

多要素認証 教職員向け

(MFA : MULTI-FACTOR AUTHENTICATION)

2026年1月版



IC-Mail を含む Microsoft365 のサービスを学外から利用する場合は、2026年2月10日以降に多要素認証が必須になります。（事務職員は先行して2025年11月に多要素認証を適用済みです）

多要素認証（MFA）とは？

多要素認証（MFA）とは、ログイン時に2つ以上の認証要素を組み合わせて本人確認を行う仕組みです。

たとえばこんな組み合わせです：

要素の種類	例
知識情報（知っているもの）	パスワード、PIN
所持情報（持っているもの）	スマートフォン、タブレット
生体情報（本人そのもの）	指紋、顔認証

例：

「パスワード」+「スマホに送られた認証コード」

「パスワード」+「顔認証」

なぜ多要素認証（MFA）が必要なのか？

従来は「パスワードだけ」でログインできていましたが、次のような問題があります。

- ・パスワードの使い回しで漏洩しやすい
- ・フィッシング詐欺やウイルスで盗まれる
- ・知らない間に他人がログインしてしまうリスク

MFA を使うことで、仮にパスワードが漏れても、不正ログインを防止できます。

大学・企業・行政機関など、あらゆる組織が多要素認証（MFA）を標準化しています。

多要素認証（MFA）導入のメリット

- ・セキュリティの大幅向上
- ・個人情報や業務データの保護
- ・情報漏えい事故の抑止
- ・サイバー攻撃への対策

認証方法の例（本学で使用予定の方式）

以下のいずれかの方法で認証を行います：

- ・Microsoft Authenticatorなどのアプリで通知を承認【推奨1】
- ・スマートフォンに届くコードを入力(SMS)【推奨2】
- ・電話による自動音声確認【推奨2】
- ・その他（セキュリティキー等）

原則【推奨1】・【推奨2】どちらも登録をお願いします。

いずれかの方法に不具合が発生した場合に認証ができなくなってしまうため、2つ以上の方法を登録するようにしてください。

SMSまたは電話のみ登録の場合は、電話番号が変更になってしまうと認証がおこなえません。

スマホアプリのみ登録の場合は、機種変更をした際に旧機種がないと機種変更後の初回認証がおこなえません。

FAQ

Q. 何度も認証するのは面倒では？

A. 学内からのアクセス（有線 LAN、無線 LAN）の場合は多要素認証が不要です。学外からのアクセスの場合は、セキュリティ向上のため多要素認証が必須となります。ご協力をお願いします。

Q. スマートフォンを持っていない場合は？

A. スマホ認証アプリ以外の代替手段（電話、SMS、PC アプリ等）を設定できます。

Q. スマートフォンの機種変更をしたらどうする？

A. P.18～22 の「多要素認証 設定の変更方法」を参考に設定を変更してください。

Q. 多要素認証を行えなくなったらどうする？

A. 学内からはパスワードのみでサインイン可能です。まずは学内からブラウザで IC-Mail 等にパスワード認証でアクセスしてください。
P.18～22 の「多要素認証 設定の変更方法」を参考に認証要素の追加・削除をしてください。

Q. パソコンのみで認証したい。

A. スマートフォンで多要素認証を設定できない方は PC アプリ、またはブラウザ拡張機能を利用することで認証が可能です。
Windows : P.23～29、macOS : P.30～35、ブラウザ拡張機能 : P.36～42。

問い合わせ

多要素認証に関するお問い合わせは大学7号館4階情報センターまでお願いします。

設定方法のマニュアルは次ページ以降を参照ください。

このマニュアルに掲載している画面イメージはサンプルです。実際の環境と異なる部分があります。また予告なしに変更となることがあります。

内容	ページ
学内から多要素認証を設定する	3～14
2026年2月10日以降に学外から多要素認証を設定する	15～17
スマートフォンを機種変更したとき、または多要素認証でログインできなくなったとき	18～22
[スマートフォンで多要素認証を設定できない場合] パソコンのみで多要素認証を行う	23～29、30～35、36～42

多要素認証 初期設定マニュアル （モバイルアプリを用いた認証）

- ① 大学公式サイト (<https://www.icc.ac.jp/>) を開き、画面最下部の「教職員用」をクリックします。

茨城キリスト教学園 大学について 採用情報 ご支援をお考えの方 EN アクセス 対象種別 検索

茨城キリスト教大学 キャリア・就職 留学・国際理解 地域・社会貢献 キャンパスライフ

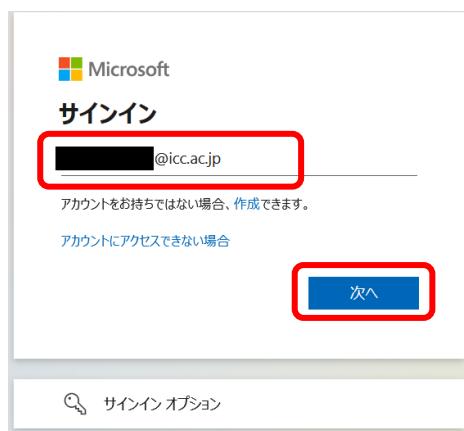
教職員用 採用情報 学校法人茨城キリスト教学園 茨城キリスト教学園中学校・高等学校
茨城キリスト教大学附属認定こども園みらい園・せいじ園 お問い合わせ

- ② 「IC-MAIL」のバナーリンクをクリックします。

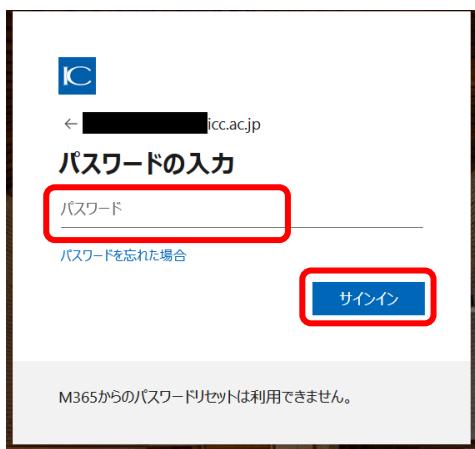


または URL (<https://outlook.office365.com/>) にアクセスします。

- ③ Microsoft のログイン画面が表示されるので、「メールアドレス」を入力して「次へ」ボタンをクリックします。



④ 「パスワード」を入力してサインインボタンをクリックします。



⑤ サインイン後、画面右上にあるアカウントマークをクリックして「アカウントを表示」をクリックします。



⑥ 「セキュリティ情報」をクリックします。

The screenshot shows the 'My Account' settings page. On the left, a sidebar lists options like '概要', 'セキュリティ情報' (Security Information), 'デバイス', 'Change password', '組織', '設定およびプライバシー', and '自分のサインイン'. The 'セキュリティ情報' link is highlighted with a red box. The main content area shows a summary card with a large circular profile picture and a 'セキュリティ情報' section with a link to '更新情報 >'. To the right, there are sections for 'Change password' and a link to 'パスワードの変更 >'.

⑦ 「サインイン方法の追加」をクリックします。

The screenshot shows the 'Security Information' page in the Microsoft Azure portal. The left sidebar includes links for Overview, Security Information (which is selected and highlighted in blue), Devices, and Password Change. The main content area is titled 'Security Information' and contains a note about using it for account sign-in or password reset. A red box highlights the '+ Add sign-in method' button. Below it are sections for 'Password' (last updated 5 years ago) and a warning about device loss.

⑧ ここでは「Microsoft Authenticator（モバイルアプリ）」をクリックします。電話 or SMS 認証を追加する場合は P.10 の「多要素認証事前設定 初期設定マニュアル（SMS・電話を用いた認証）」へ。

The screenshot shows the 'Add sign-in method' dialog box. It lists several options: 'Microsoft Authenticator' (selected and highlighted in red), 'Security key', 'Hardware token', 'Phone', 'Alternate phone', and 'Corporate phone'. The 'Microsoft Authenticator' option is described as using a one-time code from the app.

⑨ アプリのインストールの指示が表示されます。そのまま次へボタンをクリックします。

The screenshot shows the 'Microsoft Authenticator' setup dialog. It displays instructions to download the app to the phone and install it. It also provides an alternative for using a different authentication app. The 'Next' button at the bottom right is highlighted with a red box.

⑩ アカウントのセットアップ指示が表示されます。そのまま次へボタンをクリックします。



⑪ QRコードが表示されます。PCにこの画面が表示されたまま、スマートフォンで次の作業を行います。



【スマートフォンでの作業】

⑫ 認証を行うスマートフォンに「Microsoft Authenticator」アプリ（無料）をインストールしてください。

iPhone の場合「App ストア」、Android の場合「Google Play」の検索画面で「Microsoft Authenticator」を検索してインストールします。似たような名称のアプリがありますので間違えないように注意してください。

<iPhoneの場合>



<Androidの場合>



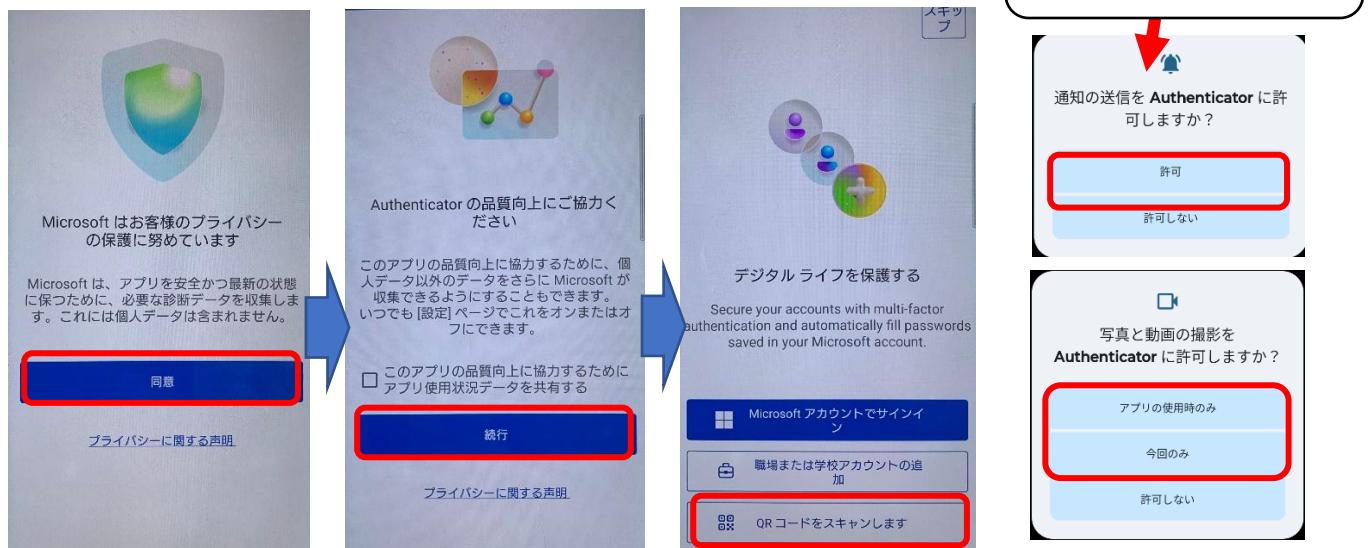
⑬ Microsoft Authenticator アプリを起動。

以下、画像のようにタップを進め、「QR コードをスキャンします」をタップします。

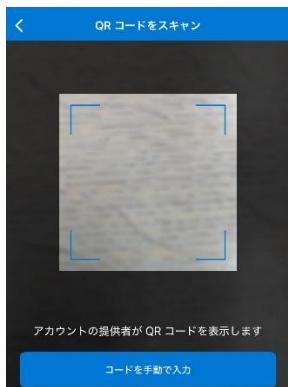
<iPhone の場合>

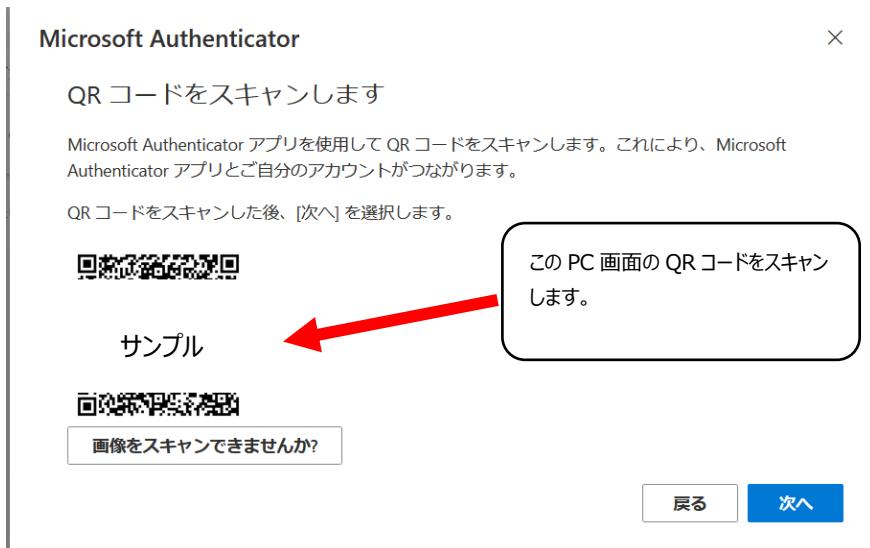


<Android の場合>



⑭ QR コードのスキャン画面で、PC 画面（P.6）に表示された QR コードをスキャンします。





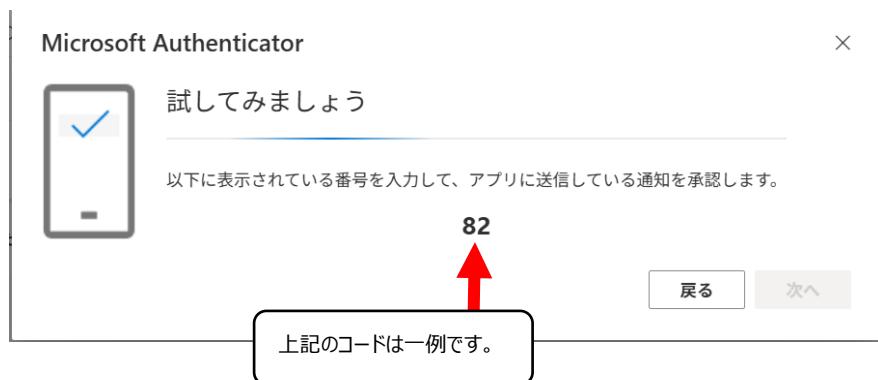
⑯ スキャンに成功するとスマホの Microsoft Authenticator アプリにアカウントが追加されていることが確認できます。



⑰ PC 画面に戻り、**[次へ]** ボタンをクリックします。

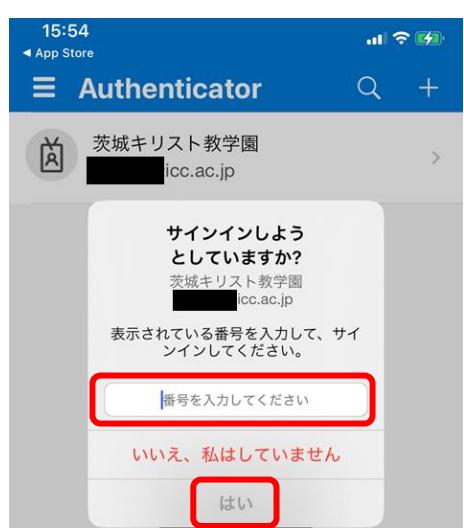


⑯ 以下の画面を表示したまま、スマートフォンを操作します。



【スマートフォンでの作業】

⑰ スマートフォンの画面に「サインインしようとしていますか？」という表示がされます。
PC 画面に表示されている 2 行の数字を入力し、「はい」をタップします。



【パソコンでの作業】

⑲ 「通知が承認されました」と表示されるので、次へボタンをクリックします。



② セキュリティ情報の画面に「Microsoft Authenticator」が追加されました。

The screenshot shows the 'Security Information' page in the Microsoft 365 portal. On the left, there's a sidebar with options like 'Overview', 'Security Information' (which is selected and highlighted in blue), 'Devices', 'Password Change', and 'Organization'. The main content area is titled 'Security Information' and contains a section for 'Sign-in methods'. It lists 'Password (1)' with a 'Change' link. Below it is a red-bordered box containing 'Microsoft Authenticator' with the subtext 'Multi-factor authentication (MFA) to push'. There's also a 'Delete' link and a note at the bottom: 'If your device is lost, please sign out from all devices'.

以上で、Microsoft Authenticator アプリを用いた認証を設定する方法は完了です。

以降は学外ネットワークから Microsoft365 にサインインする際に、自身の設定した方法で認証を行っていただく形となります。

多要素認証 初期設定マニュアル （SMS・電話を用いた認証）

① 多要素認証事前設定 初期設定マニュアル （モバイルアプリを用いた認証） P.3～5 の手順①～⑦までを参考に、「マイアカウント」の「セキュリティ情報」を開き、「サインイン方法の追加」をクリックします。

This screenshot shows the 'Security Information' page with the 'Security Information' option selected in the sidebar. In the main content area, there's a 'Add sign-in method' button which is highlighted with a red box. Other visible sections include 'Overview', 'Devices', 'Password Change', and a note at the bottom: 'If your device is lost, please sign out from all devices'.

② 「電話」をクリックします。

This screenshot shows the 'Add sign-in method' dialog box. It lists several options: 'Microsoft Authenticator' (selected), 'Security key' (disabled), 'Microsoft Authenticator' (disabled), 'Hardware token' (disabled), 'Phone' (selected and highlighted with a red box), 'Secondary phone', and 'Corporate phone'. The 'Phone' option is described as 'Call to sign in using a phone call or text message'.

③ 電話ではSMSでコードを受け取る方法と、電話で着信を受け取る方法があります。

【SMSでコードを受け取る方法】

SMS-(1) Country Codeは「日本」を選択して、Phone numberは電話番号をハイフンなしで入力し、確認方法は「コードを受け取る」を選択して、次へボタンをクリックします。

電話

電話で呼び出しに応答するか、電話でコードを受け取ることにより、本人確認ができます。

どの電話番号を使用しますか?

Country code: 日本 (+81)

Phone number: 09011112222

確認方法を選択します

コードを受け取る

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-(2) 携帯・スマートフォンのSMSに6桁のコードが届くので、PCの画面に6桁のコードを入力し、次へボタンをクリックします。

電話

+81 0 [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。

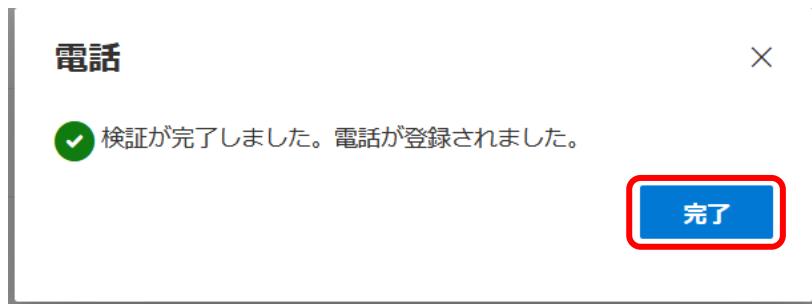
046416

コードの再送信

上記のコードは一例です。

戻る 次へ

SMS-③ 認証に成功した画面があるので、完了ボタンをクリックします。



SMS-④ セキュリティ情報に電話が追加されました。

A screenshot of a web-based security information page. The title is "セキュリティ情報" (Security Information). It says, "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。" (This is the method used for signing in to your account or resetting your password). Below this, it says "最も適したサインイン方法を使用しています。" (The most suitable sign-in method is being used) and "最も適したもののが利用できない場合のサインイン方法: 電話 - テキスト +81 90 [REDACTED] [変更](#)" (If the most suitable method cannot be used, sign-in method: Phone - Text +81 90 [REDACTED] [Change](#)). A table lists the methods: "電話" (Phone) with number "+81 90 [REDACTED]" and buttons "変更" (Change) and "削除" (Delete), and "パスワード" (Password) with a "変更" (Change) button. The entire row for the phone method is highlighted with a red box. At the bottom, there is a link "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](#)" (If you lose your device, please sign out from all devices).

以上で、SMS を用いた認証を設定する方法は完了です。

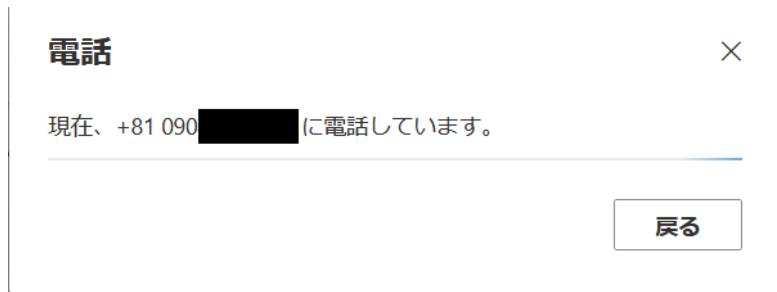
以降は学外ネットワークから Microsoft365 にサインインする際に、自身の設定した方法で認証を行っていただく形となります。

【電話で着信を受け取る方法】

電話-(1) Country Code は「日本」を選択して、Phone number は電話番号をハイフンなしで入力し、確認方法は「電話する」を選択して、次へボタンをクリックします。

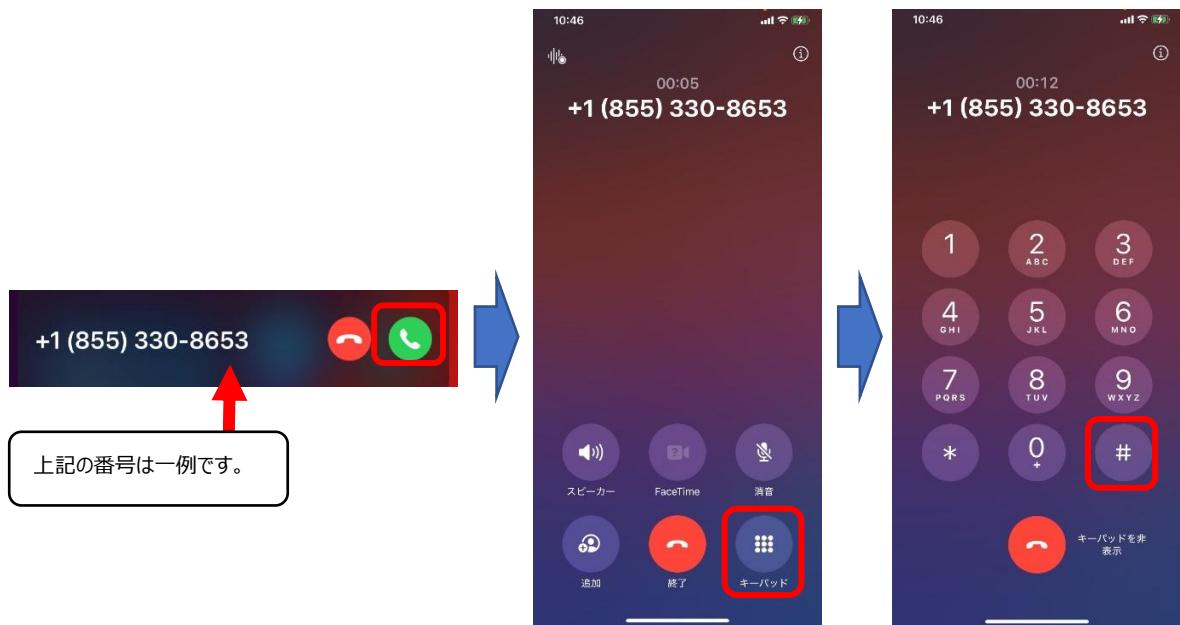


電話-(2) 先ほど指定した電話番号に Microsoft から着信があります。

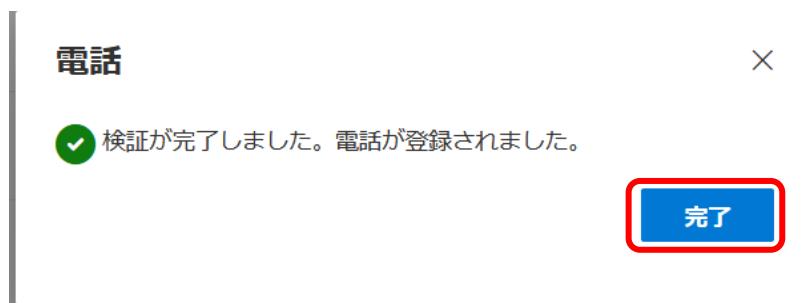


電話-(3)

電話を受けると日本語または英語で「#」を押すように指示がありますので、キーパッドを開き「#」をタップします。



電話-(4) 認証に成功した画面があるので、完了ボタンをクリックします。



電話-(5) セキュリティ情報に電話が追加されました。

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。

最も適したサインイン方法を使用しています。
最も適したものを利用できない場合のサインイン方法: 電話 - テキスト +81 90 [変更]

+ サインイン方法の追加

電話	+81 90 [REDACTED]	[変更]	[削除]
パスワード	①	最終更新日時: 5年前	[変更]

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](#)

以上で、電話を用いた認証を設定する方法は完了です。

以降は学外ネットワークから Microsoft365 にサインインする際に、自身の設定した方法で認証を行っていただく形となります。

多要素認証 必須化後設定 初期設定マニュアル

多要素認証が**必須化後**は、学外から Microsoft365 のサービスにサインインする途中で多要素認証の設定が求められます。

- ① 大学公式サイト (<https://www.icc.ac.jp/>) を開き、画面最下部のリンク「教職員用」をクリックし、



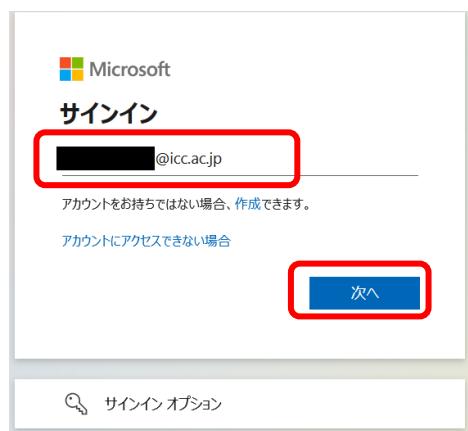
茨城キリスト教大学 大学について 採用情報 ご支援をお考えの方 EN アクセス 対象種別 検索
IC 茨城キリスト教大学 大学について 学部・大学院 キャリア・就職 留学・国際理解 地域・社会貢献 キャンパスライフ
< > 2020
...
教職員用 採用情報 学校法人茨城キリスト教学園 茨城キリスト教学園中学校・高等学校
茨城キリスト教大学附属認定こども園みらい園・せいじ園 お問い合わせ

- ② 「IC-MAIL」のバナーリンクをクリックします。

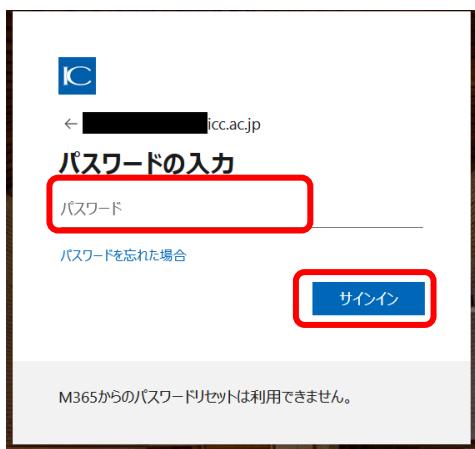


または URL (<https://outlook.office365.com/>) にアクセスします。

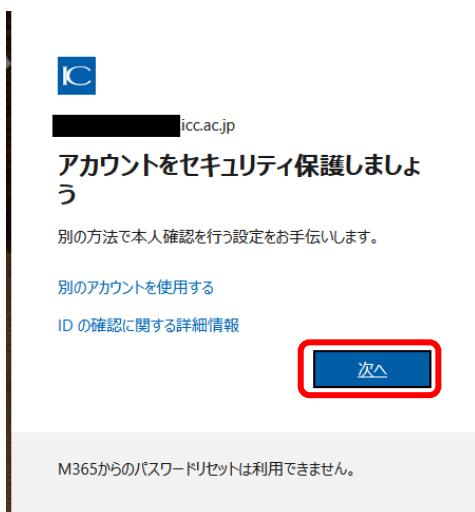
- ③ Microsoft のログイン画面が表示されるので、「メールアドレス」を入力して次へボタンをクリックします。



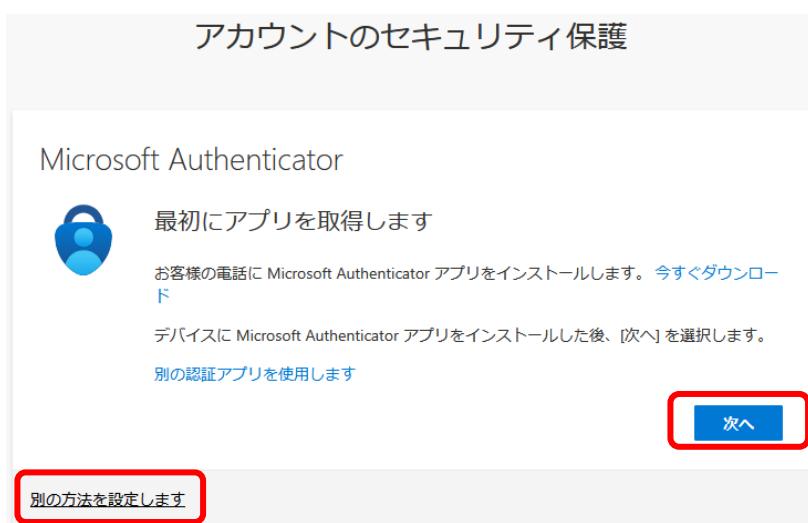
④ 「パスワード」を入力して**サインイン**ボタンをクリックします。



⑤ 「アカウントをセキュリティ保護しましょう」という画面が表示されます。**次へ**ボタンをクリックします。



⑥ Microsoft Authenticator アプリの認証を追加する場合は、**次へ**ボタンをクリックします。
SMS・電話による認証を追加する場合は、「別の方法を設定します」をクリックします。



【Microsoft Authenticator アプリの認証方法】

P.5～10 の手順⑦～⑩を参照して、手順通り設定してください。

設定に成功すると以下のような成功画面が表示されますので、完了をクリックしてください。



これで Microsoft Authenticator アプリの設定は完了です。 サインイン要求の指示に従って認証してください。

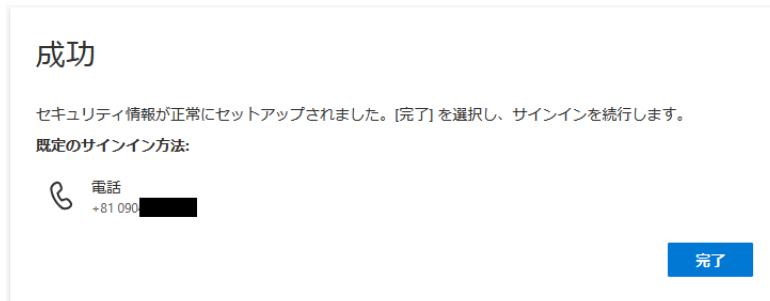
【SMS・電話の認証方法】

P.16 手順⑥の「別の方法を設定します」をクリックすると、以下の画面が表示されるので「電話」をクリックします。



P.11～14 の手順③を参照して、手順通り設定してください。

設定に成功すると以下のような成功画面が表示されますので、完了をクリックしてください。



これで SMS・電話の設定は完了です。 サインイン要求の指示に従って認証してください。

多要素認証 設定の変更方法

スマートフォンの機種変更をした場合や電話番号を変更した場合に、多要素認証の設定変更が必要になります。その際に多要素認証の設定が1つだけの場合にアクセスできなくなることがあるため、事前に2つ以上の多要素認証の設定を推奨しています。

もし多要素認証ができなくなってしまったら、まずは学内からMicrosoft365にパスワード認証でアクセスして認証要素の追加削除をしてください。学内からはパスワードのみでサインイン可能です。

多要素認証は5デバイスまで登録することができます。端末や認証方法を追加・変更・削除する場合は以下の方法を参照してください。

- ① 大学公式サイト (<https://www.icc.ac.jp/>) を開き、画面最下部のリンク「教職員用」をクリックし、

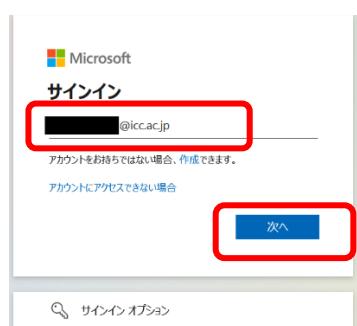


- ② 「IC-MAIL」のバナーリンクをクリックします。

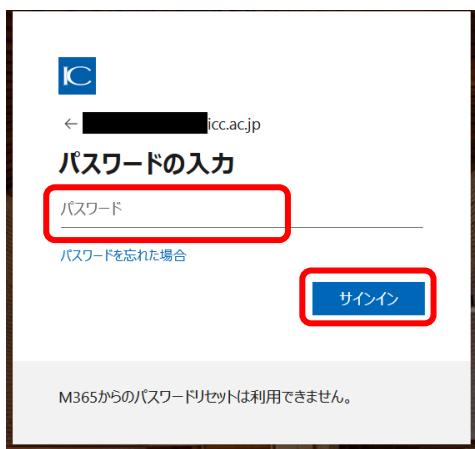


または URL (<https://outlook.office365.com/>) にアクセスします。

- ③ Microsoftのログイン画面が表示されるので、「メールアドレス」を入力して次へボタンをクリックします。



④ 「パスワード」を入力して**サインイン**ボタンをクリックします。



学外のネットワークからアクセスした場合は、多要素認証が求められます。設定した認証方法でサインイン要求を承認してください。

⑤ サインイン後、画面右上にある**アカウントマーク**をクリックして「アカウントを表示」をクリックします。



⑥ 「セキュリティ情報」をクリックします。

マイ アカウント

- 概要
- セキュリティ情報**
- デバイス
- Change password
- 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

認証方法とセキュリティ情報を最新の状態にしてください。

更新情報 >

Change password

パスワードを強力にするか、他人が知っている場合は変更します。

パスワードの変更 >

⑦ 認証方法の追加、変更、削除は以下の方法を参照してください。

【認証方法を追加する方法】

サインイン方法の追加をクリックします。

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。

最も適したサインイン方法を使用しています。

最も適したもののが利用できない場合のサインイン方法: Microsoft Authenticator - 通知 [変更](#)

サインイン方法	最終更新日時	操作
電話	+81 0 [REDACTED]	変更 削除
パスワード ①	最終更新日時: 7年前	変更
Microsoft Authenticator 多要素認証 (MFA) をプッシュする	iPhone [REDACTED]	削除
パスキー (ペイントされたデバイス) Microsoft Authenticator	Authenticator - iOS iOS デバイス	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](#)

追加したい方法を選択してください。

自分のサインイン

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方法です。

最も適したサインイン方法を使用しています。
最も適したもののが利用できない場合のサインイン方法: Microsoft Authenticator - 通知 [変更](#)

サインイン方法の追加

- Microsoft Authenticator のパスキー
顔、指紋、PIN でサインインします
- セキュリティ キー
USB、Bluetooth、または NFC デバイスを使用してサインインします
- Microsoft Authenticator
サインイン要求を承認するか、ワンタイムコードを使用します
- ハードウェア トークン
ハードウェア トークンからのコードを使用してサインインする
- 電話
コードでサインインするための通話またはテキスト メッセージを受け取ります
- 代替の電話
コードでサインインするための電話呼び出しを受ける
- 会社電話
コードでサインインするための電話呼び出しを受ける

・Microsoft Authenticator アプリの設定方法は **P.5~9 の手順⑨~⑯**を参照してください。

・SMS・電話の設定方法は **P.11~14 の手順③**を参照して、手順通り設定してください。

【電話番号を変更する方法】

「変更」をクリックします。

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。

最も適したサインイン方法を使用しています。

最も適したもののが利用できない場合のサインイン方法: Microsoft Authenticator - 通知 [変更](#)

+ サインイン方法の追加			
	電話	+81 0 [REDACTED]	変更
	パスワード ⓘ	最終更新日時: 7年前	変更
	Microsoft Authenticator 多要素認証 (MFA) をブッシュする	iPhone [REDACTED]	削除
	バスキー (バインドされたデバイス) Microsoft Authenticator	Authenticator - iOS iOS デバイス	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](#)

新しい番号を入力して設定を進めてください。

電話

×

電話で呼び出しに応答するか、電話でコードを受け取ることにより、本人確認ができます。

どの電話番号を使用しますか?

Country code	Phone number
<input type="button" value="日本 (+81)"/> ▼	<input type="text" value="090 [REDACTED]"/>

確認方法を選択します

- コードを受け取る
 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・電話の設定方法は **P.11~14 の手順③**を参照して、手順通り設定してください。

【認証方法を削除する方法】

既に設定されている方法の右側の「削除」をクリックして認証方法を削除できます。

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。

最も適したサインイン方法を使用しています。
最も適したもののが利用できない場合のサインイン方法: Microsoft Authenticator - 通知 [変更](#)

+ サインイン方法の追加			
	電話	+81 0 [REDACTED]	変更
	パスワード ①	最終更新日時: 7年前	変更
	Microsoft Authenticator 多要素認証 (MFA) をブッシュする	iPhone [REDACTED]	削除
	パスキー (バインドされたデバイス) Microsoft Authenticator	Authenticator - iOS iOS デバイス	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](#)

多要素認証 PC アプリ（WINAUTH）の設定の方法（WINDOWS PC）

WinAuth というパソコン用のアプリで、多要素認証を行うことができます。（Windows OS の PC のみ）

- ① 以下のアドレスにアクセスし、アプリ（WinAuth）をダウンロードします。

<https://winauth.github.io/winauth/download.html>



This is the latest stable version of WinAuth.

WinAuth Version 3.5

This is the latest stable version of WinAuth.

[WinAuth 3.5.1 \(2016-06-07\)](#)

MD5: 6993C999D1412C0D28CCCC8A0F9CB90C3. WinAuth.exe MD5: 3C8B42FF6BC4822FC6D874F6F21230DD

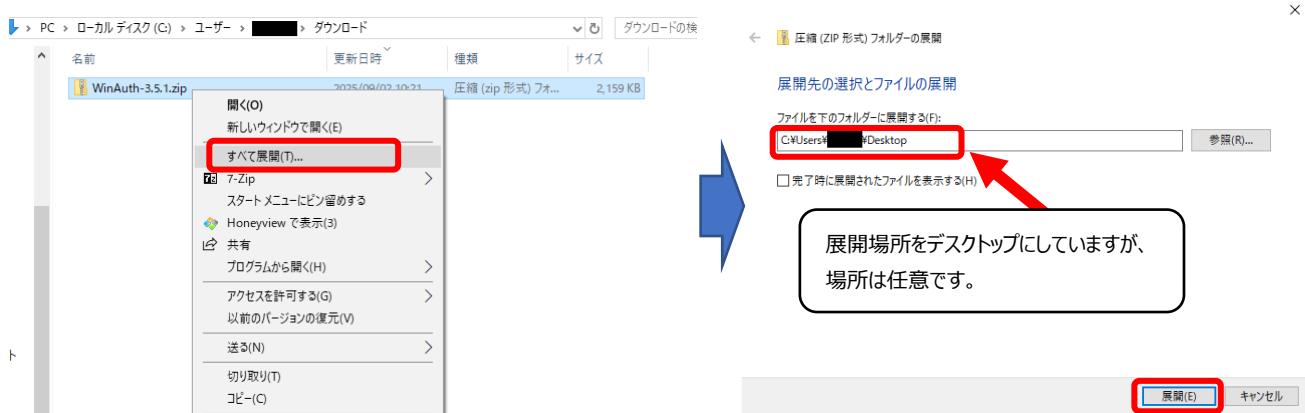
(Windows 7 / 8.x / 10 requires Microsoft .NET Framework 4.5)

For Windows 7 using pre-installed Microsoft .NET Framework 3.5

[WinAuth 3.5.1 \(.NET 3.5\) \(2016-06-07\)](#)

MD5: A4C1719B0457A90E5EA177BF87E8B09B. WinAuth.exe MD5: AFC2EE24D4DF9E4EC28D115A3E14CAC3

- ② ダウンロードした ZIP ファイルを解凍し、任意の場所に展開します。



③ アプリ（WinAuth）の展開が完了したら

P.18～19 の手順①～⑥を参照して、Microsoft365 にサインイン後にセキュリティ情報まで進んでください。

④ サインイン方法の追加をクリックします。



⑤ 「Microsoft Authenticator」をクリックします。



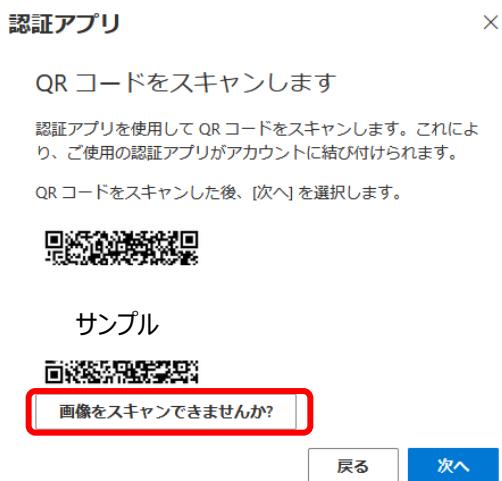
⑥ 「別の認証アプリを使用します」をクリックします。



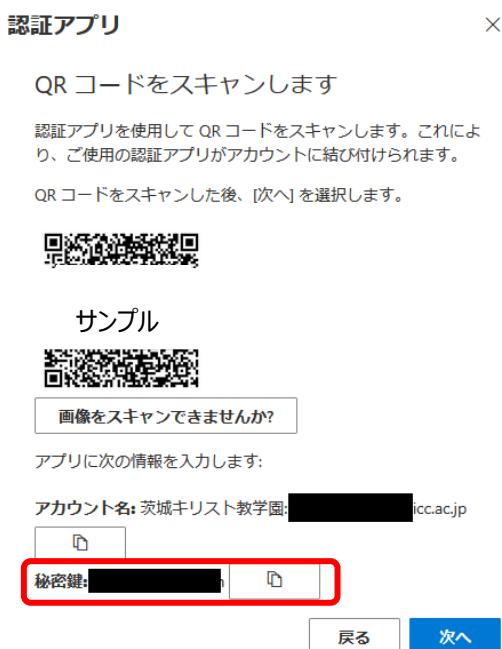
⑦ 「アカウントのセットアップ」が表示されたら、[次へ]をクリックします。



⑧ QR コードの画面では、[画像をスキャンできませんか?]をクリックします。



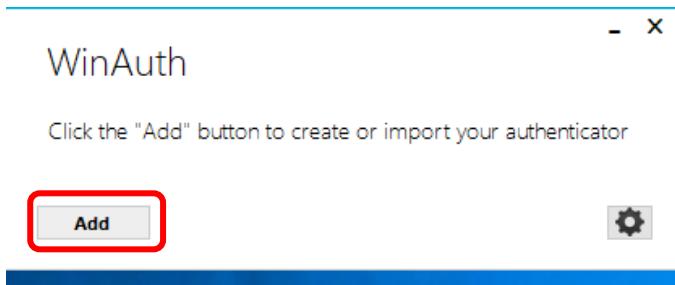
⑨ 秘密鍵が表示されます。この秘密鍵はパスワードと同様に他人に知られないようにご注意ください。



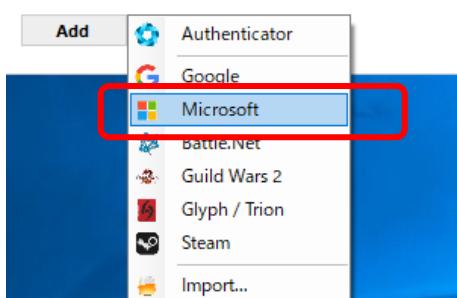
⑩ さきほどダウンロードして任意の場所に展開したアプリ（WinAuth）を起動します。



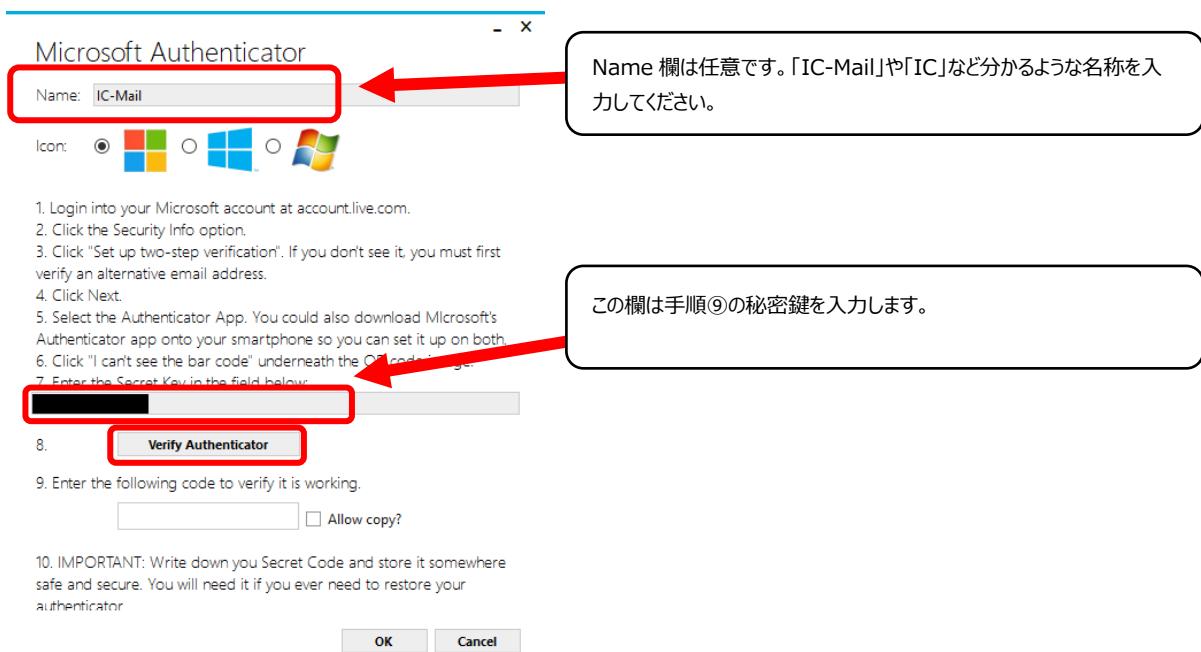
⑪ [Add]ボタンをクリックします。



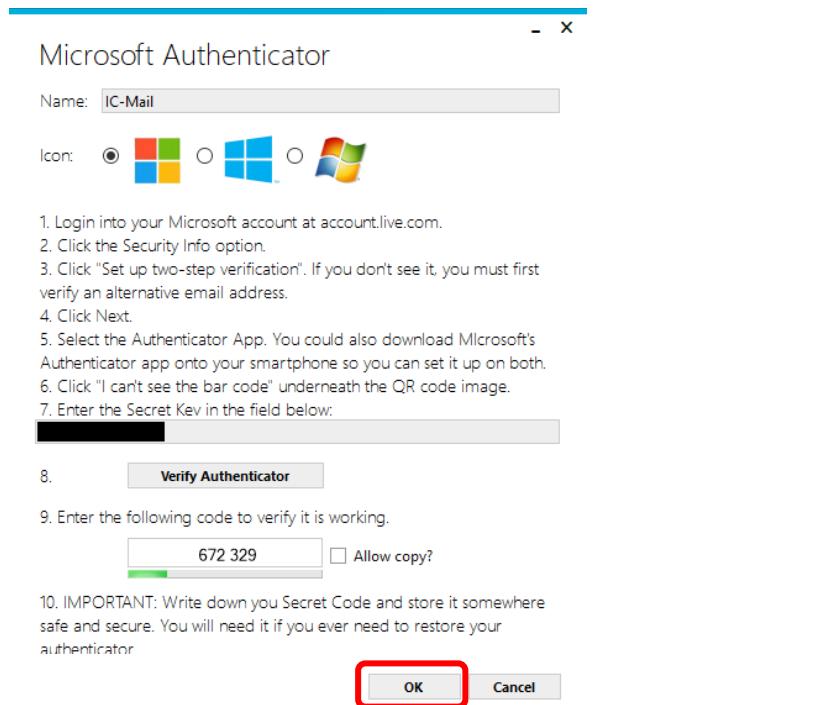
⑫ Microsoftを選択します。



⑬ 設定情報を入力します。「Name」欄と「秘密鍵」欄を入力したら、Verify Authenticatorをクリックします。



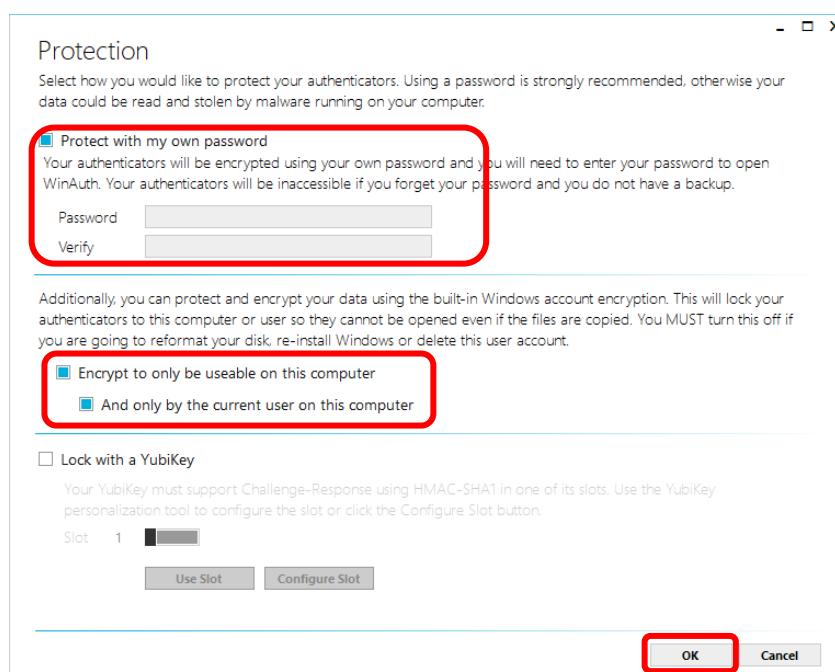
- ⑭ **Verify Authenticator**をクリックした後に、6桁の数字が表示され、緑色のバーが右に少しづつ進みます。緑色のバーが端に到達すると、新しい6桁の数字が表示されます。**OK**をクリックします。



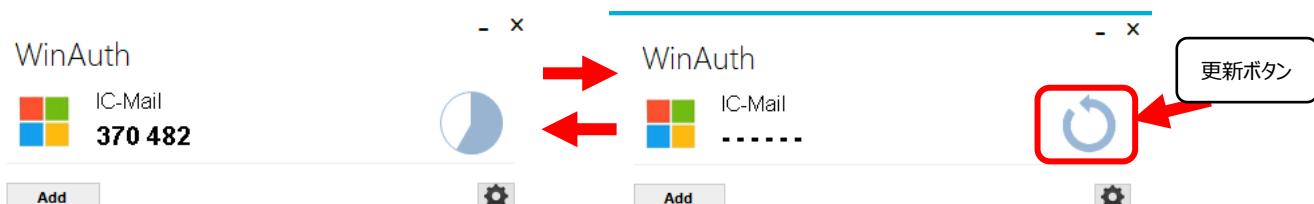
- ⑮ Protection画面について、「Protect with my own password」にチェックを入れるとWinAuthを起動する際にパスワードが必要になります。自分しか該当のPCを使用しない場合は、チェックは不要です。他人と共にしている場合は、チェックを入れてPassword欄に任意のパスワードを設定してください。Verify欄はPassword欄と同じものを入力してください。

「Encrypt to only be useable on this computer」と「Add only by the current user on this computer」はチェックを入れて使用してください。

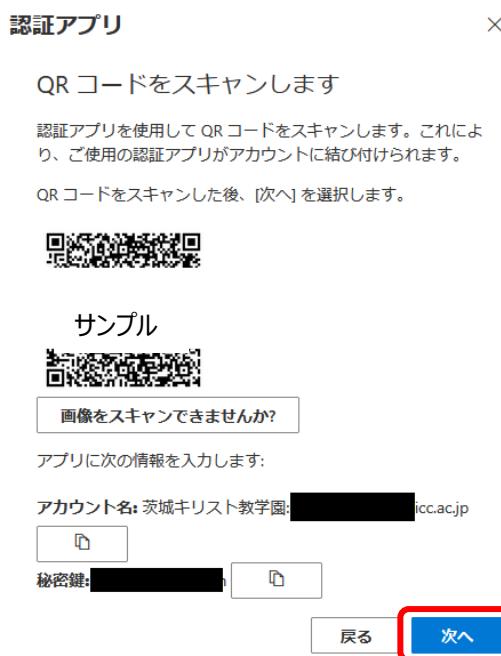
OKボタンをクリックします。



- ⑯ 6 行のコードが表示される画面が表示されます。30 秒経過すると右下図のようにコードが表示されなくなります。
更新ボタンをクリックすると新しいコードが表示されます。



- ⑰ ブラウザに戻り、次へボタンをクリックします。



- ⑱ コードの入力画面になります。アプリ（WinAuth）に表示されている 6 行のコードを入力し、次へボタンをクリックします。



⑯ セキュリティ情報に認証アプリが追加されました。

The screenshot shows the 'Security Information' page for a user account. The left sidebar includes 'Overview', 'Security Information' (selected), 'Devices', 'Password Change', and 'Organizations'. The main content area has a title 'Security Information' and a subtitle 'This is how you can use your account for sign-in or password reset.' Below this is a table with a single row:

+ Sign-in method addition	
<input type="checkbox"/> Password (1)	最終更新日時: 5年前
<input checked="" type="checkbox"/> 認証アプリ 時間ベースのワンタイム パスワード (TOTP)	変更 削除

A red box highlights the TOTP row, and a red arrow points to the 'Delete' button.

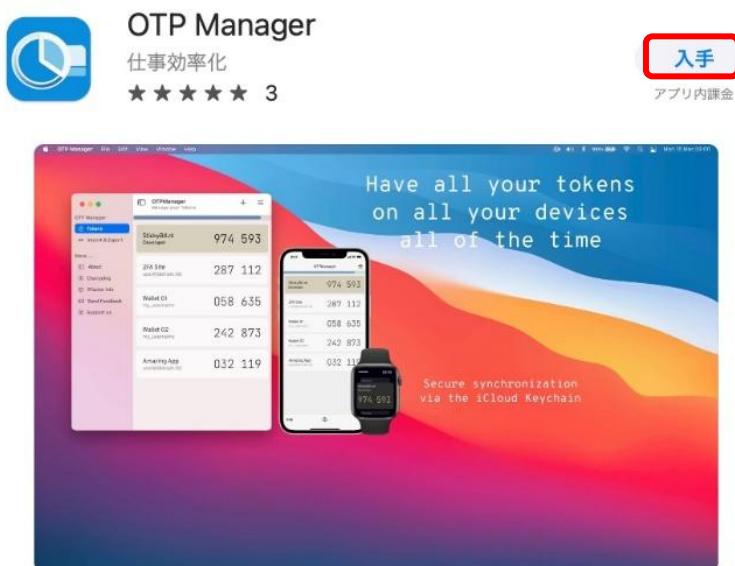
これでアプリ（WinAuth）の設定は完了です。 サインイン要求の指示に従って、WinAuth を起動しコードを入力して認証してください。

多要素認証 PC アプリ（OTP MANAGER）の設定の方法（MAC PC）

OTP Manager というパソコン用のアプリで、多要素認証を行うことができます。（macOS Big Sur(11.0)以降の PC 対応）

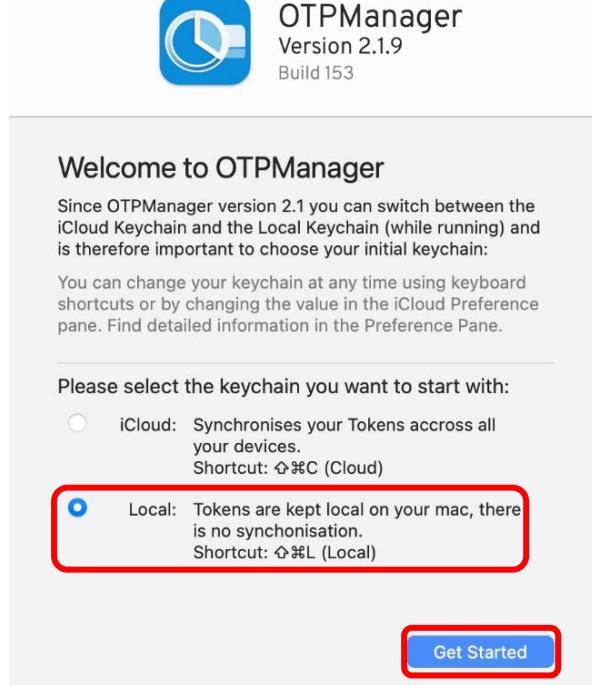
OTP Manager は Windows 用のアプリもありますが、ここでは Mac 用のアプリについて説明します。

- ① AppStore にアクセスし、アプリ（OTP Manager）をインストールします。



- ② OTP Manager を起動すると下図のような画面が表示されます。

Local: を選択して、Get Started ボタンをクリックしてください。



③ アプリ（OTP Manager）のインストールと起動が完了したら

P.18～19 の手順①～⑥を参照して、Microsoft365 にサインイン後にセキュリティ情報まで進んでください。

④ サインイン方法の追加をクリックします。

The screenshot shows the Microsoft 365 Security Information page. On the left, there's a sidebar with options: 概要 (Overview), セキュリティ情報 (Security information) (which is selected and highlighted with a red box), デバイス (Devices), and パスワードの変更 (Password change). The main content area is titled 'セキュリティ情報' (Security information) and contains the text: '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。' (This is the method used for signing in to your account or resetting your password). Below this, there's a button labeled '+ サインイン方法の追加' (Add sign-in method) which is also highlighted with a red box. At the bottom, it says 'デバイスを紛失した場合' (If you lose your device) and 'すべてサインアウトしてください' (Please sign out). There are also links for '最終更新日時' (Last updated) and '変更' (Change).

⑤ 「Microsoft Authenticator」をクリックします。

The screenshot shows the 'Add sign-in method' dialog. It lists several options: Microsoft Authenticator のパスキー (Passkey), セキュリティキー (Security key), Microsoft Authenticator (which is highlighted with a red box), ハードウェアトークン (Hardware token), 代替の電話 (Alternate phone), and 会社電話 (Company phone). At the bottom, it says '各方法についての詳細情報を確認し、選択に役立ててください' (Please review the detailed information for each method and use it to make your selection).

⑥ 「別の認証アプリを設定する」をクリックします。

Microsoft Authenticator のインストール



モバイルデバイスにアプリをインストールしてから、ここに戻って続行します。

GET IT ON
Google Play Download on the
App Store

別の認証アプリを設定する

戻る

次へ

⑦ 「アプリでアカウントをセットアップする」が表示されたら、次へをクリックします。

アプリでアカウントをセットアップする



まず、アカウントを追加します。

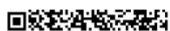
戻る 次へ

⑧ QR コードの画面では、Can't scan the QR code?をクリックします。

QR コードをスキャンします ×



サンプル



Authenticator アプリを使用して QR コードをスキャンしてください。これにより、アプリがアカウントに接続されます。

次に、戻って [次へ] を選択します。

Can't scan the QR code?

戻る 次へ

⑨ 秘密鍵が表示されます。**この秘密鍵はパスワードと同様に他人に知られないようにご注意ください。**

Enter the following into
Authenticator ×

Authenticator で QR コードスキャナーを開き、[手動でコードを入力] を選択します。

アカウント名: 名前のコピー ▾
茨城キリスト教学園: [REDACTED]@icc.ac.jp

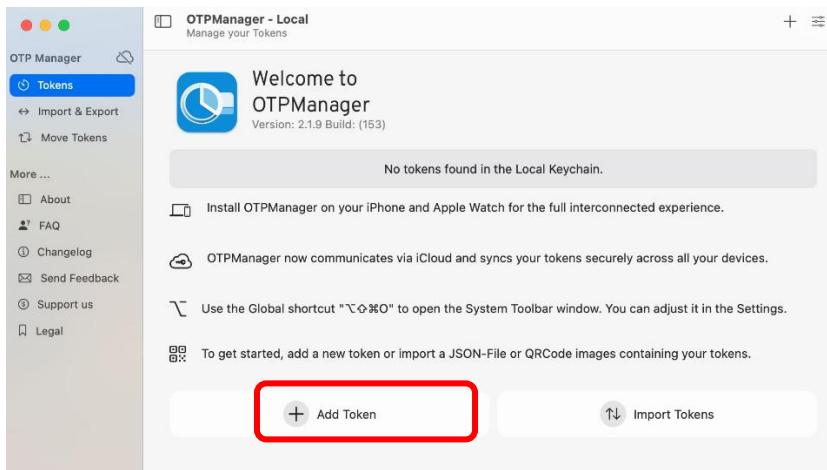
秘密鍵: キーのコピー ▾
[REDACTED]

戻る 次へ

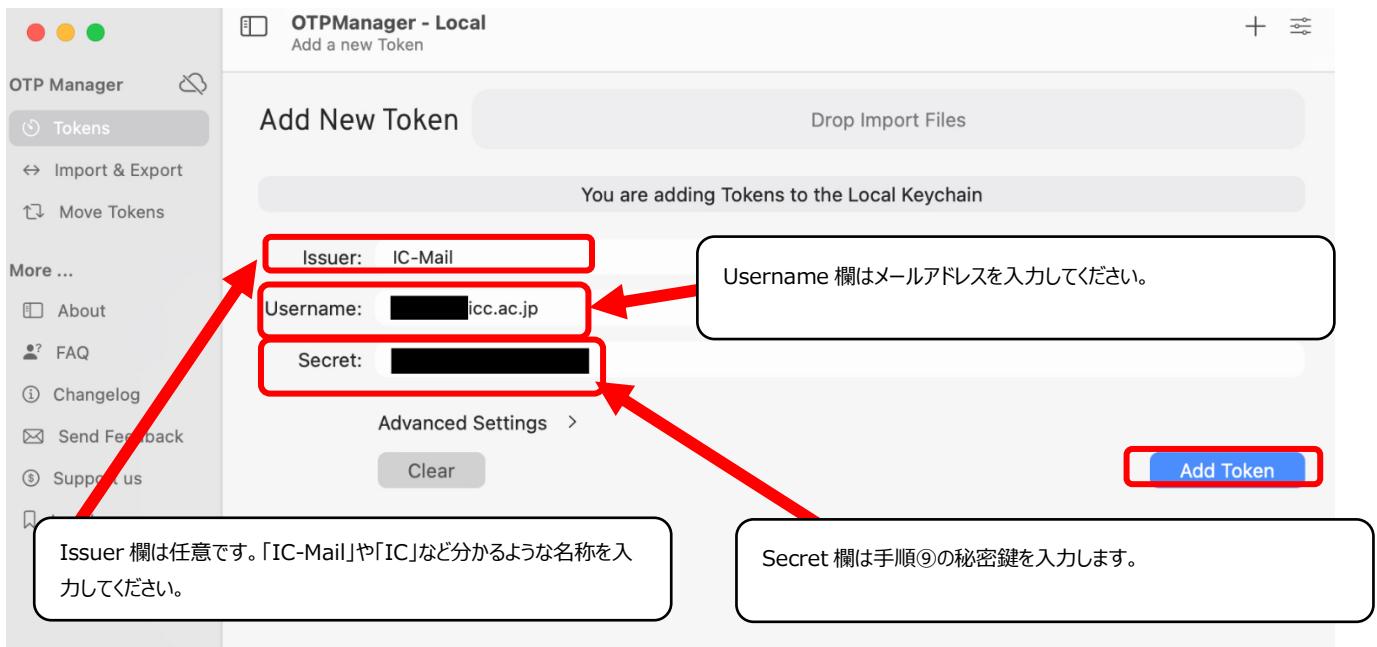
⑩ さきほどインストールしたアプリ（OTP Manager）を起動します。



⑪ [Add Token]ボタンをクリックします。



⑫ 設定情報を入力します。「Issuer」欄と「Username」欄と「Secret」欄入力したら、[Add Token]をクリックします。



⑬ ブラウザに戻り、**次へ**ボタンをクリックします。

Enter the following into Authenticator

Authenticator で QR コード スキャナーを開き、[手動
でコードを入力] を選択します。

アカウント名: 名前のコピー 
茨城キリスト教学園: [REDACTED] icc.ac.jp

秘密鍵: キーのコピー 

戻る

次へ

⑭ コードの入力画面になります。アプリ（OTP Manager）に表示されている 6 行のコードを入力し、**次へ**ボタンをクリックします。

コードの入力

×

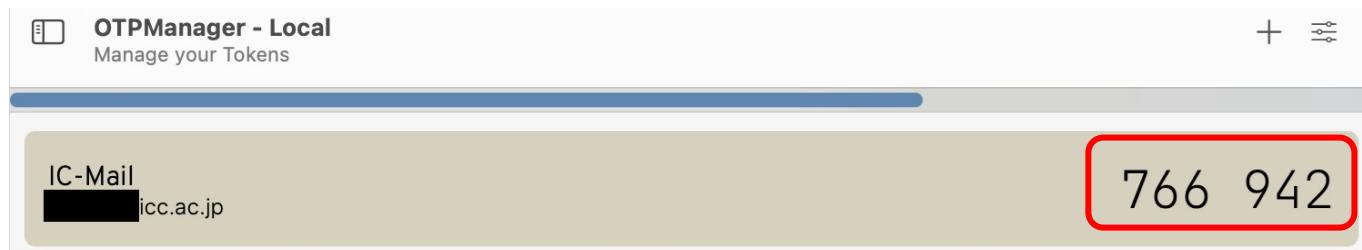
認証アプリから入手した 6 行のコードを入力してください。

コードは一例です。

766942

戻る

次へ



⑯ アプリ追加の画面が表示されたら完了ボタンをクリックします。

Authenticator アプリが追加されました



次回サインインするときは、このアプリのコードを使用してください。

完了

⑰ セキュリティ情報に認証アプリが追加されました。

The screenshot shows the 'Security Information' section of a user profile. On the left, there's a sidebar with options: 概要 (Overview), セキュリティ情報 (Security Information) (which is selected and highlighted in blue), デバイス (Devices), パスワードの変更 (Password Change), and 組織 (Organization). The main area is titled 'セキュリティ情報' and contains the message: '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。'. Below this, there's a table with a single row: '+ サインイン方法の追加'. The row details are: パスワード (Password) with a change link, 最終更新日時: 5年前 (Last updated: 5 years ago), and a '変更' (Change) button. At the bottom of the table, there's a row for '認証アプリ' (Authentication App) with the subtext '時間ベースのワンタイム パスワード (TOTP)' and a '削除' (Delete) button. A red rectangle highlights this entire row.

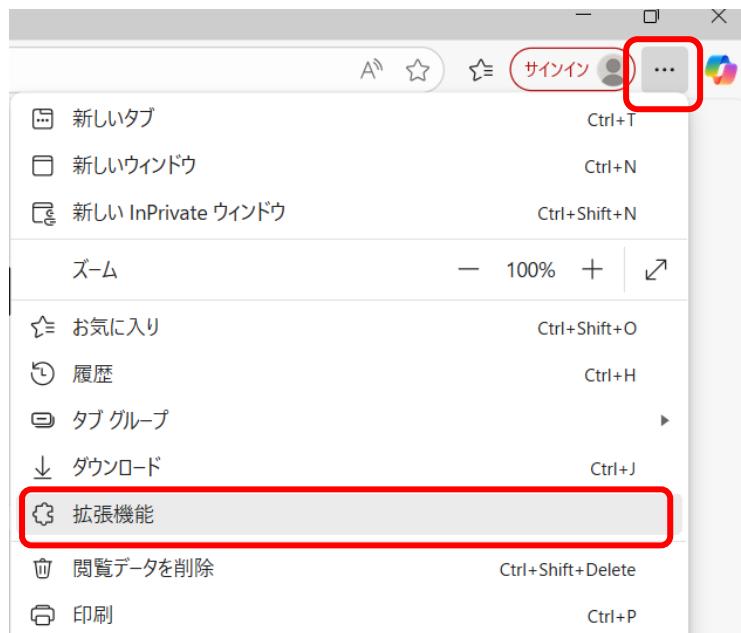
これでアプリ（OTP Manager）の設定は完了です。 サインイン要求の指示に従って、OTP Manager を起動しコードを入力して認証してください。

多要素認証 ブラウザ拡張機能の設定の方法

パソコンのブラウザ拡張機能で、多要素認証を行うことができます。（Windows、macOS どちらでも可能）

【Microsoft Edge】の場合

- ① ブラウザの Microsoft Edge を起動します。
- ② 右上の…ボタンをクリックして、拡張機能を選択します。



- ③ 「Microsoft Edge の拡張機能を検出する」をクリックします。



④ 検索欄で「authenticator」と入力して検索して、「Authenticator: 2FA Client」のインストールボタンをクリックします。

Microsoft | Edge アドオン 検出 拡張機能 テーマ

authenticator

authenticatorに関する14件の結果

All (14) 拡張機能 (14) テーマ (0)

評価

すべて ★★★★☆ & 上 ★★★☆☆ & 上

Authenticator: 2FA Client

拡張機能 ★★★★☆ (135) · mymindstorm

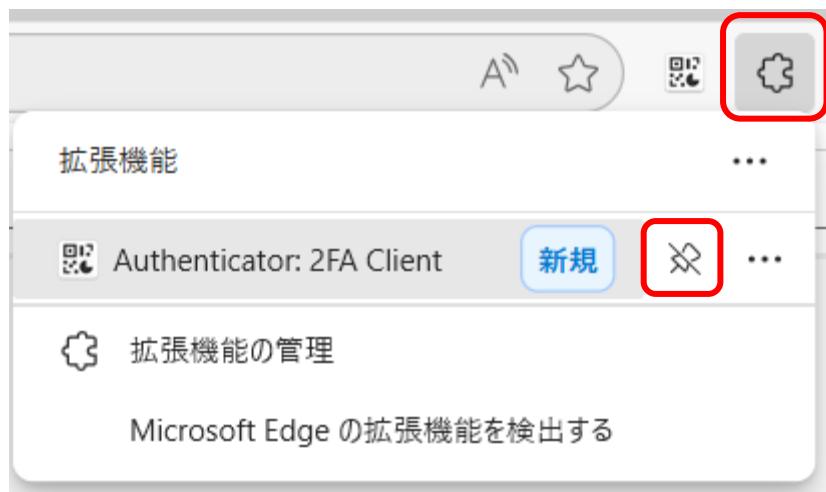
Authenticator generates two-factor authentication codes in your browser.

インストール

⑤ 「Authenticator : 2FA Client」を追加しますかと表示されたら、拡張機能の追加ボタンをクリックします。



⑥ 拡張機能のマークをクリックして、ツールバーに「Authenticator : 2FA Client」を固定します。



⑦ これで Edge の準備は完了です。

続いて多要素認証の設定手順に進みます。「Microsoft Edge」と「Google Chrome」の手順は同様です。

P.18~19 の手順①~⑥を参照して、Microsoft365 にサインイン後にセキュリティ情報まで進んでください。

セキュリティ情報まで進んだら、P.39 の手順⑧以降の作業を進めてください。

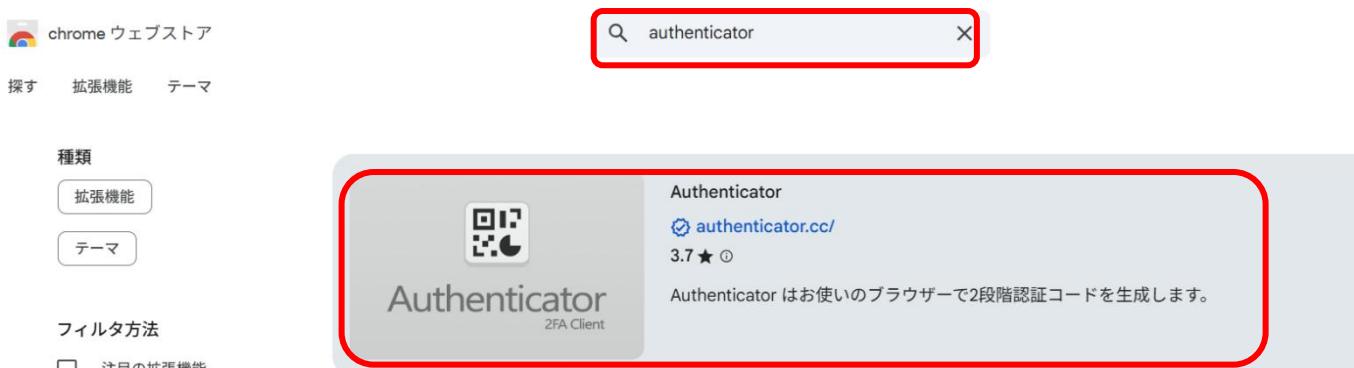
【Google Chrome】の場合

① ブラウザの Google Chrome を起動します。

② 右上の…ボタンをクリックして、「拡張機能」－「Chrome ウェブストアにアクセス」を選択します。



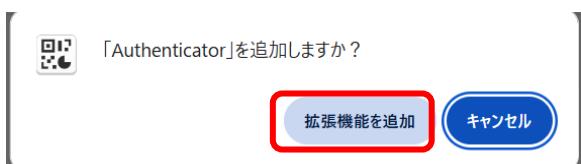
③ 検索欄で「authenticator」と入力して検索して、「Authenticator: 2FA Client」をクリックします。



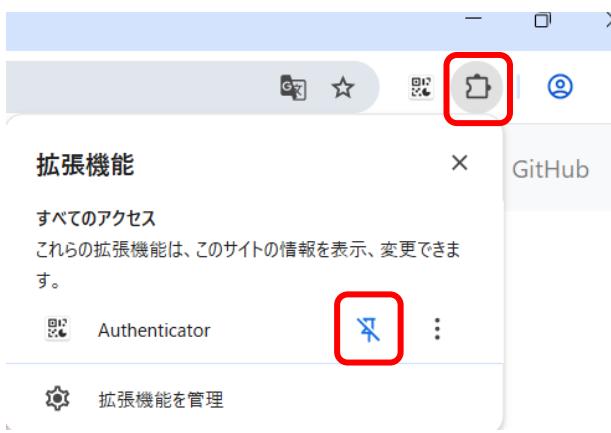
④ Chrome に追加ボタンをクリックします。



⑤ 「Authenticator」を追加しますかと表示されたら、拡張機能の追加ボタンをクリックします。



⑥ 拡張機能のマークをクリックして、ツールバーに「Authenticator」を固定します。



⑦ これで Google Chrome の準備は完了です。

続いて多要素認証の設定手順に進みます。「Microsoft Edge」と「Google Chrome」の手順は同様です。

P.18~19 の手順①～⑥を参照して、Microsoft365 にサインイン後にセキュリティ情報まで進んでください。

セキュリティ情報まで進んだら、以降の手順⑧に進んでください。

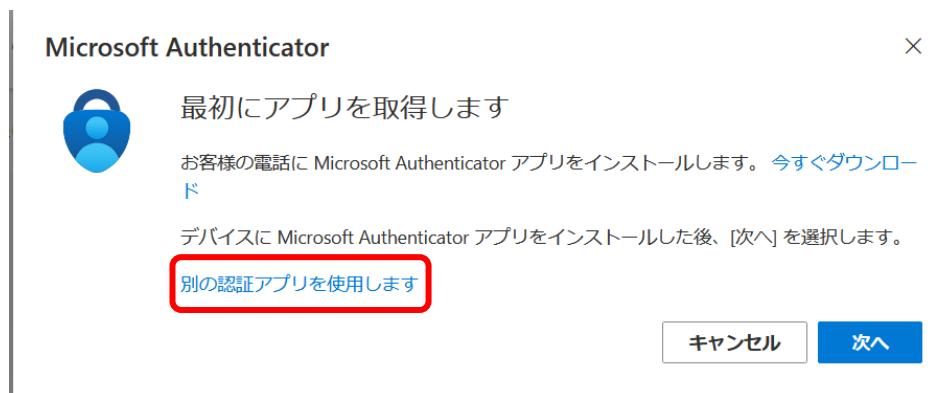
⑧ サインイン方法の追加をクリックします。



⑨ 「Microsoft Authenticator」をクリックします。



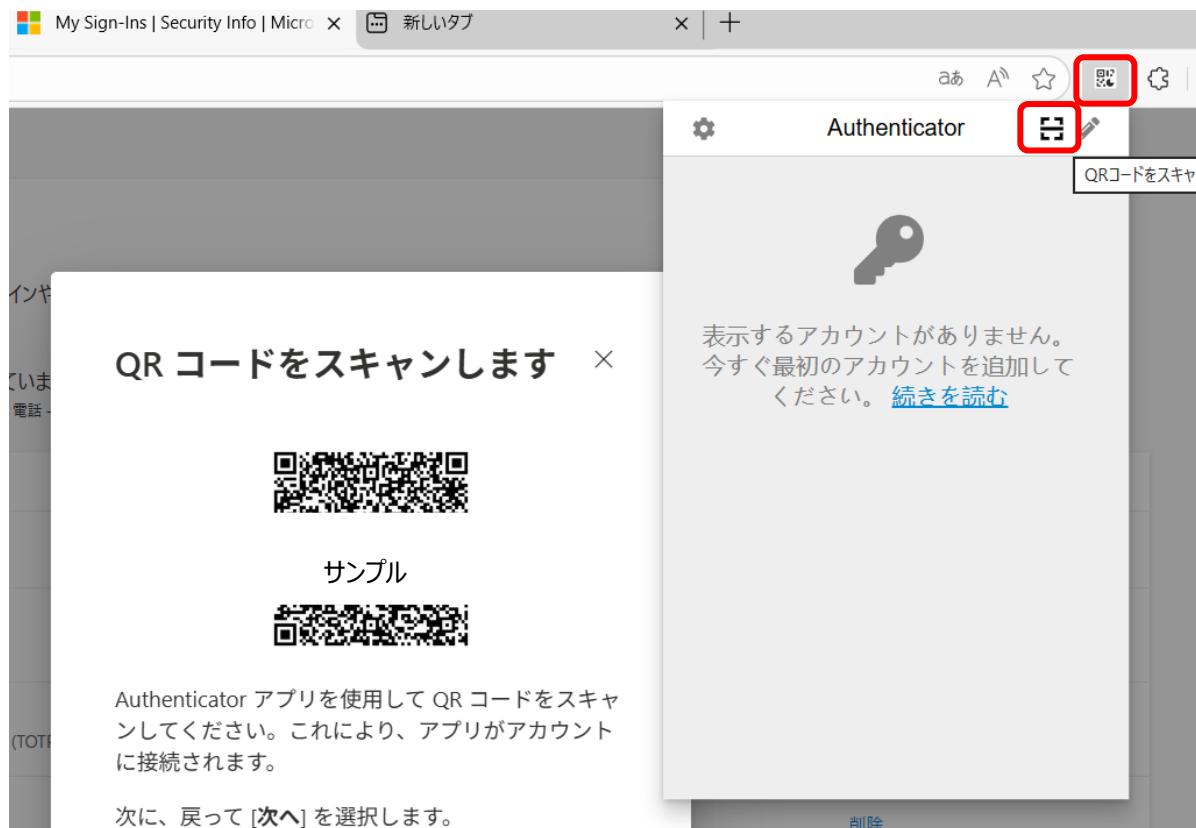
⑩ 「別の認証アプリを使用します」をクリックします。



⑪ 「アカウントのセットアップ」が表示されたら、[次へ]をクリックします。



⑫ QR コードの画面が表示されたら、Authenticator のボタンをクリックして、QR コードのスキャンボタンをクリックします。



⑬ QR コードの読み取り画面になるので、QR コード部分を囲んで読み取ってください。



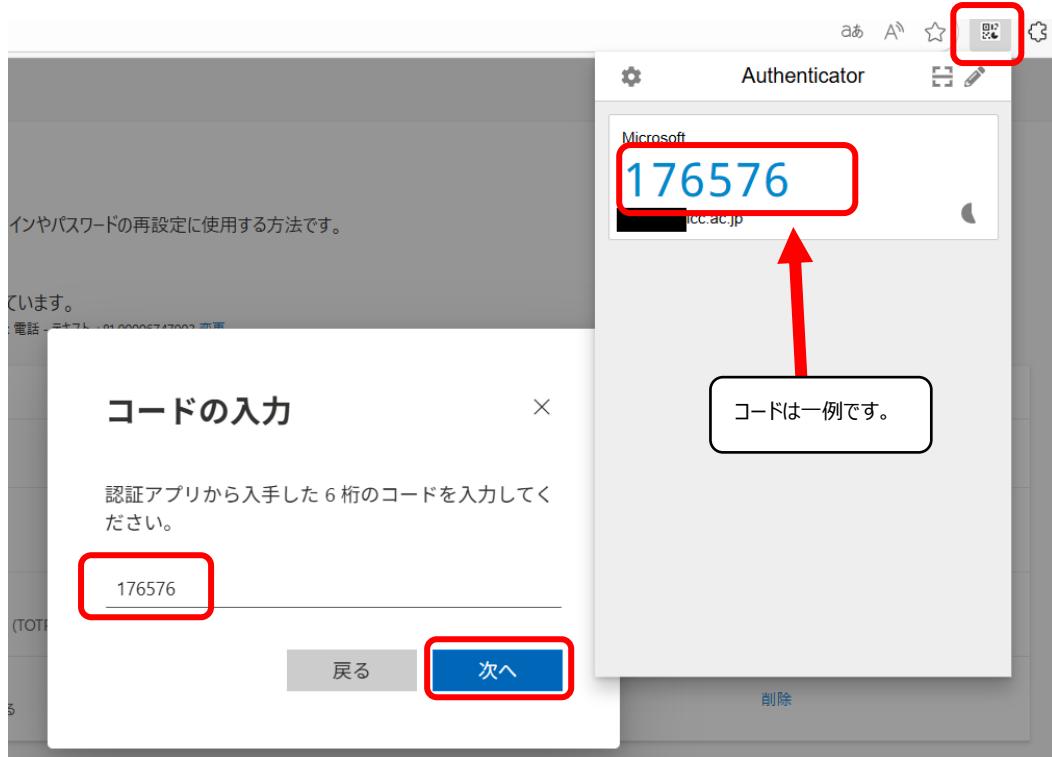
⑭ 「追加されました」と表示されたら、OKボタンをクリックします。



⑮ 次へボタンをクリックします。



⑯ コードの入力画面になったら、Authenticator のボタンをクリックし、6 行の認証コードを入力して次へボタンをクリックします。



⑰ 追加されましたと表示されたら完了ボタンをクリックします。

✓ Authenticator アプリが追加されました



⑲ セキュリティ情報に認証アプリが追加されました。



これでブラウザの拡張機能の設定は完了です。 サインイン要求の指示に従って、ブラウザ拡張機能の Authenticator を起動しコードを入力して認証してください。