AI が進化する時代の法と権利について

角元那菜

目次

1　はじめに

1.1　問題の所在

ディープラーニング技術の発展に伴って、AI は今まで以上に様々な局面で使用されることが目指されている。しかし、AI の発展とそれに従って変化する社会は人類にとって未だ経験したことのないものであり、現段階では法制度も整っているとは言い難い。本レポートでは、今後さらなる発展が見込まれる AI がどのような権利を侵害するリスクがあり、そのリスクに対してどのような法ルールを課すべきなのかについて、日本と世界の現状や展望も踏まえながら検討していく。

1.2　本レポートの構成

本レポートは以下のように構成される。

まず AI の定義と分類などについて述べることで AI に対する基本的な理解を深める。次に、プライバシー権について、伝統的プライバシー権から現代的プライバシー権で発展してきた経緯や、日本の最高裁判所におけるプライバシー権について扱う。次いで、プロファイリングについて、それにまつわる法律問題も踏まえながら論じる。そして 5 では、その先進的な対応で注目を集めている EU の一般データ保護規制（GDPR）について取り上げ、その上で今後の展望について検討していくこととする。

2　AI について

2.1　AI の定義

AI の厳密な定義については専門家たちの間でも未だに定まっていない。実際に総務省が発表した平成 28 年度版情報通信白書において、その作成に参加した専門家 13 名は全員異なる定義を提唱している。例えば、栗原聡は AI とは「人工的につくられる知能であるが、その知能のレベルは人を超えているものを想像している」と定義し、札幌市立大学で学長も務める中島秀之教授は「人工的につくられた、知能を持つ実態。あるいはそれを作ろうとすることによって知能全体を研究する分野」であるとしている。また、少し異なる角度から京都大学の長尾真教授は「人間の頭脳活動を極限までシミュレートするシステムである」と定義している[*1]。ある程度共通した定義をひとつあげるとするならば、ISO/IEC 2382:2015 に定める国際規格である「推論、学習、自己改善など、通常、人間的な知能に関する機能を遂行するデーター処理システム」ないし「人間の知性と結びつけて考えられる、推論、学習などの機能を遂行するモデル及びシステム」がある。定義が定まらない大きな理由としては、そもそも「知性」や「知能」を定義することが難しいことがあげられる。松尾豊氏は「知能」についてもあえて定義を述べるとすると「入力に応じて適切な出力をする（行動をする）」ものとする定義が「知能」を外部から観測した時の定義としては有力であると評価しており、AI を入力と出力の関係から考えることを推奨している[*2]。

[*1] 福田雅樹ほか　『AI がつなげる社会　AI ネットワーク時代の法・政策』（弘文堂、2017 年）6 頁

[*2] 福田雅樹ほか・前掲註 1）7 項

2.2　AI の分類

一様に AI と言っても、つくられた目的やそれが持つ機能によって実に様々な種類の AI が存在する。哲学者のジョン・サールは AI を分類する一つの指標として「強い AI」と「弱い AI」を提唱した。「強い AI」とは人間のように自意識を持ち、全認知能力を必要とする作業も可能な AI のことを指す。これはつまり、人間によって指示されたりあらかじめプログラミングされたりしていなくても、環境に応じて自ら判断できるということを指す。この例としてよく挙げられるのは映画『2001 年の旅』の HAL9000 だ。一方で、弱い AI とはあらかじめプログラミングされたことに関しては自動的に処理することが可能な一方で、想定外の状況に対しては反応できない AI のことである。現時点で実用段階にある AI はこの「弱い AI」に該当する。例としては無人レジや自動運転、囲碁のアルファ碁などが挙げられる。

もう一つのよく使用される分類方法としては「汎用型 AI」と「特化型 AI」がある。汎用型 AI は人間と同じように過去の経験に基づいて、想定外の出来事が起こった場合にも問題を処理することができるとされている。一方で特化型 AI とは限定された領域の課題に特化して自動的に学習、処理を行うシステムのことを指す。

2.3　機械学習

機械学習とは、コンピューターのプログラムが、データから学習して判断や推論を行うためのアルゴリズムを作成する仕組みである[*3]。主な手法としては教師あり学習、教師なし学習、強化学習、ディープラーニングなどがあるが、現在 AI の領域で最も注目を集めているのはディープラーニングである。

機械学習を行うにあたって最も重要となるのは質の高い学習用データであり、その数は多ければ多いほど精度の高い AI ができる。ここで注意すべきは「質が高い」ことである。なぜなら、集めたデータに偏りがあった場合、現在すでに存在する格差を助長することになる格差の再生産や過少代表等の問題が発生する可能性があるからだ。

機械学習を行う際、一番初めの段階ではアルゴリズムの設計や学習用データの選択などなんらかの形で人間が関与するが、一度学習モデルができると AI は人間の手を離れる。ここで発生する問題は、研究者は機械学習した AI にあるデータを与えるとどのような結果が出るかを知ることはできても、なぜそのような結論に至ったのかを知ることはできない。なぜなら AI はその過程を人間に対して説明することができないからである。これがいわゆるブラックボックス化であり、AI が下した決断等が透明性を欠いていることがしばしば問題視される。

2.4　浮かび上がる懸念点

AI によってビッグデータが解析されることによる懸念は大きく 2 つあげられる。1 つ目は個人情報保護法第 2 条 3 項にいう要配慮個人情報（「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報」）とはかけ離れたような、一見特に保護すべき内容に見えない情報

から要配慮情報を導き出すことが可能になった場合、単体では要配慮個人情報には該当しない情報の取得は

[*3] 西村あさひ法律事務所『AI の法律と論点』（商事法務、2018 年）9 頁

どのように扱われるべきなのかという問題である。詳しくは後述する。

2 つ目は現代社会にすでに存在する格差を再生産する恐れがあることである。AI が優れている点の一つは、個人が行うであろう行動を分析し、パターンを割り出すことによって予測できることである。しかし、この予測をするためのアルゴリズムに様々なバイアスがかかる可能性があることによって、いくつかの問題が生じると山本龍彦は指摘しており、格差の再生産はそのうちの一つである。さらに「うわべだけの相関関係」を汲み取ってしまう場合があることや過小代表の問題についても指摘しており、特にマイノリティに対する影響を大きくなると主張している。この論点については本レポートでは扱わないが、AI の発展に伴い発生する重要な問題であることは留意しておきたい。

3　プライバシー権

3.1　プライバシー権の発展

プライバシーの権利という考え方は、1890 年にサミュエル・D・ウォーレン氏とルイス・D・ブランダイス氏が「プライバシーの権利」という論文を発表し、その中で「ひとりにしておかれる権利 (the right to be let alone)」を提唱したことが発端である。この権利は伝統的プライバシー権とも呼ばれるものである。この時、彼らは伝統的プライバシー権を大きく 2 つに分類した[*4]。1 つ目は「秘密を守る権利、孤独を守る権利、思想・信条・感情をあらゆる形式における公開から保護される権利」であり、2 つ目は「各個人が通常、事故の思想や心情、感情をどの程度他人に伝えるかを決定する権利」である。これは後述する現代的プライバシー権と親和性を持つ。

その後、1960 年にウィリアム・L・プロッサー教授は「プライバシー」という論文の中で、伝統的プライバシー権にまつわる訴訟を不法侵入・私的事実の公開・公衆の誤認・盗用の 4 つに分類し、この分類は第二次不法行為リステイトメントに取り入れられることとなった[*5]。

しかし 1970 年代になりインターネットが発展するに伴って、「ひとりにしておかれること」、すなわち、他者の目に晒されないという消極的な権利だけで本当にプライバシー権は保護されているのだろうか、という疑問が出てくることになった。誰がいつ自分の情報を見ているのかを、個人が知ることができない状況が発生し、実際の生活では直接的に他者の目線にさらされることはなくても、自律的な人生を歩むことが困難になりうるからである。このような状況下で消極的な権利では足りず、自分の情報のゆくえを本人が積極的にコントロールすることが重要であるとした現代的プライバシー権が発展してゆくこととなった。これは自己情報コントロール権とも呼ばれる。

3.2　日本におけるプライバシー権の展開

日本においては『宴のあと』事件（東京地判昭和 39 年 9 月 28 日下民集 15 巻 9 号 2317 頁）において、伝統的プライバシー権が法的な権利として承認された。東京地判裁判所はこの事件においてプライバシー権を「私生活をみだりに公開されない権利」と定義し、民事上の人格権のうちの一つとして認めた。

ノンフィクション『逆転』判決（最判平成 6 年 2 月 8 日民集 48 巻 2 号 149 頁）もプライバシー権を考える上で重要な判例の一つである。ここでは「その者の名誉ある信用に直接関わる事項であるから、その者はみだ

[*4] 福田雅樹ほか・前掲註 1）198 頁

[*5] 石井夏生利『個人情報保護法の理念と現代的課題―プライバシー権の歴史と国際的視点』（勁草書房、2008 年）121 頁

りに右の前科等にかかわる事実を公表されないことにつき法的保護に値する利益を有」すると判断された。これは 12 年の時を経て、被告人の実名は公共のために公表が許された情報から、プライバシー上保護されるべき情報へと変化したことを示している。最高裁は前科者であっても「有罪判決を受けた後あるいは服役を終えた後においては、一市民として社会に復帰することが期待されるのであるから、その者は、前科等にかかわる事実の好評によって、新しく形成している社会の平穏を害されその更生を妨げられない利益を有する」と判断した。つまり、「人生をやり直す自由」が保障されているのである。

（1）に述べた自己情報コントロール権について、日本の最高裁は正面から認めてはいないのが現状である。しかし、京都市における市民の前科照会事件（最判昭和 56 年 4 月 14 日民集 35 巻 3 号 620 頁）や江沢民公演事件（最判平成 15 年 9 月 12 日民集 57 巻 8 号 973 頁）で判断されているように、本人の同意がない個人情報の第三者への提供は、損害賠償の対象となっている。つまり、正面からは認められていないとしても、部分的には現代的プライバシー権を認めていると捉えることができる。

さらに、住民コードと個人の本人確認情報（氏名、生年月日、性別、住所）を地方自治体と行政機関が共有し、一元的に管理することが問題となった大阪住基ネット訴訟（最判平成 20 年 3 月 6 日民集 62 巻 3 号 665 頁）も注目に値する。最高裁は「憲法 13 条は、国民の私生活上の自由が公権力の行使に対しても保護されるべきことを規定しているものであり、個人の私生活上の自由の一つとして、何人も、個人に関する情報をみだりに第三者に開示又は公表されない自由を持つ」と判断している。本判決は保護対象を「個人に関する情報」に限定しており、「開示されない自由」を明示的に保障範囲に含めていることから、自ら公開する情報やその範囲を積極的にコントロールする現代的プライバシー権ではなく、他人の目に晒されない古典的プライバシー権を保護していると理解することができる。一方で、本件 2 審（平成 18 年 11 月 30 日）においては現代的プライバシー権に関する学説の展開に対応し、憲法上の自由としての「自己のプライバシー情報の取り扱いについて自己決定する利益（自己情報コントロール権）」を提示している。大阪高裁は本人確認情報について、この性質を考慮すると、その収集、保有、利用等については①それを行う正当な行政目的があり、それらが当該要請目的のために必要であり、かつ、②その実現手段として合理的なものである場合には原則としては自己情報コントロール権を侵害するものではないと判断している。しかし、本人確認情報の漏洩や目的外利用などによる住民のプライバシーないし私生活上の平穏が侵害される具体的危険がある場合には、正当な行政目的の実現手段として合理性がないものとして自己情報コントロール権が侵害されるとみなされるとした。この大阪高裁の判断は、本人確認情報は個人の内面に関わる秘匿性の高い情報とは言えず、また、住民票コードに関しても本人確認情報の管理や利用を目的として都道府県知事が無作為に指定したものであるから、以上の目的に反しない限りはその秘匿性の程度は本人確認情報と異なるものではないと判断した最高裁判決とはかけ離れたものである。

大阪住基ネット訴訟の最高裁判決については、①「個人に関する情報をみだりに第三者に開示又は公表されない自由」を持つと述べていること、②この権利は情報セキュリティーシステムが脆弱で、そのシステムの構造上、個人情報が漏洩する「具体的な危険」さえあれば、実際に情報の漏洩が起こっていなくてもその権利の侵害を認めうるとしたことの 2 点に着目し、本判決は情報セキュリティーシステムの堅牢性にも注目して自己情報コントロール権の考え方を展開したものと評価できるという考え方[*6]もある。住基ネットシステムの目的や手段と照らし合わせてその正当性を吟味していないことや違憲審査基準を設定してその合理性を判断することなく判断をしたこと、保護対象を「個人に関する情報」を「開示されない自由」と明示的に示したことなどから、本判決は伝統的プライバシー権を保護対象としていると考えるのが妥当である。しかし、システムの安

[*6] 山本龍彦『おそろしいビッグデータ　超類型化 AI 社会のリスク』（朝日新書、2017 年）53 頁

全性や堅牢性に着目した点では昨今の IT 社会に対応した判決だとも捉えられる。なぜならインターネット上にある情報が多くなればなるほど、それを狙ってサイバー攻撃などを行う存在も増加するからだ。

4　プロファイリングについて

4.1　定義

EU の一般データ保護規制 4 条（4）は『プロファイリング」とは、自然人に関するある一定の個人的な側面を評価するために、特に、自然人の業務実績、経済状況、健康、個人的嗜好、興味、信頼、行動、所在又は移動に関連する側面の分析又は予測をするためになされる、個人データの利用から成る個人データのあらゆる形態の自動的な処理をいう」と定義している。具体的には、インターネット上で粉ミルクや哺乳瓶等ベビー用品の購買履歴という一見特に価値のない情報から、その人物が今妊娠しているというセンシティブな個人情報を、機械が自動的に導き出すことができるということを示す。

4.2　プロファイリングと個人情報保護情報保護法

プロファイリングについては 2017 年の個人情報保護法改正時では検討されなかったが「パーソナルデータの利活用に関する制度改正大綱」（以下大綱）において今後継続して検討されるべき事項の一つとして記載されている。

個人情報保護法は 17 条 2 項で本人の同意をあらかじめ得ずに要配慮個人情報を所得することは禁止している。しかし、プロファイリングによって要配慮個人情報に相当するデータを事後的に生成できる可能性があるので、実質 17 条 2 項は死文化していると指摘する「取得同視説」を提唱する声や、事後的なデータ生成の可能性自体が要配慮個人情報の「取得」に該当すると解釈する説もある。確かにこの問題は、プロファイリングが社会に浸透していくほどに大きくなると予想される問題である。だが、この問題を認識していたにもかかわらず、大綱で今後検討するとした理由はその立法過程と要配慮個人情報の取得禁止が定められた趣旨にある[*7]。その情報を実際に取得した時点で差別の要因となるような情報を明らかにすることで、取得の可能性などは含まない、文字通りの取得を禁止することとしたのである。

また、今後の検討課題として記載されたもう一つの理由として考えられるのは、もし、取得同視説の論者が懸念するように AI のビッグデータの解析によって要配慮情報に相当する情報を事後的に得る場合の可能性まで想定するとなると、要配慮個人情報の取扱いにおける「事後取得の予見可能性」を事前に認識することが困難であることなども挙げられる。

要配慮個人情報には該当しない情報から、それに相当する秘匿性を持つ情報を生成する可能性があることは否定できず、むしろこれからその精度は向上していくと考えられる。しかし、事後取得の可能性までを含めて情報取得に対して規制をかけるとすると、その範囲が広くなりすぎるあまり、経済活動などに支障が出てくる可能性がある。また、範囲を広くしすぎると、事前同意が形骸化してしまう恐れがあるのではないかと考えられる。

要配慮個人情報の取得に当たるか否かの議論は事前の予防策として重要なことは言うまでもない。しかし、購買情報などを制限することは現代社会的に厳しいことを考えると、事後的に生成された情報を利用されない権利、または破棄を依頼する権利を保障して事後救済の制度を整えることも検討されるべきだと考えられる。

[*7] 福田雅樹ほか・前掲註 1）236 頁

5　EU の一般データ保護規則と個人情報保護法について

5.1　概要

EU では 2016 年 4 月 27 日に一般データ保護規則（以下 GDPR）が成立した。GDPR は第 1 条において「本規則は自然人の基本的権利及び自由、ならびに特に彼らのデータ保護に対する権利を保護する」と規定している。基本的権利としてプライバシー権を位置付けたことは EU のプライバシー権に対する考え方の特徴であり、日本の個人情報保護法との違いが色濃く出る大きな要因となっている。人間の尊厳という考え方を軸にした GDPR はいくつかの注目すべき規定を設けている[*8]。

1 つ目は 21 条 1 項に規定された、プロファイリングに対して異議を唱える権利（right to object）である。この権利が行使された場合、事業者はプロファイリングを原則中止しなければならないとされている。これはつまり、プロファイリングに対するオプトアウトである。日本の現行法においてはプロファイリングに対して異議を唱える権利としては明記されていない。しかし、利用目的を「できる限り特定し」これを本人に通知または公表することを求める個人情報保護法 15 条及び 18 条を、個人情報をプロファイリングに使用することについても通知及び公表する義務があると解釈した場合、もし利用目的として明記していないのにもかかわらずにプロファイリングをおこなった場合には、個人情報保護法 16 条 1 項の目的外利用であるとして個人情報保護法 30 条により利用停止等の請求対象となると考えることができる[*9]。

2 つ目は自動処理のみに基づいて、自身に法的効果を及ぼす、またはそれと同じ程度自身にとって重要な決定を下されない権利であり、いくつかの条文によって保障されている。まず、22 条 1 項によって自身に法的効果を及ぼす、またはそれと同じ程度自身にとって重要な決定を下されない権利が保障されている。つまり、この条文によって、例えばプロファイリングの結果のみに基づいて銀行の融資や保険加入を断られたり、企業から不合格通知を出されたりすることは違法であるということを示す。GDPR の 22 条 2 項では①個人と事業者間の契約を締結し、これを履行するために必要な場合、② EU または加盟国の法によって承認されている場合、③個人の明示的な同意に基づく場合は、プロファイリングのみに基づいた重要な決定も例外的に許容されるとしている。しかし、このような場合でも、GDPR の 22 条 3 項に基づき、事業者は個人の権利・自由を保護するために適切な措置を講じなければならず、少なくとも人間の介在を得る権利、自らの見解を表明する権利、決定を争う権利を保障しなければならないとされている。さらに、22 条 4 項によると、22 条 2 項に基づいて例外的にプロファイリングのみに基づいて重要な決定がなされる場合であっても、その決定は原則として人種・民族・宗教などのセンシティブな属性情報に基づくものであってはならないとされている。日本の現行法においては GDPR と同じく分析行為自体は可能とされている。そして利用目的の特定や制限によって本人関与の機会を保障する設計になっている。

3 つ目は透明性の要請である。GDPR の 13 条 2 項<f>に基づき、事業者は自動処理のみに基づく決定を行っていること、その決定の「ロジックに関する意味のある情報」、「その処理の重大性及びデータ主体に及ぼす帰結」をデータ主体に対して告知しなければならないとされている。また GDPR15 条 1 項<h>に基づき、市民はこのようなデータにアクセスする権利が保障されている。この目的は「公正と透明性を確保する」ことであり、1（2）で述べたブラックボックス化による透明性の減少を解消しようとしていることが分かる。透明

[*8] 山本・前掲註 6）180 頁

[*9] 総務省ＡＩネットワーク社会推進会議「報告書 2018（案）――ＡＩの利活用の促進及びＡＩネットワーク化の健全な進展に向けて――」

性の要請はもちろん日本においてももとめられているが、自動処理に関しての直接的な規定は日本の現行法には整備されていないと考えられる。

これら 3 点に加え、GDPR は 25 条にプライバシー・バイ・デザインという画期的なアイディアを盛り込んでいる。

5.2 プライバシー・バイ・デザイン

プライバシー・バイ・デザインはプライバシー保護と AI の発展を両立することができる方法として提案されているものであり、計画的なプライバシー対策とも呼ばれる[*10]。これは様々な技術に関する設計仕様の中にプライバシーを組み込むという考え方及びアプローチのことを指し[*11]、カナダのオンタリオ州で情報プライバシーコミッショナーも務めるアン・カブキアン博士が 1980 年代から提唱している考え方である。この目的は、彼女が提唱する 7 原則（1. 事後的ではなく事前的、救済的ではなく予防的であること 2. 初期設定としてのプライバシー 3. 設計に組み込まれるプライバシー 4. 全機能性 5. 生成から廃棄までの安全性 6. 可視性と透明性 7. 利用者のプライバシーを最大限に尊重すること）を守り、プライバシーと個人の情報へのコントロールを保障すること[*12]で、企業や組織が発展し続けることを可能にすることだ。この目的からも推察されるように、カブキアン氏は論文の中で、プライバシー・バイ・デザインによってプライバシーとセキュリティ、プライバシーと事業プロセスの両者を実現することを強調している。この考え方はヨーロッパを始め、幅広く受け入れられており、実際に EU は 2016 年に成立した一般データ保護規則の 25 条に「データ保護バイ・デザイン及びバイ・デフォルト」を組み込むことでプライバシー・バイ・デザインをハードローの中に落とし込んでいる。プライバシー・バイ・デザインは必ずしも法的措置という形を持つ必要はなく、むしろ法的措置の成立は時間と手間がかかるため、自主認証制度を積極的に推進する声も多い。

AI の精度を上げて機能を向上させるためには、できるだけ多くのデータが必要となる。より多くのデータを取り込んだ AI はそこからパターンを見出し、予測の精度を上げていくからである。よって、プライバシー保護という考えは研究者や開発者、そして AI を活用して利益を上げていくことを望んでいる事業者に対しては非常に厄介な足かせとなる。だからこそプライバシーと事業プロセスの両者の実現を目指したポジティブサム的なアプローチは広く受け入れられたのだと理解できる。

日本において、プライバシー・バイ・デザインの考え方は世間一般に浸透しているとは言い難いものの、徐々に取り入れられてきている。例えば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（マイナンバー法）の第 27 条、第 28 条においては

特定個人情報ファイルを保有する行政機関・自治体などに対して「特定個人情報保護評価」と呼ばれるプライバシー影響評価を実施することが義務付けられている。プライバシー影響評価とはプライバシー・バイ・デザインを実践するにあたり、取りうる手法のうちの一つであり、これは情報システムの新規開発や改修にあたり、個人情報を取り扱うプロセス（取得、利用、保存、提供、削除・廃棄など）のどの部分で個人情報漏洩などのプライバシーへの影響（リスク）が生じ得るかを事前に評価し、それに応じたリスク対策をプログラミング段階でインプットするもの[*13]である。また、内閣サイバーセキュリティセンター（NISC）が公表している「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」においては「情報セキュリティを

[*10] 瀬戸洋一『実践的プライバシーリスク評価技法―プライバシーバイデザインと個人情報影響評価』（近代科学社、2014 年）7 頁
[*11] 福田雅樹ほか・前掲註 1）208 頁
[*12] 福田雅樹ほか・前掲註 1）209 頁
[*13] 杉山幸人「プライバシー・バイ・デザインの実務的な基本概念と重要性」情報センサー 11 月号（2017 年）

企画・設計段階から確保するための方策」として、セキュリティ・バイ・デザインの考え方を取り入れている。セキュリティ・バイ・デザインはプライバシー・バイ・デザインがその保護の対象を個人情報とプライバシーに限っていることに対して、保護の対象を情報セキュリティ全般に拡張したものである。つまり、日本においても少しずつ概念が浸透してきていると評価できるが、これからも情報保護の強化及び改善の手段として積極的に取り入れていくことが必要とされるだろう。

6　まとめ

プライバシーを保護することで得られる利益の一つは個人の心理的及び精神的安定や個人の自律性であると考えられる。そもそも AI は、人間の生活をより便利に、より豊かにするために開発されたものであって、それによって精神的安寧が奪われることは本末転倒であり、あってはならないことだ。これを防ぐためにも、自ら学習する AI のさらなる発展可能性を前提としながら、プライバシー権へのリスクとそれに対する対策を練る必要があると考えられる。この対策は万全で堅固である必要がある一方で、柔軟性も兼ね備える必要がある。さらに、行く先が不透明だからこそ事後救済ではなく予防策に対して力をいれるべきではないだろうか。なぜなら AI は日々進化しており、人が予想できていなかった事態に対しても、スピード感をもって迅速に対応することが求められているからである。

これを達成するためには国際的協調が必要不可欠であると考える。まず初めに AI 一般に関する原則の国際的な協調を図り、残りの部分は個別の領域で各国が考えていくことが有効であると思われる。この理由としては 2 点あげられる。1 点目はインターネットやサイバー空間には国境がないので、ある程度共通の事項が定められることである国に偏ることなく開発及び使用を行うことが可能になるからである。AI 一般に関する原則に関しては、すでに様々な議論がなされている。本レポートでとりあげた GDPR はその最たる例である。他の国際文書と比較しても突出して詳細かつ網羅的な規定を設けており、漠然とした概念だったコントロール権を立法上の具体的権利として実現させた点で優れているといわれる[*14]。2 点目は国によって価値観が異なるため、多くの事項に対して承認を得ることが現実的ではないからである。よって、AI 一般に関する原則は個人の尊厳を守ることなど最小限の権利の保障にとどめておくことが良いのではないだろうか。この時、すでに EU が実践しているように、ハードローとソフトローの両面から権利保護に向けたアプローチがとられることが重要だと考える。

日本の法整備に関しては、いまだ検討すべき課題は多いと思われる。特に 4（2）で触れたように、プロファイリングによって事後的に生成可能な秘匿性の高い個人情報に対してどのような保護を行うべきかについては、不確定要素が多い中でも積極的な保護に向けて動いていくべきではないだろうか。この点においては EU の GDPR に規定されるプロファイリングによって得られた情報に対して、その情報を使用されない権利を保障する等の事後救済の制度は大いに参考になる。

また、法的見解からは少し離れるものの、研究者が何を目的として開発、ないしプログラミングを行ったのかという思いや目的を重視することが、健全に AI が発展をしていく上では必要なのではないだろうか。なぜなら、AI が現時点では想像できないほど進化したとしても機械である事実は変化することはなく、人間が使用者であることに変わりはないからだ。

[*14] 石井夏生利「特集 1　個人情報・プライバシー保護の理論と課題：プライバシー権」論究ジュリスト 18 号（2016 年）

7　参考文献

・新井誠ほか『憲法Ⅱ 人権』（日本評論社、2017 年）
・石井夏生利『個人情報保護法の理念と現代的課題―プライバシー権の歴史と国際的視点』（勁草書房、2008 年）
・石井夏生利「特集 1 個人情報・プライバシー保護の理論と課題：プライバシー権」論究ジュリスト 18 号（2016 年）
・宇賀克也『個人情報保護法の逐条解説〔第 6 版〕』（有斐閣、2018 年）
・個人情報保護委員会「日本の個人情報保護政策―目的と基本構造―」（2018 年）
・杉山幸人「プライバシー・バイ・デザインの実務的な基本概念と重要性」情報センサー 11 月号（2017 年）
・瀬戸洋一『実践的プライバシーリスク評価技法―プライバシーバイデザインと個人情報影響評価』（近代科学社、2014 年）
・総務省ＡＩネットワーク社会推進会議「報告書 2018（案）――ＡＩの利活用の促進及びＡＩネットワーク化の健全な進展に向けて――」（2018 年）
・曽我部真裕ほか『情報法概説〈第 2 版〉』（弘文堂、2019 年）
・西垣通『AI 原論　神の支配と人間の自由』（講談社選書メチエ、2018 年）
・西村あさひ法律事務所『AI の法律と論点』（商事法務、2018 年）
・福田雅樹ほか『AI がつなげる社会　AI ネットワーク時代の法・政策』（弘文堂、2017 年）
・堀部政男・JIPDEC 編、アン・カブキアン著・JIPDEC 訳『プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流』（日経 BP 社、2012 年）
・山本龍彦『おそろしいビッグデータ　超類型化 AI 社会のリスク』（朝日新書、2017 年）
・宍戸常寿ほか「連載　AI と社会と法―パラダイムシフトは起きるか〔第 1 回〕テクノロジーと法の対話」論究ジュリスト 25 号（2018 年）
・宍戸常寿ほか「連載　AI と社会と法―パラダイムシフトは起きるか〔第 2 回〕データの流通取引」論究ジュリスト 26 号（2018 年）
・宍戸常寿ほか「連載　AI と社会と法―パラダイムシフトは起きるか〔第 3 回〕契約と取引の未来―スマートコントラクトとブロックチェーン」論究ジュリスト 27 号（2018 年）
・宍戸常寿ほか「連載　AI と社会と法―パラダイムシフトは起きるか〔第 5 回〕専門家責任」論究ジュリスト 29 号（2019 年）
・宍戸常寿ほか「連載　AI と社会と法―パラダイムシフトは起きるか〔第 8 回〕サイバーセキュリティ」論究ジュリスト 32 号（2020 年）
・宍戸常寿ほか「連載　AI と社会と法―パラダイムシフトは起きるか〔第 9 回〕フェイクとリアル―個人と情報のアイデンティフィケーション」論究ジュリスト 33 号（2020 年）