「快適で安全」な監視社会　― 個人の自由が保障されなくていいのか

小泉雄介　こいずみ・ゆうすけ
一九七一年生まれ。国際社会経済研究所主幹研究員。東京大学教養学部科学史および科学哲学分科卒、同大学院総合文化研究科中退。著書に『国民ＩＤ』（共著、ＮＴＴ出版）、『現代人のプライバシー』（共著、ＮＥＣ総研）など。

（『世界』第 921 号（2019 年 6 月号）掲載　©岩波書店）

暮らしの「便利」を支える超情報社会

情報社会の進展によって、「個人データは二一世紀の新たな石油（価値あるリソース）である」と言われるようになった。昨今では、申込用紙などの紙媒体やインターネットの入力フォームといった従来の手段に加え、スマートフォンや身につけたまま使えるウェアラブル端末、ＡＩ（人工知能）スピーカー、ボディカメラといった様々なＩＴ機器を通じて個人データが取得されている。これらの個人データは、ソーシャルネットワーキングサービス（ＳＮＳ）、ニュースサイト等のパーソナライゼーション（個々人に応じて情報がカスタマイズされること）、ショッピングサイトでの「ほしい物／受けたいサービス」のレコメンデーションなど、消費者にとって利便性の高いサービスを安価に提供するために使われたり、防犯・防災、健康医療、交通・物流、都市計画など各領域での社会的課題の解決にも利活用されたりしている。

ＳＮＳの交流サイト「フェイスブック」で手軽に友人とコミュニケーションし、検索エンジン「グーグル」で知りたいことを即座に検索し、インターネット販売の「アマゾン」で買いたい物のクチコミ情報を調べて購入することで、我々は従来考えられなかったような「利便性・快適さ」を享受している。マンションに防犯カメラを設置し、自家用車に車載カメラを付け、ウェアラブル端末で日々の健康を管理することで、以前にも増して「安全・安心」な生活を送ることが可能となっている。

その反面、自分に関するありとあらゆるデータが吸い上げられ、行動を管理するために利用され、「自由」が脅かされていることについては、ほとんど気付くことがない。本来、個人の「自由」と、個人の「安全」「利便性」「平等」は、我々の社会において尊重されるべき基本的な価値である。しかし現代社会では、「自由」と、「安全」「利便性」「平等」とは、一方を追求すれば一方を犠牲にせざるを得ない関係にあるのだ。

監視社会の真っ只中にいる私たち

これまでに挙げたＩＴ機器（スマートフォン、ウェアラブル端末、ＡＩスピーカー等）や

防犯カメラ・ボディカメラなどの技術は、個人からデータを絶えず取得し、個人の行動を追跡することに使われうることから、「監視技術」の一種と言える。従来は個人の監視を行なう主体といえば行政機関であったが、インターネットが普及した一九九〇年代以降は民間企業による消費者の「監視」が加速的に増えており、とりわけＧＡＦＡ（米国に本拠を置く巨大ＩＴ企業の総称：グーグル、アマゾン、フェイスブック、アップル各社の頭文字を取っている）に代表される「プラットフォーマー企業」が国境を越えて大量の個人データを取得している。

特に米国では、二〇一三年のスノーデン事件（米国中央情報局元職員エドワード・スノーデン氏が米国政府によるインターネット企業からの個人データ収集プログラムの存在を暴露した事件）で明るみに出たように、行政機関と民間インターネット企業が手を組み、いわば「ビッグブラザー」として世界中の個人から莫大な量の個人データを取得し、これらにアクセスすることが可能となっている。

一方で我々は、社会生活を送る上でこれらの「快適で安全」な監視技術に大きく依存している。自分の行動の監視につながるということが明示的には意識されずに、消費者が自ら進んで自分を識別するＩＤ（各種のカード、スマートフォン、生体情報等）を提示し、利便性や快適さを享受する場面が増えている（店舗での支払い、レジャー施設への入場、会員向けサービスの利用等）。ＳＮＳなどで、就職を含む「社会参加」のために自らの個人情報を世間に公開することも珍しいことではなくなった[1]。このように、現代社会では様々な監視技術が社会生活に不可欠な構成要素として組み込まれ、受容されている。我々は監視社会の真っ只中にいる。

フーコーとドゥルーズの監視社会論

監視社会論では、フーコーのいう「規律社会」と、ドゥルーズのいう「管理社会」の対比がよく取り上げられる。フーコーの「規律社会」では、「パノプティコン」（英国の哲学者・ベンサムが構想した単一視点から全体を監視できる刑務所施設）における規律訓練を通じて、個々人における「規範の内面化」を促し、社会規範を自発的に守らせようとする。

他方、ドゥルーズの「管理社会」[2]では、個々人の「規範の内面化」のプロセスに頼ることなく、個人の属性や資格などのデータに応じて、その行動を直接的に管理しようとする。これは、情報システムなどの中に「規範」を設計段階からあらかじめ組み込んでしまうことで、社会の構成員に自動的に規範を守らせてしまう方法である。たとえば、鉄道会社が、乗客のキセル（無賃乗車）を防ぐために、改札を自動改札にすることで、キセルという行動自体を不可能にするのがこの方法である。このような社会では、場における個人の行動の生起がコントロールされ、望ましくない行動や出来事は（情報システムの事前設定によって）未然に防がれるようになる。ＩＤや生体認証技術を用いた入退管理システムや異常行動検知システム、あるいはプロファイリング技術を用いた顧客管理システム（たとえば購買履歴に

基づくレコメンデーション、信用スコアに基づくサービス差別化）等は、こうした「管理社会」を強化するためのツール（監視技術）であると言える。

公共空間ですすむ監視カメラによる顔認識

本稿では、議論のある監視技術として、まず監視カメラと顔認識技術について取り上げたい。公共空間（公道など）や私的空間（店舗など）におけるカメラの設置および顔認識技術の導入は、それが適切に行内務省われる限り、治安の向上や消費者向けサービスの向上など、様々な便益を我々にもたらすものである。しかし、現時点では顔認識技術が社会に出始めたばかりであるため、十分なルール作りがなされていない状況にある。

英国ではいくつかの地方警察が、監視カメラと顔認識技術を用いて、特定イベントにおける参加者の顔画像と犯罪者データベース等の顔写真とをリアルタイムに照合する（自動顔照合）という実証実験を行なっている。レスターシャー警察の事例では、二〇一五年六月の屋外音楽イベント（ロックフェスティバル）で一〇万人の一般観衆相手に自動顔照合が行なわれ、同警察が保有する拘留者データベースおよび欧州刑事警察機構から得た国際犯の顔写真データベースと照合されていた。ロンドン警視庁の事例では、二〇一六年八月のノッティングヒル・カーニバルで自動顔照合が行なわれ、照合にはカーニバルへの参加を禁じられた人や、犯罪を行なうためにカーニバルに参加する可能性があるとして警察が指定した人（組織犯罪者等）のデータベースが用いられた。南ウェールズ警察の事例では、カーディフで開かれた二〇一七年六月の欧州サッカー連盟チャンピオンズリーグ決勝戦において、組織犯罪者・違法チケット販売者・フーリガンなど五十万人のデータベースを用いて自動顔照合が行なわれた。

これらは警察による自動顔照合実験であるが、民間による取り組みもある。ロンドンのキングスクロス駅前では、東京ドーム六個分の広さの土地で再開発が進められており、大学や企業、マンションなどが建設される予定になっている。この再開発の敷地内には不動産会社保有の二四〇台のカメラが設置され、センターで集中管理されている。筆者が二〇一七年六月に訪問した際には、敷地内で自動顔照合実験が行なわれており、不動産会社は警察から犯罪者や行方不明者の顔写真を含む人物データを受領していた。担当者によれば、欧州の公共空間で初めての「常時」自動顔照合とのことであった。

英国におけるこのような公共空間での自動顔照合には、プライバシー団体やデータ保護監督機関から様々な懸念が挙げられている。問題とされる一つ目の点は、顔照合の対象となる市民、個人への透明性の欠如である。英国の監視カメラコミッショナーによれば、「レスターシャーの事例では、自動顔照合を行なうことに関する通知はチケットの裏面に小さな文字でなされたのみであり、それに気付いた参加ミュージシャンが反対声明を出すなど、かなり大きな問題になった」「自動顔照合の問題は、市民は撮影されていることには気付いても、データベースと照合されていることについてはわからないことだ」とのことである。

二つ目は、顔照合データベースの内容に関わる点である。これらの事例では顔照合するデータベースの内容について公表されなかったため、自分も対象者に含まれているのではないかと思った市民も多かった。また、英国の警察では拘留者全員の顔写真（二〇〇〇万人分）を保持しているが、無実となった人のデータも継続的に保持しており、こうした人も顔照合データベースに含めていることへの批判もある。

三つ目は、顔認識技術の有効性に関する点である。英国の生体認証監督機関によれば、「自動顔照合が本当に犯罪防止に役立っているのか、どれほど正確なのかといったことのエビデンスがまだ足りない」とのことである。

四つ目は、顔認識技術は他の個人データ取得技術に比べてプライバシー侵害リスクが高いという点である。英国議会の二〇一八年の報告書は、「顔画像はＤＮＡや指紋その他の生体認証技術よりも遥かに顕著な特徴を持ち、顔画像の取得・利用・保持には重大な倫理的問題が存在する」と指摘しており、その理由として、「顔画像は本人が知ることなく容易に取得され保持されうるからである。また、顔写真データベース（パスポート、運転免許証、拘留者画像）は既に成人人口の九〇%をカバーしているからである」としている。

五つ目は、意思決定者に関する点である。前述の英国議会の報告書には、「顔認識技術のような重要な分野においては、その広範な導入に関する最終的な意思決定は警察ではなく、大臣や議会が行なわなければならない」と書かれている。なお、英国では英国議会の提言を受けて、二〇一八年七月に、警察での自動顔認識技術の利用を監督する「監視・諮問委員会」が立ち上げられている。

米国では、アマゾンが「リコグニション」という自動顔照合システムを地方警察に販売しているが、米国自由人権協会（ＡＣＬＵ）等の市民団体は二〇一八年五月、二つの警察（フロリダ州オーランド、オレゴン州ワシントン郡）がリコグニションをボディカメラと地域監視で用いたことに関して異議申立てを行なった。訴えでは、同システムはリアルタイムの市民監視を可能にし、学習用データが白人に偏っているため黒人などのマイノリティに不利に機能するとして、同システムの販売を停止するように要求している。さらに同年六月には、アマゾンの有志社員が、リコグニションの捜査機関への販売と移民税関捜査局へのサービス提供中止を求める書簡を同社のベゾスＣＥＯに送っている。

他方、マイクロソフトは二〇一八年十二月、ブラッド・スミス社長兼ＣＬＯのブログで、米国政府に対して顔認識技術の法規制を求めるという画期的な提案を行なっている。同社は、顔認識技術の乱用されるリスクとして、「顔認識の特定の利用法がバイアスを含み、違法な差別を含む意思決定を生み出すリスク」「顔認識の広範な利用が人々のプライバシーを侵害する可能性」「政府による大規模監視のための顔認識利用が民主主義の自由を損なう可能性」の三つを挙げ、特に三点目のリスクに対して、警察が仮に特定個人の公共空間での継続監視を行なうのならば、特定の監視に対する裁判所命令を取得できた場合などに限定すべきとしている。

このように、近年、海外において公共空間での自動顔照合システムの導入事例が散見され

るようになったが、その先駆けとなっている英国においても、未だ社会的なコンセンサスが十分に取られていない状況である。あまり想像したくはないが、万が一、日本において公共空間での自動顔照合システムを導入するようなことになった場合には、住民のプライバシーへの影響が甚大であるため、大規模イベント時など期間と場所を限定した利用に留めるべきであろう。また、プライバシー影響評価（ＰＩＡ）等を通じて、事前に住民への周知徹底や社会的コンセンサスの獲得を十分に行なうべきと考える。

すべての消費者はプロファイリングされている

次に、人工知能（ＡＩ）やビッグデータ分析技術を用いた「プロファイリング」について、取り上げたい。

プロファイリングとは、大まかに言うと「ある人物について、既知の情報から、その人物の既知でない情報を推定したり、将来の行動やリスクを予測すること」である。たとえば、ある人の購買履歴から、その人の収入・趣味・購買傾向・人種・宗教・持病等を推測することなどはその典型的例である。プロファイリングについてはＥＵの新たな個人データ保護規則（ＧＤＰＲ）でも規定されており、それによると、「自然人と関連する一定の個人的側面を評価するための、特に、当該自然人の業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置および移動に関する側面を分析又は予測するための、個人データの利用によって構成される、あらゆる形式の、個人データの自動的な取扱い」（個人情報保護委員会の仮日本語訳）を意味する。あるいは、米国政府のビッグデータ報告書では「小さなデータを寄せ集めて、個人のプロファイルを作り上げ、その個人の好みや行動を予測する」ことと説明されている。

プロファイリングの事例としては、前述のニュースサイト等のパーソナライゼーション、ショッピングサイトでのレコメンデーションのほか、利用者のネット上での行動履歴にもとづくターゲティング広告などが挙げられる。これらは利用者の欲しい情報や関連性の高い情報だけを取捨選択して提示するという点で、利用者の手間を省き、「利便性」の向上に大きく役立つ技術である。その反面、プロファイリングに対しては、個人のプライバシーや自律性といった観点からいくつかの課題が指摘されている。

まず、プロファイリングによって本人の望まないデータまで推測される可能性がある。ビッグデータやＡＩによって推測精度が上がることにより、プロファイリングで推測したデータは限りなく当人の個人データと同等なものになる。これにより、本人から直接取得できないデータ、本人が開示したくない属性・趣味・健康状態・年収といったセンシティブなデータについても、「個人データの取得」と実質的に同等な推測が可能になってしまう。著名な例としては、米国のスーパーマーケットが、ある十代女性の購買履歴から「妊娠している可能性が高い」とプロファイリングし、自宅に（家族がその事実を知る前に）妊娠に関連する広告が送られてしまった事例がある。また、ケンブリッジ大学の研究によれば、フェイス

ブックの「いいね！」の履歴と他の情報を組合せることで、男性利用者の性的指向の八八%、利用者の民族的素性の九五%、利用者がキリスト教徒かイスラム教徒かの八二%を正確に推測することができたという。

他にも、プロファイリングは本人の自律性を侵害する（自律的な意思決定を妨げる）可能性がある。たとえばターゲティング広告やパーソナライズされたウェブコンテンツは、いわゆる「フィルターバブル」を生み出す恐れがある。フィルターバブルとは、ネット空間において個人の好みに合わない情報がフィルタリングによって排除されることにより、利用者が自らの好みに合った情報のみに「泡」のように取り囲まれることを指す。単に自分の好きな情報に囲まれるだけであれば弊害は少なそうに見えるが、操作された情報が個人の意思決定に影響を及ぼし、ひいては民主主義のあり方にまで影響を及ぼすとなれば、話は別である。

二〇一六年の米国大統領選挙でトランプ陣営は、データ分析会社による有権者のプロファイリングに基づき、個々の有権者の心理学的属性等に合せたマイクロターゲティング広告（個別広告）を特定の地域でテレビや電子メール、ＳＮＳを通じて投入した。この大規模な政治広告によって、投票行動の誘導が行なわれ、選挙結果がトランプに有利に働いたとも言われている。

とはいえ、これらの課題に対しては、個人への透明性を向上させるという観点から対処することは可能である。そもそも本人が知らないところでセンシティブなデータの推測（プロファイリング）が行なわれているとするならば、そのような個人データの取扱いは透明性に欠けたものと言える。プロファイリングによって通常の個人データから要配慮個人情報や、本人が知られたくないような情報（年収・嗜好・健康状態等）を推測しようとする事業者は、自主的な取り組みとして、プライバシーポリシー等においてその旨と利用目的を消費者にしっかり告知することが重要であろう。また、ウェブ上でコンテンツのパーソナライゼーションを行なう事業者は、自主規制として、自らのサイトで表示される記事や検索結果に個人差や偏りがあるという事実を消費者に対して積極的に開示したり、表示結果を「ニュートラル」なものするための設定方法を説明したりすることが求められるだろう。

途上国における住民登録とＩＤカードの必要性

続いて、途上国における住民登録や国民ＩＤカードを用いた行政サービス提供について取り上げたい。筆者はこれまで中南米からアフリカまで十七カ国の途上国で現地調査を行なった。

途上国においては、日本や欧米といった先進国とは異なり基本的な住民登録に不備があるために、特に地方部の住民が様々な公共サービスを受けられずにいるケースが少なくない。たとえば乳幼児が予防接種を受けていなかったり、就学年齢の児童が義務教育を受けていなかったり、農家が肥料やプロパンガス等の給付を受けられなかったり、身分証明書がな

いために銀行口座を開設できなかったり、就職が不利になったり、選挙人名簿が不正確なために公正な選挙が行なわれなかったり、といった問題が生じている。このような問題に対処するためには、子どもが生まれた際の出生登録と、成人した際の身分証明書（国民ＩＤカード）の発行を確実に行なうことが極めて有効な対策である。出生証明書を持ち、公的な身分証明書を持つことによってはじめて、住民は社会や経済活動への参加を果たすことができる。

このように、個人が「平等」なソーシャルインクルージョンを実現するため、すなわち「公平」に社会保障・医療・教育などの公共サービスを受けたり、選挙権を行使したり、就職したり、銀行口座を開設したりするためには、そもそも住民登録や国民ＩＤカードの取得が必須である。さらに、出生登録台帳に不備がある[3]多くの途上国において、成人時の国民ＩＤカード発行に当たっての二重登録（同じ人が二回以上登録したり二人以上の名義で登録すること）を防ぐためには、本人の指紋や顔写真といった生体情報を活用することが効率的な方法となる。

しかしここで議論になるのは、国民ＩＤカードの発行に当たって指紋を採取するほとんどの国が、十指すべての指紋を採取するということである。住民の指紋は二重登録防止の目的のほか、指紋を用いたオンラインでの個人認証サービス（たとえば銀行口座開設時の本人確認）に使われることもある。しかし、これらの目的であれば十指の指紋すべてを取る必要はなく、より少ない数で十分なはずである。住民から採取した指紋のデータベースを警察と共有したり、警察にアクセス権を与えている国も多い。こうした国々では、犯罪捜査においても利用できるように、住民から十指の指紋を取っているのである[4]。

先進国で住民の指紋登録を行なっている国は韓国等を除いてほとんどないが、他の行政目的で登録された顔写真が犯罪捜査に流用されているケースはある。

米国では、連邦捜査局（ＦＢＩ）やニューヨーク市警などで捜査支援のために顔認識技術が利用されている。ＦＢＩは刑事司法情報サービス課の下にＦＡＣＥという顔画像分析ユニットを持ち、ここではＦＢＩにおける捜査の支援のために、ＦＢＩが独自に保有する顔認識システム約三〇〇〇万人分のデータのほか、国務省が保有するパスポート申請者（米国人）とビザ申請者（外国人）の顔写真データ、一八の州が保有する運転免許証等の顔写真データにアクセスしたり照会をかけたりできる。これらのデータは二〇一七年時点で合計一億二五〇〇万人分（米国成人の五十一%相当）になるという。

運転免許証やパスポート申請時の顔写真を犯罪捜査に使うことは明らかな目的外利用である。さらに、照会にあたっては令状も必要とされていないことから、米国のプライバシー団体が懸念を表明している。

監視社会化に歯止めをかけるために

フーコー的な「規律社会」とドゥルーズ的な「管理社会」を対比する視点から見ると、「管

理社会」においては、その場に往来するすべての個人に対して「規範の内面化」を必要とせず、情報システムや建物の設計等によって個人の行動をコントロールし、不都合な行動や出来事は未然に防止することが管理者によって目指される。このような管理社会の姿は、途上国において最重要な社会課題の一つである治安対策と極めて親和性が高い。「管理社会」（＝監視社会）では個人の自由よりも社会全体の安全（セキュリティ）に重きを置くことになるが、社会課題の多い途上国においては、まず情報システム等の導入を通じて個人の管理を強め、治安の向上に努めざるをえないからだ。「安全」や「平等」といった個人にとっての基本的価値が十分に実現されていない途上国においては、ドゥルーズ的な管理社会によって、もう一つの基本的価値である「自由」を制限せざるを得ない面もあろう。

しかし、治安対策の必要性が相対的に低い先進国においては、行き過ぎた監視社会化と、それによる個人の自由への侵害に対して一定の歯止めをかけることこそが喫緊の「社会課題」であろう。ＧＡＦＡ等のプラットフォーマーが大量の個人データを集めることで消費者に提供している利便性に関しても、フェイスブックの個人データ流出事件（フェイスブック上で動くアプリの開発者が五〇〇〇万人の利用者データを不正に第三者に販売した事件）などを受けて、その一極集中的なデータ利用に厳しい目が向けられるようになっている。

では監視社会化に少しでも歯止めをかけるとするならば、どうしたらよいのだろうか。筆者は、個人データ取得技術を用いたあらゆるシステムにおいて、一つの場における単一視点（パノプティコンとしての管理者）の占拠を許さず、複数視点の共存を可能とするような制度設計が必要と考える。単一視点による管理を排除し、個人に複数視点を移動することの「自由」を保障すること、すなわち、個人が単一の管理者に縛りつけられるのではなく、自分の個人データを取得し管理する管理者を選べるようにすることである。そのような複数視点間の移動の自由が保障された場においては、「ビッグブラザー」に見張られることによる萎縮効果がなくなり、様々な社会集団やコミュニティ間での領域横断的な交流、自分の所属する集団を超えた「他者」との交流が促進されるだろう。また、インターネットなどのバーチャルな世界で、あるいはリアル世界でも、いくつもの自分（ペルソナ）を生きたり、演じ分けたりすることが可能となろう。このような個人の自由をも、重層的なプライバシーの権利の一部とみなすならば、新しい意味でのプライバシーは、「単一視点（パノプティコン＝場の支配者＝ビッグブラザー）に飲み込まれない権利」と呼ぶことができるだろう。

このような自由を保障する制度設計を行なう上では、データ管理者（個人データを取扱う企業や組織）による長期間の個人の追跡を規制すること、また追跡できないように技術的手段で保証すること[5]が重要である。また、複数のデータ管理者間の結託を防ぎ、個々のデータ管理者が寡占化しないように競争させるための構造・制度（第三者機関による監督など）を導入することも重要である。すなわち、ＩＴを活用して個人データを大量に取得する「リトルブラザー」の出現を阻止することはもはや不可能だが、個人が複数のリトルブラザーを自由に選択でき、またリトルブラザーの「ビッグブラザー化」を阻止できるように、制度的・技術的な担保を行なうことが重要なのである[6]。同時に、個々のデータ管理者も、リトルブ

ラザーとして生き永らえるためには、個人に対する透明性とアカウンタビリティが強く求められることとなろう。

---

[1] ジグムント・バウマンは、デイヴィッド・ライアンとの共著（伊藤茂訳）『私たちが、すすんで監視し、監視される、この世界について』（青土社、二〇一三年）において、「（人々が）市場に出荷するよう促され、販促活動や販売活動を行なっている商品は、彼ら自身なの（だ）」「（消費者社会において）『自らを販売可能な商品にすること』は・・・個人の義務で（ある）」と述べている。

[2] 東浩紀は「情報自由論」（『中央公論』二〇〇二年～二〇〇三年）において、管理社会における権力を、ローレンス・レッシグのアーキテクチャ論も取り入れながら、「環境管理型権力」という概念に発展させた。鉄道のキセルの例は東が同書で挙げている例である。

[3] 多くの途上国では、最寄りの役所まで遠い、交通手段がない、読み書きができない、制度自体を知らないといった理由から出生登録が十分に行なわれていない。

[4] マハトマ・ガンディーは、二十世紀初頭の英国領南アフリカにおいて、インド人移民に対する差別的で強制的な十指の指紋登録への反対運動を行なったが、読み書きができないインド人のために手書き署名に代わる手段として自発的な親指指紋の登録制度の提案も行なっている。キース・ブレッケンリッジ（堀内隆行訳）『生体認証国家』岩波書店、二〇一七年。

[5] マイナンバー制度における「符号を用いた情報連携」は、このような技術的手段の一例である。

[6] ＥＵの一般データ保護規則（ＧＤＰＲ）では「データポータビリティの権利」や「忘れられる権利」、「自動意思決定に服しない権利」が明確化されたが、これらはデータ管理者のこのような「ビッグブラザー化」を阻止するための一つの制度的手段と考えられる。