

第2回 情報連携基盤技術ワーキンググループ
議事要旨

日時：平成23年3月4日（金）10：00～12：00

場所：三田共用会議所3階大会議室

出席者：佐々木良一委員（座長）、大山永昭委員（座長代理）、新井悠委員（代理）、
飯島淳一委員、小松文子委員、坂本泰久委員、神成淳司委員、手塚悟委員、
戸田夏生委員、松本泰委員、山口英委員、池田大造委員、崎村夏彦委員、
實川昌幸委員、鈴木尊己委員、中上昇一委員、長島哲也委員、坂東和彦委員、
宮坂肇委員、吉丸邦昭委員、吉本明平委員

（議事次第）

1. 開会

2. 議事

（1）情報連携基盤技術に関する論点項目

（2）番号制度 番号連携イメージ

（3）情報連携基盤技術に係る骨格案（個人に関する付番、番号連携及び情報連携）

（4）今後の開催日程

3. 参考資料

（1）情報連携基盤技術ユーザーサブWG報告

（2）第2回個人情報保護WG提出資料（骨格案）

（配付資料）

資料1：主要な論点リスト（案）

資料2：番号制度 番号連携イメージ

資料3：社会保障・税に関わる番号制度及び国民ID制度における情報連携基盤技術の骨格案（その1）

資料4：情報連携基盤技術WGの今後の開催日程について

資料5：情報連携機能の開発に留意すべきこと（山口構成員提出資料）

参考資料1：情報連携基盤技術ユーザーサブWG報告資料

参考資料2：第2回個人情報保護WG提出資料（骨格案）

(会議概要)

議事

事務局より配付資料3、参考資料1、参考資料2を説明。

山口委員より提出意見を説明。

○ 一点目として、アクセスログについて、第三者機関における解析機能や閲覧のワンストップ性を考慮しつつ、信頼し得るセキュアなクリアリングハウスで集中管理する方式も考えてはどうか。分散管理によっても、情報保有機関におけるアクセスログの改ざんは解決できない。また、開示請求についても何段ものプロセスを経ることになる。第三者機関の下で集中管理をすることを考えたかどうか。ただし、情報保有機関でもアクセスログを保有する必要がある。

二点目として、アーキテクチャについて定量的な検討を開始するべきという点である。常に連携のシステムでは失効処理というものが非常に重い処理であり、リアルタイムで番号の有効性等を確認することがシステム設計上必要であるが、現在は性能的な指標がなく、定性的に考えられている。

三点目として、まずプロトタイプを開発し、機能検証や性能予測の改定等を行しながら、スパイラル・ディベロップメント等を行ってはどうか。この手の大規模システムの開発は、一発で成功するという事は難しく、大抵失敗しながら前に進んでいく。バックオフィス連携やビジネスプロセスの最適化、各システムの適応タイミングを合わせて実現させることは奇跡である。したがって、かなり慎重なプロセスを経た方が良い。予算を多めにしても、大きな失敗をしないというロードマップを作ることも重要である。

各委員から、以下のような発言がなされた。

○ 付番と番号連携に関して、一つ一つのトランザクション毎に暗号演算する性能の検証が必要である。

付番については、住民票コードが変更される場合に、IDコードやリンクコードが変更されるのか。住民票コードが変更されたときの履歴管理方法、リンクコードの生成タイミングについて検討が必要である。

初期突合時に、同じ住所でも表記方法の違いにより機械的には識別できない可能性がある。住基ネットの4情報と各情報保有機関の4情報のフォーマットは異なるため、4情報を初期突合に利用することについて、検討が必要である。

マイポータルにログインするときに、「番号」を使えないのかと言われそうな気がする。「番号」を使ってマイポータルにログインし、情報を得たいという場合もあるのではないか。

また、暗号演算のための鍵管理を厳重にできるような仕組みが必要である。

○ 性能の問題、システムのサイズに伴うコスト及び効果の問題については、今後も検討

が必要である。まずは機能面の検討を行いたい。

- 乱数表の鍵の管理の仕方が重要である。鍵を分割して、一部を第三者機関に持たせるなど、さまざまな管理方法が考えられる。
- 住民票コードとまったく関連性のないコードを住民票コードから作るということが重要であり、乱数に決め打ちしなくてもよいのではないか。
- 共通基盤として対応する範囲は、段階的には、国で閉じるもの、地方自治体も関係するもの、民間も含まれるものなどのフェーズに分類できるが、その中で効果的なものにターゲットを絞って、具体的なプロセスを明らかにしていくことが必要ではないか。業務の面からも小さなところから着実に実現していくことが必要。共通番号の使用は、当面何をターゲットに考えているか。
- 税と社会保障分野でのユースケースへの適用可能性を検討しているところである。年金と税の分野だけで利用するような意見もあれば、民間利用の意見もあり、幅広い意見が出ている一方で、利用開始のスケジュールが基本方針に示されているところである。2015年1月のスタートは、適用分野を絞って確実に実現すべきという提案だと思うが、6月までには情報連携基盤を着実に機能させるための技術的な議論と社会的な適用分野の議論を合わせて整理しなければならないと考えている。
- 正式なスタートは全員が使える仕組みになっていないと不公平が生じるのではないか。スモールスタートとしたいが、あまり狭い範囲でスタートはさせられないのではないか。
- 過去に情報連携等の経験がない中で、技術的に不安である。ステップを慎重に踏むべきではないか。開発のスケジュールを遅らせるべきである。将来、民間あるいは多くの行政分野を考えたときには技術的な面で慎重さが必要になる。
- 銀行システムの統合の例を見ても、時間がかかることは間違いない。期間の問題については、もう一回最後のところでぜひ議論したいと考えている。一方で、正式スタート時には、スモールスタートには向かないシステムという意見もあるだろう。
- リンクコードを情報連携基盤にも保有しないという安全重視の設計は、チャレンジする価値がある。情報連携基盤でアクセスログを保存する場合のキーの値としては、今のところIDコードが必要なのではないか。また、住民票コードの一覧を情報連携基盤に置くことはリスクがあるので、それに代わる4情報突合のための連携表が必要なのではないか。
- アクセスログに関しては、資料2のような図を描いてしっかり議論したい。ログを集

中管理型にすると、いろいろな方面に影響がありそうである。住基ネット時の最高裁判決例を考えると、どのようにログを管理するか、どこまで集中管理が許されるか、検討が必要である。

- データマッチングについて抑制的にスタートするだろうと理解している。情報流通を国民に明らかにするためにも、情報連携基盤を通じて連携することは守るべきである。住基ネットでは、どこからどこへ誰がアクセスしたか、というログを残しているが、国民提供用に簡略化したログも作成している。また、利用履歴自体がセンシティブな情報と考えて、ログの集中管理は行っていない。

住基ネットに関して、住民からのログの開示請求は、実際にはほとんどない。不正アクセスの解析や犯罪捜査等のためであれば、多少手間がかかっても各所からログを集めればよいのではないか。

情報保有機関が最新の4情報を保持する必要がある。しかし、住基ネットとの連携頻度が高まると考えると、変換テーブル方式を使用する案がパフォーマンスの面からよいと評価している。

- 第三者機関の下にログを集中管理するという意味は、本来アクセスログの解析や監視を行う、不正アクセスの監視を行うべき機関の下に、ログを集中的において突合させる機能を持たせたらどうかという提案であり、政府で集中管理するという提案ではないので誤解のないようにお願いしたい。

- 医療機関等については、PHRに関するモデル事業を来年度から3年間実施する予定であり、そちらの議論とも連携しておいた方がよい。医療機関は情報漏洩に厳しい制約を求めるが、一方で薬局にもメリットがないと導入が進まない。個人情報の種類やパターン、ログの使用範囲、使用目的等の議論が進んでおり、その辺の議論を連携させていきたい。なお、モデル事業では、番号制度の導入については議論されていない。

- 情報連携基盤と個人情報保護の骨格案には、個人の同意に基づく個人情報の目的外利用の視点が不足しており、検討すべきではないか。プッシュ型の行政サービスでは、個人にとっての利便性の観点から、個人の同意のもとに個人情報の目的外の利用を行う傾向にある。この時、個人の同意をどうとらえるか、情報連携基盤にどうやって組み込むかという視点が必要である。

- アクセスログの集中管理について、例えば利用回数や見た時間等の最低限の情報だけを集中管理する案も考えられないか。第三者機関といえども外部からの脅威があるため、すべてを集中管理することは望ましくない。

- 既存の情報保有機関のシステム改修は相当の規模になり、時間がかかることが予想される。そのため、情報保有機関側の負担を考慮することが重要である。一方で、情報連

携基盤の連携機関数と機能に関係はなく、スモールスタートにしても負担は軽減されない。

番号を作ることが目的化しないように注意が必要である。例えばワンストップ・サービスでは、本人同意をどう取るか、手続きの進捗をどう確認するか等、情報連携基盤に必要な機能等をユースケースから整理して欲しい。

- この制度が開始されても、紙を使った手続きも残ることに留意が必要である。
- 法定調書を申告する民間事業者も情報保有機関として扱われ、アクセスログを取得する対象となるのか今の案ではわからない。また、番号を提示するときその番号が正しいかどうかの確認はどうするのか。金融機関などでは、郵送など、本人に番号を書いていただくことも考えられる。番号をチェックする業務フローはどうか。
- リンクコードが永続的な場合は、攻撃によりIDコードを暴露される可能性があるため、リンクコードの永続性をセキュリティの観点から検討しておくべきである。一方で、変更することになると運用やシステムに負担がかかるため、バランスを考える必要がある。
- 「番号」そのものを一定期間で変更する方法も検討しておく必要がある。
- 情報保有機関の対照テーブルについて、リンクコード、番号、利用番号、住所情報などの4情報の紐付けが本当にできるのか。マイポータルにアクセスするクレデンシャルの発行は可能か。リンクコードと番号を紐付けするユースケースについて、住基ネットを使用する場合および使用しない場合で検討していただきたい。特に紐付け作業でどのようなエラーが考えられるか整理して欲しい。
- カード発行時の本人の確認は課題である。確認方法等について、十分に時間をかけて検討する必要がある。
- システムのアプリケーションの範囲をどう見定めていくかがポイントであると思われる。アプリケーションが定まらないと、収集したログの適切性が判断できない。
- 個人情報保護の特別法で対象としている「番号に係る情報」というのは、「番号」とそれに係る情報と解釈すればいいのか。海外では、番号だけが流通してしまい勝手に利用されることを不安に思っていることもあるため、「番号に係る情報」の範囲が理解できなかった。例えば、民間事業者において、様々な情報を識別するために「番号」を使うという場合の取り扱いが対象となるのか疑問である。
- 「番号」と「番号」に紐付けられた属性情報のことであり、これらを保護の対象とし

ている。

- 個人情報是一定の目的をもって収集されるが、その後、本人の希望、同意を持って他の目的にも広く活用したいという場合がありうる。「目的外利用」の検討ではそのような活用を検討する必要があるのでは。
- 先進的な電子政府では個人の同意に基づき個人情報を利用するという方向にあると思っている。同意とは何かをシステムのりまたは制度的に明確にしなければいけない。行政組織等が持つ個人情報の民間利用のほとんどが個人の同意に基づくものと思われる。ユースケースを示されるとイメージができるのではないか。その上で制度的なフレームワークを議論すべきである。
- 安全性を重視するばかりに効率性が失われないよう、バランスが重要である。
- 昨年の調査で、個人情報の管理、責任を誰が持つべきかという日本とEUを比較した結果、日本人は個人が責任を持ちたがらないことが分かった。個人情報の管理責任を、個人が持つか、企業が持つか、国などが持つかという選択肢の中で、日本人の特性もあって、個人に対してどれだけ情報をコントロールさせることができるか考慮しなければいけない。
- 分野別の多段方式の場合、処理工数が増えることになる。システム的な実効性の検証が必要である。
- 性能の問題、開発費、開発期間などについても検討課題がある。
- 次回WGは3月15日を予定している。

以上