

情報戦略機構 2025/04/03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。



ー度インストールしたスマホアプリは、<mark>絶対に削除しない</mark>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。



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: XXYYZZXX





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。



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

このアイコンのもの

まだ起動しないでください。

設定のおおまかな流れ



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。

Authencatorはインストール済ですか?

次のページからセットアップが始まります。 セットアップを始めたら、途中でやめないこと!

何があっても、スマホのアプリは消すな!

Authenticatorの中のアカウントも消すな!

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



新型コロナ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



パスワード認証



茨大IDとパスワードを入力します。

交域大学 State Street 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 Terrate Versetry			
~		:@vc.ibaraki.ac.j	D	
)	(スワードの	入力		
				•
Л	スワードを忘れた場合	合		
				_

1つ目の多要素認証の設定開始



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。





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。



Authenticatorでアカウント設定



12



「+」をタップ

AuthenticatorでQRコード読み込み



スマホ操作

13

ください。

PCの画面を進める

パソコン操作

数値は毎回変わります。

送信している通知を承認します。

戻る

自分の画面の番号を覚えてください。

14

ここです。

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。

アカウントのセキュリティ保護 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。	アカウントのも 組織により、身元を証明するための次の
Microsoft Authenticator QR コードをスキャンします Microsoft Authenticator アブリを使用して QR コードをスキャンします。 ごれにより、Microsoft Authenticator アブリとご自分のアカウントがつながります。 QR コードをスキャンした後、[次へ] を選択します。 配像 Z キャンできませんか? Microsoft Authenticator の の の の の の の の の の の の	Microsoft Authenticator 試してみましょう 以下に表示されている番号を入力し <u>別の方法を設定します</u>

数秒以内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



戻る

次へ



認証成功→Microsoft365の画面へ



16



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





この画面は次のURLからもアクセスできます。 (<mark>要認証</mark>)

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

ttt ttt ttt ttt ttt ttt ttt ttt ttt tt	自分のサインイン 〜	品	?		
	セキュリティ情報 これは、ご自分のアカウントへのサインインやパスワードの再設定に使用する方法です。				
▶ 組織	既定のサインイン方法: Microsoft Authenticator - 通知 変更 + サインイン方法の追加				
≜ プライバシー	iPhone 13	削除			
	デバイスを紛失した場合 すべてサインアウトしてください				

方法を追加します	×
どの方法を使用しますか?	
方法を選択します	\sim
認証アプリ	
電話	
代替の電話	
会社電話	





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。



2(

21ページに進んでください

かかってきた電話に応対する



「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。



A 概要	
8 セキュリティ情報	
旦 デバイス	
🔍 パスワード	
▶ 組織	
🔅 設定およびプライバシー	
🔗 自分のサインイン	



「セキュリティ情報」で設定の確認



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<mark>紛失</mark>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。

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、Authenticatior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。

つまり、前のスマホが手元にない

