Vol.2012-CDS-5 No.6
Vol.2012-DCC-2 No.6
2012/10/17

複数端末を併用するシステムにおける匿名個人データの引継ぎ方式の提案

清水淳史[†1]　松本貴士[†1]　永井靖[†1]

スマートフォンやカーナビ等の複数の通信端末によって構成されるサービスシステムが市場に登場している。サービスシステムのさらなる普及に向け，ユーザのサービス利用開始時やサービス利用中の操作負荷を下げることが課題である。筆者らはユーザ登録時の操作負荷がサービス利用開始の障壁となっていることに着目し，ユーザが 1) ユーザ登録する事無くサービス利用を開始でき，2) サービス利用中に使用した匿名個人データをユーザ登録時に簡易かつ安全に引き継ぐ方式を開発した。また上記おいて，スマートフォン等の単一端末に複数アプリが搭載される場合に，3) サービスサーバで管理する各アプリ固有の匿名個人データをユーザ登録時に集約する方式を開発した。

A Proposal of a Taking Over Method of Anonymous Personal Data on the Multiple Terminals Mediated Systems

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

Service systems that are composed of multiple terminals like smart phones and car navigation terminals are developed nowadays. Toward further use of these systems, it is important to reduce the operation load that is performed by users when they start to use the systems. We focus attention on the fact that a user registration operation is an obstacle that prevents user's service utilization. Based on the above view point, we developed the method that enables 1) utilization of the services by users without user registration, and 2) the method that enables taking over of anonymous personal data as user's registered data easily and safely when the user registers him to the system. We also considered the case when a terminal like smart phones that has multiple applications. We developed 3) the method that aggregates anonymous personal data that are uploaded to a service server in the case.

1. はじめに

1.1 動向

スマートフォンやタブレット等の複数端末を単一ユーザが併用する通信サービスシステムが増加している。このようなサービスシステムの一つとして，カーナビとスマートフォンとを併用するカーナビースマートフォン連携システムが登場した。

1.2 課題

カーナビースマートフォン連携システムのような，複数の端末を併用するシステムの課題として以下が挙げられる。課題の説明図を図 1 に示す。

(1) 近年，フリーミアム 1)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。ここでは，サービス利用開始の障壁を下げ，多数のユーザをサービスに誘導できることが望ましい。カーナビースマートフォン連携システムにおいてもこのニーズがある。

(2) カーナビースマートフォン連携システムのようなユーザが複数端末を併用するシステムでは，ユーザが一方の端末からサービスサーバに登録したデータを，他方の端末から整合性が保証された形で参照できることが必要である。

(3) また，通信サービスを PC から利用するシステムが既存する。これらの既存システムはユーザを識別又は特定するためのユーザ登録を前提とするものが多い。しかしながら，カーナビースマートフォン連携システムにおいては，ユーザは情報入力操作がより困難な車内にて操作を行う。このため，ユーザによる操作負荷を下げることが必要である。

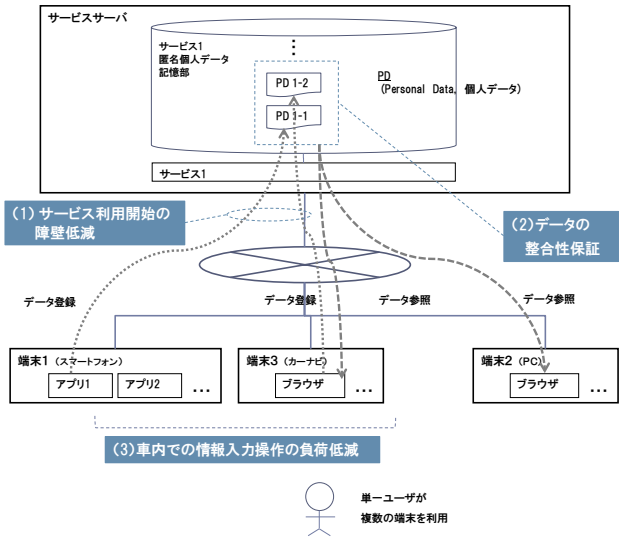

図 1　カーナビースマートフォン連携システムの課題

Figure 1　Problems on Car-Navigation – Smart Phone Collaborated System

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

Vol.2012-CDS-5 No.6
Vol.2012-DCC-2 No.6
2012/10/17

2. 関連研究

本章では関連研究を記載する。

課題(1)のサービス利用開始の障壁を下げるための手段の一つとして OAuth 2)がある。OAuth は，あるユーザがある Web サービスに提供している個人情報を別の Web サービスに提供することを認可する仕組みを提供することで，ユーザ自身によるサービス毎のユーザ登録を不要とできる。

課題(2)の解決手段として，ユーザにユーザ ID を付与し，ユーザを一意に識別する仕組みが挙げられる。

課題(3)の解決手段の一つとして米 Google 社の「Send-To-Car サービス」がある。ユーザはあらかじめ PC 上で調べた目的地情報をカーナビに転送することができる。

上記の全ての解決手段においては，ユーザはサービス利用開始前にユーザ登録を行うことを前提としている。

3. アプローチ

本章では課題を分析し，アプローチを述べる。

3.1 目標

本研究では課題(1)(2)(3)を解決する。

3.2 課題分析

筆者らは，課題(1)において，ユーザ登録の操作負荷がサービス利用開始の障壁となっている点に着目した。フリーミアムサービスでは個人化されたサービスの提供が求められる。このため，ID／パスワードの事前登録によるユーザを識別又は特定するための仕組みが必要とされる。

また，筆者らは電子認証の保証レベルに着目した。電子認証のガイドライン 2)によれば，課金サービスなど高いセキュリティを必要とするサービスを提供する場合は，認証に用いる ID やパスワード，トークン等のセキュリティ強度を所定の強度以上に高める必要がある。このため，例えばユーザが課金サービスを活用するためにはユーザ登録を避けることはできない。しかしながら，フリーミアムサービスで提供されるサービスの多くは非課金サービスである。このため，これらサービスは低い保証レベルでの認証によっても提供可能である。

3.3 アプローチ

課題分析に基づき，以下のステップでユーザをサービスに導入するシステムを考案した。課題(1)(2)(3)より，それぞれアプローチ 1,2,3 を導いた。

1. ユーザ識別（保証レベル 1 相当）で非課金サービスを提供することにより，ユーザをサービスシステムに導く。次に，ユーザにユーザ登録を実施してもらい，ユーザ登録情報に基づく認証（保証レベル 2 相当）によって，課金サービスシステムを継続的に提供する。
2. アプローチ 1 において，ユーザが一方の端末で活用していた匿名個人データを，他方の端末に同期(引継ぎ)可能とする。
3. アプローチ 1,2 においてユーザ操作負荷を最小化する。

図 2 にアプローチ 1 の説明図を示す。

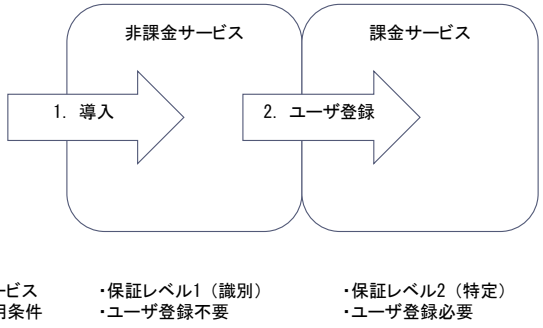

図 2　サービスシステムへのユーザの導入
Figure 2　Leading Users to a Service System

4. システム要件

本章では，アプローチに基づき策定したカーナビースマートフォン連携システムの要件を記載する。

4.1 要件

- 要件 1　匿名個人データを活用するサービスをスマートフォンからユーザ登録なしに利用開始できること。
- 要件 2　スマートフォンでサービス利用中にセンタに登録した匿名個人データを，PC 等の別の端末においてユーザ登録した際に引き継げること。
- 要件 3　引継ぎ時にユーザが入力すべきデータ量を最小化できること。

匿名個人データとは，ユーザがユーザ登録を行わずにサービスサーバに登録したデータを指す。例えば，位置情報と関連づけられたドライブ履歴情報，ドライブ計画情報などの個人が保有／活用するデータである。

要件 1,2,3 は，それぞれアプローチ 1,2,3 に対応する。

ここで，アプローチ 2 における更なる要件を挙げる。

スマートフォン等の端末には複数のアプリを搭載できる。このため，ユーザは単一の端末において，複数の異なるアプリを操作することで複数の異なるサービスを利用することが想定される。この場合，それぞれのアプリで利用していた匿名個人データを集約してユーザ登録時に引き継げることが望ましい。

- 要件 2’　単一のスマートフォンに搭載される複数のアプリの匿名個人データを引継ぎ時に集約できること

要件 2’の説明図を図 3 に示す。

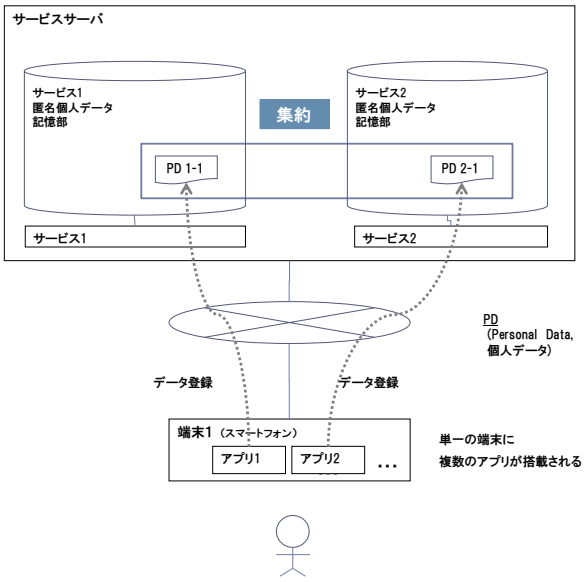

図 3　匿名個人データの集約

Figure 3　The Aggregation of Anonymous Personal Data

4.2 サービスシナリオ

要件を具体的に説明するために，サービスシナリオを示す。

要件 1，2 に対応するサービスシナリオを「ドライブ計画」サービスを例として図 4 に記載する。「ドライブ計画」サービスとは，ユーザがドライブ前に集合場所や目的地，経由地とそこでの行動計画などを Web 登録するサービスである。

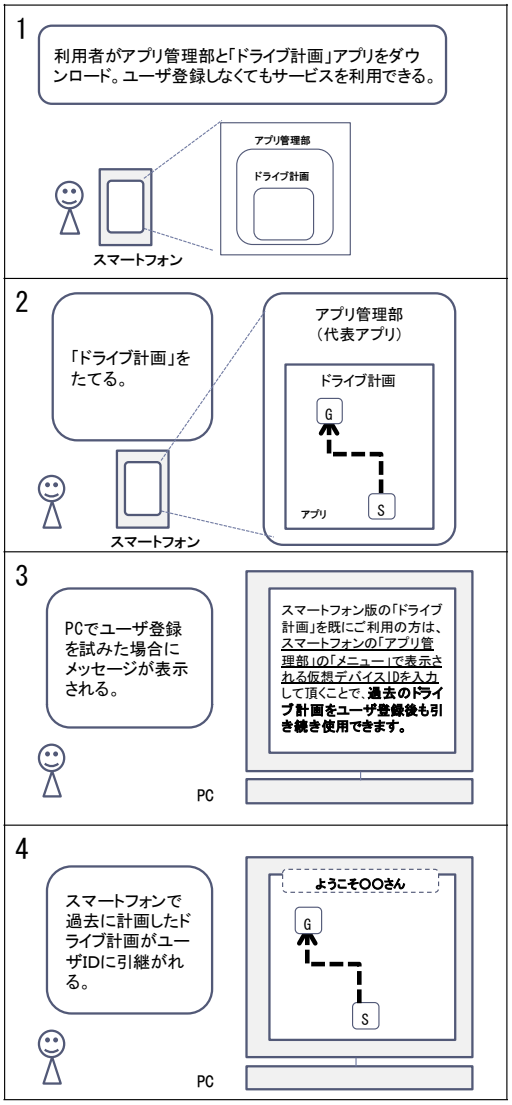

図 4　サービスシナリオ（要件 1,2）

Figure 4　A Service Scenario (Requirement 1,2)

要件 2’に対応するサービスシナリオを図 5 に記載する。

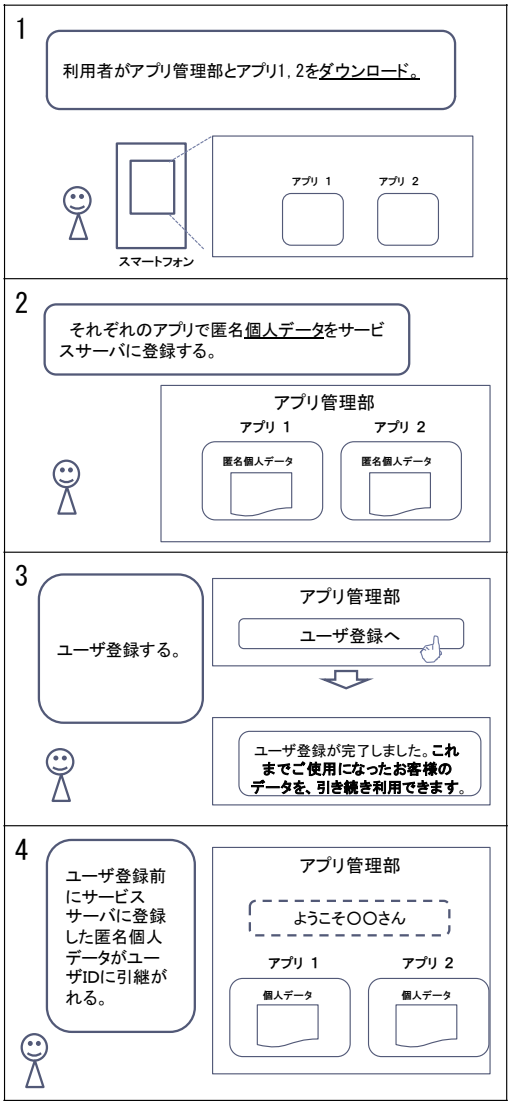

図 5　サービスシナリオ（要件 2’）

Figure 5　A Service Scenario (Requirement 2’)

5. 提案方式

本章では提案方式を説明する。

5.1 システム構成

図 6 にサービスシナリオを実現するためのシステム構成を説明する。概要を以下に示す。

- 単一ユーザがスマートフォンと PC を使用する。
- スマートフォンは通信サービスを利用するための複数のアプリケーション（アプリ）を搭載する。
- アプリ管理部は複数アプリを管理するスマートフォンアプリである。
- 匿名ユーザ（ユーザ ID が未登録のユーザ）は，スマートフォンで複数のサービスを利用し，各サービス固有の匿名個人データをアップロードする。

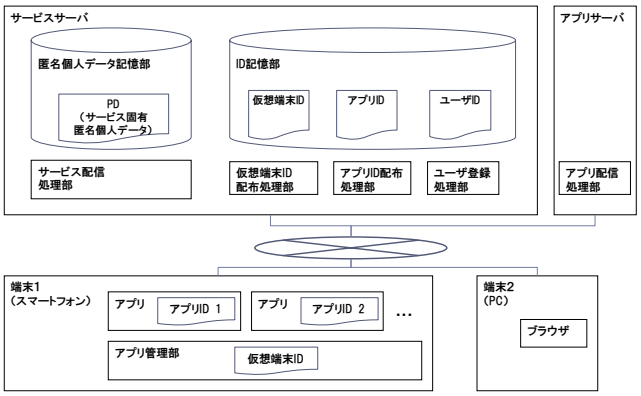

図 6　システム構成

Figure 6　System Configuration

5.2 シーケンス

前記のサービスシナリオを実現するシーケンスを図 8 に記載する。ユーザは各ステップ(Step)で以下を行う。

- Step1 アプリ管理部をダウンロード b
- Step2 サービス利用のためのアプリをダウンロード
- Step3 サービス利用中にアプリ経由で匿名個人データをサーバに登録
- Step4 ユーザ ID とパスワードを入力してユーザ登録

5.3 要件と方式の対応

要件 1 の実現方式として以下を設けた。Step1 において，スマートフォンに搭載するアプリ管理部は，初回起動の際にサービスサーバから仮想端末 ID を受信する。仮想端末 ID はサービスサーバがアプリ管理部を一意に特定するための ID である。スマートフォンはパーソナル機器であるため，仮想端末 ID はアプリ管理部に付与されるものであるが，ユーザの個体を識別するための ID としての意味を持たせることができる。仮想端末 ID は 32 バイトのデータ長とした。サービスサーバは 2^32 個のアプリ管理部を一意に識別できる。この方式により，サービスサーバはユーザによるユーザ登録を必要とせず，ユーザの個体識別が必要なサービスを提供できる。

要件 2 の実現方式として以下を設けた。サービスサーバは Step3 で「仮想端末 ID⇔アプリ ID⇔PD」を紐付ける。Step4 において，ユーザは PC からユーザ登録する際に，仮想端末 ID も併せてサービスサーバに登録する。サービスサーバは「ユーザ ID⇔仮想端末 ID」を紐づけることでデータを引き継ぐ。この方式により，ユーザはサービスサーバに登録していた匿名個人データをユーザ登録後も引継いで継続的に活用できる。

b　サービスを利用するための複数アプリを管理するためのアプリ

要件 3 の実現方式として以下を設けた。当該IDは多数のユーザが使用する多数のアプリ管理部に付与するため，桁数が大きい。このため，提案方式では少なくとも仮想端末IDと有効期限付きIDとを入力要素とするダイジェストデータを，仮想端末IDの代わりにブラウザから入力する方式を採用した c。サービスサーバにおけるダイジェストデータの生成式を以下に示す。

LEFT (Hash（仮想端末 ID_有効期限付き ID）,4)

… 式 1

_：	データの連結
Hash：	ハッシュ関数
LEFT（data, 4）：	data の先頭 4 バイトを抽出

要件 2’の実現方式として以下を設けた。サービスサーバは Step2 で「アプリ ID⇔PD」を紐づけて管理する。また，サービスサーバは「仮想端末 ID⇔アプリ ID」を紐づけて管理する。上記の条件において，Step4 にてユーザ登録時に仮想端末 ID に紐付くアプリ ID と PD とをユーザ ID に紐づけることで，各サービス固有の匿名個人データを集約することができる（図 9）。

図 7 に単一の端末に搭載される複数のアプリがセンタに登録している匿名個人データをユーザ登録時に集約するためのエンティティ-リレーションを示す。

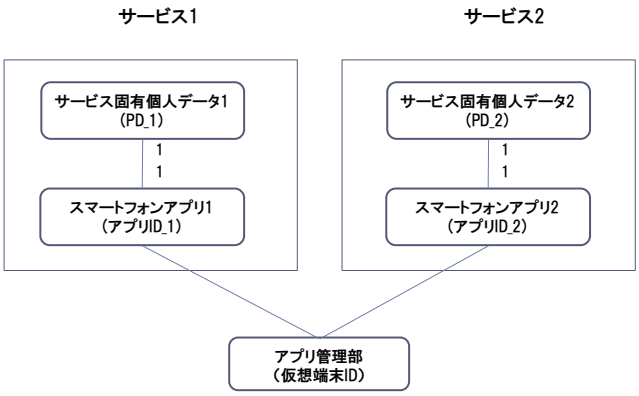

図 7 集約のためのエンティティとリレーション

Figure 7 Entities-Relations Diagram for PD Aggregation

なお，ここではユーザは仮想端末 ID を PC のブラウザから入力することとしたが，カーナビのブラウザから入力しても同様の効果が得られる。

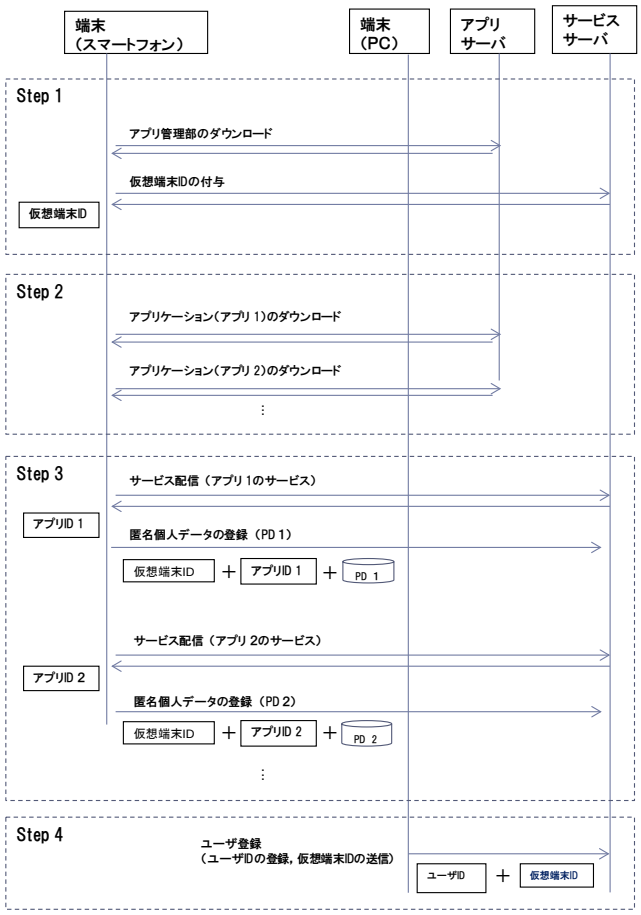

図 8 シーケンス

Figure 8 A Sequence Diagram

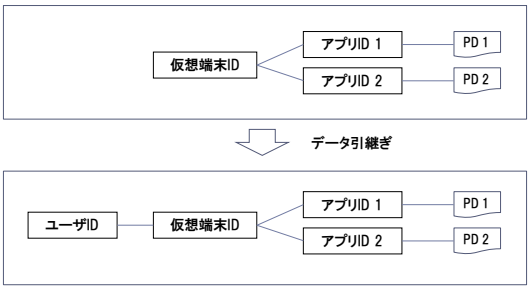

図 9 匿名個人データの集約と引継ぎ

Figure 9 Aggregation and Taking-over of Anonymous Personal Data

c ID の一意性を担保するために，有効期限内はサービスサーバは重複する有効期限対 ID を配布しない。

6. 評価

本報告では，課題に対してアプローチを策定し，アプローチに基づき 4 つのシステム要件を抽出した。本章では，これら要件に対する提案方式の有効性を評価する。

要件 1： 従来，個人識別が必要なサービスを利用するためには，ユーザはユーザ情報を登録する必要があった。提案方式では，ユーザによるサービスサーバへの情報入力を必要としない。提案方式では，ユーザがスマートフォンのアプリ管理部を初期起動した際にサービスサーバがアプリ管理部に対して仮想端末 ID を付与することで，ユーザがユーザ登録することなくユーザ個体識別が必要なサービスの利用を開始できる。参考文献 4)のアンケート結果によれば，インターネットを利用していない人の約 36%が，インターネットを利用しない理由として操作が難しいことを挙げている。提案方式によりサービス利用の障壁を下げ，上記の人をサービスに誘導する対象とすることができる。

要件 2： 従来，複数の端末間でデータを同期するためには，ユーザ登録を前提としてサービスサーバでデータ管理を行うか，もしくは，端末間で個人データ転送を行う必要があった。提案方式はユーザ登録を前提としないという利点がある。また，提案方式では，ユーザがサービスを利用する過程で，サービスサーバがサービス固有の匿名個人データを仮想端末 ID と共に記録する。このため，個人データを転送するための付加的なユーザ操作や付加的な処理時間を必要としないという利点がある。一方で，提案方式はスマートフォンがパーソナル機器であるということを前提としている。このため，単一スマートフォンを複数ユーザで共有するようなケースにおいて，ユーザ個々のデータの整合性を保証することは想定していない。このケースにおいて整合性を保証するためには，単一スマートフォン上で複数ユーザを区別する仕組みを付加する必要がある。

要件 3： 提案方式は，ユーザは式 1 の値（4 バイト）をブラウザから入力することで，ユーザ登録時に匿名個人データを引き継ぐことができる。4 バイトのデータ量は，ユーザが PC やカーナビを前にして一時的に記憶可能なデータ量である。このため，提案方式はユーザの操作負荷が低い方式と言える。

要件 2’： 単一端末に搭載される複数のアプリにおいてユーザ登録することなく個人データを活用するサービスシステムについての取り組みは，本研究が初の試みである。提案方式は，単一端末（スマートフォン）に搭載されるアプリに対してアプリを個体識別するためのアプリ ID を付与することで，サービスサーバがアプリ固有の匿名個人データを管理することを可能としている。

上記により提案方式が有効と評価する。

7. 考察

本章では考察を述べる。

(1) なりすましユーザ登録の回避

表 1 評価パラメータ
Table 1 Parameters for Evaluation

パラメータ名称	値
仮想端末 ID	32 バイト
有効期限付き ID	32 バイト
有効期限	3 日
ロックアウト期間	3 日

ここでは，提案方式におけるセキュリティ対策を説明し，そのセキュリティ強度につき考察する。パラメータを表 1 に示す。

提案方式では，悪意のあるユーザがなりすまして匿名個人データを引継ぐことを避けるために，所定の回数誤ってダイジェストデータが入力された場合に，サービスサーバは当該ダイジェストデータをロックアウトする仕組みを設けた。式 1 の値を「ロックアウトまでの誤入力回数」にて推測することは困難であるため，十分なセキュリティ強度を担保できると考える。

(2) 個人情報の保護

サービスサーバは各アプリの匿名個人データをアプリ単位で管理する。このため，各サービスの匿名個人データは，ユーザがユーザ登録を行って高い保証レベルでサービスサーバにログインできるようになるまでは集約されない。即ち，集約された匿名個人データは，ユーザが高い保証レベルで認証された時のみ参照可能となる。このため，個人情報保護の観点からも妥当な構成と考える。

8. まとめ

本章では本研究のまとめを記載する。

A) 利用者のサービス利用開始の障壁を下げる仮想端末 ID 付与方式を提案した。本方式は，複数端末を併用するサービスシステムにおいて，ユーザ登録を前提とせずにサービス提供を開始できる。

B) 入力情報を最小化しつつ安全な匿名個人データの引継ぎを可能とする，匿名個人データ引継ぎ方式を提案した。

C) 単一の端末に複数のアプリを搭載するシステムにおいて各アプリのサービス固有匿名個人データを安全に集約する方式を提案した。

カーナビ-スマートフォン連携をはじめとする複数の通信端末を併用するシステムに提案方式を適用することで，より多くのユーザをサービスに導入できると考える。

参考文献

1) J. Marín de la Iglesia and J. Labra Gayo, "Doing Business by Selling Free Services," Web 2.0, 2009: pp. 1-14.
2) Lucy Lynch, “Inside the Identity Management Game,” IEEE INTERNET COMPUTING, 2011: pp. 81-82.
3) NIST Special Publication 800-63-1, December, 2011, http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf
4) インターネット利用の決定要因と利用実態に関する研究調査, 総務省　情報通信政策研究所，平成21年3月.