「Society5.0を見据えた個人認証基盤のあり方について」（報告）

概要版

本報告では、手続・サービスが多様化・拡大する「Society5.0」社会にふさわしい、誰でも手軽に負担感なく使える個人認証基盤について、以下を整理

1．本人認証が求められる手続・サービスと、これに対応する認証情報の種類と特徴、活用可能性

2．「Society5.0」社会における具体的な認証場面への適用可能性

全体構成

第1．趣旨
- 1．Society5.0を見据えて
- 2．個人認証基盤の検討に際して考慮すべき視点の整理

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
- 2．個人認証の基本的な概念
- 3．本報告の整理の対象

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
- 1．本人認証が求められる手続・サービスの現状
- 2．対応する認証手段の現状
- 3．手続・サービスに応じた最適な認証手段の選択可能性

第4．認証情報の利用についての検討
- 1．認証情報の種類と特徴、活用可能性
  - （1）知識情報
  - （2）所持情報
  - （3）身体・行動情報
- 2．複数の認証情報の組合せ
  - （1）基本的な考え方
  - （2）認証情報の組合せ方
  - （3）その他制度・仕組みとの組合せの可能性
- 3．認証情報の保管方法と安全管理措置

第5．社会における具体的な認証場面への適用に向けて
- 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
  - （2）認証手段の多様化の可能性
  - （3）知識情報を置き換える場合の認証情報
- 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
  - （2）電子証明書についての事例検討
- 3．AIその他の先端技術の活用可能性

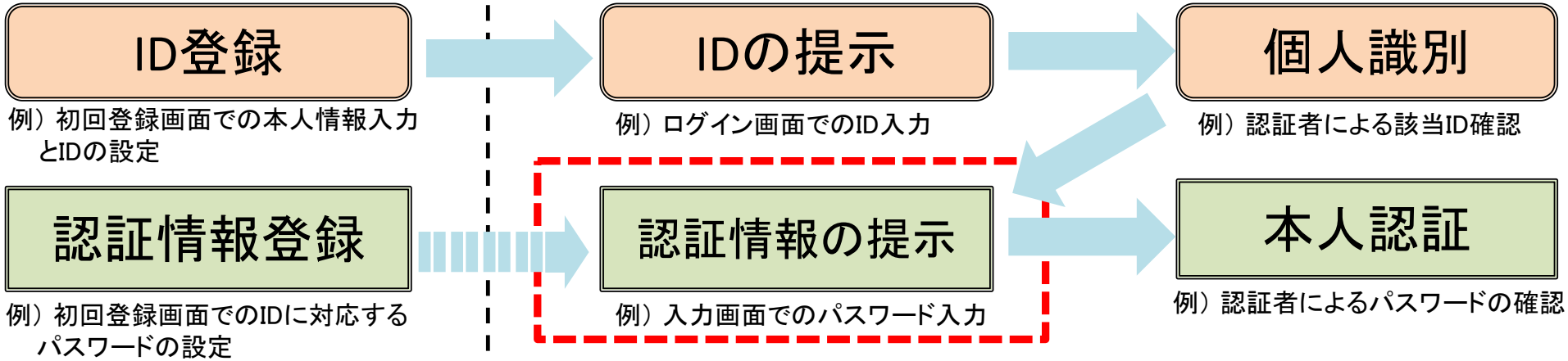
第6．おわりに

個人認証の基本的な概念（本報告のパラダイム設定）

○ 「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あり
○ ケースによって、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
→ 本報告は、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

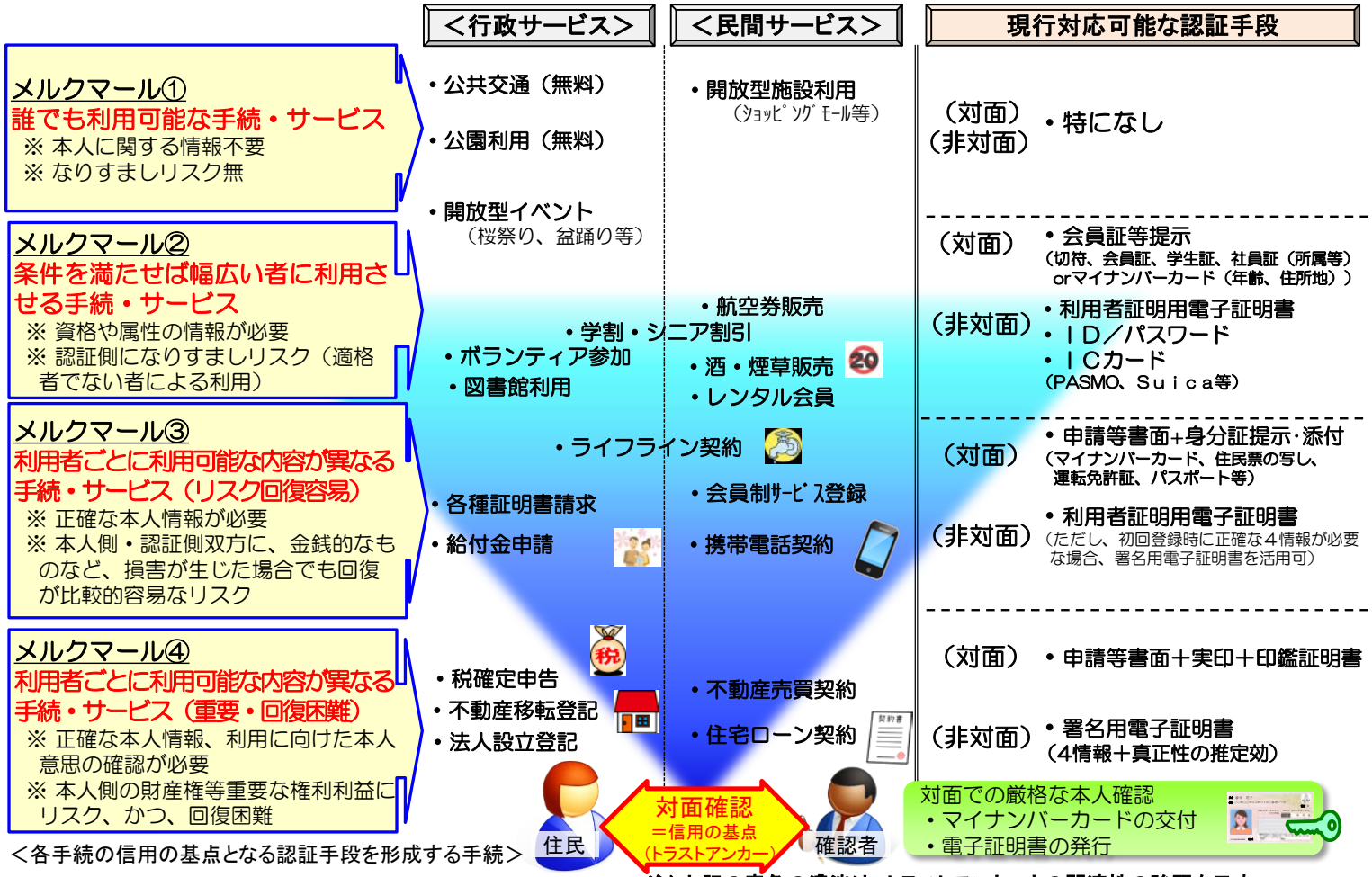
個人識別
（Identification）
個人から提示された識別情報（ID）を用いてデータベースの検索を行い、該当するIDが存在することを確認する（「1対nの照合」を行う）こと

本人認証
（Authentication）
「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



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

○　認証手段としての確実性を上げることと、利用者の利便性を上げることは、「トレードオフ」の関係
→　「トレードオフ」の関係を踏まえつつ、手続・サービスに応じて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
→　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、②精度の高い認証手段の利便性を向上、の2アプローチが考えられるのではないか



＜各手続の信用の基点となる認証手段を形成する手続＞

注）上記の青色の濃淡は、トラストアンカーとの関連性の強弱を示す

認証情報の種類と特徴

○ 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、必ずしも多様な手続・サービスの要請に対応困難

○ 例えば、身体・行動情報については、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。一方、持ち歩く必要がない等の利便性向上という点で意義はあるのではないか

→ 複数の認証情報を相互に組み合わせる複数要素認証が有効ではないか

認証情報		具体例	主たる特徴	
			利点	留意点
① 知識情報	本人しか知らない情報を持っていること	暗証番号、パスワード、質問応答 等	・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** 等	**・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 等
② 所持情報	本人しか持ち得ない情報が記録された媒体を持っていること	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	・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低い** 等	**・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** ・製造・設置コストが必要 **・情報を読み取る機器が必要** 等
③ 身体・行動情報	本人の身体・行動が持つ固有情報の差	筆跡、音声、顔、指紋、虹彩、静脈、行動パターン 等	**・持ち歩く必要がない** **・忘却・紛失がない** 等	・現状では**100%の認証は困難** ・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 等

認証情報の組合せ方

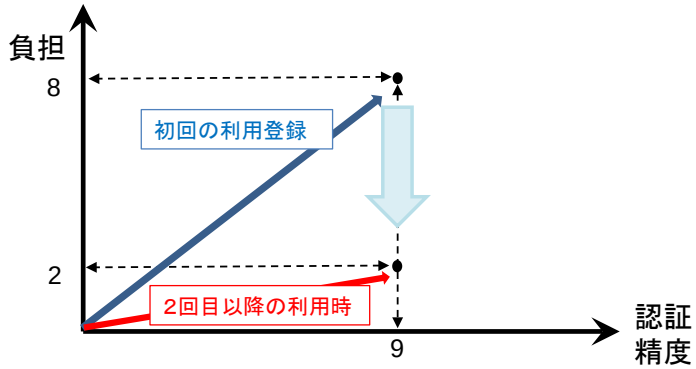
○　証明書等を活用する①トラストアンカー活用型は、証明書の発行等に対する負担感がハードルだが、認証側には個別の認証手段の構築が不要。証明書で一度本人認証されれば、その後は認証された者と同一人であることのみを証明すれば精度を維持したまま本人認証可能となるため、認証情報を置き換えることで負担減（利便性向上）が可能

○　②認証情報積み上げ型は、一つ一つの認証情報について利用者の負担感を下げ得るが、組み合わせる認証情報が多くなるほど、本人側には登録、認証側には管理の負担が発生

①トラストアンカー活用型　例：マイナンバーカード（公的個人認証）の提示

× 証明書の発行等に対する負担感が採用のハードル
↕
○ 認証側には個別の認証手段の構築が不要

○ 一度証明書で本人認証されれば、その後は同一人性のみ証明できれば精度を維持した本人認証が可能。認証情報を置き換えることでさらに負担減（利便性向上）が可能
例） PIN入力→顔情報



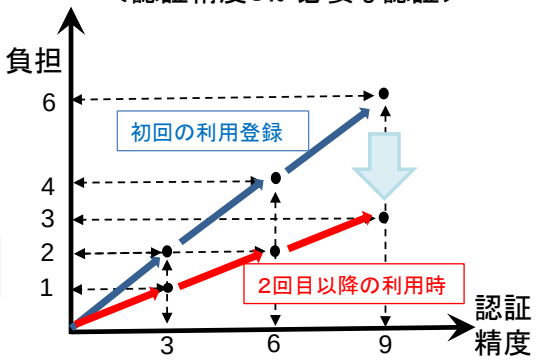
②認証情報積み上げ型　例：複数書類の提示（健康保険証＋年金手帳／ID・パス＋クレジットカード番号＋セキュリティコード等）

○ 1つ1つの認証情報に対する負担感は抑制
↕
× 多数の認証情報を、本人側は提示・登録し、認証側は管理する負担・コスト

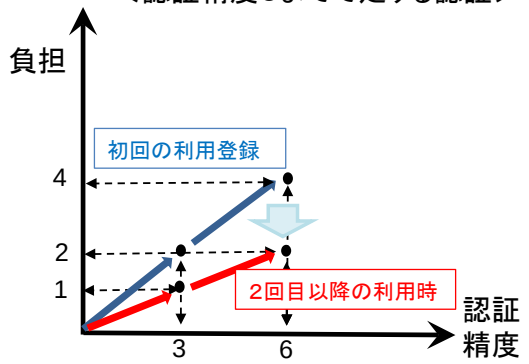
× 負担減のためには、認証側自らが仕組みを検討・構築する必要

○ サービスの内容・性質に応じた精度の設定・組合せが可能

＜認証精度9が必要な認証＞



＜認証精度6までで足りる認証＞



認証手段の多様化の可能性（認証情報の置き換え）

○　利用する認証情報を別の認証情報に置き換えることで、利便性が向上する可能性
→　例えば、パスワードやPIN（暗証番号）を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

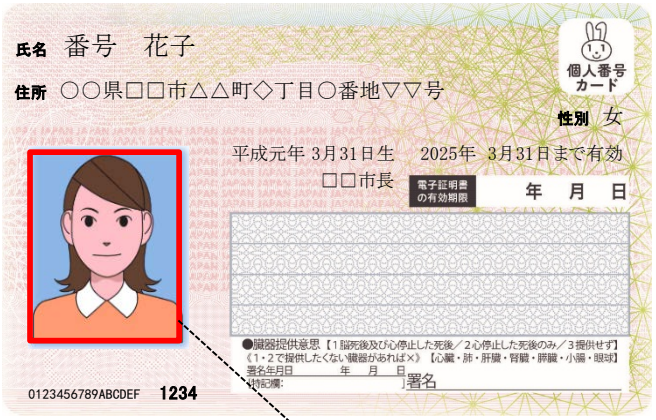
【マイナンバーカード（現行）】

①PIN入力
（＝「知識情報」）

②電子証明書所有
（＝「所持情報」）

忘却リスク減

【マイナンバーカード（PIN入力を行わない場合（案））】



PIN入力不要

認証情報の置換

①顔情報
（＝「身体・行動情報」）

②電子証明書所有
（＝「所持情報」）
※PIN入力は行わない

・　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

（事例検討）電子証明書（ＰＩＮ入力不要）

○　電子証明書のPIN入力を行わない場合も、顔情報との組合わせで新たな認証手段が可能
→　例えば、PIN入力を行わずとも、①顔写真のない健康保険証より精度の高い本人認証、②オンラインでの円滑・確実な医療保険資格の確認、の双方が実現できる可能性があるのではないか

【健康保険証】

本人（被保険者）　2020年○月○日交付

△△△△保険組合
被保険者証　記号 1234　番号 1234567

氏名　番号　花子
生年月日　平成元年3月31日生　性別　女
資格取得年月日　平成25年4月1日

発行機関所在地　東京都千代田区○○○

保険者番号　88888888
名称　△△△△保険組合　印

【マイナンバーカード（PIN入力を行わない場合）（案）】

＜現行＞

①券面所有
（＝「所持情報」）

＜認証情報の組合せ、置換（案）＞

認証精度向上

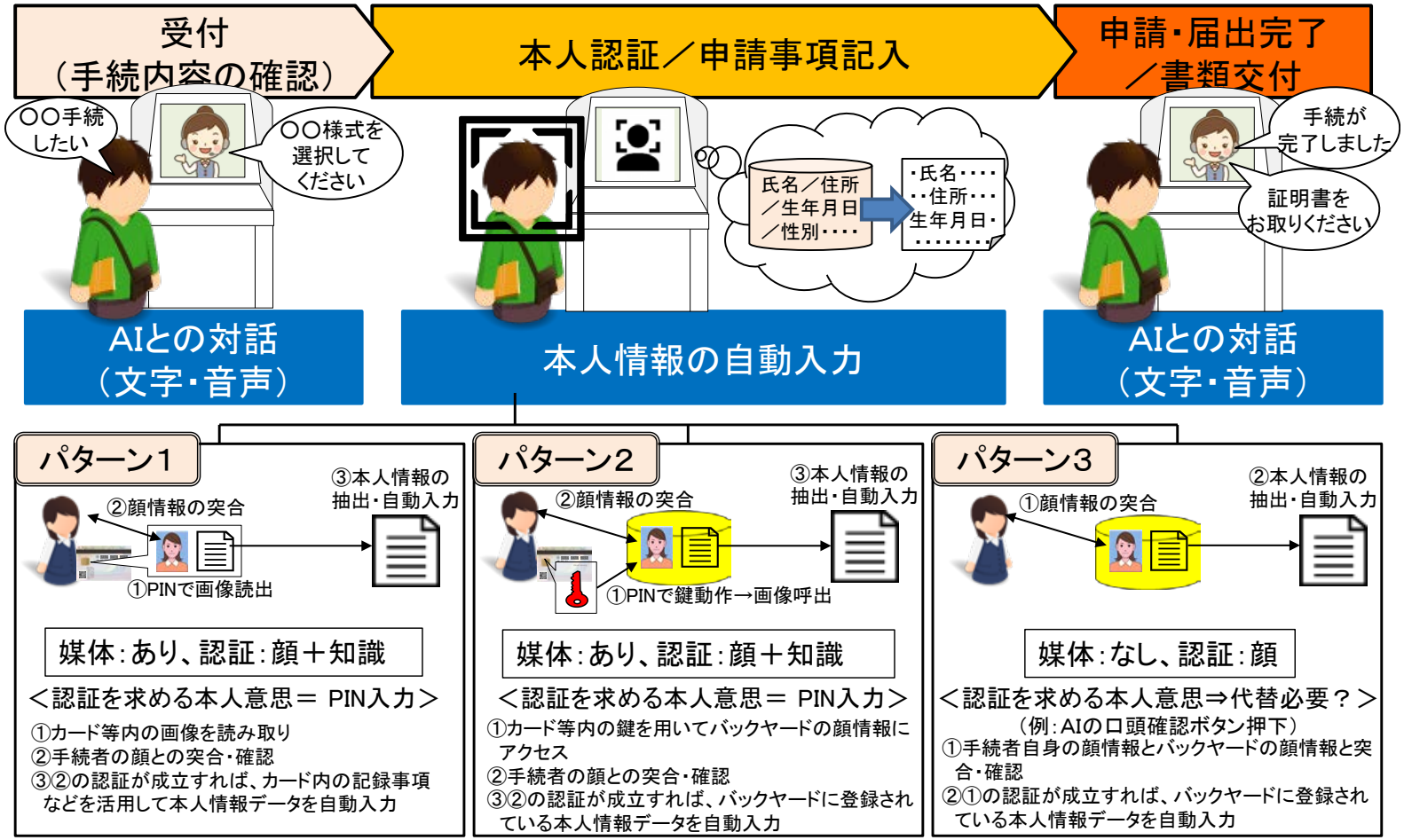
①顔情報
（＝「身体・行動情報」）

オンライン資格確認
（利便性向上）

②電子証明書所有
（＝「所持情報」）
※PIN入力は行わない

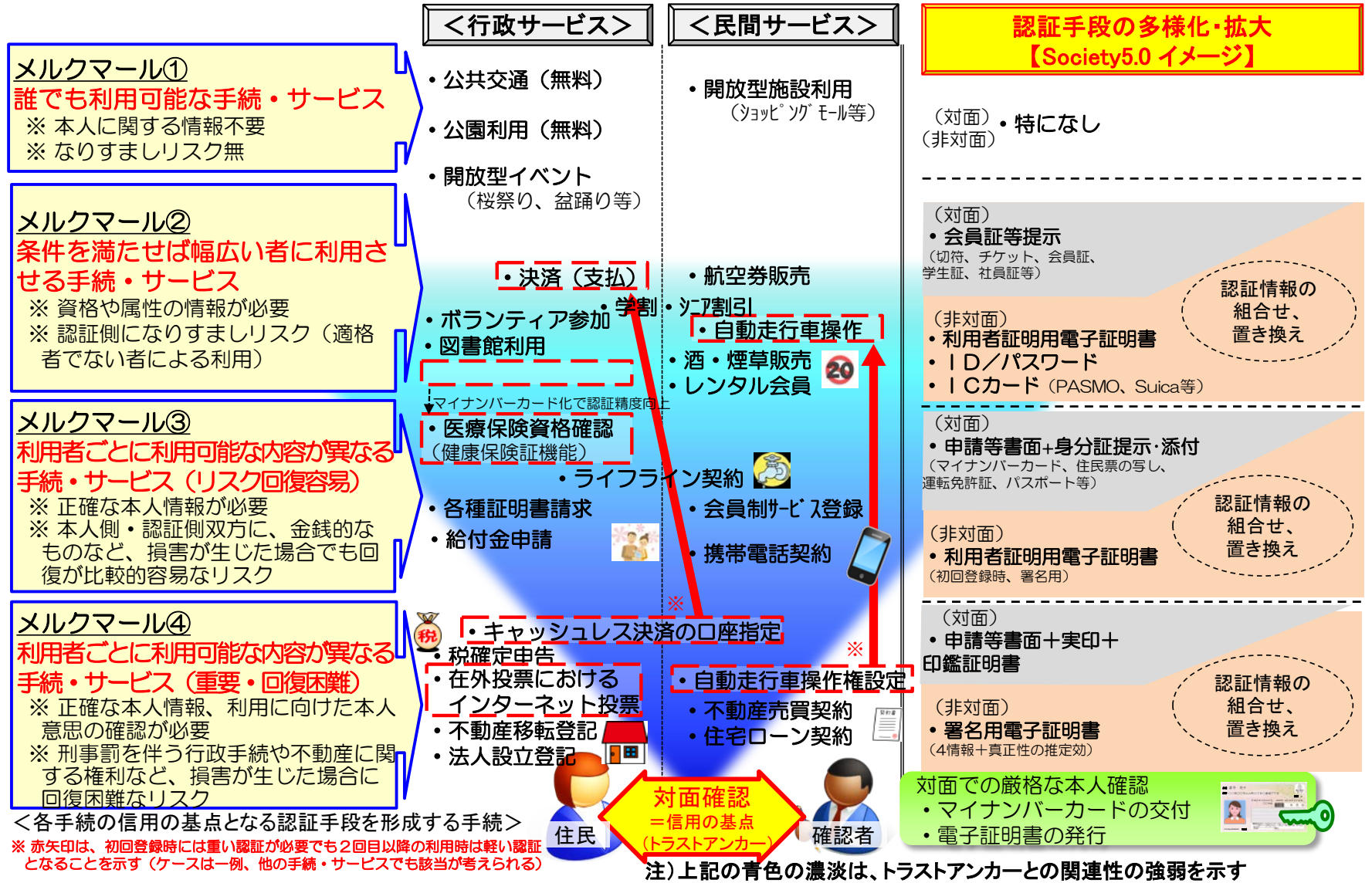
ＡＩその他の先端技術の活用可能性

○　本人認証は、主として対人の利用窓口において発生（例：行政手続における窓口業務）
○　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。対面が基本であった窓口業務についても、様々な業務改革が検討・実践
→　例えば、顔情報による本人認証とAIによる分析等を組み合わせ、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）が可能となるのではないか



認証が求められる手続・サービスの性質や内容と対応する認証手段（「将来」イメージ）

○　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。これまでの本懇談会での議論を踏まえた一つのイメージを図示



＜各手続の信用の基点となる認証手段を形成する手続＞

※ 赤矢印は、初回登録時には重い認証が必要でも２回目以降の利用時は軽い認証となることを示す（ケースは一例、他の手続・サービスでも該当が考えられる）

注）上記の青色の濃淡は、トラストアンカーとの関連性の強弱を示す