次期個人番号カードタスクフォース
中間とりまとめ

現行の個人番号カード（以下「現行カード」という。）は、平成 28 年(2016 年) 1 月に発行が開始されて以来、約 8 年が経過した。次期個人番号カードタスクフォースは、次期の個人番号カード（以下「次期カード」という。）について、デジタル社会の実現に向けた重点計画（2023 年 6 月閣議決定）に基づき検討を行い、中間とりまとめを作成した。

約 7 割の国民が保有するまで普及した個人番号カードは、対面でも非対面でも本人確認に用いることのできるデジタル社会のパスポートであり、官民のオンライン・デジタル化の基盤となるものである。その利用シーンの拡大として、健康保険証や運転免許証をはじめとする各種カードとの一体化や、各種行政手続のオンライン・デジタル化、図書館カード等として利用できる市民カード化、民間サービスにおける顧客申込等における利用が進められ、また、カード機能のスマートフォンへの搭載をはじめ、利便性向上の取り組みが進められており、個人番号カードを基盤とした安全で便利なデジタル社会の実現が期待される。技術進展に対応して個人番号カードの安全性を確保するとともに、国民にとってより利便性が高く魅力的な個人番号カードとなるよう、次期カードのあるべき姿について、検討を行った。

１．カードの機能向上に向けた重点的対策項目

(1)カードの券面記載事項

①氏名、生年月日、住所の 3 情報及び顔写真

券面の氏名、生年月日、住所、顔写真の記載については、現在、官民の様々な場面において、カードが対面での本人確認書類として利用されており、その際必要な情報となるため、次期カードでも、券面に氏名、生年月日、住所、顔写真を記載する。

また、一方で、券面に記載する 3 情報、顔写真に加え、性別及びマイナンバーを含めた券面記載事項等について、カードの提示を受ける者が確実に確認を行い、かつ効率的に登録できるようにするため、カードの IC チップに記録された券面記載事項等をスマホ等により個人情報保護に配慮しつつ、使いやすい UI で読み取ることができるアプリを国が開発し、無償で配布する。

また、住所や氏名を引き続き券面記載事項とすることにより、追記欄が満欄となり来庁する負担が国民に発生するという課題に対しては、追記欄を拡大することにより対応する（⑥参照）。

②性別

券面の性別の記載については、次期カードにおいては、以下の理由から IC チップに性別の情報を記録した上で、性別を券面に記載しないこととする。併せて、IC チップに記録した性別の情報を必要な者が負担なく読み出すことができるよう、スマホ等により個人情報保護に配慮しつつ、使いやすい UI で読み取ることができるアプリを

国が開発し、無償で配布する（①のアプリと同一のアプリ）。

・ 健康保険証と同様の配慮（希望する者についてうら面に記載）を求める要望があること。（なお、カードの健康保険証としての利用においては、性別を券面に記載しないこととしても、医療機関等でオンライン資格確認等システムにより性別を確認することができる。）
・ 引き続き IC チップに性別の情報を記録し、読み取りアプリの無償配布が行われれば、問題は生じないとの調査結果が得られたこと。

③マイナンバー

現在、マイナンバーは券面（うら面）に記載されているところ、各機関にマイナンバーを提供する際、自身のマイナンバーを券面で確認して記載や入力を行う場面が今後も多数想定されることや、カードをコピーする運用が今すぐには無くならず、支障が生じるおそれがあることにかんがみ、次期カードにおいても、うら面にマイナンバーを記載する。

一方で、性別及びマイナンバーを含めた券面記載事項等について、カードの提示を受ける者が確実に確認し、効率的に登録できるようにするため、カードの IC チップに記録された券面記載事項等をスマホ等により個人情報保護に配慮しつつ、使いやすい UI で読み取ることができるアプリを国が開発し、無償で配布する（①のアプリと同一のアプリ）。

また、紛失時等にマイナンバーを見られることに対する不安に対しては、マイナンバーが他人に見られたとしても、マイナンバーだけでシステムへのアクセスや行政手続の申し込み等は一切できないため、個人情報を盗取されたり、給付金を詐取されるなど、損害を被ることはないことの周知に努める。

④通称・旧氏

現在、外国人住民の通称や日本人住民の旧氏については、希望者は住民票に記載でき、住民票に記載された場合、カードにも必ず記載される。

これらは、社会生活上用いられていることから、住民票に記載することが可能とされており、住民票に記載した場合には、同一人性を特定しやすくするため、本人確認書類としてのカードにも記載されているものである。このことにかんがみ、次期カードも同様の取り扱いとする。

⑤その他記載事項（生年月日西暦併記、氏名フリガナ、氏名ローマ字）

氏名のフリガナについては、戸籍法・住民基本台帳法・番号法が改正され、戸籍の記載事項・住民票の記載事項・カードの券面記載事項とされ、今後、次期カードを待たず現行カードから、券面に記載される予定である。また、生年月日の西暦と氏名のローマ字については、希望者に対し、今後、次期カードを待たず現行カードから、追

記欄に記載される予定である。

次期カードにおいては、氏名のフリガナについては、当初から券面に記載される。また、生年月日の西暦については、次期カードでは追記欄ではなく、本欄の和暦に置き換えて記載することを検討する。そして、氏名のローマ字についても、次期カードでは追記欄ではなく、本欄の漢字等と併せて記載することを検討する。

⑥追記欄

追記欄については、おもて面に設けられ、引越等による新住所の追記など券面の変更内容の記載に活用されていることから、次期カードにおいても存置する必要がある。なお、うら面に設けるという案については、現在、様々な場面において様々な者が本人確認のためにおもて面を利用しているところ、うら面も必ず確認する必要が生じ、また、うら面にはマイナンバーが記載されていることから、次期カードでも追記欄はおもて面に設けるべきである。

一方で、追加欄を拡大することで、追記欄が満欄となり来庁する負担が国民に発生するという課題に対応する。なお、拡大のため、現在、おもて面にある臓器提供意思表示欄について、次期カードではうら面に設けることを検討する。うら面に設けることにより、臓器提供意思表示欄の拡大も可能となり、欄が小さく記入が難しいという課題にも対応できる。

⑦券面デザイン

券面記載事項等の変更と合わせて、偽造防止対策、ユニバーサルデザイン対応、視覚障害者への配慮等（カードのおもて裏識別対応など）を踏まえ、券面デザインの見直しを行う。

特に、大きさをはじめ、文字の読みやすさに配慮するとともに、誰もが持ちたくなる魅力的なデザインを実現する。

⑵カード等に用いる技術

①暗号方式の在り方

電子証明書の有効期間（5 年）をカード本体の有効期間にあわせ、10 年に延長する。

その前提として、10 年の有効期間に耐えうる強固な暗号方式に移行する。（公開鍵暗号方式について ECDSA 384（192 ビットセキュリティ）、ハッシュ関数について SHA-384（192 ビットセキュリティ））

なお、18 歳未満の場合は現行どおりカード本体並びに電子証明書の有効期間とも 5 年とする。

また、カードの仕様としては 256 ビットセキュリティの暗号方式（公開鍵暗号方式について ECDSA521、共通鍵暗号方式について AES256、ハッシュ関数について SHA-512）に対応できるものの採用を検討することとし、共通鍵暗号方式での GCM 対応に

ついては、Global Platform 仕様等の標準規格では採用されておらず、将来的な課題として検討する。

なお、電子証明書の有効期間を 10 年とした場合、認証局の自己署名証明書の有効期間は 20 年となり、2050 年までの有効期間となることが想定され得るところ、将来的な PQC（耐量子計算機暗号）の採用を否定するものではなく、万が一移行後に 2050 年より前に暗号方式が危殆化する見込みが生じた場合には、有効期間の 20 年を待たず、新たな暗号方式への移行を検討する。

②暗証番号の入力のユーザー利便性向上

現行カードでは、公的個人認証サービス、券面事項入力補助、といった目的別に、４つのアプリケーション（AP）が IC チップに搭載されている。次期カードでは、諸外国 eID カードの事例を参考に、暗証番号の入力を必要とする機能を集約した AP（(仮称）認証 AP）と、券面記載事項等を照合番号の入力により確認・取得できる AP（(仮称）券面等 AP）の２つに再編を行う。なお、再編により、新旧カードで AP の構成が異なることとなるが、構成を変えるだけで機能は同様とすることで、利用者の端末側の対応の負担が発生しないようにする。

この再編により、カード保持者は、現在、４つの暗証番号の設定が必要であるところ、次期カードでは、４桁と６桁以上の２つの暗証番号の設定で済むこととなる。また、署名用の６桁以上の暗証番号により、券面事項入力補助データもアクセス可能とすることで、署名の際に別途４桁の暗証番号の入力を重ねて求める負担を解消する。さらに、現行カードにおける読み取りにくく桁数が多い照合番号について、諸外国の eID カードの事例を参考に、次期カードでは６桁で読み取りやすい照合番号とする。なお、住民基本台帳事務データは、現行カードと同様、次期カードでも住民基本台帳事務に係る専用端末のみアクセス可能とする。また、署名用の暗証番号は、現在の６～16 桁の英数字を維持し、高い認証強度を次期カードでも維持するとともに、署名を行わない場合には６桁以上の暗証番号の入力を求めない（券面事項入力補助のみ必要である場合には４桁の暗証番号の入力を求める）ことを徹底する。

③J-LIS マイナンバー関係システムの刷新

次期カードの仕様の取り込みにあたっては、多くの個人番号カードの発行や利用に係る関連システムにおいて改修が生じる見込みであり、改修内容や改修スケジュールの整合確保が必要である。また、次期カードの対応を機に、より効率的なカード管理システム及び JPKI システムへの刷新が必要である。

(3)カード発行体制

①カードの速やかな発行体制

約７割の国民がカードを保有している現状にかんがみ、以下の運用上の工夫によっ

て計画的な更新を進めることにより、実質的に支障が出ないようにする。

- 現行カードでは、有効期限の３ヶ月前から更新申請が可能であるところ、次期カードでは、余裕を持って更新できるよう、さらに前から更新申請を可能とする。
- 現行カードでは、有効期限は 10 回目の誕生日（18 歳未満は５回目の誕生日）であるところ、誕生日が近くなってから更新の必要性に気づくことがあるため、次期カードでは、運転免許証と同様に、10 回目の誕生日（18 歳未満は５回目の誕生日）の一定期間後を有効期限とする。なお、誕生日のカウントにあたり、運転免許証と同様、誕生日前に更新した場合は直後に迎える誕生日をカウントに含めないものとする。

有効期限が迫っている場合の申請も含め、更なる発行時間の短縮については、費用対効果の観点も踏まえて検討する。

②更新の在り方

ア　個人番号カード自体の更新（10 年目）について

10 年目の更新時における本人確認の実施方法について、これまでの郵便局の活用における法的整理を踏まえた郵便局の活用の推進も含め、制度的な検討を継続する。

イ　現行カードにおける電子証明書のオンライン更新

現行カードの電子証明書の有効期限は５回目の誕生日であり、次期カード導入までの間、約 5,000 万枚以上の現行カードの電子証明書の更新が必要になることを踏まえ、市町村窓口や郵便局での更新体制の整備を推進するとともに、電子証明書に要求される身元確認保証レベル及び制度面・システム面の手当てについて整理し、オンライン更新などの市町村の窓口負担の軽減方策について更に検討を進める。

⑷公証名義

個人番号カードは、市町村長が、当該市町村長が備える住民基本台帳に記録されている者に交付するとされていることから、現行カードには交付主体である住所地の市町村長名が記載されている。次期カードでは、国の保証の下に発行されていることを明確化するため、券面に「日本国 JAPAN」の記載等を行うことを検討する。

２．その他重要論点

⑴次期カード発行直前に発行されるカードの電子証明書の扱い

現行カードの電子証明書に用いられる暗号アルゴリズム（RSA2048）は 2031 年１月１日以降利用不可とされているが、このスケジュールでの次期カードへの移行完了は困難と考えられる。CRYPTREC では当該基準の見直しを少なくとも５年毎に行うことになっており、次の見直しのタイミングは 2026～2027 年頃と予想されるため、状況によっては利用延長に向けた相談等の検討を行う必要がある。

なお、その場合においても、可能な限り速やかに新暗号への移行を図るため、次期カ

ード導入時期以降、現行カードの電子証明書の更新の際には、電子証明書の更新ではなく、次期カードの取得を推奨する（電子証明書の更新を案内する時期に、電子証明書の更新を案内するのではなく、交付申請書を送付して、次期カードの取得を勧奨する等（※））。

※現行の RSA2048 による電子証明書の利用がどの程度の期間許容されるかを判断し、具体的な対応案を検討する。

(2)新旧カードの切り替えに伴うカード利用機関等への影響

以下の理由により、カードに新旧の暗号を搭載するのではなく、利用者の端末側のソフトウェアの対応で、新旧両方の暗号を扱うことができることとする。

- 次期カードにおいて新旧の暗号を扱う場合、IC チップに格納すべきデータが大きく増大し、当該格納データを格納するための IC チップの用意も困難となる。また、新規発行や更新の際の所要時間の増大も懸念される。
- 一方、利用者の端末側のソフトウェアの対応については、主要なユースケースである健康保険証利用やコンビニ交付においては、ハードウェアを変えずにソフトウェアの更新で対応可能であることが確認でき、その他の場合にも概ねソフトウェアでの対応が可能であると考えられる。

また、その場合に、利用者の端末側の対応の負担を減らすため、新暗号に対応したライブラリ（利用者クライアントソフト）の提供等、利用者を支援する方策を検討する。

(3)IC チップの空き容量

現在の製品状況を参照すると、IC チップのメモリ容量の増加は困難であると推察される。一方で、新暗号方式への移行による鍵データ及び署名データのデータサイズ見直しや、AP の再編による各 AP に設定されていた暗証番号やアクセス制御設定等の統合により、一定のメモリ容量の節約を実現する。また、搭載アプリの個数など、メモリ容量の節約について検討する。

(4)ISO 認証（現在、ISO/IEC15408 の CC 認証を取得）

個人番号カードの電子空間内での最も信頼できる本人確認書類という位置づけから、現行カードにおいて取得している ISO/IEC15408 の CC（Common Criteria）認証の取得は、次期カードにおいても必須である。

なお、仕様変更に伴い、カード自体の CC 認証の取得申請を行う前に、個人番号カードの PP（Protection Profile）の CC 認証を取得し直す必要がある。仕様確定後、実際のカード自体の CC 認証取得が完了するまでに 1 年半～2 年程度が見込まれ、CC 認証取得作業と並行してカード製造に着手する場合、認証作業中の評価結果によっては、カード製造の遅延につながるような影響を与える事態が生じることもあり得、これらを念頭にスケジュールを見込むべきである。また、こうした CC 認証取得期間を短縮する方策として、

CC 認証取得時の事前相談の活用等について検討する。

さらに、今後の CC 認証は有効期限が 5 年間となることから、有効期限を延長するための再評定申請作業についても考慮に入れる必要がある。

(5)IC チップの顔写真カラー化等（現在、白黒で、容量も小さい）

現行カードの仕様においても顔認証の利用に大きな支障が生じていないことから、必ずしも顔写真カラー化は必要ではなく、そもそもチップ容量を勘案してもカラー化は困難と考えられるため、引き続き白黒のデータを格納することとする。一方で、顔写真の撮影条件こそが認証精度に大きな影響を及ぼすことから、申請時に添付する顔写真の撮影基準の明確化や申請時の顔写真の品質チェック強化等の徹底について検討する。

(6)カードの磁気ストライプ（現在、JIS 規格の磁気ストライプを実装）

現在、磁気ストライプを活用し、カードを図書館カードや印鑑登録証として活用している自治体があることや、将来的に、個人番号カードを銀行のキャッシュカードとして使う場合には、磁気ストライプを残すことが必要であることから、磁気ストライプの搭載を継続する。

(7)PUK（PIN UNLOCK KEY）の発行（海外で採用例が多い）

暗証番号がロックされた場合の備えとして、次期カードにおいては、希望者は、有効な電子証明書を使って PUK（PIN UNLOCK KEY）を設定できるようにし、4 桁の暗証番号について、ロックがかかった場合に、PUK を使用してマイナポータルアプリで暗証番号のロック解除と暗証番号の再設定ができるようにし、市町村窓口へ赴く負担を解消する。

(8)カード本体の真贋性判定機能の追加

(9)JPKI アプリの真贋性判定機能の追加

次期カードで設ける（仮称）認証 AP（1.(2)②参照）において、デバイス認証を行うための内部認証鍵を設け、デバイス認証を必要とする機関に内部認証鍵に対応した公開鍵を配付する方向で対応し、カードやアプリの真贋性判定機能の追加を実現する。また、個人番号カードの真正性を確認することができるセキュアメッセージング機能を必須とする対応も行う。

(10)電子証明書の失効理由の細分化

電子証明書の失効理由の一つである「affiliationChanged」において「死亡」の細分を設けることについては、国際標準と異なることとなり、個人情報保護の観点の検討も求められることから、難しいと考えられる。一方で、「affiliationChanged」に含まれる「海外転出」が、令和 6 年 5 月以降、失効理由でなくなることにより、「affiliationChanged」にお

ける大宗は自然と「死亡」となる。このことについて生保会社等をはじめとする署名等検証者に対して周知し、公的個人認証サービスを活用いただくことにより、そのサービスの向上や事業効率化に寄与する。

(11)個人番号カードの呼称の変更

民間事業者が公的個人認証サービスを活用する場合をはじめ、マイナンバーを利用しないカードの活用法も現実には多くあるが、こうしたケースにおいてもマイナンバーが利用されていると誤解されたり、マイナンバーの利用とカードの利用とが混同されたりする主な原因の一つとして、マイナンバーカードという呼称があると考えられる。こうした混乱を回避するとともに、国民に親しまれるカードとするため、次期カード導入を契機に、「マイナンバーカード」以外の新たな呼称を、広く国民への公募も経て検討することが有意義であると考えられる。

(12)インターフェイス仕様の公開

次期カードを利用する際のインターフェイス仕様（APDU 仕様書）について、以下の理由により、安全性の確保を前提に、これを公開する。

- カードの APDU は JIS、ISO 準拠であること。
- APDU 仕様書は通常公開されていること。
- 公開されることで、カード利用端末の開発が容易となり、カードの利活用が進むこと。
- 認証やアクセスコントロールによりセキュリティが守られていることや、CC 認証により IC カード製品の安全性が認証されれば、仕様を公開したとしてもセキュリティに問題が生じるとは考えにくいこと。

(13)（長期的論点）将来的な物理カードの必要性

令和５年５月にスマホへのカードの電子証明書の搭載が開始された。スマホ搭載が実現しても、カードの普及利活用の推進は、以下の観点からなお重要である。

- スマホを保有していない国民はまだ多いこと。
- スマホのライフサイクルは概ね５年程度と短いこと。
- カードを基盤にスマホ搭載の仕組みを設計することで、完全オンラインで効率的な仕組みが実現できていること。

一方で、カード自体の不要化については、その利便性の確保も含め中長期的な課題として、引き続き検討を続ける。

また、スマホ搭載を進めれば、スマホの生体認証等を活用する等により利便性が高まり、カードの常時携行も不要となるため、個人番号カードの機能が格段に使いやすくなり、官民のオンライン・デジタル化の進展が期待できる。その普及を進めるとともに、その改善

についても、以下の事項等について、今後検討を行う。

- スマホ用電子証明書発行の 24 時間対応
- カード用電子証明書を再取得した際により簡便にスマホ用電子証明書を再発行・更新できる仕組み
- 個人番号カードの電子証明書機能以外（券面事項入力補助 AP 機能等）のスマホへの搭載

(14)その他重要論点　JPKI 暗号化機能の追加について

現在、政府、自治体、医療分野において親展郵便で送られている情報を、受信者本人のみが復号可能な状態に暗号化して電子的に送ることを実現する「JPKI 暗号化機能」を次期カードにおいて実装することについては、その必要性、コスト、実現方式などについて、引き続き検討する。