ISSN 2186 － 3989

アメリカにおける Privacy as Trust 論の理論的前提
－新たなプライバシー権論の構築に向けて－

佃　貴弘

Theoretical Premise of “Privacy as Trust” in the United States
－ toward Reconstructing of the New Privacy Theory －

Takahiro Tsukuda

北 陸 大 学 紀 要
第49号（2020年9月）抜刷

北陸大学紀要
第 49 号（2020）
pp.37～56
〔研究ノート〕

アメリカにおける Privacy as Trust 論の理論的前提
―新たなプライバシー権論の構築に向けて―

佃　貴弘*

Theoretical Premise of “Privacy as Trust” in the United States
－toward Reconstructing of the New Privacy Theory－

Takahiro Tsukuda*

Received May 31, 2020

Abstract

In recent years, Artificial Intelligence (AI) has become a boom due to the enhancement of the network environment. The analysis of “Big Data” has made it possible to discover new data features, and Deep Learning has improved the accuracy of inferences made by artificial intelligence. Since the analysis requires collecting a large amount of personal information, the government promotes the utilization of personal data. However, it also carries the risk of neglecting privacy protection.

Traditional privacy can no longer cope with this situation. In the case of the analysis based on information provided by the individual’s consent, it is difficult to assert tort privacy because there is no invasion. The privacy self-management is also difficult since they read the privacy policy not carefully and agree to it.

To solve the problem, this article focuses on the “Privacy as Trust” in the United States. This argument is protecting personal information by fiduciary duty and it has the potentiality to improve such situations. This article summarizes the recent changes in social background and its theoretical premise in order to explain why “Privacy as Trust” has emerged.

Key words：behavioral economics, fiduciary duty, information fiduciary

1 はじめに

1-1 本稿の目的

近年、ネットワーク環境の充実化により、人工知能（AI: Artificial Intelligence）がブームになっている。「ビッグデータ」の解析により新たなデータの特徴を発見できるようになり、ディープラーニングにより人工知能が行う推論の精度が向上した。その解析には、大量の個人情報を収集しなければならないので、政府により個人データの利活用が推進さ

*北陸大学経済経営学部　Faculty of Economics and Management, Hokuriku University

れている。しかし、それは同時に、プライバシーの保護がおろそかになるというリスクも生じる。

このような状況に対して、伝統的なプライバシーでは対処できなくなっている。本人が同意して提供した情報に基づいて解析している場合、侵襲がないため、不法行為プライバシーを主張するのは困難である。また、プライバシー・ポリシーを熟読せず同意しているのが実態であり、プライバシーの自己管理も困難になっている。

1-2 Privacy as Trust 論に着目する

その問題を解決するために、本稿では、アメリカにおける Privacy as Trust 論に着目する。これは、信認義務で個人情報の保護を図る議論であり、そのような状況を改善できる可能性を秘めている。本稿は、Privacy as Trust 論が登場した理由を説明するために、近年の社会背景の変容とその理論的前提を整理していく。

Privacy as Trust 論は、信託法理で個人情報の保護を図る議論で、2010 年代のアメリカで複数の情報法研究者から提唱されている（Balkin [2016]、Richards & Hartzog [2016], Waldman [2018]など）。

この法理は、イギリス信託法に由来し、信託財産の受託者が委託者（および受益者）に対して課される義務（信認義務 fiduciary duty）などで構成される。信認義務は、注意義務（信託の本旨に従い、善良な管理者の注意をもって信託事務を処理する義務）と忠実義務（受益者のため忠実に信託事務の処理する義務）からなる。

私は、信託法理の観点から個人情報保護を図ることの可能性について、佃[2014]で検討したことがある。また、日本において、（斉藤[2018]、斉藤[2019]のような）同様の研究や（山本[2019]のような）それを批判的に検討する文献も現れてくるようになった。しかし、アメリカにおける Privacy as Trust 論がどのような前提で何を論じようとするのかについて明確でないまま議論・批判されているのが現状である。そこで、この議論を論じる前提を整理する必要がある。

1-3 本稿の概要

そこで、本稿の 2 では、プライバシーに関わる議論（プライバシー権論）が登場する社会的背景を踏まえ、それが現代の社会背景とどの点で異なるかを把握する。それを把握することにより、従来の不法行為に基づくプライバシー権論の限界を整理する。

次に、本稿の 3 では、契約に基づく保護の観点から、自律・自己決定に基づくプライバシー権論の限界を検討する。とくに、現代社会におけるプライバシー・ポリシーの運用状況を踏まえると、（リバタリアニズムのような）個人によるプライバシーの自己管理を過度に尊重し、市場メカニズムに委ねるのは困難である理由を整理する。

そして、本稿の 4 では、近年のプライバシー・ポリシーに関わる問題から、政府によるプライバシー保護政策の必要性を整理する。しかし、近年のプライバシー権論では、単純なパターナリズムに依拠するのではなく、行動経済学の知見を用いて、選択の自由との調和を図っている。Privacy as Trust 論はこのような前提に基づいてプライバシー権論が展開されていることを述べる。

最後に、本稿の 5 では、本稿の 4 までに論じたことが Privacy as Trust 論の理論的前提になっていることを確認する。そのうえで、Privacy as Trust 論に向けられる批判を整理し、その応答に必要な論点を整理する。

2 プライバシー問題が生じる社会背景の変容

2-1 プライバシー権論が登場する社会背景

2-1-1 自己情報コントロール権が登場するまでの社会背景

まず、これまでのプライバシー権論（放っておいてもらう権利、自己情報コントロール権）が登場した社会背景を整理しておこう[1]。

昔ながらのプライバシー権論（放っておいてもらう権利 right to be let alone）は、論文 Warren & Brandeis [1890]に由来する。この議論が登場した社会背景は、インスタントカメラの発明に起因するイエロージャーナリズムに対する抵抗である。このプライバシー権論の趣旨は、アメリカ不法行為法の権威 Prosser [1960]により、①プライベートな事項への侵襲（intrusion）、②プライベートな事項の公共への開示、③公衆に誤った印象を与える公表、④名前・肖像の営利目的の盗用という 4 つの不法行為プライバシー（tort privacy）の複合体であるとしてまとめられた。

これに対し、自己情報コントロール権は、Fried [1968]の論文、Westin [1967]、Miller [1971]の著書によって知れ渡った議論であり、事故に関する情報の開示を自分でコントロールできることを唱えてきた。これらの議論の背景には、データベース社会が到来し、国家による監視が問題視されたことが一般に指摘されている[2]。

2-1-2 2010 年前後から生じた社会変化

ところが、2010 年前後から、これまでのプライバシー権論では対応できないような社会変化が生じてきた。ソーシャルメディアが発展し、動画投稿サイトなどのように、誰もが多くの人に情報を発信する技術が確立した。それにより、Solove [2008:79=2008:88]は、若気の至りで SNS に投稿した内容が原因で、自分自身に不利益をもたらす現象も生み出されたと指摘した。

また、2010 年頃から IoT（Internet of Things）機器が登場して、様々な物がインターネットに接続されて情報を交換するようになった。これは、様々な所から個人情報を収集されていることを意味し、本人がその事実に気づいていない場合もありうる。IoT 機器が発展することにより、本人の個人情報管理が行き届かなくなることも生じてきた。

もっとも、誰もが多くの人に情報を発信できるとはいえども、多くの人に情報を発信するには、そのようなサービスを提供するプラットフォーム事業者を利用しなければならない。IoT 機器の利用についても、同様である。近年、プラットフォーム事業は、GAFAM（Google・Amazon・Facebook・Apple・Microsoft）のような事業者により、市場の独占化・寡占化が進んでいる。

さらに、個人データ（データベース化された個人情報）の利活用に着目されたことも指摘すべきである。これは、近年の人工知能（AI: Artificial Intelligence）ブームが関連している。ネットワーク環境が充実化され、「ビッグデータ」とよばれるほどの大量の情報を解析することが可能となった。それにより、データマイニングを行うことによって、今までに知られていないデータの特徴を発見することも可能になった。

2-1-3 プライバシー悲観論

このような社会背景の変化に伴い、Richards & Hartzog [2016]は、これまでのプライバシーの捉え方について悲観論を展開し、このプライバシー悲観論（Privacy Pessimism）の原因として 3 つ挙げている。

その１つは、①IoT 機器・ドローン・Web メール履歴の盗聴という「ぞっとするようなトラップ（Creepy Trap）」への嫌悪感があることである（Richards & Hartzog [2016:437]）。もう１つは、②損害という要件にあてはめること（Harm Fixation）に夢中になりすぎて、プライバシーとして保護すべき価値をなおざりにしてしまっていることである（Richards & Hartzog [2016:441–43]）。そして、残る１つは、③個人が自己の情報を絶対的に保護できるといった完全にコントロールできるという幻想（Control Illusion）を抱いていることである（Richards & Hartzog [2016:444]）。

この悲観論の①は、2-1-2 で述べた社会背景に関わる。また、次のパラグラフでは、Solove [2008a=2013]の類型論を基にして、どのように変容したのかを確認する。さらに、その次のパラグラフでは、この悲観論の②に関連して、不法行為プライバシーの問題点を指摘しよう。なお、悲観論の③については、本稿の 3-2 で言及することとしたい。

2-2 Solove の『プライバシーの新理論』

2-2-1 Solove の類型論

Solove [2008a:103=2013:144]は、(1)情報収集（information collection）・(2)情報処理（information processing）・(3)情報拡散（information dissemination）・(4)侵襲（invasion）の４つのグループに類型化して、プライバシーを論じている。このうち、(4)の類型は、それらとは独立した別個の、データ主体に向けられた問題を類型化したものである。これに対し、(1)から(3)までの類型は、本人（データ主体 data subject）から個人情報を取り扱う事業者（データ保有者 data holder）を通じて生じる問題を類型化したものであり、下に示すように模式化できる。

(1)データ主体からの情報収集→(2)データ保有者による情報処理→(3)第三者への情報拡散

2-2-2 情報の流れに従ったプライバシー類型論

まず、(1)情報収集の観点でプライバシーの問題を考えたとき、国家機関（警察など）による調査監視（surveillance）からの防御という観点が、従来のプライバシー権論の主たる関心事であった。しかし、ソーシャルメディアを活用したシェアリング・エコノミー型サービスでは、事情を異にする。本人（データ主体）が率先して事業者に個人情報を提供しなければ、その便益を受けることができないからである。Uber のような利用者とドライバーをマッチングさせるウェブサイト（アプリ）を想定すると、このことが想像できるであろう[3]。つまり、ソーシャルメディアの利用における個人情報の収集の問題では、個人情報が収集されている前提での保護を検討しなければならない。

データ保有者に収集された個人情報は、その(2)情報処理についてもプライバシーの問題が生じる。そこで想定されるのは、断片化された個人情報を集約（aggregation）して、特定の個人に連結させ（同定 identification）、収集時とは別の目的で利用（二次利用 secondary use）することなどである。この点については、個人情報保護法制で規制がなされている。しかし、Solove [2008a:130–132=2013:176–178]が指摘するように、本人（データ主体）が二次利用を可能にするプライバシー・ポリシーを読まずに（理解せずに）承諾している実態がある。さらに、プラットフォーム事業が寡占化する状況においては、その事業が提供するサービスの便益を受けるために、承諾せざるを得ない側面もある。そのため、データ保有者（個人情報を取り扱う事業者）が合法に保有するデータについて、自

由に利活用できる状況にある。

また、(3)情報拡散の観点についても、一定の変容を見なければならない。従来の個人情報保護の観点では、守秘義務違反などの情報の漏洩を防止することが念頭に置かれていた。しかし、近年の「パーソナルデータの利活用」に関わる議論では、複数の事業者間の購買履歴・乗降履歴を分野横断的に利活用することで、イノベーションを生み出すことが期待されている[4]。このような場合、漏洩防止の観点で個人情報保護を論じても役に立たず、個人データが第三者提供されている前提で議論しなければならない。

2-2-3 従来のプライバシー権論では困難な事象——侵襲が存在しない場合

最後に、(4)侵襲について言及しておこう。伝統的な不法行為プライバシーは、Prosser [1960]の議論を基にして 4 つの類型にまとめられ、他者からの侵襲（invasion）などがあることを前提とする[5]。しかし、近年のプライバシー問題では侵襲がない類型がある。先のパラグラフで触れたシェアリング・エコノミー型サービスやマッチング・サービス（出会い系アプリ）が挙げられる。このようなサービスでは、本人が提供に同意しているため、本人に対する侵襲を認めることが困難である。このような場合に、プロッサー流の不法行為プライバシーを成立させることは困難である。

ここで示した近年のプライバシー問題の特徴を見ていくと、不法行為（tort）でプライバシー保護を図るという考え方を見直さなければならない（Balkin [2016:1190–91]）。

本人に対する侵襲がないという事実だけから、プライバシーが保障されないという結論を導くのは妥当性を欠く。不法行為とは別の構成でプライバシー保護を考えなければならない。

3 自律・自己決定の限界

3-1 「契約」はプライバシー保護に役立つか？

3-1-1 不法行為がだめなら契約？

不法行為によるプライバシー保護が十分でないと考えたとき、自然と思いつくのは、契約にその活路を見いだすことである。アメリカ法の文脈においても、Volokh [2000:1057–58]は、取材源秘匿の約束違反者に対して言論の自由（修正 1 条）による免責を認めなかった憲法判例 Cohen v. Cowles Media Co., 501 U.S. 663 (1991) を引き合いに出して、契約法によるプライバシー保護を論じている。

このように考えると、プライバシー・ポリシーが適切ならばそれに合意するという方法でプライバシーの保護を図ることができそうである。しかし、Balkin [2016]は、契約という手段でもプライバシーの保護として十分ではないと指摘する。契約構成には、2 つの問題点があるからである。

その 1 つの問題点とは、プライバシー・ポリシーによる事業者の制限が機能しないことである（Balkin [2016:1199]）。多くのウェブサイト・アプリにおいて、プライバシー・ポリシーが示され同意を求められる。しかし、多くのユーザがそのポリシーに無関心であるため、プライバシー・ポリシーを用いた保護の方法では有効に機能しない。

もう 1 つの問題点を、Balkin [2016:1201]は医療情報の文脈で説明する。この文脈では、インフォームド・コンセントの考え方が広く普及しているので、患者への説明と同意が強く意識づけられる。しかし、患者との契約で個人情報の保護を図ろうとすると、患者が誰と合意したのか（担当医個人なのか、診療科なのか、病院なのか、医療法人なのか）が曖

昧なために、すべての個人情報について誰が何について合意したのかを把握するのが困難になるという。

3-1-2 「契約」で解決するという方法そのものの限界

さらに、Balkin [2016:1201–02]は、「契約」という方法でプライバシーを保護すること（契約モデル）自体に限界があると指摘する。たとえば、政府がデフォルト・ルールとすべきプライバシー保護のあり方を策定したとしても、その策定以前に締結された個別契約を適切な内容に結び直すとは限らないからである。

このことは、リバタリアニズム（自由至上主義 libertarianism、新ロックナー主義 neo-Lochnerian）にとって期待していない現象が生じている。この立場は、修正 1 条が契約の自由を保護していると解釈し、経済的自由を含んだあらゆる自由を最大限に保障しようとする。この立場に従えば、政府がどんなプライバシー保護規制を行っても、個別の契約にその規制を取り込ませることができなくなるからである（Balkin [2016:1202–03]）。

自由を最大限保障するためには、政府による介入を排除すべきであると考えるかもしれない。しかし、現実には行政法規による規制がなされている。それどころか、個人情報のやりとりを市場メカニズムに委ねようとすると、プライバシーを危険にさらすことになる。そこには、自分の個人情報を完全にコントロールできるという幻想を抱いているからである。この点について、3-2 で検討していく。

3-2 私的自治（市場メカニズム）に委ねられるのか？——経済学的考察に基づいて

3-2-1 市場の失敗の可能性

リバタリアニズムのように、政府の介入を可能な限り排除して私的自治に委ねることを主張することは、政治理論としてはあるかもしれない。しかし、それは、思考実験としての意義はあっても、実用的な議論にはならない。医療情報を保護する機能を果たすのは、医療保険の携行性と責任に関する法律（Health Insurance Portability and Accountability Act: HIPAA）などの行政法規であり（Balkin [2016:1201–02]）、現実には公法上の規制を受けるからである。それどころか、政府の規制なしではうまくいかず、市場の失敗の可能性がある。

市場の失敗の原因として、ミクロ経済学の教科書で一般的に指摘されるのは、(1)独占・寡占、(2)公共財、(3)外部性、(4)不確実性である。個人情報保護の文脈では、その主たる要因が、(1)と(2)ではなく、(3)と(4)にあると考えられる。その理由を(1)から(4)の順に説明する。

3-2-2 寡占状態・公共財的性質は「市場の失敗」の要因となりうるか？

個人情報保護に関する「市場の失敗」を論じるとき、(1)個人情報を取り扱う事業者について寡占化が生じていることがその要因であると単純に考えるかもしれない。たしかに、プラットフォーム事業の寡占化により、本人（データ主体）から収集した個人情報を自由かつ容易に処理することが可能となる。寡占化が進めば進むほど、複数の事業者間での個人データのやりとりを考察する必要がなくなるからである。しかし、GAFAM のようなプラットフォーム事業者が市場を独占（寡占）していても、そのことだけが理由で個人情報の保護が阻害されるとは限らない。また、シェアが小さくても、同業他社がその水準以上のサービスを提供できれば市場の失敗を回避しうるからである[6]。

また、(2)情報財[7]の公共財的性質から、「市場の失敗」が論じられることがある。つまり、情報は、複数人が同時に利用することができ（非競合性）、共有の方法でしか情報のやりと

りをすることができない（情報を提供しても、提供者はその情報を忘れない）ので技術的に排除できない（非排除性）からとされる。しかし、情報財の非排除性はその情報を他人に提供した場合に生じる（不可逆性）ので、情報を他人に漏洩させないという観点でその保護が可能である。

したがって、個人情報の適切な保護に関わる問題において、寡占化と公共財的性質はそれほど重要な要因ではないと考えられる。寡占化については、現状より適切なプラットフォーム事業者が登場していないという状態にすぎない。また、公共財的性質についても、情報の漏洩を防止するという観点で考えれば、その排除性も確保できるからである。

3-2-3 外部性・不確実性の問題

ここで、(3)外部性と(4)不確実性について、一般的な説明を確認しておこう。（経済学における）外部性とは、人々の行動が市場取引を通さずに他者に与える影響のことを指す。また、不確実性とは、人々が不完全な知識で行動しなければならないことを指し、人々が保有する情報が偏在していることが不確実性の原因に挙げられるため、しばしば「情報の非対称がある」とも表現される。そして、情報の非対称がある場合、逆選択（逆淘汰）やモラル・ハザードという市場の非効率化が生じることが知られている。

個人情報保護の文脈では、その外部性に関わるものとして、2 つのものが指摘されてきた。1 つは、Shapiro & Varian [1999:13=2018:37]のいうネットワーク外部性とよばれる効果で、製品やサービスの価値が利用者数に依存していることを指す。Shapiro & Varian [1999:183–184=2018:356–359]は、この効果により、ネットワークのサイズが大きくなると提供される価値が上昇すると指摘する。したがって、取引数量が大きくなると規模の経済から価格が低下し、プラットフォーム事業は寡占状態になりやすい。外部性が寡占化の要因と考えられる。

もう 1 つは、ある個人にとっての情報の有用度は、他人が保有する情報量によっても影響されるということである（野口[1974:45]を参照）。個人が役に立つ情報をいくら集めたとしても、誰もが知っている情報を集めただけでは、独占的な利潤を得ることができない。逆に、人々に知られていなかった情報を公にしてしまうことにより、独占的に得られた利潤を失い、非公知の状態に戻すこともできなくなる。

したがって、情報に関わる市場を論じる場合、「他人に知られていない」という外部性の問題を無視できない。

3-2-4 「コースの定理」からプライバシー権を読み解く——取引費用低減論の妥当性

このような外部性と不確実性の問題があっても、取引費用（transaction cost）を低減させれば市場メカニズムが機能するという議論がある。その論拠となっているのが、コースの定理である。この定理は、1960 年に発表した論文「社会的費用の問題」（Coase [1988:95–156=1992:111–178）に由来し、この定理から、次の 2 つの特徴が示される。

1. 取引費用がゼロの場合、いずれの法ルールを選ぶにせよ効率的な結果がもたらされる。
2. 取引費用が正の場合、効率的な結果がすべての法ルールのもとで生じるとは限らない。

「シカゴ学派」[8]と呼ばれた経済学者は、この定理の 1.の特徴から、「外部性がある状況でも、取引費用が存在しなければ、当事者間の自発的な交渉によって効率的な資源配分が実現できる」ことを「コースの定理」と呼んだ。そして、取引費用をゼロに近づければ、

市場の失敗を回避できるので、市場メカニズムに委ねることも可能であるとする。

このような「シカゴ学派」の立場からは、プライバシーは本人にとって不利になることを秘匿する権利であるとして否定的であった（たとえば、Posner [1981:271=1991:246]）。プライバシーを保護すれば、相手方に関する収集に係る費用が増加するので、「市場の失敗」の原因になると主張するからである。また、自己情報コントロール権により、自分に有利な情報のみが開示される状況を生み（Posner [1981=1991:247]）、市場の効率性を阻害する効果がある（逆選択と同様の現象が生じる）というのも理由とされる。プライバシーを可能な限り否定すると、取引費用が低減するので、外部性による市場の失敗を回避できると主張する。また、取引費用をゼロに近ければ、相手方に関する情報を容易に知ることができ、逆選択が生じることもないようで、不確実性による市場の失敗も回避できる。

しかし、取引費用をゼロにするという仮定は非現実的であり、その仮定に近づけることも困難である。現実の人間の認知的能力に限界があり、必ずしも合理的に行動するとは限らないからである。この点については、Herbert A. Simon が限定合理性（bounded rationality）という表現で以前から指摘しており、行動経済学がその議論を進化させている。

3-2-5 Solove の議論——認知的問題・構造的問題

ここで、Richards & Hartzog [2016:444 n.46]の（2-1-3 で述べた）プライバシー悲観論の③に立ち戻ろう。それは、自己に関わる情報を完全にコントロールできるのは幻想であるという内容である。その根拠は、Solove [2013]であり、個人情報の自己管理が困難なのは認知的問題と構造的問題があるからであるという。

Solove [2013:1888]のいう自己管理の認知的問題とは、多くの場合、個人情報の収集の際に提供されるプライバシー・ポリシーを読まず、読んだとしてもその内容を理解できず、理解できたとしても判断に必要な背景的知識が欠如している。また、十分に判断できるような前提があったとしても、多くの選択肢に戸惑ってしまうという問題も生じるという。

また、自己管理の構造的問題とは、個人情報を自己管理しようとする決定に構造的問題があるということである。個人情報の管理について決定するのは、その決定が適切であるかどうかが十分に判断できる前である。当該個人情報の管理を判断したときには問題ないと判断した個人情報が集積されて、知られたくない情報が管理の及ばないところに広がっていくという事態が生じている（Solove [2013:1888–93]）。

Solove [2013:1894–1900]は、このような認知的問題と構造的問題があるために、事前同意（Opt-in Consent）の方法ではうまくいかないと論じている[9]。

4 プライバシー権論の新たな流れ

4-1 プライバシー保護政策の必要性

4-1-1 市場メカニズムでプライバシー保護は期待できない

本稿の 3.では、認知的問題と構造的問題があるため、自己情報コントロール権は「個人情報の不当な取扱い及びそれに起因する不利益を防止」という目的を達成するための十分な手段にならないことを論じた。個人情報のやりとりに関する取引費用をゼロに近づければ、外部性と不確実性の問題を解消できるかもしれない。しかし、認知的・構造的問題を回避できないので、その議論は現代のネットワーク社会に適合しない。

そのため、個人情報の適切な管理を論じるには、情報の非対称性を解消するのではなく、

不確実性（情報の非対称性）があることを前提に改善策を考えなければならない。つまり、データ主体（本人）とデータ保有者（プラットフォーム事業者）との間に情報力・交渉力の差が生じているという前提で議論しなければならない。

4-1-2 本人の脆弱性・依存性

Privacy as Trust 論は、このような情報の非対称性を前提にし、データ主体とデータ保有者の関係を依頼者と専門家の関係と類似していることから、個人情報管理の適切なあり方を論じているものがある。Balkin [2016]の情報受認者（information fiduciary）論がそれに該当する。

Balkin [2016:1222]が、データ主体とデータ保有者の関係を依頼者と専門家の関係に類似すると論じるのは、情報の非対称性だけでなく、一方当事者の脆弱性・依存性が見られるからである。個人情報を有する本人が事業者の提供するサービスについてよく知らないという脆弱性（vulnerability）をもち、事業者側が提供するサービスに依存（dependence）する傾向がある。そのサービスには、個人情報の提供がなければ便益を受けられないものも多い。

4-1-3 逆選択（逆淘汰）の問題

このような情報の非対称性がある場合、逆選択のようなメカニズムが生じる[10]。つまり、本人（データ主体）からはどの事業者（データ保有者）が適切にプライバシーの保護を図っているのかを把握できないために、プライバシーの保護に厚い事業者が市場から淘汰されるという現象が生じるという。これでは、社会的に望ましくない状況に陥ってしまう。

逆選択を回避するための対策として、スクリーニングやシグナリングなどの方法があると一般に指摘されている。しかし、事業者が個人情報保護に厚いことをアピール（シグナリング）しても、消費者がその企業を選ぶとは限らない。また、消費者（データ主体となる本人）は、事業者が提供するサービスを選択するとき、自己の個人情報を適切に保護していることを重視するとは限らない（スクリーニングを行わない）からである。Hoofnagle [2016:149=2018:7]は、アメリカのプライバシー法の文脈で、プライバシーは売れないと指摘する。

4-1-4 「通知および選択」モデルの限界

また、個人情報の第三者提供について、同意を要件とする制度設計になっていることが一定の限界を示している。この点については、アメリカにおいても同様である。連邦取引委員会（Federal Trade Commission: FTC）の「公正な情報慣行の原則」（Fair Information Practice: FIP）は、「通知および選択（notice and choice）」を前提にしたモデルで設計されているからである（Gellman [2019:23]参照）。

Solove [2013:1883–1884]は、FIP などにおいて「通知および選択」アプローチを採用しているけれども、プライバシーに関する通知に関心を持たない（3-2-5 で述べた認知的問題がある）ために、ほとんどの人が自己管理していないと指摘する。その理由として、歪められた意思決定（Skewed Decisionmaking）の問題を挙げる。Solove [2013:1886–1888]は、Thaler & Sunstein [2009:9=2009:23]の議論に依拠して、自己決定論が「ほとんどすべての人が、ほとんどすべての場合に、自分たちの最大の利益になる選択をしているか、最低でも第三者がするより良い選択ができる」という誤った前提に立っていることを批判する。また、現実の個人は「限定合理性（bounded rationality）」に基づいて、「利用可能性ヒューリスティック（availability heuristic）」[11]に歪められてリスク評価をしていることもその根拠とする。

4-1-5 漏洩防止の観点の限界

このように伝統的プライバシー保護における「通知および選択」モデルに限界があるのと同様に、漏洩防止の観点で個人情報の保護を図るという手法にも限界がある。

（多くの個人情報保護法制が参照する）経済協力開発機構（OECD）のプライバシーガイドライン（OECD [2013:15]）[12]では、「個人データは、合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護すべき」（OECD8 原則§5: 安全保護措置の原則）が定められている。

しかし、現在のプライバシー問題は、データセキュリティの問題だけではない。Richards & Hartzog [2016:467]はその事例として、ニューヨーク市政府が不適切に匿名化されたタクシーの乗降履歴に関するデータを公開したために、データセット内の人物を特定できてしまった事件を挙げる。これは、乗降履歴を専門的に解析することにより、知られていない市民の動向に気づくために行われるものである。そのような解析そのものを否定すれば、産業の停滞を招きかねない。Richards & Hartzog [2016:468]は、データサイエンスの発展による「再特定化（reidentifying）」への対策として、堅牢な匿名化手法[13]に遅れないようにする必要があることを述べる。

4-1-6 政府による規制が必要

4-1 で述べたことをまとめておこう。自己情報コントロール権に位置づけられるプライバシー権論においては、本人が自分の個人情報を管理し（プライバシーの自己管理）、事業者が保有する個人情報の漏洩を防止するという観点で議論されてきた。

しかし、そのような自己管理は人間の情報処理能力を超えた行為であり、プライバシーに無関心な者が多く（プライバシーは売れない）、プライバシー不要論（やましいことは何もない）という議論もある。

また、事業者がどのように個人情報を利用しているかについても変化しており、事業者が保有する個人データを分析して、事業活動に役立てる動きも見られるようになった。そのためには、専門的に解析できる事業者に個人データの提供することもありうる（第三者提供）。もちろん、この場合、個人データを匿名加工したうえで第三者提供をするのが通常である。しかし、安全であると考えた匿名加工の方法でも、データサイエンスの技術が発展して、「再特定化」できてしまう可能性もある。

さらに、事業者が巧妙にプライバシー・ポリシーを作成することで、本人の同意を取り付けたり、本人の同意をなしでも可能な方法で匿名加工したりすることで、個人情報が容易に第三者提供されれば、プライバシー・個人情報の自己管理は困難である。

4-2 行動経済学の知見を取り入れる

4-2-1 ナッジの議論に着目する

そこで、Solove [2013:1900–03]は、ナッジ（Nudge）を活用し、部分的なプライバシーの自己管理を説いている。ナッジは、Thaler & Sunstein [2009=2009]が提唱したリバタリアン・パターナリズム（libertarian paternalism）[14]に基づく政策手法である。Sunstein [2013:2017=25–34]は、オバマ政権第 1 期に OIRA（Office of Information and Regulatory Affairs: 行政管理予算局情報・規制問題室）室長に就任したという実務経験から、ナッジが有効であると主張する。

ただ、リバタリアン・パターナリズムという表現は、個人の「選択の自由」を尊重するリバタリアニズム（libertarianism）と失業対策などのために政府による介入（自由の制

約）を認めるパターナリズム（paternalism）という相反する概念を並べている。しかし、Thaler & Sunstein [2009:4–6=2009:15–18]は、自家撞着ではないという。望ましくない取り決めを拒否したいのなら拒絶を選択する自由を与えられる（リバタリアンの側面）と同時に、政府も人々の暮らしが良くなるような選択をするように誘導する（パターナリズム的側面）からである。

4-2-2 ナッジとはどういう議論か？

Thaler & Sunstein[2009=2009]は、リバタリアン・パターナリズムの思想を実現する政策手法として「ナッジ」を用いる。Thaler & Sunstein [2009:4=2009:2]によれば、ナッジとは、「注意や合図のために人の横腹を特にひじでやさしく押したり、軽く突いたりすること」をいう。つまり、この文脈でいう「ナッジ」とは、この言葉の意味が示すように、人々を強制せずに、「選択の自由」を認めながら、人々の注意を特定の方向に向けさせて、規制の効果を実現させるような政策手法を指す。

Thaler と Sunstein は、ナッジによる政策手法を実現するために、選択アーキテクチャー（choice architecture）を重視する。たとえば、男性用トイレの小便器に黒いハエの絵を描いたことで、飛沫の汚れが 80%も減った。強制されたわけではないが、ハエの絵に向けて用を足すようになったからである（Thaler & Sunstein [2009:3-4=2009:14]）。このハエの絵のように、人々が意思決定する文脈を踏まえて一定の設計を施したものを「選択アーキテクチャー」という。

4-2-3 2 つの思考モード――速い思考（システム 1）と遅い思考（システム 2）

Thaler と Sunstein がナッジや選択アーキテクチャーを重視するのは、パターナリズムを認めない人たちが依拠するような経済人（homo economicus）の前提（完全合理性仮説）に疑問を持っているからである。

Kahneman [2011=2014]によれば、人間の思考には、「速い思考（システム 1）」と「遅い思考（システム 2）」がある（Stanovich & West [2000:658]）ということが心理学の領域で指摘されている。Kahneman [2011=2014:上巻41]は、システム1 が「自動的に高速で働き、努力は全く不要か、必要であってもわずかである」のに対し、システム2 は「複雑な計算など頭を使わなければできない困難な知的活動にしかるべき注意を割り当てる」と説明する。

たとえば、複雑な計算をする場合、システム 2 を使わずに正確な答えを導くことは難しい。もっとも、日常生活では、直感的に簡単に答えを出す（おおよその数値を答える）ことも行われている。このような「困難な質問に対して、適切ではあるが往々にして不完全な答を見つけるための単純な手続き」のことをヒューリスティックという。ヒューリスティックに答える場合、システム 1 が担当している場合が多い（Kahneman [2011=2014:上巻 177]）。しかし、ヒューリスティックを使った場合、導き出された結論にバイアスが生じる場合があり、誤った判断をすることがある（Kahneman [2011=2014:上巻第 2 部]）。

Thaler & Sunstein [2009:19=2009:38]は、ナッジの議論を展開する際に、システム 1・システム 2 の議論をそれぞれ自動システム・熟慮システムと置き換えて、同様の議論を展開している。

Solove [2013]は、このような議論を踏まえ、プライバシー・ポリシーに関する意思決定を論じている。Solove [2013:1887]は、事業者からプライバシー・ポリシーに同意を求められる場合、前述した認知的問題があるために、本人はヒューリスティックに判断せざるを得ないと指摘する。それに同意しなければ事業者のサービスによる便益を受けることはできず、プライバシー・ポリシーの条項を理解できるまで同意を留保して熟考するほど時間を割くことはしない（できない）からである。つまり、データ主体が自分の個人情報を管

理するとき、多くの場合、システム 1（自動システム）で行っているという前提で考えなければならない。

4-2-4 デフォルト・ルールをうまく設計する

多くの人がプライバシー・ポリシーをシステム 1（自動システム）で判断しているという前提に立ったとき、デフォルト（初期設定値）をどのように設定するかである。

この点に関連して、Thaler [2015=2019:下巻 245–248]は、Johnson & Goldstein [2004]による臓器提供に関するデフォルト・ルールの設計を用いて論じている。Johnson & Goldstein [2004:1715]では、臓器提供について意思表示しない場合に同意と推定するか不同意と推定するかによって、それに同意したと扱われる割合が大きく異なることが指摘されている。つまり、臓器を提供することをデフォルトにしている（意思表示がなければそれに同意したと推定する）国では臓器を提供しない選択をする者が少なく、臓器を提供しないことをデフォルトにしている（意思表示がなければそれに同意しないと推定する）国では臓器を提供する選択をする者が少なくなっているという現象が見られたというのである。

このように見ていくと、デフォルト・ルールをうまく設計すれば、プライバシーのより適切な保護を図ることができそうである。このように設計されたものが、Thaler と Sunstein のいう選択アーキテクチャーである。また、Sunstein [2015:25=2017:30]は、人々がデフォルト・ルールのままで選択するという「選択しないという選択」をすることを述べている。つまり、デフォルト・ルールが容易に変更できるとしても、人はこれを変更しようとしない傾向がある。その具体例として、Sunstein [2015:29–32=2017:35–37]は、プライバシー保護に関するデフォルト・ルールを挙げている。

4-2-5 プライバシー・バイ・デザイン論

ここで想起されるのは、プライバシー・バイ・デザイン（Privacy by Design: PbD）の議論である。これは、カナダの Ann Cavoukian によって提唱された運動で、プライバシー侵害のリスクを低減するために、事前にシステムの開発段階でプライバシー対策を考慮しておくということを説いている。

PbD の議論は、①リアクティブ（事後）でなくプロアクティブ（事前）、②デフォルト設定でプライバシー、③設計時に組み込むプライバシー対策、④ゼロサムではなくポジティブサム、⑤エンドツーエンドのプライバシーライフサイクル、⑥可視化と透明性、⑦ユーザープライバシーの尊重という基本原則で構成されている（Cavoukian [2009=2012:90–92]）。Rubinstein & Good [2013:1338]は、この基本原則そのものが（実用的・運用的なものというより）野心的なものであると指摘する。それでも、研究者によって、その要素を具体的に定義されている。

Rubinstein & Good [2013:1377–1406]は、Google と Facebook におけるそれぞれ 5 件のプライバシーに関わる事象を分析する。その事象の 1 つとして、Google がかつて提供していた Buzz というソーシャル・サービスを挙げる。そこでは、「Buzz に登録した Gmail ユーザは、自動的に他のユーザをフォローする」（ユーザのプロフィールを閲覧するすべての人がアクセスできる）ように設定され、Gmail 連絡先リストの悪用による秘密漏洩の「危険地帯」にした。もちろん、オプトアウト（積極的に拒絶する）ことで Buzz に不参加とすることができる。それでも、多くの無警戒なユーザが Buzz に飛び込んで混乱を招くことになった（Rubinstein & Good [2013:1384–1388]）。

Buzz のような事象では、PbD の基本原則の②に適合するデザイン、たとえば初期値（デフォルト値）を「フォローしない」などにすれば、混乱を回避することができたはずであ

る。Rubinstein & Good [2013:1407]は、PbD の考え方を採用していれば、これらの事象のすべてが回避可能であると結論づけている。

FTC [2012]の報告書[15]は、PbD のアイデアを取り入れている。しかし、この報告書の枠組みは、現在 FTC によって施行されている法規制の要件を超えている部分については、法律に基づく法執行措置や規制の一部として機能しないとしている（FTC [2012, pp. i, vii]）。そのため、Hoofnagle [2016:191=2018:70–71]は、FTC [2012]がプライバシーに関する規制上の義務になっていないために、企業がプライバシー保護の利益を理解し PbD を意図的に採用しない限り、たいした成功は望めないと指摘する。

4-3 デザイン・コントロール論は新たなプライバシー権論になりうるか？

4-3-1 デザイン・コントロール論の手段性

4-2 では、行動経済学の知見を踏まえ、プライバシー・ポリシーや個人情報を取り扱うウェブ・デザインについて、プライバシー保護に資するような設計を構築することを論じた。一言で言えば、デザイン・コントロール論である。

「通知および選択」モデルの場合、説明して同意をとりつければ十分であるとして、本人（データ主体）に責任を転嫁するという印象を与えることがありうる。これに対して、デザイン・コントロール論は、PbD の基本原則に沿って言えば、⑦本人のために、①事前に、②プライバシーの保護に資するような③設計を組み込めるという点で優れている。

しかしながら、このような「システム構築を前提として、その構造やアーキテクチャーをどのように設計すべきか」という議論が従来のプライバシー権論を超えた新たな議論であるとまではいえないと考えられる[16]。デザイン・コントロール論も、自己情報コントロール権と同様に、手段としての側面が強いからである。

デザイン・コントロールは、（Google や Facebook などの）プラットフォーム事業者に対してプライバシーを保護させるための手段の 1 つとして機能する。しかし、アメリカ法においても、現行の法制度の枠組みの範囲内でしか機能できない。

各事業者が行うべきデザイン・コントロール論の内容についても、個人情報の不当な取扱いを防止するという目的を見失えば、プライバシー保護に対する弊害を招く。そのためには、個人情報の不当な取扱いを防止するような、デザイン・コントロールの条件を考察しなければならない。

4-3-2 選択アーキテクトを信用しているか？

プライバシー保護に有効なデザイン・コントロールを考察するには、それを支えるナッジの手法の考察が不可欠である。実際に、ナッジの手法に対しては、心理トリックを駆使して人々を恣意的に操作するという否定的な印象を持つ者もいるからである。つまり、アーキテクチャーを設計して（場合によってはだまして）、事業者の都合のいい方向へ利用者（本人・データ主体）に選択させるのは、全体主義的な考えにつながるのではないかと批判するのである[17]。

もちろん、Sunstein 自身がそれは誤解であると否定している。このことは、すべてのデフォルト・ルールについては多くの人がデフォルトのままにしないことを Sunstein が指摘していることからも読み取れる。Sunstein がその例示として、結婚後の名字を挙げている。アメリカのすべての州で同じデフォルト・ルール（男女とも結婚前の姓をそのまま使用する）を採用しているにもかかわらず、既婚女性のほとんどがそのデフォルトを拒絶しているからである。夫婦同姓を選択する理由としてさまざまなものが考えられるが、明確な選好（clear preference）がある場合（この文脈では、夫婦の姓をどのようにしたいかに

ついて明確に決めている場合）にはデフォルト・ルールどおりにはならないと Sunstein [2015:53–55=2017:58–61]は指摘する。

このように、ナッジの手法は、強い自己決定の意思がある場合には、選択アーキテクチャーの内容よりも優先される。また、極端なデフォルト・ルール（extreme default）が設定されている場合にも、そのデフォルトを拒絶すると指摘する（Sunstein [2015:55–57=2017:61–62]）。それでも、巧妙に選択アーキテクチャーを設計して、人々が思ってもみなかった方向に操作されていることを警戒するかもしれない。このような場合、事業者による不当な個人情報の収集に対し、自己防衛をしなければならなくなる。

Brunton & Nissenbaum [2015:7–24]は、難読化（Obfuscation）による自己防衛策を論じている。たとえば、トラッキング（クッキーなどを用いたアクセス履歴の把握）を防止するための措置を講じたり[18]、検索履歴の解析を防止するために SIM カードを差し替えたりすることなどを提唱する。Richards & Hartzog [2017:1183]は、監視やデータ収集のために情報力を搾取されていることに対する抵抗する力を人々に与えている点で、この議論を好意的に評価する。しかし、その議論は同時に、事業者に対する不信（distrust）を生むと指摘し、難読化（Obfuscation）の手法は次善の策でしかないと主張する（Richards & Hartzog [2017:1207]）。

4-3-3 自己防衛（難読化）は不信を生む

Sunstein [2015=2017:62]は、選択アーキテクチャーに不信感がある場合に、デフォルトを拒絶するという現象がみられることを指摘している。つまり、人々がデフォルト・ルールに代わる提案に関して知識を持っていたり、選択アーキテクトに対して信頼度がなかったりした場合、本人（選択者）は自分で選択したいと思うからである。

しかし、このような自己決定（本人が自分で選択する）ことが必ずしも本人にとってよいことであるとは限らない。たとえば、2 段階認証プロセスのために携帯電話番号を提供すること拒絶した場合、セキュリティ面を強化することを自ら拒絶したという意味にもなりうる。もちろん、2 段階認証プロセス以外のセキュリティを選択する自由はあるべきであるけれども、選択アーキテクチャーに不信感がセキュリティ面の弱体化という悪影響を生み出すことがある。

もっとも、難読化（Obfuscation）のような自己防衛策が不信を生むことと、不信感が個人情報保護について悪影響を及ぼすことと明確な因果関係があるかどうかについては、本稿において明確に論証することではない。しかし、不信感とセキュリティ面の弱体化とがスパイラル状に作用すれば、個人情報保護に深刻な影響を与えることになる。

Sunstein [2015=2017:79]は、「十分な情報を与えられたとしたら大半の人が選ぶような事柄を反映するデフォルト・ルールを選ぶ」と指摘する。選択アーキテクチャーを設計する事業者が本人のために設計したか（信用できるか）ということが重要になってくると言える。むしろ、自己防衛策を強調することで、本人と事業者を対峙させるという発想に問題があるといえよう。

4-4 Privacy as Trust 論——信認義務に着目する

4-4-1 トラストによるプライバシーの活性化

難読化のような技法は、本人（データ主体）と事業者（データ保有者）を対峙させるという発想で考え、対立構造を導き出している。しかし、事業者が保有する個人データの適切な管理を論じるのであれば、本人の脆弱性を利用した事業者による搾取を防止すれば十分である。

そこで、Richards & Hartzog [2016]は、信託（trust）を通じてプライバシーを活性化させることを論じている。信託に着目するのは、受託者に課された一連の義務（信認義務）、とくに忠実義務（duty of loyalty：受益者の利益のためにのみ信託財産を管理する義務）による保護を図ることができると考えるからである。

このような議論には、現実社会における個人は弱い存在であるという前提がある。つまり、Balkin [2016:1215]によれば、事業者と本人との関係には、本人に脆弱性と依存性があるという。ここでいう脆弱性とは、個人情報を提供する本人がオンライン・サービスについてよく知らないということを指す。また、依存性とは、本人が事業者の提供するサービスに頼らなければならないことを指す。さらに、これらのサービスには、個人情報を提供することによってはじめて便益が得られるものも多い（Balkin [2016:1222]）。

4-4-2 事業者に専門家責任を課す

この議論が着目するのは、事業者と本人との関係が専門家と依頼者の関係と類似しているということである。たとえば、Solove [2004:102-04]は、守秘義務の観点でプライバシーを論じている。医師と患者の関係で見た場合、患者に特有の情報を収集せずに適切な治療を行うことはできない。そこで、医師に患者の個人情報を取得する権利とともに、その情報を秘匿する義務（守秘義務）も生じるような制度設計が必要となる。

本人と事業者の関係を、信託に似た関係（信認関係：fiduciary relationship）と捉える議論は、Frankel [2011=2014]の議論から来ている[19]。Frankel [2011:4–5=2014:5]は、信認関係における受託者（受認者 fiduciary）の定義は一定していないけれども、①財産または権限が委託されること、②委託者（entrustor）が受認者を信頼していること、③委託することによって委託者がリスクを負うことという 3 つの要素が共通してみられるという。

Balkin [2016:1205–06]は、この議論を踏まえ、事業者を「情報受託者（information fiduciary）」として捉えることを論じる。この議論では、事実として、専門家に依存していることを前提にして考える。そのように論じることにより、事業者がプライバシー保護を怠ったときに、専門家の過誤（professional malpractice）として捉えることが可能となるという。

本人と（個人情報を取り扱う）事業者との間で信認関係が成立したとき（それは必ずしも契約によって成立するとは限らない）に、注意義務と忠実義務が受託者に発生すると捉えるからである（Balkin [2016:1207–08]）。

5 おわりに

5-1 まとめ

本稿では、Privacy as Trust 論の理論的前提をまとめた。その前提の 1 つとして、プライバシー問題が生じる社会背景が変容していることである。事業者からそのサービスの便益を受けるために、本人が自ら個人情報を提供する場面が増えてきている。この場面では、本人が提供に同意した個人情報であるため、伝統的な不法行為プライバシーで保護することが難しい。

このような困難を避けるために、契約を使ってプライバシーの保護を図ることも考えられる。事業者が提供するプライバシー・ポリシーを読み、同意できる場合に個人情報を提供するという方法（「通知および選択」モデル）は、自己情報コントロール権とも親和的である。そのような自己決定を前提にしたプライバシー権論を強調することには、経済学的観点から疑問がある。

自己決定論を過度に強調した場合、いわゆるリバタリアニズムの思想と結びついて、個人情報のやりとりについても市場メカニズムに委ねることを重視する立場を採用しやすい。しかし、現実的に、実際の人間の行動原理を踏まえると、取引費用をゼロに近づけることが困難である。現実の人間が意思決定をする場合、判断に必要な情報を処理する能力に限界があるので、個人が限られた時間の中で最終的な意思決定をしなければならないという構造上の問題もあるからである。本人と事業者の間で個人情報をやりとりする場合、市場メカニズムに委ねることはできず、政府による政策が必要となる。

そこで、アメリカのプライバシー権論で着目されているのが、行動経済学の知見を取り入れることである。その手法として、「選択の自由」を認めながら、プライバシーの保護に資するようなデフォルト・ルールを設計することが考えられる。しかし、設計されたデフォルト・ルール（選択アーキテクチャー）が信頼できないものであれば、人々はデフォルト・ルールと異なるルールを選択する。そのデフォルト・ルールがプライバシー保護に貢献するとしても、その事業者に対する信頼が足りなければ、人々がプライバシーを危険にさらす選択肢を選ぶ場合もありうる。

Privacy as Trust 論は、このような信頼（Trust）を基にプライバシーの保護を論じている。たとえば、Richards & Hartzog [2016]は、信託（Trust）を通じてプライバシーを活性化させ、信認義務による保護を論じている。また、Balkin [2016]は、事業者がプライバシー保護を怠った場合、医療過誤などと同様の問題（専門家過誤）としてプライバシー権を論じようとしている。

5-2 今後の課題

5-2-1 今後の課題（その 1）――「自己決定」とは？

本稿では、Privacy as Trust 論が必要とされる理論的前提を整理した。しかし、Privacy as Trust 論そのものについては、紙幅の都合から、その概要を示すことにとどめ、詳細に検討を加えることができなかった。

本稿で積み残した課題には、少なくとも 2 つあると考えられる。

その 1 つは、プライバシー保護の文脈で語られる「自己決定」の意味を整理することである。本稿では、契約に基づくプライバシー保護に限界があることを論じるために、リバタリアニズムに基づく自己決定論（市場メカニズムに委ねる議論）を批判した。これは、「自己決定」をパターナリズムと対立させて説明する場合には便利である。しかし、自己決定論が必ずしもリバタリアニズムに依拠しているとは限らない。

そのため、（リバタリアン・パターナリズムの思想に基づいた）ナッジの手法による決定であっても、「自己決定」なのではないかという批判をする可能性もある[20]。しかし、ナッジの手法に基づいた決定方法は、（カント哲学のいう）自律と大きく異なり、「自己決定」であると言い切るべきではない。カントが「啓蒙とは何か？」で批判していたのは、理性的に判断できるにもかかわらず自分で判断しないことである。ナッジされた決定は、事業者への依存性を前提におくので、その決定が自律した決定と同一視できるとは必ずしも言えない。

この点について論じるには、ロールズの正義論やアッカーマンの二元的デモクラシー論などのカント的な規範理論の検討が必要である。

5-2-2 今後の課題（その 2）――Trust とは？

もう 1 つの課題は、Privacy as Trust 論における Trust の概念を整理することである。英語の Trust には、信頼（社会的関係としての Trust）と信託（法制度としての Trust）と

いう二つの異なる意味がある[21]。Privacy as Trust 論においては、論者により、その Trust を異なる意味で使っている。

たとえば、Waldman [2018:108]は、トラストでプライバシー保護を図るメリットとして、（リベンジポルノなどの）サイバーハラスメントにうまく対処できると主張する。元交際相手を「信頼して」性的な情報を共有していたのに、その信頼関係が破壊されたと論じられるからであるという（Waldman [2018:113]）。しかし、サイバーハラスメントの事例を解決する場合、不法行為プライバシーで解決する手法と何が異なるのかが明確ではない。

これに対し、本稿で扱った Richards & Hartzog [2016]の議論や Balkin [2016]の議論は、信託に着目し、信託法上認められている信認義務（とくに忠実義務）の付与からプライバシーの保護を論じている。しかし、信認義務に着目した場合、情報という無体物に対して信託法上の保護をどうやって認めるのかという問題がある[22]。また、Khan & Pozen [2019]は、誰にどの程度の義務が課されるのか明確でないと Privacy as Trust 論を批判する。

この点に関連して、Richards & Hartzog [2016:458–468]は、トラストを通じて、プライバシーを活性化させることを唱え、FTC が策定した「公正な情報取扱原則（Fair Information Practices: FIPs）」の「通知及び選択」モデルを修正することを主張する。より詳細な検討が必要であろう。

いずれの課題も、与えられた紙幅では十分に論じられないものである。次の論文で検討したい。

［付記］

本研究は、2020 年度北陸大学特別助成（奨励課題研究）「信認義務に基づいた個人情報保護の理論構築：情報管理者の専門家性に着目して」による研究成果の一部である。

脱稿後、曽我部真裕・山本龍彦（2020）「【紙上対談】自己情報コントロール権をめぐって」『情報法制研究』（7）:128–140 に触れた。この対談は、曽我部[2018]および山本[2019]の対立点が当事者によって明らかにされており、わかりやすい。また、Khan & Pozen [2019]を引用して、Privacy as Trust 論の問題点を指摘する。この批判（問題点）の内容を端的に示せば、本稿の 5-2-2 で指摘した内容と同じである。この批判に対する応答は、別の論考で行いたい。

注

1 このセクションに関わる記述については、山本[2010=2017:3–7]を参照。

2 フリードの議論については、必ずしも情報化の進展を視野に入れて自己情報コントロール権説が主張されたわけではないという指摘がある（山本[2010=2017:3–7]）。

3 Balkin [2016:1187–88]によれば、配車アプリの管理者は、利用者がいつどこに行ったかを把握する「神の視点（God View）」を持っていると指摘する。

4 本文で述べたような期待を実現するために、日本において、本人の同意に代わる条件の下で、個人情報取扱事業者間で個人データのやりとりを可能にする制度が必要性であると議論された。そして、政府の「パーソナルデータの利活用に関する制度改正大綱」に基づいて、平成 27 年の個人情報保護法改正がなされた。この点については、瓜生[2015:5, 39]を参照せよ。

5 Restatement (Second) of Torts §652A(2).

6 本文で依拠したコンテスタビリティの理論にも批判があるけれども、参入を促進して各企業のシェアを小さくして寡占化を防ぐべきという議論を論駁するには十分である。この点については、奥野・鈴村[1988:195–209]を参照。

7 日本におけるこの分野の古典的著作として、野口[1974]がある。

[8] 本稿でいう「シカゴ学派」とは、Richard A. Posner、George Stigler などの 1970 年代のシカゴ大学で教えてきた法学者や経済学者のことを指す。1990 年代のシカゴ大学で教鞭をとった Cass R. Sunstein や Richard H. Thaler は、それに含まれない。

[9] 曽我部[2018:75]は、Solove [2013]の議論を根拠に、現実の個人がプライバシー権・ポリシーを熟読して同意をするという想定があまりに非現実的であるとして、自己情報コントロール権を批判する。

[10] この点を指摘した法律学の文献として、曽我部・林・栗田[2019:120]がある。

[11] これは、「人は事例をどれだけ簡単に思いつくかどうかによって、リスクが現実のものとなる可能性を評価する。関連する例を簡単に思い浮かべることができると、そうではない場合よりもはるかに強くリスクを恐れ、不安を抱くようになりやすい」というものである（Thaler & Sunstein [2009:25=2009:47]）。

[12] OECD プライバシーガイドライン（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）の初版（1980 年）・最新版（2013 年）は、OECD のサイトから入手できる。https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

[13] より堅牢な匿名化手法として、k-匿名性（k-anonymity）や差分プライバシー（differential privacy）などがある。これらについては、中川[2016:135–206]にまとめられている。

[14] リバタリアン・パターナリズムという表現は、パターナリズムを排除して「選択の自由」を認めるという、リバタリアンの立場・「シカゴ学派」の経済学に対するアンチテーゼにもなっている。Thaler [2015=2019:下巻 153]は、この表現が登場するまで、「反・反パターナリズム」という表現を用いていたことを述懐している。

[15] 連邦取引委員会（Federal Trade Commission: FTC）のウェブサイトから入手できる。https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers

[16] 山本[2010:83=2017:9]は、デザイン・コントロール論を、疑問符をつけつつも、アメリカにおける第 3 期プライバシー権論として位置づけた。

[17] 実際に、Sunstein [2013=2017:44]が OIRA 室長に就任しようとしたときに、本文で述べたような批判を現実に受けていた。

[18] Helen Nissenbaum は、TrackMeNot というブラウザ拡張機能（Firefox アドオンなど）の貢献者の一人である。その機能により、検索エンジンにランダムな検索ワードを発行するので、検索履歴が難読化されてトラッキングを防止する役割を果たしている。

[19] 実際に、Balkin [2016:1183 n.106]や Richards & Hartzog [2016:431, 457 n.101]で、Frankel [2011=2014]の議論を参照している。

[20] 山本[2019:58–59]は、Privacy as Trust 論は自己情報コントロール権と異ならないと、本文に述べたような批判と同様の議論を展開する。その根拠として、ブルース・アッカーマンの二元的デモクラシー論（通常政治と憲法政治の区分）を比喩的に用いている。

[21] オーストラリア法の文脈であるが、Ryan [2019:9–10]は、本文と同様の観点が述べられ、両者が互いに同類（cousin）であると述べるものがある。

[22] 情報は無体物とされ信託財産性がないので、日本の信託法をそのまま使って、信認義務を論じることはできない。専門家責任に着目するのは、本人の専門家に対する代理権授与行為（委任契約またはそれに類似する無名契約）から信認義務を導けると考えるからである。

参考文献

Balkin, J. M. (2016) “Information Fiduciaries and the First Amendment,” *U.C. Davis Law Review,* 49:1183–1234.

Brunton, F., & Nissenbaum, H. (2015) *Obfuscation*, The MIT Press.

Cavoukian, A. (2009, August) *Privacy by Design: The 7 Foundational Principles.* Retrieved March 31, 2020, from Information and Privacy Commissioner of Ontario: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf =(2012) 一般財団法人日本情報経済社会推進協会(訳)『プライバシー・バイ・デザイン』日経 BP 社.

Coase, R. H. (1988) *The Firm, the Market, and the Law*, University of Chicago Press. =(1992) 宮沢健一ほか(訳)『企業・市場・法』東洋経済新報社.

Frankel, T. (2011) *Fiduciary Law.* Oxford University Press. =(2014) 溜箭将之(監訳)『フィデューシャリー』弘文堂.

Fried, C. (1968) "Privacy," *Yale Law Journal,* 77:475–493.

FTC (2012, March) *Protecting Consumer Privacy in an Era of Rapid Change.* Retrieved April 12, 2020, from Federal Trade Commission: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

Gellman, R. (2019, October 7) *Fair Information Practices: A Basic History.* Retrieved March 29, 2020, from Social Science Research Network open-access repository: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020

Hoofnagle, C. J. (2016) *Federal Trade Commission Privacy Law and Policy*, Cambridge University Press. =(2018) 宮下紘ほか(訳)『アメリカプライバシー法』勁草書房.

Johnson, E. J., & Goldstein, D. G. (2004) "Defaults and Donation Decisions," *Transplantation,* 78:1713–1716.

Kahneman, D. (2011) *Thinking, Fast and Slow*, Penguin. =(2014) 村井章子(訳)『ファスト&スロー』上下巻, 早川書房［ハヤカワ文庫 NF］.

Khan, L. M., & Pozen, D. E. (2019) "A Skeptical View of Information Fiduciaries," *Harvard Law Review,* 133:497–541.

Miller, A. R. (1971) *The Assault on Privacy*, University of Michigan Press.

OECD (2013). *OECD Privacy Framework.* Retrieved March 30, 2020, from OECD: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Posner, R. A. (1981) *The Economics of Justice*, Harvard University Press. =(1991) 馬場孝一・国武輝久(訳)『正義の経済学』木鐸社.

Prosser, W. L. (1960) "Privacy," *California Law Review,* 48:383–423.

Richards, N., & Hartzog, W. (2016) "Taking Trust Seriously in Privacy Law," *Stanford Technology Law Review,* 19:431–472.

Richards, N., & Hartzog, W. (2017) "Privacy's Trust Gap," *Yale Law Journal*, 126:1180–1224.

Rubinstein, I. S., & Good, N. (2013) "Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents," *Berkeley Technology Law Journal,* 28:1333–1413.

Ryan, P. (2019) *Trust and Distrust in Digital Economies.* Routledge.

Shapiro, C., & Varian, H. R. (1999) *Information Rules*, Havard Business School Press. =(2018). 大野一(訳)『情報経済の鉄則』日経 BP 社.

Solove, D. J. (2004) *The Digital Person*, New York University Press.

Solove, D. J. (2008) "The End of Privacy?" *Scientific American*, 2008 September:79–83. =(2008) 「プライバシーに無分別な若者」『日経サイエンス』38(14):88–94.

Solove, D. J. (2008a) *Understanding Privacy*, Harvard University Press. =(2013) 大谷卓史(訳)『プライバシーの新理論』みすず書房.
Solove, D. J. (2013) "Privacy Self-Management and the Consent Dilemma," *Harvard Law Review,* 126:1880.
Stanovich, K. E., & West, R. F. (2000) "Individual Differences in Reasoning: Implications for the Rationality Debate?" *Behavioral and Brain Sciences,* 23:645–726.
Sunstein, C. R. (2013) *Simpler*, Simon & Schuster. =(2017) 田総恵子(訳)『シンプルな政府』NTT 出版.
Sunstein, C. R. (2015) *Choosing Not to Choose*, Oxford University Press. =(2017) 伊達尚美(訳)『選択しないという選択』勁草書房.
Thaler, R. H., & Sunstein, C. R. (2009) *Nudge: Improving Decisions About Health, Wealth and Happiness*, Penguin. =(2009) 遠藤真美(訳)『実践行動経済学』日経ＢＰ社.
Thaler, R. H. (2015) *Misbehaving: The Making of Behavioral Economics*, W W Norton. =(2019) 遠藤真美(訳)『行動経済学の逆襲』上下巻, 早川書房［ハヤカワ文庫 NF］.
Volokh, E. (2000) "Freedom of Speech and Information Privacy," *Stanford Law Review,* 52:1049–1124.
Waldman, A. E. (2018) *Privacy As Trust*, Cambridge University Press.
Warren, S. D., & Brandeis, L. D. (1890) "The Right to Privacy," *Harvard Law Review,* 4:193–220.
Westin, A. F. (1967) *Privacy and Freedom.* Atheneum.
瓜生和久（2015）『一問一答 平成 27 年改正個人情報保護法』商事法務.
奥野正寛・鈴村興太郎（1988）『ミクロ経済学Ⅱ』岩波書店.
斉藤邦史（2018）「信認義務としてのプライバシー保護」『情報通信学会誌』36(2):127–138.
斉藤邦史（2019）「プライバシーにおける『自律』と『信頼』」『情報通信政策研究』3(1):73–90.
曽我部真裕（2018）「自己情報コントロールは基本権か？」『憲法研究』(3):71-78.
曽我部真裕・林秀弥・栗田昌裕（2019）『情報法概説〔第 2 版〕』弘文堂.
佃貴弘（2014）「信託法理の観点による個人情報保護の可能性」『情報ネットワーク・ローレビュー』13(1):81–93.
中川裕志（2016）『プライバシー保護入門』勁草書房.
野口悠紀雄（1974）『情報の経済理論』東洋経済新報社.
山本龍彦（2010）「プライバシーの権利」『ジュリスト』(1412):80–90. =(2017)「プライバシーの権利」『プライバシーの権利を考える』信山社,3–21.
山本龍彦（2019）「自己情報コントロール権について」『憲法研究』(4):43-59.