車載器とサーバ間の相互認証に ID ベース暗号を用いた車載 LAN データ収集システム

金森健人† 江﨑貴也† 手柴瑞基‡ 井上博之†* 小畑博靖† 石田賢治†

概要：近年，様々な機器からインターネットを介してデータを収集し，解析することでサービスを提供する IoT システムが普及してきている．IoT サービスの多くは，IoT 機器とクラウド上のサーバ間で双方向通信を用いてサービスを提供するため，サーバへ送信されるデータのなりすましや，機器の不正制御等を防ぐためにも相互認証やデータの暗号化が必要となる．本研究では，IoT 機器である車載器が車載 LAN データをクラウドへ送信し，サーバで収集および解析するような IoT サービスを想定する．サーバと車載器間の相互認証方式として，証明書ペアが不要な公開鍵暗号方式である ID ベース暗号を用いたシステムを提案し，シミュレーションにより有効性を評価した．

キーワード：ID ベース認証，車載ネットワーク，車載器, IoT セキュリティ

Kento Kanamori† Takaya Ezaki† Mizuki Teshiba‡ Hiroyuki Inoue†* Hiroyasu Obata† Kenji Ishida†

Abstract: In recent times, Internet of Things (IoT) systems are becoming increasingly common. IoT systems provide services by collecting and analyzing data from a variety of devices via the Internet. Because many IoT services function using bidirectional communication between IoT devices and servers on a cloud, mutual authentication and encryption of data is necessary to prevent data spoofing by other servers or false control of the device by unauthorized servers. In this paper, we assume that an IoT service that in-vehicle devices sends in-vehicle LAN data on the cloud, then collects and analyzes the data on servers. As a method of mutual authentication between an in-vehicle device and a server, we propose an ID-based encryption system based on public key cryptography, which does not require a certificate pair. Then, we evaluate its efficiency by simulation.

Keywords: ID-based encryption, in-vehicle network, in-vehicle device, IoT security

1. はじめに

現在普及しつつある IoT システムでは，広域ネットワークを介して様々な IoT 機器から多くのデータをクラウド上のサーバに収集することを可能としている．データの収集の他にも，収集したデータの解析を行い制御命令や処理した情報の発信等，クラウド上のサーバと IoT 機器の双方向通信行うことで更なるサービスへと応用可能である．外部のネットワークとつながる自動車を IoT 機器として考えた場合，自動車に搭載されているテレマティクスやカーナビのような車載器が外部との通信を担う場合が一般的である．数十もの電子制御ユニット（ECU; Electronic Control Unit），センサ，アクチュエータがやりとりする車載 LAN のデータを，リアルタイムに広域ネットワークを介してクラウドに送信し処理することで，センサデータや詳細なエンジン状態を含むドライブレコーダ，利用者向け運転評価サービス，運転実績に基づく損害保険等の第三者サービスに利用するようなシステムが考えられる．このようなシステムにおいては既存のプローブカーを越えたサービスが可能であるが，車載器とクラウド間，またクラウドと第三者のサービス間において安全な通信を行うための仕組み，大容量のデータをリアルタイムに蓄積し処理できるようなクラウド側のプラットフォーム，車種毎の違いの吸収の仕組み等が必要となってくる．

車載 LAN で一般的に使用されている通信プロトコルは CAN（Controller Area Network）[1]であり，その車載 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やアクチュエータの情報が大量に含まれている．近年の 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 データを収集して自動車の遠隔診断や損害保険へ応用するサービス[2]等も出現してきており，新しいビジネスへの応用が期待されている．先ほど述べたように，車載 LAN データには，自動車を利用しているユーザの活動や位置情報，自動車会社が独自で使用しているデータのフォーマット，機器の状態や制御情報が含まれているため，機器のなりすましやデータの盗聴によって，情報

†広島市立大学大学院 情報科学研究科，〒731-3194 広島市安佐南区大塚東 3-4-1．Graduate School of Information Sciences, Hiroshima City University, 3-4-1 Ozuka-higashi, Asa-minami, Hiroshima 731-3194, Japan.
‡広島市立大学 情報科学部．Department of Information Sciences, Hiroshima City University.
* 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 〒900-0031 沖縄県那覇市若狭 1-14-6．Connected Consumer Device Security Council (CCDS), 1-14-6 Wakasa, Naha, Okinawa 900-0031, Japan.

流出や不正な機器制御を可能[3]にする恐れがある．また，特定の用途としない 1 台の車載器にて複数の第三者サービス（走行状態を利用する交通情報，損害保険サービス等）に対応するためには，クラウド側に何らかのプラットフォームが必要となり，サービス毎にデータの送信先を処理するような仕組みが必要となる．また，通信データの保護や認証といったセキュリティの対策を行い，スケーラビリティのある第三者サービスに展開できるようなシステムが必要とされる．システムを構成する車載器やクラウドおよび第三者のサーバ間での相互認証や通信の暗号化を実現するためには，CPU やメモリの性能が比較的限定されている車載器での認証および暗号化の方式が課題となる．

本研究では，前述したシステムの具体的な構成として，図 1 に示すような，多数の車載器がクラウド上の特定のサーバ（以下，情報管理サーバ）と相互認証後，暗号化したデータの送受信を行い，また，車載 LAN データを利用する第三者のサーバも同様に認証をした後，情報管理サーバからデータの受け渡しを安全に行えるものとする．車載器としては自動車会社（自動車メーカー）純正の車載器を想定し，車載器と情報管理サーバは自動車会が管理しているものとする．同様のモデルを用いた筆者らの先行研究[4]では，車載器と情報管理サーバ間向けの軽量通信プロトコルについて検討を行ったが，本研究では車載器と情報管理サーバ間での相互認証について焦点を当てる．車載器とサーバ間の相互認証においては，車載器の数が膨大であることや，車載器の CPU やメモリ等が比較的低性能であることを考慮すると，車載器毎に個別の証明書が不要で，かつ認証にかかる処理数や時間が少ないものが望ましい．そのため，車載器と情報管理サーバ間の相互認証手段として，処理が少なく軽量実装が期待される ID ベース暗号[5]を取り入れた手法を検討する．評価として，従来手法で一般的である証明書を用いた相互認証方式と，ID ベース暗号を用いた方式を取り入れたものをシミュレーションにより評価し，処理時間やスケーラビリティについて比較を行う．

2. 提案システムと認証技術

2.1 システムモデル

本システムでは，自動車会社が自社の車載器からのデータを情報管理サーバに蓄積および管理し，車載器と情報管理サーバは自動車会社の組織内で管理することを想定している．また，車載器はサーバとの通信に 3G/LTE といった広域データ通信ネットワークを利用することを想定している．データを利用したい第三者のサービス事業者は，直接車載器と通信を行うではなく，クラウド上で自動車会社から必要な車載 LAN データやユーザ情報のみをやり取りする．ここでサービス事業者と自動車会社は，サービスに利用する情報の種類を事前に決めており，サービス事業者が持つ権限によって入手できる情報が決まっている．車載

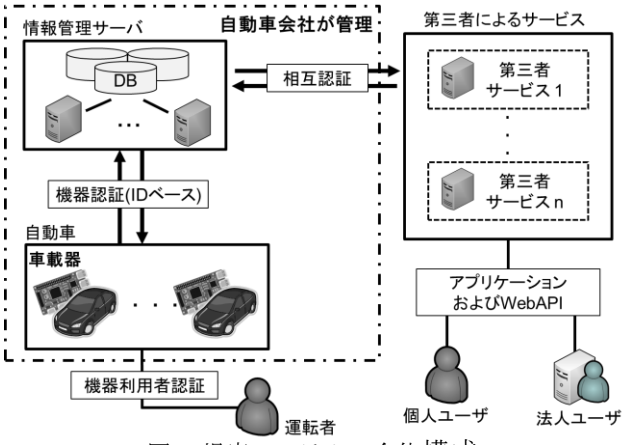

図 1 提案システムの全体構成

LAN データを活用した IoT システムとしては現在トヨタや日産が発表しているもの[6][7]がある．一方で，車載 LAN が広域ネットワークに繋がった際のセキュリティ上の課題が出てきており[8]，筆者らの先行研究でも車載器を経由した自動車へのなりすまし攻撃や DoS 攻撃の危険性を確認している[9]．このようなセキュリティ上の問題を防ぐためにも，車載器と情報管理サーバ間での相互認証とその通信の暗号化は重要である．

2.2 相互認証技術

現在一般的に使用されている相互認証方式として代表的なものは公開鍵証明書を用いた TLS（Transport Layer Security）方式である．TLS 相互認証向け技術として，事前にクライアント間と共通鍵を保持して認証を行う TLS-PSK[10]や，鍵交換時に DHE を用いる公開鍵暗号方式の TLS-DHE-RSA[11]等がある．しかし，証明書を使用した TLS での相互認証では，比較的低性能である車載器での認証および暗号化の処理や，車載器側の証明書の導入および管理を考えると，組込み機器向けの相互認証としては実装および運用上の課題が多くある．そこで本研究では，近年 IoT システム向けの相互認証技術として研究されている ID ベース暗号に着目した．

2.3 ID ベース暗号

ID ベース暗号（IBE; ID-Based Encryption）とは，利用者や機器が持っている独自の ID の情報（メールアドレスや氏名，個体識別番号等）の一部を公開鍵として用いることが出来る公開鍵暗号方式のひとつであり，双曲線写像を用いた実装方式も提案[12][13]され実用化されつつある．ID ベース暗号の特徴として，ID を基に公開鍵を利用できるため，利用者や機器に導入した個別の証明書が認証の際に不要であることが大きなメリットである．しかし，従来の証明書を用いた公開鍵暗号のように認証局の役割が不要となるわけではなく，ID から秘密鍵を生成するための信頼される機関 KGC（Key Generation Center）が必要となる．

実際に M2M 向け次世代モバイルネットワークに ID ベース通信を取り入れたシステム HIMALIS が提案されている

[14]．従来の M2M ネットワークでは IP ベース通信を使用し，IP アドレスが端末識別と位置情報を表す役割を担っていた．膨大な数が想定される M2M では，端末がネットワーク切り替えを行うと IP アドレスが変化し，端末の識別が難しくなってしまう．それを解決するために端末の識別子と位置情報を切り離し，位置情報に関係なく通信を行う ID ベース通信モデルを使用したシステムとなっており，ミドルウェアの実装も行われている[15]．また，サーバ・クライアント間で事前共有鍵を持ち，TLS による相互認証や暗号化通信を行う手法である TLS-PSK に，ID ベース暗号を取り入れた TLS-IBE-PSK[16]が提案されている．

本研究では，ID ベース暗号を TLS 通信の相互認証に取り入れた手法として，富士通研究所の酒見氏らが提案している TLS-IBE-PDK[17]を，車載器とサーバ間の相互認証に適用する．TLS-IBE-PDK の特徴として TLS で必要な証明書の検証処理が不要となるため，TLS ハンドシェイク時の処理数が従来の TLS より少なくなるといった特徴がある．この方式を提案システムに取り入れた場合に，従来の証明書を使用した TLS を用いた手法と比較して，車載器の増加やネットワークのパケットロス率の変化による相互認証に要する時間に，どの程度の差がでるかをシミュレーションにより評価した．

3. ID ベース暗号を用いた車載 LAN データ収集システム

3.1 システムの前提条件

提案するシステムの中でも車載器と情報管理サーバ間での通信における相互認証の焦点を当て，ID ベース暗号を取り入れた場合のシステムとしての有効性について，図 2 のシミュレーション環境で評価する．情報管理サーバと車載器は自動車会社の内部システムとして組織内で管理されているため，ID ベース暗号で使用する ID としては車載器の MAC アドレスのような個体指摘別番号を利用する．また，KGC も自動車会社内で運用しており，事前に必要な鍵交換等も終了している環境を想定する．車載器が故障等により交換する場合は，交換と同時に KGC 内のデータを更新し，また以前の ID に対応する鍵は失効させる．

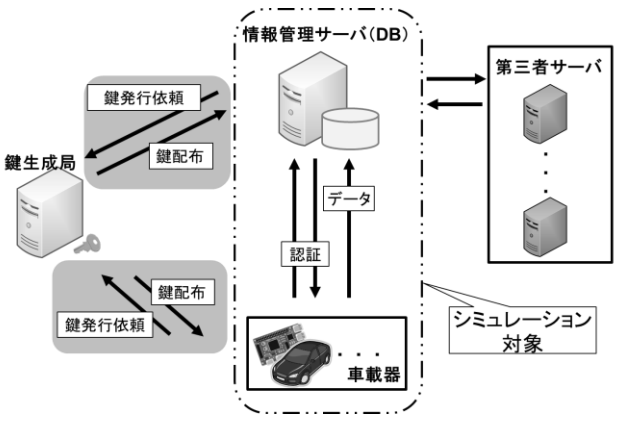

図 2 シミュレーション環境

自動車は移動体であることから，データを送信する際の通信環境の変化や通信メディアの切替えを考慮する必要があり，車載器とサーバ間の通信の初期および再開時に行う相互認証に要する時間は短いほうがよい．車載器の台数を増加させた場合に，従来の証明書を使用した TLS と提案の ID ベース暗号を利用した相互認証方式とで認証に要する時間を比較する．また，移動体の通信環境の変化として通信路のパケットロス率が変化した場合に，両方式での認証に要する時間を比較する．

3.2 シミュレーションモデル

相互認証とデータ送信のシミュレーションの対象となる部分は，図 2 に示す車載器と情報管理サーバ間の通信となる．使用したシミュレータは，ネットワークシミュレータ ns2[18]で，ID ベース暗号を取り入れた相互認証と，従来の証明書を使用した相互認証とで比較評価を行う．図 3 にシミュレーションに使用したネットワークモデルを，表 1 にシミュレーションパラメータを示す．情報管理サーバは 1 台のサーバとし，車載器は複数のクライアントとし台数を可変とした．通信路は途中に 1 台のルータをはさみ，サーバとルータ間は同一 LAN 内とし，通信帯域 10Gbps，伝送遅延 1ms とした．ルータとクライアント間は LTE 等の広域データ通信網とし，通信帯域 5Mbps，伝送遅延 50ms とした．サーバと通信を開始するクライアントの生起間隔は，台数に反比例した値を平均値とした指数分布に従う．

各クライアントは通信の開始時に相互認証のためのハンドシェイクを行うものとする．相互認証が完了したクライアントは，車載 LAN データを情報管理サーバへ送信する動作として 30 秒間 100 バイトの TCP パケットを送信する．TCP パケットを送信し終えたクライアントは通信を終了する．一連の流れを全クライアントが完了するとシミュレーションが終了するものとし，クライアント数は 1, 10, 100, 1000, 2000, 3000 台でシミュレーションを行った．台数を変化させクライアントが相互認証に要するまでの時間の

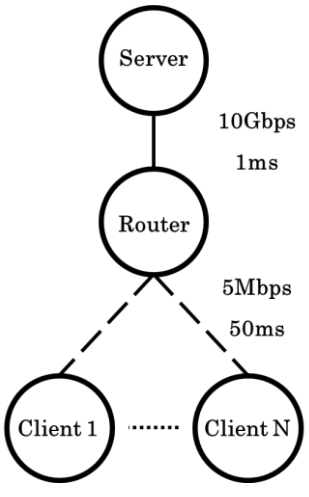

図 3 ネットワークモデル

表 1 シミュレーションパラメータ

シミュレータ名	ns-2 (ver.2.34)
クライアント数	1～3000
クライアントとルータ間の帯域	5Mbps
クライアントとルータ間の通信遅延	50ms
クライアントとルータ間のパケットロス率	0.3%
サーバとルータ間の帯域	10Gbps
サーバとルータ間の通信遅延	1ms

平均値を求め, 台数毎に 10 回シミュレーションを行った平均値を結果とする.

3.3 相互認証に要する時間の測定

シミュレーションパラメータの一つである相互認証に要する処理時間は，証明書を使用した TLS と ID ベース暗号のそれぞれで実際に測定したデータを使用する．従来の証明書を使用した TLS による相互認証のシーケンスを図 4 に示す．サーバは Hypervisor 上の VM（Virtual Machine）を使用し，クライアントは Raspberry Pi を使用した．その Hypervisor およびクライアントの仕様を表 2 に示す．従来の証明書を使用した TLS による相互認証としては ID ベース暗号を利用した相互認証と同等の暗号強度を持つ TLS-DHE-RSA を使用する．従来の証明書を使用した TLS による相互認証に要する時間の測定結果を表 3 に示す．また, ID ベース暗号を利用した相互認証の処理に要する時間については，文献[17]による先行研究のデータを使用した．

4. 評価と考察

4.1 クライアントの台数と認証に要する時間

図 5 にクライアントの台数に対する相互認証に要する時間の平均値および回帰直線を示す．証明書を使用した TLS

表 2 証明書を使用した TLS における相互認証に要する時間の測定環境

	サーバの仕様
CPU	Intel(R) Xeon(R) CPU E5-2667 2.90GHz
OS	Ubuntu 14.04 (64bit)

	クライアント（Rapberry Pi）の仕様
CPU	ARM1176JZF-S Core 700MHz
OS	Raspian (32bit)

表 3 証明書を使用した TLS における相互認証に要する時間の測定結果

サーバ処理時間① [ms]	21.7
クライアント処理時間① [ms]	429.7
サーバ処理時間② [ms]	15.9

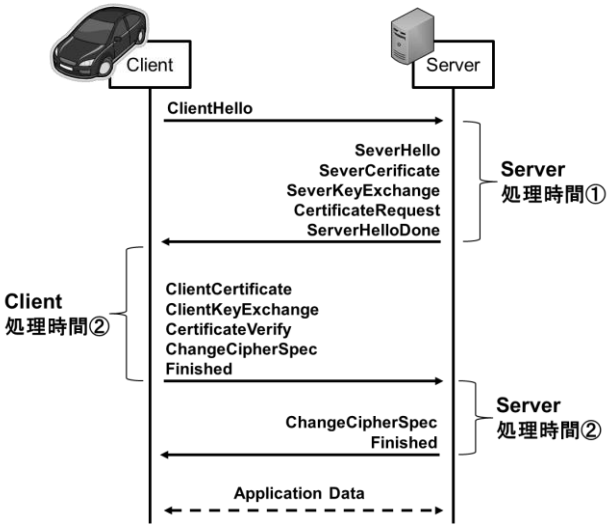

図 4 TLS における相互認証時のハンドシェイク手順

の場合と ID ベース暗号を利用した相互認証の場合，どちらもクライアント数の増加に対して線形的に相互認証に要する時間が増加している．これはクライアント数が増加したことに伴ってサーバが認証処理を行う時間より短い間隔で他のクライアントによる認証要求の到達が多発しサーバのキューにパケットが溜まったためであると考えられる．クライアント数が増加した場合でも，常に ID ベース暗号を利用した相互認証が証明書を使用した TLS による相互認証より処理時間が短いことが分かる．

また，図 6 にクライアントの台数が 100 台のときの時間経過に沿って各クライアントが相互認証に要する時間を示す．横軸は経過時間であり，縦軸はある時刻に発生した相互認証に要する時間となっている．証明書を使用した TLS では相互認証に要する時間のばらつきが多く, ID ベース暗号を利用した相互認証ではばらつきが小さいことが分かる．証明書を使用した TLS による相互認証の方が ID ベース暗号を利用した相互認証よりハンドシェイクの手順が多いこ

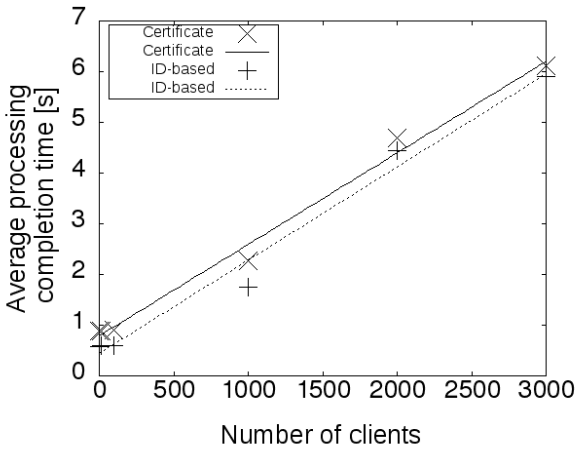

図 5 相互認証に要する時間のクライアント台数による変化

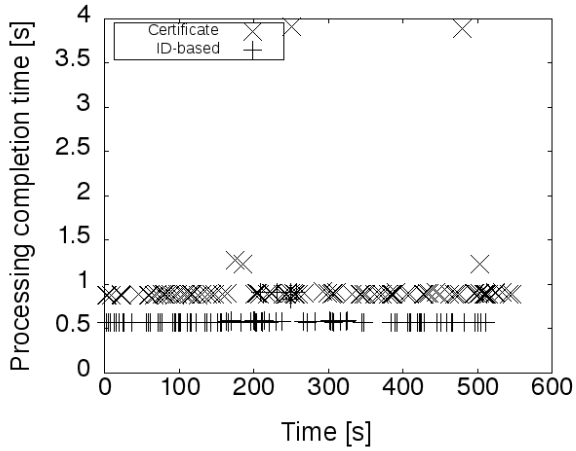

図 6 クライアント数 100 のときの
各クライアントの相互認証に要する時間

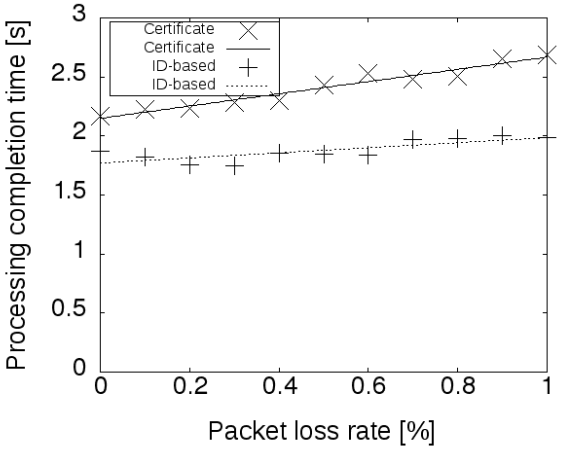

図 7 相互認証に要する時間の
パケットロス率による変化

とから通信時間が長くなり、同時間帯に競合するフロー数が多くなり，キューの増加とそれに伴うパケットロスの発生が TLS の方が多くなったと考えられる

以上の結果より，ID ベース暗号を用いた相互認証を車載 LAN データの収集システムに適用した場合，従来の証明書を使用した TLS に比べ，処理時間が約 300ms 短くなり，また処理時間のばらつきが小さくなることが分かった．提案システムでは，ID ベース暗号を利用したことで車載器とサーバ間での相互認証に要する時間が短くなった．

4.2 パケットロス率と認証に要する時間

想定するシステムでは，クライアントである車載器は移動体であり，広域データ通信網を使用するため，移動中に通信環境の変化が考えられる．そこで，通信環境の変化としてパケットロス率を 0.1%から 1.0%まで変化させ，相互認証に要する時間をシミュレーションにより測定した．図 7 にクライアント数を 1000 台としたときの，パケットロス率に対する相互認証に要する時間および回帰直線を示す．グラフでは証明書を使用した TLS を使用した場合と，ID ベース暗号を利用した場合のいずれもパケットロス率に対して認証に要する時間は線形的に増加しているが，ID ベース暗号を利用した場合が相互認証に要する時間が短く，かつ増加率が小さいことが分かった．これらのことから，提案システムにおいて車載器が搭載された自動車が広域データ通信網の電波を安定して受信できないような環境にある場合に，証明書を使用した TLS による相互認証よりも ID ベース暗号を利用した相互認証方式が有効であると言える．

5. まとめ

本研究では，車載器によって車載 LAN データをクラウド上のサーバに収集するシステムを想定し，車載器とサーバ間の相互認証に要する時間について，シミュレーションによってスケーラビリティの評価を行った．評価結果より ID ベース暗号を利用した相互認証と従来の証明書を使用した TLS による相互認証を比較した場合，クライアント数が増加してもより短い時間で相互認証が可能であることを確認した．今後は，車載器と情報管理サーバ間での ID ベース暗号を利用した相互認証，およびサーバに保存された自動車の情報を第三者が管理するサーバへの安全な情報提供の機能を実装し動作させることで，提案システム全体の機能確認および評価を行っていく．

謝辞 本論文を執筆するにあたって，富士通研究所の酒見氏にデータの提供して頂いた．ここに記して謝意を表す．また，本研究の一部は，広島市立大学特定研究費により行われた．ここに記して謝意を表す．

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] 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.
[3] 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.
[4] 江崎貴也，金森健人，鶴田智大，手柴瑞基，井上博之，“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,” 第 9 回地域間インタークラウドワークショップ，日本学術振興会産学協力研究委員会インターネット技術第 163 委員会(ITRC)地域間インタークラウド分科会 (RICC), pp.1-6, Mar. 2016.
[5] A.Shamir, “Identify-based cryptosystems and signature schemes,” CRYPTO 1984, LNCS 196, pp.47-53, Springer, 1984.
[6] 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.
[7] 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, Jun. 2013.
[8] C.Miller, and C.Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” BlackHat2015, pp.1-91, Aug. 2015.
[9] Takaya Ezaki, Tomohiro Date, and Hiroyuki Inoue, “An Analysis

Platform for the Information Security of In-vehicle Networks Connected with the External Networks," Proc. IWSEC2015, Advances in Information and Computer Security (LNCS 9241), pp.301-315, Aug. 2015.
[10] P. Eronen, and H. Tschofenig," Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)," IETF, RFC4279, Dec. 2005.
[11] T. Dierks, "The Transport Layer Security (TLS) Protocol Version 1.2," IETF, RFC5246, Aug. 2008.
[12] R. Sakai, and M. Kasahara, "ID based Cryptosystems with Pairing on Elliptic Curve," IACR Cryptology ePrint Archive, pp.1-6, Mar. 2003.
[13] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Annual International Cryptology Conference, Advances in Cryptology(LNCS 2139), pp.213-229, 2001.
[14] 福島裕介, カフレベド, 原井洋明, "次世代モバイルネットワークにおける M2M のための ID ベース通信, " 無線通信システム研究会(RCS), 電子情報通信学会技術研究報告, vol.114, no.372, pp.177-182, Dec. 2014
[15] 福島裕介, カフレベド, 原井洋明,"既存ソケットアプリケーションを ID ベース通信可能とするミドルウェアの実装と評価," 情報ネットワーク研究会(IN), 電子情報通信学会技術研究報告, vol.113, no.245, pp.49-54, Oct. 2013.
[16] 酒見由美, 伊豆哲也, 武仲正彦, 金岡晃, "事前共有鍵に基づく TLS の ID ベース暗号による拡張," コンピュータセキュリティ研究会(CSEC), 電子情報通信学会技術研究報告, vol.2013, no.47, pp.1-7, Jul. 2013.
[17] 酒見由美, 武仲正彦, 金岡晃, "ID ベース暗号による IoT 向け相互認証方式の提案," 暗号と情報セキュリティシンポジウム SCIS2015, pp.1-6, Jan. 2015.
[18] Network Simulator - ns (version 2), available at http://nsnam.sourceforge.net/wiki/index.php/Main_Page, accessed Aug. 10, 2016.