多要素認証の導入に関するご案内【重要】

2024 年 12 月　情報センター

本学では 2025 年度より、MAIN アカウントを用いた学内サービスを利用する上で多要素認証を求める運用を、全学的に取り入れることを決定致しました。多要素認証とは、各サービスへログインする際に、ID/PW に加えもう一つの認証手順を求められる仕組みのことを指します。

事前にご自身による認証方法の登録を行うことが必要となり、登録を行うことで本学の各サービスの利用が開始できるようになります。

MAIN アカウントのご利用者は、速やかに認証方法の登録をご対応頂くよう、ご協力の程宜しくお願い致します。

本学の多要素認証について(登録手順含む)は、以下オンラインガイドをご参照ください。
オンラインガイド URL：https://tr.mguolg.info/i00/mfa

QR コードを読み取ることで
もアクセスいただけます

■多要素認証の導入に関する詳細について

<導入スケジュール及び適用サービス>

① 2025 年 4 月 1 日より適用開始するサービス

・適用サービス名：Microsoft365 関連サービス
（Exchange Online(MG メール),OneDrive,Teams,Stream,Word,Excel,PowerPoint,AVD(仮想 PC 実習室)等）

② 2025 年 5 月中旬より適用開始するサービス

・適用サービス名： manaba（LMS／学習管理システム）

③ 2025 年 7 月 1 日より適用開始するサービス

・適用サービス名：教務システム

※尚、各サービスにおいては、順次多要素認証の展開を進めております。現時点で多要素認証が問われないサービスに関しても今後実装を予定していることご承知おきください。
※2024 年度時点で既に申請により有効としている方は、上記サービス全体を対象に既に有効となっております。

<本学における多要素認証とは>

以下要件を満たした場合のみ、多要素認証を要求する仕様としております。
認証方法に関しては、別紙「【参考資料】認証方法(利用者による選択)」をご参照ください。

・学外ネットワークからのログイン時のみ多要素認証を要求します。

- 学外ネットワークとは、ご自宅の回線やキャリア/公衆 Wi-fi から接続することを指します。
- 学内 Wi-Fi(1863-hepburn)接続時は、基本的に要求されません。

※但し、Microsoft の定める規則に基づくリスク判定となる為、学内 Wi-Fi 環境であっても要求されることがあります。

- 学内 Wi-Fi(Eduroam)接続時は、要求されます。
※Eduroam は国立情報学研究所(NII)が展開する学外ネットワークとなります。

・多要素認証が求められる頻度は「90 日間隔」となります。

※但し、Microsoft の定める規則に基づくリスク判定となる為、普段と異なる端末やブラウザ、場所(国や都道府県)、により 90 日以内でも認証を問われることがあります。

・推奨設定について

複数の認証方法を登録することが可能な為、状況に応じて使い分けた認証を行うことが可能となります。１つの方法でも対応可能ですが、携帯電話の紛失、機種変更、アプリ上の誤操作により、認証を受け取ることができなくなるケースが生じることもある為、代替手段として、複数の認証方法（複数の機器による設定）を組み合わせた登録を推奨しております。

・認証デバイスの紛失等によるリセット処理について

認証デバイスの紛失や機種変更等による移行により、各々の操作ができなくなってしまった場合、各キャンパスの情報センターにて再登録を行うことが可能となります。
セキュリティ観点における施策となる為、原則、ご本人の確認をさせて頂いた後にリセット処理を実施致しますので、お近くの情報センター窓口へお越しください。

尚、以下フォームへ事前に取り交わす「合言葉」をご登録頂くことで、遠方より電話による解除の手続きを受け付けることを可能としておりますのでご活用ください。
受付 URL：https://forms.office.com/r/KQ1P3ppCdP

・多要素認証の一時的な回避策について

海外出張等をはじめ、異なる環境（場所、所有機器の状況）等からのアクセスも考えられるため、多要素認証のプロセスを一時的に停止する措置を検討しております。
事前に期日・期間を指定した申請を行うことにより、多要素認証のプロセスを回避する措置を講じたいと考えておりますが、セキュリティ環境は低くなる為一時的な措置として検討しておりますので、お近くの情報センター窓口へご相談ください。
※最長の申請可能期間は、1 年間程度を想定。(サバティカル期間を考慮した期間設定)

・日本国外出張時に関する留意事項

□海外出張等による国外での利用の際は、ショートメールや電話番号による着信ができない場合があります。
国際ローミングサービス等で国外でのショートメールや電話番号機能を利用できる状態とすること、もしくは、Wi-Fi 接続が可能な認証方法(スマートフォンアプリや PC アプリ)を事前に登録することで継続してご利用頂けます。

□登録している認証方法別に、継続してご利用頂くためのいずれかの対処方法を記載致します。

① 携帯電話(スマートフォン・フィーチャーフォン)・固定電話への着電による通知

・国際ローミングサービス等で国外でのショートメールや電話番号機能を利用できるサービスを利

用ください。
・現地で利用可能な携帯電話を調達する場合は、レンタルする電話番号を事前に登録ください。
※複数の電話番号を登録することが可能です。
・スマートフォンアプリか PC アプリによるネットワーク通信による認証方法を登録ください。

② 携帯電話番号ショートメール(SMS)へのワンタイムパスワード着信による通知
・①の対処方法と同様となります。

③ スマートフォンアプリ(Microsoft Authenticator)による通知
・スマートフォンにて、ネットワーク通信(キャリア通信や Wi-Fi 通信)が可能な状態としてください。

④ PC アプリ(Windows/Mac 各 OS)による通知
・PC にて、ネットワーク通信(有線 LAN や Wi-Fi 通信)が可能な状態としてください。

皆様のご理解とご協力の程宜しくお願い致します。

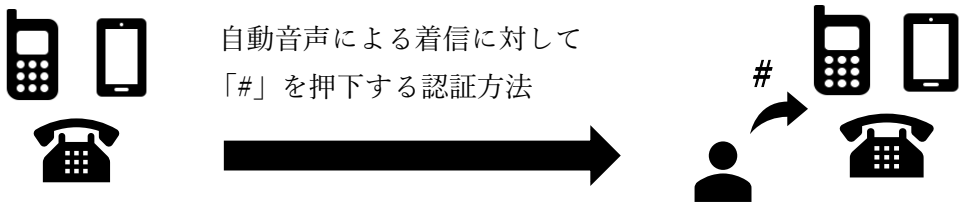
以上

別紙

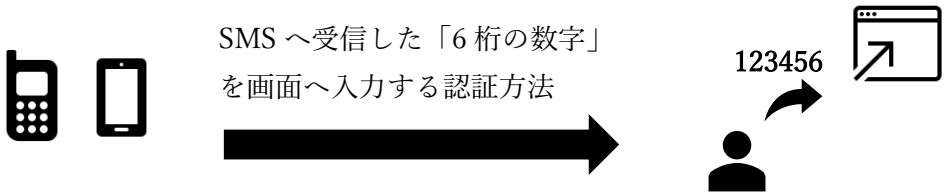
・【参考資料】認証方法(利用者による選択)

以下のいずれかを選択することで多要素認証が利用可能となります。
オンラインガイド URL：https://tr.mguolg.info/i00/mfa

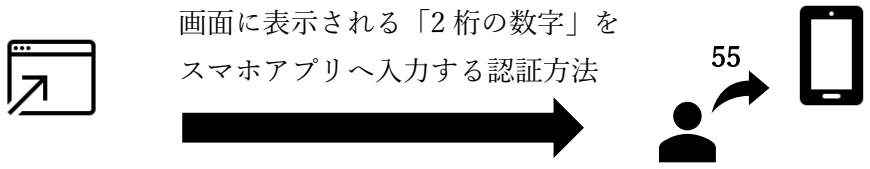
① 携帯電話(スマートフォン・フィーチャーフォン)・固定電話への着電による通知
⇒電話番号による着信(キャリア通信)が可能な環境をご準備ください。



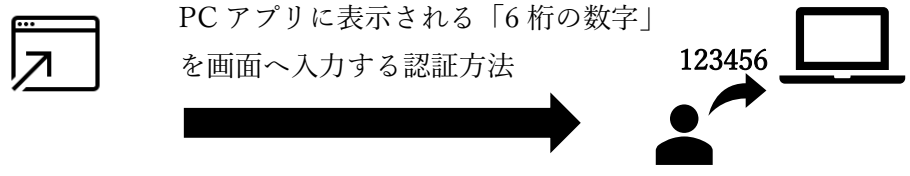
② 携帯電話番号ショートメール(SMS)へのワンタイムパスワード着信による通知
⇒携帯電話にて、ショートメール(SMS)による着信(キャリア通信)が可能な環境をご準備ください。



③ スマートフォンアプリ(Microsoft Authenticator)による通知
⇒スマートフォンにて、ネットワーク通信(キャリア通信や Wi-Fi 通信)が可能な環境をご準備ください。



④ PC アプリ(Windows/MacOS)による通知
⇒PC にて、ネットワーク通信(有線 LAN や Wi-Fi 通信)が可能な環境をご準備ください。



以上