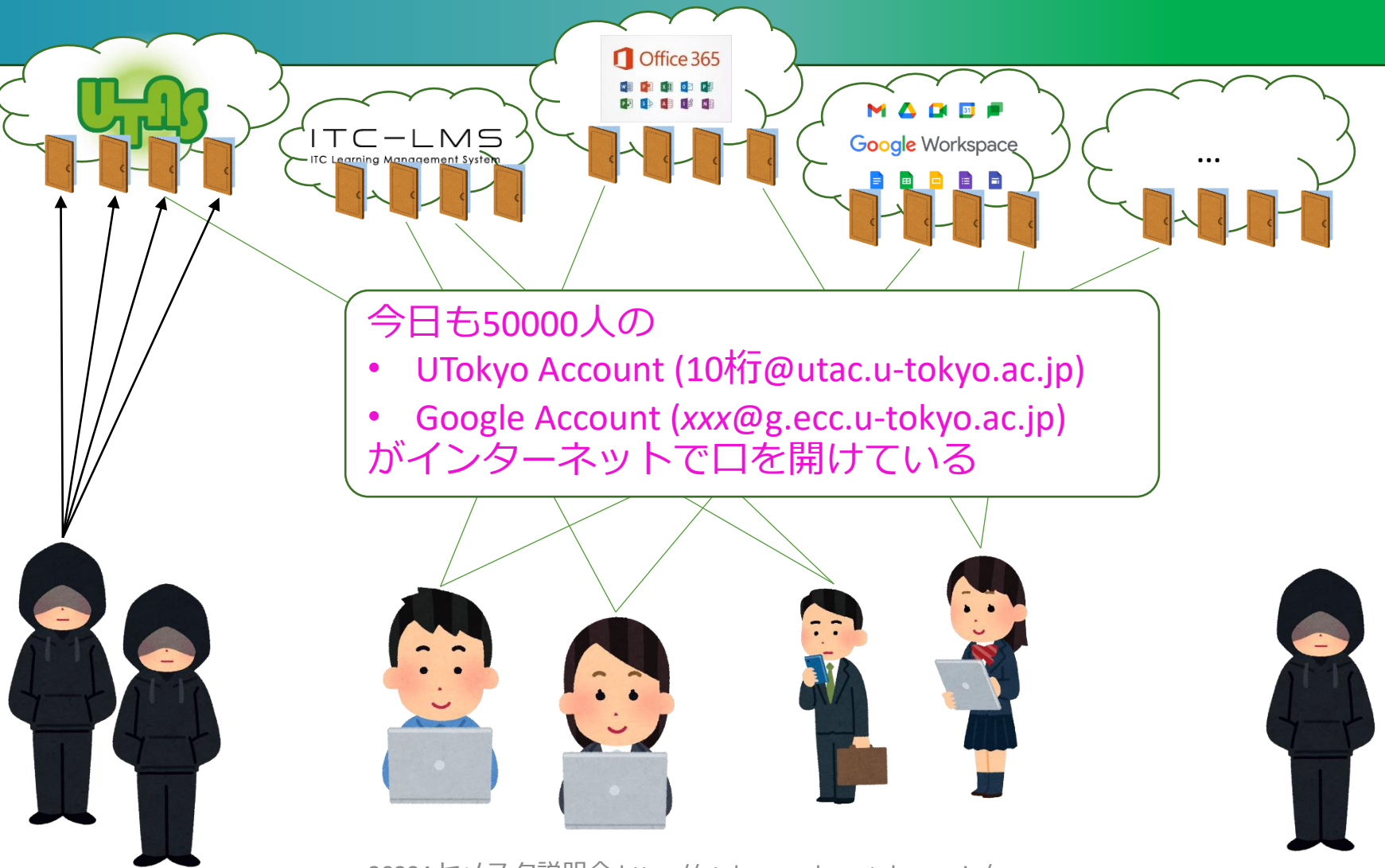
セキュリティと多要素認証

情報基盤センター長 田浦健次朗

絶対に漏らせないデータがそこにはある



サービス提供の方針

- **集約:** ほとんどのサービスに、UTokyo Account（以下 utac）だけで入れるようにする
- **どこでも:** 在宅等、場所を選ばず仕事を可能にする

⇒ データは「学内アクセスに限定」に頼らず、**強力なユーザ認証**で守る

強力なユーザ認証の基本

- ちゃんとしたパスワードを使う
- 多要素認証を使う

多要素認証とは

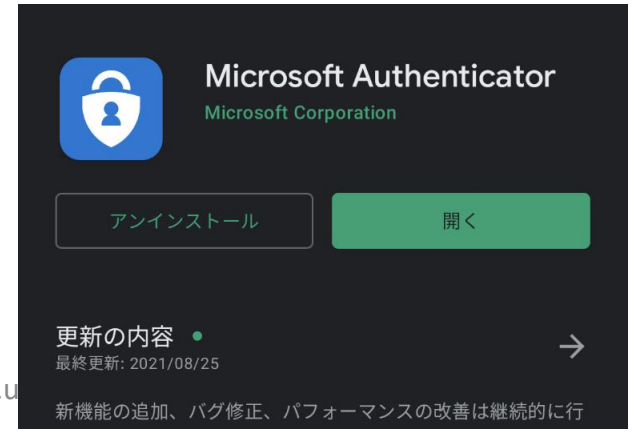
- 一般には、正当な利用者しか知る（持つ）はずのない2つ以上の情報を確認してログイン許可すること
  - パスワード、電話、スマホ、生体情報、専用デバイス、etc.
- 実際問題としては「パスワード＋何か」を使ってログインする

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、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?

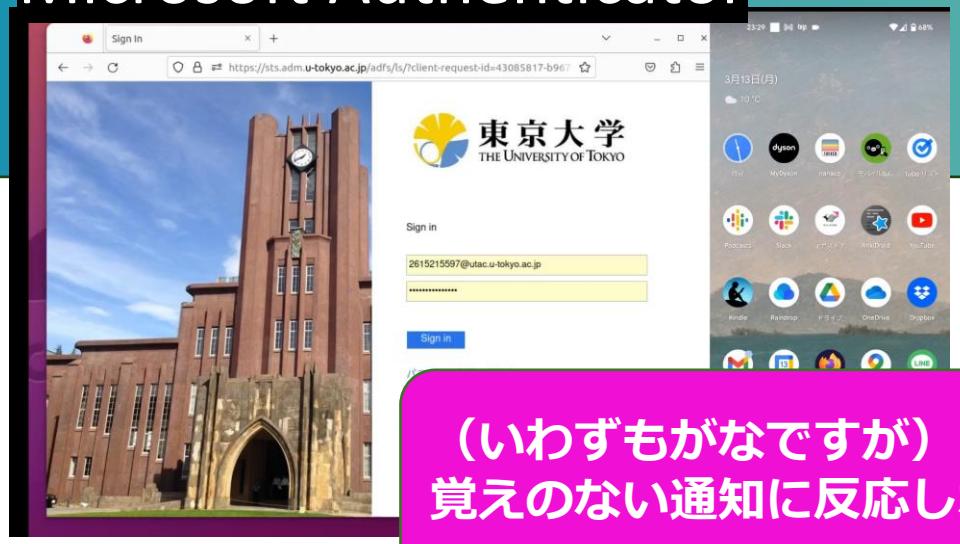
- 方法によって違いますがスマホの認証アプリMicrosoft Authenticatorを用いた方法はそこそこ楽
  - Android（Google Play Store）
  - iOS（App Store）
- スマホを常に持ち歩いている人なら≈スマホを開く+ α程度の手間



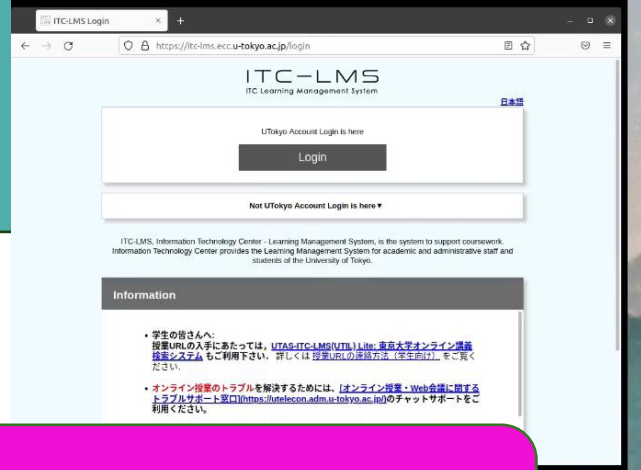
多要素認証の利用イメージ色々（utac）

- Microsoft Authenticator（携帯を開けて2桁の数字を入力 推奨）
- 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）
- 音声電話（スマホがなければ意外とおススメ? 電話に出て#キーを押すだけ）
  - 携帯
  - いえでん
- Google認証システム
  - Microsoft Authenticatorと似てますが、UTokyo Accountで使うには不便（6桁数字入力が必要）

Microsoft Authenticator

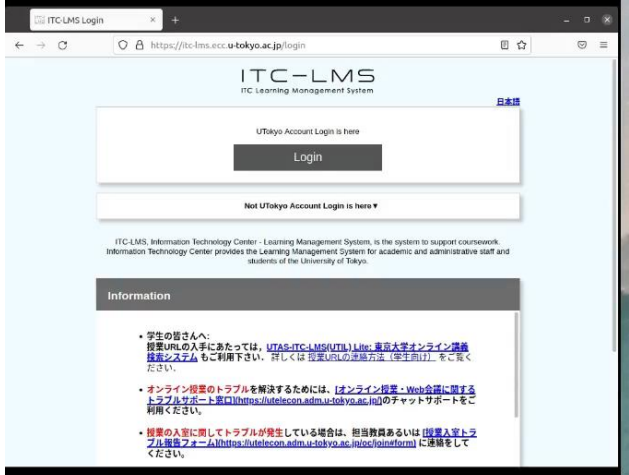


SMS （6桁）

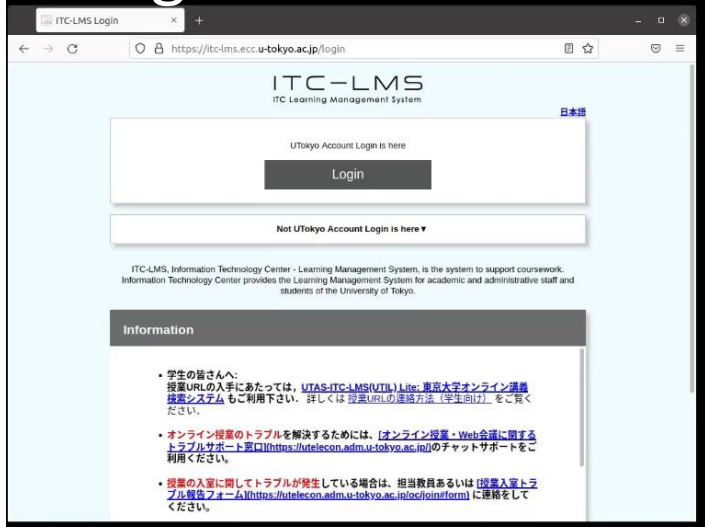


（いわずもがなですが）自分がサインインした覚えのない通知に反応しないことが前提です

音声電話（携帯）



Google （6桁）



本学の多要素認証利用率100%を目指しています

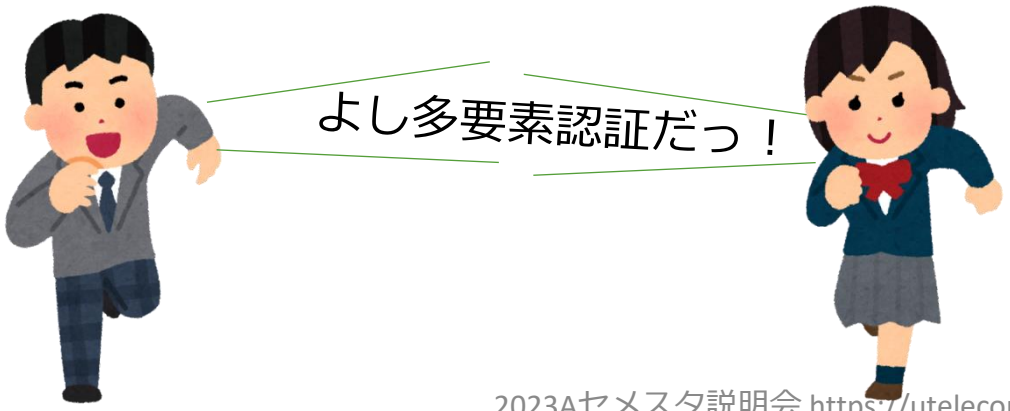
- UTokyo Portal で 多要素認証 100% で検索
  - 多要素認証の必要性（by CISO補佐・情報基盤センター 中山雅哉）
  - 部局ごとの設定率
- など
- 多要素認証なしは無防備です
  - どのくらい無防備か?

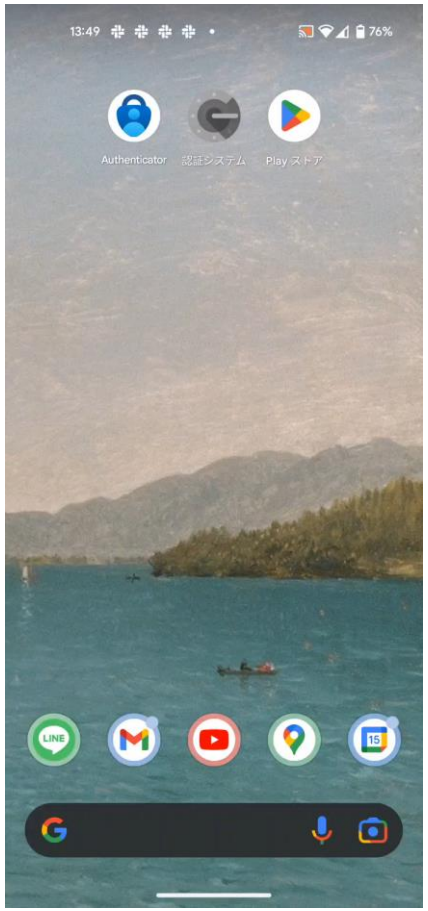
お願い

- 必要性を理解し「多要素認証はセキュリティ向上のため」と伝え、普及にご協力ください
  - UTokyo Slackを使いたければ多要素、ではなく
- Slackのみならず、UTAS, ITC-LMS, Microsoft, あらゆるサービスのセキュリティ向上のため
- 多要素認証が業務に支障をきたす場合、やめるのではなくご相談ください

Googleも多要素（2段階）認証！

- スマホでの認証操作はMicrosoft Authenticatorよりも簡単です
- スマホに特別なアプリのインストール不要
  - スマホ上でGoogleアプリ（Gmailなど）、Googleアカウントを設定しておけばよい





Googleの2段階認証が推奨されるなるほどな理由

- Googleは我々も詳細のわからない「総合的な」基準で怪しげなサインインを拒絶しています
  - パスワードが合っていても、いつもと違う場所、端末、IPアドレスからのサインインを「怪しい」として拒絶している模様
  - お客様が所有するアカウントであることを確認できませんでした。
  - *Google couldn't verify this account belongs to you. Try again later or use Account Recovery for help.*
- 2段階認証設定すると「怪しさ」が減り、拒絶されることがなくなるという仕組み
  - 中国からの学生で複数の事例が観測されています

設定方法説明ページ・動画

Account	多要素認証設定	パスワード変更
utac	utelecon: UTokyo Accountにおける多要素認証の利用	UTokyo Account利用者メニュー
Google	クラウドメール (GSuite for Education) アカウントにおける2段階認証設定のお願い	

- utac多要素認証設定方法（初めての方向けに「ゆっくり」解説していますので後ほどご覧ください）

（ついでにではありませんが）
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（新規の方は特にご注意）
  - 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」という選択ではなく）

いくつかの注意・罠

- 初期設定時の罠
- 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

初期設定時の罠

- 初期設定は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**

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」の手段としては〇
- 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