KPMG

コネクティッドカーのつぶやき

情報の価値とセキュリティ対策

kpmg.com/jp

KPMG

目次

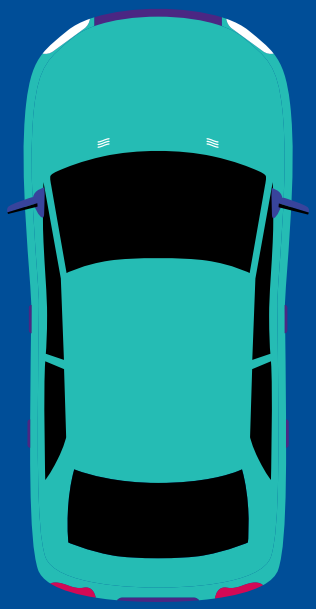
著者紹介

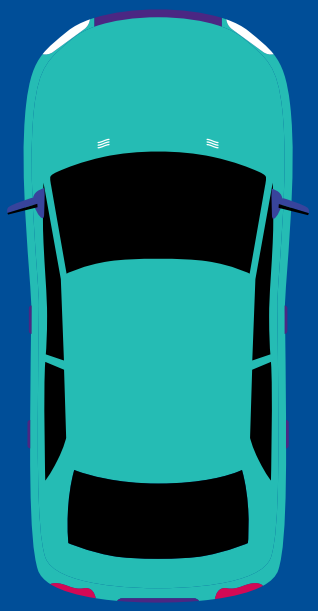
Gary SilbergはKPMG米国のNational Automotive Leaderであり、Delphi CorporationおよびFord Motor Companyのグローバルリードパートナー。自動車産業における14年以上の経験を含め、25年以上にわたるビジネス経験があり、自動車産業のグローバルトレンドについてメディアで大きな発言力を持つ。戦略、合併、買収、資産売却および共同事業の分野で多数の国内企業や多国籍企業に助言を提供している。過去5年間は、技術と自動車産業の交点に焦点を当て、自動運転車、コネクティビティ、モビリティオンデマンドサービスについて画期的な研究を行っている。

Ron PlescoはKPMG Cyber Investigations部門のprincipal兼national lead。サイバー脅威インテリジェンス（CTI）およびサイバー侵犯調査に重点的に取り組むチームを率いる。情報セキュリティおよびプライバシーを専門とする弁護士として国際的に知られており、サイバー調査、情報セキュリティ、プライバシー、アイデンティティ管理、コンピュータ犯罪、新たなサイバー脅威、テクノロジーソリューションの分野で18年の経験を有する。自動車業界に力を入れており、車のハッキングや相互接続車両のサイバーセキュリティ上の問題について、定期的に講演を行っている。KPMGに入社する前は、米国サイバー鑑識・訓練協定（NCFTA）のCEOとして、諜報活動の整備を監督した。この諜報活動により、4年間で全世界400件以上のサイバー犯罪が検挙され、20億ドル以上の詐欺を未然に防いだ。

Doron RotmanはKPMG Advisory部門のmanaging director。National Privacy Service Leaderであり、KPMG national Privacy Leadership CouncilとKPMG International Privacy Leadership teamのメンバーでもある。28年以上のキャリアを持ち、大規模な組織へのプライバシー、セキュリティ、情報ガバナンスサービスの提供に注力している。情報テクノロジー監査、会計、金融分野に豊富な経験を持ち、ハイテク、金融サービス、ヘルスケア、製造、ユーティリティ、行政部門に広範な知識を有する。

Danny LeはKPMG Advisory practiceのprincipalであり、サイバーセキュリティを専門とする。この10年はKPMG中国のコンサルティング事業の立ち上げに従事し、KPMG中国のhead of Automotive practiceを務めた。KPMGのGlobal Automotive Steering Committeeのメンバーでもある。特にモビリティサービスの開発と実施、伝統的なビジネスプロセスのオンライン化に詳しく、この分野で自動車メーカーへの助力を行っている。またKPMG米国のInformation Protection and Business Resilience practiceの創設パートナーでもあり、多数のグローバルアカウントを率いている。





Gary Silbergからのメッセージ

今日の自動車はかつてないほど「つながって」います。自宅やオフィス、携帯端末と同じようなコネクティビティ（インターネットにつながっている状態）を自動車は提供しているのです。コネクティビティはドライバーや消費者にとって非常に有益であることは確かですが、そこにはリスクも伴います。

いまや車輪のついたコンピュータへと進化を遂げた自動車の中で、人はデータやソフトウェアやセンサーに取り囲まれています。そしてテクノロジーは刻々と進歩しており、自動車がコネクティッドな（つながっている）生活の中心になる日も間近です。コネクティッドカーは煩わしい渋滞を回避したり、移動中の時間をエンタテインメントで楽しませてくれたり、大がかりな修理が必要になる前に問題を検知したり、そして何より、家族の安全を守り、無用の悲劇的な事故を回避する一助となってくれるでしょう。

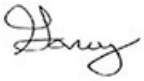
車載ソフトウェアやデバイスは、いまやドライバーがどのように運転し、どこへ行き、誰に電話をかけ、何を聴き、どのようなパーソナルデバイスにつなげるかまで把握しています。しかし残念ながら、このようなデータやコネクティビティは、自動車が走行中でも、すべてハッカーの標的になり得るのです。

電話や銀行口座と違って、走行中の自動車では、再起動やソフトウェアの更新を行うことはできません。他のデバイスとは異なり、自動車システムが侵入を受ければ命に関わります。特に高速道路を走行中にハッカーに乗っ取られたらどうなるでしょう。ドライバー以外の誰かが自動車を操れるとしたら、どのようなことが起こり得るでしょうか。

そしてこういったことすべては自動車メーカーの今後を占う上で何を意味するのでしょうか。

本書はこの2つの世界、すなわちデータが素晴らしい価値を持つ世界と、データがリスクを意味する世界について探求していきます。この2つの世界のバランスをどう取るか。データのもたらす洞察力を活用して、顧客に素晴らしいドライビング体験を提供すると同時に、データを保護するにはどうすればいいか。その方法をご提示します。

これを正しく行えば、膨大な成長の機会を生み出すことができる一方で、これを誤れば、ブランドを著しく傷つけることになってしまうのです。



Gary Silberg
Partner and National Automotive Leader

価値の高いデータを保護する

@YourCar:
「GPSによると
サードストリートで工事あり。
オークアベニューに迂回。
アレックスは2分遅れる旨、
オフィスマネジャーの電話番号
555-555-9876に
テキストメッセージを送信」

あなたが新車の購入を検討しているとします。あなたがいまどきの消費者なら、馬力や燃費はそれほど気にしないでしょう。あなたにとっていちばん大切なのは、車とデジタルライフがうまく統合されたドライビング体験です。そう遠くない未来、車はもう1つの人格、つまりあなたのモバイルデジタルアイデンティティを担うようになるでしょう。車輪のついたiPhone、すなわち車とデジタルアイデンティティの統合を最初に実現するのはどの会社でしょう？

今日の消費者はあらゆるパーソナルモバイルデバイスが、どこへ行ってもユビキタスに、シームレスにつながることに慣れています。車はその中で欠かせない要素です。自動車業界はかつてないほど複雑でテクノロジーを満載した「コネクティッドカー」を生み出すことにより、消費者の期待に応えています。この「コネクティッドカー」は遠隔操作によって、他のデバイスからなる広範なデジタルエコシステムと通信することができます。今日の平均的な自動車の車載マスターコンピュータシステムは、外界からデータを取り込むために有線、無線合わせて60以上のものとつながっています。これにはセンサー、GPSユニット、インフォテインメントのプラットフォーム、モバイルデバイスなどが含まれます。消費者であるあなたは考えもしないことかも知れませんが、実はあなたの車は「車自体」やドライバーが何をしているかについて話し続けて（発信し続けて）いるのです。

今日の自動車メーカーは顧客基盤を理解するためのデータマイニングにかけては名人です。

車のオーナーにとって、コネクティッドカーの価値はユーザ体験を高めるソフトウェアとエレクトロニクスにあります。それは運転を簡単にし、安全性を高め、個人に合った、楽しく生産的なドライビングを可能にしてくれるものです。一方、自動車メーカーにとって、コネクティッドカーの価値はそのデータにあります。そのデータが顧客について、また顧客が製品に対してどのような感想を抱いているかについて、どんなことを教えてくれるかが重要です。

ハイテクなソフトウェアとシステムを搭載したコネクティッドカーは、ドライバーの習慣や好み、リアルタイムな計測値や診断情報について、数十億ビットのデータを収集します。このデータはドライバーのニーズや行動、車のパフォーマンスなど、顧客に関する強力な洞察力を発揮してくれます。自動車メーカーはこのデータを利用して、より賢明な決定を行い、車の安全性を高めることができます。さらに自動車メーカーは新たなビジネスモデルによりそのデータを収益化し、まったく新しい顧客群を開発することができます。

おそらく自動車メーカー側から見ても顧客側から見ても最も重要なのは、コネクティッドカーのセンサー内のテレメトリーデータにより、安全性を大幅に高めることができるということでしょう。自動車メーカーはこれを利用して、ドライバーに注意を促したり、交通ルールを守るよう働きかけたり、困難な運転条件を予測してそれに備えたり、緊急通報を行ったり、ドライバーアシスト技術を通じて事故を回避したりすることもできるのです。

KPMG

テレメトリーデータの管理による安全性の向上は、自動車メーカーが究極的にデータ関連の取り組みを集中させるべき分野であると思います。なぜならデータ利用によるユーザ体験の向上よりも、自動車メーカーの強みが発揮できる分野だからです。ユーザデータを利用して優れたユーザ体験を実現する分野は、すでに異業種から消費者重視の企業が数多く参入しており、今後も熾烈な競争が続く見込みです。消費者が安全で高機能な車のメリットを享受しながらも、個人情報を自動車メーカーに提供しないという選択肢が与えられるべきか否かについては、倫理上、プライバシー上の懸念が残りますが、テレメトリーデータを利用した乗員の安全性確保は自動車メーカーが優位に立てる分野であると思います。

車が複雑なコンピュータ、あるいは車輪のついたエンドポイントになり、データや情報の量が爆発的に増えるにつれ、新たなチャンスも広がっています。しかしリスクとブランドの維持について考え方を改める必要性も生じています。

自動車メーカーは収集したデータの適切な利用を確保できて初めて、そのデータを有効活用することができます。コネクティッドカーのシステムに含まれるデータは価値を内在する一方で、多くのリスクもはらんでいます。データにはハッキング、紛失、誤用などの危険性があり、ユーザの生活を脅かし、ユーザを身体的な危険にさらす可能性があります。これは自動車メーカーにとって、財務、規制、評判の面で深刻な意味を持ちます。またデータの質と完全性も重要です。データが改ざんされれば、事業者はそれを利用して価値を生み出すことはできません。さらに個人のプライバシーと安全性の間で矛盾が生じる可能性もあります。

自動車メーカーはブランドを構築し、維持するために巨額の投資をしています。ひとたび車が「ハッキング可能」、セキュリティが確保されていないとみなされたら、そのブランドの評判がどれだけ失墜するか想像してみてください。あるいは「ハッキングされた自動車メーカー」として知れ渡ってしまったら、どのようなことになるでしょう。

今日のビジネスにおいて、おそらく特に自動車業界においては、データは新たな重要資産です。だからこそ、**今日の自動車メーカーはデータを保護することにより、消費者のブランドへの信頼を維持しなければならないのです。**私たちの経験から言っても、コネクティッドカーに出入りする貴重なデータをうまく取り扱い、管理し、分析し、保護できる会社は、車のオーナーを満足させ、購入検討者に興味を抱かせるような優れた体験を作り出すことができると言えます。

本書では、自動車メーカーが、価値の高いデータを保護し、顧客体験を向上させ、セキュリティとプライバシーの問題に対処することで、いかにして市場での差別化を図れるかについて探求していきます。

「車やトラックは車輪のついた極めて複雑なコンピュータへと進化しています。コネクティビティの増大は現実的かつ重要なサイバーセキュリティ上のリスクを伴います。最も重要なのは安全性です。多くの消費財と異なり、車のシステムが侵入を受ければ生命にかかわります。高速道路を走行中にハッカーに車を乗っ取られたらどうなるでしょう。非常に恐ろしいことですが、これは現実に起こりうるシナリオなのです。」

—Gary Silberg, Partner and National Automotive Leader, KPMG

「自動車メーカーにおける新たな資産はデータです。データは実際の価値を持つ通貨となりつつあり、保護しなければなりません。セキュリティに投資する必要があります。」

—Danny Le, Principal and Automotive Leader, KPMG Cyber Security Services

ビッグデータは多くを語る

自動車のコネクティビティの度合いが高まるにつれ、刻々と変化する時系列データを保有する自動車メーカーはそれを利用できる立場になります。なぜなら、コネクティッドカーのデータ量は明らかに膨大だからです。問題は、そのデータが何を語るかです。

成功を収める自動車メーカーは戦略的にデータを収集し、予測的分析を行って、顧客の信頼や快適性、安全性を高め、自社の事業運営を最適化し、収益を創出する新しい方法を導入していきます。

顧客の信頼、快適性、安全性を高める

自動車メーカーはデータを利用することにより、顧客の購入検討段階から、保守、アップグレードの段階に至るまで、顧客ライフサイクル全体にわたって、カスタマーリレーションシップのあらゆる側面を管理することができます。実際、コネクティッドカーは自動車を購入するという体験をデータ主導型に変え、それによってさらに顧客一人一人の満足度の高い体験に変えつつあります。たとえばあなたがディーラーに足を運ぶと、ディーラーはすでにあなたが何者で、どのようなことに興味があるかを把握していて、あなたにぴったりの製品や構成、あなたのニーズを満たすオプションを的確に勧めてくれるとしたら、どんなに気分がいいでしょう。

購入後は、コネクティッドカーのデータから、自動車メーカーがあなたの運転のクセや、あなたが通る道の種類、乗員の人数、よく聴く音楽のジャンルなどについて見極めます。この見極めにより、自動車メーカーはあなたの車内体験を向上させ、カスタマイズすることができるのです。たとえば、忙しいお母さんが寒い冬の朝、子どもを学校に送り届ける前に車内の暖房を入れておく、多忙なビジネスマンが移動中も効率よく仕事ができるようにする、事故の被害者に緊急支援を送る、自動車で旅行する人が気分にぴったりの音楽を聴きながら渋滞のないルートで目的地に到着する。そんなことができたら顧客満足度はどれだけ向上するでしょう。

自動車メーカーにとって、本領が発揮できるのは、コネクティッドカーのネットワークから収集したビッグデータを利用して、道路の安全性を高め、ドライバーの運転を助け、リアルタイムで危険を回避し、緊急応答サービスにアクセスし、良い経路を選んで交通を管理し、運転の快適性を高めることです。

自動車メーカーはデジタルなユーザ体験で勝負することもできます。ただ、この分野はApple、Google、Amazon、Spotifyといった強敵の挑戦を受けることになるでしょう。自動車メーカーはデータを収集することはできますが、ショッピングや、音楽やエンタテインメントのライブラリの提供については未経験です。この分野は開拓すべき非常に大きな市場です。

成功を収める自動車メーカーは戦略的なデータ収集と予測分析を使い次を行う。

1. **顧客体験を変容させる。**
2. **自社の事業運営を最適化する。**
3. **収益を創出する新たな方法を導入する。**

体験を主導する4つの主要なデータフロー

パフォーマンス：コネクティッドカーは車載センサーを通じてバルブやブレーキなど部品の最新状況を収集することにより、消耗に関する警告、保守の予測、保守の予約手配を行うことができます。このデータを、テレマティクスユニットを経由して自動車メーカーのクラウドと共有すれば、自動車メーカーは全車両の性能に関する計測値を蓄積し、故障率や保守の必要性などについて、かつてない規模で見極めることができます。またデータを自動車メーカーのサプライチェーンと共有すれば、部品の需要を予測することができ、保険会社と共有すればどの車種の故障率が高いかを予測することができ、ディーラーやメンテナンス業者と共有すれば先制的な保守が可能になります。

インフォテインメント：コネクティッドカーのダッシュボード内のコンソールがドライバーや乗員の使用データを収集し、GPSが位置データを収集し、テレメトリーユニットがユーザをコンテンツ、ビジネス、サービスプロバイダにつなげます。このサイクルがメディア消費の拡大や、ターゲティング広告、マーケットリサーチの機会を創出します。

ビジネス：コネクティッドカーはハンズフリー通話、自動アシスタント、ナビゲーションサービスにより、ドライバーを企業ネットワークにつなげ、車内からビジネス活動を行う手助けをします。

ヘルス：コネクティッドカーは車載センサー、Fitbitのようなウェアラブルなどの外部デバイスとのコネクティビティ、テレマティクスを使用して、身体の健康状態、処方箋、病歴のデータを収集することにより、車のオーナーに緊急応答、医療に関するリマインダー、医療機関やライフスタイルアプリ、医療健康関連サービスとの連携を提供します。

2014年のKPMGのレポート「Me, My Car, My Life」で、私たちは超コネクティッド時代に自動車業界が直面する多くの変化を正確に予測しました[1]。そして今、私たちはこう考えます。未来のインフラのコネクティビティを予期し、インフラと通信できる検知装置を自社の全車両に搭載する自動車メーカーは、カーブや交差点に差し掛かる前からそこで起こりうることをドライバーに知らせることができる、と。そのような自動車メーカーは事故を防止するために良質な情報を入手し、効率の良い運転を助け、快適な乗り心地を提供することができるでしょう。こういったことはすべて自動車ブランドにとって明白な差別化要因になります。

自動車メーカーがコネクティッドカーのデータを読み解いて乗員の快適性と安全性を高めようとすると、ユーザのプライバシー保護と安全性強化のバランスを取る必要があります。この問題についてはのちほど検討します。

事業運営の最適化

自動車メーカーはデータを利用して個々の車や車両全体のパフォーマンス、信頼性、安全性を最適化することもできます。コネクティッドカーの車載センサーは、バルブやブレーキなど部品の最新状況を収集します。そのデータにより自動車メーカーは消耗の状態を追跡し、機械的視点から車が公道を走れる状態を確保することができます。たとえばタイヤの空気圧が低い、燃費が悪化している、アラインメントがずれているといった情報です。将来はテレマティクスを利用して、たとえばドライビングの快適性を向上させたり、乗り心地の改善につなげたり、交通の流れを良くしたり、眺めや景色を良くしたりすることもできるようになるかもしれません。

1 Me, My Car, My Life
（KPMG、2014年 英語版発行、2016年 翻訳版発行）

センサーデータがあれば自動車メーカーは保守のニーズを予測したり、前もって保守の予約を入れたりすることも可能になります。車の統合システムは製品のアップデートや関連するセールスプロモーションを自動的に提供することもできるため、突然機械的な問題に悩まされることもなく、お得な情報を見逃すこともなくなります。テレマティクスデータによって可能になるその他のサービスとしては、駐車場の予約や、洗車、車の引き取り、サービス、納車の予約などが挙げられます。

また全車両のパフォーマンスデータを蓄積すれば、自動車メーカーは故障率や保守の必要性をかつてない規模で見極めることができます。これを利用して部品の需要を予測したり、手遅れになる前にリコールにつながりうる問題に対処したり、将来の調査、デザイン、イノベーション、製品開発などの際に情報を提供したりすることができます。

利益の創出

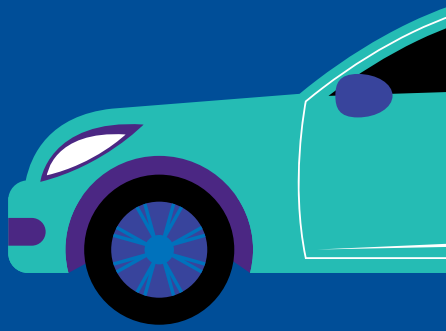
革新的な自動車メーカーなら、既存のビジネスモデルや新しいビジネスモデルを支援するため、データを収益化するでしょう。多くの自動車メーカーがプレミアムパーキング、納車サービス、レンタカー、給油や充電、カーシェアリング、コンシェルジュサービスといったモビリティサービスに着手しています。自動車そのものだけでなく、自動車周辺の製品やサービスを販売することにより、世界の自動車市場のさらに広範な部分を手中に収めようとしています。

しかしその他の収益機会に関しては、自動車メーカーは戦う必要があります。モバイルプロバイダ、アプリメーカー、コネクティッドカーメーカー、クラウドプロバイダとの熾烈な闘いになるでしょう。Google、Apple、Microsoftが車載インフォテインメントのインタフェースを所有するために、すでにどれだけの投資をしているか見てみてください。

明らかなのは、データを所有する者が勝つ、ということです。

「将来、自動車メーカーは道路の車線区分線をひく塗装メーカーや、道路標識、一時停止標識などを設置するインフラ企業と協力することになるかもしれません。全米のインフラのパーツとして、RFID、ソフトウェアチップ、その他のテクノロジーが埋め込まれるようになるかもしれません。そうなれば車は道路を良く『見る』ことができるようになるでしょう。」

—Danny Le, Principal and Automotive Leader, KPMG Cyber Security Services



自動車メーカーはコンテンツビジネスに参入すべきか？

10億ドルを投じて設立されたカリフォルニア州に拠点を置く謎の電気自動車ベンチャー企業Faraday Futureは、自動車メーカーがコンテンツビジネスに参入するべきだと考えています。Faraday Futureと同社が提携している中国のオンラインエンタテインメント企業LeEco*、コンシューマーエレクトロニクス、メディア、エンタテインメントの多様化したビジネスモデルをいかにして月額定額制の電気自動車に収束させるかについては、さまざまな憶測や議論があります。

*2017年5月、LeEcoは米国部門の大幅な人員削減を行った。

出所：LeEco plans a big electric car factory in China（Fortune、2016年8月11日号）

詳細な顧客プロフィール、たとえば、ジョン、白人男性、年齢48歳、車はホンダシビック、サンフランシスコ在住、よく聴いているのはウォリアーズのバスケットボール試合放送、スターバックスによく立ち寄る、車に乗っている時間は1日2時間、といったデータは、広告主やマーケットリサーチャーにとって大きな価値を持っています。GPSデータを組み合わせれば、コネクティッドカーを通じたロケーションに基づく広告は特に強力な機会となります。たとえばジョンが高速道路の広告看板の前を通過するとき、広告主はその情報を瞬時に入手し、ジョンをターゲットにした広告を表示する（「ウォリアーズのジャージ、ビッグセール！」）といったことができるのです。

さらにコネクティッドカーにはドライバーの運転行動に関する情報もあります。たとえばジョンは制限時速15マイル（約24キロ）以上で走る傾向があり、ロサンジェルスのダウンタウンでは渋滞した交差点を通ることが多い、といった情報です。保険会社がユーザをトラッキングし、その運転行動に応じて保険料を算出することの是非については賛否両論ありますが、保険会社がこのデータに高い関心を持つことは明らかです。それによって保険料を最適化できる可能性があるからです。

自動車メーカーが進化し、新しいサービス志向のビジネスモデルを開始すれば、当然、近い将来、データの収益化は大きなビジネスチャンスになるでしょう。しかし自動車メーカーはそこに潜む問題を認識しておく必要があります。

ひとつには、データの収益化は利益を自動車業界から奪う可能性があります。たとえば車は無料になって、充電、地図、音楽、駐車料金に対して課金する。これはビジネスのダイナミクスを劇的に変えうる問題です。サービスビジネスに参入した自動車メーカーが、製造工程を外注することさえありうるのです。

さらにデータをどこでどのように収益化するかは税務にも影響してきます。自動車メーカーはそのデータによって経済的利益を得る法人格と所管について、検討する必要があります。

さらに個人情報の共有には大きなプライバシーの問題があります（このことについては後で詳しく述べます）。このようにデータの所有権をめぐる問題は複雑であるため、収集したデータを広告主やマーケットリサーチャー、その他の第三者に販売することによって利益を得ている自動車メーカーはまだありません。

@YourCar：「電気自動車のバッテリーが予想より速く消耗している。水曜日、アレックスのカレンダーに、診断と予防整備のため1時間のサービスセンター訪問を予定」

KPMG

「自動車メーカーはそのサービス事業をサービスセンターの処理能力と合わせることにより、混雑時と閑散時の差を少なくすることができます。保守のためにやってくる顧客の訪問数を平準化することで、いちどきに集中しないようにすることができます。これによってサービスセンターに必要な資本投資が低減し、自動車メーカーがすでに投資したインフラ資産をさらに活用することができます。」

—Danny Le, Principal and Automotive Leader, KPMG Cyber Security Services

「自動車メーカーはドライバーに代わってデータのブローカーとなることができます。たとえばジョンが非常に保守的な運転をする人で、通常は短距離しか走らないなら、そのデータを共有して保険料が下がるかどうかを知りたいと思うかもしれません。セキュリティとプライバシーを熟知した自動車メーカーなら、そういったオプションを提供することができます。そうすれば顧客とサービスのマッチングを向上させることができるのです。」

—Gary Silberg, Partner and National Automotive Leader, KPMG

KPMG

危険な道

消費者の82%は、自動車ハッキングに遭ったことのあるブランドの車を買うことに慎重になるか、または絶対に買わないと答えている。

出所：Consumer Loss Barometer（KPMG、2016年）

データの価値について検討してきましたので、次は自動車メーカーが注目すべきコネクティッドカーのデータに関連するリスクの主要な2つのカテゴリー、すなわちデータセキュリティとデータプライバシーについて詳しくみていきましょう。

データセキュリティ

1人の女性が都会で車を走らせています。車が仕事のメールを読み上げてくれます。女性は駐車スペースに車を入れ、eコマースアプリを使ってスターバックスでラテを注文します。女性のスマートフォンは車と同期しているので、会社の情報や、仕事関連の連絡、クレジットカード情報が瞬時に車のコンピュータを出入りします。そのデータは保護されているでしょうか？　そのデータを保護する責任は誰にあるのでしょうか？　女性の雇用主が、電話で企業のセキュリティコントロールを使って行うのでしょうか、それとも自動車メーカーでしょうか？　あるいは女性のクレジットカード番号を保存している支払いアプリでしょうか？

データセキュリティにはデータの機密性、完全性、可用性の保護が含まれます。データセキュリティが甘ければ、金銭や身元情報、知的財産の盗難、またはさらに悪い結果につながる可能性があります。

コネクティッドカーはデータセキュリティをまったく新しい方向に導きます。なぜなら関わっているものが非常に大きいからです。米国国立標準技術研究所（NIST）が定める情報セキュリティフレームワークの3要素、すなわちデータの機密性、完全性、可用性は人命がかかってくるときには至上命題となります。システムがハッキングされれば、最悪の場合、衝突を引き起こし、ドライバーや乗員に怪我を負わせたり、死に至らしめたりするリスクがあります。交差点に差し掛かっているときや混雑した高速道路を時速70マイル（約110キロ）で走行中にあなたの車がハッキングされたとしたらどうなるでしょう？　あるいは泥棒があなたの電子鍵署名をハッキングして、車を持ち去ったら？　全米保険犯罪局（NICB）によると、この手の車両盗難は増加しているといいます[2]。

自動車へのサイバー攻撃にはさまざまな形があり得ます。ハッカーの標的となるのは、個々の車の制御システムであったり、自動車メーカーの企業システムであったり、ドライバーや乗員の個人情報を含むコネクティッドシステムであったりします。このような攻撃は現実に起きています。自動車ハッキング（car hacking）、サイバー脅威（cyber threats）といったキーワードをインターネットで検索してみてください。

「コネクティッドカーのようなIoTでは、情報セキュリティモデルに物理的セキュリティを含める必要があります。」

—Danny Le, Principal and Automotive Leader, KPMG Cyber Security Services

「データセキュリティに関連する経済的リスクは大きなものになりえます。企業がこのようなリスクをいかに先制的に管理するかを組織の税務計画に組み込む必要があります。」

—Steven Davis, Principal, International Tax, KPMG

2 Thieves go high tech to steal cars（Wall Street Journal、2016年7月5日号）

「データセキュリティとはデータの機密性、完全性、可用性を保護することです。コネクティッドカー環境においては、情報を閲覧する正当な許可を有するステークホルダのみがデータにアクセスできるよう、データを制限することです。」

—Doron Rotman, Managing Director and Privacy Service Leader, Advisory, KPMG

「あなたの車はデータや情報を発信し続けています。車と私たちの個人情報にとって、問題は誰がデータの所有者であり、データを保護する責任は誰にあるのかということです。自動車メーカーでしょうか、車のソフトウェアを設計した第三者でしょうか、アプリのメーカーでしょうか、それともドライバーの通信プロバイダでしょうか？　自動車業界はこのリスクガバナンス上の問いに答えなければならないのです。」

—Ron Plesco, Principal and National Lead, KPMG Cyber Investigations

現実にサイバー犯罪者が走行中の車を乗っ取ったという報告はまだ上がっていないものの、過去数年の間に行われたハッキングに関する会議でこのようなシナリオには現実味があることが示されています。2015年7月、Wired誌は2名のハッカーを雇って検証を行いました。雇われた2名のハッカーは、10マイル（約16キロメートル）離れたところに置かれたノートPCを使って、レポーターが運転するジープ・チェロキーがセントルイスのダウンタウンを走行中に、この車を乗っ取ることに成功しました。室温調整をいじったり、ラジオ局のチャンネルを変えたり、自分たちの画像を車内のデジタルディスプレイに表示させたり、トランスミッションとブレーキを遠隔操作で止めることさえできたのです[3]。この一件のあと、クライスラーは140万台の車両をリコールし、遠隔ハッキングされないようネットワークを更新し、新たなセキュリティ機能を追加しました[4]。その後、2016年3月、連邦捜査局（FBI）と米国運輸省道路交通安全局（NHTSA）はまさにこのシナリオについて市民に警告を発しました。インターネット経由で自動車やトラックが攻撃される可能性についてドライバーに警告したのです[5][6]。しかし2016年8月、同じハッカーコンビが物理的に車に接触することなく、エンジンコントロールユニット（ECU）をいじったり、ハンドルを取ったり、クルーズコントロールの設定を上げたり、エレクトロニックパーキングブレーキを起動することに成功しました。

その他の種類の攻撃は、車のドアを遠隔操作でハッキングして侵入し、車を盗むというものです。こういった事件はこの2年の間にあちこちで報じられています。

サイバー攻撃者が自動車業界を直接標的にすることもあります。自動車メーカーやサプライヤーの調達システムや給与支払いシステムに侵入し、知的財産、M&A情報、従業員や顧客のデータ、銀行関係のデータなど、サイバーアンダーグラウンドや送金詐欺にとって代替可能な価値のあるものなら何でも盗むのです。またサイバー攻撃者は自動車業界を標的にして、氏名、生年月日、社会保障番号、ローン情報、ソーシャルメディア情報といった消費者情報を盗むこともあります。こうした攻撃は企業システム、特にローン／リースの支払いやサービスの支払いなどeコマースシステムが標的になります。

最後に、相互に接続した車のインタフェースを通じて個人が標的にされます。その場合、攻撃者はドライバーの電話やタブレットが車に接続されている間に、その電話やタブレットに侵入しようとします。車載エンタテインメントがマーケティングチャネルとして優勢になっていくにつれ、こんなシナリオさえ描くことができます。いかがわしい広告主がジャンク広告やポップアップ広告をダッシュボードのブラウザやアプリに表示させ、製品を売り込もうとするというシナリオです。こうした手口は現在ノートPCや電話で行われていますが、自動車がコンピュータウィルスやマルウェアに感染した場合、被害の深刻さはノートPCとは比較にならないということです。

3 Hackers Remotely Kill a Jeep on the Highway—With Me In It（Wired、2015年7月21日号）
4 Chrysler recalls 1.4 million hackable cars（CNNMoney、2015年7月24日）
5 Public Service Announcement: Motor Vehicles Increasingly Vulnerable to Remote Exploits（Federal Bureau of Investigation、2016年3月17日）
6 The FBI Warns that Car Hacking Is a Real Risk（Wired、2016年3月17日）

自動運転が現実味をおびてくると、データセキュリティに関わってくるものはさらに大きくなります。2016年5月、自律走行機能を使用中の車が事故を起こし、ドライバーが死亡するという事故がありました[7]。車の制御が人間から機械に移行していく中、データセキュリティの確保はかつてないほどその重要性を増しています。

KPMGの2013年の調査レポート「Self-Driving Cars: Are We Ready?」は、自動運転車市場では安全性と信頼が大きな役割を果たすことを予測しています。我々がインタビューした多くの消費者の間には、コンピュータやスマートフォン、GPSデバイスだってよく不具合を起こすのだから、自動運転車だって不具合を起こすに違いない、という共通認識がありました。また回答者は自動運転車に関していうと、高級自動車ブランドよりもテクノロジー企業を信頼する、とも言っています[8]。

データの可用性を確保することも大きな懸案です。今日のハイテク自動車では、運転にも、フィードバックの提供にも、他の車とのコネクションにも、ドライバーと乗員の生活と活動の管理にも、すべてデータが使われます。データが紛失したり、侵害されたりすれば、このプロセスすべてにおいて機能停止が起こり得ます。そうなれば消費者は不便を強いられ、危険にさらされることにもなりかねません。たとえばお勧めの音楽が好みと違っていたり、サービス警告が然るべきときにポップアップ表示されたりしなくなれば、消費者は自動車メーカーを責めることになるでしょう。

今日、平均的な中型サイズの車にはおよそ40〜50のマイクロプロセッサ主導のシステムが搭載されており、それに必要なコードは2,000万行を超えます。ボーイングジェット機のコードが1,500万行ですから、いかに複雑かがわかります[9]。このような複雑さを考えれば、データフローの不具合が起きうることも、不具合が起きれば自動車メーカーのブランドの評判に傷がつくことも、容易に想像できます。たとえばインフォテインメントシステムは一時期、自動車購入の大きな要因でしたが、出来の良くないものも多く、Consumer Reports Reviews誌のレビューでの評価は下がっています[10]。

データプライバシー

コネクティッドカーとその他のデバイスやシステムとの間のコネクティビティや統合の度合いが高まり、車は膨大な情報にアクセスしています。自動車メーカーはデータの収集、保持、共有を適切に行う必要があります。データプライバシー問題への対応に努めている自動車メーカーにとってはいまだ多くの不確実性が残っています。

@YourCar:「インフォテインメントにソフトウェアセキュリティパッチをロード」

「各種自動車メーカーは、ハッカーに自社の車をハッキングするよう呼びかけ、成功したら報酬を支払うという、バグ報奨金をかけ始めています。このオープンソースな方法により、各種自動車メーカーは脆弱性を発見することができます。」

—Ron Plesco, Principal and National Lead, KPMG Cyber Investigations

7 Fatal Tesla Crash Won't Slow Federal Push for Autonomous Cars（Car and Driver、2016年7月21日）
8 Self-Driving Cars: Are We Ready?（KPMG、2013年）
9 Me, My Car, My Life（KPMG、2014）
10 Brand-by-Brand Guide to Car Infotainment Systems（Consumer Reports、2016年6月2日）

「コネクティビティが増大すれば、車はあらゆる情報にアクセスできます。自動車メーカーはこうした情報が不適切な目的で保持、利用されないよう、万全を期す必要があります。」

—Doron Rotman, Managing Director and Privacy Service Leader, Advisory, KPMG

@YourCar:
「アレックスの血液検査の結果を聞くため、ガルシア医師に電話（電話番号555-321-1234）」

たとえば自動車メーカーが、がんクリニックに通院しているドライバーをトラッキングしているとします。この情報は医療保険会社には隠し、医療機関には共有すべきなのでしょうか？　誰がそれを決め、どのようにその適切性を確保するのでしょうか？　医療保険会社や生命保険会社はその情報を強制的に提出させることができるでしょうか？

コネクティビティが増大し、データの量と複雑さが増しています。特にデータ量の多いモバイルデバイスがコネクティッドカーと同期しています。このような状況の中、自動車メーカーはデータの使用、所有権、収集といったさまざまな新しい問題に直面しています。どのようなデータを収集するのか。収集できるデータに制限はあるのか。同意は必要か。システムのデータに適用される法規は存在するか。どのデータについてどのような使用が許されるのか、といった問題です。

所有権の問題もあります。さまざまな会社がさまざまなコンポーネントを製作し、データプライバシーのルールも進化し続けるため、この問題はいまだ不明です。自動車を製造する企業には自社のネットワーク内のすべてのデータの所有権を主張する権利があるのでしょうか。それともデータを所有するのはドライバーの携帯電話のワイヤレス通信プロバイダでしょうか。あるいはOnStar、Siriusなど、車内でインフォテインメントや通信を提供する会社がデータの所有者になるのでしょうか？

2016年4月、ドイツの代表的なビジネス紙「Handelsblatt」が次のニュースを報じました。Appleはカメラやセンサーを満載し、膨大なデータをiCloudと共有する、高度にネットワーク化された電気自動車「iCar」の開発にあたって自動車メーカーのパートナーを探していたが、BMWともダイムラーとも交渉が決裂した、その原因の1つがデータ所有権をめぐる問題だったというのです。この報道によれば、「AppleはiCarを自社のクラウドソフトウェアに綿密に組み込みたいが、BMWもダイムラーも顧客のデータ保護を将来の戦略の重要な要にしている」というのです[11]。言い換えれば、BMWとダイムラーはデータの商業的価値を認識しているだけでなく、プライバシーに細心の注意を払っていることを前面に打ち出さなければ事業計画と規制要件との間で衝突が起きる可能性があることも理解しているのです。

11 Fighting Over the Driver's Seat（Handelsblatt、2016年4月21日）

規制の問題もまたデータプライバシーの大きな要因です。自動車メーカーは特にデータプライバシー規則により規制される極めてセンシティブな個人情報の保護に万全を期し、さまざまな法域の法を遵守することが必要になるでしょう。たとえば、最近成立した「EU一般データ保護規則(General Data Protection Regulation: GDPR)」では、個人情報を収集し、蓄積し、処理し、共有する企業が遵守しなければならないプライバシー基準が厳しくなっています。またこの規制は違反した場合の制裁金も導入しており、その金額は最高2,000万ユーロまたは会社の全世界収益の4%のいずれか高い方と巨額なものになっています。

さらに中国やロシアといった国にはデータローカライゼーションに関する厳しい法律があります。国民のデータの一次的保管や処理は自国で行わなければならないのです。もしすべての国がその国民のデータを自国が所有し保護することにすれば、自動車メーカーはデータセンターを各国に設ける必要が出てきます。そうなればコストやサービスモデルが変わり、データが利用できる範囲も制限されてくるかもしれません。最後に、地域や国ごとのプライバシー規制は、個人データの移動に制限を設けるかもしれません。マーケティングではなくサービスに必要なデータもその対象になるかもしれないのです。

もちろん消費者が便利さと引き換えにデータプライバシーを犠牲にするのは今に始まったことではありません。ETCやガソリンスタンドの自動支払いパスなどがその例です。将来、コネクティッドカーのオーナーも、ディスカウントやインセンティブ、ソーシャルネットワークとの情報共有機能と引き換えに、ある程度のプライバシーを犠牲にすることは厭わなくなるかもしれません。自動車メーカーは適切なプライバシー(現在どこを走行中とか、何を聴いているかとか)およびセキュリティの管理を確立し、ユーザが自分のデータの利用方法を選択できるようにすることが必要になるでしょう。

コネクティッドカーの中身を深く理解する

@YourCar:
「アレックスの車がレーンをジグザグに動いている。室温を18℃に下げ、『アイ・オブ・ザ・タイガー』を流す」

コネクティッドカーのデータがもたらすリスクとメリットのバランスの取り方を理解するために、自動車メーカーはまずデータがどのようにデータソースから自動車を経由してクラウドに移動し、またその逆をたどるかを理解する必要があります。

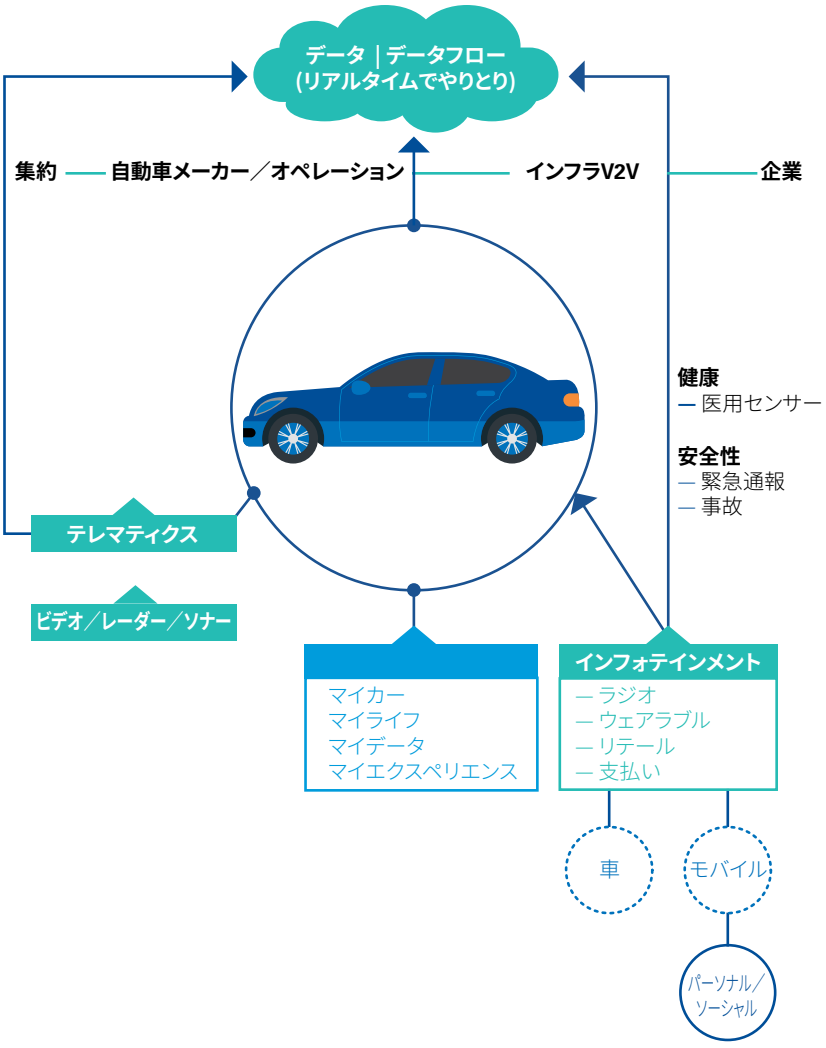
今日製造されるコネクティッドカーにはすべて車載マスターコンピュータシステムが搭載されています。有線、無線合わせて、平均すると60以上のものとつながってマザーボードにデータや情報を供給しています。車載センサーやプロセッサは車のスピードや加速などを計測します。ピンポイントGPSサービスは車の位置を追跡します。ワイヤレスインターネットアクセスはドライバーのスマートフォンやウェアラブル(スマートウォッチやフィットネストラッカー)などの外部デバイスとの同期を可能にします。先進的なテレマティクスやテレメトリーには、車内セキュリティシステムやトラッキング技術、遠隔自動車診断や制御技術があります。堅牢なインフォテインメントプラットフォームが音楽、ナビゲーション、電話などを車のコンソールに直接届けています。

ネットワークを通じてどのようなデータが流れているのでしょうか。コネクティッドカーはセンサーやテレメトリクスを使って、健康や車およびコンポーネントのパフォーマンスについて多くの情報を取り込みます。インフォテインメントシステムや同期した外部デバイスを通じて、個人情報もビジネス関連の情報も、ドライバーや乗員の通信も収集することができます。これには、(1)クレジットカード情報、(2)テキスト、通話、メール、個人の連絡先、(3)バイタルサインや処方箋、病歴などの健康情報、(4)閲覧やショッピング、視聴行動などの消費者に関するものがあります。GPSユニットおよびトラッキング技術によって収集されるデータにはその他に、車の位置情報やルート、動きがあります。

ではこのデータはどこへいくのでしょうか。この問いについては、ネットワークがクラウド、実際には複数のクラウドと相互につながることで複雑さが増します。データは自動車メーカーの自社プライベートクラウドにとどまるかもしれないし、音楽ストリーミングやナビゲーションなどのコンテンツ配信システムが所有するクラウドへ行くかもしれないし、広告主や事業者や政府機関などの第三者のところへ行くかもしれないのです。

重要なポイントは次のとおりです。自動車メーカーは消費者のアクティビティデータの使用と配布について消費者に責任を負うことになります。実際、消費者が自分のデータを使用する権利の取り消しを申し出た場合、自動車メーカーはエコシステム内の全当事者からその権利を取りあげることができなければならないのです。そのために自動車メーカーは消費者に代わって、データの在り処を常に把握し、それをどのように管理、制御するかを熟知していなければならないのです。

KPMG



データソース：

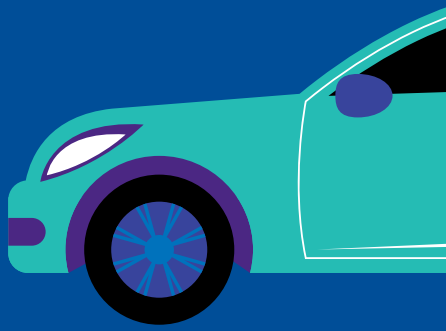
— キャビンの設定
— GPSユニット
— 車載センサー
— スマートフォンやウェアラブルなどの外部デバイス
— テレマティクスとテレメトリー
— インフォテインメントプラットフォーム

データの種類：

— 個人情報
— 位置および経路
— 健康情報
— 消費者インサイト

データフロー：

— 自動車メーカーのプライベートクラウド
— 自動車メーカーの収益化データベース
— 政府がアクセスできるプラットフォーム
— 第三者ネットワーク



KPMG

コネクティッドカーのサイバーセキュリティ

コネクティッドカーが行うすべての会話（行き来するすべてのデータ）について、自動車メーカーは、聞くべき人だけが聞けるように（アクセスすべき人だけがアクセスできるように）しなければなりません。これは簡単なことではありません。

サイバーセキュリティの観点からいえば、閉ざされた自動車システムはコネクティッドなエコシステムに比べるとはるかに安全です。コネクティッドなシステムには侵入できるポイントが多いだけでなく、自動車と第三者の間でセキュリティの確保が必要な通信が多く行われているからです。コネクティッドカーには網の目のように複雑なコネクティッドシステムが張り巡らされており、1つのシステムに侵入されれば、他のすべてにアクセスされてしまいます。情報漏洩の影響は倍増してしまうのです。

さらに、車はますます情報主導型になってきています。これは保護すべきデータの量も増大しているということであり、またデータ自体がさらに個人的かつセンシティブなものになってきており、運転や移動といった行動にとって欠かせないものになってきているということです。

さらにこの問題を複雑にしているのは、自動車はそもそも確実に安全なアーキテクチャを念頭に置いて設計されてはいないということです。自動車メーカーにとって車は機械的な物体なのであり、将来自社の車がインフォテインメントを提供したり、外部とのコネクティビティを持ったり、データを第三者と共有したり、機微情報を収集したりすることになろうとは思っていませんでした。自動車メーカーは、搭載するハイテクコンポーネントの数が増え、コンポーネント同士がつながるにつれ、システムを保護しなければならないことは知っていました。そのための最も簡単で安価な方法とは？　それは単一のフラットなネットワークにセキュリティの層を重ね、パッチを重ねる方法でした。

問題はそこです。航空機では、ネットワークは機能ごとに分かれています。飛行に関する系統と、Wi-Fiを使ってオンライン動画を再生する系統は別になっています。よってデータセキュリティとプライバシー全体を強化することができます。しかしコネクティッドカーの場合、全システムが単一のネットワークを共有しています。つまり1つのシステムにアクセスすれば、全部のシステムにアクセスできる可能性があるのです。現実の世界でこれが意味するところは、ハッカーがドライバーのスマートフォンの脆弱性を見抜き、スマートフォンにつながっている車のシステムから情報を盗み出すことができるかもしれないということです。あるいはエンジンやブレーキといった、車の操縦システムを乗っ取ることさえできるかもしれないということなのです。

たとえ技術的なことを理解するのが難しくても、コネクティッドカーに潜むデータリスクは消費者、規制当局、自動車メーカーのいずれにとっても明らかです。このため、自動車のデータ、ソフトウェア、システムに特化した業界グループが続々と現れてきています。このようなグループには、サウスウエスト研究所の自動車組み込み安全性コンソーシアム（ACES）や、SAE自動車電子システムセキュリティ委員会、米国自動車研究評議会サイバー・フィジカルシステム（CPS）タスクフォースなどがあります。

@YourCar：「中国の不明なIPアドレスがハンドル制御へのアクセスをリクエストしているため、このIPアドレスのアクセスを拒否」

自動車メーカーの85%が過去2年間に会社のシステムにサイバー攻撃を受けたことがある。

自動車メーカーの3分の2が情報セキュリティへの投資をまだ行っていない。

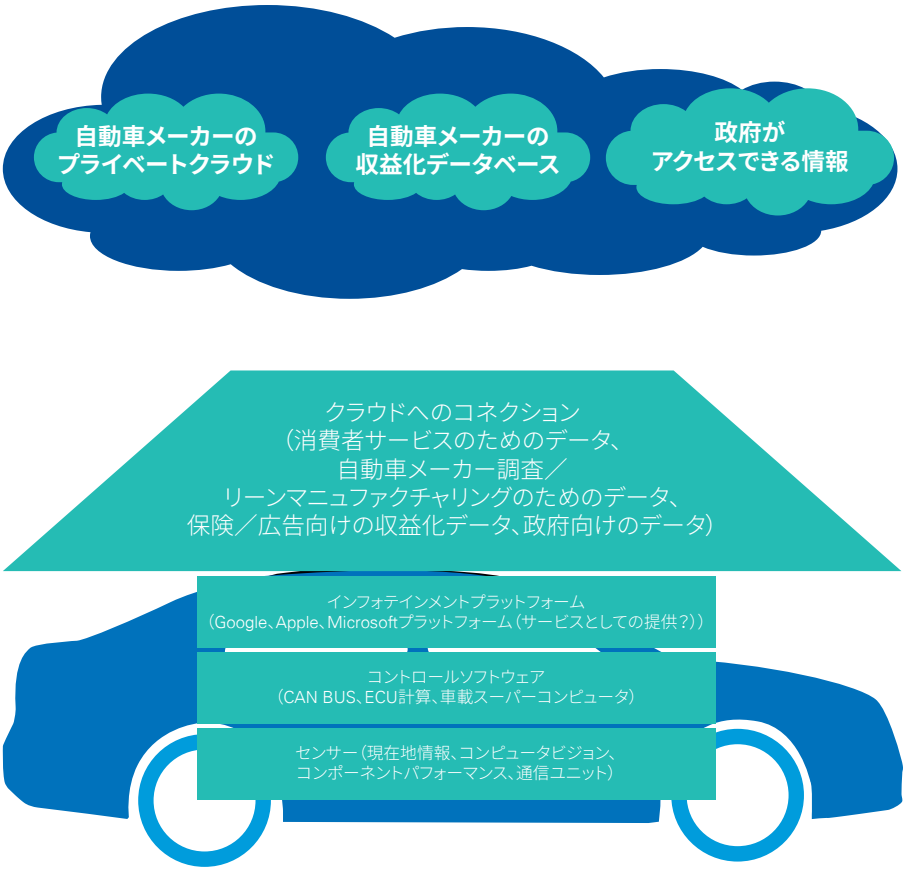
出所：Consumer Loss Barometer（KPMG、2016年）

「サイバーセキュリティに関していえば、自動車メーカーは後れを取っています。なぜなら自動車メーカーは伝統的な製造業であり、オープンかつアクセス可能でインターネットにつながったネットワークのセキュリティモデルというものに慣れていないからです。これからのセキュリティニーズを満たすモデルや方策の開発は長く複雑なプロセスになりますが、今日の自動車メーカーはサイバーセキュリティを戦略的必須事項として、自社の車に乗るドライバーを保護する必要があるのです。」

—Danny Le, Principal and Automotive Leader, KPMG Cyber Security Services

「現在、コネクティッドカーにはセキュリティが確保されていません。これは自動車の伝統的な設計手法に起因します。マスターコンピュータシステムには平均で50以上のECUが内蔵されています。この他にディーラーやメカニックと共有している診断情報もあります。現在、自動車メーカーはモバイルデバイス、アプリ、サテライトラジオなどとの相互接続性を層状に重ねており、タイヤやブレーキといった車両システムがインフォテインメントシステムや接続デバイスと別にはなっていません。これがセキュリティリスクなのです。」

—Ron Plesco, Principal and National Lead, KPMG Cyber Investigations



各々のレベルで:どのデータを収集するか？　保存するか？　共有するか？

KPMG

データの行きつくべきところ

では企業はコネクティッドカーにより収集されたデータがもたらす潜在的なビジネスチャンスと、データの不適切な取り扱いや漏洩によって生じるリスクとのバランスをどのように取るべきなのでしょうか？

検討すべき主要事項は次のとおりです。

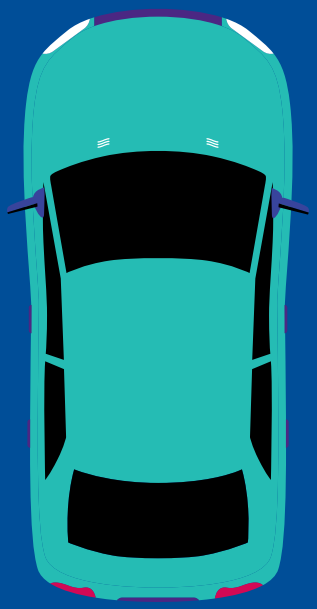
セキュリティとプライバシーを製品やソフトウェア開発の早い段階で埋め込む。
今日、サイバーセキュリティは自動車業界において「後付け」的な扱いになっており、これがリコールのような、すでに路上を走っている車に対する、コストもかかり、混乱も招く修理や軌道修正につながっています。今後は自動車メーカーの開発者やエンジニアがコネクティッドカーのソフトウェアコンポーネントを開発する全段階に、サイバーセキュリティを組み込むべきであると思います。

自動車メーカーがプライバシーやサイバーセキュリティの問題をソフトウェア開発ライフサイクルの全段階（初期概念の発表から、ソフトウェアの要件概要、設計、コーディング、テスト、インストールに至るまで）に組み込めば、そのメーカーの車は設計的に安全なものになります。セキュリティの脆弱性を早い段階で見つけ、修正することができるので、路上に出てしまってから大きな問題に発展するのを防ぐことができます。

サイバーセキュリティを全社的リスクガバナンスに反映させる。
コネクティッドカーのメーカーが直面している、重要なデータセキュリティ上の脅威の多くは、サイバーセキュリティを事業運営上の問題と捉え、より大規模なリスクガバナンスの議論へとレベルを上げることによって、対処を始めることができます。多くの自動車メーカーやサプライヤーがサイバーセキュリティを全体的なリスクガバナンスの方策に組み込もうとしています。それによってサプライチェーン、設計、製造プロセス、サービスに至るまで、サイバーセキュリティ、データプライバシー、データの保護をライフサイクル全体に埋め込むことができます。さらに自動車業界はビジネスコンサルティング会社に依頼して、このガバナンス方策の評価、設計、実施を進めています。

コネクティッドデバイスのエコシステムの進化は、大きな課題を生み出しています。新たな脅威が頻繁に出現し、境界を定めるのが難しい環境で、責任をもって安全なデバイスを開発し、構築しなければならないからです。コネクティッドカーのリスクに関して予防的かつ探知的な方法を構築しようとするならば、ビジネス戦略決定から継続的リスクマネジメントに至るまで、ガバナンスと監視を行う全体的なアプローチを用いて、責任あるコネクティッドカープログラムを作り出さなければなりません。

サイバーセキュリティ能力を社内で開発するか、外部から調達するかという問題については、自動車メーカーは情報保証（IA）やフォレンジックといった重要な分野の知識とスキルを向上させるべきだと考えます。まずは出発点として、組織的、技術的なレベルでセキュリティの問題を取り扱う中央部門、セキュリティオペレーションセンターを立ち上げると良いでしょう。



データだけでなく、エコシステム全体に目を向ける。
コネクティッドカーにおいて、データは車だけでなく、エコシステム全体を通じて流れています。このデータには、車で収集され第三者と共有されるものだけでなく、クラウドから車に流れ込んでくるものも含まれます。

データの分析はさまざまなエコシステムの参加者によって、さまざまな目的、さまざまなサービスレベルで行われます。ですから、エコシステム全体が安全で連携が取れており、エコシステム内のすべてのデータの品質が信頼できる正確なものでなければなりません。

よって自動車メーカーは車を超えたところにも目を向けなければならないのです。自動車メーカーは車から収集されるユーザデータおよび自動車データのセキュリティを設計し、所有すべきです。自動車メーカーは車が収集するデータを他のエコシステム参加者がどのように利用し、やりとりするかについて、規格や方策をコントロールできるまたとない機会を手にしているのです。

自動車メーカーはこれに投資しなければなりません。自動車メーカーがこの規格をコントロールしなければ、他のエコシステム参加者に対して劣勢に立たされてしまうかもしれません。他のエコシステム参加者はこのデータの取得における自身の役割を商品化するかもしれないのです。

顧客のデータプライバシーに関して良き市民となるべし。
車のコネクティビティの度合いが高まるにつれ、あらゆる行動が追跡され、記録され、共有されると言っても過言ではありません。車のオーナーがそれについて真剣に考え本当に理解しているとは限りません。よって責任を持って顧客データを適切に管理することは、自動車メーカーにかかってきます。

自動車メーカーはどのようなデータを収集し、それをどのように利用するのかについて完全な透明性を提供するよう努めなければなりません。データプライバシーポリシーに変更が生じたときには、顧客に適切な通知を提供するべきです。自分に関するどのデータを誰と共有するかについては、顧客に選択権を与えるべきであり、また自動車業界のプライバシーガイドラインを自主的に遵守すべきです。すでにそうしている自動車メーカーもあります[12]。

留意事項：プライバシーに関する顧客の想定を常に念頭に置くこと。そしてデータの利用は顧客が想定し、承諾する範囲にとどめること。

データセキュリティの3要素に留意する。
前述のように、NIST情報セキュリティ規格の3要素は機密性、完全性、可用性です。機密性はデータを難読化し、隠すことができる能力です。完全性はデータが無断で変更できないようにすることです。可用性は必要なときにデータにアクセスできることです。

KPMGはコネクティッドカーを含むIoTのセキュリティ確保には、コントロール、プライバシー、信頼が必要であり、それはデータの機密性、完全性、可用性のバランスを取ることで達成できると確信しています。

12 Connected Cars: Dealing with data privacy (Telematics Wire)

KPMG

新たなセキュリティリスクに備える。
テクノロジーは変化し続けています。そしてテクノロジーの変化には新たなセキュリティリスクが伴います。自動車メーカーは新たなセキュリティリスクを予測するよう、常に目を光らせていなければなりません。

たとえば最近では、各社ともコネクティッドソフトウェアのOTA（無線通信）アップデートを導入し始めています。タイヤのソフトウェアノードにソフトウェアパッチを追加するなどです。ちょうどAppleやSamsungのスマートフォンでアプリをアップデートするときのように、簡単で透明性があり手軽です。これは今日の自動車メーカーにとってわくわくするような可能性です。すべてのソフトウェアコンポーネントがシームレスにマスターコンピュータにつながることが理想だからです。しかし少し掘り下げて考えてみる必要があります。ソフトウェアのOTAアップデートはサイバーリスクを伴うからです。アップデートを有線で行うことはできるでしょうか？　Wi-Fi経由は？　安全な回線が必要でしょうか？　データは暗号化すべきでしょうか？

マスターコンピュータに入ってくる情報を暗号化する。
サイバーセキュリティの成否は車のマスターコンピュータシステムの脆弱性に大きく依存します。ですから自動車メーカーはマスターコンピュータに通信する外部デバイスからのデータ、すなわちドライバーや乗員からのインプットの暗号化を検討すべきであると思います。

自動車メーカーは、暗号化がサイバーセキュリティプログラムのコストを上昇させることを認識する必要があります。また暗号化されたデータは暗号化されていないデータよりも容量が大きいので、システムのバンド幅の問題を引き起こす可能性があることも認識する必要があります。しかしこれは投資に値すると思います。データのプライバシーと保護、安全性、信頼性について貴社のブランドを保護し、前進させれば、「セキュリティの差別化要因」ともなるでしょう。

脆弱性をテストする。
ハッカーを雇って、コネクティッドカーのセキュリティの弱点を暴くことを検討してください。フィアット・クライスラーやテスラモーターズはセキュリティ上の弱点を見事に突き、全詳細とその方法について報告したハッカーに数千ドルの報奨金を提供しています[13]。他社も見習うべきでしょう。

このようなプログラムは車載ソフトウェアのセキュリティの脆弱性について大きな教訓を与えてくれます。自動車メーカーはそれによって、新たなサイバー脅威や自社のソフトウェアの弱点を理解することができます。

「プライバシーの観点からは、データの所有権は非常に曖昧です。あなたの車のデータは誰が所有しているのでしょうか？　たとえば、あなたの車のECUのソフトウェアは、OEMや製造会社の所有権、著作権で保護されており、あなたのものではないのです。」

—Ron Plesco, Principal and National Lead, KPMG Cyber Investigations

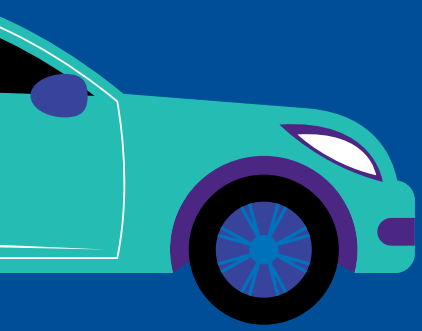
「テクノロジーが速いペースで変化していることを考えると、あらゆるイノベーションや事業の変更に関する税務計画を検討すべきでしょう。既存の税務計画戦略はもはや新しいテクノロジーと相容れない可能性があるからです。」

—Steven Davis, Principal, International Tax, KPMG

13 The automotive industry should enlist hackers to aid in cybersecurity, panelists say.（Automotive News、2016年7月22日）

「プライバシーは、セキュリティや価値と同じく、消費者の信頼の重要な要素です。コネクティッドカーメーカーが製品に対する消費者の信頼を勝ち得て、製品を買ってもらうためには、この3つのバランスを取る必要があります。」

—Doron Rotman, Managing Director and Privacy Service Leader, Advisory, KPMG



安全性を第一に。

自動車メーカーは一にも二にも、安全で信頼できる品質の高い製品を市場に出すことが使命です。安全性と信頼性は消費者が自動車ブランドに求めるものです。消費者はダッシュボードからボイステキストを送信できない車は許容しても、警告もなく故障したり、ドライバーを危険な状況に導いたり、サイバー犯罪者にブレーキのコントロールを乗っ取られるような車は許容しないでしょう。

言い換えれば、コネクティッドカーに関する議論は華やかな新機能や最新のセンターコンソールに終始してはならないのです。それよりも、車の機械系統や電気系統内の、インターネットにつながったテレメトリックセンサー群の方が重要といって良いでしょう。事故を予防できるからです。

よって自動車メーカーはコネクティッドカーのテレメトリーデータを使用して、核となるブランドの強みを強化し拡大することにより、何よりもまずユーザの身体的な安全性を確保することに焦点を当てるべきだと思います。たとえばテレメトリーデータによって、自動車メーカーは路上走行中の車のシステムをリアルタイムでモニターしたり、警報やダッシュボード警告を発したり、問題を検知することができます。人々の安全を守るため、自動車メーカーはデータを所有するだけでなく、そのデータをうまく管理し、セキュリティを確保する必要があります。

「三脚椅子」を組み立てる。

どのような新しいテクノロジーもそうですが、消費者の信頼がすべてです。人々が自分のコネクティッドカーを信頼しているなら、つまりコネクティッドカーは乗員の安全を確保し、生活を便利にし、個人情報を適切に管理してくれていると感じられるなら、顧客は満足してくれるでしょう。消費者は見返りがなければ、自分の個人情報を喜んで明け渡したりはしません。たとえばある地点から別の地点への移動にかかる時間が短縮されるとか、前方の道路で起きていることを知らせてくれるといったことです。同じように、消費者は自分の個人情報が安全に保護され、意に反して悪用されたり、知られたくない人に知られたくないことを知られたりするようなことが起きないことを期待しています。

よって自動車メーカーは消費者の信頼を三脚椅子に見立てて考えると良いでしょう。三脚は価値、セキュリティ、プライバシーです。自社のコネクティッドカーにこのうち1つでも欠けていれば、椅子はひっくり返ります。しかし3つすべてが揃っていれば、椅子は極めて長期間安定するのです。

KPMG

KPMGについて

KPMG Automotiveチームは現在自動車業界の潮流となっている複雑さを理解しています。業界に対する深い洞察力と現場での実践的な経験を活かし、自動車業界の皆様が今日の業績を強化するとともに、未来の成功を形作れるよう支援しています。また、機能横断的なアプローチを用いて、世界をリードする製造業者、自動車メーカー、サプライヤーの皆様がその目標を達成できるよう、後押ししています。豊富な経験と業界に特化した知識を用いて、クライアントが下す今日の決定が将来、最大のインパクトを生み出せるよう、指針を示しています。

お問合せ

KPMGジャパン

小見門 恵
KPMGコンサルティング株式会社
パートナー
T：03-3548-5307
E：megumu.komikado@jp.kpmg.com

井口 耕一
株式会社 KPMG FAS
パートナー
T：03-3548-5776
E：koichi.iguchi@jp.kpmg.com

twitter.com/kpmg_jp
facebook.com/kpmg.jp

この文書はKPMG米国が2016年11月に発行した「Your connected car is talking. Who's listening?」を翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織がおかれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点およびそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

本冊子で紹介するサービスは、公認会計士法、独立性規則及び利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。