Postmodern Surveillance and the Limits of Privacy

Masashi TSUBOI

Abstract

In this paper, I consider the problems of postmodern surveillance, and point out the limits of the concept of privacy. There are differences between modern surveillance and postmodern surveillance. Postmodern surveillance is any collection and processing of personal data for the purposes of influencing or managing those whose data have been garnered.

Surveillance capacities are used to sort and sift populations, to categorize and to classify, to enhance the life chances of some and to retard those of others. The problem of postmodern surveillance is the violation of human rights or human dignity in the use of data-persona that is made through the processes of such social sorting.

Professionals in information processing should be aware of the ethical aspects of their role. Since transparency is vital in our postmodern surveillance society today, we need to monitor how our personal data are exchanged in society, and to make the contents of our data-persona clear.

現代の監視とプライバシーの限界

坪　井　雅　史

はじめに

現代社会を特徴付ける言葉の一つに「監視社会」があげられる。監視が問題にされはじめたのは、それほど新しいことではない。そして、従来、権力による監視に抵抗するための概念として用いられたのは、プライバシーであった。しかし、近年の情報技術の発達にともなって、監視は量的な変化だけでなく、質的な変化の時代を迎えている。それにともなって、問題を摘出するための概念も、もはやプライバシーだけでは事足りなくなっている。この小論では、監視社会におけるプライバシーの意義を確認するとともに、その限界を指摘し、監視社会を個人の権利への侵害だけでなく、個人の生き方の問題や社会のあり方の問題として考えることの必要性を論じる。

そのためにまず、監視社会論のキーワードとなる基本的な概念が提示されてきた経緯をふり返る。次に、現代の監視の特徴と権力との関係を確認する。その上で、監視社会におけるプライバシーの意義を、特に法的な側面を中心に確認し、さらにその限界を指摘する。そして、監視社会が、社会的差別を強化し、個人の自由や自律に影響を及ぼすだけでな

く、民主主義の基盤である、自由なコミュニケーションを阻害する危険性を指摘する。最後に、こうした監視社会における専門家と市民のコミュニケーションのあり方について論じる。

1.「監視社会論」小史

「監視社会」という言葉を初めて使い、これを学問的に論じたのは、MIT 教授ゲイリー・マルクスによる「監視社会」(1985) であるとされる (田畑 2003)。

監視の問題は 1960 年代以降から、ウェーバーが指摘した近代以後の官僚制による監視の問題や、ビデオカメラの普及にともなう問題、コンピュータによるデータ収集の問題など、技術の発達にともなう、主としてプライバシーの危機の問題として論じられてきた。その後、インターネットの登場によって、監視に対する考え方そのものに大きな変化が見られ、オーウェルの『1984 年』を典型とする従来型の監視ではなく、「データベイランス」という言葉に象徴されるような、デジタル化されたデータによる監視とそれがもたらす問題が主題的に考察されるようになる。これらに関連する文献を列記すると、表 1 のようになる (田畑 2003、青柳などを参照)。

2. 現代の監視特徴と権力との関係

2.1 監視と権力

フーコーによって詳細に描き出された、近代のいわゆる規律社会では、《パノプティコン型の監視》による規範の内面化が進み、それによって自由で理性的な主体が形成されたといわれる。軍隊や工場、学校といっ

表 1

1964 年：ヴァンス・パッカード、『裸の社会』…プライバシーの危機への警鐘。
1985 年：ゲイリー・T・マルクス「監視社会」…はじめて「監視社会」という語を使用。
1990 年：ダンデカー『監視、権力、モダニティ』…ウェーバーの官僚制と監視との関係を指摘し、官僚制的な監視の拡大について論じる。
1990 年：マーク・ポスター『情報様式論』…コンピュータ・データベースによる、新たな形のパノプティコン（スーパーパノプティコン）の出現について論じる。
1993 年：オスカー・ガンジー『パノプティック・ソート』（邦題『個人情報と権力』）…パノプティック・ソートという用語で、人々を監視し並べ替えを行うメカニズムを指摘。
1994 年：クラーク「デジタル・ペルソナとデータ監視（dataveillance）」…個人の代理として利用されるデジタル・データを「デジタル・ペルソナ」と呼び、それが社会管理やマーケティングに利用される状況を論じる。
1994 年：ライアン『電子の眼』…監視社会を本格的に論じた最初の書。
1995 年：ボガード『監視のシミュレーション』（邦題『監視ゲーム』）
2001 年：ライアン『監視社会』

た近代に特徴的な閉鎖空間において、身体に対する規律訓練を通して従順に服従する臣民が産み出されたのである。監視社会論でもしばしば参照される、オーウェルのビッグブラザーによる監視は、まさにそうした国家権力に従う市民を産み出す装置であった。

もちろん現代でも、こうして規範を内面化した自律的主体としての個人を中心とした社会システムがなくなったわけではない。しかし、現代は、こうした近代的な規律社会から、ポストモダン型の管理社会へと移行していると言われている。ここでの管理社会とは 1960〜70 年代あたりに日本で流行した「管理社会論」、すなわち国家や大企業による集中管理がもたらす問題とは別物であり、この違いを理解することが、現代の監視の特徴を理解する上で重要になる。

両者の違いを、岡本は、「統制管理社会」と「自由管理社会」という表現で区別している（岡本 p. 66）。前者は、アドルノが『啓蒙の弁証法』で「管理された世界」と呼び、批判を加えた、「全体主義的支配」が行使される社会である。それに対して後者は、全体主義的な権力で人々の自由を奪うような権力ではない。人々が安全に暮らせるように、セキュリティーを確保し、リスクを管理することによって社会秩序を維持する権力である。こうした権力への批判は、アドルノらのやり方ではうまくいかない。そのことを遠藤は次のように表現している。

> 「この構造の最大の特徴は、「安心・安全社会の希求」が非イデオロギー的で普遍的な願望として措定されていること、監視を望む理由が他者の支配ではなく自らが被害者となることの回避である点である。このような論理構成は、基本的に反論を許さない。」（遠藤 p. 32）

（フーコーが規律権力と生権力との関係をどう捉えていたかは置くとして）こうした管理社会の権力は、近代型の権力ではなく、フーコーが述べた生権力、すなわち個人に対する権力というよりも統計などを用いて人口を操作する権力であり、生物としての人間からさまざまな危険を遠ざけ、安心して生きていくことを保障するために、集団全体を管理する、「セキュリティーの権力」であるとされる（岡本 p. 45）。ここでは、個々人の自由の許容度が高く、人々の生活には利便性とセキュリティーが与えられている。ただしここでは、ファシズム的な全体主義とは異なるが、一定の許容範囲からはみ出た者は排除される。

> 「リスク社会において恐怖の源泉となるのは、バウマンも指摘するように、システムから排除されるべきもの／排除されたもの／排除されることである。リスク社会においては、システムの不確実性を増大させるもの（システムの障害となる可能性のあるもの）は排除

される必要があり、また排除されたものはそのことによってシステムの潜在的敵対者とみなされる。」（遠藤 p. 34）

このように、一定の範囲内であるとはいえ、人々の自由とセキュリティーが広く保障されている限り、自由の侵害を根拠に管理社会を批判することは的外れとなる。むしろ、吉田が指摘するように、今後は、どのような自由と引き替えに、どのような自由が得られるのかを考える必要があるのである（吉田 p. 7）。

2.2　現代の監視の特徴　―監視主体の問題

上記のようなパノプティコン型の監視とは異なった意味での監視とは、どのようなものであろうか。単にパノプティコン型の監視の手段が、コンピュータやデータベースの発達・普及、検索能力の向上によって高度化した「スーパー・パノプティコン」（ポスター）とは何が異なるのか。「ポストモダン的監視」とも言われる現代の監視の特徴を、ライアンは次のように定義する。監視とは「データが集められる当該人物に影響を与え、その行動を統御することを目的として、個人データを収集・処理するすべての行為である」と（Lyon2001, p. 2）。

「データ監視（dataveillance）」というクラークの造語が端的に示すように、現代の監視は物理的な監視ではなく、コンピュータによる日常的、自動的なデータ収集によって行われる。その目的は主に二つに分かれる。一つは、多種多様な情報の中から、ある特定の個人の情報を炙り出すこと。もう一つは、ある特定の集団や現象に共通の特徴を浮かび上がらせることである。

最近話題になったNSAによるデータ監視に象徴されるように、国家による電子データの監視は、9.11以後加速したと言われている。最終的には計画段階での反対によって実現はしなかったが、例えば次のような

例がある。

> 2002年8月、米国防総省の国防高等研究計画庁は「全情報認知（TIA：Total Information Awareness）」システムの検討をはじめた。テロ後、「パトリオット法」をはじめさまざまなテロ対策を講じた米国においても、TIAは破格の計画、だった（のちにTIAは、Terrorists Information Awarenessに名称が変更されている）。TIAは、その名が示すとおり、ありとあらゆる個人の情報を網羅・収集するプログラムだ。氏名、住所、性別、生年月日といった基本情報にはじまり、運転免許証、社会保障番号、納税者番号といった公的機関の情報、さらには学歴、個人の銀行口座内容、クレジットカード履歴、航空便履歴、医療機関履歴……。そして、それら複数の情報を担保する本人認証機能に、指紋・顔・歩き方・虹彩といったバイオメトリクス情報があった。要するに、個人の存在の有無を証明するデータではなく、その人物が「どのような人間であるか」を把握するためのデータベースとICカードのシステムだ。（森 pp. 329–30）

このように、現代の監視とは、デジタル化された個人の属性や生活・行動履歴を収集し蓄積すること、またそれによって築かれたデータベースに対する、多種多様な情報技術的処理のプロセスの総体だと言えよう。

もちろん、ここでの主体は、国家とは限らない。（現在の監視の問題を扱った文献においても、従来的な国家による監視問題こそが主要な問題だとする論者もいるが。）また、大企業による労働者管理のための情報収集こそが問題というわけでもない。例えば、SNSは情報を収集することを意図していると言えるだろうか？　監視対象が予め特定されているのだろうか？　データは利用者によって自発的に発せられているが、それらは「収集されている」と言われるべきだろうか？　このように、

ここではむしろ、監視の主体の不明確さ、こう言ってよければ、誰もが、いつでも監視の主体になり得る社会において、どのよう場合に監視主体を明らかにすべきなのかが問い直されねばならない。

その際、特に注視すべきは、さまざまな監視によって集められたデータベースを統合する力である。ライアンが「監視の複合体（アッサンブラージュ）」と呼ぶ、複合的な権力の母体が創造されているのである。

こうした監視は、もちろん日本的な「管理社会論」が指摘した、企業による合理化のための労働者への管理とも結びついて、現在ではセキュリティーをも目的として、労働現場で強化されている。その一例として、森があげる例を紹介しよう。NEC が開発した「パートナーシップネット」というシステム（一般に「プレゼンスサーバー」と呼ばれる）では、「メッセンジャーソフトや電話、メールといった機能がすべて一つのインフラ上に統合されただけでなく、「状態」「場所」「時間」というプレゼンス（ユーザーの状態）もわかる。そこから他の機能が発展できる」。これによって、「社内でも社外でも当該人物が「いま、どこで、何をしている状態か」がリアルタイムでわかる」のだという。（森 p. 264）

こうした職場での監視は、入室時や PC の立ち上げ、データベースへのアクセスなどに伴う認証によって、その後のメールやウェブの利用状況や、IP 化された電話の内容に至るまで、あらゆる履歴が記録され、必要に応じて処理されるのである。また、運送業者であれば、詳細な車の運転状況の把握や、それを通しての運転技術の指導に至るまで、あらゆる面で合理化とリスク対応のための措置がとられている。こうした職場での監視は、それ自体パノプティコン型の監視に含まれる問題も抱えているとはいえ、ここでの監視の結果が、さらに別の監視の結果と結びつけられることこそが、現代的監視の特徴の一つなのである。

2.3　監視における時間性の問題

監視というと、「誰かがある人物やそれに関するデータを、現在進行形で収集している」というイメージがある。つまり監視主体は、たとえ機械化されたとはいえ、まさにその人の行動を視覚的に観察する場合と同様に、そのデータが入力された瞬間に、それを捕らえ、収集するというイメージである。

しかし、現代の監視は、もちろんそのデータが収集される時点では、上記の構造が当てはまるとはいえ、しかし、その収集の主体は、必ずしも監視主体であるある必要はない。監視の主体は、さまざまなデータベースから、さまざまな人物についてのデータを事後的に収集し、他のデータと組み合わせ、処理することによって、特定の人物の姿を作り上げ、人々についてのプロファイルを作り上げるのである。

つまり、現在の監視の主体は、同時的にデータを収集する主体とは切り離されており、事後的に監視の意図を発動させ、【その後】データを収集することができる。監視のためには、絶えず何かを見張っていなければならない。以前であれば、監視は特定の監視主体の特定の意図の下に開始されたのであるが、現在では、データを収集する主体の意図とは別の意図で監視が事後的に行われるのである。

このことが、ユニーク ID をめぐるプライバシーの問題を考える際に重要になる。

3. 監視とプライバシー

従来、監視によって奪われるものは、個人の自由であり、個人が自由に生活を送る際に前提となるプライバシーであると想定されていた。し

かし、上で見たように、セキュリティーの権力によって行われる監視は、むしろ個人の自由を確保し拡大するためにこそ必要とされている。つまり、現在ではプライバシーの確保と自由との関係は、以前のような、プライバシーの確保が自由を保障するというよりは、プライバシーを無視することによってこそ、自由が得られるという関係性の方が強くなっているということになる。

そこで、プライバシーと自由の関係を考える前に、この節ではまずプライバシーと現代的監視との関係を、特に法的な側面を中心に確認しておくことにしよう。

3.1　法概念としてのプライバシーと監視　―「公表」と「個人識別性」をめぐって

プライバシーと監視の関係を、法的側面からもう少し具体的に考えてみよう。

山本が述べるように、これまで、裁判所におけるプライバシー侵害とは、「公表されたくないことを公表されること」だった。「これに対して、ライフログ活用サービスにおいては「公表」は必須の要素ではない。収集し、保存し、分析するなどの利用が問題である。果たして「公表」を欠く場合でも、プライバシー侵害にあたることがあるのだろうか。仮にあたるとすれば「公表」に代わるどのような収集、保存、利用がプライバシー侵害になるのであろうか」。これが第一の論点である。（安岡編 p. 65）

第二の論点は、「個人識別性」の問題である。「既に行われているライフログ活用サービスにおいて、しばしば「個人情報は利用していない」、「匿名情報として利用している」との説明がなされている。これは、「個人識別性のない情報の利用であれば権利侵害は発生しない」ということ

を前提にしているようだが、果たしてそのような前提は正しいのだろうか。」（安岡編 p. 65）

・「公表」とプライバシー

平成 22 年の客室乗務員データベース事件判決において、東京地裁は、「「公表」に代わる侵害行為について、第三者に知られたくない個人に関する情報（裁判所はこれを「プライバシー情報」と呼ぶ）が「一般人の感受性を基準にして人格的自律ないし私生活上の平穏を害する態様で収集、保管又は使用された場合には、そのプライバシー情報の収集、保管又は使用はプライバシーを侵害する違法なものというべきである」と判断した（安岡編 p. 68）。また、平成 13 年の N システム事件での東京地裁判決を評価して、山本は「N システムはプライバシーを侵害する違法なものではないとしたが、ナンバープレートをキーとして移動に関する情報が大量に収集・保存されることの問題性を指摘した点には注目すべきである」（安岡編 p. 68）と述べる。

つまり、たとえ公表されなくとも、「人格的自律ないし私生活上の平穏を害する態様で収集、保管」されるだけで、プライバシーが侵害される得ることが認められているのである。もちろん、その場合、本人の同意や正当な目的がないことが前提となる。

こう考えると、例えば、インターネットの検索履歴や、GPS の位置情報などは、場合によっては人格的自律ないし私生活上の平穏害するセンシティブな情報である場合もあり得る（特定の病気について詳しく調べていたり、あるいはいかがわしい場所に頻繁に出入りしていたりといった場合）。しかし、GPS のスイッチを入れていることは、その情報を収集されることに同意したと言えるのだろうか。言いかえれば、GPS 関連のサービスを受けるには、位置情報を収集されることと引き替えで

なければならないのだろうか。

しかし、ここで重要なのは、上で問題にされているプライバシーとは、あくまでもある種のセンシティブ情報であって、それと関わらない情報は、いくら集められても、それ自体何の問題もないということである。現代の監視の問題が、さまざまな情報のデータベースをつなぎ合わせることによって生じる、新たな個人情報の生成であったことを考えれば、問題は個々のデータベースが、プライバシーを侵害せずとも、そして公表されなくとも、それだけで問題なしとは言えないであろう。

・「個人識別性」とプライバシー

個人のプライバシーに関する情報を公開するとしても、それが特定の個人を識別出来ない場合は、問題とされないことが多い。この個人識別性の問題に関しては、総務省の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が、2010年5月に提出した「第二次提言」に、次のような指摘がある。

> 「個人識別性のない情報であっても、行動履歴等の情報が大量に蓄積されて個人が容易に推定可能になるおそれがあることや、転々流通するうちに個人識別性を獲得してしまうおそれがあることから、現時点で情報に個人識別性がないことをもって、プライバシーとしての保護が完全に失われると考えるのは相当ではない。」p. 45

ここで指摘されているとおり、現代の監視では、コンピュータによって容易にさまざまな特徴が組み合わせられ「名寄せ」されてしまう。したがって、ある時点での匿名情報は、他の情報との組み合わせられる過程で、個人を識別できるようになるかも知れない。特に、匿名化が弱い場合は、個人識別性を再獲得する可能性が高い。したがって宍戸が指摘するとおり、「「照合容易性」の問題は、ライフログを含むデジタル空間

での個人情報の保護にとって、難問になっている」。（安岡編 p. 41）

また、情報公開法５条１号は、「特定の個人を識別することはできないが、公にすることにより、なお個人の権利利益を害するおそれがあるもの」を開示対象から除外しており、「個人識別性のない情報の公開により権利侵害が生じうることが前提」（安岡編 p. 70）となっている。

このように、個人識別性がない匿名の情報であっても、したがって個人情報保護法上の問題がなくても、プライバシーに関わるセンシティブ情報の流通や利用は、プライバシー侵害の可能性がある。

こうした事例から考えると、問題は次のようになる。センシティブ情報ではない、しかも一般に公開はされない情報の収集は問題になり得るか。照合容易性の程度をどのように判定するか。後者は、場合によってはプライバシーの問題とも絡んでくるが、照合によって、センシティブ情報が生成されるのでない限り、プライバシーの問題とは言いにくい面もあるだろう。

その上で、例えば、ライフログとも呼ばれる個人の生活履歴情報の収集は、それ自体プライバシーの侵害に当たるのだろうか。鍵が「照合容易性」にあるとすれば、現在では、SNS 上のライフログに関する情報はほぼ「照合容易」な情報と考えられる。つまり、それを大量に収集し他のデータと照合したり分析したりすれば、場合によっては個人のプライバシーに関する情報が生成されたり、そうでなくとも個人の詳細な人物像が明らかになるであろう。それは、たとえプライバシーの侵害には当たらないとしても、それ自体何の問題もないのだろうか。

これに関して山本は、「問題は将来、われわれが「プライバシー」の名の下に、何を保護してもらいたいと考えるかであろう」とした上で、「事業者にデータをとられないことではなく、漏えいや濫用等に対して有効なリスク・マネジメント・ストラクチャーを組み込んでもらうこと

であり、監視機関の設置を含む、堅牢なシステムの構築要求でもある」という。そして、わが国の最高裁においても、「プライバシー権侵害の有無を査定する一つのポイント」として、「システム構造の堅牢性」が審査されていると指摘する。（安岡編 p. 74）これは、プライバシー保護のための方策を、プライバシー権の保障の要件にしようとするものだが、このことは必ずしもプライバシーを持ち出さずとも、問題にしうるのではあるまいか。

3.2　ユニーク ID とプライバシー

上記のように、「照合容易性」が問題になる状況において、今後ますます問題になるであろう技術が、RFID タグであり、それに付与される固有 ID（ユニーク ID）や識別番号である。この数字の羅列は、プライバシーを侵害するものでも、個人情報でもないただの番号にすぎないと言えるだろうか。固有 ID データが大量に集まると、別のデータと突き合わせて照合することができるようになる、まさに照合容易なデータであり、それを解析することによって個人情報まで同定できる可能性がある。したがって、それ自体は重要でないとされることもある ID 番号は、大量に収集されることで個人情報など重要なデータに変質する可能性をもつものである。時間の経過や数の多さによって、その重要性が変化するわけである。

したがって、例えば「IC タグは単なる商品情報だからプライバシーとは関係ない」と言えるかは、改めて問い直されねばならない問題なのである。IC タグが、いつ、誰によって、何を読み込み／書き込まれ、それによって自分や自分の物に関する情報がどのようにデータベース化されるのかが不明である限り、いつ他の情報と組み合わされ、個人に関する詳細な情報が生成され、利用されるかわからないのである。

こうした現在の日本における消費者の不安の代表的な一例が、下記のような情報収集の例である。

「医薬品購入データ取得　T ポイントで提携の企業から　CCC が販促利用

4 千万人以上が利用する日本最大の共通ポイントサービス「T ポイント」が、ドラッグストアで会員が買った医薬品の商品名をデータとして取得し、会員に十分な説明をしないまま販促活動などに使っていることがわかった。

医薬品の購入歴は一般の商品に比べ、本人が他人には明らかにしたくないことが多い。日本薬剤師会などは「育毛剤を買った人にかつらの広告を送ったり、関節の痛みを和らげる薬を買った人に健康食品を勧めたりしないか」と懸念。厚生労働省も問題視している。」（2012 年 07 月 17 日、朝日新聞）

上記のような例は、医療情報という典型的なプライバシーに関する情報であるが故に不安をかき立てられやすいが、そうでなくとも、カードに固有 ID がついている限り、そこに結びつけられた情報は、照合容易な情報であり、したがって、CCC のようなポイントカードによるライフログ収集は、今後大きな問題になるであろう。

3.3　現代的監視社会におけるプライバシー概念の限界

ライアンは、「プライバシーには、監視を、本質的に社会的な問題ではなく、個人的な関心（不安）に還元する傾向がある」（Lyon2001, p. 4）と述べる。しかし、現代の監視は、単に個人的空間を侵害する手段ではないし、個人のプライバシーを侵害するだけではない。昨今の「プライバシー侵害」への恐れは、主に近代西洋の「所有的個人主義」の産物であるとされる。（Lyon2007, p. 184）

「プライバシーには実際、深遠な社会的側面がある一方で、監視によって今日提起される社会問題を扱うには限られた側面もあり、結果として非常に安易に個人的な事柄として解釈されている。」（Lyon2007,p. 180）

吉田は、ライアンの指摘を受け、「監視とは「社会の秩序編成」「人間集団の分類・類別化」というマクロなレベルで作動するメカニズムであり、その作動の正当性の問題を、個人の「プライバシー」の侵犯の有無というミクロなレベルの問題に還元することはできない」（吉田 2009,p. 8）と述べる。

人々がみずから進んで自分の個人情報企業に提供したり、場合によっては知らない間に同意してさまざまな情報を提供したりしている現在の状況において、プライバシーの概念はどこまで有効なのか。

現在では、人々は監視（防犯）カメラでの撮影や、電車の利用履歴や、カードやウェブの利用によるさまざまなサービスの利用履歴を収集されることにそれほど問題を感じていないように思われる。それは、利用者がその意味を理解していないからであって、誰かが詳しく教えてくれるならば、利用を差し控えたり、カメラを避けたりするようになるというものでもなかろう。履歴を残すことの見返りとして得られる、安心感やサービスの充実の方にメリットが感じられるからである。

さらには、プライベートな空間とパブリックな空間という区別も有効ではない。従来、プライバシーは、まさにプライベートな空間を他人の干渉から守るために必要とされた。逆にパブリックな空間においては、人に見られることは当然であり、それが問題にされることはあまりなかった。しかし現在では、家の中ですら、ネットとつながったある種の公共空間であると言える。また、パブリックな空間においても、そこでプライバシーが問題にならなかったのは、情報の収集コストが非常に高く

つくため、個人の行動を逐一監視することが困難であったからである。現在では、その収集のコストは劇的に低くなった。監視カメラが普及しはじめた頃には、パブリックな空間におけるプライバシーが問題にされるようにもなったが、もはや今では、監視カメラに違和感を抱く人もそれほど多くなくなっている。つまり、従来であれば、プライバシーとして秘匿された個人の生活スタイルや行動パターンなどが、空間の区別なく公開されつつあると言える。

個人情報保護の重要性は変わらないとしても、それはプライバシーを守るためというよりも、さまざまな悪用による問題を避けるため、すなわちリスク回避のためという意識が強いだろう。逆に言えば、プライバシーは、知られたら恥ずかしいと感じる情報や、いわゆるセンシティブ情報以外は、プライバシーの問題とは感じにくいということであろう。

それはちょうど、図書館司書に自分の思想傾向がどのようなものかを知られることに問題を感じなかったのと同じで、例えばamazonのような通販サイトにどのような図書を読んでいるかを知られても気にしないのと同じようなものだろう。だがもちろん、図書館司書には、その情報を漏らさない義務があったのに対して、amazonにはそうした義務はない。この重要な点で異なるとはいえ、人々の意識の中では、amazonが過去の注文履歴から私にお薦めの本を表示してくれることの便利さと引き替えに、自分の思想傾向や趣味などを知られることには、問題を感じないということだろう。それによって直接の不利益を受けるわけでもなければ、恥ずかしいことでもないのだから。

上記のように、これまで「第三者に知られたくない」情報を「一般人の感受性を基準にして人格的自律ないし私生活上の平穏を害する態様で収集、保管又は使用された場合」に、プライバシー権の侵害と考えられてきた。しかし、この「一般人の感受性」が変化してきており、何が

「人格的自律」や「私生活上の平穏」を害するかは、元々曖昧であったとはいえ、現在ではさらに曖昧になっていると言える。上記の例でいえば、今や「育毛剤を買った人にかつらの広告を送ったり、関節の痛みを和らげる薬を買った人に健康食品を勧め」たりすることの何が問題なのかと感じる人も多いだろう。T ポイント加盟店で買い物をしている限り、当たり前ではないのか。amazon がやっていることと何が違うと言うのか、と。

したがって、上記のように、日本の法律上は、プライバシーの権利を根拠にした個人情報の日常的な大量収集とそのデータベース化への抵抗は、不可能ではないとしても、それが「一般人の感受性を基準に」するものである限り、その根拠としての力は弱まる一方であるように思われる。それは、われわれが従来プライバシーとされていたある部分を、今やプライバシーとは感じなくなっているのであるから、それで全く問題はないということなのだろうか。そうではないとすれば、監視社会の問題を考えるには、プライバシーという概念とは別の根拠が必要なのではないだろうか。

4. 現代的監視社会の問題

これまでに確認したことは、現代の監視社会の問題を考える際には、従来の管理社会論で問題にされたような、管理強化による個々人の自由の圧殺や、プライバシー侵害の問題だけでは十分ではないということだった。ではその上で、監視社会にはいったいどのような問題があるだろうか。現代の監視の問題を考える際に、その社会的影響という観点からの考察が必要であることは、既にローレンス・レッシグやキャス・サンスティーンらの有名な論考がある。

例えば、キャス・サンスティーンは、パーソナライゼーシヨン、つまり収集した個人に関する情報を基に、その人に最もふさわしい情報やサービスを提供するしくみが極度に進むことによって、次のような問題が生じると言う。人々は、自分が知りたい情報にしかアクセスしなくなる。また、同じような関心を持つ人々とだけ交流するようになり、その結果、そうしたグループ内での情報は頻繁にやりとりされる反面、その外にいる人々とは情報共有されにくくなり、社会で人々に広く共有されるべき情報が行き渡らなくなる。つまり民主主義を支えるために必要な市民として知っておくべき情報が共有されにくくなる。そして、政治的・社会的な判断を下す際に必要とされる公平な視点からの自らの政治的立ち位置を理解できず、自己中心的な視点から集められた情報を基にした意見のやりとりに終始し、次第に民主主義を支える市民による議論の土俵が掘り崩されていくというのである。

また、憲法学者のローレンス・レッシグは、サイバー空間では、今後ますます規制が強化され、私たちの自由はますます脅かされるとし、サイバー空間をコントロールしようとするコード、すなわちサイバー空間でのわれわれの行為を一種の物理的な仕方で規制しようとする機能が、企業や政府によって管理されているとき、自由を守るにはどうすればいいのかを論じる。

これらは、必ずしも監視の問題に焦点を絞っているわけではないが、コードによる規制が、さまざまなパーソナライズ化した情報サービスによって、より細かにわれわれの考え方、生き方に介入してくることの問題を考えれば、どちらも監視社会の問題と密接に結びついていることが分かる。

ここでは、こうした指摘について詳細に論じる余裕はないが、それらとも結びつく問題として、ライアンが主として指摘するソーシャル・ソ

ーティングの問題について詳述しておく。

4.1　ソーシャル・ソーティング（社会的振り分け）について

ガンジーは、1993年の著書において、国家や企業によって取得された情報によって、個人がさまざまな形で「値踏みされ、選別され」る「差別的な個人評価プロセス」を「パノプティック・ソート」と名付けた（ガンジー p. 3）。

それは、「先端技術を利用した人工頭脳工学に基づく選別プロセス」であり、効率と合理性を求めて個人を識別、分類、評価、選別することを目的とし、「個人あるいは集団が、その推定上の経済的・政治的な価値に基づいて分類されていく」のだとしている（ガンジー p. 4）。

ガンジーは、パノプティック・ソートによる情報取得を、「本人の自己決定権や、自己へのアクセスをコントロールする権利の侵害」であり、「個人の尊厳を傷つける」（ガンジー p. 207–8）、言いかえれば個人のプライバシーを侵害するものであると考え、このシステムを「人間の存在を合理化し管理すること」を唯一の目的とする、「反民主主義的管理システム」であると、また「差別を具体化・制度化し、さらにはその差別を鋭く明確化する差別的技術である」と評価する（ガンジー p. 234–5）。

ただし、ガンジーが、プライバシーの核心を個人の自己決定権や尊厳と密接に関係づけている点は正しいとしても、それが情報の取得そのものに起因するものだと考えられている点で、パノプティック・ソートの分類・選別システムとしての本質と、プライバシーの侵害がどのように結びついてはいるのかは明確ではない。とはいえ、パノプティック・ソートの問題を、差別を制度化するものとしての社会的制度の観点から評価している点には留意すべきであろう。

既に述べたように、現代の監視は、従来のある特定の個人を対象にし

た単純な監視から、大量の電子データを解析することによって、広く全ての人々を対象にして行われるデータ解析型の監視であるという点で、まさにパノプティック・ソートと言ってよいものである。

それは、国民一人ひとりが異なる傾向や属性を持つことを積極的に承認しつつ、リスクの対象となった者を排除するところに特徴があった。その判定基準となるのは、決して生身の本人ではなく、収集されたデータによって構築された人格である。こうしたプロファイル化された人格のことは、「データ・ダブル」・「データイ・メージ」・「データ・ペルソナ」など、さまざまに表現されているが、現代の監視は、こうしたデータ人格を生成するところにその特徴があると言ってもよい。

そしてこのデータ人格の特徴に応じて、分類・選別し、カテゴリーごとに扱いを変えるのである。この扱いは、その対象となる本人が実際にそのような性質を持っているかとか、本当にそれを求めているか、あるいは拒否しているかとは関係なく、一方的に提供されるのである。場合によっては、それはが間違った情報によって作り上げられたデータ人格かもしれないのである。つまり、本人ではなく、データ人格こそが、本人に対する扱いを決定するのである。こうしたデータ人格が、企業の人材採用の際の資料とされることも米国では増えていると言う。あるいは、保険会社がリスクに応じて個々人の保険料を変えたり、国家の指示で航空会社がある個人の航空機への搭乗を止めたりする、しかも本人にはその理由が分からないといったことも、あり得る一例になるだろう。このように、企業や国家がデータ人格を用いて、個人の取扱を決定する、しかもそのことを本人には知らせずにそうすることは、大きな問題を孕んでいる。

したがってデータ人格は、個人の選択と、さらには個人の自己同一性をも規定する一因となっていると言ってよいが、これはプライバシー侵

害とは違った形での、個人の主体性・尊厳への侵害と言えるのではなかろうか。

さらに、こうしたデータ人格による分類と、それを基にした個々人の差別化は、いわゆる格差を拡大させる方向で機能する。リスクへの対応としての差別化は、いったん失敗した者がそれを挽回することを妨げ、成功した者をさらに優遇するからである。そこにはもちろん、従来からのマイノリティーや社会的弱者も含まれるが、そうした人々を包摂する社会ではなく、排除する社会へと向かっていくこととなる。

情報化の進展にともない、膨大な情報の中から自分が求めるものを見出すのには大変な時間とコストが必要となる。その際、データ人格に基づいてパーソナライズされた情報の提供は、今後ますます人々に求められることになるのではなかろうか。しかし、それによって人々は知らず知らずに、自ら主体的に考え、自己決定することを放棄して、企業の「お薦め」に依存し、掲示板の有力な主張に同調し、広い視野からの社会批判ができなくなるのではないだろうか。さらには、サンスティーンが指摘したような、集団分極化にともなう民主主義の危機がおとずれ、レッシグが指摘したように、人々はコードが規定する一定の範囲内での自由を、特に不満に思うこともなく受け入れるようになるのだろうか。

いずれにせよ、監視社会は、こうして個人の人格の尊厳を脅かすだけでなく、社会のありかたをも、自由や平等や民主主義を支持する者にとっては望ましくない方向へと導くもののように思われるのである。

5. 監視社会への対応と、専門家の役割

こうした問題を孕む監視社会に、私たちはどのように対処すべきなのであろうか。監視を避ければすむのだろうか。とはいえ、現在の状況で

は、それはほとんど社会生活をあきらめるということでしかない。

最も重要な課題は、監視の透明化への努力である。とはいえ、個々人のデータがどこでどのように収集されたのかまでも含めて、全てを明らかにすることは容易ではなかろう。少なくとも、個人を分類・選別する際に利用されたデータ人格がどのようなものであるのか、その内容を本人が確認し、場合によっては修正する権利を確立することだろう。

そしてそのためには、データ人格の利用のされ方そのものを監視する、中立な専門的第三者機関を設置すること、また同時に、情報処理や情報と社会との関係について研究する専門家と市民との対話の場を設けることが必要になると思われる。

それは、一つには、データ人格の利用による人権侵害が生じないよう、企業や国家のデータ利用について監視し、場合によってはその開示を求めるための窓口となる機関が必要となるからである。また同時に、将来の監視社会のあり方について、技術的にはどのようなことが可能になり、またそれが社会にどういう影響を及ぼし得るのかについて、あり得るいくつかの将来像を示し、市民が主体的にそれを評価することができるようにする、つまりは望ましい将来の社会像を選択するための手助けをするためにも必要となるだろうからである。

情報社会における専門家の役割にはあいまいな部分もあるが、だからこそ、監視社会を監視する公正な機関を設け、最も問題となる監視の複合体によって、どれほどの個人情報がデータ人格を生成することに寄与しているかを明らかにし、社会にその問題性を問う必要があるだろう。いわゆる、データの売買、使い回しの過程で、不当に誤ったデータ人格が生成されないよう、またたとえ正確であったとしても、人種による差別のように、その特徴を用いること自体が人権侵害であるようなデータの利用等が生じないよう監視する必要がある。

プライバシーの感覚は、個人差があるため、どれほどの情報の収集がプライバシーの侵害だと感じるかは、一概には判断出来ない。そのため、どの情報はオプトアウトで利用出来るのか、あるいはオプトインでなければそもそも収集出来ないようにした方がいい情報とはどのようなものか、これらについて、専門家と市民の対話の場を設け、さらには個々人ができるだけ自分自身で情報をコントロールできるようなしくみを作ることが必要であろう。

「「コード」を可視化し、非専門家とのコミュニケーションの俎上に載せることが、〈情報公共圏〉における専門家の役割として期待される」という吉田の指摘は、この意味で重要である（吉田 p. 11）。

今後、企業や国家は、リスク排除のためにますます個人データの収集に努め、人々の特性に応じた消費への欲望を促し、また社会に安全をもたらそうとする。しかし、われわれには、そこで利用されるデータがどのようにプロファイル化され、分類され、評価されるのかが明らかではない。それをできるだけ透明化することなしには、われわれの自由と尊厳が侵害されるおそれは拭いがたい。監視の透明化は、「健全な民主主義と人間の尊厳に不可欠」なのだ（Lyon2007 p. 182）。

しかし、現在の状況において、監視を透明化することがどこまで可能なのか。市民一人ひとりでは、とても不可能な課題である。ここに、情報の専門家の役割がある。監視を透明化し、市民との対話によって、監視の複合体、つまりはデーベースの連結によって、不当な個人の差別化および社会の格差拡大を防ぎ、自由と民主的な議論の土俵を守るための役割が求められるのである。

参考文献

青柳武彦（2006）、『サイバー監視社会』廣済堂

遠藤薫（2008）、「リスク社会と監視社会」、『学術の動向』2008 年 11 月号

小澤照彦（2006）、「民主主義の倫理と情報化社会」、『ぷらくしす』No.8

岡本裕一朗（2005）、『ポストモダンの思想的根拠―9・11 と管理社会』ナカニシヤ出版

ガンジー（1997）、『個人情報と権力―統括選別の政治経済学』同文舘出版（Gandy, O. H.（1993）, *The Panoptic Sort: A Political Economy of Personal Information*, Westview.）

田畑暁生（1999）、「管理社会論と情報社会論」、『神戸大学発達科学部研究紀要』6（2）

―― （2003）、「監視社会論とその射程」、『人間科学研究』10（2）

サンスティーン（2003）、『インターネットは民主主義の敵か』毎日新聞社（Sunstein, Cass R.（2001）, *Republic.Com*, Princeton Univ Pr.）

原一樹（2005）、「監視社会化の何が問題か」、松永澄夫編『環境　安全という価値は…』東信堂

ボガード（1998）、『監視ゲーム―プライヴァシーの終焉』アスペクト（Bogard, W.（1996）, *The Simulation of Surveillance: Hypercontrol in Telematic Societies*, Cambridge Univ. Press）

ポスター（1991）、『情報様式論：ポスト構造主義の社会理論』岩波書店（Poster, M.（1990）*The Mode of Information* : *Poststructuralism and Social Contexts*, Polity.）

森健（2012）、『ビッグデータ社会の希望と憂鬱』河出書房新社

安岡寛道編（2012）、『ビッグデータ時代のライフログ』東洋経済

吉田純（2010）「情報ネットワーク社会における〈監視〉と〈プライバシー〉」、『システム／制御／情報』54（6）

レッシグ（2001）、『CODE ―インターネットの合法・違法・プライバシー』翔泳社（Lessig, L.（1999）, Code: And Other Laws of Cyberspace）

Clarke, R.（1988）, 'Information Technology and Dataveillance', *Communications of the ACM* (31), pp. 29–45.

Dandeker, C.（1990）, *Surveillance, Power and Modernity*, Polity.

Lyon, D.（1994）, *The Electronic Eye: The Rise of Surveillance Society*, Polity.

―― （2001）, *Surveillance Society: Monitoring Everyday Life*, Open University Press（ライアン（2002）、『監視社会』青土社）

―― （2007）, *Surveillance Studies: An Overview*, Polity（ライアン（2001）『監視スタディーズ』岩波書店）

Marx, G. T.（1985）, 'The Surveillance Society: the threat of 1984–style techniques', *The Futurist*, June: 21–6.

Packard, V.（1964）, *The Naked Society*, David McKay Co.