

Microsoft Azure MFA（多要素認証）設定手順 （QR Code OTP c610）



「QR Code OTP c610（以下、OTP c610 と言う）」は Web サービス提供者が発行する QR コードをスキャンし、ユーザーアカウントと紐づけ、MFA（多要素認証）用ワンタイムパスワードの生成を可能にする OTP トークンです。

従来の OTP トークンと異なり、「OTP c610」は内蔵カメラを備え、『Microsoft Authenticator』『Google Authenticator』等、スマホアプリの代わりに、MFA プロセスの認証コード（数字 6 桁のパスワード）を生成する認証器（Authenticator）です。

本資料は Microsoft Azure ユーザーが「OTP c610」を設定し MFA を実現する方法を説明します。

【目次】

1. OTP c610 の概要	3
1.1. 各部の名称及び機能.....	3
1.2. 重要な注意事項.....	3
2. 事前準備	3
2.1. 準備 1 : Microsoft Azure ユーザー.....	3
2.2. 準備 2 : OTP c610 トークン.....	4
3. OTP c610 を利用して AzureAD へログインする方法 (ユーザー)	4
3.1. 初期設定 : OTP c610 の登録 (初回のみ)	4
方法 1 : 「Azure Portal」にアクセスして OTP c610 を登録.....	4
方法 2 : 「マイアカウント」にアクセスして OTP c610 を登録.....	10
3.2. OTP c610 を利用して AzureAD にログインする方法.....	12
4. OTP c610 を利用しない場合 (バインドの解除)	14
4.1. ユーザー自身で解除する方法.....	14
Step1 : 「マイアカウント」の「セキュリティ情報」より「認証アプリ」を削除.....	14
Step2 : OTP c610 の登録情報を削除.....	15
4.2. 管理者側で強制解除する方法.....	16
5. 運用方法	17
5.1. ユーザーが OTP c610 を紛失した場合	17
Step1: [管理者] 紛失した OTP c610 の強制削除.....	17
Step2: [管理者] ユーザーに新たな OTP c610 を配布、「多要素認証の再登録」を設定	17
Step3: [ユーザー] 新しい OTP c610 の登録.....	17
5.2. OTP c610 に時刻ズレが発生し、急に認証できなくなる場合.....	18

1. OTP c610 の概要

1.1. 各部の名称及び機能



1.2. 重要な注意事項

- 1、OTP c610 の液晶画面はタッチパネルではないため、画面の下に表示されているボタンを押して、操作してください。
- 2、**中央のボタンを3秒長押しすると、起動します。**
画面表示後は、中央のボタンを3秒長押しすると、電源がオフになります。
1分間、無操作状態が続くと電源を自動的にオフになります。
- 3、OTP c610 は、最大3つのアカウントを登録することが可能です。
- 4、同一サービスが発行する認証用QRコードをOTP c610 で複数回読取り登録した場合、**最後の登録のみが有効**となり、先に登録されたアカウントでは認証が不可となります。
- 5、OTP c610 はQRコードを発行するすべてのサービスで利用できるものではありません。
Microsoft MFA、Google MFA、SalesforceMFAとしてご利用ください。

2. 事前準備

下記を事前にご準備ください。

2.1. 準備1：Microsoft Azure ユーザー

Microsoft Azure のユーザーアカウントを準備してください。

2.2. 準備2 : OTP c610 トークン

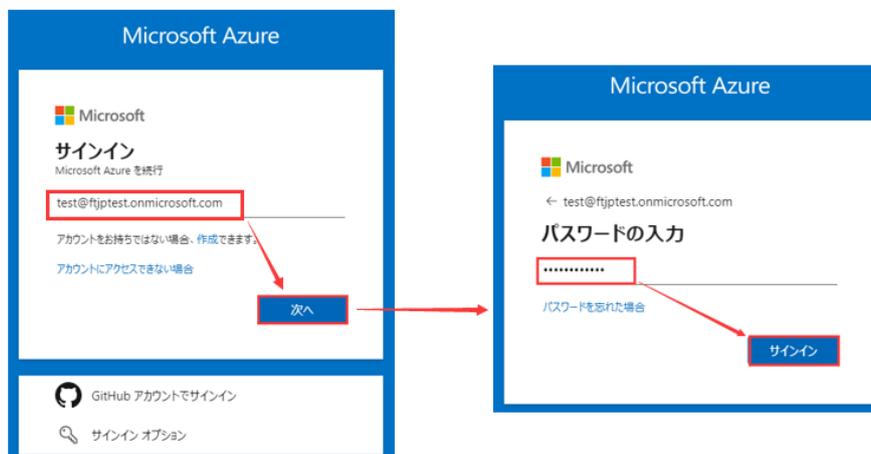
3. OTP c610 を利用して AzureAD へログインする方法（ユーザー）

3.1. 初期設定 : OTP c610 の登録（初回のみ）

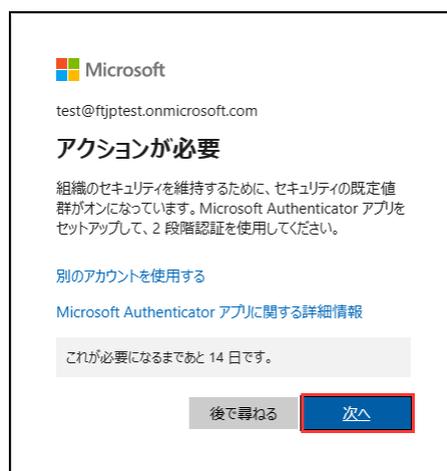
OTP c610を利用して、Microsoft AzureADにログインするため、まずはAzureADユーザーにOTP c610を登録する必要があります。下記では、2つの方法でOTP c610の登録方法を説明します。

方法1 : 「Azure Portal」にアクセスしてOTP c610を登録

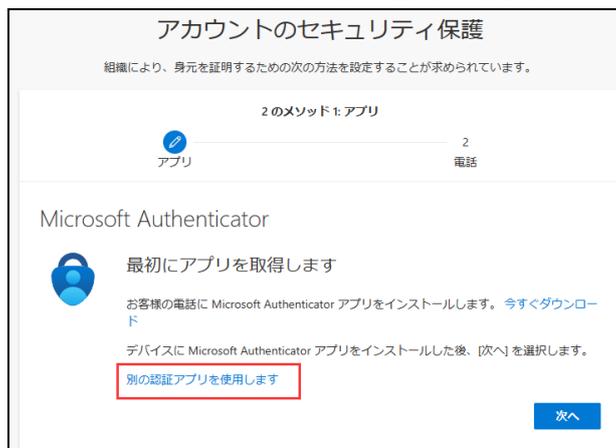
- 1、Azure Portal（<https://portal.azure.com>）にアクセスし、ユーザーアカウント及びパスワードを入力してサインインします。



- 2、MFA（多要素認証）が設定されていない場合は、下記画面が表示されます。
[次へ] をクリックします。



- 3、下記画面にて「別の認証アプリを使用します」のリンクをクリックします。



- 4、 [次へ] をクリックします。



- 5、QRコードのスキャン画面が表示されます。

OTP c610 でスキャンの準備をするため、以下の画面は表示したままの状態にしてください。



- 6、OTP c610 の中央のボタンを 3 秒長押しすると、起動します。
未登録の場合、画面に [+] のみが表示されます。



- 7、[登録] に対応する中央のボタンを押すと、右の画面に遷移します。
[次へ] に対応する中央のボタンを押します。
※前画面に戻る場合は、[戻る] に対応する左のボタンを押してください。



- 8、PC の画面に表示された QR コードに OTP c610 をかざして読取ります。
QR コードを読取り後、OTP c610 にアカウント情報（メールアドレス）が登録されます。



- 9、[選択]ボタンに対応している中央のボタンを押すと、生成されたワンタイムパスワード（6桁の数字）が表示されます。



- 10、PC 画面の [次へ] をクリックします。



- 11、コードの入力画面が表示されます。

OTP c610 の画面に表示された 6 桁のコードを入力し、[次へ] をクリックします。



- 12、本人確認のため、携帯ショートメール（SMS）によるコード認証を行います。
 携帯の電話番号を入力して、[次へ] をクリックします。

The screenshot shows the 'アカウントのセキュリティ保護' (Account Security Protection) screen. At the top, it says '組織により、身元を証明するための次の方法を設定することが求められています。' (Due to the organization, you are required to set the following method to verify your identity). Below this, it indicates '2 のメソッド 2: 電話' (2 methods, 2: Phone). There are two options: 'アプリ' (App) with a green checkmark and '電話' (Phone) with a blue pencil icon. The '電話' section is active and contains the text: '携帯ショートメール (SMS) によるコードの送信により、本人確認ができます。' (You can verify your identity by sending a code via mobile short message (SMS)). It asks 'どの電話番号を使用しますか?' (Which phone number do you want to use?). There is a dropdown menu showing 'Japan (+81)' and a text input field with '090'. Below this, there is a radio button selected for 'コードを SMS 送信する' (Send code via SMS). A red arrow points from the '次へ' (Next) button to the text '次に同意したことになります。' (By clicking Next, you agree to the following terms: Service Usage Conditions, Privacy Policy, and Cookie Policy). At the bottom left, there is a link '別の方法を設定します' (Set a different method).

- ※携帯電話のショートメール（SMS）ではなく、メールアドレスで本人認証する場合は、上記画面の左下 [別の方法を設定します] をクリックしてください。
 メールで本人認証する場合も同様の進め方になります。

- 13、ショートメール（SMS）に記載された認証コードを入力して、[次へ] をクリックします。

The screenshot shows the 'アカウントのセキュリティ保護' (Account Security Protection) screen. It says '組織により、身元を証明するための次の方法を設定することが求められています。' (Due to the organization, you are required to set the following method to verify your identity). Below this, it indicates '2 のメソッド 2: 電話' (2 methods, 2: Phone). There are two options: 'アプリ' (App) with a green checkmark and '電話' (Phone) with a blue pencil icon. The '電話' section is active and contains the text: '+81 090-... に 6 桁のコードをお送りしました。コードを以下に入力してください。' (We have sent you a 6-digit code to +81 090-... Please enter the code below). There is a text input field containing '778089'. Below this, there is a link 'コードの再送信' (Resend code). A red arrow points from the '次へ' (Next) button to the text '次に同意したことになります。' (By clicking Next, you agree to the following terms: Service Usage Conditions, Privacy Policy, and Cookie Policy). At the bottom left, there is a link '別の方法を設定します' (Set a different method).

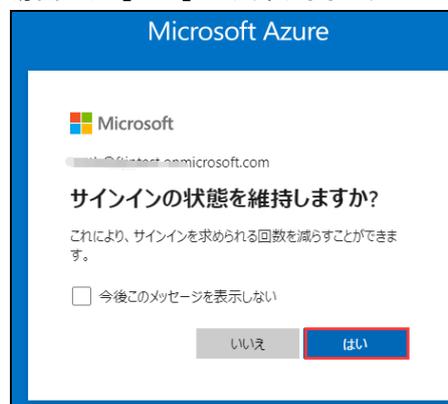
- 14、正しく検証されると、下記の画面が表示されます。[次へ] をクリックします。

The screenshot shows the 'アカウントのセキュリティ保護' (Account Security Protection) screen. It says '組織により、身元を証明するための次の方法を設定することが求められています。' (Due to the organization, you are required to set the following method to verify your identity). Below this, it indicates '2 のメソッド 2: 電話' (2 methods, 2: Phone). There are two options: 'アプリ' (App) with a green checkmark and '電話' (Phone) with a blue pencil icon. The '電話' section is active and contains the text: 'SMS が検証されました。お使いの電話が正常に登録されました。' (SMS verification was successful. Your phone has been registered normally). At the bottom right, there is a blue '次へ' (Next) button.

15、[完了] をクリックし、登録を完了します。



16、サインイン状態を維持する場合は、[はい] をクリックします。

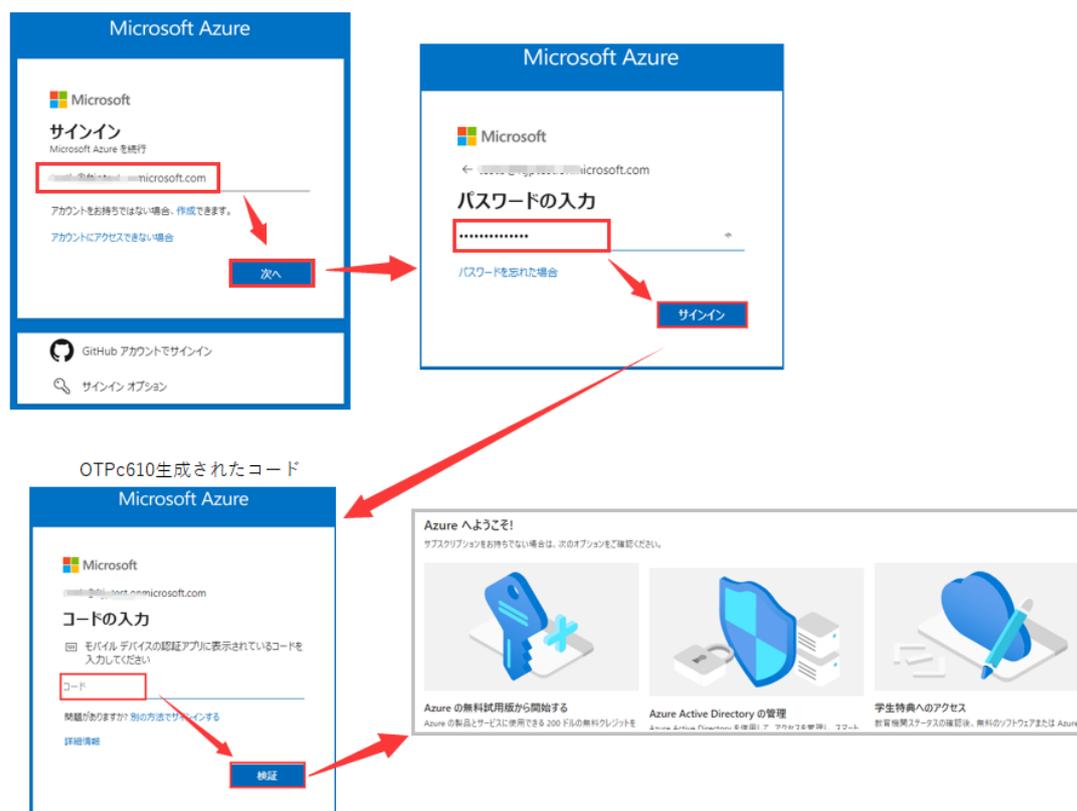


17、Azure のトップ画面が表示されます。



以上で初回設定（OTP c610 の登録）が完了しました。

次回以降、AzureAD Portal にアクセスする際はユーザーアカウント、PWD、OTP c610 より生成されたコードをそれぞれ入力してログインします。



方法 2 : 「マイアカウント」にアクセスして OTP c610 を登録

上記の AzureAD Portal より設定する方法以外に「マイアカウント」にアクセスして、OTP c610 を登録することができます。

- 1、下記 URL「マイアカウント」の「セキュリティ情報」の画面にアクセスします。

<https://mysignins.microsoft.com/security-info>

ユーザーアカウントと PWD を入力します。

- 2、認証方法が設定されていない場合は、上記 [3.1 初期設定 : OTP c610 の登録 (初回のみ)] の「2」～「15」をご参照いただき、OTP c610 を登録してください。
登録後、ステップ [9] より進めてください。

Microsoft Authenticator 及び電話の認証方法が既に設定されている場合は、下記のステップで OTP c610 を追加することができます。

- 3、 [セキュリティ情報] ⇒ [+サインイン方法の追加] の順にクリックします。



- 4、 [認証アプリ] を選択し、「追加」をクリックします。



- 5、 [別の認証アプリを使用します] リンクをクリックします。



- 6、 以降の手順は [方法 1] の「4」～「10」をご参照ください。

- 7、 正しく実行されると、「認証アプリ」が追加されます。

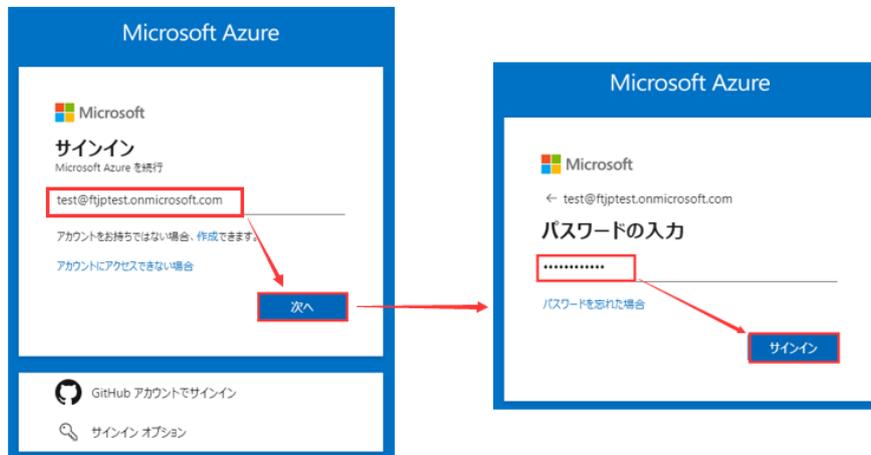


- 8、以上で登録作業が完了となります。
- 9、<https://portal.azure.com/>にアクセスし、ユーザーアカウントとOTPc610 より生成されたコードをそれぞれ入力して、ログインすることができます。

3.2. OTPc610 を利用して AzureAD にログインする方法

上記「3.1 初期設定：OTP c610 の登録（初回のみ）」で OTP c610 を登録後、OTP c610 で生成されたパスワードを利用して AzureAD にログインします。

- 1、Azure Portal（<https://portal.azure.com>）にアクセスし、ユーザーアカウント及びパスワードを入力します。



- 2、利用者のサインイン方法に [Microsoft Authenticator] を設定していない場合は、ステップ 3 に進んでください。

※ 利用者のサインイン方法に [Microsoft Authenticator] を設定した場合は、Microsoft Authenticator が優先的に認証を行い、下記の画面が表示されます。OTP c610 を利用してログインする場合は、「Microsoft Authenticator アプリを現在使用できません」を選択し次の画面で [認証コードを使用する] を選択してください。



3、認証コードの入力画面が表示されます。

OTP c610 で生成された認証コードを確認するため、以下の画面を表示した状態としてください。



4、OTP c610 の中央のボタンを 3 秒長押しすると、起動します。

[選択] に対応する中央のボタンを押すと、認証コード画面が表示されます。

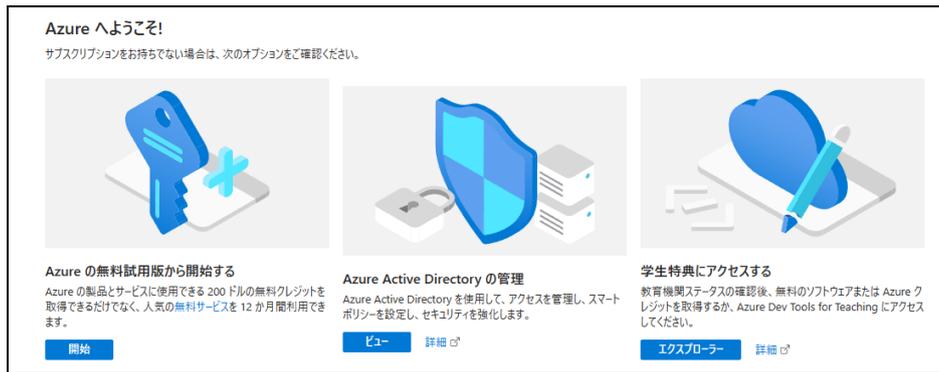
(下画像の場合、認証コードは「578830」となります。)



5、PC の認証コード入力画面に、OTP c610 で発行された認証コードを入力し、[検証] をクリックします。



6、正しく認証されると、AzureAD のトップ画面が表示されます。



以上までが OTPc 610 で AzureAD にログインする方法のご説明となります。

4. OTP c610 を利用しない場合（バインドの解除）

OTP c610 を利用しない場合は、AzureAD よりユーザーとのバインドを解除します。ユーザー自身での解除の他、管理者にて強制的に解除することも可能です。OTP c610 に登録されたアカウント情報も削除する必要があります。詳細なバインド解除の方法を下記で説明いたします。

4.1. ユーザー自身で解除する方法

ユーザーは OTP c610 の利用を停止する場合、下記 2 ステップで OTP c610 のバインドを解除できます。

Step1：【マイアカウント】の「セキュリティ情報」より「認証アプリ」を削除

- 「マイアカウント」(<https://mysignins.microsoft.com/security-info>) にアクセスします。ユーザーID、PWD、OTP c610 より生成されたコードをそれぞれ入力します。
- 【セキュリティ情報】⇒【認証アプリ】の右の「削除」をクリックして、削除します。



Step2 : OTP c610 の登録情報を削除

OTP c610 に登録されたアカウント情報を削除する手順は下記の通りです。

- 1、OTP c610 の中央のボタンを 3 秒長押し、起動します。
- 2、アカウント一覧が表示されます。[切替]に対応している左のボタンを押して、削除するアカウントを選びます。
- 3、[選択]に対応する中央のボタンを押すと、該当アカウント情報が表示されます。
- 4、[削除]に対応する右のボタンを押して、削除してください。



- 5、下記の通り、削除の確認画面が表示されます。
削除する場合は、[削除] に対応する中央のボタンをクリックします。
正しく削除されると、OTP c610 のアカウント一覧画面に戻ります。

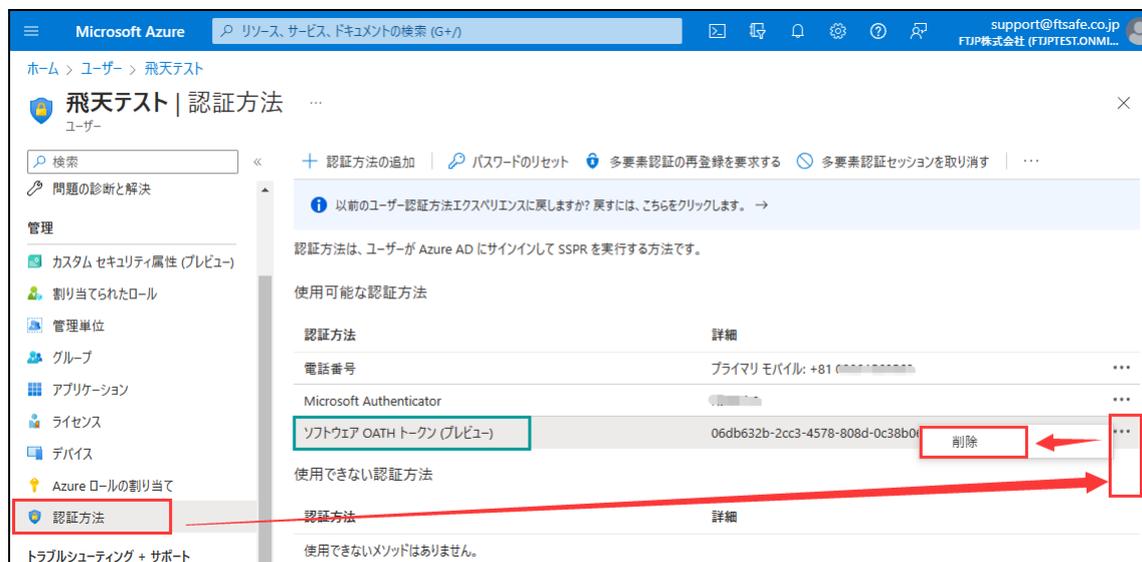


4.2. 管理者側で強制解除する方法

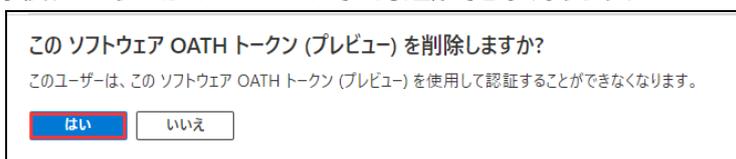
管理者は AzureAD Portal 経由で、ユーザーの OTP c610 認証方法を強制的に削除できます。

強制解除方法：

- 1、管理者権限で Azure portal (<https://portal.azure.com>) にサインインします。
- 2、[Azure Active Directory] > [ユーザー] > 該当ユーザーを選択します。
- 3、「認証方法」 > 「ソフトウェア OATH トークン」の右側の [...] をクリックしてから、[削除] をクリックします。



- 4、下記確認画面が表示されます、[はい] をクリックすると、OTP c610 の認証方法が強制的に削除されます。削除後、ユーザーは OTP c610 での認証ができなくなります。



- ※ 上記方法で AzureAD の登録方法を削除した後、OTP c610 の内部に格納された登録情報を手動で削除する必要があります。詳細は [4.1] の「Step2」をご参照ください。

5. 運用方法

5.1. ユーザーが OTP c610 を紛失した場合

ユーザーが OTPc610 を紛失した場合は、早急に管理者へ連絡してください。

管理者が AzureAD portal で、紛失した OTP c610 の削除及びユーザーの多要素認証の再登録を促すことができます。

具体的には下記の流れです。

Step1: [管理者] 紛失した OTP c610 の強制削除

管理者は AzureAD portal 経由でユーザーが紛失した OTP c610 を削除します。

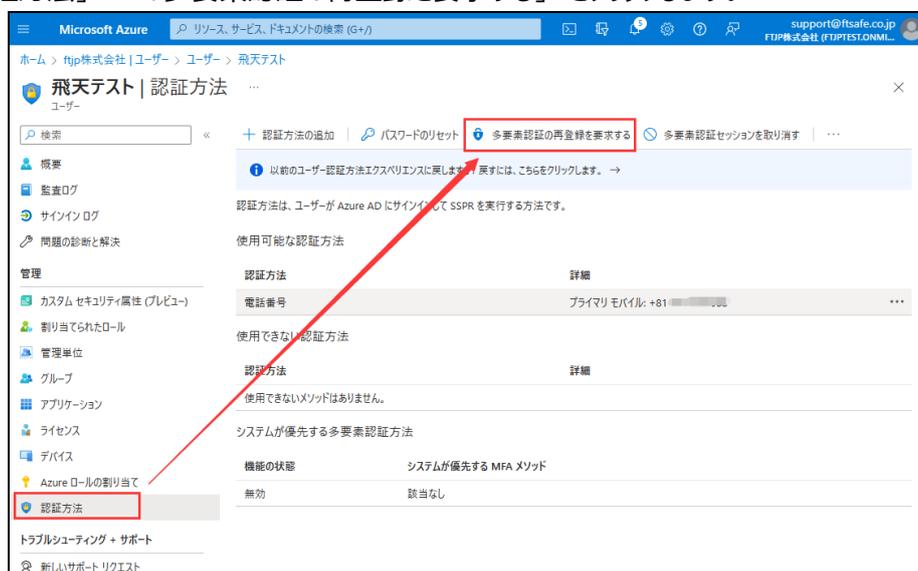
※詳細は、「4.2」を参照してください。

Step2: [管理者] ユーザーに新たな OTPc610 を配布、「多要素認証の再登録」を設定

管理者はユーザーに新しい OTPc610 を配布し、ユーザーに多要素認証の再登録を要求します。

[多要素認証の再登録を要求する] 設定方法：

- 1、管理者権限で Azure portal (<https://portal.azure.com>) にサインインします。
- 2、[Azure Active Directory] > [ユーザー] > 該当ユーザーを選択します。
- 3、「認証方法」 > 「多要素認証の再登録を要求する」をクリックします。



- 4、その後、ユーザーが AzureAD portal やマイアカウントにサインインする際、多要素認証の再登録が必須となります。

Step3: [ユーザー] 新しい OTP c610 の登録

ユーザーが Azure portal (<https://portal.azure.com>) やマイアカウント (<https://myprofile.microsoft.com>) にサインインする際、[3.1] のように初期設定となりますので、新たに OTP c610 を登録してください。

5.2. OTP c610 に時刻ズレが発生し、急に認証できなくなる場合

OTP c610 はタイムベースで、一定時間（通常は 30 秒/60 秒）ごとに一時的な認証コードを生成します。内部に小型のボタン電池を内蔵し、電力を供給しています。

長期間の利用や利用頻度により、電池の消耗又は劣化により電圧低下が発生し、時刻ズレ（内部の時計が進んだり、遅れたりする）が発生します。これにより、OTP c610 で生成された認証コードと認証サーバー側で生成されたコードが異なり不一致となるため、認証に失敗します。

[対処方法]

下記手順で OTP c610 のタイムサーバーにアクセスして、OTP c610 の時刻を再設定してください。

- 1、OTPc 610 のタイムサーバー（ <https://timesync.rakunin.co.jp/> ）にアクセスすると、QR コードが表示されます。
- 2、OTP c610 の **【左+中央】のボタンを 3 秒長押し** 起動します。上記 1 のタイムサーバーの QR コードをスキャンして、時刻を再設定します。

※詳細は、『OTP c610 利用マニュアル』の [2.6 OTP c610 の時刻再設定（時刻同期）] を参照してください。

以上