講演６．自動車安全にかかわるセキュリティの課題

自動車研究部　　※新国 哲也　　河合 英直

１．はじめに

自動車には様々な装置が搭載されている。それらを制御する各コンピュータは車両内部のネットワーク（例えば Controller Area Network: CAN）に接続され、これを介したコンピュータ同士の連携により自動車全体を統括的に制御している。近年では車両内部のネットワーク通信の高速化が進み、車両の走行・停止・転回など基本的かつ重要な機能に係る制御にも車両内部のネットワークが使用されている。

このような状況においては、車両内部のネットワーク上でやり取りされる制御信号の保全が、車両制御を確実にするための重要な要素となる。

一方で、従来はドライバが行っていた運転操作の一部を自動化する技術が提案されてきており、車載のセンサのみならず、例えば車外との通信により情報を得て交通状況を把握し、自動化技術に活用することも考えられている。

車外との通信には、悪意のあるハッキング等の不正利用のリスクを考慮しておかなければならない。このためセキュリティは自動車の安全性を確保する上で重要な課題となりつつあり、行政的な対応の在り方を検討していく事が必要である。

当研究所では、まず技術的な観点で２つのケーススタディを通して自動車セキュリティの要件について検討を開始した。また、従来型の審査・検査を含め、自動車セキュリティの確保につなげる制度的な対応についても検討を開始したので、その一部を報告する。

２．CAN の不正利用の影響例

自動車の安全性に直接的な影響を及ぼす脅威としては、主幹的な制御に係る ECU やその ECU が接続されている車両内部のネットワークの不正利用が考えられる。ステアリングやブレーキの機構にアクチュエータが使用されている自動車では、ネットワークの不正利用がドライバの操作とは関係ない車両の挙動変化につながる可能性がある。

当研究所では車両内部のネットワークの不正使用が安全性に与える影響を把握するため、車両を使った調査を行っている。図１には、車両内部のネットワークの不正利用による誤動作の例を示す。この例では、燃料残量を正しく示すはずの状況で完全な燃料切れを示した。ドライバに誤った情報を表示することは、広い意味で安全性低下につながると考えられる。

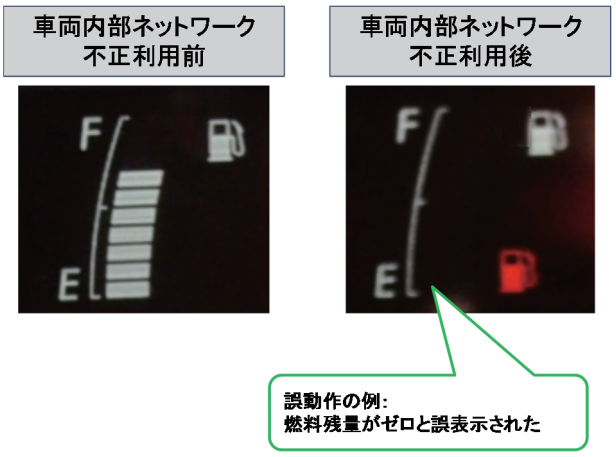

図１　車両内部のネットワークの
不正利用による誤動作の例
（燃料表示の誤動作）

３．車外との通信を使用した不正の影響例

３.１．通信を使用した不正に関するデモの概要

ここでは、2. のケースと同様に車両への挙動変化に影響を与えた別の不正アクセスのケースを説明する。無線通信を使った不正アクセスにより、多数の車両に影響を与えうる事例を示したデモンストレーションであり、以下にその内容を説明する。

このデモンストレーションは、2015 年に米国のチャーリー・ミラーにより行われ、公表された。車両の無線通信システムを利用した CAN バス（CAN の通信線）への不正アクセスであり、動画共有サイトなどを使ってデモンストレーションの内容が公表された。

３．２．無線通信システムへの不正アクセスデモンストレーション内容

攻撃対象の車両は、別のドライバによる通常の操作によりハイウェイを走行していた。チャーリー・ミラーは自宅の PC からインターネットを介して同車両にアクセスし、ドライバの操作によらず、チャーリー・ミラーの PC 操作により走行中に同車両のエンジンを停止するなどのデモンストレーションを行った。

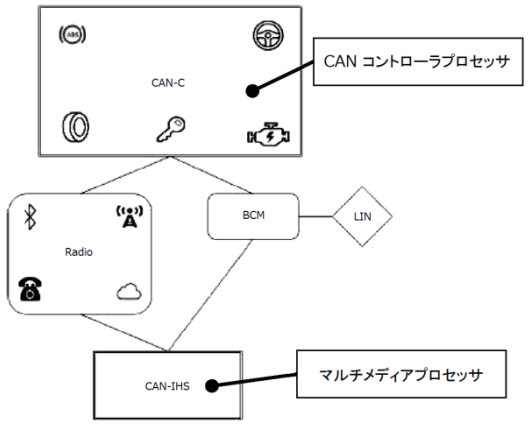

図 2 攻撃対象車の CAN バス構造
（チャーリー・ミラー報告書より抜粋）

以下には、チャーリー・ミラーの技術的な報告書[1)]から主要個所を抜粋し説明する。

CAN バスの構造は図 2 の通りである。車両の制御に係る ECU は CAN-C バス（後述の CAN-IHS バスとは別の CAN バスであり、”C”の定義についての説明は同報告書に記載なし）に、カーナビゲーションシステムなどインフォテイメント（情報と娯楽を提供する機能）系の ECU は CAN-IHS（先述の CAN-C バスとは別の CAN バスであり、”IHS”の定義についての説明は同報告書に記載なし）バスに接続されている。

以下には外部からの無線通信により CAN-C バスへの侵入が可能となった経緯について焦点を当て、チャーリー・ミラーが行った当該車両システムの解析手順に従って説明する。

３．３．対象車両の無線通信ポート

対象車両については、ナビゲーションシステムが外部との通信を行っている。外部との無線通信に関して、CAN-C を制御する CAN コントローラプロセッサには直接アクセスできないため、不正アクセスの戦略として別のポートからの侵入を試みている。まず、デフォルトゲートウェイのポートをスキャンすることで、解放されているポートとそのアプリケーションを調査した。

この中で 6667 番ポートは、通常はインターネットで使用される通信プロトコルである TCP/IP の定義として、IRC（Internet Relay Chat）server が使用するポートであり、internet を介したチャット（会話）を行う際に用いられるポートである。しかし車載システムとしてチャット機能は意味を持たないことからハッカーの目に留まることとなり、ナビゲーションシステム における 6667 番 ポートの真の役割についてさらに深く調査された。その結果、6667 番ポートは実際には D-Bus サービスに用いられていることが判明した。D-Bus サービスは、Linux OS などのプログラム間のデータのやり取りやネットワーク上の別のコンピュータ上にあるサブルーチンなどを実行することができる手段として利用されている。6667 番ポートを介せば車外から D-Bus サービスを利用できることとなるため、このポートを介した攻撃が試みられた。

３．４．不正ファームウェア（ECU 内に組み込まれるソフトウェア）による CAN バス構造の変更

ナビゲーションシステムには、マイクロコントローラーが他の電子モジュールと通信することができる高速の CAN-IHS 用ソフトウェアも含まれている。ただし、マルチメディア情報を処理するマイクロプロセッサ（以下マルチメディアプロセッサ）自体は CAN-C バスには接続されておらずマルチメディアプロセッサによる車両の制御はできない状態である。CAN-C バスの処理を行っているのは、ナビゲーションシステムに内蔵されている先述の CAN コントローラプロセッサである。D-bus により操作可能なマルチメディアプロ

セッサは、一方で CAN-C バスとの直接接続が無いため任意の信号を CAN-C バスに送信することができない。そこで CAN コントローラプロセッサを proxy（メッセージを転送する代理役）として利用することが考案された。これには車外から送られた任意のデータ（偽の CAN メッセージなど）を CAN-C バスに転送する機能を加えた不正なファームウェアを CAN コントローラプロセッサにアップロード し、同プロセッサを再起動して実行させる必要がある。先述の通り 6667 番 ポートを介して CAN コントローラプロセッサを直接操作することは不可能なため、マルチメディアプロセッサにより上記の手順を実行しなければならない。

結局このデモでは、不正なファームウェアを CAN コントローラプロセッサにアップロード し、同プロセッサを再起動する手順も発見された。

以上を整理すると、不正ファームウェアにより CAN バスの構造が変更され、外部からの無線により偽の CAN メッセージを CAN-C バスに入力することが可能となった。CAN バスの構造に着目すると、不正ファームウェア実行後では図 3 のように変化したことになる。図 3 に示した不正ファームウェア実行後の CAN バスの構造では、ゲートウェイ（CAN バス上でデータの流れを制御する仕組み）などは介さずに外部から直接 CAN-C バスに偽の CAN メッセージの入力が可能となった。

3．5．車外からの攻撃デモのケーススタディ

以上で説明したデモンストレーションを題材に、不正がなされる前の状態での潜在的な課題を抽出する。なお、ここでの検討は、独立行政法人情報処理推進機構による「自動車の情報セキュリティへの取組みガイド」[2)] を参考に行った。想定するリスクは、実際に攻撃対象の車両で発生した事象から、次の 2 つとなる。

①不正設定：メーカにより設計されたファームウェアに不正なコードが追記された

②偽メッセージ：無線を介して CAN-C バスに偽の CAN メッセージが入力された

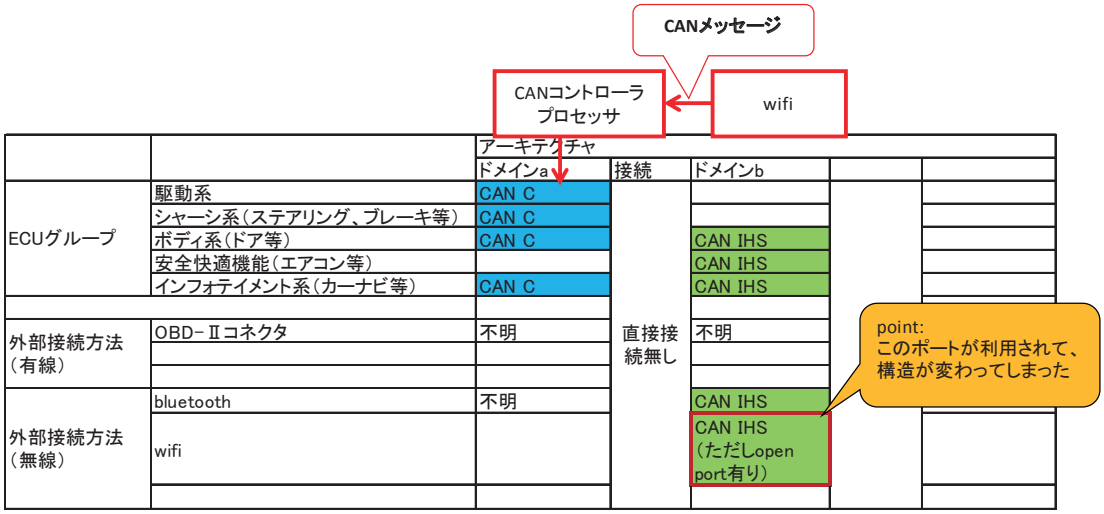

図 3　デモで使われた車両の不正ファームウェア実行後のネットワーク構造
（著者による推定を含む）

表 1　デモで使われた車両のセキュリティ対策ケーススタディ

脅威の内容	採られていた対策	採られていなかった対策	セキュリティ強化のための追加機能例
不正設定	ドメイン分割	認証機能設計	ファームウェアアップデートの認証
		アクセス制御機能設計	CAN-C バスとナビゲーションシステム間のゲートウェイ
偽メッセージ	メッセージ検証（カウンタ、チェックサム等）	認証機能設計	CAN メッセージ認証
		アクセス制御機能設計	CAN-C バスとナビゲーションシステム間のゲートウェイ

本章のケースに関して「①不正設定」の脅威に対する車両の対策はドメイン分割（ネットワークの領域分割）であったが、他にアクセス制御としてゲートウェイ 等の設置によりインフォテイメント機能を搭載したナビゲーションシステムからの CAN-C バスへのアクセスを制限しておくことや、プログラム認証（マイクロプロセッサの再立ち上げに対する権限の確認など）により、無線を介した不正ファームウェアのアップロード 及び実行は防げた可能性が考えられる。また、「②偽メッセージ」の脅威に対する車両の対策としては、メッセージ認証などにより偽の CAN メッセージによる車両の誤動作は防ぐことができると考えられる。

ここで注目したいのは、以上で説明してきたシステムにおいて、セキュリティ対策（例えばドメイン分割など）は取られていたという点である。しかし、結果として不正が成立したということから、高いスキルによる攻撃を想定した場合は、セキュリティ対策を複数、多層的に実施することが必要であると考えられる。

４．自動運転に係る課題

以上では、車両の走行や操舵といった機能に直接的な影響を与えるケースを想定して、これらの機能に係る車両内部のネットワークに対する不正に関してケーススタディを行った。これに加えて自動運転技術の進展に伴い、たとえば EDR（Event Data Recorder）といった装置により車両に保存される情報の保持が重要な課題となる。交通事故などに関連するデータ等は、原因究明及び対策の検討の観点から、事故発生後にデータの改ざんが行われないよう慎重な取り扱いが求められる。例えば暗号化技術を用いるなどにより、第三者機関が暗号鍵を管理するような手段が有用であると考えられる。

また、自動運転技術を考慮した EDR 要件については、ドライバと自動運転システムとの間のインターフェースの健全性なども記録情報として重要になる。そのため、自動運転にも対応するよう EDR 技術要件[3]が見直されることが望ましい。

５．まとめ

無線通信を使った不正アクセスのケースについて内容を説明し、対策について検討した。これらのケースでは、セキュリティ対策は取られていたものの単一的な対策にとどまっており、試行的に与えた脅威に対しては十分ではなかったことが分かった。可能な限り脅威を想定し、セキュリティ機能設計を多層的に施すことが有効である。

６．今後について

今後セキュリティ対策に係る審査・リコールの手順について検討を行うにあたり、最初のステップとして現状における車両のネットワーク構造や、それに対するセキュリティ対策の内容の把握を行うことが考えられる。なおハッカーの技術レベルは日々進化することが想定される。このため、セキュリティ対策技術に対する要件やその確認方法は適宜見直していく必要があると予想され、制度的にも課題が生じると考えられる。

また、国連の自動車基準調和世界フォーラム（UNECE／WP29）においては、自動運転に関して概念整理を行う ITS/AD（Intelligent Transport System / Automated Drive）や、ステアリングに係る自動運転の技術検討を行う ACSF（Automatically Commanded Steering Function）などのインフォーマルワーキンググループが活動している。これらの議論において、早い段階からセキュリティ対策を盛り込んだ議論を行うことが重要であると考えられる。

参考文献

1）チャーリー・ミラー, クリス・ヴァラセク” Remote Exploitation of an Unaltered Passenger Vehicle”, August 10, 2015

2）独立行政法人 情報処理推進機構、「自動車の情報セキュリティへの取組みガイド」、2013 年 3 月

3）国土交通省，「J-EDR の技術要件」 http://www.mlit.go.jp/kisha/kisha08/09/090328/01.pdf