IPA Technical Watch

IPA テクニカルウォッチ

「自動車の情報セキュリティ」に関するレポート

～ネットワーク化・オープン化が進む自動車の安全～

独立行政法人情報処理推進機構
技術本部 セキュリティセンター

IPA テクニカルウォッチ：「自動車の情報セキュリティ」に関するレポート
～ネットワーク化・オープン化が進む自動車の安全～

目次

IPA テクニカルウォッチ：『自動車の情報セキュリティ』に関するレポート
～情報セキュリティで守る自動車の安全～

2012 年 5 月 31 日

IPA（独立行政法人 情報処理推進機構）
技術本部 セキュリティセンター

１．車載ソフトウェアとネットワークの利用が進む自動車と脅威の顕在化

近年、自動車にも様々なソフトウェアが導入されるなど、情報技術の活用が進んでいる。自動車一台に搭載される車載コンピュータ(ECU：Electronic Control Unit) は 100 個以上、ソフトウェアの量は約 1,000 万行と言われており大規模になっている。自動車のコストに占めるエレクトロニクス部品の割合はエンジン車で最大 30%、ハイブリッド車では 50%、電気自動車では 70%に達する 。さらに、複数の車載カメラなど画像処理のために 100Mbps 以上の高速で大容量の車載ネットワークが求められている。また、自動車の外部とのインタフェースは OBD-II (On Board Diagnosis-II)と充電制御インタフェースのほかにも、スマートフォンやタブレット PC (Personal Computer)が持ち込まれるようになるなど多様化している。この結果、車載システムは自動車内部における車両制御等の情報処理やネットワーク接続化だけではなく、自動車外部の情報やネットワークを含めたサービスについても活用される段階にある。

一方で、2010 年には米国の研究者等により、自動車内外からの通信によって車載システムの脆弱性を攻撃することで、自動車の制御等に影響を与えることが可能であることが明らかとなった。この結果、信頼性とリアルタイム性が重要である等の車載システムと情報システムの違いはあるとは言え、認証や通信の秘匿等について脆弱な部分が存在することが解った。

今後、スマートフォンと自動車の連携や電気自動車やスマートコミュニティの普及を鑑みるに、自動車と外部ネットワークの連携はますます深まっていくと考えられる。自動車内外のネットワークからの攻撃によるインシデントが発生する事を防ぐため、自動車の開発や利用における情報セキュリティの重要性は高まってきている。IPA では 2006 年度から、組込みシステムセキュリティの一環として自動車のセキュリティについての調査・分析を行っており、その成果の普及啓発活動に取り組んできた。本レポートでは、近年の状況も含めた、自動車の情報セキュリティに関する現状と今後の対策について、主に自動車開発関係者に向けた解説を行うものである。

２．自動車の情報セキュリティの必要性が高まる背景

車載システムに対する情報セキュリティの必要性が高まる背景として、「スマートフォンの普及」「車載システムのオープン化」「電気自動車等の新しい自動車及び利用形態の出現」という、大きく 3 つの要因が考えられる。本節ではこれらについて解説する。

①スマートフォンを中心とした自動車とインターネット連携の動き

2010 年からスマートフォンの普及が加速している。スマートフォンと従来の携帯電話との違いは、ユーザでもアプリケーションを開発・提供することが可能であり、実用的なものから単純なものまで多様なアプリケーションが流通している点にある。海外では既に、スマートフォンが車内ルータとして利用されており、自動車向けのスマートフォンのアプリケーションも多く流通している。この結果として、信頼性の低いアプリケーションの脆弱性によりスマートフォンが踏み台となり、自動車の車載機やカーナビに損害を与えたり、スマートフォンを介した車内情報の漏えい等によって、運転者のプライバシを侵害するなどの危険性が想定される。また、スマートフォンを利用することで、自動車と外部ネットワークの常時接続や、海外のような車内ホットスポットが実現されれば、移動中の自動車に対して、外部からネットワーク・スマートフォンを介した攻撃が実施可能となることも考えられる。

スマートフォン以外にも、ETC（Electronic Toll Collection System）やスマートキーのように無線による接続や、電気自動車では充電プラグを経由した車載ネットワークとの接続も実装されつつある。その為、車載システムについても車外との通信を前提とした機能が開発されるであろう。このように、スマートフォンを中心とした通信環境の充実や、車外通信を前提とした車載システムの登場によって、自動車についても情報セキュリティ上の課題が発生する可能性がある。

②車載システムや車載 LAN 等におけるオープン化・汎用プロトコル等の利用促進

車載システムや車載 LAN が自動車の「走る・曲がる・止まる」という基本制御機能に与える影響が増加している。例えば、テレマティクス端末では自動車メーカが提供するサービスとして、ドアロックの制御のほか、エンジン出力の調整、ソフトウェアの更新サービスなどの機能を提供するものがある。

これらの機能の実現と併せて、コスト競争や汎用性確保のため、一部の車載システムにも Linux のような汎用 OS が利用されつつある。また、ドイツ政府から支援を受けた SEIS（Security Embedded IP-based System）等の活動によって、車載 LAN に対する Ethernet やそれに伴う TCP/IP の利用について研究開発が行われている。実用面でも、2008 年には BMW 社が車載診断インタフェースの一つとして Ethernet を搭載しており、ソフトウェアの書き換えに利用している段階にある。

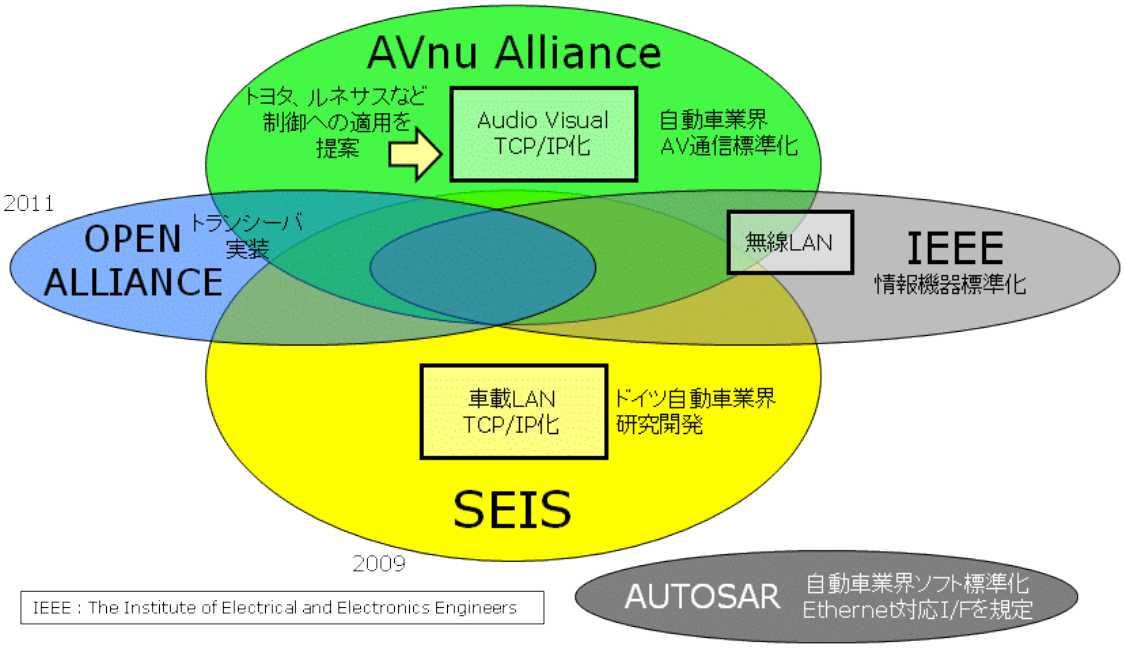

図 1. 車載 Ethernet の標準化に関する関連団体の関係

車載ネットワークの通信方式は電気的なレベルでは標準化されているが、要求命令や応答の内容など通信内容の意味については自動車メーカごとに異なることが多く、利活用の障壁となっていた。しかし、通信内容の統一化についての検討も始まりつつあり、今後車載ネットワークへの接続は容易になっていくと考えられる。自動車のネットワーク接続にインターネット等で利用されている標準規格の利用が進むことで、様々な車内外の機器や情報システムが繋がっていくことが考えられる。これによって、自動車の利用者が様々なサービスを利用することが可能になる一方で、通信内容の解析や攻撃の難易度が下がる事が考えられる。

欧州ではすでに車載ネットワークのセキュリティ対策として、EU のプロジェクトとしてセキュリティチップの開発を行っている。このセキュリティチップは、セキュリティ性能及び機能によって、「light」「medium」「full」の 3 つのレベルに分かれており、車載システムの機能や要件に従って、適切なレベルのものを選ぶ形となっている。この取組みは、現在は EVITA プロジェクトの後継となっている PRESERVE プロジェクトで実装を含めた研究開発が行われている。また、TCG（Trusted Computing Group）でも自動車への TPM（Trusted Platform Module）採用の検討が進展し、日本を含めた自動車関連企業が参画している。今後、このようなセキュリティチップもオープン化された車載システムで利用されていくことになると考えられる。

③電気自動車やカーシェアリングなど，自動車の新しい利用形態の発達

近年では電気自動車の利用も増えつつある。電気自動車では、既存のエンジン車に比べてエンジンとトランスミッション、ディファレンシャルが不要になり、代わりに数100Kg の重量がある電池を搭載するなど構成部品に大きな変化がある。また、自動車に比べて電力が潤沢に利用できる環境にあり、情報処理を行う車載システムを活用する幅も広がると考えられる。

電気自動車における大容量電池は高額であり、また充放電を繰り返すことで疲弊していく事から、電池の管理は大きな課題となる。このため、充電状況の監視や設定、過去の充電履歴等の管理のために、情報処理技術を利用していく必要がある。既に実装されている事例としては、電気自動車内部には充電状況履歴を残さず、ネットワーク上のサーバに蓄積するものがある。電池の充放電の回数と量などのデータを収集してサーバ上に積算するサービスでは、PHS（Personal Handy-phone System）または 3G/4G 携帯電話などの移動体通信機能(モバイル)が利用されている。米国ではこのような電気自動車の充電管理を行う情報等を利用して、カーシェアリングを実施する仕組みについて検討されている。

また、今後自動車が様々な情報を持つことで、利用者のプライバシと紐付けられていくことが考えられる。自動車が決裁のためにクレジットカード情報等を持った場合や個人情報はもちろん、例えば電気自動車のバッテリの充電場所・時間情報やカーナビのプローブ情報から、よく立ち寄る場所や個人の趣味嗜好などが割り出され、結果としてプライバシ情報となることも考えられる。その為、今後車載機に情報を格納するさいは、その情報の内容を鑑み、それに応じた暗号化や認証の利用等の情報漏洩対策を実施していくことが必要である。

今後、より情報技術を利用した自動車の普及や、昨今のエコドライブのような省エネを目指す風潮を受けた自動車利用の新しい利用形態を実現するためには、車載システムや車内ネットワークを含めた情報技術のさらなる活用が必須となる。そのため、情報技術の利用に応じた情報セキュリティの検討についても必要になってくると考えられる。

３．自動車に対する攻撃手法の IPA による分析

IPA では自動車に対する情報セキュリティ上の攻撃手法の分析を行う上で、図のような 3 つの経路があるとした。

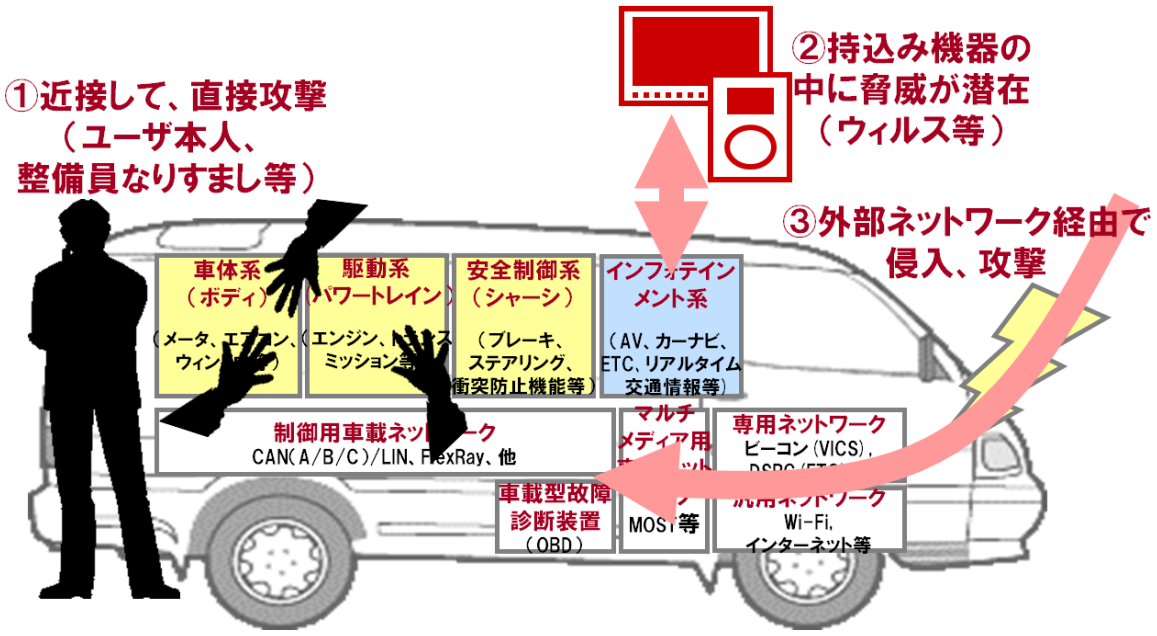

図 2．自動車に対する 3 つの攻撃手法

①直接攻撃

自動車はパソコンや携帯電話と違い、その大きさと性質から常に管理・監視下に置くことが難しい。その為、オフィス機器に比べて悪意ある攻撃者が直接自動車に触れることが容易であると考えられる。また、車検等のメンテナンス時には自動車の管理を整備員に任せねばならず、整備員になりすまされて直接自動車に攻撃を加えられる可能性がある。また、利用者自身の改造等によって、その意図の有無に関わらず自動車のセキュリティ機能が解除されることも考えられる。

②持込み機器における脅威

カーメーカが用意する自動車の機能の他に、自動車の利用者自身がアフタマーケット等で購入して自動車に設置する機器も多数用意されている。このような機器を着脱する際に、外部からウィルス等の脅威が持ち込まれる可能性がある。特にスマートフォンについては、自動車用の汎用的なアプリケーションを入手することが可能な一方で、海賊版や悪意あるコードを含んだアプリケーションも流通していることが明らかとなっている。今後、自動車が様々な機器と連携していく中では、自動車の中にも多種多様な機器が持ち込まれることが考えられるため、開発段階で予め脅威について検討しておく必要がある。

③外部ネットワークからの攻撃

自動車は利便性や安全性確保のために様々なセンサを持っており、それを利用して機能・サービスを実現している。スマートキーや車車間、路車間通信においては、通信距離は短いものの無線が利用されており、それらの傍受や悪意ある通信の割り込みといった脅威が考えられる。また、現在ではスマートフォンによる車載システムと外部ネットワークの常時接続が容易になってきていることや、車載システムのオープン化によって、外部ネットワークからの脅威が現実のものとなってきている現状にある。電気自動車では、充電する際には充電情報をネットワークに送り、状況や履歴を管理することが検討されている事から、運転中及び停車中に外部と常時接続が実現されている場合における脅威についても、検討しなければならない状況にある。

４．具体的な脅威の例

自動車の情報セキュリティ上の脅威が攻撃された被害に関しては未だ報告されていないが、米国の研究論文等では、自動車の情報セキュリティに対する攻撃が成功した事例が報告されている。ここでは、その内代表的なものを 3 つ解説する。

①車載ネットワークに対する直接もしくは持込み機器による攻撃事例

2010 年、実証実験に基づく論文「Experimental Security Analysis of a Modern Automobile」が公開された。この中では、自動車の保守点検用ポートに特別な機械を設置し、攻撃者が並走する車から車載システムの脆弱性をついた攻撃を行うことで、ブレーキやワイパーの制御に影響を与えられることが明らかにされた。この論文の中では、対象とした車載システムの行う通信の盗聴・解析が容易であったことや、通信の認証及び発信元アドレスが存在しないためなりすましが容易であったことが述べられている。また、本来であれば走行中は無視しなければならないコマンドが、走行中でも実行可能であったことが明らかにされた。

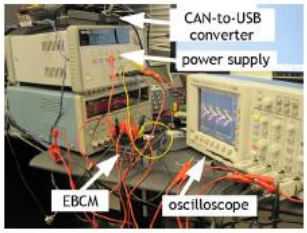

Figure 1. Example bench setup within our lab. The Electronic Brake Control Module (ECBM) is hooked up to a power supply, a CAN-to-USB converter, and an oscilloscope.


Figure 3. To test ECU behavior in a controlled environment, we immobilized the car on jack stands while mounting attacks.


Figure 7. Road testing on a closed course (a de-commissioned airport runway). The experimented-on car, with our driver wearing a helmet, is in the background; the chase car is in the foreground. Photo courtesy of Mike Haslip.

図 3. ECU 単体の解析(左)、静止時の車台上での ECU 間解析と試験(中)、
走行中の動作試験(右)

この脆弱性を悪用する攻撃を成功させるためには、情報セキュリティの専門知識と攻撃用ソフトウェアの開発能力、車載ネットワークに接続して任意の制御命令を注入するための電子基盤を作成する能力などが必要である。攻撃を行うための機材とソフトウェアは市販製品では機能不足のため新規開発が必要であり、現状では攻撃の難易度は高い。しかし、今後自動車の持つ情報資産の価値が高まり、悪意ある攻撃者たちにとっての攻撃対象となった場合は、現状の情報セキュリティ動向と同様に、攻撃を簡易化するツールが出回るといった事も考えられる。

②タイヤ空気圧監視システムへの攻撃事例

タイヤ空気圧監視システム（TPMS : (Tire Pressure Monitoring System)）はタイヤの空気圧を常時監視するシステムである。米国で初めて自動車への搭載が義務化され、空気圧が低いタイヤで高速走行をすることによるタイヤバースト(破裂)事故を防ぐ効果が期待されている。本システムではタイヤの特性上、無線通信によりタイヤの空気圧データを収集している。

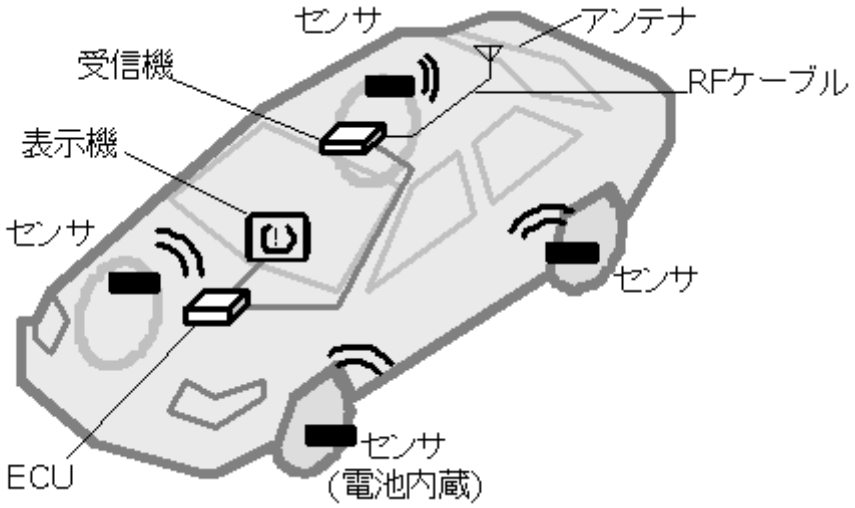

図 4. TPMS の構造

この TPMS の脆弱性を指摘する論文が、2010 年に米国で発表された「Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study」である。この研究では、TPMS の無線通信を解析し、以下の 3 点についての指摘を行っている。

1．TPMS では通信メッセージは暗号化されていないため、盗聴・解析が容易。
2．タイヤのバルブに装着した空気圧測定装置は 32bit の固有の ID を持つとともに自動車本体から 40m 離れても無線通信が可能であった。このことから路肩や高架橋などで測定すれば、特定の自動車がいつ通過したかを記録することができる。
3．TPMS の空気圧報告メッセージになりすますことができ、いつでも警告灯を点灯させることができる。

この解析は専門の知識を持つ学生が 1 週間以上かけて開発を行ったものであり、高い専門性を必要とする一方で、解析に利用した機材のコストは 1,000 ドル程度と高額では無い。

一般的な自動車に対して、安全性向上のために導入されるシステムにおいては、脆弱性の顕在化は人命にも関与する問題となるえるため、より一層の注意が必要であるといえる。

③広域ネットワークを利用した車載ネットワークへの攻撃事例

2011 年には、これまでの自動車に接触もしくは近距離からの攻撃に加え、携帯電話に繋がっている自動車に対して、遠隔地から攻撃を行う手法についての論文「Comprehensive Experimental Analyses of Automotive Attack Surfaces.」が発表された。この中ではこの攻撃に依る様々な影響について検討されているが、中でも遠隔地からのドア解錠や、悪意ある攻撃者による自動車の監視については、被害が大きくなるものと考えられる。この攻撃手法を図にしたものが、図 5 である。この攻撃では、始めにテレマティクス車載機に関して不正アクセスを行い、脆弱性を利用して遠隔操作用のクライアントを立ち上げる（図 5 中 1～5）。その後、立ち上がった遠隔操作用クライアントに対して、自動車の制御に関する任意のメッセージを送る事によって、遠隔地からのドアロック解除やエンジンスタートを実施するものである。

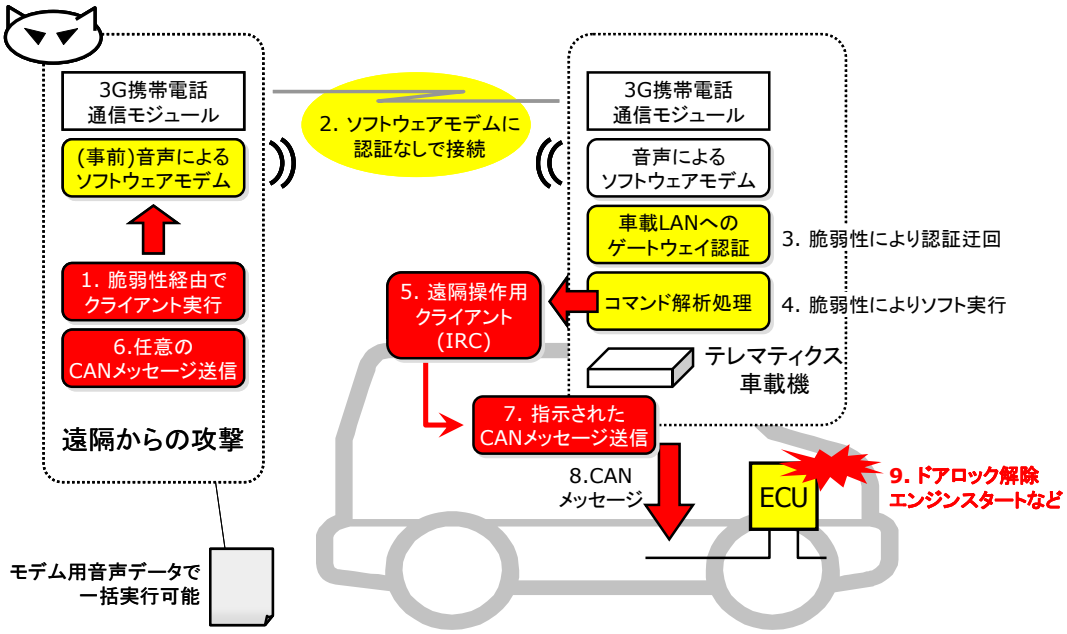

図 5. 遠隔地から自動車への攻撃例

本攻撃には、リバースエンジニアリングを利用してテレマティクス端末を解析した上で、特定の車種に対する侵入コードと実行コードを開発しており、攻撃の難易度としては高いものである。しかし、大手テレマティクスサービスの攻撃コードが開発され、それが流布された場合、被害が広範囲にわたることが考えられる。

攻撃に対する対策として、「外部からの不必要な通信を遮断する」「不要な通信サービスについては機能として削除する」「車載システム開発時にセキュアプログラミングの概念を持つ」「ソフトウェアアップデート手法を持つ」「複数の機能が連携した場合のセキュリティを検討する」ことなどが挙げられており、情報システムと同様の情報セキュリティ対策を実装することで被害を防ぐことが可能である。

５．自動車の脅威の分析

IPA では自動車の機能及びその周辺機器について、自動車が持つ８つの機能（図中 A～H）と持込み機器（図中 I）、そして自動車と持込み機器を繋ぐ経路（図中 J）の大きく 10 の要素に分類し、それぞれに対する脅威の分析を行ったものを図 6 にまとめた。図ではネットワーク接続手法を整理するために車載ネットワークを最大限に抽象化し、図中中央の太線ように１本の線で表現した。図の下側は主に標準的に自動車に搭載されている機能で、ECU、センサ、アクチュエータにも直接的、間接的に接続している。これらの機能は一部が規制によって技術基準が標準化されていたり、搭載が義務化されていたりするものである。図の上側は主に自動車にオプションとして提供されたり、利用者が後から追加して搭載する機能として整理した。図中右端の持込み機器は、利用者が自動車内に限らず利用するもので、それらと車載ネットワークは、Bluetooth や無線 LAN などの通信経路を通じて接続される。

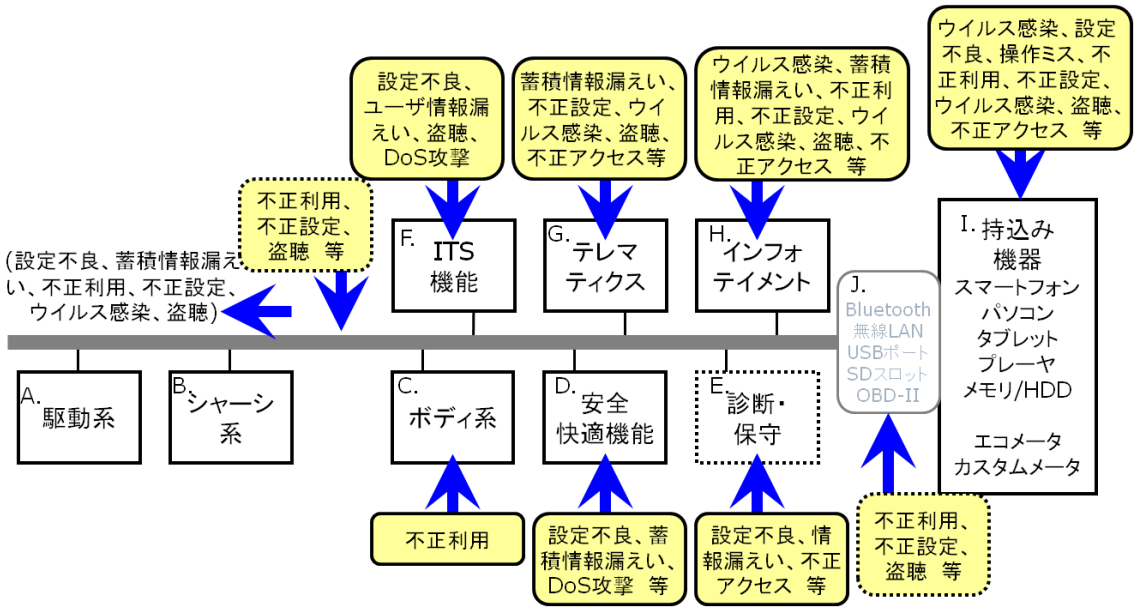

図 6.　一般的な自動車における脅威の分析

自動車の機能について、その利用用途や重要性から大きく 3 つに区分した。それが図中に点線で区分した、「基本制御機能」「拡張機能」「一般的機能」に分けた。

「基本制御機能」は自動車の基本かつ必須の機能である「走る・曲がる・止まる」機能にあたり、セーフティに大きく影響する。「拡張機能」はセーフティ確保を含めた運転支援及び快適性向上のための機能で、それぞれについて情報セキュリティ的な被害を受けた場合には個別に停止または車載制御システムから遮断してもかまわないと考えられる機能である。「一般的機能」は自動車の外部からの持込み機器からなり、ほとんどが自動車用ではない一般的な情報家電機器などである。

自動車の利用者に与える影響を考えると、「基本制御機能」を情報セキュリティの脅威から優先的に保護することが求められる。「拡張機能」にはドアロックなどを含むボディ系機能など重要な機能はあるが、「走る・曲がる・止まる」機能には直接影響しない。一般的機能は現在のところ自動車の「基本制御機能」に直接接続するような機能はない。

さらに、それぞれの機能に対するセキュリティ上の脅威について洗い出した。「拡張機能」や「一般機能」については、現在の一般的な情報セキュリティ上の脅威が考えられる。一方で、「基本制御機能」に対しては直接的な攻撃手段は現状では考えられないものの、拡張機能を踏み台にした攻撃が可能であることが事例として存在する。

車載システム及びその周辺機器及びサービスを開発・提供する際には、それが影響する範囲のセキュリティ課題について検討し、適切な対策を取り入れていくことが望まれる。

６．自動車の安全を守るために

以下に今後、自動車のセキュリティ対策を実施するための３つの指針を示す。

①ユーザへの適切な情報提供

今後、自動車と連携したサービスが増えてくるに従って、自動車及びその周辺機器が様々な情報を持ち、それぞれが自動車内外のネットワークに繋がっていくことが考えられる。その中では、自動車の利用者が「自分の身は自分で守る」という意識を持つことが必要である。その為に、スマートフォンやカーナビ、テレマティクス車載機などの機器を利用したネットワーク経由でのサービス内容のほか、常時接続やソフトウェア書換え、機器制御の有無などについて把握し、サービスや機器が停止した場合の影響や、利用者が注意すべき点について整理する必要がある。また、整理された情報を様々な手法でユーザに通知していく努力も必要となる。

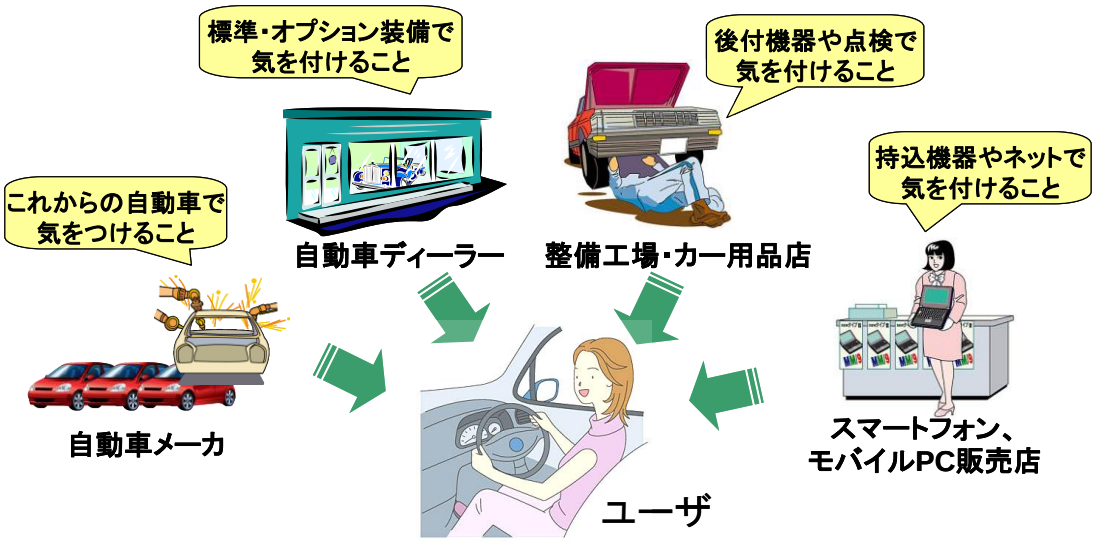

図 7. ユーザへの適切な情報提供

現在、スマートフォンやテレマティクスによる自動車向けサービスは日々進化しており、サービス内容も多様化するとともに、プライバシに関する情報を扱うなど、リスクがあるものも多い。今後新しい機器やサービスが発達していくに従って、それに応じた情報資産や脅威が発生することが考えられる。そのため、新しい機器やサービスについて、適宜、それらを利用することの利点とリスクを把握するとともに、ユーザに周知していくことが必要である。

②悪意ある攻撃への備え

自動車のセーフティについては、「機能安全」を実現するための国際標準規格がISO/DIS（International Organization for Standardization / Draft International Standard）26262として策定され、基本的な設計手順や基準が整えられている。しかし、自動車が様々な通信手法を持ち、それを活用した技術が発達する中では、現在の自動車は故障や過失だけでなく、悪意のある攻撃者からの攻撃への対応が必要である。

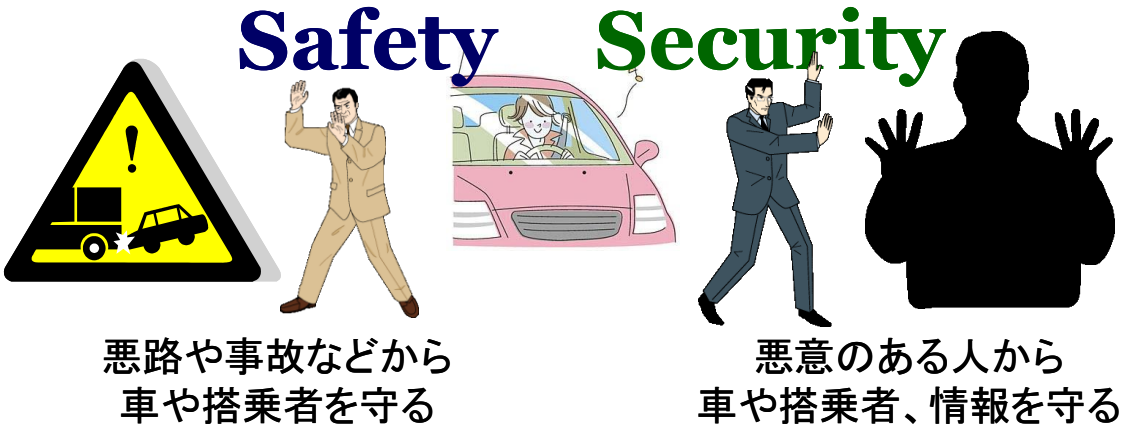

図 8. 悪意ある攻撃の認識

海外の研究事例でもあったように、安全に関しては検討されたものであっても、悪意ある攻撃に対してはまだまだセキュリティ対策が未実装である製品も存在する。今後、車載システムが汎用的になり、ネットワークに繋げられていく中では、セーフティ同様、情報セキュリティに対しても適切かつ十分な対策が必要である。

また、情報通信技術の進展により自動車の情報化も急速に進展しており、さまざまな機能やサービスが追加され、自動車には「走る・曲がる・止まる」に留まらない価値が生まれている。これによって、自動車は今までの盗難や車上荒らしといった直接的な攻撃だけではなく、情報漏洩や盗聴等の情報システム上の攻撃にさらされる可能性も高まってきている。実際に、情報セキュリティ研究者の間では、自動車の情報制御システムに対する攻撃の動機の高まりによって、自動車が「次のハッキングの開拓地」になると予測されている 。

数年以内には実用化されると見られる自動運転機能や自動ブレーキの普及や、日米欧で導入が進む ITS 等のための車車間通信や大規模な遠隔制御などについて、それを対象とした攻撃や対策について、事前にしっかりと検討することが重要となる。

③今すぐ始めるセキュリティ対策

大規模化・分散化しつつある車載システムにおいて、抜けの無い情報セキュリティ対策を実施することは簡単ではない。また、深刻なリスクを緩和しないまま製品を市場に送り出した結果、脅威が顕在化した後にセキュリティ対策を実施すると非常に大きなコストがかかる。特に自動車はパソコンやスマートフォンのような情報機器と比べて、利用期間が長いため、開発時に見落とされてしまったセキュリティ上の脅威が、利用時に顕在するリスクも高い。そのため、自動車の情報セキュリティにおいて先行している欧州の研究開発事例や、生産設備などを対象とした制御システムセキュリティの対策、家電やスマートフォン等の組込みセキュリティの対策を参考に、自動車の情報セキュリティについても、今から検討を始める必要がある。

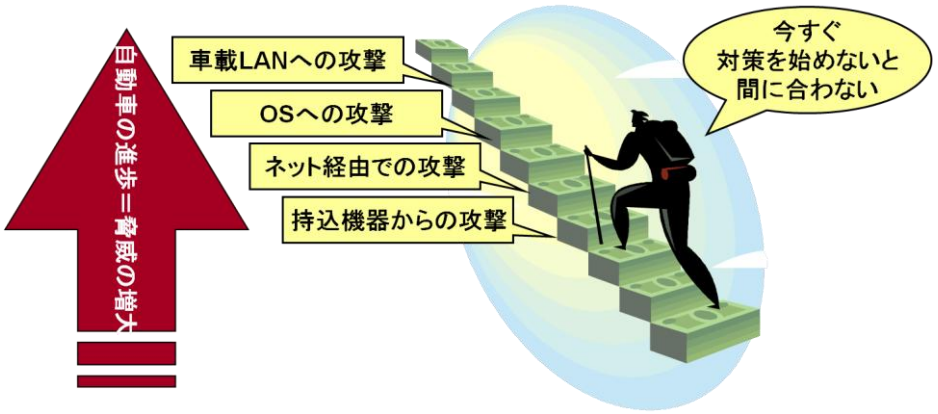

図 9. 今すぐはじめるセキュリティ対策

今後、自動車にも Ethernet や TCP/IP 等の標準化された技術や、汎用 OS の利用等によって自動車特有のプロトコル等が減ると、攻撃者が車載情報システムの解析を行う事が容易になる。また、オープン化による技術的な障壁が解消されると、自動車と連携した様々なサービスが展開されることとなり、自動車の持つ情報の価値も高まると考えられる。その為、自動車関連機器及びサービスを企画・開発する段階から製品の内部に攻撃を防ぐか、攻撃が成立しないようなしくみを取り入れる必要がある。そのため例えば通信メッセージの暗号化や通信先の ECU などの認証を行うことがあるが、こうしたセキュリティ機能の実装は機能の検証や相互運用性の確保の点で難易度が高い。セキュリティ機能を利用する場合はできるだけフレームワークなどの開発支援環境の上でカプセル化された機能を利用するなど、開発プロセスに簡単に取り入れる必要がある。

一方で、自動車におけるオープン化とネットワーク接続は、攻撃の糸口となることで脅威をもたらす面があるが、適切に利用することでソフトウェアの実行環境を安全に保つことができる面もある。例えば、オープンな技術が繰り返し利用される事によって、その技術を利用する上でのセキュリティ上の懸念点が洗い出され、技術として洗練される事が期待される他、汎用的なセキュリティ対策を導入する事が可能となる。また、ネットワーク接続によって車載ソフトウェアを適切に更新することで、既に出荷されて運用段階にある自動車に対して、車載システムの不具合や脆弱性を解消し、情報セキュリティを保つことができる。

自動車の情報セキュリティは対象範囲が従来から広い。車載制御システムの開発組織を基本としているが、スマートフォン等の後付けのデバイスや自動車の情報を利用したサービスベンダなど、自動車を利用する上では多数の組織がその開発・運用に関わっており、規模が大きい。また、車室内での音声・ビジュアル・その他情報処理、持込み機器の接続と連携、移動しながらの無線通信、クラウドやスマートグリッドとの協調など他の分野への広がりもある。このような広い範囲かつ強力な敵に対して自動車業界だけで情報セキュリティの対応を実施することは難しい。それぞれに対応する業界組織や標準化団体と連携して、自動車の情報セキュリティ対策を実現する必要がある。そのために自社内に限らず、自動車に関連する他組織の情報セキュリティ対策の情報交換と、協調した行動が必要である。

このような他組織との連携や、システム及びセキュリティの標準化を行う為には多大な時間が必要であると考えられるため、自動車に対するセキュリティ対策に関しては今すぐにでも検討を開始しなければならない。

7．まとめ

今後、より安全で便利な自動車社会の形成に向けて、自動車の情報セキュリティについて、調査・分析を進めるとともに、その普及のための活動を続けていくことが望まれる。海外の事例等を見ても、自動車の情報セキュリティに関する検討は進んでいるというわけでは無く、これから力を入れて分析・検討していくことが必要であると考えられる。IPA でも 2006 年度より組込みシステムのセキュリティとして、自動車関連機器の情報セキュリティについて調査してきたが、その中では自動車の脅威分析に CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）を利用する手法や、自動車を含めた組込みシステムを利用する上でのガイド「組込みシステムのセキュリティへの取組みガイド」の提案を行っている。このような取組みが自動車に関する情報セキュリティの向上に向けて寄与できるよう、今後も活動を続けていく予定である。

参考

・2007 年 5 月 10 日公開：
組込みシステムの脅威と対策に関するセキュリティ技術マップの調査報告書
http://www.ipa.go.jp/security/fy18/reports/embedded/index.html

・2008 年 1 月 29 日公開：
複数の組込み機器の組み合わせに関するセキュリティ調査報告書
http://www.ipa.go.jp/security/fy19/reports/embedded/index.html

・2009 年 3 月 10 日公開：
自動車と情報家電の組込みシステムのセキュリティに関する調査報告書
http://www.ipa.go.jp/security/fy20/reports/embedded/index.html

・2010 年 4 月 15 日公開：
国内外の自動車の情報セキュリティ動向と意識向上策に関する調査報告書
http://www.ipa.go.jp/security/fy21/reports/emb_car/index.html

・2010 年 9 月 7 日公開（2011 年 2 月 22 日英語版公開）：
組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）
http://www.ipa.go.jp/security/fy22/reports/emb_app2010/index.html

・2011 年 4 月 26 日公開：
2010 年度 自動車の情報セキュリティ動向に関する調査
http://www.ipa.go.jp/security/fy22/reports/emb_car/index.html

・2012 年 5 月 31 日公開
2011 年度 自動車の情報セキュリティ動向に関する調査
http://www.ipa.go.jp/security/fy23/reports/emb_car/index.html