

1 はじめに（多要素認証の導入）

Microsoft Office 365 の利用にあたり、外部からの不正アクセスやなりすまし対策のため、同クラウドシステムに用意されているセキュリティ強化機能の1つである多要素認証の機能を有効にし、一層のセキュリティ強化を図ります。

1.1 多要素認証（Multi-Factor Authentication）とは

メールソフト等にログインする際、従来は ID とパスワードのみで本人確認をしていましたが、それ以外の要素も加え、本人を認証する方式のことです。従来の認証方式と比較しセキュリティが強化され、外部からの不正アクセスやなりすまし対策に有効な認証方式です。

1.2 適用対象範囲

全学生・教職員

1.3 初期設定(電話登録)

機能活用の有無にかかわらず、対象者全員が、初期設定として携帯電話や固定電話の登録を行う必要があります。

1.4 多要素認証が要求される範囲

学外から本学の Office 365 にサインインする場合。

※ 学内からサインインする場合、多要素認証は要求されません。

1.5 用語定義

本書で使用する主な用語について記載します。

用語	説明
Office 365	Microsoft 社が提供するクラウドグループウェアサービス
アプリケーションパスワード (アプリパスワード)	Office 365 アカウントにアクセスするためのアクセス許可をアプリまたはデバイスに付与するコード ※ Outlook2016 以外のメールソフト (Outlook2013、Thunderbird 等) を利用している場合や、Outlook2016 で Exchange 以外の接続の種類 (POP や IMAP など) を選択している場合 (詳細は「4.6Outlook2016 のメールの接続の種類の確認」をご参照ください。) に使用します。
学内	以下の学内ネットワークから Office 365 にアクセスする場合を指します。 ・学内無線 LAN (YCUWL) ・教育研究 LAN ・事務 LAN
学外	学内ネットワーク以外の、自宅などから Office 365 にアクセスする場合を指します。 ※ 学内においても、携帯電話のキャリア回線を使ってアクセスする場合は、学外に該当します。

1.6 導入する多要素認証について

Microsoft Office 365 のサインインの仕組みを利用し、デバイス(PC 等)ごとにソフトウェア(WEB ブラウザやメールソフト等)単位で認証を行います。

一度多要素認証を行うと一定期間は認証状態が保持されますが、認証状態が保持されていない他の PC やブラウザ、メールソフトなどでサインインした場合は、その都度、多要素認証を要求されます。