九州大学学術情報リポジトリ
Kyushu University Institutional Repository

データポータビリティ権の可能性

河口，綾華
九州大学法学部

https://doi.org/10.15017/2800467

出版情報：学生法政論集. 14, pp.1-15, 2020-03-23. Hosei Gakkai (Institute for Law and Politics) Kyushu University
バージョン：
権利関係：

データポータビリティ権の可能性

河　口　綾　華

＜目　次＞

はじめに
第１章　情報銀行とは
第２章　プライバシーの権利
第３章　データポータビリティ権
第４章　データポータビリティ権の構成
おわりに

はじめに

今、インターネットなしの生活に戻りなさいと言われてしまったらどのような生活になるだろうか。およそ大半の人がネットと切り離せない生活になっているだろうと推測される。しかし、ネットと接することを妨げられない今、私たちのパーソナルデータや個人情報は危機にさらされているものの安全面を強化する側面もある。例えば監視カメラが設置されているからこそ安心できる社会があると同時に私たちの位置情報は特定される。家庭用電化製品にもセンサーがつけば公共の安全だけでなく、消費者の安全も守られる一方で消費者のデータがリアルタイムで収集・蓄積・分析され、それが「安全」のために公的機関に常時提供されたりすればプライバシーは全くない[1]。

そこで安全かプライバシーかという話になるかもしれないが、このご時世では両方を追い求めていくべきではないのか。つまり安全のためにプライバシーを捨て、プライバシー尊重により安全がないがしろにされるというよりも「安全かつプライバシー尊重」という風潮が大切になってきていると私は感じている。

今こそプライバシーを守るために自分の個人情報をコントロールできる仕組みが大切であり、特にデータのコントロールという面でＥＵではデータポータビリティ権が明文化された。また、膨大な個人情報を間接コントロールする機関である「情報銀行」が我が国でも認定されつつある。「情報銀行」推進のためには「データポータビリティ権」とは切り離せない論点である。第１章では情報銀行の仕組みについて、第２章では情報銀行を流通するに当たって課題点となるセキュリティ面と密接に関わるプライバシー権の変遷について、

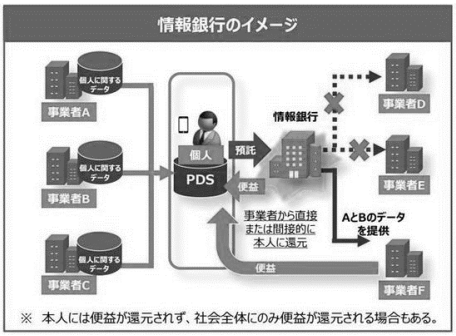
---

[1]　宍戸常寿「安全・安心とプライバシー」論ジュリ18号（2016）54頁。

第３章ではデータポータビリティ権の概要と諸外国の現状について、第４章では日本にデータポータビリティ権を導入するにあたりその根拠について以下論じていく。

第１章　情報銀行とは

情報銀行（情報利用信用銀行）とは、「個人とのデータ活用に関する契約等に基づき、ＰＤＳ（Personal Data Storeとは個人が自らパーソナルデータを事業者に与えるかどうか管理できるシステム）等のシステムを活用して個人のデータを管理するとともに、個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上、データを第三者（他の事業者）に提供する事業」[2]のことである。



パーソナルデータの利活用は個々のユーザーの行動をより深く知り、その行動から得られるニーズにいち早く気付き、そのニーズにこたえるサービスを提供できるようになるため、顧客満足度を向上できる。したがって企業にとってパーソナルデータはとても重要なものであるが、個人単体でパーソナルデータを管理し、提供することは難しい。そこで「パーソナルデータを含めた多種多様かつ大量のデータの円滑な流通を実現するためには、個人の関与の下でデータ流通・活用を進める仕組み（情報銀行等）が有効」[3]ということで「情報銀行」が発展した。多種多様かつ大量のデータを安全・安心に流通・活用できる環境を整備することで産業の競争力強化や経済活性化、国民生活の安全性や利便性も向上するとされている。

一方でセキュリティ面での懸念が残る。「データ提供先事業者による目的外の利用や再提供の抑止」[4]である。現在の指針では提供先事業者との契約で目的外利用や再提供を禁止すること等が規定されているが、情報銀行にとってお客様である提供先事業者での実効的監督は困難であるため、契約だけで禁止することには限界がある。よって、個人が自ら関与する形で流通させることができる個人データの量が限られてしまえば、情報銀行目的の利用価値が高まらなくなってしまう。

---

[2] 情報信託機能の認定スキームの在り方に関する検討会「情報信託機能の認定に係る指針ver1.0」（平成30年６月）４頁（https://www.meti.go.jp/press/2018/06/20180626002/20180626002-2.pdf）。

[3] 内閣官房IT総合戦略室「ＡＩ、ＩｏＴ時代におけるデータ活用ワーキンググループ　中間とりまとめ」（平成29年３月）５頁
（https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/dai2/siryou1.pdf）。

[4] 富士通総研「情報銀行とは何か？」
（https://www.fujitsu.com/jp/group/fri/businesstopics/data-economy/information-bank/、2019年11月14日最終閲覧）参照。

しかし、データポータビリティ権があればこのデメリットは解消されると考える。なぜなら、個人の権利を根拠にすることで提供先事業者に対して返還することを強制できる権利だからである。既にデータポータビリティ権はＧＤＰＲに明文化されているのだが、もし違反すれば13億円、または企業の場合には全会計年度の全世界年間売上高の２％のいずれか高い方といった莫大な制裁金が待ち受けているのだ。日本においても同じように個人の権利として保障することによって安全面が担保されるのではないかと思う。

第２章　プライバシーの権利

第１章では情報銀行のデメリットの解決策としてデータポータビリティ権を挙げたが、データポータビリティ権について言及する前に、個人情報を保護する権利として認められているプライバシー権について触れたい。プライバシー権は当初から個人情報保護を目的として定義されたわけではなく、社会の要請に基づいて徐々にプライバシー権の内容が変遷してきた。したがって以下の章ではプライバシー権の確立の様子、また学説が多くに分かれているので学説に関しても言及していく。

第１節　私生活秘匿権[5]

1890年にアメリカのワレンとブランダイスという二人の弁護士が共著として書いた「プライバシーへの権利」という論文から作り上げられた法律上の権利であり、当初はいわゆるイエロージャーナリズム[6]への対抗手段として考えられていた。この論文の中でのプライバシーの権利とは「一人にしておいてもらう権利（Right to be let alone)」だった。これがプライバシーの基礎とされている。日本では1960年代に「私生活秘匿権」としてプライバシー権は構成された。「宴のあと事件」からプライバシー権は広く受容され、プライバシー侵害の要件[7]は①私生活上の事実または私生活上の事実らしく受け取られるおそれのある事柄、②一般人の感受性を基準にして、当該私人の立場に立った場合に公開を欲しない事柄、③一般の人々に未だ知られていない事柄でありこのような公開によって当該私人が実際に不快、不安の念を覚えたことの三つであり、プライバシー権を「私事をみだりに公開されないという法的保障ないし権利[8]」と定義づけたのである。根拠は「個人の尊厳」に求め、「個人の尊厳は近代法の根本理念の一つであり、また日本国憲法の立脚点であるが、この理念は相互の人格が尊重され、不当な干渉から自我が保護されることによってはじめて確実なものとなるのであって、そのためには正当な理由がなく他人の私事を公開するこ

5　佐藤幸治『憲法〔第３版〕』（青林書院、2002年）53頁参照。
6　事実報道よりもあることないことを扇動的に書きたてて売り物にするジャーナリズムのこと。
7　松本昌悦「判比」『憲法判例百選Ⅰ〔第４版〕』（2000年）138頁。
8　匿名記事「判比」判時385号（1964年）12頁、29頁。

とが許されてはならない」[9]という意味のプライバシーが法的に尊重されるべきなのは言うまでもない。

第２節　自己情報コントロール権

アメリカでプライバシー権の主な関心が私生活をみだりに公開されない権利でいいのかという議論が巻き起こり[10]、同様の議論が日本でも生じた。つまり個人に関する情報のコントロールへと移行したのである。

現代で求められてきている個人情報保護に関しては伝統的なプライバシー権のみでは保障が十分ではなく、自己情報コントロール権が発達したのは個人のプライバシーを脅かすような状況が出てきたからである。ダイレクトメール業者が住民基本台帳を転写し、家族の氏名・年齢・職業・電話番号を記載した名簿を作成した宿毛市家族名簿販売事件も発生し、国民も個人情報の扱い方に関心を持つようになった。そして、プライバシー侵害として問題にされるのは(1)情報公開条例やサービス行政を旗印とした行政庁、あるいは民間調査機関をはじめとする企業による個人情報の収集とコンピュータ処理に関する「情報収集型」、(2)マスメディアによる報道、および写真誌やノンフィクション、モデル小説を通じた公表に関する「公表型」の二つである[11]。

そこで、自己情報コントロール権の提唱者である佐藤幸治教授はプライバシー権を「個人が道徳的自律の存在として、自ら善であると判断する目的を追求して、他者とコミュニケートし、自己の存在にかかわる情報を開示する範囲を選択できる権利」として定義し、人間にとって最も基本的な、愛、友情、および信頼の関係にとって不可欠の環境の充足という意味で幸福追求権の一部を構成するにふさわしいとする。ここでのプライバシー権は公権力がその意に反して接触を強要し、その人の道徳的自律の存在にかかわる情報を取得し、あるいは利用ないしは対外的に開示することが原則的に禁止される[12]。そして、その内容には自己情報の閲読・訂正・抹消請求権という意味での積極的権利が含まれる[13]。しかし、かかる請求権の具体的実現については、具体的な手法・方法を定めた法律の裏付けを必要と解される[14]。

佐藤教授は人格的自律のプライバシー権や静穏のプライバシー権は情報プライバシー権の意味に限定するべきとしている。21条２項後段、35条、38条１項、あるいは19条、21条でもカバーできないところを13条のプライバシーの権利が妥当することになるとしている。

9　匿名記事・前掲注（８）28頁。

10　山本龍彦「プライバシーの権利」ジュリ1412号（2010年）80頁。

11　棟居快行『人権論の新構成』（信山社、2008年）196頁参照。

12　佐藤幸治『日本国憲法論』（成文堂、2011年）182頁。

13　辻村みよ子・山元一編『概説　憲法コンメンタール』（信山社、2018年）87頁〔小泉良幸〕。

14　佐藤幸治『現代国家と人権』（有斐閣、2018年）439頁。

しかし最初の自己情報コントロール権説の根底はアメリカのフリード説を援用した様に見受けられるため、高度情報化社会やデータ・バンク社会を視野に入れたものではなく、人間的な愛、友情、信頼の関係の選択や形成に関心を向けたものであり、ここでの「情報コントロール」とは対人対面関係を前提としており「どこまで見せるか」の決定であって急速に成長していたコンピュータに対応するものではなかったことが分かる[15]。ただ、その後佐藤教授は「コンピュータ化は加速度的に進み、グローバル化とも結びついて、状況が大きくかつ急速に変わってきていることを実感させられました。」と述べており、前記のように現代の社会にも対応している説とはなっている。

以上から、同説は情報収集型の文脈に発想の基盤を置きながら、「情報」概念の包括性と「個人の尊厳」の一般性の故に、公表型をもカバーするものとなっている[16]。

また、佐藤教授はプライバシー情報をプライバシー固有情報とプライバシー外延情報の二つに分け、プライバシー固有情報は「その人の道徳的自律の存在にかかわる情報[17]」であり、プライバシー外延情報は「個人の道徳的自律の存在に直接かかわらない外的事項に関する個別的情報[18]」である。固有情報はプライバシー権の射程に入るが、外延情報は直ちに入らないとされている。が、外延情報も悪用されまたは集積されるとき、個人の道徳的自律の存在に影響を及ぼすものとしてプライバシーの権利の侵害の問題が生ずるとしている[19]。

第３節　超デジタル社会に対応したプライバシー権

データベースが社会全体に及ぼす影響の重大性から、その構造自体をコントロールするという客観的側面を強調し、システム構築を目的とした個人情報の収集・保存によってそれがセンシティブ情報であるか単純情報であるかに関わらず侵害されるようになる。したがって自己情報コントロール権との連続性・関連性を維持しつつも、実質的はシステム・コントロールないし構造要求としての性格を強く有するようになると言ってよい[20]。

ただ、具体的な侵害が発生していない段階で保護する法益とは何かという問題や専門性の高いシステムを裁判官が適切な判断ができるのかというような課題は残る[21]。

15　山本・前掲注（10）81-82頁。
16　棟居・前掲注（11）197頁参照。
17　佐藤・前掲注（５）454頁。
18　佐藤・前掲注（５）455頁。
19　佐藤・前掲注（５）455頁参照。
20　山本・前掲注（10）84頁。
21　山本・前掲注（10）87-88頁参照。

第４節　学説の状況

自己情報コントロール権説を精力的に批判してきた一人として阪本教授が挙げられる。彼の考えるプライバシー権は不法行為上の異形の法制度であり、国家の立場を不法行為上として限定的に解されているプライバシー権と対立利益としての表現の自由の「調整者」として考えている。しかし、国家が「侵害者」となる可能性があることも注意しなければならず、プライバシーの射程が狭すぎる。私的部門が個人情報を収集・利用することについて、“自己情報コントロール権としてのプライバシー権の侵害だ”と簡単にいうことは、避ける必要があり、侵害行為の成立要件を厳密に考えないまま、私的部門の活動を制限してよいと主張することは、一方だけの法益に荷担するもので、適切な憲法解釈ではない。

要するに表現の自由と対立するプライバシーとしてのみ考えている。つまり法的利益は「私生活上の事実をみだりに公表されない法的利益」であり、判例・学説で私たちが外部社会にオープンにしている個人情報もプライバシーとしていることに反対している。

また、「評価の対象となることのない生活状況または人間関係に関する知識・情報」のコントロール権説を主張している[22]。したがって情報の収集ないし開示、それ自体でなく、それを社会的評価にさらされうることにプライバシー侵害の本質を見出すため「公表型」の文脈にたっている[23]。ただ、なぜ「評価」が問題となるかは明らかではないとも言える。

また、曽我部教授も自己情報コントロール権説に対して懐疑的な見解を持っている[24]。自己情報のコントロール可能性を重視する背景には、自己情報の取扱いを本人が決定するという自己決定の観念があり、実定法上でどの程度自己決定が貫徹されているか検討すると、個人情報保護法では個人情報の取得のために同意は必須とされておらず（17条１項）、要配慮個人情報については原則として同意を要するとされるが、例外に広範に認められている（17条２項）。また、第三者提供を除く個人情報の取扱いについても、特定された利用目的の範囲内であれば、本人の同意は不要である（16条１項）。第三者提供については事前の同意を要するが、例外が広く認められている（23条１項）。以上から個人情報保護法において同意が果たす役割は限定的であることが分かる。したがって実定法上では自己決定が貫徹されておらず、それ自体が特別重要ではない。個人情報の社会通念上不当な取扱い及びそれに起因する不利益を防止することが目的であり、自己決定・同意の要素は基本的には手段にすぎない。手段であるならば同意以外の方法で個人情報の不当な取扱いを防止できるのであれば同意にこだわる必要性はない。

22　棟居・前掲注（11）173頁。

23　棟居・前掲注（11）197頁。

24　曽我部真裕「自己情報コントロール権は基本権か？」情報法制研究会第８回シンポジウム（2019年２月17日）（https://www.dekyo.or.jp/kenkyukai/data/8th/190217_doc02.pdf）。

第５節　これからのプライバシー権

プライバシー権理解は私人間にも通用し、その結果個人情報保護制を、自己情報コントロール権を具体化したものとして理解してきた[25]。プライバシー権を自己情報コントロール権として捉える考え方が通説化しているが、現在のビッグデータ駆動型社会だとデータ一つ一つを自分自身でコントロールすることは不可能であり、私たちも望んではいない。例えばプライバシーポリシーを読まずにすぐに同意ボタンを押すことが多々ある。同意（選択）を重視する自己情報コントロール権はかえって事業者側の免罪符となり、自己情報コントロール権を批判的に捉える学説は上記の通りである。

しかし、ビッグデータ駆動型社会だからこそ、つまりネットワークと個人が切り離せない社会だからこそ、個人の主体性を維持するには自己情報コントロール権が必要となるのではないだろうか。自分でコントロールする直接コントロール形式よりも、信頼できる誰かに自分の情報のコントロール頼むような間接コントロール形式がこれから重要となり、それこそが前記のように「情報銀行」の役割である。

第３章　データポータビリティ権

いわゆる今日のプライバシー侵害問題としてあげられるうちの「情報収集型」に対する権利として新たに浮上してきたものが「データポータビリティ権」である。昨今では情報がサービスの基盤となり、データ主体（本人）が情報の移転をスムーズに行うことができることが要請され、自分に関する情報をより積極的にコントロールする革新的な権利と言われている[26]。

第１節　データポータビリティ権の定義

ヨーロッパではデータ本来の持ち主は個人であり、個人がデータとその開示先をコントロールしてデータを流通させる個人起点のデータ流通（ＶＲＭ型）という考えをとり、ＶＲＭ型では顧客である個人が主体である。「買い手が売り手との関係性を管理する」というものであり、顧客が「自分のどういう情報を、どの企業に渡すか」をコントロールすることが可能となり、企業側はその受け取った情報から「何を提案してほしいと思っているか？」を考えて提案してくるという流れを実現している[27]。つまり経済合理性・効率性とプライバシーを比べた際にプライバシーの方に重点を置いている。これをまとめたものがＧＤＰＲである。

---

[25] 曽我部・前掲注（24）。

[26] 小向太郎「データポータビリティ」ジュリ1521号（2018年）26頁。

[27] 田中耕比古「VRM（Vendor Relationship Management）：果たしてＣＲＭの“次”なのか？」2015年５月27日（https://www.gixo.jp/blog/4644/、2019年11月14日最終閲覧）。

一般データ保護規則（ＧＤＰＲ）とはパーソナルデータに関する個人の基本的権利を保護するため、パーソナルデータの保護に関するＥＵ域内での統一的なルールを制定するものであり、2018年５月全面施行された。

ＧＤＰＲは「自然人は自らのパーソナルデータのコントロールを有するべきである」（前文７項）としており、自己情報コントロール権説の具体化となっている。

そして新たに明文化されたデータポータビリティの権利はＧＤＰＲ20条に規定されている。内容は以下の通りである。

第20条　データポータビリティの権利（Article 20 Right to data portability）[28]

１．データ主体は、以下の場合においては、自己が管理者に対して提供した自己と関係する個人データを、構造化され、一般的に利用され機械可読性のある形式で受け取る権利をもち、また、その個人データの提供を受けた管理者から妨げられることなく、別の管理者に対し、それらの個人データを移行する権利を有する。

(a)その取扱いが第６条第１項(a)若しくは第９条第２項(a)による同意、又は、第６条第１項(b)による契約に基づくものであり、かつ、

(b)その取扱いが自動化された手段によって行われる場合。

２．データ主体は、第１項により自己のデータポータビリティの権利を行使する際、技術的に実行可能な場合、ある管理者から別の管理者へと直接に個人データを移行させる権利を有する。

要するに、データ管理者から本人が自らのデータを扱いやすい電子的な形式で取り戻し、それを他のデータ管理者に移転する権利とあるデータ管理者から別のデータ管理者に直接移転する権利の二つの権利から構成される[29]。つまりデータポータビリティ権が行使されれば、個人が持ち運びできるかたちでそのデータを当人に「お返し」しなければならないのである。

データポータビリティ権の意義・目的は①個人にとっては、パーソナルデータをコントロールするという基本的権利を強化するもの、②新興企業や中小企業にとってはデジタル・ジャイアンツに支配されたデータ市場にアクセスし、より多くの消費者を得ることを可能とするものとされている[30]。

---

[28] 個人情報後委員会「一般データ保護規則（ＧＤＰＲ）の条文」25頁（https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf）。

[29] 生貝直人「EUの状況：データポータビリティの権利を中心に」（2016年11月11日）３頁（https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/detakatsuyo_wg_dai4/siryou1.pdf）。

[30] 経済産業省「データポータビリティに関する調査・検討について」（2018年７月）５頁（https://www.kantei.go.jp/jp/singi/it2/detakatuyo_wg/dai1/siryou4-2.pdf）。

それではデータポータビリティ権の対象となるデータとはどのようなものか。氏名や、住所、メールアドレス等のデータ主体が主体的にかつ認識して提供したデータである「提供データ」や検索履歴や交通データ等のサービス又は機器を利用することでデータ主体が提供したデータである「観察データ」は対象となるが、健康状態の評価や信用評価等の提供データや観察データを元にデータ管理者が作成したデータである「推定・派生データ」は対象とならない[31]。それゆえデータ主体が提供すれば権利の範疇内であるが、データ主体が自主的に提供していないデータは範囲外ということが分かる。

つまり、ＧＤＰＲはプラットフォームからの個人の離脱可能性を保障することによって、個人情報を用い＜プラットフォームによる統治＞に限界を与えようとする試みとなっているのである[32]。ただしデータポータビリティの制度はあくまで個人データに関するルールを定めたものであり、競争に関するものではないことには注意する必要がある[33]。

ＧＤＰＲ20条の立法過程において浮上した肯定的見解について言及するとＥＵ市民の６割以上が自らの個人データへのコントロール能力不足を感じており、特にクラウドサービス等におけるデータポータビリティの必要性を認識していた[34]。

一方否定的見解としては、人的資源管理システムや顧客管理システムに登録された情報は企業にとって大きな商業的価値を持つため、これらをも全体的に対象にすることは競争上の問題を惹起するという意見や、広範なデータポータビリティの導入は、競争政策と矛盾すると共に、スタートアップを含む中小企業に過度な負担を押し付け、消費者利益をも低下させることになりかねないとの意見が出ていた[35]。

明文化された現在でもなお、データポータビリティの権利の具体化として「一般的に用いられる機械可読なフォーマット」とはどのようなフォーマットか等の論点は残る。

第２節　我が国における現状

プロフィールや位置情報、購買履歴、検索履歴等の個人情報が企業に収集されている中でその一部は第三者に提供されることが多々ある。例えば委託先や子会社等に提供する場合が多い。個人情報保護法23条では個人データの第三者提供において原則本人の同意を必要としているため、企業は消費者の同意を取得しているものの消費者本人の意識が十分ではない場合が多々ある。消費者はまず自分の情報を何に使われているか理解しておらず、第三者提供に同意した覚えがない消費者も多い。また企業側も消費者が十分に理解して同

31　株式会社の村総合研究所「ＥＵにおけるＧＤＰＲ（一般データ保護規則）の運用及び対応に関する動向調査　調査報告書」(2019年３月29日)(https://www.ppc.go.jp/files/pdf/0912_shiryou2-2.pdf)。

32　生貝直人「通信分野の個人情報保護と利活用」ジュリ1534号（2019年）26頁、29-30頁。

33　小向・前掲注（26）31頁。

34　生貝・前掲注（29）７頁参照。

35　生貝・前掲注（29）７頁参照。

意をしているか不安でもある。前述した通り、同意を重要視している理由は自己情報コントロール権説が通説化しているからだと考えられているが、事実すべてに「同意」が必要とされている訳ではない。

このように情報の第三者提供には問題があるものの現在日本では金融、電力、医療分野別にデータポータビリティを推進している。つまり分野ごとに環境を整備している。特に医療分野（医療を受ける際の診断・治療等の情報）におけるデータポータビリティは７割以上が必要と感じており、他分野においても過半数が必要性を感じている[36]。特にこの分野では情報の共有を求められているからである。

電力・金融分野では消費者が機械可読な状態で情報を取り出す「開示」は一部実現しているものの、消費者個人の意思で移転させる「移転」はまだ未対応である。

医療分野では「開示」は一部紙で開示しているもののスマートフォンのカメラで紙の健診結果を読み取り、スマートフォンに取り込むサービスが提供されていてほぼ実現しており、「移転」も医療情報においては一部実現している。

まだ未対応なところが多々あるものの着実にデータポータビリティの土俵づくりが進んでおり、今後ますますデータポータビリティ権の確立が必要となっていることが分かる。

第３節　海外における現状

１．アメリカ

ネットサービスの基盤を抑えるプラットフォーマーであるＧＡＦＡがデータを支配し顧客の囲い込みを進めている。事業者間データ流通（ＣＲＭ型）が発達しており、米国主導のデータ経済圏の中でＧＡＦＡは巨大化していた。伝統的に自主責任・自己責任を基本としていたが、2012年には消費者プライバシー権利章典が制定された[37]。ＧＡＦＡからの反発もあったが、データ主権の保護を強める方向に傾きつつもある。実際に「消費者は、企業が自分からどのような個人データを収集し、どのようにそれを利用するかについてコントロールを行使する権利を有する」[38]とあり、自己情報コントロール権の現れのような考えに基づく。

オバマ政権はデータポータビリティ拡大を目指したMy Dataイニシアチブを発表した。つまり自らの個人情報を安全、適時、電子的にやり取りする技術的な枠組みを連邦政府主導で進めていく考えである。具体的にはBlue Button（医療データ）がある。

36　経済産業省・前掲注（30）11頁。

37　小川幸祐「データ保護主義の中のモビリティ・プラットフォーム戦略　ＧＡＦＡをめぐるトリレンマからの示唆」知的資産創造2019年４月号20頁、24頁（2019年）。

38　経済産業省商務情報政策局「パーソナルデータに関する海外動向」（2012年11月）６頁（https://www.meti.go.jp/committee/kenkyukai/shoujo/it_yugo_forum_data_wg2/pdf/001_04_00.pdf）。

消費者（退役軍人・Medicare受給者・兵役者）が「Blue Button」をクリックすると自分の個人データ（ＰＨＲ）を医療機関、薬局、研究所からダウンロードできる。例えばかかりつけ医院や過去の受診日、処方薬品名や予防接種、アレルギー歴等様々なデータが対象となる。

ＨＩＰＡＡ（Health Insurance Portability and Accountability Act、医療保険の携行性と責任に関する法律）の「幾つかの例外を除き、プライバシールールがカバーする医療保険と医療機関によって保有される自己の医療記録および請求記録を調査し、レビューし、コピーを受領する権利を個人に与えている」[39]がこれの法的根拠となっている。

アメリカ国民の約半数が利用という大成功を収めたものの、トランプ政権ではBlue Buttonを所管する機関に予算の大幅削減を提案したため、医療ＩＴ政策が後退する懸念が広まっている。

２．ニュージーランド[40]

ＥＵでのＧＤＰＲの可決を受け、プライバシー委員会委員長がデータポータビリティ権創設を提案した。同国民に同権利の導入必要性についてアンケート調査を実施したところ、回答者の56％がオンラインサービス間での個人データ移転を「極めて重要」「重要」と回答した。これから導入すべきかの議論を始めようとしている。

第４章　データポータビリティ権の構成

以上、検討してきたようにデータポータビリティの環境は整いつつあり、間接コントロールを実行するためにはデータポータビリティ権抜きの話では進めることができない。前述した様に直接コントロールするには現在は情報が溢れすぎているため情報銀行のような媒介的機関の需要が高まってくるが、そのデメリットを解消するためにはデータポータビリティ権を求められるからである。もし我が国でも導入するとなればどうするべきか。導入するとしたときに生じる論点について触れていく。

第１節　データポータビリティ権の位置づけ

では一体、データポータビリティ権をどのように位置づけるべきか。同権利を導入した場合に発生する主な効果はサービス間の移行を円滑にするという独占禁止のような競争政策的側面と個人データに対するデータ主体のコントロールの強化という側面[41]が挙げられ

39　経済産業省・前掲注（30）９頁。

40　生貝・前掲注（29）12頁。

41　生貝直人「データポータビリティとＡＩネットワーク社会」（2018年12月10日）17頁（http://www.soumu.go.jp/main_content/000589118.pdf）。

る。どちらの効果の方を重要視しているかという点で位置づけが異なり、根拠となる条文も変わってくる。第１項では既出のデータポータビリティ権の根拠について言及し、第２項と第３項で私見を述べていきたい。

第１項　競争法を根拠にするデータポータビリティ権[42]

個人の権利としてというよりもデータ寡占の防止という観点からデータポータビリティ権を導く考えである。元々ＥＵでプラットフォーマーに対抗するためにデータ保護に対して関心が高まってきたように感じる。ＥＵには強いＩＴプラットフォーマーが存在せず、自国のデジタル産業が弱いという背景があるため、こうした中で他国のプラットフォーマーの参入を受け入れることは国民のプライバシー保護が危うくなるばかりか、自国の既存産業に破壊的な構造変化をもたらしかねないのだ。データポータビリティ権を必要とされてきた背景を考慮すると競争法を根拠にする考え方が最も筋に合うかもしれない。

したがってデータポータビリティの本質は公正な競争であり、プラットフォームへの対抗手段としての権利であり、基本権ではないため法律によって初めて発生する。

第２項　自己情報コントロール権から導くデータポータビリティ権

これは「個人データに対するデータ主体のコントロールの強化という側面」を重要視した考えであり、データポータビリティ権を基本権として捉える。個人が各々データポータビリティ権を持っており、自由に自分のデータを移転できるようになり、自己情報コントロール権の具体的な現れとして位置付ける。基本権であるため、法律や契約によって初めて発生するものではない。しかし、前述の通り請求権の具体的実現として具体的な法律の裏付けは必要となる。

そこで既存法律の中で最も具体的な法律に近い個人情報保護法を改正し、個人データ全般のポータビリティを認めるか、新たなデータポータビリティ権のための法律を作成するか、もしくは米国のBlue Buttonのように代替性の低い重要データを保有する特定分野の適用かとするかについては日本におけるデータポータビリティの推進具合によって決めるべきだと思うが、さらにデータで溢れていく時代になっていくことを視野に入れると個人データ全般を対象にしても良いように感じる。

自己情報コントロール権説ではプライバシー固有情報とプライバシー外延情報に分けていたが、どちらもデータ上で集積されるとなるとプライバシー外延情報でさえも危険な情報になってしまうため、データの場合は情報の性質で分類せずに全般を射程範囲内とするべきだと考える。

---

[42] 山本龍彦「ＡＩ時代のプライバシーとデータ保護―プロファイリングを中心に―」（2019年２月27日）７頁（http://www.soumu.go.jp/main_content/000604968.pdf）。

第３項　契約上の権利としてのデータポータビリティ権

第１項の競争法を根拠とする考え方や第２項の自己情報コントロール権を根拠にする考え方とは違い、私人間の申込みと承諾により発生する契約関係を根拠にする考えである。上記の考え方と比べると最も簡単に当該権利を発生することができる。この考え方では契約を解除されたら初めから契約はなかったものとみなされるため勿論同権利は消滅し、解除の効果として原状回復義務がある。しかし原状回復も履行不能であった場合は目的物の返還に代わる価格返還義務となる。例えばデータを返してほしいと消費者が要求しても企業側がすでにデータを更に他の会社に移転してしまっていた場合、原状回復は履行不能となる。したがって当該データに相当する価格、更に企業側に対して債務不履行により生ずる損害賠償金を含めた価格を返還してもらうべきである。

第４項　私見

第２項の考え方は個人の権利となるが、第１項の考え方であれば個人だけでなく事業者にもデータポータビリティ権が認められるべきである。なぜなら事業者（プラットフォーム利用者）がプラットフォームとの取引的記録等を運搬できることで、ロックインが防止でき、データ市場においてより行き渡るからである[43]。しかし、ＧＤＰＲ20条での権利者はあくまで「データ主体」、つまり特定されたまたは特定可能な自然人であるため、ここでは事業者は権利者ではなくなる。なぜ個人がこの権利を持たされるのかという新たな問題が生じ、ＧＤＰＲとの整合性も問題となる。

また第３項では価格返還義務となることで大切な個人情報をお金で賠償すれば済むという風潮となる。これからデータが重宝される時代に、お金で解決できるのか甚だ疑問ではある。以上のことから自己情報コントロール権説から導くべきであると私は考える。

第２節　憲法改正とプライバシー権

今まで見てきたようにプライバシーが基本的人権であるとは国家権力の限界を定め、その限界を守るよう、個人が自らのために国家に要求する権利であり、同時に国家は他人の侵害から個人のプライバシーを守る責務も負うことが分かる。安全を名目としてプライバシーを安易に侵害するのではなく、両者の最適な実現を図るべきである。ますます注目される権利としてプライバシー権の将来はどうなるのか。データポータビリティ権を自己情報コントロール権から導くべきだと考える私にとってプライバシー権の行く末は重要であり、自己情報コントロール権は通説化しているものの批判もある。最後にプライバシー権のこれからについて言及したい。

憲法改正し、プライバシー権を明文化すべきと主張する立場は戦後当時では想定されて

43　山本・前掲注（42）７頁。

いないような権利が多々あり、そのうちの一つがプライバシー権であるため、幸福追求権から導くのではなく、時代に対応するべきであると考える。

しかし、明文化するとすれば通信の秘密や35条との整合性を見直すべきであり、プライバシー権が制限されるときはどのような場合かということも検討すべきとなっていく。

勿論、明文化せずに現状維持という立場もある。第 2 章のようにプライバシーの権利の概念とは非常に流動的なものであるため13条から導き、解釈上で認めていくという考えである。今まで解釈上で成り立ってきたため、改正するべきという積極的意義までは見つけられないと主張する。

以上の様に新しくプライバシー権から派生する権利が必要となってきた際に全て13条の幸福追求権を根拠にすることができる状態となっているが、次第に人権のインフレ化を招きかねないため、判例上でも認められているプライバシー権は明文化してもいいようにも思える。しかし権利の性質上、定義が流動しやすいため今明文化したとしても数十年後には更なる技術の発展により新しくプライバシーとして守る範囲が広がってくるかもしれない。新しい守備範囲を解釈上で導くことができなければ、また改正する必要がでてきてしまう。今後のプライバシー権の変遷の動向を見守っていくほかない。

おわりに

実務上でも自己情報コントロール権という考えは要請されており、反対意見はあるもののこれからの時代に備えてそろそろ正面から認めてもいいように思う。今回検討してきたデータポータビリティ権や情報銀行は自己情報コントロール権を前提にしたものと解されており、認めない限り実務の方が先行し、プライバシーの権利が形骸化してしまうかもしれない。今世界の企業はデータを保有してはいるが、それを活用する方法を見いだせていないのが現状である。保有したデータをいかに活用していくか日本も検討していかなければならない重要事項である。その上でデータを自由に移転しやすい基盤を事前に作っておくべきではないのか。そしてそのような状況でプライバシーについての定義もまた変化し、プライバシー保護の要請は高まるであろう。更なる経済発展とプライバシー保護の両方を勝ち取っていけるか否かは今後の日本の法整備の状況によって変わってくるのではないだろうか。

参考条文

ＧＤＰＲ

第６条　取扱いの適法性（Article 6 Lawfulness pf processing）[44]

１．取扱いは、以下の少なくとも一つが適用される場合においてのみ、その範囲内で、適法である。:

(a)　データ主体が、一つ又は複数の特定の目的のための自己の個人データの取扱いに関し、同意を与えた場合。

(b)　データ主体が契約当事者となっている契約の履行のために取扱いが必要となる場合、又は、契約締結の前に、データ主体の要求に際して手段を講ずるために取扱いが必要となる場合

第９条　特別な種類の個人データの取扱い（Article 9 Processing of special categories of personal data）[45]

１．人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータの取扱いは、禁止される。

２．第１項は、以下のいずれかの場合には適用されない。

(a)　データ主体が、一つ又は複数の特定された目的のためのその個人データの取扱いに関し、明確な同意を与えた場合。ただし、ＥＵ法又は加盟国の国内法が第１項に定める禁止をデータ主体が解除できないことを定めている場合を除く。

44　個人情報保護委員会・前掲注（28）8 頁。

45　個人情報保護委員会・前掲注（28）12頁。