セキュリティと在宅勤務
（多要素認証、UTokyo WiFi、UTokyo VPN、ウイルス対策ソフトウェア）

情報システム本部
玉造　潤史

絶対に漏らせないデータがそこにはある

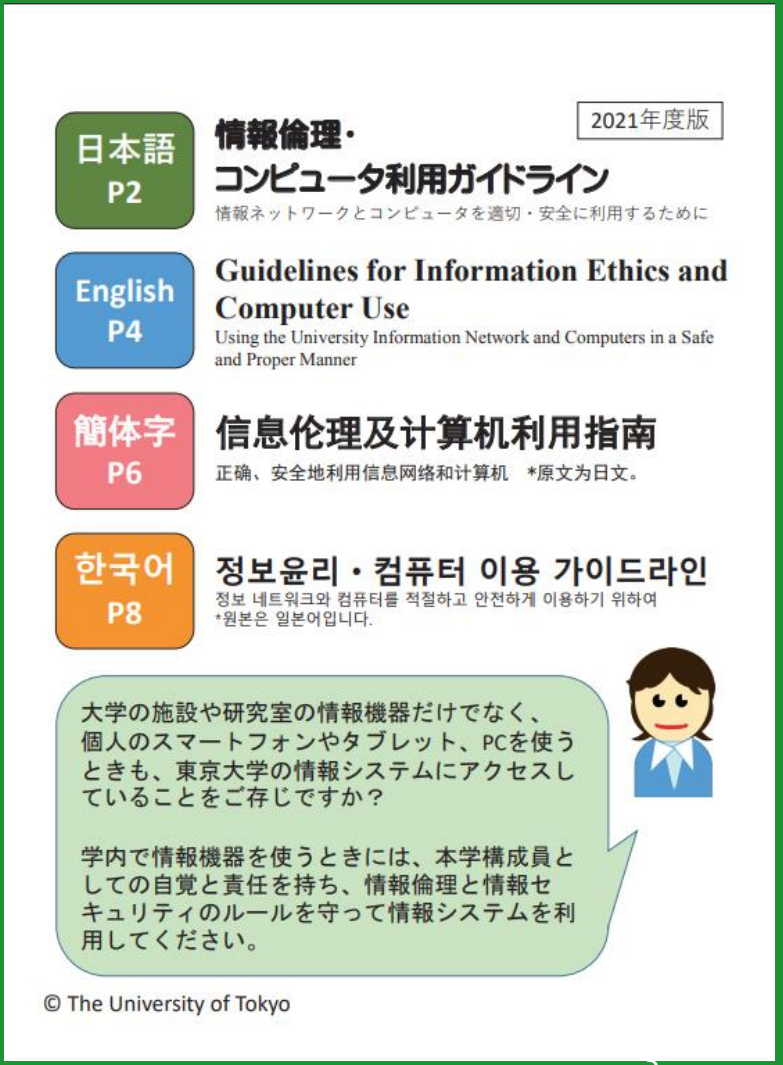
- 本学50000人の
  - UTokyo Account　(@utac.u-tokyo.ac.jp)
  - Google Account（@g.ecc.u-tokyo.ac.jp)

  アカウントとデータがインターネット、そしてダークウェブに…
- セキュリティ対策を考慮した使い方は面倒ですが、**我々はホワイトナイトとして**提供しています。
- 「アカウントは絶対に守ってください」　(守るための基本)
  - 安易なパスワードは決して使わない。
  - 長く複雑なパスワードに変更してください。

    →限度があると思いますので多要素認証の利用をお勧めします。

情報倫理・コンピュータ利用ガイドライン

- 「推測されやすいパスワードを使用しないでください」
  - 2要素認証の利用を推奨
- 「ウイルス対策とソフトウェアの脆弱性対策を徹底してください」
  - ウイルス対策ソフトウェアの提供
- 「セキュリティ対策が行われていないWiFiは利用しないでください」
  - 同じネットワークをVPNで提供



多要素認証とは

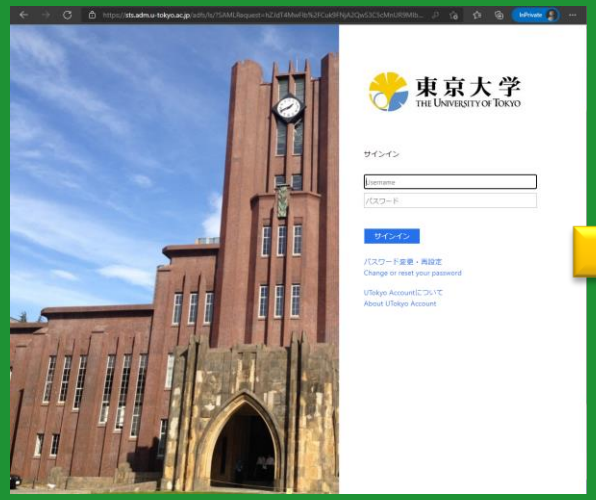
- 一般には、正当な利用者しか知る（持つ）はずのない二つ以上の情報を確認してサインイン認証をすること
- 実際には「ID＋パスワード＋何か」でサインインすることを指します
- もはやパスワードだけでは守れていない。（ブラウザに覚えさせているとほぼ何も打たない＝守れていない）

UTokyo Accountの多要素認証

- ブラウザを閉じないようにうまくつかうと1台、1日（24時間ごとに）に1回行うように設定しています。
- 本人を確認する方法は以下が利用可能です。(おすすめ順)
  - 認証アプリ　Microsoft Authenticator
  - 電話　音声（電話、会社の電話、代替の電話）
  - 認証アプリ　それ以外の Authenticator
  - 電話　SMS
- 現在はスマートフォンまたは携帯電話（固定電話）が必要です。
  - 設定した電話番号などはサインイン以外には利用しません。
  - プライバシーについての心配はありません。

1、Microsoft Authenticator の場合

- サインイン画面でサインインを行ったときの動き

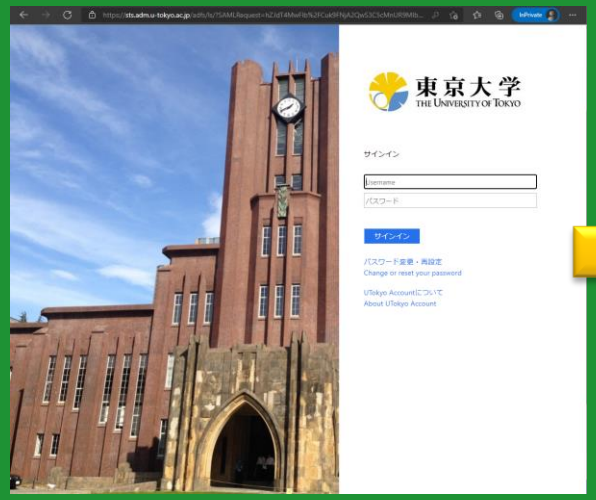


サインイン画面

スマホ画面

2、電話の場合

- サインイン画面でサインインを行ったときの動き

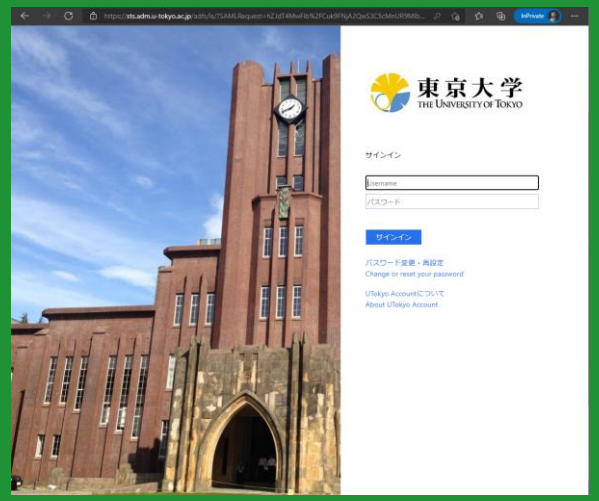


サインイン画面

スマホ音声

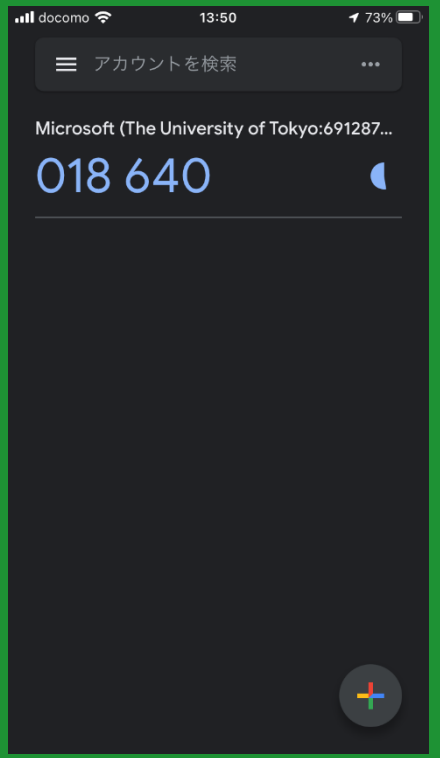
3、その他の認証アプリの場合
スマートフォンのGoogle Authenticatorの場合

- サインイン画面でサインインを行ったときの動き



サインイン画面

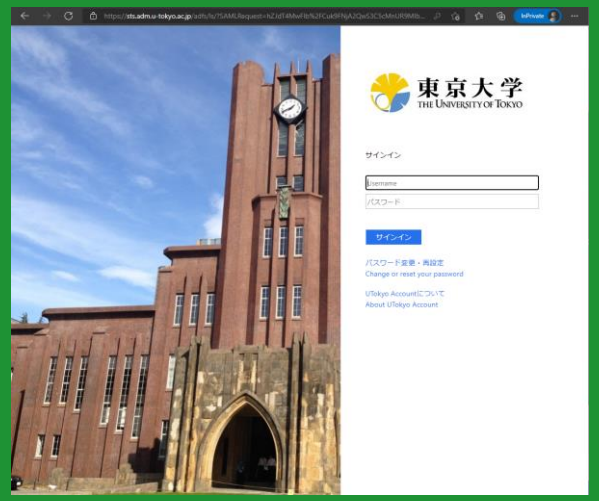
確認コード入力画面



Google Authenticator

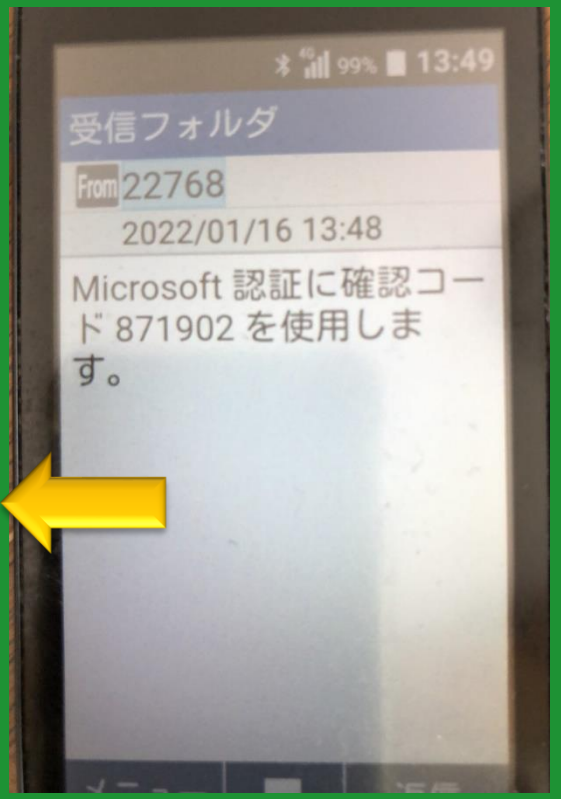
4、電話(SMS)の場合

- サインイン画面でサインインを行なったとき



サインイン画面

確認コード入力画面



携帯画面

多要素認証の設定

- 多要素認証の要素の設定を以下のページ従って行います。
- https://utelecon.adm.u-tokyo.ac.jp/utokyoaccount/mfa
  1. 認証方法の設定
  2. 多要素認証利用申請

- 認証方法を設定するときは2個以上設定してください。
  - スマホの機種変更などで使えなくなることがなくなります。
- スマホの場合は、認証アプリと電話の両方を設定することがおすすめです。

多要素認証のメリット

- 「安全性確保＝不便になる」という側面はあります。
  - ワンアクション増える
  - みなさんのアカウントを守る付加機能
  - 今後はさまざまなシステム利用で標準的になる。
    - たとえば銀行サービスなど

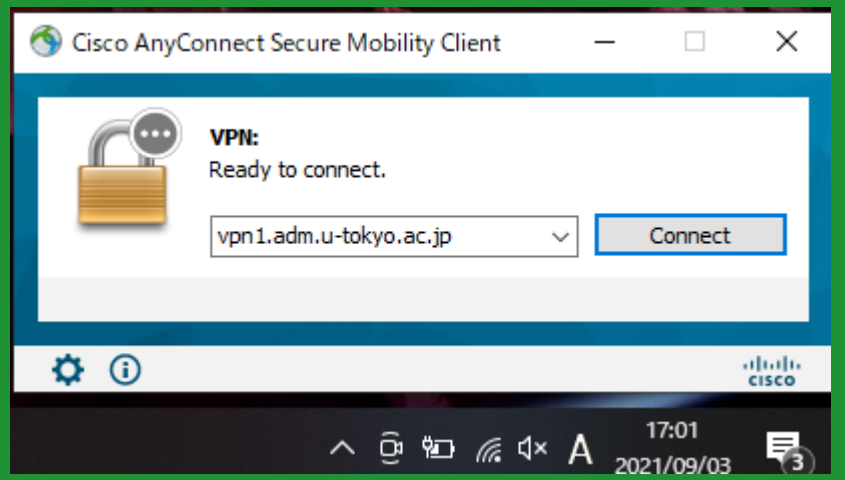
- 多要素認証を利用しているユーザへのメリット
  - みなさんのアカウントを守る手段です。
  - 新しいサービスを提供していきます。
  - 多要素認証をしている人はサインイン回数が少なくなるようになっています。（特に、モバイルデバイスなどでのサインイン）

UTokyo VPNについて

- 学外からUTokyo WiFi に接続している状態と同じ
- キャンパスでのみ利用できたシステムが利用できます。
- 説明ページ（ポータル便利帳から移行しました。）
- https://utelecon.adm.u-tokyo.ac.jp/utokyo_vpn/
  - 4月1日より、学生にも提供を開始します。
    - キャンパスからだけ利用可能なサービス、部局固有のサービスも利用可能です。
  - 現在は、WindowsとmacOS で利用できます。

UTokyo VPNの設定方法

- 学外からUTokyo WiFi に接続している状態と同じです。
- キャンパスでのみ利用できるシステムが利用できます。
- 設定方法
  1. 多要素認証の設定をしてください
     1. 認証要素の設定
     2. 利用申請後40分で利用権限が付与されます。
  2. ソフトウェアのダウンロードと
     インストールをします。
  3. 利用時にConnectボタンを押して接続
     してください。

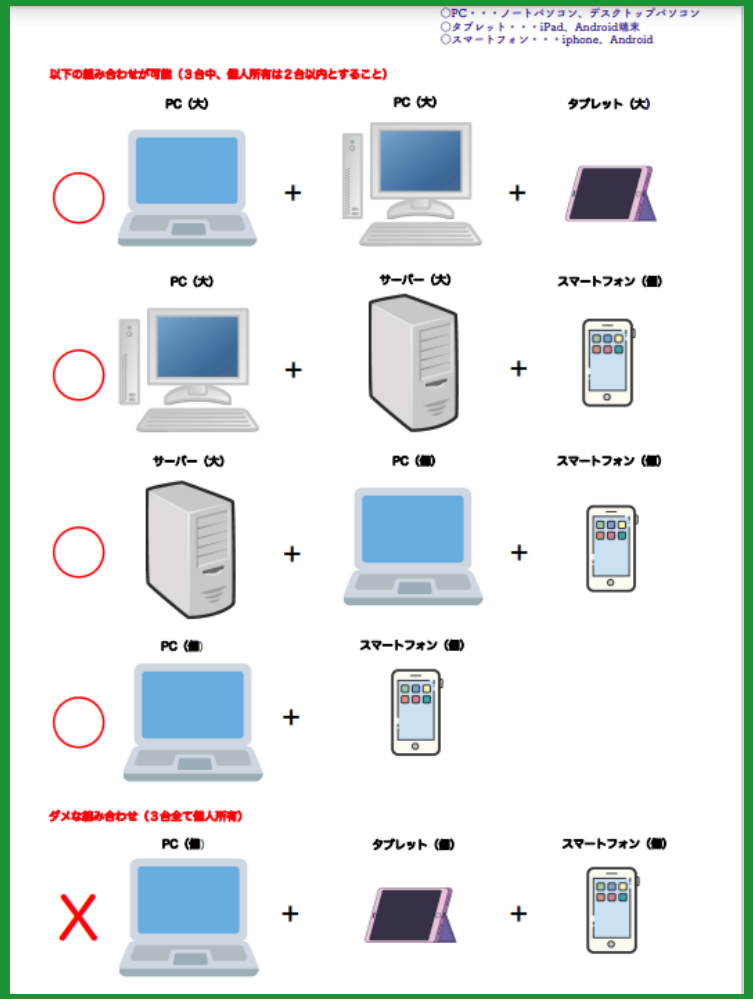


UTokyo Antivirus License

- 4月1日よりウイルス対策ソフトウェア（Trendmicro ApexOne)を提供します。
- PC(Windows,macOS),モバイル(Android,iOS), Linuxで利用可能できます。
- ひとりにつき3本です。
- うち2本を個人が所有するPCにインストールすることができます。
- 大学で利用するPCには、ウイルス対策を行うことが必要です。（このライセンスでなければいけないということではありません。）

UTokyo Antivirus Licenseについて

- 現在、ユーザ向けの提供情報を準備中です。
- utelecon サイトから提供しますのでご確認ください。



UTokyo WiFi

- 学内で使える共通WiFiです。
  - ほとんどの教室には整備済みです。
  - 2016年から教育用無線LANとして運営しています。
- UTokyo WiFiアカウント
  - https://www.u-tokyo.ac.jp/adm/dics/ja/wifi.html
- 重要な利用ポイント
  - 学生は春、教職員は夏に「情報セキュリティ教育」が必須です。
  - 半年ごとにアカウントの更新が必要です。
  - メールアドレスの登録が必須です。（学生はUTAS,教職員は人事情報システムに）

WiFi と BYOD(Bring Your Own Device)

- 2022年度から学生はご自身のPCを用意し持ってきてください。
  - https://utelecon.adm.u-tokyo.ac.jp/notice/byod
- 教室の基地局1台あたりは概ね50人が接続できるレベルで整備しています。
  - 50人が全員カメラオンの映像を送受信するような使い方は困難です。
- BYODで活用してください。
  - ITC-LMSでの資料配布
  - 教室ではカメラオフなどの使い方では問題ありません。
- 2023年までに、UTokyo WiFi のキャンパス全域整備を進めています。

在宅勤務のPC利用ガイド

コロナ禍の影響で増えた「在宅勤務」「家でもできる、実践サイバーセキュリティ」

- スタートアップ編
- 全体編

・セキュリティ管理の基本
・ディスクの管理

参考資料

UTokyo Account の機能

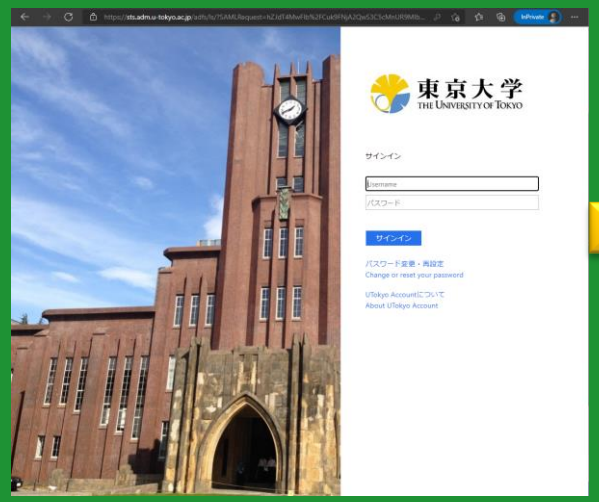
SSO(シングルサインオン)

- 現在のサービス利用ではブラウザを用います。
- 最初に一度だけサインインするだけでシステムを利用することができます。
- 上手に使うと一つのPC・デバイスなどで**24時間に1度**だけサインインが必要です。
- ブラウザを完全に閉じてしまわないことが重要です。

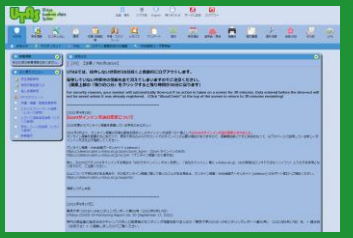
UTokyo AccountのSSO

- 1回のサインインで大学のシステムが
- 連携して使えます。

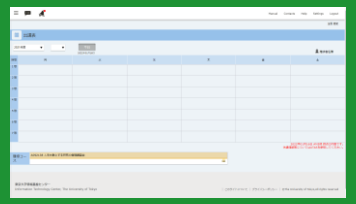
https://login.adm.u-tokyo.ac.jp/utokyoaccount



UTokyo Portal



UTAS



ITC-LMS