

お客さま各位

永和信用金庫

【重要なお知らせ】信用金庫を騙ったボイスフィッシングについて(ご注意ください)

記

最近、信用金庫を騙る不審な電話(ボイスフィッシング)が相次いでいます。犯人は、セキュリティ対策ソフト「Rapport(ラポート)」のインストールを装い、偽のソフトをダウンロードさせるなどの手口で、お客さまのインターネットバンキングの ID・パスワードを盗み取ろうとします。その後、電話で指示をしながら振込操作をさせるなど、不正送金被害につながる非常に危険な行為が確認されています。

【当金庫が絶対に行わないこと】

- 電話でセキュリティソフトのインストールをお願いすること。
- 電話やメールでインターネットバンキングの ID・パスワードをお聞きすること。
- 電話で振込操作を指示すること。

これらを求める電話はすべて詐欺です。

【Rapport(ラポート) について】

※本ソフトウェアは、インターネットバンキングを攻撃対象とするウィルス対策ソフトです。

インターネットバンキングに特化しているため、市販のウィルス対策ソフトと併せてご利用ください。

※本ソフトウェアは、パソコン専用です。スマートフォンやタブレット端末では、ご利用できません。

※本ソフトウェアは、インターネットログイン画面にてダウンロードできます。

【不審な電話を受けた場合】

- その場で操作を続けず、すぐに電話を切る。
- 不審なソフトをインストールしてしまった場合は、インターネットバンキングの利用停止・パスワード変更などをご案内いたします。
- お心当たりがある場合は、速やかに当金庫までご連絡ください。

【最後に】

当金庫では、お客さまの大切な資産を守るため、詐欺被害防止に取り組んでおります。

不審なメールやメッセージを受け取った際は、速やかに当金庫までご相談ください。

以 上



サイバー警察局便り

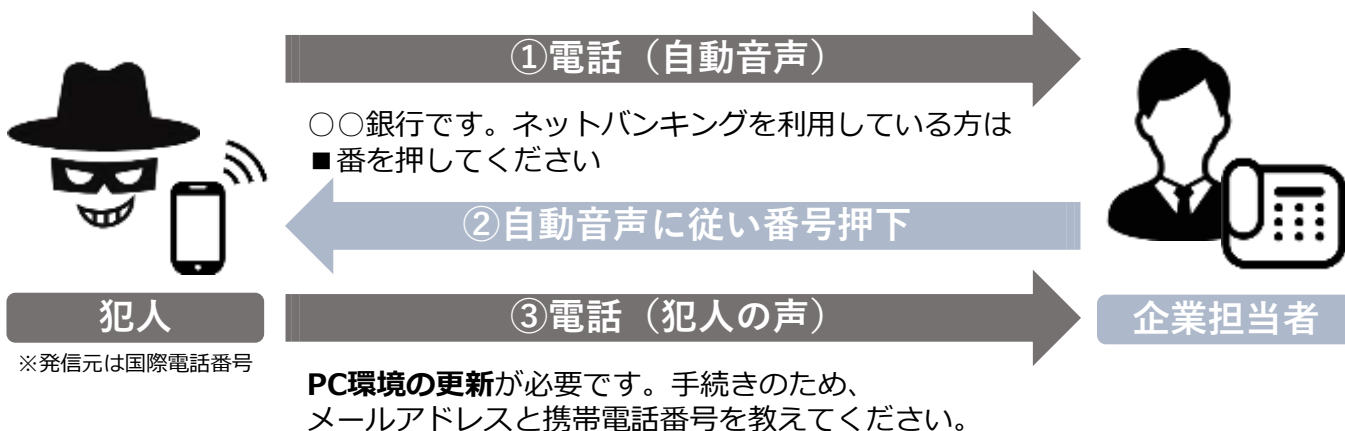
Cyber Police Agency Letter 2026 Vol.6 (R8.6)

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>

