ネットバンキング 安心設定ガイド

ログイン、振込、取引確認を安全に行うための基本設定を整えます。

画面を見ながら、一つずつ確認できます。

スマートフォンやパソコンで銀行を利用する方へ。

口座、認証情報、送金を守る説明書です。

画面や項目名は、銀行、端末、OS、契約内容で異なります。
設定をしても、詐欺や不正送金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。公的機関と銀行の公式情報を参照した独自の説明書です。特定銀行の公式マニュアルではありません。

この本の使い方

準備と端末：3〜8ページ
認証と振込設定：9〜20ページ
詐欺対策と緊急対応：21〜38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。実際のアプリやサイトでは、同じ意味の項目を探してください。

覚えておきたいこと

最初に安全な入口と端末を確認し、認証、振込、通知、詐欺への備えを順に見直します。

準備

設定を始める前に

- ☐ 銀行の公式アプリまたは公式サイトを確認します。
- ☐ 登録した電話番号とメールを使える状態にします。
- ☐ キャッシュカードや通帳にある銀行の連絡先を確認します。
- ☐ 端末の画面ロックを確認します。
- ☐ 被害が疑われる場合は38ページを先に確認します。

家族や会社名義の口座では、利用権限と連絡担当者を先に確認してください。

覚えておきたいこと

暗証番号、ワンタイムパスワード、認証コードは、銀行員を名乗る相手にも伝えません。

共通の入口：銀行アプリと端末の設定

銀行、端末、認証、取引履歴の設定場所を分けて覚えます。

- 銀行の公式アプリを開きます。
- ［メニュー］から［セキュリティ］を探します。
- 端末の［設定］で画面ロックと権限を確認します。
- 取引通知と入出金明細を開けることを確認します。

確認：4つの入口を確認できました。



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、銀行の公式ヘルプで「セキュリティ」「認証」「振込限度額」を検索します。

今日、確認する10項目

- ☐ 公式アプリ・公式サイト
- ☐ OS、アプリ、ブラウザーの更新
- ☐ 画面ロックと生体認証
- ☐ パスワードと追加認証
- ☐ 登録電話番号とメール
- ☐ 利用端末とログイン通知
- ☐ 振込限度額と振込先
- ☐ 入出金通知と明細
- ☐ フィッシングと遠隔操作
- ☐ 不正送金時の連絡手順

覚えておきたいこと

設定だけでなく、振込前後の確認と、異常を見つけたときの連絡手順まで準備します。

公式アプリと公式サイト

偽アプリや偽ログイン画面へ情報を入力しないようにします。

- App StoreまたはGoogle Playで提供元を確認します。
- 銀行の公式サイトからアプリ配布先へ移動します。
- 公式サイトは自分で登録したブックマークから開きます。
- SMS、メール、広告内のリンクからログインしません。

ロゴ、アプリ名、検索順位だけで公式と判断しません。

確認：銀行の公式アプリとブックマークを確認しました。

覚えておきたいこと

金融庁と警察庁は、公式アプリまたは事前に登録した公式サイトからアクセスするよう案内しています。

OS・アプリ・ブラウザーの更新

修正済みの安全な環境で取引します。

- 端末のOS更新を確認します。
- 銀行アプリを最新にします。
- パソコンではブラウザーとセキュリティソフトを更新します。
- 自動更新を有効にして再起動します。

更新できない古い端末では、ネットバンキングの利用を見直します。

確認：OS、アプリ、ブラウザーに未処理の更新がありません。

覚えておきたいこと

更新後に新しい権限や認証方法を求められた場合は、銀行の公式案内を確認します。

画面ロックと生体認証

紛失や置き忘れの際に、銀行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PINやパスコードを使います。
- 顔認証または指紋認証を登録します。
- 自動ロックまでの時間を短くします。

端末のロック番号を、銀行の暗証番号やログイン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

対応する銀行アプリでは、起動時や取引時にも生体認証を使います。

ネットバンキングのセキュリティ設定

ログインと送金に関係する設定を一か所ずつ確認します。

- 銀行アプリの［メニュー］を開きます。
- ［セキュリティ］または［各種設定］を開きます。
- 認証方法、利用端末、通知を確認します。
- 振込限度額と登録情報を確認します。

確認：認証、端末、通知、限度額の場所を確認しました。



操作の模式図

覚えておきたいこと

銀行により、セーフティパス、ご利用カード、ワンタイムパスワードなど名称が異なります。

使い回さないパスワード

他サービスの漏えいから銀行へ侵入されるのを防ぎます。

- 銀行専用のパスワードを使います。
- 長く推測されにくい文字列にします。
- メールや他サービスと使い回しません。
- パスワード管理機能へ安全に保存します。

ID、パスワード、暗証番号をメモアプリやメッセージに平文で保存しません。

確認：銀行のパスワードを他で使っていません。

覚えておきたいこと

全国銀行協会とIPAは、他サービスと異なるパスワードの利用を案内しています。

パスキーと生体認証

対応する場合は、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。

- 銀行が対応する認証方法を確認します。
- ［パスキー］または［生体認証］があれば登録します。
- 自分が管理する端末だけを登録します。
- 機種変更時の引き継ぎ方法を確認します。

共有端末や他人の端末へ登録しません。銀行が未対応の場合は、推奨する追加認証を使います。

確認：利用できる認証方法を確認しました。

覚えておきたいこと

対応状況と名称は銀行ごとに異なります。公式案内に従ってください。

ワンタイムパスワード

重要な取引を、一回限りの追加認証で確認します。

- 銀行の認証設定を開きます。
- アプリ型またはカード型など対応方式を確認します。
- 振込前に表示された取引内容を読みます。
- 認証コードを他人へ伝えません。

ワンタイムパスワードもリアルタイムで盗まれる場合があります。偽サイトへ入力しません。

確認：銀行が推奨するワンタイムパスワードを有効にしました。

覚えておきたいこと

コードの数字だけでなく、振込先や金額を表示する認証では内容まで確認します。

2段階認証・追加認証

パスワードが知られても、追加確認で取引を止めます。

- ログイン時の追加認証を有効にします。
- 取引時の認証も有効にします。
- 認証通知は自分の操作か確認します。
- 覚えのない承認要求は拒否します。

SMS認証だけに頼らず、銀行が推奨するアプリ認証や取引認証があれば利用します。

確認：ログイン時と取引時の追加認証を確認しました。

覚えておきたいこと

多要素認証は有効ですが、偽サイトで追加コードまで入力すると突破される場合があります。

登録電話番号とメール

重要通知と本人確認を確実に受け取ります。

- 銀行の登録情報を開きます。
- 現在使える電話番号か確認します。
- 現在使えるメールアドレスか確認します。
- 変更予定がある場合は事前に更新します。

解約済み、家族名義、退職後に使えない連絡先を残しません。

確認：登録電話番号とメールが現在のものです。

覚えておきたいこと

連絡先変更の直後は、銀行からの通知とログイン履歴を確認します。

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。

- ログイン通知をオンにします。
- 登録端末や利用端末の一覧を開きます。
- 覚えのない端末と日時を確認します。
- 不要な端末を解除し、全端末からログアウトします。

通知メールのリンクは押さず、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

銀行によっては取引完了をメールやプッシュ通知で知らせる機能があります。

振込限度額

万一の不正送金で動かせる金額を小さくします。

- ［振込限度額］を開きます。
- 1日と1回の上限を確認します。
- 普段使う金額まで引き下げます。
- 高額振込の後は、必要に応じて再び下げます。

引き上げの反映時間や追加認証は銀行ごとに異なります。予定の直前に慌てて変更しません。

確認：普段の利用に合う上限へ見直しました。



操作の模式図

覚えておきたいこと

上限は高いままにせず、必要な範囲へ絞ります。

振込先の登録と新規振込

振込先の入力ミスと、偽の口座変更依頼を減らします。

- よく使う振込先は口座名義まで確認して登録します。
- 新しい振込先は、別の手段で口座情報を確認します。
- 振込先の変更依頼は本人へ直接確認します。
- 不要な登録先を削除します。

メールやSNSだけで届いた口座変更を、そのまま信用しません。

確認：登録振込先を整理しました。

覚えておきたいこと

会社や家族への高額振込は、普段使う連絡先から本人へ確認します。

振込時の取引内容確認

認証の前に、誰へいくら送るかを確認します。

- 受取銀行、支店、口座名義を確認します。
- 金額と手数料を確認します。
- 認証画面でも振込先と金額を確認します。
- 確定後に受付番号を保存します。

相手と通話しながら、指示どおりに振込操作をしません。一度電話を切って確認します。

確認：振込前に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

一度受け付けた振込は、訂正や取消ができず、組戻しが必要になる場合があります。

利用通知と入出金明細

不正なログインや送金を早く見つけます。

- ログイン通知をオンにします。
- 振込や登録情報変更の通知をオンにします。
- 入出金明細を定期的に確認します。
- 少額でも覚えのない取引を確認します。

通知だけで判断せず、公式アプリで明細を確認します。

確認：通知と最近の明細を確認しました。



操作の模式図

覚えておきたいこと

金融庁は、利用状況通知を有効にし、残高と入出金明細をこまめに確認するよう案内しています。

キャッシュカード・デビット設定

口座と連動するカードの不正利用も早く見つけます。

- カードの利用通知をオンにします。
- 利用限度額を普段の範囲へ下げます。
- 海外利用やネット利用の設定を確認します。
- 使わない機能は一時停止を検討します。

設定できる項目は銀行やカードにより異なります。公式アプリの案内に従います。

確認：カードの通知と限度額を確認しました。

覚えておきたいこと

カードを紛失した場合は、銀行の公式窓口へ直ちに連絡します。

アプリの権限

銀行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］から銀行アプリを開きます。
- カメラ、写真、位置情報、マイクを確認します。
- 本人確認や読取に必要な範囲だけ許可します。
- 使い終わった権限を見直します。

権限を切ると、本人確認書類やQRコードの読取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

権限を求められた理由が分からない場合は、許可前に銀行の公式ヘルプを確認します。

通知のプライバシー

口座情報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。
- 銀行アプリの通知プレビューを確認します。
- ロック画面に残高や取引内容を出す範囲を絞ります。
- セキュリティ通知は受け取れる状態にします。

通知をすべて切ると、不正ログインや取引の警告を見逃す場合があります。

確認：表示内容と重要通知を確認しました。

覚えておきたいこと

宣伝通知と取引通知を分けられる場合は、取引通知を優先します。

公衆Wi-Fiと共用端末

口座情報を扱う端末と回線を選びます。

- 振込や設定変更は、自分が管理する端末で行います。
- 信頼できる自宅回線や携帯回線を使います。
- 共用PCではログインしません。
- 証明書エラーや不審な画面が出たら中止します。

通信環境だけで安全は決まりません。公式サイト、更新、認証の確認も続けます。

確認：ネットバンキングに使う端末と回線を決めました。

覚えておきたいこと

外出先で急いで送金せず、安全な場所へ移動してから確認します。

ブラウザーの保存情報と自動入力

古い端末や共用環境に認証情報を残さないようにします。

- ブラウザーに保存された銀行の情報を確認します。
- 共用端末ではパスワードを保存しません。
- 不要なログイン状態を解除します。
- ブックマークのURLを公式サイトと照合します。

偽サイトでも自動入力される場合があります。入力前にURLを確認します。

確認：保存情報とログイン状態を整理しました。

覚えておきたいこと

銀行が公式アプリの利用を案内している場合は、公式アプリを優先します。

偽アプリと偽サイト

ID、パスワード、ワンタイムパスワードを盗まれないようにします。

- 提供元と公式サイトのURLを確認します。
- ロゴや画面が似ていても信用しません。
- 急な本人確認や利用停止の表示を疑います。
- 公式アプリまたはブックマークから入り直します。

正規サイトに似たドメイン名や偽の広告は、見た目だけで判別しにくい場合があります。

確認：公式の入口から入り直す習慣を作りました。

覚えておきたいこと

メールやSMS内のリンクを安易に押さないことが、基本の対策です。

検索広告とブックマーク

検索広告から偽サイトへ入るのを避けます。

- 検索結果の［広告］表示を確認します。
- 広告を経由せず公式URLを自分で確認します。
- 正しいページをブックマークへ登録します。
- 次回からブックマークまたは公式アプリで開きます。

検索結果の上位にあることは、公式や安全の証明ではありません。

確認：公式サイトのブックマークを確認しました。

覚えておきたいこと

ブックマーク登録後も、銀行の名称変更やドメイン変更は公式案内で確認します。

フィッシングメール・SMS

偽のログイン画面へ認証情報を渡さないようにします。

- 口座停止、本人確認、未払いの通知を疑います。
- 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、暗証番号、認証コードを入力しません。

送信元名や電話番号が銀行と同じに見えても、本物とは限りません。

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

金融機関がSMSやメールでID・パスワード等を問い合わせることはありません。

電話を使った詐欺

電話で急かされても、本人確認と送金を分けます。

- 銀行、警察、役所を名乗る電話でも一度切ります。
- 相手が伝えた番号へ折り返しません。
- カードや公式アプリにある番号へ自分で連絡します。
- 暗証番号や認証コードを伝えません。

口座を守る、調査する、還付するという理由でも、相手の指示で操作しません。

確認：公式窓口へかけ直す手順を確認しました。

覚えておきたいこと

不審な電話は家族や警察相談専用電話＃9110へ相談します。

遠隔操作・画面共有

相手に画面と操作権限を渡さないようにします。

- 銀行操作中に画面共有をしません。
- 相手の指示で遠隔操作アプリを入れません。
- 入れてしまったら通信を切って操作を止めます。
- 別の安全な端末から銀行へ連絡します。

銀行、警察、サポートを名乗っても、遠隔操作中にネットバンキングを開きません。

確認：画面共有を求められたら断ると決めました。

覚えておきたいこと

遠隔操作では、入力額や振込限度額を勝手に変更される被害があります。

サポート詐欺と偽警告

偽のウイルス警告から不正送金へ進むのを止めます。

- 突然の警告音や電話番号表示を信用しません。
- 画面の番号へ電話しません。
- ブラウザーを閉じ、必要なら端末を再起動します。
- ソフトを入れた場合は銀行と警察へ相談します。

修理代や確認のためでも、遠隔操作中にネットバンキングを開きません。

確認：偽警告が出たときの閉じ方と連絡先を確認しました。

覚えておきたいこと

警察庁は、遠隔操作ソフトによりアカウント乗っ取りや不正送金のおそれがあると注意しています。

暗証番号・認証コードの扱い

本人だけが使う認証情報を守ります。

- 暗証番号とログイン情報を他人へ伝えません。
- ワンタイムパスワードを読み上げません。
- 認証通知は取引内容を見て承認します。
- カードや通帳を相手へ渡しません。

銀行員、警察官、全国銀行協会の職員を名乗っても、暗証番号やコードを尋ねる相手を信用しません。

確認：家族にも認証情報を送らないと決めました。

覚えておきたいこと

認証コードは、入力画面の相手が本物かを確認したうえで自分だけが使います。

SIM交換・電話番号乗っ取りへの備え

電話番号を乗っ取られて認証コードを奪われる被害に備えます。

- 携帯電話が突然圏外になったら異常を疑います。
- 携帯会社へすぐに連絡します。
- 銀行のログイン履歴と取引を確認します。
- SMS以外の認証方式があれば利用を検討します。

番号変更、SIM再発行、機種変更の通知に心当たりがなければ放置しません。

確認：携帯会社と銀行の公式連絡先を確認しました。

覚えておきたいこと

SIMスワップでは、第三者がSMS認証コードを受け取り、不正送金に使う手口が確認されています。

振込依頼・口座変更詐欺

知人や取引先になりすました振込指示を止めます。

- メールやチャットで届いた口座変更を疑います。
- いつもの電話番号など別の手段で本人へ確認します。
- 新しい口座名義と依頼者の関係を確認します。
- 高額振込は一人で即決しません。

急ぎ、秘密、今だけという指示は、送金前に立ち止まります。

確認：口座変更は別経路で確認するルールを決めました。

覚えておきたいこと

会社では、振込先変更を複数人で確認する手順を作ります。

還付金・公的機関を装う詐欺

受け取る手続きのふりをした送金を止めます。

- 還付金があるという電話を疑います。
- ATMやネットバンキングを操作しません。
- 役所の代表番号へ自分で確認します。
- 相手との通話を切り、家族や警察へ相談します。

ATMやネットバンキングの操作で還付金を受け取るという説明を信用しません。

確認：還付金の電話では操作しないと決めました。

覚えておきたいこと

警察庁は「還付金がある」「ATMで手続きできる」は詐欺と注意しています。

投資・副業・融資を装う送金

もうけ話や審査費用を理由にした繰り返し送金を止めます。

- SNSの投資・副業の勧誘を疑います。
- 個人名義や毎回変わる口座へ振り込みません。
- 登録業者か公式情報で確認します。
- 利益の出金前に追加送金を求められたら止めます。

必ず、確実、あなただけ、秘密という言葉で急かされても送金しません。

確認：送金前に家族や公的窓口へ相談します。

覚えておきたいこと

投資先やアプリが実在しても、勧誘者や振込先が本物とは限りません。

取引後の確認

操作した取引と実際の記録が一致するか確認します。

- 振込履歴で受取人と金額を確認します。
- 残高と入出金明細を確認します。
- 受付番号と日時を保存します。
- 銀行からの取引通知を照合します。

メールだけでなく、公式アプリの履歴を自分で開いて確認します。

確認：振込履歴と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

高額振込や新規振込の後は、その日のうちに履歴と通知を確認します。

利用後

身に覚えのない送金・ログイン

不正利用の拡大を止め、調査に必要な情報を残します。

- 公式アプリの明細とログイン履歴を確認します。
- 銀行の公式窓口へ直ちに連絡します。
- 安全な端末から認証情報を変更します。
- 警察へ通報・相談し、記録を保存します。

犯人や不審なメッセージへ返信せず、相手から届いた電話番号へ連絡しません。

確認：銀行と警察の連絡先を確認しました。

覚えておきたいこと

補償の有無や条件は銀行、状況、連絡時期などで異なります。自動的に補償されるとは限りません。

不正利用が疑われるときの対応

銀行、アカウント、端末、証拠の順で被害拡大を止めます。

- 銀行へ連絡し、口座とカードの停止を相談します。
- 別の安全な端末からパスワードと認証を変更します。
- 携帯会社へ回線やSIMの状態を確認します。
- 日時、金額、相手、画面、メッセージを保存し警察へ相談します。

遠隔操作中なら通信を切り、同じ端末で追加操作を続けません。銀行の連絡先は公式アプリ、カード、通帳から確認します。

確認：緊急時の4つの連絡・対応を確認しました。



操作の模式図

覚えておきたいこと

警察相談専用電話は#9110、消費生活の相談は188です。緊急性が高い場合は110番を利用します。

公式情報の出典（1）

出典 S01　金融庁：インターネットバンキングの不正送金に注意

出典 S02　警察庁：令和7年警察白書・不正送金の情勢

出典 S03　警察庁：フィッシング対策

出典 S04　全国銀行協会：ネットバンキング犯罪

出典 S05　IPA：不正ログイン対策

出典 S06　IPA：サイバーセキュリティ対策9か条

出典 S07　IPA：パスキーと多要素認証

出典 S08　IPA：リアルタイムフィッシング

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。金融庁、警察庁、全国銀行協会、各社公式サポートを参照しています。銀行、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　Google：Google Play プロテクト

出典 S10　Apple：iOSのアプリセキュリティ

出典 S11　Google：Androidアプリの更新

出典 S12　Apple：App Storeアプリの更新

出典 S13　三井住友銀行：SMBCダイレクトご利用手引き

出典 S14　みずほ銀行：振込・振替

出典 S15　みずほ銀行：ワンタイムパスワード

出典 S16　警察庁：SIMスワップと不正送金

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。金融庁、警察庁、全国銀行協会、各社公式サポートを参照しています。銀行、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　警察庁：サポート詐欺対策

出典 S18　国民生活センター：パソコンの偽警告に注意

出典 S19　国民生活センター：遠隔操作アプリを悪用した勧誘

出典 S20　警察庁：還付金詐欺

出典 S21　警察庁：SNS型投資詐欺

出典 S22　警察庁：サイバー事案に関する相談窓口

出典 S23　全国銀行協会：金融犯罪の相談・連絡先

出典 S24　警察庁：不正アクセス対策

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。金融庁、警察庁、全国銀行協会、各社公式サポートを参照しています。銀行、端末、OS、契約内容により画面や条件は異なります。