2015 年度　修　士　論　文

モバイル端末のプライバシー問題に関する
意識調査と世代間倫理

Intergenerational Equity on
Privacy Issue of Portable Smart Devices

加藤　弘則

Kato, Hironori

東京大学大学院新領域創成科学研究科

社会文化環境学専攻

内容梗概

モバイル端末の普及，モバイル端末に備わるセンサー機能の向上，データマイニング技術の向上に伴い，それぞれの端末が創出するデータの利活用が，サービスクオリティの向上，防災，都市計画，人口調査など，さまざまな分野で行われつつある．しかし，それらのデータの利活用にあたっては，プライバシー問題が噴出する事例も存在する．

そこで本研究では，そうしたデータ収集・利活用に関連して起こるプライバシー問題の解決・防止および，端末ユーザーが抱えるプライバシー意識を理解するため，社会学的調査方法を用い，質的調査と量的調査を行った．質的調査では，半構造化インタビューを行ったのち，KJ 法を用いて調査結果を分析した結果，モバイル端末が生み出すデータに関連したプライバシーの意識を類型化できた．プライバシー観の類型化に関しては，A.Westin による，プライバシーに対する意識をその強度に応じて「原則型グループ」「選択型グループ」「開放型グループ」の 3 つに分類した先行研究が存在するが，調査を通じて，「選択型グループ」を「納得型グループ」と「諦めグループ」に分解できた．「納得型グループ」は，データ提供や利活用などのプライバシーの制限に対して，サービスなどのインセンティブを納得して受け入れるプライバシー観であり，反対に，プライバシーの制限に対して否定的な感情を抱いていながらも，サービスの利便性などの自己をとりまく環境に否定的な感情を押し殺しつつプライバシーの制限を甘んじて受け入れるプライバシー観が「諦めグループ」である．「諦めグループ」のプライバシー観を持つ者は，サービスを利用する当事者であるため，プライバシーの制限が持つリスクを深く理解する．その後のウェブを通した量的調査で，8 割以上がモバイル端末を通じてサービスを利用する際にプライバシーに関連して「諦めグループ」を経験していると回答し，住所や氏名などの，従来からパーソナルデータと認識されていたものに加え，「位置情報」がセンシティブなパーソナルデータだと認識していると判明した．

そもそもプライバシー権は人間を人間たらしめる根本的な権利である．一度失われた権利は，その回復に多くの時間を要し，法令や慣習は世代を超えて効果を発揮し続ける．未来の世代に対して，プライバシー権をバトンタッチすることは我々の義務であり責任である．プライバシー権の保護は，今を生きる者たちだけでなく，将来の世代に向けてもなされなくてはならない．そして未来に向けて行う配慮の指針は，全体を俯瞰しつつもリスクを危惧とともに理解している存在である「諦めグループ」から得られる．世代間倫理から「諦めグループ」が持つプライバシー観を検討することで，データ収集・利活用を円滑に進める指針が見えてくる．

キーワード：プライバシー，情報倫理，センシング，世代間倫理

目次

図・表目次

Ⅰ　序論

“Would you tell me, please, which way I ought to go from here?”
“That depends a good deal on where you want to get to,” said the Cat.
“I don’t much care where——” said Alice.
“Then it doesn’t matter which way you go,” said the Cat.
“——so long as I get somewhere,” Alice added as an explanation.
“Oh, you’re sure to do that,” said the Cat, “if you only walk long enough.”
——Alice's Adventures in Wonderland

1.1 はじめに

H.M.McLuhan によって 1960 年代に提唱された「人間の身体を拡張するメディア」の概念は[1]，携帯電話・スマートフォンをはじめとするモバイル端末の普及により，私たちの生活にとって極めて身近なものとなった．モバイル端末は単なる通話や文字伝達のツールの域を超え，ハード面では音声やカメラ，温度計，気圧計など，数多くのセンサーが搭載され，形状も携帯電話に類するものだけでなく，大型のタブレット，腕時計型，眼鏡型などのウェラブルデバイスの開発が日々開発されている．またソフト面ではビジネス領域の広がりを背景に，ゲーム，ニュース，地図，フィットネスなど，さまざまなアプリケーションが日夜開発され，「身体の拡張[1]」を利便性と共に我々に実感させている．

その一方で，モバイル端末の利便性を向上させ，その機能の多くを利用するために，我々は多くのデータを提供するのが常である．端末を契約するときに行う申込用紙への記入を通じて，および免許証などによる本人確認用書類の提供をはじめ，位置情報サービス利用時における GPS データ，またサービスの利用履歴など，サービス提供企業に対して様々なデータを我々は引き渡している．

各ユーザーが生み出す情報量が莫大になると同時に，データの解析技術が向上することで，集約されたデータの利活用が注目され，バズワードとしての「ビッグデータ利活用」が叫ばれて久しい．たとえば，モバイル端末が創出する位置情報だけを例に取っても，モバイル端末によって取得できる位置情報は GPS データ，基地局データ，Wi-Fi データなどが挙げられる．端末ユーザーは，端末の利用および，地図やゲームなどのアプリケーションを通じて位置情報の利用を行い，サービス提供主体へ送信する一方，膨大な数のユーザーの位置情報を取得する電気通信事業者やアプリケーションの運営企業は，サービスクオリティの向上はもとより，人口統計，災害時の非難情報提供，商圏の分析や広告など，様々な分野でのデータの利活用を推し進めている．

しかしデータの利活用に際しては，自然環境負荷の減少や新たなサービスの発生，効率的な社会の実現などが期待できるものの，データそのものは個人が生み出したものであるため，プライバシーにかかる問題が噴出する事例が見受けられる．また，データ利活用の主体が思い描くユートピアとは裏腹に，マスメディアによる問題提起がなされる例や，端末ユーザーやサービス利用者間の議論によってデータの利活用に障壁が生じた事例がある．

利活用を円滑に進めるには，端末ユーザーのプライバシー権と，データの活用主体が持ちうるデータ利用権のバランスが肝要だといえよう．しかしプライバシー権とデータの利活用を巡る対立フィールドは，近年の技術革新やデバイスの普及によって新たに生じたものであり，問題解決にあたっての明確な指針は未だ存在せず，活発な議論の渦中にある．

これらを踏まえ本研究では，データ利活用やプライバシーに対する意識を調査し，データの利活用を巡るプライバシー意識を理解する一方，発生しうる問題の源泉と問題予防策を模索し，プライバシーに関する不安感を端末利用者に与えにくいサービス作りやデータ

の利活用方法を検討する．

なお，本論においては，モバイル端末によって得られる位置，気温などのセンサー情報，およびアプリケーションやブラウザを通じて送信されるデータなど，個人のモバイル端末から生み出されたあらゆる情報を「パーソナルデータ」と定義する．「モバイル端末」については，携帯電話，スマートフォン，タブレット端末，ノートパソコン，スマートグラス，腕時計型デバイスなど，携帯が可能でデータの送受信が可能な端末を総称する単語として用いる．

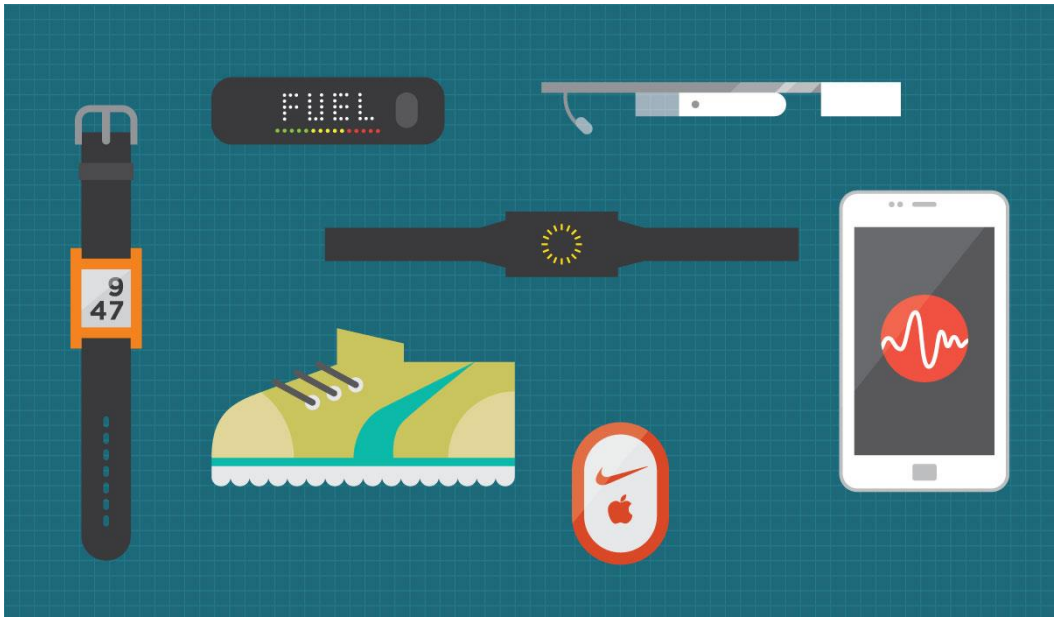

図 1 モバイル端末の例[2]

1.2 本論文の構成

本論文の構成と各章の概要を以下に示す.

まず第 2 章では，昨今におけるデータ利活用の実例やそれに伴うプライバシー問題の事例紹介，プライバシー権そのものの起源とデータ利活用時代における議論，PPDM と呼ばれる摂動化や暗号化などのプライバシー保護技術を紹介し，モバイル端末が創出するプライバシー問題の現状を検討する.

続く第 3 章ではユーザーのプライバシー観を理解するために行われたユーザースタディを紹介したうえで，既存の調査手法ではプライバシー問題の背景に存在する感情を汲み取れないことを指摘し，質的調査と量的調査を組み合わせて実施することで，プライバシーの背景に存在する感情を理解できると仮説付け，調査を提案する.

その後の第 4 章では，ユーザーのプライバシー観を理解するための調査方法を検討したうえで，半構造化インタビューによる社会学的調査手法の採用を行い，質的調査の結果を KJ 法により分析し，モバイル端末ユーザーが考えるプライバシー観の分類化を試みる．先行研究を踏まえ，プライバシーを絶対的なものと捉える「原則型グループ」，プライバシーの価値を認めない「開放型グループ」，サービスの価値を認めてプライバシーの制限を受け入れる層を「選択型グループ」に分類したうえで，さらに「選択型グループ」を「そのサービスやアプリケーションの利便性が著しく高い場合，プライバシーの制限に否定的な感情を持ちながらもプライバシーの制限を受け入れる」,「諦めグループ」と,「サービスの価値，データ収集・利活用，プライバシーの制限を心の底から納得してサービスを利用する」,「納得型グループ」に分類する.

その後，質的調査の結果を踏まえ，ウェブを通して行ったアンケート調査の実施と分析結果を検討する．モバイル端末を利用する際に感じるプライバシーに対する不安感と，その理由を調査し,「諦めグループ」の背景理解と，データ収集・利活用に伴うプライバシー問題を防ぐ方法の検討材料を収集する.

5 章では，利便性の向上を目的に行われるデータ収集・利活用に関連するプライバシー権の重要性を説いたうえで，慣習や法令によってプライバシーの制限が将来に継承されることから，データをめぐる倫理的検討を世代間倫理から行えることを示す．その後,「諦めグループ」が,「データ収集・利活用を通じて起こるプライバシーに関する否定的な感覚を抱いていながらも，サービスを利用する当事者」であることから「プライバシーが制限されることで起こる，リアルなリスク」を認識していることに触れ,「諦めグループ」が持つ危機感を汲み取ることで，データ収集・利活用のリスクを深く認知し，データ収集・利活用に伴うプライバシー問題の防止に役立てる.

最後に，第 6 章にて全体をまとめ，本論における課題と展望を論じて結尾とする.

II　研究背景

2.1 概要

スマートフォンを始めとするモバイル端末が生み出すデータは，ユーザーが利用するサービスそのものの質を向上させる以外に，複数のユーザーのデータをマイニングすることで，商圏の分析，災害時への対策，交通量調査，人口調査，都市計画など様々な場面，目的においても利活用が期待されている．

そうした背景を念頭におき，本章ではまず近年におけるデータ利活用の現状と事例を示す．その後，体系的なプライバシーに関する議論，プライバシー保護技術，プライバシーに関する社会調査に関して紹介する．

コンピュータやスマートフォンに搭載される処理能力は向上の一途をたどり，2025 年には人間の脳を超える計算能力を持つとされ [3]，インターネットは地球上の全生物がもつ記憶容量を超えるとされている [4]．新たに生み出されるデータは加速的に増加し続け，インターネット上に存在するデータの 90%以上が 2010 年以降に生み出された [3]．

しかし，モバイル端末を通じて生み出され，利活用されるデータの多くはユーザーの行動やサービス利用によって生み出されるため，個人の生活習慣と密接に関わり，プライバシーに関連する情報として捉えられる場合がある．したがって，データの円滑な利活用に際しては，個人情報にかかる法的な制約を順守するのはもちろんのこと，技術面，ユーザースタディの面からもプライバシーに配慮が必要である．

実際のデータ利活用の場面では，ユーザーへプライバシーに関する不安感を抱かせたことで感情的な否定意見がユーザーやメディアによって噴出し，データ利活用がとん挫した例がある．そもそも，データの利活用は，多くのユーザーにとって馴染の無いマイニング技術によって行われるだけでなく，データそのものに関しても，地図アプリケーションの利用に伴う GPS データや，モバイル端末の利用時の基地局データなどのサービスの背景で生み出されるデータは，技術に関する知識が乏しい場合，自分が生み出したことすら気づかない．そのうえ，仮にマイニングやデータの取扱いに関してデータ収集・利活用を行う団体がユーザーに説明したとしても，ユーザー自身が実際に自らのデータがどのように扱われているか確認する術は無い．そのため，データ収集・利活用においては「信頼」という感情を勝ち取らなければ，データ収集・利活用を円滑に進められない可能性がある．また一方で，データ保護技術は日進月歩の発展を遂げているものの，いまだ絶対的なデータ保護技術は確立されていない．しかし生み出されるデータ量が増加し，高速回線の普及や記憶媒体の多様化・大容量化などのデータをめぐる情報における環境の変化からデータの移転や複製は極めて容易くなり，プライバシー権が制限されるリスクは高い水準にある．それに呼応するように，プライバシー権も「放っておかれる権利」とする古典的なものから，データ収集・利活用の時代に応じた解釈がなされるようになったものの，ユーザーの

感情を考慮したプライバシー権の検討と議論は十分にされていない．事例，技術，プライバシー議論を詳細に追えば，データ利活用時代におけるプライバシーを理解するうえでの重要な論点は「感情」であると結論付けられる．

2.2 データ利活用の近況

そもそも，私たちが手にするスマートフォンを始めとするモバイル端末は，位置情報などの，個人の行動をデータとしてセンシングできる．また，たとえば地図サービスの利用に伴って GPS データを送信することによって現在地点が分かり，経路検索のスピードが向上するなど，アプリケーションを始めとするサービス利用に伴ってデータがサーバに送信されることで利便性が向上する．しかし，モバイル端末によってセンシングされるデータは，移動や通話，検索など，個人の行動によって生み出されるパーソナルデータである．したがって，データの利活用は「個人の行動によって生み出されたデータを利活用すること」であり，プライバシーの問題と深くリンクし，プライバシー問題を引き起こす．

モバイル端末の機能向上に伴い，GPS などの位置情報や音声，気圧などの様々なセンサーがスマートフォンをはじめとするモバイル端末に備わる．多くの人がそれらを利用するに伴い，生み出されるデータは莫大なものとなった [3]．それに呼応するかのように，データマイニング技術に関する研究は日進月歩の向上の道を辿り，データの利活用は我々の生活の利便性を高め，データ利活用は様々な光輝く可能性を提供しているかのように錯覚させる．データ利活用の場面においてプライバシーのトラブルが発生した実際の事例を紐解くことで，「利便性の向上」によってプライバシーが犠牲となることで発生する世間的影響の大きさが分かるとともに，データ利活用に伴って発生するプライバシー問題のポイントが浮き彫りとなる．

2.2.1 「ビッグデータ」というバズワード

ビッグデータとは，総務省の情報通信白書（2012）によれば「事業に役立つ知見を導出するためのデータ」とし，データの規模によってのみ定義されるものではなく，データの質，およびデータの利用目的を踏まえて定義されるとする [5,6]．

また，ビッグデータという言葉が当てはめられるデータ群は，「典型的なデータベースソフトウェアが把握し，蓄積し，運用し，分析できる能力を超えたサイズのデータ」とされ，ビッグデータとして用いられるデータの大きさを流動的に定義できる [7]．

このように，ビッグデータという言葉には主観性が伴い，データの利活用が取りざたされるようになってからは，「多くのデータをまとめて何かに役立てる」際のバズワードとしてマスメディアなどを中心に用いられる事例が見受けられる．

表 1　「ビッグデータ」という言葉を用いた新聞記事の見出しの例

「『ビッグデータ」』来占う，富士通，商用車向け渋滞情報.」（日経産業新聞, 2011.06.15）
「ビッグデータで株価など予測，日本ＩＢＭ，大量の経済記事・統計を一括分析.」（日本経済新聞, 2012.06.15）
「ビッグデータ：熱視線　蓄積・分析事業を各社強化　世界の市場，６年で５倍に・・」（毎日新聞, 2013.06.08）

図 2 ビッグデータを構成する各種データ [5]

ビッグデータというワードが浸透するに従い，データ利活用が様々な分野で急速に叫ばれるようになった．それに呼応するように，総務省は「ビッグデータは，日本再生への GPT（General　Purpose　Technology）としての ICT の潜在力を飛躍的に高める可能性を秘めている」と位置づけ [8]，東日本大震災以降の日本再生に対する糸口として国家が主体となりビッグデータに関連した施策を官民問わずバックアップする姿勢を見せている．

しかし，ここから見ていくように，個人の生活やモバイル端末の利用から生み出される

データの利活用には，プライバシーの壁が大きく立ちはだかり，実際のデータ利活用の現場ではプライバシーを巡る複雑な問題生み出す事例が見受けられる．

2.2.2 Suica 利用履歴データ販売

JR 東日本が交通系 IC カード「Suica」の利用データを外部企業へ販売した際，マスコミや SNS においてプライバシーに関する問題提起が活発になされ，利活用が停止に追いやられた．本 Suica の事例で提供されたデータは，法律内で認められるように匿名化されたものであったが，オプトアウト（離脱可能性 [9]）窓口の周知不足によって Suica 利用者に不信感を抱かせたことにより“炎上”したと分析する意見が存在する．Suica の事例により，データ利活用に伴うプライバシー問題を防ぐためには，法律を遵守するだけでなく，自己のデータの利活用を拒否できるようにアピールするなど，データ提供者が「安心感」を持てるような企業努力が必要だと示唆された．

2013 年 6 月，JR 東日本は交通系 IC カード「Suica」の利用データを日立製作所へ販売した. JR 東日本が販売したデータは, 無記名の Suica および, 記名式 Suica, モバイル Suica のデータで，私鉄を含む首都圏約 1800 駅の乗降履歴（記名式 Suica とモバイル Suica のデータに関しては，年齢と性別が含まれる）である [10]．また，各 Suica には固有の ID が割り振られているが，新たに ID を割り振りなおした状態のデータを販売した．本処理方法は，もっとも基礎的なデータベースの匿名化手法である [11]．

その後，本件がプレスリリースなどを通じて公表されると，Twitter や２ちゃんねるなどの SNS やネット掲示板で，データ利活用の重要性をプライバシー問題に関する議論が見受けられたほか，マスメディアにおいても多数記事化された [10,12]．

本件にかかるマスメディアにおける記事は，プライバシーに配慮したデータ利活用の難しさにフォーカスしたものだけでなく，個人情報保護法に則った手法でデータ利活用・売買が行われた場合にも問題が起こり得ることを示唆したものも見受けられたほか，オプトアウトを望むユーザーの窓口に関する周知不足を問題視する内容の記事も存在する [12]．
）．

表 2　JR 東日本 Suica 問題を取り上げたメディア記事の例

「Suica 利用履歴販売，JR 東は「個人情報に当たらない」との見解」（ITmedia ビジネス online, 2013.07.19）
「『Suica 履歴販売」は何を誤ったのか」（ITpro by 日経コンピュータ, 2013.10.16）
「時流・底流：Ｓｕｉｃａ履歴無断販売　個人情報，不十分な匿名化・・」（毎日新聞, 2013.09.02）

本データの販売に際して，JR 東日本は 2013 年の 3 月時点で「Suica に関するデータの社外への提供について」と題した中間報告のとりまとめを事前に行った[13]．その中で販売に際しては「駅リポートの作成を目的に『匿名化した Suica 分析用データ』を作成したが，—中略—相当数の利用者のデータが使用できなくなり，分析結果の精度が低下したり，分析の種類が制限されうる課題があることがわかった．このような課題を解決するには，データ特性を勘案し，利用者が安心・納得できる土壌づくりを踏まえた，技術の進展あるいは法整備等が望まれる．また，『匿名化した Suica 分析用データ』を外部に提供する形態ではなく，JR 東日本で統計処理を施して駅リポートを作成し，外部に提供することも，課題解決の方法の一つと考えられる．」と，課題とその解決方法を提案している[13]．

「利用者の安心・納得」という言葉が JR 東日本が Suica に関するデータの販売に際して行ったとりまとめにも明記されていることからも分かるように[13], JR 東日本は事前に Suica のデータ利活用に際してプライバシー問題が発生すると予期していたと思われるものの，結果としては「第 1 の要因は，Suica 履歴の販売について，JR 東日本が利用者にほとんど事前説明をしていなかった点である[12]」「販売したデータの具体的な中身についての説明も不十分だった．[12]」のように，事前説明や販売するデータの中身関する説明が不十分だったことから大きな問題を招いた．本件は現代の「ビッグデータ利活用」におけるユーザー理解の難しさと，個人情報保護法の枠組みを超えたプライバシーへの深い配慮を避けて通れないことを示唆した好例といえる．

2.2.3 NTT ドコモのモバイル空間統計

データ利活用に伴うプライバシー問題を検討するうえで，Suica の事例と対照的なのは，NTT ドコモによる「モバイル空間統計」である．モバイル空間統計では，携帯電話の基地局データをもとに得た，端末利用者の位置情報が他社に提供された．しかし，オプトアウト窓口の周知の徹底や，データを匿名化させる技術の詳細な解説によって，Suica の事例で見られたような目立った“炎上”は起こらず，2015 年 6 月現在もモバイル空間統計によるデータ提供サービスは継続中である．本事例により，データ提供者にプライバシーに対する嫌悪感を抱かせないように企業側がアピールすることが，データ利活用においてプライバシー問題を防ぐために効果的であると実証された．

NTT ドコモは 2013 年 10 月，基地局データをもとに取得した，地域ごとの人口分布や性別，年齢階層に関するデータを「モバイル空間統計」として同社子会社を通じて団体，企業への販売を開始した[14]．モバイル空間統計では，地図を一辺 500m から 1km のメッシュに区切り，そのメッシュ内の基地局に接続しているモバイル端末の契約情報に結びつく人の数と性別，年齢階層，居住エリアに関するデータを提供する[14]．

これにより，国勢調査などで得られなかった，たとえば「新宿に来ている 30 歳代，埼玉在住の男性の数」のような移動人口に関するデータを得られる[15]．

また，提供されるデータは，図 3 のように，1.識別子を取り除く「非識別化処理」，2.統計情報の生成である「統計処理」，3.人数が極端に少ないメッシュのデータを取り除く「秘匿処理」の三段階を経た後に提供され，NTT ドコモは「モバイル空間統計は，集団の人数のみをあらわす人口統計情報であるため，お客様個人を特定することはできません.」としている [14].

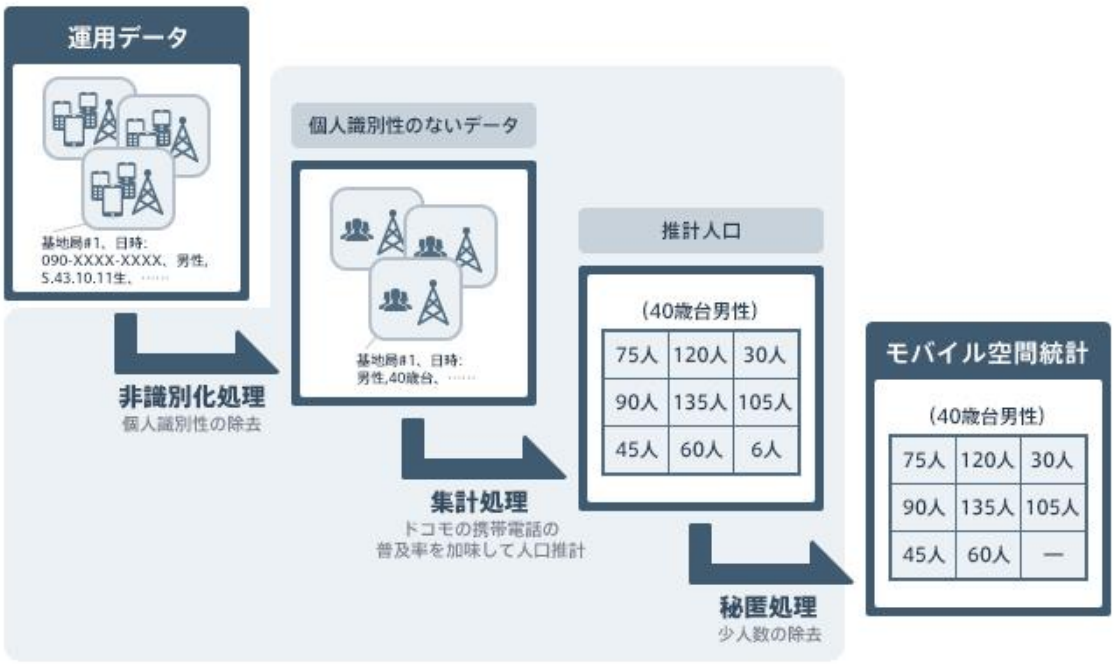

図 3 「モバイル空間統計」における匿名化処理 [14]

Suica におけるデータ販売時と異なり，SNS などではモバイル空間統計を「プライバシーの侵害」や「データの無断換金」として非難する声が見られたが，マスメディアではモバイル空間統計に関するサービス開始に関して触れるのみの記事が数多く見受けられた.

表 3 モバイル空間統計を取り上げたメディア記事の例

「第 629 回：モバイル空間統計とは」（ケータイ Watch, 2013.09.10）
「個人データ活用，企業が自主指針，ドコモ，電話番号など削除，ネット広告，情報の取得を通知.」（日本経済新聞, 2014.09.22）

マスメディアの記事内では，「自分のデータが使われることを望まない契約者は，分析対象からの除外を申請できる仕組みも整備した．[14]」「ユーザーが希望すれば，自分の携帯電話の情報を「モバイル空間統計」の対象から外すことも可能です．[14]」のように，オプトア

ウトに関する説明が伴う記事が見受けられた点も Suica のデータ販売時と明確に異なる傾向である．

このように，Suica のデータ販売とモバイル空間統計の明暗を分けたのは，「個人を特定しにくくする仕組みの“周知”」と「オプトアウトの“周知”」が大きな要因といえる．法制度のもとで利活用を行うのはもちろんのこと，いかにユーザーの「感情」を煽らないか，あるいは「安心感」を与えられるか，という点がデータ利活用を円滑に進めるための要素として極めて重要であることを浮き彫りにした対照的事例が，Suica のデータ利活用に対するモバイル空間統計だといえる．

2.2.4 国外におけるデータ利活用事例とプライバシーの侵害

さて，データの利活用に際しては，我が国に先立ち，主に米国において利活用の道が活発に模索されてきた．しかし我々の生活を豊かにするはずのデータ利活用が，より具体性をもったプライバシーの侵害を引き起こす，あるいは，「プライバシー侵害」という抽象的なデータ利活用の負の側面の可能性を実感を伴って我々に突きつけた事例が米国には存在する．日本においての利活用に伴う問題が，利用者に対する「安心感」という感情が肝であったことに対し，日本国外においては，匿名化技術の不完全さによって個人が特定できるなど，プライバシーが実害を伴って問題化した事例が目立つ．

2006 年，米国のインターネットプロバイダーである AOL 社は 2006 年 3 月から 5 月における検索クエリを約 2,000 万件以上，67 万人弱分公開した [16]．検索クエリの公開は，データ利活用に関する学術研究目的に行われたものの，公開された検索クエリデータの解析により個人が特定できるのでは，という外部からの指摘を受け，同社 CTO の Maureen Govern が引責辞任する事態にまで発展した [16]．

公開された検索クエリデータは，各コンピュータにおけるスクリーンネームを排除し，新たに ID を振りなおしたデータだったが，検索内容には，地域に関するものや，社会保障番号を検索したデータなど，一見しただけで個人の特定をイメージできるものも存在した．これに対し，NPO の World Privacy Forum は，連邦取引委員会（FTC）に抗議を行い，Electronic Frontier Foundation（EFF）は調査を求めた [17]．

本件は，現在におけるデータ利活用とプライバシー侵害の対立フィールドを明確化したのみならず，「個人の特定」が現実において何らかの危害へと繋がる可能性を示唆した．

2006 年における AOL 社の事例を踏まえ，データ利活用に関する研究などの目的でデータを提供する団体は，それまで以上にプライバシーへの配慮がより求められる事態となる．

2009 年，レンタル DVD 事業とウェブ上における動画配信を行う Netflix 社は，自社が抱える作品に関するレビュー内容や投稿日時，作品データを個人に基づく ID やユーザーネームを省いた状態で公開し，データ利活用に関するアルゴリズムのコンテストを開催した [16]．

しかし，A.Narayanan らテキサス大学の研究グループは，映画やテレビドラマ，俳優に

関するデータベースをユーザー参加型で構築する IMDb（Internet Movie Database）社の公開情報と，Netflix 社のコンテスト用データと突きあわせることで，4 名の個人を特定できたと発表し[18]，翌年 2010 年には個人が特定された 4 人が Netflix を相手取り訴訟を起こした．その後，Netflix 社は和解に応じた[19].

本件は，プライバシーの侵害が，単体のデータベースによってのみ起こるのではなく，複数のデータベースを突きあわせることによって起こることを示唆すると同時に，「匿名化」という言葉にすれば単純な工程がいかに困難かつ，「匿名化処理されたデータベース」が「個人が特定できるデータベース」へと変容するリスクを顕在化させた．また，データ利活用を巡り，「個人が特定される」ことが，いかに組織や個人の名誉を傷付け，金銭的損害を発生させるかを実例をもって証明したといえる．匿名化処理されたデータベースから個人を特定するために突きあわせるデータベースは，現時点において入手できる物だけでなく，将来のどこかの時点で生み出されるものの可能性も考慮しなくてはならない.

あるデータベースをもとに，個人を特定するプライバシーの侵害の可能性を示唆した事例は，カーネギーメロン大学の学生らが保険の公開情報をもとにマサチューセッツ州知事の既往歴を特定した例や[20]，Montjoye らはクレジットカードの利用履歴が最低 4 件の利用履歴データがあれば約 9 割の個人を特定できることを発表した事例[21]など，枚挙にいとまがない.

こうしたデータ利活用とプライバシー侵害の事例の頻発は，データ利活用がプライバシーの侵害を引き起こす可能性を実社会に対して問題として提起し，プライバシー保護技術に関する研究の活性化を促した．同様に，プライバシーそのものに関する議論や，プライバシー侵害が起こった際の問題を実務的に解決する仕組みに関する議論も，データ利活用を円滑に進めるうえで避けて通れない.

図 4 IMDb 社のデータベースを利用した，
Netflix 社のデータ利活用コンテスト用データの非匿名化[16]

2.3 プライバシーの体系と環境

本項では，プライバシーの起源および，現在のコンピュータ登場以降の議論を体系的に検討し，データ利活用に伴うプライバシー問題の理解とその解決方法についての研究を紹介する．

古典的プライバシー概念の発生には，19 世紀後半の活版印刷と写真技術の発展に伴って花開いたマスメディアにより，個人の肖像や行動などの今日でいうところのパーソナルデータが公開される事態となったことに対して人々が感じ得た，負の感情が根底に挙げられる [22]．

その後，コンピュータの登場や，データ利活用，遺伝子情報など，様々な時流の変化によってプライバシーは都度検討されてきた．しかし新たな技術が登場することで問題が発生し，その技術を踏まえたプライバシーの議論がなされるといった，対症療法的な側面が否めない．

それを踏まえて，本項目ではデータ利活用で特に考慮すべきプライバシーを「古典的プライバシー」「自由権と公共権」「自己決定権」「感情」の 4 点の切り口を念頭において議論する．

なお，本論における「環境」とは自然環境のみを表すのではなく，個々の状況や人々をとりまく状況を示す．したがってプライバシーにおける「環境」とは，プライバシーの議論が「どのような状況下でなされ，どのような変遷を辿り，どのような影響を与えたか」を示す．

2.3.1「古典的プライバシー権」とその変遷

古典的プライバシーの概念の発生は 19 世紀後半に遡る．写真技術や新聞をはじめとする紙メディアの発展を背景に，S. D. Warren，L. Brandeis らによって「プライバシーの権利」が定義された [22]．S. D. Warren らが 1880 年に発表した著作“The Right to Privacy”内で定義されたプライバシー権は，「放っておいてもらう権利」とされ，その成立根拠はプライバシー権を「人間の精神における明確に冒されるべきでない権利」と捉えることによる [22]．
また，古典的プライバシーの概念において，「公共の福祉に関する場合」はプライバシーの制限が例外的に認められると規定された [22]．こうした「データ利活用と公共」を巡る考え方は，データ利活用によって達成される「利便性の向上」と個人の自由権に基づく「プライバシー権」の対立においても，2.3.3 で挙げるように未だ大きな影響力を持つ．

S. D. Warren らによるプライバシー権の提唱後，1905 年には米国ジョージア州において写真のプライバシー権が認められ [23]，1939 年にはアメリカ法律協会によってプライバシー権の注釈が追加されたるなど [23], プライバシー権は法のもとにおいても保護される権利となる．

2.3.2「放っておいてもらう権利」から「自己決定権」へ

S. D. Warren らによって定義されたプライバシー権は，肖像権のみならず，婚姻や自死など，様々な環境においても拡張された．

例えば，1965 年，婚姻関係にある男女の避妊を禁ずる米国コネチカット州法が「プライバシー権の侵害」として違憲判断された [24]．また 1992 年には「死ぬ権利」の違法性がプライバシー権から議論された [25]．

これらの事例におけるプライバシー権の取り扱いは，古典的プライバシーの原則である「放っておいてもらう権利」ではなく，自らの問題を自らで決定する「自己決定権」の視点からプライバシーを捉えなおすものである．本論で論じる「データ利活用におけるプライバシー権の行使」が，データ利活用を許諾するか否かの決定権をデータ所有者に委ねる「オプトイン・アウト」によってなされる事例が一般化していることからも [3]，プライバシー権が自己決定権の性質を持つことは，データ利活用におけるプライバシー問題を紐解くうえで見逃せない．

2.3.3 コンピュータ時代におけるプライバシー権の議論と「自己決定権」，「公共性」

高度な処理能力を有するコンピュータと，データの保管が容易なシステムの登場を踏まえ，1967 年，今日における情報分野のプライバシー問題の開拓者のひとりである A.Westin は著作“Privacy and Freedom.[26]”において，コンピュータにおけるプライバシー権を「自己に関する情報に対するコントロール権」としたうえで，「個人や組織が，自己に関する情報提供することを自ら決定できる権利」と定義した [26]．これらの定義の背景には，当時の日進月歩のコンピュータテクノロジーの発展を踏まえ，パーソナルデータがコンピュータに集約され，プライバシーが冒される可能性が 1967 年当時からも強く予期できる環境が存在したと考えられる．

図らずも，A.Westin の予言通り，コンピュータの処理能力はムーアの法則 [27] に従い指数関数的に向上し，またデータを保管する記録媒体のボリュームや，データを転送する通信技術の開発と向上を背景に，パーソナルデータの集約および利活用とプライバシーの問題は実例を伴って具現化した．しかし 2015 年から 1967 年を振り返り，半世紀弱が経過しているにも関わらず，当時の危惧が現実となり，その諸問題の解決方法に奔走する現在を鑑みるに，将来を見据えた予防原則の視点が欠損していた，あるいは技術の利便性によってプライバシーに関する議論が後手に回っていたと言わざるを得ない．

A.Westn によるコンピュータにおけるプライバシー権の定義，およびコンピュータテク

ノロジーの発展に伴い，1972 年には A.Miller が個人を特定できるデータの売買とコンピュータの関係からプライバシーの議論を行い [28]，1983 年には D.Bumham が国家安全保障局などの政府による個人を特定できるデータの収集，および民間企業のデータに対する取り組みを背景に議論された [29].

また，1995 年には，P.Regan が遺伝子検査やポリグラフデータなど，新技術に伴って生み出されるパーソナルデータに関するプライバシー権を公共性の観点から議論した [30].

本論で深く検討するモバイル端末が創出する大規模なデータの利活用は，災害対策や人口統計，効率的な社会な実現など，公益性の視点から行われる事例も多い．また，利活用されるデータはスマートフォンなどの近年新たに登場したデバイスであるモバイル端末によって生み出されるデータであり，それら新技術によって生み出されたパーソナルデータの取り扱いを住所や氏名といった従来想定されていたパーソナルデータと同列に扱うべきかの議論もなされるべきである．加えて P.Regan が新技術によって生み出されるデータが自由権と対立するものとしたように [30], モバイル端末が創出するパーソナルデータの利活用においても，公共性と自由権の対立問題を避けて通れない.

2.3.4 データの利活用の視点から検討したプライバシー権の議論と「感情」

集約されたパーソナルデータの利活用が現実味を帯びるに従い，プライバシーは消費者やサービスユーザーの身近な問題となった．それに伴い，「パーソナルデータの蓄積・移動」ではなく，環境を考慮した「パーソナルデータの使われかた」にフォーカスした論考が登場し，より喫緊に到来したデータ利活用時代における具体的なプライバシー問題が取りあげられる．しかし，それらの議論では，ユーザが抱える「感情」の議論が見落とされがちである.

J. H. Moor によれば，コンピュータ技術によって我々は様々な情報を容易に得られるようになる一方で，その引き換えにパーソナルデータの流出を避けられない状況に我々は置かれている [31] とした．そのうえで，自らのパーソナルデータへのアクセスを制限してプライバシー権を確保する「制限アクセス理論」を提案した [31]．ネットワークによってパーソナルデータが容易に伝播する時代において，どこに自分のパーソナルデータがあるのかを完全に把握する「コントロール理論」は非現実的であり，その環境に応じてパーソナルデータの公開範囲を自分自身で決定することは，自己決定権の観点と現在におけるコンピュータを取り巻く環境を踏まえ，プライバシー権確保のひとつの解といえる．データ利活用の場面を考慮して，環境ごとにプライバシーデザインを検討する手法は，E.Goodman や H.Nissenbaum（H.Nissenbaum はここで言う「環境」を「Context」と表現している）らによっても検討されている [4,32].

一方，D. J. Solove はプライバシー権を「情報収集」「情報処理」「情報拡散」「侵襲」の 4 分類化し，それぞれに応じた問題解決方法の検討および，データ利活用におけるプライバシー問題の解決に対して，プライバシーの多元的解釈や文化的依存の側面の存在を指摘したうえでプラグマティックなものとして論じた [33].

プラグマティックな側面からデータ利活用とプライバシーを検討する事例では，後述する PPDM の研究シーンなどにおいて，現実に起こり得る身体的，あるいは金銭的な犯罪やトラブルに巻き込まれる可能性が考慮される [34,35]. たとえば，位置情報や行動履歴を取得されることによるストーカー被害や，強盗などのリスクなどは，プライバシーの侵害から連想しやすいリスクといえる．ネットバンクやクレジットカードの利用が，ウェブやモバイル端末によって行われ，それが一般的になるに従い，パーソナルデータに関連したプライバシーが「権利」を超えて個人の財産や生命リスクに影響を及ぼす存在となった．プライバシー権はセキュリティリスクの視点から論じられるようになり，その背景には，プライバシーの侵害に伴う実害の顕在化が挙げられる

また，先に挙げた JR 東日本における事例などをめぐっては，パーソナルデータを通したプライバシーの侵害によっておこりうる明確なセキュリティリスクに対する怖れだけでなく，その背景に存在する「なんだか気持ちが悪い」のような，何らかの力が自らの領域に侵入することに対する生理的嫌悪感もまた「安心感」を崩壊させる要因である．そうしたプライバシーの感情的な側面の存在は自明のものとしてプライバシー分野の研究において認知されているものの，多くの研究においては，技術などの何らかの施策によって「感情的な問題も結果的に解決される」というアプローチである．しかし，実際に起こっているモバイル端末を通して行われるデータ収集や利活用における事例では，特に SNS などにおいて（乱暴な表現をすれば）「理屈を無視した，極めて感情的な反応や意見」が顕在された．したがって，プラグマティックな視点から，データ収集や利活用に関連したプライバシー問題を検討するためには，そうした「理屈抜きで現れる感情」そのものを理解するべきである．

2.4 PPDM（Privacy Preserving Data Mining）

ここでは，技術の側面からプライバシー保護を検討し，データ利活用にともなって発生するプライバシー問題の解決手法を紹介する．PPDM と呼ばれる，プライバシー保護をともなったデータマイニングは，k-匿名化（k-anonymity）[36]，l-多様化（l-diversity），t-近接化（t-closeness）[35] などの「データに直接手を加えてプライバシーを保護する技術」である摂動化と，データの所有者のみが鍵を所有し，データを暗号化処理したままでマイニングが行われる，暗号化に分けられる [37].

各プライバシー保護技術は，それぞれ理想的な環境下においてはプライバシー保護が実現されるが，特定の環境下では個人が特定されるリスクが発生する技術も存在する．その

うえ，プライバシー保護技術には高度な暗号技術が用いられる場合や，数学的根拠をもとにアルゴリズムが生成されているため，それぞれの保護技術はその分野に精通した者でなくては根本的理解が困難である．したがって，消費者やサービスのユーザーにとっては，「プライバシー保護技術によってプライバシーが守られている」という状況を信頼した状況が発生しなくてはプライバシーに対する安心感を得られない可能性がある．技術の向上だけではユーザーの安心感は得られない可能性があり，プライバシープライバシー保護技術と独立した「感情」のフィールドの理解がプライバシー問題の解決に求められるのである．

2.4.1 k-匿名化（k-anonymity）

k-匿名化（k-anonymity）は，データの利活用主体と，パーソナルデータを保有するグループを分け，k 人以上の集合を設定する暗号化手法である [36]．k-匿名化の活用事例として NTT ドコモによるモバイル空間統計におけるデータ処理が挙げられる．モバイル空間統計では，あるメッシュ内における同一データを持つユーザーが k 人に満たない場合，そのデータを 0 人として処理を行った．これにより，データを利用する者は，1/k 以下の確率でしか個人を特定できない．

k-匿名化処理は，直感的にプライバシーレベルを捉えられるため，位置情報の秘匿化 [38] や無線センサーネットワークを通して生成されたパーソナルデータ [39] など，様々なデータ利活用に関連した匿名化処理として用いられている [40]．

k-匿名性における問題点は，k の値を増加させた場合，データの粒度が著しく上昇し，データの利活用を目的としたデータベースの利活用が困難となる点や，データの利活用主体と，パーソナルデータを保有するグループの完全な分離が現実的には困難あることが挙げられる．

また，k-匿名化処理を施したデータベース単体の場合，個人の特定は NP 困難問題となるが [41]，そのほかの類似データベースと突きあわせることで，個人を特定できる可能性が不確定に上昇するため，1/k 以上の確率で個人が特定できないとする前提が崩れる．しかしモバイル空間統計を始めとする，k-匿名化処理がなされたデータベースの運用に関しては，そのほかのデータベースと突きあわせることで k 値の原則が崩壊することに言及されていない [41]．

図 5 k-匿名化 [42]

2.4.2 l-多様化（l-diversity）

あるデータベースにおける，特定の属性の多様性に関する指標が l-多様性であり，k-匿名化処理されたデータベースにおけるセンシティブ情報に関する属性を多様化させることで匿名性を向上させることを l-多様化（l-diversity）処理と言う [35].

k-匿名化処理をセンシティブ情報に関する属性が偏ったデータベースに対して用いた場合，属性が偏っている場合は個人の属性を特定できる可能性がある．たとえば，あるデータベース内において 30 代の男性全員が特定の疾病に罹患している場合，k-匿名化処理によって同じデータが複数存在する状況となったとしても，34 歳の男性がデータベース内に存在すれば，その人は疾病に罹患していると推測可能となる．このような推測を避けるために，センシティブ情報（この例では疾病）を多様化させることで，誰がその疾病に罹患しているか判別しにくくなる．

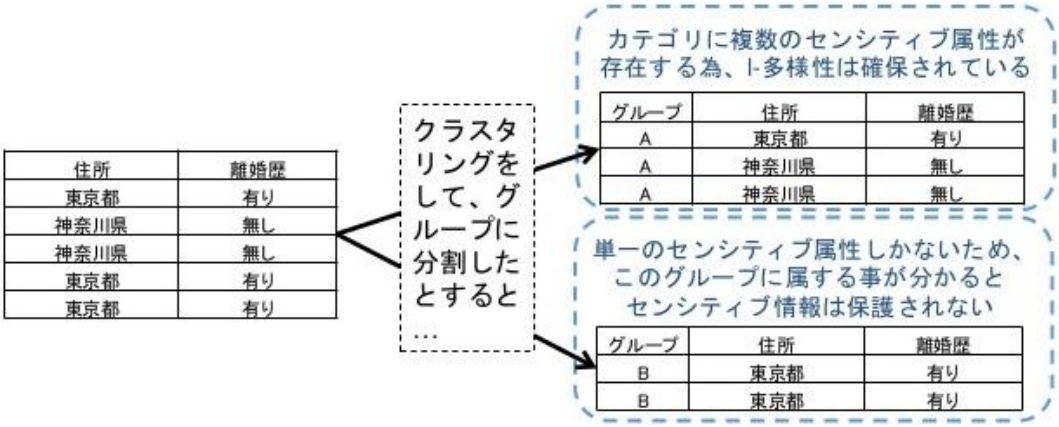

図 6 l-多様化 [43]

2.4.3 t-近接化（t-closeness）

k-匿名化処理において，秘匿されるべき属性を持つレコードの分布が偏っている場合，エントロピーと出現確率の観点より，個人情報が流出する可能性が考えられる．秘匿されるべき属性に関するレコード分布の分散を調整し，個人を特定しにくくする処理を t-近接化（t-closeness）とよぶ [35].

2.4.4 ダミー（Dummy）

ダミー（Dummy）とは，データにダミー情報を混入し，個人を特定しにくくするプライバシー保護手法である．ダミー技術を用いることで，データの持ち主とデータベース管理者以外は，どの情報が偽物なのか判別が困難である．たとえば位置情報の場合，ダミーの軌跡が自然となるようにダミー情報を生成することで，プライバシー保護の可能性が向上する [44].

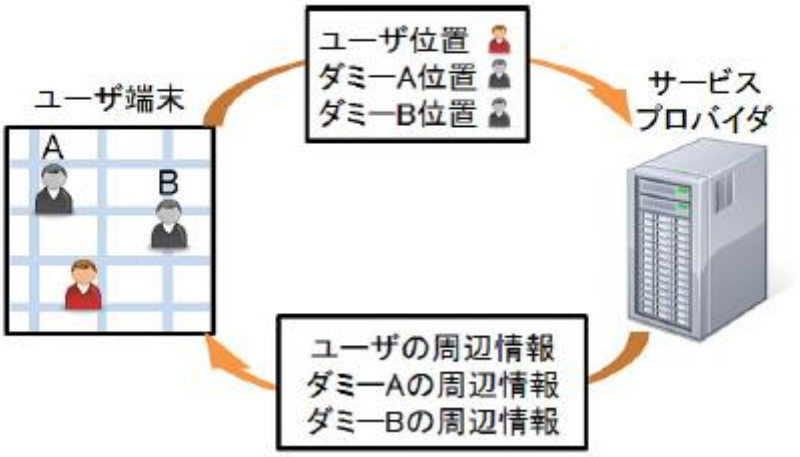

図 7 ダミー（Dummy）[45]

移動の軌跡に関する情報に関しては，ユーザー間の軌跡を交差させることで追跡可能性を低下させることが可能であり [40], 殊に位置情報の利活用についてはダミーを用いた保護技術の利用が効果的といえよう．しかし，位置情報以外のデータベースに関しては，そのデータベースに蓄積されるパーソナルデータの要素によって，自然なダミーの生成の困難さは大きく変化する．

2014 年に NTT が発表した Pk-匿名化技術においては，k-匿名化処理をしたうえで，さらにダミーレコードを付与することで，匿名性を向上させつつもデータ利活用を可能にしたとしている [46]. ダミーレコードが追加されたデータベースをマイニングする場合，ベイズ推定やエントロピーを考慮した出現確率の計算を行い，ダミーレコードが追加される前のデータベースをマイニングした場合と近い結果を導出する [46].

2.4.5 差分プライバシー

時系列ごとにデータが蓄積される種類のデータベースの場合，そのデータベースに新たに追加されたレコードにセンシティブ情報が含まれていると個人情報が流出するリスクが考えられる．そこで，レコードの増減そのものに差分を加えることで，新たに増えたセンシティブ情報を含む人の存在を隠すことが可能となる．これを差分プライバシーと言う [40].

また，時系列ごとにレコードが追加されるデータベースでは，既存のレコードを統計的に計算することで新たなレコードの推測が可能となる．

差分プライバシーを利用するデータベースでは，要求に対してラプラスノイズを加えた値を出力する [40].

2.4.6 暗号化

データベースそのものを暗号化する手法はデータマイニングにおいて基本的な手法だが，暗号鍵の安全性を保持するため，鍵長の変更が求められる．しかし一般的に，鍵長の変更時には，暗号文を平文に復号した後，新たな鍵長を用いて暗号化を行うため，復号した状況において，情報の漏えいリスクが考えられる．暗号化したまま，新たな暗号鍵を用いる場合には，データを分割する必要があるほか，二度目以降の暗号化が不可能である[47].

しかし準同型暗号を用いる Ronald Cramer らの手法を用いた場合，暗号化処理をした状態のままでマイニングが行えるほか，データ所有者のみが鍵を所有し，所有者同士は互いのデータを見られないにも関わらず，マイニング結果に限っては閲覧が可能となる[47].

また，秘密計算では，暗号化したままのデータを分散化し，その断片の計算を行うことで，データを暗号化したままの状態でマイニングを実行できる．また，分析者は個々のレコードに触れることなく，分析に関する要求のみを行い，統計分析の結果を受け取るためパーソナルデータの流出リスクが低下するとしている．

一方，情報通信研究機構の開発した準同型暗号を用いた手法の場合，データを暗号化する際に，暗号文そのものをデータ領域と付加情報に分けることで，付加情報を伸ばすことが可能となる．これにより，数十年程度が限界であった暗号鍵の寿命を 100 年以上に伸ばすことが可能となった[48].

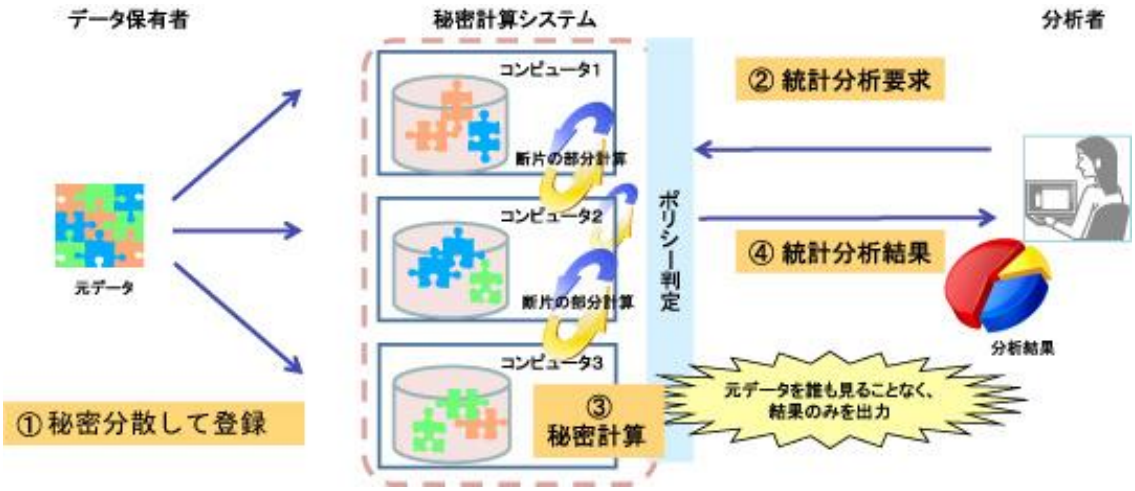

図 8 秘密計算[49]

しかし量子コンピュータの開発などの，革新的な技術発展により，暗号鍵の寿命が大幅

に変動する可能性により，準同型暗号による暗号化手法もまた恒久的な保護手法とはなりえなく，計算機技術の発展をにらみつつ暗号化手法を絶えずアップデートすることが求められる．

2.5 本章のまとめ

本章においては，まず国内外におけるデータ利活用の実例を挙げるとともに，それに付随して起こった問題を紹介した．その後，プライバシー権そのものの移り変わりと，データ利活用に関連したプライバシー保護技術を紹介した．

まず，2.2 ではビッグデータという言葉が我が国でバズワードとして叫ばれるようになってから巻き起こった，データ利活用に関する象徴的な事例である，JR 東日本の Suica 利用履歴データ販売と，NTT ドコモのモバイル空間統計を対照事例として取り上げた．両事例はそれぞれ，企業が保有するデータをマイニングした後，他の企業や団体へ有償で提供するビジネスモデルである． JR 東日本の Suica 利用履歴データ販売に関してはマスメディアやユーザーから起こったバッシングに押し切られる形でデータ販売を中止し，NTT ドコモのモバイル空間統計に関してはおおむね好意的な報道がなされた後，2015 年春現在もそのビジネスモデルは継続中である．

それぞれが販売（しようと）したデータは，現在の個人情報保護法に抵触しないデータであったほか，一定の暗号化や k-匿名化処理をした後に提供（しようと）されたものであり，一定の技術的な配慮がなされた上に行われたといえる．それにも関わらず，両者の明暗を分けたのは，データ利活用に自らのデータが用いられることを許容するか否かのオプトイン・アウトの仕組みの周知が遅れたことや，どのようにデータが利活用されるかを事前に周知できなかったからだと考えられる．また，NTT ドコモのモバイル空間統計は，JR 東日本の Suica のデータ販売の“炎上”を目の当たりにした後，起こり得る問題の対策方法を事前に検討できたことも事態をスムーズに進められた要因と考えられる．

また，ふたつの事例は，交通系カードとモバイル端末という，我々の生活にとって非常に身近かつ，それなしでは日々の生活の利便性が大きく損なわれるような存在が生み出すデータの利活用に関するものである．つまり，それぞれの事例において，我々はデータを生み出すことに対する拒否が難しい状況に置かれており，それらが生み出すパーソナルデータの利活用を巡るプライバシーに対する決断を我々は一方的に迫られる．当然ながら，利便性に伴って「データを生み出すことが避けがたい状況」に置かれ，かつデータの収集や利活用に際して嫌悪感を抱いている場合，サービスを利用しながらも，サービスとデータを巡る状況そのものに疑いの目を向ける．サービスの主体がユーザーに対してオプトアウトの窓口を用意し，周知の努力を払うことは当然として，そもそもデータの利活用というプライバシーの選択を迫ることそのものが権力的な構造を孕んでいる [3].

続く 2.2.4 では，国外におけるデータ利活用と，それに伴って起こった問題を紹介したが，

特筆すべき事例は Netflix によるアルゴリズムコンテストといえる．Netflix 社はそれまでのデータ利活用に伴って起こった他社の事例を踏まえ，個人が特定できない状態となるよう ID の振り直しや k-匿名化処理を行ったのちにコンテスト用のデータを公開した. しかし，結果を見れば，Netflix が提供した「匿名化された」としたデータベースを IMDb の公開データベースと突きあわせてマイニングを行うことで数人の個人が特定された．本件は，データマイニングによってパーソナルデータ流出する事態が，ひとつのデータベースから起こるだけでなく，様々な予期せぬ事態によって起こり得ることを示唆した．また当然ながら，Netflix 社の件では，事態の収束に伴って CEO が辞任する事態となったほか，サービス利用者に大きなマイナスイメージを植え付けた．これは，データ利活用に際してプライバシー問題が起こった場合，著しく企業のイメージを毀損するリスクが伴うことを示した例といえよう．

したがって，乱暴な表現をすれば，プライバシーに関する保護技術の進歩は目覚ましいものだという前提を評価したうえで，重大なインシデントに繋がる可能性を考慮して，盲信や過信は禁物と考えるべきである．当然ながら，一旦流出したパーソナルデータの複製や移動を止めることは困難であり，将来に渡って多大な負の影響を及ぼすリスクがある．

続く 2.3 ではプライバシー権の成り立ち，および，コンピュータ時代におけるプライバシー権についての大枠を紹介した．プライバシー権そのものが「放っておいてもらう権利」から，様々な技術の登場と，多様化するプライバシーの侵害応じて「自己決定権」へと変容した過程を描いた.「自己決定権」はデータ利活用におけるプライバシー権とも密接な関係であり，今日におけるデータ利活用に関するユーザー配慮の代表的手段であるオプトイン・オプトアウトの根底思想である．先に挙げたデータ利活用に関する事例における，JR 東日本の Suica のデータ販売に対して生じた否定的意見の理由をオプトアウト窓口の周知不足に求める報道事例も存在したことは，自己決定権に配慮することがデータ利活用を円滑に進めるための重要な要素であると社会的に認知されている好例と言える．

その後の 2.4 では代表的な PPDM について紹介した．PPDM はデータを加工する「摂動化」と，データそのものに暗号化処理を加える「暗号化」に大きく分けられる．これらのプライバシー保護技術は，理想的な環境下においてはプライバシー保護が実現するが，k-匿名化におけるデータを扱うための外部機関の設置などの，環境の実現に対するハードルの高さが技術の適用に伴う場合や，プライバシーに配慮しすぎるがあまり，マイニングをしても有益な統計情報を得られないといった可能性も存在する．

2.5.1 技術への理解と対話の有用性

今日におけるデータ利活用に関するプライバシー保護技術は，高度な数学の応用やアルゴリズムの適用によって支えられているため，それらの専門知識に精通していなくては理解が難しい．また，データ利活用時におけるプライバシー保護技術の適用は，あくまでも

データベースを保有する企業などの団体が行うものであり，ユーザーの視点からは，実際に説明された通りの保護技術が自らのレコードに関して行われているのか確認する術はない．

したがって，データ収集・利活用を行う団体は，プライバシー保護に関して技術的に最大限の努力を払うという立場をユーザーに表明するとともに，そこで行われるプライバシー保護技術や施策についてユーザー目線から理解できるよう詳細に説明するのはもちろんのこと，ユーザーに信用されるように努めることがデータ利活用に伴う軋轢を防止するために肝要といえる．

またその一方で，ここまで見てきたように，パーソナル保護を目的とした絶対的な技術は現時点において存在しない．したがって，データを収集・利活用する団体は，保護技術の弱点を理解したうえで，最大限のパーソナルデータ保護に努める姿勢が求められる．

2.5.2 データをめぐる円滑な取組とユーザー感情の理解

コンピュータ科学や数学に精通する者でなければパーソナルデータを保護する技術の理解は困難である前提はもちろん，それらの技術が実際に用いられてデータ保護が行われているかについて，データを収集・利活用する団体でなくては知る由もない．そうした，「ユーザーの目が届かない，技術を巡るブラックボックス」の存在は，データの収集・利活用を円滑に進めるうえで，大きな障壁となりえる．「何が起こっているのか分からない」からこそ，データを収集し，利活用する者たちを信用するしかない．

パーソナルデータという個人の尊厳にかかわる情報であるにも関わらず，その取扱い方法が不明瞭である場合，昨今の様々なデータ流出騒動も相まって，人々の嫌悪感や抵抗感を喚起させる．

データ収集・利活用に対する安心感は，技術論によってのみ生まれるのではなく，データを巡るブラックボックスが構造的に生じることを踏まえ，データ収集・利活用を行う団体はユーザーに寄り添う姿勢をアピールしなくてはならない．

加えて，サービスとユーザーが生み出すデータ収集は一体であるが，データ収集や利活用に否定的な感情を向ける場合がある．オプトアウトによって，そうしたユーザーの意思を尊重したとしても，サービスの主体，データ収集・利活用主体は，データを生み出すすべてのユーザーに対して一方的にプライバシーの選択を迫る．そしてデータを生み出すサービスが，通信インフラや交通機関，コミュニケーションツール，地図アプリケーションなど，生活に欠かせないものや利便性が極めて高い場合，我々はその選択から逃れられない．データを巡るオプトアウトは「嫌であれば止めることができる」という仕組みであり，声を上げない限りは，データを収集・利活用される可能性がある[3]．サービスの価値が，プライバシーに対して構造的に優位に立つ要因であることをサービスの主体は理解する必要がある．そうした構造の中に置かれ，データ収集・利活用に対して嫌悪感や負の感情を抱

いている場合，「足元を見ている」かのようなイメージの発生と，プライバシーの配慮不足に対する判断が厳しくなる可能性が示唆される．

データを巡る安心感をはぐくむためのアピールを適切に行うためには，サービスの価値を巡るサービス主体が優位となりがちな，サービス主体とユーザーの構造を理解したうえで発生するユーザーの「感情」に基づくプライバシー観と，データ収集・利活用に関する不信感が生まれる仕組みを理解しなくてはならない．

データ収集・利活用を円滑に進めるうえで，それらのユーザーの「感情」を理解したうえでプライバシーを捉えることと，プライバシー保護技術の向上は，互いに，円滑なデータ利活用を行うための片輪であり，どちらも欠かせないのである．

2.5.3 事例と技術論を踏まえたユーザースタディの必要性

データ利活用を巡り，プライバシーへの不安から軋轢が生じて利活用が中断された JR 東日本における Suica の事例や，それとは対照的に，目立った“炎上”もなくサービスが継続されている NTT ドコモによるモバイル空間統計などの実際の事例を個別に検討することで，データ利活用においては技術理解を中心に対する安心感と，オプトアウトなどの「パーソナルデータに関する自己決定権」をユーザーに提供することが肝要であるといえる．

データ利活用を巡り，パーソナルデータを保護する技術である，PPDM については，高度な数学的・情報学的知識が理解に不可欠であるばかりか，それぞれの技術においては非匿名化のリスクが示唆されるものも存在する．

したがって，データ利活用を円滑に行うための「プライバシーへの配慮」は，「技術的な配慮」と「ユーザーの感情への配慮」に大きく切り分けて検討すべきであり，技術面においてのリスクが不確定に存在し，技術がユーザーの目に届きにくい以上は，ことさらに「データ利活用の場面において，いかにユーザーがプライバシーに関する不安感を抱かせないようにする」ための感情への配慮が重要である．特に，本邦においては，米国と比較して，企業によるパーソナルデータの取扱いに関するユーザーの信用度が低いことから [50], ユーザーの感情を理解したうえで，ユーザーの信用を勝ち取ることがデータ利活用において求められる．

そしてデータ利活用に関連した，ユーザー感情への配慮は，「ユーザーが何に対して不安感を抱くか」「どのような場面で不安感を抱くか」といった，社会学的なアプローチを避けて通れない．

Ⅲ　類似研究と本研究の仮説

3.1 A.Westin によるプライバシーに関するユーザー調査

今日におけるプライバシーに関するユーザー調査の草分けのひとりである A.Westin は，1978 年より数多くの社会学的調査を手掛けた[51]．調査対象は，プライバシー一般だけでなく，消費者におけるプライバシー，医療におけるプライバシーなど，プライバシーが問題となり得る場面の多岐に渡る[51]．また，調査によっては，企業を通して行われたものや，ビジネスにおける特定のシーンに関するプライバシーに関するユーザー調査を目的に行われたものも存在する[51]．

A.Westin のユーザー調査の特徴は，それぞれの調査における解答を分類したのち，以下の 3 つに分類した点である（表 4）．これら 3 つの指標は，A.Westin やその共同研究者のみならず，多くのプライバシーに関する社会調査でも用いられている[51]．

A.Westin による社会調査の中で，データ利活用の存在を強く意識した質問文が初めて投げかけられたのは，1991 年の調査“Harris-Equifax Consumer Privacy Survey”である[51]．その中で，「個人情報が企業によって利活用されたり，移転することにに関して消費者はコントロールできない」という質問文に対して，「強く同意する」「どちらかといえば強く同意する」「どちらかといえば強く同意しない」「強く同意しない」「そう思わない」の 5 段階に分類した[51]．

また，1993 年の調査では，コンピュータによるデータ利活用を睨み，「プライバシーが保障される場合，将来的にはコンピュータの利用を大幅に制限されなければならない」という質問を行い[51]，回答を「強く同意する」「どちらかといえば強く同意する」「どちらかといえば強く同意しない」「強く同意しない」「そう思わない」の 5 段階に分類した．同様に，医療従事者がコンピュータを使用して患者のデータを扱うことや，カルテ情報などがコンピュータによって管理されることに対する意識を調査し，コンピュータが巻き起こすプライバシーの侵害に対する意識を“Computer Fear Index”と題し，「High Computer Fear」「Medium Computer Fear」「Low Computer Fear」の 3 つに分類した[51]．

表 4 A.Westin によるプライバシー3 分類[52]

原則型グループ（High and Fundamentalist）	プライバシーについて意識が強く，隠すべきものと考えるグループ
	企業に対して自分の個人情報を提供せず，その利用も認めない．そのために特別価格などの特典を得られなくても，企業による個人情報の不正使用や漏えいを避けることを優先する．
選択型グループ（Medium and Pragmatist）	プライバシーの価値を理解しているグループ．しかし，プライバシーをすべて隠すものだとしているのではなく，下記のような条件が整えば，企業に個人情報を提供し，活用させることを認める消費者．
	・消費者にとって大きなベネフィットが得られる ・企業が信頼できるプライバシーと情報セキュリティのポリシーを持っている ・重要な個人情報は法的に保護されること
開放型グループ（Low and Unconcerned）	プライバシーに対しおおらかな対応をするグループ
	プライバシーの意識レベルとしてはかなり広い範囲を含むと考えられる．

A.Westin による調査では，その調査内容に応じて，先に挙げた“Computer Fear Index”“Medical Privacy Concern Index”など，新たなラベルを適宜生み出している[51]．しかし，A.Westin によるプライバシーに対する認識の根源に横たわるのは，彼が最初期の調査によって提唱した表 4 のプライバシー3 分類であり，彼自身が Co-President を務める Japan Privacy Center が公表する彼の業績の一部でも引用されている[52]．

プライバシー3 分類は，ユーザーのプライバシー観をその強度に応じて分類をされるため，極めて直感的かつ，応用しやすい側面があるものの，そのプライバシー観が生み出された環境に対する議論は含まれない．つまり「なぜその状況において，ユーザーはそのプライバシー観を持つに至ったのか」という視点が含まれないため，ある状況下におけるユーザーのプライバシー観を客観的に理解することはできるものの，その状況下でプライバシーの侵害によってまき起こる問題の解決や予防のためには力不足である．

データの利活用が当たり前のように行われる時代において，データ収集・利活用の主体が直面するのは，ユーザーのプライバシー観の理解の必要性はもちろんのこと，現実の利

活用の場面でプライバシーを軸に巻き起こる，ときに利活用を大きく阻害する問題の解決方法の検討に対する困難さである．

そして当然ながら，「データ利活用を円滑に進めるため」という大義のもとにプラグマティックな視点からユーザーのプライバシー観を理解するのであれば，その方法は 2 つ考えられる．ひとつは，詳細な場面を想定し，それに応じて質問項目を決めて調査を行う方法である．そして，ふたつ目は，プライバシーという，定義が流動的かつ，それでいて多くの人が存在を認識する気持ちの源を理解し，プライバシーの侵害という負の感情を生み出す環境の発生を理解するという，「『プライバシー』が発生する環境を包括したうえで人々のプライバシー観を理解する営み」である．

3.2 モバイル端末とプライバシーに関する調査

モバイル端末やデータ利活用に関するユーザー調査に関しては，位置情報にフォーカスしたものをはじめ，特定のデータやシチュエーションを前提としたものが多くみられる．本邦においては，総務省情報通信政策研究所が発表した「位置情報の利用に関する意識調査[53]」と題した調査で，モバイル端末が創出する位置情報の種類に対する知識，アプリケーションの利用状況，データを提供する際のインセンティブ，データの利活用や取得・保管方法に関する意識を年代ごとに調査を行った[53]．しかし，本調査では，アプリケーションや知識などの項目に関する質問については，定量的な調査が効果を発揮したと考えられるものの，データを差し出す際のインセンティブや，データの提供を許容できるシーンなどに関する調査項目については，前述の通り，H.Nissenbaum[32]をはじめプライバシーの意識がその場面に応じて変化する可能性が示唆されているため，単純な質問紙調査によってプライバシー意識を理解するのは困難と考えられる[32]．IPA 独立行政法人 情報処理推進機構が 2010 年に公表した，「eID に対するセキュリティとプライバシに関する認知と受容の調査報告書」では，日本と欧州における，パーソナルデータに対するリスク認知やインターネット利用者の考え方に関する調査・分析が行われた[54]．報告内では，プライバシーの環境依存性を示唆しているものの，行われた調査では，「氏名」「年齢」「国籍」などのパーソナルデータを入力する際の受容度に対する調査について環境が考慮されていない[54]．

国外においては，D.Cvrcek らが位置情報に関する意識調査を行い[55]，国，男女ごとに，位置情報に関する金銭的価値，データの収集主体に対する抵抗感を調査した[55]．しかし，先に挙げた総務省による調査と同じく，先に質問項目を与えたうえで調査を行ったため，やはりプライバシーの環境的な側面が欠落しており，その結果の背景に存在する感情に対する検討が困難である．定量的な調査に関しては，企業によるデータ利活用に対する意識を社会階層別に 4,000 弱の標本を通して調査した K.Sheehan[56]や，量的調査によってオンラインユーザーは自身のプライバシーに関する関心が薄いと結論付けた G.Nowak ら[57]，社会保障番号と氏名を提供することを比較した場合は前者の方がプライバシーに対して抵抗感

を持ちうるとした G.R.Milne[58]，データを収集する団体に関する親近感の度合に応じてプライバシーに関する感覚が変化するとした E.K.Rogers[59] など，さまざまな切り口から行われたユーザーのプライバシー観に関する調査が存在する．

3.3 本章のまとめと，本研究における仮説の設定

ユーザーのプライバシー観を探り出すことを目的に行われた調査の多くは，「特定の状況におけるプライバシー観を理解するため」に行われている．しかし，スマートフォンをはじめとする，パーソナルデータが次々と生み出されるシステムに囲まれた我々にとって，プライバシーの制限や侵害は，ときとして予想外な場面においても起こり得る．したがって，特定の状況を想定して行われた調査と，同じ状況が起こり得えない限り，その調査結果がプラグマティックな力を持つには至らない．

また，H.Nissenbaum の言葉を借りれば「我々は環境（Context）に応じてプライバシーを選択し」[32]，その環境は，提供するデータの質，利活用の方法，データを収集する団体に対する感覚，その時の気分など，極めて多岐に渡るため，簡略化された状況や評価指標を用いた定量的なアプローチによってユーザーのプライバシー観を完全に理解することは難しい．

特定の状況下における定量的な手法で得られるプライバシー観に関する調査の前段階に存在する，モバイル端末に関連するプライバシー観そのものを理解する営みを行ってこそ，特定の状況下における定量的に調査したプライバシー観の理解がより一層なされ，現実に起こるデータ利活用などの局面で起こり得る問題解決に向けた，調査結果の応用がなされるのである．

プライバシー観そのものに踏み込んだ議論は，A.Westin による調査[51]が，ユーザーのプライバシー観を理解するうえで基礎的な役割を果たすと考えられるが，A.Westin による調査では，プライバシー観をその強度によって 3 分類し，さらにその結果は構造化された調査手法によって導きだされている．したがって，プライバシー観を生み出す感情面の理解は反映されていない．

実際のデータ収集・利活用を巡る場面では，技術を巡る理解の難しさから，ユーザーの「感情」が環境的なプライバシー観を左右する．したがって，A.Westin による基礎的なプライバシー観の分類を感情の理解によってさらに詳細に分類，あるいは分類目を再構成できる可能性を仮説として挙げられる．

また，先に挙げた，データの収集と利活用に際しては，データを生み出すサービスの利便性の存在を背景に，オプトアウトが用意される状況だとしても，ユーザーはプライバシーに対する決断を迫られるという，サービス提供者優位の状況が構築される．したがって，データの収集や利活用を巡るプライバシーを感情面と共に理解するためには，サービスの利便性とデータ，ユーザーとサービス主体が織りなす，サービス主体優位の構造を念頭に

おいたうえで，サービス利用に伴うデータの収集・利活用に対するプライバシー観が形成される可能性があると示唆できる．

3.4 本研究における仮説の検証方法

3.3 で掲げた仮説を踏まえ，本研究では，モバイル端末ユーザーのプライバシー観を「感情」の観点を含めて深く理解するため，A.Westin による先行研究を踏まえ，社会学的質的調査の手法を用いて，表層的なプライバシー観の背景に潜む，サービスの利便性とデータ創出，ユーザーとサービス主体における関係から生み出される「感情」を汲み取り，プライバシー観の深層理解に努める．

具体的には，まずはインタビューに類する質的調査手法を用いて，A.Westin のプライバシー3 分類を検証するとともに，それらの分類目がユーザーの感情とどのように関連しているのかを探る．これにより，モバイル端末によって作り出されるデータ収集・利活用に関するプライバシー観が，A.Westin による 3 分類に則るのか，あるいは感情の要素を加えて検討することで，分類目が A.Westin によるものと異なるのかを確認する．

サービスの利便性が極めて高い場合や，生活に欠かせないサービスである場合，そのサービスがプライバシーの制限を伴ったとしても，嫌悪感と共にプライバシーの制限を“甘んじて受け入れ”てサービスを利用する人も存在するだろう．また，そうした状況に似たものとして，プライバシーの制限を公益性や利便性を理由に“心の底から納得してプライバシーの制限を受け入れ”た場合も考えられる．しかし，これらふたつの状況は，「その場の状況を踏まえてプライバシーを検討し，サービスを利用する」という点において A.Westin の 3 分類では「選択型グループ」となる．当然ながら，両者の行動の結果そのもの（サービスを利用する）は同じであっても，その行動を形作るプライバシー観は，前者は嫌悪感を伴う「否定的」なものであり，後者は「肯定的」である．したがって，モバイル端末に関するデータ収集・利活用に対するプライバシー観は，A.Westin による 3 分類を踏襲しつつも，「選択型グループ」をサービスの価値やプライバシーの侵害に対する感情によってさらに中分類できると仮説付けられる．また，「選択型グループ」において，甘んじてプライバシーの制限を受け入れる層は，サービス利用の当事者でありながら，プライバシーに対して厳しい目を向ける．したがって，現実におけるデータ収集・利活用のシーンにおいて，“炎上”を防ぎ，スムーズなデータを巡る施策を実行するためには，サービス利用の当事者でありながらプライバシーをネガティブに検討する層の感情理解が効果的である．

そしてさらに，質的調査によって中分類した「選択型グループ」を組み込んだプライバシー観の 3 分類を量的調査によって検討する．選択型グループ内の中分類の状況が，どのような要因によって起こるのかを定量的に評価することで，実際にデータ収集・利活用のシーンで起こるプライバシー問題の要所を汲み取り，防止策の検討に役立てることが可能となる．

Ⅳ　仮説の検証

4.1 質的調査

本研究にかぎらず，意識調査にあたっては，質問紙などによるアンケートなどの量的調査と，インタビュー調査やインタビュー分析などの量的調査が考えられる．しかし量的調査やあらかじめ質問内容を設定した構造化インタビュー手法を本研究で用いた場合，調査対象者によって知識量が異なるため，位置情報に関連したデータの利活用を巡って発生したプライバシー問題や議論，匿名化・暗号化技術などを調査対象者に説明しなくては調査対象者が適切にアンケートに答えられない可能性がある．そのうえ調査に掛かる知識を被験者に事前に与えた場合，強力なキャリーオーバー効果が発生し，適切な調査結果が得られないと考えられる．

そこで，まずはモバイル端末ユーザーが抱えるプライバシーに関する意識を半構造化インタビューの形式で拾い上げた後，3.3 で掲げた A.Westin のプライバシー3 分類の再検討に繋げる．

4.2 質的調査の本調査

4.2.1 調査対象者

論者の知人および，秋葉原駅近辺，新宿駅近辺，渋谷駅近辺にて本研究に賛同する 33 名の男女（男性 15 名，女性 18 名）．（表 5）

4.2.2 調査方法と期間

調査期間は 2014 年 4 月 1 日～2015 年 5 月 31 日.「モバイル端末の位置情報とプライバシー」を題目に，喫茶店やレストランなどの飲食店にて，携帯電話やスマートフォンの所有・使用状況や，アプリケーションの使用状況，位置情報に関する知識，プライバシーに関して自由に話して頂き，謝礼として 1,000 円分のクオカードを贈呈した．また，会話内容はすべてノートによって筆記を行った．

表 5 調査対象者一覧

（S はスマートフォンの所有有無）

#	年齢	性別	職業	S
1	30 歳	男性	会社員（ウェブデザイナー）	○
2	28 歳	男性	会社員（金融）	○
3	29 歳	女性	会社員（通信）	○
4	23 歳	女性	会社員（プログラマー）	○
5	23 歳	男性	大学生（医学部）	○
6	20 歳	女性	大学生（文学部）	○
7	20 歳	女性	大学生（文学部）	○
8	31 歳	女性	会社員（サービス）	○
9	23 歳	女性	会社員（建設）	○
10	27 歳	男性	会社員（卸売）	○
11	69 歳	男性	無職	○
12	32 歳	男性	経営者	○
13	24 歳	男性	大学院生	○
14	21 歳	女性	大学生（経済学部）	○
15	36 歳	男性	会社役員	○
16	30 代	女性	大学職員	○
17	31 歳	男性	自営業（美容師）	×
18	36 歳	男性	会社員（プログラマー）	○
19	21 歳	女性	大学生（経営学部）	○
20	30 歳	女性	主婦	○
21	60 歳	男性	武道家	○
22	23 歳	女性	会社員	○
23	35 歳	男性	自営業	×
24	35 歳	男性	会社員	○
25	58 歳	女性	パート従業員	×
26	25 歳	女性	公務員	○
27	25 歳	女性	学生	○
28	22 歳	女性	学生	○
29	27 歳	女性	会社員	○
30	55 歳	男性	看護師	○
31	31 歳	女性	看護師	○
32	56 歳	男性	自営業	○
33	58 歳	女性	自営業	○

4.2.3 調査と倫理

本調査にあたっては，インタビュイーに対して，調査で知りえた情報は本研究と関連研究以外に用いないこと，個人名や年齢，性別などのパーソナルデータと発言内容などのパーソナルデータの保管は大学内で厳重に保管することを口頭，および書面にて説明した．本調査に関連した倫理の要項を記した用紙に対して署名を行う同意を得られた場合においては，署名を行った書類を本人の控えと論者用の 2 通を作成し，これをもって謝礼の受け取りを証明するものとした．収集した調査結果は A4 のノートページ 65 枚分に手書きで記録した．東京大学空間情報科学研究センターの研究倫理委員会による審査を経た後，本調査を実施した．

4.2.4 調査の分析方法

本調査の分析に際しては，KJ 法を用いた．KJ 法とは川喜田二郎によって考案された質的調査における分析手法であり [60]，そのイニシャルをとって命名された．本調査は，既存のプライバシー観に関する分類に疑問を呈し，プライバシー問題の発生メカニズムまでを理解しようとする冒険的なものであるため，全体を俯瞰しやすく，新たな発想や仮説，概念が生まれやすいとされる KJ 法を用いた．

また，川喜田によれば，真の科学的な方法のためには，データを獲得した手段・方法をガラス張りにした上でデータを提示すること，データの加工処理方法がガラス張りであること，結論が明示されていることの 3 点が必要であると述べている [60,61]．

4.2.5 調査によって得られたデータの分析の前提

インタビューによって得られた発言をカードにまとめたうえでカテゴリーごとに分類して整理を行った．恣意的な分類を避けるため，事前に用意したあるカテゴリーに，発言をすべて無理やり分類するのではなく，それらの発言については独立したものとして扱った．

4.2.6 調査によって得られたデータの KJ 法を用いた分析

インタビューによって得られた文字データをプライバシーに関する発言と，どのような事例に関連しての発言かをカードにまとめて分類を行った．例えば，「携帯ゲームとかで GPS のデータとか収集されてたとしても，プライバシー的にもやもやしても，会社が何やってるか分からないから（プライバシーを）諦めてる」という文章を「携帯ゲーム」「GPS データ」「プライバシー　もやもや」「会社が何をやっているか分からないから諦め」というそれぞれのカードに分類した．その後，各カードの内容が同じものや，近いものを集め，

その中でも頻出した項目を持つカードや，集められたカードの内容を象徴的と考えられる発言のカードを抽出した．そして作られたカードの山を親和性を考慮して空間上に配置して関係性を見出した．

表 6 KJ 法によって得られたガテゴリー分類

大分類	中分類	
原則型グループ		プライバシー権の絶対性
		データ利活用を通して生まれる利潤への嫌悪感
		匿名化技術への疑念
		プライバシー保護が実際になされているかの疑念
		データ流出への危惧
解放型グループ		企業への安心感
		自己のパーソナルデータへの無価値意識
		知識の欠落
		無関心
選択型グループ	納得型グループ	社会貢献への意識
		利用サービスへの対価
		サービスを利用するうえでの必要性の理解
		データ収集や利活用に関する説明責任
		企業などの知名度
	諦めグループ	プライバシーの制限と共にあるサービスの圧倒的有用性
		周囲（環境）の圧力
		ユーザーの声の無力感に対する自覚

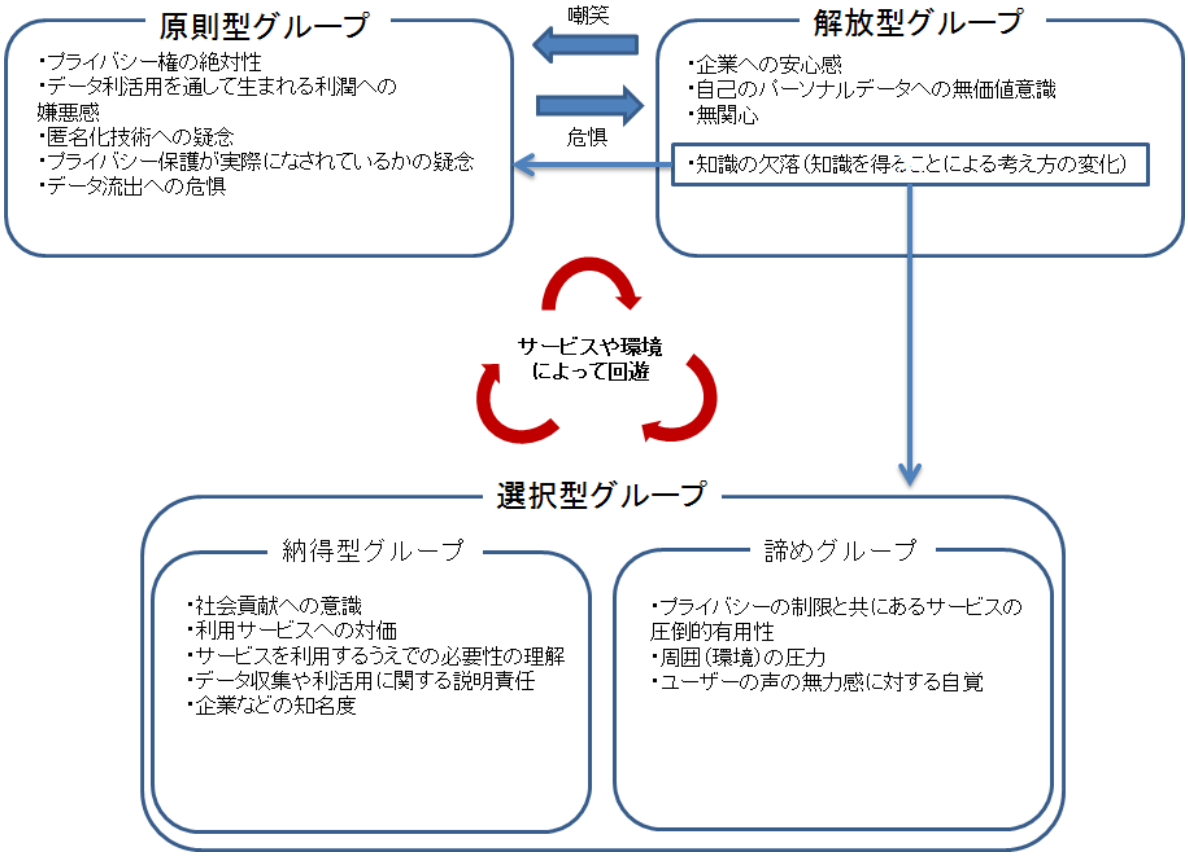

図 9 KJ 法によって得られたガテゴリー分類

4.3 質的調査の考察と，A.Westin のプライバシー3分類と選択型グループの分割

本章では，本調査の結果をもとに，モバイル端末が創出するデータに関するプライバシー観の分類化を試みるとともに，グループ観同士の関係性，およびプライバシー観と知識量についての考察を行った．

KJ 法によって得られた相互関係は，「原則型グループ」「開放型グループ」「選択型グループ」の 3 つに分類が可能であり，さらに「選択型グループ」は「納得型グループ」「諦めグループ」に分類できた．

モバイル端末とデータをめぐるプライバシー観は，各々の知識量によって形成される側面もある．聞き取り調査を通して知識に関する質問が質問者へ投げかけられることがあり，知識を入手することで，データ利活用などに対して否定的な考えを持つに至った場合が顕在された．

また，3 つの大分類グループに属する層の人々は，互いにその考え方の差異を認める傾向が見られ，特に「原則型グループ」と「開放型グループ」間では，互いを敵視する傾向が確認された．

4.3.1 原則型グループ

モバイル端末が創出するデータに伴うプライバシーを非常に強い権利として捉え，守られるべきものとして考える人々．プライバシーが侵害されるリスクに対して恐怖の感情を抱いている場合や，データ利活用に対して否定的な感情を持っている場合，データのオーナーとしての権利を激しく主張する事例が顕在する．

また，データ利活用によって企業などが利潤を得ることに対して否定的な意見も見られた．

■インタビューより

●「理由は分からないけど，とにかく気持ち悪いからやめて欲しい」

●「アプリを使う時とか，携帯を契約するときとかに，色々（データ収集に関する）説明をしてくれるけど，どれだけ安全と説明されてもとにかく嫌な気持ちを拭えない」

●「自分の行動とかの情報を知られたくないのもあるけど，いろんなデータを集めて分析だのして企業に売ったり，よくニュースになってるじゃない．ああいうのは，だいたい，誰のデータで金儲けしてるんだって感じ．許せないわ」

●「できれば誰にも自分の行動とかを知られたくない．自分は喫煙者だけど，買い物の履歴とかを知られたくないから，T ポイントカードとかタスポなんかは使わない．Suica もでき

れば使いたくない」
●「普段，奥さんに居場所を知られたら困る場所に行ったりしているし，そういう位置情報とかは，たとえ誰かに公開しないとしても，企業とかに教えたくないかな．普段やましいことをしているから，余計に自分の行動を察知されたくないんですよ」
●「自分の情報を提供したくないから，怪しいアプリとかは使わない」
●「紙に名前や住所を書くのと違って，ネットの場合はデータをコピーしたり送るのが簡単じゃない．だから，自分の情報がどんどん拡散されるのが恐いから反対」
●「情報の匿名化とか言うけど，技術のことは良く分からないし，その会社とかが本当に匿名化されているのか疑わしい．情報の保管とかも，データ流出とかよくニュースになってるし，本当に流出しないようにしてるのか疑わしい．だから，俺はデータを提供したくない.」
●「自分の情報を誰が持っているのか分からないのが恐いから止めて欲しい」
●「自分の居場所とかの情報が漏れて悪用されるかも知れない」
●「居場所とか分かってストーカーとか事件に巻き込まれたりするのが恐い．だって，たとえばその時間に誰が居るって分かったら，誰に恨まれてるか分からないし，いきなり刺されたりするかも知れないじゃないですか」
●「個人情報を集めてるのは知ってるけど，集めた情報の使い道が分からないのが恐い．使い道ないでしょ，そんなの」
●「やましいことがなくても気持ち悪いからイヤ」
●「情報を持っている会社だけが儲けるには気に入らない．どうして情報を渡した側はお金とかもらえないの？　おかしいでしょそれ」

4.3.2 開放型グループ

モバイル端末が創出するパーソナルデータに関して，無関心，あるいはその価値を認めないグループ．原則型グループに分類される考え方に対して嘲笑的な見方をした意見も見られた．

また，モバイル端末が創出するパーソナルデータに関する知識やマイニング，利活用などの現状に関する知識を有していない場合もあり，「何も知らないが故の無関心」という場合も存在した．また，そのような場合，ときに会話の中で質問者に対して質問が投げかけられ，モバイル端末が創出するデータや，データ利活用などの知識を得ることで，プライバシーに関しての考え方を改めたり，否定的な意見を持つに至るなどの状況が見られた．

■インタビューより
●「別に自分の情報が会社とかに知られても，友達とかじゃないし，まぁいっか，と思う．

だって，その会社の人は他人だし，自分と関係ないし，わざわざ私の情報をいちいち見ないと思う」
●「(データ利活用とプライバシーに関する情報を）知らなきゃ関係ない．わざわざ色々教えられると怖くなるのが人間じゃないですか．知らぬが仏」
●「お前のデータは大統領か芸能人かと（普通の人にとってのデータに価値は無い)．いちいちプライバシーのことをガタガタ言う人は自分のことを何だと思ってるのか，と思う．誰もお前のことなんて気にしてないだろう，と」
●「どうぞどうぞ好きにしてください．勝手にすればって感じですね」
●「特に気にならないし，気にしたこともない」
●「(プライバシーに気を配らない人が増えた）そういう時代でしょ？」
●「なんとなくどうでも良い」
●「会社は他人だし，友達にならともかく，自分の情報を渡しても気にならない．さすがに友達とか親とかに，自分の行動とか居場所は知られたくないかな」
●「データは束にならないと価値にならない．ひとりひとりの情報に価値なんてないし，それを企業とかがいちいち見るとは思えない．それに，見られたとしても，それがどうしたって感じ」

4.3.3 納得型グループ（選択型グループ）

A.Westin によるプライバシー3 分類における，「選択型グループ」のうち，自らのデータを渡すことに対して，納得感をもって受け入れるグループ．利便性や社会的貢献などの視点から，プライバシー権が制限されることを納得している．データの収集・利活用に関する情報を自ら収集し，リスクや便益を理解し，肯定的な感情をともなってサービスを利用している．

■インタビューより
●「自分の情報で社会が便利になるなら喜んで自分の情報を提供しますね．助け合いというか，お互いに協力し合うことで生まれる便利さとか，新しいサービスもあると思う．それに自分が一役買えるなら，それは悪くない」
●「サービスをタダで使ってるから，それでチャラかもね．Google マップとか，Youtube とか，ああいうのだって使う人の情報を集めてるからタダな訳でしょ？　だからといってお金を払ってまで使いたくないし，そこまでの嫌悪感はないかな」
●「きっとそういうののおかげ（データ提供）で（サービスを）タダで使えてると思うし，それに対して良い思いもさせてもらってるから，特にイヤな気分はないかな」
●「きちんと，会社とかが，個人情報をどのようにするのか説明してくれれば納得できるから大丈夫．そのためには，会社とかは，信用してもらえるように努力しないとね」

●「データの収集や利活用に関して，オプトアウトの仕組みを用意してくれれば全然問題ない．イヤな時に逃げられるっていう安心感があれば納得できる」
●「その場面に応じて柔軟であるべきだと思う．たとえば，無名の会社が作った怪しいサービスとかに自分の個人情報を入力したりするのは絶対にいやだけど，大きな会社だったり，国だったり，利用目的がはっきりしていればＯＫ」
●「説明の仕方にも問題があると思う．データの活用とか収集を『させてください』って感じなら納得できるけど，上から目線で来られるとイヤかな」

4.3.4 諦めグループ（選択型グループ）

A.Westin によるプライバシー3 分類における，「選択型グループ」のうち，データ利活用に嫌悪感を感じながらも，利便性に押しきられる形でプライバシーの制限を受け入れるグループ．

データの収集目的や情報の開示，保管方法，利活用方法，第三者提供などの説明責任の必要性を強く求めると同時に，オプトアウトの権利を求める声が多く見られた．しかし積極的なパーソナルデータのコントロール権をサービス提供企業に求める一方で，企業の情報漏えいや法令違反に関する報道を例に挙げて，要求が正しく受け入れられるかや，説明内容の真偽に関して疑問を唱える意見が多く見られた．

しかしサービスの利便性が高い場合，規約の文面の真偽はともかく，同意せざるを得ない．したがって携帯電話などのインフラデバイスや地図アプリケーションなど，我々の生活に不可欠なサービスに関しては，圧倒的にサービスの力が増大し，「諦め」の感情を伴って，プライバシーの制限を受け入れる．

■インタビューより
●「本当は嫌だけど，どうせ会社は色々勝手にやってると思うし，私たちが何を言っても変わらないからしょうがない」
●「会社とかに自分のデータを渡さなきゃいけないのは凄く気持ち悪いけど，便利さには負ける．だいたい，携帯やめますか，人間やめますかってレベルでしょ，今の時代は．だったら諦めて便利な方を取りますよ」
●「どうせ，反対したところで勝手に色々なことをやられる．口だけで会社とかが『個人情報は保護します』とか言ってもウソかもしれないし，自分たちは無力なんですよ．でも，ときどき，こういうのが当たり前になったら，今もそうだけど，将来はどうなってしまうんだろうかと不安になるわ」
●「(プライバシー問題があるから）だからといって，携帯電話やアプリを使わない選択肢はない．それに，いまさら，昔の生活に戻ろうとしても，不便になるのはイヤだし，周りもスマホ使うし，LINE とか使うし，アプリとか使わないと普通の社会生活すら送れなくな

る．本当は，もっと個人情報とか厳しく考えたいけどね」

●「便利なんだから諦めるしかないじゃないですか．本当に会社もよく考えてるよね．使う人がイヤだと思っても，結局会社の思い通りになるんだから」

●「アプリとか携帯を契約するときに利用規約とかあるけど，読まずに適当にサインしちゃう．本当はよくないことだと思うけど，あれにサインしたり同意しないとサービス使えないし．会社の思うつぼなんだろうけど，サービス使いたいから，イヤな気持ちになっても諦める」

●「まぁでも，いくらサービスを使うにしても，嫌なものは嫌だから，何かあるとツイッターとかで文句を書いたり，まとめブログとかのネタに反応したりすることもある．最近だと，LINE を使うか使わないかのスレで LINE を叩くレスをした．文句を言っても使ってるけど」

4.4 「納得型グループ」と「諦めグループ」によって構成される「選択型グループ」の整理

選択型グループを構成する「納得型グループ」と「諦めグループ」の差異の根底に存在するのは，「諦めグループ」における「本当は嫌だけど」のような，本来の判断である．「諦めグループ」は，「何らかの理由により，プライバシーに関する否定的な感情を持ちながらも諦めてそのサービスを利用している」のであり，裏を返せば「理由が無ければ，わざわざプライバシーの制限を認めて，そのサービスを利用しない」ということである．反対に，「納得型グループ」では，原初状態と実際の環境，その両方において，納得感をもってプライバシーの制限を受け入れてサービスを利用する．

したがって，サービスそのものの価値を V，サービスを取り巻く環境的価値を E（原初状態では E=0），プライバシーの制限を L とおき，すべてを効用と捉えた場合，表 7 のように選択型グループを 2×2 のマトリクスとして整理可能である．なお，現実における状況を「行動状態」とし，原初状態においては，「生活の必需品」のような環境的価値を検討する必要がないため，常に E=0 である．また，各マスにおける変数の総和がユーザーにとっての価値であり，もっとも大きな和のマスが合理的な行動となる．

表 7「選択型グループ」のマトリクス

ユーザーの行動状態におけるマトリクス

	プライバシー制限	プライバシー制限されない
サービス使う	(V+E,-L) →(V+E)+(-L) =V+E-L	(V+E,-L=0) →(V+E)+(-L) =V+E
サービス使わない	(V+E=0,-L) →(V+E)+(-L)=-L	(V+E=0,-L=0) →(V+E)+(-L)=0

ユーザーの原初状態におけるマトリクス

	プライバシー制限	プライバシー制限されない
サービス使う	(V,-L) →V+(-L)=V-L	(V,-L=0) →V+(-L)=V
サービス使わない	(V=0,-L) →V+(-L)=-L	(V=0,-L=0) →V+(-L)=0

たとえば，サービスの価値（V）が 1，サービスに伴う環境的価値が（E）が 3，プライバシーの制限（L）が 2 である場合，表 8 のようになり，左上のマスの効用が最も高くパレート最適となるため，行動状態においては「プライバシーが制限され，サービスを使う」が合理的な選択となる．なお，右上のマスについては，「プライバシーが制限されず，プライバシーが制限された場合と同等のサービスが受けられる状態」であり，たとえば GPS 機能をオフにした場合に地図アプリケーションの利便性が損なわれるように，「データ収集によってサービスクオリティが向上する」という前提と矛盾するため考慮しない．

対して，原初状態のマトリクスにおいては，右下のマスの効用が最も高くなり「プライバシーが制限されず，サービスも使わない」パレート最適となる．

このように，原初状態と行動状態，それぞれのマトリクスにおいてパレート最適が異なる状態は，「本当なら嫌だ」というプライバシーに関する否定的な感情がありつつもサービスを我慢して使う「諦めグループ」である．

表 8「諦めグループ」を表すマトリクスの例

ユーザーの行動状態におけるマトリクス

V=1,E=3,L=2の場合

	プライバシー制限	プライバシー制限されない
サービス使う	(1+3,-2) →(1+3)+(-2)=2	(1+3,0) →(1+3)+(0)=4
サービス使わない	(0,-2) →(0)+(-2)=-2	(0,0) →(0)+(0)=0

→左上が最も効用が高いため（実質的なパレート最適）、サービスを利用してプライバシーが制限される（右上は「プライバシーが制限されず、プライバシーが制限された場合と同等のサービスが受けられる状態」であるため考慮しない）。

ユーザーの原初状態におけるマトリクス

	プライバシー制限	プライバシー制限されない
サービス使う	(1,-2) →(1)+(2)=-1	(3,0) →(3)+(0)=3
サービス使わない	(0,-2) →(0)+(2)=-2	(0,0) →(0)+(0)=0

→右下の効用が高いため、環境的価値が存在しなければ、サービスを利用したくないと考える。

行動と感情で、パレート最適が異なるので、納得できず利用！（「諦めグループ」の状態）

次に，サービスの価値（V）が 3，サービスに伴う環境的価値が（E）が 3，プライバシーの制限（L）が 2 である場合を検討してみよう．この場合，「行動状態」，「原初状態」の両方で，パレート最適となるのは「プライバシーが制限され，サービスを使う」のマスである．つまり，「友達が使っているから仕方なく」「それが無いと生活に支障をきたす」といった現実における環境が無かったとしても，サービスそのもの価値を認め，プライバシーの制限があろうともサービスを利用する状況である．これは，サービスの価値とそれに伴うプライバシーの制限に対して納得感をもってサービス利用する，「納得型グループ」である．

表 9「納得型グループ」を表すマトリクスの例

ユーザーの行動状態におけるマトリクス

V=3,E=3,L=2の場合

	プライバシー侵害	プライバシー侵害されない
サービス使う	(3+3,-2) →(3+3)+(-2)=4	(3+3,0) →(3+3)+(0)=6
サービス使わない	(0,-2) →(0)+(-2)=-2	(0,0) →(0)+(0)=0

→左上が最も効用が高いため（実質的なパレート最適）、サービスを利用してプライバシーが制限される（右上は「プライバシーが制限されず、プライバシーが制限された場合と同等のサービスが受けられる状態」であるため考慮しない）。

ユーザーの原初状態におけるマトリクス

	プライバシー侵害	プライバシー侵害されない
サービス使う	(3,-2) →(3)+(-2)=1	(3,0) →(3)+(0)=3
サービス使わない	(0,-2) →(0)+(-2)=-2	(0,0) →(0)+(0)=0

→行動状態と同様、左上の効用が高いため、環境的価値を加味せずともサービスを利用したいと考える

行動と感情で、パレート最適が同じなため、納得して利用！（納得型グループの状態）

「選択型グループ」が「諦めグループ」と「納得型グループ」に分類されるのは，各ユーザーにおける，サービスそのものの価値判断と，環境的価値，およびプライバシー制限によるマイナス要素が異なることによる．原初状態と現実における判断が捻じれの関係にある「諦めグループ」は，あくまでも環境的価値によって“仕方なく”サービスを使っており，決して望ましい状態とはいえない．対して“健全”な状態である「納得型グループ」を作りだすには，「皆が使っている」「それが無いと生きていけない」のような環境的価値だけでなく，サービスそのものの価値を高めると同時に，プライバシーの制限を低下させるサービス作りが必要である．

4.5 知識を得ることと怖れの感情

モバイル端末を通して行われるデータの収集や利活用に関するプライバシー意識を聞き取るなかで，端末が持つセンサー技術や，データの収集方法，利活用などの知識の絶対量が少なく，プライバシーを検討する段階にないインタビュイーが確認された．

そのようなインタビュイーは主に「開放型グループ」に見られた．その場合，調査者に対して技術知識やデータ利活用によってできることなどを尋ねられることがあり，知識を提供することにより，「原則型グループ」や「選択型グループ」の考え方に変化する場合が見られた．

本研究のような，社会学的調査はもちろん，サービスを利用するうえでの説明責任を企業などのサービス提供者がきめ細やかに行えば行うほど，データの収集や利活用に際する怖れの感情が膨らむことが考えられる．

■インタビューより

・「逆にこちらから聞きたいんだけど，携帯からどんな情報が送られるの？」

→（インタビュワーが，GPS センサーや基地局データによって位置情報を把握することを説明する）

→「そんなこともできるんだ．そういうの聞くと怖くなっちゃうよね．今までは知らなかったから気にならなかったけど，やっぱり怖いし，個人情報を渡したくないって思う」

・「昔は何も考えてなかったし，知らなかったんだけど，友達にそういうの（モバイル端末のセンサーやデータ利活用に関する知識）に詳しい人が居て，会社とかがデータを集めて色んな自分の情報を知ってるって聞いて怖くなった」

・「せっかくのこういう場だから教えを請いたいです．この機械（スマートフォンを指さして）を使うとどんな情報が企業にいくの？　たとえば，地図とかのアプリを使ったりすると自分の居場所が表示されるんだけど，どうなってるのか不思議で仕方がない」

→（地図アプリの場合は，GPS データが地図アプリを運用するサーバに送信されることを説明する）

→「それじゃあ，こういうの（アプリ）の会社は私の居場所を知っているということ？　気持ち悪いね．聞かなければよかった」

4.6 グループ間における対立意識

聞き取り調査を通し，「～という人もいると思うけど」のように，自分が属するプライバ

シー観のグループ以外の存在を認知している事例が見れらた．その場合，自己が属する以外のグループの考えに対して，意見を持つことがあり，特に「原則型グループ」と「開放型グループ」の間で，対立関係が見られた．

■インタビューより
・「個人の居場所とか，端末の利用履歴とか，単体ではまったく無価値でしょ．そんなことにガタガタ言うヤツはどうかしてる」（開放型グループ）

・「自分の周りはプライバシーを気にしないし，個人情報の取扱いにも関心がない．凄く怖いことだと思う」（原則型グループ）

・「お前は王様か，キムタク（芸能人）か．誰もお前の居場所なんて気にしないし，考え過ぎの連中のせいで社会が便利になるのが邪魔されると思うと腹立たしい」（開放型グループ）

・「社会が便利になるのに，何が悪いの？　プライバシーは大事かも知れないけど，権利を主張しすぎるのはどうかと思う」（開放型グループ）

・「便利さに負けて，権利を手放していったら，とんでもないことになるかも知れない．そうなったら遅いですよ」（原則型グループ）

4.7 質的調査のまとめと未来への危惧

本調査の結果を KJ 法によって分析したモバイル端末ユーザーのプライバシー観は，A.Westin によるプライバシー3 分類を踏襲する結果となった．しかし，「選択型グループ」は，ユーザーの行動だけみれば「何らかのインセンティブなどの理由によってプライバシーの制限を受け入れている」ことには変わらないが，感情の側面において，プライバシーの制限を受け入れる理由を心の底から納得しているか，嫌々受け入れるかの差異が存在する．したがって，モバイル端末におけるデータ収取・利活用に伴うプライバシーに関するユーザー観は，A.Westin による 3 分類を踏襲しながらも，「選択型グループ」をさらに分類が可能であり，3.3 で挙げた，A.Westin によるプライバシー3 分類の見直しに対する仮説が実証されたといえよう．

「諦め」の感情を伴ってプライバシーの制限を受け入れる場合，その背後にプライバシーの制限に対して負の感情を伴うため，ひとたび利用しているサービスなどが情報流出やデータ利活用の方針を変更するなどのイベントが起こった場合，過敏に反応し，「原則型グ

ループ」のような振る舞いをすると考えられる．したがって，プライバシーの制限やデータ収集が明らかなサービスの場合は，利用者の中には，そのサービスに否定的な感覚を持ちながらも利用している層が存在し，それらが「炎上」と呼ばれるソーシャルネットワーク上の否定的意見の火種となる場合や，サービスの評判を落とすリスクとなり得る．

データ収集や利活用に対しての説明や，オプトアウトを求める声に関しては，ほぼ全グループ内で見られたが，「諦め」の感情を持つグループ内に関しては，それらが実際に機能しているかに疑問を持つ場合が見られた．

データ収集や利活用が創る未来については，原則型グループは否定的，開放型グループは楽観的（ユートピア的），納得型グループは楽観的，諦めグループは否定的であった．「諦め」の感情を持つグループ内では，将来を危惧するものの，時代の流れや企業，利便性などの巨大な力に対して，無力感にさいなまれている様子が見られた．そして，データ収集や利活用に伴うプライバシーの制限によって起こる将来を憂う気持ちが，自分をとりまく環境によって押しつぶされ，ユートピアを掲げる団体の方針に「諦めながら」従う．データの収集や利活用を円滑に進めるためには，そもそもサービスを利用しない可能性が高い原則型グループが持つ否定的意見だけでなく，データ収集や利活用に対する違和感を持ちながらも行動的には賛成の立場を取る層の感情を汲み取ることが肝要といえる．

また，サービスに関連して一旦定まった指針や慣習，デファクトスタンダードは，硬直化し，将来に対しても影響を及ぼす．データ収集や利活用がもたらす未来に対し，当事者が持ちながらも，表面化せず掻き消された危惧の意識を注意深く理解することにより，将来に対する指針が浮き上がる．つまり，「諦めグループ」を深掘りすることにより，将来の視点が生まれ，データ収集・利活用がスムーズに進むのである．

表 10 A.Westin によるプライバシーの 3 分類[52]における「選択型グループ」を「納得型グループ」と「諦めグループ」に分割した分類手法

<table>
<tr><td colspan="2">原則型グループ
（プライバシー原理主義者）</td><td>プライバシーについて意識が強く，隠すべきものと考えるグループ.</td></tr>
<tr><td colspan="2">開放型グループ
（無関心）</td><td>プライバシーに対しおおらかな対応をするグループ.</td></tr>
<tr><td rowspan="2">選択型グループ</td><td>納得型グループ</td><td>プライバシーの価値を理解している．しかし，プライバシーを絶対的に制限されてはならないものだと考えるのではなく，条件が整えば，納得感を持って，企業に個人情報を提供し，活用させることを認めるグループ.</td></tr>
<tr><td>諦めグループ</td><td>アプリケーションやデバイスが生活に欠かせない場合や，利便性が著しく高い場合に発生するサービス事業者の一方的な権力構造によって，ユーザーがプライバシーの点において諦めの境地に達したグループ．データ利活用に嫌悪感を感じながらも，利便性に押しきられる形でプライバシーの制限を受け入れる.</td></tr>
</table>

4.8 量的調査

質的調査によって，モバイル端末が生み出すデータの収集・利活用に関するプライバシー観は A.Westin による 3 分類が確認できたほか，「選択型グループ」を「納得型グループ」と「諦めグループ」に分割できた．これをもとにウェブを利用した質問紙調査を行い，データ収集・利活用に関連したプライバシー問題を解決するための視点を提供する「諦めグ

ループ」を深掘りする．サービス利用の当事者でありながらプライバシーの制限に否定的な感情を抱く「諦めグループ」を形作る要因を定量的に確認し，データ収集・利活用の勘所を探る．なお，ウェブを用いた調査に関しては，インターネットユーザーが持つ批判的な傾向が指摘される [62]．しかし，データ収集・利活用を巡っての批判的な言説や“炎上”は，SNS や匿名掲示板などのインターネット上で見られ，また本調査の目的は「サービスの当事者でありながらもプライバシーに関する不安」を抱く，「諦めグループ」を調査し，データ収集・利活用に関するリスクを汲み取り，批判的な感情から実際に起こるデータ収集・利活用を妨げる言説の防止と理解が目的であるため，インターネットユーザーを対象とした．

4.9 量的調査の本調査

4.9.1 調査対象者

インターネット上のアンケートサービス「クラウドワークス（https://crowdworks.jp/）」の登録利用者，2,956 人の男女．

4.9.2 調査方法と期間

クラウドワークスに登録するユーザーに対して質問紙調査を行う．1 回答あたり 40 円のインセンティブを提供し，それに賛同するユーザーの回答を収集する．調査期間は 6 月 18 日～6 月 30 日．調査内容は，年齢，性別，年収，スマートフォン所有の有無，以下の 3 点である．

1）モバイル端末を通して利用するアプリケーションやウェブサービス利用時のプライバシーに関する不安意識

アプリケーションやウェブサービスをモバイル端末で利用する際，どのようなシチュエーションでプライバシーに関する不安感を抱いたかをアプリケーションやサービスの選択肢を設けて調査を行った

2）諦めの感情

質的調査を通して得た分類目「諦めグループ」を理解するため，「プライバシーに関する不安感を感じながらもサービスを利用した経験の有無」「プライバシーに関する不安感を抱きながらもサービスを利用するに至った理由」を調査した．

3) 利用規約の活用状況

アプリケーションやウェブサービス利用開始時の利用規約の活用状況と，利用規約内で重要だと思う項目を選択式で調査した．

4.9.3 調査と倫理

本調査の実施にあたり，クラウドワークス上の倫理規約を遵守し，調査結果を個人が特定できない統計的データとして学術的に公表することの同意を得るとともに，東京大学空間情報科学研究センターの研究倫理委員会による審査を経た後，本調査を実施した．

4.10 量的調査の考察

4.10.1 回答者の属性

解答者の年齢は，30 代が 39.1%でもっとも多く，次いで 20 代が 30.4%であった．性別は男性が 29.9%，女性が 70.1%であった．スマートフォン所有率は全体を通じて 88.0%，年収は～200 万円が最も多かった（表 11）．

表 11 回答者の属性

（%）

年齢構成	10 代	20 代	30 代	40 代	50 代	60 代	70 代～
	3.1	30.5	39.8	20.2	5.2	1.1	0.0
性別	男性			女性			
	30.8			69.2			
スマートフォン所有率	はい			いいえ			
	88.4			11.6			
年収	～200 万円	200 万円～300 万円	300 万円～400 万円	500 万円～750 万円	750 万円～1000 万円	1,000 万円～	
	64.1	15.4	13.2	5.7	1.2	0.5	

4.10.2 プライバシー関連

スマートフォンを所有する人のうち，80.0%が「スマートフォンを使用している際にプライバシーの不安を感じた経験がある」と回答した（表 12）．そのうち「あなたは，プライバ

シーに関する不安を感じながら，アプリケーション（アプリ）やウェブサービスを利用した経験はありますか？」に「はい」と答えた回答者は 87.2%にのぼった（表 12）．これにより，「諦めグループ」に類する，「本当はプライバシーに不安要素を感じていながらも，何らかの理由でサービスを利用せざるを得なかった」という経験をした回答者のボリュームが明らかになった．

表 12 スマートフォン利用とプライバシーへの不安

（%）

スマートフォンを利用している際にプライバシーの不安を感じた経験の有無	はい	いいえ
	80.0	20.0
プライバシーに関する不安を感じながら，アプリケーション（アプリ）やウェブサービスを利用した経験の有無	はい	いいえ
	87.2	12.8

プライバシーに関する不安を感じながらも利用したサービスでもっとも多かったものは，EC（買い物），SNS であり，一方で，メッセージアプリやメール，ニュースに関するサービスを挙げる回答者は少なかった（図 10）．このことから，自分でパーソナルデータを入力する際に，ユーザーはプライバシーの不安を感じやすく，サービス利用に際して，自動的にサーバへパーソナルデータが送られるサービスに関しては不安感を抱きにくいと推測できる．

また，プライバシーに関する不安感を抱きつつもサービスを利用した経験があった回答者 2,364 名のうち，不安を感じながらもサービスを利用した理由として挙げられたのは，「便利だから」が 1,664 名，「自分の周囲がそのアプリケーションを使っているから」が 877 名，「それが無いと不便だから」が 658 名であった（図 11）．プライバシーに関する不安を感じながらも利用したアプリケーションに SNS や EC が挙がっていることから，プライバシーに関する不安を抱きながらも，サービスの利便性や，「人と繋がるため」などの，環境的価値によって，サービスを利用せざるを得ない状況に置かれる場合が生まれると推測できる．

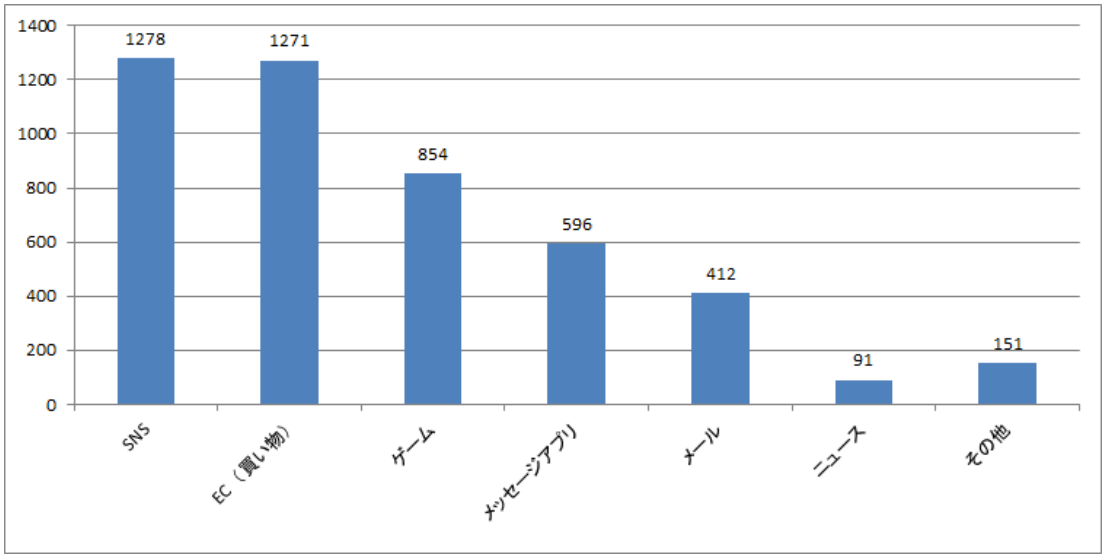

図 10 不安を感じながらも利用したサービスの内容（人）

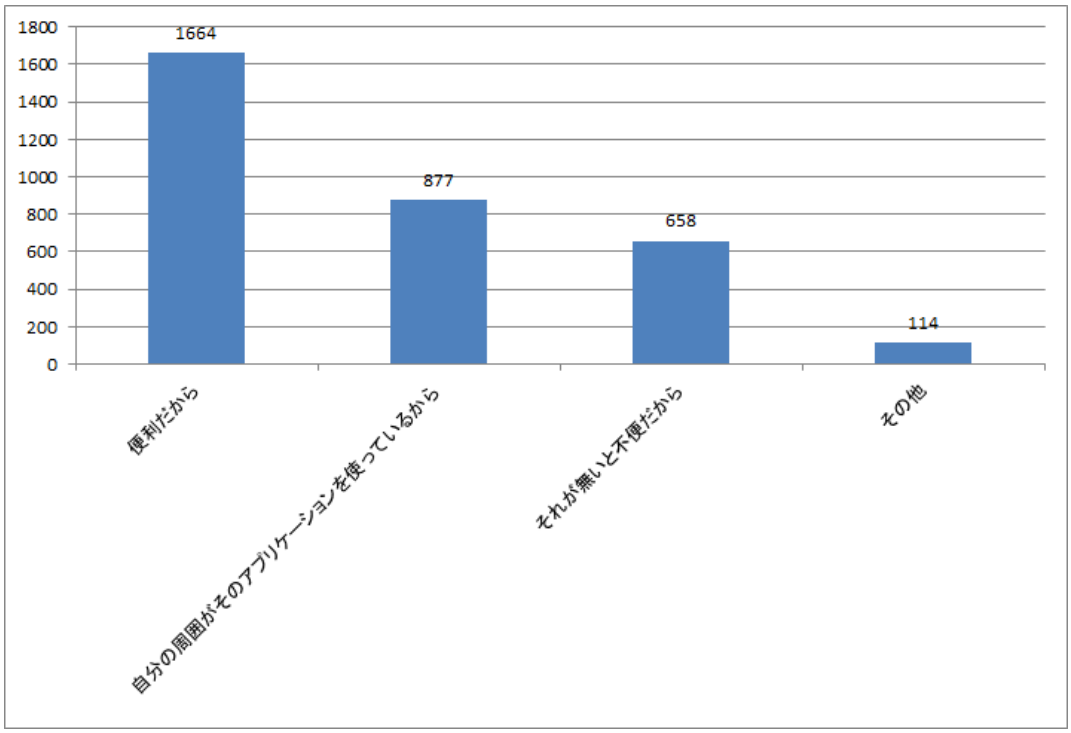

図 11 不安を感じながらもサービスを利用した理由（人）

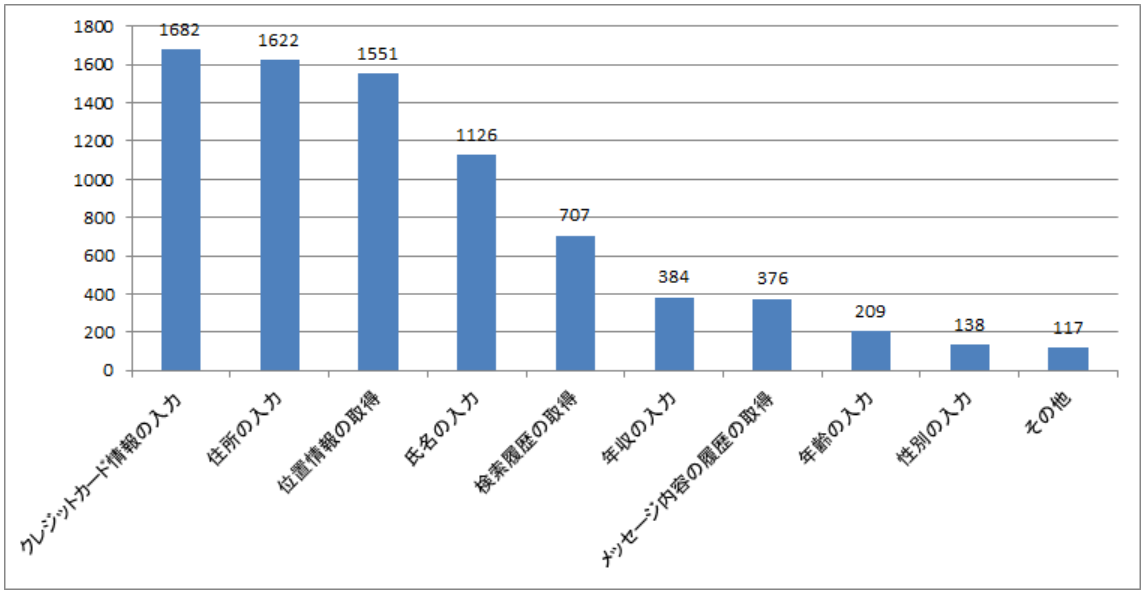

図 12 プライバシーの不安を感じさせるデータの項目（人）

また，プライバシーの不安を感じさせるデータの項目でもっとも多かったのは，「クレジットカード情報」，「位置情報」，「住所」であった（図 12）．それぞれの相関を見ると，「年齢」と「性別」，「性別」と「年収」，「検索履歴」と「位置情報」，「検索履歴」と「メッセージ内容」らが高い相関関係にあり（表 13），R を用いた並行分析によって因子を抽出したところ，「住所」「氏名」などの国税調査などで調査対象となるデータのグループ（「検索や位置情報，メッセージなどの，自分で新たに生み出すパーソナルデータに関心のあるグループ」）と，「検索履歴」や「位置情報」などのモバイル端末から得られるデータのグループ（「性別や年齢などの，固有のパーソナルデータに関心のあるグループ」）の 2 種類のパーソナルデータの区分が存在することが示唆される（表 14）．

表 13 プライバシーの不安を感じさせるデータ項目の相関関係

	年齢の入力	氏名の入力	住所の入力	性別の入力	年収の入力	検索履歴の取得	位置情報の取得	メッセージ内容の履歴の取得	クレジットカード情報の入力
年齢の入力	1								
氏名の入力	0.316310968	1							
住所の入力	0.21036528	0.614775797	1						
性別の入力	0.514505845	0.242488433	0.171685687	1					
年収の入力	0.289901304	0.283309927	0.297840663	0.329459525	1				
検索履歴の取得	0.198044336	0.254252028	0.23914335	0.184175587	0.271637125	1			
位置情報の取得	0.119819174	0.29739812	0.379729038	0.117499677	0.228728274	0.398656918	1		
メッセージ内容の履歴の取得	0.199692441	0.200241286	0.197264543	0.189845206	0.248105742	0.442867112	0.282019013	1	
クレジットカード情報の入力	0.098810352	0.298638775	0.43663194	0.08249609	0.226557194	0.234940147	0.389123167	0.190776973	1

表 14 プライバシーの不安を感じさせるデータ項目の並行分析と因子抽出

	Factor1	Factor2	Factor3	Factor4
年齢	0.636	0.128	0.172	
氏名	0.229	0.141	0.847	0.229
住所	0.147	0.114	0.522	0.536
性別	0.772			
年収	0.374	0.225	0.131	0.252
検索履歴	0.122	0.786		0.153
位置情報		0.385	0.141	0.476
メッセージ内容	0.18	499		0.155
クレジットカード情報		0.152	0.143	0.634

4.10.3 利用規約関連

サービス利用時の利用規約の確認状況については，「あまり読まない」が 42.1%でもっとも多く，次いで「ときどき読む」の 31.3%であり，「いつも読まない」「あまり読まない」「ときどき読む」の合計は 89.4%にのぼる．このことから，サービス利用に際しての利用規約が活用されていないことが分かる．

利用規約に関して「いつも読まない」「あまり読まない」「ときどき読む」場合の理由でもっとも多かったのは，「長い」の 2,459 名で，次いで「読まなくてもどうせアプリケーション（アプリ）を使う」の 994 名であった．このことから，利用規約の理解が一般のユーザーにはハードルが高く，サービスを利用するという目的が先立っている場合，用を成さない場合があると考えられる．

表 15 利用規約の活用状況

サービス利用時の利用規約の確認状況	いつも読む	ときどき読む	あまり読まない	いつも読まない
	10.5%	31.3%	42.1%	16.6%
利用規約を「ときどき読む」「あまり読まない」「いつも読まない」場合の理由」	長い	書いてあることが難しい	読まなくてもどうせアプリケーション（アプリ）・サービス使う	その他
	2,119 名	1,261 名	789 名	89 名

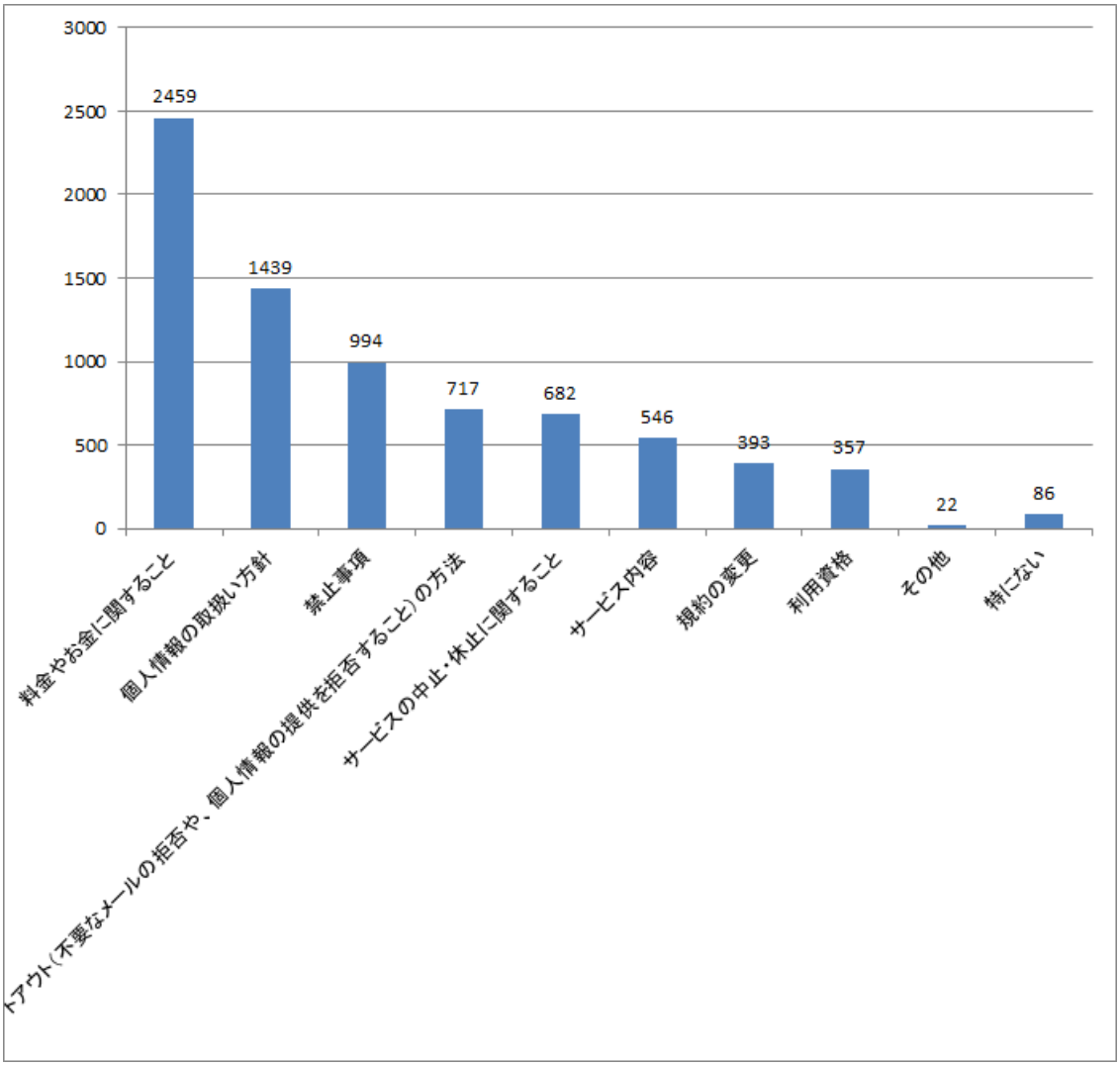

図 13 利用規約中でユーザーが気になる項目（人）

利用規約内で，ユーザーが気になる項目は，「料金やお金に関すること」が突出していた．続いて，個人情報の取扱い方針，禁止事項，オプトアウトに関心が集まる（図 13）．しかし，金銭や個人情報の取扱い方針に比べて，サービス利用の開始後に関連したオプトアウトへの関心が低いことから，利用者にとっての利用規約の位置付けは，「サービスを利用する段階における意思決定」であるといえる．還元すれば，ユーザーはサービス利用を決断した段階で，プライバシーを巡る制約を受け入れる覚悟をしている．また，日本における，企業が行うパーソナルデータの取扱いに関するユーザーの感情が否定的であることからも分かるように[50]，オプトアウトに対しても不信感を持つユーザーが存在し，「一度でもパーソナルデータを渡してしまえば，何が行われるか分からない」と考えるユーザーの存在も示唆できる．

利用規約でユーザーが気になる項目の相関関係を見ると，「禁止事項」と「利用資格」，「利用資格」と「サービス内容」，「オプトアウト」と「個人情報の取扱い方針」のペアが比較的相関関係にあり（表 16），R を用いた並行分析によって因子を抽出したところ．個人情報関係の因子と，利用資格や禁止事項などの利用そのものに関する因子が示唆された（表 17），利用規約を読む場合，個人情報やサービス内容など，自分の興味のある部分とその関連している部分のみを選び，その項目のみを読んでいると考えられる．

また，男女においての有意な差は見られなかった．

表 16 利用規約中でユーザーが気になる項目の相関関係

	料金やお金に関すること	サービスの中止・休止に関すること	禁止事項	規約の変更	利用資格	サービス内容	個人情報の取扱い方針	オプトアウト
料金やお金に関すること	1							
サービスの中止・休止に関すること	0.0765807	1						
禁止事項	0.055763825	0.096317553	1					
規約の変更	−0.007789982	0.142681088	0.231676718	1				
利用資格	0.055583552	0.127237533	0.322926642	0.203450611	1			
サービス内容	0.097436714	0.128352067	0.183417061	0.216730233	0.278382171	1		
個人情報の取扱い方針	−0.018201185	0.014455675	0.111910114	0.180778321	0.108442211	0.167790731	1	
オプトアウト	0.022266777	0.087255037	0.116772031	0.189861029	0.136619698	0.178088784	0.262057969	1

表 17 利用規約中でユーザーが気になる項目の並行分析と因子抽出

	Factor1	Factor2	Factor3	Factor4
料金やお金に関すること				0.277
サービスの中止・休止に関すること		0.106		0.28
禁止事項	0.292	0.156	0.145	0.186
規約の変更	0.134	0.968	0.187	
利用資格	0.95			
サービス内容	0.216	0.117	0.256	0.337
個人情報の取扱い方針			0.666	
オプトアウト			0.391	0.141

4.11 量的調査のまとめ

サービスに伴って発生する，データ収集・利活用に関する不安感を感じながらもサービスを利用する「諦めグループ」をこれまでに経験した回答者は全体の 80.0%にのぼる．また，その理由に，「自分の周囲がそのアプリケーションを使っているから」「便利だから」が「それが無いと不便だから」を挙げた回答者が見られ，サービスが持つ環境的価値によって，プライバシーの制限を受け入れてサービスを利用しているといえる．

サービスの利用開始に伴う利用規約については，「いつも読む」と答えた回答者は 10.5%であり，利用規約が形骸化していることがうかがえる．また，「どうせ読まなくてもサービスを使う」を，利用規約を読まない理由に挙げた回答者は 781 名にのぼり，サービスを利用しようと思い立った段階で，そのサービスが持つプライバシーの制限をはじめとするデメリットの検討は後回しになる．

量的調査を通して，モバイル端末が生み出すデータの中で特にセンシティブなパーソナルデータは「クレジットカード情報」「住所」「氏名」「位置情報」であり，それらのデータを収集・利活用する団体は特に注意を払うべきである．また，利用規約が活用されていない現状を踏まえると，利用規約中にセンシティブなパーソナルデータに関する説明をしたとしても，読まれない可能性が高い．したがって，データの収集・利活用に際しては，利用規約の文面を平易かつ，ポイントをまとめて簡略化することが効果的といえる．

また，プライバシーの不安を覚えながらも利用したサービスで，EC や SNS が挙がる一方で，ニュースサイトやメッセージアプリなどを挙げる回答が下位に並ぶことから，EC サイト利用時など，住所や氏名などを自ら記入してサーバに送信する場合以外で，どのような状況でパーソナルデータが送信されるのか理解していないユーザーが相当数居ると考えられる．その一方で，パーソナルデータとして気になる項目に，自動的に取得されることが多い位置情報が挙がることから，位置情報の取得に関しては，特にサービス提供において明確な説明が求められるといえる．

4.12 ふたつの社会調査で実証された当初の仮説

本研究において行った質的調査と量的調査の結果を合わせて論じる．まず，質的調査を通して，「原則型グループ」「開放型グループ」「選択型グループ」で構成される 4.12 で挙げた A.Westin によるプライバシー3 分類のうち，「選択型グループ」を「納得型グループ」と「諦めグループ」に分類できた．「選択型グループ」は，「サービスに関連するプライバシーの制限を理解して受け入れるグループ」である「納得型グループ」と「サービスに関連するプライバシーの制限を嫌悪感と共に，サービスの利便性などを理由に，甘んじて受け入れるグループ」である，「諦めグループ」によって構成される．

データ利活用に伴うプライバシー保護の技術が，ユーザーからは見えにくく，理解が難

しいことを踏まえてデータ利活用の事例を紐解くと，2.5 でデータ収集・利活用のケースを論じた中で挙げたように，“炎上”が起こった JR 東日本による Suica のデータ利活用の事例では，Suica という我々の生活にほぼ不可欠なツールが移動データを生み出し，利活用がなされるという事態において，オプトアウトなどの利活用を避けるための“逃げ場”が無かったことが軋轢を生んだ理由と考えられた．そのような，「本当はプライバシーの制限を受けたくないが，サービス利用を避けられない」という，諦めの感情を伴ってサービスを利用するグループが，質的調査によっても示唆された．

その後の量的調査を通して，プライバシーに関する諦めの感情を抱きながらもサービスを利用したユーザーが 8 割以上存在し，「諦めグループ」のボリュームの大きさが示唆された. 以上により, 3.3 で仮説として挙げた,「A.Westin によるプライバシー3 分類の再構成」，および「サービス主体優位の構造」が実証された．

しかし，モバイル端末に関連したパーソナルデータそのものに関しては，住所や氏名など，これまでの国勢調査や店頭アンケート，契約時などに収集されるもの（ここでは便宜的に「固有のパーソナルデータ」とする）と，位置情報や検索履歴などのモバイル端末によって新たに作り出されるもの（ここでは便宜的に「モバイル端末が生み出すパーソナルデータ」とする）に分類してユーザーは認識していると判明した．これにより，パーソナルデータの収集・利活用に関連した“感情”の理解に関しても，「固有のパーソナルデータ」と「モバイル端末が生み出すパーソナルデータ」の間で感情の発生メカニズムが異なると考えられる．よって，データ収集・利活用に伴うユーザーのプライバシー観の理解には，パーソナルデータのグループごとに，さらなる調査の必要性が示唆される．

また企業などのデータ利活用を行う団体が，ユーザーに対してプライバシーに関する技術や施策をサービスにおいてもっとも初めに説明する場は利用規約であり，サービス毎にいつも利用規約を活用する層は全体の 1 割程度であった．これにより，ユーザーが利用規約に触れる段階では，既にサービス利用を強固に決断しており，プライバシーをはじめとする，様々な規約内容に気を払わないことが示唆された．その一方で，利用規約において重要視されるのは，お金やサービスそのものに関するものと，個人情報の取扱いやオプトアウトなどのプライバシーに関するものに大きく分けられ，諦めの感情の背景にプライバシーへの不安が示唆された．これにより，企業などのデータ収集・利活用の団体が，サービスの利便性を逆手に取り，必要以上にデータ収集・利活用をしようとしたり，データ収集・利活用に対して真摯な説明を怠ると，大きな反感を買う可能性があり，“炎上”の要因となると考えられる．

V　議論・モバイル端末が創出するデータの収集・利活用と世代間倫理

5.1 世代間倫理とモバイル端末が創出するデータ

我々の身近なモバイル端末は，さまざまなパーソナルデータを日々生み出す．手のひらに収まる小さな機器からデータは送信され，データの束はサービスクオリティの向上や防災など，様々な目的を見据えて利活用がなされつつある．そしてそれに伴い，プライバシーの問題が巻き起こる．サービスを通じて得られたモバイル端末由来のデータを巡っては，そのサービスが我々にとって便利であればあるほど使用を避けられず，データの収集・利活用をもまた避けられない状況に追い込まれる場合がある．

データの収集・利活用の大義は，サービスクオリティの向上などの，ある企業とそのサービスのユーザーが恩恵を受けるものだけでなく，防犯や防災，人口統計，効率的な社会の実現など，我々全体に影響を及ぼすものも存在する．ことさら，後者に関しては，「暮らしを豊かにする」「自然環境への負荷を低下させる」といった，極めて耳障りがよく，納得や賛同を得やすい大義たちである．

しかしその一方，プライバシーに対する感覚は，ときに言語化が難しく，ともすれば「なんだか分からないけど気持ちが悪い」のような直感的な概念であるため，先に挙げた“分かりやすい”大義と天秤にかけた場合，理屈の面でプライバシーは分が悪い．とはいえ，我々の心には，確実にプライバシーに対する感覚が存在し，それは人間がアイデンティティを保ち，一人の自由な存在であるために不可欠な要素である．

再度，データの収集・利活用の目的に立ち帰れば，それは「人間のため」に帰着する．「人間（我々）のために」を大義に掲げて行う行為が，人間の尊厳の破壊にリンクするとすれば，それは大きな矛盾を孕んだパターナリズムに他ならない．

ほぼすべての科学技術が，人間の効用の最大化を目指し，時として，後戻りができない自然環境の破壊を引き起こし，あるいは生命を奪い，絶滅に追いやり，そのたびに我々は立ち止まっては反省を繰り返す．自然環境や生物など，物理的に計量が可能な事物は，破壊や消滅を容易く目測でき，種の絶滅や核汚染などの現時点の我々の科学技術をもってしても解決が不可能な状況は，極めて直感的な反省を我々に促す．

しかし，人種差別や男尊女卑など，人間の権利を人間が破壊し，収奪する行為については，人間が存在する限り回復可能性が残るものの，権利が失われた状態は，世代を超えて慣習や法として受け継がれていく．そして権利の回復にあたっては，時に人間の命を犠牲とした社会運動や政治など，多くの人々の尽力が不可欠であることは歴史を見ても明らかである．

プライバシー権は我々を人間たらしめる権利であり，人間の権利の破壊と収奪が一旦起

こった場合に，それが世代を超える問題となるのであれば，データ収集・利活用を巡るプライバシー問題を「利便性や公益性と引き換えに，プライバシー権が損なわれた社会が，果たして未来の人々にとって望ましいものであるか」という未来の視点から検討する必要がある．4.7 で挙げたように，モバイル端末におけるデータ収集・利活用に関するプライバシー問題は，データが収集・利活用されることが当然な時代が未来にとって幸せか現時点においては分からず，未来に向けた配慮や視点を考慮したうえで論じる必要がある．

現在を生きる我々の中にさえも，データの収集・利活用に対して，プライバシー権の破壊に関連した恐怖感や無力感，未来への危惧を語る意見を持つ者が居る以上，未来の人々を念頭におくことの重要性は極めて高いと言える．

本章では，「現在の世代を生きるものが，未来世代における生存可能性に対して責任を持つ」という倫理的言説である世代間倫理を用いて，モバイル端末が生み出すデータの収集・利活用に関連するプライバシー問題を検討する．そして世代間倫理から導きだされる現時点におけるデータ収集・利活用に対するプラグマティックな情報倫理を検討し，データ収集・利活用に伴う軋轢の予防策を論じる．

5.2 世代間倫理

世代間倫理とは，「現在の世代を生きるものが，未来世代における生存可能性に対して責任を持つ」という視点から出発した倫理である．主には自然環境問題を捉えるうえで用いられる倫理であり，自然破壊や資源の枯渇など，容易に回復が難しい行為をある世代が行うことによって，将来における人間の生存可能性が妨げられるリスクが生じるという考えから，現世代のあり方を模索する．

世代間倫理という言葉をはじめて用いたのは S.Frechette[63] であり，J.Rawls[64]，D.Callahan[65] の原初状態，社会契約における恩と義務の関係から，「我々が過去の人に対して恩義を感じると同時に，原初状態であれば世代間であっても不公平は存在するべきではない」という観点から世代間倫理を提唱した [63].

また，H.Jonas は世代間倫理の正当性を人間における親子から論じた [66].「ひとりの生まれ落ちた存在に対する拒みえない義務となる」として，乳飲み子とその親の関係を例にあげたうえで，乳飲み子が内在的にもつ存在当為（あるべし）を正当化する [66]．また「責任のありかとは，生成の海につかり，可視性に委ね渡され，消滅の脅威に震える存在である．乳飲み子はこのことを模範的に示している．責任は，ものごとを永遠の相のもとに見るのではなく，時間の相のもとに見なければならない [66]」とし，当為（べし）に対して，将来にわたる時間軸を加えた．

H.Jonas の世代間倫理においては，科学と技術を「後続する状態が先行する状態を常に凌駕するという点で　―中略―　唯一の永続的な反エントロピー運動であるかも知れない [66]」と表現したうえで，「両刃の剣 [66]」ととらえ，その進歩に伴うリスクの側面を注意深く

汲み取る．既に起こった，あるいは起こりつつある自然環境問題を踏まえ，「進歩自体が生み出す問題の解決のために新たな進歩が必要になるという進歩の弁証法は，いまや避けがたい[66]」という点を「未来への責任倫理にとって中心の問題である[66]」とし，「拡張主義から定常的（ホメオスタシス的）な関係を目指すものへと移行するだろう[66]」と，サスティナビリティの視点を意識する．

そしてさらに，科学技術によって得られる，まだ見ぬ未来にユートピアを重ねることに対して，「現在必要なのは事態を冷静に見据える目であり，ユートピア的幻想は，それを曇らせるだけである[66]」と強く非難する．

一方，ユートピア批判に対しては，「思考および意欲を訂正する試みとして，選択肢に影響することができる[66]」とし，「ベーコン以降，プロメテウスの流れをくむ多幸症　—中略—ギャロップで走る未来への全身に手綱を付けなければならない．　—中略—　．その限り未来への前進に手綱をつけるのは，われわれの子孫への純朴な礼儀であり，これと対をなす賢明な慎慮である[66]」と，科学技術によってもたらされる幸福な未来を楽観的な夢と位置づけ，それを盲信することで起こる問題を避ける選択肢の存在に気付くことを説く．

5.3 モバイル端末が創出するデータと未来への視点と仮説

我々にとって極めて身近で，かつ実感を得やすい，世代間倫理によって検討できる対象は，自然環境問題である．その中で我々がもっともイメージしやすい対象として挙げられるのはフクシマ問題である．東日本大震災とフクシマ問題を経験した我々にとって，原発が人の生命を脅かす大きなリスクであるという理解や警戒感は，災害発生以前と比べて，デモの頻度や大きさなどからも身近である．「現在の電気需要やそれに伴う利便性の追求によって，永き将来に渡って土地に居住できない状況や，最低数十年を超えるスパンでことに当たらなくては解決不可能な核汚染の問題を引き起こした」という現実は，いやがおうにも，世代を超えた倫理的配慮の意義を我々に突きつける．

データ収集・利活用もまた，現在を生きるものの利便性向上の追求という視点が存在し，未来に起こり得る破滅的リスクもまた存在しうる．しかし自然環境の破壊とそれに伴う将来に対するリスクが不可逆性を持ち，訪れるカタストロフのイメージが容易いのに対し，データ収集・利活用が損なう対象はプライバシーにおける“権利”という「失われた場合にどのようなことが起こるのか」というリスクのイメージが難しい点において大きく異なる．しかし，人間の基本的な権利は，「人間を人間たらしめる根源的なもの」であり，目に見えない財産が損なわれることで生じる負の側面は計り知れないほどに巨大である．

5.4 世代間倫理と生存権

5.4.1 フクシマ問題をケーススタディに生存権を検討する

フクシマ問題を振り返れば，そもそものスタート地点は，日本の経済成長に伴う電力需要に応えるとともに，地域を振興させたいという誘致運動である．

原発が各地に誘致された当時はもちろん，功利主義が浸透し，物質的に豊かな生活を目指す環境においては，リスクの算定がなされていようとも，便益を優先させる傾向が存在する．福島第一原子力発電所に関しても，誘致する過程で，税収の向上や商店の売上向上など，それぞれの利益を最大化させるため，誘致を歓迎し，最終的には，選挙で選ばれた市長が東京電力本社へ発電所の増設誘致の願いを申し出るまでになっており，災害が起こる前に歯止めを利かせるのは現実的には困難であったことからも明らかである．

典型的な功利主義のモデルによれば，全体の幸福をより増大させるために，一部の人々の利益をある程度は犠牲にしなければならない． しかし，R.Nozick によれば，「自分自身の利益のために何らかの犠牲に耐える，社会的実体は存在しない[67]」．個人には，侵害されることのない自然法的な権利が存在し，それは犯されるべきではないという立場である．そして自然法には，生命の存続が絶対的な背景として存在する．

S.Frechette と同じく，J.Rawls の原初状態の概念から検討した場合[63]，生存権は未来においても自明の権利として守られるべきものと考えられる．

5.4.2 生存権と自由権，位置情報とプライバシー権

さて，「生」が倫理における形而上学的な正義であるのと同様に，自由権もまた J.S.Mill を始めとする自由主義[68]の観点から正当化可能である．そしてプライバシー権は初期において「放っておかれる権利」であり，人間そのものが独立した「個」であることを守るための権利であった．なるほど，この観点からプライバシー権を検討した場合，プライバシーは自由権と近しい関係にあると考えられる．

しかし，パーソナルデータの収集・利活用を通じて起こる個人の特定やプライバシー権の侵害は，2.3.4 で論じたように，その人の位置情報を把握したうえで危害を加えるなどのストーカー行為のリスクなど，プライバシーの侵害が生命の危機リスクを増大させる一因となり得る．本論における調査でも明らかなように「位置情報」，つまり居場所に関するパーソナルデータをプライバシーに関連付ける理由は，気持ち悪さだけでなく，実害をイメージしやすいからである．

つまり，モバイル端末におけるデータの収集・利活用に関するプライバシー権は，端末が生み出す「位置情報」という，データを個人の居場所を物理的に特定可能なデータによって，生存権の要素を強く得るに至ったのである．

そして，個人を不必要に特定することで命の危機が訪れる可能性があるという「生命的リスク」がプライバシーの制限にリンクすることで，我々が安全に暮らすという大義のもとに正当化される自然環境を巡る倫理的配慮の論考を適用可能となる．

しかし，原発問題などの自然環境に関連した生存権の保護をデータ収集・利活用を巡る生存権の問題に当てはめる場合，我々に影響を与える仕組みが多少異なるため注意が必要である．自然環境問題は，文字通り，我々が生きるための環境に対する問題であるため，その破壊は，放射能汚染や大気汚染など，我々の健康や生死に直結する．対して，データの収集・利活用を巡るプライバシー問題は，「データの提供・利活用」により「プライバシーが制限」され，個人が特定できた場合，他者から危害を加えられるリスクが増加するなどの「生命の危機」が生じる可能性があるという 3 段階を経て生存権へと至るため，自然環境の破壊が我々に危機を一直線にもたらすことに比べ，生存が脅かされることに関するリスクの算定が困難である．

しかし裏を返せば,「データ収集･利活用によって何が起こるのか分からない」のであり，しかし行きつく先に「生命の危機」がイメージできる以上は，我々が怖れの感情を抱いて当然であり，プライバシーが制限されて当然な世界を将来の世代に対してバトンタッチすることに我々が不安を覚え，策を講じようとすることに異論は生じない．

このように，データの収集・利活用時代におけるプライバシー権は，古典的なプライバシー権の出発地点である自由権に加えて，生存権の色も帯びている．ふたつの権利の領域にプライバシー権がまたがることで，プライバシー権をサポートする根拠は強固となる．

そしてプライバシー権が複数の人権に対して影響を持つものへの変化を遂げた以上，人々がプライバシー権の制限を受けることに強い懸念を表す，あるいは次世代に残すべき大切な権利だと今まで以上に自覚したとしても不思議ではない．ましてや，コンピュータテクノロジーの急速な発展や，モバイル端末の普及，データ収集・利活用がホットな話題とされる時代においては，プライバシー権に向き合い，将来へ思いを巡らせたり，危機感を募らせたりする人々が存在することは極めて自然なことである．

5.4.3 世代間倫理と人間の権利

世代間倫理が「将来に対して現世代に生きる我々が配慮すること」を正当化するのであれば，その対象は「自然環境」を巡る配慮を形作る倫理的視点に限らない．人間という種に対しての配慮を将来に向けるのであれば，人間が生きるための物理的環境（地球）だけでなく，人間が生来持つ「権利」もまた未来の世代に対して残すべきものであり，倫理的に検討すべき課題となりえる．

プライバシー権は，人間にとって自明の権利であることに加え，科学技術を伴って複数の権利に跨り，大きな権利となった現在，守られるべきとする価値は技術の発展によって強く浮き彫りとなった．そして技術によって初めて我々に突きつけられたプライバシー権

の重要性から，我々が目を背けるのは，現世代における権利の放棄だけでなく，慣習や法令を通じて将来の世代のプライバシー権を制限することになる．現世代に生きる我々は，将来の人々が我々と同様，もしくはそれ以上に幸福であるべきであり，将来における幸福は人間を人間たらしめる権利があってこそなしえる．

5.4.4 「諦め」の感情と世代間倫理

再びフクシマ問題に戻る．原発の誘致が成功した背景には，R.Nozick の立場を引き受ければ，核汚染という，多大なる犠牲が生じるリスクがあったにも関わらず社会はそれを渋々認めたという「歪み」のうえに存在したものと考えられる．そのような社会の歪みは，リスクに怯えつつも提案された便益を受け入れたことによって生まれ，データを巡る「諦め」の感情と同様の状態に陥った個人の集合に起因すると換言できる．両者を原初状態から検討すれば，フクシマと，データ収集・利活用は，ともに権利の尊重から反対意見を露わにする人々が存在するはずである．

一旦形成された世論や社会制度，慣例は，カタストロフ（例：原発における重大事故など）が起きない限り，短期間で見直される可能性は著しく低い．こうした可能性の低さはフクシマ問題の経緯を知る我々にとってイメージしやすいものである．そしてカタストロフが起きてからでは遅いことも我々は経験している．

便益に押しきられる形で「諦め」の感情の末に行われた決断内容は，将来にわたって影響を及ぼし，世代を超えてもなお，それらは影響を及ぼし，次世代における権利を剥奪する．ましてや，社会が合意形成するなかで，「諦め」の感情を抱く層が少数派である場合，多数決の政治的慣例から，その声はかき消され，カタストロフが起こってから「やっぱりあの時の不安が的中した」と悔やむことになる．反対に，カタストロフが起きなかったとしても，日々の生活の中で，便益を享受しながらも何時までも不安感に苛まれる可能性がある．

データの収集・利活用の場合におけるプライバシー問題に対して，「諦めグループ」に属する人々は，サービス利用の当事者でありながら，プライバシー制限のリスクを日々感じている．したがって，そのサービスに伴うデータ収集・利活用に対するリスクを一歩引いた視点から，より客観的に捉えることが可能となる．

「諦め」の感情によってなされた決断が将来に渡って影響を及ぼすのであれば，リスクから導き出された「将来の世代に対して何を配慮すればよいのか」という問いの答えもまた，「諦め」の感情を持つ人々から得られる．データ収集・利活用のプライバシー問題においては，「諦めグループ」が感じる「プライバシーの制限が巻き起こすリスク」を汲み取り，将来を見据えたデータ収集・利活用の注意点，すなわち世代間倫理の射程から検討した，データ収集・利活用におけるプライバシー問題を解決するための施策が見えてくるのである．

5.4.5 将来を見据えたデータ利活用の倫理と，形の見えないカタストロフ

フクシマ問題からも明らかなように，「起こってからでは遅い」というリスクを抱える問題に関しては，目先の経済的利益や一時的な豊かさを優先するのではなく，最悪のシナリオに思惑を巡らせ，リスクをステイクホルダー全員で共有して判断する必要がある．そしてその判断は，原初状態においてなされるべきである．

モバイル端末におけるプライバシー問題やデータ利活用に関しては，国民のほぼすべてがステイクホルダーとなりうる．加えて，何が起こるか分からないどころか，これからどんな技術やビジネスが登場するかすら想像が及ばない．甘言としての「豊かさ」や利便性の向上を受け入れた先に，誰かの身，あるいは我々すべてにふりかかるかも知れぬカタストロフに関するリスクを我々は理解しているだろうか.「諦めグループ」がサービスの渦中に居ながらも感じるリスクこそが，最悪のシナリオであり，我々が「もっとも避けるべきもの」である．この点において，我々は科学技術に対して楽観的な視点から離れて疑いの目を向けるべきであり，E.Ewald における「持続可能かつ，科学を好意的に受け止める姿勢」と決別することを本論では強調したい.

コンピュータやウェラブルデバイス，処理速度やデータ転送速度などの，データの生成・処理を取り巻く状況が恐るべき速度で向上する現実の先に待ち受けるのがユートピアであるとは限らないのである．データを巡るプライバシー問題は，既存の自然環境問題における，人間と自然，命を巡る問題を超越する．有史以来，人間が人間の知能を超えるものを初めて生み出しつつあり，機械学習や統計処理と共にあるデータ収集と利活用は，我々が自ら生み出した新たな環境によって，生殺与奪を含め，あらゆる面において，我々が支配されるリスクを示唆できるのである．その点において，データを巡る施策に対して，楽観的な視点を持つことは極めて危険であり，それが利便性という甘い蜜や，我々の生活環境によってそうせざるを得ない状況（そのサービスが無くては生活に大きく支障をきたす）という，ある種の中毒とも表現できる状況の帰結として現れたものであることが確認された以上，色眼鏡を外し，リスクを今一度正視しなくてはならないのである.

5.5 世代間倫理から検討する，データの収集・利活用のプライバシー問題の解決手法

筆者が行った調査によって得られた，データ収集・利活用に対するプライバシー制限に関する「諦めグループ」は，サービス利用の当事者でありながら将来を憂う視点を持ちあわせる．現在における「これではいけない」という不安感が向けられる対象は，慣習や基

準となり（つつあり），「“このまま”ではいけない」という，将来に対する不安感を内包する．

そして，世代間倫理の射程は，自然環境を巡る科学技術だけでなく，人間の権利をめぐる環境に拡張できる可能性を先に示した．したがって，明確に時間軸を備える「諦めグループ」に対して，世代間倫理からの検討が可能となる．

「未来のために現在を汚したり，現在を犠牲に未来を買おうとしたりしないよう，われわれを守ってくれるのは畏敬だけであろう．だが，おそれのあまりに，本来の目的――人間性を委縮させずに人間を生長させること　―中略―　この目的を手段によってぶち壊してしまうことが許されない[66]」ため，我々やデータ収集・利活用の主体は，諦めのグループが発する怖れや違和感を可能な限り汲み取り，表面的な全肯定に驕ることなく，現時点の選択がもたらす直近の未来だけでなく，遠い将来に影響を及ぼすことを自覚するべきである．また，諦めのグループが積極的な意見を臆することなく表明できるよう，討議の場を積極的に用意することが，既にブレーキを掛けることが難しい，データを巡る施策の発展に不可欠である．具体的には，ユーザーがセンシティブなパーソナルデータと捉えるデータの取扱いに対して特に注意を払うほか，「諦めグループ」が活用できていない，サービス利用時の利用規約をデータ収集・利活用の主体とユーザーの「討議の場」として捉え，改善し，データの収集・利活用に関する指針を明確に提示することが肝要である．調査からも明らかなように，プライバシーに関する意識を持ちつつも，パーソナルデータの取扱い指針を示す利用規約が活用されておらず，サービスの環境的価値が利用規約の活用に対するインセンティブを無力化する．「本当は嫌だけど」のプライバシー制限に対する，利用規約を凌駕する感情は，ひとたび火が付けば，猛烈なサービスに対する反対意見へと姿を変え，データの収集・利活用を妨げ，サービスそのものへの不信感へと繋がる．また，昨今において特に収集と利活用が叫ばれる「位置情報」が特にモバイル端末が創出するパーソナルデータの中でもセンシティブなものであると認識し，その利活用が現世代を生きる者へ不安を与えるだけでなく，将来の世代に対しても，影を落とす可能性を考慮しなくてはならない．そのうえで，位置情報に重きを置きつつも，その他に関しても，データの収集・利活用を行う団体が，ユーザーに寄り添う姿勢を見せることで，現在・将来を通じてプライバシー問題を防止できる可能性が高まるのである．

VI　結論

6.1 結論

スマートフォンを始めとするモバイル端末の普及や付帯するセンサーの多様化，および取得できるデータが多岐に渡るという背景と，データマイニング技術の向上により，パーソナルデータの利活用が叫ばれている．しかし，ハードウェアや利活用のためのマイニング技術，匿名化技術が向上の一途をたどっているにも関わらず，依然としてパーソナルデータとプライバシーを巡る対立フィールドは解消されない．データ利活用は，単なる私企業の利益に寄与するばかりでなく，防災や効率的社会の実現など，公益の視点からも大きな期待が寄せられている．このため，プライバシーの軋轢を生まないデータの収集と利活用の方法を検討することは極めて重要である．そして技術と人間そのものが対立する，データを巡るプライバシーを理解するうえでは，学際的な研究手法を避けて通れない．

そのため，本研究では，実際に起こったデータとプライバシーを巡る問題の事例から問題発生の源泉を探る営みから研究を開始し，人間が抱えるプライバシー意識の根の部分を掘り起こす目的で質的調査手法を用いて，既存研究が提示するプライバシー観の分類の再検討を行った．

2 章では，データ収集と利活用の例，プライバシー権を巡る議論，プライバシー保護技術を紹介したうえで，データ収集と利活用の環境において，問題解決に至る決定的なプライバシー権を定義する議論や，完全な匿名化を成しえる技術が不在であること，プライバシーが感情によって左右されうる側面を持つことを示した．次に 3 章，プライバシーに関連したユーザースタディを紹介し，社会学的手法によりユーザーの感情を捉える議論の必要性を示すと共に，A.Westin によるプライバシー3 分類の見直しを仮説として挙げた．続く 4 章では，質的調査と KJ 法を用いて，A.Westin が提唱した「原則型グループ」「解放型グループ」「選択型グループ」から成るプライバシー3 分類のうち，「選択型グループ」を「納得型グループ」と「諦めグループ」に中分類できることを示し，両者の差異が，行動の背景にもつ感情の正負であることを明らかにした．そのうえで，ウェブアンケート手法を用いた量的調査を実施し，「諦めグループ」の背景に存在する要因を深掘りして，データ収集・利活用の勘所を探った．「住所」「クレジットカード情報」「氏名」「位置情報」が特にセンシティブなパーソナルデータと考えられているほか，利用規約が活用されていない現状が明らかになった．したがって，センシティブなパーソナルデータを収集・利活用する際には，分かりやすく要点をまとめた利用規約をユーザーに提示することが効果的と考えられるほか，特に様々なアプリケーションと共に利活用が期待されている位置情報の取得・利活用に際しては注意が必要であり，位置情報に近しい関係と考えられる移動情報も同様の注意が必要である．4 章を通して，3.3 で挙げた A.Westin によるプライバシー3 分類の見直しに関する仮説が実証された．

5 章では，モバイル端末が生み出すデータの収集・利活用に関連するプライバシー権がその他の権利と同様に重要であることを説き，権利の放棄や収奪が未来に渡って継承されることと，それがプライバシー権においても同様であることを示した．その後，「諦めグループ」が，「データ収集・利活用を通じて起こるプライバシーに関する否定的な感覚を抱いていながらも，サービスを利用する当事者」であることから「プライバシーが制限されることで起こる，リアルなリスク」を認識していることに触れた．サービスを利用する当事者でありながらも疑念を抱く「諦めグループ」が持つ問題意識は，プライバシー問題を解決するためのプラグマティックなツールとなるばかりか，バンドワゴン効果 [69] によっておこるバイアスに陥りやすい，データ収集・利活用主体，および「開放型グループ」「納得型グループ」が考えるデータによって実現する（であろう）ユートピアの盲信に対して中立的な視点を提供する．そしてそれは，漠然とした将来のリスク検討であるだけでなく，すべての者にとって当事者となりうる，自然権の一部を将来に渡って担保することにリンクし，現在の我々が持ち，将来の子孫にとっての遺産となりうる権利の継承へ向けた営みなのである．

また，データ収集・利活用を円滑に進めるというプラグマティックな目的を睨んで本論を検討した場合，サービスを提供，あるいは運営する主体は，「そのサービス自体の利便性や有用性を認めているものの，データの収集や利活用に対して嫌悪感を抱いているユーザー」が存在する可能性を理解するのが肝要である．そうしたグループは，一見すれば，すべてを納得してサービスを利用しているように見えてもデータ収集や利活用に負の感情を抱いているため，切欠さえあれば，一気に“炎上”の火種となり得るのである．“炎上”を未然に防ぎ，データの収集と利活用を円滑に進めるためには，「諦め」のグループのボリュームを見定め，彼らが抱えるデータを巡るマイナスの感情を理解し，不用意に煽り立てない施策の実行が求められる．そして，「位置情報」が“もっとも燃えやすい”パーソナルデータであり，取扱いには一層の注意が求められる．

そしてさらに，「データの収集・利活用に対して，必ずしも明るい未来のみを思い描く者ばかりではない」と念頭においたうえで，プライバシー権は我々が生来持つ権利であると同時に，未来へと受け継ぐべきものであることを忘れてはならず，現時点におけるひとつひとつのサービスや利活用の施策によって未来は作り出される．

微力ながらも，本研究が「先人樹を植えて，後人その下に憩う」の未来の実現に至るさざれ石となることを切に願う．

6.2 今後に向けた検討課題

本論を通して明らかになった今後へ向けた検討課題は以下の 3 点である．

1)

本論内のふたつの本調査によって得られるプライバシー観の分類は，個人がその環境に

応じて主観的に抱く傾向であり，サービスやその状況に応じて，分類枠を行き来すると考えられるが，その移動に関する認識分析は本研究に付帯する調査データからは不可能である．

2)

個々の「プライバシーが気になるデータ」に関して，「なぜその情報が流出，あるいは収集・利活用されると嫌な気持ちになるのか」という，パーソナルデータの種類ごとに生じる感情の整理を行う必要がある．

3)

量的調査を通して，パーソナルデータが「住所や氏名などの固有のパーソナルデータ」と「位置情報や検索履歴などのモバイル端末によって新たに生み出されるもの」に分けられた．それぞれのグループによって，ユーザーが求めるプライバシー保護への対応や，持ちうる感情が異なる可能性があるため，ユーザーが考えるパーソナルデータのグループごとに，さらなる調査の必要性が示唆される．

謝辞

本研究に関する多大なる指導とご鞭撻を頂戴したばかりでなく，研究に対する真摯な姿勢のありかたや，成果の発表方法，準備の重要さなどを学ばせて頂いたとともに，常に暖かく見守っていただきました，指導教員である東京大学空間情報科学研究センター 瀬崎薫教授，副指導教員を引き受けてくださいました東京大学大学院新領域創成科学研究科 木實新一准教授，副査を引き受けてくださいました東京大学大学院新領域創成科学研究科 清水亮教授，東京大学生産技術研究所附属ソシオグローバル情報工学研究センター 伊藤昌毅助教，東京大学空間情報科学研究センター小林博樹助教に深い感謝の意を表します．また，多くの助言を賜りました，東京大学大学院新領域創成科学研究科 福永真弓准教授，鬼頭秀一東京大学名誉教授，東京電機大学未来科学部岩井将行准教授にここに御礼申し上げます．

日本社会学会への推薦で大変お世話になりました，東京大学大学院情報学環・学際情報学府山口いつ子教授，東京大学大学院情報学環・学際情報学府 准教授三谷武司准教授に深く感謝いたします．

先輩であり，研究に対する姿勢を学ばせて頂いた，青木俊介氏，Asif Hossain Khan 氏，中川慶次郎氏，木田裕一朗氏， José Pablo Álvarez Lacasia 氏，Congwei Dang 氏，劉広文氏，Niu Hao 氏，Dunstan Matekenya 氏，江甜甜氏，孫堯氏，中山悠氏，公私に渡って仲良くして頂きました坂本敬太氏，中村直人氏，稲葉瞳氏，また研究室のメンバーとして常に刺激を頂きました森英記氏，牧山紘氏，松野有弥氏，山本直人氏，鵜飼祐太氏，星野光玖氏，鈴木孝男氏，西井香織氏，合間優陽氏，学会参加や研究室の環境の面において支えて頂きました秘書の松本夏穂氏，内藤潤氏に感謝の言葉を申し上げます．

本研究に関連する社会調査の一部は，NICT-情報通信研究機構による，研究助成によって行われました．本研究に対する意義を認めて頂き心から感謝いたします．また，本研究の実施に伴い，社会調査に協力してくださった皆さまに深く感謝します．

最後になりますが，常に暖かく見守って頂いた祖母と母，大学院入学の後押しをしてくれた優に心から深く感謝し，本論文を締めくくりたいと思います．

発表文献

■加藤宗肖, 伊藤昌毅, 清水亮, 木實新一, 瀬崎薫, "モバイル端末が創出する位置情報の利用に対するユーザー意識の質的調査, " マルチメディア, 分散, 協調とモバイル(DICOMO2014)シンポジウム, 2014 年 7 月

■加藤宗肖, 鵜飼祐太, 瀬崎薫, "モバイル端末ユーザーのプライバシー意識に関する調査から, 企業とユーザーの権力構造を検討する, " 第 87 回日本社会学会大会, 2014 年 11 月

■加藤宗肖, 青木俊介, 伊藤昌毅, 瀬崎薫, "モバイル端末が創出するパーソナルデータの利活用にかかる意識調査を世代間倫理の射程から検討する, " 電子情報通信学会大会, 2015 年 3 月

参考文献

1. De Vera J, 粕谷源蔵. マーシャル・マクルーハン著 「メディアの理解--人間拡張の原理」(marshall McLuhan; understanding media--the extensions of man. 1964). コミュニケ-ション研究. 1968(2):123-128.

2. Narrative, this week in lifelogging: Sharing our lives with wearable tech, owlet baby monitor and sesame ring , http://Blog.getnarrative.com/2013/08/this-week-in-lifelogging-sharing-wearable-tech-owlet-baby-monitor-sesame-ring/.

3. Davis K. Ethics of big data: Balancing risk and innovation. 2012.

4. Goodman E. Design and ethics in the era of big data. interactions. 2014;21(3):22-24.

5. 平成 24 年版 情報通信白書, 第 1 部, 特集 ICT が導く震災復興・日本再生の道筋, http://Www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/html/nc121410.html.

6. 鈴木良介. ビッグデータビジネスの時代. 2012.

7. Manyika J, Chui M, Brown B, et al. Big data: The next frontier for innovation, competition, and productivity. 2011.

8. 総務省, パーソナルデータの利用・流通に関する研究会報告書, http://Www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000071.html.

9. 生貝直人. オンライン・プライバシーと自主規制—欧米における行動ターゲティング広告への対応. 情報通信学会誌. 2010;28(3):105-113.

10. ITmedia ビジネス, Suica 利用履歴販売, JR 東は「個人情報に当たらない」との見解, http://Bizmakoto.jp/makoto/articles/1307/19/news141.html.

11. Sweeney L. K-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. 2002;10(05):557-570.

12. ITpro, 「Suica 履歴販売」は何を誤ったのか,

http://Itpro.nikkeibp.co.jp/article/NC/20131010/510322/.

13. JR 東日本, suica に関するデータの社外への提供について, http://Www.jreast.co.jp/chukantorimatome/20140320.pdf.

14. モバイル空間統計に関する情報 | 企業情報 | NTT ドコモ, https://Www.nttdocomo.co.jp/corporate/disclosure/mobile_spatial_statistics/.

15. ケータイ Watch, 第 629 回：モバイル空間統計とは , http://K-tai.impress.co.jp/docs/column/keyword/20130910_614763.html.

16. MarkeZine, 匿名データのはずが…日米の事件を振り返り, プライバシー対策を考える, http://Markezine.jp/article/detail/19373.

17. Before the federal trade commission washington, DC 20580, http://Www.worldprivacyforum.org/wp-content/uploads/2008/08/WPF_FTCcomplaint8162006fswp.pdf.

18. Narayanan A, Shmatikov V. Robust de-anonymization of large sparse datasets. 2008:111-125.

19. Forbes, netflix settles privacy lawsuit, cancels prize sequel, http://Www.forbes.com/sites/firewall/2010/03/12/netflix-settles-privacy-suit-cancels-netflix-prize-two-sequel/. 2010.3.10.

20. Ars technica, “Anonymized” data really isn’t—and here’s why not, http://Arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/.

21. Nature, 匿名化されたクレジットカード利用履歴から個人を特定, http://Www.natureasia.com/ja-jp/ndigest/v12/n4/匿名化されたクレジットカード利用履歴から個人を特定/61964.

22. Warren SD, Brandeis LD. The right to privacy. Harv Law Rev. 1890:193-220.

23. Shank R. Privacy: History, legal, social, and ethical aspects. Library Trends.

1986;35(1):7-18.

24. Ely JH. The wages of crying wolf: A comment on roe v. wade. Yale Law J. 1973:920-949.

25. Bigel AI. Planned parenthood of southeastern pennsylvania v. casey: Constitutional principles and political turbulence. U.Dayton L.Rev. 1992;18:733.

26. Westin AF. Privacy and freedom. 1970.

27. Schaller RR. Moore's law: Past, present and future. Spectrum, IEEE. 19 97;34(6):52-59.

28. Miller AA. The assault on privacy. Psychiatric Opinion. 1975.

29. Bumham D. The rise of the computer state. London: Weidenfeld and Nicolson. 1983.

30. Regan PM. Legislating privacy: Technology, social values, and public policy. Univ of North Carolina Press; 1995.

31. Kargupta H, Datta S, Wang Q, Sivakumar K. On the privacy preserving properties of random data perturbation techniques. 2003:99-106.

32. Nissenbaum H. Privacy in context: Technology, policy, and the integrity of social life. 2009.

33. Solove DJ. A taxonomy of privacy. University of Pennsylvania law review. 2006:477-564.

34. Chan H, Perrig A. Security and privacy in sensor networks. Computer. 2003;36(10):103-105.

35. Li N, Li T, Venkatasubramanian S. T-closeness: Privacy beyond k-anonymity and l-diversity. 2007:106-115.

36. Sweeney L. K-anonymity: A model for protecting privacy. International Journal of

Uncertainty, Fuzziness and Knowledge-Based Systems. 2002;10(05):557-570.

37. IPA 独立行政法人 情報処理推進機構, パーソナル情報保護と IT 技術に関する調査 -調査報告書-. 2012.08.

38. Gedik B, Liu L. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. Mobile Computing, IEEE Transactions on. 2008;7(1):1-18.

39. Shao M, Yang Y, Zhu S, Cao G. Towards statistically strong source anonymity for sensor networks. 2008.

40. 青木俊介. 参加型センシングのプライバシー保護手法. 2014.

41. 村本俊祐, 上土井陽子, 若林真一. プライバシ保護データ公開に向けた l-多様化適性の評価（データベース vol. 4 no. 2). 情報処理学会論文誌 論文誌トランザクション. 2011;2011(1):126-141.

42. 理化学研究所, 荒井ひろみ, 情報開示におけるプライバシー保護, http://Www.slideshare.net/AraiHiromi/ppdm. 2014.02.

43. 筑波大学大学院 ビジネス科学研究科 経営システム科学専攻 泉 晃, パーソナルデータ活用におけるプライバシー保護データマイニング(PPDM)の適用, http://Www.slideshare.net/AkiraIzumi1/ppdm-43421567. 2014.11.20.

44. Lu H, Jensen CS, Yiu ML. Pad: Privacy-area aware, dummy-based location privacy in mobile services. 2008:16-23.

45. 加藤 諒, 松野 有弥, 原 隆浩, 荒瀬 由紀, Xing Xie, 西尾 章治郎. ユーザの訪問場所の傾向を考慮したダミーによるユーザ位置曖昧化手法. 情報処理学会マルチメディア, 分散, 協調とモバイル(DICOMO2014)シンポジウム論文集. 2014.7:1174-1181.

46. 国立情報学研究所. 匿名化技術の最新動向と その課題. NII Today. 2014;No.64.

47. @IT, プライバシー保護データマイニング（PPDM）手法の種類，特徴を理解する, http://Www.atmarkit.co.jp/ait/articles/1503/24/news010.html. 2015.03.24.

48. NICT-情報通信研究機構, “暗号化状態でセキュリティレベルの更新と演算の両方ができる準同型暗号方式を開発”, http://Www.nict.go.jp/press/2015/01/19-1.html. 2015.01.19.

49. NTT セキュアプラットフォーム研究所, “秘密計算”, http://Www.seclab.ecl.ntt.co.jp/project/secure-management/secure-computation.html.

50. Kumaraguru P, Cranor LF. Privacy indexes: A survey of westin's studies. 2005.

51. ジャパン プライバシー センター (JPC), http://Www.excellent-privacy.com/exprivacy/afw_p.html.

52. 総務省, “位置情報の利用に対する意識調査”, http://Www.soumu.go.jp/iicp/chousakenkyu/data/research/survey/telecom/2014/location-info.pdf. 2014.05.

53. IPA セキュリティセンター, eID に関するリスク認知と受容の調査, 2010.

54. Cvrcek D, Kumpost M, Matyas V, Danezis G. A study on the value of location privacy. 2006:109-118.

55. Sheehan KB. Toward a typology of internet users and online privacy concerns. The Information Society. 2002;18(1):21-32.

56. Phelps J, Nowak G, Ferrell E. Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing. 2000;19(1):27-41.

57. Milne GR, Culnan MJ. Strategies for reducing online privacy risks: Why consumers read (or don’t read) online privacy notices. Journal of Interactive Marketing. 2004;18(3):15-29.

58. Armstrong D, Kline-Rogers E, Jani SM, et al. Potential impact of the HIPAA privacy rule on data collection in a registry of patients with acute coronary syndrome. Arch Intern Med. 2005;165(10):1125-1129.

59. 川喜田二郎. 発想法: KJ 法の展開と応用. 続. 中央公論社; 1970.

60. 後藤 淳子. 早稲田大学大学院スポーツ科学研究科, “東京都における車いすテニスレッスンの 普及に関する研究”. 2012.

61. 石田浩, 佐藤香, 佐藤博樹, et al. 信頼できるインターネット調査法の確立に向けて. SSJDA: RPS. 2009.

62. Shrader-Frechette KS, McCoy ED. Method in ecology: Strategies for conservation. Cambridge University Press; 1993.

63. Rawls J. Political liberalism. Columbia University Press; 2005.

64. Alverson R, Callahan D, Cummings D, Koblenz B, Porterfield A, Smith B. The tera computer system. ACM SIGARCH Computer Architecture News. 1990;18(3b):1-6.

65. Jonas H. Das prinzip verantwortung: Versuch einer ethik für die technologische zivilisation (frankfurt a. M.: Suhrkamp, 1984), 7. 責任という原理: 科学技術文明のための倫理学の試み』, 東信堂, 2000.

66. Nozick R. Anarchy, state, and utopia. Vol 5038. Basic books; 1974.

67. Mill JS, Alexander E. On liberty. Broadview Press; 1999.

68. 北川高嗣, 須藤修, 西垣通. 情報学事典. Kōbundō; 2002.

付録

■質的調査における質問項目一覧

1. 年齢

2. 性別

3. 年収

4. あなたはスマートフォンを所有していますか？
「はい」「いいえ」

5. [4.で「はい」を選んだ人に] あなたはスマートフォンを利用している際に，プライバシーに関する不安を感じたことはありますか？
「はい」「いいえ」

6. [5.で「はい」を選んだ人に]以下のどの項目に関してプライバシーの不安を感じましたか？
「年齢の入力」「氏名の入力」「住所の入力」「性別の入力」「年収の入力」「検索履歴の取得」「位置情報の取得」「会話内容の履歴」「電話帳データ」「クレジットカード情報の入力」「その他（自由記述）」
（複数選択可能）

7. あなたは，プライバシーに関する不安を感じながら，アプリケーション（アプリ）やウェブサービスを利用した経験はありますか？
「はい」「いいえ」

8. [7.で「はい」を選んだ人に]それはどんなアプリケーション（アプリ）やウェブサービスでしたか？
「ゲーム」「メッセージアプリ」「メール」「SNS」「地図」「EC（買い物）」「ニュース」「その他（自由記述）」
（複数選択可能）

9. [7.で「はい」を選んだ人に]プライバシーの不安を感じながらも，アプリケーション（アプリ）やサービスを利用した理由を以下の中から選択してください.
「自分の周囲がそのアプリケーションを使っているから」「便利だから」「それが無いと不

便だから」「その他（自由記述)」
（複数選択可能）

10. あなたはアプリケーション（アプリ）やウェブサービスを利用する際に，利用規約を読みますか？
「いつも読む」「ときどき読む」「あまり読まない」「いつも読まない」

11. [11.で「ときどき読む」「あまり読まない」「いつも読まない」を選んだ人に]利用規約を読まない理由を以下の中から選択してください.
「長い」「書いてあることが難しい」「読まなくてもどうせアプリケーション（アプリ）・サービス使う」「その他（自由記述)」

12. 利用規約のうち，気になる部分を選択してください.
「料金やお金に関すること」「サービスの中止・休止に関すること」「禁止事項」「規約の変更」「利用資格」「サービス内容」「個人情報の取扱い方針」「オプトアウト（不要なメールの拒否や，個人情報の提供を拒否すること）の方法」「その他（自由記述)」
（複数選択可能）