

# 利用開始手続き マニュアル③

情報戦略課

2025/1

Ver4.1

# 利用開始手続き③

## 目次

はじめに	二要素認証の設定をはじめる前に	<a href="#">p.3</a>
利用開始 手続き③	初回セットアップキー（QRコード）の取得	<a href="#">p.4</a>
	認証アプリのインストール(ブラウザへの拡張機能の追加)	<a href="#">p.7</a>
	セットアップキーの登録	<a href="#">p.7</a>
	iOS（iPhone・iPad）	<a href="#">p.8</a>
	Android	<a href="#">p.11</a>
	Google Chrome（ブラウザ）	<a href="#">p.14</a>
	Microsoft Edge（ブラウザ）	<a href="#">p.18</a>
	二要素認証設定の確認/利用開始手続きの完了	<a href="#">p.21</a>
FAQ		<a href="#">p.26</a>
お問い合わせ		<a href="#">p.30</a>

## 利用開始手続き手順③

### <二要素認証の設定をはじめる前に>

二要素認証は、学外から学内システムやサービスを利用する際に使用します。

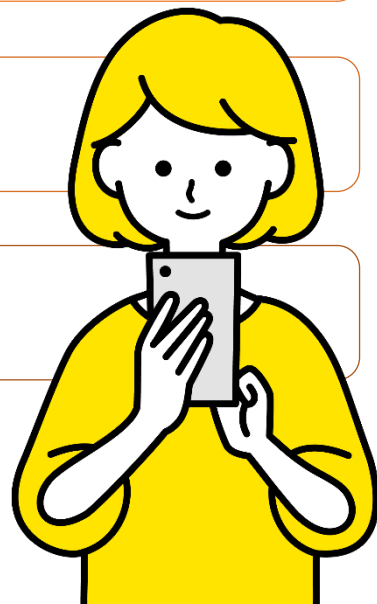
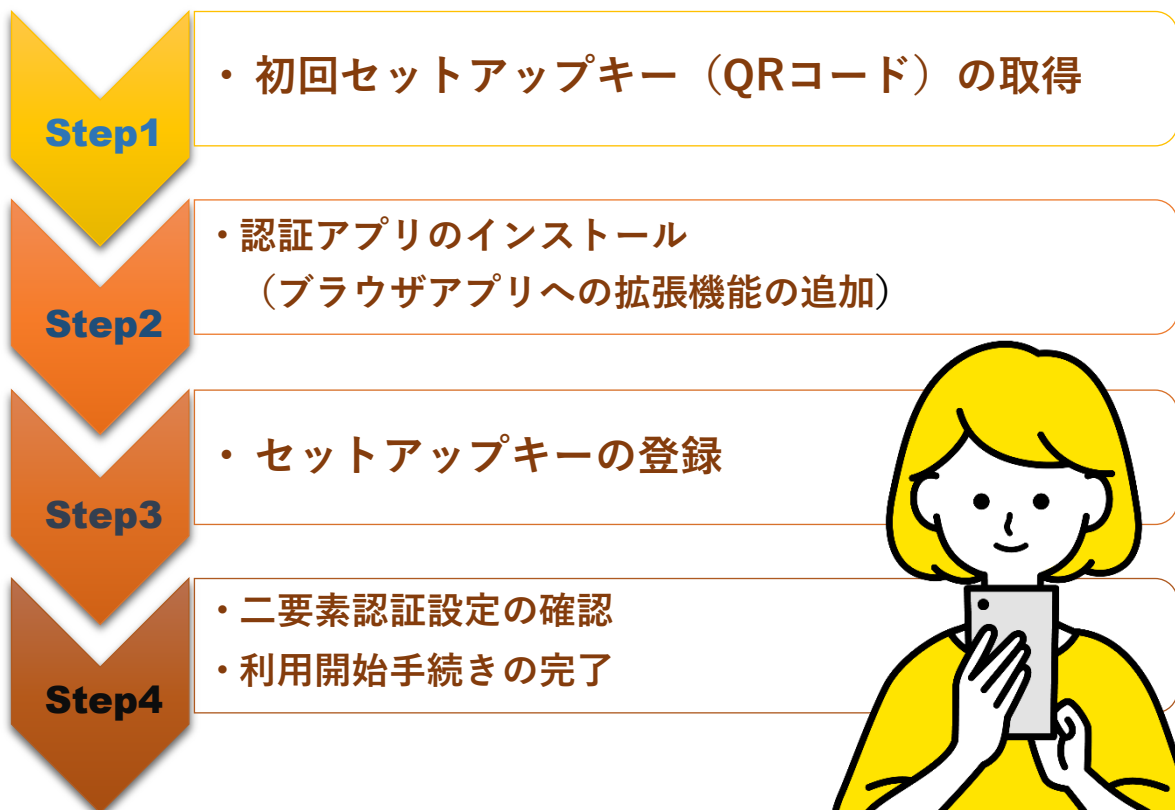
この手順を行うには、利用開始手続き手順②「本パスワード・パスワード再発行用メールアドレスの登録」まで完了している必要があります。

まだ行っていない場合は、以下 URL より利用開始手続き画面に戻り、先に手続きを完了させてください。

<https://start.cii.omu.ac.jp/>

中断した手続きを再開したい場合は、再開のポップアップで「はい」をクリックします。

二要素認証設定手順は以下の通りです。



## Step1

## ・ 初回セットアップキー（QRコード）の取得

※以下手順はWindows11を使っています。

1. 利用開始手続き②のマニュアルにて、「本パスワード・パスワード再発行用メールアドレスの登録」まで完了しました。  
「二要素認証設定」のページ下にある「二要素認証設定を始める」をクリックし、「1. 二要素認証のセットアップ」のページを表示します。



※利用開始手続きの画面を途中で閉じてしまい、左記の画面にアクセスが難しい場合は、直接下記URLにアクセスしてください。

<https://mfa.cii.omu.ac.jp/reset/request?setup=1>

二要素認証のセットアップは別タブ（別ウィンドウ）で表示されます。

利用開始手続きの画面は閉じずに、そのまま進めましょう。



大阪公立大学  
Osaka Metropolitan University

二要素認証管理システム

### 1. 二要素認証のセットアップ

OMUID/パスワードを入力してください。  
※ここに入力するのは仮パスワードではなく、あなたが先ほど設定した本パスワードです。

パスワード再設定アドレスに確認コードを送信します。

OMUID

パスワード

© 2024 大阪公立大学 情報基盤センター

3. 「OMUID」にあなたのOMUID、「パスワード」に利用開始手続き②で設定したあなたの本パスワードを入力して、「送信」をクリックします。

4. 「2. 再設定メールを送信」ページに遷移し、利用開始手続き②であなたが登録した再発行用メールアドレス宛に、システムからメールが送信されます。  
送信されたメールに記載されている確認コードを「確認コード（数字6桁）」に入力して「コードを確認する」をクリックします。

あなたの再発行用メールアドレスに送信された確認コード  
(例) 123456

再発行用メールアドレスに送信された確認コード(6桁)を入力後、「コードを確認する」をクリック



二要素認証管理システムからのメールは…

- ・ 件名 → [OMU二要素認証]二要素認証の再設定のご案内
- ・ 差出人 → 大阪公立大学 二要素認証管理システム

5. 「3. 最終確認」ページにて、「ワンタイムパスワードを設定する」をクリックします。



※「メニューに戻る」を押下すると、手順3「1. 二要素認証のセットアップ」へ戻ります。

6. すると、あなたのOMUIDとセットアップキー（QRコード）が表示されます。画面を閉じず、次の手順に進んでください。

※このセットアップキーおよびQRコードは、あなたがOMU認証システムへログインするための重要な情報です。他人に渡さないようにしてください。



初回セットアップキー（QRコード）の取得まで完了です。  
画面を閉じずに進みましょう！



Step2

- ・ 認証アプリのインストール  
(ブラウザアプリへの拡張機能の追加)


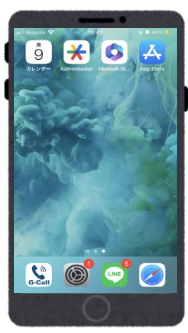

Step3

- ・ セットアップキーの登録


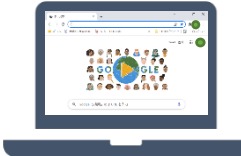

ここからはアプリをインストール（拡張機能を追加）する端末で操作を行います。利用頻度の高いご自身の端末に、以下のアプリをインストールしてください。

### Google Authenticator（Google認証システム）

#### ■ スマートフォンまたはタブレットにインストールする

	iOS (iPhone、iPad)	p.8～（アプリのインストール済の場合はp.9～） <a href="#">該当ページへ</a>	
	Android	p.11～（アプリをインストール済の場合はp.12～） <a href="#">該当ページへ</a>	

#### ■ ブラウザに拡張機能を追加する（PCの方向け）

	Google Chrome	p.14～（アプリをインストール済の場合はp.15～） <a href="#">該当ページへ</a>	
	Microsoft Edge	p.18～（アプリをインストール済の場合はp.19～） <a href="#">該当ページへ</a>	



## ■iOS(iPhone・iPad)

### <Google Authenticatorアプリのインストール>

※すでにアプリをインストールしている場合は、次のページの⑧より<セットアップキーの登録>を行ってください。

①	App Storeのアプリをクリックし起動します。	
②	App Storeの画面下部にあるメニューバーより、「検索」をクリックしてください。	
③	検索ボックスに「Google Authenticator」を入力し、表示された検索結果の「Google Authenticator」をクリックしてください。	
④	入手ボタンまたはダウンロードアイコンをクリックします。	
⑤	インストールボタンが表示された場合は、インストールボタンを押下して、パスワードの入力あるいは本人確認を行います。	
⑥	インストールが完了したら、「開く」をクリックします。Google Authenticatorが起動します。	
⑦	Google Authenticatorのアプリ起動時に、「Google認証システムでセキュリティをさらに強化」という画面が表示されたら、「開始」または「使ってみる」をクリックします。  また、Googleアカウントにログインするかどうかを聞かれた場合は、アカウントのログイン有無について選択してください。	<p>※Googleアカウントにログインしない場合は「アカウントなしでAuthenticatorを使用」をクリック</p> 



## <セットアップキーの登録>


Google Authenticatorアプリのトップページを表示します。  
「コードを追加」ボタン、  
または右下の「+」ボタンをクリックしてください。


⑧

※既にアプリを利用されている方は、  
画面右下の「+」ボタンをクリック  
します。



2通りのセットアップ方法が選択できます。  
「セットアップキーの入力」または「QR  
コードをスキャン」をクリックします。

セットアップキーを入力 

QR コードをスキャン 

QR推奨

### セットアップキーで追加

※今設定しているのと同じ端末でQRコード  
画面を表示させている場合  
⇒「セットアップキーを入力」を選択してく  
ださい。

アカウント情報の入力画面に遷移しますの  
で、「アカウント名」にあなたのOMUID、  
「鍵」に先ほどの手順で取得したセットア  
ップキーを入力し、追加ボタンをクリックし  
ます。

⑨



### QRコードで追加

※パソコンなど別の端末でQRコード画面を  
表示させている場合  
⇒「QRコードをスキャン」を選択してくだ  
さい。

端末のカメラへアクセスを求める表示が出  
た場合は「OK」をクリックしてください。

カメラ画面に切り替わったら、先ほどの手  
順で取得したQRコードをカメラで読み取り  
ます。



⑨の手順でアカウントが追加され、トップ画面に切り替わります。  
以下の2点を確認してください。

- ・ワンタイムパスワード（「3桁 3桁」の数字列）が表示されていること
- ・ワンタイムパスワードが30秒ごとに更新されること

⑩

※ワンタイムパスワードは、端末が内部で保持する世界標準時(GMT)を基準と連動しています。ワンタイムパスワードを利用する際は、世界標準時と同期をとり、正しい時刻に設定しましょう。



ワンタイムパスワードは30秒ごとに自動で変わります。

これでGoogle Authenticatorアプリへセットアップキーを登録して、ワンタイムパスワードを表示できるようになりました。  
STEP4に進み、学外からのログインを確認しましょう。

※Step 4 は p.21からです。

→Step 4 はこちら




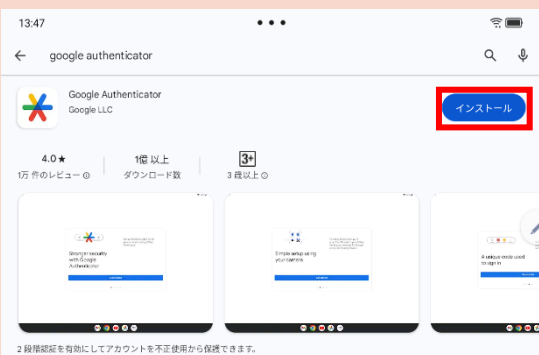
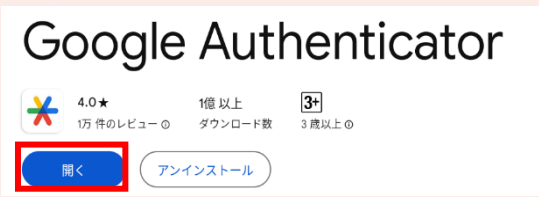



## ■ Android



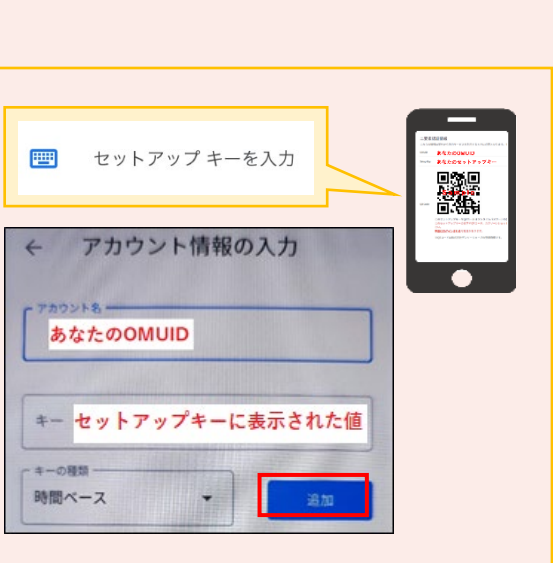
### < Google Authenticatorアプリのインストール >

※バージョンなどにより画面が異なる場合がありますので、ご自身の端末に表示された画面に読み替えて手続きを進めてください。

※すでにアプリをインストールしている場合は、次のページの手順⑥より<セットアップキーの登録>を行ってください。

①	Playストアのアプリをクリックし起動します。	 <p>Play ストア</p>
②	アプリメニュー上部の検索ボックス（アプリとゲームを検索）に「Google Authenticator」と入力し検索します。	
③	<p>検索結果から「Google Authenticator」を探し、アプリ名右横のインストールボタンをクリックします。</p> <p>※「アカウントの設定」が表示された場合は、「次へ」をクリックした後設定を行うか、または「スキップ」をクリックして設定のステップをスキップしてください。</p>	 <p>アカウント設定の完了</p> <p>アカウントを確認して、Google Play のアプリのインストールを続行してください</p> <p>次へ</p> <p>スキップ 次へ</p> <p>※スキップする場合は「スキップ」をクリックします。</p>
④	インストールボタンが「開く」に変わったらインストールが完了しています。「開く」をクリックしてアプリを起動します。	
⑤	<p>「Google Authenticatorでセキュリティをさらに強化」が表示されたら、「開始」または「使ってみる」をクリックします。</p> <p>また、Googleアカウントにログインするかどうかを聞かれた場合は、アカウントのログイン有無について選択してください。</p>	<p>※Googleアカウントにログインしない場合は「アカウントなしでAuthenticatorを使用」をクリックします。</p> 

## <セットアップキーの登録>

<p>⑥ Google Authenticatorアプリのトップページを表示します。 「コードを追加」ボタン、または右下の「+」ボタンをクリックしてください。</p> <p>※既にアプリを利用されている方は、画面右下の「+」ボタンをクリックします。</p>	
<p>⑦ 2通りのセットアップ方法が選択できます。「セットアップキーの入力」または「QRコードをスキャン」のどちらかをクリックします。</p> <p style="text-align: center;"><b>QRコードで追加</b></p> <p>※パソコンなど別の端末でQRコード画面を表示させている場合 ⇒「QRコードをスキャン」を選択してください。</p> <p>端末のカメラへアクセスを求める表示が出た場合は「許可」をクリックしてください。 カメラ画面に切り替わったら、先ほどの手順で取得したQRコードをカメラで読み取ります。</p>	
<p style="text-align: center;"><b>セットアップキーで追加</b></p> <p>※今設定しているのと同じ端末でQRコード画面を表示させている場合 ⇒「セットアップキーを入力」を選択してください。</p> <p>アカウント情報の入力画面に遷移しますので、「アカウント名」にあなたのOMUID、「キー」に先ほどの手順で取得したセットアップキーを入力し、追加ボタンをクリックします。</p>	

⑦の手順でアカウントが追加され、トップ画面に切り替わります。  
以下の2点を確認してください。

- ・ワンタイムパスワード（「3桁 3桁」の数字列）が表示されていること
- ・ワンタイムパスワードが30秒ごとに更新されること

⑧

※ワンタイムパスワードは、端末が内部で保持する世界標準時(GMT)を基準と連動しています。ワンタイムパスワードを利用する際は、世界標準時と同期をとり、正しい時刻に設定しましょう。



ワンタイムパスワードは30秒ごとに自動で変わります。

これでGoogle Authenticatorアプリへセットアップキーを登録して、ワンタイムパスワードを表示できるようになりました。  
STEP4に進み、学外からのログインを確認しましょう。

※Step4は p.21からです。



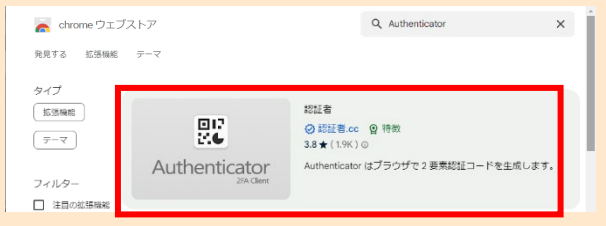
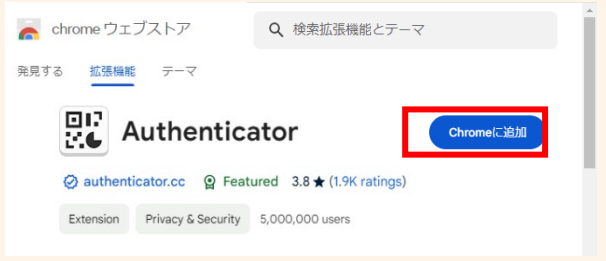

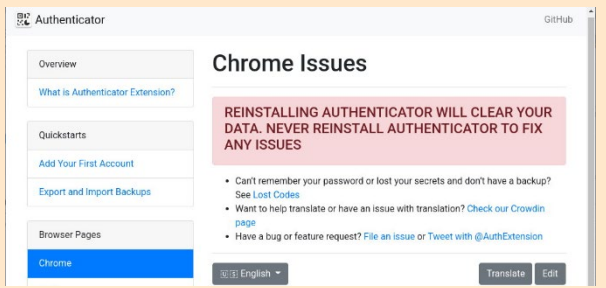
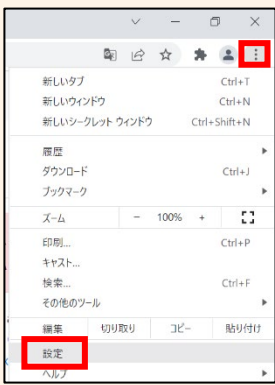
→Step 4 はこちら



## ■ Google Chrome（ブラウザ）




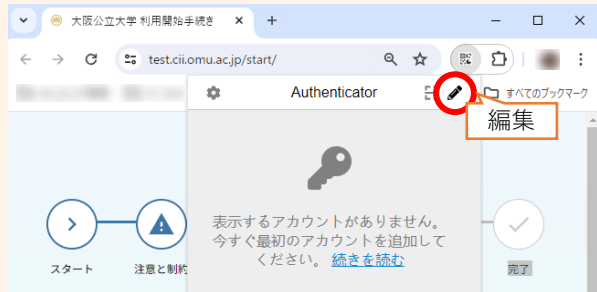

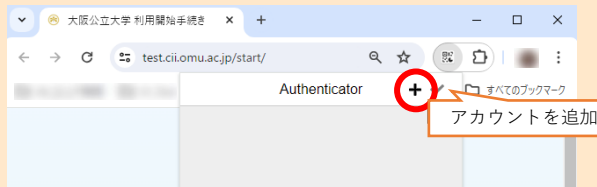
### < Authenticator 拡張機能の追加 >


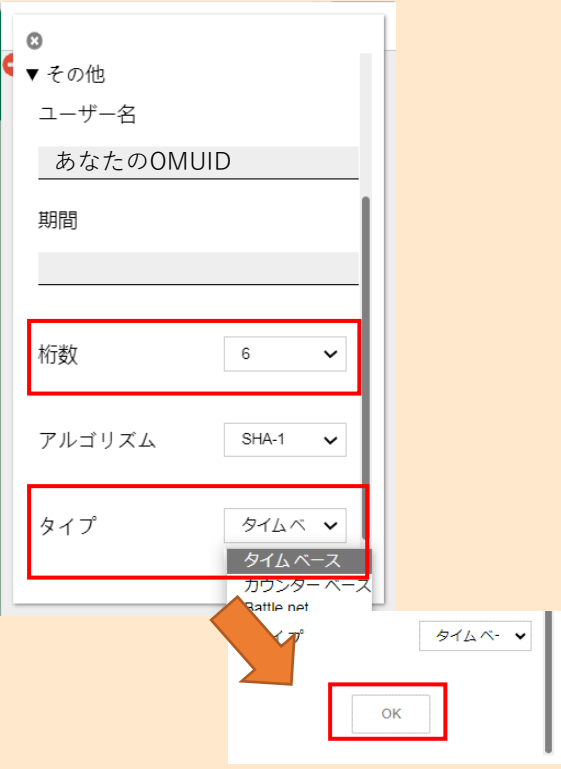
※すでに拡張機能をインストールしている場合は、次のページの手順⑨より<セットアップキーの登録>を行ってください。

<p>① Chromeブラウザを開き、 <a href="https://chrome.google.com/webstore/">https://chrome.google.com/webstore/</a> へアクセスします。</p>	 <p>左はChromeの拡張機能がダウンロードできるWebサイトです。</p>
<p>② 右上の検索ボックスへ「Authenticator」 を入力して検索します。</p>	
<p>③ 検索結果に「Authenticator」が表示され たら、選択します。</p>	
<p>④ 「Chromeに追加」をクリックします。 すると、「Authenticatorに追加します か?」というポップアップが出るので、 「拡張機能を追加」をクリックします。</p> <p>※すでに追加されている場合は、 「Chromeから削除」と表示されます。 →すでに追加されている場合は、手順⑨ へ進んでください。</p>	 
<p>⑤ 右のような画面が表示される場合があり ますが、<u>何もせず次の手順に進んでくだ さい。</u></p>	
<p>⑥ Chromeブラウザの右上「⋮」（Chrome メニュー）をクリックし、「設定」を選 択します。</p>	

⑦	左側メニューの「拡張機能」をクリックします。	
⑧	Chromeの拡張機能ページに遷移します。すべての拡張機能一覧に、「Authenticator」が追加されていれば、拡張機能の追加は完了です。	

## <セットアップキーの登録>

⑨	Chromeブラウザ右上のメニューの「  」をクリックして拡張機能のメニューを開き、Authenticatorをクリックします。	
⑩	Authenticatorが開きます。右上「  」編集メニューをクリックします。	
⑪	右上「  」アカウントの追加をクリックします。	

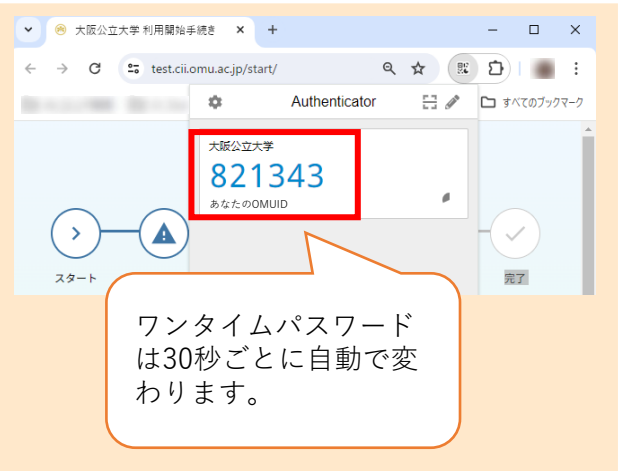
⑫	<p>右の選択が出来ますので、「手動入力」を選択します。</p>	
⑬	<p>入力画面表示されたら、以下の通り入力してください。</p> <p>○発行者：大阪公立大学 ○シークレット：&lt;初回セットアップキー（QRコード）の取得&gt;で表示されたセットアップキー</p> <p>入力できたら、「▶その他」をクリックします。</p>	
⑭	<p>その他の項目が表示されたら、以下が選択されているかを確認してください。</p> <p>○桁数：「6」 ○タイプ：「タイムベース」 ○ユーザー名：あなたのOMUID (※そのほかの項目は触れないでください。)</p> <p>すべて入力できたら、「OK」をクリックしてください。</p> <p>※「無効なアカウントのシークレット」というエラーが出る場合は、「※セットアップキーを入力して、エラーになる場合」をご参照ください。</p>	



ワンタイムパスワードが追加されました。

※ワンタイムパスワードは、端末が内部で保持する世界標準時(GMT)を基準と連動しています。ワンタイムパスワードを利用する際は、世界標準時と同期をとり、正しい時刻に設定しましょう。

⑮



これでGoogle Chromeへセットアップキーを登録して、ワンタイムパスワードを表示できるようになりました。STEP4に進み、学外からのログインを確認しましょう。

※Step4は p.21からです。


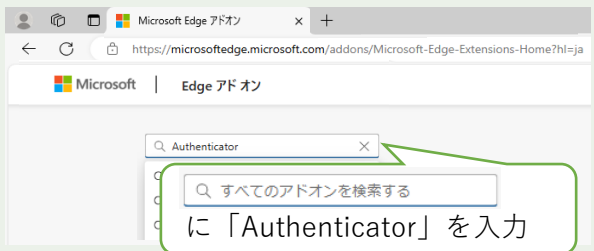

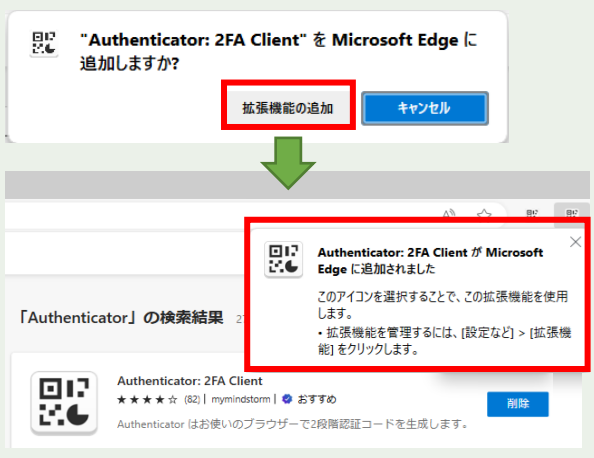
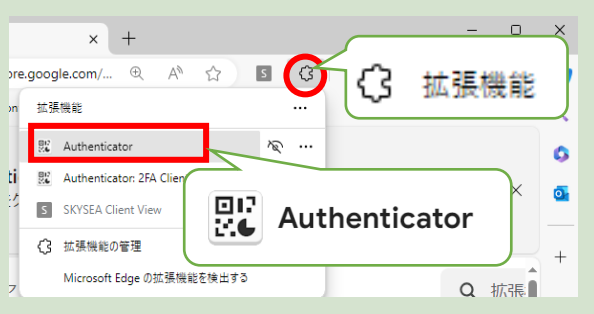
→Step 4 はこちら




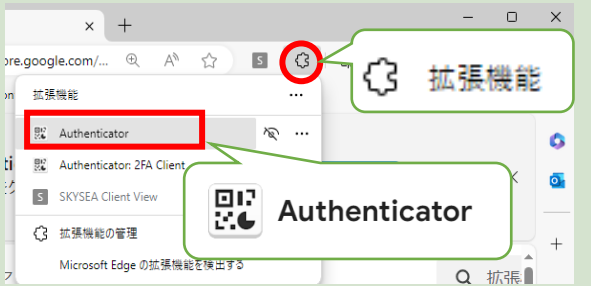

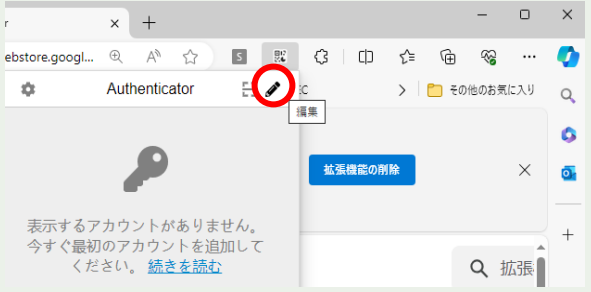

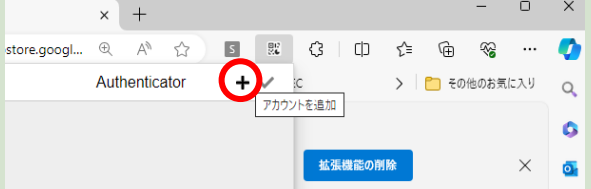

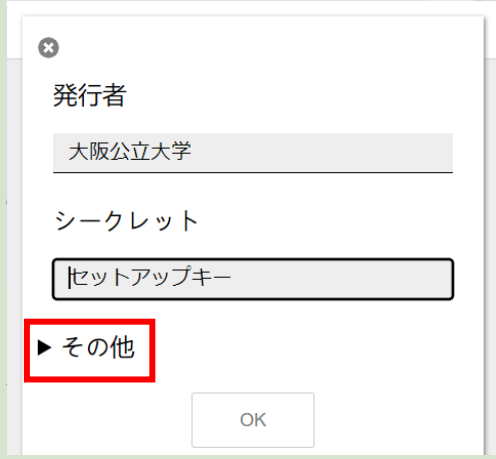
## ■ Microsoft Edge（ブラウザ）

### < Authenticator 拡張機能の追加 >

※すでに拡張機能をインストールしている場合は、次のページの手順⑥より<セットアップキーの登録>を行ってください。

<p>① Microsoft Edge ブラウザを開き、 <a href="https://microsoftedge.microsoft.com/addons/Microsoft-Edge-Extensions-Home">https://microsoftedge.microsoft.com/addons/Microsoft-Edge-Extensions-Home</a> へアクセスします。</p>	 <p>左のURLは、Edgeの拡張機能がダウンロードできるMicrosoftのWebサイトです。</p>
<p>② Edge アドオンの検索ボックスへ「Authenticator」を入力して検索します。</p>	 <p>に「Authenticator」を入力</p>
<p>③ 検索結果一覧に「Authenticator: 2FA Client」が表示されたら、「インストール」をクリックします。</p> <p>※すでに追加されている場合は、「インストール」の部分に「削除」と表示されます。 →すでに追加されている場合は、手順⑥へ進んでください。</p>	
<p>④ 「“Authenticator: 2FA Client”をMicrosoft Edgeに追加しますか？」というポップアップが出るので、「拡張機能の追加」をクリックします。</p> <p>しばらく待つと「Authenticator: 2FA ClientがMicrosoft Edgeに追加されました」というポップアップが出るのと同時に、「インストール」だったボタンが「削除」に変わります。</p>	
<p>⑤ Microsoft Edge ブラウザの右上「☰」をクリックし、拡張機能メニューを表示します。</p> <p>「Authenticator」が表示されていれば、拡張機能の追加は完了です。</p>	

## <セットアップキーの登録>

⑥	<p>Microsoft Edgeブラウザ右上のメニューの「」をクリックして拡張機能のメニューを開き、Authenticatorをクリックします。</p>	
⑦	<p>Authenticatorが開きます。右上「」編集メニューをクリックします。</p>	
⑧	<p>右上「」アカウントの追加をクリックします。</p>	
⑨	<p>右の選択が出ますので、「手動入力」を選択します。</p>	
⑩	<p>入力画面表示されたら、以下の通り入力してください。</p> <p>○発行者：大阪公立大学 ○シークレット：&lt;初回セットアップキー（QRコード）の取得&gt;で表示されたセットアップキー</p> <p>入力できたら、「▶その他」をクリックします。</p>	

その他の項目が表示されたら、以下が選択されているかを確認してください。

○桁数：「6」

○タイプ：「タイムベース」

○ユーザー名：あなたのOMUID

(※そのほかの項目は触れないでください。)

すべて入力できたら、「OK」をクリックしてください。

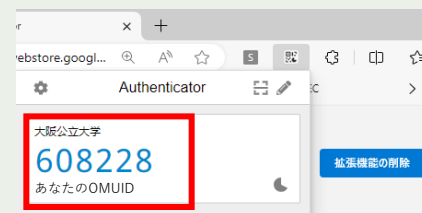
⑪

※「無効なアカウントのシークレット」というエラーが出る場合は、「※セットアップキーを入力して、エラーになる場合」をご参照ください。

ワンタイムパスワードが追加されました。

※ワンタイムパスワードは、端末が内部で保持する世界標準時(GMT)を基準と連動しています。ワンタイムパスワードを利用する際は、世界標準時と同期をとり、正しい時刻に設定しましょう。

⑫



これでMicrosoft Edgeへセットアップキーを登録して、ワンタイムパスワードを表示できるようになりました。STEP4に進み、学外からのログインを確認しましょう。

※Step4は次のページです。



## Step4

- ・二要素認証設定の確認
- ・利用開始手続きの完了

## <二要素認証設定の確認>

二要素認証の設定が正常に行われているか確認を行います。  
この手順では、学外から学内システムであるOMUポータルにアクセスできることを確認します。

※委託業者など学外の方はこの手順を踏むことができません。

Point!

※ 設定が完了したかどうかを確認するには、  
**学外(学内ネットワークに接続していない状態)から接続を確認する必要があります。**学内ネットワーク（OMUNET-1Xなど）に接続している場合は、自宅のWi-Fiやキャリア回線など学外のネットワークに接続し直してから以下を行ってください。

1. 学内ネットワーク（学内LANやWi-Fiなど）に接続していない状態にします。  
学内のWi-FiやLANに接続している場合は、接続を切断し、学外のネットワークに接続し直します。



OMUNET-1X  
eduroam (学内)  
OMUNET-HY  
Omunet-community  
etc...



キャリア回線  
学外のWi-Fi  
etc...



2. OMUポータル：<https://omu.info/st-logintest>  
へアクセスしてください。

3. OMU認証システムのログイン画面が表示されたら、OMUIDと自身で登録した本パスワード（OMU認証パスワード）を入力し、ログインしてください。

4. ワンタイムパスワード入力画面が表示されたら、Step3で表示されたワンタイムパスワード（6桁の数字）を入力して、ログインします。

ワンタイムパスワードを入力してください/Please input the one-time password

One-time password : \*\*\*\*\*

Login Reset

学外から認証するためにはワンタイムパスワードの入力が必要です。事前に設定したデバイスでワンタイムパスワードを確認して入力してください。  
ワンタイムパスワードの利用方法は、[こちらの手順書](#)を参照してください。

In order to authenticate from outside of the OMU campus, you need to input the one-time password. Please confirm the one-time password on your preconfigured device and input it.  
For more information on how to use the one-time passwords, please refer to [this manual](#).

※ワンタイムパスワード入力画面（黄色の画面）が表示されていない場合は、お使いの端末は学内ネットワークに接続していますので、学内ネットワークを切断し、学外のネットワークに接続し直してから再度お試しください。

※ワンタイムパスワードが無効ですと出る場合は、本マニュアル[FAQ・No.12](#)をご確認ください。

5. 以下の「二要素認証テスト用ページ」が表示されれば、二要素認証設定確認は完了です。



## <利用開始手続きの完了>

6. QRコードまたはセットアップキーの登録完了後、QRコード・セットアップキー表示画面を閉じて、利用開始手続き画面に戻ります。

※セットアップキー（QRコード）表示画面上での追加作業はありません。

※Google Authenticatorや拡張機能は、学外（学内ネットワークに接続していない状態）からOMUメールやOMUポータル、学生ポータル（UNIPA）などのサービスにアクセスする際に、使用します。

利用開始手続きが完了しても、**学外から学内ネットワークを利用する必要がある間は、アンインストール（拡張機能を削除）しないでください。**

7. 右下の「次へ」をクリックしてください。クリックすると、「注意」のポップアップが表示されます。二要素認証の設定が完了していない場合、学内ネットワークに接続していない状態でポータルサイトなどの各システムを利用できませんので、「いいえ」をクリックし前の手順へ戻って対応してください。完了されている場合は「はい」をクリックして、次の手順に進んでください。

利用開始手続き

スタート 注意と誓約 OMUID・PW確認 パスワード変更 二要素認証 完了

### 二要素認証設定

大阪公立大学のシステムを学外から使用するために必要な二要素認証を設定します。  
本手順では手元でスマートフォン（お持ちでない場合はPC）を手帳してから始めてください。

#### 二要素認証設定の3ステップ

1. OMU認証システムから二要素認証に必要なQRコードとセットアップキーを発行する。
2. スマートフォン・PCにアプリ「Google Authenticator」をインストールする。
3. Google Authenticatorに1.で発行したQRコードまたはセットアップキーを登録する。

利用開始手続き画面の「二要素認証設定を始める」ボタンを押してから始めてください。

スマートフォン（推奨）  PC

1. QRコードとセットアップキーの発行
2. アプリ「Google Authenticator」をインストール
3. QRコード、セットアップキー、6桁のワンタイムパスワード表示を登録

あなたのOMUID

あなたのOMUID

二要素認証の設定に上記の情報が必要となります。

[二要素認証設定を始める](#)

[戻る](#) [次へ](#) [マニュアル](#)

[トラブル・問い合わせ](#)

**注意**

二要素認証を完了していない場合、学外からほとんどのサービスを利用できません。設定は完了しましたか？

※今後学外から各サービスを利用する時は、ワンタイムパスワードによる二要素認証が必要となります。

[いいえ](#) [はい](#)



8. 以下の画面が表示されたら、利用開始手続きは完了です。



**Goal!**

**お疲れ様でした！  
利用開始手続きは以上で完了です！**

異なる端末にワンタイムパスワードを設定する時に必要になる“セットアップキー（QRコード）の確認方法”や、スマートフォンの機種変更などによってセットアップキーを再発行する際は、下記システムで手続き可能です。


二要素認証管理システム（<https://omu.info/2fa-sys>）をぜひご活用ください。



## &lt;FAQ&gt;



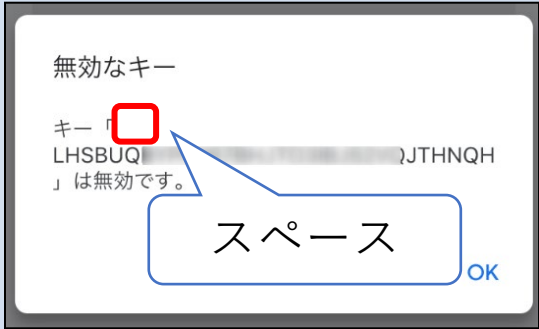
## 初回セットアップキーの取得に関するFAQ

No	問題、トラブル	回答
1	利用開始手続き画面を途中で終了してしまい、二要素認証の画面が出ません。	<a href="https://start.cii.omu.ac.jp/">https://start.cii.omu.ac.jp/</a> へアクセスしてください。 「以前に中断した手順から再開しますか？」というポップアップ画面が表示されたら、「はい」をクリックして中断した手順から再開してください。
2	初回セットアップキーの取得をしようとしていて、「1. 二要素認証のセットアップ」のページにいます。 OMUIDと仮パスワードを入力してもログインできなくて困っています。	二要素認証の設定で利用するパスワードは、 <u>ご自身で設定された本パスワード</u> となります。 仮パスワードではログインできません。
3	「2. 再設定メールを送信」ページで「コードを確認する」ボタンをクリックしてもメールが届きません。	画面中央部の送信先を確認してください。  <p>再設定メールが送信されたメールアドレスが表示されています。 表示されているメールの受信ボックスを開いてください。 受信ボックスにメールが届かない場合は、迷惑メールフォルダも確認してください。 メールが届いていない場合は、設定画面下部の「メールを再送する」をクリックして再度メールを送信してください。</p>
4	「2. 再設定メールを送信」ページで確認コードを入力しても「確認コードが違います」と出ます。	再設定メールが送信されてから、30分以内に確認コードを入力する必要があります。 30分経過してしまった場合や確認コードが違うと言われる場合は、初回セットアップキーの取得を最初からやり直してください。

## 認証アプリのインストールに関するFAQ

	問題、トラブル	回答
5	「3. 最終確認」ページで「ワンタイムパスワードを設定する」をクリックする前にページを閉じてしまいました。	初回セットアップキーの取得の手順を最初からやり直してください。
6	Googleストアに接続できません。Google Authenticatorがダウンロードできません。	Microsoftの認証アプリ（Microsoft Authenticator）でも登録可能です。やむを得ずGoogle Authenticatorがダウンロードできない場合は、上記も試してください。

## セットアップキーの登録に関するFAQ

	問題、トラブル	回答
7	認証アプリ（拡張機能）にセットアップキーを入力すると、無効なキーまたは無効なアカウントと表示されます。	<p>セットアップキーについて、入力文字列が正しいことを再度確認してください。また、セットアップキーをコピーした際に、文字列の先頭にスペースがついてしまう場合があります。先頭にスペースが入っていないかを確認し、スペースがある場合は削除してから、やり直してください。</p> 
8	Google Authenticatorで無効になったアカウントを削除したい	<p>「Google Authenticator（Google 認証システム）登録ワンタイムパスワード削除方法」のマニュアルをご確認ください。          OMUポータルトップページ&gt; マニュアル（サイドメニュー）          または、OMUポータルトップページ&gt; ポータル全体検索（サイドメニュー）から、上記マニュアルを検索してください。</p>

## 二要素認証設定の確認/利用開始手続きの完了に関するFAQ

	問題、トラブル	回答
9	学外に持ち出せない端末に二要素認証を設定してしまったため確認ができません。	学外に持ち出せない端末、特に共用端末には二要素認証の設定を行わないでください。設定してしまった場合は設定の削除を行ってください。
10	委託業者として学内で働いていますが、二要素認証設定の確認がうまくできません。	学外関係者は本マニュアルで説明している手順を行うことができません。委託業者など学外の方は、受入れの教職員に相談してください。
11	OMUIDとパスワードを入力後、ワンタイムパスワードを入力する黄色い画面が出てきません。	学内ネットワークに接続している状態だとワンタイムパスワードを入力する画面は出てきません。学内ネットワークを切断して再トライしてください。
12	ワンタイムパスワードを入力するとエラーになって先に進めません。	<p>入力しているワンタイムパスワードが本マニュアルで設定した大阪公立大学のものが再度確かめてください。</p> <p>また、ワンタイムパスワードは表示されている30秒間の間に入力する必要があります。表示中に入力を完了させてください。失敗した場合は新しく表示されたワンタイムパスワードで試してください。</p> <p>セットアップキーを複数回再発行した場合は、再度に取得したセットアップキーに紐づくワンタイムパスワードのみが有効になります。端末が正しくGMT（世界標準時）と同期されていない場合もエラーとなりますので、端末の時刻設定を「自動」にしてください。</p> <p>上記を確認してもエラーとなる場合は、p.4の「二要素認証をはじめる」ボタンの押下からやり直してください。</p> <p>利用開始手続きを完了した後にワンタイムパスワードがエラーとなって進めない場合は、二要素認証管理システムを利用してセットアップキーの再発行を行います。二要素認証管理システムマニュアルは以下のURLから参照してください。</p> <p><a href="https://omu.info/2fa-manu">https://omu.info/2fa-manu</a></p>
13	利用開始手続きを完了する前に手続き画面を閉じてしまいました。	本FAQの項番1を確認してください。

## 二要素認証/その他に関するFAQ

	問題、トラブル	回答
14	スマートフォンに加えてタブレットにもワンタイムパスワードを表示させたいです。どうすればいいですか。	<p>二要素認証管理システムを利用してセットアップキーを表示させたい端末の認証アプリ (Authenticator) に設定します。セットアップキーの表示方法は、二要素認証管理システムマニュアル&gt;「1. 現在のセットアップキーを表示する」をご確認ください。二要素認証管理システムマニュアルは以下のURLから参照してください。</p> <p><a href="https://omu.info/2fa-manu">https://omu.info/2fa-manu</a></p> <p>各端末にセットアップキーを登録する方補については、本マニュアルp.7の「セットアップキーの登録」を参照してください。</p>
15	ブラウザに設定したワンタイムパスワードは利用できますが、スマートフォンに設定したワンタイムパスワードが利用できません。	<p>セットアップキーが無効になっている可能性があります。</p> <p>利用できない端末のセットアップキー (QRコード) を設定し直してください。</p> <p>※ワンタイムパスワードのリセットは不要です。</p> <p>ご自身のセットアップキーの表示方法は二要素認証管理システムマニュアル&gt;「1.現在のセットアップキーを表示する」を参照してください。</p> <p><a href="https://omu.info/2fa-manu">https://omu.info/2fa-manu</a></p>
16	二要素認証設定画面で、「二要素認証設定をはじめ」のボタンを表示することが難しかったため、 <a href="https://mfa.cii.omu.ac.jp/reset/request?setup=1">https://mfa.cii.omu.ac.jp/reset/request?setup=1</a> のURLへ直接アクセスして、二要素認証の設定は完了しました。ですが、その後、利用開始手続きに戻れないため、利用開始手続きの完了の画面まで遷移できません。	<p>二要素認証管理システムにて、二要素認証の設定を終えた後、テストページにアクセスできるのであれば、利用開始手続きは完了と考えていただいて大丈夫です。</p>

## <お問い合わせ>

マニュアル通りに進めたがエラーが出た・ログインができないなど、利用開始手続きが進められない時は、以下のページより同様のトラブル・事例がないか確認してください。こちらのページでは、利用開始手続きで起こりやすいトラブルや、それらに関連したよくある質問を掲載しています。

また、該当する事例がない、よくある質問を確認しても解決しない場合は、ITヘルプデスクにお問い合わせすることも可能です。お問い合わせも同ページから可能です。

### ■ 利用開始手続きで困ったときは

<https://www.omu.ac.jp/cii/start-trouble/>

利用開始手続き画面の左下には、常に「トラブル・お問い合わせ」ボタンが表示されています。こちらのボタンからも上記URLにアクセスすることができます。

### ・利用開始手続き画面

利用開始手続き

スタート 注意と誓約 OMUID・PW確認 パスワード変更 二要素認証 完了

**スタート**  
大阪公立大学へようこそ

これから、大阪公立大学情報ネットワークシステムおよび各情報システム（OMUポータル、UNIPAなど）を利用するための初期手続きを行います。手続きに必要な時間は約20分です。

**手続きを始める前に**

本手続きの前に以下をご準備ください。

- スマートフォンまたはPC
- 大学発行ではない、個人のメールアドレス

※個人アドレスはパスワードを再発行する際に必要です。  
利用開始手続きは、必ずマニュアルを見ながら進めてください。

**利用開始手続きのマニュアルについて**

画面下部の「マニュアル」ボタンからマニュアルの一覧を参照してください。各ステップがどの手順に対応しているか確認し、該当のマニュアルを参照してください。最初は「マニュアル①」に従って進んでください。

戻る 次へ

トラブル・問い合わせ マニュアル

## 更新履歴

No	変更年月日	内容
1	Ver2.2	PW変更済かどうか確認する手順の追加、マニュアルを3分割、在学生用・新入生用統一
2	Ver2.3	Authenticatorのアイコン変更、アプリ更新による手順（Gmailアカウント同期設定部分）を追加、二要素認証を再設定する利用者向けの案内追加
3	2024/2	利用開始手続きマニュアル②よりOMUID・仮PW確認方法を移動・追加 学籍番号の表現を入学時期関係ないように修正
4	2024/4	「Internet Explorer」を削除。「Safari」へ置き換え
5	Ver3.0	目次をより大きくわかりやすい仕様に変更 各OSのリンク設定を修正
6	2024/8	Javascriptのフレームワーク変更に伴う利用開始手続き画面キャプチャの変更 Chrome等ブラウザや各OS画面バージョンアップによる画面の撮り直し 二要素認証管理システムリリースに伴う手順の変更
7	2024/12	二要素認証管理システムの初回セットアップ画面の直URLを追記 併せて、FAQ16を追記
8	2025/1	使用端末をWindows10からWindows11に変更