

サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和7年
5月13日
Vol. 135

ボイスフィッシング被害が引き続き発生中！

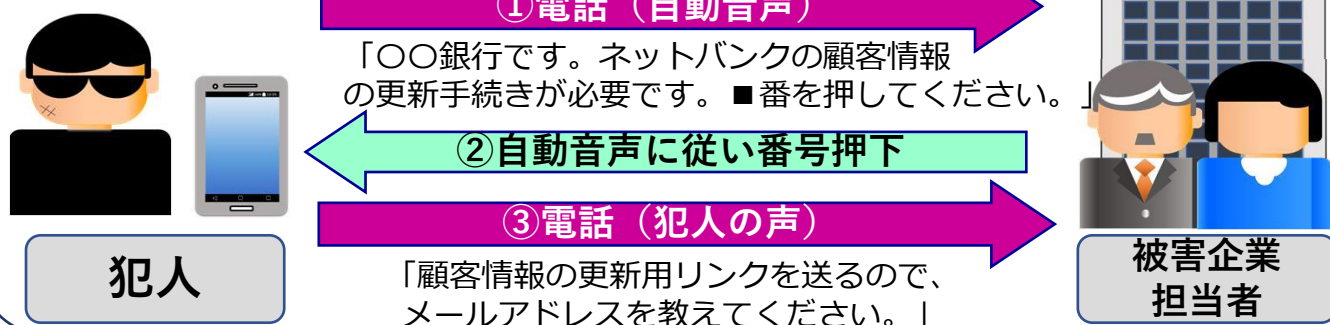
全国的に被害拡大！ 1社あたり**数億円規模**の被害も



【企業の資産を狙う手口は？】

1. 犯人が銀行関係者をかたり、企業に**電話**をかけ、自動音声ガイダンスを流す。
音声に従い番号を押すと、犯人に切り替わる。（始めから犯人が電話することもある）
2. メールアドレスを聴取し、**フィッシングメール**を送信。メール記載のリンクから偽サイトに誘導し、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。
3. 犯人はアカウント情報等を利用し、法人口座から資産を**不正送金**する。

* 架電イメージ



どう見分ける？こんな電話は偽物の可能性大！

- 発信元番号が**国際電話**（+（国番号））、または**非通知**となっている
- **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、**本物かどうか確認**する。
上記に該当する特徴がみられた場合はいちど切断し、営業店・代表電話に確認してください。
- ◆ 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利用時は、銀行公式サイト・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、**すぐに警察に通報・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>



愛媛県警察本部サイバー犯罪対策課

Tel 089-934-0110(代) / #9110

