

## 第7回戸籍システム検討ワーキンググループ 議事要旨

- 1 日 時：平成28年1月19日（火）15：59～18：06
- 2 場 所：法務省民事局会議室
- 3 出席者：安達座長，石井委員，遠藤委員，小澤委員，小松崎委員，酒井委員，高橋委員，高柳委員，中村委員，平野委員，穂積委員，本間委員，鷺崎委員，手塚オブザーバー
- 4 概 要：法務省から，配布資料に関する説明を行った後，自由討論が行われ，大要，以下のような指摘等がされた。

### 【新システムにおける戸籍情報保護方針の検討について】

- 最近，それぞれは秘匿性が高く，個人の特特定がされないよう個人情報が保護されているはずのデータについて，想定外のデータと突き合わせたり，組み合わせたりすることで個人の特特定が可能となってしまう等の問題も起きている。プライバシーや個人情報の保護は，突き詰めると本人の意図や希望に沿った情報の二次利用がされているかどうかというのがポイントになるので，想定される主要な情報連携を念頭に置いて検討を進めた方が良い。
  - ・ このワーキンググループでは，情報連携の相手方のシステムまで議論できるわけではないので，まずは戸籍情報を提供するとしたら，どのような形で提供するのかという形で検討することになる。
  - ・ マイナンバーを制度設計した際と異なり，戸籍については，将来的な戸籍情報の保持形態によっては，制度を動かしていく前に，戸籍情報を集めるというフェーズが入ってくるので，そのフェーズでの法的及びシステムの保護措置を別途考えておく必要があるのではないか。
  - ・ 情報連携をしたときの国民にとっての新たな利益と，情報連携をすることで想定されるリスクを秤にかけるような視点がないと，リスク面だけ論じていても，結論が出せないのではないか。
- 情報が漏れることは，一般論ではリスクと言えるが，情報が漏れること自体を絶対に起こってはいけないこととすると，そのリスクへの対策が形骸化してしまう。その情報が漏れるとどういう被害があるかということまで考慮して，リスクを網羅的に一覧しつつ，リスクの軽重の見極めをしなければならない。
  - ・ 確率としてどれぐらい起こり得るリスクなのか，一度起きるか，起きないかということについて対策をとるのか等，リスクの発生確率も観点として必要になる。
  - ・ 情報漏えいが，悪意のある攻撃を受けて生ずる場合と悪意のない過誤による場合の違いは，最終的には，リスクのレベル，確率と被害の度合いの違いとして考えていくことになる。さらに，確率や被害の度合いが，どれぐらいの確信度で見積もられているかが重要であり，それは過去の事例で裏付けていくしかない。
  - ・ NISC（内閣サイバーセキュリティセンター）から政府機関の情報セキュリティ対策の統一基準が示されているので，リスクの洗い出しというところは，ある程度整理されている。ただ，現在，考えられる最高峰のセキュリティ対策を行ったとしても，数年後，陳腐化する可能性もあるので，セキュリティの方針や教育訓練といったところのPDCAが可能になるような運用まで見据えた形でのセキュリティ対策が必要ではないか。

- このワーキンググループでは、最終的にシステムをどのようにするかを検討するので、システム構成をイメージしてリスク評価をしていかないといけない。特に整理が必要なのは、マイナンバーとは関係なく、まず戸籍としてどのようなリスクが考えられるかということと、マイナンバーと接続した場合、どのようなリスクが発生するかということで、サブシステムまで考えて議論していかないと、整理が難しいのではないかと。
  - 戸籍システムにおいてマイナンバーを使う業務と使わない業務を分ける整理が必要ではないか。戸籍事務の中でマイナンバーを利用しない場合は、その中ではマイナンバーは関係ないので、戸籍制度側で考えればいい話だが、戸籍事務の中でマイナンバーを利用する場合は、きっちり考えていかなければいけない。ステップを追ってどこにリスクがあるのか、最終的にどういうデータベース構造で情報を置くか、特定個人情報ファイルをどのように定義するのかを決めて、それに対する特定個人情報保護評価をする必要がある。
  - マイナンバーの関係では、年金等様々なシステムがマイナンバーに接続するときに、特定個人情報保護評価をやっているもので、ほかで検討したものをうまく活用しながら、まとめていくこともできるのではないかと。
- システムの形態としては、全部集中化した方が合理的な気がするが、現状のように分散させることで情報漏えい等の問題が発生する範囲を限定するという考え方もある。システムの形態を考えるに当たっての視点、アプローチはどう考えるべきか。
- アプローチとしては、外部との連携を含めてシステム全体というレベルでのリスクと対策がどうあるべきかを検討し、そこからサブシステム、モジュールという「全体」から「部分」へという段階的な進め方が考えられる。
  - 重要な視点としては二つあり、一つは何かが起こった時に、どういう手順で誰が、何をしたかということを追跡できるかどうかサービスへの信頼性に大きな影響を与える。もう一つは、なぜこの情報にアクセスしたかというアカウントビリティであり、戸籍のような情報を扱う場合は、トレーサビリティとアカウントビリティを他のシステム以上に強固にしておくべきではないか。
  - 情報セキュリティでは、情報の性質も大事な視点となる。情報に対してどれだけのセキュリティ強度を持たせるかについて、マイナンバーの場合は、マイナンバーと紐付いたデータを特定個人情報として厳格に取り扱うこととしている。戸籍の場合も、システムの中でどの情報を守るのかということを確認にして、位置付けを検討することが考えられる。

以 上