



企業の資産（法人口座）がねらわれている！

電話に注意！ 「ボイスフィッシング」による不正送金被害が急増

【手口の概要】

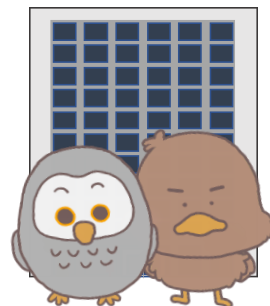
1. 犯人が銀行担当者を騙り、被害者（企業）に電話をかけ（自動音声の場合あり）、メールアドレスを聞き出す。
2. 犯人がフィッシングメールを送信し、電話で指示しながら、被害者をフィッシングサイトに誘導。そして、インターネットバンキングのアカウント情報等を入力させて、盗み取る。
3. フィッシングサイトに入力させたアカウント情報等を使って、犯人が法人口座から資産を不正に送金する。

※架電イメージ



犯人

〇〇銀行です。
ネットバンクの電子証明書の
更新手続きが必要です。
更新用のリンクを送りますの
でメールアドレスを教えて
ください。



被害者(企業)

電話

被害に遭わないための3つのポイント

◆ **知らない電話番号からの着信は信用しない！**

◆ **銀行の代表電話番号・問い合わせ窓口で確認する！！**

銀行担当者を騙る者から連絡があった場合には、銀行の代表電話番号へ連絡して確認しましょう。

◆ **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にログインする場合は、銀行公式サイトや公式アプリからアクセスしましょう。

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>



サイバーセンター公式「X」(旧Twitter)

兵庫県警察サイバーセンターではX（旧Twitter）で、サイバー犯罪やサイバーセキュリティの情報をいち早くお届けしています。

https://x.com/HPP_c3division

