プレスリリース

2025 年 2 月 25 日

慶應義塾大学
科学技術振興機構（JST）

走行中の自動運転センサーを長距離から無効化できることを発見
ー脆弱性を明らかにし、より安全な自動運転車両の開発に貢献ー

慶應義塾大学理工学部電気情報工学科の吉岡健太郎専任講師、同大学院修士課程の速川湧気、鈴木諒らと、カリフォルニア大学アーバイン校のアルフレッド・チェン助教授、同大学院博士課程の佐藤貴海は共同で、自動運転車両の LiDAR センサーシステムにおける新たな脆弱性を発見しました。本研究チームは、高速走行中の車両の LiDAR センサーが長距離から無効化可能であることを世界で初めて実証し、安全な自動運転の実現に必要な対策を提示しました。

自動運転技術は私たちの未来社会を大きく変革するポテンシャルを秘めていますが、その安全性の向上が不可欠です。本研究では、高速走行車両のセンサーを追従可能なシステムを開発し、60km/h で走行中の車両に対して 110m 離れた地点からセンサーを無効化できることを確認しました。また、最新の LiDAR センサーに対しても、既存の防御機能を回避できる新たな手法を発見しました。さらに、オープンソース自動運転ソフトウェア（Autoware）を搭載した車両での実証実験により、センサーの無効化が衝突リスクやシステム停止につながる可能性があることを明らかにしました。この研究成果は、自動運転車両のセンサーセキュリティの重要性を示すとともに、より強固な安全対策の開発につながる重要な知見を提供します。

本研究成果は、2025 年 2 月 24 日～27 日開催のセキュリティ分野のトップ国際会議「Network and Distributed System Security（NDSS）Symposium 2025」に採択され、2025 年 2 月 21 日に論文がオンライン掲載されました。なお、今回明らかになった脆弱性については各 LiDAR メーカーに共有し、一定の対策期間を経て本研究成果を公開しています。

1. 本研究のポイント

- **新しい攻撃システムの開発：** 高速で走行する車両に対して長距離（110m 以上）から LiDAR センサー[※1]攻撃を実現する「Moving Vehicle Spoofing （MVS）システム」を開発しました。赤外線（IR）カメラによって LiDAR センサー自身が発するレーザー光を追従することで現実的な車両に対する攻撃能力を得られることを示しました。また最新の LiDAR が備える防御機構を回避できる「Adaptive High-Frequency Removal （A-HFR）攻撃」を発見しました。この攻撃は、LiDAR のスキャンパターンに関する知識を利用し、より高い周波数のレーザーパルスを効果的に発生させる攻撃です。
- **世界初の実自動運転車への攻撃：** オープンソースの自動運転ソフトウェア「Autoware」を搭載した車両に対して LiDAR 攻撃を行い、衝突事故や急ブレーキが誘発されることを実証しました。また市街地走行を模して 60km/h で走行する車両に対する攻撃にも成功し、本システムの有効性を示しました。
- **自動運転の安全性と信頼性の強化：**この研究は、自動運転におけるセンサーセキュリティ問題に焦点を当てた研究です。本研究グループが特定した攻撃やそれに対する防御策は、自動運転車両がさらに安全かつ信頼性の高いものになるための重要な指針を提供します。

2. 研究背景

自動運転技術の急速な発展に伴い、車両の周囲環境を正確に把握するためのセンサー技術の重要性が高まっています。その中でも、LiDAR（Light Detection And Ranging）センサーは、高精度な 3D 空間認識能力を持つことから、多くの自動運転システムに採用されています。しかし、この LiDAR センサーの安全性と信頼性が、自動運転車の普及における重要な課題となっています。

これまでの研究では、LiDAR センサーに対する悪意ある攻撃の可能性が示唆されてきましたが、それらは主に低速・短距離の環境下での実験に限られていました[1-3]。そのため、実際の道路環境での高速走行や長距離からの攻撃に対する脆弱性については、十分な検証がなされていませんでした。また、最新の LiDAR センサーには様々な防御機構が組み込まれており、これらの防御策の有効性も未知数でした[3]。

さらに、自動運転車の実用化が進む中で、センサー攻撃が実際の交通安全にどのような影響を及ぼすかについても、実証的な研究が不足していました。特に、実際に自動運転システムを搭載した車両を用いた攻撃実験は、これまで行われていませんでした。

このような背景から、本研究では以下の 3 つの主要な課題に取り組むことにしました。

1. 高速で走行する車両に対する長距離からの LiDAR 攻撃の実現可能性
2. 最新の LiDAR センサーに搭載されている防御機構の有効性の検証
3. 実際の自動運転車に対する LiDAR 攻撃の影響の実証

3. 研究内容・成果

本研究では、自動運転車の安全性に重大な影響を与える可能性のある新たな LiDAR センサー攻撃手法の開発と実証を行いました。その中心となる成果は、MVS システムの開発、A-HFR 攻撃の発見、そして実際の自動運転車を用いた実証実験の 3 点です。

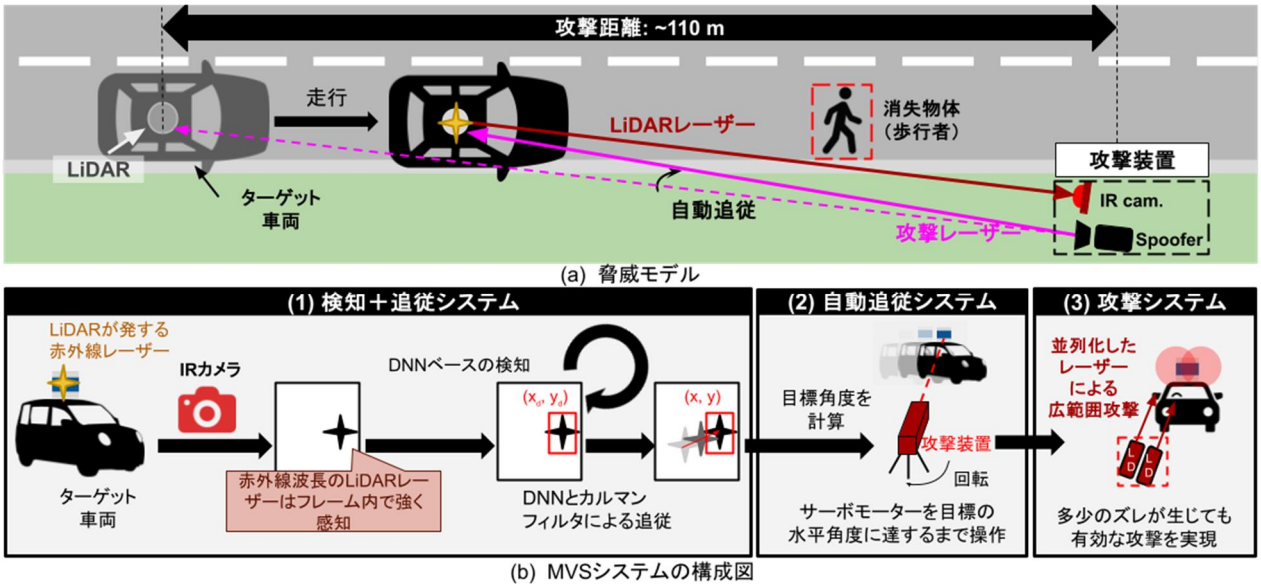


図 1： Moving Vehicle Spoofing (MVS)システム

本研究グループは図 1 に示す MVS システムを開発することで、高速で移動する車両に対して長距離から LiDAR センサー攻撃を実現しました。従来の攻撃手法では、カメラでセンサーを検出しレー

ザーを狙い当てる方式を採用していましたが、これは車両速度 5km/h、攻撃距離 10m という制限があり、実世界での適用は困難でした。しかし、新たに開発された MVS システムは、この制限を大幅に改善しました。

MVS システムは、IR カメラによるセンサー検出・追跡機構、高精度自動照準機構、そしてレーザー攻撃機構から構成されています。IR カメラの導入により、LiDAR センサー自身が発するレーザー光を正確に追跡することが可能となり、110m 以上離れた場所からでも車両に搭載された小さなセンサーを追跡できるようになりました。さらに、精密なサーボモーターと制御アルゴリズムにより、移動する標的に対して 0.1 度以下の精度で照準を合わせることが可能になりました。

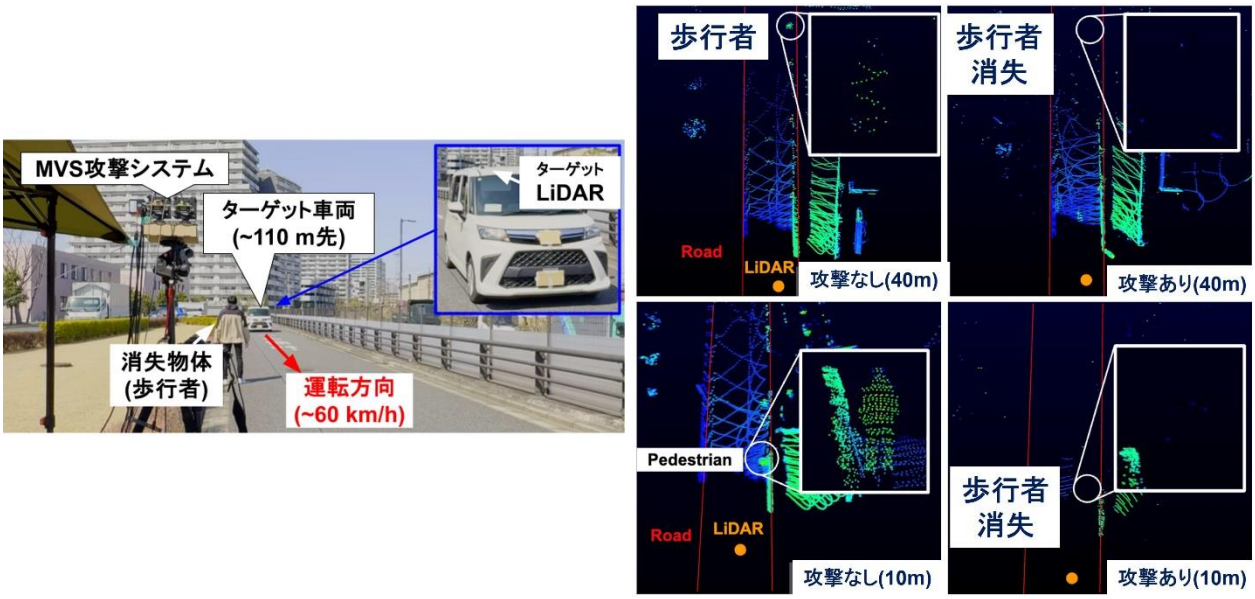
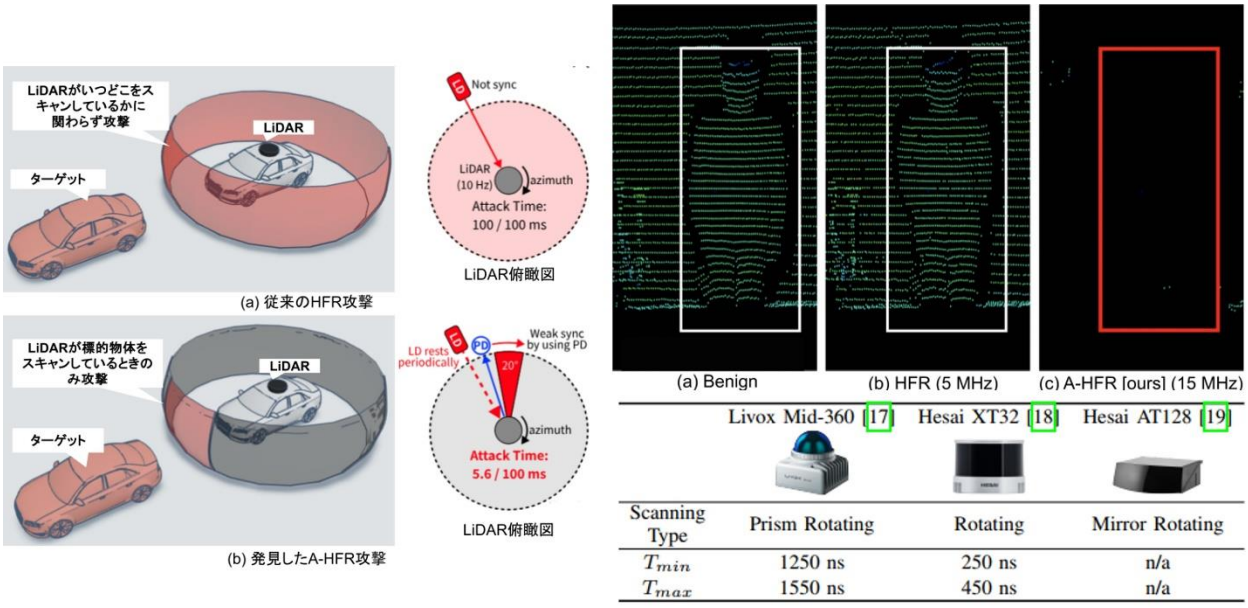


図 2： 高速走行車両への攻撃実験結果

図 2 に示す実験では、管理された実験用コースで実車に LiDAR センサーを搭載し、走行時の攻撃性能を観測しました。60km/h で走行する車両に対して、110m 離れた地点から攻撃を行いました。その結果、攻撃開始地点の 110m から車両の制動ブレーキ距離である 20m の地点までの広範囲にわたって、平均して 96%の歩行者を構成する LiDAR 点群データを消失させることに成功しました。この高い消失率は、走行中のほとんどの期間で自動運転システムが歩行者を見落とす可能性があることを意味します。実際の交通環境でこのような攻撃が行われた場合、自動運転車が歩行者を検知できず、重大な事故につながる危険性があることを示唆しています。



Scanning Type	Livox Mid-360 [17]	Hesai XT32 [18]	Hesai AT128 [19]
	Prism Rotating	Rotating	Mirror Rotating
T_{min}	1250 ns	250 ns	n/a
T_{max}	1550 ns	450 ns	n/a

図 3： 発見した Adaptive High-Frequency Removal （A-HFR）攻撃と実験に用いた LiDAR センサー

次に、A-HFR 攻撃の発見と実装により、最新の LiDAR センサーに搭載されている防御機構（Pulse Fingerprinting 機構）を回避する新たな攻撃手法を発見しました。この攻撃は、LiDAR のスキャンパターンを分析し、そのパターンに適応して高周波のレーザーパルスを生成します。従来の防御機構が想定していない高周波（最大 24MHz）で攻撃レーザーパルスを照射することで、防御機構を回避することが可能になりました。A-HFR 攻撃は、複数の防御機構を備える LiDAR モデルに対しても強力な消失攻撃に成功しました。（図 3）

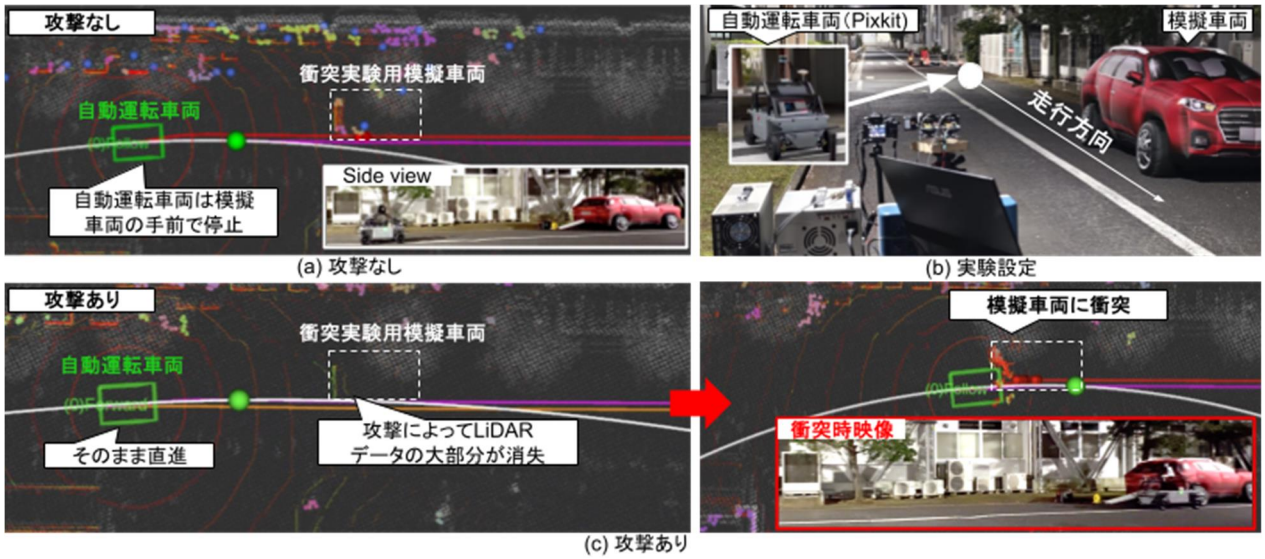


図 4： LiDAR 点群を消失させる攻撃により、自動運転車に対し衝突事故を誘発

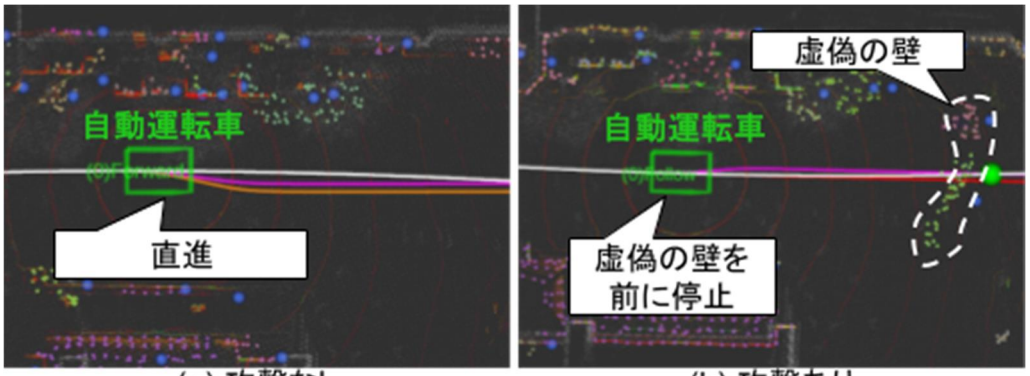


図 5： 虚偽の壁を注入する攻撃により、自動運転車に対しブレーキを誘発

最後に、実際の自動運転車を用いた実証実験に世界で初めて成功しました。オープンソースの自動運転スタック「Autoware」を搭載した自動運転車両（Pixkit）を使用し、管理された実験用コースで様々な攻撃シナリオを検証しました。まず図 4 の LiDAR 点群を消失させる攻撃では、前方の停止車両を LiDAR のデータから消去することで、自動運転車が障害物を認識できず衝突を誘発可能であることを確認しました。また存在しない物体を注入する攻撃では、虚偽の“壁”を注入することで、自動運転車にブレーキを誘発させることができました（図 5）。このような LiDAR センサーへの攻撃により、自動運転システムの意思決定プロセスに深刻な混乱を引き起こすことが可能であることを初めて実証しました。

4. 今後の展開

本研究成果は、多種多様の LiDAR センサーに対する脆弱性についての新たな知見を提供し、既存の LiDAR セキュリティの認識に新たな視点を加えました。今後、本研究グループは今回明らかにした脆弱性に対抗するための防御策の開発に注力します。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ます。また本研究成果は、コンピュータセキュリティシンポジウム（CSS）が定める倫理的配慮のためのチェックリスト※2 に従い、脆弱性をあらかじめ LiDAR メーカー及び自動運転車メーカーに通知し、一定の対策期間を経て公開しています。

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します。これらの多様なセンサーを組み合わせることで、一部のセンサーが攻撃を受けた場合でも全体の安全性を維持することが可能となると期待されます。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します。

5. 本プロジェクトについて

本研究は、科学技術振興機構（JST） 戦略的創造研究推進事業 さきがけ「社会変革に向けた ICT 基盤強化（JPMJPR22PA）」および戦略的創造研究推進事業 CREST「基礎理論とシステム基盤技術の融合による Society 5.0 のための基盤ソフトウェアの創出（JPMJCR23M4）」の一環として行われました。

＜参考文献＞

[1] Yulong Cao *et al.*, *You Can’t See Me: Physical Removal Attacks on LiDAR-based*

Autonomous Vehicles Driving Frameworks, Usenix Security’23
[2] Yulong Cao *et al., Adversarial sensor attack on lidar-based perception in autonomous driving,* ACM CCS’19
[3] Takami Sato *et al., LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies,* NDSS’24.

＜原論文情報＞
国際学会名：NDSS Symposium 2025
タイトル：*On the Realism of LiDAR Spoofing Attacks against Autonomous Driving Vehicle at High Speed and Long Distance*
著者と所属：Takami Sato[1*], Ryo Suzuki[2*], Yuki Hayakawa[2*], Kazuma Ikeda[2], Ozora Sako[2], Rokuto Nagata[2], Ryo Yoshida[2], Qi Alfred Chen[1], Kentaro Yoshioka[2]
*: 共同第一著者　1: University of California, Irvine、2: Keio University
掲 載 URL ： https://www.ndss-symposium.org/ndss-paper/on-the-realism-of-lidar-spoofing-attacks-against-autonomous-driving-vehicle-at-high-speed-and-long-distance/
プロジェクトページ：https://sites.google.com/keio.jp/keio-csg/projects/AttackonDrivingVehicle

＜用語説明＞
※1 LiDAR センサー：Light Detection And Ranging の略で、レーザー光を用いて幅広い範囲の 3D 情報を得るセンサー。野外、遠距離でも動作することから自動運転における主要センサーとして注目されている。
※2 コンピュータセキュリティシンポジウム（CSS）が定める倫理的配慮のためのチェックリスト：https://www.iwsec.org/css/2022/ethics_list.html

・研究内容についてのお問い合わせ先
慶應義塾大学 理工学部 電気情報工学科　専任講師　吉岡　健太郎（よしおか　けんたろう）
E-mail：kyoshioka47[at]keio.jp

・本リリースの配信元
慶應義塾広報室（望月）
TEL：03-5427-1541　FAX：03-5441-7640
E-mail：m-pr[at]adst.keio.ac.jp　https://www.keio.ac.jp/

・科学技術振興機構 広報課
TEL：03-5214-8404　FAX：03-5214-8432
E-mail：jstkoho[at]jst.go.jp

・JST 事業に関すること
科学技術振興機構 戦略研究推進部 ICT グループ　前田　さち子（まえだ　さちこ）
TEL：03-3512-3526　FAX：03-3222-2066
E-mail：presto[at]jst.go.jp