Deloitte.
デロイト トーマツ

Fasten your digital seatbelt

アジアパシフィック地域における
今日の自動車業界のセキュリティ対策

MAKING AN IMPACT THAT MATTERS since 1845

はじめに

自動車業界はデジタル時代に向けて全速力で進化を遂げていますが、サイバーセキュリティ対策は必ずしも同じスピードで進んでいるわけではありません。コネクテッドカーやスマートファクトリーは、従来にくらべ、インターネットとの接点が増えることでサイバー攻撃を受けやすい環境になっています。

わずか１件の侵入によって、人々が危険にさらされる可能性があるのです。また、生産の遅延や停止などにより、莫大なコストが生じ、ビジネス全体に影響が及ぶ恐れもあります。

自動車メーカーがデジタル化を進めている今こそ、セキュリティ対策を導入して精緻化する絶好のチャンスです。本レポートではIT、車両、工場の３つの自動車領域に重点を置いたセキュリティ対策を推奨しています。

上記の３領域は、環境面の違いから、それぞれのセキュリティ課題に直面していますが、同時にさらなるデジタル時代に向けて自動車業界が強化されうる有望な機会を提供しているといえます。デジタル化に向けた最良のルートは、全領域において包括的なセキュリティを確立することです。

デジタル化と並行したセキュリティ対策の成功のカギは、さまざまな部門やオフィス間でのコミュニケーションと連携であり、グローバル本社（GHQ）は自社内の知識、経験、リソースを共有するハブとして機能する必要があります。

自動車業界は、ユーザーの期待に即したデジタル化を成し遂げることが求められています。そして、データ、人、ビジネスの安全やセキュリティが最大限確保されているという確信のもと、各自動車メーカは、それぞれの達成目標に向けて加速することができるのです。

全ての自動車領域に固有の高いサイバーリスクが内在しているにもかかわらず、備えは不十分

デロイトは2022年に、アジアパシフィック地域の主要自動車メーカーを対象に、業界が直面するサイバーセキュリティ課題を調査しました。そこで判明した重要な事項の1つは、従来から運用されてきたデジタルプロセスのセキュリティ成熟度にくらべ、新しくデジタル化された、または現在デジタル化が進行中の領域のセキュリティは遅れている可能性が高いということです。

情報技術（IT）　**車両**　**工場**

- ネットワークデバイスやサーバーなどの**情報技術（IT）**システムについては、セキュリティ保護レベルが向上している傾向にあります。ITプロフェッショナルは長年にわたり、セキュリティインシデントを検出し、回避してきました。IT領域では、様々な種類のセキュリティ対策や確立されたセキュリティ製品・サービス、成功事例があるため、他の領域に比べてリスクに対処しやすくなっています。

  また、自動車業界のITチームの多く（60%以上）が、脅威や脆弱性に関する情報収集のために脅威インテリジェンスサービスを使用していると回答しました。このようなデータをセキュリティ対策のためのインプットとして早期に活用する傾向が強く見られます。

自動車業界のITチームの

60%

以上が、脅威や脆弱性に関する情報収集のために脅威インテリジェンスサービスを使用していると回答しました。

- **車両**がデジタルに対応し、コネクテッドデバイス化してきたのはごく最近のため、セキュリティが追い付いていない傾向にあります。そして規制当局もこの遅れを懸念し始めています。

  これにより現在、自動車分野では国際標準化機構（ISO）のISO/SAE 21434や、国連の規則R155およびR156といった業界規格・規則が次々と制定されています。

  例えば、多くの国が批准するUNR-155や類似の法規では、コネクテッドカーをサイバー攻撃の脅威から守るためのプロセス（サイバーセキュリティを確保するための業務管理システム：CSMS）を整備し、運用することが自動車メーカーに義務付けられています[1]。一方デロイトの調査研究結果によると、多くの自動車メーカーは依然として車両セキュリティに関するスキルと知識をブラッシュアップしている段階にあります。

  近年、自動車メーカーやサプライヤーは、セキュリティ課題がビジネス目標の達成に重要であることを認識し始めています。しかし、安全な製品を製造するためには、セキュリティ対策を設計の初期段階から組み込む必要があり、車両開発、製造、さらに出荷後の車両についても、頻繁なセキュリティテストが不可欠となります。

  一方で、開発にはスピードが求められるため、開発者がセキュリティを軽視し得る可能性もあります。DevSecOpsという手法は、ソフトウェア開発の各段階でセキュリティテストを統合してスピードとセキュリティ双方のバランスを取るように設計されたものですが、多くの自動車メーカーやサプライヤーは、まだこれを手法を取り入れられていません。

規格・規則

ISO/SAE 21434

R155

R156

- **工場**は最も困難な状況に直面しています。自動化が進むにつれて、ロボットやセンサー、人工知能（AI）などのテクノロジーが採用されていきますが、セキュリティの確保に苦労しています。

  先進運転支援システム（Advanced Driver Assistance Systems）で使用される組み込みソフトウェアは、この課題に拍車をかけています。ADASや自動運転のための安全な組み込みソフトウェアを見つけるのはとても困難です。

  またクラウドアクセスセキュリティブローカー（CASB）、IDおよびアクセスの管理、エンドポイントセキュリティといったセキュリティ管理ツールは非常に効果的ですが、自動車メーカーは自社工場内にいまだ多くのレガシーシステムを抱えているため、利用することが難しいのが現状の課題となります。

デジタル化の初期段階にある今こそ、こうしたセキュリティ技術を利用開始するチャンスです。また同時に、工場の責任者は、作業員にセキュリティの重要性を教育し始めると良いかもしれません。

1. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-advisory-securing-the-vehicles-of-the-future-aoda.pdf

脅威インテリジェンス：サイバー犯罪阻止に不可欠なツール

現代のテクノロジーは、サイバー攻撃の手法や動機について、多くの情報を私たちに与えてくれます。脅威インテリジェンスは、将来の脅威やトレンドを正確に予測するのにも役立ち、悪意ある攻撃者の一歩先を行くために最適な備えとなる情報を提供します。

脅威インテリジェンスは非常に有効でありながら、自動車業界で活用されていないツールの一つと言っても過言ではありません。多くのグローバル本社（GHQ）は、工場のオペレーションやシステム技術の安全を確保するために脅威インテリジェンスを利用していますが、車両のセキュリティの確保において、脅威インテリジェンスを利用している自動車メーカーはごくわずかです。

GHQのサイバープログラムは多くの場合、明確に確立されたプロセスと指揮系統を備えた適切な構成になっていません[2]。脅威インテリジェンスによって提供される情報を有効活用するためには、そのような構成は不可欠です。例えば、脅威インテリジェンスのデータは、自動車セキュリティのエンジニアが既知の脅威に対する保護対策をソフトウェアの設計に組み入れるのに役立ちます[3]。

脅威インテリジェンスのデータを活用することで、サイバー関連の意思決定をより適切に行うことができます。しかし、それが可能なのは、その意思決定の責任者は誰か、また、そのプロセスはどのように機能しなければならないかが周知されている場合に限られます。GHQは脅威インテリジェンスの技術とそのプロセスを社内に浸透させ、効果的に利用する方法を車両チームへ教育しなければなりません。また、自社内の関係者が脅威インテリジェンスに精通するよう支援し、社内、車両、そして顧客の安全も置き去りにされないようにする必要があります。

2. https://www2.deloitte.com/dk/da/pages/risk/cyber-risk/cyber-strategy-transformation/effective-cyber-risk-governance.html
3. https://standards.ieee.org/wp-content/uploads/import/documents/other/e2e-presentations/feb-2021/04-Securing_Connected_Autonomous_Vehicles_as_an_Industry.pdf

全てがデジタルでつながっているからこそ、セキュリティはこれまで以上に重要になっている

工場では、人の介入が減り、自動で稼働する「サイバーフィジカルシステム」へと急速に移行しています。また、車両は毎年新しいデジタル機能を搭載し、完全自動走行車の実現はかつてないほど現実味を帯びています。

人、機械、ロボット、センサー、ソフトウェア、ハードウェア、ファームウェアというように、ほぼ全てのモノや人がデジタルでつながる現代は、まさにデジタル時代といえます。しかし、自動車業界において、こうしたつながりが悪意のある力によって断たれることがないよう適切なセキュリティを整備できる段階にあるのはIT領域だけです。

車両は、UN-R155およびR156に適合する特定のセキュリティ機能を備えていなければなりません。ソフトウェアやファームウェア、そしておそらくは暗号化キーもリモートで更新できるソフトウエア アップデート OTA（Over the Air）機能はその一例として挙げられます。安全でない車両は、生命に危険をもたらします。しかし、私たちの調査では、自動車メーカーの大多数（80%）が車両のセキュリティを監視していないことがわかりました。

工場もまた、機械、ロボット、センサーをはじめとするコネクテッドデバイスが侵入を受けたり、改ざんされたりすると、安全でない車両や部品を生産したり、工場で働く人にとって危険な場所になる可能性があります。一つのサイバーセキュリティインシデントによって工場は操業停止に追い込まれ、膨大な時間とお金が失われることもありえます。ところが、デロイトの調査によれば、多数のコネクテッドデバイスのセキュリティを継続的に監視しているのは、自動車製造工場の3分の1（30%）弱にすぎません。

サイバー犯罪者はこうした状況を認識して、車両と製造工場それぞれの領域を攻撃対象としているのです。その結果として損失と損害の規模が拡大し続けていることは、継続的なセキュリティ監視を導入する十分な理由ではないでしょうか。

法律や規制もまた、急増し続けています。その中には、車両やサプライヤー工場についてサイバーセキュリティ対策を義務付けているものもあります。

自動車メーカーやサプライヤーは、自社システム、車両、工場へのサイバー脅威に対して一層警戒を強め、継続的な自動監視機能を利用して、危険が発生する前に、そして発生した場合に確実に状況を把握できる必要があります。

自動車メーカーの
80% **が自社の車両セキュリティを監視していません。**

多数のコネクテッドデバイスのセキュリティを継続的に監視しているのは、自動車製造工場の
30% **弱にすぎません。**

走るコンピュータには高速で機敏なセキュリティが必要

「車両の機能や性能」は、その機械的特徴ではなく、インストールされたソフトウェアやその設定によって、定義されることが一般化しています。まもなく、すべての自動車が「Software Defined Vehicle：SDV」、つまり車輪のついたコンピュータとなるでしょう。

あらゆるコンピュータと同様、ソフトウェアへの依存度が高まるSDVは、より高い攻撃のリスクにさらされています[4]。しかし、現在そして将来の車両は、デスクトップコンピュータよりもその危険度は高く、リスクも大きいのです。

デスクトップコンピュータやシステムへの侵入は、データの損失や製品の販売遅延を引き起こす可能性がありますが、車両への侵入は、人を傷つけ、命をも奪うおそれがあるのです。

現代のCASE（「Connected」、「Autonomous」、「Shared」、「Electric」）車両が改ざんされる可能性は、かつてないほど高まっています。ある調査によると、車両へのサイバー攻撃は2018年から2021年にかけて225%増加し、2021年には車両への攻撃の85%近くが遠隔で行われました[5]。また、同調査では、サイバー攻撃による自動車業界の損失は、2024年までに5億500万米ドルに達すると予想されています[6]。

しかし、セキュアソフトウェア開発ライフサイクル（SSDLC）によるソフトウェア開発プロセスを実行してもなお、脆弱性は発生する可能性があるのです。SSDLCでは、開発者は計画の初期段階から、セキュリティとプライバシーの保護について設計する必要があります。そして開発プロセス全体を通して、またソフトウェアが使用されている限り、継続的にテストを行わなければなりません。

自動車関連企業は、自社の技術に対するリスク、特にセキュアなソフトウェア開発面で大きく遅れをとっている車両や工場に対するリスク軽減策に取り組む必要があります。デロイトが推奨する事項には次のようなものがあります。

サードパーティであるサプライヤーのセキュリティ評価を行いましょう。サプライヤーには全地球測位システム（GPS）、エンターテインメントプラットフォーム、電動化、自動運転機能などを提供するソフトウェア企業も多く含まれますが、これらサプライヤーの開発サイクル（企画・設計・製造・テスト）の各フェーズで、セキュリティはどの程度確保されているでしょうか。

自社のソフトウェア開発プロセスを評価しましょう。自社の開発者もSSDLCの原則を適用する必要があります。またそうすることで、競合他社との差別化にもつながります。CASEが当たり前になり、車両のセキュリティはますます重要になっています。

4. https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/consumer-business/deloitte-cn-cb-software-defines-vehicles-en-210225.pdf
5. https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/
6. 同上。

企業全体、社会全体での連携した取り組み

企業活動のデジタル化が進むににつれて、ビジネスにおけるサイバーセキュリティに重要度や関心度が高まります。あらゆる事業部門や子会社がつながっている現在では、どこに脆弱性が存在するかわからない状態になっています。セキュリティ上の欠陥（デバイスへの侵入経路）が１つでもあれば、企業全体に、そして世界中に壊滅的な影響を及ぼす可能性があります。

自動車業界全体が一丸となって連携して取り組むことが、車両と私たちの安全を守る唯一の方法です。

システムやネットワーク、データセキュリティがITの関心事でしかなかった時代は終わりました。また、それぞれの子会社や事業部門がセキュリティに気を配り、個別最適なセキュリティ管理アプローチもなくなりました。現代は、社会全体でこの問題に取り組む時代なのです。

デジタル面で成熟した自動車メーカーは、このような相互関係を認識するようになり、セキュリティを全社的な関心事として管理し始めてはいますが、「皆は一人のために、一人は皆のために」というアプローチは、重要ではあるものの、自動車業界の現状からは程遠いと言えます。

自動車関連企業にとっては、会社全体のサイバーセキュリティに特化した部門を持つことが特に重要です。GHQと子会社のハブとなり、各機能や事業部門をつなげる役割が必要なのです。

GHQではない組織では特に、「全体のためのセキュリティ」という必須認識とそれに基づいた行動という点で、腰が重い状態が続いています。GHQは先頭に立って、社内全体に進むべき道を示し、そのサイバーセキュリティの革新を支援する必要があります。

行動するときは今

現在、自動車業界は特にサイバー攻撃の影響を受けやすい状態にあり、情報技術（IT）車両、工場を標的にしたサイバー攻撃は増加の一途をたどっています。自動車関連企業は、IT、車両、工場3つの領域全てにおいて、適切なサイバーセキュリティ対策の導入に向けた努力が必要になっています。そしてサイバーセキュリティは現在も将来も組織全体の必須事項でなければならないのです。

サイバー犯罪者は脆弱性を認識しており、自動車業界への攻撃を強めています。その結果は、自動車業界のみならず、ドライバー、同乗者や乗客、そして社会全体にとって悲惨なものになりかねないのです。

幸いなことに、一部のGHQはサイバー対策の重要性を認識し、最優先事項としています。今こそ、全てのGHQがそうする時であり、社内全体が追随する道を切り開くタイミングがきています。そうすることで、自動車メーカーは自社の成功を支えるだけでなく、全ての人にとってより安全な社会を育み続けることができるのです。

著者および寄稿者

Hiroshi Hayashi
Asia Pacific Cyber Automotive leader
hiroshi.hayashi@tohmatsu.co.jp

Karen Grieve
Director
kagrieve@deloitte.com.au

Eric Leo
Director
eleo@deloitte.com.au

主な連絡先

Hiroshi Hayashi
Asia Pacific Cyber Automotive leader
hiroshi.hayashi@tohmatsu.co.jp

Ian Blatchford
Asia Pacific Cyber leader
iblatchford@deloitte.com.au

中国

Boris Zhang
Partner
zhzhang@deloitte.com.cn

南アジア

Praveen Sasidharan
Partner
psasidharan@deloitte.com

日本

Hiroshi Hayashi
Partner
hiroshi.hayashi@tohmatsu.co.jp

東南アジア

Weng Yew Siah
Partner
wysiah@deloitte.com

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイトトーマツ税理士法人、DT弁護士法人およびデロイト トーマツ グループ合同会社を含む）の総称です。デロイトトーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市に約1万7千名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイトアジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務、法務などに関連する最先端のサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約415,000名の人材の活動の詳細については、（www.deloitte.com）をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited

Designed by CoRe Creative Services. RITM1403730

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301