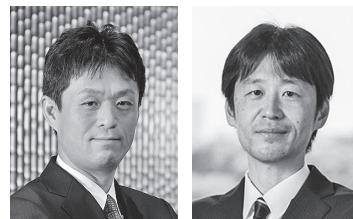


AIの知財戦略と 知財保護における課題

弁護士 福岡 真之介
 会員・弁護士 濱野 敏彦



要約

本稿では、AI（人工知能）に関するプログラム、データ、及びノウハウの知財戦略と知財保護における課題について述べる。AIの中で、特に成果をあげているディープラーニングや、ディープラーニングの中で最も使われることが多いモデルである畳み込みニューラルネットワークについては、既にそのアルゴリズム等の中心的な部分は開示されているため、新たに特許を取得することは難しい面がある。また、AIに関するノウハウは、基本的には、プログラム等を作成するベンダ側に集まることが多いため、一般的な企業としては、このような知見を蓄積していくことは容易ではない。これに対して、データについては、各企業が保護を進めることが可能である。しかも、大量に集積された情報（ビッグデータ）や、いわゆるAIの利活用による新たなイノベーションの創出の可能性の高まりを受けて、データが企業の競争力の源泉としての価値を増している。そのため、AIに関する知財保護については、主にデータについて、営業秘密や限定提供データとして保護する対策を進めることが重要である。特に、限定提供データは、ビッグデータやAIによるデータの価値の高まりを受けて創設され、本年7月1日に施行された平成30年改正不正競争防止法で新たに設けられたものであるため、各企業において限定提供データとして保護されるための管理措置等を整えていくことが重要である。また、AIに関する知財についてもオープン・クローズ戦略を検討する必要がある。

- | | |
|--|---|
| <p>目次</p> <p>1 はじめに</p> <p>2 AI（人工知能）の概念整理</p> <p>3 AIに関するプログラムの知財保護における課題と知財戦略</p> <p>（1）特許による保護における課題</p> <p>ア ディープラーニングに関するプログラム</p> <p>（ア）ディープラーニングの応用技術についての特許</p> <p>（イ）ディープラーニングに用いるデータに特徴を有する特許</p> <p>イ ディープラーニング以外の機械学習に関するプログラム</p> <p>（2）著作権による保護における課題</p> <p>（3）AIに関するプログラムの知財戦略</p> <p>4 AIに関するデータの知財戦略と知財保護における課題</p> <p>（1）弁理士法の改正による弁理士の業務範囲の拡大</p> <p>（2）限定提供データ</p> <p>ア 限定提供データが創設された背景</p> <p>イ 限定提供データの定義</p> <p>（ア）限定提供性（「業として特定の者に提供」）</p> <p>（イ）電磁的管理性（「特定の者に提供する情報として電磁的方法……により……蓄積され、及び管理されている」）</p> <p>（ウ）相当蓄積性</p> <p>（エ）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。」）</p> | <p>ウ 限定提供データに係る不正競争行為</p> <p>エ 営業秘密に係る不正競争行為との相違点</p> <p>オ 限定提供データに係る不正競争行為に対する措置</p> <p>（3）データの知財保護における課題</p> <p>ア 特許による保護における課題</p> <p>イ 実用新案による保護における課題</p> <p>ウ 著作権による保護における課題</p> <p>エ 不正競争防止法による保護における課題</p> <p>（ア）データに関する営業秘密の知財保護における課題</p> <p>（イ）限定提供データの知財保護における課題</p> <p>（4）AIに関するデータの知財戦略</p> <p>ア 限定提供データによる保護の重要性</p> <p>イ 限定提供データとして保護するための方策</p> <p>ウ データの増大と、クラウドコンピューティングサービスの利用</p> <p>5 AIに関するノウハウと知的財産による保護</p> <p>6 アーキテクチャによる保護</p> <p>7 AIに関する知財のオープン・クローズ戦略</p> <p>8 まとめ</p> |
|--|---|

と、ディープラーニング以外の機械学習との間には、本質的に異なる点があることに留意が必要である⁽¹⁰⁾。

3 AIに関するプログラムの知財保護における課題と知財戦略

プログラムについて発生する知的財産権は、基本的には特許権と著作権である。そこで、以下、特許権と著作権について記載する。

(1) 特許による保護における課題

ア ディープラーニングに関するプログラム

(ア) ディープラーニングの応用技術についての特許

まず、前述のとおり、ディープラーニングは、多階層のニューラルネットワークである。

ニューラルネットワークは、30年以上前に提案され、研究され続けてきているものである⁽¹¹⁾⁽¹²⁾。そして、実際の脳は、膨大な量の神経細胞がネットワークを形成しているため、ニューラルネットワークにおいても、層の数を多くすることは誰でも当然に考えていたことであり、当然の試みとして行われてきた⁽¹³⁾。従って、多階層のニューラルネットワークであるディープラーニングについても、そのアルゴリズム等の中心的な部分は、既に開示されており、新たに特許を取得するには難しい面がある。

また、ディープラーニングの中で成果をあげているものの多くは、ニューラルネットワークの中の1つのモデルである畳み込みニューラルネットワーク(CNN:Convolutional Neural Network) (以下「CNN」という。)を用いたものである⁽¹⁴⁾⁽¹⁵⁾。

CNNのルーツは、福島邦彦氏らによって提唱されたネオコグニトロンにある。生理学の実験から、大脳視覚野には、図形等の特徴を抽出する単純型細胞と、特徴の位置が多少ずれても、そのずれを吸収する複雑型細胞とが、階層的に結合されていると考えられている⁽¹⁶⁾。福島邦彦氏らは、この点に着目して、1979年に、単純型細胞のように特徴を抽出するS細胞の層と、複雑型細胞のように情報の位置ずれを吸収する働きを持つC細胞の層を交互に並べた多層の神経回路であるネオコグニトロンを発表した⁽¹⁷⁾。その後、1980年代に、ネオコグニトロンに対して、ニューラルネットワークにおいて一般的な学習方法である誤差逆伝播法が適用されるようになった⁽¹⁸⁾。

そして、現在のCNNの構造や学習方法は、1980年

代のものほとんど変わらない。即ち、ディープラーニングが注目されるようになって、改めてCNNが注目されるようになったといえる⁽¹⁹⁾。

このように、CNNは1980年代から現在に至るまでほとんど変わっていないものであるから、そのアルゴリズム等の中心的な部分は、既に開示されており、新たに特許を取得するには難しい面がある。

(イ) ディープラーニングに用いるデータに特徴を有する特許

ディープラーニングについては、入力データ、教師データとして特徴的なものを選択することにより、特許を取得するという方法が考えられる。

上記2記載のとおり、ディープラーニング用のプログラムに、入力となるデータと教師データを用いてディープラーニングを行うことにより、プログラムを作成することができる。そこで、入力となるデータと教師データが特徴的であれば、特許になる可能性がある。

実際、学習の方法については、単に、「ディープラーニング」、「ニューラルネットワーク」、「CNN」等と記載されているに過ぎず、特許性があるとしたら入力となるデータと教師データについてである特許出願も比較的多い。

これらの特許出願は、当該データと類似する技術分野のデータを用いることを記載している先行技術文献が見つからなければ、実務的に特許として認められる可能性があるものと思われる。

その一方で、特に画像データであれば、どの技術分野のデータであるかを問わず、ディープラーニングが一定の成果をあげることは既に明らかであるようにも思われる。それにもかかわらず、単に、ディープラーニングに用いるデータの技術分野が異なり、当該技術分野のデータを用いることが先行技術文献に記載されていないという一事を持って、特許として認めるのは望ましくない面があるようにも思われる。

特許庁の審査基準においても、ソフトウェア関連発明における進歩性判断にあたって、「種々の特定分野に利用されている技術を組み合わせたり、他の特定分野に適用したりすることは当業者の通常の創作活動の範囲内のものである。例えば、ある特定分野に適用されるコンピュータ技術の手順、手段等を他の特定分野に単に適用するのみであり、他に技術的特徴がなく、この適用によって奏される有利な効果が出願時の技術

水準から予測される範囲を超えた顕著なものでもないことは、進歩性が否定される方向に働く要素となる」とされている⁽²⁰⁾。

ディープラーニングに用いるデータの技術分野が異なり、当該技術分野のデータを用いることが先行技術文献に記載されていないという特許出願が、特許として認められていくのか、拒絶されていくのかは、現時点では明らかではない。そのため、今後の審査実務が注目される。

イ ディープラーニング以外の機械学習に関するプログラム

元々、機械学習は、ビッグデータと呼ばれる大規模データに対する処理（与えられたデータから主として統計的な処理によって有用な情報を抽出する処理）が求められるようになった際に、この中の1つの数理的モデルとして位置付けられ、実用と直接に結びついた学問と考えられるようになったものである⁽²¹⁾。

ディープラーニング以外の機械学習の種類は多岐にわたるが、例えば、現在でも性能の高い分類器として用いられているサポートベクターマシンも1990年代から用いられているように⁽²²⁾、ディープラーニング以外の機械学習は、これまでに使われてきた機械学習方法をベースに発展を続けているものであり、近時において新たな機械学習方法が急激に増えてきたというわけではない。

従って、ディープラーニング以外の機械学習の多くのアルゴリズム等の中心的な部分は、既に開示されており、新たに特許を取得するには難しい面がある。

また、ディープラーニング以外の機械学習は、上記2記載のとおり、ディープラーニングのようにルールの人為的な設定が不要なものではなく、ルールを人為的に設定して作成するタイプに属する。そのため、上記ア（イ）のディープラーニングのように、データに特徴を有する特許出願が急激に増えるというような事情はないものと思われる。

（2）著作権による保護における課題

AIに関するプログラムについても、他のプログラムと同様に、著作物として保護されうる。

しかし、著作権法が保護対象としているのは「表現」であり、アイデアは保護されないため（アイデア／表現二分論）、プログラムのアルゴリズム等

のアイデア部分は保護されないことになる。そして、プログラムの著作物の保護範囲を広く捉えると、実質的にアルゴリズムまで取り込んだアイデア保護になる可能性があるため、保護範囲は狭く解釈される傾向にある⁽²³⁾。

そのため、もちろん、AIに関するプログラムについての著作権を保有すること自体は重要であるが、著作権侵害というためには、相手方のプログラムが、こちらのプログラム著作物に類似していること等を立証する必要があるため、権利行使等までを考慮すると、プログラムの著作権を保有しているのみでは不十分な面があると言わざるを得ない。

（3）AIに関するプログラムの知財戦略

AIに関するプログラムの知財戦略については、大手IT企業等によるオープンソースソフトウェア（以下「OSS」という。）化の流れを考慮する必要がある。大手IT企業等は、ディープラーニングのフレームワーク、ライブラリ等をOSSとして公開している⁽²⁴⁾。

また、上記（1）記載のとおり、ディープラーニング、CNN、ディープラーニング以外の機械学習のアルゴリズム等の中心的な部分は、既に開示されており、新たに特許を取得するには難しい面がある。

さらに、一般的にソフトウェア関連特許の侵害は外部から侵害を把握することは容易でない。さらに、一般的に、ディープラーニングに用いられる入力データと教師データのセットが多い場合には、ディープラーニングが行われた後の結果物から、入力データや教師データを知ることは容易ではないことから、データに特徴を有する特許権の侵害を追及することが困難である⁽²⁵⁾。

これらの事情を考慮すると、AIに関するプログラムに基づいて権利行使を行う目的で特許出願をしていく戦略には、あまり利点がないように思われる。むしろ、AIに関するプログラムの応用技術を生み出した場合には、ノウハウとして保持し、特許出願をすることにより公開されることを避ける方がメリットが大きいのにも思われる。

これに対して、防衛目的や、自社に対する信頼を得る⁽²⁶⁾という観点からAIに関するプログラムの特許を取得することには十分に意味があると思われる。この際には、一定数の特許を取得する目的で、上記（1）ア（イ）記載のとおり、ディープラーニングに用いる

データに特徴を有する特許出願を行うという戦略が考えられる。

また、AIのプログラムそのものに着目するのではなく、視野を広げて、ビジネス関連発明（ビジネス方法がICT（Information and Communication Technology: 情報通信技術）を利用して実現された発明）として特許出願を行うことも検討対象となろう。

具体例の1つとして、特許庁は、IoTのモデルとして、(1) 様々なセンサ等からデータを取得、(2) 取得されたデータを通信、(3) 通信されたデータをクラウド等にビッグデータ化し蓄積、(4) 当該データをAI等によって分析、(5) 分析によって生まれた新たなデータを何らかのサービスへ利活用、(6) IoTにおけるビジネスモデルの確立からなるモデルを想定した場合、(5)の利活用や(6)のビジネスモデルの確立において、自社のビジネスモデルが化体したシステムをビジネス関連発明の特許として保護することが可能な場合があるとしている⁽²⁷⁾。

このようなビジネス関連発明の出願件数は、近年増加傾向で、2016年は約7,900件（暫定値）である。もっとも、日本は、全体の出願件数が世界第3位であるにも関わらず、ビジネス関連発明の分野では、相対的に出願件数が少ないと指摘されており⁽²⁸⁾、日本においても、ビジネス関連発明について特許出願をする伸びしろがあることが示唆されている。

4 AIに関するデータの知財戦略と知財保護における課題

AIに関するプログラムについては、前述の通り、アルゴリズム等の中心的な部分が既に開示されており、新たに特許を取得するには難しい面がある。また、開発の現場では、OSSを利用した開発が広く行われ、プログラムがコモディティ化する傾向にあるため、プログラムよりも、学習させるデータによって製品の内容・質が決まることが多くなってきている。そのため、AIの知財保護を考えた場合には、プログラムの知財保護よりも、データの知財保護の方がより重要となることが想定される。

近時、大量に集積された情報（ビッグデータ）や、いわゆるAI（人工知能）の利活用により新たなイノベーションの創出の可能性が高まり、その結果としてデータが企業の競争力の源泉としての価値を増している。具体的には、工作機械、橋梁等のセンサから得ら

れる稼働等の状況データ、気象データ、化学物質等の素材データ、自動車の車載センサ、ウェアラブル機器、スマートフォン等から得られる消費等の動向や人流データが想定されている⁽²⁹⁾。なお、これらのデータは、センサ等が収集した一次データであり、生データ・元データと呼ばれることもある。

また、上記1記載の通り、AIのうち、特に、ディープラーニングが成果をあげている。その結果として、ディープラーニングに入力データ、教師データとして用いるデータの価値も高まっている。これらのデータは、一般に、上記の生データ・元データに対して、例えば、欠損値の除去、平準化、アノテーションといった加工を行って、入力データ・教師データとして利用できるようにしたものであり、派生データと呼ばれることもある。そして、加工方法についても、加工者のノウハウであったり、加工のために前処理プログラムが利用されることもあり、加工方法そのものが知財保護の対象となることもある。

そこで、本項では、以下の順で、AIに関するデータの知財戦略と知財保護における課題について解説する。

まず、弁理士法の改正による弁理士の業務範囲の拡大について説明する。

次に、AIに関するデータについての保護のために平成30年の不正競争防止法の改正により創設され、2019年7月1日から施行されている限定提供データが創設された背景、及び、限定提供データの要件について解説をする。

そして、データにどのような知的財産が発生するかについて解説する。

最後に、データに関する知財戦略について述べる。

(1) 弁理士法の改正による弁理士の業務範囲の拡大

2018年2月27日に、弁理士法の一部改正を含む「不正競争防止法等の一部を改正する法律案」が閣議決定され、同案が第196回通常国会に提出され、平成30年5月23日に成立し、同月30日に「不正競争防止法等の一部を改正する法律」（法律第33号）が公布された。この改正法は、平成31年7月1日から施行されている（不正競争防止法等の一部を改正する法律の施行期日を定める政令、平成30年9月7日閣議決定）。

この改正により、弁理士が、その名称と責務の下で、技術上のデータ（限定提供データのうち、技術上の情報であるもの）や規格（JIS等）の案の作成に関

する相談に応ずる等の業務を行えることになった（改正弁理士法2条5項，4条3項1号，3号，4号）。

このように，AI・ビッグデータ時代に対応して，弁理士の業務範囲が拡大されており，データ分野における弁理士の活躍が期待されている。

（2） 限定提供データ

ア 限定提供データが創設された背景

限定提供データは，まさに，AIによるデータの価値の高まりを受けて創設されたものである。

限定提供データが創設された背景としては，前述の通り，ビッグデータやAIの利活用により新たなイノベーションの創出の可能性が高まり，その結果としてデータが企業の競争力の源泉としての価値を増していることがある。また，近時，益々データの量が多くなっており，ビッグデータの処理が不可欠になってきている。その中で統計的な処理による有用な情報の抽出等が行われており，その方法として，一般的な統計的な処理の他に，ディープラーニング以外の機械学習によって有用な情報（パラメータ，要素等）を分析的な手法によって抽出する方法も行われている。そして，このように，統計的な処理や，ディープラーニング以外の機械学習の進展により，ビッグデータから有益な情報を抽出することができるようになってきていることも，データの価値を高める一因になっている。

もっとも，データを第三者と共有することにより，当該データが秘密管理性や非公知性を満たさなくなってしまう，営業秘密として保護されない場合もありうる。例えば，商品として広く会員にデータが提供される場合や，秘密保持義務のない緩やかな規約に基づきコンソーシアム内でデータが共有される場合には，秘密管理性や非公知性が失われ，営業秘密として保護されない。そのため，データ保有者が，データを広く共有することに消極的になり，データの流通や利活用が十分に進まない要因になっているとの指摘がなされていた。

そこで，平成30年の不正競争防止法の改正によって，価値あるデータのうち，ID・パスワード等の管理を施した上で事業として提供されるデータについて「限定提供データ」というカテゴリーを新たに設けて，この限定提供データに対する悪質性の高い不正取得・使用等を不正競争行為と位置づけることとし，差止請求権・損害賠償請求権等の民事上の救済措置を設ける

こととなり，本年7月1日から施行されている。刑事措置については，事例の蓄積が少ない中で事業者に過度の萎縮効果を生じさせないようにするという観点から，平成30年改正では導入しないこととされ，今後の状況を踏まえて，刑事措置の導入の是非について引き続き検討することとされた。

イ 限定提供データの定義

限定提供データとは，①業として特定の者に提供する情報として，②電磁的方法（電子的方法，磁気的方法その他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，③相当量蓄積され，及び管理されている，④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。）をいう（不正競争防止法2条7項）。なお，⑤相手を特定・限定せずは無償で広く提供されているデータについては，そのデータの自由な利用を推進するという観点から，そのデータと同一の限定提供データを取得・使用・開示する行為については，不正競争防止法の差止請求・損害賠償請求等の適用が除外されている（不正競争防止法19条1項8号ロ）。

以下では，限定提供データの要件のうち，①限定提供性，②電磁的管理性，③相当量蓄積性，④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。）について述べる。

（ア） 限定提供性（「業として特定の者に提供」）

「業として」とは，データ保有者の反復継続して提供する意思が認められる場合をいう。反復継続的に提供している場合，又は，まだ実際にはデータ保有者がデータの提供を行っていない場合であっても，データ保有者の反復継続して提供する意思が認められる場合には，「業として」に該当する。例えば，データ保有者が，翌月からデータの販売を開始する旨をウェブサイトで公開している場合には，原則として「業として」に該当する。また，事業として提供している場合には，基本的には「業として」に該当する⁽³⁰⁾。

データ保有者は，法人であるか，個人であるかを問わない。また，営利・非営利を問わない⁽³¹⁾⁽³²⁾。

「特定の者」とは，一定の条件の下でデータ提供を受ける者をいう。特定されていれば，実際にデータ提供を受けている人数の多寡は問わないため，データ提供を受けている人数が1億人でも本要件を満たす。

また、「特定の者」には、例えば、(i) 会費を払えば誰でも提供を受けられるデータについて会費を支払って提供を受ける者や、(ii) データを共有するコンソーシアムが、参加について一定の資格要件を課している場合において、当該コンソーシアムに参加する者も該当するとされている⁽³³⁾。

(イ) 電磁的管理性（「特定の者に提供する情報として電磁的方法……により……蓄積され、及び管理されている」）

「電磁的方法」とは、「電子的方法、磁気的方法その他の知覚によっては認識することができない方法という」（不正競争防止法2条7項括弧書）。

限定提供データの要件として電磁的管理性が求められるのは、データ保有者がデータを提供する際に、「特定の者」に対してのみ提供するものとして管理する意思が外部に対して明確に示されることによって、「特定の者」以外の第三者の予見可能性や、経済活動の安定性を確保するためである⁽³⁴⁾。

電磁的管理性の要件が満たされるためには、特定の者に対してのみ提供するものとして管理するという保有者の意思を第三者が一般的にかつ容易に認識できるかたちで管理されている必要がある⁽³⁵⁾。

そのため、管理措置の具体的な内容・管理の程度は、企業の規模・業態、データの性質やその他の事情によって異なるが、電磁的管理性の要件を満たすためには、データ保有者が、特定の者に対してのみ提供するものとして管理する意思を有していることについて、社外の認識が可能であるような措置が取られることが必要である⁽³⁶⁾。

アクセス制限は、通常、ユーザの認証により行われ、認証の方法としては、①特定の者のみが持つ知識による認証（ID、パスワード、暗証番号等）、②特定の者のみが持っている物による認証（ICカード、磁気カード、特定の端末機器、トークン等）、③特定の者の身体的特徴による認証（生体情報等）等が挙げられる⁽³⁷⁾⁽³⁸⁾。一方、例えば、DVDで提供されているデータについて、当該データの閲覧はできるが、コピーができないような措置が施されている場合には、原則として「電磁的管理性」の要件は満たさない⁽³⁹⁾。

(ウ) 相当蓄積性

限定提供データは、「相当量」蓄積されていなければ

ならず、一定の規模が必要とされている。「相当量」とは、個々のデータの性質に応じて、データが電磁的方法により有用性を有する程度の量が存在していることを意味する⁽⁴⁰⁾。

どれくらいのデータ量であれば「相当量」といえるかについて、不正競争防止法は規定を設けていないため、解釈に委ねられるが、「相当量」とは、個々のデータの性質に応じて、データが電磁的方法により蓄積することによって生み出される付加価値、利活用の可能性、取引価格、収集・解析にあたって投じられた労力・時間・費用等が勘案されると考えられている⁽⁴¹⁾。

(エ) 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。」）

一般論として、不正競争防止法による保護が問題となるようなデータは、技術上又は営業上の情報に該当するであろう。そこで、この要件で実際に問題となるのは、定義に「但し、秘密として管理されているものを除く」と規定されている点である。

「秘密として管理されているものを除く」とは、「営業秘密」と「限定提供データ」の両方で重複して保護を受けることを避けるための要件である⁽⁴²⁾⁽⁴³⁾。即ち、あるデータが（秘密管理性を含む）営業秘密の要件を充足すれば、営業秘密として保護され、限定提供データとして重ねて保護されることはない。

例えば、料金を支払えば会員になれる会員限定データベース提供事業者が、会員に対し、当該データにアクセスできるID・パスワードを付与する場合は、原則として「秘密として管理されているもの」には該当しない⁽⁴⁴⁾。

ウ 限定提供データに係る不正競争行為

不正の手段により限定提供データを取得したものとして不正競争行為となるのは、典型的には、IDとパスワードを付与された者しかアクセスできないデータベースに、外部者が、IDとパスワードを盗んでアクセスするような行為である。

限定提供データについて不正競争行為とされるのは、以下の行為である（不正競争防止法2条1項11～16号）。

① 不正取得類型

権原のない外部者が、窃取・詐欺・脅迫等の不正の手段により限定提供データを取得、使用、開示（第三

者提供)する行為である。この類型に当たるものとして、例えば、正規会員のID・パスワードをその会員の許諾なく用いて、データ提供事業者のサーバに侵入し、正規会員のみ提供されているデータを自分のパソコンにコピーする行為が挙げられる⁽⁴⁵⁾。

② 著しい信義則違反類型

限定提供データを正当に取得した者が、不正の利益を得る目的又はデータ提供者に損害を加える目的で、限定提供データを、横領・背任に相当するような態様で使用する行為、又は開示する行為である。この類型に当たるものとして、例えば、データ提供者のための分析を委託されてデータ提供を受けていたにもかかわらず、その委託契約において委託された業務の目的外の使用が禁じられていることを認識しながら、無断で、そのデータを目的外に使用して、他社向けのソフトウェアを開発し、不正の利益を得る行為が挙げられる。

③ 転得類型(取得時悪意型)

取得時に限定提供データについて不正行為が介在したことを知っている者が、当該不正行為にかかる限定提供データを取得、使用、開示する行為である。なお、「営業秘密」とは異なり、入手経路への注意義務が転得者に課されないよう、重過失の者は対象外となっている。この類型(取得時悪意型)に当たるものとして、例えば、不正アクセス行為によって取得されたデータであることを知りながら、当該行為を行ったハッカーからそのデータを受け取る行為や、その後、自社のプログラム開発に当該データを使用する行為が挙げられる。

④ 転得類型(事後的悪意型)

取得時に限定提供データについて不正行為が介在したことを知らずに取得した者が、その後、不正行為の介在を知った場合に、データ提供者との契約等に基づいて取得した権原の範囲を超えて、限定提供データを開示する行為である。この類型(事後的悪意型)に当たるものとして、例えば、データ流通事業者が、データを仕入れた後において、そのデータの提供元が、不正取得行為を行ったという事実を知ったにもかかわらず、その後も、自社の事業として、当該データの転売を継続する行為がこれに当たる。他方で、悪意に転じる前に、その提供元と結んだ契約等に基づいて取得した権原の範囲内で開示する行為は、悪意に転じた後であっても、不正競争行為には該当しない。

エ 営業秘密に係る不正競争行為との相違点

上記①～④で述べた限定提供データについて不正競争行為は、営業秘密における不正競争と概ね同じであるが、以下の点が異なる。

第1に、著しい信義則違反類型(限定提供データを正当に取得した者が、不正の利益を得る目的又はデータ提供者に損害を加える目的で、限定提供データを使用する行為)については、限定提供データでは、限定提供データの管理に係る任務に違反する横領・背任に相当するような態様のものに限って、不正競争行為となる。なお、横領・背任に相当するような態様としては、例えば、以下のような行為が考えられている⁽⁴⁶⁾。

- ・データ提供者が商品として提供しているデータについて、専ら提供者のための分析を委託されてデータ提供を受けていたにもかかわらず、その委託契約において目的外の使用が禁じられていることを認識しながら、無断で当該データを目的外に使用して、他社向けのソフトウェアを開発し、不正の利益を得る行為
- ・コンソーシアムやプラットフォーマー等のデータ提供者が会員にデータを提供する場合において、第三者への提供が禁止されているデータであることが書面による契約で明確にされていることを認識しながら、当該会員が金銭を得る目的で、当該データをデータブローカーに横流し販売し、不正の利益を得る行為

第2に、限定提供データの転得者については、不正競争行為とされるのは、不正行為が介在していたことを知っていた場合に限られ、知らなかったことについて重過失があった場合は含まれない。

第3に、転得者が、事後的に不正行為が介在していたことを知った場合には、限定提供データの「使用」は不正競争行為とならない。また、その場合、限定提供データを「開示」する行為は不正競争行為となるが、その行為がデータ提供者との契約等で取得した権原の範囲を超えなければ、損害賠償請求、差止請求等の対象外とされている。

第4に、営業秘密では、営業秘密を使用することにより生じた物の譲渡も不正競争とされている(不正競争防止法2条1項10号)が、限定提供データを使用することによって生じた物の譲渡については、不正競争とされていない(営業秘密における不正競争防止法2条1項10号と同様の規定が設けられていない)。こ

れは、限定提供データを使用することによって生じる物の価値に対する限定提供データの寄与度等が現時点では判然としないためであるとされている。そのため、例えば、不正取得した限定提供データを用いて作成されたプログラムを譲渡する行為は、不正競争行為とはならない。

オ 限定提供データに係る不正競争行為に対する措置

限定提供データに係る不正競争行為に対しては、営業秘密の場合と同様に、差止め、損害賠償、信用回復措置等の民事上の措置が適用される（不正競争防止法3条、4条、14条）。また、損害賠償については、損害額の推定規定（不正競争防止法5条）も適用される。

限定提供データについての刑事措置は、上記ア記載のとおり、平成30年改正では導入せず、今後の状況を踏まえて引き続き検討することとされた。

(3) データの知財保護における課題

ア 特許による保護における課題

特許法の保護対象である発明とは、「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をいう」（特許法2条1項）。

「技術」とは、一定の目的を実現するための何らかの具体的態様や構成を有していることを要するとともに、その手段が実施可能であり、かつ、反復可能であることを要求されているものと解される。また、情報の単なる提示は、「技術的思想」と評価されない⁽⁴⁷⁾。

特許庁の審査においては、以下のように取り扱われている。まず、データが「情報の単なる提示（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）」であるものについては、発明の要件のうち、「技術的思想ではない」ため、発明には該当しないものとされる⁽⁴⁸⁾。それ以外のもののうち、「構造を有するデータ」（「データ要素間の相互関係で表される論理的構造を有するデータ」）及び「データ構造」（「データ要素間の相互関係で表される、データの有する論理的構造」）がプログラムに準ずるもの⁽⁴⁹⁾である場合には、これらをソフトウェアと同様の基準⁽⁵⁰⁾で、発明に該当するかについて判断される⁽⁵¹⁾。そして、発明に該当すると判断された場合において、さらに、新規性（特許法29条1項）、進歩性（特許法29条2項）等の要件を充足したときに特許されることになる。

以上からすると、データ自体が、発明（「自然法則を利用した技術的思想の創作」）に該当し、さらに、特許になる場合は少ないものと思われる。

他方、データの取得方法や加工方法については、情報処理装置・方法などとして、特許になる場合はありうる。データについては、いかに大量かつ質の高いデータを取得するかということや、データを機械学習などによる分析・解析のためにどのように加工するかということが重要であるから、データの取得方法や加工方法について特許を取得することは十分検討に値するといえよう。

イ 実用新案による保護における課題

実用新案法の保護対象は、「物品の形状、構造又は組合せに係る考案」である（1条、3条1項柱書）。従って、無体物であるデータは保護対象にならない。

ウ 著作権による保護における課題

著作権法の保護対象である著作物とは、「思想又は感情を創作的に表現したものであつて、文芸、学術、美術又は音楽の範囲に属するものをいう」（著作権法2条1項1号）。

そのため、一般的に事実を示すデータ自体が創作性を有することはほとんどない。京都大学博士論文事件では、裁判所は、「実験結果等のデータ自体は、事実又はアイデアであつて、著作物ではない以上、そのようなデータを一般的な手法に基づき表現したのみのグラフは、多少の表現の幅はあり得るものであつても、なお、著作物としての創作性を有しないものと解すべきである。」と判示し、事実を示すデータと、それを一般的な手法で表現したグラフについて、創作性がないものとして、著作物にあたらぬとしている⁽⁵²⁾。

また、著作権法では、データそのものではなくデータ集積物の一類型であるデータベースについて、一定の要件を満たすものについてはデータベースの著作物として保護対象としている。即ち、データベースを「論文、数値、図形その他の情報の集合体であつて、それらの情報を電子計算機を用いて検索することができるように体系的に構成したものをいう」（著作権法2条1項10号の3）と定義した上で、「データベースでその情報の選択又は体系的な構成によつて創作性を有するものは、著作物として保護する」（著作権法12条の2）としている。しかし、独自の基準で情報が選

扱われたり、独自の体系を有するデータベースは汎用性もなく、使い勝手が悪いので、AIを学習させるために作成されたデータベースの多くは、一般的な情報の選択・体系的な構成のものとなり、「情報の選択又は体系的な構成によつて創作性を有する」場合は少ないものと思われる。従って、AIを学習させるために作成されたデータベースに著作権が発生する可能性は比較的低いと思われる。

他方で、著作物に該当するデータを利用する場合として、誰でも容易にアクセスすることができるウェブサイトから自由にダウンロードすることができる画像等をディープラーニング用の入力データ、教師データ等として用いることが考えられる。

もっとも、このような場合には、通常は、著作権の制限規定である「情報解析……の用に供する場合」（著作権法30条の4第2号）に該当し、著作権侵害は成立しない。同様に、誰でも容易にアクセスすることができるウェブサイトから自由にダウンロードすることができる画像等を情報解析する場合も、通常は、著作権の制限規定である「情報解析……の用に供する場合」（著作権法30条の4第2号）に該当し、著作権侵害は成立しない。

このようにデータを著作権で保護できるのは限定的である点が課題である。

エ 不正競争防止法による保護における課題

データについては、営業秘密又は限定提供データとして、不正競争防止法によって保護することが考えられる⁽⁵³⁾。

(ア) データに関する営業秘密の知財保護における課題

営業秘密とは、「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つて、公然と知られていないものをいう」（不正競争防止法2条6項）。一般的には、この営業秘密の定義から、秘密管理性、有用性、及び非公知性の3つが営業秘密の要件であると言われている⁽⁵⁴⁾⁽⁵⁵⁾。

データが、上記3要件を満たす場合には営業秘密に該当する。

そして、「営業秘密」を保有する者は、窃取・詐欺・脅迫等の不正の手段により「営業秘密」を取得する行為⁽⁵⁶⁾や、不正の手段により取得した営業秘密を使用又は開示する行為等（不正競争防止法2条1項4号～

10号）に対して、差止請求、損害賠償請求、信用回復措置請求をすることができる（不正競争防止法3、4、14条）。また、民事上の不正競争行為（不正競争防止法2条1項4号～10号）に含まれる行為のうち、特に違法性が高いと認められる行為について、営業秘密侵害罪として刑事責任が定められている（同21条1項・3項）。

もっともデータを利活用するため比較的広く共有するデータについて営業秘密としての要件を満たすことが難しい点が課題である。

(イ) 限定提供データの知財保護における課題

限定提供データの要件は、上記(2)イ記載の通りである。

限定提供データは、上記(2)ア記載のとおり、ディープラーニングに利用するためのデータや、ディープラーニング以外の機械学習によって分析を行うビッグデータを念頭において創設されたものであるから、電磁的管理性等の要件を満たす管理を行えば、これらのデータが限定提供データとして保護される場合が比較的多くなるものと思われる。

そして、上記(2)イ(エ)記載のとおり、あるデータが、営業秘密の要件を充足する場合には、営業秘密として保護されるのであり、あるデータが、営業秘密と限定提供データの両方で保護されることはない点には注意が必要である。

(4) AIに関するデータの知財戦略

ア 限定提供データによる保護の重要性

上記(2)ア記載のとおり、ディープラーニングが成果をあげていること、及び、ビッグデータの分析が向上していることにより、益々、データの重要性が高まってきている。従って、AIに関するデータの知財戦略として、できる限りのデータを営業秘密や限定提供データ等の知的財産として保護・管理していくことが考えられる。営業秘密の保護・管理の方法については、従前からの議論や裁判例が積み重ねられており、これを活用することができる。

もっとも、AIに関するデータについては、コンソーシアム内、企業間、研究機関間で広く共有したいというニーズがある場合がある。また、広くデータを共有することはAIの開発において有益な場合も多いと考えられる。

しかし、広く共有するデータについて営業秘密としての保護は困難である。また、現行法の下では、前述の通り知的財産権による保護は容易ではない。そこで、AIに関するデータの保護の方法として限定提供データの活用が考えられる。限定提供データは新しい概念であり、また、まさにAIによるデータの価値の高まりを受けて創設されたものであるから、下記に記載の限定提供データとして保護するための方策を採ることが重要である。

イ 限定提供データとして保護するための方策

データを限定提供データとして保護するためには、限定提供データの管理に関するルールを策定し、当該ルールに基づく適切な管理を行うことが重要である。

限定提供データは「情報」であるため、同様に「情報」である営業秘密の管理が参考になる。

営業秘密については、適切な秘密管理規程を作成し、その秘密管理規程に基づく管理をすることにより、訴訟において営業秘密の中で最も激しく争われる秘密管理性の要件が認められやすくすることが望ましい⁽⁵⁷⁾。そのため、同様に、限定提供データについても、一定の管理規程に基づく管理により電磁的管理性が認められやすくすることが望ましい。さらに、限定提供データに対して、技術的にITシステム上のアクセス制限を加えるといったアーキテクチャ上の保護をすることが必要であろう。

また、限定提供データについての適切な管理を行うという観点からは、営業秘密と同様、従業員から入社時、異動時、プロジェクトの参加時、退職時等のタイミングで、誓約書、秘密保持契約書等を取得することが有益である⁽⁵⁸⁾。そのため、同様に、限定提供データについても、誓約書、秘密保持契約書等の対象に含めることが望ましい。

そして、社内で営業秘密に該当することを想定している情報についても、限定提供データの要件（正確には、限定提供データの要件のうち、「秘密として管理されているものを除く」という要件以外の要件）も充足する可能性がある場合には、限定提供データとして保護し得るように管理等をすることが有益である。営業秘密の場合、訴訟においては、様々な証拠等に基づいて、秘密管理性の要件を充足しているか否かを判断するため、予測可能性が低い面がある。これに対して、限定提供データの電磁的管理性の要件は、適切な

認証の措置が施されていれば認められる可能性が高いと思われるため、予測可能性が高い。従って、営業秘密に該当することを想定している情報についても、限定提供データの要件も充足する可能性がある場合には、限定提供データとして保護し得るように管理等をすることが望ましい。

ウ データの増大と、クラウドコンピューティングサービスの利用

企業がディープラーニングを利用するためには、膨大なデータを管理するためのストレージや、膨大な計算処理をするためのコンピュータ処理能力が必要となる。また、ディープラーニングにおける膨大なデータの高速度な処理を行うために重要であるGPU⁽⁵⁹⁾を各企業で揃えることは容易ではない。また、ディープラーニングを利用しないとしても、今後、益々、データの量が増大し、データ管理の負担が大きくなっていくことが想定される。

このように、データ管理の負担への対応策として、クラウドコンピューティング⁽⁶⁰⁾サービスを利用することが考えられる。経済産業省が策定する営業秘密管理指針が2019年1月23日に改訂されたが、秘密管理性については、クラウドコンピューティングサービスを利用して、営業秘密を外部のサーバ（クラウドコンピューティングサービス事業者が保有及び管理をするサーバ）で保管及び管理する場合においても、秘密として管理されていれば、秘密管理性が失われるわけではない旨が追記された⁽⁶¹⁾。これは、AI（深層学習）を用いてプログラムを作成するための機械学習データの典型例である工場の機器の稼働データ、人の行動データ等の膨大なデータを効率的に収集・分析するために、クラウドコンピューティングサービスを利用した外部のサーバによる管理が行われることが想定されることを踏まえてのものである⁽⁶²⁾⁽⁶³⁾。

このように、AIの進展とビッグデータへの対応のためには、クラウドコンピューティングサービスの利用を検討することが望ましい。

5 AIに関するノウハウと知的財産による保護

AIのうち、特にディープラーニングに関しては、様々なノウハウが存在する。

例えば、ディープラーニングを行う前のプログラムにおいて、色々な条件を決めることが必要になる。例

例えば、ニューロンの層の数、各層のニューロンの数、全体のニューロンの数、学習回数、入力データの加工方法等を決めることが必要になる。しかも、これらの条件は、何を目的とするプログラムであるか、入力データ・教師データの量・質、当該プログラムに求められる精度等によって変わり得る。

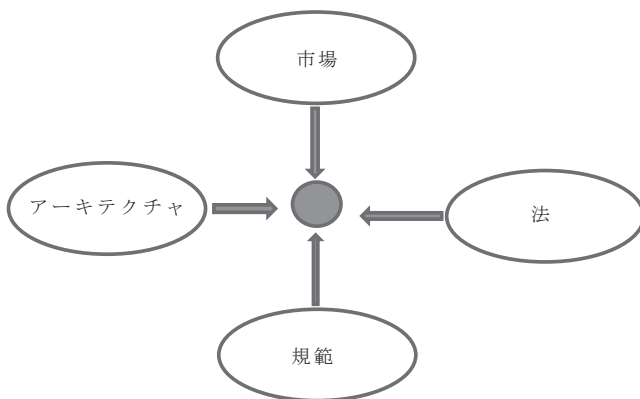
そのため、画一的にこれらの要素を決めることはできないため、経験によって得られるノウハウが重要になってくる。これらノウハウとなる知見は特許等として公開するよりも、営業秘密として管理し、不正競争防止法によって保護していくことが有益な場合が多いように思われる。

なお、これらのノウハウとなる知見は、基本的には、プログラム等の作成をするベンダ側に集まることが多いため、一般的な企業としては、このような知見を蓄積していくことは容易ではないと思われる⁽⁶⁴⁾。

6 アーキテクチャによる保護

アメリカの法学者のローレンス・レッシングは、規制は、法、社会の規範、市場、アーキテクチャの4つによってなされると分析している⁽⁶⁵⁾。そして、サイバースペースでは、それを形作るソフトウェアとハードウェアが人の振る舞いに対する制約を構成する。レッシングはサイバースペースにおいて人の振る舞いを規制するアーキテクチャを「コード」と名づけている。

【図2】⁽⁶⁶⁾



コードの例としては、IDやPWによるアクセス制限や、コピー防止機能によるコピー制限などがある。このようなコードは、技術的に迂回できる方法はあるかもしれないが、一般人からすれば、アクセス権がないデータにはそもそもアクセスすらできないといったように、強力な規制となる。

データについても、法、社会の規範、市場といった制約が存在するが、前述の通り、データに対する法律

による権利保護は限定的であり、またデータ保護に対する社会の規範は弱いといわざるを得ないのが現状である。他方で、データは、電子化されているためIT技術によるコントロールが比較的容易である。そこで、データの知財保護については、法律（契約を含む）による保護だけではなく、アーキテクチャによる保護も併せて考えることがより一層重要であるように思われる。

7 AIに関する知財のオープン・クローズ戦略

最近では、AIソフトウェア開発に習熟したユーザ（開発の委託者）の中には、AIソフトウェア開発を、自社のコアビジネス部分に関する開発とノンコアビジネス部分に関する開発に分けた上で、コアビジネス部分については、ユーザの権利の確保を図る一方で、ノンコアビジネス部分については、ユーザの権利の確保を求めないという動きも見られる⁽⁶⁷⁾。

ユーザとしては、AI開発において、自らのコアビジネスにとって重要であり、秘密性の高いデータを使用する場合には、その成果を他社に利用されたくないとするのが通常である。しかし、例えば、秘密性の高いデータを使用しない場合には、ベンダ（開発受託者）による成果物やデータの広い利用を認めてもよく、その方が開発促進による成果の享受と開発費の抑制の恩恵を受けることができる。ユーザが成果物やデータを囲い込んでしまうと、他人の成果物やデータを利用できなくなってしまうことも多く、開発が非効率となり、技術発展から取り残されてしまう恐れもある。

ベンダとしても、高度かつ効率的な開発をするためには、成果物やデータの広い利用が認められることが望ましいことはいうまでもない。しかし、ベンダとしても、ユーザが提供するデータや、それに基づいて生成される成果物についてユーザの意向を無視することはできない。

そこで、AIに関する知財についても、当事者のニーズを考慮しながら、オープンにするものとクローズにするものを切り分けて、知財の権利帰属や利用条件を決定することは合理的な選択であるといえる。このような考え方は、一般的な意味での知財のオープン・クローズ戦略⁽⁶⁸⁾と必ずしも一致するものではないが、他社に解放する領域と自社で囲い込む領域を分けて対応するという意味で、AIに関する知財についても、オープン・クローズ戦略を取ることが有効な戦

略となる場合があると考えられる。

他方で、AIに関する知財を全て自社に囲い込む戦略は、AI技術に一社のリソースのみで対応することは困難な現実を鑑みると、多くの企業にとっては、他社の有益な技術やデータを利用できないため、競争から脱落するリスクを孕むものといえよう。

8 まとめ

以上において、AIに関するプログラム、データ、及びノウハウの知財戦略と知財保護における課題について述べた。AIに関する知財保護については、ベンダ以外の企業にとって、保護していくことが重要となるのは、主にデータであると思われる。データについては、法律的には、営業秘密や限定提供データとしての保護対策を進めることが重要であると考えられる。特に広く共有するデータについては、限定提供データとして保護することが考えられる。また、併せてアーキテクチャによる技術的手段による保護の重要性も増していくと考えられる。さらに、AIに関する知財戦略については、オープン・クローズ戦略が有効な戦略となる場合があると考えられる。

以上

(注)

- (1) ImageNet Large Scale Visual Recognition Challenge (<http://image-net.org/challenges/LSVRC/>)。
- (2) 松尾豊『人工知能は人間を超えるか ディープラーニングの先にあるもの』(KADOKAWA, 2015年) 144頁~146頁。
- (3) 数万枚の写真を見て何が映っているかを当てるテストでは、人間が間違える確率は5%程度であるのに対して、ディープラーニングを用いたプログラムを用いた場合に間違える確率は2%を切る勢いである(情報処理推進機構『AI白書 2019』(角川アスキー総合研究所, 2018年) 24頁)。
- (4) 松尾豊『人工知能は人間を超えるか ディープラーニングの先にあるもの』(KADOKAWA, 2015年) 45頁。
- (5) 多田智史『あたらしい人工知能の教科書』(翔泳社, 2016年) 12頁。
- (6) 松尾豊「人工知能開発の最前線」法律時報1136号(2019年) 8頁。
- (7) 松尾豊「人工知能開発の最前線」法律時報1136号(2019年) 8頁。
- (8) 廣瀬明『複素ニューラルネットワーク』(サイエンス社, 第2版, 2016年) 2頁。
- (9) ニューラルネットワークのニューロンの層を多層にしたプログラムで、結合荷重が全て初期値となっているプログラムをいう。「学習前プログラム」と呼ばれることもある。

- (10) ディープラーニングと、ディープラーニング以外の機械学習においては、本質的に異なる点があるものの、いずれかが優れているということではない。少なくとも現時点では、ディープラーニングが成果を挙げているのは、CNN等を用いた画像の分野等が中心であり(情報処理推進機構『AI白書 2019』(角川アスキー総合研究所, 2018年) 38頁。), ディープラーニング以外の機械学習の方が成果を挙げている分野も存在する。
- (11) 合原一幸『ニューラルコンピュータ』(東京電気大学出版局, 1988年) 54頁~55頁。
- (12) 中川裕志『東京大学工学教程 情報工学 機械学習』(丸善出版, 2015年) 2頁。
- (13) 松尾豊『人工知能は人間を超えるか ディープラーニングの先にあるもの』(KADOKAWA, 2015年) 148頁~149頁。
- (14) 多田智史『あたらしい人工知能の教科書』(翔泳社, 2016年) 241頁。
- (15) 情報処理推進機構『AI白書 2019』(角川アスキー総合研究所, 2018年) 40頁~41頁。
- (16) 情報処理推進機構『AI白書 2017』(角川アスキー総合研究所, 2017年) 35頁~36頁。
- (17) 国立情報学研究所ウェブサイト (<https://dbnst.nii.ac.jp/pro/detail/498>)。
- (18) 人工知能学会監修『深層学習』(近代科学社, 2015年) 154頁。
- (19) 人工知能学会監修『深層学習』(近代科学社, 2015年) 154頁。
- (20) 特許庁「特許・実用新案審査基準」付属書B「特許・実用新案審査基準」の特定技術分野の適用例 27頁。
- (21) 中川裕志『東京大学工学教程 情報工学 機械学習』(丸善出版, 2015年) 5頁。
- (22) 中川裕志『東京大学工学教程 情報工学 機械学習』(丸善出版, 2015年) 2頁。
- (23) 中山信弘『著作権法』(有斐閣, 第2版, 2014年) 122頁~123頁。
- (24) 情報処理推進機構『AI白書 2019』(角川アスキー総合研究所, 2018年) 140頁~141頁。
- (25) この点については、2019年3月1日に閣議決定され、令和元年5月10日に成立した「特許法等の一部を改正する法律案」に含まれている査証(中立な技術専門家が現地調査を行う制度)が、裁判所においてどのように運用されるかに注意する必要がある。
- (26) 特許を有することで、企業が一定の技術力を有しているという印象を与えることがある。また、それにより取引が円滑となったり、出融資を得ることが容易になることもある。
- (27) 特許庁ウェブサイト「ビジネス関連発明の最近の動向について」(2019年3月12日)。
- (28) 同上。
- (29) 産業構造審議会知的財産分科会不正競争防止小委員会作成に係る平成30年1月付「データ利活用促進に向けた検討中間報告」3頁。
- (30) 本パラグラフにつき、限定提供データガイドライン 8頁。

- (31) 経済産業省知的財産政策室「不正競争防止法平成30年改正の概要」NBL1126号(2018年)15頁。
- (32) 岡村久道「平成30年改正不正競争防止法によるデータ保護」ジュリ1525号(2018年)17頁。
- (33) 限定提供データガイドライン9頁。
- (34) 限定提供データガイドライン10頁。
- (35) 限定提供データガイドライン10頁。
- (36) 限定提供データガイドライン10頁。
- (37) 限定提供データガイドライン10頁。
- (38) 織茂昌之『情報セキュリティの基礎』(日本理工出版会, 再版, 2006年)30頁~31頁。
- (39) 限定提供データガイドライン11頁。
- (40) 限定提供データガイドライン9頁。
- (41) 限定提供データガイドライン9頁。
- (42) 限定提供データガイドライン13頁。
- (43) 岡村久道「平成30年改正不正競争防止法によるデータ保護」ジュリ1525号(2018年)18頁。
- (44) 限定提供データガイドライン13頁。
- (45) 産業構造審議会 知的財産分科会 不正競争防止小委員会「データ活用促進に向けた検討中間報告」(平成30年1月)8頁。以下に挙げる例は、同資料による。
- (46) 産業構造審議会 知的財産分科会 不正競争防止小委員会「データ活用促進に向けた検討中間報告」(平成30年1月)。
- (47) 本パラグラフにつき、中山信弘=小泉直樹編『新・注解特許法 第2版〔上巻〕』(青林書院, 2017年)29頁〔平嶋竜太執筆部分〕。
- (48) 特許庁審査基準第Ⅲ部 第1章 発明該当性及び産業上の利用可能性(4頁)。
- (49) 「「コンピュータソフトウェア」とは、コンピュータの動作に関するプログラム、その他コンピュータによる処理の用に供する情報であってプログラムに準ずるものをいう。」「プログラムに準ずるもの」とは、コンピュータに対する直接の指令ではないためプログラムとは呼ばないが、コンピュータの処理を規定するものという点でプログラムに類似する成立を有するものをいう」(特許庁審査基準第Ⅲ部 第1章 発明該当性及び産業上の利用可能性(6頁))。
- (50) 「コンピュータソフトウェアを利用するものは、「ソフトウェアによる情報処理が、ハードウェア資源を用いて具体的に実現されている」場合は、「自然法則を利用した技術的思想の創作」に該当する。」「ハードウェア資源」とは、処理、操作又は機能実現に用いられる物理的装置又は物理的要素をいう。例えば、物理的装置としてのコンピュータ、その構成要素であるCPU、メモリ、入力装置、出力装置又はコンピュータに接続された物理的装置をいう」(特許庁審査基準第Ⅲ部 第1章 発明該当性及び産業上の利用可能性(7頁))。
- (51) 特許庁「特許・実用新案審査ハンドブック」付属書B「特許・実用新案審査基準」の特定技術分野への適用例「第1章 コンピュータソフトウェア関連発明」(24頁)。
- (52) 知財高判平成17年5月25日(裁判所Webサイト)。
- (53) 商品形態のデッド・コピー規制(不正競争防止法2条1項3号)については、有体物に対してのみ適用され、無体物であるデータには適用されないため(東京高判昭和57・4・28無体集14巻1号351頁)、データ保護に利用することはできない。
- (54) 営業秘密管理指針3頁。
- (55) 営業秘密の保護規定は、加盟国間の最低限の保護水準を定めた「知的所有権の貿易関連の側面に関する協定」(TRIPS協定)の下記規定(特許庁ウェブサイト: https://www.jpo.go.jp/shiryoku/s_sonota/fips/trips/ta/chap3.htm#anchor7setu)を担保する性格を持つものである。
- 第7節 開示されていない情報の保護
第39条〔抜粋〕
- (1) 1967年のパリ条約第10条の2に規定する不正競争からの有効な保護を確保するために、加盟国は、開示されていない情報を(2)の規定に従って保護し、及び政府又は政府機関に提出されるデータを(3)の規定に従って保護する。
- (2) 自然人又は法人は、合法的に自己の管理する情報が次の(a)から(c)までの規定に該当する場合には、公正な商慣習に反する方法により自己の承諾を得ないで他の者が当該情報を開示し、取得し又は使用することを防止することができるものとする。
- (a) 当該情報が一体として又はその構成要素の正確な配列及び組み立てとして、当該情報に類する情報を通常扱う集団に属する者に一般的に知られておらず又は容易に知ることができないという意味において秘密であること
- (b) 秘密であることにより商業的価値があること
- (c) 当該情報を合法的に管理する者により、当該情報を秘密として保持するための、状況に応じた合理的な措置がとられていること
- (56) 不正競争防止法2条1項4号で「営業秘密不正取得行為」と定義される。
- (57) 秘密管理規程の規程内容と留意点については、濱野敏彦「戦略的な情報財の保護・活用の考え方 第6回・完 秘密保持契約等による情報財の保護」NBL1117号(2018年)65~67頁参照。
- (58) 従業員から取得する誓約書、秘密保持契約書等の留意点等については、濱野敏彦「戦略的な情報財の保護・活用の考え方 第6回・完 秘密保持契約等による情報財の保護」NBL1117号(2018年)63~65頁参照。
- (59) GPU(Graphics Processing Unit)は、画像処理装置(チップ)であり、画像処理で利用するような演算処理に特化しているため、行列演算などの単純計算を得意とする(多田智史『あたらしい人工知能の教科書』(翔泳社, 2016年)306頁)。
- (60) クラウド・コンピューティングについては確立した定義は存在しないものの、一般にクラウド・コンピューティングの特徴として、高度なスケーラビリティ(拡張性)、抽象化されたコンピュータリソースであること、サービスとして提供されること、利用料金が安価であることが挙げられており、これらの特徴を有するものがクラウド・コンピューティングと呼ばれることが多い(濱野敏彦「クラウド・コンピューティングの概念整理(1)」NBL918号(2009年)24頁)。
- (61) 営業秘密管理指針11頁。

- (62) 水野紀子ほか「[限定提供データに関する指針]の解説」NBL1140号(2019年)26頁。
- (63) 産業構造審議会 知的財産分科会 営業秘密の保護・活用に関する小委員会「第四次産業革命を視野に入れた不正競争防止法に関する検討 中間とりまとめ」(2017年5月)27頁。
- (64) ただし、ドメイン(対象分野)の知識はユーザが有することが多いであろう。
- (65) ローレンス・レッシグ「CODE VERSION2.0」(翔泳社, 2007年)172頁。
- (66) 同上174頁。
- (67) コアビジネス部分に関する開発としては、例えば、本業のビジネスにおける新製品に組み込むAIソフトウェアの開発

が挙げられる。ノンコアビジネス部分に関する開発としては、例えば、バックオフィスの業務効率を改善するAIソフトウェアの開発が挙げられる。

- (68) オープン・クローズ戦略とは、「企業内部と外部のアイデアを結合させて新技術を創造するオープンイノベーション戦略をとる企業が、企業外部にオープンにしない領域を決めておくことで、自社製品の差別化や重要技術の模倣の防止を図り、価値の獲得を実現する戦略」をいう(杉村光嗣=栗野晴夫「オープンイノベーションとオープン&クローズ戦略(その1)」NBL1107号51頁)。

(原稿受領 2019.4.26)