

# 多要素認証の初回設定方法

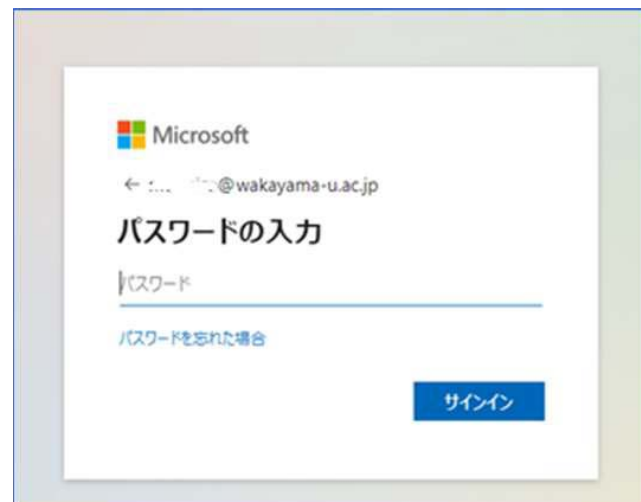
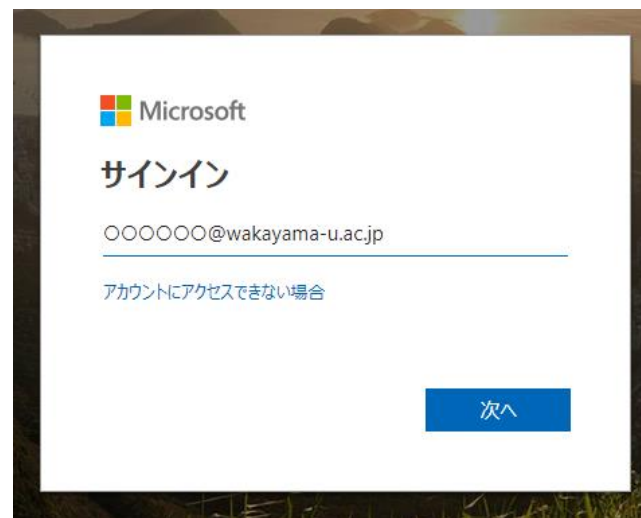
1. Webブラウザから<https://portal.office.com/>にアクセスします



2. 「サインイン」の画面が表示されますので、「[Wadai-ID]@wakayama-u.ac.jp」を入力し次へ進みます

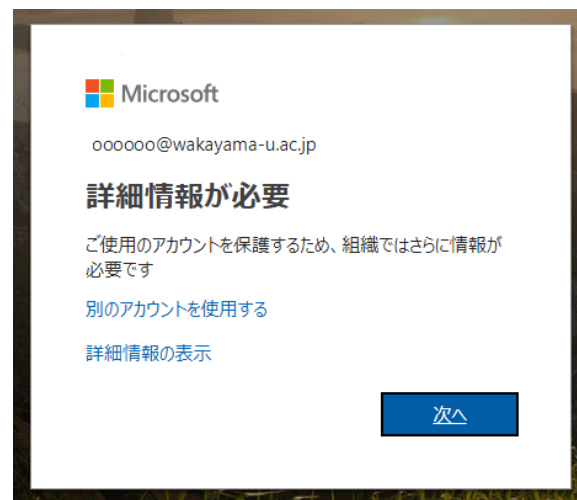


3. Wadai-IDのパスワードを入力します



# 多要素認証の初回設定方法

4. 「詳細情報が必要」の画面が表示されますので、次へ進みます



5. 「追加のセキュリティ確認」が表示されますので利用したい認証方法を選択・必要情報を入力し次へ進みます

認証方法は、

- 「認証用電話」
  - 「モバイルアプリ」
- が選択できます。



# 多要素認証の初回設定方法

## a. 「認証用電話」を利用する場合（利用する電話番号を入力）

1. テキストメッセージでコードを送信する  
→SMSでスマホ・携帯電話で受信した認証コードを入力します
2. 電話する  
→自動音声による電話がかかってくるので認証コード「#」を入力します

Microsoft  
追加のセキュリティ確認

パスワードに電話の確認を追加することにより、アカウントを保護します。アカウントをセキュリティで保護する方法についてビデオを見る

手順 1: ご希望のご連絡方法をお知らせください。

認証用電話

日本 (+81)

電話番号には、0～9の数字、ダッシュ、スペース、ピリオド、またはかっこのみを使用できます。

方法

テキストメッセージでコードを送信する

電話する

次へ

電話番号はアカウントのセキュリティのためにのみ使用されます。標準の電話料金とSMS料金が適用されます。

©2018 Microsoft 法的情報 | プライバシー

## b. 「モバイルアプリ」を利用する場合(事前にスマホへアプリのインストールが必要)

1. 「確認のための通知を受け取る」の場合  
セットアップをクリックし、次に表示されるQRコードをMicrosoft Authenticatorアプリにてスキャンします  
モバイルアプリの「認証」をタップします。

Microsoft  
追加のセキュリティ確認

パスワードに電話の確認を追加することにより、アカウントを保護します。アカウントをセキュリティで保護する方法についてビデオを見る

手順 1: ご希望のご連絡方法をお知らせください。

モバイルアプリ

モバイルアプリをどのような用途で使用されますか?

確認のための通知を受け取る

確認コードを使用する

これらの確認方法を使用するには、Microsoft Authenticator アプリをセットアップする必要があります。

セットアップ

モバイルアプリケーションが構成されました。

次へ

©2018 Microsoft 法的情報 | プライバシー



Microsoft Authenticator アプリ  
Android/iOS版インストールはこちらから  
<http://aka.ms/authapp>  
※PCではご利用いただけません

サインインを承認しますか?  
サインイン認証を完了するには、[認証] を  
タップしてください。  
Microsoft AD

拒否

認証

# 多要素認証の初回設定方法

2. 「確認コードを使用する」の場合  
表示されるQRコードをモバイルアプリのカメラ  
にてスキャンして次へをクリックします。  
モバイルアプリに表示される確認コードを入力  
し、確認をクリックします。

追加のセキュリティ確認

パスワードに電話の確認を追加することにより、アカウントを保護します。アカウントをセキュリティで保護する方法についてビデオを見る

手順 2: モバイル アプリから確認パスワードを入力してください  
アプリケーションに表示されている確認コードを入力してください。

キャンセル 確認



モバイル アプリケーションの構成

次の手順でモバイル アプリケーションを構成してください。

1. Windows Phone、Android、または iOS の Microsoft Authenticator アプリをインストールします。
2. アプリでアカウントを追加し、「職場または学校アカウント」を選択します。
3. 下の画像をスキャンしてください。

画像をスキャンできない場合は、アプリケーションに次の情報を入力してください。  
コード: 024 134 867  
URL: <https://co1pfpad03.phonefactor.net/pad/396056683>

アプリケーションに 6 桁のコードが表示されている場合、[次へ] を選択します。

次へ キャンセル

いずれの認証方法でも最後に確認メッセージが表示されるので次へをクリックします。

追加のセキュリティ確認

パスワードに電話の確認を追加することにより、アカウントを保護します。アカウントをセキュリティで保護する方法についてビデオを見る

手順 1: ご希望のご連絡方法をお知らせください。

モバイル アプリ

モバイル アプリをどのような用途で使用されますか?

確認のため通知を受け取る

確認コードを使用する

これらの確認方法を使用するには、Microsoft Authenticator アプリをセットアップする必要があります。

セットアップ 通知と確認コード用にモバイル アプリが構成されました。

次へ

# 多要素認証の初回設定方法

## 6. 追加のセキュリティ確認

手順1でモバイルアプリを選択した場合

最初に登録した認証方法が利用できない場合の認証方法（電話番号）を登録します。



The screenshot shows the Microsoft account security setup interface. At the top left is the Microsoft logo. The main heading is "追加のセキュリティ確認" (Additional Security Confirmation). Below this, there is a link: "パスワードに電話の確認を追加することにより、アカウントを保護します。アカウントをセキュリティで保護する方法についてビデオを見る" (By adding phone verification to your password, you can protect your account. Watch a video about how to protect your account with security). The section is titled "手順 3: モバイル アプリにアクセスできなくなった場合" (Step 3: If you can no longer access your mobile app). There is a dropdown menu showing "日本 (+81)" and an empty text input field for the phone number. A red warning message states: "電話番号には、0～9の数字、ダッシュ、スペース、ピリオド、またはかっこのみを使用できます。" (Phone numbers can only use digits 0-9, dashes, spaces, periods, or parentheses). At the bottom right is a blue button labeled "次へ" (Next). At the bottom left, a box contains the text: "電話番号はアカウントのセキュリティのためにのみ使用されます。標準の電話料金と SMS 料金が適用されます。" (Phone numbers are used only for account security. Standard phone rates and SMS fees apply).

# 多要素認証の初回設定方法

最後に「**アプリパスワード**」が発行されます。

- 多要素認証に対応していないアプリ等で認証を行う際に使用します。
- アプリパスワードは何回でも発行可能なので、すぐに使用しない場合はそのまま「完了」をクリックしてください。
- アプリパスワードはメモ等せずに必要になった際に都度発行してください。

## 追加のセキュリティ確認

パスワードに電話の確認を追加することにより、アカウントを保護します。 [アカウントをセキュリティで保護する方法についてビデオを見る](#)

### ステップ 4: 既存のアプリケーションを引き続き使用する

Outlook、Apple Mail、また Microsoft Office などのアプリでは、アカウントの保護のために電話を使用することはできません。これらのアプリを使用するには、職場または学校アカウントのパスワードの代わりに新たなアプリパスワードを作成する必要があります。 [詳細情報を見る](#)

このアプリパスワードで今すぐ開始:

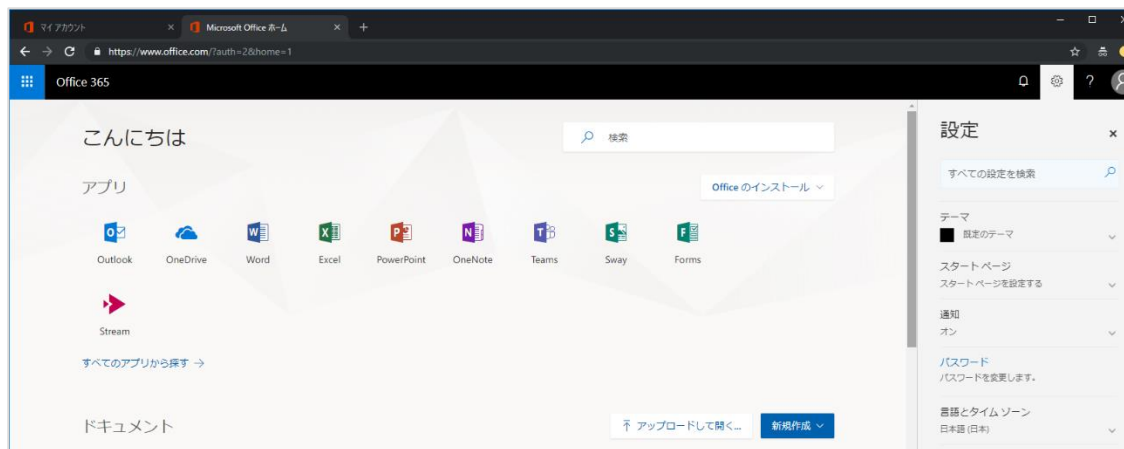


← アプリケーションパスワード

完了

# 多要素認証の初回設定方法

多要素認証設定が完了し、ポータルサイトのTOPページが表示されます



モバイルアプリにより多要素認証登録を行った場合は、  
モバイル機器の画面タップのみで二段階目の認証が完了します。

## 多要素認証上の注意事項

---

- 学外（学内にいてもLTE回線等を経由する場合は学外と同じ）からのMicrosoft365にWebログインの際は多要素認証が必須となります。将来的に利用が見込まれる場合は学外から利用可能な方法（携帯電話番号、モバイルアプリ等）にて事前に多要素認証の設定をお願いします
  - 初回登録後に他方式での多要素認証の追加設定が複数可能です。デバイスを忘れた・紛失したなどの際も予備の方式をバックアップとして登録しておくことでログインが可能となりますので、複数の要素登録を強く推奨します
  - 学内ネットワークからの利用であっても、新しいデバイスでの初回認証時や重要情報の設定時など多要素認証が必要となる場合があります
  - 「アプリによる確認コード表示方式」はLTE回線が圏外でも利用可能ですので推奨いたします
  - 特に外国出張時は音声/SMSの着信ができない場合やローミング通信料が必要になるなど、通常とは異なる環境が想定されますので事前に確認・設定をおすすめいたします
- デバイス紛失等による多要素認証の再設定は（アカウントID・パスワード再発行と同様に）本人確認が必要となるため、電話・メールではお受けできませんのでご注意ください
  - 学術情報センター窓口にて対応いたします