【５】

氏　　名	ダオ　ヴァン　トゥアン
学位の種類	博　士（工学）
学位記番号	第７６２号
認定課程名	防衛大学校理工学研究科後期課程
学位授与年月日	令和６年５月１７日
論文題目	軽量深層学習を用いた画像に基づく高精度ﾏﾙｳｪｱ分類
審査担当専門委員	（主査）慶應義塾大学　教授　斎藤　英雄
	工学院大学　教授　浅野　太
	大学改革支援・学位授与機構　教授　宮崎　和光

審　査　の　結　果　の　要　旨

近年、システムを破綻させることを目的としたマルウェアによる被害が深刻になっている。この対策として、検出したマルウェアの種類の分類が重要である。この方法の一つとして、マルウェアのコードを画像に変換し、画像分類に用いられている深層学習を利用して分類する方法がある。マルウェアの内容や実際マルウェアづいた特徴マルウェア決定する必要がないという利点があり、学習済みの深層学習モデルにより短時間で分類できるというメリットがある反面、スマートデバイス等の限られた計算リソースでは分類性能が十分ではなく、未知のマルウェアを分類すること難しいという問題があった。

著者は、これらの問題を解決するために、限られた計算リソースとして、（I）少数の GPU しか使用できない環境、及び（II）CPU しか使用できない環境の二つを考え、それぞれの環境において適切なモデルを提案している。

まず（I）の少数の GPU しか使用できない環境のために、ローカル特徴及びグローバル特徴の双方を重視し、軽量化畳み込み層、変分オートエンコーダ（Variational AutoEncoder: VAE）、及び注意機構を組み合わせた、新たな CNN-AVAE モデルを提案している。そして、提案手法が、画像ベースマルウェア分類タスクにおいて、他の CNN モデルと比べ高い精度を得られることを示している。

次に上記（II）の CPU しか使用できない環境のために、CNN や注意機構を使わない、多層パーセプトロン（Multi-Layer Perceptron: MLP）に基づいたモデルである MLP-mixer を軽量化し、オートエンコーダにより特徴を洗練させる手法を提案している。そして、提案手法が、Resnet50 や、CNN を用いない既存研究より上回る性能であることを示している。

さらに未知のマルウェアを分類することは困難であるという問題を解決するために、近年提案されたゼロショット学習が、学習データとラベルの関係を活かすことで、教師データがなくとも分類できることに着目し、学習データとラベル関係の多重性を考慮したマルウェア分類のための新たなマッピング手法を提案している。提案手法では、軽量化 CNN により作成された特徴空間とマルウェアに関する記述から作成されたラベルとでマッピングを行い、このマッピングを二段階に増やすことで、既存手法である巨大なモデルより高い精度を得られることを示している。

これらの結果は、近年とみに増大しているマルウェアによる被害への対策に関し新たな知見を示したものである。よって、学術的価値は高く、博士（工学）として合格と判定した。