サイバーセキュリティの時代を迎えた自動車社会

The Cyber Security on Automotive Industry

神山　裕 *
Hiroshi Kamiyama

要　旨

今日の車社会においては，自動運転あるいはコネクティッドという新しい機能と共に，車が外の世界と「ツナガル」，いわゆるサイバー空間の世界に足を踏み入れ，この 100 年の歴史の中で経験したことのない多くの事柄が起ころうとしている．この新しい世界では日常茶飯事となりうる，サイバーアタックの脅威とそれを守るためのセキュリティ技術について，車載器機の世界における通信の歴史を紐解きながら，業界の動向だけでなく国レベルでの取り組みも含め，実例を交えて紹介する．

Abstract

In today's car society, with the new function of automatic driving or connected, the car has entered the world outside and the world of "Tsunagaru", the so-called cyber space, and has never experienced in this 100-year history Many things are going to happen. In this new world, the threat of cyber attack and the security technology to protect it, which can be a daily event, while noting the trend of communication in the world of in-vehicle controller, not only the trend of the industry but also efforts at the national level, examples We will introduce it.

Key Words : Communication System / Cyber security, Connected Car, Controller Area Network, On-Board Diagnostics

プロローグ

2018 年 06 月 XX 日（水），今日も梅雨空のある日の朝，埼玉県にお住まいの A さんのお宅ではいつもの通り，ご主人を駅まで送っていこうと奥様が車のエンジンを掛けようとEngine Start Buttonを押していた．しかし，いつもなら数秒でスターターが回りエンジンが心地好いサウンドを奏でるのに，今朝は何度スタートボタンを押してもエンジンが回らない．ご主人は，車で送ってもらう事を諦め，近所のバス停まで走って出掛けて行った．残された奥様は，バッテリが上がってしまったかと思い，JAFを呼んでエンジンを掛けようとしたが，車はピクリともしない．

ふとスマホのメールをチェックしてみたら，怪しげなメールが 1 通．

「エンジンがかからずに，お困りの様ですね」

「私は車のリモート診断を専門に手掛けている△△△モータースの○○と申します．あなたのお車は，自動運転対応のコネクティッド・カーですから，インターネットで様々なサービスとツナガっています．このサービスの一つである，お車の始動時診断サービスを通じて，今朝ほどお客様のお車から，弊社のサービスセンター宛にエンジン始動不良という速報が飛び込んできました．もし 0.03 *BTC*（注 1）を，下記の宛先にメールでお送りいただければ，直ぐにでもあなたのお車をこちらからリモートで診断・修理をさせていただき，エンジンがかかる状態に戻して差し上げます」

こんな世界が現実のものに．

1. は　じ　め　に

これまでの自動車の世界におけるセキュリティは，メカニカルな鍵をコピーされて車が盗難に逢ったり，ドアの施錠機構をイタズラされて，車内に置いていた金品を盗まれたり，NAVI システムを盗まれる等のいわゆる泥棒による車両盗難や車内物品盗難という「フィジカル・アタック」に対するセキュリティ対策が主に取り組まれてきた．この取組の結果，エンジン・イモビライザーの普及や，車内侵入センサーの開発・法制化といった対応策が取られ，自動車の盗難などに対するセキュリティの手法として一定の効果を上げてきたのは既知のことである．

* 電子事業本部 電子設計グループ

注 1）　*BTC*：2009年に運用が開始された、仮想通貨bitcoinの単価

一方でITの世界では，インターネットという便利な通信手段の普及に伴い「情報セキュリティ」という言葉に代表されるように，パーソナルコンピュータやサーバーに対する情報搾取を目的としたサイバー空間からの攻撃が2000年頃から脅威として認識され，ワクチンソフトに代表される様々な対応策が取られてきた．しかし，近年でもウィルスの亜種が次々と誕生して，その被害も情報搾取から金品要求へと変化しながら，依然として猛威を振るっており，「サイバー戦争」という言葉を生み出し国家的な取組事項として扱われるまでになっている．

2. 車の通信とセキュリティ

2.1. 自動車における通信の歴史

自動車の世界においても，1970年代以降の排気ガス規制強化対応に始まる様々な機器に対する電子制御（コンピュータ制御）の普及により，制御機器間で必要となるデータ（情報）のやり取り（通信）が活発化し，情報量の多様化・多量化に伴い通信手段もアナログ信号からデジタル信号へと時々刻々変化を見せてきた．

近年のクルマにおいては，CAN（Controller Area Network）プロトコルを用いた制御機器間の通信が当り前のように普及し，軽自動車から高級車に至るまで車内のいたるところを通信線と電源線の両ハーネスが這い回り，高級車ではその総延長が3Kmを超えるとも言われ，現代の電子制御はこの通信無では成立しなくなっている．

2.2. 故障診断を始めとする様々なサービスの提供

CANという共通の通信プロトコルが普及する事で，車内の様々な情報がやり取りでき，この通信線を介したサービスの提供もまた様々な形で発展してきた．

モータリゼーションの発達に伴う大気汚染の悪化を改善する目的で，米国EPA（アメリカ合衆国環境保護庁）やCARB（カリフォルニア州大気資源局）が排気ガス規制を制定し法規化すると共に，車載電子制御部品の故障診断とそれに伴う通信が規格化（1996年，OBD Ⅱ）された．この規格化に伴い，CANに接続された診断対象部品との通信を容易化するための専用通信ポート（OBDポート）も同じく標準化・車載義務化され，同様に仕様が標準化された診断機を接続する事により，様々な車の診断が容易にできるようになった．

この規格化・標準化により，複雑化した電子制御に対して故障診断・修理の的確化・容易化が図られ，利便性が大幅に向上したことは言うまでもない．

また一方で，OBDポートを介して車載電子制御部品，あるいは制御通信の情報が容易にモニタできることから，ドライバーの運転状態・制御状態をこのポートに接続された無線機を経由して入手・分析することで，自動車保険の算定に役立てるなどのサービスも開発され提供されている．

2.3. クローズ⇒オープン

こうして，車の中の車載部品同士がコミュニケーションするために始まった車載通信が，車両内というクローズな環境から，診断やサービスの発展を伴う事で，いつの間にか車両外とのコミュニケーションというオープンな環境へとその立ち位置が変化してきた．

この変化の中で，2013年米国にて開催されたハッカー大会（DEFCON）においてDARPA（Defense Advanced Research Projects Agency：アメリカ国防高等研究計画局）の支援を受けた著名なハッカーが，OBD Ⅱポートや，車両内の通信ハーネスへの直接接続を介して自分たちのPCを車載通信に侵入・介在させるという大胆な実験・研究映像が発表された．[4]

また，この発表の中ではOBDポートや通信線への直接接続だけでなく，無線による車載通信への侵入や制御の可能性についても言及しており，この後に起こる「車とサイバーセキュリティ」というパンドラの箱を開けたことは間違いが無い．

一方で，車両の外とのオープンなコミュニケーションは発展をつづけ，コネクティッド・カーに代表されるように，車がIoT機器の一種として扱われるようになってきているのも周知の事実である．

2.4. 情報セキュリティからサイバーセキュリティへ

2013年のDEFCONでの発表時点では，OBDポートへの接続や車両を改造して直接接続するなど，車両内に乗り込んでCAN通信線上の情報を搾取・改ざんするという行為が脅威として紹介され，その対策を含めて車の「情報セキュリティ」という言葉で言い表された．対策としてまず取り組まれたのは，CAN通信線の内部を流れる情報を外部から容易に見られないように，また改ざんされないようにするために，標準装備されているOBDポートをメインのCAN通信線から分離したネットワークアーキテクチャ（Fig. 1）をデザインすることだった．また，このアーキテクチャを実現するために，従来からその容易性と利便性のために同一の通信線に接続されていた各ECUとOBDコネクタを通信線上で分離するためのゲートウェイユニットの導入が，各自動車メーカーにおいて始まったのもこの頃である．

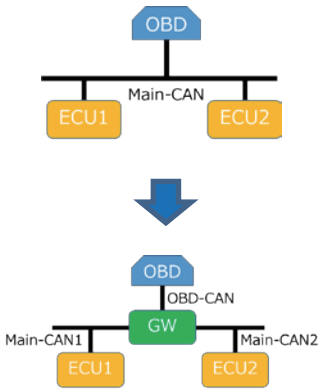

Fig. 1 Security Network Design

2.5. ツナガル クルマ

一方で，車の機能・サービス開発もこの 10 年において，今までの 100 年の歴史を根底から覆すような変革を迎えており，自動運転や電動化におけるまさに走るコンピュータと化して，機械制御から完全に電子制御へと置き換わってきている．また，競合相手に目を向けても，今までの自動車業界内での競争に留まらず，他業界から新たな考え方のクルマ作りを目指して参入してくるという競争相手が多数出現している．

こうした変革をもたらし可能とさせた要因として，車の中で制御に使われる情報の高度化，多量化とそれらを伝達可能とする通信ネットワークの高機能化・複雑化が挙げられる．

加えて，従来車両の中という閉ざされた環境下でやり取りが行われていた各種情報が，機能・サービスの高度化を目指して，これまでの診断結果の授受だけでなく制御に必要な情報までもが積極的に外部というオープンな環境とツナガルことで数多く授受され始めた．

この外部からの情報はまた，インターネットの世界に有る情報も数多く積極的に利用されており，情報授受は，3G や 4G といった公衆回線で接続されたスマートフォンを経由して車載機であるナビゲーションシステムとの間を Wi-Fi や Bluetooth といった無線を使って連携させることや，自動車のシステムの一部として組み込まれた DCU（Data Communication Unit）から直接 3G や 4G 通信を使って公衆回線に接続する事で実現されており，まさにクルマがサイバー空間とツナガッタことになる．

このツナガリは一方で，車をセキュリティの分野において前述の「情報セキュリティ」の世界から「サイバーセキュリティ」の世界へとツナグ結果となり，2015 年の DEFCON では早速，サイバー空間から遠隔地を走行している車両に攻撃を加えて，高速道路上で車両を停止させたり，ステアリングを自由にコントロールして運転者の意思とは違う方向に車両を誘導したりするという攻撃を具現化した脅威の発表が行われ，この発表に使われたクライスラー社･Jeep Cherokee のリコールにつながったとされており，サイバー攻撃によって車の安全性が脅かされるという脅威と，それを原因としたリコールという結果は，車業界に衝撃を与えたことは言うまでもない．

3. サイバーアタックから車を守る

一方で，サイバー空間の世界へ足を踏み入れるという事は，車が IT の世界にまた一歩近づいたことを意味しており，サイバー空間からの攻撃やそのセキュリティ対策においても IT の世界のそれに通じる考え方・対策が必要となる．

IT の世界と車の世界では，開発のスピードや安全に対する考え方が大きく異なっており，100 年近い車の歴史において培ってきた，各種の考え方・基準・法規などが一切通用しないような世界に放り込まれたことで，IT との融合という新たな取組が重要となってきた．

これは先行する IT 業界において起こっている，セキュリティ脅威の情報をいち早く収集し，そのセキュリティ対策までも積極的に取り入れることが車の開発に求められるということを意味しており，こうした IT 業界の先行する手法の中から，車の情報・制御を守るために，そのいくつかを取り入れる活動が既に始められている．

前述のゲートウェイユニットを使った通信トポロジーの構築による情報のプロテクトもその内の一つだが，セキュリティの世界で定着している，何重もの防御手段により守るという，多層防御の考え方に基づくと，決して一つの手法だけを取り入れれば良いという事は無く，二つ目，三つ目の防御手段が必要となってくる．

3.1. 通信の暗号化

こうした中で自動車業界においても一般的に採用され始めているのが，秘密鍵を利用したデータの暗号化と復号化を組み合わせることによる，2 つの機器間における情報授受の安全性を高める方法である．

ここで使用される秘密鍵は，個別のくるま毎，あるいは ECU 毎に異なった鍵を用意することで，その安全性を担保するため，鍵を使っている車両の情報と，使われている鍵の情報を一括して管理する仕組みもまた同時に必要となる．

またこの鍵は，発行・管理だけでなく認証局とセットで運用されることで，必要なときに鍵の認証行為を行ない常に鍵の確からしさを証明する必要が有るため，従来の自動車ライフサイクルには存在しなかった仕組やプロセスがまた要求される．

一般的にクレジットカードなどでもこうした鍵を使っ

た情報の授受が行われており，鍵の危殆化を避けるためにカード更新のタイミングに合わせて定期的な鍵の交換が行われる．

車載機に使用される鍵においても，こうした鍵の危殆化を避け安全性を担保するためにも，車の製造から廃車までを通じたライフサイクルマネージメントの確立が求められ，今までの自動車ビジネスには存在しなかったサービスや仕組みを構築する事が急務となっている．

3.2. 防御機能と検知機能の高度化

2010 年頃から本格的な普及が見られる仮想化技術などは，IT の世界においても代表的な防御技術の一つである．

外とツナガル ECU において，ソフトウェアの領域を仮想化領域と実制御領域に分けた上で，外からのデータの授受を仮想化された領域に置き，内部の制御に関わる領域と切り離すことで，万が一のウィルス感染の場合においてもその影響範囲を仮想領域のみに限定させ，内部には影響を与えない方法である．

こうした IT の世界で導入され実績を上げている防御機能を車載機器へも積極的に導入してく必要が有るが，IT の世界で確立された手法をそのまま車載機のような組込み機器に持ち込もうとしても，対象となる ECU のハードウェア構成には大きな違いがあるため，車載に適した変更や改造を加える必要が有る．一般的に組込み機器に用いられるハードウェアにはコストの壁もあることから，安価な CPU でも動作可能なように如何に軽量化されたロジックを作るか，という事が課題である．

4. 産官一体となった取組み

4.1. 基準化・法規制化

自動車会社や部品サプライヤ個別による対策技術の開発・進化だけでなく，自動車業界全体や国レベルにおいても，車のセキュリティを守る事は最重要課題として取組まれ，様々な形での基準化や法制化の動きを見せている．

米国においてはサイバーセキュリティ対策を怠った自動車メーカーを相手取って既に集団訴訟が起こされており，また上院議員の発動によりセキュリティ対策の法案化が進められており，セキュリティに対する基準化や法制化が国レベルの動きとして加速している．

2015 年には米国自動車技術会 SAE がいち早く J3061 という車向けのサイバーセキュリティガイドブックを定義し，プロセスを含めたセキュリティ技術の方向性を示しており，また日本の経済産業省も，独立行政法人情報処理推進機構（IPA）と協力して 2015 年末にはサイバーセキュリティ経営ガイドラインを作成し，自動車業界だけでなく広く産業界に対してサイバーセキュリティへの対応を求めており，今後 ISO を含めた世界的な基準化や法制化が，一層加速することは間違いない．

また，2017 年 9 月には自動運転に踏み込んだ法案 HR3388 が米国・下院を通過し，来るべき次の時代の車社会に向けた基準化・標準化，法制化の動きも着々と進んでいる．

一方，日本においても Jaspar（Japan Automotive Software Platform and Architecture）や自動車技術会，自動車工業会を中心に 2012 年からサイバーセキュリティへの対応を自動車業界における非競争領域として定義し，個社間の垣根を超えて成果の ISO 化を目指した活動を継続している．

4.2. セキュリティマネージメント

こうした法案や基準の中において新たに定義されるのが，自動車の設計・製造段階から，お客様の手に渡って，最終的に廃車されるまでのカーライフ全般に渡るセキュリティマネージメントである．

従来，自動車のライフサイクルマネージメントは，お客様に手渡された車の性能・機能を維持するための修理・メンテナンス・車検対応サービスなどが中心であったが，IT の世界においてもサイバーセキュリティは，攻撃者のアタック手法，守る側の対策，それぞれが日々進化しており，車においても同様にサイバーアタックの脅威に対するセキュリティ性能の維持・向上をするためのライフサイクルマネージメント・サービスへと大きな変革が求められる．

これは，皆さんが日々使っている PC のウィルス対策ソフトのパターン・アップデートと同じく，車載されたセキュリティ製品においても対策ソフトのアップデートが必要となる事を意味し，サービス店へのお客様の来店頻度が多くなることでご迷惑を掛けないためにも，何処にいても車載機のソフトウェアを最新のモノにできるように無線通信を使ったソフトウェアのアップデートの仕組みを構築することも，新たな課題の一つとして浮上している．

4. 新時代の自動車部品サプライヤとして

こうした自動車業界における大変革の時代を迎えて，カルソニックカンセイはいち早く，セキュリティの世界における IT 業界との融合を目指して，TOP ベンダーである仏・Quarkslab 社との連携を決断するだけでなく，今まで誰も取り組んでこなかった車向けサイバーセキュリティの専門会社 WHITE MOTION をこの 2 社による合同会社として設立し，車業界の最新技術・将来動向と IT 業界の最新セキュリティ技術を取り入れた製品をお客様に提供できる体制を整えた．

車載通信においては，従来のCAN通信に加えて、その進化形であるCAN-FD，Ethernetという新たなプロトコルが加わり，自動運転に供される車載制御部品の機能高度化に伴う制御情報の高速化・多量化を支えるための通信ネットワークの進化が着々と進んでいる．

このネットワークトポロジを根幹から支えるゲートウェイユニットもまた，カルソニックカンセイにおけるボディエレクトロニクスの中心的製品であり，通信プロトコルの多様化・多チャンネル化に加えて，ライフタイム全般に渡りセキュリティ機能をアップデートできる機能の開発を加速しており，車載通信の進化に合わせてお客様に製品提供できる体制を整えている．

また，同じく自動車のライフサイクルマネージメントにおいて重要となるセキュリティ鍵の管理においても，カルソニックカンセイは鍵の認証局機能を持つセキュリティ専門会社と共同で，設計・製造から廃車に至るまでグローバルにサポートできるセキュリティ鍵マネージメントシステムを構築して，自動車会社様の要求に答え，運転するお客様に安心と安全をお届けする準備を整えた．

6. おわりに

100年の歴史において，類を見ない大転換期に突入した自動車産業は，自動運転や電動化というお客様に提供する新しい価値向上と，併せて守らなければならない安全の提供という課題に取り組む必要性に直面している．

また，これまで経験したことのない，ITの世界との競合に打ち勝つために，これまでの業界の枠を超えた技術開発を加速させるための競争に突入した．

エピローグ

2018年07月△△日の朝，先述のAさんと同じくコネクティッドサービスに加入しているBさん宅でも，奥様がいつもの通りご主人を最寄りの駅まで送っていこうと車のエンジンを掛けて，ご主人の身支度が終わるのを待っていた．そう，AさんとBさんは同じコネクティッドサービスを利用して，毎朝の鉄道の運転状況や駅までの渋滞・回避情報を入手していましたが，唯一，コネクティッドサービスを実現する車の中のアーキテクチャとその構成部品が違っていたのです．Bさんのクルマはエンジンをスタートすると，ナビゲーションの画面に「CK&WM Inside」のロゴが出ていました．そう，Bさんの車に搭載されたECUには，カルソニックカンセイとWHITE MOTION社で開発した，最新のサイバー攻撃への対策が導入されていたのです．

残念ながらサイバー攻撃の進化とその防衛策の向上はイタチごっこで，その行きつく先は今のところ見えていない．これからのカーライフにおいて重要なのは，車がIT機器の一つだという認識を持ち，皆さんのPCと同じようにセキュリティのメンテナンスをすることです．

最新の攻撃・ウィルスに対応すべく，セキュリティソフトのUpdateを勧めるアナウンスが定期的にやってくる時代には，車のワックス掛けと同様にセキュリティのメンテナンスも忘れずに，快適なカーライフを楽しみたい．

参考文献

(1) IPA，自動車の情報セキュリティへの取組みガイド第2版，2017.03.23
(2) 岡：自動車開発のライフサイクルにおけるサイバーセキュリティ対策，2017年自動車技術会誌5月号
(3) 経済産業省，IPA：サイバーセキュリティ経営ガイドライン Ver2,0，2017.11.16
(4) Charlie Miller，Chris Valasek：Adventures in Automotive Networks and Control Units，2013 DEF CON 21
(5) SAE International：Cybersecurity Guidebook for Cyber-Physical Vehicle Systems，20160219

神山　裕