２０２６年６月２日

お客様各位

# ボイスフィッシング詐欺にご注意ください

平素より、当金庫サービスをご利用いただきありがとうございます。

現在、信用金庫を騙り、電話で不正なソフトのダウンロードやインターネットバンキングの情報を聞きだす、「ボイスフィッシング詐欺」が全国で多発しています。

**【当金庫からのお願い】**

当金庫やヘルプデスクから以下の情報を電話でお聞きすることや操作を指示することはございません。

・暗証番号・ワンタイムパスワード・メールアドレス・ソフトダウンロード

・電子証明書の更新

**【このような電話やメールにはご注意ください】**

・不正ログインがありました

・至急ログインが必要です

・電子証明書の更新が必要です

・受け取れるポイントがもうすぐ消失します

**【不審な電話等を受けた場合】**

・その場で情報は伝えない

・一度電話を切る

・当金庫に相談する

・URL 等はクリックしない

電子証明書の有効期限や更新について、信用金庫の担当者から電話することはございません。また、自動音声による案内も一切行っておりません。

■ボイスフィッシングによる不正送金被害が急増していることから、警察庁ウェブサイトにて下記の通り注意喚起を実施しております。

https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.6cpal.pdf

※出典元：警察庁サイバー警察局

お客様の大切な情報・資産を守るため、不審な電話やメールには十分ご注意ください。

お問合せは、下記電話番号までお願います。　以 上

本件に関する連絡先
情報システム部
ＴＥＬ:0244-23-5132
（平日 9:00～17:00）

あぶくま信用金庫

# 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

犯人

※発信元は国際電話番号

①電話（自動音声）

○○銀行です。ネットバンキングを利用している方は
■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）

**PC環境の更新**が必要です。手続きのため、
メールアドレスと携帯電話番号を教えてください。

企業担当者

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