別紙１－１

論文審査の結果の要旨および担当者

報告番号	※　甲　第　　号

氏　　名　　高 云

論　文　題　目

Effective Application of Artificial Intelligence Technology in Malware Detection and Classification

（マルウェアの検知と分類に対する人工知能技術の効果的な適用）

論文審査担当者

主　査　　名古屋大学教授　楫　　勇一

委　員　　名古屋大学教授　片桐　孝洋

委　員　　名古屋大学准教授　嶋田　　創

別紙１－２

論文審査の結果の要旨

高氏提出の論文「Effective Application of Artificial Intelligence Technology in Malware Detection and Classification」は、引き続き猛威を振るうマルウェアを用いたサイバー攻撃に対抗するために、いわゆる人工知能(AI)と呼ばれる技術をマルウェア検知/分類に対して効果的に適用することを目指した一連の研究をまとめたものであり、全体は 6 章から構成される。

第 1 章は序論であり、亜種も含めて年々増加するマルウェアやマルウェア検知/分類に対する AI 応用の広がりなどの背景、および、グラフニューラルネットワークなどの新しい技術のマルウェア検知/分類への応用という動機について述べている。

第 2 章は関連研究の紹介であり、マルウェアの静的解析や動的解析による特徴量抽出方法、および、マルウェア検知/分類への AI 応用の関連研究について紹介している。

第 3 章では、学習時に使われる損失関数にマルウェア検知用の学習に適した係数を追加することで、生成した識別器のマルウェア検知精度を向上させる提案を行っている。また、マルウェアの表層解析結果のデータセットを用いた評価により、提案するカスタム損失関数を導入して学習した LightGBM ベースのマルウェア識別器の有用性を示している。

第 4 章では、より高精度なマルウェア検知に向けてマルウェアバイナリの基本ブロック構造の学習による識別を目指し、グラフニューラルネットワークの一種である Graph Isomorphism Network を利用した特徴量抽出を提案した。提案手法は、バイナリの基本ブロック構造と基本ブロックごとの特徴量を学習して入力バイナリを最終的に 64 次元の特徴量ベクトルに変換する特徴量圧縮器を作成した上で、特徴量ベクトルを多層パーセプトロンで識別する構成の提案を行っている。マルウェアバイナリと無害なバイナリからなるデータセットを用いた評価により、提案する特徴量を用いた識別方法の有用性を示している。

第 5 章では、前章までの教師あり学習での成果に対し、Graph Contrastive Learning とデータ拡張を用いた自己教師あり学習による識別器を組み合わせ、教師データ無しで識別器によって出力されるクラスタリング結果からマルウェアであること、および、どのマルウェアファミリに所属するかの判定を行う提案を行い、評価においてその有用性を示している。

第 6 章は結論であり、本論文の成果のまとめについて述べている。

以上のように、本論文は、マルウェア検知/分類に適した損失関数の設定と基本ブロック構造の特徴量の圧縮方法、および、自己教師あり学習によるクラスタリングとマルウェアファミリの分類という、AI 技術によるマルウェア検知/分類性能向上に関する一連の提案を行っている。また、公開されているデータセットをもとにそれらの有用性を評価した上で既存手法と比較し、提案手法の有用性を示している。よって、情報科学の学術上・技術上の寄与が大きいと考え、本論文提出者である高氏は博士(情報学)の学位を受けるに十分な資格があるものと判定した。