高度交通システム　5－10
（2001．5．25）

バイオメトリクスによる走行中のドライバー認証技術の開発

高橋 健太　三村 昌弘　磯部 義明　瀬戸 洋一
日立製作所　システム開発研究所

要旨　ITS（Intelligent Transport Systems：高度道路交通システム）において課金を伴うサービスを提供する際には、車内の利用者を走行中に認証する必要がある。本研究では、走行中のドライバー認証に関する要件を抽出し、顔や音声などの生体情報（バイオメトリクス）を用いて、特別な操作を必要とせずハンズフリーで運転中のドライバーを認証する利用者認証システムが適していることを明らかにした。また実験の結果、車内の利用者認証技術に関して実用化の見通しをつけた。

Development of Driver Authentication Technology using Biometrics

Kenta Takahashi, Masahiro Mimura, Yoshiaki Isobe, Yoichi Seto
Hitachi, Systems Develoment Laboratory

Abstract　Authentication of a driver in a moving car is required for providing some pay services of the ITS. In this paper, we analize requirements of driver authentication and show that hands-free authentication methods using biometric information such as faces and voices are suitable for the ITS. We also show experimentally that it is possible to authenticate a person in a moving car by biometric information.

1 概要

ITSにおいて、走行中のドライバーへの情報提供や運転補助など多種多様なサービスの実現が考えられており、将来的には、有料情報の提供など走行中の電子決済を伴うサービスが考えられる。決済にあたっては、支払いの意思を確認するために利用者の認証が必要となる。利用者認証機能は、IPネットワークや路側網に設置されたアプリケーションサーバと車載端末の間で実行される端末間の相互認証（端末間認証）、および車載端末が利用者を確認する本人確認の2段階で実現される。課金の対象としては自動車を運転する運転者および同乗者が考えられるが、特に運転者を対象とした場合、運転中の安全を考えると、本人確認のために運転以外の特別な操作を必要としないなどの要件がある。

本研究では、走行中のドライバーに対する、安全性と利便性の高い利用者認証を実現する目的で、スマートゲートウェイにおける利用者認証の要件抽出、これに基づく利用者認証の実現手段の比較評価を行った。その結果、PKIベースの端末間認証および生体認証を用いた本人確認を連携した方式が適していることを明らかにした。また走行中の車内における、生体認証を用いた本人確認の予備実験を行い、その結果マルチモーダル生体認証（複数のバイオメトリクスによる融合判定）技術の開発が必要であることを明らかにした。

2 利用者認証の要件抽出

スマートゲートウェイにおける利用者認証の要件を、本人確認の利便性に関する要件、本人確認の安全性に関する要件、端末間認証に関する要件の３種類に分けて抽出した。

本人確認の利便性に関する要件としては、認証が運転中に行われることを想定し、運転に支障をきたす操作がないこと、および認証操作によそ見運転（視線の限定）が含まれないことが要求される。認証時間に関しては、運転者は認証装置である車載端末を占有することができるため特別な要件はなく、利用者が不便に思わない程度の時間で本人確認ができれば十分である。具体的には 10 秒以内の認証時間で十分と考える。

本人確認の安全性に関する要件については、情報処理振興事業協会（ＩＰＡ）策定の「運用要求策定ガイドライン」[4]に従って、本人確認時に他人を誤って受け入れてしまう確率（他人受入率）に関する要件を明確化した。スマートゲートウェイにおいてクレジットカード決済を実現するためには、犯罪発生確率が少なくとも現状のクレジットカードの盗用確率(約0.012%／年 [5])と同程度以下である必要があると考える。スマートゲートウェイにおけるクレジット決済の犯罪発生確率は、車の盗難・侵入確率（約0.45% [5][6]）と他人受入率の積で表される。従って他人受入率は、以下の式を満たすよう、2.7%以下の必要がある。

車の盗難・侵入確率×他人受入率　≤　クレジットカードの盗用確率.

これに車両盗難件数が増加傾向にあること[5]を考慮し、今後車の盗難・新入件数の倍加によってもクレジットカードと同等の安全性を実現できるよう、他人受入率に関する要件を1%以下と設定する。

端末間認証に関する要件は、単一の基地局ゾーン内でハンドオーバを発生することなく認証を完了させることを目標として設定した。具体的には、車両の最高時速を180km/h、ゾーン長さを30mとして[1]、物理層における認証時間が0.6秒以内であることを要件とした。また、基地局と車載器との無線通信の転送速度は4Mbpsであり、DSRC(Dedicated Short Range Communication)プロトコル[1]を利用することから、195KBの容量で利用者認証情報のすべてを転送できることを要件とした。

以上の要件を表 1にまとめる。ここで明確化した要件を用いて、各利用者認証方式の評価、および、システムモデルの評価を行っていく。

表 1. 利用者認証の要件

要件の分類		要件の内容
本人確認に関する要件	利便性に関する要件	・運転中の操作がないこと ・運転中に視線が限定されないこと ・認証時間が 10 秒以内
	安全性に関する要件	・他人受入率 1%以下 （犯罪発生確率がクレジットカード盗用確率以下）
端末間認証に関する要件		・端末間認証速度が 0.6 秒以内 ・最大 195KB の容量で利用者認証情報のすべてを転送できること

3 利用者認証手段の評価

２章において明確化した要件を満足する具体的な利用者認証方式を明らかにする目的で、その実現方法を本人確認の手段と端末間認証の手段の２つに分けて評価した。

3．1 本人確認手段

本人確認の手段は、提示する情報に基づき、次の3つに分類できる。

(1) 秘密情報 (ex. 暗証番号・パスワード・符丁)

(2) 所有物 (ex. 磁気カード、ICカード、トークン)

(3) バイオメトリクス (ex. 指紋、顔、音声、虹彩、etc)

運転中のドライバーの本人確認手段は利便性が重要となるため、上記の手段をインターフェースで細分化し、評価対象の項目とした。細分化の目安としてはインターフェースを介した情報の入力に接触を必要とするか否か (接触・非接触)、およびユーザが情報の意識的な提示を必要とするか否か (提示・非提示)、の2点とした。こうして細分化した本人確認手段に対し、利便性要件、安全性要件について評価を行った。なお安全性に関しては、走行中の車内における明るさ、騒音など環境の変動が他人受入率に影響を及ぼす可能性の有無についても評価を行った。結果を表2に示す。

表2 認証手段の比較

			具体例	利便性			安全性		備考
				操作	視線の限定	認証時間	他人受入率	環境変動の影響	
秘密情報	ボタン入力		PIN、暗証番号、パスワード	有	有	1～3秒程度	20%*4	無	安全性は運用依存
	音声入力		ViaVoice※1など	無	無	1～3秒程度		有	秘密情報の暴露
所有物	磁気カード		クレジットカード、ATMカード	有	有	1秒程度	0.01%*5	無	他人受入率は利用者の運用に依存
	ICカード	接触	MULTOS※2カードなど	有	有	1秒程度		無	
		密着	日立密着カードなど	有	有	1秒程度		無	
		近接	MIFARE※3カードなど	有	有	1秒程度		無	
		遠隔	リモートタグ	無	無	1秒以下		無	
生体情報	接触・提示		指紋、掌形、署名など	有	有	1～3秒程度	0.0001%から数%まで	有	
	非接触・提示		虹彩、網膜、音声など	無	有 (音声除く)	1～3秒程度		有	
	非接触・非提示		顔、耳形状など	無	無	1秒程度		有	

*1 ViaVoice は IBM Corporation の商標

*2 MULTOS は英国 Mondex International 社の登録商標

*3 MIFARE は Philips Electoronics N.V.の登録商標

*4 警察庁犯罪白書より, *5 クレジットカードの年間盗難件数より

2章で明らかにした本人確認手段の利便性要件および安全性要件を満たすものは、顔などの非接触・非提示型のバイオメトリクスによる認証がある。また、音声を用いた生体認証は非接触・提示型であるが、視線の限定を必要とせず、要件を満たしている。遠隔ICカードによる認証も利便性、安全性要件を満たしているが、カードなど所有物を用いた本人確認では、盗用による他人受入率を技術的に制御することができず、運用および利用者のセキュリティ意識に安全性が依存してしまう。一方、バイオメトリクスを用いた認証の他人受入率は統計的に求めることが可能であり[3]、環境の変動による影響を受ける可能性があるものの技術的に対処可能である。従って、スマートゲートウェイにおける本人確認手段としては、非接触・非提示型のバイオメトリクス、および音声による認証が最も適していると考える。

非接触のバイオメトリクスを用いた本人確認手段をさらに細分化し、各バイオメトリクスについて評価を行った。結果を表 3 に示す。バイオメトリクスの意識的な提示を必要とする非接触・提示型のバイオメトリクスとしては、虹彩、網膜、音声などがあり、非接触・非提示型のバイオメトリクスとしては、顔、3 次元顔形状、耳形状などがある[2]。3 次元顔形状や耳形状など、研究中で製品・実績がないバイオメトリクスに関しては、認証時間や他人受入率が不明である。

虹彩や網膜はある時間視線をとめておく必要があるため、視線の限定ありと評価した。非接触・非提示型のバイオメトリクスに関しては、顔以外は研究中であり、数年内に製品化される確証は得られていない。従って、環境変動の影響があるものの音声および顔が本人確認手段として最も適していると結論する。ただし環境変動の影響は実験的に確認する必要がある。

表 3　バイオメトリクスの比較

		利便性			安全性		備考
		操作	視線限定	認証時間	他人受入率	環境変動の影響	
非接触・提示	虹彩	無	有	1～3秒	0.0001%	小	製品・実績あり
	網膜	無	有	1秒程度	0.0001%	小	製品・実績あり
	音声(Keyword依存)	無	無	1～2秒	0.1%～数%	有	製品・実績あり
	音声(Free Keyword)	無	無	1分	0.1%～数%	有	製品あり
非接触・非提示	顔	無	無	2秒程度	0.1%～数%	有	製品・実績あり
	顔(3D)	無	無	不明	不明	有	研究中
	耳	無	無	不明	不明	有	研究中

このほか、指紋による本人確認はセンサへの接触を必要とするため、顔や音声に比較して利便性に劣るが、生体認証製品としての実績、および安全性が運用に依存しない利点から、顔や音声の代替案として位置付けられる。環境変動による精度への影響は小さいと予測されるが、代替案として調査の対象とすべきと考える。

3．2 端末間認証手段

アプリケーションサーバと車載端末間の相互認証の実現手段を検討するにあたり、(1) 相互認証方式、及び(2)相互認証と本人確認手段の連携を考慮する必要がある。(1) に関し、端末間の相互認証方式としては、対照暗号をベースにした Kerberos［7］や非対称暗号をベースにした PKI（Public Key Infrastructure）［8］が代表的である。本研究の端末間認証で対象とするアプリケーションサーバが、IP 網に設置されたものを含むことから、相互認証方式として公共性の高い PKI を採用すべきと考える。

(2) に関して、次の 3 つのモデルを想定し、2 節で示した要件に関して比較評価を行う。

① IC カード認証モデル：　IC カードに生体情報を保管し、車載端末で照合を行う

② クライアント認証モデル：　車載端末で生体情報の保管および照合を行う

③ サーバ認証モデル：　利用者認証サーバで生体情報を照合

図 1にこれらのシステムモデルの概要を示す。各モデルは、それぞれ、車載端末、基地局、路側網、アプリケーションサーバ、CA（Certificate Authority）局などからなる。CA 局は、利用者認証結果の完全性や安全性を保証する基盤技術を提供するのに必須となる。各モデルは、車載端末の構成やテンプ

レートの持ち方、認証シーケンスにそれぞれ特徴がある。

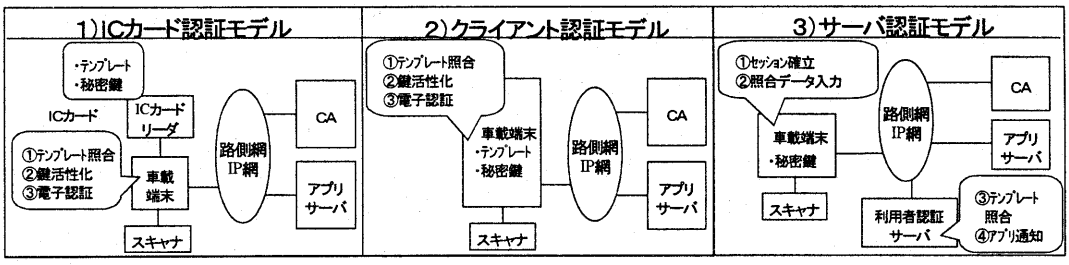

図 1 評価する利用者認証システムのモデル

IC カード認証モデルでは、利用者が車の持ち主（カーオーナー）でなくても、IC カードを持っていればサービスの提供を受けることが可能になる。クライアント認証モデルでは、該当する自家用車を運転する可能性のある人員分の利用者認証情報（テンプレート、証明書、秘密鍵）を確保する機能が必要である。サーバ認証モデルでは、利用者認証サーバが利用者のテンプレートを管理し、生体情報の照合を行う。このため利用者がカーオーナーでなくても認証可能である。以下、これらのモデルについて、利用者認証の要件に従って評価する。

利用者認証の応答時間としては、利用者認証を完了するまでの送受を含めた総通信量に比例する。①、②については、公開鍵の鍵長を 1024bit、鍵交換を Hand Shake プロトコルとすると通信量は 1～2Kbyte 程度であり、DSRC の有効転送速度を 325Kbyte/sec として転送時間は 0.01 秒以下と見積もられる。③は生体情報を転送する必要があり、その画像サイズを 200pixel×200pixel×8bit（40KB）とすると通信量は約 42Kbyte、転送時間は 0.13 秒となる。いずれも、利便性要件である 0.6 秒以下の条件を満たしている。

プライバシーに関して、クライアント認証型である①、②は、生体情報を車載端末側でクローズして処理するため、プライバシーは確保されていると考えられる。サーバ認証型の③は、他者にテンプレートを管理されている上、認証時にも生体情報を転送する必要があり、人によってはプライバシーの侵害を感じる可能性がある。

以上の評価結果を表 4に示す。

表 4 評価結果

評価要件（要求値）	システムモデル			備考（評価理由）
	①	②	③	
認証対象（カーオーナー）	◎	○	◎	①：カーオーナーなどに限定されない
応答時間（0.6 秒）	○	◎	○	②：フローが簡便である。
転送データ量（195KB）	○ 1.3KB	○ 1.3KB	○ 42KB	
プライバシー	○	○	×	③：テンプレートのサーバ管理

評価結果によると、①、②のシステムモデルの評価が高い。しかし①のモデルは、車載端末にＩＣカードリーダが必要となるため、コストの面で問題がある。従って②のモデルがスマートゲートウェイにおける利用者認証方式として適していると結論する。

4 生体認証の実用可能性検証実験

走行中の車内における顔、音声、指紋による生体認証の実用性検証、および走行中の車内環境が生体認証の精度に与える影響の明確化を目的に、実験を行った。

生体認証の精度を詳細に測定するには多数の被験者が必要となるが、今回の実験では、上記2点を目的としているため、厳密な精度評価に比べて実験の規模は小さい。具体的には、被験者12人による実験を行い、一般道あるいは自動車専用道において、助手席に乗車した被験者の顔画像、音声データ、指紋画像などの生体情報200セットと、温度、湿度、明るさ、騒音などの周辺環境を測定した。また比較のために同様のデータ収集を屋内でも行った。また、収集したデータから精度を評価し、生体認証の実用性および車内環境が精度に与える影響を検証した。

4．1 環境データ

データ収集は環境の変化による認証精度の比較のため、屋内と車内の2種類の環境で実施した。屋内および車内におけるデータ収集は、それぞれ10人および11人の被験者から、1人あたり5つずつ、合計50個および55個のデータを収集した。実用的な精度を評価するためにはさらに多くの被験者からデータを収集する必要があるが、屋内および車内データの比較は可能であると考える。

環境データのサマリを表5に示す。屋内データの収集場所は空調の設置されたオフィスであり、環境の変動は小さいのに対し、車内の環境は温度、湿度、明るさ、騒音ともに大きく変化する傾向が確認でき、特に明るさの変化が顕著である。

表5 環境データのサマリ

	屋内			車内		
	最小	平均	最大	最小	平均	最大
天候	小雨	晴/曇	晴	小雨	晴/曇	晴
気温（℃）	12	16	23	12	16	23
室温（℃）	22	22.5	23	10	20	25
湿度（%）（屋外）	31	46	57	31	46	57
湿度（%）（屋内）	34	36	38	31	46	57
明るさ（lx）	47	50	54	23	5750	56700
騒音（db）	44	52	55	51	63	77

4．2 精度評価

収集した生体情報を用いた精度評価に関して述べる。精度評価の方法は情報処理振興事業協会（IPA）策定の「精度評価ガイドライン」[3]に準じ、本人同士および他人同士の照合結果から、本人拒否率（False Rejection Rate：FRR）および他人受け入れ率（False Acceptance Rate：FAR）を計算した。ただし、本人同士の照合に関しては、データ数の不足を補うため、テンプレートに対して取得したデータ全てと照合を行っている。指紋、顔、音声の各照合の精度評価結果を、図2のROC(Receiver Operating Characteristic)カーブに示す。

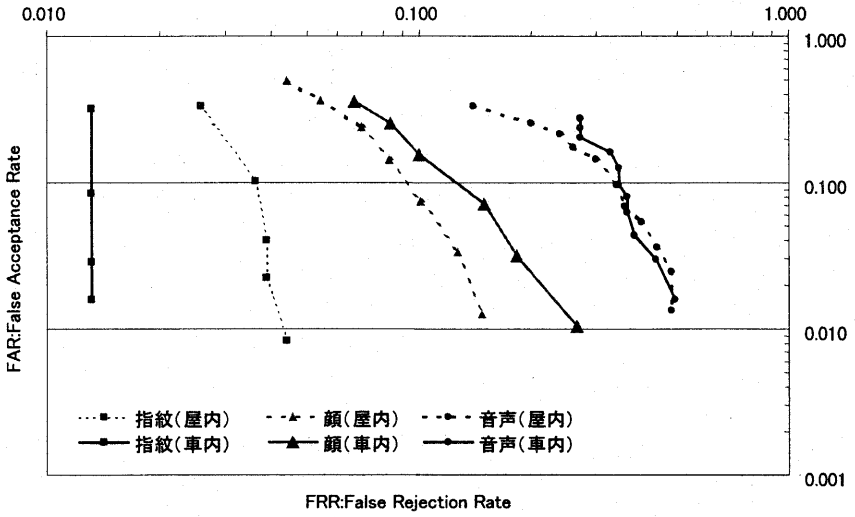

図 2　指紋、顔、音声のＲＯＣカーブ

顔照合の結果に関し、撮影環境を屋内から車内に変えることで、他人受入率を等しく設定した場合の本人拒否率は 1.5 倍程度悪化している。これは、屋内における照明の環境がほぼ一定であるのに対し、車内では走行によって常に照明環境が変化することによると考えられる。スマートゲートウェイにおける利用者認証の要求仕様である他人受入率 1%を達成するよう閾値を設定した場合、本人拒否率は 30%程度になると予想される。

音声照合の結果に関し、録音環境を屋内から車内に変えることで、他人受入率を等しく設定した場合の本人拒否率は 1.06 倍程度悪化している。顔照合に比較すると環境の変化に対する精度の影響が小さいが、これはノイズキャンセル機能付のマイクを使用しているためと考えられる。利用者認証の要求仕様である他人受入率 1%を達成するよう閾値を設定した場合、本人拒否率は 50%になると予想される。

指紋照合に関しては、車内における精度が屋内における精度を上回る結果となっているが、これは指紋照合の精度が顔照合や音声照合に比較して高いため、統計的な信頼性を十分に得るためのデータ数が不足していることによると考えられる。実質的には車内と屋内とで明確な精度の差はないと考える。指紋照合製品の実績から、他人受入率は 0.01%以下であるため、要求仕様の他人受入率 1%は十分に実現可能と言える。

以上の結果から以下を結論する。

(1) 走行中の車内における生体認証の実用性検証

顔、音声とも要求仕様である他人受入率 1%は達成できるが、単体では実用的な本人拒否率を実現できない可能性がある。

(2) 走行中の車内環境が生体認証の精度に与える影響の明確化

・顔照合では本人拒否率が 1.5 倍に悪化

・音声はノイズキャンセラにより環境の影響を抑制可能

・指紋における環境の影響はない

従って、生体認証をスマートゲートウェイの利用者認証に適用するには、以下の課題がある。

(i) 生体認証の精度向上

(ii) 車内の明るさの変化に対する顔照合のロバスト性向上

(i) に関しては、複数のバイオメトリクスを利用し、各々の照合結果を融合判定することで総合的な精度を向上するマルチモーダル生体認証技術［2］の適用が有効である。例えば、顔照合と音声照合の他人受入率をそれぞれ1%に設定し、単純なマルチモーダル生体認証技術を適用することでも、総合的な本人拒否率を10%、他人受入率を2%程度に改善することができる。さらに高度な融合判定技術を適用することで、実用的な本人拒否率を実現しつつ要求仕様を達成できる可能性がある。

(ii) に関しては、特殊なカメラの使用あるいは照明の影響を軽減する画像処理の適用などにより対処可能と考えられる。

5 まとめ

本研究では、スマートゲートウェイシステムにおける利用者認証の要件抽出、端末間認証手段および本人確認手段の評価、走行中の車内における生体認証の実用可能性検証実験を行った。その結果、PKIベースのデジタル認証および生体認証を連携した利用者認証方式が適していることを明らかにした。また、生体認証技術の実用可能性を評価した結果、他人受入率に関する要求仕様を実現するためには、マルチモーダル生体認証技術の開発が必要であることを明らかにした。

以上により、スマートゲートウェイシステムにおいて、特別な操作を要求せずハンズフリーで運転中のドライバーを認証する利用者認証システムの実用化の見通しをつけた。

なお本研究は、平成１２年度ＴＡＯ（通信・放送機構）の委託研究「走行支援システム実現のためのスマートゲートウェイ技術の研究開発」として行ったものである。

参考文献

[1] ARIB STD-T55: ELECTRONIC TOLL COLLECTION SYSTEM, 社団法人 電波産業会, 1999

[2] A.Jain, “Biometrics,” Kluwer Academic Publishers (1999)

[3] 情報処理振興事業協会 「精度評価ガイドライン」, http://www.sdl.hitachi.co.jp/ipa_biotest

[4] 運用要件策定ガイドライン http://www.sdl.hitachi.co.jp/ipa_biotest

[5] 東京防犯協会連合会 東京の犯罪発生状況,
http://www1a.mesh.ne.jp/TOBOREN/hanzaijokyo.html

[6] 警察庁編 平成10年度版警察白書,大蔵省印刷局 (1998)

[7] Kerberos: The Network Authentication Protocol, http://web.mit.edu/kerberos/www/

[8] 安藤訳、WEBセキュリティ＆コマース、オーム社 (1998)