平成29年度 情報工学コース卒業研究報告要旨

楫 研究室	氏　　名	山 中　隆 太 郎
卒業研究題目	X-headerを利用したメール送信環境のフィンガープリンティング	

近年, コンピュータとネットワークの飛躍的な進歩とともに, サイバー犯罪の規模が増大し, その手口も高度化している. なかでも, 特定の企業や個人の機密情報窃取を目的とした標的型攻撃による被害規模は大きく, 社会的な脅威となっている. 標的型攻撃の初期潜入の手段として, 偽装したマルウェアつきの電子メールをユーザに送付し, ユーザの誤操作等を誘う手口が広く利用されている. 受信者がメールの偽装に気づかず, 攻撃者が添付したマルウェアを開いてしまうと端末がマルウェアに感染してしまう. このような偽装メールは標的型攻撃メールと呼ばれる. 標的型攻撃メールでは件名や本文が受信者に関連のある内容に偽装されていることが多いため, 受信者が不正なメールであると判断することが難しい. また, 攻撃者がソーシャルエンジニアリングの手法を用い, 標的に合わせて攻撃手法を変化させることも多いため, ウイルス対策ソフト等の一般的な対策での解決が困難である.

標的型攻撃メールでは送信者情報が正規の送信者に詐称されているケースが大多数であり, そのことがメール送信者の誤操作を招く大きな要因となっている. メール送信端末やメールの配送経路等を検査することで送信者情報の詐称が発見できる場合もあるが, 組織内の端末がマルウェア等に感染し, その端末から標的型攻撃メールが送信されると, 送信端末や配送経路から不正を発見することは難しくなる. この問題に対処するには, メール送信に利用されるプログラムを含め, メール送信環境の違いを検出することが必要となる. 本研究では,RFC(Request for Comments)822 で定義されている, ユーザやアプリケーション等が任意で定義することが可能なヘッダ群である X-header を用いてメール送信環境のフィンガープリンティング技術を構成することを検討し, その検討に必要となる基礎データの収集および分析を行う.

基礎データの収集にあたっては,2014 年から 2017 年までに同一ユーザが受信したメール 48360 件を用い, メールに含まれる X-header の種別を調査し, 代表的な X-header に関してメール配送経路のどの段階で付与されるのかについて分類を行った. また, 同一送信者のメールにおける X-header の同一性, 異なる送信者のメールにおける X-header の相違等について詳細に分析を行った.

分析の結果,48360 件の受信メールから 950 種類の X-header を確認した. また, 送信者ごとにメールに含まれる X-header には一定の差異があり, 標的型攻撃メールの検知に対し有効であると考えられることを確認した. しかし, 送信している MUA(Mail User Agent) のアップデートやメールサーバの設定の変更などにより, 同一送信者内でも X-header の保有状況の変化が確認され, メーリングリストを経由して送られてきたメールでは同一送信者であっても X-header の保有状況が異なる現象も見られた. これらの観察結果より, 単純な X-header の比較では標的型攻撃の検知に使用するのは難しいという課題も浮かび上がった.