

Multi-factor authentication system How to access using VPN

2022/3/24



国立大学法人

滋賀医科大学

SHIGA UNIVERSITY OF MEDICAL SCIENCE

Overall flow

1. Access the VPN service from university's homepage.
3. Login the VPN service and select the Multi-factor authentication page.
3. Select any authentication registration page from the Multi-factor authentication page.

FIDO authentication setting can not be done from VPN.

1. Access the VPN service from university's homepage.

Faculty and staff



Students



2-1. Enter ID and password of campus mail and log in.

 滋賀医科大学
VPNサービス

Welcome to
Secure Access SSL VPN
This service is available only from outside SUMS

Username
Password

Please sign in to begin your secure session.
ユーザIDとパスワードを入力して「Sign In」ボタンをクリックしてください。
※IDとパスワードは利用者を識別するための大切な情報です。自分以外の人も使用するPCやブラウザに保存するようなことはせず、厳重に管理してください。

- ・ユーザID：メールアドレスの@より前の部分
- ・パスワード：メールのパスワード

「情報セキュリティe-learning」未修了の場合は、ログインできなくなる可能性がありますので、ご注意ください。
実施要項につきましては、[こちら](#)をご確認ください。（※毎年修了必要）

VPNサービスは、**学外から**の利用に限定しています。
学内からはサインインできませんのでご注意ください。

ID and password of campus mail.

2-2 Select the “Multi-factor authentication” from the VPN service menu.

The screenshot shows a web browser window with the URL `sumsvnet.shiga-med.ac.jp/dana/home/index.cgi`. The page header includes the Shiga University of Medical Science logo and the text 'VPNサービス'. A navigation bar contains 'Logged-in as:', 'ホーム', 'プリファレンス', and 'ログアウト'. The main content area is titled 'Welcome to the Secure Access SSL VPN,' and features a 'Web ブックマーク' section with the following items:

- Virus Scan**: ウィルス駆除ソフトのダウンロード
- SUMS Library**: オンラインジャーナル・データベース
- SUMS e-Learning WebClass 過年度コース**: 過年度のコースを参照できます。
- 学生用WEBサービス**: 学生用教務情報
- 日経BP記事検索サービス**: 日経BP社が発行する約40誌（日経メディカル、日経パソコン等）のバックナンバー記事をオンライン上で検索・閲覧できるサービス
- まるっと滋賀医大**: 学内コンテンツポータルサイト
- メールパスワード変更**: 本学メールアドレスに対するパスワード変更
- 隔離メール確認**: スпамメール隔離サーバに隔離されたメール
- CT-portal**: 利益相反管理・申請システム
- 多要素認証**: e-learningシステム(WebClass)、Webメール(Active!mail)で多要素認証が可能

An orange callout bubble points to the '多要素認証' item, containing the text: 'Select “多要素認証” (Multi-Factor authentication)'. The '多要素認証' item is also enclosed in a red rectangular box.

3. Select any authentication registration page from Multi-factor authentication page.

■ 多要素認証システムとは

学外からWebMail/WebClass 利用時に通常の ID、パスワードのほかに追加の認証を行うものです。
少なくとも1つの認証方式で多要素認証を登録してください。

☞ [多要素認証システム概要\(PDF\)](#)

認証方式	説明	利用デバイス
TOTP認証(ワンタイムパスワード)	スマートフォン/タブレットのアプリからワンタイムパスワードが発行され、そのコードを入力して認証する	PC スマートフォン
FIDO認証	多要素認証システムに自分のスマートフォン/タブレットを登録し、端末の指紋認証や顔認証を利用する	スマートフォン
イメージングマトリクス認証	毎回ランダムな並びで画像が表示されるので、事前に自分で決めた画像を順番に選択する *hgアドレスなど個人のメールアドレス以外はこちらをお使いください。	PC

詳細は下記項目をクリックしてご確認ください。(図はクリックで拡大します。)

▶ [TOTP認証\(ワンタイムパスワード\)とは](#)

▶ [FIDO認証とは](#)

▶ [イメージングマトリクス認証とは](#)

▲ [このページのトップへ](#)

■ 多要素認証システム認証設定方法(学内またはVPNからアクセス下さい)

※VPNからのアクセス方法については以下をご参照ください。

☞ [認証設定画面へのVPNからのアクセス方法](#)

1. **TOTP認証(ワンタイムパスワード認証):**設定にPCまたはスマートフォン/タブレットが必要

- [TOTP認証\(ワンタイムパスワード認証\)設定ページ](#)
- [ワンタイムパスワード認証手順\(スマートフォン\)\(PDF\)](#)
- [ワンタイムパスワード認証手順\(PC\)\(PDF\)](#)

2. **FIDO認証:**設定に【生体認証設定をしている※】スマートフォンまたはタブレットが必要

※使用するスマートフォンやタブレットが指紋認証や顔認証などで開く設定をしている必要があります。パスワード・パターンによる認証設定のみでは使用できません。

- [FIDO認証設定ページ](#)
- [FIDO認証手順\(PDF\)](#)

3. **イメージングマトリクス認証:**設定にPCが必要

- [イメージングマトリクス認証設定ページ](#)
- [イメージングマトリクス認証手順\(PDF\)](#)

FIDO authentication setting can not be done from VPN.