



## 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・急増しています。

#### 企業の法人口座を狙う、その手口とは？

- 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
- 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
- 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）

○○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！

- 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>



長野県警察公式ホームページの「サイバーセキュリティ対策」には、サイバー事案等の手口や被害に遭わないための情報が掲載されています。是非ご覧ください。

<https://www.pref.nagano.lg.jp/police/anshin/cyber/index.html>