KOMAnet アカウント(Googleアカウント)対象 2段階認証プロセスの設定ガイド

総合情報センター 2025.03.27 Ver1.1

2段階認証プロセスについて

• 2段階認証プロセスとは

従来のIDとパスワードによるログインに加え、Googleからのメッセージ等を使用して本人確認を行う方法です。これにより、アカウント情報が漏洩した場合でも、不正アクセスを防ぐことが可能となります。

目的

この新たな認証方法は、学内のシステムやデータを保護し、外部攻撃から守るための重要な対策となります。

設定方法

① 2段階認証プロセス設定ページを開く

Gmail等のGoogleアプリを開き、画面右上に表示されている自身のアイコンから「Googleアカウントを管理」を選択してください。その後、セキュリティ>Googleにログインする方法>2段階認証プロセスを選択してください。

② 2段階認証プロセスを有効にする

1. 2段階認証に使用するデバイスについて

登録したデバイスに2段階認証の本人確認メッセージを送信します。自身のア カウントでログイン済みのデバイスが登録されています。デバイスが一覧にな い場合は、画面の案内に従って追加してください。

※個人スマートフォンを利用しない場合は、大学の番号を登録し、音声通話によるコード取得 を選択してください。

なお、複数アカウントが同じ電話番号で設定する場合、一定時間内に設定できるアカ ウント数に上限があるようです。エラーとなった場合は、時間を空けて設定してくだ さい。



2. バックアップ方法の登録

1で登録したデバイスが紛失等で使用できない場合、任意の電話番号へのSMS・自動音声通話によるログインコードの 送信を許可します。登録した電話番号に届いたコードを入力し、続行してください。

※バックアップコードによる設定も可能です。個人スマートフォンを利用しない場合は、バックアップコードによる2段階認証を推奨します。

3. 2段階目の認証を追加する

2段階認証を有効にした後、ページ中ほどにある「2つ目の手順を追加してログインを確認する」から認証システムアプリ[※] などの認証方法を追加できます。デバイス買い替えや紛失時 でもログインできるよう、認証方法を追加することを推奨しま す。

※Google Authenticator、Microsoft Authenticatorなど。AndroidやiOS のアプリストアからインストールできます。





① 信頼できるデバイスについて

ログイン時に、「このデバイスでは次回から表示しない」にチェックしログインすることで、次回から2段階認証プロセスをスキップすることができます。よく利用する端末はチェックすることを推奨します。

Google からお使いの Google Pixel 7a に通知を送信 を行うには、通知で [はい] をタップします。

または、iPad で Gmail アプリを開き、そこで本人研

✓ このデバイスでは次回から表示しない

② PC教場、貸出PCの利用について

教場のPC等は、ログアウトするとPCの設定が復元されるようになっています。2段階認証プロセスの仕様上、このようなPC はGoogleアカウントにログインする度に2段階認証が必要となります。万がースマートフォンを忘れたり紛失したなどで2段階 認証が行えない場合、総合情報センターにお問い合わせください。

③認証するデバイスの変更について

買い替え等で2段階目の認証を行うデバイスを変更する場合は、新デバイスでログインを実施し、初期化・破棄する前に旧デ バイスで2段階認証を行ってください。もしくは、2-bのバックアップ方法、2-cで追加した方法で認証を行ってください。

④ 共有アカウントに適用する場合

共有アカウントは個人スマートフォンに紐づけると不便なため、2-aにおいて大学の電話番号を入力し、設定を進めてください。2段階目の認証については、利用者間でバックアップコードを共有するか、認証システムアプリ[※]をご利用ください。

※Googleが発行するQRコードを認証システムアプリで読み込むことで利用できます。認証システムに読み込ませGRコードが同じであれば、ユー ザーを問わず複数の端末か22段階認証が可能です。

※2段階認証プロセスの共有アカウントへの適用は必須ではありません。ただし、共有アカウントにもデータを保管している場合が多いた 必段階認証 プロセスを設定いただきますよう、ご協力をお願いいたします。

参考サイト: Googleアカウントヘルプ「2段階認証プロセスを有効にする」