

4 個人認証方法に関する検討

インターネットが急速に拡大した理由の一つは、ネットワーク利用者が匿名で様々なサービスを利用することが可能であったからである。しかしながら、官民に関わらず「手続き」というものは、利用者の権利・義務関係を設定するものであることから、インターネット上では、必ずしも不可欠とされなかった、本人確認、本人の同意、本人の所在、本人の所有関係といった、本人確認すなわち個人認証が必要となる。

官民連携ポータルは、官民の多様な手続きを一括して行うサービスを提供するものであることから、多様な主体が多様な手段で行っていた本人確認を、どのように扱うかが問題となる。特に政府、地方公共団体においては、行政効率の確保、個人情報保護といった観点から民間の手続きサイトとの連携は慎重である。

本章では、個人認証に係る技術動向を概観するとともに、電子商取引分野、電子政府・電子自治体分野で行われている個人認証の実例を調査することにより、多数の主体を連携させる官民連携ポータルにおける個人認証のあり方について検討を行い、現時点で、官民連携ポータルに電子政府・電子自治体の手続きを連携する際の考え方をまとめた。

(1) 検討の必要性と方法

1) 検討の必要性

従来、官民の申請手続きは、窓口や、郵送、電話などで様々な厳重さのレベルで行われている。その際に必要な書類についても、実印、認め印、身分証明書の提示、署名、対面での確認など、本人確認の厳重さに応じて要求を変えている。このような手続きがネットワークに移行していく中で、公的個人認証サービスなどの電子証明書の確認、ID・パスワードの登録などの手段で本人確認を行っているのが現状である。

窓口での手続きの場合も、手続きの種別によって本人確認の厳重さが異なるのと同様、ネットワーク上での認証についても、手続きによって確定する権利義務関係の重要性、リスクの大きさ、事故等発生時の回復の容易さなど、手続きの種類によって、厳重な認証手段・手軽な認証手段を使い分ける必要がある。

ネットワーク上での認証については、ネット通販、ネットバンキングなど、民間サービスでの実績が蓄積されつつある。また行政サービスにおいても、電子申請・手続きのスタートにより、公的個人認証サービス等による認証が始まっている。

しかしながら、手続きの性質による、本人確認(認証手段)の厳重さ(認証レベル)については、未だ、明確な関連付けが定まっておらず、申請受付事業者により、独自に判断されているのが現状である。官民連携ポータル事業を行う際には、申請受付事業者間の認証の違いを調整する時間とコストが負担になることが指摘されている。

2) 検討のアプローチ

地方公共団体における個人認証の現状及び基本的な考え方、公的個人認証サービスの

概要と、国や地方公共団体の手続きの対応状況などを整理するとともに、民間サービスにおける個人認証方法や、国内、海外のポータルにおける現状の認証方法などを整理し、官民連携ポータルにおける認証のあり方と課題について検討を行った。

また、実証実験において用いた方法とその理由、課題などもあわせて整理した。

なお、本検討会における議論の中で、官民連携ポータルについて、ビジネスモデルの点から、行政直営は適さないとの判断があった。そこで本章では、官民連携ポータルを民間事業者が運営することを想定して、個人認証に関する検討を行った。

また、認証技術やその利用については、急激に進歩、変化しており、今後とも適宜判断基準を見直す必要がある。

(2)現状

1)行政機関等に対する電子申請・手続き等における認証方法の例

電子申請・届出を行っている地方公共団体における認証方法の一例を下表に示す。厳格な本人確認が必要な手続き(住民票の写しの交付請求、市・県民税納税証明書の交付請求、固定資産評価証明書の交付請求など)では、公的個人認証サービス等を利用した電子署名が必要となっている。また、それほど厳密な本人確認を必要としない手続き(犬の登録変更届、犬の死亡届など)や、別途、本人確認の機会がある手続き(水道使用開始届、水道使用中止届など)、もともと本人確認の必要がない手続き(公文書公開請求など)については、システム利用上必要となるID/パスワードによる認証で可としている。

表4-1 地方公共団体における電子申請・届出等の認証方法の例

地方公共団体名	オンラインで可能な 手続きの数(合計)	電子署名が必要な 手続き数※	ID/パスワードに よる手続き数
岐阜県	153 件	109 件	44 件
大分県	101 件	81 件	20 件
岐阜市	32 件	24 件	8 件
大分市	31 件	27 件	4 件

※公的個人認証サービス(地方公共団体の認証局)、商業登記に基づく電子認証サービス(商業登記認証局)等による電子署名。

出所:各電子申請・届出サイトで確認(平成17年6月調査)

2) 行政機関等に対する手続きにおける電子署名の要否に関する基本的考え方

行政機関等に対する手続きについては、以下の理由から、一定の場合を除き、原則としてオンライン手続きにおいては、電子署名が必要と考えられる。

- ① オンライン手続きの課題である成りすまし、改ざん、送信否認の防止には PKI(公開鍵基盤)による電子署名が有効である(ID・パスワード方式はフィッシングやパスワード漏えいのリスクあり)。
- ② 手続きの多くに、保護すべき住民の個人情報・センシティブ情報が含まれる。
- ③ 電磁的記録の真正な成立の推定効を持つ電子署名には法的安定性あり(電子署名法第3条)。
- ④ 全国どこに住んでいる人も安い費用で利用可能な基盤(公的個人認証サービス)が整備済。
- ⑤ 手続きを提供する地方公共団体に対しても、電子署名への対応方式を提示済(共通仕様)。

ただし、以下の理由のいずれかに合致する手続きについては、相対的に必要性が低く、電子署名を要しないとすることも許容される。なお、これらの手続きであっても、将来的に他システムとの統合等の場合には、団体としての統一的な管理の必要上、電子署名が必要となる。

表4-2 電子署名を用いないことが許容される場合がある手続きの例

理由	手続き例
ア：性格上、本人確認の必要がない手続き	・ 行政公文書の開示請求
イ：別途利用時等に対面等で本人確認を行う手続き	<ul style="list-style-type: none"> ・ 職員採用試験受験申込み ・ 各種講座参加申込み ・ インキュベートルーム入居申込み ・ 青少年の家利用申込み ・ 親子でハイキング参加申込み ・ 手話通訳者派遣申込み ・ 保養施設利用券交付申請
ウ：重大な法律関係の変更等を伴わず、仮に成りすまし等が生じても権利関係の回復が容易な手続き	<ul style="list-style-type: none"> ・ 水道使用開始届 ・ 水道使用中止(廃止)届 ・ 犬の死亡届 ・ 犬の登録変更届 ・ 希望保育園変更・追加届 ・ 人材バンク登録申請 ・ 県政モニター応募 ・ 競争入札参加資格審査申請書

3) 公的個人認証サービスの概要

成りすまし、改ざん、送信否認などのデジタル社会の課題を解決しつつ、電子政府・電子自治体を実現するため、確かな本人確認ができる個人認証サービスを全国どこに住んでいる人に対しても安い費用で提供することを目的として、平成16年1月29日、公的個人認証サービスの提供が開始された。住民基本台帳カード等を用いて、各地方公共団体の窓口などで電子証明書の発行を受けられる。電子証明書の発行手数料は500円、有効期間は3年である。

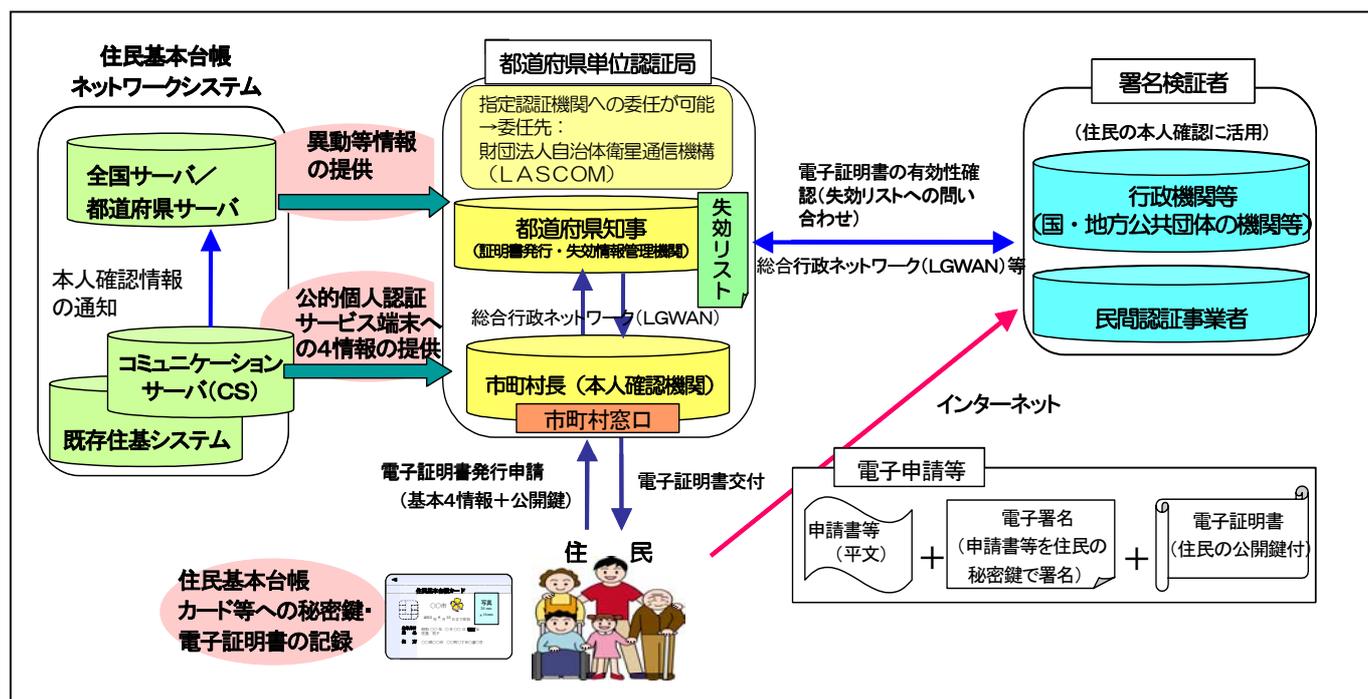


図4-1 公的個人認証サービスの概要

また、一定の要件を満たす民間認証事業者は、オンラインショッピング会社等からの電子証明書の有効性確認の請求に対応するため、公的個人認証サービス側に公開鍵証明書の有効性を確認することによりその失効等の事態（死亡、住所移転等）を把握し、失効リスト（CRL）を更新することができる。

公的個人認証サービスは、(ア)公開鍵暗号方式という高度な暗号技術に基づいて行われること、(イ)鍵ペアの作成が、利用者本人の操作によって市町村窓口の専用装置を用いて行われ、作成された鍵ペアは耐タンパ性を有するICカード(住基カード)に厳重に格納されるなど、公的個人認証サービスでは公開鍵暗号方式の鍵ペアを生成・格納する環境の信頼レベルが極めて高いこと、(ウ)住民基本台帳に登録された情報に基づき電子証明書が発行されるため、電子証明書の信頼性が非常に高いことなど、極めて安全性・信頼性の高い電

子認証サービスとして主にオンラインでの行政手続きにおいて活用されている。

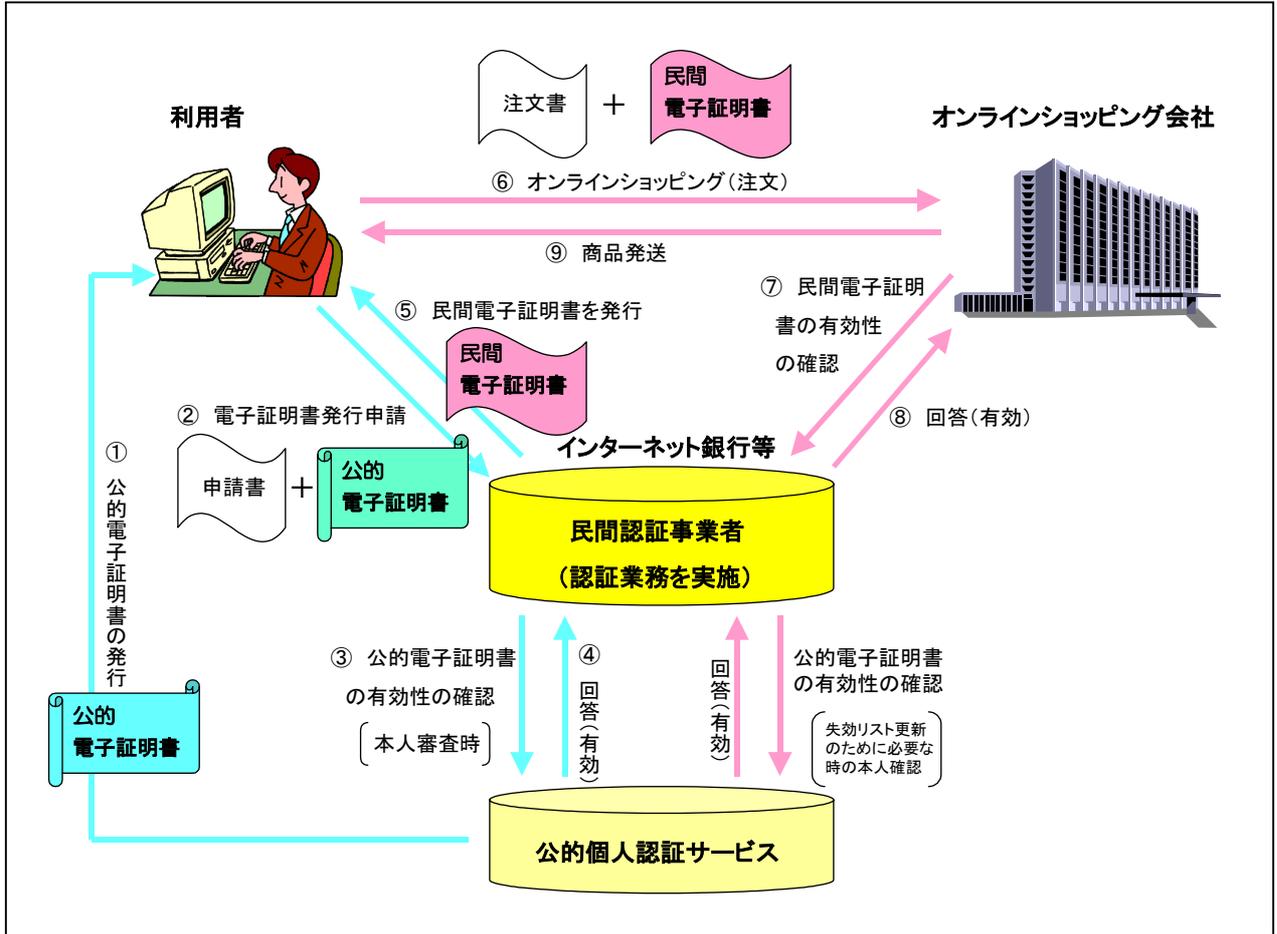


図4-2 民間認証事業者による公的個人認証サービスの利用イメージ

4) 公的個人認証サービスの普及に向けた取り組み

公的個人認証サービスの電子証明書発行件数は、平成 18 年 2 月末で 12 万 7 千枚余となっている。そこで、総務省では公的個人認証サービスの普及を促進するため、その利用範囲の拡大に取り組んでいる。

まずは、国や地方公共団体における公的個人認証に対応した電子申請の対象手続きの拡大である。平成 18 年 2 月現在、国の 11 府省庁、45 都道府県、24 都府県内の市町村(うち、全ての市町村が対応しているのは 4 県のみ)で公的個人認証に対応したシステムが整備されているが、IT新改革戦略では、全都道府県において 2008 年度までに、全市町村において 2010 年度までに公的個人認証サービスに対応した電子申請システムを整備するという目標が明記されている。

次に、公的個人認証サービスの電子証明書の有効性を確認できる者の範囲については、行政手続きを受ける行政機関等のほか、司法書士、行政書士など行政手続きの代理を行う者や公証人、医師など行政手続き等に必要な添付書類を発行する者が、連合会等の所属団体を通じて電子証明書の有効性を確認できるようにする法律の改正案を国会に提出しており、現在審議中となっている。

また、金融機関の口座開設時等における本人確認に公的個人認証サービスが利用できるよう、昨年 10 月に金融機関等本人確認法及び外国為替法の省令を改正したところである。

さらに、総務省の平成 18 年度地方行財政重点施策においては、電気、ガス、医療など公益的な分野へ利用範囲を拡大することを検討するとされており、個人情報保護に配慮しつつ、公的個人認証サービスの民間利用に向けた検討が始まっている。

加えて、こうした各種オンライン手続きにおける活用のほか、公的個人認証サービスの多面的な活用方法(電子ロッカー、電子錠、地域通貨システム、電子アンケートシステム、情報システムの職員認証(シングルサインオン)システム等)についても開発実証に取り組んでいる。

5) 民間サービスにおける認証方法の例

インターネットを用いた各種民間サービスでは、様々な認証方法が用いられている。下表はその一例である(比較のために公的個人認証など行政手続きも記載)が、認証のレベルについては、認証が厳格な順に、「第三者が認証する場合」「当事者間の認証」「当事者間の認証を行わない場合」の3つに大別できる。

第三者が認証する例としては、公的な認証基盤や民間の認証基盤の活用や、クレジットカードにおける与信照会などが挙げられる。これらは、ICカードとネットワークで、登録センターにいつでも認証を要求することができる仕組みである。また、クレジットカードなどでは、不審な購入実績については、個々に電話でカード保有者に確認するなどの手段を講じて、安全性を確保している。

当事者間で認証する例としては、予め登録した内容(ID、パスワード等)との照合による認証である。これは、初期登録したIDとパスワードで本人性を確認するものであり、スキミングやスパイウェア、フィッシングによってID、パスワードが盗まれた際には、なりすましによって被害にあう可能性がある。ID・パスワード方式については、一見簡便なように見えるが、特に複数ある場合に管理が困難になることや、最近はフィッシングやスパイウェアの脅威も増していることに留意が必要である。

一方、登録不要の掲示板への書き込みや、メールマガジンの受信においては、特に認証は行われぬ。この場合であっても、メールアドレスの登録を行うことが通常であり、利用料を必要とするプロバイダ発行のメールアドレスは有効であるが、利用料を必要としない匿名が可能なフリーメールでは申し込みを受け付けられないものも存在する。

また、ウェブ上での認証だけでなく、申請したメールアドレスへの送信や住所への郵送など、他の手段を組み合わせることにより本人確認性を高める工夫をしている例も多い。

表4-3 インターネットを用いた各種サービスの認証方法の例

認証レベル	事例	本人確認方法(例)
第三者による認証	公的な認証基盤を用いた行政手続き(電子申請)	住基カード等+電子証明書+パスワード
	民間の認証基盤を用いた行政手続き、民間手続き	電子証明書+パスワード
	クレジットカードを用いた支払い	カード番号+有効期限+与信照会(+本人への利用明細の送付)
当事者間の認証(初期登録内容との照合を行う)	ネット証券	認証方式(セキュリティコード方式、電子証明書方式)を利用者が選択できる。
	ネットバンキング	ID+生体認証・パスワード+第2パスワード
	会社のパソコンや社内ネットワークへのログイン	ICカード+生体認証・パスワード
	ネットオークション	ID+パスワード(+評判システム+エクスロー決済)
	パスワードを忘れた場合の再取得	予め設定した質問(ペットの名前など)への回答+メールアドレスへの通知
	掲示板への書き込み(登録、ログインが必要)	ID+パスワード+本名による発言+ログの保存など
当事者間の認証なし	掲示板への書き込み(登録、ログインが不要)	匿名、ログの保存
	メールマガジン	登録したメールアドレスへ送付

6) 官民連携ポータル事業者における認証

国内及び海外の官民連携ポータル事例における認証方法を下表に示す。

国内の 3 事例においては、ポータル側では住所、氏名などの入力を行い、これを申請受付事業者のサイトへ送る際に、それぞれの事業者が必要に応じた認証を行っているのが現状である。

また、I am moving.com の場合も、最初に氏名等を登録するが、ここで特に本人確認を行う訳ではなく(あくまでも自己申告)、個々の手続き先で本人確認を行っている。

表4-4 ポータル事例における認証方法の例

事例	認証方法
引越れんらく帳	<ul style="list-style-type: none"> ・連携事業者の個別ポリシーで実施
関西引越し手続きサービス	<ul style="list-style-type: none"> ・ポータル側での本人確認は無し ・引継ぎ先の各事業者サイト上での確認(方式は各事業者毎に行う)
札幌地区目的指向ポータルモデル(実験)	<ul style="list-style-type: none"> ・各手続きサイトの方法による ・北海道電力、水道局:電話受付と同様 ・北海道ガス、三ッ輪商会:受付後事業者から電話確認 ・札幌市:印刷した申請書を本人が窓口で提出
I am moving.com(英国)	<ul style="list-style-type: none"> ・最初に、氏名、電話番号、E メールアドレス、パスワードを登録する。以降は、E メールアドレスとパスワードにより自分のアカウントへのログインを行う。 ・団体によっては、顧客番号などの追加情報を入力する必要があり、これらの追加情報により認証を行っていると考えられる。 ・誤情報の送信は、Computer Misuse Act(1990)に抵触すると記載している。

出所:国内事例については各事業者へのアンケート調査による。海外事例については、ウェブ上の記載事項等をもとに作成。

(3)実証実験における個人認証方法と課題

1)ポータルにおける個人認証

今回の実証実験に参加した引越れんらく帳、関西引越し手続きサービスでは、ともにこれまでポータルでの個人認証は行っていなかったため、今回の実験でも、ポータルでの個人認証は行わず、すべて各手続きサイト側で確認が行われた。

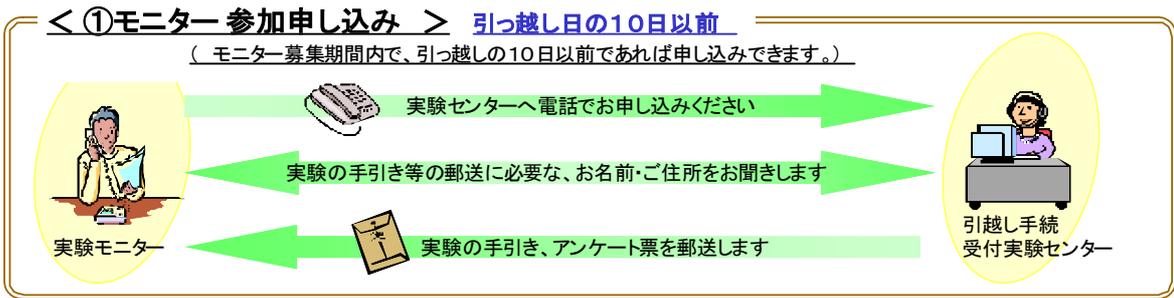
※引越れんらく帳では、30日間データを保持できる「マイれんらく帳」機能があるが、これは手続き途中などでデータを一時保存するためのものであり、手続き上の本人確認を行うものではない。

2)各手続き先における認証

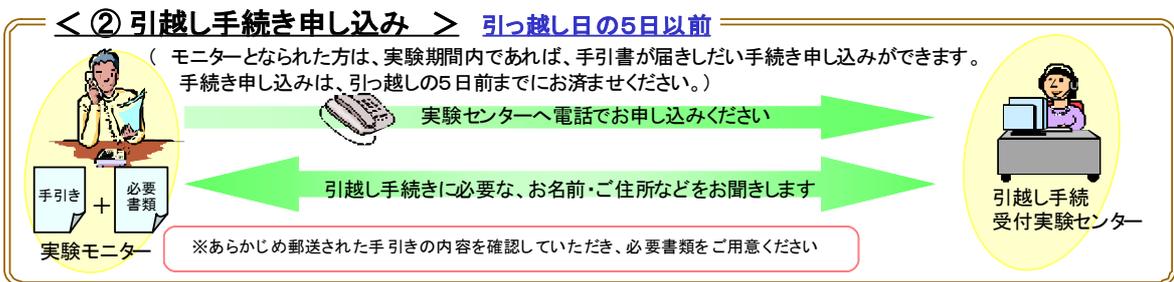
引越れんらく帳や関西引越し手続きサービスの提携先事業者は、従来どおりの方法でお客様の確認を行った。主な方法としては、お客様番号などの利用者固有の番号による確認(電力、水道など)や、加えてID、パスワードの登録、確認(クレジットカードなど)だが、引越し当日立会いなどが必要なため特にウェブ上での手続きでは特に本人確認は行わない(ガスなど)場合もある。

3)札幌官民連携引越しポータルにおける認証

札幌官民連携引越しポータルでは、あらかじめモニター登録した上で、実験センターのオペレータが利用者から電話で引越し手続きに必要な情報を聞き取り、ポータルへの登録、送信や、受付確認の連絡などを行った。



- ①の資料が届いたら、引越し予定日の5日前を目処に、実験センターのオペレータが実験モニターに電話し、引越し手続きに必要な情報を聞き取り、紙に記録。



- ②で記録した内容をもとに、実験センターのオペレータが札幌ポータルを用いて入力、送信。都市ガスについては、届出様式（必要事項記載済み）を印刷し、実験センターから事業者へFAXで送信（手動）。札幌市の届出については届出様式（必要事項記載済み）を実験センターから実験モニターへ郵送。
- 電気、水道については事業者からの受付通知電子メール、都市ガスについては事業者からの受付確認FAXをもとに、その旨を実験モニターに連絡。

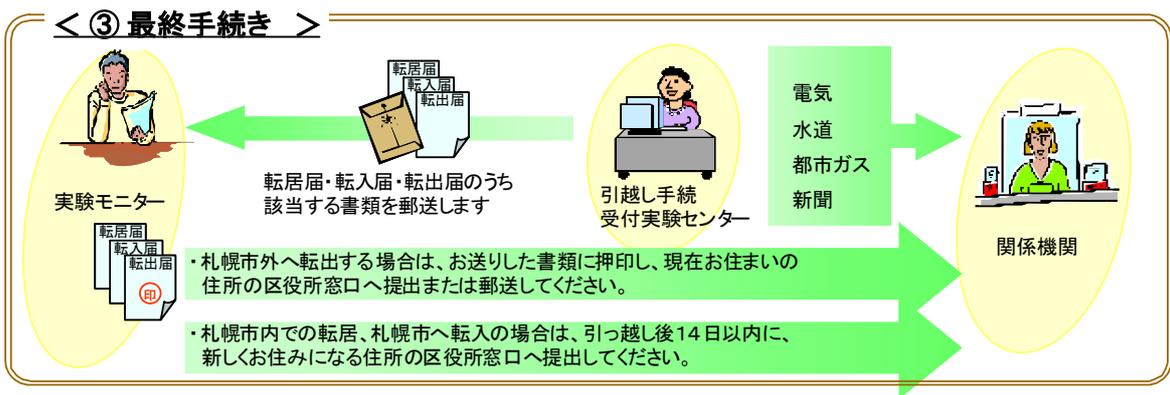


図4-3 札幌官民連携引越しポータルにおける手続きの流れ

(4)官民連携ポータルにおける個人認証のあり方

1)現状

現状の官民連携ポータルでは、以下のような個人認証方法が多く用いられている。

【民間手続き】

「引越れんらく帳」や「関西引越し手続きサービス」では、ポータル上で必要な手続きの選択と共通情報(氏名、現住所、電話番号、引越し先住所など)の入力を行い、以降の手続きは、各サイトで行う。従って、個人認証も、各サイトがそれぞれの方法で行う。

★認証方法:各サイトが定める認証方法(ID・パスワード、お客様番号など)

【行政手続き】

行政手続きについては、水道など一部を除きポータルとの連携は進んでいない。

★認証方法:各サイト(水道など)が定める認証方法(お客様番号など)

【利用者の主なメリット】

引越し時に必要な手続き(一部)を検索し、手続きサイトにアクセスできる。

どの手続きにも必要な共通情報の入力が一回で済む。

各手続きの進捗状況が確認できる。

【主な課題】

手続きの数が増えると、その分手間が増大する。

現状では、行政手続きはほとんど対応していない。

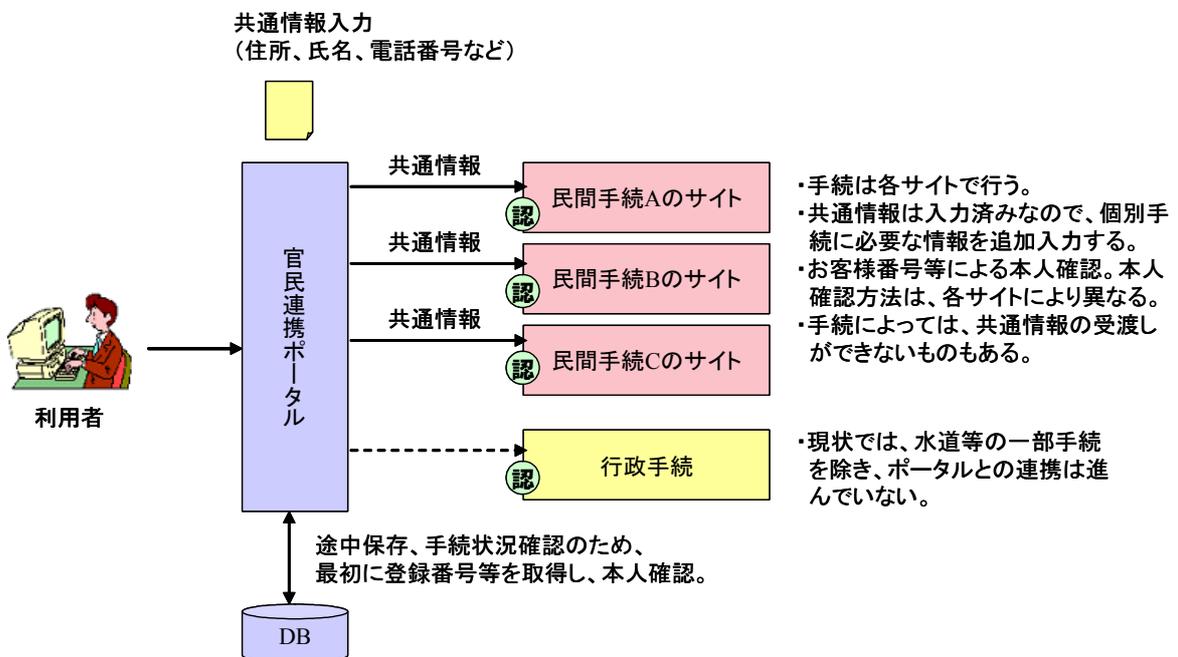


図4-4 官民連携ポータルの現状(引越ポータルの場合)

2) 今後の方向

①リンクによる連携と共通情報の受渡し(行政手続きへの拡大)

【民間手続き】

基本的には現状と同じで、ポータルでは必要な手続きサイトの検索、リンクと、共通情報の入力、受渡しのみを行い、本人確認を含む手続きは各サイトで個別に行う。現在、共通情報の受渡しが実現できていない民間手続きサイトにも拡大する。

★認証方法:各サイトが定める認証方法(ID・パスワード、お客様番号など)

【行政手続き】

ポータルにおける検索、リンク及び共通情報の受渡しを、行政手続きまで拡大する。本人確認を含む手続きは各サイトで個別に行う。

★認証方法:各サイトが定める本人確認方法(公的個人認証、ID・パスワードなど)

【利用者の主なメリット】

現状のメリットが、行政手続きまで拡大される。

【主な課題】

ポータルと各手続きサイト間で、共通情報の受渡しを行う場合には、特に手続きサイト側の対応(システム面での対応など)が必要となる。

行政手続きまで拡大するための、ポータルと各地方公共団体間の調整が必要。ポータルが全国約 2,000 の地方公共団体とそれぞれ個別に調整するのは物理的にも難しく、共同アウトソーシング等の形で調整先を統合することが望まれる。

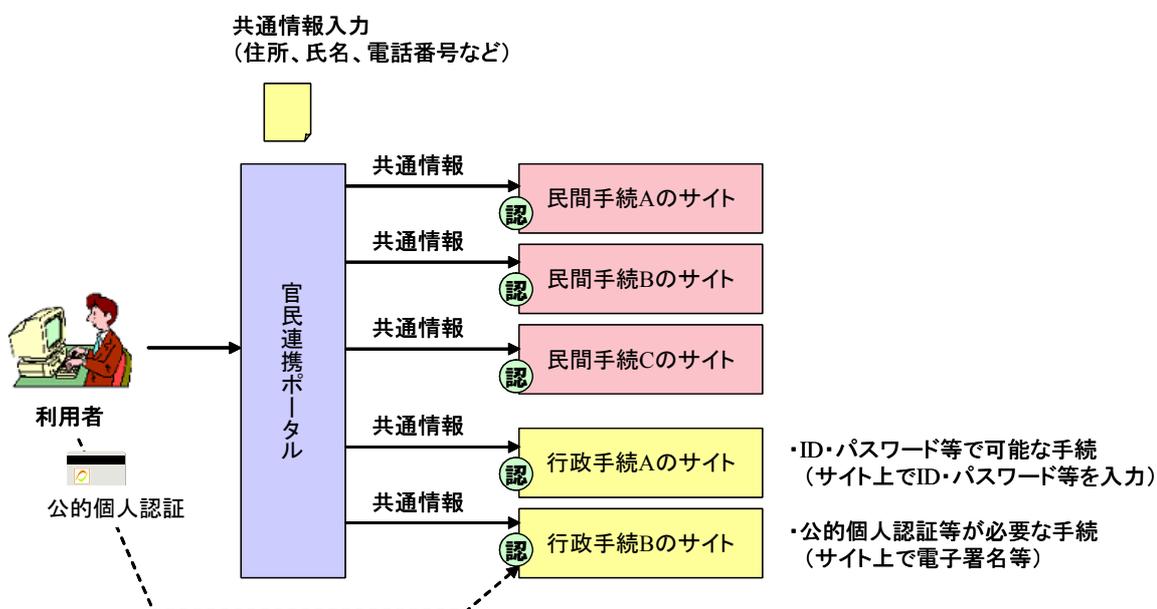


図4-5 行政手続きへの拡大

②官民それぞれを出来るかぎりワンストップ化

【民間手続き】

民間手続きにおいては、個別情報もポータル上で入力し、一括手続を可能にする。

一部の手続きについては、ポータルでのシングルサインオンを実現(各手続での認証を不要に)。ポータルのシングルサインオン以外の認証方法を用いる場合は、各サイト上で認証を行う。

★認証方法:

- ・ポータルおよびポータルの認証を用いるサイト:シングルサインオン(ID・パスワードなど)
- ・各サイト:各サイトが定める認証方法(ID・パスワード、お客様番号など)

【行政手続き】

行政手続に関しては、行政ポータル上でのワンストップ化を図る。行政ポータルとしては、各地方公共団体のサイトや共同アウトソーシングサイトなどが考えられる。

官民連携ポータルから、共通情報を受け取ることで、入力の手間を省く。

手続きに必要な個別情報などを行政ポータル上で一括して入力。

各手続きに必要な認証について、ポータル上で一括して行う。同一地方公共団体サイト内や共同アウトソーシングサイトなど、同一システム上での運用の場合、シングルサインオンなどに対応しやすい。

★認証方法:

- ・ポータルおよびポータルの認証を用いるサイト:シングルサインオン(ID・パスワードなど)
- ・電子証明書等が必要なサイト:ワンクリックで必要な数だけ電子署名、電子証明書の添付を可能にする。
- ・その他のサイト:各サイトが定める認証方法(ID・パスワードなど)

【利用者の主なメリット】

ワンストップではなく民間手続きと行政手続きのツーストップになるが、現状よりは大幅に利便性が高まる。

【主な課題】

民間手続きにおける個別情報入力も含めたワンストップ化、シングルサインオンおよび、行政手続きポータルの実現が必要となる。

ポータルが ID・パスワードなどを用いてシングルサインオンを実現する場合、ID・パスワードなどを発行・管理する業務が生じるほか、シングルサインオンを利用する手続き先のサイトに対しても、ポータルとして保証する必要がある。ポータル側が厳格な管理を行わないと、信用が得られず、シングルサインが実現しない。この負担は、ポータルのビジネスモデルの成立を考える上でも課題となる。対応策としては、既に ID・パスワードを発行している主体(プロバイダー、ネットショッピングサイト、会員向けサービスサイトなど)がポータルを運営したり、外部の認証(公的個人認証や民間認証など)を用いることが考えられる。

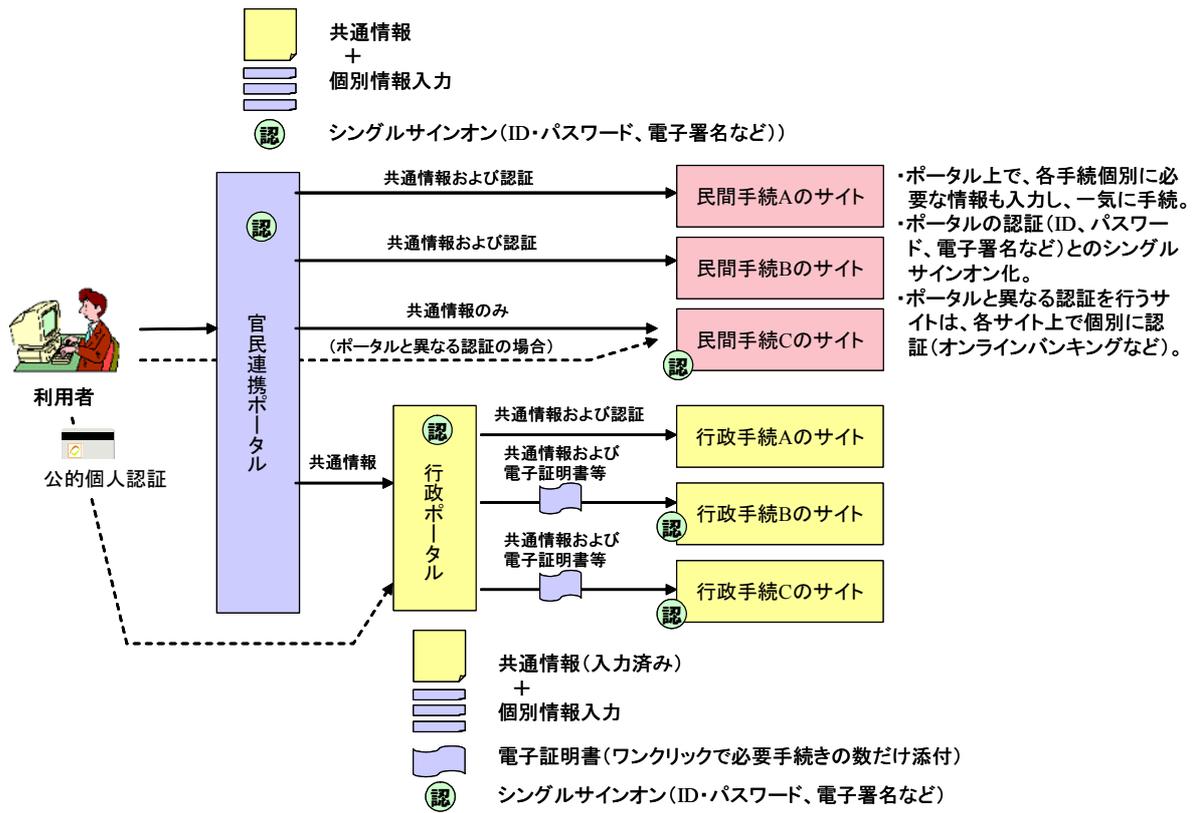


図4-6 官民それぞれを出来るかぎりワンストップ化

③ワンストップ化

【民間手続き】

ポータル上で、各手続き個別に必要な情報も入力し、一度で手続きを完了する。

ポータルと各手続きのシングルサインオンを実現。

電子証明書等もワンクリックで必要な数だけ添付。民間でも活用。

ポータルと異なる認証を行うサイトは、各サイト上で個別に認証を行う(オンラインバンキングなど)。

★認証方法:

- ・ポータルおよびポータルの認証を用いるサイト:シングルサインオン(ID・パスワードなど)
- ・電子証明書等が必要なサイト:ワンクリックで必要な数だけ電子署名、電子証明書の添付を可能にする。
- ・その他のサイト:各サイトが定める認証方法(ID・パスワードなど)

【行政手続き】

ポータル上で、各手続き個別に必要な情報も入力し、一度で手続きを完了する。

ポータルと各手続きのシングルサインオンを実現。

電子証明書等もワンクリックで必要な数だけ添付。

ポータルと異なる認証を行うサイトは、各サイト上で個別に認証を行う。

★認証方法:

- ・ポータルおよびポータルの認証を用いるサイト:シングルサインオン(ID・パスワードなど)
- ・電子証明書等が必要なサイト:ワンクリックで必要な数だけ電子署名、電子証明書の添付を可能にする。
- ・その他のサイト:各サイトが定める認証方法(ID・パスワードなど)

【利用者の主なメリット】

ほぼワンストップで、民間手続き、行政手続きをあわせた必要手続きを行うことができる。

【主な課題】

行政手続きにおいて公的個人認証サービスを用いる場合は、官民連携ポータルで失効リストの確認を可能にするなど、現行法制度(公的個人認証法)の改定が必要となる。

②の場合は、行政ポータルと各行政手続きサイトが、同一地方公共団体内、あるいは共同アウトソーシングによる同一システム内であるため、システム間連携(複数手続きのワンストップ化やシングルサインオンなど)を比較的行い易いが、官民連携ポータル(民間事業者が運営)と各行政手続きサイト(地方公共団体が運営)に分かれると、対応が難しくなる。

民間手続きにおいて公的個人認証サービスを用いる場合は、上記に加え、民間手続きサイトで失効リストの確認を可能にするなど、現行法制度(公的個人認証法)の改定が必要となる。官民連携ポータル事業者などが発行する民間電子証明書を用いる場合は必ずしも制度を改正する必要はない。ただし、民間事業者が電子証明書を発行する場合の本人確認に公的個人認証サービスを利用する場合、現行制度では、認定認証事業者等しか利用を認められておらず、他の民間事業者が利用するためには、制度改正が必要であ

る。

また、②同様、シングルサインオンのために、ポータルで ID・パスワードなどの発行、管理を行う場合は、その負荷が生じる。

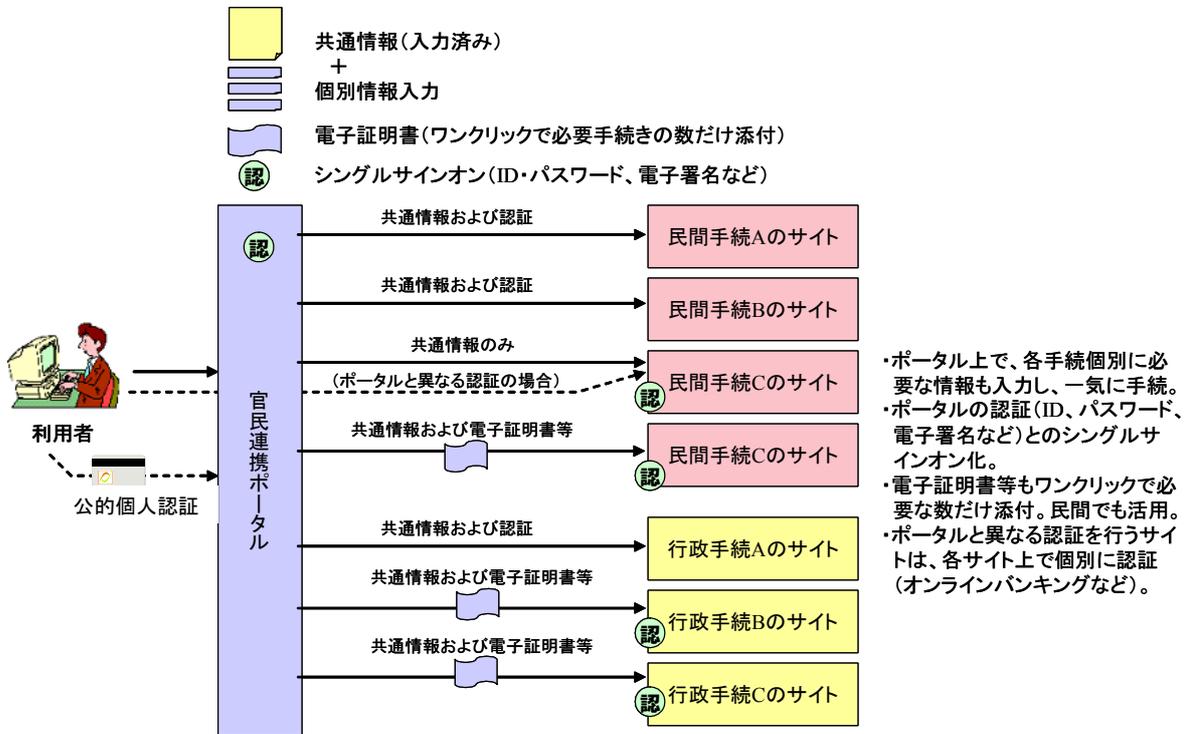


図4-7 ワンストップ化

3) 個人認証の課題のまとめ

①システム面の課題

手続き数が多くなるほど、個人認証を個別に行うのではなく、信頼性の高い認証方法でワンストップで行うことができるほうが、利用者の利便性は高い。公的個人認証サービスを用いて、個人認証をワンストップ化できれば、認証の手間は大幅に軽減されるが、公的個人認証サービスの普及や、民間などへの活用範囲の拡大など、解決すべき課題もある。

また、現在の行政機関の電子申請・届出や民間企業の電子的な手続きは、利用者本人による利用を想定しており、個人認証についても、利用者本人が直接手続きを行うこと(あるいは代理人による手続き)を前提としている。従って、ポータル事業者が個人認証を一括して行うことは、現在の仕組み上は難しい面が多い。

手続きの際の個人認証をワンストップ化するためには、

- 1) 電子署名やID・パスワードなどによる個人認証のシングルサインオン化
- 2) 各申請手続き受付事業者への電子証明書送付などの個人認証の手順をポータル上で自動化

等の方策が考えられるが、現状では、各申請手続き受付事業者は個別にそれぞれの方法で個人認証しており、このような共通での個人認証や自動化対応などを想定していない。対応には、ポータル経由での受付を想定したシステム構築(※)や、制度の整備が必要となる。

また、個人認証に限らず、ポータル事業者が申請手続き受付事業者と交渉する際、行政手続きについては、現状では 2,000 以上の個別地方公共団体との調整が必要となる。これは現実的には困難であり、例えば都道府県単位で共同アウトソーシング化により、47 箇所との調整で済むなどの対応が求められる。

(※)このようなシステムの基盤構築の一環として、全国地域情報化推進協議会によりウェブサービスを基礎としたサービス連携基盤仕様「地域情報プラットフォーム」の標準化活動が進められており、またそれに必要な技術開発が(独)情報通信研究機構により行われている。

【現行】



【ワンストップ化】



※ ポータル経由での受付を想定したシステム構築、制度づくりが必要

図4-8 個人認証の課題

②制度面の課題

前述のように、公的個人認証サービスなどの、安全性・信頼性の高い電子認証（電子署名・電子証明書）を積極的に活用し、国民の権利義務や財産に大きな影響を及ぼす手続きの電子化や、手続きにおける個人認証のワンストップ化を進めていく方向が望ましいと考えられるが、民間手続きにおいて、公的個人認証サービスの利用を可能とするためには、制度改革が必要である。

官民の各種手続きのワンストップ化を実現するため、個人情報保護に配慮しつつ、官民ポータルの主要な受付事業者となることが想定される公益事業者を中心に、公的個人認証サービスの利用範囲の拡大について検討することが適当と考えられる。