# LiDAR センサ幻惑攻撃の実世界実証研究

慶応義塾大学　理工学研究科電気電子工学専攻
吉岡　健太郎

## 1　研究目的

自動運転社会への変革によって交通事故被害者を大幅に減らす事が期待されている。一方で自動運転車が備えるセンサに攻撃することで自動運転システムを騙す新たなセキュリティ危機が生まれた。中でも自動運転車の中核的センサである Light Detection and Ranging(LiDAR)の脆弱性を突き攻撃レーザにより虚偽データを注入するセンサ幻惑攻撃は自動運転社会の重大な脅威となる（図1）。脅威の一例として自動運転車の眼前に突如壁が現れたと誤認させ、急ブレーキを誘発させ搭乗者に被害を与える攻撃が想定される。こういった事件が一度でも起きると自動運転に対する社会的信頼は失墜する。本研究の目的は LiDAR センサを備えた自動運転車に対するセンサ幻惑の脅威を取り去るため、センサ幻惑攻撃に対するセキュリティ研究を実施することである。

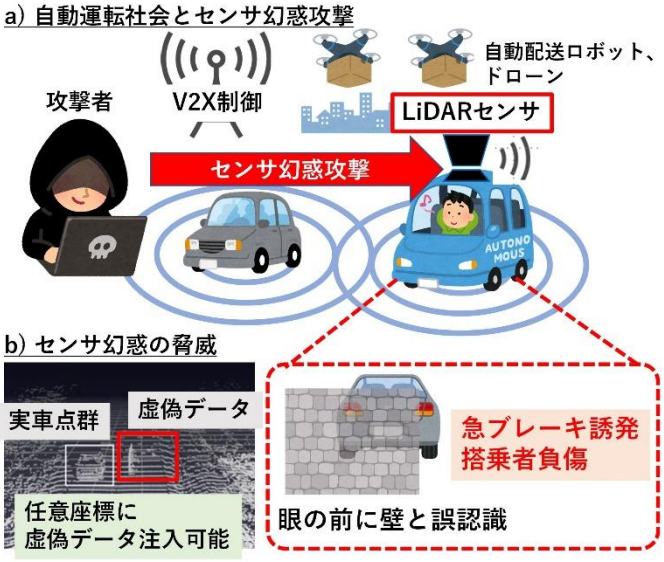


図 1 センサ幻惑攻撃の脅威

一方で従来の LiDAR セキュリティー研究では、1)調査している LiDAR センサーが初期世代の LiDAR(VLP-16)1 種類のみである、2)理論的には任意の偽装データの注入が可能とされていたが、実験による実証は行われていない、という 2 つの大きな問題があった。 これらの問題 は、LiDAR への攻撃能力と自動運転システムへの影響について、不完全・不正確な理解を引き起こす可能性がある。

## 2 研究成果

我々は LiDAR センサーセキュリティーをより深く理解するため、潜在的な脅威に対する初めての網羅的なセキュリティー調査を実施した。特に、攻撃者が偽装データを注入したり、物体を消去したりする可能性に焦点を当てている。具体的には図 2 に示す通り、新旧あわせて 9 種類の LiDAR センサーを用いた大規模な脆弱性調査を行い、特に次世代 LiDAR は、旧世代の LiDAR とは異なる LiDAR 攻撃に対する脆弱性特性を持つことを発見した。最たる例として、従来研究では攻撃手法が LiDAR のレーザー発射周期と同期し、攻撃用レーザーを照射する同期攻撃と呼ばれるものが主流であった。一方、次世代 LiDAR はレーザ

一発射タイミングのランダム化といった干渉回避機能を備えており、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。

また、本研究グループは初期世代の LiDAR に対して、同期攻撃により精微な偽装物体の注入攻撃が可能であることを示した（図 3 中の"KEIO CSG"といった文字に示す）。従来ではこのような偽装データの制御は難しかったものの、攻撃レーザー装置の改良によって可能となりました。このように攻撃能力を明らかにすることにより、本質的な防御策が立てられるようになると考えている。

| | | Velodyne | | | Ouster | Hesai | Robosense | Livox | Intel | Leddar |
|---|---|---|---|---|---|---|---|---|---|---|
| | |  VLP-16 [16] |  VLP-32c [19] |  VLS-128 [40] |  OS1-32 [23] |  XT32 [25] |  Helios 5515 [24] |  Horizon [41] |  Realsense L515 [42] |  Pixell [43] |
| General Specs | Gen. (year) | 1st-G (2016) | 1st-G (2017) | 1st-G (2017) | New-G (2019) | New-G (2020) | New-G (2021) | New-G (2020) | New-G (2019) | New-G (2019) |
| | Scanning Type | Rotating | Rotating | Rotating | Rotating | Rotating | Rotating | MEMS | MEMS | Flash |
| | Wavelength | 905 nm | 905 nm | 905 nm | 865 nm | 905 nm | 905 nm | 905 nm | 860 nm | 905 nm |
| | Vertical FOV | 30° | 40° | 40° | 45° | 31° | 70° | 25.1° | 55° | 16° |
| | Horizontal FOV | 360° | 360° | 360° | 360° | 360° | 360° | 81.7° | 70° | 180° |
| | Max. Range [m] | 100 | 200 | 300 | 120 | 120 | 150 | 260 | 9 | 56 |
| | Min. Range [m] | 1 | 1 | 0.5 | 0.3 | 0 | 0.2 | 0.5 | 0.25 | 0.1 |
| | Vertical Channel | 16 | 32 | 128 | 32 | 32 | 32 | - | - | 8 |
| Security | Simul. Firing | 1 | 2 | 8 | 32 | 1 | 1 | 1 | 1 | 3 |
| | Timing Random. | | | | ✔ | | ✔ | ✔ | ✔ | ✔ |
| | Fingerprinting | | | | | ✔ | | | | |

**図 2 網羅的な脆弱性調査**

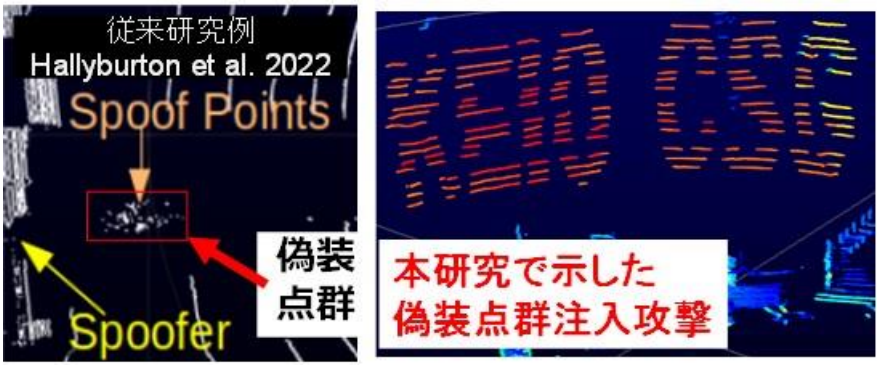


**図 3： 偽装データ注入攻撃の実証**

さらに我々は次世代 LiDAR にも有効な新たな攻撃手法の存在を明らかにし、「HFR（高周波レーザー除去）攻撃」と名付けた（図 4）。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 の計測を妨害させ、物体を消去する攻撃である。HFR 攻撃は LiDAR との同期化を必要としない非同期的な攻撃手法であり、幅広い次世代 LiDAR に対しても有効だ。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り、攻撃適用範囲も広いという特徴がある。図 4 の下部に示す通り、太陽光が多く攻撃難度が高い真夏の野外での実験でも、80 度以上の水平範囲の物体を消失させることに成功した。

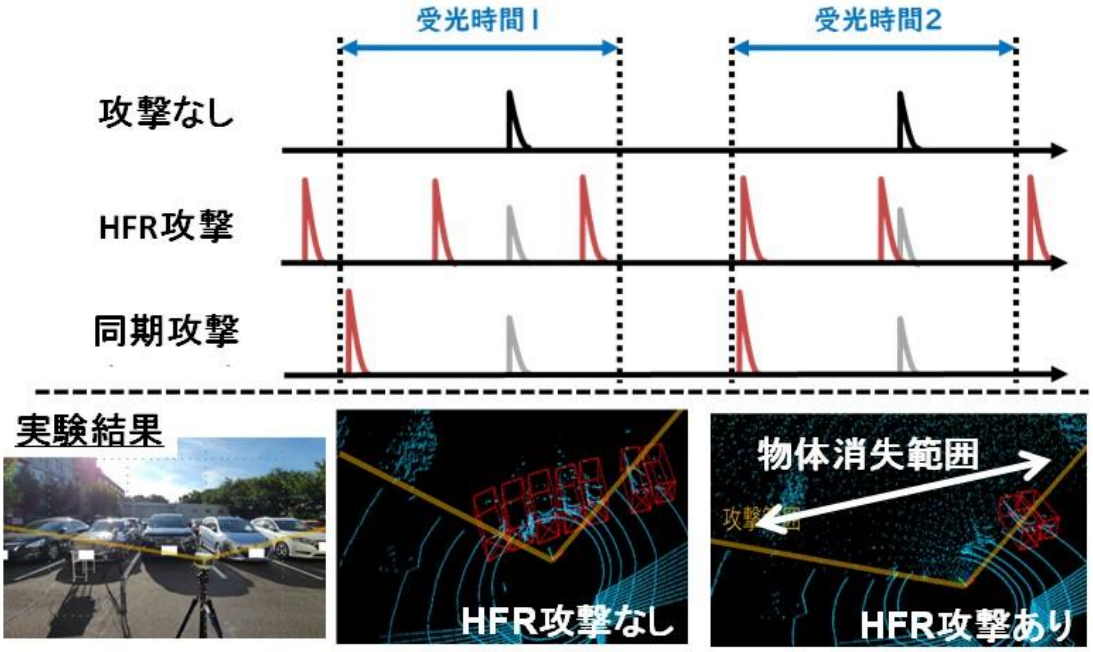


図 4 HFR 攻撃とその効果

### 3. 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理解を提供し、既存の LiDAR セキュリティーの認識に新たな視点を加えた。今後、本研究グループは本研究で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。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に従い、脆弱性をあらかじめ LiDAR メーカーに通知し、一定の対策期間を経て公開している。

さらに、研究の進行として、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。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。

### ４．まとめ

本研究では、自動運転車両に搭載された LiDAR センサーに対する新たな脆弱性を発見し、センサ幻惑攻撃の脅威を明らかにした。特に、次世代 LiDAR に対する非同期攻撃手法であ

る「HFR 攻撃」を提案し、その有効性を実証した。これらの成果は、LiDAR セキュリティーに関する従来の理解を深化させ、新たな視点を提供するものである。

本研究グループは、今後、明らかになった脆弱性に対する防御策の開発に注力する。LiDAR センサーの耐性向上や、偽装データ注入を防ぐアルゴリズムの開発などを進める予定だ。さらに、レーダーやカメラなど他のセンサーとの組み合わせによる安全性向上の可能性も探求する。

本研究成果は、倫理的配慮に基づき、LiDAR メーカーへの事前通知と一定の対策期間を経て公開された。最終的に、この研究が自動運転車両のセキュリティー強化と、社会全体への安心・安全の提供に貢献することを目指している。