プライバシー影響評価制度の検討

北　原　宗　律

（受付　2012 年 10 月 31 日）

1. は　じ　め　に

1970年代初頭，OECD 加盟諸国を中心に，個人情報処理をめぐる議論が沸騰した。国の行政機関における個人情報のコンピュータ処理が情報主体たる本人の権利利益を侵害するか否かということに，その議論の焦点が当てられた。

そして，およそ四〇年を経た二一世紀の今日において，個人情報（個人データ）およびプライバシーをめぐる状況が様変わりしつつある。個人情報保護の議論が個人データのコンピュータ処理がその契機となったことを思い起こせば，今回も，やはり，情報技術がその「様変わり」に大いに関わっているといえる。

Web2.0により，誰でもインターネット参加ができるようになり，その結果，いわゆる「ソーシャルメディア」の一大繁栄を迎えることになる。SNS，Twitter，Blog 上に並べられる膨大な量の個人情報やプライバシー情報がビッグデータ・ビジネスに吸い込まれている。個人情報の情報主体はこのビジネスに何の声も上げることができない。

もうひとつは，いわゆる「クラウド」（Cloud）の発生である。個人情報を含めて，あらゆる情報を，あの空に浮かぶ「雲」の上に置いておくのであるから，誰もがその安全性について不安に思うのも頷ける。

このような情報技術環境の変遷を踏まえて，個人情報やプライバシーの尊重が情報社会における最重要課題と考える立場から，それらの持続可能な保護措置が，様々な方法で提起されている。

そこで，本小論の目的は，個人情報やプライバシー保護に関する措置を検討することである。ここで取り上げるのは，いわゆる「プライバシー影響評価制度」である。従来型の保護制度において，ほとんどが，いわば「事後的問題解決型」であるといえる。そういう意味で，プライバシー影響評価制度を，いわば「事前問題検証型」であると捉えている。

本小論において，まず，プライバシー影響評価の定義について検討する(2)。つぎに，プライバシー影響評価の目標(3)，ならびに，プライバシー影響評価後の成果(4) について検討を加える。最後に，プライバシー影響評価の実施について検討する(5)。

2. プライバシー影響評価の定義

2.1 評価プロセス

プライバシー影響評価（PIA: Privacy Impact Assessment）は，個人情報処理を含む，プロジェクト，ポリシー，プログラム，サービス，製品，または，創業におけるプライバシーへの影響（impact）を評価（assess）し，そして，その消極的影響を回避もしくは最小化するための一手法である［1］。PIA は，可能な限り最も早い段階で開始されるべきである。それでもなおプロジェクトの成果に影響を及ぼすようなものが残されている。したがって，そのプロジェクトが展開するまで，そして展開後までも，PIA は継続さるべきである。最善の PIA は，その最初から，ステークホルダーに対して，プライバシー侵害の影響がどのように回避または最小化されたかについての見解・構想を集約する方法を提供しているのである［2］。

カナダでは，PIA は，以下のように考えられている。すなわち，PIA は，新規の，技術や情報システム及び創業，または，提唱されたプログラムやポリシーが，基本的なプライバシー要求事項を充足しているかどうかを判断する国の省庁や部局を支援するプロセスである。PIA は，また，政府機関があるプロジェクト提案のプライバシー影響への反応を予知し，結果として，影響が甚大なプログラム，サービス，もしくはプロセスの再設計を防止することにも資するものである［3］。

2009年 5 月に，ヨーロッパ委員会が，いわゆる「RFID 勧告」（「電波認証に関する勧告」）を公表した。同勧告において，同委員会は，電波認証（RFID: Radio Frequency Identification）システムにおける個人データ・プライバシー影響評価（Personal Data and Privacy Impact Assessments）の要求事項を確定した。その中での定義は以下の通りである。すなわち，「PIA とは，特定の RFID システムにおけるプライバシー及びデータ保護の影響を回避または少なくとも削減するための適切な措置を講ずるという意図のもとに，RFID システムのプライバシー・データ保護の影響を評価するための意識的・体系的努力が実行されるプロセスである」［4］。

2.2 評価ツール

オーストラリアでは，プライバシー影響評価は，以下のように捉えられている。すなわち，「PIA は，一つの評価ツールであって，プロジェクトにおける個人情報の流れを記述し，そして，そのさまざまな個人情報の流れおよびそのプロジェクト全体が個人のプライバシーに与える想定可能なプライバシー影響を分析するものである」。つまり，プライバシーの観点から当該プロジェクトのストーリーを描いているのである。したがって，PIA 実施の目的は，プ

ライバシーの影響を管理・最小化・根絶するための諸措置を特定し，推奨することであるといえる［5］。

2.3 「環境影響評価」との関連

「プライバシー*影響評価*」（PIA: privacy *impact assessment*）と「環境*影響評価*」（EIA: environmental *impact assessment*）において，いずれも，リスクの事前評価的手法等を用いることで，両者間に共通点を見出そうとしている。ただ，その評価対象において，一方は「プライバシー・リスク」であり，他方は「環境・リスク」である点が異なるのであるという［5a］。しかし，「プライバシー」は，まさに「個人」に関わる問題であり，「環境」は個人の集合体である「集団」に関わる問題というように解される。そうすると，その評価対象の本質的な差異が，相応の評価手法や評価結果を求めることになるのではないだろうか。したがって，両者の評価手法の大枠においてなら，いくつかの類似点を見出すことができるであろう。

3. プライバシー影響評価の目標

3.1 プライバシーリスクコミュニケーション

PIA の重要な目標のひとつは，プライバシー・リスクについて，効率的なコミュニケーションを図ることである。PIA は，組織の上位者の管理能力を以て，ポリシー，システム設計および調達決定を十分に周知徹底させるよう意図されている。そこでの特別ないくつかの目標を上げると，以下のようになる［6］。すなわち，a）市民との間に信用・信頼関係を築くこと，b）プライバシー問題の意識と理解を高めること，c）プロジェクトの目的と運用においてプライバシー保護が優先することを保証すること，d）プライバシー問題の明晰な説明責任を明示し，プロジェクトの管理者および共同運用者とも共有されていること，e）プライバシー要求事項に適合するために，プロジェクト稼働後のプログラムやサービスの停止もしくは実質的再検討のリスクを減少させること，f）周知のポリシー，システム設計または調達決定がプライバシーリスクの理解やリスク削減ために想定可能な諸措置に基づいて行われるよう必要な情報を決定権者に提供すること，g）業務プロセスおよび共通利用の個人情報の流れに関する基本書類，部局職員によるレビュー，ステークホルダーへの説明資料としての詳細資料，情報プライバシー手続，伝達記録などを提供すること。

3.2 プライバシー法適合性

PIA は，また，プロジェクトがプライバシー法やその他の関連法律の要求事項への適合を保証するために必要なことを明らかにしてくれる［7］。プライバシー法の諸原則は，個人情

報が処理される方法におけるプライバシー保護の最低限のものを規定しているに過ぎない。したがって，組織は，他のプライバシー関連の法律の要求事項，並びに，より一般的な公的あるいは民間機関の義務規定等にも適合しなければならない。このように，関連するプライバシー法への適合は，プライバシー影響の評価・管理にとって極めて基本的なことである。

PIA は，さらに，社会がプライバシーに与える価値を熟慮する機会を組織に提供してくれる。プライバシーだけではなく，信頼，尊厳，個人の自律や説明責任というものにも組織の目を向けさせてくれる。そして，それらの価値がプロジェクトに反映されることになる。その上，PIA は，プロジェクトの価値から，あるいは，プライバシー法の条項に追加されることもあるビジネス・ルールという観点から，プロジェクトそれ自体を評価する機会も提供してくれるものである［8］。

4. プライバシー影響評価後

4.1 推奨事項

PIA 実施後に一冊の報告書が作成される。報告書の中のすべての PIA 情報（分析情報・評価情報・その他の資料・記録）の活用は極めて有益なものである。その報告書には，当該プロジェクトの将来のための様々な推奨事項が含まれているはずである。プロジェクトのすべての構成要素に精緻に焦点を当てている PIA は，多様な推奨項目を連ねている［9］。

その PIA 報告書は，回避可能な影響やリスクを特定し，それらを除去する，もしくは受容可能レベルにまで減殺する方策を示唆してくれるはずである。例えば，a）プロジェクトの目標間，影響を受ける個々人の利害と当該組織の利害との間により均衡ある調整をもたらすような変更，b）さらなる協議の必要性，c）プロジェクトのプライバシー影響の重大性による当該プロジェクトの実施の是非，などである。

プライバシー影響分析報告書の中に，部局および外部機関は，提案の詳細な文書，プログラムやサービスにおけるデータフローの詳細なログ情報，および，プライバシー要求事項の適合情報を保有すべきである。これは，当該プロジェクト提案がさらに進捗する前に，解決する必要がある重大なプライバシー問題を確定するための有効な基礎的情報となるものである［10］。

4.2 決定ツール

PIA の実証，すなわち，その分析，評価，分析・評価結果，推奨事項の実証が進行中の，有効な意志決定ツールを提供している。そのドキュメントは，プロジェクトチーム，上位管理者およびその他のステークホルダーにとっての価値ある情報源となり，プロジェクトに参

入した者，もしくはプロジェクトに関わる者とコミュニケーションをとることができ，それらの者を教育することもできる［11］。PIA は当該プロジェクトの次の段階の計画の中に取り込まれていく。

5. プライバシー影響評価の実施

5.1 リスク管理

PIA は，方法論的には，リスクの評価・管理プロセスに基づいている。もし，個人データの取扱を実施している政府機関または民間企業，もしくはその他の組織が，プライバシー侵害を引き起こすような計画の実行を回避できるならば，それは，リスクを最小化したことになる。PIA 提案者たちは，個人を識別できる情報を収集・保有し，それらのリスクを特定・回避・最小化するための PIA の実施から様々な利益を得てきた組織にとっての多様なリスクを特定してきた［12］。

プライバシーリスクには多くの原因がある。リスクは，組織内の脆弱な部分から，あるいは，プロジェクトの設計や実行から発生することもある。また，リスクは外部の脅威，例えば，ソーシャルエンジニアリングの手口で人を騙したり，あるいは，組織のアクセスコントロールの弱点に乗じて欲しい情報を手に入れる悪意の行為者からもたらされることもある。特に，オーストラリア，カナダ，ニュージーランド，イギリスおよびアメリカ合衆国で用いられる PIA ガイドは，個人を識別できる情報の収集・保有組織が直面するリスクを特定している［13］。

5.2 プライバシー影響評価の実施

5.2.1 評価の開始

まず，評価を実施する当たって，PIA が必要かどうかを問うことがその最初の質問となる。すなわち，「当該プロジェクトにおいて，個人情報が収集・利用・提供されるのか？」と問わねばならない。これは，評価の出発点として知られている。もし，個人情報が，プロジェクトのいかなる段階においても含まれることがなければ，当該プロジェクトは，情報プライバシーに無視できる影響しか与えないということになり，PIA は必要ではなくなるだろう［14］。この段階では，評価テンプレートの「モジュール A」が利用される。つまり，テンプレート・モジュール A は，1）組織名，2）開始評価の責任者の情報，3）当該プロジェクトの概略情報，4）プロジェクトにおける個人情報の収集・利用・提供，というような質問項目で構成されている。

5.2.2　評価計画

プロジェクトの内容とその展開ステージが最善の PIA プロセスを確定する。この段階では，評価テンプレートの「モジュール B」が利用される。モジュール B は，当該プロジェクトのタイプと展開するステージに適合した評価テンプレートの指針と事例を明示している［15］。

プロジェクトの評価によって，組織は，最適な PIA プロセスを手に入れることができる。プロジェクト評価は，1）プロジェクトの範囲，2）プロジェクトのタイプ，3）プロジェクト展開のステージ，というような質問項目から構成されている。

5.2.3　情報の流れの描写とプライバシーフレームワーク

このプロセスが実行されるのは，プロジェクトにおける情報の流れとプライバシー関連立法と組織ルールを理解するためである［16］。ここで利用されるのは，評価テンプレートの「モジュール C」である。モジュール C は，想定できるプライバシー問題を特定し評価することができるようにプロジェクトの情報の流れを詳細に描いてくれる。

モジュール C は，プロジェクトの個人情報の流れを描写するためのものである。これは，プロジェクトのプライバシー影響を分析する基礎を形成する。すなわち，1）個人情報の収集，2）個人情報の利用と提供，3）自己に関する情報へのアクセス権，4）自己情報の修正権，5）セキュリティ措置，6）データの質を保証するプロセス，7）認証管理システム，というような質問項目から構成されている［17］。

5.2.4　プライバシー評価分析

データ管理者が情報の流れを描写したので，その管理者は，そのプロジェクトがプライバシーに対して積極的なもしくは消極的な影響をもたらすのかを詳細に分析する必要がある。この分析には以下の項目が含まれる［18］。すなわち，1）プライバシー影響の重大性の程度，2）その影響は必然か回避可能か，3）その影響とプロジェクト目標との関係，4）特定の個人情報の情報主体の選択権への影響，5）プロジェクトが受容可能なプライバシー結果をもたらすかそれとも耐え難いプライバシー影響をもたらすか。

モジュール D は，分析のための出発点であり，データ管理者がプロジェクトのプライバシー影響を描くのに役に立つ。モジュール E とモジュール F は，プライバシー保護法の諸原則との関係における適合性について質問をしている。ただ，モジュール E は，政府機関向けであり，モジュール F は民間部門または非営利組織向けである。

モジュール D において，プライバシー影響分析は，以下のような項目を検証する。すなわち，1）情報の流れが個人の選択にどのように影響を与えるのか，2）個人生活への侵入の度合い，3）プライバシー法の適合性，4）プロジェクトが社会的期待をどの程度充たすのか，というような質問項目で構成される［19］。

5.2.5　プライバシー管理

この段階では，プロジェクト管理者が，プロジェクト内の消極的なプライバシー影響を除去または削減する措置を考えなければならない。この措置は，必ずしも組織の目標をすべてカバーするものでなくてもいい。管理者は可能な措置を見出すことによって，プライバシー影響への適切な対応となり，なおもプロジェクトの目標到達へと導くこととなろう。この段階がより広範囲のプロジェクトリスク管理プロセスへと吸収されていく［20］。例えば，組織は，プライバシー強化技術（PETs）を用いて，個人情報の収集を最小化する一方で，組織をプロジェクトの目標達成へと導くことができるのである。

5.3　適合性チェックリスト

5.3.1　モジュールE　チェックリスト

モジュールEチェックリストは，プロジェクト内での個人情報の処理方法がプライバシー法に規定される諸義務に適合する否かを検証するために用いられる。政府機関は，このモジュールを修正して個別要求に合わせることが可能である。また，当該PIAと機関固有のプロセスとを電子ネットワーク化したり，概要や複製を添付することもできる［21］。

本チェックリストの質問項目は「情報プライバシー原則」（IPPs: the Information Privacy Principles）および「国家プライバシー原則」（NPPs: the National Privacy Principles）に関わっている。IPPsは，オーストラリアおよびACT政府機関が，個人情報に関して，その収集・記録蓄積・提供・蓄積・保全を含めて，どのように管理するかを規定している。IPPsは，また，自己の個人情報へのアクセス権ならびに修正権を認めている。

それらの機関がチェックリストの中で「いいえ」と応えたならば，当該機関は，プライバシー法の下での個人情報を収集する権限を失うことになる。それらの機関は，プライバシー担当管理監から，あるいは，法律団体や適切な外部機関から，IPP適合のための追加助言を得なければならない［22］。

以下が本チェックリスト内の質問項目である。

IPP 1－収集の方法と目的
IPP 2－関係個人による個人情報の請求
IPP 3－一般的な個人情報の請求
IPP 4－個人情報の蓄積と保全
　a）安全保全措置
　b）外部提供に関わる情報の保全
IPP 5－記録保有者による保有記録に関する情報
IPP 6－情報へのアクセス

IPP 7－記録の変更
IPP 8－記録保有者の個人情報に関する安全性事前チェック義務
IPP 9－関連目的にのみ利用される個人情報
IPP 10－個人情報の利用制限
IPP 11－提供
NPP 7－識別子
NPP 8－匿名性
NPP 9－越境データ流通
NPP 10－センシティブ情報
IPP 適合性－結論

5.3.2　モジュール F　チェックリスト

このチェックリストは，民間組織用であり，すべての民間医療機関にも適用される。このチェックリストを利用することによって，組織は，プロジェクト内の個人情報の処理方法を評価することができ，プライバシー法の下での当該組織の義務項目の適合性を評価することができる。必要な場合には，当該組織の実情に応じて，このモジュールを変更することも可能である［23］。

本チェックリストの質問項目は「国家プライバシー原則」（NPPs: the National Privacy Principles）に関わっている。NPPs は，組織の個人情報の管理方法について規律している。つまり，個人情報に関して，収集，利用と提供，情報の質と保全措置，開示，アクセス権と修正権，識別子，匿名性，越境データ流通，センシティブ情報，などについて規定しているのである。

それらの機関がチェックリストの中で「いいえ」と応えたならば，当該機関は，プライバシー法の下での個人情報を収集する権限を失うことになる。それらの機関は，プライバシー担当管理監から，あるいは，法律団体や適切な外部機関から，IPP 適合のための追加助言を得なければならない［24］。

6. お わ り に

プライバシー保護措置の新しい取組として，主に，オーストラリアの，現行のプライバシー影響評価制度を検討してきた。筆者は，当初から，プライバシーの影響をどのように測るのかということについて，疑問を抱きながら，同検討を進めてきた。ここに至っても，その疑問は消えていない。確かに，オーストラリア，カナダ，ニュージーランド，およびアメリカ合衆国等では，「個人情報保護法」や「データ保護法」ではなく，「プライバシー法」という

表現が使用されている。そのことから，この領域においても，やはり，「プライバシー」という表現方法を用いることは想定内のことであろう。

プライバシー影響評価の最重要課題は，個人情報処理システムについて，プライバシーの観点から，システムに含まれているであろう諸問題を，「事前に」，すなわち，システムの「稼働前に」，検証することである。そして，その検証結果をシステムに取り込むということである。この事前検証が同評価制度の最大特徴のひとつであるといえる。

もうひとつの特徴は，システムの目的と運用ステージに対応した「チェックリスト」が用意されていることである。そのリスト上の質問に応じることで，当該システムが，プライバシー法や各種プライバシー原則に適合していることが判明するという方式をとっている。システム保有者のコンプライアンス精神の高揚を狙っている。

ただ，「『プライバシー』影響評価」というものの，評価の対象となるものは，すなわち，アセス（Assess）されるものは，「個人情報」の「流れ」であることが明確になった。「プライバシー」と「個人情報」が同じものであると「肌」で感じ取ることができない筆者にとっては，このことも，いわゆる「文明の衝突」の一端なのであろうか。

ともあれ，この「プライバシー影響評価」の後に用意されているのが「プライバシー・バイ・デザイン」（PbD: Privacy by Design）である。PbD は，システムやプロジェクトにおいて，設計・計画段階からプライバシー保護措置を盛り込むことを義務づけるところの技術的・組織的手法である。したがって，PbD は，いわば，「デフォルト」で，すなわち，「標準」として，プライバシー保護措置が盛り込まれているという考え方である。そうすると，PIA が PbD を条件づける，あるいは，PIA は PbD の前提となる，ということができる。このように，PbD は，PIA と密接な関連性を有しているが，PbD ついては，稿を改めて検討することにしたい。

参照・引用文献

［1］ David Wright/Paul De Hert, Introduction to Privacy Impact Assessment, in: David Wright/Paul De Hert (eds.), *Privacy Impact Assessment,* Springer 2012, pp. 5–6.

［2］ Cf. Ibid.

［3］ Government of Canada, *Privacy impact Assessment Guidelines: A Framework to Manage Privacy risks Guidelines,* p. 1.

［4］ The European Commission, *Privacy and Data Protection Impact Assessment Framework for RFID Applications*, 12 Jan. 2011, p. 4.

［5］ [Australian Guide 2006]: Australian Government Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, August 2006, p. 4.

［5a］参照，瀬戸洋一他『プライバシー影響評価 PIA と個人情報保護』中央経済社2010年，83頁以下。

［6］ Government of Canada, ibid., p. 2.

［7］ [Australian Guide 2010]: Australian Government Office of the Privacy Commissioner, *Privacy Impact*

Assessment Guide, Revised May 2010, pp. vi－viii.
［8］ Ibid., p. viii.
［9］ Ibid., p. xvii.
［10］ Government of Canada, ibid., p. 22.
［11］ Australian Government Office of the Privacy Commissioner, ibid., p. xvii.
［12］ David Wright/Paul De Hert, ibid., p. 10.
［13］ Ibid., pp. 10－11.
［14］ Australian Guide 2010, ibid., p. xi.
［15］ Ibid., p. xiii.
［16］ Ibid., pp. xxiv－xxvii.
［17］ Ibid., pp. xiv－xv.
［18］ Ibid., pp. xxviii－xxxvi.
［19］ Ibid., pp. xxxvii－xxxviii.
［20］ Ibid., pp. xxxvii－xxxviii
［21］ Ibid., pp. xvi－xvii.
［22］ Ibid., pp. xxxix－lxi.
［23］ Ibid., pp. lxii－lxxxvi.
［24］ Ibid., p. lxii.