Android 向けモバイルゲームにおける MOD アプリを用いたチート行為の現状分析

論文番号：M-1
テクノロジーデザイン講座
上西研究室　小谷 将太郎

近年, モバイルゲーム市場は世界的に拡大する一方, ゲームのデータやプログラムを改ざんするチート行為が課題となっている. チート行為の中には, ゲーム内通貨の不正取得や, 広告の削除など, ゲームの公平性や運営会社の収益に影響を及ぼすものがある. MOD アプリは, チート行為の手法の 1 つであり, ユーザーはチートの機能が実装された改造済みアプリをダウンロードするだけで, チートを行うことができる. MOD アプリの流通が, チート行為を容易にし, その被害を拡大させる一因となっている.

本研究では, 人気タイトルに関わらず大規模にチート情報を収集し、時間的側面に着目した分析によって、モバイルゲームにおけるチートのリスクの把握とチート対策の有効性を定量的に明らかにすることを目的とする.

MOD アプリを配布する Web サイトから, Android の MOD アプリに関するスレッド情報と, Google Play ストアにおける正規アプリのメタデータを自動収集し, MOD アプリの公開時期やカテゴリなどを統計的に分析した. さらに, 正規アプリの APK ファイルを解析し, チート対策の手法の 1 つである global-metadata.dat の暗号化の有無と, 正規アプリ公開から MOD アプリ公開までの日数の関係を調査することで, チート対策手法の有効性を分析した.

その結果, MOD アプリの公開数は増加傾向にあること, 6.4% の MOD アプリが正規アプリ公開当日に公開されていること, 幅広いカテゴリのゲームが MOD アプリの対象となり得ることが明らかになった. また, global-metadata.dat の暗号化はリバースエンジニアリングに時間的コストを与え, チート行為を抑制する効果があることが示された. 一方で, 暗号化していた場合でも, 当日に MOD アプリが公開される事例が存在することから, 当日の MOD アプリ公開を防ぐには, 他のチート対策技術の併用が必要であることが示唆された.

ゲーム開発者は, 迅速なチート開発が行われる事例から, MOD アプリのリスクを開発初期から考慮する必要がある. MOD アプリ開発者の技術力は向上しており, その技術力を過小評価することはリスクを高めることにつながる. 今後は, さらなるデータソースの拡充や, 複合的なチート対策技術の有効性の評価が課題となる.