



サイバーニュース

R 2 年 第 5 号
奈良県警察本部
サイバー犯罪対策課

オンラインゲームユーザを狙う脅威とその対策



総務省の平成30年版情報通信白書によると、インターネット利用者(対象13歳以上)の約3割がオンラインゲームを利用しており、20歳から29歳では45.5%が、13歳から19歳にあっては50.7%が利用しています。

「eスポーツ(Electronic Sports)」の日本での認知も広がっており、さらにオンラインゲームの利用者が増えることが考えられます。

オンラインゲームユーザを取り巻く脅威



- ◆ ゲーム内チャットや動画共有サイトなどを悪用して
- ◆ 「無償でゲーム内通貨を得られるツール」を餌に不正なURLリンクを開かせる
- ◆ 関連動画から偽アプリのインストール先に誘導



- ◆ 認証情報や決済情報などを詐取
- ◆ アカウントの乗っ取りや金銭被害
- ◆ アフィリエイト目的の誘導でサイバー犯罪者資金稼ぎに加担

※ アフィリエイト: 誘導先にアクセスしてもらうことで報酬を得る仕組み

ゲーム内のチャット機能などを使った手口に注意してください。

- 正規ログインページを装った偽サイト(フィッシングサイト)へ誘導し、IDとパスワードや個人情報、クレジットカード情報を盗み出す
- 人気ゲームに見せかけた「偽アプリ」と一緒にコンピュータウイルスをインストールする
- トレード話を持ちかけてゲームアカウント、アイテムや金銭をだまし取るなど

詐欺行為やセキュリティの脆弱性を突く手口などに注意してください。



7つの対策

1. 犯罪の手口を知る

各ゲーム事業者やセキュリティ事業者などの注意喚起情報を定期的に確認しましょう。



2. メールやチャット内のURLリンクを不用意に開かない

ゲームアカウントへのログインはブックマークに登録した公式サイトや公式アプリから行いましょう。

アプリを入れる際は、公式のアプリストアを利用しましょう。ただし、インストール前にアプリの提供元や利用者の評価などをよく確認しましょう。



3. アカウントを厳重に管理する

第三者に推測されにくいパスワードを指定するとともに、サービスごとに異なるIDとパスワードを設定しましょう。



4. セキュリティソフトを利用する

不正サイトへのアクセスやマルウェアへの感染リスクを下げるため、必ずセキュリティソフトを利用しましょう。



5. OSやファームウェアを正しく更新する

ネットにつながるゲーム機も脆弱性対策が必要です。各メーカーによるOSやファームウェアの更新プログラムを適用しましょう。



6. 家庭内ネットワークの安全を確保する

不正サイトへのアクセスや不適切なアプリの利用をブロックしてくれるセキュリティ製品などを利用しましょう。



7. RMTやチート行為に手を出さない

他のプレイヤーとのトレードは、ゲーム事業者提供の公式のトレードサービスを利用しましょう。また、チート行為は損害賠償や刑事罰の対象となる可能性があります。

※ RMT(リアル・マネー・トレーディング)

ゲームのデータやキャラクター、アイテムなどを現実の通貨や物品を対価に取引する行為。買い手か売り手のどちらかが先渡しするため、代金やアイテムだけを持ち逃げされるトラブルが起こることがある。

※ チート

コンピュータゲームにおいて、データの改竄や不正な操作によって、想定していない結果を得ること。

それらの動作を行わせる不正プログラムをチートツールといい、それを餌にランサムウェア(身代金要求型ウイルス)をインストールさせる手口もある。



警察への相談・ご意見・ご要望

総合相談電話

0742-23-1108 又は #9110



【参考】トレンドマイクロ株式会社「オンラインゲームユーザを狙う脅威とその対策」

https://www.is702.jp/special/3654/partner/12_t/