千葉工業大学 統合認証システム
利用ガイド

第1.5版

２０２６年1月１５日

情報システム委員会
総務部（情報システム担当）

目 次

1. 千葉工業大学 統合認証システム 概要

千葉工業大学 統合認証システム（以下、「統合認証」）は、「シングルサインオン」と「二要素認証」の機能を備えた認証システムです。

「シングルサインオン」とは、一度の認証で、複数のサービスにログインできる仕組みです。同一ブラウザで複数のサービス（例：CIT ポータルと Google Workspace など）にログインする際、ログイン作業が簡便になり利便性が向上します。

「二要素認証」とは、認証の際に 2 つの異なる認証要素を要求するセキュリティの仕組みです。仮に 1 つの認証要素が漏洩しても不正アクセスを防げるため安全性が高まります。

本学では以下のサービスが統合認証の対象サービスとなります。これらの対象サービスにログインする際は、統合認証を経由して認証を行います。次ページのイメージ図を参照ください。

統合認証 対象サービス一覧

2025 年 7 月 2 日以前	2025 年 7 月 3 日以降
・学認 ・Adobe	・学認 ・Adobe ・CIT ポータル ・Google Workspace（工大メール等） ・Microsoft 365 ・VPN 接続サービス

千葉工業大学 統合認証システム イメージ図

統合認証 対象サービス

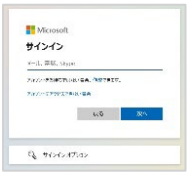
２０２５年７月時点

Google Workspace

CIT ポータル

GakuNin

学認



Microsoft 365

Adobe

VPN 接続サービス

ログイン要求

ログイン完了

統合認証システム

第１要素目の認証

パスワード認証

二要素認証
未設定の場合

二要素認証
設定済の場合

第２要素目の認証

ワンタイムコード認証

もしくは

パスキー認証

事前に設定したアプリに表示されるワンタイムコードによる認証

事前に設定したデバイスでの顔認証や指紋認証等による認証

2. 二要素認証とは

二要素認証とは、認証の際に 2 つの異なる認証要素を要求するセキュリティの仕組みです。仮に 1 つの認証要素が漏洩しても不正アクセスを防げるため安全性が高まります。

統合認証における二要素認証では、第 1 要素目の認証は「MARINE ユーザーID」と「パスワード」による認証、第 2 要素目の認証は「ワンタイムコード」もしくは「パスキー」による認証となります。

認証の安全性をより強化するため、統合認証の利用者は、二要素認証（ワンタイムコード、パスキー）の設定を各自で行ってください。

ワンタイムコード認証とは

Authenticator（オーセンティケーター）と呼ばれるワンタイムコードを生成するアプリに表示される一度限りのコード（数字 6 桁）を入力する認証方式です。アカウント情報の漏洩やフィッシング詐欺による不正アクセスにも強く、安全な認証方式です。
Authenticator は主にスマートフォンにインストールして使いますが、PC のブラウザ拡張機能を使って Authenticator を使用することもできます。

Authenticator は複数の種類が存在します。統合認証で利用できる主な Authenticator は以下の通りです。

［利用できる主な Authenticator の種類］

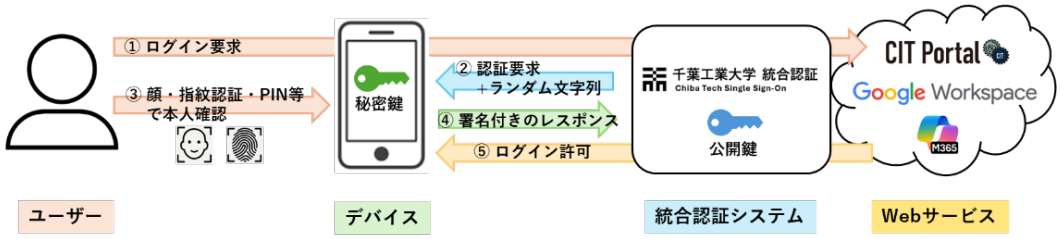
デバイス種別	OS	利用できる主な Authenticator の種類
スマートフォン	iOS/Android	Google Authenticator・Microsoft Authenticator・FreeOTP
PC	Windows/macOS	Chrome 拡張機能・Edge 拡張機能

※本書では、上記表に記載された Authenticator のうち、赤字で示したものを使用する手順を紹介しています。

パスキー認証とは

スマートフォンや PC などのデバイスによる顔認証、指紋認証、PIN コード、パターン認証、USB セキュリティキーなどを用いて認証を行う方式です。パスワードを覚える必要がなく簡単に認証することができ、アカウント情報の漏洩やフィッシング詐欺による不正アクセスにも強い、安全な認証方式です。

［パスキーを使った認証の流れ］



パスキー認証は比較的新しい認証技術のため、古いデバイスや OS では利用できない場合があります。

［パスキーに対応した主な OS と要件］

デバイ種類	OS	OS バージョン	主な要件
スマートフォン	iOS	iOS 16 以降	・パスコードが設定されていること（顔認証、指紋認証も併用可） ・iCloud キーチェーンが有効であること
	Android	Android 9 以降	・画面ロック(PIN、パスワード等)が有効であること
PC	Windows	Windows 10 (22H2) 以降	・Windows Hello（顔認証、指紋認証、PIN のいずれか）が設定されていること
	macOS	macOS Ventura (13) 以降	・ロック解除方法が有効になっていること（Touch ID、パスワード） ・iCloud キーチェーンが有効になっていること

※ 上記の要件を満たしていても、機種やその他の条件によってはご利用いただけない可能性がございます。

［パスキーに対応した主なブラウザ］

Google Chrome 、Safari 、Microsoft Edge

※ ブラウザ以外のアプリケーションはパスキー認証に対応していない場合があります。パスキー認証を設定したことによりアプリケーションにログインできない場合は、パスキー認証の設定を一旦削除してアプリケーションにログインしてください。

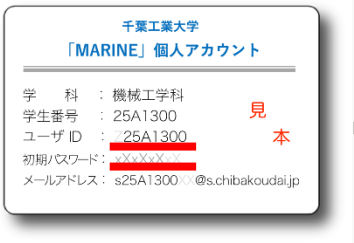
3. 第1要素目の認証（パスワード認証）

3-1 第1要素目の認証方法

統合認証における第 1 要素目の認証は、「MARINE ユーザーID」と「パスワード」による認証です。

入学時に配布された「MARINE 個人アカウントカード」に記載されたユーザーID とパスワードを入力してサインインします。（ご自身でパスワードを変更済みの場合は、変更後のパスワードを入力します。）

第1要素認証画面

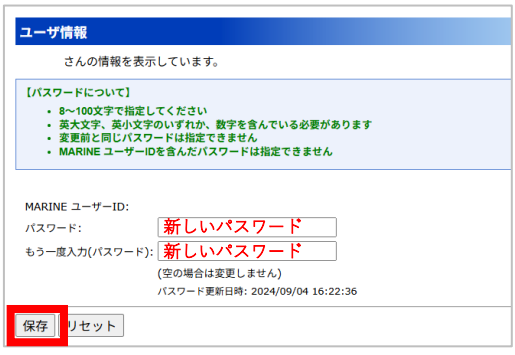


3-2 第1要素目のパスワード変更方法

第 1 要素目のパスワードを変更するためには、MARINE アカウントのパスワードを変更する必要があります。

MARINE アカウントのパスワードを変更するためには、「MARINE Account Center」にログインし、新しいパスワードを 2 回入力後、「保存」ボタンを押して下さい。

MARINE Account Center URL： https://mac.chibatech.ac.jp/



4. 第2要素目の認証（ワンタイムコード認証・パスキー認証）

4-1 第2要素目の認証方法

統合認証における第２要素目の認証は、「ワンタイムコード」もしくは「パスキー」による認証です。

「ワンタイムコード認証」を設定した場合は、事前に設定したワンタイムコードアプリに表示されたワンタイムコード（数字６桁）を入力してサインインします。

「パスキー認証」を設定した場合は、「パスキーでサインイン」を選択した後に、事前に設定したデバイスでの顔認証、指紋認証、PIN コード、パターン認証や USB セキュリティキーなどを用いて認証を行います。（認証方法は使用するデバイスや設定により異なります。）

「ワンタイムコード認証」と「パスキー認証」の両方が登録してある場合は、どちらを使ってログインするか選択することができます。

ユーザー自身がワンタイムコードもしくはパスキーを事前に登録していない場合は、第二要素目の認証はスキップされます。認証の安全性をより強化するために、8～21 ページの手順を参照して、「ワンタイムコード」もしくは「パスキー」の設定を行って下さい。

4-2 ワンタイムコードの設定方法（iPhoneの場合）

（1）iPhone に「Google Authenticator」をインストールする

① iPhone で「App Store」を開き「Google Authenticator」を検索する、もしくは iPhone で以下の QR コードを読み込み「Google Authenticator」にアクセスする。

② 「Google Authenticator」を「入手」する。

③ インストールされた「Google Authenticator」を起動し、「開始」をタップする。

④ 「ログイン」もしくは「アカウントなしで Authenticator を使用」のどちらかをタップする。（任意）
「ログイン」を選択した場合は、Google アカウントでログインをする。

個人 Google アカウントでログインすることを推奨いたします。

[ログインを推奨する理由]
ログインすることでワンタイムコードの登録情報がアカウントに保存されます。このため、端末を変更した場合に、新しい端末で同じ Google アカウントにログインするだけで Google Authenticator を再設定でき、設定情報が失われる心配がありません。

[個人 Google アカウントを推奨する理由]
大学の Google アカウント（工大メールアドレス）でログインした場合、Google Authenticator へログインする際に統合認証のワンタイムコード入力が必要となることがあります。しかし、Google Authenticator にアクセスできないとワンタイムコードを確認できず、ログインできない状況となる可能性があります。

⑤ 以下の画面が表示されたら一旦 iPhone 側の作業は終了し、（2）の手順に進んで下さい。

（2）「統合認証アカウントコンソール」にログインし、Authenticator を登録する

① PC（タブレット等でも可）のブラウザで、「統合認証アカウントコンソール」にアクセスする。

統合認証アカウントコンソール

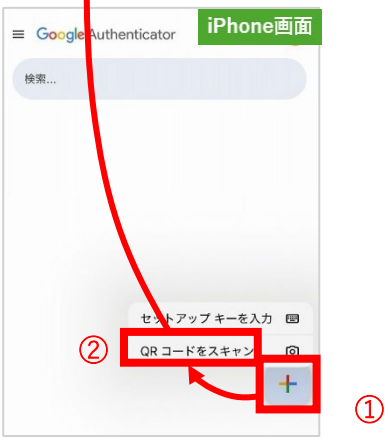
https://sso.chibatech.ac.jp/realms/marine/account/

② MARINE ユーザーID とパスワードを入力して「Sing In」をクリックする。

③ 統合認証アカウントコンソールメニューの「アカウント・セキュリティ」をクリックし、次に「サインイン」をクリックする。

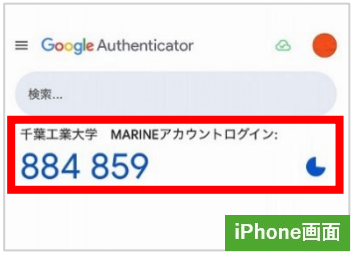
④ 「二要素認証」の配下にある「ワンタイムコードアプリを設定する」をクリックする。

⑤ QR コードが表示されたら、iPhone にインストールした Google Authenticator を起動し、右下の「 + 」ボタンから「QR コードをスキャン」をタップし、QR コードを読み込む。



⑥ QR コードの読み込みが完了したら、Google Authenticator に 6 桁のワンタイムコードが表示されるようになります。

※ワンタイムコードは一定時間毎に変わり続けます。



⑦ 「ワンタイムコード」欄に、iPhone の Google Authenticator 上に表示されたワイムコードを、「デバイス名」欄に任意の名称（例：iPhone）を記入し、「送信」をクリック。

⑧ ワンタイムコードアプリの配下に、登録したデバイス名が表示されます。

⑨ 以上でワンタイムコード認証の設定は完了です。

統合認証にログインする際、ワンタイムコードを使った二要素認証ができるようになりました。

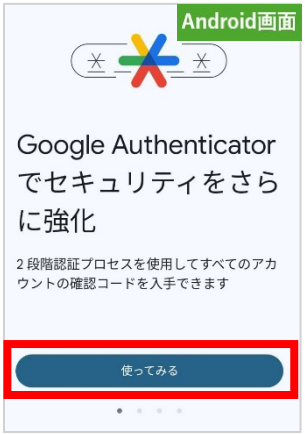
4-3 ワンタイムコードの設定方法（Androidの場合）

（1）Android に「Google Authenticator」をインストールする

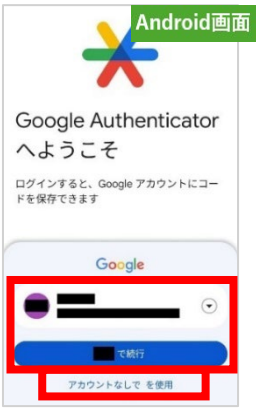
① Android 端末で「Play ストア」を開き「Google 認証システム」を検索する、もしくは Android 端末で以下の QR コードを読み込み「Google 認証システム」にアクセスする。

② 「Google 認証システム」を「インストール」する。

③ インストールされた「Google 認証システム」を起動し、「使ってみる」をタップする。



④ Google アカウントでログインして使用するか、「アカウントなしで使用」のどちらかを選択する。（任意）



個人 Google アカウントでログインすることを推奨いたします。

[ログインを推奨する理由]
ログインすることでワンタイムコードの登録情報がアカウントに保存されます。このため、端末を変更した場合に、新しい端末で同じ Google アカウントにログインするだけで Google Authenticator を再設定でき、設定情報が失われる心配がありません。

[個人 Google アカウントを推奨する理由]
大学の Google アカウント（工大メールアドレス）でログインした場合、Google Authenticator へログインする際に統合認証のワンタイムコード入力が必要となることがあります。しかし、Google Authenticator にアクセスできないとワンタイムコードを確認できず、ログインできない状況となる可能性があります。

⑤ 以下の画面が表示されたら一旦 Android 側の作業は終了し、（2）の手順に進んで下さい。

（2）「統合認証アカウントコンソール」にログインし、Authenticator を登録する

① PC（タブレット等でも可）のブラウザで、「統合認証アカウントコンソール」にアクセスする。

統合認証アカウントコンソール

https://sso.chibatech.ac.jp/realms/marine/account/

② MARINE ユーザーID とパスワードを入力して「Sign In」をクリックする。

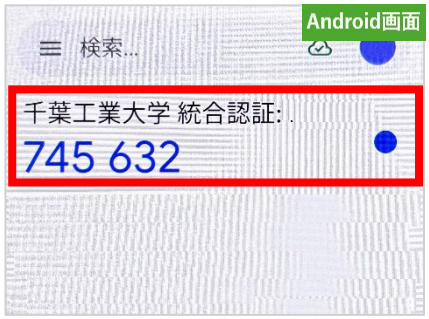
③ 統合認証アカウントコンソールメニューの「アカウント・セキュリティ」をクリックし、次に「サインイン」をクリックする。

④ 「二要素認証」の配下にある「ワンタイムコードアプリを設定する」をクリック。

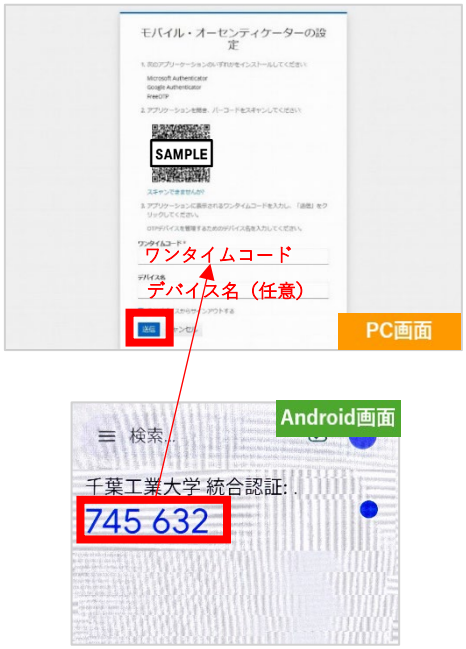
⑤ QR コードが表示されたら、Android にインストールした Google Authenticator を起動し、右下の「 + 」ボタンから「QR コードをスキャン」をタップし、QR コードを読み込む。

⑥ QR コードの読み込みが完了したら、Google Authenticator に 6 桁のワンタイムコードが表示されるようになります。

※ワンタイムコードは一定時間毎に変わり続けます。



⑦ 「ワンタイムコード」欄へ、Android 端末の Google Authenticator 上に表示されたワンタイムコードを、「デバイス名」欄へ、任意の名称（例：Android）を記入し、「送信」をクリック。



⑧ ワンタイムコードアプリの配下に、登録したデバイス名が表示されます。

⑨ 以上でワンタイムコード認証の設定は完了です。

統合認証にログインする際、ワンタイムコードを使った二要素認証ができるようになりました。

4-4 ワンタイムコードの設定方法（PC＋Chromeの場合）

（1）PC の Chrome に「Authenticator」をインストールする

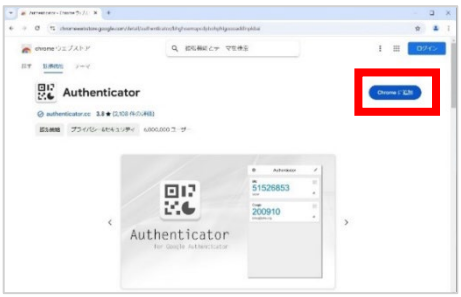
① PC（Windows もしくは macOS）で Chrome を起動し、「Chrome ウェブストア」から「Authenticator」(開発元：authenticator.cc)にアクセスする。

Chrome ウェブストア
https://chromewebstore.google.com/

Authenticator（開発元：authenticator.cc）
https://chromewebstore.google.com/detail/authenticator/bhghoamapcdpbohphigooaddinpkbai

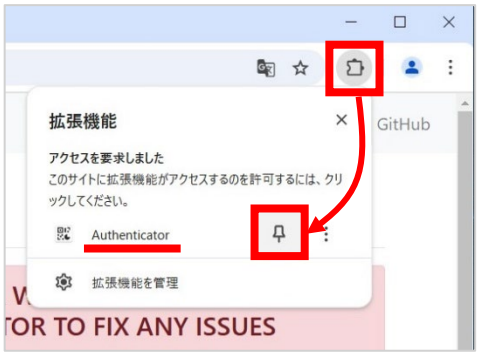
工大メールアドレスで Chrome にログインしている場合、「Chrome ウェブストア」にアクセスできないため、一旦ログアウトしてから「Chrome ウェブストア」にアクセスして下さい。

② 「Chrome に追加」をクリックする。

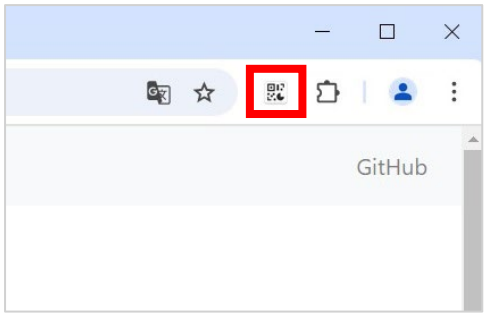


③ 「拡張機能を追加」をクリックする。

④ 赤枠の「拡張機能」アイコン（ ）をクリックし、「Authenticator」をピン留めする。



⑤ ピン留めが完了すると、「Authenticator」のアイコン（ ）が常に表示されます。



（2）「統合認証アカウントコンソール」にログインし、Authenticator を登録する

① Chrome で「統合認証アカウントコンソール」にアクセスする。

統合認証アカウントコンソール

https://sso.chibatech.ac.jp/realms/marine/account/

② MARINE ユーザーID とパスワードを入力して「Sign In」をクリックする。

③ 「統合認証アカウントコンソール」のメニューから、「アカウント・セキュリティ」をクリックし、次に「サインイン」をクリックする。

④ 「二要素認証」の配下にある「ワンタイムコードアプリを設定する」をクリックする。

⑤ QR コードが表示されたら、Chrome の「Authenticator」アイコン（ ）をクリックし、「QR コードをスキャン」アイコン（ ）をクリックする。

⑥ QRコードの部分をドラッグして囲む。

⑦ 「追加されました」と表示されたら、「OK」ボタンをクリック。

「QR コードが認識できません」と表示されることがあります。この場合、一旦、17ページの❶～❺の手順を実施し、その後⑧の手順に戻って下さい。

⑧ 「Authenticator」アイコン（ ）をクリックするとワンタイムコードが表示されるようになっていることを確認する。

※ワンタイムコードは一定時間毎に変わり続けます。

⑨ 「ワンタイムコード」欄に、Authenticator 上に表示された 6 桁のワンタイムコードを入力し、「デバイス名」欄に任意の名称（例：My PC）を入力し、「送信」をクリック。

⑩ ワンタイムコードアプリの下に、登録したデバイス名が表示されます。

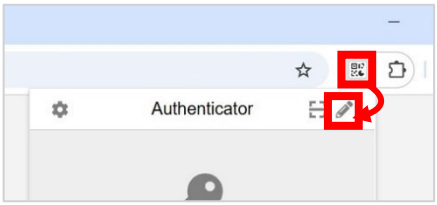
⑪ 以上でワンタイムコード認証の設定は完了です。

統合認証にログインする際、ワンタイムコードを使った二要素認証ができるようになりました。

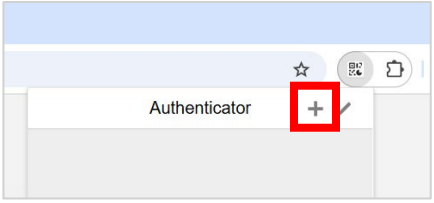
Chrome の Authenticator で QR コード読み取った際に、「QR コードが認識できません」と表示された場合の追加手順

❶ QR コードの下にある「スキャンできませんか？」をクリックすると、「キー」が表示されるので、「キー」をコピーする。

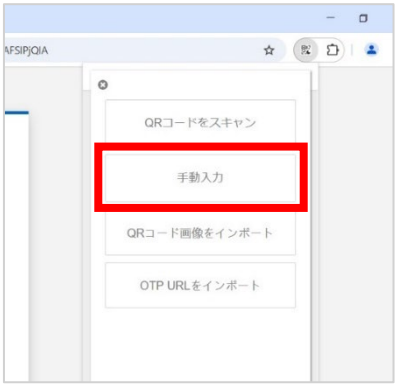
❷ 「Authenticator」アイコン（ ）をクリックし、「編集」アイコン（ ）をクリックする。



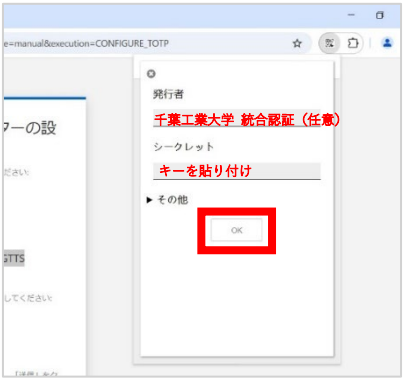
❸ 「アカウントを追加」アイコン（ ）をクリックする。



❹ 「手動入力」をクリックする。



❺ 「発行者」に任意の文字列（例：「千葉工業大学 統合認証」）を入力し、「シークレット」に、❶でコピーしたキーを貼り付け「OK」をクリックする。



前ページの⑧の手順に戻って下さい。

4-5 パスキーの設定方法（スマートフォンの場合）

① パスキーに対応したスマートフォンをご用意する。（OS のバージョンやその他の要件は、5 ページを参照してください。）

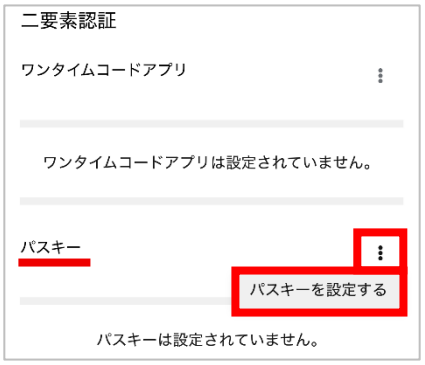
② スマートフォンのブラウザで、「統合認証アカウントコンソール」にアクセスする。

統合認証アカウントコンソール
https://sso.chibatech.ac.jp/realms/marine/account/

③ MARINE ユーザーID とパスワードを入力して「Sign In」をタップする。

④ 「メニューボタン」→「アカウント・セキュリティ」→「サインイン」をタップする。

⑤ 「パスキー」の横にある「⋮」ボタンをクリックし、「パスキーを設定する」をクリックする。



⑥ パスキー登録画面で登録ボタンをクリックする。

⑦ パスキーの保存場所に関する選択肢が表示された場合は、任意の場所を選択します。（デバイスにより選択肢は異なります）

⑧ 登録したパスキーのラベルを入力します。（任意）

⑨ パスキーの配下に登録したパスキーのラベルが表示されます。

⑩ 以上でパスキー認証の設定は完了です。
統合認証にログインする際、パスキーを使った二要素認証ができるようになりました。

4-5 パスキーの設定方法（PCの場合）

① パスキーに対応した PC を用意して下さい。(OS のバージョンやその他の要件は、5 ページを参照してください。)

② PC のブラウザで、「統合認証アカウントコンソール」にアクセスする。

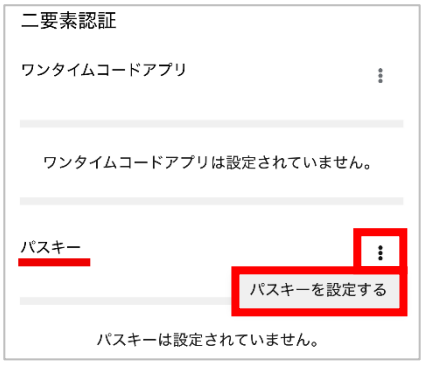
統合認証アカウントコンソール

https://sso.chibatech.ac.jp/realms/marine/account/

③ MARINE ユーザーID とパスワードを入力して「Sign In」をタップする。

④ 「メニューボタン」→「アカウント・セキュリティ」→「サインイン」をタップする。

⑤ 「パスキー」の横にある「⋮」ボタンをクリックし、「パスキーを設定する」をクリックする。



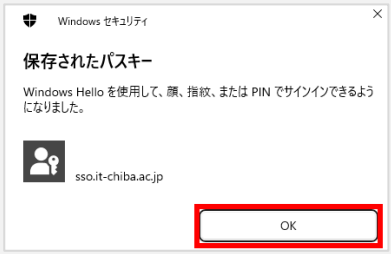
⑥ パスキー登録画面で登録ボタンをクリックする。

⑦ パスキーの保存場所や認証方法の選択肢が表示された場合は、任意の選択をします。

※ デバイスにより選択肢や画面遷移は異なります。

（例）Windows で顔認証を選択する場合

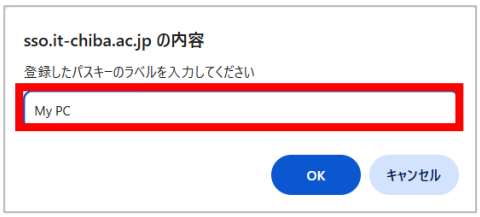
顔認証を行う。



（例）Mac で指紋認証を選択する場合

指紋認証を行う。

⑧ 登録したパスキーのラベルを入力する。（任意）



⑨ パスキー配下に登録したパスキーのラベルが表示されます。

⑩ 以上でパスキー認証の設定は完了です。統合認証にログインする際、パスキーを使った二要素認証ができるようになりました。

4-7 ワンタイムコード・パスキーの設定削除手順

① 統合認証アカウントコンソールにログインします。

統合認証アカウントコンソール
https://sso.chibatech.ac.jp/realms/marine/account

② メニュー欄の「アカウント・セキュリティ」から「サインイン」を選択します。

③ 「ワンタイムコード」と「パスキー」の配下に登録済みのラベル名が表示されますので、削除したい項目の右側にある「削除」ボタンをおします。

④ 確認メッセージが表示されたら、「削除の確認」を選択します。

⑤ 以上で、「ワンタイムコード」もしくは「パスキー」の設定情報の削除は完了です。

4-8 第2要素目の認証で、認証方式を切り替える方法

第２要素目の認証でワンタイムコードとパスキーの両方が設定済みの場合、先に設定した認証方式が優先的に表示されます。表示された認証方式とは異なる認証方式を選択したい場合は、「別の方法を試す」をクリックし、任意の認証方式を選択してください。

① この例では、第２要素目の認証をする際に、パスキー認証が優先的に表示された。

② ワンタイムコードで認証したい場合は、「別の認証方法を試す」をクリックし、ログイン方法選択画面で「ワンタイムコードアプリケーション」を選択する。

4-9 第2要素目の認証で、優先的に表示される認証方式を変更する方法

第２要素目の認証でワンタイムコードとパスキーの両方が設定済みの場合、先に設定した認証方式が優先的に表示されます。登録の順序を調整することで、優先的に表示される認証方式を変更することができます。

例えば、先にワンタイムコードを登録し、その後パスキーを登録した場合は、ワンタイムコードが優先的に表示されます。パスキーが優先的に表示されるように変更したい場合、一旦ワンタイムコードの設定を削除し、その後ワンタイムコードを再設定することにより、パスキーを優先的に表示させることができます。

5. 統合認証のログアウト

5-1 統合認証からログアウトする方法

ブラウザを全て閉じることで統合認証からログアウトされます。ただし、「ログイン状態の保存」にチェックを入れた状態でログインした場合は、ブラウザを閉じても一定期間統合認証へのログイン状態が保持されるため、次回ブラウザを起動した際に自動的に統合認証にログインされた状態になることがあります。

このような状態で統合認証から確実にログアウトしたい場合は、「統合認証アカウントコンソール」にアクセスし、画面右上のアカウント名をクリックして「サインアウト」を選択してください。

統合認証アカウントコンソール
https://sso.chibatech.ac.jp/realms/marine/account

6. Q&A

Q1 デバイスの故障・紛失等により二要素認証ができなくなりました。

デバイスの故障・紛失等の理由により二要素認証ができなくなった場合、統合認証システム管理者（情報システム担当）で二要素認証の登録（ワンタイムコード・パスキーの登録）をクリアすることが可能です。

二要素認証の登録をクリアするためには、必ず本人確認が必要となりますので、情報システム担当窓口で学生証を提示してください。

情報システム担当
場所：津田沼キャンパス 1 号館 2 階
電話：047-478-0227
E メール：i-staff@chibatech.ac.jp

Q2 携帯電話の機種変更の際に注意すべきことはありますか。

二要素認証に使用していたデバイスが使えなくなることにより、アカウントコンソール（https://sso.chibatech.ac.jp/realms/marine/account）へログインできなくなることを避ける必要があります。

既に二要素認証が登録されている場合、各サービスへのログインだけでなく、アカウントコンソールへのログイン時にも必ず二要素認証が求められます。機種変更によりデバイスが変わると、二要素認証ができなくなる可能性があり、その場合はアカウントコンソールへログインできないため、二要素認証の登録削除や新規登録の操作が行えなくなります。

このような状況を回避するためには、以下の何れかの方法を推奨いたします。

1. 機種変更する携帯電話以外のデバイス（タブレットや PC など）でも二要素認証ができるようにあらかじめ設定しておく。
2. 機種変更前の携帯電話が操作可能なうちにアカウントコンソールにログインし、いったん二要素認証の設定を削除してから機種変更を行い、その後、新しい端末で二要素認証を新たに設定する。

なお、二要素認証の設定が機種変更後の端末に引き継がれる場合もありますが、機種やアプリ等の仕様により異なるため、必ずしも引き継がれるとは限りませんのでご注意ください。

Q3 アプリ版のMicrosoft 365 にパスキー認証でサインインできません。

アプリ版の Microsoft 365 は、内蔵ブラウザがパスキーに対応していないことにより、パスキー認証を利用したサインインができません。

パスキー認証ができないことにより、アプリ版 Microsoft 365 へサインインできない場合は、統合認証アカウントコンソールでパスキーの設定を一旦削除してからアプリ版 Microsoft 365 へサインインして下さい。

（「4 - 7　ワンタイムコード・パスキーの設定削除手順」参照）

なお、ワンタイムコード認証は、アプリ版 Microsoft 365 へサインインする際にもお使いいただけます。

また、アプリ版ではなく、Web 版の Microsoft 365 はパスキー認証に対応したブラウザ（Google Chrome・Safari・Microsoft Edge）を使えば、パスキー認証でサインインすることが可能です。

Q4「無効なワンタイムコードです」と表示されます。

ワンタイムコードによる二要素認証を行う際、ワンタイムコードアプリに表示された 6 桁のコードを入力しても「無効なワンタイムコードです。」と表示されることがあります。

端末の時刻がずれていることが原因となっている可能性がありますので、ワンタイムコードアプリをインストールした端末（スマートフォンや PC 等）の時刻がずれていないか確認し、ずれている場合は修正してください。