AIM AOYAMA GAKUIN UNIVERSITY INSTITUTE OF INFORMATION AND MEDIA

本学で導入される多要素認証について

2026-3-27

青山学院大学 情報メディアセンター

多要素認証とは

多要素認証（Multi-Factor Authentication）とは、システムにログインする際、従来の「IDとパスワード」だけでなく、別の要素を組み合わせて本人確認を行う、より安全な（認証）セキュリティの仕組みです。
パスワードは「知識情報（知っていること）」ですが、これに加えてスマートフォンなどの「所持情報（持っているもの）」や、指紋などの「生体情報（あなた自身）」を組み合わせることで、万が一パスワードが他人に知られてしまっても、不正アクセスを未然に防ぐことができます。

多要素認証にはいくつかの方式がありますが、本学のシステムでは、皆様の利用環境に合わせて以下の3つの認証方式から選択(*)して利用することができます。ご自身にとって最も使いやすい方法をご登録ください。

・メールワンタイム認証　※旧名称：OTP認証(メール)
・Authenticator認証　※旧名称：OTP認証（Authenticator）
・生体認証
※2026.3.27：より分かりやすい名称に変更しました。

それぞれの認証方式について、次のページ以降で説明いたします。

(*)2026.3.27以降、複数の認証方式を設定しておくことで、ログイン時、別の認証方式を選択することが出来るようになりました。

本学で利用可能な多要素認証方式

① メールワンタイム認証
登録したご自身のメールアドレス宛に、ワンタイムパスワード（1回限り有効な数字のコード）が送信される方式です。

メリット　：専用のアプリが不要で、すぐに設定・利用できます。
デメリット：メールの受信が遅れる場合や、オフライン環境でパスワードを受け取れない場合があります。

② Authenticator認証
スマートフォンにインストールした「認証アプリ（Google Authenticator、Microsoft Authenticatorなど）」に表示される
ワンタイムパスワードを入力する方式です。

メリット　：電波の届かないオフライン環境でもコードを確認でき、メールのような遅延もありません。
デメリット：アプリのインストールが必要です。また、スマートフォンの機種変更や紛失をした場合、
引き継ぎや再設定の手続きが必要になります。

③ 生体認証
お使いのスマートフォンやPCに搭載されている**指紋認証や顔認証**（Touch ID、Face ID、Windows Helloなど）を利用して
ログインする方式です。

メリット　：コードの入力やアプリを開く手間がなく、最も安全かつスムーズにログインできます。
デメリット：生体認証に対応したスマートフォンやPCが必要です。また、端末の性能により認証精度が悪くなる可能性もあります。

AIM

AOYAMA GAKUIN UNIVERSITY
INSTITUTE OF INFORMATION
AND MEDIA

www.aim.aoyama.ac.jp