資料3－8

平成 23 年 6 月 17 日
情報連携基盤技術ワーキング・グループ　構成員
長島　哲也

第 5 回情報連携基盤技術ワーキンググループ開催時に配布された資料に関する意見

1．情報連携方式と番号連携方式の関連性と取り得る組み合わせについて

第 1 回～第 4 回情報連携基盤技術ワーキンググループ開催時に提示された情報連携基盤に持つべき機能の内、番号連携機能や情報連携機能が対応しなければならない要件や制約として下記の文書が要綱に示されている。

> 「社会保障･税番号要綱」の P5 下部に下記、番号連携に関する国民の懸念への対応策が記述されている。
>
> 「②「個人情報の追跡・突合に対する懸念」については、(a)～略～情報保有機関～略～による**分散管理**とし、(b)～略～**「番号」を情報連携の手段として直接用いず**、当該個人を特定するための情報連携基盤等及び情報保有機関のみで用いる**符号を用いる**こととし、(c)さらに**当該符号を「番号」から推測できない**ような措置を講じる。」

また、「個人情報の一元管理」に関する要件や制約は下記の様に指摘されている。

> 「社会保障･税番号要綱」の P5 上部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、②**個人情報を一元的に管理することができる機関又は主体が存在しないこと。**また、「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）の P1 「第1 個人に対する付番、番号連携及び情報連携」「1．基本的な考え方」の（2）情報連携基盤の構築に当たっては、住民基本台帳ネットワークシステム（以下「住基ネット」という。）に係る最高裁合憲判決（最判平成20年3月6日）で示された個人情報を一元的に管理することができる機関又は主体が存在しないこと、 ～中略～ **より一層高度の安全性を確保することが求められるのではないか。」**

さらに、要綱に示された「番号」や符号そのものの取り扱いについては、個人情報保護ワーキンググループの意見として「個人を特定する ID」や「ID を暗号化した符号」も個人情報と認識する委員が多かった。これらの骨格案や要綱、個人情報保護 WG の意見をまとめると番号連携機能や情報連携機能に対して下記「要件または制約」が課せられると認識する。

要件①:「番号」を用いた情報連携をしてはいけない
要件②:他情報保有機関が利用している「符号」と、自情報保有機関が利用している「符号」を一元的に管理してはいけない

これら番号連携機能や情報連携機能に関しての「要件または制約」を加味した上で、第 5 回情報連携基盤技術ワーキンググループで提示された「情報連携基盤構築に当たっての論点整理」（資料３－１、資料３－２、資料３－３）中の番号連携方式(【案1】～【案5】)、および、情報連携方式(【案1】「ゲートウェイ方式」、【案2】「アクセストークン方式」)について、システム設計における両方式(番号連携方式と情報連携方式)の実現可能性や関連性について検討した結果、実現可能性に関する懸念や両方式間の関連性が及ぼすシステム構築上の要件が発見されたため、ここに報告する。

- **検討結果－１**

  番号連携方式【案１：全ての情報保有機関間で「番号」を用いて情報連携を行う方式】については前述の「要件①:「番号」を用いた情報連携をしてはいけない」を満たせないため、実現可能性が低い。

- **検討結果－２**

  情報連携方式に「アクセストークン方式」を採用した場合、後述の理由**＜アクセストークン方式による情報連携の検討＞**により、要綱や骨格案で提示された番号連携機能や情報連携機能に際しての「要件または制約」を満足できる番号連携方式は【案2】、【案3】のみである【しかし、この番号連携方式を用いた情報連携方式はゲートウェイ方式に極めて酷似している】。

  ＜アクセストークン方式による情報連携の検討＞

  アクセストークン方式で情報連携を開始する前処理として、アクセストークンを用いた連携許可の処理が全て完了し、情報連携を行う2者間の通信内容【図１参照】を詳細に検討した。この際、通信メッセージ(コンテンツ)内で個人を特定するID（識別子)として、番号連携方式で候補となっている ID のうち、何がふさわしいかを前述の「要件①」と「要件②」を踏まえ考察した。【図2参照】。

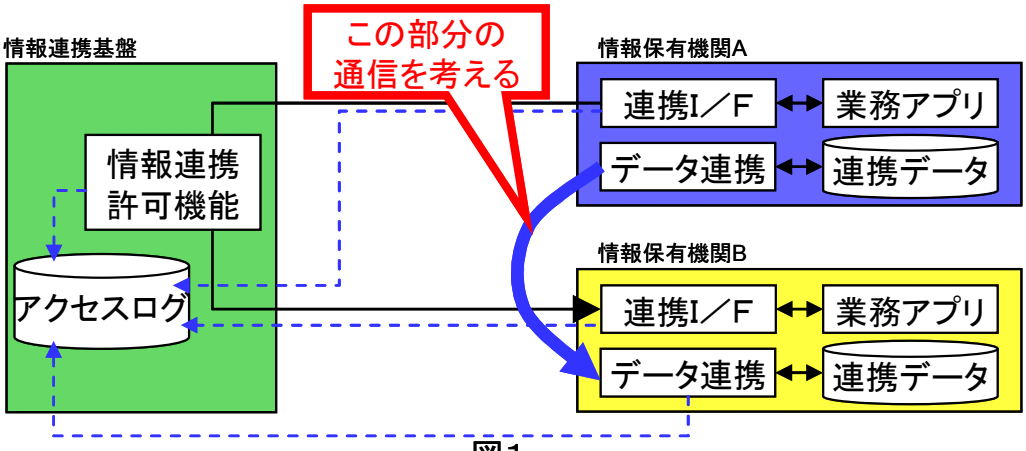

図1

図2の吹き出しに記載したように「要件②」で指摘されている「リンクコード a とリンクコード b

が同時に同一情報保有機関で保有してしまう危険性」や「リンクコード a とリンクコード b が同一情報保有者である事を示す情報を当該情報保有機関以外のどこかに保有しないと処理が完結しない」問題点が発生する。しかし、同一情報保有者である事を示す情報、すなわち、リンクコード a とリンクコード b を同時に保有する事自体が「要件②」に抵触する。また、図1中の仮名 ID に「番号」を指定する事も考えられるが、これは「要件①」に抵触する。また、仮名 ID に ID コードを指定する事も考えられるが、個人情報保護ワーキンググループの意見では、ID コードそのものも「個人を特定する ID」や「ID を暗号化した符号」と認識する委員が多かった事を踏まえると、「要件①」の範疇と認識される可能性が高く、抵触の可能性が高い。

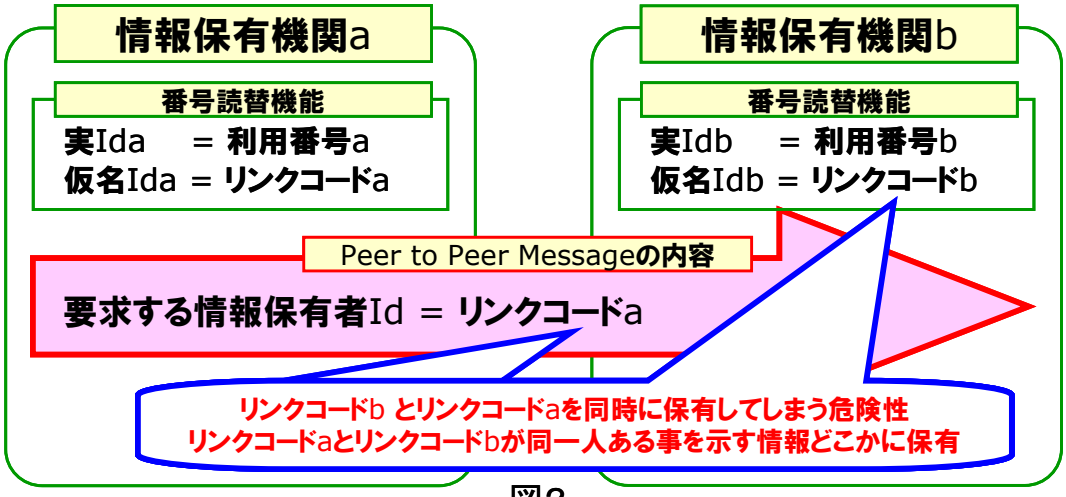

図2

この問題点は2者間通信の前提では解決できないため、3者間通信を前提とせざるを得ない【図3参照】。結局のところ、この方式はゲートウェイ方式に酷似しており、「要件①」「要件②」を前提としてアクセストークン方式を用いて情報連携実現可能性は低いと言わざるを得ない。

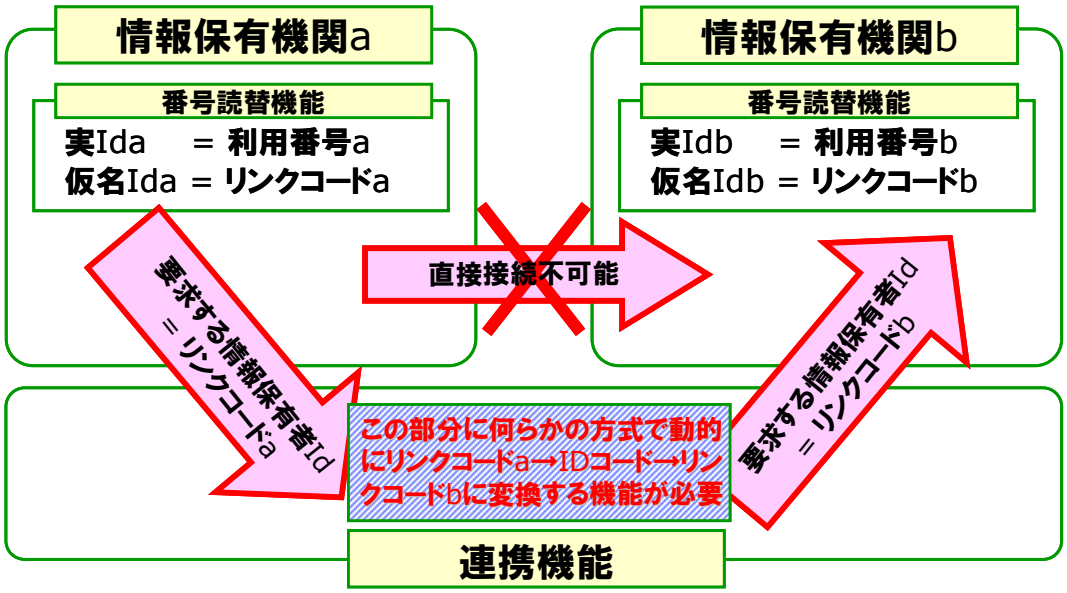

図3

以上の様な検討結果であったが、要綱や骨格案で指摘されている番号連携や情報連携の「要件や制約」の解釈が当意見の前提と異なり、下記の2つの要件が無くなり、2者間通信

> 要件①:「番号」を用いた情報連携をしてはいけない
> 要件②:他情報保有機関が利用している「符号」と、自情報保有機関が利用している「符号」を一元的に管理してはいけない

で情報連携を実現できた場合を想定する。その場合、同一 ID で番号連携している【案1】、【案4の「番号」を利用する機関又は特定の分野】および【案5の「番号」を利用する機関又は特定の分野】の3つの番号連携方式はアクセストークン情報連携が可能と考えられる。

- **検討結果－3**
  情報連携方式に「ゲートウェイ方式」を採用した場合、番号連携方式には【案1】～【案5】どの方式も適用可能である。ただし、「検討結果－1」より実質的には番号連携【案1】の実現可能性は低い。

結論として、情報連携方式と番号連携方式には下記の関連性が存在し、要綱の内容に鑑みた場合、ゲートウェイ方式の方が優位と思われる。

		情報連携方式	
		ゲートウェイ方式	アクセストークン方式
番号連携方式	案1 全ての情報保有機関間で「番号」を用いて情報連携を行う方式	○ 要綱記載の対応策を講じるとすると、等案は条件を満たせない。	×
	案2 各情報保有機関毎に異なるリンクコード割り当て.共通するIDコードを経由して双方を紐付け、情報連携する方式	○	△ 極めてケートウェイ方式に酷似
	案3 各情報保有機関毎に異なるリンクコード割り当て.共通するIDコードを経由して双方を紐付け、情報連携する方式	○	△ 極めてケートウェイ方式に酷似
	案4 「番号」を利用する機関間又は持定の分野内での連携は共通のIDコード用いそれ以外は機関毎に異なるリンクコードを割り当て、情報連携する方式。	○	×
	案5 「番号」を利用する機関間又は持定の分野内での連携は共通のリンクコード用いそれ以外は機関毎に異なるリンクコードを割り当て、情報連携する方式。	○	×

2. 情報連携方式の比較について

「情報連携基盤構築に当たっての論点整理」に示されている情報連携方式である「ゲートウェイ方式」と「アクセストークン方式」の比較に関して、システム構築という観点を中心に意見を述べる。

「社会保障・税番号要綱」で例示として揚げられている利用範囲の大半が地方公共団体を含んでいることから、情報連携を行う情報保有機関は少なくとも約 1,750 の市町村が対象と考えられ、さら省庁関連の行政組織を加えて約 2,000 におよぶ情報保有機関の連携を想定するべきと考える。情報連携をするために、これらの情報保有機関間を接続するため形態を以下図4に示す。

ゲートウェイ方式　　**アクセストークン方式**

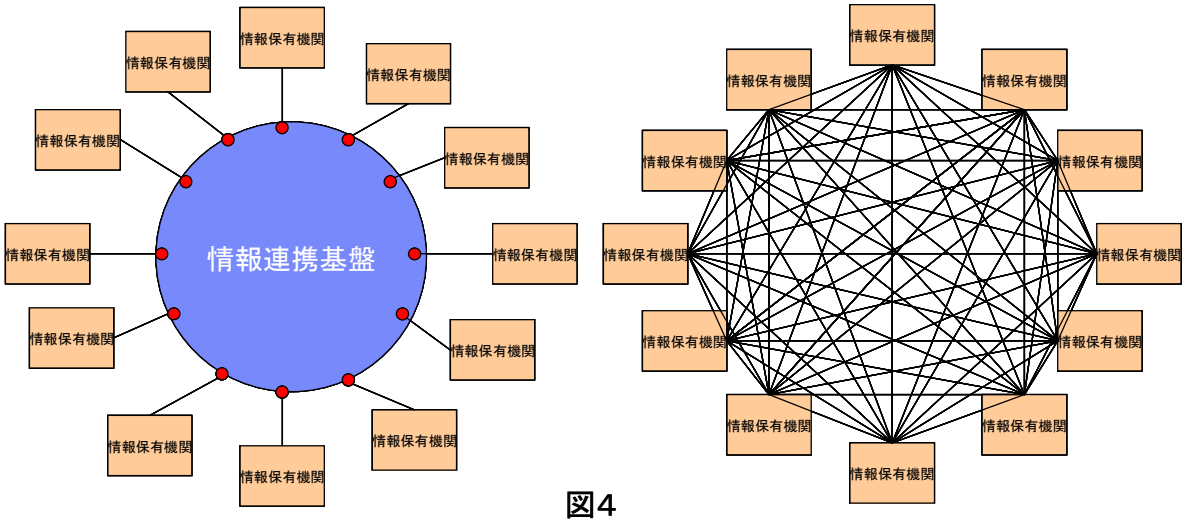

図4

このような接続形態における連携インターフェースの構築を考えた場合、構築・設定・テストが必要となる対象接続数は、両方式の接続形態の違いから以下図5のような規模になると考えられる。

- **ゲートウェイ方式**
- 2,000 x 1 = 2,000接続

アクセストークン方式

2,000 x (2,000-1) ÷ 2 = 1,999,000接続

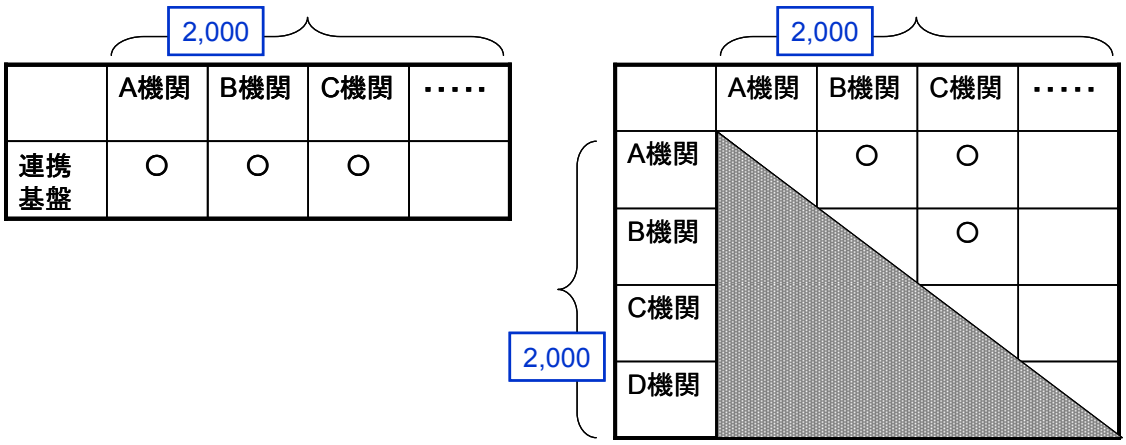

図5

前述のような接続数の差異に加えて、両方式の違いに起因する連携インターフェースの構築・設定・テスト等にかかる作業内容や、運用・管理、性能などを以下のように比較した。

比較項目	アクセス・トークン方式 （拠点間直接接続）	ゲートウェイ方式 （連携基盤経由接続）
情報保有機関間の接続数	1,999,000接続	2,000接続
システム構築（新規/変更/追加） ネットワーク アプリケーション （プログラム・データ形式等）	各々の接続間で個別に設定・調整・テストが必要 各々の接続間で個別に開発・調整・テストが必要	連携基盤と各ノードとの間で設定・調整・テストのみ 各々の接続間で個別に設定・調整・テストが必要
ログ（証跡）管理	情報連携基盤および情報保有機関に分散	情報連携基盤側で集中管理
送受信性能 データ転送性能	論理的には直接接続なので、ゲートウェイ方式より優位だが、転送性能の大部分はネットワーク性能に依存するため差はほとんどない	論理的には間接接続なので、アクセストークン方式より劣位だが、転送性能の大部分はネットワーク性能に依存するため差はほとんどない
通信方式・形式等の標準化対応	各々の接続機関間で調整できてしまため、標準への統制が困難	情報連携基盤で統制できるため、標準化しやすい
障害時の影響	情報連携が2者間通信のため、障害時の影響は限定的に見えるが、アクセストークン発行には情報連携基盤が必要であるため、ゲートウェイ方式との差は軽微である	各情報保有機関間の連携に与える影響は大きい
適合領域	少数の機関間を接続する場合に優位	多数の機関間を接続する場合に優位

上記のようにシステム構築にかかる負荷のみならず、運用面や管理面をみても、接続数が膨大なことによる課題は多いと考える。多数の情報保有機関が情報を連携して、「社会保障・税番号要綱」に記述されているような「国民の利便性向上」を目指すためには、参加する情報保有機関に過度の負担をかけないような情報連携基盤を構築することが重要と考える。

以上