

信用金庫を騙る

詐欺電話・詐欺メールにご注意ください!!

本年 5 月以降、金融機関を騙る詐欺電話（ボイスフィッシング）が全国で多数発生しているとの報告を受けています。

ボイスフィッシングとは、金融機関の担当者を騙って企業や個人に電話して（自動音声の場合もあります）、言葉巧みにメールアドレスを聞き出すなどの方法で「セキュリティ強化のためのソフト」と称する不正利用のための遠隔操作ソフトをインストールさせ、お客さまがご利用の端末を遠隔操作することにより不正送金を行うなどの手口のことを言います。

当金庫をはじめとする信用金庫や全国信用金庫協会が、お客さまに対して

- ① 口座番号やキャッシュカードの暗証番号などお客さま情報の確認や連絡先の提供をお願いすること
- ② インターネットバンキングのお客さま ID やパスワードを確認すること
- ③ 現金などの支払いを要求すること

は、いずれも一切ありません。

このような内容と同じような電話やメールを受信した場合には、安易に相手に伝えたりせず必ず先に当金庫へ確認していただくようお願いいたします。

またこのような被害にあってしまったかもしれないなど、ご心配やお気づきの点がございましたら、直ちにご利用端末の電源のシャットダウンを行い、以下のサポート窓口へご連絡いただくか、当金庫お取引店窓口へご連絡ください。

本件に関する問い合わせ先
すわしんサポートセンター
(諏訪信用金庫 事務部内)
電話 : 0120-03-1917

ボイスフィッシングについて、くわしくは次のページをご覧ください。





サイバー警察局便り

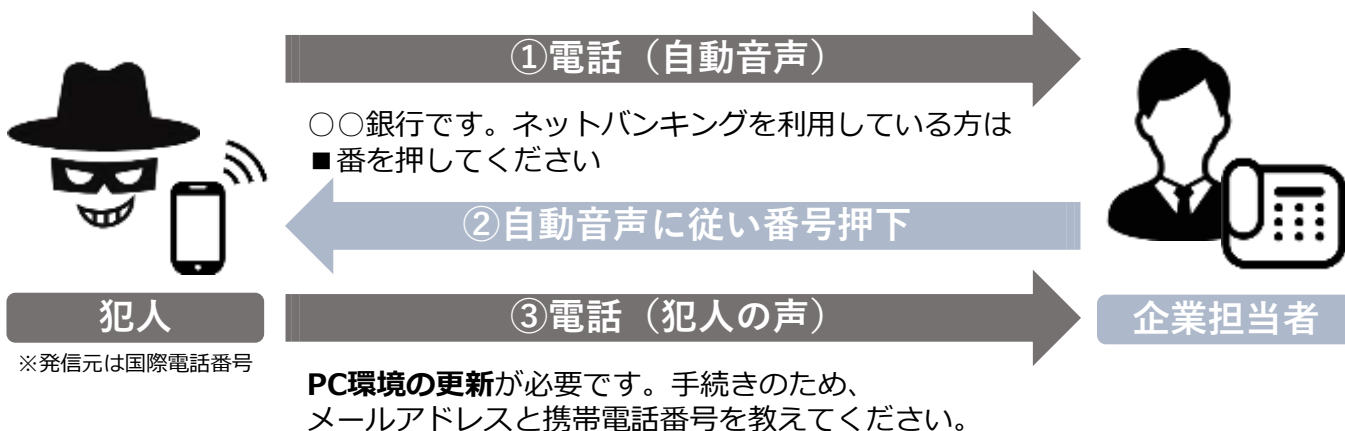
Cyber Police Agency Letter 2026 Vol.6 (R8.6)

巧妙化する「ボイスフィッシング」被害に注意

遠隔操作ソフトを悪用した手口が新たに発生

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手口を変えて再発

※ 架電イメージ



- I. 偽メールのリンクをクリックさせ、「セキュリティ強化のためのソフト」と称する**遠隔操作ソフトをインストール**、企業側の端末を遠隔操作
- II. SMSのリンクをクリックさせて偽サイトに誘導、ネットバンキングのID・パスワードを窃取
- III. Iの遠隔操作している企業端末に偽の画面（「システム更新中」等）を表示その間にIIのID・パスワードを悪用して不正送金を実行

被害を未然に防ぐために社内で徹底！

- 銀行をかたるメールやSMSに記載のリンク等へのアクセスは禁止
- 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

 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>

