2018年2月14日

パナソニック株式会社
トレンドマイクロ株式会社

# パナソニックとトレンドマイクロが、コネクテッドカーのサイバーセキュリティソリューションの共同開発に合意

パナソニック株式会社（本社：大阪府門真市、代表取締役社長：津賀一宏、以下、パナソニック）とトレンドマイクロ株式会社（本社：東京都渋谷区、代表取締役社長 兼 CEO：エバ・チェン、以下、トレンドマイクロ）は、今後普及が見込まれる自動運転・コネクテッドカーに対するサイバー攻撃を検出および防御するサイバーセキュリティソリューションを共同開発することに合意しました。

本共同開発により、アクセルやブレーキなど自動車の走行を制御するECU※1およびカーナビなどの車載インフォテインメント機器（IVI※2）やテレマティクス※3機器に対するインターネット経由のサイバー攻撃を検知・防御するソリューションを開発し、安全な自動運転・コネクテッドカーの実現を目指します。

コネクテッドカーの分野では、ハッキングにより、ハンドルやブレーキシステムを制御されるリスクが確認されています。また、日々新たに発見される脆弱性を突いた遠隔操作の危険性も指摘されています。このため、個々の車両内部のみで対策するだけでなく、クラウドから常に車両に対する監視を行うことにより新しい攻撃が発生していないか分析し、その結果をすべての車両のサイバー攻撃対策に活かしていくことが、今後ますます重要となります。

本共同開発では、パナソニックのオートモーティブ侵入検知・防御システムのCAN侵入検知・防御技術※4を、監視ECUなどに実装し、ブレーキやハンドルなど自動車の走行を制御するECUへの不正コマンドを検知します。また、トレンドマイクロのマルウェア※5解析技術などのセキュリティインテリジェンス・ノウハウを活用したIoT機器向けセキュリティソリューションTrend Micro IoT Security※6を、カーナビなどの車載インフォテインメント機器（IVI）に実装し、インターネット経由の脆弱性を狙う攻撃パケットを検知します。さらに、これら双方が検知した結果であるログを収集し、セキュリティ監視クラウド上の解析プラットフォームに送信し、解析します。本解析情報をもとに不審な通信の検知および防御につなげます。

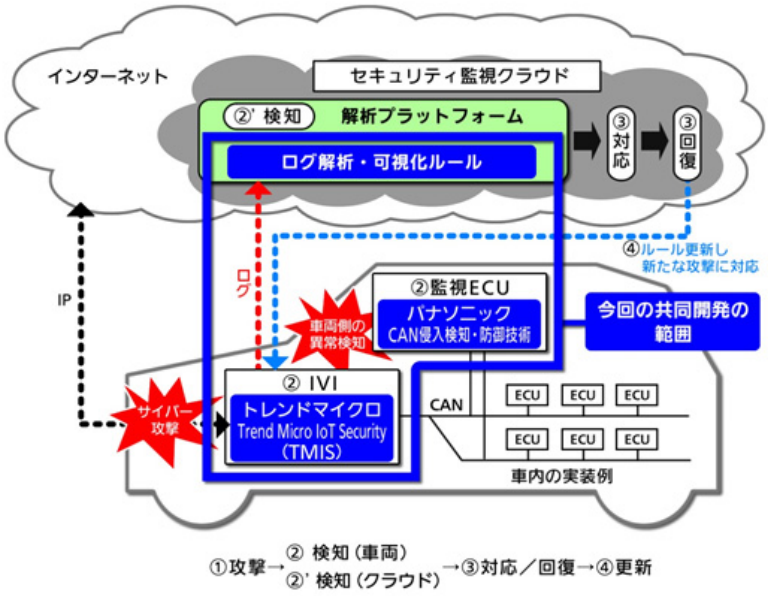
これにより、自動運転・コネクテッドカーに対するサイバー攻撃を防ぐための、車両側からクラウドまで含めたソリューションの提供が可能になります。両社は、2020年以降のサービス実用化を視野に、共同開発を進めてまいります。

## 【お問い合わせ先】

オートモーティブ＆インダストリアルシステムズ社
オートモーティブ企画部 広報宣伝課 田村・山口 電話045-939-6103

トレンドマイクロ株式会社
パブリックリレーションズグループ 中吉（なかぎり）・牧野・高橋
〒151-0053東京都渋谷区代々木2-1-1 新宿マインズタワー12F
TEL：03-5334-3658 FAX：03-5334-3648 MAIL：pressweb@trendmicro.co.jp

## ■今回実施する共同開発の構成図




※1 Electronic Control Unit：エンジンやステアリングなどのアクチュエータを制御するコンピュータ。

※2 in-vehicle infotainment：車載インフォテインメント機器

※3 テレマティクス：自動車への情報提供サービス。

※4 CAN侵入検知・防御技術：ECU間通信に使用されるCAN（Control Area Network）上に不正なコマンドが流れていないかを監視し、不正と検知した際にはそのコマンドを無効コマンドとして処理する技術。

※5 マルウェアMalware：不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードの総称で、コンピュータウイルスもこれに含まれる。

※6 Trend Micro IoT Security：Linuxなどの汎用OSで動作し、外部とIP通信を行う組み込み機器を対象とするセキュリティソリューション。

以上