JA バンク（JA・信連・農林中金）

JA バンクを装ったフィッシングメールにご注意ください！

本人確認を求めるメールはすべて詐欺です！

JA バンクを装った詐欺メールをお客さまへ送信し、リンク先より偽サイトに誘導して、ID・パスワード・暗証番号等を盗み取り、不正に送金を行う犯罪が発生しています。

電子メール・SMS に記載のリンク先で JA ネットバンクの ID・パスワードや暗証番号等を入力するよう求められても、絶対に入力・回答しないでください。

JA バンクでは、電子メールによる本人確認は行っておりませんので、本人確認を求める連絡やリンク先はすべて詐欺です。

今回セキュリティ対策として 2025 年 10 月 20 日より以下の対応を行いますので、ご理解いただくとともに、ご利用者様自身においても被害に遭わないための取組みをお願いいたします。

＜対策１＞振込・振替取引の限度額引き下げ
振込・振替取引の限度額を 1 日あたり 300 万円から 100 万円に変更します。

＜対策２＞振込・振替およびペイジーの限度額引き上げにかかる反映時期の変更
ワンタイムパスワードのご利用有無にかかわらず、振込・振替およびペイジーの限度額引き上げの反映を 7 日後（※）とします。
※限度額引き上げの受付完了後午前 0 時を 7 日経過した後

＜対策３＞利用者自身による IB 利用停止
ログイン ID を用いた利用者自身によるネットバンクの利用停止が可能な機能を追加します。

フィッシングメールの件名は以下のとおりであり、メールを受信しても絶対にアクセスしないでください。

＜確認されているフィッシングメールの件名例＞

・お客様情報確認のお願い（JA ネットバンク）
・お取引目的等の再確認
・【JA ネットバンク】【重要なお知らせ】お客様情報確認のご回答のお願い

＜電子メールでお取引目的やお客様情報を確認することはありません＞
　お客さまとお取引のある JA から「お客様情報確認書」が圧着式往復はがき、または封書でお手元に届くことがあります。これはマネー・ローンダリング防止対応の一環として 、お客さまに関する情報やお取引目的等を定期的に確認するものですが、JA バンクにおいては、電子メールや JA ネットバンクを経由した確認依頼は行っておりません。
　口座番号・暗証番号等を電子メール等でお尋ねすることはございませんので、そうしたものに回答しないようにご注意ください。

＜フィッシング詐欺に遭わないために＞
・JA ネットバンクを装った、不安を煽る（取引の規制、取引目的の確認など）、儲け話を持ち掛けるといった不審なメールは絶対に開封せず削除する。
・また、犯罪者が勝手に取引上限額を引き上げる場合もあるため、身に覚えのない「変更連絡」の確認メールが来ていないか注意する。
・定期的に JA ネットバンクの公式サイトからログインし、身に覚えのない取引がないか確認する。

＜取引限度額の確認、変更方法＞
・取引限度額が高額に設定されている場合、高額な被害となるケースが確認されています。
・以下の方法で設定されている限度額を確認いただき、必要に応じて適切な金額までの変更を検討ください。
　お取引メニュー※から「振込・振替」を選択　＞　「振込・振替限度額の変更」を選択　＞　現在の限度額が表示されますので、必要に応じて変更を検討ください。
※　スマートフォン版では、JA ネットバンクトップ画面の左上「お取引」から選択
※　ブラウザ版では、JA ネットバンクトップ画面の上部メニューから選択

　万が一不正サイトに口座情報等を入力してしまった場合、速やかにお取引 JA または JA ネットバンクヘルプデスクあてにご連絡いただき、JA ネットバンクの利用を停止ください。

【お問い合わせ先】
フリーダイヤル：0120-058-098
お問い合わせ時間：平日 9:00～21:00
土日祝日 9:00～17:00