画像付き操作マニュアル

Googleアカウントの安全設定

自分専用の端末にパスキーを作り、2段階認証と予備のログイン手段を整えます。スマートフォンをなくしても困らないよう、復旧情報も一緒に確認しましょう。

個人用Googleアカウント向け PCを基本に AndroidとiPhoneも補足

目標 普段は安全にログインし、端末をなくしたときは別の方法で入れる状態にする。

この順番で設定します

1 **復旧情報を確認**
再設定用メールと電話番号 — 3・4ページ

2 **2段階認証を有効化**
普段使う本人確認方法も確認 — 5・6ページ

3 **バックアップコードを保管**
主な端末と別の場所に保管 — 7ページ

4 **パスキーを作成**
自分専用のPC・スマートフォン — 8・9ページ

5 **予備を整えて点検**
物理キー・アプリ・SMS・端末 — 10〜15ページ

用語 パスキーは端末等で使うログイン用の鍵。物理キーはUSB・NFC等の機器。バックアップコードは使い切りの予備コードです。

図は公式手順に基づく説明図で、実際のGoogle画面のスクリーンショットではありません。アカウントやOSにより表示は異なります。実アカウントでの設定変更・ログイン試験は行っていません。

出典 [01] [02] [03] [04] [12]

準備

設定するアカウントを確認する

まず公式の設定画面を開きます。複数のアカウントを持っている場合は、設定先の取り違えを防ぎます。

Googleアカウント → セキュリティとログイン
https://myaccount.google.com/security

図 1 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **自分専用の端末を用意** OSとブラウザを更新し、画面ロックを有効にします。端末のPINやパスワードは他人に教えません。
2. **公式ページを開く** ブラウザのアドレス欄に myaccount.google.com と入力します。必要なら設定するアカウントでログインします。
3. **アカウントを確認** 右上のプロフィール画像や丸いアイコンを開き、メールアドレスが設定したいものか確かめます。
4. **セキュリティ画面へ進む** 「セキュリティとログイン」を選びます。「セキュリティ」と表示される場合もあります。

確認 設定したいアカウントで、セキュリティの設定画面を開けた。

覚えておくこと 対象は個人用Googleアカウントです。職場・学校・お子様用では設定や権限が異なります。図は説明用に再構成しており、実画面の配置・文言は環境で変わります。

出典 [01] [02] [12]

復旧情報 1

再設定用のメールアドレスを登録する

ログインできなくなったときに備え、別のメールアドレスを登録します。そのメール自体にログインできることが大切です。

セキュリティとログイン → Googleにログインする方法 → 再設定用のメールアドレス
https://myaccount.google.com/security

図 2 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **再設定用メールの項目を開く** 「再設定用のメールアドレス」を選び、求められたら本人確認を行います。
2. **別のメールアドレスを入力** このGoogleアカウントのログイン用アドレスとは異なり、普段確認できるものを入力します。
3. **確認メールで本人確認** 入力したメールの受信箱を自分で開き、確認コードなど画面で指示された方法で登録を完了します。
4. **登録状態を確認** 設定画面に戻り、登録したアドレスの表示と、確認待ちになっていないことを確かめます。

確認 別のメールを受信でき、再設定用メールとして登録されている。

覚えておくこと 復旧先のメールにもパスキーや2段階認証を設定しましょう。同じスマートフォンでしか開けない状態を避け、別の端末から使う方法も確認しておきます。

出典 [04] [05]

復旧情報 2

再設定用の電話番号を登録する

現在使っている、自分で管理する携帯電話の番号を登録します。古い番号が残っていないかも確認します。

セキュリティとログイン → Googleにログインする方法 → 再設定用の電話番号
https://myaccount.google.com/security

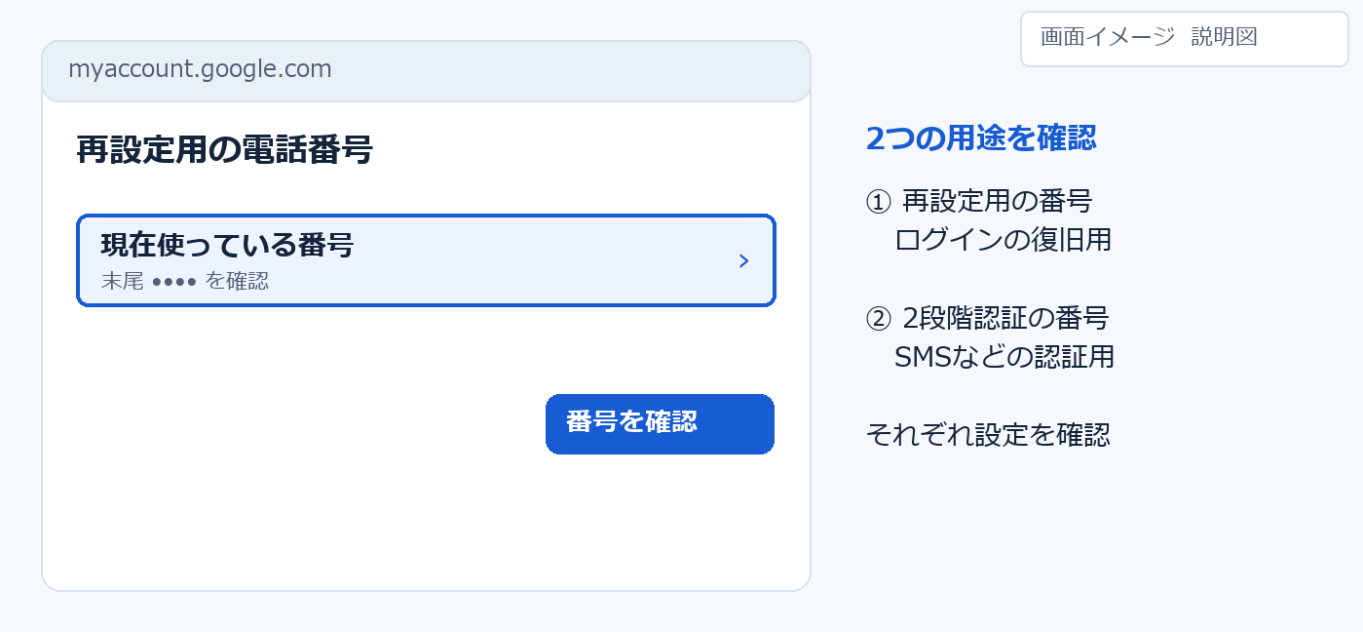

図 3 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **電話番号の項目を開く** 「再設定用の電話番号」を選び、必要な本人確認を行います。
2. **番号を登録または変更** SMSを受け取れる自分の携帯電話番号を入力します。国・地域と番号の形式を画面で確認します。
3. **SMSなどで確認を完了** 自分で開始した操作で届いた確認コードを、開いているGoogleの本人確認画面に入力します。
4. **現在の番号か確認** 登録後の表示を確認します。番号を変えたら、12ページの2段階認証用の番号も別に確認します。

確認 現在SMSを受け取れる番号が、再設定用の電話番号になっている。

覚えておくこと 再設定用の番号と、2段階認証でSMSを受け取る番号は用途が異なります。一方を更新しただけで、両方の確認が済んだと思わないようにします。

出典 [04] [05] [09]

基本設定

2段階認証を有効にする

パスワードでログインする場合に、もう一つの本人確認を加えます。最後に「有効」の状態まで確認しましょう。

セキュリティとログイン → Googleにログインする方法 → 2段階認証プロセス
https://myaccount.google.com/signinoptions/two-step-verification

図 4 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **2段階認証の項目を開く** 「2段階認証プロセス」または「2段階認証プロセスを有効にする」を選びます。
2. **使う本人確認方法を設定** 画面の案内に従い、Googleからのメッセージ、パスキー、セキュリティキーなど利用できる方法を設定します。
3. **有効化まで完了する** 本人確認を済ませ、「有効にする」など最後の操作まで進みます。確認方法を追加しただけで終えないようにします。
4. **予備の方法を追加** 有効になったことを確認し、7ページでバックアップコードを取得します。主な端末以外の手段も用意します。

確認 2段階認証が有効で、普段使う方法と予備の方法を確認できた。

覚えておくこと パスキーでログインすると、追加の認証手順が省略されます。コードが出ないだけでは無効とは判断できません。設定画面の状態を確認します。

出典 [01] [02] [03]

スマートフォンでの本人確認

Googleからのメッセージを確認する

ログイン済みのスマートフォンに届く確認通知を使います。自分が今始めたログインだけを承認します。

2段階認証プロセス → Googleからのメッセージなどの確認項目
https://myaccount.google.com/signinoptions/two-step-verification

図 5 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **受け取るスマートフォンを確認** Androidでは対象のGoogleアカウントにログインします。iPhoneではGmailやGoogleなど対応アプリにログインします。
2. **通知を受け取れる状態にする** スマートフォンをインターネットに接続します。通知設定も確認し、画面ロックを有効にします。
3. **自分のログインで通知を確認** 別のウィンドウなどからログインを始め、通知が出たら端末・時刻などを確認します。番号照合があれば照らし合わせます。
4. **心当たりがある場合だけ承認** 自分の操作だと確認できたときだけ承認します。始めていないログインは「いいえ」などで拒否します。

確認 自分のスマートフォンで通知を受け取れ、承認する条件が分かった。

覚えておくこと これはSMSとは別の仕組みです。通知を連打されても承認しません。表示場所は概算の場合があるため、場所だけで本人の操作か決めないようにします。

出典 [01] [08]

予備のログイン手段 1

バックアップコードを発行して保管する

スマートフォンが使えないときに備える、使い切りの予備コードです。「バックアップキー」と混同しないよう区別します。

セキュリティとログイン → 2段階認証プロセス → バックアップコード
https://myaccount.google.com/signinoptions/two-step-verification

図 6 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **2段階認証を有効にしておく** 5ページで有効化を済ませます。バックアップコードの項目を開き、必要なら本人確認を行います。
2. **コードを取得する** 「バックアップコードの取得」などを選びます。通常は8桁のコードが10個発行されます。
3. **紙などで安全に保管** 印刷し、スマートフォンとは別の、重要書類を置くような場所に保管します。ダウンロードした場合も保存先を管理します。
4. **使い方と更新方法を確認** ログイン時に「別の方法を試す」からバックアップコードの方法を選び、未使用のコードを1個入力します。

確認 コードを取り出せる場所に保管し、1個につき1回だけ使えると分かった。

覚えておくこと 新しいセットを発行すると古いセットはすべて無効になります。紛失・流出が疑われる場合は再発行します。コードをメール・チャット・このマニュアルに書き込まないでください。

出典 [03]

パスキー 1

パソコンにパスキーを作成する

指紋認証・顔認証・端末のPINなどでログインする方法です。自分専用で、ロックを管理できるパソコンに作成します。

セキュリティとログイン → Googleにログインする方法 → パスキーとセキュリティキー
https://myaccount.google.com/signinoptions/passkeys

図 7 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **パスキーの設定を開く** myaccount.google.com/signinoptions/passkeys を開き、設定対象のアカウントで本人確認を行います。
2. **パスキーの作成を選ぶ** 「パスキーを作成する」などを選びます。保存先の選択画面が出たら、この端末・パスワード管理機能などを確認します。
3. **保存先に応じて本人確認** Windows Hello、指紋・顔認証、端末やパスワード管理機能のPINなど、表示された方法で作成を完了します。
4. **登録一覧を確認** パスキーの一覧に追加されたことを確認し、どの端末・管理機能に保存したかを覚えておきます。

確認 自分専用の保存先にパスキーが作成され、登録一覧で確認できた。

覚えておくこと 端末を使ってロック解除できる人は、パスキーも使えるおそれがあります。共有PCには作成しません。パスキーを作っても既存のパスワードや復旧手段は自動では削除されません。

出典 [02] [12]

パスキー 2

スマートフォンにパスキーを作成する

AndroidもiPhoneも、ブラウザから同じ設定ページを開けます。保存先と画面ロックの状態を確認しましょう。

スマートフォンのブラウザ → パスキーの設定ページ
https://myaccount.google.com/signinoptions/passkeys

図 8 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **画面ロックと保存先を準備** OSとブラウザを更新します。iPhone・iPadでAppleの保存機能を使う場合は、iCloudキーチェーンも有効か確認します。
2. **パスキーの設定を開く** ブラウザでパスキーの設定ページを開きます。Androidではすでに自動登録されたパスキーが表示されることもあります。
3. **必要に応じて作成する** 「パスキーを作成する」から、表示される保存先を確認して作成します。指紋・顔認証・画面ロックなどで本人確認します。
4. **別の端末からの使い方も確認** PCで「別の方法を試す」→パスキーを選び、QRコードが出たらスマートフォンで読み取ります。近くでBluetoothも有効にします。

確認 スマートフォンのパスキーを確認し、保存先と予備のログイン方法が分かった。

覚えておくこと 同期されるかどうかは保存先の仕組みによります。同じ同期先だけに頼らず、紙のバックアップコードや別保管の物理キーも用意します。QRコードは自分で開いたログイン画面のものだけ使います。

出典 [02] [14]

予備のログイン手段 2

予備の物理セキュリティキーを登録する

USBやNFCで使う小さな機器です。予備を持つ場合は、2本目もGoogleアカウントに個別登録します。

パスキーとセキュリティキー → パスキーを作成する → 別のデバイスを使用
https://myaccount.google.com/signinoptions/passkeys

図 9 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **対応するキーを用意** パスキーを保存する場合はFIDO2対応が必要です。使うPCやスマートフォンのUSB端子・NFCへの対応も確認します。
2. **キーへパスキーを作成** パスキー作成から「別のデバイスを使用」を選び、セキュリティキーを選択します。接続し、画面の指示に従います。
3. **キーのPINやタッチで確認** 求められた場合はキーのPINを設定・入力し、キーに触れます。2段階認証用として登録する経路では、その画面の案内に従います。
4. **予備も登録し別に保管** 2本目でも同じ登録を行い、「持ち歩き用」「予備」など区別できる名前にします。予備は同じバッグに入れず保管します。

確認 主に使うキーと予備のキーが、それぞれ登録されている。

覚えておくこと 空のキーを買うだけでは予備になりません。「2段階認証の第2の手段として登録」と「キーにパスキーを作成」は役割が異なります。端末のPINとキーのPINも別物です。

出典 [02] [06] [16]

SMS以外の選択肢

認証アプリを予備の方法に追加する

Google認証システムなどで、時間ごとに変わる確認コードを作ります。通信できない場面でもコードを生成できます。

セキュリティとログイン → 2段階認証プロセス → 認証システム
https://myaccount.google.com/signinoptions/two-step-verification

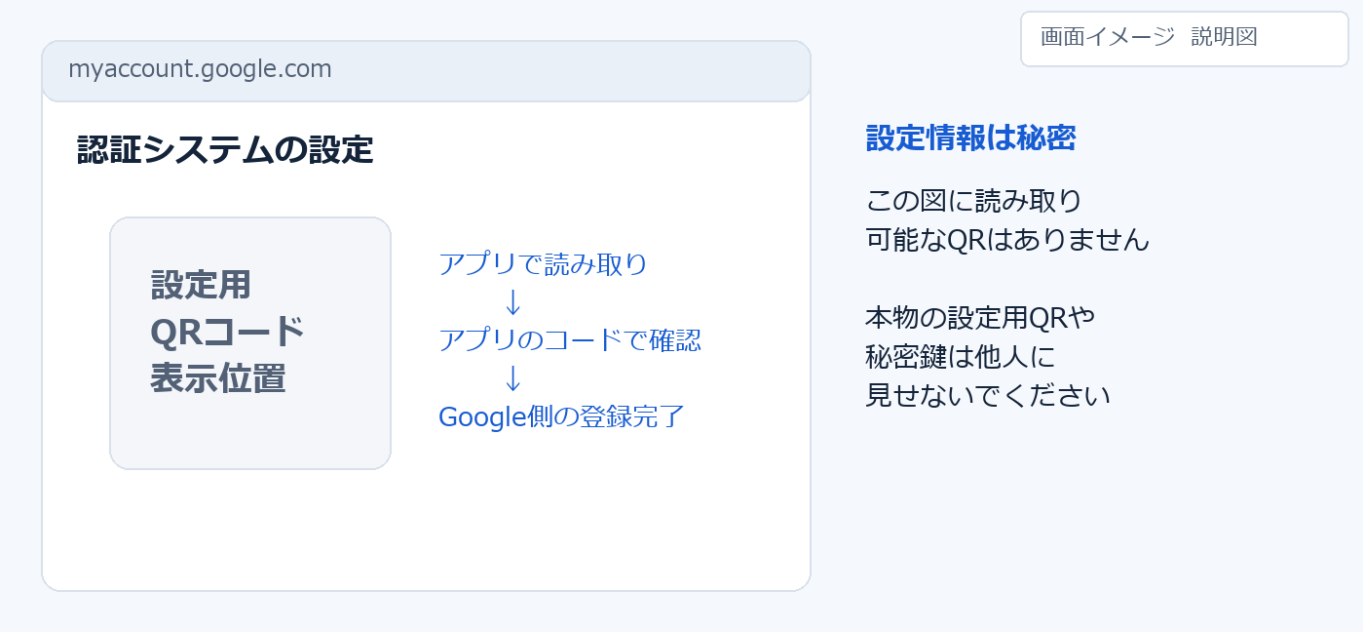

図 10 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **公式のアプリを用意** Google認証システムを使う場合は、Google PlayまたはApp Storeで提供元を確認してインストールします。
2. **認証システムの設定を開始** 2段階認証の設定から「認証システムを設定」などを選びます。PCとスマートフォンを併用すると読み取りやすくなります。
3. **QRコードをアプリで登録** Googleの設定画面に出たQRコードをアプリで読み取ります。同じスマートフォンだけなら、表示される手動設定の案内も確認します。
4. **コードで登録を完了** アプリに表示された確認コードを設定画面へ入力します。認証システムが追加されたことを確かめます。

確認 アプリでコードが生成され、Google側の設定でも登録を確認できた。

覚えておくこと 設定用QRコードや秘密鍵は他人に見せません。コードを同じGoogleアカウントへ同期する場合でも、そのアカウントに入れないとき用の別手段を残します。偽サイトへコードを入力しないことも必要です。

出典 [07] [12]

SMSの位置づけ

2段階認証でSMSを使う設定を確認する

SMSも追加の本人確認に使えます。利用する場合は、パスキーなどを主な方法にし、SMSだけに頼らない構成を目指します。

セキュリティとログイン → 2段階認証プロセス → 電話番号などのSMS受信項目
https://myaccount.google.com/signinoptions/two-step-verification

図 11 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **2段階認証側の番号を開く** 2段階認証の画面で、SMSや音声通話を受け取る電話番号の項目を探します。表示名や選べる方法は環境により異なります。
2. **SMSを受信する番号を設定** 利用する番号を追加・変更し、SMSなど選択可能な方法を選びます。4ページの再設定用番号も別に確認します。
3. **届いたコードで確認** 自分で開始した操作で受信したコードを、開いているGoogleの確認画面に入力し、登録を完了します。
4. **SMS以外でも入れるようにする** パスキー、Googleからのメッセージ、認証アプリ、物理キーなど、使える別の方法とバックアップコードを整えます。

確認 SMS用番号を確認し、SMSが届かなくても使える方法を用意できた。

覚えておくこと SMSは電話番号の乗っ取りや、コードを聞き出す詐欺に弱点があります。知らない確認コードは他人に伝えません。SMSを削除する判断は、別の方法で入れることを確認してから行います。

出典 [01] [09] [12] [14]

仕上げの点検

端末と連携アプリを見直す

ログイン方法を強くするだけでなく、すでにログインしている端末や、データを渡しているアプリも確認します。

セキュリティとログイン → お使いのデバイス ／ サードパーティとの接続
https://myaccount.google.com/security-checkup

図 12 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **セキュリティ診断を開く** myaccount.google.com/security-checkup を開き、注意が必要な項目を一つずつ確認します。
2. **利用端末の一覧を確認** 「すべてのデバイスを管理」で端末・セッションの詳細を確認します。手放した端末や自分のものか不明な接続はログアウトします。
3. **最近の変更を確認** セキュリティ関連のアクティビティで、覚えのないログインや復旧情報の変更がないかを確認します。
4. **アプリとの接続を確認** myaccount.google.com/connections を開きます。サービスと権限を確認し、不要な接続は影響を読んでから解除します。

確認 使う端末とアプリを確認し、心当たりのない変更がないか点検できた。

覚えておくこと 同じ端末に複数のセッションが出ることや、自動同期で時刻が更新されることがあります。接続解除しても相手が保存済みのデータは消えません。使うサービスは別のログイン方法も確認します。

出典 [10] [11] [12] [15]

機種変更と紛失に備える

機種変更は、古い端末を使えるうちに準備します。紛失した場合は、残っている方法でログインして保護を進めます。

ログインできない場合 → Google公式のアカウント復元ページ
https://accounts.google.com/signin/recovery

図 13 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **機種変更の前に準備** 再設定用メール・番号とバックアップコードを確認します。新しい端末でパスキーや認証アプリを使えるか確認してから旧端末を手放します。
2. **紛失時は別の方法を試す** 別端末のパスキー、登録済みの予備キー、パスワードとバックアップコードなど、画面に表示される方法を選びます。
3. **紛失端末のアクセスを止める** ログイン後に紛失端末のセッションをログアウトし、該当パスキーも削除します。Android自動作成分は端末のログアウト手順も確認します。
4. **どの方法でも入れない場合** 公式の復元ページで、普段使う端末・場所から質問に回答します。不正利用が疑われる場合はパスワードや復旧情報も点検・変更します。

確認 主な端末が使えない場合に、次に使う手段と公式の復元先が分かった。

覚えておくこと 一部の新しい認証・復旧情報が使えるまで最長7日ほどかかる場合があります。変更後7日間は以前の復旧先へコードが届く場合もあります。復元の成功や即時反映は保証されません。

出典 [02] [04] [13] [14] [15]

完了チェック

設定後の確認と定期点検

チェック欄には、実際に確認できた項目だけ印を付けます。パスワード・PIN・コードそのものは、この用紙に書きません。

- ☐ **設定先** 目的のGoogleアカウントで操作した。
- ☐ **復旧メール** 別のメールを受信でき、確認が済んでいる。
- ☐ **復旧電話** 現在使う番号で、SMSを受け取れる。
- ☐ **2段階認証** 設定画面で「有効」を確認した。
- ☐ **パスキー** 保存先を確認し、自分専用端末で作成した。
- ☐ **予備手段** 主な端末が使えなくても使える手段を用意した。
- ☐ **コード保管** バックアップコードを主な端末とは別に保管した。
- ☐ **SMS番号** 使う場合、2段階認証側の番号も確認した。
- ☐ **端末とアプリ** 手放した端末や不要な連携を見直した。

ログイン確認 今使える端末のログイン状態を残し、別のウィンドウや端末で、用意した方法が使えるか確認します。使えない場合は既存の手段を消さず、公式の案内を確認します。

定期的に確認すること

機種変更・電話番号変更・復旧メールの変更時に見直します。端末の更新と画面ロック、使い回さないパスワードも続けましょう。

点検日 _____年 ____月 ____日 次回点検 _____年 ____月 ____日

出典 [01] [02] [03] [04] [10] [12] [14]

希望者向けの追加設定

さらに保護を強くしたい場合

狙われるリスクが高い方は高度な保護機能を検討できます。利用条件と、ログインできなくなった場合の方法を先に確認します。

Google 高度な保護機能プログラムの公式案内
https://landing.google.com/advancedprotection/

図 15 説明用に再構成した画面イメージ 実画面の配置や文言は環境で異なります

1. **高度な保護機能の内容を読む** パスキーやセキュリティキーを使うログインに加え、アプリによるデータへのアクセスなどにも制限が加わります。
2. **登録前に予備の手段を準備** 再設定用メール・電話番号、別のパスキーや予備キーを整えます。使っているメールアプリなどへの影響も確認します。
3. **必要な場合だけ登録する** 公式案内の手順に従います。高度な保護機能では、通常のバックアップコードはダウンロードできません。
4. **復元用の連絡先も検討** 設定に表示される場合は「アカウント復元用の連絡先」で信頼できる人を登録できます。再設定用メールとは別で、相手の承諾が必要です。

確認 必要な保護の強さと、利用できる予備・復旧手段を確認できた。

覚えておくこと 復元用の連絡先は、招待が7日間有効で、承諾後も利用開始まで7日かかります。提供状況はアカウント等で異なります。家族や支援者にもパスワード・通常の認証コードを渡さないでください。

出典 [03] [04] [06] [16]

参照資料 1

公式資料と確認範囲

Google公式ヘルプを参照し、一般の個人アカウント向けに手順を整理しました。番号は各ページ下部の出典に対応しています。

[01] 2 段階認証プロセスを有効にする

https://support.google.com/accounts/answer/185839?hl=ja

[02] パスワードの代わりにパスキーでログインする

https://support.google.com/accounts/answer/13548313?hl=ja

[03] バックアップ コードを使用してログインする

https://support.google.com/accounts/answer/1187538?hl=ja

[04] 復元オプションを設定する

https://support.google.com/accounts/answer/183723?hl=ja

[05] 再設定用情報を更新する

https://support.google.com/accounts/answer/17299765?hl=ja

[06] 2 段階認証プロセスにセキュリティ キーを使用する

https://support.google.com/accounts/answer/6103523?hl=ja&co=GENIE.Platform%3DDesktop

[07] Google 認証システムで確認コードを取得する

https://support.google.com/accounts/answer/1066447?hl=ja

[08] Google からのメッセージを使用してログインする

https://support.google.com/accounts/answer/7026266?hl=ja

資料の読み方 各ページ下部の出典番号、またはこの一覧のURLから公式ヘルプを開けます。操作を始める前に、アドレス欄と対象アカウントを確かめてください。

参照資料 2

困ったときの公式資料

設定項目が見つからない場合や、復元・不正利用への対処が必要な場合は、以下の公式資料を確認してください。

[09] Google からテキスト メッセージが届いた場合

https://support.google.com/accounts/answer/3367674?hl=ja

[10] アカウントにアクセスしたデバイスを確認する

https://support.google.com/accounts/answer/3067630?hl=ja

[11] Google アカウントと他のデベロッパーのアプリとのリンクを管理する

https://support.google.com/accounts/answer/13533235?hl=ja

[12] アカウントのセキュリティを強化する

https://support.google.com/accounts/answer/46526?hl=ja

[13] Google アカウントや Gmail を復元する方法

https://support.google.com/accounts/answer/7682439?hl=ja

[14] 2 段階認証プロセスに関する一般的な問題を解決する

https://support.google.com/accounts/answer/185834?hl=ja

[15] ハッキングまたは不正使用された Google アカウントを保護する

https://support.google.com/accounts/answer/6294825?hl=ja

[16] 高度な保護機能プログラムに関するよくある質問

https://support.google.com/accounts/answer/7539956?hl=en

確認日と限界 2026年10月26日に公開されている公式資料を確認しました。これは資料の確認日で、Googleの更新日ではありません。認証後の実画面・各機種の動作は未検証です。

本書は独自に作成した解説資料で、Googleの公式マニュアルではありません。図中のメールアドレス等は架空・マスク表記です。秘密情報の記入欄は設けていません。