

多要素認証システム ワンタイムパスワード(TOTP)認証 (Mac - OTP Manager)

2024/9/27



国立大学法人

滋賀医科大学

SHIGA UNIVERSITY OF MEDICAL SCIENCE

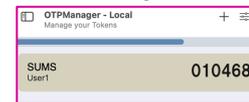
はじめに

1. 多要素認証システムは「**学外から**」GmailやVPNにアクセスするに際し、必要になるものです。

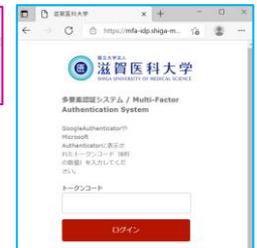
▶ 詳細は[多要素認証システム概要\(PDF\)](#)をご参照ください。

2. 本作業はアプリOTP Managerを使用したTOTP認証（多要素認証システムの1つ）の初期設定になります。

OTP Managerの画面



TOTPログイン画面



3. 本作業ではPCを使用します。設定にはPCの時刻が正確である必要があります。

4. 初期設定は学内からのみ実施可能です。有線LANまたは無線LAN「sums-wireless」に接続して操作してください。

※初期設定後は、学外からVPNを通して設定変更できます。

▶ VPNのアクセス方法は[認証設定画面へのVPNからのアクセス方法](#)をご参照下さい。

- ◆ 携帯やPC等複数台に設定する場合は、下記マニュアルもあわせてご参照ください。

▶ [\(補足\)複数の端末を登録する方法\(PDF\)](#)

※学外のPCに設定する際も、TOTP認証設定が完了している機器が1台は必要です。

目次

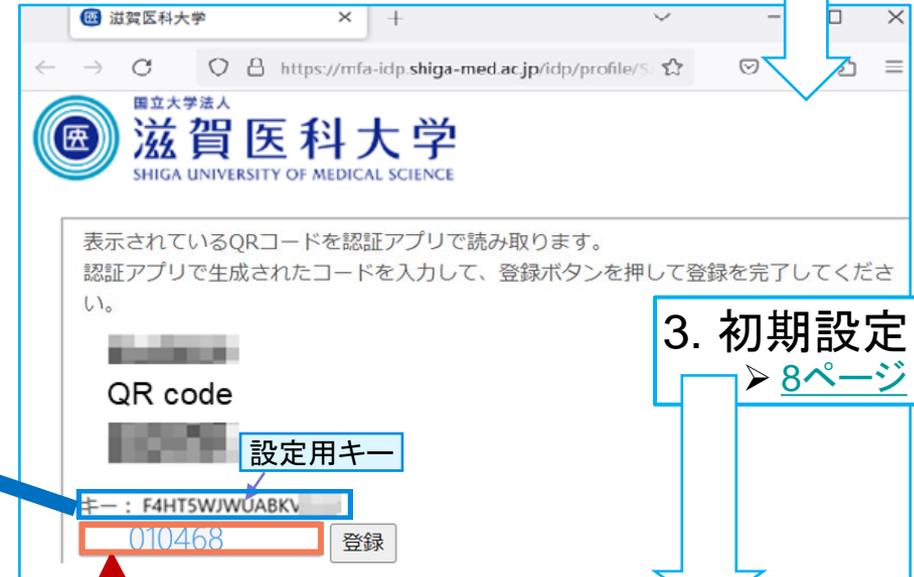
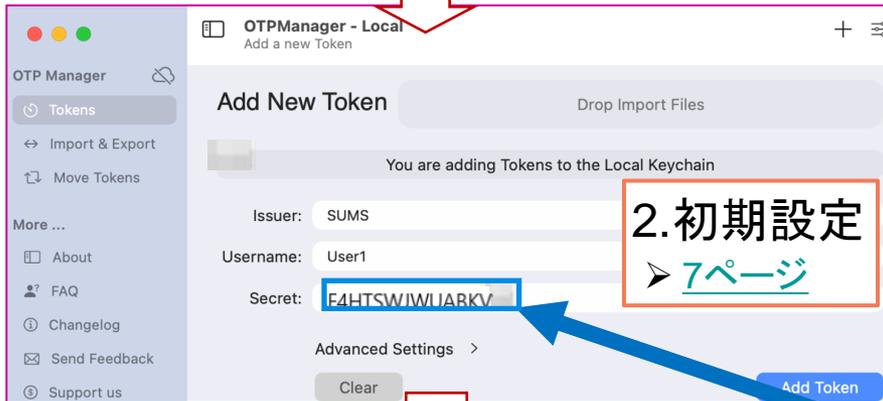
1. ワンタイムパスワード (TOTP) 認証の初期設定		4ページ												
<table border="1"> <tr> <td colspan="2">全体の流れ</td> <td>4ページ</td> </tr> <tr> <td>1-1</td> <td>OTP Managerの導入</td> <td>5ページ</td> </tr> <tr> <td>1-2</td> <td>OTP Managerの初期設定</td> <td>7ページ</td> </tr> <tr> <td>1-3</td> <td>TOTP認証の初期設定</td> <td>8ページ</td> </tr> </table>		全体の流れ		4ページ	1-1	OTP Managerの導入	5ページ	1-2	OTP Managerの初期設定	7ページ	1-3	TOTP認証の初期設定	8ページ	
全体の流れ		4ページ												
1-1	OTP Managerの導入	5ページ												
1-2	OTP Managerの初期設定	7ページ												
1-3	TOTP認証の初期設定	8ページ												
2. 初期設定後の利用方法 ~学外からGmail/VPNへのログイン方法		9ページ												
3. OTP Managerのバックアップ&復元方法		11ページ												
<table border="1"> <tr> <td colspan="2">設定済の端末での処理(バックアップ)</td> <td>11ページ</td> </tr> <tr> <td colspan="2">未設定の端末での処理(復元)</td> <td>13ページ</td> </tr> </table>		設定済の端末での処理(バックアップ)		11ページ	未設定の端末での処理(復元)		13ページ							
設定済の端末での処理(バックアップ)		11ページ												
未設定の端末での処理(復元)		13ページ												

1. ワンタイムパスワード (TOTP) 認証の初期設定

■ 全体の流れ

1. OTP Manager  をインストール [▶ 5ページ](#)

(Web) 多要素認証システムの TOTP 認証設定ページ [▶ 5ページ](#)



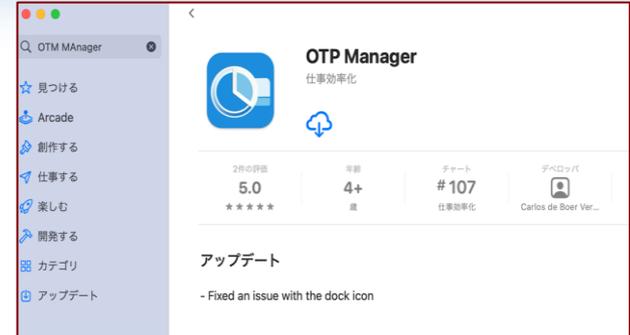
ポイント

OTP Manager 初期設定 → TOTP 認証設定ページの 設定用キー を入力

TOTP 認証設定ページの 初期設定 → OTP Manager の ワンタイムパスワード (トークンコード) を入力

1-1. OTP Managerの導入

Apple StoreからOTP Managerをインストールします。



PCからTOTP認証の設定ページにアクセス

最初にTOTP認証の設定ページを表示するには多要素認証システムにアクセスします。

Step1

1)多要素要素システムにアクセスします。

▶ 多要素認証システムのページ
(<https://mfa-idp.shiga-med.ac.jp/wptotp/>)

注意

- ・PCで設定してください。
- ・学内有線LANまたは無線LAN「sums-wireless」に接続して操作してください。

2)ユーザー情報を入力し、
ログイン します。

Step2

OTP Managerの初期設定時で読み取るQRコードや設定用キーが表示されます。



ポイント 後日、携帯等複数の端末で多要素認証システムを使用する場合

TOTP認証の設定ページに表示された同じQRコードまたは設定用キーをPCや携帯等各端末に読み込ませることで全ての端末で同じワンタイムパスワードが表示されます。

例)最初にOTP ManagerでTOTP認証設定を行った後の場合

初期設定時に使用したQRコード/シークレットキーを印刷/保管しておくことを推奨します。

同じQRコードスキャン

同じ設定用キー入力

ご自身のQRコード

キー入力

入力

登録

注意 最初に1つの端末で多要素認証の設定を完了させてください。その後、印刷/保管されたQRコードおよびキーを他の端末に読み込ませてください。 ➤ [\(補足\)複数の端末を登録する方法\(PDF\)](#)

Microsoft Authenticator

Google Authenticator

スマートフォン/タブレット向けアプリ

PC向けアプリ

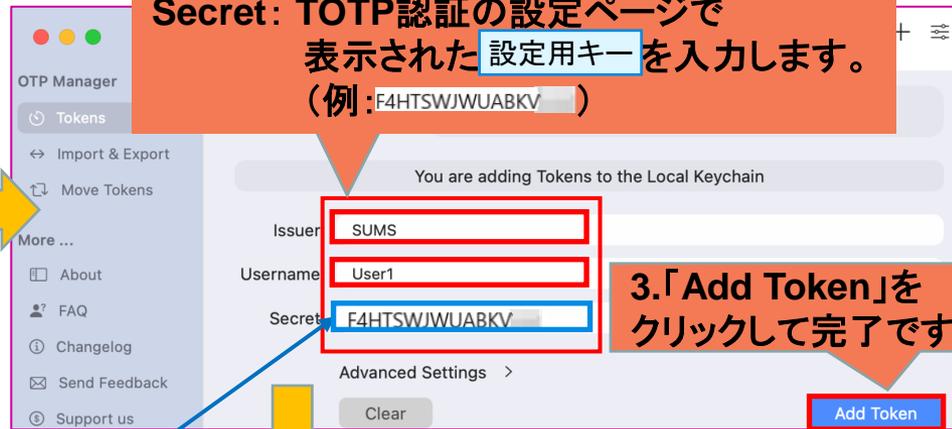
OTP Manager

1-2. OTP Managerの初期設定

OTP Managerを起動します。TOTP認証の設定ページで表示された**設定用キー**など必要事項を入力し、登録します。

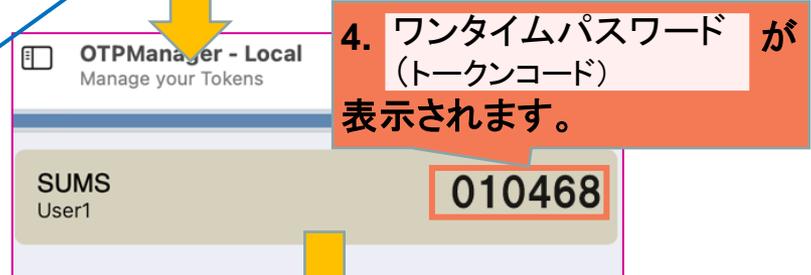


2. 下記の項目を入力します。
issuer: 任意の文字列 (例:SUMS)
Username : 任意の文字列 (例:ユーザID)
Secret: TOTP認証の設定ページで表示された**設定用キー**を入力します。
 (例: F4HTSWJWUABKV)



TOTP認証の設定ページ

➤ [詳細は5ページ参照](#)



TOTP認証設定やVPNへのアクセス時に左記の**ワンタイムパスワード**を使います。
 (トークンコード) ➤ [11ページへ](#)

1-3. TOTP認証設定

OTP Managerで表示された6桁の認証コード(トークンコード)をTOTP認証設定ページに入力し、登録します。

注意

- 本手順を行わないと、ワンタイムパスワードは機能しません。
- 多要素認証のページのみ初期設定の場合、学内LANに接続してください。

OTP Manager

※認証コードは**30秒**毎に新しいパスワード(ワンタイムパスワード)を発行します。



TOTP認証の設定ページ



多要素認証システム / Multi-Factor Authentication System

表示されているQRコードを認証アプリで読み取ります。
認証アプリで生成されたコードを入力して、登録ボタンを押して登録を完了してください。

1. 生成されたワンタイムパスワード(トークンコード)を入力します。



2. 「登録」を実行します。

注意

Enterキーを押すだけでは登録完了しません。
登録をクリックしてください。



3. 処理が完了します。

2. 初期設定後の利用方法 ~学外からGmail/VPNへのログイン方法

Gmail/VPNへのアクセス時に多要素認証の画面が表示された場合、以下の手順を実施して下さい。

Step1

国立大学法人
滋賀医科大学
SHIGA UNIVERSITY OF MEDICAL SCIENCE

多要素認証システム / Multi-Factor Authentication System

ユーザ名

パスワード

ログインを記憶しません

送信する情報を再度表示して送信の可否を選択します。

ログイン

パスワードをお忘れの方はこちら

1-1.学内メールのID、パスワードを入力します。

1-2.ログインをクリックします。

Step2

国立大学法人
滋賀医科大学
SHIGA UNIVERSITY OF MEDICAL SCIENCE

多要素認証システム / Multi-Factor Authentication System

認証方式を選択してください

FIDO or イメージングマトリクス

ワンタイムパスワード(TOTP)

2.「ワンタイムパスワード(TOTP)」を選択します。

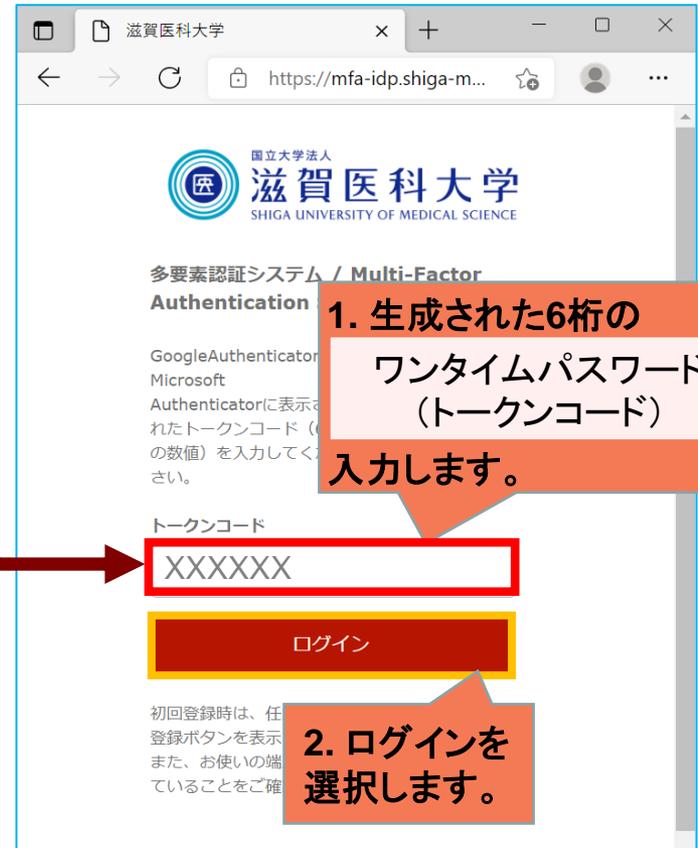
OTP Managerを起動します。トークンコードにOTP Managerで表示される
ワンタイムパスワード
(トークンコード)

OTP Manager

※認証コードは**30秒毎**に新しいパスワード
(ワンタイムパスワード)を発行します。



起動

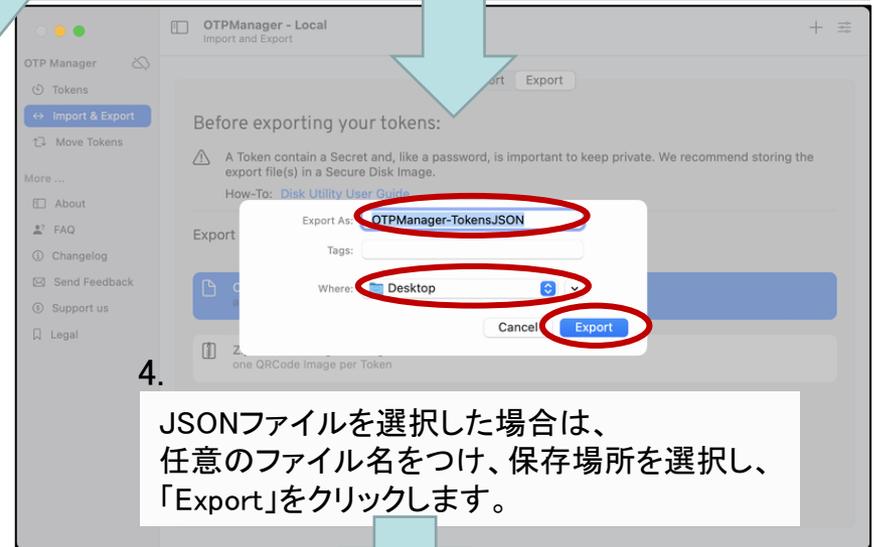
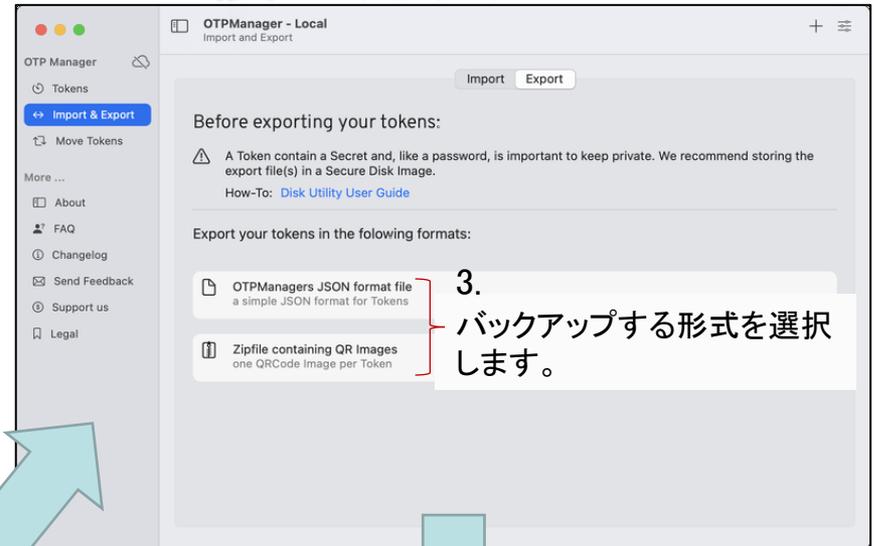
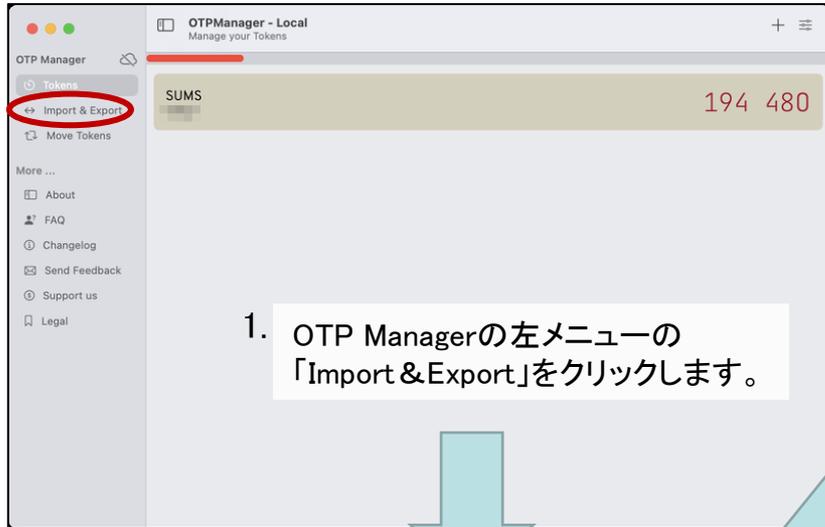


1. 生成された6桁の
ワンタイムパスワード
(トークンコード)
を入力します。

2. ログインを
選択します。

3. OTP Managerのバックアップ & 復元方法

設定済の端末での処理(バックアップ)



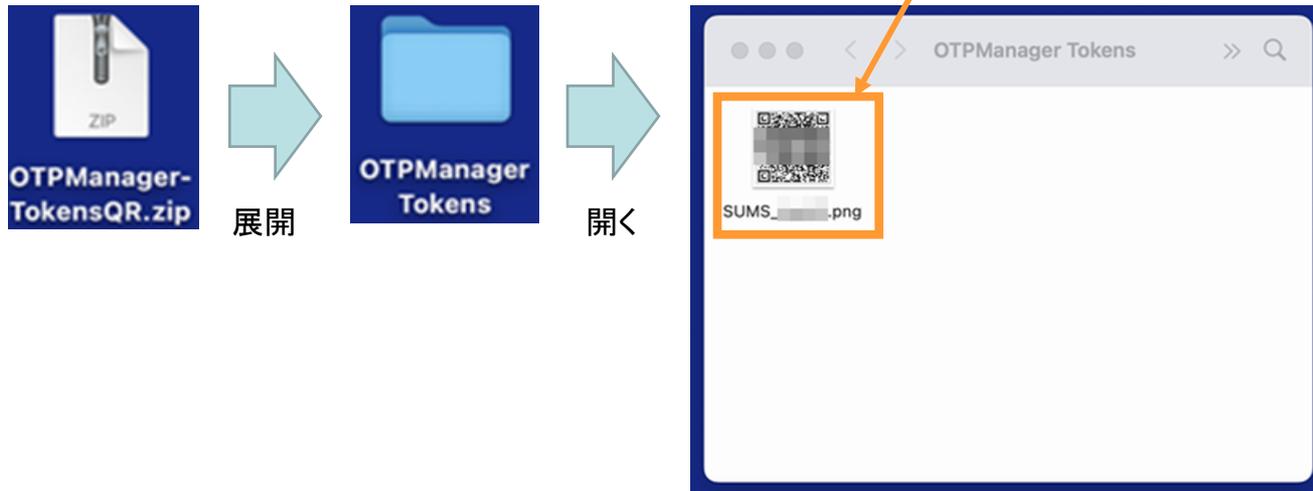
5. JSONファイルまたはQRコード(Zipファイル)がダウンロードされます。



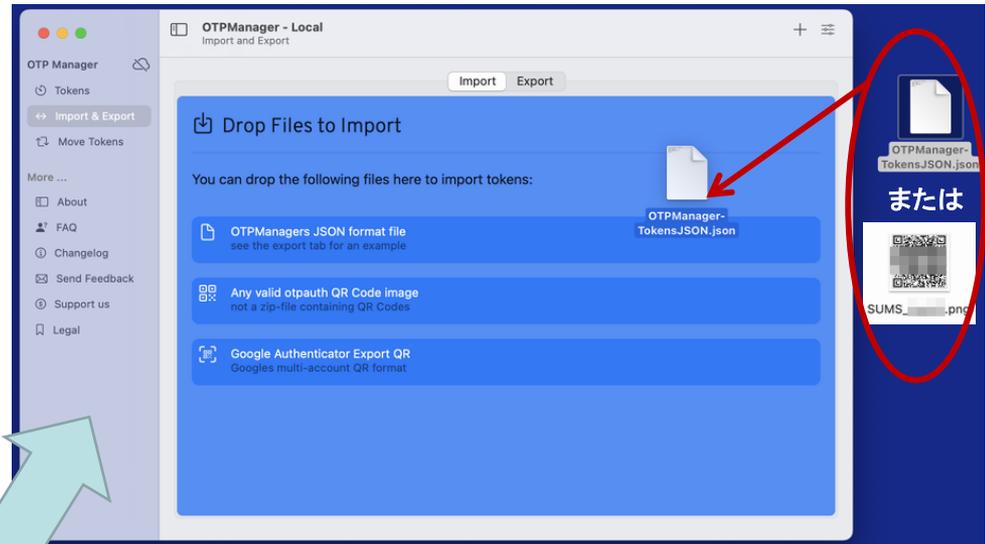
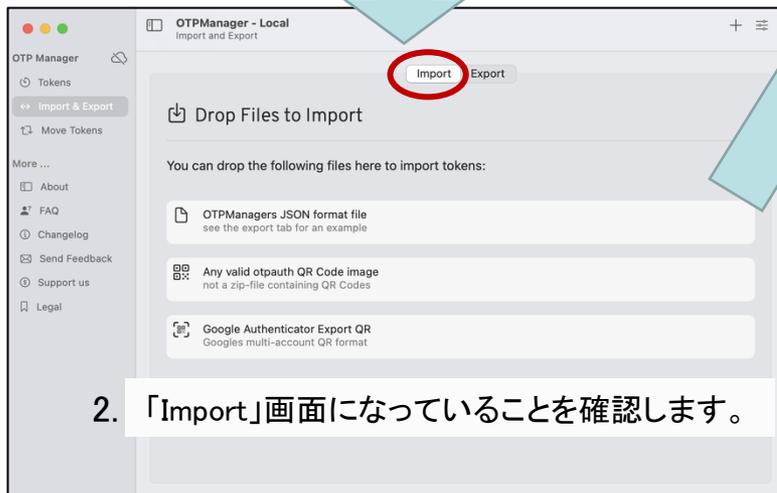
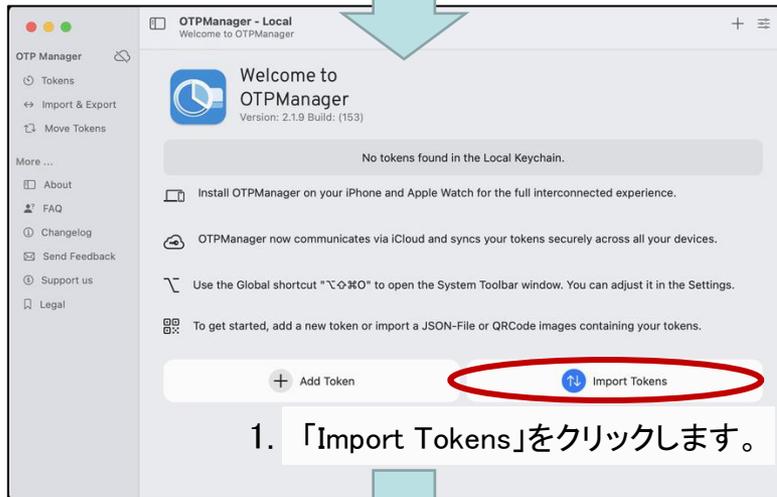
6. ドライブ等を使用して、新しく設定(復元)するPCへバックアップ設定ファイル(OTPManager-TokensJSON.json または OTPManager-TokensQR.zip)を移動します。

ポイント

※QRコードを指定した場合は、展開してお使いください。



未設定の端末での処理(復元)



3. 12ページの手順6.で移動したバックアップ設定ファイル (OTPManger-TokensJSON.json または OTPManger-TokensQR.zip)をドラッグアンドドロップします。

ポイント

※QRコードを指定した場合は、展開してお使いください。

➤ 12ページ参照

