琉球大学学術リポジトリ

パブリック・フォーラムとしての公共空間における位置情報と匿名性

メタデータ	言語: 出版者: 琉球大学法文学部 公開日: 2012-11-22 キーワード (Ja): キーワード (En): 作成者: 高橋, 義人, TAKAHASHI, Yoshihito メールアドレス: 所属:
URL	http://hdl.handle.net/20.500.12000/25437

パブリック・フォーラムとしての公共空間における位置情報と匿名性

高　橋　義　人

はじめに

政治思想において公私の区分は政治・経済・社会の関係を説明し、日常生活の選択を特徴づける中心的ロジックの一つだが、この区分は歴史的・文化的に形成されてきた概念なので必ずしも自明ではない。公私を区別する目的によって意味は変わる[1]。よく知られているのは複数の対立概念の組み合わせで説明する定義である。例えば、アーレント（Hannah Arendt）によれば、「私と公の区別は、必要性と自由、空虚と永遠、恥と誇りの対比に一致するが、必要性、空虚、恥に対応する場所が私的領域だというわけでもない。隠されるべきものと公に開示されるものがあることが、二つの領域の最も初歩的な意味である」[2]。

「可視性」と「集団性」を基準とすれば、公と私は「公開されアクセス可能な事項に対して隠された事項」、「集団に関わる事項に対して個人的な事項」という対立関係で定義される。具体的には、「シティズンシップ」、「フェミニズム」、

[1] Raymond Geuss, *Public Goods, Private Goods* (Princeton University Press, 2001)；邦訳（山岡龍一）『公と私の系譜学』（岩波書店、2004年）；Jeff Weintraub and Krishan Kumar (eds.), *Public and Private in Thought and Practice: Perspectives on a Grand Dichotomy*, ch.1 (The University of Chicago Press, 1997)；Maurizio Passerin d'Entreves and Ursula Vogel (eds.), *Public and Private: Legal, political and philosophical perspectives*, ch.1 (Routledge, 2000)；Zizi A. *Papacharissi, A Private Sphere: Democracy in a Digital Age*, ch.2 (Polity Press, 2010)；Norberto Bobbio, *Democracy and Dictatorship* (Polity Press, 1997)；アンソニー・ギデンズ（秋吉美都ほか訳）『モダニティと自己アイデンティティ：後期近代における自己と社会』第五章（ハーベスト社、2005年）。

[2] Hannah Arendt, *The Human Condition*, p73 (The University of Chicago Press, 1998)；邦訳（志水速雄）『人間の条件』（筑摩書房、1994年）。「公共のまなざしから隠しておくべき、政治的活動から保護しておくべき領域」が「私的領域」である。

「経済」、「社会関係」という四つのモデルが指摘できるだろう[3]。

古代ギリシャにおける公私の区別はポリスの政治に対する〈oikos＝生産と分配を規制する制度として家庭〉であった。開かれた公共空間＝公共の広場（アゴラ）と隔離され閉ざされた私的空間＝財産と家族の場所が対比されていた[4]。この区別を継承しているのがシティズンシップ・モデルである[5]。このモデルではパブリックとは政治的討議（熟慮と討議による私的選好の転換のプロセス）を実体化するような環境、もしくは市民として個人が集団的自己決定のプロセスに参加する領域を意味する。これら公共性を表象する空間／領域は私的な家庭生活の非政治性と対照をなしている[6]。

古代ギリシャやシティズンシップ・モデルにみられるプライベートと家の結合はフェミニズム・モデルにも共通している。フェミニズムの理論でもプライ

---

[3] Jeff Weintraub, "The Theory and Politics of the Public/Private Distinction" in Jeff Weintraub and Krishan Kumar (eds.), *Public and Private in Thought and Practice.*

[4] Arendt, *The Human Condition*, p.58.

[5] トクヴィルの「政治社会」、アーレントの「公的領域」、ハーバーマスの「公共圏」である。ただし、「公論」についての考え方は、ハーバーマスとアーレント／トクヴィルでは異なる。アーレント／トクヴィルにとって「公論」は理性の力ではなく専制である。トクヴィルが民主的な「多数者の専制」を警告したように、アーレントも「公論」を明確に否定している。see Arendt, *On Revolution*, p217 (Pengunin Books, 1963)；邦訳（志水速雄）『革命について』（筑摩書房、1995年）；Alexis de Tocqueville, *Democracy in America*, vol.1, pp258-261 (Vintage Books, 1990)；Dana Villa, *Public Freedom*, ch.4 (Princeton University Press, 2008).

[6] アーレントの公的領域は物理的にも境界線が画定されていたが、ハーバーマスの公共圏は物理環境にそれほど依存しているわけではない。公共圏の典型は18世紀のカフェだが、印刷技術を基盤としたメディアもまた公共圏を形成していた。つまり、公共空間は物理的な場所にだけ生じるわけではない。両者の議論については、さしあたり以下のテクストを参照。see Arendt, *The Human Condition;* Seyla Benhabib, *The Reluctant Modernism of Hanna Arendt, New Edition* (Rowman & Littlefield Publishers, Inc., 2000)；Dana R. Villa, "Theatricality in the Public Realm of Hannah Arendt" in Marcel Henaff and Tracy B. Strong (eds.), *Public Space and Democracy* (University of Minnesota Press, 2001)；Jurgen Habermas, *The Structural Transformation of the Public Sphere*, translated by Thomas burger with the assistance of Frederick lawrence (The MIT Press, 2001)；邦訳（細谷貞雄・山田正行）『公共性の構造転換』（第二版、未来社、1994年）;Charles Talor, *Modern Social Imaginaries*, ch.6 (Duke University Press, 2004)；邦訳（上野成利）『近代：想像された社会の系譜』（岩波書店、2011年）；See John B. Thompson, *The Media and Modernity: A Social Theory of the Media*, ch.4 (Stanford University Press, 1995).

ベートという言葉は「家庭 / 家事 domestic」とほぼ互換的に使われる。プライベートは社会が女性と伝統的に結びつけてきた空間であるのに対して、パブリックは男性が「活動」する領域である[7]。しかし、シティズンシップ・モデルと違って、フェミニズム・モデルのパブリックは「政治」だけでなく、家の外部の事項すべて（「経済」を含む）を意味している。この点は経済モデルとは異なる。経済モデルではパブリックは「政府」の領域を、プライベートは個人や企業による「市場」が作用する領域（市場に基づく市民社会）を表象している。この場合の「私的領域」は契約や交換、非人格性などから特徴付けられる[8]。

さらに社会関係モデルからみると、公共空間は「開かれ共有された空間」＝見知らぬ者たちが集まり、多様な属性をもつ人々が共存できる空間、「見知らぬ者たちの流動的な社会関係」から構成される社会空間である。シティズンシップ・モデルと違って、社会関係モデルの公共生活では、市民が協働する集団的な「活動」ではなく、多様な個人が共存し「交流」できる環境の方に重点がある[9]。そして、このような公共生活と対比されるのが「私的な家庭生活」や「緊密で小規模コミュニティの生活」である。つまり公共空間は偶発的な社会関係

---

[7] フェミニズムが批判した公私の分断とは両者の優位 / 劣位という関係性である。see Carole Pateman, *The Disorder of Women* (Stanford University Press, 1989) ; フェミニズムからみたアーレントについては、ボニー・ホーニッグ編（岡野八代・志水紀代子訳）『ハンナ・アーレントとフェミニズム：フェミニズムはアーレントをどう理解したか』（未来社、2001年）参照。

[8] 経済モデルでは、「公共空間」は政府 / 国家が所有・開設した場所であり、「私的空間」は私人の財産や市場に基づく自発的秩序を意味している。パブリック・フォーラムの法理がこの区分と一致している。

[9] ジェイコブズが健全な都市生活＝公共生活のためには都市計画が重要であることを論じていたように、社会関係モデルでは公共生活は物理的環境と密接に関係していることも特徴である。see Roger Scruton, "Public Space and the Classical Vernacular," in Nathan Glazer and Mark Lilla (eds.) , *The Public Face of Architecture: Civic Culture and Public Spaces* (The Free Press, 1987) ; 都市の公共空間の政治的意味について、see Don Mitchell, *The Right to the City: Social Justice and the Fight for Public Space* (The Gulford Press, 2003) ; Timothy *Zick, Speech Out of Doors; Preserving First Amendment Liberties in Public Places* (Cambridge University Press, 2009) ; Marcel Henaff and Tracy B. Strong (eds.) , *Public Space and Democracy* (University of Minnesota Press,

による世界であるのに対して、私的空間はより親密で管理された環境と捉えられるのである[10]。

このように政治思想や社会理論では目的に応じて公私の解釈は多様だが、(抽象的と物理的な意味で) 公私の領域 / 空間にアクセスするインターフェイスが違えば、公私の認識が変わることもある[11]。例えば、テクノロジーは自宅での個人的な行為 (読書や音楽鑑賞など) を「公共の場所」に持ち出すことによって、場所の意味を曖昧にした。公園でイベントに参加している人と iPod で音楽を聴いている人、カフェで友人と対話する人とモバイル端末からネットに接続して仕事をする人、これらの人にとって場所の意味は同じだろうか。その空間は公共的なのか、個人的に管理されているのか。もちろん公私をどう理解するかによって答えは異なるが、テクノロジーが「公共の場所にいる」という経験を複雑にしているといえるだろう[12]。

2001) ; Setha Low and Neil Smith (eds.) , *The Politics of Public Space* (Routledge, 2006) ; Nicholas Blomley, *Rights of Passage: Sidewalks and the regulation of public flow* (Routledge, 2010) ; 合衆国におけるニュー・アーバニズムと市民的共和主義の関係は、see M. J. Sandel, *Democracy's Discontent: America in Search of a Public Philosophy*, pp335-36 (Harvard University Press, 1996) ; 邦訳 (小林正弥監訳)『民主政の不満 (下)』268 頁 (勁草書房、2011 年)。

[10] 社会関係モデルの系譜には、セネット (Richard Sennet)、ジェイコブズ (Jane Jacobs)、アリエス (Philippe Aries) があげられる。さしあたり以下を参照。Richard Sennett, *The Fall of Public Man* (Penguin Books, 1976) ; Sennett, *The Uses of Disorder: Personal Identity and City Life* (W.W. Norton, 1970) ; 邦訳 (北山克彦・高階悟訳)『公共性の喪失』(晶文社、1991 年) ; Jane Jacobs, *The Death and Life of Great American Cities* (Vintage Books edition, 1992) ; 邦訳 (山形浩生)『アメリカ大都市の死と生』(鹿島出版、2010 年) ; Philippe Aries, *Centuries of Childhood: A Social History of Family Life* (Pimlico, New Edition, 1996) ; 邦訳 (杉山光信・杉山恵美子)『子供の誕生』(みすず書房、1981 年)。

[11] Jason Farman, *Mobile Interface Theory: Embodied Space and Locative Media* (Routledge, 2012) ; テクノロジーと公私の境界線の関係については、see Susan Landau, Surveillance or Security: *The Risks Posed by New Wiretapping Technologies*, ch.6 (The MIT Press, 2010) ; Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, ch.1 (Stanford University Press, 2010) .

[12] Adriana de Souza e Silva and Jordan Frith (eds.) , *Mobile Interfaces in Public Spaces: Locational Privacy, Control, and Urban Sociability*, ch.2 (Routledge, 2012) ; Michael Bull, Sound Moves: *iPod Culture and Urban Experience* (Routledge, 2007) .

このような意味でテクノロジーが人々の認識や社会規範に影響することは過去の事例からもうかがわれる。例えば、カメラとプライバシーの関係がわかりやすいだろう。イーストマン（George Eastman）の「コダック・カメラ」以前のカメラは公共の場所に持ち出して使うには大きすぎたことから、写真撮影は閉ざされた「私的空間」のなかで専門家によって行われなければならなかった。しかし、コダック社のカメラの普及によって、1880年代後半には路上のアマチュア・カメラマンが増加する。こうしたカメラの流行には、プライバシーの認識を変える点で、それまでの社会規範を動揺させる効果があった。もちろんプライバシーというコンセプトそのものは目新しいものではない。1880年代以前にもあった[13]。しかし、メディアの違いによって伝達される情報の効果が違うように、文字・写真・ビデオにはそれぞれ異なる「侵害」の効果や形態がある[14]。カメラはそれまで意識されていなかった「侵害」を明らかにすることによって、プライバシーに対する認識や慣習を変えたのである[15]。

それでは、ポータブルカメラは公私のあり方、プライバシーの認識をどのような意味で変えたのか。端的にいえば、公共空間においても人は一定のプライバシーを期待していること、見知らぬ者たちが行き交う路上にもプライバシーがあることを認識させたといえるだろう。つまり、公共の場所では人々はある程度で関わり合いつつ、お互いに無関心な匿名の存在だが、カメラは公共の場所での匿名性＝プライバシーを変えたといえる。公共の場所にいる人が誰かに写真を撮られるとき、その人はもはや匿名の存在ではなくなるからである[16]。

1880年代のカメラと同じことは現代の情報テクノロジー（例えば、Wi-Fi、

---

[13] Robert C. Post, *Constitutional Domains: Democracy, Community, Management*, ch.6（Harvard University Press, 1995）.

[14] John Durham Peters, *Speaking into the Air: A History of the Idea of Communication*, pp.174-75（The University of Chicago Press, 1999）.

[15] see Louis Brandeis and Samuel Warren, "The Right to Privacy," 4 Harv. L. Rev. 193（1890）.

[16] Adriana de Souza e Silva and Jordan Frith, *Mobile Interfaces in Public Spaces: Locational Privacy, Control, and Urban Sociability*, ch.2（Routledge, 2012）.

CCTV、スマートフォン、GPS、IDカード、マイクロフォン、検索エンジン、赤外線センサ、クラウド、ネットワーク・プリンタ、スマートTVなど）にも考えられるだろう。ただ、これらテクノロジーの問題は、プライバシーの脅威になるかどうかではなく、それぞれの特性に応じて公私についての人の認識や経験を再定義するインターフェイスになりうることだと思われる。

そこで、本稿では合衆国憲法を素材として、公共空間におけるプライバシーとしての匿名性を考えてみたい。合衆国憲法の権利条項は政府による私的領域への干渉を制限している。特に修正第四条は一定の領域に侵入する政府（警察など法執行機関）の行為を対象としているが、ブランダイスとウォーレンの主張以降、プライバシーの保護範囲は拡張されてきた。財産権や住居など物理的空間だけでなく、より抽象的には個人の内心やコミュニケーションから家族・婚姻・性的関係・生殖のような生活の領域まで多岐にわたっている[17]。これらの保護を論じる場合には、何らかの意味で公私二元論が前提となる。しかし、公私の区別をどのように理解するとしても、私的領域＝プライバシーを保護するというロジックを単純に適用できる範囲は縮小しているのではないかと思われる。情報テクノロジーの発達は公私の区別を複雑にして、その境界線を流動化させている。その結果として、これまでの判例法理では、一方で擁護しやすい「私的領域」を保護しながら、他方では曖昧化した領域の保護を放棄している面もあったと思われる。

具体的には、次のような手順で議論を展開したい。まず、プライバシーとしての匿名性について、二つの意味を修正第一条の法理から確認する。次に、公共の場所での位置情報を追跡する警察の行為が争われた最近の修正第四条事件を素材として、従来のプライバシーの法理を検証する。最後に、位置情報はどのような意味で「プライバシー」なのか、「侵害」はどのような場合に生じるのかを考察する。以上の作業を通して、公私の空間とテクノロジーの関係を論

[17] Jon L. Mills, *Privacy: The Lost Right*, ch. Ⅲ（Oxford University Press, 2008）.

じるための視座もえられるのではないかと考えている。

Ⅰ．言論の自由と匿名性

「匿名であること anonymity」とは「名前のない状態 anonymia=the state of being unnamed」を由来し、辞書的には「公に個人が特定されていない、個人を特定できる情報が公開されていない状態」をいう。この匿名性はプライバシーの一要素として捉えられる[18]。例えば、Alan Westin は次のように論じている[19]。

匿名性とは、人が公共の場所にいるときや、公共的な活動に参加しているときに、個人を特定されたり、監視されたりしないことである。人は地下鉄に乗車し、球場に行ったり、街路を歩いたりすることがある。このとき彼は周囲の人からみられていることをわかっている。しかし、彼が有名人でなければ、個人として特定されたり、周囲の人に知られている場合に作用する行為や役割のルールに縛られることを望んでいない。こうした状態において、人はその周辺の状況に紛れ込むことができる。公共の場所において意図的・組織的に監視されていることをわかって、それをおそれるとすれば、人がオープン・スペースや公共の広場で求める息抜きや自由を損なうことになる。…もう一つの匿名性は思想を匿名で公表することである。ある人はコミュニティになにか思想を公表したいと考えているとする。しかし、著者としてすぐに特定されることを望んでいない。特に公権力から特定されたくないこともある。…このような二つの匿名行為の核心は公共的なプライバシー（public privacy）の願

[18] Raymond Wacks, *Privacy: A Very Short Introduction*, ch.1（Oxford University Press, 2010）.

[19] Westin は民主国家におけるプライバシーを「孤独 solitude」・「親密性 intimacy」・「匿名性 anonymity」・「保全 reserve」という四つの状態から定義している。この定義は他者からの距離を基準にしていると思われる。see Alan F. Westin, *Privacy and Freedom*, ch.2（Atheneum, 1968）.

望である[20]。

Westinによれば、プライバシーとしての匿名性とは、「公共の場所にいるときや公共的な活動に参加しているときに個人を特定・監視されたりしないこと」（存在の匿名性）と「思想を匿名で公表すること」（言論の匿名性）を意味している。つまり、「公共的プライバシー／匿名性」とは、公共の場所での行動や言論活動について名前のない状態が維持されることだといえる。まず本章では、言論の自由の法理から匿名性の意味を確認しておきたい。

1．「匿名の言論」と萎縮効果

言論の自由の法理では匿名性は萎縮効果の関連で論じられる。刑事規制だけでなく、政府の情報収集活動＝「監視・調査」は言論を萎縮させるからである[21]。情報収集だけでは物理的な損害が生じるわけではないので違法性を立証することは単純ではないが[22]、政府による情報収集は言論活動、知る権利、政治団体への参加を萎縮させると考えられている[23]。それでは、萎縮効果を除去するために保護される言論形態として「匿名の言論」はどのように理解される

---

[20] Westin, *Privacy and Freedom*, p31.

[21] 具体的には、日常の行動に対する監視、デモや集会への参加者の特定、書籍など購読歴・閲覧履歴の調査、政治団体との結びつきの調査、証拠の提出命令などがある。Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, ch.15（Yale University Press, 2011）；Daniel J. Solove, "The First Amendment as Criminal Procedure," 82 N.Y.U.L. Rev. 112（2007）；萎縮効果について、see Frederick Schauer, "Fear, Risk, and the First Amendment: Unraveling the Chilling Effect," 58 B. L. Rev. 685, 692-93（1978）；毛利透『表現の自由：その公共性ともろさについて』（岩波書店、2008年）。

[22] 政府が反戦活動家の情報を収集していた事件では「情報が本人の意思に反して利用されるかもしれないという未確定のおそれ以外に、特定の予見しうる害悪を立証しえない」とされた。see Laird v. Tatum, 408 U.S. 1（1972）。「適切な理由がなく、保護された団体活動に従事している労働者を写真撮影することは活動を萎縮させる」こと、映像の記録によって「報復されるかもしれないというおそれを生み出す」ことについては、see National Steel v. N.L.R.B, 156F.3d 1268（D.C. Cir. 1982）.

[23] 従って、政府による情報収集の範囲が「重大な政府利益 substantial government interest」を達成するために限定されていない場合には「過度の広汎性」から違憲と

のだろうか。

匿名の文書は人類の発展において重要な役割を果たしてきた。歴史を通して長い間、抑圧された集団や党派は匿名ゆえに抑圧的な慣習や法を批判できたのである。匿名でなければできなかっただろう。イングランドの出版許可法は植民地にも施行された。出版者・著者・配布者の氏名の開示は政府を批判する文書の流通を抑制することを知っていたからである。…アメリカ革命以前には植民地の愛国者たちは著者名や配布の事実そのものを隠さなければならなかった。… "the Federalist Papers" さえ仮名で出版された。建設的な目的から匿名を選択することもあるのは明白だ[24]。

多くの偉大な文学作品は仮名で執筆する偉大な作家から生み出された。著者は誰かという読者の好奇心や公衆の関心にかかわりなく、著者は自分の属性を開示するかしないかを自由に判断できる。匿名を選択するのは、経済上の関係やフォーマルな人間関係への配慮、社会的オストラシズムへの懸念から、あるいは自分のプライバシーをできるだけ保持したいという単なる欲求に動機づけられるのかもしれない。ただ、動機はどうであれ、少なくとも文学作品に関しては匿名作品を市場に参入させる利益は、参入条件として氏名の開示を求める公共的利益よりも大きいことは確かだ。従って、匿名を選択する著者の判断は、出版物の内容の記述と同じように修正第一条が保護する言論の自由の一部だといえる[25]。

これら二つの判決によれば、匿名の言論の意義とは、人間関係や排除・失職などの不利益をおそれず、社会的評価・経済的損失を心配しないで自由に発言

なりうる。See Members of the City Council v. Taxpayers for Vincent, 466 U.S. 789, 801 (1984) ; Thornhill v. Alabama, 310 U.S. 88, at 98 (1940) ; NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958) ; Neil M. Richards, "Intellectual Privacy," 87 Tex. L. Rev. 387 (2008) .

[24] Talley v. California, 362 U.S. 60 (1960) , at 64-65.

[25] McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995) , at 341-42.

できること、また匿名ゆえにメッセージ内容についての読者の偏見が除去され、テクスト自体に活力が与えられることである（思想の平等）。

2．「匿名の言論」の政治的価値

McIntyre 判決は「匿名の言論」の特に政治的意義を秘密投票＝「報復をおそれずに自己の良心に従って発言する権利」の歴史に位置づけた。この事件では州政府は「選挙に関わる公正な情報の提供」と「詐欺などの害悪防止」という目的から匿名文書の配布禁止を説明していたが、法廷意見は「過度に広汎な規制手段」を正当化できないとして州政府の見解を否定したのである[26]。

合衆国憲法の下では匿名の文書配布は有害な詐欺ではない。意見の主張と異論の名誉ある伝統である。匿名性は多数派の専制に対する防御手段である。これは権利章典、特に修正第一条の目的を具体化している。修正第一条の目的とは不寛容な社会の報復から少数者を保護すること、彼らの考えを抑圧から保護することである。場合によっては、匿名の権利（right to remain anonymous）は濫用されるかもしれない。しかし、ことの性質上、政治的言論は不快な結果を伴ったとしても、総じてアメリカ社会は、言論の自由の誤用の危険性よりも言論の自由の価値を重視してきたのである（514 U.S. at 352.）。

この判決では「匿名の言論」と「少数者」の保護が明確に関連付けられたことが重要である。さらに、その後の Watchtower Bible 事件では法廷意見は「戸別訪問」という情報伝達手段の歴史に言及しながら、「エホバの証人」の「伝道活動」に対する規制は彼らだけでなく、市民の言論活動にも影響することを

---

[26] この事件では問題となったオハイオ州選挙法には、①著者もしくは発行者の氏名・住所が記載されていない選挙文書の配布の禁止、②選挙運動期間に虚偽情報の配布に対する詳細な禁止を規定していた。

論じた[27]。

間違いなく、本件条項は宗教活動だけでなく政治活動にも適用される。…条例が多くの言論を対象としていることだけで憲法上は問題となる。次のような点で、条例は修正第一条が保護する価値だけでなく、「自由な社会」という理念に対して攻撃的だからだ。つまり、日々のパブリック・ディスコースにおいて、市民は隣人に語りかけたいと思えば、政府に情報を提出し許可を最初にえなければならない点である。市行政による許可証発行が迅速に処理され、申請者に負担を課さない事務処理だったとしても、言論活動の許可を義務づける法律は合衆国の国民的な財産と憲法の伝統から大きく逸脱している（536 U.S. at 165-166.）。

この事件の争点となった条例は「訪問勧誘員」が事前の許可なく住民の私有財産に「立ち入ること」を禁止し、もし立ち入る場合には「勧誘許可証」を自治体からえなければならないことを定めていた。申請者が「許可申請書」を提出すれば「許可証」が発行されることになっていたが、条例は「訪問勧誘する者は許可申請書で身元を開示すること」、「市の捜査機関は提出された情報を自由に利用できること」も規定していた[28]。このような許可制度は宗教的少数者を抑制するだけでなく、市民の自発的で自然なコミュニケーションを広い範囲で妨げるおそれがあると考えられたのである。

休日や週末に政治運動に積極的に参加するかどうかを判断しようとする人は許可を

[27] Watchtower Bible & Tract Society of New York, Inc. v. Stratton, 536 U.S. 150 (2002)

[28] 536 U.S. at 154. 具体的に「許可申請様式」には次の記入項目が列挙されていた。「①登録者の氏名・住所および登録日以前の過去五年間の住所、②営業、奨励、勧誘、団体、活動の目的・趣旨および／もしくは提供する商品・サービスの説明、③雇用者もしくは所属団体の氏名・住所。これについては申請者との正確な関係と職権を示す雇用者もしくは所属団体から発行された信用証明書を添付すること、④勧誘活動に要する時間、⑤登録者が活動しようとする各地所の個別の住所、⑥登録者の営業もしくは活動目的に関わるその他の情報」。

えるまでビラを配布できない。路上で市政策に反対票を投じようと隣人に呼びかけるような自発的な判断さえも、まずは市長の許可をえなければ、合法的に実行できないことになってしまう（536 U.S. at 167.）。

最終的に法廷意見は条例がコミュニケーションのプロセスに及ぼす影響の深刻さを指摘することで、規制には「公共の事項に関する自由で開かれた討論を妨げる」効果があると結論づけている。

以上にみるように、匿名性は民主政治における少数者の言論を促進する（＝多数者による専制を抑制する）ために必要不可欠であり、匿名性を奪うことは市民の自発的な政治参加＝「公共の関心事についての力強い討論」を縮小させることにつながるといえる。

3．話者と聴衆の匿名性と応答責任

合衆国の判例法理では「匿名の言論」は修正第一条によって保護された言論形態である。では、存在の匿名性についてはどう理解されるのか。この点について、McIntyre 判決のスカリア裁判官反対意見が示唆的である[29]。スカリア裁判官によると、「特殊な環境において個人にアイデンティティの開示を強いることは、修正第一条の権利を抑制する」効果があると認められてきた[30]。しかし、それは、個人が特定されれば「政府役人や私人からの威嚇、嫌がらせ、報復を受けるだろう」という「理に適った蓋然性」を立証しえた者が「（そうした場合でなければ）本来は有効である開示要件の適用除外を求める権利」であって、先例は「包括的な匿名の権利」を保障したわけではないという。むしろ選挙過程においては、匿名の言論は虚偽や詐欺に結びつきやすいことが重視

---

[29] スカリア裁判官は「匿名であることの権利」よりも「選挙過程のインテグリティの保護」を優先した。McIntyre v. Ohio Election Comm'n, 514 U.S. at 382, Scalia, J. dissenting.

[30] Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87 (1982) ; Bates v. Little Rock, 361 U.S. 516 (1960) ; NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958) .

されるのである。

確かに匿名によって自由に振る舞えるようになれば、人は自分の行為に責任を負わなくなることもある。他者に対して応答責任を負わないことは人を解放して偽りのない言論を可能にすると同時に、コミュニケーションの基盤となる「人間関係資本 social capital」を損なう側面もあるだろう[31]。従って、こうした匿名の負の側面と他者への応答責任をどのように調整するのかが憲法の問題となったのである。

反対に、顕名（話者の属性の開示）の言論を比較してみよう。例えば、住宅からの表現物の掲示を（自宅を含めて）全面的に禁止していた市条例の憲法適合性が争われた事件では、最高裁は「自宅」という場所に着目している。

話者の属性は人を説得しようとする試みにとって重要な要素だ。退役将官や受勲経験のある退役軍人の自宅前に掲示された「湾岸に平和を」という言葉には、10歳の子どもの寝室窓や通行車両のバンパーに掛けられたメッセージ以上に異なる反応を引き起こす可能性がある。社会主義の支持表明が工場の壁やサンドイッチマンの広告板ではなく、豪華な邸宅の庭園に掲示されているときには異なる意味を伝達するだろう[32]。

場所によって異なるメッセージが伝えられることを最高裁は評価したのである。「自宅」という場所は話者のアイデンティティ＝属性に関する情報としてメッセージの一部になるからである。話者にとって自己の属性を開示するかしないかはコンテンツの重要な要素である。このように、匿名の言論が問題とな

[31] Robert D. Putnam, *Bowling Alone: The Collapse and Revival of American Community*, ch.8 (Simon and Schuster Paperbacks, 2000)；邦訳（柴内康文）『孤独なボウリング：米国コミュニティの崩壊と再生』（柏書房、2006年）；Scott L. McLwan, David A. Schultz, and Manfred B. Steger (eds.), *Social Capital: Critical Perspectives on Community and "Bowling Alone"* (New York University Press, 2002).

[32] City of Ladue v. Gilleo, 512 U.S. 43, at 56 (1994).

るのは応答責任を負う「話者」の場合である。本来的には言論活動は自己を開示するものだから、何らかの理由で匿名が必要になるときに応答責任と調整する問題が生じる。

それでは、聴衆にとって匿名性はどう捉えられるのだろうか。聴衆の匿名性は言論の自由ではなく、各種のプライバシー保護に関わって論じられてきた。例えば「自宅」におけるわいせつフィルムの所持が問題となった事件では、合衆国最高裁判決（マーシャル裁判官法廷意見）は「各人が望ましいと思うものを見聞きする権利」とプライバシーの関連性を論じている。

情報・思想を受けとる権利を憲法典が保障していることはいまや確立されている。…この権利はわれわれの自由な社会にとって基本的権利である。本件のコンテクスト、つまり人が自宅で印刷物やフィルムの単なる所持が訴追されているような場合には、この権利は別の側面をもつ。私的領域（privacy）への政府の介入から自由であることもまた、きわめて限られた状況を除けば、基本的な権利だからである[33]。

そもそも本来的には聴衆は匿名の存在である。前述したように、匿名性はプライバシーの一要素であり、保護がなければ社会的批判によって抑圧されてしまうような、慣習にとらわれない自由を促進することがプライバシー＝私的領域を保護する目的である[34]。それゆえ、プライバシーの法理は一定の「自己」決定を保護し、また多数者の専制よる萎縮からそうした決定の主体である個人を擁護してきた。プライバシーは多数者の先制を抑制均衡の手段として、威嚇や全体主義的介入を防止するように機能している[35]。特に個人の生活環境への政府の侵入は厳格に制限されなければならない[36]。つまり、プライバシーを保

[33] Stanley v. Georgia, 394 U.S. 557, at 565（1969）.
[34] Neil M. Richards, "Intellectual Privacy," 87 Tex. L. Rev. 387（2008）.
[35] Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, p110（Yale University Press, 2012）.
[36] 私的領域＝自宅は修正第四条で保護される。see Harris v. United States, 331 U.S. 145,

護することは「個々の対象を社会的な詮索」から遮断することである。「応答責任から遮断することによって、個人の領域を保護している」のである[37]。

しかし、公共の場所では市民のプライバシー＝匿名性はどうだろうか。公共の場所で市民が話者となるときには、言論の自由によって話者の匿名性（＝固有名と属性の秘匿）が保護されるかもしれないが、聴衆である市民は（言論活動に積極的にコミットしないかぎり）匿名性を保護されないことになる。伝統的な法理では、公共の場所では「プライバシーの合理的期待 reasonable expectation」は低いと考えられるからである。

これまで法的な意味のプライバシーは世界を二つの領域に分割する二元論で捉えられてきた。つまり、いったん公開されたものはもはや私的とはいえない。何らかの方法で情報が公開されるならば、その情報は私的ではなくなる。公共の場所で自分の振る舞いを他者に開示している場合には、それは私的ではない。プライバシーを欲するならば、シンボルとしての「自宅」に待避しなければならないのである。しかし、こうした公私二元論に限界はないだろうか。特に情報テクノロジーが高度に浸透したユビキタス社会では、公私二元論は困難ではないか。次章では、具体的な事件から公私二元論の問題点を検証する。

Ⅱ．公共の場所における匿名性

これまで合衆国の連邦最高裁は公共の場所には「プライバシーの合理的期待」はないと判示してきた。修正第四条の法理では「合理的期待」審査に依拠するかぎり、公共の場所での監視に対してプライバシーは保護されないことになる[38]。

at 155-74 (1947) (Frankfurter, J., dissenting) ; Body v. United States, 116 U.S. 616, at 625-32 (1886) .

[37] Robert Gerstein, "Intimacy and Privacy" in Ferdinand David Schoeman (ed.) , *Philosophical Dimentions of Privacy* (Cambridge University Press, 1984) ; Ferdinand David Schoeman, *Privacy and Social Freedom*, ch.1 and ch.6 (Canbridge University Press, 1992) .

[38] 警察が（「ポケベル beeper」と呼ばれる）位置追跡装置を自動車に取り付けていたこ

Jones事件ではこの論理をどの程度まで維持するのかが問題になった。最高裁は情報テクノロジーの進化にどう対応するのか、従来の二元論を転換するのかが注目された[39]。以下では、合衆国連邦最高裁の多数意見と結果同意意見を検証しながら、従来の法理の問題点を考えてみたい。

Jones事件の経緯は以下の通りである。FBIは被告（Jones氏）の妻の名義で登録した車輌にGPSのトラッキング機器を取り付けることを認める捜査令状をえた。令状ではコロンビア特別区で10日以内で設置することを許可されたが、しかし捜査員は11日目にメリーランドで（公共の駐車場内）機器を取り付けた。その後、被告車輌の移動を28日間追跡した結果、被告らを麻薬売買の共同謀議の容疑で起訴した。州地方裁判所はGPSデータを公表しなかったが、その他のデータを証拠として認めた。車輌が公道上にあるときには、被告はプライバシーを期待できないと考えたからである（被告は有罪）。それに対して州上訴裁判所は原審を破棄して、GPS機器を使用した（令状によらない）証拠を承認することは合衆国憲法修正第四条を侵害する旨を判示した。連邦最高裁も上訴審を支持した。

1. スカリア裁判官による法廷意見

スカリア裁判官によれば、本件の争点はGPS（global-positioning-system）追跡装置を個人の自家用車輌に取り付けて公道上の移動を監視することが修正第四条の「捜索・押収」にあたるのかである。政府は公道では「プライバシー

とが問題となった事件では「公道を走行する者はその移動についてプライバシーを期待できない」という理由で修正第四条は適用されなかった。United States v. Knotts, 460 U.S. 276 (1983).

[39] United Sates v. Antone Jones, 2012 U.S. LEXIS 1063; Daniel Solove, "United States v. Jones and the Future of Privacy Law: The Potential Far-Reaching Implications of the GPS Surveillance Case", retrieved from http://docs.law.gwu.edu/facweb/dsolove/files/BNA-Jones-FINAL.pdf; Daniel Solove, "The Potentially Profound Implications of United States v. Jones" retrieved from http://www.concurringopinions.com/archives/2012/01/the-potentially-profound-implications-of-united-states-v-jones.html

の合理的期待」はないことを次のように主張した。

① 捜査員が接近したジープ（その車底）と公道上の位置について、公道では周囲からみられているので被告には「プライバシーの合理的期待」はない。
② Katz 事件以降の判決に基づけば、本件行為は「捜索」ではない。
③ 自動車の外観は公共の眼に晒されているので、外観の検査は「捜索」ではない[40]。

しかし、こうした主張をスカリア裁判官はおおよそ以下の理由で否定した。
① 修正第四条の権利内容は Katz 判決の定式によって変わるわけではない。根本的には「修正第四条が採択されたときにあった、一定のプライバシー」を保障しなければならない。修正第四条が列挙している領域は政府による不法侵入の具体例である[41]。Katz 判決はこの理解を否定したわけではない。「財産権は修正第四条の侵害を判断する唯一の手段ではない」が、だからといって「それまで認められてきた財産の保護をやめた」（506 U.S. , at 64.）わけでもない。「政府が情報を収集するために憲法上保護された領域を物理的に侵入する場合には修正第四条の侵害になりうる」（460 U.S., at 286.）。「プライバシーの合理的期待」は過去の諸権利（財産権と社会通念上認められるもの）の保護を表している。
② 政府は二つの「ポケベル」事件を根拠としている。第一の Knotts 事件はコンテナに「ポケベル」を設置し、その位置を監視したことが争われた[42]。対象になったのは「公道上の（コンテナを運んでいる）車輌の位置と被告のキャビン付近の容器が下ろされた場所の位置」だった。このような情報は秘匿さ

---

[40] New York v. Class, 475 U.S. 106（1986）.
[41] 参照されているのは、Alderman v. United States, 394 U.S. 165（1969）、Soldal v. Cook County, 506 U.S. 56（1992）である。
[42] United States v. Knotts, 460 U.S. 276（1983）,at 278.

れているわけではないので、「プライバシーの合理的期待」はない[43]。第二のKaro事件ではポケベルのコンテナへの「設置」が「捜索・押収」になるのかが争点だった[44]。最高裁はこれを否定した。政府がコンテナに物理的に接触したのは、コンテナが被告の手に渡る前だったからである。この結論は本件の結論と完全に一致している。Karo事件の被告はポケベルを含めてコンテナを受け取ったので、（ポケベルが位置を監視することに使用されたとしても）ポケベルがあることに反対する資格はない。しかし、本件被告（Jones）の立場は違う。政府が情報収集機器を不当に設置した時点で被告はジープを所有していたからである。

③　政府が根拠とした先例は本件では重要ではない。本件では「捜査員は被告の自動車の外観を検査する以上に立ち入っている」からである。「機器をジープに取り付ける」という行為は「保護された領域を侵害している」のである。

このように、スカリア裁判官の法廷意見は不法行為論を復活させた点では注目される。修正第四条の保護内容を「合理的期待」だけでなく不法行為論で補足することによって、全体としての保護範囲を広く捉えたようにみえるが、それぞれの保護範囲を限定しているようにも思われる。

2．アリート裁判官の結果同意意見

法廷意見が「不法行為」論を重視したのに対して、アリート裁判官は「合理的期待」審査の手法そのものを再検討している点で、より踏み込んだアプローチだと思われる[45]。アリート裁判官は、本件では「被告の車輌の動きを長期間

[43] Knotts判決の争点は問題の情報についての「合理的期待」であって、「不法行為」ではない。被告がコンテナを入手する前に所有者の同意をえてポケベルはすでにコンテナにあったからである。

[44] United States v. Karo, 468 U.S. 705（1984）でも、Knotts事件と同じように、ポケベルが設置されたときには、コンテナは第三者の手元にあり、被告の所有物ではなかった。従って、問題は「元の所有者の同意による設置は、ポケベルの存在を知らない買い手にコンテナが移されたときにも…捜査・押収になるのか」であった。

[45] Ginsburg、Breyer、Kaganら各裁判官が同意している。彼らは「不法行為」審査では

監視することが被告のプライバシーの合理的期待を侵害するのかどうか」を審査すべきだという。そして、法廷意見の論理の欠点を次のように指摘した。

① 法廷意見は本当に重要なこと（＝長期間の位置追跡のためのGPSの利用）を見過ごして、代わりに瑣末な問題（＝それ自体では自動車の機能を妨げないほど小さく軽量の機器を車底に取り付けた行為）を過度に重視した。こうした物の設置は不法行為法でも賠償の根拠にならないほど些末な事項である。しかし、法廷意見の論理に基づくならば、不法侵入がない状態で長期間の監視が行われた場合には（例えば、連邦政府がGPS追跡装置を各自動車に装備するように自動車業界に要求もしくは説得した場合）プライバシーは保護されないことになる。

② 法廷意見には首尾一貫性がない。法廷意見の論理では、警察がGPS機器を車輌に取り付けて、短期間でも自動車を追跡すれば、修正第四条は適用される。しかし、長期間にわたって陸と空から警察が同じ車輌を追跡しても修正第四条の対象にならない。本件で修正第四条が適用されたのは、被告の妻が被告専用にするために車輌を被告に譲渡した後（この車輌は妻名義で登録されていた）、捜査員がGPS機器を取り付けたからである。しかし、取り付けが譲渡前であれば別の結論になる。つまり、法廷意見は被告の「動産受託者の財産権」を前提にしているが、受託者が動産の侵害について訴訟を提起できるのは、動産を受託している期間に損害が生じた場合だけである。従って、被告の妻が被告に車輌の鍵を渡す以前に機器を取り付けていた場合には、被告は不法侵入を主張しえないことになる。

③ 法廷意見に基づけば、修正第四条の保護範囲が州によって変わってしまう。夫婦共有財産制度（community property）を採用し、夫婦統一財産法（the Uniform Marital Property Act）を制定している州であれば、被告は車輌所有者である。GPSの取り付けと譲渡の時期は問題にならない。他方で、そうし

なく、プライバシーの「合理的期待」審査を中心に考えている。

た夫婦財産制度を採用していない州では、妻名義での車輌登録は妻の単独所有を推定する根拠とみなすのが一般的である。

④　法廷意見の不法行為論では、追跡対象について（物理的ではなく）電子的な接触（electronic contact）による場合には面倒な問題を生じる。これまでは動産への不法侵入というためには物理的接触が要件だったが、コンピュータ・システムへの電子的接触の場合には見解が分かれるからである[46]。

以上のようにアリート裁判官は法廷意見を矛盾点や難点を指摘した上で、本件の状況における「合理的期待」を次のように論じた。

人の公道上の移動について比較的短期間のモニタリングはわれわれの社会が合理的だ（reasonable）と認めてきたプライバシーの期待に適合している。しかし、犯罪捜査を目的とした長期間のモニタリングはプライバシーの期待に悪影響を及ぼすだろう。社会の期待とは、そのような目的で警察は個人の自動車の移動をきわめて長期にわたって密かに監視したり、記録なんかしないだろう（実際には大抵はありえないだろう）というものである（アリート裁判官意見）。

つまり、アリート裁判官によれば、プライバシーの問題は場所が公的か私的かというような単純な二元論ではない。より複雑な要素（監視の時間・定量・性質）から公私のグレーゾーンを評価しなければならないといえるだろう。

3．ソトマイヨール裁判官の結果同意意見

ソトマイヨール裁判官は法廷意見とアリート裁判官の意見に同意したが、い

[46] 例えば、本件のFBI捜査員が盗難車輌探知システムを密かに起動して被告を追跡するような場合に、「システムを起動するためのシグナルを送信することが動産への不法侵入になるのか」。アリート裁判官によれば、裁判所によっては、あるPCから別のPCに情報が送信されるときに生じる電気の伝送だけも「侵入」になると判示したものもある。see CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, at 1021 (SD Ohio 1997).

くつかの点で最も大胆な理由付けを展開しているように思われる。

修正第四条は財産に対する不法侵入だけに関係するわけではない。むしろ、不法侵入がない場合でも「社会が合理的だと認めている、プライバシーについての主観的な期待を政府が侵害するようなときには、修正第四条の捜索が生じる」(Katz, 389 U.S. 347, at 361, Harlan, J., concurring)。Katz 判決では修正第四条の範囲は「物理的な侵害の有無で決まるわけではない」と判示して、財産権に着目した従来の方法を拡張したのである。しかし、法廷意見が明らかにしたように、Katz 判決の合理的期待テストは優勢になったが、それ以前のコモンロー上の不法行為テストを破棄して、これに取って代わったというわけではなかった（ソトマイヨール裁判官意見)。

ソトマイヨール裁判官は不法行為論と合理的期待論をともに認めて、合理的期待を審査する際には、監視期間の長短だけでなく、さらに多くの要素を考慮すべきことを主張している点が特徴的である。具体的には GPS 監視の性質・影響を次のように論じた。

GPS モニタリングは、公共の場所での人の移動を正確に包括的に記録する。この記録はその人の家族・政治・職業・宗教・性などの人間関係について豊富な情報を反映している。…政府はそうした記録を保存し、後で情報として効果的に取り出すこともできる。また、従来の監視技術と比較すれば、GPS モニタリングは費用がかからず、任意に秘密裏に行えるので、警察実務の権力濫用を抑制する通常のチェックを免れる。…政府が監視できるという認識は人間関係や表現活動の自由を萎縮させるだろう。個人のアイデンティティのプライベートな側面をあきらかにするようなデータを収集する政府の無制限の権力は濫用されやすい。結局のところ、GPS モニタリングは（政府が自由な裁量でトラッキング対象を選択すれば、いかなる人についてでも、相当程度の個人情報を比較的低コストで収集･利用可能にするという点で)

「市民と政府の関係を民主社会に反するやり方で変える」[47]かもしれない（ソトマイヨール裁判官）。

つまり、公共の場所での人の移動に関して、プライバシーの社会的な合理的期待があるのかを考える際には、監視技術の発達、政府の権力濫用の危険性、言論・宗教・人間関係の自由に対する萎縮効果、民主社会における監視の弊害など、GPS監視の性質・態様・影響をあわせて評価すべきだという。その上でソトマイヨール裁判官は合理的期待審査を次のように再定義している。

人の政治的・宗教的信条や性的な習癖などを政府が確定できるような方法で、自分たちの動向が記録され、集約されることを人々が予期していると考えるのが合理的かどうかを検討すべきである（ソトマイヨール裁判官）。

さらに、より本質的だと思われる問題提起は「第三者に自発的に開示された情報についてはプライバシーを期待できないという前提を考え直すこと」の必要性を主張している点である。

このアプローチはデジタル時代に適していない。デジタル時代には、日常の仕事をしながら、人々は多くの個人情報を第三者に開示している。…アリート裁判官が述べているように、便利な「価値あるもの」とプライバシーはトレードオフだと思っている人、あるいは「プライバシーの縮小」を「不可避」だと諦めて受け入れている人もいるかもしれない。過去に自分が訪問したすべてのウェブサイトのリストを令状のないまま政府に開示することを人が不満なく受け入れるとは、少なくとも私は思っていないけれども。ただ、社会の期待はどうであれ、憲法上保護されるのは、修正第四条の法理が「秘密」をプライバシーの必要条件として考えるのをやめる場

[47] United States v. Cuevas-Perez, 640 F.3d 272, 285（CA7 2011）, Flaum, J., concurring.

合だけである。ある限定された目的で一定の公衆に自発的に開示された情報はすべて、まさにそれだけの理由で（自発的に開示されたという理由だけで）修正第四条の保護を奪われるのである（ソトマイヨール裁判官）。

ソトマイヨール裁判官はアリート裁判官以上に合理的期待審査の内容を大胆に再構成している。特に最後の「秘密パラダイム」の放棄が今後の事件でどう評価されるのかは注目されるだろう[48]。

このようにJones判決はいくつかの点で従来の方針を転換したが、公共の場所でのプライバシーが保護される可能性は拡大したとも単純には思われない。また、法廷意見も個別意見にしても、GPSによって特定された位置情報がどのような意味でプライバシーになるのか、その侵害はどのような状況で生じうるのか、テクノロジーの発達をどのように評価すべきかなどの点では必ずしも明確ではない。そこで、次章では公共空間における位置情報の意味をテクノロジーとの関係から考えてみたい。

Ⅲ．存在の匿名性と位置情報プライバシー

2007年のiPhoneのスマートフォン市場への参入を契機に位置情報を扱う多様なサービスが急速に普及した。もはや位置を特定するテクノロジーは警察・救急など緊急システムだけで用いられるものではない。位置情報はPC、スマートフォン、デジカメ、ネットワーク・プリンタなど多くの情報機器に組み込まれている。これらテクノロジーとサービスはプライバシー（＝存在の匿名性）にどのよう影響するのか、どのような場合に位置情報がプライバシーだといえるのか。「位置情報プライバシー location privacy」という概念に着目したい[49]。

[48] Daniel Solove, *Digital Person*, pp42-44.

[49] Blumberg and Eckersley, "On locational privacy and how to avoid losing it forever" retrieved fromhttps://www.eff.org/wp/locational-privacy

1．位置情報とプライバシー

位置情報とプライバシーの結びつきは新しいわけではない。例えば1930年代の（合衆国農務省による）航空地図の作成が契機だったと考えられるが、当時はプライバシー＝匿名性の侵害はさほど関心を引かなかった。人の所在地が容易に特定・売買されるようになって初めて位置情報が問題となったといえる[50]。位置情報とプライバシーを争点化した社会工学的コンテクストとして、①データベースの進化と②位置認識テクノロジーの普及を指摘できるだろう。情報はデジタルのデータベースに集約・保管され、市場で交換されうること、データの解析手法は空間／場所などリソースへのアクセスを管理するように機能すること、つまり本人認証システムに結びついている。

①データベースの進化

90年代半ば以降のコンピュータのネットワーク化はデータベース化を促進させた。それ以前には、記録は特定の保管場所でだけでアクセス可能だった。もしくは別の場所で記録を閲覧したい場合には、保管場所の規則に従ってアクセスしていた（コピーの郵送など）。しかし、記録のデジタル化によって、個別の記録だけでなく記録システム全体の検索・複製・移転が可能になった。デジタル化による保管コストの低減は記録が永久に保管され、移動することを意味していた[51]。

プライバシーと関わって、データベースの重要な特徴の一つは、人間と違っ

---

[50] 地図作成のテクノロジーの発展とプライバシーの結びつきに関しては、see Mark Monmonier, *Spying With Maps: Surveillance Technologies and the Future of Privacy*（The University of Chicago Press, 2002）.

[51] Mark Poster, *The mode of information: Poststructuralism and Social Context*, ch.3（Polity Press, 1990）；邦訳（室井尚・吉岡洋）『情報様式論：ポスト構造主義の社会理論』（岩波書店、1991年）；David Lyon（ed.）, *Theorizing Surveillance: The panopticon and beyond*（Routledge, 2006）；D. Lyon, *Identifying Citizens: ID Cards as Surveillance*（Polity Press, 2009）；邦訳（田端暁生）『膨張する監視社会：個人識別システムの進化とリスク』（青土社、2010年；）

てコンピュータの「記憶は消去されないこと」である[52]。そもそもプライバシーを保護する究極の方法は「記憶の消去」である。人が通常とは異なる振る舞いをするとき、あるいは公共の場所で政治活動に参加するとき、匿名を保護すること（＝ある時間と場所に誰が何をしていたのかを記憶＝記録しないこと）が重要になる。しかし、オンライン・カメラ、顔面認証システム、位置情報システムの発達によって、政府や企業はある場所での出来事や人々の行動を正確に記録・集約・結合・保管できるようになった[53]。こうしたデータに基づいて政府も企業も人々の場所や時間に関わるプロファイルを作成し、それによって人々の行動を追跡＝予測しようとしている。記録はもはや消去されることはなく、別の時間・場所で収集された記録と集約・照合・結合されるのである。

さらにデータベースの特徴は、どんな情報が収集されて、誰がアクセスしているのかについて、市民（情報主体）は知らない（もしくは意識していない）ことである。オンラインで情報を収集するアーキテクチャは十分に理解されているとはいえない。電話やインターネットは単一ではなく様々な媒体から構成される複雑なシステムであるので、一般市民だれもがシステム内部のアーキテクチャを理解して自分で管理できると考えるのは無理がある。

また、より深刻な問題は、一方で多くの人はプライバシーを失うことを心配しつつ、他方では消費者として人は情報をデータベースにすすんで提供している事実である。例えば、クレジットカード会社による買物履歴の記録やAmazonによる購入履歴の管理にはさほど注意を向けない。個人情報と交換でえられる利益に価値があると考えているからである[54]。日常生活において利用

[52] 「暗い記憶あるいは色あせてゆく切り抜きに捕らえられた細部はいまやコンピュータのデジタル・マインド、個人データの肥沃な領域をもった巨大データベースに永遠に保存される」。Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," 53 Stan. L. Rev. 1393, at p1394.

[53] Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York University Press, 2011) ; David Lyon (ed.) , *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (Routledge, 2003) .

[54] Reg Whitaker, *The End of Privacy: How total surveillance is becoming a reality*, ch.5 (The New Press, 1999) .

するオンライン・サービスの大半は個人の基礎的なデータ（メールアドレス・氏名・住所・電話番号など）との交換によっている。従って、SNSのユーザが増える（情報の共有量が増える）ことはサービス事業者の市場価値を高めることになるし、市場価値が高まれば、さらに情報の共有が促進されるのである[55]。

②位置認識テクノロジーの普及

GPSやSIPを使ったロケーションサーバの位置情報サービスが普及する以前にも電話を用いて位置を特定する方法はあった[56]。ただ、かつての位置認識テクノロジーは緊急システムで用いられることが想定されていたのに対して、今日のトラッキングは広い範囲で実用化されている。位置情報は利便性・娯楽・利潤のために売買される財であり、消費者はその利便性のために監視を受容しているのである[57]。

それでは、位置情報とプライバシーの関係はどのように概念化されるのだろうか。位置情報を共有することで常に侵害が生じるとはいえない。一般的に、位置情報の開示には本人の同意があること、（許可されていない）他者が位置

[55] 例えば、Facebookは様々な情報シェア機能を追加しながら成長を続けている。特にプライバシーが問題化した機能として、ニュース・フィード機能がある。これは人のプライバシー認識の違いが要因になったと思われる。ニュース・フィードについては、http://jp.techcrunch.com/archives/20100422facebook-edgerank/、Facebookの公式サイトによる説明は、http://f-navigation.jp/manual/contactfriend/newsfeed.html、写真投稿については、http://www.rbbtoday.com/article/2012/04/11/88235.html、参照。

[56] 例えば、電波の三角測量による位置の特定する技術は緊急通報システム（Enhanced 911）で採用されていた。Enhanced 911とは、米連邦情報通信委員会（FCC）によって開発された、携帯電話から緊急通報ダイヤル（911）への連絡を行い、同時に通話者の位置を特定する技術である。それまで携帯電話から緊急連絡を行うときには、携帯キャリアへの接続を経由してアンサーポイントに接続されていた。それに対して、Enhanced 911では、プロバイダーやキャリアによらず、通信は通常の電話回線と同じように直接近くのアンサーポイントへと接続され、位置確認が行われる。E911システムの運用については、救急だけでなく警察にも位置情報は利用可能であったことから、携帯電話が警察による追跡装置に容易に変わりうることが指摘されていた。参照、http://www.sophia-it.com/content/Enhanced+911

[57] 監視が標準化し受容されるプロセスについては、see William G. Staples, *The Culture of Surveillance: Discipline and Social Control in the United States*, ch.1（St. Martin's Press, 1997）.

履歴を追跡しないことが前提とされている。この期待が裏切られるときに侵害が生じるだろう。例えば、次のような場合である。

a．入店と同時に店員が客の身元を確認し、オンラインのデータベースに保管されている個人情報・購入履歴・クレジットカード履歴などに基づいて消費行動を予測し、商品を薦めるような場合。
b．メンバーと位置情報を共有するソーシャル・ネットワーク・サービスにおいて自分がサインアップしていない位置情報広告を受信するような場合。

つまり、侵害が生じうるのは、本来の目的から離れて、情報のコンテクストが変わったときである。このことは、場所には関係なく、人が匿名を期待する状況があることを示唆している。ユビキタス社会では物理的な場所の性質に応じてプライバシーが問題になるわけではない。他者からどの程度の距離をとるのか、他者のアクセスをコントロールできるという意味での「匿名性」を奪われることが侵害を感じる要因だと考えられよう。

2．位置情報と監視

以上のように、位置情報を追跡・共有することは監視であり、モバイル・インターフェイスが普及した社会では、政府・企業・個人が監視主体になる。政府による監視だけを特に強調すべきではない[58]。むしろ企業の方が人の消費生

[58] 監視には政府と企業による「トップ・ダウン」型監視と、市民の間で生じる「付帯的」監視がある。政府の様々な監視システムに対する不信は国によって違う。政府に対する信頼度の違いは政府が市民の個人情報に政府がアクセスすることを市民がどう感じるのかにも影響している。see Adriana de Souza e Silva and Jordan Frith, *Mobile Interfaces in Public Spaces*, pp121-27; Colin J. Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance*, pp9-17（The MIT Press, 2008）；福祉国家的な給付サービスには個人情報の収集が必要なこともあるが、程度を越えれば問題である。see John Gilliom, Overseers of the Poor: Surveillance, *Resistance, and the Limits of Privacy*（The University of Chicago Press, 2001）.

[59] Eli Pariser, *The Filter Bubble: What the Internet is Hiding from You*（Penguin Press,

活に深く浸透している点では深刻かもしれない[59]。監視は公私の区分を超えて浸透しているのである。

①政府

政府による監視は「ビッグ・ブラザー」(George Orwell) や「パノプティコン」型監視 (Michel Foucault) のメタファーで論じられてきた[60]。これらのメタファーはわかりやすいが、分析概念としてはさほど有益でもない[61]。普遍化しているのは大量の情報を全方位で記録するような「毛細血管」型の監視 (dataveillance = all-seeing surveillance) だからである[62]。つまり、監視技術は「観る / 観られる」という関係性の操作ではなく、情報収集とデータベースにある。ユビキタス社会の監視が問題になるのは、人々を「正常化 / 標準化」するからではなく、むしろ (多様性を認めた上で) 人の行為・考え方・態度を予想可能にして、管理するからだと考えられる。予測は望ましくない行為を予防して、望ましくない人物を排除することに役立つ。また、もともとはさほど

2011)；邦訳 (井口耕二)『閉じこもるインターネット：グーグル・パーソナライズ・民主主義』(早川書房、2012年)。

[60] ジョージ・オーウェル (高橋和久訳)『一九八四年 (新訳版)』(早川書房、2009年)；フーコーは、現代社会では人をコントロールし、行為を正常化 (normalize) するためには監視と統計が重要になることを指摘した。監視による規律と抑制の効果の例として、フーコーはベンサムの考案によるパノプティコンの構造を論じている。see Michel Foucault (translated by Alan Sheridan), *Discipline and Punish: The Birth of the Prison* (Vintage Books, 1977)；邦訳 (田村俶)『監獄の誕生』(新潮社、1977年)；T. L. Dumm, *Michel Foucault and the Politics of Freedom* (Rowman & Littlefield Publishers, INC., 2002).

[61] EFF (Electronic Frontier Foundation) のアプローチは「ビッグ・ブラザー」的な監視を想定しているようにみえる。EFFによれば、人がアクセスされたくないと思う一定の情報 (例えば「反戦集会に行ったか」「中絶クリニックに入ったか」など) に対する政府の「侵入」が位置情報プライバシーの問題である。EFFが提唱する位置情報プライバシーについては、see https://www.eff.org/;「ビッグ・ブラザー」のメタファーがもはや古い点については、see Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, ch.10 (Yale University Press, 2011).

[62] Solove, *The Digital Person*, ch.1; Whitaker, *The End of Privacy*, ch.5; Colin J. Bennett, "The Public Surveillance of Personal Data: A Gross-national Analysis," in David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy* (University of Minnesota Press, 1996).

重要でない日常の行為も、データベースに集約されるときには新しい情報に転化しうる。こうした監視に対しては（政府から）「隠すものは何もない」と考えてもあまり意味がない。人の行為は本人が知らない事柄も語っている。ある人のデータが別の人の重要な情報を追加することもある。こうした情報は権力の源泉にもなる。

ただ、政府による監視がすべて悪でもない。例えば、J. M. Balkinは「監視国家」を「権威主義的情報国家 authoritarian information state」と「民主的情報国家 democratic information state」に区別して論じている。権威主義的情報国家は情報を貪欲に収集するだけで、決して開示しない国家である。情報を開示せずに市民から秘匿する。政府の権威を損なうおそれのあるものをすべて「国家機密」として扱う。「機密」に関わる規則や規制を増殖させ、政府の活動を説明しないまま市民を法に服従させる。権利侵害や失政について説明応答責任を果たさず、情報を操作しながら統治権力を保持しようとする。反対に、民主的情報国家は効率的な統治と安全保障を確保するために必要な情報だけを収集する。正当な理由なく市民をタグづけたりはしない。民主的情報国家は（例えば、教育・科学研究、医療・農業など）価値ある情報を市民に公開する。政治的意思決定のプロセスに関わる情報へのアクセスを認めて、市民が政府に対して説明応答責任を問うことを可能にする。権力濫用を防ぐのは情報へのアクセスと公開だからである[63]。このように、権威主義的情報国家を抑制し、民主的情報国家に方向づける基本的リソースが憲法である[64]。

---

[63] Jack M. Balkin, "The Constitution in the National Surveillance State", pp204-5, in J. M. Balkin and Reva B. Siegel (eds.), *The Constitution in 2020* (Oxford University Press, 2009).

[64] ただ、政府と企業の協働関係の場合は問題がある。企業は個人情報を集約して、新規顧客の獲得や望ましくない顧客の排除にも利用しているが、こうした情報を別の企業や政府と売買することもある。ただ、憲法は私的団体を直接には対象としていないので、政府が情報収集を企業にアウトソーシングすれば、憲法上の制約を受けないことにもなりかねない。

②企業

企業の広告活動にとっても個人情報はなくてはならないものである。例えば、Google のメールクライアントではメール内の文字列が自動的に分析され、関連広告が画面に現れる仕組みになっている[65]。こうした高度にコンテクスト化された広告には個人情報は不可欠であり、位置情報もその一つである。

位置情報広告（location-based advertising）の仕組みは簡単である。典型的には、ユーザが配信サービスにサインアップしておけば、サービス対象の店舗の近くを通りかかるとクーポン付き広告が配信されるというような仕組みである。企業にとってはユーザが店舗の近くにいるときに（＝最も利用しそうなときに）サービスを通知できる点で、ユーザにとってはクーポンを（必要とする場所で）手軽に受信できる点で、位置情報サービスは両者に便利である[66]。しかし、このような広告もまた監視であり、企業が個人をモニタしていることを意味している。

位置情報広告の問題は、モバイル情報機器の特性による面もある。ある調査によれば、人はモバイル端末を PC よりも「パーソナル」だと思っている。そのため、PC よりもスマートフォンで未承認広告を受信することを私的空間への侵入の度合いが強いと感じている[67]。従って、事業者はユーザに選択権があ

[65] Google は検索技術、電子メールクライアント、オープン・ソースのソフトウェアの開発などで知られるが、その収益の大部分は広告という点で本質的には広告企業である。Google の成り立ちと影響力について、さしあたり以下を参照、スティーブン・レヴィ（仲達志・池村千秋 訳）『グーグル：ネット覇者の真実』（阪急コミュニケーションズ、2011 年）；Siva Vaidhyanathan, *The Googlization of Everything: And Why we should worry* (University of California Press, 2011)．

[66] 位置認識広告には①プッシュ型と②プル型という二つのサービス類型がある。プッシュ型はユーザの端末にオファーを送信するサービスであり、プル型はユーザがログインして、自分がいる場所の近くで何かサービスを提供している店がないか探すような方法をいう。プッシュ型には、さらに広告を送信する二つの方法（非リクエスト型と間接的リクエスト型）がある。非リクエスト型はユーザに広告メールを勝手に送信するのに対して、間接的リクエスト型は広告受信の同意をユーザにあらかじめ求めるものである。see Bernhard Kolmel and Spiros Alexakis, "Location Based Advertising", retrieved from http://www.e-lba.com/YellowMap_Location%20Based%20Advertising%20mBusiness%20Conference%202002.pdf.

[67] see Matti Leppaniemi and Heikki Karjaluoto, "Factors influencing consumers'

ることを丁寧に説明する必要がある。例えば、次のようなポリシーである。

当社では、モバイル・データ・サービス、緊急サービスの提供、また地理案内、天気、位置確認、子どもの安全確認のためのアプリケーションとツールのような当社とサード・パーティーが作成した位置情報アプリケーションとサービスをご提供することなど、様々な目的からモバイル機器の位置データを収集・利用しています。従って、当社では位置情報アプリケーションを提供する場合、お客さまのスマートフォンで利用可能な個々の位置トラッキング機能をオンにするかどうかについて、お客さまにお知らせし、選択していただいています[68]。

Google ロケーション・サーバー（GLS）で使用している Wi-Fi アクセス・ポイントのシグナルはユーザを識別しませんが、ご自身のアクセス・ポイントを GLS に追加されたくない場合（オプトアウト）は次の手順に従ってください[69]。

いずれも消費者が自らの選択でサービスに加入していること（個人情報を管理できること）がサービス提供の前提となっている（選択的加入）。その上で、収集される情報の種類や処理の方法を次のように説明する。

当社ではサービスの利用情報と顧客情報を各事業と市場調査に使用することがあります。利用情報には当社のワイヤレス・サービスをご利用時のウェブサイトのアドレスが含まれます。これらデータにはお客さまの検索語句も含まれます。また、利用情報にはご利用端末の位置、ご利用のアプリケーションと機能も含まれます。顧客情報には当社製品とサービスのご利用に関する情報（データ通信・通話、端末の

willingness to accept mobile advertising: a conceptual model", International Journal of Mobile Communications, Vol.3, No.3. pp197-213（2005）.

[68] Verizon Wireless 社のポリシーを参照。http://www22.verizon.com/privacy.

[69] Google 社の説明を参照。http://support.google.com/maps/bin/answer. pyhl=ja&answer=1725632.

タイプ、利用時間)、また他者から当社に提供される人口統計と関係性のカテゴリー(ジェンダー、年齢、スポーツの好み、行きつけの店、ペット所有など)が含まれています。当社は個人を特定しない方法で情報を結合することがあります。そして、当社が統計事業と市場調査レポートを作成するために使用し、他社と共有することもあります。また、当社では、他社が事業・市場調査レポートを作成するために、個人を特定しない方法で位置情報を他社に提供することもあります。当社のお客さまはこれらレポートに情報を提供するかどうかを選択できます[70]。

このような説明によれば、情報がどう処理されているのかをユーザが確認する手段が確保されているわけではない。情報の保管期間や情報提供の相手方についても明確に説明されているとは言いがたいとすれば、選択的加入論はその前提を欠いていると思われる[71]。

③個人

相互に位置情報を共有している個人の間でもプライバシー侵害が生じる場合もある。「路上での自由な交流/街路の眼差し」はコミュニケーションを補強し、都市生活の安全性を維持する上では必要だが、他者を排除する相互監視にもなりうる点には注意を要する[72]。

位置情報に基づくソーシャル・ネットワーク・サービス(SNS)はユーザが相互にフォローすることで機能している。ユーザが位置情報をコントロールする方法は情報を共有するメンバー数を制限するか、もしくは特定の場所を選択

[70] Verizon Wireless 社のポリシーを参照。http://www22.verizon.com/privacy.

[71] Joseph Turow, *Americans and Online Privacy: The system is broken. A report from the Annenberg public policy center of the University of Pennsylvania* (2003) retrieved from http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf.

[72] Jane Jacobs, *The Death and Life of Great American Cities* (Vintage Books edition, 1992) ; Oscar *Newman, Defensible Space; Grime Prevention through Urban Design* (Macmillan, 1972) .

して「チェックイン」するかである[73]。しかし、トップダウン型監視と同じように、自分の位置情報に誰がアクセスしているのかを多くのユーザは認識していない／できない。サービス事業者のポリシーが曖昧だからである。

結局、位置情報プライバシーの侵害では、誰と・どこで・どのように情報を共有するのかは重要な要素である。位置情報を限定された小集団で共有すること（foursquare）、誰かの位置情報を広範囲の参加者で共有すること（Whrrl）、あるいはTwitterで位置情報を共有することは同じではない[74]。位置情報プライバシーを維持するには、このような位置情報が共有されるコンテクストの差異にも留意すべきだと思われる。

3．情報テクノロジーとプライバシー侵害

今日の位置情報サービスで用いられているモバイル・インターフェイスは、90年代最初にゼロックスのパロアルト研究所（XEROX Palo Alto Research Center）のMark Weiserらが提唱した「ユビキタス・コンピューティング」という理念を原型としている[75]。Weiserらが適切に指摘したように、ユビキタス社会では情報のコントロールのあり方が問題となる。位置情報は、いつ・どこで・誰と・どのように共有するのかをコントロールできないとき、人はプ

---

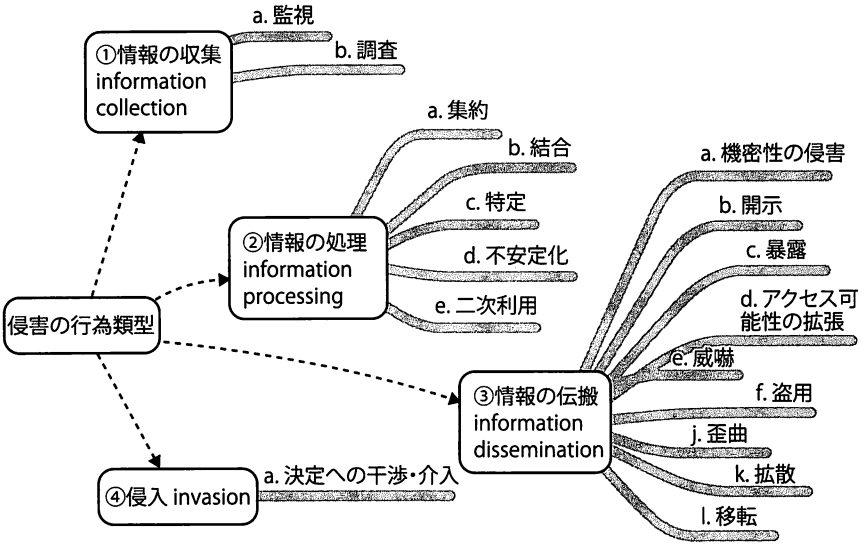
[73] 調査によると、多くの人は自宅とその近所の位置情報を共有することは望んでないが、レストランのような公共の場所で自分の位置情報を開示することは気にしていないという。see A. J. Brush, John Krumm, and James Scott, "Exploring end user preferences for location obfuscation, location-based services, and the value of location," in Proceedings of UbiComp 2010, retrieved fromhttp://research.microsoft.com/apps/pubs/default.aspx?id=135611

[74] 規模・範囲については、〈foursquare〉と〈Whrrl〉のソーシャル・サービスを参照。https://ja.foursquare.com/about/newfrom=hp、http://www.crunchbase.com/product/whrrl。〈Twitter〉については、http://twinavi.jp/ を参照。

[75] 「ユビキタス・コンピューティング ubiquitous computing」とは、端的に言えば、コンピュータはデスクトップに拘束されずに、ネットワークを通じて日常生活に浸透すべきだという理念である。See M. Weiser, R. Gold and J.S. Brown, "The origins of ubiquitous computing research at PARC in the late 1980s," IBM Systems Journal, 38 (4), 693-696 (1999).

ライバシーの「期待」が害されたと感じるのである。

では、「コントロールできない」とはどのような意味だろうか。この点について、D. Solove によると、侵害は、①情報の収集、②情報の処理、③情報の伝搬、④侵入という四つの基本類型に分類可能である。この類型にはさらにサブカテゴリーがある（下図参照）[76]。



位置情報の場合には、特に「監視」と密接に関わるプロセス①②から次のように説明できるだろう。

a．位置情報をどのように処理して保管するのか、調査に関わって、政府と企業の間の情報共有や協働関係があるのかなどについて明確な説明がないこと。このことはユーザ / 市民（データ主体）にとってコントロールの喪失感につながる。

b．ユーザ / 市民が自分の情報にアクセスして誤りを訂正できないこと、情報がどのように利用されているのかについて確認する手続がないこと。こうし

[76] Daniel J. Solove, *Understanding Privacy*, pp103-4.（Harvard University Press, 2008）.

た状況は「排除」である。

c．情報の断片（郵便番号・購入履歴・位置履歴など）を「集約」し、個人と結びつけて「特定」すること。それだけではプライバシーとはいえない情報が別の情報と「結合」され、相互に関連付けられた情報は「二次利用」されることもある。

こうした侵害を抑制するためには「監視者の監視」がまず必要である。少なくとも、データ保持者対して、透明性の確保、答説明責任の確立、権限濫用に対する強力な罰則、データの完全消去（二次利用・流用の防止）についてルール化を指摘できるだろう。

むすびにかえて

本稿では、公共空間における匿名性の意味を特に位置情報とプライバシーの関係から検証した。十分に論じたとはいえないが、いくつかの問題点を整理してむすびにかえたい。

プライバシーを複雑にしている要因は、私的でも公的でもない領域／事項があることである。しかし、法的にはプライバシーの保護範囲を画定しているのは公私二元論の解釈である。私的領域の保護は正当だが、そこから遠くなるほどプライバシーの法的地位は不確かになる[77]。

判例上、プライバシーの範囲を画定する公私二元論にはいくつか側面がある[78]。例えば、誰かの寝室をのぞき見する場合、警察が被疑者の通信を傍受する場合には、少なくとも二つの侵害が考えられる。一つは私的領域の侵害を理由とするコンセプト（領域の公私二分論）、もう一つは観たり聴かれたりした

[77] 自己情報コントロール権という場合もすべての個人情報が保護対象になるわけではない。see Daniel J. Solove and Paul M. Schwartz, *Privacy, Information, and Technology*, ch.1（Wolters Kluwe, third edtion, 2011）.

[78] ①主体、②領域（空間）、③情報について公私の二分論がある。see Nissenbaum,

ものの情報内容を理由とするコンセプトである（情報の公私二分論）。これらの二分論は具体的な事件ではコンテクストに組み込まれているが、侵害を判断するにあたって二分論をどう評価すべきかが問われるだろう。

（物理的／抽象的）領域と情報内容は独立した概念である。これまでの修正第四条の審査では、情報内容よりも物理的／抽象的な領域もしくは空間の二分論が優先されてきたといえる[79]。例えば、熱線暗視カメラを使用して人の住居内部を探るためには修正第四条の令状を要する。「修正第四条は自宅の入口で明確に境界線を引いている」[80]。ただし、警察がヘリコプターを駆使して被告の所有する建物の上空（400フィート）から建物の開口部分を覗いても、被告には「プライバシーの合理的期待」はない。警察は「見晴らしのいい公共の場所から見えるもの」を確認しているからである[81]。上空では裸眼でなく航空カメラを使用してもいい[82]。

こうした領域の区別は、Jones判決のような位置情報のトラッキング事件ではより難しい問題になる。修正第四条の保護範囲の画定にあたって、これまでの公私二分論で判別しづらいグレーゾーンにどのように対応するのかという問題である。Jones判決の法廷意見と個別意見の解決策はそれぞれ今後の可能性を示唆しているが、位置情報とプライバシーの関係については論じなかった点ではなお課題も残したといえる。

では、そもそも位置情報はどのような意味でプライバシーと結びつくのだろうか。位置情報は単純に公私に分類されるものではない。確かに街のカフェにいるときや繁華街を歩いているとき、その人の位置情報は完全に「秘密」＝私的とはいえないが、公共の場所でも人はある程度の匿名性を期待することはありうる。公共の場所で位置を開示していることだけでは、第三者が位置履歴（そ

Privacy in Contex, ch.5.

[79] California v. Greenwood, 486 U.S. 35（1988）.

[80] Kyllo v. United States, 533 U.S. 27（2001）.

[81] Florida v. Riley, 488 U.S. 445（1989）.

[82] Dow Chemical Co v. United States, 476 U.S. 227（1986）.

れに付随する人間関係など）に自由にアクセスすることを許可していることにならないからである。位置情報の開示のレベルには様々な差異があることを留意しておくべきである。従って、位置情報プライバシーが侵害されたかどうかは、情報への不当なアクセスを制限できるかに関わっていると考えられる。

かつてブランダイス裁判官は制憲者が考えていたプライバシーを保障するためには修正条項を20世紀の社会に「翻訳」する必要があることを主張した。ブランダイスはテクノロジーの進化を予見していたかのように次のように述べている。「政府が秘密の引き出しから書類を取り出すことなく、法廷で複写できるような方法、自宅内の最も親密な出来事を陪審員に開示できる方法がいつかは発達するかもしれない」[83]。ブランダイスの想像以上にテクノロジーが進化した「ユビキタス」で「パーベイシィブ」なネットワーク社会では、位置情報はプライバシーの一要素である。

そう考えれば、テクノロジーを考察対象としてどのように理解すべきだろうか。テクノロジーは社会的・政治的・経済的な制度と相互依存の関係にあり、人の認識や社会規範にも影響してきた。修正第一条の法理は「匿名の言論」を保護してきたが、権利を行使できるかどうかは、逆探知されない公衆電話を利用できるか、匿名のwebブラウズを可能にするソフトがあるかによって違うだろうし、あるいはテクノロジーはオンラインの匿名性の意味さえ変えるだろう。「プライバシーの合理的期待」が依拠する社会の慣習や規範もテクノロジーと無関係ではなかった[84]。このような意味で、情報＝コミュニケーション・テクノロジーは公私の空間にアクセスするためのインターフェイスといえる[85]。

---

[83] Olmstead et al. v. United States, 277 U.S. 438 (1928), at 474, Brandeis, dissenting.

[84] Stuart Shapiro, "Place and Space: The Historical Interaction of Technology, Home, and Privacy", The Information Society 14: 275-284 (1998) ;Thomas C. Schelling, *Micromotives and Macrobehavior* (W W Norton & Co Inc, 1978).

[85] Jeffrey Rosen and Benjamin Wittes (eds.), *Constitution 3.0: Freedom and Technological Change* (Brooking Institution Press, 2011) ; Lee Tien, "Architectural Regulation and the Evolution of Social Norms", in Jack M. Balkin (ed.), *Cybercrime: Digital Cops in a Networked Environment* (New York University Press, 2007) ; *Solove, The*

かつてテレビが私的空間のなかで公共的なパフォーマンスを経験可能にしたように、モバイル・テクノロジーは私的空間の経験を公共空間において可能にしている。このことによって、公共空間のかたちがどのように変わりつつあるのかについてはまた別途論じたいと思う。

以　上

（2012年6月30日提出）

Digital Person, ch.6; Lessig, *Code version* 2.0, ch.4（Basic Books, 2006）; Cass Sunstein, "Switching the Default Rule," 77 NYU L. Rev. 106（2002）; Joel R. Reidenberg, "Lex Informatica: The Formulation Policy Rules Through Technology," 76 Tex. L. Rev. 533（1998）.