2007－EIP－35 (7)
2007／3／17

人物の所在情報の取得あるいは秘匿の今日的意義

中野潔[*1]

ユビキタスネットワーキングの普及に伴い，情報面でのプライバシー侵害が問題になるようになってきた。本稿では，まず，船越，青柳，小林の理論をレビューした。船越は，「存在や行為の痕跡」を各主体が制御することが必要だが，実現については難しいので議論が必要であるとした。青柳は，不可侵私的領域に属する情報については法的強制力を行使してでも保護すべきだが，それ以外の部分では自由な流通を許して，電子商取引などを隆盛に導くべきだと主張した。小林は，憲法 13 条により保障される基本的人権として「みだりに行動を記録されない自由」があるとした。筆者は，不可侵私的領域に属さない存在や行動の痕跡も，記録して統合すれば，個人のセンシティブな情報について確度高く推定できてしまうと考え，小林の考えにおおむね賛同した。RFID などを用いて存在や行為を記録することで目的を果たす，ユビキタスネットワーク社会ならではのシステムへの期待が高まっている。これらシステムの利用を全面否定せずに，「新しい法理」を形成していくしかないと考える。

Contemporary Meaning of Acquisition and Suppression of Human Location Information

Kiyoshi NAKANO[*1]

The invasion of privacy in respect of information has come to become a problem with the spread of ubiquitous networking. The author reviewed the theory of Funakoshi, Aoyagi, and Kobayashi first in this paper. Funakoshi pointed out the necessity and dificulty of control of trace of existence or an act by each subject. Then he concluded that an argument is required to solve this problem. Aoyagi insisted that we should block leaks of information belonging untouchable personal domain even if we use legal force. Then he claims that we should permit free circulation of information outside of the domain to make electronic commerce prosperous. Kobayashi presupposed that there is "freedom in which action is not recorded indiscriminately" as fundamental human rights secured by Article 13 of the constitution. The author joins in with Kobayashi's claim because if someone records and unifies the trace of the existence and action which do not belong to the untouchable personal domain, he/she could extrapolate sensitive information with high degree of certainty. The expectation for the system which would be available only in the ubiquitous network is growing. The example of the system is what achives the purpose by recording existence and an act using RFID etc. The author thinks that "a new principle of law" must be formed without denying use of such kind of systems completely.

1. はじめに

ユビキタスネットワーキングの普及に伴い，RFID を用いたシステムの応用が広がってきた。[01),02)03),04),05)]一方で，情報面でのプライバシー侵害が問題になるようになってきた。市民が嫌がる，あるいは，懸念する，本人以外の主体による個人情報活用行為の中には，個人情報保護法によって，防げるものもあれば，防げないものもある。

まず，多数の人の情報を保持している事業者以外の者は，強い拘束を受けない。また，電子メールのアドレスや RFID のチップの ID など，それだけでは個人識別情報とならない情報と，そのアドレスや ID の持ち主(物理世界における実名がわかっていない)の所在や行為に関する情報を束にして記録しても，別に法律違反にはならない。

本稿では，船越[06)]，青柳[07)]，小林[08)] のこの分野に関連する言明を分析することで，ユビキタスネットワーク会における個人情報などの扱いに関する問題点について考察する。本稿では，紙数の関係もあり，監視(防犯)カメラや GPS 機能付き携帯電話などに関連するところは，原則として触れない。RFID を用いた各種システムや各種 ID を用いた電子商取引システムを念頭に置く。

2. で，ユビキタスネットワーク社会におけるプライバシーと個人情報に関する 3 人の先人の意見をまとめる。3. で，社会で人と人とが付き合うときの基本的材料とでも呼ぶべき個人識別情報の共有性について考える。また，基本的な個人識別情報への各種個人情報のひも付けの問題にも触れる。4. で，利便性を享受するためには，各種個人情報を各種の事業者に開示せざるを得ないという現実と，それがトレースされ統合されることによるリスクについて論じる。5. では，RFID を用いた児童生徒の安全確保システムに関する保護者の意見を示して，RFID を用いたシステムが事実として，社会に受け入れられているという現実提示の材料とする。6. が，むすびである。

なお，本節でいう個人情報とは，必ずしも個人情報保護法で定義している個人情報と同義であるとは，かぎらない。

2. ユビキタスネットワーク社会におけるプライバシーと個人情報

*1 大阪市立大学, Osaka City University

2．1．ユビキタスネットワーク社会におけるプライバシー

2．1．1．プライバシーと不可侵私的領域

船越は，【群れて暮らす人間は相互の個人空間侵害に対しては，一定限度までは受忍し合い，その侵害が生存基盤の限度を越える場合にのみ妨害排除ができる】仕組み，すなわち，スペーシング機構(自分の周りに警戒領域や不可侵の領域を作り，それへの他者の踏み込みに応じて対抗する仕組み)を議論の出発点としている。[09]

これをもとに，【古来から，人は個体と個体とを分かつ心理的物理的情報空間を本能的・社会文化的に持っていて，それを基盤に群れているが，その心理的物理的情報空間を社会的規範として表出し，法的保護に値する利益と認めたのがプライバシーの権利ではないだろうか】――と主張する。知られたくないことを知られるという，守りたい領域への踏み込みも，物理空間への踏み込みと同様に捉えるのである。

青柳も，この点については，船越に賛同し，このスペーシング機構におけるスペースを「不可侵私的領域」と呼ぶ。【人間が社会的な生活を営む限り，必ず他者とのふれあいは生じ，情報や環境を共有するわけであるから，私的領域のすべてが不可侵とまではいえない。私的領域のうちの，ある小さな限定的な領域を「不可侵私的領域」として，互いに尊重しあうのがいいのだ】――とし，これを基礎としてプライバシーの問題を論ずるべきだとする。[10]

船越は，電子ネットワーク時代のプライバシーについての，スミーディングホフの言明を引用している。そのプライバシーは，(1)個人の人格に関するプライバシー，(2)個人データのプライバシー，(3)個人の通信のプライバシー，(4)匿名性――の4つに類型化されるという。[11] (2)に該当するものとして，スミーディングホフは，個人の消費活動記録，医療記録，入信状況記録，租税記録，保険記録，犯罪記録などをあげているという。

青柳は，プライバシーについて2つの定義を示した。【倫理的な意味におけるプライバシーは，互いに尊重しあうべき不可侵私的領域の概念である】，【法益としてのプライバシーは，公共の利益に反しない範囲において不可侵私的領域の存在を主張し，そのような領域に属する事柄の決定や個人情報の処理について一定の関与をする権利である】――の2つである。[12]

2．1．2．利益との引き替えによるプライバシー情報の提供

自己の情報関連のプライバシーに関する市民の意識についての認識においては，小林の理解も青柳のそれ(一部は後出)と大きく差があるわけではない。小林は，【われわれは普段，利便性などと引き替えにプライバシー情報の断片をばらまいていることを意識していない。しかし，意識したからといって，携帯電話やクレジットカードの利用を止める人は稀であろう。多くの人は，敵性に管理される限り，この程度のプライバシー情報の切り売りは差し支えないと考えている。

(中略)おそらくわれわれのプライバシー意識は，何らかの形で情報社会化との折り合いをつけようとしていると考える。それは，想像するに，利便性など一定の利益と引き替えに，プライバシー情報を提供するのは差し支えない，しかし(あるいはそれ故にこそ)，情報の管理には万全を期してほしい，という意識である。】と論じる。[13]

本稿では，基本的に，個人についての情報やデータに関する問題を論じる。スミーディングホフの論でいえば，(2)の問題が主で，状況に応じて，(1)や(4)の問題に触れる可能性がある。青柳の論でいえば，法益としてのプライバシーに議論を限定する。

以下で論じ，また，紹介していくように，筆者は，小林の問題意識に強く触発されている。しかし，小林が主に監視カメラについて論じているため，本稿では，小林の問題意識を見据えつつも，船越と青柳を主に引用しながら，論じていく。

2．2．「リトル・ブラザーズ」に関する課題

詳しくは，3．および4．で主に，船越と青柳を引用しながら論じるが，その前段階として，小林の指摘する「リトル・ブラザーズ」(小林は，この概念を東浩紀の造語をそのまま用いたものとする)に関する問題意識を示す。【われわれは，好むと好まざるとに関わらず，[引用者注：監視カメラに例示される，公的私的，多種多様な監視装置である]「リトル・ブラザーズ」の監視下におかれている。(中略)個々の「リトル・ブラザー」が把握するプライバシー情報は，通常，それだけでは，プライバシーの主体に不当な害毒をもたらすものではない。これらの情報が予期せぬ利用をされたり，流通して他の「リトル・ブラザー」の保有する情報と統合されたりするとき，プライバシーの主体に多大な害悪をもたらす可能性がある。】と，小林は指摘する。[14]

この，個々に収集された情報が単独ではプライバシーに対する大きな脅威にならないとしても，基本的な個人識別情報などにより，名寄せされたとき，脅威になりうる――という認識は，後出の船越や青柳の論においては，薄い。

しかし，ユビキタスネットワーク社会におけるプライバシーや個人情報の問題について論じるとき，これこそが大きな課題になる――と筆者は判断している。

2．3．ユビキタスネットワーク社会における個人情報とその経済的価値

次に，プライバシー一般ではなく，個人情報の問題について，みてみる。

船越は，【取引相手の個人データを収集するとき，可能な限り収入・負債・資産・支払能力など，その人の経済的データの収

集が情報価値を大きく左右するのであって，その人が温かい人か冷たい人か，おしゃべりかどうかなどの情報は，さほど重要ではない。ところが，温かい性格かどうか等の情報は，日常生活の対人認知に欠かすことのできない重要な内容である。】とする。[15]

この経済的データであるか否かが，個人情報の経済的価値に直結するという。個人に関する情報が経済的価値を持たない場合と持つ場合とについて，【社会的な存在形態に注目する場合と経済的価値に重きを置く場合とを区別する必要がある。】と指摘している。[16]（船越はそういう言葉を使っていないが）高度情報化社会においては，社会的な存在形態に関することが大きな割合を占めていた伝統的プライバシーと別に，経済的価値があるゆえに侵害されうる情報プライバシーの重みが増えてきたというのが，船越の主張の一端であると思われる。

この文脈の中に留まるかぎり，経済的な価値を持つ個人情報の問題は，ユビキタスネットワーク社会特有の問題とは，ならない。詳しくは，後で述べるが，社会的存在形態に関する情報の一種として，小林が指摘するように，特定の時刻に特定の場所にいたか否かという情報が存在し，これがユビキタスネットワーク社会特有のプライバシーあるいは個人情報の問題となってきうる。

青柳は，【プライバシーに属さない個人情報】といった表現で，個人情報の過剰な保護に関し，疑問を呈している。[17]【ユビキタステクノロジーの側から[引用者注：プライバシー問題について]一段の対応が必要であることは論を俟たないが，同時にプライバシー過保護の状態から脱却して，さらにプライバシーに属さない個人情報は一種の公共財として積極的にその活用を図ることについて国民的な合意形成を行なうことが必要である。】として，船越のいう経済的な価値を持つ個人情報の活用促進を示唆する。

2．4．経済的価値を持つ個人情報の実態

船越は，また，氏名，住所，性別，生年月日，社会保険番号，収入，資産，負債，家族状況，学業成績，思想信条，職歴，健康状態や病歴，前科前歴，社会的身分など，そしてそれらを蓄積して分析し，個人の消費行動や嗜好を割り出した解析データも個人情報と呼ぶ――としている。[18]

2．3．で示したように，船越が，経済的価値に着目して個人情報を分けたのに対し，青柳は，情報の形式に着目して，【狭義のデータ・プライバシー】と【狭義のインフォメーション・プライバシー】とに分けた。前者は，【当該情報がデータすなわち無機質の単語や数値によって構成されていて，それ自体では具体的な意味を持たないけれども，情報主体が公開を欲しないデータが含まれている場合に関わるプライバシー】であり，後者は，【無機質の単語や数値などのデータが，有機的つながりを持っていて，ストーリー性のあるインフォメーションを構成している場合に関わるプライバシー】である】としている。[19]

青柳のいう狭義のデータ・プライバシーは，前出の船越が具体的な項目名をあげた情報に相当し，狭義のインフォメーション・プライバシーは，前出の「個人の消費行動や思考を割り出した解析データ」に近いものと考えられる。

3．個人識別情報の開示性とひも付け

3．1．ひも付けとその拠り所

本章では，まず，サイバー空間上の主体，あるいは，ユビキタスネットワーク社会において，何らかの形で他と識別できる主体が，現実の個人名と直接，結び付かなくても，ハンドル名や ID によって他と区別でき，当該主体の過去の行為などとの一体性が，ハンドル名や ID によって，蓋然性高く推測できるケースを考えてみる。

船越は，吉田正俊の研究として，【約 130 名からなる地方のメーリングリスト】における次のような現象を紹介している。[20]【仮名】(ハンドル名)で参加する新規参加者(後出の常連との面識はない)に，歓迎のメッセージを送るのは，【いわゆるオフ会】で互いに顔見知りの約 5%の常連のみで，その後新規参加者が書き込みをしても，無視されることが多く，多くは脱落していく。

船越は，これを【インターネットの匿名・仮名社会においても，その核を個人認知可能な集団におくこと】の証拠として位置づけている。[21] こうした現象は，実名，実物，ハンドル名などの組み合わせに関し，各人の意識の中で，次のような識別容易性，行為予測可能性のグループ分けがなされている結果であるとは，考えられないだろうか。

すなわち，(1)実名を知る人物とサイバー空間上の識別子との対応(ひも付け)関係が確認されている存在，(2)実名は知らなくても人間の実物を知っている人物とサイバー空間上の識別子との対応(ひも付け)関係が確認されている存在，(3)実在の人物との対応関係が確認されていないが，サイバー空間上の識別子によって，当該サブ空間(電子会議室など)での過去の行為の蓄積が一定の人物像を結んでいる存在，(4)実在の人物との対応関係が確認されておらず，当該サブ空間での過去の行為の蓄積もない存在――である。

小林の示唆する情報の「統合」の怖さを考慮にいれないかぎり，(2)や(3)の状態は何らの問題も引き起こさない。人は，容貌，姿態やハンドル名などにより，他者を区別できなければ，社会生活を営むことができず，日常的に，この区別を行っている。そして，他者から見られる物理空間や他者に読まれるサイバー空間の記述物において，見られたり読まれたりしたら本当に困ることを通常しない。読まれるからこそ，サイバー空間で誰にでも，あるいは，特定の会議室メンバーに読まれるものを記述する。

容貌，姿態やハンドル名は，他者に見られて識別の道具となり，また他者の行為と自己の行為とを区別する拠り所となることを前提とした存在なのである。

3．2．ひも付けの影響

青柳は，【○○町に××という名前の男が居住しているという個人情報，及び某ビデオレンタル店にアダルトビデオばかり頻繁に借りに来る男がいるという情報があるとする。どちらも単独ではプライバシーとはまったく関係がない。しかし，ひとたびこの二つの情報を本人の意思に反して結びつけ(中略)ると，一転してプライバシーに属する情報となる。

このような結び付け行為(前項でいうゴフマンのアンカリング)こそがプライバシー侵害の本質なのだ。住所・氏名などの基本的な個人情報は，プライバシー侵害情報の不可欠な部品ではあるが，原則的にはそれ自体にプライバシー性があるわけではない】と論じている。[22]

青柳は，アダルトビデオを頻繁に借りるという，通常，本人が公言したがらず，店舗から漏れないかぎり公にならない情報を例に，それと実在の顕名の人物とのひも付けを問題にする。

しかし，小林の示唆するとおり，公道における行動であっても蓄積されて，同一人物にひも付けられれば，影響を生じうる。配偶者のある人物が，ラブホテル街に週末ごとに出没する事実が蓄積されれば，一定の推測を生むのは避けられない。公道であるからには，他者に見られる可能性が情報化社会の進展の前からあり，何らかのきっかけでそれが記録されても，その危険性は，情報化社会以前と同様である――という反論がありうる。しかし，大量の情報収集および蓄積と高速の処理が可能になった社会と，それ以前とを単純に類似の論理で捉えるのは，危険である。

3．3．個人識別情報の公共性

船越は，【第一に氏名・住所等の個人識別データが基盤になり，その上に資産情報・信用情報等が積み重なる。個人識別データが不備ではその後の個人情報の蓄積は意味をなさない。】と個人識別データの重要性を論じている。[23]

そして，3．1．で筆者も記したように，個人を基本的に識別するための情報は，社会生活の基本的道具だとする。船越は，【顔見知り小集団の時代から近代市民社会を経て現代の巨大社会に至るまで，人の群れの基盤は個人認知にあり，個々の識別コードを相互に共有し利用して社会が成り立っていること(後略)】は，事実である――としている。[24]

【当人が欲するか否かにかかわらず，基本的に社会的共有を原則とするのが個人識別データである。

そのことと，私的生活空間への無断侵入や私的事項を一般に開示されることを拒否する権利とを混同すべきでない。したがって，氏名・住所・電話番号等は，人が社会生活を営む上で原則秘密の個人情報ではなく，原則的に開示されてはじめて，互いに社会生活を円滑に行うことが可能な基盤情報である。】と，船越は，個人識別データの開示性について述べている。なお，船越は，いまだ知られていない電話番号の意に沿わない公開に関する判決に触れ，電話番号をいわゆる自己情報コントロール権の論議の対象範囲として扱うことがあることを，否定してはいない。[25]

青柳は，基本的な個人識別情報を含む個人情報を公共財として扱えないか――という問いについて，費用と便益とのバランスで捉えるべきだと指摘する。青柳の主張は，4．1．に示すが，それを読むかぎりでは，青柳は，基本的な個人識別情報は社会的な道具であるから公共性のあるものとして扱え――という船越と同じ主張をしているのでは，なさそうである。

3．4．RFIDの問題点

RFID(電子タグ)の問題について，青柳は，児童の安全確保システムや小売の業務効率化システムのように，RFID の効果が高いと認識されている分野において，日本では応用が進んでいるが，米国では，青柳にいわせると【ヒステリック】ともいえる反発によって，進んでいないと説明する。[26]

青柳は，ロバティの次のような言明を，賛同の意思をもって引用している。【ロバティは指摘する。電子タグを自由で民主的な社会に対する"脅威"とするためには，政府はすべての街角の数よりもたくさんの電子タグ・リーダー(読み取り装置を設置しなければならない)。また電子タグが政府以外の者に読まれたり破壊されたりしないようにしなければならない。しかし，技術は誰でも使えるのだから，そんなことは到底不可能だ。】――と言及している。[27]

同じく，【警察は市民を「見張る」ためにビデオカメラを使うことができるが，同時に市民も警察の蛮行を記録するためにビデオカメラを使うことができる。】，【電子タグは，企業に消費者の購入行動を追跡する機会を与えるが，彼らが行なうことはすべて記録に残るので企業は乱用をしにくくなる。】と引用する。[28]

しかし，青柳は，小林のいう「リトル・ブラザー」の持つ情報が，基本的な個人識別情報などをキーにして，名寄せされたときの脅威の可能性を軽視しすぎているように，筆者には思われる。RFIDは，個人や，個人が携える商品を非常に細かく分類，あるいは，完全に個々に同定しうる形で管理するための道具であり，個人の持つ RFID の ID が当該個人の実名とひも付けされる可能性は，決して小さくないのではないだろうか。

筆者は，RFID を活用した児童の安全確保システムや小売の業務効率化システムの効力を高く評価している。評価しているからこそ，それが内包する社会的影響について，真摯に受け止める必要があると考える。

4．ユビキタスネットワーク社会の推進とプライバシー侵害

4．1．費用と便益とのバランス

青柳は，個人情報の活用について，費用と便益とのバランスをみながら，論議すべきだと主張する。

費用については，基本的な個人識別情報が【広範囲に流通してしまって悪用される危険性が増加すること，それに関連する人々の不安(負担感)】である――とする。[29]【ユビキタステクノロジーの側もプライバシーを保護する仕組みを開発し，社会制度の方も種々の対策を講じるはずだから，全般的な費用は徐々に低下するはずである。しかし，それまでの間はかなり大きい費用である】とする。

便益については，【基本的な個人識別情報及びプライバシーに属さない個人情報は各自がどんどん供出することによって，電子タグの活用範囲を拡大し，かつ電子商取引にも役立たせることがユビキタス社会の建設のためには絶対に必要なのだ。しかし，そのユビキタス社会者まだ到来していないから，(中略)[引用者注:便益は]当初は目に見えない程度のレベルから出発する。】とし，【当初の段階では費用が便益を大幅に上回っている】ことを認めている。[30]

しかしながらと，青柳は続ける。個人情報は使わないで他の情報で代替するということができず，便益が十分に大きければ，【ETCやJR東日本のSuica，携帯電話，インターネット上の電子商取引などは，利用することによって持ち主の現在位置やその他諸々の情報が分かってしまうが，人々はまったく抵抗感なく使用】するのである――と主張する。

さらに，【結局，将来の姿ではあっても，いまのうちからその便益を見積もって，現状では費用がそれを上回っていても，基本的な個人識別情報やプライバシーに属さないそれ以外の個人情報は公共財として扱うことを容認して，ユビキタス社会の建設に協力することが求められているのである】と，商社出身者らしい論理を展開する。[31]【個人情報も，利用の推進の過程でさまざまなトラブルが発生して，その都度，対応策が工夫されて実行され，初めて費用が低減するというものである】とまでいう。

4．2．電子商取引との関連

船越は，【完全匿名を許すサイバースペースにおいては責任を伴わない発言が可能であり，人の群れの原点であった個人識別データでさえ仮面の下に隠れてしまう事態が持ち上がっている。(中略)

他方で，電子商取引の進展は，個人データの経済的価値を求めて，情報の収集・管理・加工・利用・販売が国際的に強化されている。人は自分の「行為」と「存在」の痕跡を，無断で自動収集・蓄積・利用されかねない状況にある。

こうして，サイバースペース社会は，これまでの名誉・プライバシー・肖像権・氏名権を内容とする人格権の枠組みだけでは，人格権侵害の受皿として不十分になった。】と指摘し，人の群れ方の新しいルールと，個人情報の経済的利用に関する新しい法理が必要になったと主張している。[32]

青柳は，4．1．でも示したように，船越のような，個人情報の自由な利用を求める動きと，その弊害を減じるための法理の見直しといった功罪のバランス論をとらない。不可侵私的領域に該当する部分については，国家権力が介入してでも，プライバシーを保護させるように強制し，それ以外の部分では，自由にするべきであるとする。

4．3．トレースの問題

4．3．1．「存在」と「行為」の痕跡

船越は，筆者の読むかぎり，分散して保持される情報の統合による危険性については，自明的には指摘していないようであり，この点で小林と異なる。しかし，情報が分散して保持されることの問題点については，言及している。

船越は，自己情報コントロール権の理念と現実について，次のように論じている。【販売店，銀行，カード会社，個人信用保証機関，ガソリン・スタンド，プレイガイド，ホテル，交通機関，レンタルショップ，市役所，保健所，医療機関，介護福祉機関，教育機関と，ありとあらゆるところにその人の「存在」と「行為」の痕跡が記録される。

(中略)わが国の現状は，本人の意思とは無関係に，その人の「存在」と行為の「痕跡」が各事業体に電子記録されている。

(中略)全国レベルの自己情報コントロール・ネットワークが必要となる。】とし，一方で難問が生じるとする。[33]

【第一に，(中略)顧客情報の利用に関して各事業者は自社の独自性を失うことを危惧するであろう。(中略)

第二に，情報主体が，アクセス権，訂正権，取消権等を行使する場合，どの事業者にどんなデータを開示したか，あるいは児童記録されているかを，すべて自己管理する必要が出てくる。すると，それを当然のようにして自己責任論が登場する。(中略)

自己責任を全うするには，[引用者注:自己情報を開示する相手の金融機関が金融機関自身の情報を偽りなく載せていることの保証など]必要な情報の確実な入手が前提となり，その前提を実現する道程を作らずして自己責任原則を唱えるのは大きな無理がある。】

さらに，船越は，【サイバースペース以前】と【サイバースペース時代】とでは，個人に関する各種情報の性質をプロットした図において，「a」が原点だったのが「b」が原点になるような変化が生じた――とする(図表1。文章の後に置いた)。[34]

4．3．2．「名寄せ」の可能性

高度情報化社会以前でも，社会の一部に対して，個人は，少

しずつ情報を開示していた。しかし，現行の個人情報保護法に関する論議でもあったように，個人に関する情報が，名寄せされて，本人の知らないところで，本来統合されて見られるとは思っていなかったことまで集められた詳細な像が形成されてしまうことを社会の人々は危惧した。原点をbに置いた形で図表1をみてみると，センシティブな情報まで開示され，それらが個人識別コードで名寄せされてしまう状況が見てとれる。

さらに，小林の指摘する「統合」の危険性がある。ユビキタスネットワーク社会では，個人が，社会空間の中のさまざまな場所で，ネットワークにアクセスし，必要な情報を受信して入手する。その際に，自分に関する各種の情報を送信する必要がある場合が多い。その過程において情報が盗み見される可能性が，わずかではあるが出てくる。また，個人が立ち寄った場所やそこでのネットワーク上の行為などが記録され，それが，嗜好，性癖，思想信条などを蓋然性高く推測する材料とされる可能性が，わずかではあるが出てくる。

4．4．みだりに行動を記録されない自由

4．4．1．基本的人権としてのみだりに行動を記録されない自由

監視カメラについての論議なので，主に物理空間における行動を念頭に置いているが，小林は，みだりに行動を記録されない自由を主張する。[35] 公の場所を写す監視カメラが取得する情報は，この自由を侵害するものだという。

小林は，【憲法上保証されているほとんどの権利は，みだりに行動を記録されない自由を前提としている。(中略)「政治的表現の自由」(中略)は，取材，資料や筆記具の入手，出版社の打ち合わせその他多くの行動を前提にして，初めて実現するものである。このような行動が公権力や第三者によって記録されるとすれば，それは，表現の自由に対して，重大な萎縮効果を及ぼす懸念がある。したがって，みだりに行動を記録されない利益は，憲法13条により保障される基本的人権であると考えるべきである。また，この利益は，公権力との関係のみならず，私人間においても同様に保護されるべきであるから，私法上の権利としても理解されるべきである。】と主張する。そして，この自由はプライバシー権の一つであるとする。

行為の中には，記録されても差し支えないものもあるが，小林は，【行動の目的は多くの場合外観から判別不可能であるし，監視カメラが特定の行動のみを他の行動から分別して撮影することは技術的に不可能である。したがって，みだりに行動を記録されない自由については，その目的にかかわらず権利性が認められ，具体的事情により保護の程度に格差が発生し得ると考える。】と結論づける。[36]

4．4．2．「存在」と「行為」の統合に対する配慮

この論理は，物理空間におけるRFIDによる移動の記録，そしてサイバー空間における(実名にひも付けされていなくとも)個人を他と区別しうる情報を伴った各種行為の記録にも，広げて適用することが可能であろう。実名にひも付けされていない個人識別情報によるものであれば，その自由の対象にならないという反論がありうる。しかし，それを推し進めると，他人の空似であると抗弁できるのだから，カメラによる記録もプライバシーを侵害しないという論を招きかねない。

消費者として行動するとき，あるいは，鉄道の利用客として行動するとき，4．3．で引用したように，われわれは，同意の上で，あるいは，同意の有無について意識することなく，存在や行為の痕跡を残している。とすれば，記録されない自由を，それぞれの瞬間で放棄しているという反論も成り立つ。

しかし，その理論を進めると，個人情報保護法も要らないことになる。個人情報保護法の対象となる個々の情報は多くの場合，同意の上で，あるいは，同意の有無について意識することなく書き込んだり，(わずかではあるが)一部の同窓会の名簿のように，当然のごとく卒業校に残した情報が転用されたりしたものである。そしてそれは，以前なら当たり前のように行われていた。

そうした情報が名寄せされ，非常に安価に高速処理をされて，各種のPR行為の宛先になったりすることが，「昔から同様のことがなされていた」という説明では片付けられないほどの影響を及ぼしうることになったのである。

ユビキタスネットワーク社会においても，「存在や行為の痕跡」の記録とその統合について，同様の配慮をすべきであると考える。

5．児童生徒の安全を確保するシステムへの保護者の期待

3．4．で紹介した青柳が指摘するように，RFIDを用いて社会に貢献するシステムの試用が，各地で始まっている。筆者が会長代行を務める「大阪安全・安心まちづくり支援ICT活用協議会(略称大安協)」では，児童生徒の安全確保に主眼を置いた情報通信システムの実証実験を，7つほど主導した。[37]

本節ではそのうち，大阪市住吉区の私立帝塚山学院小学校および吹田市の市立古江台中学校の保護者に対して，実施したアンケート結果の一部を示す。いずれも，RFIDを児童生徒に持たせて，校門で登下校をチェックするものである。前者は，パッシブタグ(電池を内蔵しない)を交通用非接触ICカードのように，玄関のリーダーにかざす方式，後者はアクティブタグ(電池を内蔵する)を持って校門を通過すると，電波が数m飛んで，検知する方式である。後者はまた，敷地内にアンテナを40本ほど立て，生徒が敷地内にいれば検知し，十数分以上検知できなければ，警告通知を職員室などに自動で送る仕組みにな

っている。

図表 2 と図表 3 は，帝塚山学院小学校の児童の保護者に，RFID をアクティブタグタイプにし，児童が特に意識しなくても登下校時に校門や通学路の自動販売機のチェックポイントで，通過チェックができるようにすることへの意向を聞いたものである。[38] 図表4は，古江台中学校の保護者に，RFID による安全確保システムの利用継続意向を聞いたものである。[39] いずれも，高率でシステム利用について肯定している。

このように，RFID を用いたシステムへの期待は大きい。児童生徒を対象としているので大人を対象にしたときと同一視できないとはいえ，人の動きを追跡するシステムでさえ，支持を得ている。プライバシーの侵害の可能性があるから使わないようにする－－という論理を市民に納得してもらうのが難しい状況になっている。

「存在や行為の痕跡」の記録とその統合について，社会全体でその対策について真剣に話し合う時期が来ていると思われる。

6．おわりに

ユビキタスネットワーキングの普及に伴い，情報面でのプライバシー侵害が問題になるようになってきた。

本稿では，船越，青柳，小林の理論をレビューした。船越は，動物が自分の周りに，他者が踏み込んだら警戒する，あるいは，反撃するスペースを確保しているというメカニズムを，人間の情報面にも適用して考察し，「サイバースペース社会」においては，人の群れ方の新しいルールと，個人情報の経済的利用に関する新しい法理が必要になった－－と結論づけた。特に，「存在や行為の痕跡」を各主体が制御することが必要だが，実現については難しいので議論が必要であるとした。青柳は，船越の理論に一部同調し，このスペースを不可侵私的領域と名付け，不可侵私的領域に属する情報については法的強制力を行使してでも保護すべきだが，それ以外の部分は自由な流通を許して，電子商取引などを隆盛に導くべきだと主張した。小林は，主に，監視カメラに関する判例を分析，考察し，憲法 13 条により保障される基本的人権として「みだりに行動を記録されない自由」があるとした。

筆者は，個々の場面では，公道の特定の場所を歩いていた－－など，青柳のいう不可侵私的領域に属さない存在や行動の痕跡も，記録して統合すれば，個人のセンシティブな情報について確度高く推定できてしまうと考え，小林の「みだりに行動を記録されない自由」の概念におおむね賛同する。

一方，児童生徒の安全確保システムといった，RFID などを用いて存在や行為を記録するシステムへの期待が高まっていることも示した。ユビキタスネットワーク社会ならではのシステムである，これらの利用を全面否定せずに，船越のいうように「新しい法理」を形成していくしかないと考える。

今後，監視(防犯)カメラや GPS 機能付き携帯電話による存在や行為の記録とその統合の問題を含めて，考察を深めていきたい。

[注，参照文献]

01) 浅野幸治，中野潔『安全安心なまちづくりと情報通信技術』情処研報 2005-EIP-27，pp.9-16，2005

02) 安藤茂樹，中野潔『IC タグ関連の政策に関する一考察』情処研報 2005-EIP-28，pp.11-18，2005

03) 安藤茂樹，中野潔『防犯防災分野への RF-ID の利用とその公的支援』情処通信学会関西支部　発表会　2005 年 7 月 13 日，2005

04) 中野潔『記名式非接触型 IC カードによる非常時の所在地確認に関する一考察』情処 EIP 研究会　社会情報学フェア 2005 論文集，pp.11-14，2005

05) 安藤茂樹，中野潔『RFID の活用による環境保護推進における公的実証実験の役割』情処 EIP 研究会　社会情報学フェア 2005 論文集，pp.15-20，2005

06) 船越一幸『情報とプライバシーの権利』北樹出版，2001

07) 青柳武彦『サイバー管理社会』電気通信振興会，2006

08) 小林正啓『第 7 章　ネットワークロボットの法的問題について－ネットワーク監視カメラ・防犯カメラの設置運用基準－』(中野潔，小林正啓ら著「社会安全システム」採録)，東京電機大学出版局，2007

09) 06)と同じ。p.37

10) 07)と同じ。p.113

11) 06)と同じ。p.123

12) 07)と同じ。p.170

13) 08)と同じ。p.163

14) 08)と同じ。p.163

15) 06)と同じ。p.122

16) 06)と同じ。p.123

17) 07)と同じ。p.56

18) 06)と同じ。p.124

19) 07)と同じ。p.124

20) 06)と同じ。p.100

21) 06)と同じ。p.101

22) 07)と同じ。p.174

23) 06)と同じ。p.122

24) 06)と同じ。p.126

25) 06)と同じ。p.126

26) 07)と同じ。p.254

27) 07)と同じ。p.374

28) 07)と同じ。p.372

29) 07)と同じ。p.219

30) 07)と同じ。p.220

31) 07)と同じ。p.220

32) 06)と同じ。p.153

33) 06)と同じ。p.147

34) 06)と同じ。p.151

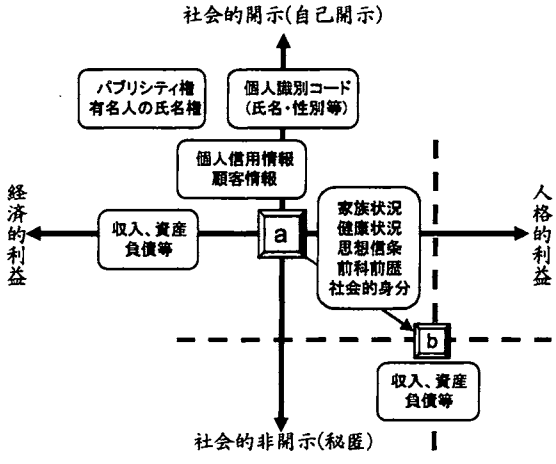
35) 08)と同じ。p.168

36) 08)と同じ。p.168

37) 中野潔『11.1 情報通信技術による防犯実証実験の事例の概要』p.252(中野潔, 小林正啓ら著「社会安全システム」採録), 東京電機大学出版局, 2007

38) 中野潔, 瀬田史彦(大阪市立大学), 伊藤京子(大阪大学)が, 学校, PTAおよび株式会社NAJの協力を得て, 2006年1月に実施した。設問と回答の用紙を学校を通じて保護者に配付し, 学校を通じて回収した。有効回答数は504

39) 中野潔の参加する「ICタグ生徒安全確保実証実験推進グループ」が2006年2月に実施した。配付と回収の方法は38)とほぼ同じ。有効回答数は150



図表1 個人情報の位相概念図(船越による。文献06) p.151)

Q15 現在は、児童がICカードを読み取り機にかざしていますが、校門を通過するだけでICカード等を自動的に読み取る方式もあります。自動的に読み取る方式について、どのように考えますか？

選択肢	件数	比率(%)
利用したい	390	77.4
利用したくない	49	9.7
その他	58	11.5
無回答	7	1.4
合計	504	100.0

図表2 帝塚山学院小学校の保護者のアクティブタグの利用意向

Q16 同じくICカードを読み取る方式で、自動販売機に設置した読み取り機で通過する児童のICタグを読み取ることで、安全管理を行うことについて、どのように考えますか？

選択肢	件数	比率(%)
利用したい	366	72.6
利用したくない	84	16.7
その他	43	8.5
無回答	11	2.2
合計	504	100.0

図表3 帝塚山学院小学校の保護者の通学路における自動販売機にのせた読み取り機の利用意向

Q7 今後も生徒(子供)にICタグを携帯させたい

選択肢	件数	比率(%)
そう思う	90	60.0
思わない	6	4.0
どちらともいえない	45	30.0
未記入	9	6.0
合計	150	100.0

図表4 古江台中学校の保護者のICタグの利用継続意向