【重要】信用金庫を騙る不審な電話（ボイスフィッシング）にご注意ください

現在、信用金庫の職員や担当者を騙り、インターネットバンキングの利用者から情報を盗み取ろうとしたり、不正な操作をさせたりする**「詐欺電話（ボイスフィッシング）」**の被害や不審な入電が全国で報告されています。

主な手口としては、**「電子証明書の更新手続きが必要である」と電話でアプローチ**し、聞き出したメールアドレス宛にフィッシングサイトの URL を送り、インターネットバンキングの ID・パスワードなどのアカウント情報を入力させて盗み取ろうとします。また、**「セキュリティを強化するソフトを入れる必要がある」と案内**し、不正なソフトをダウンロードさせた上で、振込操作を促し資金をだまし取るケースも確認されています。

「信用金庫」や「信用金庫協会」などが、お客さまに対して「自動音声ガイダンス」「ショートメール（SMS）」「電子メール」を通じて個人情報をお尋ねすることや、セキュリティ対策ソフトのダウンロード等を案内することは一切ありません。
また、電子証明書の有効期限や更新手続きについて、当金庫の担当者からお電話をすることもありません。

万が一、不審な電話やメールを受け取った場合は、指示に従わず、速やかに下記問い合わせ窓口へご連絡ください。

本件につきましては、下記の「サイバー警察便り」もご参照ください。

【本件に関するお問い合わせ窓口】
しずおか焼津信用金庫 事務部：054-629-1113　（受付時間：平日 9:00～17:00）

地域の未来によりそう
しずおか焼津信用金庫

サイバー警察局便り

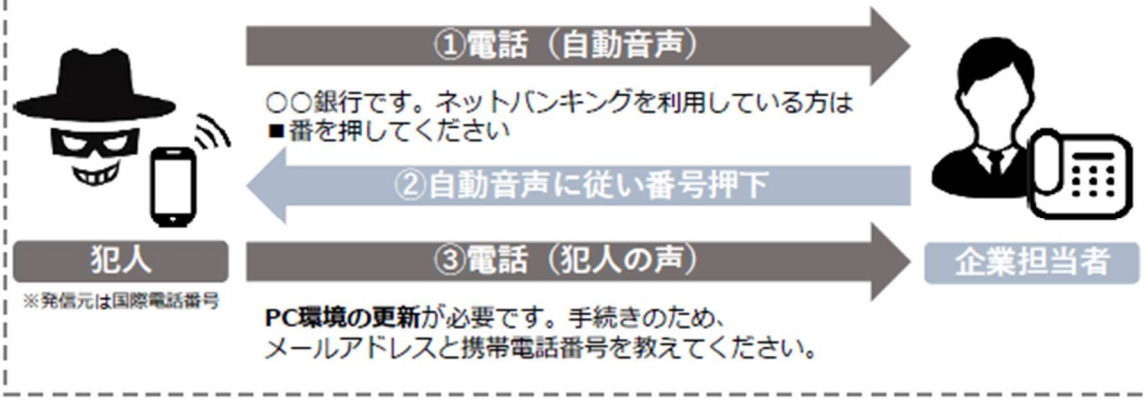
Cyber Police Agency Letter 2026 Vol.6 (R8.6)

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

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