NEWS RELEASE

2026 年 7 月 13 日
VicOne 株式会社

VicOne、「DEF CON 34」でロボット・フィジカル AI 領域の セキュリティコミュニティ「Robotic Hacking Community」を立ち上げ

～CTF 形式のチャレンジで AI ロボットに対する攻撃シナリオを再現し、サイバーリスクが安全性に及ぼす影響を検証～

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、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る世界最大級のハッカーカンファレンス「DEF CON 34」において、コミュニティ「Robotic Hacking Community（以下 RHC)」を立ち上げます。

RHC は、ロボットとフィジカル AI のセキュリティをテーマとするコミュニティです。VicOne は、2025 年に設立したイノベーション研究ラボ「LAB R7」で進めるフィジカル AI 領域の脅威研究

を起点に、研究者、開発者、セキュリティリサーチャーがロボットの認識、判断、動作に関わるセキュリティ課題を検証・共有できる場として、RHC を企画・運営します。

RHC では、ハンズオン形式のワークショップや研究発表に加え、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」を主要コンテンツとして予定しています。同チャレンジでは、参加者がデジタルツイン環境にチャレンジ API を通じてアクセスし、攻撃と防御の両面からロボティクスセキュリティを実践的に学ぶことができます。

■広がるフィジカル AI と複雑化する安全性リスク

ロボット、ドローン、ヒューマノイドなどに代表されるフィジカル AI は近年、管理されたデモ環境から工場、倉庫、公共空間、現場業務へと活用の場を広げています。こうしたシステムは機械設計や制御ロジックだけでなく、センサー、API、ファームウェア、AI モデル、クラウド接続サービスなど多様な要素に依存するようになっており、従来の機械的な故障だけでは説明できない安全性リスクが広がっています。機械部品が故障していなくても誤った指示に従う、改ざんされた AI モデルを信頼する、意図しない制御経路が実行されるといった形で AI ロボットの認識、判断、動作に影響が及ぶ可能性があります。

「LAB R7」は過去 18 か月の間に、フィジカル AI 領域における 20 件以上の公開済みセキュリティインシデントおよび脆弱性情報を確認しており、ロボットの自律化、ネットワーク化、AI 化が進むことでアタックサーフェス（攻撃対象領域）が急速に拡大していることを明らかにしています。

■サイバーリスクを 6 つの領域で検証

RHC の主要コンテンツとなる「セーフティ・ストレステスト」は、フィジカル AI を取り巻く新たな安全性リスクを、管理されたデジタルツイン環境で検証するために開発されました。参加者は、デジタルツイン上に再現されたロボットを対象にミッションを解き進める CTF 形式を通じて、サイバー攻撃がロボットの認識、判断、動作に及ぼす影響を体験できます。

想定される攻撃シナリオは、安全性に関わる 6 つの領域に分けてミッション化しています。

- AI ロボットの推論を狙うプロンプトインジェクション
- タスク実行の挙動を改変する、汚染された AI ポリシーモデル（Poisoned AI Policy Models）
- AI ロボットの認識を欺く敵対的な視覚入力（Adversarial Visual Inputs）
- クラウド・API 環境の脆弱性
- ROS 2 や DDS など、ロボティクス向け通信規格の脆弱性
- 組み込みファームウェアの信頼チェーンに関する脆弱性

このテストでは、物理シミュレーションに基づくロボティクスシミュレーター上に構築した Real2Sim デジタルツインを活用し、オープンソースの小型ロボット「Reachy Mini Lite」と、モバイルマニピュレーター「LeKiwi」を再現しています。参加者には、チャレンジ API を通じて個別に分離された実験環境が提供されるため、実機を危険にさらすことなく攻撃シナリオを安全に検証できます。

こうした検証は、メーカーや運用事業者がサイバーリスクを安全性評価の対象に含めるうえでも有効です。メーカーにとっては、製品の安全性評価、導入前テスト、市場投入後のモニタリングで確認すべき観点が広がります。運用事業者にとっても、現場の安全確保、立ち入り制限区域の管理、システム稼働率、インシデント対応、作業員や設備の近くで稼働する AI ロボットへの信頼性を考えるうえで、サイバーリスクを運用上の安全性と結びつけて評価しやすくなります。

VicOne は、新たな攻撃シナリオをデジタルツイン上で繰り返し検証できる形にすることで、自動車向けサイバーセキュリティ、脆弱性研究、サイバーフィジカルリスク評価で培った知見を AI ロボットのセキュリティ強化に活かし、メーカーや運用事業者による安全性評価の拡張に貢献します。

■VicOne 最高経営責任者（CEO）マックス・チェンのコメント

大規模言語モデル（LLM）や視覚言語モデル（VLM）がロボットの「頭脳」として組み込まれるようになると、プロンプトインジェクションは AI が誤った出力を生成するだけの問題ではなく、AI ロボットの誤った動作が人や周囲に影響を及ぼすリスクへと発展します。AI ロボットの安全性は、機械的な信頼性だけで語れるものではありません。フィジカル AI システムが周囲の状況を認識し、推論し、動作するようになるにつれ、サイバーセキュリティは安全性を支える重要な要素となります。

■「Robotic Hacking Community」開催概要

【カンファレンス名】「DEF CON 34」
【会期】2026 年 8 月 6 日（木）～9 日（日）（現地時間）
【会場】ラスベガス・コンベンション・センター（米国ネバダ州ラスベガス）
【コミュニティ名】「Robotic Hacking Community（RHC）」
【RHC 会場】West Hall 4、Level 1、Room 1309
【特設サイト（英語のみ）】https://roboticchackingcommunity.com/
※今回の「セーフティ・ストレステスト」への参加は最大 80 チームまでとなります。

NEWS RELEASE

VicOne について

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、ロボット、ドローン、ヒューマノイドなどのフィジカル 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