

ビッグデータから論じるプライバシー保護についての検討 － パーソナルデータとの交差領域における 財産権の制限について －

A Study about Privacy Protection discussed from Big Data.

川上 正隆*

要約

ビッグデータの中でもパーソナルデータについては利活用による高いイノベーション効果が期待されているそして、パーソナルデータは個人情報や個人に関する情報により構成されているため、プライバシーを保護する考えが議論の中心である。しかし、プライバシー権により個人を保護することには十分な期待ができない。

一方、ビッグデータは必ずしも個人に関する情報だけでは構成されておらず、パーソナルデータとビッグデータは、交差領域があるものの両者は完全一致するものではない。そこで、従前ではあまり議論されていないビッグデータの保護の検討をすることにより、交差領域がビッグデータとして、およびパーソナルデータとして重畳的に保護されることが可能となる。そして重畳的な保護の効果として、交差領域ではプライバシーの強い保護が期待できるのである。

【目次】

はじめに

1. パーソナルデータ保護の沿革
 - (1) 世界の動き
 - (2) 日本の動き
2. パーソナルデータのプライバシー論
 - (1) パーソナルデータによるプライバシー侵害の可能性
 - (2) 法運用にみるプライバシー保護
 - (3) プライバシー論の問題
3. 事業者によるプライバシー保護
 - (1) 事業者による保護の問題
 - (2) 事業者による社会基盤整備の必要性
4. 財産権としてのビッグデータの保護
 - (1) 知的財産法による保護
 - (2) 著作権法
 - (3) 不正競争防止法
5. ビッグデータ保護の3ステップ

* 青山学院大学法学研究科客員教授。

(1) 知的財産の保護領域

(2) ビッグデータ保護の3ステップ

結語

<ケーススタディ>

はじめに

現在、ビッグデータについての議論はパーソナルデータが中心で進められている。そしてパーソナルデータ議論では主としてプライバシーが論じられている。パーソナルデータの構成要素である個人に関する情報¹⁾を提供した個人を保護するためにプライバシーの保護について論じることは重要である。

一方、ビッグデータについてはパーソナルデータに係る領域についてはプライバシー論が論じられているものの、プライバシーとは関係のない領域についての議論はあまり積極的にされていない。そもそもビッグデータのなかで経済的効果が高いという理由でパーソナルデータが議論の中心となっているようであるが、ビッグデータは個人情報や個人に関する情報のみの集合体ではない。すなわち「ビッグデータ＝パーソナルデータ」ではないのであるにも係らず、ビッグデータの議論はパーソナルデータの議論に置き換えられることが多く、しかもプライバシー論が主流である。しかしビッグデータとは、個人に関わらない様々な情報もビッグデータを構成するし²⁾、場合により個人に関する情報量よりも遙に多大な情報が存在するとも考えられよう。とするとビッグデータについては保護論の中心となっている領域と保護についての議論がなされていない領域(「複合メガ・システムの法制度領域」)があることが明確である。

しかしビッグデータにせよパーソナルデータにせよ、「情報」の集合体であることは同じであり、決して独立した存在ではない。そのため両者には交差領域が存在する³⁾。つまり、プライバシー論の領域とは異なる領域のビッグデータ保護が可能であれば、交差領域の構

1) 個人に関する情報＝個人情報ではない。個人情報保護法(現行法)による定義(2条1項/改正法でも同義)で「この法律において「個人情報」とは、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等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。)をいう。」とあり、個人に関する情報の中で特定識別性のある情報が個人情報である。そしてパーソナルデータは個人を特定できない情報をデータベース化したものである。

2) 例えば、ビッグデータの項目として「ブログ書き込み発信、SNSつぶやき発言、GPS位置生活情報、防犯カメラ映像、センサー情報、ネット検索閲覧取引履歴などから始まって、隣接する日常の気象環境情報、相互運用可能な状態になっている各種のデータベースの断片情報」(菊池純一編『知財のビジネス法務リスク』(白桃書房、2014年)139頁)との説明がある。

3) 交差ししないパーソナルデータ領域は、ビッグデータのような膨大な情報ではない領域である。例えば個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン(平成26年改正版)では個人情報保護法の対象とする個人情報取扱事業者とは過去6ヶ月以内に5000人以上の個人情報を取り扱った事業者であるとして情報量で分けている。

成要素を提供した個人に対してはより強い保護が期待できるのである。

1. パーソナルデータ保護の沿革

(1) 世界の動き

まず、パーソナルデータの保護について世界と日本の沿革について簡単に整理してみる。

国際間で経済取引が活発になれば、当然のことながら情報の流通も活発になる。その中で、国を越えた情報、特に個人に関する情報の取り扱いについては、自国民あるいは他国民を守るという観点から早い時期から検討されていた。

1980年、OECD（経済協力開発機構）⁴⁾は「プライバシー保護と個人データの越境流通についてのガイドラインに関する理事会報告」⁵⁾、いわゆるOECDガイドラインを採択した。これは全5部の構成であるが、特に「第2部 国内適用における基本原則」⁶⁾は、日本の個人情報保護法のみならず、世界に与えた影響は大きい。

1993年に発足したEU（欧州連合）は、2年後の1995年に「個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令（データ保護指令）」⁷⁾を採択した。この指令は域内だけでなく域外の第三国への個人データ移転の原則⁸⁾があり、EU域外の国に対してもデータ保護を求めたものである。

1990年代、カナダのAnn Cavoukian, Ph.D.が“Privacy by Design”（プライバシー・バイ・デザイン）を提唱した。これは「プライバシー情報を扱う〈あらゆる側面〉において、プライバシー情報が適切に取り扱われる環境を〈あらかじめ〉作りこもうとする〈コンセ

4) OECD（Organisation for Economic Co-operation and Development）とは、先進国間の自由な意見交換・情報交換を通じて、1) 経済成長、2) 貿易自由化、3) 途上国支援に貢献することを目的とした国際機関で、現在（2015.6）では34カ国が参加している。

5) “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”

6) “PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION”

個人データを取り扱う場合の原則として“Collection Limitation Principle（収集制限の原則）”、“Data Quality Principle”（データ内容の原則）、“Purpose Specification Principle”（目的明確化の原則）、“Use Limitation Principle”（利用制限の原則）、“Security Safeguards Principle”（安全保護の原則）、“Openness Principle”（公開の原則）、“Individual Participation Principle”（個人参加の原則）、“Accountability Principle”（責任の原則）のいわゆるOECDプライバシー・ガイドライン8原則を定めている。

7) “The Data Protection Directive : Directive on the protection of individuals with regard to the processing of personal data and on the free Movement of such data”

8) “Article 25 - Principles”では“1. Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.”としてEU域内から第三国へ個人データの移転する場合は、原則として当該第三国が十分なレベルの保護措置を確保していることを条件としている。

プト」⁹⁾ というプライバシー保護のためのシステム¹⁰⁾ であり、現在ではプライバシー保護に関する世界的潮流とも言える。

OECD、EU に続き APEC (アジア太平洋経済協力)¹¹⁾ も 2004 年、「APEC プラバシー・フレームワーク (“APEC Privacy Framework”)」を採択し、OECD ガイドラインと同様に個人に関する情報の保護を参加国に求めると共に、2007 年には「APEC 越境プライバシールール (“Cross Border Privacy Rules”)」を策定し、国境を越える個人に関する情報の取扱いの保護を求めた¹²⁾。

なお、OECD は現在ガイドラインの見直しを議論中であり、EU はデータ保護指令に代わるものとして「データ保護規則」¹³⁾ の制定が検討されている。

(2) 日本の動き

日本では、1964 年「宴のあと事件」¹⁴⁾ にて「いわゆるプライバシー権は私生活をみだりに公開されないという法的保障ないし権利として理解される」と判示され、司法判断によりプライバシー権の解釈がなされた。そして、「1960 年代以降、判札上のプライバシー議論が展開する一方で、1970 年代に入ると、個人情報保護法制の実現に向けた取組」¹⁵⁾ がはじまった。さらに、住民基本台帳の電算化に伴い、地方公共団体の個人情報保護条例が多数制定された。その後、「インターネット社会の進展、住民基本台帳法の改正による国民葬番号制への懸念、EU 保護指令の「十分なレベルの保護」の問題、国内における個人情報漏えい事件の多発といった状況を受け、1999 年以降に入ると個人情報保護法の立法

9) 堀部政男/JIIPDEC『プライバシー・パイ・デザイン』(日経 BP 社、2012 年) 10 頁。

10) Privacy by Design は 7 つの原則で構成されている。すなわち “Proactive not Reactive; Preventative not Remedial” (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)、“Privacy as the Default Setting” (初期設定でプライバシー保護が有効化されていること)、“Privacy Embedded into Design” (IT システムのデザインにプライバシー保護が組み込まれること)、“Full Functionality – Positive-Sum, not Zero-Sum” (全機能であること。ゼロサムではなくポジティブサム)、“End-to-End Security – Full Lifecycle Protection” (データのライフサイクル全般で保護されること)、“Visibility and Transparency – Keep it Open” (可視化と透明化が確保されたプライバシー保護の仕組みと運用であること)、“Respect for User Privacy – Keep it User-Centric” (ユーザーのプライバシーを最大限に尊重すること)、である。

11) APEC (Asia-Pacific Economic Cooperation) とは、環太平洋地域における多国間経済協力を進めるための非公式なフォーラムで 21 の国と地域の経済協力枠組みである。

12) 国単位では、例えばアメリカは「1970 年以降、プライバシー保護法を数多く成立させるようになった。公的部門に関しては、1974 年プライバシー法 (Privacy Act of 1974) が成立し、民間部門に関しては、自主規制を基本とし、特に機密性が高い情報を扱う分野において、数多くの個別法が成立されている。」(石井夏生利『個人情報保護法の理念と現代的課題』(勁草書房、2008 年) 419 頁) であったが、2015 年 2 月、CPBR / Consumer Privacy Bill of Rights (消費者プライバシー権利章典) 法案を公表し、ある意味で包括的なプライバシー保護法制定を試みている。

13) “General Data Protection Regulation : REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data”

14) 東京地判昭和 39 年 9 月 28 日判例時報 385 号 12 頁 (宴のあと事件)。モデル小説により私生活が公開されたとしてプライバシー権侵害で訴えた事案。「石に泳ぐ魚事件」(後出) も同様である。

15) 石井・前掲注 12) 472 頁。

化が議論されるように」¹⁶⁾ なり、議論の末、個人情報保護の法制は、2003 年「個人情報の保護に関する法律（個人情報保護法）」¹⁷⁾ として成立した。

個人情報保護法は 2005 年に民間事業者への完全施行がされたが、その後いわゆるビッグデータが登場する。ビッグデータについては IT 社会を支える基盤として、また様々なイノベーション創出の可能性も世界的な潮流として期待されている。我が国政府もビッグデータの活用を成長戦略の一角に位置づけ、例えば、ビッグデータの中でも経済・産業に与える影響が大きいとされているパーソナルデータについては、2013 年 12 月に政府より「パーソナルデータの利活用に関する制度見直し方針」¹⁸⁾ が打ち出され 2014 年 6 月には「パーソナルデータの利活用に関する制度改正大綱」¹⁹⁾ が公表された。さらには本年の通常国会にて成立が予定されている個人情報保護法改正により、積極的なデータ利活用が期待され、この動きと並行してビッグデータ（あるいはパーソナルデータ）についての法律論も活発に論じられていた。

一方、2014 年後半の 7 月には、大手教育事業者において大規模な個人情報流出事故が発生し、個人情報保護の強化が要請される社会問題となった。そして教育事業者事故を受けて、経済産業省は 8 月に「個人情報保護法等の遵守に関する周知徹底の要請」²⁰⁾ の文書を発出した。これは、法やガイドラインの改正に先立ち、速やかに個人情報の保護を徹底するため、「①社内の安全管理措置、②委託先及びその先に関与する事業者の監督、③外部からの適正な個人情報の取得」を求めるものであり、この要請の内容は「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」に引き継がれ、12 月に改訂版が公表された²¹⁾。さらに 10 月には、国際的にサービスを展開している事業者向けに、パーソナルデータの取得時における消費者への情報提供・説明に関する事項を取りまとめた「オンラインサービスにおける消費者のプライバシーに配慮した情報提供・説明のためのガイドライン」²²⁾ が公表された。また、2015 年 1 月には不正競争防止法により保護がなされている営業秘密についての「営業秘密管理指針（全部改訂）」が公表された。その後、2015 年 5 月には年金事業者による大規模な個人情報の流出事故が発生した。

そして、個人情報の保護とパーソナルデータの利活用を目的とした、個人情報保護法の改正が成立した²³⁾。

16) 石井・前掲注 12) 474 頁。

17) 我が国の個人情報保護法は OECD8 原則に基づいた内容である。

18) 高度情報通信ネットワーク社会推進戦略本部「パーソナルデータの利活用に関する制度見直し方針」（2013 年 12 月 20 日）。

19) 高度情報通信ネットワーク社会推進戦略本部「パーソナルデータの利活用に関する制度改正大綱」（2014 年 6 月 24 日）。

20) 経済産業省（<http://www.meti.go.jp/press/2014/08/20140818001/20140818001.html>）。

21) 経済産業省（http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guIDeline.pdf）。

22) 経済産業省（<http://www.meti.go.jp/press/2014/10/20141017002/20141017002.html>）。

23) 第 189 回通常国会で審議され、2015 年 9 月 3 日成立した。なお、改正個人情報保護法の施行は附則では「公布の日から起算して 2 年を超えない範囲」とされている。

このように個人に関する情報は、利活用による利便性と情報流出などの危険性という突出した両面の性格を有している。したがって、個人を保護するという観点から、世界および日本においてプライバシー論が議論されるのは当然である。

2. パーソナルデータのプライバシー論

(1) パーソナルデータによるプライバシー侵害の可能性

ビッグデータは「情報通信技術の進展は、多種多様かつ膨大なデータ、いわゆるビッグデータを収集・分析することを可能とし、これにより新事業・サービスの創出や我が国を取り巻く諸課題の解決に大きく貢献する等、我が国発のイノベーション創出に寄与するものと期待されている」が、その中でも「特に利用価値が高いとされているパーソナルデータ」²⁴⁾については、多くの事業者が利活用についての検討を行っている。

一方、改正個人情報保護法が目的としているように、「本人の利益のみならず社会全体の利益の増進のためにパーソナルデータの利活用を益々促進することが望まれる一方、プライバシー保護の観点からは、これまでと同様、適切な取扱いが求められている」²⁵⁾としてプライバシーの観点からパーソナルデータの保護が必要とされている。

ところで、個人を特定しない情報²⁶⁾の集合体たるパーソナルデータ（集合匿名情報や統計情報など）により個人のプライバシーが問題となる（プライバシー侵害が生ずる）可能性があるのだろうか。これについては例えば「〇〇地域の住人の特性」とか「△△体型の男性の特性」など、住んでいる地域や外部から認識できる情報により属性情報が判明することで当該属性所属者のプライバシー問題が生ずる可能性がある。この他にも職業や収入、病歴など本人が開示している情報が属性情報に含まれることにより偏見や差別的な問題が生ずることも考えられる。過去においても科学的に根拠がない血液型による性格診断といったテレビ番組により血液型属性情報者に対する問題が生じたケースがある²⁷⁾。

24) 方針・前掲注18)。

25) 大綱・前掲注19)。

26) 個人情報保護法（改正案）では、「パーソナルデータ」という用語は使用していないが、改正法2条9項にて「この法律において「匿名加工情報」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないよう個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。一 第一項第一号に該当する個人情報当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

二 第一項第二号に該当する個人情報当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。」と定義しており、「特定の個人を識別できない情報」の集合体である。

27) 放送倫理・番組向上機構（BPO）放送と青少年に関する委員会「「血液型を扱う番組」に対する要望」（2004年12月8日）。委員会の中では「これまで娯楽番組として見過ごしてきたが、最近の血液型番組はますますエスカレートしており、学校や就職で血液型による差別意識が生じている」という指摘もある。<http://www.bpo.gr.jp/?p=5125>

このようなことが考えられるため、個人を特定しない情報であるパーソナルデータと言えども個人の保護のために、プライバシー論が生ずるのである。

(2) 法運用にみるプライバシー保護

では、プライバシーに基づく個人の保護の実情はどうか。

まず、前述のようにプライバシー権は法で定義された権利ではなく判例法理である。したがってパーソナルデータに起因してプライバシー侵害を受けた個人は、裁判によりプライバシー権の主張を展開する必要がある。しかしそれは個人に対して裁判の維持という期間的・金銭的負担を求めるものである。まず裁判に要する期間をいくつかの裁判事案でみると、プライバシー権で争われた「宴のあと事件」では約3年間²⁸⁾、「石に泳ぐ魚事件」では約8年間²⁹⁾の期間を要している。個人情報出事故の事案では、「宇治市住民基本台帳漏洩事件」³⁰⁾では約3年間³¹⁾、「早稲田大学名簿提出事件」³²⁾では約5年間³³⁾、「エステサロン事件」³⁴⁾では約5年間³⁵⁾を要している。これらの事案での原告（プライバシー侵害や個人情報流出された者）は1人ないし少数³⁶⁾であり、裁判期間が長ければ多くの負担、とりわけ訴訟費用などの金銭的負担が一人あたりについて大きくなる。では、裁判の結果として負担に見合った損害賠償が認められるのであろうか。これについては、例えば「宴のあと事件」では請求額100万円に対して10万円が、「宇治市住民基本台帳漏洩事件」では請求額33万円に対して一人あたり1万円および弁護士費用5千円が、「早稲田大学名簿提出事件」では請求額110万円に対して一人あたり5千円が、「Yahoo! BB事件」では請求額10万円に対して一人あたり6千円が、「エステサロン事件」では、請求額115万円に対して3万5千円（12人）および2万2千円（1人）が損害賠償額として認められた。この金額が多い少ないというのは主観であるが、少なくとも数年を要する訴訟費用にははるかに及ばない。つまり、プライバシー侵害あるいは個人情報流出等の事故の被害者は、救済のた

28) 昭和39年判決（宴のあと事件）の提起は昭和36年（ワ）第1882号。

29) 最高判平成14年9月24日判例事報1324号5頁（石に泳ぐ魚事件）の一審提起は平成6年（ワ）第25182号。

30) 市から業務の委託を受けた会社の従業員が、市の担当者の了解を得て、住民基本台帳のデータを光磁気ディスクにコピーして持ち出しが、後にこれを名簿等の販売業者に売却した事案。

31) 最高判平成14年7月11日判例地方自治265号10頁（宇治市住民基本台帳漏洩事件）の一審提起は平成11年（ワ）第1311号。

32) 大学が講演会を開催するに際し申込者である学生の同意を得ることなく、参加者名簿を警察に提出したことにつき、プライバシー侵害の不法行為に基づく損害賠償を大学に求めた事案。

33) 東京高判差戻控訴審平成16年3月23日判例時報1855号104頁（早稲田大学名簿提出事件）の一審提起は平成11年（ワ）第7043号。

34) システムで保管していたエステティックサロンに関するアンケート等の回答がインターネットで閲覧可能状態となり、個人情報第三者に流出した事案。

35) 東京高判平成19年8月28日判例タイムズ1264号299頁（エステサロン事件）の一審提起は平成14年（ワ）第27790号他。

36) 原告側は、「宴のあと事件」は1人、「石に泳ぐ魚事件」は1人、「宇治市住民基本台帳漏洩事件」は3人、「早稲田大学名簿提出事件」は3人、「Yahoo! BB事件」は5人、「エステサロン事件」は13人である。

めに裁判により損害賠償を求めても、実質的により多額の金銭的負荷を負うのである。では、損害賠償以外で被害者（原告）が請求できる救済措置はあるだろうか。プライバシー論は民法（不法行為）に基づく救済論である。したがって条文上は「損害賠償請求（709条）」に加え「名誉毀損における原状回復（723条）」³⁷⁾ 措置を請求することも可能である。しかし、723条を請求している事案はあまりない。その理由は明確ではないが、謝罪広告により自己（原告）に関する情報が公開されるという二次被害の発生リスクにより請求を躊躇うことも考えられる。

プライバシー侵害や個人情報流出事故等は、情報による侵害の発生と言える。その場合、被害者が求めるエンフォースメントは「差止請求」ではないだろうか。損害賠償により多少なりとも金銭的救済は可能であるが、自己に関する情報が何らかの形で流通している以上、二次被害、三次被害の発生可能性は否定できない。したがって本来は、「情報の流通を差し止める」ということが必要である。例えば「石に泳ぐ魚事件」では、「人格的価値を侵害された者は、人格権に基づき、加害者に対し、現に行われている侵害行為を排除し、又は将来生ずべき侵害を予防するため、侵害行為の差し止めを求めることができるものと解するのが相当である。」と判示して人格権に基づいて出版の差し止めを認めた。しかし差止請求は不法行為法の条文上は認められてはいない。判例上もプライバシー侵害により差止請求を認めた事案は非常に少なく、「石に泳ぐ魚事件」以外では、「北方ジャーナル事件」³⁸⁾、「ジャニーズ・ゴールドマップ事件」³⁹⁾、「ジャニーズ・おっかけマップスペシャル事件」⁴⁰⁾ などしかない。

「北方ジャーナル事件」は「実体法上の差止請求権の存否について考えるのに、人の品性、徳行、名声、信用等の人格的価値について社会から受ける客観的評価である名誉を違法に侵害された者は、損害賠償（民法710条）又は名誉回復のための処分（同法723条）を求めることができるほか、人格権としての名誉権に基づき、加害者に対し、現に行われている侵害行為を排除し、又は将来生ずべき侵害を予防するため、侵害行為の差し止めを求めることができるものと解するのが相当である。けだし、名誉は生命、身体とともに極めて重大な保護法益であり、人格権としての名誉権は、物権の場合と同様に排他性を有する権利というべきであるからである」としたうえで本件について「本件記事を掲載する本

37) 民法723条「他人の名誉を毀損した者に対しては、裁判所は、被害者の請求により、損害賠償に代えて、又は損害賠償とともに、名誉を回復するのに適当な処分を命ずることができる。」

38) 最高判昭和61年6月11日判例時報1194号3頁（北方ジャーナル事件）。知事選挙の立候補予定者であった被上告人が、その名誉を傷つける内容の記事が掲載された雑誌の販売等の差し止めを申請した仮処分が認められなかったことについて、一方上告人は同命令が違憲違法であるとして、損害賠償を請求した事案。

39) 東京地判平成9年6月23日判例時報1618号97頁（ジャニーズ・ゴールドマップ事件）。芸能人の自宅や実家住所、電話番号等を掲載した書籍の出版企画に対して、私生活の平穏という人格的利益（プライバシー権）侵害を主張して出版差し止めを求めた事案。

40) 東京地判平成10年11月30日判例時報1686号68頁（ジャニーズ・おっかけマップスペシャル事件）。前記事案と同様に、芸能人の自宅や実家住所、電話番号等を掲載した書籍の出版企画に対して、私生活の平穏という人格的利益（プライバシー権）侵害を主張して出版差し止めを求めた事案。

件雑誌の発行によつて事後的には回復しがたい重大な損失を受ける虞があつたということが出来る」として差し止めを認めた。

「ジャニーズ・ゴールドマップ事件」では、裁判所はまず、「プライバシー権という表現は、必ずしも一義的なものではないので、ここでは、本件紛争の実質から、私生活の平穩を享受するという人格的な利益ととらえることとする」として、プライバシー権という表現は避けつつ、「本件書籍の出版、販売によって、原告タレントらの私生活の平穩を享受するという人格的利益にさらに大きな被害が発生する可能性が高い」うえ、「そのような被害は、その回復が極めて困難な性質のもの」であるため、「被害の発生を避けるために本件書籍の出版、販売を差し止めることも許容されるものというべきである」として人格的な利益に基づき差し止めを認めた。

一方、「ジャニーズ・おっかけマップスペシャル事件」で裁判所は、「一般に、他人に知られたくない私的事項をみだりに公表されない利益（以下「プライバシーの利益」という。）は、個人の人格的生存に不可欠な人格的利益として法的保護に値するというべきものである。そして、公表されたある事項が法的保護の対象となる「他人に知られたくない私的事項」と認められるためには、その事項が、「(a) 私生活上の事柄であること、(b) 一般人の感性を基準にして、公開を欲しないであろうと認められる事柄であること、(c) 一般の人々に未だ知られていない事柄であることを要するものと解される。」とプライバシーの利益を示したうえで「プライバシーの利益の原状回復の困難性に鑑みると、個人のプライバシーの利益を違法に侵害する表現行為については、その表現行為の内容が専ら公益を図る目的のものでないことが明白であり、かつ、被害者が重大にして著しく回復困難な損害を被るおそれがある場合に限って、例外的にその事前差し止めが許されるものというべきである」と重大にして著しく回復困難な損害を被るおそれがある場合差し止めが出来る限定し、そして「一般人であっても自分の住居の所在地がメディアによって広く公表されるようなことがあれば相当の脅威を感じるのが自然であると思われるが、特に右のような事態に直面することが予想される原告らの心理的な負担や不安感には極めて深刻なものがあるものと推測される。したがって、本件書籍の出版、販売が継続されれば、原告らが重大にして著しく回復困難な損害を被るおそれがあることも明らかである。以上によれば、本件書籍の出版、販売を差し止めることは許容されるものと解すべきである」と判示して差し止めを認めた。

このようにプライバシーを根拠として差止請求が認められる場合は極めて限定的であり、単に人格権の侵害だけでは認められず、プライバシーに係る受忍限度を超えた（回復困難な被害）強い違法性が存在する場合に限られる。それはパーソナルデータに係る事案であっても、差止請求が認められる場合はこれらの事案と同様にかなり限定的であると考えられる⁴¹⁾。

41) むしろ認められる場合は稀有と言っても良い。

(3) プライバシー論の問題

以上の検討からみると、プライバシーによる個人の保護は現状では効果が期待できない。しかしパーソナルデータにおいて、データ提供者たる個人の保護が不十分であれば、パーソナルデータへの警戒が利活用の萎縮を生じ、期待されている効果が発しにくくなる。

世界的潮流と言える“プライバシー・バイ・デザイン”の考え方からは、個人を保護するプライバシー論が当然ではあるがパーソナルデータを社会で積極的に利活用するのであれば、個人を保護するための社会基盤が整備されている必要がある。しかし前述のように、日本ではプライバシーを基に個人が保護を求めたとしても、損害賠償額は数万円程度であり（裁判費用を含めれば損失となる）、差し止めはほとんど認められない。つまりパーソナルデータに対する個人のエンフォースメントという社会基盤が未整備なのである。

この点について、プライバシーに基づくエンフォースメントの効果を高めるためには、個人に対して判例法理であるプライバシー権を法制化して権限を付与する、あるいは集団代表訴訟制度の導入により集団としての権限を付与するという方法である。しかし、権限を付与した個人に訴権を認めた場合、100万人、1000万人、1億人といった構成要素数だけ訴権が生じ、膨大な量のパーソナルデータが、たった一人の求めにより使用が差し止められ、あるいは再使用のためにデータの再構成が必要となり、パーソナルデータは恒常的に個人の数だけ予測困難なリスクを内在することとなる。そのためパーソナルデータにだけプライバシー権や集団代表訴訟を認めるには、相当の合理的根拠がなければ立法化は難しいであろう。

次に考えられるのは、パーソナルデータ保有者の事業者によるエンフォースメントである。本来、データを提供した個人が自らに起因して自らのプライバシー侵害等を起こすことは稀である。パーソナルデータにより何らかの事故が生ずる場合、それは専ら保有事業者に起因するであろう。事業者はパーソナルデータの利活用により利益を得ることができるが、同時にデータ提供者たる個人を保護するという責務を負う。その責務は、パーソナルデータによる事故や侵害が生じないような管理をすると共に、不幸にも何らかの事象が生じて個人に被害が生ずるような場合には、速やかな救済を行うというものである。それは個人に比して社会的な影響力が強い事業者に求められる当然の責務と言える⁴²⁾。つまり事業者はデータを提供した個人が保護されるための社会基盤としてセーフティ・ネットを構築する必要がある。では、事業者はパーソナルデータを基にしてどのようなエンフォースメントが可能なのか、次項で検討を行う。

42) 個人情報保護法は個人情報を取り扱う事業者に適用される法であるが、1条の法目的には、現行法・改正法ともに「個人の権利利益を保護することを目的とする」と明記されている。

3. 事業者によるプライバシー保護

(1) 事業者による保護の問題

進化した情報化社会では、事業者は比較的簡単に大量の情報を収集し保有することが出来る。個人が有する情報量よりも遥かに多くの情報を保有する事業者は、情報量という点で社会的強者である。しかし、情報に関する事故が生じた場合、事業者のダメージは情報量に比例して大きくなるし、特にそれが個人に関する情報であれば被害は情報提供者たる個人にも被害は及ぶ。それを回避するため、我が国において情報法の構成は、事業者に対して情報の管理や行為に対する規制法の構成をとっている⁴³⁾。

例えば個人情報やパーソナルデータで議論されている個人情報保護法は、個人情報（改正法ではパーソナルデータも含め）の保護を法目的としているが、個人情報自体に何等かの権利を付与するのではなく、個人情報やパーソナルデータの取り扱いや管理等について事業者へ義務を課すことで情報の保護を図る仕組みをとる事業者規制法である⁴⁴⁾。法違反行為が認められた場合には、当該事業者が行政指導あるいは罰則を受けるが、第三者による不正行為により個人情報が侵害を受けた場合、事業者や個人にエンフォースのための訴権はない。

ビッグデータの収集には、情報の社会インフラを有している事業者が有利である。その社会インフラの一つに情報基盤としての電気通信事業があり、規制法として電気通信事業法である。その中で情報の保護という点では、通信の秘密⁴⁵⁾が最も重要な規定である。しかし通信の秘密は第三者だけでなく電気通信事業者自体にも課せられている義務であり、義務違反の場合は事業者事態も処罰される⁴⁶⁾。そして事業者や個人によるエンフォースメントは規定されていない。

このように、パーソナルデータについて現行法は情報保有事業者に対して規制や罰則な

43) つまり、これは、①事業者よりも力が弱い個人の保護・救済論、②事業者は必ず事故を起こす（事業者性悪説）、という前提に基づくものである。

44) 個人情報保護法 20 条（安全管理措置）「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」

個人情報保護法 21 条（従業員の監督）「個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。」

個人情報保護法 22 条（委託先の監督）「個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。」

45) 電気通信事業法 3 条「電気通信事業者の取扱中に係る通信は、検閲してはならない。」

同 4 条 1 項「気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」

46) 電気通信事業法 179 条 1 項「電気通信事業者の取扱中に係る通信（第百六十四条第二項に規定する通信を含む。）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。」

どが課すことで、情報の事故による個人への被害発生を防ぐ事前構成となっている⁴⁷⁾。そして事業者はこれらの規制に沿って情報の管理を行っており、一定の効果は認められる。

しかし、不幸にも事故が生じた場合、すなわち事業者のエンフォースメントの効果はあまり期待できない⁴⁸⁾。しかしながら、大量に情報を保有する事業者であれば、経済力があり、かつ情報による利益を得ており、事故が生じたとしても自力による救済は可能であり、実際に個人情報事故のほとんどにおいて事業者が倒産等には至っていない。つまり事業者は経済的にも強者なのである。それに対して情報提供者たる個人のほとんどは事業者のような大きな経済力を有さず、事業者に比して経済的弱者と言える。しかし、多くの事故事例で同様の結果となっているが、ひとたび個人に対して何等かの被害が生ずる事故が発生した場合、当該事業者自体は法処分の対象とはなるが、事業者が個人を保護・救済するための事後的な法は構成されていないのである。さらに前項で説明したように、日本ではプライバシーに基づく議論が中心であるが、プライバシー権は人格権に基づくものであり、事業者が個人に代位してプライバシー権を行使することは出来ない。それ故、多くの事案で同様であるが、事業者による事後的措置は十分とは言えない⁴⁹⁾。

(2) 事業者による社会基盤整備の必要性

パーソナルデータについては利活用による高い産業イノベーション効果が期待されているにも関わらず、現行法をみるとデータ提供者である個人の保護は専らプライバシー論で論じられているが個人にとっては保護・救済効果が期待できず、データ保有事業者は自らが制裁を受けるものの個人を保護・救済する術を有していない。また、事業者も事故対応として事前の情報保護（安全管理）については法の義務として実施しているものの、事後的な救済施策については積極的に取り組んではいない。その結果、ビジネスとしてのパーソナルデータ利活用は、常に漠とした不安（自分のプライバシーや個人情報は大丈夫なのか）が生じ、利活用への障害ともなり得る⁵⁰⁾。

そのため現時点で求められる方法論としては、事業者による事後的な個人の保護・救済のための社会基盤の整備である。なぜならば、個人に係る情報は常に使用されており、立法による保護を待つ時間的余裕はなく、かつ、法に依拠せずとも個人を守ることはパーソ

47) この他、不正競争防止法も情報保護のための行為規制法であるが、個人情報以外の情報も対象としており、次項において検討を行う。

48) この点については文末「ケーススタディ」を参照のこと。

49) 例えば、先のケーススタディでは金銭的な損害賠償請求の訴えは個人から生じていないが、大手印刷事業者から情報が流出した個人に対して「お詫び」として一人当たり 500 円の金券を送付されたのみである。

50) 例えば、JR 東日本・Suica データ販売（2013）では、Suica の乗降履歴情報を個人と特定できない情報に加工して日立製作所へ販売したものであるが、利用者あるいは報道による批判を受け、最終的には販売を中止した。また、情報通信研究機構による大阪駅ビルでのカメラ撮影による個人を特定しない形での利用客動向実証実験（2014）はプライバシー侵害などの批判を受け、実験を中止した。

ナルデータを利活用して利益を得ている事業者の責務だからである⁵¹⁾。つまり個人に関する情報について事業者による事故が生じたのであれば、それが自らに起因するか、あるいは第三者による不正な行為によるかに係らず、事業者は情報提供者たる個人に対して責任を負う加害側となるからである。損害賠償に相当する金銭的補償については、裁判によらずとも事業者が迅速にかつ従前より高額で個人個人に対して補償するシステムを導入することで可能である。差し止めについてであるが、第三者の行為を民事的に制限する差し請求は現行法をみても例外的な法構成である。この点について、一つは金銭的補償による補完である。従前の損害賠償は、個人情報流出等による直接の損害に対する賠償であり、情報が流通することによる継続的潜在的な発生リスクに対する損害は認めていない。それを社会基盤として金銭的補償に置き換えることで個人個人の救済を図る。今一つは、情報の流通は主として情報ネットワークで生ずるため、ネットワーク上から情報を消去する日本版「忘れられる権利および消去する権利」⁵²⁾を確立する社会基盤の整備である。EU データ保護規則案 17 条で規定されている「データ主体に対し、自らに関する個人データを管理者に削除させる権利、及び、そのデータのさらなく拡散を管理者に停止させる権利」⁵³⁾のことである。同条は 9 項からなる条文であるが、1 項本文で「データの対象者には、以下のいずれかに該当する場合、特にその人物が子供のときに開示した個人データについて、その人物に関連する個人データの削除とそのデータの頒布の中止を管理者に実行させる権利がある。」⁵⁴⁾として個人の権利を、そして 2 項で「第 1 項で規定する管理者がその個人データを公開していた場合、そのデータを処理している第三者に対してデータの対象者が個人データのコピーまたは複写へのすべてのリンクを消去するよう要求している旨を通知するなど、管理者が責任を持つデータの公開に関して技術的手段を含むあらゆる合理的手段を管理者は取らなければならない。管理者が個人データの第三者による公開を認可していた場合、管理者はその公開について責任を負うものとみなされる。」⁵⁵⁾としてデータ管理者の義務を定めている。データ保護規則はまだ未成立であるが、この考え方に基づく社会基盤をパーソナルデータ事業者が整備するのである。

51) 事業者としての CSR (Corporate Social Responsibility) の立場からも、ステークホルダーを幅広く捉えて個人々々も対象とすることは社会的要請である。

52) “General Data Protection Regulation : Article 17 Right to be forgotten and to erasure”

53) 石井・前掲注 12) 70 頁。

54) “1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:”

55) “2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.”

パーソナルデータは法の整備よりも早い速度で利活用が進んでいる。事業者の責務として、個人を守るセーフティ・ネットとしての社会基盤を確立する必要がある。

4. 財産権としてのビッグデータの保護

(1) 知的財産法による保護

パーソナルデータのプライバシー論を検討してきたが、パーソナルデータとビッグデータは一致するものではなく、ビッグデータとしての領域がある。ここであらためて各々の領域について確認をすると、パーソナルデータは、個人に関する幅広い情報で⁵⁶⁾ データベースを構成するものである⁵⁷⁾。一方、ビッグデータは「既存の技術では管理するのが困難な大量のデータ群」⁵⁸⁾ とのように、IT の発展により可能となった想像を絶する量のデータである。量とはデータの規模としての量的側面およびデータの項目（内容）という質的側面の両面を指す。そして、ビッグデータの質的側面という点では、個人に関する情報だけでなく、個人とは無関係な情報（気象情報や宇宙の情報）も包含する。そして、ビッグデータは、特定の目的のために収集されあるいは編集・加工された集合データ（特定集合データ）および目的毎に編集・加工が可能となるために収集された集合データ（汎用集合データ）により構成される。

そしてビッグデータには、パーソナルデータとは関係のない情報も存在し、その領域では仮にビッグデータのための領域でもデータ流出等の事故が生ずれば、プライバシー問題は生じないものの、保有事業者あるいはデータ提供元に被害や損害が生ずるであろう。

では、ビッグデータの保護を如何に図るのか、パーソナルデータのプライバシー論とは異なり、これについての議論は積極的には行われていない⁵⁹⁾。しかし、パーソナルデータ領域以外のビッグデータでも高いイノベーション効果は期待されており、保護は必要である。それは、ビッグデータ自体の保護を図ることで客体に強い排他性を付与すること、あるいはビッグデータ利活用行為を保護することでビジネスを保護する方法が考えられる。しかし保護論が未整備であれば、事業者は利活用を躊躇するおそがある⁶⁰⁾。なぜならば、ビッグデータは容易に収集・管理・利用等ができるのではなく、相当のリソースを要し、

56) 例えば総務省の「パーソナルデータの利用・流通に関する研究会報告書」ではパーソナルデータを「個人識別性を有する「個人情報」に限定することなく、広く「個人に関する情報」と定義している。

57) 個人情報保護法2条6項では「個人データ」を「この法律において「個人データ」とは、個人情報データベース等を構成する個人情報をいう。」と定義しており、「情報」と「データ」を区別している。

58) 野村総合研究所『IT ロードマップ』（東洋経済新報社、2014年）44頁。

59) 例えば、パーソナルデータの議論は、民法（プライバシー）・行政法の研究者が主体であり、知的財産法の研究者は参加していない。

60) この点については、「日本がビッグデータ後進国になってもいいのか」としてYahoo! JAPANが問題提起（2014）をしたことがあり、内容は「政府の検討委員会にビッグデータを扱う事業者が呼ばれていない。これでは我々事業者の声が届かない。」と主張している。（http://www.huffingtonpost.jp/2014/01/21/bigdata-ahoo_n_4635623.html）と指摘している。

言わば事業者の努力の賜物である。したがってビッグデータ（あるいはビッグデータを利用するビジネス・スキーム）の保護が叶わないのであれば、期待されるイノベーション効果が期待できないのである。

そこで、パーソナルデータでのプライバシーという人格的利益の保護論ではなく、情報は知的財産である⁶¹⁾という財産権的利益の観点からの保護論を試みたい。つまり財産権の保有者である事業者の視点からの保護論であり、個人を保護するプライバシー論とは保護の主体が異なる。しかし、事業者としてビッグデータを構成する情報の収集・蓄積や管理、加工、編集、管理に係るリソース（費用、期間等）は、情報量の増大と共に飛躍的に増加するが、事故が生じた場合の対応費用も相当の額は必要であるため⁶²⁾、事業者の権利として何らかの保護が適わなければ、結局はビッグデータの保護も適わないのである。

ところで、プライバシー論と事業者の財産論とは別途独立したものではない。なぜならば、冒頭の図のように、ビッグデータとパーソナルデータは重複する部分がある、つまり事業者の責務としてパーソナルデータを保護する領域であり、事業者の権利としてビッグデータを保護する領域である。この義務と権利が交差する領域は、結果的にはそこに関連する個人を直接あるいは間接的に保護するという強い保護が期待できる領域となるのである。

（２）著作権法

ビッグデータをデータの集合体と捉えるのならば、データベースが考えられる。そして著作権法ではデータベースを保護の対象ともしている。すなわち著作権法12条の2では、「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。」としており、データベース自体は著作権法2条1項10号の3にて「データベース 論文、数値、図形その他の情報の集合物であつて、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。」と定義している。法の要件を具備して著作物として認められるデータベースには著作権による権利保護が可能なのである。

データベースの著作権に係る裁判事案としては、「タウンページデータベース事件」⁶³⁾で「タウンページデータベースの職業分類体系は、検索の利便性の観点から、個々の職業を分類し、これらを階層的に積み重ねることによって、全職業を網羅するように構成されたものであり、原告独自の工夫が施されたものであって、これに類するものが存するとは認

61) 例えば、「知的財産法は、ある種の情報の独占的利用を認める制度である」（中山信弘『財産的情報における保護制度の現状と将来』岩波講座「現代の法10」（岩波書店、1997年）275頁）との説明がある。

62) 2014年7月の大手教育事業者は事故対応費用として200億円以上を予定している。

63) 東京地判平成12年3月17日判例時報1714号128頁（タウンページデータベース事件）。原告の職業分類体系によって構成された電話番号情報のデータベースと職業別電話帳には、それぞれデータベースの著作権が認められるとして、被告の業種別データベースの差し止めおよび損害賠償を命じた事案。

められないから、そのような職業分類体系によって電話番号情報を職業別に分類したタウンページデータベースは、全体として、体系的な構成によって創作性を有するデータベースの著作物であるということが出来る」と判示している。タウンページデータベースとは、個人に関する情報でもある電話番号情報を基にしており、その情報量からみてパーソナルデータ領域に属するとも言えるかもしれないが、本事案においてデータベースの著作物として保護が認められたことは特筆すべきである。

しかしながら、ビッグデータがデータベースの著作物として認められるためには三つの課題がある。第一は、収集されたデータだけでは特定集合データであろうと汎用集合データであろうと「選択又は体系的な構成」がされておらず、データベースではないと考えられている。先の事案では、個々の職業に分類する前の電話番号情報はデータベースではない。第二は、収集したデータを編集・加工してデータベース化をしたとしても、すべてのデータベースが著作物として保護の対象となるものではない。「情報の選択又は体系的な構成」に「創作性」が認められなければならない。先の事案では「独自の工夫が施されたものであって、これに類するものが存するとは認められない」程度でなければならない。つまり IT のデータベースと著作権法のデータベースは一致しないのである。そして第三は、大量の情報が恒常的に収集・蓄積、あるいは編集・加工されることが多いビッグデータはナノ秒の単位で客体に変化するが、そのように情報量や内容が常に変化し一定とはならない客体を保護の対象として捉えられるかという点である⁶⁴⁾。

(3) 不正競争防止法

ある種の情報は「営業秘密」として不正競争防止法により保護がされている。すなわち不正競争防止法2条6項では「この法律において「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って、公然と知られていないものをいう。」として「情報」が営業秘密として認められる場合の定義をしている。そして不正競争防止法は著作権法のように権利付与法ではなく、2条1項4乃至9号にて営業秘密に係る6類型の不正競争行為を定義するという行為規制法である。つまりビッグデータが不正競争防止法により保護されるためには、営業秘密であることが求められる。

営業秘密の場合、データベースの著作物とは異なり創作性は求めている。法が求める要件は「秘密管理性」、「有用性」、「非公知性」の三要件と解釈されている。この三要件について、「秘密管理性」とは、当該情報を秘密として管理するという保有者の意思という主観的要素および客観的にみて秘密として管理していることが認められるという客観的要素から成る。客観的要素には具体的に「①当該情報にアクセスできる者が制限されていること（アクセス制限の存在）、②当該情報にアクセスした者に当該情報が秘密であること

64) この点については、特に差止請求の場合に差し止めの対象となる客体の特定が困難となり得る。

が認識できるようにされていること（客観的認識可能性の存在）」⁶⁵⁾と解説されている。そして経済産業省が公表している「営業秘密管理指針」⁶⁶⁾が具体的な管理方法の基準とも考えられている⁶⁷⁾。次に「有用性」は、当該情報が保有者の事業活動にとって有用であることで、直接、間接の益を問わない。例えば実験の失敗データのようなネガティブ・インフォメーションも「当該情報自身を利用して不必要な研究開発費用の投資を回避・節約できる等の意味で有用性が認められる場合」⁶⁸⁾と解説されている。そして、「非公知性」は、当該情報が「保有者の管理下以外には一般的に入手することができない状態にあること」⁶⁹⁾と解説されている。

では、ビッグデータがこの三要件を具備するかであるが、「有用性」については、「いわゆるビッグデータの収集・分析を可能とし、このことが、新産業・新サービスの創出や我が国を取り巻く諸課題の解決に大きく貢献するなど、これからの我が国発のイノベーション創出に寄与するものと期待されている。」⁷⁰⁾との指摘のように、ビッグデータには産業や事業に資する何らかの有用性が内在しているために利活用が積極的に議論されているのである⁷¹⁾。したがってビッグデータは有用性を具備すると考えられる⁷²⁾。

次に「非公知性」であるが、ビッグデータには種々様々な情報の集合体であるが、その情報のすべてが秘密情報とは限らない。報道されたニュースや地理的情報など、公知の情報も収集されて集合体をなす。しかし営業秘密の非公知性は、社会で誰も知らないという絶対的な秘密を求めているのではなく、社会一般には入手できない状態にある情報である。そのため「公知のデータベースからデータを集めたとしても、それに付加価値のある情報を加え、又は利用して、データベースとして再編し、これが部外者に漏洩しないよう厳重管理している場合は非公知である」⁷³⁾という、公知情報が含まれていても非公知となり得る判断がされる。したがってビッグデータは非公知性も具備すると考えられる。

問題は「秘密管理性」である。要件としては、法は保有者に対して秘密状態を維持する

65) 経済産業省知的財産政策室編『逐条解説不正競争防止法平成23・24年改正版』（有斐閣、2012年）41頁。

66) 不正競争防止法で営業秘密の保護を受けるために必要となる最低限の水準の対策を示すもので、平成15年に公表され、その後数度の改訂を経て、平成27年に全面改訂された。

67) 営業秘密管理指針による法運用形成については、川上正隆「秘密管理性判断における法運用形成過程の検討および問題提起」青山ビジネス・ローレビュー2巻1号（2012年）にて論じている。

68) 経産省・前掲注65)42頁。

69) 経産省・前掲注65)42頁。

70) 大綱・前掲注19)。

71) もちろん、ビッグデータの構成要素の中には事業に役立たない情報も存在するであろうが、そのような情報を含めて全体としてビッグデータが構成されているのであれば、当該情報はネガティブ・インフォメーションと考えることが出来る。

72) もっとも、事業には直接利用されないアリーステージのデータは司法判断として「有用性」は認められにくいと考えられる。この点については川上正隆「「営業秘密」と「業務上の有用情報」に係る法的課題の研究」青山ビジネス・ローレビュー4巻1号（2015年）にて論究している。

73) 金井重彦・山口三恵子・小倉秀夫『不正競争防止法コンメンタール改訂版』（LexisNexis、2014年）265頁。

ための管理を求めている。法が営業秘密を保護する根拠の一つは、保有者の管理努力とも言えよう。ところがビッグデータは、そもそも IT の発展により従来では想像しえない量の情報の集合体である。特に、事業者保有の単一サーバーではなく、クラウド⁷⁴⁾でデータを保有する場合、保有者として法が求める程度の管理が可能であろうか。そもそも直接の管理を前提としていないクラウドサービス⁷⁵⁾に対する管理性を求めるということは矛盾もしている。この点から考えると、ビッグデータはそもそも管理という概念をある意味で否定しているため、秘密管理性が認められにくいとも考えられる⁷⁶⁾。

このように検討を行うと、知的財産法の中である種の情報を保護することが期待できる著作権法あるいは不正競争防止法でもビッグデータの保護は十分ではない。それはビッグデータとパーソナルデータの交差領域の保護もまた十分ではないことを意味する。では交差領域に存する個人の保護のためにビッグデータの保護を如何に図るのか、次項であらためて検討を行いたい。

5. ビッグデータ保護の3ステップ

(1) 知的財産の保護領域

我が国では「知的財産」を法で定義している。すなわち知的財産基本法2条1項では「この法律で「知的財産」とは、発明、考案、植物の新品種、意匠、著作物その他の人間の創造的活動により生み出されるもの（発見又は解明がされた自然の法則又は現象であって、産業上の利用可能性があるものを含む。）、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営業秘密その他の事業活動に有用な技術上又は営業上の情報をいう。」として客体の定義している。さらにそれらの客体を保護する制度として、2条2項では「この法律で「知的財産権」とは、特許権、実用新案権、育成者権、意匠権、著作権、商標権その他の知的財産に関して法令により定められた権利又は法律上保護され

74) 「ネットワーク上にあるコンピュータを使って高度な処理を実現する技術であり、2006年頃から注目されるようになった。ネットワーク上にある複数のコンピュータ群が利用者の要求に応じて様々なコンピュータ処理を行うもので、利用者からはハードウェアを意識せずに使うことができる。クラウド（雲）の中身はわからなくても、そこから有益なサービスが降ってくるということをイメージして呼ばれるようになったと言われている。」（小向太郎『情報法入門第3版』（NTT出版、2015年）6頁）。

75) 例えば、AmazonのクラウドサービスAWS（Amazon Web Services）では、バージニア、オレゴン、カルフォルニア、サンパウロ、アイルランド、フランクフルト、シンガポール、シドニー、北京、東京にデータセンターを設置していると説明されている。他のクラウドサービスでも同様に世界にクラウドサーバーが点在しているが、グローバルに展開しているクラウドのインフラを一か国の法律で管理できるのかという問題がある。

76) この点については、営業秘密侵害に関する裁判事案でも、秘密管理性で営業秘密が否定されることも多く、例えば進行中であるが、大量の個人情報を持ち出したとされる大手教育事業者事件の刑事裁判でも、被告は情報の取得は認めたものの、スマートフォンを接続しただけで容易にデータ複製が可能であったことなどから、秘密として管理されたものではない、との主張をしている。

る利益に係る権利をいう。」と規定している。

この1項および2項の関係について表したのが次表である。

1 項	2 項	
	客体	保護法制
発明	特許権	特許法
考案	実用新案権	実用新案法
植物の新品種	育成者権	種苗法
意匠	意匠権	意匠法
著作物	著作権	著作権法
その他の人間の創造的活動により生み出されるもの EX. 半導体集積回路	回路配置利用権	半導体集積回路保護法
商標	商標権	商標法
商号	商号	商法、会社法
事業活動に用いられる商品又は役務を表示するもの	商品等表示	不正競争防止法
営業秘密	営業秘密	不正競争防止法
その他の事業活動に有用な技術上又は営業上の情報		

この表でわかるように、1項で定義された客体のほとんどは何等かの保護方法が法制度化されている。しかし、「その他の人間の創造的活動により生み出されるもの」および「事業活動に有用な技術上又は営業上の情報」は、抽象的に規定されている。このうち、例えば半導体集積回路の回路配置に関する法律（半導体集積回路保護法）2条1項にて「この法律において「半導体集積回路」とは、半導体材料若しくは絶縁材料の表面又は半導体材料の内部に、トランジスターその他の回路素子を生成させ、かつ、不可分の状態にした製品であつて、電子回路の機能を有するように設計したものをいう。」とあるようなものが人間の創造的活動により生み出されたと言えるが、収集・蓄積されただけのビッグデータは創造される前段階であり前者には属さないと思われる。ビッグデータはむしろ後者の「事業活動に有用な技術上又は営業上の情報」に該当すると思われる。知的財産の定義の最後にあるこの文言は、知的財産はある種の情報であるとの考えの基、具体的に定義した客体以外の客体を保護できる余地を残したものと考えられる。知的財産基本法が成立した2002年にはまだビッグデータという言葉は存在せず⁷⁷⁾、具体的な客体には含まれていないが、ビッグデータに期待される産業へのイノベーション効果という観点からみて、「事業活動に有用な技術上又は営業上の情報」に該当すると考えられるのである。

では「その他の情報」に客体としてビッグデータが含まれるとして、如何なる制度をもって保護をなすかである。

77) “Big Data”の言葉としての初出は2010年の英国エコノミスト誌とも言われている。

(2) ビッグデータ保護の3ステップ

①不法行為法による保護

知的財産基本法でみたとおり、具体的な客体の場合は特許法や不正競争防止法などの特別法による保護がされているが、特別法領域以外では汎用的な保護法制すなわち不法行為法（民法 709 条）による保護が考えられる⁷⁸⁾。

前項ではプライバシー論を論じ不法行為法による効果に疑問があることを論じている。しかし先の検討は個人という主体による不法行為のエンフォースメントである。ここで論じたいのは、知的財産たる客体であるビッグデータを保有する主体（事業者）を保護するための不法行為論である。したがって不法行為法としては同じであるが、エンフォースメントに対するアプローチが異なるのである。

知的財産法は不法行為法の特別法でもある。すなわち民法 709 条「故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う。」の条文中「他人の権利」とは特許権などの知的財産権も包含するのであり、知的財産権侵害の損害賠償は民法 709 条を根拠としている。そして「法律上保護される利益」が存すれば知的財産権ではない知的財産も民法 709 条の対象となりえる。

この点について旧民法 709 条では「故意又ハ過失ニ因リテ他人ノ権利ヲ侵害シタル者ハ之ニ因リテ生シタル損害ヲ賠償スル責ニ任ス」として保護対象は「他人ノ権利」と文言解釈上は限定しており、「桃中雲右衛門事件」⁷⁹⁾でもそのように判示した。しかしこの限定解釈は後の「大学湯事件」⁸⁰⁾にて拡大解釈され、その後、権利侵害要件は違法性と捉えられる解釈が法運用の通説となった。したがって旧法下でも直接の知的財産権侵害ではない、知的財産に対する侵害行為も不法行為法による保護が行われていた。現行法はその法運用の確認規定と言える。

不法行為法による知的財産の保護の事案としては、「木目化粧紙事件」⁸¹⁾、「自動車整備

78) 例えば、ドイツや中国の不正競争防止法には一般条項があるが、日本の不正競争防止法は限定行為のみであり、不法な行為に対する一般条項は民法 709 条しかない。

79) 大審院判大正 3 年 7 月 4 日刑録 20 輯 1360 頁（桃中雲右衛門事件）。判示は「蠟盤ニ吹込マシメタル楽曲ヲ他ノ蠟盤ニ写シ取りテ音譜ヲ製造シ利ヲ営ムコトノ正義ノ觀念ニ反スルハ論ヲ埃タサル所ナリト雖モ是レ独リ雲右衛門ノ演奏シタル楽曲ニ付キテ然ルニアラスシテ他ノ知名ノ音楽家ノ演奏シタル楽曲ニ付キテモ亦同一ノ弊害ヲ生スルヲ免カレス然レトモ之ニ関スル取締法ノ設ケナキ今日ニ在テハ之ヲ不問ニ付スル外他ニ途ナシトス」として、著作物性が否定された楽曲に対する侵害行為は権利侵害が成立しないため、これに対する特別法がなければ不問に付するしかない、としている。

80) 大審院判大正 14 年 11 月 28 日民集 4 巻 670 頁（大学湯事件）。判示は「侵害ノ対象ハ、売買ノ目的物タル所有権若ハ其ノ老舗ソノモノニ非ズ、得ベカリシ利益即是ナリ。斯ル利益ハ、吾人ノ法律觀念上、不法行為ニ基ク損害賠償請求権ヲ認ムルコトニ依リテ之ヲ保護スル必要アルモノナリ」として不法行為の対象を拡張し、得べかりし利益であるとした。

81) 東京高判平成 3 年 12 月 17 日判例時報 1418 号 120 頁（木目化粧紙事件）。家具の表面に貼付加工される木目化粧紙の原画を模倣した行為に対して著作権侵害および所有権侵害により差し止め及び損害賠償を求めた事案。

著作権法上の文芸、学術、美術又は音楽の範囲に属せず、著作物性を有しないとされた事案。

システム事件」⁸²⁾、「ライントピックス事件」⁸³⁾、「通勤大学法律コース事件」⁸⁴⁾ などがある。これらの事案は、いずれも著作権侵害を否定したうえで、知的財産を創造した先事業者の努力（法的保護に値する利益）を侵害する行為は不法行為である、というロジックで知的財産の保護を行っている。

この中で「自動車整備システム事件」は約6万件のデータベースに対する複製権侵害事件であり、ビッグデータ保護の参考ともなりえる事案である。対象は「自動車整備業者において、見積書、作業指示書、納品書等の作成が容易にできるほか、顧客や車両等に関する入力データをデータベース化し、顧客管理やダイレクトメールの発送等に活用できるように構成されたものであるが、日本国内において実在する四輪自動車に関する一定の情報を収録したデータベースである「諸元マスター」を構成要素として」おり、「自動車整備業用システムにおいて使用されるもので、自動車整備業を営む者に対し、実在の自動車に関する情報を提供する目的で作成された」原告のデータベースである。そして裁判所は三つの観点で原告データベースの創作性を否定し、つまり著作権法の保護対象ではないと判示した。まず、「対象となる自動車の選択について」は、「実在の自動車を選択した点については、国内の自動車整備業者向けに製造販売される自動車のデータベースにおいて、通常されるべき選択であって、本件データベースに特有のものとは認められないから、情報の選択に創作性があるとは認められない」と、自動車整備のためには実在の自動車を選択するのが当然であるとして創作性を否定した⁸⁵⁾。次に、「自動車に関するデータ項目の選択について」は、「自動車検査証に記載する必要のある項目と自動車の車種であるが、自動車整備業者用のシステムに用いられる自動車車検証の作成を支援するデータベースにおいて、これらのデータ項目は通常選択されるべき項目であると認められ、実際に、他業者のデータベースにおいてもこれらのデータ項目が選択されていることからすると、本件データベースが、データ項目の選択につき創作性

82) 東京地中間判平成13年5月25日判例時報1774号132頁（自動車整備システム事件）。

83) 知財高判平成17年10月6日裁判所HP判例検索システム（ライントピックス事件）。ホームページ上でニュース記事及び記事見出しを掲載している新聞社が、その見出し語句と同一の語句を使用している者に対し、記事見出しの無断複製が著作権侵害あるいは不法行為にあたるとして、差し止め及び損害賠償を求めた事案。

84) 知財高判平成18年3月15日裁判所HP判例検索システム（通勤大学法律コース事件）。出版社が、他出版社による法律問題解説書に対して自社出版物の著作権侵害および不法行為で差し止め及び損害賠償を求めた事案。

85) なお、原告はさらに「原告によるデータソースの評価や実在の自動車か否かの判断が反映されている点で、自動車の選択に創作性を有する」とも主張していたが、その点についても「実在の自動車か否かの検証に一定の評価や判断が伴うことは、実在の自動車か否かを確認するための情報の収集過程において一定の知的作業を要するというにとどまり、情報の選択の創作性を基礎付けるものではない。また、ダミーデータ及び代表データを収録している点は、原告が作出した架空のデータを収録したということにすぎないから、そのことが情報の選択の創作性を基礎付けることはない」として創作性が否定された。

を有するとは認められない」と、自動車整備に必要な項目を選択⁸⁶⁾したにすぎないとして創作性を否定した⁸⁷⁾。さらに、データの順番についても「他の業者の車両データベースにおいても、型式指定－類別区分番号の古い順に並べた構成を採用していることが認められるから、本件データベースの体系的な構成に創作性があるとは認められない」として創作性を否定したのである。そして以上の点から、「本件データベースは、データベースの著作物として創作性を有するとは認められない」と判示したのである。したがって原告の自動車整備データベースは著作物としては認められず、著作権による保護は受けられないのである。

一方、被告については、原告のデータベースの複製行為を認めたうえで、本件は旧民法下での事案であるが「民法709条にいう不法行為の成立要件としての権利侵害は、必ずしも厳密な法律上の具体的権利の侵害であることを要せず、法的保護に値する利益の侵害をもって足りるというべきである。そして、人が費用や労力をかけて情報を収集、整理することで、データベースを作成し、そのデータベースを製造販売することで営業活動を行っている場合において、そのデータベースのデータを複製して作成したデータベースを、その者の販売地域と競合する地域において販売する行為は、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である」として権利侵害ではなくても不法行為が成立する場合の存在を認めたうえで、まず、「本件データベースの開発に5億円以上、維持管理に年間4000万円もの費用を支出していることが認められる。」とデータベース開発に要した原告の負荷を認め、そして「原告と被告は、共に自動車整備業用システムを開発し、これを全国的に販売していたことが認められるから、自動車整備業用システムの販売につき競業関係にあり、証拠によると、実際に、富士モータースにおいて、従前は原告システムを導入していたものの、その後、被告システムに変更したことが認められる。また、被告は、上記認定のとおり、本件データベースの相当多数のデータをそのまま複製し、これを被告の車両データベースに組み込み、顧客に販売していた」という被告の行為に対して「被

86) 本事案の項目は「型式指定番号」、「類別区分番号」、「メーカー」、「車種」、「型式」、「種別」、「用途」、「車体形状」、「寸法」、「軸重」、「定員」、「最大積載量」、「車両重量」、「車両総重量」、「エンジン形式」、「総排気量」、「燃料」である。

87) なお、原告はデータ項目に関しさらに「メーカーや車種について、一般に使用されているものと異なる名称を用いていること」あるいは「上記データ項目の一部に原告独自のコード番号が付されている点」についても創作性を主張していたが、その点についても「すでに選択された車両の情報について、その車名や車種の名称として独自の名称を用いているというにすぎないから、情報の選択の創作性を基礎付けるものではない」あるいは「このコード番号は、すでに選択された情報に付された番号にすぎないから、情報の選択の創作性を基礎付けるものではない」として創作性が否定された。

また、数値データについても「各数値データが、参照した資料に記載された数値そのものではなく、原告によって検証されたデータである点において創作的な特徴を有すると主張するが、各データについて、正確な数値を収録しているからといって、それが、データの選択についての創作性を基礎付けるものではない」として、これについても創作性が否定された。

告が本件データベースのデータを被告データベースに組み込んだ上、販売した行為は、取引における公正かつ自由な競争として許される範囲を甚だしく逸脱し、法的保護に値する原告の営業活動を侵害するものとして不法行為を構成するといふべきである」として不法行為の成立を認めたのである。つまり、著作物としてのデータベースは否定（知的財産権を否定）したが、原告が努力して開発した自動車整備データベースという「情報の集合体」を知的財産として不法行為法により保護したと言える。

先のビッグデータの構成要素でみると、量的側面ではビッグデータではないが、質的側面からはビッグデータと同様であり、また、自動車整備に資するデータベースという点で特定集合データと言える。一方創作性の否定から、IT 的にはデータベースではあるが著作権法のデータベースではない。しかし、ビッグデータを収集・蓄積して管理をするためには、事業者として相当の努力（費用、期間、システムなど）が必要であり、現にその努力に対する侵害行為（ビッグデータの不正な持ち出しや悪意の流出など）が行われたために、不法行為の成立が認められたのである。

ビッグデータとパーソナルデータの交差領域は、財産権および人格権に基づく不法行為により、事業者および個人が法の保護を求めるが、損害賠償は認められるが、情報の流通を差し止めるという差止請求の成立が難しいという問題は解消されない。

②不法行為の特定化

不法行為により事業者がビッグデータを保護することは可能であるが、一般不法行為では保護客体が必ずしも明確ではないため、善意の事業者においても「予期せぬ侵害」に巻き込まれるおそれがあり、かえって事業への委縮効果を生じかねない。また、ビッグデータの保有事業者にしても、保護客体の要件が個別事案毎の判断となると客体の定常化が望めない。したがって不法行為による知的財産の保護には「その適用の前提事実と要件をできる限り明示してその射程距離の予測を可能とすべき」⁸⁸⁾との指摘は妥当である。そのため、利活用の委縮を生ずることなくビッグデータを不法行為法により保護するのであれば、ある種の不法行為を特定不法行為とする不法行為法の法運用による客體明確化の形成というステップが考えられる。

これについては、先に検討した「プライバシー権」のように司法による不法行為法の法運用で形成された権利構成がある。さらに知的財産領域でも「パブリシティ権」の権利構成がされた事案がある。パブリシティ権は専ら「顧客吸引力」に着目されているが、

88) 松村信夫『新・不正競争訴訟の法理と実務』（民事法研究会、2014年）849頁。

物のパブリシティ権については「ダービースタリオン事件」⁸⁹⁾にて否定されたものの、人のパブリシティ権については「ピンクレディ事件」⁹⁰⁾にて最高裁が「肖像等は、商品の販売等を促進する顧客吸引力を有する場合があります、このような顧客吸引力を排他的に利用する権利（以下「パブリシティ権」という。）は、肖像等それ自体の商業的価値に基づくものであるから、上記の人格権に由来する権利の一内容を構成するものということができる。他方、肖像等に顧客吸引力を有する者は、社会の耳目を集めるなどして、その肖像等を時事報道、論説、創作物等に使用されることもあるのであって、その使用を正当な表現行為等として受忍すべき場合もあるというべきである。そうすると、肖像等を無断で使用する行為は、〔1〕肖像等それ自体を独立して鑑賞の対象となる商品等として使用し、〔2〕商品等の差別化を図る目的で肖像等を商品等に付し、〔3〕肖像等を商品等の広告として使用するなど、専ら肖像等の有する顧客吸引力の利用を目的とするといえる場合に、パブリシティ権を侵害するものとして、不法行為法上違法となると解するのが相当である。」と判示した。

プライバシー権およびパブリシティ権はともに人格権に由来しているため、訴権は個人であり事業者ではない、つまり特定不法行為類型は人格権的保護の場合であり、物のパブリシティ権が否定されたように財産権的保護は認められず、事業者保護のための特定不法行為は構成されない、との考えも成り立つ。であればビッグデータは一般不法行為による保護は可能であるが、特定不法行為の形成は困難である。しかし「ダービースタリオン事件」は物のパブリシティ権は否定したものの、判示のとおり所有権と名称等使用との関係についての判断であり財産権を否定したものではない。また、「ピンクレディ事件」は「人格権に由来する」と判示しているが、同時に「顧客吸引力を排他的に利用する権利は、肖像等それ自体の商業的価値に基づくものである」とも判示しており、この点から本事案で判断された「人のパブリシティ権」は人格権のみならず財産権も根拠としている指摘もある⁹¹⁾。したがって、ビッグデータを事業者の保有する知的財産たる財産権として（パーソナルデータを包含する場合はデータ提供の個人の人格権も含め）保護するために、何等かの特定不法行為類型を構成する法運用は可能なのである。

89) 最高判平成16年2月13日裁判所時報1357号1頁（ダービースタリオン事件）。所有する競走馬の馬名等を使用したゲームソフトに対し、パブリシティ権侵害を主張して、ゲームソフトの製作、販売等の差し止めと損害賠償を求めた事案。「競走馬の名称等が顧客吸引力を有するとしても、物の無体物としての面の利用の一態様である競走馬の名称等の使用につき、法令等の根拠もなく競走馬の所有者に対し排他的な使用権等を認めることは相当ではなく、また、競走馬の名称等の無断利用行為に関する不法行為の成否については、違法とされる行為の範囲、態様等が法令等により明確になっているとはいえない現時点において、これを肯定することはできないものというべきである。したがって、本件において、差し止め又は不法行為の成立を肯定することはできない。」と判示した。

90) 最高判平成22年2月2日裁判所時報1549号1頁（ピンクレディ事件）。タレントの写真を無断で掲載した週刊誌に対し、当該タレントの肖像が有する顧客吸引力を排他的に使用する権利が侵害されたと主張して損害賠償を求めた事案。

91) この点については、「人格権と密接不可分な財産権説」（辰巳直彦『知的財産法 下』（青林書院、2013年）617頁）がある。

そしてビッグデータとパーソナルデータの交差領域では、財産権のみならず特に人格権に対する侵害回避のために差止請求が認められると考えられる。このように、事業者のビッグデータ利活用保護のエンフォースメントのために、特定不法行為類型化による法運用が期待される。

③立法論による保護

現行法解釈でビッグデータの保護を行うのであれば特定不法行為類型化が望まれる。しかし、特定不法行為の判断基準や客体の定義など、法運用形成には新解釈の構成と判例の蓄積という期間を要する。そのため、解釈論の次のステップは立法論による保護となる。

もちろん、問題解決のための安易な立法論は避けるのが当然ではある。しかしビッグデータは現行法制定時には存在しなかった（立法者の予想範囲を超えた）新しい概念であり、立法による保護をしようとしたらどのような方法が考えられるのか、その方向性の検討を試みたい。

ビッグデータを保護する方法としては、「客体の直接的保護」と「客体の間接的保護」が考えられる。直接的保護とは、客体を権利化することにより排他権や請求権を付与する方法で、特許権による保護という特許法の類型である。間接的保護とは、客体の創造や利活用といった客体の動きを保護する方法で、不正競争防止法による行為規制類型である。

直接的保護であるが、ビッグデータの要件を定義し権利化が出来れば、独占的排他権を有した強い客体として事業者は安心して利活用が叶う。しかし直接的保護には少なくとも二つの問題がある。一つは、ビッグデータは汎用性をもった膨大な量の情報集合体であり、そのような汎用性をも単一の事業者に独占させるとすれば、より大量の情報を有する事業者のみしか保護がされず、期待される産業界におけるビッグデータ・イノベーションは生じない。二に、恒常的に変化する情報の集合体は定常化とは程遠い存在であり、形式的定義はできたとしても、客体の実質的明確化が不可能であり、第三者は常に「定常化しない情報に対する予期せぬ侵害」に怯えることとなる。したがって、ビッグデータの権利化という立法方向性は困難である。

間接的保護であるが、ビッグデータを活用したビジネス・スキームは、現行法すなわち特許法（ITを利用した発明）や著作権法（プログラム）による保護が可能である。保護が求められるのはむしろデータの収集・蓄積時であろう。データを収集し、クラウドなどで蓄積する場合、そこに発明のような新規性・進歩性のある技術は使用されることもあるが、多くは既存のIT、特に情報管理に必須であるセキュリティ技術を組み合わせることで効率的なシステムを構築するであろう。しかし、ハッキング等の外部からのサイバー攻撃に備え、システム構成の主要部分は外部とは遮断して容易には分からないよう

にしている⁹²⁾。ビッグデータのように大量の情報を収集・蓄積する事業者にとっては、システム構成がリソースがかかる重要な部分とも言える。この点に着目し、事業者が努力して構成したシステム（特許性はないが）が創造した（収集した）成果物（ビッグデータ）を保護する方法である。ITでのデータ保護には例えば不正アクセス禁止法がある。システムへの不正アクセスを抑制することで、不正取得や改ざんからシステム内のデータの保護している。しかし法の射程は「不正アクセス行為」であり、不正アクセスにより流出したデータあるいはデータを利用したビジネスは他法による保護が必要である。また同法のエンフォースメント刑事罰のみであり事業者による直接のエンフォースメント（民事的請求措置）は行えない。半導体集積回路の回路配置に関する法律（半導体集積回路保護法）では、半導体の心臓部でもある集積回路⁹³⁾の回路配置⁹⁴⁾に対して独占的な回路配置利用権⁹⁵⁾を付与することで、他者による同様の回路利用による半導体品製造⁹⁶⁾を抑制する間接的手法である。そこで、このような既存法の保護論を組み合わせることで、ビッグデータの間接保護を図る方法論である。概念的には、事業者が構成するシステムにある程度の構成力が認められるのであれば、当該システムに対して権利を付与することで、そのシステムにより集積されたビッグデータを間接的に保護するものである。もちろん、直接的保護と同様に汎用性が高いビッグデータの独占問題がある。しかし、ビッグデータに対して直接の権利を付与するのではなく、集積のためのITシステムへの権利付与であり、異なるITシステム（集積方法）であれば同様のビッグデータの並存が可能である。また、既存技術を組み合わせることから、ITシステム設計が重畳する場合もあるが、事業者が独自開発したITシステムであれば権利は及ばない⁹⁷⁾とすることで、ITシステムの同一類似リスクを回避できる。

ビッグデータとパーソルデータの交差領域の点では、財産権としてのITシステム保護のみならず、プライバシー保護の潮流たるプライバシー・バイ・デザインは「ITシステムのデザインにプライバシー保護が組み込まれること」との原則が示すように、ITシステムに親和性がある概念であり、プライバシー・バイ・デザインに基づくITシ

92) 例えば、外部ネットワーク経由で情報を収集するのであれば、外部環境との接続インターフェイスを設置せざるを得ないが、管理などのホスト側と外部環境は切り離して直接接続を出来ないようにすること（DMZ）は当然である。

93) 半導体集積回路保護法2条1項「この法律において「半導体集積回路」とは、半導体材料若しくは絶縁材料の表面又は半導体材料の内部に、トランジスタその他の回路素子を生成させ、かつ、不可分の状態にした製品であつて、電子回路の機能を有するように設計したものをいう。」

94) 半導体集積回路保護法2条2項「この法律において「回路配置」とは、半導体集積回路における回路素子及びこれらを接続する導線の配置をいう。」

95) 半導体集積回路保護法11条前文「回路配置利用権者は、業として設定登録を受けている回路配置（以下「登録回路配置」という。）を利用する権利を専有する。」

96) 半導体集積回路保護法2条3項「この法律において回路配置について「利用」とは、次に掲げる行為をいう。一 その回路配置を用いて半導体集積回路を製造する行為」

97) 半導体集積回路保護法12条1項では「回路配置利用権の効力は、他人が創作した回路配置の利用には、及ばない。」としており、回路配置利用権は絶対権ではなく相対権である。

システムの設計により、プライバシーという人格権も保護が可能となる。

結語

パーソナルデータの保護、その領域に関係する個人あるいはプライバシーの保護について、従来あまり議論がされていないビッグデータの側面から保護制度の検討を行ってきた。そして法運用などにより交差領域の効果的な保護が期待できる。

一方、個人情報保護法の改正および法運用のためのガイドラインの改正が未成立なため、パーソナルデータの定義および具体的内容が現時点では明確ではない。しかし改正法関連が成立すれば、パーソナルデータ領域とビッグデータ領域の交差領域あるいは交差しないビッグデータのための領域が明確となるであろう。そこで次の段階として、各々の領域に属する情報の性格や定義の検討を行い、保護制度の精緻を行うものである。

〈ケーススタディ〉

本文中では、個人情報の事故が発生しても事業者によるエンフォースメントは期待できないと説明をした。事業者による大量の個人情報流出事故は幾度か生じており、2014年の大手教育事業者による事故、2015年の年金事業者による事故などは記憶に新しい。そこで、ケーススタディとして事業者が保有する個人に係る情報で事故が生じた場合、法がどのように動き個人はどのような救済を受けたのか、実際の事案を振り返ってみる。

大手教育事業者や年金事業者の事故は進行中で結論が出ていないため他事案での検討となるが、類似事案として大手印刷事業者の個人情報流出事故がある。委託先元従業員による約863万件の個人情報という、大手教育事業者の事故以前としては国内最大規模の情報流出事故である⁹⁸⁾。

経緯として、当該委託先元従業員は2007年2月1日に幫助罪で逮捕された。インターネット通販詐欺グループに顧客情報という個人情報を売却したことに基づくものである。その後、27日に窃盗罪で再逮捕されている。MOディスクに個人情報のデータファイルを記録（複写）して自宅に持ち帰ったが、そのMOディスクは大手印刷事業者の管理物であり、それを無断で持ち出したというMOディスクの窃盗行為である。そして3月13日に窃盗罪により起訴された。被害はMOディスク1枚（250円相当）である。東京地方裁判所八王子支部で4月27日に初公判が開かれ、10月31日に懲役2年、執行猶予5年の判決が下り、事件としてはこれで終焉した。

98) 大手印刷事業者が販促用ダイレクトメールのために各社から預かっていた個人情報が、業務委託先の社員により持ち出され、その一部が売却された事件。持ち出した理由は、業務を自宅で行うためであったが、契約終了の約1年後、金銭的貧窮のために自宅にあった情報を売却したものである。持ち出された個人情報は43社分、計863万7405件とされている。

この事案に関して考えられる法適用について、まず刑事から検討する。当該委託先元従業員は再逮捕容疑の窃盗罪で起訴されたが、幫助罪では起訴されておらず、その理由は公表されていない。考えられる理由として、当該詐欺グループは当該顧客情報の取得以前から詐欺を行っており当該顧客情報の有無に係らずその後も詐欺を行っていたことから、幫助が成立しにくいと判断したのではないか⁹⁹⁾。委託先元従業員は、委託業務で顧客情報を取り扱っており、その情報を無断で家に持ち帰り売却したという点で、背任あるいは業務上横領も考えられるが本件では適用されていない¹⁰⁰⁾。

個人情報保護法にも刑事罰があるが、法は事業者規制法であり、本件では大手印刷事業者が法の対象となり委託先元従業員ではない。

サーバーで管理されていた情報（データベース）を持ち出したという点では、不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）考えられるが、委託先元従業員は、委託期間中に当該サーバーおよび顧客データベースに対して正当なアクセス権を有しており、不正にアクセスしたものではないので、本法は適用されない¹⁰¹⁾。

不正競争防止法では営業秘密という情報に対する侵害行為類型を刑事罰として規定している。本件では民事も含めて本法が適用されていない。サーバーで管理されていた顧客データベースが営業秘密であることが必要であるが、当時の報道から考えるに、委託先元従業員が有していたアクセス権の認証方法、すなわち ID およびパスワードについて、ID は複数の者が共有で使用していたうえ、委託先元従業員が契約解除後も本人のアクセス権を削除せず、またパスワードも長期にわたり変更していなかった、つまり委託先元従業員は契約解除後もサーバーおよび顧客データベースに対するアクセス権を有していたという点から、営業秘密の要件の一つである事業者による「秘密管理性」¹⁰²⁾が充足しないと考えられたと思われる。

民事、つまり事業者による直接のエンフォースメントであるが、本件は行為としては不

99) 幫助は、「道具や場所を与えるなどの有形的な形態のもののみならず、犯罪に関する情報を提供したり」（前田雅英『刑法総論講義第3版』（東京大学出版、1998年）434頁）とあり、本件のような顧客情報の提供でも幫助行為となり得る。そして、「正犯に物的・精神的な援助・支援を与えることにより、その構成要件該当行為の遂行を促進し、さらには構成要件該事実の惹起を促進すること」（山口厚『刑法』（有斐閣、2006年）159頁）との説明があるが、本件では詐欺グループは正犯である通販詐欺を従前より実行しており、本件顧客情報の提供により詐欺の実行が促進されたとは必ずしも言い切れず、詐欺に対する幫助罪の起訴を見送ったと考えられる。

100) 推測であるが、背任については、情報持ち出し理由が自宅での業務遂行のためであり背任には成立しにくい、業務上横領については、情報窃盗罪が無いのと同様、持ち出したのは複製データで元データ自体は大手印刷会社にあるため横領が成立しにくい、と考えられる。

101) 仮に適用されたとしても、不正アクセス禁止法はシステム等への不正アクセスを行っただけで、つまりデータの不正取得や改ざん等を行わなくても、不正アクセス行為自体を刑事罰に処す法制度である。実行者に対する刑事罰という点でけん制効果は期待できるが、民事的規定はないため、被害を受けた事業者が個人による直接のエンフォースメントは望めない。

102) 大手教育事業者の裁判で被告側は、データベースへのアクセス ID が他の従業員と共同だった点や、スマートフォンを業務用パソコンに接続することでデータが容易に複製できた点などを挙げて、秘密管理性の主張している。

正競争防止法2条1項7号の営業秘密に係る不正競争行為に該当する¹⁰³⁾が、本法は適用されていない。先に挙げた理由により、そもそも当該顧客情報が営業秘密ではないと判断される可能性があるためであろう。そのため不正競争防止法による損害賠償請求および差止請求は行えない。

営業秘密に該当しないとしても、不法行為あるいは契約期間中の債務不履行による損害賠償の請求が可能である。そして本件で大手印刷事業者は事故対応に数十億円を要したとも言われており¹⁰⁴⁾、相当の損害が生じたことは確かである。しかし損害を被った大手印刷事業者は損害賠償請求の民事訴訟を提起していない。おそらくは、委託先元従業員が顧客情報を売却したという動機は生活費に困窮したための金銭目的であり、そのような者に対して損害賠償を請求しても、そもそも回収の期待が出来ず、裁判費用がかかるだけであるため提起しなかったのであろう。次に、情報の流出を差し止める、つまり情報の流出による二次被害、三次被害の防止であるが、本件でみると、約863万件の個人情報の大多数は第三者に流通しておらず、すべて委託先元従業員の家から回収された。また、詐欺グループに売却された約15万件についても詐欺グループの逮捕に伴い押収された。しかし、仮に第三者に流通していた場合、事業者が直接に個人情報の流通を差し止める術はなかった¹⁰⁵⁾。委託先元従業員に対しては債務不履行に伴う履行の強制により事実上個人情報の使用を差し止めることも可能であるが、流通した個人情報を善意に取得した第三者に対しては債務不履行に基づく履行強制は請求できない。第三者に対しては不法行為に基づく請求しかできないが、原則は損害賠償請求のみであり、2-(2)で説明したとおり、差止請求が認められるのは極めて限定的である。しかも事業者はプライバシー権あるいはパブリシティ権に基づく訴権を有しておらず、したがって本件にかぎらず、同様の事案においても情報の流通に対する事業者による差し止めは行われていない。

このように、本件は当時としては我が国最大の個人情報流出事故であったが、MOディスク1枚の窃盗罪という法運用だけに留まったと考えられる¹⁰⁶⁾。

103) 不正競争防止法2条1項7号「営業秘密を保有する事業者（以下「保有者」という。）からその営業秘密を示された場合において、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密を使用し、又は開示する行為」。保有者より正当に営業秘密を開示されたのち、事後的に図利加害目的で当該営業秘密を使用する行為。

104) 個人情報流出事故が発生した場合、情報が流出した個人に対する損害賠償額は極めて低いことは前述のとおりである。事故の対応として多大な費用が生ずる要因として、郵送料、お詫びの金品、新聞広告、コールセンター等がある。

105) 例えば、大手教育事業者の事故では名簿業者に流通した個人情報の差し止めや回収は行われていない。

106) 営業秘密の不正取得行為等には不正競争防止法で刑事罰規定があるが、そもそも「情報（営業秘密にかぎらず）」の窃取等の罪、すなわち「情報窃盗罪」は我が国では規定されておらず、情報を記録した媒体（デジタル機器や印刷物）に対する行為との構成にならざるを得ない。