

幕別町消費者被害防止 ネットワークニュース

第99号



「遠隔操作アプリ※」を悪用して借金をさせる、副業や投資の勧誘に注意！

全国の消費生活センターには、副業や投資を勧誘され、「お金がない」と断る消費者に対して、事業者が遠隔操作アプリを悪用して借金をさせるといいう悪質な手口に関する相談が、20代の若者を中心に多く寄せられています。

トラブルの流れ

- ① 副業サイトやSNS広告を見て興味を持ち、事業者に連絡し、登録する。
- ② 始めに安価なマニュアルを購入するよう勧められる。
- ③ 「説明に必要」などと言われ、遠隔操作アプリのインストールを求められる。
- ④ 画面共有での説明中に高額なサポートプランを勧誘され、「お金がない」と断ると、貸金業者から借りるように言われる。
- ⑤ 画面を共有したまま、相手からの指示を受けて借金をさせられ、指定した口座に振り込むよう指示される。
- ⑥ 聞いていたとおりには儲けられず、借金だけが残る。

アドバイス

※遠隔操作アプリとは、自分のスマートフォンやパソコンに遠隔地の第三者が接続して両者が画面を共有しながら、第三者が遠隔操作を行うことができるアプリのこと。

- うまい儲け話を信用しない。
- 遠隔操作アプリを安易にインストールしない。
- 遠隔操作で貸金業者に登録してしまった場合は、IDやパスワードを変更し、悪用されないように対策をする。
- 借金してまで契約しない。

このような事業者は「元手がない」と言う「すぐに元が取れる」と貸金業者からお金を借りさせようとしています。しかし、借金を返せる保証は一切なく、事業者に解約や返金を求めても突然連絡が取れなくなるなり、トラブルの解決が困難になる恐れもあります。不安に思った場合は、消費生活センターに相談してください。

相談事例紹介

子どものスマホゲームの高額課金

今月の相談

小学生の子どもが親の知らない間にスマートフォンゲームアプリをダウンロードし、課金をして遊んでいた。クレジットカードの明細書を見て高額な請求に気が付いた。親が同意していない契約なので返金してほしい。

最近、子どものオンラインゲームの無断課金の相談が目立ちます。このような相談では、子どもが保護者の同意なく行った未成年者契約として、事実関係をまとめた経緯書と再発防止策や契約の取消返金を求める書面を相談者が作成し、アプリストア運営会社提出して話し合います。ただし、子どもが保護者のアカウントでログインして課金した場合は、子どもが操作したかの判断が難しいため、保護者が行った契約と見なされてしまうこともあり、注意が必要です。

【このようなトラブルに遭わないために】

- 子どもに端末を渡す前に、Apple・Googleなどのアカウントをサインアウトしておく。
- 利用時間や課金、閲覧を制限する「ペアレンタルコントロール」を設定する。
- パスワードは厳重に管理し、定期的に変更する。
- クレジットカードの決済完了メールが届くように設定し、必ず確認する。
- 家族で共有する端末にはクレジットカード情報を登録しない。
- 家族で利用のルールを話し合う。

トラブルが発生した場合はすぐに消費生活センターに相談してください。



問 幕別町消費生活センター（☎55-5800）

地区	相談受付	場所
札内	月曜～金曜	札内コミュニティプラザ 消費生活センター
幕別	火曜・木曜	役場 1階相談室
忠類	第2・4水曜	忠類コミュニティセンター
	午前9時～午後4時 (札内:第1・3・5水曜は午後7時まで)	

見守り 新鮮情報

事例1

宅配業者名で **SMS** が届いた。ちょうど荷物が届く予定だったので、SMSに書かれていた **URL** を **クリック** して、記載されていた指示どおりに、**ID** や **パスワード** 等を入力した。しかし、その後11万円を **不正利用** されていたことが分かった。(60 歳代)

事例2

スマートフォンに「ETCカードを更新するように」との **メール** が頻繁に入るようになった。所有しているクレジットカード会社発行のETCカードの手続きが必要なのかと思い、**URL** を開いて **メールアドレス** や **パスワード**、**クレジットカード番号** 等を入力した。その後、カード会社に連絡をすると **覚えのない決済** があり、1万2千円が使用されていた。(70 歳代)



SMS や メール での フィッシング詐欺に注意

ひとこと助言

正規のサイトから
アクセスしよう



見守るくん

- 実在する組織をかたるSMSやメールを送信し、IDやパスワード、暗証番号、クレジットカード番号等、個人情報を詐取したうえ、クレジットカード等を不正利用するフィッシングに関する相談が多く寄せられています。
- 記載されているURLにはアクセスせず、事前にブックマークした正規のサイトや正規のアプリからアクセスするようにしましょう。
- フィッシングサイトに個人の情報を入力してしまうと、クレジットカードや個人情報を不正利用されるおそれがあります。絶対に入力してはいけません。情報を入力してしまったら、同じIDやパスワード等を使っているサービスを含め、すぐに変更し、クレジットカード会社や金融機関等に連絡しましょう。
- IDやパスワード等の使い回しを避けることで被害の拡大を防ぐことができます。
- 困ったときは、すぐにお住まいの自治体の **消費生活センター** 等にご相談ください(消費者ホットライン 188)。