ミニ特集「セキュリティ」

自動車に迫る脅威とサイバーセキュリティ

倉地 亮
（附属組込みシステム研究センター／情報システム学専攻）

はじめに

近年，カーナビゲーションシステム，キーレスエントリーシステム，自動駐車支援システムなど様々な機能を実現するため，自動車にはECU（Electronic Control Unit）と呼ばれる制御用のコンピュータが多数搭載されています．今後も自動車の快適性や安全性を向上するために，自動車に搭載されるECUの研究開発は益々進められます．近い将来には自動運転を実現し，それらを利用した新たなモビリティサービスへの期待が高まっています．

しかしながらその一方で，自動車のサイバーセキュリティ上の脅威が多数の研究で指摘されており，自動車のサイバーセキュリティ強化は今後発売される自動車に対して必須となっています．そこで，昨今では，各自動車で発生した異常を車両外部に配置されたVehicle Security Operation Center（VSOC）が遠隔監視することで，早期に自動車の異常を検出し，脅威を排除するための侵入検知システムの適用が進められています．

そこで，本コラムでは，自動車に迫る脅威と適用が進められる侵入検知システムについて簡単に紹介し，これらに関連する技術的課題と情報システムの関係について紹介します．

自動車に迫る脅威

自動車に迫る脅威は多岐に渡ります．自動車に搭載されるECUをハッカー（攻撃者）がのっとり，事故を引き起こすことが懸念されます．このとき，乗員や車両周辺の人員の安全が脅かされる可能性があります．また，今後は電気自動車が普及すると，自動車に充電された電力を他の電力網へと売電する際，その売電分の金額が受け取れる仕組みが検討されています．このとき，売買した電力に対する代金が搾取されるなど金銭的な価値が脅かされる可能性があります．さらには，攻撃者により大量の自動車に対して同時に異常が引き起こされ，大量の自動車が走行不能状態に陥ると，販売店や修理工場のサービスが妨害される可能性があります．最後に，自動車の位置情報が他人に追跡されることにより，自宅や学校あるいは職場が特定され，個人のプライバシーが漏洩するという懸念があります．このように，安全（Safety），金銭的（Financial），運用（Operational），プライバシー（Privacy）の４つの観点で各脅威が評価され，よりリスクの高い脅威を排除する必要があります．このとき，各自動車に発生する異常をなるべく早く検出するための仕組みとして，侵入検知システムが必要になります．

自動車の侵入検知システム

近年，自動車に対するセキュリティ上の脅威を排除するために，図１に示される侵入検知システムに関する研究が盛んに行われています．より具体的には，自動車内に配置された車載IDS-ECUと呼ばれる制御用コンピュータが制御システムの異常を監視することにより実現されます．その上で，車載IDS-ECUは，自動車メーカが運用するVSOCへと異常の有無をレポートします．一方，VSOCでは多数の車両からレポートを受信し，それらのレポートをSIEM（Security Information and Event Management）と呼ばれるソフトウェアで一次解析を実施した上，抽出された異常がありそうなレポートを深く分析します．このとき，異常がありそうな車両に搭載される車載IDS-ECU上の異常検知アルゴリズムを更新することにより，様々な異常に対応することが想定されています．さらに，もしあるECUの脆弱性が発見される場合には，無線通信を介したソフトウェアアップデート（以降では，OTA: Over The Airと呼ぶ）が行われ，脆弱性が発見されたECUのプログラムがアップデートされます．また，見つかった脆弱性については自動車分野のISAC（Information Sharing And Analysis Center）であるAuto-ISACに報告され，他の自動車メーカ等へも脆弱性情報が共有されることになります．このような自動車の侵入検知システムの運用が徐々に進められていますが，様々な技術的な課題が存在しています．

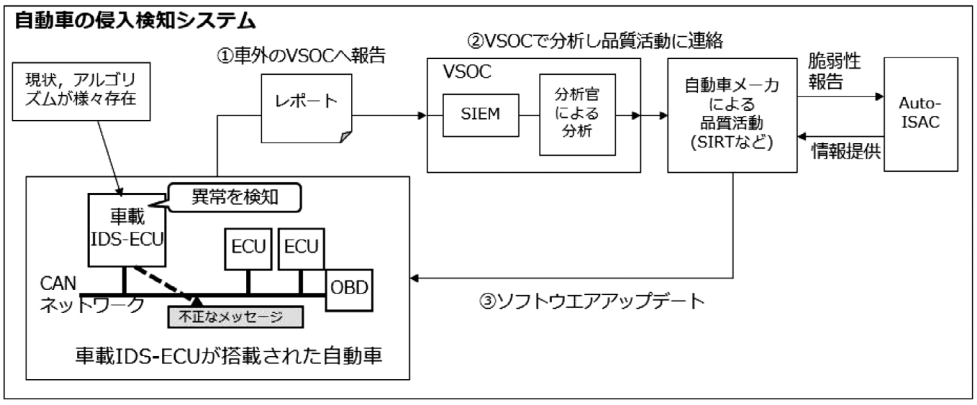

図１. 自動車の侵入検知システム

まず，前述する脅威を排除するために，ECUが扱う通信メッセージにはメッセージ認証技術が適用されています．これにより，攻撃者によるなりすましや改ざんを防ぐことが可能になります．さらには，ECUの開発時には様々なセキュリティ評価を実施することで，その品質を確保しています．より具体的には，脅威分析，脆弱性分析，侵入テスト等が適用されています．また，設計開発時の問題を低減するため，業界標準の開発プロセスが適用され，適切な設計開発や評価が行われた証拠や説明責任が要求されています．またECUに脆弱性が存在する場合には，OTAを用いて確かに正しいプログラムデータに更新することができる認証機構や異常を早期に発見し対応するための運用組織が必要になります．さらに，ECUのアップデートが適切に完了しないと車両を動作させることができないため，予め決められた時間内にOTAが完了するように設計される必要があります．このとき，例えば，自動車のバッテリを枯渇させるほどECUのアップデートに時間がかかると，次に自動車に乗りたいときに，動かせなくなるなどの問題があります．

次に，車載IDS-ECUには制御ネットワークに適した侵入検知アルゴリズムが適用されています．例えば，ルールベースのアルゴリズムを用いてネットワークのトラフィック負荷を監視したり，機械学習を用いて学習されたモデルから外れるようなメッセージ転送が行われていないか監視する場合も存在しています．これらを実行する車載IDS-ECUの多くは組込みシステムであり，マイコン上のプロセッサやメモリ等のハードウェアリソースには厳しい制約が課されているため，サーバなどの高性能なプロセッサ上で実現されるアルゴリズムをそのままでは実装できないなどの制約があります．このため，より適したアルゴリズムの研究開発が必要になります．

自動車の外部に配置されるVSOCでは自動車から送られてくるレポートの内容に従い，ログを解析し車両内では検出できなかった異常を検出することが要求されます．このとき，ログを転送する無線通信ネットワークには，認証や暗号化等が施されます．一方，転送されるログの内容については標準化されておらず，自動車メーカ特有のログから異常を検出しなければならない等の課題があります．

また，Auto-ISACでは自動車業界だけではなく，他の業界等でも発生しているインシデント情報を収集し，自ら配信するデータベースに情報を登録しなければなりません．このとき，ISACの運用者らは，新たな脅威に関連する情報を収集し，それらの真偽や重要性を判断した上で，データベースに登録し情報を配信する必要があります．

交通事故が発生する場合には，交通事故調査が行われます．このとき，現状の交通事故調査においては，自動車の制御システムに不具合がなかったことを自動車メーカの担当者が法廷で証言することにより信頼が担保されています．このため，今後は第３者が検証可能なログ等を自動車内外に残すことにより，自動車メーカに不正がなかった証拠が必要になることが予想されます．しかしながらその一方で，自動車のデジタルフォレンジックに関する研究はまだ始まったばかりであり，自動車内で十分に一貫したログが揃っていないなどの理由から十分に解析できないことが課題です．このため，今後は自動車のデジタルフォレンジック技術を確立し対応する必要があります．また，サイバー攻撃により交通事故が発生する場合には，より複雑な問題になります．例えば，サイバー攻撃により事故が発生したのか，制御システムの不具合により事故が発生したのか，乗員の運転操作のミスにより事故が発生したのか判断することが難しくなります．このような理由から，自動車のデジタルフォレンジック技術はより重要な研究課題になりつつあります．

おわりに

本コラムでは，まず自動車のサイバーセキュリティ上の脅威を説明させていただきましたが，身近なところにサイバーセキュリティの脅威が迫ってきていることがお判りいただけたのではないかと思います．次に，自動車の脅威に対応するために自動車の侵入検知システムが構築されつつある一方で，様々な課題があることを説明しました．適用されつつあるシステムの複雑さや課題点をご理解いただけたのではないかと考えます．また，自動車の侵入検知システムを実現するためには情報システムに関する幅の広い知識が必要になります．より具体的には，ECUのような組込みシステムでは，ハードウェア及びソフトウェアに関する技術や知識が必要になりますし，OTAでは通信プロトコル，VSOCでは大規模なデータ処理技術などが含まれます．さらに，情報セキュリティの観点では，設計・

開発・評価に用いられる様々な技術やアルゴリズム等を知る必要がありますし，運用上の管理や組織間でスムーズに情報を伝達するための技術や仕組みへの理解が必要です．このように身近にある自動車の研究開発においても，情報システムの様々な技術を深く知らなければ，実現できないということがご理解いただけるのではないかと考えます．

最後に，このコラムを読んで，情報システムに関心のある学生が少しでも増え，自動車のサイバーセキュリティの研究分野に少しでも興味を持っていただければ幸いです．

http://tamatebako.i.nagoya-u.ac.jp/6865/