

カナダのプライバシー・個人情報保護法

筑波大学図書館情報メディア系准教授

石井 夏生利

ISHII Kaori

- I はじめに
- II 連邦法
- III 州法
- IV プライバシー・バイ・デザイン
- V おわりに

I はじめに

本稿は、カナダのプライバシー・個人情報保護に関する法制度の概要及びプライバシーに関する最近の動きを取り上げ、日本の今後の議論の発展に貢献することを目的とする。

プライバシー・個人情報保護の国際的な議論を見る時に、日本では、EU及びアメリカの動向を注目する傾向がある。しかし、他の国や地域に目を向けることも比較法的な観点からは重要と考えられる。

カナダは、フランス及び英国の植民地時代を経て今日の独立国家を築いており、ヨーロッパと深い関係を有する。1931年のウェストミンスター憲章採択以降、英連邦王国に属している。また、カナダは、北アメリカ大陸北部に位置しており、米国との間には8,891キロにも及ぶ米国との陸上国境がある。米国とは自由貿易協定により世界最大の貿易関係にあり、米国の経済的影響を常に受

ける立場にある。カナダの政治制度は、立憲君主制、議院内閣制、連邦制が併用されている¹⁾。

越境データ移転について、カナダは、2001年12月20日、欧州連合(EU)から、個人情報保護及び電子文書法(Personal Information Protection and Electronic Documents Act, PIPEDA)が十分な保護レベル²⁾を有するとの認定を受けた³⁾。十分に認定は、カナダがEUにとって重要な貿易相手国であるという要素が勘案された結果である⁴⁾。また、オンタリオ州発祥の「プライバシー・バイ・デザイン」(Privacy by Design, PbD)が国際的な広がりを見せており、この概念は、プライバシー論議を牽引する役割を果たしている。

カナダのプライバシー・個人情報保護法制については、これまでも複数の成果が公表されてきた⁵⁾。しかし、それらは、やや期間が経過しているものや、特定のテーマに焦点を絞ったものであるため、改めて、カナダの動向を改めて取り上げる意味はあると考えられる。

日本では、2015年9月3日に個人情報の保護に関する法律が改正された。その過程では個人情報の識別性及び匿名化が大きな論点として議論された⁶⁾。また、同じく注目を集めてきた越境データ流通に関しては、個人情報保護委員会がEU及びアメリカ等との協力対話を進めている⁷⁾。この

1) カナダの概要については、藤田直晴ほか著・日本カナダ学会編『はじめて出会うカナダ』(有斐閣, 2009年)、日本カナダ学会のウェブ・サイト (<http://jacj.jp/>) 等参照。

2) EUデータ保護指令第25条1項は、「加盟国は、取り扱われている又は移転後の取扱いが意図されている個人データの第三国への移転は、本指令の他の規定に従って採択された国内規定の遵守を侵すことなく、当該第三国が十分なレベルの保護措置を確保している場合に限って、行うことができることを定めなければならない。」と定め、十分な保護レベルを講じていない第三国へのデータ移転を禁止できる規定を置いている。

EUデータ保護指令は、2016年4月27日付の一般データ保護規則の採択によって廃止されることとなったが、十分に仕組みは同規則にも引き継がれている。

3) Commission Decision C (2001) 4539, 2002 O.J. (L 2) (EU).

4) European Commission, *Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World*, COM (2017) 7 final (Jan. 10, 2017), http://europa.eu/rapid/press-release_IP-17-16_en.htm.

ような個別論点を深く論じることも重要ではあるが、本稿では、全体的な視点から、EU及びアメリカとバランスを保ちつつ、プライバシー・個人情報保護制度を展開しているカナダの状況について、法制度、論点、PbDの取組を整理することとした。

II 連邦法

1 管轄

カナダは、10の州 (province) 及び3の準州 (territory)⁸⁾ で構成される連邦国家であるが、米国とは異なり、連邦優位の連邦制を採用している。そして、公的部門・民間部門それぞれに包括的な個人情報保護法が制定されている。1867年憲法 (Constitution Act, 1867) (1982年に英領北アメリカ法から改称) 第92条及び第92A条は、州の組織や財政等、専属的な州の立法権限を定めている。連邦については、同法第91条に基づき、財政、郵便、通貨、国防、著作権等の専属的立法権限が定められている。同条29項は、「この法律により州の議会に専属的に付与された事項の部類の列挙から明らかに除外された事項の部類」と規定し、残余権限は連邦政府に属することを明らかにしている⁹⁾。

しかし、プライバシーに関する権限は、1867年憲法に定められていない。同法第92条13項は、「州の財政及び市民権」と定めているため、州が管轄を有するよう見えるが、個人データが州を超えて移転する場合をカバーするものではな

い。同法第91条2項「通商の規制」が連邦法の管轄であること、第92条10項「州と他の州を結ぶか又は州の境界を越えるその他の工事及び事業」を除く地方工事及び事業が州法の管轄であること、第91条柱書の「カナダの治安、秩序、善政のために法律を制定すること」が連邦議会の役割とされていることからすると、連邦法の権限であるとも考えられる。

この問題は、個人情報保護及び電子文書法 (PIPEDA) の制定により顕在化した。同法は、営利活動との関係で個人情報を取り扱う国内全ての民間事業者、及び、銀行や航空会社などの連邦規制事業において従業員情報を取り扱う事業者に適用される。同法第26条2項は、州内の民間事業者に規制が及ぶという問題を調整するために、カナダ総督において、州法がPIPEDAと「実質的に類似」 (substantially similar) すると判断した場合に、命令により、当該州内で行われる個人情報の収集、利用又は開示から、同法の規律する組織又は活動を適用除外できる旨を定めている。現在は、ブリティッシュ・コロンビア州、アルバータ州、ケベック州の民間部門向け個人情報保護法、及び、オンタリオ州、ニュー・ブランズウィック州、ニューファンドランド&ラブラドル州の個人健康情報に関する法律が実質的に類似するとの判断を受けている¹⁰⁾。しかし、州内で行われる個人情報の収集、利用及び開示を規制する連邦の権限、連邦法及び州法の相互関係は、裁判所の判決で明らかにする必要がある¹¹⁾。

連邦法の管轄に特に異議を唱えているのは、ケ

5) 長内了・佐藤信行「カナダの個人情報保護法」堀部政男編『情報公開・個人情報保護』ジュリスト増刊 (1994年) 297-301頁、佐藤信行「カナダ (個人情報保護法制の国際比較—民間部門を中心として—) 比較法研究第64号 (2002年) 38-47頁、消費者庁「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」(2009年3月) (http://www.ppc.go.jp/files/pdf/personal_report_2003caa_4.pdf) 167-222頁 (佐藤信行担当部分)、消費者庁「諸外国等における個人情報保護制度の監督機関に関する検討委員会・報告書」(平成23年3月) (http://www.ppc.go.jp/files/pdf/personal_report_2303caa.pdf) 125-145頁 (河合理穂子担当部分)、堀部政男・JIPDEC編『プライバシー・バイ・デザイン プライバシー情報を守るための世界的新潮流』(日経BP社、2012年)、新保史生「プライバシー・バイ・デザイン (特集 個人情報・プライバシー保護の理論と課題)」論究ジュリスト第18号

(2016年夏号) 16-23頁等。

6) 高度情報通信ネットワーク社会推進戦略本部 (IT総合戦略本部)「パーソナルデータに関する検討会」(<http://www.kantei.go.jp/jp/singi/it2/pd/>)。

7) 個人情報保護委員会「各国機関との連携」(<http://www.ppc.go.jp/enforcement/cooperation/cooperation/>)。

8) 連邦制度をとるカナダでは、州 (province) に指定された地域以外を準州と呼ぶ。準州の自治権は限定的であり、立法権や行政権は連邦政府が持っている。また、歳入のほとんどを連邦政府から得ている。岸上伸啓「準州 (Territory)」日本カナダ学会カナダ豆知識 (<http://jacs.jp/dictionary/dictionary-sa/09/19/653/>)。

9) Constitution Acts, 1867 to 1982 (Can.). 邦訳は、国立国会図書館調査及び立法考課局「各国憲法集(4)カナダ憲法」(2012年3月) 9-10頁、45-48頁参照。

ベック州である。同州の情報プライバシー委員会は、2003年12月11日に実質的に類似するとの判断が発効したことを受け、州の控訴裁判所に対し、PIPEDAの排他的管轄が憲法に違反すると主張して提訴した。しかし、その手続は2006年以降停止している¹²⁾。また、ケベック州は、PIPEDAの十分性認定とは別に、民間部門の個人情報保護法について十分性を得るための手続を進めたものの、第29条作業部会¹³⁾の「ケベックにおける個人データ保護に関する7/2014意見」(2014年6月4日付採択)¹⁴⁾によって、ケベック法の適用範囲(州を超える場合)、透明性の原則、アクセス権、「機微情報」の概念、転送の原則に関する課題が残されていると指摘され、十分な保護レベルを有するとの意見を受けることはできなかった。PIPEDAの十分性認定は、実質的に類似する法令を含む¹⁵⁾、ケベック州は、独自の行動を取ったことにより不安定な立場に置かれている。

2 連邦法

カナダには、連邦法として、公的部門を規律するプライバシー法(Privacy Act)¹⁶⁾、民間部門を規律するPIPEDA¹⁷⁾が存在する。

プライバシー法の背景には、1982年カナダ憲法第1章「カナダ権利及び自由憲章」(Canadian Charter of Rights and Freedoms)¹⁸⁾が存在している。その第7条は、人の生命、自由及び身体の安全に

関する権利、第8条は不当な捜索及び押収を受けない権利を定めている。これらの規定はプライバシーを明示したものではない。しかし、連邦最高裁判所は、過去の判例を引用しつつ、プライバシー保護が自由かつ民主的な社会を守るために必要であることを、プライバシー法が憲法類似の立場にあることを述べている¹⁹⁾。プライバシーは、解釈により憲法上の保護を受けているといえる。

また、プライバシー法の基本理念を考える際には、情報へのアクセス法の対法として制定されているということが重要である。プライバシー法及びPIPEDAは、そもそも「情報へのアクセス法及びプライバシー法を制定し連邦裁判所法及びその他の関連法を改正する法律」(An Act to enact the Access to Information Act and Privacy Act, to amend the Federal Court Act, and to amend certain other acts in consequence thereof)という1つの法律の別表1及び2として制定されたものであり、一体としてでなければ理解できない部分が多いとされている²⁰⁾。

3 プライバシー法²¹⁾

(1) 概要

カナダでは、プライバシー法の制定に先立ち、1977年人権法(Human Rights Act)²²⁾第2条(b)項が、個人のプライバシー保護と個人情報を含む記録へのアクセスを定めていた²³⁾。プライバシー

10) Office of the Privacy Commissioner of Canada, *Provincial legislation deemed substantially similar to PIPEDA*, <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/legislation-related-to-pipeda/provincial-legislation-deemed-substantially-similar-to-pipeda/> (last visited Jan. 20, 2017).

11) 1 BARBARA MCISAAC ET AL., *THE LAW OF PRIVACY IN CANADA* 27-30 (2015).

12) Organizations in the Province of Quebec Exemption Order, SOR/2003-374 (Nov. 19, 2003), <http://laws-lois.justice.gc.ca/eng/regulations/SOR-2003-374/page-1.html>.

13) 第29条作業部会は、監督機関又は各加盟国が指名した代表者、EUの機構等の代表者、欧州委員会の代表者で構成される助言機関である。一般データ保護規則では、欧州データ保護会議へと改組され、その権限は大幅に強化されている。

14) Article 29 Data Protection Working Party, *Opinion 7/2014 on the Protection of Personal Data in Quebec*, WP 219 (Adopted on Jun. 2014), <http://ec.europa.eu/justice/data->

[protection/article-29/documentation/opinion-recommendation/files/2014/wp219_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp219_en.pdf).

15) *Id.* at 4.

16) R.S.C., 1985, c. P-21.

17) S.C. 2000, c. 5.

18) Part I of the Constitution Act, 1982.

19) Lavigne v. Canada (Office of the Commissioner of Official Languages), [2002] S.C.C., 53, paras. 24, 25; Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401, [2013] S.C.C. 62, para. 22.

20) 消費者庁・前掲「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」170頁。

21) 消費者庁・前掲「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」及び同・前掲「諸外国等における個人情報保護制度の監督機関に関する検討委員会・報告書」参照。

22) 1976-77, c.33, s.1.

23) *Supra* note 11, at 3-6.

法は、人権法の廃止とともに成立した。

プライバシー法は、1983年7月1日に施行された法律であり、全77条及び附則で構成される²⁴⁾。同法は、連邦政府機関が収集、利用及び開示する個人情報又は連邦政府の従業員の情報を保護するための規定を設けるとともに、個人に対し、連邦政府機関が保有する個人情報へのアクセス権及び訂正請求権を与えている(第2条)。

同法は、政府機関に対し、個人情報の収集を運用中の計画又は活動に直接関係するものに制限すること、可能な場合には直接本人から収集すること、個人に対し収集目的を通知すること、情報の正確性、最新性及び完全性を保障するための合理的措置を講じること、収集目的に沿う範囲内で個人情報を利用すること、本人の同意なき開示の原則禁止、利用又は開示に課する記録の保持等を義務づけている(第4条～第9条)。個人情報は、ある形態に記録されている識別可能な個人に関する情報をいうと定義され、(a)人種、国籍又は民族の出自、肌色、宗教、年齢又は既婚若しくは未婚の別、(b)個人の教育、医療、犯罪若しくは雇用の履歴に関する情報又は個人が関わっている金融取引に関する情報、(c)個人割り当てられた識別番号、記号その他細目、(d)個人の住所、指紋又は血液型、(e)個人の個人的意見又は見解、(f)黙示的又は明示的な私的又は秘密の性質を有する、個人から政府機関に送付された通信及びその返答、(g)個人に関する他者の意見、(h)個人への報償を与える目的で行われる他者の意見、(i)個人の名前であって、他の個人情報とともにその個人の情報を明らかにするであろうものなどが含まれる(第3条)。

同法は、政府機関の長に対し、政府機関が管理する個人情報を個人情報バンク(personal information banks)に登録し、その概要を公開するよう義務づけている。政府機関は、自己が管理しつつも個人情報バンクに登録していない情報の種類も公開しなければならない(第10条～第11条)。

個人は、個人情報バンクに含まれる個人情報へのアクセス権、訂正請求権等を有する(第12条～第28条)。

監督権限を行使するのは、同法に基づき設置された連邦プライバシー・コミッショナー(Privacy Commissioner of Canada)である。コミッショナーは、独任制の独立機関である。コミッショナーは、総督において、国璽の委任に基づき、上院及び下院の各承認された政党の代表と協議した後に、上院及び下院の決議を経て指名される。任期は7年間であり、再任可能である(第53条)。コミッショナーは政府から独立しており、議会へ直接報告義務を負う(第38条～第39条)。現コミッショナーは、ダニエル・テリエン(Daniel Therrien)氏である。

コミッショナーは、個人情報の違法な取扱い、個人情報へのアクセス拒否、個人情報へのアクセスの不当な遅延に関する苦情について、それを受けて調査する権限を有する。調査は職権によって行使することもできる。コミッショナーは、証言録取、資料の閲覧及び写しの取得、立入検査等の権限を有し、苦情に十分な理由があると認めるときは、政府機関の長に対し、認定事項及び勧告を含む報告書を提供する。適切な場合には、期間制限を付し、勧告に沿って講じられた措置又は措置が講じられなかった場合の理由を通知するよう、当該政府機関の長に求める(第29条～第35条)。コミッショナーは、交渉、仲裁及び和解を通じて、紛争を解決しようとするオンブズマン(又はホンブスパーソン)として位置づけられており、不服申立に関する判断は拘束力を有しない。

アクセス権を拒否された個人は、コミッショナーに対して申し立てた苦情の結果を受領した後、連邦裁判所に提訴することができる。コミッショナー自身も、個人から同意を得ることにより、連邦裁判所に提訴することが認められる(第41条、第42条)。アクセス権以外のケースに関する提訴権は認められていない。

なお、法制度上の義務ではないが、カナダ財務省の指令に基づき、連邦政府機関²⁵⁾ではプライバシー影響評価が実施されている²⁶⁾。

同法は、制定から30年以上を経過しているが、大きな改正はなされていない。

24) 関連する規則及び命令については下記のウェブ・ページ参照 ([https://www.priv.gc.ca/en/privacy-topics/privacy-](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/r_o_a/)

[laws-in-canada/the-privacy-act/r_o_a/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/r_o_a/))。

25) プライバシー法第3条の定める政府機関を対象とする。

(2) コミッショナーによる改正提案

連邦議会の情報アクセス・プライバシー及び倫理に関する常設委員会（Standing Committee on Access to Information, Privacy and Ethics）は、2016年3月から11月にかけてプライバシー法の調査を行った。コミッショナーは、下記の3つのテーマに基づく法改正を提案している²⁶⁾。

テーマ1：技術的变化

- 1 情報共有に関する合意の要件を明確化すべきである。
- 2 政府機関による個人情報の安全保護措置に関する義務を法定すべきである。
- 3 個人情報の侵害に関するコミッショナーへの報告を義務化すべきである。

テーマ2：立法的現代化

- 4 収集のための明確な必要条件を設けるべきである。
- 5 コミッショナーの権限について、苦情調査のためのオンブズパーソンモデル形態から拘束的命を下す権限に置き換えるべきである。
- 6 コミッショナーへのプライバシーに関する苦情を独立審査するための制定法上の仕組みを設けるべきである。
- 7 新規又は重大な変更が加えられた計画について、政府機関にプライバシー影響評価を義務づけ、実施に先立ちコミッショナーに提出することを義務づけるべきである。
- 8 政府機関に対し、プライバシーとの関係性を協議するために、立法及び規則案を提出するに先立ち、それらをコミッショナーへ提出するよう義務づけるべきである。
- 9 コミッショナーに対する、一般への教育及び研究の任務を明文化すべきである。
- 10 本法を5年ごとに見直すべきである。

テーマ3：透明性の強化

- 11 政府機関のプライバシー問題が公益に関係

する場合は、コミッショナーの守秘義務を解除して一般に公表する裁量を与えるべきである。

- 12 執行協力のために、コミッショナーが国内外の相手と情報を共有する能力を拡大すべきである。
- 13 コミッショナーに対し、苦情が些細な場合など特定の理由に基づく場合に、苦情を拒否し調査を停止する裁量を与えるべきである。
- 14 広範なプライバシー問題や、法執行機関から受けた適法なアクセス請求について、政府機関の報告義務を強化し、透明性を高めるべきである。
- 15 大臣の事務所、首相の事務所、及び外国へのアクセス権に本法の適用範囲を拡大すべきである。
- 16 個人情報のアクセス請求の例外を制限すべきである。

4 個人情報保護及び電子文書法²⁸⁾

(1) 概要

個人情報保護及び電子文書法（PIPEDA）は、民間部門における個人情報の取扱いを定めている。同法は、2000年4月13日に成立し、2001年から2004年にかけて段階的に施行された。最終改正は2015年6月23日である。PIPEDAは、前半が個人情報保護法、後半が電子文書法で構成されている。コミッショナーの監督権限は、同法に基づき民間部門にも及ぶようになった。

同法は、営利活動の過程での個人情報の取扱いに関する基本的規則を定めている。その目的は、技術が情報の流通及び交換を一層促進する時代において、個人情報に関する個人のプライバシー権を認識するとともに、当該状況で通常人が適切と考える目的のために組織が個人情報を収集、利用又は開示する必要性を認識する方法において、個人情報の収集、利用及び開示を対象とする規則を

26) OPC, *Privacy Impact Assessments*, <https://www.priv.gc.ca/en/about-the-opc/opc-operational-reports/opc-privacy-impact-assessments/> (last visited Jan. 20, 2017). 指令は2010年4月1日に施行された。

27) OPC, *Review of the Privacy Act - Revised recommendations* (Nov. 1, 2016), <https://www.priv.gc.ca/en/>

[privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_r/pa_ref_rec_161101/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_r/pa_ref_rec_161101/).

28) OPC, *An Overview of the Office of the Privacy Commissioner of Canada and Federal Privacy Legislation*, https://www.priv.gc.ca/en/about-the-opc/publications/guide_ind/ (last visited Jan. 20, 2017).

設けることにある(第3条)。

同法は、現実世界とオンライン世界を問わず、事業規模を問わず平等に適用される。PIPEDAはカナダの民間事業者に適用されるが、前記の通り、実質的に類似すると判断した州法はその適用を除外される。しかし、その判断を受けた州であっても、無線局及びテレビ局、航空会社、鉄道会社及び通信事業者等の連邦規制事業者による従業員情報の取扱いには法が適用される(第4条1項(b)号、第26条2項)。また、PIPEDAは、民間事業者が関与する営利取引の過程で、州又は国を超えて流通する全ての個人データに適用される。

PIPEDAは、プライバシー法が適用される政府機関、ジャーナリズム、芸術又は文学目的のみで個人情報を収集、利用又は開示する組織、私的目的で個人情報を収集、利用、開示する個人には適用されない(第4条2項)。

組織の従業員の氏名、肩書き、勤務先住所、電話番号及び電子メールアドレスには適用されない(第2条)。ただし、連邦規制事業者の従業員及び採用応募者の情報は適用対象である。

個人情報は識別できる個人に関する情報を意味する(第2条1項)。個人の氏名、人種、民族的出自、宗教、既婚未婚の別、学歴、電子メールアドレス及びメッセージ、IPアドレス、年齢、身長、体重、医療記録、血液型、DNAコード、指紋、声紋、収入、購買履歴、支出習慣、銀行情報、クレジット／デビットカード情報、借入れ又は信用報告、納税申告、社会保障番号又は他の識別番号が含まれる。一般的に、個人情報の範囲は広く解釈され、多くの関連裁判例が出されている²⁹⁾。

PIPEDAは、民間事業者による個人情報の収集、利用又は開示について、附則1に列挙されたカナダ規格協会の「個人情報保護に関するモデルコード」³⁰⁾の遵守を求めており、この諸原則が基

本的なプライバシーの義務となっている(第5条1項)。

本則では、諸原則の例外を定めるという手法が取られている(第7条～第9条)。

諸原則の概要は次の通りである。

第1原則 説明責任

組織は、諸原則の遵守を監視するプライバシー保護の責任者を指名する。組織は、情報が第三者によって取り扱われる間、契約又は他の手段により同等の保護レベルを提供する。組織は、個人情報の保護手順を実施し、苦情や問い合わせに対応する手続を設け、従業員を訓練し、組織の方針や手順を説明することなどにより、諸原則を実践する方針及び実務を実施する。

第2原則 目的の特定

組織は、収集前又は収集時に個人情報の収集目的を特定しなければならない。組織は、個人情報の収集目的を明確化する。収集目的は口頭又は文書により個人に通知される。収集時の目的以外で利用する場合、新たな目的は利用前に特定される。法の定める場合を除き、利用に先立ち個人の同意が必要である。この原則は、第4及び第5原則と密接に関連する。

第3原則 同意

個人情報の収集、利用又は開示について、個人の「認識及び同意」が必要である³¹⁾。組織は、通常、収集時に利用又は開示への同意を取得するが、利用目的を変更するような場合には、利用前に、利用又は開示への同意を取得する。組織は、製品又はサービスの提供条件として、明示的に特定された適法な目的を達成するために必要な範囲を超えて情報を収集、利用又は開示することについて、個人に同意を求めているのではない。同意の取得には、個人の合理的な期待

29) OPC, *PIPEDA Interpretation Bulletins*, <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/> (last visited Jan. 20, 2017).

30) Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96.

31) 法、医療、安全上の理由から同意を求めることが不可能又は非現実的な場合がある。法執行目的である場合や、本人が未成年、重症患者、精神的に不能な場合などが当てはまる。個人と直接の関係を持たない組織、例えば、慈善団体やダイレクトマーケティングを行う組織が他の組織からマーケティングリストを受領するような場合には、提供者側が開示前に同意を取得することが期待される。

も関係する。組織が同意を求める方法は状況によって異なり得るが、機微性の高い情報は、一般的に明示的な同意を求めるべきである。個人は、法的又は契約上の条件に従い、いつでも同意を取り消すことができる。

第4原則 制限的収集

個人情報の収集は、組織が特定した目的に必要なものに制限される。情報は、適切かつ適法な手段により収集される。収集される情報の量と種類は、特定した目的を満たすために必要なものに限定される。この原則は、第2及び第3原則と密接に関係する。

第5原則 制限的利用、開示及び保持

個人情報は、個人の同意がある場合又は法により義務づけられる場合を除き、収集目的以外の目的で利用又は開示されてはならない。個人情報は、目的を達成するために必要な期間のみ保持される。目的達成のために必要ではなくなった個人情報は、破棄、消去又は匿名化されるべきである。この原則は、第2、第3、第9原則と密接に関係する。

第6原則 正確性

個人情報は、利用目的に必要な限りで正確、完全かつ最新でなければならない。組織は、情報の収集目的を達成するために必要でない限り、個人情報を日常的に更新してはならない。第三者に開示された情報を含む、継続的に利用される個人情報は、正確性の義務が明確に制限されない限り、一般的に正確かつ最新であるべきである。

第7原則 安全保護

個人情報は、情報の機微性に適した安全保護措置によって保護される。安全保護措置は、個人情報の紛失又は盗難、無権限アクセス、開示、複写、利用又は修正から保護する。保護措置には、物理的、組織的及び技術的措置を含む。

第8原則 公開

組織は、個人情報の管理に関する方針及び実

務についての特定の情報を個人が容易に利用できるようにする。

第9原則 個人のアクセス

請求に基づき、個人は、自己の個人情報の存在、利用、及び開示についての通知を受け、当該情報へのアクセスを与えられる。個人は、適切な場合には、情報の正確性及び完全性に異議を唱え、訂正させることができる³²⁾。請求に基づき、組織はその個人に関する個人情報を保有しているか否かを個人に伝えなければならない。情報源を示すことが奨励される。加えて、組織は、当該情報の利用理由、及び、情報を開示した第三者に関する説明を提供すべきである。個人において個人情報が不正確又は不完全であることをうまく立証できた場合、組織は請求に応じて情報を修正しなければならない。修正は、異議が出された情報の性質に応じて、情報の訂正、削除、又は追加を含む。適切な場合、修正された情報は、当該情報にアクセスできる第三者に送信される。異議が個人の満足する形で解決されない場合、未解決の異議の内容は組織によって記録される。適切な場合には、未解決の異議は、当該情報にアクセスできる第三者に送信される。

第10原則 遵守の問題

個人は、上記の諸原則の遵守に関する問題を組織の遵守責任者に対処させることができる。組織は、苦情処理手順を設け、全ての苦情を調査しなければならない。

第3原則との関係で、個人の同意は、組織の活動が向けられる個人において、個人が同意をした個人情報の収集、利用、開示の性質、目的及び結果を理解することが合理的に期待される場合に限り有効であると定められている（第6.1条）。

個人は、PIPEDAに違反する個人情報の取扱いについて、組織の苦情対応の結果に満足しなかった場合には、コミッショナーに苦情を申し立て

32) 一定の状況では、組織は、個人に関して保有する全て個人情報へのアクセスを提供できない場合がある。アクセス義務の例外は限定的かつ具体的でなければならない。アクセスを拒否する理由は、請求に基づき個人に提供すべきである。例外

には、提供するのに法外な費用を要する情報、他者への言及を含む情報、法的、安全上又は営利的な独占販売上の理由により開示できない情報、及び、弁護士と依頼者又は訴訟上の特権に服する情報が含まれる。

ることができる。コミッショナーは、職権でも苦情調査を開始することができる(第11条)。コミッショナーは、証言録取、証拠の受領、立入検査、記録の写しの取得等の権限を有する。また、仲裁又は和解といった紛争解決手段を用いる場合がある。コミッショナーは、苦情対応の開始から1年以内に、認定事項及び勧告、当事者が達した和解、適切な場合には、期間制限を付し、勧告に沿って講じられた措置又は措置が講じられなかった場合の理由を通知すべきことなどを記した報告書を用意し、当事者に送付する(第11条~第13条)。コミッショナーは、PIPEDA違反に対して制裁金や損害賠償を命じる権限はない。

個人は、コミッショナーの報告を受けた後又は苦情調査を行わない旨の通知を受けた後、原則として1年以内に、苦情を連邦裁判所に持ち込むことができる(第14条)。コミッショナーも個人に代理して苦情を持ち込むことができる(第15条)。裁判所は、組織に対し、違反実務を正すこと、組織の是正措置を公表すること、個人が被った侮辱等の被害を賠償することを命じることができる(第16条)。コミッショナーは、組織がPIPEDAに違反し又は勧告に従わないと信じる合理的理由がある場合には、組織との間で遵守合意を結び、コミッショナーによる提訴等を停止することができる(第17.1条)。同様の要件の下で、監査を実施する権限も有する(第18条)。

コミッショナーは、PIPEDA及び実質的に類似と判断された州法の適用について、議会への年次報告義務を負う(第25条)。その他の権限及び職務としては、一般への啓蒙、議会の立法提案への指針提供、議会、個人、組織による問い合わせへの回答、国際協力等がある。

以上の他、コミッショナーには、カナダラジオテレビ・電気通信委員会(Canadian Radio-television and Telecommunications Commission)及び連邦競争局(Federal Competition Bureau)とともに、反スパム法(Canada's anti-spam legislation)³³⁾の監督権限を有している。

(2) 2015年改正

PIPEDAは、2015年6月18日、デジタルプライバシー法(Digital Privacy Act)³⁴⁾により改正された。同法の改正事項は多岐にわたっており、有効な同意の要件としての個人の合理的期待、コミッショナーと組織間の遵守合意、公益性が認められる場合におけるコミッショナーの守秘義務の解除、事業活動上の電子メールの適用除外、連邦事業の範囲の拡大、係る事業の採用応募者情報の保護、詐欺の探知・予防目的のための同意の例外、事業承継等に伴う同意なき個人情報の利用又は開示、出訴期間の短縮化³⁵⁾等に及んでいる。

特に重要な改正事項は、データ侵害報告制度の新設である³⁶⁾。組織は、その管理する個人情報について、安全保護措置違反(データ侵害)が、個人に重大な被害を与える現実的危険をもたらすと合理的に信じる場合、コミッショナー及び影響を受ける個人に対し、係るデータ侵害を報告しなければならない。加えて、他の組織や政府機関が被害を軽減できるなど、一定の要件を満たす場合には、他の組織等にも通知しなければならない。小売業者がクレジットカード発行銀行又は法執行機関に通知する場合等が該当する。データ侵害を起こした組織は、侵害に関する全てを記録しなければならない。コミッショナーの要請があれば記録を提出しなければならない(改正後の第10.1条)。報告・通知義務や記録義務に違反する行為は、最高10万ドルの罰金に処せられる。

データ侵害とは、個人情報の紛失、無権限アクセス又は無権限開示であって、組織の安全保護措置違反又は係る措置を講じなかったことから生じるものをいう(第2条1項)。「重大な被害」には、身体的被害、侮辱、名誉又は関係性の侵害、雇用、事業又は職業上の機会の喪失、財政的損失、なりすまし、信用記録への悪影響及び財産的損失が含まれる。

データ侵害報告制度の改正は、カナダ産業省による連邦規則が制定された後に施行される。その他は女王の裁可を得た2015年6月18日に施行された。

33) S.C. 2010, c. 23.

34) Bill S-4.

35) 1年から45日以内に変更された。

36) 2015, c.32, s.10.

(3) 同意とプライバシー

コミッショナーは、2016年5月、「同意とプライバシー」と題する討議文書を公表した。これは、PIPEDAの要は同意であるという認識に基づき、スマートフォン、クラウド・コンピューティング等の技術や、個人情報への無制限アクセス及び自動処理等の企業実務の変化を踏まえ、同意モデルの改善又は代替策の提案、主たる論点の概要を述べること等を内容とする³⁷⁾。個人は、ビッグデータ・IoT (Internet of Things) によるビジネスモデルが変化する中で、プライバシーに関する意思決定の責任を負わされているが、一旦組織に収集された情報について、何が生じているかを完全に理解することはできない。そこで、報告書では、1) 同意の強化、2) 同意の代替策、3) アカウンタビリティに基づくガバナンス、4) 執行モデルの見直しを検討事項に掲げている。

1) では、プライバシーポリシー及び通知における透明性の向上、メタデータのタグ付け等によるサービスを跨いだプライバシー選好の管理、技術特有の安全保護措置の設定、プライバシーの初期設定 (PbD)、2) では、匿名化、「禁止区域」(“No-Go Zones”) の設定、適法な事業上の利益のための例外の拡大、3) では、実務規範による透明性及び公開性、プライバシー・トラストマークの設定、自主的取組がそれぞれ列挙されている。

2) のうち、「禁止区域」は、個人情報の収集、利用及び開示を通常人が当該状況で適切と考える目的のためにのみ認めることを定める第5.3条を発展させ、不適切な利用を禁止するという考え方である。また、報告書では、「注意ゾーンを進める」(“Proceed with Caution Zones”) と題し、機微情報などの特定種類の情報、自動化された個人に関する決定やプロファイリングなどの特定の取扱い、又は一定の脆弱な集団を保護するための手続を強化するという考え方も示されている。

4) では、命令権限を持たないというコミッショナーの問題意識が明らかにされている。

III 州 法

1 特 徴

個人情報保護法は、全ての州で制定されている。いくつかの特徴を挙げると、次の通りである。

情報自由及びプライバシー保護法 (Freedom of Information and Protection of Privacy Act, FIPPA, FOIP, FOIPP) は、公的機関に適用され、情報へのアクセス権及び個人情報の取扱いに関する一定の規律を定める³⁸⁾。この法令は全ての州で定められている。同法に加え、いくつかの州では、地方の公的機関に関する情報自由及びプライバシー保護法が制定されている。

個人情報保護法 (Personal Information Protection Act, PIPA) は、民間事業者に適用され、個人情報の取扱いに関する一定の規律を定める³⁹⁾。民間事業者に適用される一般法は、一部の州が制定している。

健康情報の保護に関する各法令は、医療分野に特化したものであり、医療従事者が管理する健康情報へのアクセス権を個人に与えるとともに、健康情報の取扱いに関する規律を定める。

プライバシー法 (Privacy Act) を定める州もある。これは、連邦のプライバシー法とは異なり、プライバシー侵害を不法行為とし、損害賠償や差止請求を認めるものである。

監督機関については、情報プライバシー・コミッショナー (Information and Privacy Commissioner) を設置する州が多い。拘束的命権限を有する監督機関もあれば、オンブズマンを設置する州、委員会制を採用する州もある。監督機関は、情報へのアクセス権に関する不服申立ての調査、仲裁及び解決、プライバシーに関する苦情の調査及び解決、違反事例の職権調査、立法提案、計画又は方針に関する意見提供、新技術及び/又はデータ・マッチング計画とプライバシーとの関連性に関する意見提供、アクセス権とプライバシー権に影響を与えるあらゆる事項の調査、一般への啓蒙とい

37) OPC, *Consent and Privacy* (May, 2016), https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/.

38) 州によって略称は異なる。

39) 同上。

った権限を有する。監督機関の命令権限がない場合は、裁判所への申立手続が設けられている。監督機関は、州議会に属する独立官であること、州議会に任命されること、州議会に直接報告を行うことなどによって、独立性が担保されている。

2 ブリティッシュ・コロンビア (British Columbia) 州

(1) 主な法令

- ・情報自由及びプライバシー保護法 (FIPPA)⁴⁰⁾ : 1992年6月制定。
- ・個人情報保護法 (PIPA)⁴¹⁾ : 2003年10月23日制定。同法は、2004年10月12日、PIPEDAと「実質的に類似」する法令であると認められている。同法第30.1条は、公的機関の管理する個人情報について、原則としてカナダ内でのみ保存及びアクセスしなければならない旨を定めている。データローカライゼーションを定めた規定である。
- ・電子健康 (個人健康情報へのアクセス及びプライバシー保護) 法 (E-Health (Personal Health Information Access and Protection of Privacy) Act)⁴²⁾
- ・プライバシー法⁴³⁾

(2) 監督機関⁴⁴⁾

情報プライバシー・コミッショナーは、1993年に設立された。コミッショナーは、FIPPA及びPIPAの監督権限を有する。現コミッショナーはドリュー・マッカーサー (Drew McArthur) 氏である。コミッショナーには拘束的命令権限がある。

3 アルバータ (Alberta) 州

(1) 主な法令

- ・情報自由及びプライバシー保護法 (FOIP)⁴⁵⁾ :

1994年6月制定, 1995年10月1日施行。

- ・個人情報保護法 (PIPA)⁴⁶⁾ : 2003年12月4日制定, 2004年1月1日施行。同法は、2004年10月12日、PIPEDAと「実質的に類似」する法令であると認められている。2010年5月1日の改正によりプライバシー侵害通知の制度が導入された。
- ・健康情報法 (Health Information Act, HIA)⁴⁷⁾ : 同法に基づきプライバシー影響評価が義務づけられている。

(2) 監督機関⁴⁸⁾

独立監督機関は、情報及びプライバシー・コミッショナーである。現コミッショナーは、ジル・クレイトン (Jill Clayton) 氏である。コミッショナーは、拘束的命令権限を有している。

コミッショナーは、上記3つの法令の監督権限に加え、自動車情報アクセス規則 (Access to Motor Vehicle Information Regulation) に基づく審査権限を有する。

4 サスカチュワン (Saskatchewan) 州

(1) 主な法令

- ・情報自由及びプライバシー保護法 (FOIP)⁴⁹⁾ : 1991年制定, 1992年4月1日施行。
- ・地方機関の情報自由及びプライバシー保護法 (LA FOIP)⁵⁰⁾
- ・健康情報保護法 (Health Information Protection Act, HIPA)⁵¹⁾

(2) 監督機関⁵²⁾

独立監督機関は、情報プライバシー・コミッショナーである。現コミッショナーは、ロナルド・J・クルゼニスキー (Ronald J. Kruzeniski) 氏である。

コミッショナーは、上記3つの法令に基づく監督を行うが、命令権限は有しない。

40) R.S.B.C. 1996, c. 165.

41) S.B.C. 2003, c. 63.

42) S.B.C. 2008, c. 38.

43) R.S.B.C. 1996, c. 373.

44) Office of the Information & Privacy Commissioner for British Columbia, <https://www.oipc.bc.ca/> (last visited Jan. 20, 2017).

45) R.S.A. 2000, c. F-25.

46) S.A. 2003, c. P-6.5.

47) R.S.A. 2000, c. H-5.

48) Office of the Information and Privacy Commissioner of Alberta, <https://www.oipc.ab.ca/legislation.aspx>, (last visited Jan. 20, 2017).

49) S.S. 1990-91, c. F-22.01.

50) S.S. 1990-91, c. L-27.1.

51) S.S. 1999, H-0.021.

52) Office of the Saskatchewan Information and Privacy Commissioner, <http://www.oipc.sk.ca/> (last visited Jan. 20, 2017).

5 マニトバ (Manitoba) 州

(1) 主な法令

- ・情報自由及びプライバシー保護法 (FIPPA)⁵³⁾ : 1997年6月28日制定, 1998年5月4日施行。
- ・個人健康情報法 (Personal Health Information Act, PHIA)⁵⁴⁾ : 1997年6月28日制定。
- ・プライバシー法⁵⁵⁾

(2) 監督機関⁵⁶⁾

独立監督機関はマニトバ州のオンブズマンである。現在は、シャーリーン・パキン (Charlene Paquin) 氏が務めている。オンブズマンには、FIPPA 及び PHIA に加えて、オンブズマン法、公益開示 (内部通報者保護) 法 (Public Interest Disclosure (Whistleblower Protection) Act, PIDA) に基づく苦情調査権限が与えられている。

その他、オンブズマンは、死亡調査法に基づく検視報告書の勧告、児童及び家族サービス法に基づく児童死亡審査報告書の勧告の実施を監督している。

6 オンタリオ (Ontario) 州

(1) 主な法令

- ・情報自由及びプライバシー保護法 (FIPPA)⁵⁷⁾ : 1988年1月1日制定。
- ・地方情報自由及びプライバシー保護法 (Municipal Freedom of Information and Protection of Privacy Act, MFIPPA)⁵⁸⁾ : 1991年1月制定。
- ・個人健康情報保護法 (Personal Health Information Protection Act, PHIPA)⁵⁹⁾ : 2004年5月20日制定, 同年11月1日施行。同法は、2005年11月28日に PIPEDA と「実質的に類似」する法令であると認められている。

(2) 監督機関⁶⁰⁾

独立監督機関は、情報プライバシー・コミッショナーである。現コミッショナーは、ブライア

ン・ビーミッシュ (Brian Beamish) 氏である。コミッショナーは上記各法令の監督を行い、命令権限も有している。

7 ケベック (Quebec) 州⁶¹⁾

(1) 主な法令

唯一のフランス語圏であるケベック州は、公的部門及び民間部門の包括的法令を定めた州として、情報自由及び個人情報保護法のパイオニアといわれている。

ケベック州の人権及び自由憲章 (Charter of Human Rights and Freedoms)⁶²⁾ の第5条は、「何人もその私生活を尊重される権利を有する。」と定めており、プライバシー権を保障したものと解釈されている。個人情報保護に関する主な法令は次の通りである。

- ・公的機関が保有する文書へのアクセス及び個人情報保護を尊重する法律 (An Act respecting access to documents held by public bodies and the protection of personal information)⁶³⁾ : 1982年制定。
- ・民間部門における個人情報保護を尊重する法律 (An Act respecting the protection of personal information in the private sector) : 1993年6月制定, 1994年1月1日一部を除いて施行。同法は、2003年12月11日、PIPEDA と「実質的に類似」する法令であると認められている⁶⁴⁾。
- ・ケベック州民法第35条～第41条 (Extracts from the Civil Code of Québec, articles 35 to 41)⁶⁵⁾

ケベック州民法は、第2編第3章に「名誉及びプライバシーの尊重」を設け、第35条で「何人も、自己の名誉及びプライバシーを尊重される権利を有する」と定めている。第36条は、プライバシーの侵害態様、第37条は、他者に関するファイルを作成する者は、重大かつ適法な理由を有しなければならないこと、第38条は、本人によ

53) C.C.S.M., c. F175.

54) C.C.S.M., c. P33.5.

55) C.C.S.M., c. P125.

56) Manitoba Ombudsman, <https://www.ombudsman.mb.ca/> (last visited Jan. 20, 2017).

57) R.S.O. 1990, c. F.31.

58) R.S.O. 1990, c. M.56.

59) S.O. 2004, c. 3, Schedule A.

60) Information and Privacy Commissioner of Ontario, <https://www.ipc.on.ca/> (last visited Jan. 20, 2017).

61) *Supra* note 11, at 4-95-4-110.

62) R.S.Q., c. C-12.

63) R.S.Q., c. A-2.1.

64) R.S.Q., c. P.39-1. PIPEDA の憲法適合性及び EU の十分性との関係は、前記 II 1 参照。

65) C.C.Q.-1991. 1991, c.64.

るファイルの閲覧及び訂正権、第39条は、ファイルを作成する者は、ファイルに含まれる情報への当該個人のアクセスを拒否してはならないこと、第40条は、ファイルの正確性、完全性、確実性、第41条は、個人の権利行使の条件及び態様を決定する裁判所の権利を定めている。

上記の民間部門における個人情報保護法は、民法第35条から第40条の定める権利行使のために、民法第1525条⁶⁶⁾の意味する事業活動の過程で、他者に関する個人情報の収集、保有、利用又は第三者への提供についての特定の規則を設けることにある。民法を補完するために制定された法律という点においても特殊性がある。

(2) 監督機関

情報プライバシー委員会 (Commission d'accès à l'information du Québec) が監督権限を有する。委員長はジャン・シャルティエ (M^e Jean Chartier) 氏である⁶⁷⁾。委員会は委員長及び副委員長を含めて最低5名で構成され、監視部門及び仲裁部門に分かれている。委員は、首相の申し立てに基づき、州議会の3分の2以上の賛成により任命される。

委員会の監視部門は、公的部門の法令について、法の適用及び法が遵守されている程度を調査する、公的機関同士で締結された合意を承認する、本法に基づく規則案等への意見を述べる、個人情報の提供に関する登録簿を保持するための規則を定める、公的機関が保有するファイル内の個人情報の機密性が保持されているか否かを確認する、といった権限を有する。委員会は、ファイルに含まれる個人情報の機密性が尊重されているか等を調査し、必要に応じて命令を下す権限を有する。委員会は、文書へのアクセスや個人情報保護に関する拒否決定を受けた個人の申立てを審査する権限を有する。委員会は、当事者の権利を保護するために適切を考える命令を下し、事実又は法に関するあらゆる問題を判断することができる。

委員会は、民間部門の法令については、個人情報へのアクセス若しくは訂正、又は、利害関係人から提出されたマーケティングリストに関する第25条⁶⁸⁾の適用についての争いを調査し、決定を下す権限を有する。委員会には、個人情報保護に関するあらゆる事柄や企業による情報の取扱実務について、職権又は苦情申し立てにより、調査を行う権限を有し、勧告又は命令を下す権限を有する。委員会は、5年ごとに州議会に民間部門法の適用に関する報告書を提出しなければならない。

8 プリンズ・エドワード・アイランド (Prince Edward Island)

(1) 主な法令

・情報自由及びプライバシー保護法 (FOIPP)⁶⁹⁾ : 2001年5月15日制定, 2002年11月1日施行。

(2) 監督機関

情報プライバシー・コミッショナーが監督権限を有する。現コミッショナーは、カレン・A・ローズ (Karen A. Rose) 氏である。コミッショナーには拘束的命権限が与えられている。

9 ニュー・ブランズウィック (New Brunswick) 州

(1) 主な法令

・情報への権利及びプライバシー保護法 (Right to Information and Protection of Privacy Act, RTIP-PA)⁷⁰⁾ : 2009年6月19日制定, 2010年9月1日施行。同法は、1998年個人情報保護法及び1978年情報権法を廃止する形で制定された。

・個人健康情報のプライバシー及びアクセス法 (Personal Health Information Privacy and Access Act)⁷¹⁾ : 2009年6月19日制定。同法は、2011年11月17日、PIPEDAと「実質的に類似」する法令であると認められている。

66) 1名以上の者が組織的な経済活動を実施することは、本質的に営利的であるか否かにかかわらず、財の生産、管理、譲渡、又はサービスの提供で成り立っており、それは事業活動を構成する。

67) Commission d'accès à l'information du Québec, <http://www.cai.gouv.qc.ca/> (last visited Jan. 20, 2017).

68) 何人も、自己に関する個人情報をマーケティングリス

トから除外して欲しい場合は、いつでも、リストの保有者又は利用者に対し、口頭又は文書の請求により、情報を削除させる権利を有する。

69) C. F-15.01.

70) S.N.B. 2009, c. R-10.6.

71) S.N.B. 2009, c. P-7.05.

(2) 監督機関⁷²⁾

情報アクセス・プライバシー・コミッショナーが監督権限を有する。現コミッショナーは、アン・E・バートランド (Anne E. Bertrand) 氏である。RTIPPA の制定以前は、オンブズマン法に基づく監督制度が設けられていたが、RTIPPA に基づき、新たにコミッショナーが設置された。旧法との違いは、コミッショナーに苦情調査権限が与えられた点である。ただし、コミッショナーに命令権限はない。

10 ノバ・スコティア (Nova Scotia) 州

(1) 主な法令

- ・情報自由及びプライバシー保護法 (FIPPA)⁷³⁾ : 1993 年制定, 1994 年施行。
- ・地方政府法⁷⁴⁾ : 1999 年制定。地方の情報自由及びプライバシー保護法である。
- ・プライバシー審査官法 (Privacy Review Officer Act, PRO Act)⁷⁵⁾ : 2009 年 9 月制定。この法律は、市民が州の公的機関によってプライバシーを侵害されたと感じた場合には、コミッショナーに苦情を申し立てることができる。
- ・個人健康情報法 (PHIA)⁷⁶⁾ : 2012 年 5 月制定, 2013 年 6 月 1 日施行。
- ・個人情報国際開示保護法 (Personal Information International Disclosure Protection Act)⁷⁷⁾ : 同法は、州のデータ・ローライゼーション法である。公的機関及び地方政府は、それらが保有するあらゆる個人情報 (サービス提供者が代わりに行動する場合を含む) が、原則として、カナダ内に保持され、カナダ内でのみアクセスされ、開示されることを保障する義務を負う。

(2) 監督機関⁷⁸⁾

情報プライバシー・コミッショナーが監督権限

を有する。現コミッショナーは、キャサリン・トゥリー (Catherine Tully) 氏である。コミッショナーは、独立のオンブズパーソンであり、命令権限を有しない。

11 ニューファンドランド&ラブラドル (Newfoundland & Labrador) 州

(1) 主な法令

- ・2015 年情報へのアクセス及びプライバシー保護法 (Access to Information and Protection of Privacy Act, ATIPPA)⁷⁹⁾ : 2015 年 6 月 1 日制定。同法については、2005 年施行の情報自由法が存在していたが、見直しにより新法が制定された。
- ・個人健康情報法 (Personal Health Information Act, PHIA)⁸⁰⁾ : 2008 年 6 月 4 日制定。同法は、2012 年 10 月 10 日に PIPEDA と「実質的に類似」の法令である旨の認定を受けている。
- ・プライバシー法⁸¹⁾

(2) 監督機関⁸²⁾

ATIPPA 及び PHIA の監督は、情報プライバシー・コミッショナーが担っている。現コミッショナーは、ドノヴァン・モロイ (Donovan Molloy) 氏である。命令権限は付与されていないが、勧告を執行するために裁判所への申立を行うことができる。

12 ユーコン (Yukon) 準州

(1) 主な法令

- ・情報アクセス及びプライバシー保護法 (Yukon AIPPA)⁸³⁾
- ・健康情報プライバシー及び管理法 (Health Information Privacy and Management Act, HIPMA)⁸⁴⁾ : 2016 年 8 月 31 日施行。

72) Office of the Access to Information and Privacy Commissioner, New Brunswick, <http://www.info-priv-nb.ca/> (last visited Jan. 20, 2017).

73) 1993, c. 5. 1977 年に情報自由法を制定した最初の州である。

74) 1998, c. 18.

75) 2008, c. 42.

76) 2012, c. 31.

77) 2006, c. 3.

78) Office of the Information and Privacy Commissioner, Nova Scotia, <https://foipop.ns.ca/> (last visited Jan. 20, 2017).

79) S.N.L. 2015, c. A-1.2.

80) S.N.L. 2008, c. P-7.01.

81) R.S.N.L. 1990, c. P-22.

82) Office of the Information and Privacy Commissioner, <http://www.oipc.nl.ca/> (last visited Jan. 20, 2017).

83) R.S.Y. 2002, c.1.

84) S.Y. 2013, c. 16.

(2) 監督機関⁸⁵⁾

情報プライバシー・コミッショナーが監督権限を有する。現コミッショナーは、ダイアン・マクレオド・マッケイ (Diane McLeod-McKay) 氏である。オンブズマン法に基づき指名される。

13 ヌナブト (Nunavut) 準州

(1) 主な法令

・情報アクセス及びプライバシー保護法 (ATIPP)⁸⁶⁾ : 1996年12月31日及び2007年12月31日施行。

(2) 監督機関⁸⁷⁾

情報プライバシー・コミッショナーが ATIPP の監督権限を有する。現コミッショナーは、エレイン・ケナン・ベンゲ (Elaine Keenan Bengts) 氏である。命令権限はない。

14 ノースウェスト準州 (Northwest Territories)⁸⁸⁾

(1) 主な法令

・情報アクセス及びプライバシー保護法 (ATIPP)⁸⁹⁾ : 1996年12月31日施行。
・健康情報法⁹⁰⁾ : 2015年10月1日施行。

(2) 監督機関

ヌナブト準州と同様、エレイン・ケナン・ベンゲ氏である。

IV プライバシー・バイ・デザイン⁹¹⁾

プライバシー・バイ・デザイン (PbD) は、カナダ・オンタリオ州の前情報プライバシー・コミ

ッショナーである、アン・カブキアン (Ann Cavoukian) 博士が、1990年代から提唱してきた考え方である。カブキアン博士は、現在は、トロントにあるライアソン大学 (Ryerson University) のプライバシー・ビッグデータ研究所 (Privacy & Big Data Institute) の常任理事を務めている。

PbD の概要は次の通りである⁹²⁾。

PbD は、様々な技術に関する設計仕様の中に、プライバシーを組み込むという考え方及びアプローチをいう。これは、「公正情報実務」(Fair Information Practices) に関する諸原則を、情報処理技術及びシステムの設計、運用及び管理の中で確立させることによって達成することができる。このアプローチは、(1)情報技術、(2)事業活動、並びに、(3)物理的設計及びインフラに適用される。

PbD は、プライバシー促進技術 (PETs) に「ポジティブサム」のアプローチを加えた考え方であり、PbD は、プライバシー影響評価 (Privacy Impact Assessment, PIA) のもととなる概念である。カブキアン博士の説明で最も強調されているのは、「ポジティブサム」への発想の転換と、PbD がプライバシーとセキュリティの「両者に有利」となることである。

最近では、PbD の認証制度も開始されており、認証を受けた事業者も登場している⁹³⁾。PbD の目的は、次の基本7原則を遵守することで、プライバシーと個人の情報へのコントロールを保障し、組織が持続的に競争上の優位を得ることにある。

PbD の7原則は次の通りである⁹⁴⁾。

「1 事後的ではなく事前的、救済的ではなく予

85) Yukon Information and Privacy Commissioner, <http://www.ombudsman.yk.ca/> (last visited Jan. 20, 2017).

86) S.N.W.T. (Nu) 1994, c.20.

87) Information and Privacy Commissioner of Nunavut, <http://www.info-privacy.nu.ca/> (Jan. 20, 2017).

88) <https://www.justice.gov.nt.ca/en/access-to-information-held-by-public-bodies/https://www.justice.gov.nt.ca/en/files/legislation/access-to-information-and-protection-of-privacy/access-to-information-and-protection-of-privacy.a.pdf> <https://www.justice.gov.nt.ca/en/files/legislation/health-information/health-information.a.pdf>

89) S.N.W.T. 1994, c.20.

90) S.N.W.T. 2014, c.2.

91) 新保・前掲「プライバシー・バイ・デザイン」参照。

92) Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Jan. 2011), <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>.

93) Privacy and Big Data Institute, <http://www.ryerson.ca/pbdi/privacy-by-design/certification/> (last visited Jan. 20, 2017).

94) Information & Privacy Commissioner, Ontario, Canada, *Privacy by Design, 7 Foundational Principles*, <http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/> (last visited Jan. 20, 2017). 邦訳は、堀部政男・JIPDEC 編・前掲『プライバシー・バイ・デザイン—プライバシー情報を守るための世界的新潮流』参照。

防的であること。

プライバシー・バイ・デザイン（PbD）のアプローチは、事後的よりもむしろ事前的措置により特徴付けられる。それは、発生前にプライバシー侵害事象を予測し、予防する。PbDは、プライバシーリスクの顕在化を待つものでもなければ、プライバシー違反が一旦発生してからそれを解決するための救済を提供するものでもない—それは、それらの違反が発生するのを予防することを目的としている。要するに、プライバシー・バイ・デザインは、事象の後ではなく、前に来るものである。

2 初期設定としてのプライバシー

我々は皆、あること—初期設定ルール—を確信することができる！プライバシー・バイ・デザインは、あらゆる所与のITシステム又は事業活動の中で自動的に個人データが保護されるよう保障することによって、最大限のプライバシーを提供しようとしている。個人が何もしない場合、彼らのプライバシーはいまだ無傷で維持される。自己のプライバシーを保護するために個人の側で求められることは何もない—それはシステムに初期設定で組み込まれている。

3 設計に組み込まれるプライバシー

プライバシー・バイ・デザインは、ITシステム及び事業活動の設計及び構造に組み込まれる。それは事象が起きた後の付属に留めるものではない。その結果、プライバシーは、提供されている中心機能の本質的構成要素となる。プライバシーは、機能性を損なうことなくシステムに不可欠なものである。

4 全機能性—ゼロサムではなくポジティブサム

プライバシー・バイ・デザインは、不必要なトレード・オフがなされるときに、時代遅れのゼロサムアプローチを通じるのではなく、ポジティブサムの「両者に有利な」(win-win) 態様で、全ての適法な利益及び目的を収めようとしている。プライバシー・バイ・デザインは、両者を有することが可能であると証明することで、プライバシー対セキュリティのように、誤った見せかけの対立

を回避する。

5 生成から廃棄までの安全性—ライフサイクル全般の保護

プライバシー・バイ・デザインは、情報が収集される最初の要素に先立って、システムに組み込まれており、当該データの全ライフサイクルにわたり安全に拡張される—強力な安全保護措置は最初から最後までプライバシーにとって本質的である。このことは、全てのデータが安全に保持され、そして、取扱いの最後の段階で、適時に安全に破棄されることを保障する。このように、プライバシー・バイ・デザインは、ゆりかごから墓場まで、端から端まで安全な情報管理のライフサイクルを保障する。

6 可視性と透明性—継続的開示

プライバシー・バイ・デザインは、全ての利害関係者において、いかなる事業活動又は技術が関係しようとも、実際に、独立の検査に従い、宣言した約束及び目的に従い運用していることを保障しようとする。その構成部分及び運用は、利用者に対し、また、提供者にも同様に、可視性及び透明性を維持する。信用するが確認することを覚えておくこと。

7 利用者のプライバシーを最大限に尊重すること—利用者中心の維持

とりわけ、プライバシー・バイ・デザインは、設計者及び運用者に対し、強力なプライバシーの初期設定、適切な通知、及び利用者にとって親切な選択肢の付与といった措置を提供することで、個人の利益を最高に維持することを求める。利用者中心の維持。」

PbDのプライバシーは、1983年のドイツの国勢調査判決が「情報自己決定権」に言及したことに由来している⁹⁵⁾。プライバシーは、何かを隠すこと（秘密性）ではなく、コントロールできることを意味する。

PbDが国際的に広く認知を受けるきっかけとなったのは、2010年10月に開催された第32回データ保護・プライバシー・コミッショナー国際

95) 国勢調査判決については、藤原静雄「西ドイツ国勢調査判決における「情報の自己決定権」」一橋論叢第94巻5号

(1985年) 728-746頁参照。

会議における、PbDに関する決議である⁹⁶⁾。PbDは、2012年3月26日に米国の連邦取引委員会が公表した「プライバシーレポート」⁹⁷⁾の3本柱の1つに掲げられ、EUの一般データ保護規則⁹⁸⁾では、第25条「データ保護・バイ・デザイン及びバイ・デフォルト」として導入された。日本では、衆議院内閣委員会の2015年5月20日付「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に対する附帯決議」⁹⁹⁾及び参議院内閣委員会の2015年8月27日付同法律案に対する附帯決議¹⁰⁰⁾の中で、PbDへの言及がある。PbDは、カナダの法令の中では立法化されておらず、また、そもそも立法化を前提とする考え方ではないが、その考え方は世界的な広がりを見せている。

PbDを実装する技術や分野に制限はないが、2012年に公表された「PbDの運用」(Operationalizing Privacy by Design)¹⁰¹⁾の中で、9つの適用分野が紹介されている。具体的には、監視カメラ、バイオメトリクス、スマート・メーター及びスマート・グリッド、モバイル機器/通信、近距離無線通信(Near Field Communication)、RFID及びセンサー技術、IP位置情報、遠隔医療、ビッグデータ及びデータ分析に用いることができるとされている。

ビッグデータ、IoT、さらには人工知能(Artificial Intelligence)が発展する中で、PbDの重要性に疑いの余地はないと考えられる。他方、PbDの実現には技術的措置が不可欠であり、諸原則を具体化する際の工夫と努力が必要となる。

V おわりに

カナダの国内法を概観すると、オンブズマンであることによる権限の制限、PIAの立法化、データ侵害通知の立法化、州法と連邦法の管轄、州法特有の規制(データ・ローカライゼーション法)、十分性認定への影響といった問題が存在する。

オンブズマンは、連邦と多くの州が取り入れている制度であるが、特に連邦のコミッショナーの判断に拘束力を持たせるか否かが課題となる。この点は、独立監督機関による強力な法執行を掲げるEUから見た場合には、弱点となり得る。州のコミッショナーの中には命令権限を有するものもある。連邦政府の関係者からは、現行制度を変更してまで命令権限を付与する必要はないとの意見も聞かれるが、国際的協力も行う執行機関にとって、権限強化は最大の課題であり続ける。

PIAは立法化を必須とする仕組みではなく、連邦政府では、指令に基づき実施されてきた。しかし、ビッグデータ時代の中で、個人情報の取扱いへの効果的ガバナンスを行うためには、特に政府部門において立法化する意義はあると考えられる。国際的にも、EUの一般データ保護規則では、「データ保護影響評価」として立法化されている。日本でも、マイナンバー法(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)に基づく特定個人情報保護評価が実施されている。

データ侵害通知は、侵害を犯した側に報告のインセンティブがないことから、立法による義務づけを必要とする制度である。アルバータ州の民間部門向け個人情報保護法及びPIPEDAの改正により、民間事業者の侵害通知が義務化されること

96) 32nd International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy by Design (Oct. 2010), <https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf>.

97) Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (Mar. 26, 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

98) Parliament and Council Regulation 2016/679, 2016 O.J. (L 119) 1-88 (EU).

99) http://www.shugiin.go.jp/internet/itdb_rchome.nsf/html/rchome/Futai/naikaku28215527A5B4800A49257E4C00043F53.htm.

100) http://www.sangiin.go.jp/japanese/gianjoho/ketsugi/189/f063_082701.pdf.

101) Ann Cavoukian, *Operationalizing Privacy by Design* (Dec. 2012), <http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf>.

となった。データ侵害通知（セキュリティ侵害通知）は米国カリフォルニア州法を発祥として各州に広まった制度であり、EUの一般データ保護規則でも、「個人データ侵害通知」として立法化されている。日本でも、2015年9月3日のマイナンバー法改正により、個人情報保護委員会への漏えい報告制度が導入された。

州法と連邦法の管轄は国内法の問題であり、明文が存在しないことに原因がある。また、カナダは連邦優位の制度を採用しているものの、ケベック州ではプライバシー・個人情報保護の分野で先んじて立法化に踏み切ったという経緯も管轄問題を複雑化させていると考えられる。このような認識の食い違いは、十分性認定にも影響している。一部の関係者からは「実質的に類似」するとの判断を受けたケベック州において、第29条作業部会から否定的評価を受けたことは、PIPEDAの十分性認定にも影響を与えかねないとの声が上がっている。EUの一般データ保護規則では、十分性認定を4年ごとに定期審査する規定を新設していることから、PIPEDAもEUの規律を意識する形で改正を求められることが予想される。

データ・ローカライゼーション法は、クラウド・コンピューティング・サービスの利用を妨げたり、個人データの自由な流通を阻害しかねないため、個人情報の保護と自由な流通のバランスを図るという、個人情報保護制度の理念に沿わない制度といえる。実際、ロシアの監督機関が、2016年11月10日のモスクワ市裁判所決定を受け、国内のデータ・ローカライゼーション法に基づき、LinkedInのウェブ・サイトをブロックするという事態も生じている¹⁰²⁾。カナダのデータ・ローカライゼーション法は、ブリティッシュ・コロンビア州やノバ・スコティア州の政府機関のみに適用されるものであるが、この法令の存在意義は慎重に考えるべきと思われる。

PIPEDAの議論において注目すべきは、「同意」の考え方である。PIPEDAの2015年改正法は同意の判断に「個人の合理的期待」を明文で取り入れ、連邦のコミッショナーは、「同意とプラ

イバシー」の中で、通常人が不適切と考える個人情報の収集、利用及び開示を「禁止区域」として禁止するという考え方を提案した。効果的な「同意」の議論が深化すれば、日本の法解釈にとっても参考にすることができる。

PbDは、カナダの中でも特殊な取組であり、国際的な存在感を高めることに重要な役割を果たしている。日本でも、関係者の間でPbDは知られるようになってきているが、理念を理解するのみならず、いかに実装するかという技術的な具体論を進める必要がある。

カナダが国際的動向を踏まえつつ、同時に国内の問題を解決しなければならないのは、日本と共通している。カナダの議論は日本にとっても示唆を得られるものが多いと考えられることから、その状況には常に目を向ける必要がある。

102) Privacy Laws & Business, International e-news, *Russia blocks LinkedIn as a result of data localisation*

requirement (Nov. 17, 2016), http://www.privacylaws.com/Int_e-news_18_11_16.