資料2

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２）

平成２３年3月２３日
情報連携基盤技術ワーキング・グループ

第２　個人の本人確認（マイポータル・ＩＣカード等）

１．基本的考え方

（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

「当面の情報連携の範囲は、年金、医療、福祉、介護、労働保険の各社会保障分野と国税・地方税の各税務分野とする」（基本方針Ｐ．６）ことから、マイ・ポータル等はセンシティブな個人情報を取り扱うこととなる。

住基ネット訴訟に係る最高裁判決に対応するためには、マイ・ポータルにログインするための本人認証は、高いセキュリティレベルに対応できる認証方法とするなど、個人情報保護の観点や情報の一元管理を回避する厳格な仕組みが必要であり、「「番号」を利用する際、利用者が「番号」の持ち主本人であることを証明するための本人確認（公的認証）の仕組みを構築するため、既存のシステムである公的個人認証及び住民基本台帳カードを番号制度の導入に合わせて改良し、活用することにより、本人確認を行う」（基本方針Ｐ．７）。

（２）公的個人認証サービス及び住民基本台帳カードの改良

一方、公的個人認証サービスや住民基本台帳カードは、もともと「番号」と「番号」を所持する者との関係を確認するために設けられたものではないことから、社会保障・税に関わる番号制度及び国民ＩＤ制度で活用していくために、いくつかの改良が必要である。

具体的には、マイ・ポータルにログインするために、①公的個人認証サービスに認証用途を付加すること、②電子証明書の有効期間の延長など公的個人認証サービスの利便性を高めること、③法令等で「番号」を確認することが認められている民間事業者が電子的に本人確認を行うことができるよう署名検証者を民間事業者に拡大すること、④住民基本台帳カードの券面に「番号」を記載することを検討すること等が考えられるのではないか。

２．マイ・ポータルの利用

（１）マイ・ポータルの機能

マイ・ポータルには、次の４つの機能を持たせることとしてはどうか。

①自己情報へのアクセスログを確認する機能

②各情報保有機関が保有する自己情報を確認する機能

③電子申請を経由する機能（ワンストップサービス）

④行政機関等からのお知らせを表示する機能（プッシュ型サービス）

（２）マイ・ポータルにおける情報管理のあり方

マイ・ポータルが取り扱う情報を内部的に管理するため、利用者の申請により各利用者固有の情報を管理する領域を確保し、利用者フォルダ（マイ・ポータルの利用者に情報提供するためのシステム上の作業領域で、個人とはリンクコードのみで紐付けられ管理されているもの。）を開設する（（３）③参照）こととし、個人情報保護の観点や情報の一元管理を回避する観点から、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。

（３）マイ・ポータルにログインするための認証

①　ログインのためのアクセスキー

ＩＤコードやリンクコードをＩＣカード内に格納してマイ・ポータルにログインするためのキーにすることは、情報連携のための共通の識別子であるＩＤコードやリンクコードがインターネット上を流通することになり、セキュリティの観点から相応しくないのではないか。

「番号」は、他人に容易に知られてしまう「見える」番号であり、これをキーとしてログインすることは、成りすまし等の具体的危険性が高いことから、相応しくないのではないか。

このため、公的個人認証サービスに認証用途を付加し（４．（１）参照）、署名用の電子証明書とは別に認証用の電子証明書を発行することとし、認証用の電子証明書のシリアル番号（以下「認証用シリアル番号」という。）を、次の観点から、ログインするためのキーとして利用することとしてはどうか。

(a) 「番号」やＩＤコードとは論理的な関連性はなく、仮に当該シリアル番号が流出しても、ＩＤコード等を知ることはできないこと

(b) 電子証明書等は暗号化して送付するが、仮に認証用シリアル番号が盗まれたとしても、秘密鍵自体は本人しか有しないため、当該認

証用シリアル番号だけでは、認証することはできないこと

(c) 現行の公的個人認証サービスの署名用の電子証明書のシリアル番号（以下「署名用シリアル番号」という。）と同様に、認証用シリアル番号は一意性があるものとすることができること

一方で、認証用シリアル番号は電子証明書の有効期間満了により失効するものの、民間事業者も含め、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する危険性が高まることから、次の対策を講じるべきではないか。

(a) 現行の公的個人認証サービスと同様に、認証用途以外の目的で使用することを法律上明確に禁止すること

(b) 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や情報保有機関の管理する各利用番号と認証用シリアル番号との紐付けは行わないこと

(c) 電子証明書が本人のものであるかどうかは認証局に問い合わせることとし、当該認証局はマイ・ポータル運営機関又は各情報保有機関に対し、情報連携基盤を通じて、当該者のリンクコードを伝達する仕組みとすること

② 認証用シリアル番号と認証局用リンクコードの紐付け

認証局は、利用者の申請によりＩＣカードに認証用の電子証明書を格納する際に取得した４情報をもって、情報連携基盤に認証局用のリンクコードの生成を要求し、生成された認証局用のリンクコードと認証用シリアル番号を紐付けしておくこととしてはどうか。

③ マイ・ポータルへのログインの手順

マイ・ポータルにログインする手順としては次のとおりとしてはどうか。

(a) 利用者フォルダの取得（初回にアクセスする際の対応）

ⅰ）利用者は、ＩＣカードをリーダライタにセットし、暗証番号を入力し、公的個人認証サービスの署名用の電子証明書（４情報が含まれている。４.（４）参照）等を利用して、利用者フォルダ取得の電子申請を行う。

ⅱ）マイ・ポータル運営機関は、利用者の電子証明書を付した電子申請を受領し、認証局に対して電子証明書の有効性確認を行い、電

子申請の正当性を確認する。

iii）マイ・ポータル運営機関は、マイ・ポータルが取り扱う情報を内部的に管理するため、各利用者固有の情報を管理する領域である利用者フォルダを開設する。

iv）マイ・ポータル運営機関は、利用者の申請による４情報をもって、情報連携基盤にマイ・ポータル用のリンクコードの付番を要求する。

v）マイ・ポータル運営機関は情報連携基盤から通知された当該リンクコードと利用者フォルダを紐付ける。

(b) ログイン（アクセスする都度の対応）

i）利用者は、マイ・ポータル上にあるログイン・ボタンをクリックした後、ＩＣカードをリーダライタにセットし、暗証番号を入力して、公的個人認証サービスの認証用の電子証明書等（４．参照）を利用して、ログイン要求を行う。

ii）利用者が送付する認証用の電子証明書等は暗号化してマイ・ポータル運営機関に対し送付する。

iii）マイ・ポータル運営機関は、認証局とやりとりして、認証用の電子証明書の有効性を確認し、利用者の認証を行う。

iv）認証がされた場合、マイ・ポータル運営機関は認証用シリアル番号を情報連携基盤へ送付する。送付後は、マイ・ポータル運営機関に認証用シリアル番号が蓄積しないよう削除する。

v）情報連携基盤は、認証用シリアル番号を認証局へ送付する。送付後は情報連携基盤に当該番号が蓄積しないよう削除する。

vi）認証局は、あらかじめ認証用シリアル番号に紐付けられた認証局用リンクコード（２.（３）②参照）を、情報連携基盤に振り出す。

vii）情報連携基盤は、当該認証局用のリンクコードからＩＤコードを介して、マイ・ポータル運営機関にマイ・ポータル用のリンクコードを振り出す。

viii）マイ・ポータル運営機関は、当該マイ・ポータル用のリンクコードから、当該利用者の利用者フォルダを特定する。

ix）マイ・ポータル運営機関は利用者に対して、ログインに成功したことを通知する。

（４）自己情報へのアクセスログを確認する機能

マイ・ポータルで確認できるアクセスログについては、第１の６．のと

おりである。

アクセスログを確認する手順としては次のとおりとしてはどうか。

ⅰ）マイ・ポータルにログイン後、利用者が、自己情報へのアクセスログの確認をマイ・ポータル運営機関に要求する。

ⅱ）マイ・ポータル運営機関は、利用者フォルダと紐付いているリンクコードを通じて、情報連携基盤に問い合わせをする。

ⅲ）情報連携基盤は、情報連携基盤に記録されているアクセスログの情報を、マイ・ポータル用のリンクコードを通じて、マイ・ポータルの利用者フォルダに送付する。

ⅳ）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アクセスログの情報は削除する。

（５）各情報保有機関が保有する自己情報を確認する機能

情報保有機関が保有する自己情報は、情報保有機関において適切に管理するべきものであり、マイ・ポータルに蓄積することは極力回避するべきではないか。

マイ・ポータルは、情報保有機関と認証連携を行い、情報の閲覧は、情報保有機関が有するサイトから行うことも検討してはどうか。この際、既存の技術を活用しつつ、マイ・ポータルへログインした際の認証結果を情報保有機関に引き継ぐ方法を検討してはどうか。

自己情報を確認する基本的な手順としては次のとおりとしてはどうか。

ⅰ）利用者は、マイ・ポータルにログイン後、情報保有機関が保有する自己情報を確認することをマイ・ポータル運営機関に対して要求する。

ⅱ）マイ・ポータル運営機関は、利用者フォルダに紐付いているマイ・ポータル用のリンクコードを通じて、情報連携基盤に問い合わせる。

ⅲ）情報連携基盤は、マイ・ポータル用のリンクコードをＩＤコードに変換し、さらに、情報保有機関のリンクコードを振り出して、情報保有機関に伝達をする。

ⅳ）情報保有機関は、当該リンクコードから、情報保有機関が保有する利用番号を通じて、必要な情報を取り出し、当該情報を情報連携基盤を通じて、マイ・ポータルに送信をする。

ⅴ）マイ・ポータル運営機関は、利用者フォルダに個人情報を一時的に保存して、マイ・ポータルに表示する。

ⅵ）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。

（６）電子申請を経由する機能（ワンストップサービス）

利用者は、マイ・ポータルに公的個人認証サービスの認証用の電子証明書等によりログインすることとなるが、社会保障や税の分野における電子申請のように、センシティブな個人情報を取り扱うことが想定されている場合には、申請書の文書の真正性を推定する効果が働くことや改ざんを防止する必要があることから、あらためて、公的個人認証サービスの署名用の電子証明書等で申請を行う必要があるのではないか。

情報保有機関に対する電子申請については、情報保有機関の責任において署名検証を行う必要があるのではないか。

なお、必要な手続きはマイ・ポータルのトップページから、各情報保有機関のサイトにリンクを張り認証連携することで、利用者が各手続きの電子申請を行うこととするが、典型的なサービスについて、一度、電子申請をすれば、申請が必要な全ての情報保有機関に送付され処理される仕組み（ワンストップサービス）も検討することとしてはどうか。

（７）行政機関等からのお知らせを表示する機能（プッシュ型サービス）

情報保有機関が利用者に対してお知らせする事項がある場合には、当該情報は、マイ・ポータルの利用者フォルダに送付する仕組みとしてはどうか。

お知らせを表示する手順としては次のとおりとしてはどうか。

ⅰ）情報保有機関が利用者に対して伝達事項がある場合には、情報保有機関のリンクコードを通じて、情報連携基盤に必要なお知らせ情報を送付する。

ⅱ）情報連携基盤は、情報保有機関のリンクコードをＩＤコードに変換し、さらにマイ・ポータル用のリンクコードを振り出して、マイ・ポータルの利用者フォルダに、お知らせ情報を送付する。

ⅲ）利用者がマイ・ポータルにログインするまで、当該情報は利用者フォルダに保存することとし、利用者がマイ・ポータルにログインした際、当該お知らせ情報を表示する。なお、当該お知らせ情報には、リンクが張られており、必要な電子申請等を行うことができるようにする。

ⅳ）利用者が閲覧した場合や、当該情報を表示する期限が切れた場合には、当該情報が利用者フォルダから削除される。

（８）自宅以外でのマイ・ポータルの利用

マイ・ポータルは、自宅のパソコンで利用できることはもちろん、自宅

にパソコンがない場合であっても、例えば、現在は証明書等の発行に利用されている行政キオスク端末で利用が可能となる仕組みとするべきではないか。

そのためには、コンビニエンスストアなど、既存のインフラやサービスを有する民間事業者と連携を図ることを検討してはどうか。

３．窓口等における本人確認

法令等で「番号」を確認することが認められている機関は、書面又は電子的な方法により、本人確認をした上で、「番号」を確認する必要がある。

（１）書面により本人確認及び「番号」確認を行う場合

①　本人がＩＣカードを所持していない場合

法令等で「番号」を確認することが認められている機関の窓口等（以下「窓口等」という。）においては、利用者に対し、本人確認書類（運転免許証等）の提示を求め、本人であることを確認した上で、「番号」の申告を求め、本人から申告された「番号」を書面に記載することとしてはどうか。

②　本人がＩＣカードを所持している場合

ＩＣカードのＩＣチップ内に「番号」を安全に格納し、窓口等において確認し利用できる仕組みとしてはどうか（５．（４）参照）。

なお、窓口等の体制が未整備の場合は、ＩＣカードに記載された「番号」を書面に記載することも考えられるか。

（２）電子的に本人確認及び「番号」確認を行う場合

窓口等が書面を使わず電子的に本人確認及び「番号」確認を行う場合には、公的個人認証サービスの仕組みを活用して本人確認をした上で、ＩＣカードから「番号」を取り出す仕組みを検討してはどうか。

４．公的個人認証サービスの改良

（１）認証用途の付加の必要性

社会保障・税に関わる番号制度及び国民ＩＤ制度において求められる本人確認は、文書を伴わないアクセスであり、不正データに誤って電子署名をするリスクを回避するため、認証用途の付加を行う必要があるのではないか。

なお、認証用の電子証明書は、署名用の電子証明書と異なり、文書の真

正性の推定効が働かないことから、特に、検証者に対しては、署名用の電子証明書と適切に使い分ける義務を課した上で、システムとしてその実行を担保する仕組みとしてはどうか。

（２）鍵ペア

認証用途として利用した鍵ペアを、署名用途として利用した鍵ペアとして利用するリスクを回避するため、ＩＣカードのＩＣチップ内には、署名用途の鍵ペアと認証用途の鍵ペアを別々に格納するなどの措置を講じることとしてはどうか。

（３）電子証明書の発行

現在、公的個人認証サービスについては、市町村が発行する住民基本台帳カードに市町村の窓口において厳格な本人確認を行った上で、都道府県知事が電子証明書を発行しており、このことが信頼性の担保となっていることから、同様の方法とするべきではないか。

（４）電子証明書の記録事項

署名用の電子証明書は、現行と同様に、４情報、署名用シリアル番号、有効期間の満了日等を記録し、認証用の電子証明書には、４情報は記録せず、認証用シリアル番号、有効期間の満了日等を記録することとしてはどうか。

（５）電子証明書の有効期間・更新

電子証明書の有効期間については、現在３年間とされているところであるが、暗号方式を強化した上で、５年間に延長することとしてはどうか。

現在、失効した電子証明書を更新する場合には、利用者は、住所地市町村の窓口に出向き、本人確認を受けた上で電子証明書の発行を申請する必要があるが、利用者の利便性を高めるため、利用者がオンラインで電子証明書を更新できる仕組みを検討してはどうか。

（６）ＩＣカード以外のデバイス

携帯電話等ＩＣカード以外の媒体については、それのみでは当該媒体が真に本人のものであるかどうかの確証が得られないことから、ＩＣカード以外の媒体の利用を希望する場合においては、公的個人認証サービスを格納するＩＣカードを所持し、かつ、本人の同意がある場合に限り、セキュリティが確保されることを前提に、当該媒体に公的個人認証サー

ビスを格納することを可能とする仕組みを検討することとしてはどうか。

（７）署名検証者の拡大等

３．（２）のとおり、法令等で「番号」を確認することが認められている民間事業者が電子的に本人確認を行えるようにするため、また、将来的に、情報連携する範囲を民間事業者に拡大するためには、民間事業者において、より安全に本人確認を行う取引環境を整えることが前提となることから、署名用途及び認証用途に係る検証者について民間事業者にも拡大することとしてはどうか。

その際、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。

５．ＩＣカード（住民基本台帳カードの改良）

（１）ＩＣカードの交付

国民に対して自己情報へのアクセス記録を確認する権利を保障する観点から、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。

法定代理人や任意代理人による取得については、住基カードの取得の手続きと同様に、代理人の本人確認等の手続きを適切に行うことを検討してはどうか。

（２）ＩＣカードの発行

ＩＣカードの発行にあたっては、現在の住民基本台帳カードが、市町村の窓口において厳格な本人確認を行った上で発行しており、このことが信頼性の担保となっていることから、同様の方法とすべきではないか。

また、ＩＣカードの機能については、現行の住民基本台帳カードが、①住民が転入届の特例を受け、②全国の行政機関で本人確認を行い、③住民の日常生活において民間事業者との契約等の手続の場面での本人確認を行うことを可能とするとともに、市町村が様々なサービスにＩＣカードを活用できるようにすることを目的として設けられたものであることから、ＩＣカードは当該機能も併せて持つこととしてはどうか。

（３）券面記載事項

現行の住民基本台帳カードについては、タイプＡ（氏名のみ、顔写真無し）及びタイプＢ（４情報、顔写真あり）があるが、取引における本

人確認を厳格に行うため、ＩＣカードは、４情報及び顔写真を券面に記載することとしてはどうか。

「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。

ＩＣカード券面に「番号」を記載することを望まない者に対する対応についてどう考えるか。

（４）ＩＣチップ記録事項

ＩＣカードの券面に記載されている「番号」が偽変造されていないことを確かめるため、ＩＣチップ内に「番号」を安全に記録し、窓口等は、ＩＣカードの券面記載事項（４情報、顔写真及び「番号」等）をリーダライタ及びソフトウエアで確認することができるようにしてはどうか。

ＩＣチップ内の「番号」を確認するためのソフトウエアについては、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ものとしてはどうか。

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。

第３　法人に対する付番

１．付番対象

基本方針においては、「法人等に対して付番する「番号」については、商業・法人登記の申請に係る会社法人等番号を活用した番号とする。会社法人等番号を有しない法人等に対して付番する「番号」については、今後検討する」（基本方針ｐ．５ Ⅱ １．（１））とされている。

会社法人等番号は、商業・法人登記の申請にかかる会社法人等に対して各法務局から付与される番号であるが、登記を要しない法人・国・地方公共団体・人格なき社団等など、一部の法人等に対しては付与されていない。

このため、付番対象は、会社法人等番号を有する法人本店のほか、登記を要しない法人、国・地方公共団体、国税・地方税の納税義務を有する人格なき社団等など付番機関の長が適当と判断したもの（以下「登記のない法人等」という。）とし、登記のない法人等については、付番機関が独自の「番号」を

付することとしてはどうか。

なお、法人の事業所に関しては、必ずしも会社法人等番号を有しないこと等から「番号」の付番は困難であるが、国税と地方税とで源泉徴収又は特別徴収を行う給与支払事務所の範囲が重複しており、これらに関しては部内番号等の情報を共有していくこととすべきではないか。

２．登記のない法人等に対する付番方法

番号の基礎となる会社法人等番号は、登記所コード４桁＋登記簿種別２桁＋個別番号６桁の計１２桁の整数で構成されているが、登記のない法人等に対しては、既存の登記所コードと重ならない番号を使用して付番することとしてはどうか。

３．番号の変更

会社法人等番号は平成２４年度以降、管轄登記所外への移転登記又は組織変更の登記を行っても会社法人等番号が変更されない仕組みとなる予定であり、「番号」についても同様に、変更しないこととしてはどうか。

また、重複付番を避けるためにも一度使用した番号は再利用しないこととしてはどうか。

４．番号の通知

法人は公的認証の利用又は券面に表示された番号を提示して税又は社会保障サービスを受けることを想定していないことから、番号の通知は紙により行うこととしてはどうか。

５．検索及び閲覧

「法人等に対して付番する「番号」は、広く一般に公開されるものであり、自由に流通させることができ、官民を問わず様々な用途で利活用するものとする。」（基本方針ｐ．５ Ⅱ １．（１））とされている。

このため、法人等に対する付番機関においては、法人等の基本３情報（商号又は名称、本店又は主たる事務所、会社法人等番号）の検索、閲覧ができるサービスをホームページで提供することを基本としてはどうか。

第４　その他

１．企業コードについて

ＩＴ戦略本部電子行政に関するタスクフォース（以下「タスクフォース」という。）においては、行政の電子化によって企業の利便性の向上や行政の業務効率の向上を図る観点から、企業コードの整備及びその活用のための施策について検討している。

今後の検討の方向性としては、ニーズの把握、費用対効果の検証を前提として、例えば、番号制度により付番される法人番号と他の行政分野や民間分野で使用されている法人の識別番号との紐付け・置換の推進、行政機関間での企業情報の相互参照による行政手続における公的添付書類の削減、民間の電子商取引等においても信頼性が保たれた企業のアイデンティティを表す属性情報の参照の充実、用途・利用者・利用場所等を考慮した企業認証の整備等が考えられるのではないか。

また、企業コードには、網羅性　（法人等に対して網羅的に付与）、一意性（法人等に対して重複なく付与）、一貫性（法人等の商号変更、移転等が生じてもコードは不変）、非再利用性（法人等が消滅しコードに空きが生じても他に割当しない）、開放性（誰でも利用可能）、参照可能性（コードの公開）、非譲渡可能性（企業の所有権や商号が譲渡可能されても、コードは譲渡されない）等の性質が備わっていることが望ましいと考えられるが、上記のような施策を推進するに当たっては、番号制度により付番される法人番号を活用し、その上で、求められる性質を満たすための仕組みをタスクフォースにおいて検討することが考えられるのではないか。