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

SafeNet Trusted Accessを使ったOffice 365証明書認証

Ver.1.0
2019 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」で発行した電子証明書を使って、ジェムアルト株式会社のクラウドアクセス管理サービス「SafeNet Trusted Access」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：SafeNet Trusted Access / SafeNet認証サービス
  ※以後SafeNet Trusted Accessは「STA」、SafeNet認証サービスは「SAS」と記載します
- SaaS：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
  - Azure AD Connect （Office365へのIDプロビジョニング用）
  - SafeNet Authentication Service Sync Agent 3.7.9461.9461 （SASへのIDプロビジョニング用）
- JS3 プライベート認証局Gléas（バージョン1.16.9）
  ※以後「Gléas」と記載します
- クライアント：Windows 10 Pro / Microsoft Edge / Excel 2016
  ※以後「Windows」と記載します
- クライアント：macOS Mojave / Safari / Excel for Mac / SafeNet Authentication Client 10.2
  ※以後「Mac」と記載します
- 認証デバイス：SafeNet eToken 5110+
  ※以後「eToken」と記載します

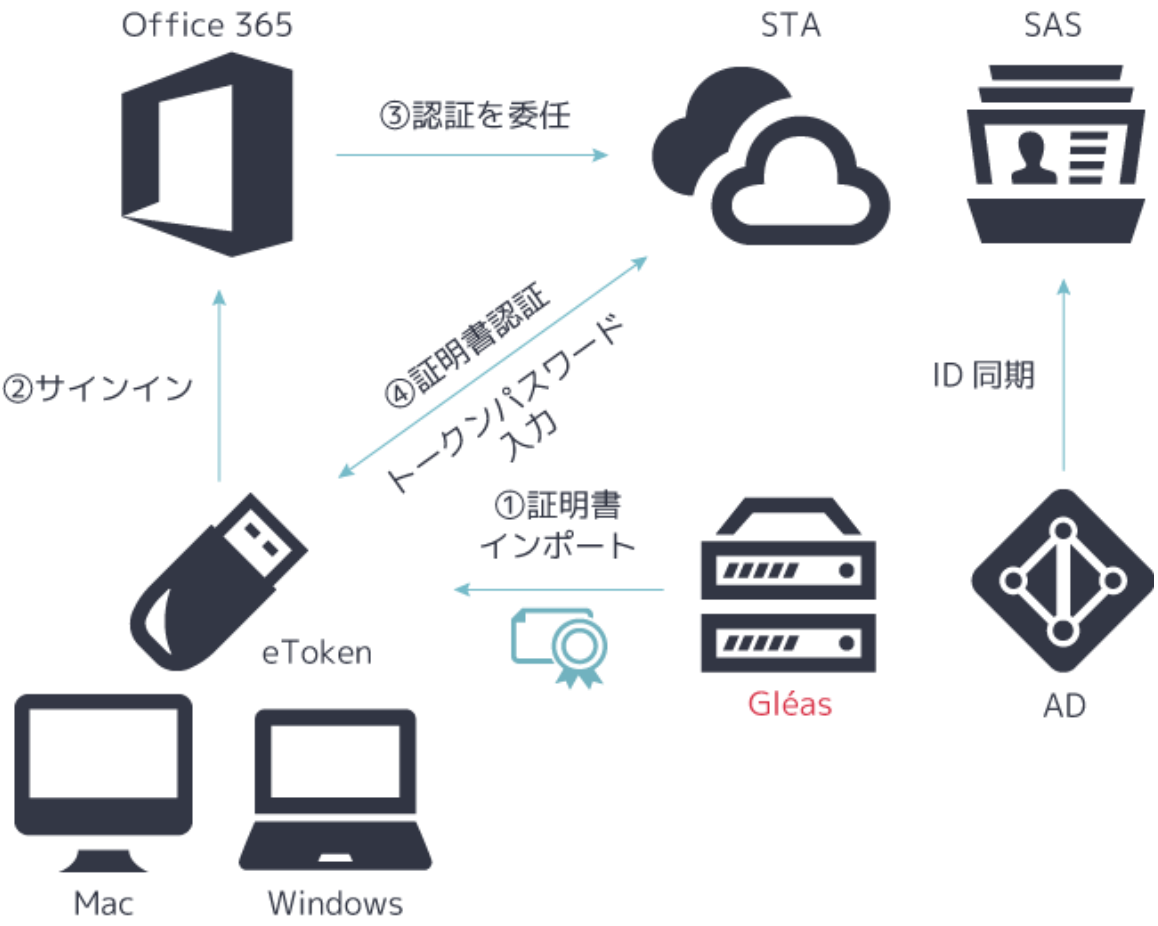
以下については、本書では説明を割愛します。

- ADのセットアップ
- STAおよびSASの基本設定
- ADとSASの連携設定
- Office 365とSTA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
- eTokenの初期化、トークンパスワード設定等の基本操作
- Windows、Mac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からeTokenに証明書をインポートし、クライアントとなるWindows、MacにeTokenを挿入する
2. クライアントのブラウザ、ExcelからOffice 365へサインインする
3. Office 365はSTAに認証を委任し、クライアントとSTAで証明書認証が行われる
4. eTokenのトークンパスワードを入力してOffice 365へのログインが完了する

1.4. 電子証明書発行時の注意事項

Gléasでクライアント証明書を発行する際には、Office 365のログインユーザ名を証明書の一般名（CN）とUPN（ユーザプリンシパル名）を記載し、またCRL配布ポイントが証明書に含まれる必要があります。

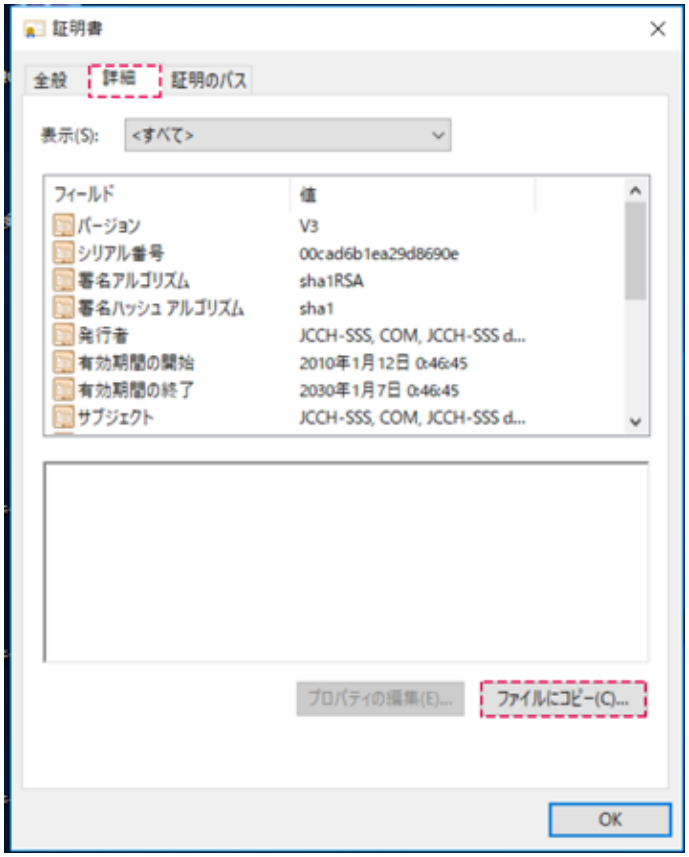
2. STA の設定

2.1. Gléas の認証局証明書インポート

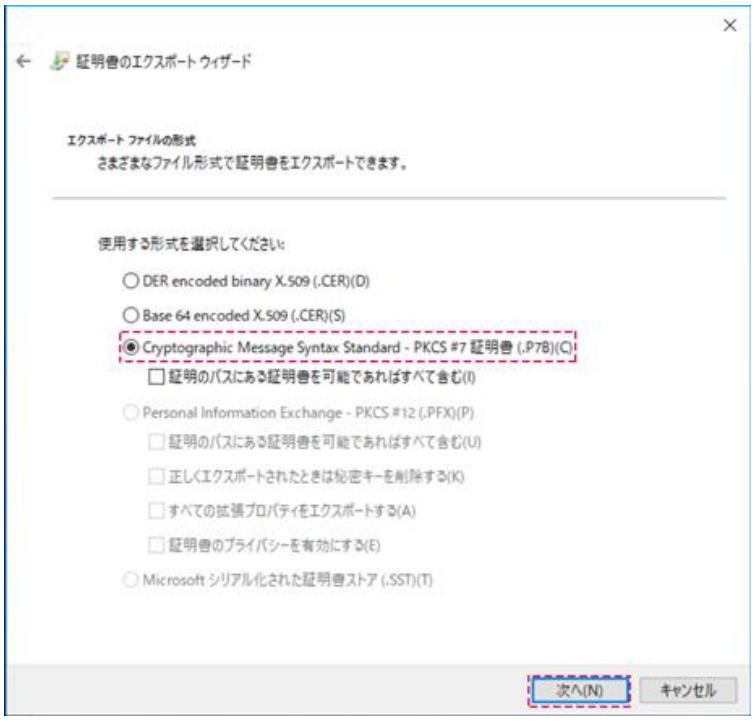
Gléas が発行したクライアント証明書を、STA が信頼できるようにするため、Gléas の認証局証明書を STA に登録します。

Gléas の管理画面から[認証局]へ進み、発行局をクリックします。[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。

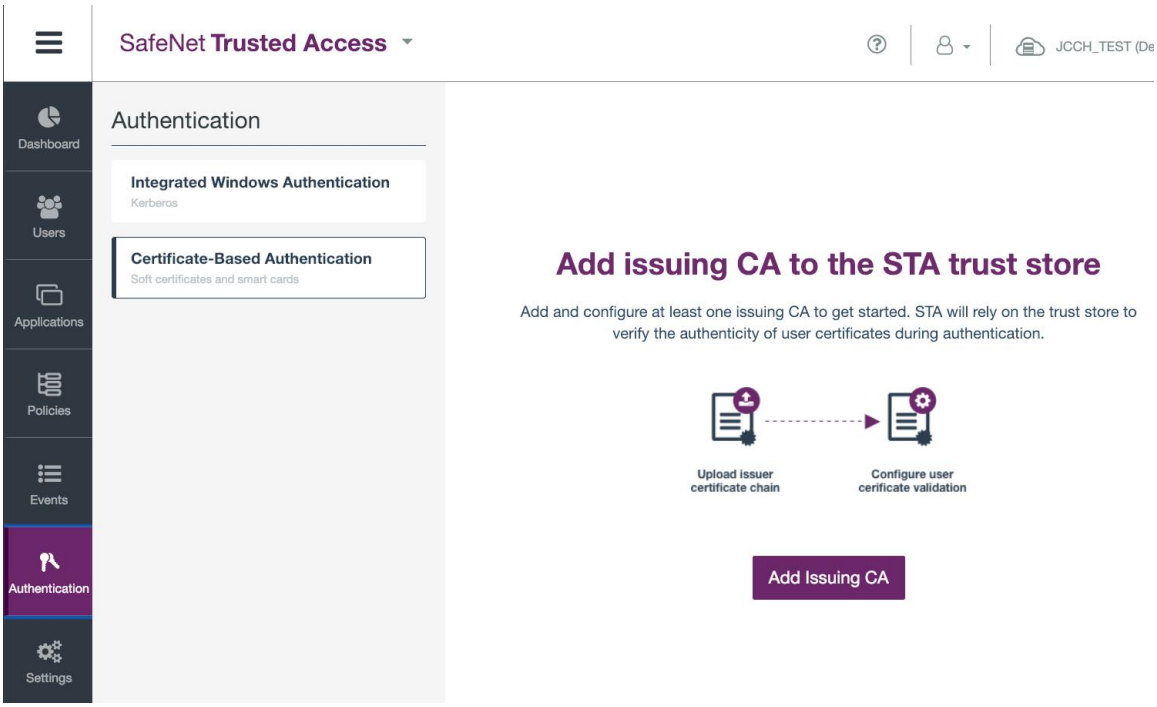
ダウンロードした証明書ファイルを Windows で開き、[詳細]タブを開きます。



[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します
[次へ]をクリックし、[Cryptographic 〜]にチェックを入れ、[次へ]をクリックして、エクスポートされる PKCS#7 証明書ファイル名前を付けて保存します。

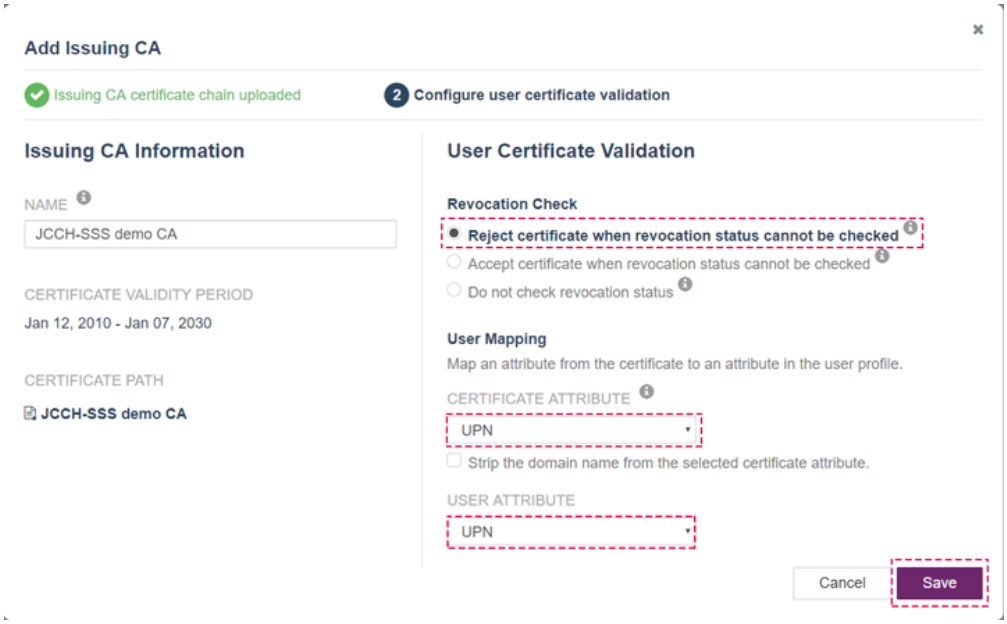


STA の管理画面で[Authentication]→[Certificate-Based Authentication]と進み、「Add Issuing CA」をクリックします。



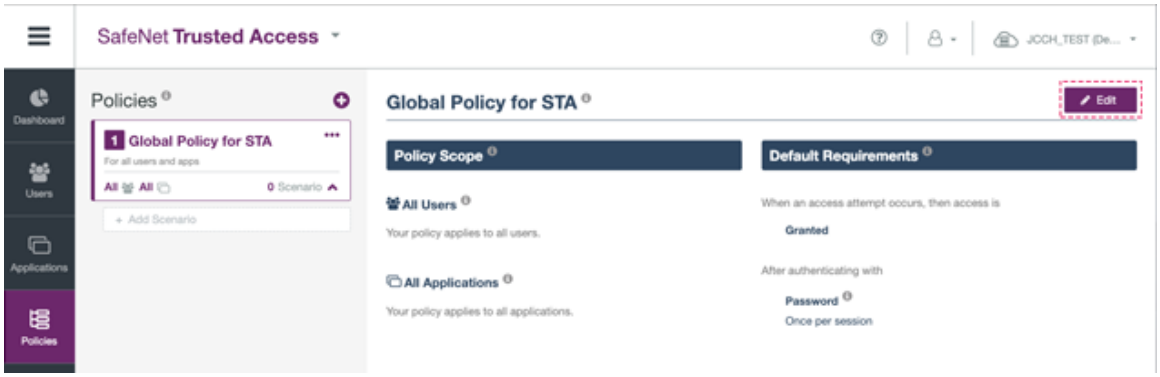
本項でエクスポートした PKCS#7 証明書（Gléas の認証局証明書)ファイルをアップロードします。

[Revocation Check] で [Reject ～] を選択し、[User Mapping] の [CERTIFICATE ATTRIBUTE]で[UPN]を選択し、[USER ATTRIBUTE]で[UPN]を選択して、[Save]をクリックします。



2.2. 認証ポリシー

[Policies] → [Global Policy for STA] → [Edit]をクリックします。



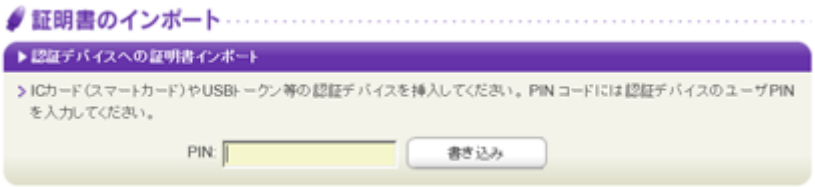
[Default Requirements]で[Certificate-Based ～]を選択し、[Save]をクリックします。
これで STA での認証に証明書が使われるようになりました。

3. GléasでのeTokenの設定

3.1. eToken への電子証明書インポート

GléasのRAにログインし、eToken用に発行した証明書の詳細画面まで移動します。
eTokenを管理者端末に接続し、画面上部の[トークンへのインポート]をクリックします。
※事前にeTokenのパーソナライズを行っている必要があります。

認証デバイスに事前に設定したPIN（暗証番号）を入力し、証明書のインポートを行います。



元の画面に戻ればインポートは成功です。
この時に画面を下にスクロールしていくと、インポート先のデバイス情報が付加されています。

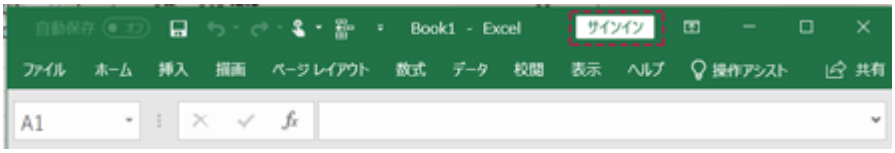
また[認証デバイス]メニューでは、この認証デバイスにインポートした証明書を確認することが可能となります。

※Gléasでは、パーソナライズした認証デバイスをエンドユーザに配布し、エンドユーザに証明書のインポートを行わせることも可能です。詳細はJS3までお問い合わせください

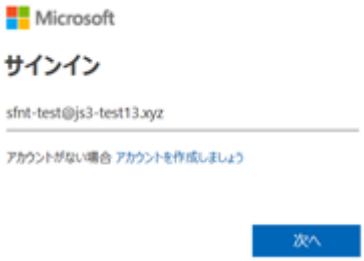
4. クライアントからOffice 365へのログイン

4.1. Windows で Excel を使う場合

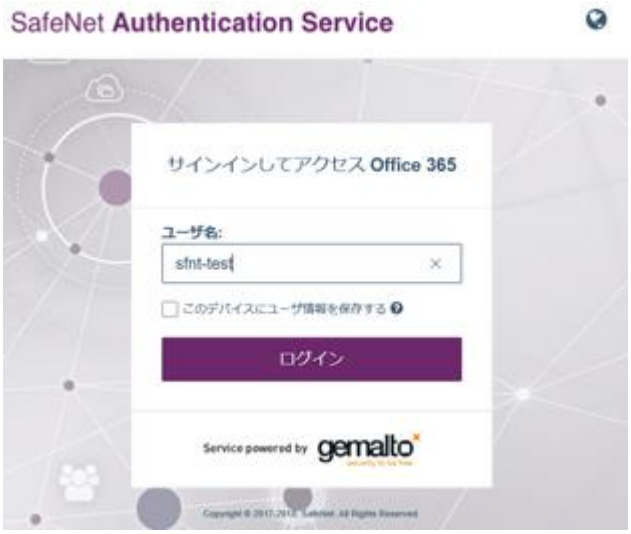
Windowsに証明書インポート済みのeTokenを挿入し、Excelを起動してサインインします。



Office 365のアカウントを入力し、[次へ]をクリックします。



SASのユーザ名を入力して[ログイン]をクリックします。



eTokenにインポートされた証明書を選択して[OK]をクリックします。

eTokenに設定されたトークンパスワードを入力して[OK]をクリックすると、Office 365へのログインが完了します。

4.2. Windows で Edge を使う場合

あらかじめSTAの管理画面でUser Portalの設定をしておきます。Edgeを起動し、User Portalのログインを開きます。

SASのユーザ名を入力し[ログイン]をクリックします。

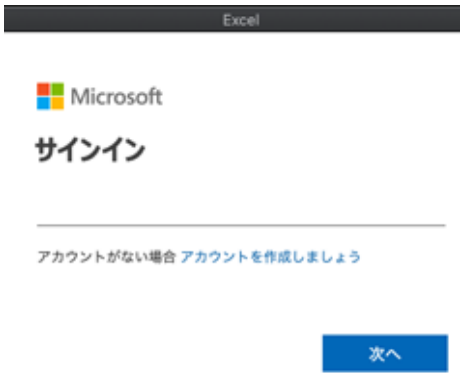
eTokenにインポートされた証明書を選択して[OK]をクリックします。

eTokenに設定されたトークンパスワードを入力して[OK]をクリックすると、User Portalのログインが完了します。

[Office 365]をクリックすると、SAMLによる認証連携が行われ、ユーザ操作なしでOffice 365へのログインができます。

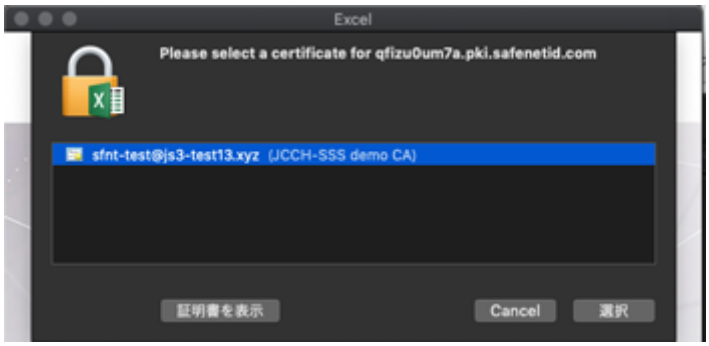
4.3. Mac で Excel for Mac を使う場合

Mac で eToken を使う場合は、あらかじめ SafeNet Authentication Client をインストールしておく必要があります。証明書をインポート済みの eToken を Mac に挿入して Excel を起動します。

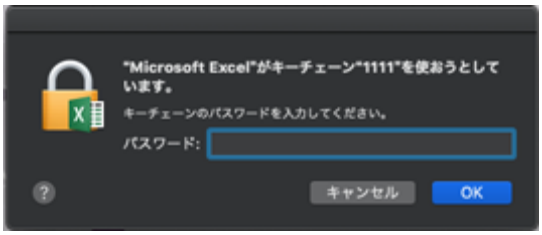


Office 365のアカウントを入力し、[次へ]をクリックします。

SASのユーザ名を入力して[ログイン]をクリックします。



eTokenにインポートされた証明書を選択して[OK]をクリックします。



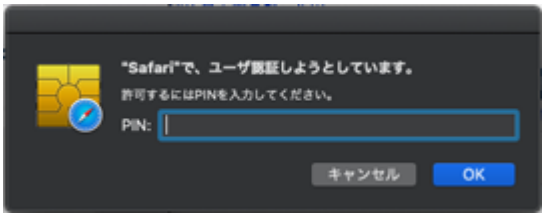
eTokenに設定されたトークンパスワードを入力して[OK]をクリックすると、Office 365へのログインが完了します。

4.4. Mac で Safari を使う場合

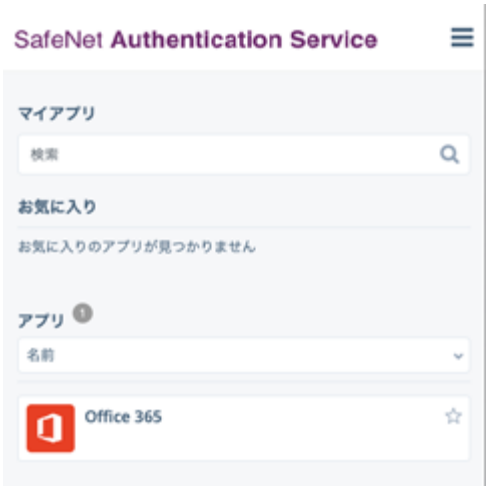
あらかじめSTAの管理画面でUser Portalの設定をしておきます。Safariを起動し、User PortalのログインURLを開きます。

SASのユーザ名を入力し[ログイン]をクリックします。

eTokenにインポートされた証明書を選択して[OK]をクリックします。



eTokenに設定されたトークンパスワードを入力して[OK]をクリックすると、User Portalのログインが完了します。



[Office 365]をクリックすると、SAMLによる認証連携が行われ、ユーザ操作なしでOffice 365へのログインができます。

5. 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。

■STA や eToken に関するお問い合わせ

ジェムアルト株式会社　IDP 事業部
Tel:　　03-6744-2111
Mail:　　SalesEnterprise-Japan@gemalto.com

■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