車載の社外品ドングルに対する近接攻撃の検証

北川 智也[1]　垣内 正年[2]　新井 イスマイル[2]　猪俣 敦夫[3]　藤川 和利[2]

概要：自動車の故障診断端子から Controller Area Network (CAN) バスにメッセージを送信することで，ブレーキ操作・速度メータの偽装などの不正制御ができることが知られている．一方で故障診断端子に取り付けて，スマートフォンから車両情報を取得できる社外品ドングルが容易に入手可能だが，その危険性については十分な考察がない．数種類の社外品ドングルの仕様や性能を調査したところ，それらの多くが CAN バスに任意の偽装メッセージを送信可能であった．また，一部はスマートフォンとの接続を横取りできた．本論文では，実車を用いて 31m 程度離れた場所から攻撃可能なことを示し，社外品ドングルを取り付けた際の安全上の脅威について検証結果を報告する．

キーワード：Controller Area Network (CAN)，車載ネットワーク

Verification of the proximity attack on the automotive with aftermarket dongle

Tomoya Kitagawa[1]　Masatoshi Kakiuchi[2]　Ismail Arai[2]　Atsuo Inomata[3]
Kazutoshi Fujikawa[2]

Abstract: It is known that fraudulent control such as braking, spoofing of speed meter and the like can be performed by transmitting a malicious message from the OBD-II port of a car to a Controller Area Network (CAN) bus. An aftermarket dongle that can be attached to the OBD-II port is readily available, but there is not enough consideration on the security risk. We investigate the specifications and performance of several types of these dongles and found many of them were able to send arbitrary any messages to the CAN bus. In this paper, we show that it is possible to attack from a place about 31m away from the actual vehicle, and report the verification results on the threat in case of attaching such dongle.

Keywords: Controller Area Network (CAN), In-Vehicle Network

1. はじめに

車載ネットワークには Controller Area Network (CAN) が広く利用されており，日本においても J-OBD2 として 2010 年から製造される新車に搭載が義務付けられている [1]．このことから CAN は車載ネットワークにおける事実上の標準となっているといえる．一方，CAN バスは共有バスであり，なりすましたメッセージを送ることでスピードメーターの表示を偽装したり，運転者の意思に反してステアリングを操作したり，ブレーキを操作するといった攻撃が行えることが知られている [2][3]．一方で，後付けの OBD-II 端子に取り付ける社外品ドングルが発売されており，こうした製品を経由して攻撃できる可能性が指摘されている [4]．こういった背景がありながら，特に日本国内でどの程度社外品ドングルが使用されているかは今まで明らかになっていなかった．また，社外品ドングルが搭載された車では，具体的にどのような攻撃が可能か調査した事例はなかった．社外品ドングルの多くは Bluetooth または

[1] 奈良先端科学技術大学院大学情報科学研究科
Graduate School of Information Science, Nara Institute of Science and Technology
[2] 奈良先端科学技術大学院大学総合情報基盤センター
Information iniTiative Center, Nara Institute of Science and Technology
[3] 東京電機大学
Tokyo Denki University

図 1　clone チップを搭載する Bluetooth 版ドングルの例

図 2　clone チップを搭載する Wi-Fi 版ドングルの例

Wi-Fi インタフェースを備えている．認証機能が不十分な社外品ドングルは車外から不正にアクセスされる可能性がある．また，OBD-II ポートは常時電源であり，社外品ドングルは自動車の所有者の目を盗んでバックドア的に仕掛けることも容易であることから，駐車時に第三者が不正にドアロックを解除するといった攻撃をする可能性もある．本論文では，社外品ドングルを取り付けた際の安全上の脅威について検証を行う．また，実車を用いて車外の離れた場所から CAN バスに対して攻撃が可能なことを示す．

2. 基本技術

2.1 CAN バス

CAN は ISO15118 で標準化された通信プロトコルである．CAN の特徴として，1. 1 つの通信線に複数の ECU が接続されるバストポロジである，2. バスが空いていればすべての ECU がメッセージを送信できる CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) 方式，3. 同時にデータが送信されて際に CAN ID を用いた送信権の調停を行う (アービトレーション) が挙げられる．

2.2 ELM327 とその clone チップ

ELM327 は Elm Electronics 社が開発し，販売している OBD-II-シリアル変換チップである [5]．複数の通信プロトコルに対応しており，CAN にも対応している．シリアルインタフェースから AT コマンドによって制御できる．

ELM327 の実態は PIC マイコンにプログラムを書き込んだものであり，初期のバージョンではコピープロテクトがなされていなかった．そのため，Elm Electronics 社が販売するものではないコピー製品が出回っている状況である．本論文では，このクローン製品を clone チップと呼ぶ．

ELM327 は狭義にはチップそのものを指すが，ELM327 の clone チップに Bluetooth インタフェースや Wi-Fi インタフェースが搭載された製品を指して”ELM327”とするものが出回っている．clone チップが搭載された Bluetooth 版ドングルの例を図 1 に，Wi-Fi 版ドングルの例を図 2 にそれぞれ示す．これらのドングルは 3.2，3.3 で述べるように認証機能が不十分なものとなっており，本論文はこの脆弱性に特に着目している．

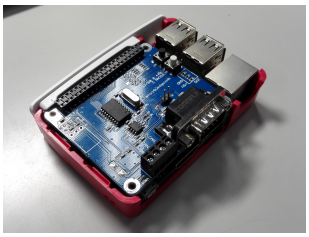

図 3　Raspberry Pi 3 に PiCAN2 を搭載したデバイス

こういったドングルと Bluetooth または Wi-Fi インタフェースを通して接続して，車両のデータの表示や故障診断が行えるスマートフォン向けアプリが多く公開されている [6][7]．

ELM327 および clone チップはデフォルトでは OBD 規格に従って ECU にリクエストを送信し，応答を受信するように設定されているが，AT コマンドにより設定を変更することで，任意の CAN メッセージを送信できる．

3. 実験と評価

実験は図 3 に示すような Raspberry Pi 3 に CAN インタフェースとして PiCAN2 を搭載したデバイスで行った．また Wi-Fi と Bluetooth インタフェースは Raspberry Pi 3 に内蔵のものを使用した．CAN バスの速度は最も用いられている 11 bit ID，500kbps とした．

図 1，図 2 に示す clone チップを搭載する Bluetooth 版ドングルおよび Wi-Fi 版ドングルにおいては，電波法令に定められている技術基準適合証明が取得されていることが確認できなかった．したがって，下記の対応によって電波法を遵守して適法に実験を行う．3.2，3.3 の実験については，これらのドングルをシールドボックス内で稼働させて行った．3.4 の実験については屋外で実験するため，USB インタフェースを備えた ELM327 と技術基準適合証明を受けた Bluetooth 内蔵の Raspberry Pi 3 を接続し，Bluetooth 版ドングルを適法状態に模倣したシステムを構築して用いた．

3.1 ドングルの利用率の予備調査

clone チップを搭載した社外品ドングルが国内でどの程度使われているかの予備調査として，世界中の無線 LAN アクセスポイントの情報を収集しているプロジェクトである WiGLE[8] でデータを収集した．社外品ドングルにはいくつかのバリエーションがあり，著者らの調べでは，Wi-Fi 版に関しては WiFi_OBDII, WiFiOBD, iOBD2, CLKDevices

の 4 種類の SSID があることが分かっている．

国土地理院が公開している日本の東西南北端点の経度緯度 [9] に基づき，経度 122.93361〜153.98638，緯度 20.42527〜45.55722 の範囲で SSID によるフィルタリングを行い，その中から日本国内の座標となっているデータのみに絞った．2017 年 8 月 28 日に収集し，観測された地点の都道府県ごとに集計した結果を表 1 に示す．

表 1 WiGLE による Wi-Fi 版ドングルの観測件数

都道府県	WiFi_OBDII	WiFiOBD	iOBD2	CLKDevices
北海道	2	0	0	0
茨城県	1	0	0	0
埼玉県	3	0	0	0
東京都	6	3	0	0
神奈川県	1	0	0	0
愛知県	2	0	0	0
京都府	2	0	0	0
長崎県	1	0	0	0
合計	18	3	0	0

WiFi_OBDII の SSID を持つものが国内では 18 件観測されており，最も多く出回っていると考えられる．次いで WiFiOBD の SSID が 3 件観測されている．どちらの SSID も東京都での観測件数が最も多くなっている．iOBD2 と CLKDevices の SSID を持つものは観測されておらず，国内ではあまり出回っていないと思われる．

3.2 Wi-Fi 版ドングルの評価

実験に用いた clone チップを搭載する Wi-Fi 版ドングルは正規版の ELM327 に比べて，機能が限定されていた．Wi-Fi 版ドングルは電源投入と同時に SSID が WiFi_OBDII のアクセスポイントとして検出可能となる．暗号化はオープンネットワークとなっており，周囲から誰でも接続可能である．クライアントがアクセスポイントに接続すると，DHCP によって 192.168.0.0/24 の IP アドレスが割り当てられる．この状態で 192.168.0.10 の TCP ポート 35000 を通して clone チップに AT コマンドを送信できる．クライアントが 1 台接続していると，アクセスポイントのブロードキャストは続行しているものの，2 台目以降のクライアントは接続を試みても接続できない．

Wi-Fi 版ドングルの CAN メッセージ送信能力を調べるために，Raspberry Pi 3 をドングルと同じ CAN バス上に配置し，ドングルから CAN メッセージを送信すると同時に，Raspberry Pi 3 上で can-utils[10] の canbusload ツールを使って，CAN メッセージを観測した結果を表 2 に示す．表の値は 1 分間の平均値である．

表 2 Wi-Fi 版ドングルの CAN メッセージ送信能力

送信方法	フレーム数/秒	CAN バスの占有率 (%)
ATSH なし，受信待ちあり	5.30	0.14

実験に用いた Wi-Fi 版ドングルは任意の CAN メッセージを送信するために必要な ATCAF0 コマンドや ATSH コマンドを受け付けないものであったため，CAN ID が 0x7DF の OBD フォーマットに従ったメッセージしか送信できない．また，ECU からの応答を待たないようする ATR0 コマンドも使用できなかったため，送信速度が大幅に制限されている．

このように，同時に 1 台のクライアントだけが接続できる仕様であったが，Wi-Fi ではアクセスポイントになりすまして Deauthentication パケットを送信することによって DoS 攻撃ができることが知られている [11]．Wi-Fi 版ドングルでもこの方法でセッションを横取りすることができることを確認した．

3.3 Bluetooth 版ドングルの評価

Bluetooth 版ドングルは電源投入と同時に周囲の Bluetooth デバイスから検出可能な状態 (discoverable) となり，1 台クライアントが接続されると検出不可能な状態 (non-discoverable) となる．著者らの調べでは，Bluetooth 版ドングルとのペアリングに必要な PIN は 0000 または 1234 で固定されているため，周囲から誰でも接続可能である．また，実験に用いた Bluetooth 版ドングルは BD アドレスが，AA:BB:CC:11:22:33 と不適切な状態で出荷されていたため，場合によっては BD アドレスを第三者が推測できる可能性がある．検出不可能な状態では，名前問い合わせにも応答しない状態となるため，ドングルの BD アドレスを知っていてもその場にドングルが存在するかどうか確認することは出来なくなる．

Wi-Fi 版と同様に Bluetooth 版ドングルの CAN メッセージ送信能力を調べるために，Raspberry Pi 3 をドングルと同じ CAN バス上に配置し，ドングルから CAN メッセージを送信すると同時に，Raspberry Pi 3 上で can-utils の canbusload ツールを使って，CAN メッセージを観測した結果を表 3 に示す．表の値は 1 分間の平均値である．

表 3 Bluetooth 版ドングルの CAN メッセージ送信能力

送信方法	フレーム数/秒	CAN バスの占有率 (%)
CR	183.63	4.96
ATSH なし	26.38	0.71
ATSH あり	12.98	0.35

送信方法で CR は，1 つのメッセージを送信する手順の後，キャリッジリターン (CR) を連続して送信することで同じメッセージの送信を繰り返す方法である．1 バイトの通信で CAN メッセージを送信できるため，最も送信速度が速くなる．ATSH なしは CAN ID は固定でデータが変化する場合を想定しており，毎回送信するデータを clone チップに送信する．ATSH ありは複数の CAN ID を 1 つの clone チップから送信する場合を想定しており，毎回 ATSH

表 4　車種毎の攻撃可否

攻撃	車 1(A 社製, 2008)	車 2(A 社製, 2013)	車 3(A 社製, 2014)	車 4(B 社製, 2013)
ドアロック解錠・施錠	○	○	○	×
メーター偽装	○	○	○	○
エンジン停止	○	×	×	○
アクセル無効化	○	×	×	×
変速比の固定	○	×	×	×

コマンドと CAN バスに送信するデータを clone チップに送信するため，送信速度は最も遅くなる．

最も早い CR の方法でもバスの占有率は 4.96%にとどまっている．CAN バスに無意味なデータを大量に送信し，バスの帯域を圧迫させることができれば Denial of Service (DoS) 攻撃を行うことができるが，Bluetooth 版ドングルを用いて DoS 攻撃はできないといえる．

3.4　実車での評価

実車での評価は，車 1(A 社製, 2008 年式)，車 2(A 社製, 2013 年式)，車 3(A 社製, 2014 年式)，車 4(B 社製, 2013 年式) の 4 台で行った．行った攻撃と攻撃可否を表 4 に示す．

A 社製の車のドアロック解錠・施錠に関しては，キーレスエントリーによる解錠時の CAN バスキャプチャから解錠している CAN メッセージを特定し，そのメッセージを再送することによって解錠することができた．車 4 に関してはキーレスエントリーによる解錠時の CAN バスキャプチャを再送しても解錠することはできなかった．

メーターに関しては，両メーカーとも CAN バスで制御されており，なりすましのメッセージを送信することで容易に車速やタコメーターの表示を偽装することができた．ただし，正規のメッセージも送信されているため，最も短い周期で CAN メッセージを送信できる方法を用いても正規のメッセージと偽装メッセージにメーターがそれぞれ交互に応答しようとして，針が両メッセージが指定する値の間を行き来するような挙動を示す．

車 1 のエンジン停止については，可変バルブ機構のアクチュエータを強制作動させるコマンドを送信すると，アイドリングが不安定になりエンジンが停止する．車 4 についてはアイドリングストップ時に CAN バスに流れていたメッセージを再送することでエンジンが停止する．この方法で強制的にエンジンを停止した場合，エンジンチェックランプが点灯し，自動的には再始動しない．何れも走行中にエンジンが停止することはなかったが，攻撃を継続していれば停車と同時にエンジンが停止する．

車 1 のアクセル無効化と変速比の固定については，トランスミッション ECU からエンジン ECU への何らかの要求メッセージと思われる CAN ID のメッセージを一部改変して送信すると行える攻撃である．アクセル無効化時は，アクセルを全開にしてもエンジンの回転数が上がらず，クリープ現象による前進以上に進めなくなる．この攻撃は，運転者がアクセルを全開にしたところで攻撃を中断することで意図的に急発進させることもできる．変速比の固定攻撃中は低速側の変速比で固定され，速度を上げていくとエンジンの回転数も上がっていき燃費が悪化する，という問題も考えられる．

なお，本節の内容は既出の攻撃手法を試し，CAN メッセージ送信による攻撃可否を確認したにすぎず，各自動車に対して新たな脆弱性を発見して報告するものではない．

3.4.1　ターゲット車両が静止状態での攻撃

Bluetooth の Class2 では有効範囲は 10m とされているが，車内に取り付けたドングルに車外から通信する場合，電波の減衰もあるため通信距離は 10m 程度と予想される．実際の通信可能な距離を確かめるため，車 3 と PiCAN 2 を接続し，Raspberry Pi 3 に内蔵の Bluetooth インタフェースを通して，Blueooth 版ドングルと同様に通信できるように構成した．実験は車両が静止している状態で距離を 1m ずつ変えながら行った．ターゲットとなるドングルの BD アドレスは既知であるとする．RSSI の計測は hcitool rssi コマンドで行い，10 回計測した平均結果を表 5 に示す．

実験の結果，ターゲット車両から 20m を離れると攻撃成功回数が大きく低下するが，31m 離れた地点までは通信できることが分かった．RSSI は車両から離れるにつれて概ね減少していることが分かる．

3.4.2　ターゲット車両が移動状態での攻撃

ターゲット車両が一定速度で移動している際の攻撃可否について実験した結果を表 6 に示す．

本実験条件においては，速度によって成功率は変化しない結果となった．50km/h より速い速度の場合やターゲットとなるドングルの BD アドレスが既知でない場合の検証は今後の課題となる．

4.　対策

OBD-II 端子は常時電源であるため，キーを抜いた状態でドアロックを施錠状態にしていたとしてもバックドア的に動作する．社外品ドングルは簡単に取り付けることができ，運転者は取り付けられていることに気付きにくいため，仕掛ける敷居が低い．対策として，OBD ガードのような物理的に OBD-II 端子にアクセスできなくする防犯用具を利用することが挙げられる．

表 5　距離毎の攻撃可否

距離 (m)	RSSI(dBm)	攻撃成功回数 (10 回中)	成功時の接続時間 (秒)
0	-2.4	10	6.37
1	-4.1	10	6.22
2	-15.5	10	4.44
3	-13.6	10	4.23
4	-19.2	10	5.17
5	-21.3	10	5.08
6	-22.4	9	4.10
7	-25.0	10	4.92
8	-25.7	10	4.79
9	-24.2	10	4.98
10	-25.7	9	4.83
11	-25.3	10	5.13
12	-25.6	10	5.14
13	-24.9	10	4.99
14	-26.9	9	4.97
15	-29.5	8	5.24
16	-28.5	10	5.05
17	-30.1	7	5.62
18	-30.3	9	4.98
19	-30.8	6	5.06
20	-33.3	4	5.99
21	-	0	-
22	-31.0	7	6.64
23	-	0	-
24	-32.0	2	7.14
25	-	0	-
26	-30.0	4	6.45
27	-30.7	3	7.65
28	-29.0	2	7.09
29	-28.3	3	5.37
30	-26.0	5	7.42
31	-32.0	3	8.45
32	-	0	-
33	-	0	-

表 6　車速毎の攻撃可否

車速 (km/h)	成功回数 (10 回中)
10	10
20	9
30	9
40	10
50	9

5. おわりに

本論文では，社外品ドングルを利用している車両の近接攻撃の可能性について検討した．まず，clone チップを用いた Wi-Fi 版ドングルおよび Bluetooth 版ドングルでは CAN バスに任意のメッセージを送信できることを示し，Bluetooth 版ドングルを適法に模倣したシステムではターゲット車両が静止状態で 31m 程度離れた場所から通信可能であることを確認した．また，ターゲット車両が 50km/h で走行していても攻撃できることを確認した．

今後は，Wi-Fi 版ドングルを適法に模倣したシステムでの攻撃可否の調査や社外品ドングルの利用率調査をより網羅的に行う．

参考文献

[1] 国土交通省, ”排出ガス測定方法及び車載式故障診断装置の基準等を改正しました。,” http://www.mlit.go.jp/kisha/kisha06/09/091101_2_.html (2017/08/28 閲覧).

[2] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., ⋯ Savage, S., *”Experimental security analysis of a modern automobile,”*. IEEE Symposium on Security and Privacy, pp. 447-462 (2010).

[3] Checkoway, Stephen and Mccoy, et. al., *”Comprehensive Experimental Analyses of Automotive Attack Surfaces,”* SEC’11 Proceedings of the 20th USENIX conference on Security (2011).

[4] Paul Wagenseil, *”How Car Wi-Fi Dongles Could Lead to Disaster,”* https://www.tomsguide.com/us/obd2-dongle-dangers,news-21590.html (2017/08/28 閲覧).

[5] Elm Electronics, *”ELM327 OBD to RS232 Interpreter,”* https://www.elmelectronics.com/wp-content/uploads/2016/07/ELM327DS.pdf (2017/08/28 閲覧).

[6] https://play.google.com/store/apps/details?id=org.prowl.torque (2017/08/28 閲覧).

[7] http://www.iobd2.com/ (2017/08/28 閲覧).

[8] https://wigle.net/ (2017/08/28 閲覧).

[9] 国土交通省 国土地理院, ”日本の東西南北端点の経度緯度,” http://www.gsi.go.jp/KOKUJYOHO/center.htm (2017/08/28 閲覧).

[10] https://github.com/linux-can/can-utils (2017/08/28 閲覧).

[11] https://www.aircrack-ng.org/doku.php?id=deauthentication (2017/08/28 閲覧).