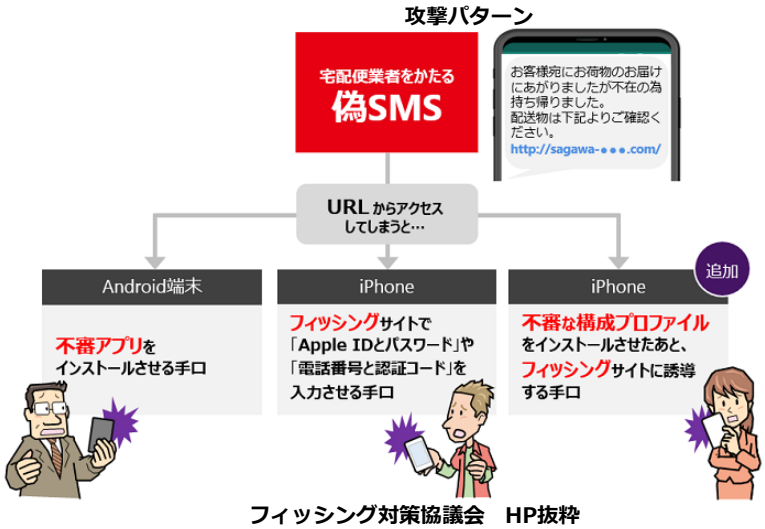
回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security News Letter Vol.48

あさまセキュリティニュースレター

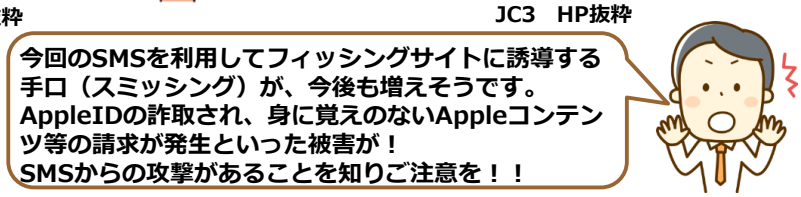
スマートフォンのSMSを利用した運送系企業のフィッシング急増中！(2019年5月17日)

↑携帯番号で送れるショートメッセージサービス



フィッシング対策協議会　HP抜粋

JC3　HP抜粋



攻撃のパターン

- SMSを利用し、偽サイトに誘導、偽のアプリをインストール、AppleID等の入力をさせる
- 不正に入手した情報で決済サービス等を利用、その他サービスへの不正アクセスも
- 不正アプリインストールさせることにより、スマホ内の情報搾取、スマホ画面をロックし金銭要求、他のSMS宛に勝手に配信等、様々な攻撃

被害

サービスの不正利用　**情報搾取**　**身に覚えのない請求**　**不正アプリインストールによる様々な被害**

対策

- SMSを利用した攻撃の手口を知る、SMSのフィルタリング設定を見直す
- 手口、本文の内容等、巧妙化しているため、少しでもおかしいと思ったら、サービス提供元に確認する
- 最新の情報を得る、最新の脅威を知る、手口を知る、セキュリティに対し常に意識をもつ

情報源

フィッシング対策協議会　https://www.antiphishing.jp/

日本サイバー犯罪対策センター　https://www.jc3.or.jp/　JC3で検索！（Amazon、Line、Apple等、偽メールの最新情報掲載）

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414