Microsoft Entra ID の 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 Entra ID 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。

※Microsoft Entra ID の UI や項目名称は、将来的に変更される可能性があります。実際の画面と差異がある場合は、最新の Microsoft 公式ドキュメントをご参照ください。

【目次】

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ありません。画面下部のボタンを使用して操作してください。

2、 **中央ボタンを 3 秒長押しすると、電源のオン/オフが可能**です。
1 分間操作が無い場合、自動的に電源がオフになります。

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、 同一サービスの QR コードを複数回登録した場合、**最後の登録のみが有効**となります。

5、 OTP c610 はすべての QR コード認証サービスに対応しているわけではありません。
TOTP（RFC6238）に対応したサービス（**Microsoft MFA、Google MFA、Salesforce MFA** 等）で利用可能です

2. 事前準備

下記を事前にご準備ください。

2.1. 準備 1 ： Microsoft Entra ID 管理者とユーザー

Microsoft Entra ID の管理者とユーザーアカウントを事前準備してください。

2.2. 準備 2 ：ユーザー用 OTP c610 トークン

3. 認証方法ポリシー及び条件付き

3.1. 認証方法ポリシーに［ソフトウェア OATH トークン］を有効

OTPc610 はハードウェアトークンですが、Entra ID では［ソフトウェア OATH トークン］として登録する必要があるため、管理者は Entra ID の認証方法ポリシーで［ソフトウェア OATH トークン］を「有効」にする必要があります。

［手順］

1、 管理者は Microsoft Entra 管理センターにサインインします。

2、 ［Entra ID］＞［認証方法］＞［ポリシー］の順に移動し、［ソフトウェア OATH トークン］をクリックします。

3、 「ソフトウェア OATH トークンの設定」画面で［有効にする］を選択し、ターゲットを指定します（下図は［MFA Group］のグループが対象）。設定が終わったら［保存］をクリックします。

4、 ［ソフトウェア OATH トークン］が「有効」になっていることを確認できます。

3.2. 条件付きアクセスポリシーの設定（必要に応じて）

条件付きアクセスポリシーは、特定のユーザー、グループが指定されたアプリにアクセスする際に、MFA を求めるポリシーを作成できます。

※条件付きアクセスポリシーは必須ではありませんが、MFA 認証を強制するためには設定が必要となる場合があります。

詳細は、以下の URL を参照してください。
https://learn.microsoft.com/ja-jp/entra/identity/authentication/tutorial-enable-azure-mfa?bc=%2Fazure%2Factive-directory%2Fconditional-access%2Fbreadcrumb%2Ftoc.json&toc=%2Fazure%2Factive-directory%2Fconditional-access%2Ftoc.json#create-a-conditional-access-policy

以下では、特定のユーザーやグループが Microsoft Entra 管理画面にアクセスする際に、MFA 認証が必要となる設定方法を例として説明します。

1、 管理者は Microsoft Entra 管理センターにサインインします。

2、 ［Entra ID］>[条件付きアクセス］ の順に移動し、［新しいポリシーの作成］を選択します。

3、 ポリシーの名前を設定します。割り当てユーザーやグループを指定します。

4、 ターゲットリソースを設定します。
例：Microsoft 管理ポータルにアクセスする際に、MFA 認証が必要の場合、［クラウドアプリ］の対象に［Microsoft 管理ポータル］を指定できます。

5、［許可］>［アクセス権の付与］に、［多要素認証を要求する］をチェックして［選択］をクリックします。

6、画面の左下の［ポリシーの有効化］を［オン］に設定し、［作成］をクリックします。

7、以上で、条件付きアクセスポリシーが作成されます。

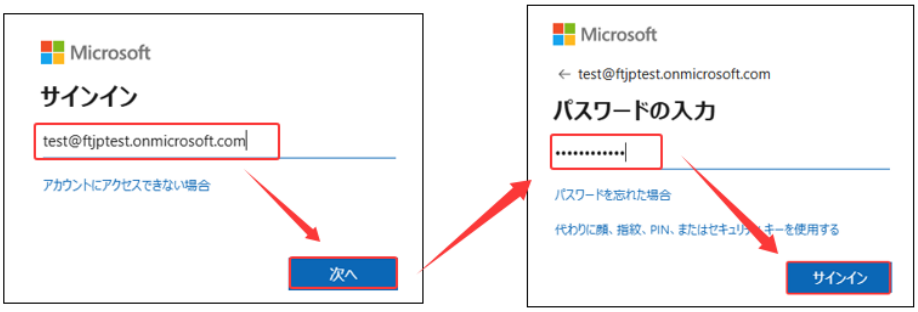
4. OTP c610 を利用して EntraID へサインインする方法（ユーザー）

4.1. 初期設定：OTP c610 の登録（初回のみ）

OTP C610 を利用して Microsoft Entra ID にサインインするためには、まず Entra ID ユーザーが OTP C610 を登録する必要があります。以下では、2 つの方法で OTP C610 の登録方法を説明します。

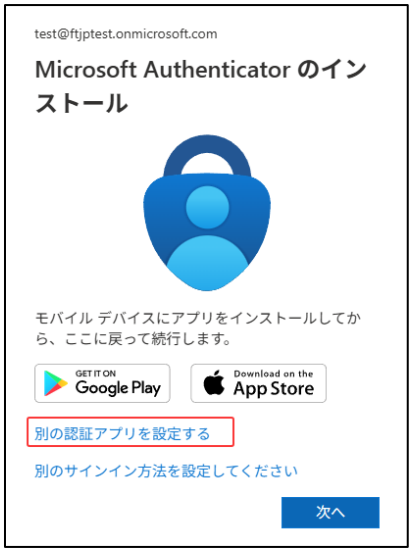
方法 1：「Microsoft Entra 管理センター」にアクセスして OTP c610 を登録

1、 ユーザーが Microsoft Entra 管理センターにアクセスし、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**「別の認証アプリを設定する」**のリンクをクリックします。
※「別の認証アプリを設定する」が表示されない場合は、認証方法ポリシーの設定が正しく行われていない可能性があります。本資料の［3］を参照し、設定内容をご確認ください。



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。

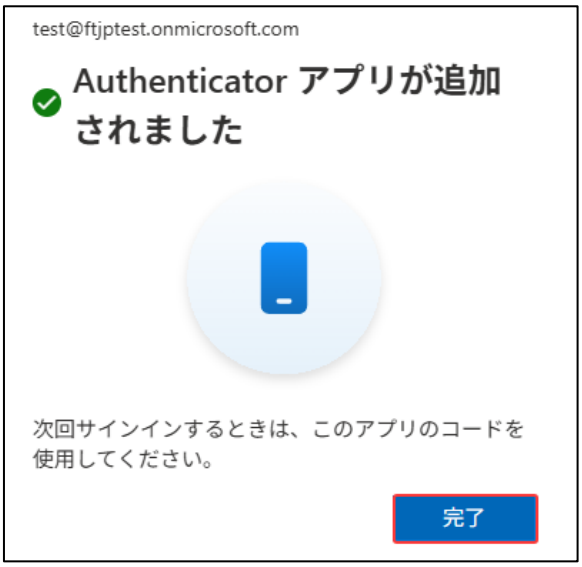
9、 [選択]ボタンに対応している中央のボタンを押すと、生成されたワンタイムパスワード（６桁の数字）が表示されます。

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、［完了］をクリックし、登録を完了します。



13、サインイン状態を維持する場合は、［はい］をクリックしします。

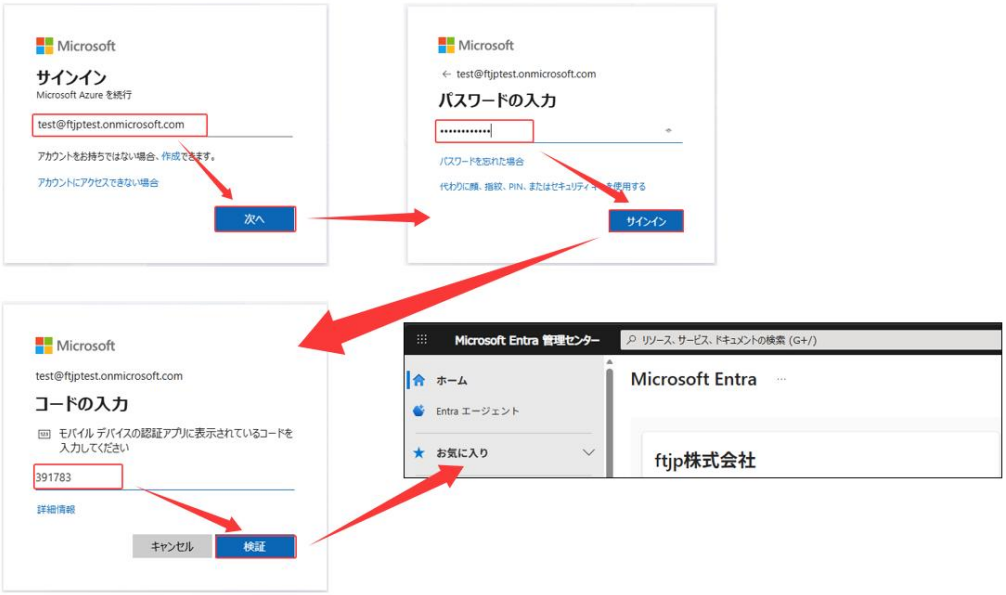
※ サインインの状態を維持したい場合は「はい」を選択します。これにより、次回以降のサインインが簡単になります。

※ 状態を維持したくない場合は「いいえ」を選択します。この場合、次回サインインする際には再度認証が必要になります。

14、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、Microsoft Entra 管理センター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サインインできます。



方法 2：「セキュリティ情報ページ」にアクセスして OTP c610 を登録

上記の Microsoft Entra 管理センターより設定する方法以外に「セキュリティ情報ページ」にアクセスして、OTP c610 を登録することができます。

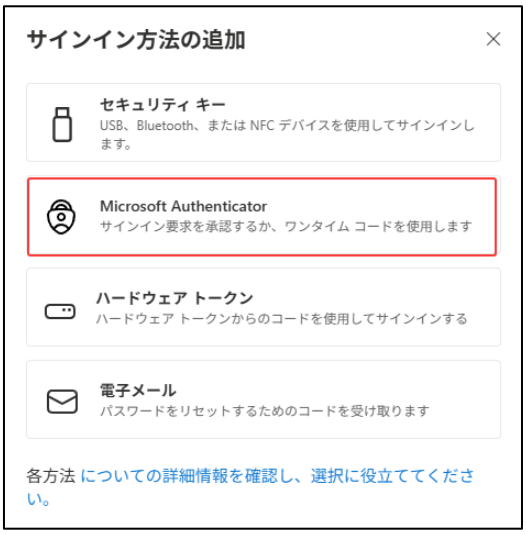
1、 下記 URL の「セキュリティ情報ページ」にアクセスします。
https://aka.ms/mysecurityinfo
ユーザーアカウントと PWD を入力します。

2、 認証方法が設定されていない場合は、上記［方法 1］の「2」～「12」をご参照いただき、OTP c610 を登録してください。

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、 ［Microsoft Authenticator］を選択します。



5、 ［**別の認証アプリを設定する**］リンクをクリックします。

6、 以降の手順は［方法 1］の「4」～「12」をご参照ください。

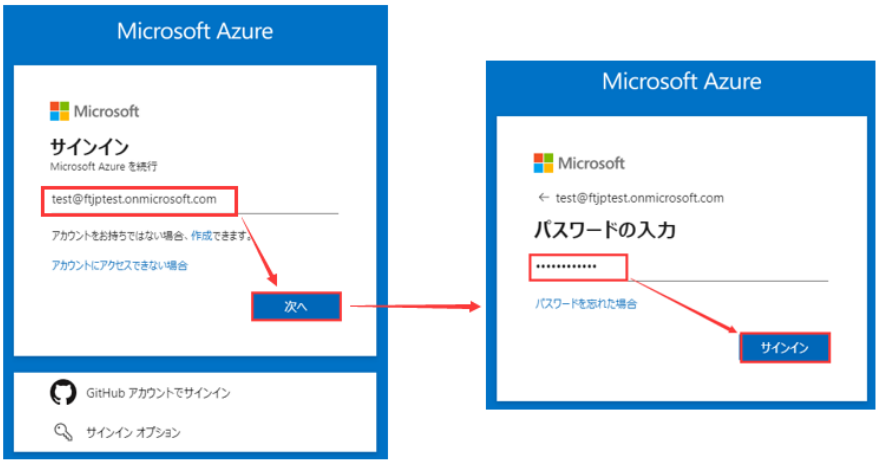
7、 正しく実行されると、「認証アプリ」が追加されます。

8、 以上で登録作業が完了となります。

4.2. OTPc610 を利用して Microsoft Entra にサインインする方法

上記「4.1 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 Microsoft Entra 管理センターにサインインします。

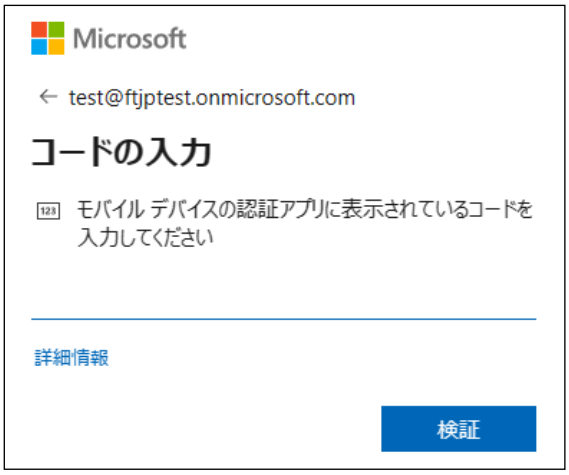
1、 ユーザーが Microsoft Entra 管理センターにアクセスしし、ユーザーアカウント及びパスワードを入力します。



2、 ユーザー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。

※ ユーザーの既定のサインイン方法として［Microsoft Authenticator］が設定されている場合、下記画面のように優先的に表示されます。
OTP c610 を利用する場合は、「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。

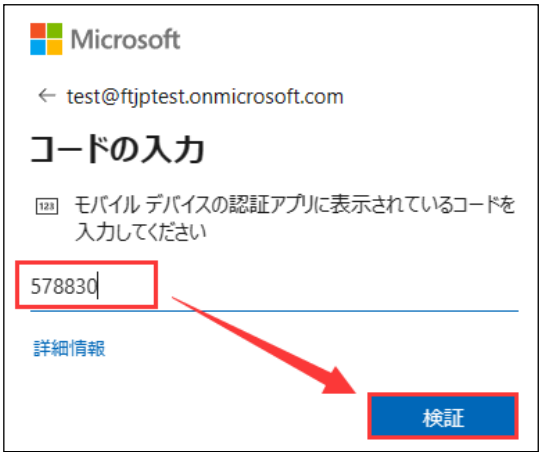


4、 OTP c610 の中央のボタンを 3 秒長押しすると、起動します。

［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、Microsoft Entra 管理センターのトップ画面が表示されます。

以上までが OTPc 610 で Microsoft Entra にサインインする方法のご説明となります。

5. 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、ユーザーとのバインドを解除できます。
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。

5.1. 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：「セキュリティ情報ページ」より「認証アプリ」を削除

1、「セキュリティ情報ページ」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。

2、 ［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。

5.2. 管理者側で強制解除する方法

管理者は Microsoft Entra 管理センターを経由で、ユーザーの OTP c610 認証方式を強制的に削除できます。

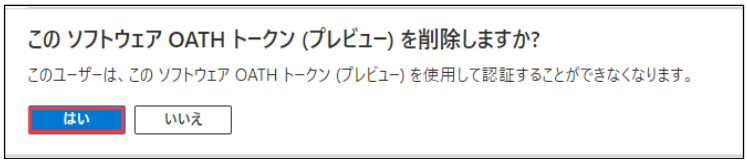
強制解除方法：

1、 管理者が Microsoft Entra 管理センターにサインインします。

2、 [Entra ID] > [ユーザー] > ［すべてのユーザー］ > 対象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 Microsoft Entra 管理センター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［5.1］の「Step2」をご参照ください。

6. 運用方法

6.1. 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 Microsoft Entra 管理センター経由でユーザーが紛失した OTP c610 を削除します。
※詳細は、「5.2」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 Microsoft Entra 管理センターにサインインします。
2、 [Entra ID] > [ユーザー] >[すべてのユーザー] > 対象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、 そうすると、ユーザーが Microsoft Entra 管理センター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 Microsoft Entra 管理センターや「セキュリティ情報ページ」にサインインする際、［4.1］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。

6.2. 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。表示用単 3 電池とは別に、内部に小型のボタン電池を内蔵し、内部時計の電力を供給してます。

長期間の利用やボタン電池残量の低下により、内部時計にズレ（進み/遅れ）が発生する場合があります。その結果、サーバー側の時刻と一致せず、認証に失敗することがあります。

※OTP c610 は外部のタイムサーバーと直接通信するわけではありません。
QR コードを介して時刻補正情報を取得し、内部時計を補正する仕組みです。

■［対処方法］
専用の時刻同期ページ（https://timesync.rakunin.co.jp/）にアクセスし、
表示された QR コードを OTP c610 でスキャンすることで、時刻補正を行ってください。

■［手順］
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