The 21st Century Public Policy Institute

21世紀政策研究所　研究プロジェクト

データに関する権利のあり方

報 告 書

2023年3月

21世紀政策研究所

はしがき

デジタル社会は、データ駆動型社会でもある。サイバー空間とフィジカル空間が高度に融合する中で、多くの経済的・社会的活動がデータと結びつくことでより効率的なものとなり、またこれまで以上の便益や価値を生むことが期待される。その反面で、データによって個人や企業、さらには社会全体が把握され分析される結果として、差別や格差が生まれたり、社会的・国家的利益が損なわれるおそれが高まったりもしている。リスクを適切にコントロールしつつ、データの利活用を促進することを通じて、健全なデジタル社会を形成することは、いまや喫緊の課題といってよいであろう。

そのようなデータ利活用のためのルールを、適正で実効性あるものとするためには、国家の垣根、民間と政府の垣根、事業分野の垣根、企業と市民・消費者の垣根、そして実務と研究の垣根等の諸々の境を超えて、それぞれの知見や経験を持ち寄り、共通の認識と議論の基盤を意識的に培っていくことが求められる。

「データに関する権利のあり方の整理プロジェクト」は、データの利活用促進及び米 EU など各国との連携に向けた議論を日本が積極的に主導するため、データ提供者・利用者の権利に係る国内外の法制度や議論の動向等を把握・分析し、データに関する権利のあるべき姿について提言することを目的として、2022 年 4 月に設置された。

同プロジェクトは、データ利活用に先進的に取り組む企業における責任者のほか、デジタル法務を専門とする法律家、そして法学・経済学・情報政策の研究者の合計 9 名により構成され、同年 12 月に至るまで合計 8 回の会合を開催した。時にはゲストスピーカーの貴重なインプットもいただきながら国内の政府や企業・団体の動向だけでなく、海外や国際機関における議論の状況についても最新の知見を共有した上で、データに関する権利のあり方について各研究委員の立場から多角的に論じたのが、本報告書である。

データ利活用のためのルールを設計・運用していくためには、その構成要素の一つとして、誰にいつ、どのような内容のデータに関する権利が認められ、それがいかにして行使・実現されるのか、またその権利の名宛人として誰がどのような義務を負うのかという議論が欠かせない。そのような議論を通じて、「総論賛成、各論反対」にとどまらず、信頼性あるデータ流通（Data Free Flow with Trust）を具体的な場面に応じた適正で実効性ある規律に落とし込み、また、適時に見直しをしていくことが可能になるものと思われる。そのような議論に向けて、本プロジェクトとその成果である本報告書が広く活用されることを

期待したい。

データ利活用促進の必要性を日本社会に否応なしに意識させた、新型コロナウイルス感染症になお一定の警戒を要する時期に、本プロジェクトは実施された。この場を借りて、困難な情勢の中で本プロジェクトに参加いただいた研究委員、ゲストスピーカー、オブザーバ各位に加えて、研究主幹という身に余る大役を持て余し気味であった私を終始サポートしていただいた経団連 21 世紀政策研究所のみなさんに、心より御礼を申し上げたい。

2023 年 3 月

研究主幹　　宍戸　常寿

目　　次

※本報告書は、21 世紀政策研究所の研究成果であり、経団連の見解を示すものではない。

※はしがき及び各章の記載は執筆者個人の見解に基づくものであり、必ずしも執筆者が所属する組織及び団体の公式見解を示すものではない。

研究委員一覧

研究主幹

宍　戸　常　寿	東京大学大学院法学政治学研究科教授

委　　員（順不同）

高　口　鉄　平	静岡大学学術院情報学領域教授
酒　井　麻千子	東京大学大学院情報学環准教授
生　貝　直　人	一橋大学大学院法学研究科教授
水　町　雅　子	宮内・水町 IT 法律事務所弁護士
望　月　健　太	法律事務所 LAB-01　ニューヨーク州弁護士
藤　田　和　也	アステラス製薬(株)渉外部渉外グループ課長
長谷川　正　憲	キヤノン(株)知的財産法務本部知的財産渉外第三部長
小　柳　　輝	Z ホールディングス(株)GDPO 部長

第１章　データに関する権利のあり方についての整理
―序論的考察

東京大学大学院法学政治学研究科教授

宍戸　常寿

１．はじめに

デジタル社会においては、サイバー空間とフィジカル空間の融合が進展する結果として、①あらゆる情報がデータ化され分析可能となる、②生成されるデータの量に対して、利用者の認知や注意力の限界があらわになる、③データがよりパーソナライズ化される、④データの収集・拡散が加速する、⑤データが流通する「アーキテクチャ」を通じてプラットフォーム事業者によるデータの管理が強まるなどの点が、その特徴として指摘されてきた。デジタル社会が、データ駆動型社会といわれるゆえんである。

このような中で、データの利活用に伴う様々な主体の利益を保護するためにも、また、データの利活用を促進するためにも、データに関する権利のあるべき姿を考えるべきであるといわれてきた。もはや財やサービスと並ぶ資源となったデータについて、適正な社会的ルールが設定されなければ、データの利活用から生まれる便益とコストを帰属・配分していくこともできず、安心してデータを利活用することもかなわないであろう。その点で、社会的ルールの基礎的な構成要素である「権利」という観点からデータの利活用を考えていくことは必要であろう。

他方、「権利」は多義的な概念であるとともに、デジタル化以前の社会を適正に運営するために鍛えられてきた道具でもある。例えば、所有権は代表的な権利の一つであるが、有体物をその対象としている。その所有権のイメージで「データの権利」を語る場合は、他の権利をイメージしながら「データの権利」を語る場合とは当然にその意味合いが異なってくるし、有体物の特性に即した過剰な効果をデータについても生じさせてしまうことになる。

だからといって直ちに所有権のイメージで「データの権利」を語ってはいけないということでは、もちろんない。有体物について所有権という形で設定されてきたルールを、データについても妥当させるべき場面では、それが適切であろう。しかし逆に、所有権のイメージのままで「データの権利」に固執すると、かえってデータの特性、ひいては上記のよう

なデジタル社会の特徴にはそぐわない場面も出てくるはずであり、それが翻ってデータの利活用や主体の利益保護を阻害する結果となることも考えられるのである。

権利は、適正な社会的ルールを設定・運用するための道具となる概念である。適正なデータ利活用や主体の利益保護のルールはいかにあるべきかを議論することが大事であって、そのために、具体的にどのような権利のイメージを用いるのが有用かということを問題にするべきであろう。

本論文では、このような観点から、データに関する権利について、若干の概念整理を行うことにしたい。

２.「権利」の概念

（１）権利の基本的な用法とその多義性

「権利」は、日常用語としても用いられるし、道徳や倫理における基本的な概念でもあるが、ここでは、適正な社会的ルールの検討という観点から、法的な権利の概念について整理するところから始めたい。

一般に、法的な権利の基本的な用法としては、「自由」（ある人が他人に対して義務を負っていない場合）、「請求権」（ある人に対して他人が義務を負っており、その他人に義務の履行を求めることができる場合）、「権能」（ある人が自分や他人の法的地位を自分の意思で変更できる場合）、「免除」（ある人が他人によって自分の法的地位が変更されない場合）というように分類できるといわれてきた。実際の具体的な権利は、この４つの用法すべてを包含している場合もあるし、どれか一つの場合もある。

このように基本的な用法一つ取ってみても既に権利という概念は多義的であることがわかるが、さらに話を進めるために、日本で現に妥当している実定法秩序における権利という概念について検討してみることにしたい。

（２）主観的権利の前提としての客観法

社会を構成する主体と主体の間には、家族、友人、取引、職場など、多様な生活関係が存在する。この生活関係は、道徳や宗教、慣習など、様々な社会的ルールによって規律されているが、そのルールが法規範である場合には、この生活関係は法関係と呼ばれる。法規範にも様々な存在形態があるが、国家の定める法律以下の法令の規定によって法規範が表現されることが現在では多いので、法関係は「法律関係」と呼ばれることも多い。

例えば、殺人罪について定める刑法の規定は、殺人を犯した者に刑罰を科すというだけでなく、およそ「人を殺してはならない」という法規範を含んでいる。このように人に何らかの義務づけを行う規範は、客観法といわれる。このように「人を殺してはならない」という客観法があれば、「自分には他人に殺されない権利があるのだ」といおうと思えばできないこともないが、法の世界では、そのような意味で「権利」という概念を用いないことが多い。

（３）主観的権利―利益と意思

法の世界で「権利」（主観的権利）という場合には、客観法が存在していることを前提に、それを発動する意思の力が特定の主体に認められている場合をいう。その代表例として、売買契約の場面を考えてみよう。売主と買主の間に「買主は売主に代金を支払え」という内容の売買契約が締結されると、売主と買主の取引関係は、法的に見れば、買主は売主に代金を支払う義務を負い、売主は買主に代金の支払いを求める権利を有するという関係が成立することになる。これは、買主に対して、「買主は売主に代金を支払え」という客観法を遵守して行動するよう求める法的な力が、売主に発生したということである。

このように、自分の利益のために、客観法を遵守して作為（～せよ）または不作為（～するな）を求める意思の力が法的に認められている場合、言い換えると「利益」と「意思」がともに備わっている場合が、日本の実定法秩序で権利という概念が用いられる典型的な場面といえる。

（４）様々な権利―物権・債権・人格権

このように、主観的権利は客観法を前提としているため、その客観法の内容によって、例えばどのような生活関係を対象としているかによって、分類することができる。本稿の冒頭に挙げた所有権は、所有者が物（動産・不動産）を直接かつ排他的に支配し、使用・収益・処分する権利である。その結果、所有者は、例えば所有物を盗んだ者に対して、所有権に基づいて返還を求めることができる。所有権のような、人と有体物の関係に着目した権利を物権という。

これに対して債権は、ある人に対して作為や不作為を要求する権利であり、（３）で述べた権利の概念が用いられる典型的な場面に当たる。上の例でいえば、代金の支払いを求める権利がこれに当たる。

物権と債権は、取引関係、したがって経済秩序にとって基礎的なルールの体系である民法の体系を構成しているが、もう一つ、データに関わる権利を考える上で重要な体系を成す権利として、人格権がある。これは、個人の人格的な価値や利益それ自体を内容とする権利である。伝統的には生命・身体や名誉、現在ではプライバシー、肖像、氏名、さらにはパブリシティも、最高裁判所の判例によって、人格権ないし人格的利益として法的な保護を受けることが認められるようになっている。人格権は物権と同じく排他的な権利であり、それを侵害する者に対して妨害の排除や差止めを請求できる。

（５）権利と裁判

権利の内容である利益が円滑に実現された場合、上の例であれば買主が売主に代金を支払った場合には、権利や法の問題を深刻に考える必要はないが、売主に買主が代金を支払わなかった場合には、まずは客観法に違反する（違法）状態が生じる。その場合に、売主が権利を実現したい場合には、国家が用意している裁判制度を利用して、買主を被告として、代金の支払いを請求する訴えを提起するということになる。

このように、実定法上の権利は、最終的には、国家の用意する裁判手続を通じて実現されることが想定されている。

（６）小括

このように、（主観的）権利という概念は、主体と主体の関係を規律する客観法の存在を前提に、意思と利益を要素として、裁判制度での実現と結びつけてイメージされている。法学研究としてはさらに様々な留保や検討を要するが、本稿の目的からすれば、ひとまずこの程度の概念整理で十分であろう。

というのは、ここまで述べた範囲でも、デジタル社会を適切に運営するルールのあり方を考える上で、様々な論点が引き出せるからである。本稿の対象から外れるが、例えば、「人工知能（AI）は権利を持つか」が議論されることがある。これは突き詰めると、AI を自然人や法人と同じ、客観法によって規律される生活関係の一方の主体として見るか、それとも自然人や法人の道具として見るかによって決まる問題である。前者の立場を採り、かつ、AI が出した判断を権利行使の「意思」と評価するのであれば、「AI が権利を持つ」と表現することになる。重要なのは、そのような立場を採ることが社会的ルールとして適切かどうかを、AI の開発や社会実装の状況を踏まえて、具体的な場面に応じて考えること

であって、「AI は権利を持つから」「AI は権利を持たないから」という出発点を先に決めて議論しないということであろう。

３．データに関わる権利の論点

（１）誰の権利か

２で整理した権利の概念を踏まえて、以下では、データに関する権利を考える際の論点を、いくつか考えてみることにしたい。

まず、権利には主体が必要であるが、データに関する権利の主体の問題がある。最初に考えられるのは、データの内容が特定の主体に関するものであり、当該主体が当該データに関する権利を持つ、という場合である。その代表は個人情報保護法である。個人情報保護法は、個人情報によって識別される特定の個人を本人とした上で、個人情報取扱事業者に対する保有個人データの開示、訂正、利用停止の請求権を本人に認めている。さらに、データが必ずしも特定の主体を識別しなくても、当該データの利活用により何らかの影響を受ける、またはその可能性のある人は、当該データに関する権利を持つというように、権利の主体を広げていくこともできる。

他方、データの内容ではなく、データの成り立ちに着目して、データに関する権利の主体が決められることもある。企業がデータを生成ないし取得し、加工してデータベースで管理する、必要な場合に事業に利活用したり第三者に販売したりするときには、他の企業が当該企業のデータを盗むようなことは法的に禁止されるべき場合があり、進んでそのような行為をした企業に対して、当該企業が損害の賠償やデータの利活用の差止めを求める権利が認められるべき場合があるだろう。このような場合には、データを作成した者は、データに関する権利を持つということができる。

進んで、契約で購入した等、このようなデータを正当に譲り受けた者、あるいは、データ本体でなくデータに関する権利を正当に譲り受けた者も、データに関する権利を持つといってもよいであろう。さらに、データは有体物よりも流通が容易であり、またその流通が適正になされることがデジタル社会の健全な発展に必要であると考えるならば、データの流通に関わる者にも、何らかの権利を認め、その活動を法的に保護するということも考えられる。

ところで、ここまでデータの内容、あるいはデータの成り立ちに即してデータに関する権利の主体について考えてきたが、両者の権利が両立し得ることにも注意しなければなら

ない。企業が管理する顧客のデータベースは、本人の個人情報として保護されると同時に企業の営業秘密としても保護されるということが通例であろう。このような場合に、データの本人や、データの利活用により影響を受ける者に排他的な権利を認める場合には企業によるデータの利活用は成り立たなくなるだろうし、逆に本人の利益や意思を考慮せずにデータを利活用できる権利を企業に認める場合には、本人の保護が不十分となるだろう。

（２）何に関する権利か

データに関する権利を考えるに当たっては、権利の主体ではなく、権利の対象となるデータの性質に着目することもできる。データの内容が個人に関する場合、すなわち個人データについては個人情報保護法がある。日本の個人情報保護法は、個人に関する情報であって特定の個人を識別できるものを個人情報として定義するが、容易照合性がある情報も、また個人識別符号を含む情報も、個人情報に該当するとしている。

そうでないデータは非個人データということになるが、その中にはまったく個人に関連しない自然現象に関するデータや統計データだけでなく、広い意味で個人に関連する情報（個人情報でない個人関連情報）も含まれている。いわゆるパーソナルデータの利活用に当たってかねて問題とされてきたのは、非個人データとして個人情報保護法の規律が及ばないまま流通し利活用するうちに、個人を特定したり、さらには特定の個人を識別したりすることになって、本人の利益を侵害するおそれが生じるのではないかということであった。

非個人データの中には、企業・法人に関するものも多様に存在する。中には、企業・法人が開示する自己の経営に関するデータもあれば、産業データもあり、営業秘密として保護されるものもある。

このようにデータの性質が様々であり、また、当該データの利活用による便益やリスクも様々であることから、適切な社会的ルールを設定するためには、データの具体的な性質をよく分析した上で、それに関する権利やその内容を定めることが必要になろう。

（３）行使・実現できる権利か

最後に、データに関する権利を考える場合には、その実現の方法までも射程に入れるべきであり、そうでなければ権利といってみても、結局は絵に描いた餅にすぎないことになるだろう。一般には、権利の主体が、違法な権利侵害がある、またはそのおそれがあることに気づいて、相手方に対して権利を行使することが想定されている。しかし、データに

関する権利については、情報技術や情報通信技術の発展と相俟って、その主体が権利の侵害やそのおそれに気づかない、気づいた時には既に違法なデータの利活用や提供が終わったりデータが消去済みだったりして、権利行使のタイミングを失してしまった、また、誰が権利を侵害する者として権利行使の相手方になるのかがわからない、といった問題が生じやすい。

このような状況で、データに関する権利を真に実効あらしめようとすれば、単に権利を認めるというだけでなくて、これから当該データが利活用される、誰がデータを取得している等の情報を何らかの形で本人に知らせ、権利行使の機会を確保する必要が出てくる。個人情報保護法が、個人情報取扱事業者に通知や公表を義務づけているのは、そのような仕組みの一例である。さらに進んで、このような自分が権利を有するデータの所在や利活用について通知を受ける利益自体を権利として構成することも考えられる。

また、本稿の冒頭で述べたことに関わるが、現在のデジタル社会ではデータの収集・拡散が早く、また、その利活用のされ方により思わぬ価値や利益を生んだり、関係者に大きな不利益をもたらしたりということが起こりうる。そうすると、データに関する権利については、通常の権利とは異なる行使の仕方を認めるということも考えられる。例えばデータの利活用について許諾した後にも、その後の展開を見て、許諾を撤回する権利、ないし以後の利用停止を求める権利を権利の主体に認めることにより、データの流通や利活用を促進することができる場合もあるだろう。

このような対応には、もちろん逆の懸念もある。事後的にデータの利用許諾を撤回されても、その間に正当であったデータ利活用を通じて、また他のデータと結合して新たに生成されたデータまで消去しなければならないとすれば、データ利用者の不利益は大きく、さらには社会公共の損失ということも起こりうるであろう。

しかし、こうした問題は事後的な許諾の撤回等に限られたことではなく、例えばある集団のデータについて、多数の主体は利活用に同意しているが、一部の主体が反対している場合、とりわけデータの中で全体と部分を切り分けることが容易でない場合にも、構造的に同様の問題が起きている場合も多い。そのような場合に、個々の主体に全体ないし当該主体に関するデータの利活用を拒否する権利を認めるのか、そうではなくて別の利益保護の仕組みを用意するのかも、データに関する権利を考える上では、重要な問題となり得る。

さらにいえば、大規模な個人情報データベースの漏えいのような場合に、漏えいされた本人が個別的に権利を行使する、とりわけ裁判制度を利用することは期待しがたい。権利

行使のコストが、裁判制度によって実現される個人的利益を上回る場合が多いからである。このような場合には、適格消費者団体による消費者団体訴訟のような集合的な行使を念頭に置いて、データに関する権利を構成することも考えられる。さらには、私人間での裁判制度を通じた権利の行使・実現だけでなく、ADR や公法的規制を含めた、行政機関等による権利の保護・実現と組み合わせることも、必要とならざるを得ない。

４．データに関する権利へのアプローチ

（１）既存のデータに関わる権利

データに関する権利を検討する上では、２で述べたとおり、主体、データの性質、権利の行使・実現という３つの面から考えただけでも、多種多様な考慮が必要になることがわかる。

ここで既存の実定法秩序に検討の対象を移すと、データそれ自体に対する権利というよりも、むしろデータの利活用等の取扱いが、既存の権利や法的仕組みによって保護されることがある、というのが現状であるように思われる。

まず、データの利活用により影響を受ける利益を保護する権利ないし法的な仕組みが存在する。プライバシー権をはじめとする人格権、著作権や著作者人格権、そして営業秘密の保護が挙げられよう。

次に、既存の権利ないし法的な仕組みがデータの利活用を対象にする場合がある。これは著作権法上の支分権が代表であるが、実は表現の自由も、データを発信し受領する行為を保護する機能を有している。データの利用・提供をビジネスとする場合には営業の自由の保障が及ぶ場合があり、企業間での契約がデータの利用・提供を内容とする場合にも、契約上の諸権利が生じることになる。

最後に、上のようなデータの利活用、ないしデータ利活用の影響を受ける利益を実現・回復するための、いわば手段的な権利ないし請求権がある。人格権や著作権侵害に対する損害賠償請求権や差止請求権はその代表であり、個人情報保護法が定める保有個人データの開示、訂正、利用停止の請求権もその例ということができる。

このように現在の実定法秩序では、データに関する権利に関するルールは、体系的に整理され設計されているとは言い難い状況にある。そこで、既存の権利ないし法的仕組みを参照して、具体的にデータに関する権利を考えるとどうなるか、いくつかのアプローチを検討してみたい。

（２）所有権的アプローチ

「データ・オーナーシップ」という言葉が用いられる場合には、暗黙の裡に物権の中でも代表的な所有権をイメージしつつ、データに関する権利が考察されているのではないかと思われる。特定の主体がデータを排他的に支配すべきであり、その利用・収益・処分を当該主体に専属させることが求められるような場面、例えば自己の管理下にある秘密そのもののようなデータ等にはこのようなアプローチが適しているかもしれない。しかし今まで述べたとおり、このような所有権的アプローチは、データを流通させ、他のデータと結合して利活用することで利益を生むというデジタル社会において、データに関する権利へのアプローチとしては一定の限界があるように思われる。

また、所有権については単独所有がイメージされがちだが、世帯や企業等の組織と構成員の情報が重なる場合などは、むしろ共有・合有・総有といった共同所有の規律が参考とされるべき余地があるように思われる。

（３）財産権的アプローチ

データが財産的価値を有することに着目し、その価値を保護する諸権利のイメージで、データに関する権利を構想するアプローチである。これは、財産的価値を有するデータについては適切であろうし、経済学の知見を活用して適正なデータ流通のためのルールを設計する上では欠かせない視点である。

他方、財産的価値は高くないが、その利活用により不利益が生じる者がいるようなデータについて、この財産権的アプローチだけで外部不経済の問題を処理しきれるかどうかは難しいところであり、後述の（５）のようなアプローチと補完する必要があるだろう。

また、データの財産的価値は、流通され利活用されてはじめて生じることもあるだろうから、そのような場合にデータの利活用による収益の帰属をいかに適正に定めるかということが重要となろう。

（４）契約的アプローチ

（３）とも連続的であるが、私的自治ないし契約自由の原則というこれまでの私法のデフォルト・セッティングによって、データの取扱いも規律されればよいとするアプローチである。現在の実定法秩序における私人間のデータの流通・利活用は、ここから出発していると見ることもできよう。データが多種多様であり、データの利活用もそれによる便益も

リスクも多種多様であることからすれば、当事者間で交渉して柔軟にルールを設定していくこのアプローチの意義は高いということができる。

他方、契約締結に至る様々なコストが高いほか、契約の遵守を確保するための権利の行使・実現の方法について、現在の実定法秩序では様々な課題があることは既に見たとおりである。データに関する権利を議論すべきだとされる背景に、契約ベースでのデータの流通が進んでいないとみられる日本の現状があることからすれば、このアプローチだけでも不十分であることは明らかであろう。

一つには民法の典型契約（有名契約）のように、データの流通・利活用に応じて契約を標準化・規格化して法律に定めを置くことが考えられる。また、契約上の権利が第三者により侵害される可能性に対処するためには、公示をはじめとする何らかの制度と組み合わせることが考えられる。

（５）人格権的アプローチ

データの利活用により影響を受ける個人の人格的利益の保護という観点から、データに関する権利を設定し法的保護を与えるアプローチであり、プライバシー権がこれに相当する。この場合、当該主体の人格的利益として保護されるべき範囲を適切に画さなければ、データの利活用を不当に損なうおそれがある。

この関連で、日本では人格権ないし人格的利益が判例により、個別の場面で承認されるにとどまっており、憲法や法律により明文化されておらず、そのために不法行為法や個人情報保護法などの法的な規律との関係について、法制上も学説上も一致がなく不安定な状態にあることの問題点は指摘しておかなければならない。裏を返して言えば、デジタル社会において、個人が対等な人格を持つ存在としてお互いを尊重するということの意義について、国際的な制度対話の基礎ともなるような根源的な議論が、日本で未成熟であることを示すものでもある。

（６）基本権的アプローチ

（５）と重なるところもあるが、憲法の定める基本的人権（基本権）として、データに関する権利を構想するアプローチである。本稿の冒頭で述べたとおり、デジタル社会においてデータが重要な地位を占めることからすれば、人権として認められるべきデータに関する権利もあることは否定しがたいように思われる。

他方、単なる権利を超えて、データについての基本権を認めることは、より重要な法的な効果をもたらすものである。基本権は、立法権を含む国家権力に対して向けられるものであり、以後は法律による安易な変更を許さないという点で安定的な基礎を提供する反面で、ルールの設計・変更の柔軟性を縛ることにもつながる。その点では、仮にデータ基本権を論じる際にも、あくまで理念的な権利の宣言にとどめる方が良いとも考えられる。

さらに、基本権は国家権力と個人の法的地位の非対称性に基づき、国家権力の側に、時には単なる作為・不作為を超えて、制度の設定・運用を含む重い義務を課すものでもある。このようなデータに関する基本権を認める場合には、デジタル社会で時には国家権力をも上回る力を持つ、グローバルなデジタルプラットフォーム事業者への対応をも考慮するべきであろう。現に EU で説かれている「デジタル立憲主義」は、まさにデジタルプラットフォーム事業者に対する憲法的規律の必要性を説くものである。

５．若干の帰結

（１）個別具体的な検討、主観的権利と客観法のハイブリッド

以上、データに関する権利へのアプローチとして考えられるものをいくつか挙げたが、それぞれに利点と課題があることは明らかであろう。当たり前のことだが、結局はデータの流通・利活用により得られる便益と、権利の内容として保護すべき利益とを見据えながら、これらのアプローチを適切に組み合わせていくことが必要と思われる。

次に強調しなければならないことは、そもそもデータに関する権利を認めることの適否自体も議論の対象となるということである。そもそも主体が行使し実現する主観的権利という構成を採用せずとも、客観法を定めてその公法的な遵守の仕組みを定めることでも、データの流通・利活用と保護のバランスを構築できる場合もある。さらに上で述べたように、データに関する権利という構成を取る場合であっても、客観法の定める制度による補完が有用ないし必要と思われる場合も多い。

例えば個人情報保護法制は、利用目的の特定を中心に、個人情報取扱事業者等の義務を定め、個人情報の形態が個人データである場合には第三者提供における同意のように本人関与を強化し、さらに保有個人データである場合には本人の請求権を認め、これらについて個人情報保護委員会の監視・監督権限を定めるという複合的な仕組みを採用している。これまで述べたデータに関する権利の抱える困難さに即してみれば、このように主観的権利と客観法のハイブリッドな規律が適切に設計されることが必要であろう。

（２）データに関する権利を議論する意味

このことはむろん、データに関する権利を議論する意味がないということではない。権利を基本的な構成要素としてルールを設定・運用するということは、権利を有する者を起点として、それに対応する義務を負う者がいるという関係が成立し、それがネットワーク上に広がっていって社会が形成されることを前提とする。

データの内容に関する個人や、データの生成や加工に貢献した企業から見ると、デジタル社会はともすると、データが自分の手の及ばないところへ流れていき、思わぬところで利活用されて不利益を被ったり、利益が他の者に帰属したりといったことが容易に起きそうな、不安に充ちた社会である。そうであるが故に、個人がデータの利活用に対する懸念を表明したり、企業がデータ提供を躊躇したりといった課題が生じているところである。

信頼性あるデータ流通（DFFT）の理念を実現する上で、データを取り扱う主体のガバナンス､国の定めるルールやそのエンフォースメントの信頼性が議論されることが多いが、その基礎として、データに関わる主体と主体の間に、主観的な権利と義務の関係という形で具体的な「絆」が結ばれることは、まさにデータの流通と利活用への信頼を生み出す原動力となるものである。

筆者の見るところ、データに関する権利を議論することの意味は、何よりもこのような社会のあり方にコミットすることにあり、その上で具体的な場面においては、既存の権利の概念やその前提、既存の権利を参照したアプローチを柔軟に組み合わせて適切なルールを設定・運用することが必要であると考える。本稿がそうした議論を進めるための一助になっているとすれば、幸いである。

第２章　個人情報に対する個人の権利強化と利活用の両立に向けて

宮内・水町 IT 法律事務所

弁護士　水町　雅子

個人情報保護の必要性については論をまたず、またデータ利活用の必要性についても、日本社会において理解されているものと思われる。他方で、個人情報保護とデータ利活用をどのように両立させていくかについては、いまだ議論の続いているところである。本稿では、データの中でも個人情報に焦点を当て、個人情報保護の実効性を高めた上で、個人情報保護を前提としながら、企業がデータ利活用を行えるよう、どのような方策が考えられるか、現状の課題から考えていきたい。

まず、個人情報の範囲が一般の想像よりも広いため、利活用するデータから個人情報を除外することには一定のハードルがあることを述べたうえで、個人情報を実効的に保護するための課題、実効的な保護のあり方について、データ利活用の観点も鑑み、個人情報不適正取扱い時の本人救済、そして個人情報に関する透明性のある説明の浸透などについて述べていくこととしたい。

１．個人情報の範囲は広い

（１）物や状態等に関する情報であっても個人情報に該当しうる

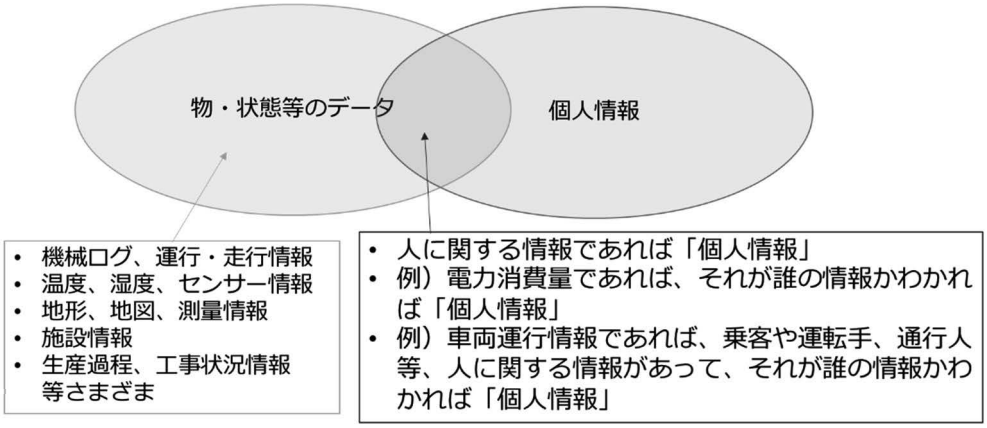
「個人情報に該当しないデータの利活用であれば、個人情報保護法の問題がない」と考える向きもある。確かに、「個人情報」でも「個人に関する情報」でもなければ、個人情報の保護に関する法律（以下、「個人情報保護法」という。）の問題は生じないと考えられる。しかし、個人情報の範囲は、一般に想像されるよりもかなり広範であり（図-1 参照）、多くの者が「非個人情報」と誤解しているデータであっても、法律上は「個人情報」に該当する場合がある。

個人情報とは、個人情報保護法２条１項で定義されているが、平たくいえば、生存する個人に関する情報であって、誰の情報かがわかるものをいう[1]。この定義から、物や状態

[1] 個人情報保護法２条１項では、①生存する個人に関する情報であって、個人識別符号が含まれるもの（同項２号）、又は②生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他

等に関する情報は個人情報ではないと言えそうである。温度・走行情報・地図・機械ログ・生産過程情報などは個人情報ではない場合が多い。もっとも、物や状態等に関する情報であっても、それが同時に人に関する情報であれば、個人情報に該当する場合がある。

図-1　物・状態等のデータと個人情報



例えば、走行情報は物に関するデータであるものの、運転者 ID を含んでいれば、運転者の個人情報に該当する可能性がある[2]。機械ログや生産過程情報についても、操作者 ID などが含まれていれば同様に個人情報に該当する可能性がある。また、ドライブレコーダーによる録画情報に運転者・同乗者・通行人・他の車両運転者等が映り込んでいれば、これも個人情報に該当するし、地図についても、居住者等の情報が含まれていれば個人情報に該当する。このように、物や状態等に関する情報であっても、記録項目等を確認しなければ、個人情報に該当しないかどうかを判別することはできない。

（２）個人情報の提供も該当範囲が広い

また個人情報／個人データの提供に該当する範囲も、一般に想像されるよりもかなり広範である。例えば、ID と氏名は別表で管理したうえで、日ごろ取り扱うデータは氏名

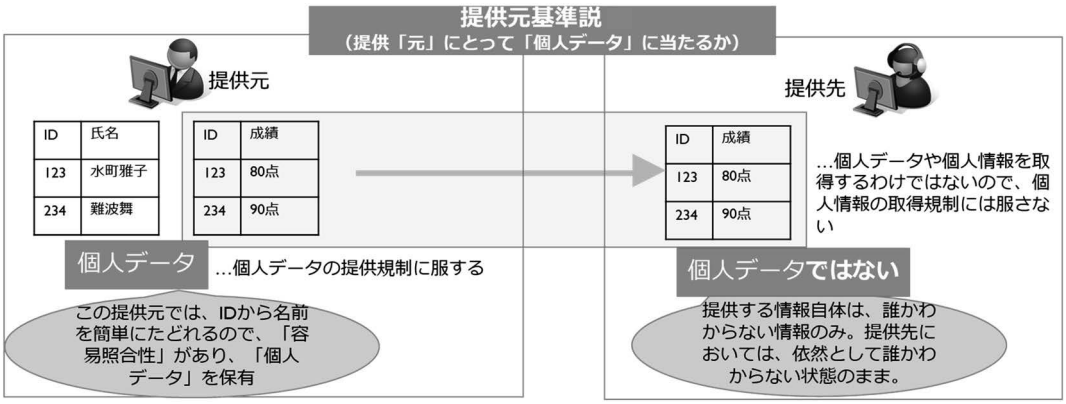
の記述等（文書、図画若しくは電磁的記録に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）（同項１号）が個人情報に該当すると定義されている。①②とも、重要な要素は、「生存する個人に関する情報」であること、および特定の個人を識別することができることであるため、本文のように記した。

[2] 走行情報に運転者氏名自体は含まれておらず、運転者 ID しか含まれていないとしても、社内で運転者 ID と運転者氏名等の情報を困難なく紐づけられる状態等であれば、「容易照合性」（（２）で後述する。）ゆえに運転者 ID しか含まれていない走行情報も、個人情報保護法上の個人情報に該当する。

ではなく ID で管理している場合があるとする（図-2 の左側参照)。この場合に、氏名を提供せずに、ID と日ごろ取り扱うデータのみ（図-2 でいうと ID と成績のみ）を提供した場合であっても、現行法の解釈上は、個人情報／個人データの提供となる。

なぜかというと、個人データの提供は個人情報保護法上規制されているが、個人データが提供されているかどうかをどう判断するかというと、「提供元」を基準に判断するからである。図-2　個人情報／個人データの提供でいえば、ID と成績が提供情報となるが、提供元においては、ID から氏名が容易にたどれる状態になっている。個人情報保護法 2 条 1 項 1 号で、「他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるもの」も個人情報に該当すると規定されており、これは「容易照合性」と呼ばれる。そのデータ単体で見たら誰の情報かわからない情報であっても、他の情報（ここでいえば、氏名）と容易に照合でき、それによって誰の情報かがわかるものであれば、個人情報に該当する。したがって、図-2 の右側のように、ID と成績のみの提供であって、提供先においては誰の情報かがわからない状態であっても、提供元にとっては個人情報／個人データであるがゆえに、これは個人情報／個人データの提供に該当する。

図-2　個人情報／個人データの提供



（3）氏名を削除しただけでは匿名加工情報にならない

「個人情報であっても匿名加工すれば、簡単に利活用できる」と考える向きもある。確かに、個人情報保護法上、匿名加工情報であれば、目的外利用も第三者提供も容易に行うことができる。

もっとも、匿名加工情報は、法定された匿名加工基準を遵守しなければならず、その

方法が非常に厳格である。例えば、氏名や生年月日の日、健康保険被保険者証の記号番号の削除だけでは、適法な匿名加工情報とは認められない。匿名加工のためには、ID を置換したり、特異な情報（例えば、身長 200 センチ、「難病のため首相を退任した」などの情報）を削除したり、その他適切な措置を取らなければならないとされている（図-3 参照）。データの状態によっては、匿名加工によってデータの有用性が下がる可能性もある。また特に、特異な情報などは機械的な加工が難しいし、人間の目で一件一件確認していったとしても何が特異な情報に該当するかにかかる判断が難しい場合もある。このように、データによっては、適法な匿名加工が非常に難しい場合も考えられる。

図-3　匿名加工基準／仮名加工基準

<table>
<tr><th></th><th>仮名加工情報</th><th>匿名加工情報</th></tr>
<tr><td rowspan="5">加工基準</td><td colspan="2">① 特定の個人を識別することができる記述等の削除又は復元できない置換
→例）氏名削除、住所丸め、生年月日の日削除</td></tr>
<tr><td colspan="2">② 個人識別符号の削除又は復元できない置換
→例）マイナンバー削除、保険証記号番号削除、生体認証情報削除</td></tr>
<tr><td rowspan="2"></td><td>③ 情報を相互に連結する符号の削除又は復元できない置換
→例）内部IDの置換・削除</td></tr>
<tr><td>④ 特異な記述の削除又は復元できない置換
→例）身長200センチ情報の丸め・削除</td></tr>
<tr><td>③ 不正に利用されることにより財産的被害が生じるおそれのある記述等の削除又は復元できない置換
→例）クレジットカード番号削除</td><td>⑤ 個人情報データベース等の性質を踏まえたその他の適切な措置</td></tr>
</table>

なお、「匿名加工情報」よりも加工強度が弱い「仮名加工情報」も認められている。仮名加工情報の場合は、加工方法が明確で（氏名等・個人識別符号・財産的被害が生じる恐れのある記述等の削除等。図-3 参照。）、比較的容易に加工・作成できると考えられる。もっとも、仮名加工情報の場合は、事実上の目的外利用（利用目的の事後変更が容易。変更後の利用目的の公表が必要。）はできるが、第三者提供は極めて困難である。

また、匿名加工情報よりもさらに加工の強度が高い、完全な統計情報（図-4 参照）であれば、個人情報保護法の規制は課せられないが、統計情報ではデータの有用性が下がる可能性がある。

図-4　加工強度／規制の比較

規制強い
加工強度弱い

生の個人情報	• そのままの状態（生データ）
仮名加工情報	• パッと見、誰かわからなくなっている情報だが、法的には原則個人情報のまま 　• ①特定の個人を識別できる記述等（氏名・住所・生年月日・郵便番号等）の削除・置換 　• ②個人識別符号の削除・置換 　• ③不正利用により財産的被害のおそれがある記述等の削除・置換 • 個人情報への**義務が一部軽減** • **内部利用目的に限定**
匿名加工情報	• 誰かわからなくなっている情報 　• ①特定の個人を識別できる記述等（氏名・住所・生年月日・郵便番号等）の削除・置換 　• ②個人識別符号の削除・置換 　• **③連結符号等の削除・置換** 　• **④特異な記述等の削除** 　• **⑤個人情報データベース等の性質を踏まえたその他の措置** • **容易な手続で**利活用・外部提供可能 • 内部利用目的に**限定されない** • 再識別は禁止
統計情報	• 特定の個人との対応関係がなく、完全に個人情報でも個人に関する情報でもない • 匿名加工情報との境界は曖昧な部分が残る

規制弱い
加工強度強い

（４）小括

データ利活用に際して個人情報を除外できれば、個人情報保護法の問題が生じないため、利活用にかかるハードルが比較的低いものと思われる。もっとも、以上のように、個人情報の範囲は広く、匿名加工も難しい場合があるため、データ利活用に際して、個人情報を除外するのが難しい場合もある。

そこで、以下では、利活用するデータに個人情報が含まれる場合があることを想定し、データ利活用に際して、個人情報が現状よりも実効的に保護され、データ利活用にかかる国民的合意が醸成されうるための方法について検討していきたい。

２．本人はどのような権利・保障を受けるべきか

（１）現状の法規制

では、個人情報を利活用するためにはどうすればよいか。1 つの方法は加工である。繰り返しになるが、法定の加工基準を満たす匿名加工情報を作成すれば、個人情報保護法上、容易に目的外利用や外部提供が可能となる。また、匿名加工情報よりも加工が容易である仮名加工情報を作成すれば、外部提供は難しいものの、内部での利活用は容易である。これらの加工情報では目的を達成できない場合は、本人同意を取得するか、又は本人同意がなくとも個人情報の内部利用は目的外利用の要件を満たせば、適法となる。外部提供であればオプトアウト・委託・共同利用などの構成で適法に行うことができる。

個人情報の対象者である本人はどのように保護されるかというと、加工情報であれば、法定の加工基準を満たす適切な加工によって、自分の情報であることが「匿名加工情報」であればわからないように、「仮名加工情報」であれば一見した状態ではわからないようになっていることで保護される、というのが現在の個人情報保護法の考え方であろう。また、加工情報ではなく個人情報のままであっても、個人情報保護法上、不適正利用規制、目的外利用規制や第三者提供規制、海外提供規制、安全管理措置等の規制が存在し、かつ本人には開示・訂正・利用停止請求権が認められている。このように、現行法上でもすでに様々な規制がなされており、本人の権利も一定程度認められているといえる。

しかしながら、現状を見てみると、現行法に基づく規制と本人権利保障だけでは、企業側のデータ利活用はなかなか進まず、また個人情報の対象者である本人としても、自身の個人情報が保護されていると感じづらいとも考えられる。では、現行法以上に、どのような対応がなされれば、個人情報の保護とデータ利活用の両立が促進されるのだろうか。筆者は、個人情報不適正取扱い時の本人救済、そして個人情報に関する透明性のある説明の浸透が重要と考える。

（２）救済

いざ個人情報が不適切に取り扱われた場合に、現状で消費者が取り得る方法としてはSNS 等の世論に訴えかけるといった方法が考えられ、それ以外の方法を取るのが難しいとも考えられる。現行の個人情報保護法では、個人情報の不適切取扱い時の制裁として、①罰則、②行政制裁（命令・勧告等）を定めているが、①罰則対象となる取扱いも少なく、また②行政制裁がなされたか否かは被害を受けた本人に通知されない場合もある。結局のところ、現行法下では個人の救済は、訴訟によるしかない構成とも考えられるが、個人情報の悪用等については損害額が小さい場合が多いということもあり、個人にとっては費用面からも心理面からも提訴のハードルが高い。個人の実効的救済のためには、認定個人情報保護団体や個人情報保護委員会等による苦情処理・紛争仲裁等の機能を検討・強化するべきと考える。

そして個人情報の本人のみならず、個人情報を取り扱う企業側にとっても、上記の仲裁等の手法を経ることでメリットがある制度となると、仲裁等に協力的な企業が増えることが期待される。個人にとってのメリットしかないとすると、企業側の対応としては消極的なものとなり、企業側に仲裁等へ応じる義務を法律上課すことを検討せざるを得ない。

しかしいくら法律上対応義務を課したところで、企業として仲裁等に応じても何らメリットがないと、問題解決に向けた積極的協力を得られにくい可能性も考えられ、制度としてワークするためには、本人のみならず企業側にとってもインセンティブの付与が重要であろう。そこで、仲裁等対応に応じる企業については、例えば、P マークに上乗せして認証する等して、公共調達や民民間契約でも有利としたり、委託元が委託先を選定する際の望ましい基準とすることなども考えられるだろう。また、行政制裁を行うか否かを個人情報保護委員会が検討する際に、企業が仲裁等対応に応じたか否かを一つの考慮要素とするという方法も考えうる。

（３）透明性のある説明

①　自分の個人情報の取り扱われ方をイメージできるように

（２）では個人情報が不適切に取り扱われた場合の救済について述べたが、通常時においても、本人が自分の個人情報の取り扱われ方について、より理解できるように環境整備を行うことも必要である。

個人情報を取り扱われる側にとっては、自身の個人情報が、誰に何を目的にどのように取り扱われているかが、現状ではわかりにくい。現行法上も、個人情報の利用目的や安全管理措置概要などを通知等する義務を課しているものの、企業のプライバシーポリシーや利用規約を読んでも、自分の個人情報の取扱いに関するイメージを持ちにくいと考えられる。現状では、具体的な取扱い実態を理解したうえで個人情報を預けるというよりも、「大企業だからおかしな取り扱いはしないだろう」といった企業に対する信用・イメージで個人情報を預けているというのが、消費者の感覚に近いようにも思われる。

個人情報の取扱い実態がブラックボックス化してしまうと、いざ、消費者側の想定と異なる取り扱われ方をしていた時に、企業側は著しく信頼を失いがちである。現状を改め、個人情報を取り扱われる側からみて、自分の個人情報がどのように利用、提供等されるかを理解し、具体的にイメージできるように、透明性のある説明がなされるべきである。

②　企業に過負荷をかけずに透明性のある説明を～プライバシーポリシー

多くの企業においても、個人情報保護の重要性は強く認識されており、個人情報保護のために様々な対策が講じられているし、プライバシーポリシー等の公表も行われている。しかし、個人情報を取り扱う企業側からすれば、個人情報の利用方法等は多岐にわたるため、具体的にどのようにすれば透明性のあるわかりやすい説明となるかが非常に難し

いという実務上の課題がある。そのため、現行のプライバシーポリシーのような網羅的抽象的記載にならざるをえないという実情も考えられる。透明性のあるわかりやすい説明が求められるとは言っても、その対応が企業に過負荷をかけるものであると、企業側の対応もなかなか進みづらかったり、形式的なものになったりする恐れがある。個人情報について透明性のある説明を、企業側の過負荷なく行うためにはどうしたらよいか。

1 つの方法として、プライバシーポリシーの記載事項・記載粒度の見直しが考えられる。現状でも利用目的や第三者提供について記載しているのであるから、その記載粒度を消費者側にわかりやすいように整えることが考えられる。

例えばプライバシーマーク付与事業者においては、プライバシーマーク対応として、全ての個人情報について台帳記載の上、利用目的の特定等を行っていると考えられるので、これを活用して、現状のプライバシーポリシーよりも詳しく、わかりやすい説明を公表するという方法も考えられる。また GDPR が適用される欧州企業等では、プライバシーポリシーで、個人情報の取扱いが必要となる企業側の正当な利益（GDPR6 条 1 項(f)、13 条 1 項(d)、14 条 2 項(b)）の説明などを行っているので、それを参考にする方法も考えられる。

③　企業に過負荷をかけずに透明性のある説明を～プライバシー影響評価

海外でも実施されているプライバシー影響評価の手法を用いる方法も考えられる。プライバシー影響評価とは、例えるなら環境影響評価のような事前評価を個人情報に対して実施するものである。環境影響評価とは、大規模な開発事業などを実施する際に、事業者が、あらかじめその事業が環境に与える影響を予測・評価し、住民や関係自治体などの意見を聴くとともに、それらを踏まえてより良い事業計画を作ることにより、適正な環境配慮がなされるようにするための手続をいう（環境影響評価法 1 条参照)。プライバシー影響評価では、個人情報を取り扱うビジネス・施策などを実施する際に、一般人やステークホルダー、専門家の意見を聴きながら、あらかじめプライバシーに与える影響を予測し、かかる影響を排除又は十分に軽減するための対策を検討・実装することにより、プライバシー権保護とビジネスの成功との両立を図ることとなる。

プライバシー影響評価は、GDPR では実施義務が課せられている（GDPR35 条)。英米法圏ではプライバシー影響評価（Privacy Impact Assessment、PIA）と呼ばれるが、大陸法圏ではデータ保護影響評価（Data Protection Impact Assessment、DPIA）と呼ばれている。日本でもプライバシー影響評価は、マイナンバー関連では「特定個人情報保護

評価」として行政手続における特定の個人を識別するための番号の利用等に関する法律で実施義務が課せられており（同法 28 条)、特定個人情報保護評価指針も公表されている。

規格・認定等制度としても、ISO/IEC 29134：2017 Information technology − Security techniques − Guidelines for privacy impact assessment や JIS X 9251:2021 情報技術―セキュリティ技術―プライバシー影響評価のためのガイドライン等が発行されており、『「情報銀行」認定制度 データ倫理審査会 運用ガイドライン』でも上記 ISO や JIS 規格を元にプライバシー影響評価について記載されている。

全企業においてプライバシー影響評価を実施するのは、企業負荷から鑑み難しいかと思われるが、GDPR のデータ保護影響評価の義務付け基準等を参考として、リスクの高い類型についてはプライバシー影響評価を検討することも望ましいと考える。また、プライバシー影響評価は、評価項目や評価手法に法定基準があるわけではないので、より負荷を減らした形で簡素化して実行したり、又はプライバシー影響評価の重要要素を踏まえてプライバシーポリシーの記載を充実させるなどの方法も考えられるだろう。

プライバシー影響評価の実践例として、筆者が日本電気株式会社協力の下作成した「顔認証を利用した顔パスイベント入場に関する個人情報リスク評価 DPIA・PIA」[3]や（図-5 参照)、姫路市協力の下作成した「総務省実証事業における姫路市行政情報分析基盤個人情報リスク評価 PIA」[4]（図-6 参照）があるため、参照されたい。

図-5　顔認証 PIA からの抜粋

日本電気株式会社の有する顔認証技術を用いてイベントに顔パス入場する仕組みに関して、プライバシー影響評価を実施した。

顔認証により、来場者は手ぶら（チケットレス）で、そして入場待ち時間が短縮する等、スムーズにイベントに参加することができ、また、不正入場の防止や接触レスなどの利点もある。他方で、重要な個人情報である顔画像が万一悪用されたり流出してしまえば、プライバシーに与える影響は非常に大きく、また様々な場所での監視につながる懸念や、顔認証の精度の問題等もある。顔認証の活用といった比較的新しい取組みはイノベーションに欠かせないものではあるが、個人情報やプライバシー権の保護がまずもって大前提であり、プライバシーに与える悪影響を防止・軽減する対策を事前に十分講じた上で、適法・適正に技術が活用されていくことが重要であるため、プライバシー影響評価を行った。

以下は、当該評価の一部を抜粋したもの。

[3] https://www.miyauchi-law.com/f/210812necpia.pdf
[4] https://www.miyauchi-law.com/f/180628PIAhimeji.pdf

1.1　顔パス入場の概要

①申込時

利用者

・Webから申込み
・氏名、生年月日、住所、電話番号、メールアドレス、パスワードを入力する
・**「顔パス入場」を利用したい場合に限り**、顔写真データの登録の同意を行い、顔写真データをアップロードする
・いったん登録した後に、顔写真登録の取消も可能

②入場時

顔パス利用者

※顔パス入場者以外は、通常ゲートから通常通り入場

・顔パス入場者は、顔パス入場ゲートのカメラで撮影した顔写真データをアップロードして識別・認証することの同意を行う。同意された場合のみウォークスルー用のゲートに進む
・ゲートのカメラで顔写真を撮影
・認証できた場合は、入場ゲートが自動的に開く
・認証できなかった場合は、通常ゲートから通常通り入場するか、係員に問い合わせる

5

3　顔パス入場の個人情報保護のポイント（対策まとめ）

顔写真データは、大変重要な個人情報です。また、顔認証が悪用等されると、なりすましや監視等につながる懸念もあります。顔認証技術を利用・提供する企業にはこれらのリスクその他のプライバシー権侵害や不正行為を防止するため、様々な対策を応じる必要があります。NECでは本評価記載の通りの措置を講じており、その主なポイントは以下の通りです。

主なポイント

① **顔写真データ自体はすぐに削除**
・顔写真データを利用者が登録後、速やかに顔認証システムでは「特徴量抽出 *」を行います。特徴量抽出後は、速やかに登録された顔写真データ自体を削除します。
・来場時にゲートで撮影した顔写真データも、速やかに特徴量抽出を行い、撮影データを削除します。
*特徴量抽出：まず、画像中から顔を検出した後、顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した顔特徴量を抽出します。顔識別・顔認証は、この特徴量を用いて実施します。

② **希望者だけが、顔パス入場**
・**顔パス入場希望者以外は、通常ゲートから通常通り入場できます。**

③ **NECが提供する顔認証機能では、氏名・住所等の情報は保持しません**
・ID・顔写真データ、顔写真データから抽出した特徴量のみを保持します。このうち、顔写真データは上記の通り特徴量抽出後速やかに削除するため、ID及び特徴量のみ保存しています。
・但し、Y社の催事管理システムでは、申込者情報として氏名・住所・電話番号・メールアドレス・ID等の情報を保存しています。

④ **セキュリティ**
・様々なセキュリティ対策を履践しています。NECではPマーク付与認定及びISMS認証を取得しています。

10

5.3　入場するために顔画像を登録しなければならないのか

某イベントに参加したいです。
でも、そのために顔画像を登録したり顔認証をするのは嫌です。

希望者だけ、顔画像による顔パス。通常ゲートからチケット提示でも入場できます

- 顔認証による顔パス入場は、あくまで希望者だけが対象。
- 顔パス入場以外に、通常ゲートからチケットを提示し、通常の方法で入場することができます。顔パス入場か通常入場かは自由に選択可能です。通常入場を選択した場合にも来場者に不利益はありません（もっとも、通常入場の際は、入場待ちリスク、係員との接触リスク等はあり）

取消可能

- 一度顔パス入場を申し込んだ方でも、顔パス入場する前までであれば取消が可能。
- 取消を希望された場合は、顔写真、特徴量その他の個人情報を速やかに削除します（但し、問合せ対応のためIDだけは取消済のIDとして記録し保持しておく）。

残存リスク

- 取消時については、NECだけでなく、X社・Y社においても確実に削除されることを確認する必要があります。

15

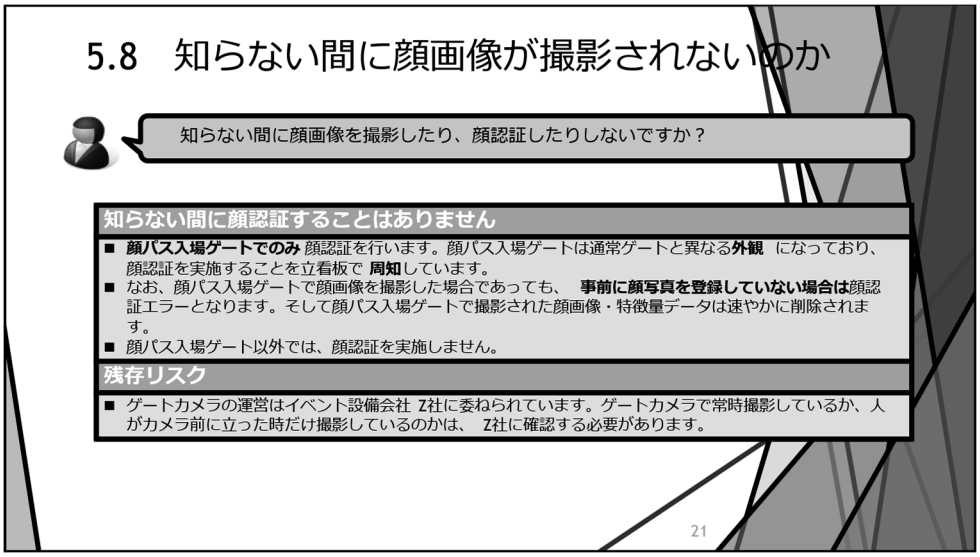
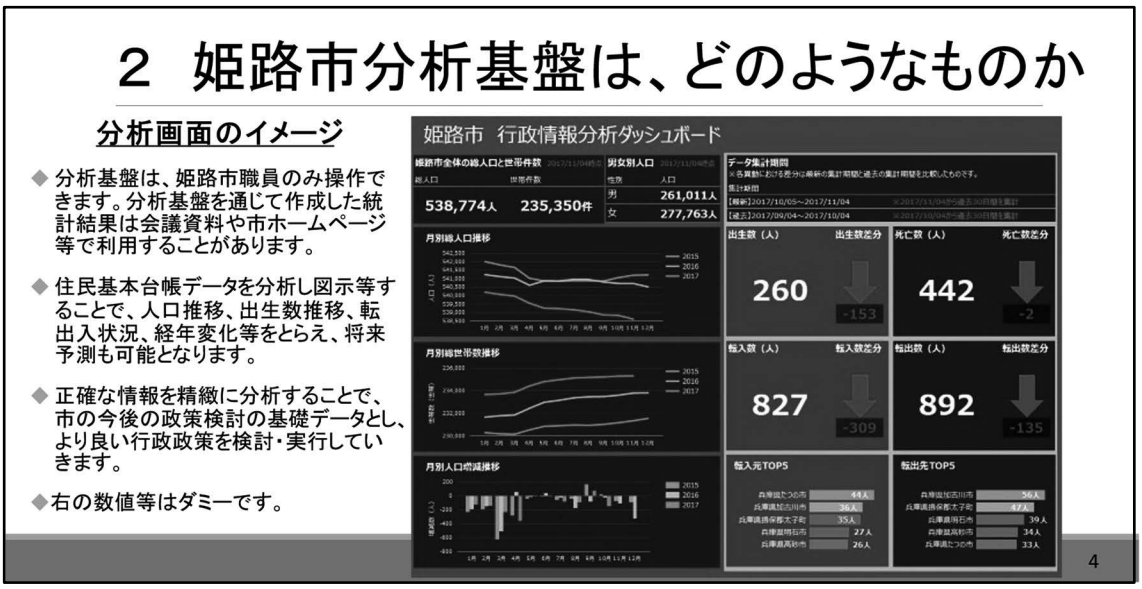


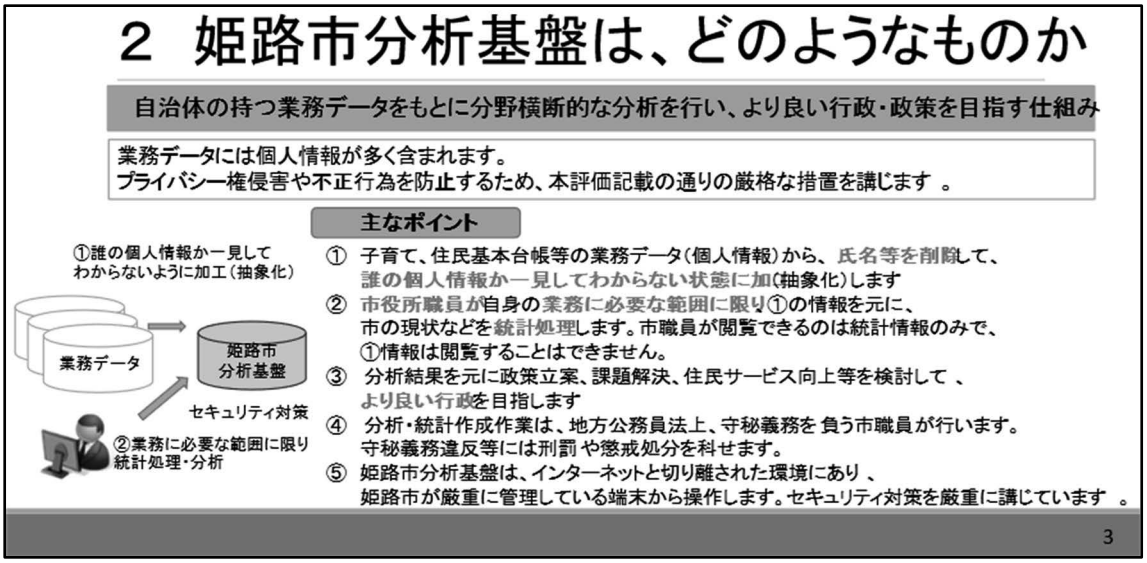
図-6　姫路市 PIA からの抜粋

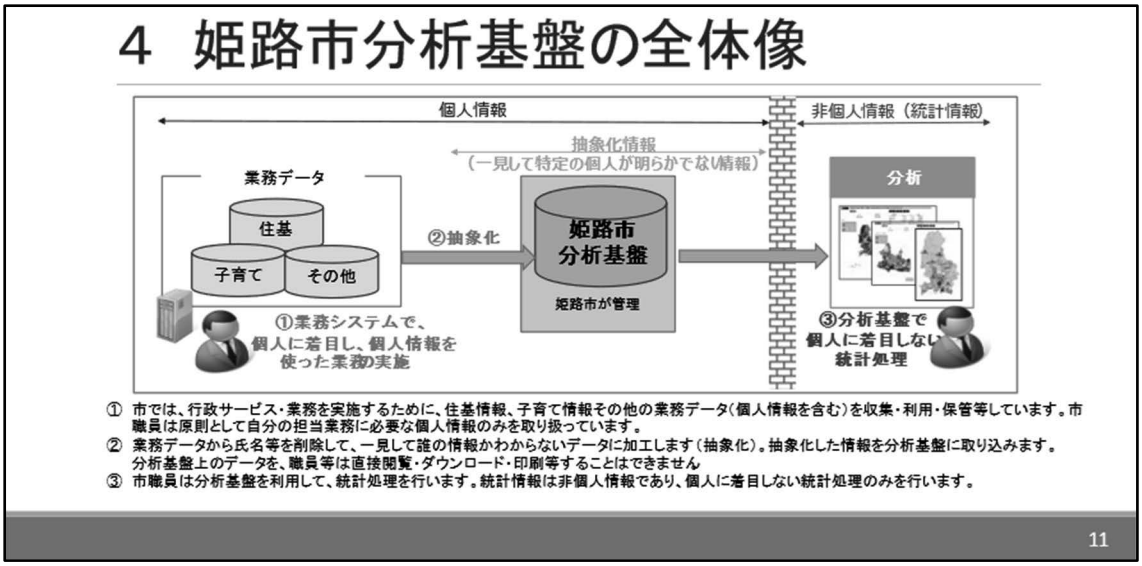
市役所の持つ業務データを活用して、エビデンスに基づくより良い政策立案（EBPM）を行うために、姫路市が開発・運用するデータ分析基盤システムについて、プライバシー影響評価を実施した。

人口減少・少子高齢化が進展する中で、限られた「ヒト・モノ・カネ」を「情報」により、これまで以上に効果的かつ計画的に活用することより、効率的な行政運営と住民の QOL 向上を目指す仕組みであり、かつ前例や職員の経験・勘などに依存しない、第三者による検証が可能で透明性の高いエビデンスベースの政策立案を推進するという重要な行政目的を有するものではあるが、活用する業務データの多くに個人情報が含まれるため、プライバシーへの悪影響を防止・軽減するため、プライバシー影響評価を実施した。

以下は、当該評価の一部を抜粋したもの。







④　第三者機関の事前審査

また、より良い取り組みとしては、企業側が自ら透明性のある説明を行うだけではなく、認定個人情報保護団体や個人情報保護委員会等の第三者機関による事前審査を受けるという方法も考えられる。（２）では、これら第三者機関による苦情処理・紛争仲裁等について記載したが、苦情処理・紛争仲裁等は、個人情報の不適正取扱いに対する事後救済の方法であるが、個人情報の適正取扱いに対する事前審査をこれら第三者機関によって行うということも考えられる。苦情処理・紛争仲裁等は、個人情報の不適正取扱いについて、個人情報を取り扱われた本人と個人情報を取り扱った企業側を第三者機関が仲裁等するという手法となるが、事前審査は、個人情報の不適正な取扱いが起こらないように、ま

た個人情報を取り扱われる本人と個人情報を取り扱う企業側で、個人情報の適正取扱いに対する認識齟齬が生じないように、第三者機関が個人情報の具体的な利用目的・共同利用等について、事前に審査・仲裁等することになる。

個人情報を取り扱われる本人にとってのメリットとしては、長文かつ抽象的なプライバシーポリシーや利用規約の記載を逐一確認して自ら同意するか否かを判断するだけではなく、中立・専門性を有する第三者がその企業の個人情報取扱いについて事前判断することで、プライバシー権保護に資することが考えられる。個人情報を取り扱う企業にとってのメリットとしては、事前に第三者機関にて審査を受けることで、ビジネスを開始したのちに個人情報の利用目的・外部提供等が違法・不適切と主張・指摘されることを防止できることが考えられる。

全ての個人情報取り扱いについて、第三者機関の事前審査を受けることは実務上難しいと考えられるが、プロファイリングその他本人からみてわかりにくい個人情報の取扱いや、本人の権利利益に重大な影響を及ぼしかねない個人情報の取扱いについて、第三者機関の事前審査を受けることが考えられるのではないか。また、その際、③で紹介したプライバシー影響評価の手法を併用することもできる。企業自らプライバシー影響評価を実施したうえで、第三者機関の事前審査を受けるという手法である。

⑤　民間主導の取り組みを

上記のような透明性のある説明を行った企業については、現行法下では萎縮傾向が強い公益目的での個人情報利活用や共同利用を認めるなどの制度設計も考えられるだろう。いずれにせよ、個人情報にかかる透明性のある説明を行うためには、企業実務を踏まえ、民間主導で検討を進めると良いと考える。国主導であると、企業実務や企業負荷が十分踏まえられない可能性もある。より現実的な、より実務に即した取り組みとするためにも、民間主導で検討した上で、将来的には個人情報保護委員会ガイドラインなどで広く示すという方法が良いと考える。

３．おわりに

個人情報保護とデータ利活用の両立は重要な課題である。個人情報を取り扱われる本人の権利利益を十分に守りながら、企業に過負荷をかけずにデータ利活用を両立できるよう、よりわかりやすい個人情報の取扱いに改め、本人の権利利益が実効的に守られるよう、制度改善が求められるといえよう。

第３章　製薬企業における健康・医療情報の利活用に向けた課題と期待

アステラス製薬株式会社 渉外部渉外グループ課長

藤田　和也

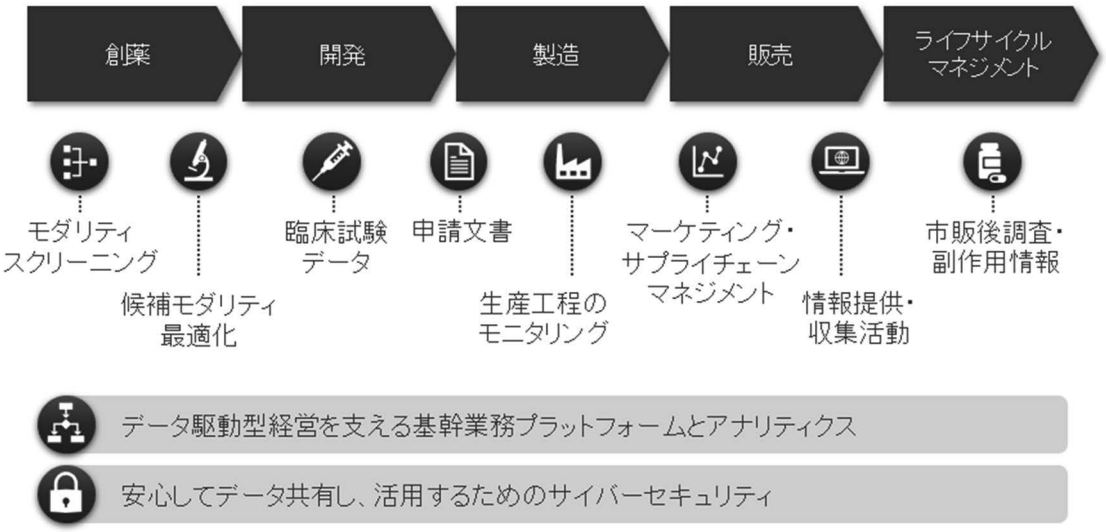
１．製薬企業における情報の利活用

（１）製薬産業は情報産業

研究開発型の製薬企業の使命は患者さんに革新的な医薬品をいち早く届けることである。医療用医薬品の研究開発においては、数百億円から 1,000 億円以上の多額の費用と、9 年から 16 年という長い期間が必要となる[*1]。また成功確率も非常に低く、低分子医薬品の場合、1 万分の 1 から 3 万分の 1 と言われている[*2]。この医薬品の研究開発の成功確率を高めて、研究開発の期間を短くし、患者さんに少しでも早く新しい医薬品を届けるとともに、効率的な医薬品の研究開発によって患者さんの負担を軽減するためには、様々な情報の利活用が鍵となる。

図表-1 に示したように、当社では、創薬、開発、製造、販売、ライフサイクルマネジメント、このバリューチェーンを通じて「価値」をつくり、届ける活動をしているが、現在では、このバリューチェーン全てにおいて膨大なデータを扱っている。

図表-1：アステラス製薬の各バリューチェーンにおけるデータの利活用



（２）製薬企業における健康・医療情報の利活用

製薬産業では、バリューチェーン全般にわたって、要配慮個人情報に該当する健康・医療情報の利活用も始まっている。各々のバリューチェーンにおいて、情報の活用目的と必要な情報は異なる。具体的には図表-2 に示したように、例えば、創薬研究においては、疾患発症メカニズムの解明や創薬標的・バイオマーカーの探索等のために、ゲノム・オミックス解析の情報や特殊な検査・画像の情報など、疾患固有の詳細な患者さんの情報が必要となる。また、臨床開発では患者さんのリクルートや試験の層別化デザイン等での利用を目的として、電子カルテのような標準化された質の高い医療情報が必要となる。一方で、市販後調査や医薬情報提供においては、研究や開発に求められるような詳細な情報は必要ないものの、医薬品の安全性・有効性情報の収集や最適な薬剤使用の検討のために、レセプトや DPC（診療群分類包括評価）のような、より多くの患者さんから集められた網羅的な医療情報が必要となる。さらに、これまでは病気になってからの治療が中心であったが、個人が生まれてから亡くなるまでのライフコース全般にわたり、様々な健康医療、介護支援のソリューションを開発し、提供するためには、PHR（パーソナルヘルスレコード）など、個人のライフコースにわたる情報の利活用が必要となる。

図表-2：製薬企業における健康・医療情報の利活用

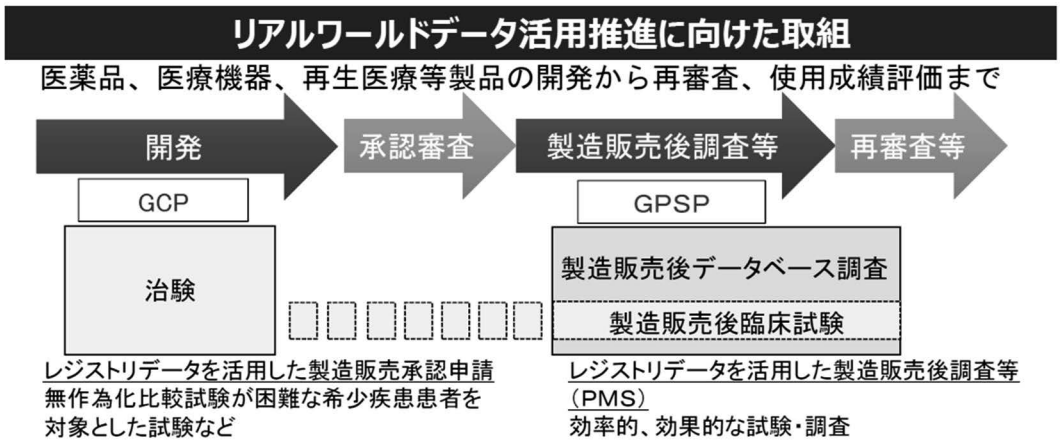
	必要な情報	主な活用目的
研究	疾患固有の詳細な患者さんの情報 ・ ゲノム・オミックス解析の情報 ・ 特殊な検査・画像等の情報	・ 発症メカニズムの解明 ・ 創薬標的の探索 ・ バイオマーカーの探索
開発	標準化された質の高い医療情報 ・ 診療結果、電子カルテ等	・ 患者リクルート ・ 試験デザイン（層別化） ・ 適応追加の検討
市販後調査	診療結果も含まれた医療情報 ・ レセプト、DPC、電子カルテ等	・ 安全性・有効性の検証 ・ 使用実態の把握
医薬情報提供	より多くの患者から集められた医療情報 ・ レセプト、DPC、電子カルテ等 （網羅的・悉皆的）	・ 疾患治療の深い理解 ・ 最適な薬剤使用の検討 ・ 診断・治療への貢献
他分野展開	目的に応じた多種多様な情報 ・ 個人の健康関連情報（PHR）等	・ 健康医療、介護支援のソリューション検討

レセプト：診療報酬明細書、DPC：診療群分類包括評価、PHR：個人健康記録

（注）出典：医薬産業政策研究所　医療健康分野のビッグデータ活用研究会報告書 Vol.3(2018 年 5 月)をもとに作成　【2022 年 11 月 28 日に利用】

より具体的な活用場面としては、図表-3 に示すように、研究対象をランダムに 2 つの群に分けて、治療などの介入を行う群と、プラセボ（偽薬）や標準治療を行う群とで、結果に差が出るかを比較する研究デザインである無作為化比較試験がある。この試験は、医薬品を上市する際には基本的に必要となる試験であるが、患者数が少ないために、無作為化比較試験が困難な希少疾患患者を対象とした治験においては、有効性や安全性の比較のための外部対象として、リアルワールドデータが医薬品の製造販売承認申請に活用できるようになっている。また、製造販売後調査へのリアルワールドデータの活用も始まっており、効率的、効果的な試験や調査が推進されている。当社でもリアルワールドデータを活用した製造販売後調査を実施している[*3]。

図表-3：製薬産業における健康・医療情報の活用場面



出典：健康・医療戦略推進本部ホームページ　第 2 回　医薬品開発協議会　資料 2-4
【2022 年 11 月 28 日に利用】
https://www.kantei.go.jp/jp/singi/kenkouiryou/iyakuhin/dai2/siryou2-4.pdf
注釈：GCP：臨床試験の実施の基準に関する省令に示された基準
GPSP：製造販売後の調査と試験の実施の基準に関する省令に示された基準

このように製薬企業は、健康・医療情報を活用することによって、医薬品の研究開発における患者さんの負担を減らすとともに、研究開発期間を短くすることで、患者さんに少しでも早く革新的な医薬品を届けようとしており、一部では既に具体的な取り組みも始まっている。

しかしながら、日本において、健康・医療情報を利用する際には、まだまだ課題も多く、障壁なく利活用できる状況にはないと考えている。詳細は次の章で説明する。

２．個人情報の利活用に向けた法制上の課題と期待

製薬企業が利用できる医療情報は、原則、同意をもとに入手したデータか匿名加工データに限定される。製薬企業は、基本的には、同意を取得して、医療情報を活用しているが、過去の医療情報を用いた研究を実施する際など、同意取得が困難な場合もあり、そのような場合には、利活用が十分に進んでいない。また、匿名加工情報については、その情報の性質上、医薬品の研究開発への利用は限定的である。以下に現状を整理して説明する。

（１）個人情報保護法における課題

①　同意の限界

製薬企業は直接患者さんから医療情報を入手する場合は少なく、医療機関が患者さんから入手した医療情報を二次利用することが多い。個人情報保護法においては、原則として、本人同意のない目的外利用や要配慮個人情報の取得、個人データの第三者提供を認めていないので、製薬企業は原則、医療機関が患者さんから同意をもとに入手した医療情報を利用することになるが、同意を得るための説明と同意取得を行う医療機関の手間や手続き等の負担は非常に大きいと思われる。このため、医療情報を利活用する際に同意を原則とすることには限界があると考えられる。個人情報保護法では、学術研究に係る例外規定や公衆衛生に係る例外規定など、あらかじめ本人の同意を得ないで、個人データを第三者へ提供することが許容されるケースもあるが、企業はこれらの例外規定を十分に活用するのは難しい状況にある。以下に現状を整理して説明する。

②　学術研究に係る例外規定

個人情報保護法では、学術研究機関等が学術研究目的で個人情報等を取り扱う場合は、一般の個人情報取扱事業者が遵守する以下の規制については、例外規定が適用される。

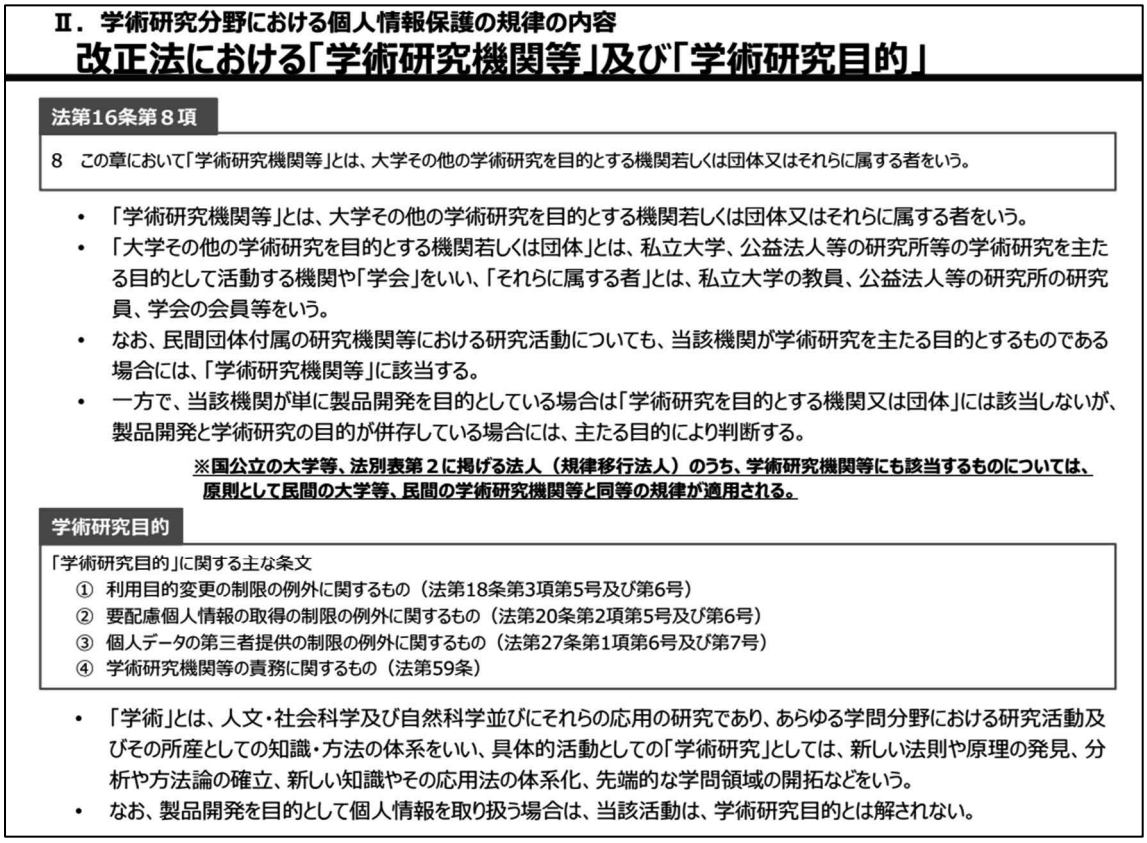
１．利用目的変更の制限に関するもの

２．要配慮個人情報の取得の制限に関するもの

３．個人データの第三者提供の制限に関するもの

しかしながら、この学術研究に係る例外規定は「学術研究を目的とする機関若しくは団体又はそれらに属する者」に限定されており、通常、民間企業や私立病院単独では、同様の研究を行う場合であっても例外規定が適応されない。このため、企業が単独で個人情報保護法上の学術研究に係る例外規定によって個人情報を入手して利活用することは難しい状況にある。

図表-4：学術研究分野における個人情報保護の規律の内容



出典：個人情報保護委員会ホームページ　第 176 回　個人情報保護委員会　資料 2　【2022 年 11 月 28 日に利用】
https://www.ppc.go.jp/files/pdf/210623_shiryou-2.pdf

また、「個人情報の保護に関する法律についてのガイドラインに関する Q&A」[*4] の Q11-6（大学等の学術研究機関等と民間企業や私立病院等が、学術研究目的の研究を共同で行う場合における個人情報の取扱いに関して留意すべき点を教えてください。）の回答（同 Q&A の A11-6）には、学術研究機関等と企業が学術研究目的の研究を共同で行う場合における個人情報の取扱いに関しても記載があり、学術研究機関等が共同研究を行う第三者（学術研究機関等であるか否かを問わない）に対して個人データを学術研究目的で提供する必要がある場合には、本人の同意を得ずに個人データを提供することが許容されている。

しかしながら、ただし書きとして、「ただし、当該共同研究の目的が営利事業への転用に置かれているなど、必ずしも学術研究目的とはみなされない場合には、提供に当たってあらかじめ本人の同意を得る必要があることに留意が必要です」という解釈に幅のある記載があり、学術研究機関等と企業の共同研究においても、企業が学術研究に係る例外規定によって個人情報を入手して利活用することは難しい状況にある。

③　公衆衛生に係る例外規定

個人情報保護法においては、公衆衛生の向上のために特に必要がある場合であって、本人の同意を得ることが困難であるときには、あらかじめ本人の同意を得ないで、個人データを第三者へ提供することが許容されている。

従来は、「公衆衛生の向上のために特に必要がある場合」の定義が曖昧であったが、同法の令和 3 年度改正によって整備された「個人情報の保護に関する法律についてのガイドラインに関する Q&A」の Q7-25 の回答（A7-25。図表-5 参照）においては、「一般に、製薬

図表-5：個人情報の保護に関する法律についてのガイドラインに関する Q&A

Q７－25　医療機関等が保有する患者の臨床症例について、有効な治療方法や薬剤が十分にない疾病等に関する疾病メカニズムの解明を目的とした研究のために、製薬企業へ提供することを考えています。本人の転居等により有効な連絡先を保有していない場合や、同意を取得するための時間的余裕や費用等に照らし、本人の同意を得ることにより当該研究の遂行に支障を及ぼすおそれがある場合は、本人同意なしに提供することは可能ですか。

Ａ７－25　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはなりませんが、公衆衛生の向上のために特に必要がある場合であって、本人の同意を得ることが困難であるときには、あらかじめ本人の同意を得ないで、個人データを第三者へ提供することが許容されています（法第27条第１項第３号）。

医療機関等は、あらかじめ患者の同意を得ないで、当該患者の個人データを第三者である製薬企業へ提供することはできません。

しかし、一般に、製薬企業が行う有効な治療方法や薬剤が十分にない疾病等に関する疾病メカニズムの解明、創薬標的探索、バイオマーカー同定、新たな診断・治療方法の探求等の研究は、その結果が広く共有・活用されていくことで、医学、薬学等の発展や医療水準の向上に寄与し、公衆衛生の向上に特に資するものと考えられます。

また、医療機関等が、本人の転居等により有効な連絡先を保有していない場合や、同意を取得するための時間的余裕や費用等に照らし、本人の同意を得ることにより当該研究の遂行に支障を及ぼすおそれがある場合等には、「本人の同意を得ることが困難であるとき」に該当するものと考えられます。

したがって、医療機関等が保有する患者の臨床症例に係る個人データを、有効な治療方法や薬剤が十分にない疾病等に関する疾病メカニズムの解明を目的とした研究のために製薬企業に提供する場合であって、本人の転居等により有効な連絡先を保有しておらず本人からの同意取得が困難であるときや、同意を取得するための時間的余裕や費用等に照らし、本人の同意を得ることにより当該研究の遂行に支障を及ぼすおそれがあるときには、同号の規定によりこれを行うことが許容されると考えられます。

なお、当該製薬企業においては、提供を受けた際に特定された利用目的の範囲内で個人データを取り扱う必要があり、上記研究のためという利用目的の達成に必要な範囲を超えて、提供を受けた個人データを取り扱うことは原則できません。また、法第27条第１項第３号の規定において個人データを提供できるのは「特に必要がある場合」とされていることからも、当該医療機関等が提供する個人データは、利用目的の達成に照らして真に必要な範囲に限定することが必要です。具体的には、利用目的の達成には不要と考えられる氏名、生年月日等の情報は削除又は置換した上で、必要最小限の情報提供とすることなどが考えられます。

この外、医療機関等及び製薬企業には、倫理審査委員会の関与、研究対象者が拒否できる機会の保障、研究結果の公表等について規定する医学系研究等に関する指針や、関係法令の遵守が求められていることにも、留意が必要です。

（令和３年６月追加・令和４年５月更新）

出典：個人情報保護委員会ホームページ　個人情報の保護に関する法律についてのガイドラインに関する Q&A　【2022 年 11 月 28 日に利用】
https://www.ppc.go.jp/personalinfo/faq/APPI_QA/

企業が行う有効な治療方法や薬剤が十分にない疾病等に関する疾病メカニズムの解明、創薬標的探索、バイオマーカー同定、新たな診断・治療方法の探求等の研究は、その結果が広く共有・活用されていくことで、医学、薬学等の発展や医療水準の向上に寄与し、公衆衛生の向上に特に資するものと考えられます」と記載された。これによって、企業が行う医薬品の研究開発が公衆衛生に資するということが明記されたと認識しており、個人情報の利活用の推進に向けた大きな一歩であったと考える。

一方で、企業では多種多様な研究を行っていることから、研究対象である「製薬企業が行う有効な治療方法や薬剤が十分にない疾病等に関する研究」や「本人の同意を得ることが困難であるとき」の定義について、企業として判断が難しい状況も依然としてある。また、企業では公衆衛生に係る例外規定が厳格に運用されており、企業が公衆衛生に係る例外規定によって個人情報を入手して利活用することは、現状では十分には進んでいない。

（２）次世代医療基盤法における課題

企業が医療情報を利用するもう一つの方法として、匿名加工された医療情報を利用するという方法がある。2018 年に健診結果やカルテ等の個々人の医療情報を匿名加工し、医療分野の研究開発での活用を促進する法律として、次世代医療基盤法（正式名称：医療分野の研究開発に資するための匿名加工医療情報に関する法律）が施行された。詳細は図表-6 に示したが、次世代医療基盤法は、医療情報の第三者提供に際してあらかじめ同意を求める個人情報保護法の特例法であり、一定の要件を満たすオプトアウト（あらかじめ通知を受けた本人又はその遺族が停止を求めないこと）により、 医療機関等から認定事業者へ医療情報を提供することができ、また、認定事業者から利活用者へ匿名加工医療情報を提供することができるというものである。

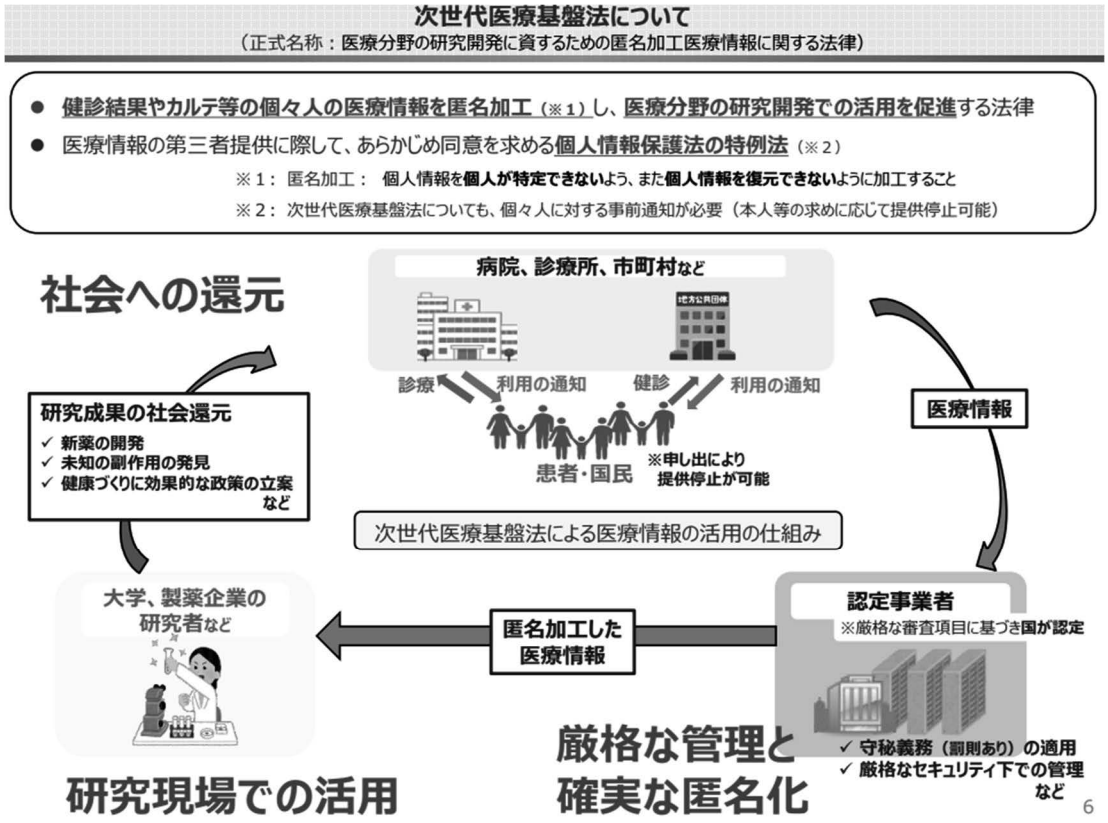
しかしながら、認定事業者の利用実績を確認すると、実際にはその利用は限定的な状況である。以下のような理由から認定事業者から提供される匿名加工医療情報は、医薬品の研究開発には十分に活用できていないと考えている。

・希少な症例など、研究開発を行う際の重要な医療情報項目は削除される
・同一対象群に関する継続的・発展的なデータ提供が困難である
・個人識別符号に該当するゲノムデータは匿名加工できないので、法の対象外となる

現在、次世代医療基盤法検討ワーキンググループにおいて、制度の見直しについて検討されており、仮名加工医療情報の利活用に係る新たな枠組みの創設の方向性が示されていることか

ら*5、上記課題のいくつかは解決に向けて検討が進んでいるようであるので、期待したい。

図表-6：次世代医療基盤法について

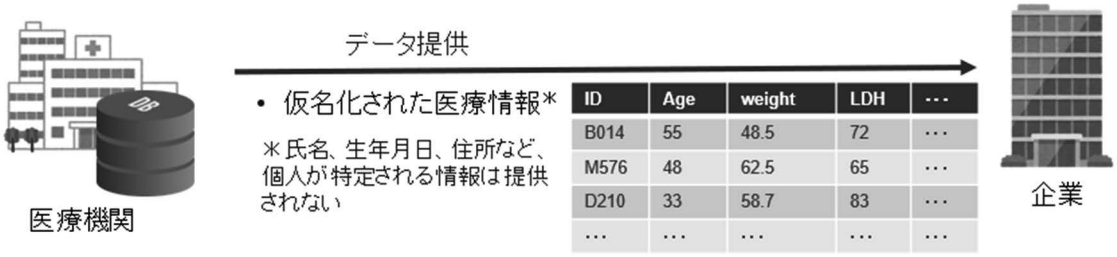


出典：内閣府ホームページ　次世代医療基盤法　制度の概要　次世代医療基盤法とは-印刷版　【2022 年 11 月 28 日に利用】
https://www8.cao.go.jp/iryou/gaiyou/pdf/seidonogaiyou.pdf

（３）期待する姿

製薬企業において医学研究や創薬を行う際には、多くの場合必要となるのは、図表-7 に示したように、「顕名」の医療情報ではなく、氏名等を削除することで仮名化された医療情報である。しかしながら、（１）に記載した理由から、仮名化を行ったとしても、あらかじめ本人の同意を得ない限り、原則として、特定された利用目的の達成に必要な範囲を超えた利用や第三者提供を行うことはできない。また、個人情報保護法の令和２年改正によって「仮名加工情報」が創設され、利用目的の変更が許容されるようになったことは画期的であると考えるが、内部利用に限定され、第三者提供はできないため、薬事申請等に活用できないなどの課題もあり、医薬品の研究開発への活用は限定的である。

図表-7：共同研究における製薬企業の患者さんの医療情報の入手について



ID	Age	weight	LDH	…
B014	55	48.5	72	…
M576	48	62.5	65	…
D210	33	58.7	83	…
…	…	…	…	…

以上のことより、同意原則の入口規制から、同意を必要としない代わりに信頼できる第三者機関で適切な利用審査を実施する出口規制に変えていくことが、患者さんの保護にもつながり、重要と考えている。企業が医薬品の研究開発の目的に利活用する際には、本人が識別されないように適切に仮名化した医療情報を、第三者機関による利用目的の審査の下、情報の活用状況に関する本人への透明性を確保したうえで、必ずしも本人の同意によらなくても、オプトアウト等で利用できるような制度が整備されることを期待する。

３．健康・医療情報のデータ基盤の課題と期待

（１）健康・医療情報のデータ基盤に関する課題

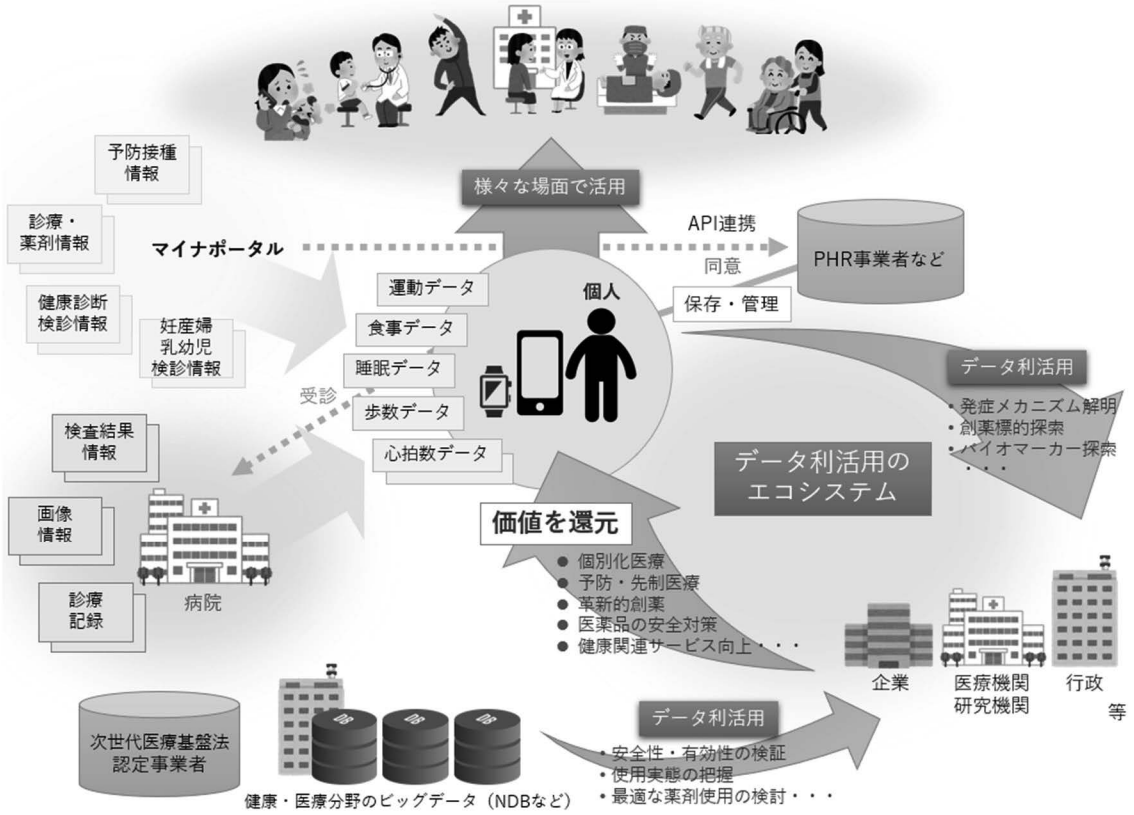
2020 年に本格的に流行が始まった COVID-19 は日本の健康・医療情報基盤の課題を浮き彫りにした。例えば、個人と保健所や医療機関、医療機関同士の連携が、電話等のアナログな手法で行われ、緊急時にも手間と時間がかかっていた。また医療機関間のデータ連携が不十分なために、いつも受診している医療機関とは異なる医療機関を受診した際には、再度検査が行われる場合などもあり、医師や患者さんの手間がかかるうえに、医療費削減の観点からもデータ連携は大きな課題である。このような課題を解決するためには、個人を起点にしてライフコースにわたる情報を管理し、各組織と連携することが重要であると考える。

個人起点のヘルスケア分野の健康・医療情報の活用を進めるための鍵は、個人が生まれてから亡くなるまでのライフコース全般にわたるデータを蓄積し、個人による閲覧や、医療機関との共有を可能とする仕組みのパーソナルヘルスレコード（PHR）である。次頁の図表-8 に、健康・医療情報の利活用のイメージを示す。

政府が推進しているデータヘルス改革[*6] のもと、健診データや薬剤データなど様々な健康・医療情報が既にマイナポータルで閲覧できるようになっている。このことは健康・医療情報の利活用に向けた大きな一歩であると思うが、現状では、電子カルテの情報はマイ

ナポータルで閲覧することはできず、医療機関から本人が取得する必要がある。

図表-8：健康・医療情報の利活用のイメージ



加えて、医療機関で取得された医療情報は医療機関において管理されており、本人であっても自身の情報にアクセスすることは容易ではなく、自身の医療情報を他の医療機関における治療・診断等に活用することにも、依然として障壁がある。

また自分自身の健康・医療情報を、個人を起点として、本人同意のもとで、企業も含めた様々な主体が適切に二次利用できるような仕組みの整備も不十分であり、図表-8 に示したような健康・医療情報活用のエコシステムの構築は進んでいないと認識している。

（2）期待する姿

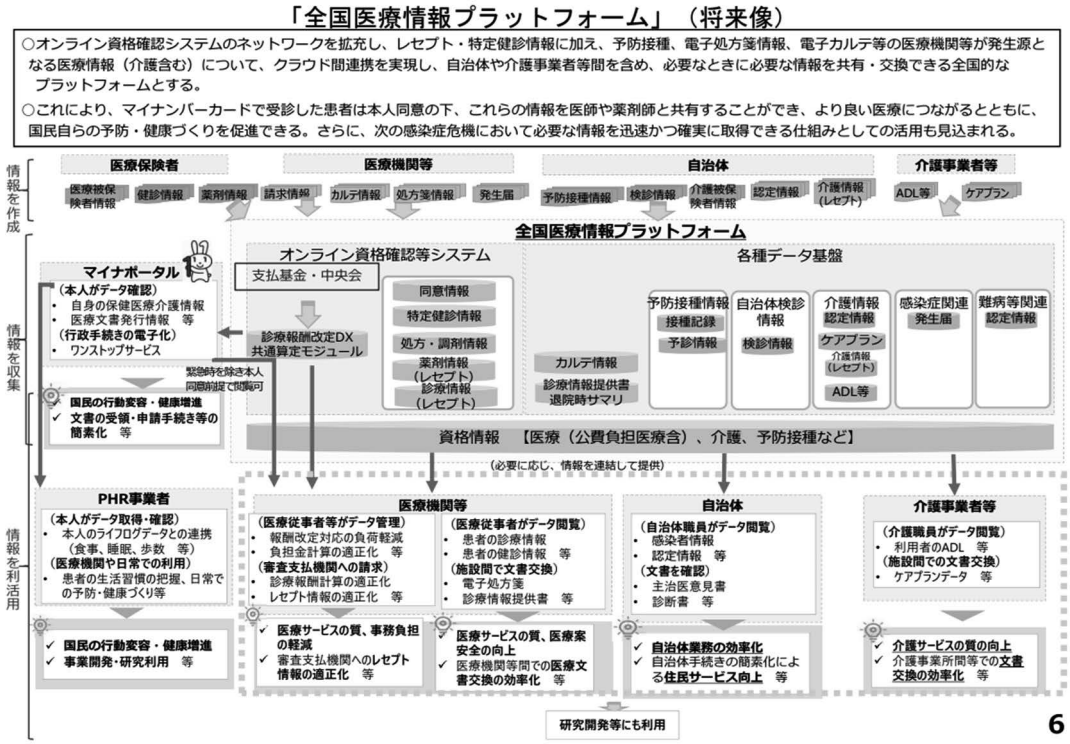
まずは、自らの医療情報へのアクセスの改善に向けて、電子カルテ情報を含む医療情報をマイナポータルで閲覧できる基盤整備については、政府で推進されているデータヘルス改革の工程表[*6]にも記載があるが、早期に実現することを期待する。

次に、自らのマイナポータルに集まってきた健康・医療情報を、API（Application

Programming Interface）を通じて民間 PHR 事業者などへ連携するなど、自らの健康・医療情報を自らコントロールして利活用できるような権利やデータ基盤などの仕組みの整備が進むことを期待する。

2022 年 9 月に発足した「医療 DX 令和ビジョン 2030」厚生労働省推進チームの第 1 回目の会議資料には、図表-9 に示した全国医療情報プラットフォームの構築が示されている。このプラットフォームは、レセプト・特定健診情報に加え、予防接種、電子処方箋情報、電子カルテ等の医療機関等の医療情報について、クラウド間連携を実現し、自治体や介護事業者等間を含め、必要なときに必要な情報を共有・交換できる全国的なプラットフォームである。この仕組みにより、マイナンバーカードで受診した患者さんは本人同意の下、これらの情報を医師や薬剤師と共有することができ、より良い医療につながるとともに、 国民自らの予防・健康づくりを促進できる仕組みになっている。本人同意のあり方については実効性のある運用を検討する必要があると考えるが、このプラットフォームが迅速かつ確実に整備されることを期待する。

図表-9：全国医療情報プラットフォーム



出典：厚生労働省ホームページ　「医療 DX 令和ビジョン 2030」厚生労働省推進チーム　第 1 回 資料 1【2022 年 11 月 28 日に利用】
https://www.mhlw.go.jp/content/10808000/000992373.pdf

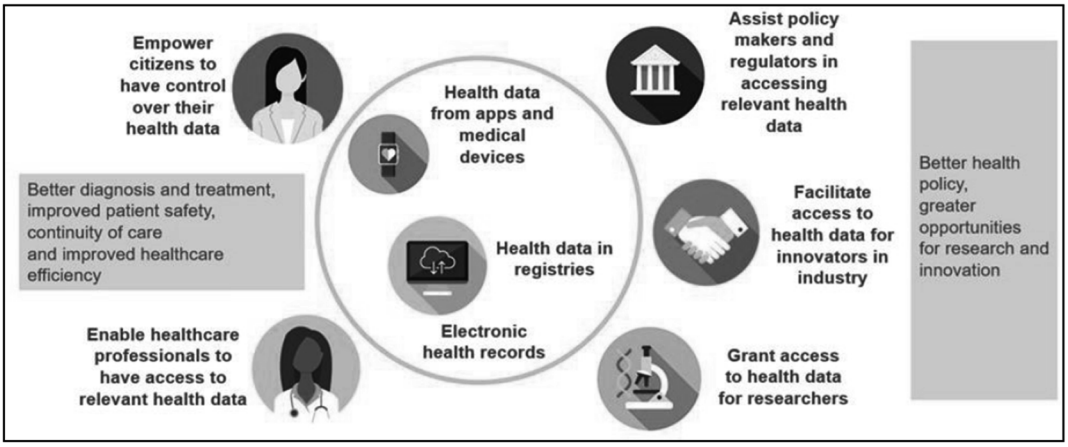
４．European Health Data Space（EHDS）について

健康・医療情報の利活用は、国民により良い医療を提供するだけでなく、将来の医学の発展にも不可欠なものであることから、利活用の推進に向けて海外でも取り組みが進んでおり、EU では 2022 年 5 月に欧州でのヘルスデータを安全に利活用と共有するための仕組みである European Health Data Space（EHDS）法案の概要が公表された[*7]。

この EHDS においては、一次利用として個人が自身のヘルスデータにアクセスできるだけでなく、自身が選択した医師が自身のヘルスデータへアクセスできるようにする権利を有する仕組みになっている。

また二次利用としては、研究、イノベーション、公衆衛生、政策立案、規制活動、個別化医療のために、本人が識別されない形に加工されたヘルスデータを、ヘルスデータアクセス機関による活用目的の審査の下で、本人同意なしで、オプトアウトで利用できる仕組みが提案されている。日本の個人情報保護法でも例外規定が認められている公衆衛生のためだけではなく、イノベーションを目的とするヘルスデータの利用も本人同意なしで認められていることが画期的である。

図表-10：EHDS について



出典：COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Strasbourg, 3.5.2022 COM(2022) 196 final （Publication date 3 May 2022）,p.13, https://health.ec.europa.eu/publications/communication-commission-european-health-data-space-harnessing-power-health-data-people-patients-and_en. © European Union, 1995-2022, Created by Directorate-General for Health and Food Safety. 【2022 年 11 月 28 日に利用】

一方で、データ基盤に関しては、ヘルスデータの二次利用のための新しい分散型インフラ（HealthData@EU）の創設が提案されており、ヘルスデータの二次利用を希望する場

合は、ヘルスデータアクセス機関に利用許可を申請し、データ活用の目的などを審査される仕組みが考案されている（出典：COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Strasbourg, 3.5.2022 COM(2022) 196 final(Publication date 3 May 2022）,p.9-11, https://health.ec.europa.eu/publications/communication-commission-european-health-data-space-harnessing-power-health-data-people-patients-and_en. ©European Union, 1995-2022, Created by Directorate-General for Health and Food Safety.）。

日本においても EHDS を参考に、同意原則の入口規制から、同意を必要としない代わりに利用審査を行い、オプトアウトもできるようにする出口規制に切り替えて、個人が自分自身の健康・医療情報をコントロールできる権利を確保しながら、一次利用・二次利用に活用できるような法制度とデータ基盤が整備されることを期待する。

５．健康・医療情報の利活用に対する理解醸成について

健康・医療情報の利活用を推進するためには、大前提として、健康・医療情報の利活用に対する国民の理解醸成が必要であり、そのためには国民が、健康・医療情報の持つ意義や可能性を十分認識・理解することが重要になる。

個人がプライバシーを制御しつつ、自身の健康・医療情報をコントロールできるようになれば、自身の健康管理・予防・未病対策に活用できるほか、企業等における活用も含めて自身で検討・判断することで、健康・医療情報の利活用に対するコンピテンシーの向上も期待できる。また国民が、健康・医療情報の利活用によって創出された新しい製品やサービスの恩恵を受けることによって、国民一人ひとりの情報の提供に対するインセンティブも高まり、それに基づく健康・医療情報の利活用が、さらに新たな製品・サービスの開発・実装につながっていくというエコシステムの構築が期待できる。

また、健康・医療情報の利活用に対する国民の理解醸成に向けては、産学官医が連携して具体的な活動を推進していくことが必要であり、シンポジウム開催などの国民啓発活動も有用であると思われる。さらに中長期的には、国民が健康・医療情報の利活用の意義を正しく理解できるように、初等中等教育の強化も重要であると考える。

６．まとめ

製薬企業の使命は革新的な医薬品を患者さんに早く届けることである。様々な健康・医

療情報を活用することで、医薬品の研究開発を効率化することができ、治験に参加する患者さんの負担を軽減できるとともに、研究開発の期間を短くし、患者さんに少しでも早く医薬品を届けることができる。製薬企業が実施する新薬の研究開発は、ビジネスと完全に切り離すことは難しいものの、必要とされる患者さんに早く新薬を届け、また新しい治療法の開発、ひいては日本の医療の発展につながる活動であり、そのための健康・医療情報の活用は患者さんをはじめとする様々なステークホルダーに価値を提供できるものと考えている。日本において、健康・医療情報の利活用の推進に向けて、法制度やデータ基盤の環境が整備されることを期待する。

参考文献・資料

*1：日本製薬工業協会　製薬協ガイド　2022　【2022 年 11 月 28 日に利用】
*2：日本製薬工業協会　DATA BOOK 2022　【2022 年 11 月 28 日に利用】
*3：医薬品医療機器総合機構　スーグラ錠 25mg,50mg に係る　医薬品リスク管理計画書【2022 年 11 月 28 日に利用】
https://www.pmda.go.jp/RMP/www/800126/99381dc5-3a82-4336-aeba-912ccd0305a8/800126_3969018F2029_016RMP.pdf
*4：個人情報保護委員会　個人情報の保護に関する法律についてのガイドラインに関するQ&A【2022 年 11 月 28 日に利用】
https://www.ppc.go.jp/personalinfo/faq/APPI_QA/
*5：健康・医療戦略推進本部ホームページ　健康・医療データ利活用基盤協議会　第 7 回次世代医療基盤法検討ワーキンググループ　資料 1【2023 年 2 月 21 日に利用】
https://www.kantei.go.jp/jp/singi/kenkouiryou/data_rikatsuyou/jisedai_iryokiban_wg/dai7/siryou1.pdf
*6：厚生労働省ホームページ　データヘルス改革推進本部　データヘルス改革に関する工程表【2022 年 11 月 28 日に利用】
https://www.mhlw.go.jp/content/12601000/000788259.pdf
*7：European Commission ホームページ
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0197&from=EN
【2022 年 11 月 28 日に利用】

第４章　Society 5.0 時代のデータに関する本人の権利とデータプライバシーの保護のあり方について

Ｚホールディングス株式会社　GDPO 部長

小柳　　輝

１．はじめに

今時代は大きな変革期を迎えている。20 世紀後半から始まった情報社会はこれまでにないスピードで進展し、AI をはじめとした革新的なデジタル技術が大きく飛躍した現在においては、人々がその生活の全般にわたってデジタル技術と共に歩む時代になっている。そして、これら新たなデジタル技術の原動力となっているのがデータである。

新たな時代、Society 5.0 では、情報社会が追求した利便性や効率性の実現からさらに一歩前に進み、人間中心の社会を実現していくことが求められる。経団連では、Society 5.0 とは、「創造社会であり、『デジタル革新と多様な人々の想像・創造力の融合によって、社会課題を解決し、価値を創造する社会』」[1]としている。

筆者は、2020 年 5 月から 2022 年 9 月までの約 2 年半にわたって、ヤフー株式会社（以下「ヤフー」という）において Data Protection Officer（データ保護責任者。以下「DPO」という）を担当し、また、2020 年 10 月から現在まで、Z ホールディングス株式会社においてグループ内の事業会社におけるデータプライバシーの保護を担当しており、本稿では、新たな時代において企業が求められるデータプライバシーの保護のあり方について、新たな時代における本人の権利のあり方との関係でみていくこととしたい。

２．デジタル技術の進展がデータプライバシーに与える影響

Society 5.0 は人間中心の社会である。この基本的な考え方は、新たな時代のデータプライバシーの保護のあり方を考えるうえでも極めて重要である。新しい時代においては、人々はこれまでよりも大きなデータプライバシー上の脅威に晒され得ることとなる。「時代が変わった」と言われるほどのインパクトのある変化を前にして、企業に求められるデータプライバシーの保護は、前の時代のそれとは質的に異なることとなるのはある意味

[1] 経団連「Society 5.0 ―ともに創造する未来―」
https://www.keidanren.or.jp/policy/society5.0.html

当たり前のことである。

そこで、現在のデジタル技術の進展がデータプライバシーにどういった影響を及ぼしているのかということについて、いくつか例を挙げてみていくこととしたい。

（1）技術の進歩一般がもたらす影響

データを原動力として実現する技術の進歩は、そもそも一般的にデータプライバシーへの影響を内包する可能性が高い。そして、技術の進歩は全く新しい何かが生まれるというより、既存技術を新たに組み合わせたり、拡張したり、他分野へ応用したりして生じるケースが多い。そして、このようにして生まれた「新たな技術」は、データプライバシーへの影響について、企業の目線からは「既存技術の延長線上のもの」としてとらえられがちである。

たとえば、行動履歴を分析してサービスのリコメンドをすることと、行動履歴を分析してスコアリングサービスを提供することは、分析対象となるデータに量的な差はあれど、技術的にやっていることはほとんど変わりがない。もともとこのようなリコメンドを行っていた企業からすれば、「もうすでにやっていること」であり、「約款のここで読み込めるもの」という状況が生じる。

しかしながら、分析対象となるデータの主体（以下「本人」という）の側からすれば、リコメンドとスコアリングでは自身への影響が全く異なり、「さすがに別のものである」と評価されるのではないか。企業の活動は営利を目的とするものであり、とかくその現場においては「できる根拠を探す」という方向に思考が行きやすく、まさに「約款のここで読み込めるからできる」といった考えに陥りやすい。企業内において、本人の側に立ってデータプライバシーへの影響を分析し、それが本人や社会から受け入れられるものであるのかということを冷静に判断できなければ、社会から受け入れられてサービスを提供することはできず、ときには大きな炎上に発展し、場合によっては行政指導を受けたり、今の規律が適切なのかという議論を呼んだ結果、法改正に至ったりすることすらあり得る。企業においては、新たな技術が既存技術の延長線上にあるからといって、データプライバシーへの影響がその延長線上にあるとは限らないということについて、十分な留意が必要である。

また、これまでにないスピードで技術の進歩が生じている現代において、本人が新たな技術による影響を正しく理解することに期待することにはそもそも無理がある。上記の例でいえば、「約款のここで読み込める」のかどうなのかということすら、本人には判断

がつかないという状況が生じている。このような状況では、これまでの延長線上で企業がユーザーに対して求められるコミュニケーションを考えるというのはもとより不適切である。Society 5.0 の実現によって多くの社会課題が解決され、人々の生活がより豊かになることについて社会からの期待は非常に大きい。企業はその担い手として、これまでとは全く次元の異なる透明性と説明責任、そして自らの振る舞いがユーザーや社会から受け入れられるものであるのかということについて冷静に判断し、その結果を具体的行動に反映していく倫理観が求められている。

（２）データの蓄積と計算能力の向上がもたらす影響

デジタル技術の進展は、それまでとは桁違いな大量のデータの蓄積と計算を可能にした。現代において人々の行動は細かく記録され、それが分析可能な状況になっていることは周知のとおりである。

ところで、ある人に関する情報が蓄積されていった場合何が起きるのであろうか。たとえば、「A さんが何月何日に〇〇にいた」というデータと、「何月何日、A さんは朝〇時に起きて、まず電気をつけてそのあとポットのスイッチを入れ、お湯が沸くのを待っている間にテレビをつけて…」というデータでは相当程度質が異なるということは論を俟たないであろう。ある人に関するデータは、網羅性が高まれば高まるほど、その人の実態を鮮明に浮かび上がらせることになる。網羅性の高いデータは、「その人そのもの」に近づいて行ってしまい、それにはつまり、その人の人格が投影されているということである。

このように考えると、自らのユーザーや株主などのステークホルダーをはじめとする社会が、企業のデータプライバシーの保護に対して日に日に厳しい目を向けるようになってきていることは極めて合理的であると理解できる。企業が新しい時代において分析しようとしているのは人々の人格なのであるということについて、深い自覚をもつことが必要である。また、このことは一昔前にあった「データは誰のものか」という議論が、新しい時代においてはもはや成り立たないということを明らかにする。人格を投影するものである以上、本人を中心として考え、本人がどのような権限をもち、企業はどのように利用することが許されるのか、という思考にならざるを得ない。

さらに、新しい時代においてはデータが人格を表すものであるという前提にたつと、企業のデータに関する同意取得やその前提となる説明は、本人からの人格的利益の処分を求めるためのものであるということになる。そして、これらの具体的あり方を検討するの

に重要なのは、本人の予期には限界があり、その処分が有効である範囲はあくまでもその予期の範囲でしかあり得ない、という点である。また、さらにいえば、そもそもその処分を求めることのできる限界がどこであるのか、ということについても検討する必要がある。新しい時代において企業は、すでに起きている「ゲームチェンジ」を適切にとらえ、求められているデータプライバシーの保護をより一層真剣に考え、実現していかなければならない。

（3）オンラインとオフラインの融合がもたらす影響

オフラインの社会、ここでは対面の社会についてオフラインの社会とするが、オフラインの社会においては、通常、人は置かれている状況や対する相手によってどうふるまうのか、相手にどのような情報を与えるのかということを選択している。他方で、オンラインの社会においてはどうであろうか。確かに、オンラインにおいても自らが参加しているコミュニティのような場においては、当該コミュニティ参加者の誰にどの情報を与えるのかということの選択はできている部分もあるが、対企業ではこれがある意味で崩壊しているのではないか。

オフラインでの買い物の場合、通常私がどこの誰であるのかということは、よっぽど近所の常連でもない限り店員は知っているわけではない。私がどういう興味や動機をもってある店を訪れ、商品の何に重要性を見出しているのかというようなことは、私が店員に伝えない限り、店員は知る由もない。ところが、オンラインの買い物の場合、私がどこの誰であるかはもちろん、今何に興味をもっていそうで、買い物かごに何が入っていて、何は検討したけれども候補から除外した、ということがすべて分かっている[2]。オンラインとオフラインでは、現実問題として、ある人に関する情報について主導権をもつ者が正反対になっているという状況が生じている。このことについて、社会から一定程度許容されたものであるとするとしても、オンラインとオフラインが融合するといわれている Society 5.0 の新しい時代において、オンラインのトレーサビリティを介してオフラインにおける情報の紐づけが強まった結果、現状のオンラインにおける状況がオフラインでも生じる、つまり、オフラインにおいても、自己の情報の他者への開示に関する選択が事実

[2] このことは、オンラインでは機械的な処理がされているということが社会から一定程度受け入れられている根拠になっているものと思われる。他方で、新しい時代においては、データが人格を表すものであることは前述のとおりであり、機械的な処理であれば問題がないという根拠にはならない点に留意が必要である。

上困難になるようなことが生じかねず、そしてそれを果たして我々の社会は許容するのであろうか、ないし、どこまで許容するのであろうか。

自己をどのようなものとして認知し、それを前提に自己がどのようなものとして他者から認識されたいのかについて自己決定できること、そして、具体的な自己に関する他者の認識に関与するための方法として、自己に関するどの情報を、いつ、誰に、どのように開示するのか自己決定できることというのは、人が保護を求める極めて基本的な利益である。オンラインとオフラインが融合することで、企業は多くの領域で今まで以上の便利さやお得な体験を提供することができるようになることは疑う余地もないが、他方で、Society 5.0 時代のオンラインとオフラインの垣根を超えたデータの利活用は、やり方を間違えると人々の人格的利益への新たな挑戦にもなりかねず、企業が十分かつ適切な配慮をしながら進めなければ到底社会から受け入れられるものではないという点について、企業はしっかりと留意しなければならない。

（４）統計データが個々人に与える影響、個人に対する評価が同じ属性をもつ他者にもたらす影響

現状においては、一般的に、統計は自由に使えるものであるという認識が、少なくとも企業の中では広く共有されているものと思われる。しかし、データが人格を表すものとして存在していることを前提にすると、明確にこれは懐疑的に見るべきである[3]。

問題は、「統計によっても、同じ属性をもつことが分かっている他者に対しては影響を及ぼす、他者に対して新たな属性を付与する契機になり、新たな属性を付与されることによって、自己の評価や権利利益に影響が及び得る」という点で、企業はこの点を直視すべきである。

さらに問題を深刻にするのは、このことが、「いくら自己のデータの他者による取り扱いについて本人が気を付けていたとしても、本人は他者の自己に関する認識に対して、満足のいく関与をすることができなくなる可能性があること」を示している点である。統計は万能ではなく、いつまでも「統計の神話」の上に胡坐をかいていては、「この企業はデータプライバシーに適切な配慮をしていない」というように、いつか足元をすくわれることになりかねないという点について十分認識し、統計を慎重に扱うことが求められる。

---

[3] そもそもの問題として、実態として、企業において「統計」というものが統一的な定義をもって扱われているかといえば全くそのようなことはないと思われるが、それについてはここでは触れない。

統計が万能ではないという点について1つ具体的な例を挙げるとすると、ヤフーにおいて2020年4月に行った「新型コロナウイルス感染症のクラスターの早期発見のための政府への情報提供」の例がある。

新型コロナウイルス感染症（以下「新型コロナ」という）の感染拡大を受け、政府は、2020年3月に「新型コロナウイルス感染症の感染拡大防止に資する統計データ等の提供の要請」[4]を行った。当時は、クラスターの発生を封じ込めることが感染拡大防止のために重要であるとされており、ヤフーにおいてもその保有するデータを分析して、クラスターの早期発見に資するデータを作成、政府に対して提供できないか検討しており、検索データと位置情報等を利用して、一定の精度をもって「クラスターが発生している可能性のあるエリア」を示す「統計データ」が作成可能であることを確認していた。

しかしである。このデータを統計データであるからといって、手放しに利用や提供して良いのかという点について十分に考慮しなければ、データを扱う会社としてその責任を全うすることはできない。なぜならば、この統計データは、ある特定のエリアにおいて新型コロナのクラスターが発生している可能性が高いことを示すデータであり、その影響は、統計データを作成するためにデータを提供いただいた方々以外にも影響を及ぼす。たとえば、東京都〇〇区△△一丁目周辺でクラスターが発生している可能性が高いという分析結果であった場合、それによる影響は、〇〇区△△一丁目に関係のある人々全体に及ぶ。そこに住む人もいれば、そこに職場がある人もいて、そこに関わらないでいることのできない人がいる。仮にこれが統計だから問題ないとして何ら制限なく利用や提供された結果、これが公表されたら何が起きたであろうか[5]。そこに住む人は学校に通うことができるか、会社に通勤できるか。そこには要介護者がいるかもしれない。当時の状況では、介護を行う人が怖くなってしまい訪問介護ができなくなってしまうということはあり得ない話ではない。そして、その結果要介護者が死亡してしまったようなケースが生じないとも限らないのである。

統計は誰の情報であるかはわからないが、統計の元データになった人と、そうでなくとも同じ属性をもつ誰かに影響を与え得る情報なのであり、それへの適切な配慮が求められるのである。

なお、新型コロナのクラスターの早期発見のための政府への情報提供について、ヤ

4 https://www.meti.go.jp/press/2019/03/20200331017/20200331017.html
5 実際、ヤフーに対してクラスターの情報は公開すべき、というご意見も頂戴していた。

フーにおいては、統計データの元データを提供いただく方からは同意を取得し、また政府との間では、統計データの利用目的を制限して公表は禁じ、提供するデータの内容はヤフーが任意に決定すること、ヤフーは任意に統計データの提供を停止できることを求め、政府に対して国民に不安や疑念が生じることのないよう国民に対して積極的な情報発信等必要な措置を継続的に実施すること、データの活用による影響に適切に配慮すること、その利用の成果を公表することなどを求める協定書を締結して実施した。また、協定書においては、透明性確保のために協定書の内容を公表することも求めた[6]ほか、統計データの元データを提供いただく方からの同意取得にあたっては特設ページを開設し、データ提供の目的等について詳細な説明を行った[7] [8]。

３．企業に求められる対応

新しい時代ではデータを原動力として新たな技術が生まれる。ユーザーに安心してデータを預けてもらって利用させてもらえなければ、企業はそもそも新しい時代における競争のスタートラインにすら立つことができない。Society 5.0 の時代において、企業がデータの取り扱いについてユーザーや社会からの信頼を失うことは、極めて大きな経営上のリスクになる。他方で、これまで見てきたように、新しい時代においてはデータの利活用にあたって非常に多岐にわたる配慮が求められ、「こういう時にはこのようにする」というようなマニュアル的な思考はもはや一切通用しなくなっている。企業は、ユーザーや社会の現在に寄り添い、その期待や予期を敏感に感じ取って自らの行動がどう評価されるのか冷静かつ客観的に考え、それを前提に自らの行動を律していかなければならない。このような状況において企業が取り得る唯一の手段は、適切なプライバシーガバナンスを構築することである。

その際に留意しなければならないのは、問題になっている事柄が「ユーザーから受け

---

6 https://about.yahoo.co.jp/pr/mhlw_agreement_20200413.pdf

7 https://privacy.yahoo.co.jp/notice/202004.html

8 なお、政府への情報提供に関してはもう 1 つ考慮すべき事項があった。それは、「政府と市民社会は一定の緊張関係の下になければならない」ということである。歴史を紐解けば、非常時への対応や公衆衛生上の必要を理由として政府が市民社会に情報の提供を求め、それがいつしか恒常的なものとなったり当初の範囲から広がったりすることとなり、結果的に一定の属性を有する者に対する不当な弾圧のためにそれらが用いられてきたということは否定しがたい事実であり、まさに新型コロナの感染拡大初期は非常時であり公衆衛生上の必要がある状況にあった。厚生労働省をはじめとする政府がそのようなことをするとは思っていないわけではあるものの、ヤフーの対応が悪しき前例となり、政府と市民社会の緊張関係を崩壊させる「蟻の一穴」になることは何としてでも避けなければならなかった。

入れられるのか」というような主観的な要素に関わるものであるという点である。求められているのは、社会との対話の中で得た感覚を頼りに、目の前の取り組みを適切に分析してリスクを掬い上げ、それを経営判断のための情報として提供することのできる仕組みづくりである。このような仕組みは、当然ながら自然発生的に生じるものではあり得ず、企業は仕組みとしてこれを担保する仕掛けを「意識的に」組み込んでいかなければならない。そしてその上で、そういった仕組みを組み込んで適切な対応を取っていることについて、客観的に説明可能である必要がある。

このような客観的に説明可能な仕組みとして筆者が極めて有効であると考えているのが DPO によるデータ利活用の監視とデータの取り扱いに関する意思決定にあたっての助言の提供のプロセスである。

（１）設置が求められる DPO とは

DPO とは、欧州一般データ保護規則（GDPR）において一定の種類のデータを大規模に処理する者などに設置が義務付けられているものであり、独立した立場から法令や自らが定めるデータ保護の方針の遵守状況の監視等の業務を行う者とされている。他方で、Society 5.0 時代に求められているのは、上記のとおり法令や既存のルールへの適合性だけでなく、自らのデータに関する取り組みが「ユーザーから受け入れられるのか」という点に対する冷静かつ客観的な評価を踏まえた意思決定である。したがって、新しい時代の企業における DPO は、この点に関する役割についても担うことを明確にしておく必要がある。

（２）DPO 設置の際の留意点

新しい時代の企業における DPO についてもう少し詳細にその役割等に触れると、DPO は、企業内にいながら、事業部門はもとより、データプライバシーの保護やセキュリティの戦略を立案し実施する部門など、企業内のデータを扱い、または、その取り扱いについて何らかの決定を行う部門から独立した立場にあり、その取り扱いやこれに関する決定を監視して客観的な立場から、もっといえばユーザーや社会の側の視点から意見を述べる役割を担う者であって、いわばデータ領域における監査人というべきものである。そして、意思決定者は、DPO の意見を踏まえて、自らのデータの取り扱いに関する意思決定を行う。企業の中で DPO のような立場にある者は相当特殊であり、企業にはその設置にあたっていくつか留意すべき事項がある。

① 専門性維持のための支援

DPO には、法令に関する深い理解はもとより、ユーザーや社会との対話の中でその期待を的確にとらえる能力、自社のデータの取り扱いの詳細や利用しているシステム、これまで行ってきたコミュニケーションの内容等に関する知識が求められる。DPO には相当高度な専門性が求められる故、その獲得および維持のための資金とサポートメンバーを含む適切な人的リソースの提供が必要になる。

② 必要な情報へのアクセス

DPO を設置したとしても、社内の必要な情報へのアクセスや意思決定を行う会議への出席ができなければ DPO はその役割を果たすことができない。少なくとも、自社のデータの取り扱いに関する重要な意思決定にあたっては DPO の意見を求めなければならないことを社内規程で定めるなどの対応が必要になる。

なお、DPO はデータに関する取り組みの企画や開発のできるだけ初期の段階からその取り扱いを監視し、助言をすることが望ましい。できるだけ早期に多角的なリスク評価とそれに基づく意思決定が行われることで、必要な見直しにかかるコストを低減することができるからである。

③ 独立性と自律性の確保

DPO は、企業の利益や論理から切り離した独立した立場から自社内のデータの取り扱いを監視し、助言をする者として位置付けなければならない。GDPR においては、DPO がその業務遂行に関して何らの指示も受けないことを確保しなければならないとしたうえで、業務遂行に関して解雇したり罰則を与えたりすることを禁じている。また、DPO が他の業務を兼務すること自体は禁じていないが、利益が相反することのないようにしなければならない[9]としている。これらの取り扱いは新しい時代において企業が DPO を設置するにあたって大いに参考にすべきである。

④ 心理的安全性の確保

DPO の設置の目的は、不適切なデータの取り扱いが極めて大きな経営上のリスクになっている状況に鑑みて、通常の企業の意思決定過程では出てきにくい、主観的な評価を前提とするユーザーや社会の側の視点に立った意見を意思決定の俎上に載せることにある。しかしながら、企業の中にあってこのような意見を述べることは、ときとして極めて

9 DPO が適切に機能するために、ビジネス部門や、会社の経営に関する意思決定をする役職（CEO、CFO、人事や財務、マーケティング、IT 部門の責任者等）との兼務は認められていない。

困難であり相当な度胸と覚悟のいることであって、DPO には大きな心理的負担がかかる。そもそも DPO は、事業を支援するバックオフィス部門とは根本的に役割が異なり、そのことについての全社的な理解なしに DPO がその職責を果たすことは困難である。そこでとりわけ重要になってくるのが、これに関する会社トップからの積極的な情報発信と具体的なフォローである。

（3）DPO の導入方法

次に、DPO の導入にあたって具体的に留意すべき点について触れたい。

① DPO の選任のあり方

DPO は独立した立場にあり、自らの知識と経験を総動員して考え、その良心のみに従って判断し、意見をすることが求められる。DPO には、自らの職責に対する深い自覚と、とりわけ高い職業倫理が求められる。

また、誤解を恐れずにいえば、DPO はデータの保護のみを目的としない高度なバランス感覚が求められる。ユーザーがデータの利活用を許容するか否かは、サービスの提供を受けることでどのような便益の提供を受けることができるのか、そのサービス提供に必要なデータの利活用であるのか（そうであることを適切に説明しているのか)、一度データの利活用に同意した場合でも事後的にその同意を撤回できるのか等の様々な要素との関係で判断しているはずであり、DPO は「ユーザーが許容するか」「ユーザーの期待を裏切るデータの利活用でないか」という点を検討する際に、これらを適切に考慮できなければならない。たとえば、無料の情報提供サイトにおいてデータを利用した広告を出すといった場合に、DPO がデータの保護のみを目的としている場合、「データを利用した広告は本人の権利利益を侵害するおそれがあるので不適切である」といった意見をしてしまうことが考えられるが、これは、ユーザーや社会の側の視点に立って考えても、多くの場合バランスを欠いた意見であるということになろう。無料サイトは広告で利益を上げることで成り立っており、ユーザーが広告を出さないのであれば無料サイトを有料にしてもよいと考えているかといえば、それは一般的にはそうではないと思われる。ユーザーが問題としているのは、広告の掲載そのものではなく、また、データを利用した広告そのものでもなく、そのための具体的なデータの使われ方や広告の内容、広告の表示方法であると思われることから、DPO としては、どのようなデータを分析の対象とするのか、あるいはしないのか、また、どういう属性の分析を許し、あるいは許さないのか、広告の表現としてどのよ

うなものを許容し、あるいは許容しないのか等々の点について、事業部門がどのようなルールの下に実務を運用し、またどのようにその遵守状況を確認するのかについて説明を求め、必要に応じて客観的な意見を述べるべきである。

企業が DPO を選任する場合、前述の法令に関する深い理解、ユーザーや社会との対話の中でその期待を的確にとらえる能力、自社のデータの取り扱いの詳細や利用しているシステム、これまで行ってきたコミュニケーションの内容等に関する知識等の専門能力を有している者であることに加え、高い職業倫理を有し、高度なバランス感覚を有する者をその候補とすることが必要になってくる。

② 具体的な DPO の設置方法

DPO に求められる資質は多岐にわたり、また、高い専門性を有することが求められ、そのうえ独立性の維持のために利益相反が許されないこととなると、果たしてそのような人材をいかに確保するのかということが重大な課題となる。

ユーザーや社会が企業に対して求めるデータプライバシーの保護に対する期待は今後も大きくなっていくことが予想され、この観点からは自社において適切な人材育成をしていかなければならないことは論を俟たないが、では、新しい時代を担っていく企業の DPO 設置が 3 年後や 5 年後でよいかといえば、そういうわけにはいかないであろう。中長期的には、ないし、最終的には単独で独立した DPO の設置を目指すとしても、短期的には複数の者で補完しながら DPO の機能を果たすこと（チーム制の DPO）を考えてもよいであろう。

これには 2 つの場合があり得、専門性の確保が問題となる場合は、特定の領域について専門性を有する者が複数で DPO の機能を果たすことが考えられる。また、独立性の確保が問題となり得る場合は、主たる DPO を設置し通常はその者が DPO の役割を果たしつつも、具体的事案において独立性が問題となる場合については、その問題となる事案に関し、DPO の役割を代行する者をあらかじめ定めておくような対応が考えられる。

なお、企業グループにおいては、特定の事業領域に係る複数の企業で共通の DPO を設置するという対応も考えられるほか、親会社が子会社等に対して DPO を派遣する取り組みや、極めて高い専門性が求められる特定の事例や、独立性の維持が困難となってしまった特定の事例について、親会社が当該事例に限定して DPO の機能を果たす者を派遣するなどの対応も考えられる。いずれにしても、DPO を導入するための工夫は様々に考えられ、企業の実態に即し、DPO が適切にその役割を果たすことのできる体制を構築するこ

とが望まれる[10]。

③ DPO の意見の取り扱い方

前述のとおり、企業がデータの取り扱いについてユーザーや社会からの信頼を失うことが極めて大きな経営上のリスクになっている中で、DPO は、通常の企業の意思決定過程では出てきにくい、主観的な評価を前提とするユーザーや社会の側の視点に立った意見を意思決定の俎上に載せることを目的として、自社のデータの取り扱いやこれに関する決定を監視し、客観的な立場から、ユーザーや社会の側の視点から意見を述べる役割を担い、意思決定者は DPO の意見を踏まえて、自らのデータの取り扱いに関する意思決定を行う。したがって、意思決定者は DPO の意見を尊重する必要はあるが、必ずしも DPO の意見を採用する必要はない。

DPO の意見と、事業部門の意見や法務部門の法令の解釈に関する見解を含むバックオフィス部門の意見が相違した場合、意思決定者はいずれの意見を採用するのか、ないし、DPO と事業部門・バックオフィス部門とのさらなる意見調整を求めるのかを判断することになる。その際、適法か違法かの評価が相違している場合については、たとえば外部の弁護士への意見照会をするなどして意思決定のための補足の資料を用意すること等で対応することが考えられるが、問題は、「ユーザーが許容するか」「ユーザーの期待を裏切るデータの利活用でないか」といった主観的な点についての評価が相違している場合である。

このような場合、問題となっているのが主観的要素であるがため、DPO はその客観的根拠を示すことができないことが普通で、意思決定者がこれを DPO に求めることは不適切である。他方、それではどのように意思決定をしていいのか判断がつかず、スタックしてしまうということが懸念されることから、DPO においては、たとえば、過去の類似事例におけるユーザーの反応やそれによって生じた影響、議論になっている案件で同様の反応が起きた場合に想定される影響等についてできる限り分かり易く伝える等の努力をしなければならない。また、意思決定者がその場で突然判断を求められても判断に迷ってしまうことはある意味当然であり、意思決定者は普段からデータプライバシーの保護の必要性

[10] 筆者の所属する Z ホールディングスにおいては、DPO の事業会社への派遣のほか、DPO を設置済みのデータを取り扱う主要な事業会社 19 社の DPO の専門性の維持・向上のために、国内外の法令やいわゆる炎上事例を含むインシデントや執行事例の発生状況等に関する勉強会を開催したり、各社の DPO が個別の事案で判断に迷った場合の相談の受付、法律事務所等の外部意見の取得サポート等の取り組みも行っている。

に関する認識やその求められる程度に関する感度を高めておく必要がある。他社におけるものも含め、DPO が定期的にプライバシーインシデントや執行事例の発生状況、それによる影響等について、意思決定者にレクチャーすることで、意思決定者がユーザーや社会の期待の現在地を把握できるようにしておくことが望ましい。

なお、通常のビジネスの現場では、「異論をはさむのであれば対案や解決策を提案する」というのが求められる姿ではあるものの、DPO は独立性を維持しなければならないという特殊性ゆえ、問題となっている取り組みの実施を前提とした提案をすることが許されない点に留意が必要である。DPO がこれをしてしまうと、その提案が適切なものであるのか、客観的な立場から評価する者がいなくなってしまい、DPO によるデータ利活用の監視と助言の体制が崩壊してしまうからである。

４．最後に

我々は今時代の大きな転換点にある。新たな時代の到来は、人々の可能性を大きく発展させる可能性を秘めている。Society 5.0 の実現を担う企業は、これまでも社会の変革を的確にとらえ、この社会の一員として受け入れられ、認められながら共に成長してきた。

新たな時代において飛躍の原動力となるデータは、生身の人間との関連を強め、その意味合いを大きく変えつつある。データが「その人そのもの」に近づいていく、そしてデータにその人の人格が投影されるということは、企業のその取り扱い如何によっては、その人の人格的利益や自由に影響を与えてしまうということである。そして、企業が営利を追求する活動においてデータを利活用する中で生じるこれらの間の衝突は、人格的利益や自由と経済的利益や自由との衝突であって、社会から求められる保護のレイヤーが一段異なるものの衝突であることに留意しなければならない。新たな時代においては、これまでの時代の体制を前提に単に両者のバランスを適切に取っていくという発想では、社会の期待に応えていくことはできないのである。

独立性と自律性を有する DPO を設置することの必要性は、まさにこの点から導き出される。企業のこれまでのデータの利活用に関する意思決定では、程度の差こそあれ、「違法でない領域は自由な領域である」とか、「約款で説明していることは実施可能である」ということが前提であったところがあるのではないか。しかしながら、このような考え方は、新しい時代において意味合いを変えているデータを取り扱うにあたっては、ユーザー

や社会から受け入れられなくなる可能性が極めて高い。新しい時代において、企業の利益や論理から切り離した独立した立場から、企業内のデータの取り扱いを監視し、データに関する意思決定にあたってこれを冷静かつ客観的に評価し、ユーザーや社会の側の視点から助言する DPO を設置することで、企業はユーザーや社会の期待を適切に認識し、これを織り込んだ経営をすることができるのである。

新たな時代においても、それぞれの企業がユーザーや社会からの信頼を勝ち取るために切磋琢磨していくことでユーザーや社会に受け入れられるデータの利活用が進み、それによって社会課題が解決され、人々の生活がより便利で豊かになり、そうして多くの人々が自己の可能性をより広げていくことで社会全体が発展していく将来を実現していくことが期待されている。

第５章　データをめぐる権利の「周辺問題」
―経済学的視点からの考察―

静岡大学学術院情報学領域教授

高口　鉄平

１．はじめに

経済活動、社会活動へのデータの利活用が進展するとともに、データをどのように捉えればよいか、データの利用についての望ましいルールとはいかなるものか、といった議論が盛んになってきている。とくに、個人情報（個人データ）については、どのような法的制度が望ましいのかについてさまざまな見方があり、結論が出ていない（望ましいか否かは別としても、一意に見解が定まっていない）ようだ。

個人情報に関する法的制度の整備は、その背景にある「個人（あるいは政府や企業）は個人に関するデータに対してどのような権利を持つと考えるべきか」という問いへの回答に依存する。極端な例として、もしも個人が自身に関するデータやデータから生じる影響に何らの権利も持たないという考え方が正しいとされる世界であれば、個人情報保護法はほぼ無用となる。逆に、個人が自身に関するデータに関してあらゆる権利を有する世界であれば、政府や企業が個人情報を扱うことがきわめて困難となる法制度となるだろう。したがって、近年盛んな個人情報に関する法的制度の議論について望ましい解を導出するためには、データをめぐる権利とは何かという点について理解し、利害関係者（個人、政府、企業）の間で一定の合意を得ることが重要である。

データをめぐる権利について検討し、望ましい法的制度を定めるというのは、法的、法学的視点の検討が中心となる。また、権利については本来的には哲学的検討も必要かもしれない。いずれにしても、本稿ではそのような検討をおこなうことは筆者の能力上できない。その代わり、本稿では、データ、とくに個人に関するデータをめぐる権利の「周辺問題」を検討したい。

ここで、「周辺問題」とは、「権利を行使する、また、権利をもとに行動するために必要な条件、環境についての問題」といったことを指している。本稿では、個人が有するべき権利として指摘されているいくつかの視点、また、特定の権利を前提としたいくつかの制度について、それらが機能するために解決しなければならない課題を提示する。とくに、

経済学的視点からみて検討が不足しているのではないかと筆者が考えている課題を提示したい。

本稿では、現在指摘されている、権利についての複数の主要な視点および制度に対し、そのそれぞれについて課題を検討する。逆にいえば、それらの視点、制度のうちどれが望ましく、どれが望ましくないかという結論を出すものではない。したがって、本稿には、将来的に権利や制度が定まった際には結果として不要となる検討が含まれるかもしれない。しかし、いかなる権利、制度が望ましいかを議論する過程でこそ、本稿で提示する課題を捨象してはならないと考えている。その意味で、法的議論に現在進行形で寄与できる考察を試みたい。

以降で考察するそれぞれの権利、制度について本稿で提示する課題は、基本的にはすべて同じ根本的課題に集約できる。そこで、個別の考察をおこなうまえに、この根本的課題について示しておきたい。

本稿の考察の根底にある課題は、「個人情報を利活用することで生み出される経済的な価値が明確にはあきらかにされていない、また、あきらかにすることに十分な関心が向けられていないのではないか」、というものである。さらに、「個人情報を経済財として扱うべきか否かという視点に対して、制度整備の方向性に必ずしも整合性が見られない部分があるのではないか」という課題も示しておきたい。

２．プライバシー、個人の権利利益に関する議論に触れて

本節では、個人情報保護法におけるプライバシー、個人の権利利益に関する議論を踏まえ、それらに対する主要な考え方をベースとした際の経済学的な課題を考察したい。

曽我部・山本（2020）、高木（2022a）、高木（2022b）、GLOCOM 六本木会議（2022）などの検討、提言によると、個人情報保護法におけるプライバシーや個人の権利利益に関する考え方について、憲法学において通説的であったものとして自己情報コントロール権があり、これに対し、意思決定指向利益モデルに基づいた法制度であるべきだとする見解も提示されている。重ねて言及するが、それぞれの考え方の望ましさを検討すること、また、ぞれぞれの考え方を詳細に示すことは本稿の目的ではない。本稿では、仮にこれらのいずれかの考え方に基づいて法的制度が整備されるとすれば、それぞれ、いかなる経済学的視点が重要となるかについて示す。

（1）自己情報コントロール権に関して

はじめに、自己情報コントロール権に関して考えてみたい。自己情報コントロール権に基づけば、自身の情報については基本的に自身がコントロールできることとなる。現代ではさまざまなサービスで自身の情報を企業に提供するか否かを意思決定する場面に遭遇するが、その際に、どのような情報は提供するか、どのような目的であれば提供するか、といったことをすべて自身で決めるというようなことが想定される。

この自己情報コントロール権に対して挙げられている問題点、課題の一つに同意の問題がある（曽我部・山本 2020）。個人が自身の情報をコントロールする場面、例えば企業による情報の収集、利用を認めるか否かを意思決定する場面において、ほんとうに個人が正しく意思決定できる（同意する／しないを決められる）か、という問題である。これはきわめて現代的な問題であろう。インターネットを通じたサービスが多様化し、情報の利活用が進展するとともに、扱われる情報の種類、量は増加し、目的も多様化する。これにともない企業が提示するプライバシーポリシーの分量も膨大になり、そのようななかで個人がすべてを完全に理解して同意するということは現実的には難しい。

この同意の問題に対して、近年ではさまざま取り組みがなされているようだ。この点、同意の問題は、基本的には同意するか否かを意思決定するための情報量が個人の能力を超えるという点に帰着すると筆者は考えている。したがって、それを解決する取り組みとしては、個人の能力の範囲内で正しい同意ができるように意思決定するための負担を工夫して軽減することが中心となっているように思う。具体的には、プライバシーポリシーの提示の仕方を工夫し、個人にとってわかりやすいインターフェースにすることなどが挙げられ、企業、あるいは政府でさまざまな取り組み、検討がなされている。

一方で、個人が自身の情報を企業（あるいは政府）に提供するか否かを意思決定する場面において、「その情報を活用することでどれほどの経済的な付加価値が生み出されるか」という「情報」について、これまで個人は必ずしも十分に把握できていなかったのではないか。

個人にとって、自身が提供する情報がいかなる経済的な価値につながっているかという「情報」は、同意に関する意思決定に少なからず影響を与えるものと考えられる。現在でも、自身の情報がどのように使われ、自身に提供されるどのようなサービスに結びつくかは利用規約等で示されているだろう。一方で、自身の情報の活用によって企業が「どれほどの収益をあげているか」は、個人にはわからないのが現状である。同じサービスを受けるた

めの情報の提供であっても、例えばそれによって莫大な収益をあげているということを個人が知るか否かで、意思決定、すなわち自己の情報のコントロールは変わる可能性がある。

当然、個人の情報を利活用することがどの程度の経済的価値につながるかは、実際にはどのくらいの質量の情報が蓄積されるかなどに左右されるため、厳密な把握は困難であろう。また、情報を収集、蓄積した時点では生み出される価値が未知である場合もあるだろう。この点で、主体としての各企業がこのような経済的価値を把握するのは現実的ではないかもしれない。さらに、仮に大きな付加価値を生み出していたとしても、一個人の情報ベースに還元してみると、その価値は微々たるものともいえる。

しかし、もし個人が提供する情報が結果として生み出す経済的価値の多寡によって意思決定が異なるのであれば、産官学の連携等を通じてその価値を把握する取り組みが求められる。例えば、総務省の AI 経済検討会などでは（個人データに限らないが）データが生み出す価値の測定が試みられているが、こういった取り組みがいっそう必要であると考える。

穿った見方をすれば、個人が提供する情報が企業の収益につながっていることがあまりに強調されると個人の情報提供が停滞するかもしれないという、「寝た子を起こすな」という発想も生じるかもしれない。しかし、こういった点が不透明なことが、個人から見た企業の不信感につながっていることも考えられる。また、GAFA といった巨大企業が個人の情報を駆使して現在の地位を占めているという脅威は個人レベルでも感じられるだろう。そうであれば、経済的価値が明確化されることで、例えば個人の「自身の情報が（自身への直接的なメリットのみならず）企業に経済的メリットをもたらすのであれば、自分は誠実で社会的責任を果たしている企業にその経済的メリットを享受してほしい」といった発想から、より情報を利活用できる機会を得られる企業も出てくるのではないか。

（２）意思決定指向利益モデルに関して

つぎに、意思決定指向利益モデルに関して考えてみたい。高木（2022b）の研究、また高木（2022a）、GLOCOM 六本木会議（2022）では、個人情報保護法は自己情報コントロール権を実現したものではないというのが政府の見解であるとしたうえで、OECD「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事勧告」の立案の経緯、趣旨を踏まえ、意思決定指向利益モデルと呼ばれる考え方を指摘している。

意思決定指向利益モデルは、例えば GLOCOM 六本木会議（2022）の提言では「本人が自己の情報の流れを自己で決定するということではなく、個人データ処理に基づく他者に

よる評価・決定が本人の自己決定を阻害し得ることに対して本人が防御する権利であること（GLOCOM 六本木会議 2022、p.3)」という説明がなされている。そして、意思決定指向利益モデルに基づき法制度が実現することで、医療健康データ等の二次利用ルールに関する問題、自動運転システムの個人の映り込みの問題、教育分野の個別最適化に関するアルゴリズムの適切性の問題等について解決が実現するとされている。

本稿では、このうち個人データの二次利用について着目したい。意思決定指向モデルでは他者による評価･決定が個人に影響を与えることを避けるという考え方であることから、統計量に集計する二次利用は個人の同意が無くとも許容されるとする（ただし、同時に無制限にデータが転々と流通することは防ぐべきともしている点は強調しておきたい)。

この点、企業の経済活動に目を向けた場合、個人データを統計量に集計して二次利用することで、それが企業による評価・決定が個人に影響を与えることはないとしても、企業の収益、利潤につながる可能性がある。例えば、二次利用を通じて自社のサービス展開のヒントが得られたり、商品開発につながったりする場合である。

ここで、仮に二次利用によって企業が追加的利潤を得られる場合、そのことについて個人がどうかかわるべきかという点は重要であろう。二次利用について個人の同意が必要無い制度を前提とすると、企業から見れば（その可能性があれば）二次利用で制限なく利潤を獲得する可能性を探れる。したがって、個人は一次利用のための企業への情報の提供の同意時に、このような可能性を認識しておくことが重要ではないか。

一個人の情報が生み出す二次利用を通じた経済的価値（利潤）は微々たるものかもしれない。しかしながら、今後さらなるデータ流通を目指すのであれば、個人から見て「知らないところで自分の情報から企業が利潤を得ているかもしれない」という不信感を生じさせることは望ましくない。過去の個人情報をめぐる漏えい事故や不適切な利用の事例を振り返っても、法的な問題以上の不信感が生まれているケースもあると思われる。個人の理解がいっそう求められる。

もっとも、高木（2022a）によれば、個人データは data controller が利用目的を設定し作成するものであり、個人情報はその個人のものであるという捉え方が適切でないとされている。意思決定指向モデルによる制度整備が進められる場合、個人がこういった理解を正しく受け止めておかなければ、やはり（個人の無理解だとしても）不信感がデータの流通を阻害する可能性がある。

３.「公益」に関する議論に触れて

前節では個人情報保護法そのものをいかに捉えるかという観点からの二つの考え方に基づき経済学的視点からの検討を加えたが、本節ではデータを利用する目的としての「公益」について、既存の議論を検討したい。基本的な市場メカニズムにおいては、個人は効用最大化、企業は（私的な）利潤最大化を目指す。したがって、私的な利益とは異なる「公益」については、市場メカニズムとは異なる仕組みで考える必要がある。個人情報が「公益」にもつながるとすれば、その意味での利活用のあり方を検討しておくことが重要である。

（１）Authorized Public Purpose Access（APPA）に関して

「公益」に対する個人情報の利活用については、世界経済フォーラム第四次産業革命日本センターが Authorized Public Purpose Access（APPA）というモデルを提唱している。APPA とは、「医学医療の発展や公衆衛生の向上等の、合意がなされた特定の公的な目的のためであれば、必ずしも明示的な個人同意によることなく個人の人権を別の形で保障し、データへのアクセスを許可することで目的とする価値を実現するモデル（世界経済フォーラム第四次産業革命日本センター 2020、p.9）」である。

APPA の考え方は、公的な目的のためであれば同意によらないデータアクセスを目指す点で、自己情報コントロール権が及ばない分野を設定する試みともいえそうである。もちろん、現在の個人情報保護法においても、「人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」には第三者提供において本人の同意は不要となっているが、「特定の公的な目的」の定義次第であるものの、その目的の範囲はより広い印象を受ける。

また、医療分野の個人情報の利活用という比較で見ると、前節で示した意思決定指向モデル以上の利活用を目指すもののようにも感じられる。意思決定指向モデルにおいては同意が無くとも許容される利用として二次利用が挙げられていたが、APPA の考え方では個人の人権は別の形で保障する前提とはいえ、統計量ではなく個人情報そのものを同意無しで利用するように見える。

APPA のような考え方を検討するうえでは、当然「公益」の定義が重要となる。「公益」があまりにも広く定義されれば、情報を同意無しで利用される個人の立場からみれば理解を得られなくなる。一方で定義が狭すぎると、APPA の本来の意義が損なわれる。何が「公益」か、という問題は根源的なものであり結論を得るのは難しいが、まずは定義について

十分な理解の醸成が求められる。

その際、本稿での検討課題である経済的な価値という意味では、「公益と（企業等の）私的利益の重複可能性」が重要である。仮に「公益」が私的利益をまったく重複しないのであれば、（公益の定義が理解されるものであれば）個人・企業間でのやり取りを通じた個人情報の利活用とは異なる、一つの利活用のあり方といえるかもしれない。一方で、「公益」と私的利益に重複する部分があるとすれば、その取扱いについて慎重な検討が必要である。個人の同意によることなくデータへのアクセスが許可されるとすれば、それは個人の意思が反映されない一種の強制力がはたらくこととなる。そういう状況下でのデータの利用が特定の主体の私的利益につながるということは、特定の主体に制度によって利益を配分することになるからである。

（２）EHDS に関して

「公益」と指摘利益の重複可能性という点について、現実には完全に重複を避けることは難しいように思われる。「公益」を実現する過程では民間企業の協力は一定程度必要となる場合が多いと考えられるからである。

この点を考えるための一助として、EU の European Health Data Space（EHDS）を取り上げる。EU（2022）によれば、EHDS は個人が自身の健康データを管理しよりよい医療のためにそのデータを利用可能にするとともに、EU 自体が既存の障害なしに十分に健康データを活用できるようにするためのものであり、2022 年にその法案が提案された。加藤（2022）によると、EHDS は電子健康データの二次利用に対する障壁を取り払うためのものであるとされている。また、加藤（2022）によると EHDS はその前年の GDPR 下のヘルスケア活用の影響評価を踏まえたものであり、この影響評価での二次利用とは、個人への医療等の提供という一次利用とは別の利用で、そこには社会保障のほか、創薬や医療機器開発が含まれているようだ。そして、この二次利用を同意不要で利用実現しようとするものとされている。

EHDS を参考にすると、医療、健康分野のサービスには創薬等、民間企業の活動が含まれてくる。したがって、医療の発展を「公益」的に捉え、その「公益」のために個人データを活用するとなると、その活用の成果はどうしても民間企業の指摘利益と重なることが避けられない。この状況を前提として、医療に限らず、「公益」への個人情報の活用を議論しなければならないだろう。また、個人の権利をどのように考えるにしても、少なくとも

こういった認識、理解を個人が持っておくことが重要である。

その際、APPA が示唆していると考えられる一次利用までを個人の同意不要で実現するのか、（意思決定指向利益モデルと同じ方向性にも思われる）EHDR のように二次利用を同意不要で実現するのか、あるいは、二次利用であっても私的利益につながる利用は個人の同意を必要とするのか。制度次第で個人情報利活用のあり方は大きく変わってくる。

４．個人情報の「取引」について

前節では「公益」のための個人データ利活用について、市場メカニズムによらないあり方を検討してきたが、本節では逆に市場メカニズムを活用した個人データの利活用のための制度について検討したい。

現在、日本では個人が自身の情報を企業等と経済財のように取引する枠組み、制度が整備されている。その最たるものは、データ取引市場である。データの取引は、データという性質上、通常の財の取引のように自然に市場が形成されるわけではないが、民間サービスとしてその市場機能が提供されている。例えば、エブリセンスジャパン株式会社は個人と企業の間でのデータの取引も可能とする IoT データ取引市場「Every Sence」を提供している。

また、データ取引市場のように直接的ではないものの、データ取引市場と同様に個人の情報を「取引」する対象として捉える制度として情報銀行がある。情報銀行は政府によって検討されてきた制度であり、「実効的な本人関与（コントローラビリティ）を高めて、パーソナルデータの流通・活用を促進するという目的の下、本人が同意した一定の範囲において、本人が、信頼できる主体に個人情報の第三者提供を委任するというもの」とされている。通常、個人はサービスを利用する企業等と自身の情報の提供について同意、提供をおこなうが、情報銀行は個人の情報を集約して、より多くの企業が利用できるようにするものである。

個人からみると、どのように自身の情報を企業に利用させてよいかについて情報銀行との間で同意するだけでいいことになる。情報銀行は、個人が同意（委任）した条件に従って、利用したい企業に提供するからである。つまり、個人情報を利用したい企業それぞれと同意する煩雑さがなくなるということになる。さらに、情報銀行を通じて自身の情報を利用した企業から便益を受けることができる。企業からみると、必ずしも直接自社とつながっていなかった個人の情報について、情報銀行を通じて利用できる可能性が拡がる。

データ取引市場や情報銀行のような個人情報を「取引の対象」とする制度は、個人情報が生み出す経済的価値を明示化させる。情報の「売り手」としての個人も、「買い手」としての企業も、その情報の経済的価値を捉えなければ、その取引価格が妥当か判断できないからである。この点で、本稿でこれまで検討してきた個人情報保護法の考え方や公益の捉え方における、個人情報の経済的価値に対する「見えにくさ」の問題が解消される。

ただし、個人情報を「取引の対象＝経済財」とする制度についても、重要な課題が残されている。

第一に、個人情報を経済財として捉えることと、個人情報保護法との不整合である。第2節でみたように、自己情報コントロール権であっても、意思決定指向利益モデルであっても、どちらにしても個人情報を経済財として扱っていない。個人が自身の情報の取引主体として意思決定することは自己情報のコントロールともいえそうであり、自己情報コントロール権と親和性があるようにもみえるが、プライバシーと経済財（財産）とは大きく異なる。また、意思決定指向利益モデルでは統計量による二次利用は個人の同意が無くとも許容されるが、そうなると二次利用によって生み出される経済的価値が取引に反映できない可能性がある。

第二に、個人や企業が市場価格を評価することの困難性である。すでに見てきたように、個人情報を活用することによる経済的価値を正確に捉えることは企業であっても難しく、個人であればいっそう困難である。そのような状況では、データ取引市場であっても情報銀行であっても、取引主体が妥当な意思決定をおこなえず、結果として個人情報の利活用が望ましい水準から過少／過大となる可能性がある。

５．おわりに

本稿では、個人情報をめぐるさまざまな考え方について、それらにおける経済学的課題を示してきた。重ねて述べると、どのような考え方が望ましいかについては経済学的視点のみで判断できるわけではなく（むしろその他の視点が重要であるとも思われ）、本稿では何も結論を出すことはできない。一方で、現在議論されているどのような考え方でも、経済学的視点で検討が十分でない点があることを提示することを本稿では試みた。

そもそも、個人情報に関する法制度が議論され始めた時代と現在では、個人情報の利活用の可能性がまったく異なる。現在では、個人情報が生み出す経済的価値が「周辺問題」の域を超えているように思われる。この意味では、どのような法制度を目指すにしても、

また、そのための検討をおこなうにしても、その経済的価値について「あることはわかっているが、どのくらいあるかは厳密にわからなくても問題ない」という姿勢ではなく、たとえ困難であったとしても厳密に捉えることを「試みる」ことが求められるのではないか。

参考文献

EUROPEAN COMMISSION（2022）" COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL A European Health Data Space: harnessing the power of health data for people, patients and innovation"

GLOCOM 六本木会議（2022）『デジタル社会を駆動する「個人データ保護法制」にむけて』

加藤尚徳（2022）「EHDS（European Health Data Space）の議論を踏まえた NFI からの 4 つの提言」内閣府規制改革推進会議第 9 回医療・介護・感染症対策ワーキング・グループ資料

曽我部真裕・山本龍彦（2020）「自己情報コントロール権をめぐって」『情報法制研究』第 7 号、pp.128-140.

高木浩光（2022a）「高木浩光さんに訊く、個人データ保護の真髄」（聞き手：小泉真由子）『情報法制レポート』（情報法制研究所）第 3 号、pp.47-99.

高木浩光（2022b）「個人情報保護から個人データ保護へ（6）」『情報法制研究』第 12 号、pp.49-83.

第６章　ノンパーソナルデータの保護のあり方と データ流通・利活用の促進：知的財産法を中心に

東京大学大学院情報学環　准教授

酒井麻千子

１．はじめに

Society 5.0 で実現する社会においては、IoT（Internet of Things）によって全ての人とモノがつながり、膨大なデータがサイバー空間に集積される。そして Society 5.0 では、AI がこのビッグデータを解析し、解析結果がフィジカル空間の人間にフィードバックされることで、従来できなかった新たな価値が産業・社会にもたらされることを企図している[1]。令和 3 年にデジタル庁が策定した「包括的データ戦略」[2]では、この Society 5.0 の実現へ向けて、広範で多様なデータをつなげて活用し、新たな価値を創出することを目標に、データの利用者の視点に立ったデータ構造（アーキテクチャ）の共有、これを支えるデータ環境の整備が求められた。そして、データの連携及びそれを利活用したサービスを提供する基盤（プラットフォーム）の構築が重要政策として取り上げられている。

以上のように、データの蓄積・集約、分析、利用等を活性化させるための政策が掲げられる一方で、データの流通や利活用の促進にあたっては、データの不正利用やデータ流出、さらにはデータを通じた技術ノウハウの流出等によって、データを活用した産業の創出に悪影響が生じる懸念が示されており、データの保護や適切なデータの取扱いルールの策定が求められる。また、データは単に保有するだけでなく、大量に集積し、さらに加工や分析を行うことで価値が創出される・向上するという側面もあることから、データの流通や利活用をより促進するための制度枠組みの整備も求められているところである。

いわゆるデータについては、パーソナルデータ（特定の個人が識別できるかどうかによらず、個人に関する情報[3]）とそれ以外のノンパーソナルデータに大きく分類される。この

1　内閣府ウェブサイト「Society 5.0」（https://www8.cao.go.jp/cstp/society5_0/ ）

2　デジタル庁「包括的データ戦略」（令和 3 年 6 月 18 日）
https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/576be222-e4f3-494c-bf05-8a79ab17ef4d/210618_01_doc03.pdf

3　デジタル庁＝内閣府知的財産戦略推進事務局「プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0」（令和 4 年（2022 年）3 月 4 日）
(https://cio.go.jp/sites/default/files/uploads/documents/digital/20220304_policies_data_strategy_outline_01.pdf) の 44 頁、また 31 頁の図 15 を参照。その他、「パーソナルデータ」について、「個人

うち前者のパーソナルデータを含むデータの取扱いについては、本報告書の他章でも検討されているように、個人情報保護法をはじめとする法令及びガイドラインを参照しながら、適切な措置を講ずることが求められる。他方で、産業データ等のノンパーソナルデータの取扱いについては、前述のように近年の IoT や AI 等の情報通信技術の発展によってその利用価値が高まっており、データの保護・コントローラビリティ確保及びデータへのアクセス確保等に係る議論が必要であり[4]、本プロジェクトにおいても保護の仕組みについて整理が必要であることが指摘されてきた。

本章ではノンパーソナルデータを対象とし、データの法的保護としてどのような方法があるのかについて知的財産法を中心にまとめた上で、データの保護・コントロールとデータへのアクセスの調整を検討する上で知的財産法上問題となりうる点について検討する。

２．データの特徴

経済学的には、無体物であるデータは非競合性・非排除性を有するとされる。すなわちデータは同時に複数の者が消費（利用）でき、誰か一人の消費によって他者の消費量が減少しない（追加的な費用なしに全員が同じ量を同時に消費可能である）。そしてデータは複製が容易であるため、知的財産法による保護や囲い込み等によるデータの実質的支配等によって人工的に一定の排除性を生み出さない限り、データの共有が加速度的に進むことから排除性を持たせることも難しいという特徴がある。

またデータは多くの場合、データそれ自体に価値があるのではなく、データの加工や分析等を通じてデータを事業活動に利用する方法を開発することで価値が創出され、またある種のデータにおいては、多量のデータが集積されることで価値が創出されるという特徴があるといわれている[5]。その意味では、集積や加工・分析が行われていない、いわゆる生データと、それらを集積しデータベース化したものや解析や分析に適した形（構造化されたデータ）として構成したデータでは、その価値や保護の可否も異なる可能性がある。

さらに、特に近年の IoT データ等に顕著なように、データはリアルタイムでどんどん生

情報に加え、個人情報との境界が曖昧なものを含む、個人と関係性が見出される広範囲の情報を指す」と説明するものとして、総務省「平成 29 年版　情報通信白書」（2017 年）53 頁等を参照。

4 特にプラットフォーム上でのノンパーソナルデータのコントローラビリティ確保について、取引されるデータのタイプに応じて検討したものとして、デジタル庁＝内閣府知的財産戦略推進事務局・前掲注(3)28-30 頁参照。

5 経済産業省「AI・データの利用に関する契約ガイドライン 1.1 版」（令和元年 12 月）（https://www.meti.go.jp/press/2019/12/20191209001/20191209001-1.pdf）2 頁。

成される（中には毎秒生成されるようなものもある）ため、ある程度のまとまりで見た場合であっても、その量や質が定まらず非常に流動的であり、例えばデータの保護を考える際にも、どのデータを保護することになるのかを決めることが難しい[6]といえる。

３．データの法的保護

データの法的保護を考えるにあたり、民法上は、無体物であるデータは一般に所有権等の対象とならないため、所有権等の概念に基づいてデータに係る権利の有無を定めることはできない（民法 206 条等）。

次に「情報の保護」、特に財産的価値のある情報の保護を検討する際に対象となる知的財産法制度によってデータの保護を捉えることは可能だろうか。知的財産法制度が対象とする知的財産には、①発明や著作物等のように人間の創造的活動によって生み出されるもの、②商標、商号その他事業活動に用いられる商品又は役務を表示するもの及び③営業秘密その他の事業活動に必要な技術又は営業上の情報が含まれる（知的財産基本法 1 条）。

その他、民法上の不法行為による保護、そして契約による保護がある。

（１）知的財産法によるデータの保護

知的財産法における情報の保護の方法としては、例えば特許法や著作権法のように、発明や著作物といった保護に値する一定の情報について所有権類似の排他的権利を認める制度を設けるもの（権利付与型）や、不正手段により営業秘密を取得する等、特定の情報利用行為に対する法的救済を認めるもの（行為規整型）に分けられる。この分類に基づいて、データの保護可能性を検討する。

①　権利付与型：特許法

特許法における保護の対象となる発明は、「自然法則を利用した技術的思想の創作のうち高度のもの」（特許法 2 条 1 項）と定義される。ここで、「提示される情報の内容にのみ特徴を有するものであって、情報の提示を主たる目的とするもの」[7]は技術的思想ではないと理解されているため、一般的にデータは「発明」に該当しない。

ただし、データ構造や構造化されたデータがコンピュータの処理を規定するという点で

6　*See* P. Bernt Hugenholz, *Data property in the system of intellectual property law: Welcome guest or misfit?* in: S.Lohsse, et. al. (ed.), Trading Data In The Digital Economy: Legal Concepts And Tools 73, 93 (2019).

7　特許庁「特許・実用新案審査基準」第 III 部 第 1 章 発明該当性及び産業上の利用可能性 2.1.5(2) (4 頁)参照。

プログラムに類似する性質を有する場合には、これらは（コンピュータ）ソフトウェアと判断され、ソフトウェア発明と類似の保護を受けうることがある。すなわち、(ソフトウェアである)「データの有する構造が規定する情報処理が、ハードウエア資源を用いて具体的に実現されている」[8]場合、「自然法則を利用した技術的思想の創作」として「発明」に該当すると考えられている[9]。

またデータの生成方法や加工・分析方法については、「物を生産する方法の発明」として保護に値する場合もありうると考えられるが、この方法により生成されたデータへの排他的支配がきわめて広範に及ぶことになり、当該方法を利用した更なる技術革新を阻害する恐れがある点にも留意が必要である[10]。

② 権利付与型：著作権法

著作権法で保護の対象となる著作物は「思想又は感情を創作的に表現するものであつて、文芸、学術、美術又は音楽の範囲に属するもの」（著作権法 2 条 1 項 1 号）と定義され、典型的には文章や画像、音楽、プログラム等が該当する（同法 10 条 1 項各号)。問題となるデータが著作物であるか否かは個々のケースごとに判断され、要件を満たせば著作物として保護の対象になる。しかし、特に本章で対象とする産業データは、センサやカメラ等の機器を用いて機械的に創出されるものが多く、創作性を認めることが困難な場合が多いと考えられる[11]。

また著作権法では、データベースも著作物として保護の対象になる。データベースの著作物性については、その情報の選択又は体系的な構成によって創作性を有する必要がある(同法 12 条の 2 第 1 項)。これも個別に判断されるが、特に産業データにおいては、網羅性の高いデータベース構築が求められることに加え、フォーマットが標準化されていることが多い点を踏まえると、創作性が認められる場合は限定的であると考えられる[12]。

---

8 同「特許・実用新案審査ハンドブック付属書 B」 第 1 章　コンピュータソフトウエア関連発明 2.1.2（24 頁）参照。

9 前田健「データの集積・加工の促進と知的財産法によるデータの保護」パテント 73 巻 8 号（2020 年）205 頁。

10 この点を指摘し、データの加工方法が「物を生産する方法の発明」に該当し、当該方法で生産されたデータの譲渡及び使用を禁止できる場面は「かなり例外的な場合に限られる」とするものとして、前田・前掲注(9)205-206 頁。

11 経済産業省・前掲注(5)14 頁。

12 経済産業省・前掲注(5)14 頁、前田・前掲注(9)207 頁、上野達弘「自動集積される大量データの法的保護」パテント 70 巻 2 号（2017 年）32 頁等を参照。

③　行為規整型：不正競争防止法－営業秘密

不正競争防止法が対象とする営業秘密は、「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」（不正競争防止法 2 条 6 項）と定義されている。すなわち、①秘密管理性、②有用性、③非公知性の 3 要件を満たすデータは不正競争防止法上の営業秘密に該当する[13]。これらのデータについて、不正な手段により営業秘密を取得・開示する行為や、不正の利益を得る目的又は保有者に損害を加える目的で当該営業秘密を使用又は開示する行為等、2 条 1 項 4 号乃至 10 号に該当する行為を不正競争行為として、データ保有者は、侵害の差止めや損害賠償請求等の民事上の救済、また特に違法性が強い一定の行為につき刑事上の救済を受けられる。

しかし、本章で検討するようなデータの流通・利活用の促進という観点からは、多くの企業間等でのデータ共有やデータ流通が前提となってくることから、特に③非公知性の要件を満たすことが難しい場合が多いことが想定される[14]。

④　行為規整型：不正競争防止法－限定提供データ

平成 30 年の不正競争防止法改正によって新設されたのが限定提供データに係る規律である。1．でも述べたように、「多種多様なデータがつながることにより新たな付加価値が創出される産業社会の実現に向けては、データの創出、収集、分析、管理等の投資に見合った適正な対価回収が可能な環境が必要である」一方で、「利活用が期待されるデータは、複製が容易であり、いったん不正取得されると一気に拡散して投資回収の機会を失ってしまうおそれがある」[15]ため、これらの行為に対する法的措置の導入が求められていた。この状況を受け、データを安心して提供できる環境整備を目的として、「商品として広く提供されるデータや、コンソーシアム内で共有されるデータ等、事業者等が取引等を通じて第三者に提供するデータ」[16]を念頭に、「限定提供データ」を定義し、これに係る不正取得、使用、開示行為を不正競争として位置付けたものである。

13　営業秘密として保護を受けうるデータの例として、経済産業省・前掲注(5)14 頁では、例えば、「データが、製造業における生産方法に関するノウハウやセンサメーカのデータクレンジングのノウハウ、サービス開発業者におけるデータをサービスに活用するノウハウ等データ創出やデータの流通・利活用に携わる者のノウハウが化体されたもの」（かつ 3 要件を満たすもの）が示されている。

14　秘密保持契約等によってクローズドな集団内でデータを共有する場合は営業秘密としての保護が及びうるが、例えばコンソーシアム内でのデータ共有についてはどこまで保護が及ぶか不透明であると指摘するものとして、前田・前掲注(9)209 頁。

15　経済産業省知的財産政策室編『逐条解説不正競争防止法（第 2 版）』（商事法務、2019 年）103 頁、また経済産業省「限定提供データに関する指針」（平成 31 年 1 月 23 日、令和 4 年 5 月改訂）6 頁参照。

16　経済産業省・前掲注(15)6 頁。

限定提供データは、「業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その他人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理されている技術上又は営業上の情報（秘密として管理されているものを除く。）」をいい（同法 2 条 7 項）、①業として特定の者に提供する情報で、②電磁的方法によって相当量蓄積されており、③電磁的方法によって管理されている、④技術上又は営業上の情報であって、⑤秘密として管理されていないことといった要件を満たすものが該当する[17]。営業秘密との対比としては、公知であっても相手を特定・限定して提供されたデータを対象とする点、電磁的蓄積によって価値を有するデータである点、そして当該データを特定の者に提供するというデータ保有者の意思を第三者が認識できるように管理されており、かつアクセス制御等が施されている必要がある点などが挙げられる[18]。

この限定提供データにつき、2 条 1 項 11 号乃至 16 号に該当する行為を不正競争行為として、データ保有者は差止請求及び損害賠償請求等の民事的救済を受けうる。ここでは、限定提供データ保有者の利益を直接的に侵害する行為等の悪質性の高い行為を「不正競争」として規定しており、例えば限定提供データの善意取得者が法的責任をできるだけ回避できるようにする等、限定提供データ保有者と利用者の保護のバランスに配慮し、全体としてデータの流通や利活用が促進されるよう、限定提供データの取引の安全を重視した規定ぶりであると思われる[19]。法改正の目的が独占のコストを下げて流通をより容易にしつつ，正当利用者が萎縮して流通が阻害されないようにするものと解される[20]一方で、限定提供データの保護によりデータの流通が阻害されるといった批判[21]もある。平成 30 年の法改正は施行後 3 年を目安に見直しが要請されており、本年 5 月に中間整理報告[22]が出され、限定提供データに係る規律について、制度面の見直しで提示された論点の一部につき指針の改訂を行うと共に、今後も継続的な検討を進めることが示された。さらに 2023 年 3 月には小委員会での検討を踏まえた報告書[23]が出された。

---

17 また、無償で公衆に利用可能となっている情報と同一の限定提供データの取得・使用・開示は不正競争行為に該当しない（同法 19 条 1 項 8 号ロ）。

18 経済産業省・前掲注(15)9-19 頁。

19 経済産業省・前掲注(15)20 頁。

20 前田・前掲注(9)211 頁。

21 山内貴博「平成 30 年改正不正競争防止法への実務的対応」ジュリスト 1525 号 （2018 年）26 頁。

22 産業構造審議会知的財産分科会不正競争防止小委員会「デジタル社会における不正競争防止法の将来課題に関する中間整理報告」（令和 4 年 5 月）
https://www.meti.go.jp/shingikai/sankoshin/chiteki_zaisan/fusei_kyoso/pdf/20220517_1.pdf

23 産業構造審議会知的財産分科会不正競争防止小委員会「デジタル化に伴うビジネスの多様化を踏まえ

（２）民法上の不法行為該当性

データの蓄積や加工・分析に際しては一定の資本や労力が投じられることから、例えばこれをデッドコピーするような行為について民法 709 条の不法行為が成立するか。特にここまで検討してきたように、知的財産法制度によってデータの保護を達成するのは難しいことも多く、不法行為による保護が求められる場面は相対的に多くなるものと想定される。

この点、特別法である知的財産法と不法行為法の関係については、一般的に、知的財産法が許容した行為について不法行為法上の責任を認めるのは「法秩序の判断として矛盾する」場合がある[24]点が指摘されるところであり、裁判例でも、著作物性が否定されたデータベースについて不法行為による保護を認めた事例[25]は存在するものの、著作物に該当しない作品の利用行為について不法行為の成立を否定した最高裁判決[26]を筆頭に、知的財産法に違反する行為がない場合に不法行為を認めないものが多い。他方で、常に不法行為が成立しないと理解するのではなく、問題となる行為に際して、知的財産の保護と自由な利用に係る知的財産法の規律の態度が明確でない場合、つまり本章に即して言えば「データ保護の可否について現在の知的財産法体系が完結的にそれを定めてい」[27]ない場合においては、不法行為の成立の余地があることが指摘されている[28]。

（３）契約による保護

当事者間でデータの提供・受領がなされる場合、具体的なデータの保護の内容については利害関係者間の契約を通じて図られることが多い。例えば、当事者間で秘密保持契約を

た不正競争防止法の在り方」（令和 5 年 3 月）
https://www.meti.go.jp/shingikai/sankoshin/chiteki_zaisan/fusei_kyoso/pdf/20230310_1.pdf

24 窪田充見『不法行為法−民法を学ぶ（第 2 版）』（有斐閣、2018 年）143 頁。なお同頁では、常に不法行為が成立しないかはなお不明であり、後述の[北朝鮮映画事件]で示されたように特別な事情が存在する場合や、問題となっている知的財産の種類によっても判断が異なりうる点が指摘されている。

25 東京地中間判平成 13 年 5 月 25 日判時 1774 号 132 頁[翼システム事件]。費用や労力をかけて作成されたデータベースをデッドコピーし、元のデータベースの販売地域と競合する形で販売した行為につき、「公正かつ自由な競争原理によって成り立つ取引社会において、著しく不公正な手段を用いて他人の法的保護に値する営業活動上の利益を侵害するものとして、不法行為を構成する場合があるというべき」として、不法行為の成立を認めた。

26 著名なものとして、最判平成 23 年 12 月 8 日民集 65 巻 9 号 3275 頁[北朝鮮映画事件]では、「著作物に該当しない著作物の利用行為は、同法が規律の対象とする著作物の利用による利益とは異なる法的に保護された利益を侵害するなどの特段の事情がない限り、不法行為を構成するものではないと解するのが相当である」と判示している。

27 前田・前掲注(9)213 頁。

28 前田・前掲注(9)214 頁では、特に特許法や著作権法においてデータが排他権の対象となっていないことについて、「データに対する創作のインセンティブを確保するために排他的支配を認める必要性はなく、自由な利用を認めるべきであるという、立法による積極的な政策決定までは読み取ることはできないと考える」と主張する。また山根崇邦「情報の不法行為を通じた保護」吉田克己・片山直也（編）『財の多様化と民法学』（商事法務、2014 年）373 頁も参照。

締結することでデータを営業秘密等として保護することが可能になる。また、提供したデータの具体的な保管方法、データの利用方法、データの品質保証、提供データをもとにさらに生成されたデータの取扱い等について定めることも可能である。他方で、契約当事者以外の者は当該契約に拘束されず、また具体的な保護内容は契約に左右される[29]。特にノンパーソナルデータの流通においては、二者間だけでなくさらに多くの当事者が参加してデータの連携や共有を行うことも想定されるため、参加者間での利害調整を行う必要も生ずる[30]。

（4）まとめ

ここまで見てきたように、日本のノンパーソナルデータの保護については、所有権類似の排他的権利を付与して保護を図る権利付与型ではなく、特定の情報利用行為に対する法的救済を図る行為規整型による保護のあり方が模索されてきたといえる。そして、いわゆるビッグデータを念頭に置いた形で、平成 30 年不正競争防止法改正によって限定提供データに係る規律を新設した。また、データの具体的な保護内容やデータの管理方法等については契約で定めることで、柔軟にデータの共有・流通及び利活用を進めていくことが予定されていると考えられる。

特に、排他的権利をデータに付与することに対する懸念は世界的に共通しているといえる。例えば EU においては、機械的に生成された未加工の非個人又は匿名データの経済財としての取引可能性を高めることを目的に、2017 年、「データ製作者権（Data Producer's Right）」を創設し、当該データを対象に、そのデータ製作者に物権的な権利を認めるという案が提案されたことがある[31]。しかしこれに対して産業界及び学界から強い懸念や批判

---

29 この点、データ契約において「合理的な契約交渉・締結を促進するとともに、その取引費用を削減し、データ契約の普及を図る等の観点から契約で定めておくべき事項を示した」ガイドラインとして、経済産業省・前掲注(5)がある。

30 この点について、デジタル庁＝内閣府知的財産戦略推進事務局・前掲注(3)参照。

31 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS "BUILDING A EUROPEAN DATA ECONOMY", COM (2017) 9 final (10 Jan. 2017), p.13; COMMISSION STAFF WORKING DOCUMENT on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy, SWD(2017)2 final (10 Jan. 2017), p.33. この提案に加え、もう一つの権利の方向性として、データの不正利用があった場合にデータ保有者に他の当事者を訴えることができるようにする「一連の純粋に防御的な権利（a set of purely defensive rights）」を付与する、という案も提案された。SWD(2017) 2 final, p.33-34. これは、日本の限定提供データに係る規律と類似する側面があるが（山根崇邦「ビッグデータの保護をめぐる法政策上の課題―欧米の議論を手がかりとして―」パテント 73 巻 8 号（2020 年）109 頁）、こちらの案に対しても、既存の営業秘密保護法制とのバッティング等の懸念が示された。両提案の詳細については山根・同 101-111 頁参照。

が示され[32]、具体的な審議は進まなかった[33]。データに物権的な権利を付与することの問題点として挙げられたのは、「データ」の定義について、データが流動的であることから保護対象の確定が難しい点[34]、1 つのデータに複数の権利関係が認められうるため権利関係が複雑化し、かえってデータの流通を阻害しうる点[35]、契約等に基づく事実上のコントロールが与えられており、排他的権利がなくとも問題がない点[36]等であった。

確かに、データには管理のための技術や契約によってデータ保有者に事実上の支配が存在し、この事実上の支配に伴うロックイン効果等の弊害を減らす必要があることに加え、データは流通や利活用によって価値を増大させることが期待されるため、ここにさらに排他的権利を認めてしまうと、むしろコントロールが強化される可能性が強まってしまうと考えられる。また、権利付与による保護が想定されている発明や著作物等の知的財産は、無体物である以上有体物と比べてその外延は不明瞭であるものの、流動的なデータとの対比においては、一種の成果物としての外形を認識しやすいという違いもある。その意味で、データの法的保護を考える上では、排他的権利の付与ではなく、営業秘密及び限定提供データの保護に係る規律のような行為規整によるアプローチが今後も採られていくものと考えられる。

４．データの流通環境の整備へ向けたデータ保護と利活用のバランス

３．で検討してきたように、データの法的保護としては、営業秘密や限定提供データに該当するようなデータの管理体制が敷かれている場合、不正競争防止法により特定のデータ利用行為に対する法的救済が与えられる。また、データの取得や第三者への提供といった場面で締結される契約や利用規約等、あるいは技術的手段によって、データの事実上のコントロールが可能である。

---

32 例えば、COM(2017)9 final に対するパブリックコンサルテーションの結果では、「ほとんどの回答者は、所有権タイプの権利の創出であれ、ライセンス義務によるものであれ、規制による介入を支持しない」ことが示されている。Summary report of the public consultation on Building a European Data Economy (31 May 2017). また、マックスプランク研究所による反対声明（J. Drexl et al., 'Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public consultation on Building the European Data Economy'', 2017, Max Planck Institute for Innovation and Competition Research Paper No 17-08）等も参照。

33 むしろデータへのアクセスの確保の観点により、議論が集中・移行していったと思われる。例えば、Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. OJ L 303/59.

34 Hugenholz, *supra* note6, at 93.

35 *Id.* at 62.

36 Drexl et al, *supra* note 32, at 2.

（１）データ流通環境における利害関係の調整

これに対して、当事者間でデータから得られる価値を公平に配分してデータの利活用を促進させ、データの流通環境を整備していくためには、競争法的な観点から利害関係の調整が求められるところである。例えば、FRAND（fair, reasonable and non-discriminatory）条件でのライセンス供与やクロスライセンス等の可否を検討し、積極的に実施していくことが求められる。

また契約においても、不当な契約とならないよう、契約法制のアップデート[37]、あるいは契約のひな型やデータ契約のガイドライン等を提示していくことが考えられる[38]。

（２）データのオープン化・共有化

さらに、データの種類やデータが用いられる分野によっては、データの共有やオープン化をより進める方針を採るということも考えられる。例えば、研究データの共有や、行政の有するデータのオープン化といったことに加え、医療や金融等の特定の分野で用いられるデータについて共有を促進するための取組みが想定されうる。

これらの動きについて本章で検討する余裕はないが、知的財産法との関係では、技術の創出段階においてデータの共有やオープン化が進むことによって、より価値の高いデータを創出し、ハードウェア開発等を進めることができるといった指摘や[39]、オープンデータを活用した知財創出[40]の提案もなされており、データの保護だけでなく、データの共有や利活用の促進を積極的に行うことも重要であることが改めて意識されている。

（３）データへのアクセス

また、データ流通環境の整備へ向けて、例えば営業秘密や限定提供データに該当し一定の保護が認められうるデータへの第三者のアクセスをどの程度認める必要があるか、といった論点が想定される。

この点、欧州委員会が 2022 年 2 月に公表したデータ法案でも、製品を所有するユーザ

---

37 ハードローとしてのデータ契約法の方向性について、例えば、Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final (23 Feb. 2022). の第 4 章を参照。また、ハードローとしてのデータ契約法の問題点については、落合孝文ほか「座談会 EU データ法構想と包括的データ活用法制の可能性」L&T 97 号（2022 年）16-17 頁等を参照。

38 例えば、経済産業省・前掲注(5)等を参照。

39 酒井將行「データ駆動型人工知能の知的財産保護」知的財産法政策学研究 62 巻(2022)36-39 頁。

40 山本飛翔「オープンデータの活用と知財戦略」パテント 72 巻 9 号(2019)64 頁。

と第三者との間で、特定の目的を達成するために厳密に必要な場合、秘密保持のための措置が実行された上で、第三者がデータ保有者の営業秘密の開示を受けることができるといった規定（5 条 8 項）が設けられており[41]、営業秘密の保護をデータへのアクセス提供義務が上回る状況を作り出しうるものである。

日本においても、データの流通・利活用を促進するために、データへのアクセスをどこまで強化すべきか（またそれは法制度によるものか、ガイドライン等によって進めるのか）といった点が問題となりうると考えられる。

５．おわりに

本章ではノンパーソナルデータの保護および流通・利活用の促進について、知的財産法を中心に検討してきた。筆者の能力不足により雑駁なまとめとなってしまったが、お読みになる方にとって幾許かの知見を得られるものとなっていれば幸甚である。

41 前掲注(37)参照。

第７章　「データ権」創設の提言～製造業の視点から～

キヤノン株式会社知的財産法務本部知的財産渉外第三部長

長谷川正憲

１．はじめに

製造業、中でもとりわけ当社を含む電機メーカーにおいて、データを取り扱うビジネスはそれほど盛んに行われていないと思われるかもしれない。しかし、製品の開発などにおいてデータの活用は欠かせず、古くから他社／他者との間でデータをやりとりすることは頻繁に行われてきた。また、近年では事業環境やビジネス形態の変遷に伴い、ハードウェアの販売を主体とするビジネスからサービスを提供するビジネスへの比重が高まってきており、その中でもデータは非常に重要な役割を果たしている。

本稿では、システムベンダーでもサービスプロバイダーでもなく、主にハードウェア製品を主力ビジネスとしてきた当社を含む伝統的な電機メーカーを想定した場合に、その企業がビジネスにおいてどのようにデータを活用してきた（いる）のか、その際の権利処理はどうしているのかを知的財産および契約の観点を中心に考察し、データ活用を促進するためのデータ保護の望ましい制度のあり方の一案として「データ権」の創設を提案したい。

２．製造業ビジネスにおけるデータの活用

ここでは、当社のケースを参考にしながら、電機メーカーによる主なデータの活用事例を紹介する。

（１）技術導入の例

電気機器は多種多様な技術の集積によって成り立っており、また特に日本には数多くの電機メーカーが存在しそれぞれの会社が多種多様な技術を保有していることから、会社間の技術連携が非常に盛んに行われてきた。実際には一定の条件で他社に特許権の実施を許可する特許ライセンスというかたちで特許権のみを対象とするアレンジメントもあれば、もっと大がかりな、例えば半導体製造プロセスの技術導入などのように特許権のみならず製造工程やレシピ等の情報が提供される場合もある。後者の場合、提供される情報の中には当然ながら各種データも含まれる。このようなデータを含む情報はノウハウと呼ばれ、ノウハウを他社に提供し所定の範囲で利用を許可することはノウハウライセンスと呼ばれ

てきた。また、このような特許ライセンスやノウハウライセンスを含むコラボレーションは、必ずしも電機メーカー同士といった同業、競合企業間だけでなく、異業種間、産学連携または大企業とスタートアップ／ベンチャー企業間のコラボレーションなどにおいても行われている。

（２）機器から生成されるデータの例

電機メーカーが、自社が販売した製品のタイムリーな修理対応等のサポートを可能とするために､顧客の手元にある製品の使用状況や稼働状況をモニターし､そこで抽出したデータを取得して利用することもまた古くから行われてきた｡例えば複写機のビジネスの場合、顧客が使用している複写機が故障または何らかのトラブルに見舞われた際に、その症状を示すデータを含む通知がメーカーのサポート部門に届き、速やかにサービスマンが顧客のもとに出向いて修理対応するというのが､その典型的な例である｡そして近年では､IoT や DX の進展に伴ってあらゆる製品がつながり連携し、データのやりとりを通じて更に付加価値の高いサービスの提供ができるようになっている。

また、機器から取得したデータを、将来製品の開発や改善に活かすということも良く行われている。例えば当社でも医療機器の分野において、機器から得られたデータに対して AI を活用し、CT 診断装置の開発を行った。具体的には、臨床の場で得られたデータを元にディープラーニング技術を用いてノイズ低減をはじめとする CT 画像の画質改善および画像再構成技術の開発を行っている。

（３）データマネジメントサービスの例

近年特に増えてきているのが、顧客のデータを預かり、その保管とマネジメントのサポートをするデータマネジメントサービスである。例えば当社の場合でいえば複写機、プリンタやスキャナといった事務機器を開発製造している強みを活かし、顧客企業の社内に膨大に存在する各種書類を電子化し、クラウド上で保管および管理するサービスを請け負ったり、各種帳票の入出力やワークフロー管理のサポートをするサービスなども行っている。また、やはり自社で製造販売しているカメラ製品とそれを用いた撮影体験の付加価値を高めるべく、顧客が撮影した写真データを預かり、クラウド上で保管と管理のサポートを行うといったサービスもある。

このようなデータマネジメントサービスを提供するほとんどのケースにおいて、クラウ

ド環境は外部プラットフォーマーが提供するサービスを利用しており、自社でプラットフォームを構築してはいない。電機メーカーがこのようなサービスを提供するのは、その会社が取り扱っているハードウェア等の製品の機能を活かしたり付加価値を増大させるためであって、データマネジメント自体を主たる目的としているわけではないからである。

（４）データ自体を取引対象とするサービスの例

上記（１）から（３）は、多かれ少なかれ何らかのかたちでハードウェア製品の開発や販売をサポートするためにデータを利活用するケースである。これに対し、最近では電機メーカー各社もハードウェアの販売に依存しない新たなビジネスの開拓に力を入れてきており、その中でデータそれ自体を取引対象とするようなビジネスモデルも出現してきている。当社の場合、野球などスポーツの試合やアイドルのパフォーマンスなどで被写体を全周囲から多数のカメラで撮影した撮影画像を元に 3D 空間データを再構成し、顧客が好きな位置と角度から鑑賞できるような特殊なコンテンツを作成する技術を開発した。この技術を用いたビジネスでは、顧客からコンテンツの制作を請け負うことはもちろん、当社自ら制作したコンテンツを販売するようなビジネスモデルも考えられる。

このようなケースは、コンテンツ等のデータそのものを取引の対象とすることを主目的とする新しい事例といえる。

３．データを活用するビジネスの権利処理

（１）データは誰のものか

上記２（１）の技術導入のケースでは、ノウハウの提供元となる企業がデータを含めたノウハウの所有権を保有していることは自明であろう。また、２（３）のデータマネジメントサービスの場合も、元のデータの保有者即ち顧客がデータの権利を保有していることも明らかである。

しかし、例えば２（１）のケースにおいても、データの授受がなされた後、技術導入を受けた側においてその改良や改善等をした場合、その改良されたデータ（もしくはそこから元のデータを除いた改良部分）の権利が誰に帰属するかは一概に明確とはいえない。２（２）の機器から生成されるデータの場合も、機器を製造販売した電機メーカーがそのデータの権利を有するのか、または機器を利用している顧客が権利を有するのか、実際に提供されるサービスや生成されるデータの内容および性質が千差万別であることを踏まえる

と、やはり必ずしも一律に誰のものだと言い切れるわけではない。この点は、２（４）のデータ自体を取引対象とするサービスにおいても同様であるうえ、更に２（４）の場合は制作物に著作性が認められて著作物となる場合には、著作権法上の著作者の認定も絡むこととなり更に複雑となる。

従って、２（１）や２（３）の所有者が自明の場合以外のケースでは、データ全般の所有者ないしは権利者をどう認定するかについての基本理解やこれを定めた法律が存在しないため、実務においては当事者間で締結する契約の中で保有者を取り決めることとなる。

（２）データの利用条件の設定

契約においてデータの保有者を取り決める際に、そのデータの利用条件、すなわちそのデータをどのように当事者が利用できるのかについても併せて同じ契約の中で取り決めることになる。上記２で挙げたいずれのケースにおいても、それを対象とする契約書は知的財産部門がレビューするのが一般的であろう。仮にそのような契約を知的財産部門ではなく一般法務を担当する法務部門がレビューする場合であっても、少なくとも契約の対象となるデータを含むノウハウ等の帰属とその利用条件を定める部分は考え方において知的財産権の帰属ないしはライセンスと類似しており、またケースによって特許権や著作権、はたまた営業秘密などが直接関係してくることもあるため、やはり知的財産部門が担当するようになっている企業が多いと思われる。従って、データ等のノウハウの取り扱いについては、知的財産権のそれと同様の方法で設定することが多い。

具体的な条件設定の仕方について、２（１）の技術導入を例にとって紹介する。特許権とデータを含むノウハウを合わせて提供する技術導入の場合、まず特許権については技術供与側当事者（ライセンサー）が保有する特許権のうち契約の対象となる範囲を定めるが、その定め方には様々な方法がある。個々の特許番号等で特定することもあれば、対象となる製品や技術を特定してその開発や製造のために使用される特許全般というように大まかに特定したり、ある特定の日付を設定しその日以前の優先日を有する特許権すべてとすることもある。そして、いずれかの方法で特定された特許権について、所定の範囲（例えば半導体製造工程の開発と使用、その工程により半導体を製造し販売する、など）の通常実施権の許諾というかたちで技術導入側当事者（ライセンシー）に利用の許可を与える。一方、ノウハウについてもその範囲をできるだけ明確に規定したうえで利用条件を設定するが、それがデータであれその他のものであれ、また著作権や営業秘密など何らかの法律で

保護されるものであれそれ以外であれ、とりたてて区別することなくまとめて同じ条件でやはり特許権などの知的財産権と同様の所定の目的(例えば半導体製造工程の開発と使用、その工程により半導体を製造し販売する、など）に利用できる旨を取り決めている。このように、ノウハウの利用条件の設定の仕方は、特許権等の通常実施権の設定と非常に似た形になる。更に言えば、実際に導入した技術を使用するにあたっては、この技術は特許権であるとか、この技術はデータであるとか、著作物であるとか、権利の種別等を常に意識するようなことはしていない。

なお、特許権にせよノウハウにせよ、ライセンシーによる利用の結果生まれた改良技術の帰属と利用条件の設定にもまた様々なバリエーションが存在する。特許発明については特許法に定める発明者の認定と職務発明による使用者への帰属という原則があるがそれを前提として、特許権についてもノウハウについても、改良技術についての権利を（ａ）ライセンサーに移転させたうえであらためてライセンシーに利用許可をしたり、(ｂ）あくまで改良行為を行ったライセンシーの帰属としたり(その際､ライセンシーからライセンサーに対してグラントバックというかたちで改良技術についての実施許諾ないしは利用許諾をすることも考えられる)、または（ｃ）改良技術全般をライセンサーとライセンシーの共有にして両者利用可能とすることもある。ライセンシーにおいて生まれた改良技術が特許発明に該当するのかノウハウに該当するのかは厳密に切り分けられない（同じ技術であっても、特許出願するかしないかで結論が容易に変わり得ることもある）ため、特許発明とノウハウをまとめてこれら（ａ）から（ｃ）のうちいずれか同じ取り扱いとすることが多い。（ａ）から（ｃ）のどの取り扱いにして更に具体的にどのような条件設定にするかは、想定される改良技術の内容、当事者の関係、更には対価条件なども踏まえて当事者の合意のもとに決められるべきものである。

一方、技術導入の対価については、特許権とノウハウとで考え方に異なる点がある。特許権の場合、すべて一括または分割での払い切りとすることもあれば、対象製品一台あたり幾らというランニングロイヤルティ方式などが考えられる。一方、ノウハウについては、それが実際に特定の製品において使用しているのか否かの判断が困難な場合も多く、またそもそも法律等で定められた権利ではないためその権利期間の終期も定められていない。従って、ノウハウの場合にランニングロイヤルティ形式を採用すると対象が不明確なまま場合によっては永久に対価の支払が必要となることになりかねないため、その利用の対価は、払い切りで行われるのが通常である。払い切りの場合、ライセンシーがその所定の対

価を払ってしまえば提供されたノウハウについて契約の条件に従ってその後永続的に利用することができる。

また、２（２）の機器から生成されたデータの場合についても簡単に触れておきたい。前述の通り、生成されたデータが誰に帰属するのかはやはり法律等に照らしても判然とせず、契約または利用規約の中で当事者間の合意事項として帰属を定めたり、敢えて帰属には明示的に触れずに利用条件のみを定めることもある。いずれにしても、このケースでもやはり当事者間の合意が、データの帰属や利用条件を定める根拠となる。なお、とりわけ一般消費者である顧客からデータ等の情報を企業が受領する場合には、個人情報保護やその他法律上の定めに従って受領したデータの使用目的や開示範囲等を伝えたうえで同意を取得する等の措置を講じる必要があるのは当然である。

４．データの帰属と活用をめぐる制度上の課題と提言

（１）帰属における課題と「データ権」という考え方

前述の通り、特許権にせよデータを含むノウハウにせよ、その帰属は当事者間の合意である契約や利用規約で定められるのが一般的である。しかしノウハウの場合には、特許権などと違って法律等で定められた帰属に関する原則が存在せず、また取引の形態や類型も多岐に渡るため、どのような取り扱いが一般的で適切なのかという共通理解が存在しない。更には、ノウハウの所有者が定まったとしても、所有者がどのような権限（例えば独占権の有無）を有しているのかも判然としない。従って、当事者は、本来であれば自身に認められるであろう権利（帰属と権限）を意識することができないまま契約をしているケースがあるのではないか。また、帰属と権限が不明確であるが故に、実際の契約においては帰属の問題には敢えて深入りせず、知的財産権のアレンジメントから活用の部分の考え方だけを拝借し、それぞれの当事者が何をできて何をできないのかという効果面からのみ規定するにとどめることもしばしばである。

今後ますますデータの重要性と価値が高まっていくことは論を俟たない。現在のように当事者双方が権利への理解についてあやふやなまま契約を締結し続けるままで果たして良いのだろうか。むしろ、ビジネスの類型や対象となる技術やデータの内容別にその帰属と権利者に与えられる権限に関する原則的な考え方を整理し、いわば「データ権」というようなものを世界に先駆けていち早く日本で法整備することを考えても良いタイミングなのではないだろうか。そして、その「データ権」により契約当事者が原則的な制度と権限を

正確に理解したうえで、それぞれの取引における帰属や利用の具体的な条件は基本的には当事者の自由意思に任され契約にて様々なアレンジメントが設定可能になっているというのが理想的な姿ではないだろうか。このような「データ権」という権利を創設することは、以下（２）で後述する利活用段階における課題であるライセンシーの保護にもつながると考える。

なお、契約自由の原則に委ねるとはいえ、当事者の合意内容が正当な根拠なくいずれかの当事者にのみ一方的に有利なケース、例えば一方当事者によるデータの独占や囲い込みを許してしまうような条件になっているために改良技術などについてデータの利活用が阻害されてしまうおそれ生じるような条件の場合は、法律による一定の規制を及ぼすことも考えるべきである。ただしその場合は、実態を踏まえたうえで規制の対象となる行為についてできるだけ具体的に明確化し、制約が及ぶ場面を可能な限り限定的にして慎重な運用がなされるべきである。

（２）利活用における課題（ライセンシー保護の必要性）

当事者間の帰属と利用条件が明らかになったとしても、データを含むノウハウには、特許権をはじめとする知的財産権には無い課題が存在する。具体的には、ライセンサーが倒産してしまった場合や、事業譲渡などを通じて対象のノウハウに関する権利を第三者に譲渡してしまった場合に、ライセンシーが既に受領していたそのノウハウを無条件で利用し続けることができるかという問題である。本来、一旦契約にて合意が成立し、その下で利用が許可されたデータ等のノウハウは、その後のライセンサー側の行為や事情の如何にかかわらずライセンシーが継続して利用できてしかるべきである。上記３（２）で述べた通り、ノウハウ利用の対価には払い切りのアレンジメントが採用されることが多く、ライセンシーは、対価を支払った以上は対象のノウハウを永続的に利用できるという理解と期待を持っている。そのようなライセンシーの権利は当然保護されるべきだからである。

しかし、現行の法制度ではライセンシーが保護されない余地があり、不安定な立場に置かれている。この問題について、以下、データ等のノウハウと同じビジネスで取り扱われ同じ契約で定められることも多い特許権や著作権、更には不正競争防止法で保護される営業秘密や限定提供データの場合と比較しながら見ていきたい。

①　特許権の場合

特許権については、平成 23 年法改正によっていわゆる当然対抗制度が導入され、通常

実施権は何らの要件を備えなくとも権利の発生後の第三者に対抗できることとなった（特許法第 99 条）。従って、何らかの事情でライセンサーから第三者に権利が移転した場合であっても、ライセンシーは引き続きその権利を実施し続けることができるため、問題はない。

② 著作権の場合

著作権についても令和 2 年改正で同様に当然対抗制度が導入され（著作権法第 63 条の 2）、基本的には問題はなくなった。ただし、著作物のうちソフトウェアの場合には未だ解決できていない課題があると思われるので、必ずしもデータの話ではないが関連する話としてここで指摘しておきたい。

製品に搭載するファームウェアや、サービスに利用するアルゴリズムなどのソフトウェアを外部から調達する場合、そのソフトウェアについてプログラミング言語等の人間が理解でき改変できるソースコードのかたちで提供される場合は、稀である。ソースコードは提供元のソフトウェアベンダーにとってのいわば製品設計図であり、ノウハウの固まりだからである。また、導入する企業側においても、むやみに外部からソースコードを受け取って秘密保持等の不要な義務を負うのは避けたいという事情がある。従って、大多数の取引において提供されるのは、コンピュータ上で実行可能な、人間では解読できないブラックボックスの二値データ、いわゆるオブジェクトコードのみである。このような場合、著作権法上の当然対抗制度で保護されるのは、あくまでオブジェクトコードの利用権ということになる。しかし、ソフトウェアは絶えずアップデートを繰り返していかなければならないため、ソフトウェアの供給元がソースコードとその権利を保有していてアップデートに対応してくれている間は良いものの、もし供給元が倒産やその他の事情でソフトウェアを手放し、アップデートの対応をできなくなってしまった場合、導入した企業はその後のビジネスにおいて自己の製品やサービスに使用しているソフトウェアのアップデート対応をできないという深刻な状況に陥る。解決策のひとつとして、ライセンサーとライセンシーが取引を開始する段階でソースコードを第三者（エスクロウ・エージェント）に預託し、ライセンサーが倒産等した場合、エスクロウ・エージェントがエスクロウ契約で予め定められている一定の条件の下でそのソースコードをライセンシーに開示するソフトウェア・エスクロウという仕組みが提供されている。しかし、必ずしもライセンサーがライセンシーの保護のためにソフトウェア・エスクロウの利用に同意するとは限らないし、敢えて有償でこのようなサービスを利用せずとも何らかの制度的な手当てによってライセンシーの保

護が図られた方が望ましいのは当然である。

③　営業秘密および限定提供データの場合

データを含むノウハウは、不正競争防止法に定める営業秘密または限定提供データに該当する場合は同法の保護対象となる。しかしながら不正競争防止法には、特許法や著作権法等に設けられている権利者から許諾を受けたライセンシーの保護に係る規定、すなわち当然対抗制度が存在しない。まさにこの点について、同法の改正も見据えて各種論点の審議を行っている経済産業省 産業構造審議会 知的財産分科会 不正競争防止委員会でも議論と検討がなされたが、2022 年 12 月 14 日付で経済産業省からパブリックコメント募集とともに発表された「デジタル化に伴うビジネスの多様化を踏まえた不正競争防止法の在り方（案）」に詳説されているように、「営業秘密及び限定提供データに関するライセンシーの保護制度の措置にあたっては、法理論上なお整理すべき課題がある中で、特許法等と同様の制度措置を行うことへの潜在的なニーズは存在するものの、現時点では実際のトラブル事例が顕在化していないことから、実務の動向を注視し、取り得る措置について、関係省庁等と調整しつつ、引き続き検討を継続していく」との結論となり、残念ながら当面の手当ては見送られている。ここで「法理論上なお整理すべき課題」として様々な指摘がされているが、とりわけ利用権アプローチ（営業秘密等を利用する利用権を新たに設定し、当該権利の対抗力を規定するアプローチ）については、「不競法で保護される営業秘密等が事業譲渡等に伴い移転された場合については、特許権等の譲渡とは異なり何らかの権利が同一性を保って移転したとみることはできず、譲受人が現に保有する情報が営業秘密等の要件を満たすときに、不正競争に該当する行為を行っている者に対して不競法上の差止請求権や損害賠償請求権が成立するか否かが問題となる」とのことである。つまり、不正競争防止法による営業秘密や限定提供データの保護は、あくまで第三者による不正取得や不正使用を禁じる行為規制のかたちで設けられているだけであり、営業秘密や限定提供データそれ自体には、特許権や著作権のような何らかの権利があるわけではないという指摘である。この指摘に対しては、営業秘密や限定提供データにも権利を付与する制度を創設することが、最も直接的な解決策になるのはいうまでもない。そのうえであれば、利用権について他の知的財産法と同様に当然対抗制度を設けることが可能になるのではないだろうか。

④　データを含むノウハウの場合

一口にデータを含むノウハウといってもその範囲は非常に広く、ものによって特許権、

著作権の対象にもなり得ることもあれば、または営業秘密や限定提供データに該当する可能性もあるが、もちろんこれらのいずれにも該当しないデータも多く存在する。従って、データを保護するための権利は、やはりこれら諸法とは別の枠組みで「データ権」という独自の権利として設けることが望ましい。仮に「データ権」と他の法律に基づく保護（例えば限定提供データ）に二重に該当することになったとしても、それは趣旨が異なる複数の法律の保護対象になったというだけのことであり、むしろ二重のプロテクトの中で権利者がどのような救済を受けるかを決定できる方が、データ保護の観点からはメリットが大きいであろう。

そして、「データ権」を創設したうえで、他の知的財産権と同様に当然対抗制度も導入すれば、ライセンシーは後の事情の変化を心配することなく安心して利用を継続することができる。

５．今後の検討に向けて

本稿は、あくまで電機メーカー、それも伝統的にハードウェアビジネスを主力事業としてきた企業の視点からデータ活用の実態とその課題を紹介したうえで、「データ権」の創設という提言を行った。しかし、実際に「データ権」の制度設計をするにあたっては、考慮すべき事項が山積している。例えば（ａ）他の業界、とりわけデータをまさにビジネスの対象として扱っている企業において問題意識に異なるところは無いのか（「データ権」などという新たな権利を創設して本当に問題は無いのか）、（ｂ）本稿で紹介した以外の、筆者が想定できていないまったく別のデータ活用の実態があったときに「データ権」はどのように影響するのか、（ｃ）データが創出される状況にはどのようなバリエーションがあり、それぞれの場合においてデータの保有者、権利者はどのように定められるのが適切なのか、（ｄ）「データ権」を取得した権利者に認められるべき権限はどのようなものが望ましいのか、（ｅ）データは容易に国境を超え海外において使用されることも想定されるが、そのような場合に日本法に基づく「データ権」にどう実効性を持たせることができるのか、そして何より（ｆ）特許権や著作権のように権利対象がはっきりとしておらず、ともすれば日々変更が加ったり他のデータと混ざってしまうことも容易に有り得るデータというものに対して果たして適切に権利を与えることができるのか、といった課題がすぐに思い浮かぶ。これら課題の検討にあたっては、様々な業種の様々な立場の方々から情報収集をして分析のうえ課題を整理し、更には法制度との関係では学識者有識者の知見をいただきながら慎

重に進めていく必要がある。

確かに不正競争防止小委員会の取りまとめで言われているように、現時点ではデータに関するトラブル事例がそれほど顕在化していないというのは事実であろう。しかし、だからといって当面状況を見守るのではなく、今後世界的にデータ利活用の重要性が増していくことを見据えて検討を進め、世界に先駆けて日本でいち早く制度導入することができれば、データの利活用を更に促進し、ひいては日本の産業を活性化することにつながると考える。

本稿による提言が、データ活用と保護のあるべき制度を検討されるうえで少しでも参考になれば幸いである。

第８章　米国におけるデータの保護制度
～米国統一商事法典（UCC）第 12 編の新設～

法律事務所 LAB-01
米国弁護士（ニューヨーク州、ワシントン DC）
FIP、CIPM、CIPP/E、CIPP/US

望月　健太

１．はじめに

経団連の提言「DFFT 推進に向けたデータ流通政策」が述べているように、我が国においては、現行の法律に照らせばデータは無体物であり、民法上の所有権の対象とはならないため、所有権の概念に基づいてデータに関する権利の有無を定めることはできない[1]。そこで、各法がデータの分類や側面に応じてその適正な取扱いを定めながら、契約等の私的自治の下で保護や利活用に供されている状況である。例えば、個人データについては個人情報保護法等が規定しつつ、非個人データについては不正競争防止法の他、著作権法、特許法、商標法、実用新案法、意匠法を含む知的財産権に関連する法令等が規定しているが、これらの法令等によってカバーされないデータも含め、契約実務上必要な規定が置かれている状況である[2]。

この点、個人データ及び非個人データいずれの取扱いについても、法定要件を超えた部分或いは法令等の定めがない部分のみならず、法令等が定める部分の具体的な運用についてさえ、必ずしも公平かつ画一的な取扱いがなされている訳ではなく、とりわけ取引当事者ではない第三者との関係についてはさまざまな運用がなされているのが実情である。これが契約交渉の場合であれば、市場環境や商慣習、当該案件の性質・取引固有の事情、当事者の立場といったさまざまな考慮要素に左右されるため一定程度致し方ない部分はあるが、第三者の保護については、どこまで法令等で定めていくのか、どこまで私的自治に委ねるのかを、テクノロジーやビジネスモデルの進展を横目に見ながら検討を続けていく必要がある。とりわけ、欧米各国のデータ関連政策が数年後我が国に輸入される傾向がより一層顕著になっているが、単純に社会経済文化的背景の異なる欧米各国のデータ関連政策をそのまま我が国に持ち込むのではなく、そこから示唆を得ながら「日本ならでは」の

1　一般社団法人 日本経済団体連合会「提言『DFFT 推進に向けたデータ流通政策』」（2021 年 11 月 16 日）6 頁。
2　経済産業省「AI・データの利用に関する契約ガイドライン　1.1 版」（2019 年 12 月）、14-26 頁、https://www.meti.go.jp/press/2019/12/20191209001/20191209001-1.pdf（2022 年 11 月 23 日最終閲覧）。

データ関連政策を打ち出していくことが非常に重要であり、その意味で欧米各国のデータ関連政策をまず正確に理解することが必要不可欠である[3]。

そこで本稿では、数ある欧米各国のデータ関連政策の中から、米国におけるデータに関する法制度の最新動向を取り上げたい。というのも、例えば欧州におけるデータ関連政策や法制度については既に多くの先行研究が見られ、また実際に我が国のデータ関連政策や実務にも大きな影響を及ぼしているところ、長きにわたる官民両方の強固な日米関係を踏まえれば、本来米国におけるデータ関連政策や法制度についても同程度ないしはそれ以上に考慮に入れた上で政策立案を行っていく必要があろう。特に、後述するように、2022 年 7 月に米国統一商事法典（Uniform Commercial Code: UCC）が修正され、「支配可能な電子記録（Controllable Electronic Record: CER）」に関する第 12 編が新設されたことは注目に値するものであり、Web 3.0 を推進する我が国としても無視できない政策動向である[4]。こうした状況を踏まえ、本稿では、まず米国におけるデータに関わる法令を簡単に紹介した後、UCC 第 12 編の内容について詳述し、最後に我が国のデータ関連政策ないし法制度への示唆について述べることとする。

２．米国におけるデータの法的位置づけと関係法令の現状

英米財産法上、財産は、物的財産（real property）と人的財産（personal property）とに分類され、前者は日本の不動産とほぼ同義であり、後者は動産（chattel）と無体財産（intangible property）とに分類される[5]。この点、動産は狭義の有体物としての財産の意味で用いられることが多いものの[6]、例えば後述する米国統一商事法典（UCC）の第 9 編（担保取引）では、動産自体を具体的に定義してはいないものの、権原証書（documents）、動産抵当証書（chattel paper）、売掛債権（accounts）その他の無体財産等を含む幅広い概念として捉えられており、時代の要請とともにその範囲は徐々に拡大されてきていると言われている[7]。なお、UCC 第 9 編は、一般無体財産（general

---

3 望月健太「『Data Free Flow with Trust』の意味を考える」（merpoli、2019 年 3 月 20 日）、https://merpoli.mercari.com/entry/2019/03/20/070000（2022 年 11 月 23 日最終閲覧）。

4 「経済財政運営と改革の基本方針 2022　新しい資本主義へ～課題解決を成長のエンジンに変え、持続可能な経済を実現～」（2022 年 6 月 7 日）17 頁、https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/2022/2022_basicpolicies_ja.pdf（2022 年 11 月 23 日最終閲覧）。

5 田中英夫編代『英米法辞典』（東京大学出版会、2006 年）675 頁。なお、無形財産には、預金、株式、社債、公債等や各種無体財産権の他、一般の債権も含まれるとされている。

6 同上、140 頁。

7 日本銀行信用機構室「米国の動産担保法制について」（日本銀行調査月報、2003 年 8 月号）3 頁。

intangible）の定義を置いており、売掛債権、動産抵当証書、商業不法行為債権（commercial tort claims）、預金口座（deposit accounts）、権原証書、物品、証書、投資財産、信用状権利（letter-of-credit rights）、信用状（letters of credit）、貨幣、採掘前の石油、ガス、その他の鉱物以外の、行為物を含むあらゆる人的財産を意味するとし、支払無体財産（payment intangibles）及びソフトウェアも含まれるとしている[8]。

英米の物権法は、権原（title）や不動産権（estate）概念を中心に構成されているため、所有権（ownership）という用語の意味についても厳密に用いられている訳ではなく[9]、よってその権利の対象も有体物の場合もあれば知的財産権のような無体物の場合もあり得る。

以上を踏まえると、米国においては、日本のように「データは無体物であり民法上の所有権の対象とはならない」とまで言い切ることはできないと思われるものの、少なくともデータという観点からは整理されておらず、それぞれの法令がデータの分類や側面に応じてケースバイケースで適用され得るといった理解が適切であろう。そして、それぞれの法令がデータの分類や側面に応じてその適正な取扱いを定めながら、契約等によってもその保護や利活用が定められている点は、日本と近い状況にあると考えられる。もっとも、米国は第一次的法源として判例法主義を採用しており先例拘束の原則があること、法的救済についてはコモンローに基づく救済とエクイティに基づく救済に区別されること、そして本稿との関係では、米国は連邦制を採用しているため、連邦法と州法でさまざまな法令が存在することにも注意を要する[10]。以下では、個人データと非個人データに分けて、米国における法令の現在の状況について概説する。

（１）個人データ

前述のように、米国では大きく連邦法と州法の 2 種類があるが、まず日本の個人情報保護法や EU の一般データ保護規則（General Data Protection Regulation: GDPR）のような、個人データの保護に関する包括的な連邦法はまだ存在しておらず、セクター毎にさまざまな連邦法が制定されている状況である。もっとも、2022 年 7 月 20 日、「米国データプライバシー保護法（American Data Privacy and Protection Act: ADPPA）」の法案

8 UCC §9-102(a)(42). なお、ソフトウェアとは、コンピュータ・プログラムおよび当該プログラムに関連する取引に関連して提供される補助的な情報を意味し、物品の定義に含まれるコンピュータ・プログラムは含まれないとされている。UCC §9-102(a)(76).

9 田中・前掲注 5)『英米法辞典』614 頁。

10 小田哲明=クリス・ミズモト「米国におけるデータの保護および国際間移転」（日本知財学会誌 Vol.16 No.2-2019）13 頁。

が、米国における連邦レベルの包括的な個人データ保護法案として史上初めて議会に提出されることが可決され[11]、現在も米国議会で審議が続けられている状況である。これについては、同年 8 月 15 日、米国カリフォルニア州プライバシー保護局（California Privacy Protection Agency: CPPA）が、ADPPA に反対する旨の書簡をナンシー・ペロシ下院議長（民主党、カリフォルニア州）及びケビン・マッカーシー下院議員（共和党、カリフォルニア州）宛てに送付した模様であり[12]、ADDPA の成立可能性についてはまだ予断を許さない状況となっている。

既存のセクター毎の連邦法については、紙面の関係上全ての連邦法を網羅的に解説することは困難ではあるものの、大きく分けて以下のような連邦法が存在している状況である。

① 医療プライバシー分野[13]

医療プライバシー分野については、1970 年に制定された「包括的なアルコール乱用及びアルコール依存症の予防、治療及びリハビリテーション法」や 1972 年に制定された「薬物乱用防止、治療及びリハビリテーション法」における秘密保持要件を実施する「薬物使用障害患者記録の守秘義務に関する規則」、1996 年に制定された「医療保険の相互運用性と責任に関する法律（Health Insurance Portability and Accountability Act: HIPAA)」、2009 年「アメリカ復興・再投資法」の一部として制定された「経済的・臨床的健全性のための医療情報技術法（Health Information Technology for Economic and Clinical Health Act: HITECH)」、2008 年に制定された「遺伝情報差別禁止法（Genetic Information Nondiscrimination Act)」、2016 年に制定された「21 世紀治癒法」等が挙げられる。

この点、医療保険の相互運用性と責任に関する法律（HIPAA）を例に挙げれば、同法は保護対象保健情報（protected health information: PHI）及び電子保護対象保健情報

---

11 西村あさひ法律事務所「米国の連邦レベルでの個人情報保護法に関する最新動向 American Data Privacy and Protection Act (ADPPA)の議会への提出」（個人情報保護・データ保護規制ニューズレター、2022 年 7 月 22 日号)、
https://www.nishimura.com/sites/default/files/newsletter_pdf/ja/newsletter_220722_data_protection.pdf（2022 年 11 月 23 日最終閲覧)。

12 California Privacy Protection Agency, Re: H.R. 8152, The American Data Privacy and Protection Act – Oppose (August 15, 2022), https://cppa.ca.gov/pdf/hr8152_oppose.pdf (last visited November 23, 2022).

13 PETER SWIRE & DEBRAE KENNEDY-MAYO, U.S. PRIVATE-SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS (2d ed. 2018) PP. 163-186. なお、HIPAA プライバシールールの条文については、
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html 参照（2022 年 11 月 23 日最終閲覧)。

（electronic protected health information: ePHI）を保護の対象としており、保健医療提供者、保健計画、保健医療クリアリングハウスといった事業者のみならず、そうした適用事業者に代わって保護対象保健情報（PHI）等を取り扱う事業提携者（business associate）にも適用される。その上で、いわゆる「HIPAA プライバシールール（HIPAA Privacy Rule)」というものがあり、対象事業者は原則としてプライバシーノーティスを制定しなければならず、また保健医療目的での保護対象保健情報（PHI）等の利用・開示は可能であるものの、それ以外は本人のオプトイン同意が必要であるとか、本人には事業提携者を含む対象事業者に対し保護対象保健情報（PHI）等へのアクセス権や複製権が認められている等がある。

② 金融プライバシー分野[14]

金融プライバシー分野においては、1970 年に制定された「公正信用報告法（Fair Credit Reporting Act: FCRA)」、同法を修正する法案として 2003 年に成立した「公正かつ正確な信用取引法（Fair and Accurate Credit Transactions Act: FACTA)」、1999 年に制定された「グラムリーチブライリー法（Gramm-Leach-Bliley Act: GLBA)」、2010 年に制定された「ドッド＝フランク・ウォール街改革・消費者保護法」の他、1970 年に制定された「銀行秘密法」や 2001 年に制定された「国際的なマネーロンダリング防止及びテロ資金供与防止法」も挙げることができる。

この点、グラムリーチブライリー法（GLBA）を例に挙げれば、同法は金融機関による非公開個人情報（nonpublic personal information）の取扱いについて規定したものであり、より厳しい州法に専占せずまた私的訴権（private right of action）もないが、顧客に対する初回及び年次のプライバシー通知が必要であるとか、関連のない第三者（nonaffiliated third parties）に非公開個人情報を開示する場合には、原則として消費者にその旨事前に明示するとともに、オプトアウトの機会を提供しなければならない等が規定されている。

[14] *Id.* at 187-216. なお、グラムリーチブライリー法（GLBA）の条文については、https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf 参照（2022 年 11 月 23 日最終閲覧)。

③ 教育プライバシー分野[15]

教育プライバシー分野においては、1974 年に制定された「家族教育の権利とプライバシーに関する法（Family Educational Rights and Privacy Act: FERPA）」及び「児童の権利保護に関する修正（Protection of Pupil Rights Amendment）」、2001 年に制定された「どの子も置き去りにしない法（No Child Left Behind Act）」が挙げられる。

この点、家族教育の権利とプライバシーに関する法（FERPA）を例に挙げれば、同法は政府助成金を受領している全教育機関に適用され、学生の教育記録（education record）や当該記録に含まれる個人識別可能情報（personally identifiable information）を保護するものである。同法では、次のいずれかの要件に該当しない限り、教育記録の第三者に対する開示が原則としてできないこととなっている：①個人が識別可能ではない情報であること、②ディレクトリ情報であって学生がその開示を拒否していないこと（但し当該ディレクトリ情報の作成・使用前に学生にオプトアウトや開示拒否の機会を提供しなければならない）、③親権者又は 18 歳以上の学生（或いは大学生）の同意があること、④親権者又は 18 歳以上の学生（或いは大学生）本人への開示であること、⑤健康安全目的（health or safety purposes）といった例外に該当すること、である。もっとも、学生の教育記録から個人識別情報を本人の同意なく開示できる例外も複数規定されているところ、成績指標値（Grade Point Average: GPA）のような成績情報は学生本人のオプトイン同意がない限り開示できないとされている。

④ テレマーケティング及びマーケティングプライバシー分野[16]

テレマーケティング及びマーケティングプライバシー分野においては、1991 年に制定された「電話消費者保護法（Telephone Consumer Protection Act: TCPA）」、「電話勧誘による消費者詐欺・侵害防止法（Telemarketing and Consumer Fraud and Abuse Prevention Act）」に基づき 1995 年に制定された「電話勧誘販売規則（Telemarketing Sales Rule: TSR）」、2005 年に制定された「迷惑ファクシミリ禁止法（Junk Fax Prevention Act: JFPA）」、2003 年に制定された「未承諾のポルノグラフィーおよびマーケティング攻撃に対する規制法（Controlling the Assault of Non-Solicited Pornography

---

15 *Id.* at 217-230. なお、家族教育の権利とプライバシーに関する法（FERPA）の条文については、https://www.ecfr.gov/current/title-34/subtitle-A/part-99 参照（2022 年 11 月 23 日最終閲覧）。

16 *Id.* at 231-262. なお、未承諾のポルノグラフィーおよびマーケティング攻撃に対する規制法（CAN-SPAM）の条文については、https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf 参照（2022 年 11 月 23 日最終閲覧）。

and Marketing Act: CAN-SPAM）」、1996 年に制定された「電気通信法（Telecommunications Act）」、1984 年に制定された「ケーブルコミュニケーション政策法（Cable Communications Policy Act）」、1988 年に制定された「ビデオプライバシー保護法（Video Privacy Protection Act: VPPA）」が挙げられる。

この点、未承諾のポルノグラフィーおよびマーケティング攻撃に対する規制法（CAN-SPAM）を挙げれば、同法は、米国に向けて又は米国から電子メールによる製品又はサービスの広告を行う全ての者に適用されるものであり、商用電子メールの内容を規制しつつ、無料のオプトアウトを義務化している。また、連邦通信委員会（FCC）の実施規則によりモバイルサービスの商用メッセージ（mobile service commercial messages: MSCMs）についても規制しており、例えばショートメッセージサービス（SMS）で商用メッセージを送信する前に対象者本人からオプトイン同意を取得しなければならないとされており、また対象者本人がいつでも当該同意を撤回できるようにしなければならないと規定している。なお、同法は州法に専占するものの、私的訴権はない。

⑤ 職場プライバシー分野[17]

職場プライバシー分野においては、前提として年齢、国籍、障害の有無といった理由に基づく差別を広く禁止する複数の連邦法がベースとして存在するが、ます福利厚生管理の観点からは、上記の HIPAA に加えて、1985 年に制定された「包括予算調整法（Consolidated Omnibus Budget Reconciliation Act: COBRA）」、1974 年に制定された「従業員退職所得保障法（Employee Retirement Income Security Act: ERISA）」、1993 年に制定された「育児介護休業法（Family and Medical Leave Act: FMLA）」が存在し、データの収集や記録保持の観点からは、前述の FCRA や 1938 年に制定された「公正労働基準法（Fair Labor Standards Act: FLSA）」、1970 年に制定された「労働安全衛生法（Occupational Safety and Health Act: OSHA）」や 1989 年に制定された「内部通報者保護法（Whisleblower Protection Act）、1935 年に制定された「全国労働関係法（National Labor Relations Act: NLRA）」や 1986 年に制定された「移民改革統制法（Immigration Reform and Control Act: IRCA）」、そして 1934 年に制定された「証券取

[17] *Id.* at 263-300. なお、障がいを持つアメリカ人法（ADA）の条文については https://www.ada.gov/law-and-regs/ada/ を、
公正信用報告法（FCRA）の条文については https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf をそれぞれ参照（2022 年 11 月 23 日最終閲覧）。

引所法（Securities Exchange Act）」も挙げられる。この他、1988 年に制定された「ポリグラフ使用従業員保護法（Employee Polygraph Protection Act）や、1968 年「通信傍受法（Wiretap Act）」、1986 年「電子通信プライバシー法（Electronic Communications Privacy Act: ECPA）」、1986 年「通信保存法（Sored Communications Act: SCA）」を含む電子監視法も挙げられる。

この点、雇用前のバックグラウンドチェックを例に挙げれば、特定の専門家に対するバックグラウンドチェックが法令で求められているケースもあるが、公開情報をベースに候補者のバックグラウンドチェックを行う限りは一般的に合理的な慣行であるとされている。他方、バックグラウンドチェックが差別的であるとして制限される根拠として、いくつもの法令が援用されることがあり、注意が必要である。特に、「障がいを持つアメリカ人法（Americans with Disabilities Act: ADA）」がオファー前後のメディカルスクリーニングを規制していたり、公正信用報告法（FCRA）が雇用者によるリファレンスチェック目的での調査用消費者報告（investigative consumer report）の取得を規制していたりするため、候補者の雇用前のステップを慎重に進める必要がある。もっとも、雇用後についても職場モニタリング等に対するさまざまな規制があることは言うまでもない。

次に、州法については、ほぼ全ての州でデータ侵害通知法が定められている他、セクター毎にさまざまな個人データの保護に関する法律が制定されている状況である[18]。もっとも、2020 年に施行された「カリフォルニア州消費者プライバシー法（California Consumer Privacy Act: CCPA）」を皮切りに、コロラド州、コネチカット州、バージニア州、ユタ州が個人データの保護に関する包括的な州法を定めている状況であり、カリフォルニア州においては、2023 年 1 月より、CCPA を大幅に改正する「カリフォルニア州プライバシー権法（Carifornia Privacy Rights Act: CPRA）」が施行される予定となっている[19]。このカリフォルニア州プライバシー権法（CPRA）については、2023 年 1 月下旬から 2 月上旬頃に見込まれている施行規則の制定が待たれるところではあるが[20]、一定の要件を満たす事業者に適用され、第三者やサービスプロバイダー、契約者との関係につ

---

18 *Id.* at 39-66.

19 International Association of Privacy Professionals (IAPP), US State Privacy Legislation Tracker: Comprehensive Consumer Privacy Bills (2022), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf (last visited November 23, 2022).

20 David Stauss, CPPA Board Advances Proposed CPRA Regulations (Husch Blackwell LLP, October 29, 2022), https://www.bytebacklaw.com/2022/10/cppa-board-advances-proposed-cpra-regulations/ last visited November 23, 2022).

いても規律がある[21]。また、利用目的の通知等に関する規定や所定の要件を満たすプライバシーポリシーの開示や更新に関する規定、消費者による権利行使への対応等に関する規定も広範に含まれている[22]。この点、消費者の個人情報の第三者への売却や共有に際しては、消費者に対し通知を行うとともにオプトアウトの権利を原則として認めなければならない点や、消費者による権利行使を理由とした差別が禁止されている点、いわゆる「ダーク・パターン」を用いて得られた消費者の同意は有効ではないとされている点が特徴的である[23]。

（２）非個人データ

次に、非個人データである。米国においても、他国と同様に非個人データという切り口でその活用や保護に関し包括的に規定した連邦法や州法は存在せず、対象となる非個人データの種類によって、それぞれ連邦法及び州法で定められている状況である。以下では、いくつか代表的なものを取り上げる。

①　営業秘密

まず、営業秘密についてである。営業秘密は、先例拘束の原則の下、州法におけるコモンローに基づき、不法行為に対する民事的救済により保護されてきた[24]。営業秘密の保護に関する統一的な見解を示すモデル法として、1939 年に制定された不法行為法リステイトメント及び 1979 年に制定された統一営業秘密法（Uniform Trade Secret Act: UTSA）があり、各州が採択することで州法として制定されてきた[25]。そのような中、連邦レベルにおいては、まず刑事法分野において営業秘密の保護を強化するため、1996 年に連邦経済スパイ法（Economic Espionage Act: EEA）が制定され、長年にわたり運用されてきたが、2016 年に同法を改正する形で、連邦営業秘密保護法（Defend Trade Secrets Act: DTSA）が制定されたことによって、連邦レベルでも民事的救済を求めることが可能になっている[26]。もっとも、DTSA と州法は併存する形になっていることから、

---

21 カリフォルニア州プライバシー権法（CPRA）の条文については、https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20 Version%203%29_1.pdf を参照（2022 年 11 月 23 日最終閲覧）。

22 同上。

23 同上。

24 小田=ミズモト・前掲注 10)「米国におけるデータの保護および国際間移転」14 頁。

25 同上。

26 三菱 UFJ リサーチ＆コンサルティング「海外におけるデータ保護制度に関する調査研究 調査報告書」（平成 29 年度産業経済研究委託事業、2017 年 11 月）9 頁、https://www.meti.go.jp/meti_lib/report/H29FY/000807.pdf（2022 年 11 月 23 日最終閲覧）。

実務上は、営業秘密の不正使用に対し DTSA 又は関係する州法のいずれに基づく主張を行うべきかが重要となっている[27]。この点、営業秘密の不正使用に対する DTSA に基づく救済手段としては、①事前通告なしの差押命令（ex-parte seizure）、②差止命令（injunction）、③損害賠償請求、そして④故意又は悪意による営業秘密の不正使用時に認められ得る懲罰的損害賠償（exemplary damages）がある[28]。

② 著作権

次に、著作権についてである。まず連邦憲法第 1 条第 8 項第 8 号は、「連邦議会は、著作者及び発明者に対して、それぞれ著作及び発明に対する排他的権利を一定の期間に限り付与することにより、科学及び有用な技芸の振興を促進する・・・権限を有する」と規定している。この点、同規定の解釈から、当初は実演といった固定されていない著作物は同規定に基づいて著作権法の対象にすることができず、そこに州の著作権法が成立する余地があったとされる[29]。もっとも、1976 年に制定された現行の連邦著作権法においては、固定された著作物は発行・未発行を問わずその保護の対象とされており、州の著作権法は未固定著作物のみを保護の対象としている状況である[30]。この 1976 年連邦著作権法については、いわゆる「額に汗（sweat of the brow）」理論を用いて編集著作物や事実・データを集積した編集物を保護してきたが[31]、Feist 連邦最高裁判所判決以降、最低限度の創造性（minimal degree of creativity）が要求されることとなったため、編集著作物としてではなくデータ自体に価値がある場合は、著作権による保護は限定的になる可能性があるとされている[32]。なお、著作権侵害に対する救済手段としては、①差止請求、②廃棄請求、③損害賠償請求、④訴訟費用回避請求、⑤弁護士費用回復請求、⑥刑事制裁、⑦輸入差止措置等があり、懲罰的賠償はない[33]。

---

27 浅井敏雄「2016 年米国連邦民事トレードシークレット保護法の概要」（月刊パテント Vol.69 No.15、2016 年 12 月）98 頁、https://system.jpaa.or.jp/patents_files_old/201612/jpaapatent201612_098-107.pdf (2022 年 11 月 23 日最終閲覧)。

28 18 U.S.C. § 1836. 同上、101-103 頁。

29 山本隆司「アメリカ著作権ビジネスを探る」（Right Now! 2003 年 10 月号（創刊 2 号））29 頁、http://www.itlaw.jp/Right%20Now.pdf（2022 年 11 月 23 日最終閲覧）。

30 同上。

31 三菱 UFJ リサーチ＆コンサルティング・前掲注 22)「海外におけるデータ保護制度に関する調査研究調査報告書」 9 頁。

32 小田=ミズモト・前掲注 10)「米国におけるデータの保護および国際間移転」15 頁。

33 17 U.S.C. § 502, 504, 505, 506, 603. 遠藤誠「米国（アメリカ）の知的財産法」（BLJ 法律事務所、2014 年 12 月 24 日）6 頁、https://www.bizlawjapan.com/wp-content/uploads/usa_chizaihou_01.pdf（2022 年 11 月 23 日最終閲覧）。

この他、1998 年には、1976 年連邦著作権法を改正する形で、デジタルミレニアム著作権法（Digital Millennium Copyright Act: DMCA）が制定され、いわゆる「ノーティスアンドテイクダウン」の制度や、コピーコントロールやアクセスコントロールといった著作権保護システムの回避の禁止をはじめとする新たな規定が導入された[34]。

③　特許権及び商標権等

そして、特許権及び商標権についても簡単に触れておきたい。

まず、米国における特許法の歴史は長く、最初の連邦特許法は 1790 年に制定された[35]。その後、連邦特許法は、判例の積み重ねとともに何度も改正されてきたが[36]、2011 年のリーヒ・スミス米国発明法（Leahy-Smith America Invents Act）は、それまで米国が何年にもわたり維持してきた「先発明主義」を、当時既に多くの国が採用していた「先願主義」に移行する等、連邦特許法にとって大きな転換点となるものであった[37]。これにより、同一の内容の発明であっても、先に出願されたものが優先されることとなった。

連邦特許法上、特許を受けることができる対象（＝法定主題（Statutory Subject Matter)）が明確に規定されている訳ではなく、判例や米国特許商標庁（United States Patent and Trademark Office: USPTO）が作成・公表している「特許審査手続マニュアル（Manual for Patent Examination Procedure: MPEP)」が手がかりとなる[38]。それによれば、情報ないしデータ自体やコンピュータ・プログラムないしソフトウェア自体のような物理的又は有形的な形状を伴わないものは法定主題の製品（products）には該当しないとされており[39]、また、物理的又は有形的な要素を伴うデータであっても判例上の例外（抽象的アイデア、自然現象、又は自然法則）であり、かつ他の要素が判例上の例外を著しく超えるものでなければ特許適格性を満たさないとされている[40]。特許として保護されるためには、新規性や非自明性等の特許要件を満たす必要もあり、データ自体に価値が

---

34 文化庁「インターネット上の著作権侵害（海賊版）対策 ハンドブック―米国編―」（2021 年 3 月）27 頁、
https://www.bunka.go.jp/seisaku/chosakuken/kaizoku/assets/pdf/kaizokuban_handbook_usa.pdf（2022 年 11 月 23 日最終閲覧）。

35 遠藤・前掲注 33)「米国（アメリカ）の知的財産法」2 頁。

36 Ladas & Parry LLP, A Brief History of the Patent Law of the United States (May 7, 2014), https://ladas.com/education-center/a-brief-history-of-the-patent-law-of-the-united-states-2/ (last visited November 23, 2022).

37 *Id.*

38 United States Patent and Trademark Office (USPTO), Manual of Patent Examining Procedure (MPEP), Ninth Edition, Revision 10.2019, Last Revised June 2020, https://www.uspto.gov/web/offices/pac/mpep/s2106.html#ch2100_d29a1b_139b2_397 (last visited November 23, 2022).

39 *Id.* at §2106.03 Eligibility Step 1: The Four Categories of Statutory Subject Matter [R-10.2019].

40 小田=ミズモト・前掲注 10)「米国におけるデータの保護および国際間移転」15 頁。

あったとしても、特許権による保護は限定的になる可能性があるとされている[41]。なお、仮にデータ自体について特許権が付与された場合であって、当該特許権の侵害が行われたときは、特許権者は、差止め[42]や損害賠償請求[43]を行うことができる。

次に、米国の商標制度は、連邦商標法（ラナム法（Lanham Act）；米国特許商標庁（USPTO）における商標登録により、米国全州に及ぶ権利が発生)、州商標法（各州において商標を実際に使用することにより、実際に使用している州内において権利が発生）及びコモンロー（商標を実際に使用することにより、実際に使用している地域に限定される形で権利が発生）から構成されている[44]。この点、連邦商標法について言えば、①不道徳、欺瞞的、中傷的な商標、②アメリカ合衆国、アメリカの州や自治体、または外国の旗章や紋章を含む商標、③生存中の特定の個人又は死去した米国大統領を示す名称を含む商標、④連邦商標登録されている又は米国において使用が継続する商標・商号と混同、誤認、欺罔を生じる可能性のある商標、⑤記述的商標又は欺罔を生じ得る記述となる商標、⑥地理的名称を示す又は地理的誤認を生じさせる商標、⑦苗字であるに過ぎない商標、⑧全体的に機能的である商標は、原則として連邦商標登録することができないとされている[45]。なお、仮に商標権侵害が行われた場合には、差止めや金銭的救済を求めることができる[46]。

この他、意匠制度については連邦特許法に規定されており、また、日本の実用新案に相当する制度は米国には存在しないとされている[47]。

３．米国における新たな動き：新設された米国統一商事法典（UCC）第 12 編

（１）米国統一商事法典（UCC）とは

米国統一商事法典（UCC）は、1942 年に米国法律協会（American Law Institute: ALI）と統一州法委員会（Uniform Law Commission: ULC）が、米国各州の民事・商事取引に係るルールの共通化を目的として、共同事業として作成に着手したものである。そ

41 同上。
42 35 U.S.C. § 283.
43 35 U.S.C. § 284.
44 遠藤・前掲注 33)「米国（アメリカ）の知的財産法」3 頁。
45 15 U.S.C. § 1052. 日本貿易振興機構（JETRO)「米国における事業進出マニュアル～知的財産権～」(2014 年 1 月)、5 頁、https://www.jetro.go.jp/ext_images/_Reports/02/2018/200ecc156f4a5a82/5-report_us_ip_201401.pdf （2022 年 11 月 23 日最終閲覧)。
46 15 U.S.C. § 1114 & 15 U.S.C. § 1117.
47 遠藤・前掲注 33)「米国（アメリカ）の知的財産法」2-3 頁。

の後 1951 年に最終草案が作成され、1952 年に最初の UCC が発表された[48]。

UCC は、1987 年以降頻繁に修正が加えられており、そのプロセスは、商法の専門家が作成したドラフト版を ALI/ULC が承認（endorsement）し、各州にその採択を薦めるモデル法案の最終版 UCC として発表される形となっている。UCC の各条項の文言及び解釈については、ALI/ULC のメンバーで構成される編集委員会（Permanent Editorial Board: PEB）が述べた公式コメントが重要視される[49]。

すなわち、UCC は「モデル法文」であって、米国各州がその法文を実際に法律として採択して初めて、法的拘束力のある制定法（各州の州法）となる。米国では、各州の州法を統一するにあたり、連邦法を制定するのではなく、「モデル法文」を作成し、それを各州に採択させる方法が採られているところ、UCC には、実質的に米国の連邦商事法的な地位が付与されている。現在では、米国の各州が、必要に応じて若干補正した上で、UCC を採択している状況である[50]。

なお、UCC は以下の編（Articles）から構成されている[51]。

第 1 編　：総則（General Provisions）[2001]

第 2 編　：売買（Sales）[2002]

第 2 編 A ：リース（Leases）[2002]

第 3 編　：流通証券（Negotiable Instruments）[2002]

第 4 編　：銀行預金および銀行取り立て（Bank Deposits and Collections）[2002]

第 4 編 A ：資金移動（Funds Transfers）[2012]

第 5 編　：信用状（Letters of Credit）[1995]

第 6 編　：詐害的大量売却（Bulk Transfers）[1989]

第 7 編　：倉庫証券・運送証券その他の権原証券
（Warehouse Receipts, Bills of Lading and Other Documents of Title）[2003]

第 8 編　：投資証券（Investment Securities）[1994]

第 9 編　：担保取引（Secured Transactions）[2010]

---

48 日本貿易振興機構（JETRO）「Uniform Commercial Code（米国統一商事法典：米国）」、https://www.jetro.go.jp/world/qa/04A-011046.html（2022 年 11 月 23 日最終閲覧）。

49 同上。

50 同上。

51 Uniform Law Commission, Uniform Commercial Code, https://www.uniformlaws.org/acts/ucc (last visited November 23, 2022).

（２）米国統一商事法典（UCC）第 12 編の内容

2022 年 7 月、ALI と ULC は、UCC の修正案を採択した[52]。今次修正は、UCC に「支配可能な電子記録（controllable electronic records: CER)」という新たな概念を導入する第 12 編を新設しつつ、第 9 編を中心に関連規定の修正も行っている。この新たな第 12 編は、主に仮想通貨、代替不可能なトークン（NFTs)、電子記録によって証される売掛債権や支払無体財産（accounts and payment intangibles）を対象にしたものであり、これまで不明確であった論点、すなわち、デジタル財産の購入者は、第三者の財産的請求権からどの程度解放された形で同財産を取得するのかや、被担保者は、どのようにしてデジタル財産の担保権を完成（perfect）させ、同担保権の優先権を確保し、そして担保権を行使するのかといった論点につき一定のルールを示した内容となっている[53]。一方で、デジタル財産自体が法令上証券又はコモディティのいずれに該当するのかといった論点や、デジタル財産への課税、送金業法やマネーロンダリング法のデジタル財産への適用の論点は取り扱わないものとなっている[54]。ここでは、第 12 編がどのような内容になっているかを概説する。

まず、支配可能な電子記録（CER）の定義である。第 12 編は、支配可能な電子記録（CER）を「支配権（control）に服し得る電子媒体に保存された記録」と定義しつつ[55]、以下のような既存の関連商事法によってカバーされるものについては除外するとしている[56]。

① 支配可能な売掛債権（controllable account）

② 支配可能な支払無体財産（controllable payment intangible）[57]

③ 預金口座（deposit account）

---

52 Uniform Law Commission & American Law Institute, Amendments to the Uniform Commercial Code (2022) (July 13, 2022), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=67fe571b-e8ad-caf8-4530-d8b59bdca805 (last visited November 23, 2022).

53 Juliet M. Moringiello, Edwin E. Smith & Steven O. Weise, The ALI/ULC Project on Emerging Technologies and the UCC: Proposed 2022 Amendments to the UCC (Strafford, September 13, 2022), PP.15-16, https://s3.us-east-1.amazonaws.com/media.straffordpub.com/products/proposed-ucc-amendments-for-cryptocurrencies-nfts-linked-electronic-payment-rights-and-other-digital-assets-2022-09-13/presentation.pdf (last visited November 23, 2022).

54 *Id.*

55 なお、UCC §1-201(b)(31) は、「記録」を「有形媒体に刻まれた情報、または電子媒体やその他の媒体に保存され、知覚可能な形で検索可能な情報」と定義している。

56 UCC §12-102(a)(1).

57 支払無体財産（payment intangible）とは、UCC における一般無形財産（general intangible）であって、その債務者（account debtor）の主たる債務が金銭債務であるものをいう（UCC §9-102(a)(61)）。

④　動産担保証券を証する電子記録（electronic copy of a record evidencing chattel paper）

⑤　権原の電子文書（electronic document of title）

⑥　電子マネー（electronic money）

⑦　投資財産（investment property）

⑧　移転可能記録（transferable record）

したがって、支配権（control）に服さないデジタル財産や、E-SIGN 法や統一電子取引法（UETA）が定める移転可能記録、UCC 第 8 編のオプトインを含む投資財産等のような他の商事法令で既に規定されているデジタル財産は CER の定義からは除外される形となっている[58]。なお、この支配可能な電子記録（CER）の定義において特徴的なのは、「ブロックチェーン」や「分散型台帳」、「公開鍵・秘密鍵」といった用語はあえて使用せず、技術的に中立な用語を使用している点である。これは、今次 UCC の修正が、既知の技術のみならず、将来の技術にも適用されるようにするための意図的なものであるとされている[59]。

その上で、第 12 編は本人の「支配権（control）」についても規定しており、電子記録、電子記録に付随又は論理的に紐付く記録、或いは電子記録が記録されているシステムが以下の全ての要件を満たす場合に、本人は支配可能な電子記録（CER）に対する支配権を有するとしている[60]。

①　本人に対し、電子記録に係る実質的に全ての利益を自ら利用する権限を付与するものであること（この権限自体は排他的である必要はない）

②　本人に対し、他人が電子記録に係る実質的に全ての利益を利用することを妨げることができる排他的権限を付与するものであること

③　本人に対し、他人に支配権を譲渡する排他的権限を付与するものであること

④　上記に列挙した権限を有しているものとして、本人が暗号鍵又はアカウント番号の使用を含むそれ自体を、第三者に対して容易に特定できるようなものであること

つまり、本人が支配可能な電子記録（CER）に対する支配権を得るためには、当該支配可能な電子記録（CER）に係る電子記録、電子記録に付随又は論理的に紐付く記録、

58 Moringiello, Smith & Weise, *supra* note 53, at 19.

59 Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates, Amendments to Uniform Commercial Code Aim To Provide Clarity on the Transfer of Digital Assets (The Distributed Ledger: Blockchain, Digital Assets and Smart Contracts, October 6, 2022), https://www.skadden.com/-/media/files/publications/2022/10/amendments_to_uniform_commercial_code_aim_to_provide_clarity_on_the_transfer_of_digital_assets.pdf (last visited November 23, 2022).

60 UCC §12-105(a).

或いは電子記録が記録されているシステムが、上記全ての要件を満たさなければならないということになる。この点、上記②及び③の「排他的（exclusive）」の定義についても規定があり、以下いずれかの場合であっても権限が排他的となる[61]。

- 支配可能な電子記録（CER）、支配可能な電子記録に付随又は論理的に紐付けられた記録、或いは電子記録が記録されているシステムが、支配可能な電子記録（CER）の用途を制限しているか、若しくは、支配権の移転又は喪失、或いは電子記録によって付与される利益の修正を含む変更を引き起こすようにプログラムされたプロトコルを有している場合
- 本人が、当該権限を他人と共有することに同意している場合

なお、③「他人に支配権を譲渡する排他的権限を付与するものであること」という要件については、いわゆる「マルチシグネチャーウォレット」（取引に係る署名に複数の秘密鍵を必要とする技術を用いたウォレット）の使用により譲渡する権限が発生する場合や、支配可能な電子記録（CER）を記録するシステムに組み込まれたプロトコルの一部として自動的に変更が行われる場合も満たされるとされている[62]。

以上のように、第 12 編は、支配可能な電子記録（CER）という新たな概念を導入しつつ、それに対する本人の支配権について規定している訳であるが、こうした支配可能な電子記録（CER）を本人から譲り受けた場合についても規定している。すなわち、支配可能な電子記録（CER）の買主（purchaser）は、売主（transferor）が有していた（又は譲渡する権限を有していた）当該支配可能な電子記録（CER）に関する全ての権利を取得し、他方、当該支配可能な電子記録（CER）の全てではなく一部のみ買い取った者については、その範囲内でのみ権利を取得するとしている[63]。その上で、「適格買主（qualifying purchaser）」についても定義を置いており、支配可能な電子記録（CER）の全部又は一部の買主であって、当該支配可能な電子記録（CER）に対する他の財産権的主張の通知を受けず（without notice）、善意で（in good faith）、かつ価値あるものとして（for value）当該支配可能な電子記録（CER）の支配権を取得した者は、適格買主と

---

61 UCC §12-105(b). なお、UCC §12-105 は、「排他的」の定義との関係で、支配権を他人と共有しておらずその権限が排他的とは言えない場合や、権限の排他性が推定される場合、他人を通じた支配権の確立や他人に代わって支配権を有しているという認識（acknowledgement）の要否等についても規定を置いている。

62 Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates, *supra* note 59.

63 UCC §12-104(d).

して保護される[64]。よって、例えばある支配可能な電子記録（CER）について権利を有すると主張する、競合する第三者が現れたとしても、適格買主の要件を満たせば、そうした競合する第三者の請求権に服さない形で、当該支配可能な電子記録（CER）に関する支払いや履行その他の財産的権利を取得することになる。このことは、例えば、盗難されたNFTを善意で取得した買主は、当該NFTを盗難された者による如何なる請求権にも服さない形で、当該 NFT を取得することになり、適格買主は手厚く保護されることがここから読み取ることができる[65]。

この他、第 12 編において興味深い規定としては、支配可能な売掛債権（controllable account）又は支払無体財産（payment intangible）に係る債務者（account debtor）の弁済についても規定を置いている点である。すなわち、支配可能な売掛債権又は支払無体財産に係る債務者は、原則として以下いずれかの者に支払うことで、弁済を行うことができるとしている[66]。

① 支配可能な売掛債権又は支払無体財産を証する支配可能な電子記録（CER）の支配権を有する者

② 過去に支配可能な電子記録（CER）の支配権を有していた者であって、当該債務者が以下全ての要件を満たす通知（notice）を受けていなかった場合[67]：

（ⅰ）過去に支配権を有していた者又は支配権を譲り受けた者によって署名されていること

（ⅱ）支配可能な売掛債権又は支払無体財産を合理的に特定していること

（ⅲ）支配可能な売掛債権又は支払無体財産を証する支配可能な電子記録（CER）の支配権が譲渡されたことを、当該債務者に通知するものであること

（ⅳ）名前、識別番号、暗号鍵、事業所、アカウント番号等、合理的な方法で譲受人を特定していること

（ⅴ）債務者が譲受人に支払うべき商業的に合理的な方法を提供していること

つまり、支配可能な売掛債権や支払無体財産に対する支払債務を有する者は、当該支配可能な売掛債権や支払無体財産を証する支配可能な電子記録（CER）の支配権を有する者、又は過去にそうした支配権を有していた者に支払いを行うことでその債務を消滅さ

64 UCC §12-102(a)(2) & §12-104(e).
65 Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates, *supra* note 59.
66 UCC §12-106(a).
67 UCC §12-106(b). なお、UCC §12-106(d) は、通知が無効となる場合について規定している。

せることができるが、後者の場合については、あくまでも相手方が現に支配可能な電子記録（CER）の支配権を有していないことにつき通知を受けていない、すなわち善意である必要がある。したがって、もし上記のような通知を受けていたにもかかわらず、現に支配可能な電子記録（CER）の支配権を有しない者に支払いを行ったとしても、債務を履行したことにはならず、弁済は無効となってしまうため、注意が必要である。

この他、第 12 編は、準拠法に関する規定も置いており、原則として支配可能な電子記録（CER）等が所在する法廷地法が適用されるものの、支配可能な電子記録（CER）等において指定することも可能であるとしている[68]。仮に準拠法が指定されていない場合は、コロンビア特別区（Washington, D.C.）の法律がデフォルトで適用されることとなるが、今後コロンビア特別区が UCC 第 12 編の内容に変更を施して法律を制定した場合には、当該変更後の法律がそのまま準拠法とはならず、あくまでも UCC 第 12 編の内容通りに適用されることになるとされている[69]。

（３）UCC 第 9 編（担保付取引（Secured Transactions））における関連の修正

以上が支配可能な電子記録（CER）に関する UCC 第 12 編の内容であるが、関連する修正が担保付取引に関する UCC 第 9 編にも施されており、支配可能な電子記録（CER）、支配可能な売掛債権及び支払無体財産に係る担保権の対抗要件（perfection）と優先順位を明確化する内容となっている。まず、同修正では、支配可能な電子記録（CER）や売掛債権及び支払無体財産は、それぞれ一般無体財産（general intangible）、売掛債権（accounts）、そして支払無体財産（payment intangible）という、既存の担保財産のカテゴリーに該当するとされ、よって担保契約（security agreement）や与信公示書（financing statement）における既存の担保財産の記載を変更する必要はないとされている[70]。その上で、支配可能な電子記録（CER）については、上記の通り一般無体財産であるとして、通常の担保権設定ルール（担保権が有効に成立する（attach）ための要件は、①担保権者が、合意に従い、担保財産の占有を取得するか或いは債務者が担保財産を記述した担保証書（security agreement）に署名すること、②対価（value）が債務者に付与

---

68 UCC §12-107.

69 *Id.*

70 Sandra Feldman, The Uniform Commercial Code (UCC) is amended to address emerging technologies (Walters Kluwer, September 9, 2022), https://www.wolterskluwer.com/en/expert-insights/uniform-commercial-code-ucc-amended-to-address-emerging-technologies (last visited November 23, 2022).

されること、そして③債務者が担保財産について権利を取得することである[71]）が適用されるとしている[72]。

もっとも、注意を要する点としては、支配可能な電子記録（CER）や売掛債権又は支払無体財産に対する担保権は、与信公示書の登録（filing）のみならず、UCC 第 12 編が定義する支配権によって対抗要件を具備させることが可能であるとしており[73]、当該支配権によって対抗要件が具備された支配可能な電子記録（CER）や同売掛債権又は支払無体財産の担保権は、与信公示書の登録によってのみ対抗要件が具備された担保権よりも優先するとされていることである[74]。つまり、担保権が対抗力を有し他の債権者に優先権を主張し得るようになるためには、上記の担保権設定ルールを満たすとともに、担保財産の占有を取得するか又は与信公示書を登録し、公示の要件を満たす必要があるところ[75]、公示の要件を満たす与信公示書の登録後に支配権が得られた場合であっても、支配権が与信公示書の登録に優先することになる。このように、支配可能な電子記録（CER）や同売掛債権又は支払無体財産の担保権については、その支配権に強い効力が認められているため、これが実務上どのような影響を及ぼすことになるのか引き続き注視していく必要がある。

なお、今次 UCC の修正により、電子マネー（electronic money）という概念も新設され、当該電子マネーの担保権についても支配権によって対抗要件を具備させることができるとされている（もっとも、電子マネーが預金口座に入金されている場合は、通常の預金口座に関するルールが適用されることになる）[76]。

（４）今次 UCC の修正に関する今後

以上が UCC 第 12 編及び第 9 編における関連の修正の内容である。前述の通り、UCC はあくまでも「モデル法文」であって、米国各州がその法文を実際に法律として採択して初めて、法的拘束力のある制定法（各州の州法）となるため、支配可能な電子記録

---

71 沖野眞已「約定担保物権の意義と機能―UCC 第 9 編の「効率性」に関する議論の素描―」（学習院大学法学会雑誌、1998 年 9 月 20 日）78 頁。
72 Feldman, *supra* note 70.
73 UCC §9-314.
74 Feldman, *supra* note 70.
75 沖野・前掲注 71）「約定担保物権の意義と機能―UCC 第 9 編の「効率性」に関する議論の素描―」80 頁。
76 Feldman, *supra* note 70. 但し、支配権の対象とならないマネーは除外され、例えば政府の中央銀行が発行する暗号資産は含まれ得る。

（CER）という新たな概念の導入や関連するルールが各州でどのように制定されまた運用されていくのかについては、今後の推移を見守っていく必要がある。2022 年 8 月時点では、アイオワ州、インディアナ州、ネブラスカ州、ニューハンプシャー州が早くも採択したようであるが、本修正の影響はまだ限定的であり、ケースバイケースで判断していく必要があろう[77]。いずれにしても、今次 UCC の修正においては、施行日とは別途「調整日（adjustment date）」）に関する規定を置いており、支配可能な電子記録（CER）に係る既存の権利者が新たなルールを遵守できるよう十分な時間的余裕を与えるため、施行日前に確立された優先順位を無効にする可能性のあるような、今次 UCC の修正に含まれる特定の優先順位ルールは、調整日まで施行されない予定となっている[78]。そうしたことからも、米国内でこの新たなルールがどのように広がっていくのか、また米国外向けてどのような影響を及ぼしていくことになるのか、今後注目に値するであろう。

４．おわりに

2021 年 2 月に設置された法務省法制審議会担保法制部会は、2021 年 4 月以降、担保法制の見直しに関する広範な議論を継続しているが、その論点の一つとして、「動産を目的とする新たな規定に係る担保権の対抗要件等の在り方」が含まれている[79]。この点、物権変動は意思表示のみによってその効力を生じるところ（民法第 176 条）、物権変動において権利を取得した者が、その権利を第三者に対して主張するためには対抗要件が必要となっている[80]。その上で、動産の物権変動の対抗要件は、当該動産の引渡し（占有の移転）とされており（民法第 178 条）、この引渡しには、①現実の引渡し（同法第 182 条 1 項）、②簡易の引渡し（同条 2 項）、③占有改定（同法第 183 条）、④指図による占有移転（同法第 184 条）が含まれる（これ以外にも、法人が動産を譲渡する場合には「動産譲渡登記」も存在する）[81]。もっとも、観念的な方法である占有改定による引渡しは、設定者

---

77 Practical Law Finance, States Begin to Adopt UCC Article 12 Covering Digital Assets (Thomson Reuters, August 1, 2022), https://ca.practicallaw.thomsonreuters.com/w-036-4779?transitionType=Default&contextData=(sc.Default)&firstPage=true (last visited November 23, 2022).

78 UCC §A-305 & §A-306.

79 法務省法制審議会担保法制部会は、2021 年 4 月以降、本稿執筆時点までに、合計で 28 回会合が開催されてきている（直近の会合は、2022 年 11 月 8 日に開催された第 28 回会議）。これまでの累次の会合に係る資料や議事録等については、法務省法制審議会担保法制部会のページ（https://www.moj.go.jp/shingi1/housei02_003008.html）に掲載。

80 安永正昭『講義　物権・担保物権法〔第 4 版〕』（有斐閣、2022 年 9 月 30 日）27-39 頁。

81 安永・前掲注 80)『講義　物権・担保物権法〔第 4 版〕』105-111 頁。

が引き続き目的物の占有を継続することから、第三者から見ると占有改定の存在の有無及びそれがなされた時期が判然としないため、（たとえ占有の外観を信頼して取引した者を保護する即時取得制度を設けているとしても）担保権の公示として不十分ではないかとの問題が指摘されており[82]、当該問題も踏まえて、個別動産又は集合動産を目的とする新たな規定に係る担保権の対抗要件等のあり方が、法務省法制審議会担保法制部会で引き続き検討されている状況である。

ところで、現行民法上、動産とは不動産以外の全ての物とされており（民法第 86 条）、また、物とは有体物をいうとされている（同法第 85 条）。所有権は所有物について生じる権利であり、同じく「有体物」であることが必要となっている（同法第 206 条）。つまり、前述したように、無体物であって有体物ではないデータは、現行民法上の物ではなく、よって動産の範疇にも入らず、故に動産の物権変動に関するルールには服さないこととなる。この点については、法務省法制審議会担保法制部会の過去の資料を見る限り、UCC 第 12 編のような議論がなされているようには見受けられない。

もとより、こうした状況の中で、UCC 第 12 編のような法制度を我が国民法においても性急に導入すべきなのか、或いは導入できるのかといった論点は多岐にわたる。とはいえ、集合物を含む動産や債権の担保取引を包括的に規定した UCC 第 9 編（担保付取引）がある中で、今次修正によって支配可能な電子記録（CER）に関する第 12 編も新設し、新たなテクノロジーやビジネスモデルを踏まえたデータに関するルールメイキングを米国が進めていることについては、冒頭で述べたように、我が国におけるデータに関するルールメイキングを進めていく上でも注目に値するであろう。デジタル庁及び内閣府知的財産戦略推進事務局の「プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0」で述べられているような、継続的な環境分析とルールの更新がここでも応用されることを期待する[83]。

82 日本銀行信用機構室・前掲注 7)「米国の動産担保法制について」9 頁。
83 デジタル庁・内閣府知的財産戦略推進事務局「プラットフォームにおけるデータ取扱いルールの実装ガイダンス　ver1.0」（2022 年 3 月 4 日）40-41 頁。

第９章　EU データ法構想とデータ活用法制

一橋大学大学院法学研究科教授

生貝　直人

１．はじめに

EU（欧州連合）では現在、ウルズラ・フォン・デア・ライエン欧州委員会の発足後間も無い、2020 年 2 月に公表された欧州データ戦略[1]に基づき、データ法（Data Act）やデータガバナンス法（Data Governance Act）をはじめとする大規模なデータ関連法制枠組の立法作業が進められている。我が国では、社会・経済活動の中核的資源と目されている各種データの活用を進めるにあたり、法制面では主として個人情報保護法や知的財産法といったデータの保護に関わる法制度の改正を中心とした措置を進めてきた。他方で、本稿で主題とする EU で形成されつつあるデータ関連法制枠組は、データの活用そのものに焦点を当てた、「データ活用法制」と称すべき立法のアプローチである。本稿では、EU のデータ活用法制に向けた立法の動きについて概観した上で、我が国の今後のデータ関連法制のあり方についての示唆を論じる。

２．データ法案

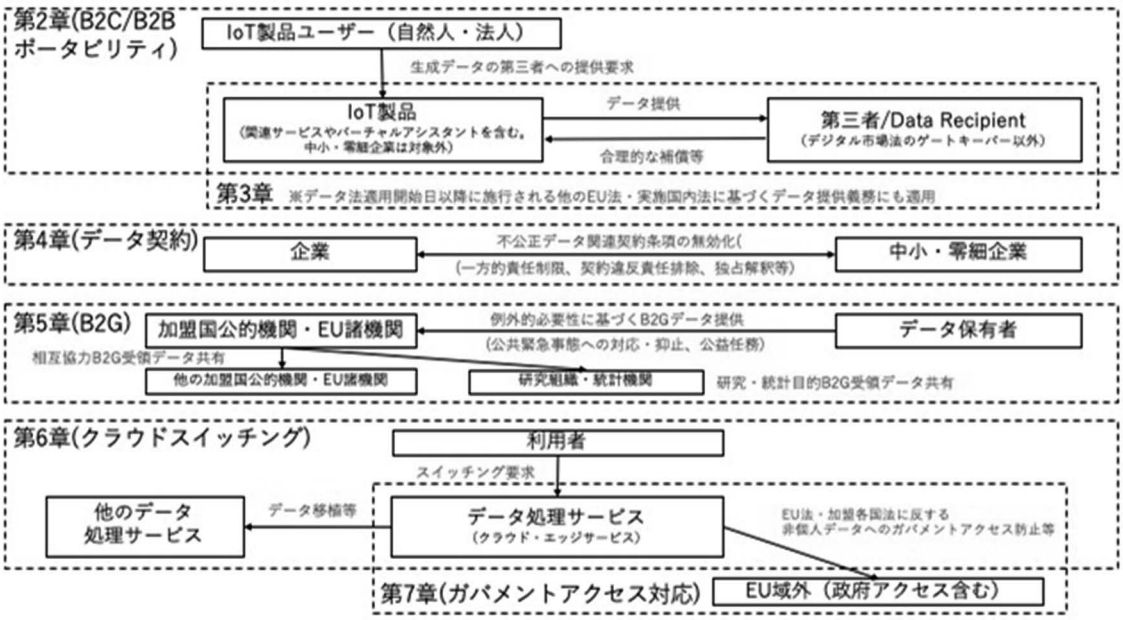
2022 年 2 月に欧州委員会から提案されたデータ法案[2]は、特に B2C（Business to Consumer）、B2B（Business to Business）、B2G（Business to Government）それぞれの関係性におけるデータアクセスの法的・経済的・技術的障壁に対処し、個人データ・非個人データ双方のデータ活用を促進するための様々な措置を規定している。同法案は全 11 章からなり、第 1 章には適用範囲や定義に関する規定が置かれ、第 8 章から第 11 章には監督機関や施行に関する規定が置かれる。以下では、データ活用に関わる主な事項を定めた第 2 章から第 7 章の規定を 4 つのパートに分けて概観する（図表-1 参照）。

---

1 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, A European strategy for data, COM/2020/66 final.

2 Proposal for a Regulation of European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) (Text with EEA relevance), COM(2022) 68 final.

図表-1：データ法案第 2 章～第 7 章の概要



（1）IoT デバイス生成データのポータビリティ

第 2 章「企業と消費者、企業と企業のデータ共有」では、IoT 家電やコネクテッドカー、インターネット接続された産業機械等を含む IoT デバイス（関連サービスやデバイスを操作するバーチャルアシスタントを含む）から生成されたデータについて、そのデバイスの利用者（自然人・法人を問わない）自身によるアクセスと活用を可能とするための措置を規定する。IoT デバイスの設計者・製造者は、自らの IoT デバイスの利用により生成されたデータに対して容易にアクセスできるようにデバイスを設計しなければならず、その利用者が指定した第三者に対してもデータの提供を行わなければならない。当該第三者には、例えばコネクテッドカーにテレマティクス保険を提供する事業者や、修理事業者等のアフターマーケットサービスが念頭に置かれる[3]。同規定は、GDPR 第 20 条で規定される自然人のデータポータビリティ権の対象を IoT デバイスの文脈に特化した形で強化し、またその行使可能な主体を法人にまで拡大するものとして位置付けられる。さらに第 3 章では、現在検討が進む各種の分野ごとのデータ関連法制にも適用される、データ提供方法についての共通規定が置かれ、データを提供する事業者と利用者の求めに応じてデータを受け取る第三者の間での補償のあり方などが規定されている。

[3] 後述するデジタル市場法において指定される巨大なデジタルプラットフォーム（ゲートキーパー）は、同規定に基づきデータを受け取ることができる第三者からは除外される。

（２）データ契約規制

第 4 章では、特に大企業と中小・零細企業の間で結ばれるデータ関連契約についての契約規制が規定されている。データは知的財産法制で保護される領域は少なく、その保護や利用については、データの生成に関与する複数の事業者の間や、データ提供者と受領者の間で結ばれる契約上の関係性が重要な役割を果たす。本章では、特に大企業と中小・零細企業の間でのデータ契約に関する交渉力の不均衡に着目して、一方的な責任制限や契約違反責任排除、独占解釈等の不公正契約条項を無効とする規定を置いている。

（３）B2G データ共有

第 5 章では、民間企業等が保有するデータを、公的機関が公益目的のために利用可能とする B2G データ共有に関する規定が置かれている。民間企業が保有するデータは、パンデミックや大規模災害への政策的対応、あるいは EBPM（Evidence Based Policy Making）の実現のために重要な役割を果たす。本章はそのような公益目的でのデータ活用を可能とする、企業から政府へのデータ提供について EU 共通のルールを創設するものである。B2G データ共有に対する企業側への対価は 2 つの類型に分けられており、「公共の緊急事態への対応」に必要なデータの提供は無償とされ、それ以外の場合（法律で規定された公益の実現に必要であり、代替手段によるデータ入手が困難な場合等）には一定の合理的な補償が行われる。同規定に基づきデータを取得した公的機関には、当初データアクセスを行った目的以外での利用の禁止等の規律が課されるが、目的に適合する科学研究や分析を実施する場合には、学術研究機関等への再提供を行うこともできる。

（４）クラウドサービス

第 6 章では、クラウドサービスやエッジサービスを含むデータ処理サービスの利用者によるスイッチングを促すための規定が置かれている。現在データの多くはクラウドサービス上において処理されているが、それが単一のサービスにロックインされる状況が生じると、データの自由な流通を阻害することになる。本章では、2018 年の EU 域内自由流通枠組規則[4]において自主規制の促進に留められたデータ処理サービス間のデータポータビリティに関する規定を強化し、データ処理サービス提供事業者に対し、利用者のスイッチン

[4] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.), OJ L 303, 28.11.2018, p. 59–68.

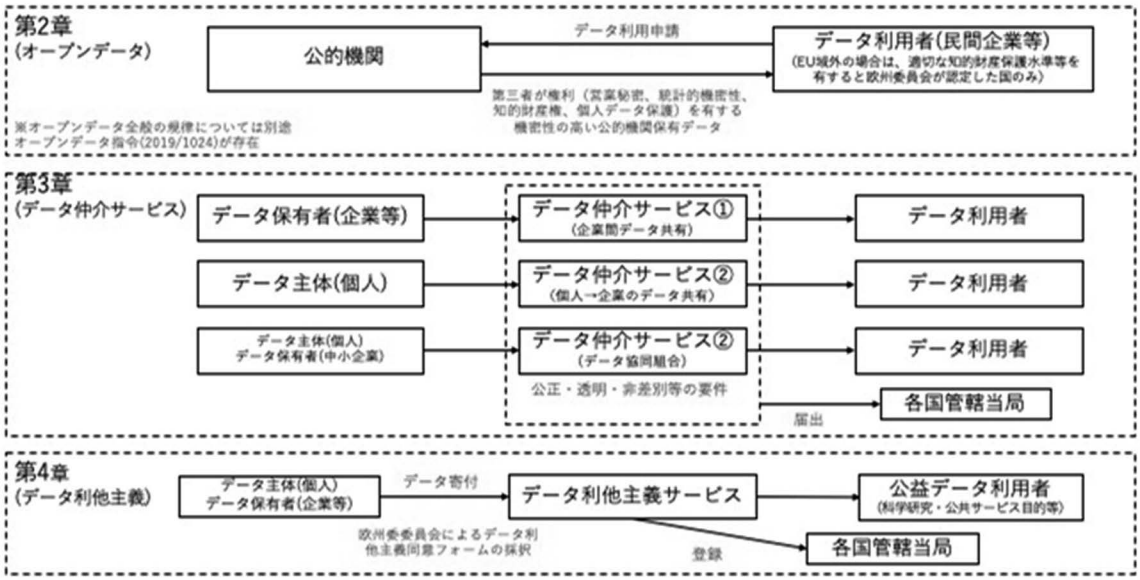
グ要求に対応する法的義務を課す。

さらに第 7 章では、それらデータ処理サービス上に保存されたデータに対する、EU 域外の政府によるガバメントアクセス防止義務を規定する。データ処理サービスの提供者は、EU 法や加盟国法に反する非個人データへのガバメントアクセスを防ぐため、契約上の取り決めを含むあらゆる妥当な技術的、法的及び組織的措置を講じなければならない[5]。

３．データガバナンス法

データ法案と対をなすデータガバナンス法は、2020 年 11 月に欧州委員会により提案され、2022 年 5 月に制定、適用開始は 2023 年 9 月が予定される。データガバナンス法は全 9 章からなり、データ活用に関わる主な規定を定める第 2 章から第 4 章の内容は以下の通りである（図表-2 参照）。

図表-2：データガバナンス法第 2 章～第 4 章の概要



（１）オープンデータ

第 2 章「公的部門が保有する特定カテゴリの保護対象データの再利用」では、公的機関が保有するデータの民間企業等への提供、すなわちオープンデータに関する規定が置かれている。EU では従来から公的機関が保有するデータのオープンデータ化に関する法制度

[5] 個人データに関しては GDPR 第 48 条によりデータ管理者一般に同様の義務が課されており、本規定は GDPR の規定をデータ処理サービスに関して非個人データに拡張するものと位置付けられる。

が存在しており、2019 年 6 月には既存の指令を改正する形でオープンデータ指令[6]が制定されているが、第三者の営業秘密や統計的機密性、知的財産権、個人データ保護などの対象となるデータは対象外とされていた。本章は、オープンデータ指令を補完し、それら特定カテゴリのデータを再利用可能とするための特別な枠組を設ける。

（２）データ仲介サービス

第 3 章「データ仲介サービス（data intermediation services）に適用される要件」では、様々な主体のデータ共有を仲介するサービスについて、(a)データ保有者によるデータ利用者へのデータ提供支援サービス（特に企業間のデータ共有を念頭に置いた、二者間・多者間のデータ交換や共同利用を支援するサービスであり、データ保有者と利用者を繋ぐインフラ提供等を含む）、(b)自らの個人データ等を提供する個人とデータ利用者を仲介するサービス（GDPR の権利行使支援を含む）、(c)複数の個人や中小企業等が共同でデータ提供条件等の交渉を行うデータ協同組合（data cooperatives）に関わるサービスの 3 つのカテゴリを設け、それらを提供する主体の監督当局への届出義務と、他サービスからの構造分離や価格・サービス条件の公正・透明・非差別性等の義務を課す。また、データ法案第 7 章におけるクラウドサービス事業者に対する義務と同様に、EU 域外政府からのガバメントアクセス等を防止する措置を採ることも求められる。

（３）データ利他主義サービス

第 4 章「データ利他主義（data altruism）」は、データの自発的寄付に基づく公益利用を促進するサービスを提供する主体に対する監督当局への登録枠組を設け、登録を受けた事業者は「EU 公認データ利他主義組織」のラベルとロゴを使用することができる。公認事業者は非営利組織でなければならず、その事業の実施にあたっての記録作成や年次報告書の作成義務等が課される。また、欧州委員会による「データ利他主義同意フォーム」の採択についても規定される。

４．分野別の立法

前述のデータ法案とデータガバナンス法は、欧州委員会が欧州データ戦略において提示

[6] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), OJ L 172, 26.6.2019, p. 56–83.

した欧州共通データスペース（European Common Data Space）構想の制度的な共通基盤として位置付けられており、これら 2 法を土台として、分野の特性に応じたデータ活用法制の検討が進められている。

（１）欧州ヘルスデータスペース法案

2022 年 5 月に欧州委員会が提案した欧州ヘルスデータスペース法案[7]は、健康・医療分野のデータ活用を促進するため、患者に医療やケアサービスを提供するための一次利用（primary use）、医学研究や政策形成、医薬品・医療機器等の開発のための二次利用（secondary use）に分けたデータ活用の法的枠組と、そのための基盤となるデータ共有インフラのあり方を規定している。

一次利用については、患者本人のデータポータビリティを強化する形で、自らの診療情報や処方箋記録、検査結果などのヘルスデータを、医療機関等から再利用しやすいデジタル形式で受け取ることを可能とすると共に、本人の意思に基づき、他の医療従事者への提供とそれに基づく医療・ケアサービスを受けることを可能とする。加盟国は、それらヘルスデータの共有を可能とするデータインフラである MyHealth@EU への参加が義務付けられる。二次利用については、ヘルスデータを科学研究や医薬品・医療機器開発等のイノベーション、公衆衛生、政策立案等に利用可能とするため、加盟国ごとにヘルスデータアクセス機関を設立し、その許可に基づくヘルスデータの二次利用を可能とする。それらのデータは、加盟国が参加する分散型二次利用インフラである HealthData@EU インフラを通じて共有される。

（２）自動車データ

現時点では具体的な法案は公表されていないが、2022 年の 3 月から 8 月にかけて、自動車、特にコネクテッドカーのデータ及び機能・リソースへのアクセスに関わる立法構想の意見募集が行われている[8]。コネクテッドカーから生成されたデータは前述したデータ法案第 2 章の対象となり、製造者・設計者は利用者へのデータアクセス提供と第三者データ共有義務が課されるが、本構想では、データ法案のデータアクセス義務を、自動車分野に特化した形で強化・具体化する方針が示されている。具体的には以下の 3 つの選択肢が意

[7] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space (Text with EEA relevance), COM(2022) 197 final.

[8] Call for evidence for an impact assessment - Ares(2022)2302201, Access to vehicle data, functions and resources.

見募集の対象となっている。

第一の選択肢は、データ法で付与される利用者のデータアクセス権に加え、機能（例：シェアードモビリティサービスにおける車両ドアの遠隔解錠）やリソース（例：ナビゲーションサービスにおける車両ダッシュボード上の制限速度情報の表示や、電気自動車関連サービスにおけるバッテリー充電／放電）へのアクセスを可能とすることである。

第二の選択肢は、上記第一の選択肢に加え、市場投入のための型式承認時に、データ、機能、リソースへの遠隔・特定フォーマットでのアクセスが可能であることを証明することを義務付けることである。これには、車載診断ポートへの継続的かつ安全なアクセス確保も含まれる。

第三の選択肢は、上記第一・第二の選択肢に加え、データ・機能・リソースへのアクセス方法や条件についても特別の規定を置くことである。

（３）デジタルプラットフォーム

欧州データ戦略及び欧州共通データスペース構想に直接含まれるものではないが、並行して EU が活発な立法作業を進めるデジタルプラットフォーム規制の中においても、データ活用促進と関わりの深い事項が含まれている。

2020 年 12 月に欧州委員会が提案し、2022 年 9 月に制定されたデジタル市場法[9]は、EU 域内の月間アクティブユーザー数 4,500 万人以上等の要件を満たす特に巨大なコアプラットフォームサービス（CPS）を提供するデジタルプラットフォームを「ゲートキーパー」として指定し、競争政策的観点からの各種義務を課す立法である。CPS には、オンライン媒介サービス、検索エンジン、SNS、ビデオ共有サービス、メッセンジャー、オペレーティングシステム、クラウドコンピューティングサービス、及びそれらの CPS 提供事業者が提供する広告サービスが含まれる。

第 5 条から第 7 条に規定されるゲートキーパーに課される義務は、サービス上での自己優遇の禁止や、決済手段拘束の禁止、オペレーティングシステム上でのアプリストアの開放、サービスやデバイスの相互運用性確保など多岐に渡る。その中でも、特に第 6 条第 9 項では、CPS の利用に関連してエンドユーザー（CPS を利用する自然人又は法人）が提供した、又はそこでの活動により生成されたデータの効果的なポータビリティを、エンドユー

[9] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), OJ L 265, 12.10.2022, p. 1–66.

ザーが指定した第三者への転送を含めて無償で提供することが義務付けられる。また、同条第 10 項では、ゲートキーパーに対して、CPS のビジネスユーザー（CPS 上でエンドユーザーに商品やサービスを提供する自然人又は法人）に対しても、その CPS の利用に関連して提供・生成されたデータについて同様のポータビリティを確保する義務が課される。これらの規定は直接的にはサービス間でのスイッチングの円滑化による競争促進を目的としたものだが、データ法案第 2 章の IoT データ規定と類似した形で、デジタルプラットフォームに集約されたデータの本人や第三者による更なる活用を促す可能性がある。さらに同条第 11 項では、オンライン検索エンジンを提供する第三者事業者の要求に応じて、ゲートキーパーが提供するオンライン検索エンジンでエンドユーザーが行った検索に関するランキング、クエリー、クリック及び閲覧データへのアクセスを、匿名化した上で、公正、合理的かつ非差別的な条件で提供する義務も規定される。

５．データ活用法制のあり方

最後に、本稿で概観してきた EU のデータ活用法制から、我が国はいかなる示唆を得ることができるかについての私見を述べる。

第一に、冒頭で触れた通り、我が国ではこれまで、データの活用を促進するにあたり、個人情報保護法の改正に基づく匿名加工情報・仮名加工情報制度の導入や、不正競争防止法の改正に基づく限定提供データの導入など、データの保護に関わる法制度の見直しというアプローチに力点を置いてきたと言える。ある意味ではそれらデータ保護法制と対極をなす、B2B、B2C、B2G 等の関係性におけるデータアクセスの法的強化を中心とした、データの「活用」に直接の焦点を当てる EU の立法を参考に、我が国としても本格的なデータ活用法制の検討を行う意義はあるはずである。他方でそれは、データ保護法制の弱体化を意味するものと考えるべきではない。原理的に、より多くのデータを、より多様な主体が活用可能となることは、データの悪用や誤用のリスクの増大と不可分である。デジタルプラットフォームなどの巨大企業に集積された大量の個人データを本人の意志に基づき中小の新規参入企業に移転可能とする上では、移転先企業の信頼性確保が必要となるであろうし、大規模な B2G データ共有を可能とする立法は、政府自身によるデータ保護体制に対する社会からの十分な信頼がなければ実現し得ないだろう。EU の本格的なデータ活用法制の整備には、GDPR をはじめとする強固なデータ保護法制の存在が前提にあると考えるべきである。我が国においても、個人データ・非個人データを問わず、データの保護と活

用を表裏一体とした立法を念頭に置くべきである。

第二に、EU データ活用法制の各種規定は、我が国においても、例えばデータ法案第 3 章のデータ契約規制については経済産業省の「AI・データ契約ガイドライン」として、データガバナンス法案第 3 章のデータ仲介サービスについては総務省・経済産業省と一般社団法人日本 IT 団体連盟の協業による情報銀行認定制度として、それぞれ関係性の深いソフトローの施策が進められてきたところである。EU においても、データ法案などのハードローの策定は短期の間に行われたわけではなく、データ法案の原型となる 2017 年の「欧州データ経済の構築[10]」政策文書での B2B・B2G データ共有政策オプションの提示、それらをソフトローとして具体化した 2018 年の「共通欧州データスペースに向けて[11]」政策文書などの数年来に渡る検討とステイクホルダーとの協議を経て、今般のハードローの制定作業に至っている。さらに、関連法制の多くは、データポータビリティの強化・拡張を含め、GDPR の実質的な見直しを伴うものでもある。環境変化の激しいデータ分野において、ハードローの立法を行うべきか否か、行うとしてもいつ行うべきかの見極めは困難であるが、データに関して何らかの新たなルールが必要なのであれば、ソフトローは本来、過渡的なプロセスとしての位置付けを有するはずである。ハードローとしての立法の選択肢を常に視野に入れた検討を継続的に行うと共に、立法の後も、その不断・機敏（アジャイル）な見直しを前提とした政策検討を行うことが必要である。

第三に、その賛否につきいずれの立場を採るにせよ、本稿で触れた EU のデータ活用法制の多くは、EU 域内に向けたサービスの提供や、EU 域内に IoT 製品等を販売する我が国の企業にも直接適用される可能性があることに加え、GDPR やその前身である 1995 年データ保護指令が我が国を含む世界各国における個人データ保護法制の参照軸とされてきたように、EU 域外の各国においても同様の立法が進められる可能性は高い。特に近年の EU データ活用法制は、デジタルプラットフォーム等が扱うデジタルデータに主眼を置いていた GDPR と異なり、サイバー・フィジカル融合の進展に伴い本格的に拡大する、IoT デバイスから生成されるリアルデータの国際的ルール形成に、EU が本格的にイニシアティブを取ろうとする動きと見ることができる。データ法案第 2 章や自動車データの立法

[10] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS "BUILDING A EUROPEAN DATA ECONOMY", COM/2017/09 final.

[11] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS "Towards a common European data space", COM/2018/232 final.

構想は、データを生成するデバイスを製造・提供する事業者と、データを活用する関連サービスを提供する事業者の間での、いまだ国際的な共通理解が存在しないデータの利用権に関するルール形成、いわば「データは誰のものか」という問いを巡る現在進行形のポリティクスという側面を有する。その結論は、リアルデータの活用に活路を見出そうとする我が国の産業界の国際競争力にも影響を与えうる。EU のルール形成に対して、我が国の官民それぞれが、どのような関与を行うべきかを検討していく必要性は高いはずである。

データに関する権利のあり方

21 世紀政策研究所　研究プロジェクト
（研究主幹：宍戸　常寿）

2023 年 3 月
一般社団法人 日本経済団体連合会　21 世紀政策研究所

〒100-8188　東京都千代田区大手町 1-3-2
TEL：03-6741-0901
FAX：03-6741-0902

ホームページ：http://www.21ppi.org/

21世紀政策研究所
The 21st Century Public Policy Institute