情報処理学会論文誌 Vol.56 No.12 2253–2264 (Dec. 2015)

集合論的記法を用いたプライバシと個人の関係性整理技法の提案

吉本 明平[1,a)] 下道 高志[2]

受付日 2015年3月9日, 採録日 2015年9月2日

概要：プライバシにかかわる情報と個人の関係性を数学の集合論的記法を用いて表記する手法を提案する．これによってプライバシに関する客観的かつ合理的な議論を可能とする．「行政手続における特定の個人を識別するための番号の利用等に関する法律」の施行や「パーソナルデータの利活用に関する制度改正大綱」の公表など，日本国内におけるプライバシの取扱いについての議論が活発化している．そこでは個人に関する情報と個人との関係性や情報の共有範囲の検討が不可欠である．しかし，これらの検討において情報の関連範囲を明確に記述し論理的，具体的な議論を行う方法論が未整備であった．本稿では集合論的記法を応用し，プライバシにかかわる情報と個人の関係性を具体的に表記し，明確に議論する方法論を提案する．さらに，この記法を用いて情報の共有範囲の表記，情報とコンテクストの関係表記，プライバシの状態遷移の表記を行い，この記法の効果を確認した．また，実際に課題としてプライバシに関する議論がなされた実例への適用を行いこの記法の有効性の検証を行った．

キーワード：プライバシ，集合論，属性情報，情報コントロール権

A Proposal of an Arrangement Technique of a Relationship with a Privacy and an Individual by Applying a Technique of the Set Theory

Akihira Yoshimoto[1,a)] Takashi Shitamici[2]

Received: March 9, 2015, Accepted: September 2, 2015

Abstract: We propose a method for representation by using the mathematical set theory notation of the information and personal relationships involved in privacy, thereby enabling the objective and rational discussion of privacy. Argument about privacy became active in Japan such as an operation of "the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure" or a publication of "Policy Outline of the Institutional Revision for Utilization of Personal Data". It is indispensable to consider about a relation of individuals and information and the sharing reach of the personal information in these arguments. But the methodology, which describes specifically and logically relevant range of information, was unimproved. In this paper we propose a representation technique that can describe specifically and clearly the relationship with an individual and the information by applying a technique of the set theory. In addition to that, we have confirmed the effectiveness of this notation by performing a representation of a sharing reach of an information, a relationship of information and context and a transition of privacy state. Finally, we have applied this method to verify the validity to the example actually privacy becomes an issue.

Keywords: privacy, set theory, personal attribute, right to control information

1. はじめに

2013年5月に公布された「行政手続における特定の個人を識別するための番号の利用等に関する法律」[1]の施行にともない，個人情報に対する新たなカテゴリとして「特定

1 一般財団法人全国地域情報化推進協会
The Association for Promotion of Public Local Information and Communication, Minato, Tokyo 105–0001, Japan
2 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120–8551, Japan
a) yoshimoto@applic.or.jp

個人情報」が導入され，その取扱いに関する規範が強化されている．特定個人情報は同法で導入された「個人番号」をともなう個人情報のことであり，「個人番号」が持つ強力な個人特定能力から通常の個人情報に比べプライバシインパクトが大きく慎重な取扱いが必要とされている．そして，特定個人情報の適切な取扱いを確保すべく「特定個人情報保護評価指針」[2] が示されている．

一方で，パーソナルデータの取扱いに関してプライバシの保護を前提としつつも積極的な活用を進めるべきとされ，高度情報通信ネットワーク社会推進戦略本部を中心に制度整備が進んでいる．同本部決定によって 2013 年 12 月に「パーソナルデータの利活用に関する制度見直し方針」[3] が出され，パーソナルデータの積極的な活用とそのための個人情報保護法改正などの検討が進んでいる．同方針に，『個人情報及びプライバシーの保護を前提としつつ，パーソナルデータの利活用により民間の力を最大限引き出し，新ビジネスや新サービスの創出，既存産業の活性化を促進するとともに公益利用にも資する環境を整備する．さらに，事業者の負担に配慮しつつ，国際的に見て遜色のないパーソナルデータの利活用ルールの明確化と制度の見直しを早急に進めることが必要である』と謳われている．同じく同本部におかれた「パーソナルデータに関する検討会」で 2014 年 6 月に決定された「パーソナルデータの利活用に関する制度改正大綱」[4] では，「個人情報」の範囲明確化や本人同意なしにパーソナルデータを第三者提供可能とするための「個人の特定性を低減させたデータへの加工」などの検討を行い早期に法整備を行うべきとした．そして，「パーソナルデータの利活用に関する制度改正に係る法律案の骨子（案）」[5] では個人情報の定義を指紋や顔認証データ，電話番号や旅券番号などの符号へ拡充すると同時に個人特定能力を低減させ第三者提供を可能とする「匿名加工情報（仮称）」の概念が明記された．

このように特定個人情報，個人情報，パーソナルデータの取扱いなど個人のプライバシにかかわる詳細な議論が活発に行われているが，そこで必要となるプライバシにかかわる情報と個人の関係を明確に記述する方式が未整備である．たとえば個人に関する属性情報の共有範囲や，属性情報とその対象である個人や公開可否などの決定権を持つ個人などとの関係を具体的に表現する表記方法がない．その結果，共通認識に基づいた検討や正確な合意に基づく規定，ルールの作成の妨げとなっている．

本稿は集合論の表記方法を応用することにより，属性情報と個人の関係性や情報の共有範囲などプライバシ関連の諸範囲を具体的に定義，表記する方式を提案した．さらに属性情報に関し考察を行い，実例に応用することを試みた．本提案方式を用いるによって，プライバシ関連法整備などの議論の一助となることを論じている．

2. 自己情報コントロール権と属性情報

2.1 自己情報コントロール権とは

本稿では「個人」としていわゆる自然人を扱う．自然人たる個人はその性質として氏名や住所，病歴，思想信条など様々な属性情報を持っている．そして，望む自己像を形成するため，その属性情報をどの範囲にどのような経緯で公開するかを決定する．この属性情報の流通をコントロールする権利を「自己情報コントロール権」と定義する．

ある人物について理解する場合，共有された属性情報を通じてその個人を理解することになる．個人の性質は情報化され他者に伝えられ，個人に紐付けられた属性情報として処理される．属性情報は個人の性質そのものである．

その共有された属性情報に基づいた個人に対する評価が自己像である．他者は共有された属性情報からその個人を理解し，様々な評価を下す．他者が理解するのは個人に関する共有された属性情報だけである．結果として個人に関する一種の写像として自己像が形成される（**図 1**）．

そこで，個人は自分が期待する自己像を他者に形成させるため，その属性情報について公開や秘匿を選択する．望む自己像を実現するために，他者と共有する属性情報を選択し，必要なものを必要な経緯で必要な対象者にだけ共有しようとする．また，共有を必要と考えない属性情報については秘匿しようとする．このような自身の情報について，公開や秘匿を決定する権利は個人の自由として，いわば法的に認められた権限であると考え自己情報コントロール権と呼んでいる．

2.2 他者による情報コントロール権

属性情報の流通を他者が制御する場合もありうる．他者の支配下に置かれた情報であっても，自身に関する情報であれば一定の自己情報コントロール権は認められると通常解釈される．しかし，他者にもある程度は情報に対するコントロール権が認められる状況もある．

たとえばソーシャルメディアで完全公開されたプロフィールなどは他者から他者へ広く流通する可能性がある．この

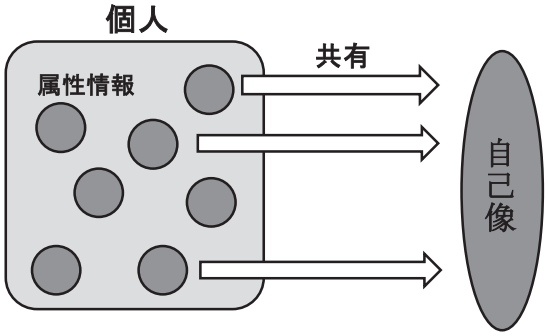

図 1 属性情報の共有と自己像
Fig. 1 Self-image and shared attributes.

ような情報は公開段階で他者に一定のコントロール権が及ぶことを許容したと考えられる．すでに，自身についての属性情報であるが，自己情報コントロール権にのみ左右される，自身のみコントロール可能な情報とはいえない状態となる．

本稿では自身の属性情報に限らず，他者の情報を含めて広く属性情報の流通を制御する法的な権限のことを「情報コントロール権」と呼ぶ．自己情報コントロール権は情報コントロール権の一部と考える．

属性情報を他者と共有することは，他者に情報コントロール権を認めることとなる場合がある．つまり，属性情報を中心に整理すると，属性情報の流通にともない属性情報に対する情報コントロール権を持つ個人は変化することとなる．

3. 関連研究

個人のプライバシについて論じるに，プライバシ権には確定的な定義は存在しない．日本においては自己情報コントロール権を定義とする説が有力とされるが，それを問題視する主張もある．これら情報とコントロール権の関係性についての検討は本稿の主題とする表記方法が活用できる部分である．本稿ではいったん，自己情報コントロール権のアプローチをとって表記方法の検討を進める．

まず，情報を財産権的 [6] に扱う自己情報コントロール権という考え方には問題があると指摘する意見 [7] がある．林 [8] は『情報という財貨は，もともと公共財的性質を持っているから，「占有」から「所有」へといった排他性の強い財に対する権利付与方式になじまず，これに事前に権利を設定することには困難がともなう』としたうえで『コントロールは手段であって保護の内容や権利ではない』と述べている．

しかし，自己情報コントール件的な整理，つまり財産権的に整理する場合には当然ながら，排他的な財として定義しない場合においても情報と個人の関係性は重要となる．むしろ排他的に定義できないからこそ関係性を端的に表現する手法が必要となる．そこで，本稿では自己情報コントロール権的な考え方をとり，情報と個人の関係を個人の権限として整理する形で表記方法の定義を進める．

情報と個人の関係性に関する研究としては，情報と個人のつながりを，個人の特定性や匿名性に着目して属性情報とプライバシの関係性として表記する研究が見られる [9]．ここでは情報を観測する Actor の視点で，個人など entity にかかわる情報がお互いにどのように関連性を持つか，つながり（relation）を持つかでプライバシに対する影響を整理している．つまり，Actor にどのような自己像が形成されるかを情報の relation を中心に表現している．

さらにこの考えを発展させ，個人に関する情報を object layer，information layer，contents layer の 3 階層に整理して Actor がどのように情報を認知するかを整理する表記方式も提唱されている [10]．

匿名性の観点からはプライバシを匿名性の双対として知識論理の手法で整理する研究がある [11]．ここでは行為者が情報に対してどのようなアクションをとったか，それによってどのような知識を得たかが論点となっている．

これらの研究は情報に対する観測者や行為者を中心に情報に対する認識の状況を整理して個人の特定性や匿名性の観点でプライバシを評価するものである．属性情報を中心にそれを知る個人や関係する個人の全体を整理する方式となっていない．

4. プライバシの集合論的表記

4.1 集合論的表記の意義

属性情報を中心とした表記方法を定義するために集合論的表記方法を応用する．ある属性情報に着目したときに，それにかかわる個人をその属性情報に関連する個人の集合として表現する．数学的な記法を利用することで論理的な表現を可能とする．

まず，属性情報の共有範囲を集合論的に表現することが可能である．属性情報についてプライバシの観点から考察するには，その属性情報がどの範囲で共有されているかを明確に表現することが重要となる．属性情報の共有範囲を定義する最少単位を個人と考えたとき，ある属性情報の共有範囲はその属性情報を共有する個人の集合として表記することができる．

さらに，数学的な集合の表記法を導入することで論理的に共有範囲を表記できる．たとえば，共有範囲の拡大は集合の元の増加として表現される．あるいは，いくつかの共有範囲が統合するといった変化は集合の結合として表現できる．このように集合論の記法を用いることで属性情報にかかわる個人の変化を数学的に数式によって明確に表現することができる．

4.2 属性情報と個人の関係の表記

属性情報を中心とした整理を集合論の記法で行う場合，集合に性質を持たせることで単なる共有範囲の表現にとどまらず，「特定の関係性を持って共有している範囲」という詳細な表現も可能となる．たとえば，単に属性情報を知っているだけの集合，知っていてかつ情報コントロール権も持つ集合というように集合ごとに性質を持たせることで属性情報と一定の関係性を持つ個人の範囲を表現することができる．

属性情報と個人の関係は多様であるが，集合論を用いた表現は柔軟であり，様々な分類を用いて整理することができる．集合には様々な性質を定義することが可能であり，分析の要件に応じた分類を定義すればよい．属性情報の流通にともなう変化をどのような軸で分類，分析したいかに

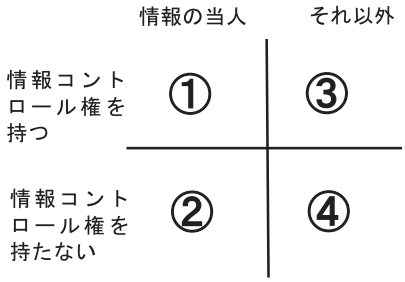

図 2 個人との関係の四象限
Fig. 2 Four dimension of relationships between individuals.

よって適切な性質を持つ集合を定義できる．

4.3 プライバシ分析のための関係性表記

前節で述べたように集合論的表記では個人と属性情報の様々な関係を分類して表記することが可能である．そこで本稿では個人と属性情報との関係を属性情報の流通にともなうプライバシへの影響を評価するために

- 属性情報の対象である個人
- 属性情報に対する情報コントロール権を持つ個人
- 単に知っているだけの個人

という 3 種類の集合に分類して表記する．

まず，ある属性情報に着目すると個人はその属性情報が表している人間，つまり情報の当人とそれ以外に大別される．また，その属性情報に対して情報コントロール権を持つ個人と持たない個人にも大別される．この 2 つの軸で属性情報と個人の関係は四象限に分類される（**図 2**）．

ある属性情報 d についてその情報が表す人間を

$Pdef(d)$：a Person defined by d

と表記する．また，その属性情報について情報コントロール権を持つ人間を

$Ppos(d)$：a Person possessing d

と表記する．さらに，その情報が表現する対象ではなく，また情報コントロール権も持たないが情報を知っている傍観者を

$Pspc(d)$：a Person spectating d

と表記する．

図 2 の象限に合わせると①および②が $Pdef(d)$ に相当する．①および③が $Ppos(d)$ に対応する．そして④が $Pspc(d)$ となる．

一般に $Pdef(d)$，$Ppos(d)$，$Pspc(d)$ ともに複数人が該当しうるため，それぞれ個人の集合として表記される．

$$Pdef(d) = \{p1, p2, p3 \ldots pn\}$$
$$Ppos(d) = \{p1, p2, p3 \ldots pn\}$$
$$Pspc(d) = \{p1, p2, p3 \ldots pn\}$$

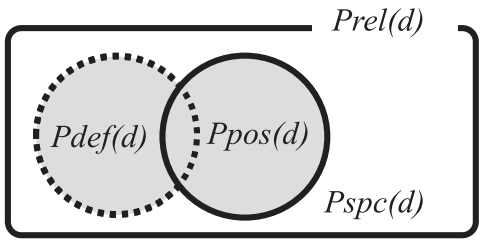

図 3 共有範囲の定義
Fig. 3 Definition of shared scopes.

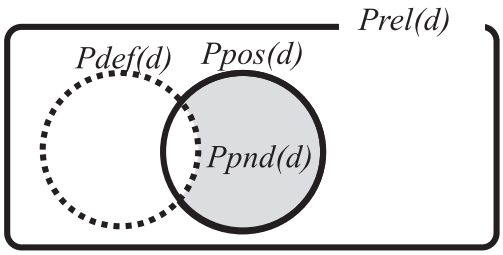

図 4 属性の対象外だがコントロール権を持つ集合
Fig. 4 Rights to control except scope of attributes.

ここで pn は特定個人を表す．

このように属性情報と個人の関係を個人の集合として表記することができる．

属性情報の共有範囲全体をその属性情報に関わるすべての個人の集合 $Prel(d)$ と考えれば共有範囲全体は

$$Prel(d) = Pdef(d) \cup Ppos(d) \cup Pspc(d)$$

と表記することができる．定義から

$$Pdef(d) \cap Pspc(d) = \emptyset$$
$$Ppos(d) \cap Pspc(d) = \emptyset$$

である（**図 3**）．

さらに，属性情報が表記する対象ではないが情報コントロール権を有する個人の集合を

$$Ppnd(d) = Ppos(d) \backslash Pdef(d)$$

と表記する（**図 4**）．

逆に，属性情報が表記する対象であるが情報コントロール権を持たない個人の集合を考えることも可能であり，

$$Pdnp(d) = Pdef(d) \backslash Ppos(d)$$

と表記する（**図 5**）．

図 2 の分類では $Ppnd(d)$ は③，$Pdnp(d)$ は②に対応する．

4.4 属性情報の共有範囲を決定づけるコンテクスト

ここまで属性情報の共有範囲を「属性情報に関わる個人の集合」として属性情報を中心にみて表記する方法を定義してきたが，共有状態をより正確に表記するためにはさらにパラメータとしてコンテクストを考える必要がある．属

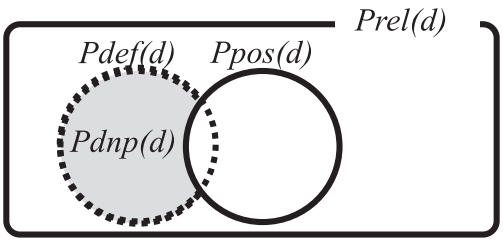

図 5 属性の対象だがコントロール権を持たない集合
Fig. 5 Un-control rights except scope of attributes.

性情報にかかわる個人は固定されておらず，属性情報が流通するなかで変化する．その変化を表現するためのパラメータとしてコンテクストを導入する．

属性情報の共有範囲はその情報内容だけで決定されるものではない．誰についての情報なのか，すなわち $Pdef(d)$ については情報内容が指し示す個人であり，情報内容で定まる部分が大きい．しかし，誰に情報コントロール権があるのか，すなわち $Ppos(d)$ については情報内容自体では必ずしも定まらない．

情報コントロール権の有無は同じ情報であっても情報流通の中で属性情報がおかれている背景・文脈によって異なるため，これをコンテクストと呼び，集合論的表記のパラメータの 1 つとする．たとえば，個人間の親展情報というコンテクストで伝えられた情報は，第三者に公開することは許されないと考えるのが通常である．一方で，その情報を SNS などの公開の場で知ったのであれば同じ SNS のコンテクストでは第三者との話題に出すことは許されるだろう．

属性情報がおかれる背景や文脈であるコンテクストは多様な要素から構成されており，単純な評価は困難である．一方で，属性情報の流通という時系列の流れの中で変化する要素としてパラメータの性質を備える．本稿では表記方法の定義を進めるため，コンテクストをパラメータとして簡略に表現して議論を進める．コンテクストについては 8 章でも改めて触れる．

4.5 属性情報とコンテクストの関係の表記

情報の共有範囲は同じ情報であってもどのような経緯，どのような背景で情報が準備されたかなどのコンテクストによって異なる．そのためコンテクストをパラメータとした表記方法を導入する．

あるコンテクスト cnt に対する $Ppos(d)$，$Pspc(d)$ を

$$Ppos(d, cnt)$$

$$Pspc(d, cnt)$$

と表記する．たとえばある個人 p はコンテクスト $cnt1$ では傍観者である $Pspc(d)$ に，コンテクスト $cnt2$ では情報コントロール権を持つ $Ppos(d)$ に，すなわち

$$p \in Pspc(d, cnt1), \quad p \in Ppos(d, cnt2)$$

となりうる．

$cnt1$ の文脈では秘匿されている情報 d を限定された個人 p には教えるが公開などの情報コントロール権は認めないとする．この場合，$p \in Pspc(d, cnt1)$ である．次に，$cnt2$ では状況が変わり，情報 d が広く一般公開されて p のみに限定されたものではなくなり必然的に公開などの情報コントロール権も認めうる状況になったとする．この場合，$p \in Ppos(d, cnt2)$ と変化する．

4.6 個人特定性とコンテクストの関係

$Pdef(d)$ に関しては誰に関する情報であるかという個人との紐付きが集合を決定づける．属性情報 d が誰を表しているか，d から誰が特定されるかが集合 $Pdef(d)$ の元を決定づける．属性情報から個人が特定される性質を本稿では「個人特定性」と呼ぶ．個人特定性を持つ属性情報 d は $Pdef(d)$ を持ちうる．

属性情報の個人特定性は属性情報の内容自体で決定される部分が多いが，コンテクストに依存する面もある．同じ属性情報に対してもコンテクストに応じて背景知識が異なると個人が特定される場合，されない場合が生まれる．背景知識との組合せによって個人が特定される場合があるからである．

個人特定性のコンテクストへの依存度合いは属性情報の種類によって異なる．たとえば，一般に実名 [12] といわれる公的機関によって定義された個人名はコンテクストに依存せず個人特定性を発揮する識別子である．よって，実名とともに公的機関によって管理される戸籍や住民基本台帳などはコンテクストに依存せずに $Pdef(d)$ を持ちうる d の例である．一方でソーシャルメディアなどに用いられる仮名はコンテクスト内では個人を特定するが，コンテクストが変化すると個人特定性を失う可能性のある識別子であり，仮名をともなう属性情報が $Pdef(d)$ を持つかはコンテクストに依存する．

また，個人特定性がコンテクストに依存する場合でも，いったん個人が特定された場合，コンテクストが変化しても個人特定性は変化しにくい．一度誰に関する情報であるかが知られた状況で，コンテクストが変化したからといって，その事実が忘れ去られることを期待するのは困難だからである．

個人特定性とコンテクストの関係は単純な依存関係と整理できないため，本稿では $Pdef(d)$ は個人特定性に依存すると整理するにとどめ，パラメータとしてコンテクストに依存するとはしない．個人特定性については 8 章であらためて述べる．

ここまで本節ではプライバシを集合論的アプローチによって探求することによって，

- 属性情報の共有範囲や個人との関係
- 属性情報とコンテクストの関係

の表記方法を定義した．次章ではこれらの表記方法を利用し，具体的な適用を行う．

5. 集合論的表記の適用

前章では，プライバシにおける集合論的表記方法を定義した．本章では具体的に

- 自己情報コントロール権所在の表記
- プライバシの状態遷移の表記

への適用を試みる．本章では表記を簡略化するためにコンテクストパラメータを省略している．

5.1 自己情報コントロール権所在の表記への適用

集合論的表記を用いることで属性情報について情報コントロール権を持つ者の定義，自己情報コントロール権の適用範囲の定義などを具体的に行うことができる．

たとえば，情報の当人は情報コントロール権を持つべき，つまり自己情報コントロール権を完全に認めるべきとする考えを集合論的表記で表すと $Pdef(d) \subseteq Ppos(d)$ であり，$Pdnp(d) = \emptyset$ となる（図 **6**）．

あるいは，属性情報の当人以外には情報コントロール権を認めない場合には $Pdef(d) = Ppos(d)$ であり，$Ppnd(d) = \emptyset$ となる（図 **7**）．

このように自己情報コントロール権に対する様々な考え方を明確に曖昧さなく表現することができる．

5.2 プライバシの状態遷移の表記への適用

集合論的表記を応用することにより，属性情報のプライバシ上の状態変化を共有範囲の変化として表記し，その遷移などを表現することができる．

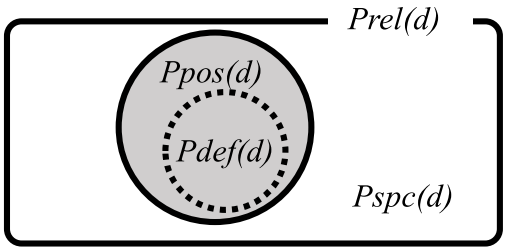

図 6 自己情報コントロール権を絶対とする場合
Fig. 6 Absolute rights to control self-information.

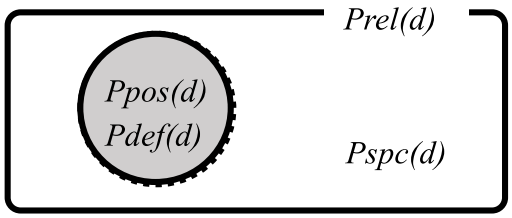

図 7 情報の当人にのみコントロール権を認める場合
Fig. 7 Permitted rights to control self-information.

5.2.1 プライバシ上の状態定義

状態遷移を表記するにあたって，まず属性情報のプライバシ上の状態を情報の共有範囲に着目して以下のように 3 段階に分類する．

プライベート（Pr）：本人しか知らない状態

シェアード（Sh）：特定のコンテクストで特定の人間の間で共有されている状態

パブリック（Pb）：共有範囲が無制限，あるいは特定できない状態

属性情報はその内容や性質にかかわらず，上記の 3 段階いずれかの状態に属すると考えられる．

状態の遷移は通常，情報が発生することから始まり，プライベート，シェアード，パブリックと順方向に遷移するが，時には逆方向の遷移も発生しうる．順方向の遷移は情報の生成および公開によって生じ，逆方向の遷移は情報の秘匿および破棄によって生じる．

逆方向の遷移はいわゆる「忘れられる権利」[13] に相当し，実際には実現困難である場合が多い．逆方向の遷移のためには物理的なデータ削除だけでなく，記憶にある情報を公開させないための制度やモラル啓発などさらに困難な要素がある．匿名化も逆方向遷移手段の 1 つと考えることができるが，以下の議論では属性情報の加工は新たな属性情報の生成と整理して元の属性情報のプライバシ状態遷移とは区別する．

状態の遷移を実行する法制度的な権利，権限を「情報コントロール権」，特に自身の情報について状態を遷移させる権利を「自己情報コントロール権」と整理することができる．

5.2.2 状態遷移の表記

次に，前項で定義したプライバシ状態の遷移を集合論的表記で表記する．プライバシ状態の遷移は，属性情報の共有範囲の変化として表記することができるので，集合論的表記を応用することが可能である．そこで具体的な応用を試みる．

まず前述の 3 つのプライバシ上の状態定義を集合論的表記を用いて改めて定義すると下記のようになる．

***Pr* 状態の定義**

$$Prel(d) = Pdef(d) = Ppos(d)$$
$$Pspc(d) = \emptyset, \quad Ppnd(d) = \emptyset, \quad Pdnp(d) = \emptyset$$

Pr 状態では傍観者である $Pspc(d)$ は空集合である．また，Pr 状態の性質から共有範囲全体である $Prel(d)$ の構成員すべてが情報コントロール権を持つと考えられ $Ppnd(d)$, $Pdnp(d)$ も空集合である．

***Sh* 状態の定義**

$$Prel(d) = Pdef(d) \cup Ppos(d) \cup Pspc(d)$$

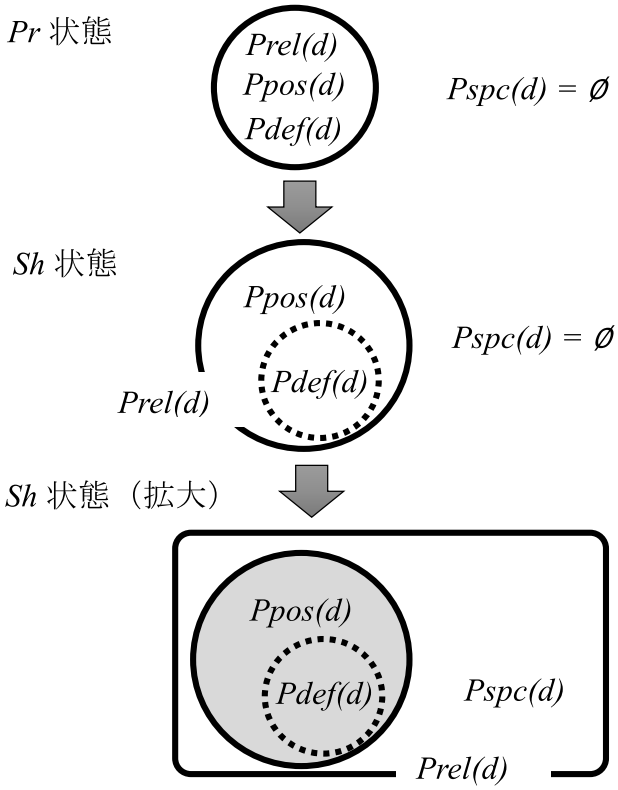

図 8 プライバシ状態の遷移
Fig. 8 Transitions of privacy status.

Sh 状態では属性が表す個人である $Pdef(d)$ 以外の者とも情報は共有されている．また，その中には情報コントロール権を持つ者と持たない者が考えらえるので $Ppos(d)$ と $Pspc(d)$ が存在する．

特殊な状態として属性情報を知っている個人はすべて情報コントロール権を持っている，つまり $Pspc(d)$ が空集合であり，

$$Prel(d) = Pdef(d) \cup Ppos(d)$$

となることもありうる．

一般的には，$Pdef(d) \subseteq Ppos(d)$ であるが，自身に関する情報でありながら，自身に情報コントロール権がない状態，すなわち自己情報コントロール権が否定された $Pdnp(d) \neq \emptyset$ も理論上考察可能である．

***Pb* 状態の定義**

$$Prel(d) = Pdef(d) \cup Pspc(d)$$

Pb 状態では情報を知っている個人は不確定であり，あらゆる個人が $Prel(d)$ の元になりうる．また情報コントロール権の制約はほぼ不能の状態であり，情報コントロール権を持つ個人の集合 $Ppos(d)$ は情報を知るすべての個人とするか，逆に誰も明確に情報コントロール権を持たない状態，つまり $Ppos(d)$ は空集合と定義するかのいずれかとなる．Pb 状態を他の状態に遷移させることが事実上困難であることを考慮し，明確な情報コントロール権の所有者はいない，つまり $Ppos(d) = \emptyset$ と整理する．

典型的な遷移は図 8 のように表記できる．この例では Pr 状態にあった属性情報から情報の対象者ではないが情報コントロール権を持つ人物，すなわち $Ppnd(d)$ が現れて Sh 状態になっている．しかしこの状態ではまだ情報を知っているだけの $Pspc(d)$ は空集合である．

次に情報の共有範囲がさらに拡大して $Pspc(d)$ が現れる．この状況でも自己情報コントロール権は保障されており，情報の対象者である $Pdef(d)$ はすべて $Ppos(d)$ の部分集合となっている．つまり $Pdnp(d)$ は空集合である．

このように集合論的表記を用いることで各プライバシ状態の定義を明確にすることができるため，その遷移も具体的に表現し，議論することができる．

6. 属性情報の性質と情報コントロール権の所在に関する考察

前章で定義した表記方法を応用することにより，属性情報の性質と情報コントロール権の所在の関係性の考察を試みる．

6.1 属性情報の性質

属性情報には遺伝子情報や思想，信条のように属性情報が表す個人の集合である $Pdef(d)$ が自身に閉じた状態で本質的に持っている情報と，購買履歴や乗降履歴のように他者との相互作用の結果として生成され，生成の当初から他者との関係性の中に存在する情報がある．これらを以下のように表記する．

innate personal data ($InPD$)：当人が本質的に備えている情報

mutual personal data ($MuPD$)：他者との相互作用から生まれる情報

$InPD$ は当人だけが情報を持つ，個人に閉じた状態がある一方，$MuPD$ は必ず他者との情報共有があり個人に閉じた状態はない．$InPD$ は他者とは無関係に，属性が表す個人の集合 $Pdef(d)$ に内在して自発的に生じうるため，誰とも共有されず 1 人に閉じた状態で存在しうる．一方で $MuPD$ は他者との相互作用によって生じることから，ある情報 d に対して相互作用相手にも必然的にわたる情報 d' が必ず存在する．よって 1 人に閉じた状態で存在することがない．たとえば購買履歴である d に対しては，d と類似の情報である販売履歴 d' が販売側にもわたる．

d と d' は必ずしも同じ内容とは限らないが，ここでは議論を単純化するため，$MuPD$ としては双方で共通の部分を扱うものとする．たとえば購入した当人が所有する購買履歴 d は当然に自分が購入したという事実を含む．一方で販売履歴 d' には誰に売ったかは含まれない場合もありうる．ここでは $MuPD$ は相互作用の双方で共有される d' 部分，たとえば買った商品名を対象とし，d のみに含まれ d'

と重なりのない部分，たとえば誰が買ったかという情報は $InPD$ の一種として取り扱うこととする．

6.2 $InPD$ の情報コントロール権所在についての考察

属性情報に対する情報コントロール権の所在はどうあるべきかを前項で定義した $InPD$ と $MuPD$ の双方について考察する．

$InPD$ は自身に内在する性質として持つものであり，通常は当人に情報コントロール権があって当然であると解釈される．すなわち，

$$Pdef(InPD) \subseteq Ppos(InPD) \tag{1}$$

である．

Pr 状態ではその定義から

$$Pdef(InPD) = Ppos(InPD)$$

であり式 (1) が成り立つことは自明である．

Sh 状態では情報コントロール権のみを持つ集合である $Ppnd(InPD)$ が定義可能である．$Ppnd(InPD)$ はコンテクストに依存するので $Ppnd(InPD, cnt)$ と表記される．

$$Ppnd(d, cnt) = Ppos(InPD, cnt) \backslash Pdef(InPD)$$

つまり，

$$Ppos(InPD, cnt) = Pdef(InPD) \cup Ppnd(InPD, cnt) \tag{2}$$

と表記することができる．

式 (2) の各項では，第 1 項は個人特定性が，第 2 項はコンテクストが支配的な要素となる．なぜならば，第 1 項である $Pdef(InPD)$ は，4.6 節で整理したとおり個人特定性に依存する集合である．第 2 項である $Ppnd(InPD, cnt)$ はパラメータとしてコンテクストを持ち，個人特定性には非依存にコンテクストごとに何らかの判断基準を持って情報コントロール権を持つ，持たないを判定し元を定義することとなるからである．

$InPD$ の Sh 状態の情報コントロール権の所在範囲は，個人特定性によって制約される $Pdef(InPD)$ と，個人特定性とは無関係なコンテクストごとの個別規定で制約される $Ppnd(InPD, cnt)$ の和集合と整理できる．

6.3 $MuPD$ の情報コントロール権所在についての考察

$MuPD$ は発生した時点ですでに何らかのコンテクストの中にあり Pr 状態は存在しない．よって，Sh 状態における情報コントロール権の議論となる．

$MuPD$ に対しては当人が情報コントロール権を必ず持つ，つまり式 (1) に相当する

$$Pdef(MuPD) \subseteq Ppos(MuPD)$$

の条件は必ず成り立つとはいえない．$MuPD$ は相互作用から生まれるため相互作用を与える側，受ける側どちらか一方に全権があるとはならず，双方に相互作用が生じた際のコンテクストに依存して何らかの情報コントロール権がありうる．一方で，双方に必ず情報コントロール権があるともいえず，どちらか一方のみの場合もありうる．たとえば個人に対する観察や調査の結果は調査対象当人についての情報でありながら，当人が収集された情報に対して公開や破棄などの情報コントロール権を持たない場合も考えうる．また，情報の分析結果などでは，自身のことでありながら当人が認識していな事実を他者だけが知っている状態すら考えられる．

$MuPD$ の Sh 状態の情報コントロール権の所在については $Pdef(MuPD)$ に情報コントロール権の絶対的な保障がないため，式 (2) に相当する

$$Ppos(MuPD, cnt) = Pdef(MuPD) \cup Ppnd(MuPD, cnt)$$

は成立しない．$Pdef(MuPD)$ から情報の当人でありながら情報コントロール権を持たない者の集合である $Pdnp(MuPD)$ を除く必要がある．$Pdnp(MuPD)$ はコンテクストに依存するので，パラメータとしてコンテクストを導入し，

$$Ppos(MuPD, cnt) = (Pdef(MuPD) \backslash Pdnp(MuPD, cnt)) \cup Ppnd(MuPD, cnt) \tag{3}$$

と表記することができる．

$MuPD$ の Sh 状態における情報コントロール権の所在範囲は $InPD$ 比べてコンテクストパラメータへの依存が大きいといえる．式 (3) から $MuPD$ の情報コントロール権の所在範囲は個人特定性によって制約される $Pdef(MuPD)$，個人特定性とは無関係なコンテクストごとの個別規定で制約される $Ppnd(MuPD, cnt)$，個人特定性とコンテクスト双方に影響を受ける $Pdnp(MuPD, cnt)$ の 3 種類に整理できる．$Pdef(MuPD)$ と $Pdnp(MuPD, cnt)$ はともに個人特定性が成立要件となる項であるが，後者はパラメータとしてコンテクストを持ちコンテクスト依存の性質も持つ．cnt 依存項を 2 つ含む式 (3) で表される $Ppos(MuPD, cnt)$ は cnt 依存項が 1 つである式 (2) で表される $Ppos(InPD, cnt)$ に比べてコンテクストパラメータへの依存が大きいといえる．

なお，自己情報コントロール権を絶対的に認めるべきとの考え方もある．その場合，式 (1) に相当する

$$Pdef(MuPD) \subseteq Ppos(MuPD)$$

が絶対的な要件となる．

7. 実例に対する応用

本章では集合論的表記方法をプライバシ関連検討の実例に適用し，その有効性を検証する．

7.1 第三者による観測結果としての属性情報

独立行政法人情報通信研究機構が中心となって大阪駅ビル「大阪ステーションシティ」で実施された「大規模複合施設における ICT 技術の利用実証実験」は 92 台のデジタルビデオカメラを設置して通行する一般人を撮影し，顔認証技術が大規模災害時の避難誘導へ応用可能性であるかを検証する実証実験である [14]．

この実証実験においては個人の顔画像を取得するという性質から，これがプライバシ権の侵害にあたるのかについて詳しく議論されている．本実験の報告書ではプライバシ権との関係について

① 画像の撮影
② Work-ID の生成
③ 映像解析処理の実施による特徴量情報の生成
④ 移動経路情報の生成
⑤ 顔特徴量解析または歩行者検知解析
⑥ JR 西日本らへの人流統計情報の提供

を検討課題としている．

たとえば「画像の撮影」について報告書では『何人も，その承諾なしに，みだりに撮影されない法律上の利益を有するというべきである』とし，さらに被撮影者の行動記録に直結することからも『みだりに撮影されない法律上の利益は，プライバシー権の一内容としても法律上保護されると解するべきである』としている．

ここで，撮影された画像は撮影者があってこそ成立するものであり，観測結果として得られる典型的な $MuPD$ である．

$MuPD$ である撮影画像情報 d について撮影段階では属性が表す個人だが情報コントロール権を発揮できない個人の集合 $Pdnp(d)$ が存在する．むしろ $Pdef(d) = Pdnp(d)$ といえる状況である．画像の撮影を行っていることは広報されている．しかし，撮影されたくないと希望する個人がいたとして，撮影の事実を知りえても撮影を避けるために鉄道駅に行かない，つまり鉄道駅を利用しないという選択肢をとれない場合は多い．結果，実質的には当人の望む望まないにかかわらず撮影されることとなり，当人に撮影されない，つまり情報を生成しないという自己情報コントロール権を行使しうる状況とはいい難い．

当人が撮影をされないという自己情報コントロール権を持ちにくいという点についてこの実証では画像情報が揮発性メモリ上にごく短時間存在するだけであり，人間が閲覧する機会がないことからプライバシ権の侵害はないかあっても些細であるとしている．撮影時のコンテクストでは $Pdef(d) = Pdnp(d)$ であり，当人は情報コントロール不能であるが，属性情報が表す個人ではないが情報コントロール権を持つ側，つまり $Ppnd(d)$ である撮影側ですら情報 d に直接アクセスすることはなく，他のコンテクストに移行するまでもなく破棄されるのでプライバシ侵害にはならないとの整理である．撮影された画像は揮発性メモリ内で即座に次に述べる「特徴量情報」に変換されて利用されることとなる．その際に利用される 1 台のカメラフレーム内で撮影された個人ごとに付与される Work-ID と呼ばれる識別子も特徴量情報の生成とともに消去される．

次に「特徴量情報」に対する情報コントロール権の所在について考察する．特徴量情報は撮影画像から「顔特徴量解析」「歩容解析」「マルチモーダル解析」によって個人識別が可能な情報として生成される．特徴量情報について報告書は『顔画像や歩容等から生成される特徴量情報は，パスワード等と異なり，変更できないから，指紋や虹彩，DNA 情報等の生体認証情報と同程度の法的保護が必要である』と述べている．この実証実験では特徴量情報については当人には情報コントロール権はない．プライバシ権の侵害について報告書は『プライバシー権の侵害がないとは言えない』と結論づけている．

特徴量情報については $MuPD$，$InPD$ 双方の観点から情報コントロール権の所在についての考察が可能である．特徴量情報は観測あるいはその解析結果として得られる情報で，当人すら認識していないものである．観測という相互作用から生まれる特徴量情報は典型的な $MuPD$ である．しかし，顔の特徴である特徴量情報は当人の生体からくるものであり，DNA などと同様に当人に本質的に備わる情報であるという観点からは $InPD$ の性質も備えている．つまり $MuPD$，$InPD$ 双方の観点から情報コントロール権の所在についての考察が可能である．

特徴量情報は撮影画像から生成され，特徴量情報など（特徴量情報および撮影された時刻，場所，判定された対象者の性別と概算年齢）として記録され移動経路情報の作成に利用される．特徴量情報などは観測対象者が観測範囲である大阪ステーションシティを退出したと認識された場合や営業時間終了後に削除される．

特徴量情報に関するコンテクストの流れは撮影画像の段階から整理すると，撮影時 ($cnt1$)，揮発性メモリ内で特徴量情報に変換される段階 ($cnt2$)，特徴量情報などとして移動経路情報作成に利用される段階 ($cnt3$) に分けられる．

プライバシ権侵害の可能性について特徴量情報 d を $MuPD$ として考察した場合，撮影時コンテクスト $cnt1$ では式 (3) から，

$$Ppos(d, cnt1) = (Pdef(d) \backslash Pdnp(d, cnt1)) \cup Ppnd(d, cnt1)$$

である．撮影を避けるために鉄道駅の利用を控えることは

できないとすれば，

$$Pdef(d) = Pdnp(d, cnt1)$$

であるので，

$$Ppos(d, cnt1) = Ppnd(d, cnt1)$$

となる．$Ppnd(d, cnt1)$ は実証実験実施者と同値である．実証実験実施者の集合を P とすると

$$P = Ppos(d, cnt1) = Ppnd(d, cnt1)$$

である．撮影結果が揮発性メモリにある段階 $cnt2$ では上述のとおり，誰も具体的な情報コントロールは行使できない状態である．つまり

$$Ppos(d, cnt1) = P \rightarrow Ppos(d, cnt2) = \emptyset$$

次に特徴量情報などとしての利用段階の $cnt3$ では，また実証実験実施者がコントロール可能となり

$$\begin{aligned} Ppos(d, cnt1) &= P \rightarrow Ppos(d, cnt2) \\ &= \emptyset \rightarrow Ppos(d, cnt3) = P \end{aligned}$$

$Ppos(d, cnt3)$ に関して式 (3) の

$$\begin{aligned} &Ppos(d, cnt3) \\ &\quad = (Pdef(d) \backslash Pdnp(d, cnt3)) \cup Ppnd(d, cnt3) \end{aligned}$$

を改めて考えたとき，

$$Ppnd(d, cnt3) = P$$

となる．ゆえに，

$$Ppos(d, cnt3) = (Pdef(d) \backslash Pdnp(d, cnt3)) \cup P$$

である．このとき，

$$Ppos(d, cnt3) = P$$

とすると，

$$Pdef(d) \backslash Pdnp(d, cnt3) = \emptyset$$

つまり

$$Pdef(d) = Pdnp(d, cnt3)$$

となり，当人に情報コントロール権がない状況が確認できる．

一方で，$InPD$ として $Ppos(d)$ の定義を特徴量情報などとしての利用段階のコンテクスト $cnt3$ について考えた場合，式 (2) から

$$\begin{aligned} Ppos(d, cnt3) &= Pdef(d) \cup Ppnd(d, cnt3) \\ &= Pdef(d) \cup P \end{aligned}$$

となるべきである．

しかし現状では

$$Ppos(d, cnt3) = P$$

であり $Pdef(d) = \emptyset$ となってしまうため上式が成り立たない．

特徴量情報は $InPD$ ではないと整理するか，もしくは $Ppos(d, cnt3) = P$ を否定し $Pdef(d)$ に自己情報コントロール権を与える，すなわち特徴量情報の利用を拒否する権利があるとするべきとなる．数式化することによって $cnt3$ の段階で自己情報コントロール権を認めるべきかの議論がより明確になる．

7.2 ポイントカードによる購入履歴などの第三者提供

大手ポイントカードである T ポイントカードを運営するカルチュア・コンビニエンス・クラブが，T ポイントカードに関する利用規約を変更し，個人情報の提供を「共同利用」から「第三者提供」へ切り替えたことについては多くの注目を集めた [15]．

従来はカルチュア・コンビニエンス・クラブとグループ会社およびポイントプログラム参加企業との間の「共同利用」と定義されていた T ポイントカード会員の個人情報を，グループ会社とポイントプログラム参加企業や TSUTAYA 加盟店などの T 会員向けサービスを提供する企業に「第三者提供」すると変更したものである．そして，会員当人からオプトアウトによる第三者提供の停止を可能とした．

主要な情報である利用履歴（商品の購入履歴など）について考察すると，商品の購入などの相互作用によって生じる情報であるので $MuPD$ と考えることができる．購入者が T カードを提示しなくても店舗はどのような商品が購入されたかの情報を取得するので，$MuPD$ としての購入履歴情報は購入者と販売者の双方で共有される．しかし，一般的に購入履歴情報は誰が購入したかという個人特定性は低く，プライバシインパクトは低い．

ところが，購入者が T カードの提示を行うことで個人特定情報との紐付きが生じる．個人に関する情報として情報コントロール権の所在について考察することが可能である．

T カードと紐付いた形での購入履歴に関してのコンテクストの流れは，商品を購入して T カードを提示する段階 ($cnt1$)，購入履歴情報が商店で収集された段階 ($cnt2$)，購入履歴情報がグループ会社などと共有された段階 ($cnt3$)，共有された情報が分析され活用された段階 ($cnt4$) に分類できる．

購入段階 $cnt1$ において購入履歴情報 d について式 (3) は

$$\begin{aligned} &Ppos(d, cnt1) \\ &\quad = (Pdef(d) \backslash Pdnp(d, cnt1)) \cup Ppnd(d, cnt1) \end{aligned}$$

である．T カードを提示するかの自由は完全に購入側にあ

ることから，属性が表す個人だが情報コントロール権のない集合や，逆に属性が表す個人ではないが情報コントロール権を持つ集合は空集合といえるので

$$Pdnp(d, cnt1) = \emptyset, \quad Ppnd(d, cnt1) = \emptyset$$

であり，

$$Ppos(d, cnt1) = Pdef(d)$$

となる．

いったん収集されると販売店舗経由でカルチュア・コンビニエンス・クラブが全権を持つため逆に

$$Pdef(d) = Pdnp(d, cnt2)$$

となり，

$$Ppos(d, cnt2) = Ppnd(d, cnt2)$$

となる．

従来の「共同利用」では共同利用相手も含めた全体が $Ppos(d, cnt2)$ であった．したがって，情報の共有段階である $cnt3$，そのあとの情報分析や利活用段階の $cnt4$ においては

$$Ppos(d, cnt3) = Ppnd(d, cnt3) = Ppos(d, cnt2)$$
$$Ppos(d, cnt4) = Ppnd(d, cnt4) = Ppos(d, cnt2)$$

となっていた．

この段階ではすでに $Pdef(d)$ によるコントロールは不能の状態となる．

共同利用が第三者提供へと変わることで $Ppnd$ がカルチュア・コンビニエンス・クラブと提供先に分類される．カルチュア・コンビニエンス・クラブの情報利用者に対応する $Ppnd$ を $Pccc$，提供先の情報利用者に対応する $Ppnd$ を $Pp3$ とすると

$$Ppos(d, cnt2) = Pccc$$
$$Ppos(d, cnt3) = Pdef(d) \cup Pccc$$
$$Ppos(d, cnt4) = Pccc \cup Pp3$$

$cnt3$ における $Pdef(d)$ がオプトアウト形式による第三者提供の停止に相当する．

$cnt3$ では自己情報コントロール権は確保されている．そこで，ここでの課題は自己情報コントロール権の所在よりも自己情報コントロール権を実行に移すうえで必要となる有効な本人同意の取得方法やオプトアウト手順の妥当性といった議論となる．

$cnt3$ 段階のオプトアウト手順の妥当性の観点では，本人がオプトアウト権の存在を第三者提供の実施前に知り，権利行使が可能となっている必要がある．第三者提供先が追加される場合など，状況の変化から第三者提供実施までの時間間隔で十分なオプトアウト機会が提供されているかの議論となる．

第三者提供先の追加など状況の変化から最初の第三者提供実施までの期間を $cnt3'$ とすると，本人に周知されるまでの間 $Ppos(d, cnt3') = Pccc$ となってる期間があるのではないかという懸念となる．

8. 今後の課題

8.1 個人の定義

本稿では情報コントロール権を持つ個人の集合などを議論するにあたり個々の個人の定義については詳述していないが，より広範囲に適用するには個人の定義を明確にする必要がある．簡単には物理的な 1 人が 1 個人であり，その集合が本稿の定義である集合体になる．しかしコンテクストに依存する形で物理的な 1 人が複数の人格を持つことがあり，そのような状況への対応は今後の課題である．

物理的に 1 人の人間が複数の個性，すなわちペルソナを持ち，それぞれに独立したアイデンティティを主張することは十分に考えうる．たとえばSNS などのネットワーク社会を対象に議論する場合，ここでの個人はそれぞれの SNS に登録されたアカウントのことと考えることもできる．この場合，1 人の個人が複数のアカウントを使い分け，さらにそれぞれに属性情報に対する異なる権限を主張することは十分にありうる．

8.2 個人特定性の定義

個人と属性情報の紐付きは個人特定性の議論となる．本稿では個人特定性をコンテクストに単純に依存しないとし，$Pdef(d)$ をコンテクスト依存とせずに扱っている．しかし，一般的には個人特定性はコンテクストに依存する面があり，個人特定性の詳細な扱いは今後の課題である．

ある属性情報が個人を特定しうるかは誰がどのような背景知識を持ったコンテクストでその情報を扱うかに依存して変化する．つまり，属性情報の観測者に依存して個人特定性は変化する．本稿では属性情報を中心とした表記方法を提案している．属性情報そのものを独立して扱うため，誰がその属性情報を観測し，評価するのかという点について表現されない．

複数の属性情報が組み合されることで個人が特定され，あるいはプロファイリングによる個人像が形成されるといった状態の記述は観測者を中心に観測対象の属性情報を集合的に取り扱う方式に利点がある．属性情報中心につまり個々の属性情報を独立して着目する本稿の方式での整理が困難な部分であり，引き続き検討を要する．

8.3 コンテクストの定義

本稿において Sh 状態はコンテクストに依存するとしてパラメータ cnt を導入し集合の定義を行ったが，逆にコン

テクストを個人の集合として定義することも考えられ今後の課題である．

コンテクストを独立したパラメータで表記可能であると仮定することで，コンテクスト依存である情報コントロール権の所在を情報コントロール権を持つ個人の集合として表記することができた．

しかし，コンテクストの定義自体複雑なものであり，単純にパラメータとして表記できない場合も考えられる．その場合コンテクストそのものを関連する個人の集合としてとらえ，表記することも検討することができる．

この場合，個人の集合としてのコンテクストと，個人の集合としての情報コントロール権の所在を多元的に考察する必要が生じる．

9. まとめ

本稿では，プライバシと個人の関係性を表記可能とするために，集合論的表記方法を定義した．本表記方法を用いることにより，

- 属性情報の共有範囲や個人との関係
- 属性情報とコンテクストの関係

の表現を可能とした．この表記方法を用いることによって，自己情報コントロール権の所在表記やプライバシの状態遷移表記を行うことが可能である．

次に，属性情報の性質と情報コントロール権の所在に関する考察に本表記方法を応用して実施し，プライバシ関連の考察に対する有用性を示した．

さらに，近年注目された 2 事例，監視カメラによる顔認証の事例，ポイントカードの利用履歴第三者提供の事例の考察を本方式で行い，実例における適用性の検証を行った．

いずれにおいても本表記方式によって議論を明確化することに成功し，十分有効な表記方法であることが確認できた．

参考文献

[1] 平成二十五年法律第二十七号
[2] 特定個人情報保護評価指針，入手先 ⟨http://www.cas.go.jp/jp/seisaku/bangoseido/kojinjoho/⟩.
[3] パーソナルデータの利活用に関する制度見直し方針，入手先 ⟨http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/dec131220-1.pdf⟩.
[4] パーソナルデータの利活用に関する制度改正大綱，入手先 ⟨http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryou2.pdf⟩.
[5] パーソナルデータの利活用に関する制度改正に係る法律案の骨子（案），入手先 ⟨http://www.kantei.go.jp/jp/singi/it2/pd/dai13/siryou1.pdf⟩.
[6] 石井夏生利：プライバシー・個人情報の「財産権論」，情報通信政策レビュー，No.4 (2012).
[7] 青柳武彦：「プライバシー＝自己情報コントロール権」説の批判的一考察，情報社会学会誌，Vol.2, No.3 (2008).
[8] 林紘一郎：「個人データ保護」の法益と方法の再検討：実体論から関係論へ，情報通信学会誌，Vol.31, No.2 (2013).
[9] Veeningen, M., de Weger, B. and Zannone, N.: Modeling Identity-Related Properties and Their Privacy Strength, *Proc. FAST2010*, LNCS 6561, pp.126–140, Springer (2011).
[10] Veeningen, M., de Weger, B. and Zannone, N.: Formal Privacy Analysis of Communication Protocols for Identity Management, Information Systems Security, *Proc. ICISS2011*, LNCS 7093, pp.235–249, Springer (2011).
[11] 塚田恭章，真野 健，櫻田英樹：フォーマルメソッドによるセキュリティ&プライバシ，NTT 技術ジャーナル，pp.22–25 (2011).
[12] 折田明子：ソーシャルメディア利用における「名乗り」とプライバシー：「実名」には何が求められるのか，経営情報学会 2012 年秋季全国研究発表大会予稿集 (2012).
[13] 一般社団法人電子情報技術産業協会：EU データ保護資料改定に関する調査・分析報告書 JEITA IS-12-情シ-4 (2012)，入手先 ⟨http://www.kantei.go.jp/jp/singi/it2/pd/dai10/siryou1-2.pdf⟩.
[14] 映像センサー使用大規模実証実験検討委員会調査報告書，入手先 ⟨http://www.nict.go.jp/nrh/iinkai/report.pdf⟩.
[15] 2014 年 11 月 1 日 T 会員規約を改訂しました，入手先 ⟨http://www.ccc.co.jp/customer/⟩.

吉本 明平

一般財団法人全国地域情報化推進協会．1993 年大阪大学大学院修士課程修了．修士（理学）．日本電気にて電子政府，電子自治体関連コンサルティングに従事．一般財団法人全国地域情報化推進協会にて地域情報化関連の標準化に取り組む．政府「社会保障・税に関わる番号制度情報連携基盤技術ワーキンググループ構成員」，「次世代電子行政サービス基盤等検討プロジェクトチーム引越ワンストップサービス実現検討 WG 構成員」，「電子私書箱（仮称）構想の実現に向けた基盤整備に関する検討会ユースケース検討 WG 構成員」等を歴任．

下道 高志 （正会員）

1982 年慶應義塾大学卒業．サン・マイクロシステムズで UNIX 国際機能の開発，Java，アイデンティティ技術，クラウド API の仕様策定・実装等に従事．日本オラクルで官民におけるアイデンティティ技術およびビッグデータ関連技術の適用実装に従事．2014 年東京電機大学後期博士課程修了．同年より東京電機大学情報セキュリティ研究所研究員．博士（工学）．警察庁総合セキュリティ対策会議委員，IPA Ruby 標準化ワーキンググループ委員，総務省スマートクラウド研究会技術ワーキンググループ構成員，ISO SC27/WG5 エキスパート等を歴任．