資料7

（第４回情報連携基盤技術WG（4/12）提出資料）

質問書提出の経緯

2011 年 4 月 11 日
情報連携基盤技術 WG 構成員
山口英

これまで情報連携基盤 WG の検討では、事務局提出の「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およびその２）が提示され、この文書を叩き台として議論を行ってきた。
この文書は、今後の法律検討、さらにはシステム設計の上流工程を行う場合の基本文書となる。ところが、この文書については（１）記述が曖昧な点が数多くある、（２）本来制度設計およびシステム設計において早期に検討すべき事項が将来検討事項として整理されているものがある、（３）さまざまな課題に対する解決方法には技術的解決と制度的解決があり、それらは相補的であり、また性質の異なるものであるにも関わらず、制度面での解決方法を提示しないまま技術的解決ばかりを考えるために無意味に複雑なシステムを構成している、（４）技術的合理性の無い設計が含まれている、（５）そもそも最高裁判決に対応することを上位要件にしているが、その技術的解釈を明確にしていない、等の問題がある。さらには、いわゆるシステムおよび制度設計の上位工程文書として読んだ場合、複数の選択肢とその基準が示されていないまま「〇〇としてはどうか」というような提案が行われているが、第二、第三の選択肢の提示も無いのは、設計の善し悪しを判断することも難しい。さらには、この文書は、通常の日本語から見ても、システムと制度を考える上で、解読が難解で、整合性についても疑問が残る。
このようなことから、山口から個人的に御願いをしたシステム開発および制度についての専門家（複数）と私的勉強会を開き、そこでどのような問題が有るかを検討した。その結果、膨大な疑問、質問、疑念がまとめられることになった。このような質問書を提出することは異例ではあるが、質問書が（第１版）と書かれているように、実はまだまだ質問が生まれてきている。
この質問書では、質問の趣旨、想定される答えなども記載した。これは、徒に事務局を混乱させることが目的ではなく、骨子案がよりよいものになるために、質問の趣旨を明記することで、当該記述箇所について再点検してほしく、さらには、もしも記述に不備があるならば、その修正を自ら行うことを促すことが目的である。
恐らく、骨格案は、霞ヶ関における各省協議を経て、中途半端な妥協、協議の結果、さらに意味不明な文書になることが予想される。そのような状況にならないためにも、現時点での骨子案が、明確かつ合理的に構成されることに資することを期待した質問書である。事務局における、真摯な対応を御願いしたい。
以上。

情報連携基盤技術に関する質問（第一版）

2011 年 4 月 11 日
情報連携基盤技術に関する私的勉強会
世話人 山口英

骨格案各事項の根拠への疑問

（情報連携基盤技術 WG 事務局にお答えいただきたい）

【質問先】
骨格案（その１）2 ページ
2.(3)情報保有機関ごとに付与されるリンクコードを用いる情報連携

【質問】
ID コードを情報保有機関と共有させないことについて、「情報保有機関ごとに異なるリンクコードを付与し、情報保有機関はそれぞれのリンクコードを用いて情報連携基盤にアクセスすることとすべきではないか」とあるが、その理由について、「仮にこれ（ID コード）を情報保有機関も共有し（略）こととすると、万一漏洩した際にはその影響が他の情報保有機関にも波及する可能性がある」からとされている。ここで、他の情報保有機関にも波及するという影響とは、どのような脅威のことを指しているのか。具体的に、ID コードが誰に漏洩した場合に、誰によってどのような「影響」がもたらされると想定しているのかを回答いただきたい。

【趣旨】
政府基本方針は、情報連携基盤について「各機関間の情報連携は情報連携基盤を通じて行わせることにより、情報連携基盤がデータのやり取りの承認やアクセス記録の保持を行い（略）個人情報保護に十分配慮した仕組みとする」としているが、その実現に際して、ID コードとリンクコードを用いた方式を採用する狙いは、はたして情報漏洩対策なのか。そうではないのではないか。

【想定される答え】
情報漏洩対策のつもりでこのようにした。政府基本方針の趣旨が情報漏洩対策以外のところにあるというのであれば、それが何なのか明らかにしたい。

【質問先】
骨格案（その１）2 ページ
3. (1)「番号」と ID コード・リンクコードの付番のあり方

【質問】
「住民票コードから『番号』を生成する方式と、住民票コードから ID コード、さらにリンクコードを生成する方式は別の方式とし」との記述があるが、その理由は何か。直前の文に「『番号』を含めた「見える」利用番号から情報連携に用いる ID コードに直接アクセスできないようにするという観点から」とあるが、これが理由か。しかしそれは、続く文の「『番号』から論理的に ID コードに辿れないようなものとすべき」の理由にはなるものの、「別の方式とし」の理由にはならないのではないか。なぜ、「別の方式」としなければならないのか、その理由を説明いただきたい。あるいは「別の方式」が何を指すのかの理解に齟齬があるのであれば、「別の方式」が何を意味するのかを説明いただきたい。

【趣旨】
「住民票コードから『番号』を生成する方式と、住民票コードから ID コード、さらにリンクコードを生成する方式は別の方式とし」との記述は、根拠のない記述であり、削除すべきではないか。本当に書きたかったことは別にあるのであれば、それを書くべきではないか。

この記述は、続く「(3)『番号』の生成方法」において参照されており、「3.(2)とは異なる方法とすべき」とする根拠として「3.(1)で述べた観点から」と書かれている。そもそも 3.(1)のこの記述に根拠がないのであれば、全体として根拠のない決定をしていることになるから、ここを明確にすることは些末な論点ではないことを申し添える。

【質問先】
骨格案（その１）2 ページ
3.(2)ID コード及びリンクコードの生成方法

【質問】
リンクコードと ID コードの相互変換の方式として、「可逆暗号方式」と「コード変換テーブル方式」があるところ、コード変換テーブル方式を採用しないとしているが、その理由は何か。「コード変換テーブル方式は、同一の機関において住民票コード（注：この「住民票コード」との記述は「リンクコード」の誤記ではないか）と ID コードのリストの一元管理を行う必要があり、その場合、万一漏洩した際の影響範囲が広くなる可能性があることから」との記述があるが、それが理由か。可逆暗号方式であっても漏洩時のリスクは同等ではないのか。漏洩リスクが同等ならばコード変換テーブル方式を排除する理由がないところ、それ以外に何かの理由があって決めているのか。であれば、その理由を明らかにされたい。

【趣旨】
可逆暗号方式とコード変換テーブル方式とで、どちらが個人情報保護の観点で優れているかは、どちらでも同等ではないか。同等であるなら、骨子案の段階でどちらか一方に決めてしまうのは避けるべきではないか。骨子案は、個人情報保護のためと、住基ネット最高裁合憲判決に適合するために、必要十分な最小限の要件を決めるためのものであり、それら要件に影響しない観点から、具体的な実装方法に踏み込んで決定するのは、骨子案の趣旨から逸脱しているのではないか。

【想定される答え】
ご指摘の通り、根拠がないことが明らかになったので、ID コードとリンクコードの変換方式は、可逆暗号方式とコード変換テーブル方式の両方があり得ることの記述にとどめ、骨子案ではどちらかに決めないこととする。

【質問先】
骨格案（その１）3 ページ
3.(3)「番号」の生成方法

【質問】
住民票コードから「番号」を生成する方法として、コード変換テーブル方式を採用することが適切としているが、その理由は何か。「3.(2)とは異なる方法とすべき」というのが理由か。他に理由はないのか。

【趣旨】
そもそも、「3.(2)とは異なる方法とすべき」とする「3.(1)で述べた観点」に根拠がない。本当の理由は別にあるのではないか。住民票コードは 11 桁であり、「番号」もおそらく 11 桁前後のものであろうところ、可逆暗号方式によってそれらの変換をすることは、桁数が短いために、当該暗号を破られる等の技術的セキュリティ上のリスクが無視できないなど、本当の理由は別のところにあるのではないか。

【想定される答え】
ご指摘の通り、本当の理由は別のところにあった。理由の記述が誤っていたので修正する。

【質問先】
骨格案（その１）3 ページ
3.(4)「番号」と ID コード・リンクコードの管理のあり方

【質問】
「情報連携基盤においては、ID コードのみを保有することとし、リンクコードは情報連携ごとに可逆暗号で生成して、連携終了後直ちに消去することとすべき」とあるが、その理由は何か。直前に書かれている文の「情報の分散管理により、漏洩時の波及リスクを最小化する観点から」とあるのが理由か。ならば、漏洩時の波及リスクとして具体的に、何が誰に漏洩したときに誰が何をすることによりどんな波及があって、それがどんな脅威をもたらすと想定しているのか、具体的に示して頂きたい。漏洩リスクによる脅威を回避することが理由であるならば、可逆暗号方式ならばその脅威は解消されるのか。その理由は何か。

【趣旨】
漏洩リスクによる脅威の回避が理由であるなら、可逆暗号方式であってもそれは回避できないのであり、「可逆暗号で生成して、連携終了後直ちに消去することとすべき」には、根拠がないのではないか。

【想定される答え】
ご指摘の通り、根拠がないことが明らかになったので、ID コードとリンクコードの変換方式は、可逆暗号方式とコード変換テーブル方式の両方があり得ることの記述にとどめ、骨子案ではどちらかに決めないこととする。

【質問先】
骨格案(その 1)　4 ページ
(7)分野別に考慮すべき事項とリンクコードの付与単位について

【質問】
「分野」の定義が曖昧ではないか。分野の定義が曖昧なため、何が「分野を越えた情報連携」なのか分からない。
また、自治体等では、「分野を越えた個人情報」を管理している。この時、付与されるリンクコードがひとつだとすると、他の情報保有機関との連携を行う業務は、強制的に同一のリンクコードの付与することになる。これは、セキュリティリスクを増やすことにならないのか？

【質問先】
骨格案(その 1)　4 ページ
(1)番号連携の前提としての紐付けの必要性

【質問】
「セキュリティの観点から論理的関連性を持たないものとなる」という記述があるが、この「セキュリティの観点」の意味が分からない。複雑な紐付けの考え方は、「番号」「ID コード」「リンクコード」の整合性の確立と保持を難しくしている。また、「番号」と「リンクコード」の整合性をチェックする手段が提供されていない。
これは、セキュリティの一般的な要件である「完全性」に課題があることになる。また、「可用性」の面でも課題が多い。「機密性」「完全性」「可用性」がバランスよく実装されて初めてセキュリティを考慮した設計と言える。
現在のやり方は、情報保有機関毎に紐付けを行うことになるが、コスト等の制約から間違った紐付けが行われる場合もあると考えられる。これは、個人情報の漏洩に繋がる。

【趣旨】
住基ネットが利用できる場合、出来ない場合の情報保有機関毎に紐付けコスト等が検討されていない。コストには制約があり、その制約から紐付けのエラーが起きる。

【質問先】
骨格案（その１）4 ページ
4. (1) 番号連携の前提としての紐付けの必要性

【質問】
「リンクコードと『番号』及びその他の利用番号は、セキュリティの観点から論理的関連性を持たないものとなる」との記述があるが、「論理的関連性」とはいかなる意味か。可逆暗号方式による変換は「論理的関連性」があるが、コード変換テーブル方式による変換は「論理的関連性」がないという意味か。また、「セキュリティの観点から」とは、どのようなセキュリティの脅威のことを想定した記述なのか、具体的に回答いただきたい。

【趣旨】
ここで言うべきことは、セキュリティに関係なく、単に次のことではないのか。

「リンクコードは情報連携基盤によって無作為に生成されたものとなることから、情報保有機関は、リンクコードからそれに対応する当該機関が保有する『番号』等を得るためには、事前に何らかの準備が必要である。この準備は、……」

【想定される答え】
ご指摘の通りなので、趣旨に従って修正する。

【質問先】
骨格案（その１）7ページ
5.(4)情報連携の手順

【質問】
「照会先情報保有機関においては、当該リンクコードに係る個人の情報連携対象個人情報を付して、情報連携基盤を通じて照会元情報保有機関に対して、回答すべきではないか」とあるが、照会先情報保有機関から照会元情報保有機関への個人情報の回答方式としては、情報連携基盤を通さずに直接回答する方式もあり得るところ、それを採用しない理由は何か。

【趣旨】
確かに、政府基本方針には、「番号制度構築に当たっては、各機関間の情報連携は情報連携基盤を通じて行わせることにより、情報連携基盤がデータのやり取りの承認やアクセス記録の保持を行い（略）個人情報保護に十分配慮した仕組みとする」とあるが、この「通じて」という記述は、個人情報のデータそのものを情報連携基盤を通じさせるとは書かれておらず、「データのやりとりの承認」を情報連携基盤を通じてしていれば、「情報連携基盤を通じて行わせることにより（略）個人情報保護に十分配慮した仕組み」としたことになるのではないか。したがって、情報連携基盤を通さずに直接回答する方式の採用を排除する理由がない。

【想定される答え】
ご指摘の通り、理由がないので、情報連携基盤を通さずに直接回答する方式も選択肢として残すよう修正する。

【質問先】
骨格案（その１）8 ページ
6.(3)アクセスログの保存期間

【質問】
アクセスログ（政府基本方針における「アクセス記録」のことを指す）の保存期間の検討について、「不正アクセスや情報漏洩によって犯罪を構成する可能性に鑑み」とあり、電子計算機使用詐欺罪の公訴時効が 7 年であることとの関係を検討すべきとされているが、保存期間の根拠として「不正アクセスや情報漏洩によって犯罪を構成する可能性」を関連付ける理由は何か。他に検討すべき根拠があるのではないか。

【趣旨】
アクセス記録の保管が必要なのは、国民が自己情報のアクセス記録を確認できるようにするためであり、その趣旨は、システムに対する不正アクセス等の懸念からというよりも、国民が情報保有機関が自己の情報を不適切に扱っていないかを確認できるようにすることが主要な趣旨であるはずではないか。それならば、行政機関情報公開法や行政機関個人情報保護法等を根拠として検討すべきものではないのか。

【想定される答え】
ご指摘の通りなので、趣旨に従って修正する。

【質問先】
骨格案（その１）9 ページ
7.(2)既存システムと情報連携基盤をつなぐインターフェイスの確保

【質問】
情報保有機関の既存システムを情報連携基盤に接続するために、直接既存のシステムを改修するのではなく、既存のシステムの差異を吸収するインターフェイス（アダプタ等）を確保するとのことであるが、その実現方法として参考するものを、「住基ネットにおいて用いられるコミュニケーション・サーバー方式」に限定している理由は何か。

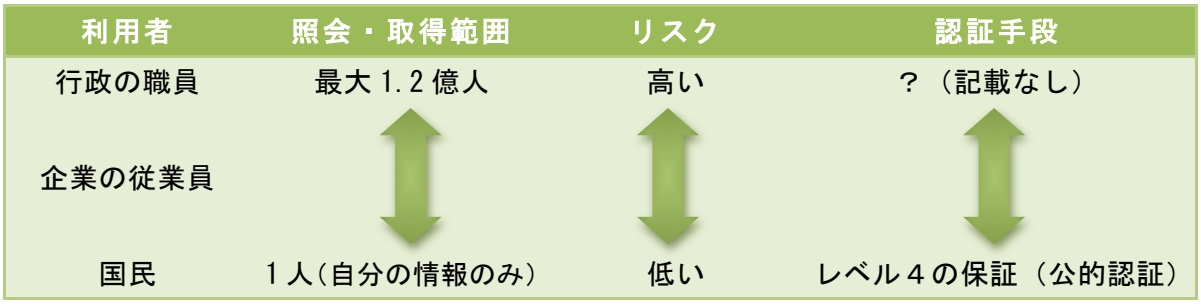
【趣旨】
システムインターフェイスの差異を吸収するアダプタの設計に際しては、住基ネットのコミュニケーション・サーバ方式に限定せずに幅広く検討するべきではないか。住基ネットでは基本四情報を扱うものであったのに対し、情報連携基盤では基本四情報よりもセンシティブな個人情報を扱うこととなるのであるし、住基ネットでは地方公共団体等しか接続しないものであったのに対し、情報連携基盤では将来的に民間事業者の接続を想定しているのであるだから、セキュリティの面で、住基ネットのコミュニケーション・サーバ方式よりも優れた技術方式があるならばそれを採用する可能性があることを排除せずに検討すべきではないか。

【想定される答え】
住基ネットのコミュニケーション・サーバ方式に限定する理由はない。「住基ネットにおいて用いられるコミュニケーション・サーバー方式等」としており、必ずしも他の方式を排除する記述ではないが、ご指摘を踏まえて、幅広く検討するものとする。

【質問先】
全体。特に骨子案（その２）１ページ「１．基本的な考え方」

【質問】
一般利用者に対する認証方式を具体的に示している一方で、行政職員に対する認証手段や本人確認方法を、規定していないのはどうしてか？リスクベースのアプローチの観点に立てば、より強い権限を持つ職員の ID 管理基準を規定したほうが望ましいのではないか？

【趣旨】
- 「（１）高いセキュリティレベルに対応できる認証方法の必要性」において、広い分野でセンシティブな個人情報を扱うため、また、住基ネット最高裁判決に対応し、一元管理を回避するため、利用者（国民）の本人認証として公的認証（公的個人認証と住基カード）を活用するとある。
- 上記の要件を満たすのが目的であれば、利用者個人ではなく、より強い権限をもつ、行政職員に対する本人確認や認証手段も規定したほうがよい。しかし、骨格案ではそれに関する記載がない。



- 上図にある通り、行政職員（特に情報連携基盤の職員）は全国民の個人情報の取得可能性があるにもかかわらず、認証手段が記述されていない。一方、国民は自身の情報にアクセスするだけに過ぎないにも関わらず、認証手段（トークン）については、保証レベル４相当の過度なものを求められる。（「保証レベル」の考え方については、内閣官房「オンライン手続きにおけるリスク評価及び電子署名認証ガイドライン」を参照。）

【想定される答え】
国民だけでなく行政職員の ID 管理（認証手段や本人確認）についても明記すべきである。リスクベースのアプローチを採用し、サービスや業務のリスク評価に基づいて求められる保証レベルを定義し、その保証レベルに応じて、適切な本人確認・認証手段の採用を行う。行政職員の ID 管理手法を明確にする。なお、一般利用者（国民）については、自身の情報を参照するサービスに留まるので、必ずしも公的個人認証のような強固な認証手段のみを求める必要はない。

情報連携基盤

（情報連携基盤技術 WG 事務局にお答えいただきたい）

【質問先】

全体

【質問】

情報連携基盤の一元管理の可能性をなくすために、情報連携基盤の機能を分解して検討すべきではないか？

【趣旨】

- システムの合憲性の担保のためには、情報連携基盤に求められる機能を分解し、機能が一極集中しないように配慮する必要がある。これは、システムの可用性、パフォーマンス、柔軟性、拡張性といった観点からも重要である。情報連携基盤には以下の機能が必要であると読み取れる。

  1. 振り分けサービス（どの情報保有機関に情報が存在するか示すサービス）
  2. 認可サービス（情報連保有機関にアクセストークンを発行するサービス）
  3. 「番号」の付番
  4. ID コード、リンクコードの付番
  5. リンクコード変換
  6. ログ収集

【想定される答え】

情報連携基盤の機能を分解して検討すべきである。1～5 の機能に分解した上で、1 つの機関ではなく、複数の機関に分散してそれらの機能を運用させることで、合憲性を確保し、情報連携基盤に権限が一極集中しない、柔軟な制度設計、システム設計をすべきである。

各機関等の識別

（情報連携基盤技術 WG 事務局にお答えいただきたい）

【質問先】

全体。特に骨子案（その１）ページ６「（３）情報連携の際の適切なアクセス制御」

【質問】

情報保有機関自体の識別・認証の方式を検討すべきではないか？また、情報保有機関に対して情報連携する資格を有しているかの認定制度を検討すべきではないか？

【趣旨】

情報連携に際し、情報保有機関の職員を限定し、端末やデータベースへのアクセスを制御するという方式が想定されているが、そもそも情報保有機関のサーバやサービスを識別し、認証する方法は考慮されていない。さらに、情報保有機関が、情報連携を行うための資格を有しているかを認定するための仕組みが検討されていない。

【想定される答え】

情報保有機関だけでなく情報連携に関わる全てのサーバやサービスを識別し、認証する方法を検討する必要がある。さらに、それらが、情報連携を行うためのセキュリティ基準、組織的信頼度、システム運用ポリシーなどを有しているか監査し、監査条件をクリアしていた場合に認定を行う組みやそのための第三者認定組織が必要である。

不明瞭な書きぶりの修正

（情報連携基盤技術 WG 事務局にお答えいただきたい）

【質問先】
骨格案（その 2）9 ページ
4.(7)署名検証者の拡大等

【質問】
「署名用シリアル番号や認証用シリアル番号のセキュリティを確保した上で、検証者側のコスト負担を軽減するため、民間事業者が共同で検証を行う仕組みも検討してはどうか」とあるが、「署名用シリアル番号や認証用シリアル番号のセキュリティ」とはいかなる意味か。明確にされたい。

【趣旨】
どのような意味でのセキュリティの要件を満たす必要があるのかを明らかにしない限り、認証用証明書の利用を民間事業者にまで拡大することを許してよいのか、個人情報保護の観点から判断できない。

【想定される答え】
不明

【質問先】
骨格案（その１）5 ページ
4.(2)4 情報の突合の必要性

【質問】
「リンクコードが情報保有機関の個人情報データベースに紐付けられるためには」として、基本 4 情報による突合が必要で、そのために住基ネットを活用するとあるが、これは、情報保有機関が情報連携基盤の利用に参加するに際して、最初に 1 回だけ行うものなのか、それとも、常時それをするという意味なのか。

【趣旨】
最初に 1 回だけ行う趣旨で書かれているように推察するところ、この書きぶりでは、常時それをするという意味に読まれてしまうのではないか。最初に 1 回だけ行う作業について述べていることを明確にするべきではないか。

あるいは、出生児についてこの処理が必要という意味で「常時それをする」という意味なのかもしれないが、出生児の処理の実現方法については、別途検討する必要があるのではないか。

また、これらの点は、「4.(3)リンクコードと『番号』等との対照テーブル」についても同様であり、4.(3)の記述はほぼ 4.(2)と同じことを述べているので、4.(2)に統合して書いた方がよいのではないかという点も申し添える。

【想定される答え】
ご指摘の通りなので、趣旨に従って修正する。

「番号」の用途

（情報連携基盤技術 WG 事務局にお答えいただきたい）

【質問先】
骨格案（その 2）10 ページ
5.(3)券面記載事項

【質問】
「『番号』の持ち主であることを証明するため、IC カード券面に『番号』を記載することとし、偽変造防止のための技術的な工夫を施すべきではないか」とあるが、『番号』は「見える番号」であることから、番号だけで「持ち主であることを証明する」ことにはならないのであり、そのような用途に使用してはならないとするべきものではないか。『番号』を券面に記載することの真の目的は、紙による手続きにおいて、本人が『番号』を書類に記載する際の備忘録として使うためではないのか。そうであれば、券面上の番号はメモにすぎないのであるから、番号の記載部分についての偽変造防止は不要ではないか。

【趣旨】
質問の通り。

【想定される答え】
不明

技術的に不可能な記述

（情報連携基盤技術 WG 事務局にお答えいただきたい）

【質問先】
骨格案（その 2）10 ページ
5.(4)IC チップ記録事項

【質問】
「IC チップ内の『番号』は、法令等で『番号』を確認することが認められている機関が『番号』を確認する場合に限り、システム上加工可能なデータとして取り出せることを検討してはどうか」とあるが、その一方で、「IC チップ内の『番号』を確認するソフトウェアについては、IC カードを利用して本人確認をする必要がある者に対して交付する」とある。当該ソフトウェアが民間事業者に提供される前提である以上、それ（法令等で認められている機関だけがデータとして取り出せる）を実現することは、技術的に容易でないのではないか。

【趣旨】
IC チップ内のデータを、権限のある者にだけ閲覧可能するというセキュリティ要件を設定してしまうと、これには様々なセキュリティ上の攻撃手法があり得るため、実現が困難になるのではないか。セキュリティ上危ういことを実現しようとすると、それが破られて、制度自体への批判の根拠とされかねないという問題があるのではないか。券面に記載されている事項は、電子的な方法でも同様に誰でも閲覧可能なものとし、なりすましの防止だけを要件とすべきではないか。

【想定される答え】
不明

用語の誤りの指摘

（情報連携基盤技術 WG 事務局にお答えいただきたい）

【質問先】
骨格案（その１）7 ページ
6.アクセスログの保存及び提供

【質問】
「アクセスログ」という記述があるが、これは「アクセス記録」の誤記ではないか。

【趣旨】
1 ページの政府基本方針からの引用にあるように、政府基本方針では「アクセス記録」という用語が用いられている。「アクセスログ」とすると、一般的な意味でのサーバ等へのアクセスログのことと誤解されるので、このような用語のばらつきは無視できない問題を生じさせるのではないか。

個人情報保護 WG の第 4 回では、骨格案（その 2）の 2.(4)にある「保存されているアクセスログの情報は削除する」との記述に対して、同 WG 小向委員から、「不正アクセス対策のためにアクセスログは重要なのにすぐに削除するというのはいかがなものか」との趣旨の質問が出されたが、これは、「アクセス記録」と一般的な意味でのアクセスログとの混同が生じたために出された無用な質問だったのではないか。

【想定される答え】
ご指摘の通りなので修正する。

名寄せ・突合

（情報連携基盤技術 WG 事務局にお答えいただきたい、場合によって情報保有機関、銀行などの金融機関などからヒヤリングすべきではないか）

【質問先】

- 骨子案（その１）５ページ「（２）４情報の突合の必要性」
- 同６ページ「（４）情報連携の手順」

【質問】

４情報だけに依存した突合に限定せずに、業務の要件の応じた多様な名寄せ・突合の方法を検討すべきではないか？特に民間企業が本人から４情報を取得するという方法は現実的であるか？

【趣旨】

- 現行案では、情報保有機関が保有する４情報を最新にするために住基ネットを補助システムとして利用することを想定している。
- 突合に関してエラーが発生した場合、最終的にそれを正確な状態にするには、本人の介在が必要である。
- ２情報や３情報しか持っていない情報保有機関の対処方法が不明確である。
- 民間企業の側で、「情報連携について本人の同意を得て本人から入手した４情報を用いて」とあるが、本末転倒である。金融機関などは今回の番号制度のメリットとして、行政側から顧客の住所などの個人情報を取得することを挙げている。

【想定される答え】

現状の日本年金機構などが実施している突合のノウハウなどを参考に、業務の要件の応じた多様な名寄せ・突合の方法を検討すべきである。４情報だけに依存した突合に限定すべきではなく、突合のフローに利用者本人が確認行う手順を組み込むべきである。また、情報の取得に際し、極力民間企業の負担を掛けないようにすべきである。

付番

（情報連携基盤技術 WG 事務局にお答えいただきたい、場合によって情報保有機関などからヒヤリングすべきではないか）

【質問先】

骨子案（その１） １ページ「２．情報連携の原則」の（２）
同２ページ「３.付番と番号管理について」

【質問】

住民票コードを基にした付番では、本制度の対象者となる国民全てをカバー出来ていないため、別の付番方法も検討すべきではないか？

【趣旨】

- 現行案では、「住民票コードに対応した新しいコード」としており、「番号」も ID コードもリンクコードも全て住民票コードを基に付番をする事になっている。
- しかし、下図のように業務によってカバーしなければならない対象は変わる。住民票コードは、ほとんどの利用者をカバーしているが、制度に必要な全てをカバーしているわけではない。

	日本人		外国人		
	日本在	在外	日本在	かつて在日	それ以外
生者			外国人登録制度 （24 年から住基へ）		
死者	・戸籍の除票記録 ・年金記録				

■ 住民票コードでカバーしている領域
--- 年金業務で本来カバーしなければならない領域
--- 納税業務で本来カバーしなければならない領域

【想定される答え】

住民票コードだけに基づく付番では、制度に関わる利用者全てをカバーしているわけではない。対象者の最大値をカバーしている年金業務などを参考に、付番方法を見直すべきである。

IC カード

（情報連携基盤技術 WG 事務局にお答えいただきたい、場合によって地方自治体、内閣官房情報セキュリティセンター（NISC）などからヒヤリングすべきではないか）

【質問概要】

IC カードや電子証明書の配布対象は、マイポータルで自己情報へのアクセス記録確認を行いたい利用者だけになるのか？

【質問先】

骨子案（その２）５ページ「（５）IC カード（住民基本台帳カードの改良）」）

【質問】

IC カードや電子証明書の配布対象は、マイポータルで自己情報へのアクセス記録確認を行いたい利用者だけになるのか？

【趣旨】

- 「自己情報へのアクセス記録を確認する者等に対しては、ＩＣカード及び電子証明書を発行し、交付すべきではないか」とある。
- 市町村窓口での発行、タイプ B（顔写真あり）を採用と書かれているが、そのような方法で、制度開始までに全国民に番号を配布することは困難であると考える。
- 『社会保障・税に関わる番号制度についての基本方針』にも全国民に IC カードを配布することは明記されていない。

【想定される答え】

1. 希望した者のみに IC カードや電子証明書を配布したほうが良い。よって、以下の観点で、IC カードを窓口で配布する方法以外の番号の配布方法もあわせて検討する。
   - 番号の配布方法（例：窓口もしくは郵送）
   - 番号の配布媒体(例:IC カードもしくは紙もしくはプラスチックカード)
   - 認証手段・クレデンシャル（例：電子証明書もしくはパスワード）
   - クレデンシャルの提供者（例：公的認証機関もしくは民間認証機関）
   - 本人確認方法（本人と番号やクレデンシャルの結びつけ方法）

民間における情報連携と住基ネットの４情報の関係について

（情報連携基盤 WG 事務局にお答えいただきたい）

【質問先】

骨格案(その 1)　6 ページ

5.情報連携について

(4)情報連携の手順

【質問】

「情報連携の手順」の説明では、「民間の機関の側で情報 連携について本人の同意を得て本人から入手した 4 情報を用いて、情報連 携基盤を通じて照会し、住基ネット側の 4 情報と合致した場合のみにリンクコードを付番するといった仕組みを検討すべきではないか」とある。

これは、そもそも何のための番号制度なのかということを無視しているのではないか？また、基本方針にある「国民にとって利便性の高い社会」に反するのではないか？

「本人の同意を得て本人から入手した番号を用いて、情報連 携基盤を通じて照会しリン クコードを付番する」べきであり、そうしたシステムを提案するべきなのではないか。

【趣旨】

情報保有機関が保持すべき「対照テーブル」の作成の負荷や手間が大きすぎることは、結果的に、「国民にとって利便性の高い社会」にならない。

本人確認

（情報連携基盤 WG において御議論いただきたい）

【質問先】
骨格案（その２）

【質問】
マイポータル以外での、オンラインでの本人確認と番号の関係について検討されるべきではないか。利用者から「番号」を証明して欲しい多くの組織は、情報連携基盤に直接接続されない組織になる。現在の案では「番号が記載されたカード」を対面で示すしかない。オンラインでの証明は、コピー等も考えられるかもしれないが、これは改ざんのリスクが高い。利用者の利便性や、「番号」を証明して欲しい多くの組織の立場からは、オンラインでも「番号」が証明される手段があるべきであるが、その方法がないし、また、実現を不可能にするかもしれないシステムが提案されている。
こうしたことは、コピー等のセキュリティレベルの低い方法を推奨しかねないし、また、番号が法的に利用できる分野においても番号の利用を阻害する。

【趣旨】
番号に関するユースケースが十分に検討されていないため、現実的なシステムが提案されていないように見える。
韓国の「公認認証局」が発行する「公認証明書」では、番号（住民登録番号）は直接的に記載されないが、番号を証明できる仕組みが取られている。

情報連携基盤に関する個人情報保護に関する質問（第一版）

2011 年 4 月 11 日
情報連携基盤技術に関する私的勉強会
世話人 山口英

個人情報保護への配慮及び住基ネット最高裁判断枠組みへの適合性
（個人情報保護 WG で御議論いただきたい）

【質問先】
骨格案（その１）2 ページ
3.(2)ID コード及びリンクコードの生成方法

【質問】
1. ID コードとリンクコードの生成方法として、コード変換テーブルによる管理を行わず可逆暗号を用いることとした点について

情報連携基盤では、異なる情報保有機関同士の情報連携を図るために、ID コードからリンクコード、またリンクコードから ID コードに遡る処理が必要不可欠であるところ、個人情報保護に十分配慮した仕組みとするため、及び最高裁判断枠組みへ適合するための要件（以下、保護適合要件という。）を満たすために、コード変換テーブル方式（乱数を用いてコードを変換し、変換前後のテーブルを保持する）の採用を避け、可逆暗号方式（その都度可逆暗号によってリンクコードから ID コード、又は ID コードからリンクコードを生成する）の採用を検討しているところであるが、この判断は必要かつ十分なものか。

質問１の１
可逆暗号により生成する方式は、保護適合要件を満たすために十分なものと言えるか。
質問１の２
コード変換テーブルによる管理方式を避けることは、保護適合要件を満たすために必要なものか。

【趣旨】
情報連携基盤技術 WG では、情報連携基盤技術の骨格案検討にあたり、個人情報保護に十分配慮した仕組みとするため、並びに、住民基本台帳ネットワークシ

ステム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、及び、何人も個人に関する情報をみだりに第三者に開示又は公表されない自由を有することなどの判断枠組み（以下、最高裁判断枠組みという。）に適合した形で個人情報を取り扱うシステムとするため、いくつかの技術要件を検討しているところであるが、検討しているそれぞれの技術要件が、個人情報保護への十分な配慮及び最高裁判断枠組みへの適合性として、十分な要件であるか、また、必要な要件であるか、個人情報保護WGの見解を求めたい。

【想定される答え】
質問1の1への回答：十分である。ただし、当該可逆暗号の鍵の機密性が保たれなければならない。
理由：最高裁判断枠組みに適合するには、情報保有機関が他の情報保有機関と個人情報を無秩序に突合できないようにする必要があり、そのために、各情報保有機関ごとに異なる「リンクコード」を用いて各リンクコード間の突合を情報連携基盤のみが可能とする方式には合理性がある。この突合を情報連携基盤のみが可能とするにあたり、鍵の機密性が保たれた可逆暗号を用いることは、十分である。

質問1の2への回答：必ずしも要しない。
理由：リンクコードの突合を情報連携基盤のみが可能とするにあたり、コード変換テーブルによる管理方式を用いることもできる。このときコード変換テーブルのデータの機密性が保たれなければならないが、可逆暗号の鍵も同様に機密性が要求されるのであるから、可逆暗号方式とコード変換テーブル方式のどちらを用いても同じであり、コード変換テーブル方式を避けることは必要でない。

【質問先】
骨格案（その１）3 ページ
3.(4)「番号」と ID コード・リンクコードの管理のあり方

【質問】
2.　リンクコードの管理のあり方として、情報連携基盤においてはリンクコードは生成後直ちに消去することとした点について

情報連携基盤においては、ID コードからリンクコードを生成する処理が必要不可欠であるところ、保護適合要件を満たすため、生成されたリンクコードを連携終了後に直ちに消去する方式を検討しているところであるが、この判断は必要かつ十分なものか。

質問 2 の 1
生成されたリンクコードを連携終了後に直ちに消去する方式は、保護適合要件を満たすために十分なものと言えるか。
質問 2 の 2
生成されたリンクコードを連携終了後に直ちに消去することは、保護適合要件を満たすために必要なものか。

【趣旨】
1.の質問に同じ。

【想定される答え】
質問 2 の 1 への回答：十分である。
理由：とくになし。

質問 2 の 2 への回答：必ずしも要しない。
理由：可逆暗号で生成されたリンクコードを直ちに消去したとしても、当該可逆暗号が利用可能であればいつでも同じリンクコードを生成することができる。当該可逆暗号が情報連携基盤以外で利用不可能とする必要があるが、それには当該可逆暗号の鍵の機密性が保障されなければならない。鍵の機密性が保たれるならば、同様に生成されたリンクコードの機密性も保たれるはずであり、また、リンクコードの機密性を保てないのであれば鍵の機密性も保たれないはずである。よって、リンクコードを直ちに消去することは必要でない。

【質問先】
骨格案（その１）7ページ
5.(4)情報連携の手順

【質問】
3. 情報連携の手順として、情報連携基盤において個人情報そのものは保存しないようにするとした点について

情報連携の手順は、まず、照会元の情報保有機関が、情報連携を行う対象者のリンクコードを用いて情報連携基盤に問い合わせ、次に、情報連携基盤が、当該照会に係る情報連携の内容が法令によって許可されているものか確認した後に、照会先情報保有機関のリンクコードを生成して、当該照会先情報保有機関に当該リンクコードを伝達し、最後に、照会先情報保有機関が対象個人情報を情報連携基盤を通じて照会元情報保有機関に対して回答するというものであるが、このとき、保護適合要件を満たすために、情報連携対象の個人情報は、情報連携基盤を通じて回答がされることにとどめ、情報連携基盤においては保存されないようにすることを検討しているところであるが、この判断は必要かつ十分なものか。

質問3の1
個人情報を情報連携基盤を通じて回答する際に情報連携基盤に保存されないようにすることは、保護適合要件を満たすために十分なものと言えるか。
質問3の2
個人情報を情報連携基盤を通じて回答する際に情報連携基盤に保存されないようにすることは、保護適合要件を満たすために必要なものか。

【趣旨】
1.の質問に同じ。

【想定される答え】
質問3の1への回答：十分でない。
理由：最高裁判断枠組みに適合するためには、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が必要である。情報連携の際に、情報連携対象の個人情報が情報連携基盤を通じて回答されるのであれば、情報連携基盤の運営機関は、当該個人情報を記録することが可能となるのであり、その個人情報はIDコードと紐付けて記録することも可能である。したがって、情

報連携基盤が個人情報を保存しないようにするというだけでは保護適合要件を満たすのに十分でなく、照会先情報保有機関は、情報連携対象の個人情報を情報連携基盤を通じることなく照会元情報保有機関に回答するようにするなど、何らかの技術的解決策が必要である。

質問3の2への回答：必要である。
理由：情報連携基盤において情報連携時の個人情報が保存されることとなれば、情報連携基盤が個人情報を一元的に管理することができる機関となることから、最高裁判断枠組みに適合するためには、情報連携基盤において情報連携時の個人情報が保存されないようにすることは必要である。

【質問先】
骨格案（その 2）3 ページ
2.(3)マイ・ポータルにログインするための認証

【質問】
4. マイ・ポータルのログイン認証方式として、認証用シリアル番号は認証局においてのみリンクコードと紐付けが行われるようにした点について

マイ・ポータルにログインするための認証方式として、認証用の電子証明書のシリアル番号をログインするためのキーとして使用することを検討しているところ、認証用シリアル番号が民間事業者を含め、各情報保有機関において蓄積されると、認証用シリアル番号を利用してデータマッチングされる危険性が高まることから、保護適合要件を満たすため、認証用シリアル番号は認証局（公的個人認証サービスの電子証明書を発行する機関をいう。以下同じ。）においてのみリンクコードと紐付けが行われることとし、マイ・ポータル運営機関の利用者フォルダと認証用シリアル番号との紐付けは行わず、マイ・ポータル運営機関は、利用者がログインする際、認証用シリアル番号を情報連携基盤に送付して、認証用シリアル番号を蓄積しないよう速やかに削除することを検討しているところであるが、この判断は必要かつ十分なものか。

質問 4 の 1
認証用シリアル番号を蓄積しないよう速やかに削除することは、保護適合要件を満たすために十分なものと言えるか。
質問 4 の 2
認証用シリアル番号を蓄積しないよう速やかに削除することは、保護適合要件を満たすために必要なものか。

【趣旨】
1.の質問に同じ。

【想定される答え】
質問 4 の 1 への回答：認証用の電子証明書をマイ・ポータル以外でも用いることを予定しているのであれば、十分でない。
理由：認証用の電子証明書をマイ・ポータル以外でも用いることを予定しているのであれば、認証用シリアル番号がマイ・ポータル以外にも送付されることになる。認証用シリアル番号が民間事業者にも送付されることとなれば、認証

用シリアル番号を利用したデータマッチングの危険性が高まる。このデータマッチングの危険性は、マイ・ポータルにおいて認証用シリアル番号を蓄積しないよう速やかに削除したところで、払拭されるものではない。

質問４の２への回答：認証用の電子証明書をマイ・ポータル以外では用いないものとするのであれば、必要でない。
理由：質問４の１への回答の通り、認証用電子証明書はマイ・ポータル専用としなければ保護適合要件を満たさない。認証用電子証明書がマイ・ポータル専用のものであるなら、認証用シリアル番号はマイ・ポータルにしか送付されないものとなることから、認証用シリアル番号を用いたデータマッチングの危険はないこととなり、マイ・ポータルにおいて認証用シリアル番号を蓄積しないようにすることは、必要でない。

【質問先】
基本方針 5 ページ

【質問】
5.　情報連携基盤を総務省が担うとされている点について

政府・与党社会保障改革検討本部の社会保障・税に関わる番号制度についての基本方針（平成 23 年 1 月 31 日）では、「個人に対する付番及び情報連携基盤を担う機関の所管は、総務省とする。」とされているが、情報連携基盤を総務省が担うことは、保護適合要件を満たすために十分なものと言えるか。

【想定される答え】
回答：総務省が情報保有機関のひとつとして情報連携基盤に接続する場合には、十分でない。
理由：総務省が情報保有機関として情報連携基盤に接続する場合には、総務省が情報保有機関と情報連携基盤の双方を兼務することとなる。この場合、総務省は、他の情報保有機関のリンクコードを生成することが可能で、それを総務省が保有する個人情報と突合することが可能となる。これは、総務省が個人情報を一元的に管理することができる機関となることから、最高裁判断枠組みに適合するために、十分でない。保護適合要件を満たすには、情報保有機関として情報連携基盤に接続することを予定していないいずれかの機関が情報連携基盤の運営機関を担うことが必要である。

【質問先】
骨格案(その 1)　2page
「2.情報連携の原則」

【質問】
「３．付番と番号制度について」において番号、ID コードの分散管理が記述されており、その理由を最高裁判決の整合性にあるように記述されている。これの関係が分からない。
最高裁判決では、「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」ことを要求していうのであって、番号、ID コードの分散管理を明確に要求しているのではない。現在の「日本年金機構」のように住民票コードを取り込んでいる例でもある「日本年金機構」は違憲という見解なのか？

【趣旨】
最高裁判決の整合性に関しては、個人情報保護 WG を中心に議論されるべき。

「リンクコード」「ID コード」の個人情報としての扱いについて

（個人情報保護 WG で御議論いただきたい）

【質問先】

骨格案(その 1)　3page

(5)「番号」と ID コード・リンクコードの個人への通知の必要性

【質問】

「リンクコード」「ID コード」は、ID コード・リンクコードについては、個人に通知されるものではないものとされている。これは、利用者の開示要求によっても開示されないものとするのか？

【趣旨】

「リンクコード」「ID コード」が個人情報保護法における個人情報に当たるのか？明確になるべき。

国民の権利保護

（個人情報保護 WG で御議論いただきたい）

【質問先】

全体。特に、骨格案（その２）２ページ「自己情報へのアクセスログを確認する機能」「各情報保有機関が保有する自己情報を確認する機能」

【質問】

国民が、自身の情報をマイポータルで確認できるだけでは、「自己情報コントロール」という観点から不十分ではないか？情報連携に関して、本人が同意する仕組みも追加すべきではないか？

【趣旨】

- 『社会保障・税の番号制度についての基本方針』の「理念・実現すべき社会」において、「⑤ 国民の権利を守り、国民が自己情報をコントロールできる社会」とある。一方、『骨格案（その２）』では、自己情報のコントロールに関しては、マイポータルの一機能として「自己情報へのアクセスログを確認する機能」「各情報保有機関が保有する自己情報を確認する機能」という表現に留まっている。
- そもそも、「自己情報コントロール」やそれに関する権利、求められる機能が定義されていないということもあるが、「自己情報コントロール」には単なる自身の情報確認という意味だけでなく、本来は情報保有機関をまたがる情報連携に関して本人が介在する権利や機能という意味も含まれるはずである。

【想定される答え】

自己情報コントロール権の観点から、また、柔軟な情報連携の実現の観点から、本人同意の仕組みも追加すべきである。単なる個人情報の「開示請求権」だけでなく、情報保有機関から別の機関への自己情報の連携に対して、本人の同意を取り付けるオプトイン、オプトアウトの標準的な仕組みが必要であると考える。

情報連携

（個人情報保護 WG 事務局へお答えいただきたい。場合によっては保有機関などへもヒヤリングいただきたい。）

【質問先】

骨子案（その１）５ページ「５．情報連携について」

【質問】

情報連携の目的、連携先・連携元の情報保有機関、個人情報の種類、連携パターンについて、法令に予め全て記載し、それらが増える毎に法改正するというアプローチは、多種多様な情報連携を目的とした場合、使い勝手やそこへのガバナンスという観点で、現実的ではないのではないか？

【趣旨】

- ５．（１）は、住民基本台帳法が対象業務を法律に明記しているというアプローチをとっているため、それを踏襲していると思われる。
- しかし、今回は基本４情報だけではなく様々な属性情報を連携させることもある。
- ５．（２）において、「５．（１）により定められた情報連携基盤及び情報連携対象個人情報のリスト」の中に含まれていることを条件とし、情報連携基盤が「その都度承認を行う」とある。このホワイトリストと突合し、照会元、照会先、目的、個人情報の内容等がすべて一致して初めて、「照会元情報保有機関による情報連携の照会」が行われ、例外は認めないというアプローチである。これでは、使い勝手を損うと思われる。
- また、ガバナンス上、お手盛りにならないように、この「リスト」を誰が作成するかについても検討する必要がある。

【想定される答え】

今回の制度では、住民基本台帳法と異なり、多様な個人情報を連携する可能性があるから、法令で全てを規定しておくのは、現実的なアプローチとは言えない。柔軟な制度設計という観点に立てば、法令では一定の連携ポリシーや基準を規定するに留め、個別の連携範囲やパターンについて、第三者機関による許可によって、実施されるべきである。

マイポータル

（個人情報保護 WG で御議論いただきたい）

【質問先】

- 骨子案（その２）２ページ「（２）マイ・ポータルにおける情報管理のあり方」の下から２行目
- 同５ページ下から２行目
- 同６ページ下から４行目　　等

【質問】

マイポータルからのログアウト毎に利用者の情報を削除するというのは、利便性を損ねるのではないか？一元管理を避け合憲性を担保するためには、利用規約などで本人同意を取り付ければ、十分なのではないか？

【趣旨】

- 『骨格案（その２）』において、随所に「利用者の個人情報が利用者フォルダに極力蓄積しないように、ログアウトの度に利用者の個人情報のうち必要のないものについては消去する仕組みとしてはどうか」や、「利用者がマイ・ポータルからログアウトすると同時に、利用者フォルダに一時的に保存されている情報保有機関の情報を削除する」という表現が見られる。
- 住基ネット最高裁判決に配慮した対応と推測できる。
- 情報連携基盤から都度取得し、ポータルで都度削除する方式は、利用者の利便性を損なう可能性がある。

【想定される答え】

都度本人の情報を削除する必要はない。利用規約などで、本人同意を取り付ければ、利用者の権利保護という観点においても、十分なのではないかと考える。そのためにも本人同意のための枠組みが必要である。

情報連携の原則

（個人情報保護 WG で御議論いただきたい）

【質問先】

骨格案(その 1)　P1

２．情報連携の原則

【質問】

「情報連携の原則」は、「情報連携基盤」以外での情報連携も含め、個人情報保護 WG にて議論されるべきではないか？

「情報連携の原則」は、

(1)　「情報連携基盤」による情報連携

(2)　番号を利用した「情報連携基盤」によらない情報連携

(3)　従来の「基本４情報」等を利用した「情報連携基盤」によらない情報連携

こうした範囲で検討されるべき。

【趣旨】

現状は「情報連携基盤」の適用範囲が曖昧。「情報連携基盤」での情報連携の敷居が高いほどの、情報連携がなされないか、または、迂回された情報連携を助長することになる。そのため利用されない「基盤」になる可能性が高い。

【質問先】
骨格案(その 1)　1 Page
(2)「見えない」ID コードを用いる情報連携

【質問】
骨格案(その 1)の「2.情報連携の原則」は、個人情報保護 WG の見解も同じなのか？
国民が認知していない見えない番号による個人情報連携を行うことの是非の議論もあるのではないか。いずれにせよ.情報連携の原則は、個人情報保護 WG で先に議論されるべき論点なのではないか？

【趣旨】
情報連携の原則について、個人情報保護 WG で議論されるべき。

IDコード等が漏洩した際の影響の記述について

（個人情報保護WG事務局にお答えいただきたい）

【質問先】

骨格案(その1)　2page

「2.情報連携の原則」

【質問】

骨格案(その1)の「2.情報連携の原則」において「IDコードは情報連携基盤において管理されることとなるが、仮にこれを情報保有機関も共有し、それで情報連携基盤にアクセスさせることとすると、 万一漏洩した際にはその影響が他の情報保有機関にも波及する可能性がある」という記述がある。一方、全ての情報保有機関は、最新の基本４情報を保持することも要求している。漏洩することの影響として、IDコードと基本４情報とで何が違うのか？

【趣旨】

「情報漏洩のリスクの低減」と「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」の要求は別物であることを明確にすべき。

「番号」の個人 からの変更請求について

（個人情報保護 WG で御議論いただきたい）

【質問先】

骨格案(その 1)　3page

(6)「番号」と ID コード・リンクコードの変更可能性

【質問】

番号の変更を許した場合の、「情報保有機関」における「番号」の扱いについての考察がたりないのではないか？

【趣旨】

番号の変更に対して、戸籍等の「ネームロンダリング」のような問題に対処するための手段も同時に検討される必要があるが、その考察がない。