淡陽ビジネス Web バンキング　及び
淡陽インターネットバンキング　ご契約者様各位

拝啓　時下ますますご清栄のこととお慶び申しあげます。
平素は格別のお引き立てを賜り厚くお礼申しあげます。

近年、金融機関を装う電話でメールアドレスを聞き出し、偽サイトへ誘導して ID・パスワードを盗み取り、不正送金を行う「ボイスフィッシング」が多発しています。特に法人口座が狙われていますので、ご注意ください。

新たな手口のポイント

- 事前電話: 金融機関の担当者を装い、「電子証明書の更新」などを理由に電話をかけ、手続きに必要なメールを送るとしてメールアドレスを聞き出します。
- 偽サイト誘導: 聞き出したメールアドレスに偽のリンクを送付し、インターネットバンキングの ID・パスワードを入力させ盗み取ります。
- 不正送金: 盗取した情報でインターネットバンキングにログインし、お客様の口座から不正に送金します。

絶対に守っていただきたいこと

- **電話でメールアドレス、ID・パスワード等の個人情報は絶対に教えないでください。** 当組合や警察、行政機関の職員を名乗る場合でも同様です。
- インターネットバンキングへのログインは、必ず当組合の公式ホームページから行ってください。
- ID・パスワードは厳重に管理し、限られた担当者以外には知らせないでください。
- 不審な電話やメールを受けた場合は、決して対応せず、速やかに当組合までご連絡ください。

被害に遭ってしまったら

- 直ちに最寄りの警察署またはサイバー犯罪相談窓口にご連絡ください。
- 当組合にも速やかにご連絡ください。

当組合から電話でメールアドレスや ID・パスワードをお伺いすることは決してありません。
被害を防ぐために、ご理解とご協力の程よろしくお願い致します。

敬　具

令和７年４月

淡陽信用組合

サイバー警察局便り

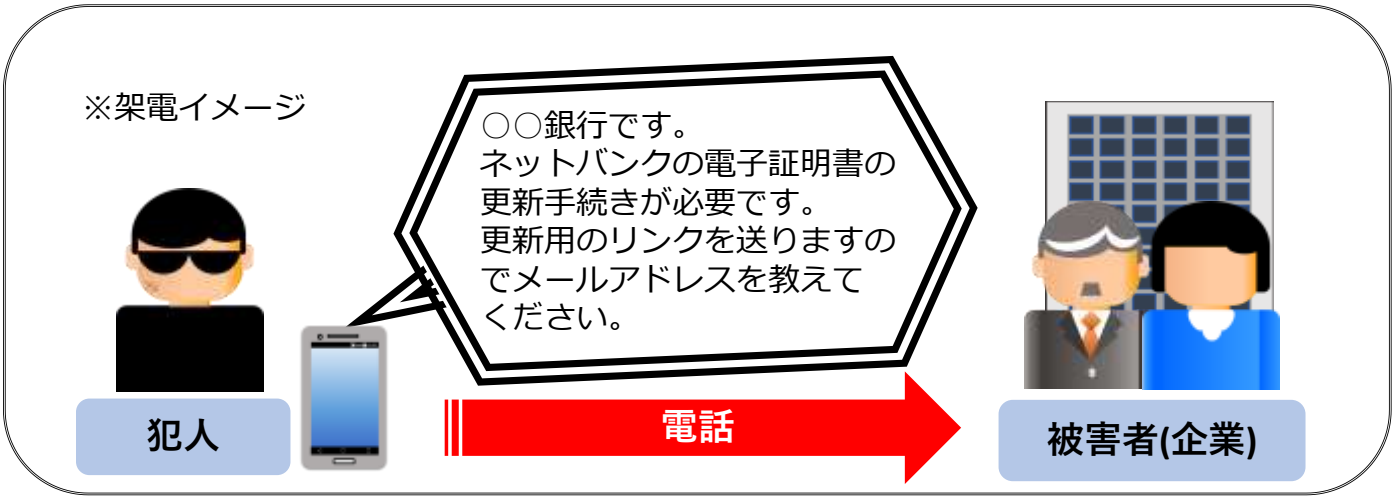
Cyber Police Agency Letter 2024(R6) Vol.15

今、企業の資産（法人口座）がねらわれている！！

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。



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

JBA 一般社団法人 全国銀行協会　金融庁 Financial Services Agency　警察庁 National Police Agency　JC3 日本サイバー犯罪対策センター