# 先端科学技術研究科　修士論文要旨

| | | | |
|---|---|---|---|
| 所属研究室<br>（主指導教員） | 大規模システム管理<br>（笠原　正治　（教授）） | | |
| 学籍番号 | 2311160 | 提出日 | 令和 7年 1月 16日 |
| 学生氏名 | 田口　穂鷹 | | |
| 論文題目 | eBPFを活用したオートエンコーダによるリアルタイムカーネル内侵入検知システム | | |

要旨

従来の機械学習を活用した侵入検知システム (Intrusion Detection System: IDS) は，学習モデルの推論性能に着目しているが，カーネル・ユーザ空間の間で発生するコンテキストスイッチコストを無視している．既存研究では，量子化した学習モデルをextended Berkeley Packet Filter (eBPF) にオフロードすることで，カーネル空間内でリアルタイムなIDSを実現している．ただし，学習済みモデルに対して量子化パラメタを調整するため，追加の学習によるモデルの微調整ができず，継続的なモデルの更新を困難にしている．本稿では，教師なし学習であるオートエンコーダ (Autoencoder: AE) と代表的な量子化手法であるQuantization-Aware Training (QAT) を組み合わせることで，継続的な学習を可能にするリアルタイムカーネル内IDSを提案する．実証実験より，提案方式の有効性を推論精度とパケット処理性能の観点から検証する．