

# ICカードを用いた自動車運転履歴の管理システムの提案

## A Proposal for Driving Record Management System for Automobiles Using IC Card

武田 昌宏†  
Masahiro Takeda

山本 宙†  
Hiroshi Yamamoto

辻 秀一‡  
Hidekazu Tsuji

### 1. はじめに

近年、主に運転免許証の偽造防止を目的として運転免許証をICカード化することが警察庁により計画されている[1]。また非接触型ICカードが情報を繰り返し読み書きできる、読み書きの操作が簡単である等の利点から急速に普及している。

本研究ではICカードの利点に着目して、操作の簡単な自動車盗難防止システム、運転履歴の管理システムを統合したシステムを提案する。自動車盗難防止システムではIC免許証に毎回異なる鍵を保存することで安全性を高めている。運転履歴の管理システムでは違法運転の履歴を管理し、優良運転者に利益を付与することで違法運転を奨励する。

### 2. 研究背景

#### 2.1 速度遵守／自動車盗難防止

交通死亡事故原因の中でも最高速度違反が占める割合は大きい。死亡事故を減らすためには、制限速度を守り安全運転を心がけることが大切である。また認知はしているものの、検挙数が著しく少ない自動車の盗難を防止することは、盗難による被害額を抑えることができる。[2]

#### 2.2 ICカードの利点

ICカードの利点として、データを書き換えることできる、非接触の場合はかざすだけでデータのやり取りができる、カードだから持ち運びが容易、などが挙げられる。

提案する統合システムはこれらICカードの利点を十分に活かしたものとなっている。盗難防止システムではカードが非接触形態であるという点を活かして、ドライバーにとって煩わしくないシステムとなっている。また免許証に鍵を保存するために、書き込み可能であるという点も活用している。履歴管理システムではカードへの書き込みの汎用性から、IC免許証にプライバシーと切り離れた違法運転履歴データのみを残している。またカードの携帯性により車を交換しても本人の履歴として処理できる。

### 3. システム概要

#### 3.1 自動車盗難防止システム

このシステムは降車時に毎回異なる鍵をIC免許証に保存することによって安全性を高めている。また家族共用で車を使用する場合もあるので、使用するドライバーの数だ

† 東海大学大学院工学研究科情報理工学専攻,  
Course of Information Science and Engineering,  
Graduate School of Engineering, Tokai University

‡ 東海大学情報理工学部情報メディア学科,  
Department of Information Media Technology,  
School of Information Science and Technology,  
Tokai University

け鍵を用意する。その鍵を用いることで安全性を高めるだけでなく、各々のドライバーに適した車内環境を整えることができる。運転するドライバー毎にシートやバックミラー、サイドミラーの位置が違うので、それらを車側システムによって調整する。

#### 3.2 運転履歴の管理システム

このシステムは違法運転の履歴を管理し、優良運転者に利益を付与する。従来、速度違反をして捕まったら罰則金を支払っていたが、提案では制限速度を守る、即ち違法運転を行うとドライバーにポイントを付与して、与えられたポイントで自動車の保険料を割引するシステムである。

### 4. システム詳細

統合システムはIC免許証(以下、免許証)、車側システム(カーナビゲーション機能を含む)、地上側システム、警察管下のデータ管理センターから構成される。

#### 4.1 自動車盗難防止システム

このシステムで登場するのは免許証と車側システムだけである。またイモビライザーと併用する。以下に処理の流れを示す。

1. ドライバーは最初に車を使うときに一度だけ免許証データの初期設定を車側システムとの間で行う。最初の鍵がここで免許証に書き込まれる。
2. 乗車時に車側システムと免許証の間で通信を行い、免許証に保存されている鍵が一致すればドアが開錠される。また、免許証保有者が運転するように車側システムが車内環境を調整する。(サイドミラー、バックミラー、シートの位置など)
3. イモビライザーによりトランスポンダ内蔵のキーでID照合をし、IDが一致すればエンジンを始動する。
4. 降車時に、次に車を動作させるための新しい鍵を免許証に書き込む。

#### 4.2 運転履歴の管理システム

従来方式との最も重要な違いは、「抜き打ち検査ではなく全数検査である」という点である。速度を守ることに對して不公平感をなくし、違法運転を奨励する。違法運転を行ったか否かということが速度違反で捕まるのと同じぐらい「運しだい」ならば、制限速度を守らなくなる可能性がある。ここでカーナビを使えば全数検査が可能であるが、問題となるのがカーナビの精度である。詳述は4.2.3に示すが、このシステムを導入するドライバーの相当数を正しく判定する必要がある。また全数検査を徹底するとドライバーの全運転履歴を記録することになるのでプライバシーの問題が懸念される。これは4.2.4で扱う。以下に処理の流れを示す。

1. 運転中は車側システムのカーナビがもつ道路情報と連動して、違法運転の履歴を車側システムに蓄積する。
2. 蓄積されたデータは、地上側システムが設置してあ

る場所を訪れたときに自動的に（車から降りることなく）データ管理センターに電波で送信される。

3. 車側システムに違法運転の履歴データが蓄積されていて、データ管理センターに未送信の場合は車を降りるときにその未登録データを免許証に書き込む。
4. 免許証を特定の場所（交番、コンビニ等）に持って行けば未登録データをデータ管理センターに登録することができる。

#### 4.2.1 地上側システムの設置場所

山奥を運転する場合などを考えると常時インターネットに接続するというのは現実的ではないので、特定の場所（例えばインターチェンジ、ガソリンスタンド、コンビニエンスストアの駐車場）に地上側システムを設置する。設置する側のことを考えると、「この場所を訪れると自動で登録できる」というのが宣伝になれば、設備投資をしてもらえる可能性が高い。

またカーナビの補助的な役割で違法運転の判定精度を高めるという目的で、現行のオービス/Nシステムを拡張して地上側システムとし、車側システムのカーナビ機能と通信を行う。一方、高速道路と一般道が並走している区間など、道の判定が難しそうなポイントのみ補助的に地上側システムを設置する。

#### 4.2.2 走行速度測定方法

車側システムがもつ道路情報にチェックポイントをあらかじめ設定しておく。チェックポイント AB 点間の距離を情報としておき、A 点を通過してから B 地点を通過するまでの時間を計り、距離と時間から平均速度を算出する。

#### 4.2.3 カーナビゲーション精度

4.2 で述べたように、全数検査を公平に行うためにはカーナビの精度の高さが要求される。現在のカーナビは道を一本間違えることが稀にあり、そのせいでポイントが付かなくなるとしたらドライバーが制限速度を守る可能性は極めて低い。

現在国家機関と民間企業の連携によって、準天頂衛星システム (QZSS) を利用した高精度測位実験計画が推進されている[3]。GPS の弱点を QZSS が補うことによって、今よりさらに高精度な測位が可能となる。今回の提案では地上側システムを導入することによって判定精度を高めているが、より高い精度が要求されるので、このシステムの利用が必要不可欠になってくる。

#### 4.2.4 プライバシー問題

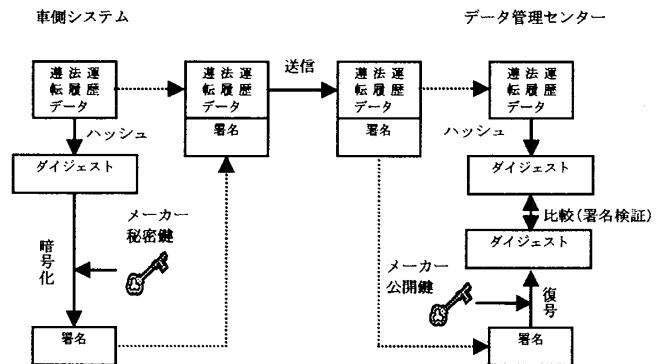
公平性を保つために全数検査を徹底するとプライバシー問題が懸念されるので、それを回避する方法も重視する。具体的にはカーナビが違法運転を判断するシステムとし、車側システムにのみ全ての運転履歴を記録する。これにはプライバシーの問題があるので直接車外システムには出さず、違法運転の履歴データ（データベースへ未登録のポイント、通算違法運転距離数、最近の違反時点/今回車を降りた走行距離と時刻）のみを外部システムに送信することでドライバーのプライバシーを保護する。

### 5. データ改ざん

悪意あるユーザが自前のリーダーライターを使って、IC 免許証（以下、免許証）内に入っている違法運転の履歴データ（以下、データ）を改ざんする恐れがあるので、それを防

ぐ必要がある。具体的には車側システムが免許証にデジタル署名[4]を施し、データ管理センターは送られてきたデータが改ざんされていないかデータを更新する。ここで車側システム（カーナビ機能含む）は物理的にもソフト的にも改ざんすることが非常に困難であるという前提である。

まずドライバー A（以下 A）が車を購入したときに、メーカーが各車用に秘密鍵と公開鍵を生成する。そして秘密鍵を耐タンパ性をもった車側システムに封入し、公開鍵はメーカーから直接警察のデータ管理センターへ登録する。A が車を降りるときは、データのダイジェストを秘密鍵（A は絶対に知ることのできない）でデジタル署名し、免許証に転送する。A は免許証を特定の場所に持って行けばデータを転送することが出来る。そしてデータ管理センターはデータが改ざんされていないかデータベースを更新する。もし途中で A がデータを改ざんしていれば、署名検証のときにダイジェストが一致しないので容易に検出することが出来る。



### 6. おわりに

本論文ではドライバー、警察、自動車保険会社の三者が登場するが、それぞれにとってメリットのあるシステムとなっている。ドライバーは制限速度を守るとポイントを付与され、そのポイントで保険料の割引を受けることができる。警察は死亡事故につながりやすいとされる最高速度違反や自動車の盗難が減少する。保険会社としては、交通事故や自動車の盗難が減少すれば保険金を支払う額が通常より減少する。

### 7. 参考文献

- [1] セキュリティ産業新聞 “免許証 IC カード化へ”  
<http://www.secu354.co.jp/intv/intv05021001.htm>
- [2] 警察庁統計  
<http://www.npa.go.jp/toukei/>
- [3] 宇宙航空研究開発機構 JAXA “準天頂衛星を利用した高精度測位実験システム”  
<http://qzss.jaxa.jp/>
- [4] PKI 関連技術に関するコンテンツ “デジタル署名”  
<http://www.ipa.go.jp/security/pki/024.html>