令和７年12月19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急増しているため、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（2025年（R7）Vol.12）

サイバー警察局便り

Cyber Police Agency Letter　2025 Vol.12 (R7.12)

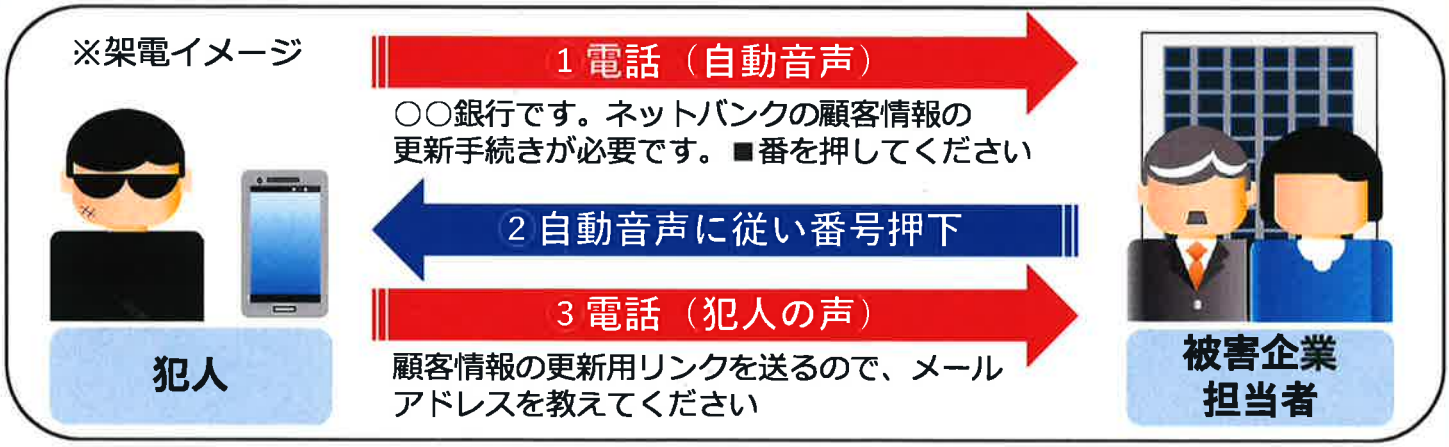
その電話、本当に銀行からですか？

電話を利用する「ボイスフィッシング」被害が再び発生

ボイスフィッシングによる法人口座を狙った不正送金被害が再発・急増している。

企業の法人口座を狙う、その手口とは？

1. 犯人が銀行関係者をかたり、企業に電話をかけ、メールアドレスを聴取する
2. メールを送信して偽サイトに誘導し、ネットバンクの認証情報等を入力させる
3. 犯人は認証情報等を利用し、法人口座から企業の資産を不正送金する



どう見分ける？こんな電話は偽物！

- 発信元番号が国際電話（+国番号）である（例：+1 800 123 4567）
- 自動音声ガイダンスが流れたのち、人間の声に切り替わる
- 通話中にメールアドレスを聴取され、リンク付きメールが送られる

社内で徹底！被害を防ぐために

- **銀行から電話があれば、営業店・代表電話に折り返し、本物かどうか確認する**
- **インターネットバンキング利用時は、銀行公式サイト・アプリからアクセスする**

詐欺電話対策として"国際電話着信ブロック"もあります

みんなでとめよう!!国際電話詐欺 → https://www.npa.go.jp/bureau/safetylife/sos47/case/international-phone/

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

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