

第 3 回 STAMP ワークショップ発表概要

タイトル

Connect Car を対象とした STAMP/STPA の事例紹介

Analysis report for Connected Car using STAMP/STPA

著者・発表者

デロイト トーマツ リスクサービス 株式会社 林 浩史

Deloitte Tohmatsu Risk Service Hayashi, Hiroshi

概要

近年コネクテッドカーを対象としたサイバーセキュリティアセスメントや侵入テストが頻繁に行われている。

一般に TARA (Threat Analysis and Risk Assessment) などの手法が用いられているが、コネクテッドカーをシステムとしてとらえた場合、STAMP/STPA を用いた分析を併用して行うことでより深い分析が期待できる。

本報告では、コネクテッドカーの機能の一つである Virtual Car Key システムに関する分析を行った結果を事例として紹介する。

Virtual Car Key は、スマートフォンなどのモバイルデバイスを用いて車両のドアをロック・アンロックし、エンジンの始動・停止などを行う機能である。

これは次世代の自動車利用の形態の一つとして注目されているカーシェアリングなどを実現する基礎技術の一つである。一方で車両の重要機能とスマートフォンのような IT 機器を直接接続する機能であり、車両側だけでなく、スマートフォンも含む系全体としてのサイバーセキュリティ対策が必要となる技術分野である。

この機能は近年多くの車両メーカーによって実装提供され始めており、その実装形態も様々である。我々は一般論に基づく機能要件をベースに仮想システムを構築し、サイバーリスク分析を行った。

本報告では、Virtual Car Key に求められる機能とそれから導きだされる要件、およびそれを実装した場合に想定されるリスクなどについて、STAMP/STPA を用いて分析した結果を報告する。あわせて、東京電機大学チームが開発を進めている MRC-IOT のプロトタイプを併用して、準定量分析を行った結果についても併せて報告する

キーワード

- (1) サイバーセキュリティ
- (2) IoT
- (3) Virtual Car Key
- (4) コネクテッドカー
- (5) IPA STAMP/STPA Workbench