URL　https://journal.ntt.co.jp/article/30148
DOI　https://doi.org/10.60249/24115102

J-Auto-ISACの取り組みに見る「共助」のあり方——高まるサプライチェーンリスクへの次の一手

今やサイバーセキュリティは，ありとあらゆる領域に関連するトピックとなっています．日々の暮らしや経済活動に欠かせない「車」も例外ではありません．今，車をめぐってどのような脅威が存在し，それに対して自動車産業はどのような対策を進めようとしているのかを，Japan Automotive ISAC（アイザック）サポートセンター長と，NTTセキュリティ・ジャパン シニアコンサルタントの対談を通して紐解いていきます．

キーワード：#自動車産業サイバーセキュリティガイドライン，#サプライチェーン攻撃，#J-Auto-ISAC

なかじま　かずき
中島　一樹[†1]
たかはし　ひでゆき
高橋　秀行[†2]

Japan Automotive ISAC　サポートセンター センター長[†1]
NTTセキュリティ・ジャパン[†2]

自動車産業は100年に一度の変革期 脅威の高まりという課題も浮上

高橋：現在，自動車産業は100年に一度の変革期を迎えているといわれています．具体的にはどのようなトレンドが起こっているのでしょうか．

中島：皆さんもどこかで「空飛ぶクルマ」の話題を聞いたことがあると思います．2025年に控える大阪・関西万博では，新たなモビリティとして日本のスカイドライブ社をはじめ国内外の企業が空飛ぶクルマを運航し，その後の商用化も見据えられています．また地上を走る車に関しても，日本各地で自動運転の実証実験が行われています．海外ではすでにAlphabet傘下のWAYMOがロボットタクシーの提供を開始するなど，いよいよ実用化の段階に入ってきました．

車そのものの進化は，自動車産業にも変革を迫っています．これまで自動車産業は「製造業」，つまり工場で車を生産し，ディーラーで販売するというビジネスモデルに立脚してきました．これからは，自動運転をはじめとした新たな付加価値を提供するモビリティビジネスへの転換が求められています．これが100年に一度の大変革期といわれるゆえんです．

高橋：未来のクルマには，どのような特徴があるのでしょう．

中島：Connectivity，Autonomous，Shared Service，そしてElectricの4つが変革のキーワードで，頭文字を取って「CASE革命」とも呼ばれています．

まずConnectivityですが，これからの車は，道路や信号，他の車，あるいはクラウドサービスなどさまざまなものとつながっていくコネクティッドカーとなります．Autonomousとは文字どおり自動運転を意味します．Shared Serviceとは，カーシェアやライドシェアといった新たなサービスで，所有から共有への移行を意味します．最後のElectricは，電動化のことです．「電気自動車への変換」というのは誤解です．これまでの車は，ハンドルやタイヤ，ブレーキといったコンポーネントは，歯車やワイヤーといった物理的な仕組みで制御されていました．

しかし今では，こうしたコンポーネントはCAN（Controller Area Network）やイーサネットなどの車載ネットワークを介して，走る，曲がる，止まるをECU（Electronic Control Unit）によって制御しています．ECUは車1台当り平均で30個，高級車では100個以上も搭載されるようになっています．

これにより，つながる車，先進運転支援システム，そして自動運転といった技術面での大きな進化を遂げつつあります．一方で新たな懸念も生じています．具体的にはハッキングのリスクです．2013年のトヨタ・プリウスとフォード・エスケープに対するハッキングのデモを皮切りに，これまで複数の研究者によって自動車を対象にしたさまざまなハッキング手法が報告されてきました．現実には，ハッキングに起因する重大事故は起きていませんが，脅威は近づいているといっていいでしょう．

サイバーリスク

高橋：車そのものに対するリスクに加え，自動車業界そのものもリスクにさらされていますね．残念ながら，国内の主要自動車メーカーではすでに，マルウェア感染による工場の操業停止を余儀なくされる事態を経験しています．とりわけ，メーカーそのものが侵入されたのではなく，サプライチェーンを構成する取引先や海外拠点がまず侵害を受け，その余波を受けて生産が止まってしまう事態になっていることは，最近の特徴だと考えています．

実は，こうした問題は自動車業界に限りません．2023年には，大阪の病院がランサムウェアの被害に遭いました．病院食を納入している給食事業者のVPN（Virtual Private Network）装置に残っていた脆弱性が悪用され，リモート接続回線を通してランサムウェアに感染してしまったことが報告されています．このように，取引先，サプライチェーンを経由して侵入され，ランサムウェアに感染する事例が相次いでいます．いくら自社のシステムを固めていても，取引先やサプライチェーンに「穴」があり得る以上，どこかから攻撃されても不思議ではありません．

深刻なのは，事業継続に重大な影響を及ぼしてしまうことです．ランサムウェアはシステムやデータを暗号化し，「元に戻し

てほしければ金銭を支払え」と身代金（ランサム）を要求してくることから名付けられました．この身代金はもちろんですが，企業にとってダメージが大きいのは，事業を支える生産システムや営業システム，病院であれば電子カルテシステム，あるいはメールなどのコミュニケーションシステムが暗号化されてしまい，仕事ができなくなってしまうことです．数日から数週間，場合によっては数カ月にわたって開店休業状態になってしまいます．

加えて，システムを暗号化する前にデータを盗み出し，ダークウェブなどで公開するぞと脅したり，DDoS（Distributed Denial of Service）攻撃を行ったり，さまざまな手口が報告されています．背に腹は代えられないと身代金を支払ったとしても，相手は「犯罪者」です．身代金の増額やおかわりを要求してくることもあります．また，警察庁などの調査では，身代金を支払っても復旧できないケースは珍しくありません．

背景には，サイバー攻撃の組織化があります．かつては，攻撃者が自らランサムウェアを開発し，ばらまいて金銭を要求するケースもあったようですが，今やそうした方法は稀です．マルウェアそのものを開発し，サービスとして提供する「Ransomware as a Service」に加え，脆弱なVPN機器やID・パスワードなどのアカウント情報を提供し，企業に侵入する糸口を用意する「イニシャルアクセスブローカー」，そうした情報や攻撃によって詐取された情報を売買するダークウェブやリークサイトの運営者など，複数のプレイヤが存在し，それぞれがランサムウェア攻撃をビジネスとして展開しています．

金銭を目的としたこうした組織的なサイバー犯罪者に加え，国家や軍といった後ろ盾を持つ高度な攻撃も横行しています．しかも近年では，サイバー犯罪者と国家支援型の攻撃の間にも重なりがみられるという調査もあります．私たちは今，こうした時代の中にあるのです．

中島：こうした状況を踏まえ，世界経済フォーラムでは国際紛争や自然災害と並んで「サイバーリスク」を主要なグローバルリスクととらえていますね．

高橋さんもおっしゃったように，一口にサイバー攻撃といっても，いくつかの主体があります．まず国の組織として活動するサイバー軍があり，そこに政府の金銭的支援を受けるハッカー集団，それ以外のサイバー犯罪者などです．攻撃者の活動に多額の国家予算が付いている以上，サイバー攻撃がゼロになることはないでしょう．

一方，攻撃対象となるプログラムの脆弱性は残念ながら増え続け，連日のように報告されています．ITシステムを構成するOSやミドルウェアに関しても相当数がありますが，コネクティッドカーが搭載するソフトウェアのコード行数は，スマートフォンの数十倍になっており，なお増え続けています．おそらくコネクティッドカーに関係する脆弱性も増え続けていくでしょう．

サイバー攻撃者は，こうした「弱いところ」があれば，すかさず狙ってきます．コネクティッドカーのセキュリティを確保するには，車の設計，製造，さらには販売された後のメンテナンス時のソフトウェアアップデートに至るすべてのフェーズで取り組む必要があると考えます．

もう1つ，巨大なピラミッド構造で構成される自動車業界として留意すべきリスクがサプライチェーン攻撃です．日本の企業の99.5%は中小企業であり，予算や人材などに十分なリソースを割けないのが実情です．結果として，日本では他国に比べて，取引先企業を踏み台にしたサイバー攻撃による被害が多くなっています．こうした状況を変えていくには，中堅規模以下の組織のセキュリティレベルを底上げしていくことが喫緊の課題であるととらえています．

共助による業界全体のセキュリティ対策底上げをめざす 外部の目も活かしリスクベースで即効性のある対策を

高橋：こうしたサイバーリスクに対し，具体的にはどんなアプローチが有効だとお考えですか．

中島：私は大きく3つのアプローチがあると思います．

1番目は自組織単体で対応する「自助」です．セキュリティ人材は質・量ともに不足している一方で，攻撃側は高度化，多様化，自動化が進んでおり，圧倒的に攻撃者優位な状況です．

すでに自助だけで十分な対策を行うのは現実的ではないと考えています．

2番目は政府・公的機関による「公助」です．サイバー空間は国単位で管理されているのが実態です．中国でGoogle検索やLINEが使えなかった経験をされた方も多いと思います．サイバー空間は陸，海，空，宇宙に続く第五の国際紛争領域といわれ，各国がサイバー部隊を増強していますが，我が国は周辺国に比べて多勢に無勢の状況で，公助のみに依存するのは難しい状況です．

となると重要な取り組みは3番目の「共助」です．企業や組織どうしが集まり，互いに知見を高め合いながら業界全体でサイバーセキュリティを守っていく取り組みです．

我が国には，重要インフラ分野において官民連携で取り組むCEPTOARという組織や，組織内でセキュリティインシデントの初動対応に取り組む産官学の「CSIRT」が連携する日本シーサート協議会，そして，業界として取り組むISAC（Information Sharing and Analysis Center）があります（**図1**）．

私たち自動車産業は，OEM（メーカー）からティア1，ティア2……と，数十万社による多階層の巨大ピラミッド構造となっており，サプライチェーンの裾野の広さが特徴です．そこでコネクティッドカーのサイバーセキュリティを守ることを目的に，2021年2月，自動車メーカー14社と主要サプライヤー21社が発起人となって「Japan Automotive ISAC」（通称：J-Auto-ISAC）を設立し，共助の枠組みを整備しています．

またICT-ISACなど他の業界のISACとも定例会を開き，連携強化を進めているほか，米国のAuto-ISACとも連携しています．

高橋：自動車業界は，共助の取り組みが進んでいますね．J-Auto-ISACもそうですが，日本自動車工業会と日本自動車部品工業会では2020年3月に共同で「サイバーセキュリティガイドライン」を公開し，自動車産業全体のセキュリティの底上げに取り組んできました．個社がバラバラにセキュリティ対策を求めるのではなく，自動車産業として標準的にめざすべき項目をまとめたもの

です．

2024年 8 月28日には最新版であるv2.2が公開されています．自動車産業は，中島さんがおっしゃったようにピラミッド構造となっていますが，業界内での役割・立場や企業規模に応じて 3 つのレベルを設定し，レベルごとに満たすべき事柄が示されています．ガイドラインとともに「自動車産業セキュリティチェックシート」が用意されており，2025年 3 月末までに各社が達成することをめざすという，実践的な取り組みです．

例えば「情報セキュリティ事件・事故発生時の対応体制と責任と役割を明確化している」という項目があります．文字にすると単純ですが，具体的には，情報セキュリティ統括役員が任命され，その役割や責任が明確化されているか，さらに情報セキュリティ部署が設置され，役割や責任が明確化されているか，セキュリティ事故が発生した際の連絡ルートやフローは整備されているか……といったさまざまな事柄が要求されています（**図 2**）．

このガイドラインを受けて，「何から始めればよいのか分からない」「難しくてよく分からない」，そして「どこまでやればよいのか分からない」と悩む声もお聞きしています．これに対して私たちが専門的な立場からアドバイスしたいのは，「自社の現状，リスクを正しく把握すること」，そのうえで優先順位を付け，「リスクに対して即効性のある対策から実施していくこと」です．

私たちが健康を保つには，闇雲に薬を飲んでも意味はなく，かえって害となりかねません．定期的に健康診断を行い，問題があればより詳しく検査し，適切な治療を行い，きちんと回復しているか，悪化しないかと経過を観察しながら完治をめざし，場合によってはリハビリによってより身体を正常な状態に近づけていきます．

サイバーセキュリティも同様です．自社の現状やリスクを把握したうえで必要な対策を取り，その後も監視を続け，再発防止やレジリエンス強化に向けた新たな手を打っていくことが重要です．その意味で，最初の診断はとても重要です．専門家によるヒアリングのほか，ツールを用いたスキャンなどによるシステム診断はもちろん，物理的な施策や社員のリテラシー，管理体制などを総合的に把握することが重要です．

ただ，いきなりすべてを行う必要はありませんし，そんなリソースもないでしょう．健康診断的なものをめざすのであれば，まずは専門知識を持つ第三者によるリスクアセスメントからスタートすることをお勧めしています．

また，外部の攻撃者目線で自社がどのように見えているかを評価し，設定ミスや放置された脆弱性などを発見する「Attack Surface Management（ASM）」のようなシステム診断も重要です．攻撃者は，どこか弱いところがないかを偵察し，攻撃してきます．ですので，攻撃者目線で脆弱なところがないかを確認するだけでも，健康診断としては非常に有効です．

もう 1 つお伝えしたいポイントが，即効性のある対策から実施していくことです．あれもこれも，すべての対策を一気に実施することは非現実的です．リスクベースで，つまり「現時点でもっとも自分たちにとって脅威となるもの」に対して手を打っていくことが効果的です．

自動車産業において今何がもっとも脅威かというと，やはり，サプライチェーンを狙ったランサムウェア攻撃でしょう．残念ながら，サプライチェーンの対策ができていない企業が64%以上あるという調査結果もあります．そこで，VPN機器の脆弱性から侵入されるケースが多いことを踏まえ，その脆弱性対策を実施するほか，リモートアクセス時の認証強化，そして，それでも被害に遭う可能性はゼロにはできないことを前提にバックアップを取得するといった

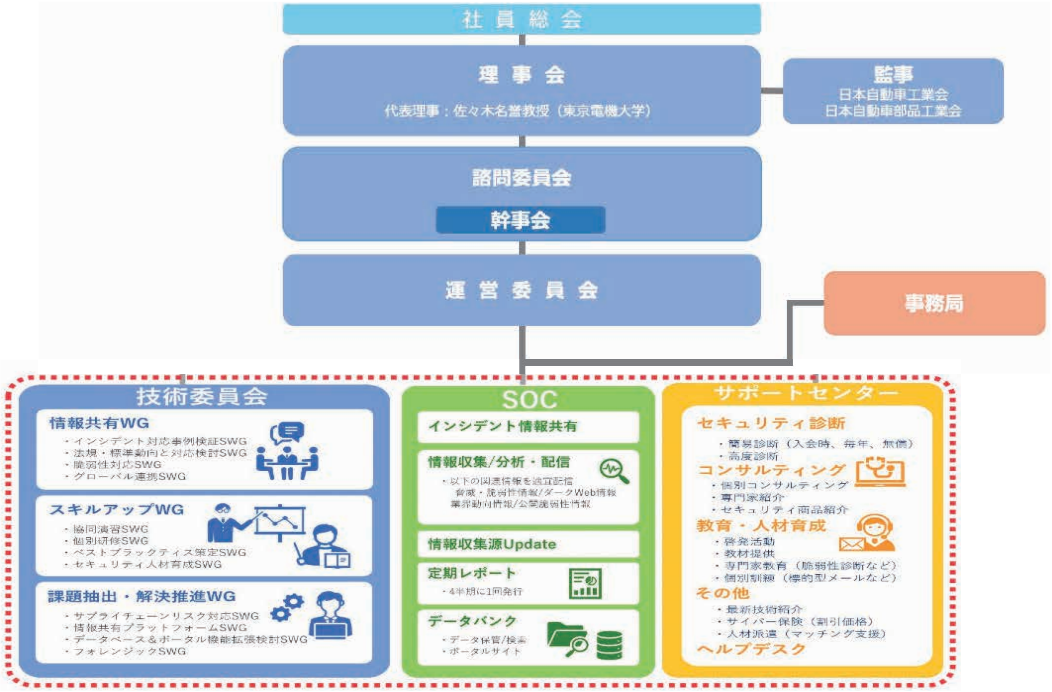

図 1　一般社団法人 Japan Automotive ISAC 概要

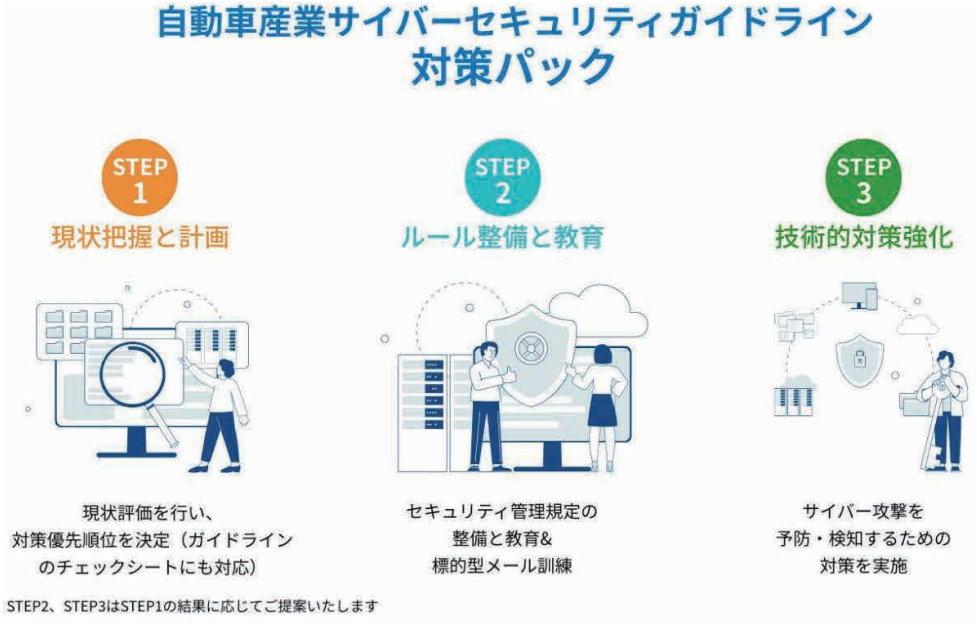

図２　自動車産業サイバーセキュリティガイドライン対策パック

対策が必要だと考えられます．

人や組織の対策も欠かせません．ガイドラインに含まれる項目のうち，技術的な対策は全体の４分の１程度です．ルールや運用，人に対する教育のほうが大きな割合を占めています．社員全体に対するリテラシー教育はもちろん，運用に携わるセキュリティエンジニアの育成は大きな課題です．セキュリティ教育やメール訓練等を提供するサービスや教育プラットフォームも登場していますので，それらの活用も検討すべきでしょう．

中島：J-Auto-ISACではこうした動きも視野に入れつつ，主に３つの組織を中心にさまざまな活動を展開してきました．

まず，技術委員会では，自動車メーカー，サプライヤー，セキュリティの専門家が一体となってワーキンググループを設置し，サプライチェーンリスクやSBOM（Software Bill of Materials）といった業界共通の課題に取り組んでいます．

２番目のSOC（Security Operation Center）は，一般的なSOCとは異なります．一般的にSOCは，監視して攻撃を検知することが主なミッションですが，J-Auto-ISACのSOCは主に脅威情報や脆弱性情報の収集・分析・管理を行っています．日々報告される大量の脆弱性情報をAI（人工知能）で車に関するものにフィルタリングし，さらに専任のアナリストの目で精査して特に重要なものについては解説を加えて会員に提供しています．自社で脆弱性情報の解析を行うとなると多額の費用と多くの人的リソース，さらに専門的な知見が必要となりますが，それを肩代わりするかたちです．

３番目のサポートセンターは，業界全体のセキュリティレベルの底上げに取り組んでいます．ISAC内では他社のインシデント情報などの機密情報を共有しますから，一定のセキュリティレベルを担保することを目的に，入会時に加え，定期的に会員組織のサイバーセキュリティ診断を実施しています．まさに，高橋さんのおっしゃった健康診断にあたるものです．

自動車産業は大きな変革に直面していますが，その歩みがセキュリティ面での問題によって阻害されてはなりません．自動車産業にかかわってきた方，そしてこれからモビリティビジネスへの参入を検討されている方々には，ぜひJ-Auto-ISACへの参画をご検討いただきたいと思います．

高橋：ぜひ共助の取り組みを進めていきたいですね．

もう１つ，最後にお伝えしておきたいことがあります．それは「経営者を巻き込もう」ということです．サイバー攻撃がたびたび報道される中，対策を強化したくても「そこはIT部門でうまくやっておいてね」と，丸投げに近い状態で指示だけをされて，苦労されている方も少なくないと思いますが，今や，経済産業省／情報処理推進機構（IPA）の「サイバーセキュリティ経営ガイドライン」にも示されているとおり，サイバーセキュリティは経営課題です．

経営者にセキュリティを自分事としてとらえてもらうためには，やはり「自社の状況」を正確に，分かりやすく伝えていくことが不可欠だと思います．「自動車産業セキュリティチェックシート」の結果を示し「同業他社に比べてこれだけ低い位置にあり，不合格です」と伝えるのも１つの手でしょうし，外部の専門家にアドバイスを求めるのも良いかもしれません．まずは自社の状況をはっきり伝えて経営者を巻き込み，そのうえで自助，共助，公助の取り組みを進めていくことが，安全なモビリティの実現に不可欠だと考えます．

（左から）　中島　和樹／ 高橋　秀行

本稿で紹介した内容や，取り組み内容に関して興味がある方は，お問い合わせください．

◆問い合わせ先

NTTセキュリティ・ジャパン
営業本部 マーケティング部
E-mail　nsj-pr @ security.ntt