Society5.0を見据えた個人認証基盤のあり方について

（報告）

平成３０年６月

Society5.0を見据えた個人認証基盤のあり方懇談会

目次

第１．趣旨 1
　１．Society5.0 を見据えて 1
　２．個人認証基盤の検討に際して考慮すべき視点の整理 1
第２．個人認証の基本的な概念（本報告のパラダイム設定） 2
　１．基本的な概念の整理の必要性 2
　２．個人認証の基本的な概念 2
　３．本報告の整理の対象 3
第３．本人認証が求められる手続・サービスと対応する認証手段 3
　１．本人認証が求められる手続・サービスの現状 4
　２．対応する認証手段の現状 6
　３．手続・サービスに応じた最適な認証手段の選択可能性 7
第４．認証情報の利用についての検討 8
　１．認証情報の種類と特徴、活用可能性 8
　　（１）知識情報 8
　　（２）所持情報 9
　　（３）身体・行動情報 9
　２．複数の認証情報の組合せ 10
　　（１）基本的な考え方 10
　　（２）認証情報の組合せ方 11
　　（３）その他制度・仕組みとの組合せの可能性 12
　３．認証情報の保管方法と安全管理措置 13
第５．社会における具体的な認証場面への適用に向けて 14
　１．多様化・拡大する手続・サービスへの対応可能性 14
　　（１）本人認証が求められる場面の多様化・拡大 14
　　（２）認証手段の多様化の可能性 15
　　（３）知識情報を置き換える場合の認証情報 15
　２．公的部門における認証場面への適用の可能性 16
　　（１）認証手段の選択に向けた視点 16
　　（２）電子証明書についての事例検討 16
　３．ＡＩその他の先端技術の活用可能性 18
第６．おわりに 19

Society5.0を見据えた個人認証基盤のあり方について
（報告）

第１．趣旨

１．Society5.0を見据えて

近年モノのインターネット化（Internet of Things、以下「ＩｏＴ」という。）やビッグデータ、人工知能（Artificial Intelligence、以下「ＡＩ」という。）、ロボットなどに代表される第４次産業革命と呼ばれる産業・技術革新が世界的に進みつつあり、生産や消費といった経済活動だけでなく、働き方などライフスタイルも含めて経済社会のあり方が大きく変化しようとしている。

とりわけ、ＩｏＴによって、流通、交通、個人の健康状況など様々な情報をデータ化し、ネットワークでつなげて利用することが可能となると見込まれる。消費者側から見れば、インターネットを通じて、個々にカスタマイズされたサービスを、今までよりも低価格で好きな時に適量購入でき、又は、潜在的に欲していた新しいサービスを享受できるようになることが期待される。

我が国では、ＩｏＴを含む第４次産業革命のイノベーションを取り込んだ超スマート社会を「Society5.0」と位置付け、世界に先駆けて実現することを目指している。

【参考】第５期科学技術基本計画　（平成28年１月22日閣議決定）（抄）

第２章 未来の産業創造と社会変革に向けた新たな価値創出の取組
（２）世界に先駆けた「超スマート社会」の実現（Society 5.0）

（略）ＩＣＴを最大限に活用し、サイバー空間とフィジカル空間（現実世界）とを融合させた取組により、人々に豊かさをもたらす「超スマート社会」を未来社会の姿として共有し、その実現に向けた一連の取組を更に深化させつつ「Society 5.0[2]」として強力に推進し、世界に先駆けて超スマート社会を実現していく。

2　狩猟社会、農耕社会、工業社会、情報社会に続くような新たな社会を生み出す変革を科学技術イノベーションが先導していく、という意味を込めている。

２．個人認証基盤の検討に際して考慮すべき視点の整理

あらゆるモノやサービスがインターネットでつながる「Society5.0」において、多様化・拡大する様々な手続・サービスを個人が広く利用できるためには、その前提として、安全で確実な個人認証基盤が重要であ

る。

本報告は、こうした将来を見据え、誰でも手軽に負担感なく使える「Society5.0」にふさわしい個人認証基盤、とりわけ個人が本人であることを証明するために用いる認証手段の種類や特徴、将来的な活用可能性について整理することを目的とする。

第２．個人認証の基本的な概念（本報告のパラダイム設定）

１．基本的な概念の整理の必要性

「認証」という語については、用いられる場面によって異なる行為や事象を指す場合がある。

例えば、「指紋情報を『認証』に用いる」と表現する場合、その内容として、

① 全ての個人の指紋情報を、あらかじめデータベースに登録し、各個人を識別するＩＤとして活用する

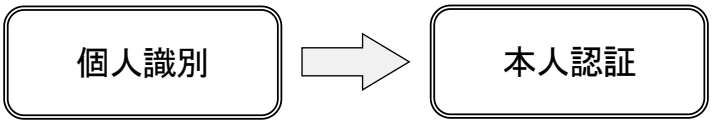
② 希望する個人が、あらかじめ自ら指紋情報を登録し、本人しか持ち得ない秘密の暗号鍵として活用する

の２通りのケースが典型的には考えられる。

①②の両ケースは、本人又は認証する者・機関の双方について、責任範囲や情報の保護のあり方等、議論に当たって考慮すべき事項が大きく異なることとなるため、基本的な概念を整理し、議論の対象を明確にしておくことが必要である。

２．個人認証の基本的な概念

個人認証の基本的な流れは、「個人識別」と「本人認証」によって構成される。

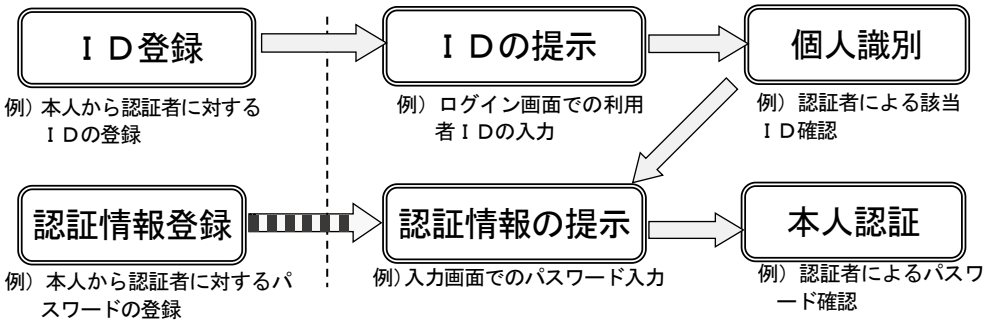


・「個人識別」（Identification）は、個人から提示された識別情報（ＩＤ）を用いて、保有するデータベースの検索を行い、該当するＩＤが存在することを確認する（「１対ｎの照合」を行う）こと、とされ

ている。

・「本人認証」（Authentication）は、「個人識別」によって区別された個人について、当該個人本人だけが備えているものとして登録された情報（「認証情報」）と照合し、当該個人が確かに本人であることを確認する（「１対１の照合」を行う）こと、とされている。

・さらに、「個人識別」は①ＩＤの登録、②ＩＤの提示及び③識別によって、「本人認証」は①認証情報の登録、②認証情報の提示及び③認証によって、構成される。



３．本報告の整理の対象

本報告は、「Society5.0」において多様化・拡大する手続・サービスの内容や性質に応じ、利用しようとしている者が本人であることを負担感なく証明する方法について整理しようとするものである。

この観点から、「個人識別」のために登録が必須となる「ＩＤ」としてどのような情報を用いるかではなく、手続・サービスの利用者が本人であることを証明する「本人認証」の場面で用いる「認証情報」について、整理することとする。

したがって、１．の①又は②のケースについては、②を念頭に整理していくこととするものである。

第３．本人認証が求められる手続・サービスと対応する認証手段

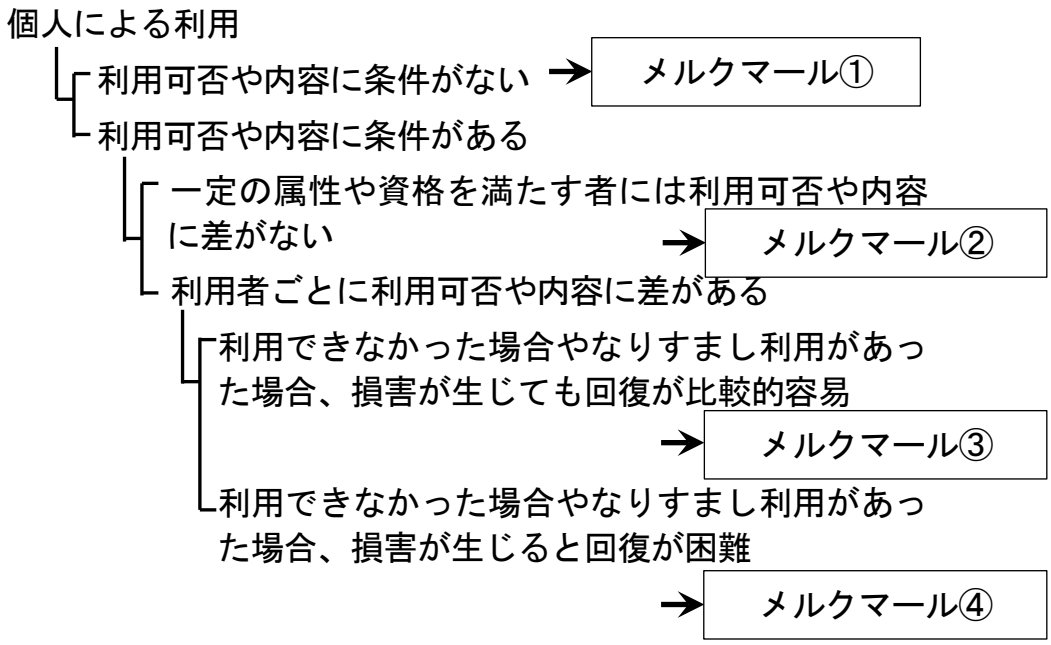
本人認証の今後に向けた議論に先立ち、現状の手続・サービスと対応する認証手段を俯瞰することで、本人認証の手段とそれが必要となる場面の広がりを確認する。特に、本人側や認証側に生じ得るリスクと回復の困難さは、どのような認証手段を選択するか検討する際の重要な視点

であるため、この点を勘案して以下整理する。

１．本人認証が求められる手続・サービスの現状

現在、官民の各種手続・サービスの内容や性質に応じ、対面・非対面での様々な本人認証が用いられている。

現状の各種手続・サービスから場合分けを行い、必要となる本人に関する情報やその精度、用いられている認証手段を対応させると、以下のメルクマール①から④までのように整理できるのではないか。



メルクマール①：誰でも利用可能な手続・サービス

- 利用するために特別の属性や資格は必要なく、利用可能な手続・サービスの内容に差異がないもの。
- 利用者が本人であることを証明するための特別の情報や手段は不要。
- 例えば、無料で利用できる公園や開放型施設の利用などが該当。

メルクマール②：条件を満たせば幅広い者に利用させる手続・サービス

- 利用するために一定の属性や資格を満たす必要があり、満たさない者と比較して利用可能な手続・サービスの内容

に差異があるもの。

- 当該属性や資格を満たしている本人であることを証明するための情報や手段が必要。
- 現状、手続・サービスに応じて発行される会員証等の提示のほか、初回登録後には利用者証明用電子証明書やＩＤ・パスワード方式により確認されている。
- 例えば、有料の官民交通サービスの利用（運賃支払が条件）、市民マラソン等のボランティア参加や図書館利用（当該市町村の住民であることが条件）、酒・タバコ販売（成人年齢に達していることが条件）などが該当。

メルクマール③：利用者ごとに利用可能な内容が異なる手続・サービス（リスク回復容易）

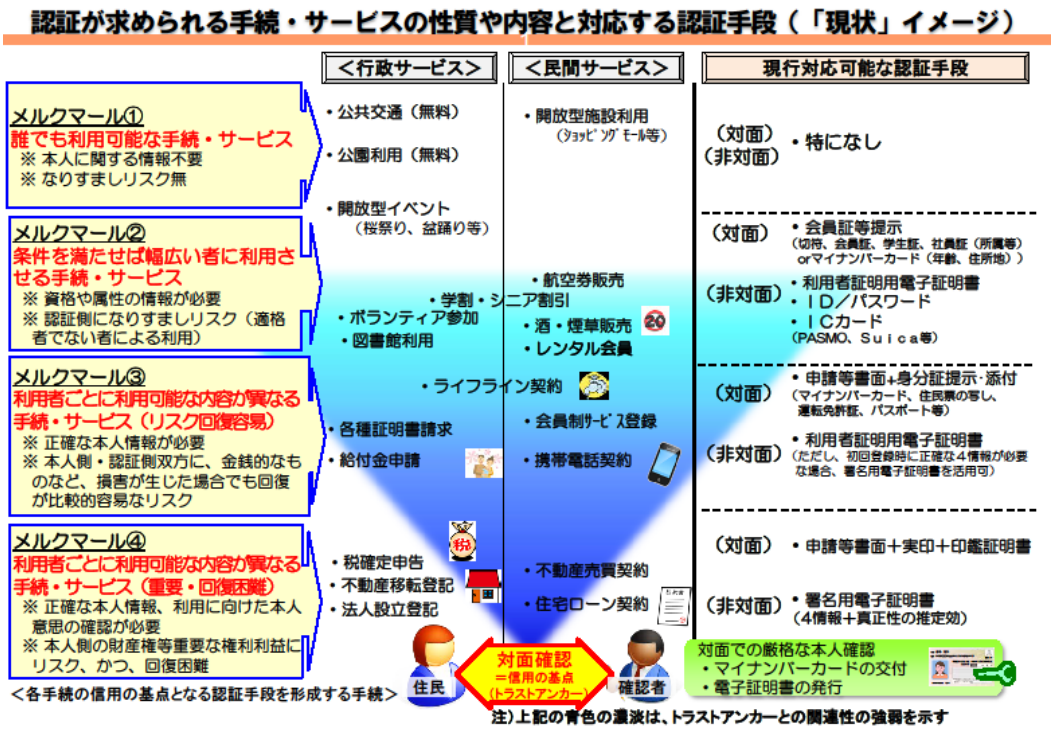
- 利用者ごとに利用可否や内容に差異があるものであって、メルクマール④に該当しないもの。本人の利用ができない又は他人によるなりすまし利用があった場合本人又は認証側の双方にリスクがあるが、金銭的なものなど損害を回復することが比較的容易であるもの。
- 正確な本人に関する情報と当該情報に紐付く本人であることを証明するための手段が必要。
- 現状、申請書等の書面に身分証明書を提示・添付する方法のほか、署名用電子証明書により確認されている。
- 例えば、ライフライン契約（住所情報が必要）、各種証明書請求（請求者を特定する基本４情報などが必要）などが該当。

メルクマール④：利用者ごとに利用可能な内容が異なる手続・サービス（重要・回復困難）

- 利用者ごとに利用可否や内容に差異があるものであって、本人の利用ができない又は他人によるなりすまし利用があった場合、刑事罰を伴う行政手続や不動産に関する権利など、損害が生じた際に、回復することが困難であるもの。
- 正確な本人に関する情報と当該情報に紐付く本人であること、及び、当該手続・サービスを利用する本人の意思が真正であることを証明するための手段が必要。

・　現状、申請書等の書面に実印を押下し印鑑証明書を添付する方法のほか、署名用電子証明書により確認されている。

・　例えば、不動産移転登記や不動産売買契約、法人設立登記などが該当。



２．対応する認証手段の現状

認証手段については、用いる認証情報の客観性や利用頻度によって精度が異なることを踏まえ、手続・サービスの内容や性質に応じて適切に選択されることが必要である。

１．で分類した認証手段は、①会員証やＩＤ／パスワードなど、本人が自ら設定・登録した情報を基に認証を行う場合と、②身分証の提示など、本人以外の公的機関が本人情報であることを「証明」した情報（Certificate）を基に認証を行う場合に大別できる。

・　①と比較して②は、用いる認証情報に客観性があるほか、「証明」の段階で一度本人認証を受けていることから、認証手段としての確実性（認証の精度）が高くなる。

・　また、①と比較して②は、同程度の精度を実現する認証手段を

認証側自らが構築しようとする場合よりも、必要なコストを低減することができる。

また、これら設定・登録され、又は「証明」された認証情報は、時間の経過によって異動が生じる可能性があるが、様々な認証場面で用いられ、本人を指す情報であることが確認され、仮に情報に変更があれば、その都度新しい情報に変更されること（変更がなければ、変更されていないことが都度確認されること）により、いわば「鮮度」が高いことが確保されれば、より信用度（精度）が高まることとなる。

なお、この点、住民票に記載された情報は、転入届の際に市町村窓口において対面で確認をするものであることに加え、各種手続又は市町村長や地方公共団体情報システム機構による身分証の発行・書換えの度に参照される（いわば「鮮度」が高い）ことからも、他の情報と比較して本人情報としての信用度が高いと評価できるのではないか。

更に、この住民票に記載された情報について、改めて公的機関が本人との紐付けを対面で確認して発行し、かつ、異動情報が随時反映されるマイナンバーカードや公的個人認証の電子証明書は他の認証情報と比較して信用度が高いと言えるのではないか。

３．手続・サービスに応じた最適な認証手段の選択可能性

１．の分類から読み取ることができるように、本人認証が必要となる手続・サービスの内容や性質に応じ、①認証手段としての確実性（本人が利用を拒否され、又は他人がなりすまし利用するリスクの低減）や、②利便性の確保（本人側の負担（手間、工数）の削減、認証側のコスト抑制等）をどこまで求めるかは異なる。

また、同時に、手続・サービスの内容や性質に応じ、各種リスクや負担について、本人側が負うべきか認証側が負うべきかについても、異なることとなる。

一般的に、認証手段としての確実性を上げようとすれば、本人側が認証のためにとるべき手続が増えるため、利用者の利便性を上げようとすることとは「トレードオフ」の関係にあると言える。

「トレードオフ」の関係性を踏まえつつ、手続・サービスにおいて必要とされる情報やその精度に対応できる最適な認証手段を選択できるよ

うにすることが求められているのではないか。

また、インターネットを通じた非対面での手続・サービスが拡大すれば、現在、対面での利用を想定して簡易な手段を採用している場面にあっても、一定レベルの精度をもった本人認証が必要となる場合があると考えられる。

手続・サービスに応じた認証手段の選択に当たっては、①本人以外の者が利用するリスクの低減が必要な場合等に、より精度の高い認証手段を活用していくこと、②精度の高い認証手段の利便性を向上していくこと、の２つのアプローチが考えられるのではないか。

第４．認証情報の利用についての検討

個人が本人であることを証明する「本人認証」に必要となる認証情報については、一般的に、「知識情報」(As You Know)、「所持情報」(As You Have)、「身体・行動情報」(As You Are) の３つに分類される。

具体的にどのような認証情報を用いるかによって実現する認証の精度や利便性は大きく異なるが、本人認証の今後に向けた議論の前提として、３分類の特徴、単独又は組み合わせての活用可能性を整理することとする。

１．認証情報の種類と特徴、活用可能性

（１）知識情報

「知識情報」とは、「本人しか知らない情報」であり、例えば、暗証番号、パスワード、質問応答等が該当する。

忘却や第三者による推測のおそれがあるため単独で用いるには限界があるが、特別の読み取り機器やスキルが不要であるため利用範囲が広い点で意義があるのではないか。

主な利点	主な留意点
・変更することが容易 ・利用範囲が広い（既に広く普及） ・利用者側に特別の情報読み取り機器が不要	・忘却の可能性 ・推測による攻撃が可能 ・虚偽メール、資料盗取や会話盗聴による不正入手の懸念

「知識情報」については、本人拒否又は他人受入により生じるリスク

が低い場合は単独で、リスクが高い場合は複数の認証情報と組み合わせて用いることにより、今後創出される様々な手続・サービスへの対応可能性が広がるのではないか。

（２）所持情報

「所持情報」とは、「本人しか持ち得ない情報が記録された媒体」であり、例えば、鍵、身分証明書、ＩＣカード、磁気カード、電子証明書（秘密鍵）、携帯電話、スマートフォン等が該当する。

記録される媒体によって利便性が異なるが、一般的には、本人認証に際して直面し得る記憶の限界（覚えきれない、忘れてしまう等）や身体的リスク（指紋情報を盗取するために指そのものを奪う等）に対して、個人やその情報を技術的に保護する点で意義があるのではないか。

利点	留意点
・取り替えることが容易 ・忘却がない ・暗号技術や耐タンパ技術により情報保護が可能 ・盗取時に身体的リスクが低い	・利用時に所持している（持ち歩く）必要 ・暗号技術の強度を維持する必要 ・媒体自体の紛失・盗難のリスク ・記録された情報の盗み見られるリスク ・製造・設置コストが必要 ・情報を読み取る機器が必要

「所持情報」については、通信端末を記録媒体とすることで、今後創出される様々なインターネット上の手続・サービスへの対応可能性が広がるのではないか。

この場合、特に、高頻度で利用される手続・サービスにおいて、より効果を発揮することが見込まれるのではないか。

（３）身体・行動情報

「身体・行動情報」とは、「本人の身体・行動が持つ固有情報の差」であり、例えば、筆跡、音声、顔、指紋、虹彩、静脈、行動パターン等が該当する。

取り替えが困難であり、流出時に個人の情報を保護することが難しいほか、100%の認証は困難である等の諸点に留意が必要だが、既にスマートフォン端末の起動などの際に用いられているなど、持ち歩く必要がない等の利便性向上という点で意義があるのではないか。

利点	留意点
・持ち歩く必要がない ・忘却・紛失がない	・現状では 100%の認証は困難（本人拒否率・他人受入率の閾値設定が必須） ・加齢その他の身体的特徴の変化で認証できなくなる懸念 ・取り替えることが困難 ・流出時に情報の消去が困難 ・技術進歩によるなりすましリスクの増加の懸念（例：3D プリンタ等） ・盗取時に身体的リスクの懸念 ・本人の意図なしに個人識別が行われる懸念 ・副次的な身体情報（例：虹彩から薬物常習者の兆候が判明等）が取得される懸念 ・心理的抵抗感への配慮が必要 ・生体情報を読み取る機器が必要

「身体・行動情報」については、救急搬送時、高齢期（要介護期）、災害発生時（避難時）、死亡後等、所持や記憶による認証情報の提示が必ずしも期待できないリスク等発生時に、より効果を発揮することが見込まれるのではないか。

また、「身体・行動情報」による認証の精度の現状を踏まえ、導入する場合には、本人拒否又は他人受入により生じるリスクが低い手続・サービスにおいて、利便性を向上する観点から、検討することが適当ではないか。

２．複数の認証情報の組合せ

（１）基本的な考え方

各認証情報は、利用する場合の負担や利便性、情報保護上のリスクや利点、認証の精度等に差異があり、単独では、必ずしも認証が求められる多様な手続・サービスの要請に応えきれない。

このため、複数の認証情報を組み合わせることについて、利用者の利便性に対する配慮から実際の導入が進んでいるとは言えない状況にあるものの、一般的に必要性は認識されており、様々な手法が検討されている。

例えば、認証を求める利用者が本人であるかが疑わしい場合に、他の認証情報の提示を求めるというリスクベース認証という手法が考えられる。具体的には、利用者が通常利用している通信端末のアドレス情報などを把握しておき、異なる端末から認証が求められた場合については、追加的な認証情報の提示を求める方式が既に採用されている。

各認証情報の特徴を踏まえ、複数の認証情報を相互に組み合わせて補完し合い、認証の精度を強化（なりすましリスクを低減）して活用する複数要素認証が有効ではないか。

＜参考＞公的個人認証の電子証明書の場合

公的個人認証サービスの場合には、①電子証明書（秘密鍵）の「所持」と、②暗証番号（ＰＩＮ）という「知識」の２つの情報を用いており、①の紛失・盗難や②の不正入手のリスクを補完し合っている。

（２）認証情報の組合せ方

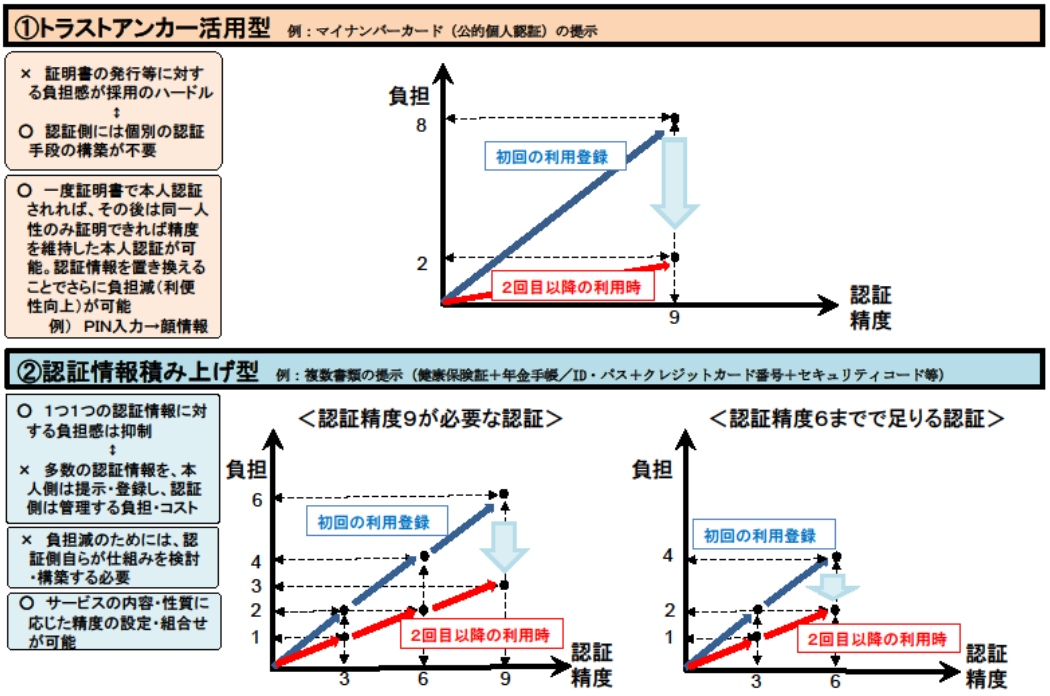
複数の認証情報の組合せ方として、①いわゆるトラストアンカー（信用の基点）となるような単独でも精度の高い認証情報を中核とし、他の認証情報を組み合わせて利用する方法（第３．２②で述べた、身分証など公的機関が発行する「証明」を用いる場合が主として該当。本報告では以下「トラストアンカー活用型」という。）、②単独では精度が高くはない認証情報を多数組み合わせて利用する方法（本報告では以下「認証情報積み上げ型」という。）の二つを大きく観念することができる。

①トラストアンカー活用型は、中核となる認証情報の精度を維持するためその取得時に一定の負担がある一方、認証側にとっては、自ら個別に認証手段を構築する必要がなく、認証情報を登録・管理する負担・コストを低く抑えることができる。さらに、一度証明書によって精度の高い本人認証が行われれば、その後は既に認証された者と同一人であることのみを証明することで、精度を維持したまま本人認証できるため、他の認証情報を用いて負担減（利便性向上）を実現することが可能となる。

②認証情報積み上げ型は、一つ一つの認証情報に対して利用者側が感じる負担感を抑えることができるが、組み合わせる認証情報が多くなる

ほど、本人側には提示・登録、認証側には管理のための負担・コストが必要となる。

（参考）認証情報の組合せ方（イメージ）



認証情報の組合せ方については、本人側の感じる負担感や認証側に生じるコスト等の特性を踏まえ、用いられる手続・サービスの内容や利用される場面に応じて、適切に選択することが必要ではないか。

（３）その他制度・仕組みとの組合せの可能性

各認証情報を利用する場合の負担や利便性、情報保護上のリスクや利点、認証の精度等の差異に対し、複数の認証情報を組み合わせることのほか、認証情報以外の手法を組み合わせることにより、補完することが考えられるのではないか。

例えば、認証において本人が拒否され、又は他人が受け入れられた結果生じた損害を事後的に補償・回復する保険類似の制度が考えられる。具体的に、クレジットカードにおいては、利用者が事後的に明細を確認することで不正を発見することができる仕組みを用いている。不正利用の完全排除に必要となるコストと、事後的に必要となる補償コストとの

バランスを適切に見込むことができれば、結果として、このような設計も想定可能と考えられる。

例えば、特に身体・行動情報に関しては、取り替えがきかず偽造リスクがあるが、特定の空間への入退所など、防犯カメラ等によって正しく本人が利用したか追跡できる利用環境を組み合わせることで、本人認証に用いることが考えられる。

本人側の負担軽減の観点から利便性の高い認証情報を用いつつ、認証以外の制度・仕組みや本人認証を行う利用環境を整えることによって、なりすましのリスクや被害の程度を抑制することも可能となるのではないか。

３．認証情報の保管方法と安全管理措置

認証情報については、①本人が所持する媒体に保管する場合（本報告では以下「本人媒体保管型」という。）、②外部サーバーに保管する場合（本報告では以下「外部サーバー保管型」という。）を想定することができる。

①本人媒体保管型であれば当該媒体を適正に管理する責任が個人側に発生し、②外部サーバー保管型であれば、当該サーバーを設置する側が安全管理措置を行うシステム上の責任を負うこととなる等の違いがある。

個人の利便性を重視すれば②外部サーバー保管型を検討してはどうかという議論があり得るが、一方、情報が流出した場合の被害の拡大について、①本人媒体保管型は当該媒体に紐付く範囲に限定可能、②外部サーバー保管型は当該サーバーに保管された全ての情報にリスクが及び得る等の違いがある。

例えば、指紋等情報をＩＣキャッシュカードに紐付けて管理する金融機関においては、①本人媒体保管型又は②外部サーバー保管型の方式の特徴を踏まえ、各金融機関の方針に沿った方式が採用されている。

認証情報の保管方法については、本人側や認証側の責任や負担、想定される被害の範囲等の特性を踏まえ、用いられる手続・サービスの内容や利用される場面に応じて、適切に選択することが必要ではないか。

とりわけ、外部サーバーに認証情報を登録する場合は、流出時の被害

を抑える、機微な個人情報をむやみに取得することを避ける、といった点に留意が必要ではないか。また、採用するとしても、本人が希望する場合に利用できる仕組みとすることが適当であり、オプトイン（利用に関して本人から事前に許諾を得ない限り行わない方式）・オプトアウト（本人から利用停止の意思表示があれば受け入れられる方式）の導入が前提ではないか。

第５．社会における具体的な認証場面への適用に向けて

第３.及び第４.に確認及び整理した本人認証の現状や特徴を踏まえ、Society5.0 社会における具体的な認証場面への適用の可能性について検討を試みる。

１．多様化・拡大する手続・サービスへの対応可能性

（１）本人認証が求められる場面の多様化・拡大

ＩＣＴを活用した「超スマート社会」において、インターネット等による手続・サービスが多様化・拡大することに伴い、認証が求められる場面もそれぞれ多様化・拡大していくことが見込まれる。

例えば、現在キャッシュレスが志向され、決済手続が簡素化されていくと見込まれるが、その前提として決済に必要となる本人認証の負担をいかに低く抑えるかが課題となり得る。利用登録時、決済口座等と本人を紐付ける際には精度の高い本人認証を行いつつ、決済場面ではより利便性の高い認証情報を用いることが必要となるのではないか。

また、例えば、自動運転や高度道路交通システム（ITS: Intelligent Transport Systems）の研究が進みつつあるが、完全自動走行によって免許を持たない者であっても自動走行車を操作することが可能となる場合にも、自動走行車の操作権限を有する者であることを確認するため本人認証が必要となるのではないか。この場合、本人とその操作権限の及ぶ車を紐付ける際には精度の高い本人認証を行いつつ、実際の操作場面ではより利便性の高い認証情報を用いることが必要となるのではないか。

いずれの場合にも、性質上、利用を開始する時点では精度が高い本人認証が必要であり、その高い信用度に基づき、利用場面では利便性の高い認証情報を組み合わせて用いることが可能となるのではないか。

（２）認証手段の多様化の可能性

手続・サービスの内容や利用される場面に応じて、様々な認証手段を用意しておく観点から、利用する認証情報を別の認証情報に置き換えることで利便性を向上することが考えられるのではないか。

例えば、現在広く活用されているＩＤ・パスワード方式のパスワードや公的個人認証のＰＩＮ（暗証番号）という「知識情報」について、別の認証情報に置き換えることで忘却のリスクを低減できる可能性がある。

現在使われているパスワードやＰＩＮという「知識情報」について、別の認証情報に置き換えることで利便性が向上し、多様化・拡大する手続・サービスへの対応可能性が広がることが期待できるのではないか。

（３）知識情報を置き換える場合の認証情報

知識情報を別の認証情報に置き換える場合、忘却・紛失のリスクがない身体・行動情報を用いることが考えられるのではないか。

身体・行動情報については、単独で 100%の認証は困難であるほか、取り替えが困難であり、仮に流出した場合、個人の情報を完全に保護できるかについては課題がある。

また、特に、指紋や虹彩などの通常視認できない身体・行動情報は、本来他人に知り得ない機微な個人情報であることから、利用者の間に心理的忌避感が生じうることについて相当の配慮が必要であると考えられる。この観点から、例えば、顔情報については、最も基本的な個人に関する情報であり、外部に示されたものであることから、他の身体・行動情報と比較して本人認証に用いることを検討する余地があると考えられるのではないか。

パスワードやＰＩＮという「知識情報」について、顔情報に置き換えることで、プライバシー保護に配慮しつつ、一定の本人認証が可能となるのではないか。

仮に顔情報を本人認証に用いることを検討する場合、偽造画像によるなりすましリスクがあるため、まずは完全に非対面での利用ではなく、本人が利用していることを物理的に確認できる特定の場所・空間での利

用を検討することが適当ではないか。

２．公的部門における認証場面への適用の可能性

（１）認証手段の選択に向けた視点

行政手続など公的部門における認証については、その性質上、高い精度を維持することが求められるが、技術の進展も踏まえつつ、利用者目線に立った利便性向上に継続的に取り組むことも重要である。その際、第３．及び第４．に確認及び整理した認証情報の現状や特徴を踏まえ、認証の精度と利便性の双方の確保の観点から、最適な手段を選択するという視点が不可欠である。

例えば、マイナンバーカードの利用者証明用電子証明書については、本人以外の公的主体が対面確認の上で発行する認証情報であり、本人が自ら設定するＩＤ・パスワードに比較して認証の精度が高い認証手段であるが、市町村窓口でマイナンバーカードを受け取る際などにあわせて発行するなどの方法をとれば、スマートフォン等の通信媒体を記録媒体とすることによって、認証の精度を維持しつつ利便性が向上するのではないか。結果として、現在ＩＤ・パスワードが広く使われている本人認証の場面において対応可能性が広がるのではないか。

例えば、マイナンバーカードの署名用電子証明書については、精度が高い本人認証に加えて、当該手続・サービスを利用する本人の意思確認を行うことが可能である点で、他の認証情報と別途の機能があるため、この機能を用いる必要がある手続・サービスについては、引き続き、署名用電子証明書の利用を維持する必要があるのではないか。

また、現在行われている認証手段について、１．の検討を踏まえた見直しを行うことにより、手続・サービスに応じ新たな認証手段を採用することが考えられるのではないか。

例えば、マイナンバーカードの電子証明書を事例として、ＰＩＮ入力を顔情報に置き換えることの可能性と意義について検討してはどうか。

（２）電子証明書についての事例検討

電子証明書についてＰＩＮ入力を行わない場合、それ単独では本人し

か持ち得ない電子証明書を「所持」していることの確認までが可能となるが、あわせて顔情報を認証情報として組み合わせれば、それぞれ単独で活用する場合とは異なる、新たな認証手段として仕組むことも可能となるのではないか。

具体的には、現在健康保険証で行っている医療保険資格の確認の場面に用いることにより、ＰＩＮ入力を行わずとも、①顔情報を通じ、顔写真のない健康保険証よりも精度の高い本人認証を行い、かつ、②電子証明書の情報と紐付けることにより、オンラインで円滑かつ確実に医療保険資格の確認を行う、という双方を実現できる可能性があるのではないか。なお、医療機関においては、認知症患者や意識不明の患者の利用が想定されるため、ＰＩＮ入力は負担となり得るという観点からも、この方式の実現が期待されている。

【医療保険資格確認】

（健康保険証 → 電子証明書（ＰＩＮなし）＋顔情報）

	本人側	認証側
利　便　性	（変化なし）※	「向上」※※
認証の精度	「向上」※※※	

※　本人側はいずれにしても券面又は電子証明書の記録媒体の持ち歩きが必要

※※　認証側は、医療保険資格についてオンラインで即時確認が可能となるメリット

※※※　顔写真がないことにより生じているなりすましは低減

また、正確な本人認証とオンラインでの即時かつ確実な資格・属性情報の確認が可能となるため、窓口での各種証明書請求や給付金請求などの場面に利用できるようになる可能性があるのではないか。

【各種証明書請求、給付金請求】

（身分証＋申請書 → 電子証明書（ＰＩＮなし）＋顔情報）

	本人側	認証側
利　便　性	「向上可能」※	「向上可能」※※
認証の精度	「向上する場合有」※※※	

※　本人側については、オンラインでの情報確認の結果、申請書記載等が省略できる場合は利便性が向上
※※　認証側については、オンラインでの情報確認の結果、自動交付・自動処理が行える場合は利便性が向上
※※※　顔写真がない身分証等での本人認証と比較すれば精度が向上

なお、認証に用いる顔情報について、本人が所持する記録媒体又は認証側のいずれに保管するかによって差異はあり、後者の場合には、本人側には登録の負担、認証側には管理の負担が生じ得ることに、十分留意する必要があるのではないか。

３．ＡＩその他の先端技術の活用可能性

社会生活において、個人が本人であることを証明して手続を行い、又はサービスを受ける場面は、主として対人の利用窓口において発生するものである。

例えば行政手続においても、転出入等の住民異動の届出から、各種給付金サービスを受けるための申請、登記申請に至るまで、いわゆる窓口業務こそ本人認証を前提とした多くの業務が集中していると言える。

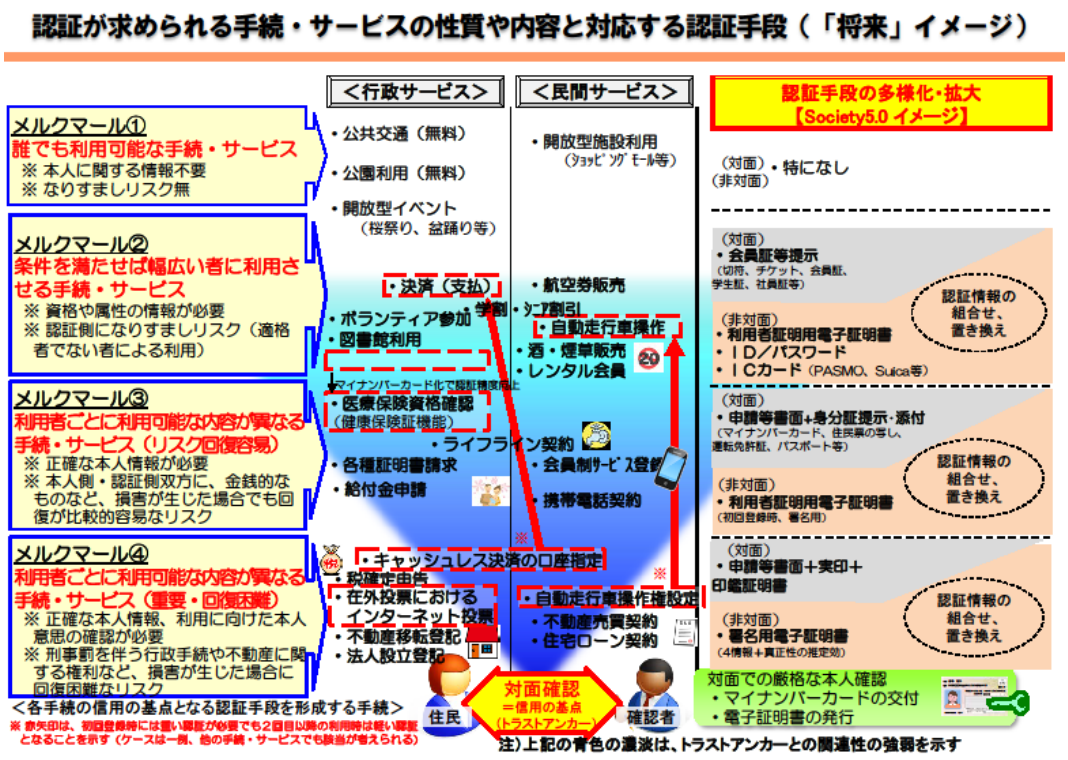
一方、人口減少に伴い、我が国全体で労働力が不足する中、行政においても職員と仕事の適切なマッチングが不可欠。職員・社員による対面での手続・サービスが基本であった、いわゆる窓口業務についても、官民問わず様々な業務改革が検討・実践されつつある。

プライバシーの観点に十分配慮する必要があるが、例えば、２.（２）のように、顔情報を認証情報として本人認証を行い、ＡＩ（機械学習技術）によって当該個人に最適な手続・サービスを分析、音声認識・応答技術を用いて音声で手続・サービスを案内することができれば、行政窓口のイノベーション（ＡＩ端末により、24 時間行政手続の実施等）を図ることが可能となるのではないか。

以上の観点と同様、ＡＩ、ＩｏＴ、ロボティクス等の各種技術と認証情報を提示するための各種技術を組み合わせることで、認証が必要となる手続・サービスそのものを構造的に改革できる可能性があるのではないか。

第６．おわりに

将来に向けて多様化・拡大する手続・サービスに応じ、どのような認証手段が最適かについて、網羅的に整理することは困難であるが、第５．までの確認及び整理の内容を踏まえた一つのイメージとして、以下を提示する。



今後、Society5.0 を見据えた個人認証基盤のあり方を模索するに当たり、総務省をはじめとする公的部門においては、まずは、第５．の２及び３に検討した事例の実現可能性について、更に検討を深めて頂くことを期待したい。具体的な検討及びその先の実践の過程において、また、日進月歩する技術の進展によって、各認証情報及びその組合せの持つ新たな可能性や課題が明らかになることが想定されるが、本報告がその検討の基礎的な視点を提供することを期待しているものである。