

多要素認証 設定マニュアル

情報戦略機構
2023/03/08版

このマニュアルでは、パソコンとスマホの2つを使いながら
設定をする方法を示します。
スマホだけで行おうとすると、ここに示す手順では設定できません。

「多要素認証の設定」とは

これから行う作業では、
本学の認証システム上の茨大IDと
個人が所持している「スマホ」とを対応づけます。



この資料に書いてある設定手順を開始したら、
後戻りや中断をせずに、必ず最後まで終わらせてください。



一度インストールしたスマホアプリは、**絶対に削除しない**でください。

スマホ側でアプリを削除しても、認証システム側の
設定情報が残るためリセットしたことになりません。
登録スマホをなくした状態と同じなので認証不能
になります。

用意するもの

以下のものを手元に用意してください。

- 自分のパソコン
- 自分のスマートフォン
- 自分の茨大IDとパスワード



茨大ID: XXXX@vc.ibaraki.ac.jp

Password: XYZZXX

事前準備

多要素認証に用いるアプリをスマホにインストールしてください。



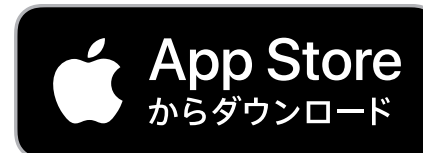
このアイコンのもの

公式ストアから
Microsoft Authenticator (無料)
をインストールしてください。

まだ起動しないでください。



Android : Google Play



iPhone : App Store

設定のおおまかな流れ

Microsoft365に
アクセスを試みる

多要素認証の認証方式を2種類 設定します。

認証アプリを用いた
認証方式の設定

1つ目の認証方式：認証アプリを
使う認証方式を登録します。

Microsoft365に
サインイン成功

電話番号を用いた
認証方式の設定

2つ目の認証方法：電話番号を
用いた認証方法を登録します。

完了！



認証手段を複数登録しておかない
とスマホの機種変更時に認証不能
になり、完全に詰みます。

以降のページで使用している画面は、2023年1月時点のものです。
将来、画面が少し変わっているかもしれませんが、似た項目を選んで進めてください。

Microsoft365にアクセスを試みる

パソコン操作

パソコンで設定を開始します

Webブラウザで情報戦略機構の
Webサイトにアクセス

<https://www.iims.ibaraki.ac.jp/>

「Mail, Microsoft365」のボタンをクリック

情報戦略機構
Institution for Information Management and Strategy

TOP 学生対象 ▾ 教職員対象 ▾ セキュリティ ▾ その他 ▾ 学内限定 (整理中) ▾

Mail, Microsoft365
Microsoft365

Password, 多要素認証
茨大IDについて
多要素認証

Wi-Fi, ネットワーク
情報機器利用登録システム

Teams

Frequently Asked Questions

問い合わせ, 相談
インシデント通報
Contact Center

機構からのお知らせ [\[全件\]](#)

【お知らせ】 デジタルサポート窓
2023-01-10 **[New!]**

【注意喚起】 Windows 8.1のサ:
【障害情報】 Thunderbird利用障
【お知らせ】 緊急メンテナンス
2022-12-16

【お知らせ】 【復旧】 Microsoft:
【障害情報】 【復旧】 本学のメー
障害について 2022-12-02

IIMSデジタルサポートでの対面対応について
新型コロナウイルス感染拡大防止のため、PCに関する相談など、IIMSデジタルサポート窓口での対面対応は当面の間、予約

サインイン画面

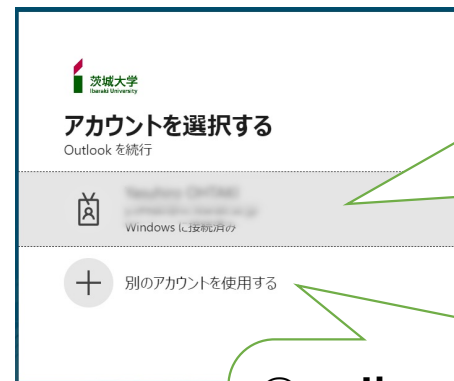
パソコン操作

サインイン画面が出ます



サインイン画面が出ずに、Microsoft365の画面になったら、何かしらの認証が済んでいます。[21ページ](#)に進み、設定を確認してください。

左の画面ではなく、以下のような画面が出る場合があります。



@vc.ibaraki.ac.jp
で終わる茨大ID
を選択する。

@vc.ibaraki.ac.jpで終わるものが
なければ、
「別のアカウントを使用する」
をクリックする。

パスワード認証

パソコン操作

茨大IDとパスワードを入力します。

茨城大学
Ibaraki University

サインイン

XXXXX@vc.ibaraki.ac.jp

アカウントをお持ちではない場合、作成できます。
アカウントにアクセスできない場合

次へ

サインイン オプション

茨城大学
Ibaraki University

← @vc.ibaraki.ac.jp

パスワードの入力

.....

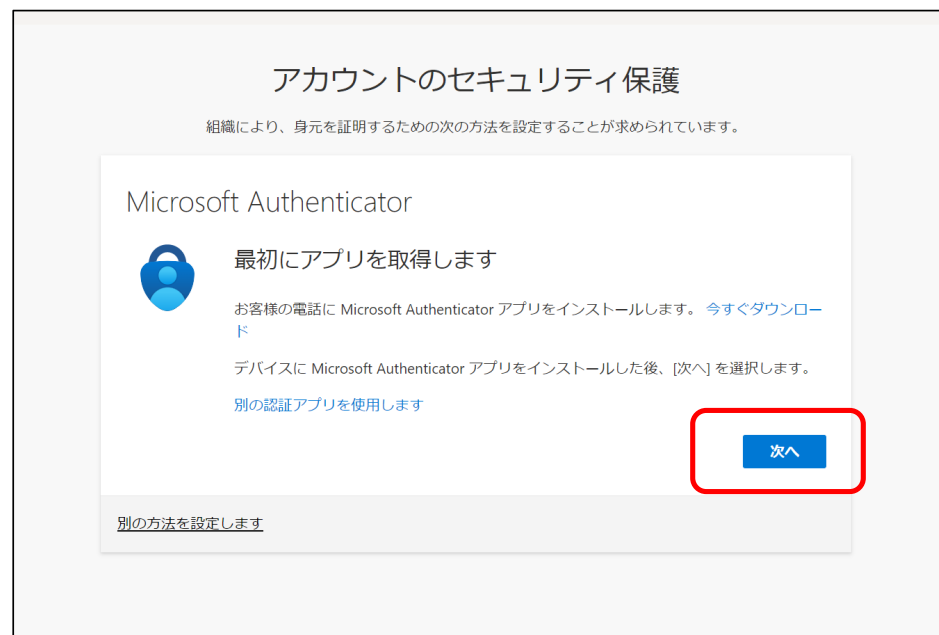
パスワードを忘れた場合

サインイン

1つ目の多要素認証の設定開始

パソコン操作

多要素認証の設定が行われていなければ、「詳細情報が必要」画面になります。



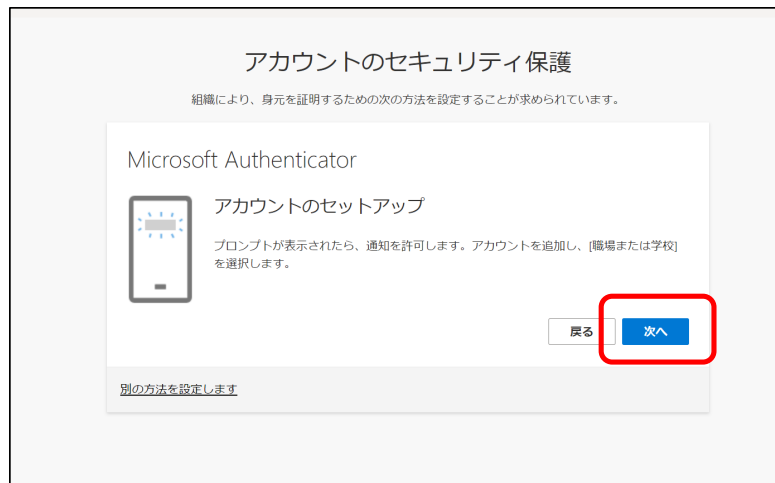
「詳細情報が必要」の画面ではなくMicrosoft365の画面になったら、多要素の設定は済んでいる可能性があります。
21ページに進んでください。

QRコードの表示

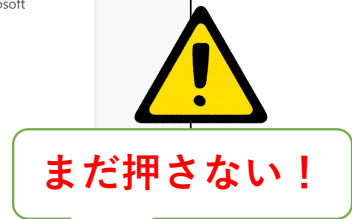
パソコン操作

認証アプリを使用した認証方法を
設定していきます。

QRコードが表示されたら、**PCの画面を
そのままにして次の手順に進んでください。**



このQRコードは後の手順で
Authenticatorアプリで読みます。
**通常のカメラアプリで
読むではありません。**



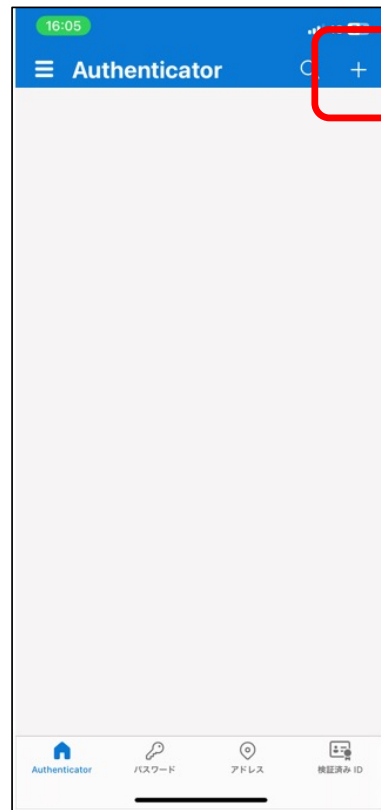
Authenticatorでアカウント設定

スマホ操作

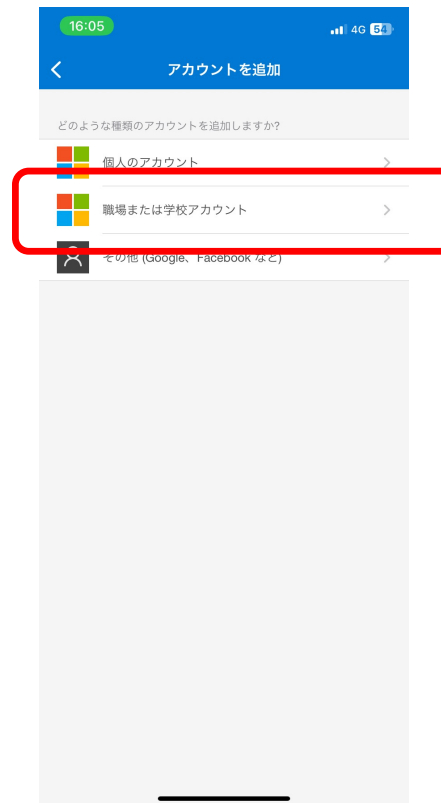
次は、スマホの操作です



Authenticator
アプリを
起動します。



「+」をタップ



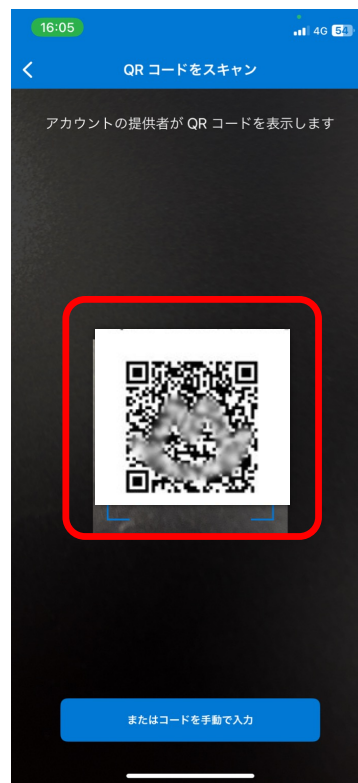
「職場または学校アカウント」を選択

AuthenticatorでQRコード読み込み

スマホ操作



「QRコードをスキャン」を選択



PC画面のQRコードを取り込みます



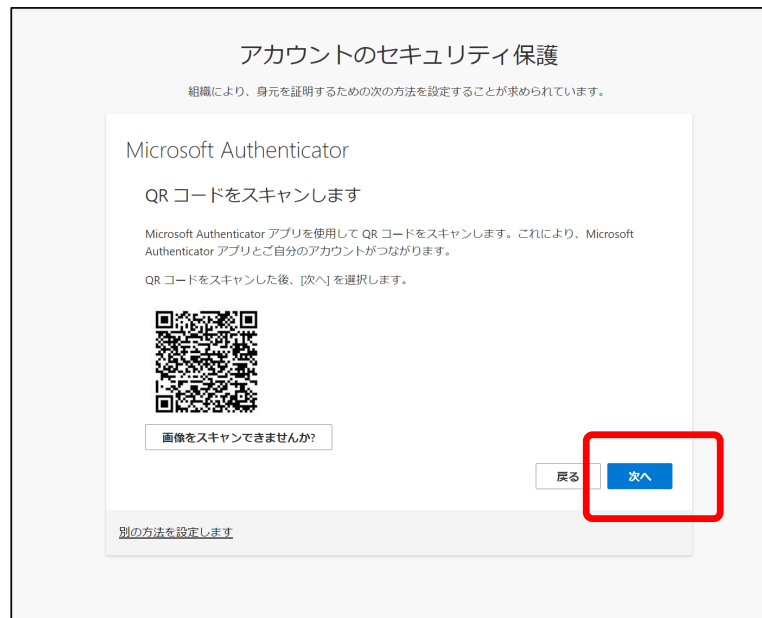
取り込み画面から変化したら次の手順に進んでください。

PCの画面を進める

パソコン操作

パソコンの操作

「次へ」をクリックすると、PC画面に**2桁の番号**が表示されます。



ほぼ同時にスマホアプリにも通知が送られます。
スマホ画面の説明は次のページです。

番号をスマホアプリに入力

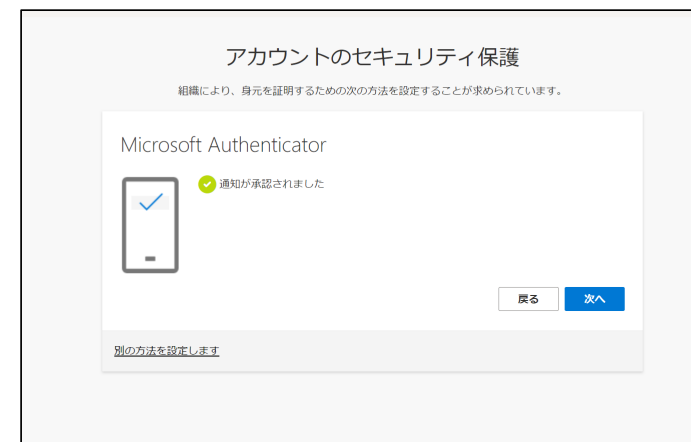
スマホ操作



通知を受けたスマホ画面には
「サインインしようとしていますか？」
というポップアップが表示されているはずです。

PC画面に表示されている番号を
アプリのポップアップ画面に入力し、
続いて「はい」をタップします。

「はい」をタップすると
スマホ画面のポップアップが消え、
PCの画面が右のようになります。

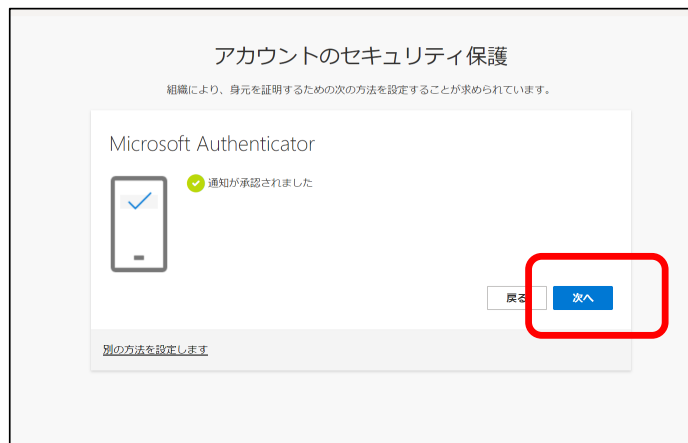


これで Authenticatorアプリは終了してかまいません。

認証成功→メール画面へ

パソコン操作

「次へ」をクリック、「成功」の画面になります。



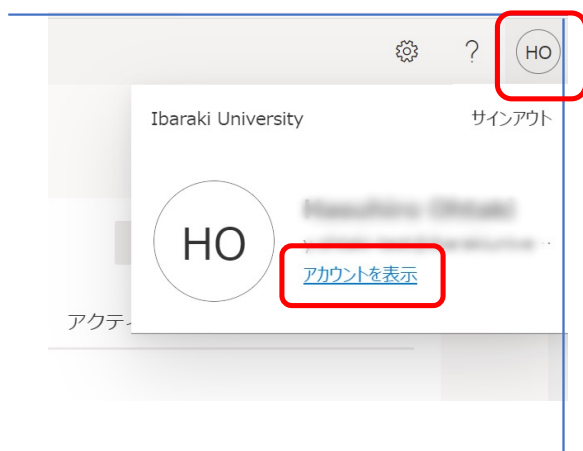
1つ目の認証方式の設定が終わりました。

続いて、スマホの機種変更時に困らないように
2つ目の認証方式の登録に進みます。

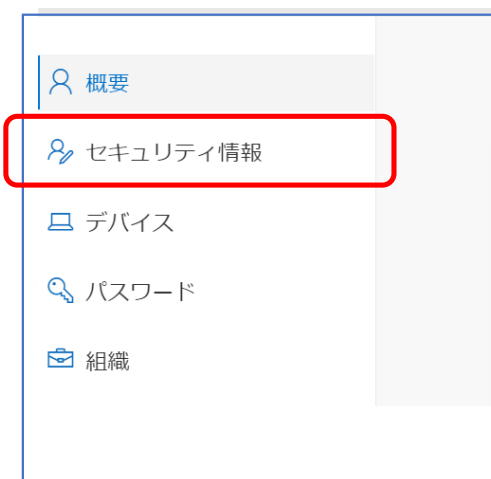
2つ目の認証方式の登録の開始

パソコン操作

メール画面の右上の自分のアイコンから、
「アカウントを表示」を選択



左端から「セキュリティ情報」をクリック



この画面は次のURLからもアクセスできます。
(要認証)

<https://myaccount.microsoft.com/?ref=MeControl>



「セキュリティ情報」画面

パソコン操作

現在の設定状況が表示されます。
「+サインイン方法の追加」をクリック



「電話」を選択→電話番号を入力

「電話」を選択し「追加」をクリック

方法を追加します

どの方法を使用しますか?

電話

キャンセル 追加

どちらでもかまいません

日本(+81)を選択

(自分のスマホの)
電話番号を入力

電話

電話で呼び出しに回答するか、携帯ショートメール (SMS) によるコードの送信により、本人確認ができます。

どの電話番号を使用しますか?

日本 (+81)

コードを SMS 送信する
 電話する

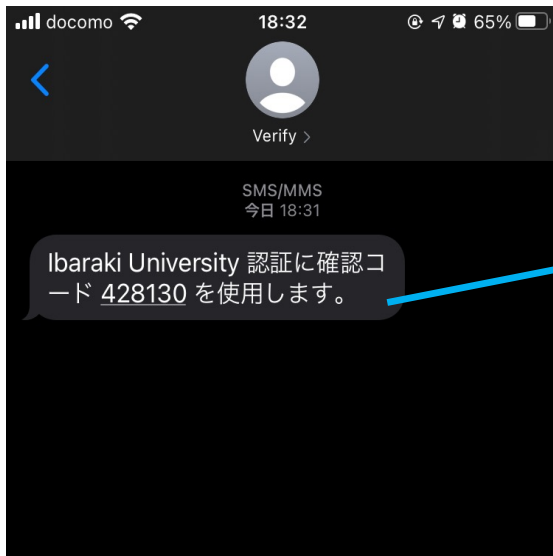
メッセージとデータの通信料が適用される場合があります。[次へ]を選択すると、次に同意したことになります: [サービス使用条件](#) および [プライバシーと Cookie に関する声明](#)。

キャンセル 次へ

SMSで送信されたコードをPCに入力する

「コードをSMS送信する」を選択した場合

6桁のコードがSMSで送信されます。
SMSに届いたコードをPC画面に入力します



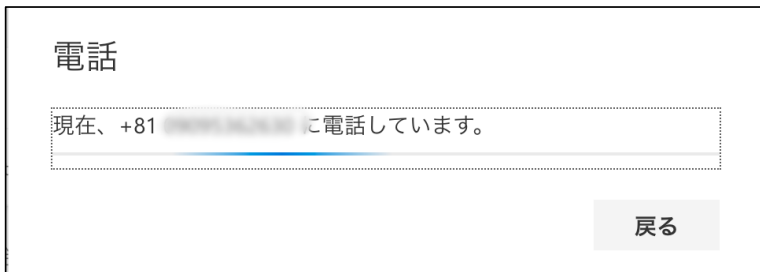
コードが着信まで少し時間がかかります。
SMSが届かない場合、「戻る」をクリック。
電話番号の間違いや着信拒否設定などを
確認してください。

A screenshot of a PC web interface titled 'アカウントのセキュリティ保護' (Account Security Protection). Below the title, it says '組織により、身元を証明するための次の方法を設定することが求められています。' (Depending on the organization, the following method is required to verify your identity). The main section is '電話' (Phone). It displays '+81 [redacted] に 6 桁のコードをお送りしました。コードを以下に入力してください。' (We have sent you a 6-digit code to +81 [redacted]. Please enter the code below). The input field contains '428130' and is highlighted with a red box. Below the input field is a link for 'コードの再送信' (Resend code). At the bottom right, there are two buttons: '戻る' (Back) and '次へ' (Next), with '次へ' highlighted in a red box. At the bottom left, there is a link for '別の方法を設定します' (Set a different method).A screenshot of the PC web interface showing the successful verification step. The title is '電話' (Phone). Below it, a green checkmark icon is followed by the message: 'SMS verified. Your phone was registered successfully.' At the bottom right, there is a '次へ' (Next) button highlighted in a red box.

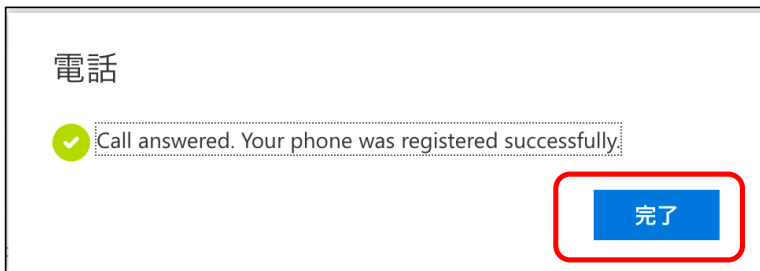
21ページに進んでください

かかってきた電話に対応する

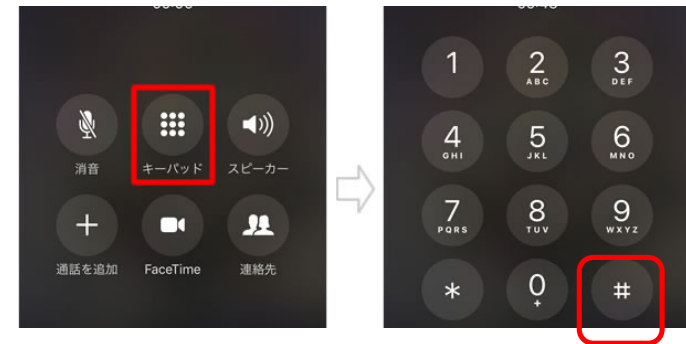
p.18で「通話」を選択した場合



PCの画面が
変わります。



入力した電話番号に電話がかかってきます。
電話を取った後、音声の指示に従って
キーパッド画面を出し、# を押します。

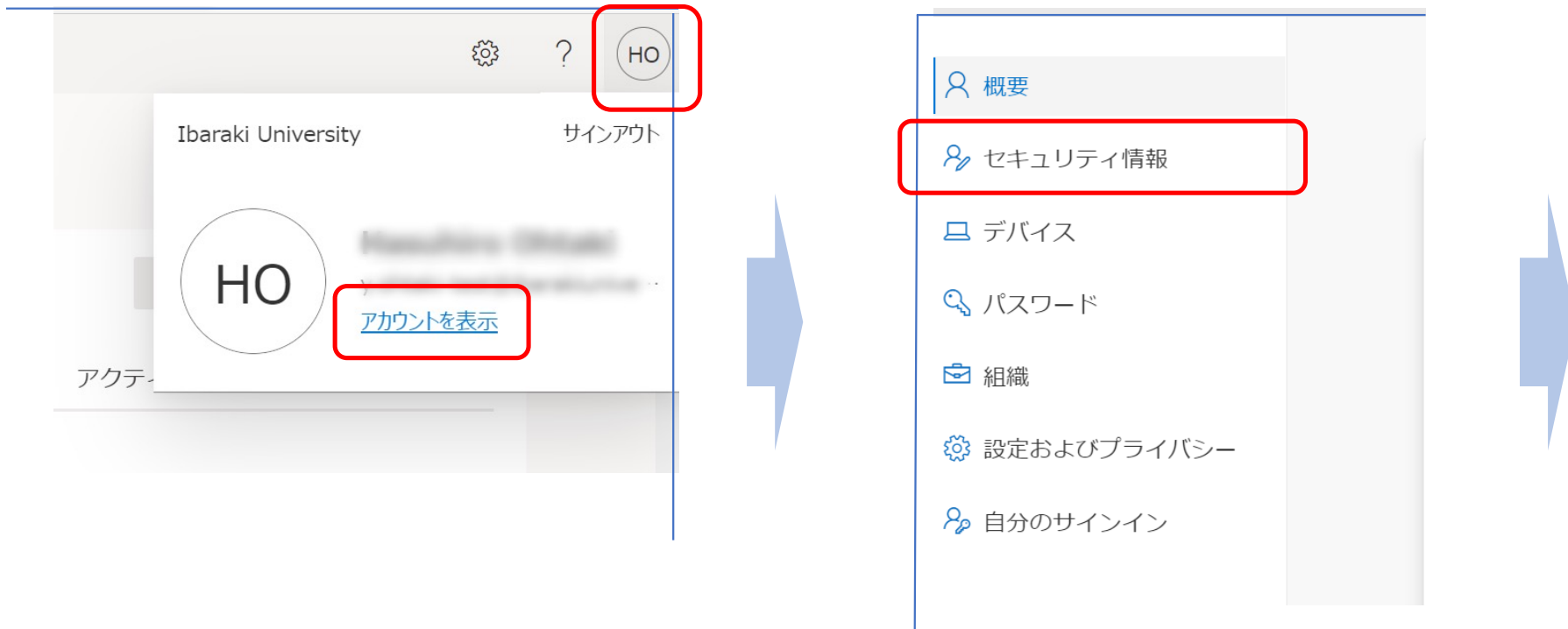


電話を切ります



「通話」で固定電話を登録すると、その場所以外で認証できなくなります。お勧めしません。
また固定電話が光電話の場合、パルス回線の設定になっていると「#」が機能しません。

設定できたか確認しましょう。



必ず2つの認証方式を登録してください！

認証アプリを使った多要素認証では、

「紐づけたMicrosoft Authenticatorが入っているスマートフォンを持っている人」だけが「本人」と認識されます。

つまり、

- ・ スマートフォンから Authenticator を消してしまった人
- ・ スマートフォンを紛失した人
- ・ 機種変して、紐づいていたAuthenticatorがない人

などは、認証アプリを使った認証ができません。

つまり、前のスマホが手元がない

その場合でも、2つ目の認証手段（電話番号）が登録されていればそれを使って認証を行い、認証アプリを設定し直すことができます。登録されていない場合には**完全に詰んだ状態**になります。



機種変更時は特に注意！

データやアプリを移行しても、Authenticatorの紐付け情報は移行されません。機種変更と同時に電話番号も変えてしまうと認証不能になります。