［新たなモビリティ時代のサイバーセキュリティ―セキュリティによるジャパン・ブランドの向上に向けて―］

② 自動車分野の CASE 革命とサイバーセキュリティ

松原　豊 | 名古屋大学大学院情報学研究科　倉地　亮 | 名古屋大学大学院情報学研究科
高田広章 | 名古屋大学大学院情報学研究科

自動車のサイバーセキュリティ

多くの自動車には，先進運転支援システム（Advanced Driving Assistant System，ADAS）や車載インフォテインメントシステム（In-Vehicle Infotainment，IVI）が搭載され，車載ソフトウェアが大規模・複雑化している．開発効率化のために，汎用システムや IT 分野で用いられるソフトウェアが数多く使用されるようになってきている．一般に，大規模なソフトウェアにはバグ（不具合やセキュリティ上の脆弱性の総称）が存在する．ゲートウェイを介して，大規模なソフトウェアを搭載する機器と，車載制御ネットワークとが接続されると，車載制御システム自身の不具合だけでなく，そこに物理的に接続されるソフトウェアの問題も，自動車のセーフティに影響を及ぼす要因の１つになり得ると文献 1）で述べた．

自動車業界は CASE と呼ばれるキーワードを中心に，大きく変革していると言われている．CASE の主な対象範囲を図 -1 に示す．Connected の C は，自動車が，周辺の自動車（Vehicle to Vehicle，V2V），信号機や道路，料金所などの道路上のインフラストラクチャ（Vehicle to Infrastructure，V2I）などと繋がることで情報を共有し，新たなサービスを提供しようという考え方であり，V2X（Vehicle to X，X にはいろいろなモノが入る）と総称される．Autonomous の A は，自律的かつ自動的に動作することを意味し，高度な運転支援や自動運転によって事故ゼロを目指すという考え方である．Shared & Services の S は，人が移動したいと思ったときに，自由かつ柔軟に利用するモビリティ（自動車だけでなく，自転車，バス，電車，ライドシェアやレンタカーを含む移動体）を選択できるようにしようという考え方のもとで，複数名で自動車を共有すること，および共有を前提としたサービスを指す．Electric（電動化）の E は，自動車制御システムの構造において，電動化がさらに進むということを意味する．本稿では，自動車制御システムの変革を俯瞰した後，CASE のそれぞれの観点において，自動車セキュリティの課題や展開について述べる．

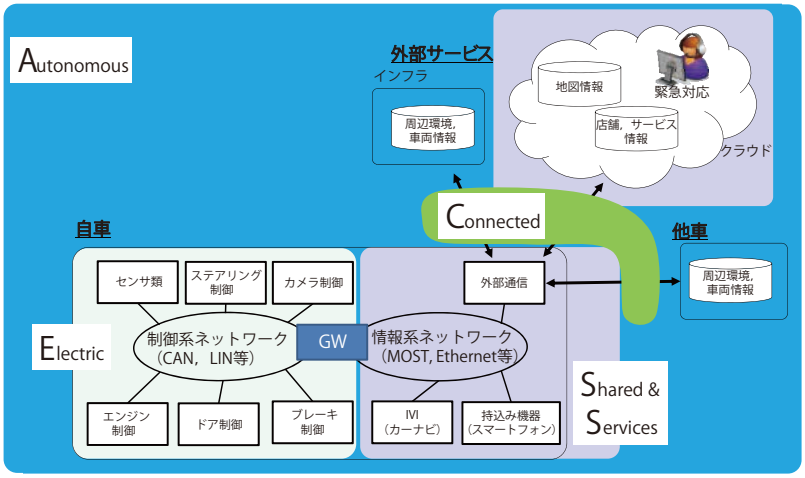
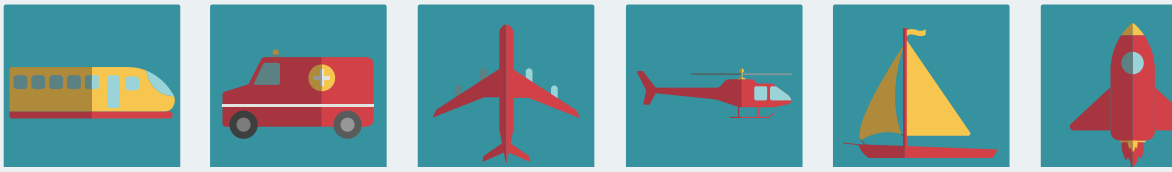


図 -1　CASE の主な対象範囲



CASE に向けた自動車の変革

CASE というキーワードを中心とする自動車の変革の中で，自動車にかかわる情報システムも大きく変わろうとしている．ここでは，車載組込みシステムに起こりつつある変化を，3 つの観点から述べる．

1 つ目の変化として，情報処理と制御の融合を挙げることができる．従来，自動車の制御系と，カーナビゲーションシステム（カーナビ）やカーテレマティクスなどの情報系との間は，疎な結合であった．特に，情報系からの情報を元に制御を行うことは，カーナビの情報を用いてトランスミッションを制御するなど，限定的な使途にとどまってきた．これが，自動運転では地図の活用が必須となり，V2X 通信で得られる情報を制御に活用することが増加していくと考えられる．必然的に，情報系の組込みシステムに要求されるディペンダビリティ，特に安全性やセキュリティに対する要求が，高まることになる．さらに，自動車を移動サービスを提供する手段の 1 つと捉えると，自動車全体が，クラウド上の情報システムから制御されることになる．

2 つ目の変化として，自動車の制御システムが，自律分散型から集中制御型へ変わろうとしていることを挙げることができる．自動車のコンピュータ制御は，個々の機構をコンピュータ制御することから始まった．最初にコンピュータ制御が導入されたのはエンジンであり，その後，ブレーキやステアリングなどもコンピュータ制御されるようになった．従来も，これらの個々の機構の制御システムは，車載ネットワーク経由で制御情報をやりとりして，高度な制御を自律分散的に実現していたが，全体を統括するのはあくまでも人（運転者）であった．

自動運転システムは，このような人の役割をコンピュータで置き換えようとするものであり，必然的に，集中制御的なアーキテクチャになる．自動車全体を統括制御するコンピュータは，ビークルコンピュータやセントラル ECU（Electronic Control Unit，車載の制御用コンピュータのこと）と呼ばれている．

このような集中制御型への変化は，自動運転車に限らず，起こりつつある．これは，自動車に搭載できるコンピュータの性能向上によりそれが可能になってきたことに加えて，次に述べる遠隔ソフトウェアアップデートの必要性も理由の 1 つになっている．数十個の車載の ECU のすべてを，遠隔アップデートに対応させるのは容易ではない．遠隔アップデートするソフトウェアがビークルコンピュータに集まっていれば，遠隔ソフトウェアアップデートは相当容易になる．

3 つ目の変化として，ソフトウェアアップデート，特に OTA (Over The Air) での遠隔ソフトウェアアップデートが必須と見なされるようになってきたことが挙げられる．従来も，販売店等で車載のソフトウェアをバージョンアップすることはあったが，基本的には，ソフトウェアに不具合があった場合の修正に限られていた．しかし，自動車をとりまく環境の変化が著しい現在では，必要な機能をすべて開発してから自動車を出荷するという考え方では，商品性が低いものとなってしまう．そこで，スマートフォンのように，自動車を出荷した後に新たなソフトウェアをインストールして機能を上げていくことが重要になってきている．また，サイバーセキュリティの面からも，脆弱性が発見された場合に迅速に修正するために，遠隔でのソフトウェアアップデートが必須と考えられる．もちろん，ソフトウェアアップデートの仕組みを用いてマルウェアが送り込まれる可能性は否定できず，諸刃の剣であることは言うまでもない．

これら 3 つのことから，自動車における情報システムやソフトウェアの重要性が高まっているということが言える．たとえば，フォルクスワーゲンは，ソフトウェア会社になるというメッセージを出している．また，Software-Defined Vehicle という用語が出てきたことも，このことを典型的に表している．

これらの変化から，車載組込みシステムに使われる要素技術にも，次のような変化が起きつつある．

まず，プロセッサについては，従来の車載制御システム向けのマイコンよりもはるかに高性能なものが適用されようとしている．それらの多くは，元々はモバイル機器やカーナビなどの情報処理システム向けに開発されたものである．

OS を含むソフトウェアプラットフォーム（SPF）については，車載制御システム向けには，AUTOSAR 仕様に準拠したものが広く使われつつある．従来の AUTOSAR 仕 様（AUTOSAR Classic Platform と呼ばれることになった）は，制御システム向けには適したものであるが，情報処理システム向けには要件が合致しない面があるため，新たに AUTOSAR Adaptive Platform と呼ばれる仕様の検討・開発が進んでいる．AUTOSAR Adaptive Platform では，OS には POSIX 準拠のものを使用している．

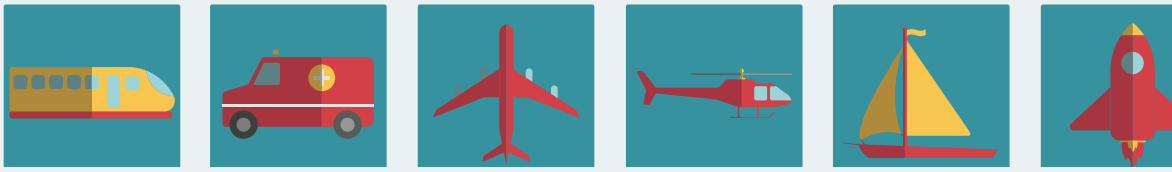
車載ネットワークについては，従来は CAN（Controller Area Network）や LIN（Local Interconnect Network）が広く使われてきたが，大容量のデータ転送が必要なところには，MOST（Media Oriented Systems Transport）に加えて，Ethernet を車載システムの要件に合致するように修正し，適用されようとしている．車載システム向けに Ethernet を修正した規格を，車載 Ethernet と総称している．

いずれの要素技術についても，IT 分野の技術が，必要な修正を加えつつ，車載組込みシステムに適用されようとしていると言うことができる．ただし，いずれにおいても，従来の車載組込みシステム向けの技術が使われなくなるというわけではない．

CONNECTED

近年，車両へさまざまなサービスを提供するために，インターネットにつながったり，高度道路交通システム（Intelligent Transport Systems，ITS）を活用することにより道路利用者の安全性の向上と環境負荷を減らすことを目的としたコネクテッドカーと呼ばれる車両が販売されている．コネクテッドサービスの実用例としては eCall が挙げられる．eCall は 2018 年より欧州で搭載が義務付けられた自動緊急通報システムのことであり，車両に搭載される GPS 座標を含む緊急通報を自動で発信することにより実現される．事故後に人が通報できない場合や通報の遅延による事故被害の拡大を防ぐことが期待されており，欧州だけでも毎年数千人の命が救われ，重傷者の数も低減できると試算されている．現在では，eCall の仕組みを利用して，車両の健全性を遠隔から監視する取り組みが欧州の車両メーカを中心に行われており，車両を車両外にある遠隔地のオペレーションセンタから監視する仕組みが整いつつある．

協調型 ITS（Cooperative ITS, C-ITS）は，車車間通信（V2V）および路車間通信（V2I）における無線通信をベースとする技術である．C-ITS アプリケーションは，道路上の警告や交通情報を運転手に提供し，その後で自律的に自動車を制御することを目的とする ITS アプリケーションである．より具体的な例として，車両同士が通信することにより，隊列走行や高速道路での合流調停を行う．C-ITS アプリケーションの効果として，交通流の効率化が期待されている．さらには，物流トラックや長距離バス等を隊列走行させることにより運転者に対する運転負荷を低減するなどの効果が期待されている．C-ITS には多くの利便性がある一方で，関連する無線通信に対してセキュリティとプライバシを担保しなければ，普及が危ぶまれる可能性があることが指摘されている．たとえば，救急車や警察車両のような緊急車両になりすまして他車両の走行を妨害できてしまうと，道路の利用効率が低減する可能性がある．このため，V2X 通信では送信されたメッセージの正当性を各車両で判断することが要求される．V2X 通信を保護するためには暗号技術が必須であり，車両や路側機などの ITS ステーションの証明書の管理のために公開鍵基盤を利用することが想定されている．このような技術によって，機密性や完全性の保証，なりすまし防止，否認防止を実現



することが想定されている．

V2X 通信の代表的な公開鍵基盤には，米国運輸省（U.S. Department of Transportation，USDOT）の SCMS（Security Credential Management System）と，欧州標準化委員会（Comité Européen de Normalisation，CEN）の後ろ盾の基で，ETSI（European Telecommunications Standards Institute）が開発している C-ITS Trust Model の 2 つがある．これら 2 つの規格には，V2X 通信の信頼の起点となる証明書の発行の仕組みや失効手順等に違いがある．このため，2 つの規格の Harmonization（調和）が検討されている．

もう 1 つの考慮するべき重要な問題は，ユーザのプライバシである．自動車の場合，車両の位置情報を長期に渡り追跡されることにより，運転手や乗員のプライバシが漏洩するという課題がある．このため，車両の位置情報を追跡できないように匿名化された識別子を割り当てることにより，長期にわたる追跡から保護することが検討されている．

また，C2C-CC（CAR 2 CAR Communication Consortium）では，TAL（Trust Assurance Level）と呼ばれる ITS ステーションの信頼性レベルを定義しており，V2X 通信を通じて他車両に影響を与えることができるのは，高い信頼性レベルで開発された車両であることが規定されている．

AUTONOMOUS

自動運転に関するセーフティとセキュリティについては，自動運転車が搭載するシステムの自動運転レベル（安全に関する責任の範囲），サービス（車両の利用形態），想定運行範囲，外部との連携範囲，システムのアーキテクチャ（構造）などが多種多様であることから，一般的に議論するのは難しい．国際的な議論の場である自動車基準調和世界フォーラム（WP29）での議論[2]や，国内でのガイドライン[3]でも，自動運転のセーフティやセキュリティの重要性は明記されているものの，具体的な方法論や対策については，現在進められている国際規格や標準での議論に委ねられている．

車両に搭載される自動運転システムは，主に，センサによって周辺環境や自車両位置を認知する機能，自車両位置から目標位置への運行，軌道を計画する判断機能，アクチュエータの制御機能の 3 機能で構成される．認知機能と判断機能は，従来はドライバが担ってきたが，自動運転レベル 1 ～ 2 ではそれらの一部が，3 ～ 5 では，条件や制限が存在する場合もあるが，全機能がシステムによって実現される．自動運転レベル 3 以上になると，システムによって予見可能ないしは回避可能な人身事故が発生してはならないという方針が検討されている[2, 3]．セキュリティの観点では，自動運転システムによる予見（認知機能と判断機能）と回避（判断機能と制御機能）に影響する攻撃に対しては，セーフティを確保する上で特に対策が必要と考えられる．

認知機能は，センサが認識した情報を統合して，自車両の周辺状況や自車両位置を認知し，判断機能が利用する情報を集約する．特に，センサが認識した情報や，地図情報などの完全性と可用性が重要となる（個人情報やプライバシの観点では機密性も必要になってくる）．センサ類は，GNSS（Global Navigation Satellite System），IMU（Inertial Measurement Unit），Lidar（Light Detection and Ranging），単眼／複眼カメラなど多様であるが，基本的には，物理現象をアナログ信号として捉え，それをディジタル信号に変換してコンピュータで扱えるようにする装置である．

センサに対するセキュリティの脅威について，近年数多くの研究論文が発表されている．センサに対して妨害信号を送信することで，システムが誤認識するような攻撃や，カメラによる画像に対して，ディープラーニングを含む機械学習による物体認識機能の性能限界をつく攻撃が報告されている．単一のセンサに対する攻撃は，確かに脅威であるが，安全性にどう影響するかは，自動運転システムの構成，制御アルゴリズムなど，内部構造に大きく依存する．現

在検討されている自動運転システムには，複数種類のセンサを組み合わせて状況や物体認識する技術（センサフュージョンと呼ばれる）を導入しているものが多い．センサフュージョンにおいて，不確実性のある情報，もしくは意図的に改ざんされた情報が含まれることを想定して対応できれば，センサ単体に対する攻撃の影響は限定的であろう．しかし，たとえば，地図情報や時刻情報などは，完全性や可用性が失われると，判断機能や制御機能に直接的に影響を及ぼす可能性が高い．

このように，自動運転では，従来の自動車と比べて，制御に悪影響を及ぼし得る攻撃の経路，境界（アタックサーフェス）が急激に増加する．安全分析やセキュリティ脅威分析によって，単一の故障もしくは攻撃によって安全に影響を及ぼし得るポイントを列挙して対策することが非常に重要となる．車両だけでなく，自動運転に関係する周辺装置である，クラウドサーバ，インフラセンサの機能が安全性に影響を及ぼすアーキテクチャも考え得る．たとえば，クラウド上の地図データ，OTA による更新用制御プログラム，道路信号情報などが侵害された場合に，安全性への影響が懸念される．車両だけでなく，サービスレベルから俯瞰し，包括的に対策する視点が必要となる．

SHARED AND SERVICES

それぞれの人が１台の自動車を所有し，自動車のみで最短経路で移動しようとする考え方から，複数の利用者によって自動車を共有することで社会や地域において最適な移動手段を実現しよう（もちろん，個人レベルでも自動車保有コストを下げられる場合もある）とする新しい考え方が登場している．具体的なサービスとしては，フィンランド発の Whim，スウェーデン発の UbiGO，米国ロサンゼルス発の GoLA などがある．この変化をセーフティとセキュリティの観点で考えると，個人最適化から，個人レベルのセキュリティを確保しながら社会最適化への移行であると捉えることができる．

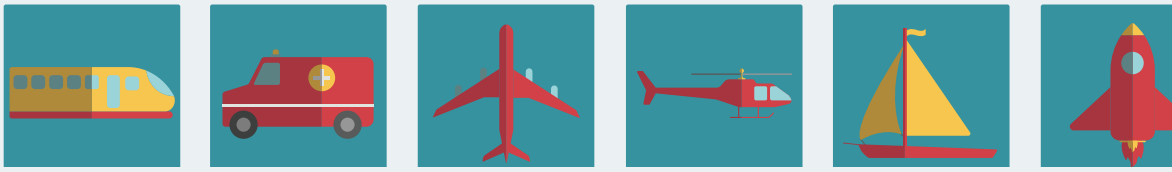
１台のモビリティが不特定多数の利用者によって共同利用されるようになると，内在する資産が侵害される可能性を考える必要が出てくる．

ここでは，自動車に限定して考えてみたい．自動車を専有する場合には，鍵によって利用者を制限できているので，車内の空間は信頼できる空間であるという前提を置くことができた．もちろん，車上荒らしやキーの電波を不正に増幅させるリレー攻撃などの不正行為が実際に発生しているので，物理的なセキュリティに対する考慮は必要である．

シェアリングサービスは，時分割によって車内が共有されるということなので，自身が利用する時間の前後は車内が信頼できない空間となる．車内に置かれた物理的なモノだけでなく，たとえば，料金の支払いに関する情報，ETC カード情報，カーナビに登録した走行データや検索履歴，外部サービスの利用履歴，ドライブレコーダに記録された車内外の動画，音声といった個人情報，プライベート情報などの情報資産が侵害される可能性が出てくる．したがって，これらを守るためには，利用者が切り替わるタイミングで，車内の状況（設備や搭載機器などの物理的なものも含む）や情報を利用前の状態に戻しておくのが基本的な考え方である．情報に関しては，利用者の情報を消去するのではなく，保護・管理できる仕組みを構築することで利便性とセキュリティを確保できる可能性もある．たとえば，ネットワーク網を活用して，クラウドやスマートフォンと連携することで，利用者に関する情報を，利用の前後で自動的に保存，復帰することも可能であろう．いずれにしても，シェアリングサービスでは，利用者の登録と認証が厳格になされ，利用者の真正性や否認防止といった性質の保証が特に重要となってくる．

ELECTRIC

近年，さまざまな自動車メーカからさまざまな電



気自動車（Electric Vehicle, EV）や PHEV（Plug-in Hybrid EV）が販売されている．EV の普及のためには，充電システムやその通信方式の国際標準化が必須である．国や地域で電力の供給方式に違いが存在するものの，共通する充電コネクタや通信プロトコル等を定義することにより EV の車両側に搭載する充電制御システムの共通化を実現することが目されている．

充電通信規格に関する国際標準規格として，欧州や北米の自動車メーカを中心に，ISO/IEC 15118 が策定されている．ISO/IEC 15118 の規格名は「Vehicle to Grid - Communication Interface」である．ISO/IEC 15118 では，車両と充電ステーションの間の通信から，EV を V2G（Vehicle 2 Grid）と呼ばれる電力網に接続することまでを想定している．この充電通信規格では，EV が供給された電力量に対する料金を支払ったり，V2G に接続する EV が他車両に電力を融通する代わりに売電分の金銭を受け取ることが想定されている．このため，従来の車両とは異なり，充電スタンドになりすまし EV 車両から金銭を搾取したり，充電量をごまかして充電料金を踏み倒す等の新たな脅威にさらされる可能性がある．さらには，充電に関する使用履歴が漏洩するとプライバシの問題につながるなどの懸念がある．

一方で，EV 車両だけでは対策ができないため，充電スタンドなどの機器に対してもセキュリティ強化が要求されている．このため，ISO/IEC 15118 では，必要なレベルの機密性を定義し，交換されるデータの整合性と信頼性の両方を検証するためのアルゴリズムを定義している．さらに，データの整合性と信頼性や否認防止を検証するために，秘密鍵と公開鍵で構成される鍵ペアを使用し，機器認証を実施した上で暗号通信が行われることが想定されている．

今後の展望

CASE 革命の到来とともに，自動車関連企業にとっては，自動車市場の競争が激化しており，新たな機能，サービスを先行して市場に投入するスピード感と柔軟性も必要となっている．その一方で，自動車のセキュリティに関する取り組みの重要性が増している．自動車に適した開発プロセスだけでなく，運用・保守を含むライフサイクル全体の業界標準，セキュリティ対策技術などの整備が急がれる．

自動運転や V2X の普及に向けて，自動車が IoT 化している．IoT ではサービス全体の一部として車両を捉えるので，車両単体でのセーフティやセキュリティを議論するだけでは，利用者や歩行者等の安心を実現することはできない．サービスレベルもしくは社会レベルで自動車と向き合い，どのようなサービスを受容するのか，しないのかを社会全体で議論することが重要である．自動車を活用した新たなサービスを長期的に運用することは，複雑な社会技術システムを運用することにほかならない．開発段階では想定できなかったセーフティおよびセキュリティに関するリスクが将来見つかることを想定し，サービスのライフサイクルを管理する仕組みを構築した上で，そのディペンダビリティやレジリエンス性を社会全体で継続的に議論し，評価すべきである．

参考文献

1) 松原　豊，倉地　亮，高田広章：自動車分野のセーフティとセキュリティの動向と展望，情報処理，Vol.58, No.11 (Nov. 2017).
2) Framework document on automated/autonomous vehicles, WP.29-177-19 (2019).
3) 国土交通省自動車局：自動運転車の安全技術ガイドライン（2018）.

（2019 年 10 月 30 日受付）

松原　豊（正会員） yutaka@ertl.jp
名古屋大学大学院情報学研究科准教授．リアルタイム OS，ネットワーク技術，安全技術，セキュリティ等の研究に従事．博士（情報科学）．

倉地　亮（正会員） kurachi@nces.i.nagoya-u.ac.jp
名古屋大学大学院情報学研究科附属組込みシステム研究センター特任准教授．リアルタイムスケジューリング理論，車載制御システムの設計技術等の研究に従事．博士（情報科学）．

高田広章（正会員） hiro@ertl.jp
名古屋大学未来社会創造機構教授．同大学院情報学研究科教授・附属組込みシステム研究センター長を兼務．APTJ（株）代表取締役会長兼 CTO．リアルタイム OS，リアルタイムスケジューリング理論，組込みシステム開発技術等の研究に従事．博士（理学）．