プライバシー影響評価手法の行政情報システムへの適用検討

瀬戸　洋一

１．はじめに

2006 年春，日本の外務省は，電子パスポートを発行した．電子パスポートにはバイオメトリクス（顔画像）が格納されている．究極の個人情報と言われるバイオメトリック情報を扱うため，システムの構築および運用に当たって，海外では，個人情報の保護に関する影響評価（プライバシー影響評価；Privacy Impact Assessment）が実施されている．電子政府および自治体システムにおいて同様の配慮がされている．日本でも，行政情報システムあるいは民間基幹系システムの構築運営において，個人情報管理における安全性の確保とステークホルダー（納税者，利用者）に合意が得られる評価体制の整備が急務である．

本発表では，プライバシー影響評価 PIA の概要と各国の実施状況，日本において実施する場合の課題と対策に関し明らかにする．

2．個人情報を扱う情報システムの構築における課題

プライバシーと個人情報は混同し用いられることがある．一般に個人情報は個人を識別できる属性を指す．例えば，氏名，生年月日，性別などが該当し，個人情報保護法などで定義されている．一方，プライバシーは，イメージで捉えられることが多い．個人情報の取扱い手続きは，法律の定めに従うことで解決するのに対し，プライバシーの権利をめぐる問題は，個人情報における法律の規定にみられるような基準が必ずしも存在しないことが原因である．また，プライバシーという価値に対する考え方が個々人異なることから，その判断基準も主観的な要素に影響される．

したがって，個人情報を扱う情報システムを構築する場合，ステークホルダーの同意を得られるプライバシー影響評価 PIA のような客観的な評価体系が必要である．PIA は，米国で 1970 年代から公的機関で実施されてきた技術評価が元になっている．2002 年施行の電子政府法により実施が義務付けられている．このため，米国の出入国管理システム US-VISIT では PIA が実施されている（表1参照）．

一方，日本においては，個人情報とプライバシーが混在し理解されていることと，個人情報を扱うシステムにおけるPIA実施の法的な根拠が整備されていないため，行政および民間組織においてPIAが実施されていないため，システムの構築，サービスへの適正性が曖昧になっている問題がある．

表１　各国の PIA 実施状況

国名	法律、ガイドライン、ポリシー	独立検証機関	実施主体	その他
カナダ	法律で説明責任明示、ガイドライン、ポリシーで手順等を公開	あり	個人情報を取り扱うシステムを構築・運用・管理する行政機関	国レベルで予算執行前のPIA実施を義務．各省庁、各州にPrivacy Officerが存在．省庁から独立したPrivacy Commissionerがアドバイス
米国	法律で義務化	未確認	個人情報を取り扱うシステムを構築・運用・管理する行政機関	電子政府法で情報セキュリティ管理法の制定に加えPIAを義務化（電子政府法208条）．実施組織内にPrivacy Officerが存在
オーストラリア	Privacy Actが存在する	あり	政府や自治体の部門が自主的に採用	国勢調査のデータ分析方式の変更案などで採用
ニュージーランド	Privacy Actが存在する	あり	政府や自治体の部門が自主的に採用	全政府共通のオンライン認証システム構築などで採用
香港	法律は、義務できないが、実例が存在する	あり	政府や自治体の部門が自主的に採用	香港IDカードのICカード化プロジェクトなどで採用

3．プライバシー影響評価 PIA とはなにか

プライバシー影響評価 PIA は，個人情報の収集を伴う IT システムの導入または改修にあたり，プライバシーへの影響を「事前に」評価し，システムの構築・運用を適正に行うことを促す一連のプロセスである．設計段階からプライバシー保護策を織り込み，導入後にも運用状態を把握することにより，「公共の利益」と「個人の権利」を両立させることを目的に実施される．

図1に示すように，PIA はプライバシー・フレームワーク，プライバシー・アセスメントおよびプライバシー・アーキテクチャから構成される．

産業技術大学院大学　産業技術研究科

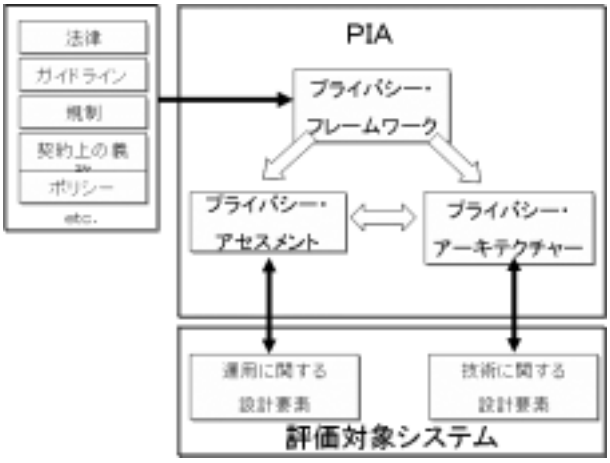

図１　PIA フレームワーク

①プライバシー･フレームワーク：入力として与えられた法制度の一覧を元に，当該 IT システム設計に必要となるプライバシー要件の抽出やチェックリストなどを定めることで，後続のプロセスに必要なプライバシーガイドラインを作成する．
②プライバシー･アセスメント：プライバシー･フレームワークの結果を元に，システムのデータフロー分析，およびチェックリストなどを用いプライバシーに関する影響分析を行う．ここで確認した課題は，プライバシー･アーキテクチャに引き継がれ，技術的な観点から解決を行う．
③プライバシー･アーキテクチャ：プライバシー･フレームワークを元に，システム設計仕様を検討し，具体的なプライバシーに関する問題解決を図る．

４．検討

欧米と日本では，プライバシー影響評価 PIA を実施するにあたり，いくつかの相違点がある．

(1) PIA を実施するための法的な根拠がある．例えば，カナダではプライバシー法 (Privacy Act)，米国では電子政府法 (The E-Government Act of 2002) により，個人情報を取り扱うシステムの構築に当たって PIA を実施しないと予算が許可されない．

(2) 欧米では，PIA の実施の目的として，法律を遵守することによりシステム構築の予算確保を行うことを第 1 の目的としている．重要なのはシステム運用時に情報の管理が適正に行われていることにあるが，システム運用における適正評価に PIA が実施されていることを，確認できていない．

(3) 日本において PIA を実施する法的な根拠はない．法的な根拠はないが，納税者，利用者などのステークホルダーへの説明責任として，個人情報の取得の目的および適切な運用がされていることを明確にする必要がある．

日本において PIA を実施するためには，法的な根拠を補完するために国際標準の適用が有効である．PIA のガイドラインを考慮して ISO/IEC15408 の機能要件を検討し設計に反映，および，ISO/IEC 17799 により，リスク分析･管理策の検討に利用することは有益である．2つの国際標準規格を適用することにより適正なシステムの構築運用ができる．欧米においては，プライバシー･フレームワーク，ガイドラインに則した自己評価であるが，上記の提言が実現できれば，日本においては，国際標準に準じた第三者評価になるため，欧米の PIA より高い信頼度の評価が行えると考える．

５．まとめ

日本は PIA を実施するための法律が未整備である．このため，何らかのコンプライアンスに乗せる必要がある．1つは，システムを構築する場合の国際標準規格 ISO/IEC15408 である．もうひとつは，ISO/IEC17799(27001)である．システムを構築するときに ISO/IEC15408 ベースで開発し，運用に際しては ISO/IEC17799 をベースで行えば，PIA に相当する効果が得られると考える．

参考文献

[1] 瀬戸洋一：バイオメトリックセキュリティ，ソフトリサーチセンター，2004 年
[2] 総務省：「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担保の仕組みについての研究会」報告書
http://www.soumu.go.jp/denshijiti/pdf/jyumin_p_4.pdf
[3]US-VISIT Program Privacy Impact Assessment, July 1, 2005.
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisitupd1.pdf
[4]M. Rotenberg：The Privacy Law Sourcebook 2004 United States Law, International Law, and Recent Developments, Electronic Privacy Information Center, 2004.
[5]瀬戸洋一：法務省受託研究　プライバシー影響評価手法 (PIA) と出入国管理システムへの適用に関する調査研究，2007 年 3 月