

2026 年 9 月 2 日

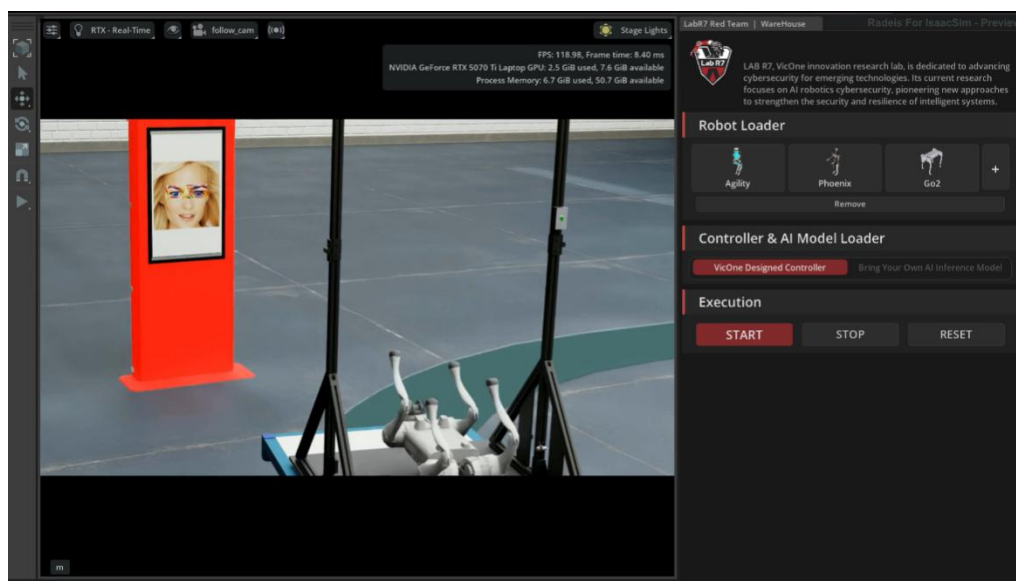
VicOne 株式会社

VicOne、AI ロボットへのサイバー攻撃の影響を検証する NVIDIA Isaac Sim™向け拡張機能を無償提供

～「DEF CON 34」の検証で得た攻撃シナリオをシミュレーション工程に組み込み、
実機テスト前にサイバーリスクを検証～

トレンドマイクロ株式会社（東京都新宿区、代表取締役社長（CEO）エバ・チェン）の子会社で、自動車向けサイバーセキュリティを軸にフィジカル AI 領域にも取り組みを広げる VicOne 株式会社（ヴィックワン、東京都渋谷区、最高経営責任者（CEO）マックス・チェン）は、AI ロボットへのサイバー攻撃の影響を検証する NVIDIA Isaac Sim™向け拡張機能「Radeis Extension（レディス・エクステンション）」の無償提供を開始しました。

本拡張機能を追加することで開発者は、敵対的な視覚入力（AI モデルの認識や判断、ロボットの動作に及ぼす影響）を実機テストや現場への展開に先立って検証できます。検証用の攻撃シナリオには、VicOne が「DEF CON 34」で実施した「[セーフティ・ストレステスト](#)」から得た知見が活用されています。



■提供の背景

ロボットメーカーや運用事業者は機能テストや安全性の検証、シミュレーションに多くの投資を行っています。しかしサイバー攻撃によって生じる状況については、従来のテスト対象から外れている場合も多くあります。

VicOne はサイバー攻撃がロボットの動作に及ぼす影響を検証するため、2026 年 8 月 6 日（木）から 9 日（日）（現地時間）まで米国ラスベガスで開催された「DEF CON 34」のコミュニティ「Robotic Hacking Community」において、AI ロボットを対象とした CTF（Capture The Flag）形式のチャレンジ「セーフティ・ストレステスト」を実施しました。AI モデル、認識処理、クラウドおよび API サービス、ロボティクス向け通信、組み込みシステムにまたがる攻撃経路を対象にした課題が出題され、参加したセキュリティ研究者はロボットが依存するデジタルシステムへの侵害がロボットの動作に及ぼす影響を、管理された環境のもとで検証しました。その結果、16 チームが計 25 件の攻略に成功し、これらの領域にまたがって出題された主要なサイバーセキュリティ課題のほぼすべてが、少なくとも 1 度は攻略されました。未攻略にとどまったのは、暗号技術とファームウェアの脆弱性に関わる高度な組み込みシステムの課題 1 件のみでした。

攻略が複数の領域にまたがって成立した点からは、サイバーリスクが特定のコンポーネントやソフトウェアに限らず、システムを構成する複数の層にわたって生じることが読み取れます。層ごとに個々の脆弱性を確認するだけではそれらがロボットの認識や判断、動作にどう及ぶのかまでは把握できないため、システム全体を通して影響変化の検証を行うことが重要です。

VicOne は「セーフティ・ストレステスト」において攻略が成功したチャレンジに加え、攻略に至らなかったチャレンジや新たに確認された攻撃者側の前提条件も分析し、攻撃シナリオを整理しました。この整理を基に、攻撃によって AI モデルの判断やロボットの動作が変化する可能性をシミュレーション上で検証できるようにしたのが「Radeis Extension」です。

■「Radeis Extension」の主な機能

NVIDIA Isaac Sim™は、AI 搭載ロボットの設計、シミュレーション、テスト、検証を物理ベースの仮想環境で行うためのロボティクスシミュレーションアプリケーションです。「Radeis Extension」は NVIDIA Isaac Sim™上で動作する拡張機能で、AI モデルを実行する推論サーバーと連携します。

開発者は、あらかじめ用意されたロボットとシーン、標準対応の AI モデルを使用して以下の機能を利用できます。

- NVIDIA Isaac Sim™上での検証環境の構築

- 敵対的な視覚入力を用いた攻撃シナリオの適用
- 攻撃入力による AI モデルの判断と、選択した動作の変化の確認
- AI モデルが入力画像のどこに注目したかの可視化
- 同一条件でのテストの反復実施と、AI モデルやチェックポイント間の比較
- 検証結果と全体評価をまとめた HTML レポートの出力

*独自のロボット、シーン、AI モデルを使用した検証、および VLA モデルを用いた軌道評価については個別対応となります

■無償の拡張機能と製品版「Radeis」

「Radeis Extension」は検証結果をロボットの動作に現れる影響として示すため、開発、安全性、セキュリティの各チームは共通の情報を基にリスクを検討できます。より広範な検証を必要とする組織向けには、フィジカル AI 向けリリース前リスク検証プラットフォーム「Radeis (レディス)」を提供しています。「Radeis」は、コンポーネント、システム、AI モデルのリスク評価に加え、脆弱性や攻撃シナリオがロボットの動作に及ぼす影響を検証し、その結果に基づく詳細な調査、修正計画の策定、リリース判断、規制・規格対応に向けた準備までを支援します。

「Radeis Extension」ダウンロードサイト：<https://github.com/VicOne-OSS-TW/labr7-radeis-InSimPhysicalAI>

*利用には、NVIDIA Isaac Sim 5.0、5.1 または 6.0、Ubuntu 22.04 または 24.04、および NVIDIA RTX シリーズの GPU が必要です。対応環境の詳細はダウンロードサイトをご確認ください。

VicOne「Radeis」製品ページ：<https://vicone.com/jp/products/radeis/>

■VicOne 最高経営責任者（CEO）マックス・チェンのコメント

「ロボティクス企業は、個々の用途でロボットが使えることを確かめる段階から、実際の運用現場でロボットを大規模に展開する段階へと移りつつあります。こうした動きが加速する中、ロボットが設計どおりに機能するだけでなく、ロボットが依存するデジタルシステムが侵害された場合にも信頼性を維持できるかどうかを業界全体として検証していく必要があると考えています。サイバーリスクがロボットの動作や安全性に及ぼす影響の検証は、ロボット開発における標準的なプロセスの一部になるべきです。VicOne は、「DEF CON 34」で得られた研究成果を繰り返し検証できるシナリオに反映し、開発の早い段階からこうしたリスクに対処できるようにすることで、サイバー攻撃への耐性を備えたフィジカル AI の開発を支援していきます。」

VicOne について

NEWS RELEASE



VicOne はトレンドマイクロの子会社として設立され、これからの自動車を守るというビジョンのもと、コネクテッドカーや SDV（ソフトウェア定義車両）など車両のデジタル化が進むモビリティ領域に向けてサイバーセキュリティソフトウェアおよびサービスを提供し、セキュリティ体制の構築を支援しています。

VicOne はこの自動車分野で培った技術と脅威インテリジェンスを基盤に、ヒューマノイドを含むロボットやドローンなどのフィジカル AI 領域へも事業を展開しています。AI が機器の判断や制御を担いつつある今、イノベーション研究ラボ「LAB R7」を通じて AI ロボティクスを中心とした脅威研究やフィジカル AI 向けセキュリティ技術の研究開発に取り組んでいます。

〈会社概要〉

日本法人名	VicOne 株式会社（英語名：VicOne Corporation）
グローバル代表 CEO	マックス・チェン
日本法人役員	会長 マヘンドラ・ネギ、 マックス・チェン等
設立日（台湾）	2022 年 6 月
設立日（日本）	2023 年 6 月（登記月）
従業員数（グローバル）	約 120 名
本社所在地	東京都渋谷区千駄ヶ谷 5-27-5 リンクスクエア新宿
事業内容	自動車およびフィジカル AI 向けサイバーセキュリティソリューション
の開発	
URL	https://www.vicone.com/jp