

# 多要素認証 全学生教職員向け

(MFA : MULTI-FACTOR AUTHENTICATION)

2026 年 9 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、多要素認証が必須になります。

**まずは 3～7 ページまで読んで順に設定をしてください。**

それ以外のページは補足情報ですのでお時間のある時に適宜ご覧ください。

## 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」

「スマートフォン」+「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

【重要な変更】マイクロソフト社からの発表によりますと、2027年2月1日以降、多要素認証にて「SMS」と「音声電話による認証」は利用できなくなります。

利用可能な認証方法は、

- ・パスキー【推奨】
- ・モバイルアプリ（Microsoft Authenticator）
- ・PC アプリ / ブラウザ拡張機能

となります。

現在、多要素認証にて「SMS」または「音声電話による認証」のみを設定されている方は、パスキーなど他の認証方法の追加登録をお願いいたします。

## 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. スマートフォンの機種変更をしたらどうする？

A. パスキーを設定済みの状態で新旧のスマートフォンに同じアカウントでサインインすれば、パスキーは自動で同期されます。そのためパスキーを利用している方は機種変更をしたとき特に作業はありません。

パスキー以外の設定をした場合は P.8～9 の「多要素認証 設定の変更方法」を参考にしてください。

Q. 多要素認証を行えなくなってしまったらどうする？

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.8～9 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. スマートフォンを持っていない？

A. PC アプリ、またはブラウザ拡張機能で認証が可能です。ブラウザ拡張機能の設定は P.10～14 を参考にしてください。

## 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   |
|-----------------------------------------|-------|
| パスキーを設定する                               | 3～7   |
| 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 | 8～9   |
| パソコンのみで多要素認証を行う                         | 10～14 |

### ⚠【重要】学内ネットワークでの接続について

学内の Wi-Fi や有線 LAN に接続している場合は、これまで通り多要素認証は要求されません。  
本設定 (パスキー) は、「自宅や外出先など、学外から Microsoft 365 にサインインする際」に必要となります。

### 💡【ポイント】

登録作業はスマートフォンから「1 回だけ」行えば完了です。一度登録すれば、スマホだけでなくパソコンでログインするときの鍵としても自動的に使えるようになります。(条件によっては都度登録となります)

## 1. 設定を始める前のチェック (動作環境確認)

必ず以下の指定ブラウザを使い、スマホの設定を確認してから進めてください。

### 🍏 iPhone (iOS) をお使いの方

- 使用ブラウザ：必ず Safari (標準ブラウザ) を使用してください。  
※LINE、X (旧 Twitter)、大学アプリ内のリンクから開くとエラーになります。
- スマホの設定：「設定」アプリ > 最上部の「自分の名前」> 「iCloud」> 「キーチェーン」が オン であること。



- PC 連携の準備：パソコンでログインするときの鍵として使うため、スマホの Bluetooth を「オン」にしてください。

### 🤖 Android をお使いの方

- 使用ブラウザ：必ず Google Chrome を使用してください。
- スマホの設定：指紋認証、顔認証、または画面ロック (パターン・PIN コード) が設定されていること。
- PC 連携の準備：パソコンでログインするときの鍵として使うため、スマホの Bluetooth を「オン」にしてください。

## 2. 【初回のみ】パスキーの登録手順（スマホで作業）

手元のスマートフォンを使って「鍵」の登録を行います。パソコンでの操作は不要です。

### 🍏 パターン A : iPhone (iCloud キーチェーン)

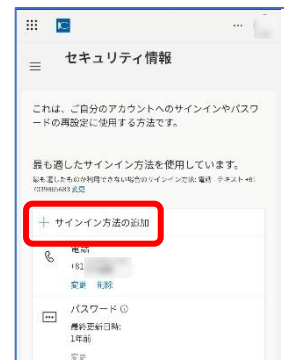
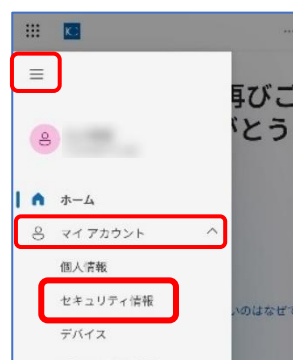
#### 1. マイ アカウントにアクセスする

スマホの Safari から、大学 HP の IC-Mail にアクセスし、現在の認証方式でサインインします。  
受信トレイ右上の〇マークから「アカウントを表示」をタップします。



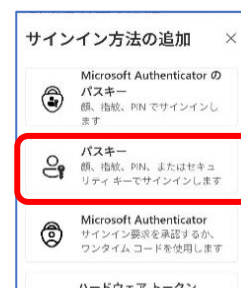
#### 2. セキュリティ情報を開く

画面内の左上にある「三」>「マイアカウント」>「セキュリティ情報」>「+ サインイン方法の追加」の順にタップします。



#### 3. パスキーを選択する

メニューから「パスキー」を選択し、「追加」をタップします。



#### 4. iCloud への保存に同意する

iPhone の画面下部から  
「「iCloud キーチェーン」にパスキーを保存しますか？」  
というダイアログが表示されます。「続ける」をタップします。



#### 5. 認証を行う

Face ID（顔認証）、Touch ID（指紋認証）または  
デバイスのパスコードによる認証をし、本人確認を行います。

#### 6. 登録を完了する

Microsoft の画面に戻り、登録した鍵の名前(例：ICpasskey など)  
を入力して「次へ」>「完了」をタップすれば終了です。

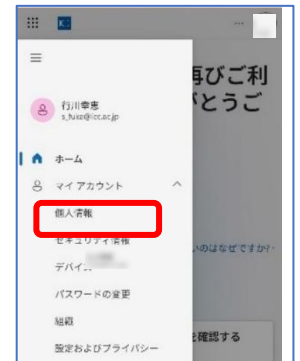
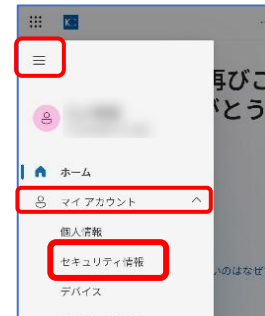


 パターン B : Android (Google パスワード マネージャー)

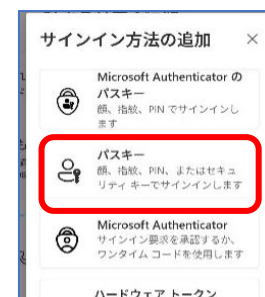
1. Microsoft マイ アカウントにアクセスする  
スマホの Google Chrome から、大学 HP の IC-Mail にアクセスし、現在の認証方式でサインインします。  
受信トレイ右上の〇マークから「アカウントを表示」をタップします。



2. セキュリティ情報を開く  
画面内の左上にある「三」>「マイアカウント」>「セキュリティ情報」>「+ サインイン方法の追加」の順にタップします。



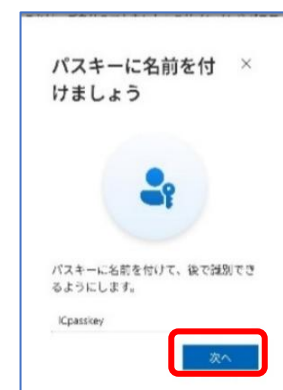
3. パスキーを選択する  
サインイン方法の追加から「パスキー」を選択します。



4. 保存先を選択する  
Google パスワードマネージャーのパスキー作成画面が表示されます。  
自分の Google アカウントが保存先に選択されていることを確認します。  
指紋、顔、またはパターン/PIN コード入力を求められますので、普段通りロックを解除します。



5. 登録を完了する  
Microsoft の画面に戻り、登録したパスキーの名前（例：ICpasskey など）を入力して「次へ」>「完了」をタップすれば終了です。



### 3. 【次回から】サインインの手順（用途に合わせて2通り）

学外から Microsoft 365 にサインインする際の手順です。（※学内ネットワーク接続時はこの認証はスキップされます）

#### パターン1：スマートフォンでサインインする場合

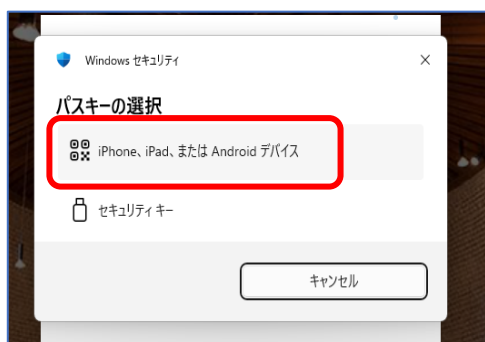
1. サインイン画面（Outlook や Teams アプリなど）で大学のメールアドレスを入力し、「パスキーを使用する」をタップします。
2. スマホの画面下部に生体認証が表示されるので、そのまま 指紋・顔認証・PIN を行うだけでサインインが完了します。

#### パターン2：パソコン（PC）でサインインする場合（クロスデバイス認証）

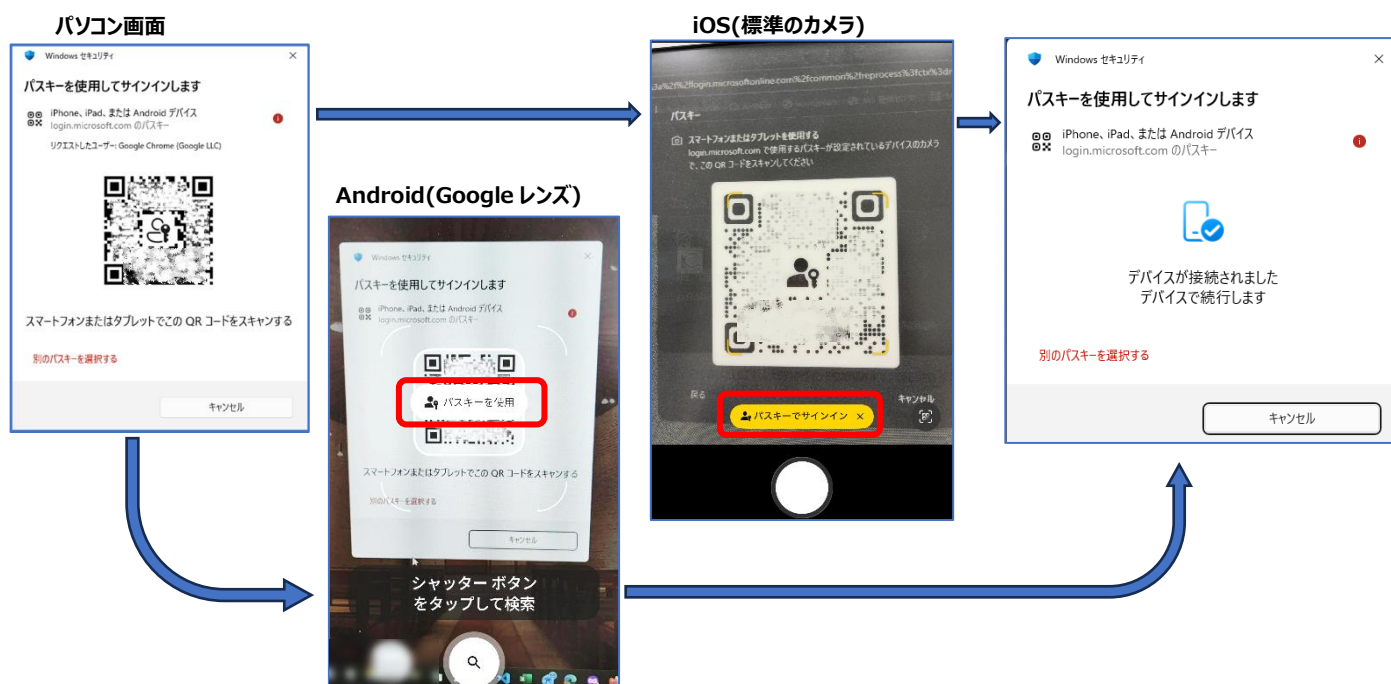
※事前に、パソコンとスマートフォンの両方で Bluetooth がオンになっていることを確認してください。

（デスクトップパソコンでは Bluetooth が実装されていない機種が多いためご注意ください。）

1. パソコンのブラウザ等で IC-Mail サインイン画面を開き、大学のメールアドレスを入力します。
2. 「パスキーの選択—iPhone、iPad、または Android デバイス」をクリックします。



3. パソコン画面に QR コードが表示されます。スマホの「標準カメラアプリ」や「Google レンズ(Android)」で読み取りスマホ側で生体認証を行います。（LINE アプリのコードスキャナなどでは読み込めません）



#### 4. トラブルシューティング（ヘルプデスク用 FAQ）

##### Q1. 学内にいるのにパスキーを求められます

原因：スマホや PC が、大学の公式 Wi-Fi（学内ネットワーク）ではなく、携帯電話のキャリア回線（4G/5G）やモバイルルーター等に接続されている可能性があります。

対処法：端末の Wi-Fi 設定を開き、学内ネットワークに正しく接続されているか確認してください。

##### Q2. パソコンでのサインイン時、「近くのデバイスが見つかりません」とエラーになります

原因：パソコンまたはスマホの Bluetooth がオフになっているか、端末同士が物理的に離れすぎています。

対処法：双方の端末の Bluetooth 設定が「オン」になっているか確認してください（※機器同士のペアリング操作は不要です）。スマホをパソコンのすぐ近くに置いて再試行してください。

##### Q3. iPhone で「続ける」のポップアップが出ない、または QR コードを読み取っても反応しません

原因：Safari 以外のブラウザ（Chrome やアプリ内ブラウザ）を使用している可能性があります。

対処法：iPhone での初期登録操作は、必ず Safari（標準ブラウザ）を使用してください。また、iCloud キーチェーンがオンになっているか確認してください。

##### Q4. Android で「Google パスワード マネージャー」以外のアプリが起動してしまいます

原因：自動入力サービスが Google 以外（他社製パスワード管理アプリなど）に設定されている可能性があります。

対処法：スマホの「設定」>「パスワードと自動入力」から、自動入力サービスが「Google」に設定されているか確認してください。

パスキーを Google パスワードマネージャー、もしくは iCloud キーチェーンに保存していれば、スマートフォンを機種変更してもパスキーを引き継ぐことができます。しかしそれ以外の方法で多要素認証を設定すると、スマートフォンの機種変更したときに多要素認証の設定変更が必要になります。

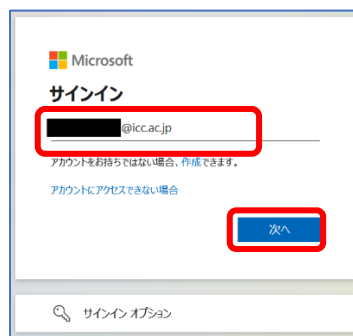
もし多要素認証ができなくなったら、まずは学内から Microsoft365 にパスワード認証でアクセスして認証要素の追加削除をしてください。学内からはパスワードのみでサインイン可能です。

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/>) から「IC-MAIL」を開きます。  
または URL (<https://outlook.office365.com/>) にアクセスします。



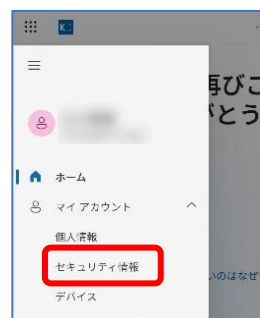
- ② Microsoft のログイン画面が表示されるので、「メールアドレス」を入力して「次へ」ボタンをクリックします。  
学内ネットワーク：「パスワード」を入力します。  
学外ネットワーク：自身が設定した多要素認証の方法でサインインしてください。



- ③ サインイン後、画面右上にある「丸マーク」をクリックして「アカウントを表示」をクリックします。



- ④ 「マイアカウント」の左上にある「三」>「セキュリティ情報」の順にクリックします。



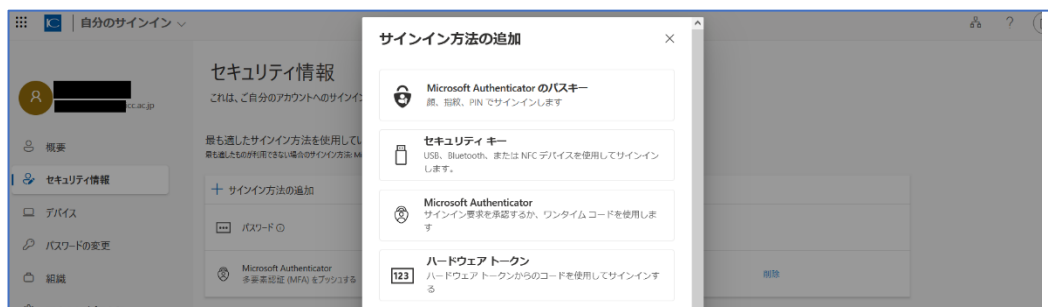
⑤ 認証方法の追加、削除は以下の方法を参照してください。

### 【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。



追加したい方法を選択してください。



### 【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。



パソコンのみで多要素認証をする方法について、アプリやブラウザ拡張機能を使うことが可能です。

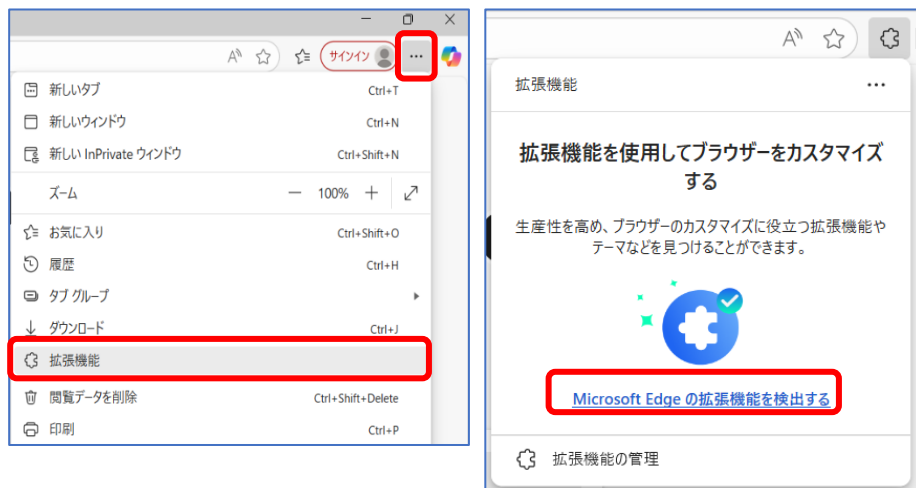
アプリの場合、Windows なら WinAuth、MacOS なら OTP Manager などが有名です。ご自身で最新版を取得して設定方法を調べてください。

ここではより簡便なブラウザ拡張機能で多要素認証を行う方法を説明します。（Windows / Mac どちらでも可能）

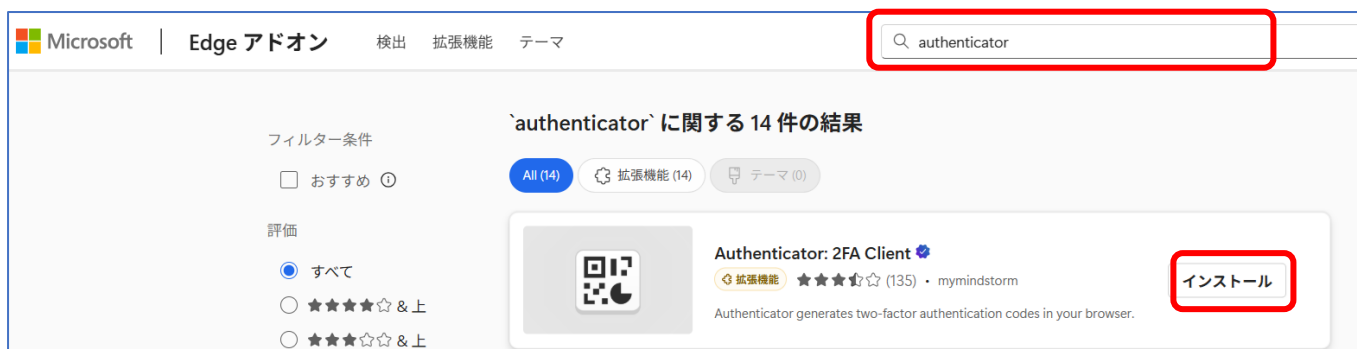
### 【Microsoft Edge】の場合

- ① Microsoft Edge を起動します。

右上の「…」ボタン>「拡張機能」>「Microsoft Edge の拡張機能を検出する」の順にクリックします。



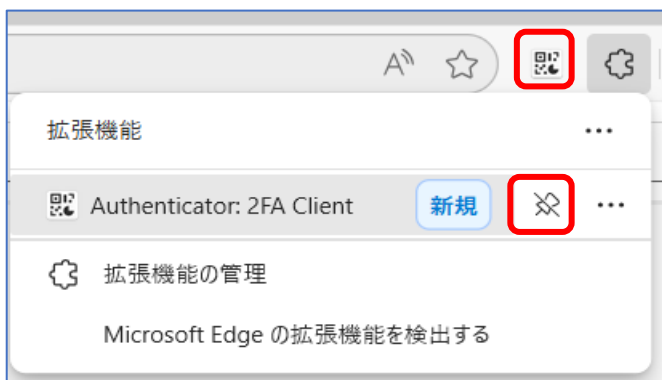
- ② 検索欄で「authenticator.cc」と入力して検索して、「Authenticator: 2FA Client」のインストールボタンをクリックします。



- ③ 「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。



- ④ 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。



⑤ これで Edge の準備は完了です。

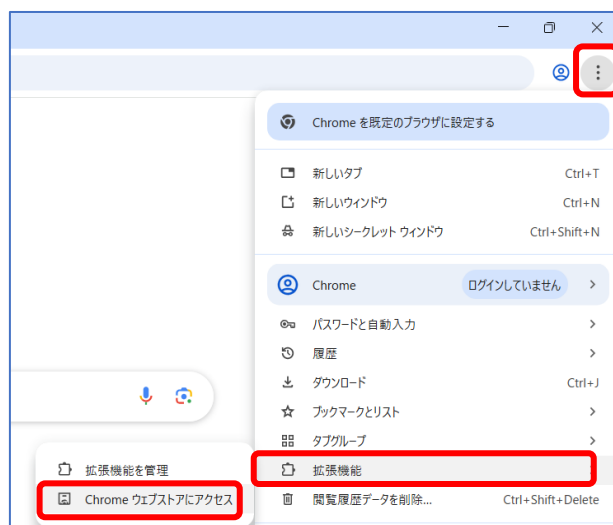
続いて多要素認証の設定手順に進みます。「Microsoft Edge」と「Google Chrome」の手順は同様です。

P. 8～9 の手順①～⑤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。

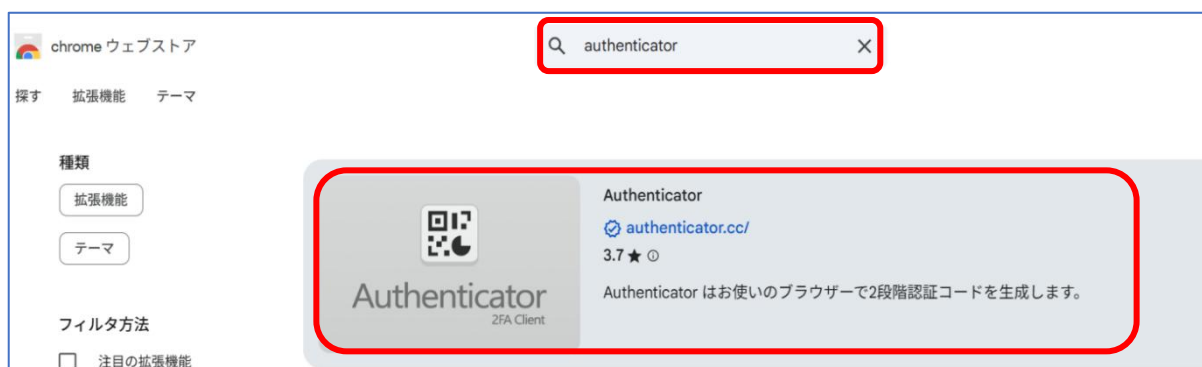
#### 【Google Chrome】の場合

① Google Chrome を起動します。

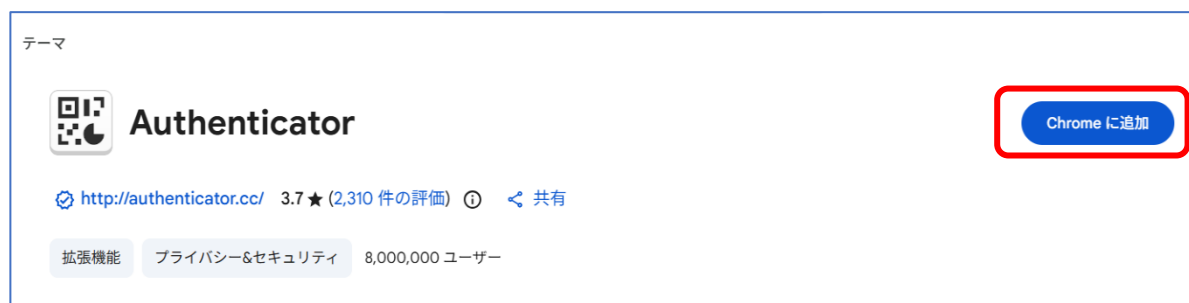
右上の☰ボタン>「拡張機能」>  
「Chrome ウェブストアにアクセス」の順にクリックします。



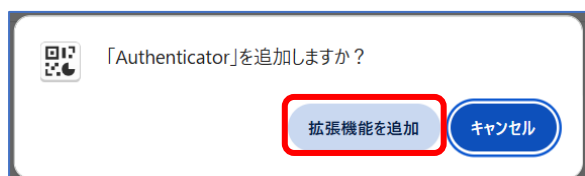
② 検索欄で「authenticator.cc」と入力して検索して、「Authenticator: 2FA Client」をクリックします。



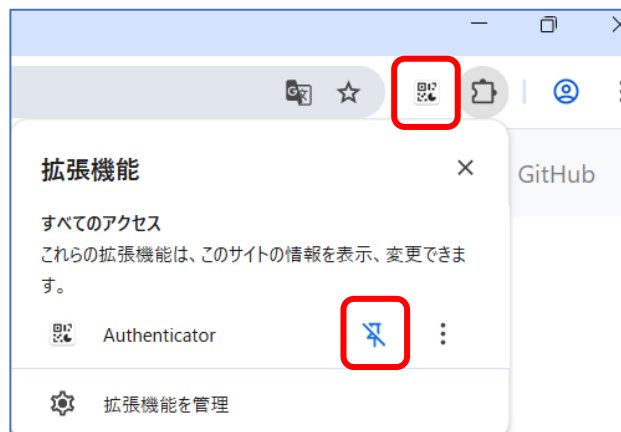
③ Chrome に追加ボタンをクリックします。



④ 「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。



- ⑤ 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。



- ⑥ 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。

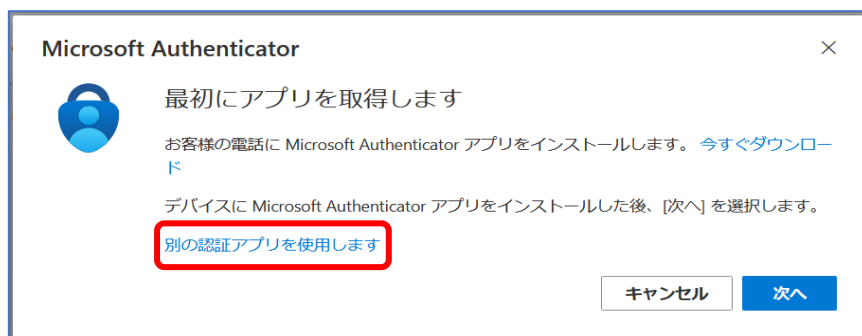
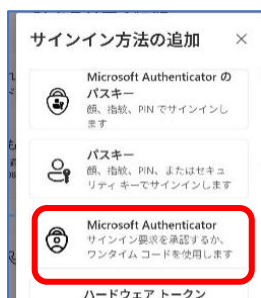
**P. 8～9 の手順①～⑤を参照して、Microsoft365 にサインイン後にセキュリティ情報まで進んでください。**

セキュリティ情報まで進んだら、以降の手順⑦に進んでください。

- ⑦ サインイン方法の追加をクリックします。



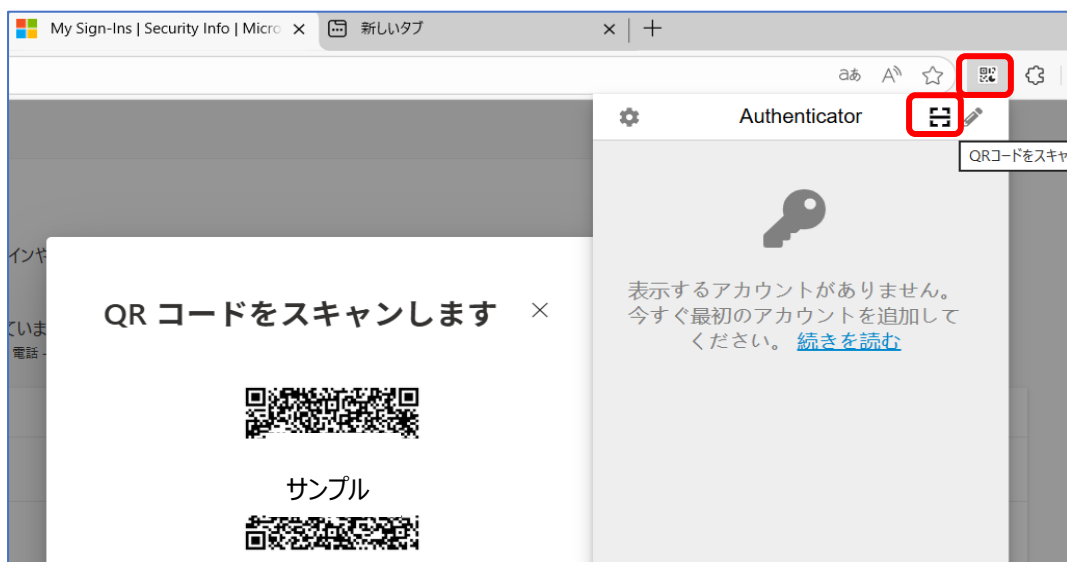
- ⑧ 「Microsoft Authenticator」>「別の認証アプリを使用します」をクリックします。



「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。

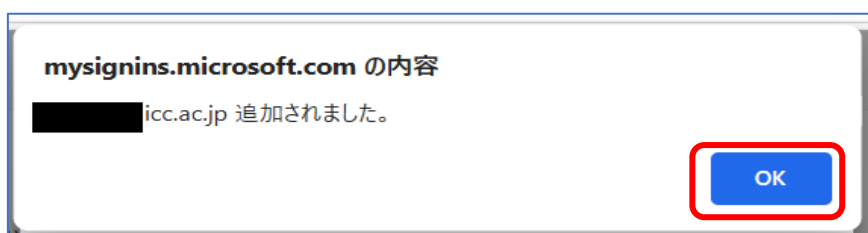
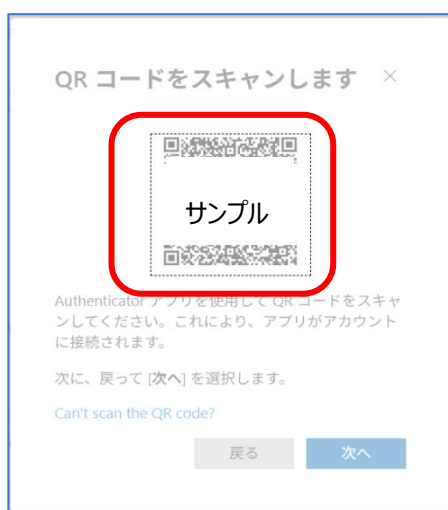


- ⑨ QRコードの画面が表示されたら、Authenticator のボタンをクリックして、QRコードのスキャンボタンをクリックします。

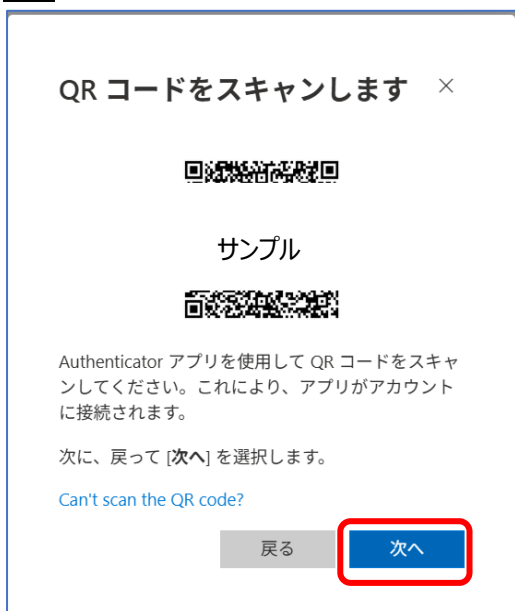


QRコードの読み取り画面になるので、QRコード部分を囲んで読み取ってください。

「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。



- ⑩ **次へ** ボタンをクリックします。



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 桁の認証コードを入力して次へボタンをクリックします。その後、「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。



設定完了です。以降はサインインのときブラウザ拡張機能の Authenticator からコードを入力して認証してください。

- ⑪ 職場のパソコンと自宅のパソコンなど複数の場所で異なるパソコンを利用している場合、次の作業に進んでください。

「Authenticator」>「歯車のアイコン」>「バックアップ」>「バックアップファイルのダウンロード」の順でクリックして、バックアップファイルを保存します。そのファイルを USB メモリ等で異なるパソコンに持っていきます。

異なるパソコンでもまず①から⑤の手順でブラウザ拡張機能の Authenticator を追加します。「Authenticator」>「歯車のアイコン」>「バックアップ」>「バックアップのインポート」>「バックアップファイルのインポート」の順でクリックしてバックアップファイルを選択します。



以上で複数のパソコンから共通の設定でログインできるようになりました。