



実在する運送会社、携帯電話事業者、金融機関やインターネット通販事業者などを騙った偽のショートメッセージサービス（SMS）によるフィッシング（スミッシング）に関する相談が、依然多数寄せられています。

メッセージ内のリンク先にアクセスすると

- フィッシングサイトに誘導され個人情報やクレジットカード番号などを盗み取られる
- 偽アプリ（コンピュータウイルス）のインストールを促されて、個人情報などを盗み取られる

などの被害を受け、その後、利用しているサービスへの不正アクセスや、身に覚えのない料金請求を受けてしまう危険性があります。

ショートメッセージ（SMS）以外でも偽のメールが送られてくることも多くあるので

- メッセージ内の[リンク先（アドレス）](#)からはアクセスしない  
(よく利用するサイトはブックマークしておくか公式アプリで利用する。)
- 万が一、アクセスしてしまった場合は誘導されたサイト内で  
[個人情報を安易に入力しない](#)
- 提供元が不明な[アプリはインストールしない](#)

ように注意しましょう。

