

# 第一回 留学報告書

2024年 12月

高橋秀明

2024年夏より Columbia University, Department of Computer Science, Ph.D.課程に進学しました、高橋秀明です。第一回目となる本報告書では、渡米から最初の学期を終えるまでのなんやかんやを報告させていただきます。

## 1. 渡米

4月に進学先を決定し、5月ごろに住居も決まりました。物件は大学が所有しているアパートで、家賃は相場よりは安いです。7月末までは Apple で AI/ML Software Engineer のインターンシップをしつつ、基本的には遊んで暮らしていました。8月上旬に渡米し生活の立ち上げを始めましたが、家具や家電類は備え付けられていた上に、インテリア等には特にこだわりのない性格のため、最初の2日くらいで部屋の準備は完了しました。銀行口座も2日目に開設しました。授業が始まるのは8月末からで、それまでは特になにもやる事がなかったため、もっと遅くに来てよかったと思います。

## 2. ニューヨークでの生活



Columbia University はニューヨークのマンハッタン島の北西部に位置し、有名な Times Square までは電車で15分くらいの距離です。地下鉄やバスは基本的には時間通りに来ますし、本数も多く24時間営業のため、車がなくても特に問題ないです。本格的な和食レストラン、日本製の製品をメインに扱うコンビニや薬局なども多いため、割高であることに目をつむれば、東京とあまり変わらない生活ができると思います。また、ニューヨークはピザやベーグルが有名ですが、実際種類も日本に比べてかなり多く、とても美味しいです。

## 3. 授業

Columbia University の CS Ph.D.では最初の2年半で授業を10個受講する必要がある、

今学期は Machine Learning と Security の二つを受講しました。どちらの授業もそこまで忙しくはなく、ほかの学生に比べてかなりゆとりがある生活を送っており、研究にもそれなりに時間を費やすことができました。

Machine Learning は理論面に重点を置いており、実質的に線形代数と統計の授業でした。成績は 3 回の試験および機械学習モデルの精度を競うコンペティションによって決まります。試験は CS Department の中で最も難しいと言われるほどで、毎回平均点が 20~30%ほどでした。コンペティションではクラス内で 1 位になり、試験の成績もある程度良かったため、無事 A を取ることができました。

Security も座学が中心で、2 回の試験および 2 つの宿題で成績が決まります。宿題は実践的なものが多く、ファイル暗号化ツールを作ったり、演習用の Web アプリを攻撃してみたりといったものでした。試験であまり手ごたえを感じなかったため、まだ成績発表がなされていませんが、かなりそわそわしています。

#### 4. 研究

研究面では、「ゼロ知識証明の回路の実装に脆弱性がないかを検知する」というプロジェクトに取り組んでいます。自分で提案した研究プロジェクトということもあり、なかなか楽しく取り組んでいます。ゼロ知識証明とは、入力  $x$  に対して出力  $y$  を返すようなプログラム  $P$  があるとき、「私は  $P$  の出力が  $y$  となるような入力  $x$  を知っている」ということを、入力  $x$  を公開することなく証明する技術です。この際、証明者はプログラム  $P$  を適切な多項式制約に変換する必要があるのですが、この制約が不十分もしくは過剰であると、適切な証明を生成することができなくなってしまいます。パターンマッチングや形式検証を用いた先行研究は近年発表されているのですが、スケーラビリティや False Positive といった問題を抱えています。まだプロジェクトは始まったばかりですが、すでに自作のプロトタイプのツールを使っていくつか脆弱性を発見することができているので、次の報告書までには実用に耐えるツールを完成させられたらなと思っています。

#### 5. 最後に

改めまして、留学を支援していただいている船井情報科学振興財団の皆様にご挨拶申し上げます。ご期待に応えることができるよう、より一層努力を重ねたいと思います。