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CA Gléas ホワイトペーパー

SeciossLinkを利用したSAMLシングルサインオン（Office 365編）

Ver.1.1
2020 年 9 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。

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CA Gléas」で発行した電子証明書を利用して、セシオス株式会社の提供するシングルサインオン（SSO）サービス「SeciossLink」を経由して Microsoft Corporation の提供するOffice 365に対しSecurity Assertion Markup Language（SAML）を用いたシングルサインオン環境を構築するための設定例を記載します。

※iOSについては、OfficeアプリやExchange ActiveSyncでの先進認証の手順も記載しております

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参考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。

- 【SSOサービス】SeciossLink
- 【認証局】JS3 プライベートCA Gléas （バージョン2.1.4）
  ※以後、「Gléas」と記載します
- 【アプリケーション】Office 365 E3
  ※以後、「Office 365」と記載します
- 【クライアント：PC】Microsoft Windows 10 Pro バージョン1909
  ※以後、「PC」と記載します
- 【クライアント：タブレット】Apple iPad（iPadOS 13.7）
  ※以後、「iPad」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。

- Office 365の基本設定
- SeciossLinkのシングルサインオン設定
  ※セシオス株式会社のWEBサイトでOffice 365認証連携を含めたSeciossLinkの設定方法が記載されたマニュアルが公開されています

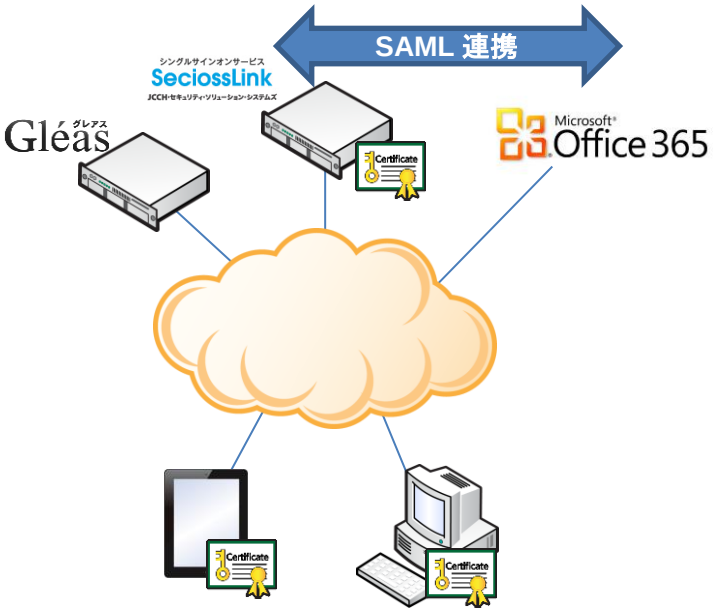
参考URL：https://seciosslink.com/manual/manual_cate/Office 365

- 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。

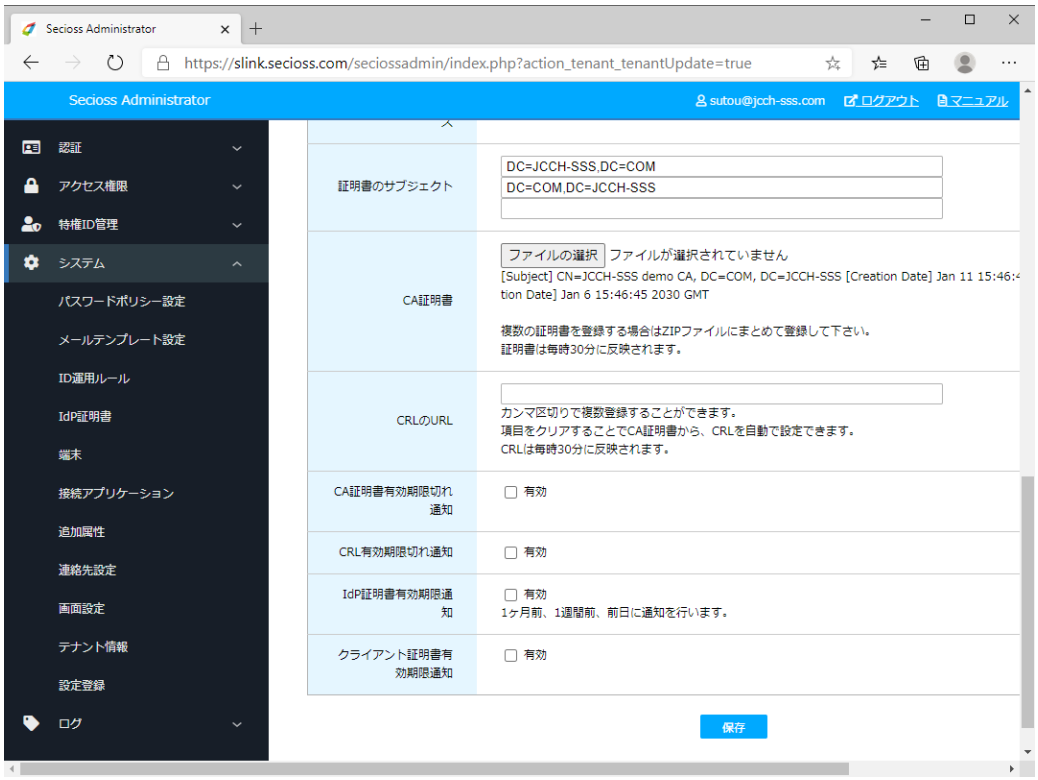


1. デバイス（PC・iPad）はGléasよりクライアント証明書を取得します。
2. ブラウザでOffice 365サインイン画面（https://login.microsoftonline.com）にアクセスし、SeciossLinkの管理画面でシングルサインオン設定を実施しているドメインユーザを入力（ブラウザが記憶している場合は既入力）します。
3. SeciossLinkから有効なクライアント証明書を要求されるので、Gléasより取得した証明書により認証をおこないます。
4. 続いてSeciossLinkに登録したユーザIDとパスワードによる認証がおこなわれます。この時のユーザIDはクライアント証明書のサブジェクトのcn（Common Name）が利用されます。
5. SeciossLinkへのログインに成功すると、自動的にOffice 365に転送されます。

2. SeciossLink の設定

2.1. 信頼する認証局の設定

SeciossLinkに管理者としてログインし、画面上部のメニューより[システム]をクリックします。左ペインの[システム管理]メニューより[テナント情報]をクリックすると、右ペインに以下の設定画面が表示されるので以下を設定します。



- [証明書のサブジェクト]には、アクセスを許可するクライアント証明書のサブジェクトを入力（前方一致か後方一致で空欄不可。3つまで入力可能）
- [CA証明書]には、[ファイルを選択]ボタンを押して事前に準備したGléasの認証局証明書を選択しインポート
- [CRLのURL]には、失効リスト（CRL）の取得用のURLを入力

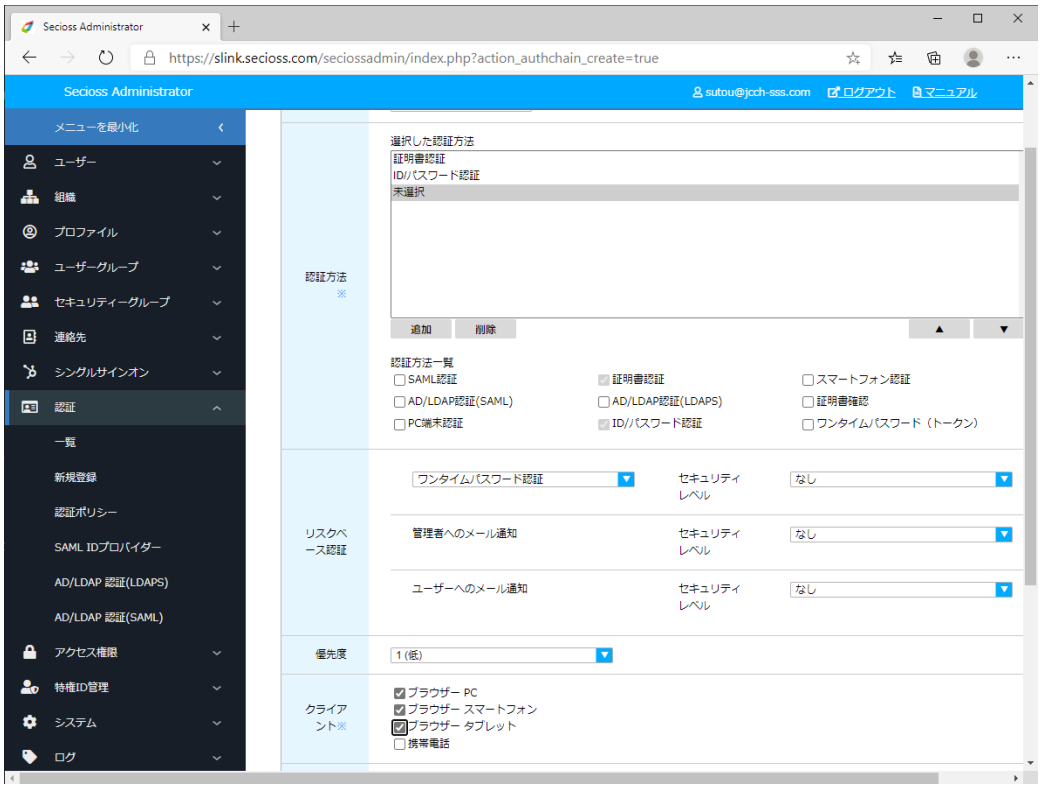
  ※GléasのデフォルトのCRL配布ポイントは以下のとおりです。SeciossLinkからアクセス可能である必要があります

  http://hostname.example.com/crl/ia1.crl

  ※SeciossLinkは、失効リストを定期的に自動取得します

2.2. 認証ルールの作成

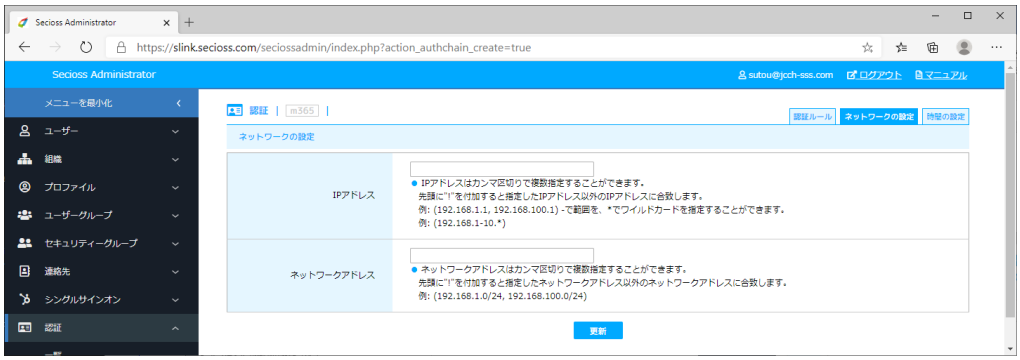
上部メニューより[認証] > [新規登録]をクリックします。
新規設定画面で以下を設定します。



以下を設定します。

- [ID]には、認証ルールを識別する任意の ID 名を入力
  [認証方法]には、[証明書認証]と[ID/パスワード認証]を[追加 AND >]を使って選択
  ※パスワード入力を省略したい場合は、[証明書認証]だけにすることも可能
- [優先度]には、他の認証ルールと併用する場合の優先度を選択（数字が大きい方が優先）
- [クライアント]には、[ブラウザー PC]、[ブラウザー スマートフォン]、[ブラウザー タブレット]をチェック後、[登録]をクリックします。

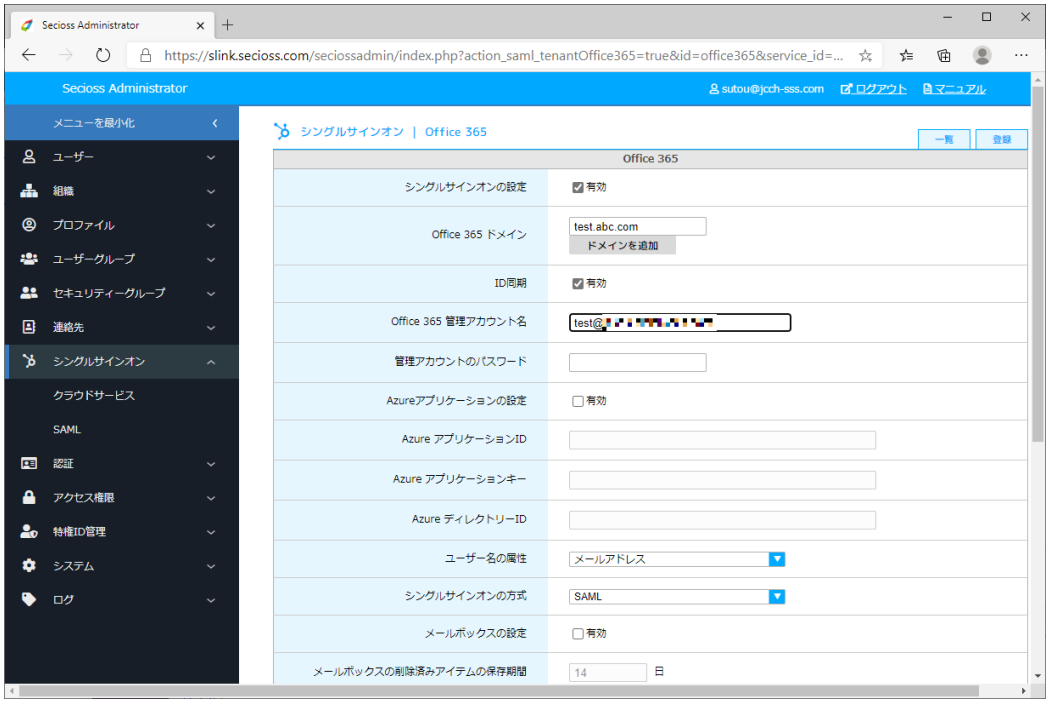
認証ルールが作成されると、このルールを適用するクライアントのアクセス元 IP アドレスの制限（[許可するネットワーク]）や、時刻による制限（[許可する時間]）の指定が可能となります。



SeciossLink では複数の WEB サービスにシングルサインオンをおこなう際などに、特定の WEB サービス（Office 365 等）に限定してクライアント証明書認証を追加するような設定も可能です。
詳細は[アクセス権限]メニューを参照してください。本ドキュメントでの説明は省略します。

2.3. シングルサインオンの設定

※ 本設定は Office 365 の管理画面でドメインのセットアップが完了した後に実施してください
左ペインより[シングルサインオン] > [クラウドサービス] をクリックし一覧より[Office 365]を選択（操作の欄をクリック）します。



以下を設定します。

- [シングルサインオンの設定]を有効
- [Office 365 ドメイン]に利用するドメインを記述
- [ID 同期]を有効
- [Office 365 管理アカウント名]および[管理アカウントのパスワード]を入力

3. Gléasの管理者設定（PC）

GléasのUA（申込局）より発行済み証明書をクライアント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

3.1. UA（ユーザ申込局）設定

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

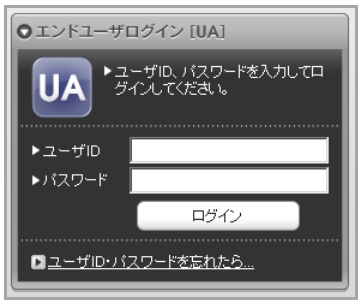
設定終了後、[保存]をクリックし設定を保存します。
各項目の入力が終わったら、 [保存]をクリックします。

以上でGléasの設定は終了です。

4. クライアント側での操作（PC）

4.1. クライアント証明書のインストール

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。



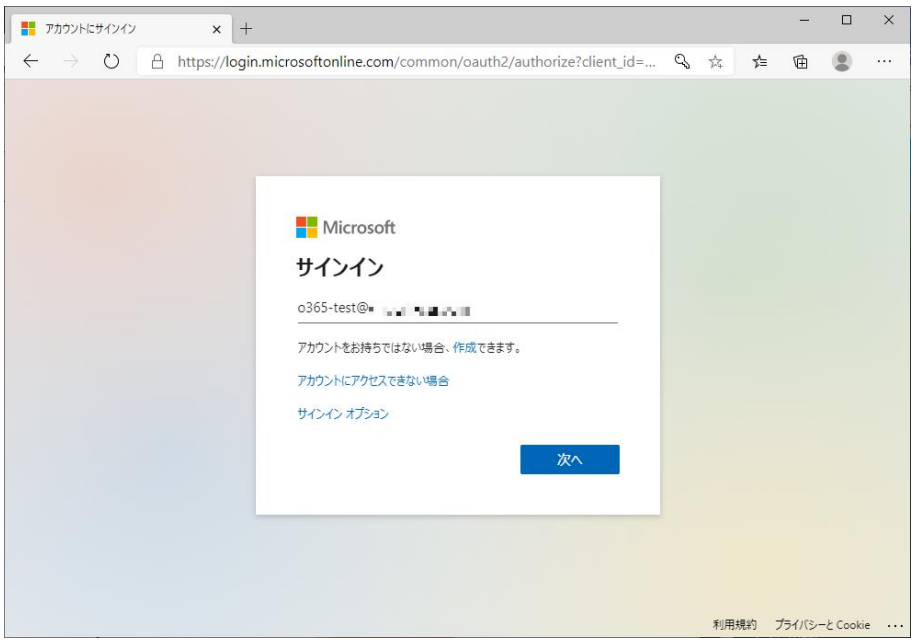
ログインすると、ユーザ専用ページが表示されます。
[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。
※初回ログインの際は、ActiveXコントロールのインストールを求められるので、画面の指示に従いインストールを完了してください。

「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

アウトします。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。

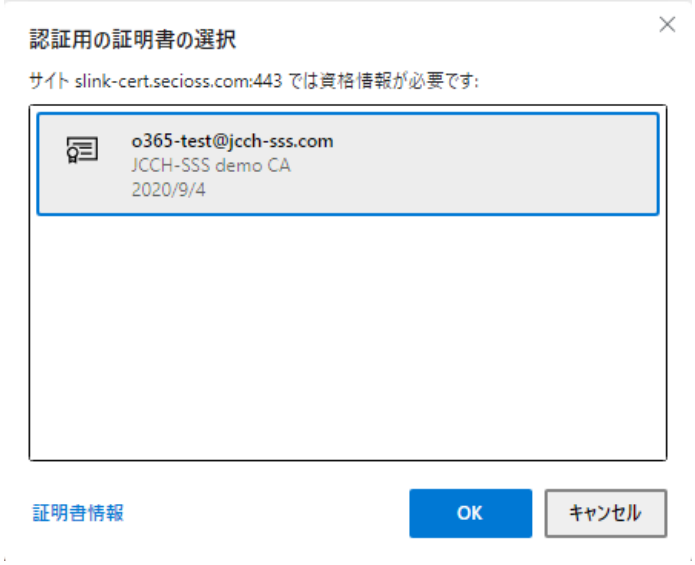
4.2. Office 365 へのシングルサインオン

Edgeブラウザを起動してOffice 365（https://login.microsoftonline.com）へアクセスし、ユーザIDを入力して[次へ]をクリックします。



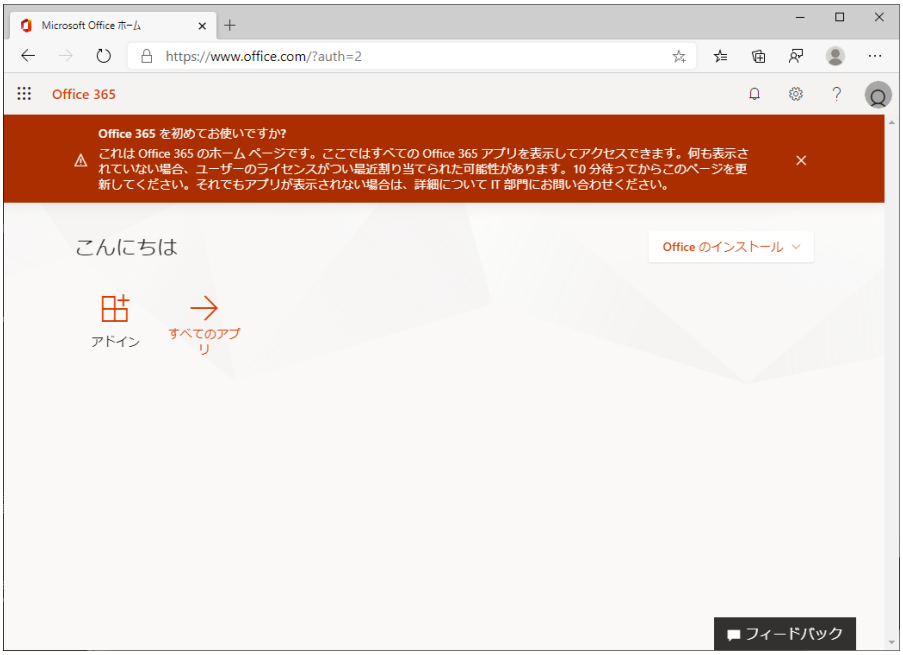
クライアント証明書の選択が表示されますので証明書を確認して[OK]をクリックします。

※設定によっては、クライアント証明書の選択ダイアログが出ない場合もあります



SeciossLinkのログイン画面が表示されます。このときのユーザIDはクライアント証明書のサブジェクトのcn値となります。

SeciossLinkでのログインパスワードを入力し、[ログイン]を入力するとOffice 365 ログイン後の画面に転送され、ログイン完了です。



SeciossLinkにユーザ登録されていないサブジェクトcn値を持つクライアント証明書や、[テナント情報]で設定したものと異なるサブジェクトの証明書でアクセスした場合は以下のとおりエラーとなります。

クライアント証明書のない状態や、失効したクライアント証明書でアクセスした際には以下のようなエラーとなります。

※失効情報がSeciossLinkに伝搬されている必要があります

5. Gléasの管理者設定（iPad）

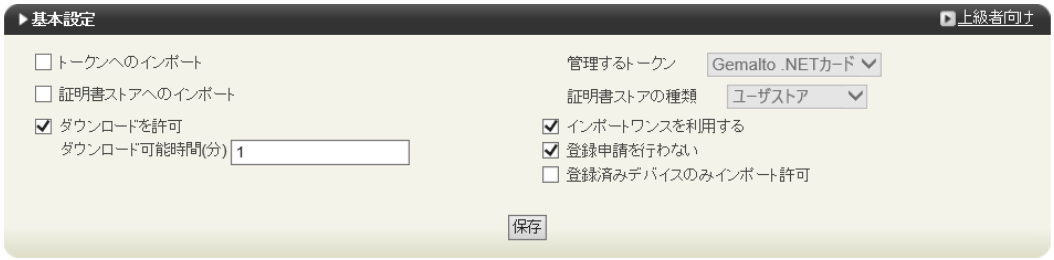
※下記設定は、Gléas 納品時等に弊社で設定を既に行っている場合があります

5.1. UA（ユーザ申込局）設定

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、iPad用となる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
- [インポートワンスを利用する]のチェック、[ダウンロード可能時間(分)]の設定
  この設定を行うと、GléasのUAからダウンロードしてから、指定した時間（分）を経過した後に、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）。このインポートロックにより複数台のiPad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。



[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。

- [iPhone用レイアウトを利用する]にチェック
- [iPhone構成プロファイル基本設定]の各項目を入力
  ※[名前]、[識別子]、[プロファイルの組織名]、[説明]は必須項目となります

設定終了後、[保存]をクリックして設定を保存します。

以上でGléasの設定は終了です。

6.クライアント側での操作（iPad）

GléasのUAに接続し、発行済みのクライアント証明書・構成プロファイルのインポートを行います。

6.1. 構成プロファイルのインストール

iPad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、[構成プロファイルのダウンロード]をタップし、ダウンロードを開始します。

※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

ダウンロードが終了すると以下のメッセージが表示されるので閉じてください。

[設定] > [一般] > [プロファイル]で表示されるプロファイル一覧から、ダウンロード済みプロファイルに表示される証明書をタップします。

「インストール」をタップします。

ここで[詳細]をタップするとインストールされる証明書情報を確認できます。
インストール完了後は[完了]をタップしてください。

ブラウザを再表示し、UAの画面にて[ログアウト]をタップしてUAからログアウトしてください。
以上で、iPad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]をタップした時点から管理者の指定した時間を経過した後にUAへ再ログインすると、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不可能となります。

この他に、iOS端末の識別番号を用いて端末を限定してクライアント証明書を配布することも可能です。詳細は弊社営業担当までお問い合わせください。

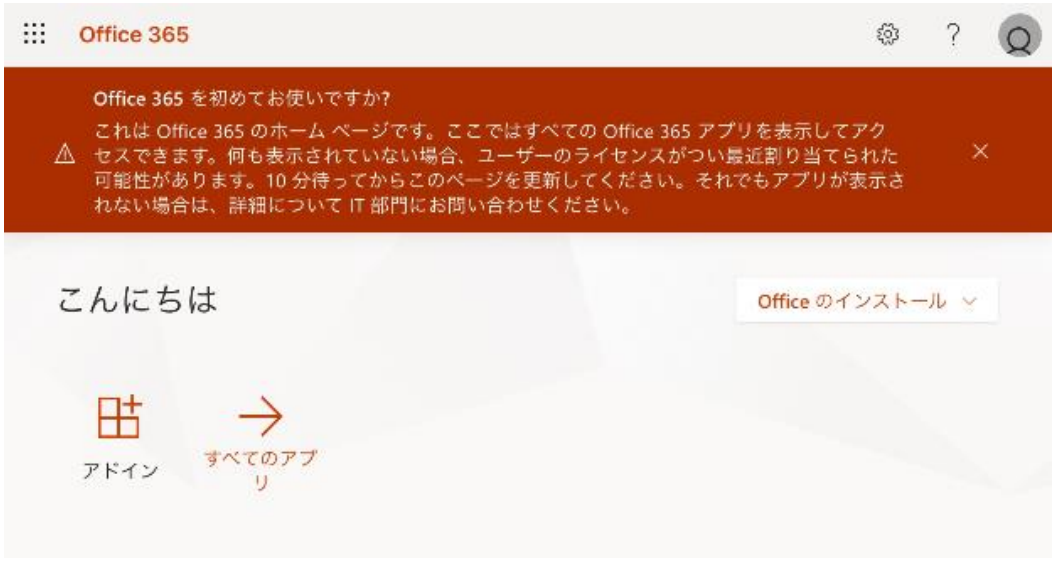
6.2. Office 365 へのシングルサインオン

SafariでOffice 365へアクセスします。URLは以下のとおりです。
https://login.microsoftonline.com
SeciossLinkの管理画面でシングルサインオン設定を実施しているユーザIDを入力して[次へ]をタップしてください。

認証に使用するクライアント証明書がある場合は以下のメッセージが表示されます。

[続ける]をタップするとSeciossLinkのログイン画面へ転送されます。

SeciossLinkでのログインパスワードを入力し、[ログイン]をタップするとOffice 365のログイン後の画面に転送されます。

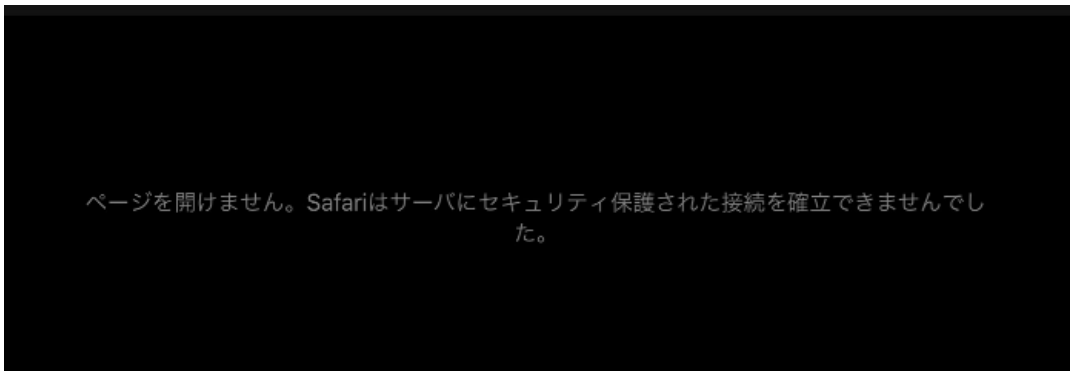


認証に使用する証明書がない場合は以下の状況に応じたエラーとなります。

・SeciossLinkにユーザ登録したcn値を持つクライアント証明書がない場合。

・[テナント情報]で設定した認証局にて発行した証明書がない場合、もしくは失効された証明書でアクセスした場合。

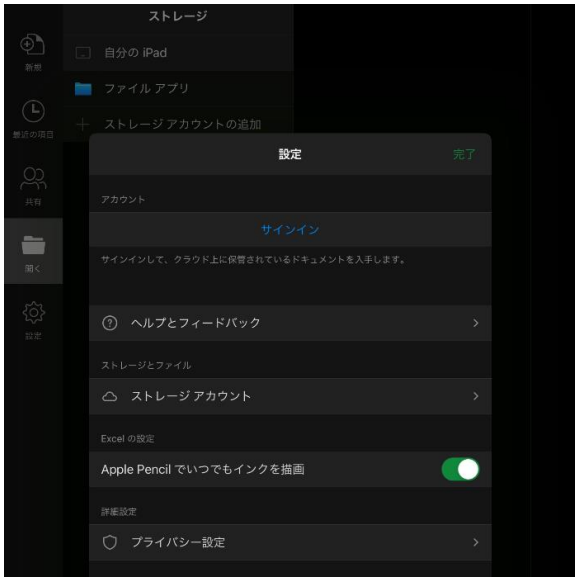
※失効情報がSeciossLinkに伝搬されている必要があります。



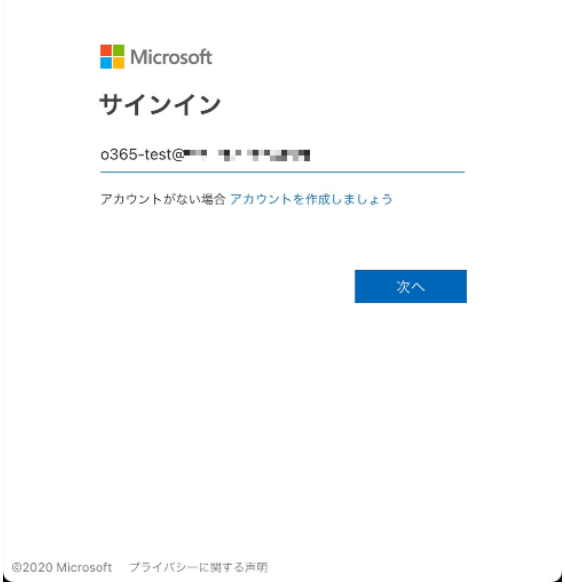
6.3. Office アプリでの先進認証

※以下の手順を実施する前にApp StoreよりMicrosoft Authenticatorアプリをインストールしておく必要があります

Officeアプリ(Excel)を起動し、[設定] > [サインイン]をタップしアカウントの追加を行います。



SeciossLinkの管理画面でシングルサインオン設定を実施しているドメインユーザのIDを入力して[次へ]をタップしてください。



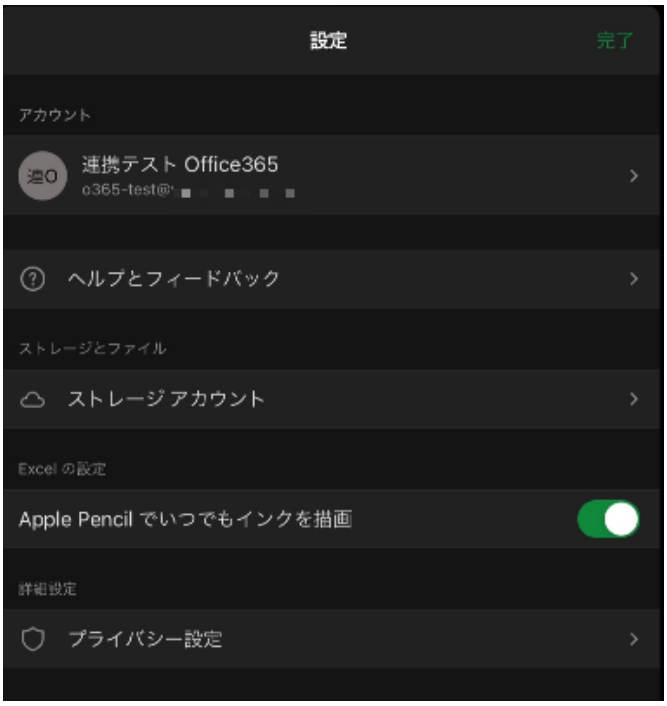
証明書認証がバックグラウンドで実行され、成功するとSeciossLinkのログイン画面に転送されます。

この時に提示可能な証明書が複数ある場合は、選択ダイアログが表示されます。

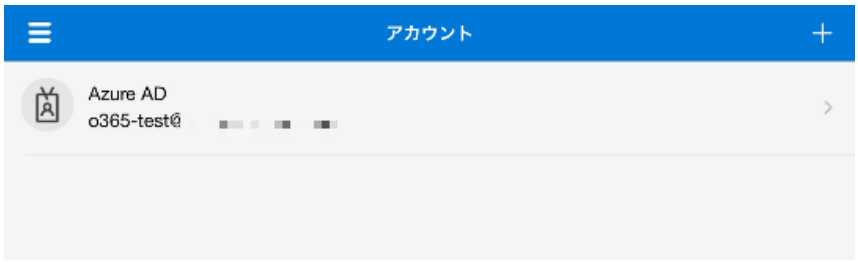
SeciossLinkでのログインパスワードを入力し、[ログイン]をタップするとログインが完了し、MS Authenticatorへのサインイン確認が表示されるので[続行]をタップします。

続いてMS Officeへのサインイン確認が表示されるので[続行]をタップします。

Officeアプリの画面に戻り、アカウントが追加されたことが確認できます。



また、Microsoft Authenticatorを見るとAzure ADにログインできていることを確認できます。



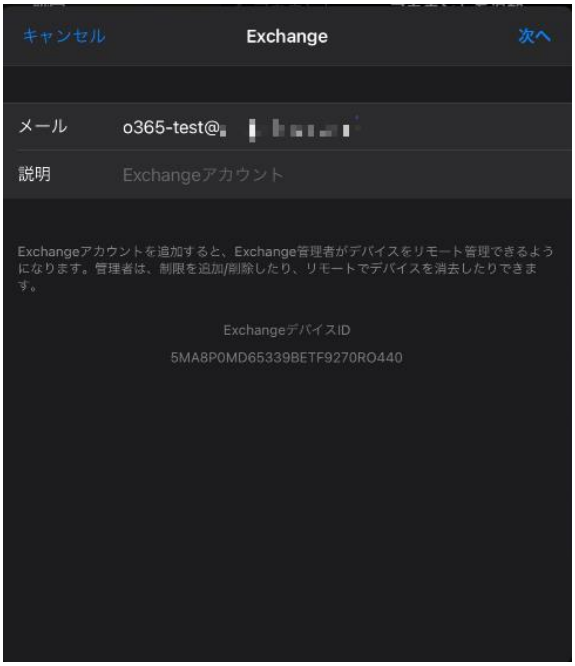
Microsoft Authenticatorを認証に使うMS社の他のモバイルアプリも、この認証結果情報を参照します。

6.4. Exchange ActiveSync での先進認証

※本手順ではMicrosoft Authenticatorは不要です

[設定] > [メール] > [アカウント]から[アカウントを追加]をタップし[Microsoft Exchange]をタップします。

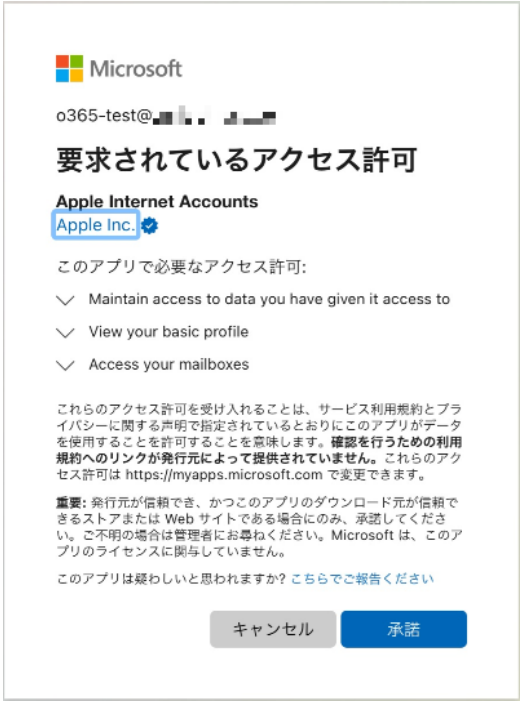
[メール]へSeciossLinkの管理画面でシングルサインオン設定を実施したドメインユーザを入力し[次へ]をタップします。



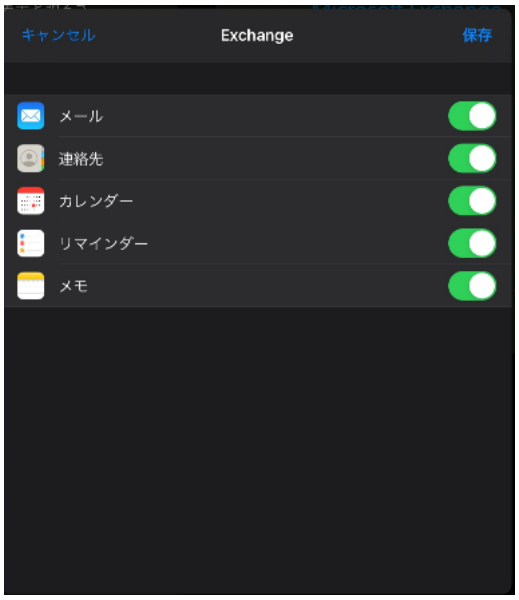
Exchangeへのサインインで[サインイン]をタップします。

証明書認証がバックグラウンドで実行され、成功するとSeciossLinkのログイン画面に転送されます。

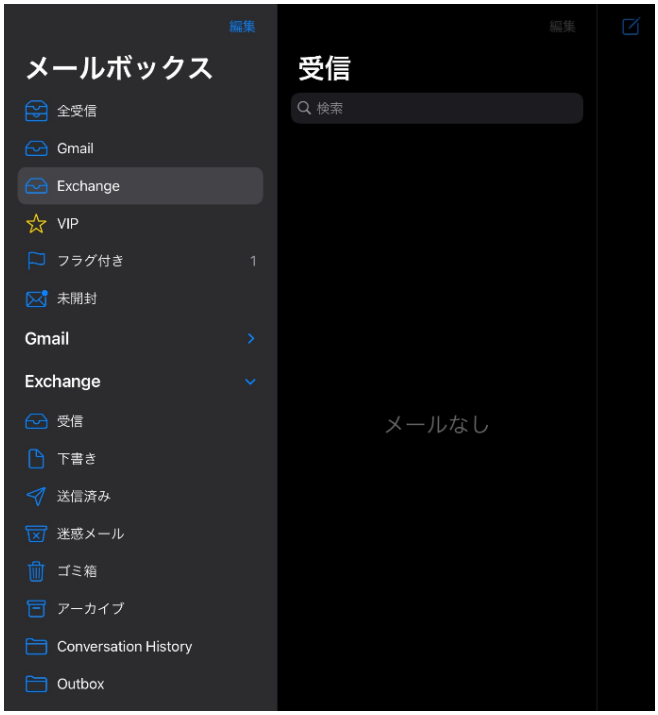
SeciossLinkでのログインパスワードを入力し、[ログイン]をタップするとログインが完了しアクセス権の許諾の画面が表示されるので[承諾]をタップします。



Exchangeアカウントの紐づけ画面が表示されるので必要に応じて変更し[保存]してください。



以上でExchangeへのログインは終了です。
メールアプリを起動するとExchangeアカウントのメールが確認できます。



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。

■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

■SeciossLinkに関するお問い合わせ

株式会社セシオス

Tel:　03-6877-5217

Mail:　slink-jcch@secioss.co.jp

管理者ガイド：

https://seciosslink.com/manual/manual_cate/managementguide

ユーザガイド：

https://seciosslink.com/manual/manual_cate/userguide