情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2014-GN-90 No.2
Vol.2014-CDS-9 No.2
Vol.2014-DCC-6 No.2
2014/1/23

スマートフォン連携車載機における匿名個人データの引継ぎ・集約方式の提案

清水淳史[†1]　松本貴士[†1]　永井靖[†1]

スマートフォン連携車載機においてサーバ型の通信サービスを更に使いやすくしていくためには，(1)ユーザがユーザ登録操作を車両内で行うことなくサービスを利用開始でき，(2)ドライブ中に使用する各サービスの匿名個人データ(走行履歴や地点登録情報など)をユーザ登録時に集約し，(3)ユーザ登録後も継続的に参照できることが必要である。筆者らはこれら要件を実現するために，１）サービスを実現する各スマホアプリに固有ＩＤを付与し，２）固有ＩＤと匿名個人データとを紐づけてセンタで保持し，３）初回ユーザ登録時に固有ＩＤとユーザＩＤとを紐付けることで匿名個人データをユーザＩＤに引継ぎ・集約する機能を開発した。評価により，従来技術のCookieを拡張する端末側蓄積方式を採用した場合はユーザ登録時のスマホアプリとサーバ間の匿名個人データの伝送によってユーザ待ち時間を生じてしまうのに対して，提案方式はユーザ待ち時間をほぼ0とすることで利便性が高いことを確認した。

Proposal on Taking-over and Aggregation Method of Anonymous Personal Data for In-Vehicle Terminals that Cooperate Smartphones

There are three requirements for improving usability of server-oriented communication service on In-Vehicle Terminals that cooperate smartphones. The first requirement is utilizing services by users without login operation in vehicles. The second requirement is aggregation of each service's anonymous personal data on an user registration process. The third requirement is that the data must be able to be referred by the users continuously after the process.
To realize these requirements, we developed the function that 1) assigns unique ID to each smartphone application, 2) stores anonymous personal data that is bound with the unique ID, 3) aggregates the anonymous personal data and takes over the data to a newly registered user ID. In the evaluation, we compared the conventional method (terminal side storing method which was implemented using Cookie) and the proposed method. As a result, whereas in the case with the conventional method, the method forces users to wait for the closing anonymous personal data transmission duration, in the case with the proposed method, the method forces users almost no waiting duration.

ATSUSHI SHIMIZU[†1]　TAKASHI MATSUMOTO[†1]
YASUSHI NAGAI[†1]

-
‘

1. はじめに

スマートフォン（以下，スマホ）のアプリケーション（アプリ）を車両内で活用するという顧客ニーズに応え，スマホ連携車載機が製品化されている。ユーザはスマホ連携車載機を使用して，車両内でサーバ型サービスを利用することができる。

スマホ連携車載機とは，ユーザが車載機とスマホとを接続し，車載機ディスプレイに出力されるスマホの画面を見ながら，車載機からスマホのアプリを制御することができる車載機である。

スマホ連携車載機を利用する環境は，オフィスなどでPCを利用する環境とは異なり，ユーザ操作のための動作に制約がある。このため，ユーザがサーバ型のサービスを簡易に利用するための，新しいサービスの利用方法が求められている。1)

本研究では，従来のPCなどで従来行われてきたユーザIDとパスワードをセンタに事前登録してサービスを利用する方式とは異なり，車両内においてスマホ連携車載機を活用する場合にユーザ登録なしでサービスの利用を開始する方式を提案する。

2. スマホ連携車載機の要件

2.1 スマホ連携車載機の概要

（１）スマホ連携車載機

車載機画面からスマホアプリを操作し，スマホ画面出力を車載機ディスプレイに出力する技術として Mirror Link 2)がある。CE4A 3)は，Mirror Link の仕様として Terminal Mode を提唱している。Terminal Mode はあるデバイスから遠隔でもう一方のデバイスを操作するためのインタフェースを規定している。その適用範囲には車載機とスマホが含まれており，その中ではスマホ連携車載機が提案されている。

スマホ連携車載機は以下のように動作する。

†1 (株)日立製作所 横浜研究所
Hitachi, Ltd., Yokohama Research Laboratory

Vol.2014-GN-90 No.2
Vol.2014-CDS-9 No.2
Vol.2014-DCC-6 No.2
2014/1/23

① スマホは自端末の画面出力を，Bluetooth または USB などの通信路を介して車載機に伝送する。

② 車載機はユーザによる車載機ディスプレイのタッチ操作イベントを，スマホ画面を操作するためのコマンドに変換し，スマホに送信することでスマホアプリを操作する。

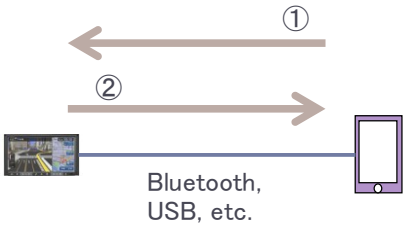

図 1　スマホ連携車載機
Figure 1　System Consisting of In-Vehicle Terminal and Smartphone

（2）スマホ連携車載機のサービス例

車両内で活用することを想定したセンタ型サービスとして地点登録サービスがある。地点登録サービスとは，ユーザが地点情報（ドライブ途中にスマホで撮影した写真データと車両の走行履歴とによって構成される）をサービスサーバに記録し，サービスサーバの地図と重ね合わせ，旅の記録として，端末（スマホ連携車載機）から継続的に参照できるようにするサービスである。

地点登録サービスは，①ユーザが車外でスマホに搭載されたカメラを使用して撮影した写真データ，②ドライブ中の車両の走行履歴という，２種類のデータを活用する。

これらデータは，車外と車内という異なる利用シーンで取得されるデータである。このため，ユーザの利便性を考慮すると，これらデータを取り扱うスマホアプリとサービスの組み合わせの各々である「①'カメラアプリおよび写真蓄積サービス」と「②'走行履歴取得アプリおよび走行履歴蓄積サービス」は、①'と②'とが独立した形態で実装されることが望ましい。

上述のように，利用シーンとそこでのユーザの利便性を優先すると，①'と②'が独立した形態で実装されることが望ましいが，一方で，地点登録サービスとしては①のデータと②のデータを集約(マージ)してユーザに対して閲覧可能とする必要がある。

（3）ユースケース

前記のような特徴を持つ地点登録サービスを利用するためのユースケースを図 2 で説明する。ユーザは地点登録サービスを以下のように利用する。

ユーザは，車に乗車してスマホにダウンロードしておいた②'走行履歴取得アプリを起動し，走行履歴をサーバに蓄積しつつ目的地に向かう。次に，ユーザは目的地に到着し，そこで①'カメラアプリを起動して景観の写真を撮影する。最後に，ユーザは自宅に戻り，スマホから走行履歴(及び地図)と写真を重ね合わせて閲覧する。

ユーザは，それぞれのサービスを利用する際に，スマホアプリを起動(ＵＣ１：初期登録)し，データをセンタに蓄積(ＵＣ２：サービス仮利用)する，という一連のユースケースを実施する。また，例えば自宅に戻った後等に，何れかのスマホアプリからユーザＩＤを登録(ＵＣ３:本登録)する。

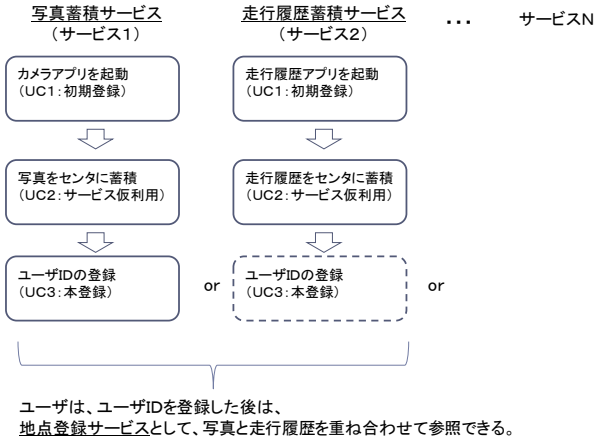

図 2　ユースケース
Figure 2　Use-Case

上記のユースケースにおいて，ユーザの利便性を高めつつサービス提供していくためには，以下の課題がある。

（課題１）ユーザは，センタにデータを蓄積するタイプのサービスである写真蓄積サービスや走行履歴蓄積サービスを，ユーザ登録操作無しに手間無く使い始められること。

（課題２）ユーザは，自宅に戻りユーザ登録した後に，ユーザ登録前にセンタに登録しつつ利用していたデータ（写真と走行履歴）を，引き続き参照できること。ユーザ登録操作は，いずれかのアプリから単一回のみで済ませられること。

（課題３）ユーザが同一のスマホから利用する異なる２つのサービス（①'写真蓄積サービス，②'走行履歴蓄積サービス）のデータを，手間なく集約(マージ)できること。

2.2 スマホ連携車載機に求められる要件

スマホ連携車載機においてセンタ型サービスを更に使いやすくしていくためには，以下が必要である。

前述の（課題１）より（要件１）を，（課題２）より（要件２）を，（課題３）より（要件３）を導いた。

Vol.2014-GN-90 No.2
Vol.2014-CDS-9 No.2
Vol.2014-DCC-6 No.2
2014/1/23

（要件１）ユーザが，所望のサービスとそれを実現するスマホアプリとを，車両内で事前準備することなく簡易に利用できる仕組みが必要である。事前準備とは，①スマホアプリのダウンロード，②センタへログインするためのユーザ ID やパスワードの入力等である。

ここで特に，②については，ユーザがサーバにユーザ ID 登録を行っていない状態であっても，前記のサービス例のような，サーバにユーザのデータを登録しつつ利用するタイプのサービスを利用開始できることが望ましい。

（要件２）現行のサービスの多くは，ユーザがサービスでサーバに登録して利用するデータをユーザ ID と紐付けて管理することを前提としている。このため，ユーザがユーザ登録していない（又は，ログインしていない）状態でセンタに登録したデータについては，ユーザがサービスの利用を終了した後は，ユーザと無関係なデータとしてしか扱えない。即ち，サービスを提供するサーバは，上記のようなデータを匿名または特定の個人の記録として管理していくことができない。

このため，ドライブ中にユーザが車両向けのサービスで使用する走行ログや地点登録情報などの匿名個人データ（以下，記録と呼ぶ）をユーザ登録の際にユーザ ID と紐付けて引継ぎ，各ユーザが自身の個人の記録として継続的に参照できる仕組みが必要である。

さらに，ユーザが単一のスマホで複数のサービスを利用していた場合であっても，ユーザの利便性を考慮すると，ユーザ登録操作は何れかのスマホアプリを介して単一回のみで済ませられる必要がある。

（要件３）ユーザは，単一のスマホから複数の異なるサービスを使用することが想定されるため，各サービスで登録した個人の記録をユーザ登録時に集約できることが必要である。

3. 先行研究

従来のユーザ ID とパスワードを事前登録することによりユーザ登録する方法は，ユーザによるサービス利用開始の障壁を高めてしまうため，この課題に取り組んだ研究がある。

例えば，ユーザがサービス利用に必要なユーザ属性情報を，オンデマンドにサービスプロバイダ間で共有することを許可し，新規サービスにユーザ登録する場合に必要な情報を既に登録してあるサービスから引用することでユーザの入力の手間を省く方式が提案されている。4)

4)で紹介されている OAuth 等のアイデンティティ連携方式は，ユーザ ID とパスワードを登録する手間を省くことができる。しかし，車両内での一定の長さのある数字，文字，句読点を組み合わせたパスワードを入力する操作が必要とされる。この操作を車両内で行うのは困難であり，（要件１）を満たすことができない。

また，ユーザが端末から Web サイトにアクセスしてサービスを利用する時に，Web サイトが（１）端末に対して Cookie 5) と呼ばれるデータを送信し，（２）Cookie に対応するユーザの操作履歴を記憶しておくことで，ユーザが前回 Web サイトで行った操作履歴を再現する方式がある。

しかし，この Cookie は，ユーザがスマホで撮影した写真データや車両の走行履歴などの Web サイト外で生成されるデータと紐付けて管理することは想定されておらず，サーバにユーザのデータを登録しつつ利用するタイプのサービスを利用開始することができないため，（要件１）を満たすことができない。

また，学内情報システムの一時利用者に対して，本人が日常的に利用している交通系 IC カードやプリペイド決済用 IC カードを用いて PIN コードを発行する方式が提案されている。6)

6)では，一時利用者は，各々が所有するＩＣカードに記憶されるデータを基にシステムが発行した PIN コードでサービス利用を開始することができる。しかし，サービス利用を開始した後，より多くのサービスを利用できる上位のユーザに移行した場合に，サービス利用時のデータを上位のユーザに引き継ぐことは考慮されていないため，（要件２）を満たすことができない。

また，（要件３）を課題として取り組んだ研究例は無い。

それぞれの先行研究の要件への対応状況を表 1 に示す。

表 1　先行研究の要件への対応状況

Table 1　Precedence Research vs. Requirements

	要件１	要件２	要件３
アイデンティティ連携方式（OAuth 等）4)	×	○	×
Cookie5)	×	×	×
一時利用者向け認証システム 6)	○	×	×

また，上記の Cookie に機能付加することで機能面での（要件１）～（要件３）を満たそうとしても，ユーザはサービスのサーバに端末側で生成されるデータを蓄積しつつサービスを利用することができない。このため，ユーザは（１）端末側で生成されるデータをサーバに対して送信し

Vol.2014-GN-90 No.2
Vol.2014-CDS-9 No.2
Vol.2014-DCC-6 No.2
2014/1/23

てサービスを利用し,(2)サービスを利用し終わった後は,再度，サーバから端末にデータをダウンロードして蓄積した後に,(3)端末上のサービス利用のためのアプリケーションを終了することとなる。このため，上記の送信とダウンロードにおいて，ユーザに待ち時間が発生してしまうという性能面での課題がある。

そこで，本研究では，機能的な（要件１）～（要件３）の全てを満たしつつ，利用時の性能面での課題を解決してユーザの利便性を高めるための方式を提案する。

4. 提案方式

関連技術に新たな機能を付加して要件を満たす方式を提案する。提案方式のシステム構成を図 3 に示す。

システムは，サーバ側のサービスサーバとアプリサーバ，端末側のスマートフォンによって構成され，3G， LTE，インターネットなどの通信回線を介して接続される。

サービスサーバは，スマホアプリへのサービスの配信とアプリ ID の配布を行う。ここで，サービスサーバは，同一のサービスを提供するアプリであっても，当該アプリを搭載するスマホの個体が異なる場合には，それぞれ異なる固有の値をアプリ ID として各スマホアプリに対して割り当てる。また，サービスサーバにログインするユーザを認証するためのユーザ ID とパスワードを保持する。

アプリサーバは，スマホへのスマホアプリの配信を行う。

スマホ上ではアプリ管理部が動作する。このアプリ管理部は，スマホ上の複数のスマホアプリに対して起動要求を送信するなどの制御，サービスサーバにユーザ登録やログインを行うためのユーザインタフェース画面の提供，ダイジェストデータ（後述）の保持を行う。

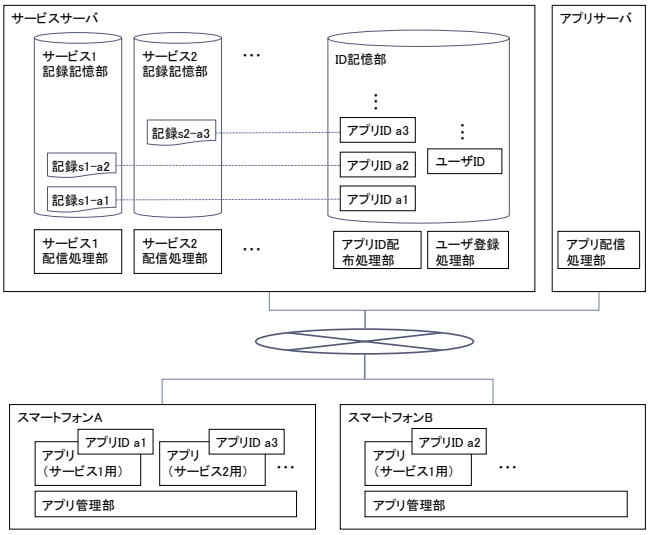

図 3　システム構成
Figure 3　System Configuration

4.1 ユーザ登録なしサービス利用開始機能

（要件１）を満たすためにユーザ登録なしサービス利用開始機能を開発した。

本機能は図 4 に示す以下のステップで実現する。

(1) ユーザは車外で事前にアプリサーバからダウンロードしたスマホアプリを，車内で起動する。サービスサーバは，スマホアプリが初回起動される場合に，スマホアプリに対してアプリ ID (a1, a2, …) を付与する。(a1: application ID 1）次にユーザは，スマホと車載機とを無線又は有線で接続する。

(2) サービスサーバは，ユーザがアプリ利用中に記録を記録記憶部に蓄積する。記録は，個々のスマホアプリに固有に付与されたアプリ ID （s1-a1, s2-a3, …）に紐づけて蓄積される。(s1: service ID 1)

上記により，サービスサーバは従来のようにユーザ ID に紐付けて記録を管理する代わりに，アプリ ID に紐付けて記録を管理することができるようになる。

このようにして，ユーザはユーザ登録を行うことなくて，サーバにユーザのデータを登録して利用するタイプのサービスを利用開始でき，（要件１）を満たすことができる。

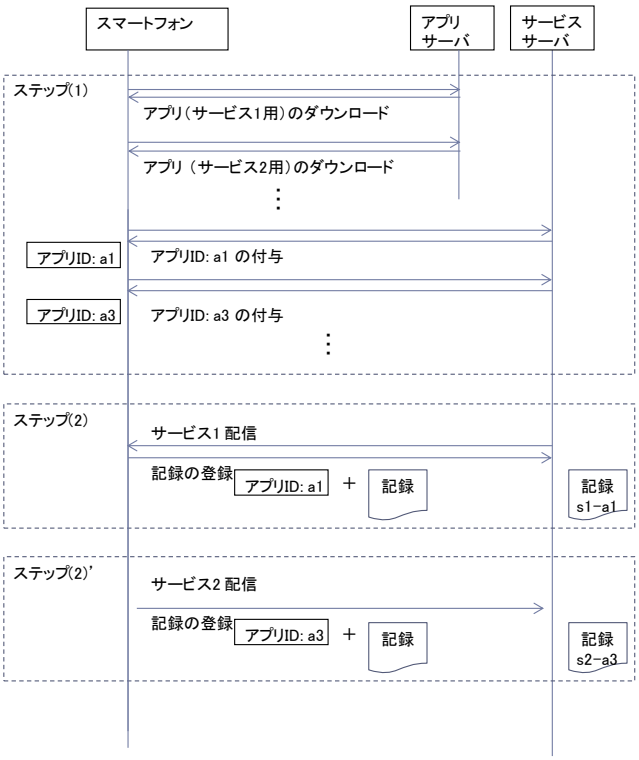

図 4　シーケンス図(ステップ(1) (2))
Figure 4　Sequence Diagram (Step (1), (2))

Vol.2014-GN-90 No.2
Vol.2014-CDS-9 No.2
Vol.2014-DCC-6 No.2
2014/1/23

4.2 匿名個人データの引継ぎ機能

（要件２）を満たすために匿名個人データの引継ぎ機能を開発した。

本機能は図 5 に示す以下のステップで実現する。

(3) サービスサーバは，ユーザがスマホアプリを終了する時に，スマホに対して記録を引継ぐ際に利用するダイジェストデータ（s1-a1, s2-a3, …）を送信する。それぞれのスマホアプリは受信したダイジェストデータをアプリ管理部に引き渡す。

(4) ユーザはスマホのアプリ管理部から初回ユーザ登録した時に，ダイジェストデータの全てをサービスサーバに送信する

(5) サービスサーバは受信したダイジェストデータに対応するアプリ ID を検索し，当該アプリ ID に対応する記録の全てをユーザ ID に紐づけて引継ぐ。

上記により，サービスサーバは，アプリ ID と紐付けられていたユーザがユーザ登録していない（又は，ログインしていない）状態でセンタに登録していた記録を，新たに登録されたユーザ ID と紐付け直すことができるようになる。

このようにして，（要件２）を満たすことができる。

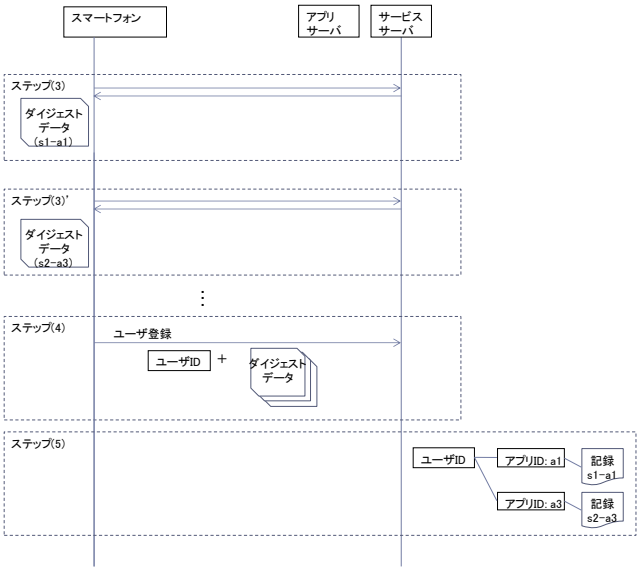

図 5　シーケンス図(ステップ(3) (4) (5))
Figure 5　Sequence Diagram (Step (3) (4) (5))

本機能において使用するダイジェストデータを式 1 に示す。ダイジェストデータはサービスサーバにおいて，単一スマホに搭載される複数アプリのそれぞれのアプリ毎に生成する。表 2 にダイジェストデータ生成のためのパラメータおよびその値を示す。

LEFT (Hash（アプリ ID, 有効期限付き ID）,N)
…　式 1

Hash：　ハッシュ関数
LEFT（data, N）：　data の先頭 N バイトを抽出

表 2　ダイジェストデータのパラメータ
Table 2　Parameters for Digest Data

パラメータ名称	値
アプリ ID	64 バイト
有効期限付き ID	64 バイト
有効期限	3 日

以降で，ダイジェストデータを実運用するための詳細を説明する。

（ダイジェストデータの衝突回避）

サービスサーバは生成したダイジェストデータと同値のダイジェストデータがあり，その有効期限が切れていない場合は，再度ダイジェストデータを生成することで値の衝突を回避する。

（ダイジェストデータを消去するタイミング）

各アプリは，ユーザがサービスおよびアプリの利用を終了し，ダイジェストデータをアプリ管理部に引き渡したタイミングで，これを自身の一時記憶域から消去する。アプリ管理部は，各アプリから受信したダイジェストデータを永続記憶域に保持し，サービスサーバにダイジェストデータを送信したタイミングでこれを消去する。サービスサーバは，記録をユーザ ID に引き継いだタイミング，または，ダイジェストデータ生成に利用した有効期限付き ID が有効期限を迎えたタイミングでこれを消去する。上記により，不要となったダイジェストデータがサービスサーバやスマホに蓄積されることを防ぐ。

4.3 匿名個人データの集約機能

（要件３）を満たすために匿名個人データの集約機能を開発した。

本機能は図 5 のステップ(5)において実現する。

ステップ(5)において，ユーザが単一のスマホで複数のサービス（サービス 1，サービス 2，…）を利用していた場合には，アプリ管理部はそれら複数のサービスに対応するダイジェストデータをサービスサーバに対して送信する。サービスサーバはこれら複数のダイジェストデータに紐づけられている記録を集約してユーザ ID に引き継ぐ。

Vol.2014-GN-90 No.2
Vol.2014-CDS-9 No.2
Vol.2014-DCC-6 No.2
2014/1/23

上記により，アプリ管理部は複数のサービスに対応するダイジェストデータを，それらサービスに対応するそれぞれのスマホアプリから集約する役割を果たすことができるようになる。

このようにして，サービスサーバは集約されたダイジェストデータをユーザ登録時に把握することができるようになり，（要件３）を満たすことができる。

さらに，以下により，ユーザは記録を継続的に集約し続けることができる。

- スマホのアプリ管理部は，ユーザが初回ユーザ登録の後にログインする度に，各スマホアプリがセンタから受信して保有しているダイジェストデータを集約し，これら複数のダイジェストデータをセンタに送信する。
- センタは受信した複数のダイジェストデータとログイン時にユーザが入力したユーザ ID とを紐付ける。

5. 実システム運用における課題の解決方法

本章では，提案方式を実システムで運用するための前提となるサービス提供方針の策定，および，それぞれのサービスサーバで記憶するデータ（記録）の管理方式の策定を行う。

5.1 電子認証の保証レベルとサービス提供方針

NIST, ISMS は保護するべき情報をレベル分けし，それに見合うレベルで情報を管理することで情報の安全性を担保する電子認証の保証レベル（表 3）を定義している 7)8)9)。

定義によれば，保証レベル 2 であれば課金サービスを提供する際に必要とされるユーザ情報や個人データを取り扱うことが可能であるが，保証レベル 1 では漏洩時の被害が小さい個人データのみ取り扱うことができる。

表 3　保証レベルの定義
Table 3　Definition of Assurance Level

レベル	定義	解説
1	主張するアイデンティティの正当性の信用が（ほとんど）ない	主張するアイデンティティの正当性の信用が（ほとんど）ない状態。例えば，自己登録ＩＤとパスワードの利用によるサービスの利用等がこれにあたる。
2	いくらかの信用性	全般的に見てある程度の正当性が主張するアイデンティティに存在する状態。初期にアイデンティティの確認を必要とする公的サービスにおいて広く適用が可能である。誤認証によって起こる影響が一時的なもので済むような場合等がこれにあたる。
3	高い信用性	アイデンティティの正当性主張において高い信頼性を必要とする処理に適している。例えば特許申請時での特許情報の送信等，秘密情報の開示が競合相手に大きな利益を生ませるような場合に適用される。また，その財政ロスは重大ではあるが，壊滅的ではなくレベル４ は妥当ではない場合等。
4	とても高い信用性	アイデンティティ正当性の主張において大変に高い信頼性を必要とする処理に適している。例えば法執行機関における犯罪情報を含んだデータベースへのアクセス等，情報が開示したときに多大な問題を起こす場合等。

このため，保証レベルを考慮しつつユーザをサービスに導入する方針として，以下を策定した。

ユーザを匿名個人として識別（保証レベル 1 相当）して非課金サービスを提供することにより，ユーザをサービスに導入する。次に，ユーザにユーザ登録を実施してもらい，ユーザＩＤとパスワードに基づく認証（保証レベル 2 相当）によってユーザを特定して課金サービスを継続的に提供する。（図 6）

近年，基本的なサービスや製品を無料で提供し，さらに高度な機能や特別な機能について料金を課金するフリーミアム 10) と呼ばれるビジネスモデルが提唱され，そのコンセプトに基づくサービスシステムが普及しているが，本研究で策定した上記の方針はその一つとして位置づけられると考える。

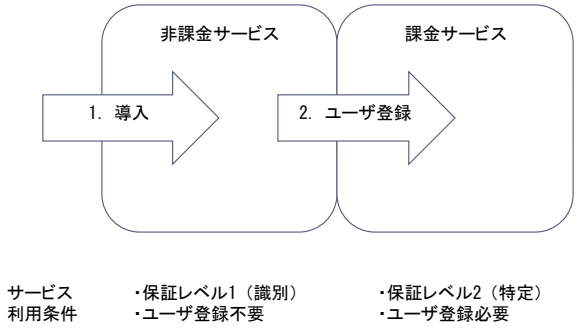

図 6　ユーザをサービスに導入する方針
Figure 6　Policy for Leading Users to Services

上記の方針を前提としてそれぞれのサービスを提供する際には，サービスサーバは，上記の遷移前と遷移後のそれぞれの保証レベルにおいて取扱いが許容される個人データのみを，ユーザから収集する方針とする。

5.2 記録の有効期限

システムを実運用可能とするために，以下の記録の運用方針を策定した。

フリーミアムでは，①サービス利用開始の障壁を下げ，まずは多数のユーザをサービスに誘導することでサービスの価値を高め，②その高めた価値を提供しつつ正規ユーザ

を獲得し，③これら正規ユーザに高度なサービスを有料で提供するという一連のサイクルを想定する。

本研究でもこのフリーミアムの考え方を採用し，ユーザが正規ユーザとなる前から記録をサービスサーバに登録するサービス提供方針をとっている。この方針における課題として，正規ユーザ登録を行わないユーザが多数存在する場合，サーバにユーザIDに引き継がれない記録が蓄積されてしまうという点が挙げられる。このため，これら蓄積されるデータの有効期限を規定してサービス提供する必要がある。

既存のフリーミアムサービスの例として，フリーメールサービスがある。これらは無料で使用開始できるが，サーバが収容するメールデータを一定量以下に抑えるために，例えば「３ヶ月間ログインなしの場合データ（メール）を消去する」という前提のもとでサービス提供している。本研究においてもこの前提の置き方を採用し，記録の有効期限を設定した。

6. 評価

6.1 利便性の評価

ここでは，提案方式の利便性を評価する。

先行研究の章で述べたアイデンティティ連携方式やCookieなどの既存技術では，端末側で生成される地点情報のようなデータを，サーバで管理することを想定していない。このため，ユーザがサービス利用中にサーバに蓄積しつつ利用した各サービスの記録を，次回にユーザがサービスを利用する際にも継続的に利用できるようにするためには，サービス利用の終了時に一旦スマホにダウンロードして蓄積しておく必要がある。

このスマホ側で記録を蓄積する方式を Cookie を拡張することで実現する方式を端末側蓄積方式と呼び，提案方式と比較する。

利便性を評価するために，それぞれの方式の操作ステップにおける所要時間を試算した。

（端末側蓄積方式）

(1)　ユーザは車外で事前にアプリサーバからダウンロードしたスマホアプリを，車内で起動する。サービスサーバは，スマホアプリが初回起動される場合に，Cookie をスマホアプリに送信する。次にユーザは，スマホと車載機とを無線又は有線で接続する。

(2)　サービスサーバは，ユーザがアプリ利用中に記録をCookie と紐付けて一時的に蓄積する。

(3)　サービスサーバは，ユーザがスマホアプリを終了する時に，スマホに対して記録を送信する。それぞれのスマホアプリは受信した記録をアプリ管理部に引き渡す。

(4)　ユーザはスマホのアプリ管理部から初回ユーザ登録した時に，アプリ管理部が蓄積している記録の全てをセンタに送信する。

(5)　サービスサーバは受信した記録の全てを，ユーザ ID に紐付けて引き継ぐ。

提案方式と端末側蓄積方式の相違点を以下，および，Figure 7 に示す。

提案方式のステップ(3)では，サービスサーバはスマホアプリに対して，各サービスに対応するダイジェストデータを，アプリ ID を紐付けたうえで，スマホアプリに対して送信する。これに対し，端末蓄積方式のステップ(3)では，サービスサーバはスマホアプリに対して，各サービスに対応する記録をスマホアプリに対して送信する。

提案方式のステップ(4)では，アプリ管理部が，各スマホアプリから受信したダイジェストデータを集約してサービスサーバに対して送信する。これに対し，端末側蓄積方式のステップ(4)では，アプリ管理部が各スマホアプリから受信した記録を集約してサービスサーバに対して送信する。

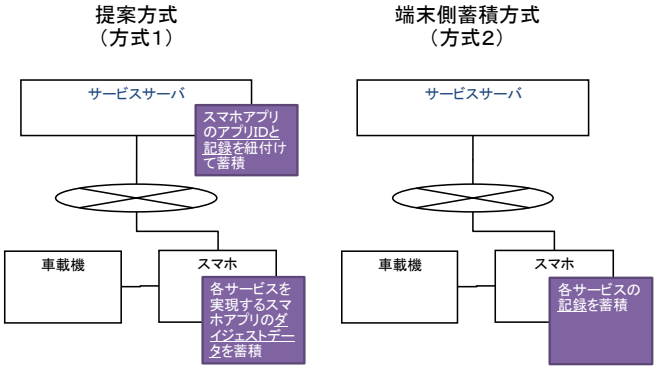

図 7　提案方式と端末側蓄積方式の比較

Figure 7　Proposed Method vs. Client Side Storing Method

提案方式と端末側蓄積方式，それぞれの操作ステップにおける所要時間を試算した。所要時間として，①ユーザ操作に必要な時間，②スマホ⇔サービスサーバ間のデータ伝送待ち時間がある。①については，両方式間で差異が無く，②については差異が有るため，②を比較した。（表 4）

試算では，表 5 のパラメータを前提とした。各アプリの記録の平均データ量（10MByte（B））については，地点登録サービスにおける写真（複数枚）のデータ量と走行履歴のデータ量とを合算した。

端末側蓄積方式はステップ(3)とステップ(4)のそれぞれにおいて，27 秒，533 秒の待ち時間が発生してしまう。これに対し，提案方式はデータ伝送待ち時間がほぼ発生せず，ユーザを待たせることの無い利便性が高い方式と言える。

表 4　データ伝送待ち時間の比較

Table 4　Comparison of Data Transfer Wait Time

操作 ステップ	スマホ⇔サービスサーバ間 データ伝送待ち時間	
	提案方式	端末側蓄積方式
(1) (2)	―	―
(3)	サービス利用終了時に, スマホアプリにダイジェストデータを伝送。 （c: 4B ） **約 0 秒**	サービス利用終了時に, スマホアプリに記録を伝送。 （b: 10MB） **27 秒**
(4)	サーバに複数のダイジェストデータを伝送 （a×c: 80B） **約 0 秒**	サーバに複数の記録を伝送 （a×b: 200MB） **533 秒**
(5)	―	―

両方式間で差異が無い場合は―を記載

表 5　評価用パラメータ

Table 5　Parameters for Evaluation

記号	パラメータ名称	値
a	初回ユーザ登録を行うまでにユーザが起動するアプリの数（起動アプリに重複があってもよい）	20 個
b	各アプリの記録の平均データ量	10MB
c	ダイジェストデータのデータ量	4B
d	広域無線通信の回線速度	3Mbps

7. 考察

利便性の評価（6.1）において，端末側蓄積方式のステップ(3)でデータ伝送による待ち時間が発生することを記載した。これを回避する手法として，各スマホアプリが地点登録サービスを利用する度に，サービスサーバにデータを逐一アップロードせず，スマホアプリ内に保持しておくという手法が考えられる。この手法を採用することで，ユーザはステップ(3)の 27 秒を待つ必要は無くなり，ステップ(4)の 533 秒のみ待てば良いことになる。

しかしながら，地点登録サービスはそのサービスの特性から地点情報をサービスサーバ上の地図と重ね合わせて表示する必要があるため，この手法を採用することはできない。

このため，サーバ側で管理して複数のユーザが共有することが適している地図のようなデータと，ユーザが個々にサーバにアップロードする地点情報のようなデータの双方を活用する種類のサービスについては, 提案方式が適する。

上記より，提案方式は端末側蓄積方式と比較して，より幅広いサービスに適用できる。

また，今後，クラウドの様々なサーバの情報を分散・統合・編集が容易という特徴とモバイルデバイスのリアルタイム性の高い情報を取得できるという特徴を活用した通信サービスへの期待は大きく 10)，これらサービスは増加していくと予測される。提案方式はこれらサービスに適用できる。

8. まとめ

本研究では，サーバ型の通信サービスを更に使いやすくしていくために，ユーザが（１）ユーザ登録操作を車両内で行うことなく所望のサービスの利用を簡易に開始することができ，（２）ユーザがユーザ登録を行う際に，各サービスでサーバに記録しつつ利用していた匿名個人データ（ドライブ中に登録する走行履歴や地点登録情報など）を引継ぎ・集約して個人の記録として継続的に参照できる方式を提案した。

また，利便性の評価により，提案方式はサービス利用終了時とユーザ登録時にユーザによるデータ待ち時間がほぼ発生しない利便性が高い方式であることを確認した。

また，考察により，今後増加することが予測される，サーバで管理して複数のユーザが共有する地図のようなデータとユーザがサーバにアップロードする地点情報のような個人のデータの双方を活用する種類のサービスに対しても，提案方式の適用が適することを確認した。

参考文献

1) De Figueiredo, D., “The Case for Mobile Two-Factor Authentication”, IEEE, Security & Privacy, Volume 9, Issue 5, Sept.-Oct. 2011, pp.81-85
2) Car Connectivity Consortium (CCC), “Mirror Link”, http://www.mirrorlink.com/
3) Consumer Electronics for Automotive (CE4A), “Terminal Mode Technical Architecture Release Version 1.0”, 2010 http://www.ce4a.org/
4) 高橋, アイデンティティ管理の現状と今後, 電子情報通信学会誌, Vol. 92, No. 4, 2009.
5) A. Barth, U. C. Berkeley, “IETF RFC 6265 HTTP State Management Protocol”, April, 2011. http://tools.ietf.org/html/rfc6265
6) 清水，岡部，吉田 ,”一般カードを使った一時利用者向け認証システムの設計と実装”， 情報処理学会論文誌，コンシューマ・デバイス＆システム　Vol. 3, No.1, 34-35 (Mar. 2013)
7) 情報マネジメントシステムセンター http://www.officegate.jp/security/
8) NIST Special Publication 800-63-1, December, 2011, http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf
9) 平成１６年度情報セキュリティ対策推進事業　「PKI を利用したアプリケーションの実用化に向けての課題と方向性調査」 http://www.japanpkiforum.jp/shiryou/sougo_k/fy2004_interop_report/x_auth_survey.pdf
10)　J. Marín de la Iglesia and J. Labra Gayo, "Doing Business by Selling Free Services," Web 2.0, 2009: pp. 1-14.
11)　クラウドとモバイルデバイス―"ケータイ"との融合が切り開く新たな地平線 山下哲也　（株）NTTドコモ 情報処理 Vol.50 No.11 Nov. 2009