

2026 年 7 月 6 日

ボイスフィッシングの新たな手口にご注意ください

他の金融機関において、インターネットバンキングを狙ったボイスフィッシングによる不正送金被害が発生しており、最近では、パソコンやスマートフォンの遠隔操作を組み合わせた手口も確認されています。不審な電話・メール等に対しては、誘導された操作を絶対に行わないようご注意ください。

1 詐欺の手口

- ・ 自動音声で連絡があり、応答すると有人に切り替わる（最初から犯罪者が有人の電話をかけてくるケースも確認されています）。
- ・ 有人対応に切り替わった後、ウイルス対策ソフトの更新や取引制限の解除等を口実として、ログイン情報やメールアドレスを聞き出される。
- ・ 金融機関を装ったメールで送られてきたリンクをクリックすると、意図せずに遠隔操作ソフト等のインストールが行われます。
- ・ インストール後、「システム更新中」等の画面が偽装され、その裏側で遠隔操作により不正送金が行われます。

2 お客さまへのお願い

JA よりお客さまに対して、ネットバンク取引にかかるお客さまのログイン ID・パスワード・メールアドレス等を聴取することはございません。

被害防止のため、以下の点にご注意ください。

- ① JA 担当者を名乗る者から電話があった際は、お取引に必要な情報を回答せず、担当者の部署・氏名等を聞いたうえ、（案内された折り返しの連絡先ではなく）JA の代表番号から担当者に連絡するなど、慎重に対応してください。
- ② メール等に記載されているリンクをクリックしたり、QR コードを読み取ったりして、案内されたサイトにアクセスしないでください。

万が一、電話でログインに必要な情報を回答したり、不正サイトに情報を入力した場合は、緊急時のセキュリティ対策として、お客さまの端末から利用停止（※）の操作が可能です。

操作方法でご不明点等がある場合は、JA ネットバンクヘルプデスクにお問い合わせください。

不審な電話を受けた場合や被害に遭われた場合は、お客さまの所在地管轄の警察署およびお取引 JA までご連絡ください。

リンク先を設定

https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.6cpal.pdf

警察庁が発行している「サイバー警察局便り（2026Vol.6）」も併せてご参照ください。

(※)利用停止の操作方法是[緊急利用停止機能の操作方法ページ]をご参照ください。

リンク先を設定

<https://www.jabank.jp/securities/emergencystop>

本件に関するお問い合わせ先

JA ネットバンクヘルプデスク

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