

2026年7月3日

金融機関を装ったボイスフィッシングによる不正送金にご注意ください

金融機関の職員などを騙る犯人が電話でフィッシングサイトへ誘導し、口座のログインパスワード等を入力させて不正送金を行う「ボイスフィッシング」の被害が急増しています。本ボイスフィッシングの新たな手口として、**『遠隔操作ソフト』を悪用した詐欺被害**が確認されておりますので、以下の手口を確認のうえ、より一層ご注意くださいようお願いいたします。

●確認されている新たな手口の例

- ①銀行を騙った電話（自動音声）がかかってくる。電話にでると「PC環境の更新が必要」などと言われ、メールアドレスと電話番号を教えるよう指示される。
- ②伝えたメールアドレスや電話番号あてにメッセージが届き、**記載されているリンク先から「セキュリティ強化のためのソフト」と称する遠隔操作ソフトをインストールするよう指示される**。インストールすると、犯人に端末を遠隔操作される。
- ③メッセージのリンクから偽サイトへ誘導され、インターネットバンキングのID・パスワードを入力させられて情報を盗み取られる
- ④**②の遠隔操作している被害者端末上に偽の画面（「システム更新中」等）を表示される**。お客さまが操作できない間に③の盗み取られたID・パスワードを悪用され不正送金されてしまう。

●被害に遭わないために

- ・銀行から電話があった際には、営業店や代表電話に折り返し、本物かどうか確認するようにしてください。
- ・銀行を騙るメールが届いたら、記載されているURLや2次元コードには絶対にアクセスしないでください。
- ・**十六銀行がパスワードや暗証番号等をお尋ねすることは一切ありません**。そのような電話（自動音声を含む）やメールはすべて詐欺ですので、絶対に教えないでください。

万一、被害に遭われた場合は、下記連絡先および最寄りの警察署へご通報ください。

【不正利用時など緊急のご連絡先】

電話番号	受付時間
0120-69-5416	24時間365日

以上