次期個人番号カードタスクフォース
中間とりまとめ概要

デジタル庁
Digital Agency

中間とりまとめ概要 ①

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、顔写真は、官民様々な場面で利用されることから、現行どおり記載する。

② 性別は、引き続きICチップに性別の情報を記録すれば問題は生じないとの調査結果が得られたことから、次期カードにおいては、 ICチップに性別の情報を記録した上で、券面に記載しないこととする。

併せて、スマホ等を通じ、ICチップから性別を含む４情報、マイナンバー等を読み取れるアプリを国が開発し、無償配布する。

③ マイナンバーは、各機関にマイナンバーを提供する際にカードが活用されると考えられることから、券面記載は現行どおり、券面（裏面）に記載する。

④ 通称・旧氏は、個人番号カードが住民票に記載された者に交付される本人確認書類であること等に鑑み、現行どおり（住民票に記載された場合、カードにも記載。）とする。

⑤ その他の記載事項については、今後、現行カードから、氏名のフリガナが券面記載事項に追加される予定であり、また、希望者に対し、生年月日の西暦と氏名のローマ字とが、追記欄に記載される予定である。次期カードにおいてさらに取り組みを進め、券面記載事項の生年月日を和暦から西暦に変更するとともに、氏名のローマ字を追記欄での対応から券面に記載することについて、検討する。

⑥ 追記欄を拡大する。併せて、現在、おもて面にある臓器提供意思表示欄について、追記欄の拡充の観点から、裏面への配置の可能性について、検討する。

⑦ 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を踏まえ、券面デザインの見直しを行う。特に、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。

現行のマイナンバーカード（おもて面）

現行のマイナンバーカード（うら面）

中間とりまとめ概要 ②

（２）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。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は５年とする。

・ 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））

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ECDSA 521、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。

中間とりまとめ概要 ③

② 暗証番号の入力のユーザー利便性向上等

・ 電子証明書や券面記載事項の入力等のために搭載されたアプリケーション（AP）の再編を行う。再編後のAPの名称についても、検討する。

現行カード： ４つのAPが搭載され、カード保有者は４つの暗証番号の設定が必要。

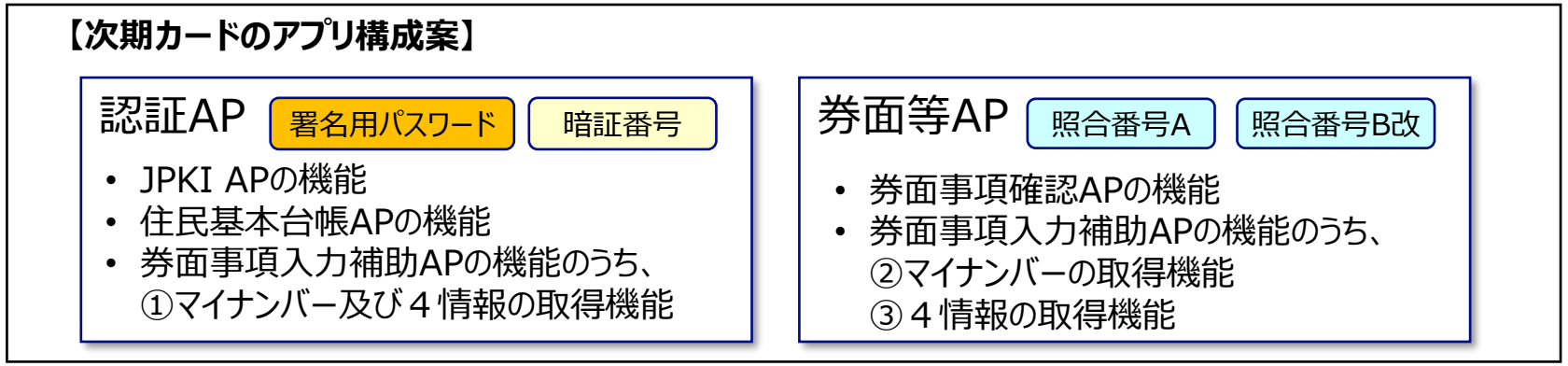
次期カード：APを下の２つに再編する。これにより、暗証番号は２つになる。

（仮称）認証AP： 暗証番号の入力を必要とする機能を集約したアプリケーション

（仮称）券面等AP：カード券面に印字された照合番号の入力により券面記載事項等を確認・取得できるアプリケーション

・ これに伴い、暗証番号の設定・入力の負担軽減、照合番号の合理化等を実現する。

（署名用の暗証番号の照合に成功した場合、４桁の暗証番号の照合を不要とする等の変更を実現）



・ なお、将来的には、スマホの生体認証等を活用する等により、暗証番号を不要とすることを検討する。

③ J-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。

中間とりまとめ概要 ④

（３） 発行体制

① カードの速やかな発行体制

・ カードの更新について、計画的な更新が進められるように、以下のように運用を工夫する。

現行カード：有効期限の３ヶ月前から更新申請可能。有効期限は10回目の誕生日（18歳未満は５回目の誕生日）。

次期カード：有効期限の３ヶ月前よりさらに前から更新申請を可能とする。

また、更新忘れを防ぐため、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。

・ 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

＜マイナンバーカード自体の更新（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。

＜現行カードにおける電子証明書の更新＞

・ 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。

中間とりまとめ概要 ⑤

（４） 公証名義

・ 国の保証の下に発行されていることを明確化するため、カード券面に「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

（１）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。

・ 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。

※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

・ 有識者の知見によると、ハードウェアの交換までは不要であると見込まれているため、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。

・ その場合に、重要となる利用者の端末側の対応の負担軽減のため、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。

中間とりまとめ概要 ⑥

（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。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、ISO/IEC15408のCC認証の取得は必須である。

・ 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、個人番号カードプロテクションプロファイルの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。

中間とりまとめ概要 ⑦

（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、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、暗証番号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する。

PUKの設定方法（案）

中間とりまとめ概要 ⑧

（８）（９）カード本体･JPKIアプリの真贋性判定機能の追加

・ 認証のためのアプリケーションに、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、機能の追加を実現する。マイナンバー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「affiliationChanged」に、「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」となることから、このことを署名等検証者に周知し、事業の効率化に活用いただく。

（１１）個人番号カードの呼称の変更

・ 民間事業者が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、マイナンバーカードという呼称のためにマイナンバーが利用されていると誤解されるなど、マイナンバー利用事務とカードの利活用が混同されている場合がある。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。

中間とりまとめ概要 ⑨

（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、公開されることで、マイナンバーカード利用端末の開発が容易となり、マイナンバーカードの利活用が進むことから、安全性の確保を前提にこれを公開する。

（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は、重要である。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、今後検討を行う。

（１４）その他重要論点（JPKI暗号化機能の追加）

・ JPKI暗号化機能を追加し、現在、政府、自治体、医療分野で親展郵便で送っている情報を、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仕組みについては、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。