資料２－１

情報連携基盤の構築に当たっての論点整理

平成２３年６月３０日
情報連携基盤技術ワーキング・グループ事務局

本資料は、前回同様、検討・整理する必要があるもののうち、①アクセス記録、②マイ・ポータルについて、事務局からたたき台を示したものである。

１　アクセス記録

アクセス記録は、行政機関、地方公共団体及び関係機関による、情報連携基盤を通じた「番号」に係る個人情報のやりとりについて、その日時、主体、情報の種類、根拠などについて、国民自ら確認することを目的として生成されるものである。

社会保障・税に関わる番号制度においては、基本理念の１つとして、「行政機関の保有する「番号」に係る個人情報の適正な取扱いを確保し、当該個人情報へのアクセス記録を国民自ら確認できる社会を目指すこと」を挙げている。

この国民一人ひとりが自らの「番号」に係る個人情報へのアクセス記録を確認するための機能をマイ・ポータルで提供するが、アクセス記録に関して、以下の要件を検討する必要があると考える。

(1) アクセス記録の内容

アクセス記録の内容については、①自己の個人情報に対する情報連携に基づくアクセス、②情報連携の対象となった個人情報の種類、③法令に基づいた情報連携に係るアクセスであることを確認するための情報（主体、根拠法令等）が含まれている必要があると思われる。これを踏まえて、マイ・ポータルで表示するアクセス記録の項目を検討する必要がある。

情報連携に係る処理に関するログには、①管理用のシリアル番号、②情報連携に係るアクセスを行った日時、③情報連携の根拠（法令等で予め定められた情報連携のパターン）、④情報連携元の情報保有機関の名称、⑤情報連携先の情報保有機関の名称、⑥情報連携対象個人情報の種類、⑦情報連携元の情報保有機関の担当部署、⑧情報連携先の情報保有機関の担当部署、⑨情報連携元の情報保有機関において使用された端末、⑩情報連携先の情報保有機関において使用された端末、⑪提供された情報連携対象個人情報の内容、⑫情報連携対象個人情報の用途などが含まれると考えられる。このうち、①から⑥までは情報連携基盤で、⑦・⑨・⑪・⑫については情

報連携元の情報保有機関で、⑧・⑩・⑪については情報連携先の情報保有機関で生成され、保管されるものと考える。

(2) アクセス記録の生成方法

アクセス記録を生成するに当たっては、情報連携に係る処理に関するログ（(1)の①から⑥までのログ）から必要な情報を抽出して、当該情報を本人が確認することができる形式に変換することが考えられる。

具体的には、(1)の①から⑫までのログのうち、情報連携基盤で保管されるログ（(1)の①から⑥まで）には、情報連携の対象となった個人情報の種類、法令に基づいた情報連携に係るアクセスであることを確認するための情報（主体、根拠法令）が含まれていることから、この情報連携基盤で保管されるログに基づいて、マイ・ポータルで確認するためのアクセス記録を生成することが考えられる。

なお、マイ・ポータルに表示するアクセス記録の生成単位についても、検討が必要である。例えば、情報連携により自己の個人情報が提供された事実は「情報連携先より回答を行った日時」を基準としたアクセス記録のみでも確認が可能である。一方で、全てのアクセス記録を確認するためには、「情報連携元より要求を行った日時」を基準としたアクセス記録についても生成し、表示することも考えられる。

また、片方のログのみ記録されている場合（「情報連携先より回答を行った日時」の記録が無い場合）には、「情報連携元より要求を行った日時」を基準としたアクセス記録のみ表示したうえで、情報連携が中断され、情報連携による自己の個人情報は提供されなかったこと等を同時に示すといった対応が考えられる。

(3) アクセス記録の表示方法

マイ・ポータルにアクセス記録を表示する際は、これらの内容を本人が理解できるように自然言語へ変換する必要がある。なお、自然言語への変換は、用語や表現振りの最適化を行うことが望ましい。

(4) アクセス記録の編集

マイ・ポータルで自己のアクセス記録を表示させるためには、保存されたすべての情報連携に係るアクセス記録の中から、自己のアクセス記録を特定する必要がある。これを行うためには、対象者を特定することができる何らかのキー情報をアクセス記録に付与しておく必要がある。情報連携に関連するシステムにおいて、対象者を特定することができるキー情報と

して活用することができる情報として保持されているのは、ＩＤコード又はリンクコードであると考えられる。したがって、ＩＤコード又はリンクコードのいずれかをアクセス記録に付与して管理する必要があると考える。

⑸ アクセス記録の保管場所

アクセス記録の保管場所については、情報連携基盤又はマイ・ポータルで保管することが考えられる。情報連携基盤にはアクセス記録を生成するために必要なログが保管されており、情報連携基盤にアクセス記録の生成機能を搭載することを考慮すると、情報連携基盤に管理機能を併せて搭載して、アクセス記録を保管することが考えられる。この場合、情報連携基盤でアクセス記録を生成・保管し、マイ・ポータルからの要求に応じて、該当のアクセス記録をマイ・ポータルに提供することが想定される。

一方、マイ・ポータルでアクセス記録を保管することとした場合には、情報連携基盤におけるアクセス記録の生成後、マイ・ポータルにアクセス記録が提供されることになることから、マイ・ポータルにアクセス記録の管理機能を搭載することになる。

なお、アクセス記録の保管場所をマイ・ポータルとした場合、ＩＤコードをキー情報とすることは、マイ・ポータルでＩＤコードが保持されることになるため、ＩＤコードの性質上適当ではないと思われる。

⑹ アクセス記録の完全性確保

冒頭でも述べたように、社会保障・税に関わる番号制度においては、基本理念の１つとして、「行政機関の保有する「番号」に係る個人情報の適正な取扱いを確保し、当該個人情報へのアクセス記録を国民自ら確認できる社会を目指すこと」を挙げている。そのためには、当該個人情報へのアクセス記録の内容が正確であること、つまり、完全性を確保することが必要である。完全性確保のために必要な措置としては、アクセス記録生成時においては誤りの無い内容を記録すること、また、アクセス記録生成後の保管においては、不正な改ざんから保護すること等が想定される。

なお、アクセス記録の生成に係る仕様が更新されることに伴い、誤ったアクセス記録が生成されてしまうといったことの無いよう措置を講ずることも必要である。

⑺ アクセス記録及び情報連携に係るログの保管期間

アクセス記録及び情報連携に係るログの保管期間については、関連する法令を踏まえた上で検討する。

なお、アクセス記録及び情報連携に係るログを長期に保管することによる運用面及び費用面での負担を考慮すると、保存期間を必要最小限に止め、情報連携基盤及び情報保有機関において費用面で過度な負担が生ずることがないよう配慮する必要がある。これらの点を踏まえ、保管期間について引き続き検討する必要があると考える。

⑻ 第三者機関の監査範囲

第三者機関は、情報連携に関して、情報連携基盤を随時監査する権限・機能を有し、また、「番号」に係る個人情報の取扱いについて、資料の提出、説明等を求め、調査や実地の検査を行う。

これに伴い、第三者機関は、情報連携に関するアクセス記録のみならず、情報連携基盤及び情報保有機関において保存する情報連携に係るログについて、必要に応じて調査・分析する。

したがって、情報連携基盤及び情報保有機関における情報連携に係るログは、第三者機関による監査の範囲に含まれると考えられ、取得及び保管が求められると想定される。かつ、必要に応じ、第三者機関の監査に対応するため、資料の提出及び説明のための機能や体制を整備することが考えられる。

なお、第三者機関による監査の対象となる情報連携に係る処理のログ等については、ログの多くは個人情報が含まれているため、一元管理することは適当ではないことから、情報連携基盤及び情報保有機関のそれぞれに分散して管理し、必要に応じて各機関からログを収集して監査する方式が考えられる。一方、ログ情報の保護、完全性の担保等を重視し、情報連携に係るすべてのログを一括して管理した上で、第三者機関が監査を行う方式も考えられる。

２　マイ・ポータル

⑴ マイ・ポータルの役割

マイ・ポータルは、社会保障・税に関わる番号制度において、国民に提供される情報にアクセスするための入り口となるウェブサイトである。

社会保障・税に関わる番号制度においては、情報保有機関が保有する自己の「番号」に係る個人情報等を確認できるように、かかる情報を、個人一人ひとりに合わせて表示することができるようにするため、ポータルを設けることとしている。

個人は、マイ･ポータルを通じて、①自己の「番号」に係る個人情報についてのアクセス記録の確認、②情報保有機関が保有する自己の「番号」に

係る個人情報の確認、③電子申請、④行政機関等からのお知らせの確認を行うことができることとする。

なお、マイ･ポータルにおいては、大規模災害時や、重大な機器等の故障等が発生した場合においても業務を継続することができるような措置を講じるものとする。

⑵ マイ・ポータルの利用者フォルダへのログイン手順

マイ・ポータルでは、自己の「番号」に係る個人情報等は利用者フォルダという個人ごとの領域に格納され、当該個人がこの領域に格納された情報等を確認することができるようにする。この利用者フォルダにログインする際の本人確認方法としては、公的個人認証サービスが提供する認証用電子証明書を使用することとしている。

なお、利用者フォルダへの利用に先立ち、利用者である個人に関する情報をマイ・ポータルに設定するための初回登録を行うが、この際には、公的個人認証サービスが提供する署名用電子証明書及び認証用電子証明書の２つの電子証明書を使用することとしている。

マイ・ポータルの利用者フォルダに関する初回登録手順及びログイン手順の流れ（イメージ）は、資料２－２のとおりである。

初回登録時には、マイ・ポータルの利用者は、マイ・ポータルに対して署名用電子証明書による利用者フォルダ利用申請を行い（マイ・ポータル側では署名用電子証明書の有効性確認後、署名用電子証明書に記録された氏名等の４情報の抽出及び当該４情報によるマイ・ポータル用リンクコードの取得及び登録を行う。）、この処理の完了後、利用者は、マイ・ポータルに対して、利用者フォルダへのログインの際に必要となる認証用電子証明書の提供を行う（マイ・ポータル側では認証用電子証明書の有効性確認後、認証用電子証明書のシリアル番号を抽出し、利用者フォルダへのアクセスキーとして登録する。）。

また、初回登録後の利用者フォルダへのログイン時には、認証用電子証明書の提供による本人確認を行い、本人確認後、当該利用者の利用者フォルダ画面を表示させる。

⑶ マイ・ポータルの利用者フォルダにおける前回ログイン日時の表示

上記⑵のとおり、マイ・ポータルの利用者フォルダは、利用者の本人確認を行った上で、格納された情報を確認することができる仕組みであるが、本人以外の者が本人と偽ってログインしていないことを確認するための１つの手段として、利用者フォルダにログインした後の画面に、前回ログイ

ン時の日時を表示させることが考えられる。表示される前回ログイン時の日時について、ログインを行った本人に身に覚えがない場合には、マイ・ポータルに問い合わせること等ができ、これが不正なログインを発見する端緒となることも考えられる。

(4) マイ・ポータルにおける個人の情報の保持

マイ・ポータルでは、自己の「番号」に係る個人情報についてのアクセス記録の確認や情報保有機関が保有する自己の「番号」に係る個人情報の確認を行うことができるようにするに当たり、アクセス記録や情報保有機関が保有する個人情報の提供を受けるための処理を行う。また、本人からこれらの処理を行うために必要な情報（氏名等の４情報、認証用電子証明書のシリアル番号等）の提供を受けて、マイ・ポータル内で必要な設定を行うことが考えられる。

マイ・ポータルで表示する情報については、①本人による利用者フォルダログイン後、速やかに該当の情報が画面に表示されて本人がこれを確認することができるようにするため、事前に必要な情報をマイ・ポータルに収集・蓄積しておくという考え方（本人による確認の即時性を重視）と②マイ・ポータルでは必要な状態になるまでできる限り情報を保有しないようにするため、本人による利用者フォルダログイン後に、情報保有機関から該当する情報をマイ・ポータルに収集して、画面に表示させるという考え方（マイ・ポータルにおける情報保持の回避を重視）がある。

①の考え方では、本人による情報の確認が速やかに行われることが見込まれるが、マイ・ポータルに情報が蓄積されている状態が続くことになることから、マイ・ポータルが情報保有機関と類似の位置づけになるのではないかとの指摘がある。一方、②の考え方では、情報の保持は必要最小限となるが、利用者フォルダログイン後、本人が情報を確認するまでに時間を要することが懸念される。

なお、利用者フォルダに格納された情報で、本人による確認が行われた情報については、ログアウト後、消去することが考えられる。マイ・ポータルには、これを実現するための仕組みを構築する必要があると思われる。さらに、利用者フォルダに格納する情報について、マイ・ポータルで確認した情報を改めて本人が確認することができるよう、本人が情報を確認してログアウトする前に、一定のファイル形式でダウンロードすることができるようにする機能を提供することについて、検討する必要があると思われる。

また、マイ・ポータルに保持する必要がある情報については、個人情報

の適正な取扱いを担保する必要があると思われる。
　そこで、マイ・ポータルには、情報保有機関と同様のセキュリティ対策を組み込んだ仕組みを構築する必要があると思われる。

⑸ 認証用電子証明書の有効期間切れ又は失効等が発生した場合の対応
　マイ・ポータルの利用者フォルダは、初回登録により利用者本人に関する情報を格納する領域として開設され、保持されることになる。
　この利用者フォルダについては、認証用電子証明書による認証を本人確認方法として利用し、認証用電子証明書のシリアル番号を利用者フォルダへのアクセスキーとして使用する場合、認証用電子証明書の有効期限が切れた場合や失効した際には、認証用電子証明書による本人確認を行うことができず、利用者フォルダにログインすることができなくなるという課題がある。
　この点については、再度、本人において認証用電子証明書を取得し直した上で、マイ・ポータルで初回登録と同様の登録作業を行い、取得し直した認証用電子証明書のシリアル番号を従前から使用していた利用者フォルダの新たなアクセスキーとして設定することが考えられる。

⑹ マイ・ポータルの利用者フォルダの保持期間
　マイ・ポータルに設定された利用者フォルダについては、本人の死亡又は国籍喪失を伴う海外転出等、本人が「番号」の付番要件を喪失するまでは、保持し続けることが求められるのではないかと思われる。
　また、「番号」の付番要件を喪失した後も、例えば、本人の死亡に伴い代理人が相続等に係る手続を行う際にマイ・ポータルの利用者フォルダで本人の情報を確認する必要が生じる可能性があることを考慮すると、一定の期間は、マイ・ポータルにおいて利用者フォルダを保持する必要があるのではないかとの考えがある。ただし、マイ・ポータルにおいて、本人が「番号」の付番要件を喪失したことを把握する方法については、引き続き、検討を要すると思われる。

⑺ 代理人によるマイ・ポータルの利用
　マイ・ポータルの利用者については、情報保有機関が保有する自己の「番号」に係る個人情報の確認等を行おうとする本人とともに、本人に代わってこれを行う代理人（注）が想定されている。
　そのため、マイ・ポータルには、代理人として本人に代わってログインする者であることを登録するための機能が必要であると思われる。また、

当該機能と併せて、マイ・ポータルが提供する本人に関する情報を代理人においても確認することができるようにする機能、代理人が本人に代わって確認することができる情報の範囲を特定する機能、マイ・ポータルに登録された代理人の登録を解除するための機能等が必要ではないかと思われる。

なお、マイ・ポータルが提供する本人に関する情報を代理人においても確認することができるようにする機能に関しては、代理人による情報の確認方法について、①代理人の利用者フォルダに本人に関する情報を格納した上で代理人がこれを確認する方法と②本人の利用者フォルダに代理人もログインすることができるように設定した上で、代理人が本人の情報を確認する方法があると思われる。

①の方法では、本人に関する情報を本人と代理人の２つの利用者フォルダに格納することとなり、その際には、格納すべき情報の判別を行う必要があるが、本人しか確認することができない情報を代理人が確認することを回避することができると思われる。一方、②の方法では、本人に関する情報を１つの利用者フォルダに格納することになるが、格納された情報を本人及び代理人の双方が確認することになり、本人と代理人の間で利益相反となるおそれのある情報についても代理人が確認することができる可能性があることから、利益相反となるおそれがある情報か否かを情報保有機関側であらかじめ判別する等の対応が必要であると思われる。

（注）　マイ・ポータルにおける代理人には、法定代理人と任意代理人が想定されている。