6W-01

ISO/IEC29100 を評価指標とした プライバシー影響評価の実施と課題

浦田有佳里† 下村憲輔† 白石敬典† 田娟† 中原道智† 慎祥揆† 瀬戸洋一†

公立大学法人首都大学東京 産業技術大学院大学†

1．はじめに

個人情報を扱うシステムの構築には，プライバシー影響評価の実施が有効である［1］．

PIA の実施には適正な評価基準が必要である．評価基準は OECD8 原則を基準に作成していた．2011 年にネットワークなどを用いた新しい利用分野に対応する国際標準 ISO/IEC29100 が発行された．ISO/IEC29100 は，ICT システム設計の指針を規定するプライバシーフレームワークに関し，OECD8 原則より現状の技術に即している[1]-[4]．このため，監視カメラシステムの PIA の評価基準を ISO/IEC29100 を利用し，評価を行った．本発表では，評価実施の課題とその対策について考察を行う．

2. プライバシー影響評価

プライバシー影響評価（Privacy Impact Assessment 以下，PIA）の定義は，個人情報の収集を伴う情報システムの導入または改修にあたり個人情報への影響を「事前」に評価し，法的問題とプライバシーリスクの問題回避または緩和のための法的・運用的・技術的な変更を促す一連のプロセスであり，個人情報に関するリスクマネジメント手法である[1]．

PIA を行う際に評価指標を作成する．図１に示すように評価指標は，参照規程文書から導出した要求事項に個人情報保護の法を適用し，評価項目とする．評価項目をチェックリスト形式に一覧化したものが評価シートとなる[1]．

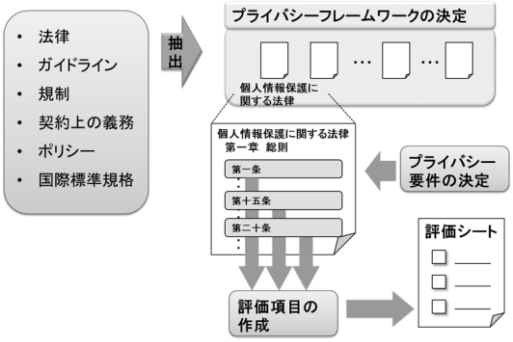

図１ PIA におけるリスク評価の基準作成

3. OECD プライバシー原則と ISO/IEC29100

3.1 OECD8 原則

OECD プライバシーガイドラインは，1980 年に OECD において採択されたプライバシー保護と個人のデータの国際流通についてのガイドラインに関する OECD 理事会勧告の附属文書である．個人情報の取扱いに関する基本原則（OECD8 原則）を規定している．

各国の個人情報保護法と人情報保護制度は OECD8 原則の影響を受けている[2]．

3.2 ISO/IEC29100

デジタル社会が進み，個人の情報がインターネット上で扱われるようになった．このため，新たなプライバシーの国際標準規格が必要になってきた．

ISO/IEC 29100 は，プライバシー保護のためのフレームワークを規定したものである．プライバシーフレームワークの国際標準規格として発行され，プライバシー11 原則等を定義している[3]．

4. PIA 評価基準へ ISO/IEC29100 の適用

4.1 OECD8 原則と ISO/IEC29100 の比較

監視カメラシステムに対する PIA では要求事項 ISO/IEC29100 を適用した評価シートを作成し，影響評価を実施した．

従来の評価シートは OECD8 原則を基準に作成した．規定されている内容の差異を明確にするため，表 1 に示すように OECD8 原則と ISO/IEC29100 の 11 原則の項目を比較した．表 1 より OECD8 原則は，ISO/IEC29100 にある「同意と選択」「データ最小化」「コンプライアンス」の項目が明示されていない．これは，個人の権利や利活用に関して，現状に則した考慮点が不足していると考えることができる．

表 1　OECD8 原則と ISO/IEC29100 の比較

ISO/IEC29100の11原則	OECD8原則
同意と選択	ー
目的の正当性と詳述	目的明確化の原則
収集の制限	収集制限の原則
データ最小化	ー
利用、保持、開示の制限	利用制限の原則
正確性と品質	データ内容の原則
公開、透明性および通知	公開の原則
個人参加およびアクセス	個人参加の原則
説明責任	責任の原則
情報セキュリティ	安全保護の原則
コンプライアンス	ー

4.2　ISO/IEC29100 を基準とした評価項目

評価シートは，ISO/IEC29100 を大項目とし，詳細項目は，内部規定文書（社内規定，契約書）と外部規定文書（法令や規格，ガイドライン）である参照規程文書の観点から要求事項を抽出する[1]．従来，評価シートの大項目は OECD8 原則で作成していた．現在，システム環境や個人情報の利用に関し，例えば，監視カメラシステムのように利用環境は大きくことなっている．また，個人情報を扱うシステムは国境を越えて利用するようになっている．したがって，各国が利用できる国際標準 ISO/IEC29100 が開発された．

PIA の評価指標には，ISO/IEC29100 を基準に作成することで新たな利用環境にも適用できると考える．OECD8 原則を基準として評価シートを作成する場合，個人の権利や利活用に関しての項目明確化に問題があったが，ISO/IEC29100 を基準とした場合，この問題が回避できる．

例えば，

- 個人情報提供の意味のある同意
- 個人情報提供の選択
- 不必要な情報の複製・加工の回避

の問題が是正できる．

次節にて ISO/IEC29100 を基準として開発した評価シートについて説明する．

5. 監視カメラシステム PIA への適用評価

監視カメラシステムを対象に PIA を実施した．

PIA の評価基準として ISO/IEC29100 を使用し，評価シートの大項目を設定した．

ISO/IEC29100 の評価項目への適用は既存の制定やガイドラインを利用することで補完が可能である．監視カメラシステム PIA 評価指標においては，「同意と選択」の評価項目は参照規定による補完により，個人情報保護の法律の第 17 条「適正な取得」を適用できると解釈した．

OECD8 原則を基準とした評価項目による影響評価と比べ，ISO/IEC29100 を基準とした影響評価は，プライバシーリスクマネジメントに影響を及ぼす諸要因を，法律上・行政上，契約上，業務上などからフレームワークを構築し，網羅されている．

また，ICT システムを設計する際に指針となるプライバシー・アーキテクチャ・フレームワークが提示されており，より詳細な管理について明確になっている．国際標準である ISO/IEC29100 を用いることで海外からの十分性を満たしていると評価される[4]．

6.　おわりに

OECD8 原則を利用した評価基準では，現在の技術進歩や個人情報利活用の仕組みを考慮した基準が漏れる．新たな国際標準である ISO/IEC 29100 が発行され，PIA の評価実施時に ISO/IEC 29100 を基準とした評価項目を作成した．既存の制定やガイドラインを利用することで法的解釈への補完ができ，技術進化や情報の利活用に向けて，適正なリスク評価を実施することが可能である．

参考文献

[1]　瀬戸洋一　：　実践的プライバシーリスク評価技法，近代科学社，2014 年
[2]　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 年
[3]　ISO/IEC 29100 プライバシー原則，2011 年
[4]　野村総合研究所：　プライバシーにかかわる標準化の動向，2014 年
https://www.nri.com/jp/event/mediaforum/2014/pdf/forum207_1.pdf

---

「Implementation of privacy impact assessment using ISO / IEC 29100 as evaluation criteria」

† Yukari Urata, † Kensuke Shimomura, † Keisuke Shiraishi,
† Tian Juan, † Michitomo Nakahara,
† Shin Sang Gyu , † Yoichi Seto
† Advanced Institute of Industrial Technology