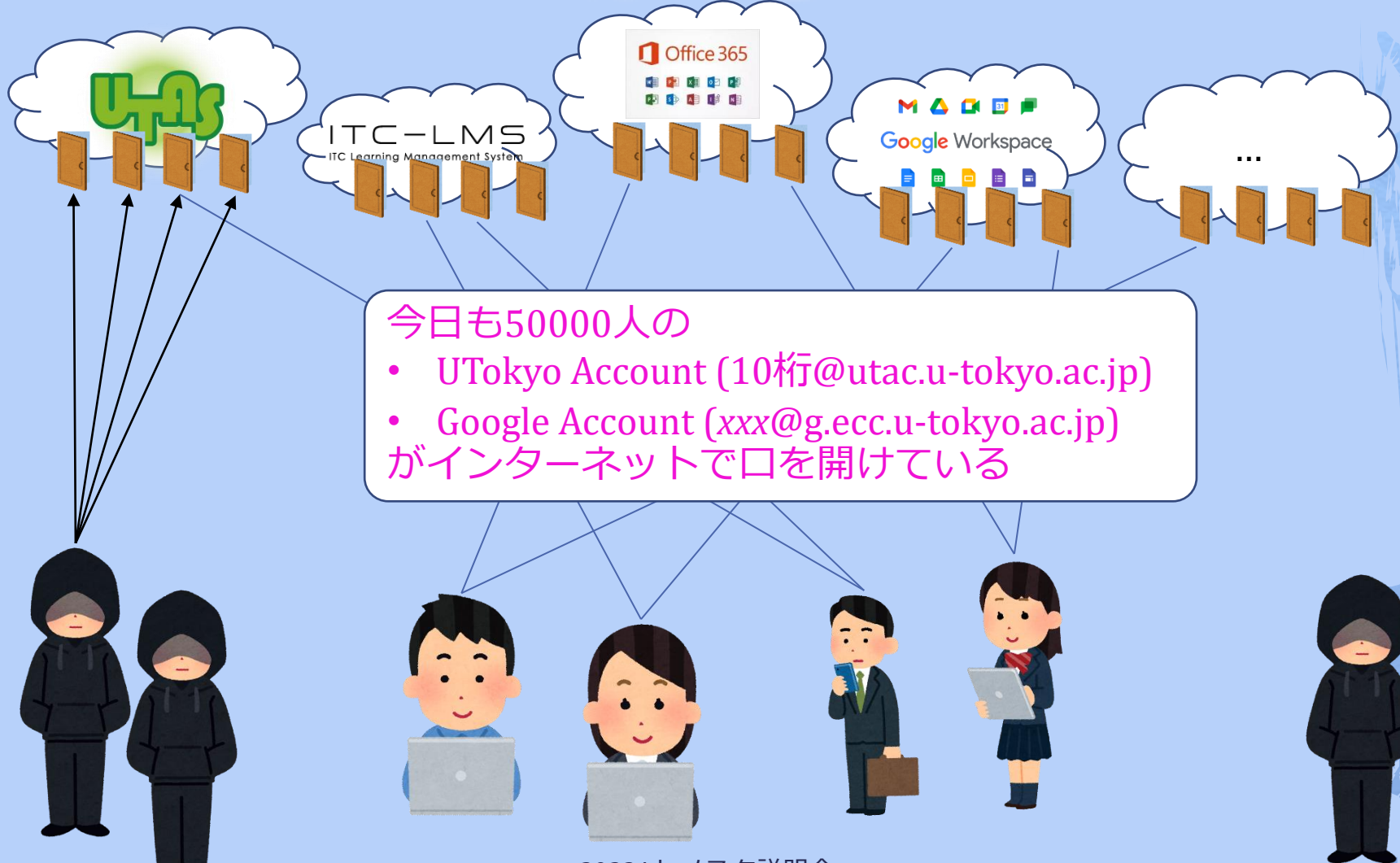


# セキュリティと多要素認証

---

情報基盤センター 田浦健次郎

# 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 

# ちゃんとしたパスワード

## ◆ 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があります（無理やりExcelでやってみただけです）
- ◆ 問題：絶対覚えられない（次スライド）

## ◆ 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

# 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○
- ◆ 急に入力を要求されたときに取り出せない可能性や、取り出せても手動で入力する必要があるなど、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 (解) 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



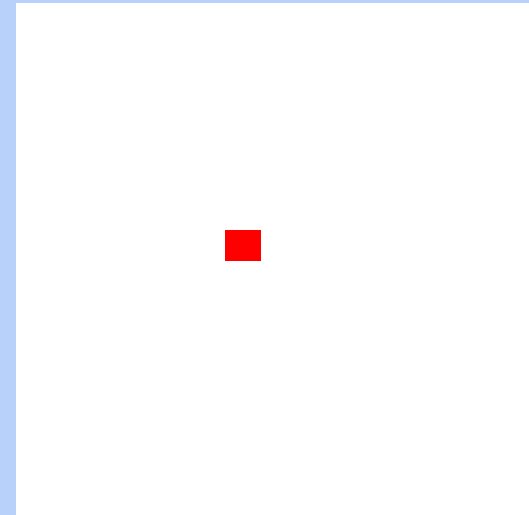
# 多要素認証とは

- ◆ 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
- ◆ バラバラなアカウントを統一＋それを強固に守る ⇒ 安全性と利便性を両立

パスワード (盗まれる・当てられる)



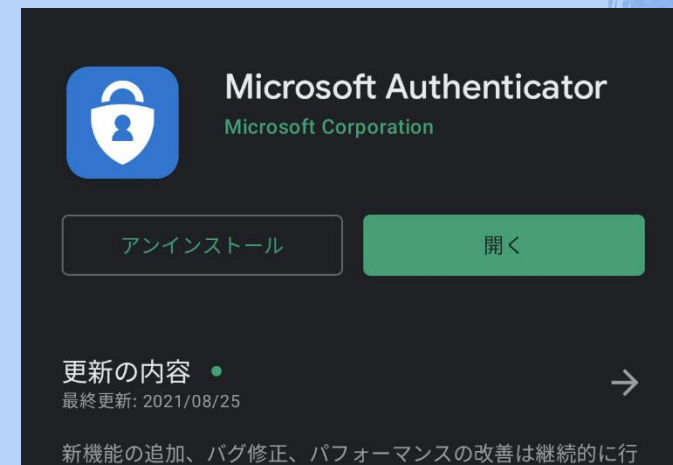
多要素 (例: スマホ) 盗まれる

# 面倒くさくないですか？

- ◆ 方法によって異なりますがスマホの認証アプリを用いた方法はかなり楽です
- ◆ UTokyo Account → Microsoft Authenticator
- ◆ スマホを常に持ち歩いている人なら≈**スマホを開く一手間**

- ◆ Android

- ◆ iOS



# 多要素認証デモ (utac)

- ◆ Microsoft Authenticator (推奨; 携帯を開けてタップするだけ)
- ◆ SMS (携帯電話に飛んでくる6桁の数字)
- ◆ 音声電話 (スマホじゃ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)

# 今後は多要素認証が必須ですか？

- ◆ セキュリティ向上（情報漏洩事故防止）のため強く推奨
  - ◆ 「必須か？」と問わず是非ご利用開始下さい
- ◆ 利便性と両立し、普及率を高める（利用率100%に近づける）のが現在の目標
- ◆ 当面、新しく導入するサービスを多要素認証必須とする方針
  - ◆ UTokyo VPN
  - ◆ UTokyo Slack



# お願い

- ◆ 特に学科で事務でSlackを使う場合「多要素認証はセキュリティ向上のため」と伝え、これを機に普及にご協力ください
  - ◆ 多要素はSlackのためならず
- ◆ 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





# Googleも多要素（2段階）認証！

- ◆ スマホでの認証操作はMicrosoft Authenticator同様簡単です
- ◆ 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はこちらの知らない「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ようです
  - ◆ 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

Account	多要素認証設定	パスワード変更
utac	<a href="#">utelecon: UTokyo Accountにおける多要素認証の利用</a>	<a href="#">UTokyo Account利用者メニュー</a>
Google	<a href="#">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</a>	<a href="#">ECCS利用者メニュー</a>

## ◆ [utac設定デモ](#)

# utac多要素認証にまつわる諸々

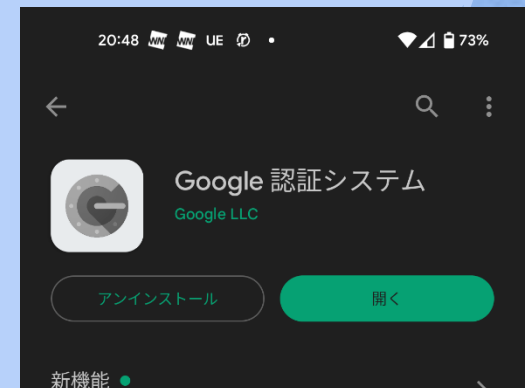
- ◆ 初期設定時の罠
- ◆ 要素は二つ以上設定がおススメ
- ◆ 「あの障害（こないだはa○）」対策
- ◆ スマホ・携帯を持っていない（持たない主義）
- ◆ しょっちゅう認証を求められるようになった気がする

# 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) 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

# 要素（認証手段）は二つ以上設定

- ◆ スマホと、別の電話（家の電話、職場の電話）を設定しておくのが吉
  - ◆ スマホを忘れても大丈夫
  - ◆ スマホを買い替えた時も大丈夫（別の方法で設定ページにサインインしてスマホを自力で再設定できる）
- ◆ Googleの2段階認証も同様
  - ◆ 固定電話（職場・いえ）
  - ◆ Google認証システム（6桁入力）







# 携帯電話会社の障害対策は？

- ◆ Google認証システム（6桁を入力する方式）は携帯の通信障害時でも使えます
- ◆ 実はMicrosoft Authenticatorも同じ使い方ができます
- ◆ その方法（動画）
  - ◆ スマホでMicrosoft Authenticatorアプリをタップして起動
  - ◆ The University of Tokyoを選択、6桁を表示

# スマホも携帯も持っていない（持たない主義）

- ◆ 多要素認証専用に必要な以下のいずれかの利用をご検討ください
  - ◆ 大学が貸し出しているガラ携電話（480円/月）
  - ◆ 固定電話x2（いえでんと職場電話）
    - ◆ 初期設定時に罫があります（おたずねください）
  - ◆ 専用ハードウェアトークン
    - ◆ 試験的に貸し出し中（物理的には10000円/台程度。費用負担方式検討中）
  - ◆ 専用セキュリティキー Yubico
    - ◆ 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）
    - ◆ 設定方法案内は少々お待ちください（巷に溢れていますがutacでの正解がわかりにくい）

# しよっちゅう認証を求められることがあった

- ◆ 8月の一時期、複数の方から頻繁に認証が必要で面倒過ぎ、多要素認証をやめたいという要望
- ◆ その時期、再認証頻度の設定を（あるガイドラインに従い）変更していた（一日に一度）
- ◆ その結果以下のような状況が発生したと分析
  - ◆ ブラウザ外で動くアプリ（VPN, Officeアプリなど）がパスワードを覚えず、パスワードを毎日、アプリごとに打つことになった
  - ◆ 「多要素の」認証が面倒というよりも（普通の）認証（パスワード入力）の頻度が問題であったと分析
  - ◆ ⇒ その後14日に一度に変更しています（今後も調整）



# 多要素認証取り消し方法 (...じゃなかったあの時に戻りたい)

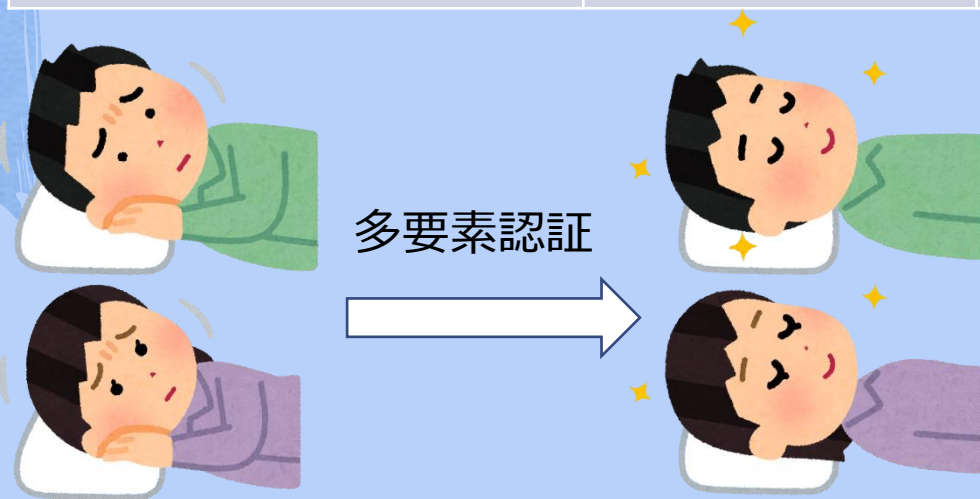
- ◆できるだけ思い止まって、と言った上で...
- ◆トラブルが生じるなど取り消しが必要な場合、通常のuteleconサポート窓口

<https://utelecon.adm.u-tokyo.ac.jp/support/>  
メールフォームからお申し込みください

- ◆UTokyo Accountをご記入ください
- ◆トラブルの症状を記入いただけると幸いです

# まとめ：多要素認証は安心を与えます

データのありか	代表的脅威	防衛手段
クラウド (UTokyo/Google Account)	パスワード流出	強固なパスワード・多要素認証
スマホ	物理的盗難・紛失	画面ロック（生体認証、番号入力）
PC	物理的盗難・紛失	手動ログイン、画面ロック、暗号化ドライブ



著作権フリー  
転載自由  
添削歓迎

ユータック  
パスワード入れたら  
スマホとる  
そのひと手間で  
秋しづかな

[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

口語訳：認証するたびにスマホを取る一  
手間は面倒だけど、それをしているから  
今日も安心して仕事ができるんだなあ