ネットショッピング 安心設定ガイド

買い物アカウント、支払い情報、注文内容を安全に守ります。

画面を見ながら、一つずつ確認できます。

スマートフォンの買い物アプリを使う方へ。

アカウント、支払い、注文情報を守る説明書です。

画面や項目名は、アプリ、端末、OS、更新状況で異なります。
設定をしても、詐欺や不正利用を完全に防げるわけではありません。



操作の模式図

覚えておきたいこと

第1版 2026年9月20日。公的機関と各社公式サポートを参照した独自の説明書です。特定サービスの公式マニュアルではありません。

この本の使い方

準備とアカウント：3〜14ページ
支払いとプライバシー：15〜24ページ
詐欺対策と購入後：25〜38ページ
公式情報の出典：39〜41ページ

画面例は操作場所を示す模式図です。実際のアプリでは、同じ意味の項目を探してください。

覚えておきたいこと
最初にアプリとログイン方法を確認し、その後に支払い、個人情報、購入後の対応を見直します。

設定を始める前に

- ☐ スマートフォンの画面ロックを確認します。
- ☐ 登録メールと電話番号を使える状態にします。
- ☐ カード会社の連絡先を確認します。
- ☐ 利用中の買い物アプリを整理します。
- ☐ 被害が疑われる場合は38ページを先に確認します。

家族や会社名義のアカウントでは、管理する人と支払い方法を先に確認してください。

覚えておきたいこと

注文履歴、カード明細、登録情報を確認できる状態で始めます。

共通の入口：アプリと端末の設定

買い物アプリ、端末、カード会社の設定場所を分けて覚えます。

- 買い物アプリの［アカウント］を開きます。
- ［ログインとセキュリティ］を探します。
- スマートフォンの［設定］から権限を確認します。
- カード会社のアプリで本人認証と通知を確認します。

確認：3つの設定場所を開けました。



操作の模式図

覚えておきたいこと

項目名が見つからない場合は、アプリ内のヘルプで「セキュリティ」「ログイン」「支払い」を検索します。

今日、確認する10項目

- ☐ 公式アプリと更新
- ☐ 画面ロックと生体認証
- ☐ パスワードまたはパスキー
- ☐ 2段階認証と復旧情報
- ☐ ログイン履歴と通知
- ☐ 支払い方法と3Dセキュア
- ☐ 配送先とアプリ権限
- ☐ 偽サイトとフィッシング
- ☐ 返品・定期購入・返金
- ☐ 不審な注文への対応

覚えておきたいこと

アカウントを守る設定と、購入直前の確認を組み合わせます。

公式アプリの確認

偽アプリや改変されたアプリを避けます。

- App StoreまたはGoogle Playを開きます。
- アプリ名と提供元を確認します。
- 公式サイトからストアへ移動して確認します。
- 不要または出所不明のアプリを削除します。

広告やSMSのリンクから直接インストールしません。似た名前やロゴだけで公式と判断しません。

確認：利用中の買い物アプリの提供元を確認しました。

覚えておきたいこと

AndroidではGoogle Play プロテクトの警告を無視しません。iPhoneではApp Storeの提供元を確認します。

OSとアプリの更新

修正済みの安全な版を使います。

- スマートフォンのOS更新を確認します。
- App StoreまたはGoogle Playを開きます。
- 買い物アプリと決済アプリを更新します。
- 自動更新を有効にして動作を確認します。

更新を長期間止めたままにしません。古い端末で更新できない場合は、買い物や決済への利用を見直します。

確認：OSと主要アプリに未処理の更新がありません。

覚えておきたいこと

更新時に新しい権限を求められた場合は、必要性を確認してから許可します。

画面ロックと生体認証

紛失や置き忘れの際に、買い物アプリを開かれにくくします。

- 端末の画面ロックを有効にします。
- 推測されにくいパスコードやPINを使います。
- 顔認証または指紋認証を設定します。
- 自動ロックまでの時間を短くします。

端末のロック解除番号を、買い物アプリのパスワードと同じにしません。

確認：画面ロックと生体認証を確認しました。

覚えておきたいこと

対応するアプリでは、起動時や支払い時にも生体認証を設定します。

ショッピングアプリのアカウント設定

ログインと復旧に使う情報を最新にします。

- アプリの［アカウント］または［マイページ］を開きます。
- ［ログインとセキュリティ］を開きます。
- 登録メール、電話番号、認証方法を確認します。
- 不要な連携サービスや端末を外します。

確認：登録情報と認証方法を確認しました。



操作の模式図

覚えておきたいこと

サービスにより、設定名と利用できる認証方法は異なります。

使い回さないパスワード

一つの漏えいから複数サービスへ侵入されるのを防ぎます。

- 買い物サービスごとに別のパスワードを使います。
- 長く推測されにくい文字列を設定します。
- パスワード管理機能へ安全に保存します。
- 漏えいや使い回しの警告を確認します。

メール、SNS、買い物サービスで同じパスワードを使いません。家族や販売者へ教えません。

確認：主要な買い物アカウントで使い回しがありません。

覚えておきたいこと

パスワード管理機能を使うと、サービスごとに異なる長いパスワードを管理できます。

パスキー

対応サービスでは、入力するパスワードを減らしてフィッシングに備えます。

- アプリのセキュリティ設定を開きます。
- ［パスキー］または［生体認証］を探します。
- 自分が管理する端末へ登録します。
- 予備端末や復旧方法も確認します。

他人や共有端末にパスキーを登録しません。機種変更前に引き継ぎ方法を確認します。

確認：利用できるサービスでパスキーを確認しました。

覚えておきたいこと

メルカリやYahoo! JAPANなど、パスキーに対応するサービスがあります。

2段階認証

パスワードが知られても追加確認でログインを止めます。

- ［ログインとセキュリティ］を開きます。
- ［2段階認証］を有効にします。
- 認証アプリ、確認通知、SMSなどから選びます。
- バックアップ方法を安全な場所へ保管します。

確認コードや承認通知を他人へ渡しません。自分が操作していない承認要求は拒否します。

確認：利用できるアカウントで2段階認証が有効です。

覚えておきたいこと

Amazonなど、ログインとセキュリティ画面から2段階認証を設定できるサービスがあります。

復旧用メールと電話番号

ログインできないときに安全に本人確認できるようにします。

- アカウントの登録情報を開きます。
- 現在使えるメールアドレスか確認します。
- 現在使える電話番号か確認します。
- 機種変更や番号変更の前に更新します。

退職、解約、家族名義など、使えなくなる連絡先を残しません。

確認：復旧情報が現在の連絡先です。

覚えておきたいこと

復旧情報が古いと、不正利用への対応やパスワード再設定が難しくなります。

ログイン通知と利用端末

不正ログインを早く見つけます。

- セキュリティ通知をオンにします。
- ログイン履歴や利用端末を開きます。
- 覚えのない端末と日時を確認します。
- 不要な端末をログアウトします。

通知メールのリンクを押さず、公式アプリを自分で開いて確認します。

確認：利用端末と最近のログインに不審なものがありません。

覚えておきたいこと

Yahoo! JAPANなどでは、新しい端末からのログインを知らせる機能があります。

支払い方法の設定

使う支払い方法を必要なものへ絞ります。

- アプリの［支払い方法］を開きます。
- 登録カードとコード決済を確認します。
- 使わない支払い方法を削除します。
- 支払い時の本人確認を有効にします。

共有端末や他人のアカウントへ自分のカードを登録しません。

確認：必要な支払い方法だけが登録されています。



操作の模式図

覚えておきたいこと

カード会社のアプリでも、本人認証と利用通知を確認します。

本人認証サービス（3Dセキュア）

オンライン決済でカード会員本人かを追加確認します。

- カード会社の公式アプリや会員ページを開きます。
- 本人認証サービスの登録状況を確認します。
- 携帯電話番号やメールを最新にします。
- 決済時の認証要求を内容まで確認します。

認証コードを販売者やサポート担当へ伝えません。自分が購入していない認証要求は承認しません。

確認：利用するカードで本人認証サービスを確認しました。

覚えておきたいこと

経済産業省は、EC利用に備えて本人認証サービスの設定を案内しています。

カード情報の保存

保存する支払い情報を減らします。

- 登録済みカードの一覧を開きます。
- 期限切れや使わないカードを削除します。
- 共有アカウントでは保存を見直します。
- カード番号をメッセージで送信しません。

カード情報を保存しない場合でも、偽サイトへの入力や端末の不正利用には注意が必要です。

確認：登録カードと名義を確認しました。

覚えておきたいこと

カードを再発行した場合は、古い情報を削除して定期購入の支払い先も確認します。

購入確定時の確認

誤注文と第三者による購入を減らします。

- 支払い前に商品名と数量を確認します。
- 合計金額、送料、手数料を確認します。
- 配送先と支払い方法を確認します。
- 生体認証や確認コードは内容を見て承認します。

急かされても、認証画面の金額やサービス名を見ずに承認しません。

確認：購入確定前に4項目を確認する習慣を作りました。

覚えておきたいこと

家族で端末を共有する場合は、購入のたびに認証を求める設定を使います。

利用通知とカード明細

不正利用を早く発見します。

- カード会社の利用通知をオンにします。
- コード決済の通知もオンにします。
- 注文履歴とカード明細を照合します。
- 少額でも覚えのない利用を確認します。

通知だけで判断せず、カード会社の公式アプリや明細を自分で開いて確認します。

確認：支払いの利用通知と明細を確認しました。

覚えておきたいこと

身に覚えのない請求は、すぐにカード会社へ連絡します。

配送先と個人情報

保存する住所と連絡先を必要な範囲へ絞ります。

- 登録済みの氏名、住所、電話番号を確認します。
- 古い住所や不要な配送先を削除します。
- 共有アカウントの配送先を見直します。
- 出品者へ不要な個人情報を送りません。

配送に必要な情報以外を、チャットやレビューへ書き込みません。

確認：古い住所と不要な連絡先がありません。

覚えておきたいこと

注文前に配送先を確認すると、誤配送による情報漏えいも減らせます。

アプリの権限

買い物アプリが使える情報を必要な範囲へ絞ります。

- 端末の［設定］から買い物アプリを開きます。
- カメラ、写真、位置情報などを確認します。
- 利用目的に合わない権限をオフにします。
- 使うときだけ許可する設定を検討します。

権限を切ると、バーコード読み取りや現在地からの店舗検索が使えない場合があります。

確認：必要な権限だけが有効です。



操作の模式図

覚えておきたいこと

Androidはプライバシーダッシュボード、iPhoneはプライバシー設定やレポートで利用状況を確認できます。

カメラ・写真・位置情報・マイク

画像、現在地、音声へのアクセスを目的に合わせます。

- 商品撮影を使う場合だけカメラを許可します。
- 写真は必要な項目だけを選びます。
- 位置情報は配送や店舗検索の必要性を確認します。
- 音声検索を使わない場合はマイクをオフにします。

本人確認書類や伝票の画像を、通常の商品写真と同じアルバムへ放置しません。

確認：買い物に不要な権限を外しました。

覚えておきたいこと

OSの版により、正確な位置情報や選択した写真だけを許可できる場合があります。

通知のプライバシー

配送先、商品名、金額を周囲から見られにくくします。

- 端末の通知設定を開きます。
- 買い物アプリの通知プレビューを確認します。
- ロック画面へ注文内容を表示する範囲を絞ります。
- セキュリティ通知は受け取れる状態にします。

すべての通知を切ると、不正ログインや決済の警告を見逃す場合があります。

確認：ロック画面の表示と重要通知を確認しました。

覚えておきたいこと

宣伝通知とセキュリティ通知を分けて設定できる場合があります。

買い物に使う通信環境

アカウントと支払い情報を扱う環境を選びます。

- OSとブラウザーを最新にします。
- 支払いや設定変更は信頼できる回線で行います。
- 共有端末や共用PCではログインしません。
- 利用後は注文内容とログイン通知を確認します。

無料Wi-Fiで警告や証明書エラーが出た場合は操作を中止します。回線を切り替えて公式アプリから開き直します。

確認：買い物に使う端末と回線を決めました。

覚えておきたいこと

通信環境だけで安全は決まりません。公式アプリ、更新、認証の確認も続けます。

偽アプリの見分け方

本物に似せたアプリへIDやカード情報を渡さないようにします。

- ストアで提供元の名称を確認します。
- 公式サイトに掲載されたストアリンクと照合します。
- 要求する権限とレビュー履歴を確認します。
- 公式確認ができないアプリを入れません。

ロゴ、アプリ名、評価の高さだけで公式と判断しません。

確認：公式の提供元と配布先を確認しました。

覚えておきたいこと

AndroidではPlay プロテクトの警告、iPhoneではApp Storeの開発元表示を確認します。

偽サイトとURL

実在する店を装った偽サイトを避けます。

- 購入前に公式サイトのURLか確認します。
- 会社名、住所、電話番号を確認します。
- 極端な値引きと不自然な支払い方法を疑います。
- ブックマークや公式アプリから入り直します。

検索結果の上位やSNS広告でも安全とは限りません。ロゴが同じでもURLと販売者を確認します。

確認：購入前にURLと事業者情報を確認しました。

覚えておきたいこと

消費者庁は、URL、連絡先、価格、支払い方法、不自然な日本語の確認を案内しています。

フィッシングメールとSMS

偽のログイン画面へ情報を入力しないようにします。

- 配送、支払い、アカウント停止の通知を疑います。
- メッセージ内のリンクを開きません。
- 公式アプリを自分で開いて同じ通知を確認します。
- ID、カード番号、確認コードを入力しません。

普段使う事業者名でも、送信元表示だけでは本物と判断できません。

確認：通知は公式アプリから確認する習慣を作りました。

覚えておきたいこと

消費者庁は、SMSやメールで突然カード番号の入力を求められても入力しないよう案内しています。

配送通知を装うメッセージ

配送を装ったフィッシングと不正アプリを避けます。

- 不在通知や住所確認のSMSを疑います。
- URLを押さず、配送会社の公式アプリを開きます。
- 追跡番号は注文履歴から確認します。
- アプリのインストールや認証コード送信を拒否します。

注文直後に届いた通知でも、リンク先が正規とは限りません。

確認：配送状況を注文履歴と公式アプリで確認しました。

覚えておきたいこと

配送会社名を検索して出た広告ではなく、公式アプリや保存済みの公式ページから確認します。

SNS広告と極端な値引き

関心に合わせて表示された広告から偽サイトへ誘導されるのを避けます。

- 広告を見てもすぐに購入しません。
- 商品名と販売店を別に検索します。
- 相場より極端に安い理由を確認します。
- 公式サイトと返品条件を確認します。

期間限定、残りわずか、今だけ無料など、急がせる表示だけで判断しません。

確認：広告以外の情報でも販売店を確認しました。

覚えておきたいこと

消費者庁は、SNS広告のURLや極端な値引きだけで安全と判断しないよう注意を促しています。

商品と販売者の確認

商品と取引相手を購入前に特定します。

- 商品説明、型番、サイズ、状態を確認します。
- 販売者名と連絡先を確認します。
- モールでは実際の出店者を確認します。
- 画像や説明に不自然な点がないか確認します。

大手モール内の商品でも、販売者はモール運営会社とは別の場合があります。

確認：商品と販売者を確認しました。

覚えておきたいこと

高額品やブランド品は、正規販売店や鑑定、保証の条件も確認します。

レビューと出品者情報

レビューだけに頼らず販売者を判断します。

- 評価数と投稿時期を確認します。
- 同じ表現が続くレビューを鵜呑みにしません。
- 低評価の内容と販売者の対応を確認します。
- 外部サイトの評判も確認します。

星の数、ランキング、著名人の名前だけで安全や品質を判断しません。

確認：複数の情報から販売者を確認しました。

覚えておきたいこと

口コミは参考情報です。販売条件、事業者情報、商品説明と合わせて確認します。

返品・キャンセル条件

届いた後の対応条件を購入前に確認します。

- 購入前に返品と交換の条件を開きます。
- 期限、送料、対象外の商品を確認します。
- 注文確定画面を保存します。
- 返品連絡はアプリ内の正規窓口から行います。

通信販売には、訪問販売のような一般的なクーリング・オフ制度がありません。事業者の返品特約を確認します。

確認：返品条件と連絡方法を確認しました。

覚えておきたいこと

返品不可と表示されている場合は、自己都合での返品が難しいことがあります。

定期購入とサブスクリプション

一回だけの購入か、継続契約かを見分けます。

- 初回価格だけでなく総額を確認します。
- 回数、次回発送日、解約条件を確認します。
- 最終確認画面と申込内容を保存します。
- 解約後は受付記録と請求を確認します。

アプリを削除しただけでは解約にならない場合があります。事業者の手順で解約します。

確認：契約期間、総額、解約方法を確認しました。

覚えておきたいこと

低価格のお試し表示でも、定期購入が条件になっていないか確認します。

フリマとモール内の連絡

プラットフォームの確認と補償が使える範囲で取引します。

- 連絡と支払いはアプリ内で行います。
- 外部SNSや個人間送金への移動を断ります。
- 取引画面と相手の情報を保存します。
- 問題は運営会社の正規窓口へ報告します。

販売者から外部チャット、銀行振込、コード決済へ誘導されても応じません。

確認：連絡と支払いがアプリ内で完結しています。

覚えておきたいこと

個人間取引では、事業者との通信販売と同じルールや補償が適用されない場合があります。

コード決済の返金詐欺

返金のふりをした送金指示を止めます。

- ［欠品なのでコード決済で返金］という連絡を疑います。
- LINE追加や画面共有をしません。
- ［送る］や送金の操作をしません。
- 公式窓口と消費者ホットライン188へ相談します。

返金を受けるために、送金操作、暗証番号入力、画面共有を求める相手を信用しません。

確認：返金は購入履歴の正規窓口から確認します。

覚えておきたいこと

国民生活センターは、コード決済で返金すると言われたら詐欺を疑うよう注意を促しています。

注文履歴と購入後の確認

注文内容と請求の違いを早く見つけます。

- 注文後にアプリの［注文履歴］を開きます。
- 商品、金額、販売者、配送先を確認します。
- 発送と返金は履歴から確認します。
- カード明細と照合します。

メールの注文確認だけに頼らず、公式アプリの注文履歴を確認します。

確認：注文履歴とカード明細が一致しています。



操作の模式図

覚えておきたいこと

身に覚えのない通知は、メールのリンクではなく公式アプリから調べます。

購入後

身に覚えのない請求

不正利用の拡大を止めます。

- 家族の利用と複数注文の合算を確認します。
- 買い物アプリの注文履歴を確認します。
- カード会社へすぐに連絡します。
- アカウントのログイン履歴と認証方法を見直します。

相手から届いた番号ではなく、カード裏面や公式アプリにある連絡先を使います。

確認：請求元、注文履歴、連絡先を確認しました。

覚えておきたいこと

カード停止や再発行が必要かは、カード会社の指示に従います。

不正利用が疑われるときの対応

アカウント、支払い、取引の被害拡大を止めます。

- 別の安全な端末からパスワードを変更します。
- すべての端末からログアウトし、2段階認証を確認します。
- 買い物サービスとカード会社へ連絡します。
- 記録を保存し、188または警察相談＃9110へ相談します。

不審な相手と連絡を続けず、画面共有や遠隔操作アプリを使いません。証拠となる注文番号、日時、メッセージを保存します。

確認：変更、ログアウト、連絡、記録の順を確認しました。



操作の模式図

覚えておきたいこと

スマートフォンを紛失した場合は、端末の遠隔ロックと回線停止も行います。

公式情報の出典（1）

出典 S01　消費者庁：偽サイトに注意

出典 S02　消費者庁：カード不正利用に注意

出典 S03　経済産業省：本人認証サービスを設定

出典 S04　IPA：不正ログイン対策

出典 S05　IPA：パスワードの安全な使い方

出典 S06　Google：アカウントのセキュリティ強化

出典 S07　Apple：2ファクタ認証

出典 S08　Google：Google Play プロテクト

各項目名をクリックすると公式ページが開きます。

覚えておきたいこと

確認日：2026年9月20日。公的機関と各社公式サポートを参照しています。アプリ、端末、OS、契約内容により画面や条件は異なります。

公式情報の出典（2）

出典 S09　Apple：iOSのアプリセキュリティ

出典 S10　Google：Androidアプリの更新

出典 S11　Apple：App Storeアプリの更新

出典 S12　Google：プライバシーダッシュボード

出典 S13　Apple：アプリプライバシーレポート

出典 S14　国民生活センター：インターネットトラブル

出典 S15　国民生活センター：コード決済の返金詐欺

出典 S16　国民生活センター：通信販売と返品

各項目名をクリックすると公式ページが開きます。

覚えておきたいこと

確認日：2026年9月20日。公的機関と各社公式サポートを参照しています。アプリ、端末、OS、契約内容により画面や条件は異なります。

公式情報の出典（3）

出典 S17　国民生活センター：定期購入トラブル

出典 S18　消費者庁：インターネット消費者トラブル

出典 S19　消費者庁：ネット通販の購入時の確認

出典 S20　メルカリ：不正利用対策

出典 S21　Yahoo! JAPAN：パスキーでのログイン

出典 S22　Amazon：2段階認証

出典 S23　Apple：購入履歴の確認

出典 S24　Google：不審なアクティビティへの対応

各項目名をクリックすると公式ページが開きます。

覚えておきたいこと

確認日：2026年9月20日。公的機関と各社公式サポートを参照しています。アプリ、端末、OS、契約内容により画面や条件は異なります。