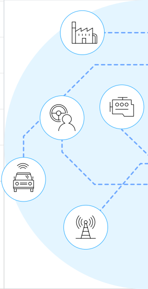
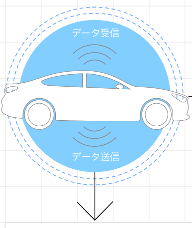
データ・ストーリー



コネクテッド・カー・セキュリティー

モビリティーの未来を支える

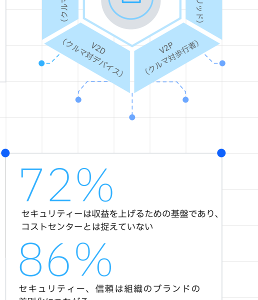


SDV（Software Defined Vehicle）の時代が来ます。コネクテッド・カーの普及台数は2027年までに3億6,700万台に達し、エンドポイント* 数は大幅に増えると見込まれています。インカー（車両内）とアウトカー（車両外）の両方で、サイバー脅威にさらされる領域が新たに何億も生まれることになります。さらに、生成AIの利用が広がることで、サイバー脅威の状況はより複雑になると考えられます。

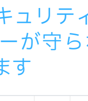
* エンドポイントとは、通信ネットワークに接続して情報を交換する端末や機器のこと

自動運転車やドローン、空飛ぶ車（eVTOL：電動垂直離着陸機）* といった高度なモビリティー技術は、今後コネクティビティーをより複雑なものに変えていくでしょう。一方、コネクテッド・カーのセキュリティーやプライバシーへの取り組みに関して、多くのメーカーや自動車サプライヤーは、現行の基準や規制対応に追われ、将来予想されるサイバー攻撃への計画まで十分に検討できていないのが現状です。

* 電動垂直離着陸機（eVTOL）とは、ヘリコプターのように垂直に離着陸する空のモビリティーのことで、滑走路などの大がかりな設備を必要としない



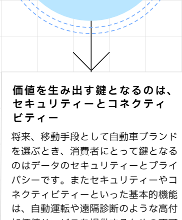
自動車業界の経営層も、コネクテッド・カーのセキュリティーの強化が、製品価値やブランド力を高めると考えています。[1]



72%
セキュリティーは収益を上げるための基盤であり、コストセンターとは捉えていない

86%
セキュリティー、信頼は組織のブランドの差別化につながる

消費者はセキュリティーがしっかりしていて、プライバシーが守られているブランドを選ぶ傾向にあります

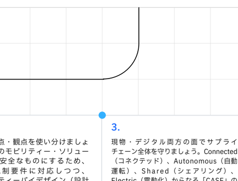


自動車業界は、ドライバー、同乗者、歩行者などの安全を確保し、プライバシーを守るため、サイバーセキュリティーの強化に力を注いでいます。一方、消費者も特定のブランドを選ぶ要因として、サイバーセキュリティーに注目しています。シェアカーや自動運転車を利用するときに、セキュリティーとプライバシーが優れたブランドを選ぶと答えた消費者は53%もいました。[2]

価値を生み出す鍵となるのは、セキュリティーとコネクティビティー

将来、移動手段として自動車ブランドを選ぶとき、消費者にとって鍵となるのはデータのセキュリティーとプライバシーです。またセキュリティーやコネクティビティーといった基本的機能は、自動運転や遠隔診断のような高付加価値サービスを提供するための不可欠な要素です。

EVの各機能のために、消費者が支払ってもよいと考えている平均額[3]



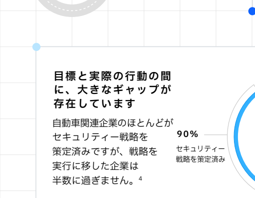
実行に向けてのヒント

1. プロダクト・ライフサイクル全体にセキュリティーとプライバシーを組み込みましょう。セキュリティーに対しては、サプライヤーや顧客を含めたすべての関係者が責任を持つことで、セキュリティーを強化します。

2. 複数の視点・観点を使い分けましょう。将来のモビリティー・ソリューションを安全なものにするため、現行の規制要件に対応しつつ、セキュリティーバイデザイン（設計段階からセキュリティーを意識すること）のコンセプトで戦略を練ります。

3. 現物・デジタル両方の面でサプライチェーン全体を守りましょう。Connected（コネクテッド）、Autonomous（自動運転）、Shared（シェアリング）、Electric（電動化）からなる「CASE」のエコシステムを守る計画を立案します。共通の標準やツール、外部の専門技術を活用して、効率性を上げられます。

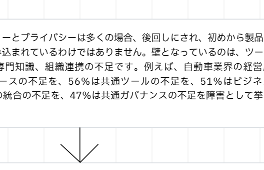
自動車業界のCEOはセキュリティーとプライバシーを重要課題と考えている



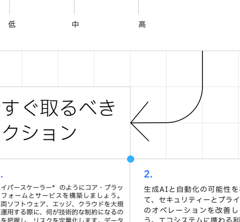
セキュリティーとプライバシーは、自動車業界のCEOにとって、サステナビリティーに次ぐ重要な課題です。データ漏洩など、自動車のサイバーセキュリティーとプライバシーが、収益とブランド評価に影響を与えます。エッジ接続、OTA（無線経由の）ソフトウェア・アップデート、通信事業者との連携、といった複雑な問題に取り組むためには、リーダーのコミットメントとチームワークが求められます。

目標と実際の行動の間に、大きなギャップが存在しています

自動車関連企業のほとんどがセキュリティー戦略を策定済みですが、戦略を実行に移した企業は半数に過ぎません。[4]



セキュリティーとプライバシーは多くの場合、後回しにされ、初めから製品開発と生産に組み込まれているわけではありません。壁となっているのは、ツール、リソース、専門知識、組織連携の不足です。例えば、自動車業界の経営層の63%はリソースの不足を、56%は共通ツールの不足を、51%はビジネス・ユニット間の統合の不足を、47%は共通ガバナンスの不足を障害として挙げています。[5]



前途は多難か？

コネクテッド・カーが多くのコネクティビティー機能を搭載すればするほど、クルマへの攻撃領域は急速に拡大していきます。サイバーセキュリティー・リスクについて考えるとき、自動車業界の経営層はブランド・イメージへの評判は気にしているものの、現実の脅威については過小評価しているようです。リスクを軽減するためには、コネクテッド・カーを設計する段階からセキュリティー機能をデフォルトで組み込むべきです。[6]

今すぐ取るべきアクション

1. ハイパースケーラー* のようにコア・プラットフォームとサービスを構築しましょう。車両ソフトウェア、エッジ、クラウドを大規模運用する際に、何が技術的な制約になるのかを把握し、リスクを定量化します。データ分析から得られるインサイト（洞察）を利用して、セキュリティー、パフォーマンス、信頼性を損なうことなくデータ、ネットワーク、エンド・ユーザーを融合する堅牢なインフラストラクチャーを設計しましょう。

   * ハイパースケーラーとは、拡張可能なクラウド・アーキテクチャーを有する大規模なクラウド・サービス・プロバイダーのこと

2. 生成AIと自動化の可能性を検討して、セキュリティーとプライバシーのオペレーションを改善しましょう。エコシステムに携わる利害関係者全体からの知見を活用し、エコシステム全体の回復力を高めます。すべての関係者が十分な投資をしている必要があるでしょう。

3. 事業計画を作成する際には、将来を見据えましょう。ソフトウェアを主体としたコネクテッド・カーが持つ脆弱性を考慮しましょう。セキュリティーとプライバシーのブランド価値、収益機会を基本計画に組み込みましょう。

このトピックについてのインサイトや解説をさらにご覧になりたい方へ

関連情報：

- Helping to secure privacy for data generated by connected cars
- Accelerating security（邦訳：クルマのセキュリティー対策を加速せよ）

こちらのページから今すぐ登録が可能です。リサーチに基づくインサイトを得て、ビジネス上の意思決定にお役立てください。

サイバーセキュリティーのためのAIと自動化について、より詳しく知りたい方は以下をご覧ください。

- AI and automation for cybersecurity（邦訳：サイバーセキュリティーを支えるAIと自動化）
- The CEO's guide to generative AI: Cybersecurity（邦訳：「生成AIを以って生成AIを制す」― 新たな局面を迎えるサイバーセキュリティー対策とは）
- The power of AI: Security

IBM

IBM Institute for Business Value

出典：1: IBM IBV The new era of cloud security. 2: IBM IBV Automotive 2030: Racing to a digital future. 邦訳「2030年自動車業界の将来展望 - デジタルの未来へ突き進め -」 3: IBM IBV Electric vehicles: An on-ramp to sustainable mobility. 邦訳「持続可能なモビリティー社会の実現を目指して - EVシフトが加速する -」 4および5: IBM IBV Prosper in cyber economy, 2022. 6: IBM IBV open standards benchmarking, IT and OT risk, security, and resilience 2020, unpublished.

DRQO0E0Z-JPJA-00