FireEye iSIGHTインテリジェンス

つながるクルマ：道路はハッカー天国

FireEye

スペシャル・レポート / 2016年6月

イントロダクション

モノのインターネット（IOT）革命の加速により、乗用車の接続性が強化されています。その結果、一般消費者が大きく影響を受ける可能性が高くなっています。

今日では、車両のほとんどの機能、つまりハンドル、アクセル、ブレーキ、リモート・スタート、そしてドア・ロック解除までもが、車両の内部および外部の両方で作動するさまざまなデジタル・システムから発信されたコマンドを受け入れるソフトウェアによって制御されています。ところが、このソフトウェアには、何百万行ものコードが含まれており、このコードには悪意のある人物が悪用できる脆弱性が存在する可能性があります。

FireEye iSIGHTインテリジェンス・アナリストとMandiantコンサルタントは、車両の内部と外部システムに対するこの大きな脅威について検討し、車両搭載ソフトウェアの脆弱性による脅威の上位5件について評価を行いました。具体的には、以下のとおりです。

車両に無断で物理的に接近する

メーカーまたはサードパーティのストレージ・システムから個人を特定できる情報を窃取する

車両の運転を故意に操る

車両システムをハイジャックして、悪意のあるサイバー活動をできるようにする

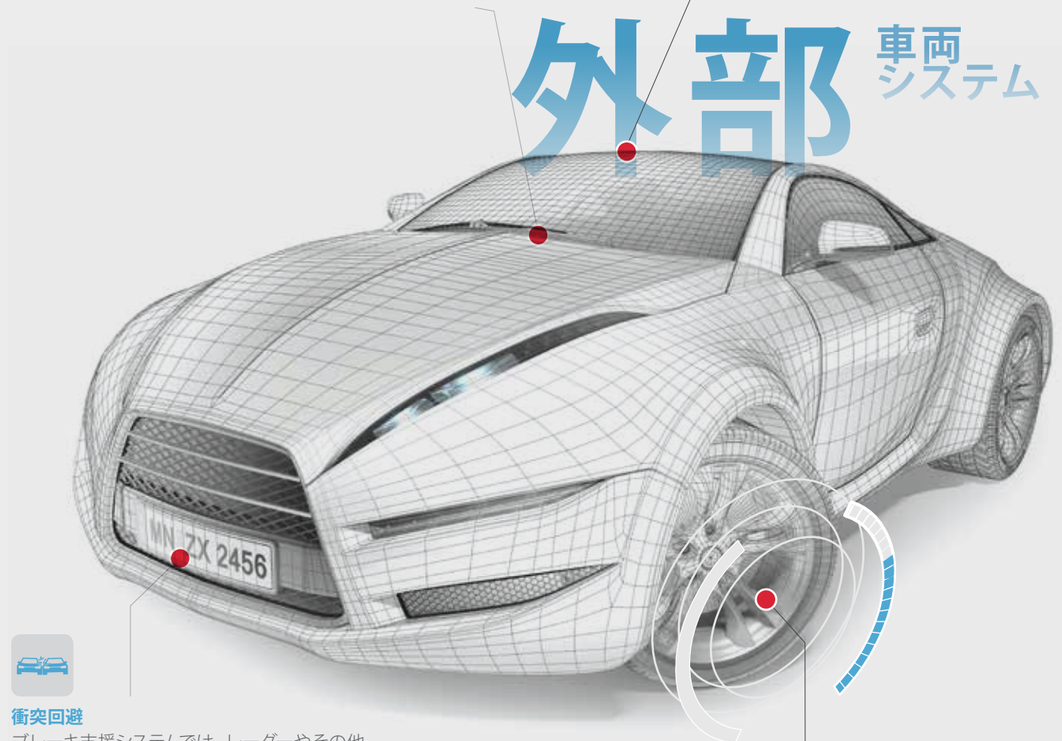
車両をランサムウェアに感染させ、身代金が支払われるまでは車両を運転できないようにして、身代金を要求する

車両間通信

「V2V」とも呼ばれます。周囲の車両との間隔空けや車線変更を支援しながら、運転向上に役立てることができる他のデータを使用するために、車両はますます自律的に通信し合うようになっています。[1] やがては、車両-インフラストラクチャ間通信（V2I）により、車両が交通信号や道路標識と通信することにより、交通の流れをスマートに管理し、道路の利用状況に関するデータを共有できるようになるものと思われます。V2VまたはV2Iを利用するドライバー支援システムを操ることで、安全性が徐々に低下していき、衝突が起こる可能性があります。

WI-FIインターネット・アクセス

新型車両では、無線アクセス・ポイントを売りにしていることがよくありますが、セキュリティで保護されておらず、車両の他のシステムに接続されている場合は、悪用される危険性が高まります。広い帯域幅を利用してやれることが増えていることから、悪意のある行為者が引き起こし兼ねない損害も増える可能性があります。



衝突回避

ブレーキ支援システムでは、レーダーやその他のセンサーを使って、衝突寸前にそれを検知することがよくあります。セキュリティ侵害を受けた車両では、操られたデータがこの機能を制御するECUに送信される可能性があります。その結果、正常に機能しなくなったり、突然ブレーキがかかったりして、車両が無理に停車させられたり、乗客が怪我をしたりしかねません。

タイヤ空気圧監視システム（TPMS）

タイヤ空気圧を監視するシステムは、短距離無線接続で頻繁に通信を行いますが、この接続は車両固有マルウェアの感染経路として悪用される可能性があります。すでに複数の大学で、TPMS内の脆弱性が実証されています。[2]

[1] "Vehicle-to-Infrastructure (V2I) Communications for Safety," *U.S. Department of Transportation*, October 27, 2015, http://www.its.dot.gov/factsheets/v2isafety_factsheet.htm
[2] Bright, Peter, "Cars hacked through wireless tire sensors," arstechnica, August 10, 2015, http://arstechnica.com/security/2010/08/cars-hacked-through-wireless-tyre-sensors/

内部 車両システム

車両運転電子制御ユニット（ECU）
セキュリティが低下した車両では、ハンドル、ブレーキ、およびアクセルを制御するECUが操られる可能性があります。また、速度計やエンジン温度計も、偽のデータを表示し、車両は正常なのに不調であるかのように見せかけたり、逆に不調を隠されたりする可能性があります。

キーレス・エントリ
これまで、泥棒は信号ブースタと傍受機器を使って、ロックされた車両にキーレス・エントリ・システムを通じて無断でアクセスしてきました。[4]　自動車の技術革新における最新のトレンドには、キーレス・エントリとリモート・スタートを実現するモバイル・アプリケーションがあります。

テレマティックス・システム
現代の多くの車両には、高度なテレマティックス・システムが搭載されており、無線、Bluetooth接続とUSB接続、GPS、および携帯電話支援機能が統合されています。ごく最近では、ますます多くの車両が、乗車している人に小型の無線LANを提供するWi-Fiアクセス・ポイントを売りにしています。これらの通信技術のそれぞれが、車両に侵入し、最終的には乗っ取るための手段を与えているのです。

オンボード診断（OBD）ポート
運転習慣の測定、機械類の診断、またはドライバー・エクスペリエンスの向上に使用する機器を接続できる自己診断ポート。このポートは、マルウェアの侵入口になる可能性があります。[3]　たとえば、あるメカニックが、セキュリティ侵害を受けた診断ツールを使って、複数台の車両にうっかり感染させてしまう可能性があります。

クライメート・コントロール：
車両内部の環境は、ドライバーの快適さを左右します。その結果、車両を安全に運転する能力にも影響する可能性があります。セキュリティ侵害を受けたECUを通じてクライメート・コントロール・システムを操ることで、真夏の時期に温風を吹き出させ、ドライバーが車両を止めて車外に出ざるを得ない状況にする可能性があります。

[3] Darren Pauli, "Mechanic computers used to pwn cars in new model-agnostic attack ," *The Register*, March 13, 2016, http://www.theregister.co.uk/2016/03/13/mechanic_computers_used_to_pwn_cars_in_new_modelagnostic_attack/
[4] Nick Bilton, "Keeping Your Car Safe from Electronic Thieves," *New York Times*, April 15, 2015, http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html

テレマティックス

オーディオ・システム
USBまたはストリーミング・メディアを介した感染経路

GPSナビゲーション
脅威をもたらす行為者が、GPSディスプレイに偽信号を送って、ドライバーを本来の道から外れさせたり、保存された目的地情報を収集して移動パターンを把握したりする可能性があります。

連絡先リスト
車載コンピュータに保存された情報には、PIIが含まれている可能性があります。

WEBブラウザ
Webブラウザには、悪用可能な脆弱性が存在することがよくあります。

USB
セキュリティ侵害を受けた携帯電話やその他のデバイスを介した感染経路

FireEyeでは、車両に現在発生しているリスクと可能性のあるリスクを分析しながら、公開された情報を検討して、さまざまな脅威のシナリオ、発生確率、および影響の可能性の評価を行いました。当社では、車両搭載ソフトウェアの脆弱性による脅威の上位5件を以下のように判断しています。

- 車両に無断で物理的に接近する
- メーカーまたはサードパーティのストレージ・システムから個人を特定できる情報を窃取する
- 車両の運転を故意に操る
- 車両システムをハイジャックして、悪意のあるサイバー活動をできるようにする
- 車両をランサムウェアに感染させ、身代金が支払われるまでは車両を運転できないようにして、身代金を要求する

リスク1

車両に無断で物理的に接近できるようにする

すぐ近くまで近づいて車両に無断で乗り込む方法は、最も簡単であるため、一番多い手口です。この方法は、最新技術で強化された車両に最も直接的かつ現実的な脅威をもたらします。これは明らかに、多くの自動車メーカーが、物理的な点火系統を携帯電話のアプリケーションやワイヤレス・キーフォブを活用するキーレス・システムに置き換えてきたためです。[5] 無断侵入方法ではほとんどの場合、車両とドライバーが持ち歩くキーフォブの間の無線通信を悪用します。[6]

脅威のシナリオ	攻撃者は、車両接続技術の脆弱性を悪用して、車両に無断で乗り込んだり近づいたりします。	
可能性	高	• 長年にわたり、自動車泥棒はロックされた車両に物理的に入り込む方法を探し求めてきました。車両に傷を付けたり物理的な証拠を残さずにそれができるようになったため、抑止力が低下しました。 • すぐ近くに接近して近距離で悪用する複数の機能により、攻撃者は驚くほど簡単にセキュリティで保護された車両スペースに近づくことができます。
影響	中	• 顧客は、盗まれやすい車両や車上荒らしの被害に遭いやすい車両をあまり購入したがりません。 • 盗難のリスクが増大しているため、セキュリティで保護されていない車両の保険料は増額される可能性が高くなります。 • セキュリティで保護されていない車両が盗まれた場合、メーカーが責任を問われる可能性があります。そして、規制当局が、衝突安全性テストや燃費などと同様に、車両サイバーセキュリティの格付けを規定する可能性もあります。[7]

[5] Paul Einstein, "Bye-bye, car key? Keyless systems taking over," *CNBC*, December 14, 2014, http://www.cnbc.com/2014/12/12/bye-bye-car-key-keyless-systems-taking-over.html
[6] Andy Greenberg, "This Hacker's Tiny Device Unlocks Cars and Opens Garages," *Wired*, August 6, 2015, http://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/
[7] Doug Newcomb, "Michigan Senator Proposes Auto Industry Step Up Cybersecurity Efforts To Avoid Legislation," Forbes, March 30, 2016, http://www.forbes.com/sites/dougnewcomb/2016/03/30/michigan-senator-proposes-auto-industry-step-up-cybersecurity-efforts-to-avoid-legislation/

リスク2

個人情報の窃取

多くの犯罪者、ハクティビスト、および国家支援を受けた攻撃者にとって、個人を特定できる情報（PII）を収集することは最優先事項の1つです。現代の車両は、車両のオペレーティング・システムと通信する無数の市販デバイスと対話するために、運転中にPIIを大量に収集します。その結果、今や車両は金融情報の窃取に関心のある者にとって、攻撃経路に加わりました。また、この新しい攻撃経路は、移動先、ドライビング・スタイル、速度違反や交通違反の可能性に関する、表面上は何の変哲もないデータなど、生活パターン・データへとアクセスを拡大する可能性もあります。

さらに、ディーラーと通信する自動メンテナンスまたは診断サービスが、ディーラーやメーカーの各種システム上に保存されているPIIを探す犯罪者にとって都合のよい攻撃経路を与えるという危険性を招いてしまうこともあります。車両に関してデータの保護要件と保管要件（ローカルとクラウドベースの両方）を規定する法律は、今のところ未成熟です。これはつまり、プライバシー・ポリシーがメーカー間で一貫しておらず、消費者が悪用に対して脆弱なまま置き去りにされているということです。

脅威の行為者は、以下に示すタイプの情報に関心を持っている可能性があります。これらは、車両のシステムを通じてアクセスされたり、車両自体に保存されることがあります。

車両情報	個人情報
型式、モデル、年	所有者の名前、住所、電話番号、電子メール
GPS（全地球測位システム）の位置と速度	所有者の人口統計学データ
車両識別番号	社会保障番号
システムの診断データ	携帯電話の連絡先リスト
車両がオンまたはオフの時間	モバイル・アプリケーションのログと設定

攻撃によっては、保存されている複数の情報を利用します。その一例が、盗難車のGPS情報に関連するものです。この情報には、所有者の自宅の住所を明らかにする「自宅」という目的地が含まれていることがよくあります。保存されている車庫のコードと組み合わせると、車両の被害は自宅への侵入盗難につながる可能性があります。自動車テレマティックス・システムの複雑さが増し、機能が増えるにつれて、攻撃の対象がEメール、バンキング、その他の機密性の高いモバイル・アプリケーションにまで広がる可能性があります。

脅威のシナリオ	自動車データ・ストレージ・システムが侵害を受け、その結果、顧客のPIIが窃取された。	
可能性	高	• クラウド・ストレージの場合、自動車の販売代理店やメーカーは、PIIを入手しようとしている犯罪グループと国家レベルの攻撃グループのどちらからも侵入の標的とされる可能性があります。 • ローカルな自動車ストレージの場合、これは、ドライバーの自宅に物理的にアクセスするための格好の標的となることがあり、犯罪の誘因が高まります。 • 2014年の半ば以降、国家レベルと見られる攻撃グループが、政府や医療など、他の業界の大規模なPIIのストレージを意図的に標的にしていることが確認されています。
影響	中	• 機密性の高いPIIを保護する業界の能力に関連する、消極的なメディアの関心。 • 脆弱性のインシデントに対応した政府の規制により、業界のコンプライアンス・コストが上昇する可能性があります。 • 窃取されたPIIを通じて行われたサードパーティの侵害に関連する訴訟。 • 影響を受けた顧客に対するクレジット・カードのモニタリング・サービスに関連したコスト。

リスク3

車両の運転を故意に操る

車両セキュリティの研究者であるCharlie Miller氏とChris Valasek氏は、セントルイス・ハイウェイでの走行中に車両を運転しながら、車両のシステムをリモートでハイジャックできることを実証しました。[8] ますます多くの車両がインターネットに接続し、これまでになく機能が増えていることから、悪意のある攻撃者にとっては、これらの拡大する機能に存在する脆弱性を利用するための選択肢が増えると思われます。

脅威のシナリオ	悪意のある攻撃者や犯罪者が車両の制御システムを乗っ取り、意図的に衝突させたり、ドライバーに怪我をさせたりする。	
可能性	中	• 長距離の攻撃は実行が難しく、特定の車両の脆弱性について幅広い調査が必要です。 • 犯罪者や他の攻撃者は、故意の器物損壊や人身傷害ではなく、データの窃取に高い投資効果を見出す可能性があります。
影響	高	• 人身傷害や器物損壊、重大な交通渋滞。これらはすべて、意図的な車両の衝突が成功した結果として考えられます。 • 自動車メーカーは、適切に保護されていない車両に対する責任を問われる場合があります。 • ドライバーは、ソフトウェアの脆弱性により危険だと思われる車両の購入を避ける可能性があります。

[8] Andy Greenberg、『Hackers Remotely Kill a Jeep on the Highway—With Me In It』*Wired* 2015年7月21日、http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

リスク4

電子制御装置を利用した悪意のあるサイバー活動のサポート

現在の平均的な自動車には、約70の電子制御装置（ECU）[9]、WiFiや4Gなどの複数のネットワークを備え、ギガバイトのデジタル・ストレージを持っている可能性があります。[10] 実際には、最新の自動車は、コンピュータ、ローカルおよび広域エリア・ネットワーク（LAN/WAN）、ファイル・サーバーから構成される最新のコンピュータ・ネットワークに匹敵します。モバイル・デバイスやインフラストラクチャの悪用でわかるように、悪意のある活動は、テクノロジーの発展に追随してきました。[11] サイバー攻撃者が悪意のある活動をサポートするために、自動車を次の標的と見なす可能性があると考えるのは妥当です。

現在、サイバー活動にとって価値のある指揮管制ノードとして機能するために必要な接続性を備えている車両はまれです。ただし、車両がインターネットを通じて、より多くの帯域幅を必要とする他のサービスに接続すれば、侵害やハイジャックを受ける可能性は高まります。

脅威のシナリオ	車両のECUや他のコンポーネントが侵害を受けたり、他の悪意のあるサイバー活動をサポートするために悪用されたりする。	
可能性	低	• サイバー活動作戦のためのインフラストラクチャ・ノードとして機能するために必要な広範囲の接続性を備えている車両は、それほど多くありません。 • 車両がインターネットや他の通信サービスに接続すれば、それだけ可能性は高まります。
影響	低	• 特に車両のコンポーネントをハイジャックする攻撃者は、自分の存在を所有者に見えないようにしようとするため、運転中に車両自体に重大な不具合が発生する可能性は低そうです。 • 車両の被害に対する調査が行われると、ドライバーはこのような調査の間に車両を使用できなくなる可能性があり、ブランドの評判に傷が付きます。 • ECUのハイジャックの無防備な被害者が、悪意のある活動への共謀の罪に問われる場合もあります。

[9] Robert N. Charette、『This Car Runs on Code』、IEEE Spectrum、2009年2月1日、http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code
[10] 東芝セミコンダクター＆ストレージ社の製品、自動車インフォテイメント・システム向けストレージ・ソリューション、http://toshiba.semicon-storage.com/ap-en/product/automotive/info-storage.html
[11] Yong Kang、Zhaofeng Chen、Raymond Wei、『XcodeGhost S: A New Breed Hits the US』、FireEye Blogs、2015年11月3日、https://www.fireeye.com/blog/threat-research/2015/11/xcodeghost_s_a_new.html

リスク5

ランサムウェアの配備による被害者の恐喝

ランサムウェアはこれまで、ほとんどが個人ユーザーや企業を標的とし、個人のコンピュータでファイルの暗号化を解除するために、一般の人々や企業が数百ドルを支払うよう仕向けてきました。つい最近では、ランサムウェアは警察署や病院を攻撃しています。このような組織は、バックアップを十分にしていない場合、身代金を支払うよりほかありません。システムの制御を取り戻すために、ビットコインなどの匿名性の高い仮想通貨で数千ドルを支払った例も、いくつか報告されています。[12] より高い収益を求めるよう変化していることから見て、特に米国では日常生活で自動車への依存度が高いことを考えると、犯罪者は車両向けのランサムウェアを開発して仕掛ける気になると思われます。個人消費者と企業のどちらについても、数万ドルを費やした車両の制御を取り戻すために数千ドル支払うというのは、妥当な予測です。

脅威のシナリオ	車両のECUがランサムウェアによって操作不能に陥る	
可能性	低	• これまで、車両システム用に特別に設計されたランサムウェアのサンプルが使用または公表されたことはありません。 • ランサムウェアの標的は、一般的なユーザーのコンピュータから、より規模の大きい組織に移行しており、中でも病院が特に懸念されます。
影響	高	• 一般の人々にとって車両は重要であることから、身代金が支払われる可能性は高く、サイバー犯罪者が車両用に設計したランサムウェアを構築して仕掛けることへの金銭的な動機が高まります。整備工の助けがあれば、ドライバー1人でもソフトウェアを再インストールできる場合があります。 • ハイウェイ全体の車両がランサムウェアによって操作不能に陥ると、公共サービスの途絶が急速にエスカレートする可能性があります。

[12] Richard Winton、『Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating』、Los Angeles Times、2016年2月18日、http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

こうした新たなリスクの発生を考えると、自動車メーカーとサプライヤは車両の従来の操作上の安全性を保証する必要があるだけでなく、車両の操作とドライバーのプライバシーの両方について安全性を保証する必要があります。それには、急速に進化する状況において脅威と脆弱性の本質を継続的に理解し、これらのリスクから保護するための強力なセキュリティ対策を事前に講じる必要があります。脅威の攻撃者は絶えず進化しているため、1回のリスク評価では不十分です。

FireEyeは業界をリードする脅威情報、インシデント・レスポンス、およびレッド・チーム能力と、ICS分野の専門知識を組み合わせることにより、自動車業界が防御、検知、および対応能力を向上できるよう支援します。FireEyeのレッド・チーム・サービスとペネトレーション・テストは、自動車業界の企業に対し、実際の攻撃に対応してきた経験を提供し、メディアにネガティブな見出しが載るリスクを回避します。

レッド・チームが関与する場合は、断固たる攻撃者が、機密情報の窃取やデバイスまたはシステムの乗っ取りなどの特定の目的を達成できるかどうかを評価するという明確な目標を設定します。一方、ペネトレーション・テストは、アプリケーションやIoT、ワイヤレス・テクノロジーなどの重要なシステムおよびネットワークの特定の領域について、防御のために導入されているセキュリティ対策を評価します。

FireEye　iSIGHTインテリジェンスのホライゾン・チームは、新しいテクノロジーや地政学的な開発によってもたらされるリスクの戦略的な予測を行い、変化するセキュリティ脅威にさらされるリスクを、お客様や一般の人々がより的確に評価できるよう支援します。

詳細については、FireEyeまでお問い合わせください。

www.fireeye.com/redteam.html

〒101-0054 ファイア・アイ株式会社
東京都千代田区神田錦町3-22
テラススクエア8階 | 03−4577−4401 | Japan@fireeye.com

www.FireEye.jp

FireEye