



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

Azure AD 証明書ベース認証を使用したシングルサインオン

Ver.1.0

2023年8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
Azure AD 証明書ベース認証を使用したシングルサインオン

目次

1. はじめに	6
1.1. 本書について	6
1.2. 本書における環境	7
1.3. 本書における構成	9
2. Web サーバの設定	10
2.1. Web サーバの設計	10
2.2. サーバ証明書の登録	11
2.3. SAML SP 証明書の登録	14
2.4. SAML SP メタデータの登録	17
2.5. ヴァーチャルホスト設定	18
3. AzureAD の設定	19
3.1. セキュリティグループの作成	19
3.2. 証明機関を構成	21
3.3. 証明書ベース認証の有効化	23
3.4. 認証バインドポリシーを構成	25
3.5. ユーザー名バインドポリシーを構成	27

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

3.6.	エンタープライズ アプリケーションの登録.....	29
3.7.	エンタープライズ アプリケーションの割り当て.....	38
4.	Web サーバ起動	39
4.1.	SAML IdP メタデータを Web サーバに登録	39
4.2.	Web サーバ起動	39
5.	AP サーバの設定	40
5.1.	アプリケーションの設計.....	40
5.2.	アプリケーションを実装.....	41
5.3.	AP サーバ起動.....	41
6.	Gléas の設定	42
6.1.	証明書テンプレートの設定	42
6.2.	アカウント作成と証明書発行	43
6.3.	証明書の配布設定 (Windows 向け)	46
6.4.	証明書の配布設定 (iPhone 向け)	48
6.5.	証明書の配布設定 (Android 向け)	51
7.	クライアントの設定.....	53
7.1.	Windows にクライアント証明書をインポート	53

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

7.2.	iPhone にクライアント証明書をインポート	55
7.3.	Android にクライアント証明書をインポート	58
8.	証明書ベース認証によるアプリケーション利用	61
8.1.	Windows デバイスでアクセス	61
8.2.	iPhone デバイスでアクセス	65
8.3.	Android デバイスでアクセス	68
9.	その他	71
9.1.	認証ユーザ情報をアプリケーションに伝播	71
9.2.	多要素証明書認証について	72
9.3.	失効確認について	73
9.4.	即時失効について	74
9.5.	サインインのログについて	75
9.6.	失効リストのサイズ制限について	76
10.	問い合わせ	77

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、Azure Active Directory の証明書ベース認証 (CBA)をおこないアプリケーションにアクセスする構成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利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 Azure Active Directory
 - ※以後「Azure AD」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 2.6.0)
 - ※以後「Gléas」と記載します
- Webサーバ : AlmaLinux8.7 / Apache 2.4.37
 - (mod_ssl / mod_auth_mellon / mod_proxy / mod_headers)
 - ※以後「Webサーバ」と記載します
- アプリケーションサーバ : AlmaLinux8.7 / Node.js v10.24.0
 - ※以後「APサーバ」と記載します
- クライアント : Windows 10 Pro (22H2) / Microsoft Edge 115.0.1901.203
 - ※以後「Windows」と記載します
- クライアント : iPhone 14 (iOS 16.3) / Safari 16.3
 - ※以後「iPhone」と記載します
- クライアント : Google Pixel 7 Android13 / Chrome 115.0.5790.139
 - ※以後「Android」と記載します

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

以下については、本書では説明を割愛します。

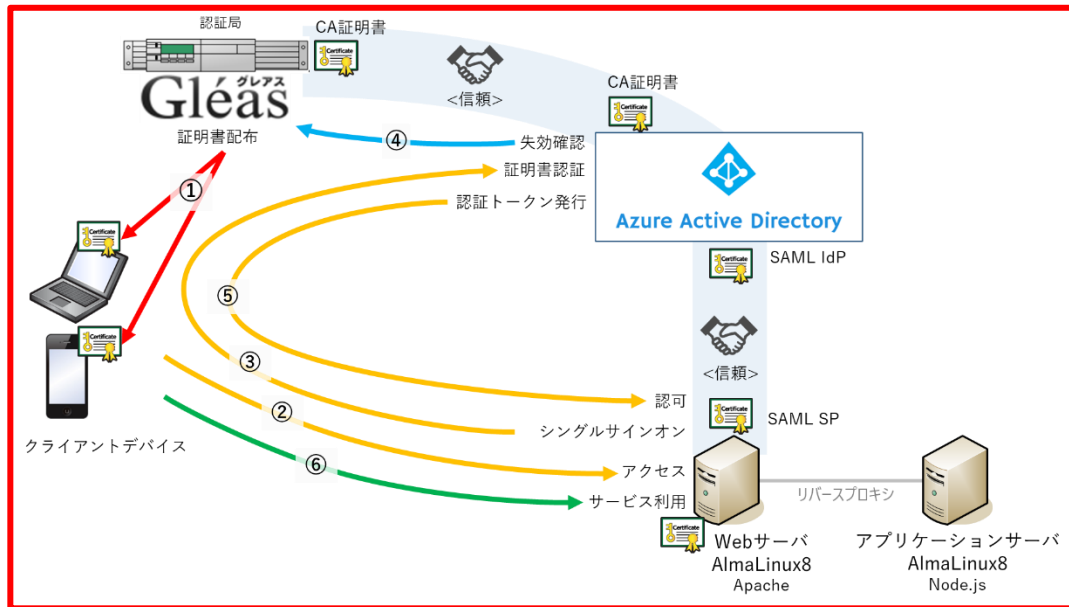
- Azure ADの基本設定
- Webサーバの基本設定（ネットワークや Apache の基本的な公開設定）
- APサーバの基本設定（ネットワークや Node.js の基本設定）
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作

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、Web サーバにサーバ証明書および SAML SP 証明書、クライアントデバイスにはクライアント証明書を発行する。
2. AzureAD 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. AzureAD に、SAML SP として Web サーバを登録する。
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. PC では Edge ブラウザ、iPhone では Safari ブラウザ、Android では Chrome ブラウザより Web サーバに HTTPS アクセスする。②
6. Web サーバは、Azure AD にシングルサインオン。③
7. Azure AD は、クライアント証明書認証を行う。③、④
証明書を提示しない、期限切れ、または失効している、端末はクライアント証明書認証に失敗。成功すると認証トークンを発行する。
8. 認証トークンを受け取った Web サーバは、アプリケーションの利用を許可（認可）。⑤
9. Web サーバは、アプリケーションにリバースプロキシしてサービス利用可能となる。⑥

2. Web サーバの設定

SAML SPとして動作するWebサーバを設定します。

※本手順では、サーバで事前にApacheがインストールされていることが前提です。

※Apacheは mod_ssl, mod_auth_mellon, mod_proxy, mod_headers モジュールを有効化します。

2.1. Web サーバの設計

アプリケーションの公開するための Web サーバの構成を決定します。

アプリケーション名	デモアプリ
アプリケーションのURLパス	/demo_app
サーバFQDN	sp.jcch-sss.com
プロキシURL	http://app-server:3000/demo_app/
サーバ証明書のパス	/etc/httpd/conf/server.crt
サーバ秘密鍵のパス	/etc/httpd/conf/server.key
SAML SP証明書のパス	/etc/httpd/conf/demo_app.crt
SAML SP秘密鍵のパス	/etc/httpd/conf/demo_app.key
SAML SP の EntityID	https://sp.jcch-sss.com/demo_app
SAML 名前ID形式	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Assertion Consumer ServiceのURLパス	/saml/demo_app/postResponse
Single Logout ServiceのURLパス	/saml/demo_app/logout
SAML SPメタデータのパス	/etc/httpd/conf/sp-metadata.xml
SAML IdPメタデータのパス	/etc/httpd/conf/idp-metadata.xml
アクセスログのパス	/etc/httpd/logs/demo_app-access_log
エラーログのパス	/etc/httpd/logs/demo_app-error_log
アプリケーションのサインオンURL	https://sp.jcch-sss.com/demo_app/
認証ユーザをあらわすリクエストヘッダ	x-auth-user: "ユーザプリンシパル名"
マイアプリへのリダイレクトURL	https://sp.jcch-sss.com/myapps

プライベート認証局 Gleás ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

2.2. サーバ証明書の登録

Web サーバに適用するサーバ証明書を発行します。

※本手順では、Gleásで事前にサーバアカウントを作成してあることが前提です。

※アカウント名、ホスト名は、2.1 項の [サーバFQDN] を入力

Gleás RA (登録局) にログインし、該当のサーバアカウントのページへ移動します。



プライベート認証局 Gléas ホワイトペーパー

Azure AD 証明書ベース認証を使用したシングルサインオン

小メニューの[証明書発行]をクリックし、アカウントに対し証明書を発行します。

証明書発行

この画面では証明書要求の作成を行います。
左側の「サブジェクト」と「属性」の内容で証明書要求を作成します。
右側のテンプレートの中から必要なものを選択して「発行」を押してください。

発行

サブジェクト

- CN=
- DC=

属性

- 発行局:
- 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サーバ証明、SSLクライアント証明
- 別名(DNS):

選択されているテンプレート

- 必須 デフォルト設定
- 必須 SSLサーバ証明書

選択可能なテンプレート

- なし

証明書詳細画面から[ダウンロード]をクリックし証明書をダウンロードします。

証明書情報

開始日: 終了日:

説明: 最終更新: 編集

サブジェクト

- 一般名:
- ドメインコンポーネント:
- ドメインコンポーネント:

基本情報

- 作成日:
- 有効日数: 366
- 失効日:
- 失効理由:
- 期限終了日:
- 状態: 有効な証明書
- 処理の状態: 有効な証明書
- トークン必要:
- バージョン: 4

証明書情報

- 認証局:
- 暗号アルゴリズム: rsa
- ダイジェストアルゴリズム: sha256
- 鍵長: 2048
- 鍵用途: 電子署名、鍵の暗号化
- 拡張鍵用途: SSLサーバ証明、SSLクライアント証明
- 別名: DNS名

証明書ファイル

- 証明書要求: あり
- 作成日時:
- 証明書: あり
- 作成日時:
- 秘密鍵: あり
- 作成日時:

テンプレート情報

テンプレート情報

デフォルト設定 SSLサーバ証明書

※ダウンロード時に証明書、秘密鍵を取り出す際のパスフレーズを指定します。

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

Gléasからダウンロードしたサーバ証明書 (.p12ファイル) をWebサーバにアップロード
します。

.p12ファイルからPEM形式の証明書を取り出して配置します。

※OpenSSLで行なう例 (パスワードの入力が必要となります)

```
openssl pkcs12 -in [.p12 ファイル] -nokeys -clcerts | openssl x509 -out /etc/httpd/conf/server.crt  
chmod 644 /etc/httpd/conf/server.crt
```

.p12ファイルからPEM形式の秘密鍵を取り出して配置します。

※OpenSSLで行なう例 (パスワードの入力が必要となります)

```
openssl pkcs12 -in [.p12 ファイル] -nodes -nocerts | openssl rsa -out /etc/httpd/conf/server.key  
chmod 400 /etc/httpd/conf/server.key
```

2.3. SAML SP 証明書の登録

SAML SPとして使用する署名用証明書をGléasから発行します。

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]からアカウントを作成します。

※アカウント名は、2.1 項の [アプリケーションのURLパス] に準じたものを入力

新規アカウント作成

アカウント情報の入力

このページではアカウントの新規作成を行います。
アカウントは証明書を発行する対象(エンドエンティティ)のことで、このページで指定したアカウント名が証明書の発行先となります。
★の付いている項目は入力必須項目です。

アカウント情報

アカウント名 *

名前(姓) *

名前(名) *

メールアドレス

パスワード

パスワード(確認)

パスワード(自動生成)

プリンシパル名

[上級者向け設定](#)

小メニューの[証明書発行]をクリックし、アカウントに対し証明書を発行します。

証明書発行

この画面では証明書要求の作成を行います。
左側の「サブジェクト」と「属性」の内容で証明書要求を作成します。
右側のテンプレートの中から必要なものを選択して「発行」を押してください。

証明書発行

下記の内容で証明書を発行します。よろしければ「発行」を押してください。

サブジェクト

CN=

O=

DC=

属性

発行局:

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

Netscape 拡張: 有効

CRL 配布点:

選択されているテンプレート

必須 デフォルト設定

必須 区分CRL

選択可能なテンプレート

なし

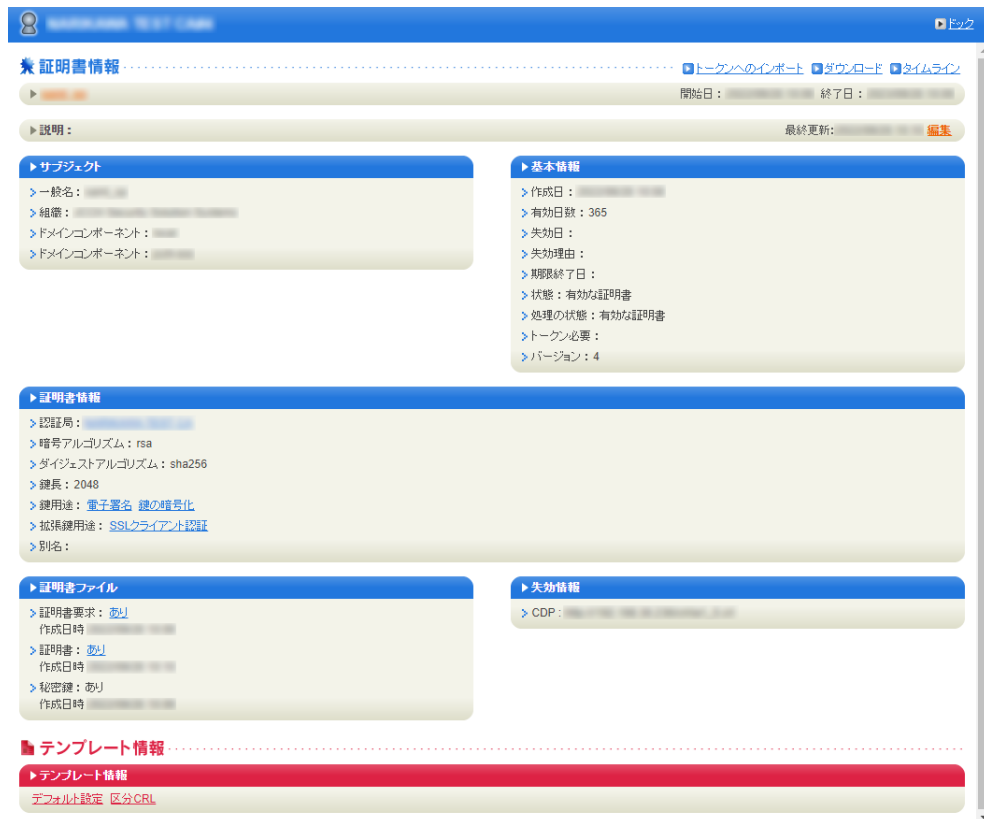
[上級者向け設定](#)

[詳細に戻る](#)

[全て解除](#)

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

証明書詳細画面から[ダウンロード]をクリックし証明書をダウンロードします。



※ダウンロード時に証明書、秘密鍵を取り出す際のパスフレーズを指定します。

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

GléasからダウンロードしたSP証明書 (.p12ファイル) をWebサーバにアップロードします。

.p12ファイルからPEM形式の証明書を取り出して配置します。

※OpenSSLで行なう例 (パスワードの入力が必要となります)

```
openssl pkcs12 -in [p12 ファイル] -nokeys -clcerts | openssl x509 -out /etc/httpd/conf/demo_app.crt  
chmod 644 /etc/httpd/conf/demo_app.crt
```

.p12ファイルからPEM形式の秘密鍵を取り出して配置します。

※OpenSSLで行なう例 (パスワードの入力が必要となります)

```
openssl pkcs12 -in [p12 ファイル] -nodes -nocerts | openssl rsa -out /etc/httpd/conf/demo_app.key  
chmod 400 /etc/httpd/conf/demo_app.key
```


2.4. SAML SP メタデータの登録

SAML SP を定義するためのメタデータ (.xmlファイル) を作成します。

※2.1 項の設計に準じた SAML SP メタデータの作成コマンド実行例

```
OUTFILE=/etc/httpd/conf/sp-metadata.xml
APP=demo_app
FQDN=sp.jcch-sss.com
ENTITYID=https://sp.jcch-sss.com/$APP
SP_ENDPOINT=/saml/$APP
SP_CERT=/etc/httpd/conf/$APP.crt
X509=`openssl x509 -in $SP_CERT | grep -v '^-----'`

cat << EOS > $OUTFILE
<EntityDescriptor entityID="$ENTITYID"
  xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
    AuthnRequestsSigned="true">
    <KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>$X509</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>$X509</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://$FQDN$SP_ENDPOINT/logout"/>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    </NameIDFormat>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://$FQDN$SP_ENDPOINT/postResponse"
      index="0"/>
  </SPSSODescriptor>
</EntityDescriptor>
EOS

chmod 644 $OUTFILE
```

作成された SAML SP メタデータダウンロードします。

※上記の例では /etc/httpd/conf/sp-metadata.xml

2.5. ヴァーチャルホスト設定

アプリケーションを公開するためのヴァーチャルホストを設定します。

※2.1 項の設計に準じたヴァーチャルホスト設定の作成コマンド実行例

```
OUTFILE=/etc/httpd/conf.d/vhost-demo_app.conf
FQDN=sp.jcch-sss.com
APP=demo_app
SERVER_CERT=/etc/httpd/conf/server.crt
SERVER_PKEY=/etc/httpd/conf/server.key
SERVER_CHAIN=/etc/httpd/conf/server-chain.crt
IdP_METADATA=/etc/httpd/conf/idp-metadata.xml
SP_METADATA=/etc/httpd/conf/sp-metadata.xml
SP_CERT=/etc/httpd/conf/$APP.crt
SP_PKEY=/etc/httpd/conf/$APP.key
SP_ENDPOINT=/saml/$APP
PROXYBASE=http://app-server:3000

cat << EOS > $OUTFILE
<VirtualHost *:443>
    ServerName $FQDN
    CustomLog logs/$APP-access_log combined
    ErrorLog logs/$APP-error_log

    SSLEngine on
    SSLCertificateFile      $SERVER_CERT
    SSLCertificateKeyFile  $SERVER_PKEY
    #SSLCertificateChainFile $SERVER_CHAIN

    <Location />
        MellonEnable      info
        MellonEndpointPath $SP_ENDPOINT
        MellonSPPrivateKeyFile $SP_PKEY
        MellonSPCertFile   $SP_CERT
        MellonSPMetadataFile $SP_METADATA
        MellonIdPMetadataFile $IdP_METADATA
    </Location>
    <Location /$APP>
        AuthType      Mellon
        Require        valid-user
        MellonEnable  auth
        RequestHeader set X-AUTH-USER %{MELLON_NAME_ID}e env=MELLON_NAME_ID
        RequestHeader set X-Forwarded-Proto https
        RequestHeader set X-Forwarded-Port 443
    </Location>

    ProxyPreserveHost On
    ProxyPass          /$APP $PROXYBASE/$APP
    ProxyPassReverse  /$APP $PROXYBASE/$APP

    Redirect /myapps https://myapps.microsoft.com/
</VirtualHost>
EOS

chmod 644 $OUTFILE
```

3. AzureAD の設定

3.1. セキュリティグループの作成

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。

Azure Active Directory 管理センター にログインします。

メニュー [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) "AzureAD CBA グループ"
- [グループの説明] に任意の説明を入力
※例) " AzureAD 証明書ベース認証連携に使用"
- [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を選択
- [作成] をクリック

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

[ホーム](#) > [JCCHセキュリティソリューションシステムズ | グループ](#) > [グループ | すべてのグループ](#) >

新しいグループ ...

 フィードバックがある場合

グループの種類 * ⓘ
セキュリティ

グループ名 * ⓘ
AzureAD CBA グループ

グループの説明 ⓘ
AzureAD 証明書ベース認証連携に使用

メンバーシップの種類 * ⓘ
割り当て済み

所有者
1 人の所有者が選択されました

メンバー
2 メンバーが選択されました

[作成](#)

3.2. 証明機関を構成

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`

Azure Active Directory 管理センター にログインします。

メニュー [セキュリティ] > [証明機関] を選択します。

[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

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

証明書ファイルのアップロード ×

証明機関の証明書を含む .cer ファイルをインポートします。発行者、中間、およびルート証明機関の証明書が必要です。
[詳細](#)

証明書 *

ルート CA 証明書である ^①

はい
 いいえ

証明書失効リストの URL ^①

デルタ証明書失効リストの URL ^①

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所属する Azure AD ユーザに対して証明書ベース認証を有効化します。

Azure Active Directory 管理センター にログインします。

メニュー [セキュリティ] > [認証方法] を選択します。

[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
- 確認メッセージが表示されたら [確認しました] をクリック
- [保存] をクリック

プライベート認証局 Gléas ホワイトペーパー

Azure AD 証明書ベース認証を使用したシングルサインオン

ホーム > JCHセキュリティソリューションシステムズ | セキュリティ > セキュリティ | 認証方法 > 認証方法 | ポリシー >

証明書ベースの認証 の設定

証明書ベースの認証は、認証に x.509 証明書とエンタープライズ公開キー基盤 (PKI) を使用するパスワードレスでファイナングに強い認証方法です。 [詳細情報](#)。

有効化およびターゲット 構成

有効にする

含める 除外

ターゲット すべてのユーザー グループの選択

グループの追加

名前	種類	登録
AzureAD CBA グループ	グループ	省略可能

保存 破棄

3.4. 認証バインドポリシーを構成

証明書ベース認証の認証強度を設定する認証バインドポリシーを構成します。

Azure Active Directory 管理センター にログインします。

メニュー [セキュリティ] > [認証方法] を選択します。

[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。

- [認証バインド] の [保護レベル] に [単一要素認証] を選択

※多要素認証を選択すると、証明書による単一要素認証を多要素認証とみなすことができます。
詳しくは 9.1 項を参照

- [認証バインド] の [保護レベル] の [規則の追加] をクリック

- [ルールの編集] で [証明書の発行者] を選択

- [証明書の発行者識別子] に先に登録した証明機関を選択

- [保護レベル] に [単一要素認証] を選択

[保存] をクリック

- 確認メッセージが表示されたら [確認しました] をクリック

- [保存] をクリック

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

ルールの編集

ルールの編集

- 証明書の発行者
- ポリシー OID

注: 特別な規則により、証明書が指定された保護レベルにバインドされます。

証明書の発行者識別子 * ⓘ

O="JCCH Security Solution Systems Co., Ltd.", DC=com, DC=j... ▼

保護レベル ⓘ

- 単一要素認証
- 多要素認証

保存

破棄

3.5. ユーザー名バインドポリシーを構成

証明書ベース認証でクライアント証明書と AzureAD ユーザを紐づけるためにユーザー名バインドポリシーを構成します。

Azure Active Directory 管理センター にログインします。

メニュー [セキュリティ] > [認証方法] を選択します。

[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] の [証明書フィールド] を以下のように設定

優先順位	証明書フィールド	ユーザー属性
1	PrincipalName	userPrincipalname
2	RFC822Name	指定なし
3	SubjectKeyIdentifier	指定なし
4	SHA1PublicKey	指定なし

※証明書の別名(UPN) を Azure AD ユーザの UserPrincipalName 属性と突合して認証します。

- [保存] をクリック
- 確認メッセージが表示されたら [確認しました] をクリック
- [保存] をクリック

プライベート認証局 Gléas ホワイトペーパー

Azure AD 証明書ベース認証を使用したシングルサインオン

ホーム > JCCHセキュリティソリューションシステムズ | セキュリティ > セキュリティ | 認証方法 > 認証方法 | ポリシー >

証明書ベースの認証 の設定

証明書ベースの認証は、認証に x.509 証明書とエンタープライズ公開キー基盤 (PKI) を使用するパスワードレスでファイシングに強い認証方法です。[詳細情報](#)。

有効化およびターゲット **構成**

認証バインド

すべての証明書バインドの既定の保護レベルを選択します。既定値をオーバーライドするには、特別な規則を作成します。

保護レベル 単一要素認証 多要素認証

[規則の追加](#)

ルールの種類	識別子	保護レベル
証明書の発行者。	O="JCCH Security Solution Systems Co., Ltd...	単一要素認証

ユーザー名バインド

バインドを作成するユーザー属性を選択します。最初の証明書フィールドは、ユーザー名バインドの優先順位が最も高くなっています。

証明書フィールド	ユーザー属性
1 PrincipalName	userPrincipalName
2 RFC822Name	ユーザー属性の選択
3 SubjectKeyIdentifier	ユーザー属性の選択
4 SHA1PublicKey	ユーザー属性の選択

⚠ 証明書ベースの認証 (CBA) が有効になっているユーザーには有効な証明書があることを確認してください。CBA は多要素認証 (MFA) に対応しているため、有効な証明書がない場合、ユーザーは、CBA を 2 番目の要素として使用することや、MFA に他の方法を登録することができなくなります。[詳細情報](#)

[確認しました](#)

[保存](#) [破棄](#)

3.6. エンタープライズ アプリケーションの登録

Web サーバを Azure のエンタープライズ アプリケーションとして登録します。

Azure Active Directory 管理センター にログインします。

メニュー [エンタープライズ アプリケーション] > [すべてのアプリケーション] を選択
します。

[新しいアプリケーション] をクリックします。

Azure AD ギャラリーの参照で[独自のアプリケーションの作成] をクリックします。

- [お使いのアプリの名前は何か?] に任意の名前を入力
※ここでは 2.1 項の [アプリケーション名] を入力
- [アプリケーションでどのような操作を行いたいですか?] に [ギャラリーに見つ
からないその他のアプリケーションを統合します (ギャラリー以外)] を選択
- [作成] をクリック

独自のアプリケーションの作成

フィードバックがある場合

独自のアプリケーションを開発している場合、アプリケーション プロキシを使用している場合、またはギャラリーにないアプリケーションを統合する必要がある場合は、ここで独自のアプリケーションを作成できます。

お使いのアプリの名前は何か?

アプリケーションでどのような操作を行いたいですか?

オンプレミスのアプリケーションへのセキュリティで保護されたリモート アクセス用のアプリケーション プロキシを構成します

アプリケーションを登録して Azure AD と統合します (開発中のアプリ)

ギャラリーに見つからないその他のアプリケーションを統合します (ギャラリー以外)

作成

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

アプリケーションの概要画面に遷移します。

The screenshot shows the Azure AD application overview page for 'デモアプリ' (Demo App). The page is divided into several sections:

- 概要 (Overview):** This section is currently selected in the left-hand navigation menu. It includes a 'プロパティ' (Properties) card with fields for '名前' (Name), 'アプリケーション ID' (Application ID), and 'オブジェクト ID' (Object ID).
- Getting Started:** This section contains five numbered steps to get the application up and running:
 - 1. ユーザーとグループの割り当て:** Assign specific users or groups to the application for access.
 - 2. シングルサインオンの設定:** Configure single sign-on using the user's own Azure AD credentials.
 - 3. ユーザーアカウントのプロビジョニング:** Provision user accounts for the application automatically.
 - 4. 条件付きアクセス:** Create conditional access policies for secure access to the application.
 - 5. セルフサービス:** Enable self-service so users can request access based on their Azure AD profile.
- What's New:** This section contains three announcements:
 - Sign in charts have moved!** The new Insights view shows sign-in info along with other useful application data.
 - Delete Application has moved to Properties** You can now delete your application from the Properties page.
 - Getting started has moved to Overview** The Getting Started page has been replaced by the steps above.

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

[シングルサインオンの設定] の [作業の開始] をクリックします。

- [シングル サインオン方式の選択] で [SAML] をクリック

シングル サインオン方式の選択 [判断に役立つヘルプの表示](#)

 無効 シングルサインオンが有効になっていません。ユーザーは、[マイ アプリ] からアプリを起動できません。	 SAML SAML (Security Assertion Markup Language) プロトコルを使用した、アプリケーションに対する多機能かつセキュリティで保護された認証。
 パスワードベース Web ブラウザーの拡張機能またはモバイルアプリを使用したパスワードの保存と再生。	 リンク マイ アプリや Office 365 アプリケーション起動プログラム内のアプリケーションへのリンク。

SAML によるシングル サインオンのセットアップに遷移します。

[↑](#) メタデータ ファイルをアップロードする [↶](#) シングル サインオン モードの変更 [☰](#) このアプリケーションを Test | ...

SAML によるシングル サインオンのセットアップ

フェデレーション プロトコルに基づく SSO 実装により、セキュリティ、信頼性、エンド ユーザー エクスペリエンスが向上し、実装が容易になります。OpenID Connect または OAuth が使用されていない既存のアプリケーションの場合は、できるだけ SAML シングル サインオンを選択してください。[詳細については、こちらをご覧ください。](#)

以下をお読みください [構成ガイド](#) [☑](#) デモアプリ を統合するためのヘルプ。

1 基本的な SAML 構成 [編集](#)

識別子 (エンティティ ID)	必須
応答 URL (Assertion Consumer Service URL)	必須
サインオン URL	省略可能
リレー状態 (省略可能)	省略可能
ログアウト URL (省略可能)	省略可能

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

[メタデータファイルをアップロードする] をクリックします。

- 2.5 項でダウンロードした SAML SP メタデータを選択

※2.1 項の [SAML SP メタデータのパス] のファイル名を入力

- [追加] をクリック

↑ メタデータファイルをアップロードする シングルサインオンモードの変更 ☰ このアプリケーションをTest | ...

メタデータ ファイルをアップロードします。
以下のフィールドの値は デモアプリによって提供されます。値を手動で入力することもできますし、構成済みの SAML メタデータ ファイルが デモアプリ によって提供されている場合にはそれをアップロードすることもできます。

"sp-metadata.xml"

追加 キャンセル

基本的な SAML 構成 編集

識別子 (エンティティ ID)	必須
応答 URL (Assertion Consumer Service URL)	必須
サインオン URL	省略可能
リレー状態 (省略可能)	省略可能
ログアウト URL (省略可能)	省略可能

- [識別子 (エンティティ ID)] が入力されていることを確認
- [応答 URL (Assertion Consumer Service URL)] が入力されていることを確認
- [サインオン URL (省略可能)] にアプリケーションのサインオン URL を入力
※2.1 項の [アプリケーションのサインオン URL] を入力
- [リレー状態 (省略可能)] は入力されていないことを確認
- [ログアウト URL (省略可能)] が入力されていることを確認
- [保存] をクリック

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

基本的な SAML 構成

保存 | フィードバックがある場合

識別子 (エンティティ ID) * ⓘ
Azure Active Directory に対してアプリケーションを識別する一意の ID。この値は、Azure Active Directory テナント内のすべてのアプリケーションで一意である必要があります。既定の識別子は、IDP で開始された SSO の SAML 応答の対象ユーザーになります。

既定

✓ ⓘ

[識別子の追加](#)

応答 URL (Assertion Consumer Service URL) * ⓘ
応答 URL は、アプリケーションが認証トークンを受け取る場所です。これは、SAML では "Assertion Consumer Service" (ACS) とも呼ばれます。

イン... 既定

✓ ✓ ⓘ

[応答 URL の追加](#)

サインオン URL (省略可能)
サービス プロバイダーによって開始されたシングル サインオンを実行する場合は、サインオン URL が使用されます。この値は、アプリケーションのサインオンページの URL です。ID プロバイダーによって開始されたシングル サインオンを実行する場合は、このフィールドは不要です。

✓

リレー状態 (省略可能) ⓘ
リレー状態は、認証が完了した後にユーザーのリダイレクト先となるアプリケーションを指示します。通常、値は、ユーザーをアプリケーション内の特定の場所に移動する URL または URL パスです。

ログアウト URL (省略可能)
この URL は、SAML ログアウト応答をアプリケーションに返送するために使用します。

✓

[X] をクリックして閉じます。

※エンタープライズ アプリケーションのシングルサインオンのテスト確認が表示されたら [いいえ] をクリックします。

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

[②属性とクレーム] の[編集]をクリックします。

- [必要な要求] の[一意のユーザー識別子(名前 ID)]の値をクリック
- [名前識別子の形式]に[電子メールアドレス]を選択
- [ソース] に [属性] を選択
- [ソース属性] に [user.userprincipalname] を選択
- [保存] をクリック



要求の管理 ...

保存 変更の破棄 | フィードバックがある場合

名前 nameidentifier

名前空間 http://schemas.xmlsoap.org/ws/2005/05/id...

名前識別子の形式の選択

名前識別子の形式 * 電子メールアドレス

ソース * 属性 変換
 ディレクトリスキーマ拡張 (プレビュー)

ソース属性 * user.userprincipalname

要求条件

SAML クレームの詳細オプション

[X] をクリックして閉じます。

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

- [追加の要求] に以下を設定

名前	名前空間	ソース	ソース属性
name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	属性	user.userprincipalname
surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	属性	user.surname
givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	属性	user.givenname
emailaddress	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	属性	user.mail

属性とクレーム ... ×

[+](#) 新しいクレームの追加 [+](#) グループ要求を追加する [☰](#) 列 | [🗨️](#) フィードバックがある場合

必要な要求

クレーム名	種類	値
一意のユーザー識別子 (名前 ID)	SAML	user.userprincipalnam... ***

追加の要求

クレーム名	種類	値
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ***

[▽](#) 詳細設定

[X] をクリックして閉じます。

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

[③SAML 証明書] の [トークン署名証明書]の[編集]をクリックします。

- [署名オプション] に [SAML 応答とアサーションへの署名]を選択
- [署名アルゴリズム] に [SHA-256] を選択
- [通知の電子メールアドレス] は未使用
- [保存] をクリック

SAML 署名証明書

アプリに対して発行される SAML トークンに署名するために Azure AD によって使用される証明書を管理します

保存 + 新しい証明書 ↑ 証明書のインポート | フィードバックがある場合

状態	有効期限	拇印
アクティブ		

署名オプション: SAML アサーションへの署名

署名アルゴリズム: SHA-256

通知の電子メール アドレス

[X] をクリックして閉じます。

- [アプリのフェデレーション メタデータ URL] をコピーして保存しておく

プライベート認証局 Gléas ホワイトペーパー

Azure AD 証明書ベース認証を使用したシングルサインオン

ホーム > エンタープライズ アプリケーション | すべてのアプリケーション > デモアプリ > デモアプリ | SAML ベースのサインオン

概要

デプロイ計画

問題の診断と解決

管理

プロバティ

所有者

ロールと管理者

ユーザーとグループ

シングルサインオン

プロビジョニング

アプリケーション プロキシ

セルフサービス

カスタム セキュリティ属性

セキュリティ

条件付きアクセス

アクセス許可

トークンの暗号化

アクティビティ

サインイン ログ

使用状況と分析情報

監査ログ

プロビジョニング ログ

アクセス レビュー

トラブルシューティング + サポート

新しいサポート リクエスト

SAML によるシングル サインオンのセットアップ

フェデレーション プロトコルに基づく SSO 実装により、セキュリティ、信頼性、エンドユーザー エクスペリエンスが向上し、実装が容易になります。OpenID Connect または OAuth が使用されていない既存のアプリケーションの場合は、できるだけ SAML シングル サインオンを選択してください。詳細については、こちらをご覧ください。

以下をお読みください [構成ガイド](#) デモアプリ を統合するためのヘルプ。

- 基本的な SAML 構成**

識別子 (エンティティ ID)	https://sp.jcch-sss.com/demo_app
応答 URL (Assertion Consumer Service URL)	https://sp.jcch-sss.com/saml/demo_app/postResponse
サインオン URL	https://sp.jcch-sss.com/demo_app/
リレー状態 (省略可能)	省略可能
ログアウト URL (省略可能)	https://sp.jcch-sss.com/saml/demo_app/logout
- 属性とクレーム**

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
一意のユーザー ID	user.userprincipalname
- SAML 証明書**

トークン署名証明書	アクティブ
状態	
拇印	
有効期限	
通知用メール	
アプリのフェデレーション メタデータ URL	https://login.microsoftonline.com/d2b7c5b8-3049...
証明書 (Base64)	ダウンロード
証明書 (未加工)	ダウンロード
フェデレーション メタデータ XML	ダウンロード

検証証明書 (オプション)	
必須	いいえ
アクティブ	0
有効期限切れ	0
- デモアプリ のセットアップ**

Azure AD とリンクするアプリケーションを構成する必要があります。

ログイン URL	https://login.microsoftonline.com/d2b7c5b8-3049...
Azure AD 識別子	https://sts.windows.net/d2b7c5b8-3049-41f5-88d...
ログアウト URL	https://login.microsoftonline.com/d2b7c5b8-3049...
- デモアプリ でシングル サインオンを Test**

シングル サインオンが機能していることを Test します。ユーザーがサインインするには、ユーザーをユーザー とグループに追加しておく必要があります。

[Test](#)

[X] をクリックして閉じます。

3.7. エンタープライズ アプリケーションの割り当て

登録したエンタープライズ アプリケーションをユーザーに割り当てて、利用できるようにします。

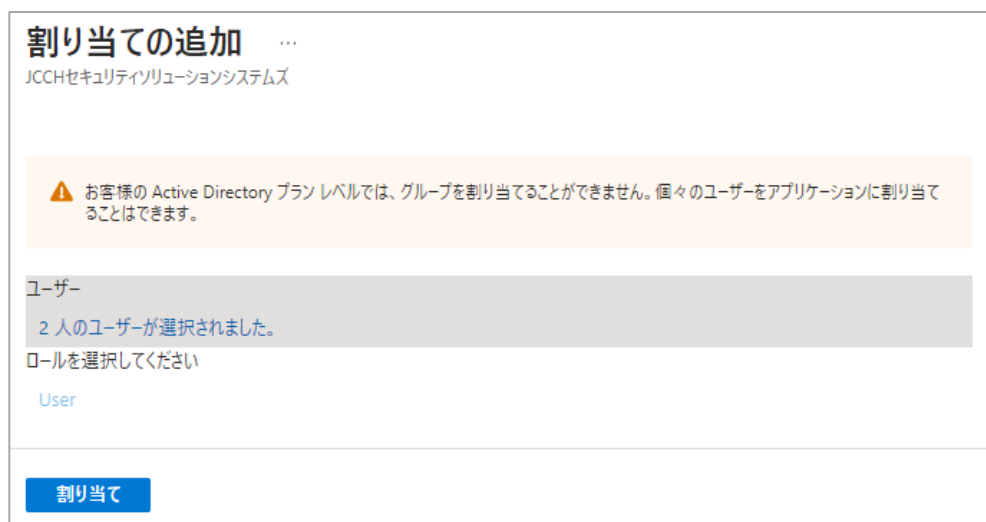
Azure Active Directory 管理センター にログインします。

メニュー [エンタープライズ アプリケーション] > [すべてのアプリケーション] を選択します。

登録したアプリケーションを選択して、アプリケーションの概要画面に遷移します。

[ユーザーとグループの割り当て] をクリックします

- [ユーザーまたはグループの追加] をクリック
- エンタープライズ アプリケーションを割り当てるユーザーを選択
- [割り当て]をクリック



4. Web サーバ起動

4.1. SAML IdP メタデータを Web サーバに登録

Webサーバで、Azure から SAML IdP メタデータをダウンロードします。

これはAzureからの認証メッセージが正しいことを検証できるようにする操作です。

※以下のコマンドで 2.1 項の [SAML IdPメタデータのパス] に配置

※IdPメタデータURL は3.6 項で取得した [アプリのフェデレーション メタデータ URL] を使用

```
curl -o /etc/httpd/conf/idp-metadata.xml [IdP メタデータ URL]
chmod 644 /etc/httpd/conf/idp-metadata.xml
```

4.2. Web サーバ起動

準備ができたならWeb サーバを起動します。

これによりWebサーバは SAML SP として動作します。

※以下のコマンドで Webサーバを起動

```
sudo systemctl start httpd
```

5. AP サーバの設定

APサーバを設定します。

※本手順では、サーバで事前に Node.js がインストールされていることが前提です。

5.1. アプリケーションの設計

検証用アプリケーションの構成を決めます。

Listen tcpポート番号	3000
ログインユーザ表示	認証済みAzureADユーザのユーザプリンシパル名を出力
ログアウトリンク表示	Single Logout Service へのリンクを出力 リンクを踏むとログアウト後、マイアプリポータルへリダイレクト
その他	HTTPリクエストヘッダを出力

5.2. アプリケーションを実装

アプリケーションを Node.js で実装します。

※以下のコマンドで 5.1 項の設計に準じたアプリケーションを実装

```
cat << 'EOS' > /usr/local/src/demo_app.js
"use strict";

const http = require("http");
const listen_port = 3000;
const slo_path = "/saml/demo_app/logout";
const return_to = "https://sp.jcch-sss.com/myapps";

const server = http.createServer((request, response) => {
  var headers = "";
  Object.keys(request.headers).forEach((key) => {
    headers = headers + `<li>${key}: ${request.headers[key]}</li>`n`
  });
  response.writeHead(200, {"Content-Type": "text/html; charset=UTF-8",
    "Cache-Control": "no-cache"});

  response.write(`
<html><body>`n`
<h1>Welcome! </h1>`n`
<h4>${request.headers["x-auth-user"]}</h4>`n`
<a href='${slo_path}?ReturnTo=${return_to}'>Logout</a>`n`
<h3>Request Header</h3>
<ul>`n`
  ${headers}`n`
</ul>`n`
</body></html>`n`
`);
  response.end();
});

server.listen(listen_port);

console.log(` The server has started and is listening on port : ${listen_port}`);
EOS

chmod 644 /usr/local/src/demo_app.js
```

5.3. AP サーバ起動

```
node /usr/local/src/demo_app.js
```

6. Gléas の設定

6.1. 証明書テンプレートの設定

Azure AD の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
別名 (プリンシパル名)	アカウント (プリンシパル名)

6.2. 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]メニューから[上級者向け設定] 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
- [アップロードする]にローカルの CSV ファイルを選択

※CSV ファイルは以下の形式

列名	値
cn	アカウント名 ※証明書のサブジェクト一般名となります ※UA のログインユーザ ID となります
sn	名前 (姓)
givenname	名前 (名)
password	パスワード ※UA のログインパスワードとなります
upn	プリンシパル名 ※証明書の別名 (UPN) となります ※AzureAD のユーザープリンシパル名と一致させてください

- [作成]をクリック

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

▶ アカウント情報 ▶ 上級者向け設定

▶ アカウント名 ★

▶ 初期グループ なし
 [ここをクリックしてユーザを参加させるグループを選択](#)

▶ その他の設定
 証明書を発行する
 連続して登録を行う

▶ 種類 ユーザ コンピュータ サーバ 認証局 CSVファイル一括登録 LDAP

▶ アップロードするファイル upload.csv

- 内容を確認し[実行]をクリック

+ インポート内容の確認

👤 指定したファイルの内容

指定されたファイルの最初の9件を表示しています。
 下部の「実行」ボタンを押すと、以下のファイルの内容がアカウント登録申請者一覧に反映されます。

▶ 指定されたファイルの最初の9件				
アカウント名	姓	名	メールアドレス	プリンシパル名
...
...
...
...
...
...
...
...
...

全 9件

▶ このファイルで間違いがなければ「実行」ボタンを押してください。

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

[アカウント]>[登録申請者一覧]メニューを選択します。

※しばらくするとアップロードしたユーザ情報がアカウント登録申請として登録されます

- [全て許可する] をクリック
- [実行] をクリック



CSV の内容が Gléas アカウントとしてインポートされます。

※しばらくするとアップロードしたアカウントに対してクライアント証明書が自動的に発行されます

6.3. 証明書の配布設定 (Windows 向け)

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。

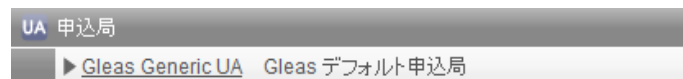
※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

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。

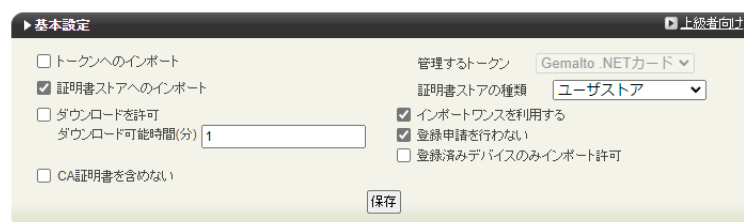
※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します



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。

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

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]

6.4. 証明書の配布設定 (iPhone 向け)

GléasのUA (申込局) より発行済み証明書を iOS にインポートできるように設定します。

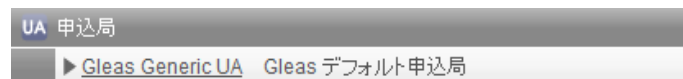
※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

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

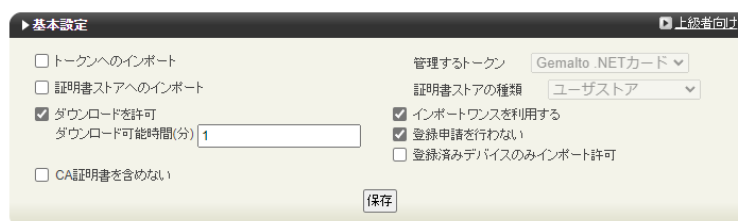


[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [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。

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン



設定完了後、[保存]をクリックし保存します。

[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な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

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

【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）



認証デバイス情報

▶ iPhone / iPad の設定

iPhone/iPad 用 UA を利用する

画面レイアウト

iPhone 用レイアウトを使用する ログインパスワードで証明書を保護

Mac OS X 10.7以降の接続を許可

OTA(Over-the-air)

OTAエンロールメントを利用する 接続する iOS デバイスを認証する

OTA用SCEP URL

OTA用認証局

デフォルトを利用

iPhone 構成プロファイル基本設定

名前(デバイス上に表示) サンプルプロファイル

識別子(例: com.jcch-sss.profile) local.jcch-sss.profile

プロファイルの組織名 JCCHセキュリティソリューション・システムズ

説明 サンプル構成プロファイル

各項目の入力が終わったら、[保存]をクリックします。

6.5. 証明書の配布設定 (Android 向け)

GléasのUA (申込局) より発行済み証明書を Android にインポートできるように設定します。

※ 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

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]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、証明書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証明書ファイルのインストールを制限することができます。

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

基本設定 上級者向け

トークンへのインポート

証明書ストアへのインポート

ダウンロードを許可
ダウンロード可能時間(分)

CA証明書を含まない

管理するトークン Gemalto .NETカード

証明書ストアの種類 ユーザストア

インポートワンスを利用する

登録申請を行わない

登録済みデバイスのみインポート許可

設定完了後、[保存]をクリックし保存します。

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

Android の設定

Android 用 UA を利用する

ダウンロードの動作

ログインパスワードで証明書を保護

数字のみの PIN を表示

証明書ダウンロードの種類 PKCS#12ダウンロード

証明書のダウンロードに必要な情報の入力画面が展開されるので、以下設定を行います。

- [数字のみのPINを表示]をチェック
- [証明書ダウンロードの種類]を[PKCS#12ダウンロード]を選択

各項目の入力が終わったら、[保存]をクリックします。

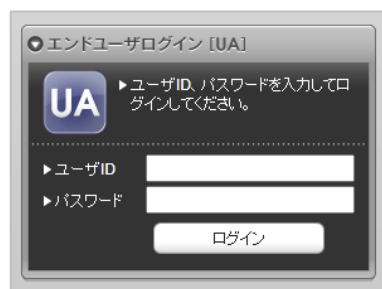
7. クライアントの設定

7.1. Windows にクライアント証明書をインポート

PCのブラウザ (Edge) で、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。



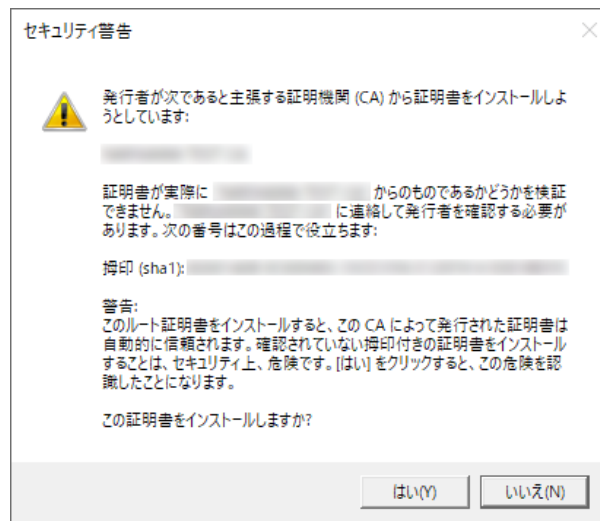
ログインすると、ユーザ専用ページが表示されます。

[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。



プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

※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。



7.2. iPhone にクライアント証明書をインポート

iPhoneのブラウザ (Safari) で、UAにアクセスします。

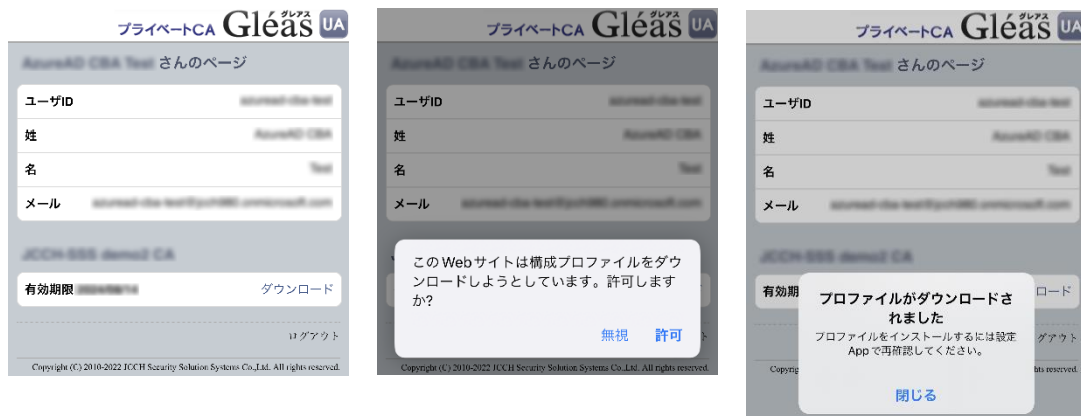
※URL `https://[UAのFQDN]/[UAの名前]/ua`

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。

[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

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

画面の表示にしたい設定を開くと、プロフィー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。

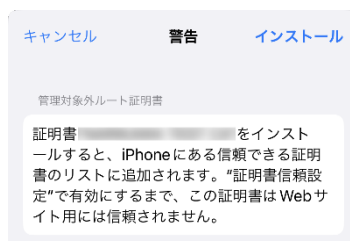


[インストール]をタップして続行してください。

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]をタップ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。



プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

なお [詳細] をタップすると、インストールされた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。



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。



7.3. Android にクライアント証明書をインポート

Androidのブラウザ (Chrome) で、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。

[ダウンロード]をタップし、証明書ファイルのダウンロードをおこないます。



※「証明書 PIN」の値を「証明書を抽出」のパスワードとして入力します。

※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

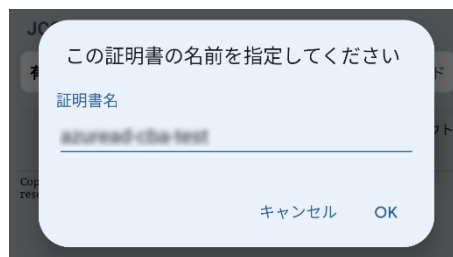
[OK]をタップして続行してください。

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

「証明書の種類の用途」のダイアログが出るので、用途を選択します。



[OK]をタップして続行してください。



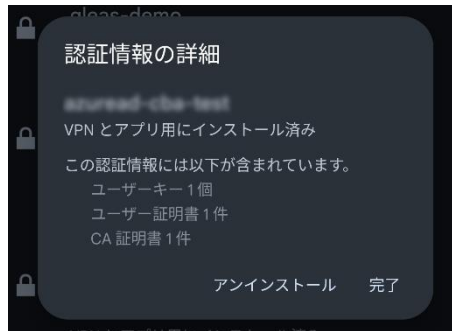
[OK]をタップします。

Chrome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、Androidでの証明書ファイルのインストールは終了です。

プライベート認証局 Gleás ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

[設定]>[セキュリティ]>[詳細設定]>[暗号化と認証情報]>[ユーザー認証情報]>[証明書
の名前]とタップすると、インストールされた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。



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。

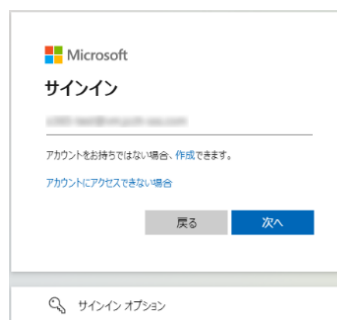


8. 証明書ベース認証によるアプリケーション利用

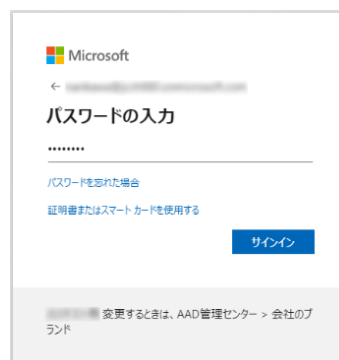
8.1. Windows デバイスでアクセス

PCのブラウザ (Edge) からアプリケーションのサインオンURLにアクセスすると、Azure AD のサインイン画面に遷移します。

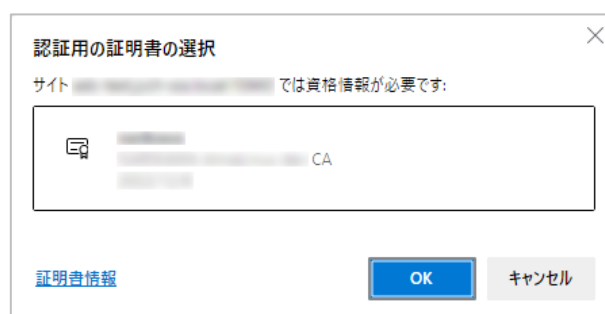
[ユーザー名]を入力して次へをクリックします。



[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。

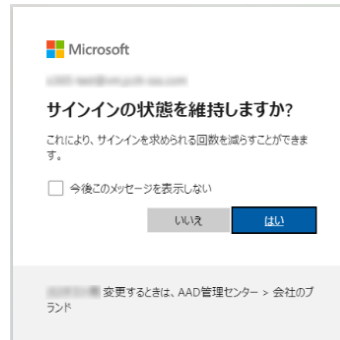


クライアント証明書を選択して[OK]ボタンをクリックします。

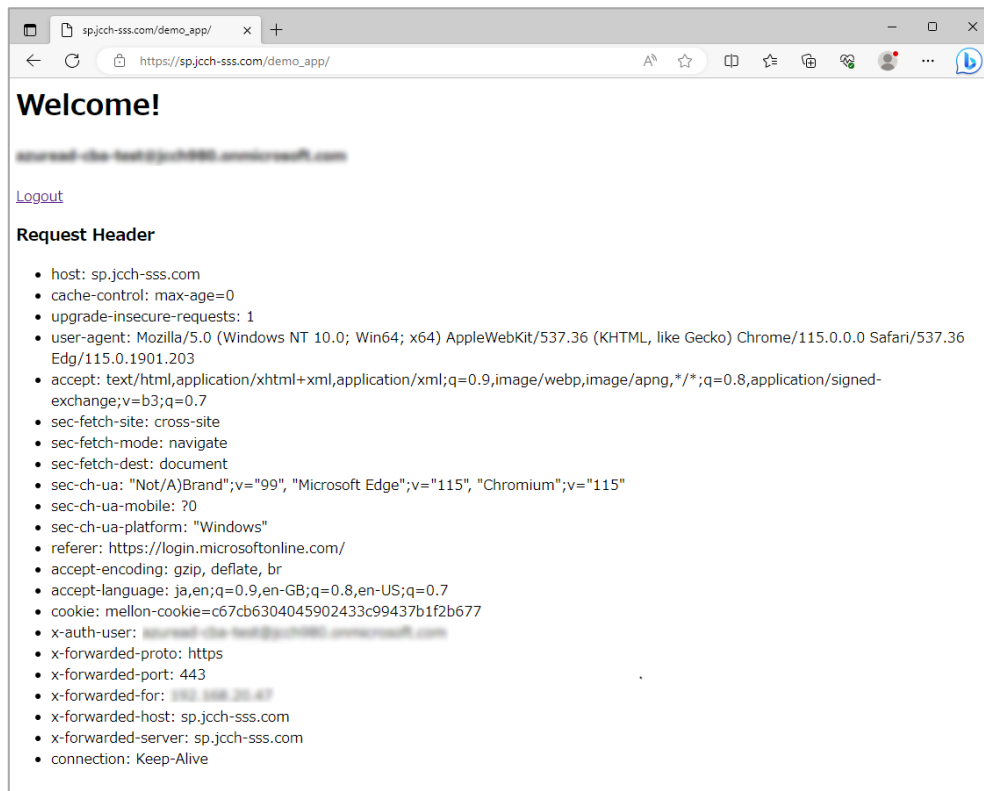


プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

[はい]または[いいえ]をクリックすると、サインインしてWebアプリケーションにアクセスできます。



※以下は 5.2 項のアプリケーションにアクセスした例



プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

マイ アプリ ポータルからログインすることもできます。

※URL <https://myapps.microsoft.com/>

同様にクライアント証明書を選択してサインインすると、マイ アプリ ポータルにアクセスできます。



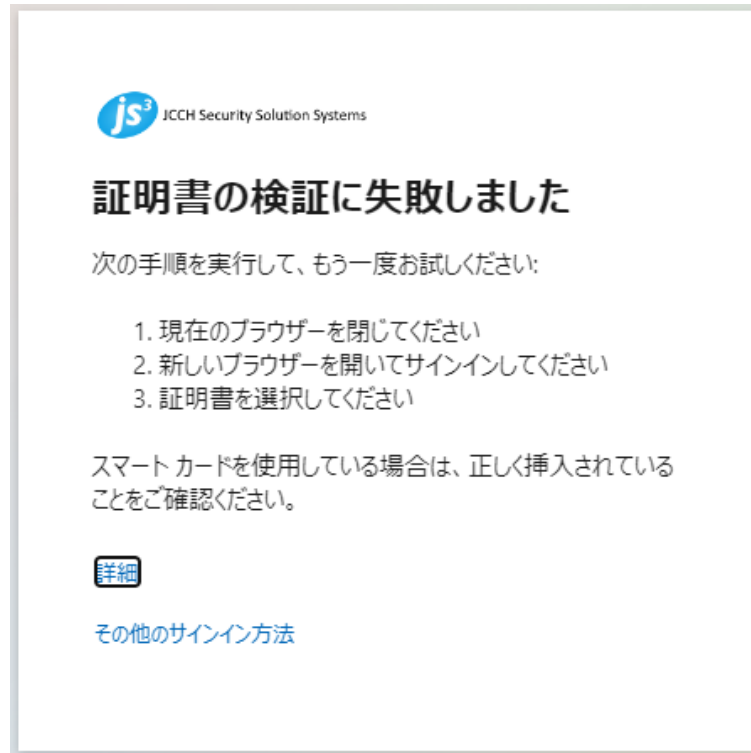
[アプリ]一覧から登録した「エンタープライズ アプリケーション」をクリックすると

Webアプリにアクセスできます。

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

証明書を持っていない場合や、失効された証明書を提示した場合はアクセスに失敗します。

※以下は失効されたクライアント証明書でアクセスした例



The screenshot shows a web page with the following content:

js³ JCHH Security Solution Systems

証明書の検証に失敗しました

次の手順を実行して、もう一度お試しください:

1. 現在のブラウザを閉じてください
2. 新しいブラウザを開いてサインインしてください
3. 証明書を選択してください

スマートカードを使用している場合は、正しく挿入されていることをご確認ください。

[詳細](#)

[その他のサインイン方法](#)

8.2. iPhone デバイスでアクセス

iPhoneのブラウザ (Safari) からアプリケーションのサインオンURLにアクセスすると、

Azure AD のサインイン画面に遷移します。

[ユーザー名]を入力して次へをタップします。



[証明書またはスマートカードを使用する]をタップします。

クライアント証明書を選択して[選択]をタップします。



プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

[はい]または[いいえ]をクリックすると、サインインしてWebアプリケーションにアクセスできます。

js³ JCH Security Solution Systems

アカウント: [redacted]

サインインの状態を維持しますか?

これにより、サインインを求められる回数を減らすことができます。

今後このメッセージを表示しない

いいえ **はい**

設定が変更するときは、AAD管理センター -> 会社のブランド

※以下は 5.2 項のアプリケーションにアクセスした例

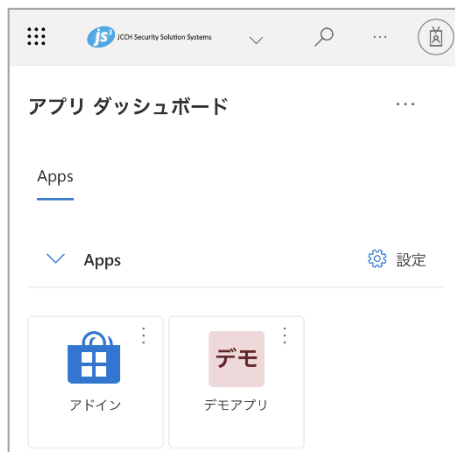
```
Welcome!
[redacted]
Logout
Request Header
• host: sp.jcch-sss.com
• accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
• cookie: mellon-cookie=cb6e8a6c3462ede82af35b3e23f643d9
• user-agent: Mozilla/5.0 (iPhone; CPU iPhone OS 16_3 like Mac OS X)
  AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.3 Mobile/15E148
  Safari/604.1
• accept-language: ja
• referer: https://login.microsoftonline.com/
• accept-encoding: gzip, deflate, br
• x-auth-user: [redacted]
• x-forwarded-proto: https
• x-forwarded-port: 443
• x-forwarded-for: [redacted]
• x-forwarded-host: sp.jcch-sss.com
• x-forwarded-server: sp.jcch-sss.com
• connection: Keep-Alive
```

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

マイ アプリ ポータルからログインすることもできます。

※URL <https://myapps.microsoft.com/>

同様にクライアント証明書を選択してサインインすると、マイ アプリ ポータルにアクセスできます。

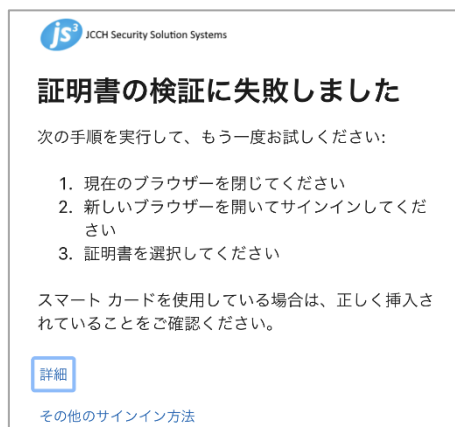


[アプリ]一覧から登録した「エンタープライズ アプリケーション」をクリックすると

Webアプリにアクセスできます。

証明書を持っていない場合や、失効された証明書を提示した場合はアクセスに失敗します。

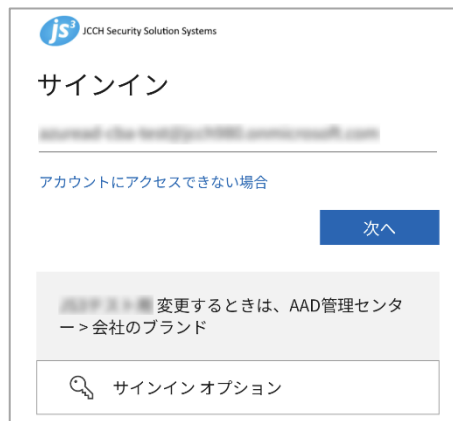
※以下は失効されたクライアント証明書でアクセスした例



8.3. Android デバイスでアクセス

Androidのブラウザ (Chrome) からアプリケーションのサインオンURLにアクセスすると、Azure AD のサインイン画面に遷移します。

[ユーザー名]を入力して次へをタップします。



[証明書またはスマートカードを使用する]をタップします。

クライアント証明書を選択して[選択]をタップします。



プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

[はい]または[いいえ]をクリックすると、サインインしてWebアプリケーションにアクセスできます。

サインインの状態を維持しますか?

これにより、サインインを求められる回数を減らすことができます。

今後このメッセージを表示しない

いいえ はい

設定を変更するときは、AAD管理センター -> 会社のブランド

※以下は 5.2 項のアプリケーションにアクセスした例

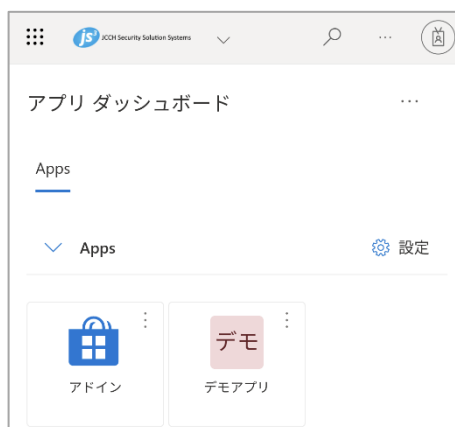
```
Welcome!
Logout
Request Header
• host: sp.jcch-sss.com
• cache-control: max-age=0
• upgrade-insecure-requests: 1
• user-agent: Mozilla/5.0 (Linux; Android 10; K)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/115.0.0.0 Mobile Safari/537.36
• accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,*/*;q=0.8
• sec-fetch-site: cross-site
• sec-fetch-mode: navigate
• sec-fetch-dest: document
• sec-ch-ua: "Not(A)Brand";v="99", "Google Chrome";v="115", "Chromium";v="115"
• sec-ch-ua-mobile: ?1
• sec-ch-ua-platform: "Android"
• referer: https://login.microsoftonline.com/
• accept-encoding: gzip, deflate, br
• accept-language: ja-JP;ja;q=0.9,en-US;q=0.8,en;q=0.7
• cookie: mellon-cookie=3bbb918f687253657bd092318d090464
• x-auth-user:
• x-forwarded-proto: https
• x-forwarded-port: 443
• x-forwarded-for:
• x-forwarded-host: sp.jcch-sss.com
• x-forwarded-server: sp.jcch-sss.com
• connection: Keep-Alive
```

プライベート認証局 Gléas ホワイトペーパー
Azure AD 証明書ベース認証を使用したシングルサインオン

マイ アプリ ポータルからログインすることもできます。

※URL <https://myapps.microsoft.com/>

同様にクライアント証明書を選択してサインインすると、マイ アプリ ポータルにアクセスできます。

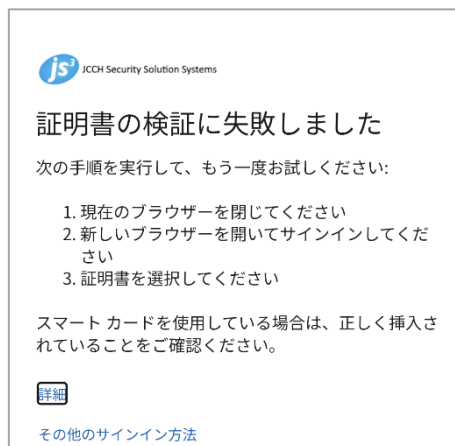


[アプリ]一覧から登録した「エンタープライズ アプリケーション」をクリックすると

Webアプリにアクセスできます。

証明書を持っていない場合や、失効された証明書を提示した場合はアクセスに失敗します。

※以下は失効されたクライアント証明書でアクセスした例



9. その他

9.1. 認証ユーザ情報をアプリケーションに伝播

本書の構成では、Azure AD での認証ユーザ情報をアプリケーションに伝播させています。

- Azure ADが認証トークンを発行

認証が成功すると、Azure AD は認証トークンを発行します

認証トークンのメッセージには認証済みユーザ情報が含まれます

メッセージには名前IDとして Azure AD のユーザプリンシパル名が記載されます

※その他 [追加の要求] として他のユーザ情報も送信可能です (3.6 項の「属性とクレーム」)

- Webサーバが認証トークンを受け取る

Webサーバは認証トークンから取り出したユーザ情報をHTTPリクエストヘッダに追加します

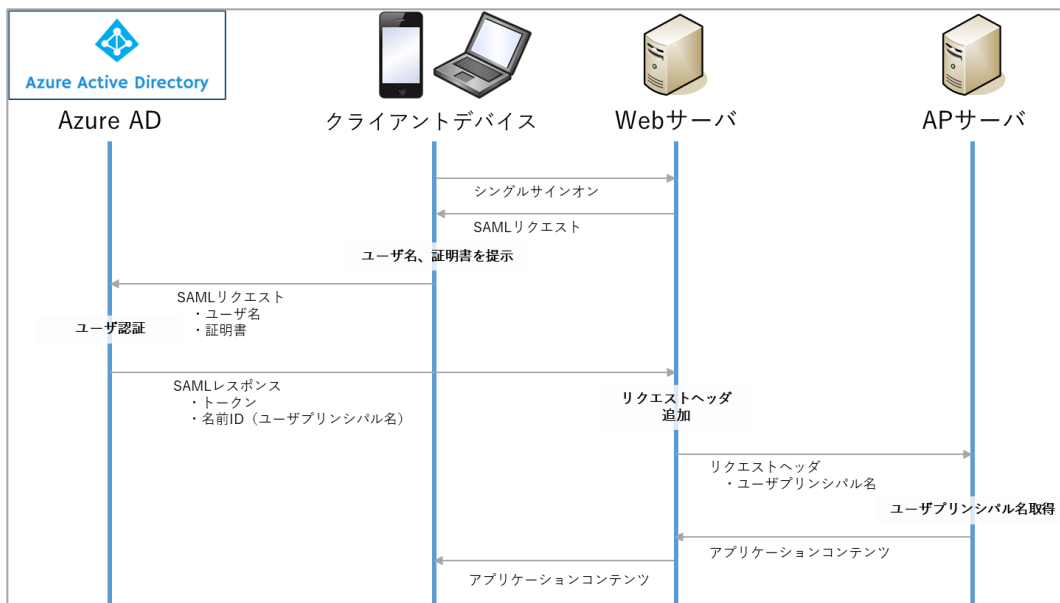
リクエストヘッダを追加したHTTPリクエストをアプリケーションにリバースプロキシします

※設定例は 2.5 項を参照

- アプリケーションがユーザ情報を受け取る

リクエストヘッダからユーザ情報を取り出すことができます

※実装例は 5.2 項を参照



9.2. 多要素証明書認証について

USBトークンやスマートカードなどの認証デバイスに証明書を格納し「所持(デバイス)、知識(PIN)」の2要素での認証を運用しているケースにおいて、AzureAD 証明書ベース認証を多要素認証とみなして動作させることが可能です。

証明書ベース認証の[保護レベル]を[多要素認証]に設定した状態での証明書認証は多要素認証を実施したものとして取り扱われます。

条件付きアクセスポリシーで[多要素認証を要求する]を設定したアプリケーションを証明書認証のみで多要素認証を行ったこととしてアクセス可能となります。

※多要素証明書認証の検証は弊社では行っておりません

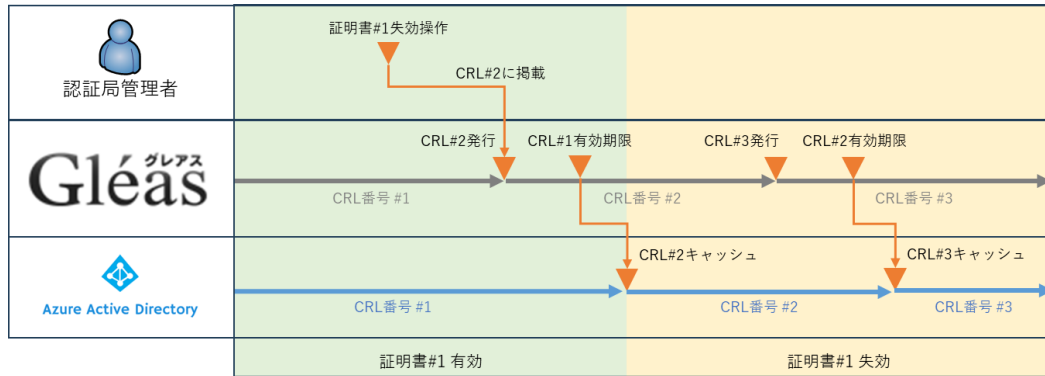
9.3. 失効確認について

Azure AD 証明書ベース認証は、証明書の失効を確認するために証明書失効リスト(CRL)を使用します。(OCSPはサポートされていません)

証明機関の設定として登録した [証明書失効リストのURL] からCRLをダウンロードしてキャッシュします。CRLの有効期間が切れると最新のCRLを再ダウンロードしてキャッシュを更新します。

AzureAD 証明書ベース認証は、このキャッシュされたCRLを用いて失効確認を行うため、認証局での証明書失効操作は即時反映されません。

※失効操作が失効確認に反映されるまでのイメージ



9.4. 即時失効について

ユーザがデバイスを紛失したなどの理由で即時の失効が運用上必要な場合、Azure AD 上でユーザの認証トークンを無効化することでアクセスを無効にする方法も考えられます。

例として、以下のコマンド操作で認証を無効化、以降のサインインを停止します。

- 管理者権限で PowerShell を起動
- 管理者の資格情報で MSOL サービスに接続

```
$msolcred = get-credential  
connect-msolservice -credential $msolcred
```

- 認証トークンの無効化

```
Set-MsolUser -UserPrincipalName [ユーザのプリンシパル名] -StsRefreshTokensValidFrom (Get-Date)
```

※この操作で現在の認証が無効化されます

- サインインを停止

```
Set-MsolUser -UserPrincipalName [ユーザのプリンシパル名] -BlockCredential $true
```

※この操作で該当ユーザのサインインが禁止されます

9.5. サインインのログについて

AzureAD 証明書ベース認証の状況は、Azure AD のサインイン ログから確認することができます。

Azure Active Directory 管理センター にログインします。

メニュー [サインイン ログ] を選択するとログが一覧表示されます。

一覧からは以下を確認することができます。

ユーザー	サインインしたユーザー
アプリケーション	アクセスしたアプリケーション
状態	成功：認証が成功したログ 失敗：認証が失敗したログ 中断：証明書を要求しているログ
IPアドレス	アクセス元IPアドレス

証明書を要求しているログは [状態] が中断となっているのでログを選択すると、

[アクティビティの詳細:サインイン] から以下を確認できます。

基本情報	許可された時刻	アクセス日時
	ユーザー	アクセスしたユーザー
	アプリケーション	アクセスしたアプリケーション
場所	IPアドレス	アクセス元IPアドレス
デバイス情報	ブラウザ	アクセスブラウザの種類
	オペレーティングシステム	アクセスOSの種類
認証の詳細	認証方法	証明書認証のときは X.509 Certificate
	成功	true なら認証成功
追加の詳細	ユーザー証明書の***	認証時に提示された証明書情報

9.6. 失効リストのサイズ制限について

弊社での検証は行っておりませんが、本書作成時の情報として、Azure AD 証明書ベース認証で扱える失効リスト (CRL) はダウンロードサイズ 20MB の制限がありました。こちらに影響される運用上の制約が懸念されますが、以下のような方法での回避が検討可能と考えます。

- Gléas に複数の認証局を構成
 - ※認証局ライセンスの追加が必要となります
- Azure ADの認証機関に2つの認証局を登録
 - ※[ルート証明書]、[証明書失効リストのURL]をそれぞれ登録します
- 証明書ベース認証の認証バインドポリシーにルールを追加
 - ※どちらの認証局から発行した証明書でも認証できるようにします
- 失効の上昇状況から認証局からの証明書の新規発行を休止
 - ※休止するタイミングは発行済み証明書の有効日数と失効の増加傾向から決定します
 - ※有効期限が切れた証明書は失効リストに掲載しない仕様なため、新規発行を休止することで時間経過と主に失効リストのサイズは小さくすることができます
- 新規証明書の発行元を切り替える
 - ※Gléas はテンプレートを更新することで証明書の発行元を変更することができます
 - ※複数の発行元を切り替えて運用することで失効リストの肥大化を抑えることが可能です
 - ※この他、発行する証明書の有効期間を短く設定することも失効リストの肥大化を防ぐことに繋がります

10. 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