

電子政府推進対応ワーキンググループ
報告書（案）

平成 22 年 10 月

電子政府推進対応ワーキンググループ

目 次

第1章 電子政府推進対応ワーキンググループのスコープ	
1. 電子政府推進対応ワーキンググループの位置づけ	1
2. 本ワーキンググループにおける検討の視点	1
(1) 電子行政サービスの利用率の向上	2
(2) 行政システム上の情報の利活用の促進	3
3. 本ワーキンググループの検討スコープ	3
第2章 国民本位の電子行政の実現に向けた方策	
1. 民間IDの利活用	5
2. 公的な認証手段の利活用	6
3. 魅力ある電子行政サービスの拡大	6
第3章 本ワーキンググループにおける議論の内容	
1. 民間IDの利活用	8
(1) 既存IDのクレデンシャルの有効活用	8
(2) ID・クレデンシャルの安全性・信頼性を測る共通の基準について	10
(3) 電子行政サービスとID・クレデンシャルとの保証レベルを媒介とする対応関係の明確化について	11
(4) 民間IDの認定制度（信頼フレームワーク）の確立	12
(5) その他	15
2. 公的な認証手段の利活用	18
(1) 認証用途の付加	19
(2) 記録媒体の拡張	20
(3) その他	20
3. 魅力ある電子行政サービスの拡大	21
第4章 今後の進め方	
1. 検討経緯と基本的な考え方	23
2. 提案されたユースケース	24
(1) 市民協働ポータルサイト	24
(2) 官民連携プラットフォーム	26

第1章 電子政府推進対応ワーキンググループのスコープ

1. 電子政府推進対応ワーキンググループの位置づけ

高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）の「新たな情報通信技術戦略」（平成22年5月11日）において、「国民本位の電子行政の実現」は戦略の重要な柱として位置付けられている。そして、こうした電子行政の共通基盤とされたのが国民ID制度であり、個人情報保護を確保し、府省・地方自治体間のデータ連携を可能とする電子行政の共通基盤として、社会保障・税の共通番号の検討と整合性を図りつつ、2013年までの導入を目指すこととされている。併せて、インターネットを通じて利便性の高いサービスを提供するため、民間IDとの連携可能性を検討することとされている。

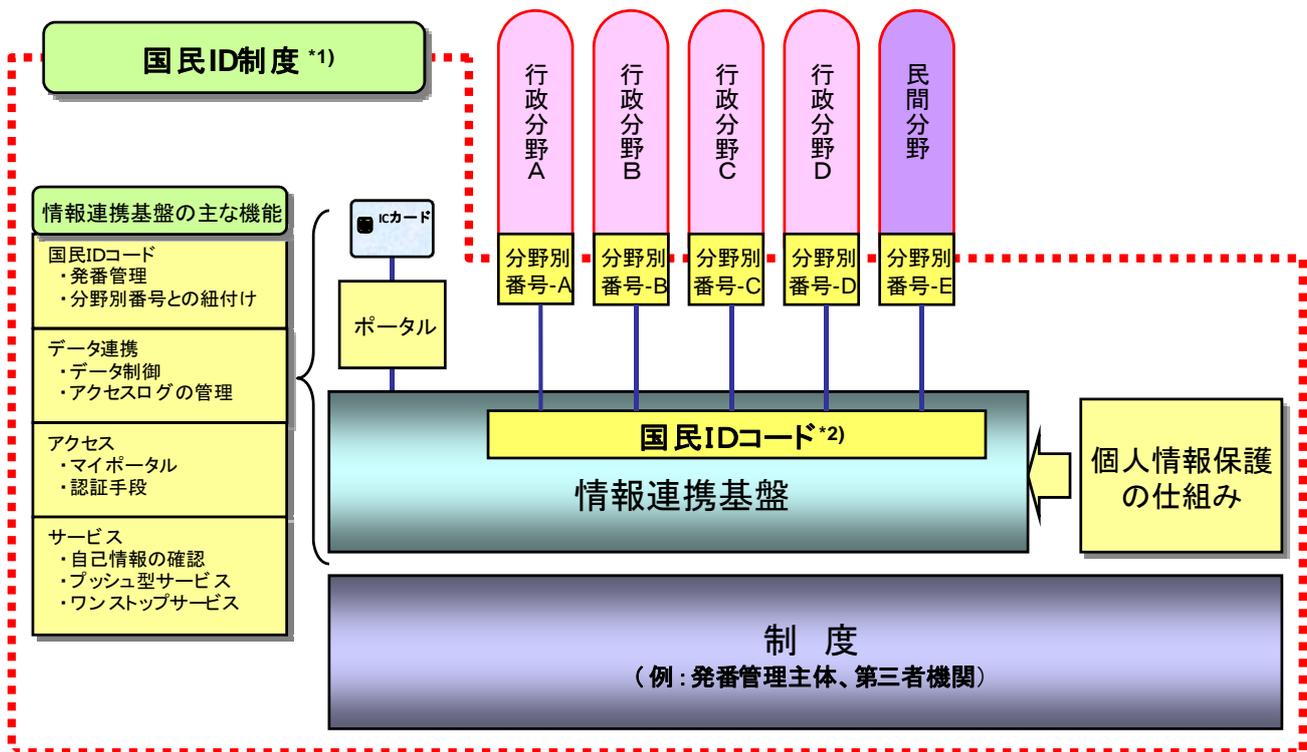
また、「新たな情報通信技術戦略 工程表」（平成22年6月22日）において、総務省は、上記の目標を実現するための2010年・2011年の短期の取組みとして、行政業務システムと民間事業者との連携に係る実証実験等を実施することとされたところである。

総務省においては、グローバル時代におけるICTに関するタスクフォースの地球的課題検討部会において、ICTの利活用を促進するための諸方策が検討されてきた。電子政府については、国民本位の電子行政の実現に向け、具体的な検討課題やアクションプランの明確化の必要性が指摘され、その検討の途上で、こうしたサービス利用で想定される番号の考え方について、総務省から原則が示され、この4月には、上記部会に「電子政府推進対応ワーキンググループ」が設置された。

本ワーキンググループにおいては、政府の新たな情報通信技術戦略において総務省の役割とされた事項の具体化等を図るなど、国民本位の電子政府・電子自治体の実現に向け、検討課題やアクションプランの明確化を行うこととされ、設置以降10回の会合を重ねて、検討を進めてきたところである。

2. 本ワーキンググループにおける検討の視点

新たな情報通信技術戦略に掲げられた国民ID制度は、新たな情報通信技術戦略が目標として掲げる国民本位の電子行政の実現に向けて、利用者目線という視点から国民の要望に応じていくための制度である。これを実現していくためには、国民IDコードを活用し、各分野で個別に管理される個人情報について、国民が自らアクセスして、自ら容易に確認できるようにするとともに、分野間で効率的な情報連携を可能とするような情報連携基盤を整備していくことが必要となる。（参考までに、内閣官房情報通信技術（IT）担当室が「電子行政に関するタスクフォース」に提出した国民ID制度のイメージを以下に示す。）



*1) 国民ID制度： 国民IDコードを活用し、個人情報保護を確保しつつ、各分野間（行政機関間等）でデータ連携を可能とする情報連携基盤と制度。

*2) 国民IDコード： 個人を一意に識別するための数字や文字列。

図1 国民ID制度のイメージ図

出典：「電子行政に関するタスクフォースにおける検討課題 説明資料」（内閣官房 情報通信技術（IT）担当室）〔第1回電子行政に関するタスクフォース（平成22年9月15日）資料〕

新たな情報通信技術戦略で示された国民本位の電子行政の実現に向けて議論を行った結果、本ワーキンググループにおいては、以下の二つの観点から検討を行う必要がある、というコンセンサスが得られている。

第一は、より多くの国民が電子行政サービスにアクセスし、利用電子行政サービスの利用率を高めていくためには、どのような課題の解決が必要か、という観点である。

第二は、行政システム上で保有されている情報について、組織や業務の壁を越えた共有、利活用を促進していくためには、どのような課題の解決が必要か、という観点である。

（1）電子行政サービスの利用率の向上

現在、電子行政の多くの手続きで採用されているアクセス手段としては、公的個人認証サービスにおける電子証明書によるもの（平成21年度末現在、その発行枚数の累計は、約146万枚）、ID／パスワードによるものが挙げられる。

電子行政サービスの利用率の向上を図っていくためには、このような、電子行政サービス

へのアクセス時(ログイン認証時)に用いられる情報(以下、クレデンシャルという。例としては、パスワードや電子証明書があげられる。)の発行、配布、利用のプロセスについて、更なる向上を図るための具体策を検討するとともに、国民の利用を促す魅力的なサービスの提供についても検討していく必要があるのではないか、と考えられる。

(2) 行政システム上の情報の利活用の促進

電子行政サービスを国民への訴求力の強いものにしていくためには、「国民が便利を実感できる」という行政サービスの原点に立ち返った検討が期待される場所である。こうした観点から、組織間・業務間での情報共同利用を進めるための具体策を明確化して、行政手続きに際しての国民利用者の負担軽減を図ることは、本ワーキンググループにおいても重要な検討課題であると考えられる。

上記の点については、既に内閣官房の「社会保障・税に関わる番号制度に関する検討会」やIT戦略本部の「電子行政に関するタスクフォース」において検討、議論が進められており、ここでの議論との矛盾、重複をさけて検討を進めていくことが必要となる。

3. 本ワーキンググループの検討スコープ

本ワーキンググループにて、その重要性が確認された検討の視点は以上のとおりであり、今回の検討においては、国民が多様な電子行政サービスにアクセスするためのアクセス手段の在り方を検討するとともに、「国民が便利を実感できる、魅力あるサービスの実現」という課題が、電子行政の議論の原点であることにかんがみ、行政システム上の情報の利活用の促進についても適時検討の俎上にあげ、議論することとされたところである。

今回のスコープを上記のような範囲とすることの理由に関連して、下記のような指摘が行われたところである。

- 電子行政サービスに対するアクセスの問題、行政機関間、官民の組織間の情報の共同利用の問題については、いずれも、国民が便利を実感できる、魅力ある電子政府を実現していく上で車の両輪となる重要な検討課題であり、本ワーキングにおいても、そうした観点に立って議論を進めていくべきではないか。
- 行政組織間・業務間での情報の共同利用を推進するにあたって、その前段階において、電子行政に対するアクセス手段に係る課題、すなわち、クレデンシャルや認証に係る課題をクリアすることが必要となるのではないか。
- 上記2.(2)の観点の議論については、既に内閣官房の「社会保障・税に関わる番号制度に関する検討会」において検討されており、可能な限り、ここでの議論との整合性をとるよう工夫していくべきではないか。

- 電子行政サービスの利用率を向上させるためには、既存のクレデンシャルの発行、配布プロセスに関わる国民の負担が重く、クレデンシャルが普及に結びついていないことを、最も重要な問題点として認識することが重要ではないか。
- クレデンシャルや認証に関わる課題と、組織間・業務間での情報の共同利用に関わる課題は、下図に示すとおり、「縦の議論」と「横の議論」として明確に分けて論ずべきものであり、本ワーキングの議論においては、「縦の議論」を行うべきではないか。

なお、本ワーキンググループの議論の対象である、縦の議論及び横の議論の相互の関係性に係る図が提出されたため、以下に掲げることとする。

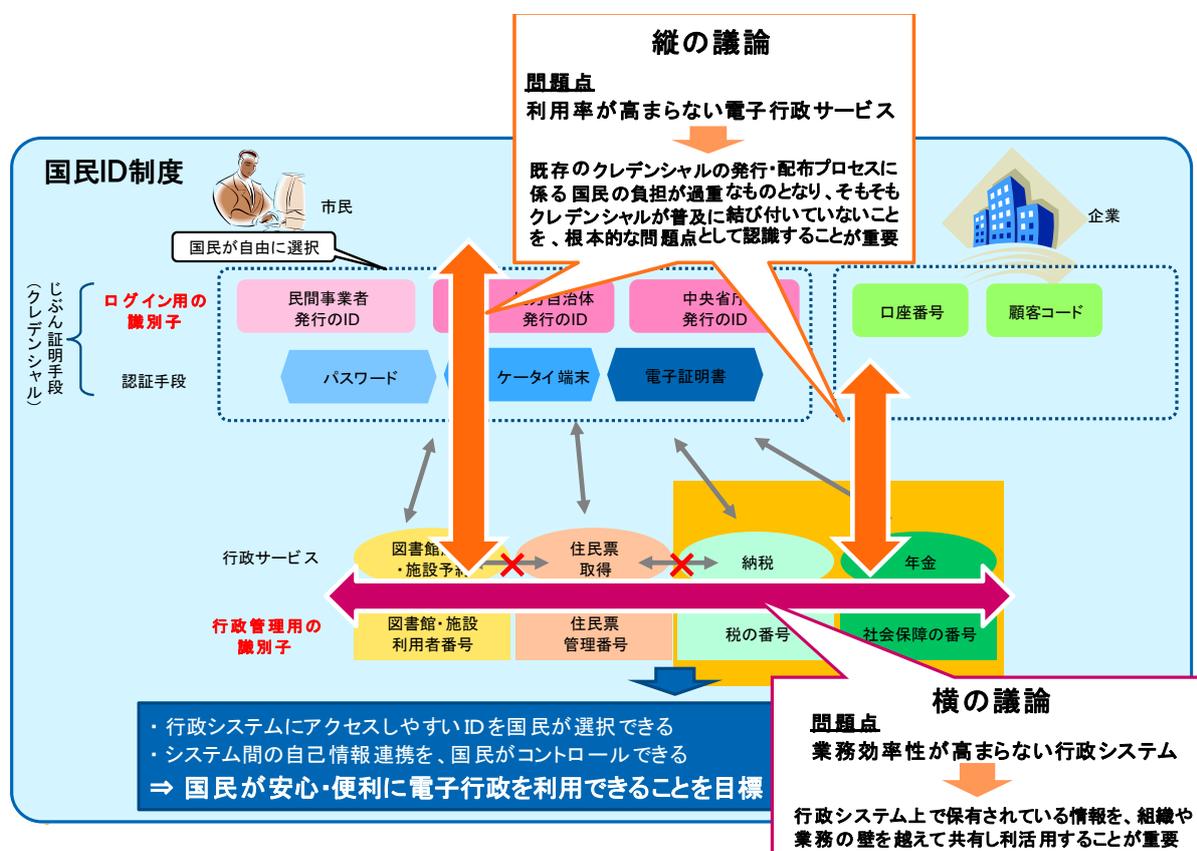


図2 電子政府・電子自治体が抱える2つの構造的な問題
(村上構成員提出資料)

第2章 国民本位の電子行政の実現に向けた方策

前述の通り、前章2.(2)の観点についての議論については、既に内閣官房の「社会保障・税に関わる番号制度に関する検討会」やIT戦略本部の「電子行政に関するタスクフォース」において検討が進められていることから、今回の検討は国民が多様な電子行政サービスにアクセスするためのアクセス手段の在り方を中心に行うこととする。

上記の「アクセス手段の在り方」という観点から、本ワーキンググループにてこれまで提案され、議論された具体策を整理すると、概ね以下の3点に集約できるのではないかと考えられる。

1. 民間IDの利活用
2. 公的個人認証サービスの利用拡大
3. 魅力ある電子行政サービスの提供

以下、順にそれぞれの意見の概要を記載する

1. 民間IDの利活用

電子行政サービスの拡大に当たっては、「安全」、「確実」、「低コスト」といった国民の要請を満たしつつ、仕組みが設計・運用されることが重要となる。民間IDの利活用は、こうした仕組みの導入によって、府省・地方自治体間の情報連携やその時に求められる国民本人の監視・コントロールによる自己に関する情報の活用の仕組みが整備されたときに、その仕組みを国民が利用する際の認証手段の一つとして、民間IDを含む認定されたIDを位置付けるものである。

民間IDの利活用については、電子行政サービスへのアクセス容易性の向上に係る課題に対し、国民がよく使っている既存の民間事業者発行のIDを用いて認証できるようにすることが有効ではないかとの指摘があった一方、そもそもその発行・提供主体が多種多様であり、身元確認の方法も個別に選択されており、その安全性・信頼性について様々な課題が指摘され得ることから、後に示すように、IDの信用力の担保を目的とした認定制度の確立が検討課題の一つとして指摘されている。その際、こうしたスキームについては、民間事業者の意向を踏まえ、国や地方公共団体の関与を最小限にとどめ、発行・提供主体自らの主体性と責任に基づき、信用力のある自らのIDを提供していく仕組みの整備が必要ではないか、との指摘も見られたところである。

また、こうした民間ID等によって利用可能な電子行政サービスの範囲については、カバーされる認証レベルの範囲をより高いレベルまで広げようとする、認定制度においてより厳格な基準での認定・監査を受ける必要があり、そこにはコスト（初期コスト、維持・運用コスト）も影響してくることから、後に示すように、発行・提供主体において、カバーする

手続きの範囲とコストや認定制度への参画のインセンティブの間の相互の適正なバランスの可否が、重要な検討課題として指摘されている。

2. 公的な認証手段の利活用

公的な認証手段、特に公的個人認証サービスについては、政府内でのこれまでの議論においても、今後、速やかで自律的な普及を促し、様々なオンライン手続等の認証基盤として発展・定着を図っていくことが目標とされ、目標実現のために、利用サービスの拡大、利便性の向上、行政分野における更なる利用促進等を図ることが課題とされている。

既に総務省においては、平成 21 年 8 月 12 日に公表された「公的個人認証サービス普及拡大検討会 中間取りまとめ」において、①認証用途の付加、②記録媒体の拡大、③オンライン更新、④有効期間の延長、⑤署名検証者の拡大（民間事業者への拡大）、⑥利用用途の拡大（署名メール及び暗号メール）といった 6 つの普及拡大方策が提言されている。

また、IT 戦略本部の「新たな情報通信技術戦略」においては、「公的個人認証サービスの利便性向上・用途拡大のための検討を 2010 年度中に行い、検討結果に基づく改善を速やかに行う」こととされている。さらに、「新たな情報通信技術戦略 工程表」において、こうした利便性向上等を目的とした施策は、同戦略が掲げる「国民 ID 制度の導入と国民による行政監視の仕組みの整備」と連携しながら推進することとされている。

後にも示すように、今回のワーキンググループの検討においては、現行の公的個人認証サービスについて、先の中間とりまとめで示されたような方策の具体化の検討を進め、認証手段として国民に対し普及浸透を図っていくためには、以下のような視点も加味しつつ、指摘された課題への適切な改善・解決策を図っていくことも必要ではないか、との指摘もあったところである。

- (ア) 費用対効果の検証（これを実現するためにいくら費用がかかり、どれだけの利便性の改善や利用者視点に立った成果を見込まれるか）
- (イ) 対応の優先順位付け（普及率向上等のために優先的に解決すべき課題を明確化）

3. 魅力ある電子行政サービスの拡大

本ワーキンググループの議論では、既に示した民間 ID の利活用及び公的な認証手段の利活用の共通の前提として、魅力ある電子行政サービスの必要性が再三指摘されたところである。例えば、以下のような指摘があった。

- 電子行政サービスにアクセスする際の事前準備として、多様な機関から添付書類を取り寄せ、準備する必要がある場合がある。添付書類が要求される場合があると、

- ・ オンラインによる提出のために電子ファイル化すること
- ・ 複数の機関から添付書類を取り寄せる際に、それぞれの窓口で直接出向いて個別に申請を行う必要があること

など、利用者の多大な負担となることが想定される。

- 官民連携による情報の共同利用の推進によって、官民の業務の効率化にのみならず、こうした国民による添付書類の取寄せ、提出の省力化にも大きく寄与することが期待できるのではないか。これは実現した時の効果も明確であり、電子行政サービスへのアクセスを検討する前提として、こうした魅力的なサービスの在り方、実現方法についても検討する必要があるのではないか。
- 電子行政サービスの利便性の高さを国民・民間事業者に広く周知する広報活動も重要であり、また、利用者にあわせた効果的な電子行政サービスの情報の提供、電子行政サービスの利用に際する魅力的なインセンティブの付与といった方策も有効ではないか。

第3章 本ワーキンググループにおける議論の内容

以下では、前章にて整理された3つの具体策について、本ワーキンググループで指摘された課題等を示すこととする。

1. 民間IDの利活用

標記の具体策の概要については、第2章に示したとおりである。

さらに、本施策について、本ワーキンググループの議論の過程で指摘された検討課題については、概ね以下の4点に整理できると考えられる。以下、課題ごとに、主な意見の概略を記載することとする。

- (1) 既存IDのクレデンシャルの有効活用
- (2) ID・クレデンシャルの安全性・信頼性を測る共通の基準について
- (3) 電子行政サービスとID・クレデンシャルとの保証レベルを媒介とする対応関係の明確化について
- (4) 民間IDの認定制度（信頼フレームワーク）の確立

(1) 既存IDのクレデンシャルの有効活用

標記については、電子行政サービスへのアクセス向上における課題として、ログイン認証に必要な情報、いわゆるクレデンシャル（例 パスワード、電子証明書など）の発行・配布・利用プロセスに係る手続きが煩瑣であることが考えられることから、それらを補完する選択肢として、国民が普段よく使っている既存の民間事業者発行のIDを用いて認証できるようにすることが有効ではないか、との指摘があった。この点については、更に次のような指摘があった。

- 現状では、多くのオンライン手続きで採用されているクレデンシャルは、公的個人認証サービスの電子証明書であり、その発行枚数（発行累計）は、平成21年度末現在、約146万枚であり、その普及は我が国全国民（平成21年度末現在、約1億2,708万人）の1%程度である。（なお、上記の指摘に関しては、参考資料として、クレデンシャルの普及率を海外比較した下記表1が提出された。これは、「電子政府ガイドライン作成検討会 セキュリティ分科会報告書」等を基に作成したものとして提出されたもので、表の中で、「人口普及率」とは、「人口に占める、発行枚数の割合」を意味するものとされ、「韓国」の欄の「半強制」の趣旨については、韓国では民間サービス（インターネットバンキング、オンライントレード、10万ウォン以上のインターネットショッピング）の利用において、公認認証書の使用を強制していることを表した、とされたところである。）

	エストニア	ベルギー	韓国	オーストリア	デンマーク	スウェーデン	フィンランド	日本
人口(万人)	約134万人	約1,058万人	約4,846万人	約823万人	約551万人	約918万人	約532万人	約1億2,715万人
発行枚数(年)	約105万枚 (2009)	約850万枚 (2008)	約1,790万枚 (2008)	約10万枚 (2007)	約134万枚 (2009)	約230万枚 (2009)	約24万枚 (2009)	約146万枚 (2009)
人口普及率 *注1	約80%	約80%	約37%	約1%	約24%	約26%	約5%	約1%
証明書の取得	義務 (15歳以上)	義務 (12歳以上)	任意 (半強制*注2)	任意	任意	任意	任意	任意
発行機関	民間	行政、民間	民間	行政	民間	民間	行政、民間	行政
導入年	2002年	2003年	1999年	2004年	2003年	2002年	1999年	2004年
証明書	ICカード、(SIM カード?)	ICカード	ICカード、その他 ハードウェア、ソ フトウェア証明書	ICカード、ハード ウェア証明書	ソフトウェア証明 書	ハードウェア・ソ フトウェア証明書	ICカード、SIM カード	ICカード
格納場所								
発行方法	対面	対面	対面	対面	対面不要	ハードウェア証 明書の場合、対 面	対面	対面
電子証明書	署名・認証 各1枚	署名・認証 各1枚	署名・認証兼用	署名用2枚	署名・認証兼用	署名・認証 各1枚	署名・認証 各1枚	署名用1枚

表1 海外電子政府比較

- 電子政府先進国と言われる韓国においても、公認認証書の保有を国民に半強制とするといった条件の下でも、9年間で人口普及率37%までしか普及しなかった。電子行政サービスの認証手段について、国民に対する強制発行・配布ではなく、国民の任意取得に委ねる場合には、十分な普及が期待できないのではないかと。
- それに対して、一般に広く使われている既存の民間IDのクレデンシャルを活用すれば、電子行政サービスの利用時の認証における利用者負担を引下げ、短期間でアクセスの容易性を上げ、電子行政サービスの利用を促進する効果を生み出す。加えて、新たなクレデンシャルの発行・配布を不要とする予算節約の効果もある。

また、これらの指摘に対して、以下のような意見があった。

- 公的個人認証が人口比で「1%程度にしか普及していない」との意見があるが、そもそも利用率100%を目指すことは困難であり、数値を示すのであれば、もともとオンライン手続きが必要な対象や頻度も示すべきではないかと。
- 利用率が高まらない論点としては電子行政サービスへのアクセスの観点から説明されてきたが、利用率が高まらない主因としては、「国民ニーズに合致した魅力的な電子行政サービスが提供されていない。」「電子行政サービスの利用に係る広報の不足。」「国民生活や意識の変化に対応した新たなサービス開発に向けた取り組み不足。」などがあるのではないかと。
- 表1は「クレデンシャルの発行状況」の国際比較であり、表題のように電子政府の比較を行うのであれば、バックヤードでのデータ連携の状況等も記載する必要がある。利用者

とってのメリットの差が良く分からない。

- 韓国について、人口普及率37%というが、総人口には電子証明書を利用しないであろう児童などが含まれている。母数を経済活動人口にした場合の普及率は約80%である。この数字は決して小さくないのではないか。
- 韓国について、現在の水準に突然普及したわけではない。実際に使用されながら今の水準まで来たのであるから、現在、公的個人認証の普及が低いレベルにとどまっているとしても、今後普及する見込みがないとは一概に言えない。
- 日本においては、行政手続の手段として認められている民間発行の電子証明書も利用が進んでいない。諸外国においてはすでに国民全員に番号が付与されているなど社会状況の違いも考慮すべきである。

(2) ID・クレデンシャルの安全性・信頼性を測る共通の基準について

標記については、米国（2005年～）や韓国（2002年～）といった先進的な海外の電子政府のサービスにおいては、電子政府における民間IDの利用が実践されており、我が国においても、IDやクレデンシャルの安全性・信頼性を測る基準を明確化し、その基準によってIDと利用可能な電子行政サービスを特定すれば、同様に実現可能ではないか、との指摘があった。この点については、更に次のような指摘があったところ。

- ID・クレデンシャルが安全で信頼できるかどうか、またID・クレデンシャルの安全性・信頼性がどの程度であるかを評価する基準として、保証レベルの考え方が重要である。
- 保証レベルについては、内閣官房におけるオンライン手続におけるリスク評価及び電子署名・認証ガイドラインや、海外での取組を十分踏まえつつ十分に議論していくことが必要ではないか。
- また今後、ID・クレデンシャルを、国境を越えて利用する機会が高まる可能性があることから、我が国の独自性を発揮することよりも、海外における保証レベルの考え方との整合性を確保することが重要となるのではないか。
- 海外の動向（マネー・ロンダリング対策の事実上の国際スタンダードである FATF（Financial Action Task Force：金融活動作業部会）の勧告による身元確認方法の見直しに対する国際的な要請等）と照らしあわせて考慮すると、身元確認やIDの提供を「だれ」が行っているかだけでなく（組織）、「どのように」行っているか（プロセス）についても加味しながら、公正・中立な第三者機関の客観的な立場で適切に信頼性が判断される

ことが適当である。

- IDの提供を「だれ」が行っているかも重要であるという意見もあるが、IDの提供とは、登録時の「身元確認」のことなのか、アクセス時の「認証」のことなのかを整理して議論する必要があるのではないか。免許証等の身元確認用の証明証を行政が発行するのは当然であるが、認証も行政が発行したID・クレデンシャルを常に使うべきであるとはかぎらないのではないか。

また、これらの指摘に対して、以下のような意見があった。

- 保証レベルの検討は、IDが利用される分野にあわせて行われるべきであり、画一的な保証レベルを検討することは適当ではない。
- 我が国の国民性を考えると、IDの提供を「だれ」が行っているかも重要視される。実際に、行政が本人確認をし、IDを保証することについては、国民、民間企業、地方自治体などから一定のニーズがある。なお、本人確認を行う行政機関には、手続きに関する義務や公務員等に対する罰則が法律上規定されていることで信用力を確保している。
- ID・クレデンシャルの安全性・信頼性の議論を行う際には、法的な推定効の課題についての検討が必要である。

(3) 電子行政サービスとID・クレデンシャルとの保証レベルを媒介とする対応関係の明確化について

標記については、上記(2)で示されたとおり、各種電子行政サービスにおいて内容やリスク等の特性に即して要求される保証レベルと、保証レベルごとに求められるクレデンシャルの要件(身元確認情報のクレンジング等を含む)を定義・規定し、相互の対応関係を明確化した対応表を策定することが必要ではないか、との指摘があった。

さらに、本ワーキンググループでは、電子行政サービスの申請手続きに係るアクセス容易性の向上に向けて、具体的なアクションプランを検討するという目的に照らすと、この対応表にあたるものの存在が不可欠である、との指摘があり、一定の仮説の下で、試行的な分類による対応表として、委員から別紙の「保証レベルに応じた行政手続きの分類事例」の提示があったところである。

なお、こうした対応表について、以下のような補足の指摘があった。

- 本対応表は、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」が示すリスクのうち金銭的損害に係るリスクのレベル分けとともに、米国の取組みを参考にしている。

- この試行的な分類によると、一部の電子行政サービスを除いて、個人が利用する我が国の電子行政サービスの多くが概ね保証レベル2以下に相当するのではないかと。
- さらに保証レベルという側面からみると、レベル3の手続きについても民間IDの活用を想定することは可能である。例えば、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」における保証レベルの考え方に照らし合わせて、ネットオークションに利用されている、ある民間のIDを例にとり考えると、取得手続きにおいて、申請者が登録した住所に指定配送業者が訪問し、運転免許証等の身分証明書の提示による本人確認を行っているある民間IDは、レベル3に相当すると考えられるのではないかと。

また、これらの指摘に対して、以下のような意見があった。

- 試行的な取り組みとして、保証レベルの対応表が構成員から提示されたが、個々の行政サービスの保証レベルは、そのサービスを提供する主体が決めることから、対応表の汎用性については議論が必要ではないかと。
- また、内閣官房「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に記されている保証レベルの考え方との整合性に関して、国民が戸惑うような事態は避けるべく留意が必要である。
- なお、同ガイドラインでは、各種電子行政サービスにおいて要求される保証レベルは、あくまでサービス提供主体が金銭的損害に係るリスクや機微情報の漏えいに係るリスク、その他のリスク、二次的被害、申請者等の特性、回復可能性などを総合的に勘案した上で合理的に選択されることとなっている。
- 試行的な検討において、我が国の電子行政サービスの多くが概ね保証レベル2以下に相当するとされているが、その判断には慎重な議論が必要である。
- 例に挙げられた民間のIDの信用性には、そのIDのクレンジング（有効性の定期的な確認）の観点から、レベル3に相当すると判断するのは難しいのではないかと。
- パスポートの発給申請など、電子行政サービスがもたらすリスクが大きいレベル4の分野もあり、全てを民間IDのみに委ねるとの誤解を招くことのないようリスクの許容可能性を十分勘案して、民間IDの適用可能な電子行政サービスを特定しておくことが重要となる。

（4）民間IDの認定制度（信頼フレームワーク）の確立

標記については、民間のポータル事業者や決済事業者等が発行したIDを、行政機関のサ

イトへのログインに利用できるようにする、信頼フレームワークを整備することが必要ではないか、との指摘があった。この点については、更に次のような指摘があった。

- 米国においては、民間のポータル事業者や決済事業者等が発行したIDを、政府機関のサイトへのログインに利用できるようにしている、米国の信頼フレームワークは、民間主導でありながらも、現在までのところ特段問題も発生していないと認識している。よって、行政のサポートを受けた取組みとして、我が国が参考にできる制度モデルとなり得るのではないか
- このような先進事例を参考にしながら、我が国においても、既に存在する民間事業者の認定制度（有機食品認定制度等）の考え方や、民間主導という考え方を踏まえて、我が国固有の事情や関係主体の要望を取込みつつ、信頼性が高い民間ID（あるいは民間IDを発行する事業者）に関する認定制度（信頼フレームワーク）を民間において整備することが必要ではないか。
- こうした認定は、ID発行事業者の業務内容を審査することによって成立する。審査内容には、身元確認・登録プロセス、データのクレンジング、クレデンシャルの管理、プロトコルの実装などを含めることが重要となる。また、審査・認定は、定期的かつ継続的に実施されなければならない。このような認定制度を整備することによって、認定された民間IDの信用力を担保する。
- また、信頼フレームワークでは、関係主体の合意を前提として、リスクの許容範囲が決定され、その範囲内で関係主体が担うべき役割や機能、それらに対応する責任分担や免責事項、補償方法等が規定される¹。
- 民間事業者においては、民間IDの提供について以下のような考えがありうるのではないか。
 - ・自らのIDの利用範囲を広げ、利用者の利便性の向上に役立つことで、自社のウェブサイトへのログイン率を高められる効果（ひいては、顧客の囲い込みや自社サービスへの誘導・利用促進というビジネスにつながる効果）が期待できる。
 - ・今後、これまでより格段に電子政府・電子自治体の利便性を高めるという価値が実現されることによって、新たなビジネスモデルが成立することが期待される。
- 信頼フレームワークの確立においては、民間主導で作成された監査基準・信頼性基準や、公正・中立な第三者機関（民間事業者）が客観的な立場で適切にIDの信頼性を評価する認定スキームなど、既に参考となる制度モデルが存在するため、これをベースにして、我

¹ 責任分担の定義と免責事項、補償方法等の定義は、信頼フレームワークの有無にかかわらず、組織をまたがった認証を行う場合必要である、との意見があった。

が国固有の事情の反映等の差分を中心に効率的に検討を始められる。

また、これらの指摘に対して、次のような意見があった。

- 信用フレームワークについては、米国で問題なく運営されているといっても、日本に導入して良いとは限らず、我が国の国情や国民性に配慮し、導入の適正や可否を考えるべきである。
- IDを認定する主体や、その認定の方法などがまだ具体的に明確になっていないのではないかな。
- 民間IDの認定及び保証レベルの保証を行う信頼フレームワークの確立については、組織の安定性や持続可能性も含めた認定・監査が必要であり、制度確立に向けて多大な人的労力と時間、コスト、さらにはまったく新しい法的枠組みも必要となる恐れがある。
- 民間で発行されるIDの継続的な本人確認を行うのであれば、そのためのコストの規模が全体制度の運営の中でどれほどを占めるか、慎重な検討が必要ではないかな。
- 民間IDによる認証の制度については、不測の事態における責任分界点について、考え方やスキームにかかる全体の枠組みを、制度の構築に先だって整理することが必要である。
- 民間IDはそもそも民間企業が主体となって、配布・管理されるものであり、信頼フレームワークにおける認定においては、それぞれが民間のビジネスとして成立していることが必要である。公的な資金注入を期待すべきではない。
- 現在、高いセキュリティが求められないIDについては、多くの民間企業がビジネスの一部として運営することに成功している。しかし、より高い保証レベルの民間IDを扱う場合には、身元確認やデータのクレンジング等に係るコスト負担が増し、これに伴って、ビジネスの成立が難しくなり、高い保証レベルの認定取得を希望する民間ID事業者が現れなくなるのではないかな。
- 民間IDの提供において、「自らのIDの利用範囲を広げる」こと自体が、投資と維持コストを高めてしまうことになるのではないかな。

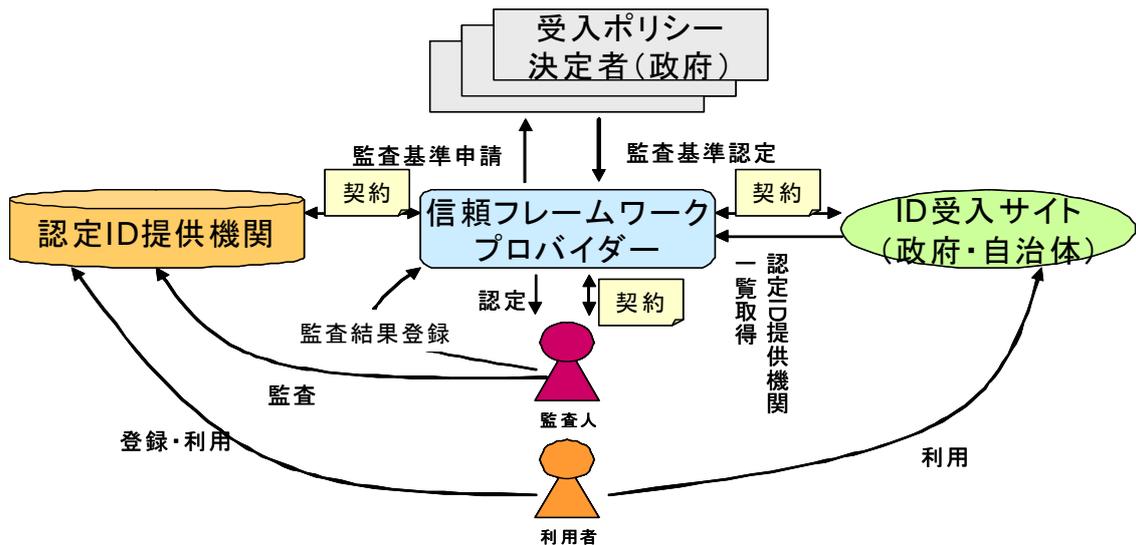


図3 米国の信頼フレームワークの事例

(5) その他

上記以外で、民間IDに関連して議論された点を参考として以下に記す。

①他の組織が保有している身元確認情報を有効活用できるようにする制度の確立

ある組織が厳密な身元確認を行った上で保有している高い信頼性を持った利用者の自己に関する情報を、IDを発行する事業者が有効活用できるようになれば、厳密な身元確認を効率的かつ安価に行うことが可能となるではないか、との指摘があった。この点については、更に次のような指摘があったところである。

- 例えば、犯罪収益移転防止法施行規則では、特定の目的に関して、他の特定事業者が行った本人確認を利用する本人確認方法が認められている。こうした仕組みを金融分野という特定の範囲内だけでなく、特定の基準を満たした幅広い分野にまで拡げることを認める制度を整備することが必要である。
- 一方、クレデンシャルやそれに紐づくID等の利用者の自己に関する情報については、国民主役の電子政府の確立、及びプライバシー保護の観点から、個人の意思に従って、自己に関する情報のやりとりが行われることが重要である。
- 個人の意思に従って、IDを発行する事業者が当該個人の情報を活用できる仕組みを確立するには、
 - (ア) 自己に関する情報の引渡しに関して個人の同意や承諾を得るための仕組み（図4を参照）
 - (イ) 引渡しされた自己に関する情報についても、その後アクセス可能となるようにし、併せて国民が内容を確認して、情報保有主体に対して閲読、訂正、抹消請求を求めるこ

とができる仕組み

(ウ) 利用者に対し、引渡し等の処理が適正に完了したことが通知され、その証跡が適正に保存されるための仕組み

という3つの仕組みを確立することが必要となる。

また、これらの指摘に対して、以下のような意見があった。

- 犯罪収益移転防止法施行規則における、他の特定事業者が行った本人確認の利用は、目的が特定されていることや、最初の直接的なダメージの回避が行われているので、クレデンシャルの信頼性は高いが、他行での被害に対する責任は負っていないのではないか。また、情報を与えた個人は、他行で利用されていることを認めているのか。

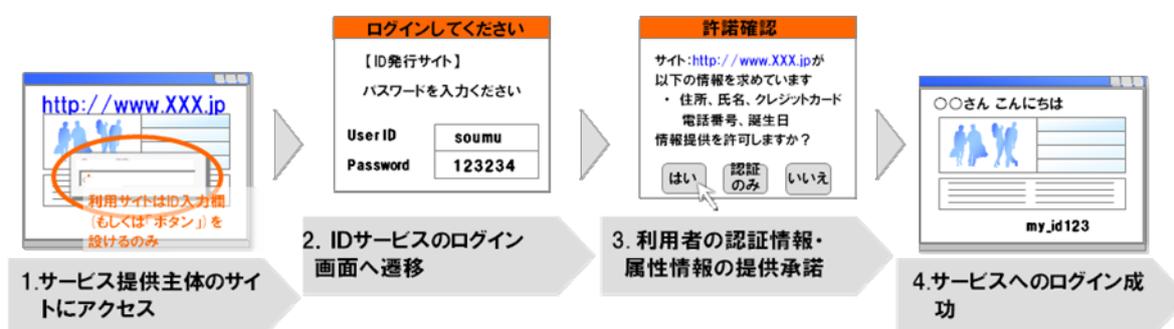


図4 利用者本人の同意に基づいて利用者の自己に関する情報の提供が行われるイメージ

②国際的なオープンスタンダードにそったデータ形式やAPI、プロトコル等の共通標準仕様の策定

データ形式やAPI、プロトコル等に関しては、国際的な共通化、標準化を図ることが不可欠ではないか、との指摘があった。この点については、更に次のような指摘があったところである。

- 民間IDの受入れや身元確認情報のやりとりに際して、システム接続時の対応が各主体ごとに個別対応になると多大な無駄が発生することから、データ形式やAPI、プロトコル等に関しては、共通化、標準化を図ることが不可欠である。
- オープンな民間企業の参加の下で、国際的な標準化動向も取込みつつ、共通標準仕様が策定されることが重要となる。こうした取組みを通じて公正な競争が生まれ、市場が効率化されることにより、コスト削減につながる効果も期待される。なお、民間IDの代表的な認証方式は、下記のとおりである（図5及び図6参照）
- また別の観点として、当該分野において、国際的な政策協力をを行い、標準化を先導することができれば、この面での我が国の国際競争力の強化に繋がる可能性がある。

【民間IDの例】

民間IDによる認証方式例として、OpenID方式と、SAML方式を以下に示す。

(1) OpenID方式

インターネットで普段、よく使っている民間ID（例 Yahoo, Google）を用いて、他の民間事業者が提供するウェブサイトにログイン（認証）し、サービスを受けるもの。

【特徴】 OpenID に対応の認証サーバを提供する複数の事業者（例 Yahoo、Google）が利用者の認証情報を提供。サービス提供者は認証サーバを複数選ぶことができ、利用者がアクセスする際は、それらの内から一つ選択し、情報提供の承諾を行う手順を経て、ログインを行う。

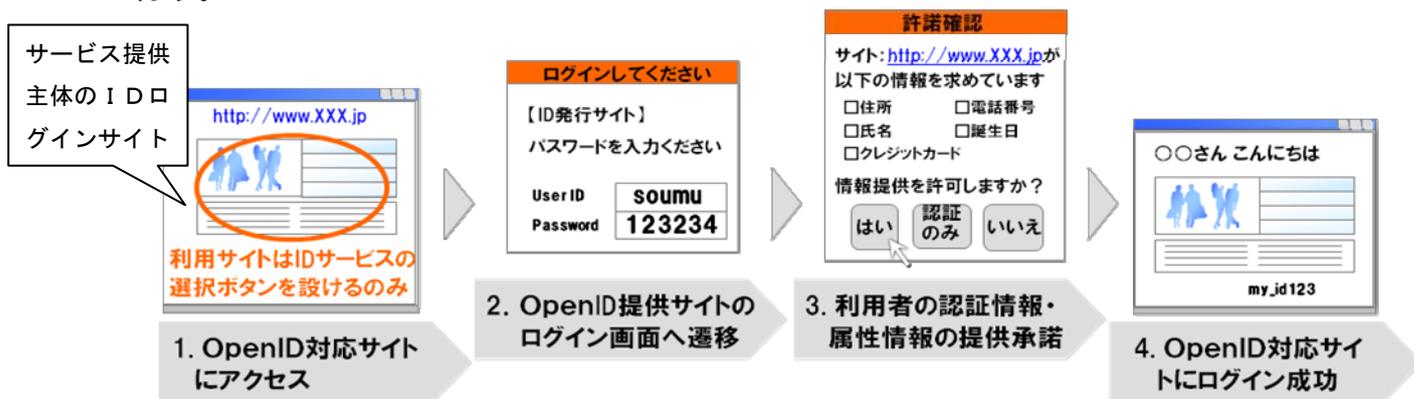


図5 OpenID方式による認証手順のイメージ

(2) SAML方式 (Security Assertion Markup Language)

企業などの組織等で使用されるIDを用いて、提携している他のサイトにログインし、サービスを受けるなど、組織間のシステムで認証情報を安全に交換するもの。

【特徴】 利用者の認証情報は、特定の認証サーバから提供。利用者の事前承諾を得た上で、利用者が一度、ログインを行えば、他のサイトを利用の際に、利用者が意識することなく自動的に認証が行われ、サービスを受けることが可能。なお、提携していないサイトは、特定のサーバから利用者の認証情報が得られない。

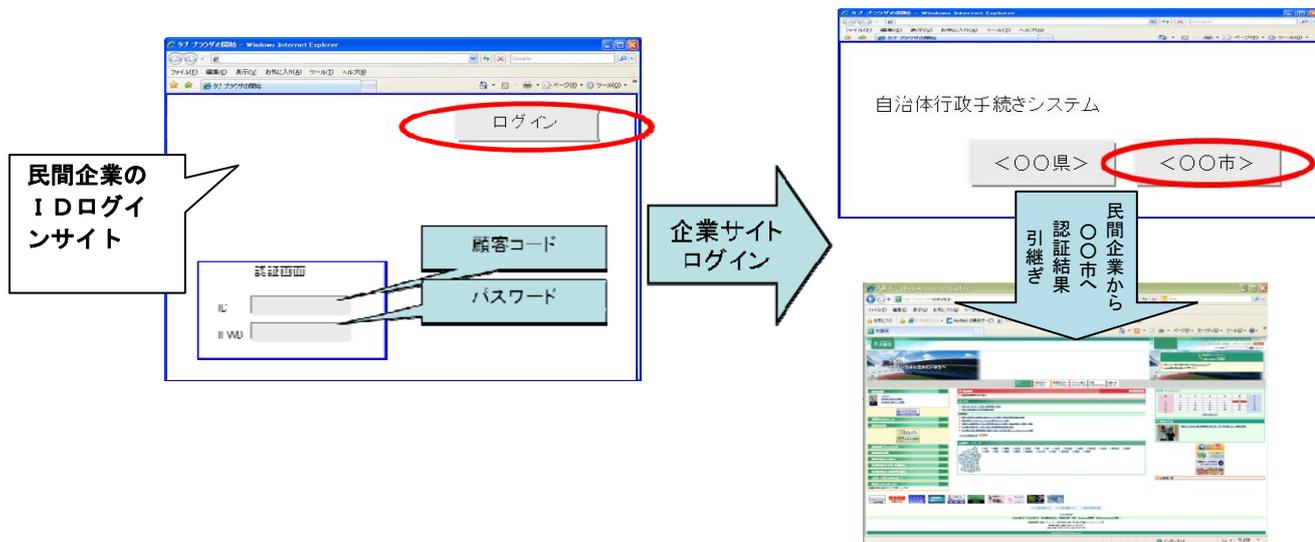


図6 SAML方式による認証手順のイメージ

③電子行政サービスへのアクセス手段に関する政府・自治体による周知広報

電子行政サービスへのアクセス手段に関して、政府・自治体による周知広報が必要ではないか、との指摘があった。この点については、更に次のような指摘があったところである。

- 高齢者や障害者、情報リテラシーが十分とは言えない国民を中心に、電子行政サービスへのアクセス手段から取り残される人々が出てくること懸念されることから、多様な代替手段を提供する仕組みを用意し、国民一般の行政サービスの利用を支援できるようにしておくことが重要である。
- 情報リテラシーやセキュリティ意識が不十分で、フィッシング詐欺やなりすましによる被害に遭遇する可能性が高い利用者を、電子行政サービスへのアクセス手段の利用に際してどのように守るか、その対策も必要である。
- 電子行政サービスへのアクセス手段の利用者である国民に情報リテラシーが必ずしも十分にあるとは限らないことを考慮すると、利用者の使い勝手の良さを高める努力を常に行うことが必要である。
- 利用者にとってのユーザビリティを高めるため、以下のような方策を講じることが有用ではないか。
 - ・ 国民のクレデンシャルの選択等についてのアドバイザーや仲介者としての機能を果たすポータルサイトの構築
 - ・ 国民が普段よく使っている民間のポータルサイトから電子行政サービスへの誘導
- 国民に対して、電子行政サービスへのアクセス手段の安心・安全な利用に関する普及啓発を図る観点から、教育用ツールの提供や情報提供のための専用サイトの開設、セミナーや教室の開催等を実施することが有用ではないか。これらの周知広報活動は、民間関連組織による自発的な取組みに加えて、政府・地方自治体を実施することが望まれる。

2. 公的な認証手段の利活用

公的な認証手段、特に公的個人認証サービスについては、政府内でのこれまでの議論においても、今後、速やかで自律的な普及を促し、様々なオンライン手続等の認証基盤として発展・定着を図っていくことが目標とされ、目標実現のために、利用サービスの拡大、利便性の向上、行政分野における更なる利用促進等を図ることが課題とされている。

IT戦略本部の「新たな情報通信技術戦略」（平成22年5月11日）においては、「公的個人認証サービスの利便性向上・用途拡大のための検討を2010年度中に行い、検討結果に基づく改善を速やかに行う」こととされている。さらに、「新たな情報通信技術戦略 工程表」（平

成 22 年 6 月 22 日)において、こうした利便性向上等を目的とした施策は、同戦略が掲げる「国民 ID 制度の導入と国民による行政監視の仕組みの整備」と連携しながら推進することとされている。

総務省においては、平成 21 年 8 月 12 日に公表された「公的個人認証サービス普及拡大検討会 中間取りまとめ」において、以下の 6 つの普及拡大方策が提案されている。

- (1) 認証用途の付加
- (2) 記録媒体の拡大
- (3) オンライン更新
- (4) 有効期間の延長
- (5) 署名検証者の拡大 (民間事業者への拡大)
- (6) 利用用途の拡大 (署名メール及び暗号メール)

以上のうち、本ワーキンググループの議論の過程で主に言及された方策は、(1) 認証用途の付加、(2) 記録媒体の拡大、の 2 点である。以下、課題毎に、主な意見の概略を記載することとする。

(1) 認証用途の付加

現在、公的個人認証サービスの電子証明書は、電子申請・届出の際に、電子署名が付された文書に本人がその意思をもって作成した文書として、署名・押印のある文書と同一の法的効力を付する署名用途のみ活用されている。

本ワーキンググループの議論において、今後、国民のニーズを満たす多様な電子行政サービスを利用する際に、公的個人認証サービスの電子証明書がより一層活用されるためには、その本人であって、なりすましではないことを保証する認証用途を付加することが必要ではないか、との指摘があった。

以上の点に関して、更に次のような指摘があった。

- 認証用の電子証明書を利用するに伴い、認証用の電子証明書がどのレベルの保証レベルに適合するかを明らかにした上で、保証レベルを媒介として利用可能な電子行政サービスを決定することが重要ではないか。
- 低い保証レベルで十分な電子行政サービスにおいて、必要以上に高い保証レベルを持つクレデンシャルが要求されるという保証レベルのミスマッチの問題が指摘されていることから、このような点に十分配慮して、適切な保証レベルで認証用の電子証明書を利用することが適当ではないか。
- 電子行政サービスにアクセスする際のクレデンシャルについて、「大 (高) は小 (低) を

兼ねる」という考え方が必ずしも安全側の発想に立脚していないのではないか。重要な用途に用いるべき実印を日常的に用いれば、実印を悪用した不正行為を誘発する恐れがあることと同様であろう。

- 一方、高い保証レベルを持つクレデンシャルは、当然、下位レベルのクレデンシャルを要求する電子行政サービスにも利用可能であるから、セキュリティレベルに合わせ異なる認証機能を一つのサイトから提供する手間や、ログインの際の利便性（煩わしさ）を勘案すると、高い保証レベルでのログインを図ることも有用であると考えられる。

（２）記録媒体の拡張

現在、公的個人認証サービスの電子証明書の記録媒体については、技術的基準を満たす IC カードのみとなっている。

本ワーキンググループの議論において、公的個人認証サービスの電子証明書の記録媒体を IC カード以外に拡張することで、電子行政サービスへのアクセスが容易かつ簡便になるのではないか、との指摘があった。

標記については、「公的個人認証サービス普及拡大検討会 中間取りまとめ」において、セキュリティ確保と普及状況等を考慮し、携帯電話端末（SIM カード）等に記録媒体を拡大することが提案されている。

以上の点に関して、更に次のような指摘があった。

- 電子証明書の記録媒体の拡張については、韓国の電子政府の事例が参考になると考えられる。韓国の電子政府では、ログイン認証時に使われる公認認証書（電子証明書）の記録媒体として、IC カード以外に、パソコン、FD、CD-ROM、USB トークン、携帯電話が認められている。
- こうした取組みと公認認証書の利用を促進する施策との相乗効果によって、韓国では、現在、経済活動人口の約 80% が公認認証書を保有している。

（３）その他

上記の 2 つの施策以外に、公的個人認証の利用の拡大に関連し指摘された点を、参考として以下に記す。

- 公的個人認証サービスへの理解促進を図り、国民にとってより身近なものとするためには、公的個人認証サービスの利用場面やメリット等についての情報提供および広報活動を継続的に行いつつ、公的個人認証サービスを一般化させる工夫を施す必要があるのではないか。

3. 魅力ある電子行政サービスの拡大

第2章で示した通り、民間IDの利活用及び公的な認証手段の利活用の共通の前提として、魅力ある電子行政サービスの拡大の必要性が指摘されている。

例えば、韓国の電子政府は、公認認証書の記録媒体の拡大等の施策に加え、利用率の高い行政手続きのオンライン化や、オンライン手続きの利用者に対する税金の還付といった特典の付与等の利用促進策を効果的に展開することにより、公認認証書の高い水準の普及率を実現しているという報告があった。

本施策について、本ワーキングの議論の過程で指摘された検討課題は、「行政機関と民間事業者における利用者情報の連携」と考えられる。本施策にかかる主な意見の概略は以下の通りである。

- 内閣官房における「次世代電子行政サービス基盤等検討プロジェクトチーム」（平成21年12月21日中間報告発表）で検討されてきたように、官民連携による行政サービスの質の向上がきわめて重要である。
- 電子行政サービスについては、単に利用率の向上だけではなく、サービスを利用することによって利用者にとってのベネフィット（利便性や効率の向上）をもたらすこと、社会全体の効率向上につながるものが重要である。
- 官民の情報連携は、添付書類の取寄せ・提出の省力化にも大きく寄与することが期待されるが、この点は国民にとっての電子政府実現の具体的メリットとして、重要な要素の一つである。
- 本施策について、官民の業務の効率化のみならず、行政サービスにおける国民の利便性の向上のためには、官と民の情報連携のためのプラットフォームを民間において構築することが有効ではないか。
- そのプラットフォームを通じて、利用者本人の同意を前提に、地方自治体が保有する住民情報を用いて、生命保険会社による個人年金給付における生存（現況）確認や銀行による新規口座開設等を可能にするといった活用方法が考えられるのではないか。
- 官民連携による情報の共同利用については、「官民連携による情報の共同利用を通じた、顧客・国民への良質なサービスの提供や利便性の向上」が究極的な目的として位置づけられるべきではないか。行政の効率化、企業のコスト削減といったサプライサイドのメリットのみならず、官民連携によって国民に対してより良質で利便性の高いサービスを提供していくという顧客視点が重要ではないか。

- 本施策は企業のコスト削減のためではなく、あくまで契約者たる国民の利便性向上が目的となり、国民が便利を実感できるサービスにつながるとともに、企業からの要望に応えることが期待できる。

また、魅力ある電子行政サービスという観点からは、その他に以下のような指摘もあったところである。

- 魅力ある電子行政サービスを提供できたとしても、利用者に認知されなければ利用されない。利便性が高いことを国民・企業に広く認知してもらうための広報活動の工夫・充実が重要である
- 電子行政サービスの利用を促進するためには、その内容に加え、利用者にあわせた電子行政サービスの効果的な情報の提供や、電子行政サービスの利用に際して魅力的なインセンティブをつけるといった方策も有効ではないか。

第4章 今後の進め方

1. 検討経緯と基本的な考え方

前章までに示したとおり、当ワーキングにおいては、「国民本位の電子行政の実現」に係る諸課題、すなわち、「電子行政サービスに対するアクセス手段の在り方」や「魅力ある電子行政サービスの在り方」に関する議論を行ってきたところであり、その概要は第3章に示したとおりである。

中でも「民間IDの利活用」「公的認証手段の利活用」等の論点について、様々な角度から検討を重ねたところである。この点、「公的認証手段の利活用」については、政府全体の新たな情報通信技術戦略において、手段の改善と利活用の拡大に向け、課題と方向性、行程表等が整理されつつあると考えられる一方、「民間IDの利活用」については、なお、様々な論点と指摘が見られるところであり、今後とも、継続した検討が望まれるところである。

しかしながら、以下の点については、本ワーキンググループの構成員の間で、大きな意見の相違はないのではないか、と考えられる。

- ①「国民が便利を実感できる、魅力ある電子行政サービスの実現」という課題が、電子行政の議論の原点であり、いずれの課題についても、常にこの原点に立ち返って検討を進めるべきこと。政府の新たな情報通信技術戦略に示されたとおり、これは可能な限り早期に実現すべき課題であって、着手できる施策から、速やかに実行していくべきであること。
- ②こうしたサービスを支えるICT基盤と制度の実現に向け、政府には、課題の明確化と、その解決に向けた不断の努力が求められること。特に、こうしたサービスのメリットについて、目に見える形で国民に示し、その実現の必要性について理解を得ていく努力が重要であること。
- ③「民間のID利活用」「公的認証手段の利活用」のいずれも、国民本位の電子行政サービスの実現に向け、重要な検討課題であること。関連する制度や予算の議論と並行して、「利活用に関する具体的なニーズ」「実現した場合のメリット」等について、国民の目に見える形で示していく必要があること。

こうした検討経緯、特に、国民本位の電子行政サービスの実現に向け、政府として着手できる施策から速やかに実行していくことが重要との指摘が多くなされたこと等にかんがみ、本ワーキンググループとしては、まずは、現在の技術・制度環境の下で、政府が以下を目的とする実証実験に可能な限り早期に着手し、実行することを提言するものである。

- (ア) より多くの国民が電子行政サービスにアクセスし、電子行政サービスの利用率の向上を図る観点から、「民間のIDの利活用」「公的認証手段の利活用」について、利用者の立場から見たニーズを明確化すること。

- (イ) 行政システム上で保有されている情報について、組織や業務の壁を超えた共有、利活用を促進し、国民利用者の利便性の向上を図る観点から、行政組織間、又は行政－民間の間の情報の共有、利活用について、利用者の立場から見た具体的なニーズを明確化すること。
- (ウ) 上記（ア）、（イ）のニーズに応えたアクセス手段やICT基盤が実現した場合、一般の利用者にどのようなメリットが生ずるか、具体的に目に見える形で提示するとともに、利用者の意見を収集すること。併せて、実現に向けた技術的・制度的課題の明確化を図ること。

本ワーキンググループとしては、こうした実証実験を通じて、その結果を行政機関や企業、一般の利用者の間で共有することで、これまでの検討において残された論点についても、更に有効かつ効率的な議論が可能となるものとする。

この8月には、政府のIT戦略本部に「電子行政に関するタスクフォース」が設置され、9月より、新たな情報通信技術戦略に示された方針に沿った、具体的な議論が開始されたところである。本ワーキンググループとしては、総務省が、これまでに示した検討結果や、今後実施される実証実験の成果を、適時上記タスクフォースの議論にも反映するよう努め、国民本位の電子行政の実現に向けた取り組みが、更に加速・推進されることを期待するものである。

本ワーキンググループにおいては、複数の委員から、以上を具体化した実証実験に関する提案が行われたところである。本ワーキンググループの検討結果を、より適格に実証実験に反映させる観点から、以下、その提案の概要を記載することとする。

もとより、政府が上記実証実験を実施していくにあたっては、国民・事業者の多様な意見・アイデアを反映させる観点から、一般公募を通じ、実証実験に関する具体案を幅広く募り、透明かつ公正な手続きで、上記の目的に沿った案を採択していくことが必要であることは言うまでもない。

2. 提案されたユースケース

上記のとおり、本ワーキンググループの議論においては、実証実験のユースケースについて、以下の2つの提案があった。

- (1) 市民協働ポータルサイト
- (2) 官民連携プラットフォーム

(1) 市民協働ポータルサイト

本ユースケースは、地方自治体サイト（本番サイト）とユーザーの間に「市民協働サイト」

というマッシュアップサイトを構築、既存自治体サイトの変更を最小限にしなが、認定ID提供機関を想定したID提供機関のIDを用いて、下図に示されているとおり、市民が自治体に対して、多様な行政サービスの実処理（本番）手続きを行うものである。

対象とする行政手続きのセキュリティレベルについては、本ワーキンググループの議論の中で、試行的に作成し提出された別紙の表における、保証レベル1及びレベル2を想定する。

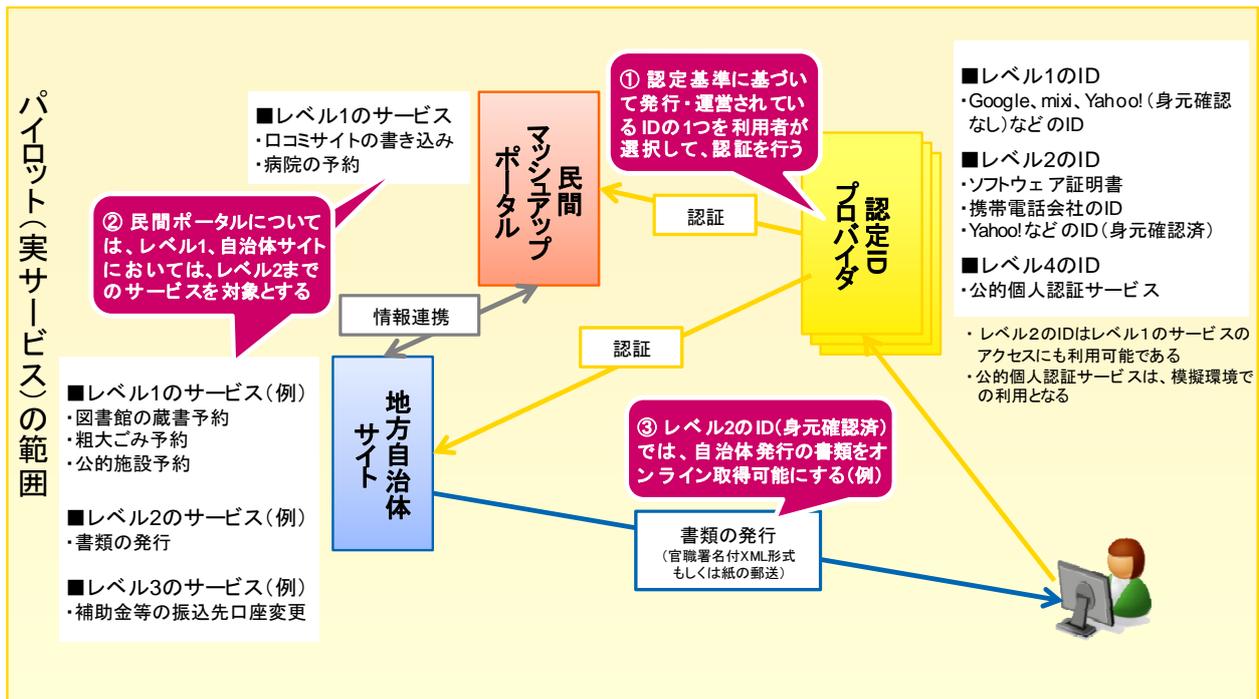


図7 市民協働ポータルサイトの実証イメージ

なお、本ユースケースでは、関与主体の拡大や、制度的な課題の解決に伴って、検証範囲を段階的に拡大することを想定している。

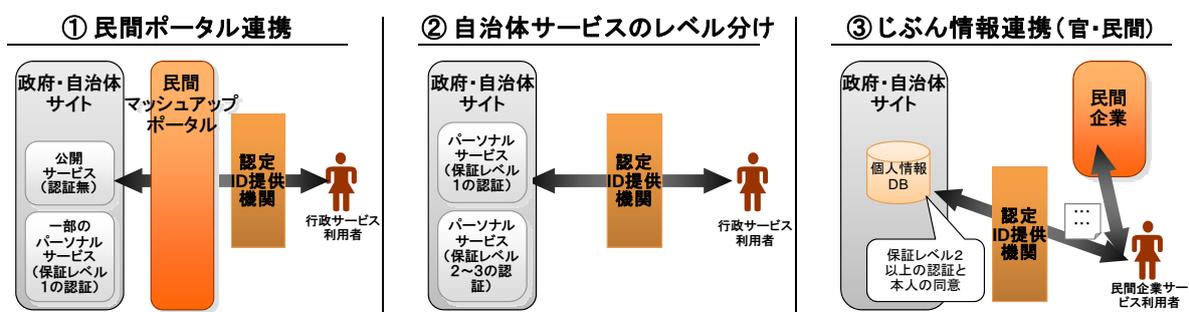


図8 実証実験における検証範囲の段階的な拡大

本ユースケースを通じて、下記の検証項目を検証することを目的とする。

① 番号の原則（総務省）との整合性

「国民の権利確保（自己情報コントロールによる利用範囲の明確化）」や「プライバシー保護（含名寄せ防止）」、「費用最小」などの各項目を満たしているか

② セキュリティレベルに応じた行政サービスとIDの整理・検証

(ア) 4つのレベルのうち、レベル1～3を実施。パイロット対象となるサービス選定と分類を行う。

- ・ レベル4については、一般市民が利用するサービスでは、ほとんど存在しないため、優先順位は低い
- ・ 但し、制度検討としては、レベル4についても継続

(イ) 認定IDとしては、以下を候補とする。各サービスごとにどのIDが好まれるか、定量的（利用状況統計）、定性的（利用者アンケート）に評価する

- ・ 公的個人認証（相当の）ICカード（利用目的制限があるため模擬環境とする）
- ・ ソフトウェア証明書（実サービスのものを使う）
- ・ 携帯電話会社ID（実サービスのものを使う）
- ・ ポータルサイトID（実サービスのものを使う）などを対象とする。

(ウ) 認定ID制度検討に関するフィードバック

IDプロバイダを仮想監査することを通じて、IDプロバイダ、トラスト・フレームワーク・プロバイダ、監査人それぞれの要件を洗い出す

③ ステークホルダーごとの便益対コストの評価

利用者の利便性： どのIDが使いやすく・導入の手間がかからず、安心かを評価

自治体の効率性： 業務の効率化、システム対応コスト等の評価 → 政府・自治体全体のコストシミュレーションを実施

民間企業のニーズ： 民間IDプロバイダのニーズ調査、個人データ連携先企業のニーズ調査

上記の検討項目に加えて、民間IDの利活用において指摘されている継続的な身元確認のコスト負担や問題発生時の責任分担に係る課題への適切な改善・解決策を検討する。

(2) 官民連携プラットフォーム

本ユースケースは、行政機関と民間事業者間における利用者情報の連携を実現するために、以下のような構成を持つ官民連携プラットフォームを民間において構築するものである。具体的なサービスとしては、地方自治体が保有する情報で年金支給における生存（現況）確認などを検証の題材として想定しており、利用者の認証には、公的個人認証サービスの利用を想定する。

本ユースケースでは、下記の検証項目を想定している。

- ①国民の利便性向上の評価
- ②民間事業者の業務効率化の評価
- ③自治体の業務効率化の評価
- ④官民連携プラットフォームに求められる機能に係る評価

【別紙】保証レベルに応じた行政手続きの分類事例(崎村構成員提出資料)

保証レベル	リスクの影響範囲と身元確認方法(注1)	OMB M04-04の例	想定される行政手続きの事例(注2)	保証レベルに応じた自治体の行政手続きの分類事例(子育て関連の場合)	主な利用者
1	・サービス側で個人情報を取り扱わないもの ・金銭的影響:なし	① 公園の年間入園許可証の申請 ② My.ED.govで自身で登録したユーザIDとパスワードを使いカスタマイズページを作る場合 ③ whitehouse.govのWebサイトでのオンラインディスカッションに参加する場合	① 公立病院のWebサイトにて健康診断の予約 ② 地方自治体の図書館サイトの蔵書予約 ③ オープンガバメントの意見徴集サイトでコメントを書き込み	主に予約・相談系サービス ・親子向け・子供向け施設予約 ・コミュニティイベント予約 ・相談・問合せ ・口コミサイトへの書き込み ・健康診断・予防接種の予約	・一般市民
2	・サービス提供時に個人情報が必要なもの ・個人のレベルで金銭的影響が大きいもの ・金銭的影響:100万円以下(注3)	① Gov Online Learningサイトで利用者が報酬や昇進に関係する必要なトレーニングを修了していることを示す ② 受給者が社会保障Webサイトを通じて自身の住所記録を変更する場合 ③ 政府機関のプログラムクライアントが銀行口座、プログラムの資格または支払い情報を更新する場合	① 職業訓練サイトで、訓練修了証をオンラインで取得 ② 年金や手当を振り込む銀行口座をオンラインで変更(認証だけでなく、口座確認によっても保証レベルを担保している) ③ 住民票や印鑑証明書をオンラインで申請し取得(一方、現状の窓口取得は、委任状でも可であるため、レベル1と言える)	主に申請・申込系サービス (金銭の支給がない、もしくは、単発的な経済的支援系サービス) ・小児医療費助成の申請 ・高度技能訓練促進費の申請 ・自立支援教育給付金の申請 ・育成医療費助成の申請 ・公衆浴場無料券(母子父子家庭向け)申請 ・子育てサービス(自宅ヘルパー)入会 (継続的な経済的支援系サービス) ・子ども手当の申請 ・母子及び寡婦福祉資金の申込 ・ひとり親医療費助成の申請 ・母子福祉対策資金貸し付けの申込 ・障害児福祉手当の申請	・一般市民
3	・大量の個人情報にアクセスできるもの ・組織のレベルで金銭的影響が大きいもの ・金銭的影響:1000万円以下(注3)	① 特許弁理士が合衆国特許商標局に対し、機密の特許情報を電子的に提出する場合 ② ある供給業者が、大規模な政府調達について、一般調達局の契約担当官に対する口座を維持している場合 ③ 緊急救助隊員がインシデントを報告し、運営上の情報を共有し、対策活動をコーディネートするために、災害管理報告Webサイトにアクセスする場合 ④ 政府機関の職員または委託業者が、リモートシステムを使用して、潜在的に機密な、個人顧客情報へのアクセスする場合	① 金融機関の担当者が、住基ネットにアクセスし、契約者の現状を一括確認 ② 社会労務士が、eGovサイトにて、社会保障に関する申請を、顧客の代行で実施 ③ 司法書士が、オンラインで土地を登記 ④ 企業担当者が、政府公募案件を電子応札 ⑤ 自衛隊員や消防署職員が、災害時に個人情報にアクセス ⑥ 弁理士が、特許庁に機密の特許情報を電子的に提出	該当するサービスなし	・士業資格者 ・企業担当者 ・政府関係者
4	・国家安全保障に大きく関わるもの ・金銭的影響:1000万円以上。(注3)	① 法執行官が、犯罪歴が格納されている法執行データベースにアクセスする場合 ② 復員軍人援護局の薬剤師が規制医薬品を調剤する場合 ③ 政府機関の捜査官が、リモートシステムを使用して、潜在的に機密の個人顧客情報へアクセスする場合	① 警察が、犯罪歴と法執行に関するDBIにアクセス ② 政府の捜査員が、リモート(例えば、自宅や現場からノートPC)で大量の個人情報にアクセス	該当するサービスなし	・政府関係者

(注1) 米国内務省「連邦政府機関向け電子認証ガイドンス」(OMB M-04-04)を元に、分かりやすさ重視で表記

(注2) 米国内務省「連邦政府機関向け電子認証ガイドンス」(OMB M-04-04)の「2.4. 保証レベルおよびリスクプロファイル:説明および例」の内容から、日本の行政サービスの場合を仮定し作成した。

(注3) 一回あたりの補償前被害の額の例。H.22.8.31公表のオンライン手続きにおけるリスク評価及び電子署名・認証ガイドラインより。被害発覚までの総額で勘案すべき、

OMBの重大度表現(OMB M04-04の表参照)に合わせ、補填後金額で表現すべきなどの指摘あり。なお、金額の重大度は損害を負担する主体により異なるので注意が必要。

【別紙】保証レベルに応じたID／発行主体の例(崎村構成員提出資料)

保証レベル	身元確認方法 (注1)	レベルに相応する ID／発行主体の例	主な利用者
1	・電子メールアドレスが申請された場合、有効性(到達性)を確認する。	・Yahoo!(身元確認なし) ・Google ・Mixi ・楽天 等	・一般市民
2	・申請者の氏名と住所等、及び身元確認に有効な他機関の登録情報(クレジットカード番号等)が記載された申請書により申請する。	・金融機関(犯罪収益移転防止法による規定) ・携帯電話(携帯電話不正利用防止法による規定) ・Yahoo!(ウォレット) 等	・一般市民
3	・申請者の氏名や住所等の公的な台帳との照合、または申請書に添付された公的証明書(住民票等)によりチェックする。 ・申請者の氏名と住所等が記載された申請書に本人の電子署名(郵送の場合は署名又は捺印)を付与して申請する。	・特定認証局 (電子署名法による規定) ・Yahoo!(身元確認あり)	・士業資格者 ・企業担当者 ・政府関係者
4	・対面のみ可で、上記に加え、重複登録ではないことを確認する。	・公的個人認証サービス(注3) ・パスポート (新規発行の場合、戸籍抄本、住民票、他の身分証明書、写真が必要) ・運転免許証 (新規発行の場合、住民票、他の身分証明書、写真、試験合格証が必要)	・政府関係者

(注1) 米国国立標準技術研究所「電子認証に関するガイドライン」(NIST Special Publication 800-63)を元に作成
今回は説明を簡略化するために身元確認基準部分のみを引用した。