プライバシー、秘密、セキュリティ

ポール・B・トンプソン

出典:

Paul B. Thompson, 'Privacy, secrecy and security', *Ethics and Information Technology* vol. 3, no. 1, 2001, p.13-19.

キーワード:

データ・セキュリティ(data-security)、論理的セキュリティ(logical security)、個人のセキュリティ(personal security)、プライバシー(privacy)、リスク(risk)

要約

本論文の著者トンプソンは、パーデュー大学哲学科の教授であり、応用倫理学と技術の哲学の専門家である。

コンピュータ倫理学において、しばしば議論となるのがプライバシーに関する諸問題である。だが、そもそもプライバシーという概念それ自体が曖昧である。そこで、トンプソンは、この曖昧な概念を用いずに問題を分析するのが最良であると言う。すなわち、身体と所有物を守る権利(rights to secure person and property)という、最も基礎的で異論が少なく、最も普遍的に認められている権利としての分析である。この分析によるリスクに基いたアプローチ(risk-based approach)は、プライバシーを論じる時に、われわれが何を倫理的に重要だと考えているのか、を明らかにする。トンプソンによれば、こうしてセキュリティの問題が明確になったなら、プライバシーに関する本当の問題も明らかになるであろう。

以下では、トンプソンの論文を要約する形で紹介していく。本稿の構成と各節のタイトルは、原文に従った。

序

法や倫理学において用いられる「プライバシー」という言葉は、独自の概念や善として特定されてはおらず、習慣や便宜によって関連付けられた問題の集合として示されている。現在でも大きな影響力をもつウォーレンとブランダイスの論文(1890 年)は、「プライバシーは実在する善(a positive good)であり、個人および非政府組織はプライバシーという政治的権利の維持に対する利害関心を持つ」という見解の発端となった。これによれば、プライバシー権とは「放っておかれる権利(a right to be let alone)」である。プライバシー権は政府に対してのみ成立する権利ではない。ある人の孤独を一般の人々が邪魔することもまた、プライバシー権によって禁じられる。この見解以後の数十年、プライバシーという概念は拡張して解釈される傾向がある。

トンプソンは、この拡張解釈の傾向に異を唱える。彼は、ウォーレンとブランダイス流の概念では、情報技術がプライバシーを脅かしうる理由を明らかにできないと言う。トンプソンの着眼点は、これらの倫理的問題を、プライバシーではなく秘密とリスクの問題として捉えることである。

プライバシーとセキュリティ

そもそも、なぜプライバシーは重要なのか。そして、プライバシーと近年の情報技術は、どのように関係しているのか。トンプソンは、近年のプライバシー解釈を整理する。

・プライバシーは、妨害を受けない権利というロック流概念と、自律というカント流概念の直接的な延長である。コンピュータを用いたプライバシー侵害として知られているのは、1989 年に女優レベッカ・シェイファーが電子データベースから住所を知られたために殺された事例である。

・電子的な監視の事例。監視を知っている労働者が感じる精神的ストレスや、経済データ分析を用いた従業員雇用、資金に関する決定が論点となる。この場合、プライバシーは内在的価値ではなく道具的価値をもつと見なされる。また、電子商取引のセキュリティ、これに関する技術的・法的アプローチなど広範な問題を、すべてプライバシーという範疇に含める人々もいる。

・社会学的観点からのアプローチ。いくつかの社会理論は、国民に対する監視能力の増大を国家権力の拡大と捉える。そして、情報技術とそれによる新たな監視形態の出現は、市民の利益より政府や営利組織を優先する社会的権力関係の産物として解釈される。

このようなアプローチは、いずれも道徳的諸権利や市民的自由などの広範な集合を包括するのがプライバシーであると想定する、包括的(expansive)解釈をとる。

しかし、カルヴィン・ゴットリーブは包括的見解を批判する。彼は用語を以下のように再定義する。

まず、プライバシーは、社会的・文化的・法的概念であり、この三つの側面は、国ごとに非常に異なっている。守秘(confidentiality)は、管理上の責任である。すなわち、データバンクの管理者とデータを管理される個人の双方が同意する規則によるデータ管理の方法に関わる。セキュリティは技術的問題である。これは、管理者によって定められたデータアクセスの規則が、パスワードの使用、暗号などの技術を用いて、どのように実施されうるかということに関わる。

ゴットリーブによれば、守秘はコンピュータの専門家にとって重要な倫理的問題でありつづけ、セキュリティはより重要な技術的問題となりつつある、だがプライバシーは必要ではない。文明化された自由なすべての社会で保証されるべきは個人のセキュリティである、とゴットリーブは述べる。そして、個人データのセキュリティは、個人のセキュリティという目的の手段であるかもしれないが、データのセキュリティとプライバシーとは本来まったく異なった事柄である。

トンプソンはこの定義を用い、プライバシーという概念の代わりに守秘とセキュリティという概念を用いて議論を進める。ゴットリーブはデータのセキュリティと個人のセキュリティとを結び付ける。データが危険に晒されることは個人の危害につながりうるのだから、データのセキュリティは個人のセキュリティに対する利害関心と直接に結びつくのである。

情報と個人の危害との関係は、以前にも議論されている。ジェイムズ・レイチェルズは、個人に関す

る情報が原因で、ある人が何らかの仕方で他人から誤った扱いを受ける事例をいくつか挙げている[「なぜプライバシーは重要なのか」、松永喜代文訳『情報倫理学研究資料集 I』、87-95 頁、1999 年]。

ただし、レイチェルズの主張は、このような例がプライバシーの重要性を示すと考えるのは誤解を招くということである。むしろ彼の主要な見解は、われわれには、さまざまな人々と異なる種類の関係を維持する必要があるということ、そして、プライバシーという概念は、これらの人間関係の違いに注目することによって、より明確に理解されるということである。レイチェルズはプライバシーそれ自体の価値を否定しない。しかしながら、ゴットリーブと同じく、レイチェルズは個人情報の乱用とプライバシーの問題とを切り離す。

情報の乱用に関して、このアプローチを取るのはレイチェルズだけではない。シセラ・ボクは、個人情報の乱用や、デリケートな情報の公開によって生じうる困惑や脅迫の可能性を議論している。ボクによれば、事業者や政府組織は、幾つかの活動を公衆や報道機関の詮索から守る必要があり、この必要は公衆の知る権利よりも重視される。ここでボクが論点としたのは、プライバシーではなく秘密(secret)である。

トンプソンは、このボクの路線を支持する。ここまで挙げた事例に含まれる倫理的問題は、「情報は公開すべきだという一般的前提に反して、秘密にすることが擁護されうるかどうか」と問うならば、より明らかになる。ボクによれば、身体の保護と所有物の防護という基礎的な権利が危険に晒されることが示された場合、秘密にすることは擁護可能である。

これらの見解をもとに、トンプソンは包括的アプローチを否定すべき理由を述べる。 いくつかの文脈で、「プライベート」という語は「秘密」「守秘」という言葉とほぼ同義語である。例えば、われわれが「彼女は、困惑を避けるため、自分の人生のある部分をプライベートなものにしておきたい」とか「医療記録はプライベートにしておくべきだ」と言う時、言明の意味を変えることなしに「守秘」という語を「プライベート」という語に置き換えることができる。特に重要なのは、秘密によって生じる利益が、秘密の公開によって侵害される場合があることである。例えば医療情報は、雇用などの機会に、ある人に不利益を与えるために用いられうる。また、デリケートな情報の公開で人々が感じる困惑も、特定の状況では心理的危害の一形態である。われわれは、心理的苦痛や機会の剥奪が悪だと明言するために、ウォーレンとブランダイス流のプライバシー権に訴える必要はないし、レイチェルズ流の関係の違いという概念に訴える必要もない。ゴットリーブが示唆するように、これらは自由で文明化された社会で守られるであろう利益である。

冒頭で、プライバシーは単に道具的価値をもつにすぎないという見解を紹介したが、、ウォーレンとブランダイスのプライバシー概念は、それ以上の価値を想定している。また、レイチェルズは、プライバシーをロールズ流の基本財--ある人がよき生についてもつ基本的構想に本質的な財--とみなす。プライバシー権は、物理的場所と心理的な個人的関係の双方を含む活動の一領域を、他者の介入から守るためにある。
だが、これ以上のものを要求すると、プライバシーは非常に曖昧で状況依存的なものとなってしまう。

例えば、ふたりの人たちが一つの住居に同居しているとしよう。彼らは、隣人の部屋から聞こえる物

音が、自分達のプライバシーを侵害していると主張するかもしれない。だが、同居相手がたてる物音に対してもう一方がプライバシー侵害だとは言えない。なぜなら、彼らは、あらかじめ共有することに同意した空間を互いに使っているからである。しかし、このようなプライバシーの議論と、秘密や情報についての議論とは全く関係ない。

その一方、秘密と情報には緊密なつながりがあるように見える。ある事柄が秘密であるなら、情報を知らない人間が少なくとも一人いることになる。だが、ある人にプライベートな事柄があると知られているとしても、必ずしもそれがプライバシー侵害にはなるわけではない。例えば、ある人の宗教的実践が多くの人々に知られているとしよう。しかし、そのことで彼の実践がプライベートなものでなくなるわけではない。その情報を知った誰かが彼を差別したなら、この人のプライバシーは侵害されるかもしれない。だが、この種の情報は、ほとんどの社会で容易に入手できるものである。従って、私的な情報の重要性は、単にそれを知ることにあるのではなく、入手した情報をどのように用いるかということにあると言える。

秘密、セキュリティとリスク

人々が秘密を保ちたいと思う理由は数多くある。ここでトンプソンは、コンピュータ技術と個人のセキュリティに関係する三つの理由を挙げる。

(1) 危害を企てている行為者が、それに必要な情報を直ちに得られないならば、この危害の実行を遅らせたり阻止したりすることができる。だが、コンピュータを使ったなら、多くの情報が直ちに得られ、容易かつ迅速にその行為を実行できてしまう。

(2) 情報それ自体が、個人のセキュリティ権によって守られるべき私的所有物であるという場合がある。情報技術は、このような情報の性質やその範囲に大きく影響する。

(3) 商業や公的な保護システムの多くは、今やコンピュータや電子データベースに依存しつつある。従って、これらのシステムの故障や偶発的事故は、公的または個人的な安全を脅かす。

これらの理由は、いくつかの点で非常に異なる倫理的考察を含んでいるが、二つの共通点がある。第一に、これらの事例はすべて、秘密とセキュリティという観点から明確にされうる。第二には、倫理的諸問題に共通する点を特徴づけるのに、リスク分析を用いることができる。

悪意(Malicious intent)

既出の事例に含まれている秘密とセキュリティの問題を見ていこう。まず問題となるのは、コンピュータを用いる人間がもつ悪意である。レベッカ・シェイファーの事例は、人々がアカウントやパスワードと同じように、自分の住所や電話番号を秘密にしたいと望む理由を示している。コンピュータや電子データベースの増大によって、狡猾な人間がほとんど露見することなく情報を手にする機会が作り出された。そこで問題になるのは秘密である。

知的所有権

コンピュータとデジタル情報システムは複製を可能とし、テキストや画像、録音された音声などを交

換するのに用いられる。これによって知的所有権が脅かされる。所有者の許可なしに個人の所有物を奪うのは、通常、所有者の個人的セキュリティの侵害であると考えられる。

それに対して、自分の知的所有権を電子的な手段によって盗まれた人は、剽窃された、あるいはパテントを盗まれたのだと見なされてきた。ある意味で、知的所有権に関する問題は、単に悪意の下位分類に位置する問題である。だが、知的所有権の保護の場合、秘密の役割は大きく異なる。秘密というものは、所有物と考えられている営業秘密や多くの情報の本質である。他方、版権やパテントは秘密にすることによってではなく、法律によって知的所有権を保護する。ともあれ、版権、営業秘密、パテントなどを盗むことは、明らかに秘密の侵害だと考えられているが、これは通常プライバシーの侵害だとは考えられていない。

システムセキュリティ

西暦 2000 年問題や「I LOVE YOU」ウィルスによって、人々は、社会秩序や個人保護の大部分が情報システムに依存していると気づきつつある。以前のセキュリティは、保護の対象となるものをある場所に孤立させ、その部屋を施錠すること、すなわち物理的セキュリティであった。だが、対象物が情報という形でコンピュータにあり、そのコンピュータがいくつものシステムによってリンクするようになった現在、システムセキュリティは、物理的セキュリティから秘密や論理的セキュリティに大きく依存するようになった。これまでは、この種の秘密をプライバシー権と捉えようとはされていなかった。論理的セキュリティで守る必要がある秘密は、人々の私的生活に明白に関わってはいない。しかし、システムセキュリティの問題に必要な処置は、悪意による個人情報の入手や知的所有権の盗用の場合と同じ仕方でなされる。

つまり、上で挙げたすべての事例において、セキュリティは、重要な情報から誰かを排除することに依存しているのである。そこで、これらの事例での道徳的正当化もまた同じ仕方でなされる。多くの事例で、「権限を持たない人々が情報を探している」という単なる事実が、情報の危険な使用が企てられているということの証拠になる。そして、セキュリティの目的に関して、少なくとも以下の三つの問いがある。

1. **排除されている人々が情報を入手しうる可能性には、どのようなものがあるか。**

この答えは、偶然的な情報開示の可能性、そして排除されている人々の情報探索が成功する可能性とにあるだろう。この二つには違いがある。秘密だとは誰も考えないことが明白な情報の場合、偶然の情報開示や情報探索成功の可能性が高いとしても、全体的なリスクは明らかに低い。偶然的な情報開示の可能性のほうが情報探索が成功する可能性よりも有意に低い場合、秘密領域への意図的侵入の可能性が、個人や所有物に対する危害の見込みを分析する重要な要素になる。

2. **もしも情報が排除されている人々に渡ったならば関係者が受けるだろう危害とは、どのようなものか**

排除されている人々の意図や情報の入手方法に関する事実が、リスクの査定には重要である。悪意ある情報探索によって危害が生じる見込みは、明らかに高い。また、偶然の発見や有益な情報探索から危害が生じる可能性は、ゼロではないが殆どないと考えられるだろう。そして、無目的な情報検索によって生

じる危害は、この二つの間に位置する。

レベッカ・シェイファー殺人犯は、あらかじめ危害を加える目的をもってデータベースを用いた。では、特定の目的なしにスターの住所を探した人が後に危害を加える目的をもつという見込みはどうか。体系的な査定によって、危害に関する最初のリスク概算が修正される。目的のない情報探索が見かけほど無目的ではないと考えられるなら、追加的な考察によってリスクは当初より高く査定されうる。

この他にも考慮されるべき点がある。関係者が利益を受ける可能性と危害とが埋め合わされるかもしれない。例えば、あなたの住所を知った人が、あなたがなくした財布を返すために、この情報を使うことがありうる。パーティーの主催者や中古車を買おうとする人が、善意で住所のデータベースを探すかもしれない。このような機会は概ね歓迎されるだろう。このような利益の倫理的重要性は、セキュリティの議論で考慮されるべきである。ただし、利益と危害が埋め合わされると常に仮定すべきではない。

3. 関係者が受けるかもしれない危害はどのように深刻か

セキュリティ権は、個人の身体や所有物に対する暴力によって侵害される。殺人や窃盗は、どちらもセキュリティ権の侵害であるが、死の方がはるかに深刻である。このような順位付けによって、軽減されたリスクと資源消費の関係が考察される。一般的に、身体と所有物に対するセキュリティ権は、受ける危害がかなり深刻な場合に生じると考えられる。つまり、いくつかの危害形態--鉛筆泥棒、軽い傷害など--は、セキュリティリスクのレベルではない。ただし、基本的なセキュリティ権によって保護される心理的危害や不快という形態が存在するかどうかという点は、議論されるべきだろう。

トンプソンによれば、上で分類した三種の問題は、リスクに基いたアプローチを取るときに、それぞれ三種の問題領域--悪意、知的所有権、システムセキュリティー--に当てはめることができる。リスクに基いたアプローチの主な利点は、概念の明確さである。人々を悪意から守る事に関する技術的・道徳的問題の多くはまた、知的所有やシステムセキュリティの保護の問題とも関係している。三種類の事例において、秘密を守ることの価値は、ウォーレンとブランダイス流のプライバシー権から引き出されるのではなく、成員を危害から守るという社会の義務から引き出される。これらの事例は、プライバシーの侵害からではなく、秘密の侵害が関係者にもたらすリスクという点から分析する方が、より多くの実りある分析が得られるだろう。

リスクに基いたアプローチの問題点

しかしながら、リスクに基くアプローチにつきまとう解釈的、倫理的な問題がある。 リスク分析は、認識論的、倫理的、政治的、心理学的本質を持つ厄介な問題を隠蔽する魅力がある。長年、リスク分析の専門家たちは「望ましくない出来事の可能性と価値の測定は、すべて技術的分析によってなされ、倫理的、政治的問いは技術的に測定されたリスクを受け入れるかどうかという点に限定されねばならない」という考えを奨励した。実際、技術的議論に倫理や価値に関する議論を差し挟むのは難しい。リスクに基いたアプローチは、単にこの衝突をコンピュータ倫理学に持ち込んだだけだという懸念も生じるだろう。

リスク分析学会の元会長スロヴィクは、「リスク分析の専門家たちの間で生じている論争のほとんどは、…ある程度まで、リスクという概念の複雑で社会的に決定された本質を理解し損ねていることに由来する」と言う。スロヴィクによれば、危害や損害、損失という点からしかリスクを考えない人々は、可能な未来としてリスク概念を理解する場合に、人々の自発性、同意や意図が果たす役割を無視している。では、情報技術に関する問題で、この古典的問題がどのように論じられるのか、とトンプソンは続ける。

例えば、技術的リスクに対する哲学的なアプローチのひとつは、リスクと利益を期待値として解釈する功利主義である。しかし、このアプローチで生じる問題は、効用を最大にする決定規則が、将来の不確実な予測に応じて変動する点である。ここで考慮すべきは、人々の同意を、リスクに対する倫理的に適切な応答として考える見解である。新しい技術に対するリスクに基いたアプローチが、同意の役割を無視すると考える人々が挙げる事例がある。

食糧、農業などのバイオテクノロジーに関しては、功利主義的な思考スタイルが広まってきた。政府の規制機関によって行われたリスク分析では、消費者の健康や安全に与える危害の重大な可能性は明確にならなかった。政府規制官は、消費者は、遺伝子加工食品にラベルを貼ることで、わずかな客観的利益を得るだけだと論じた。消費者達が、これらの食品のリスクを受け入れるか拒絶するかを自分自身で決定したいと望んでいるという証拠は無視され、消費者の遺伝子加工食品を拒絶する権利はないがしろにされた。

このバイオテクノロジーの事例で問題となるのは、規制官が個人の同意に関係する倫理的問題への感受性を欠いている事である。このような事例では、公衆のリスクに対する考えと技術的に訓練されたエリートのリスクに対する考えとの間に緊張関係がある。情報技術の問題が個人的・集団的なセキュリティの弱さとして考えられ始めた時、同じ問題が生じる。

データセキュリティの場合は、倫理的問題をリスク-ベネフィットのトレードオフと、インフォームド・コンセントとの緊張関係として分析するのが最良だろう。このような場合、プライバシーからリスクに基いた分析への移行が倫理的問題を解決するわけではない。しかし、リスクに基いた分析は、何が問題なのかをより明確にすることができるだろう。要するに、リスクに基いた分析に問題があるということが、このアプローチを斥ける理由にはならない。むしろ、その長所と短所を明確にすることが、この分析の基盤となる。

プライバシーに関するいくつかの考察

セキュリティのリスクが、より明確に理解されるなら、プライバシー権についてもまた、問題となる事例がはっきりと特定される。例えば、市場調査のために電子データベースをスキャンするという事例にリスク分析を用いたとしても、この行為を個人のセキュリティの侵害と見なすのは難しい。もちろん食料品店のチェーンがレジのデータをセキュリティを脅かすような仕方で使うことは常に可能である。だがこの行為は危険視されるほどではない。この直観を維持したままで、プライバシー権を倫理的に重要な仕方で情報技術の使用に耐えるよう形成することができるだろう。

ここでトンプソンは、先に指摘した点との関連に触れる。プライバシーを尊重するには、たとえ保護

された情報領域の存在が知られているとしても、その領域を侵害してはならない。例えば、ある人の宗教的行為や性的行為は、仮に隣人や知人がそれについて多少知っていると予測される場合でさえも、依然として「プライベート」なものである。コンピュータ・ネットワークを通じて、ある人の保護された領域の情報を知ったとしても、それでこの保護された領域がプライベートでなくなるわけではない。情報を得た人は、それを偶然知っただけなのか、あるいはデータ・マイニングによって知ったのかには関係なく、その情報を無視せねばならない。つまり、情報が知られるかどうかよりも、情報を知った人がそれをどう扱うか(悪用するか、無視するか)という点が重要である。

トンプソンによれば、プライバシーは基本的自由であり道具的善であるのと同時に、基本的な善(基本財)でもある。もしもプライバシーを基本財だと考えるなら、それは個人の尊厳(dignity)と同じようなものである。資本主義社会において、通常、裕福な人は自分の尊厳を守る力をもつが、貧しい人はもたない。
これと関連して、トンプソンは二点を指摘する。

(1)　たとえ貧しい人々が持つわずかな所有物のセキュリティや安全が保証されているとしても、まだなお満たされていない正義の責務がある。情報に対するアクセスに格差があるということは、富める人々はより多くの情報を発見し、貧しい人々はよりわずかな情報しか発見できないという状況を作り出す。コンピュータは、この格差に影響するだろう。

(2)　さらに、貧しい人々のセキュリティを脅かす乱用によって情報へのアクセス格差が生じる場合と、侵害されているのが貧しい人々の尊厳(プライバシー)である場合とを区別するのは重要である。たとえリバタリアンであっても、裕福な人々には貧しい人々に危害を加える権利はないことを認めるだろう。

この考察によって、プライバシー権が懸念される事態を包括的にではなく分離して考えるための、最後の議論が生じる。貧しい人々の利益を要求する自由主義者や急進派の人々が、情報技術の倫理に関しては、最も基礎的な所有権と個人のセキュリティ権を危険にさらす曖昧なアプローチを採用するのは皮肉である。だが、プライバシーの問題として記述されているのは、まさに個人のセキュリティの問題である。個人や所有物に危害を加えかねないコンピュータの使用を誰も擁護しないだろう。そして、このような危害のリスクがある使用は、明らかに倫理的評価や訴訟の対象である。情報技術が個人のセキュリティを脅かすという点から道徳の基礎が明確になったなら、プライバシーに関する本当の問題がより明らかになるだろう。

紹介者コメント

確かに、プライバシーという言葉はわかりにくく広範囲にわたる。セキュリティとリスクの問題に還元するならば、議論は容易になるだろう。また、コンピュータ技術や国家の情報公開などの問題を分析するには有効であるかもしれない。

しかし、プライバシーに関して生じる問題すべてを議論するのに、リスク分析だけで十分かという疑問は残る。例えば、たとえ悪用されないと知っているとしても、他人には知られたくない情報はある。また、通常われわれが人々と会話を交わすとき、相手によって知らせる私的情報の内容や程度は異なるだろ

う。多くの人は、親しい友人には私的な情報を伝えても構わないが、あまり親しくない人、自分が嫌いな人、社会的に立場が異なる人には、私生活について語りたくないと思うだろう（逆に、匿名では私生活を語れるが、親しい人にはそれを知られたくないという場合もある）。それは、端的に知られたくないのである。あるいは、このような私的情報のコントロールから人間関係に濃淡が生じるともいえる。この点を認めるなら、必ずしもプライバシーとリスク分析とは同一視できない。むしろ、レイチェルズ流のプライバシー概念の方に、より一層の説得力があるように思われる。

（鶴田 尚美）