

# Microsoft365

## 多要素認証設定マニュアル

### (Microsoft Authenticator)

情報システム課 ヘルプデスク

#### 目次

はじめに .....	1
多要素認証とは .....	1
認証方法について .....	1
パスワードレス認証について.....	2
注意事項 .....	2
設定手順 .....	2
Microsoft Authenticator アプリについて.....	3
① 端末へのインストール方法 .....	3
② 初回起動時の利用について(アプリインストール後) .....	4
多要素認証とパスワードレス認証の設定について.....	5
③ 認証デバイス登録方法 .....	5
多要素認証設定後サインインする方法 .....	12
確認コードの入力が求められた場合 .....	14
スマートフォンで入力番号が確認できなかった場合.....	15
機種変更時に必要な手順について .....	16

※Microsoft 社の仕様変更により、画面が変更になる場合があります。

## はじめに

本学では、学外のネットワークから Teams や Outlook などの Microsoft365 へサインインする際に、多要素認証を導入しています。

### 多要素認証とは

- ID/パスワード入力に加え、スマホ通知の承認や、ワンタイムパスワードコードの入力による本人確認を行うことで、本人以外の第三者が不正にアクセスすることを防止する仕組みです。

### 認証方法について

- 多要素認証を使用した Microsoft365 への認証方法は主に 4 通りとなります。  
「Microsoft Authenticator」で認証を行う方法は 3 もしくは 4 となります。
- ※ 「Microsoft Authenticator」とは、Microsoft 社から無償で提供されている認証用のアプリケーションです。

本マニュアルでは、Microsoft Authenticator アプリを利用した **3 と 4** を解説します。

1. アカウントとパスワードを入力後、Microsoft へ自動音声による電話着信を依頼し、着信時に「#」キーの入力が求められるので、「#」キーを押してサインインする方法。
2. アカウントとパスワードを入力後、Microsoft へ SMS で数字 6 桁のセキュリティコード発行を依頼し、受け取ったコードを Microsoft365 に入力してサインインする方法。
3. **Microsoft Authenticator アプリをスマートフォンにインストールし、アカウントを入力後、アプリで画面に表示された 2 桁の番号を入力し、[はい]をタップしてサインインする方法。**
4. **Microsoft Authenticator アプリをスマートフォンにインストールし、アカウントとパスワードを入力後、アプリに表示された数字 6 桁のセキュリティコードを Microsoft365 に入力してサインインする方法。**

上記の 1 や 2 にあるような、電話や SMS を使って認証される方は、[「Microsoft365 多要素認証設定マニュアル \(電話・SMS\)」](#)を参照してください。

## パスワードレス認証について

Teams や Outlook などでは利用する本学 Microsoft 365 アカウントは、「**パスワードレス認証**」が利用できます。  
「**パスワードレス認証**」は、サインイン時にパスワードを入力する必要が無く、認証時にパスワード漏えいの恐れが無い、次世代の認証として利用が進んでいます。

- 従来のサインイン方法
  - ・「**ID**」+「**パスワード**」による従来の認証(学内ネットワークのみ利用可)
  - ・「**ID**」+「**パスワード**」に加え、「**認証デバイス**」による多要素認証(本人確認)を加えた認証(学外ネットワークからサインインする場合は必須)
- パスワードレス認証のサインイン方法
  - ・「**ID**」+「**認証デバイス**」による本人確認を兼ねた認証(学内外ネットワークで利用可)

## 注意事項

- ネットワークに接続されていない環境では、多要素認証の設定ができません。
- 学内のネットワーク(公衆無線 LAN 含む)を利用する場合に限り、多要素認証を行わずに Teams や Outlook などを利用することができます。
- 学外のネットワークから Microsoft365 にサインインする際は、認証デバイスによる多要素認証にて本人確認を行う必要があります。
- 「Microsoft Authenticator」の対応 OS は「iOS 最新の 3 つのバージョンのいずれか」、「Android OS 8.0 以降」です。
- 設定完了後も Microsoft Authenticator アプリは、アンインストールしないでください(※機種変更した場合は除く)。
- このマニュアルでは、スマートフォンは iPhone、ブラウザアプリは Safari を使用しています。  
機種によっては表示される画面が異なる場合がございます。

## 設定手順

下記のページ番号に従って進んでください。

### 手順 1 Microsoft Authenticator アプリのインストール

→[P.3「①端末へのインストール方法」](#)

### 手順 2 Microsoft Authenticator アプリの初回起動

→[P.4「②初回起動時の利用について\(アプリインストール後\)」](#)



### 手順 3 多要素認証とパスワードレス認証の設定

→[P.5「③認証デバイス登録方法」](#)

## Microsoft Authenticator アプリについて

### ① 端末へのインストール方法

※既にアプリケーションをインストールしている場合は、[P.5「多要素認証とパスワードレス認証の設定について」](#)以降をご確認ください。

手順	
<p>「Microsoft Authenticator」をインストールします。</p>	<p>&lt;Microsoft Authenticator&gt;</p> <div data-bbox="737 636 1034 940">  </div> <p>&lt;iPhone の場合&gt;</p> <p>「App Store」からインストールします。</p> <p><a href="https://apps.apple.com/jp/app/microsoft-authenticator/id983156458">https://apps.apple.com/jp/app/microsoft-authenticator/id983156458</a></p> <div data-bbox="762 1218 1002 1456">  </div> <p>&lt;Android の場合&gt;</p> <p>「Google Play」からインストールします。</p> <p><a href="https://play.google.com/store/apps/details?id=com.azure.authenticator&amp;hl=ja">https://play.google.com/store/apps/details?id=com.azure.authenticator&amp;hl=ja</a></p> <div data-bbox="762 1747 1002 1984">  </div>

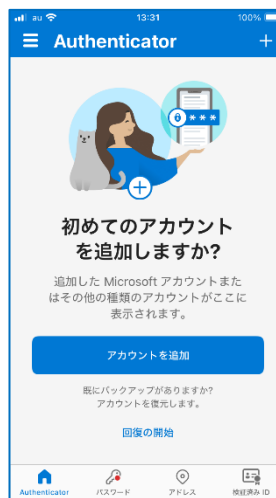
## ② 初回起動時の利用について(アプリインストール後)

### 手順

インストール完了後、初回起動時に表示されます。[承諾する]-[続行]-[スキップ]をクリックします。



この画面が出てきたら、下記手順に沿って多要素認証を設定してください。

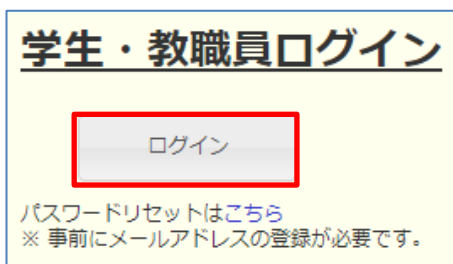
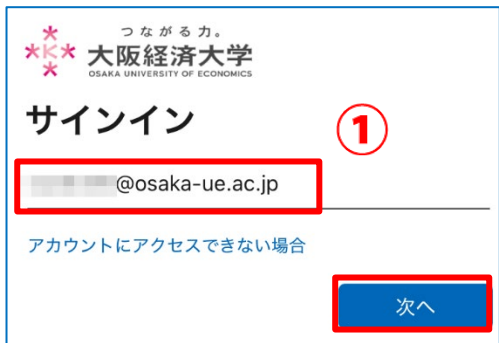
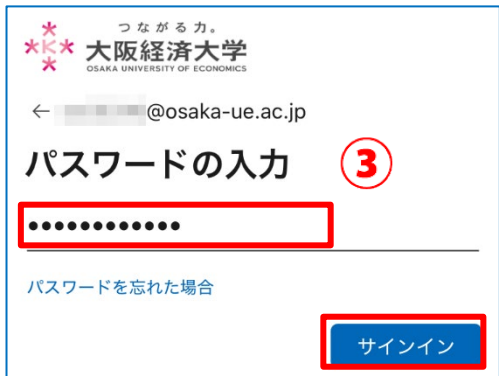


## 多要素認証とパスワードレス認証の設定について

### ③ 認証デバイス登録方法

※スマートフォンを使用して設定してください。

※以下の手順では、スマートフォンは iPhone、ブラウザアプリは Safari を使用しています。

手順	
1. スマートフォンで KVC にアクセスします。	https://kvc.osaka-ue.ac.jp/
2. [ログイン]ボタンをタップします。	
3. サインイン画面が表示された場合は、ID を入力後 [次へ]、パスワード入力後[サインイン]をタップしま す。 ID 欄： <b>「ユーザー名」+ @osaka-ue.ac.jp</b> <b>※ID とメールアドレスは違う場合があります。</b> パスワード欄： 本学システムユーザー名に対応したパスワード	 <p style="text-align: center;">↓</p> <div style="border: 1px solid orange; padding: 5px; width: fit-content; margin: 0 auto;">       ID を入力すると画面が        遷移し、パスワード入力        の画面が表示されます。     </div> 

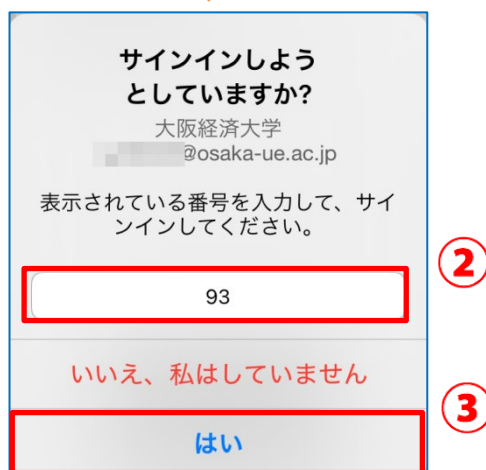
<p>4. [次へ]をタップします。</p>	
<p>5. [次へ]をタップします。</p>	
<p>6. [このリンクをクリックして、アカウントをアプリにペアリングします。] をタップします。</p>	

7. [開く]をタップします。	
8. Microsoft Authenticator アプリが開き、通知の許可を求められたら、[許可]をタップしてください	
9. 本学アカウントが追加されます。	
10. ブラウザアプリに戻り、[次へ]をタップします。	

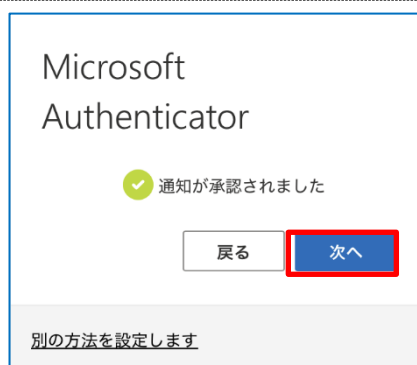


11. ブラウザアプリに 2 桁の番号が表示され、Microsoft Authenticator アプリに通知が届くため、通知をタップします。

Microsoft Authenticator アプリにて、ブラウザアプリに表示された番号を入力して[はい]をタップすると、手順 9 と同じ画面が表示されます。



12. ブラウザアプリに戻り、[次へ]をタップします。



<p>13. [完了]をタップします。</p> <p>以上で多要素認証の設定は完了です。 パスワードレス認証の設定を行う場合、下記の手順を実施してください。</p>	
<p>14. 「Microsoft Authenticator」アプリを起動します。</p>	
<p>15. 本学アカウントをタップします。</p>	
<p>16. [パスワードレス サインイン要求の設定]をタップします。</p>	

17. [続行]をタップします。

※表示されていない場合は、画面を下へスクロールしてください。



18. 2 桁の番号が表示され、自動的に番号の入力画面が開くため、2 桁の番号を入力して、[はい]をタップします。

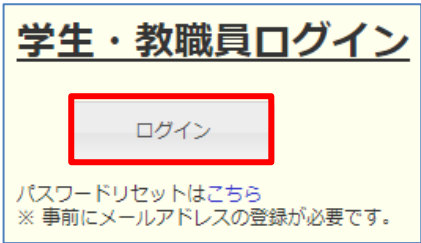

※2 桁の番号を確認できなかった場合、[番号が表示されません]をタップすると、番号が再度表示され、自動的に入力画面に戻ります。



本学アカウントをタップし、「パスワードレス サインイン要求」と表示されていれば設定完了です。

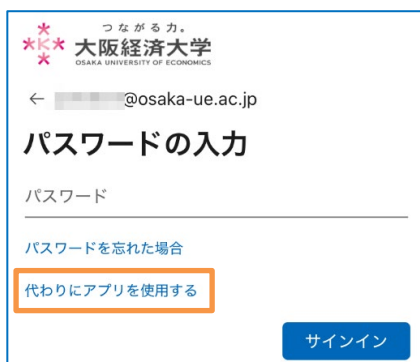


## 多要素認証設定後サインインする方法

手順	
1. KVC にアクセスします。	<a href="https://kvc.osaka-ue.ac.jp/">https://kvc.osaka-ue.ac.jp/</a>
2. [ログイン]ボタンをクリックします。	
3. 認証画面が表示された場合は、ユーザー名を入力し、[次へ]をクリックします。  ID 欄： <b>「ユーザー名」+ @osaka-ue.ac.jp</b> <b>※ID とメールアドレスは違う場合があります。</b>	

4. 2 桁の番号が表示され、Microsoft Authenticator アプリに通知が届くため、アプリを起動し、2 桁の番号を入力し、[はい]をタップします。

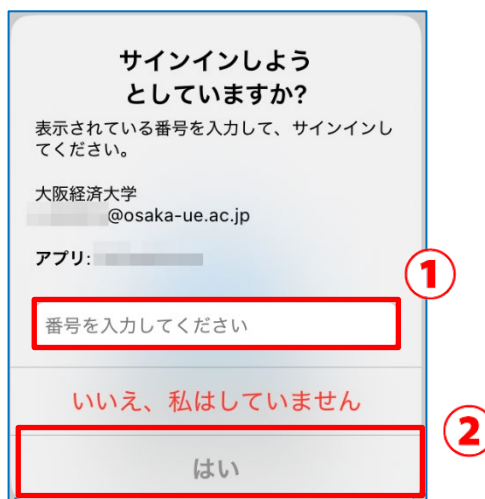
※ユーザー名を入力後、パスワード入力画面が表示された場合は、[代わりにアプリを使用する]をタップしてください。



※6 桁の確認コード入力を求められた場合は、[P.14「確認コードの入力を求められた場合」](#)を参照してください。

※スマートフォンでアクセス時、入力する番号を確認できなかった場合は、[P.15「スマートフォンで入力番号が確認できなかった場合」](#)を参照してください。

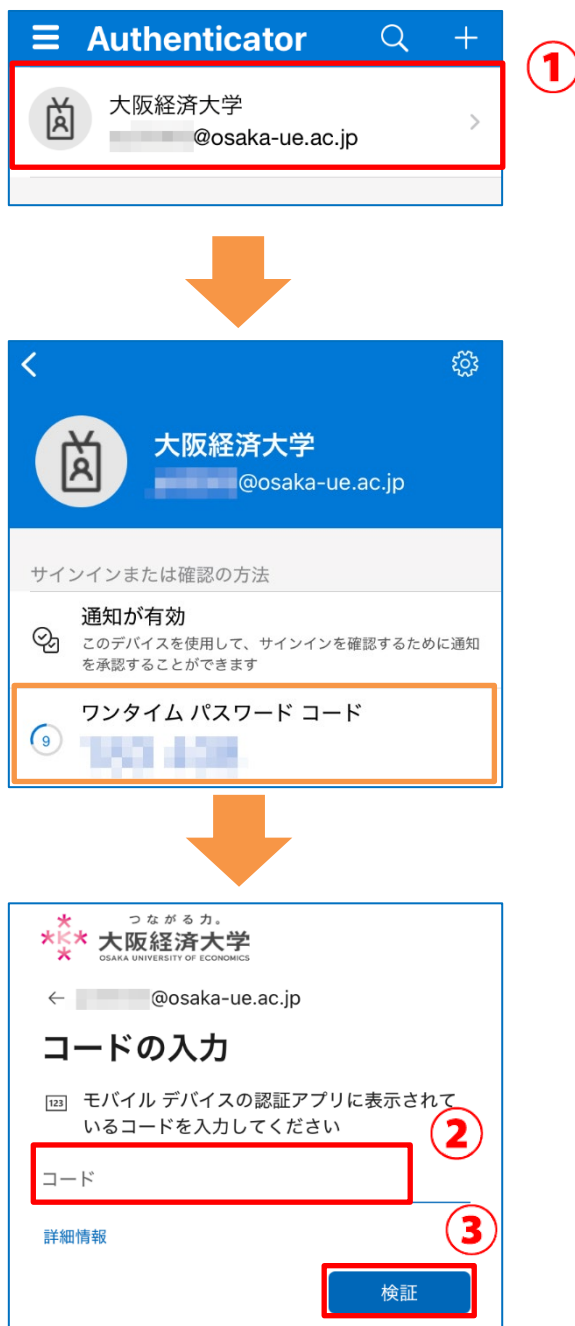




## 確認コードの入力が求められた場合

### 手順


Microsoft Authenticator アプリを起動し、アカウント名をクリックします。[ワンタイムパスワードコード欄]に表示されている 6 桁のコードをパソコンのコード入力画面に入力し、[検証]をクリックします。



The screenshot illustrates the steps for entering a confirmation code in the Microsoft Authenticator app:

- Step 1:** The app's main screen shows a list of accounts. The account "大阪経済大学" (Osaka University) with email "@osaka-ue.ac.jp" is selected, indicated by a red box and a circled "1".
- Step 2:** The app displays the "サインインまたは確認の方法" (Sign in or verification method) screen. The "ワンタイム パスワード コード" (One-time password code) option is selected, indicated by a red box and a circled "2".
- Step 3:** The app displays the "コードの入力" (Code entry) screen. The user is prompted to enter the 6-digit code displayed on their mobile device. The input field is highlighted with a red box and a circled "2". A "詳細情報" (More info) link is also visible, highlighted with a red box and a circled "3". The "検証" (Verify) button is at the bottom right, also highlighted with a red box.

スマートフォンで入力番号が確認できなかった場合

手順	
<p>[番号が表示されません]をクリックすると、番号が確認できます。[番号を入力してください]をクリックすると、入力画面に戻ります。</p>	<div> <p><b>サインインしよう としていますか？</b></p> <p>大阪経済大学 @osaka-ue.ac.jp</p> <p>表示されている番号を入力して、サインインしてください。</p> <p>アプリ: Microsoft Teams</p> <p>番号を入力してください</p> <p>はい</p> <p>いいえ、私はしていません</p> <p><b>番号が表示されません</b></p> </div> <p>↓</p> <div> <p>キャンセル <b>番号を入力してください</b></p> <p>        つながる力。  <b>大阪経済大学</b>        OSAKA UNIVERSITY OF ECONOMICS        @osaka-ue.ac.jp     </p> <p><b>サインイン要求を承認</b></p> <p>        Authenticator アプリを開き、表示されている番号を入力してサインインします。     </p> <p><b>43</b></p> <p>アプリに数字が表示されませんか？ 最新バージョンにアップグレードしてください。</p> <p>Microsoft Authenticator アプリを現在使用できません</p> </div>






## 機種変更時に必要な手順について

スマートフォンの機種変更などにより、認証に使っているスマートフォンが変わる際は、こちらの手順をご参照ください。

多要素認証の方法や、多要素認証に使っているスマートフォンの情報を、ご自身で変更する手順です。

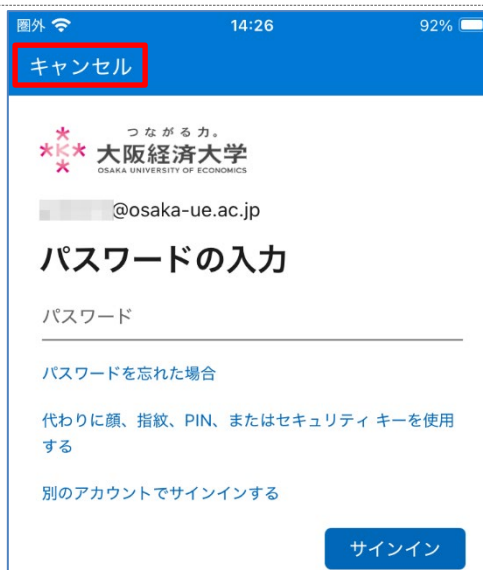
※ 機種変更前のスマートフォンが手元にない場合や、故障や初期化で認証の通知が来ない場合は情報システム課までご連絡ください。

手順	
1. <a href="#">P.12「多要素認証設定後サインインする方法」</a> を参照して、KVC にログインしてください。	
2. 上部の[Microsoft365]をタップします。	
3. メールが表示されるので、画面右上の[アカウントマネージャー]-[アカウントを表示]をタップします。	
4. 「セキュリティ情報」の[更新情報]をタップします。 ※ 認証デバイスによる承認が求められた場合、 <a href="#">P.13「多要素認証設定後サインインする方法」手順 4</a> を参照して承認してください。	

<p>5. 出てきたセキュリティ情報の、「Microsoft Authenticator」の下にある[削除]をタップします。</p>	
<p>6. 確認画面が表示されるので、[OK]をタップします。</p>	
<p>7. 画面上に「認証アプリが削除されました」と表示されるので、削除されたことを確認します。</p>	

<p>8. Microsoft Authenticator アプリを起動し、アカウント名をタップします。</p> <p>機種変更前の端末はデバイス内のアカウントを削除することで、多要素認証の通知が届かないように設定ができます。</p>	
<p>9. 右上の歯車マークをタップします。</p>	
<p>10. [アカウントの削除]をタップします。</p>	
<p>11. [はい、このアプリのみです]をタップします。</p> <p>※Android 端末で設定した場合は、表示されません。</p>	

12. [キャンセル]をタップします。  
Android 端末の場合は「←」をタップします。



13. [無視]をタップします。
- 削除はこれにて完了です。
- [P5.「多要素認証とパスワードレス認証の設定について」](#)を参照して、新しいスマートフォンを操作して、新規登録を行ってください。

