

情報保護評価に関する論点

主な論点

- 第 3 情報保護評価の対象に関する論点
- 第 4 情報保護評価ガイドラインに関する論点
 - 既存の関連制度との関係性・インセンティブ
- 第 5 情報保護評価の実施の仕組みに関する論点
 - 実施の時期
 - 必要性の判断（しきい値評価）基準
 - 情報保護評価（重点項目評価）報告書の記載事項
 - 情報保護評価（全項目評価）報告書の記載事項
 - 国民の意見聴取のあり方

第 1 本SWGI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SWGIでは、諸外国のPIAや我が国における環境影響評価制度、政策評価等を踏まえ、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不十分で、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¹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り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

- 情報保護評価の評価対象を、「個人情報」保護にとどまらない、国民の「プライバシー」保護とすることとする。
- 行政機関等は個人情報保護法令を遵守するだけではなく、国民の憲法上の権利であり民事上も法的に保護されるプライバシー侵害を行ってはならない義務を負っている。

さらに比例原則等の観点から、行政作用を行う際にはより制限の程度が少ない手段を選択しなければならないものと考えられるため、行政機関等は行政作用を行う際に、原則としてよりプライバシー侵害性の低い措置を採るべきものと考えられる。

個人情報保護法令はプライバシーを中核とする私人の個人情報を保護するためのものであるが、それによりプライバシーに係るとされている問題のすべてが解決されるわけではないと解される。

そこで情報保護評価では、個人情報保護法令の遵守にとどまらずプライバシー保護についても評価を行うものとする。情報保護評価報告書の記載様式項目についても、個人情報保護法令に基づく質問だけでなく、

それを敷衍するプライバシー保護の観点に基づく質問を設けることとする。

情報保護評価は、個人情報保護及びプライバシー保護について行政機関等が負っている義務、責務を達成するための、体系的評価制度となるものと考えられる。¹

(ご参考) 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、行政機関個人情報保護法を適用した場合の利用目的に関する規制を例とすると、同法は利用目的をできる限り特定することを要求しており（同3条1項）、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならないものとしている（同条3項）。また、本人から直接書面に記録された当該本人の個人情報を取得するときには、あらかじめ本人に対し利用目的を明示しなければならず（同法4条柱書）、またかかる場合以外についても、一定の個人情報ファイルについては、その利用目的が個人情報ファイル簿を通じて公表されることとなる（同法11条1項、10条1項3号）。

しかし、個人情報の特定の項目や特定の種類の、具体的にどのような目的に利用されるのかについてまでは特定、通知、公表する義務を負わない。

○ また、行政機関が個人情報を保有するに当たっては、法令の定める所掌事務を遂行するため必要な場合に限らなければならないとされている

¹ なお、情報保護評価という新たな制度を導入するからには、国際的な水準を踏まえた上で日本における固有の制度のあり方を検討すべきであると考えられるが、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。

(同法3条1項)が、その必要性を通知、公表する義務を負わない。

- これに対し、プライバシー保護を目的とすると、個人情報の特定の項目や特定の種類がなぜ必要なのか、また具体的にどのような目的に利用されるのかについて事前に特定し、積極的に公表していくことが考えられる。

(参考資料5「情報保護評価(全項目評価)報告書の記載様式項目(案)」

4 取り扱う個人情報の中では、行政機関個人情報保護法で求められる義務より広く、個人情報の特定の項目や種類がなぜ必要で、どのように利用されるかを記載するようにしている)

- また、行政機関個人情報保護法では、個人情報ファイル簿について一般公表することを要求している(同法11条)が、プライバシー保護を目的とすれば、より広い事項について公表を行っていくことが考えられる。

(参考資料5「情報保護評価(全項目評価)報告書の記載様式項目(案)」

では、行政機関個人情報保護法で求められる義務より広い事項について、分析・検討・公表を行うようにしている)

第3 情報保護評価の対象に関する論点

- 情報保護評価の対象は、大綱上、『「番号」に係る個人情報⁴を取り扱うシステム』とされている(大綱第3 VI12(2))。すなわち、「番号」に係る個人情報の生成、収集、保持又は利用等を行うシステムが、情報保護評価の対象であると考えられる。

- 「番号」に係る個人情報を取り扱うが、情報システムを用いない手作業処理については、情報保護評価の対象外とすることが考えられる。

その理由としては、システムでの処理は、データ連結・データ流通・データ転用・大量処理・高速処理が容易で、プライバシーに与える影響度が高いと考えられるが、システム処理に比べ手作業処理はプライバシーに与える影

⁴ 「番号」に係る個人情報とは、①「番号」、②情報連携基盤を通じた情報連携の対象となるものとして法定された社会保障及び税分野の個人情報、③(情報連携基盤を通じた情報連携の対象とはならないものの、)法令に基づき「番号」を取り扱い得る事務において「番号」と紐付いて扱われる社会保障及び税分野の個人情報をいう(大綱第3 IV)。

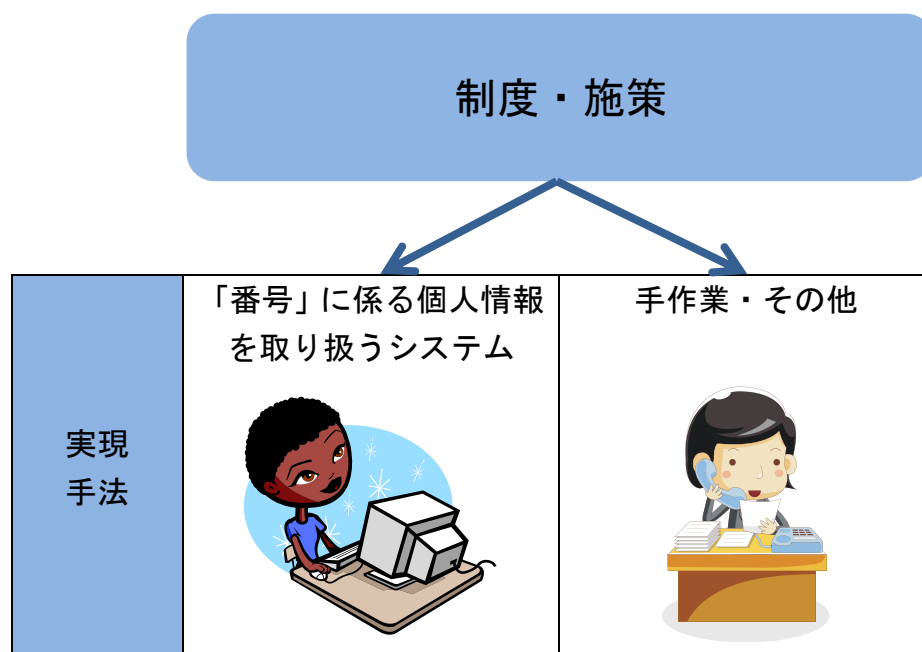
響度が低いと考えられるためである。

- 「番号」に係る個人情報を取り扱う制度・施策（たとえば、番号制度が制度・施策に該当し、これに対して個々のシステムが「番号」に係る個人情報を取り扱うシステムに該当する。）については、どのように考えるべきか。

情報保護評価はあくまで「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あり、制度・施策自体に対して情報保護評価を実施しても、漠然とした評価しか行えないのではないかと懸念がある。また制度・施策の是非はあくまで国会にて審議する事項であると考えられる（ただし、専門的機関として第三者機関が、当該制度・施策における「番号」に係る個人情報の保護について意見を有する場合は、一般の助言・勧告権限又は内閣総理大臣への意見具申権限等に基づき意見を述べることができる）。

しかしその一方で、「番号」に係る個人情報を取り扱う制度・施策を実施する前に情報保護評価を実施すれば、制度・施策がプライバシーに対して与える悪影響を事前に検討し、軽減することも可能となると考えられる。

制度・施策についてどのように考えるべきか。



- ただし、情報保護評価の対象外であっても、実施機関の任意の判断により、自主的な評価として情報保護評価の枠組みを用いることができるものとして

かどうか。

第4 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。

(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
 - …本資料第2を基に作成
 - ③情報保護評価の対象
 - …本資料第3を基に作成
 - ④情報保護評価の実施の仕組み
 - …本資料第5を基に作成
 - ⑤情報保護評価の必要性の判断（しきい値評価）基準（質問票）
 - …参考資料2を基に作成
 - ⑥情報保護評価（重点項目評価）報告書の記載様式（質問票）
 - …参考資料4を基に作成
 - ⑦情報保護評価（全項目評価）報告書の記載様式（質問票）
 - …参考資料5を基に作成
 - ⑧プライバシーに配慮したシステム設計・運用のための指針

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。

- 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り基本方針、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5 情報保護評価の実施の仕組みに関する論点

1 実施の時期について

- 情報保護評価は、大綱上、「番号」に係る個人情報を取り扱うシステムを『開発又は改修する前に』実施するものとされている（大綱第3 VI12（2））。
- 具体的には、①予算政府案、②要件定義、③基本設計、詳細設計の時点が考えられる。

（参考資料1「情報保護評価の実施タイミングについての考え方」
ご参照）

いつの時点で情報保護評価が実施可能となるかはシステムごとに検討状況や体制の状況が異なると考えられることから、情報保護評価が可能な程度にシステムの詳細が決定されているか、情報保護評価の結果を反映してもコスト増、スケジュール遅延につながらない時期かなどを踏まえた上で、各実施機関で具体的な実施時期について判断することとしてはどうか。

2 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することが考えられる。

(2) 必要性の判断

- 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、必要性の判断基準はどうすべきか。

(参考資料2「情報保護評価の必要性の判断（しきい値評価判断）基準（案）」ご参照)

- <ご参考>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

(3) 必要性に応じた仕組み

上記の必要性の判断（しきい値評価）基準により、システムを以下の三区分に分類することとしてはどうか。

- i 対象外
- ii 必要性が高くないもの（情報保護評価（重点項目評価）のみの実施）
- iii 必要性が高いもの（情報保護評価（全項目評価）の実施）

(参考資料3「情報保護評価の実施の仕組み(案)」ご参照)

ただし情報保護評価の対象は、上記第3の通り、「番号」に係る個人情報を取り扱うシステムであるため、マイナンバー(「番号」)を利用するもの又は情報連携基盤を利用するものについてのみ、しきい値評価を行うこととする。

i 対象外

- ①行政機関又は関係機関にてしきい値評価を実施
- ②しきい値評価質問票に答えることで、対象外であることが確認される

○ iについても、しきい値評価報告書(参考資料2 情報保護評価の必要性の判断(しきい値評価)基準(案)の回答部分)を公開するべきか。

ii 必要性が高くないもの

- ①行政機関又は関係機関にてしきい値評価を実施
- (論点) ②行政機関又は関係機関にて情報保護評価(重点項目評価)報告書を作成する
- 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、審査対象を抽出してサンプリングチェック(※2)
- ⑤しきい値評価報告書及び情報保護評価(重点項目評価)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(⑤)。ただし、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…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（④）ことで、杜撰な評価がなされないようにする。

また、しきい値評価実施後に何らかの問題があった際は、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しきい値評価を通じて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。

※ 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。

※（論点）情報保護評価（重点項目評価）報告書の記載様式項目は、情報保護評価（全項目評価）報告書の記載様式項目を簡略化する形で作成してはどうか。

（参考資料 4 「情報保護評価（重点項目評価）報告書の記載様式項目（案）」ご参照）

iii 必要性が高いもの

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

(論点 1) ②行政機関又は関係機関にて情報保護評価 (全項目評価)
報告書を作成する

(論点 2) ③パブリックコメント等で広く国民の意見を求める

④第三者機関にて、全件について、評価の内容面及び手続面審査を行う

⑤しきい値評価報告書及び情報保護評価 (全項目評価) 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)。また、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全件審査する (④)。

※ (論点 1) 情報保護評価 (全項目評価) 報告書の記載事項は、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 5「情報保護評価 (全項目評価) 報告書の記載事項 (案)」

ご参照)

※ (論点 2) 国民の意見聴取はどのようにあるべきか (全件義務付ける
べきか、対象を限定して義務付けるべきか、各機関の裁量に
よるべきか)。

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とする。

- 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ものとする。

4 報告書の公表について

- 報告書の全文公表を原則義務付けることとする。
- ただし、報告書全文を公表することで情報セキュリティ上のリスクとなりうる場合⁸や安全保障上のリスクとなりうる場合も考えられ、かかる懸念を有する情報保有機関が第三者機関に対しても不十分な情報しか提供しないことも考えられることから、一定の場合には、第三者機関へは全文を提出した上で、国民に対しては要約を公表することとしてはどうか。
- 国民に対して要約を公表する場合は、第三者機関へ提出する報告書に、どの部分を要約公表とするのか、なぜ要約公表とするのかを記載することとし、その内容や理由付け等が不十分であると第三者機関が判断した場合には、第三者機関が是正を促すことが考えられる。
- また、報告書の一覧性を確保するために、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が考えられる。

第6 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こととすることが考えられる。

以上

⁸ たとえば、ネットワーク構成、サーバ構成、アプリケーションのバージョン情報、サーバの物理的位置などを公表すると、セキュリティ上のリスクとなりうることが考えられる。