2017 年度 湘南藤沢学会「研究助成基金」成果報告書

総合政策学部 4 年
尾崎周也

活動名称

シンポジウム「マルチメディア、分散、協調とモバイル(DICOMO2017)シンポジウム」での論文・研究発表

活動日程と場所

日程：2017 年 6 月 28 日～2017 年 6 月 30 日

場所：北海道札幌市 定山渓万世閣ホテルミリオーネ

活動の目的

現在取り組んでいる研究テーマについて対外発表を行うことで研究をブラッシュアップするため。対外発表を行うことで研究に関するフィードバックを得るとともに、他組織からの参加者との交流を深め意見交換を行うことで、今後の研究活動に生かすことを目的とする。

活動内容と成果

私の研究は電子メールの通信経路の暗号化を行うものだ。電子メールには既存のセキュリティシステムが施されているが、一部の攻撃に対しては脆弱である。その攻撃の中でも中間者攻撃と呼ばれるものがあり、それに対応するのが私の研究テーマである。

先に述べた“MTA-STS”であるがインターネットプロトコルの標準化団体、IETF の UTA Working Group で目下検討中の新しいセキュリティシステムだ。私が実証実験の中で実装した“MTA-STS”は動作する OSS 実装(誰でも利用できる形に公開されたもの)として現在(2017 年 4 月 9 日)唯一のものである。また現在の大手メールサービスの“MTA-STS”の利用状況について調査を行なった。

参加をした「マルチメディア、分散、協調とモバイル(DICOMO2016)シンポジウム」は情報処理学会の諸研究会がネットワークに関する研究分野を中心

に、分散システム・ITS・セキュリティなど分野横断的に開催するシンポジウムだ。本シンポジウムは 3 日間に渡り合宿形式で開催され、学術的な研究論文のみならず、事例報告、問題提起など幅広く議論が行われた。私は「MTA-STS : SMTP MTA Strict Transport Security を用い暗号化された電子メール通信経路の確立とその実装」というタイトルでシステムセキィリティの部門での発表を行った。

発表の際のフィードバックからこれまで見落としていた、MTA-STS の普及は既存技術の普及と同種の問題を持つことに気がつき、今後の研究の課題にしたい。また会期中には他分野のセッションを含め知見を広めることができたとともに、多くの研究者と交流を深め意見交換を行った。

謝辞

本発表は、慶應義塾大学**湘南藤沢学会 「研究助成基金 2017」**の支援によって行われた。