❸ 自動車分野のセーフティとセキュリティの動向と展望―自律走行の実現に向けて―

松原　豊　倉地　亮　高田広章（名古屋大学大学院情報学研究科）

自動車制御システムの発展経緯

自動車の制御システムは，軽量化や，排ガス規制に対応するため，機械式の制御から，コンピュータを中心とする電子制御へと発展してきた．近年の自動車には，電子制御装置（Electronic Control Unit（ECU））と呼ばれる制御コンピュータが，高級車の場合で 100 個近く搭載されている．センサ，カメラ，モータ，ハンドル，エンジンやブレーキなどの機器と ECU 間は，ハーネスと呼ばれる通信ケーブルによって接続され，車載制御ネットワークを構成している．

より安全で快適な運転環境を実現するため，最近の自動車には，さまざまな先進運転支援システム（Advanced Driving Assistant System（ADAS））が搭載されている．たとえば，運転者が指定した車速を維持しつつ，前方の走行車を検出した場合には，その先行車との距離を適正に維持して追従するアダプティブ・クルーズ・コントロール（Adaptive Cruise Control（ACC））や，走行車線を維持するようハンドル操作を支援するレーン・キープ・アシストシステム（Lane Keeping Assist System（LKAS））などが搭載され，複数の ECU が互いに通信しながら，アクセルやブレーキ，ハンドルを連動することで，高度な制御を実現している．車載制御ネットワークの通信プロトコルとしては，Controller Area Network（CAN）や Local Interconnect Network（LIN）が事実上の標準となっている．一部の高級車には，通信帯域のより広い，FlexRay や Ethernet が導入されている．

現在のほとんどの自動車には，車載インフォテイメントシステム（In Vehicle Infotainment（IVI））が搭載されている．IVI の役割は，道案内や，ラジオ，テレビ，CD や DVD などのメディア再生機能が主機能であったが，最近では，道路交通サービスからの最新情報の受信，運転者の携帯電話を始めとする持込機器との連携機能，好みのアプリケーションをインストールして多様なサービスを楽しむアプリケーション実行機能を備えている．一部の自動車では，インターネット，自動車メーカによる顧客サービスや，ほかの外部サービスと接続するための外部通信ユニットも搭載されている．高機能化に伴い，IVI には，サーバや汎用 PC 向けの Linux を組込み機器向けにカスタマイズした組込み Linux や，スマートフォンで使用される Android など，IT 分野で広く利用されている（と同時に，セキュリティの脆弱性が数多く報告されている）OS やソフトウェアが採用されることが多い．IVI や持込機器のサービスが，自動車の走行速度，走行距離，アクセルやブレーキの操作情報などの制御に関する情報を使用する場合，これらの機器と車載制御ネットワークが直接，もしくはゲートウェイを介して間接的に接続される．このことが，自動車のセーフティを脅かすセキュリティの問題の根本原因となっている．

自動車のセーフティ

自動車の安全技術

現在の自動車のセーフティ確保に関する考え方や規制は，その自動車が販売，使用される国によって異なるが，基本的には，自動車メーカごとに販売先国の規制，ルールに基づいた上で，独自の安全対策

と品質管理のもとで販売されている．安全技術を大きく分類すると，事故を未然に防止するための予防安全技術と，事故が発生した後の搭乗者や歩行者等の被害を軽減するための衝突安全技術に大別される．予防安全技術の例としては，ACC や LKAS，自動ブレーキ等が該当する．一方，衝突安全技術としては，シートベルト，エアバッグ，フレームの物理的構造の工夫等が挙げられる．

予防安全技術は，危険を予測し，事故を回避・予防する技術であり，これまでは運転者（人間）の能力に頼った上で，それを支援する面が強かったが，センサやカメラと，制御システム（アクセル，ブレーキ，ハンドル等の制御）をコンピュータによって連動させる技術が市場に投入されている．たとえば，自動ブレーキシステムは，前方の障害物をセンサ，カメラ，レーダ等で検知し，障害物に衝突するおそれがある場合に運転者へ回避操作を行うよう警報し，さらに障害物との衝突が避けきれないと判断した場合には，自動的にブレーキ制御を行う．衝突事故を防ぐ安全機能として有効である一方で，当然ながら 100% 事故を防止できるわけではない．加えて，似たような機能であっても，採用している技術や仕組みが異なる場合には，障害物検知の精度，作動条件，ブレーキ性能が異なるので，うまく活用するためには，運転者が実際に動作を経験することが重要である．

衝突安全技術は，事故が起きた場合でも搭乗者や歩行者への物理的な影響を軽減するために，（コンピュータによる制御が行われるものもあるが）主に機械的な装置，工夫によって実現される．国や第三者機関による安全性能評価の対象になっており（日本では国土交通省および（独）自動車事故対策機構が実施），これらの観点における国内の自動車メーカのセーフティは，これまで世界でも最高レベルであることが示されてきた．最近では，ボルボ社やスバル社が，衝突時の歩行者への衝撃を軽減するために，歩行者用エアバッグを搭載した自動車を市場に投入している．

セーフティ確保の基本的な考え方

セーフティに関する国際規格 ISO/IEC Guide 51 では，セーフティ侵害のリスクを低減する方策として，設計時には，(1) 本質的な安全設計，(2) 保護装置，(3) 使用に関する情報提供の 3 ステップで，使用時には，使用者による追加保護装置やトレーニング等で対策するべきであるとの指針がある．この観点から，これまでの自動車安全技術は，(1) と (2) を考慮した上で，（運転免許証を持つという意味で）一定レベル以上にトレーニングされた運転者に対して情報提供することで，全体としてセーフティ侵害のリスクを低減しようと試みてきたといえる．加えて，最近の ADAS は，従来 (3) や運転者に頼っていた領域を小さくし，(2) の範囲を広め，全体としてリスクをより低減する傾向であると捉えることができる．

安全システムの開発プロセス

自動車制御システムに，電子制御システムやコンピュータが使用されるようになると，電子装置やソフトウェアの誤動作が自動車全体のセーフティに影響するようになった（自動車の安全に影響を及ぼし得るシステムを安全関連システムと呼ぶ）．2000 年代以前から，欧州を中心に，コンピュータを搭載した安全関連システムのリスク分析・評価，開発プロセス，セーフティが確保されていることの説明等の方法や作成文書の規格化が議論されてきた．電気・電子・プログラマブルシステムの機能安全に関する国際規格 IEC 61508 をベースとする自動車分野規格 ISO 26262 の第 1 版が 2011 年に発行された．自動車メーカや部品サプライヤにて対応が進められた結果，セーフティに関係する電子制御システムにおいて不具合が発生したとしても，安全対策を追加することによって，自動車のセーフティを確保しようとする機能安全の考え方が普及している（表 -1 の左側を参照）．

	セーフティ	セキュリティ
対象範囲	• 開発対象のシステムのみ • 安全関連システムの系統的・物理的な故障への対策 • 非安全関連システムから安全関連システムへ影響防止	• 開発対象のシステム＋つながるシステム • 対象システムの脆弱性に対する意図的な攻撃への対策
前提	• 利用者，開発者，第三者は信用できる（可能な限り，リスクを低減するよう行動する）	• 利用者，開発者，第三者は何らかの意図を持って行動する（脅威となる）場合がある
基本的な考え方	• 本質的な安全設計，機能安全，使用者への情報提供の順で対策検討 • 故障検出時にシステムを安全状態に遷移，維持するフェイルセーフが基本 • フェイルセーフが有効でない場合には，冗長系で信頼性を高める	• システムのセキュア状態は存在しない • 脅威はなくならない．むしろ，時代とともに増加すると考えるべき • 想定される脅威，脆弱性に，開発段階で可能な限り対策 • 運用段階でも，対策の追加，修正を継続
対策への要求レベル指標	• SIL（Safety Integrity Level）	• SAL（Security Assurance Level） • TAL（Trust Assurance Level）
規格・ガイドライン	• ISO/IEC Guide 51 を筆頭に，グループ規格 IEC 61508，分野ごとの規格（自動車の場合は，ISO 26262）が整い，それぞれ改訂されている	• 情報セキュリティに関しては普及段階にある（たとえば ISO 15408） • 自動車に関しては，JASO 自動車の情報セキュリティ分析ガイド，SAE J3061 等

表 -1　セーフティとセキュリティの違い（規格やガイドラインにおける考え方の観点から）

自動車のセキュリティ

セキュリティの脅威

自動車セキュリティの脅威は，主に，制御システムに対して何らかの意図的な攻撃がなされた場合に自動車の制御が奪われてしまう，もしくは運転者の意図が無効化されてしまうという，制御システムの機能の完全性と可用性が侵害されてしまう脅威と，自動車内のコンピュータが有する情報（制御に用いる情報，自動車や運転者を特定できる個人情報，自動車の走行履歴や行動を把握できる個人情報・プライバシ情報等）の機密性，完全性，可用性が侵害されてしまう脅威に大別される．

前者の脅威としては，セーフティを担うソフトウェアに対して，車載制御ネットワーク経由でなりすましメッセージを送信する攻撃や，ECU のソフトウェアを不正なものに書き換える攻撃などが 2010 年頃から報告されている．2013 年 C. Valasek らは，フォード社のエスケープとトヨタ社のプリウスに対して，車内の制御ネットワークに CAN メッセージを流すことで，ブレーキの無効化や，運転手が意図しないステアリング操作など，制御を乗っ取ることができることを示した．2015 年と 2016 年の DEF CON（セキュリティに関する講演やイベントが多数開催される国際会議）では，C. Miller らが，ジープ社のチェロキーに対して携帯電話網を通じて，ECU のファームウェアを書き換えた上，自動車の操舵を完全に遠隔から実行した事例が報告された．この結果，脆弱性を持つ自動車に対してリコールが発生し，自動車メーカが責任をとる事態となった．最近では，高度な運転支援機能を持つ自動車のセンサを対象とする物理的な攻撃の事例も報告されている．2016 年の DEF CON では，J. Liu らの研究グループが，テスラ社の電気自動車に搭載される物体検出用レーザセンサに対して，自動車の前方から妨害電波を送り，物体の検出状態を意図的に操作できる事例も報告されている．

後者の脅威は，米国 E. J. Markey 上院議員によって 2013 年に実施された，自動車メーカ 20 社に対するセキュリティ対策などに関する質問状，およびその報告書にて，ある程度明らかになっている [1]．具体的には，IVI に保存されている走行情報，運転者情報等の管理方法には，統一的な管理ポリシーやルールがなく，情報の保存期間や使用用途が情報取得者（アプリケーション）によって異なっていることに加えて，情報収集に関して利用者に対して十分に通知されていないことが指摘された．現在，自動車メーカ 12 社で構成される Auto Alliance（Alliance of Automobile Manufacturers）において，重要項目の 1 つとして議論されている．

自動車のセキュリティの課題

自動車特有のセキュリティの課題として，主に以下が存在する．

(I) 製品の利用期間が長く，車種や利用範囲が多様であるため，開発時の想定が困難であること

国内の自動車の利用期間は，年々長期化しており，2016 年 3 月末の乗用車（軽自動車を除く）の平均使用年数は 12.76 年である．自動車に対するセキュリティの脅威は，年々増加すると考えると，開発する自動車に対する脅威をどのように想定して，対策するべきかという課題がある．

(II) 複数領域の脅威や脆弱性の多角的かつ網羅的な分析が困難であること

安全系，ボディ制御系，マルチメディア系など，複数の領域で構成される複雑な自動車制御システムを対象に，横断的，多角的に分析する標準的な手法がない．安全分析やセキュリティ分析のための手法はこれまで数多く提案されており，我々も具体的な攻撃手順ををキーワードとしてリスク分析を支援する手法である HAZard and OPerability study（HAZOP）ベースの脅威分析手法を提案している [2]．今後は，複数の分析手法を組み合わせ，セーフティとセキュリティを同時に分析する方法や，つながるクルマや自動走行システムなど複数の機能やサービスが連携する複雑なシステムを対象とする分析手法を研究する必要がある．

(III) 計算機リソースやコストに制約があるため，対策に適用できる技術に制限があること

自動車では，すべての ECU にセキュリティ対策を入れることは，システムが複雑化するだけでなく，マイコン性能やメモリ容量の増加につながるため，コスト制約の観点からも難しい．加えて，ネットワーク帯域も限られているので，IT の世界で使用されている技術（たとえば，暗号化，鍵交換，TLS/SSL など）をそのまま利用するのが難しい場合もある．性能の限られるコンピュータやネットワークで，コスト効率の高いセキュリティ対策技術が求められる．

(IV) セキュリティ対策基準がないこと

自動車セキュリティの何をどこまで対応するべきかという基準が存在していない．IEC 61508 第 2 版，改訂が進められている ISO/DIS 26262 第 2 版や，北米を中心とする技術者団体 SAE（Society of Automotive Engineers）のガイドブック J3061 においても，セキュリティ対策の基準については言及されていない．現在，自動車のセキュリティ対策基準や，セーフティとセキュリティを両立するための規格やガイドラインの検討が進んでいる．

車載ネットワークに関するセキュリティ対策技術

表 -1 でも示したように，自動車に関するセキュリティ対策を規定した標準規格は存在しておらず，各所で標準化案やガイドラインが検討されている段階である．欧州を中心とする自動車のソフトウェアプラットフォームを標準化する AUTomotive Open System ARchitecture（AUTOSAR）では，2014 年に Secure Onboard Communication 仕様（SecOC）が発行された．この仕様の中では，ペイロードが 8 バイトしかない CAN メッセージに対して，なりすましと改ざんを検出する Message Authentication Code（MAC）の一部のみを付与する手法が提案されている．MAC を切り詰めることで攻撃者のランダム攻撃により高々 1 回のなりすましが成功する場合はあるものの，攻撃者が連続してなりすましを成功させることは難しい．自動車の制御システムでは値が急激に変化する場合には，同値の信号を複数回連続して受信しないと制御を実行しないなどのポリシーで設計されていることが多く，切り詰めた MAC を用いることでも連続して攻撃を成功させることが難しいため，自動車の設計ポリシーに適したセキュリティ技術といえる．

研究レベルでは，CAN コントローラを改造することにより，なりすましメッセージを防ぐための手法がいくつか提案されている [3),4)]．これらの技術は，ハードウェアを改造するのみで ECU の制御やソフトウェアを大きく変更する必要がないため，既存する電子制御システムへの適用が容易などのメリットがある．

自律走行に向けたセーフティとセキュリティの課題

セーフティに関する課題

SAE が発表している自動運転車の自動化レベルに関する標準規格 J3016 では，自動運転レベルを 5 段階に分類している．普及段階にある ADAS は，人間が走行状況を監視し，運転作業をしている中で，一部の走行を支援するというレベル 1 にとどまっている．最近では日産自動車社やアウディ社から，運転作業におけるシステムの担う範囲が拡大し，人間の監視のもとで一部の走行作業を担う（レベル 2），人間が走行状況を監視することなく，システムが要求した場合にのみ人間が運転作業をする（レベル 3）が発表された．走行状況の監視，すべての運転作業をシステムが行う（レベル 4, 5）といった自動車は，まだ研究開発段階であるが，近い将来，市場に登場してくる可能性がある．このような状況を踏まえると，今後も自動車制御システムの大規模化・複雑化が進むと予想される．

自律走行車におけるセーフティは，レベル 3 の自律走行では，条件は付くものの，ISO/IEC Guide 51 における安全確保の考え方の（1）と（2）の範囲でできる限りリスクを低減し，最終的にシステムが運転者に依頼（システムが状況判断できない，もしくは動作できないことが想定されていると思われる）した場合にのみ，（3）に頼るという位置付けである．レベル 4 以上では，基本的には運転者に頼ることなく，システムが運転者の代替としてセーフティを確保することが求められる．

予防安全技術において，安全の責任を，運転者から制御システムに移行する際の 2 つの課題を考えてみる．従来のレベル 2 までは，危険（事故の発生）が予測できた際には，まず運転者に通知し，運転者自身がブレーキを踏む，ハンドルを切る等の動作を取る．それでも危険が回避できそうにない場合にはシステムが介在してできる限りの動作をするというものであった．それに対して，レベル 3 以上では，安全の責任が基本的には制御システムが担うことになるので，走行中に危険を検出した場合の行動として，アクセルを切ってブレーキを効かせて止めればよいのか，ハンドルを切って走行経路を変えればよいのか，停止した後にいつ走行を再開すればよいのかなどの判断を制御システムが担うことになる．この判断をどのように正確かつ安全に実行するかという課題がある．

2 つ目の課題は，自動車の部品や制御システムに故障が発生した場合，従来では運転者に対して，フロントパネルで通知してディーラや修理場に移動するという動作を，どこまで制御システムが担うかということである．レベル 3 では，運転者に運転を依頼することも許されるが，レベル 4 では，故障発生後も，（機能や性能を限定した上でも構わないので）継続して走行するフェールオペレーショナルが求められる．現実的には，（人間が運転していたとしても）継続走行が困難な場合もあるので，制御システムと運転者の責任範囲を明確化して運用することも有効であろう．セーフティにおいて重要なことは，責任と，制御の権限の所在が一致することである．人間が責任を持つ場合は人間の運転操作の優先度，権限を高くするべきであるし，一方，制御システムが責任を持つ場合には，走行操作の権限はシステムを高優先度とする．これが正しく設計されないと，人間とシステムの意図が錯綜し，事故を招くリスクが生まれる．

現在の機能安全規格 ISO 26262 では，安全関連システムに故障が発生した際には，安全状態に移行して，その状態を維持すること（フェイルセーフ）を基本としている．今後は，故障が発生した場合でも，機能を減らす，もしくは限定して処理を継続すること（フェイルオペラブル）の考え方が必要になってくる．また，ADAS に使用されるセンサが故障していなくても，その性能限界やアルゴリズム等によってもセーフティが損なわれる状況を想定した Safety of the Intended Functionality（SOTIF）の議論が進んでいる．

セキュリティに関する課題

前節で述べたように，複雑化・高度化する自動車制御システムに対して，継続して，従来のセキュリティ脅威に対策する必要がある．加えて，自動車の自律走行技術が発展して，運転者の負担が減る，もしくは運転者自身が存在しないという状況になると，自動車が，個人の移動手段ではなく，共用移動手段となる場面が増えてくる．この変化は，セキュリティの観点で大きな違いがある．すなわち，自動車の所有者（もしくは親しい人間）が運転することが想定できる場合には，運転者はリスクを低減するよう行動するという前提を置けるのに対して，悪意のある運転者が，容易に，物理的に車両へアクセスできることを想定する場合には，自動車内の IVI，ECU やネットワークへの物理的な攻撃が一気に容易になる．

運転支援や自動走行において，複数の自動車間（車車間）や，自動車と路面上の機器間（路車間）での通信が出てくると，他の自動車や機器から得られた情報をどれだけ信じてよいかを考える必要がある．信頼できる自動車からの情報を優先して使いたい，あるいは，信用できない自動車からの情報を使いたくないなどのユースケースが想定される．Car 2 Car Communication Consortium（C2C-CC）では，車車間および路車間通信におけるセキュリティについて議論されており，信用保証レベル（Trusted Assurance Level（TAL））を定義し，レベルごとのセキュリティ要件を定義している．この TAL のコンセプトは，各自動車の信用保証レベルの必要性を訴えるものであり，さまざまな自動車や設備が混在する状況で，効率的に自動走行を実現するためには重要な考え方である．

セーフティとセキュリティの今後の展望

自動車のセキュリティに関する取組みは，まだ始まったばかりであり，自動車に適した開発プロセス，運用・保守，業界基準，セキュリティ対策技術などの整備が期待されている．特に，自動車のセーフティを侵害するサイバー攻撃に対して早急に対策する必要があり，より快適で安全な自動車の開発が期待されている．

自動走行技術への期待や IoT 化の流れによって，自動車を取り巻く環境は大きく変わりつつある．あらかじめ想定した，人やモノだけを繋げることができる閉じた環境（クローズドシステム）だけでなく，さまざまな人やモノ，サービスが自由に繋がる開かれた環境（オープンシステム）を前提とするパラダイムシフトが起きつつある．このような複雑なシステムを社会で運用する上で，開発段階では想定できない，セーフティおよびセキュリティに関するリスクが見つかることを受け入れた上で，どのような開発プロセス，製品ライフサイクルを構築していくべきかという広く長い視点での議論を始める時期が迫っているように思われる．

参考文献

1) Markey, E. J. : Tracking & Hacking : Security & Privacy Gaps Put American Drivers at Risk (2015).
2) Wei, J., Matsubara, Y. and Takada, H. : A Security Analysis Method Using Attack-oriented Guidewords for Embedded Systems, Springer Recent Advances in Systems Safety and Security (2016).
3) 畑　正人，田邉正人，吉岡克成，大石和臣，松本　勉：不正送信防止：CAN ではそれが可能である，Computer Security Symposium 2011(CSS2011) (2011).
4) Kurachi, R., Matsubara, Y., Takada, H., Adachi, N., Miyashita, Y. and Horihata, S. : CaCAN - Centralized Authentication System in CAN, Proceedings of the Escar 2014 Europe Conference (2014).

（2017 年 8 月 22 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附属組込みシステム研究センター助教．組込みシステム向けのリアルタイム 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）．