TOKIO MARINE NICHIDO
リスクマネジメント最前線
2014 | No.39

自動車に対するサイバー攻撃の危険性と対策

近年、コネクテッドカーと呼ばれる、何らかの通信機器が備えられた車両が急増しつつある。IEEE[1](米国電気電子学会)によると、2025 年には全車両の 6 割がコネクテッドカーになると予測されている。また、追突防止装置等の ASV(先進安全自動車)機器も普及し、自動車の情報化が急速に進んでいる。しかしそのような中で、自動車の新たなリスクとしてサイバー攻撃の危険性が指摘されている。

本稿では、自動車の進化について概説するとともに、自動車に対するサイバー攻撃の現状と、今後の対策の方向性について解説する。

1. コネクテッドカーの普及と自動車の進化

コネクテッドカーの普及が進められているのは、通信により幅広い分野で自動車の利便性が拡大するためである。具体的には、自動車への通信接続によって、SNS、ナビゲーション、安全運転支援等の多岐にわたる機能が車内で利用できるようになる。

例えば、スマートフォンの OS を開発している Apple 社（iOS）と Google 社（Android）は、ともに自動車との連携を強めており、スマートフォンと自動車との通信接続が、2015 年以降本格的に普及する見込みである。スマートフォンと自動車の通信接続により、スマートフォン上で利用されている様々なアプリケーションが、車載モニターを通じて利用できるようになると考えられる。

自動車との通信による価値としてもう一つ強く進められているものが、事故時緊急通報である。欧州では、eCall[2]という事故時緊急通報機能の車両への搭載義務化が、2015 年の開始にむけて検討されている。また近年、衝突防止装置等の安全運転支援機器の導入が進んでおり、さらに通信接続により、車々間通信[3]等の ITS（高度道路交通システム）導入も進み、より安全な交通システムの実現が期待されている。

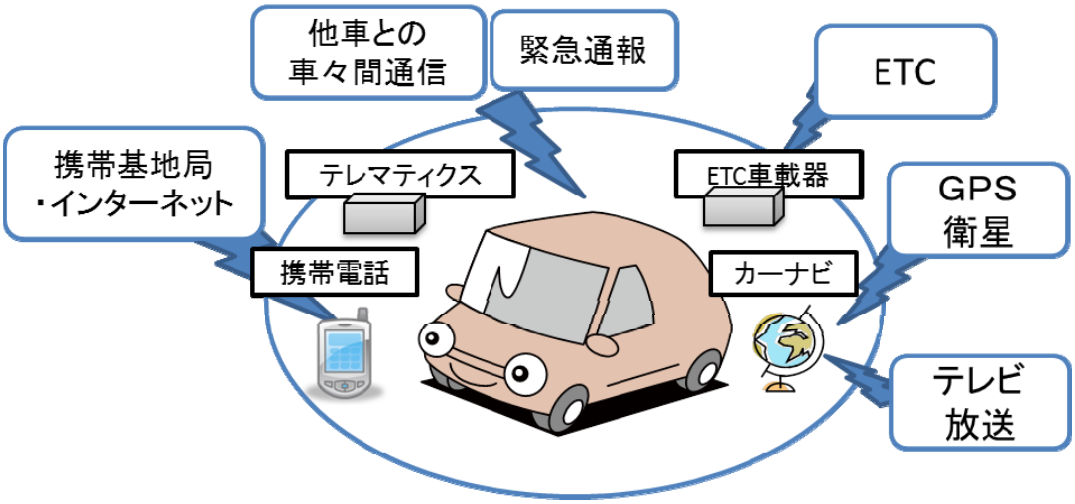
通信接続は、自動車の利用価値を大きく向上させ、今後、上述したような新たな付加価値が見い出されることは間違いないが、自動車の高度情報化は必ずしも良い点だけではない。これらの情報機器が自動車に組み込まれることによって、自動車を管理するうえで、サイバーセキュリティの観点からの対策が必要になるのである。

---

1 IEEE http://www.ieee.org

2 eCall http://ec.europa.eu/digital-agenda/en/ecall-time-saved-lives-saved

3 車両同士が、位置やブレーキ操作等の情報を共有し、危険回避等につなげる技術。



■図１　自動車とつながる機器と通信の例（弊社作成）

2. 自動車へのサイバー攻撃

いわゆる自動車へのサイバー攻撃については、実際に起こりうるのはまだかなり先のことである、と考える向きが多いかもしれない。しかし、それは誤りである。自動車にはすでに様々な情報機器が組み込まれており、電子的な攻撃によって多様な被害を起こしうる。そして、実際に、すでに自動車に対する電子的な手法による攻撃が発生している。

最もわかりやすい例は、イモビライザーに対する攻撃である。イモビライザーとは、近年自動車の鍵に組み込まれるようになった機能で、鍵に IC チップを組み込むことで、エンジンを点火する際に ID の認証を行い、不正な情報を感知した場合にエンジンがかからないようにするものである。当初は絶対に破れないとされていたが、現在では簡単に解除できてしまう機器が不正に製造・販売されており、実際に盗難被害が発生している。

しかし、より大きな話題となったのは、カリフォルニア大学の Savage 氏とワシントン大学の河野氏らの研究によって遠隔から車載 LAN に進入できることが実証された[4]、という 2011 年の発表である。このような攻撃方法は、実際にはまだ行われておらず被害は発生してはいないと考えられるが、この研究では、携帯電話回線・ラジオ回線・Bluetooth 等の種々の方法により、ドア開錠・エンジン停止・車載パネルへの誤表示・車内の音声記録／位置情報の取得等を不正に実行できることが実証された。また 2013 年には、twitter 社の Charlie 氏と IOActive 社（セキュリティサービス企業）の Chris 氏らの研究により、実際に販売されている車に対してコンピューターによる攻撃を行い、エンジン停止等を不正に操作できることが示された[5]。さらに、2014 年には同じく Charlie, Chris らによって、Bluetooth の脆弱性を用いて車外から侵入し、自由な車両操作ができることが実証されてい

[4] Comprehensive Experimental Analyses of Automotive Attack Surfaces, CAESS, Stefan Savage, Tadayoshi Kohno ほか、2011-06-03

[5] Charlie M., Chris V., Adventures in Automotive Networks and Control Units DEFCON21,(2013)

る[6]。現在の自動車は、サイバー攻撃の観点から見ると、安全ではないと言えるだろう。

先に挙げたような攻撃は、車両のシステムに侵入するものである。しかし、情報化された自動車への攻撃方法はそれだけではない。

例えば、現在想定されている車々間通信として、前方の自動車が急ブレーキをかけた場合、後続車も急ブレーキをかけるように動作する、という案がある。これは、後続車から見えにくい箇所にある危険に対処する方法として有用である。しかし逆に言えば、「他車が急ブレーキをかけた」という事実がなくても、急ブレーキになりすましたシグナルを発することで、周囲の車両を意図的に止めてしまうことができる、ということを意味している。

また、より直接的な方法として、センサーに誤検知させるという方法がある。現在利用されている衝突防止装置は、代表的な安全運転支援装置のひとつであるが、カメラやレーダー等、いくつかの方法で前方を検知している。すなわち、センサーを電波等の何らかの手法で妨害し、前方に障害物があると誤認させれば、任意の自動車に急ブレーキをかけさせることができると考えられる。ここで着目すべきことは、対象の車に対するハッキングが必須ではないという点である。安全運転支援装置を搭載した自動車に対して、本来車内からしか行うことのできなかった操作を車外から行うことができる可能性が示されている。

表１に、上記のとおり紹介したもの以外にも、現時点で発生した、あるいは危険性が指摘されている自動車および交通環境へのサイバー攻撃とその発生状況の例をまとめた。今後、コネクテッドカーの普及により、同様の事例の増加が予想される。

■表１　現時点で発生または危険性が指摘されている車・交通環境へのサイバー攻撃の例

被害概要	攻撃概要	発生レベル
車両盗難	イモビライザーを特殊機器で無効化	犯罪発生
	リモートキーロックを電波妨害または電波中継し無効化	犯罪発生
遠隔操作による車両の利用停止	イモビライザーを遠隔起動し、車両を移動不可にする	犯罪発生
運転支援機器の外部からの作動	相手車両システムへの不正侵入、または悪意ある通信・電波により、運転支援機器を外部から作動させる	危険性指摘
他人による車両の自由な操作	Bluetooth 回線等から車両制御システムへ侵入し、ドア開錠や表示パネルの改ざん、任意のアクセル・ブレーキ・ハンドル操作等を実施	実験的に実証
車内情報漏えい	警察車両の車内からの撮影映像を無線で盗聴	漏えいを研究者が実証
信号機の表示書き換え	文字表示可能な交通掲示板に任意の文字を表示	犯罪発生

※本表は一例を示すものであり、網羅性を保証するものではない。

出典：生活機器の脅威事例集[7]、2011 年度自動車の情報セキュリティ動向に関する調査[8]等をもとに弊社作成

6 Charlie M., Chris V., Black Hat conference(2014)

3. 企業および自動車利用者が行うべき対策

これらのサイバー攻撃に対し、国や企業は対策に乗り出している。2014 年 11 月 6 日には衆議院本会議において、サイバーセキュリティ基本法が可決・成立しており、今後、犯罪対策や国民への啓発活動が進められていくものと思われる。また、多くの車両メーカーでは、サイバーセキュリティの担当者が新しく雇用され、対策の研究を進めている。しかし、これらの対策を有効にするためには、国や企業とともに、自動車利用者自身で対策を実施することも必要である。

利用者がとるべき対策は、基本的にはコンピューターの利用時と同じものが想定される。具体的には､会社で承認されていないUSBメモリーやスマートフォンなどを自社ネットワークに繋げない、怪しいファイルを開かない、OS やソフトのセキュリティ更新を徹底するといった対策の他に、独立行政法人 情報処理推進機構(IPA) やセキュリティに関するニュースサイトで常に最新の情報を確認し、指示されたセキュリティ対策をすぐに実行する、といった基本的な情報機器の管理であり、これらの対策は、自動車の情報化においても今後必要になると思われる。

また、自動車の情報化が今後もますます進むことは明らかであるが、それにより、自動車の利用時や、機器の購入時に新たな課題が多数生まれることが予測される。例えば、

・社員個人の所有するスマートフォンと社有車の接続により、リスクがもたらされないか

・車両の通信を利用したサービスのパスワードはどう管理すればよいのか

・新たにカーナビを購入した時に、このカーナビが不正なソフトウェアの入り口にならないか

といった課題の検討が必要になることが予測される。今後の自動車管理に当たっては、機器に対する適切な使用管理と、社員のセキュリティ・リテラシーの啓発を意識していく必要がある。

自動車の管理においても、セキュリティ面の管理能力が必要であることは間違いない。しかし IPA の試算では、現在日本にはセキュリティの専門家が８万人不足しており[9]、企業における人材の確保は喫緊の課題となっている。これは検討段階ではあるが、免許試験や更新の際に、セキュリティ指導を項目として取り入れる必要性も議論されている[10]。今後は、自動車の利用者には、これまでのように車両整備の知識だけではなく、セキュリティに関する知識が求められることになる。さらに企業においては、自動車のセキュリティ運用計画の策定が求められる。

IoT(Internet of Things：モノのインターネット)の発展とともに、情報がインターネット上に配置される規模は今後一段と拡大していく。企業の経営者や総務部門においては、自動車の利用にあたって、今後はセキュリティ意識の啓発と、対策を実施できる人員が必要になる可能性が高いことを意識していただきたい。起こりうる犯罪の種類は拡大しており、これまで想像もできなかったような事件が発生する可能性もある。例えば、トレンドマイクロ社[11]は、自動車をハッキングして、身

---

7 「生活機器の脅威事例集」　重要生活機器連携セキュリティ研究会

8 「2011 年度自動車の情報セキュリティ動向に関する調査」　独立行政法人 情報処理推進機構 (IPA)

9 「サイバーセキュリティ戦略」 IT 戦略本部情報セキュリティ政策会議

10 「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」IPA

11 「潜在する脅威の顕在化トレンドマイクロ 脅威予測 2015 年とその後」 TrendLabs

代金目的で運転手を閉じ込めてしまう犯罪が起こる可能性を示している。さらに、自動車へのサイバー攻撃を踏み台にして、その自動車を所有する会社のシステムそのものへの侵入を行う等、自動車が情報システムの新たな穴となることも考えられる。今後の自動車の高度情報化に伴い、自動車のサイバーセキュリティ管理は、自社のためだけでなく、より安全な社会の実現のためにも必須となる。

本稿が、企業と自動車利用者にとって、自動車のサイバーセキュリティへの取組みを始める契機となれば幸いである。

［2014 年 12 月 22 日］

～ コネクト社会で広がるリスクとソーシャルエンジニアリング ～

自動車の通信接続と同様、あらゆるものの接続が進んでいる。IoT(Internet of Things:モノのインターネット)と表現されるこの動きは、複数の機器が取得する情報を連携させることで、新たな価値を生み出そうというものである。

しかし、ここには大きなリスクが潜んでいる。多数のものが接続されるということは、重要な情報に行きつくルートが増加することを意味する。すべてのルートが十分に防護されれば良いが、その中に一点でも脆弱な部分があれば、それを経由してシステムの内部に侵入される可能性がある。

例えば、スマートフォンに対するウィルス等はすでにインターネット上に多数存在するため、利用者がマルウェア(悪意あるソフトウェア)とは認識せずにダウンロードしてしまうことがありうる。ウィルスに感染したスマートフォンとの接続の結果、攻撃ルートが多様化し、より進入が容易になる可能性があることは否めない。自動車に搭載するカーナビに、製造時にマルウェアが埋め込まれた例があり、さらに特殊な例では、衣服に使用するアイロンにマルウェアが埋め込まれた例がある[12]。このように、製品を通じて個人が所有するデータ全体への感染拡大・侵入が発生すれば、その被害は単独製品にとどまらない。

ここで何よりも意識しておかなければならないことは、サイバー攻撃が高度な技術と知識を持った者のコンピューター操作のみによって行われる、というのは誤解であるということである。他人からパスワードを聞き出したり、あるいは自らの望む操作を他人に行わせたりすることで不正に利益を得る方法には、コンピューターの知識を必要としない方法も多い。例えば、メール等を利用して偽サイトに誘導し、パスワードやクレジットカード情報を入力させるフィッシング詐欺や、他人になりすまして利用者に機械を操作させるオレオレ詐欺等は、高度なコンピューター技術によってシステムを攻撃するのではなく、利用者を騙す従来からある手法である。このようにパスワードを聞き出す手法は多数生み出されており、「ソーシャルエンジニアリング」と呼ばれている。

■図2 パスワードを聞き出すソーシャルエンジニアリングの例(弊社作成)

このようにサイバー攻撃は、良く知られているように純粋に機械的脆弱性を利用する攻撃だけでなく、他人から重要情報を聞き出す手法も組み合わせることで行われるのが、昨今の実態である。近年は、機器自体のセキュリティ向上はもちろんであるが、それを利用する人間のセキュリティ・リテラシーを向上する必要性が飛躍的に高まっている。

12 「つながる IT 社会の安心・安全の確保に向けて」重要生活機器連携セキュリティ研究会

東京海上日動リスクコンサルティング株式会社
自動車リスク事業部
〒100-0005 東京都千代田区丸の内 1-2-1 東京海上日動ビル新館 8 階
Tel.03-5288-6586 Fax.03-5288-6628
http://www.tokiorisk.co.jp/

