2026 年 11 月 10 日

お客さま各位

株式会社武蔵野銀行

不審なアプリや偽のメール・SMS による不正送金にご注意ください

不審なアプリや偽のメール・SMS による不正送金にご注意ください。大切なご預金を守るため、まず「１．不正送金を防ぐための３つの基本対策」をお願いいたします。

１．不正送金を防ぐための３つの基本対策

（１）**アプリは、必ず公式ストアから入手してください。**インストールは、App Store または Google Play ストアから、ご自身で行ってください。

（２）**口座残高と入出金明細を定期的に確認してください。**アプリや通帳で、身に覚えのない出金・振込がないかご確認ください。

（３）**身に覚えのない取引や通知に気づいた場合は、すぐに当行へご連絡ください。**取引のほか、ログイン通知や認証コードにもご注意いただき、お取引店または下記窓口へご連絡ください。

２．不正アプリ・なりすましを防ぐためのスマートフォン別の注意点

【iPhone（iOS）をお使いの方】

- Apple を名乗るメール・SMS・電話で、リンク先への入力や電話口での伝達を求められても、Apple アカウントのパスワード・確認コードは入力したり伝えたりしないでください。（Apple 公式サポートでも、これらの情報を他人に教えないよう案内されています。）
- 身に覚えのないサインインの承認は、許可しないでください。
- 身に覚えのないサインイン通知が届いたり、ご自身で変更していないのにパスワードが変更されたりした場合は、Apple の公式サポートへご相談ください。

【Android をお使いの方】

- アプリをインストールする際は、メール・SMS・広告・突然の警告画面のリンクからではなく、ご自身で Google Play ストアを開いて行ってください。
- 電話・メール・SMS などの相手から指示されても、「不明なアプリのインストール」「画面共有・遠隔操作」「ユーザー補助」などを許可しないでください。
- 不審なアプリをインストールしたり、相手にスマートフォンの操作を許可したりした場合、または見覚えのないアプリに気づいた場合は、武蔵野銀行アプリを使わず、別の端末・電話から当行へご相談ください。

３．不審な画面やアプリに気づいたときの対応

（１）不審な画面のボタンを押したり、パスワードなどを入力したりせず、操作を中止してください。

（２）遠隔操作や乗っ取りが疑われる場合（例：不審なアプリをインストールしてしまった、画面共有・遠隔操作を許可してしまった、操作していないのに画面が動く、身に覚えのない取引・通知

があるなど）は、スマートフォンの電源を切ってください。そのような端末では、操作を続けないでください。

（３）別の端末・電話から、お取引店または下記窓口へすぐにご連絡ください。銀行のログイン情報を不審なサイトに入力してしまった場合や、身に覚えのない取引・ログイン通知がある場合も、同様にご連絡ください。

※身に覚えのない振込・請求がある場合は、警察へもご相談ください。

【お問い合わせ先】

- **武蔵野銀行 インターネット・ヘルプデスク**
  電話番号：**0120-44-6340**
  平日 9:00～17:00（土・日・祝日・12 月 31 日～1 月 3 日を除く）
- **インターネットバンキング不正アクセス対応窓口**
  電話番号：**0120-69-6340**（上記以外の時間）

４．参考情報・これまでのお知らせ

警察庁 サイバー警察局便り「不正アプリによる不正送金被害が発生」
https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.18cpal.pdf
2026年9月17日：【武蔵野銀行アプリ】スマートフォンのウイルス感染による不正送金にご注意ください
2026年10月1日：Android スマートフォンをご利用のお客さまへ

※App Store、Apple AccountはApple Inc.のサービスマークです。iPhoneの商標はアイホン株式会社のライセンスに基づき使用されています。Android、Google Play は Google LLC の商標です。

以　上