別紙様式第２号

学位論文及び審査結果の要旨

横浜国立大学

氏　　名　新井　悠
学　位　の　種　類　博士（情報学）
学　位　記　番　号　環情博甲第５４８号
学位授与年月日　令和６年３月２５日
学位授与の根拠　学位規則（昭和 28 年 4 月 1 日文部省令第 9 号）第４条第１項及び横浜国立大学学位規則第５条第１項
学　府・専　攻　名　環境情報学府　情報環境専攻
学　位　論　文　題　目　サイバーセキュリティ領域における機械学習の適切な利用に関する研究
論　文　審　査　委　員　主査　横浜国立大学　教　授　松本　勉
横浜国立大学　教　授　森　辰則
横浜国立大学　教　授　四方 順司
横浜国立大学　教　授　吉岡 克成
横浜国立大学　准教授　白川 真一

論文及び審査結果の要旨

近年，機械学習の発展と社会への浸透が進み、サイバーセキュリティ領域においても同技術の活用が始まっている。例えば不正プログラムを検知するセキュリティ対策ソフトウェアにおいて、この判定に機械学習が利用されている一方で、他分野のような活用の広がりが十分に見られていない。さらに、攻撃者による故意の特徴量改変等、セキュリティ分野の応用ならではの課題が存在し、機会学習の特性を十分に理解した利用がされているか十分な検証が行われていない。

本論文では、序論の第 1 章の後に、第 2 章において機械学習をサイバーセキュリティの領域で積極的に活用することを検討し、社会的な問題であるダークウェブの犯罪関連サイトの自動検出への応用を提案している。提案方式では、効率的にダークウェブから犯罪に関連したフォーラム、いわゆる闇掲示板を自動的に特定出来ることを確認している．その際、従来のようにダークウェブサイトのコンテンツに着目した検知手法では、隠語の使用により検知率が低下することに着目し、サイトを構成するサーバプログラムの特徴である HTTP（ハイパーテキストトランスファープロトコル）ヘッダに着目した特徴量を用いることで高い検知率を実現している。次に第 3 章では市販のセキュリティ対策ソフトウェアにおいて機械学習による検出を主たる検知手法としている製品に対して、その検知を回避される可能性を調査している。調査の結果、機械学習による検出機能を単体で組み込んでいる製品に対して回避がされるおそれがあることを明らかにしている。具体的には機械学習の特徴量となっていることが推測されるファイル内の領域に無害なファイルに含まれる文字列を挿入することで特徴量を強制的に改変することで、検知が回避されることを示している。加えて従来型のパターンファイル検出と機械学習による検出機能をハイブリッドで使用している製品に対しても回避がされる恐れがあることも明らかにしている。そして結言を第４章にまとめている。

このように本論文は、機械学習のサイバーセキュリティ領域への有効活用の促進とその際の課題を明らかにしており、当該分野に貢献する内容を有していると評価できる。研究成果の公表は、査読付論文誌論文 2 篇が出版済みであり、評価を受けている。

上記より、本論文は博士（情報学）の学位論文として十分な価値を有すると論文審査委員全員一致で認め、令和 6 年 1 月 30 日（火）、10 時 50 分から 12 時 10 分まで博士論文発表会を実施し、終了後の 12 時 15 分から 12 時 35 分まで、審査委員全員出席のもとで、新井悠氏の最終試験を実施した。発表会参加者は 27 名であり、充実した質疑応答がなされた。

学力試験として情報セキュリティを中心とする専門分野および情報工学関連分野における

口頭試問を行い、これらの分野の研究に関する深い専門知識と理解力、表現力、および質疑応答における適切な対応能力を同氏が有することを確認した。

外国語は、国際会議において英語にて発表していることをもって、十分な学力を有すると判定した。また博士課程後期修了に必要な単位をすべて取得していることを確認した。

これらから、新井悠氏は最終試験に合格であると、論文審査委員全員一致で判定した。

以上の論文審査委員会の結論に基づき、令和 6 年 2 月 13 日（火）に開催の環境情報学府情報環境専攻会議にて審議し、全員一致で本論文を博士（情報学）の学位論文としての価値があるものとして環境情報学府教授会に付議することを決定した。その後、環境情報学府学務委員会での確認を経て、令和 6 年 3 月 4 日（月）に開催された環境情報学府教授会において審議を行い、無記名投票により、新井悠氏に博士（情報学）の学位を授与することを決定した。

注　論文及び審査結果の要旨欄に不足が生じる場合には、同欄の様式に準じ裏面又は別紙によること。