NEWS RELEASE

2026 年 3 月 XX 日
VicOne 株式会社

VicOne、フィジカル AI／ロボティクス領域のサイバーセキュリティリスクをテーマにウェビナーを 3 月 25 日に開催

～脅威動向とリスクを解説し、設計・開発から運用までの実践ポイントと VicOne の最新ソリューションを紹介～

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分野のリーディングカンパニーである 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 3 月 25 日（水）13 時より、フィジカル AI およびロボティクス領域における最新のサイバーセキュリティリスク動向と対策をテーマとしたウェビナーを開催します。
本ウェビナーでは、ロボットや自律・自動化機器そして次世代の「フィジカル AI」を守るためのサイバーセキュリティ研究を推進する VicOne のイノベーション研究ラボ「LAB R7」が 2025 年に発表したホワイトペーパーの内容をもとに、AI ロボティクスにおけるサイバーセキュリティリスクとその防御策について解説します。

IoT 社会の進展により、あらゆる機器がインターネットに接続され、私たちの生活を豊かにする反面、サイバー攻撃は高度化・巧妙化しています。特に AI ロボットに代表される「フィジカル AI」は、物流、医療、公共空間など実社会の現場へ急速に浸透しており、その利便性が期待される一方でロボット特有の複雑なアタックサーフェス（攻撃対象領域）が生まれ、新たなリスクを生み出しています。

こうした動向を受け、欧州の「EU AI Act（欧州 AI 法）」に代表されるように、AI の活用にはリスクの程度に応じた厳格な規制が適用され始めており、開発者や運用事業者には設計段階からのリスク対策が求められています。

本ウェビナーでは「LAB R7」が発表したホワイトペーパーを軸に、AI ロボティクスに対するサイバー脅威の最新動向やサプライチェーンに潜むリスクに触れながら攻撃されやすいポイントを整理し、設計・開発から運用までの対策の考え方を解説します。

あわせて、こうした課題認識のもと、VicOne が新たに提供を開始したロボティクスおよびフィジカル AI 向けサイバーセキュリティソリューションについても紹介し、現場での対策検討に役立つ実践的な情報をお届けします。

プログラム／登壇者

本ウェビナーは「LAB R7」の最新研究に基づく「脅威分析」と、現場での対策を実現する「ソリューション紹介」の二部構成でお届けします。

- プログラム 1：『AI ロボットのサイバーセキュリティ最前線：物理的脅威と対策』
  VicOne 株式会社　執行役員　技術統括　原 聖樹

  最新レポートを引用しながら、ロボティクス・システム特有のアタックサーフェスを整理。プロンプトインジェクションやセンサー欺瞞といった最新の攻撃手法を解説し、独自のフレームワーク「Robot Threat Matrix（RTM）」を用いた設計思想をご紹介します。

- プログラム 2：『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 』
  VicOne 株式会社　日本地域代表　カントリーマネージャー　小田 章展

  既存のロボットシステムから次世代機までをカバーする、VicOne の新たなセキュリティソリューションの全体像を、法規制（EU AI Act 等）への対応と併せてご紹介します

ウェビナー概要

【主催】VicOne 株式会社
【日時】2026 年 3 月 25 日（水）13:00～14:00
【形式】Zoom によるオンライン配信
【参加費】無料
【詳細・お申込み】ウェビナーに関する詳細や参加申し込みについては下記 URL をご覧ください。
https://info.vicone.com/ja/mar-2026-webinar

■VicOne「LAB R7」ホワイトペーパー：「AI ロボットのサイバーセキュリティリスクとその対策」
今回のウェビナーでも詳説する本ホワイトペーパーは、AI ロボティクスを取り巻くサイバーリスクとその対策を分析し、AI ロボットや自動化システムにおけるアタックサーフェスを以下の 5 つの層に分類しています。各層における脆弱性を指摘するとともに、設計・開発段階から運用までのライフサイクル全体を通じたセキュリティ対策の重要性を提言しています。

1. 物理層：露出したポート等からの物理的な侵入
2. センサー層：外部からの信号干渉による環境認識の歪曲
3. AI モデル層：判断ロジックを乗っ取る敵対的サンプル攻撃やプロンプトインジェクション

4. 通信層：OTA（無線通信アップデート）の改ざんや中間者攻撃
5. ソフトウェア/クラウド層：ミドルウェアや連携プラットフォームの脆弱性

レポートの全文は、https://info.vicone.com/ja/ai-robot-cybersecurity-risks-and-countermeasures_jp をご覧ください。

■システムと AI の多層防御を実現する VicOne「LAB R7」のソリューション

「LAB R7」は VicOne が自動車セキュリティで培った知見をさらに広げ、ロボットの乗っ取りやプライバシー情報の漏えい、AI モデルへの攻撃による誤動作など、フィジカル AI 特有の脅威を分析するとともに、設計・開発段階からのセキュリティ対策を実現するための技術研究を進めています。また、AI ロボットのライフサイクル全体を対象としたセキュリティソリューション開発にも取り組んでいます。

- Radeis（レディス：ロボティクスの開発・設計段階におけるセキュリティ対策支援ソリューション）
  AI モデルやソフトウェアの脆弱性スキャン、攻撃シミュレーション（AI レッドチーミング）などを通じて、プロンプトインジェクションや不正な動作につながる既知・ゼロデイのリスクを高精度で特定し、優先度を自動判定します。さらに、SBOM／HBOM／CBOM の自動生成・管理にも対応し、複雑なサプライチェーン管理と法規制への準拠を効率化することで製品の安全性を担保します。

- Rthena（アテナ：稼働中のロボットを保護する運用段階向けセキュリティソリューション）
  ロボットのシステム状態や挙動を継続的に監視し、コアシステムの改ざんや不正な変更、異常な動作をリアルタイムで検知することで、インシデントの早期発見と迅速な対応を可能にします。また、RSOC との連携によりフリート全体のセキュリティ状況を一元管理でき、必要なデータのみを送信する効率的な仕組みで運用コストの低減にも貢献します。

- xPhinx（スフィンクス：ロボティクス・エッジ AI 向け AI 挙動保護ソリューション）
  ロボティクスにおけるエッジコンピューティング環境において、VLM/VLA の入出力をリアルタイムに監視し、プロンプトインジェクションやジェイルブレイク、不適切な挙動、データ漏えいをリアルタイムに検知・無害化します。クラウドに依存しない軽量設計により低遅延・オフライン運用を実現し、脅威インテリジェンスに基づく脅威・リスクモデルの継続更新にも対応します。

VicOne について

VicOne は、これからの自動車を守るというビジョンを持ち、自動車産業向けに幅広いサイバーセキュリティソフトウェアやサービスを提供しています。自動車メーカーの厳しい要求に応えるために開発された VicOne の各ソリューションは、現代の車両が必要とする高度なサイバーセキュリティの各種要件に適合し、大規模な運用にも応えるように設計されています。VicOne は、トレンドマイクロの子会社であり、トレンドマイクロが 30 年以上にわたって培ってきたサイバーセキュリティ技術をベースにしています。自動車サイバーセキュリティのグローバルリーダーとして、サイバーセキュリティにおける独自の深い知見を活かした先見性を提供し、お客様が安全でスマートな車両を開発できるよう支援しています。

〈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	東京都新宿区新宿 4-1-6　JR 新宿ミライナタワー
事業内容	自動車向けサイバーセキュリティソリューションの開発
U R L	https://www.vicone.com/jp