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	小出　駿
学位の種類	博士（情報学）
学位記番号	環情博甲第 2218 号
学位授与年月日	令和 3 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	A Study on Analyzing Cyber Attacks through Active and Passive Observation (能動的観測と受動的観測によるサイバー攻撃分析に関する研究)
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　准教授　吉岡克成 横浜国立大学　講　師　白川真一

論文及び審査結果の要旨

インターネットをはじめとする情報通信ネットワークにおけるサイバー攻撃が大きな問題となっている。一般にサイバー攻撃を詳細に観測し、分析する際は、観測のための仕組みを構築し、観測対象に能動的に介在する能動的観測と、観測対象に介在せずに通信やログなどを分析する受動的観測が行われる。

本論文は、この２つの観測方法をうまく組合せることで効率的効果的にサイバー攻撃の観測と分析を行う手法について検討したものであり、全 6 章から構成されている。第１章で序論を、第２章で能動的観測と受動的観測とその課題について述べている。

第３章ではユーザの興味や関心を引くことでソフトウェアダウンロードなどを行わせ、マルウェア等に感染させる、いわゆるソーシャルエンジニアリング型の攻撃を行う悪性 Web サイトの探索、検知、分析を行っている。人間のユーザによる操作を模倣し、インターネット上を探索し、これらの悪性サイトを発見するクローラを実装し、多数の悪性 Web サイトを発見すると共に、Web アクセスログから、悪性サイトを訪問したユーザの振る舞いを分析している。

第 4 章では、偽のセキュリティ情報を公開し、ユーザの興味をひくことで悪性サイトに訪問させ、攻撃を行う新しい脅威に着目し、第 3 章の研究で構築したクローラを用いてこれらの悪性サイトの探索を行い、多数の悪性 Web サイトを発見している。さらに、Web アクセスログや検索エンジンの結果の分析により、サイバー脅威に関するセキュリティ情報を主要な検索エンジンで探索すると、その大部分が悪性サイトへ誘導する検索結果となり得ることを示している。

続く第 5 章では、マルウェア等が生成する通信のうち、ネットワークプロトコルヘッダに現れる特徴に着目し、攻撃元のマルウェアや攻撃ツールを判別する手法を提案している。マルウェアや攻撃ツールは効率的に通信を行うため、OS 等の機能を使わず、ヘッダを含めたパケット全体を独自生成する場合があることに着目し、この特徴を調べることで、パケットレベルで攻撃元のマルウェアを高い精度で判別することに成功している。

最後に 6 章で本論文は締めくくられている。

上記のいずれの成果も能動的分析と受動的分析を効果的に組合せることで飛躍的な成果を上げており、本論文が取り上げる分析手法の有効性を示している。特に第 4 章で述べられている、偽セキュリティ情報により攻撃を行う悪性 Web サイトの分析については、これまでそ

の実態が知られていなかったが、本研究により、詳細な分析が行われた点が高く評価されており、国際会議 DIMVA2020 で論文賞を受賞している。また、第 5 章で提案されたプロトコルヘッダの特徴に基づく分析手法は、現在、IoT マルウェアによる攻撃通信の識別などにも広く用いられており、先駆的な成果となっている。

本論文は、サイバー攻撃の観測・分析という重要な課題に対して実効性の高い手法を提案するものであり、サイバーセキュリティ分野に貢献する内容を有すると評価できる。

研究成果の公表は、査読付論文誌論文 1 篇が出版済みであり 2 篇が採録済みである。また査読付き国際会議での発表が 2 件ある。

よって、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 3 年 2 月 5 日（金）、12 時 45 分から 14 時 15 分まで博士論文発表会を実施し、終了後の 14 時 15 分から 14 時 45 分まで、審査委員全員出席のもとで、小出駿氏の最終試験を実施した。博士論文発表会は、COVID-19 感染の状況を踏まえ、発表者と審査委員 5 名、および、その他の一般参加者がオンライン会議システムを通じて参加した。発表会参加者は総計 38 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、小出駿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 3 年 2 月 15 日（月）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 3 年 3 月 1 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、小出駿氏に博士（情報学）の学位を授与することを決定した。