# 車載機器のセキュリティと安全性

応般

倉地 亮　松原 豊　高田 広章（名古屋大学大学院情報科学研究科）

## 自動車とサイバーセキュリティ

近年，自動車に対するセキュリティの脅威事例が多数報告されている．2015 年には，乗員の安全性を侵害する脆弱性を持つ自動車がリコールとなるなど，自動車のセキュリティ対策が早急に求められている．特に，自動車の安全性を侵害する脅威については，自動車業界団体を中心に対策技術が検討されているが，自動車の電子制御システムは，今後ますます発展することが予想されていることと，自動車特有の脅威やリスクが存在することを考えると，安全性とセキュリティを両立するためには，非常に多くの課題がある．

本稿では，自動車の電子制御システムの発展経緯を踏まえ，自動車のセキュリティの現状と今後取り組むべき課題について概説する．

### 車載電子制御システムの発展

自動車の電子制御システムは，一般に車載電子制御システムと呼ばれ，Electronic Control Unit（ECU）と呼ばれる電子制御装置が互いに通信することで制御を実現する分散制御システムである．ECU 間の通信ネットワークは車載制御ネットワークと呼ばれ，Controller Area Network（CAN）と呼ばれる通信プロトコルが多くの自動車で採用されており，事実上の標準となっている．

より快適な運転環境を実現するために，近年の自動車は自動ブレーキや前車追従などの高度な運転支援を行う先進運転支援（Advanced Driving Assistant System（ADAS））が搭載されつつある．また，インフラ（道路やロードサイドユニット）やクラウドなどのネットワークに自動車を接続する“つながるクルマ”を実現することで，より快適で安全な運転環境を実現することが検討されている．将来的に，自動走行（automated driving）や自律運転（autonomous driving）が普及することを考えると，今後ますます電子制御システムの大規模化・複雑化が進むと予想される．

### 自動車の安全性とセキュリティ

自動車が電子化される中で，電子制御システムが自動車の安全性に大きな影響を及ぼすようになった．電子制御システムが提供する機能によって，自動車の安全性を確保する機能安全の考え方が普及している．この流れを受けて，自動車業界では，自動車の電気・電子システムの機能安全に関する国際規格 ISO 26262 への対応が進められてきた．現在の ISO 26262 では，電子制御システムの故障による安全性への影響は考慮されているが，セキュリティの脅威による安全性の侵害については考慮されていない．しかし，サイバー攻撃による自動車への影響と，故障による自動車への影響が同じ場合には，安全対策がセキュリティ対策としても有効に働く可能性がある．このため，**表 -1** に示すように安全性とセキュリティでは対象範囲や考え方に違いがあるものの，安全対策のみでは不十分な個所に，セキュリティ対策を効果的に組み合わせることで，自動車の安全性とセキュリティを両立することが求められている．

## 自動車セキュリティの現状

### セキュリティ脅威の事例

近年，自動車のセキュリティに対する脅威事例が多数報告されている．特に深刻なセキュリティ脅威事例

| | セーフティ（安全性） | セキュリティ |
|---|---|---|
| 対象範囲 | ・開発対象のシステム<br>・安全性にかかわる，システムの系統的・物理的な故障への対策 | ・開発対象のシステム**＋つながるシステム** |
| 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 |
| 実現するための基本的な考え方 | ・システムを安全状態に遷移，維持する<br>・フェー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<br>・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 |
| 対策への要求レベル指標 | ・SIL (Safety Integrity Level) | ・SAL (Security Assurance Level)<br>・TAL (Trust Assurance Level) |
| 国際規格 | ・グループ規格に加えて分野ごとの規格が整いつつある | ・情報セキュリティの規格はすでに普及段階にある（たとえば ISO/IEC 15408（Common Criteria）がある<br>・**自動車／ IoT セキュリティに関しては，まだ整備されていない** |

表 -1　安全性とセキュリティの対比

として，安全性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注入する攻撃や，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報告されている．

2010 年，Koscher らが，自動車の CAN ネットワークに直接機器を接続することで，エンジンやワイパー，ドアロックなどを操作可能であることを示した[1]．また，2011 年に Checkoway らは，先の研究において，車内のネットワークにアクセスできることの前提は妥当でないということを指摘した上で，車内のネットワークに直接触れることなく，故障診断ツールや CD プレイヤ，Bluetooth，携帯電話網など広範囲の経路から車内の制御ネットワークに侵入可能であることを実験的に検証した[2]．さらに，無線による遠隔操作，位置追尾，車内の音の盗聴などの可能性についても指摘した．

Francillon らは，スマートキー（Passive Keyless Entry and Start（PKES））の脆弱性として，LF 帯の電波信号を中継することで，自動車のスマートキーが自動車から離れた場所にあっても，第三者に自動車のドアの開錠やエンジンのスタートができることを指摘した[3]．

自動車の操舵などの制御ののっとりについては，2013 年，Valasek らが，Ford 社 Escape とトヨタ社 Prius 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，制御をのっとることができることを示した[4]．この手法については，詳細なレポートがインターネット上で公開されている．この実験を通じて，自動車メーカによって，セキュリティの強度（たとえば，ECU ファームウェアの書き換えの容易さ，パワーステアリング ECU によるステアリングを切る条件など）が大きく異なることも明らかになった．

2015 年に開催されたハッカーのイベントである DEF CON では，Miller らが，Jeep 社 Cherokee 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[5]．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．

## 自動車のセキュリティの課題

数多くの ECU が搭載される自動車が，さまざまなネットワークに接続されると，自動車のセキュリティが必須となるが，それには大きく 2 つの課題が存在する．1 つ目は，現在の自動車のセキュリティをいかに強化するかである．これまでの自動車の脅威，脆弱性の事例から，現在販売されている自動車は，セキュリティ対策が十分ではないことが示されており，特に走行時の安全にかかわるセキュリティ対策技術が必要とされている．2 つ目は，将来的につながるクルマのサイバーセキュリティをどのように確保するかである．つながるクルマに対する脅威や攻撃は未知であることから，今後開発が進められる独自ネットワーク（車車間，路車間など）や，インターネットを介したサービス（ス

マートフォンなどの持ち込み機器）に対するセキュリティ対策技術が求められている．

### 情報セキュリティとの違い

自動車には，セキュリティに関するいくつかのリスクが存在する．1つ目は，サイバー攻撃によってシステムが誤動作し，自動車の安全性が損なわれる可能性があることである．2つ目は，自動車の走行履歴や位置情報などの個人情報，自動車の設計情報，音楽や放送のディジタルコンテンツなど価値のある情報が流出・改ざんされることである．3つ目は，自動車がサイバー攻撃の踏み台にされることである．たとえば，踏み台となる自動車のプローブ情報を改ざんするなどして，意図的に交通渋滞を引き起こすことが想定される．特に1つ目のリスクは，情報セキュリティの対象とする一般的な情報システムとは異なるリスクである．

想定するリスクが異なるだけでなく，守るべき資産にも違いがある．情報セキュリティでは，情報の機密性，完全性，可用性という3つの性質に着目しており，これらを保証することを目的とする場合が多い．一方，自動車のセキュリティでは，自動車の安全性の対象となる「人の生命，健康，財産または環境」（JIS X 0134より一部引用）のうち，情報は財産の一部にすぎない．このため，自動車のセキュリティにおいては，最終的に守りたい資産が情報とは限らない．より具体的には，運転者や歩行者の人命だけでなく，車両自体や，電気自動車のバッテリに蓄えられた電気などの物理的な資産も含まれる．

## 自動車のセキュリティ対策

### セキュリティ対策の難しさ

これまでの自動車の開発では，自動車内のECUや通信ネットワークが信頼できることを前提に，いかに効率的に性能や安全性，信頼性を実現するかを中心に設計開発がなされてきた．しかしながら，前述する脅威事例により，攻撃者からのサイバー攻撃を防御するための対策技術が必要とされている．より具体的には，自動車メーカは，販売する自動車に対するセキュリティのリスクを洗い出して評価し，受容できないリスクに対しては，リスクをなくす，もしくは受容可能なレベルまで低減する対策が求められる．

一方で，現実的には，自動車特有のセキュリティ対策の難しさが存在する．

**(1) セキュリティリスク分析が難しい**

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．現在は，Attack treeを用いた脅威分析や，リスク評価手法としてCRSS（CVSS based Risk Scoring System）やRSMA（Risk Scoring Methodology for Automotive system）が提案されており，**表-2**に示すようなリスク評価基準からリスク値を導出する手法が示されている．今後はこれらの手法をベースに改良が行われ，実車両への適用が検討されていくと予想される．

**(2) セキュリティ対策基準がない**

一般的に，セキュリティ対策を強化すれば，その分コストは増加する．特に，コスト制約の厳しい自動車では，無用なコストアップを避けるべきだが，セキュリティの何をどこまで対応するべきか基準がない．近い将来改訂される機能安全規格ISO 26262では，セキュリティに関する内容も盛り込まれるといわれているが，現時点では，自動車のセキュリティに関する国際規格は発行されておらず，検討段階である．

**(3) 計算機リソースに制約がある**

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．そのため，性能の限られるコンピュータを用いた，コスト効率の高いセキュリティ対策技術が求められている．

### 提案されている対策技術

自動車業界を中心にセキュリティ対策技術が検討されている．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

| パラメータ | 概　　要 | 区分（※ 1） | 数値（※ 2） |
|---|---|---|---|
| AV：攻撃元区分<br>（Access Vector） | 脅威エージェントがシステムをどこから攻撃可能であるかによって区分する | ローカル | 0.395 |
| | | 隣接 | 0.646 |
| | | ネットワーク | 1.0 |
| AC：攻撃条件の複雑さ<br>（Access Complexity） | 脅威エージェントがシステムを攻撃する際に必要な条件の複雑さによって区別する | 高 | 0.35 |
| | | 中 | 0.61 |
| | | 低 | 0.71 |
| Au：攻撃前の認証要否<br>（Authentication） | 脅威事象を実現するために対象システムの認証が必要であるかどうかによって区分する | 複数 | 0.45 |
| | | 単一 | 0.56 |
| | | なし | 0.704 |
| C：機密性への影響<br>（Confidentiality Impact） | 脅威事象が発生した際に，対象システム内の機密情報が漏えいする影響によって区分する | なし | 0.0 |
| | | 軽微 | 0.275 |
| | | 甚大 | 0.660 |
| I：完全性への影響<br>（Integrity Impact） | 脅威事象が発生した際に，対象システム内の改ざんされる影響によって区分する | なし | 0.0 |
| | | 軽微 | 0.275 |
| | | 甚大 | 0.660 |
| A：可用性への影響<br>（Availability Impact） | 脅威事象が発生した際に，対象システム内の機能が遅延・停止する影響によって区分する | なし | 0.0 |
| | | 軽微 | 0.275 |
| | | 甚大 | 0.660 |

（※ 1）“区分”は，各影響を 3 つのランクに分類した結果を示す，（※ 2）“数値”は，“区分”で分類された脅威に対するリスク値を示す
JASO-TP150022015- 自動車情報セキュリティ分析ガイドより出典

表 -2　リスク評価基準

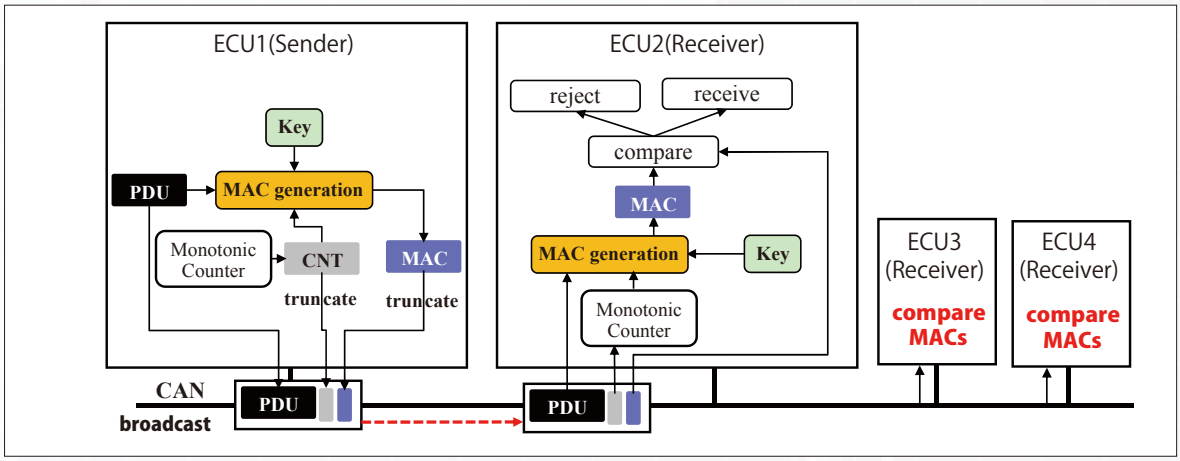


図 -1　AUTOSAR における Secure Onboard Communication 仕様 (SecOC) では，
Message Authentication Code (MAC) の一部を CAN メッセージに付与する対策方法が記述

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，**図 -1** に示す方法で 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たかだか 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．2011 年，畑らは，CAN コントローラを改良することで，正規 ECU がほかの ECU から送信されるなりすましメッセージをエラーフレームで上書きすることにより，不正送信阻止する手法を提案している [6]．2014 年，倉地らが，AUTOSAR と同様に CAN メッセージに付与される MAC の一部を監視ノードのみが検証する集中型セキュリティ監視システム

| Trust Ass. Level (TAL) | Requirements | | | Implications | | |
|---|---|---|---|---|---|---|
| | Minimum Target of Evaluation (TOE) | Minimum Evaluation Assurance Level (EAL) | Minimum (Hardware) Security Functionality | Prevented (Internal) Attacker acc. to CC | Potential Security Implications | C2X Use Case Examples |
| 0 | None | None | None | None | Not reliable against security attacks in general | Some limited, e.g. using trusted C2I infrastructures |
| 1 | +ITS Station software | EAL 3 | Only software security mechanisms | Basic | Not reliable against simple hardware attacks (e.g., offline flash manipulation) | Non-safety, but most privacy relevant use cases |
| 2 | +ITS Station Hardware | EAL 4 | + dedicated hardware security (i.e., secure memory & processing) | Enhanced Basic | Not reliable against more sophisticated hardware attacks (e.g., side-channel attacks) | C2C-CC day one use cases (e.g., passive warnings and helpers) |
| 3 | +private network of ECUs | EAL 4+ (AVA_VAN.4 vulnerability resistance) | + basic tamper resistance | Moderate | C2X box secure as stand alone device, but without trustworthy in-vehicle inputs | Safety relevant relying not only on V2X inputs |
| 4 | +relevant in-vehicle sensors and ECUs | EAL 4+ (AVA_VAN.5 vulnerability resistance) | + moderate – high tamper resistance | Moderate – High | C2X box is trustworthy also regarding all relevant in-vehicle inputs | All |

Minimum Level

S. Goetz and H. Seudié : “Operational Security”, C2C-CC 2012 より出典

表-3　Trust Assurance Levels (TAL) and certification

を提案している[7]．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．

## つながるクルマのサイバーセキュリティ

### 持ち込み機器

自動車の利便性を向上するために，スマートフォンなどの持ち込み機器を，ヘッドユニットやカーナビと接続し連携させる機能の搭載が進められている．また，自動車の診断用ポート（OBD-II）に専用機器を接続することで，保険会社が走行距離を監視したり，家族で車両の位置情報を共有したりするなどのサービスが提供されている．持ち込み機器に脆弱性があると，自動車内に配置された ECU が高いセキュリティレベルで設計されていたとしても，自動車への不正アクセスが容易に可能となる可能性がある．

### 車車間，路車間通信

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いる．その中で，**表 -3** に示される信用保証レベル（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，自動運転技術などで自動車間の連携においても必要とされるものである．たとえば，車車間や路車間通信で，ほかの自動車やロードサイドユニットから得られた情報をどれだけ信じてよいかを考える場合，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．このとき，自動車が要求される基準を満たしていることを，その開発時に TAL などの認証を得ておくことで，情報の発信源が確かに信頼できることを確認できる．さらに，公開鍵基盤（PKI）を利用することで，自動車メーカの枠を超えて，互いの自動車が信頼

し合う方法も検討されている．

### □ 利用形態の多様化

自動車の利用率を高めるため，カーシェアリングのように，ある利用者の使用後に点検や整備を行うことなく，そのままほかの利用者が自動車を使用する新しい利用形態が存在する．このとき，悪意のある利用者がカーシェアリングを使用すると，いとも簡単に車両へ物理的にアクセスすることができ，車両に細工をすることが可能となるため，利用者の安全性や，プライバシーに配慮した遠隔監視技術などが必要とされている．

## ❖ 重点的に取り組むべき課題

自動車を取り巻く環境は大きく変わりつつあり，セキュリティも保証する対策が早急に必要とされている．しかしながら，現状ではその取り組みは始まったばかりであり，自動車に適したセキュリティ対策技術，設計開発プロセス，運用方法，業界基準などの整備が期待されている．特に，自動車の安全性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望まれている．

**参考文献**


1) Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B. , Anderson, D., Shacham, H. and Savage, S. : Security Analysis of a Modern Automobile, IEEE Symposium on Security and Privacy (2010).
2) Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F. and Kohno, T. : Comprehensive Experimental Analyses of Automotive Attack Surfaces, USENIX Security (Aug. 10–12, 2011).
3) Francillon, A., Danev, B. and Capkun, S. : Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars, Cryptology ePrint Archive, Report 2010/332 (2010).
4) Valasek, C. and Miller, C. : Adventures in Automotive Networks and Control Unit (2013), http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf
5) Miller, C. and Valasek, C. : Remote Exploitation of an Unaltered Passenger Vehicle (2015), http://illmatics.com/Remote%20Car%20Hacking.pdf
6) 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).
7) 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 (Oct. 2014).


（2016 年 3 月 31 日受付）


❖倉地　亮（正会員）　kurachi@nces.is.nagoya-u.ac.jp

名古屋大学大学院情報科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）．

❖松原　豊（正会員）　yutaka@ertl.jp

名古屋大学大学院情報科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，リアルタイムスケジューリング理論，安全技術，セキュリティ等の研究に従事．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．同大学院情報科学研究科教授・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．