令和７年 12 月１日
JA バンク（JA・信連・農林中金）

法人口座を狙った**ボイスフィッシング**にご注意ください

最近、他の金融機関において、法人口座資金を狙った、フィッシングによるインターネットバンキング不正送金事犯の被害が立て続けに発生しています。

基本的にＪＡよりお客様に対して、ネットバンク取引に関してお客様のログイン ID・暗証番号・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。以下の対応により被害に遭わないようご注意ください。

１．ＪＡ担当者を名乗る者から電話があった際は、担当者の部署・氏名等を聞いた上、JA の代表番号から担当者に折り返し連絡するなど、慎重に対応すること。
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、フィッシングサイトにアクセスしないこと。

万が一不正サイトに情報を入力してしまった場合は、緊急時のセキュリティ対策として、ユーザ単位で利用停止がお客さまの端末で操作可能です。操作方法でご不明点等ございましたら、法人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、お客様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。

（※)ユーザ単位での利用停止の操作方法は「よくあるご質問・企業管理・ユーザ管理 Q18」をご参照ください。

【銀行を騙った者から一般企業宛てに電話連絡があった後、フィッシングメールが送られてくる事例】

１．Ａ会社にＢ銀行担当者を名乗る者（以下「犯人」という。）から電話がかかってきた（先立って銀行名を騙った自動音声の電話がかかってくる場合もあり)。
２．犯人から「インターネットバンキングの電子証明の期限が切れているので更新してもらいたい。これからメールで URL を送信するので、メールアドレスを教えてほしい。」と言われたので、Ａ会社担当者はメールアドレスを教えた。
３．その後、Ａ会社宛てにリンクが書かれたメール（フィッシングメール）が届いた（犯人との通話は継続している状態)。
４．Ａ会社担当者がそのメールに書かれたリンクをクリックすると、ID やパスワードを入力する画面（フィッシングサイト）が表示された。
５．犯人の電話指示に従い、Ａ会社担当者が契約者番号・ID・パスワードを入力すると、

次に取引実行パスワードやワンタイムパスワードを入力する画面が表示された。

6．さらに犯人の電話指示に従い、A会社担当者がワンタイムパスワードを入力すると、犯人から「手続きは終了した。」と言われ、通話を終えた。

7．その後、A会社担当者がA会社の口座残高を確認すると、資金がA会社と全く無関係の法人口座へ不正送金されていることが判明した。

警察庁が発行している「サイバー警察局便り（2025Vol.1）」も併せてご参照ください。

本件に関するお問い合わせ先
法人 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 9:00～18:00