【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	はし	じめに	2
	1.1	必要なソフトウェア	2
2	ソフ	フトウェアのインストール	3
	2.1	Secure Access Client のインストール	3
	2.2	Google Authenticator のインストール	3
3	ソフ	 フトウェアのセットアップ	4
	3.1	Secure Access Client のセットアップ	4
	3.2	2 要素認証のセットアップ	6
4	学内	内専用ページへのログイン	.10
5	iOS	S 端末のみを使用した 2 要素認証	.13

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<u>手順 2.ソフトウェアのインストール</u>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<u>手順 3.ソフトウェアのセットアップ</u>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<u>手順 2.2 Google Authenticator のインストール</u>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<u>手順 3.2 2 要素認証のセットアップ</u>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。

÷	接続の追加	
以下の必須 を追加しま	フィールドに入力し、ボタンをクリック す。	して接続
タイプ		
Policy Se	cure (UAC) または Connect Secure (VF	PN)
接続名		
(オプショ:	ン)	
URL *		
https://pu	Ilse.juntendo.ac.jp/gakunai	
ユーザー名		
(オプショ:	ン)	
認証タイ	プ	>
L11L		
(オプション	ン)	
ロール		
/		

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。

(4)



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<u>手順4. 学内専用ページ</u> へのログインに進んでください。

- PC のブラウザから <u>https://pulse.juntendo.ac.jp/gakunai</u> ヘ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<u>手順 5. iOS 端末のみを使用した 2 要素認証</u>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。
- 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。

1	*校法人 順天堂 順天堂大学 Welcome to 順天堂大学 学内専用ページ	
2	Username Password 3 Sign In	Please sign in to begin your secure session.

	Welcome to 順天堂大学 学内専用ページ	
	追加 二要素認証アプリに対するユーザー アカウント	
	スマートフォンやタブレットに二要素認証アプリケーション(Google Authenticator)を インストールする必要があります。	
	1. アプリの設定:	
	二要素認証アプリを開き、下の QR コードをスキャンして、「■■■■■■」ユーザ ー アカウントを追加します。	
	QR コードが使用できない場合は、 次のテキストを入力します。	
	2. アプリケーションが生成したトークンコードの入力:	

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。

Welcome to 順天堂大学 学内専用ページ	
追加 二要素認証アプリに対するユーザー アカウント	
スマートフォンやタブレットに二要素認証アプリケーション(Google Authenticator)を インストールする必要があります。	
1. アプリの設定:	
ニ要素認証アプリを開き、下の QR コードをスキャンして、「 ローロー 」ユーザ ー アカウントを追加します。	
QR コードが使用できない場合は、 <u>次のテキストを入力します。</u>	
2. アプリケーションが生成したトークンコードの入力:	まない場合は、 <u>ROT+ストを入れします。</u> まない場合は、 <u>ROT+ストを入れします。</u> ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・

 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。



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 ヘログインします。

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。

	((0)) アクティブな接続は ありません		
	接続		Ð
	スワイプおよびタップ (o) して接続/切断		
1	pulse.juntendo.ac.jp/gakunai	((0))	:

- 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。

	●順天堂大学		
	順天堂大学 学内専用ページ		
	Please sign in to begin your secure session.		
2	Username		
	Password		
3	Sign In		

- 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。
- ③ 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

Pulse Connect Secure - その他の認証 情報ページ		
Welcome to 順天堂大学 学内専用ページ		
デバイスで二要素認証アプリを開き、認証コードを表示して、 ID を確認します。		
テハイスに対するアクセス権限がない場合は、以前に保存した バックアップ コードのいずれかを使用してください。		
認証コード: トークン:		
ログイン		

⑥ 下記画面になれば接続完了となります。

合せください。

1 アクティブな接続 ● pulse.juntendo.ar	c.jp/g
接続	ŧ
スワイプおよびタップ 🕪 して接続/切断	
pulse.juntendo.ac.jp/gakunai	:

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

 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。

	((の)) アクティブな接続は ありません		
	接続		Ð
	スワイプおよびタップ (m) して接続/切断		
1	pulse.juntendo.ac.jp/gakunai	((0))	:

- 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) $\lceil \text{Sign In} \rfloor \epsilon \beta \gamma \tau l \sharp t$.

	順天堂大学 学内専用ページ
2	Please sign in to begin your secure session.
2	Password
3	Sign In

 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。

	大学
Welcome to 順天堂大学 学内専用	ページ
スマートフォンやタブ ション(Google Auther 要があります。	レットに二要素認証アプリケー nticator)をインストールする必
1.アプリの設定:	
二要素認証アプリを シして、「 」 しま す。	[]] き、下の QR コードをスキャ ユーザー アカウントを追加
④ QR コードが使用でき <u>入力します。</u>	ない場合は、 <u>次のテキストを</u>

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

く アカウント情報の入力	
8	
アカウント	
<i>+</i> -	
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。



① 下記画面になれば接続完了となります。

1 アクティブな接続 pulse.juntendo.a	c.jp/g
接続	Ð
スワイプおよびタップ (o) して接続/切断	
pulse.juntendo.ac.jp/gakunai	:

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。