平成３１年３月４日

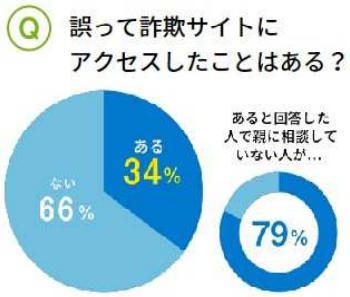
# サイバーセキュリティ関連情報（３月号）

鳥取県警察本部サイバー犯罪対策課

## ○ スマホを所持する中学生の様々なリスク

NTTドコモは、2018年12月14日から17日にかけて、全国の13歳から15歳のスマートフォンを所有している中学生男女180名に対してインターネット調査を実施した結果を発表した。

「49%が親との利用ルールを決めているが、うち63%はルールを破った経験がある」「およそ3人に1人が詐欺サイトへのアクセス経験があり、うち79%は親に相談していない」「48%が紛失、破損、盗難などのトラブルにあったことがある」などであった。




（グラフ：NTTドコモ）

また、親に隠れて行った行動を見ると「プリペイドカードなどを用いて内緒で課金したことがある（19%）」「有害サイトを閲覧した事がある（19%）」「漫画、音楽などの違法アップロードサイトを閲覧したことがある（19%）」などの回答も目立った。

中学生にスマホを持たせる際には、親子でしっかりと利用ルールを話し合い、事前にできる限りの対策をとっておくことが必要となります。

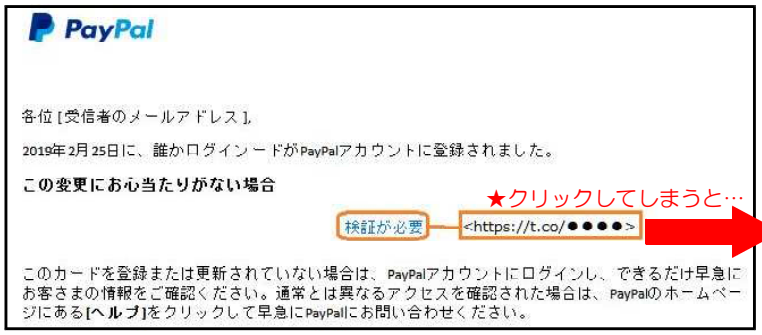
引用　NTTドコモ　https://www.nttdocomo.co.jp/special_contents/benefit_po/b_support/
https://www.nttdocomo.co.jp/special_contents/benefit_po/b_charge/index.html

## ○ 「PayPal」「Amazon」などを装ったフィッシング攻撃に注意

「PayPal」「三井住友カード」「Amazon」「ゆうちょ銀行」などを装ったフィッシング攻撃が確認されているとして、フィッシング対策協議会が注意喚起を行っている。

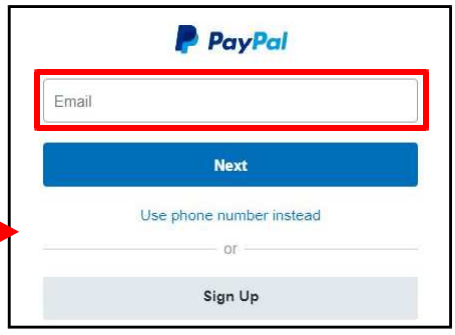
メール本文では、「検証が必要（PayPal）」「第三者によって不正にログインされた（三井住友カード）」「あなたのアカウントは閉鎖されます（Amazon）」などと不安を煽るような説明があり、リンク先からフィッシングサイトに誘導しようとするもの。

同協議会ではフィッシングサイトで、情報（メールアドレス、パスワード、個人情報、クレジットカード情報等）を絶対に入力しないよう、また、類似した攻撃へ注意するよう呼び掛けている。




フィッシングメール本文（PayPal）

**（リンク先のクリック禁止）**




誘導先のフィッシングサイト（PayPal）

**（情報の入力禁止）**

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