十六銀行
16FG

商品・サービス

２０２５年１２月１２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

電話やメールを巧みに組み合わせた手口による不正送金が増えています。特に、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。

お客さまのログインパスワードやワンタイムパスワード等の入力を求めるメールや電話は詐欺です。第三者からの指示で、パスワード等を入力したり、口頭で伝えたりすることは絶対に行わないようお願いします。

●確認されている手口の例

① 犯人が銀行員などを名乗って電話をかけ（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サイトのＵＲＬや２次元コードを記載したメールを送信し、電話で指示しながら正当なサイトを模倣した偽サイト（フィッシングサイト）へ誘導する。
③ 偽サイトでインターネットバンキングの情報等を入力させ、ＩＤやパスワード等を盗み取る。
④ 偽サイトに入力させた情報を使い、犯人が被害者の口座から不正送金を行う。

●被害に遭わないために

・心当たりのない電話番号や国際電話（「+」で始まる番号）からの着信には、相手の部署や氏名等を確認したうえで、折り返し連絡するなど慎重に対応してください。
・不審なメールが届いたら、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

出典:警察庁ウェブサイト
(https://www.npa.go.jp/bureau/cyber/pdf/R7_Vol.12cpal.pdf)を加工して作成

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？

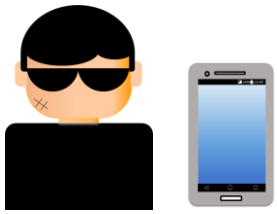
電話を利用する「ボイスフィッシング」被害が再び発生

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

※架電イメージ



犯人

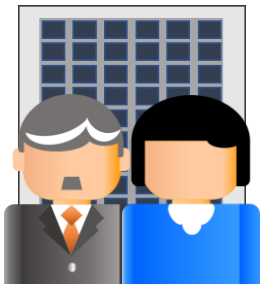
①電話（自動音声）

○○銀行です。ネットバンクの顧客情報の更新手続きが必要です。■番を押してください

②自動音声に従い番号押下

③電話（犯人の声）

顧客情報の更新用リンクを送るので、メールアドレスを教えてください



被害企業担当者

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