

## フィッシング詐欺・携帯電話回線の乗っ取り（SIM スワップ）に ご注意ください

当行において、フィッシング詐欺をきっかけに携帯電話回線が不正に乗っ取られ、スマートフォンアプリの振込機能等を悪用された不正送金事案が発生しています。

金融機関やクレジットカード会社を装った**フィッシング詐欺（嘘のメール）**と、携帯電話番号を第三者に移す**SIM スワップ**を組み合わせた手口による被害が増加しています。お客さまにおかれましては、不審なメールやSMSに十分ご注意ください。

### 主な手口

- ① 「本人確認」「緊急のご連絡」など金融機関やクレジットカード会社を装ったメールやSMSが届く
- ② メール・SMS内のリンクから偽サイトへ誘導され、ID・パスワード・暗証番号・個人情報を入力してしまう
- ③ 入手した情報を使って携帯電話番号が第三者に移管され、SMS認証を悪用して不正に送金等が行われる。

### お客さまへのお願い

- ・ 身に覚えのないメールやSMS内のリンク先へ遷移し、ご自身のID・暗証番号・ワンタイムパスワードを入力しないでください。
- ・ 金融機関やクレジットカード会社からの「本人確認」「緊急のご連絡」は公式サイトや公式アプリにてお手続きください。
- ・ フリーメールアドレスや不自然な日本語のメールには特にご注意ください。
- ・ 暗証番号は他社サービスと同一にしないようご注意ください。

### ※金融庁チラシ：[金融庁 詐欺被害注意喚起チラシ](#)

次のような事象があった場合は速やかに警察に通報するとともに、当行および携帯電話会社へご連絡ください。

- 突然、携帯電話が繋がらなくなった。
- 覚えのないアプリ再登録通知が届いた。
- 身に覚えのない取引を確認した。

«お問い合わせ先»

業務統括部 金融犯罪対策室  
TEL 0952-22-2112

<https://www.sagabank.co.jp/>