

# フィッシングからの 証券口座不正取引 に注意!

## 証券会社を装ったフィッシング詐欺 による不正取引が増えています!



何かの認証かな?  
とりあえずリンクから  
入力しよう!

〇〇証券からの重要なお知らせ

平素から〇〇証券を利用いただきありがとうございます。

オンラインサービスの規約変更に伴い、ログインパスワードの確認を行いますので、下記のリンクから内容を確認していただき  
よろご協力をお願いいたします。

待って!

確認画面に進む



### 絶対ダメ! 不正取引されてしまうよ

対策

- ・メール内のリンクを触らないで!  
正規のアプリ、ブックマークしたサイトからアクセスしよう
- ・多要素認証を利用しよう  
証券会社の用意するセキュリティ設定をしましょう
- ・迷惑メールブロックサービスを利用しよう  
携帯キャリアやプロバイダのサービスを活用しよう
- ・パソコン・スマートフォンをアップデートしましょう



山梨県警察本部 サイバー犯罪対策課

警察本部総合相談電話 #9110



# サイバー犯罪対策課からのお知らせ

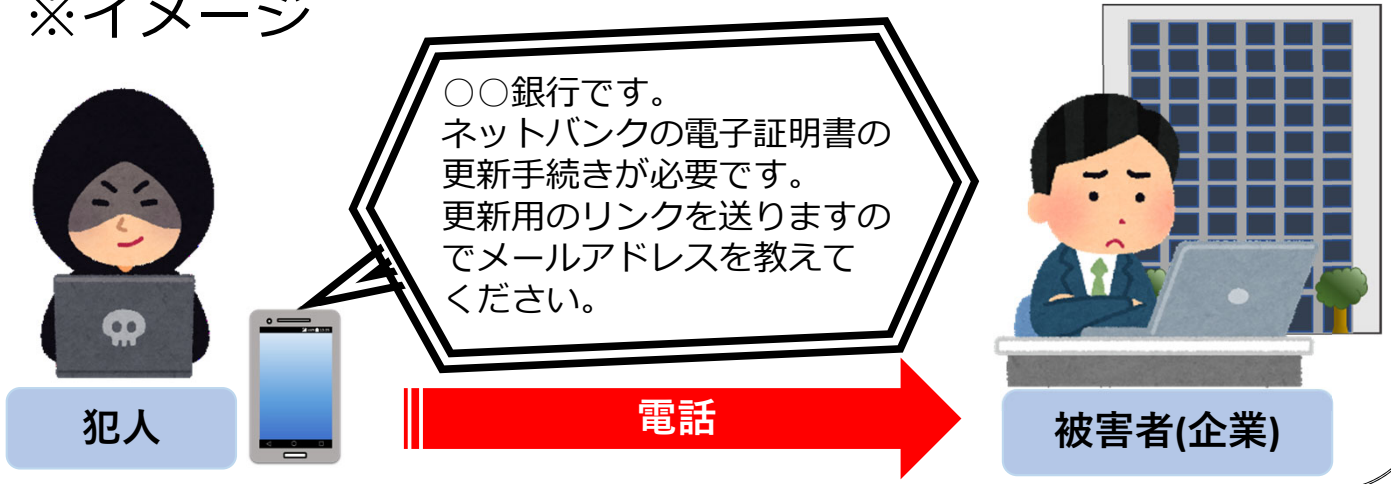
## 企業の資産（法人口座）がねらわれています！！

### 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。

#### ※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>



山梨県警察本部  
サイバー犯罪対策課



警察庁  
National Police Agency