

情報化時代のプライバシー概念の再構成

山口県立大学
情報化推進室

吉永 敦征*

Reconstruction of the concept of privacy in the information age

Nobuyuki YOSHINAGA

OFFICE for Information and Technology Yamaguchi Prefectural University

本論文の目的は、情動的プライバシーの概念を捨て、情報の使用をプライバシーとみなすことで、プライバシー概念の再構成を行うことである。本考察ではプライバシーを情報へのアクセスや情報のコントロールとしてではなく、パブリックな評価においてプライバシー情報を使用しないこととして捉える。本プライバシー観を採用することでプライバシー情報の保護が可能であることを示し、プライバシーを保護するためには、情報自体にプライバシーマークを付与すること、パブリックな場面においてプライバシーマーク情報の利用・評価を行わないこと、また評価の基準・プロセスを公開すること、プライバシー情報へのアクセス記録を公開することの4点が重要であることを指摘する。

キーワード：プライバシー 自己決定 情報のコントロール プライバシマーク

The purpose of this paper is to reconstruct the concept of privacy to break with a concept of informational privacy and to regard a use of information as a privacy. In this article, I argue that privacy is not defined as “restricted access theory” or “control theory”, but is not to be used as a means to evaluate or use the information in public. Protection of privacy is possible in four practical ways based on my definition of privacy. First, to label a “privacy mark” on the information. Second, not to evaluate or use the information that has a “privacy mark” label on it when we make public decisions. Third, to open processes and criteria of making decisions in public. Fourth, to reserve and publish information that have records who accessed to information with privacy mark.

key words: privacy self-determination Control of information privacy mark

1 既存プライバシーのモデルの問題点

プライバシーを考察するためのモデルは複数存在する。プライバシーの本質を捉えるために情動的プライバシー、印象操作としてのプライバシー、還元主義的プライバシー、自己決定権としてのプライバシー、などのモデルが存在し、それぞれがプライバシーの一面についての説明を行っているが網羅的な説明がなされているわけではないという意味で、プライバシー概念そのものを統合するのは難しい状況である。しかしながら自己決定権としてのプライバシーを強調するこ

とで、情報化時代に対応できるプライバシー概念の再構成が可能であることを本論文で明らかにする。

たとえば情動的プライバシーには「アクセス制限」や「情報のコントロール¹」といった馴染みのあるプライバシーの捉えかたが存在する。またプライバシーを他の権利に還元する主張として「派生的な権利としてのプライバシー²」などが存在する³。印象操作としてのプライバシーは、たとえばゴフマンが提示したドラマトルギーに代表される考え方である。

それぞれのプライバシー観は馴染み深いものである

*nyoshi@ypu.jp 本論文は電子情報通信学会、技術と社会・倫理研究会にて発表した内容を元に加筆・訂正を行ない議論を洗練したものである。

が、それぞれに問題を抱えていることも事実である。前者の二つに存在する基本的な考え方は、他人に知らせたくない情報をプライバシーとしてみなすこと、また積極的にどの情報を他人へと伝えるかをコントロールすることにその本質がある。本来は主体のコントロール下にあるべき種類の情報を他者が知ることによってプライバシーが侵害されるという考え方である。しかしながら他者が知るだけでプライバシーが侵害される、というのは基準としては行き過ぎであり、侵害されたか否かの判断を行うための条件が必要である。その条件として、情報へのアクセス制限・情報のコントロールを行い他者が私についての情報にアクセスできない状況をつくりだすことが必要となる。知られたくない情報に誰もがアクセスできる状況にしていけないときに、その情報へのアクセスが行われたならばプライバシーが侵害されたと判断できることになる。

つまり、プライバシーはある種の状況における情報へのアクセスを制限することで成立する、という考え方が「アクセス制限」のテーゼである。たとえば窓を開けたまま大声で喧嘩をしている場合と、窓を閉めた状態で喧嘩をしている場合を考えてみたい。前者の場合には窓が開け放たれているという状況であり、音を漏らさないようにしているとは誰も思わないだろう。たまたま通りかかった通行人が喧嘩の内容を聞いたとしても通行人がプライバシーを侵害とは言いづらい。その一方で閉めた窓に耳をくっつけながら喧嘩の内容に聞き入っている人物はプライバシーを侵害しているとみなすことができるだろう。この事例をプライバシーの侵害と見なす背景には、制限された情報へのアクセスが試みられているという判断が存在しているように思われる。つまりアクセスが制限された情報へアクセスされないことがプライバシーであるとみなすことについて、それが自然であると捉えていることに他ならない。この意味でアクセス制限には情報のコントロールという要素が含まれなければならない。窓を開け閉めするという行為のうちに情報をコントロールしているということが含意されているからである。

プライバシーの説明として頻繁に用いられる「放っておいてもらう (the right to be let alone)」こと

は物理的に安全が確保されることから始まり、物理的に他者から隔離され人生を謳歌すること、他者からの干渉を受けないことと変化してきている⁴。プライバシーとは他者の目を気にすること無く自由に行うことを保証する権利であり、現在では情報へのアクセスを行わせないという解釈がなされている。これは日常的なプライバシーとして馴染み深い考え方であり、ここから情報へのアクセス制限や情報のコントロール権としてのプライバシーという考えへと進んでしまうのは仕方がないことかもしれない。

さらにプライバシーは印象操作を行うものであり、社会の中での自己のあり方(他者からの見え方)をかたちづくるために重要な役割を果たしているという指摘もある。自己像をつくりあげるためには周囲への情報の流通をコントロールする必要があるからである⁵。この点からも自己についての情報をコントロールするというアイデアは魅力的に写る⁶。

しかしアクセス制限や情報のコントロールには2つの問題が存在する。1つはまさに現代の課題である「潜在的なプライバシーの侵害」をうまく取り扱うことができないという問題であり、もう1つは情報への制限やコントロールを行うことで他者の思考や評価を差し控えさせてしまう問題である。

たとえば自宅の外にいる人物が盗聴器を所有していたとしよう。私はプライバシーの侵害を恐れ、彼に盗聴器の使用を止めるように要請することにしたいと考えているが、それはどのような理由で可能になるのだろうか。先の例では「窓を閉めておく」ことで私は情報へのアクセスや情報のコントロールを行う意思を持ちそれを表明し、それゆえにそれらの情報へのアクセスがプライバシーの侵害を構成すると主張できるが、盗聴器は窓の存在を気にせず家の内部の音声を拾うだろう。その状況では私がコントロールしたい情報に対して私が示せる意思が盗聴器の使用をコントロールできない限り表明することができない。どのようにして私がコントロールしたい情報があることを、あらかじめ盗聴器を使用している人物が把握することができるのだろうか。それがわからない限りは、盗聴器を使用されどのような情報が知られようとも、わたしが盗聴器をコントロールする対策を行っていない以上はプライバシーの

¹ Westin, 1967

² Volkman, 2003

³ 情報の目的外使用を禁ずることで情報の流通に制限をかけるという方法でプライバシーの保護を行うパターンも存在する。“EU DIRECTIVE 9546EC”がこれにあたる。目的外使用の問題点はわれわれの日常的な行為を遂行することが難しくなる点にあり理論として取り扱うには困難である。われわれが情報の提供者が意図し期待した仕方でのみ情報を取り扱うわけではない。たとえば周囲をなごませようと下品な冗談を口にした友人に対して、「彼は下品な人間だ」と思うこと自体が「なごませる」という目的外使用と考えられる。これはわれわれの日常の直観から大きくかけ離れてしまっており、目的外使用の禁止をプライバシーとして個人が負うべきものとして定義することには無理があると思われる。

⁴ Warren and Brandeis, 1890

⁵ 大谷は「匿名性」という文脈ではあるが情報の流通のコントロールと印象操作のための匿名性(プライバシーの側面)をうまくまとめあげている。大谷卓史2008, pp.179-190.

⁶ センシティブな情報という観点からも情報のコントロール権という考えは素直に導き出せるとも考えられるが、本論では問題が複雑になるためにセンシティブな情報については直接は取り扱わない。しかしセンシティブな情報についても私の提出するモデルの中にきれいに収まるだろう。

侵害とすることができない。だが盗聴器を使用するのは私ではなく他人である。つまり、情報の流通を決定するのが本人ではなく他人のコントロールに依存してしまうような情報の存在を可能にするテクノロジーが一般的になってしまったのである⁷。無線LAN網を利用したLocation Service⁸が開始されている現在、私についての情報のコントロールはもはや私の手には無い⁹。

彼が盗聴器を使用すればプライバシーは侵害されるかもしれないし侵害されないかもしれない、だが使用しなければプライバシーが侵害はされることはない。それゆえに盗聴器の使用を禁止したくなるかもしれないが、機器が使用されない限りはプライバシーは侵害されていないために、プライバシーの侵害を根拠として盗聴器を使用しないことを相手に要求することはできない。プライバシーの侵害を避けるために、侵害されていないプライバシーを主張することは論点先取である。

さらにより重要なこととして情報のコントロールは他者に情報を提供しない（させない）という意味で他者の自由を制限しているといえる。他者に私についての情報を認識させないことで、他者が有する自由や生命や所有の権利と矛盾することがあり、それが根本的な問題として残ることになる。この問題は印象操作としてのプライバシーにも内在している。たとえばあなたの同僚が感染症に罹っていることを「健康な人物像」を維持したいがために隠している状況を想像してもらいたい。事実を知りさえすればわれわれは予防をすることができるが知らなければ感染の危機に直面することになる。また、仕事に失敗しない人物像をつくりあげたいがために、あなたが参加しているプロジェクトに発生させてしまったミスを隠そうとしてプロジェクト全体の業務を増加させてしまっている同僚がいる状況を想像してもらいたい。ミスの初期の段階であれば立て直すことも容易だったかもしれないプロジェクトであったが、隠蔽工作の結果あなたの休日は無くなることになるかもしれない。

プライバシーを他の権利に還元する立場である派生的な権利としてのプライバシーでは盗聴器のケースは解決できると考えられている。派生的な権利としてのプライバシーは、私が有している権利を侵すかたちで取得された情報もしくは他の権利を侵害する手段として私についての情報を使用する場合にのみプラ

イバシが侵害されたとする考え方である。盗聴器の事例も派生的な権利としてのプライバシーを適用することで解決することができるかもしれない。盗聴器を持っているだけでは私のいかなる権利も侵害していない、それゆえプライバシーは侵害されていないが、盗聴器が使われたさいにはプライバシーの侵害として考えることができる。なぜならば、権利はその権利が侵害される可能性をからも保護されなければならないからである¹⁰。これは情報化社会にも対応可能なモデルであると考えたくなるかもしれないが、プライバシーが還元される権利がどのような権利であるのかが問題であろう。Volkman は論文の中で、身体に対する第一の所有を自分に認めている。他人に見せたくないと思っている絵画を所有している者が他人の目に触れさせないことが可能であるように、身体についてもその第一の取扱いについては身体所有者にあるという主張をしている。そして、盗聴器を使用したことが私のプライバシーの侵害であることを述べるために、身体第一の所有権への侵害が行われているからプライバシーが侵害されているという議論を行っているが、盗聴されることでどのような所有権が侵害されていると（私の身体を使用している）考えられるのだろうか¹¹。

2 プライバシ概念と情報の関係についての整理

プライバシー概念についての混乱を解消するために情報について次の3つの区別をつけることとする。「1. 情報を知られること」、「2. 情報を利用されること」、「3. 情報によって評価されること」の3つである。

「1」についての懸念はパノプティコン的監獄と表現されることが多く、監視社会や管理社会というネガティブな印象で語られることが多い。知られること自体を避けようとする態度であるが、知られるという点についてはプライバシーの侵害は発生していないと私は考える。理由は後述する。「2」については私たちの社会的な利益・不利益との関わりが強い。すなわち資産情報や病歴、職業、遺伝情報、位置情報（Locational Privacy）などであり、それら情報を利用されることで不利益を被ることが、また利益を得ることがある種類のことがらである。「3」については人間関係で問題となる。たとえば昆虫採集が趣味であることについて嫌悪感を示されること、男

⁷たとえばRFID が引き起こすプライバシーの問題についてはVance 2006 が詳しい。

⁸Location Service が引き起こす可能性があるプライバシーの問題と解決については、Blumberg, Eckersley, 2009 が詳しい。

⁹当然ながら、無線LANの電波が届かなくするような、また盗聴器を無効にするような、さらに監視カメラにも撮影されても大丈夫なように小型の移動ボックスに入り込んで街中を移動している場合に、そのボックスの中を撮影すること中の音声を盗聴しようとするのはプライバシーの侵害と見なすことができるだろう。だが理解してほしいのは、私たちがまったく知らないような新たな機器が開発され、それら機器によって私たちの生活のすべてが見られ聞かれるという状況が発生したときに、「あなたは何ら対策をしていない。つまりコントロールしようとする意思が無いのだからプライバシーの侵害にはなっていない」という主張をされたときに情動的プライバシーを使用することで有効な議論をつくることのできるかどうかという点である。本文中の表現を用いて考えるならば「窓の存在にそもそも気が付いていない人たち」のプライバシーは情動的プライバシーの概念で成立するとは考えられないのではないだろうか。

性エステへ通っていることが知られ嘲笑の対象となること、または週末に行っている孤児院でのボランティア活動を同僚に知られ、職場で賞讃されることになるなど、情報を知ったものがどのような評価をするのかというその点に関わりがある。

「2」、「3」が他者によって行われなくようにするために「1」についての条件を課そうというのが「アクセス制限」や「情報のコントロール」である。知られることが無ければ利用されることも評価されることも無いからである。つくりあげたい清廉潔白な自己像のために、ポルノサイトを閲覧しているということを知られなくようにするというのはわかりやす過ぎる例であろう。社会的に良き人物たろうとすること、他者からの非難を受けないように慎重に行うこと、そのために自身の欲求を抑えること、それらの情報が正しく伝わるようにすること、これらは本人が望む人物像の追求というポジティブな行いであり、印象操作を行うためには「1」は必須であると考えられるだろう¹²。

しかし、プライバシーが侵害される・保護されるという議論において着目すべきは「2」と「3」についてである。「2」と「3」が行われなく「1」についてを問題視する必要はない。あなたが生活をしている家はあなたの一日の生活のすべてを知っているだろう（知るという認知的状態になり得たとしても）それを問題視するものはいないと同様である¹³。もしあなたの家が「あなたは深夜に酔って帰ってきて家族に迷惑をかけた。だから私はあなたを家にいれない」という具合に入手した情報をもとに家がなんらかのことは行ったとするならば問題だろうが、あなたに何も行われなくときには何か情報を知られたからといって何も問題はない。

次に五分間だけすべての記憶を失い、次の五分間にすべてのことを思い出す記憶障害を持った人物Johnを想定してみよう。また、あなたについての情報が、それも決して人に知られたくないような情報Xが存在するとも想定しよう。Xを知られることで、あなたが長年にわたりつくりあげてきた評価が崩れ去ってしまうことになるような情報である。そしてJohnが偶然にもその情報Xを知ってしまったとする。プライバシーが侵害されるということ、自己像をつくり上げるために他人に情報を知らせないことであると考えた立場でならば、JohnがXを知った時点でプライバシーは侵害されたことになる。

だがここでは奇妙な事態が発生する。あなたのプライバシーは5分間侵害され、次の5分間は侵害されず、次の5分間は侵害されということが繰り返されることになる。プライバシーが侵害されたことによって何かが失われると考えるなら、この例では失われた何かは5分後には回復し、そしてその5分後には再び失われることになる。Johnの記憶が正常なときに失われるものは、あなたが「社会の中でこうありたいと願う人物ならば行わないだろうことを行っている人物」という評価であり、Johnの記憶に問題が発生したときに回復するのはあなたが周囲からこのように思われたいと求める人物像である。だがこれは他人があなたについて行う評価をコントロールしようとしていることであり、あなたについての判断を行わせないことを他人に要求しているということである。「知られる」ことによって失うものは「他人の評価のコントロール」であるが、他人の評価をコントロールすること、すなわち他人が自由に考えることを阻害することは私の権利とはいえない。

「1」を制限することで他者が持つ自由や生命や所有の権利を侵害する可能性がある以上「1」は強すぎる条件でありプライバシーとして認めることはできない。プライバシーを取り扱うために考慮すべきは「2」と「3」の2点であり、このことが示すことは情報そのものではなく情報の利用のされ方・評価のされ方にプライバシーの本質があるという点である。

3 プライバシの定義

本論文ではプライバシーを情報のコントロールという観点ではなく行為の側面から取り扱い自己決定の観点から取り扱うことにする¹⁴。それは上記の「2」、「3」が人間の行為に関するものだからである。われわれの社会は他者から干渉されない領域と他者と共存する領域とに分けられる。個人が自由に振る舞うことができる領域と、他者と相互に制限を受けつつ共存する領域である。前者がプライベートな領域であり後者がパブリックな領域である。プライベートな領域内で行われる行為を保証することがプライバシーであり、たとえば良心・思想の自由、どの大学へ進学するか、どの企業へ就職するか、子どもを何人もうけるかなどは他人から干渉される必要が無い選択であり、選択は個人々に委ねられている。つまり、自己決定することが社会的に認められていることとプライバシーを同じものとみなすことができるのであ

¹⁰ Volkman 2003, p.206

¹¹ 派生的な権利という考え方はクリアな視点を与えてくれるが、所有の本質である「排他的な使用権」という考え方と「情報」との折り合いの悪さのために議論は失敗しているように思われる。

¹² 杞憂に過ぎないかもしれないが、望むべき人物像からの逸脱の手段としての匿名性や情報のアクセス制限・情報のコントロールは、望ましくないかもしれないがそれを指すのが悪いというわけでは無いという選択肢を狭めていくのではないだろうか。

¹³ 「1」、「2」、「3」が明確に区別できないという疑問を持つことは理解できるが、利用されることのない情報・評価されることのない情報というものを想定することは可能であろう。その情報が端的に存在し、ただ知られているだけで、今後一切の利用や評価がなされないような場合にはいかなる問題も無く区別することは可能である。もしここに問題があると主張するならば、人が何かを知ること自体が問題の源泉であるという主張を行う必要があるだろう。

る。この観点からプライバシーを考察することで情報というものを直接に取り扱わずにプライバシーを取り扱うことができるようになる。それは「アクセス制限」や「情報のコントロール」に内在する問題点である「他者の有している種々の権利の侵害」を行うこと無くプライバシーを取り扱うことができることを意味する。

プライベートな情報を他者が手に入れ、それをもとに前節「2」、「3」を行うことは情報を手に入れた人物の自由である。あなたがある政治団体の集會に参加したことが、対立関係にある政治団体を支援している会社の上司に知られた結果、上司があなたを敵視することは上司の自由である。そこに何ら問題は無い。あなたが上司を蔑むようになることもまた自由である。プライベートな情報について、それをもとにどのような判断を行うこともあなたの自由である。友人が信じている宗教が明らかになった結果、あなたが友人関係を止めることも、次第に疎遠になっていくことも、嫌悪感を抱きつつも従来と同様の関係を維持していくのもすべてあなたの自由である。それはすべての人間に同様に付与されるべき自由でありまさにプライバシーそのものである。自由に考えること、自由に判断すること、自由に信じること、自由に行為すること、これらがまさに自己決定の範疇内のことがらであり、プライバシーそのものである。私のプライバシーを求めるのであれば、他人にも同様のプライバシーが必要である。盗聴器を持って家の前に立っている人物はプライバシーの侵害は行っていない。内容をプライベートに利用する分には、内容についていかなる評価を下すことも彼の自由である。

留意すべきはプライベートな情報にもとづいてパブリックな決定を行わないようにすることである。上司が支援している政治団体と対立関係にある政治団体の集會に参加したために地方へと左遷させられるという事態は問題であり、プライバシーとして保証されている行為を理由として制裁が行われしまっている。このことこそがプライバシーの侵害を構成する

のである。なぜならば政治団体の集會に参加することは私の自由であり、それを阻害することは私の自由を阻害していることになる。上司から出される「参加しても構わないが地方に行ってもらおう」という条件は、私に自由に行為することを禁止している。つまり、プライベートな情報をパブリックに利用しないこと、パブリックに評価しないこと、これこそが情報のプライバシーを守るということに他ならない。「参加した」という情報が私の自由を阻害する要件となつてはならないのである。盗聴器を使用して手に入れた情報を元に暴露本を執筆し許可無く公表したならばそれは情報を利用したという意味でプライバシーの侵害であるといえる¹⁵。

4 情報化時代におけるプライバシー

プライバシーが保護されるという観点で重要なことは、プライベートな情報について個々の人物がプライバシーを有する人物に評価されないことではなく、評価されることを保証すること、その一方でパブリックな判断・評価に対してプライベートな情報を利用しないということである。そのために必要なことは、

1. プライバシだとみなされる情報にプライバシーマークを導入する。プライバシーマークは情報の対象者が付与しても良いし、基準を策定してもよい。ただし第一の権利は情報の対象者にあるものとする。
2. パブリックな判断・評価の方法を公開すること。プライバシーマークが付与されている情報を、パブリックな判断・評価の材料としないことを徹底する。
3. プライバシ情報がパブリックな場面で使用されていないことを明らかにするために判断・評価の基準・方法、実際のプロセスを外部に広く公開する。
4. プライバシ情報を取り扱うものは、プライバシー情報へのアクセス記録を公開する。

プライバシーマークはオプトイン・オプトアウトの

¹⁴ 吉永敦征, 土屋俊, 2000, pp.17-22.

¹⁵ パブリックということが指し示す内容が曖昧であり実質を欠いているということは筆者も理解している。パブリックとプライバシーの間の境界線は常に変化し、社会的規約によって定まるものであり明確に定義することはできない。そのため事例によっては判断が難しいケースがあるだろう。たとえば中間団体がパブリックであるのかどうかという疑問はもっともであるが、それも社会的規約によって定めるしかなないと答えざるをえない。たとえば住所はプライバシー情報なのかどうかという点についてさらに具体的に考えてみたい。どこに居を構えるかはわれわれの自由であり自己決定することができる内容である以上プライバシー情報であると考えることができるだろう。このとき、支給交通費をできるだけ節約したい企業が、他の点ではまったく同じ条件の応募者2名のうちできるだけ勤務地に近いほうを採用しようと判断することはプライバシーの侵害になってしまい、それは現在のわれわれの活動と齟齬をきたすだろうという指摘が考えられる。実際に経費を削減するために「より近い方を採用する」という判断は納得がいくものだろう。この意味では住所はプライバシー情報ではないということになる。その一方で出身地差別を避けるためには住所を利用するかたちで何かを決定することは行ってはならない。このときは住所は利用すべきでない情報でありプライベートな情報と見なすことができる。つまり1つの情報であっても、場合によってはプライバシー情報であり、かつまたプライバシー情報では無いということになる。それゆえに情報をプライベート、パブリックに分けることに実質が伴わないためこの議論は無効であるという批判が成立する。この批判に対しては次のように反論することができる。住所はプライベートな情報であり、それをパブリックに利用することはプライバシーの侵害である。なぜならば、どこに住むかはまさに個人の問題であり、たとえば交通費が支給されなくとも勤務することは可能であり、交通費が負担になるようであれば転居すればよいだけのことである。転居するのは本人の自由であり、いつでも行うことができるのだ。

¹⁶ 社会の変化に伴い過去には許容されていた行為が現在が許容されないということは想定可能である。そのためプライバシーマークの取り下げについても検討する必要があることは事実である。

どちらの方式で付与してもかまわないし、基準にもとづき他者によって付与されてもかまわない。この基準はシンプルな形で求めることが可能である。私たちが行為 x を自己決定できる行為として行うことが認められているさいに、人物 A が x を行うことについての情報一般がプライバシー情報であると考えられる。つまり x の内容（私たちが行うことが許されている行為）がプライバシーマークの対象であり、 x を決めることがすなわちプライバシーマークを決めることになる。どの行為がいつの段階でどこまで可能なかは社会的規約によって定められるものであり、この基準は常に揺れ動いている。しかし上記の方法でプライバシーマークを付与することは可能である¹⁶。

なにかしらのパブリックな決定が行われたとき、たとえば政治団体の集会への参加の後に左遷が決まった場合には、そのプロセスや判断の公表を求めることでプライバシーの侵害かどうかを判明できる。左遷の判断材料にプライバシーマークが付与されている情報が無いことを明らかにすることでプライバシーの侵害は行われていないことを示すことが可能であり、プライバシーマーク付きの情報が判断材料として利用されていたことが判明した場合にはその決定はプライバシーの侵害であり、正しくない判断と結論づけることができる。すなわちプライバシーを保護するという点で求められることはパブリックな決定がなされた場合の、その基準・方法・プロセスを決定された内容と同時に公開することである。

プライバシー情報を取り扱うものはすべてプライバシー情報へのアクセス情報も公開することでプライバシーの侵害か否かを判断させることが可能になるため、プライバシー情報へのアクセス記録を公開することはプライバシー情報を取り扱うものの義務となるだろう。プライバシー情報へのアクセス記録は、何らかのパブリックな決定が行われたさいに、その決定にプライバシー情報が利用されていないことを示す重要な情報となる。逆説的ではあるが、プライバシー情報にアクセスしたというプライバシー情報を公開することでプライバシーが確保されるのである。

5 結論

本論文では、情動的プライバシーの概念を捨て、情報の使用にプライバシーを適用することで、プライバシー概念の再構成を行った。本考察ではプライバシーを情報へのアクセスや情報のコントロールとしてではなく、パブリックな評価においてプライバシー情報を使用しないこととして捉える。本プライバシー観を採用することでプライバシー情報の保護が可能であることを示し、プライバシーを保護するためには、情報自体にプライバシーマークを付与すること、パブリック

な場面においてプライバシーマーク情報の利用・評価を行わないこと、また評価の基準・プロセスを公開すること、プライバシー情報へのアクセス記録を公開することの4点が重要であることを指摘した。

参考文献

- [1] Alan Westin *Privacy and Freedom* New York: Atheneum, 1967
- [2] Andrew J. Blumberg, Peter Eckersley *On Locational Privacy, and How to Avoid Losing it Forever* ELECTRONIC FRONTIER FOUNDATION, 2009
- [3] Richard Volkman *Privacy as life, liberty, property* Ethics and Information Technology, 2003, PP.199-210.
- [4] Vance Lockton, Richard S. Rosenberg *RFID: The next serious threat to privacy* Ethics and Information Technology, 2005, PP.221-231.
- [5] Warren and Brandeis *The Right to Privacy* *Harvard Law Review* Vol.IV December 15, No.5, 1890
- [6] Deborah G. Jonson, 水谷雅彦・江口聡監訳『コンピュータ倫理学』オーム社, 2002
- [7] 大谷卓史『アウト・オブ・コントロール』岩波書店, 2008
- [8] 水谷雅彦編『応用倫理学講義3情報』岩波書店, 2005
- [9] 吉永敦征, 土屋俊「大学におけるプライバシー保護の現状」『電子情報通信学会技術研究報告 信学技報Vol.100 No. 383』, 2000 pp.17-22.