

利用者用

多要素認証設定マニュアル

-共有アカウントの設定-

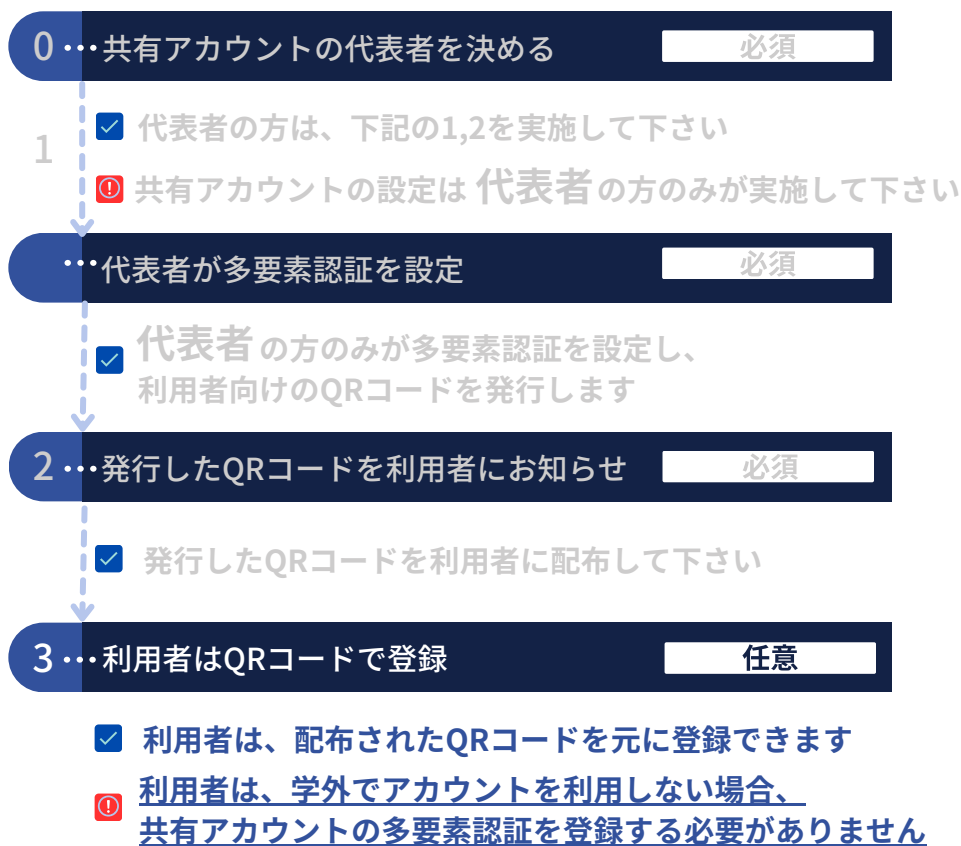
はじめに

本マニュアルは、複数人で使用しているアカウント（共有アカウント）に対する多要素認証の利用者用設定マニュアルです。

代表者が設定を行っていることが前提となりますのでご注意ください。

**共有アカウントを学外ネットワークで利用しない場合、
本設定を実施する必要はありません。**

共有アカウントの多要素認証設定における全体の流れ



目次

1 認証端末とQRコードの準備

2 QRコードの読み取り

3 ログイン方法

利用者用

多要素認証設定マニュアル -共有アカウントの設定-

1 認証端末とQRコードの準備

下記二点をお手元にご準備ください。

- ・代表者より配布されたQRコード
- ・ご自身の個人アカウントで多要素認証を設定した端末（スマートフォンorパソコン）

※スマートフォン以外の携帯電話をお使いの方は、パソコンで設定が必要です。

下記リンクより「1. 事前準備」を設定してください。

<https://ict.kanto-gakuin.ac.jp/browser/>

2 QRコードの読み取り

<スマートフォンをご利用の場合>

下記の赤枠に沿って、タップをしてください。

QRコードをスキャンする際は、配布されたQRコードを読み込んでください。

アプリのトップに共有アカウントが追加されれば完了です。

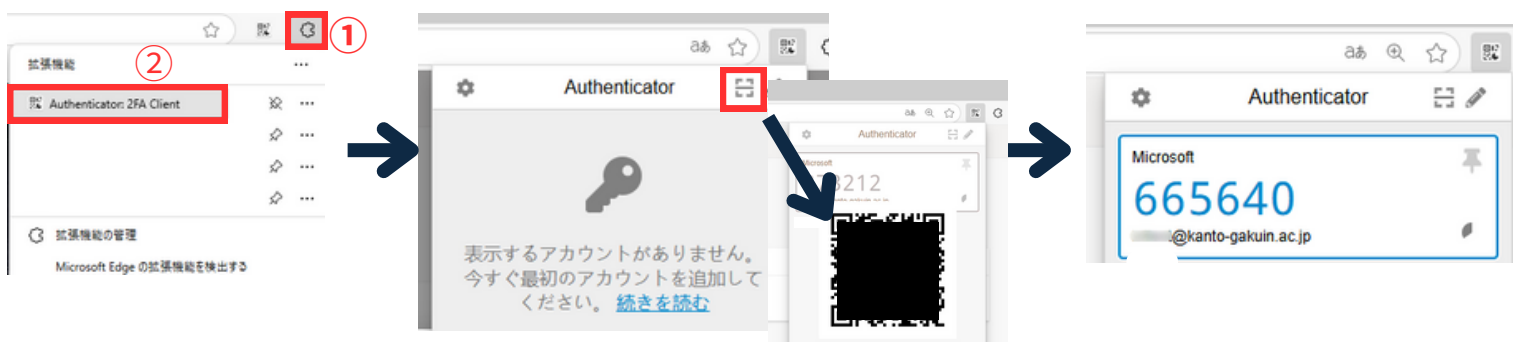


<パソコンをご利用の場合>

ブラウザの拡張機能より、Authenticatorアプリを起動し、赤枠部分をクリックしてください。

QRコードをスキャンする際は、配布されたQRコードを読み込んでください。

一覧に共有アカウントが追加されれば完了です。



多要素認証設定マニュアル

-共有アカウントの設定-

3 ログイン方法

<スマートフォンをご利用の場合>

認証時に、下記のように「コードの入力」画面が表示されます。

Authenticatorアプリを起動し、共有アカウントに表示されている6桁の番号を入力してください。

※コードの有効期限は30秒です。



<パソコンをご利用の場合>

ブラウザの拡張機能より、Authenticatorアプリを起動し、赤枠部分をクリックしてください。

QRコードをスキャンする際は、配布されたQRコードを読み込んでください。

一覧に共有アカウントが追加されれば完了です。

