

【Android 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	2
1.1	必要なソフトウェア	2
2	ソ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 認証システムのインストール	3
3	ソ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	5
4	学内専用ページへのログイン	9
5	Android 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 Android 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

Google Play 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 認証システム (Android) **※本郷キャンパス学内専用ページへアクセスする際に必要です。**

Google Play 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。

※iPhone 版 Google 認証システム (Google Authenticator) をご利用の場合は Android での「Google 認証システム」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

Google Play ストアより「Secure Access Client」および「Google 認証システム」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。

既にインストール済みの方は[手順 2.2 Google 認証システムのインストール](#)へ進んでください。

「Google Play ストア」を開き「secure access client」を検索してインストールしてください。



Ivanti Secure Acces...
Pulse Secure

インストール

2.2 Google 認証システムのインストール

「Google 認証システム」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 iPhone 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。

「Google Play ストア」を開き「Google 認証システム」を検索してインストールしてください。



Google 認証システム
Google LLC

インストール

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。

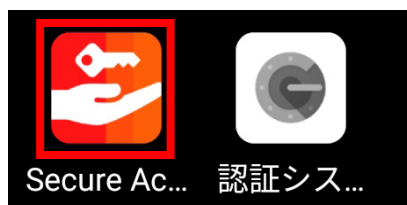
既に両方のセットアップが完了している方は[手順 4.学内専用ページへのログイン](#)へ進んでください。

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、該当の URL（下記参照）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、接続名に「順天堂学内専用ページ」と入力し画面下部にある「追加」をタップします。

← 接続の追加

以下の必須フィールドに入力し、ボタンをクリックして接続を追加します。

タイプ

Policy Secure (UAC) または Connect Secure (VPN)

接続名

順天堂学内専用ページ

URL *

https://pulse.juntendo.ac.jp/gakunai

ユーザー名

(オプション)

認証タイプ

パスワード

レルム

(オプション)

ロール

(オプション)

追加 接続

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 認証システム」にて2要素認証のセットアップ済み、もしくはiPhone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. Android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。

Welcome to
順天堂大学 学内専用ページ

② Username
Password

③

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:

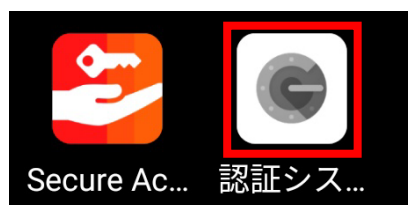
二要素認証アプリを開き、下の QR コードをスキャンして、「**順天堂大学**」ユーザー アカウントを追加します。

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。](#)

サンプル QRコード

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 認証システム」アプリを開いてください。



5 「Google 認証システム」にアカウントを追加します。

初めて「Google 認証システム」をインストールした方は画面下部の「使ってみる」をタップし 1 つ目のアカウントのセットアップ画面から「QR コードをスキャン」をタップします。

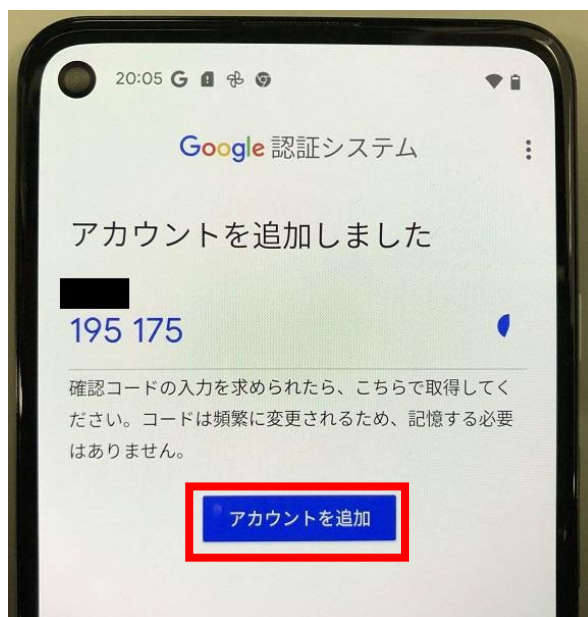
既に「Google 認証システム」をご利用の方は、画面下部の「+」アイコンをタップし「QR コードをスキャン」をタップしてください。



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。



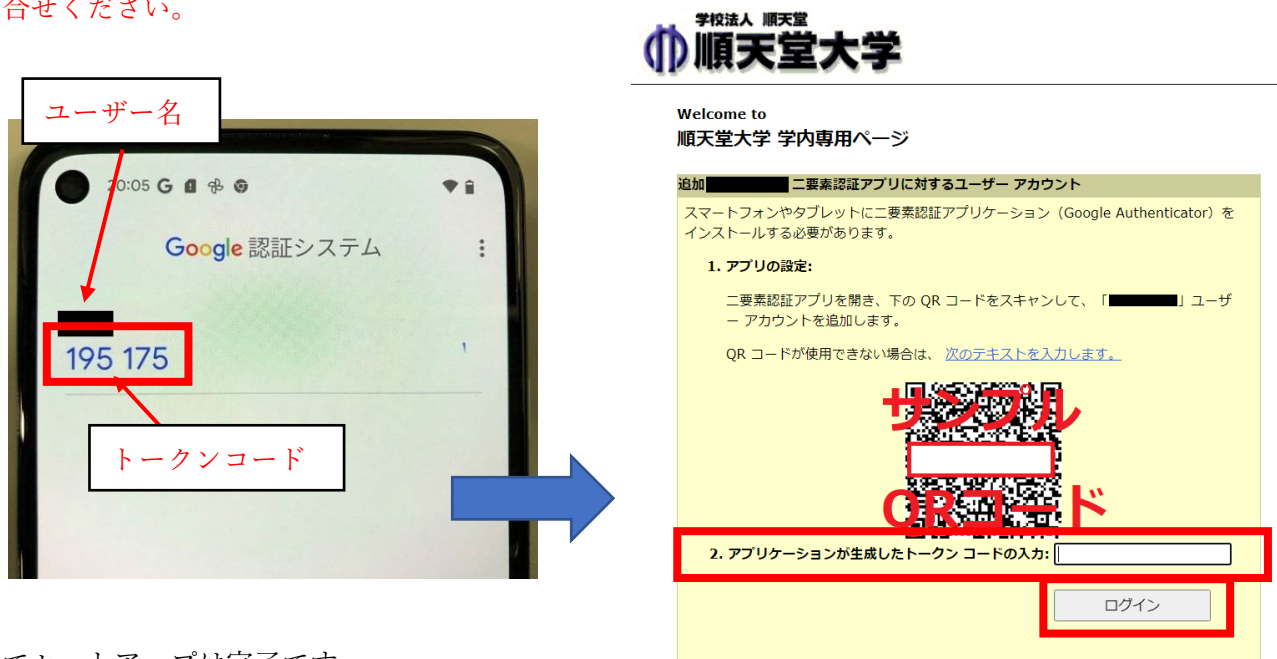
- 7 正常に読み取れると「アカウントを追加しました」と表示されますので、画面中部の「アカウントを追加」をタップしてください。



- 8 ③で表示された QR コード画面の下部にある「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⑦で追加した「Google 認証システム」のトークンコード入力し、「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の「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 2 要素認証アカウントのトークンを確認し「認証コード」へ入力してください。
- 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。

接続
Pulse Connect Secure - その他の認証情報ページ

学校法人 順天堂
順天堂大学

Welcome to
順天堂大学 学内専用ページ

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。

デバ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

最初に接続するとき以下画面が表示されることがあります。
「OK」をタップして下さい。

接続リクエスト

Secure Access がネットワークトラフィックを監視するため VPN 接続をセットアップしようとしています。信頼できるソースである場合にのみ許可してください。

VPN がアクティブになると画面の上部に  が表示されます。

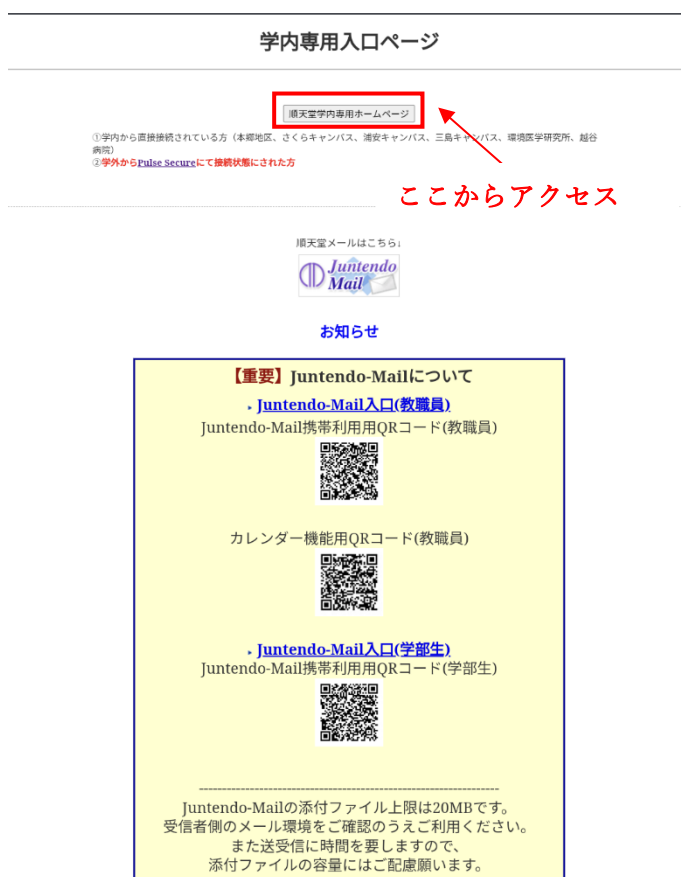
キャンセル OK

- 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 からポータルサイト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://portal.med.juntendo.ac.jp/>



- 8 ログアウトする場合は、「Secure Access Client」アプリの順天堂学内専用ページをタップして「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 Android 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の「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。

接続

学校法人 順天堂
順天堂大学

順天堂大学 学内専用ページ

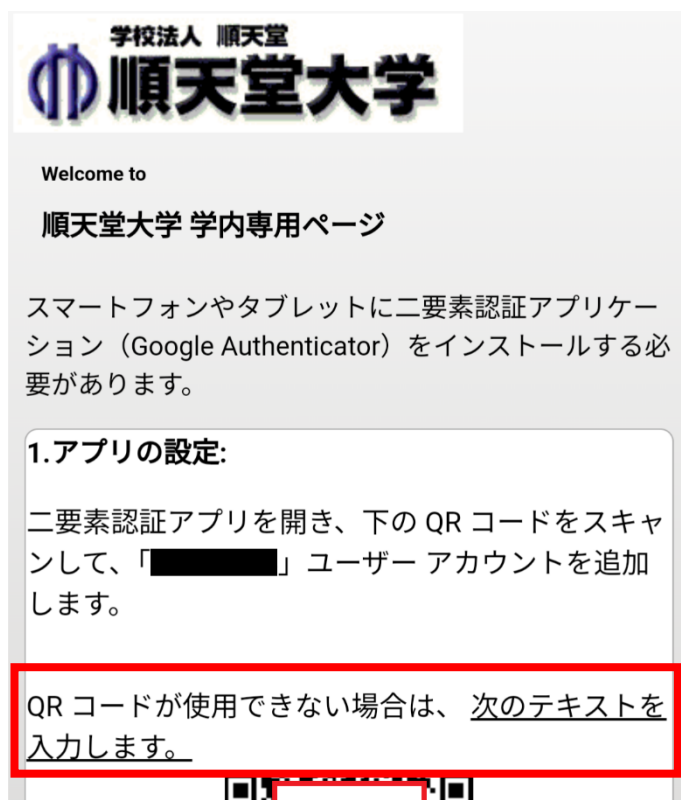
Please sign in to begin your secure session.

Username

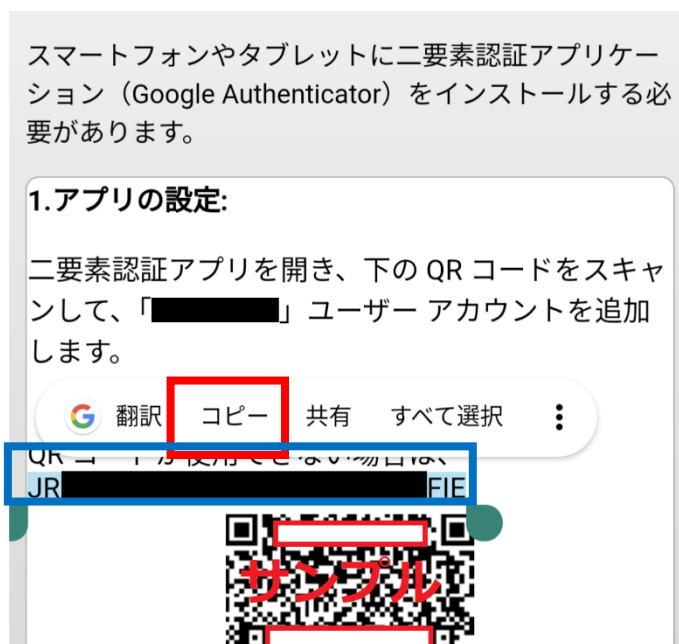
Password

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。



- 5 表示された文字列をコピーしてください。
※文字列は QR コードの上部（下図の青枠）に表示されます。
※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。



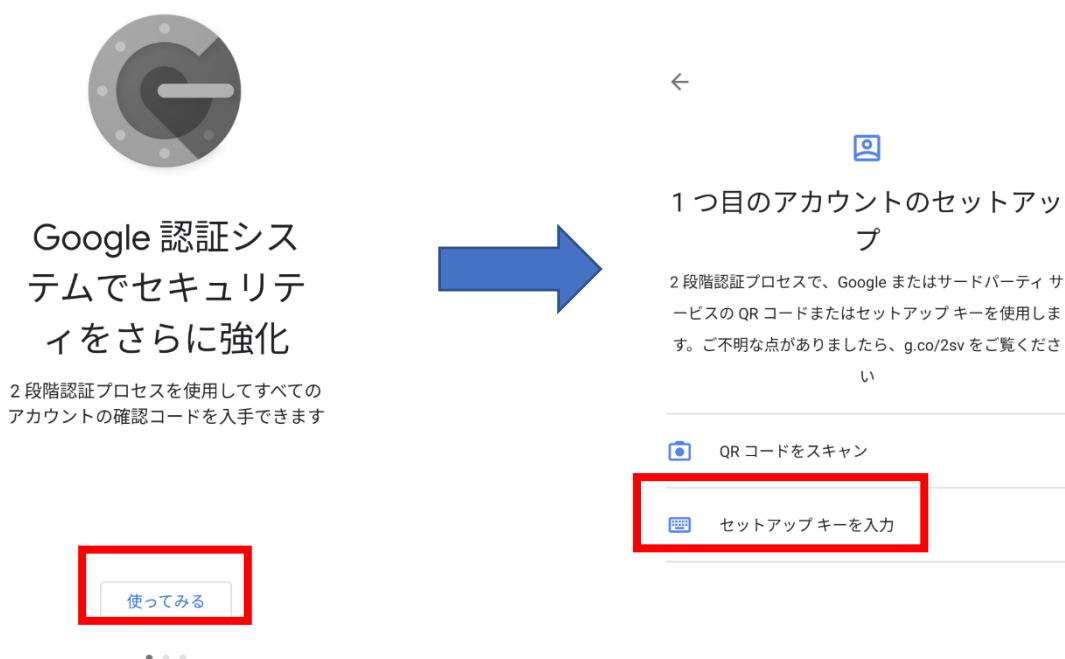
- 6 手順 2.2 でインストールした「Google 認証システム」アプリを開きます。



- 7 「Google 認証システム」にアカウントを追加します。

初めて「Google 認証システム」をインストールした方は画面下部の「使ってみる」をタップし 1 つ目のアカウントのセットアップ画面から「セットアップキーを入力」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「セットアップキーを入力」をタップしてください。

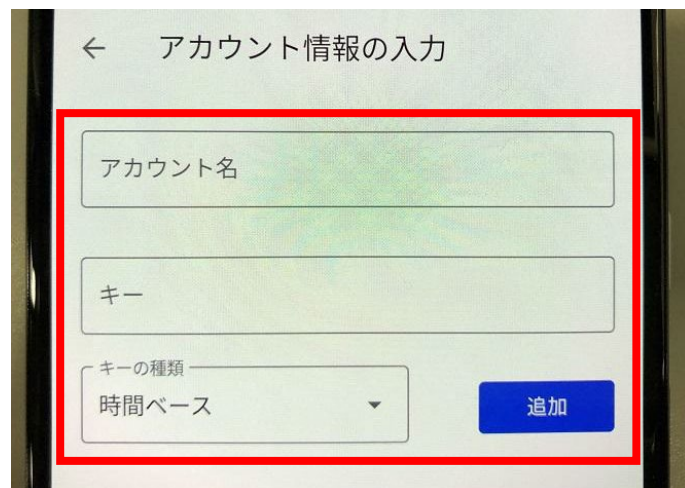


- 8 アカウント情報の入力画面より「アカウント名」と「キー」を入力し、追加をタップします。

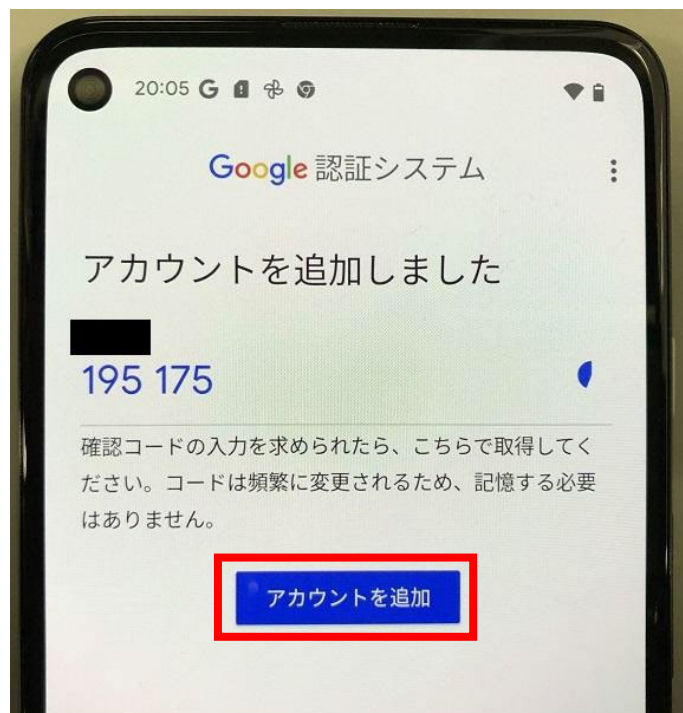
アカウント名：任意の文字

キー：⑤でコピーした文字列

キーの種類：時間ベース



- 9 「アカウントを追加しました」と表示されたら画面中部の「アカウントを追加」をタップしてください。

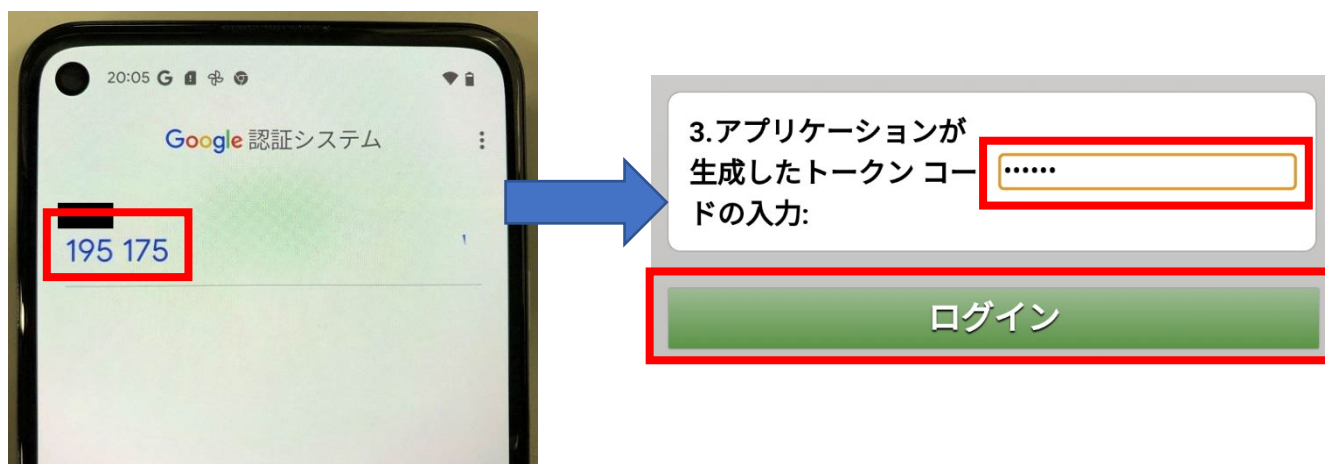


- 10 表示されたトークンを確認し「Secure Access Client」アプリを開いてください。

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。



- 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。