3V-5

ICPV（Information Control Platform in Vehicle）システムの設計

魯 文心†　井手口 哲夫†　奥田 隆史†　田 学軍†

愛知県立大学　情報科学研究科†

1. はじめに

近年、カーシェアリングが普及しつつである。家庭用自動車と比べて、レンタカーでは、１台の車両に対して、複数の利用者がいるという大きな特徴がある。そのため、車を借りる度に、自分に適切な運転環境を設定する必要がある。本稿では、カーシェアリングの会社を対象に、ICPV システムを設計し、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。

2. システム構成

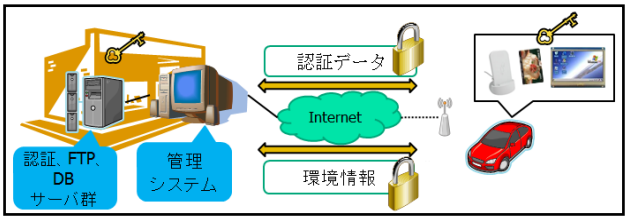

図１：システムイメージ

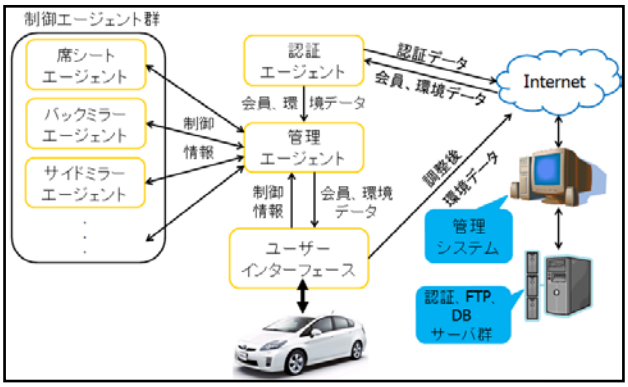

図２：システム構成

本システムは、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１、図２参照）。

■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。

■制御エージェント群：管理エージェントからの環境情報を基づいて、各備品を制御する。

■ユーザーインターフェース：実際の操作画面であり、環境設定などを行う。

■管理システム：日常業務を管理する。デ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、環境情報などを保存する。

■認証サーバ：会員かどうかの判別、権限の付与、利用時間の測定を行う。

■FTP サーバ：環境情報ファイルを保存する。

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

- 運転席シート：高さ、前後、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、温度、湿度
- ラジオ：好きな音楽のスタイル、番組
- その他

3.2　制御対象に対応する処理アルゴリズム

■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．利用の流れ

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。次に、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

Design of ICPV System
Wenxin Lu†　Tetsuo Ideguchi†　Takashi Okuda† and Xuejun Tian†
†Graduate School of Information Science and Technology, Aichi Prefectural University

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

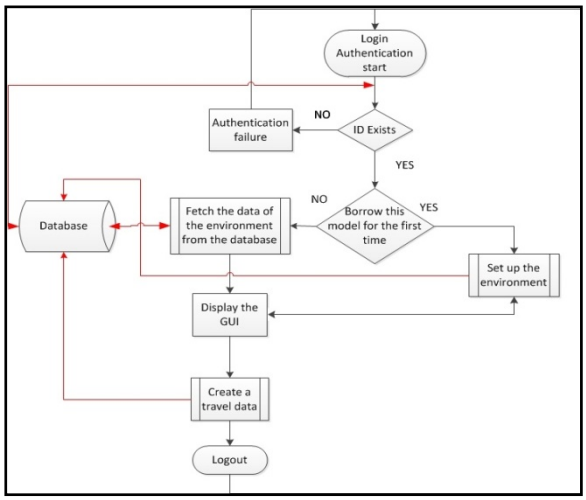

図 3：処理フローチャート

5. 暗号化方式

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。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)[1]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 数の関係を示している。本稿では、鍵長が 128-bit の AES を利用する。

表 1：ブロックと鍵長、Round の関係[1]

	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

6. プロトタイプシステム

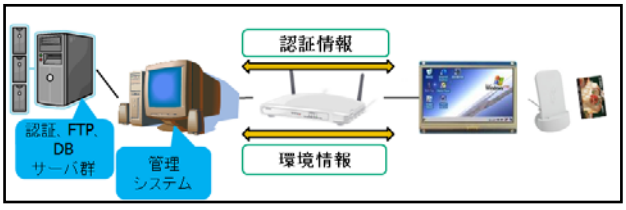

図 4：プロトタイプシステム

プロトタイプシステムに関しては、車載機として、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。

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 (WinCE)

本稿では、Microsoft 社が提供している PC/SC(Personal Computer/Smart Card)に準拠した Smart Card Functions を用いて、WinCE 環境におけるカード ID 読み取り API を開発する。

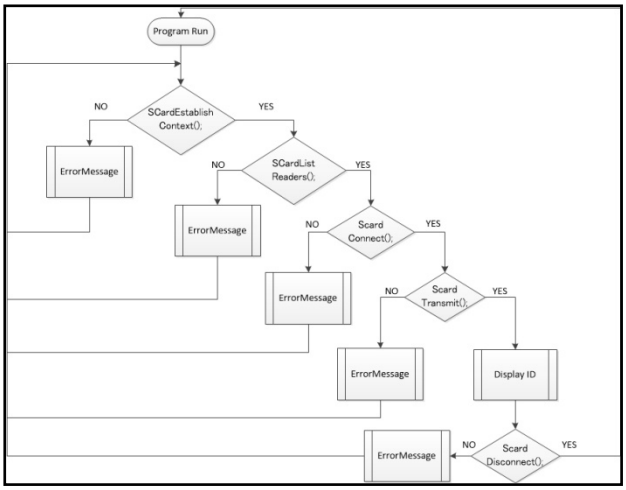

図 5：カード ID 読み取り API のフローチャート

7. まとめ

本稿では、ICPV システムを設計し、マイコンを用いてプロトタイプシステムの開発について述べた。AES 暗号方式を用いて、セキュリティ機能を実現する。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 24 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]”Announcing the ADVANCED ENCRYPTION STANDARD (AES)”, FIPS 197, National Institute of Standards and Technology (NIST)

[2]福田将之、井垣宏、中村匡秀、“ホームネットワークシステムにおけるリアルタイムな家電制御サービスの実現”、信学技報、IN2008-33(2008-7)