卒　業　論　文

題　　目

動的解析による
Android マルウェアの解析

指導教員

河野 健二 准教授

平成 26 年度

慶應義塾大学 理工学部 情報工学科

吉川無我 (61123114)

卒　業　論　文　要　旨

学　科	情報工学	学籍番号	61123114	フリガナ 氏　名	ヨシカワムガ 吉川無我

(論 文 題 名)

動的解析による Android マルウェアの解析

(内 容 の 要 旨)

現在，Android 端末は世界中で広く用いられている．しかし，Android 端末を標的とした悪意ある Android アプリのマルウェアによる被害が発生している．Android アプリのマルウェアは感染した端末の個人情報を盗み取って外部サーバへ送信したり，バックグラウンドでメッセージを送信することでユーザに気づかれることなく不正な課金を行う．このような Android アプリのマルウェアによる被害を防ぐためにはマルウェアの解析が必要である．

Android アプリのマルウェアを解析する方法の 1 つとして，マルウェアを実際に動作させて解析を行う動的解析がある．既存の動的解析手法・ツールではエミュレータ環境において解析を行っている．しかし，エミュレータ環境において挙動を変えるマルウェアを正確に解析することは難しい．

本研究では，実機上でマルウェアを動作させて解析を行う手法を提案する．本研究ではマルウェアの Java クラスファイルにログコードを挿入し，その実行ログを得ることで，動的に解析を行う．Java クラスファイルを書き換える Java ライブラリを用いることで，マルウェアのクラスファイルにログコードを挿入する．

提案手法によってマルウェアを解析できることを示すために実験を行う．提案手法を 11 個のマルウェアに適用し，Android の実機 (Nexus 5 Android 4.4.4) でこのマルウェアを実行した．その中の 1 つのマルウェアから外部から悪意あるコードを入手するメソッドのログを，2 つのマルウェアからは SMS を送信するメソッドのログを得ることができた．さらに，iMatch というマルウェアが SMS を不正に送信する方法を特定することができた．

（内容の要旨は約25行程度で記入のこと）

慶 應 義 塾 大 学 理 工 学 部