プレスリリース

2024 年 2 月 13 日

慶應義塾大学
科学技術振興機構（JST）

自動運転用 LiDAR センサーに対する網羅的セキュリティー調査を世界で初めて実施

ー新たな脆弱性を発見し有効な防御策開発へ道ー

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。早期段階で脆弱性を特定し、それらを解消することが求められています。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らは、カル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、同校博士課程学生の佐藤貴海と共同で、自動運転用のセンサーが持つ脆弱性に焦点を当てた初めての網羅的セキュリティー調査を実施し、どのような対抗策が必要か明らかにしました。

本研究では新旧あわせて 9 種類の LiDAR センサーに対する網羅的な脆弱性調査を行い、新たな攻撃手法「HFR（高周波レーザー除去）攻撃」の実用性を実証しました。その結果、さまざまな種類の 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ー問題に新たな警鐘を鳴らすとともに、その防御策の開発につながる大きな一歩として、自動運転の安全性向上が期待できます。

本研究成果は、2024 年 2 月 26 日（米国太平洋時間）から始まるセキュリティー分野のトップ国際会議「Network and Distributed System Security（NDSS）」に採択され、論文が掲載されました。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

・**新しい脆弱性の発見：**自動車の LiDAR※1 センサーが悪意ある攻撃者によって操作される新しい脆弱性を明らかにしました。高周波レーザーを攻撃者がセンサーに照射することで、センサー上で広範囲の物体を消去したり、偽装データを注入したりするような攻撃が可能です。この攻撃は最新の LiDAR にも有効で、既存の安全対策が必ずしも有効でないことを示しています。

・**大規模な計測研究：**9 種類の LiDAR と 3 種類の主要な物体検出器※2 に対する大規模な測定研究を初めて行いました。これにより、センサーがどの程度攻撃に対して脆弱であるか、または安全であるかの評価を明らかにしました。

・**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ー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

現代の自動車、特に自動運転車両の開発において、LiDAR センサーは中核的役割を担っています。LiDAR は車両の周囲環境を精密に探知し、物体との距離を高精度に測定することで、自動運転の安全性を大いに向上させます。

しかしながら、LiDAR の脆弱性を突き、攻撃レーザーにより虚偽データを注入する新たなセキュリティー課題も生じています。悪意ある攻撃者が LiDAR をだますことで、存在しない物体を偽装することが可能になり、自動運転車両の安全性が大きく脅かされる可能性があります。この問題を克服するためには、LiDAR の脆弱性を徹底的に分析し、これらの潜在的な脅威に対抗するための効果的な対策を見つけることが急務となっています。

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りました。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ります。

3. 研究内容・成果

		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 1： 実施した網羅的な脆弱性調査

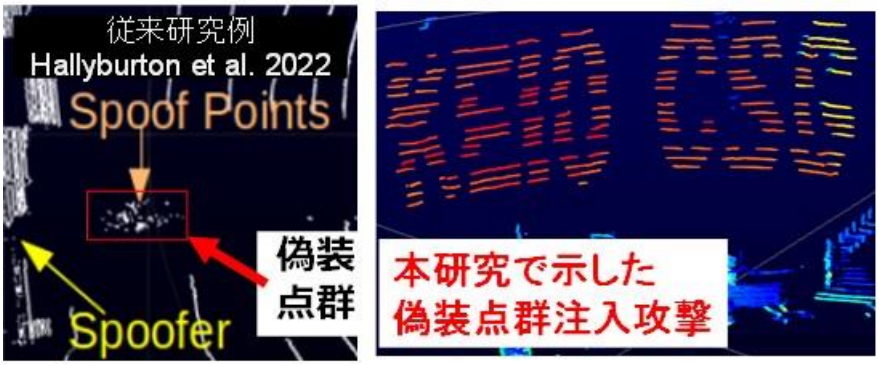

図 2： 偽装データ注入攻撃の実証

本研究グループは 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ました。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ます。具体的には図 1 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※3 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ました。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

主流でした[1,2]。一方、次世代 LiDAR 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ました。

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ました（図 2 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ります。

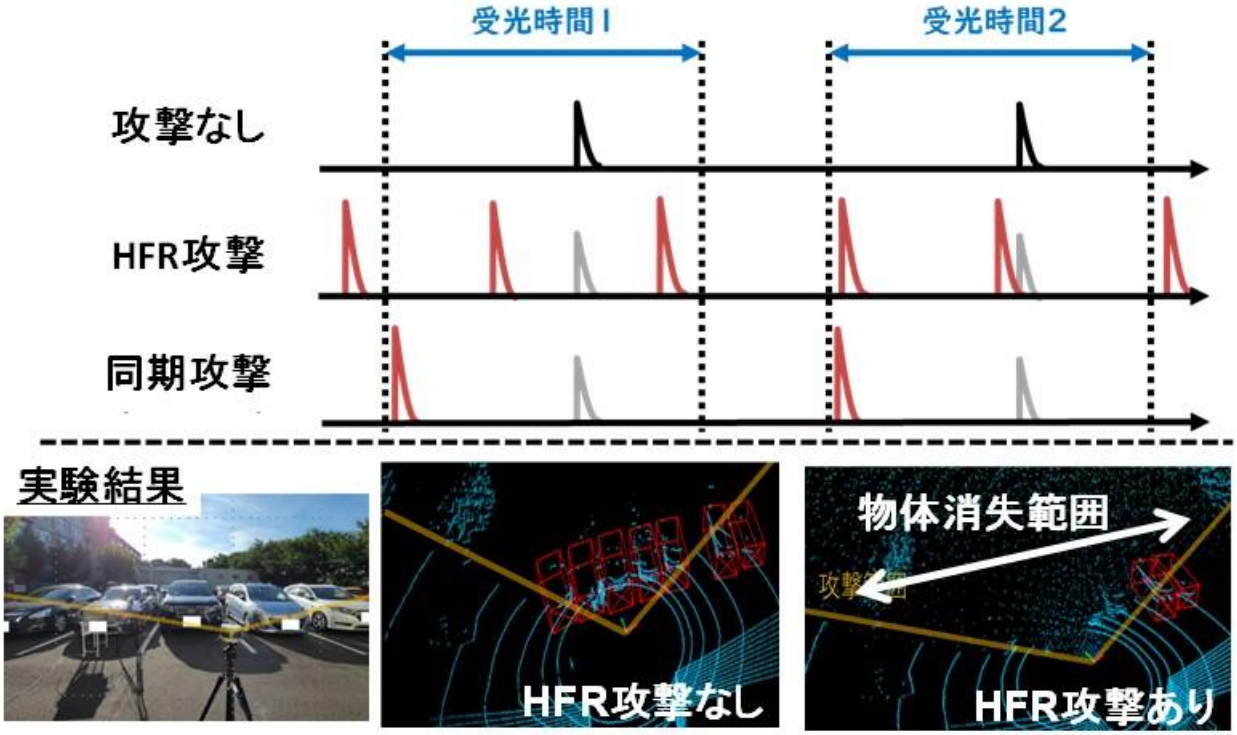

図 3： HFR 攻撃の特徴と実験結果

さらに、本研究グループは次世代 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」と名付けました（図 3）。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す。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、さまざまな種類の次世代 LiDAR に対しても有効です。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ります。図 3 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ました。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る予定です。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※4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ます。

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)」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

＜原論文情報＞

国際学会名：NDSS Symposium 2024

タイトル：*LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies*

著者と所属：Takami Sato[1*], Yuki Hayakawa[2*], Ryo Suzuki[2*], Yohsuke Shiiki[2*], Kentaro Yoshioka[2], Qi Alfred Chen[1]

*: 共同第一著者

1: University of California, Irvine

2: Keio University

＜用語説明＞

※1 LiDAR：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 物体検出器：主に 3D 空間上の点群データから特定の物体や形状を識別、検出するための技術。自動運転車両では、例えば人や車といった物体を検出するために用いられる。

※3 次世代 LiDAR：システムオンチップ（SoC）と呼ばれるアプローチを用いて、光検出器や読み出し回路などの全てのコンポーネントを単一のチップに搭載する、新しいタイプの LiDAR。このアプローチにより、LiDAR はコストを低減しながらレーザー発射タイミングのランダム化といった複雑な測定機能の搭載を可能にする。

※4 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