ゲーム業界の
チート事例
から学ぶ

セキュリティ対策の重要性

株式会社DNPハイパーテック

チート対策の重要性

ゲームアプリにおいて、セキュリティが重要であることは言うまでもありません。
「セキュリティは大切だ」
「セキュリティを考えないなんてありえない」
そこまでは考えつつも、実際にリスクを一つ一つ検証することは少ないのではないでしょうか。

今回は、セキュリティリスクの種類とセキュリティ対策ツールがそれらのリスクをどのように低減しているのかを見ていきましょう。

チートとは、スコア・お金などゲーム内のパラメータ（プログラム）の変更により、ゲーム進行が有利に進めるよう不正を行うことです。実際のチートの例を簡単にご紹介します。

- アイテムを不正に取得
- ゲームルールを破壊するような挙動を行う
- 本来は課金をしなければならない機能を不正に利用する

チートによって発生する一番大きな問題としては、**ゲーム運営会社にとっての収益源に直接ダメージを与えること**です。特に昨今で多い、Free to play(基本無料) ゲームでは収益の 80% 以上を上位 20% のヘビーユーザーから課金してもらうことによって成立していると言われています。彼らがゲームを辞めてしまったり、課金をしなくなるなどの遠因の一つとしてチートがあります。

また、ゲーム内ランキング上位には不正をしているユーザーが並んでいる、なんてことになれば運営団体への信頼は一気に損なわれ、公平でないゲームの烙印を押されることになります。

ユーザー離れが進むと App Store をはじめとした**レビューサイトでの評価が一気に下がります**から、長期的にゲームそのものの体力を奪っていくともいえるでしょう。

著作物の抜き取りも見逃せません。イラストやボイスデータなどの資産が不正に流用されることにより、ゲーム自体の知的財産権も侵害されることとなり、版権元とのトラブルにつながる恐れもあります。

今日においては、チート対策はゲーム事業、ひいては企業が成長していく上で欠かせないリスクヘッジとなっています。では、実際にチート対策を進めていく上で、チート・チーターについて理解を深めていきましょう。

健全なゲームの状態	チート放置による被害	チート対策のメリット
課金箇所で会社収益を得る	課金機会の損失 収益低下	ゲーム収益を守る
レビュー評価でKPIを向上	レビュー炎上による KPIの低下	ゲーム本来の評価を得る
ユーザの切磋琢磨で ランキングが形成される	ランキング改ざんの横行 ユーザー離れ	ゲームの公平性を保つ
コラボイベントで IPコンテンツを使う	IPコンテンツ抜き取り 信用問題	法律の保護を受けやすい

チーターのモチベーション

他のプレイヤーや開発者への嫌がらせ？

チートはそもそもなぜ発生するのでしょうか。ルールに従って遊ぶ方が楽しいはずのゲームを自分から破壊しに行くのですから、それ相応のメリットが彼らにはあると考えるのが自然です。

チーターのモチベーションは人間の根源的な欲求から来ているのではないでしょうか。そう、私たちも自然に少しは思ったことのあるような、**お金と人から羨望の眼差しを浴びたい**という気持ちです。

ガチャやカードゲームの流行により アカウント売買などが流行

チーターのモチベーションとしてわかりやすく、さらに大きな問題となりやすいのが、**不正に利益を得ることを目的としたチート**です。リアルマネートレード (RMT) を活用して、ゲーム内で不正に取得したアイテムや、不正にスコアを獲得したアカウントを実際のお金で販売することにより利益を獲得します。

また、チートを行いたいユーザーに、**改造したアプリケーションを販売して資金を獲得する**ケースもあります。特に OS カーネルやチートツールを独自で開発できるほど技術力の高い個人・グループにおいては、チートを利用したいユーザーにそれらを販売する事例が後を絶ちません。もし実行犯をチーターだとするなら、彼らに武器を配る、いわば武器商人のような存在がいるというわけです。

自己顕示欲・承認欲求

他者の作成物を解析し暴くことに快感を覚えたり、ゲーム内の他のプレイヤーに圧倒的な勝利を収めることで承認欲求を満たしたいチーターも多く存在しています。

以前は、高価な解析ツールしか存在していなかったり、インターネット上に情報が少ない状況が続いていましたが、現在はオープンソースソフトウェアや無料で利用できる解析ツールが公開されていたり、コミュニティの発達により情報量が増えているため、チートを利用することへの敷居が著しく低くなっています。

そして SNS や動画サイトの爆発的な普及とともに、チーターの自己顕示欲・承認欲求をより簡単に満たすことができる環境が生まれています。

金銭
不正に利益を得ることを目的とする。

自己顕示欲・承認欲求
他者の作成物を解析し暴くことにより実力を示し、承認欲求を満たす。

悪意あるチートは4段階

チートを実行するためには大きく分類して4段階の難易度があります。チートの悪質度ではなく、あくまでチート自体の技術難易度であるということにご注意ください。

難易度 低　改造されたゲームを入手する

1つ目は、**別の開発者が製作した改造（MOD）アプリを利用する方法**です。組織的に運営している海賊版サイトを訪問し、改造済みアプリを取得します。一般的な端末で利用することができますので、チートを実行するリスクが低く、ITリテラシーが低いユーザーでもある程度使いこなせてしまいます。

一方で、ゲーム会社の一部では、容姿やユーザーインターフェースの変更など、ゲームの本質に影響を与えない要素であれば、MODをある程度容認してユーザーにより楽しんでもらおうとする考え方も広まりつつあります。

難易度 中　ゲームを改ざんするアプリを入手する

2つ目はゲーム特化型の改ざんアプリを利用することです。WebやSNS上で公開されている特化型のチートアプリやシステムを悪用するアプリを入手します。

端末上で改ざんを行う場合は、端末のRoot化やJailBreak(JB)が必要となることが多く、利用にはある程度の英語力や技術リテラシーが必要となります。

しかしながら、Root化やJailBreak(JB)のツールや手順はインターネットで検索すると発見できるものですので、ゲーム特化型の改ざんアプリに手を染めることはチーターにとっては難易度の高いことではありません。

難易度 高　プログラム改ざんツールを利用する

3つ目は、個別のゲームタイトルにとらわれない、開発フレームワークなどに対する汎用的な改ざんアプリを利用することです。GitHubやWebサイトから汎用的な解析・改ざんツールを手に入れ、システムやアプリの変更を行います。エンジニアリングの高いレベルが要求されるため、ゲーム開発の現場においては、自分だったらこのように改造するだろうということを念頭に置いて対策を進める必要があります。改造アプリを作る場合はRoot化は不要ですが、端末上で改ざんを行う場合は、Root化が必要となります。

難易度 超高　チートツールを自分で開発し、クラッキングする

4つ目は、OSカーネル（OSの中核部分に位置するソフトウェア）やチートを行うためのツールを開発することです。これらを開発するには高い技術力が必要になるため、個人というよりは、エンジニアリングに強い組織・団体が開発を進めていることがほとんどです。彼らはいわゆる「元請け」としてこれらを改ざんするソフトウェアを利用してゲームをプレイするユーザーへと販売して収入を得るというビジネスモデルが成り立っています。そのため、金銭目的でのチートが後を立たなくなっています。

チート対策と保護対象の検討

優先して保護すべき対象とは

お客様によって優先順位は変化しますが、概ね右記の4種類に分類されることが多いです。

1. 収益に直結する箇所
2. 画面に見えているパラメータ
3. 重要なアルゴリズム
4. コンテンツ

1. 収益に直結する箇所

課金データを管理する箇所、課金された後にアイテムを生成する仕組みなどは優先的に保護が必要です。

2. 画面に見えているパラメータ

画面に見えているパラメータは検索しやすく攻撃対象になりやすい箇所です。チートを利用しているという風評が広まってしまうとゲーム自体のブランドを毀損することになりますので、こちらも保護が必要です。

3. 重要なアルゴリズム

いうまでもなく、ゲームの根幹を揺るがすようなアルゴリズムには保護が必要です。

例えば、位置情報を利用するゲームでは位置情報を管理するアルゴリズムが不正利用されると、移動距離に応じて報酬を得られるゲームにも関わらず、チートにより数千キロも移動して報酬を得ることができるなど、ゲーム自体の根本的な崩壊につながりかねません。

4. コンテンツ

ゲーム内で利用される画像、音楽、音声データなどのコンテンツも重要な対象となっています。

仮に漏えいすると、チートのせいで発生した事象であっても使用許諾の超過などによって開発元が損害賠償を求められるケースもあります。

チート対策と保護対象の検討

ゲームの種類ごとにチートを分類すると ...

影響あるゲーム	チート行為	チート対策のメリット
マルチ対戦	ステータス改変	アクセス制御 データ暗号化／二重化
ストーリー重視	ステージ／シナリオの解放	
位置情報使用	ゲームプレイの自動化 パラメータの偽装	システム情報の検証 異常値の検出
IPコンテンツ使用	IPコンテンツ抜き取り信用問題	コンテンツの暗号化
全て	改造アプリの作成	ハッシュ値のチェック 署名情報のチェック
	プログラムの改ざん	プログラムの暗号化 プログラムの難読化
	想定外の状況でのプレイ （Root／エミュレータ）	特徴的なファイルの検出

チート利用者が多く イタチごっこなマルチ対戦ゲーム

チートの利用が良く行われるものとしてマルチ対戦が可能なゲームがあります。ステータスを改変して著しく自分のキャラクターを強化することや、近年スマートフォンでも流行しているFPS・TPSゲームでは照準を自動で相手に合わせる「オートエイム」、壁を透けさせることで相手の位置を把握する「ウォールハック」などのチートが有名です。対戦ができないMMORPGなどのジャンルであっても、不正にレベルを変化させたり、ステージを解放するチートなども存在しています。

対策は？

まずは、データの配置場所を適切にすることでアクセスを制御することです。例えば、アイテムやパラメータなどのリアルタイムな通信ができない箇所においては、それらのデータをクライアント側で管理するのではなく、サーバー側に置くことによってデータの改ざんから守ることができます。

ただ、リアルタイム性が求められるゲームにおいては、クライアント側に置かざるを得ない場合も多いでしょう。そこで、**データを保存するときは必ずエンコードし、利用するときにはデコードするなどの暗号化のルール**を決めておくと良いでしょう。

なぜかオーストラリアに？ 位置情報を利用したゲームでは「位置飛ばし」が流行

近年では、GPS・位置情報を利用したゲームも流行しています。これらにおいては、自動で少しずつ位置情報を改ざんしたり、歩行数などのパラメータを偽装するなどのチートが考えられます。

本来は特定の位置に行かないと得られないアイテムを不正に取得するなどのチートはいたちごっこのように生まれています。

チート対策と保護対象の検討

対策は？

このようなケースでは、データの定義を厳密にすることが重要です。例えば、「300m の距離を移動するときの上限は時速 300km までとする」としておけば、それを超えた速度で移動している端末はチートを利用している可能性があると検知することが可能です。

位置情報の検証方法に関しては、この分野のセキュリティ対策で長年培ってきた弊社のノウハウから、より効果的な解決策がご提案できます。

IP コンテンツを利用しているゲームは、知的財産権の保護に注意

アニメや漫画を原作とした IP コンテンツを利用しているゲームは著作権をはじめとした知的財産権の不正利用には特に注意を払う必要があります。

仮に、ゲームの開発会社の瑕疵によりIPコンテンツの原画が不正に流用された場合、損害賠償などの責任問題が発生する可能性もあります。

対策は？

利用する画像や音楽などのデータを暗号化することが最も効果的です。画像ファイルや映像ファイルを暗号化せずにクライアント側にダウンロードした場合、保存されている位置の解析により直接アプローチを仕掛けてダウンロードすることが可能になります。可能ならばサーバー側には常に暗号化されたファイルしかおかず、クライアント側にも暗号化されたファイルのみをダウンロードさせるようにしましょう。

全てのゲームに共通する、汎用的な脅威への対策は？

改造アプリの作成は、特徴的なデータの突合で確認！

改造アプリはハッシュ値が当然オリジナルのものとは異なりますし、署名情報が古かったり、発行元が異なっている場合も大いにあります。改造アプリを発見した場合は、そのアプリの特異な箇所を特定し、一つずつ対策をぶつけていくことが有効となります。

データの暗号化難読化をお忘れなく！

プログラムを改ざんされないためには、クライアントとサーバー両方で取り扱うデータは暗号化・難読化できないかを検証しましょう。

守りたいものに合わせたチート対策が重要

チート対策は「何を守るのか」をまず定めそれに適した対策が必要です。また、継続して行うことも非常に重要です。チーターは日々様々な攻撃方法や脆弱性を見つけてきます。

日々更新されていくチーターの技術への対策をアップデートし、大切なゲームを守りましょう。

ゲームを守るなら、CrackProofをぜひご活用ください

チーターはおかしな環境でプレイしていることも

Root化やエミュレータを利用したプレイによって、想定している挙動を狂わせる場合もあります。

当然、利用している環境が違うので、チーターのプレイデータの特異な部分より検出することが可能です。

ここではゲームアプリにフォーカスを当ててご説明しましたが、当社DNPハイパーテックが開発したCrackProofは15年以上の実績を持ち、アプリを不正な解析・改ざんから保護する耐タンパ技術であらゆるクラッキング（不正な解析・改ざん行為）の被害を防ぎます。

CrackProofの特長とは

1.あらゆるアプリへの攻撃を多角的に防御

クラッキングを防ぐためには、アプリ自体を直接解析する「静的解析」と、アプリ実行中の動作情報を解析する「動的解析」の両方を防御することが重要です。

CrackProofは、静的・動的ともに悪質な解析を阻止し、さらに不正な実行環境も検知、これら3つの保護機能により、難読化だけでは守れない攻撃からアプリを多角的に保護します。

2.開発済みのアプリへの適用が簡単

アプリを直接セキュリティ処理するため、開発段階でソースコードに組み込む作業は不要。CrackProofクラウド上にアプリをドラッグ＆ドロップするだけで、開発済みのアプリにも、自動的に強固なセキュリティ処理が施されます。ダウンロード・動作確認後、すぐにリリース可能です。

3.導入後も安心のフォローでお客様とともに対策を

導入後の国内サポートも充実。お客様のパートナーとなり、さらなるクラッキング対策のご相談などを通して、貴社のアプリを守るお手伝いをいたします。

企業概要

商　号　株式会社DNPハイパーテック

設　立　1994年5月18日
2015年 DNPグループになる

所在地　〒600-8813
京都市下京区中堂寺南町 134番地
京都リサーチパーク ASTEM棟５F

資本金　4000万円
（大日本印刷株式会社100%連結子会社）

代表者　代表取締役社長　友村潤一

CrackProofの詳しい情報や
アプリのセキュリティ知識が身につくダウンロード資料はこちら

https://www.hypertech.co.jp

お問い合わせはこちら

https://www.hypertech.co.jp/contact/

未来のあたりまえをつくる。
DNP