

Google 2段階認証 設定方法

Gmail をメーラーなど pop で受信する場合は 2 段階認証の設定を推奨しています。2 段階認証の詳しい説明は下記 URL をご参照ください。

<https://www.google.com/landing/2step/>

本資料では

- ・ 2 段階認証の設定を有効にする
- ・ 2 段階認証が有効になった状態での、他端末でのログイン方法
- ・ pop で受信するアプリケーション固有のパスワードを生成する
- ・ 2 段階認証の設定を有効にする

の手順について記載しています。

1 2段階認証の設定を有効にする

1.1 ご自身の Google メールアカウントにログインします。

<https://mail.google.com/a/xxx.teikyo-u.ac.jp/> ※xxx の箇所は各ドメイン



1.2 画面右上に表示されている、自身のメールアドレスをクリックし、「アカウント」をクリックします。



1.3 セキュリティの項目を選択し、パスワード欄にある「2段階認証プロセス」の「設定」をクリックします。



- 1.4 2段階認証プロセスの説明が表示されるので、画面右側の「設定を開始」をクリックします。



- 1.5 まず 2 段階認証の時に使用する確認コードを受け取るための方法と携帯端末の設定を行います。確認コードの受け取りはメール又は音声通話を選択できます。お好きな方をお選びください。

■メールでの受け取り方法

- A) 「コードの受け取り方法」で「テキストメッセージ(SMS)」をチェックし、その後で携帯のメールアドレスを入力しご利用の携帯キャリアに合わせてドメイン名を選択して下さい。そして「コードを送信」ボタンをクリックして下さい。

携帯端末を設定する

1 2 3 4

どの電話番号にコードを送信しますか？

信頼できないパソコンや端末からログインすると、お使いの携帯端末に Google から数字のコードが送信されます。

携帯電話のメール アドレス

* * @ docomo.ne.jp

このアドレスは、アカウントのセキュリティ保護に役立ちます。データ通信料金がのりも場合が異なります。

コードの受け取り方法

テキストメッセージ(携帯電話のメール)

音声通話

戻る コードを送信

- B) 入力した携帯電話のメールアドレス宛てに確認コードが記載されたメールが「noreply@google.com」より送信されてきます。
メールは数分以内に送られてきますが、届かない場合は迷惑メール対策設定などがされていないか、確認してください。



- C) 確認コードを入力し、「確認」ボタンをクリックします。次の画面が表示されることを確認します。



■ 音声通話での受け取り方法

A) 「コードの受け取り方法」で「音声通話」をチェックし、その後で電話番号を入力して下さい。そして「コードを送信」ボタンをクリックして下さい。入力した電話番号に非通知で着信があります。

B) 電話に出ていただくと確認コードが自動応答で再生されます。

携帯端末を設定する

1 2 3 4

どの電話番号にコードを送信しますか？

信頼できないパソコンや端末からログインすると、お使いの携帯端末に Google から数字のコードが送信されます。

電話番号 例: 070-1234-5678

• Google はこの番号をあなたのセキュリティ保護にのみ使用します。
• 文字列が数回入力できない場合があります。

コードの受け取り方法

テキスト メッセージ (携帯電話のメール)

音声通話

C) 再生された確認コードを入力し、「確認」ボタンをクリックします。次の画面が表示されることを確認します。

携帯端末を確認する

1 2 3 4

コードをお知らせする電話を 0■■■■宛てにおかけします

確認コードを入力してください

123456

確認コードは6桁です。

コードを取得していない場合

1.6 正しい確認コードが入力されると、以下画面が表示されます。

この画面で「このパソコンを信頼できるパソコンとして登録する」にチェックをすると現在使用されているパソコンが信頼できるパソコンとして保存されます。その場合、このパソコンからは2段階認証を行なわなくても通常のユーザー名とパスワードによる認証だけでログインが可能となります。他の人のパソコンを借りて設定している場合や、常に2段階認証を行なうようにする場合はチェックを外して下さい。

※ 設定は Cookie に保存されます。よって同じパソコンでもブラウザが異なれば2段階認証によるコードの入力が必要となります。また Cookie を削除されると「信頼できるパソコン」の設定は削除されます。

このパソコンを信頼しますか？

1 ————— 2 ————— 3 ————— 4

信頼できるパソコンや端末で確認コードの入力が求められるのは 30 日に 1 回だけです。

携帯端末を紛失しても、信頼できるパソコンから確認コードを入力せずにアカウントにアクセスできる場合があります。このパソコンのアクセス権限を持つユーザーを信頼できる場合にのみ、信頼できるパソコンとして登録することをおすすめします。

このパソコンを信頼できるパソコンとして登録する
信頼できるパソコンの設定は、Google アカウント設定画面でいつでも変更できます。

« 戻る **次へ »**

1.7 最終確認画面が表示されますので、「確認」をクリックします。

確認

1 ————— 2 ————— 3 ————— 4

2 段階認証プロセスを有効にする

信頼できるパソコンや端末から `it-house_test@it-house.teikyo-u.ac.jp` アカウントを使用してログインする際にコードの入力が求められるのは、30 日に 1 回だけです。

携帯端末を紛失した場合は、アカウント設定で情報をいつでも変更できます。

2 段階認証プロセスの確認コードの受け取りにサードパーティの音声データプロバイダを利用する場合は、2 段階認証プロセスとともに使用されるサービスに Google Apps SLA (サービスレベル契約) は適用されません。SLA については、こちらをご覧ください。

« 戻る **確認**

- 1.8 2段階認証プロセスの画面が表示されます。これで設定は完了し、対象の Google アカウントで 2 段階認証が有効となりました。

2 段階認証プロセス

確認コード	アプリ固有のパスワード	登録済みデバイス
メインのコード受け取り方法		
	メインの電話番号 0 [redacted]	編集
	コードの送信方法: 追加日	音声通話 2014/09/03

2 段階認証プロセス: 有効
2014/09/03 に保護アカウントを保護しています。
[無効にする](#)

2 2段階認証が有効になった状態での、他端末でのログイン方法

2段階認証が有効の状態、認証されていない端末でのログインする場合、再度確認コードが発行されます。その際の説明をします。

2.1 メールシステムへアクセスし、ログイン ID（メールアドレス）、パスワードをそれぞれ入力します。

2.2 2段階認証のプロセスとして確認コードの入力を求められます。

※確認コードは2段階認証の設定時に選択した受け取り方法で通知されます。

「音声通話」を選択した場合には登録した電話番号宛てに電話があり、自動応答メッセージで確認コードが流れます。「テキストメッセージ」を選択した場合には登録したメールアドレス宛てに確認コードが含まれるメールが送信されてきます。

2.3 電話又はメールにて通知があった確認コードを入力して下さい。入力が終わったら「確認」をクリックして下さい。



2段階認証プロセス

コードがまだ届かない場合 [コードの再送信](#)

コードをお知らせするための通話が次の電話番号に発信されました:
__***

123456|

確認

このパソコンの情報を 30 日間保持する

「このパソコンの情報を 30 日間保存する」にチェックをした状態でログインに成功すると、このパソコンは信頼できるパソコンとして保存され次回からは確認コードの入力が不要となります。

- 2.4 確認コードを受け取るためのバックアップ用電話番号などを登録していない場合は次のような画面が表示されることがあります。今回は省略しますので「後で通知」と書かれたリンクをクリックしておいて下さい。

アカウントにアクセスできなくなることを防ぐため、バックアップコードを取得してください

旅行中など端末を使用できない場合でも、アカウントにアクセスできるようにしてください。2段階認証プロセスのバックアップコードを取得しましょう。

ほんのわずかな時間で、バックアップコードセットを印刷またはダウンロードできます。

1. 下の [設定画面に移動] ボタンをクリックしてください
2. [バックアップ オプション] まで下にスクロールします
3. [バックアップ コード] に記載されている手順を行います

完了です！

[詳細](#)



- 2.5 メールシステムへのログインが完了しました。



このように2段階認証が有効になっている場合、(1)ユーザー名とパスワードでログイン、(2)確認コードを取得して入力、という2段階のログイン作業が必要となります。確認コードをどのように取得するのかは、事前に設定した電話番号やメールアドレスになります。また、Android や iPhone などのスマホアプリを使って確認コードを取得できますが、本資料では省略させていただきます。

3 アプリケーション固有のパスワードの取得

Google アカウントにアクセスする一部のアプリケーション（携帯端末の Gmail や Outlook など）では、確認コードの入力を求められません。このようなアプリケーションを使用するには、確認コードを使用せず、通常のパスワードの代わりにアプリケーション固有のパスワードを入力します。アプリケーション固有のパスワードが必要な一般的なアプリケーションや端末は次のとおりです。

- POP/IMAP メール クライアント（Outlook、Mail、Thunderbird など）
- スマートフォンの Gmail や Google カレンダー
- Windows Mobile や iPhone 用の ActiveSync
- YouTube モバイル

通常、アプリケーション固有のパスワードは、2 段階認証プロセスを有効にした後で、アプリケーションや端末ごとに 1 回だけ入力すれば済みます。

- 2.1 2 段階認証に関する設定画面を表示します。画面右上に表示されている、自身のメールアドレスをクリックし、「アカウント」をクリックします。



- 2.2 「セキュリティ」の項目の「2 段階認証プロセス」から「設定」をクリックします。



- 2.3 「アプリ固有のパスワード」タブをクリックします。画面下部の「アプリケーション固有のパスワードの管理」と書かれたリンクをクリックします。この際、再度パスワードを求められる場合がありますので入力してください。

2段階認証プロセス



- 2.4 アプリケーション固有のパスワードは使用するアプリケーション毎に作成します。今回は「Windows パソコンのメール」を選びました。選択肢には「その他（名前を入力）」もあり、自分で名称を設定することもできます。名称を入力したら「生成」をクリックします。



- 2.5 アプリケーション用のパスワードが生成されました。パスワードは各アプリケーションで今まで Google アカウントのパスワードを入力していた箇所に代わりに入力して下さい。2 段階認証を有効にした後でもアプリケーションから Google サービスが利用できるようになります。



- 2.6 生成されたパスワードは次のように一覧で表示されます。アプリケーション毎に複数生成することができます。また、使用しなくなったパスワードは速やかに「取り消し」をクリックして破棄することをおすすめします。



3 2段階認証設定を無効にする

3.1 2段階認証はいつでも無効にすることができます。

2段階認証に関する設定画面を表示します。画面右側に2段階認証が有効かどうか表示されています。無効にされる場合は「無効にする」と表示されたリンクをクリックして下さい。



3.2 無効化の確認画面が表示されます。2段階認証を無効にして宜しければ「無効にする」ボタンをクリックして下さい。2段階認証が無効となります。(「2段階認証プロセスの設定も消去する」にチェックが入っていると確認コードなどを取得するために設定した電話番号などの情報も全て消去されます)。



以上で2段階認証の設定が無効になりました。