クルマのセキュリティー対策を加速せよ

クルマの信頼性とデータ・プライバシーのレースに勝つために

IBM Institute for Business Value

Executive Report
Automotive

IBM の自動車業界ソリューション

今日のクルマは、センサーやコンピューターを搭載しクルマに関わるデータを収集する「走るデータセンター」と言えるでしょう。それらのデータにリアルタイムにアクセスし、「つながる」時代の消費者がクルマに関する体験に期待する新たなサービスを構築するため、IBM は自動車業界の取り組みをご支援します。IBM の自動車ソリューションは、IBM Watson によるアナリティクスをはじめとする革新的なテクノロジーを採用し、完成車メーカーからサプライヤーにまで対応します。これらのソリューションは、安全で信頼性が高く、ブランド力や顧客満足度を向上させるような製品やサービスを構築することを可能とします。詳細は Web サイトにてご覧ください。
https://www-935.**ibm.com**/industries/jp/ja/automotive/

防御、検知、対応

2014 年、IBM はクルマのセキュリティーに関する報告書「Driving security: Cyber assurance for next-generation vehicles」を公開し、セキュリティーのライフサイクルへのアプローチとして「設計、製造、運用」という 3 つのフェーズの概念を提唱した。[1] 今まさに、この概念について掘り下げて検討すべき時期に来ている。クルマのセキュリティーに関する議論では、「運用」フェーズで検討すべきクルマ自体とプライバシーへの脅威に対する関心が高いため、本稿ではこの「運用」フェーズに重点を置いて論ずることにする。「運用」フェーズは、消費者が最も共感しやすいフェーズであり、かつ自動車メーカーにとっても脆弱性をついた不正アクセスの防御、不審行動の検知、迅速かつ正確な対応に関するテクノロジーの評価が比較的容易なフェーズでもある。

エグゼクティブ・サマリー

コネクテッドカー、その誕生を主導したのは消費者だ。いつの時代もクルマでの旅行に音楽は必需品だった。かつての 8 トラックのオーディオ・プレーヤー（カー・オーディオ用のカートリッジ式の磁気テープ再生装置）の時代は、いつしか何千もの曲を保存できるスマートフォンの時代へと移行した。そして、クルマのスピーカーからストリーミングで流れてくる音楽が聴けることは当然だ。

簡単そうに思えるが、クルマを外部の機器と接続するのは意外と難しい。例えば、クルマに Bluetooth の機能があっても、同乗者に Wi-Fi のホットスポットとしての機能を提供できないのは何故だろうか。IBM のビジネス・シンクタンクである IBM Institute for Business Value が最近行った調査「A new relationship — people and cars（邦訳：人とクルマの新たな関わり）」によると、調査対象の消費者のうち 49% が、今後 10 年以内にクルマは安全に接続できる IoT デバイスの 1 つになるだろうと予想する。[2]

現代の旅行者は、複数の交通手段を乗り継ぎながらも、常に一貫性のあるパーソナライズされたデジタル体験を望む。旅行者の情報は様々なテクノロジーで共有されているが、インターモーダル輸送（異なる輸送機関を組み合わせて運ぶ輸送形態）を利用する彼らは一人ひとりが独立した存在であるため、データの活用に際してはガバナンスとプライバシーに大きな懸念がある。例えば、旅行者がある交通手段から別の交通手段に乗り換えた場合、この個人データは最初の交通手段から完全に削除されることが保証されなければならない。また、旅行中に取得された個人データは、最終的に削除されるまで適切に保護され、暗号化された状態で最短期間のみ保持されることも保証される必要がある。

今のところ、このようなコネクテッド機能が悪用された例はそれほど多くない。最近では、クルマの制御を奪うことが可能だとする実験など、不安をあおるような研究報告がニュースを騒がせているが、クルマの脆弱性をついた大規模なセキュリティー被害はまだ現実のものとなっていない。[3] 現在、マルウェアやランサムウェアの格好の標的となっているのは、デスクトップ PC やノート PC、さらには携帯電話やタブレットといった汎用的なコンピューティング・プラットフォームである。ただし、これら標的への侵入は各種セキュリティー機能の向上により難しくなっているため、攻撃者がコネクテッドカーをはじめとする IoT にその矛先を向けることも予想される。[4]

消費者の 56% が、将来のクルマの購入においては、セキュリティーとプライバシーが重要な判断軸になるだろうと答えている

コネクテッドカーの時代では、**セキュリティーが担保されて、初めてクルマの安全性は確保される**

セキュリティーの理念は、企業の DNA に組み込まれ、かつクルマのライフサイクル全体を通して有効でなければならない

危険に晒されているのは、消費者の安全やプライバシーばかりではない。コネクテッドカー時代においては、自動車メーカーや電気通信事業者、保険会社といったモビリティー・エコシステムの関係者も、大きな責任リスクに晒されている。攻撃者や研究者に脆弱性をつかれないようにすることは不可能である。このため自動車メーカーには、可能な限り脆弱性のない製品を作り出し、徹底的かつ継続的にテストを行い、研究者による調査結果や事実確認を真摯に受け止め、修正などの対応結果を公開するといった、誠実な企業姿勢が求められる。クルマは「走るデータセンター」へと進化を遂げつつある。こうした中でサイバー・セキュリティーやデータ・プライバシーの課題に取り組むためには、伝統的な自動車業界だけではなく他業界も巻き込んだ組織横断的なアプローチが求められる。

さらに自動車メーカーには、コネクテッドカーの安全性やセキュリティー、またプライバシーの機能強化に対する取り組みについて、透明性のある事業運営が求められる。前述のセキュリティーに関する報告書によると、消費者の 56% が将来のクルマの購入において、セキュリティーとプライバシーが重要な判断軸になるだろうと答えている。[5] 消費者は最新のテクノロジーを求める一方で、安全性、セキュリティー、データ・プライバシーの 3 要素を同時に兼ね備えた製品を期待しているのだ。

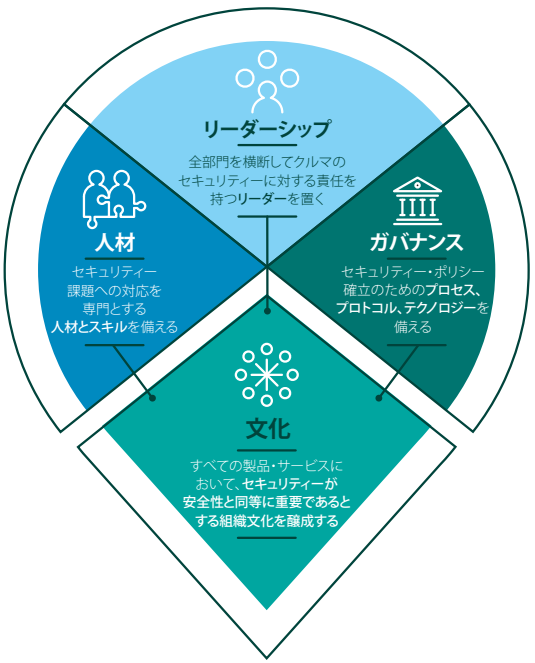
成功に向けたプラットフォームの構築

自動車メーカーは確固たる準備の基盤があって、初めて効果的なセキュリティー・ソリューションを提供できる。このプラットフォームが持つべき重要な側面が 2 つある。1 つは、組織の DNA にセキュリティーの理念がしっかり組み込まれていること。もう 1 つは、組織がデータの使用方法やプライバシー問題、所有など、あらゆる点を考慮した堅牢なデータ・モデルを保持していることだ。この 2 つの点は自動車メーカーにとって、そして何よりも消費者にとって重要である。これら 2 つの要素が備わって、ようやく自動車メーカーは「設計、製造、運用」の各フェーズのセキュリティー対策として、「不正アクセスの防御」、「不審行動の検知」、「迅速で正確な対応」に本格的に取り組むことができるのである。

セキュリティーの理念を組織の DNA に組み込む

コネクテッドカーのセキュリティー確保は、組織全体で取り組むべき課題である。さらに経営層から一般の従業員までセキュリティーに対する意識を高め、自動車メーカーの組織文化となるまで浸透させる必要がある（図 1 参照）。また、「設計、製造、運用」の各フェーズでセキュリティー対策を実現するための新たな視点が必要だ。それは従来、最重要視されてきた安全性と同じレベルにまで、セキュリティーの位置付けを高めるという視点だ。IoT の時代、ひいてはコネクテッドカーの時代においては、安全性はセキュリティーなくしてはありえない。ただセキュリティーの理念は、管理職も含めたほとんどの従業員に自然に備わっているわけではない。だからこそ、意識的にセキュリティーについて学ぶことが肝要なのである。特に自動車メーカーでは、あらゆる事業プロセスにセキュリティーの理念を体系的に組み入れる必要があり、従業員はこうした業務を反復することでセキュリティーの重要性を会得することができる。

図 1
自動車メーカーがセキュリティー対策に取り組み、組織文化として根付かせることで、初めてクルマのセキュリティーが安全性と同等に重要なものだと見なされる



業界のパートナーを取り込む

自動車業界の人材が、業界のテクノロジーと安全性モデルを熟知していることに疑念を挟む余地はない。しかしサイバー・セキュリティーを取り巻く現状や組織犯罪については、情報セキュリティーの専門家の方がより深く理解していることもまた真実である。IBM Institute for Business Value が最近発表したレポート「Automotive 2025: Industry without borders（邦訳：2025 年自動車業界の将来展望）」によると、最も消費者の心に響いたデジタル体験は、自動車メーカーではなく他業界のパートナーが設計したものだった。[6] このような結果となったのは、このデジタル体験のインターフェースが、クルマよりもはるかに身近な顧客体験をもたらす、携帯電話をはじめとしたコンシューマー・デバイスをベースとしていたためである。ここから得られる教訓は「最良のソリューションを構想するにあたっては、多彩な分野における深い専門知識を持った業界外部の人材を取り込め」ということである。

クルマの設計・製造・管理は、そのすべての行程において多数の異なる組織が関わる複雑な作業だ。そのため、1 つの組織が責任を持ってセキュリティーに関する戦略を策定・実行し、組織間の活動を統括する必要がある。このような組織のリーダーを「サイバー・セキュリティーのボス」と呼ぶことがある。この呼称は別として、この役割を担う組織には、設計・製造・販売を含む各組織と協業するための権限の付与が不可欠だ。またこの組織には「設計、製造、運用」の全フェーズを通じて、従業員一人ひとりがセキュリティーに関する理念や脅威についてのシナリオを描き、対策を講じることができるよう、組織間のスムーズなコミュニケーションを担保することが求められる。

自動車メーカーはまた、他業界からセキュリティーの専門家を採用し、様々な部署のキーとなるポジションに配置することが肝腎である。彼らは、セキュリティーの慣行に潜む不備を特定して対策を講ずるとともに、セキュリティーの理念を従業員に啓発する役割が期待される。

自動車業界は、従来の業界のテクノロジーの枠を超え、専門外の領域にまでその活動範囲を広げつつある。この状況に対応するため、自動車業界は IoT やセキュリティーの専門家と共同で業務に取り組むようになった。こうした専門家の中には、ソフトウェアやファームウェアのアナリスト、通信・ネットワークのエンジニア、クラウド・アーキテクト、モバイル・デバイス開発者、脅威分析のアナリスト、データ・サイエンティストなども含まれる。また、自動車メーカーは脅威情報（IP アドレスをキーとした脅威情報のデータベース）を共有するために、業界内の企業とも協業を進めるべきである。さらに、外国政府による諜報活動のような、業界全体に対する脅威を早期に検知するためには、業界をまたいだ連携も必要となってくる。

具体的な協業方法には、外部から招いた研究者に様々な自動車関連製品の試験を実施してもらい、自動車メーカー視点でフィードバックを受けることも含まれる。研究者のモチベーションは、その研究成果の評価だけではなく、報酬によっても上げることができる。そのため、まだ明らかとなっていない脅威と対峙する際には、社内の品質管理チームではなく、不具合発見による報奨金プログラムを活用することで、外部の研究者に効果的に働いてもらうことも有効な手段となるだろう。

最終的に自動車メーカーは、自社がコネクテッドカーのセキュリティー、ひいては安全性とプライバシーの強化に向けて積極的に対策を講じていることを消費者に知ってもらう必要がある。透明性を確保するためには、脆弱な点があればその詳細リストを公開すべきであり、またクルマのセキュリティーが最新版であることを確認できるツールを消費者に提供する必要もある。自動車メーカーが信頼を獲得し、ブランド・ロイヤルティーを育成するためには、研究者との協業や消費者との関係性構築が鍵となるだろう。

データの利用状況と所有権を把握する

セキュリティーやプライバシーの要件を評価する際には、データの利用状況と所有権を明確に把握することが肝要になる。これには実際に発生するデータ自体のみならず、データの収集、送信、保存を行う場所と方法の把握も含まれている。また、データの所有権が自動車オーナーと自動車メーカーのどちらに帰属するかを判別する必要もある。そして、この分類に基づいてデータの防御方法も検討すべきである。

実は、それぞれのデータの最終的な所有権を明確化することは容易ではない。例えば、天気や地図といった情報が自動車メーカーに帰属することは間違いない。また、消費者の電話番号や通話記録、テキスト・メッセージなどの所有権が消費者に帰属することも明らかである。では、車載センサーが収集したテレメトリー情報（遠隔計測装置で測定した様々なデータ）の所有権は一体誰が持つのだろうか。これは法律で規定されている場合を除き、データの所有権は自動車のオーナーに帰属していると見なされ、事前に消費者から同意が得られた場合にのみ、自動車メーカーによるデータの送信、保存、利用が可能であるということを認識すべきである。[7]

明らかにセンシティブな情報で、個人を特定できるデータは「デジタル・ペルソナ」のカテゴリーに分類すべきかもしれない。以下に例を挙げる。

- クルマは運転の仕方でドライバーの気分を察知し、適切に対応できる可能性がある。例えばドライバーが荒っぽい運転をした場合、クルマはドライバーの気分を落ち着かせるために、ヘビー・メタルを流すラジオ局からゆったりとしたジャズを流す局に自動で切り替える。
- クルマのハンドルに心拍数を計るモニターが搭載される可能性もある。モニターが心拍数の異常を検知した場合、クルマは自動的に自律走行モードに切り替わり、救急サービスへ連絡がいく。

クルマが取得する個人データの現状

現時点で既にクルマは様々な個人データを取得している。例えば、カーナビゲーションのシステムはクルマの位置情報を収集し、自動車メーカーのバックエンド・システムに送信している。こうした情報は、運転パターンの分析やナビゲーション・アプリへのフィードバックに利用されることもある。ただし、このようなデータは匿名化し、自動車オーナーやドライバー個人が特定できないように加工する必要がある。また、消費者がスマートフォンをクルマと接続して使用し、連絡先や通話履歴、またテキスト・メッセージなどをクルマと同期させて外部と連絡を取る場合は、データを暗号化する必要がある。そしてドライバーがクルマから降り、スマートフォンとクルマの接続が切れた時に、これらのデータはすべて削除され、次のドライバーがデータにアクセスできないようにしなければならない。

- ドライバーが事故にあった場合、もしくは緊急を要する健康状態に陥った場合に限り、クルマがドライバーの診療記録（電子カルテやお薬手帳等の情報）にアクセスし、この記録を救急隊員に通知する。

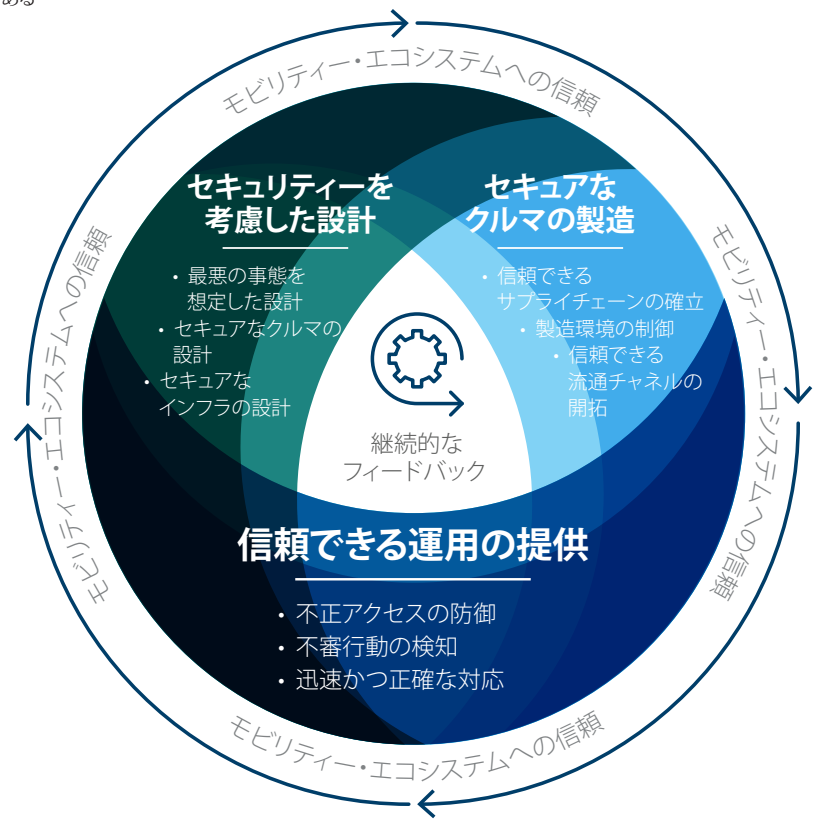
自動車メーカーが上記のような事例を実現するのは簡単なことではない。消費者が、自分のデータが本当に安全に扱われていると確信できるまでは、コネクテッドカーがもたらす本質的な恩恵を享受することはないだろう。

設計、製造、運用フェーズにおけるセキュリティー対策を実施する
本稿では「運用」フェーズに重点を置いて論ずることにしているが、他の 2 つのフェーズについても簡潔に論じたい。なぜなら、信頼のおけるモビリティー・エコシステムを構築するためには、この 3 つのフェーズそれぞれが重要な構成要素となっているからである（図 2 参照）。

セキュリティーの設計をする際には、クルマそのものへの攻撃だけでなく、クルマとインフラ間のコネクテッド（連結）部分への攻撃にも備えなければならない。セキュリティー対策を万全のものとするためには、設計段階から最悪の事態を想定し、障害の発生まで十分に考慮しておく必要がある。例えば、不正アクセスによりバスの運行システムのすべての連結部分が機能しなくなった場合でも、闇雲に ECU（電子制御装置）にすべての制御を委ねることは控えなければならない。

セキュアなクルマを設計するうえでは、まず設計プロセスの初期段階からセキュリティー重視の思考を持つことが肝腎だ。これにはクルマの使用中に発生し得るあらゆる脅威に対する評価指標を定義しておくことも含まれる。なお、ここで想定した脅威のモデルは、設計チーム全員で共有できるようにする。次に必要となるのが、安全なインフラの設計である。この工程においては、クルマだけでなく、信号機や高速道路の料金ゲート、他の車両といったクルマと情報をやり取りするすべての構成要素を考慮しなければならない。ここで構成要素間における整合性を確実に担保できるか否かが、その後のインフラ構築の命運を左右する。

図 2
コネクテッドカーがもたらす本質的な恩恵を享受するためには、セキュリティーへの包括的なアプローチが不可欠である



セキュアなクルマを製造するためには、サプライチェーンや製造現場だけでなく、消費者と直接やり取りをする流通チャネルへの配慮も必要だ。また、信頼できるサプライチェーンを確立するには、不正対策が不可欠だ。つまり、自動車部品のサプライチェーンに偽造品や欠陥品が入り込まないよう、部品が工場から出荷されクルマの中に組み込まれるその時点まで、一貫して不正が行われないようにしなければならない。

製造環境のコントロールに関しては、IT システムと製造システムを統制的に捉える視点が必要だ。それぞれのシステムの機能、アプリケーション、インターフェース、プロトコルを把握し、アクセス権を考慮したセキュリティー・ポリシーや適切なセキュリティー・コントロールを確立することで、製造環境の安全性を担保できる。また、流通チャネルの信頼性を高めるには、供給側のプロセスと類似する点もあるが、最も注視すべきは、クルマが工場からディーラーを経由して最終的に消費者へ運ばれるその過程だ。物流会社などの第三者を経由してクルマが輸送される場合、その過程で不正な行為が行われないような安全管理体制の構築が求められる。

ここで確認しておきたいことは、セキュリティーの対象となるのがクルマや自動車メーカーだけではないということだ。例えば、ディーラーやサービス・センター、外部の部品提供者なども当然その対象に含めなければならない。自動車業界が**信頼できるモビリティー・エコシステム**を構築するには、利害関係者全員を監視、監督する必要がある。つまり、徹底したセキュリティー施策とは、今日のニーズを満たすだけでなく、将来起こりうる事態に対しても柔軟に対応できるものでなければならない。それ故に、堅牢な認証機能によるセキュリティー管理やアクセス権限に関する規則、システム管理機能の強化、アクセス・キーの管理などによってモビリティー・エコシステム上のどの領域においてもセキュアで信頼に足る環境を作り上げる必要がある。

クルマをコントロールしているのは自動車メーカーであるが、そのクルマに接続してサービスを提供したいと考える関係者は少なくない。自動車メーカーはクルマの価値を高めるために、その関係者を取り込むべくオープン・プラットフォームを接続ポイントとして用意する。ただ、このプラットフォームがセキュリティーの専門家が呼ぶところの「広範囲な攻撃対象領域」となる危険性がある。そのため自動車メーカーは、オープン・テクノロジーを熟知したパートナーが提供するセキュリティー・ソリューションと互換性のあるプラットフォームを選択しなければならない。

信頼できる運用を提供する

これまで論じてきた基本的な項目が達成できれば、自動車メーカーは「設計、製造、運用」フェーズのうち、「運用」におけるセキュリティーの強化が可能になるだろう。クルマが道路を走る「運用」のフェーズにおいて、ドライバーが求めるものは、不正アクセスを防ぎ、不審な行動を検知し、迅速かつ正確な対応を可能にするテクノロジーやサービスだ（図 3）。自動車メーカーやクルマの製造販売に関わる関係者は、クルマのオーナーから特段要求がない限りは、オーナーの負担にならない範囲でこれらの実現に取り組まなければならない。ドライバーが安全性、セキュリティー、プライバシーに関する判断を求められるのは、緊急事態に直面した時に限定されるべきである。

不正なアクセスを防御する

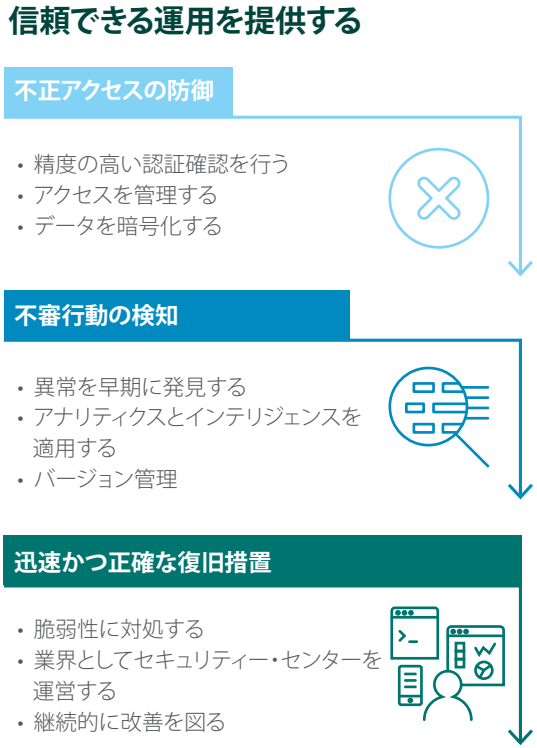
精度の高い認証確認を行う

認証とは本人であることを検証するプロセスだ。認証にはクルマに対するものと、Web ポータルやモバイル・アプリケーションといったインターフェースに対するものがある。クルマを構成するコンポーネントもまた、コンポーネント同士やクルマのインフラとの間で認証確認をする。これらの作業は、ドライバー、アプリケーション、コンポーネントから送られたコマンド（指示）が、正規のものであることを確認するために行われる。ここで確認できるのは、コマンドの送信者が誰であるのか、あるいはコマンドを送ったコンポーネントはどれなのかということであり、何を実行できるかについては認証の際に規定するものではない。

精度の高い認証確認を行うには、ユーザー名とパスワードだけでは不十分である。コネクテッドカーの活用においては、信頼できるセキュリティー・モジュールが不可欠になる。具体的には以下のようなものだ。

- 認証機能として、ログイン時に双方向で確認できる機能を備える。ECU のようにインタラクティブでないコンポーネントには、より強固な認証機能を実装する
- データベース検索（クエリー）の時点で ID が実在するか照合する
- 認証情報や暗号キーの保管、署名、管理は固有の方法で行う。さらに 2 要素認証やアウトオブバンド認証（ワンタイム・パスコードのようにアクセスされているチャネルとは別のチャネルを介した第二の認証要素）の技術を利用して認証の安全性を担保する

図 3
「信頼できる運用」フェーズの構成要素



コネクテッドカーにおける信頼性の高い認証機能の実例

以下は、コネクテッドカーを取り巻くモビリティー・エコシステムにおける、信頼性の高い認証機能とその利用法の実例である。

- ユーザーはモバイル・アプリケーションや Web ブラウザーで本人確認をする。するとアプリケーションやブラウザーはバックエンド・システムと通信し、ユーザーがクルマの所有者であることを確認する。確認が取れたことでユーザーは、所有するクルマをモニターし、管理することが可能になる。
- スマート信号機や沿道に設置されたスマート・インフラが、急なカーブでの減速といった特定のアクションをクルマに指示することも可能になるだろう。第三者によるこの仕組みの悪用を防ぐため、インフラのコンポーネントには、信頼性の高い認証技術を用いたデータ通信が求められる。
- ECU や制御コンポーネントは、信頼できる認証機能を持ち、当局からのメッセージが受信できる必要がある。これにより、不正なデバイスから送られてくる悪意のあるコマンドの受信を未然に防ぐことができる。
- 更新プログラムを実行する際には、ローカルでインストールする場合でも、OTA（Over-the-air）を経由する場合でも、マルウェアのインストールを防ぐため信頼性の高い認証確認を行う必要がある。
- サービス・センター、修理センター、コンテンツ・プロバイダーなどのサード・パーティーにも、信頼できる認証機能を備えることが求められる。
- アプリは認証された信頼のおけるものを 使用する。

- 柔軟さと拡張性を常に考慮する。OAuth や SAML などのオープン・スタンダード技術の採用も検討する [8]
- 暗号化プロセッサーを搭載する
- 不正改変の防止策を講じる

また、認証機能はそれぞれのクルマごとに固有なものである必要がある。例えば、ドライバーの運転パターン分析や体重の自動測定による本人確認には、エントリー・キーや携帯電話の署名機能の活用が必須となる。

アクセスを管理する

アクセスの管理とは、車内およびクルマと外部のコンポーネント間のアクティビティーを制御することだ。これらのアクティビティーには、要求者の認証確認結果やその要求のタイプ（メッセージの制御、読み取り要求、書き込み要求など）、あるいは要求者の置かれた状況（クルマの走行速度や位置情報など）に基づき、その実行を許可する仕組みが求められる。

車内においては、ECU が悪意のあるアクティビティーの標的になる可能性がある。そのため ECU には、アクセス・ルールを補完する機能が必要となる。ただ、ECU の処理能力には限界があるため、多数のエンド・ポイントでこのアクセス・ルールを管理することは煩雑な作業になりかねない。しかし、数は少ないがアクセス・ルールを強化するための戦略がいくつか考えられる。例えば、サブシステム機能が管理するコンポーネントごとにグループ化する方法だ（例：ブレーキとハンドルの組み合わせ）。

データを暗号化する

暗号化による保護の対象としては、電子メールやテキスト・メッセージ、連絡先といった消費者の個人情報に加えて、設定情報やテレメトリー情報も含まれる。データは車内のみならず、クラウド上にある自動車メーカーのサービス・ネットワークや外部パートナーのシステム上など、その保管場所は多岐にわたる。また、クルマのオペレーション・ネットワークやモバイル・ネットワーク、あるいは Wi-Fi や Bluetooth、狭域通信（DSRC）など、多種多様なネットワークを経由してやり取りされる。

コントローラー・エリア・ネットワーク（CAN）バス全体に暗号化を適用した場合、プロセッサーに負荷が集中し、遅延が発生する可能性がある。このため、現時点では実現性の高い選択肢とはいえない。自動車メーカーが暗号化の仕組みを車両システムの設計に組み込む際、リスクを評価する必要はあるが、すべてのコンポーネントに対して絶対的なセキュリティー対策を講じることは難しい。

前述のとおり、暗号化はセキュリティー・モジュールに依存する。顧客データにさらに 1 つ要件を加えるならば、暗号化にゼロ知識技術を活用することだ。ゼロ知識モデルでは、自動車メーカーや関係するサード・パーティーはデータの暗号を解読しない。データはエンド・ツー・エンドで保護され、消費者だけが暗号を解読できる仕組みになっている。多くのクラウド・プロバイダーは、ゼロ知識モデルへの移行を進めている。

昨今、自動車メーカーは攻撃を防ぐ手段として、侵入検知防御システム（IDPS）のクルマへの実装を非常に重視するようになった。これは、各社が従来のメカニカルな課題への対応と同じアプローチを取ることで、単一のコンポーネントや機能の追加、改変によってセキュリティー上の各課題を解決しようとする試みだ。

しかし、このアプローチには 2 つの欠点がある。1 つ目は、IDPS による保護の仕組みは事前に設定したルールに基づいて実行されるため“予測可能”なタイプの攻撃にしか対処できない点だ。もし攻撃者がコードに書かれていない新しい侵入経路を見つけた場合、対処は不可能である。2 つ目は、攻撃者が車載コンポーネントへの不正アクセスによりクルマの制御を奪うだけではなく、将来的に IoT 化されたクルマのネットワーク環境から、ランサムウェアを使った金銭の要求やクレジットカード情報といった個人データの悪用に攻撃の軸足を移す可能性があるという点だ。これに IDPS は対応できない。

効果的な防御策を講ずるためには、まず包括的な視点に立ちエンド・ツー・エンドのセキュリティーを設計する必要がある。戦略としては、当事者同士が意見を交わし合い、互いに補完し合えるような階層型のアプローチを取るべきである。

アクセス管理の実例

以下は、コネクテッドカーを取り巻くモビリティー・エコシステムで実現されている、アクセス管理の事例である。

- ブレーキの ECU へ制御メッセージの送信が許可されているのは ABS（アンチロック・ブレーキ・システム）だけである。これ以外のシステムが制御メッセージを送信するには、ABS からのリクエストが必要だ。この場合、ABS はアクセス管理の制御規則に基づいて作動する。また、ブレーキの ECU 自体の作動も制御規則に準ずる必要がある。例えば、ABS 以外の機関から制御メッセージが送られてきた場合や認証確認が確実に行われなかった場合は、メッセージを無視するといった規則だ。
- クルマがバレー・モード（ホテルやレストランのスタッフによる代理駐車サービス利用時のモード）に設定された場合、ストレージ・コンパートメントをロック状態とし、クルマの移動範囲は半径 0.5 マイルまで、運行速度は時速 25 マイルまでに制御できるようにする。
- メールやテキスト・メッセージ、電話による所定の手続きを踏んだドライバーやコンポーネントだけが、データにアクセスできるようにする。自動車メーカーが管理するクラウド・サービスは、クルマのテレメトリー情報（位置情報、速度、走行距離など遠隔計測装置で測定したデータ）にはアクセスできるが、ドライバーのモバイル端末のデータにはアクセスできない。ただし、クルマの所有者は、自動車メーカーや保守サービス会社などとの日程調整のために、彼らに自身のカレンダーへのアクセスを許可することも可能である。

不審な行動を検知する

異常を早期に発見する

検知機能によって早期警告が可能となる。早期警告に従い、システムが自動で適切な対応を取る、もしくは手動で対応することで、安全性やセキュリティー、プライバシーが侵害される前に、不正なアクセスを防御することができる。

外部からの侵入を検知するうえで重要なのは、検知機器をクルマのどの部分に設置するかを戦略的に決めることだ。検知機器としては、車載インフォテイメント（IVI）、バス・システム、セントラル・ゲートウェイ、次世代の車両アーキテクチャーに搭載されるドメイン・コントローラーなどが考えられるが、ECU 自体の場合もある。これらのコンポーネントが生成したイベント（IVI からの活動ログやコントロール・バスでモニターされた通信など）からも不正検知のためのデータは収集される。

前述のとおり、クルマの IDPS 実装にはメリットがあるが、検知フェーズにおいては限界もある。IDPS は事前に設定したルールに基づくシステムであり、主に CAN（コントローラー・エリア・ネットワーク）内に点在する ECU 間のコミュニケーションから検知、推測する。ここで得られる情報は重要ではあるが、特に IDPS が活用する分析手法が複雑である場合、車内のセキュリティーに関するイベントについては比較的限定された範囲でしか示唆を提示できないだろう。CAN バス上の機能は主に安全性に焦点を当てている。人の命を守るという点においては非常に重要な機能だが、外部のネットワークや OS データ上の疑わしい点や不審な行動を全体像から俯瞰して検知することはできない。単純な攻撃であれば検知できることもあるが、巧妙な場合はほとんど検知できないだろう。

アナリティクスとインテリジェンスをセキュリティーに適用する

セキュリティーに関する分析は、個々のクルマへの攻撃だけでなく、モビリティー・ネットワークの信頼性に対する攻撃もカバーする必要がある。過去に収集した認証データを活用することで犯罪科学分析が可能となり、攻撃者の侵入経路を突き止めることができる。

自動車メーカーは、車両故障の予測・分析サービスなどのアナリティクス技術の活用において長足の進歩を遂げつつある。この技術により、機械部品の故障はその時期も含めて予測できるようになった。同様の予測能力が、今セキュリティーの分野でも期待されている。個々のクルマの使用状況や過去のセキュリティー問題のケースを参考に予測するのだ。

コンテクストに基づき、不審な行為を検知する包括的なソリューションを活用して、データの収集と処理はクルマ側で実施する。また、それとほぼ同時に一連のイベント・データを分析プラットフォームに送信する。このプロセスは、クルマの計算能力と各車両のデータ・ポイントとバックエンド・システムとのデータ送受信容量のバランスを見ながら実施される。

バージョン管理

バージョンの更新は安全面において欠かせない。これは、クルマに装備されているセキュリティー・モジュールの諸要素と検知機能がともに最新バージョンであり、かつ最新のセキュリティー・パッチが適用されたコンポーネントを搭載しているという証である。また、車載コンポーネントに改ざんや不正改良が行われていないことを保証するものでもある。

バージョン保証システムは、まずシステム自体の信頼性が不可欠だ。次に、すべてのコンポーネントが信頼できるものであることが保証されなければならない。さらにすべてのコンポーネントのデジタル署名を自動車メーカーから提供されるマスター・データと照らし合わせ、有効なものであることを確認する必要もある。車載インフォテイメント（IVI）は、それ自体複雑なものであり、多くのオープン・ソース・ライブラリーのソフトウェアから構成されている。これらのライブラリーのバージョン情報と署名は、定期的に保守・点検されたものでなければならない。自動車メーカーは、消費者に対しての透明性を確保するために、定期的に情報をダッシュボードや IVI への掲示で提供する必要がある。単純ではあるが、「このクルマに搭載されたモジュールはすべて有効で最新の状態です」といったメッセージを定期的に提供することで、顧客から信頼を獲得し続けることができるだろう。

脆弱性を分類する

脆弱性は多様な形態で発生する。そのため、自動車メーカーと当局は連携してその深刻度に応じて、クルマに関する脆弱性を分類するシステムを確立すべきだ。例えば、人への危害はデータの損失よりも優先度が高い、など。脆弱性の分類によって対応の優先順位が異なってくる。

安全性の復旧措置は迅速かつ正確に行う

脆弱性に対処する

機能面のアップデートは、顧客の利便性に関わる問題だ。一方でセキュリティーのアップデートは、安全性、セキュリティー、プライバシーの面で、顧客にとって極めて重要な問題である。クルマや関連するインフラに脆弱性が発見された場合、攻撃者が脆弱な部分を攻撃する前に、自動車メーカーはパッチを開発し、対象となるすべてのクルマに漏れなく適応させなければならない。

アップデート版は OTA（Over-the-air: ECU などのソフトウェアを無線通信で更新する機能）で提供するとともに、顧客が好きな時にディーラーなどのサービス・センターで入手できるようにしておくべきだ。自動車メーカーは、OTA でアップデートを実行する場合やクルマの運転に関するデータを収集する場合には、所有者から事前に同意を得なければならない。また、クルマが譲渡されて所有権が移行した場合にも、新たな所有者から同意を得る必要がある。この際、IVI や Web ポータル上の同意ボタンをクリックするだけの簡単な方法で同意を得ることもできる。

OTA によるアップデートの仕組みは複雑だ。自動車メーカーから各クルマへアップデート情報を送信する時には、データの損壊を防ぐために、信頼できる通信方法が確保されていることが前提となる。そして、アップデート後は信頼できるモジュールを使った署名の検証が必要になる。また、アップデート・プログラムがインストールされた後には、最終的なテストも必要になってくる。

OTA によるアップデートを開始する際には、事前にクルマが適切な状態にあることを確認する必要がある。例えば、クルマが動いている最中に、パワートレインのコンポーネントをアップデートすることは賢明とはいえない。もしアップデート期限までに適切な状態を確保できない場合は、所有者はクルマをセーフ・モードに切り替えるか、またはサービス・センターに持ち込むかのいずれかの方法でアップデートを完了させる必要がある。

VSOC（自動車セキュリティー・オペレーション・センター）を設置する
自動車メーカーは、クルマの運転に関するあらゆる情報を収集、分析、評価し、対応する必要がある。これらのタスクを実行するために、専用の機関である VSOC（自動車セキュリティー・オペレーション・センター）を開設すべきだ。VSOC の主な任務は、コネクテッドカーの安全性やセキュリティー、プライバシーに関する課題を取りまとめて、管理・運営することである。VSOC はクルマの最前線に立って、セキュリティーに関するオペレーション全般を行う。地域、メーカー、クルマのモデルなどにより、事前に定められた対象車両群に対し、サイバー脅威をモニタリングする。さらにセキュリティー・インシデントに対処するため、モニタリングした脅威を分析し、情報を整理したうえで共有する。このように VSOC では適切な人材を抱え、プロセスを管理し、最新のテクノロジーを把握することで、サイバー脅威をモニタリングし、犯罪科学調査を行い、インシデント管理やセキュリティー報告を実施する。

VSOC のミッションは以下のとおりである。

- サイバー脅威のモニタリングや全体像の把握
- サイバー・インシデントへの備えと適切な対処の実施
- サイバー攻撃を遡っての調査
- セキュリティー・インシデントの兆候の検知
- 事業の安定的な継続と問題が生じた場合の迅速な復旧
- 業界インフラのサイバー攻撃からの防御
- サイバー・リスクやコンプライアンスに関する報告書の作成

VSOC は、既存の組織でいえば IT SOC（IT Security Operations Center）に相当する存在だ。VSOC のセキュリティー・アナリストは、自動車業界に対する技術的な深い知識を有し、攻撃の対象となり得る車両のメーカーやモデル、バージョンにも精通している必要がある。そして当然のことながらアナリストには、広範なサイバー・セキュリティー分野における専門知識も求められる。

継続的に改善を図る

すべてのプロセスに通じることだが、経験は教訓として次に生かされなければならない。例えば、自動車メーカーは前述の犯罪科学手法を社内で行うセキュリティーの検証試験と組み合わせて、研究開発（R&D）に反映させていくべきだ。このサイクルを循環的に実行することで、継続的な改善が可能となる。設計の初期段階からこの循環サイクルを回すことで、設計上の欠陥も早期に発見し、解決することができるだろう。

この循環サイクルは、攻撃者の動機や戦略を理解するうえで役に立つ。またこの知見により、脅威への対抗措置は強化され、加えてセキュリティー面における「設計」と「製造」の品質も高められるだろう。ここで得た教訓は、自社のコネクテッドカーを取り巻くモビリティー・エコシステムの利害関係者のみならず、Auto ISAC（Automotive Information Sharing and Analysis Center）のように業界全体が連携して運営する組織とも共有すべきである。この他にも同様に、業界標準やベスト・プラクティスを追求するため、自動車業界が主導して進める取り組みがいくつかある。AUTOSAR（AUTomotive Open System ARchitecture）、EVITA（E-safety vehicle intrusion protected applications）、クルマのサイバー・セキュリティーに関するガイダンスを提供する SAE International の standard J3061 などがその例だ。今後、我々が自律走行を実用化する過程の中で、コネクテッドカーの IT セキュリティーやプライバシーに関する更なる詳細な法律や規則が増えていくことが望まれる。

究極的には、自動車メーカーには安全性の担保と並行して、より高い基準を満たしたセキュリティーとプライバシーの提供が求められる。コネクテッドカーの時代を迎え、顧客が望む安全性と機能性だけでなく、セキュリティーをも確実に提供できる自動車メーカーが最良のポジションを獲得することになるだろう。

コネクテッドカー時代の競争に勝ち抜くための 5 つの問い

- 社内およびパートナー企業がセキュリティーの基準を安全性の基準と同等のレベルにまで引き上げるために取っている戦略やアプローチはどのようなものか。
- 攻撃の対象や攻撃者の侵入経路、不正アクセス用のプログラムを理解するために、コネクテッドカーに関する過去および現在のセキュリティー情報をどのように活用しているか。
- クルマをより安全な乗り物にするための継続的なフィードバックをどのように実施しているか。
- サード・パーティーやパートナー企業とのコネクテッドカーに関するセキュアなデータの共有はどのように行っているか。
- セキュリティーに関する専門知識を習得し、これをモビリティー・エコシステムと共有するためにどのような仕組みを構築しているか。

協力者
Arndt Kohler, Associate Partner, IBM Security Europe

Dr. Yaron Wolfsthal, Associate Director, Cyber Security Center of Excellence, Israel

Dr. Yair Allouche, CTO Connected Vehicle Security, Cyber Security Center of Excellence, Israel

Rob Carson, Content Strategist/Writer, IBM Institute for Business Value, IBM Digital Services Group

April Harris, Visual Designer, IBM Institute for Business Value, IBM Digital Services Group

日本語翻訳監修者
鈴木のり子
日本アイ・ビー・エム株式会社
グローバル・ビジネス・サービス事業
オートモーティブ・サービス事業部
シニア・マネージング・コンサルタント

著者について

Christopher Poulin は、IBM X-Force security research グループの元 Research Strategist である。コネクテッドカーをはじめとするIoTの脅威情報やセキュリティーに関する造詣が深い。情報セキュリティー分野における業務経験は 25 年を超える。米国防総省を担当したほか、ソフトウェア開発から小規模専門セキュリティー・コンサルタント会社の設立まで幅広い分野で活躍した。

Giuseppe Serio は、自動車産業界および航空宇宙・防衛業界にて、サイバー・セキュリティーに対する IBM Global Solution Leader を務める。彼は 20 年以上にわたり、世界各国のクライアントとセキュリティー課題の解決に向けた取り組みを行う。コネクテッドカーのセキュリティー課題に対峙した経験もある。IBM 社内の研究部門やセキュリティー部門、さらには IoT 事業部門などと連携を取り、業界特有のニーズに応えるセキュリティー・ソリューションの開発・実用化に取り組んでいる。
IBM に入社する以前は、PwC コンサルティングでシニア・コンサルタントを務め、多くの国際的な事業変革プロジェクトを手掛けてきた。
連絡先：giuseppe.serio@de.ibm.com

Ben Stanley は、IBM Institute for Business Value に所属し、Global Automotive のリーダーを務める。自動車業界におけるソート・リーダーシップのコンテンツ策定と戦略的なビジネス・インサイトの提言に関する責任を担う。世界の自動車業界大手企業と 39 年以上にわたり、事業戦略やビジネスモデル・イノベーションの分野で協業してきた。中国の上海で 5 年間、IBM Automotive Center of Excellence の責任者を務めた経歴も持つ。
連絡先：ben.stanley@us.ibm.com　Twitter：@BenTStanley

詳細について
IBM Institute for Business Value の調査結果の詳細については iibv@us.ibm.com までご連絡ください。IBM の Twitter は @IBMIBV からフォローいただけます。発行レポートの一覧または月刊ニュースレットの購読をご希望の場合は、**ibm.com**/iibv よりお申し込みください。

iPad またはアンドロイド向け無料アプリ「IBM IBV」をダウンロードすることにより、IBM Institute for Business Value のレポートをタブレットでもご覧いただけます。

変化する世界に対応するためのパートナー
IBM はお客様と協力して、業界知識と洞察力、高度な研究成果とテクノロジーの専門知識を組み合わせることにより、急速な変化を遂げる今日の環境における卓越した優位性の確立を可能にします。

IBM Institute for Business Value
IBM グローバル・ビジネス・サービスの IBM Institute for Business Value は企業経営者の方々に、各業界の重要課題および業界を超えた課題に関して、事実に基づく戦略的な洞察をご提供しています。

注釈および出典

1 Poulin, Christopher. “Driving security: Cyber assurance for next-generation vehicles.” IBM Institute for Business Value. 2014. http://www-935.ibm.com/services/us/gbs/thoughtleadership/automotivesecurity/

2 Stanley, Ben and Kal Gyimesi. “A new relationship – people and cars: How consumers around the world want cars to fit into their lives.” IBM Institute for Business Value. 2016.
http://www-935.ibm.com/services/us/gbs/thoughtleadership/autoconsumer/
邦訳「人とクルマの新たな関わり - 消費者の生活におけるパートナーへと変化するクルマ - 」
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&htmlfid=GBE03718JPJA&attachment=GBE03718JPJA.PDF

3 Greenberg, Andy. “Hackers remotely kill a Jeep on the highway – with me in it.” Wired. July 21, 2015.
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

4 既に我々は IoT をターゲットとしたマルウェアを確認している。例えば、Mirai というマルウェアは、1 億台を超えるコネクテッド監視カメラとデジタル・ビデオ・レコーダーで感染が確認されており、その他ホーム・ルーターからベビー・モニターまで、あらゆるものを標的とする。現在、路上を走行する自動車の数は 10 億台を超える。このわずか 1% でもボットネットに取り込まれ、大規模な分散型サービス拒否（DDoS）攻撃に利用されたとしたらどうなるだろうか。

5 Stanley, Ben and Kal Gyimesi. “A new relationship – people and cars: How consumers around the world want cars to fit into their lives.” IBM Institute for Business Value. 2016.
http://www-935.ibm.com/services/us/gbs/thoughtleadership/autoconsumer/
邦訳「人とクルマの新たな関わり - 消費者の生活におけるパートナーへと変化するクルマ - 」
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&htmlfid=GBE03718JPJA&attachment=GBE03718JPJA.PDF

6 Stanley, Ben and Kal Gyimesi. “Automotive 2025: Industry without borders.” IBM Institute for Business Value. 2015. http://www-935.ibm.com/services/us/gbs/thoughtleadership/auto2025/
邦訳「2025 年自動車業界の将来展望 - 境界線のない業界 - 」
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&htmlfid=GBE03640JPJA&attachment=GBE03640JPJA.PDF

7 データの所有権は、その帰属が常に明らかなわけではない。例えば、店舗の付近を走行するクルマの交通量、車名やモデル（消費者の潜在的な購買能力を判断する）、さらには上顧客を追跡するための VIN（車両識別番号）などの情報を知りたい、と考える小売事業者もいるだろう。しかしクルマに関する情報には、交通量のように一般公開されているものもある一方で、車名やモデルなどのようにメーカー固有の情報もある。また VIN のように、直接的には個人の特定につながらないが、依然として機微情報と見なされるデータもある。

8 OAuth（Open Authorization）は、Web、モバイル、デスクトップの各アプリケーションへのセキュアな権限の認可をサポートするオープン・プロトコルだ。SAML（Security Assertion Markup Language）は、サービス・プロバイダーと ID プロバイダー間における、認証情報や認可情報の交換をサポートするオープン・データ形式である。

IBM Global Business Services, Route 100, Somers, NY 10589

Produced in the United States of America, January 2017

本書は英語版「Accelerating security - Winning the race to vehicle integrity and data privacy -」の日本語訳として提供されるものです。