# 自動車に対するサイバー攻撃の危険性と対策（第２報）

近年の自動車は高度な情報処理用のコンピュータを内蔵し、また、インターネットと接続を行う機能を持つものが非常に多い。これは自動運転をはじめとするASV（Advanced Safety Vehicle：先進安全自動車）の制御や、車内の情報端末表示のために活用されている。自動車がより安全・快適な移動手段になってきていると同時に、「動くコンピュータ」としてサイバー攻撃の危険性にさらされていることを意味する。

前回、弊社発行の本誌「自動車に対するサイバー攻撃の危険性と対策」（2014年12月22日）[1]にて、自動車に対するサイバー攻撃によって、車両からの情報漏えいや、車両が遠隔操作される危険性があることを示した。発行後、実際に市販車に対する遠隔操作が可能であることが研究者によって発見され、自動車のリコールやソフトウェアのアップデートという形でメーカーが対応を迫られるケースがみられた。

そこで本稿では、自動車に対するサイバー攻撃に関する第２報として、2015年中に発生した事案を中心に紹介し、車両利用者における対策について解説する。

## １．市販車で実際に行われた攻撃

### （１）テレマティクスサービスへの攻撃

まず、テレマティクスサービス[2]への攻撃が可能なことが証明された事例を紹介する。一例として、ゼネラルモーターズ（GM）社の「OnStar」というサービスへの攻撃が可能であることが示された[3]。「OnStar」はスマートフォンのアプリ上で車両の鍵の開閉、エンジンのオンオフ等ができるというサービスである。このサービスの無線通信を偽装して第三者が車両の遠隔操作を行うことができることが示され、GM社はセキュリティ対応を迫られた。GM社に限らず、他の会社の同種のサービスにおいても同様の脆弱性が発見されている。

このようなテレマティクスサービスを経由した攻撃の中で最もセンセーショナルだったのは、クライスラー社の車両において、無線通信による攻撃によってアクセル・ブレーキの操作やエンジンの停止等、ほとんどの動作をコントロールできる脆弱性が発見されたことである。

これはテレマティクスサービスの脆弱性を踏み台に車内ネットワークに侵入し、ソフトウェアを書き換えることで、第三者による操作を可能にするもので、その後のクライスラー社のリコールにつながった。車両へのハッキング対策を目的としたリコールとしては世界初の事例である。ただし、先のGM社の例からもわかるように、これは特定の会社に限ったものではない。現在、主要な車両メーカーは全てテレマティクスサービスを展開しており、同様の危険性をはらんでいる。

---

[1] http://www.tokiorisk.co.jp/risk_info/up_file/201412221.pdf

[2] 自動車内の機器と携帯電話回線を利用して情報をやりとりして行われるサービスの総称。位置情報、車両挙動のアップロードやインターネットページの表示、車両の遠隔操作等を提供するものが多い。

[3] http://gigazine.net/news/20150731-ownstar/

### （２）アフターマーケット機器への攻撃

異なる手法が取られた攻撃として、OBD2 端子[4]を経由した攻撃も発見された。近年、この端子に接続し、燃費管理や安全運転評価を行うアフターマーケット機器がいくつも販売されている。攻撃の対象となったのは、GM社のシボレーにアメリカの保険会社 Metromile 社が配布していた OBD2 端子に接続する装置を設置した車両であった。Metromile 社は自動車の運転の仕方に合わせた保険料を請求する商品を販売しており、その保険料算定ツールとしてフランスの Mobile Devices 社が開発した装置の配布を行っていた。この装置は利用者の運転情報を保険会社に無線通信で送信する機能をもっていた。

今回発見された攻撃は、この装置の脆弱性を利用して無線通信から車内ネットワークに侵入するものであり、スマートフォンのショートメッセージサービスを使用するだけでブレーキを操作できることが示されている[5]。この事例は、アフターマーケット機器により、脆弱性が付加されることがあることを立証した意味で重要である。現在はカーナビやドライブレコーダー等、多種多様な機器を車両に搭載することができるが、これらの機器を正規ディーラー以外から購入するケースも多く、そのような機器の取り付けが脆弱性を拡大しうるといえる。

■表１　2015 年に発見された車両に対するハッキング手法例[6]

| 攻撃方法 | 対象となったメーカー |
|---|---|
| テレマティクスサービスへの<br>侵入による遠隔操作 | クライスラー |
| テレマティクスサービスの<br>乗っ取りによる遠隔操作 | GM<br>BMW<br>ダイムラー<br>クライスラー |
| 車両内部からの<br>悪意あるコードの実行 | テスラモーターズ |
| テレマティクス機能をもつ装置を<br>経由した車両の遠隔操作 | GM |

## 2. 自動車メーカーや関連業界による対策の動き

これらの脆弱性に対し、メーカーは種々の対策を迫られた。先に挙げたような攻撃は、日々新たな手法が発見される。そのため、セキュリティアップデートが頻繁に必要になる。特に 2015 年、無線通信によるセキュリティアップデートは自動車関連業界で大きな広がりをみせた。例えば、テスラモーターズ社はクライスラー社と同様、外部からの攻撃が可能なことが証明され、リコールによる対応ではなく、無線アップデートによる対応を行った。このようなソフトウェアに対するアップデートは今後、自動車においても当然のものとなると思われる。

---

[4] On-Board Diagnostics second generation／車両診断コネクタ

[5] http://gigazine.net/news/20150812-wireless-car-control/

[6] Gigazine 等を参考に弊社作成

また、サイバーセキュリティ面からみて安全な車両をつくる動きも広がっている。例えば、自動車用機能安全規格にあたるISO26262は車載機器のセキュリティ設計に関する考え方を取り込んだ第２版発行の議論が始まっている。Black Hatやescar等、ハッキングやセキュリティに関する学会・会議では車両に対する攻撃は旬なテーマとして扱われ、対策に関する議論が急速に進められている。

しかし、それらの安全対策が充実したとしても、自動車のサイバーセキュリティは課題が大きい。

まず自動車はＰＣと異なり、衝突等で人や物を傷つける危険性があり、ハッキングによって人命にかかわる事態が起きうるという特徴がある。そのため、ＰＣよりも一段高いセキュリティが求められる。その一方で、利用者自らがアフターマーケット機器を取り付けるといった改造も一般に行われている。先に挙げたOBD2端子を経由した攻撃の例は、直接狙われているのはアフターマーケット機器であり、利用者が車両に取り付けた機器が攻撃されることが幾多にも及ぶ。例えば、カーナビ等を購入して車両に後付するケースは枚挙にいとまがないが、カーナビの製造段階からウイルスが混入していたという例もある[7]。そのため、対策の必要性はメーカーに限らず関連業界にも及ぶ。

また、自動車はＰＣと異なり、屋内等の閉ざされた場所ではなく駐車場に駐車するため、外部の人間が接近しやすいという課題がある。近づくことで可能になるサイバー攻撃も多様に存在する。危機管理としてのハードルは、むしろＰＣより高いといわざるを得ない。

## 3. 車両利用者における対策

今後、車両を安全に利用するためには、「自動車という新しい情報端末が増えた」と考え、留意する必要がある。

特に自動車は、これまでになかった新たな情報をもつ可能性がある。代表的なものの１つが、位置情報である。例えば、取引先の住所や従業員、役員宅の所在地等の情報が取得できる。また、ASV等で利用されるカメラ情報や、車内での通話情報等も守るべき重要な情報である。現状ではカメラを搭載している車両は多くないが、警察車両に搭載していたカメラの映像がインターネット上に公開されてしまったという事件が起きたことがある[8]。これは捜査情報等の漏えいにつながるものであった。監視カメラや屋内カメラ等の映像が意図せずインターネット上に公開されてしまう事件はしばしば起きており、情報漏えいの原因の１つである。車両は運転を行うための機械であるだけでなく、様々な情報を取得、保存、送信している可能性がある点を理解し、それに合った対策が必要である。

車両セキュリティ管理であっても、対策として必要なことは他のあらゆるリスク管理と大きくは変わらない。重要な点は「平時の予防」と「危機管理」である。すなわち、「危険がないように予防策を取ること」「万が一事態が起きた時の対応策を決めておくこと」である。以降、車両利用者における対策について解説する。

---

[7] https://www.ipa.go.jp/files/000013360.pdf 組み込みシステムセキュリティー　カーナビ，独立行政法人 情報処理推進機構 セキュリティセンター

[8] https://www.ipa.go.jp/files/000024414.pdf 「2011年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 セキュリティセンター

### （１）ソフトウェア脆弱性およびアップデートの確認と情報収集

第一に、車両のソフトウェア脆弱性情報、アップデート情報には敏感にならなければならない。先に挙げたテスラモーターズ社のように、今後、無線によりソフトウェアアップデートがなされるケースが定着すると思われる。リコールを行うことに比べれば手間や時間の短縮になり、メリットが大きいようにみえるが、残念ながら自動的にアップデートがなされるというのは完全に安心できるものではない。脆弱性があれば遠隔的に不正なソフトウェアをインストールされてしまう危険性があるためである。実際にテスラモーターズ社は 2015 年４月、DNS ハイジャック[9]を受けており、これを利用して不正なソフトウェアが侵入する可能性が存在した。ＰＣに対するセキュリティ情報は日々、様々なセキュリティ企業やメーカー、政府機関から公表されている。それと同様に、今後は車両に関してもセキュリティ情報が流れるようになり、その都度確認を行う必要があるという意識をもたなければならない。これは「平時の予防」の観点で重要である。

さらに、脆弱性情報に気を付けておくというのも対策を検討するうえで重要である。大規模なサイバー攻撃は予兆があり、すでに海外で発生している手法が日本に遅れて入ってくることも多い。その際、いち早く情報に気が付いていれば、あらかじめ予防策を検討しなおすことも可能である。また、場合によっては、事前に危機対応を想定した体制に切り替えてしまうこともできる。例えば、政治的意図をもったサイバー攻撃は日を決めて行われることがあり、リスクの高い日が特定できることがある。また、ポートスキャン[10]の増加等、大規模な攻撃前のシグナルが検知されることがあるため、事前の対策検討も可能である。少なくとも「自動車は攻撃されうる」という理解のもと、情報収集を行うことが対策の第一歩である。

### （２）アフターマーケット機器の安全性確認

アフターマーケット機器は、導入前に安全性の確認をしていただきたい。少なくとも、なるべく長期的なサポートが信頼できるメーカーの機器を使用することをお勧めする。セキュリティという観点では購入後、時間が経ってから脆弱性が発見され、アップデートの必要が生じる可能性がある。「将来的なサポートに信頼をもちうる機器を利用する」といった点は今後、重要性が高まるといえる。

また、2015 年に攻撃手法が発見された OBD2 端子は、かねてよりリスクの高さが指摘されている。実際、イモビライザー[11]無効化装置等、OBD2 端子を利用する悪意ある装置も市場に出回ってしまっている。OBD2 端子の使用はサイバーセキュリティの観点からは特にリスクが高いことを知り、慎重な機器選定をしていただきたい。安全な機器を使用することは「平時の予防」につながり、また将来的なアップデート・サポートが期待できるということは「危機管理」であるともいえる。

---

[9] 第三者がドメイン名管理サーバを乗っ取る攻撃。これによりある特定のページを全く異なるページとすり替えることができる。

[10] コンピュータの特定ポートが利用可能な状態にあるかを調査すること。脆弱性のある端末を探すために攻撃の前段階として行われることがある。

[11] 鍵に IC チップを埋め込み、ID 認証を併用することで不正な方法ではエンジンが始動できないようにする機能。

その他注意すべき点として、今後スマートフォンと車両の接続が増える点がある。テレマティクスサービスの多くはスマートフォンと接続し、情報のやりとりを行う。先に挙げたように、スマートフォンからの鍵の開閉、エンジン操作等ができるものも多い。すなわち、スマートフォンの管理が車両の管理とつながる危険性がある。そのため、企業ではスマートフォンは個人のものを利用するケースも多いが、これらのテレマティクスサービスの導入には慎重になるべきである。

一方で、電話や音楽等のためにスマートフォンと車両を接続するケースは今でも存在するが、今後、種々のサービス利用のために接続するケースも増えると思われる。利用者のスマートフォンと接続することは、利用者のセキュリティ管理の影響を受けてしまう恐れがあり、スマートフォン側のセキュリティホールの影響を受ける可能性がある。接続自体を行ってよいかという点が議論になる場合も考えられる。「車両は企業の情報管理機器」という認識のもと、管理を行う必要がある。

### （３）自動車販売元へのより詳細な情報の提供依頼

これら、多くのリスクが現れることを考えると、今後の自動車ディーラーやリース会社に求められるものは大きい。

例えば、顧客の移動場所等に関する情報についても、販売元がもちうる可能性が全くないともいい切れず、情報管理の重要性がさらに高まる。販売元における情報管理は利用者が気を付ける点ではないが、そのような情報を渡しているという理解は必要である。過去の事件として、整備工場を離職した社員がテレマティクス機能を使用し、いやがらせ目的で過去に修理した車両のエンジンが起動できないように操作した事件もある[12]。

そのため、自動車ディーラーやリース会社の情報管理体制は車両を購入する際の評価点の１つと考えるべきである。これは安全性もさることながら、車両内でクラウドを利用したサービスの利用が増えるとともに、日常的なサポートの必要性が高まるという理由からである。例えば、クラウドを利用したサービスを購入する際には、システムに関する問い合わせ窓口があるか、といった点は確認をすべきであろう。適切な情報管理が行われていることは「平時の予防」として重要であり、継続的に予防、危機管理を検討するうえでも、また何より実際の危機発生時には自動車ディーラーやリース会社の協力は欠かせないからである。

ここで挙げた３点は、従来自動車管理では重視されず、情報機器管理で行われていたものである。車両の管理を総務部門が行う企業は多いと思われるが、今後はＩＴ部門の協力も必要になるといえる。「自動車は動くコンピュータである」ということを改めて強調したい。

[12] https://www.ipa.go.jp/files/000024329.pdf 「自動車の情報セキュリティ脅威と対策の動向」独立行政法人 情報処理推進機構 セキュリティセンター

## 4. 今後について

車両に対するサイバー攻撃は、その危険性が長く指摘されてきたものであるものの、本格的に注目を集めるようになったのは最近のことである。

実際のハッキングについては、経済的動機をはじめ、いたずら、いやがらせ、テロ等と、多様な目的で行われる。2020 年の東京オリンピックまでに自動走行車を導入するという政府の方針もあり、車両セキュリティを狙った事件の発生が危惧されている。誰もが経験のない事例だからこそ、予防策も不十分であり、危機対応が十分にできない可能性は高い。また、その危険性の程度も現状では評価しきれない点が多く、どのような対策が有効なのか、まだまだ不透明である。

車両のセキュリティ対策はまさしくリスクの最前線であるため、本稿以降も大きな事件・ニュースが出る可能性が高い。その際には、新たに予防策を検討しなければならなくなる可能性もある。リスクの存在を正しく認識したうえで、車両のセキュリティ動向について、今後も注目していただきたい。

［2016 年 1 月 25 日発行］

東京海上日動リスクコンサルティング株式会社
自動車リスク本部
〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23 階
Tel.03-5288-6586 Fax.03-5288-6628
http://www.tokiorisk.co.jp/