車載組込みシステムの情報セキュリティ強化に関する提言

2013年9月

高田 広章†1　　松本 勉†2

†1：名古屋大学 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／
TOPPERSプロジェクト 会長

†2：横浜国立大学 大学院環境情報研究院 教授
情報・物理セキュリティ研究拠点長

提言の背景

脆弱性報告やインシデントの増加

- この2～3年，車載組込みシステムの情報セキュリティ上の脆弱性が学会等で報告される事例が増えている。

[1] S. Checkoway 他：Comprehensive Experimental Analyses of Automotive Attack Surfaces, USENIX Security, 2011年8月.

[2] C. Miller and C. Valasek：Adventures in Automotive Networks and Control Units, DEF CON 21, 2013年8月.

- また，情報セキュリティ上のインシデントもいくつか報告されている。

対策の基準がない

- 自動車にどれだけの対策をすべきかという基準がないために，自動車業界として対応が進んでいない。

提言のスタンス

- 自動車の情報セキュリティ確保技術に関して，本格的な検討・研究を実施すべきである。
  - 欧州では，EVITA，SeVeCom，PRESERVE，OVERSEEなど，自動車の情報セキュリティに取り組む大規模プロジェクトが複数実施されている。
- 一方で，自動車の開発から廃棄までのライフサイクルを考えると，情報セキュリティ強化に早期に着手することが必要であり，本格検討・研究の成果を待てない状況である。
- そこで，この提言では，本格検討・研究の成果が出るまでに，早急に着手すべきことについて提案する。
- なお，取り組みにあたっては，以下のガイドも参考にすることを推奨する。

[3] IPA セキュリティーセンター：自動車の情報セキュリティへの取組みガイド，2013年3月．

提言のスコープ

車載組込みシステムの情報セキュリティリスク

- 車載組込みシステムに対する情報セキュリティ上の攻撃によるリスクには，次の2つがある。
  (a) 自動車が誤動作し，自動車の安全性（safety）が脅かされる
  (b) 車載組込みシステムが持つ個人情報が流出する

この提言のスコープ

- この提言では，重大度の点から，上記（a）のリスクに対する脅威と，それに対する対策のみを扱う。
- 外部からの情報を信じる必要があるアプリケーション（隊列走行など）は，セキュリティ要件が大きく異なるため，この提言では対象外とする。

考慮すべき脅威

- 車載組込みシステムの安全性に対する脅威として，現時点で考慮すべきものは以下の通りである。

脅威(1) 車内のCANに直接的に攻撃のための機器が取り付けられ，CANに不正なメッセージを流しこまれることは，明らかな脅威である。ただし、このような装置設置攻撃は，車の内部に物理的にアクセスして行われる(例えば，ブレーキがかからなくするためにブレーキオイルを抜くというような)車の機構への直接的な攻撃とも類似しており，それがなされ得ることが，直ちに許容できない脅威であるとは言えない。

脅威(2) OBD-IIポートに攻撃のための機器をつなげられ，CANに不正なメッセージを流しこまれる脅威は，(標準化されたコネクタが車室内に出ているという)攻撃の容易性の観点から，脅威(1)より危険性が高いと言える。

脅威(3) インターネット等のネットワーク越しの操作により，CANに不正なメッセージが流されると，非常に危険である。具体的には，CANにつながっているECUのいずれかが，ネットワーク越しに乗っ取られるケースが考えられる。これは，一度に複数の車に対して攻撃を行い得るという点でも，危険性が高い。

また，近接無線(Bluetoothなど)や持ち込み機器(車内に持ち込んだ携帯電話など)を経由して同様のことができる場合も，危険性が高い。

脅威(4) ECUのソフトウェアの不正書換えは，それがどのような経路でなされるかによらず，明らかに大きな脅威である。不正書換えが見逃されてECUが動作した場合，自動車の安全性に深刻な影響を及ぼし得るという点で，極めて危険性が高い。

脅威に対する対策方針

- 脅威(1)～(4)に対して，自動車側で実施する対策の方針として，以下を提案する。

脅威(1)の対策方針　緊急に対応する必要性は相対的に低い。ただし，リーズナブルなコストでCANに対する攻撃の可能性を軽減する仕組みの導入は検討すべきである。

脅威(2)の対策方針　早急に対応すべきである。不正なメッセージ(OBD-IIポートに接続する診断機器が送信するメッセージ以外のIDを持つCANメッセージ)が，OBD-IIポートから車内のCANに流されることを防止すれば，かなり改善される。

さらに，診断機器からのアクチュエータの強制駆動機能などにより，OBD-IIポートからの正当なメッセージで自動車の安全性が脅かされる可能性がある場合には，十分な対策が必要である。

脅威(3)の対策方針　自動車のネットワーク接続が進む中で，車外のネットワークとの接続点となるECUでのセキュリティ強化は重要性を増しており，十分な対策が必要である。

実際，市販車のインフォテイメントユニットの乗っ取りに成功したという報告もされており [1]，現在の対策で十分か，検討を進めるべきである。

脅威(4)の対策方針　ECUのソフトウェアが不正に書き換えられることを抑止する何らかの仕組みは，既に導入されていると思われるが，不正書換えの完全な阻止は容易ではない。

そこで，不正書換えを抑止する仕組みに加えて，ECUのソフトウェアが不正に書き換えられていることを検出する仕組みの導入も検討すべきである。

脅威に対する対策技術の例

- 脅威(1)～(4)の対策方針を実現する技術の例として，以下を挙げることができる。

脅威(1)(2)(3)の対策技術例1　CANメッセージの不正送信を検出するための仕組みとして，CANにメッセージ認証コード(MAC)を導入する方法が検討されている。

脅威(1)(2)(3)の対策技術例2　リーズナブルなコストでCANメッセージの不正送信を阻止する仕組みとして，以下の提案がある。

[4] 畑正人, 田邉正人, 吉岡克成, 松本勉：CANにおける不正送信阻止方式の実装と評価，電子情報通信学会技術研究報告 ISEC2012-74, pp. 15-22, 2012年12月.

脅威(2)の対策技術例1　現在の技術で可能な対策として，OBD-IIポートに出すCANと車内のCANをゲートウェイで分離し，ゲートウェイで不正なCANメッセージを中継しないようにする方法がある。

脅威(2)の対策技術例2　診断機器からの強制駆動機能の不正使用については，自動車の走行中は強制駆動を機能させないなどの対策が考えられる。

脅威(3)の対策技術例　車外のネットワークとの接続点となるECUでのセキュリティ強化には，既存の情報セキュリティ技術が適用可能な場合が多い。

脅威(4)の対策技術例　不正書換えを防止する仕組みとしては，ソフトウェアの書換え時に，書換え装置またはソフトウェアを認証する方法などが用いられている。

不正書換えを検出する仕組みとしては，トラステッドブートなどがある。