

2025 年 8 月 6 日

J A バンク北海道

J A ネットバンクサービスを装ったフィッシング詐欺事例について

現在、犯罪者が JA バンク利用者の貯金を狙ってフィッシングメールを利用者あてに送付しており、偽の JA ネットバンクサイトも確認されております。

確認されているフィッシングメールでは、JA ネットバンクが緊急停止されたとの内容や、取引目的の再確認等の取引時確認のため等あたかも正当な内容であるかのような文面でメール受信者を欺き不正サイトに誘導したうえ、不正サイトでは、JA ネットバンクのログイン ID、ログインパスワードおよび口座情報等の入力求められます。

なお、金融機関としてお客様の取引目的等の定期的な確認は実施しているものの、メールや SMS にて JA ネットバンクへのログインを誘導して聞きとりを行う方法は実施しておりません。

もし、上記情報やその他認証に必要な情報を入力してしまった場合は、口座残高を不正送金される被害に遭う可能性があるため、不審なメールを受信された場合は、メールを削除いただき、メールに記載されている URL、不正サイトには、絶対にアクセスしないようご注意ください。

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。

<確認されたフィッシング詐欺事例について>

① 事例概要

- マネー・ローンダリング対策の一環で取引目的の再確認を行う旨の不審メールを受信。
- 受信メールのリンク先をクリックしたところ、「JA 名」「店舗名」「口座番号」の入力を求められたため、これを入力してしまう。
- その後、音声ガイダンスにより数字 2 桁の認証番号を伝えられ、その認証番号をガイダンス終了後に入力するよう案内があり、指示通りこれを入力。
- その後、再度画面が切り替わり「生年月日」と「キャッシュカードの暗証番号」の入力を求められたためこれを実施。
- 同日中に残高が不正送金されていることが判明。

② 被害を防ぐために

本件事案を例にとれば、以下の点被害防止のため改めてご注意くださいようお願い申し上げます。

- ☆ 本件事案のようなメールや SMS で重要な情報の取得を試みる施策は実施していないため、少しでも不審に感じた場合は口座をお持ちの JA にお問い合わせください。
- ☆ JA ネットバンクにおける振込限度額は必要最低限の設定を推奨します。(被害額拡大防止に繋がります)

以 上