

2016 年度 中野香織ゼミ卒業論文

2016 年度 卒業論文

ライフログ拡大社会における
プライバシーの意識調査

駒澤大学経営学部市場戦略学科

中井 舜

目次

はじめに

第1章 プライバシー登場の背景

第1節 第1期 伝統的プライバシー権の発展期(1890年～1960年頃)

第2節 第2期 現代的プライバシー権・法と経済学の提唱期(1960年代後半～1980年頃)

第3節 第3期 情報プライバシーとサイバースペース論議の発展期(1990年代後半～2000年代半ば頃)

第2章 プライバシーについて

第1節 プライバシーの定義

第2節 プライバシーの範囲

第1項 計数される消費者

第2項 ライフログ

第3項 電子マネー

第4項 監視カメラ・人の移動履歴

第3章 ビッグデータについて

第1節 ビッグデータ登場の背景

第2節 ビッグデータの定義

第4章 仮説と検証

第1節 仮説

第2節 調査概要

第3節 検証結果

第5章 研究の考察と提案

第1節 結果考察

第2節 まとめ

参考文献

はじめに（研究背景、目的？）

昨今のマーケティング、主にリサーチ分野において、ICT(Internet and Communication Technology)分野の発達に伴い、ビッグデータを有効活用する動きが活発化している。消費者個人の消費動向を把握することは、マーケティングにおいて重要な役割を持っているからだ。

現状、インターネット上の履歴や、SNS の情報、ポイントカードや磁気カード等を利用した商品の購入情報等、消費者のプライベート情報が取得されており、その範囲は拡大している。

今後、IoT (Internet of Things)の普及、ビッグデータの発展などにより、この傾向は加速度的に強まることが予想される。

消費者の行動を企業が消費者の「逆トレーサビリティ」をビッグデータをとって把握、理解することで、より良い製品、サービスを消費者に提供できることであろう。

その一方で、ビッグデータは消費者のプライベート情報そのものと言ってもよい、非常にデリケートなものも含まれている。その扱い方を誤れば、消費者の反感を買うことも十分にあり得る。実際、個人情報漏洩をはじめとする企業の不祥事が後を絶たない。

本論文では、消費者の企業によるビッグデータ活用におけるプライバシーに関する意識の調査を目的とする。

第1章 プライバシー登場の背景

石井(2012)は、プライバシー権の提唱国であるアメリカ合衆国におけるプライバシー権の歴史的発展過程を「第 1 期 伝統的プライバシー権の発展期(1890 年～1960 年頃)」、「第 2 期 現代的プライバシー権・法と経済学の提唱期(1960 年代後半～1980 年頃)」、「第 3 期 情報プライバシーとサイバースペース論議 の発展期(1990 年代後半～2000 年代半ば頃)」の 3 期に区分している。本章では、石井の論文を要約したものを紹介する。

第 1 節 第 1 期 伝統的プライバシー権の発展期(1890 年～1960 年頃)

人間のプライバシーにおける権利は、1980 年に Samuel Warren と Louis Brandeis が著した「The Right to Privacy」においてその礎を築くこととなった。同論文は、個人のプライバシーを、「ひとりにしておいてもらう権利」(the right to be let alone)として提唱した。

20 世紀に入ると、多数のプライバシー侵害訴訟が提起された。それを不法行為の観点から分類・整理し直したのが、ウィリアム・L・プロッサーである。プロッサーは、1960 年に「プライバシー」と題する著名な論文を掲載した。諸判決を分析したプロッサーの 4 類型(「不法侵入」、「私的事実の公開」、「公衆の誤認」、「盗用」)は、第 2 次不法行為リステイメントに取り入れられた。

第 2 節 第 2 期 現代的プライバシー権・法と経済学の提唱期(1960 年代後半～1980 年頃)

1960 年代中盤に差し掛かると、特にコンピュータ化との関係で、新たなプライバシー問題へと関心が寄せられるようになった。このような事態への対応に大きな影響を与えたのは、現代的プライバシー権であると石井は述べている。この概念は、ウェスティンの『プライバシーと自由』(1967 年)、ミラーの『プライバシーへの攻撃』(1971 年)によって世界的に有名になった。ウェスティンによれば、「プライバシーとは、個人、グループまたは組織が、自己に関する情報を、いつ、どのように、また、どの程度他人に伝えるかを自ら決定できる権利」であるという。また、ウェスティンは個人情報を個人的な人格を決定する権利として考えた場合、それを財産権として定義するべきだとも述べた。

このウェスティンの主張に対し、ミラーは『プライバシーへの攻撃』の中で次のように批判した。財産権論として定義する意義として、情報が乱用された際の提訴権をデータ主体に付与することである。しかし、財産権論は、ウォレン&ブランダイスの初期の議論ですでに不適切として退けられている。また、商業上で価値のあるリストを作り出すのは、データ主体ではなく第三者としての企業であるため、データ主体に財産権を認める裏付けがない。

第3節 第3期 情報プライバシーとサイバースペース論議の発展期(1990年代後半～2000年代半ば頃)

第3期の議論は、「情報プライバシー」に「財産権」を認めることが可能かどうかを中心だった。情報を「所有」という発想が出てきたのはこの時代に入ってからである。

プライバシー・個人情報の財産権論の利点としては、第一に社会的費用の内部化、第二に、個人への選考の機会の付与という二点である。第一の社会的費用の内部化は、消費者が自身の個人情報を「所有」することができるようになることで、情報において、企業に対して圧倒的弱者であった消費者が、取引をできるようになる、ということである。第二の、個人への選好機会の付与は、消費者が自身の情報を取引できるようになることで、自身の情報を取引する状況を選べるようになる、という利点である。

その他にも、個人情報を蓄積する者の不正な富を排除できることや、自主規制を重視するアメリカ文化への適合性などが利点として挙げられている。この時期に共通する問題背景は、第三者が個人の収入、興味、職歴、健康、購買及び嗜好といった情報を大量に収集し、今日におけるビッグデータに近いものを作り上げている事態が生じていること、それによって、目に見えない形で個人が監視されたり、個人の人物像が無断で形成・利用されたりしていることである。この時に初めて、現在の情報社会におけるプライバシー管理の土台が完成したものと思われる。

第2章 プライバシーについて

第1節 プライバシーの定義

プライバシーは、前述したサミュエル・ウォレンとルイス・ブランダイスが著した「The Right to Privacy」における、「ひとりにしておいてもらう権利」(the right to be let alone)が原型である。その原型をより詳細に定義する。

日本弁護士連合会(2012)によると、プライバシーとは、「一人または複数の個人が、自分自身または自分自身に関する情報を他人の目に触れないようにした上で、選択的に開示できること」を指すという。またそれに付け加えて、プライバシーは文化、若しくは個人によって異なり、共通するものとしては、その個人に固有の何か、若しくはその個人にとって他人に知られたくないものを内包しているということであるという。

第2節 プライバシーの範囲

第1項 計数される消費者

現在の社会では、わたしたち消費者のあらゆる個人データが特定の企業や国家によって収集、管理、運用されている。具体的には、氏名、年齢、住所にはじまり、保有資産、職歴、病歴、通信履歴、購買履歴、交友関係、過去の位置情報など、多岐に渡り存在する(現状で

は、これらの情報は散在して存在するのみだが、将来的にすべての情報が紐づけられる可能性は大いにある)。

ローマの皇帝カイザル・アウグストは、人類最初の人口統計を紀元前後に行った。その時から消費者は計数されていたという。大量の個人データを収集、保持、利用するという強いインセンティブにおいて、企業や国家は、現在まで消費者の個人データを収集してきたのだ。しかし、現在の高度情報化社会において、計数する者は過去のそれとは違う力を手に入れた。それが、コンピュータおよび、インターネットなどの ICT の力である。

第2項 ライフログ

1. ライフログの概要

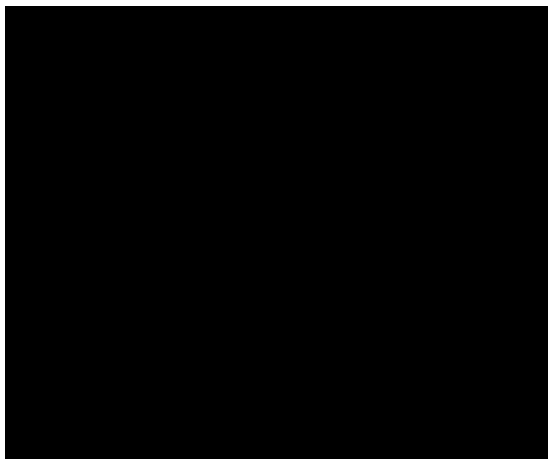
アマゾンや楽天など、インターネットで通信販売のウェブサイトを開覧すると、「最近チェックした商品」や、それに基づいたおすすめ商品を表示されることがある。(図 1 参照) また、通信販売以外の企業のウェブサイトを開覧した場合でも、同じようにその企業の広告が表示される。(図 2 参照) これは、そのウェブサイトで会員登録等の個人を特定できる手続等を消費者が行ったかの有り無しに関わらず起こる。つまり、事業者は自社のウェブサイトへの消費者からの閲覧履歴を保存し、それを基に再訪問があったかどうかを把握できるという事である。これは、事業者がユーザーの個性を基により個人に特化したサービスを提供できる、という点ではユーザーにとって便利な仕組みである。その一方で、便利なサービスを提供するために、「誰からのアクセスか」というアクセスデータを記録、保存することで可能になる。便利さとプライバシー保護をどのように調整するかという問題がある。

このような、インターネット等におけるユーザーの閲覧履歴や検索履歴等をライフログ (life log) という。

図 1 amazon のバナー広告



図 2 global data 社のバナー広告



2. ライフログの定義

総務省(2010)は、ライフログの定義に関して以下のようにまとめている。

「ウェブサイトの閲覧履歴、電子商取引サイトにおける購買・決済履歴、携帯端末の GPS (Global Positioning System 全地球測位システム) により把握された位置情報、携帯端末や自動車に搭載されたセンサー機器により把握された情報、デジタルカメラで撮影された写真、ブログに書き込まれた日記、SNS(Social Networking Service) サイトに書き込まれた交友関係の記録、非接触型 IC を内蔵した乗車券による乗車履歴等から抽出された情報が含まれる。」

このことから、ライフログとは、「デジタルデータとして蓄積された個人の生活の履歴」であるとまとめることができる。

3. ライフログのメリット・デメリット

Federal Trade Commission(2009)は、ライフログにおけるユーザー側のメリットを以下の3点としてまとめている。

第一に、広告料収入に支えられて、コンテンツの無料提供を受けられること。第二に、ユーザーが関心をもった広告、つまり、その人にとって価値のある広告が、労せずしてその人に届けられる利便性。第三に、ユーザーが望まない広告が減少する可能性である。

日本弁護士連合会(2012)は、ライフログの問題点として7点を以下のように述べている。第一に、ユーザーが知らないうちに情報が収集されていること。第二に、ライフログの実態がよく分かっていないこと。第三に、プライバシー侵害の可能性。第四に、誰の関心ごとであるかについての誤解可能性。第五に、ユーザーの知る権利の制約。第六に、平等性を損なうおそれ。第七に、犯罪組織によって利用され、経済的・物理的被害を生じさせるおそれである。

第3項 電子マネー

1. 電子マネーの概要

近年、電車などの交通機関、コンビニエンスストア、レストランなど、身近な場面で電子マネーでの取引がしばしば行われるようになってきている。電子マネーを用いて決済をすることにより、わざわざ貨幣を財布から出したり、おつりを計算する手間が省けたりするだけでなく、ポイントが貯まったりすることがあり、消費者にとっての有益性は大きい。

しかし、電子マネーは、情報の通信によって決済を行う性質上、特定の電子マネーと別のそれとは区別できるようになっていなければならない。また、履歴も残る。必ずしも所有者が識別される必要性はないが、クレジットカードや、携帯電話の IC チップを用いたもの等、個人情報との紐付けができるものであった場合、プライバシー侵害の可能性が存在することになる。日本弁護士連合会 (2012) 参照

2. 電子マネーの定義

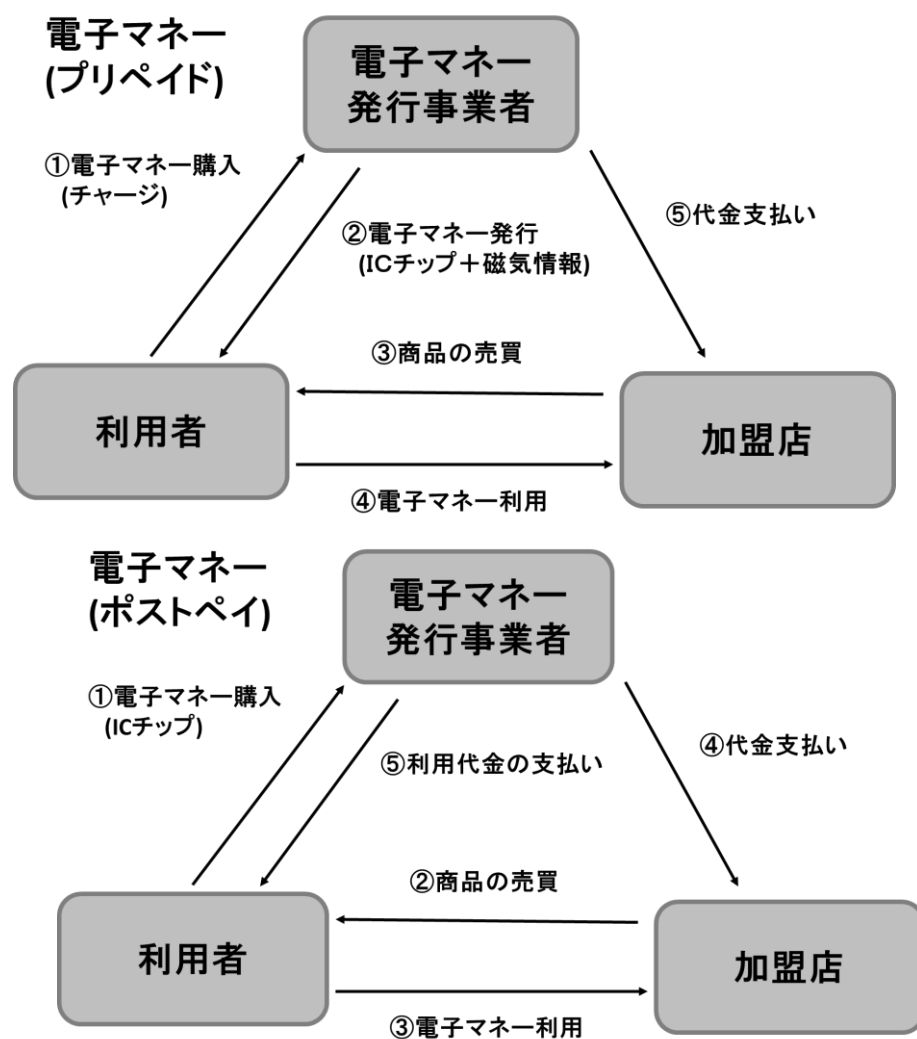
大蔵省(1998)によると、「利用者から受け入れられる資金に応じて発行される電磁的記録を利用者間で授受し、あるいは更新することによって決済が行われる仕組み、または、その電磁的記録自体」を電子マネーの定義としている。

3. 電子マネーの分類

電子マネーの分類としては、様々な視点からの分類が存在するが、本論文では、岡田(2008)による主要なものを紹介することとする。

利用者が資金を支払う時期に応じて、あらかじめ現金をチャージするプリペイド電子マネー、あとで銀行の預金口座から引き落とされる後払い決済サービス(ポストペイ)に分類される。(図 3)

図 3 電子マネーの決済の流れ(経済産業省(2008)より筆者が作成)



発行主体・目的に応じて、鉄道会社が主に交通カードとして発行するもの、電子マネー発行会社が、あらゆる場所で利用するために発行するもの、クレジットカードに代わるものと

して発行するものに分類される。

4.電子マネーの将来

電子マネーはデジタル情報であり、その性質上、伝達・マッチングが容易である。日本弁護士連合会(2012)によると、以下の3点の展望が望めるという。

第一に、多様な業者間における取引履歴等個人情報の共同利用である。他社での取引情報を利用してマーケティングを行うようになる可能性がある。その方が、きめ細やかで、対象者にフィットした営業活動が可能になるだろう。

第二に、位置情報とのリンクである。岡田(2010)によると、位置情報とリンクすることで、それを活用したクーポンや広告を配信することが可能になると指摘されている。

第三に、官民の情報共用である。国や地方自治体が所有する個人情報を取得し、電子マネーによる取引履歴他とマッチングすれば、より精度の高いマーケティング等が可能となる。

第4項 監視カメラ・人の移動履歴

私達の身の回りには、無数の監視カメラが目を見つめている。店舗、施設、駅、道路等、そのほとんどに設置された監視カメラが市民の顔、行動を録画、記録している。現在の監視カメラは、ビデオテープでアナログデータを扱っていた過去に比べ、ハードディスクにデジタルデータを貯蔵しており、顔認証システムによる特定の人物の検索、照合が極めて容易になっている点が特徴的である。顔認証システムとは、監視カメラで撮影された被写体から人の顔を抽出、目、鼻、口などのパーツの位置関係や特徴を数値化、データベースに登録された人物と照合するものである。

監視カメラ同士をネットワークで結合し、システムとして組みなおせば、特定の人物の行動が逐一補足することができる。また、携帯端末のGPS機能や、基地局情報等を利用した人の移動履歴を記録、監視することも技術的に可能となってきた。日本弁護士連合会(2012)参照

第3章 ビッグデータについて

前章で述べた電子マネーや監視カメラ等のライフログは、本章で紹介するビッグデータとして集積される。

第1節 ビッグデータ登場の背景

成耆政(2015)がビッグデータ登場の背景を以下のようにまとめている。世界的なコンサルティング企業である McKinsey&Company (2011) はビッグデータの登場背景を次のようにまとめている。まず第1に、企業の顧客データトレッキングおよび収集行為の増加をあげている。顧客データがインターネットやスマートフォンなどの多様なメディアをつうじてトレッキングされ、オンラインのみならず、オフライン上でもユーザー情報、消費者行

動に関する情報などの収集が可能になった。第2に、貯蔵メディアとカメラモジュール、ディスプレイ価格の引き下げなどはマルチメディアコンテンツの使用拡散と、これに関する情報の増加をもたらした。高画質の動画はすでにインターネットの全体トラフィックの70%以上を占めているといわれ、今後、増え続けるであろう。第3に、TwitterやFacebookなどSNSの急激な拡散とともに、テキストなどの非定型化データの急増である。すなわち、Facebookでは、1カ月に1人のユーザーが平均90以上のコンテンツをアップロードし、YouTubeでは1分毎に24時間分量の動画がアップロードされている。第4に、M2MやIoTなどの通信技術の発展により通信ネットワークで発生するデータ量の増加である。すなわち、M2MやIoTなどの活性化をつうじてデータをユーザーが生成せず、インフラ自体が大量のデータを生成させるようになった。

また、城田(2012)によると、「なぜ今ビッグデータなのか?」とし、まず第1に、ビッグデータの民主化をあげている。これは、今のビッグデータは我々の日々の生活に密着した環境から生成されたことを意味している。第2に、ハードウェアの価格性能比の向上、ソフトウェア技術の進化をあげている。すなわち、コンピュータの価格性能比の向上やハードディスク価格の下落、大量データを汎用品のサーバで高速に処理できる「ハドゥーブ(Hadoop)」の登場、さらにはクラウドコンピューティングの台頭などによってビッグデータを蓄積・処理しやすくなったからである。第3に、クラウド(コンピューティング)の普及をあげている。すなわち、高性能のコンピュータがハードディスクなどのストレージ、そしてデータ分析のためのツールなどを自前で用意する必要性がなくなったことである。たとえば、Amazonのクラウドコンピューティングサービスを使えば、大容量のデータ処理環境を構築しなくても分析が可能である。

以上をふまえ、ビッグデータの登場背景をまとめてみると、第1に、技術進歩によるデータの貯蔵・処理・分析能力の急激な拡大、第2に、データの貯蔵・処理費用の急激な減少、第3に、非構造化データの急激な増加と処理の必要性の向上、そして第4に、データの貯蔵方法のデジタル方式への転換の加速化などをあげることができる。すなわち、「インターネットの発展によりクラウド化が進み、その次の段階としてビッグデータに幅広い分野での応用が可能になった」ということである。

第2節 ビッグデータの定義

McKinsey(2011)によると、「ビッグデータとは、通常のデータベース管理ツールが貯蔵・管理および分析可能な範囲を超える規模のデータ」と定義づけている。

IT業界における市場調査およびコンサルティング企業であるIDC(International Data Corporation)は、次のいずれかの条件を満たすデータをビッグデータと定義している。すなわち、第1に、100TB以上のデータを有していること、第2に、音声や映像、金融取引情報、センサーなどのハイスピードストリーミングデータを利用していること、第3に、年率60%以上の成長率で生成されるデータであること、などである。そして、データを解析

する際、スケーラブルなインフラを使用することも条件としている。そして、IDC はデータベースではなく、企業や組織の業務遂行に焦点を当てて、多様な種類の大規模データから安いコストで価値を抽出し、データの超高速収集・発掘・分析をサポートできるように考案された次世代技術およびアーキテクチャーと定義づけた。

以上の特性をまとめてみると、ビッグデータには量的、質的、そして速度的側面に特徴があると思われる。

独立行政法人 情報処理推進機構(2012)によると、ビッグデータには解析対象にテラバイト、ペタバイトといった大量なデータとしての **Volume**(量)、利用者の目的に合致する価値を持つ **Variety**(多様性)、リアルタイム処理を行う上で十分な **Velocity**(速さ、データの新鮮さ)の 3 つの性質があるという。本論文では、このビッグデータの定義として独立行政法人 情報処理推進機構(2012)の定義を扱うこととする。

第 4 章 仮説と検証

第1節 仮説

前述の先行研究では、高度情報通信社会において利用されるサービスやインフラストラクチャーと、それらのデータの集積であるビッグデータについて述べた。冒頭でも述べたように、これらは消費者が有益なサービスを受ける上で重要なものである。一方で、消費者のプライベート情報が当事者の目の届かないところで利用されている、という事実も存在する。このジレンマの中で、消費者はその事実をどのように受け止めているのか、ということを明らかにする。本論文では、主にスマートフォンにおけるアプリケーションの利用において、消費者の意識を調査することとする。

スマートフォンの利用において、消費者がプライベート情報を第三者に発信する機会として以下の 2 つを設定した。一つはアプリケーションをダウンロードするとき。もう一つは、アプリケーション(主に SNS アプリケーション)を利用しているときである。前者に関連する仮説として、スマートフォンのアプリケーションをダウンロードするときの情報開示の項目に目を付けた。アプリケーションの情報開示とは、アプリケーション側から要求される個人のスマートフォンに格納されている情報である。この情報開示にも 2 つの種類が存在する。必須情報と、そうでない情報である。前者は、アプリケーションを利用する上で必須の情報である。例としては、SNS アプリでのカメラ機能を活用するためのカメラへのアクセス権限がそれにあたる。後者は、電話番号や、アプリ内課金の権限などである。

消費者はこれらの情報開示の項目が多いほどアプリのダウンロードに抵抗を感じ、少ないほど抵抗を感じないのではないだろうか。これらのことを踏まえ、仮説 1 として消費者は、スマートフォンでアプリケーションをダウンロードするとき、情報開示の項目

が多いほど抵抗を感じる、とした。そして、消費者がプライベート情報を第三者に発信するもう一つの機会として、アプリケーションを利用している段階があると先に述べた。消費者は、アプリケーション(特に SNS)を利用する上で、自己のプライベート情報を開示しがちである。それは、アプリケーションを利用するにあたり、サービスを受けることの利益が、プライバシーを開示することによる不利益よりも大きいからなのではないだろうかと考えた。その事から、仮説 2 として、プライバシーへの関心が高い消費者は、プライバシーへの関心が低い消費者に比べ、ネット上のサービスを受けるために、その利用における対価としてのプライバシーを重視する傾向がある、とする。

第 2 節 調査概要

前述した仮説を検証するための調査としては、紙面としてのアンケート調査を駒澤大学の学生 60 名に対して実施した。仮説を検証するため、プライバシーの関心の高低を計測する尺度として佐藤ら(2013)の論文から引用、一部修正したものを利用した。また、セキュリティリテラシーを測る指標として、総務省(2012)から一部引用したものを載せている。後に述べるが、これらの尺度を利用し、自身のプライバシーへの関心の高いグループと、プライバシーへの関心の高いグループを設定した。また、仮説 1 を証明するため、紙面では、回答者にスマートフォンのアプリケーションをダウンロードする状況をイメージしてもらうものである。具体的には、SNS、ゲーム、キュレーションアプリの三種類である。また、それらに関しても、それぞれダウンロード時に要求される情報の多いパターンと少ないパターンの二つを用意した。その中で、要求される情報について回答者がどのように感じたかを評価してもらった。これを t 検定にて検証し、有意差を算出する。

仮説 2 では、SNS で個人情報に関わる投稿を行ったかどうかについて調査した。こちらは、カイ二乗検定にて検定し、有意差を算出する。

第 3 節 検証結果

仮説 1 は、ペア 1,3,5,6 が SNS、7,9,11,12 がゲーム、13,15,17,18 がキュレーションアプリという風に対応している。結論としては、SNS アプリでは、2 項目において 5%水準で有意差が見られ、ゲームアプリに関しては、4 項目すべて 1%水準で有意差が見られた。キュレーションアプリでは 3 項目に 1%水準で有意差が見られた。SNS アプリの質問項目では半分か、キュレーションアプリでは 1 項目において有意差が見られなかった。従って、仮説 1 は一部支持とする。(図 4)

図 4 アプリケーション別情報開示項目の多少による回答の比較結果

質問項目		平均値	t 値	自由度	有意確率
ペア 1	Q11不信を感じる項目多 Q12不信を感じる項目少	-.3333	-2.199	59	.032
ペア 3	Q11落ち着かない気持ちになる項目多 Q12落ち着かない気持ちになる項目少	-.3833	-2.326	59	.023
ペア 5	Q11不安を感じる項目多 Q12不安を感じる項目少	-.2833	-1.883	59	.065
ペア 6	Q11気が重く感じる項目多 Q12気が重く感じる項目少	-.1833	-1.420	59	.161
ペア 7	Q14不信を感じる項目多 Q13不信を感じる項目少	.6000	5.028	59	.000
ペア 9	Q14落ち着かない気持ちになる項目多 Q13落ち着かない気持ちになる項目少	.3833	3.598	59	.001
ペア 11	Q14不安を感じる項目多 Q13不安を感じる項目少	.4833	3.744	59	.000
ペア 12	Q14気が重く感じる項目多 Q13気が重く感じる項目少	.2833	3.294	59	.002
ペア 13	Q16不信を感じる項目多 Q15不信を感じる項目少	.6333	4.788	59	.000
ペア 15	Q16落ち着かない気持ちになる項目多 Q15落ち着かない気持ちになる項目少	.4000	3.421	59	.001
ペア 17	Q16不安を感じる項目多 Q15不安を感じる項目少	.5000	3.581	59	.001
ペア 18	Q16気が重く感じる項目多 Q15気が重く感じる項目少	.1167	1.154	59	.253

仮説 2 では、プライバシーへの関心が高いグループと、低いグループを分類し、それぞれに SNS への個人情報を投稿した経験があるかを質問し、カイ二乗検定を行った。その結果、プライバシーへの関心が高いグループは SNS へ個人情報を投稿した経験が少ないという結果で、5%の水準で有意であるという結果が出たため、仮説 2 は支持とする。(図 5)

図 5 プライバシーへの関心の高低における SNS への個人情報の投稿経験の比較結果

			Q17SNS個人情報投稿有無		合計
			はい	いいえ	
group仮説2	プライバシー関心の高いグループ	度数	18	11	29
	プライバシー関心の低いグループ	度数	27	4	31
合計		度数	45	15	60
カイ 2 乗検定					
	値	自由度	漸近有意確率 (両側)	正確有意確率 (両側)	正確有意確率 (片側)
Pearson のカイ 2 乗	5.006 ^a	1	.025		

第5章 研究の考察と提案

第1節 結果考察

本調査では、消費者が特定のサービスを利用する際に、自身のプライバシーを考慮するのかどうかということと、プライバシーへの関心の高低と、それらプライバシーを重視することとの間で相関関係があるのかどうかを検証した。その結果、前者に関しては、一部支持という形ではあるものの、特定のサービスを利用する上で消費者は自身のプライバシーを考慮しているという結果が得られた。また、後者に関しても、支持という結果が得られ、プライバシーへの関心の高い消費者は、ネット上のサービスを利用する上では、その対価としてのプライバシーを重要な取引材料としてみなしているということが分かった。逆説的に言えば、プライバシーへの関心の低い消費者は、同じ状況下では自身のプライバシーを重要視しているとは言えない、ということでもある。

以上のことから、プライバシーへの関心の高い消費者は、スマートフォンのアプリケーションをダウンロードするとき、情報開示の項目が多いほど抵抗を感じ、そのダウンロードの際、自身の提供するプライバシーとサービスの内容を天秤にかけ、判断を下すというプロセスが存在するのであろう。一方で、プライバシーへの関心の低い消費者は、スマートフォンのアプリケーションをダウンロードするとき、情報開示の項目が多いほど抵抗を感じるものの、ダウンロードの際に自身のプライベート情報を考慮するというステップを踏まない傾向にあるのだと考えられる。

第2節 今後の提案

今回の研究は、消費者の個人情報を欲し、また取り扱う企業、そして行政は、彼らのデリケートな部分に対してどのようにアプローチするべきかのヒントになるだろう。具体的には、消費者がアプリケーションをダウンロードするプロセスがある程度クリアになったことである。プライバシーへの関心の高低によって、消費者がアプリケーションをダウンロードするプロセスが異なる点は、企業にとって一つのヒントに成り得るものである。

本論文の反省として、仮説1では、一部支持という結果になったという点がある。その原因として、二つの事が考えられる。一つは、情報開示の項目の数である。SNSでは情報開示の項目が多いパターンが8項目、ゲームでは6項目、キュレーションでは4項目だった。

「気が重く感じる」の項目において、キュレーションでは有意差が現れなかったのは、それが原因の一つであると考えられる。二つ目は、例として使ったアプリの性質である。今回SNSは、最も有意差が出なかったアプリであるが、その原因として、情報開示の項目が少ないアプリとして例示したものが、ネガティブイメージのある出会い系サイトとして見受けられるものであったため、回答者が情報開示というよりアプリそのものに嫌悪感を抱いた可能性がある。それが要因で有意差が出なかったと考えられる。

また、プライバシーへの関心の高い、低いという二つの領域でのみしか扱わなかったが、この領域を複雑にすることで、また違った結果が出るかもしれない。アプリケーションをダウンロードする際の個人情報を開示する旨の項目の種類、数の差で比べてみても面白いかもしれない。

参考文献

- ・飯塚周一(2015) 「M2M /IoT のビジネスモデルと今後の展望ー IoT とインターネットビジネスの変革ー」『日本情報経営学会誌』 Vol 35, No.4 27-33
- ・石井夏生利(2012) 「プライバシー・個人情報の「財産権論」ーライフログをめぐる問題状況を踏まえてー」『情報通信政策レビュー』 第二巻、66-87
- ・大蔵省(1998) 電子マネー及び電子決済の環境整備に向けた懇談会報告書
- ・岡田仁志(2008) 『電子マネーがわかる』 日本経済新聞出版社
- ・岡田仁志(2010) 「電子マネーのデータプロテクションー 匿名勾配の自由と購買履歴の活用の調和」『NBL』 922 号 22-29
- ・海部美知(2013) 『ビッグデータの覇者たち』 講談社
- ・河村進(2013) 『おうちで学べるプログラミングのきほん』 翔泳社
- ・経済産業省(2008) 新たな支払サービスの現状と課題について
- ・佐藤広英 太幡直也(2013) 「インターネット版プライバシー次元尺度の作成」『パーソナリティ研究』 vol.21 312-315
- ・サムエル・D・ウォレン/ルイス・D・ブランドイス (外間寛訳) (1959) 「プライバシーの権利 (一)」法律時報第 31 巻第 7 号
- ・城田真琴(2012) 『ビッグデータの衝撃』 東洋経済新報社
- ・首相官邸 日本経済再生本部(2015) 『『日本再興戦略』改訂 2015ー未来への投資・生産性改革ー」
- ・成耆政(2015) 「ビッグデータ (Big Data) の利活用による戦略的企業経営管理ーその概念、現状、そして活用の経済的分析」『松本大学研究紀要』 第 13 号 51-72
- ・総務省(2010) 利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会
- ・総務省(2012) 「青少年のインターネット・リテラシー指標」
- ・独立行政法人 情報処理推進機構(2012) 『つながる IT がもたらす豊かなくらしと経済』 独立行政法人 情報処理推進機構
- ・日本弁護士連合会(2012) 『デジタル社会のプライバシーー共通番号制・ライフログ・電子マネー』 航思社
- ・藤井章博(2015) 「IEEE 論文に基づく IoT 研究動向の 計量書誌学的調査」『科学技術動向』 149 号 19-24
- ・みずほ情報総研(2015) 「IoT(Internet of Things)の現状と展望-IoT と人工知能に関する

調査を踏まえて-」 みずほ産業調査

- ALAN F. WESTIN (1967) PRIVACY AND FREEDOM
- ARTHUR R. MILLER (1971) THE ASSAULT ON PRIVACY : COMPUTERS, DATA BANKS, AND DOSSIERS
- FTC Staff Report(2009)
Self-Regulatory Principles For Online Behavioral Advertising
- IDC(2012) The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east
- McKinsey Global Institute(2011)Big data: The next frontier for innovation, competition, and productivity
- Pamela Samuelson(2000)”Privacy as Intellectual Property?”52 STAN. L. REV. 1125:1130-1136
- Peter Mell Timothy Grance(2011) NIST によるクラウドコンピューティングの定義
- PETER P. SWIRE & ROBERT E. LITAN(1998).
NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8
- RESTATEMENT (SECOND) OF TORTS(1977)
- Samuel Warren, Louis Brandeis(1890) “The Right to Privacy” Harvard Law Review,4(5):193-220
- William L. Prosser(1960) Privacy, 48 CALIF. L. REV. 383

参考サイト

- 新約聖書メッセージ(アクセス日時 2016 年 11 月 24 日)
http://www.logos-ministries.org/new_b/lk2.html
- マッキンゼーアンドカンパニー(2016 年 12 月 02 日)
McKinsey&Company.<http://www.mckinsey.com/>
- シナノリンク株式会社 HP IoT とは(2016 年 12 月 02 日)
http://www.shinanoe.co.jp/activities_m2m_01.html
- FUJITSU 公式サイト Hadoop とは (2016 年 11 月 24 日)
<http://www.fujitsu.com/jp/products/computing/storage/lib-f/tech/beginner/hadoop/>

プライバシーとネットリテラシーに関する意識調査

中野ゼミ 4年 中井舜

■大変お忙しいところ申し訳ありませんが、調査へのご協力をよろしくお願いいたします。
本アンケートは、今後の研究活動の資料とする事を目的としており、
お答えいただいた内容は統計的に処理しますので、ご迷惑をおかけすることは
絶対にございませ。少々お時間をいただきますが、是非ご協力をお願い申し上げます。

記入日 年 月 日

Q1.性別をお答えください。(当てはまるものに○を書いてください)

- ① 男性 ② 女性

Q2.学年をお答えください。

- ① 1年生 ②2年生 ③3年生 ④4年生

Q3.パソコンを使う頻度で最も近い番号に○を書いてください。

- ①毎日 ②三日に一回程度 ③週に一回程度 ④一カ月に一回程度 ⑤使わない

Q4.スマートフォンを使う頻度で最も近い番号に○を書いてください。

- ①毎日 ②三日に一回程度 ③週に一回程度 ④一カ月に一回程度 ⑤使わない

Q5.以下の各項目について、ネット上の匿名な不特定多数の人に対してどのくらい知られたくないと感じるか、一番当てはまる選択肢に、○を 1つだけ つけてください。

	知られたくない	どちらかという 知られたくない	どちらかという 知られてもよい	知られてもよい
1.悩み事	4	3	2	1
2.過去の出来事	4	3	2	1
3.病歴	4	3	2	1
4.自分の生い立ち	4	3	2	1
5.買い物の履歴	4	3	2	1
6.普段の生活パターン	4	3	2	1
7.友人関係	4	3	2	1
8.思想信条	4	3	2	1
9.閲覧したサイトの履歴	4	3	2	1

	知られたくない	どちらかという 知られたくない	どちらかという 知られてもよい	知られてもよい
10.出身地	4	3	2	1
11.恋人配偶者の有無	4	3	2	1
12.趣味	4	3	2	1
13.血液型	4	3	2	1
14.性別	4	3	2	1
15.家族構成	4	3	2	1
16.生年月日・年齢	4	3	2	1
17.職業	4	3	2	1
18.本名	4	3	2	1
19.会社名・学校名	4	3	2	1
20.容姿・顔写真	4	3	2	1
22.住所	4	3	2	1
23.クレジットカードの番号	4	3	2	1
24.銀行の口座番号	4	3	2	1
25.暗証番号・パスワード	4	3	2	1

Q6. ネットでのプライバシーについて、以下の項目についてあなたの態度を教えてください。
一番当てはまる選択肢に、○を 1つだけ つけてください。

	そう思う	ややそう思う	あまり そう思わない	そう思わない
1. 発信した情報は多くの人に広まることを理解している。	4	3	2	1
2. 書き込みをした人物は特定され得ることを理解している。	4	3	2	1
3. インターネット上で一度公開された情報は、多くの人にすぐ広まり、完全に消すことが困難であることを理解している。	4	3	2	1
4. SNSへ個人情報や写真を掲載することにより、連絡先や名前を公開され攻撃されたり、事件に巻き込まれる等のリスクが伴うことを理解している。	4	3	2	1
5. SNSを通じてプライバシー・個人情報・交友関係に関わる情報の収集が行われている可能性があることを理解している。	4	3	2	1
6. 自らの情報を公開する範囲に注意している。	4	3	2	1
7. スマートフォンのアプリケーションも、パソコンのアプリケーションと同様に、欠陥(バグ)を含んでいたり、意図的に悪意のあるものも存在することを理解している。	4	3	2	1
8. スマートフォン上のアプリケーションの中には、プライバシー・個人情報を自動で外部に送信するものもあることを理解している。	4	3	2	1
9. アプリケーションの利用登録では、必要以上の情報発信に注意している。	4	3	2	1
10. スマートフォンアプリケーションをダウンロードする際には、当該サイトおよび提供元の信頼性・安全性を確認している。	4	3	2	1
11. アプリケーションには、パソコンのアプリケーションと同様に、ウイルスが混入している可能性があることを理解している	4	3	2	1
12. アプリケーションのインストール時に表示される「アクセス許可」先の情報(電話番号、現在位置等)を確認して、アクセス許可先の情報を限定する、もしくは当該アプリケーションをインストールしない等、アプリケーションによってプライバシー・個人情報が漏洩しないよう注意している。	4	3	2	1

	そう思う	ややそう思う	あまり そう思わない	そう思わない
13.パソコンや携帯電話などには、氏名や住所などを含むプライバシー・個人情報が含まれていることを理解している。	4	3	2	1
14.インターネット上のプライバシー・個人情報は悪用される恐れがあることを理解している。	4	3	2	1
15.写真に位置情報が記録されていることがあることを理解している。	4	3	2	1
16.自分や他の人のプライバシー・個人情報をSNSなどに書き込むと、当該情報が悪用される恐れがあることを理解している。	4	3	2	1
17.ID・パスワードを厳重に管理している。	4	3	2	1
18.共用のパソコンでは自分の利用履歴が残る可能性があることを理解している。	4	3	2	1
19.サイトへの閲覧履歴が、企業もしくは第三者に取得されていることを理解している。	4	3	2	1
20.非接触型ICカード(suica、PASUMOなど)の利用履歴から、第三者に自身の位置情報が取得されることを理解している。	4	3	2	1
21.電子マネーもしくはポイントカード(suicaやpontaカード)の利用履歴から、購入履歴や傾向が第三者に取得されることを理解している。	4	3	2	1
22.GPSを利用することで、自身の位置情報が第三者に取得されていることを理解している。	4	3	2	1
23.監視カメラによって、自身の行動が第三者に取得されていることを理解している。	4	3	2	1

■ここからは、スマートフォンのアプリケーションの利用状況についてお聞きします。

Q7. 平均的な一日のあなたのスマートフォンの利用時間を教えてください。(使わない場合は、0分と記入してください。)

()分

Q8. 平均的な一日のあなたの SNS アプリ(Twitter や facebook など)の利用時間を教えてください。(使わない場合は、0分と記入してください。)

()分

Q9. 平均的な一日のあなたのゲームアプリの利用時間を教えてください。(使わない場合は、0分と記入してください。)

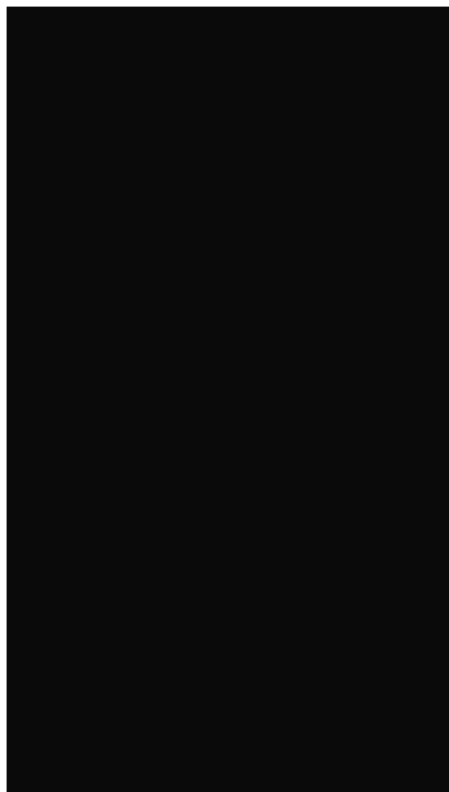
()分

Q10. 平均的な一日のあなたのキュレーションアプリ(スマートニュースや Naver まとめなど)の利用時間を教えてください。(使わない場合は、0分と記入してください。)

()分

Q 11.実際に SNS のアプリケーションをダウンロードしようとしている状況を思い浮かべてください。

以下の画面が表示されたとき、あなたの態度として、以下の項目に当てはまる選択肢に○を1つだけつけてください。



	そう思う	やや そう思う	あまり そう思わない	そう思わない
不信を感じる	4	3	2	1
わくわくする	4	3	2	1
落ち着かない気持ちになる	4	3	2	1
嬉しい気持ちになる	4	3	2	1
不安を感じる	4	3	2	1
気が重く感じる	4	3	2	1

Q 12.実際に SNS のアプリケーションをダウンロードしようとしている状況を思い浮かべてください。

以下の画面が表示されたとき、あなたの態度として、以下の項目に当てはまる選択肢に○を1つだけつけてください。



	そう思う	やや そう思う	あまり そう思わない	そう思わない
不信を感じる	4	3	2	1
わくわくする	4	3	2	1
落ち着かない気持ちになる	4	3	2	1
嬉しい気持ちになる	4	3	2	1
不安を感じる	4	3	2	1
気が重く感じる	4	3	2	1

Q 13.実際にゲームのアプリケーションをダウンロードしようとしている状況を思い浮かべてください。

以下の画面が表示されたとき、あなたの態度として、以下の項目に当てはまる選択肢に○を1つだけつけてください。



	そう思う	やや そう思う	あまり そう思わない	そう思わない
不信を感じる	4	3	2	1
わくわくする	4	3	2	1
落ち着かない気持ちになる	4	3	2	1
嬉しい気持ちになる	4	3	2	1
不安を感じる	4	3	2	1
気が重く感じる	4	3	2	1

Q 14.実際にゲームのアプリケーションをダウンロードしようとしている状況を思い浮かべてください。

以下の画面が表示されたとき、あなたの態度として、以下の項目に当てはまる選択肢に○を1つだけつけてください。



	そう思う	やや そう思う	あまり そう思わない	そう思わない
不信を感じる	4	3	2	1
わくわくする	4	3	2	1
落ち着かない気持ちになる	4	3	2	1
嬉しい気持ちになる	4	3	2	1
不安を感じる	4	3	2	1
気が重く感じる	4	3	2	1

Q 15.実際にキュレーションメディアのアプリケーションをダウンロードしようとしている状況を思い浮かべてください。

以下の画面が表示されたとき、あなたの態度として、以下の項目に当てはまる選択肢に○を1つだけつけてください。



	そう思う	やや そう思う	あまり そう思わない	そう思わない
不信を感じる	4	3	2	1
わくわくする	4	3	2	1
落ち着かない気持ちになる	4	3	2	1
嬉しい気持ちになる	4	3	2	1
不安を感じる	4	3	2	1
気が重く感じる	4	3	2	1

Q 16.実際にキュレーションメディアのアプリケーションをダウンロードしようとしている状況を思い浮かべてください。

以下の画面が表示されたとき、あなたの態度として、以下の項目に当てはまる選択肢に○を1つだけつけてください。



	そう思う	やや そう思う	あまり そう思わない	そう思わない
不信を感じる	4	3	2	1
わくわくする	4	3	2	1
落ち着かない気持ちになる	4	3	2	1
嬉しい気持ちになる	4	3	2	1
不安を感じる	4	3	2	1
気が重く感じる	4	3	2	1

Q 17.SNS に関する質問です。あなたは、SNS 上で個人を特定できる情報(顔写真や本名、学校名など)や、位置を特定できる情報(訪ねた施設など)などを投稿したことがありますか(自身のプロフィールページ等含む)。

当てはまる選択肢に○をつけてください。

1.はい(Q18 へ)

2.いいえ(Q20 へ)

Q18. 前の質問で「1.はい」と答えた方に質問です。個人情報(個人や位置など)を特定される投稿をする上で、あなたの態度に最も近い選択肢に 1つだけ ○をつけてください。

	当てはまる	どちらかといえば 当てはまる	どちらかといえば 当てはまらない	当てはまらない
1. 自身の個人情報が流出している自覚がなかった。	4	3	2	1
2. 自身の個人情報が流出している自覚はあったが、 気に留めなかった。	4	3	2	1
3. その他(ほかに何かあればよろしくお願いします。)	()			

Q19. 前の質問で「1.はい」と答えた方に質問です。あなたが SNS で載せた情報(写真や動画をもとにそれと推測できるもの含む)に当てはまるもの すべてに ○をつけてください。

1.本名 2.学校名 3.容姿・顔写真 4.住所 5.出身地 6.恋人配偶者の有無 7.趣味

8.血液型 9.性別 10.生年月日・年齢 11.職業 12.電話番号 13.その他()

Q20. 前の質問で「2.いいえ」と答えた方に質問です。なぜ個人情報(個人や位置など)を特定される投稿をしなかったのか、あなたの態度に最も近い選択肢に 1つだけ ○をつけてください。

	当てはまる	どちらかといえば 当てはまる	どちらかといえば 当てはまらない	当てはまらない
1.自身の個人情報を流出させることになると思ったため。	4	3	2	1
2.自身の個人情報を流出させることになるとは思わなかったが、機会がなかったため。	4	3	2	1
3.その他(ほかに何かあればよろしくお願いします。)	()			

調査は以上になります。
ご協力ありがとうございました！