

# ボイスフィッシング(ビッシング)にご注意！

## ◎ボイスフィッシング（ビッシング）とは

電話を利用して個人情報や金銭を不正に取得しようとする詐欺手法です。

## ◎主な手口

1. 偽の電話：攻撃者は、銀行や税務署などの職員を名乗り、口座情報や個人情報聞き出そうとします。特に、緊急性を演出することで、被害者の警戒心を薄める手法が多く見られます。
2. 自動音声の利用：自動音声を使って「口座が不正利用されています」といったメッセージを流し、被害者に特定の番号を押させることで、担当者に繋げる手法もあります。
3. スプーフィング：発信者番号を偽装し、信頼できる番号からの電話に見せかけることで、被害者を騙す手法です。

## ◎対策

- ①公式確認：不審な電話を受けた場合は、すぐに電話を切り、公式の連絡先を通じて確認することが重要です。
- ②多要素認証の導入：可能であれば、多要素認証（MFA）を導入し、セキュリティを強化することが推奨されます。
- ③教育と啓発：企業や個人がボイスフィッシングの手口を理解し、警戒心を持つことが重要です。

\*ボイスフィッシングは、従来のフィッシング詐欺よりも心理的な影響力が大きく、対策が難しいため、常に注意が必要です。



# サイバー警察局便り

Cyber Police Agency Letter 2025 Vol.12 (R7.12)

## その電話、本当に銀行からですか？

### 電話を利用する「ボイスフィッシング」被害が再び発生

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**再発・急増**している。

### 企業の法人口座を狙う、その手口とは？

1. 犯人が銀行関係者をかたり、企業に**電話**をかけ、メールアドレスを聴取する
2. **メール**を送信して偽サイトに誘導し、ネットバンクの認証情報等を入力させる
3. 犯人は認証情報等を利用し、法人口座から企業の資産を**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

#### 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



被害企業  
担当者

### どう見分ける？こんな電話は偽物！

- 発信元番号が**国際電話**（+国番号）である（例：**+1 800 123 4567**）
- **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、営業店・代表電話に折り返し、本物かどうか確認する
- 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する



詐欺電話対策として“国際電話着信ブロック”もあります

みんなでとめよう!!国際電話詐欺



<https://www.npa.go.jp/bureau/safetylife/sos47/case/international-phone/>

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>



一般社団法人  
全国銀行協会

金融庁  
Financial Services Agency



警察庁  
National Police Agency



日本サイバー犯罪対策センター