

「ボイスフィッシング詐欺」にご注意ください

実在する金融機関の担当者を名乗って企業に電話をかけ、メールアドレスを聞き出したうえで偽サイトなどに誘導し、口座情報やインターネットバンキングのログインID・パスワードなどを盗み取る「ボイスフィッシング」という手口が2024年の秋以降、全国で相次いで確認されています。十分ご注意ください。

ボイスフィッシングの手口について

1. 金融機関の担当者を騙った犯人が企業(被害者)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. 犯人は聞き出したアドレス宛に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(偽のサイト)に誘導。インターネットバンキングのログインID・パスワードなどを入力させて情報を盗み取る
3. 偽のサイトに入力させたログインID・パスワードなどを用いて、犯人が法人口座から資産を不正に送金する

ボイスフィッシングの被害に遭わないために

- ・ 知らない電話番号からの着信は信用しない！
- ・ 金融機関の代表電話番号・問い合わせ窓口で確認する！！
- ・ メールに記載されているリンクからアクセスしない！！

当金庫から、電子メールや電話などでログインIDやパスワードをお聞きすることや、入力をお願いすることはありません。

不審な電話がかかってきた、不審なメールを受け取った、不審な画面が出現した場合は、下記までご連絡ください。

水沢信用金庫 お問い合わせ窓口 TEL0197-23-2498

受付時間9時 ～ 17時(土・日・祝日・金融機関休業日は除く)

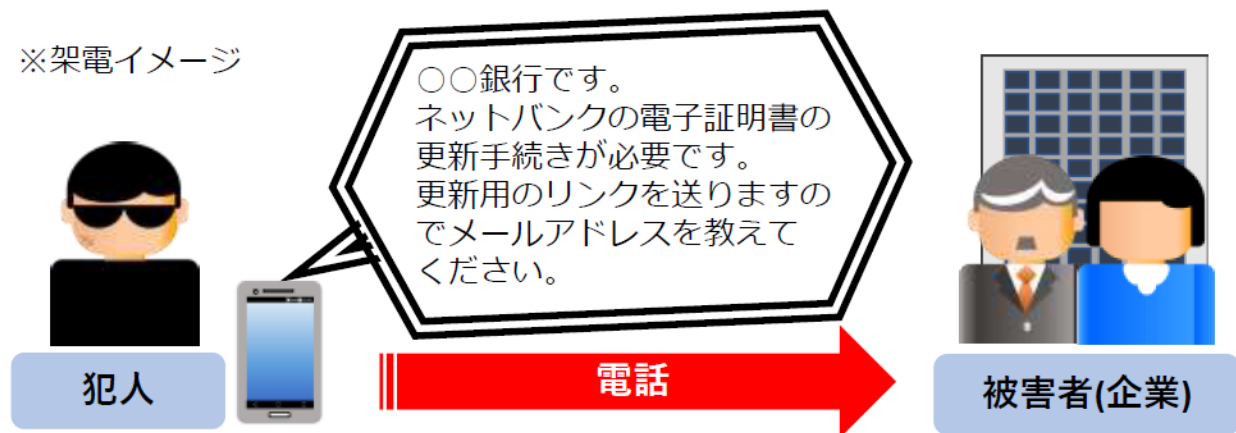
今、企業の資産（法人口座）がねらわれている！！

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



ボイスフィッシング被害に遭わないために！3つの対策

◆ 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するなど、慎重に対応してください。

◆ 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>



岩手県警察本部サイバー犯罪対策課の公式X(Twitter)はQRコードから！
サイバー空間を悪用した犯罪の手口やサイバー犯罪の被害に遭わないための情報をお知らせしています。

岩手県警察本部生活安全部サイバー犯罪対策課
令和7年3月18日発行



岩手県警察

Iwate Prefectural Police



警察庁

National Police Agency



@Iwate_cyber