

第5回情報連携基盤技術WG意見書

2011年6月16日

情報連携基盤技術 WG 構成員 宮坂肇

表題の件につきまして、下記の通り意見を申し上げます。

1. 番号連携方式に係る意見(第5回WG資料3-1、3-2)

(1)本WGにおける検討の進め方について

案1～案5における方式比較にあたり、案1は「社会保障・税番号要綱」(第5回WG資料4-2, P.5)における基本的な考え方から逸脱することから、検討の対象外としてもよいのではないかと考えます。

また案1を除いた案2～案5は、符号変換方式による違い(可逆暗号方式とコード変換テーブル方式)と情報連携用符号の付番単位による違い(共通の符号を共有する範囲)との組み合わせであることから、その比較にあたり、双方の論点に絞った検討を行うことが効率的であると考えます。

更に、上記の論点の検討にあたり、後者はプライバシーへの影響等の制度面の色合いが濃いことから個人情報保護WGと共同検討を行いつつ、本WGとしては前者の符号変換方式による違いについての検討を優先させ、技術的視点に立った実現性や運用コスト等の比較を行ってはいかがでしょうか。

(2)符号変換方式における検討要素

符号変換方式の比較に当たり、第5回WG資料3-1、3-2に示される検討要素に加え、私が検討の必要性を認識している項目について別表1に示します。尚、別表1において影響度の評価は案であり、今後の詳細検討にて正確に評価を行うこととしてはいかがでしょうか。

(3)情報連携用符号の付番単位における検討要素

情報連携用符号の付番単位として、案3ではすべての情報保有機関にリンクコードを付番する、案4は特定分野で同じIDコードを付番する、案5は特定分野で同じリンクコードを付番する、としておりますが、実質的には案4と案5は同義と見なせる為、すべての情報保有機関に別の符号を付番するか(案A)、特定分野の機関には共通の符号を付番するか(案B)、という論点に絞ることができると考えます。

これより、第5回WG資料3-1、3-2に示される検討要素に対し、当該論点に係るものを絞ると別表2のようになるものと考えられ、これらについて検討が必要であるものと考えます。尚、別表2において影響度の評価は案であり、今後の詳細検討にて正確に評価を行うこととしてはいかがでしょうか。

2. データ送受信方式に係る意見(第5回WG資料3-1、3-3)

方式の採否にあたっては、コストや信頼性等の観点において、連携対象とするデータのサイズやその頻度、また情報連携基盤や情報保有機関におけるシステム稼働時間や信頼性要件、更に情報保有機関におけるネットワーク接続性や帯域等の総合的な判断が必要となるものと考えられ、両方式共に一長一短であると考えます。そのような意味では、方式の採否を行わず、両方式の特性を鑑み使い分けを行う選択肢もあるものと考えます。

一方で、資料 3-3 に示されるプライバシー影響度の観点では、大きく考えが分かれることが予想され、制度面で当該観点に沿った方式の採否が求められる可能性もあることから、個人情報保護 WG やプライバシー影響評価に係る有識者との共同検討を経て、今後の議論を進めていくことが肝要と考えます。

3. 代理機能や扶養情報の管理に係る意見

個人の属性情報として代理人との関係や扶養関係を基盤で管理する等の議論がありましたが、システムの実現方法の議論を行う前に、これらの法律上の定義やその解釈、及び番号制度にて対象となるユースケースを鑑みこれらを管理する仕組みの必要性について先んじて議論をする必要があるものと考えます。

また、これらの管理において最も課題となる事項として、代理人における権限や当該本人における委任意志、及び扶養関係の事実確認が考えられ、本WGのスコープである番号制度における個人情報保護や情報連携における技術検討とは別の観点に立った議論が必要になるものと考えます。

4. アクセスログに係る意見

WG では、アクセスログの保管場所やアクセスログの保護方法等が議論されていましたが、第三者機関による監視、監査及び監督等の制度的要件を踏まえ、情報連携基盤及び情報保有機関間で分散管理されるログの証拠性や監査性をどのレベルまで保証する必要があるのか、ログに保持すべきデータ項目の内容やその粒度によっても、集積されたログそのものに対してプライバシーへの影響が発生する可能性がある、ログの管理、保全に関するシステムコストが膨大となる可能性がある等の課題が考えられます。

この論点につきましても、上記の制度的側面を意識した検討が不可欠である為、個人情報保護 WG との共同検討を経て議論を進めていく必要であるものと考えます。

別表1. 符号変換方式における検討要素とその影響度

検討要素		主な懸念等	影響度
1	符号生成時の処理性能	<ul style="list-style-type: none"> コード変換テーブル方式の場合、乱数生成時間に加え、テーブル内の重複チェックと重複時の再乱数生成が必要になります。 	中
2	高負荷時の符号変換処理性能とコスト	<ul style="list-style-type: none"> 可逆暗号方式の場合、暗号処理速度に加え、暗号処理装置の並列化・冗長化が必要となります。 	小
		<ul style="list-style-type: none"> コード変換テーブル方式の場合、テーブル検索速度やデータベースサーバとの通信処理に加え、データベースサーバの並列化・冗長化が必要となります。 	中
3	国民の出生や在留外国人等の追加及び情報保有機関が増大した際の処理性能とコスト	<ul style="list-style-type: none"> コード変換テーブル方式の場合、国民(出生や在留外国人等)や情報保有機関を追加する度に該当分のレコード領域の確保が必要となります。また検索対象レコードの増大に伴い、テーブル検索速度が低下します。 	大
4	障害時及び災害時の信頼性確保	<p>障害時及び災害時の信頼性確保策として2センターによる運用とした場合、下記を考慮する必要があります。</p> <ul style="list-style-type: none"> 可逆暗号方式の場合、センター間で暗号処理装置の暗号鍵データの共有が必要となります。 	小
		<ul style="list-style-type: none"> コード変換テーブル方式の場合、センター間で日々更新されるテーブルの同期が必要となります。 	大
5	障害時の復旧コスト	<p>単一拠点内で機器等の障害が起こった場合の復旧コストとして下記を考慮する必要があります。</p> <ul style="list-style-type: none"> 可逆暗号方式の場合、暗号処理に用いる暗号鍵のバックアップを行った上で、復旧時には暗号処理装置への再設定作業が必要となります。 	小
		<ul style="list-style-type: none"> コード変換テーブル方式の場合、日々更新されるテーブルの定期的なバックアップを行った上で、復旧時にはテーブルの復元作業が必要となります。 	中
6	一元管理性(※)	<ul style="list-style-type: none"> コード変換テーブル方式の場合、情報連携基盤にてすべての情報保有機関におけるリンクコードを電磁的手段で記録することとなる為、一元管理と見なされる可能性があります。 	大

※「社会保障・税番号要綱」(第5回WG資料4-2, P.5)「6. 住民基本台帳ネットワークシステム最高裁判決との関係」の②に定義される用語とします。

別表2. 情報連携用符号の付番単位における検討要素とその影響度

	検討要素	主な懸念等	影響度
1	符号変換性能及びコスト	<ul style="list-style-type: none"> 案Bの場合は特定分野の機関間の符号変換が不要であるのに対し、案Aの場合はすべての機関間の符号変換を必要とする為、当該処理に係る性能やコストを考慮する必要があります。 	小
2	不正マッチングのリスク	<ul style="list-style-type: none"> 案Bの場合、特定分野の機関間で同一の符号を用いる為、情報連携基盤を介さず当該機関間で同一符号による不正マッチングが行われるリスクがあり、これを抑制するための手段を検討する必要があります。 	大