

2025年 4月 7日

お客さま各位

株式会社東和銀行

銀行を騙る不審な電話（ボイスフィッシング）による
インターネットバンキングの不正送金に関するご注意について

警察・サイバー関連の情報提供機関等より、地方銀行の法人向けインターネットバンキングなどで発生している不正送金事案に関する注意喚起が行われています。

注意喚起には、複数の地方銀行のインターネットバンキングサービスにおいて、銀行を騙って、悪意のある第三者から「インターネットバンキングの契約情報を更新する」「取引に制限がかかる」「不正なアクセスがあった」などと不安を煽り、言葉巧みに、お客さまのメールアドレスやインターネットバンキングの契約情報、ワンタイムパスワード情報を聞き出す不審な電話（自動音声を含む）が確認されているとあります。

<具体的な手口事例>

- 犯人が銀行担当者を騙り、電話（自動音声を含む）により、メールアドレスを聞き出す。
- 聞き出したメールアドレスあてにフィッシング*メールを送信し、電話で指示しながらフィッシングサイトに誘導して、契約者情報やパスワード情報等を入力させ、盗み取る。
※ 実在のサービスや企業を騙り、偽のメールやSMSで偽サイトに誘導し、IDやパスワードを盗んだり、マルウェアに感染させたりする手口。
- フィッシングサイトに入力された情報を使って、インターネットバンキングサービスにログインして、口座から不正に送金する。

<被害にあわないためのポイント>

- 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。
- 不審な電話を受けた場合は、お取引店へ連絡して確認するなど、慎重に対応する。
- メールやSMSに記載されているリンクからアクセス（URLをクリック）しない。
- 電話・SMS・メールなどで契約者情報やパスワードなどの入力を求められても、絶対に入力や回答しない。
- 振込限度額が、普段のお取引金額と比べ過大になっていないか確認する。
- 振込時は承認機能のご利用により複数人で確認する。

当行は勿論、通信事業者や警察等の第三者が、お客さまのパスワード等の秘密情報を電話によりお聞きすることは絶対にありません。

このような電話があった場合は、直ぐに電話を切り、誘導された操作については絶対に行わないでください。

<お問い合わせ先>
ネットバンキング共同受付センター
0120-108-373

以上



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。

※架電イメージ



犯人



〇〇銀行です。
ネットバンクの電子証明書の
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。

電話



被害者(企業)

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>

