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	Yin Minn Pa Pa
学位の種類	博士（工学）
学位記番号	環情博甲第 381 号
学位授与年月日	平成 28 年 3 月 24 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　情報メディア環境学専攻
学位論文題目	A Study on Detecting Cyber Attack Resources by Coordinated Passive and Active Monitoring
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　長尾智晴 横浜国立大学　教　授　森　辰則 横浜国立大学　准教授　四方順司 横浜国立大学　准教授　吉岡克成

論文及び審査結果の要旨

近年、サイバー攻撃の多様化複雑化が進み、多数のコンピュータを悪性プログラム、すなわちマルウェアに感染させ、これを一斉に制御することで大量のアクセスを対象に集中させ、サービス妨害を行う DDoS (Distributed Denial of Service)攻撃や、特定の組織や個人を狙って巧妙に加工されたなりすましメールやマルウェアを送ることで秘密裏に侵入を行い、重要情報を窃取する標的型攻撃などが社会問題化している。

サイバー攻撃を実施する攻撃者は、脆弱なホスト群に侵入しこれらを操作してさらに多様な攻撃を試みる。このように攻撃者はネットワーク上に自らが利用可能な計算資源、情報資源を有している。本論文は、従来から行われている受動的観測に能動的観測技術を融合すると効果的にこれらのサイバー攻撃リソースを検出できるのではないかとのコンセプトに基づき行った研究をまとめたものである。本論文で観測・検知を行う対象のサイバー攻撃リソースとして、インターネットにおける基幹システムの１つであるドメインネームシステム (DNS) と、近年飛躍が著しい IoT (Internet of Things, モノのインターネット) を扱っている。

DNS においては、攻撃者が権限を有しているドメイン名や当該ドメインの権威サーバ、および、それらに対応する IP アドレスの関係に着目し、正常利用とは異なる特徴を見出すことで、これを用いてサイバー攻撃に悪用されている悪性ドメイン、悪性権威 DNS サーバ、それらの IP アドレスを特定する手法を提案している。従来悪性ドメイン、悪性 IP アドレスに関する検知手法は多く検討されているものの、悪性権威 DNS サーバを検知対象にすることは初めての試みであり、これにより、ブラックリスト等の既存知識に頼ることなく、高い精度で検知を実現している。また IoT においては、IoT を構成する様々な組み込み機器が共通に有する脆弱な Telnet プロトコルの存在に着目し、この脆弱性を模擬する囮システム(ハニーポット)を構築することで、IoT において活動する不正プログラム(マルウェア)の捕獲、詳細解析を世界で初めて行っている。

本論文は 8 章からなり、第 1 章の序論に続き、第 2 章で背景となる受動的観測手法、能動的観測手法、DNS におけるサイバー攻撃、Telnet プロトコルを狙った攻撃について説明している。3 章では、本論文を貫く方法論として、受動的観測技術と能動的観測技術の効率的な連携方法について説明している。具体的には、新たなサイバー攻撃に対する、気づき(Awareness)、悪意の確認(Confirmation of Maliciousness)、付加情報収集(Enrichment)という 3 つのフェーズからなる観測のフレームワークを提案している。さらに観測技術群の体系化を行

い各フェーズにおいて有効な観測技術を説明している。4 章では関連研究について述べ、5 章では悪性権威 DNS サーバの特徴に関する事前調査を行い、その後の手法検討、提案の基盤としている。6 章では、5 章の調査に基づき、悪性ドメイン、悪性権威 DNS サーバ、それらの IP アドレスの関係を受動的観測と能動的観測を用いて導き、さらにこれらの関係においてサイバー攻撃に悪用される場合に突出して多く見られる 3 つの特徴に注目し、新たな検知手法の提案と評価を行っている。7 章では IoT ハニーポットの提案を行い、受動的な観測による感染ホストの検知と能動的観測による感染ホストの詳細情報取得を提案している。さらに 8 章で本研究のまとめと今後の課題について述べている。

以上のように、本論文は、受動的観測と能動的観測を駆使してサイバー攻撃に用いられるリソースを検知することで、よりセキュアなインターネットの実現に貢献できる実用的かつ効果的な手法を提案しており情報セキュリティ分野の研究に大きく貢献するものである。また、本論文の研究内容は、2 篇の査読付論文誌論文、2 篇の査読付国際会議論文(うち 1 件は最優秀論文賞を受賞)、1 件の査読付き国際会議ポスター発表, 3 篇の研究会論文(うち 1 篇は年間最優秀技術報告賞を受賞)が研究会・シンポジウム論文により公表されており、学会からも高い評価を得ている。

よって、本論文は博士（工学）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、平成 28 年 2 月 9 日（火）15 時から 16 時 30 分まで、環境情報 1 号棟 515 号室において博士論文発表会（公聴会）を開催した。博士論文発表会は 43 名の参加者を得て、活発な質疑応答がなされた。同日 16 時 30 分より 17 時まで、環境情報 1 号棟 7 階ゼミ室において論文審査委員全員出席のもと、Yin Minn Pa Pa 氏の最終試験を行った。審査委員からの博士論文に関する質問、情報セキュリティを中心とする専門分野および工学分野における専門知識に関する質問に対する応答から、専門知識、博士論文の内容の公表状況について十分であることを確認した。外国語については、英語による論文執筆ならびに国際会議発表があることをもって学力を確認した。また、履修単位が修了要件を満たすことを確認した。これらから、同氏は最終試験に合格であると、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、平成 28 年 2 月 12 日に開催した環境情報学府 情報メディア環境学専攻会議にて審議し、全員一致で本論文を博士（工学）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、平成 28 年 3 月 7 日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、Yin Minn Pa Pa 氏に博士（工学）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。