スマートカーのサイバーリスクに関する事例分析

自動車メーカーは先端テクノロジーガバナンスをどう確立すべきか？

昨今、自動車に搭載されたテレマティクスシステムやソフトウェアのセキュリティ脆弱性を悪用して、運転席に座ったり車両に直接触れることなく、極めて重要な車両制御システムや駆動系部品など数多くの車両機能を制御できてしまうという事例がいくつも公表されている。あるセキュリティ研究者は、こうした脆弱性は一般に普及しているノートPCからでも悪用できると指摘しており、同様の脆弱性を持つ車両モデルも発見されていないだけで、実際には多数存在する可能性があると考えられる。

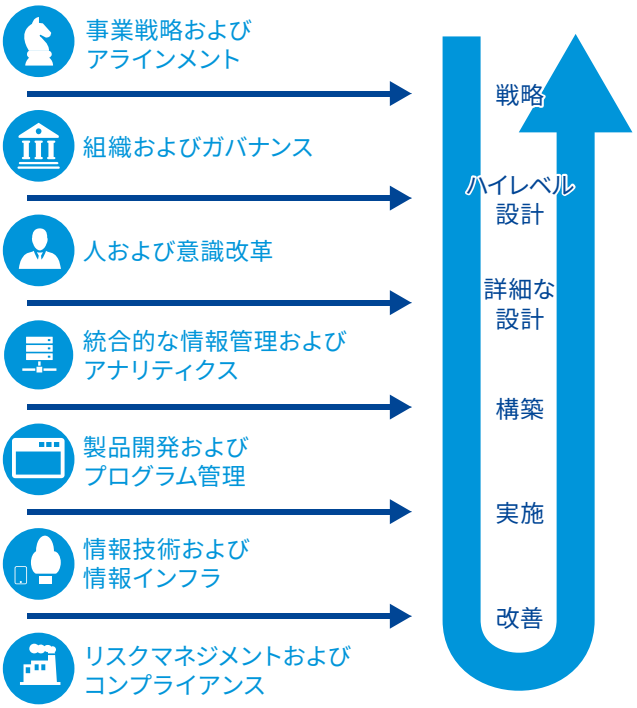
これまでに公表されているセキュリティの脆弱性やそれを悪用した事例の多くは、高速道路を一定の速度以上で走行しているときなど、限られた条件が揃ったときにのみ有効になるものであり、一般利用者の安全性に直ちに重大なリスクを及ぼすわけではない。むしろ、これらの事例は業界のより広い分野で、スマートカー・スマートドライブ戦略やガバナンスモデルについて再検討を促すきっかけとみることができる。今後はネットワーク接続技術によって持続的革新の機会や必然的ニーズがますます増えていくと同時に、業界がこうした破壊的な行為に“冷静かつ責任ある形”で対応していく必要性も高まるだろう。

新たな接続リスクに対応するための枠組み

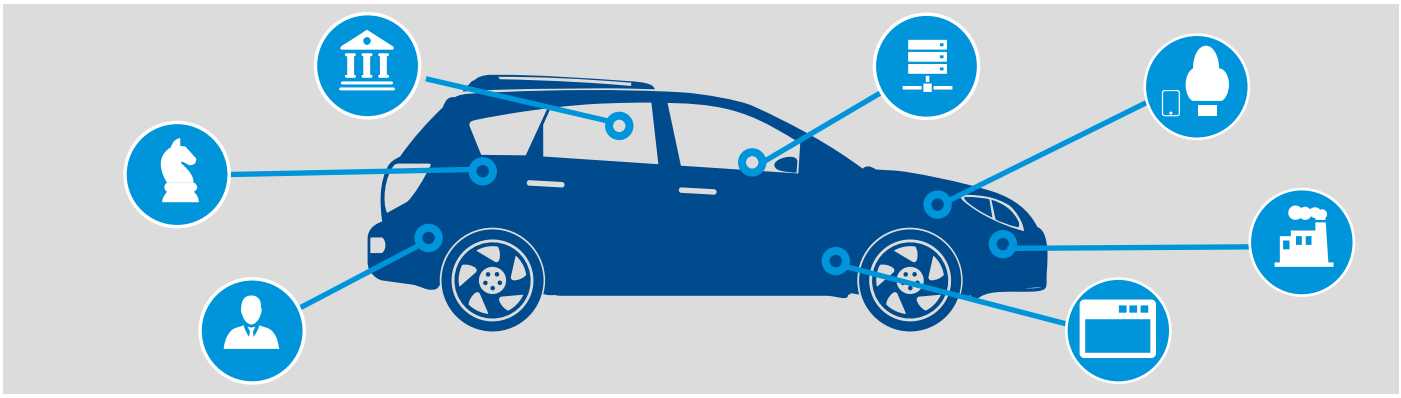
ネットワーク接続機器（コネクテッドデバイス）におけるエコシステムの進展は、新たな脅威が頻繁に出現し、リスクの境界を明確に定義しにくい環境において、信頼できるセキュリティを確保した機器を開発・製造するうえで重要な課題を提起している。

KPMGのコネクテッドデバイス提供フレームワーク（CDDF: Connected Device Delivery Framework）は、継続的なリスクマネジメントを通じた事業戦略上の意思決定に基づいてガバナンス機能や管理機能を提供する包括的なアプローチを採用しており、責任を持ってスマートカープログラムを構築するための基盤と体制を提供するものである。

KPMGでは、最近のスマートカーにおけるサイバー脆弱性の事例を使って、CDDFではスマートカーのリスクに対する予防措置やリスク検出手段の構築がどのように策定されるかについて分析した。



KPMGサイバーセキュリティアドバイザリー



事業戦略およびアラインメント

事例

革新的技術と遠隔操作機能により、車両の安全性に新たな未知の脅威が生まれた。

推奨事項

- サイバーセキュリティ上の検討事項を、戦略的計画立案上の決定と車両設計の重要な要素として組み込むこと
- IT、セキュリティ、リスクの側面から見た適切な意見を事業戦略上の決定に盛り込むこと

人および意識改革

事例

脆弱性の改善のために車両のリコールをしなければならなかった。

推奨事項

- 無線ネットワークを利用したOver-the-air（OTA）でのパッチ提供により、リコールを防ぐこと
- 消費者にテレマティクス機能を解除できるという選択肢を与えることにより、消費者にまだ自分の車両を制御できているという安心感を与えること
- 技術上のリスクに関して消費者をより適切に啓蒙するためのディーラー研修プログラムを強化すること

製品開発およびプログラム管理

事例

脆弱な無線受信機やファームウェアのために遠隔制御が可能になり、システムコードを書き換えることができた。

推奨事項

- 「設計によるセキュリティ」という原則を製品開発ライフサイクルに組み込むこと
- 開発上の重要な節目ごとに侵入テストを実施すること
- リバースエンジニアリングの防止に役立つようにファームウェアを暗号化すること

リスクマネジメントおよびコンプライアンス

事例

新たに、車両のサイバーセキュリティ基準や消費者向けプライバシーおよびセキュリティ評価システムを立法化する可能性がある。

推奨事項

- 規制監視チームを設置することにより、積極的に規制当局を参画させ、政策や基準の策定への影響力行使に貢献すること
- ネット接続車両のプログラムガバナンス委員会を編成することで、ネット接続車両戦略、進行中のリスク、市場での進展状況を監視すること
- テレマティクスとネット接続プログラムを内部監査・企業リスク管理の計画立案プロセスに組み込むこと

組織およびガバナンス

事例

携帯電話ネットワークを通じて遠隔操作により車両に接続することができた。この脆弱性は、テレマティクス機能を提供するプロバイダーの問題により可能となった。

推奨事項

- サードパーティベンダーとのコミュニケーションやコラボレーションを強化することにより、セキュリティおよびプライバシー上のリスクを積極的に管理すること
- サードパーティベンダーに対するセキュリティ基準の実行と監視を強化すること
- サードパーティベンダーに対して定期的に脆弱性の評価と監査を実施すること

統合的な情報管理およびアナリティクス

事例

携帯電話ネットワークをスキャンし、脆弱なソフトウェアを搭載した車両のGPS座標軸、車両ID番号（VIN）、構造、型式、IPアドレスを閲覧することができた。

推奨事項

- 製品設計全体を通じてデータガバナンスを強化し、適切に分類することにより、GPS座標軸やVINを含む消費者データを保護すること
- サードパーティベンダーとの間で消費者情報をやり取りする必要性を検討し、データ所有と利用要件を定義すること
- 送信時に消費者データや車両データを暗号化すること

情報技術および情報インフラ

事例

極めて重要な車両駆動系部品のセキュリティが十分に確保されておらず、また無線システムやメディアシステムから正しく分離されていなかった。

推奨事項

- 極めて重要な駆動系部品には、分離されたコントローラ・エリア・ネットワーク（CAN）を義務づけること
- リモートコマンドを送信する際に特定の認証署名を必要とするセキュリティ制御装置を設計すること
- 車両侵入検出システムを設置し、悪意のある接続を積極的に特定すること

KPMGサイバーセキュリティアドバイザリー

得られた教訓

幸運なことに、業界の意識を高め車両のサイバーセキュリティを向上させるための事例としてこれを活用するという意図を持ったセキュリティ研究者により、こうしたスマートカーの脆弱性は特定された。多くの技術と同様に、セキュリティが完璧に確保された状態というのは現実的ではないだろうが、過去の出来事から学び、ガバナンスのプロセスや統制システムを確立することにより、将来、よからぬ出来事が起こる可能性やその影響を抑えることに貢献することができる。それには極めて重要な5つのステップがあり、KPMGでは、自動車業界においてそれらが役立つことと期待している。

1. ネットワーク接続機器（コネクテッドデバイス）を開発する組織は強固なエンタープライズリスクおよびガバナンス活動を確立することにより、革新的戦略と先端テクノロジーリスクとの間の適切なバランスを確保しなければならない。

2. サイバーセキュリティおよびデータプライバシーについては、車両技術設計のすべての側面に組み込まなければならない。無線機能や遠隔アクセス機能については、徹底的な脆弱性・侵入テストの対象とすべきである。

3. 極めて重要な駆動系部品を、遠隔アクセス機能から多層的かつセキュリティが確保された形で分離することを義務づける。資産分類に関する原則を活用し、極めて重要な車両部品の特定と分類を行う。

4. 持続的脆弱性管理プログラムとタイムリーかつ効果的な修正プロセスが、自動車メーカーにとって、顧客サービスを改善し消費者の信頼を得るうえで新たに取り組むべき領域となっている。セキュリティ上の修正は前向きに行うべきものであり、利便性の高い方法で提供すべきものである（たとえば、無線による修正等）。

5. サードパーティベンダーは車両のサイバーセキュリティ向上に不可欠な要素となっている。強固な監視プロセスは、ベンダーに目を配り、制約を課し、詳細なセキュリティ要件を適用するものでなければならない。自動車メーカーを問わず、またどれだけ多くのベンダーがそのネットワーク接続エコシステムを構成しているかを問わず、サイバーセキュリティリスクは究極的にはOEMの責任体制、また多くの場合には、その説明責任のなかに存在する。

KPMGサイバーセキュリティアドバイザリー

今後の規制上の変更点

2015年7月21日、サイバー脆弱性によりドライバーの安全性に対する懸念が高まっていることを受けて、エドワード・J・マーキー上院議員（民主党、マサチューセッツ州選出）とリチャード・ブルーメンサル上院議員（民主党、コネチカット州選出）は「マイカー・セキュリティ & プライバシー法案（SPY Car Act: Security & Privacy in Your Car Act）」を議会に提出した。この立法案では、米国高速道路交通安全局（NHTSA）と連邦取引委員会（FTC）が、自動車メーカーを対象とした連邦基準を策定・実行することにより、車両のサイバーセキュリティを向上させドライバーのプライバシーを保護するよう指導することになるだろう。そして、こうした新たな連邦基準は、下記の規定を実行することで、自動車メーカーにさらに強固なガバナンスとプロセスの透明性を義務づけることになるだろう。

- ハッキングからの保護、データのセキュリティ、ハッキングの軽減を含むサイバーセキュリティ基準
- 透明性、消費者の選択、マーケティング上の禁止事項を含むプライバシー基準
- 車両が連邦セキュリティやプライバシー基準に照らして、どの程度適切にその性能を発揮しているかを消費者に知らせる、サイバーダッシュボード

SPY Car法が「モノのインターネット（IoT）」に直接対応する最初の連邦法案となるなかで、ネットワーク接続機器（ここではスマートカー）のリスクに対してガバナンスを求める声が高まっていることは明らかである。この法律が最終的に成立するか否かにかかわらず、自動車メーカーはさらに厳格なセキュリティおよびプライバシー要件を適用し、自社の消費者を保護することが期待されている。

KPMGの先端テクノロジーリスクサービスについて

テクノロジーがビジネスに与える影響を否定することはできない。クラウド、コネクティビティ、モバイル、サイバーセキュリティ、IoTが職場に浸透し、ワークスタイルを変えつつある。これにより、組織はこれまで以上に思考を速め、柔軟に対応し、テクノロジーとビジネスとの間でどのように整合性を確保していくのかについて工夫することを余儀なくされている。KPMGの先端テクノロジーリスクサービスとサイバーセキュリティアドバイザリーサービスは、クライアントがこの新たなデジタル世界において責任ある形で事業を展開していくことを支援している。テクノロジーやリスク管理の専門家で構成されるKPMGの優れたネットワークが、クライアントの事業を評価し、そのリソースとKPMGのパワーを投入することにより、リスクと業績のバランスを最適なものとする。その結果、クライアントは安心感とさまざまなプラットフォームを管理するための柔軟性を得て、適応性に富んだ事業ソリューションを実現できる。また、組織はその目標達成を妨げる破壊的な力に影響されることなく、先端テクノロジーのメリットを享受することが可能となる。

KPMGサイバーセキュリティアドバイザリーグループ
cybersecurity@jp.kpmg.com
www.kpmg.com/jp/cyber-security