資料2

今後の論点についての参考意見

平成 23 年 7 月 28 日

情報連携基盤技術ＷＧ構成員　坂本泰久

１．アクセス記録について

今後の論点のうち（８）第三者機関の監査範囲について、ログを集約して管理することは、個人情報そのものに加えて、その更新履歴やアクセス履歴も含めた個人情報のライフサイクルを包括して管理することになり、最も大きなプライバシ保護上のリスクとなる。したがって、情報連携基盤のログと情報保有機関のログは各々で分散して管理し、必要に応じて第三者機関の法的権限にもとづき各機関から収集する方法が、目的外のデータマッチングのリスクを低減する設計方針と整合しており、妥当と考える。その際、第三者機関への情報保有機関システムへのアクセス特権の付与については、セキュリティホールになりうることや監査対象が入退室情報など情報連携のログを超えて多岐にわたること等から慎重に取り扱う必要がある。一方で、監査を効率化するために各情報保有機関におけるログのデータフォーマットを共通的にしておくことは有用である。

論点のうち（５）アクセス記録の保管場所については、アクセス記録の範囲が情報連携基盤で管理しているログを指し、情報保有機関で管理するログは含まない、という理解のもとで、後述のマイポータルの論点（４）と同様の理由で、情報連携基盤に保管し、必要に応じてマイポータルに提供する方法が適当と考える。

２．マイポータルについて

今後の論点のうち（４）マイポータルにおける個人の情報の保持に関して、①事前の蓄積と②ログイン後の取得の選択については性能要件に依存するため、マイポータルの主要な利用ケースを想定した実証実験を行い確認することが望ましい。①では大規模の未読情報が蓄積され続けることに関するデータ容量および安全性の評価が、②では符号変換を含めた応答時間の評価が必要である。見解としては、マイポータルを利用しない人にとってのデータ集積のリスクを抑えるため、応答時間が許容範囲以内であれば、②の方法で要求に応じて取得するのが安全かつ経済的と考える。

論点のうち（７）代理人によるマイポータルの利用での①代理人フォルダで表示と②本人フォルダでの閲覧の選択について、一般的に、代理人の扱いは業務分野毎の相違が大きく、汎用的な方式に統一することが難しいため、各保有機関の個別の対応を前提に、情報連携基盤への影響を少なくする方向が望ましい。見解としては、①のほうがセキュリティポリシー管理の実装が容易であり、情報の制御が確実にできると考える。

マイポータルは、固有の個人情報や「番号」を保有せず、多人数でなく個人ごとのデータ処理が中心になることから、他の情報保有機関と全く同等の規制対象とはならないと思われるが、複数の情報保有機関からの個人情報が一時的に集約するため、他の情報保有機関と同レベルのシステム上

のセキュリティ対策が必要である。また、マイポータルは国民自らが確認することになるため、新規情報の有無、既読未読の区別といった情報の状態通知について標準的な仕組みを規定し、情報保有機関側の必要性に応じて選択的に実施できることが望ましい。

３．データ送受信方式について（第６回ＷＧ資料３－２の補足）

異なる符号の利用を前提とした、案１（ゲートウェイ方式）と案２（アクセストークン方式）の実現方式の一例と目的外の名寄せリスクに関する比較を表１に示す。

案１、案２ともに異なる符号は情報保有機関間では共有されないが、案１では情報連携基盤を経由して個人情報を送受するのに対し、案２では情報連携毎に都度発行するトークンを共有して情報保有機関間で個人情報を直接送受信する。

いずれの案においても、単独者の不正の脅威に関するリスクは小さいと考えられる。案１では、すべての個人情報は情報連携基盤を経由するが、対象となる情報保有機関でしか解読できないように暗号化されるため、情報連携基盤で認識することはできない。案２では、個人情報は情報連携基盤を経由せず、またトークンは該当処理でのみ有効とするため、該当処理以降の情報保有機関の名寄せには利用できない。

一方、２者間が結託する脅威を想定した場合は、いずれの案においても目的外の名寄せのリスクがある程度存在する。例えば、情報保有機関の２者が結託する場合には、データ送受信時に規定範囲外の個人情報を正当な個人情報の値の一部として不正に挿入しうる。また案２では該当処理のみ有効であるべきトークンを両者で保存し、情報連携基盤への承認を得ずに個人情報を送受信しうる。情報連携基盤と情報保有機関の１者が結託する場合には、情報保有機関の規定範囲を超えた不当な情報連携の要求を情報連携基盤が承認し、情報保有機関に個人情報を集約することがありうる。特に案１は情報保有機関の接続が情報連携基盤に一元化されているため、通信接続の論理的な遮断等によるリスク低減は困難である。

このような２者以上の結託に起因するリスクについても、アクセス制御、通信接続の制御、ログ記録などの機能実装の工夫によって一部回避もしくは検知できる可能性があるが、事象の発生確率は低くなるため、制度的な抑止が十分であればシステム的な対策を行わないという判断もありうる。

以上のとおり、総合的見解としては、異なる符号の利用を前提とした場合には、個人情報の集約の防止という観点では両案に大きな相違はないと考える。

なお本検討では、「番号」および基本４情報は情報連携には利用しないものとし、そのリスクは考慮していない。

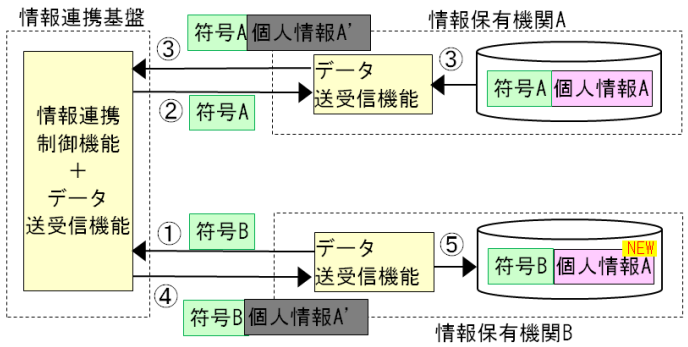
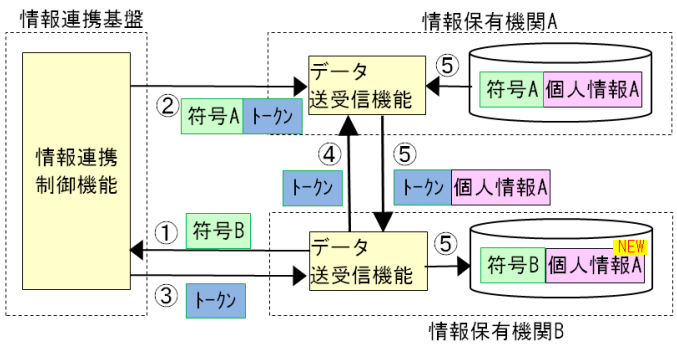
４．「番号」を用いない情報連携について

将来的に幅広い行政分野において情報連携を可能とするにあたり、情報保有機関に「番号」の取得を前提としない「符号」のみによる情報連携の選択肢を提供することが望ましい。利点としては、既存の個人情報との紐付け管理対象が「符号」のみとなりシステム対応が簡素化されるとともに、「番号」に係る個人情報に該当しないため制度的対応も軽減される。

その際の課題の１つに、基本４情報等での突合が容易に実施できない場合に、どのように同一人の情報であることを確認し、「符号」と情報保有機関の固有の識別子との紐付けを行うか、という点がある。対策の一例としては、個人毎のオプトインを前提とし、情報保有機関のオンラインサイトで、ＩＣカードの電子証明書を確認することで紐付けが可能となるが、対応が困難な情報保有機関も多くあると思われる。

上記の課題は、非常災害時の情報連携基盤の活用に向けても重要な観点であり、「番号」やＩＣカードを忘失した場合でも、自己申告の個人情報から臨時暫定的な「符号」を生成するなど、迅速に必要な情報連携ができる運用方策をあらかじめ検討しておく必要がある。その際、特別の対応として「番号」情報自体の送受信が必要な場合には、識別子としてではなく情報連携する個人情報の一部として取り扱う方法が、平常時を含めたリスク管理上は妥当と考える。

表１　異なる符号の利用を前提としたデータ送受信方式の目的外の名寄せリスクに関する比較

		案１（ゲートウェイ方式）	案２（アクセストークン方式）
実現方式例	情報連携元の情報保有機関Ｂが、情報連携先の情報保有機関Ａから、Ｘさんの個人情報Ａの値を取得する場合の処理手順の一例		
		①情報保有機関Ｂは情報連携基盤にＸさんの符号Ｂを示して個人情報Ａを要求する。②情報連携基盤は、政省令で定められた情報連携であることを確認した後、符号Ｂを情報保有機関ＡにおけるＸさんの符号Ａに変換し、情報保有機関Ａに個人情報Ａを要求する。③情報保有機関Ａは、符号Ａに対応する個人情報Ａの値を、情報保有機関Ｂにしか解読できない形式の個人情報Ａ´に暗号化し、情報連携基盤に回答する。④情報連携基盤は、符号Ａを符号Ｂに変換し、情報保有機関Ｂに個人情報Ａ´とともに回答する。⑤情報保有機関Ｂは、Ａ´を復号しＸさんの個人情報Ａを得る。	①情報保有機関Ｂは情報連携基盤にＸさんの符号Ｂを示して個人情報Ａを要求する。②情報連携基盤は、政省令で定められた情報連携であることを確認した後、符号Ｂを情報保有機関ＡにおけるＸさんの符号Ａに変換するとともに、該当処理でのみ有効なトークンを発行して、情報保有機関Ａに個人情報Ａの要求を伝える。③情報連携基盤は、情報保有機関Ｂにトークンを送付する。④情報保有機関Ｂは、情報保有機関Ａにトークンを送付し、情報を要求する。⑤情報保有機関Ａは、トークンに対応する個人情報Ａを、情報保有機関Ｂに回答する。
情報保有機関を跨る目的外のデータマッチング（名寄せ）	脅威	定性的なリスク分析	
	外部による盗用と不正利用	リスクは小さい ・情報保有機関毎に符号が異なるため名寄せできない	リスクは小さい ・情報保有機関毎に符号が異なるため名寄せできない ・トークンは該当処理のみ有効であるため名寄せには利用できない

のリスク	情報保有機関１者の不正	リスクは小さい ・他の情報保有機関の符号は取得できない ・取得できる個人情報範囲は情報連携基盤により制御される	リスクは小さい ・他の情報保有機関の符号は取得できない ・取得できる個人情報範囲は情報連携基盤により制御される ・トークンは該当処理のみ有効であるため名寄せには利用できない
	情報保有機関２者の結託	リスクは中程度 ・情報保有機関間での送受信手順において、規定範囲外の個人情報を正当な個人情報の値の一部として不正に挿入しうる ・ただし他の情報保有機関には波及しない	リスクは中程度 ・情報保有機関間での送受信手順において、規定範囲外の個人情報を正当な個人情報の値の一部として不正に挿入しうる ・該当処理のみ有効であるべきトークンを両者で保存し、情報連携基盤への承認を得ずに個人情報を送受信しうる ・ただし、他の情報保有機関には波及しない
	情報連携基盤の不正	リスクは小さい ・各情報保有機関の暗号鍵を入手しない限り、情報連携基盤では個人情報を解読できない	リスクは小さい ・不正なトークンを発行したとしても、情報連携基盤には個人情報は送受信されない
	情報連携基盤と情報保有機関の結託	リスクは中程度 ・情報保有機関の規定範囲を超えた不当な情報連携の要求を情報連携基盤が承認し、情報保有機関に個人情報を集約することがありうる ・情報保有機関の接続が情報連携基盤に一元化されているため、通信接続の論理的な遮断等によるリスク低減は困難 ・すべての情報保有機関に波及する	リスクは中程度 ・情報保有機関の規定範囲を超えた不当な情報連携の要求を情報連携基盤が承認し、情報保有機関に個人情報を集約することがありうる ・すべての情報保有機関に波及する