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	原　悟史
学位の種類	博士（工学）
学位記番号	環情博甲第 2175 号
学位授与年月日	令和 2 年 9 月 30 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　（論博の場合は第 2 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	IoT 機器に対するマルウェア持続感染の分析に関する研究
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

近年、ルータや IP カメラといった組込み機器、いわゆる IoT 機器がサイバー攻撃の対象となり、多くの機器がマルウェア感染するなど社会的な問題となっている。特に 2016 年に出現した Mirai と呼ばれるマルウェアは世界で数十万台の機器に感染し、史上最大規模のサービス妨害攻撃を行うなど、大きな脅威となっている。これに対して、機器の所有者等に注意喚起を行い、マルウェアの駆除を行う活動が国内外で行われている。Mirai に代表される IoT マルウェアの多くは、強い感染力を有するものの、機器の電源を再起動するとシステム内から消去されるという特性を持っており、専門的知識を有さない所有者であっても駆除が容易であった。すなわちこれらの IoT マルウェアは、再起動後も感染状態を維持するために不揮発領域に自身の複製を残したり、再起動後に自身の複製を自動実行するように設定を変更したりするといった機能を有していなかった。当時は IoT 機器のシステムやハードウェアの多様な構成に対し再起動への汎用的な耐性を持たせることが難しかったことが要因ではないかと推察される。

しかし、2018 年に出現した VPNFilter というマルウェアは、感染した機器の再起動後も活動を続ける「持続感染性」を有しており、数十万台に感染したと報告されている。その後も持続感染性を有する IoT マルウェアが報告されている。ウイルス対策ソフトウェアなどのセキュリティ対策ソフトウェアの導入が必ずしも容易でない IoT 機器に対して、持続感染性を有するマルウェアは大きな脅威であり、感染すると、専門知識のないユーザによる駆除は非常に困難となる。

本論文は、この IoT 機器に対するマルウェア持続感染の分析に関する研究を主題とし、全７章から構成されている。第１章で序論を、第２章で関連研究を示した後、第３章で IoT 機器に対するマルウェア持続感染の分析の概要を示し、得られた研究成果の関係を説明している。

第 4 章では持続感染型 IoT マルウェアの実態調査と実機による概念実証を示している。持続感染型 IoT マルウェアはこれまでいくつかの事例があるものの、その実態について体系的な整理は行われていなかった。このため本論文では持続感染型 IoT マルウェアの実現形態を整理し、主に不揮発性メモリへの設定変更という方法と、ファームウェア更新機能を

悪用したファームウェア差し替えによる方法に大別されることを示している。そして、どちらの場合についても、実機を用いて実際に持続感染があり得ることを実証している。

続く第 5 章では、持続感染型 IoT マルウェアへの直接的な対策として駆除手順を導出することを目指し、当該マルウェアを動的解析して、持続感染のための動作を明らかにする方法を検討している。すなわち、持続感染の対象となる機器が入手可能であり、それを動的解析の実行環境として利用できるというシナリオで、実機によるマルウェア動的解析を行うための手順について明確にしている。一般に製品として流通する組込み機器は事後的な改変や改良を行うことが難しく、これを動的解析環境として用いることは難しい。そこで、動的解析を行う上で必須となる機能を定義し、それを実現するために IoT 機器に必要となる要素を明らかにしている。さらに、実際の機器を用いて、これらの要素が満たされるかどうかを分析している。

第 6 章においては、第 5 章と対になる提案として、仮想マシンを用いた IoT マルウェア動的解析手法を示している。持続感染挙動を引き出すために、様々な機器のファームウェアからファイルシステムの構造を抽出し、それらを動的解析環境に付加することにより、解析の効果を向上させている。そして本論文は第 7 章で締めくくられている。

以上のように本論文は、大きな問題となっている持続感染型 IoT マルウェアに対して実効性の高い対策を導入するものであり、サイバーセキュリティ分野に貢献する内容を有していると評価できる。

本論文を構成する主要な研究成果は、査読付論文誌論文 2 篇、情報処理学会および電子情報通信学会のシンポジウム論文 2 篇、査読付き国際会議ポスター発表 1 件により公表され、評価を受けている。

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、令和 2 年 7 月 17 日（金）、12 時 50 分から 14 時 20 分までの環境情報 1 号棟 515 号室における博士論文発表会終了後の 14 時 30 分から 15 時 00 分まで、同室において審査委員全員出席のもとで、原　悟史氏の最終試験を行った。博士論文発表会は、COVID-19 感染の状況を踏まえ、上記会場には、発表者と審査委員 5 名、および 2 名の一般参加者が集い、その他の一般参加者はオンライン会議システムを通じて参加するハイブリッド方式で実施した。発表会参加者はオンラインを含め総計 45 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、原悟史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 2 年 7 月 27 日（月）に開催の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、令和 2 年 9 月 7 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、原悟史氏に博士（工学）の学位を授与することを決定した。