セキュリティ チェックリスト



家の戸締まりのように、
スマホとアカウントを見直しましょう。

使っているサービスだけ、ひとつずつ。
確認できたらチェックを付けてください。

まずは、今日やることを絞ろう

- iPhone・iPadの人：01で2ファクタ認証と電話番号を確認します。
- Googleを使う人：02のセキュリティ診断から確認します。
- どの端末でも：03でOSとアプリの更新を確認します。
- iPhoneの設定を終えたら：01の盗難デバイスの保護を確認します。

全14セクション・106項目。使っていないサービスは飛ばしてください。
元の内容：2026年10月29日版 ／ デザイン更新：2026年11月2日
ニュースは記載日時の情報です。現在の状況は各サービスの公式情報で確認してください。

全体を見渡して、必要なところから

安全のための14のポイント

黄色の「詳細」から、チェックと設定の手順に進めます。

スマホとログインを整えよう

01 Apple Accountを守ろう

詳細 → 03ページ

2ファクタ認証と、復旧・盗難時の備えを確認します。

02 Googleアカウントを守ろう

詳細 → 06ページ

診断から、ログインと復旧の設定を見直します。

03 OSとアプリを最新にしよう

詳細 → 10ページ

OS・ブラウザ・アプリを更新し、自動更新を確認します。

04 パスワードの使い回しをやめよう

詳細 → 12ページ

同じパスワードを使い回しているサービスを見直します。

05 パスワード管理アプリを決めよう

詳細 → 13ページ

パスワードの保存先と、困ったときの備えを確認します。

06 パスキーの使い方を確認しよう

詳細 → 14ページ

パスキーの基本と、機種変更時の考え方を確認します。

よく使うサービスを見直そう

07 LINEを守ろう

詳細 → 15ページ

ログイン許可、パスコード、連携アプリを見直します。

08 買い物のアカウントを守ろう

詳細 → 16ページ

買い物に使うサービスの認証とログインを確認します。

09 宅配便の偽通知に備えよう

詳細 → 18ページ

荷物の通知に見せかけた偽SMS・メールに備えます。

10 旅行のアカウントを守ろう

詳細 → 20ページ

予約・航空会社のアカウントと、偽の案内に備えます。

11 SNSのアカウントを守ろう

詳細 → 22ページ

各SNSの認証、ログイン状況、連携アプリを確認します。

12 Notionの設定を見直そう

詳細 → 24ページ

ログイン方法と、ページの共有・公開範囲を確認します。

詐欺とその他の設定に備えよう

13 詐欺の手口と対処を確認しよう

詳細 → 26ページ

よくある手口と、被害が疑われるときの相談先を確認します。

14 その他の設定と証券口座を見直そう

詳細 → 30ページ

ChatGPT、不要なアカウント、SBI証券の設定を確認します。

全14セクション・106項目

使わないサービスは、飛ばして大丈夫です。

01 Apple Accountを守ろう

iPhone・iPadを使う人

Apple Accountが乗っ取られると、写真・支払い・「探す」機能まで影響します。（Apple）

☐ 2ファクタ認証がオンか、確かめておこう

公式情報：Apple

① 設定 > [自分の名前] > サインインとセキュリティ
② 「2ファクタ認証」をタップ
新しい端末でサインインするとき、パスワードに加えて、6桁の確認コードが必要になります。コードは、自分のiPhoneやMac、または登録した電話番号に届きます。すでに有効な場合もあります。オンになっているか確認してください。

☐ 信頼できる電話番号に、今使っている番号を入れておこう

公式情報：Apple

① 設定 > [自分の名前] > サインインとセキュリティ > 2ファクタ認証
② 「信頼できる電話番号を追加」をタップして、番号を入れる
古い番号が残っていたら、新しい番号に変えます。iPhone以外で受け取れる番号もあると安心です。
「セキュリティキー」は、物理的なキーの話です。今回は気にしなくてOK。

☐ 使っていない古い端末を、リストから消そう

公式情報：Apple

① 設定 > [自分の名前] を開いて、下へスクロール
② 知らない端末や使わない端末をタップ
③ 「アカウントから削除」
このあとの復旧用連絡先のために、先に整理します。

☐ Mac・iPadなど持っている人は、同じApple Accountでサインインしておこう

公式情報：Apple

「信頼できるデバイス」は、同じApple Accountでサインイン済みの端末のことです。
このiPhoneだけが、信頼できる端末で、しかも確認コードを受け取れる電話番号にアクセスできる唯一の端末だと、なくしたり壊れたりしたときに、確認コードを受け取れなくなります。（Apple）
追加したい端末で、同じApple Accountにサインインして、出てきた6桁のコードを入力します。
分からないときは、公式ヘルプで手順を確認してください。

☐ 復旧用連絡先を決めておこう

公式情報：Apple

① 設定 > [自分の名前] > サインインとセキュリティ
② 「復旧用連絡先」 > 「復旧用連絡先を追加」
③ 家族や、信頼できる人を選ぶ（最大5人）
自分が入れなくなったとき、家族に手伝ってもらえます。家族に、自分のデータの中身は見られません。
自分と相手の両方で、iMessageがオンになっている必要があります。
自分のAppleの端末も、相手の端末も、iOS 15・macOS Monterey 12以降である必要があります。古い場合は、先に見出し③で更新します。（Apple）
ファミリー共有のメンバーなら、自動で追加されます。ほかの人は、メッセージアプリで、依頼を承諾してもらう必要があります。

☐ 故人アカウント管理連絡先を決めておこう

公式情報：Apple

① 設定 > [自分の名前] > サインインとセキュリティ
② 「故人アカウント管理連絡先」 > 「故人アカウント管理連絡先を追加」
③ 家族や、信頼できる人を選ぶ
④ 「アクセスキー」を相手に渡す（メッセージで送るか、プリントして渡す）
自分に万が一のことがあったとき、家族が写真やメモなどのデータにアクセスできるようにする設定です。
上の「復旧用連絡先」とは別のものです。「復旧用連絡先」は、自分が入れなくなったときに、手伝ってもらう人です。

パスワード、パスキー、支払い情報は、この設定では見られません。パスワードの備えは、⑤の1Passwordの「エマージェンシーキット」などで行います。（1Password）

☐ 盗難デバイスの保護をオンにして、常ににしよう

公式情報：Apple・iPhoneガイド

「常に」にすると、このあと設定変更に1時間待つことがあるので、最後にやります。（Apple）
すでにオンのこともあります。出てこないときは、iOSが17.3以降か、2ファクタ認証・パスコード・Face ID（またはTouch ID）・「探す」・「利用頻度の高い場所」がオンか確認します。（Apple）
「利用頻度の高い場所」は、設定 > プライバシーとセキュリティ > 位置情報サービス > システムサービス > 利用頻度の高い場所と経路です。
Touch IDの機種は、「Touch IDとパスコード」です。

① 設定 > Face IDとパスコード > パスコードを入れる
② 「盗難デバイスの保護」をオン
③ 「セキュリティ継続が必要」を「常に」にする
iPhoneを盗まれて、パスコードを見られても、Apple Accountなど大事な設定を変えられにくくなります。
使いにくければ、あとから変えられます。まずは「常に」でOK。

困ったとき

分からないときは、Appleサポートに電話で聞こう。

・ 電話：**0120-277-535**（日本国内から。通話料無料の番号です）

- 受付時間などは、公式ページで確認してください。（Apple）
- 一部の携帯会社や回線では、料金がかかることがあります。
- 有料の保険「AppleCare」とは別です。
- Googleは、アカウントへのログインについての電話での問い合わせには対応していません。（Google）

02 Googleアカウントを守ろう

Gmail・Googleを使う人

☐ Google セキュリティ診断を受けよう

公式情報：Google

診断で緑の盾なら、下の項目は確認だけでOKです。（Google）

① Googleで「Google セキュリティ診断」と検索
② 上に出る「スポンサー」の広告は無視。公式のページを開く
③ Googleアカウントにログインした状態で開く
④ 出てきた「直したほうがいいところ」を、上から直す（2段階認証など）
パソコンでもスマホでも同じです。不安なときは、Googleアカウントにログインして、プロフィール写真 > 推奨される対応 からも開けます。

☐ 2段階認証プロセスをオンにしよう

公式情報：Google

① Googleアカウントを開く > セキュリティとログイン
② Googleにログインする方法 > 「2段階認証プロセスを有効にする」を選ぶ

☐ バックアップコードを作って、印刷しておこう

公式情報：Google公式ヘルプ

① 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」で作る（スマホが使えないときの予備です）

② 印刷して、パスポートなどと同じ、安全な場所に置く
コードは8桁で10個です。新しく作ると、古いコードは使えなくなります。誰にも教えないでください。

☐ 再設定用のメールアドレスを入れよう。もう1つ別のGmailアカウントで設定がおすすめ

公式情報：Google

変更したあと7日間は、前のアドレスにもコードが届くことがあります。（Google）

① 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」
② メールアドレスを入れて、画面の指示に沿って進める
メインのGmailとは別に、予備用のGoogleアカウントをもう1つ作っておきます。ログイン用とは別の、普段使うメールアドレスでもOKです。（Google）ログイン用のアドレスに「+」をつけた別名は、同じアカウントなので、予備になりません。

☐ 再設定用の電話番号も入れておこう

公式情報：Google

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」
画面の指示に沿って進めます。

☐ アカウント復元用の連絡先に、信頼できる人を入れておこう

公式情報：Google公式ヘルプ

① セキュリティとログイン > Googleにログインする方法 > 「アカウント復元用の連絡先」
②「アカウント復元用の連絡先を追加」を押して、家族など信頼できる人のメールアドレスを入れ、「リクエストを送信」を押す
ログインできなくなったときに、助けてもらえます。再設定用のメールとは別のものです。相手には、セキュリティ通知は届きません。
リクエストは7日間有効です。相手が承認してから、使えるようになるまで、さらに7日かかります。締め出される前に、設定しておきましょう。

☐ パスキーを作ろう

公式情報：Google

パスキー認証あり。設定がおすすめです。（Google）
myaccount.google.com/signinoptions/passkeys で「パスキーを作成する」を押します。自分のスマホ・PCだけで行います。
iPhoneはiCloudキーチェーンがオンである必要があります。（Google）

☐ ログイン中のデバイスを見ておこう

公式情報：Google

セキュリティとログイン > お使いのデバイス > すべてのデバイスを管理 > 知らない端末を選んで「ログアウト」

☐ つながっているアプリを見ておこう

公式情報：Google

Googleアカウントの「リンク済みアプリ」のページで、知らないアプリを選びます。「Google でログイン」なら「「Google でログイン」機能の使用を停止」、リンクされたアカウントなら「リンクを削除」、アクセス権なら「アクセス権を削除」を押します。（Google）

☐ アカウントのセーフ ブラウジング保護強化機能をオンにしよう

公式情報：Google公式ヘルプ

① Googleアカウントを開く > セキュリティとログイン
②「アカウントのセーフ ブラウジング保護強化機能」まで進んで、「セーフ ブラウジング保護強化機能の設定を管理」を選ぶ
③「セーフ ブラウジング保護強化機能」をオンにする
ChromeとGmailで、フィッシングやマルウェアへの保護が強くなります。オンにして、Chromeにログインし、カスタ

ムパスフレーズを使わずに同期をオンにしていると、Chromeの保護強化機能もオンになります。（Google）
URLやダウンロードなどの情報をGoogleに送って、危険がないか確認する仕組みです。
Chromeだけで設定するときは：Chromeの設定 > プライバシーとセキュリティ > セキュリティ > 「保護強化機能」（Google公式ヘルプ）

☐ Androidの人：機種によって画面が違うので、AIと一緒に確認しながら進めてください。

「（自分の機種名）で、最低限やっておくべきセキュリティ設定を教えて」と聞いてみよう。
その中で、2段階認証は必ずオンにしておこう。

☐ Androidの人：Google Playの購入の確認を、毎回にしよう

公式情報：Google公式ヘルプ

① Playストアを開く > 右上のプロフィール写真
② お支払いと定期購入 > 購入の確認 > 確認の頻度
③ 「毎回」を選ぶ
身に覚えのない購入を防ぎます。「毎回」は初期設定ですが、変えていないか見ておきましょう。（Google Play）
機種やGoogle Playのバージョンで、文言が違うことがあります。

メールアドレスの整理

メールアドレスが何個もあると、守るところも増えます。少しずつ、減らしていきましょう。

☐ 使うメールアドレスを、少なくしていこう

① 毎日使うサービスから順番に、メインのメールアドレス（Gmailなど）にまとめる
Apple Accountのメールアドレスも、変えられます：（Apple）
① 設定 > [自分の名前] > サインインとセキュリティ
② 「主要メールアドレス」をタップ
③ 古いアドレスを残すなら「主要メール」をオフ、外すなら「アカウントから削除」をタップ
④ 新しい主要メールアドレスを入れて、確認する
確認のメールが届くので、開いて進めます。「アカウントから削除」したメールアドレス（iCloudメール以外）は、30日間、別のApple Accountに使えません。（Apple）
今のメールがiCloudメールだけの人は、画面が少し違います。分からないときは、①のAppleサポートへ。

☐ Gmailは+を付けて、使い分けもできる

公式情報：Gmailヘルプ

自分のアドレスの、「@」の前に「+名前」を付けるだけです。例：yourname+shopping@gmail.com
どれも、今のGmailに届きます。ショッピング用、学校用など、受け取りを分けたいときに便利です。
サイトによっては、「+」の付いたアドレスを受け付けないことがあります。そのときは、ふつうのアドレスで登録します。

Gmailの設定（パソコン）

ここはパソコンで進めます。後から自宅で確認しても大丈夫です。

乗っ取られたときのサインを、Gmailで見ておきましょう。

☐ Gmailの設定を見直そう（転送・フィルタ・委任・POP/IMAP）

公式情報：Google公式ヘルプ

パソコンのブラウザでだけできます（スマホのGmailアプリでは見られません）。
Gmailを開く > 右上の設定アイコン > 「すべての設定を表示」
①「メール転送とPOP/IMAP」タブ：知らない転送先がないか。POPやIMAPの設定が正しいか
②「フィルタとブロック中のアドレス」タブ：「転送する」や「削除する」のフィルタが、自分で作ったものか
③「アカウントとインポート」タブ：「アカウントへのアクセスを許可」に、知らない人がいないか。「名前」と「POP3を使用して他のアカウントのメッセージを確認」に、自分以外のアドレスがないか
④「全般」タブ：署名と不在通知が自分のものか。不在通知が、いらないのにオンになっていないか
知らない転送を見つけたら、転送を止めて、パスワードを変えてください。（Google公式ヘルプ）

☐ 前回のアカウント アクティビティで、知らないログインがないか見よう

公式情報：Google公式ヘルプ

パソコンでだけできます。Gmailを開く > 画面の右下の「詳細」
「このアカウントのアクティビティ」に、ログインの日時、アクセスの種類（ブラウザ、POP、IMAPなど）、IPアドレスと場所が出ます。
心当たりがなければ、すぐにパスワードを変えてください。

☐ 怪しいメールはフィッシングを報告しよう

公式情報：Google公式ヘルプ

パソコンのGmailで、メールを開く > 返信アイコンの横の⋮ > 「フィッシングを報告」
Googleは、メールでパスワードを聞くことはありません。リンクの先でパスワードを求められても、入れません。自分でサイトを開きます。
Googleからのセキュリティ通知が、偽物かもしれないと思ったら、myaccount.google.com/notifications を、自分で直接開いて確認します。

参考：Xで話題になった設定（Google公式のおすすめではありません）

・銀行・証券・カードの登録メールを、普段のGmailと分ける：Gmailを乗っ取られても、お金のサービスのパスワード再設定まで広がらないようにするため

・Googleに登録したメインのカードを外す：乗っ取られたときの、被害を小さくするため

・Googleに保存した銀行・証券のパスワードを消す：乗っ取られたときに、保存したパスワードを見られないようにするため

・フォトやGmailにある身分証の写真を消す：乗っ取られたときに、なりすましに使われる材料を減らすため

やるかどうかは自分で判断してください。消す前に、必要なものはバックアップを取りましょう。

03 OSとアプリを最新にしよう

使っている端末ごとに確認

OSとアプリの更新は、新しく見つかった弱点をふさぎます。お金もかからず、セキュリティの第一歩です。

参考ニュース（2026年10月時点）

ニュース：10/27に公開されたパソコン版Chromeの更新で、52件の弱点が直されました（いちばん深刻な「Critical」が4件）。（Chrome Releases）10/28に、国家サイバー統括室も、更新を呼びかけています。（国家サイバー統括室）
Android版のChromeにも、同じ番号の更新が出ています。（Chrome Releases）

☐ iPhone・iPadのOSを、最新にしよう

公式情報：Apple

① 始める前に、iCloudかパソコンで、バックアップを取る（Apple）
② 充電器につないで、Wi-Fiにつなぐ（通信量をたくさん使うので、モバイル回線は避けます）
③ 設定 > 一般 > ソフトウェアアップデート を開く
④ 更新があれば、「ダウンロードしてインストール」を押す
⑤ 同じ画面の 自動アップデート >「自動インストール」をオン
自動アップデートをオンにしておくと、あとは夜間の充電中に、勝手にやってくれます。

☐ iPhoneのアプリも、最新にしよう

公式情報：Apple

設定 > アプリ > App Store で、「アプリのアップデート」がオンか見ます。

☐ Androidの人：Androidも、最新にしよう

公式情報：Google

Wi-Fiにつなぎ、充電を75%以上にしてからやります。
設定 > システム > ソフトウェア アップデート で確認して、更新があれば、画面の案内に従います。

☐ Androidの人：アプリの自動更新を、オンにしよう

公式情報：Google Play

Google Play > 右上のプロフィール写真 > 設定 > ネットワーク設定 > アプリの自動更新
「アプリを自動更新しない」以外を選びます。

☐ Macを持っている人は、MacのOSも最新にしよう

公式情報：Apple公式

① 画面の左上のアップルメニュー > システム設定 > 一般 >「ソフトウェアアップデート」
② 更新があれば、「アップデート」「アップグレード」「今すぐ再起動」のどれかを押す。出ていなければ、「お使いのMacは最新の状態です」と表示されます
③ インストールが終わるまで、Macをスリープにしたり、蓋を閉じたりしないで待つ（途中で何度か再起動します）

始める前に、Macのバックアップを作っておくことを、Appleはすすめています。インストールの前に、Macにログインするときの管理者パスワードを聞かれます。

☐ Macの自動アップデートも、オンにしよう

公式情報：Apple公式

システム設定 > 一般 > ソフトウェアアップデート の「自動アップデート」の横の ⓘ を押して、項目をオンにして、「完了」を押します。

・「新しいアップデートがある場合はダウンロード」：確認なしで、自動でダウンロード
・「macOSアップデートをインストール」：macOSの更新を、自動でインストール
・「セキュリティ対応とシステムファイルをインストール」：緊急のセキュリティ対応などを、自動でインストール
ノートパソコン（MacBook）は、自動でダウンロードするとき、電源アダプタにつないでいる必要があります。

☐ MacのApp Storeアプリも、最新にしよう

公式情報：Apple公式

App Storeを開いて、更新を確認します。

☐ Windowsを使っている人は、Windowsも最新にしよう

公式情報：Microsoft

Windows 11：スタート > 設定 > Windows Update > 「更新プログラムの確認」を押す

☐ パソコンのChromeも、最新にしよう

公式情報：Chrome公式ヘルプ

WindowsもMacも、同じ手順です。
① Chromeを開く
② 右上の：（その他）> ヘルプ > 「Google Chromeについて」
③ この画面を開くと、更新があるかどうかを、自動で確認します
④ 「再起動」と出たら、押す（更新は、再起動したときに反映されます）
⑤ 「再起動」が出ていなければ、最新です
開いていたタブとウィンドウは、再起動すると自動で戻ります（シークレットウィンドウは戻りません）。すぐ再起動しないときは「後で」を選べます。その場合は、次にChromeを再起動したときに更新されます。
Windows：更新を反映するには、開いているChromeのウィンドウとタブを、すべて閉じてから、開き直します。
Mac：Chromeを「アプリケーション」フォルダに入れているなら、「Google Chromeについて」の画面の「すべてのユーザーに対してChromeを自動的に更新」を押すと、そのパソコンの全ユーザーで、自動更新になります。
iPhoneのChromeは、App Storeのアプリの自動更新で、AndroidのChromeは、Google Playのアプリの自動更新で、最新になります（上の項目がオンならOK）。

表示が違うときは、OSのバージョンや機種で場所が変わることがあります。

04 パスワードの使い回しをやめよう

使っているサービス共通

使い回しは、家中の鍵を同じにしているのと同じです。（IPA）一気に全部は大変なので、順番にやりましょう。移動時間に少しずつでもOKです。

iPhoneはiOS 18以降なら「パスワード」アプリが入っています。（Apple）管理アプリを決めるのは⑤です。

☐ 漏洩の危険があるパスワードを検出がオンか見よう

公式情報：Apple

設定 > アプリ > パスワード >「漏洩の危険があるパスワードを検出」がオンか見ます。

☐ パスワードアプリのセキュリティで、使い回しや弱いパスワードを見よう

公式情報：Apple

① 「パスワード」アプリを開く >「セキュリティ」
② アカウントをタップして、「パスワードを変更」

☐ Googleにパスワードを保存している人は、パスワード チェックアップで確認しよう

公式情報：Google

パソコンのChrome：右上の⋮（その他）> パスワードと自動入力 > Googleパスワード マネージャー >「チェックアップ」
ほかのブラウザ：passwords.google.com を開く >「パスワード チェックアップに移動」>「パスワードを確認」

☐ 変えるときは自動で作られる強いパスワードを使おう

公式情報：Apple

サイトやアプリでパスワードを変えるとき、出てきた強いパスワードを使います。

☐ パスワードは、サイトごとに別にしよう

公式情報：Google

アカウントごとに、異なるパスワードを使います。

☐ すでにメモなどに書いたパスワードは、パスワードアプリ（または⑤の管理アプリ）に移そう

公式情報：Apple

① 「パスワード」アプリ（または⑤で決めた管理アプリ）に、パスワードを入れる
② 元のメモ・写真・スプレッドシート・Gmailの下書きなどから、消す
Appleの「パスワード」アプリの中にある「メモ」欄（セキュリティ質問・PIN番号などを書く場所）は、アプリの機能なので、使ってOKです。

05 パスワード管理アプリを決めよう

自分に合う保存先を選ぶ

パスワードをしまっておく「金庫」のようなアプリです。パスワードを自分で覚えなくてよくなります。（Apple）

☐ パスワードをしまう管理アプリを、1つ決めよう

次のどれかから、1つに決めます。パスワードをそこにまとめます。
・Appleの「パスワード」アプリ（iOS 18以降）（Apple）
・Googleパスワード マネージャー（Chrome / Android）（Google）
・それ以外のアプリ（1Passwordなど）
サイトごとに別のパスワードを作っても、アプリが覚えてくれます。（Apple）

☐ 1Passwordなどを使う人：アカウントパスワードは、ほかのサイトと同じにしない

公式情報：1Password

アカウントパスワードは、アプリを開く鍵です。
今まで使い回していたパスワードを、アカウントパスワードにするのは、やめましょう。

☐ 1Passwordを使う人：エマージェンシーキットを、印刷して、パスポートなどの書類と一緒に置こう

公式情報：1Password

① 1Password.com にサインイン
② 右上の自分の名前 > Manage Account
③ 「Save Emergency Kit」を選んで、PDFを保存
④ 印刷して、パスポートなどの書類と一緒に、安全な場所に置く
印刷したキットに、アカウントパスワードも書いておきます。
アカウントパスワードを忘れたり、アプリに入れなくなったときの、最後の鍵です。

☐ 自動入力で使うアプリを決めよう

公式情報：Apple

① 設定 > 一般 > 自動入力とパスワード
②「パスワードとパスキーを自動入力」をオンにして、使うアプリ（「パスワード」アプリ、1Passwordなど）にチェックを入れる
保存先がいくつもあると、どこに入っているか、分からなくなります。使うアプリを決めておきましょう。
Androidの人：機種によって画面が違うので、AIと一緒に確認しながら進めてください。

06 パスキーの使い方を確認しよう

設定する前の基本

パスキーは「家の鍵」、パスワードは「合言葉」のようなものです。パスキーを作るとき、「どこに保存する？」と聞かれたら、⑤で決めたアプリ（「パスワード」アプリなど）を選びます。（Apple）

☐ パスキーを作っても、2段階認証は、そのまま残しておこう

公式情報：Google

Googleアカウントでは、パスキーを追加しても、今の認証や復元の設定は変わりません。（Google）
パスキーでログインすると、2段階認証の2つ目の手順は省かれます。（Google）

07 LINEを守ろう

LINEを使う人

参考ニュース（2026年10月時点）（2026年10月2日更新）

・「LINE VOOM」は2026年9月30日で終わりました。「新しいLINE VOOM」を名乗るページは偽物です。（LINE公式ヘルプ）

・「投票してほしい」というメッセージ、宅配業者を名乗るSMS、「アカウント停止・ロック」を名乗るメールに注意しましょう。（LINE公式ヘルプ）

・お金の被害にあったら、⑬の「困ったとき」へ。

☐ ログイン中の端末を見て、知らない端末はログアウトしよう

公式情報：LINEガイド

ホーム > 設定（歯車）> アカウント >「ログイン中の端末」

☐ ログイン許可をオフにしよう（PCやiPadでLINEを使わない人）

公式情報：LINEヘルプ

ホーム > 設定（歯車）> アカウント >「ログイン許可」をオフ

☐ パスコードロックをオンにしよう

公式情報：LINEヘルプ

ホーム > 設定（歯車）> プライバシー管理 >「パスコードロック」
パスコードは忘れないようにしましょう。忘れると、LINEの削除と再インストールが必要です。バックアップしていないトーク履歴は消えます。

☐ LINEの認証番号やパスワードは、誰にも教えないようにしよう

公式情報：LINEヘルプ

認証番号を使うのは、自分でLINEの引き継ぎをするときだけです。

☐ 公式のメールは@line.meで終わる。@line.meで終わらないメールは、詐欺の可能性があります

公式情報：LINEヘルプ

☐ LINEのパスワードを、ほかのサービスと同じにしないようにしよう

公式情報：LINEヘルプ

08 買い物のアカウントを守ろう

Amazon・楽天・Yahoo!・メルカリ

フィッシングの報告のうち、EC系が約47.9%を占めています（2026年9月）。（フィッシング対策協議会）

参考ニュース（2026年10月時点）

2026年9月は、Amazonをかたるフィッシングが、報告全体の約33.2%で一番多くなりました。（フィッシング対策協議会）

☐ 不審な注文返金のメールやSMSは、リンクを開かないようにしよう

公式情報：フィッシング対策協議会 / IPA

メールやSMSのリンクは押さず、公式アプリか公式サイトから確認します。（IPA）

☐ Amazon：2段階認証をオンにしよう

公式情報：Amazon

① アカウントサービス > 「ログインとセキュリティ」
② 「2段階認証 (2SV)の設定」の横の「編集」> 「はじめる」
③ 画面の指示に従う（ワンタイムパスワードは、テキストメッセージか認証アプリで受け取ります）

☐ Amazon：パスキーを設定しよう

公式情報：Amazon

パスキー認証あり。設定がおすすめです。（Amazon）

① アカウントサービス > 「ログインとセキュリティ」
② 「パスキー」の横の「設定」> 「設定」
③ 画面の指示に従う

☐ 楽天：パスキーを設定しよう

公式情報：楽天

パスキー認証あり。設定がおすすめです。（楽天）

① パスキー対応の楽天のサービスに、ID・パスワードでログイン > 「パスキーを設定する」
② 登録メールに届く認証コードを入れて「認証して設定に進む」
③ 端末の認証（指紋・顔・PINなど）を許可して「続ける」

☐ Yahoo!ショッピング：パスキーを設定しよう

公式情報：Yahoo! JAPAN IDガイド

パスキー認証あり。設定がおすすめです。（iPhone）（Android）（パソコン）

① Yahoo! JAPAN・Yahoo!ショッピングなどの対応アプリを開く
② アプリで、パスキー（指紋・顔・画面ロックでログイン）の設定をオンにする
ブラウザーから設定したいときは、Yahoo! JAPAN IDガイドの「パスキーでのログイン」ページから設定ページを開き、パスキーを追加します。（iPhone）（Android）（パソコン）

☐ メルカリ：パスキーを登録しよう

公式情報：メルカリ

パスキー認証あり。設定がおすすめです。（メルカリ）

① マイページ > 設定 > 「アカウント設定（個人情報設定）」> 「パスキー設定」
② 「パスキーを登録する」をタップ > 届いた認証番号を入れる
③ もう一度「パスキーを登録する」> 端末の認証を行う

☐ 登録しているカードを見直して、使わないカードは消そう

Amazon：アカウントサービス > お客様の支払い方法 > 消すカードを選ぶ > 「Amazonウォレットから削除する」（Amazon）
楽天：楽天会員情報の管理画面 > お支払い方法 > 消すカードのごみ箱マーク > 「削除」（楽天市場ヘルプ）
メルカリ（アプリ）：マイページ > 設定 > アカウント設定 > 支払い方法 > 「編集」> 消すカードの「ゴミ箱」アイコン > 「削除」（メルカリ）
メルカリで選んでいるカードは、消せません。別の支払い方法を選んで「更新する」を押してから、消します。（メルカリ）

09 宅配便の偽通知に備えよう

ヤマト運輸・佐川急便・日本郵便

参考ニュース（2026年10月時点）

2026年9月は、SMSから誘導するフィッシングの報告は減っていますが、宅配業者をかたる文面の報告は続いています。（フィッシング対策協議会）

・ 佐川急便で、9月30日に不正アクセスが見つかりました。（佐川急便 第1報）

・ 6月21日〜9月30日の送り状の氏名・住所・電話番号や、スマートクラブの会員情報など、最大約5,323万件（重複を含む）が流出した可能性があります。クレジットカード情報とパスワードは含まれていません。（佐川急便 第5報・10/23）

・ 佐川急便を装った不審なメール・SMS・電話に気をつけましょう。URLは開かず、個人情報も入れません。（佐川急便 第5報）

リンクは開かず、公式の場所から確かめます。（IPA）

☐ 不在通知配達できませんでしたのSMSは、リンクを開かないようにしよう

ヤマト運輸：SMSで、ご不在連絡やお届け予定のお知らせは送っていません。（ヤマト運輸・ヤマトHD）
佐川急便：SMSでのご連絡は行っていません。URLを開かずに削除します。（佐川急便）
日本郵便：ショートメールでのご不在連絡のお知らせは行っていません。（日本郵政）
日本郵便のサイトには、例外として、郵便局物販サービス社が不在時に送るSMSもあると書かれています。（日本郵便）

判断に迷うときは、リンクを開かず、日本郵便のお問い合わせ先に連絡します。（日本郵便）

☐ 荷物の確認は、公式アプリか、自分で開いた公式サイトからしよう

ヤマト運輸：公式アプリか、「荷物お問い合わせシステム」（ヤマトHD）
佐川急便：公式サイトか、公式アプリ、「佐川急便LINE公式アカウント」（佐川急便）
日本郵便：自分で開いた公式サイト（日本郵便）
届いたメッセージのリンクではなく、自分で開いた画面から調べます。（IPA）

☐ リンクから、アプリを入れないようにしよう

日本郵便の公式ページにも、不審なメールやSMSで「不正なアプリケーションをダウンロードさせる」手口があると書かれています。（日本郵便・日本郵政）

☐ 会員サービスは2段階認証をオンにしよう

クロネコメンバーズ：ログイン＞左上のアカウント情報＞「セキュリティ」＞2段階認証設定の「変更」＞「設定する」を選ぶ＞「設定を確認する」＞「設定する」（ヤマト運輸）
佐川急便スマートクラブ：2段階認証があります。認証コードのメールの送信元は「@sagawa-exp.co.jp」です。（佐川急便）

☐ 日本郵便（ゆうID）：パスキーを作成しよう（ゆうIDを使っていない人は、飛ばしてOK）

公式情報：ゆうID

パスキー認証あり。設定がおすすめです。（ゆうID）

ゆうID：右上のメニュー（3本線）> ログイン情報 > ご利用中のログイン画面 > ログイン方法の変更・設定 > 「パスキーを作成する」（ゆうID）
郵便局アプリ：右下のアカウント > ゆうID登録情報 > ログイン方法の変更・設定 > 「パスキーを作成する」（ゆうID）
パスワードを削除した場合、アプリ版の「郵便局のネットショップ」にログインできないことがあります。そのときは、Web版の「郵便局のネットショップ」を使います。（ゆうID）

10 旅行のアカウントを守ろう

じゃらん・JAL・ANA・Booking.com

参考ニュース（2026年10月時点）

2026年9月のフィッシング報告では、航空系が全体の約4.6%でした。（フィッシング対策協議会）

・2026年10月1日、ANAは、宿泊施設を装い、WhatsAppなどで届く不審なメッセージに注意するよう呼びかけました。個人情報やクレジットカード情報を入れさせる偽サイトへ誘導するURLが含まれます。（ANA）

・2026年9月11日、ANAは、ANAを装った詐欺メールに注意するよう呼びかけました。「お客様番号」「Webパスワード」「クレジットカード情報」の入力を促す例があります。（ANA）

☐ じゃらん：リクルートIDの2段階認証をオンにしよう

公式情報：リクルートID

① リクルートIDの会員情報変更画面にログイン
② ログインとセキュリティ > 2段階認証の「設定」をクリック
③「電話番号」「メール」「認証アプリ」から選んで、届いた認証コードを入れる
最後に「復旧用メールアドレス」も設定しておきます。

☐ じゃらん：リクルートIDのパスキーを設定しよう

公式情報：リクルートID

パスキー認証あり。設定がおすすめです。（リクルートID）

① リクルートIDのパスキーのページで「パスキーを設定する」を押す（リクルートID会員情報からも設定できます）
② 「パスキーを登録する」を押す
③ 端末の案内に従って、生体認証を行う
パスキーを設定したあとも、パスワードでログインできます。生体認証に対応していない端末では、パスキーは使えません。自分だけが使う、信頼できる端末でだけ設定します。（リクルートID）

☐ JAL：パスキーを登録しよう

公式情報：JAL

パスキー認証あり。設定がおすすめです。（JAL）

① JALにログイン > 会員登録情報 > パスキー登録・変更・削除
② SMSのワンタイムパスワードを入れる >「新規登録する」
③ 端末の生体認証または画面ロックで認証
パスキーの登録には、SMSのワンタイムパスワードが必要です。SMSが使えるのは、JMB日本地区の会員です。（JAL）

アプリ内ブラウザーでは使えません。外部のブラウザーを使います。（JAL）

☐ ANA：ワンタイムパスワードが届くメールアドレスを、最新にしておこう

公式情報：ANA

ANAマイレージクラブの「メールアドレスの登録・変更」で確認します。
ワンタイムパスワードは、「ANAからの重要なお知らせ」を受け取る設定のメールアドレスに届きます。

☐ Booking.com：予約確認支払いのお願いのメッセージは、リンクを開かないようにしよう

宿泊施設やBooking.comを名乗って、予約を保つためとして、支払い情報の共有を急がせるメッセージ（WhatsAppにも届く）に注意します。（Booking.com）
Booking.comは、メール・電話・SMS・WhatsAppでクレジットカード情報の共有をお願いしません。（Booking.com）

リンクを押す前に、予約確認書の内容を確かめます。不安なときは、Booking.comのカスタマーサービスに問い合わせます。（Booking.com）
リンクを押してしまったときは、すぐBooking.comのカスタマーサービスに連絡します。パスワードをリセットして、2段階認証を有効にします。カード情報を入れたなら、カード会社にも連絡します。（Booking.com）

☐ Booking.com：2段階認証をオンにしよう

アカウントの「セキュリティ設定」から、2段階認証を有効にします。（Booking.com）

11 SNSのアカウントを守ろう

Instagram・Facebook・Threads・X・TikTok・YouTube・Discord

Instagram・Facebookのアカウントに侵入されると、スパムの送信に利用される可能性があります。（Meta）

☐ Instagram・Facebook：アカウントを削除・ブロックすると脅すメッセージの、リンクは開かないようにしよう

公式情報：Meta

Metaを名乗る不審なメールやメッセージの、リンクや添付ファイルは開きません。
Metaからの連絡は、fb.com・facebook.com・facebookmail.com・instagram.com・meta.com・metamail.comのメールドメインからだけ届きます。（Meta）
パスワードやクレジットカード情報の入力を求めるメッセージには、返信しません。（Meta）

☐ Instagram：二段階認証をオンにしよう

公式情報：Instagramヘルプ

① プロフィール > メニュー > アカウントセンター > 「パスワードとセキュリティ」
② 「二段階認証」 > アカウントを選ぶ
③ 方法を選んで、画面の指示に従う（「認証アプリ」がおすすめ。SMS・WhatsAppも選べます）
ログイン時の「このデバイスを信頼する」は、自分だけが使う端末でだけ押します。

☐ Facebook：二段階認証をオンにしよう

公式情報：Facebookヘルプ

① 右上のプロフィール写真 > 設定とプライバシー > 「設定」
② アカウントセンター > パスワードとセキュリティ > 「二段階認証」 > アカウントを選ぶ
③ 方法を選ぶ（セキュリティキー・認証アプリ・SMSのどれか）
スマホが使えないときのための、10個のリカバリーログインコードも取れます。

☐ Threads：二段階認証をオンにしよう

公式情報：Instagramヘルプ

① Threadsアプリで、プロフィール > メニュー > 「Metaアカウント」
② 「パスワードとセキュリティ」で、二段階認証の設定を管理します。

☐ Instagram・Facebook・Threads：パスキーを作ろう

公式情報：Meta

パスキー認証あり。設定がおすすめです。（Meta）
共有の端末や公共の端末では、作りません。まだ使えない人もいます。（Meta）

① 使っているアプリの設定を開く
② Metaアカウント > ログインとセキュリティ

③ パスキー > 「パスキーを作成」

☐ X：2要素認証をオンにしよう

公式情報：Xヘルプ

① スマホ：プロフィールアイコン > 設定とプライバシー > アカウント > セキュリティ > 「2要素認証」
② パソコン：もっと見る > 設定とプライバシー > セキュリティとアカウントアクセス > セキュリティ > 「2要素認証」
③ 「ショートメール」「認証アプリ」「セキュリティキー」の3つから選べます。
メールアドレスが未確認の場合は、先に確認を求められます。

☐ TikTok：2段階認証をオンにしよう

公式情報：TikTok

① プロフィール > メニュー > 設定とプライバシー > 「セキュリティ」
② 「2段階認証」> SMS・メールアドレス・認証アプリ・パスワードから、2種類以上を選ぶ
③ 「オンにする」をタップ

☐ YouTube：②のGoogleアカウントを守るを、先にやっておこう

YouTubeは、Googleアカウントでログインします。（YouTubeヘルプ）

☐ Discord：認証アプリで2段階認証をオンにしよう

公式情報：Discord・Discord

① アバター > 歯車 > アカウント > 「認証アプリを有効にする」
② Google AuthenticatorかAuthyでQRコードを読み取る（秘密キーを入れる方法もあります）
③ 出てきた6桁のコードを入れる > バックアップコードをダウンロードして、安全な場所に保管

☐ Discord：パスキーを追加しよう

公式情報：Discord

パスキー認証あり。設定がおすすめです。（Discord）

スマホ：アバター > 歯車 > アカウント > セキュリティキー > 「追加」
パソコン：ユーザー名の隣の歯車 > マイアカウント > パスワードと認証 > 「セキュリティキーを登録する」
画面の指示に従って、パスキーを保存します。バックアップコードも、ダウンロードして保管しておきます。

☐ Discord：知らない人のQRコードやリンクは、開かないようにしよう

公式情報：Discord・Discord

自分で出していないQRコードのログイン画面が出たら、すぐに「キャンセル」を押します。間違えて承認してしまったときは、パスワードを変えて、すべての端末からログアウトします。
知らない人のDMのリンクは押しません。パスワードや「トークン」は、誰にも教えません。

12 Notionの設定を見直そう

共有・公開範囲も確認

Googleでログインしている人は、Googleアカウントで二段階認証をオンにしていると、Notionへのログインでも、ほかのデバイスでの認証が必要になります。（Notion）

☐ 二段階認証を設定しよう

公式情報：Notion

パスワードを設定している人が対象です。IDプロバイダー（Google Workspaceなど）経由でログインしている組織の人は使えません。（Notion）

① サイドバーの設定 > 自分の名前
② アカウントのセキュリティで、二段階認証の横の「認証方法を追加する」
③「認証システムからのコード」か「コードをSMSで受け取る」を選んで、設定を終える
④ 初めてなら、そのあとで、バックアップコードを保存（Notion）
地域によっては、SMSを選べず、認証システムアプリだけになります。（Notion）

☐ パスキーを追加しよう

公式情報：Notion

パスキー認証あり。設定がおすすめです。（Notion）

パソコン（Web・デスクトップ）：サイドバーの設定 > 自分の名前 > アカウントのセキュリティ >「パスキーの追加」> 保存する場所を選ぶ
スマホ：サイドバーの設定 > マイ設定 >「パスキーの追加」> 保存する場所を選ぶ
パスキーは、最大5つまで追加できます。IDプロバイダー（Okta、Microsoft Azure、Google Workspaceなど）でのログインを求める組織の人は使えません。（Notion）

☐ ログイン中のデバイスを確認して、知らないものはログアウトしよう

公式情報：Notion

デバイスの一覧で、知らない端末の横の「ログアウト」をクリックします。
全部まとめて切るときは「すべてのデバイスからログアウト」です（今使っている端末はそのままです）。
新しい端末でログインしたときに届くメールに心当たりがなければ、メールの「これは私ではありません」を選びます。
新しい端末がログアウトされます。（Notion）

☐ つながっているアプリ（コネクション）を見直して、使っていないものは外そう

公式情報：Notion

① 設定 > コネクション
② 見直したいコネクションを選ぶ
③ 使っていないものは「接続を解除」
ページごとに外すときは、ページ右上の••• > その他 > コネクションの中の、外したいコネクション >「接続を解除」。

☐ Webに公開になっているページがないか、確かめよう

公式情報：Notion・Notion

ページをWebに公開したり、「リンクを知るWeb上の全ユーザー」にしたりすると、ページの作成に関わったNotionユーザー全員の名前、プロフィール写真、メールアドレスが、Webページのメタデータに含まれます。（Notion）

① 設定 > 公開ページで、公開されているページの一覧を見る（リンクを知っていれば誰でも見られるページも出ます）
② 公開をやめるページを開く > 上の共有 > Web公開タブ > 「公開停止」
③ 「リンクを知るWeb上の全ユーザー」が残っていると、リンクを知る人は見られます。共有を開き、その横のメニューから「削除」を選びます。
ページをWebに公開すると、サブページも公開されます。

☐ 家計簿など、個人情報のページは、共有範囲を確認しよう

公式情報：Notion

ページの上の「共有」を開くと、そのページにアクセスできる人と、権限が見えます。
心当たりのない人や、不要な共有があれば、その人の名前の横のメニューを開いて「削除」を選びます。（Notion）

13 詐欺の手口と対処を確認しよう

困ったときは、ここから

☐ 確認コード（ワンタイムパスワード）は、メールやSMSのリンク先の画面には入れないようにしよう

犯人が、偽サイトに入れたコードを、そのまま本物のサイトで使う手口があります（リアルタイムフィッシング）。（フィッシング対策協議会）
パスキーは、偽サイトには使われない仕組みなので、フィッシングに強いです。（フィッシング対策協議会）

☐ 自分で何もしていないのに、確認コードのSMSが届いたら、公式アプリか、ブックマークから入って、パスワードを変えよう

誰かが、ログインしようとしている可能性があります。（フィッシング対策協議会）
SMSのリンクは開きません。（フィッシング対策協議会）

☐ パスワードが漏れたかもしれないと思ったら、すぐにパスワードを変えよう

メールやSMSを開いただけでは、被害は出ません。（IPA）
リンク先で、情報の入力やアプリのインストールをしていなければ、基本的に被害は出ません。（IPA）
IDやパスワードを入れてしまったら、すぐに変えます。（IPA）
同じパスワードを、ほかでも使っているなら、そこも変えます。（IPA）

☐ 情報が漏れましたというメールやSMSは、リンクを開かず、公式サイトのお知らせで確かめよう

公式情報：IPA

突然届くメールやSMSは、基本的に詐欺だと考えて、無視して削除します。（IPA）
本物か迷ったら、自分で公式サイトを探して、そこから問い合わせます。（IPA）
自分の名前が書いてあっても、本物とは限りません。（IPA）
「個人情報の漏えい」は、フィッシングでよく使われる口実です。（警察庁）

☐ カード情報が漏れたと知ったら、カード会社に連絡しよう

公式情報：IPA

不正に使われていないかの確認、利用停止、再発行を相談します。（IPA）
偽サイトにカード情報を入れてしまったときも、すぐカード会社に相談します。（IPA）

☐ カードの利用明細を、しばらく定期的に見て、身に覚えのない支払いがないか確かめよう

公式情報：IPA

参考ニュース（2026年10月時点）

最近のニュース：GMOインターネットグループの「お名前.com デスクトップクラウド」で、不正アクセスがありました。（GMO第13報）犯人が情報を載せていたサイトは、10/28の午前4時ごろ、止められました。GMOは、そのサイト

に「アクセスしない」「情報を広めない」ように呼びかけています。（GMO第13報）

詳しくは、下の参考情報を開いて確認してください。

GMO不正アクセスのまとめ（10/29 12:40時点）

何が起きたか

・「お名前.com デスクトップクラウド」で、第三者の不正アクセスがありました。（GMO第1報）

・お客様の情報が外部に持ち出されたことを、会社が確認しています。（GMO第4報）

・取引口座で、身に覚えのない取引があったという報告もあります。（GMO第2報）

・対象のサービスは、デスクトップクラウドの全プランです。ほかのサービスでは、影響は確認されていません。（GMO第2報・適時開示）

・犯人は金銭を要求しました（約80億円）。GMOは、要求に「永久に応じない」と言っています。（GMO第13報・GMO第12報）

時系列（日本時間）

・10/19 お客様の問い合わせで調査を開始。10/20 不正なプログラムを確認。（GMO第2報）

・10/21 4:00 全プランのサーバーを停止。脅迫メールを受け取る。（GMO第2報・GMO第13報）

・10/22 警察に相談。影響の可能性があるサーバーは26,739件。（GMO第2報）

・10/24 お見舞金（一律5,000円）と、不正取引の損失の補償を発表。（GMO第4報）

・10/27 12:30 攻撃者とみられる者が、情報と称するものを公開したことを確認。事実と異なる内容が含まれるおそれがあります。（GMO第10報）

・10/27 19:10 「特別お見舞金」と、犯人につながる情報への懸賞金（総額上限100万米ドル）を発表。（GMO第12報）

・10/28 4:00ごろ 犯人サイトのドメインが停止。（GMO第13報）

・10/28 12:00 懸賞金のサイトを開設。18時までに113件の情報提供。（GMO第14報）

・10/29 12:40 犯人の特定につながると考えられる有力な情報を入手し、警察などに提出する予定と発表。懸賞金のサイトへの情報提供は270件（11:30時点）。（GMO第15報）

影響を受けた人

・影響の可能性があるのは、サービスのサーバー内に保存されていた情報です。取引口座のログイン情報も含まれます。（GMO第2報）

・お見舞金（一律5,000円）は、現在サービスを使っているすべての人が対象です。不正取引の損失の補償は、GMOが「本件に起因する」と認めた取引の、実際に出た損失などが対象です。申請方法は、11/6（金）までに案内されます。（GMO第4報）

・犯人のサイトにアクセスした人の情報は、犯人に取られています。使っていない人も同じです。（GMO第11報）

・便乗したメールやSMSの詐欺にも注意が必要です。（GMO第11報）

自分に関係あるかの確かめ方

・「お名前.com デスクトップクラウド」を契約していたか、確認します。していなければ、このサービスのお客様ではありません。（GMO第2報）

・情報が公開されたお客様には、GMOから個別に連絡が来ます。（GMO第12報）

・不安なときは、電話03-5456-2560（24時間）に相談します。（GMO第13報）

やること：使っていない人

- [ ] **犯人のサイトを見に行かない**

公式情報：GMO第11報

- [ ] **転載・再投稿・リンクの共有をしない**

公式情報：GMO第13報

- [ ] **被害金を取り戻すという連絡は、リンクを開かず、応じない。GMOがパスワードや認証コードを聞くことはありません**

公式情報：GMO第11報

- [ ] **犯人のサイトを開いてしまったら、ウイルス対策ソフトでフルスキャンする**

公式情報：GMO第12報

やること：使っていた人

- [ ] **別の端末から、取引ツールと取引口座のパスワードを変えて、ログイン中の接続を切る**

公式情報：GMO第2報

- [ ] **同じパスワードを使っているほかのサービスも変える**

公式情報：GMO第2報

- [ ] **取引先が二段階認証を出していれば、設定する**

公式情報：GMO第2報

- [ ] **ウイルス対策ソフトでフルスキャンして、バックアップを取る**

公式情報：GMO第5報

新しい犯人サイトを見つけたら

・開かず、広めず、GMOの通報フォームに知らせます。（GMO第14報・通報フォーム）

状況は変わるので、最新を確認しよう。（GMOの重要なお知らせ）

困ったとき

・iPhone・iPad・Macの設定が分からない：①の「困ったとき」の、Appleサポート（0120-277-535）に電話（Apple）

・ほかの設定が分からない：AIに「小学生にも分かるように教えて」と聞いてOK

・身に覚えのないログインがあった：そのサービスで、すぐにパスワードを変える（④）

・消費生活のトラブル、だまされたかもしれない：消費者ホットライン188に電話（消費者庁）

・警察に相談したい（急ぎではないとき）：警察相談専用電話#9110に電話。急ぎのときは110番（政府広報オンライン）

・情報が漏れて、どうしたらいいか分からない：IPA 情報セキュリティ安心相談窓口（03-5978-7509）に電話（IPA）

14 その他の設定と証券口座を見直そう

ChatGPTのブラウザ作業・不要なアカウント・SBI証券

☐ 使わなくなったサービスのアカウントは、削除しよう

公式情報：IPA

削除すると情報が消えるかは、サービスによって違います。利用規約とプライバシーポリシーで確認します。（IPA）

☐ ChatGPTのChrome拡張は、ChatGPTアプリのInstallから入れよう

公式情報：OpenAI

① ChatGPTのデスクトップアプリを、最新にする（OpenAI）
② ChatGPTのデスクトップアプリ：設定 > Computer Use
③ Chromeの横の「Install」を押して、拡張機能ストアのページを開く
④ ChatGPTの拡張機能を入れて、ブラウザの許可の画面を確認する
ストアのページで、提供元がOpenAIか確かめます。（Chrome ウェブストア）
⑤ Computer Useに戻り、Chromeの横にManageと出ていればOK。Installのままなら、③からやり直す（OpenAI）

☐ ChatGPTが新しいWebサイトを使う前に確認してきたら、まずAllow onceを選ぼう

公式情報：OpenAI

「Allow for all sites」は選びません。確認なしで、どのサイトでも使えるようになるためです。（OpenAI）

☐ ログイン情報などの重要な情報は、ChatGPTのブラウザ作業に渡さないようにしよう

必要なとき以外は、秘密や重要な情報を送りません。作業中は、毎回の確認を自分で見ます。（OpenAI）

☐ メールやSMSのリンクから、アプリを入れないようにしよう

国税庁を名乗り、Android用の不正なアプリを入れさせるメールが出ています。（フィッシング対策協議会・2026年9月30日）

証券口座（SBI証券）

☐ SBI証券：パスキーを登録しよう（SBI証券を使っていない人は、飛ばしてOK）

公式情報：SBI証券

パスキー認証あり。設定がおすすめです。（SBI証券）

先に、端末側でパスキーが使える状態にしておきます。（SBI証券）
① SBI証券にログイン > セキュリティ設定 > パスキー認証 > 「変更」で登録します（SBI証券）
同じパスキープロバイダ（iCloudキーチェーン、Googleパスワード マネージャーなど）なら、パソコンとスマホで同じパスキーを共有できます。（SBI証券）

作れる数は、サイトによって違います（例：SBI証券は10個まで）。（SBI証券）

☐ SBI証券：ログインパスワード無効設定を有効にしよう（パスキーを登録した人）

公式情報：SBI証券

① パスキーでログイン > 各種制限設定 > 「ログインパスワード無効設定」を有効にします
パスワードでのログインができなくなり、パスキーだけで入れるようになります。パスキーを登録している人だけが、設定できます。（SBI証券）
有効にすると、「アプリ・ツールのログイン制限設定」も自動でかかります。（SBI証券）
あとで解除するときは、パスキーでログインして、同じ画面から行います。「アプリ・ツールのログイン制限」は、別に解除が必要です。（SBI証券）
無効設定中にパスキーを失くしたら、サポートに問い合わせます。（SBI証券）
無効設定をしても、フィッシングには、引き続き注意します。（SBI証券）