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	髙田 一樹
学位の種類	博士（工学）
学位記番号	環情博甲第 2140 号
学位授与年月日	令和 2 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　（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	金融系マルウェア長期観測に基づく MITB 攻撃の解析および対策の研究
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、インターネットバンキング等の金融機関サービス利用者をターゲットとしたサイバー攻撃による不正送金や情報盗取の被害が、社会問題となっている。これらのサイバー攻撃の主要な攻撃方法にマルウェアによる Man-In-The-Browser 攻撃（以下、MITB 攻撃）があり、注目を集めている。MITB 攻撃は、マルウェアが感染 PC の Web ブラウザにメモリインジェクション等の方法で入り込み通信内容の改ざん等を行う攻撃である。MITB 攻撃により、インターネットバンキング等の正規の Web サイトが感染 PC 上で改ざんされ、不正送金や情報盗取が発生する。

本論文は、インターネットバンキング等の金融機関サービス利用者をターゲットとした不正送金や情報盗取を行うマルウェア（以下、金融系マルウェア）の行う MITB 攻撃の実態を解明し、対策技術を開発することを目的としている。また、一般にサイバー攻撃とその対策は、ある攻撃手法に対する対策手法を実施するとその対策手法を無効化した攻撃手法に変化するため、さらに対策手法を更新するといった攻撃者と防御者による“攻防無限ループ”に陥るという問題が生じる。本論文では、攻防無限ループにおいて攻撃の変化に対して対策を適切に更新することにより MITB 攻撃による被害を低減し、最終的に攻防無限ループを防御者優位で終わらせることを可能とする MITB 攻撃対策のエコシステムを提案している。本論文は全 7 章からなり、第 1 章は緒論を述べ研究の背景を説明し、第 2 章で関連研究を説明している。3 章では、金融系マルウェアの挙動を長期観測し攻撃対象などの変遷を調査する方法を提案している。4 章では MITB 攻撃の中核をなす悪性 JavaScript の動的解析手法、5 章では、主に日本で流行した MITB 攻撃の分類と、分類に基づく既存対策の効果を評価している。6 章では MITB 攻撃対策のためのエコシステムを説明し、7 章で結論を述べている。

MITB 攻撃は攻撃対象の銀行サイト等を定義した攻撃設定情報を攻撃者の制御サーバから取得し、それに基づき、銀行サイト等の改ざんや通信の盗聴などを行う悪性 JavaScript をダウンロード、実行することで攻撃が行われる。攻撃設定情報は攻撃対象の金融サイト等重要な情報が記載されており、攻撃の変遷に従い更新されるため、この内容を正確に把握す

ることが重要である。そのため、本論文では、金融系マルウェアを長期動的解析し、定常的に攻撃設定情報を取得、収集解析する手法を提案している。さらに、MITB 攻撃の核となるサイト改ざんや盗聴の機能が実装された悪性 JavaScript を動的解析する環境を提供し、実際にサイト改ざんにより注意喚起文の削除される様子や、パスワードや暗証番号を不正に要求する様子などを再現し、対策に役立てている。このような解析により数年にわたる金融系マルウェアの解析を行った結果に基づき、本研究では MITB 攻撃の分類を行うと共に、既存の対策の効果を定性的に評価している。さらに、これらの対策と攻撃が本質的には同様の権限下で行われており、互いに決定的な対応が出来ないことから生じる「攻防無限ループ」状態に着目し、継続的かつ効率的な対策の実施により攻撃者のコストを増加させ、最終的に攻防無限ループを終息に導くというコンセプトを示している。また、このコンセプトに基づき、国内の金融系マルウェアへの対策を実施した実例を示している。

以上のように、本論文は、社会的な問題となっている金融系マルウェアによるサイバー攻撃について実際の攻撃やマルウェアの観測・分析により具体的かつ詳細な分析を行い、実効性の高い対策を導出しており、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、3 篇の査読付論文誌論文、9 篇の電子情報通信学会および情報処理学会のシンポジウム論文、 1 件の国際会議発表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 2 月 5 日（水）10 時 40 分から 12 時までの環境情報 1 号棟 305 号室における博士論文発表会終了後の 12 時 05 分から 12 時 30 分まで、同棟 3 階 304 室において審査委員全員出席のもとで、高田一樹氏の最終試験を行った。37 名の参加者を得て充実した質疑応答がなされた博士論文発表会を踏まえ、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、高田一樹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、令和 2 年 2 月 17 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 3 月 2 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、高田一樹氏に博士（工学）の学位を授与することを決定した。