Vol.2013-DPS-155 No.9
Vol.2013-MBL-66 No.9
2013/5/23

ICPV(Information Control Platform in Vehicle) システムの開発とその考察

魯　文心[†]　　井手口　哲夫[†]　　奥田　隆史[†]　　田　学軍[†]

近年、自動車は日常生活において重要な居場所として、情報化が急速に進んでおり、様々なユビキタス機能が続々登場している。例えば、ETC、アイサイトなどが挙げられる。一方、家庭用自動車では、利用者が少数あるいは固定であるという特徴がある。それに対して、レンタカーなどのカーシェアリングでは、1 台の車両において、多数の利用者がいるという大きな特徴がある。そのため、車を借りるとき、毎回運転環境を設定する必要があり、ドライバーに対する自動車内の最適な空間の実現が重要となる。本研究では、カーシェアリングの会社を対象に、ICPV(Information Control Platform in Vehicle)システムを設計し、いつでも、どこでも、自動的に最適な運転環境を提供する新しいサービスを提案し、利用者の利便性の向上に加えて交通事故の低減を目指す。

A Study on Development of ICPV(Information Control Platform in Vehicle) System

Wenxin Lu[†]　　Tetsuo Ideguchi[†]　　Takashi Okuda[†]　　Xuejun Tian[†]

Recently, cars become the important place in daily life. With progress of the computerization in the cars, various ubiquitous services appeared. For example: ETC and EeySight. On the other hand, for one private car, the number of drivers is not many and usually fixed. In contrast, for one rental car or sharing car, there are a lot of drivers. For this reason, the drivers should adjust the driving environment every time when they borrowed a car. Thus, to provide the optimum driving environment to the drivers become an important challenge. In this paper, we design a platform called ICPV(Information Control Platform in Vehicle) System, which provides optimum driving environment to the drivers whenever and whatever car they will drive, so that the drivers will feel convenient and the traffic accident will be reduced.

1. はじめに

近年、カーシェアリングが普及しつつである。カーシェアリングとは、家庭用自動車のようにマイカーを所有するのではなく、複数の人が共同で車を所有する（シェアリング）仕組みである。会員登録するだけで、パソコンや携帯から予約し、無人のカーステーションで 24 時間利用可能である。レンタカーと比べて、便利で手軽に借りられるというメリットがある。また、駐車場代やガソリン代、保険料などの維持費がかからないので、車の使用頻度が高くない人にとっては、マイカーより費用が安いというメリットがある。カーシェアリングの車両においては、一台の車両に対して、身体特徴や運転習慣の異なる多数の利用者が存在するという大きな特徴がある。そのため、車内の運転環境が常に変わっており、車を借りる度に、利用者に対して最適な運転環境を設定することが必要となる。「2011 年度乗用車市場動向調査」[1]によると、今後カーシェアリングの利用希望は 12%である。また、カーシェアリングの非利用の理由としては、「自家用車で用が足せる」: 88%、「他人と共有するのが嫌だ」: 22%などが主である。毎回運転環境を設定するのに手間がかかる上に、運転環境が適切ではないと、正しい運転姿勢を保てなく、運転者が疲れやすくなり、交通事故を起こす可能性が高くなる。

この問題を解決するために、我々の先行研究 [2]において、ICPV システムの設計を述べている。本稿では、ICPV システムを改善し、AES 暗号方式を用いて、セキュリティ機能を実装し、マイコンを用いたプロトタイプシステムについて述べる。

2. システム概要

図 1 にはシステムのイメージを示している。

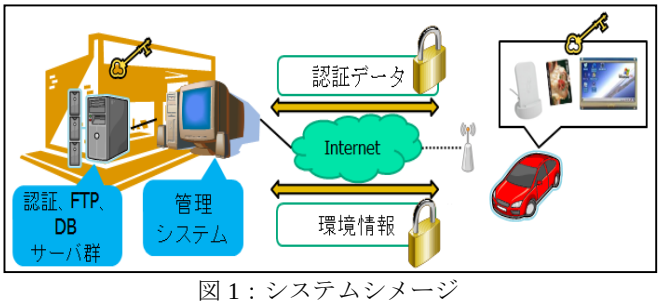

図 1：システムシメージ

本システムでは、情報制御用マイコンと個人認証用 IC カードリーダを車内に実装する。店舗側には、管理システムとサーバ群を実装する。利用する前に、唯一の ID 番号が記録されている非接触型会員カードを発行する。その時、利用者の氏名、性別などの個人情報も店舗側のデータベー

† 愛知県立大学大学院情報科学研究科
Graduate School of Information Science and Technology, Aichi Prefectural University

スに登録する。また、運転環境情報や走行状況などは店舗側のデータベースに保存される。運転環境情報を会員カードへ書き込み、インターネットを経由せず高速に環境情報を車載器に伝送するという方法もあるが、カード紛失した際、情報が全部なくなるということを考慮し、採用していない。また、近年通信インフラ整備の向上により、実際にインターネットを経由してサーバから情報を取り出す方式でも、人が遅延を感じずに済むため、利用上支障がないと考えられる。さらに、利用者の身体特徴に基づいて、運転環境情報を分析することによって、身体特徴に対する最適な運転環境を把握でき、よりよいサービスを提供することが出来る。

本システムは個人情報や業務機密を扱うため、キュリティの面を考慮し、情報のやり取りは暗号化してから行う。暗号方式については、共通鍵暗号方式の代表的な方式である AES(Advanced Encryption Standard)[3]を利用する。AES 暗号方式は、電子政府推奨暗号化方式であり、安全性が高い、処理速度が速いなどの特徴がある。

本システムでは、各備品を制御する制御エージェント群と、認証エージェント、管理エージェント、ユーザーインターフェース、管理システム、認証サーバ、データベースサーバ、FTP サーバから構成される。それぞれの機能を以下に示す（図 2 を参照する）。

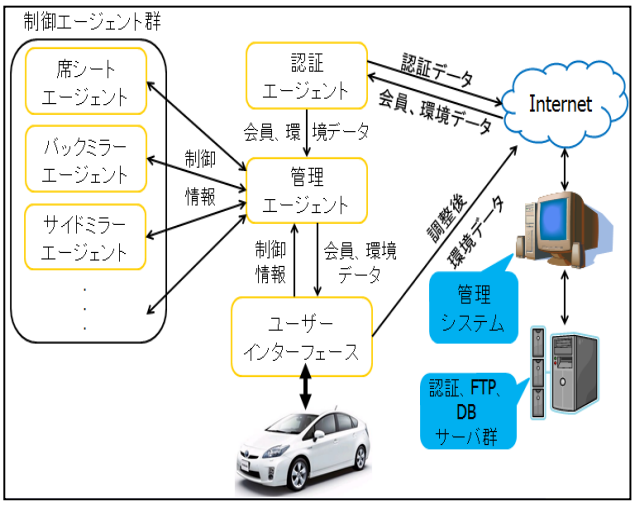

図 2：システム構成

- 認証エージェント：会員カードによって、個人認証を行う。認証成功後、データベースから情報のやり取りが可能となる。
- 管理エージェント：制御する部品の情報を管理する。制御要求があった場合、制御エージェントに制御信号を送信する。
- ユーザーインターフェース：実際の操作画面である。環境設定などを行う。
- 管理システム：日常業務を管理する。テータの操作や帳面作成などを行う。
- データベースサーバ：会員情報、車両情報、走行情報、運転環境情報などを保存する。
- 認証サーバ：会員であるかどうかを判断、権限の付与などを行う。

3. 本システムの制御対象と処理アルゴリズム

3.1 制御対象

本システムの制御対象を以下に示す。

- 運転席：高さ、前後位置、傾き
- ハンドル：高さ、長さ
- サイドミラー、バックミラー：角度
- エアコン：風向き、温度、湿度
- ラジオ：好きな音楽のスタイル、番組
- その他

3.2 制御対象に関する処理アルゴリズム

制御に関する処理手法を以下に示す。

- シート、ミラー、ハンドル：車種別で、備品位置をモデル化し、初めて乗るとき、調整結果を記憶し、今後同じ車種に乗る際、同じ環境を提供する。
- エアコン：22℃を標準温度とする。外部温度と設定温度を対として記憶し、次回乗るとき、その時点の外部温度と同じ外部温度（なければ±2℃を許す）のデータはすでに存在する場合、それに基づいて、その時の設定温度と同じ温度を設定する。なければ、基準温度と設定する。また、外部の温度との温度差を提供できるようにする。
- ラジオ：好きな音楽のスタイルやラジオ番組を予め登録しておいて、時間帯や利用シーンに応じて、自動的に再生する。

4. システムの処理方式

(1) 利用者のログイン処理

車を借りるとき、まず会員カードを用いてログインする。この時、システムはデータベースへカード ID が存在するか問い合わせを行う。

(2) 利用車種の問い合わせと環境設定

この車種は初めて乗るかをデータベースへ問い合わせする。初めてであれば、環境設定が要求される。設定完了後環境情報はデータベースに保存される。初めてでなければ、データベースから環境情報を取得し、自動的に設定される。

(3) 運転環境の調整

走行中、いつでもユーザーインターフェースを用いて運転環境を調整することができる。調整された環境情報は自動的にデータベースへ保存される。

(4) 返却処理

車を返却するとき、走行データ（走行距離、借りる時間、返す時間、etc.）が自動的に集計され、データベースへ保存される。

以上の処理を図 3 に示す。

Vol.2013-DPS-155 No.9
Vol.2013-MBL-66 No.9
2013/5/23

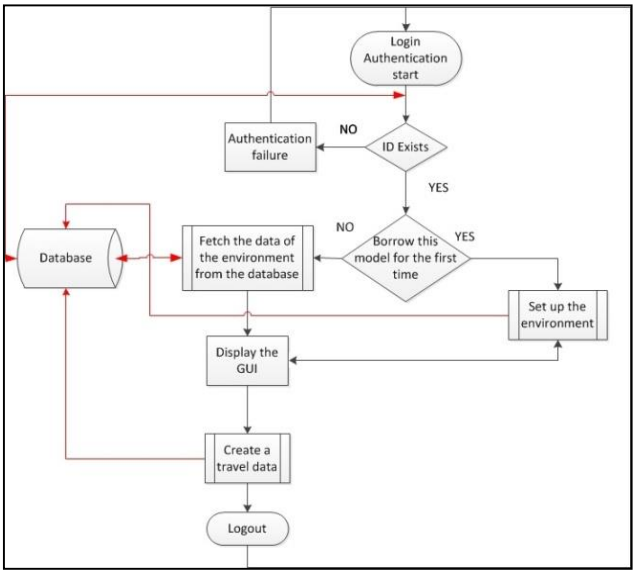

図 3：処理フローチャート

5. データベース設計

本システムではリレーショナルデータベース[4]を用いる。まず概念モデルについては、データベースに 4 つのリレーションが存在する（図 4 を参照する）。それぞれは、利用者、車を借りる（返す）、車、環境の設定である。また、それぞれのリレーションにおいては、様々の属性が存在する。例えば、利用者というリレーションでは、氏名、生年月日、性別、電話番号、住所、免許証番号などの属性を持つ。そして、車を借りる（返す）というリレーションにおいて、認証、借りる時刻、返す時刻などの属性が存在する。本来、カーシェアリングは無人店舗なので、料金精算も自動的に行われるために、課金というリレーションが存在するべきであるが、本稿では対象にしていない。

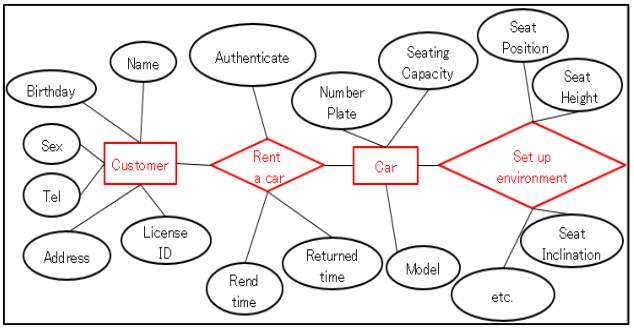

図 4：データベースのリレーション

実際のデータベースは 4 つのテーブルが存在する（図 5 を参照する）。それぞれは利用者、車、運転環境、ログである。利用者テーブルは利用者の個人情報を保存する。車テーブルは車の情報を保存する。運転環境テーブルはだれがいつどの車両に対して、どんな環境を設定したかを保存する。

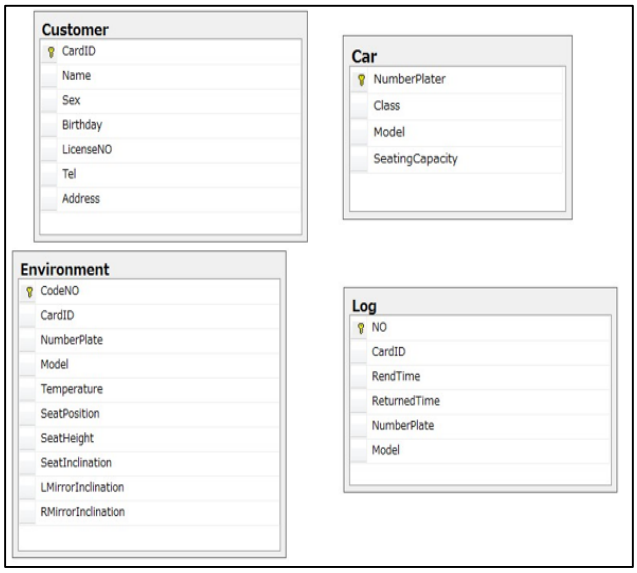

図 5：データベースのテーブル

利用者が車を借り、会員カードを用いてログインするとき、システムは利用者テーブルへ会員 ID が存在するかどうかについて問い合わせを行う。ログイン成功後、運転環境テーブルへその利用者がその車種における環境情報が存在するかどうかについて問い合わせを行う。ここでは、複数の結果がでる場合が想定されるので、その場合、一番新しい情報を使う。運転環境テーブルの主キーである CodeNO については、環境を設定した時点の時刻を使う。例えば、2013 年 4 月 13 日 10 時 15 分 10 秒に設定した場合、CodeNO が 20130413101510 となる。こうすると、同じ CodeNO を発生することが避けられる。また、利用者テーブルに身長、上肢長、股下高などの人体寸法データを入れ、それらの情報と運転環境テーブルの情報を結びつけて分析することによって、身体特徴に対する最適な運転環境を把握でき、よりよいサービスを提供することが出来る。

6. 暗号方式

本システムでは、個人情報を扱うため、セキュリティを考慮しなければいけない。セキュリティ対策の一つとしては、データをすべて暗号化してから、伝送するという方式を考えられる。暗号化方式については、共通鍵暗号方式の代表的な方式である AES(Advanced Encryption Standard)を利用する。

AES では、平文を 128 ビット毎のブロックに区切って暗号化を行う。各ブロックは 4×4 の行列として暗号化される。鍵長は 128-bit、192-bit、256-bit の 3 つがある。暗号化においては、SubBytes、ShiftRows、Mixcolumns、AddRound-Key の 4 つの変換処理から構成される Round を鍵長に応じた回数で実行する。表 1 にブロックサイズと鍵長、Round 数の関係を示す。本稿では、鍵長が 128-bit の AES を利用する。例えば、共通キーを「test001」にし、送信する情報を「氏

Vol.2013-DPS-155 No.9
Vol.2013-MBL-66 No.9
2013/5/23

名：愛知太郎」とする場合、暗号化された結果は「6C942EB023BEFAF6FEB36960355989D3」となる。図 6 に情報は暗号化されてから伝送されるイメージを示す。

表 1：ブロックと鍵長、Round の関係

	ブロックサイズ (bit)	鍵長 (bit)	Round (回)
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

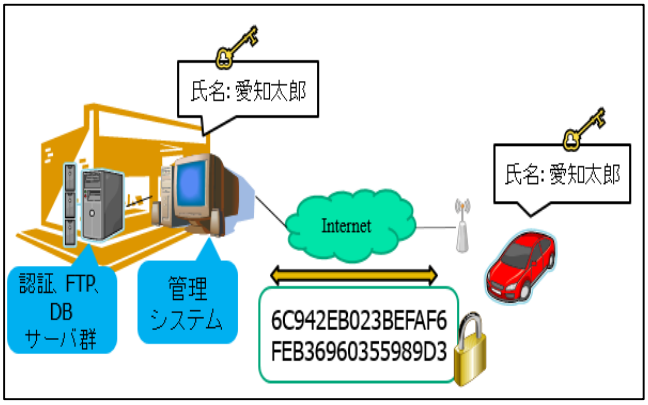

図 6：情報伝送のイメージ

7. プロトタイプシステム

我々は、マイコンを車載器としてプロトタイプシステムの開発を行う。マイコンは QT210 評価ボード(QT210 評価ボードのスペックを表 2 に示す)を用いる。プログラミング言語は C#を使用する。ネットワーク環境は LAN を利用する。データベースは Microsoft® SQL Server® 2008 R2 Express を利用する。カードリーダは SCM Microsystems 社の NFC リーダライタ SCL010 を使う。また、WinCE 環境におけるカード ID 読み取り API については、Microsoft 社が提供している PC/SC(Personal Computer/Smart Card)[5]に準拠した Smart Card Functions[6]を用いて開発を行う。具体的には、SCardEstablishContext()、SCardListReaders()、SCardConnect()、SCardTransmit()、SCardDisconnect()の五つの関数を使用する。それぞれの機能を以下に示す。

- SCardEstablishContext()：リソースマネージャに接続し、カードリーダへの接続環境を準備する。
- SCardListReaders()：挿入されているカードリーダをリストアップする。
- SCardConnect()：指定したカードリーダへの接続を確立する。
- SCardTransmit()：カードリーダへコマンドを与える。カードリーダからの返り値を受け取る。
- SCardDisconnect：指定したカードリーダの接続を切断する。

API の処理プロセスを図 7 に示す。

表 2：評価ボードのスペック

CPU	Samsung Cortex-A8 S5PV210
RAM	DDR2 512M
Network Interface	・10/100M Ethernet ・802.11n WIFI
OS	Windows Embedded CE 6.0

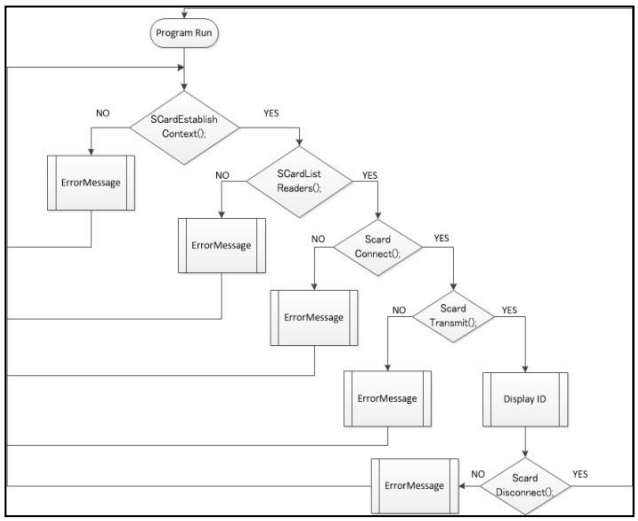

図 7：カード ID 読み取り API のフローチャート

8. まとめ

本稿では、ICPV システムを改良し、マイコンを車載器としてプロトタイプシステムの開発について述べた。さらに、AES 暗号方式を用いるセキュリティ機能の実現について検討した。今後の課題として、カーシェアリング会社における業務の流れを調べ、業務管理システムを開発する予定である。

謝辞

本研究の一部は、平成 25 年度文部科学省科学研究費助成基盤研究(C)(24500087、24500088)の支援を受けて行った。

参考文献

[1] 一般社団法人 日本自動車工業会, 2011 年度乗用車市場動向調査, URL: http://release.jama.or.jp/sys/news/detail.pl?item_id=1553
[2] Wenxin Lu, Tetsuo Ideguchi, Takashi Okuda, Xuejun Tian, A Study on Design of ICPV System, 2012 年電子情報通信学会通信ソサイエティ大会講演論文集, BS-5-14, Sep.2012(富山大学)
[3] Announcing the ADVANCED ENCRYPTION STANDARD (AES), FIPS 197, National Institute of Standards and Technology (NIST)
[4] 増永 良文,リレーショナルデータベース入門［新訂版］, 株式会社 サイエンス社
[5] ISO 7816 - Smart Card Standards Overview, URL:http://www.smartcardsupply.com/Content/Cards/7816standard.htm
[6] Smart Card Functions (Windows CE 5.0), URL: http://msdn.microsoft.com/en-us/library/ms937004.aspx