

高齢者ドライバの安全を確認するシステムの提案

山岸 弘幸*, 寺澤 圭史, 鈴木 秀和, 渡邊 晃(名城大学)

Proposal of a Safety Confirming System of Senior Drivers

Hiroyuki Yamagishi, Keiji Terazawa, Hidekazu Suzuki, Akira Watanabe (Meijo University)

1. はじめに

ユビキタス社会において、「人」、「車両」、「道路」を情報通信技術によって一体化した ITS (Intelligent Transport Systems) が新しい交通システムとして今後注目されると考えられる。特に、ドライバに安心・安全を提供するサービスが年々増加している。しかし、高齢化社会が深刻化する中、高齢者ドライバを見守るためのサービスが不足している。本稿では、高齢者ドライバを抱える家族に安心・安全なサービスを提供する方式を提案する。

2. テレマティクス

テレマティクスとは、自動車などの移動体に通信システムを組み合わせ、リアルタイムに情報サービスを提供するシステムである。国内ではトヨタの「G-BOOK (1)」や日産の「カーウィングス」、海外では GM の「OnStar」など、各自動車会社が独自のサービスを展開している。特に、G-BOOK ではニュース・天気予報・交通情報の提供、オペレータサポートなど、様々なサービスが提供されている。

しかし、これらのサービスはすべてドライバ自身を対象としたサービスである。また、独自の管理センターを利用しており、一般ユーザには公開されていないクローズなサービス形態となっている。今後、高齢化社会が想定される日本では、高齢者ドライバの安全を家族がいつでも確認できるサービスが必要になると考えられる。

3. 提案方式

車内に設置されたカメラからのセンサ情報、およびカーナビゲーションの GPS 機能から取得した位置情報などをセンサボックスに収集する。その後、センサボックス内の情報を携帯電話経由でインターネット上のサーバに蓄積する。携帯電話網を経由して通信するため、どこからでも報告が可能である。センサボックスと携帯電話の間は Bluetooth で接続する。この方法では携帯電話網のセキュリティだけに頼ることができないため、センサボックスとサーバ間は確実な認証と暗号化通信を行う必要がある。ここで、暗号化通信には PCCOM (2) を用いることが可能である。サーバ側では通知された情報をユーザが閲覧しやすいように加工処理を行う。センサ情報の蓄積方法として、以下の 2 つの方式が考えられる。

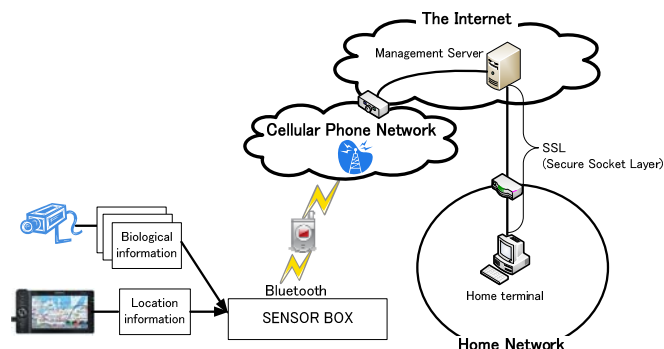


Fig.1. Gathering method 1

方式 1 : サーバ蓄積方式

センサボックスに収集した情報を定期的にインターネット上の管理サーバに記録する (Fig.1 参照)。管理サーバの内容は SSL を用いて、いつでもホームネットワークから閲覧することが可能である。この方法では、ホームネットワークの端末に特別なアプリケーションが不要である。

方式 2 : センサボックス蓄積方式

センサボックスにセンサ情報を蓄積しておき、情報を閲覧したい時にホームネットワーク側からセンサボックスに情報を要求する。この方式では、インターネット網に管理サーバを設置する必要はないが、端末側に専用のアプリケーションが必要である。

4. むすび

高齢者ドライバの安全を家族が確認できるシステムを提案した。今後は、センサボックスとサーバ間の認証方式、暗号化方式の詳細、提供アプリケーションの内容について検討する予定である。

文 献

- (1) “G-BOOK”, <http://g-book.com/pc/default.asp>
- (2) 増田. 他: “NAT やファイアウォールと共存できる暗号通信方式 PCCOM の提案と実装”、情報処理学会論文誌, Vol. 47, No. 7, pp. 2258-2266, 2006



高齢者ドライバの安全を 確認するシステムの提案

名城大学 理工学部

山岸 弘幸、寺澤 圭史、鈴木 秀和、渡邊 晃

研究背景

- ITS (Intelligent Transport Systems)
 - 「人」、「車両」、「道路」を情報通信技術によって一体化したシステム
 - 交通事故、渋滞などの道路交通問題を解決し、交通機能の利便性を向上させるシステム
 - 例：自動料金収受システム (ETC)
道路交通情報通信システム (VICS)
- テレマティクス (Telematics)
 - Telecommunication (通信) と Informatics (情報科学) の造語
 - 自動車などに通信システムを組み合わせて、リアルタイムに情報サービスを提供
 - 例：トヨタ「G-BOOK」、日産「カーウィングス」、GM「OnStar」など

G-BOOK

- **概要**

- 携帯電話やパソコン、車載器などから利用できるコンテンツサービス

- **サービス内容**

- MAP On Demand : 地図の更新サービス
- PROBE Communication : リアルタイムプローブ
- MUSIC On Demand : Bluetoothオーディオ搭載
- WEB On Demand : クルマとネットの融合サービス
- Safety & Security : ドライバの安心と安全を確保



ドライバー自身に対するサービス



ドライバーを見守るためのサービスが不足している！！

研究の目的

- 今後の高齢化社会
 - 高齢者ドライバを見守るサービスが必要
 - どこからでも、高齢者ドライバの現在の状態を知る
 - 蓄積情報：位置情報、生体情報
- セキュリティの確保
 - 個人情報の改竄、漏洩を防止



確実な認証、暗号化通信

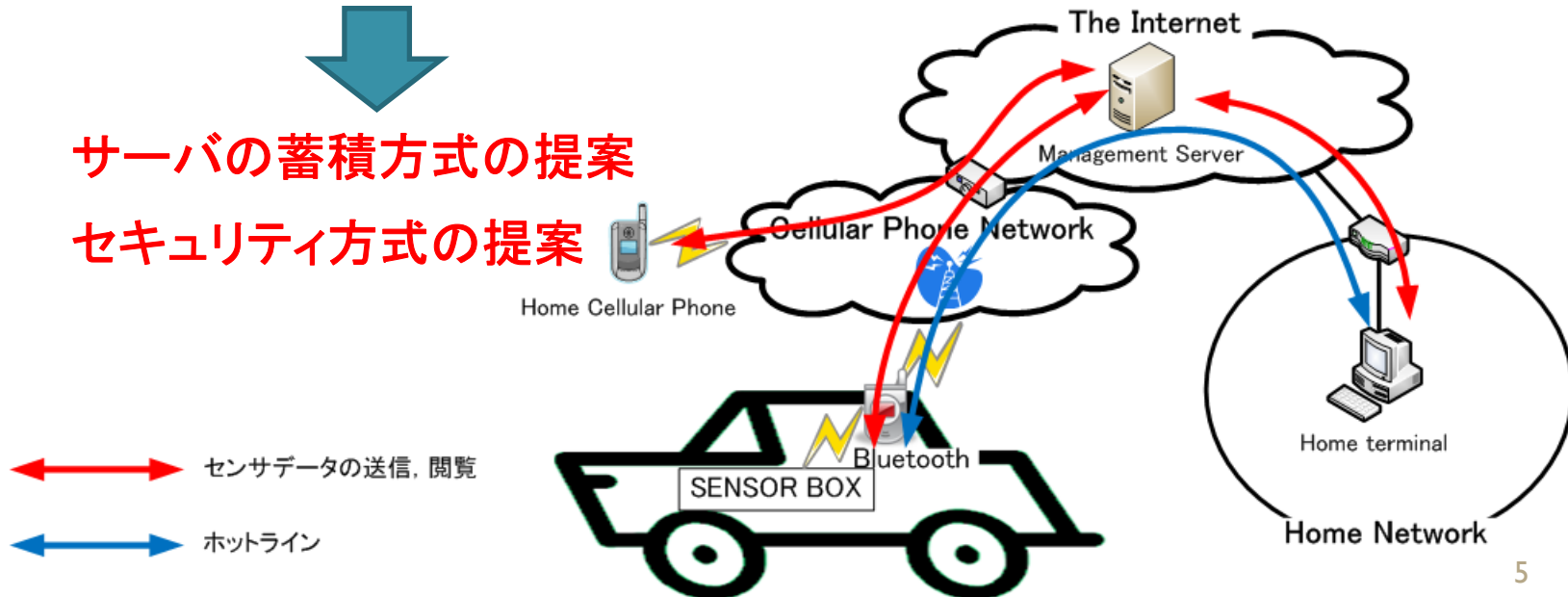
提案方式

- 概要

- センサボックスに蓄積情報（センサデータ）を収集
- センサデータはサーバに蓄積
- 携帯電話網を経由してセンサデータを送信
- 特定の人がサーバ情報を閲覧
- センサボックスと端末間にホットラインを確保

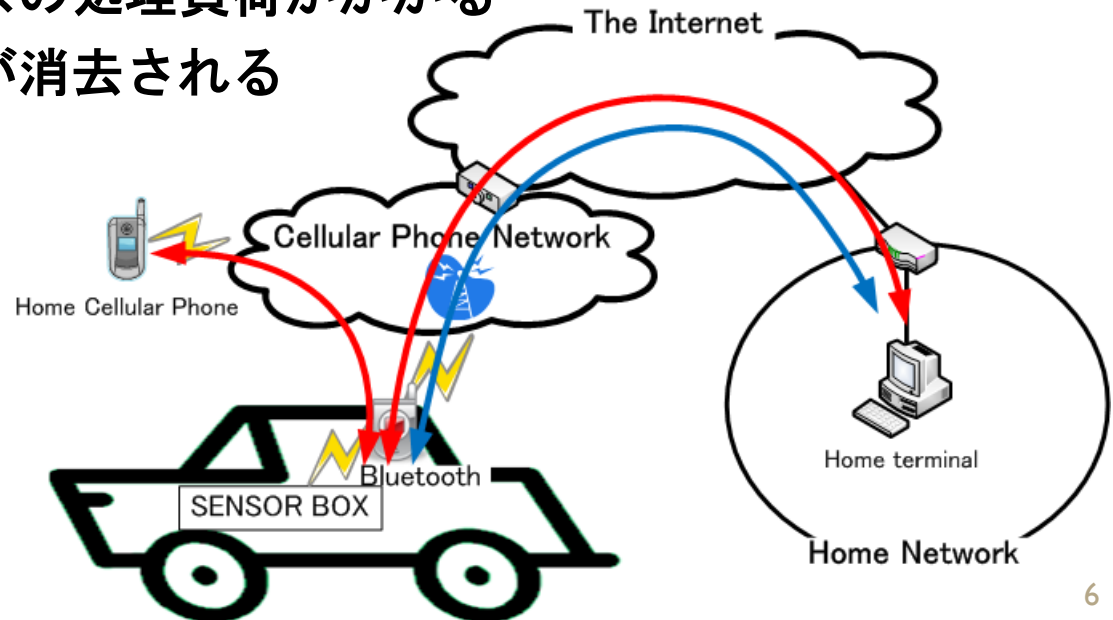
サーバの蓄積方式の提案

セキュリティ方式の提案



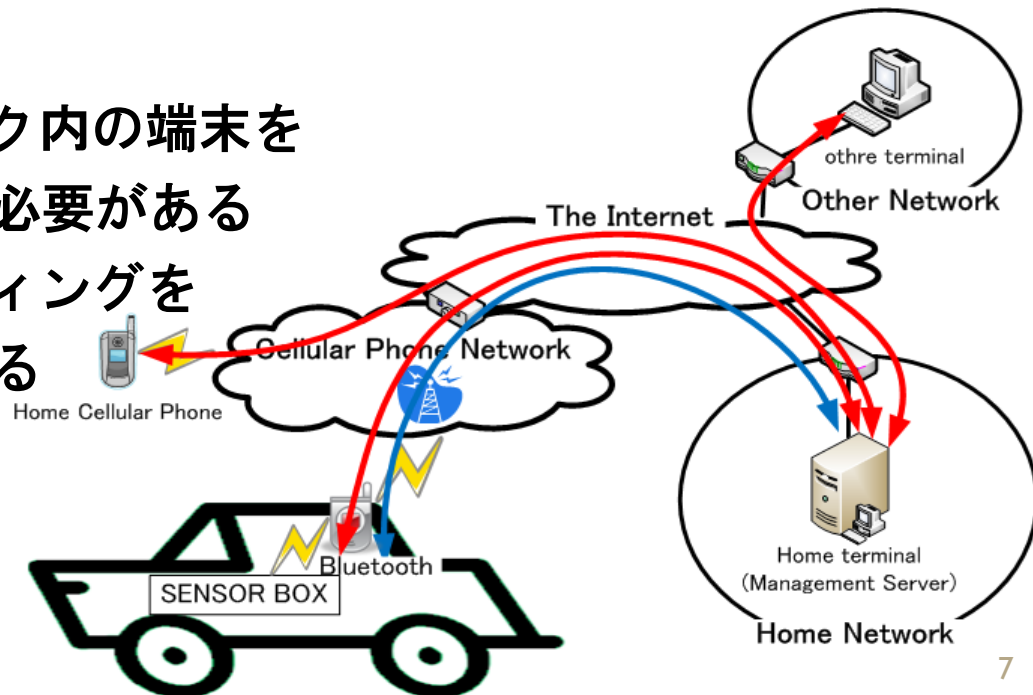
センサボックス蓄積方式

- センサボックスにサーバの機能を追加し、端末からセンサデータを閲覧する方式
- 利点
 - 閲覧したい時だけ、端末を起動すればよい
- 欠点
 - センサボックスの処理負荷がかかる
 - 過去のデータが消去される可能性がある



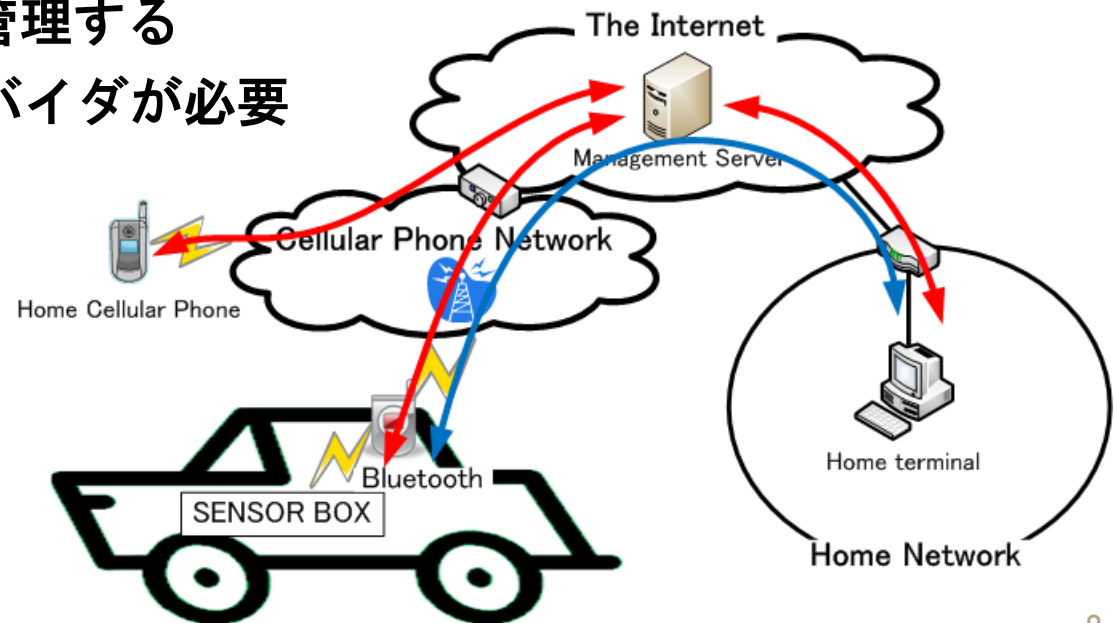
家庭端末蓄積方式

- ホームネットワーク内の端末をサーバとし、センサデータを家庭内のサーバに蓄積する方式
- 利点
 - どこからでも情報を閲覧することが可能
(但し、NATの設定が必要)
- 欠点
 - ホームネットワーク内の端末を常時起動しておく必要がある
 - ポートフォワーディングを設定する必要がある





インターネット蓄積方式

- インターネット上にサーバを設置し、センサデータを蓄積する方式
- 利点
 - どこからでも情報を閲覧することが可能
- 欠点
 - 管理サーバを管理するサービスプロバイダが必要



セキュリティ実現方式

- SSL (Secure Socket Layer)
 - 上位層で暗号化処理
 - サーバ側は公開鍵証明書が必要（クライアント側の環境に依存しない）
 - 利点
 - ・ 現在の環境に対応
 - ・ 端末に新しく機能を追加する必要がない  センサデータの送信、閲覧に利用できる可能性大
 - 欠点
 - ・ 処理速度が遅い、ホットラインで通信を行う際、双方に公開鍵証明書が必要
- PCCOM (Practical Cipher COMMunication) (※)
 - カーネル内で暗号化処理を行うオリジナルの暗号化技術
 - 利点
 - ・ NATを通過できる
 - ・ アプリケーションに依存しない  ホットラインに利用できる可能性大
 - 欠点
 - ・ カーネルの改造が必要

※ 増田、他:「NATやファイアウォールと共存できる暗号通信方式PCCOMの提案と実装」、
情報処理学会論文誌Vol. 47、No. 7、pp. 2258-2266、2006

むすび

- **まとめ**
 - ITSとテレマティクスの概要を説明
 - サーバの蓄積方式を提案
 - 個人情報改竄、漏洩を防ぐセキュリティ技術
- **今後の検討課題**
 - サーバの蓄積方式の選定
 - 認証、暗号化方式の選定
 - 携帯電話網を経由した通信の実装

ご清聴ありがとうございました

付録 暗号化方式の比較

	SSL	PCCOM
処理速度	×	○
証明書	× (必要)	○
カーネル改造	○	× (必要)
エンドサーバ通信	○	△ (改造要)
エンドエンド通信	×	○
汎用性	× (HTTPのみ)	△