〈原著論文〉

ビッグデータ時代におけるプライバシー
――カナダを中心として――

竹　井　　潔

抄　録

ICT（情報通信技術）の急速な進展に伴い，ビッグデータがネット上で生成・収集・蓄積し流通している。ユビキタスネットワークでさまざまなデバイスやセンサーによりリアルタイムにデータが自動収集され，膨大なデジタルデータが生成されている時代となった。ビッグデータを資源として利活用していくことが期待され，社会的価値の創出として注目されている。しかし，一方プライバシー保護の問題を避けて通ることはできない。本稿では，プライバシーの諸概念を確認し，ビッグデータ時代におけるプライバシーの保護について，主にその先進国であるカナダのプライバシーなどを中心に検討を行う。

キーワード：プライバシーの保護，プライバシー法，PIPED 法，OECD プライバシーガイドライン，ビッグデータ，プライバシー・コミッショナー，プライバシー・バイ・デザイン（PbD），プライバシー影響評価（PIA）

1. はじめに

情報通信技術（ICT）の急速な進展に伴い，膨大なデジタルデータがネット上で生成・収集・蓄積し流通している。2013 年はビッグデータ元年といわれているが，まさにこの数年でビッグデータ時代に突入した感がある。ユビキタスネットワークでさまざまなデバイスやセンサーによりリアルタイムにデータが自動収集され，膨大なデジタルデータが生成されている時代となった。このようなビッグデータを資源として利活用していくことが，新たなビジネスの創出や社会的な問題解決への糸口として期待され，社会的価値の創出として注目されている。データの情報収集から活用するまでのプロセスは，自動処理されるものから，個人個人が端末で発信する Facebook やツイート等の SNS や，ネットにおける検索キーワード，位置情報等のライフログも対象となる。構造化データや非構造化データを問わず，あらゆるデータが対象となる。村田・折戸が「捨てることなく蓄積

政治経済学部・政治経済学科　論文受理日 2015 年 7 月 8 日

される多種多様かつ大量の個人情報を利用した，パーソナルマーケティングから個別医療に至るまでの，さまざまなパーソナライズドサービスの有効かつ効率的な提供は，ビッグデータサービスの枢要な地位を占めるものとして認識されている。」[1] と述べているように，大量のパーソナルデータからなるビッグデータの利活用はビジネス機会を創出し，個人へのサービス向上や利便性を高めることに寄与すると考えられる。しかし，一方で大量のパーソナルデータを利用することはプライバシーの問題を避けて通ることはできない。

2. ビッグデータ時代

総務省の『情報通信白書 平成 26 年度版』によると，2012 年時点のデータ流通量は約 2.0 エクサバイトであったが，2013 年は 13.5 エクサバイトが見込まれている。また，国際的なデータ流通量は 2011 年の約 1.8 ゼタバイトから 2020 年には約 40 ゼタバイトに達するとしている[2]。このように，データ流通量は飛躍的に増加してビッグデータ時代となってきた。

ビッグデータの定義については，まだ確立されたものがないが，ビッグデータは，「既存の一般的な技術では管理するのが困難な大量のデータ群」[3]（城田）のことを示す。ビクター・マイヤー＝ションーンベルガーは，ビッグデータを「小規模ではなしえないことを大きな規模で実行し，新たな知の抽出や価値の創出によって，市場，組織，さらには市民と政府の関係などを変えること」[4] と捉えている。

また，『情報通信白書 平成 24 年度版』では，ビッグデータを「事業に役立つ知見を導出するためのデータ」とし，「ビッグデータを用いて社会･経済の問題解決や，業務の付加価値向上を行う，あるいは支援する事業」[5] と目的的な定義が述べられている。

ビッグデータを活用することの意義は，「ICT の進展に伴い多種多量なデータの生成・収集・蓄積等がリアルタイムで行うことが可能となり，そのようなデータを分析することで未来の予測や異変の察知等を行い，利用者個々のニーズに即したサービスの提供，業務運営の効率化や新産業の創出等が可能となっている点」[6] にある。

政府は 2013 年 6 月に成長戦略の柱に据える IT 活用の一環としてビッグデータの活用を挙げている。2013 年「世界最先端 IT 国家創造宣言」において，「「情報資源」の活用こそが経済成長をもたらす鍵となり，課題解決にもつながる」[7] として，ビッグデータなどの活用により，新たな付加価値を創造していく必要性があることを提言した。

『情報通信白書 平成 24 年度版』では，ビッグデータの活用における個人情報の問題について，「個人に関するデータの取扱いをめぐる問題など実社会への適用において生じる制度的課題，技術開発の進展状況等に関する国際的な動向を踏まえつつ技術的課題の解決に取り組むことが求められている」[8] としている。そして，「個人情報等にも配慮しつつ，M2M 等のセンサーネットワーク等を通

じて生成・収集等される多種多量のデータについて，社会全体で共有可能な知識や情報の創発が促進されるよう蓄積・公開・流通・連携等させることを通じ，分野横断的かつリアルタイムに解析等利活用して，社会的課題の解決や経済の活性化を実現することも重要である。」[9]と述べられている。

2013年にJR東日本が年齢，性別，乗降駅などICカード乗車券の利用データを他社に提供して個人情報の扱いについての批判を招いたことは記憶に新しい。ビッグデータを活用していく上で個人情報の取り扱いを十分配慮し，個人情報やプライバシーの保護をしていくためのルールやガイドラインの見直しが求められている。

3. プライバシーの権利の概念

プライバシーとは何か，プライバシーの権利について諸説があるが，いまだ明確な定義はない。プライバシー権が普及して世に認知されるようになったのは，ウォーレンとブランダイス（S. D. Warren & L. D. Brandeis）による有名な論文「プライバシーの権利（*The right to privacy*, 1890）」において，「一人で放っておいてもらう権利（the right to be let alone）」と定義されたことによる。ここでは，生活の権利として，「生活を楽しむ権利」，「自由･安全な権利」，そして「放っておいてもらう権利」が述べられている[10]。しかし，「一人で放っておいてもらう権利」だけではプライバシーの権利をとらえきれない状況が生じ，「自己に関する情報をコントロールする権利」としてプライバシーの権利をとらえることが通説となってきている。

以下，プライバシーの権利の概念について，いくつかとりあげて特徴を見ておきたい。

(1) Whalen v. Roeは，合衆国最高裁判所においてプライバシーの権利を包括的にとらえ，「一つは，私的事柄を開示されないということに対する個人の利益であり，もう一つは，一定種類の重要な決定を独立に行うことができるということに対する利益である」[11]と指摘した。ここにプライバシーの権利が，「私的事柄を開示されないということに対する個人の利益」（情報プライバシー権）と「一定種類の重要な決定を独立に行うことができるということに対する利益」（人格的自律権）とを包括するものであることが明示された。

(2) 佐藤は，プライバシーの権利の概念として，以下のような特徴を指摘する[12]。

1)「プライバシーの権利」は「貧欲の権利」といわれるように，単一の包括的な定義は不能であると主張される。

2)「プライバシーの権利」の古典的定義は，「ひとりで居させてもらいたい」という把握である。この定義に関して，①自由一般ないし権利一般の意味合いをもち，広汎に失する。②「一人で居させてもらえない」場合ではあるが，プライバシーの侵害とは言えない場合が多々考えられる。③消極的な響きを持ちすぎるなどが指摘される。

3）人間の尊厳の一局面論として「プライバシーの権利」を把握する。広汎すぎ，「権利」として提示するには明確性を欠いている。

4）高度に個人的ないし親密な決定に対する公権力による干渉からの自由としてとらえる。個人が自己に関する事柄を公権力から干渉されることなくどこまで自由に決定できるかは，個人の「行為の自由」に関する重要事項であるが，この問題を「プライバシーの権利」の問題とすることは，その問題の真の性質を曖昧ならしめる危険があるとともに「プライバシーの権利」を曖昧なものとする危険がある。

5）「静穏のプライバシー」の意味に解する説。「静穏のプライバシー」は，静穏を乱しあるいは神経を刺激するものからの自由のこと。具体的には，訪問販売，いりもしない郵便，いわゆる“捕らわれの聴衆”，騒音や悪臭などの問題が指摘される。これらの問題をもってプライバシーの権利の問題とするのは，該権利を不当に曖昧ならしめることにならないかの疑問をぬぐいきれない。

また，佐藤は「プライバシーの権利」の構造と存在理由について，Gross を取り上げている。

（3）Hyman Gross は，論文“*The Concept of Privacy*”（1967）[13] においてプライバシーの「強い意味」と「弱い意味」とを区別すべきことを提唱し，「強い意味においては，同意語を持たず，侵犯者が人の私的事柄を知るようになる侵入（intrusions）または侵犯者が自分の知っている人の私的事項を他者に知らせる開示（disclosures）であるとし，弱い意味においては，同意語をもち，精神的平穏，独居，人格的自律といったものがそれにあたる」[14] とした。

Gross は，プライバシーとは，「人と知り合うことまたはその人にとって個人的な生活事項を知ることが制限されている，人間生活の状態」，「自己の個人的な事項の享受をわかち合うことにつきコントロールが及んでいる状態」という。この Gross の定義は多くの論者によって捉えられることとなった[15]。

（4）Daniel J. Solove はプライバシーの概念について 6 つの型に分類している。

「①放っておいてもらう権利（the right to be alone）②自己への限定的アクセス（limited access to the self）―他者からの望まないアクセスから自己を保護する能力③秘密（secrecy）―ある種の事柄の他者からの秘匿化④自己情報のコントロール（control over personal information）―自己に関する情報に対するコントロールの行使能力⑤人格性（personhood）―ある人のパーソナリティや個性 / 個別性，尊厳の保護⑥親密性（intimacy）―ある人の親密な関係や人生の奥深い部分にかかわる諸側面についてのコントロールやそれらへの限定的アクセス。」[16] これらは，オーバーラップするものの，それぞれプライバシーに関する特有の視点があるとダニエルは述べている。

また，ダニエルは，プライバシーを 4 つのグループに分けプライバシー類型論（Taxonomy of Privacy）を論じている。この類型論は，データ主体（直接影響を受ける個人）に対してプライバシー

侵害を引き起こす様々な種類の活動に基づいている。ダニエルによるプライバシー類型論は，(1) 情報収集，(2) 情報処理，(3) 情報拡散，(4) 侵襲の 4 つのグループに分けた，プライバシーの問題を生じさせる以下の諸活動から構成される[17]。

1. 情報収集（Information collection）
   - 監視（Surveillance）：個人活動の観察・聴取・記録
   - 尋問（Interrogation）：さまざまな形態からなる情報の質問や徹底調査
2. 情報処理（Information processing）
   - 集約（Aggregation）：個人についての様々なデータの結合
   - 同定（Identification）：特定個人への情報の関連づけ
   - 非セキュリティ状態（Insecurity）：蓄積された情報を機密漏洩や不正アクセスから保護する際の不注意
   - 二次利用（Secondary use）：データ主体の同意なしに，収集時とは別の目的で収集データを利用すること
   - 排除（Exclusion）：データ主体の個人が，他者が保有する個人データが得られないことや，そのデータの取り扱いや利用に参加できないこと
3. 情報拡散（Information dissemination）
   - 守秘義務関係破壊（Breach of confidentiality）：個人情報を守秘するという約束を破ること
   - 開示（Disclosure）：他者が個人の評判を判断する仕方に影響を与えるその人物に関する真実の情報を明かすこと
   - 暴露（Exposure）：他者の裸体や悲観，あるいは身体的機能を暴露すること
   - アクセス可能性の増大（Increased accessibility）：情報のアクセス可能性を増幅すること
   - 脅迫（Blackmail）：個人情報を開示するという脅迫
   - 流用・盗用（Appropriation）：データ主体のアイデンティティを他の人物の目的や利益のために利用すること
   - 歪曲（Distortion）：個人についての虚偽の，もしくは誤解を招く情報を拡散すること
4. 侵襲（Invasion）
   - 侵入（Intrusion）：静穏または独居を妨げる侵入行為
   - 意思決定への介入（Decisional interference）：データ主体にかかわるプライベートな事柄への意思決定に立ち入ること

ダニエルは，データ主体となる個人に対してプライバシーの問題が発している活動，あるいはプライバシーの問題が発生する可能性のある活動に焦点を当てて，プライバシーの多元的な側面を示している。

4. 日本の個人情報保護法について

日本は，国レベルで 1988 年に「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が制定され，2003 年に個人情報保護法が制定された。個人情報保護法は OECD のプライバシーガイドラインを基調にして作成されている。

総務省では 2012 年 11 月より「パーソナルデータの利用・流通に関する研究会」[18] を開催し，個人情報やプライバシー保護に配慮したパーソナルデータの利活用の方策について検討を開始した。ルールを明確化した上で，個人情報保護ガイドラインの見直し，同意取得手続の標準化等の取り組みを推進するほか，番号制度における「特定個人情報保護委員会」の機能・権限の拡張などの整理を踏まえた第三者機関（プライバシー・コミッショナー）の体制整備，個人データを加工して個人が特定される可能性を低減したデータの個人情報及びプライバシー保護への影響に留意した取扱いなどを含む「パーソナルデータの利活用に関する見直し方針」[19] を提言している。

2015 年 6 月 24 日高度情報通信ネットワーク社会推進戦略本部の「パーソナルデータの利活用に関する制度改正大綱」[20] が報告された。大綱は，パーソナルデータを積極的に活用するために適切なルールを整備し，その結果として我が国の産業振興や国際競争力の強化に役立てることを目的に検討された結果報告である。

個人情報保護法の改正に向けての取り組みが検討されてから政府は 2015 年 3 月 10 日，個人情報保護法の改正案を閣議決定した[21]。それまで，利用目的に本人の同意が求められる第三者提供等を本人の同意がなくても行うことを可能とする枠組み（オプトアウト方式）を導入することが検討されていたが，改正案ではオプトアウト方式の導入は見送られた。改正案で特徴的なのは，匿名加工情報の扱い方を定めたり個人情報保護委員会の設置などである。

5. プライバシーの潮流

世界における最近のプライバシーの潮流としては，30 数年ぶりの OECD プライバシーガイドラインの改正や，EU データ保護規則の「忘れられる権利」の概念やアメリカの「消費者プライバシー権利章典」等があげられる。

(1) OECD プライバシーガイドライン

OECD（経済開発機構）は，1978 年から国境を超えるデータの流れおよび個人データとプライバシーの保護について検討がなされ，1980 年 9 月 23 日に「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会勧告」(Recommendation of the Council of concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data)[22] を制定した。ガイドラインではプライバシー保護と個人データの国際流通に関する必要事項を定めて「OECD プライバシー 8 原則」（①収集制限の原則，②データ内容の原則，③目的明確化の原則，④利用制限の原則，⑤安全保護措置の原則，⑥公開の原則，⑦個人参加の原則，⑧責任の原則）を明示した。堀部によると OECD プライバシー 8 原則は，アメリカの 1974 年プライバシー法（「アメリカの 8 原則」①公開の原則②個人アクセスの原則③個人参加の原則④収集制限の原則⑤使用制限の原則⑥提供制限の原則⑦情報管理の原則⑧責任の原則）がモデルとなった[23]。

OECD プライバシーガイドラインは国際的なプライバシー保護と個人データの国際流通についての世界で初めての国際的合意である。ガイドラインはプライバシー保護への取り組みについて，各国がプライバシー保護制度の整備をしていく際に参照されるデファクトスタンダードとしての役割を果たしている。ガイドラインでは，OECD 加盟国に対し，「ガイドラインに掲げているプライバシーと個人の自由の保護にかかわる原則を国内法において考慮すること」，「プライバシー保護の名目で個人データの国際流通に対する不当な障害を除去することに努めること」，「ガイドラインの履行について協力すること」などの勧告を示した[24]。

2013 年，OECD プライバシーガイドラインは 30 数年ぶりに改正された[25]。しかし，OECD プライバシー 8 原則に変更はなされていない。改訂では，加盟国に対し，「プライバシーの保護と情報の自由な流通に対し，政府内の最も高いレベルでリーダーシップを示し実行すること」，「ガイドラインを，すべてのステイクホルダーが関与するプロセスを通して履行すること」，「公的部門および民間部門の双方に勧告を広く浸透させること」等が勧告された[26]。

(2) 忘れられる権利

2012 年 1 月 25 日，欧州委員会はプライバシー保護に関する「個人データの取扱いに係る個人情報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規則（一般的データ保護規則）の提案」(Proposal for a 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 (General Data Protection Regulation) (2012))[27] を提案・公表した。

従来の EU データ保護指令を抜本的に改正するもので，その大きな特徴は，データ本人の権利として「忘れられる権利 (the right to be forgotten)」(17 条) が新設されたことであった。その後「忘

れられる権利」は 2013 年，欧州議会の修正により「消去権」となった。

しかし，「忘れられる権利」という名称やその権利性の台頭は，表現の自由とプライバシーの両者の対立がより鮮明になったものであるといえる(28)。

(3) 消費者プライバシー権利章典

2012 年 2 月 23 日，オバマ米大統領が情報化時代の青写真として，「消費者プライバシー権利章典」(Consumer Privacy Bill of Rights)(29) を公表した。「消費者プライバシー権利章典」では，消費者は個人データに関して①個人のコントロール（Individual Control），②透明性（Transparency）③コンテクストの尊重（Respect for Context）④セキュリティ（Security）⑤アクセスと正確性（Access and Accuracy）⑥焦点を絞った情報収集（Focused Collection）⑦説明責任（Accountability）など，7 つの権利を持つとされる。特に個人のコントロールの権利については，インターネット上でのオンラインターゲッティング広告の事業者に個人データを収集・利用させることを拒否でき，個人の追跡を禁止する Do Not Track の原則が示されている。

6. カナダにおけるプライバシー保護

カナダはプライバシー保護先進国といわれている。カナダでは 1970 年代初頭からプライバシーに関して検討するタスクフォースが設立された。そして，「現在および将来の個人の権利とそれに付随する価値，ならびに自動情報ファイルシステムに含まれるデータの収集，保管，処理，使用によってプライバシーの侵害が発生する可能性によって生じる問題」について検討がなされた(30)。その成果が「プライバシーとコンピュータ（privacy and computer）」に報告された。しかしながら，報告書では差し迫った法制定の提案がなされなかったため，連邦政府は法制定の検討準備のためにプライバシーに関する省庁間委員会（Interdepartmental Committee on Privacy）を設けた(31)。

1974 年に「プライバシー保護法（Protection of Privacy act）」が制定された。「プライバシー保護法」はプライバシー保護の観点から刑法典や他の法律を改正するために制定されたものである。

1977 年には「差別の禁止及び個人のプライバシー保護に関するカナダの現行法を拡張する法律」（An Act to extend the present laws of Canada that prescribe discrimination and that protect the privacy of individuals）―略称「カナダ人権法」（Canadian Human Rights Act）が成立した。ここでは，連邦の公的部門における「公正な情報処理」が盛り込まれた。

1982 年に英国カナダ法の改正によりカナダ憲法成立が決まり，カナダ史上初めて人権規定として「カナダ権利自由憲章」(Canadian Charter of Rights and Freedoms)(32) が制定された。プライバシー権や知る権利に関しては，その下位法として「プライバシー法（Privacy Act）」と「情報へのアクセス法（Personal Information Act）」が 1982 年に制定された。「プライバシー法」は政府機

関の公的部門（パブリック・セクター）を対象としたものである。

その後 2000 年に民間部門（プライベート・セクター）を対象とした個人情報保護法として「個人情報保護及び電子文書法（PIPED 法：Personal Information Protection and Electronic Documents Act）」が制定された。

ところで個人データないしプライバシーを保護することを目的とする法律の制定には 3 つの方式がある。すなわち，①一つの法律で公的部門（パブリック･セクター）と民間部門（プライベート･セクター）を対象とするオムニバス方式（統合方式），②公的部門と民間部門とをそれぞれ別の法律で対象とするセグメント方式（分離方式），③公的部門と民間部門のそれぞれの部門について，特定の分野で保護措置を講じるセクトラル方式（個別分野別方式）である(33)。

オムニバス方式はヨーロッパ諸国に多く，セクトラル方式はアメリカに見られるが，カナダの場合は，「プライバシー法」（パブリック・セクター）と PIPED 法（プライベート・セクター）のセグメント方式である。以下にプライバシー法と PIPED 法について触れる。

(1) プライバシー法（Privacy Act）(34)

カナダのプライバシー法は 1982 年に制定され，1983 年 7 月に施行された。その目的は，「自己自身に関する個人情報であって行政機関が管理するものについて個人のプライバシーを保護し，かつ個人にかかわる情報へのアクセス権を与える，カナダの現行の諸法律を拡充すること」(35)である。

プライバシー法には 3 つの基本的な構成要素がある。「一つは，連邦政府によって保管されている個人情報の合法的アクセスを承諾すること，連邦政府は，公正な情報収集，保存，利用，開示の義務を負うこと，プライバシー・コミッショナーという，独立したオンブスマンの地位を制定することである。プライバシー・コミッショナーはプライバシー法に基づき，問題を解決したり，不服申し立てに対する調査を行う。」(36)

プライバシー法は，77 ヵ条からなるが，「カナダ人権法」におけるプライバシー保護に関する規定 14 ヵ条を引き継いでより詳細に拡充したものである。カナダは，1980 年の OECD プライバシーガイドライン採択時に OECD 加盟国の中で採択を棄権した国の一つである(37)。

OECD のガイドラインに「連邦国家という特別の場合には，ガイドラインの順守は，連邦制における権力の分割によって影響を受けることもある」(38) とあるように，カナダが連邦国であり，また OECD が勧告であり法的拘束はないといえども影響力が大きい.

また，OECD ガイドラインは個人データの国際流通について経済的背景に基づいており，プライバシー法が「政府保有情報公開法である情報へのアクセス法の対法であり，CSA モデルコードをベースにすることが困難であった」(39) という理由などから，カナダは OECD ガイドラインの採択を棄権したと思われる。

しかし，プライバシー法の条項は詳細な規定であり，OECD8 原則と対比してみると，それに準

表 1　OECD8 原則とプライバシー法

OECD8 原則	プライバシー法条項[40]
①収集制限の原則 （Collection Limitation Principle）	4 条（個人情報の収集），5 条（直接収集すべき個人情報等）
②データ内容の原則 （Data Quality Principle）	6 条（行政目的に利用する個人情報の保存等）
③目的明確化の原則 （Purpose Specification Principle）	5 条（直接収集すべき個人情報等）
④利用制限の原則 （Use Limitation Principle）	7 条（個人情報の利用）
⑤安全保護措置の原則 （Secure Safeguards Principle）	6 条（行政目的に利用する個人情報の保存等）
⑥公開の原則 （Openness Principle）	8 条（個人情報の開示），9 条（開示記録の保持），26 条（第三者である個人に関する情報）
⑦個人参加の原則 （Individual Participation Principle）	12 条（アクセス権等）
⑧責任の原則 （Accountability Principle）	19 条～ 28 条（政府の責任）[41]

（国立国会図書館　調査立法考査局「カナダのプライバシー法（上）（下）」のプライバシー法条項を参照して作成）

じて対応している条項があることもわかる。（表 1）

ただし，責任の原則は，OECD ガイドラインでは，データ管理者の責任であるが，プライバシー法においては，政府における行政機関の長としての責任が広範囲かつ詳細に言及されている。

1980 年の OECD の勧告においては，ガイドラインの適用範囲をプライバシーと個人の自由に対して危険性のある公的部門または民間部門の個人データに適用すること，個人データの自動処理についてのみガイドラインを適用すること等が提言されている。プライバシー法では公的部門の個人データに対する適用である。また，個人データに関しては，「識別可能な個人に関する情報であって，その形態にかかわりない」[42] と言及されているように，個人データの自動処理についてのみに限定したものではない。

プライバシー法での大きな特徴といえるのは，監視･救済機関としてのプライバシー･コミッショナーをオンブスマンとして設置していることである。プライバシー・コミッショナーに関するプライバシー法の条項は，77 条の中で 29 条から 77 条まで 48 ヶ条に及んでいる。プライバシー･コミッショナーの地位は各省の次官相当とし，次官のすべての権限を有し，任期は 7 年である。プライバシー法はプライバシー保護を目的として個人情報の取り扱いに関し詳細な規定が定められているが，村松は「この法の実効性を高めているのが，議会によって選任されるプライバシー･コミッショナーである」[43] と述べている。

(2) PIPED 法（Personal Information Protection and Electronic Documents Act）[44]

PIPED 法は，プライベート・セクターでの商業活動において，組織による個人情報の収集，利用または開示の規定を定めるものである。PIPED 法は，組織が経済目的で妥当な必要性により個人情報を収集，利用または開示することと，個人のプライバシー権とのバランスを求めるものである。

PIPED 法の適用は，商業活動において個人情報を収集，利用または開示するすべての組織，連邦での活動，事業またはビジネスにおいて従業員の個人情報を収集，利用または開示を行うすべての組織が対象となる。ただし，PIPED 法が適用されないのは，（a）プライバシー法が適用される政府機関，（b）私的あるいは家庭内の目的のみで個人情報を収集，利用または開示する個人，（c）報道，芸術，または文学の目的のために個人情報を収集，利用または開示することにおいてである。

PIPED 法は 3 段階において施行された。まず第一段階（2001）は，連邦政府によって規制されたプライベート・セクター（電気通信，放送，銀行，州間の輸送と航空産業など）に適用され，州間や国際貿易での個人情報をカバーした。第二段階（2002）は，個人の健康情報が法の対象となった。第三段階（2004）は，州内で個人情報を収集，利用，開示している州内の全組織へ法の対象が適用拡大した[45]。

PIPED 法では，プライバシー 10 原則を規定している。カナダでは，カナダ規格協会（CSA: Canadian Standard Association）が「個人情報保護に関するモデルコード」を定めて国家規格となっているが，これは OECD8 原則に対応する 10 原則となっている。

カナダのプライバシー 10 原則は，①責任の原則（Accountability）②目的明確化の原則（Identifying Purpose）③告知・同意の原則（Consent）④収集制限の原則（Limiting Collection）⑤利用・開示・保持制限の原則（Limiting Use, Disclosure, and Retention）⑥正確性の原則（Accuracy）⑦安全保護措置の原則（Safeguards）⑧公開の原則（Openness）⑨個人参加の原則（Individual Access）⑩コンプライアンス挑戦の原則（Challenging Compliance）である。

PIPED 法もプライバシー・コミッショナーを不服申し立ての処理機関，法全般の運用責任機関として位置づけている。プライバシー・コミッショナーは，組織の PIPED 法の遵守に関しあらゆる不服申し立てを受付け，調査して問題解決する権限を持っている。プライバシー・コミッショナーによる救済がうまくいかなかった場合には，司法裁判所に対する訴訟の提起となる。プライバシー・コミッショナーはまた，組織の個人情報管理の実践を監査する権限を持っている。そして，プライバシー・コミッショナーは PIPED 法やプライバシー法においてその運用責任として最も重要な役割を担う位置づけである。パブリック・セクター，プライベート・セクターともに，プライバシー・コミッショナーがオンブスマンとしての機能を果たしている。

プライバシー・コミッショナーはカナダ国民のプライバシー権を監督・擁護する権限が与えられ，プライバシー法や PIPED 法の監視する責任を負うものである。プライバシー・コミッショナーが

さまざまなプライバシー問題に対して実施・調査してきた内容は公開することが PIPD 法で義務づけられており，Office of the Privacy Commissioner of Canada のホームページ上で公開されている[46]。

(3) プライバシー保護の手法（プライバシー・バイ・デザイン，プライバシー影響評価）

カナダでは，プライバシー保護策としてプライバシー・バイ・デザイン（PbD）やプライバシー影響評価（PIA）を先進的に行ってきている。

プライバシー・バイ・デザイン（Privacy by Design）は 1990 年代にカナダのオンタリオ州のプライバシー・コミッショナーである Ann Cavoukian が提唱したものである。

プライバシー・バイ・デザインは，プライバシー対策を設計段階で事前に埋め込む概念である。アン・カプキアンはプライバシー・バイ・デザインについて「さまざまな技術の設計仕様の中にプライバシーを織り込むフィロソフィーでありアプローチである」[47] と述べている。

プライバシー・バイ・デザインの特徴は，サービスやアプリケーション等のシステム企画・設計段階からプライバシー対策を組み込んで，設計から保守までのライフサイクル全般において，体系的かつ継続的にプライバシー保護の一貫した取り組みを行うことである。新しいシステムを導入するとき等にプライバシー対策を事前に織り込んでいく考え方である。プライバシー・バイ・デザインは以下の 7 つの基本原理がある[48]。

①事後的ではなく事前的（Proactive），救済的でなく予防的（Preventative）
②初期設定（Default Setting）としてのプライバシー
③デザインに組み込まれる（Embedded）プライバシー
④全機能的―ゼロサムではなく，ポジティブサム
⑤最初から最後までのセキュリティすべてのライフサイクルを保護
⑥可視性と透明性―公開の維持
⑦利用者のプライバシーを尊重―利用者中心主義を維持する

アン・カプキアンはこれらの原則の適用について，「プライバシー・バイ・デザインの原則は，あらゆる種類の個人情報に適用され得るが，医療情報や財務データといった機微なデータには，特に強力に適用されなければならない。プライバシー対策の強度は，データの機微性の高さに相応する傾向がある」[49] と述べている。特にカナダでは，医療情報の情報化がすすんでおり，連邦出資の連邦政府出資の Canada Health Infoway Inc[50] が中心となりデジタルヘルスを推進している。

プライバシー・バイ・デザイン（PbD）の実施にあたっては，事前にプライバシーの影響度を評価するプライバシー影響評価（PIA：Privacy Impact Assessment）を実施する。また，プライバシー強化技術（PET：Privacy- Enhancing Technologies）を採用し，統合する[51]。

PET は個人のプライバシー保護を強化する技術である。PET の例として，トロントの公共交通

機関構内で何千台もの監視カメラを設置する計画段階において，PbD の考え方による PET を使用し，ビデオ監視画像の暗号化を行うことにより乗客の不必要な識別を防ぐというプライバシー保護策を実施したことなどである(52)。

プライバシー影響評価は，1990 年代半ば，カナダをはじめとしてプライバシー・コミッショナーやコンサルタント，学者の間で議論されてきた。環境保全における「環境影響評価（Environmental Impact Assessment）」の考え方などを参考にして考案されたものである。

プライバシー影響評価は，情報システムの企画・設計を行うにあたり，収集する個人情報提供者のプライバシーへの影響を事前に評価するもので，情報システムのライフサイクル全般プロセスにおいて，プライバシーのリスク低減を目指すものである。

プライバシー影響評価はプライバシー・バイ・デザインの具体的な手法として実施される位置づけであり，事前にシステムのライフサイクルに対してプライバシーリスクを検討し，設計段階でプライバシー対策を織り込んでいくものである。カナダでは，プライバシー影響評価におけるシステム関連チェックポイントに PIPED 法に定めているプライバシー 10 原則の項目がプライバシー指針として広く用いられている(53)。

7. ビッグデータ時代のプライバシーの課題

ビッグデータ時代においては，国境を越えてデータの移転が加速し，プライバシーの保護及び個人の自由とデータの自由な流通との調和を図ることが求められる。そのためにもデータの扱いに関する国際的な取り組みとルールの随時見直し徹底化が必要である。OECD の改訂等国際的なルールの見直しが図られてきているが，一方プライバシーの国際的枠組みを理解するために，宮下が指摘するように「プライバシーを巡るアメリカとヨーロッパの衝突が現存しており，プライバシーの基本的な価値観である自由と尊厳を巡る対立」(54) を認識しておくことが重要である。

また，ユビキタスネットワークで M2M（Machine to Machine）などセンサー等を通じて個人に見えない形で自動収集される多種多量のデータは，個人への「告知と同意」のないまま収集されるケースが増大する。さらに収集されたビッグデータは本人への「告知と同意」がないままに 2 次利用される。2 次利用に匿名化されたデータが使われても，別のデータとの対応関係で身元の特定化が可能となりうる。ションベルガーは，「一見しただけでは個人情報と言えないデータでも，ビッグデータの枠組みの中で扱えば，容易に個人レベルまでさかのぼることができるし，私生活も事細かに推定できる」(55) と指摘する。

ビッグデータによるプライバシーのリスクが高まり，法令・ガイドラインを整備してプライバシー保護の取り組みを一段と強化することが必要である。しかし，クレイグ・マンティは，テクノロジーの進化が今までの個人情報保護のアプローチ，すなわち情報の収集を規制するアプローチの

限界を露わにしていると指摘し，「オンライン上に存在する自分の個人情報を見つける手段をユーザーに提供するのは事実上不可能だし，情報収集への同意を取り付けるのも難しくなっている」と述べている(56)。マンディは「ビッグデータのポテンシャルを抑え込む「データ収集と保有を制限する」これまでのやり方から，「データ使用の管理」へと法と規制の焦点をシフトさせることが，ビッグデータ時代のプライバシーを守る対策の第一歩になる」(57) と時代遅れのプライバシー保護法に対して一石を投じている。

また，現行の個人情報保護法やプライバシー保護法は，「個人情報の収集･処理する手続きは，「告知と同意」方式がプライバシー保護の基本となっている」(58) ので，ビッグデータ時代になり，「告知に基づく同意」という個人情報の収集・処理によるプライバシー保護の仕方は根底から揺らいでいく可能性が大きい。

ビッグデータの時代におけるプライバシー保護対策を検討していくうえで，プライバシーの問題を生じさせる諸活動に焦点を当てたダニエルによるプライバシー類型論（Taxonomy of Privacy）はプライバシーの多元的な側面を提示している。

プライバシー保護の対策として，新たな情報システムを構築あるいは変更していく際に，カナダで Ann 教授が開発して実績をあげているプライバシー・バイ・デザイン（PbD）やプライバシー影響評価（PIA），プライバシー強化技術（PET）の 3P との包括的な取り組みが期待される。その際，プライバシー類型論で示されているプライバシーの多元的な場面を想定して検討していくことが望ましい。

また，プライバシー保護の運用面においてプライバシー・コミッショナーはカナダにおいても中核となる役割を果たしてきている。我が国においても今後プライバシー・コミッショナーの制度の設置・効果的運用が望まれる。平成 25 年にパーソナルデータの利用・流通に関する研究会が提出した「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，「我が国におけるプライバシー･コミッショナー制度（パーソナルデータの保護のための独立した第三者機関）について検討を行うことが必要である。」(59) と提言されている。

我が国の個人情報保護法の改正では，個人情報の監視監督権限を有する第三者機関を「個人情報保護委員会」として設置することが決まっている。「個人情報保護委員会」が日本におけるプライバシー・コミッショナー制度の幕開けとなることが期待される中，カナダのようにプライバシー法において早くからプライバシー・コミッショナー制度を中核に置き，プライバシー保護の実績を上げてきているカナダのライバシー･コミッショナー制度のモデルは，今後プライバシー･コミッショナー制度を施行し運用していくうえで大いに参考となろう。

8. 終わりに

ジョージ・オーウェルが『1984 年』で描いた独裁者「ビッグブラザー」は，未来の監視社会のメタファーとして語られる。まさに現在はオーウェルが描いた「ビッグブラザー」に通じる監視社会となってきた感があるが，安岡らは，監視を「単純監視」（古典的監視）と「解析的監視」（現代的監視）とに分けている[(60)]。数多くの監視カメラや GPS（位置情報システム）により我々の行動を日常的に監視する。こうした監視は我々の外部的な行動を視覚的に観察する「単純監視」に属するものである。

一方，我々の日常的なあらゆる行動がライフログとして大量に収集・保存され解析される「解析的監視」は今後のビッグデータ時代の大きな特徴となる。我々の無意識の行動もすべてが解析され，パーソナルデータとしてビジネス等で利活用使される。

プライバシー保護とパーソナルデータの利活用はトレードオフの問題である。プライバシー保護のためのルールやガイドラインは，パーソナルデータを収集・蓄積し適正に利活用することとプライバシーの保護との調和を図ることが目的となる。しかし，ビッグデータ時代は，本人の無意識の行動によるパーソナルデータは，ルールやガイドラインだけではプライバシー保護の限界が生じてくる。事前にプライバシーを作りこむプライバシー・バイ・デザインにプライバシー保護の大いなる期待がよせられるが，予期しないパーソナルデータの 2 次利用が多数生じうることも考えなくてはならない。また，過度なプライバシー保護のためにその社会的費用をいたずらに増幅させることも気を付けなければならないし，ビッグデータの利活用を促進させるための障壁ともなる。

プライバシー保護に対する考え方が，各国で様々であるが，パーソナルデータを取り扱うタイプとして，大きく EU 型と米型に分けられる。EU 型はデータ削除に関する個人の権利としての「忘れられる権利」や，「データもち運びの権利」，「同意の明示」等，個人の権利主導でパーソナルデータを慎重に扱うオプトイン型（パーソナルデータの利用に関し，対象者から明確な許諾が得られない限り利用しない）である。個人の尊厳としてプライバシーの保護を考えるのが EU 型である。それに対し，米型はどちらかというとビジネス主導型でビッグデータの利活用に積極的なオプトアウト型（ダイレクトメールなど企業等から送られてくる情報を個人が拒否する）の傾向である。カナダの全国勧誘電話禁止名簿では勧誘電話を減らすために，希望する個人の家の電話や携帯電話，Fax，IP フォーン等の電話番号を National Do Not Call List に登録するオプトアウト型を実施している[(61)]。

プライバシーの概念について，文化の違いや民族の違いなどで各国のとらえ方が異なるので，今後プライバシーや個人の尊厳についてもっと議論する必要があるであろう。グラハム・グリーンリーフは，33 か国のプライバシー法について比較して，論文[(62)] においてその結果を報告している。日

本はベトナム，チリとともにデータ・プライバシー法のヨーロッパ的要素（“European” elements of data privacy laws）が十分備わっていない最下位のグループに位置づけられており(63)，「日本はアジアの法の中で最もヨーロッパ的な要素が少ない（Japan as the least “European” of Asian laws）」(64) と評価されている。さらにグラハム・グリーンリーフは，日本がデータ保護機関（data protection authorities）の欠如等の最大の原因もあって，「日本はアジアの中で最も劣ったデータ・プライバシー法を持つ国の一つである」(65) とも述べている。

我が国においては，個人情報保護法に関して特に議論がなされているのは，パーソナルデータの利活用に関する見直しで「本人の同意なしで個人データを利用できる」ようにすることの是非など，個人の権利の側面というより，経済的側面からのデータ利活用論議が多い。EU 諸国へのデータ流通やグローバル企業からの反対もあり，「本人の同意なしで個人データを利用できる」ことは今回見送られたが，森が「その漏えいを防ぐためのセキュリティのあり方や罰則といった表面の部分ばかりで，それらの包括的な解析がいかにプライバシー足りうるかという質的な部分にはあまり触れられていない」(66) と述べているように，パーソナルデータを含め，膨大なデータが国際間を行き交うビッグデータの時代に，今後ますますプライバシーの質的な部分の議論が必要であろう。

注

⑴　村田潔，折戸洋子「誰がプライバシーを侵害するのか」『経営情報学会誌』vol. 22　No. 4　経営情報学会　2014　pp. 240

⑵　総務省『情報通信白書　平成 26 年度版』（2014.7）（http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/pdf/）〈アクセス 2015.6.13〉

⑶　城田真琴『ビッグデータの衝撃』東洋経済新報社　2012　p27

⑷　ビクター・マイヤー＝ションベルガー，ケネス・クキエ　斎藤栄一郎訳『ビッグデータの正体』講談社　2013　p18

⑸　総務省『情報通信白書　平成 24 年度版』（2012.7）（http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/pdf/）〈アクセス 2015.6.13〉

⑹　同上

⑺　官邸「世界最先端 IT 国家創造宣言」（2013.6）https: //www.kantei.go.jp/jp/singi/it2/kettei/pdf/20130614/siryou1.pdf〈アクセス 2015.6.13〉

⑻　総務省『情報通信白書　平成 24 年度版』（2012.7）

⑼　同上

⑽　Samuel D. Warren and Louis D. Brandeis, “*The Right to Privacy*”, *Harvard Law Review Vol. 4, No. 5* 1890, pp. 193–220

⑾　佐藤幸治「権利としてのプライバシー」『ジュリスト』6 月 5 日号 No. 742 有斐閣　1981　pp. 158–171

⑿　同上　pp. 159–164

⒀　Hyman Gross, “*The Concept of Privacy*”, *42 New York University Low. Review* 34, 1967

⒁　佐藤幸治「権利としてのプライバシー」p. 162

⒂　同上　pp. 162–164

*その他，論者のプライバシー定義。

Fried「自己に関する情報に対するコントロールである」

Westin「自己に関する情報をいつ，どのように，どこまで他者にコミュニケートするかを自ら決めるという個人，集団または組織の要求である」
Miller「自己に関する情報の流通をコントロールする個人の能力である」これらは，「情報プライバシー権」として知られる。
Parker「われわれの各種部分をいつ，誰によって知覚されてよいかに対するコントロールである」
Gerety「個人のアイデンティティの親密性に対するコントロールないし親密性の自立である」

⑯ Daniel J. Solove, *Understanding Privacy*, Harvard University Press, 2009 pp. 12–13（大谷卓史訳『プライバシーの新理論―概念と法の再考』みすず書房　2013　pp. 17–18）

⑰ Daniel J. Solove, *Understanding Privacy*, pp. 10–11, pp. 101–170（大谷卓史訳『プライバシーの新理論―概念と法の再考』p. 12，pp142–251）

⑱「パーソナルデータの利用・流通に関する研究会」（2012.11）http://www.soumu.go.jp/main_sosiki/kenkyu/parsonaldata/〈アクセス 2015.6.2〉

⑲「パーソナルデータの利活用に関する制度見直し方針」（2014.12）https: //www.kantei.go.jp/jp/singi/it2/kettei/pdf/dec131220–1.pdf〈アクセス 2015.6.2〉

⑳「パーソナルデータの利活用に関する制度改正大綱」（2015.6）http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryou2.pdf〈アクセス 2015.6.2〉

㉑ 内閣官房情報通信技術（IT）総合戦略室「個人情報の保護に関する法律及び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の一部を改正する法律案」（2015.3.10）http://www.cas.go.jp/jp/houan/189.html〈アクセス 2015.6.14〉

㉒ OECD, The Recommendation of the Council of 23rd September 1980: Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, (1980) http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#guidelines〈アクセス 2015.6.14〉

㉓ 堀部政男『OECD プライバシーガイドライン』JIPDEC（一般財団法人日本情報経済社会推進協会）2014　p. 11

㉔ 同上　p222

㉕ OECD, The Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, (2013) http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf〈アクセス 2015.6.14〉

㉖ 堀部政男『OECD プライバシーガイドライン』pp. 173–174

㉗ European Commission, Proposal for a 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 (General Data Protection Regulation), (2012) http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf 〈アクセス 2015. 6.14〉

㉘ 国会図書館「忘れられる権利をめぐる動向」（2015.3.10）（http://dl.ndl.go.jp/view/download/digidepo_9055526_po_0854.pdf? contentNo=1）〈アクセス 2015.6.13〉

㉙ The white House, **Consumer Data Privacy in a Networked World: A framework for protecting privacy and promoting privacy and promoting innovation in the global digital economy, (2012.2)**（https://www.whitehouse.gov/sites/default/files/privacy–final.pdf）〈アクセス 2015.6.13〉

㉚ 堀部政男『OECD プライバシーガイドライン』p73

㉛ David H. Flaherty, *Protecting privacy in Surveillance Societies*, the university of North Carolina press Chapel Hill and London, 1989 p244

㉜ the Minister of Justice, Canadian Charter of Rights and Freedoms, (1982)（http://laws–lois.justice.gc.ca/eng/const/page–15.html）〈アクセス 2015.6.13〉

⑶3 堀部政男「個人情報保護法の考え方」(H16.7.14)（http://www.mext.go.jp/b_menu/shingi/gijyutu/gijyutu1/006/shiryo/04080202/003.htm）〈アクセス 2015.6.14〉
⑶4 the Minister of Justice, Privacy act, (2015.6.9)
（http://laws-lois.justice.gc.ca/eng/acts/P-21/）〈アクセス 2015.6.13〉
（邦訳　国立国会図書館　調査立法考査局　法務課「カナダのプライバシー法（上）」『レファレンス』No. 418　1985　pp. 148-167，国立国会図書館　調査立法考査局　法務課「カナダのプライバシー法（下）」『レファレンス』No. 419　1985　pp. 117-138）
⑶5 「カナダのプライバシー法（上）」p. 154
⑶6 Nancy Holmes Law and Government Division, Canada's Federal Privacy Laws, (2008.9.25)（http://www.parl.gc.ca/Content/LOP/ResearchPublications/prb0744-e.htm）pdf〈アクセス 2015.6.14〉
⑶7 堀部政男『OECD プライバシーガイドライン』pp. 31-32　尚，OECD ガイドラインの採択を棄権した国は，オーストラリア，カナダ，アイスランド，アイルランド，トルコおよびイギリス。
⑶8 「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 OECD 理事会勧告」(1980.9) http://www.mofa.go.jp/mofaj/gaiko/oecd/privacy.html〈アクセス 2015.6.14〉
⑶9 佐藤信行「カナダ」『比較法研究』有斐閣　2002　p. 47
⑷0 プライバシー法条項は「カナダのプライバシー法（上）」pp. 148-167，「カナダのプライバシー法（下）」pp. 117-138 を参照した。
⑷1 「カナダのプライバシー法（下）」pp. 117-138
行政機関の長の責任・権限として，19 条（内密に入手した個人情報等），20 条（連邦・州間問題），21 条（国際問題および国防），22 条（法律の執行及び調査等），23 条（保証証明），24 条（有罪宣告を受けた個人），25 条（個人の安全），26 条（第三者である個人に関する情報），27 条（弁護人・依頼人間の秘密），28 条（医療記録）
⑷2 「カナダのプライバシー法（上）」p. 154
⑷3 村松明子「個人情報保護制度について―カナダのプライバシー法を中心に―」『岩手大学大学院人文社会学研究科研究紀要』岩手大学院　人文社会学研究科 2003
⑷4 the Minister of Justice, Personal Information Protection and Electronic Documents Act, (2015.6.9)（http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf）〈アクセス 2015.6.14〉
⑷5 Nancy Holmes Law and Government Division, Canada's Federal Privacy Laws, (2008.9.25)（http://www.parl.gc.ca/Content/LOP/ResearchPublications/prb0744-e.htm）pdf〈アクセス 2015.6.14〉
⑷6 Office of the Privacy Commissioner of Canada,（https: //www.priv.gc.ca/index_e.asp）〈アクセス 2015.6.14〉
⑷7 Ann Cavoukian, *Privacy by Design*,（https: //www.ipc.on.ca/images/resources/privacybydesign.pdf）〈アクセス 2015.6.20〉
⑷8 Ann Cavoukian, Privacy by Design The 7 Foundational Principles,（https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/）〈アクセス 2015.6.20〉
⑷9 同上
⑸0 Canada Health Infoway,（https://www.infoway-inforoute.ca/en/）〈アクセス 2015.6.29〉
⑸1 Ann Cavoukian, Privacy by Design,（https://www.ipc.on.ca/images/resources/privacybydesign.pdf）〈アクセス 2015.6.20〉
⑸2 Ann Cavoukian, *Privacy by Design Book … Take The Challenge,* Information and Privacy Commissioner of Ontario Canada (2009.1) pp. 30-31（https://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf）〈アクセス 2015.6.23〉
⑸3 「住民のプライバシーの保護に関する新しい考え方と電子自治体におけるそのシステム的な担保の仕組みについての研究会」報告書（PDF）(2001.3)（http://warp.da.ndl.go.jp/search/

archivesearch/WE01-Search.do;jsessionid=361D39E2A477CA2FA98A30E564946880.app01）〈アクセス 2015.6.20〉

(54) 宮下紘「プライバシー・イヤー 2012―ビッグデータ時代におけるプライバシー・個人情報の国際動向と日本の課題―」『Nextcom』vol. 12　2012　KDDI 総研 p38

(55) ビクター・マイヤー＝ションベルガー，ケネス・クキエ　斎藤栄一郎訳『ビッグデータの正体』p228-229

(56) クレイグ・マンティ「オンライン個人情報とプライバシー」『フォーリン・アフェアーズ・リポート』2014　No. 3　フォーリン・アフェアーズ・ジャパン p9

(57) 同上

(58) 『ビッグデータの正体』pp. 230

(59) 「パーソナルデータの利用・流通に関する研究会　報告書（案）～パーソナルデータの適正な利用・流通の促進に向けた方策～」pdf（2014.5）（http://www.soumu.go.jp/main_content/000225513.pdf）〈アクセス 2015.6.14〉

(60) 安岡寛道編　曽根原登，穴戸常寿『ビッグデータ時代のライフログ』東洋経済　2012　pp. 198-199

(61) National Do Not Call List（https://www.lnnte-dncl.gc.ca/dncla-adncl-eng）〈アクセス2015.6.28〉

(62) Graham Greenleaf, "*The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108*", Edinburgh School of Law Research paper series No 2012/12, 2012

(63) Ibid. p. 12

(64) Ibid. p. 17

(65) Graham Greenleaf, "*Independence of data privacy authorities: International standards and Asia-Pacific experience*", University of Edinburgh School of Law Working Paper Series No 2011/42, 2011 p37

(66) 森健『ビッグデータ社会の希望と憂鬱』河出文庫　2012　p215

Privacy in the Big Data Age:
Centering on Canada

Kiyoshi TAKEI

Abstract

With the rapid progress of ICT (Information and Communication Technology) networking, Big Data is being collected, accumulated and circulated. Data is automatically collected in real time by various devices and sensors by a ubiquitous network. Our time has become an era in which a vast quantity of digital data is being generated. Utilizing Big Data as resources is common practice and the creation of social values through the use of Big Data is increasing. However, we cannot bypass the problem of privacy protection. This paper explores the concept of privacy and considers protection of privacy in the Big Data age, and focuses particularly on Canada as a nation advanced in the protection of privacy.

Key words: Privacy protection, Privacy Act, PIPEDA (Personal Information Protection and Electronic Documents Act), OECD Privacy Guideline, Big Data, Privacy Commissioner, Privacy by Design (PbD), Privacy Impact Assessment (PIA).