自動車サイバーセキュリティ：
コネクテッドカーへの
セキュリティ対策は万全か？

pwc

www.pwc.com/automotive

はじめに

本レポートは、2018年5月にPwC米国法人で発刊された『Cyber readiness: are auto companies prepared to counter the risk of an attack?』の日本語訳版です。

今日、自動車はインターネットや周辺環境とより密に接続されつつあり、単なる移動手段を超えた付加価値の高いサービスへ変貌を遂げようとしています。

カーシェアリングサービスは既に広く認知され、ロボタクシーや無人の食品配達サービス車などの実現も、目の前まで迫っています。一方で、企業がコネクテッドカーや自動運転車を適切に運用するには課題も多く、中でもサイバー脅威への対応は、最重要課題の一つといわれています。

自動車に対するサイバー攻撃の影響は、これまでのIT製品に対するものとは大きく異なり、ステアリングやブレーキの操作といった制御機能へ侵入された場合には利用者の安全が損なわれる事態も推測されます。現時点ではサイバー攻撃によるこうした被害の報告はされていませんが、サイバー攻撃の可能性に関する研究者の報告は多数存在するため、対策が急務だといえます。

こうした脅威の増大を背景に、自動車のサイバーセキュリティ対策に関する国際規格の整備が進められています。日本でも官民が協調し、安全で快適なモビリティ社会の実現に向けたセキュリティ基盤を構築しつつあります。

本レポートでは、自動車をめぐるサイバー脅威とその対応について、米国の専門家が見解を示しています。これらの見解を、自社における自動車セキュリティ管理態勢の高度化にぜひお役立てください。

自動車業界は大きな転換期を迎えている。インターネット接続が当たり前のこととなったいま、プライバシー、そして安全性が脅かされるリスクは増大している。自動車メーカー各社はコネクテッドカーを求める消費者の声に応えようと本格的に動き出しているが、モバイル接続に潜むサイバーリスクへの対応が十分ではない企業もある。

防御の甘さは、2015年に二人のセキュリティ研究者がインターネット経由で車両をハイジャックしてみせた事実からもうかがい知れる。このハイジャックでは、ハンドルを回し、短時間とはいえブレーキを無効にし、エンジンをオフにすることに成功した[1]。この結果の意味することは明らかであり、ただちに問題視された。その３年後にあたる現在、インターネットベースの自動車はさらに増え、ハイジャックのリスクは爆発的に増大している。消費者はつながることで得た利便性に慣れきっており、この傾向に変わりはなさそうだ。ただし、利便性が高まれば、その分リスクも大きくなる。一般的に、現在のセキュリティ保護策では、新たなリスクへの対策として十分であるとはいえない。

1. Andy Greenberg, Wired, “The Jeep Hackers are Back to Prove Car Hacking Can Get Much Worse,” Aug. 1, …” https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

コネクテッドカーに潜むサイバーリスク

2015 年に二人の研究者が車両ソフトウェアにリモートでハッキングしてまもなく、米国国土安全保障省（DHS）はサイバー攻撃の脅威の高まりを理由として、二つの研究プロジェクトに 400 万ドルを投じてコネクテッドカーのセキュリティ評価を実施した[2]。2016 年にはあるセキュリティ企業の研究者が、車両エンターテインメントシステムにランサムウェア攻撃につながる脆弱性を発見した[3]。昨年夏には、DHS の国家サイバーセキュリティ通信統合センター（NCCIC）と産業制御システムサイバー緊急事態対応チーム（ICS-CERT）が、車載テレマティクス制御モジュールで発見されたサービス拒否攻撃につながる新たな脆弱性について、複数の自動車メーカーに対し勧告を行った[4]。

インターネット経由の侵入

消費者の需要によって自動車における新たなテクノロジーの導入が促進されるにしても、セキュリティ保護策があらゆるサイバーリスクに対して万能というわけではない。現在販売されているほぼ全ての自動車にはテレマティクスユニットなどのコンポーネントが搭載され、これが外部世界との接続を提供する。コネクテッドカーには各種コンポーネントが存在するため、インフォテインメント、診断機能、エンジン制御ユニット（ECU）のような中核的機能のリモート攻撃の標的となり得る。最新の車両は、リアルタイムのステータス情報を提供する機能やさまざまなリモート制御機能を備えている。これらの機能では、Bluetooth、Wi-Fi、セルラー無線信号を使用して通信を行うが、その基盤となるコンピュータープラットフォームのソフトウェアとハードウェアの両方に脆弱性が潜んでいることが多い。搭乗者は携帯電話などの機器を通じて、自動車のダッシュボードに搭載されたインフォテインメントシステムに接続し、さまざまな操作を行う。車両がコネクテッドデバイスと化しているため、セキュリティ侵害が発生すれば、制御が乗っ取られる恐れがある。攻撃者は車両から実行可能なあらゆる機能を制御できるため、生命にかかわる重大な事故が引き起こされる恐れもある。たとえリモート接続機能を使用していなくても、リスクはある。 自動車と企業は相互につながっており、テレマティクスを通じて侵入されれば、企業の防御が破られてしまう。従って、企業にとって自動車がリスク発生源となる可能性がある。現在のところ、コネクテッドカーに侵入されて悪意ある操作が行われた既知の実例はないが、現実となるのは時間の問題だろう。セキュリティ研究者は、車両の重要領域がハッキングされる可能性を示した。今後さらに機能やテクノロジーがつながるようになれば、脆弱性も増加するだろう。自動運転に向かう動きが、脅威をより一層深刻なものにする。

消費者のプライバシーの侵害

コネクテッドカーに関するもう一つの懸念は、消費者のプライバシーだ。車両内ネットワークを通じて膨大な量のデータ（地理位置、速度、運転が乱暴かどうかなど）が収集され、自動車がさらにつながるように進化すれば、取得されるデータの量も増加する。自動車関連データの販売はまだ始まったばかりだが、商業的可能性があるため、爆発的に広がることは間違いない。保険、広告、エネルギーをはじめとする多くの企業が自動車関連データに関心を寄せている。自動車企業にとって、利益率の高い収益源となるだろう。ただし、自動車関連データの販売に伴い、消費者のプライバシーには重大な懸念が生じる。

「車両がコネクテッドデバイスと化しているため、セキュリティ侵害が発生すれば、制御が乗っ取られる恐れがある。攻撃者は車両から実行可能なあらゆる機能を制御できる...」

2. “https://securityledger.com/2015/11/dhs-funding-research-into-secure-updates-for-vehicles/”.
3. Paul, The Security Ledger, “Update: DHS Funding Research Into Secure Updates for Vehicles,” May 16, 2018 (updated from Nov. 9, 2015); “https://securingtomorrow.mcafee.com/mcafee-labs/defcon-connected-car-security/”.
4. Mark Rockwell, FCW, “DHS, vendor warn on automotive cyber flaws,” Aug. 3, 2017; “https://fcw.com/articles/2017/08/03/auto-cyber-cert-rockwell.aspx”

コネクテッドカーのリスクに立ち向かう

サイバーリスクへの対応の必要性は多くの企業が理解しているものの、ビジネスの問題ではなくテクノロジーの問題として扱われることが多く、サイバーリスクへの対抗手段は限られる。サイバー犯罪者はますます巧妙で狡猾な攻撃手法を用いるようになっている。自動車企業がこれからも事後対応的なセキュリティおよびリスク管理しかできないのであれば、十分なセキュリティ対策を講じることができず、重大なサイバーリスクにさらされ、侵入によって被害を受ける恐れがある。

品質管理

自動車メーカー各社の対応はいまだ後手に回っており、先手を打てないまま、見つかった問題の修正に終始するばかりだ。このようなアプローチには、法的責任を負う可能性や高いコストを伴うリコール、評判の低下など問題が多い。企業に必要なのは、潜在的な脆弱性を見つけ出して修正し、要件を作成してベンダーに伝達することだ。この予防的な事前対応を困難ととらえている自動車メーカーもあるが、不具合を特定して修正するプロセスは従来の品質管理と同様だ。サイバーの世界では、コネクテッドカーの脆弱性が製品の欠陥に直結する。サイバーセキュリティコンポーネントをエンジニアリングプロセスに組み込み、他の製品の不具合と同様に脆弱性を修正することで、既存の品質管理システムを活用できる。

設計段階でサイバーセキュリティを組み込む

自動車の製品設計では、必須要素としてセキュリティを組み込む必要がある。従来の IT ソリューションやエンタープライズ・サイバーセキュリティ・ソリューションとは異なり、セキュリティの技術や機能を後付けすることはできない。従って、製造または本稼働の前に、脆弱性を識別して対処する必要がある。一般的に自動車の製品開発ライフサイクルは 3 ～ 5 年であるため、テストサイクルが 1、2 年では不十分だ。初期テストで脆弱性の大半が認識されるが、時間が経ってから見えてくる不具合もある。さらに、不具合を特定した後は、修正が完了し、新たな脆弱性が生じていない

「サイバーの世界では、コネクテッドカーの脆弱性が製品の欠陥に直結する」

ことを確認するための再テストが必要だ。反復的なセキュリティテストが加わることで開発サイクル全体が延びる可能性があるが、早期に問題を解決しておくことが修正コストの削減につながる。長い目で見れば、セキュアな設計によってリコールを減らし、法的責任を問われるリスクを低減し、ブランドの評判を守ることができる。

サイバーセキュリティをサプライチェーンに組み込む

サプライチェーンにセキュリティを組み込むことは、サイバーセキュリティの予防的アプローチに不可欠だ。コネクテッドカーの先進コンポーネントの多くはサードパーティーサプライヤーから提供されている。とはいえ、製造後に見つかった欠陥は、サプライヤーではなくメーカーのブランドの欠陥と見なされる。自動車メーカーはベンダーにテスト結果を連絡し、セキュリティ要件を事前に策定して指示し、徹底的に要件を遵守させる必要がある。

情報共有

自動車業界ではサイバーセキュリティ要件に関する明確な標準がいまだ確立されていないが、自動車情報共有分析センター（Auto-ISAC）がコネクテッドカーのサイバーセキュリティに関するベストプラクティスを発表している[5]。Auto-ISAC は、自動車のサイバーセキュリティリスクに対する自動車業界の準備と対応の支援のため、サイバー脅威情報を集約する組織である。自動車企業が脅威情報の共有と分析に力を入れることで、Auto-ISAC が強化される。

Auto-ISAC は本年初め、自動車サイバー脅威に関する協力協定を DHS と締結した。この協定によって、自動車業界と連邦政府の専門家の協力が進む。

5. Automotive Information Sharing and Analysis Center(Auto-ISAC), Cision PR Newswire, “Auto-ISAC signs cybersecurity agreement with DHS,” Jan. 25, 2018; https://www.prnewswire.com/news-releases/auto-isac-signs-cybersecurity-agreement-with-dhs-300588475.html

企業にとってのサイバーリスク

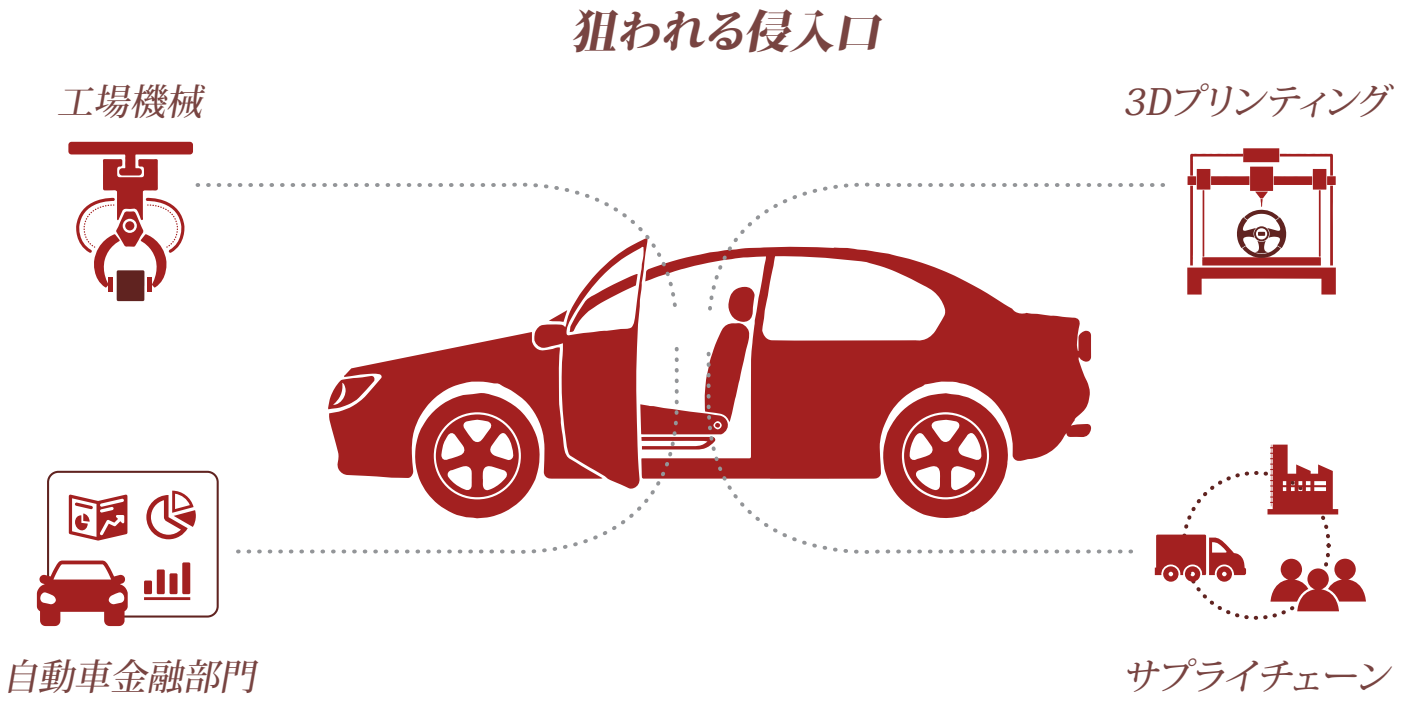
自動車の安全性は、全ての本番プラットフォーム、内部運用、サプライチェーンを横断してサイバー防御を統率する全社規模のプログラムによって支えられていなければならない。一つの領域に弱点があれば、それが他の領域にも広がり、車両故障、工場の停滞、顧客データのハッキング、知的財産の窃取などにつながる恐れがある。明らかな侵入口として狙われるのは次の部分だ。

1. 工場機械： 装置は100%の稼働時間を前提として構築されていることが多く、パッチ適用やアップグレードのため停止することはほとんどない。十分な制御システムを持たない他のレガシーテクノロジーと同様に、このような機械は企業とその業務機能にリスクをもたらす。特にインターネットに接続している場合に顕著だ。

2.3D プリンティング： プロトタイピングや付加製造のプロセスでは3Dプリンティングの活用が進んでおり、そのために使用するデジタルファイルが盗まれる可能性がある。

3. 自動車金融部門： 自動車金融部門は大量の顧客データを収集する。データが盗まれれば、経済的損失と評判の失墜が企業にとって打撃になる。

4. サプライチェーン： どのサードパーティーも何らかのリスク要素をもたらす。小規模ベンダーは十分なセキュリティ管理策を備えていないことが多く、固有の脆弱性がある。IoTによってOEMとサプライヤーのかかわり方が変わり、透明性と効率性が向上することで、サプライチェーンのリスクは急速に増大する。



「自動車の安全性は、全社規模のプログラムによって支えられていなければならない。一つの領域に弱点があれば、それが他の領域にも広がる恐れがある」

エンタープライズリスクに対抗する

サイバーリスクへの対応の必要性は多くの企業が理解しているものの、ビジネスの問題ではなくテクノロジーの問題として扱われることが多く、サイバーリスクへの対抗手段は限られる。サイバー犯罪者はますます巧妙で狡猾な攻撃手法を用いるようになっている。自動車企業がこれからも事後対応的なセキュリティおよびリスク管理しかできないのであれば、十分なセキュリティ対策を講じることができず、重大なサイバーリスクにさらされ、侵入によって被害を受ける恐れがある。

包括的かつ階層型のアプローチ

サイバーレジリエンスを備えた企業は、予防、検知、対応、フィードバックの仕組みを含めて、サイバー攻撃に対抗するための包括的なアプローチを開発している。しかし、絶対確実なソリューションは存在しない。予防策をすり抜け、検知されないまま進行する攻撃もある。成熟したグローバルな自動車企業は、年間数百件の軽微な攻撃と数十件のより本格的な攻撃を受けることを覚悟すべきだ。攻撃を防ぐ、あるいは抑制するには、複数のセキュリティ管理策と、予防、検知、対応のための確立された手順を組み合わせた階層型アプローチが必要である。

最優先すべきは、インシデントの防止だ。攻撃を受けて対応するよりも攻撃を防ぐ方が、必然的にコストが少なくて済む。しかし、攻撃を受けた後は、被害を食い止めるために、できるだけ迅速に攻撃を検知する必要がある。躊躇なく速やかに行動することで、損害を抑えられるだけではない。侵入者が一時的に活動を停止して社内ネットワークのどこかに潜み、後で攻撃を再開しようとする手法を阻むことができる。残念ながら、侵入検知には平均 6 ～ 18 カ月かかるのが実状だ。多くの企業は水面下で侵入されていることに気づいていない。従って、侵入を検知した場合は、侵入者がさらに深く社内ネットワークに潜り込み、被害を広げることのないように、徹底的に対応する必要がある。

次に、サイバー脅威から企業を守るための業界のベストプラクティスをまとめる。

1. 最高責任者レベルの協力を得てセキュリティ文化を醸成する。他の重大リスクと同様に、最高責任者レベルの幹部や取締役会の協力を得て、セキュリティの予算を確保し、企業全体でセキュリティ文化を醸成することが求められる。全従業員が共通のセキュリティ認識を持ち、サイバー攻撃を防止するための各自の役割と責任を理解しなければならない。侵入は組織のどこでも起こる可能性があり、一箇所での怠慢が他の部分にも影響を及ぼしかねない。上層部の姿勢、教育、人事ポリシーを通じて、セキュリティポリシーとサイバーリスクに関する認識の強化を企業文化に取り入れる必要がある。

認識不足はフィッシングの横行のような明らかな問題を招く。古典的ではあるが、無防備な従業員に対してはいまなお有効な手法である。引っかかった従業員がたった一人でも、攻撃者はフィッシングによって大きな見返りを得ることができる。従業員がマルウェアを含む E メールのリンクを開けば、組織全体に感染してしまう。

2. 資産と脅威の優先順位を設定する。全ての資産を保護しようとすればコストがかさむため、高価値の資産を絞り込んで徹底的に保護することが望ましい。また、現在および数年後の未来の脅威、害をもたらす可能性の高い攻撃者を分類し、優先順位を設定することも必要だ。脅威情報

「残念ながら、侵入検知には平均6～18カ月かかるのが実状だ。多くの企業は水面下で侵入されていることに気づいていない」

サービスを利用して業界の最新の脅威を把握し、セキュリティオペレーション手順に反映させている企業もある。

3. プロセスを定義し、統合する。明確に定義されたプロセスがあれば、インシデントの検知から対応までの時間を短縮できる。財務、運用、ブランドがリスクにさらされる度合い、侵入されたシステムの数や種類に基づいて潜在的影響を段階的に分類したマトリクスを作成し、内外の関係者への通知計画をはっきりさせておく。また、侵入とは関係なく内外の事象によって起こる誤検知を判別できる感知および分析機能も導入する。

重大なインシデントと軽微なインシデントの切り分けのため、どのビジネスユニットに通知するか、危機関連の広報戦略を展開すべきかどうかを含め、各種トリアージ手順を定める。インシデントは軽微なものが大半を占めているとはいえ、インシデントに関する定期的な測定基準を確立することは、改善、コスト削減、リスク低減の余地があることを示すパターンを把握するのに役立つ。

先進企業は教訓を生かすための構造化されたプロセスを通じて、手順や方策の見直しと更新を行っている。何がうまくいって、何がうまくいかなかったか？ 改善するにはどうすればよいか？ 具体的には誰がどのように対応する必要があるか？ これらの問いに対する答えを計測プログラムに組み込む。インシデント後の具体的な改善点を管理して実装することで、将来の攻撃に備えた知識を体系的に蓄えることができる。

4. サイバーセキュリティ中核チームのベストプラクティスに従う。 ベストプラクティスとして、インシデント対応にかかわる三つの重要部門（情報またはサイバーセキュリティ、法務、企業広報）の常任委員でワーキンググループを作る。このグループ内で対応のための調整役を担うリーダーを一人選出し、チームメンバーの間での混乱、遅れ、伝達不足を防止する。

この中核的グループが計画および手順を実地検証し、サイバーインシデントへの対応をシミュレーションする。このような演習を、攻撃を受けた場合に迅速かつ効果的に対応するための全体戦略の一環として行う。典型的なシミュレーションでは、重大度マトリクス（重大なインシデントから軽微なインシデントまで）の検証と関連措置（攻撃の性質を判定するためのフォレンジックデータの収集、内外の連絡の調整、予備計画の検討など）を含む。

5. サプライチェーンのリスクに対応する。 自動車企業はパートナーの事業運営において潜在的なセキュリティ侵害が発生していないかどうかを監視し、各種システムへのユーザーアクセスを管理する必要がある。小規模ベンダーはセキュリティ手続きが緩い傾向があり、特殊なリスクをもたらすことから、監査条項と義務付けられたテスト手順を盛り込む。

6. 先進のツールやテクノロジーに投資する。 ますます巧妙化する脅威主体および媒介に対抗するとともに、重要な企業データが組織やサプライチェーンを通して流出するリスクを低減するには、最新のテクノロジーが必要とされる。クラウドを活用したサブスクリプションベースのサービスの機能やインフラストラクチャーを利用するのは、そのための一つの方法である。このようなサービスでは、リアルタイムのアップデートにより情報を集約し、最新かつ動的な防御を維持する。ただし、各組織固有の運用環境に適したツールを展開し、設定することも同様に重要だ。

「インシデント後の具体的な改善点を管理して実装することで... 将来の攻撃に備えた知識を体系的に蓄えることができる」

コネクテッドカーの普及と完全自動運転車が主流となる 10 年以内の将来を見据え、自動車業界は大きな課題を抱えている。これらのテクノロジーは業界を一変させるだけではなく、企業の評判や将来の財務に悪影響を与えかねない、より大きなサイバーリスクも生み出すと考えられる。このようなリスクを低減するには、自社組織とサプライチェーンに脅威を認識するとともに、脅威に対抗するプロセスを遵守するサイバーセキュリティの文化を根付かせる必要がある。クラウドベースのサービスを活用すれば、リアルタイムのアップデートにより情報を集約し、絶え間なく変化し続ける脅威主体および媒介を追跡できる。さらに、侵入による被害を抑えられる最新のツールやテクノロジーに投資することも不可欠だ。

サイバーセキュリティ対策には、手間もコストもかかる。しかし、この取り組みによって自動車産業とその顧客の路上での安全を守ることが可能になる。

お問い合わせ

この記事で取り上げたテーマについてのご相談をご希望の場合、
以下までお問い合わせください。

PwC - US Automotive Practice

Ray Telang
Partner, US Automotive Leader
Tel: +1 (313) 394 6738
ramesh.d.telang@pwc.com

Mike Lambert
Principal, Automotive Technology
Tel: +1 (248) 613 5601
mike.lambert@pwc.com

編集、寄稿

Gloria Gerstein
Tel: +1 (212) 787 4607
gloria.gerstein@pwc.com

一般的なお問い合わせ

Diana Garsia
Senior Manager, US Automotive
Tel: +1 (973) 236 7264
diana.t.garsia@pwc.com

www.pwc.com/automotive

PwC - US Cybersecurity Practice

Rik Boren
Partner, Cybersecurity & Privacy,
Industrial Products Leader
Tel: +1 (314) 206 8899
rik.boren@pwc.com

Rob Shein
Manager, US Advisory
Tel: +1 (202) 445 4447
robert.j.shein@pwc.com

日本のお問い合わせ先

PwCコンサルティング合同会社
東京都千代田区丸の内2-6-1 丸の内パークビルディング
03-6250-1200（代表）

林 和洋
パートナー
kazuhiro.hayashi@pwc.com

www.pwc.com/jp

本報告書は、PwCメンバーファームが2018年6月に発行した『Cyber readiness: are auto companies prepared to counter the risk of an attack?』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/knowledge/thoughtleadership.html
オリジナル（英語版）はこちらからダウンロードできます。 https://www.pwc.com/automotive
日本語版発刊年月：2018年8月　管理番号：I201806-3