資料３

情報保護評価に関する論点

第１　本SWGにおける検討の視点

○　情報保護評価とは、「番号」に係る個人情報が適切に取り扱われているかを確認するために行うもので、諸外国で採用されているプライバシー影響評価（Privacy Impact Assessment、以下「PIA」という。）に相当するものである。

○　一般的に、PIAとは、情報システムの導入等にあたりプライバシーへ及ぼす影響を事前に評価し、その保護のための措置を講じる仕組みをいう。PIAの実施時期としては、プライバシーへ及ぼす影響に大幅な手戻りなく対応できるようにするため、システム設計の変更が可能であるシステム開発前が適当と考えられている。PIAの具体的な実施方法としては、個人情報の収集目的や収集方法、利用方法、管理方法などを検討し、そのシステムがプライバシーに配慮した設計となっているか確認するなどの方法が採られている。

○　本SWGでは、諸外国のPIAや我が国における環境影響評価制度等を踏まえ、情報保護評価の実施枠組みを検討し、情報保護評価ガイドラインを作成することとする。

第２　情報保護評価の目的

以下を目的として、情報保護評価を実施することが考えられる。

①プライバシーに対する影響やリスクについて分析を行い、かかる影響やリスクを軽減するための合理的措置を講じること

②情報保有機関における「番号」に係る個人情報の取扱いやシステムに対する透明性を増し、情報保有機関がどのような情報を収集するのか、なぜ情報を収集するのか、どのように情報を使用するのか、どのように情報を安全に格納するのかについて、国民に対しわかりやすい説明を行うこと

③情報保有機関がシステムのライフサイクル全体を通じてプライバシーへ配慮した設計を行ったことを、国民に対し示すこと

（参考資料１「諸外国におけるPIAの目的・役割」ご参照）

第３　情報保護評価の実施の仕組みに関する論点

１　情報保護評価のフローについて

（１）情報保護評価のフロー

情報保護評価のフローを、以下の通りとすることが考えられる。

①システムを開発・改修する行政機関・関係機関にて
　情報保護評価を実施し、報告書を作成する
②第三者機関による承認を受ける
③報告書を公開する

（２）第三者機関による承認

○　諸外国では、第三者機関による承認が行われない例が多い。

負担軽

オーストラリア･イギリス：承認プロセスは特段定められていない。
アメリカ：実施機関内のレビュー官による承認後、予算当局に提出
カナダブリティッシュコロンビア州・アルバータ州：第三者機関によるレビューを受ける。
カナダ（連邦）：実施機関内の責任者による承認後、第三者機関に提出する。さらにプライバシー法上の義務である個人情報バンクを所管する財務委員会にも提出を行い、PIAの義務的要件の履行について確認を受ける。

負担重

（参考資料２「諸外国におけるPIAについて」承認方法、第三者機関の役割及びその他欄ご参照）

○　実施機関内のみで情報保護評価プロセスが完結すると、情報保護評価の実施や報告書の質の担保が難しい場合がありうるため、日本では、第三者機関が情報保護評価の報告書を承認することとした（大綱第３Ⅵ12（２））。

○　但し、第三者機関による情報保護評価の承認が、第三者機関の一般的な調査権限、監督権限と衝突しないか整理する必要がある。

２　情報保護評価の対象システムについて

○　情報保護評価の対象を、「番号」に係る個人情報を取り扱う行政機関及び関係機関のすべてのシステムとする場合、参考資料３の通り、非常に多数のシステムが対象となる可能性がある。

（参考資料３「情報保護評価の対象となりうるシステム」ご参照）

○　「番号」に係る個人情報の保護を図りつつ、第三者機関が精査可能な仕組みとするためには、どのような枠組みが考えられるか。

たとえば、プライバシーに対する影響度に応じて第三者機関の承認対象を変更する、審査方法を変更する、第三者機関以外の第三者の目が届くようにすることなどが考えられ、具体的な枠組みの例として、以下の案などが考えられる。

（参考資料４「情報保護評価の実施枠組み（案）」ご参照）

案①　影響度に応じて、第三者機関の承認対象を変更する案

（１）プライバシーに対する影響度が軽微なシステム
　　→情報保護評価の対象外又はしきい値評価のみを実施
（２）プライバシーに対する影響度が通常程度のシステム
　　→行政機関又は関係機関にて評価実施
　　→第三者機関にて**サンプリング**チェック
（３）プライバシーに対する影響度の高いシステム
　　→行政機関又は関係機関にて評価実施
　　→第三者機関にて、**全件**を承認対象とする

※　諸外国では、上述の通り、そもそも第三者機関による承認が行われない例が多いため、影響度に応じて承認対象を変更している例は見当たらない。但し、すべてのPIAではなく任意のPIAについてのみ助言・レビューを行っている第三者機関もあることから、第三者機関側でレビュー対象を選択する場合もあるものと推測される。

案②　国民に広く意見を伺い、さらに、影響度に応じて第三者機関の審査方法を変更する案

（１）影響度が軽微なシステム
　　→情報保護評価の対象外又はしきい値評価のみを実施

（２）影響度が通常のシステム

→行政機関又は関係機関にて評価実施

→行政機関又は関係機関にて**パブリックコメント**に付し、国民の意見を反映

→第三者機関にて、**全件**を承認対象とするが、パブリックコメント等**手続面の審査のみ**を行う

（３）影響度の高いシステム

→行政機関又は関係機関にて評価実施

→行政機関又は関係機関にて**パブリックコメント**に付し、国民の意見を反映

→第三者機関にて、**全件**について、評価の**内容面の審査**及びパブリックコメント等**手続面の審査**を行う

（参考資料５「パブリックコメント概要」ご参照）

※　手続面の審査のみ行うという点は、カナダ連邦財務委員会におけるレビューが参考になると思われる。

（参考資料２「諸外国におけるPIAについて」カナダ（連邦）承認方法欄ご参照）

※　諸外国では、PIAの実施に当たりパブリックコメント等の措置を講じている例は見当たらない。しかし各国とも、PIAの役割として、プライバシーに対する考え方を国民・消費者等へ説明することを重視しており、事業により悪影響を受け得る組織や個人等の意見を聴取し、多角的なリスク分析を行うよう推奨している。

この点を踏まえると、情報保護評価をパブリックコメントに付し広く意見を伺うことは、情報保護評価の趣旨にも合致するものと考えられる。

※　なお、我が国においても、制度の流れの中に、地域の情報を熟知している住民等や、地域の行政に責任を有している都道府県知事の意見を聴く手続を取り入れているものもある*（参考資料６ご参照）*。

※　また、案①と案②を組み合わせ、案①にパブリックコメント手続を盛り込むことも考えられる。

○　上記のような枠組みとする場合、（１）（２）（３）に分類する基準をど

うすべきか。たとえば、情報連携基盤との接続の有無、取り扱う「番号」に係る個人情報の量・種類・主体数、一組織内利用のみにとどまるか否か、収集目的の明確性、使用技術などの基準が考えられる。

（諸外国例）

アメリカ：情報の主体（職員、委託先又は公衆）、情報の内容、他システムとの接続・共有の有無、収集目的、収集権限など

オーストラリア：情報の内容、目的、法的根拠、情報の性質・機微性など

イギリス：使用技術、目的、識別子、認証要件、情報量、情報の主体数、連結、データ収集、品質保証、セキュリティ、開示、保管、適用除外など

カナダ：機微性、同意取得、通知、情報源、決定過程、他目的共有、識別子、公衆の懸念、個人情報の分離、セキュリティ

（参考資料７「諸外国におけるPIA要否等判断基準」ご参照）

３　情報保護評価の実施・承認の義務付け強化について

○　情報保護評価の実施及び承認の義務付けを強化するために、情報保護評価が未実施・未承認の場合は、情報連携基盤への接続を不可とする権限を第三者機関に付与してはどうか。

４　報告書の公表について

○　報告書の公表を義務付けることとしてはどうか。但し、報告書全文を公表することでシステムセキュリティへのリスクとなりうる場合も考えられることから、全文を公表するか要約を公表するかについては、行政機関又は関係機関の裁量とすることとしてはどうか。

（参考資料２「諸外国におけるPIAについて」公開及び非公開事由欄ご参照）

第４　情報保護評価ガイドライン作成に関する論点

○　情報保護評価ガイドラインには、①情報保護評価の実施の仕組み、②情報保護評価報告書の記載様式（質問票）を記述してはどうか。

○　質問票作成に当たっての参考資料として、諸外国の質問票及びISO22307 等

を踏まえることとしてはどうか。

第５　地方公共団体における情報保護評価に関する論点

○　地方公共団体における情報保護評価については、どう考えるべきか。

以上