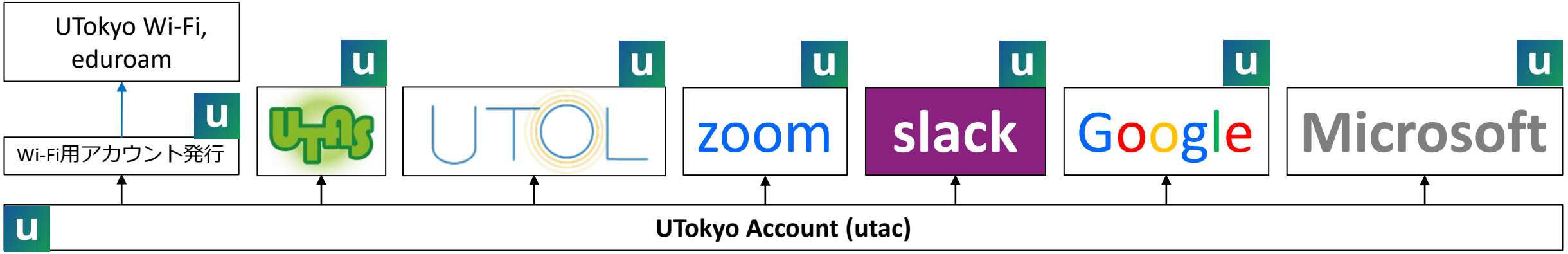
東京大学のITシステムの基本

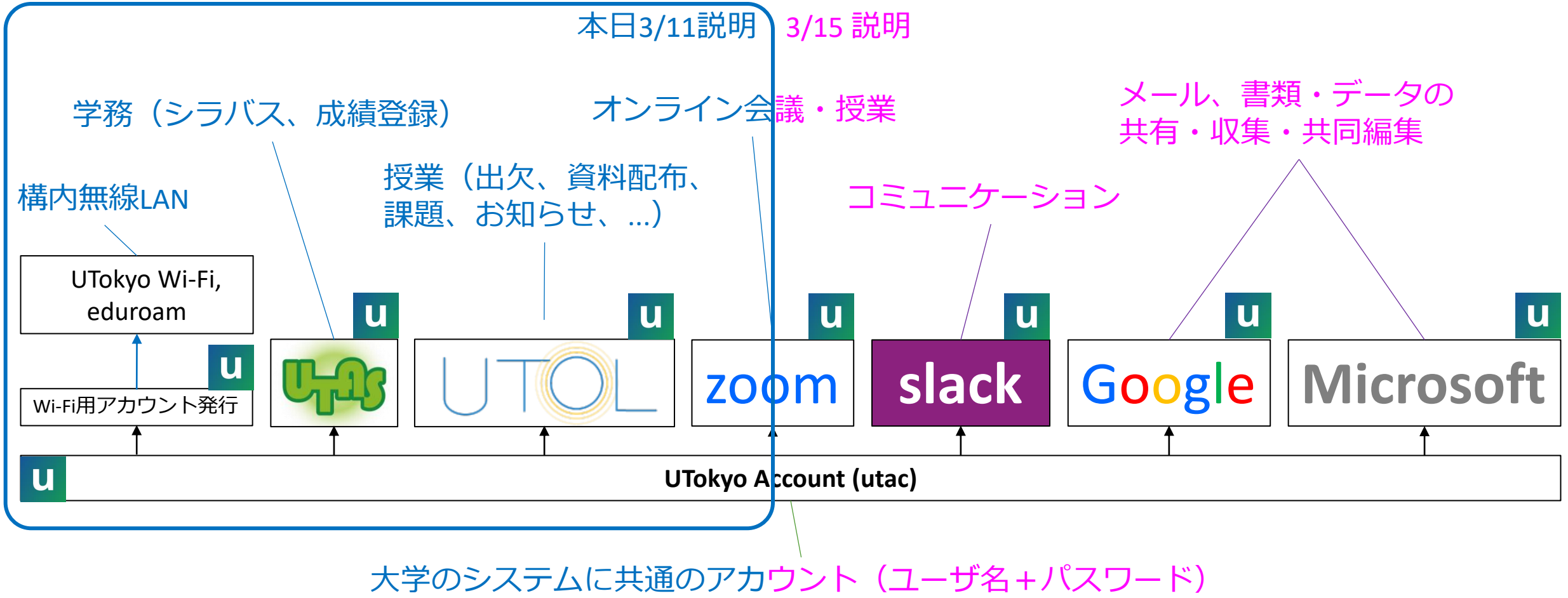
情報基盤センター長 田浦健次朗

代表的なシステム一覧

- 箱からサインインページへ飛べます
- u からutelecon の説明ページへ飛べます
  - 初めてのサインインの前に一読ください



システム概説


本日3/11説明
3/15 説明
学務（シラバス、成績登録）
オンライン会議・授業
メール、書類・データの
共有・収集・共同編集
構内無線LAN
授業（出欠、資料配布、
課題、お知らせ、…）
コミュニケーション
UTokyo Wi-Fi,
eduroam
Wi-Fi用アカウント発行
UTOL
zoom
slack
Google
Microsoft
UTokyo Account (utac)
大学のシステムに共通のアカウント（ユーザ名＋パスワード）

本パート概要

- utelecon について一言
- UTokyo Account
  - ～とは
  - 初期設定、特に多要素認証
- 情報セキュリティ教育
- Wi-Fi
- 多要素認証（中級）

本パート概要

- uteleconについて一言
- UTokyo Account
  - ～とは
  - 初期設定、とくに多要素認証
- 情報セキュリティ教育
- Wi-Fi
- 多要素認証（中級）

質問? utelecon をご利用ください

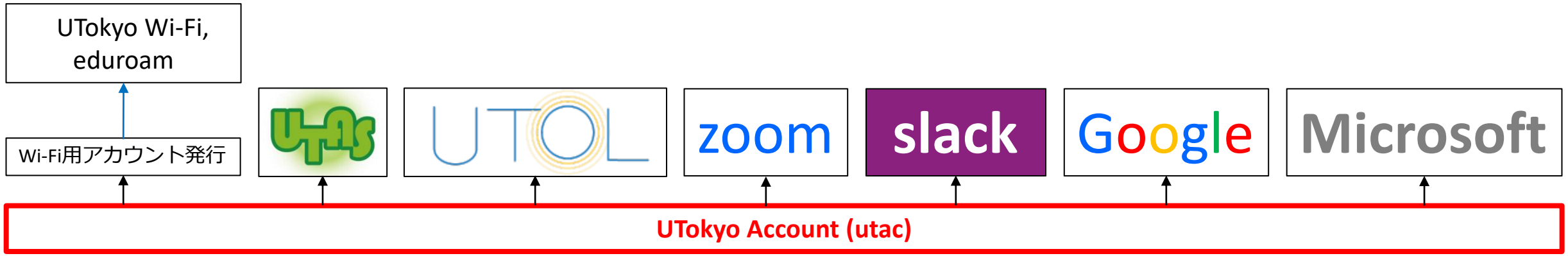
- Google で検索
  - 東大の Zoom? ⇒ utelecon zoom
  - 東大の Microsoft? ⇒ utelecon microsoft
  - … かなりの確率で見たいページがヒットします
- サポート
  - チャット、メールフォーム、Zoom

https://youtu.be/aPigliX-Nyg

本パート概要

- uteleconについて一言
- UTokyo Account
  - ～とは
    - 初期設定、とくに多要素認証
- 情報セキュリティ教育
- Wi-Fi
- 多要素認証（中級）

UTokyo Account (utac) とは



- はじめに utac ありき
- 大学のITシステムを使うための共通アカウント
- 共通のユーザ名、パスワードで多くのシステムが使えます
- Single Sign On, SSOなどと呼ばれます

UTokyo Accountの正体

- 10桁の数字@utac.u-tokyo.ac.jp
- 「10桁の数字」は教職員であれば職員証に書かれています（右端の10桁）

000000 00*xxxx xxxxxx*

↓

xxxxxxxxxx@utac.u-tokyo.ac.jp
があなたのUTokyo Account

通称・略称

- 名前が長いので通称・略称がよく使われます
- 「十桁」（読み方：じゅっけた）
  - 例：先生の十桁を教えてください
- 「utac」（読み方：ユータック）
  - あなたのユータックを教えてくださいとはあまり言いません

本パート概要

- utelecon について一言
- UTokyo Account
  - ～とは
  - 初期設定、とくに多要素認証
- 情報セキュリティ教育
- Wi-Fi
- 多要素認証（中級）

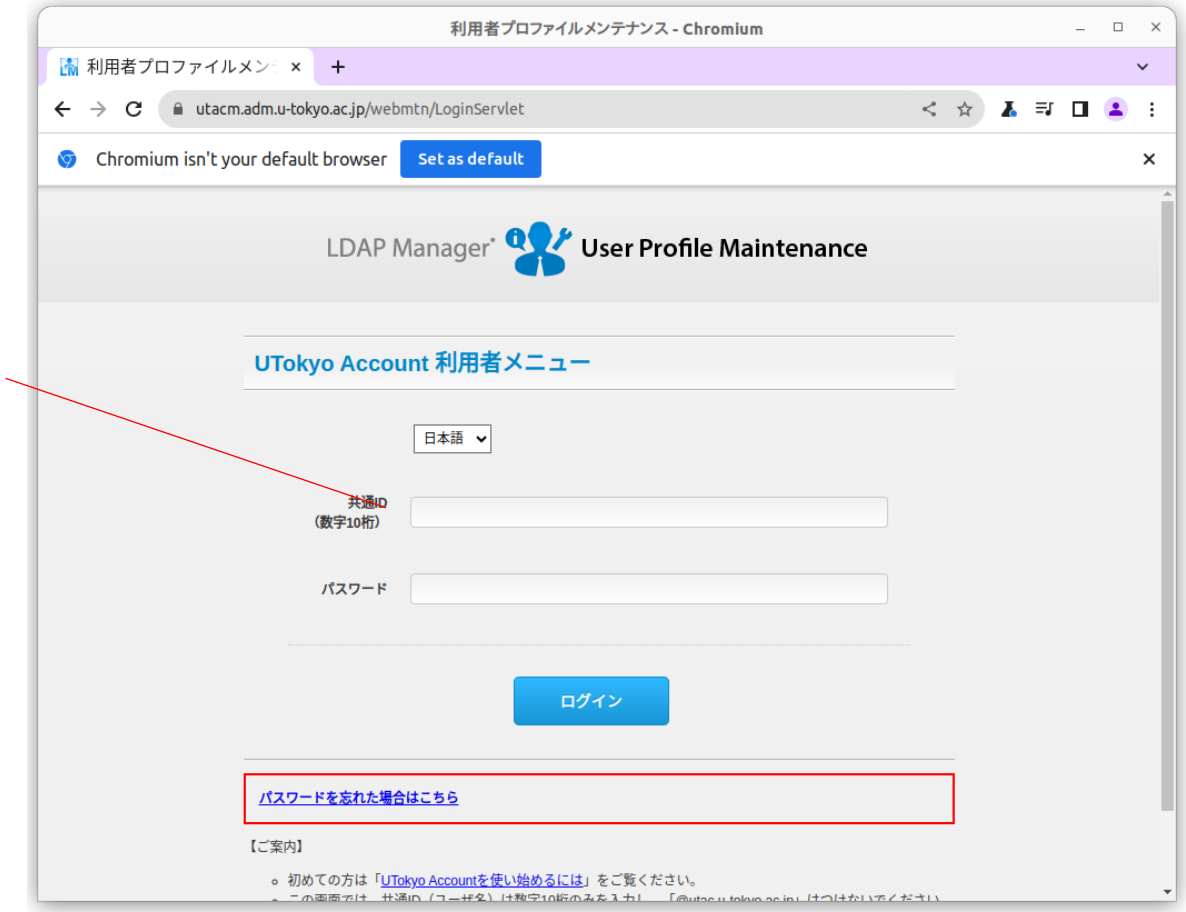
UTokyo Accountで実際にITシステムを使うまでの準備

utelecon utokyo account 

1. 「10ケタ」と「初期パスワード」を入手
   - 所属部局（学部や研究科）の人事部から
2. パスワードを設定
   - 初期パスワードのままでは使えません
   - （今は）この時点で一部システム（UTAS、UTOLなど）にログイン可能
3. 多要素認証を設定
   - 全てのシステムにログインが可能

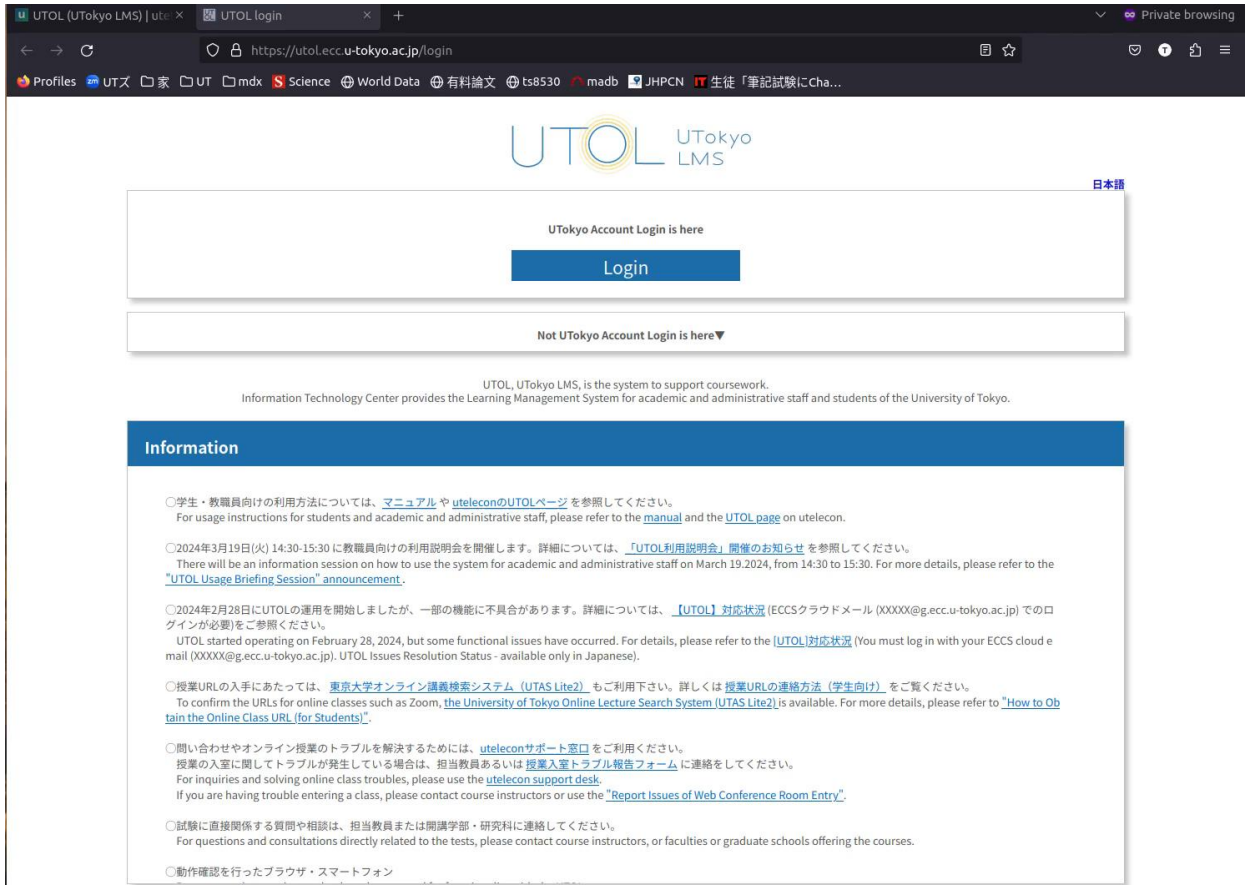
UTokyo Accountパスワード設定画面

10桁を（@utac以降はナシで）入力



ためしにUTOLにログインしてみる

- 注：多要素認証を設定（後述）した場合の画面です
- たった今は多要素認証なしでもUTOLは使えますが、もうすぐ多要素認証なしでは使えなくなります



https://youtu.be/RqbacxwxeFA

多要素認証

utelecon 多要素

多要素認証とは

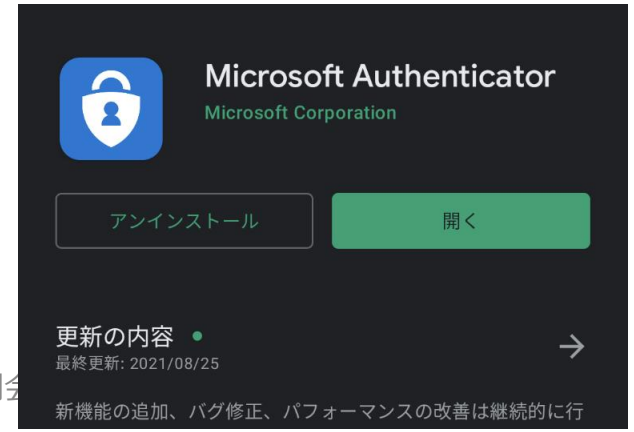
- 一般には、正当な利用者しか知る（持つ）はずのない2つ以上の情報を確認してログイン許可すること
  - パスワード、電話、スマホ、専用デバイス、生体情報、etc.
- パターン1: パスワード＋何か
- パターン2: 「パスワードレス認証」
  - スマホ＋生体情報
  - 専用デバイス＋生体情報など

なぜ多要素認証?

- 多要素にすることでパスワードだけの状態よりも「格段に」安全になる
  - 特に、標的型メール・フィッシング（※）に対する防御
  - （※）メールに埋め込まれたリンクなどで攻撃者のサイトへ誘導しパスワードを入力させる
- バラバラなアカウントを統一（SSO）＋それを強固に守る
  ⇒ 安全性と利便性を両立

面倒くさくないですか?

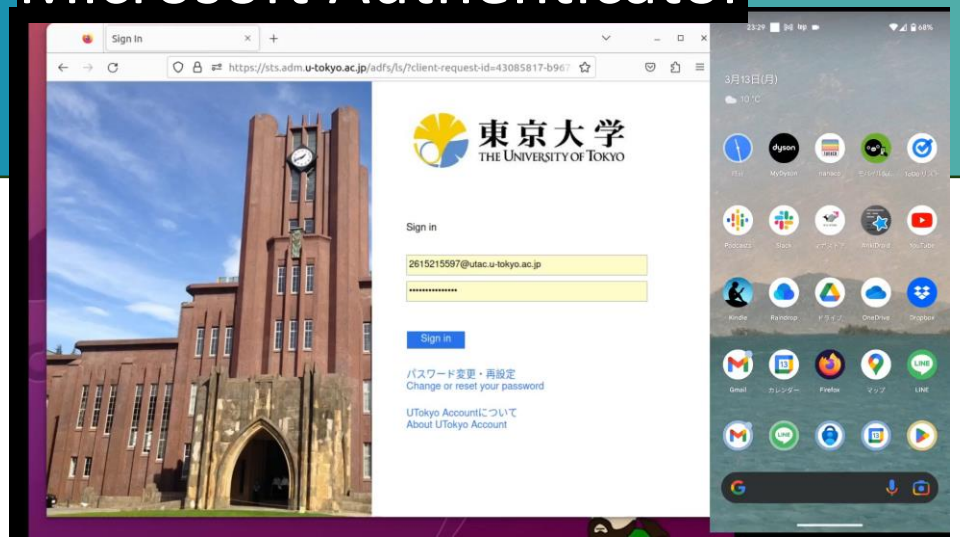
- 方法によって違いますがスマホの認証アプリMicrosoft Authenticatorを用いた方法はそこそこ楽
  - Android（Google Play Store）
  - iOS（App Store）
- スマホを常に持ち歩いている人なら≈スマホを開く+ α程度の手間



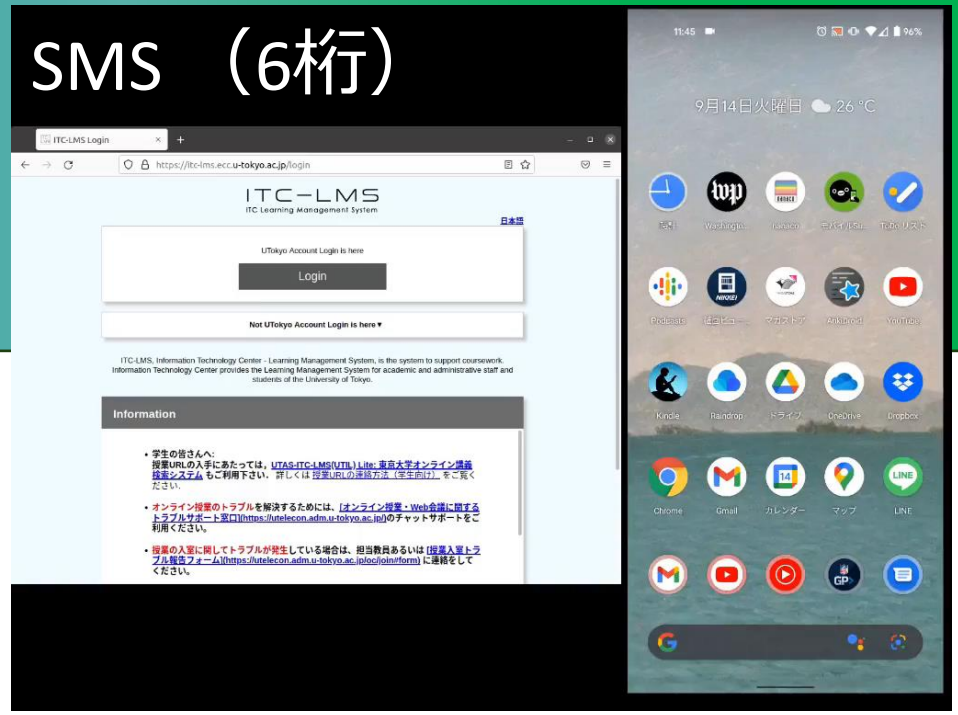
多要素認証の色々な方法（パスワード＋何か）

- Microsoft Authenticator（推）
  - 携帯を開けて2桁の数字を入力
- 携帯のショートメッセージサービス（SMS）
  - 携帯にテキストで飛んでくる6桁の数字をサイトに入力
- 音声電話（携帯、いえでん）
  - 電話に出て#キーを押す スマホがなければ意外と推?
- Google認証システム
  - アプリを開いて表示される6桁の数字をサイトに入力

Microsoft Authenticator

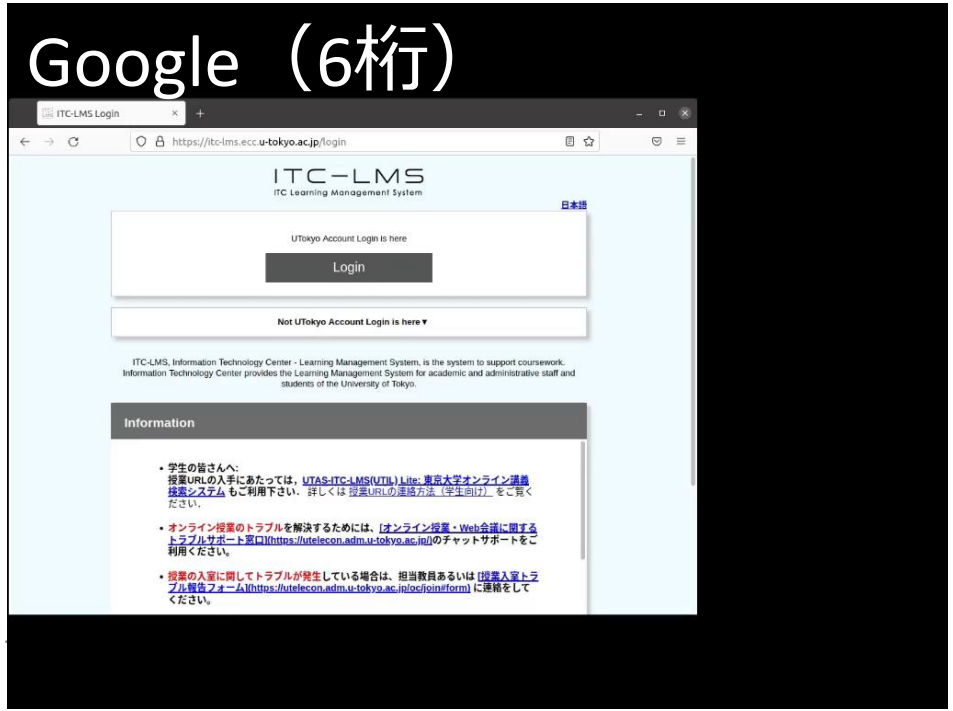


SMS （6桁）



音声電話（携帯）

Google （6桁）



多要素認証の初期設定方法

- 作業完了後、実際に有効化されるまで最大40分ほどかかります
- 何かの直前ではなく、余裕をもってゆっくり作業ができる時間にやってください
- やり方をゆっくり解説していますので作業前に是非ご覧ください→

utelecon 多要素 設定

多要素認証の初期設定時の罠

- 以下をやる必要がある
  - (a) 本人確認方法（アプリ？SMS？家電？）設定
  - (b)「多要素認証ON」というフラグの設定
  - (c) （最大）40分待つ
- (a)を終えて(b) を忘れてしまうケースが多発
  - 忘れると多要素認証が必須のサービス（UTokyo VPN, UTokyo Slack）アクセス時に「サービスを利用する権限がない」旨のエラー
- **初期設定ページに従い最後(b)までやり遂げてください**

東大では多要素認証が(ほぼ/もうすぐ)必須です

- UTokyo Portal で 多要素認証 100% で検索
  - 多要素認証の必要性（by CISO補佐・情報基盤センター 中山雅哉）
  - 部局ごとの設定率
- 多要素認証なしでは使えないサービス
  - 今： UTokyo Wi-Fi (※) , UTokyo Slack, UTokyo VPN
  - もうすぐ（2024/5～6月）：すべてのシステム
  - (※)：すでに発行済みUTokyo Wi-Fiはアカウントは失効（2024/4/30）まで有効

本パート概要

- utelecon について一言
- UTokyo Account
  - ～とは
  - 初期設定、とくに多要素認証
- 情報セキュリティ教育
- Wi-Fi
- 多要素認証（中級）

必須 情報セキュリティ教育

- 簡単なe-learning + テスト（3択 x 10題）
- テストに合格するまで以下が使えません
  - UTokyo Wi-Fi
  - UTokyo Slack
  - UTokyo VPN

東京大学 情報セキュリティ教育

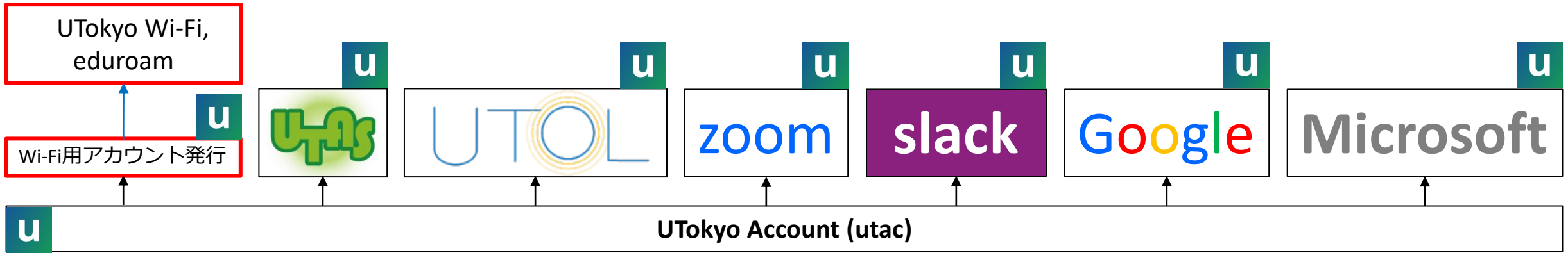
またはこのリンクから

- 本学全員必修（「テスト受けるか、Wi-Fi/Slack/VPNをあきらめる」という選択ではありません）

本パート概要

- utelecon について一言
- UTokyo Account
  - ～とは
  - 初期設定、とくに多要素認証
- 情報セキュリティ教育
- Wi-Fi
- 多要素認証（中級）

Wi-Fi


UTokyo Wi-Fi,
eduroam
Wi-Fi用アカウント発行
UTOL
zoom
slack
Google
Microsoft
UTokyo Account (utac)

Wi-Fi用アカウント発行ページ

- アカウント発行ページで「新規申請」を押す
- EmailでWi-Fi専用の
  - ユーザ名（u24XXXXXX@wifi.u-tokyo.ac.jp）
  - パスワード
  - が送られてきます

UTokyo Wi-Fiにつなぐ

- 要約
  - ネットワーク名（SSID）: 00000utokyo
  - Security: WPA2 Enterprise
    に、Emailで送られてきたユーザ名とパスワードでつなぐ
- 詳細はデバイス（Windows, Mac, Android, iPhone, iPad, ...）、機種によっても異なるのでutelecon を参照してください

utelecon wifi 

eduroamにつなぐ

- ネットワーク名（SSID）：eduroam
  - UTokyo Wi-Fi（00000utokyo）と同じユーザID, パスワード、設定方法でつなげます
- 東大キャンパス内のみならず、他の大学や研究機関でも（高い確率で）使えます
- 東大構内ネットワーク限定のページ・リソースにアクセスできない場合があります（キャンパス外ネットワークにつながった状態）

結局何をすればよいかのまとめ

- ✓utacパスワード変更ページに、もらった10桁＋初期パスワードでサインインしてパスワード変更
- ✓多要素認証を設定
- ✓情報セキュリティ教育（テスト）をクリア
  ⇒ 色々なシステムにアクセスできます
- ✓Wi-Fiアカウント発行ページでアカウント発行
  ⇒ 構内でUTokyo Wi-Fi, eduroamにつなげます

本パート概要

- utelecon について一言
- UTokyo Account
  - ～とは
  - 初期設定、とくに多要素認証
- 情報セキュリティ教育
- Wi-Fi
- 多要素認証（中級）

パスワードレス認証

多要素認証いくつかの注意・罠

- スマホ買い替え
- スマホ・携帯電話を持っていない（持たない主義）
- 海外出張
- 携帯会社の通信障害

スマホ買い替え

- アプリ（Microsoft Authenticator, Google認証アプリ）の設定はスマホを買い替えると引き継がれない
- 本人確認方法がアプリ「だけ」だとそこで詰んでしまう!
- 対策
  - 本人確認方法をもう一つ（電話など）登録する
  - アプリの設定は設定ページで一旦消してやり直す

スマホや携帯を持っていない（持たない主義）

- 多要素認証専用に以下いずれかをご検討ください
  - 大学貸し出し**ガラ携電話**
  - 大学貸し出し**専用ハードウェアトークン** 
    - 購入すると10000円/台程度。費用負担方式検討中
  - **専用セキュリティキー** YubiKey 
    - USBポートに刺すか近接無線通信（NFC）でPCと接続
    - 自費購入下さい（Amazonなど）
    - 設定方法案内
  - **固定電話x2**（いえでんと職場電話）
    - 出張時に困るので結局持ち歩ける方法を推奨

（海外）出張

- NG 固定電話（職場・いえ）だけだと
- OK 持ち歩き型の道具
  - 自分のスマホ（※）
  - 大学貸し出しガラ携（※）
  - 専用ハードウェアトークン
  - 専用セキュリティキー
- （※）海外出張時はローミングサービスが通じている場合
  - 大学ガラ携についてはSoftbankのページで機種＝**Kyocera DINGO ケータイ for Biz** で確認ください

携帯電話会社のデータ通信障害

- NG ショートメッセージ
- NG Microsoft Authenticatorの2桁を入力する方法
  - 通知が届かなくなるため
- OK 音声電話
  - 音声通信が生きている前提
- OK 6桁を入力する方式（通常、通信は不要）
  - 専用ハードウェアトークン、セキュリティキー
  - Google認証システム
  - 実はMicrosoft Authenticatorも6桁入力方式がある（動画）
    - スマホでMicrosoft Authenticatorをタップして起動
    - The University of Tokyoを選択、6桁を表示

多要素認証の利用終了方法（…じゃなかったあの時に戻りたい）

- できるだけ思い止まって、と言った上で…
- それでも利用終了したい場合、本人確認方法再登録および利用終了ページからお申し込みください
- トラブル時に設定をやり直（再登録）したい場合も同じページから
- 業務に支障をきたす理由がある場合、やめる前にご相談ください

まとめ：多要素認証で安心な暮らしを

田浦作
（凡人）

多要素を
設定しないと
無防備やねん

金子亮大作
(utelecon メンバー)

ログインの
安全守る
スマートフォン

大澤悠一作
(utelecon メンバー)

サインイン
一手間かけて
安全に

在宅勤務のPC利用ガイド もご覧ください
面倒だと感じたら「やめた!」と思う前に症状をお知らせいただけるとありがたいです

付録：パスワードについて

ちゃんとしたパスワード

- **あなただけに覚えられる**パスワード
  - 巷で推奨（？）されている方法
  - 自分に思い出せる長い文章を思い浮かべてある規則で文字を取り出す
    - Windows ga 1 ban te koto ha nai to omoimasu ⇒ Wdsg1bntkthntmms
  - AIに生成されてしまう可能性は否定できないが…
- **乱数**パスワード（王道）
  - 一番安全（例：大文字小文字数字混ぜて12文字）
  - 生成方法：例えばこのExcel
    - 注：Linux pwgenコマンド、スクリプト言語などもっと普通な方法はあります（無理やりExcelでやってみただけです）
  - 問題：なかなか覚えられない（次スライド）

乱数パスワード覚えられない問題

- 紙に書いておく?
- 「いざというとき」の手段としては○
- 入力を要求されることが稀なら紙でも耐えられる
- だが一般には解決策といえるかは怪しい
- ⇒コンピュータに保存（＋コピペ）したくなる

乱数パスワード覚えられない問題 ほげ.docx 方式

- 端末内（ローカルフォルダ）に暗号化されたファイル（word で作成可能）を作りUTokyo Accountのパスワードをメモしておく「ほげ.docx」
  - 見本 (パスワード： eeyoWei3)
- Word:「ファイル」→「情報」→「文書の保護」→「パスワードを使用して暗号化」

ほげ.docxのパスワードは?

- A: 記憶可能なものに設定
- Q: え？それって（初めからutacに記憶可能なパスワードを使うのと）同じことでは?
- A: 否。「ほげ.docx」がその端末に物理的にさわらないと開けられないようにしていれば「ほげ.docx」はすでにある程度安全
- UTokyo Accountパスワードはインターネットに開いた入口の鍵であることに注意!
- utacは以下の(a)(b)（の弱い方）で守られている
  - (a) 乱数パスワード
  - (b) 端末の物理セキュリティ＋ログインセキュリティ＋ほげ.docxのパスワード