「重要」当信用組合を騙った
不審な音声通話（ボイスフィッシング）にご注意ください。

2025年3月17日

現在、銀行や信用金庫、農協等の担当者を装い、お客様情報等の確認を求め、お客様の個人情報や法人の口座情報等の不正取得を行おうとする音声通話を利用した詐欺手口が生じているとの情報が寄せられています。今後、全国信用組合中央協会や信用組合においても同様の詐欺手口が生じるかもしれません。下記の事項にご注意いただきますようお願い申し上げます。

＜ボイスフィッシングの事例＞

① 「○○信用組合です。ネットバンキングの電子証明書の更新手続きが必要です。
　更新用のリンクを送りますのでメールアドレスを教えてください。」という電話がある
② 送付されたリンクにアクセスしてしまうことでフィッシングサイトへ誘導される
③ フィッシングサイトにインターネットバンキングのアカウント情報などを入力
④ フィッシングサイトで入力した情報を使って不正送金が行われてしまう

こうしたボイスフィッシング被害に遭わないために、３つの対策をして下さい。

① 知らない電話番号からの着信は信用しない
② 銀行の代表電話番号・問い合わせ窓口で確認する
③ メールに記載されているリンクからアクセスしない

また、当組合では音声通話による上記のような情報発信はしておりませんので、少しでも不審と感じたら、すぐに当組合のお問い合わせ窓口までご連絡ください。

【本件に関するお問い合わせ先】
本部　総合企画部　0120-097-874
受付時間（平日）　9：00～17：00

育てよう 未来に向けた 地域の絆
埼玉信用組合
イメージキャラクターのカワセミどっとくんです。

今、大切な資産が狙われています！！

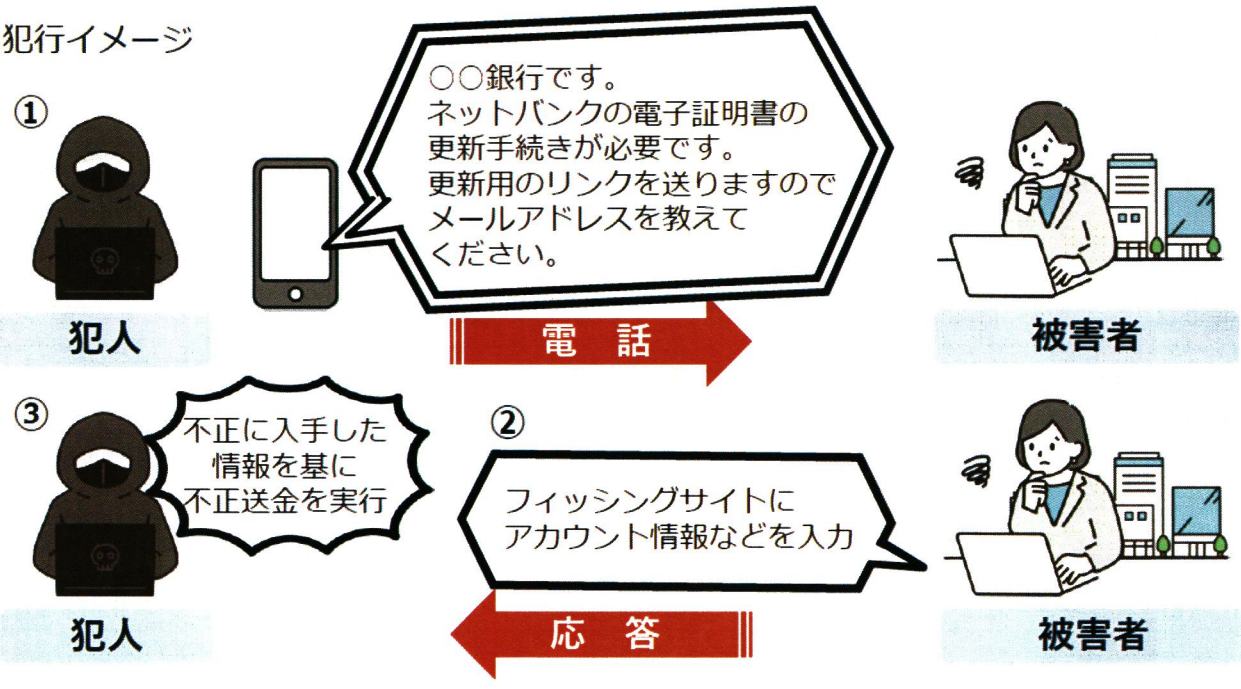
電話に注意！「ボイスフィッシング」による不正送金被害が急増

ボイスフィッシング（ビッシング）とは、音声（Voice）とフィッシング（Phishing）とを合わせた造語で、**音声通話を利用して個人情報や金融情報などを窃取しようとする詐欺の手口**です。**企業・個人問わず、詐欺の電話が確認されています**ので、注意しましょう。

▸手口の概要

1. 犯人が銀行担当者を騙り、被害者に電話をかけ、メールアドレスを聞き出す。
2. 犯人がフィッシングメールを送信し、電話で指示しながら、被害者をフィッシングサイトに誘導。そして、インターネットバンキングのアカウント情報等を入力させて、盗み取る。
3. フィッシングサイトに入力させたアカウント情報等を使って、犯人が被害者の口座から資産を不正に送金する。

※犯行イメージ



ボイスフィッシング被害に遭わないために！3つの対策

- **知らない電話番号からの着信は信用しない！**
- **銀行の代表電話番号・問い合わせ窓口で確認する！！**

  銀行担当者を騙る者から連絡があった場合には、銀行の代表電話番号へ連絡して確認するなど、慎重に対応しましょう。
- **メールに記載されているリンクからアクセスしない！！！**

  インターネットバンキングにログインする場合は、銀行公式サイトや公式アプリからアクセスしましょう。

もしも、被害に遭ってしまったら警察に通報・相談を！

サイバー事犯に関する通報等の窓口 ➡ https://www.police.pref.saitama.lg.jp/c0070/kurashi/joho110-cyber.html

埼玉県警察 サイバーセキュリティレポート　R6.12
サイバー局サイバー対策課