# 【iOS 版】

# Secure Access Client 接続手順

順天堂大学

浦安キャンパス情報ネットワーク管理室

2023/9/1

# 目次

# 1 はじめに

本手順書は iOS 端末から学内ネットワークへ VPN 接続するための手順書です。
VPN ソフトウェアのインストールから学内専用ページへのログインまでの手順を記載しています。

## 1.1 必要なソフトウェア

- **Web ブラウザ**
  任意のブラウザで構いません。

- **Secure Access Client**
  App Store ストアよりインストールしてください。
  ※インストール手順は手順 2.ソフトウェアのインストールに記載しています。

- **Google Authenticator（iOS）**
  App Store ストアよりインストールしてください。
  ※インストール手順は手順 2.ソフトウェアのインストールに記載しています。
  ※Android 版 Google Authenticator（Google 認証システム）をご利用の場合は iOS での「Google Authenticator」のインストールは不要です。

# 2 ソフトウェアのインストール

App Store ストアより「Secure Access Client」および「Google Authenticator」をインストールします。
既に両方のアプリのインストールが済んでいる方は手順 3.ソフトウェアのセットアップへ進んでください。

## 2.1 Secure Access Client のインストール

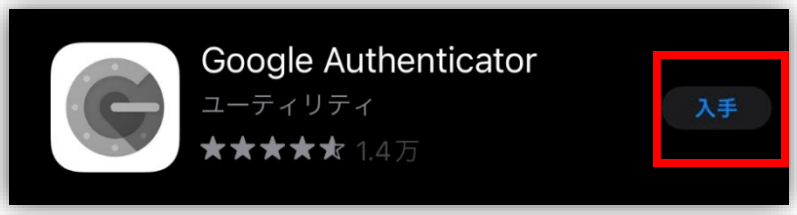
「Secure Access Client」のインストールを行います。
既にアプリをインストール済みの方は手順 2.2 Google Authenticator のインストールへ進んでください。
「App Store」を開き「Secure Access Client」を検索してインストールしてください。


## 2.2 Google Authenticator のインストール

**※本郷キャンパスの学内専用ページへアクセスる際に必要なアプリです。**

「Google Authenticator」のインストールを行います。
既にインストール済み、もしくは Android 版 Google 認証システム（Google Authenticator）をインストール済みの方は手順 3. ソフトウェアのセットアップに進んでください。

「App Store」を開き「Google Authenticator」を検索してインストールしてください。




**以上で必要なソフトウェアのインストールは完了です。**

# 3 ソフトウェアのセットアップ

Secure Access Client および 2 要素認証のセットアップを行います。
既に両方のセットアップが完了している方は手順 4.学内専用ページへのログインへ進んでください。

## 3.1 Secure Access Client のセットアップ

「Secure Access Client」のセットアップを行います。
「Secure Access Client」のセットアップが完了している方は手順 3.2 2 要素認証のセットアップへ進んでください。

① 手順 2.1 でインストールした「Secure Access Client」アプリを開きます。

② 「企業 E メールまたは URL」欄に、下記URLをコピー＆ペーストで入力してください。
【浦安キャンパス】https://secure.nurs.juntendo.ac.jp/
【本郷キャンパス】https://pulse.juntendo.ac.jp/gakunai

③ 入力後「接続」をタップします。
※コピー＆ペーストするとスペース（空白）が入る可能性がありますのでご注意ください。

④　接続先の追加 画面表示されますので、画面下部にある「追加」をタップします。

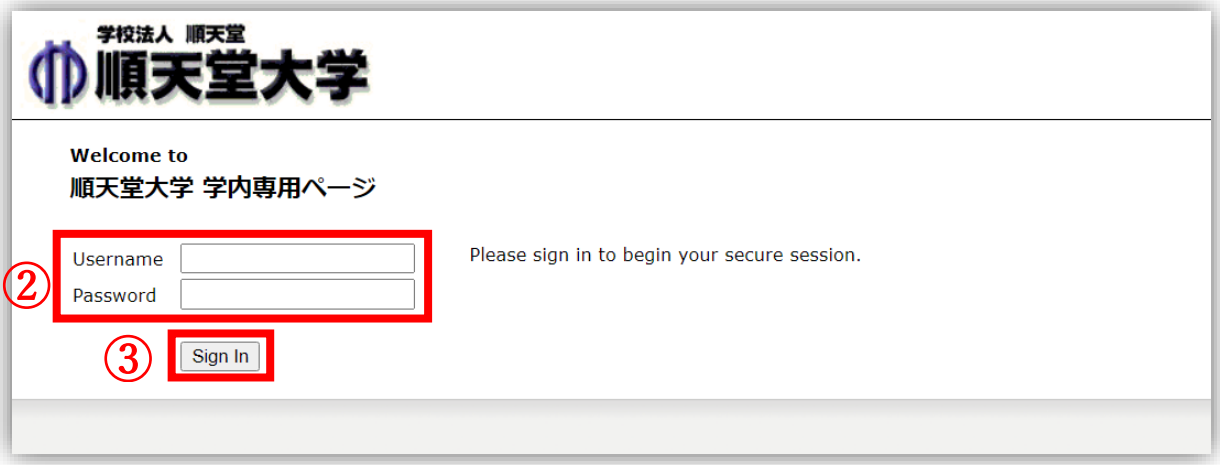

⑤　下記ダイアローグが表示されますので「許可」をタップのうえパスコードを入力します。

## 3.2 2 要素認証のセットアップ

2 要素認証のセットアップを行います。
既に「Google Authenticator」にて 2 要素認証のセットアップ済み、もしくは Android 版 Google 認証システム（Google Authenticator）にて 2 要素認証のセットアップ済みの方は手順 4. 学内専用ページへのログインに進んでください。

① PC のブラウザから https://pulse.juntendo.ac.jp/gakunai へアクセスしてください
※PC のブラウザを使用しない場合は手順 5. iOS 端末のみを使用した 2 要素認証を参照してください。
※学内 LAN、法人 LAN、ゲスト Wi-Fi（hongo-guest）からはアクセスできません。

② Username に順天堂メールのユーザー名(@juntendo.ac.jp を除いた部分)、Password に順天堂メールのパスワードを入力してください。
③ 「Sign In」をクリックします。正常にログインできると 2 要素認証登録のための QR コードが表示されます。




④ QR コードが表示されたら、手順 2.2 でインストールした「Google Authenticator」アプリを開いてください。


⑤ 「Google Authenticator」にアカウントを追加します。

初めて「Google Authenticator」をインストールした方は画面下部の「開始」をタップし
1 つ目のアカウントのセットアップから「QR コードをスキャン」をタップします。

既に「Google 認証システム」をご利用の方は、画面下部の「＋」アイコンをタップし「QR コードをスキャン」をタップしてください。

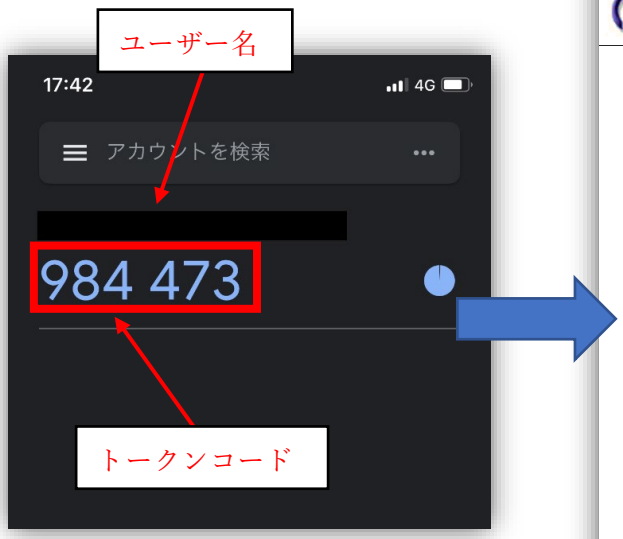
⑥　③の「Sign In」後に表示された QR コードを読み取ってください。

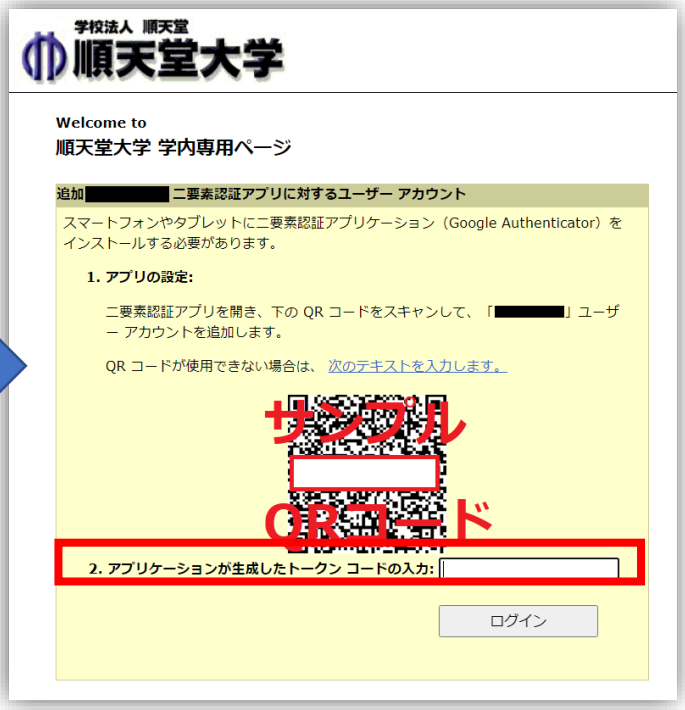

⑦ 正常に読み取れると「アカウントを追加しました」と表示されますので、画面中部の「アカウントを追加」をタップしてください。


⑧ ③で表示された QR コードの画面下部にある「2.アプリケーションが生成したトークンコードの入力：」に入力し、「ログイン」をクリックしてください。

※認証コードは 30 秒毎に更新されます。更新されるまでにトークンコード入力しログインをタップしてください。

※5 回入力に失敗するとアカウントがロックされます。ロックされた場合は情報センターまでお問合せください。




以上でセットアップは完了です。

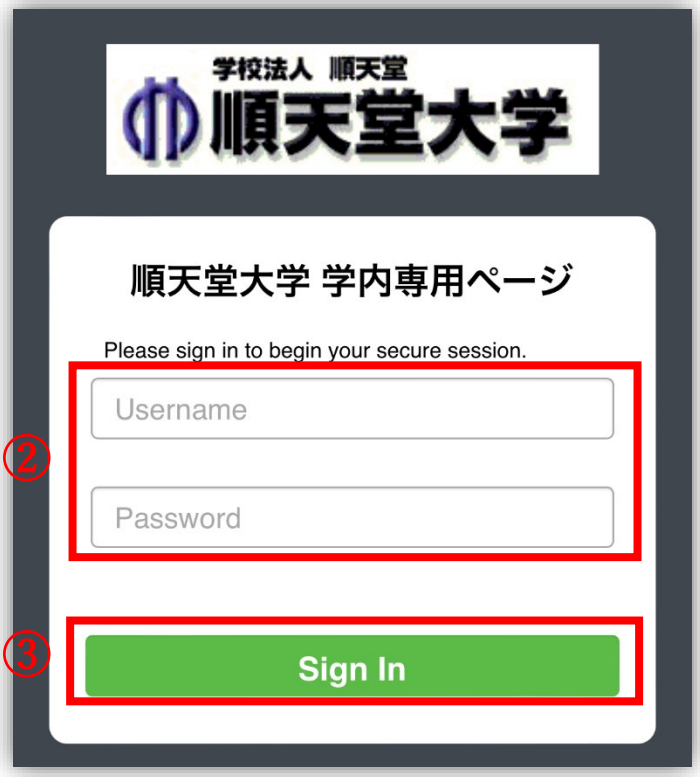
# 4 学内専用ページへのログイン

セットアップを行った「Secure Access Client」と「Google 認証システム」を利用し、学内専用ページへログインします。

① 手順 3.1 Secure Access Client のセットアップで追加した接続先をタップして「接続」をタップしてください。


② Username に順天堂メールのユーザー名(@juntendo.ac.jp を除いた部分)、Password に順天堂メールのパスワードを入力してください。

③ 「Sign In」をタップします。



④　認証コードが求められるので手順 3.2 でセットアップしたアカウントのトークンを確認し「認証コード」へ入直してください。

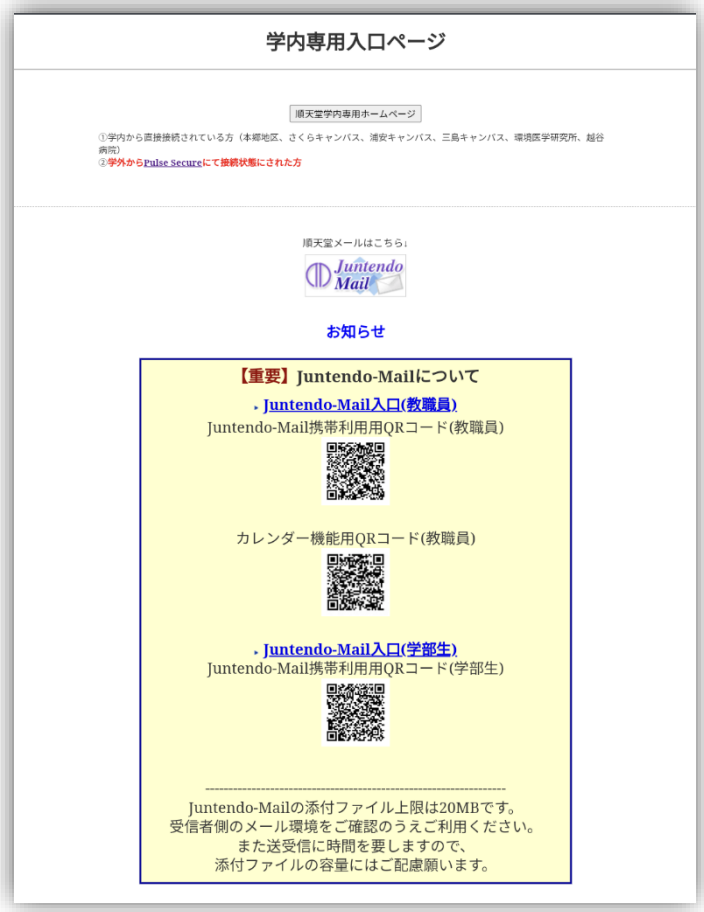
⑤　認証コードを入力し、ログインをタップしてください。

※認証コードは 30 秒毎に更新されます。更新されるまでにトークンコード入力しログインをタップしてくだい。

※5 回入力に失敗するとアカウントがロックされます。ロックされた場合は情報センターまでお問合せください。


⑥　下記画面になれば接続完了となります。

⑦ ブラウザ（Chrome など）を起動し、以下 URL から学内専用ホームページへアクセスして下さい。合わせてブラウザへのブックマーク（お気に入り）登録してください。
https://www.juntendo.ac.jp/private/



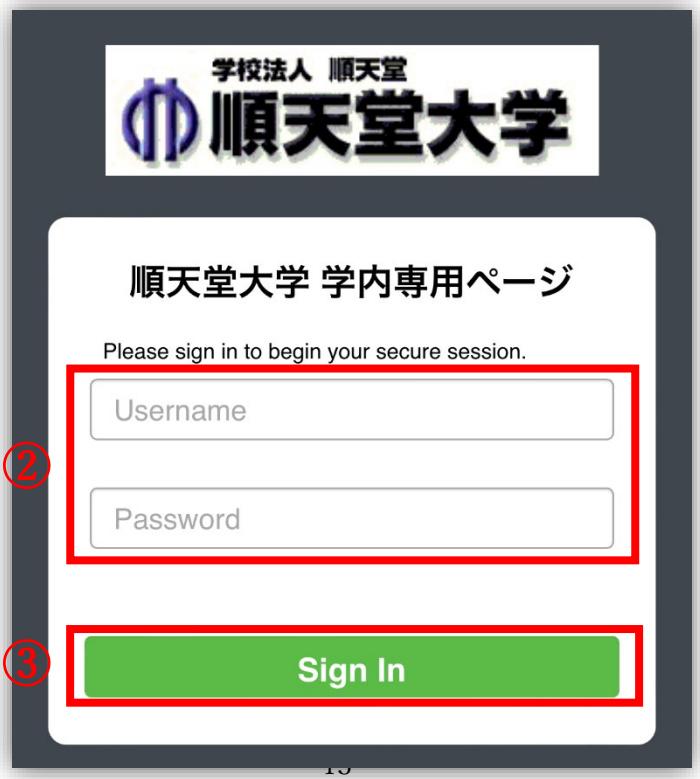

⑧ ログアウトする場合は、「Secure Access Client」アプリの URL をタップして「切断」をタップします。再度ログインする場合は、「Secure Access Client」のアプリ起動し本項の①から実施してください。

# 5 iOS 端末のみを使用した 2 要素認証

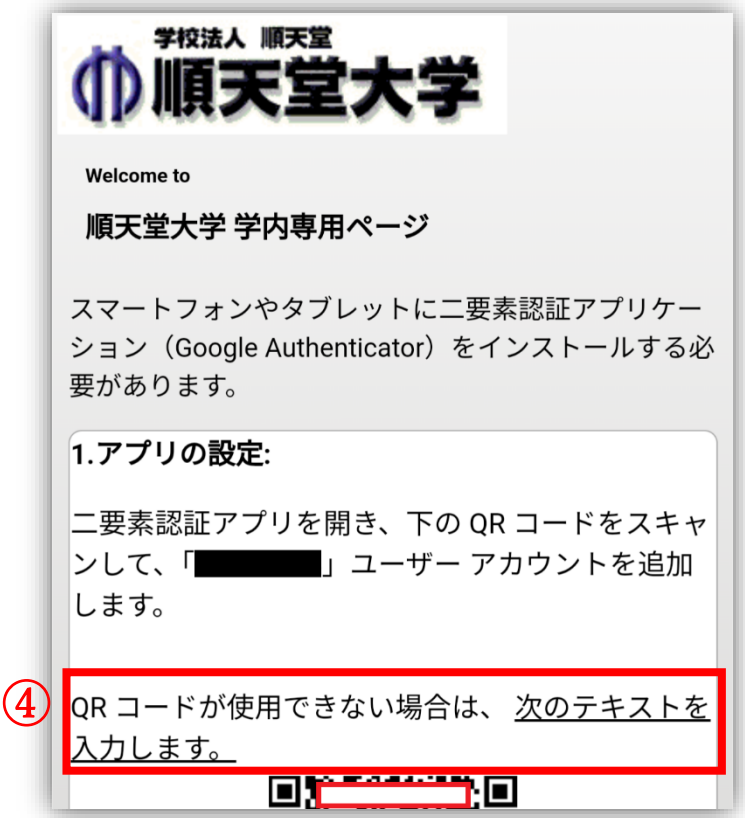
① 手順 3.1 Secure Access Client のセットアップで追加した接続先 URL をタップして「接続」をタップしてください。


② Username に順天堂メールのユーザー名(@juntendo.ac.jp を除いた部分)、Password に順天堂メールのパスワードを入力してください。

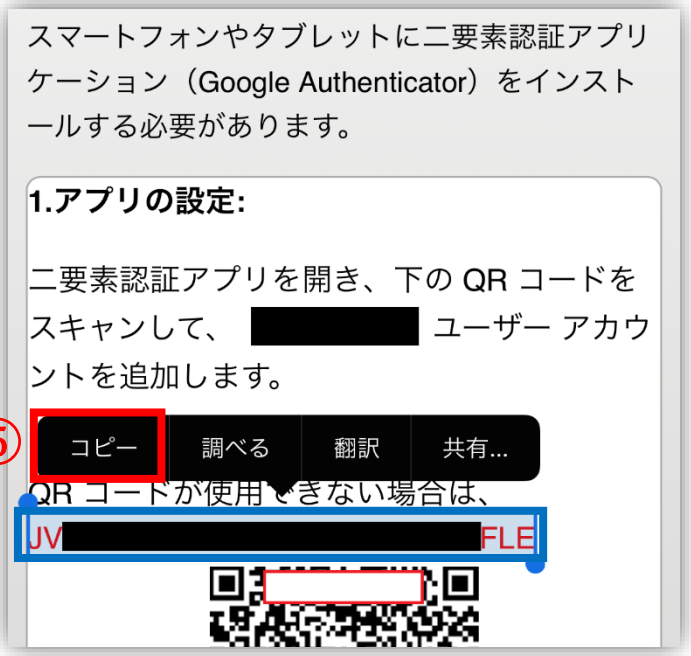
③ 「Sign In」をタップします。



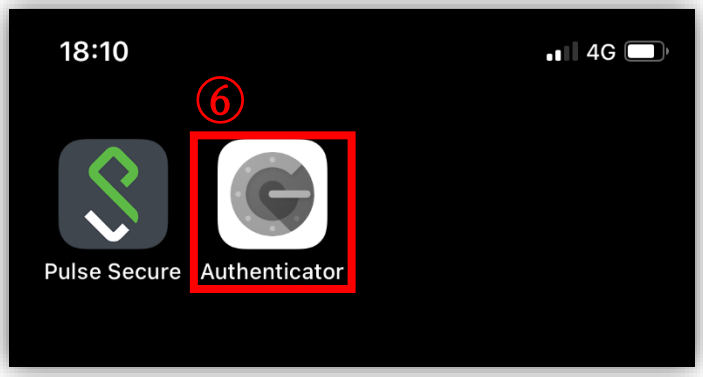
④　その他の認証情報登録ページが表示されますので「次のテキストを入力します。」をタップしてください。




⑤　表示された文字列（青枠）をコピーしてください。
※セキュリティのため以下の画像では文字列を隠してあります。



⑥　手順 2.2 でインストールした「Google Authenticator」アプリを開きます。




⑦　「Google Authenticator」にアカウントを追加します。

初めて「Google Authenticator」をインストールした方は画面下部の「開始」をタップし 1 つ目のアカウントのセットアップから「セットアップキーを入力」をタップします。

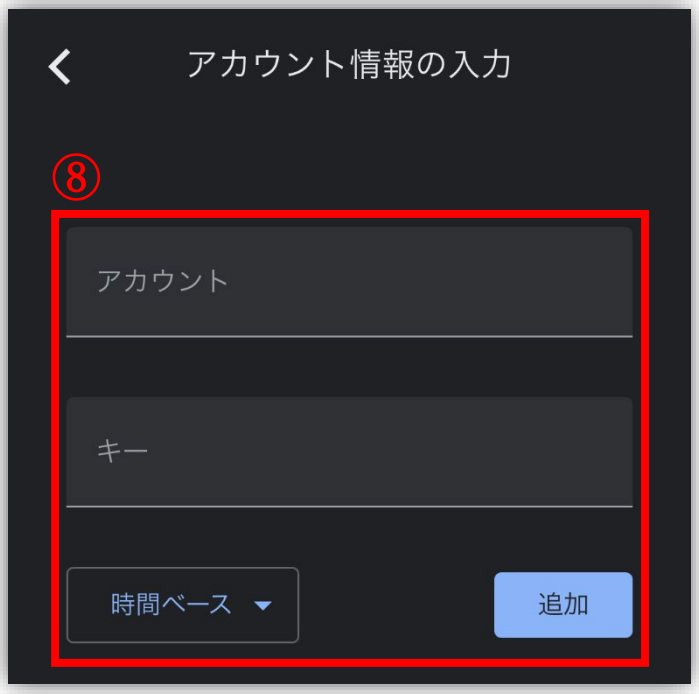
既に「Google Authenticator」を利用している方は画面右下の「＋」アイコンをタップし、「セットアップキーを入力」をタップします。

⑧　アカウント情報の入力画面より「アカウント名」と「キー」を入力し、追加をタップします。

アカウント名：任意の文字

キー：⑤でコピーした文字列

キーの種類：時間ベース




⑨　アカウントを追加完了後下記画面が表示されます。

⑩　表示されたトークンを確認し「Secure Access Client」アプリを開いてください。
確認したトークンを下部にある「3.アプリケーションが生成したトークンコードの入力：」に入力し、「ログイン」をタップしてください。
※認証コードは 30 秒毎に更新されます。更新されるまでにトークンコード入力しログインをタップしてくだい。
※5 回入力に失敗するとアカウントがロックされます。ロックされた場合は情報センターまでお問合せください。


⑪　下記画面になれば接続完了となります。


接続が完了したら手順 4.学内専用ページへのログインの⑦を参照してください。