In-depth argument on information

情報論議

根掘り

葉掘り

きれいは汚い，汚いはきれい：
監視をめぐって

名和小太郎

情報管理 56(5), 322-324, doi: 10.1241/johokanri.56.322 (<http://dx.doi.org/10.1241/johokanri.56.322>)

21世紀に入り，プライバシー保護の環境が大幅に変化してしまった。第1に，民間セクターに一望監視システムが現われた。第2に，人々の社会活動の多くが，そして私生活の多くも，実空間からサイバー空間へと移されてしまった。第3に，新しく出現した技術がプライバシー保護の概念を揺るがしている。第4に，プライバシー保護よりもセキュリティ，とくに監視が重視されるようになった。

*

*

まず第1の点について。2010年，グーグル前CEOのエリック・シュミットは語った。「グーグルはあなた方が入力することをさらさら求めない。われわれはあなた方が居る場所を知っている。われわれはあなた方が居た場所を知っている。われわれはあなた方が考えていることを知っている」と。このようなシステムはグーグルだけではない。たとえば，フェイスブックもそうだ。

*

*

ここでヨハネ黙示録のつぎの言葉を想起する人もあるだろう。「小さき者にも，大いなる者にも，富める者にも，貧しき者にも，自由人にも，奴隷にも，すべての人々に，その右の手あるいは額に刻印を押させ，この刻印のない者はみな，物を買うことも売ることもできないようにした」。現代の刻印は指紋であり，DNA配列であり，検索履歴であり，SNS記録である，ということになるだろう。

つぎに第2の点について。いまいったフェイスブックは加入時に氏名（実名），住所，履歴，顔写真などの入力をユーザーに求めている。それは入力後ただ

ちに全ユーザーに公開される。そこでは「公開」がデフォルトになっている。

フェイスブックは，当初ここに「ビーコン」というシステムを組み込んでおり，そのアフィリエイト——広告会社，通販会社——から，かれらのもつ顧客データを収集し，これをオプトアウトの形でユーザーに公開していた。このビーコンが問題視された。

ことの発端は，シーン・レーンという男が指輪をインターネット上のサイトからひそかに購入したことにあった。かれはこれを妻に贈り，その妻を驚かす心算だった。だが，その妻は，そしてその「友達」も，レーンの購入をフェイスブック上でただちに知ってしまった。くわえて，その指輪の購入先が安売りサイトであったことも。個人の私生活がサーバー空間にはみ出し，それが不特定多数者に知られてしまったことになる。レーンはここにプライバシーの侵害があったとしてカリフォルニア北部地区連邦地裁に訴訟を起こした。これが360万人を巻き込む集団訴訟へと拡がった。

2007年，地裁が改めて示した和解によって，この訴訟はあっけなく終結した。フェイスブックが受け入れた条件は，第1にビーコンを停止すること，第2に中立的な「デジタル信用基金」創設のために720万ドルを拠出し，べつに弁護士費用として230万ドル支払うこと——この2つであった。集団訴訟に参加したユーザーはなににも得るものがなかった。この訴訟は2013年まで，控訴審で尾をひいたが，結局，地裁の示した条件で決着した。

フェイスブックはその後もユーザーの顔写真を収

集している。現在では、ユーザーが顔写真を入力すると、ただちにそれは、すでに保有されている顔写真データベースと照合される、という。最新の顔認識技術は、一卵性双生児を別人として認識できるまでになった、とも言われている。フェイスブックはフェイスバンクとなった。

*

*

第3の点についてはどうか。たとえばGPSがある。これを捜査に使ったばあい、それは法的に許されることなのだろうか。これが麻薬取引人のアントワヌ・ジョーンズに対する訴訟において問題となった。

捜査当局はジョーンズのジープにGPS機器をひそかに取り付けジープの行き先を追いかけて、これで証拠を固め、ジョーンズを逮捕することができた。2005年、コロンビア地区連邦地裁はかれを有罪とし、罰金刑を科していったんは釈放したが、再逮捕し終身刑に処した。

だが、ジョーンズは捜査当局の行動を憲法修正第4条侵害であると控訴した。それは控訴審によって認められ、さらに連邦最高裁へと上げられた。

その修正第4条は、「不合理な逮捕捜索、もしくは押収に対し、身体、住居、書類、および所有物の安全を保障される人民の権利は、これを侵害してはならない」と示している。

刑事事件の捜査手法は、20世紀に入ると、電話の盗聴、無線機による追跡、赤外線による探知と多様化し、これに対応して最高裁は、さまざまな解釈を示してきた。

ここでつぎのような論理が作られた。まず令状なしの個人の所有物への捜査は認められない。だが、公道を走行するばあいであれば、令状なしに個人の自動車に捜査用の無線発信機を搭載することは許される。なぜならば、公道は公共空間であり、そこは公衆の眼に曝される場所であり、だれも、そこでは「プライバシーへの期待」をもつことができないから（情報管理 2005, vol. 48, no. 3「私的空間の範囲—個人情報保護をめぐる—」参照）。

2012年、連邦最高裁はGPS機器を容疑者の自動車にひそかに搭載することは修正第4条侵害になる、と示した。修正第4条に関する「プライバシーへの期待」基準は否定され、修正第4条の解釈は、一転してそれを制定した18世紀に戻ってしまった。

だが、判決文を読んでみると、判事たちがGPSは巨大な監視システムとなりうるとの懸念をもっていたことがわかる。ある判事はつぎのように指摘している。GPSデータは追跡する相手の立寄り先を暴露してしまう。それは、精神科医、形成外科医、中絶クリニック、AIDS治療センター、ストリップ・クラブ、刑事事件弁護士、労働組合事務所、モスク、シナゴグ、教会であったりする、と。この懸念が判決を反時代的な方向へと逆行させたのかもしれない。

審議中ではあったが、べつの判事はつぎのような発言をしていた。10年もたてば人口の90パーセントがSNSのユーザーとなり、その各人が500人の「友達」をもつようになるだろう、このとき一般人の「プライバシーへの期待」も変化するはずだ、と。

ここでつけ加えれば、新しく出現したプライバシー保護にかかわる技術はGPSだけではない。さきに示したフェイスブックのビーコン、そして顔認証システムがある。また、すでに別稿で紹介した全身透視画像技術がある（情報管理 2013, vol. 56, no. 1「バーチャル・ストリップ・サーチ 対 修正第4条」参照）。

このような環境のなかで、「プライバシー・バイ・デザイン」という概念も提唱されている。これはプライバシー保護という理念のなかに技術製品を封じ込める設計法を指す。だがこれで満足するほど、技術者は、そして起業家も、ナイーブではないだろう。

*

*

つぎに第4の点について。ここでは、9.11事件以降、国土安全保障局（DHS）がひそかに構築してきた「パーフェクト・シティズン」というシステムがある。2010年、『ウォールストリート・ジャーナル』がその存在をすっぱ抜いた。これは政府機関に対するインターネット経由の攻撃を探知、防止するシス

テムである。その探知行動は修正第4条侵害となる可能性をもつ。

DHSはまだ事前評価の段階に過ぎないと批判をかわした。だが実施段階になれば、当然、民間の事業者の手を借りなければならない。現にAT&Tは参加を表明している。

DHS長官のジャネット・ナポリターノは「あなたは私に50フィートの梯子を見せる。私はあなたに51フィートの壁を見せよう」と言った。アリゾナ州知事時代に経験した国境警備についての言葉である。このトラウマから脱けられないためか、パーフェクト・シティズンの開発予算は膨れ上がり、ついに待たがかった、ともいう。

いっぽう、国家安全保障局 (NSA) は、2007年より「プリズム」というシステムを使ってAT&T、ベライゾン、グーグル、フェイスブック、スカイプなどから通話記録、映像データ、ログイン・データなどを収集しているらしい。それを2013年6月に『ワシントン・ポスト』が、そして『ガーディアン』が明らかにした。NSAはこの行為を外国諜報監視法にもとづくものであると釈明かつ正当化している。

*

*

第4点についてもうひとつ。2013年5月、連邦議会にとんでもない法案が提出された。それは「国境セキュリティ・経済機会・移民近代化法」である。その800ページを超える法案のなかには、さりげなく、「写真照合」(photo matching) というキーワードが埋め込まれている。

雇用主は、だれかを雇用するとき、当人のもつ「バイオメトリクス労働認証カード」を市民権・移民業務局のもつ「雇用認証強化システム」と照合しなければならない。カード上に記載されるデータは氏名、住所であり、さらに社会保障番号 (SSN) と顔写真に関するバイオメトリクス・データとなる (注記すれば、SSNが日本の「マイナンバー」の先例となる)。

当面、この法案の対象者は外国人とされている。だが、連邦政府は旅券をもつ米国市民へも、このシステムの適用を求めている。人権保護団体のなかには、いずれは全国民へと広がるだろう、とみる向きもある。

すでに2004年、議会は諜報改革・テロリズム防止法を制定しており、社会保障局 (SSA) に対して、SSNカードにセキュリティ機能を組み込めと定めていた。

話がそれ、そして時代が戻るが、1970年の国勢調査をまえにして、米国民のあいだでは論争が生じた。それは調査表の記載項目のなかにプライバシー侵害になるものがある、という指摘であった。結果として、「信仰」「喫煙」「副業」「加盟組合」「ペット」そして「SSN」が消された。なぜか「浴室とシャワーの有無」は残されたが。いずれにせよ、古き良き時代は去った。

*

*

21世紀初頭、民間セクターには、すでにグーグル、フェイスブックといった巨大な一望監視システムが稼働している。それはインフラストラクチャとして機能し、大きすぎて潰せない、までに成長した。

いっぽう、政府の監視システムは、セキュリティ保護という名目のもとにその実体を隠しつつ、にもかかわらず、そこへ民間のシステムを取り込んでいく (情報管理. 2012, vol. 55, no. 3「戦争,あるいは犯罪,あるいは悪戯」参照)。

このような環境のなかで、プライバシー侵害にかかわる技術がセキュリティに、さらには一望監視にと、転用されるようになった。ここでは技術が新しい秩序を設け、その^{あお}煽りを受けて、伝統的な法制度は揺らぎつつある。

*

*

「技術は汚くて法律はきれい」なのか。それとも「法律は汚くて技術はきれい」なのか。