

利用者様からいただいたご質問のうち主なものについては、こちらに随時掲載していきます。
また、掲載済みの質問についても内容を更新する場合がありますのでご承知おください。

No.	ご質問	回答
1	多要素認証のセットアップは必須でしょうか。	多要素認証は、学外からWebメールにログインする際に必要です。そのため、 ・Webメールを利用しない方（メールクライアント（アプリケーション）や転送設定で対応している場合等） ・Webメールを使うが、学内（正確にはIPアドレスが133.1.0.0/16のネットワーク環境）でのみ使用し、学外では利用しない方 以上の方々は、多要素認証のセットアップは不要です。 但し、普段は学外からWebメールを使わない方でも、いつか必要が生じる場合に備えて、多要素認証のセットアップをしていただくことを推奨いたします。
2	多要素認証のセットアップをしないと、どうなりますか。	多要素認証が適用された後は（適用タイミングはNo.3のとおり）、学外からWebメールにログイン出来なくなってしまいます。 学外からWebメールにログインする必要がある方は、多要素認証が適用された後、学内から多要素認証のセットアップをお願いします。
3	多要素認証の適用（運用）開始はいつですか。	2024年8月29日（木）～10月31日（木）の中で、部局等管理者様から申請があった日に適用いたします。 適用日がご不明な場合は部局等管理者様にご確認ください。 基本的には各日15時頃に適用しますが、時間は多少前後する場合があります。
4	多要素認証の適用日より前に多要素認証をセットアップすることはできますか。	多要素認証のセットアップは、多要素認証が適用された後（適用タイミングはNo.3のとおり）でないと出来ませんので、ご了承ください。
5	メールクライアント（アプリケーション）（例：Outlook, Thunderbird等）を利用している場合でも、多要素認証が必要でしょうか。	今回メールクライアントは多要素認証の導入対象外ですので、メールクライアントのみ使用している方（Webメールを使わない方）であれば、多要素認証のセットアップは任意です。
6	ポータルサイト（ https://www.mail.osaka-u.ac.jp/ ）も多要素認証が必要になるのでしょうか。	今回ポータルサイトは多要素認証の導入対象外ですが、現在検討中で、今後導入する可能性もあります。
7	既に他のシステム（全学IT認証基盤システム（大阪大学個人ID）、ICHOメール、OUMail）で多要素認証を行っています。再度多要素認証の登録が必要なのでしょうか。	はい。 お手数ですが左記の各システムとは別に、キャンパスメール用の多要素認証セットアップが必要です。
8	【部局等管理者様向け】 多要素認証の無効化、初期化とは何でしょうか。 いつ何のための行う処理でしょうか。	次の部局等管理者向けマニュアル1-1, 1-2をご覧ください。 https://ccc.osaka-u.ac.jp/files/mfa-manual-kanri.pdf
9	多要素認証のセットアップに何度も失敗します。原因は何でしょうか。	一つの原因として、デバイス（スマートフォン等）の時刻設定が不適切であることが考えられます。時刻設定が手動設定となっている場合は、自動設定を有効としてください。 Androidの設定方法： https://support.google.com/android/answer/2841106?hl=ja iPhoneの設定方法： https://support.apple.com/ja-jp/guide/iphone/iph65f82af3e/ios
10	多要素認証アプリをインストールしていたスマートフォン等を機種変更/紛失したため、多要素認証が出来ず学外からWebメールにログイン出来なくなっていました。	新しいスマートフォン等をご準備の上、学内（正確にはIPアドレスが133.1.0.0/16のネットワーク環境）で、多要素認証の再セットアップをお願いします（学内からログインする場合は、多要素認証は求められません）。 セットアップ手順は次のマニュアルでご確認ください。 https://ccc.osaka-u.ac.jp/files/mfa-manual.pdf 但し、お急ぎの場合や、学内に行く機会が無くセットアップが出来ない場合は、ご所属部局のキャンパスメール部局管理者様に、多要素認証の無効化をご依頼ください。無効化すると、学外からでも多要素認証不要でログインできます。
11	6桁認証コードを入力しても多要素認証に失敗します。	6桁の認証コードを入力する際、多要素認証アプリで正しいアカウントを選択されているでしょうか。 例えば本学の一般的な教職員であれば、多要素認証アプリに次の3種類のシステムのアカウントが登録されているケースが一般的ですが、キャンパスメールご利用時はこのうち③のアカウントを選択してください。 ①全学IT認証基盤システム（大阪大学個人ID）：多要素認証アプリ上では「osaka-u u123456x」等と表示 ②ICHOメール：多要素認証アプリ上では「国立大学法人 大阪大学 u123456x@icho2.osaka-u.ac.jp」等と表示 ③キャンパスメール：多要素認証アプリ上では「Osaka Univ. Campus Mail user+ccc」等と表示 上記③に相当するアカウントが存在しない場合は、当FAQ No.4の手順でご対応ください。
12	これからスマートフォンの機種変更をしますが、どうすれば良いでしょうか。	一例として、次の手順でご対応ください。 ①機種変更する前に、任意のデバイス（パソコン等）でWebメールにログインする。多要素認証の際に表示される「今後30日間この端末（ブラウザ）では多要素認証を省略する」チェックボックスにチェックを付けておく ②機種変更の後、①と同じデバイス・WebブラウザでWebメールにログインして（①でチェックを付けておけば、多要素認証不要でログインできます）、多要素認証の設定画面にアクセスする ③新しいスマートフォン等で多要素認証のセットアップを行う
13	スマートフォンを持っていませんが、どうすれば良いでしょうか。	パソコンで、ご使用中のWebブラウザにアドオン（拡張機能）をインストールすると、多要素認証アプリの代わりとすることができます。 Google Chrome： https://chrome.google.com/webstore/search/authenticator Firefox： https://addons.mozilla.org/ja/firefox/ Microsoft Edge： https://www.microsoft.com/ アドオンによる多要素認証のセットアップ手順については、上記アドオン名等で検索していただくか、次の全学IT認証基盤システムの多要素認証マニュアルP.8～の情報を適宜読み替えてください。 https://web.auth.osaka-u.ac.jp/portal/ja/mfa-guide.pdf
14	複数の多要素認証アプリ（複数のスマートフォン等）において、同じメールアドレスの多要素認証設定を行った場合はどうなりますか。	最後に多要素認証のセットアップをした多要素認証アプリ（スマートフォン等）のみ有効になります。
15	学外からVPNで接続する場合、多要素認証は必要ですか。 （事務職員が事務情報ネットワークのVPN端末を使用する場合等）	不要です。 （正確には、VPNによりIPアドレスが133.1.0.0/16の範囲内へ接続する場合で、例えば事務情報ネットワークのVPN端末はこれに該当します）

<p>同じメールアカウントを複数人で使用していますが、この場合はどうすれば良いでしょうか。</p>	<p>学内からアクセスする場合、多要素認証は不要なので、複数人でも技術的には利用可能です。 (但し情報セキュリティの観点からは、複数人で同じパスワードを共有することになるので一般的には推奨されません)</p> <p>学外からのアクセスであれば、多要素認証が必要になりますが、多要素認証は一つの認証アプリ（スマートフォン等）でしか利用できません。</p> <p>よって、この場合は例えば次のような運用対処をご検討ください。</p> <ul style="list-style-type: none">・1名は多要素認証設定で、残りはメール転送等によりメールの受信のみ行う（送信作業は、多要素認証を設定している1名に集約する）・Webメールではなくメールクライアント（Outlook, Thunderbird等。多要素認証不要）を利用し、アカウントをIMAPで設定する・メールクライアント設定マニュアル：https://www.mail.osaka-u.ac.jp/files/manual-mailclient.pdf・IMAPについての参考サイト：https://pr.toriatez.jp/navi/howto/2117.html <p>なお、再掲となりますが、情報セキュリティの観点からは、複数人で同じパスワードを共有することになり一般的には推奨されないため、この機会にアカウントの運用自体の見直しもご検討いただけますと幸いです。</p>
---	--