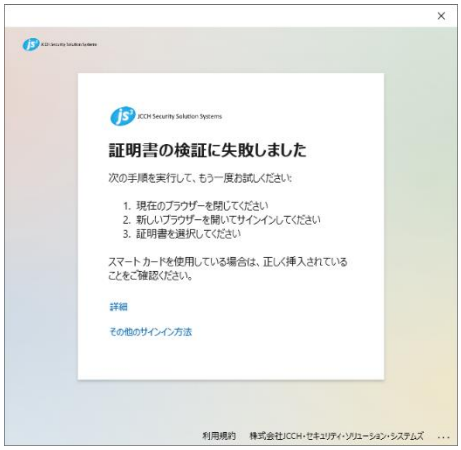


証明書を持っていない場合、

失効済み証明書を提示した場合、

Entra ID側の証明書ユーザーID情報と合致しない証明書を提示した場合

に認証は失敗します。



5. その他

5.1. 証明書ユーザーID を用いた認証制御について

高アフィニティな設定で証明書ベース認証を構成した場合、デバイスから提示された証明書とEntra IDの証明書ユーザーID (CertificateUserIDs) の合致をもって認証が行われます。

この仕組みにより特定証明書に対する認証可否をEntra ID 側から制御可能となります。例えば、デバイスを紛失したなどの理由で即時の認証停止が必要な場合、Entra ID のから証明書ユーザーID (CertificateUserIDs) か削除することで証明書認証を禁止することができます。

以下は証明書認証の制御を PowerShell で行うコマンド例です

- PowerShell を起動

※以降の操作の前に Microsoft Entra モジュールのインストールが必要です。

```
Install-Module Microsoft.Entra -AllowClobber
```

- 証明書ユーザーID を追加して認可

```
# Entra ID に接続
Connect-Entra -Scopes User.ReadWrite.All

# 証明書ファイルから証明書ユーザ ID を取得（*は証明書ファイルのパス名）
$targetCertPath = '**********'
$certUserId = (Get-EntraUserCertificateUserIdsFromCertificate -Path $targetCertPath).SKI

# 現在の Entra ID ユーザー情報を取得（*はプリンシパル名）
$targetUserId = '**********'
$user = Get-EntraUserCBAAuthorizationInfo -UserId $targetUserId

# 新しい認可情報を作成
$newAuthorizationInfo = @{ certificateUserIds = @()}
foreach ($item in  $user.AuthorizationInfo.CertificateUserIds) {
  $newAuthorizationInfo.certificateUserIds += $item.OriginalString
}
$newAuthorizationInfo.certificateUserIds +=$certUserId

#証明書ユーザ ID を更新
$uri = "https://graph.microsoft.com/v1.0/users/${targetUserId}/?$select=authorizationinfo"
$headers = @{'ConsistencyLevel' = 'eventual' }
$params = @{ authorizationInfo = $newAuthorizationInfo }
Invoke-MGGraphRequest -Method patch -Uri $uri -OutputType PSObject -Headers $headers -Body $params

# Entra ID から切断
Disconnect-Entra
```

※この操作以降、指定された証明書での認可されます

- **証明書ユーザーID を削除して認認可拒否**

```
# Entra ID に接続
Connect-Entra -Scopes User.ReadWrite.All

# 証明書ファイルから証明書ユーザ ID を取得（*は証明書ファイルのパス名）
$targetCertPath = '**********'
$certUserId = (Get-EntraUserCertificateUserIdsFromCertificate -Path $targetCertPath).SKI

# 現在の Entra ID ユーザー情報を取得（*はプリンシパル名）
$targetUserId = '**********'
$user = Get-EntraUserCBAAuthorizationInfo -UserId $targetUserId

# 新しい認可情報を作成
$newAuthorizationInfo = @{ certificateUserIds = @()}
foreach ($item in  $user.AuthorizationInfo.CertificateUserIds | Where-Object {$_.OriginalString -ne $certUserId }) {
  $newAuthorizationInfo.certificateUserIds += $item.OriginalString
}

#証明書ユーザ ID を更新
$uri = "https://graph.microsoft.com/v1.0/users/${targetUserId}/?$select=authorizationinfo"
$headers = @{'ConsistencyLevel' = 'eventual' }
$params = @{ authorizationInfo = @{ certificateUserIds = $newCertUserIds }}
Invoke-MGGraphRequest -Method patch -Uri $uri -OutputType PSObject -Headers $headers -Body $params

# Entra ID から切断
Disconnect-Entra
```

※この操作以降、指定された証明書では認可拒否されます

5.2. 証明書ユーザ ID の取得について

弊社では、Gléas から発行済み証明書の情報を Entra ID の証明書ユーザ ID 形式で CSV エクスポートする機能も提供可能です。

また、CSV をアップロードして EntraID の証明書ユーザ ID を更新する PowerShell サンプルコードなども提供可能ですのでご検討の際にはご相談ください。

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