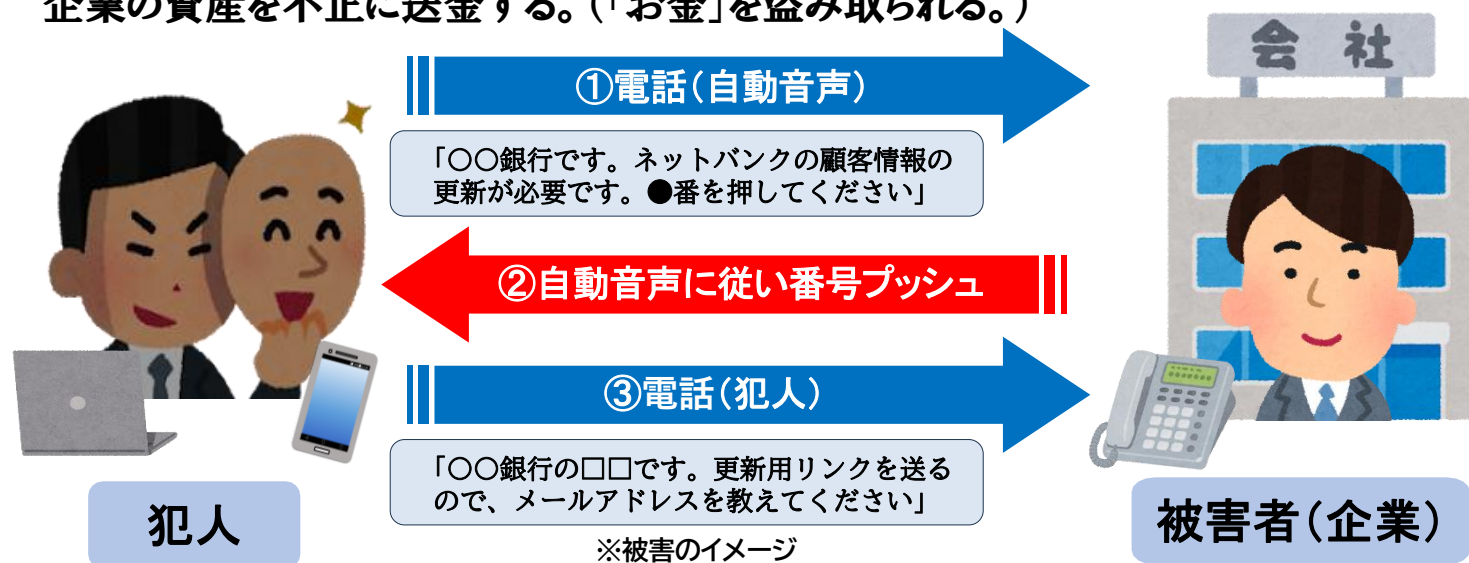


# あなたの会社の資産(法人口座)がねらわれています！

## 不審電話に注意！「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)に電話をかけメールアドレスを聞き出す。  
(自動音声のアナウンスに従って番号をプッシュすることで犯人とつながる場合あり)
2. 被害者のメールアドレス宛てに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る。「情報」を盗み取られる。
3. 盗み取られたアカウント情報等を使って、犯人が法人口座から犯人側の口座に、企業の資産を不正に送金する。「お金」を盗み取られる。



## ボイスフィッシング被害に遭わないために！

- ◆ 知らない電話番号（特に+から始まる国際電話）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！！  
銀行担当者をかたる者から連絡があった場合には、一度電話を切り、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。

**職場全体で対策の徹底を！従業員相互の声掛けと相談が被害を防ぎます！**

**『これってボイスフィッシング!?』 そんな時は 迷わず警察に通報を！**

都道府県警察本部のサイバー犯罪相談窓口はちら⇒  
<https://www.npa.go.jp/bureau/cyber/soudan.html>



**【安全・安心まちづくり通信】**

山形県・山形県警察本部



カモンくん