

VPN用二要素認証の設定

2024/2/29版

生研電子計算機室のVPNは、vpn0.iis.u-tokyo.ac.jp から vpn1.iis.u-tokyo.ac.jp に変わります。
vpn1.iis.u-tokyo.ac.jp では二要素認証が必要となります。
mail.iis.u-tokyo.ac.jp の二要素認証とは別のシステムとなりますので、改めて設定をお願いいたします。

VPN用二要素認証の初期設定

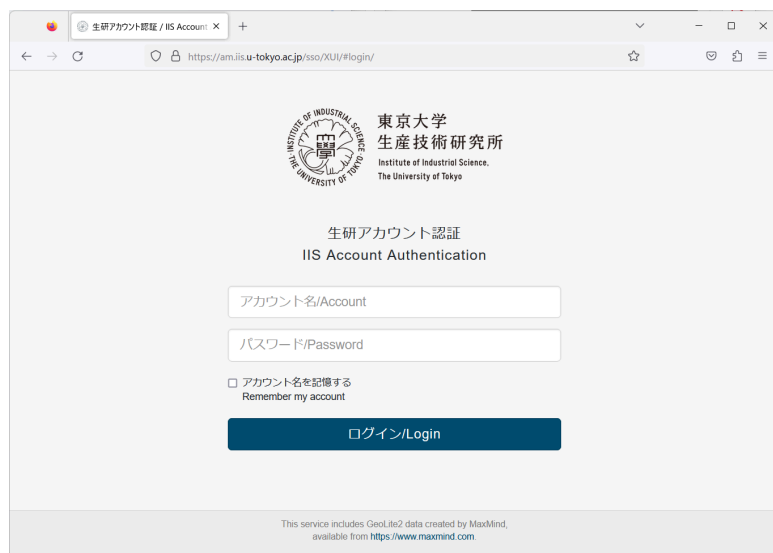
vpn1.iis.u-tokyo.ac.jp にアクセスする前に、以下の設定をお願いいたします。

二要素認証サーバの以下のURLにアクセスしてください。

<https://am.iis.u-tokyo.ac.jp/sso/XUI/#login/&service=TOTPRegistration&ForceAuth=true>

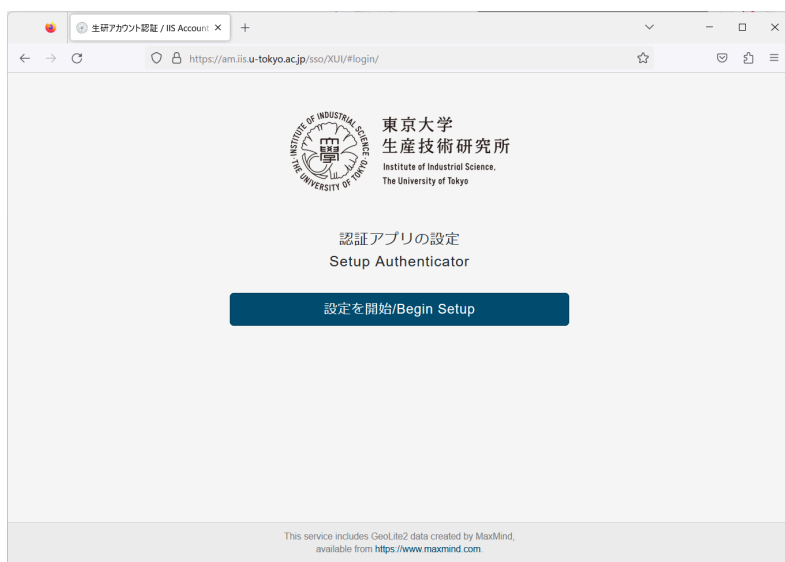
生研アカウントとパスワードを入力してください。

※アカウント名に @iis.u-tokyo.ac.jp は入力しないでください。エラーとなってしまいます。



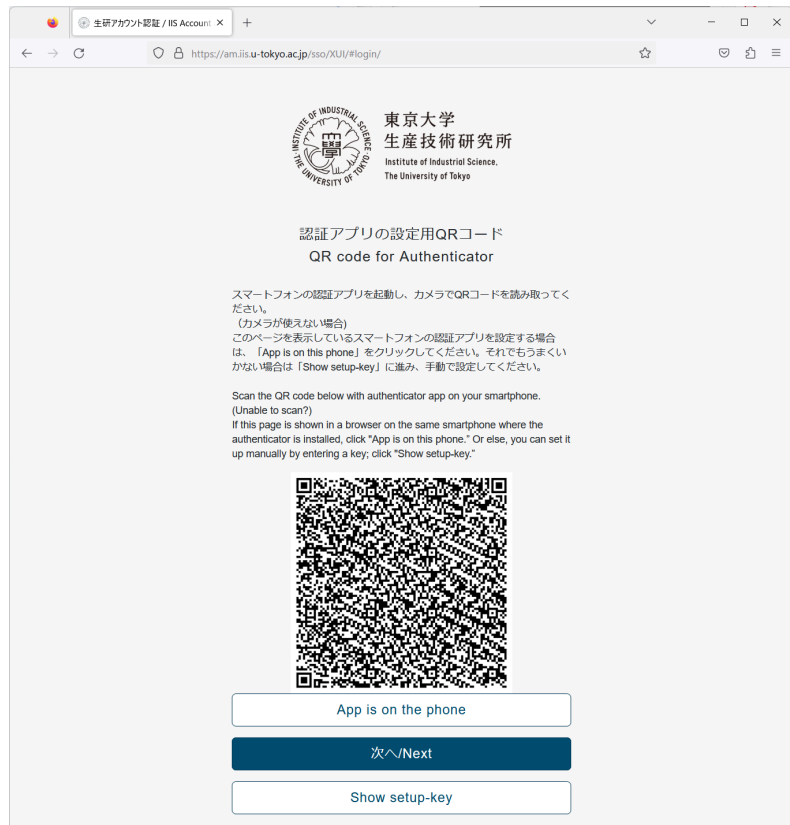
The screenshot shows a web browser window with the URL <https://am.iis.u-tokyo.ac.jp/sso/XUI/#login/>. The page header includes the logo of the Institute of Industrial Science, The University of Tokyo. The main content area is titled "生研アカウント認証" (IIS Account Authentication) and "IIS Account Authentication". It features two input fields: "アカウント名/Account" and "パスワード/Password". Below these fields is a checkbox labeled "アカウント名を記憶する" (Remember my account). A blue "ログイン/Login" button is positioned at the bottom of the form. A small footer note states: "This service includes Geolite2 data created by MaxMind, available from https://www.maxmind.com."

ログインすると、「認証アプリの設定」画面になります。「設定を開始」を選択してください。



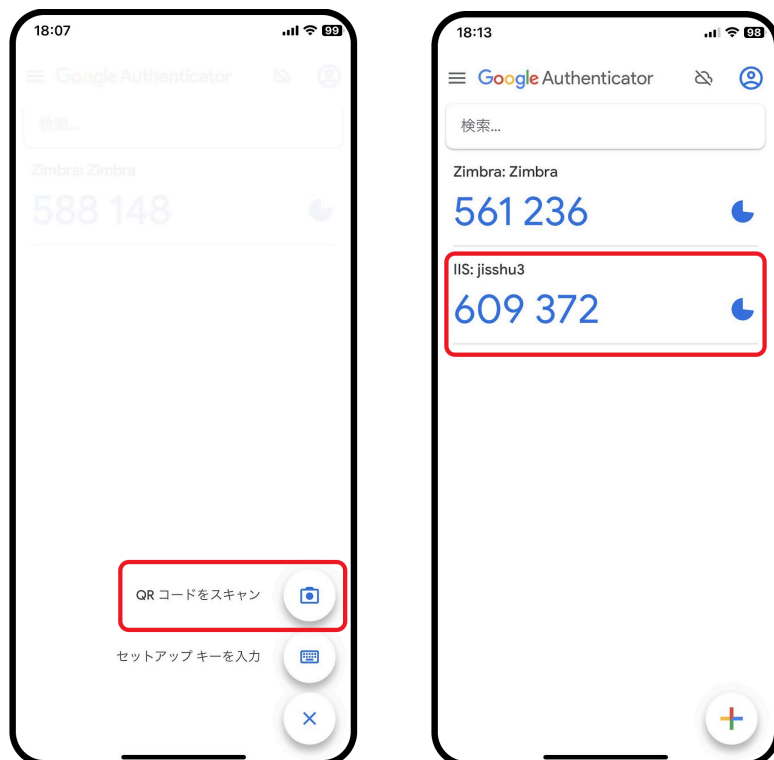
The screenshot shows the same web browser window after login. The page title is "認証アプリの設定" (Setup Authenticator) and "Setup Authenticator". A prominent blue button labeled "設定を開始/Begin Setup" is centered on the page. The footer note remains the same: "This service includes Geolite2 data created by MaxMind, available from https://www.maxmind.com."

QRコードが表示されます。スマートフォンの Authenticator で読み取ってください。ここでは Google Authenticator を使った場合で説明します。



1. スマートフォンでGoogle Authenticatorを起動し、右下の「+」をタップします。
2. 「QRコードをスキャン」を選択し、QRコードを読み込みます。

Google Authenticatorでは、「IIS:アカウント名」でコードが表示されるようになります。



ブラウザ側では、「次へ/Next」を選択してください。
「認証アプリによる二要素認証(TOTP)」の画面になります。
スマートフォン上のコードを入力し、「検証」を選択してください。

東京大学
生産技術研究所
Institute of Industrial Science,
The University of Tokyo

認証アプリによる二要素認証 (TOTP)
2FA with Authenticator (TOTP)

コード/Code

検証/Verify

This service includes GeoLite2 data created by MaxMind,
available from <https://www.maxmind.com>.

検証が成功すると「次回の二要素認証」の画面になります。初回は「いいえ」を選択してください。

東京大学
生産技術研究所
Institute of Industrial Science,
The University of Tokyo

次回の二要素認証
Do you want to skip 2FA next time?

このブラウザでの次回ログイン時には二要素認証を省略しますか？
自分専用の端末でない場合は、「いいえ」を選んでください。（「はい」
を選んだ場合でも一定期間が経過すると再び二要素認証が必要となります。）

Do you want to skip 2FA next time with this browser?
Select "No" if the computer is not for your exclusive use. (Even if you
choose "Yes", 2FA will be required again after a certain period of time has
passed.)

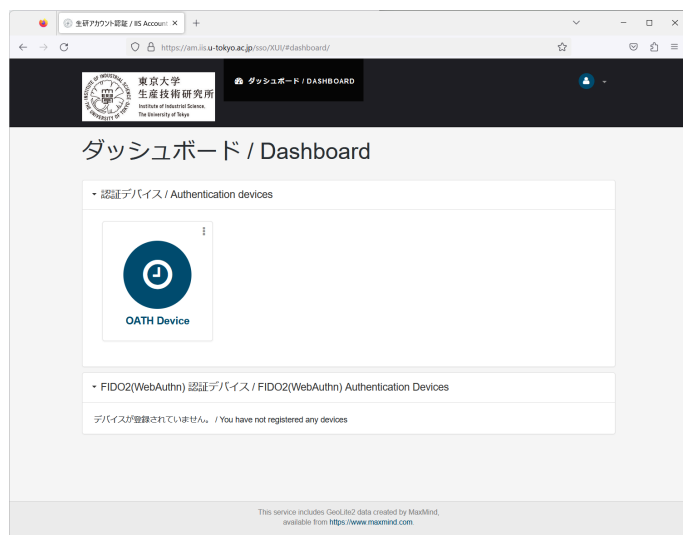
はい/Yes (I'd like to skip)

いいえ/No

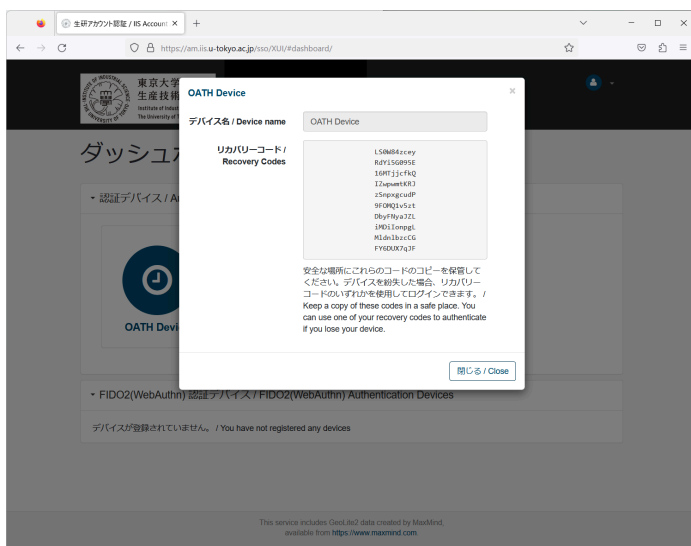
この決定を記憶する
Don't ask this question again

This service includes GeoLite2 data created by MaxMind,
available from <https://www.maxmind.com>.

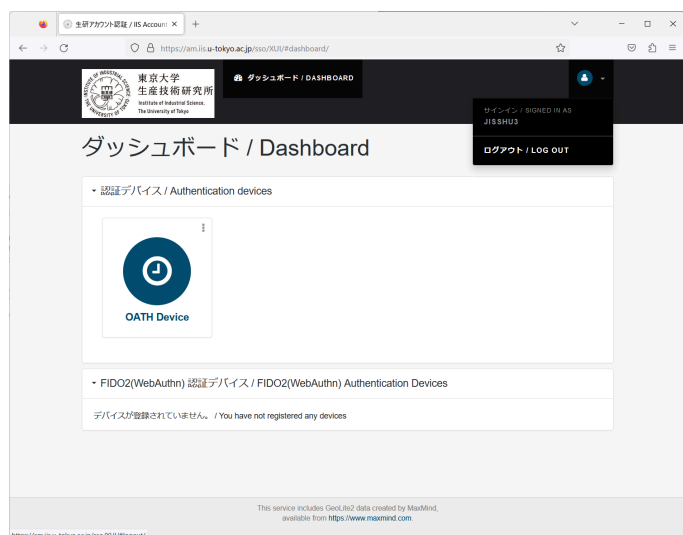
ダッシュボードが表示されます。



「OATH Device」を選択してください。リカバリーコードが10個表示されます。コピーして保管してください。二要素認証のコードを入力する際にリカバリーコードの一つを入力することでログインすることもできます。スマートフォンの紛失、機種変更などの際に二要素認証のリセットをする際にも必要となります。



右上の ▼ から「ログアウト」を選択してください。ログアウト画面になれば、設定完了です。



AnyConnectのインストール

これまで vpn0.iis.u-tokyo.ac.jp や全学VPNを利用して、すでにCisco AnyConnect (Cisco Secure Client) をインストール済みの場合はこの手順は不要です。P.7の「VPNの利用」に進んでください。
まだ AnyConnectをインストールしていない場合は、以下の手順を実施してください。

Android の場合

Google Play Store から Cisco Secure Client をインストールしてください。提供者が、Cisco Systems, Inc. であることを確認してください。

Apple iOS/iPad OS の場合

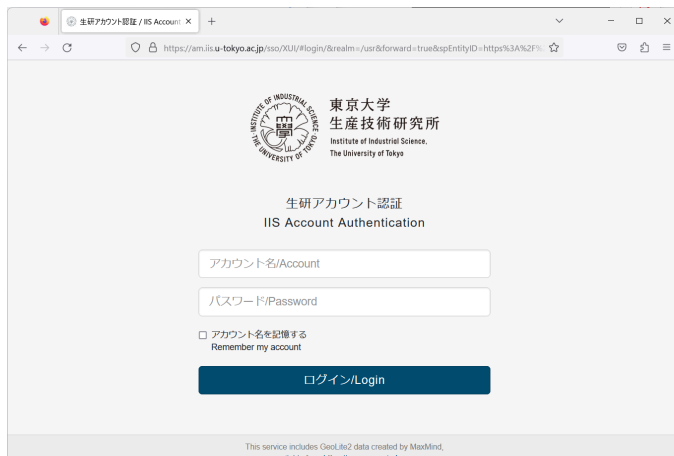
App Store から Cisco Secure Client をインストールしてください。提供者が、Cisco Systems, Inc. であることを確認してください。

Windows, macOS, Linux の場合

以下のURLにアクセスしてください。

<https://vpn1.iis.u-tokyo.ac.jp/>

上記URLにアクセスすると、<https://am.iis.u-tokyo.ac.jp/ss0> の二要素認証画面に移行します。生研アカウント (@iis.u-tokyo.ac.jp は入力しないでください。エラーとなってしまいます)とパスワードを入力し、スマートフォンに表示される二要素認証のコードを入力してください。



生研アカウント認証
IIS Account Authentication

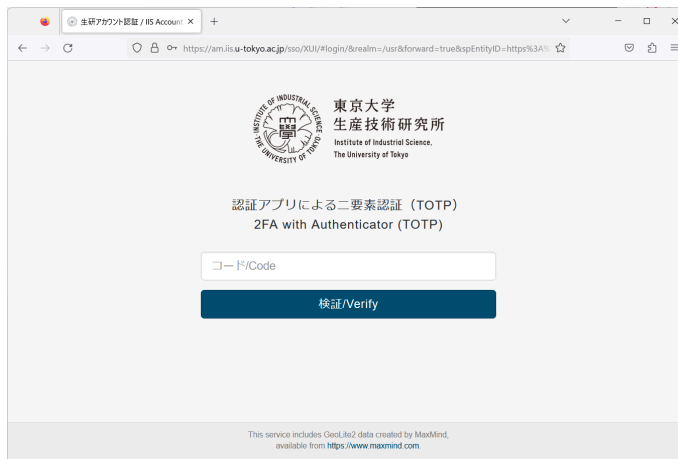
アカウント名/Account

パスワード/Password

アカウント名を記憶する
Remember my account

ログイン/Login

This service includes GeoLite2 data created by MaxMind, available from <https://www.maxmind.com>.



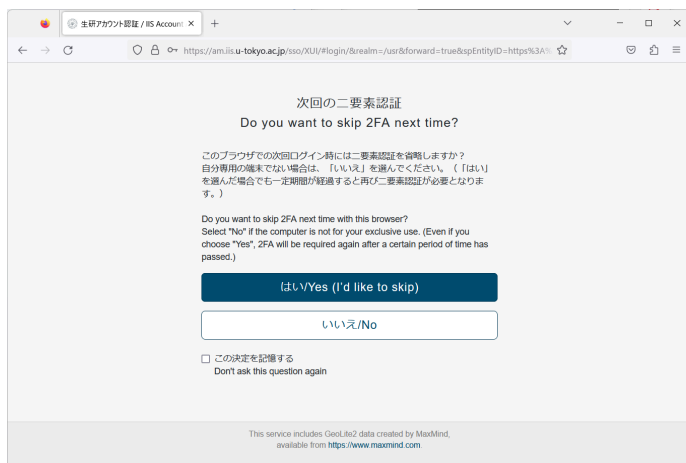
認証アプリによる二要素認証 (TOTP)
2FA with Authenticator (TOTP)

コード/Code

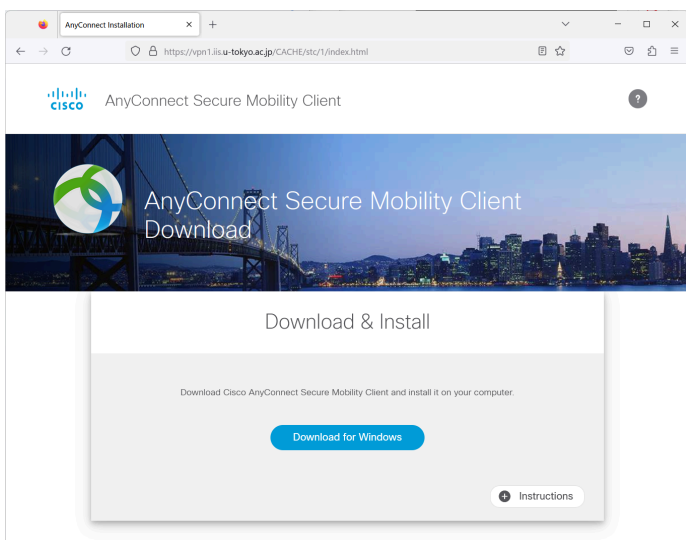
検証/Verify

This service includes GeoLite2 data created by MaxMind, available from <https://www.maxmind.com>.

「次回の二要素認証」の画面では、「いいえ」を選択してください。



AnyConnect のダウンロード画面になります。「Download for ...」をクリックしてダウンロードし、インストールしてください。



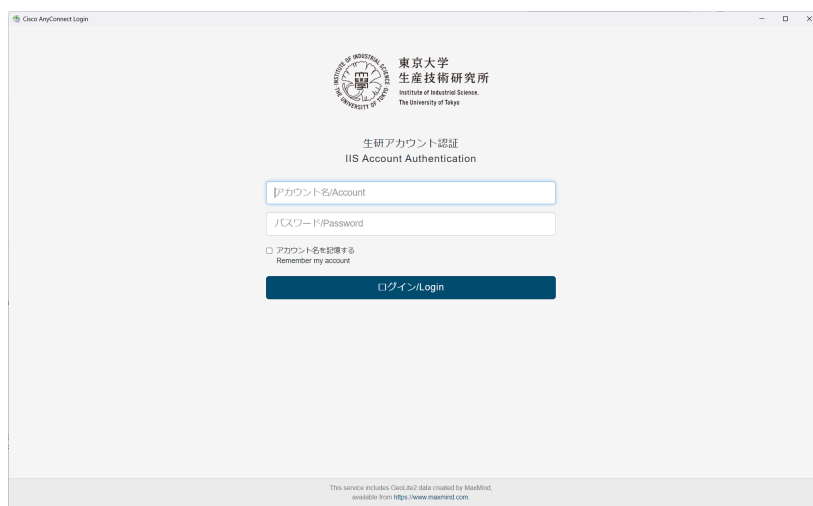
VPNの利用

AnyConnect を起動し、vpn1.iis.u-tokyo.ac.jp と入力します。「Connect」を選択してください。以下はWindows版で説明します。

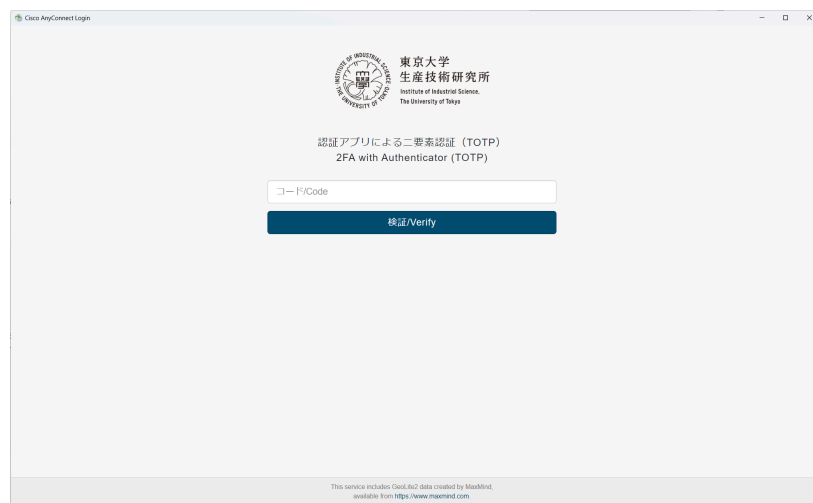


AnyConnect内蔵のブラウザが起動し、「生研アカウント認証」の画面が表示されます。生研アカウントとパスワードを入力してください。

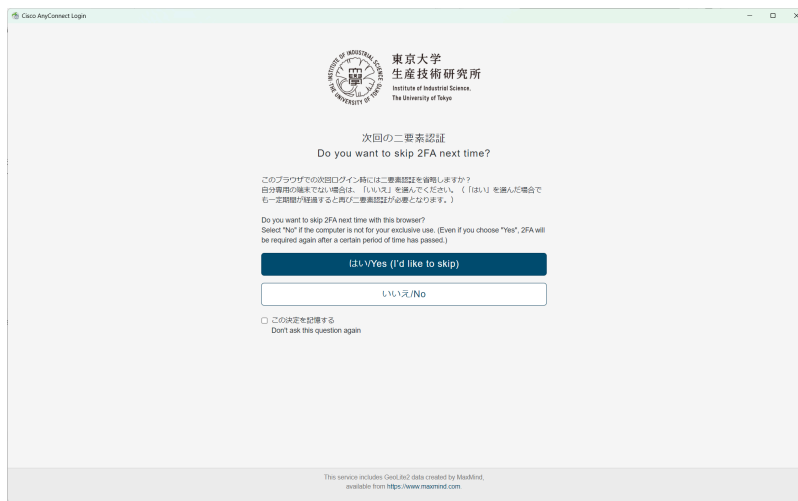
※アカウント名に @iis.u-tokyo.ac.jp は入力しないでください。エラーとなってしまいます。



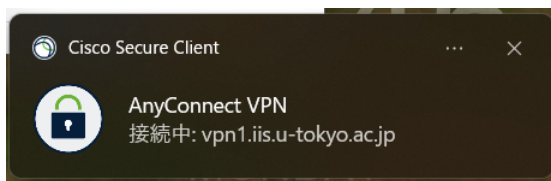
「認証アプリによる二要素認証」の画面になります。スマートフォンのAuthenticatorに表示されるコードを入力して「検証」を選択してください。



「次回の二要素認証」の画面になります。この画面で「はい」を選択すると、同じ端末からのVPNアクセスでは30日間は二要素認証のコード入力が省略されます。自分専用の端末でない場合はかならず「いいえ」を選択してください。



「Connected: vpn1.iis.u-tokyo.ac.jp」と表示され、VPN接続が開始されます。



VPN接続を終了する場合は、AnyConnectのアイコンをクリックし、「切断」を選択します。



二要素認証の再設定が必要な場合

スマートフォンの機種変更、紛失などのために二要素認証の設定を行いたい場合は以下の手順に従ってください。

二要素認証サーバにログインしてください。

<https://am.iis.u-tokyo.ac.jp/sso/>

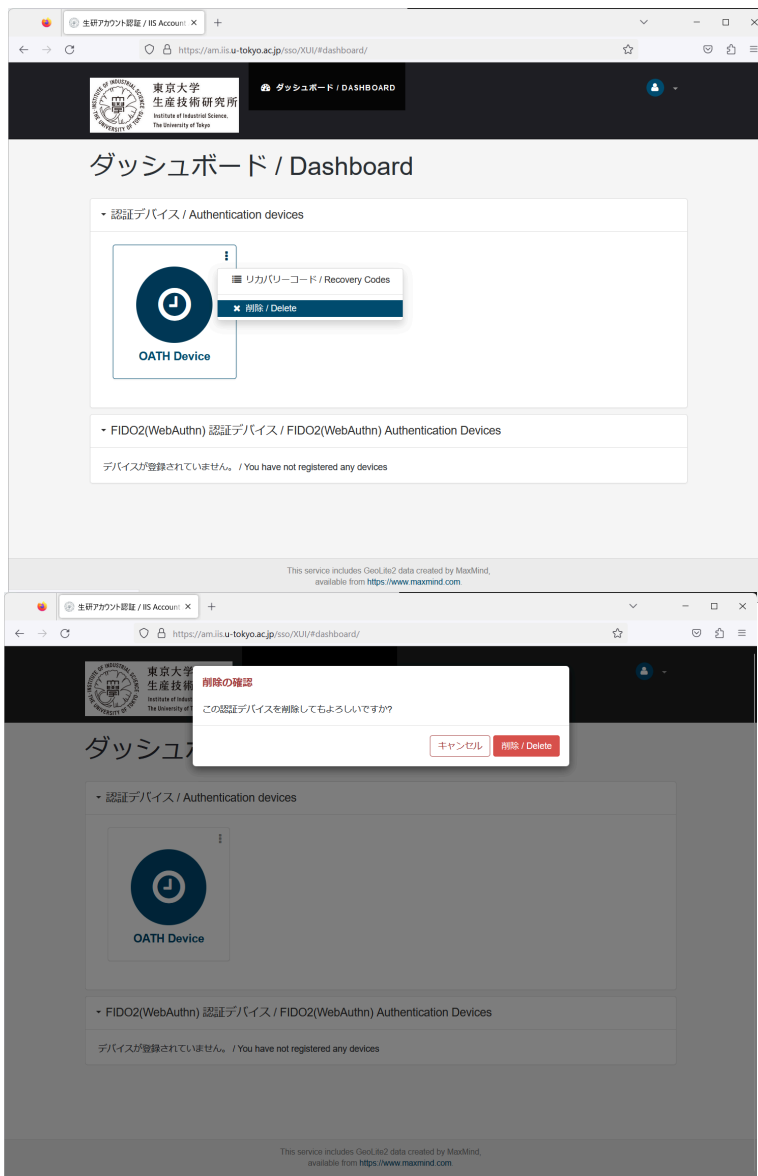
二要素認証の省略期間内であれば、二要素認証のコード入力は不要です。

もしくは、リカバリーコードを使って二要素認証をしてください。

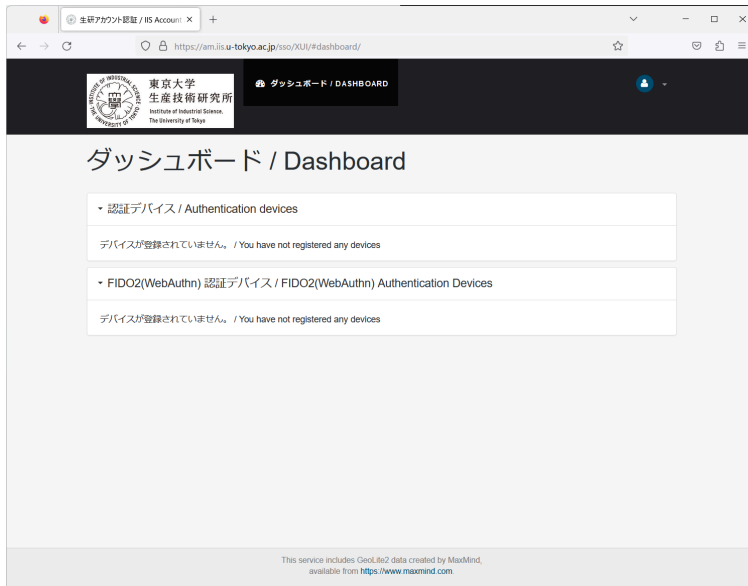
これらの方法でログインができない場合は、電子計算機室 cc-staff@iis.u-tokyo.ac.jp に

Subject: (申請) VPNの二要素認証初期化
で、所属と生研アカウント名を明記の上、ご連絡ください。

ログインできたら、「OATH Device」の右上の ⋮(タテ3つのドット)から「削除/Delete」を選択してください。



認証デバイスが「デバイスが登録されていません」という状態になります。



ログアウトしてください。その後、「[VPN用二要素認証の初期設定](#)」の手順に従ってください。

