全車載 LAN データをクラウドサービスで安全に利用するためのシステムの試作

江﨑 貴也[†] 金森 健人[‡] 鶴田 智大[‡] 手柴 瑞基[‡] 井上 博之[†*]
[†]広島市立大学大学院情報科学研究科 [‡]広島市立大学情報科学部
[*]重要生活機器連携セキュリティ協議会(CCDS) 研究開発センター

E-mail: {ezaki@v6., hinoue@}inet.info.hiroshima-cu.ac.jp

自動車の車載 LAN のデータには，実際の運転状況を表す車速，ハンドル，ブレーキ等の様々な状態だけでなく，車両の制御状態や各種センサの情報等が大量に含まれている．既存のプローブカーでは必要なデータのみを利用していたが，広域データ通信サービスの低価格化と高速化により，車載 LAN データを全てクラウドに上げ，リアルタイムに利用することで新たなサービスの展開が可能となってきている．本研究では，センサ情報や制御情報を含む全ての車載 LAN データをクラウド上に安全かつリアルタイムに蓄積し，車種毎に異なるデータを解析し抽象化した情報として，車両利用者，自動車ディーラー，損害保険会社等の第三者に対してその情報を安全に提供し利用するためのシステムを検討する．提案システムのプロトタイプを，小型 Linux マシンを使った車載器とクラウドサービス上に実装し，実車のトラフィックに適用し検証を行った．また，その結果をもとにサービス実現のための考察を述べる．

キーワード 車載 LAN，CAN，クラウド，セキュリティ

1. はじめに

自動車の車載 LAN のデータには，実際の運転状況を表す車速，ハンドル，ブレーキ等の様々な状態だけでなく，車両の制御状態や各種センサの情報等が大量に含まれている．このような制御情報やセンサ情報をやりとりするための車載 LAN プロトコルとしては CAN（Controller Area Network）[1]が一般的に使用されており，CAN の物理ネットワークを構成する CAN バスには電子制御ユニット（ECU; Electronic Control Unit）やセンサに加えて，カーナビやテレマティクス機器のような車載器も接続されてきている．3G/LTE のような広域データ通信サービスの低価格化に伴い，車載 LAN がつながる自動車の診断端子に専用のドングルを接続し，SAE J1979[2]のような診断プロトコルや GPS を用いて取得した自動車の状態を送信することで，走行距離に応じた保険料を設定したり，利用者に様々なサービスを提供したりするようなものが欧米で登場しつつある[3][4].

更なる低価格化が期待できる広域データ通信サービスを利用し，全ての車載 LAN データをクラウドに上げることで，遠隔診断や損害保険会社による運転リスク分析等のサービス展開が可能となる．この様なサービスを複数の車種に対して実現するためには，自動車メーカーや車種毎に異なる車載 LAN データのフォーマットの違いを吸収する仕組みがクラウド側に必要となる．また，サービスの形態によっては常時自動車の状態を把握する必要があるため，リアルタイム性を考慮する．車載 LAN が広域ネットワークのような外部のネットワークにつながることで，情報セキュリティについての問題がでてきており[5], データをクラウドに上げる際の安全性も考慮する必要がある．そこで本研究では，全ての車載 LAN データをインターネット経由でクラウド上に安全かつリアルタイムに蓄積し，車種毎に解析し抽象化した情報を，車両利用者，自動車ディーラーおよび損害保険会社等の第三者にその情報を安全に提供し利用するためのシステムを検討する．また，提案システムのプロトタイプを試作し，実車のトラフィックに適用することで検証を行い，その結果を基にクラウドサービス実現についての考察を述べる．なお，今回想定する車載 LAN は，現在一般的に使用されている CAN を想定する．

2. 車載 LAN データの活用とセキュリティ

2.1. 車載 LAN データの活用例

広域データ通信網を介して自動車の情報を収集する研究としてプローブカーがある[6]. プローブカーとは，自動車を複数のセンサ装置と見立てて交通情報や天候情報を把握するために使用される自動車のことである．多数のプローブカーから, 車速やワイパーの動作等の車両の状態や, GPS から得られる位置情報を収集し解析することで，渋滞情報や降雨状況といった交通や環境の情報を知ることができる．これらを利用して渋滞情報を可視化し，渋滞を避けるルート選択をすること

で交通の円滑化を図る研究や[7], 救急車が目的地に着くまでの時間を短縮するため手法の検討[8]等が行われている．プローブカーでは，車速やワイパー, ABS の動作状況等の情報を車種毎の違いを吸収した形で，広域ネットワークを使用して情報管理センターに送信する方式を採っている．しかしプローブカーによるサービスの提供は，複数台の情報を集約することで実現されており，その情報を個々の自動車を対象とするサービスの実現には不向きである．

自動車には CAN バスにつながる OBD-Ⅱ（On-board diagnostics 2）と呼ばれる診断端子が備わっており，車載器が OBD-Ⅱ端子とインターネットにつながることで車載 LAN の情報を利用するサービスがある[9]．こういったサービスでは SAE J1979 によって定められた診断要求メッセージを送信し, ECU からの診断応答メッセージによって得られた情報によってサービスを提供する方法や，あらかじめ車種を限定する[10]といった方法が用いられている．しかし，車載 LAN に使用される CAN プロトコルの脆弱性により，車載 LAN の情報を利用する際に盗聴やなりすましをされる危険性があるため，サービスの安全性を考える必要がある．

2.2. 車載 LAN セキュリティに関する関連研究

今回想定する車載 LAN プロトコルである CAN は，送信元アドレスを持たず，共有バスを使用したブロードキャスト通信でメッセージを送受信する. CAN の 1 メッセージあたりのペイロードは最大 8 バイトであるため認証や暗号化等は困難であり，通信速度は 500kbps と低速であることからなりすまし攻撃や DoS 攻撃に弱いといった脆弱性がある. CAN へのなりすまし攻撃に関する研究として, CAN バスにつながる車載器にセルラーネットワークを介して不正アクセスを行い，制御プログラムを書き換えることで CAN バスに不正なメッセージを送信して遠隔操作を行った事例がある[11]．この結果として，約 140 万台のリコールが発生する事例となった．このような攻撃の対策に関する研究では, CAN で使用される識別子である CAN ID に対してホワイトリストを使用したフィルタリング[12]や，CAN バス上のメッセージを監視する IDS（Intrusion Detection System）を ECU 内に設置することで，特定のメッセージ頻度を監視して異常を検知する手法[13]に関する研究がある．しかし，CAN データは車種によって異なることから，静的なフィルタリング機構を作ることは難しく，攻撃の対策については研究段階となっている．

著者らも先行研究として，車載 LAN や ECU に対する攻撃の危険性を評価する攻撃検証用プラットフォームを開発して検証を行い，検証結果を基に防御手法についての検討をした[14]．攻撃検証では，乗っ取られた車載器からインターネットを経由した CAN バスへの攻撃を想定し，外部ネットワークから車載器に対して攻撃命令をすることで, なりすまし攻撃や DoS 攻撃が可能であることを確認した．また，防御手法として車載 LAN トラフィックに機械学習アルゴリズムを適用し，動的なルールによるフィルタリング機能をもつセキュリティゲートウェイを提案している[15]．2.1 節でも述べたように，車載 LAN データをクラウド上に集約してサービス展開ができる一方で，このような車載 LAN プロトコルの脆弱性から，車載 LAN データをクラウドで利用するサービスを行う際には，通信の安全性を確保して盗聴を防ぐ仕組みが必要である．

3. 提案システムの試作

3.1. 提案システムの設計と構成

既存の車載 LAN データを利用するサービスでは，サービス毎に車載 LAN に接続する車載器があり専用のサービスサーバに対してデータを送信する形態を採っている．複数のサービスを同時に利用するには車載器が複数となり，コストや機能追加のような保守の面からスケーラビリティの確保が難しい．全ての車載 LAN データをクラウド側で処理する方式では，1 台の車載器で車載 LAN データを特に解釈することなくクラウドに送信することから，車載器は単純な機能で済みコストおよび保守の面からも既存のサービスに比べて，有利である．また機能やサービスの追加もクラウド側で実施できることになる．そこで提案システムでは，自動車の情報を全体的に管理する情報管理サーバをクラウド上に設置し，情報管理サーバが車載器の情報を集約することで機器の負荷を抑え，複数の第三者へそれぞれ必要な情報のみを提供する方式を採る．各サービスに必要となる自動車の情報を情報管理サーバが提供することで，サービスのために必要な処理をクラウド側で全て行うことができ，専用の機器を必要とせず負荷を抑えることができる．ただし，情報収集元の自動車や，第三者サービスが増加した場合は，情報管理サーバには高いスケーラビリティが求められることになるが, AWS（Amazon Web Service）や Google Cloud Platform のようなクラウドサービス等を使用することにより，ネットワーク性能や

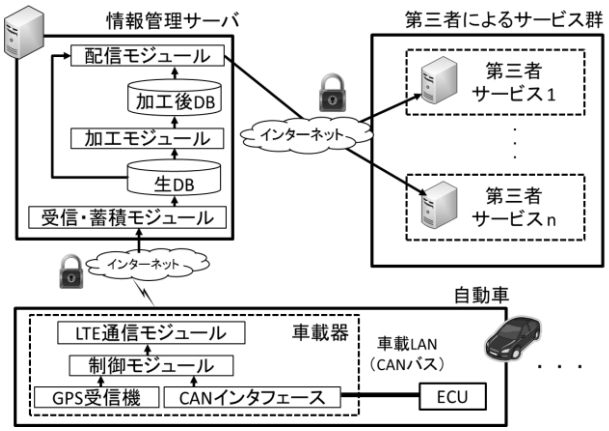

図 1 提案システムの全体構成

処理性能に関するスケーラビリティの問題は解決できると考えられる. 加えて, 2.2 節でも述べたように，車載 LAN データの保護が必要となるため，情報管理サーバにより車載器と第三者のサーバの仲介を行い，それぞれの通信路においてデータの送受信は安全な通信路を用いて行う.

提案システムの構成を図 1 に示す. 車載器は CAN インタフェースと LTE 通信モジュールを搭載し，CAN バスから受信したデータと GPS 受信機から受信したデータを暗号化して逐次インターネットを介して情報管理サーバに送信する. 情報管理サーバは車載器から受信したデータの復号を行い，生データベース（以下，生 DB）に蓄積する. 情報管理サーバ上の加工モジュールはそれぞれの生 DB の車載 LAN データを車種毎の解釈に基づいて抽象化し, 加工後データベース（以下，加工後 DB）に蓄積する. 配信モジュールは配信ポリシーに基づいて生 DB もしくは加工後 DB からデータを取得し，暗号化して第三者のサービス事業者が管理するサーバ（以下, サービスサーバ）へ提供する. そして，サービスサーバは提供されたデータを復号して自身のサービスに利用することで車種に依存しない多様なサービスの提供が可能となる.

ここで考えられる第三者サービスとして例えば，自動車メーカーやディーラーがセンサやエンジンの状態を含む車載 LAN データを利用した不具合箇所の検出する遠隔診断サービス，実車の走行時の評価等を行うサービスや，損害保険会社が運転リスク評価を行い，評価結果で保険料の調整を行うサービス，また，自動車の所有者や家族へ向けた運転評価，燃費計算，ドライブマップを提供するサービス等がある. サービスを組み合わせることでカーシェアサービスでユーザや車両の管理等に応用もできる. 提案システムで提供できるサービスは，情報管理サーバが送信する情報の中身や頻度を変えることで柔軟に構成することができる.

3.2. 提案システムでの通信方式の検討

車載 LAN から送信するデータサイズは比較的小さく，短時間で多くのメッセージを送信する必要があることから，センサネットワークで使用されるような通信方式の適用を考える. その通信方式として, 環境センサや BEMS の通信プロトコルに使用されている IEEE1888[16]を車載 LAN のデータ転送に使用することが考えられるが，IEEE1888 は HTTP 通信を使用するためヘッダサイズが数百バイトと大きく，軽量なデータを高頻度に転送するには必要帯域が大きくなってしまうため，今回は採用しない. 次に，IoT や M2M 向け軽量プロトコルである MQTT(Message Queue Telemetry Transport)プロトコル[17][18]が考える. MQTT では，ヘッダが 2 バイトと小さく，Pub/Sub モデルを使用していることから，車載 LAN データの収集と収集したデータの管理と提供が容易に行うことができるため，車載 LAN データの収集に適しているプロトコルであると考えられる. また，MQTT プロトコルは，TLS によって暗号化通信もできるため, 本研究では MQTT over TLS の方式を検討する. しかし, MQTT プロトコルは TCP を使用するため，一般的にリアルタイム性を求める場合に使用される UDP と，暗号化に OpenSSL を使用した 1 対多向けの L2 VPN を組み合わせた UDP + L2 VPN の独自プロトコルと比較検討する. 車載 LAN の情報のアプリケーション層のデータフォーマットとしては，サービスの多様性や情報の扱いやすさの点から JSON 形式を使用する.

3.3. 通信方式の実装と評価

最初に提案システムのプロトタイプの一部として，図 1 における車載器と情報管理サーバの生 DB 格納までを，3.2 節で挙げた MQTT と UDP を用いて実装した. MQTT の実装ではオープンソースの Mosquitto を使用した. Mosquitto は C 言語で実装されている MQTT プロトコルを使用するアプリケーションであり，プロトタイプシステムには Mosquitto を車載 LAN データをクラウド上に送信するように拡張したものを実装した. また，プロトタイプシステムでの VPN は OpenVPN を用いて実装し，車載器に情報管理サーバで生成した鍵を事前に保持しておくことで VPN 通信を行った. 使用した車載器の仕様を表 1 に示す. 車載器として CAN インタフェースを搭載した組み込み向け小型 Linux マシンを利用し，USB ドングル型の通

表 1 車載器の仕様

項目	内容
OS	Linux (Raspbian)
CPU	ARM Cortex-A7 900MHz
RAM	1GByte
Storage	16GByte (MicroSD card)
Interface	USB, PIO, I2C, LTE データ通信, CAN

信モデムを利用し LTE 通信網を介して情報管理サーバと通信する.

実験環境の詳細を図 2 に示す. 通信方式の評価実験として, 車載器が車載 LAN データを受信してから, 情報管理サーバに蓄積するまでのスループットやパケットロス率, 遅延および車載器の CPU 使用率を測定した. 実験には実車トラフィックの収集や送信が再現できる CAN 解析ツールを使用し, 市販のハイブリッド乗用車のイグニッション ON から 5 分間キャプチャした実車の CAN トラフィック(597,062 メッセージ)を利用した. 車載器と情報管理サーバ間の通信には実行有効速度 6Mbps の LTE 通信網（OCN モバイル ONE）を使用した. スループットとパケットロス率は 5 分間のうち生 DB に蓄積したメッセージ数から算出する. 遅延は, 車載器が CAN データ受信時のタイムスタンプと, そのデータを生 DB に蓄積した時のタイムスタンプの差を算出し, 全時間の平均値をとる. 車載器の CPU 使用率は, 1 秒毎の対象のアプリケーションのプロセスの CPU 使用率を測定し, 測定時間の平均値とする. 暗号化によるオーバーヘッドも検証するため, これらの項目を UDP を用いた独自プロトコル上で, VPN を使用した場合と使用しない場合, TCP を用いた MQTT 上で TLS を使用した場合と使用しない場合の 4 通りで測定を行った.

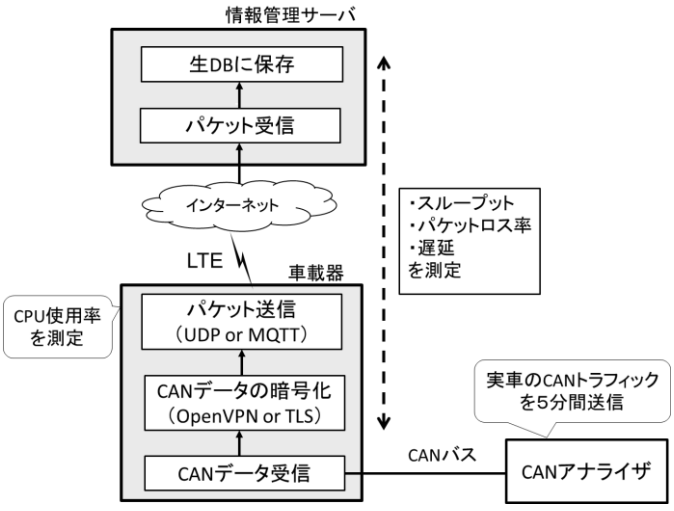

図 2 通信方式の評価実験の構成

表 2 通信方式毎の測定結果

	UDP	UDP＋VPN	MQTT	MQTT over TLS
DB 保存パケット数	589181	560761	597058	597046
パケットロス数	7881	36301	4	16
スループット[pps]	1895.3	1803.8	1920.6	1920.6
パケットロス率[%]	1.32	6.08	0.00	0.00
車載器 CPU 使用率[%]	28.1	28.5	31.7	37.9
遅延 [ms]	150	374	151	241

実験結果を表 2 に示す. UDP と MQTT の暗号化によるオーバーヘッドを比較すると, パケットロス率に関して MQTT はほぼ 0%であるのに対して, UDP は約 1.3～6.1%となっている. 遅延に関して MQTT は約 1.6 倍であるのに対し, UDP は約 2.5 倍となっている. 車載器の CPU 使用率に関しては, MQTT は 30%台で, UDP は 20%台となっており, いずれも車載器の CPU 負荷は低く抑えられている. これらの実験結果より, 全車載 LAN データを暗号化し, 遅延が少なく送信できる MQTT over TLS を使用した方式が, 今回のシステムでは秀れているといえる.

3.4. 実装を通じて得られた課題

プロトタイプシステムでは, セキュリティ対策として通信の暗号化を行い, 遅延やスループット等も考慮し, 車載器に低負荷で実装できる通信方式の検討をした. 今回は通信の暗号化方式のみに着目し検討を行ったが, 実際は鍵交換の方法や, 車載器や情報管理サーバや第三者のサービスサーバのなりすましを防ぐための相互認証の仕組み等を取り入れる必要がある. 認証方式としてはユーザのスマートフォンを用いた個人認証や, マイナンバーカードのような公的認証基盤を利用した認証方式等がある. また, 今回 UDP と比較し秀れているという結果になった MQTT は TCP ベースであることから, その他の TCP を用いた他の通信方式との比較検討も必要である. その他, クラウド上で車載 LAN データのトラフィック分析を行うことによる攻撃検出や, クラウド上での機械学習によるフィルタリングのようなセキュリティ対策を行う既存研究[19]もあり, 今回のシステムでもこういったクラウド上の処理により自動車の異常を検知する機構の実装にも応用可能である.

4. 第三者向けクラウドサービスの試作

4.1. クラウドサービスの実現

車種が異なることに依存しないクラウドサービスを実現するためには，車載 LAN データをどのような意味で解釈するかのルールが必要である．今回は車載 LAN データの解釈ルールは事前に解析を行い準備する，もしくは自動車メーカーと連携してルールを入手しているものと想定する．提案システムでは全車載 LAN データがクラウド上に送信されることから，ユーザが利用する端末や OS に依存せず汎用性を持たせられる Web アプリケーションを利用したサービスが実現可能である．今回は車両所有者や損害保険会社のような第三者向けクラウドサービスのプロトタイプを，Web アプリケーションを利用して，車載 LAN データを監視および解析しサービス提供する運転管理サービスを実装する．

4.2. プロトタイプシステム

クラウドサービスのプロトタイプである運転管理サービスは，現在の自動車の状況を表示する運転詳細機能，ある一定期間内の運転評価を行う運転評価機能，ある一定期間内の運転した経路情報を表示する運転履歴表示機能の 3 つの機能を持つ．サービスの利用には，最初にユーザ登録および自動車情報の登録を行い，次に自身が所有する自動車の情報を，情報管理サーバに送信することで運転管理サービスを利用できる．今回のサービスでは，サービスサーバに提案システム上の加工後 DB に加えてユーザの個人情報と車載器の情報を登録するユーザ管理 DB を持つ運転管理サービスの構成を図 3 に示す．運転管理サーバは，加工後 DB をさらに最新のデータのみを保存する最新加工後 DB と，全ての加工データを保存する履歴加工後 DB と二種類の DB で構成される．今回実装した運転管理サービスを実車での車載 LAN データに適用し，車載 LAN データのみで運転評価が実現可能かの実験を行った．運転評価サービスの結果を示すページを図 4 に示す．今回は独自の基準を用いて運転評価を行っているが，このように車載 LAN データの解釈ルールさえあれば，ユーザが所持する自動車の車種に依存せず，サービス提供者はクラウドサービスを提供できることが確認できた．

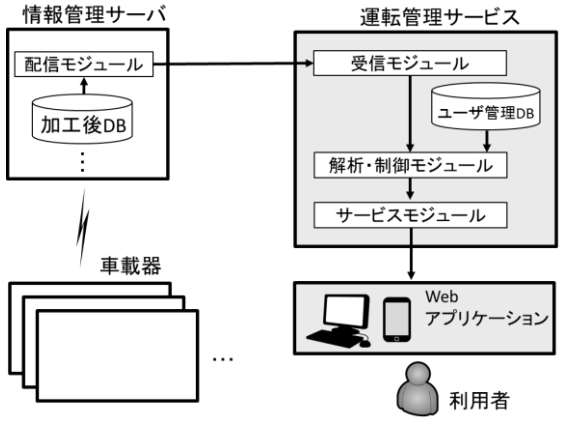

図 3 運転管理サービスの構成

4.3. クラウドサービスの応用

近年の自動車では ADAS(Advanced Driver Assistance System)の搭載も普及してきており，事故を直前で防ぐことや，防止することが実現してきている．今回作成した運転詳細機能や，評価機能を応用することで，蛇行運転，居眠り運転等の人為的な事故を起こす予兆を検出することも可能となる．また，遠隔診断による物理的な危険性の検出，事故後に運転状況の検証をする等，ADAS のような搭載システムに加えて，クラウド側でもリアルタイムにデータ処理をすることで安全性の向上を図ることができる．3.4 節で述べたように提案システムに相互認証を組み込むことで，車両使用者の特定と個人情報の扱いが可能となるため，周辺情報に合わせてコンテンツ情報を配信するような，よりパーソナライズされた情報サービスへの展開も可能となる．

5. まとめ

本研究では，全ての車載 LAN データをクラウド上に収集し，安全にサービスへの利用が可能となるようなシステムの提案をした．提案システムにおける安全な通信路の確保のための検討を，UDP ＋ VPN と MQTT over TLS で行い，結果から MQTT over TLS が秀れていることが分かった．また，提案システムを利用したクラウドサービスのプロトタイプシステムを作成し，車種の違いに

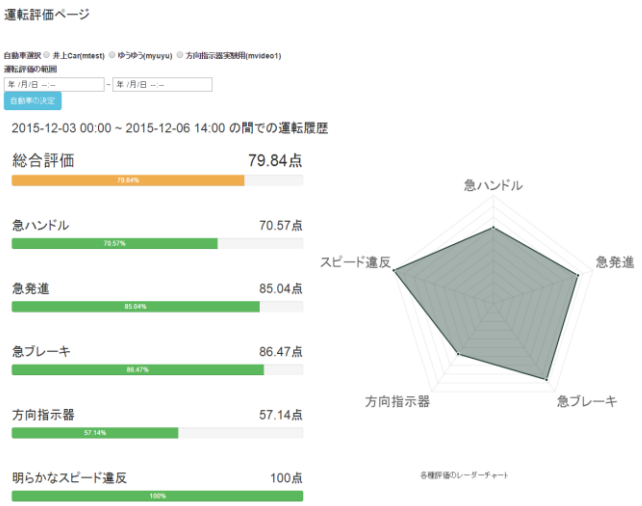

図 4 運転評価ページ

依存しない柔軟なサービスの提供が可能であることを示した．今後の課題として，機器認証の仕組みの導入やスケーラビリティの評価，実車に搭載しての実証実験を行うこと等がある．

参考文献

[1] International Organization for Standardization, “Road vehicles, controller area network (CAN), Part 1: Data link layer and physical signaling,” ISO IS11898-1, 2003.

[2] SAE International, “SAE J1979: E/E Diagnostic Test Modes,” Vehicle E E System Diagnostic Standards Committee, Aug. 2014.

[3] 国土交通省, “テレマティクス等を活用した安全運転促進保険による事故の削減について海外調査報告,” 第7回自動車関連情報の利活用に関する将来ビジョン検討会資料, Sep. 2014.

[4] Vinli, “Turn Your Car Into A Connected Car Of The Future,” https://www.vin.li/press, 参照 Feb. 23, 2016.

[5] 押田大介, 竹森敬祐, 川端秀明, 磯原隆将, ”繋がる車のセキュリティ,” コンピュータセキュリティシンポジウム 2014(CSS2014), pp.651-658, Oct. 2014.

[6] 砂原秀樹, 佐藤雅明, 植原啓介, 青木邦友, 村井純, “IPCar: インターネットを利用した自動車プローブ情報システムの構築,” 電子情報通信学会論文誌, vol.J85-B, no.4, pp.431-437, Apr. 2002.

[7] 橋本浩良, 河野友彦, 門間俊幸, 上坂克巳, “交通円滑化対策のためのプローブデータの分析方法に関する研究,” 平成 22 年度国土交通省国土技術研究会, 2010.

[8] 南部繁樹, 吉田傑, 赤羽弘和, “プローブデータの分析に基づく救急車への緊急走行支援方策の検討,” IATSS review, vol.34, no.3, pp.55-62, Dec. 2009.

[9] トヨタメディアサービス株式会社：T-Connect, http://tconnect.jp/, 参照 Jan. 26, 2016.

[10] 株式会社ゼットエムピー, “車載 CAN データのクラウド構築サービス対象車種を拡充-日産・ノートに対応．車両情報をスマホ経由でリアルタイム送受信-,” プレスリリース, https://www.zmp.co.jp/wp-content/uploads/2014/05/pressrelease_20130620.pdf, 参照 Jan. 26, 2016.

[11] C.Miller, and C.Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” DEFCON23, Aug. 2015.

[12] 矢嶋純, 長谷部高行, 鳥居直哉, 松本勉, “「攻撃メッセージの無効化機能を備えたホワイトリスト CAN ハブ」の実装評価、及び、エラーフレームによる無効化機能を用いたホワイトリスト CAN ハブの提案,” 暗号と情報セキュリティシンポジウム 2016 (SCIS2016), Jan. 2016.

[13] Tobias Hoppe, Stefan Kiltz, and Jana Dittmann, “Applying Intrusion Detection to Automotive IT - Early Insights and Remaining Challenges,” Journal of Information Assurance and Security, vol.4, no.3, pp.226-235, Jun. 2009.

[14] Takaya Ezaki, Tomohiro Date, and Hiroyuki Inoue, “An Analysis Platform for the Information Security of In-vehicle Networks Connected with the External Networks,” The 10th International Workshop on Security (IWSEC2015), Advances in Information and Computer Security (LNCS 9241), pp.301-315, Aug. 2015.

[15] 伊達友裕, 手柴瑞基, 江崎貴也, 井上博之, “車載 LAN のセキュリティゲートウェイにおける機械学習を用いた動的ルール生成,” 暗号と情報セキュリティシンポジウム SCIS2016, pp.1-6, Jan. 2016.

[16] H. Esaki, and H. Sunahara, “Live E! Project; Sensing the Earth with Internet Weather Stations,” Proc. of SAINT07, pp.1-8, 2007.

[17] International Business Machines Corporation (IBM), Eurotech, “MQTT V3.1 Protocol Specification,” http://public.dhe.ibm.com/software/dw/webservices/ws- mqtt/mqtt-v3r1.html, 参照 Dec. 20, 2015.

[18] 粕谷 貴司, 近藤 正芳, 茂手木 直弥 他, “スマートシティのための MQTT プラットフォームの検証,” 情報科学技術フォーラム講演論文集 v13, pp.1-6, Aug. 2014.

[19] 芳賀智之, 氏家良浩, 鶴見淳一, 岸川剛, 前田学, 松島秀樹, 安齋潤, “クラウドを利用した車載ネットワーク向け統計的異常検知システムの提案,” 暗号と情報セキュリティシンポジウム 2016 (SCIS2016), Jan. 2016.