ITU-T におけるコネクテッド・カーにおけるセキュリティ技術の標準化動向

元 ITU-T SG17　副議長
国立研究開発法人情報通信研究機構　中尾（なかお）　康二（こうじ）

1. つながる車のセキュリティ標準化の意義・必要性

自動車がインターネットなどのネットワークへ接続され自立的になるにつれ、オンボードシステムのセキュリティ及びその安全性は自動車産業にとっても最優先事項になっている。近年の自動車における新しい接続サービスや無人運転機能の配備は、悪質なハッカーにとって、自動車が恰好の攻撃標的になってきているとも言える。さらに、今日の自動車内に組み込まれる多数のECU（電子制御ユニット）は、Wi-Fi、携帯電話、インターネットなどの多様な外部ネットワークへの接続が想定され、自動車の製品ライフサイクルを通して、自動車が提供する複雑なシステムの安心・安全を確保することが喫緊の課題となる。

上記の課題に対し、「つながる車の時代における安全性確保、セキュリティ確保」という視点で、国際標準化がいろいろな標準化機関において始まっている。それらの成果物は、つながる車におけるセキュリティ枠組み、脅威分析、セキュリティ対策などにおける標準的な技術仕様などを国際レベルで策定することにより、国際的技術仕様が多くの利益関係者（ステークフォルダー）にとって有益で共通のリファレンスとなり、さらにそれらが国際的な認証規定などの材料になることも期待できる。本稿では、ITU-T SG17（セキュリティ）における「つながる車のセキュリティ標準化」の動向について概説する。

2. SG17での標準化活動

(1) ITSセキュリティのための課題13

ITU-T SG17は、全般的なセキュリティの規格化を目的とする研究グループであるが、その中の課題（Question）13は「高度交通システム（Intelligent Transport System（ITS））におけるセキュリティ」を扱っている。本課題は、2017年秋に成立した新課題で、「つながる車」の環境を想定した技術検討からスタートしており、セキュリティ枠組みやガイドラインの策定及びつながる車に関連する技術課題を広く取り扱っている。

(2) ITSセキュリティの勧告化作業の現状

現状、ITU-T SG17 課題13においては、**表**に示す勧告群の策定を進めている。

本表において、特に注目される勧告内容について、以下に概説する。

A）勧告 X.1373（ITS通信デバイスのためのセキュアなソフトウェア更新機能）の改版

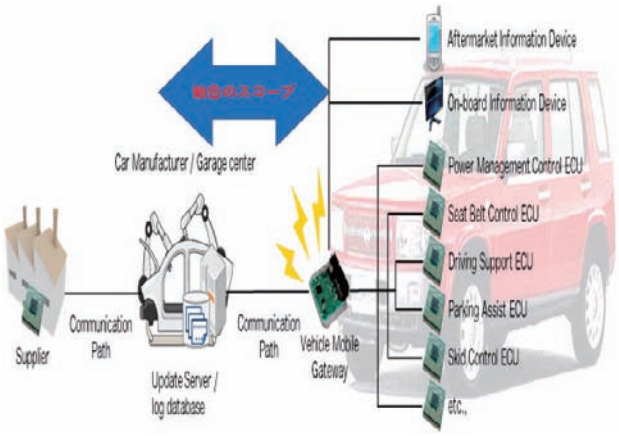
概要：2017年3月に発行された勧告X.1373は、車に搭載されるECU（電子制御ユニット）で動作するソフトウェア（ファームウェアも含む）の更新を行うための、セキュアな手順（更新作業終了確認のための電子署名の活用など）を勧告化していた（スコープは**図1**）。現在、本勧告の改定作業を進めており、勧告の範囲の拡大化、各国のOEMの要件の反映などを進めているところである。

B）勧告草案 X.itssec-2（V2X通信システムのためのセキュリティガイドライン）

概要：車と車、車と路側（インフラ）、車とノーマティック機器（スマートフォンなど）、車と人との間の接続（通信）を想定し、各々の接続において想定できるユースケース

■表．ITU-T SG17　課題13における作業中の勧告群

勧告名	タイトル	凍結時期
X.1373rev	Secure software update capability for intelligent transportation system communication devices	Sep-21
X.itssec-2	Security guidelines for V2X communication systems	Sep-19
X.itssec-3	Security requirements for vehicle accessible external devices	Mar-20
X.itssec-4	Methodologies for intrusion detection system on in-vehicle systems	Mar-20
X.itssec-5	Security guidelines for vehicular edge computing	Sep-21
X.edrsec	Security guidelines for cloud-based event data recorders in automotive environment	Sep-21
X.eivnsec	Security guidelines for the Ethernet-based in-vehicle networks	Sep-21
X.fstiscv	Framework of security threat information sharing for connected vehicles	Sep-21
X.mdcv	Security-related mis-behavior detection mechanism based on big data analysis for connected vehicles	Dec-20
X.srcd	Security requirements for categorized data in V2X communication	Dec-20
X.stcv	Security threats in connected vehicles	Sep-19

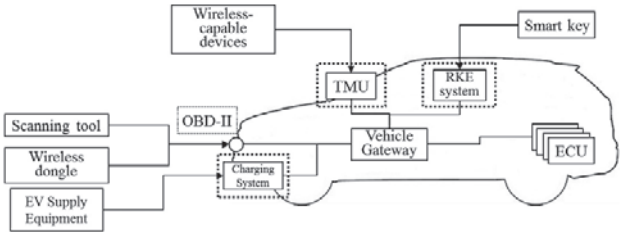


■図1.　旧勧告X.1373におけるスコープ（現改版では、本スコープを拡張している）

及び脅威を抽出し、そのためのセキュリティガイドラインを導出している。

C）勧告草案 X.itssec-3（アクセシブル外部機器のためのセキュリティ要求事項）

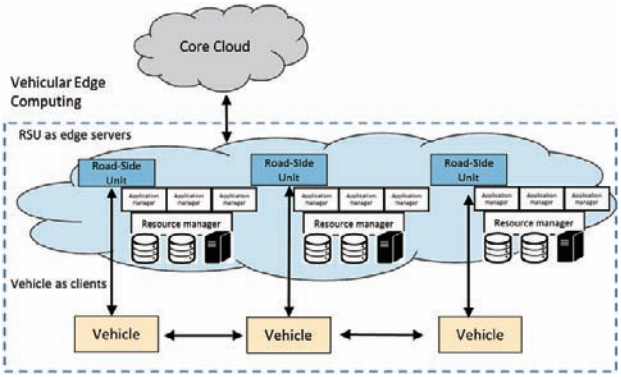
概要：車の中に配備される、OBD-II、TMU（Telematic Management Unit）、RKE（Remote Keyless Entry）システム、Chargingシステムなどの外部へのアクセスを可能とするインタフェースに注目し、それらを介した外部機器（Scanning tool, Wireless dongle, Smart key等）からのアクセスにおける脅威及びセキュリティ要件を洗い出し、標準化ドキュメントとしてまとめている。図2は、本勧告草案にて想定されるインタフェースと外部機器を表している。



■図2.　想定されるインタフェースと外部機器

D）勧告草案 X.itssec-4（車システム内のための侵入検知メカニズム）

概要：本勧告草案は、ECUに直接的なインパクトを与える車内のネットワーク（CAN）への侵入を検知する手法に焦点を当て、車に適用可能な、シグネチャーベース検知、エントロピーベース検知、自己類似性検知など、車への実装が想定できる軽量な侵入検知手法についてまとめたものである。



■図3.　車のためのエッジコンピューティングの概念

E）勧告草案 X.itssec-5（車のためのエッジコンピューティングのセキュリティガイドライン）

概要：本勧告草案は、図3で示す車のためのエッジコンピューティングの環境を想定し、その環境に内在する脅威、脆弱性分析を行い、参考となるユースケースを用いたセキュリティ要件をまとめている。

F）勧告草案 X.stcv（つながる車におけるセキュリティ脅威）

概要：UNECE（国際連合欧州経済委員会）のWP29（World Forum for Harmonization of Vehicle Regulations）で策定された「サイバーセキュリティ勧告」において、各国のOEMベンダー間の合意の中でまとめられた「セキュリティ脅威」をベースに、ITU-T SG17の中で共通的な脅威情報としての活用を目的として、課題13で「セキュリティ脅威情報」の勧告化を進めている。（2019年9月に凍結予定）

3.　おわりに

本稿では、ITU-T SG17　課題13において現在進行中の勧告化作業につき、概観した。これらの活動の多くは、韓国（主に、Hyundai Motor）及び中国（中国OEMとの連携によるセキュリティベンダー）からの提案となっている。日本としても、重要な勧告案については、課題としての可否判定、内容精査などを積極的に実施する必要があると考える。例えば、2019年1月に開催されたITU-T SG17会合においては、中国の通信事業者と20社の中国OEMとの連携で、「Security guidelines for network-based driving assistance in autonomous vehicles（自動走行における運転アシスタントをネットワーク事業者主導で実施するためのセキュリティガイドライン）」の提案がなされている。本提案については、日本、韓国が時期尚早と強硬に反対したため、保留となったが、今後の進展が注目される。