令和８年６月

帯広信用金庫

「ボイスフィッシング」被害にご注意ください！

遠隔操作ソフトを悪用した新たな手口で、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しています。

犯人が法人インターネットバンキングの利用者に対して「セキュリティ強化のためのソフト」をインストールさせ、企業側の端末を遠隔操作することにより不正送金を行うといった新たな手口が確認されております。

詳しくは、下部のＰＤＦ（『サイバー警察局便り』）をご覧ください。

【手口の概要】

① **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**

↓

② **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**

↓

③ **①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②のＩＤ・パスワードを悪用して不正送金を実行**

☞銀行を語るメールや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！

豊かな十勝の未来のために
帯広信用金庫

サイバー警察局便り

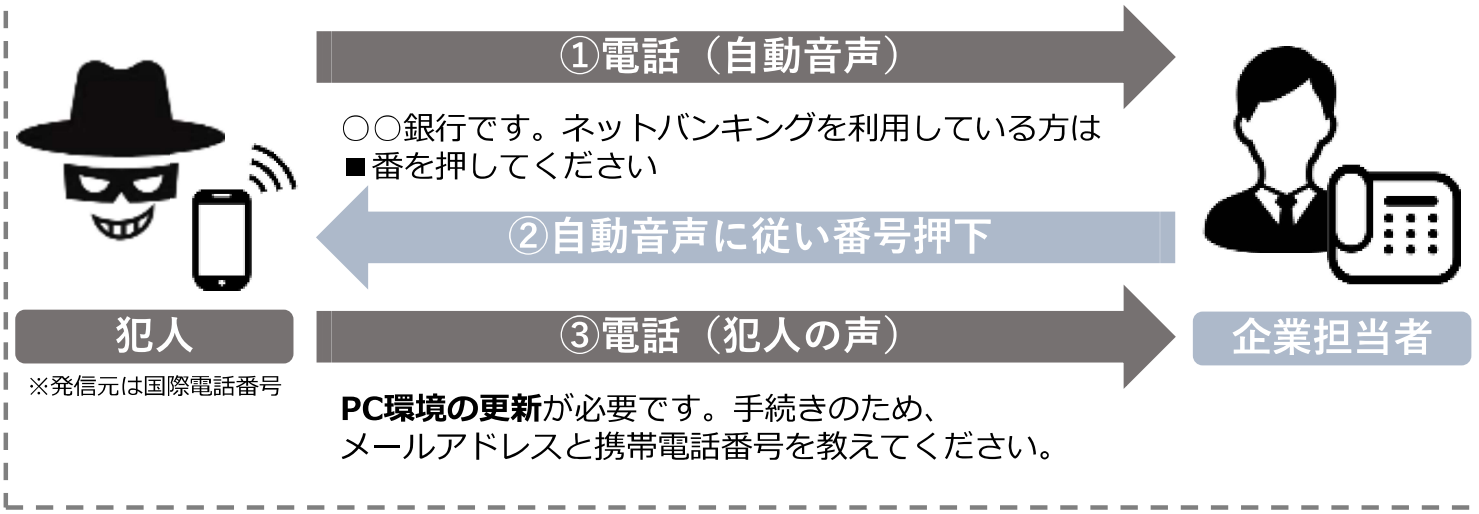
Cyber Police Agency Letter 2026 Vol.6 (R8.6)

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