Cyber Security News

R8.6

銀行等を名乗った電話等

音声を交えた犯罪の手口

ボイスフィッシング

に注意！

ボイスフィッシング

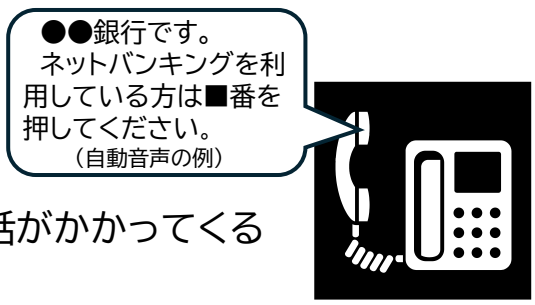
実在のサービスや企業を名乗って偽のメールやSMSで偽サイトに誘導し、ID、パスワードや個人情報を盗んだり、マルウェア（悪意あるソフトウェア）に感染させたりする手口をフィッシングと呼びますが、偽のメールやSMSだけでなく電話等の音声（ボイス）を交えて行うものを

ボイスフィッシング

（Voice Phishing）

と呼びます。（「ビッシング」と呼ぶこともあります）

自動音声から始まることや企業担当者に直接電話がかかってくることもあります。



令和7年のボイスフィッシングによる不正送金被害

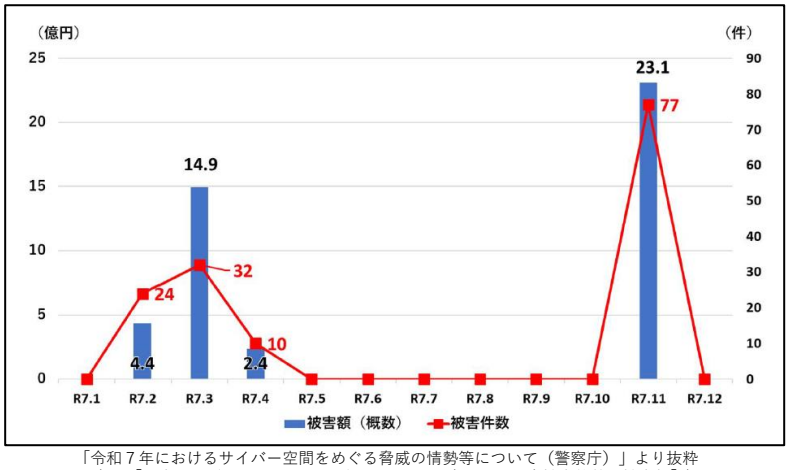
令和6年秋から令和7年4月にかけてボイスフィッシングによる法人口座の不正送金被害が急増し、同年11月には再び急増しました。

警察庁の資料によると、被害額（概数）は、

令和7年3月中　14億円超

令和7年11月中　23億円超

となっています。



「令和７年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）」より抜粋
（p29【図表23：ボイスフィッシングによる法人口座の不正送金被害件数・被害額】）

令和8年のボイスフィッシングの手口

令和8年には、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、遠隔操作ソフトをインストールさせてくるなど、手口を変えて再発しています。

CyberSecurityNews（巧妙化する「ボイスフィッシング」被害に注意）を参照し、対策をとりましょう。 https://www.police.pref.kanagawa.jp/kurashi/cyber_hanzai/mesd7047.html

神奈川県警察サイバーセキュリティ対策本部

Cyber Security News

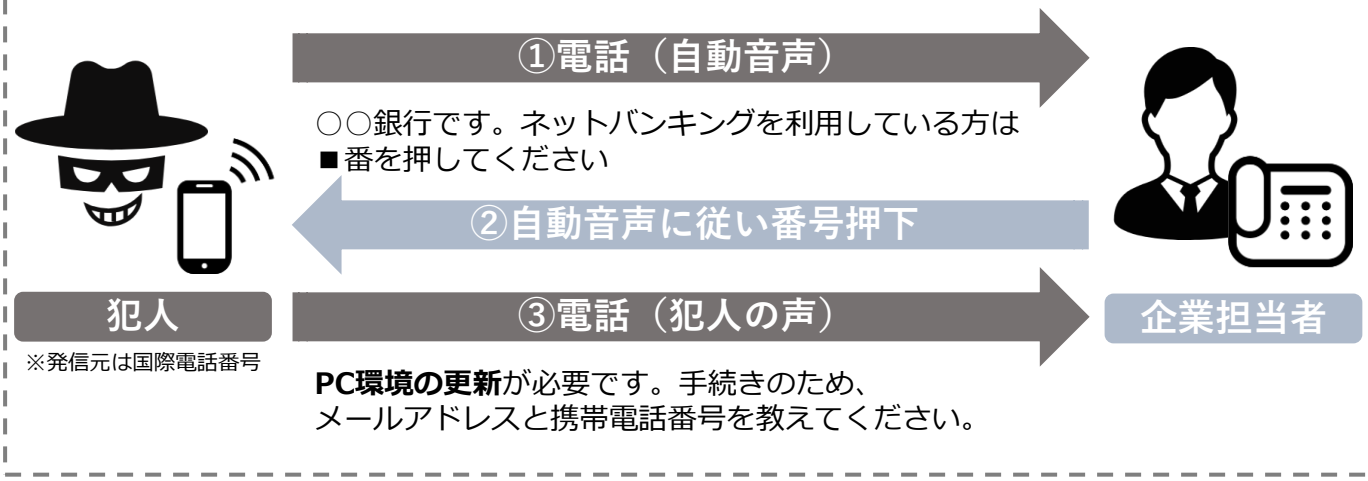
R8.6

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 JBA JAPANESE BANKERS ASSOCIATION
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
神奈川県警察 サイバーセキュリティ対策本部