令和７年３月１８日

両 備 信 用 組 合

インターネットバンキング取引における「ボイスフィッシング」による不正送金に関する注意喚起について

現在、金融機関を騙る「ボイスフィッシング」による不正送金事案が他県で確認されているため、下記により注意喚起申し上げます。

当組合では、自動音声による案内等は一切行っておりません。また、自動音声や電話、E-mail、SNS 等でお客様の契約情報やログインＩＤ・パスワード等をお伺いすることも一切ありません。当組合を騙る自動音声の電話があった場合は、決して対応しないでください。

また、口座に不審な取引等が確認される場合は、最寄りの支店までお問い合わせください。

１．確認されている手口

（１）犯人が銀行担当者を騙り、被害者（企業）に電話をかけ（自動音声の場合あり）、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、犯人が口座から資産を不正に送金する。

２．被害を防ぐための対策

（１）上記手口のような電話があった場合は、すぐに電話を切り、誘導された操作を絶対に行わない。また、金融機関が送信する電子メールでお客さまの個人情報やインターネットバンキング契約者情報などの入力を求めることは絶対にないため、契約者情報等を絶対に入力せず、速やかにメールを削除する。

（２）知らない電話番号には出ない、知らない電話番号からの着信は信用しない。

（３）信用組合の担当店窓口に確認する。

※信用組合担当者を騙る者から連絡があった場合には、信用組合の担当店窓口へ連絡して確認するなど、慎重に対応する。

（４）メールや SMS に記載されているリンクからアクセスしない。

【参考資料】

サイバー警察局便り（2024 年（R6）Vol.15）

サイバー警察局便り

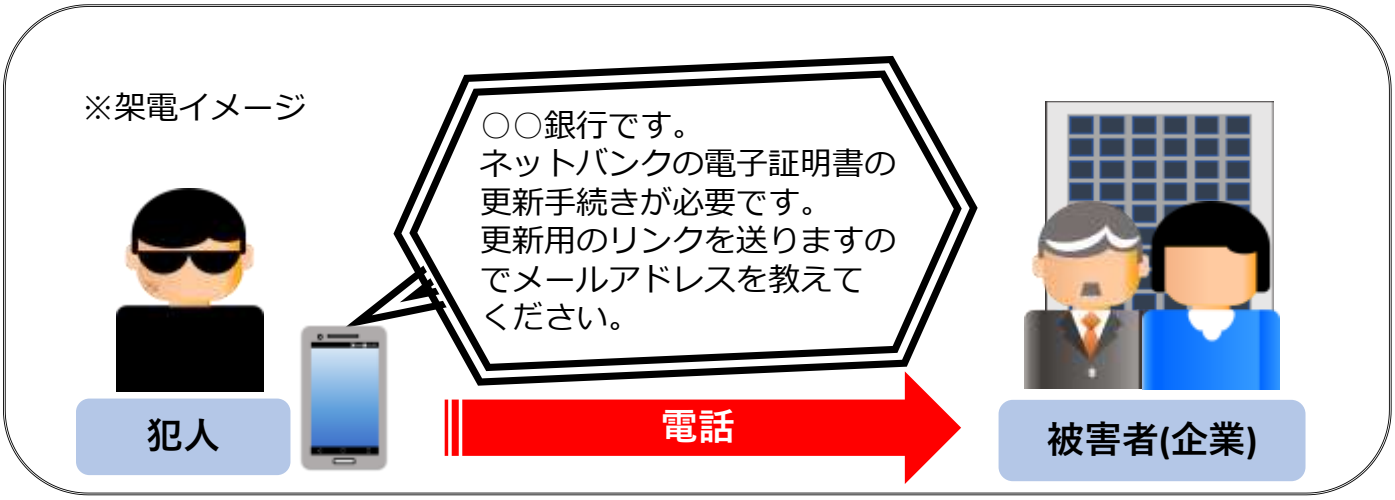
Cyber Police Agency Letter 2024(R6) Vol.15

今、企業の資産（法人口座）がねらわれている！！

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

【手口の概要】

1. 犯人が銀行担当者を騙り、被害者（企業）に電話をかけ（自動音声の場合あり）、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、犯人が法人口座から資産を不正に送金する。



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、慎重に対応してください。
- **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てください。

もしも、被害に遭ってしまったら警察に通報・相談を！

最寄りの警察署又はサイバー犯罪相談窓口 https://www.npa.go.jp/bureau/cyber/soudan.html

JBA 一般社団法人 全国銀行協会　金融庁 Financial Services Agency　警察庁 National Police Agency　JC3 日本サイバー犯罪対策センター