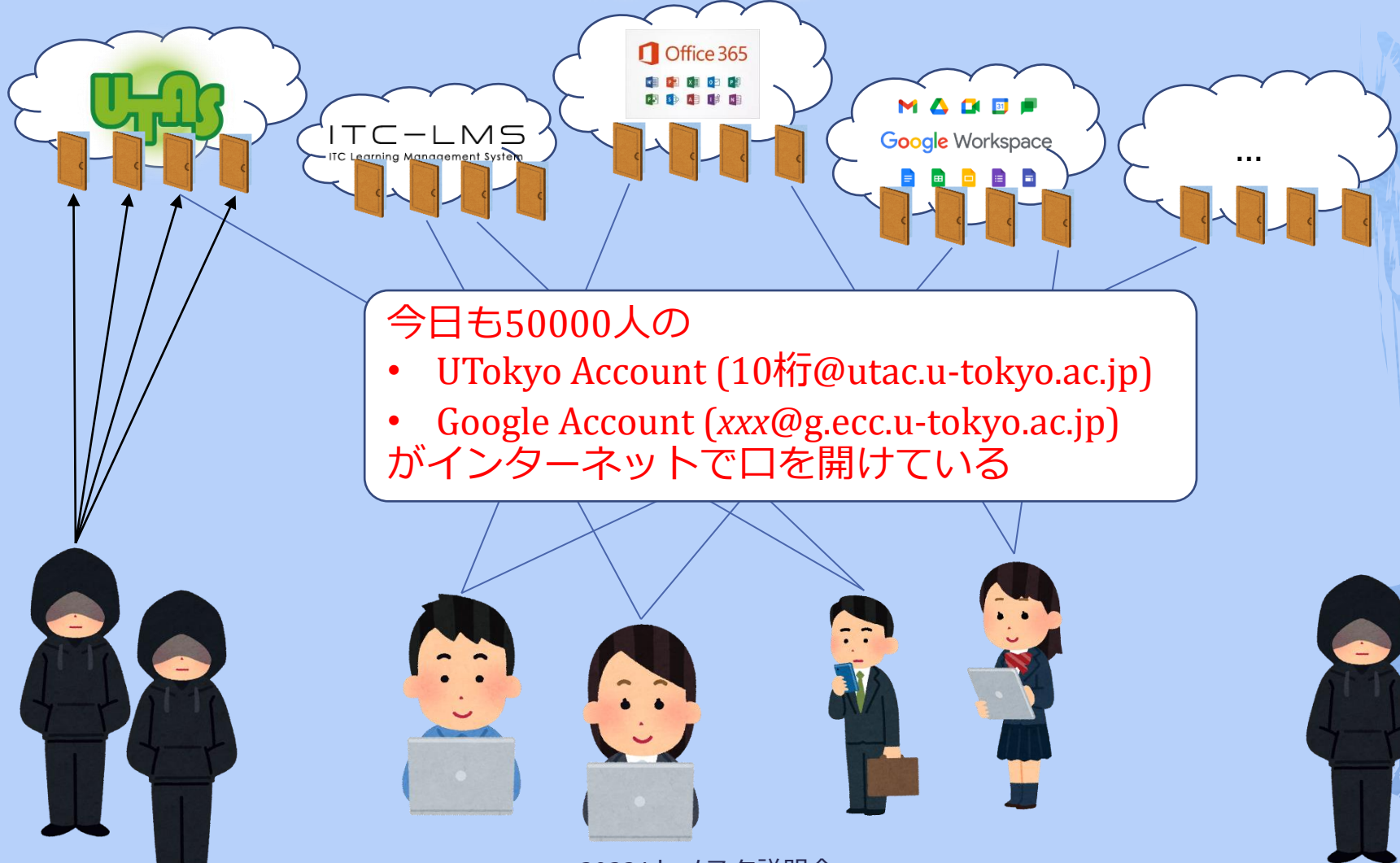


セキュリティの強化と多要素認証

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

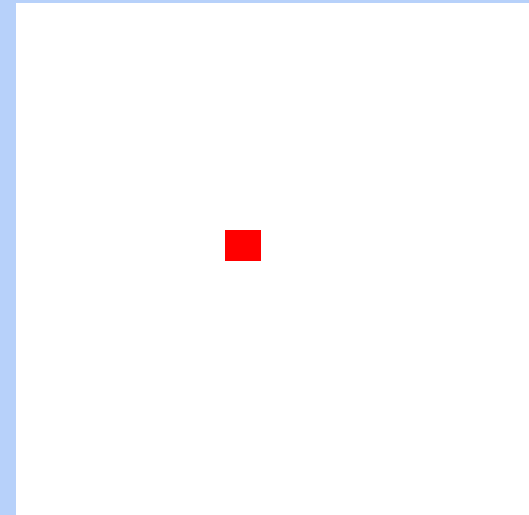
多要素認証とは

- ◆ 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」安全になります
- ◆ 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)



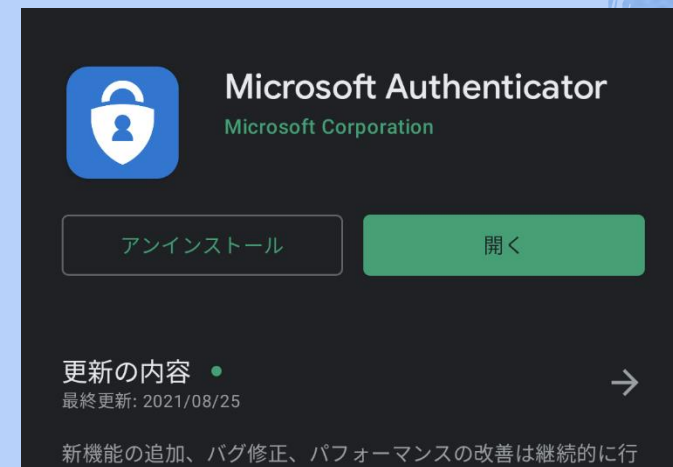
多要素 (例: スマホ) 盗まれる

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 (UTokyo Account)

- ◆ 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
- ◆ 利便性と両立し、普及率を高める（必須化の準備をする）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

- ◆ 学生に「多要素認証はセキュリティ向上のため」と伝え、設定をするようご指導ください
 - ◆ Slackに必要みたいだから、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

Googleも多要素（2段階）認証

- ◆ Q: スマホのあなたのログインですか「はい」「いいえ」みたいなダイアログは誰が出している?
 - ◆ Google認証アプリ?
 - ◆ Googleアカウント

設定方法

Account	多要素認証設定	パスワード変更
UTokyo	<u>utelecon: UTokyo Accountにおける多要素認証の利用</u>	<u>UTokyo Account利用者メニュー</u>
Google	<u>Googleアカウントセキュリティ</u>	<u>ECCS利用者メニュー</u>

多要素認証にまつわるtips

- ◆ 初期設定時の落とし穴
- ◆ 要素は二つ以上設定がおススメ
- ◆ 携帯会社（こないだはa○）の障害の時...
- ◆ 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

初期設定時の落とし穴

- ◆ 初期設定は以下の二つをやる必要がある
 - ◆ (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
- ◆ (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

要素は二つ以上設定がオススメ

- ◆ スマホと、別の電話（家の電話、職場の電話）を設定しておくと、**スマホを忘れても大丈夫**
- ◆ **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）

携帯電話障害おきたら大丈夫？

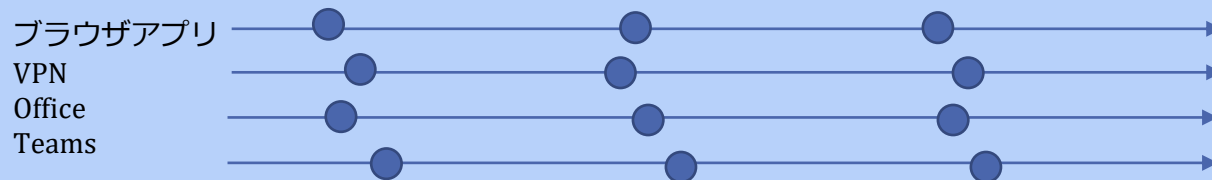
- ◆ Microsoft Authenticator, Google認証システムなどは携帯のデータ通信障害時でも使えます（通信がいらない）

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いずれかの利用をご検討ください
 - ◆ 固定電話（いえでんと職場電話）
 - ◆ 大学が貸し出している携帯電話（480円/月）
 - ◆ 専用ハードウェアトークン
 - ◆ 試験的に情報システム本部で貸し出し中（物理的には10000円/台程度。費用負担の方式検討中）
 - ◆ 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

しよっちゅう認証を求められることがあった

- ◆ 一時期（8/〇〇-）複数の方から面倒すぎるので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（1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えず、パスワードを毎日、アプリごとに打つことになった
 - ◆ ⇒ その後14日に一度に変更しています



多要素認証取り消し方法 (多要素じゃない認証に戻りたい)

- ◆できるだけ取り消さない、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：枕を高くして寝るには

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



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

スマホとる
ひと手間かけて
心はのどか