タザキ財団留学報告書２０２４年６月　（田村花）

先日無事にケンブリッジ大学での修士論文を提出し、９ヵ月間のコンピュータサイエンスの修士課程はあっという間に終わってしまいました。短い期間に色々なことを学び、研究する喜びを発見し、研究をこれからも続けたいと思うようになった期間でした。授業は、デジタル信号処理、コンピュータセキュリティ、サイバー犯罪、人間中心の AI 研究、ブロックチェーンなど多様な分野で受けました。特にコンピュータセキュリティの研究に興味があったので、コンピュータセキュリティのコースで、分野の基礎となる論文を数多く読み、議論することが楽しかったです。また、ケンブリッジ大学の研究者グループの 1 つであるコンピュータセキュリティ・グループの一員として、毎週多くの講演やミーティングに参加し、よりカジュアルな場でコンピュータシステムの防御や保護に関する理解を深めることができました。特に、この分野のパイオニアである故元指導教官のロス・アンダーソン教授の指導には感謝しています。アンダーソン教授のサイバーセキュリティ経済学における洞察は、現実に近いセキュリティにおけるインセンティブの影響やその他の現実的なセキュリティの複雑性に私の目を開かせてくれました。

私の修士論文の目的は DNN（Deep Neural Networks）のモデルパラメータを抽出するというタイプのサイバー攻撃の性能を精査することで、現在どれほどの速度でどの程度の攻撃が可能なのかを分析することです。結果的には現存のサイバー攻撃の速さを何倍か加速することに成功し、規模の小さい人工知能だったら実際に活用されているモデルのパラメーターを盗むことができるということを示すことができました。さらにこの内容の論文を NeurIPS という有名な大きい機械学習の国際会議に提出することができました。指導教官のロス・アンデルソン教授が３月末に突然お亡くなりになられた時はどうなるかと一時期思いましたが、ありがたくもディープマインドの研究者である副指導教官とケンブリッジでの新しい指導教官のサポートのおかげでここまで来られたと思います。

さらに、ケンブリッジ大学での修士課程での研究は、私に新たな道を開けてくれました。修士課程を始める前は迷っていたのですが、修士論文に取り組んでいる間に研究に興味とやりがいを見出すことができ、研究の道を歩もうと決意することができました。お陰様で、インペリアル・カレッジ・ロンドン、トロント大学、ケンブリッジ大学の 3 校から博士課程への合格通知を得ることができました。インペリアル・カレッジ・ロンドンとトロント大学からは学費免除と生活費援助の奨学金付きの合格通知だったのですが、ケンブリッジ大学の恵まれた研究環境での研究を希望していたので、Tazaki 財団様の援助を引き続き頂けることになってケンブリッジ大学に残れることになり、たいへん有難く思っております。博士課程では、人工知能のセキュリティの研究を続ける予定です。さらに、7 月からはドイツのダルムシュタット工科大学での研究インターンをしています。私が今まで関わってこなかったハードウェアのサイバーセキュリティの研究など、私にとって未知の分野の研究を行っている研究者が多く、非常に刺激的です。10 月から始まるケンブリッジでの博士課程の前に、視野を広げ、共同研究の糸口をつかむことができればいいなと考えております。

学業以外でもケンブリッジは面白い人と機会に巡り合える場所で、これからも三年間ここで暮らせることを楽しみにしています。ケンブリッジで出会った人たちは様々な文化背景を持っていて、そのような人たちと、例えば各国の教育制度について比較するなど、とても興味深い会話をすることができました。また、大学が斡旋してくれているボランティア活動の一端を担い、サイバーセキュリティについて興味を持っている女子高生のチューターをする機会にも恵まれました。まだまだ女性の少ない IT 分野に次の世代の女子学生に関心を向けてもらえるような活動は有意義で、今後もこのような活動に貢献していきたいと思っています。自由時間には、大学の音楽室を使ってフルートやピアノを楽しんでいます。

Tazaki 財団様の変わらないサポートはいつも私の力になっております。私の可能性を信じていただけている分、期待に沿える結果を出したいという気持が、私を前進させてくれているのだと思います。修士課程在学中へのご支援、誠にありがとうございました。また、博士課程在学中も引き続きよろしくお願いいたします。