

【ロボット・AI 技術分野】

仮訳

自動運転車の安全性の欠陥に光を当てる(米国)

「ステッカー攻撃」実行のコストと難易度の低さを実証

2025 年 3 月 4 日

著者： Brian Bell



カリフォルニア大学アーバイン校(UC Irvine) Donald Bren School of Information & Computer Sciences の研究者らが、自動運転車の交通標識認識(TSR)システムには存在しない道路標識を認識させられたり、実際の道路標識を見落とさせられたりする恐れがあり、異常で危険性の高い運転につながる可能性があることを実証した。

2025 年 3 月 4 日 カリフォルニア州アーバイン — カリフォルニア大学アーバイン校 (UC Irvine) の研究者らが、停止や速度制限の道路標識に貼られた多色ステッカーが自動運転車を混乱させ、予測不可能で危険な運転を引き起こせることを実証した。

先般サンディエゴで開催された [Network and Distributed System Security \(NDSS\) Symposium](#) での [プレゼンテーション](#) にて、UC Irvine の Donald Bren School of Information & Computer Sciences の研究者らは、これまでは仮説とされていた、安価で容易に利用可能な悪意ある攻撃が、自動運転車の AI アルゴリズムによる道路標識

の検出を不可能にしたり、あるはずのない標識を表示させたりする可能性について説明している。どちらの攻撃であっても、自動運転車による道路標識の無視、意図しない緊急停止やスピード違反等を引き起こす可能性がある。

最も代表的な 3 パターンの AI 攻撃設計を含んだ今回の研究は、トップセラーブランドの自動運転車での交通標識認識(TSR)システムに関する初めての大規模な調査であると研究者らは言う。

「Waymo は毎週 150,000 件以上の自動運転サービスを提供し、道路にはオートパイロットを装備した何百万台もの特斯拉車が走っています。自動運転技術は、米国や世界の日常生活の不可欠な部分になりつつあるのです」と、UC Irvine のコンピューターサイエンス准教授で本研究論文の共著者の [Alfred Chen](#) 氏は言う。「これらのシステムの脆弱性が悪用されると、生死に関わる安全上の危険につながる可能性があるため、セキュリティの重要性が注視されています」。

UC Irvine コンピューターサイエンスの博士課程の学生として本研究を実施した、本研究論文の第一著者で Meta のリサーチサイエンティストである Ningfei Wang 氏は、研究チームが選択した攻撃ベクトルは、自動運転車による道路標識の認識に使用される AI アルゴリズムを混乱させる、多色の渦巻いたデザインのステッカーであると説明する。

「これらのステッカーは、Python や画像処理ライブラリ等のオープンソースプログラミング言語にアクセスできれば誰でも安く簡単に作ることができます」と Wang 氏は言う。「これらのツールにグラフィックカード付きのコンピューターとカラープリンターを組み合わせるだけで、自動運転車の TSR システムによる認識を失敗させることができます」。

Wang 氏はまた、本研究プロジェクトでの興味深い発見は、現行の商用 TSR システムの多くに共通する空間的記憶設計の関与であると付け加える。この設計は、隠蔽攻撃(車両の視界から標識が取り除かれるように見せる)には効果がある一方で、偽造された停止標識による攻撃を「予想以上に容易にしている」と説明する。

Chen 准教授は、今回の研究は、現実世界のシナリオにおける商用車両へのセキュリティの脅威について初めて調査したものであると指摘する。

「学会は自動運転車のセキュリティについて長らく研究しており、最先端の自動運転技術のセキュリティにおいて実際の様々な脆弱性を発見してきました」と Chen 准教授は言う。「しかし、これらの研究は主に理論的な設定に限定されており、商用自動運転車システムでのこのような脆弱性への理解を非常に制限しています。私たちの研究は、このような非常に重要なギャップを埋めるものです」。

この分野におけるこれまでの研究のうちの小さな領域に焦点を当てることにより、同准教授の研究グループは、無効となった仮説、不正確さや虚偽の主張を明らかにすることができたと Chen 准教授は説明する。例えば、これまでの学術研究では、商用 TSR システムにおける空間的記憶設計の共通的な存在を認識することがなかった。Chen 准教授の研究チームのメンバーは、以前に開発した学術研究設定でこの設計をモデル化した際に、最先端の研究コミュニティによる初期の報告と主張に直接的な疑問を投げかける結果を明らかにした。

「今回の研究は始まりに過ぎないと考えています。そして、学界と産業界のより多くの研究者が、現実世界の自動運転車に対するこのような種類のセキュリティの脅威による実際の影響と重要性を体系的に再考察することを願っています」と Chen 准教授は言う。「このことは、私たちの街路や高速道路での安全性の確保に向けた行動の必要性を、社会的なレベルで実際に理解するために不可欠な最初の一步となります」。

Chen 准教授と Wang 氏に加え、本研究プロジェクトには、元 UC Irvine の大学院生 Takami Sato 氏と Yunpeng Luo 氏、UC Irvine 大学院生 Shaoyuan Xie 氏、ドレクセル大学のコンピューターサイエンスの Kaidi Xu 准教授が含まれる。本研究は、米国立科学財団(NSF)と UC Irvine が会員として所属する、米国運輸の CARMEN + University Transportation Center が支援した。

訳：NEDO（担当 イノベーション戦略センター）

出典：本資料は、米カリフォルニア大学アーバイン校(UCI)の記事 “UC Irvine study shines headlights on consumer driverless vehicle safety deficiencies”

(<https://news.uci.edu/2025/03/04/uc-irvine-study-shines-headlights-on-consumer-driverless-vehicle-safety-deficiencies/>) を翻訳したものである。

(Reprinted with permission of the University of California, Irvine)