



宅配業者を装ったSMSに注意！

宅配業者の不在通知を装ったスミッシング（※SMS（ショートメッセージサービス）によるフィッシング）が多発しています。

宅配業者を装ったSMSを受信し、URLにアクセスしてしまうと・・・

○『Android端末』の場合

〈手口〉不正なアプリをインストールさせる。

〈発生する被害〉同じ内容のSMSを見知らぬ宛先に多数送信される。

キャリア決済サービスが不正利用される。 等



○『iPhone端末』の場合

〈手口〉フィッシングサイトで「AppleID」と「パスワード」等を入力させる。

〈発生する被害〉Appleアカウントに不正アクセスされる。

キャリア決済サービスが不正利用される。 等

対処方法

- ★「機内モード」に設定し、SMSの送信を防ぐ。（Android端末の場合）
- ★携帯電話会社に問い合わせ、不正なアプリのアンインストール、必要であれば、端末を初期化する。（Android端末の場合）
- ★キャリア決済サービスの不正利用がないか携帯電話会社に確認する。

被害に遭わないために

- SMSに記載されたURLに安易にアクセスしない！
- パスワード等を安易に入力しない！
- 「提供元不明のアプリ」をインストールしない！



参考：情報処理推進機構（IPA）

< <https://www.ipa.go.jp/security/anshin/mgdayori20200220.html> >