



被害拡大の恐れあり！

～過去に発生したボイスフィッシングに使用されたサイトと同様の特徴が見られるサイトを複数観測～

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

- ▶ 昨年より、ボイスフィッシング（ビッシング）による法人口座を狙った不正送金被害が継続して発生している
- ▶ 全国的に被害拡大しており、1社あたり数億円規模の被害も確認されている

企業の資産（法人口座）を狙う手口は？

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。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）
2. メールアドレスを聴取し、フィッシングメールを送信。メール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等を入力させる
3. 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

※架電イメージ



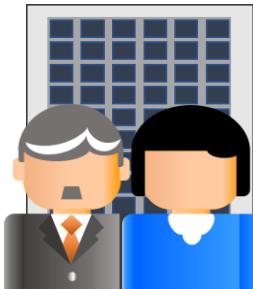
犯人

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押下

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



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聴取され、リンク付きメールが送られる

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みられた場合はいちど切電し、営業店・代表電話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！

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>

