

銀行から電話…はたして本物？企業の資産が危ない

電話を利用する「ボイスフィッシング」被害が多発！

- ➡ 昨年より、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継続して発生
- ➡ 全国的に被害が拡大しており、1社あたり**数億円規模**の被害も確認

企業の資産を狙う手口「ボイスフィッシング」とは？

1. 犯人が銀行関係者をかたり、企業に**電話**をかけ、自動音声ガイダンスを流す
2. 音声に従い番号を押すと、犯人に切り替わる（始めから犯人が電話することもある）
3. メールアドレスを聞き出し、**フィッシングメール**を送信
4. メールに記載のリンクから偽サイトに誘導し、インターネットバンキングのアカウント情報を入力させる
5. 犯人はアカウント情報等を利用し、法人口座から資産を**不正送金**する

※犯行の流れ（例）

①電話（自動音声）

〇〇銀行です。ネットバンクの顧客情報の更新手続きが必要です。■番を押してください

②自動音声に従い番号を押す

③電話（犯人の声）

顧客情報の更新用リンクを送るので、メールアドレスを教えてください



犯人



被害企業
担当者

どう見分ける？こんな電話は偽物の可能性大！

- ➡ 発信元番号が**国際電話**(+ 国番号)、または**非通知**となっている
- ➡ **自動音声ガイダンス**が流れたのち、人間の声に切り替わる
- ➡ 通話中に**メールアドレスを聞かれ**、リンク付きのメールが送られる

社内で徹底！被害を防ぐために

◆ 銀行から電話があれば、**本物かどうか確認する！**

上記に該当する特徴があったら、一旦切って、銀行の問合せ先に確認してください

◆ メールに記載されている**リンクからアクセスしない！！**

インターネットバンキング利用時は、銀行公式サイト・アプリからアクセスしてください

もしも、被害に遭ってしまったら警察に通報・相談を！



北海道警察公式HP
サイバーセキュリティひろば

北海道警察



YouTube動画
サイバーセキュリティ講座

