

# ショートメッセージ（SMS）を利用した フィッシングにご注意ください



ショートメッセージ（SMS）を利用したフィッシングのことを「**スミッシング**」といいます。

宅配便業者等を騙る偽ショートメッセージを利用して偽サイトへ誘導する手口で、アカウントのIDやパスワード、銀行口座等の情報を盗み取られたり、**不正なアプリをインストール**させられて、スマートフォン内のデータを不正使用される可能性があるため注意が必要です。

## 偽のSMSから被害に遭う流れ

偽のSMS

宅配便を騙ったSMS

お荷物のお届けにあがりましたが  
不在のため持ち帰りました。  
ご確認ください。

<http://...org>

URLに  
アクセス

iOS(iPhone等)端末の場合

Android端末の場合

偽サイト  
に誘導

運送

アカウント認証

セキュリティ許可の認証が必要です。

ID : IDを入力

パスワード : パスワードを入力

認証コード送信

ID・パスワード等  
を入力させる

不正なアプリを  
インストール  
させる

運送

配送状況確認ボタン  
インストール

会員登録 再配達

おしらせ 配送料金 企業情報

入力情報  
は犯人へ

スマートフォンを  
悪用される

- ・電話番号や認証コードも入力させられる場合も
- ・アカウントを乗っ取られ、情報を窃取される
- ・不正利用され、身に覚えのない代金請求がある事も

- ・自分の電話番号で偽のSMSが不特定多数に送信される
- ・そのSMSを受信した相手から問合せが来る事も
- ・スマートフォン内のデータを窃取され不正使用される



- ・ふだん利用するサイトはブックマークに登録し、ブックマークや公式アプリからアクセスする
- ・ウイルス対策ソフトなどのセキュリティソフトを導入しておく
- ・SMSやメール等に記載されたURLは安易に開かない！！
- ・流出の危険に備えて、ID・パスワードは使い回しをしない