

Office365 多要素認証の初期設定

（スマートフォンを認証デバイスとする）

作成：	2020年4月16日
更新：	2020年6月3日
	2020年11月12日

概要

Office365 各種サービスへのログインは、セキュリティ強化のため多要素認証となっており、ログインの際に、[1 要素目]としてメールアドレスとパスワードの入力に加えて、[2 要素目]として「Microsoft Authenticator」（スマートフォン上のアプリ）でのログイン承認操作、もしくは、SMS（ガラケーのショートメッセージ）に通知される承認番号の入力操作、による多要素での認証が必要です。

本手順書での記載内容

- スマートフォンによる Office365 多要素認証の初期設定手順
 - Office365 ウェブ画面での多要素認証の開始
 - スマートフォンでのモバイルアプリ「Authenticator」の設定（Android / iOS）
- フィーチャーフォン（ガラケー）を利用したい場合は、ポータルより別の初期設定マニュアルを確認ください。

Office 365 の各種サービス

- Outlook、Teams、OneDrive、SharePoint などが対象
- アプリケーションとウェブブラウザ（OWA）のどちらからのログインも対象

注意事項

- 多要素認証設定後は、Office365 のウェブ画面またはアプリケーションへのサインイン時には、Authenticator によるサインインの承認をしてください
- センター内（NCVC ネットワーク）からの利用は、多要素認証の発生頻度が緩和します
- Office365 の利用場所（自宅 Wi-Fi と NCVC-Wi-Fi の間など）の移動や、利用デバイス、利用アプリが増えたり変わったりする度に多要素認証が発生します
- 同じ場所・デバイス・アプリの場合、多要素認証が 1 ヶ月程度の頻度で発生します
- スマートフォンの紛失に備えて複数台登録をお勧めします
 - 手順はポータルを参照ください。

1. Office365 多要素認証の初期設定手順

QR コードの読取が発生するため、

「 【スマホ側操作】」記載は、手順はスマートフォンで、

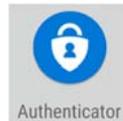
「 【PC側操作】」記載は、PC やタブレットで

2 台用いて操作してください



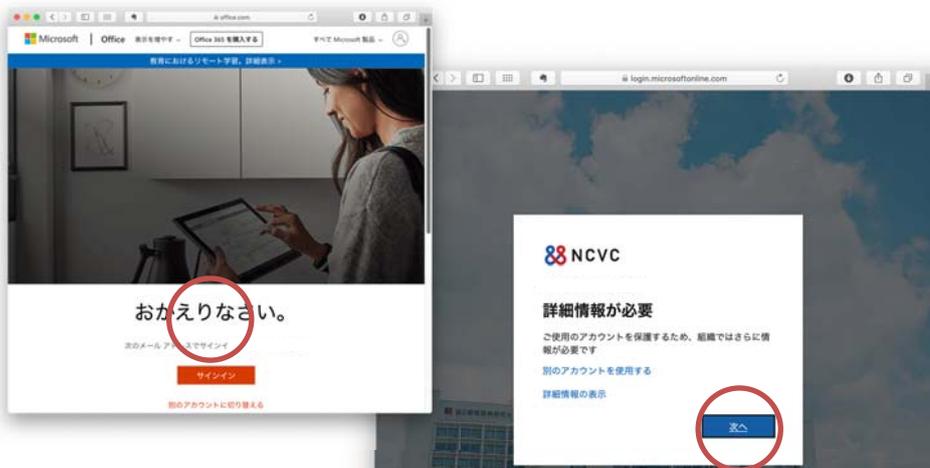
1-1. 【スマホ側操作】最初にスマートフォンに Microsoft Authenticator をインストールする

- ・他社 Authenticator も存在するので注意
- ・Android 端末は GooglePlay から
- ・iOS (iPhone/iPad) 端末は AppStore から



1-2. 【PC側操作】<https://www.office.com> へウェブブラウザ (Edge、Chrome、Safari など) でサインインし、「詳細情報が必要」と出るので、[次へ]

- ・既にサインインされている場合には、一度サインアウトしてから行う



1-3. 「追加のセキュリティ確認 手順1 ご希望のご連絡方法をお知らせください」が表示されるので、Authenticator (モバイルアプリ) を使用するスマートフォンの情報を入力

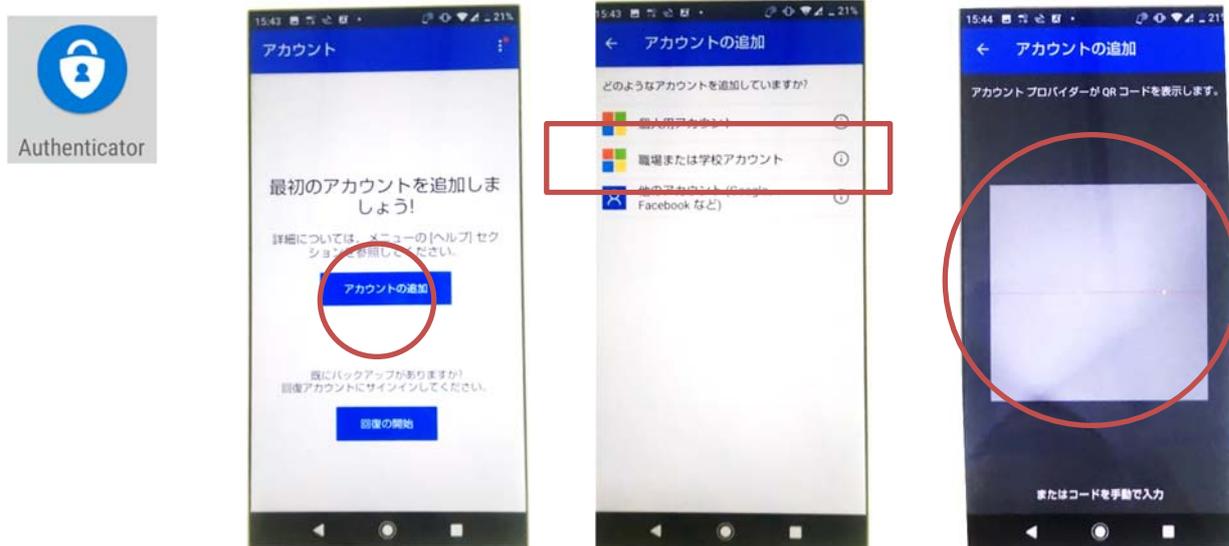
- ・ A. ドロップダウンメニューは、**[モバイルアプリ]**を選択
- ・ B. 「モバイルアプリをどのような用途で使用されますか？」で[確認のため通知を受取る]を選択
- ・ C. [セットアップ]を押すと、「モバイルアプリケーションの構成」が開く
- ・ 間違えた場合、「モバイルアプリケーションの構成」を[キャンセル]して選択し直す



1-4. 【スマホ側操作】 Authenticator を起動し、次のとおり設定して、手順 3 の「モバイルアプリケーションの構成」の QR コードを読み取る

- ・ [アカウントの追加] - [職場または学校アカウント] と選択
- ・ カメラへのアクセスを求められる場合には、[許可]する
- ・ カメラが起動するので QR コードを読み取る

A. Android 端末の画面変遷 (iOS は次ページ記載)



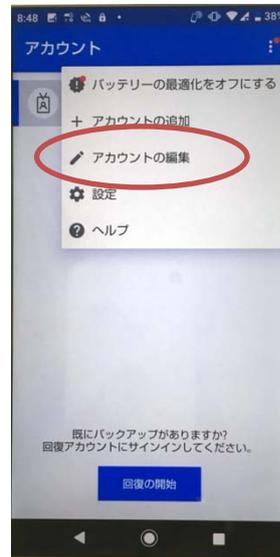
※ 貸与スマホ (AQUOS) では、既に、以下の様「Ncvc」という組織名で設定されている場合がありますので、「Ncvc」の設定を削除して本手順を進めてください。

※ 貸与スマホ (AQUOS) の場合には、以下のように「Ncvc」という組織名で設定が既にある場合があります。その際には「Ncvc」の設定を削除して本手順を進めてください。
(管理者メモ：スマホでOutlook アプリ既使用情况の場合、「Ncvc」設定が存在)

右肩[:]を選択

[アカウントの編集]を選択

[X]を選択し削除



B. iOS (iPhone) 端末の画面変遷



1-5. 【スマホ側操作】QRコードを読み込むと、Authenticator アカウントに組織名が表示される



Android 上の Authenticator 画面



iOS 上の Authenticator 画面

1-6. 「モバイルアプリケーションの構成」画面で [次へ] を押す



1-7. 「追加のセキュリティ確認」が表示された後、

※ ここで「失敗しました」となった場合には、手順 1-3 より再開する



[次へ] が青くなったらを押す

※ [次へ] が青くならないとき、手順 1-4 で「職場または学校アカウント」が選択されていないことがあるため、手順 1-3 より再開する

※ ここで「タイムアウト」した場合には、[再試行] を押して継続する



1-8. 「追加のセキュリティ確認 手順2 こちらからお客様のモバイルアプリケーションデバイスに連絡する」が表示された後、



【スマホ操作】 Authenticator の承認通知が表示されるので承認する



Android
別アプリ起動中



Android
Authenticator 起動中



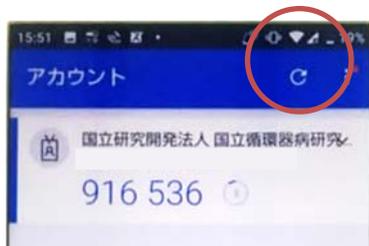
iPhone
待機画面上



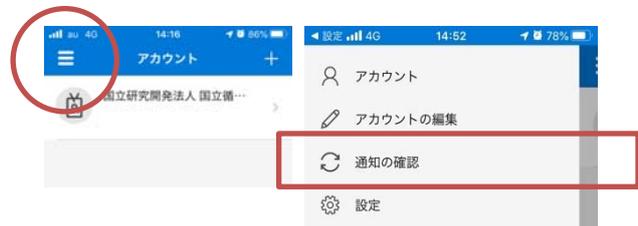
iPhone
Authenticator 起動中

※ 承認通知が来ないとき、以下を行う

1. 1-9 の画面が見えている場合、本手順をスキップする
2. 1-9 の画面が見えていない場合、Authenticator 画面から、以下の様に確認する



Android 端末は右肩の丸いボタン



iOS は左肩メニューから、通知の確認

1-9. 「追加のセキュリティ確認 手順3」が表示されるので、国番号を「日本 (+81)」を選択し、電話番号を入力、[次へ]を押す

モバイルアプリ (Authenticator) が利用できない場合、ここで登録される電話番号に

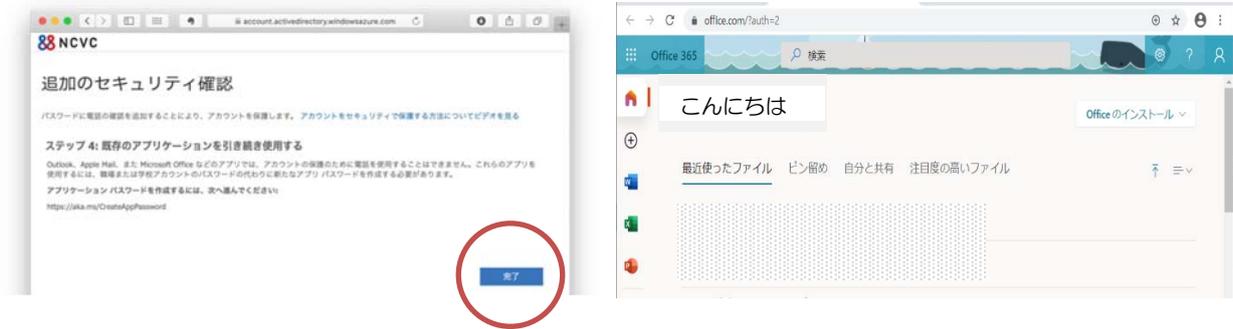
- SMS にコードを送信、コードを利用して o365 にログインできる
- 着信があり、指示に従ってログインできる
- 可能であれば、スマートフォン紛失時を考慮すると別電話が良い

国番号の選択メニューで、
日本 (+81) は下の方





1-10. 「追加のセキュリティ ステップ 4 既存アプリケーションを引き続き使用する」が表示されるので[完了]を押して、Office365 画面が表示されると、多要素認証の設定は完了し、ウェブ画面へのサインインが完了する。



- ※ 以後、Office365 サインイン時には、手順 1-8 の承認操作が必要となります
- ※ Office365 の利用場所（自宅 Wi-Fi と NCVC-Wi-Fi の間など）の移動や、利用デバイス、利用アプリが増えたり変わったりする度に多要素認証が発生します
- ※ 同じ場所・デバイス・アプリの場合、多要素認証が 1 ヶ月程度の頻度で発生します
- ※ センター内（NCVC ネットワーク）からの利用は、多要素認証の発生頻度が緩和します

以上