

サイバーセキュリティ パートナーシップだより



電話とメールを組み合わせた新手口

ボイスフィッシングに注意！

金融機関を騙って**企業**に電話をかけた後、フィッシングメールを送りつけ、**法人口座**の情報を盗み取る「**ボイスフィッシング**」が確認されています。犯人は、最初に電話をかけることでメールの信ぴょう性を高め、受け手を信じ込ませるので、注意をお願いします。

手口の概要

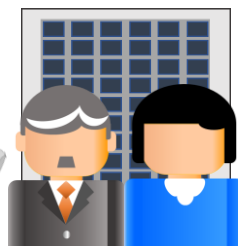
- 1** 犯人が金融機関の担当者を騙り、被害者（企業）に電話をかけ、メールアドレスを聞き出す。※自動音声の場合あり

※電話イメージ



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

- 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。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** 盗んだアカウント情報を使って、犯人がインターネットバンキングに不正にログインし法人口座から預貯金を不正送金する。

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！**
- ☑ **金融機関の代表電話番号・問い合わせ窓口で確認する！！**
金融機関担当者を騙る者から連絡があった場合には、金融機関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、金融機関の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>

