2023 年度年次報告書
社会変革に向けた ICT 基盤強化
2022 年度採択研究代表者

吉岡 健太郎

慶應義塾大学 理工学部
専任講師

サイバーとフィジカルを横断したセンサセキュリティ研究

研究成果の概要

本研究グループは、自動運転用 LiDAR センサーのセキュリティー特性を明らかにするため、新旧あわせて 9 種類の LiDAR センサーと 3 種類の主要な物体検出器に対する大規模な測定研究を行った。その結果、次世代 LiDAR は旧世代の LiDAR とは異なる脆弱性特性を持つことを発見した。具体的には、次世代 LiDAR ではレーザー発射タイミングのランダム化といった干渉回避機能が備えられており、これらの機能によって従来の同期攻撃が無効化されることを明らかにした。

さらに、上記のセキュリティー解析を元に、新たな攻撃手法「HFR（高周波レーザー除去）攻撃」の実用性を明らかにした。HFR 攻撃は、攻撃用のレーザーパルスを対象となる LiDAR のレーザー発射周波数よりも高い周波数で大量に発射することで、電波妨害のように対象 LiDAR の計測を妨害し、物体を消去する攻撃である。本研究グループは、HFR 攻撃が様々な種類の LiDAR センサーにおいて物体消失を起こすことが可能であり、市街地における運転といった現実に近い攻撃シナリオでも実用的であることを実証した。

今後は、本研究で明らかにした脆弱性への対策に注力する。具体的には、悪意のあるレーザー攻撃に対する LiDAR センサーの耐性を向上させる技術や、偽装データの注入を防ぐ新たなアルゴリズムの開発を進める予定である。さらに、異なる種類のセンサー（レーダーやカメラなど）との組み合わせによる安全性向上の可能性も探求する。最終的に、本研究成果が全世界の自動運転車両のセキュリティー強化、そしてそれによる社会全体への安心・安全の提供に貢献することを目指す。

【代表的な原著論文情報】

1) “LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies”, Takami Sato*, Yuki Hayakawa*, Ryo Suzuki*, Yohsuke Shiiki*, Kentaro Yoshioka, Qi Alfred Chen *共同第一著者, NDSS Symposium 2024.
2) R.Suzuki, T. Sato, Y.Hayakawa, K. Ikeda, O. Sako, R. Nagata, Q. Chen, K.Yoshioka, "WIP: Towards Practical LiDAR Spoofing Attack against Vehicles Driving at Cruising Speeds", Vehicle Sec, 2024.
3) Y.Hayakawa, T. Sato, R.Suzuki, K. Ikeda, O. Sako, R. Nagata, Q. Chen, K.Yoshioka, "WIP: An Adaptive High Frequency Removal Attack to Bypass Pulse Fingerprinting in New-Gen LiDARs", Vehicle Sec, 2024.