個人のプライバシーを考慮したサービス提供のためのデータモデル設計

玉井 睦† 坂本 一仁† 松永 昌浩†

†セコム株式会社 IS 研究所
181-8528 東京都三鷹市下連雀 8-10-16 セコム SC センター
{mu-tamai, takah-sakamoto, m-matsunaga}@secom.co.jp

あらまし
近年，インターネットや様々な機器等から大量かつ多様なデータの収集が容易になった．このように取得したデータを利用し，個人に対してプロモーションやサービス提供をする状況においては，提供した覚えがない等のプライバシーに係る不信感や不快感を与えてしまう場合がある．本稿では，パーソナリティとアイデンティティの概念から，サービス等を受けた個人が，プライバシー侵害と判断する 3 つの条件を仮定した．そして，個人に対してあるサービス等を提供する時，そのサービス等が個人にとってプライバシー侵害と感じるか否かを判定するために，パーソナルデータを管理する情報システムに必要なデータモデルを設計した．

Data Model Design for Providing Service in Consideration of Individual Privacy

Mutsumi Tamai† Takahito Sakamoto† Masahiro Matsunaga†

†Intelligent Systems Laboratory, SECOM Co., Ltd.
SECOM SC center, 8-10-16 Shimorenjaku, Mitaka, Tokyo 181-8528, JAPAN
{mu-tamai, takah-sakamoto, m-matsunaga}@secom.co.jp

Abstract In recent years, the collection of large amounts of various data has become easier from the Internet and various equipment. Utilizing this data in the context of promotions and services offered to an individual may lead to distrust and discomfort in terms of privacy if the individual has no recollection of providing such information. In this paper, we built three hypotheses from the personality and the identity concepts, for the determination of privacy when the individual had received the service. We then designed the data model required for the information system to manage personal data in order to determine whether or not individuals feel invasion of privacy when receiving service from other parties.

1 はじめに

大量かつ多様なパーソナルデータを利用して，個人に特化したプロモーションやサービス提供を行う場面が増えている．その際，事業者が行う利用規約やプライバシーポリシーの提示, パーソナルデータの取得，必用に応じた同意の取得といった一連の枠組みがあるが, サービス提供時に利用者が受けるプライバシーに係る不信感や不快感を必ずしも解消できているわけではない．

本稿では，サービス提供時にプライバシーに係る不信感や不快感を与えないためにサービス事業者側が配慮すべきことを考える．サービス

利用者が受けるプライバシーに係る不信感や不快感は解明されていない部分が多いが，我々はパーソナリティやアイデンティティの概念と深く係りがあると考え [1][2]，不信感や不安感に至る心理メカニズムを分析し，基本概念を構築した．

そして，本稿で示す基本概念から，サービス事業者がサービス利用者のプライバシーに係る不信感や不快感に配慮するためには，3 つの条件を満たすか否かの判断が必要であると仮定し，その判断を行うために必要な観測可能データを管理するためのデータモデルを設計した．

本稿で設計したデータモデルを利用することで，パーソナルデータを高度に分析したサービス提供であっても，利用者が感じる不信感や不快感を軽減しつつサービス提供が可能となると期待される．

2　基本概念の設計

本節では，サービス提供時に，サービス事業者が何に配慮すればよいかを決定するための基本概念を設計する．まず，パーソナリティとアイデンティティの関係を踏まえて，個人がサービスを受けた際に不信感や不快感を覚えるに至る心理メカニズムを説明するモデルを構築する．そして，サービス利用者に不信感や不快感を与えるサービス提供となる原因を考察する．

2.1　パーソナリティモデル

パーソナリティという言葉の語義は，ラテン語のペルソナ（persona）であり，パーソナリティには以下の 4 つの意味が含まれるという [3]．

(1) **その人がもっている個人的な性質の総体**

(2) **その人が劇中で演じる役割**

(3) **個人の尊厳性**

(4) **他人から見える外観的な人柄**

パーソナリティモデル（図 1）は，これらを基に設計した基本概念である．2.2 から 2.9 で，パーソナリティモデルについて説明する．

2.2　心理的アイデンティティ

アイデンティティ管理技術においてアイデンティティの意味するところは，エンティティの属性集合である [4]．パーソナリティモデルでは，この意味とは異なる概念として**心理的アイデンティティ**と記述する．

2.2.1　心理的アイデンティティの定義

エリクソンが確立したアイデンティティ概念は，パーソナリティ概念を説明するフロイトの自我理論を発展させた理論であり，エリクソンによれば，自我アイデンティティは自我のサブシステムとして働き，自我の社会的機能を意味する [5]．従って，パーソナリティモデルにおいて，心理的アイデンティティはパーソナリティの一部を構成する要素で，心理的な機能を担う概念であるとする．これを踏まえて心理的アイデンティティを，**自分と社会との関係で自分をまとめる機能**と定義する．

2.2.2　心理的アイデンティティの機能

自分と社会との関係で自分をまとめる機能には，他人の評価をどのように受け入れるかという側面と，他人に対してどのように振る舞うかという側面があると考えられる．

エリクソンのアイデンティティ概念の本質は，自己イメージの統合である [5]．本稿では，自己イメージの統合を，自分と社会との関係の中で，**(1) その人がもっている個人的な性質の総体**を形成する働きであると解釈し，他人の評価をどのように受け入れるかという側面を表すものとする．

一方，ゴッフマンは，アイデンティティを，提示し演じ管理する対象とし，アイデンティティ管理の戦略を類型化している [6]．本稿では，この考え方の機能的側面を取り入れ，自分と社会との関係の中で，個人的な性質を提示し演じ管理することは，すなわち，他人に対してどのように振る舞うかという側面を表すと解釈する．そして，**(2) その人が劇中で演じる役割**は，振る舞いの結果として表れる個人的な性質であると解釈する．以上より，心理的アイデンティティは以下の 2 つの機能を持つ．

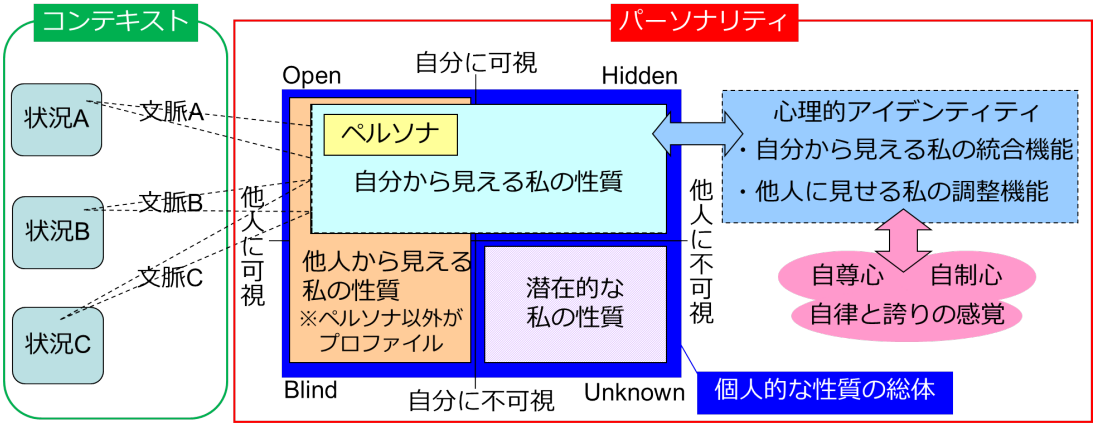

図 1: パーソナリティモデル

I. 自分から見える私の統合機能

自分から見える私の統合機能は，個人が認識した状況における自分に関する性質を，自分自身の性質として受け入れる機能である．具体的には，個人がパーソナルデータを利用したサービス等を受けた際に，個人の心理として働く機能である．

II. 他人に見せる私の調整機能

他人に見せる私の調整機能は，個人が認識した状況に対して適切だと思う個人的な性質を，見せたり隠したりする機能である．具体的には，個人がパーソナルデータを開示する際に，個人の心理として働く機能である．

2.2.3 自尊心・自制心との関係

エリクソンは，**自尊心を失うことのない自制心**の感覚から，**自律と誇りの感覚**が生まれ，逆に，不能感，自制心の喪失感，過剰にコントロールされている感覚から，疑惑と恥の感覚が生まれるという [5]．パーソナリティモデルでは，心理的アイデンティティは自制心と自尊心に基づき，自律と誇りの感覚が得られるように働くとする．この自尊心を失うことのない自制心は，**(3) 個人の尊厳性**に係わると考えられる．また，疑惑と恥の感覚は，本稿で対象とする個人が覚える不信感や不快感につながる感覚であると考えられる．

本稿では，自律と誇りの感覚が得られない時，すなわち，心理的アイデンティティがうまく働かない時，個人は不信感や不快感を覚えると仮定し，この状態を**個人がプライバシー侵害と感じる状態**として扱う．

2.3 個人的な性質の総体

心理的アイデンティティが対象とするのは，個人が認識している自分に関する個人的な性質である．一方，パーソナリティには，**(4) 他人から見える外観的な人柄**という意味も含まれる．

パーソナリティモデルでは，個人的な性質の総体を自分と他人の可視性から定義した．本稿では，可視性を表すモデルとして，ジョハリの窓 [8] を用いた．

図 1 において，自分に可視の領域にある個人的な性質を，「自分から見える私の性質」とする．他人に可視の領域にある個人的な性質を，「他人から見える私の性質」とする．Unknown の領域にある個人的な性質を，「潜在的な私の性質」とする．2.4 から 2.6 で，これらの個人的な性質がもつ意味を説明する．

2.4 自分から見える私の性質

自分から見える私の性質は，個人が認識している自分に関する個人的な性質であり，心理的アイデンティティの対象となる個人的な性質である．

2.4.1 可視性と認識

自分から見える私の性質には，個人の認識の観点で以下の 3 つの状態がある．

- **自分に関する性質であることの認知**
- **他人に知られていることの認知**
- **自分自身の性質であることの自覚**

パーソナリティモデルでは，自分から見える私の性質を，単に，自分に関する性質であることを認知した状態とする．そして，Open の領域は，自分に関する性質であることを認知し，且つ，ある状況では他人に知られていることを認知した状態とする．Hidden の領域は，自分自身の性質であることを自覚し，且つ，ある状況では他人に知られていないことを認知した状態とする．

2.4.2 心理的アイデンティティとの関係

心理的アイデンティティを前述した認識の観点で説明する．自分から見える私の統合機能は，認知した自分に関する性質を，自分自身の性質であると自覚する機能である．他人に見せる私の調整機能は，自覚している自分自身の性質を，状況に合わせて開示するかしないかを調整する，あるいは，他人に知られていることを認知した自分に関する性質を状況に合わせて訂正する機能である．

2.4.3 ペルソナ

パーソナリティモデルでは，他人に見せる私の調整機能によって開示される個人的な性質を**ペルソナ**と呼ぶ．これは，パーソナリティの語義としてのペルソナではなく，「断片化した私」[7] すなわち，その人の社会的な顔を指すペルソナである．

他人に見せる私の調整機能によって状況に合わせて開示されたペルソナは，自分自身の性質であることの自覚があり，ある状況では他人に知られていることを認知している個人的な性質となる．例えば，氏名，住所，生年月日等，個人が明示的に開示した情報がペルソナである．

そして，ある状況では開示されなかった個人的な性質は，Hidden の領域となる．従って，Hidden の領域における，他人に不可視という意味は，自分以外の誰にも知られていないという意味ではなく，ある状況で知られていないということである．どのような状況でも開示していない個人的な性質が，自分以外の誰にも知られていないと認知している個人的な性質である．

2.5 他人から見える私の性質

他人から見える私の性質は，2.4.1 の個人の認識がどうあるかに係わらず，他人が知っている自分に関する個人的な性質である．具体的には，事業者が保有する，ある個人のパーソナルデータである．

2.5.1 プロファイル

他人から見える私の性質の内，個人に対して何らかの方法で，その個人的な性質がペルソナであることの確認が取れている場合には，ペルソナと合致した個人的な性質である．この確認は，自分自身の性質であることと，ある状況で知られていることの確認である．それ以外の他人から見える私の性質を，パーソナリティモデルでは**プロファイル**と呼ぶ．

プロファイルは，前述の確認が取れていないため，他人からは，その個人が自覚している個人的な性質なのかどうか，或いは，その状況で開示するつもりがあるのかどうかはわからない個人的な性質である．例えば，本人以外から取得した住所，電話番号，メールアドレス等の情報や，防犯カメラで撮影された映像，センサや端末のログデータの分析結果として得られた人物像等である．

2.5.2 Blind の領域にあるプロファイル

2.4.1 の個人の認識では，Blind の領域は，自分に関する性質であることを認知していない，且つ，ある状況で他人に知られていることを認知していない状態となる．

Blind の領域にあるプロファイルは，具体的には，事業者が保有していることに個人が気づいていないパーソナルデータである．

そして，事業者がパーソナルデータを利用して，個人に特化したプロモーションやサービスを提供した状態は，Open の領域で表される．

この時，本稿で対象としている，プライバシーに係わる不信感や不快感を与える恐れがあると考えられる．これについては後述する．

2.6　潜在的な私の性質

潜在的な私の性質は，自分も認識しておらず他人にも認識されていない潜在的に存在する自分に関する個人的な性質である．例えば，遺伝子情報等の分析で初めてわかる個人的な性質である．事業者が分析することで知り得たとき，その個人的な性質はプロファイルとなる．

2.7　コンテキスト

パーソナリティモデルでは，状況と文脈を合わせてコンテキストと呼ぶ．パーソナリティモデルにおける状況と文脈について説明する．

2.7.1　状況

本稿では，個人がパーソナルデータの開示に係る判断の際に認識する状況（以降，**開示の状況**と呼ぶ.）と，個人がパーソナルデータを利用したサービス等を受けた際に認識する状況（以降，**利用の状況**と呼ぶ.）を想定する．

開示の状況は，例えば，パーソナルデータを開示する際に，プライバシーポリシー等で個人が認識する利用目的や，どの事業者に開示するか，あるいは開示する人物，開示する際の日時や場所である．利用の状況は，例えば，サービス等で個人的な性質が開示される際に，個人が認識する利用の仕方や，どの事業者，あるいは誰が利用したか，開示された日時や場所，誰と供にいるかである．

2.7.2　文脈

パーソナリティモデルでは，各々の状況と自分から見える私の性質が紐付いて，個人に認識された状態を**文脈**と呼ぶ．2.2 で述べた，心理的アイデンティティの 2 つの機能の内，他人に見せる私の調整機能が働く際に認識される文脈は，開示の状況と紐付いたものとなる．また，自分から見える私の統合機能が働く際に認識される文脈は，利用の状況と紐付いたものとなる．

2.8　文脈の判断

文脈は，心理的アイデンティティが働く際に，以下の 3 つの条件で判断されると仮定した．

- **条件 1：既知の必然性**
- **条件 2：自己合致性**
- **条件 3：状況の妥当性**

既知の必然性は，他人に個人的な性質を知られる過程に自らの行為を顧みることができるかどうかが判断される．

自己合致性は，他人が認識している自分に関する個人的な性質が，自分で自覚できる個人的な性質かどうかが判断される．

状況の妥当性は，個人が認識した自分に関する個人的な性質と状況が個人の意図によく当てはまり適切であるかどうかが判断される．

尚，他人に見せる私の調整機能によって開示されたペルソナはこれら 3 条件を満たした個人的な性質である．そして，自分から見える私の統合機能が働く際の，既知の必然性と状況の妥当性の判断は，利用の状況と紐付いた自分から見える私の性質が，開示の状況ではどうであったのかが影響する．

2.9　不信感や不快感を与える場合

本稿の仮定に従えば，文脈が前述の 3 条件を満たさない時，2.2 で述べた個人がプライバシー侵害と感じる状態となり，不信感や不快感を覚えると考えられる．本稿で対象とする，事業者がパーソナルデータを利用して，個人に特化したプロモーションやサービスを提供する場面での，3 条件を満たさない場合について説明する．

2.9.1　既知の必然性を満たさない場合

既知の必然性が満たされない場合，個人は，事業者がなぜ伝えたことのない個人的な性質を知っているのかという不信感を覚えることになる．プロファイルは開示の状況をどの程度個人が認識しているのか事業者にはわからないため，誰に開示したかを個人が認識していないプロファイルが利用された場合には既知の必然性が満たされない．また，仮に事業者がパーソナルデータを取得した時点ではペルソナであることが確認できたとしても，長時間経過したものは，個人が開示したことを忘れていて既知の必然性が満たされない場合も考えられる．

2.9.2　自己合致性を満たさない場合

自己合致性が満たされない場合，個人は，受け入れ難い個人的な性質によって名誉感情が害される不快感を覚えることになる．プロファイルの内，特に分析結果によって得られた人物像を利用した時，自己合致性が満たされない場合があると考えられる．

2.9.3　状況の妥当性を満たさない場合

状況の妥当性が満たされない場合，個人は，意図しない利用の仕方がされる不快感，あるいは，その利用の状況では隠しておきたい秘密が露呈する不快感を覚えることになる．プロファイルは，開示の状況に含まれる利用目的を個人がどの程度認識しているのか事業者にはわからず，利用の仕方を個人が認識していないプロファイルが利用された場合には状況の妥当性が満たされない．

また，仮に事業者がパーソナルデータを取得した時点ではペルソナであることが確認できたとしても，長時間経過したものは，個人が利用目的を忘れる，もしくは，個人の気が変わり当初の意図と合わなくなっていて状況の妥当性が満たされない場合も考えられる．

さらに，開示の状況では想定していない利用の状況の場合，例えば，サービス提供時に開示された個人的な性質を知られたくない人物と一緒にいる場合等，利用の状況が適切ではなく状況の妥当性が満たされない場合もある．

3　データモデルの設計

サービス利用者に不信感や不快感を与えるサービス提供の状況か否かを判定するために，パーソナルデータを管理する情報システムに必要なデータモデルの設計を行った．

2 節で述べた基本概念に基づけば，文脈が 3 条件を満たしているか否かを判定するための，観測可能なデータを管理できればよい．

パーソナルデータがどのような状況で取得され，そのパーソナルデータがどのような状況で利用されるか，そして，取得した時に個人がどの程度状況を認識しており，どのような意図を持っていたのかを表すデータを，関連性を持って管理する必要がある．本稿ではこのデータモデルを**人時空間モデル**と呼ぶ．

3.1　人時空間モデル

人時空間モデル（図 2）は，サービス事業者が，サービス利用者視点の文脈及び，個人の認識や意図の状態を関連性を持って管理するためのデータモデルである．

人時空間モデルは 4 つのモデルから構成される．サービス事業者が管理するパーソナルデータを，2.3 で述べた他人に可視の領域にあるペルソナやプロファイルを区別して表現するためのモデルをアイデンティティモデルと呼ぶ．

サービス事業者が実施するサービスで利用するパーソナルデータと，サービス提供時に開示されるパーソナルデータを表現するためのモデルをサービスモデルと呼ぶ．

2.7 で述べた，状況や文脈を表現するためのモデルをコンテキストモデルと呼ぶ．また，3 条件の判断に係わる個人の認識や意図の状態を表現するためのモデルを意図モデルと呼ぶ．

人時空間モデルを構成する各モデルについて説明する．

3.1.1　アイデンティティモデル

アイデンティティモデルは，サービス利用者個人の属性の集合であり，ペルソナ属性とプロファイル属性でサービス利用者の属性の実態を表す．ペルソナ属性は，ある時点でサービス利用者本人が開示した氏名，住所，生年月日等のサブ属性の集合であり，プロファイル属性は，ある時点で本人以外によって開示されたサブ属性や，システムにより推定されたサブ属性の集合である．

アイデンティティモデルでは，サービス事業者が取得したパーソナルデータを，サービス利用者本人が開示の意思を持って開示したもの（ペルソナ）か，そうでない（プロファイル）かを区別して管理する．その理由は，取得したパーソナルデータを，サービス利用者の開示の状況の認識と関連付けて管理するためである．

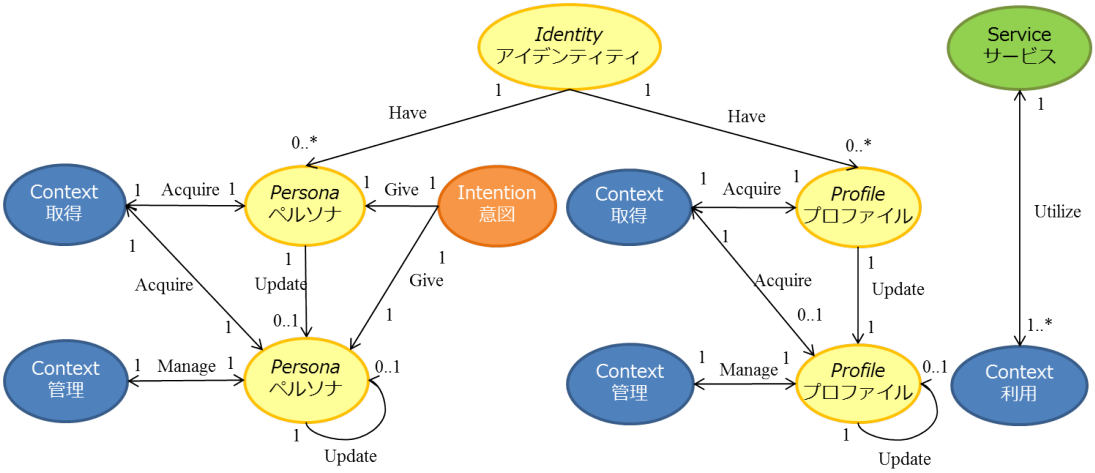

図 2: 人時空間モデル

3.1.2 サービスモデル

サービスモデルは，サービスに利用する個人の属性と，サービス提供時に開示される個人の属性を，アイデンティティモデルのペルソナ属性やプロファイル属性のサブ属性（氏名，住所，メールアドレス等）への参照情報として持つ属性集合である．

3.1.3 コンテキストモデル

コンテキストモデルは，アイデンティティモデルのペルソナ属性やプロファイル属性の取得時，管理時における状況，サービスモデルで表されるサービスを実施する際に想定される状況を属性として持つ属性集合である．コンテキストモデルはタイプとして取得，管理，利用があり，下記でそれぞれを説明する．

取得のコンテキスト

取得のコンテキストは，アイデンティティモデルのペルソナ属性やプロファイル属性を誰が，誰から，いつ，どこで，どのように取得したか等の状況を属性として記録し，対象のペルソナ属性やプロファイル属性に対するリンクを保持する．

管理のコンテキスト

管理のコンテキストは，取得済みのペルソナ属性やプロファイル属性について，誰が，いつ，どのように変更，削除等の処理を行ったかという状況を属性として記録し，対象のペルソナ属性やプロファイル属性に対するリンクを保持する．

利用のコンテキスト

利用のコンテキストは，サービスモデルで表されるサービスを実施する際に想定される，誰が，誰に対し，いつ，どこで，どのようにサービス提供を行うのかという状況を属性として記録し，対象のサービスモデルに対するリンクを保持する．

3.1.4 意図モデル

意図モデルは，アイデンティティモデルのペルソナ属性の取得時における，サービス利用者がどのような利用目的に対しどのような同意状態 [9] のもと，ペルソナ属性を開示したのかといった，サービス利用者の意図や認識を表す情報を属性として持つ属性集合である．

3.2 人時空間モデルの使用例

サービスモデルからそのサービスで利用される個人の属性がわかり，その個人の属性を管理するアイデンティティモデルとリンクする取得のコンテキストと管理のコンテキスト，意図モデルがわかる．そして，サービスモデルとリンクする利用のコンテキストもわかる．

例えば, 既知の必然性の判定では, 利用のコンテキストと取得のコンテキストを比較し，利用の状況から開示の状況を個人がどの程度想起できるかを判定する．コンテキストのどの属性を比較し，どのような手法を用いて判定するかという組み合わせは多数考えられるが，手法の選定及び結果の評価については今後の課題とし，本稿では具体的な判定方法については述べない．

3.3 人時空間モデルの表現方法

人時空間モデルは OWL や RDF 等で表現可能である．また，独自のスキーマとして XML や JSON 等で設計してもよい．

4 まとめ

本稿では, パーソナリティとアイデンティティの関係を踏まえて，個人がサービスを受けた際に不信感や不快感を覚えるに至る心理メカニズムを説明するパーソナリティモデルを設計した．そして，サービス利用者に不信感や不快感を与えるサービス提供の状況は，パーソナリティモデルに基づけば，文脈が既知の必然性，自己合致性，状況の妥当性の 3 条件を満たさない時であると導いた．

また，サービス提供の状況が，3 条件を満たすか否かを判定するために必要な，サービス利用者視点の文脈及び，個人の認識や意図の状態を関連性を持って管理するためのデータモデルとして，人時空間モデルを設計した．

本研究の要となる 3 条件はパーソナリティモデルに基づく仮説であり，3 条件を満たしていれば不信感や不快感を与えないかどうかは検証されていない．3 条件の具体的な判定方法と合わせて結果の検証を今後の課題とする．

最後に，本研究のプライバシー問題に対するアプローチは，大量で多様なパーソナルデータを個人が如何にコントロールするかというものではなく, サービス事業者が, 大量で多様なパーソナルデータを如何に“ 空気を読んで ”利用できるかというものである．今後，パーソナルデータを利活用して行くためには，サービス利用者に選択の責任を負わすのではなく，サービス事業者側が個人のプライバシーに配慮することが重要になるであろう．

参考文献

[1] 大谷卓史. プライバシー論におけるコントロール理論の限界 : 自己アイデンティティ提示とプライバシーの文脈依存性. 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ, Vol. 110, No. 113, pp. 13–19, Jun 2010.

[2] ダニエル・J・ソローヴ, 大谷卓史訳. プライバシーの新理論 - - 概念と法の再考. みすず書房, Jun 2013.

[3] 岡本栄一. こころの世界 - 図説心理学入門. 新曜社, May 1983.

[4] 独立行政法人情報処理推進機構セキュリティセンター. アイデンティティ管理技術解説, Jan 2013.

[5] E．H．エリクソン. アイデンティティとライフサイクル. 誠信書房, Jun 2011.

[6] アーヴィングゴッフマン. スティグマの社会学 - 烙印を押されたアイデンティティ. せりか書房, 改訂, Apr 2001.

[7] 山崎重一郎. 非集中的 Web アイデンティティとペルソナ : 「私」中心の Web と OpenID,OAuth(＜特集＞ Web アイデンティティと AI). 人工知能学会誌, Vol. 24, No. 4, pp. 519–526, Jul 2009.

[8] businessballs.com. johari window. http://www.businessballs.com/johariwindowmodel.htm.

[9] 佐藤慶浩. データプライバシー対策をグローバル対応するための顧客情報管理データベースの設計と運用のプラクティス—連絡先情報をプロモーション連絡に利用する事例—. デジタルプラクティス, Vol. 6, No. 1, pp. 5–12, Jan 2015.