資料３

情報保護評価に関する論点

主な論点

第１　本SWGにおける検討の視点
第２　情報保護評価の目的
　　○　目的
　　○　評価対象・保護対象
第３　情報保護評価ガイドラインに関する論点
　　○　記載事項
　　○　既存の関連制度との関係性・インセンティブ
第４　情報保護評価の実施の仕組みに関する論点
　　○　実施の仕組み
　　○　必要性の判断（しきい値評価）
　　○　必要性に応じた仕組み
第５　地方公共団体における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当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

１　情報保護評価制度の趣旨について（総論）

○　番号制度は、①より公平・公正な社会、②社会保障がきめ細やかかつ的確に行われる社会、③行政に過誤や無駄のない社会、④国民にとって利便性の高い社会、⑤国民の権利を守り、国民が自己に関する情報をコントロールできる社会の実現を目指し、導入されるものである。

○　しかしその一方で、番号制度導入により、国家により個人の様々な個人情報が一元管理されるのではないかといった懸念や、「番号」に係る個人情報が不正に追跡・突合されるのではないかといった懸念、財産その他の被害が発生するのではないかといった懸念が生じることが考えられる。

○　そこで、これらの懸念を踏まえ、国民の「番号」に係る個人情報が適切に取り扱われる安心・信頼できる番号制度の構築のために、次の目的から情報保護評価を実施するものとする。

２　情報保護評価の目的について

①　事後的な対応にとどまらない、積極的な事前対応を行うこと

○　一度流出した情報はその回収が困難であるなど、プライバシー侵害はその回復が容易でない側面も多い。そのためプライバシー保護のためには事後的な対応のみでは足りず、事前にプライバシー保護のための評価・確認を行うことが重要である。

○　そこで、事後的な対応にとどまらず、プライバシーに対する影響やリスクについて事前に分析を行い、かかる影響やリスクを軽減するための合理的措置を事前に講じることとする。また事前評価を行うことで、事後の大規模な仕様変更を防ぎ、不必要な財政支出を防ぐことも可能であると考えられる。

②　情報保有機関が国民のプライバシー保護にどのように取り組んでいるかについて、情報保有機関自身が宣言し、国民の信頼を獲得すること

○　情報保有機関における「番号」に係る個人情報の取扱いやその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とする。

○　番号制度では原則として、本人同意を前提としない仕組みが想定されている。そのため、各情報保有機関において「番号」に係る個人情報が具体的にどのように収集、利用、保管、廃棄されるのかを国民に対し明確に示すことが、重要である。情報保有機関が国民のプライバシー保護にどのように取り組んでいるかについて、情報保護評価を通じて情報保有機関が宣言・説明することは、国民に信頼していただける番号制度システムの構築に資するものと考えられる。

③　第三者機関が確認を行うことで、①②についての厳格な実施を担保すること

○　国民のプライバシー保護のためには、各情報保有機関が保有する「番号」に係る個人情報を当該機関が責任を持って取扱うことが必要であるが、各機関内のみに閉じた評価・確認を行うのみにとどまらず、各機関から独立性を保った、専門性を有する第三者機関がさらに確認を行うことで、情報保護評価の厳格な実施を担保し、情報保護評価制度をより実効的なものとする。

３　情報保護評価の評価対象・保護対象について

情報保護評価の対象は、「個人情報」保護にとどまらない、国民の「プライバシー」保護とすることが考えられる。つまり、情報保護評価の評価対象は、個人情報保護法令の遵守確認にとどまらない、プライバシー保護とすることが考えられる。

（１）個人情報保護法令遵守とプライバシー保護との差異

○　個人情報保護法令遵守とプライバシー保護との具体的な差異としては、法令遵守はあくまで一定の規制・基準・要件をクリアするものであるのに対し、プライバシー保護は、個人情報保護法令を遵守するのみにとどまらず、さらにより一層の保護措置を追求するものと考えられる。換言すれば、プライバシー保護を目的とした評価は、法令遵守といった基準クリア型ではなく、ベスト追求型の評価であると考えられるのではないか。

○　たとえば、行政機関の保有する個人情報の保護に関する法律（平成十五年五月三十日法律第五十八号）（以下、「行政機関個人情報保護法」という。）を適用した場合の第三者提供を例とすると、同法は利用目的の範囲内の第

三者提供を認めており（同８条１項）、その際、個人情報ファイル（同２条４項）に該当する場合は、経常的な提供先などを公表するものとしている（同１１条１項及び１０条１項）[1]が、提供時期や頻度、提供場面、提供先での管理方法などについては公表する義務を負わない。

○　また同法は、提供先が法令の定める事務又は業務の遂行に必要な限度で利用し、かつ利用について相当な理由があるなどの一定の場合に、利用目的外の第三者提供についても認めており（同８条２項）、この場合も個人情報ファイルに該当する場合は、経常的な提供先などを公表するものとされている（同１１条１項及び１０条１項６号）。

しかし、利用についての相当な理由などの要件にかかる具体的事実を公表する義務はなく[2]、また目的内提供同様、提供時期や頻度、提供先での管理方法なども公表する義務を負わない。

（参考資料５別紙「行政機関の保有する個人情報の保護に関する法律関連条文抜粋」ご参照）

○　これに対し、プライバシー保護を目的とすると、行政機関個人情報保護法上の義務よりもより広い事項について公表を行っていったり、第三者提供を制限的に運用したりすることが考えられる。

（２）諸外国におけるPIA

○　諸外国におけるPIAも、単なる法令遵守確認にとどまらない、プライバシーに対する影響を分析・評価するものとして理解されている。

（３）情報保護評価の目的からの検討

○　また上記２の情報保護評価の目的からも、情報保護評価の対象を法令遵守確認だけではない、プライバシー保護とすべきではないかと考えられる。

1　経常的な提供先には、継続的な提供先のほか、一定期間ごとに提供する提供先、不定期であっても依頼があれば必ず提供することとしている提供先なども含まれる。

2　要件を充足しない目的外提供がなされている場合、本人は利用停止請求権（同法３６条）を行使することができ、かかる利用停止請求は行政手続法上の「申請」（行政手続法２条３号）に該当するため、行政機関の長は、できる限り具体的な審査基準を作成して公にしておく義務があり、たとえば利用についての相当な理由についても基準を示すべきものと解される（同５条）。しかし、個々の事例における相当な理由については、特段公表する義務が課されるものではないものと解される。

○　国民の信頼獲得という目的からは、法令を遵守するだけにとどまらず、説明責任を積極的に果たしていくことが望まれる。

○　また国民の懸念としては、国家が法令を遵守していないという懸念よりも、国家が法令を遵守しながらも国民のプライバシーに対し脅威を与えるような運用をしていないかといった懸念の方が考えられ、かかる懸念に対しても説明責任をきちんと果たしていくことで、国民に信頼していただける番号制度の構築に資するものと考えられる。

第３　情報保護評価ガイドラインに関する論点

１　情報保護評価ガイドライン

（１）ガイドラインの汎用性

○　情報保護評価の対象は、「番号」に係る個人情報を取り扱うシステムとするが、ガイドライン作成に当たっては、一般的なシステム全般にも広く活用できるよう配慮するものとしてはどうか。

（２）ガイドラインの記載事項

○　情報保護評価ガイドラインの記載事項を以下とすることが考えられる。

①情報保護評価とは何か
②情報保護評価の目的
③情報保護評価の対象
④情報保護評価の実施の仕組み
⑤情報保護評価報告書の記載様式（質問票）

（参考資料１「諸外国におけるPIAガイドラインの記載内容」ご参照）

（３）報告書の記載事項

○　情報保護評価報告書の記載様式の項目は、どのようなものが考えられるか。たとえば、個人情報のフローをまず示し、そこから導き出されるプライバシーへ与える影響について、収集・使用・管理・提供・抹消など情報

のライフサイクルごとに対策を記載していくことなどが考えられる。

（参考資料２「情報保護評価報告書の記載様式項目（案）」、参考資料３「諸外国におけるPIA質問票」、参考資料４「諸外国におけるPIA報告書」ご参照）

２　既存の関連制度との関係性について

○　情報保護評価ガイドライン策定に当たっては、情報保護評価に関連すると考えられる既存制度との関係性の整理が必要である。

（参考資料５「情報保護評価と関連既存制度との関係について」、参考資料６「情報保護評価に関連する認定制度」、参考資料７「政府統一基準群について」ご参照）

○　①個人情報ファイル簿等については、個人情報ファイル簿等と情報保護評価の両制度間の調整を図る必要がないか、検討することとしてはどうか。

○　②プライバシーマーク、④ISMS適合性評価又は⑤ITセキュリティ評価及び認証制度（JISEC）の認証を取得済みである機関並びに③政府統一基準群にのっとった基本方針、対策基準及び実施手順を策定・実践している機関については、情報保護評価の特定項目の省略など、情報保護評価の実施に向けたインセンティブをどのように考えるべきか。インセンティブを設けるとすれば、どのようなものが考えられるか。

第４　情報保護評価の実施の仕組みに関する論点

１　情報保護評価の実施の仕組みについて

（１）　総論

○　「番号」に係る個人情報を取り扱うシステムは、非常に多数に渡ることが想定される。

○　「番号」に係る個人情報を取り扱うシステムすべてを、情報保護評価の対象とすることも考え得る。しかし、非常に膨大な量のシステムすべてについて情報保護評価を実施し第三者機関の承認を受けるとすると、実施機関及び第三者機関の情報保護評価に係るコストを現実的に考慮すれ

ば、情報保護評価制度が、対象範囲は広範なものの個々の評価内容が乏しい、形式的な制度にもなりかねない。情報保護評価の対象にすべてのシステムを取り込もうとすると、逆に情報保護評価が十分に機能しなくなる可能性があるのではないか。

○　情報保護評価の目的を達成し、実効性のある仕組みとするためには、広く浅く一律の情報保護評価を実施するのではなく、情報保護評価の必要性に応じたメリハリのある仕組みとしてはどうか。

（２）必要性の判断（しきい値評価）

○　そのためには、まず情報保護評価の必要性を判断（しきい値評価）する必要があるが、必要性の判断の基準は、上記第２の情報保護評価の目的を踏まえたものとしてはどうか。具体的には、たとえば以下のものを必要性が高いものとすることが考えられる。

【第２の２①　事前対応を行う目的に対応するもの】

*プライバシーに対するリスクが高いもの[3]
*事後的対応のみでは、被害が発生した際にその被害が甚大なもの[4]
*大規模システム等で、事後の仕様変更に多大なコストがかかるもの

【同②　国民の信頼を獲得する目的に対応するもの】

*「番号」に係る個人情報が取り扱われる流れ、利用目的、利用方法がわかりづらいもの[5]
*過去に漏えい事故などがあったその他の理由により、国民の懸念が大きいもの

【同③　第三者機関の確認により実効性を確保する目的に対応するもの】

*専門的、特殊又は複雑なシステムで、評価について専門家の検証が

3　考え得るリスクを想定し（たとえば、不正取得、不正利用、不正提供、流出、紛失、情報の不正確性など）、それらのリスクが高いか否かを測る質問を設けることなどが考えられる。

4　甚大な被害が考えられるかを測る質問（たとえば、個人情報に基づき行政上の決定を行っているか、個人に相当程度の財産的又は精神的損害を与えるような被害が発生し得るかなど）を設けることなどが考えられる。

5　流れが複雑なもの、複数機関にて「番号」に係る個人情報が取り扱われるもの、利用目的が漠然としているもの、利用方法が多岐に渡るものなどが考えられる。

必要なもの

○　この基準により必要性の高さを測るとした場合、各項目を測るための質問はどのようなものが考えられるか。

○　＜参考＞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８「諸外国におけるPIA要否等判断基準」及び参考資料３「諸外国におけるPIA質問票」４（２）＜セクションⅡ―リスク分野の特定及び分類＞ご参照）

○　上記の基準等を詳細化したしきい値評価質問票を作成し、かかる質問票に回答することでしきい値評価報告書を作成するものとしてはどうか。

○　また、しきい値評価を行うことで、簡易版の情報保護評価を実施できるような仕組みとしてはどうか。つまり、しきい値評価の質問票を、諸外国で行われているPTA（Privacy Threshold Analysis）レベルよりもさらに進めて、スモールスケールPIAに相当するようなものとしてはどうか。

（３）必要性に応じた仕組み

上記の必要性判断（しきい値評価）を受け、以下のような枠組みに分岐していくこととしてはどうか。

（参考資料９「情報保護評価の実施の仕組み（案）」ご参照）

ア　しきい値評価質問票のうち数問に答えることで、すぐに対象外と判断してよいもの

→情報保護評価の**対象外**

○　アについても、しきい値評価報告書を第三者機関に送付して、第三者機関にてサンプリングチェックを行うべきか。また、しきい値評価報告書を公開するべきか。

イ　しきい値評価質問票全問に答えるが、その結果必要性が高くないと判断されるもの

①行政機関又は関係機関にて**しきい値評価**を実施
②行政機関又は関係機関の**裁量**により、
　パブリックコメント等で**広く国民の意見を求めるかどうか判断**する
③第三者機関にて、**サンプリングチェック**（※２）
④しきい値評価報告書を**公開**する

※１　国民…公開された報告書を通じて、行政機関又は関係機関が国民のプライバシー保護にどのように取り組んでいるか確認する（④）。但し、当該機関の判断で、さらに広く国民の意見を聴取することも考えられる（②）。

第三者機関…基本的に、行政機関又は関係機関の責任で情報保護評価プロセスを完結するものとするが、第三者機関がサンプリングチェックを行う（③）ことで、杜撰な情報保護評価がなされないようにする。

また、情報保護評価実施後に何らかの問題があった際は、情報保護評価を通じて、当該システムの概要と、当該機関のプライバシーに対する考え方を調査の初めに把握し、報告書の記載事項と実態の乖離などの問題がないか、第三者機関が調査することが可能であると考えられる。

※２　第１回サブワーキンググループ資料では、第三者機関にて手続面の審査を行う案も記載したが、上記第２の２情報保護評価の目的③の通り、第三者機関の承認は、情報保護評価の実効性を確保するものであるため、手続面の審査を行うよりも、内容面審査を行う方が目的に資するのではないか。

ウ　しきい値評価質問票全問に答えた結果、必要性が高いと判断されるもの

必要性の高いものについてはより丁寧で充実した仕組みとすべく、全件について専門家による審査を行い、かつ各機関の裁量により、広く国民の目で多角的な視点から評価を見ていただくことを検討することとしてはどうか。

①行政機関又は関係機関にて**しきい値評価**を実施 ②行政機関又は関係機関にて**情報保護評価**を実施 ③行政機関又は関係機関の**裁量**により、 　パブリックコメント等で**広く国民の意見を求めるかどうか判断**する ④第三者機関にて、**全件**について、 　評価の**内容面の審査及び手続面の審査**を行う ⑤情報保護評価報告書を**公開**する

※　国民…公開された報告書を通じて、行政機関又は関係機関が国民のプライバシー保護にどのように取り組んでいるか確認する（⑤）。但し、当該機関の判断で、さらに広く国民の意見を聴取することも考えられる（③）。
　第三者機関…専門性を有する機関として審査する（④）。

２　第三者機関による承認について

○　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

○　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、監督権限等と衝突しないか整理する必要がある。

（資料２「諸外国の第三者機関が承認を行わない理由について」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することが考えられる。

○　情報連携基盤に接続しない機関のうち、情報保護評価を未実施の機関や未承認の機関については、一般の助言・勧告権限等に基づき、第三者機関が是正を促すことが考えられる。

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する。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や安全保障上のリスクとなりうる場合も考えられることから、一定の場合には要約を公表することとしてはどうか。

○　全文公表が必要な場合に要約公表がなされた場合や、公表された要約の内容では不十分な場合は、第三者機関が、行政機関又は関係機関に対し、一般の助言・勧告権限等に基づき、是正を促すことが考えられる。

○　情報保護評価報告書の一覧性を確保するために、情報保護評価報告書は各機関にて公開するのではなく、第三者機関のWebサイトなどで一括して公開す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

○　地方公共団体に対しても、情報保護評価の実施を義務付けるべきか。

以上