資料４

次期個人番号カードタスクフォース 第1回資料

次期個人番号カード仕様に係る検討事項について

2023年9月7日

デジタル庁
Digital Agency

検討事項一覧

タスクフォースにおける主な論点（案）について(1/2)

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 →券面記載すべきか。（身分証として、提示やコピーの運用に留意）
		②性別 →券面記載すべきか。する場合でも、うら面にもっていけないか。又は、ICチップの記録のみで十分か。（事実上の必要性・法令上の整理）
		③マイナンバー →券面記載すべきか。又は、ICチップの記録のみで十分か。又は、現在のQRコードの記録のみで十分か。（事実上の支障）
		④通名・旧姓 →現在の在り方で良いか。（現在の在り方/通名：ある場合、必ず記載。旧姓：希望者は住民票に記載された場合、カードにも記載。）
		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） →記載事項とするか。記載する場合、追記欄か本欄か。
		⑥追記欄 →追記欄は必要か。必要とした場合、追記欄が満了になるケースがあり、追記欄を大きくできないか。又は、うら面に配置できないか。
		⑦券面デザイン →魅力ある券面デザインのあり方。券面の偽造防止・ユニバーサルデザインにも対応。
	(2)カード等に用いる技術	①暗号方式の在り方 →より強固なものへ換装するか、それにより、電子証明書の有効期限を５年から10年に延長してカードとあわせることができないか。
		②暗証番号の入力のユーザー利便性向上 →現在、４つの暗証番号を、ロングとショートの２つにするか。また、ロングを入力の場合、ショートを入力不要とするか。
		③J-LISマイナンバー関係システムの刷新 →更改内容、スケジュールはどうなるか。
	(3)発行体制	①カードの速やかな発行体制 →次期カードに求められる製造技術等を踏まえつつ、早期発行・交付体制の構築のためどのような方策があるか。
		②オンライン更新の在り方 →役所に赴かずに更新できないか。この場合において、マイナンバーカードに要求される身元保証レベル等について維持することが必要と考えられるが、どう整理するか。
	(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か。

タスクフォースにおける主な論点（案）について(2/2)

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 →現在、電子証明書で採用している暗号（RSA2048）の適格性（2030年末まで）について、猶予期間が設けられないか。
	(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 →次期カードにおいて、新暗号のみならず、旧暗号も処理できることとして、カード利用機関における二重の対応を不要にすることができるか。
	(3) ICチップの空き容量 →必要性やコスト等を勘案した場合、ICチップ容量や空き容量をいかにすべきか。
	(4)ISO認証（現在、ISO15408のCC認証を取得） →次期カードにおいて、満たすべきセキュリティ要件をどのように規定し、その内容を担保すべきか。
	(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） →カラー化・容量増化（解像度アップ）を行うか。
	(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） →磁気ストライプの搭載を継続するか。廃止するか。（現在の印鑑登録証等の利用や将来のクレジットカード利用等に留意）
	(7) PUK（PIN UNLOCK KEY）の発行（海外で採用例が多い） →市町村窓口への往訪を不要とするためにPUKを採用するか。（盗難・紛失等のセキュリティリスクについて確認）
	(8)カード本体の真贋性判定をオンラインで行える機能の追加 →カード本体の真贋性判定をオンラインで行える機能の追加が必要か。（米国PIVカードの例も参考に検討）
	(9)JPKIアプリの真贋性判定機能の追加 →JPKIアプリにも、他の3つのアプリと同様にアプリの真贋性を判定する機能を実装するか。
	(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ができないか。
	(11)個人番号カードの呼称の変更 →次期個人番号カードの導入に合わせ、「マイナンバーカード」以外の新たな呼称を採用するか。また、その場合、いかなる呼称が適当か。
	(12)インターフェイス仕様の公開 →カードの利用を促進するために、カードのインターフェイス仕様(APDU仕様書)を公開できないか。
	(13)（長期的論点）将来的な物理カードの必要性 →スマートフォンのマイナンバーカード機能の搭載が実現され、普及した後には、物理的なカードはそもそも不要とならないか。
	(14)その他重要論点

検討事項各論
１．カードの機能向上に向けた重点的対策項目
２．その他重要論点

(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(1/3)

券面記載すべきか。（身分証として、提示やコピーの運用に留意）

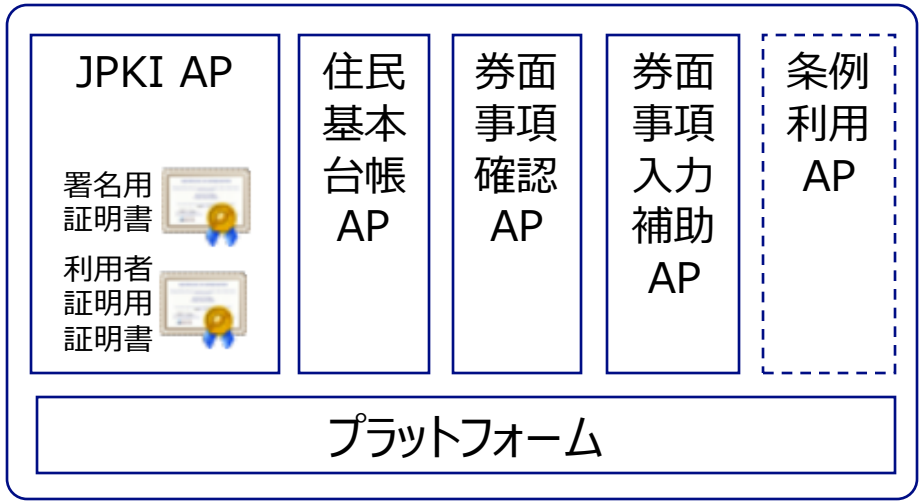
1. 現行のカード仕様及び運用

○ 現行のマイナンバーカードは、おもて面に氏名、生年月日、住所、性別等の本人確認用の情報と顔写真が券面記載され、対面での本人確認に広く活用されている。

○ また現行のカードのICチップには、4つのカードAPが搭載されており、それぞれアクセスコントロールの元、一定の券面記載事項を読み出すことが可能となっている。

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）



マイナンバーカードのカードAP構成

(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(2/3)

	マイナンバー取得、本人確認における役割	アクセスコントロール
JPKI AP	（署名用） • 電子申請に利用	暗証番号（6～16桁の英数字）
	（利用者証明用） • マイナポータル等のログインに利用	暗証番号（4桁の数字）※
住民基本台帳AP	• 住民票コードを記録 • 住基ネットの事務の為に住民票コードをテキストデータとして利用可能	暗証番号（4桁の数字）※
券面事項確認AP	（目的） • 対面における券面記載情報の改ざん検知 • 対面における本人確認の証跡として画像情報の利用 （記録する情報） • 券面情報：４情報＋顔写真の画像 • 裏面情報：マイナンバーの画像	• マイナンバーを利用できる者 表と裏の券面情報 ：照合番号Ａ（マイナンバー１２桁） • マイナンバーを利用できない者 表の券面情報のみ ：照合番号Ｂ（１４桁：生年月日６桁＋有効期限西暦部分４桁＋セキュリティコード４桁）
券面事項入力補助AP	• マイナンバーや４情報を確認（対面・非対面）し、テキストデータとして利用することが可能 【記録・利用する情報】 ①マイナンバー及び４情報並びにその電子署名データ ②マイナンバー及びその電子署名データ ③４情報及びその電子署名データ	①については、暗証番号（４桁の数字）※ ②については、照合番号Ａ（マイナンバー１２桁） ⇒これにより、券面目視によりマイナンバーを入力するようなケースで正誤チェックが可能となる。 ③については、照合番号Ｂ（１４桁：生年月日６桁＋有効期限西暦部分４桁＋セキュリティコード４桁）

※「暗証番号（４桁の数字）」については、統一の設定も可能。但し、生年月日やセキュリティコード等と同一は不適当。

(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(3/3)

2. 課題・論点

○ 現在の券面事項（氏名、生年月日、住所、顔写真（※性別については別の論点として次頁にて説明））については、
- 盗難・紛失時の情報漏洩の恐れ等から券面への記載を止め、ICチップに記録するのみとする案1、
- 対面で身分証として使う際、全ての場面で読取端末の用意があるとは限らないため、現行どおりとする案2が考えられる。

○ デジタルの推進である以上、理想は案の１であるが、そのためには、現実に対面で本人確認を必要とする全ての現場で、ICカードを読み取る環境が整っていることが必要となる。現時点ではまだ、案の２とすることが現実的か。

	案1	案2
券面記載事項	券面に氏名・住所・生年月日・顔写真を記載しない	券面に氏名・住所・生年月日・顔写真を記載する（現行から変更なし）
ICチップ	券面のデータ・4情報＋マイナンバーのテキストデータを格納（現行から変更なし）	
懸念点等	• 全ての本人確認の現場で、ICチップ内のデータの読み出しが必要である。 • 読み出し方式（暗証番号入力か、認証鍵の配布か、など）についても、よく検討する必要がある。 • マイナンバー証としての提示やコピーをする運用が今すぐにはなくならず、支障が生じる恐れがある。 • マイナンバー証としての価値が下がり、取得減につながる等の懸念がある。	• 本人確認を行う側の使い勝手は良いが、紛失・盗難時の個人情報漏洩等の懸念がある。 • カードを提示する側も提示される側も、不必要な情報を提示・入手する場合がある。

(1)カードの券面記載事項　②性別(1/2)

券面記載すべきか。する場合でも、うら面にもっていけないか。又は、ICチップの記録のみで十分か。（事実上の必要性・法令上の整理）

1. 現行のカード仕様及び運用

○　（前述の論点「①氏名、生年月日、住所の3情報及び顔写真」に示す現行のカード仕様及び運用と同様）

現行のマイナンバーカード（おもて面）

(1)カードの券面記載事項　②性別(2/2)

2. 課題・論点

○ 現行の健康保険証においては、性別の裏面記載ができることとなっている。

○ この際、以下の3案の対応が考えられるが、対面目視で性別の確認をする必要がある機会がどの程度あるかなど、改めてよく検討すべきか。

- 券面への記載を止め、ICチップに記録するのみとする案1、
- 券面の裏面に記載し、ICチップにも記録する案2（現行よりは目立たない）
- 券面の表面に記載し、ICチップにも記録する案3（現行どおり）

	案1	案2	案3
券面記載事項	券面に性別を一切記載しない	券面の裏面に性別を記載する（裏面記載）	券面に性別を記載する（現行から変更なし）
ICチップ	券面のデータ・4情報＋マイナンバーのテキストデータを格納（現行から変更なし）		
懸念点等	• 性別については、ICチップ内のデータによる確認が必要となる。	• 性別の券面での確認が必要となる際、マイナンバーもあわせて提示することとなる。	• 健康保険証と同様の配慮が必要との要望がある。

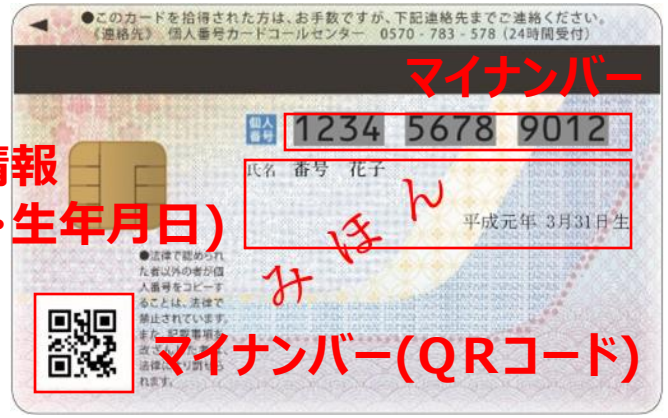
(1)カードの券面記載事項　③マイナンバー(1/2)

券面記載すべきか。又は、ICチップの記録のみで十分か。又は、現在のQRコードの記録のみで十分か。（事実上の支障）

1. 現行のカード仕様及び運用

○ 現行カードは、マイナンバーを提示してよい相手に対してのみ、裏面を提示する運用を想定しており、裏面には、マイナンバー、マイナンバーQRコードの他、必要最低限の情報として本人情報(氏名、生年月日)が記載されている。

○ ICチップ内には券面のデータ及びテキストデータにマイナンバーが記録されている。



現行のマイナンバーカード（うら面）

(1)カードの券面記載事項　③マイナンバー(2/2)

2. 課題・論点

○ マイナンバーカードの盗難・紛失時に、漏洩したマイナンバーが悪用されるのではないかとの懸念がある。このため、以下の3案が考えられるが、対面目視でマイナンバーを読み取るケースがどれくらい残っているのか、検証が必要か。

- 券面に何も記載せず、ICチップにのみマイナンバーを記録する案1、
- 券面にQRコードのみ記載し、ICチップにもマイナンバーを記録する案2、
- 現行どおり、裏面に記載する案3

	案1	案2	案3
券面記載事項	券面にマイナンバー・QRコードを記載しない	券面にQRコードのみ記載する。	券面（裏面）にマイナンバーを記載する（現行どおり）
ICチップ	券面のデータ・4情報＋マイナンバーのテキストデータを格納（現行から変更なし）		
懸念点等	• 全ての本人確認の現場で、ICチップ内のデータの読み出しが必要となる。 • マイナンバー証としての提示やコピーをする運用が今すぐにはなくならず、支障が生じる恐れがある。 • マイナンバー証としての価値が下がり取得減につながる等の懸念がある。	• マイナンバーの取得にはQRコードのスキャン読み取りが必要となる。 • マイナンバー証としての提示やコピーをする運用が今すぐにはなくならず、支障が生じる恐れがある。 • マイナンバー証としての価値が下がり取得減につながる等の懸念がある。	• マイナンバーカードの盗難・紛失時に、漏洩したマイナンバーが悪用されるのではないかとの懸念がある。

(1)カードの券面記載事項　④通名・旧姓

現在の在り方で良いか。（現在の在り方/通名：ある場合、必ず記載。旧姓：希望者は住民票に記載された場合、カードにも記載。）

1. 現行のカード仕様及び運用

○ 現在のマイナンバーカードでは、特別永住者や日本人の配偶者等の在留資格を持つ方で、かつ住民票上に通称名（通名）を持つ方の場合、本名と通称名を併記している。

○ 旧姓については、平成31年の住民基本台帳法施行令の改正により、併記の請求手続を行うことで住民票及びマイナンバーカードに旧姓（旧氏）を併記することが可能である。

旧姓(旧氏)

旧姓(旧氏)記載イメージ

2. 課題・論点

○ マイナンバーカードは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。

○ 併記ではなく、カード券面に通称名のみを記載し、氏名はICチップのみに記載することがありうるか。この場合において、券面を提示して行う官民の各種手続時における本人確認が可能か。混乱をきたさないか。また、悪用される危険性等についてどう考えるか。

○ 姓（旧氏）の取扱については、変更しないということでよいか。（旧姓（旧氏）のみカードに記載するニーズはなく、本人確認書類としても不適当なのではないか。）

(1)カードの券面記載事項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)

記載事項とするか。記載する場合、追記欄か本欄か。

1. 現行のカード仕様及び運用

○ 氏名のフリガナが戸籍の記載事項とされたことに伴い、マイナンバーカードにもフリガナが券面記載事項とされる予定である。

○ 令和6年5月の海外利用に合わせ、生年月日の西暦及び氏名のローマ字の併記についても、追記欄での対応が予定されている。

フリガナ・ローマ字記載のあるカードの実例イメージ

2. 課題・論点

○ 将来的に生年月日の西暦及び氏名のローマ字の併記対応を、追記欄の対応から券面記載事項とするか。

※マイナンバーカードにおける氏名のローマ字表記は、旅券で公証されたローマ字表記と一致させることに留意。

(1)カードの券面記載事項　⑥追記欄

追記欄は必要か。必要とした場合、追記欄が満了になるケースがあり、追記欄を大きくできないか。又は、うら面に配置できないか。

1. 現行のカード仕様及び運用

○ 現行カードのおもて面に追記欄があり、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。

○ なお、追記の際、ICチップ内の券面データやテキストデータ、署名用証明書等は最新の内容に更新されている。

追記欄

現行のマイナンバーカード（おもて面）

2. 課題・論点

○ 追記欄のあり方について、どう考えるか。そもそも追記欄は必要か。

○ 必要とした場合、追記欄が不足し、そのためにカードの再発行となるケースもあることから、追記欄を広げられないか。例えば、うら面にも配置できないか。

(1)カードの券面記載事項　⑦券面デザイン(1/2)

魅力ある券面デザインのあり方。券面の偽造防止・ユニバーサルデザインにも対応。

1. 現行のカード仕様及び運用

○　現行のマイナンバーカードの券面デザイン・セキュリティ対策を以下に示す。

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）

No.	セキュリティ対策	内容
1	パールインキ	見る角度によって２色に変化して見え、偽変造が困難である
2	コピー牽制	コピー機等で複写した場合、隠れた文字が浮かび上がり、真正なカードのコピーであることを判別する
3	シェーディング加工	顔写真のエッジにぼかし加工を施すことで、顔写真の貼り替えを困難にする
4	レーザーエンクレーブ	レーザー光でカード基材を黒く変質させることで印字する

(1)カードの券面記載事項　⑦券面デザイン(2/2)

2. 課題・論点

○ 前述の論点①～⑥とあわせて見直しを検討する予定である。

○ 券面デザインによっては、顔認証付カードリーダ（健康保険証）への影響が生じる可能性があることに留意する必要がある。

○ 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（カードの表裏識別対応など）を踏まえたデザインとするべきか。（例えば、Suicaは端に切り欠きが入っており、表裏を区別することが可能である。）

(2)カード等に用いる技術　①暗号方式の在り方(1/2)

より強固なものへ換装するか、それにより、電子証明書の有効期限を５年から10年に延長してカードとあわせることができないか。

1. 現行のカード仕様及び運用

○ 現行のマイナンバーカードの電子証明書は、仕様策定当時の暗号方式の安全性基準に基づき、RSA 2048bit及びSHA-256が用いられており、当該アルゴリズムを使った電子証明書の有効期間が5年となっている。また電子証明書の有効期限は券面に印刷されない為、市町村窓口にて券面に電子証明書の有効期限を追記する等の運用を行っている。

○ 現行のマイナンバーカードは、カード自体の有効期間が10年であるのに対し、電子証明書の有効期間が5年となっており、電子証明書更新の為に市町村窓口に行く必要がある。

項目	現行カード
カードの有効期間	10年
電子証明書の有効期間	5年
公開鍵暗号方式[セキュリティ強度※]	RSA 2048bit[112]
ハッシュ関数[セキュリティ強度※]	SHA-256[128]

※　セキュリティ強度の定義はNISTのガイドライン(SP800-57 Part1, Revision 5, May 2020)による。同ガイドラインでは、2031年以降に使用する暗号のセキュリティ強度は128以上とすることを推奨している。

(2)カード等に用いる技術　①暗号方式の在り方(2/2)

2. 課題・論点

○ カードの有効期間と電子証明書の有効期間が異なるため、電子証明書の有効期間をカード本体の有効期間である10年に合わせ、10年の有効期間に耐えうる強固な暗号方式に移行する。

○ 電子政府推奨暗号リスト(CRYPTREC)では、RSA 2048bitの利用は2030年までとしており、次期カードの切り替えにあたって、暗号方式の見直しが必要であることから、暗号方式はECDSA等の楕円曲線暗号をベースとしたものとし、またハッシュ関数は現行のSHA-256と同等かそれ以上のものに見直すこととし、ICチップの処理能力を勘案し方式を、技術検討WGでの検討を踏まえ、選定する。

○ 暗号方式の変更にあたっては、認証局における新暗号への対応が必要であり、カード用・スマホ用の新旧で合計2システムの並行運用が必要になることや、各省庁・自治体・民間の署名等検証者のシステムへの影響も十分に考慮する必要がある。この点についても、技術検討WGにおいて十分な検討を求める。

項目	現行カード	次期カード	
カードの有効期間	10年	10年	
電子証明書の有効期間	5年	10年	
公開鍵暗号方式　[セキュリティ強度]	RSA 2048bit[112]	ECDSA 256bit　[128]	ECDSA 384bit　[192]
ハッシュ関数　[セキュリティ強度]	SHA-256[128]	SHA-256　[128]	SHA-384　[192]

※GPKIと相互認証するためには、RSA3072、ECDSA256、ECDSA384のいずれかに変更する必要がある。（「政府認証基盤（GPKI）における暗号アルゴリズムの移行に係る周知及び依頼について」令和５年７月デジタル庁）

(2)カード等に用いる技術　②暗証番号の入力のユーザー利便性向上(1/2)

現在、４つの暗証番号を、ロングとショートの２つにするか。また、ロングを入力の場合、ショートを入力不要とするか。

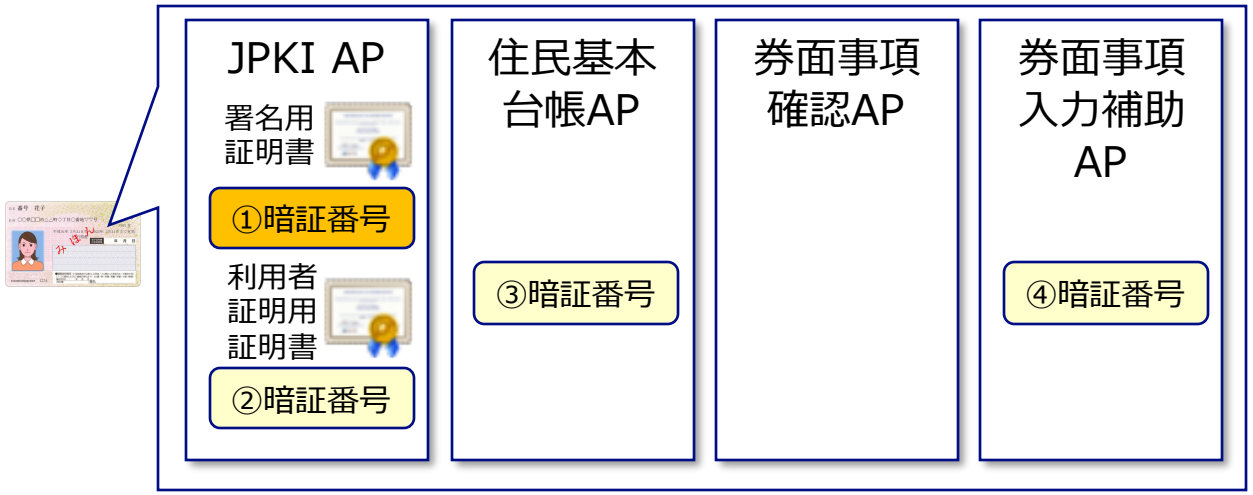
1. 現行のカード仕様及び運用

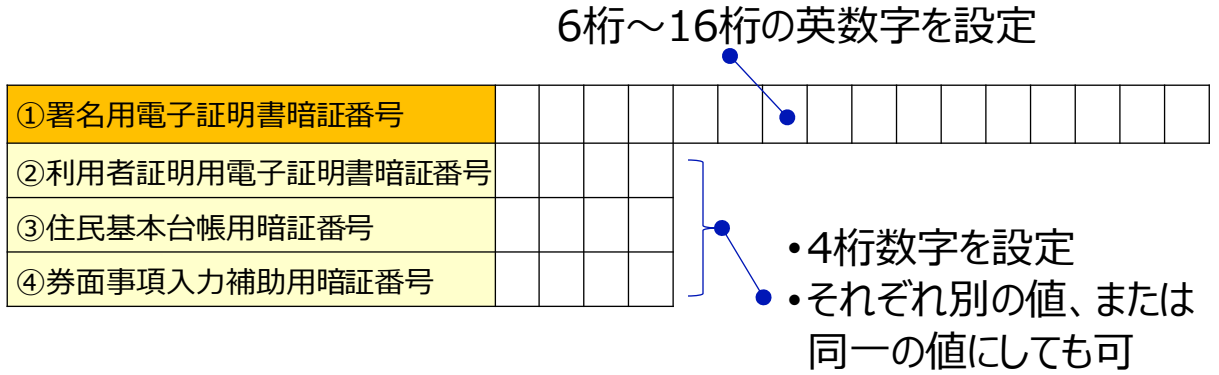
○ 現行のマイナンバーカードには、4種類のカードAP（JPKI AP、住民基本台帳AP、券面事項確認AP、券面事項入力補助AP）が格納されており、そのうち券面事項確認APを除く3種類に本人が設定する4種類の暗証番号が設けられている。

○ 4種のうち、JPKI APのうち署名用電子証明書暗証番号は6桁～16桁の英数字を設定し、残り3種の暗証番号は4桁数字を設定することとなっている。4桁の暗証番号3種は同じ暗証番号とすることも可能となっている。

○ 4種類の暗証番号の設定や利用が分かりにくいとの声がある。また複数のカードAPを利用する場合、それぞれで暗証番号の入力が必要であり、入力の手間や操作が煩わしいなどの声がある。
（例　券面事項入力補助APで④暗証番号入力後、JPKI APで利用者証明書用電子証明書の②暗証番号を入力）

【現行カード】





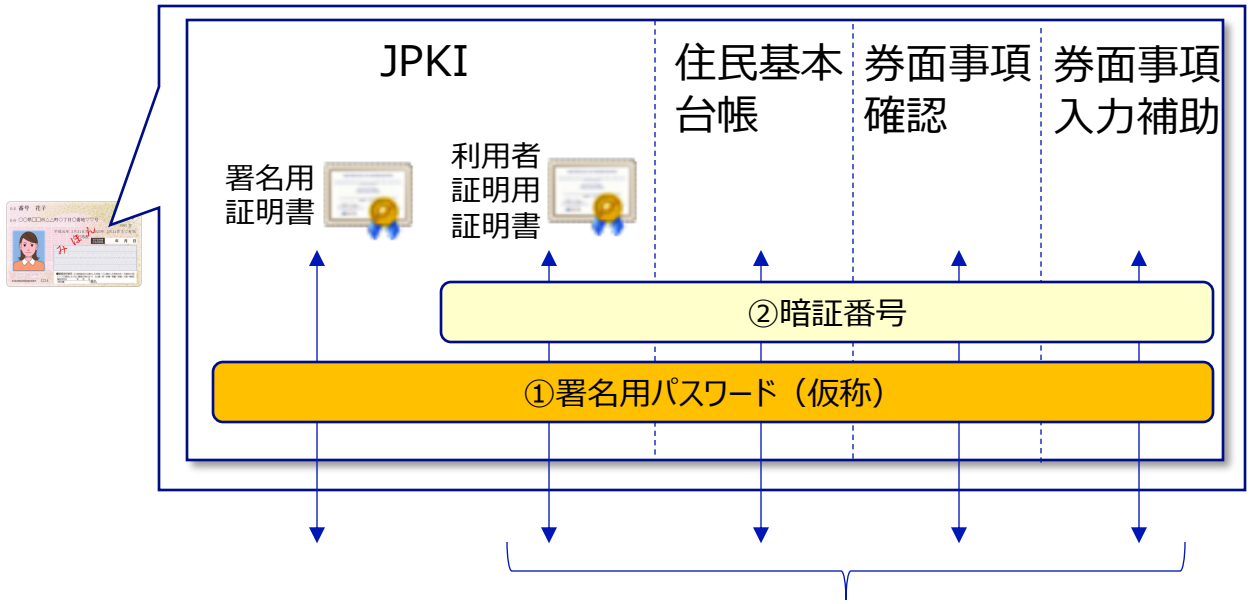
(2)カード等に用いる技術　②暗証番号の入力のユーザー利便性向上(2/2)

2. 課題・論点

○ 次期カードにおいては、署名用パスワードと暗証番号(4桁)の2種に統合し、かつ署名用パスワードの照合に成功した場合、暗証番号(4桁)の照合を不要とする等の変更を実現できないか。

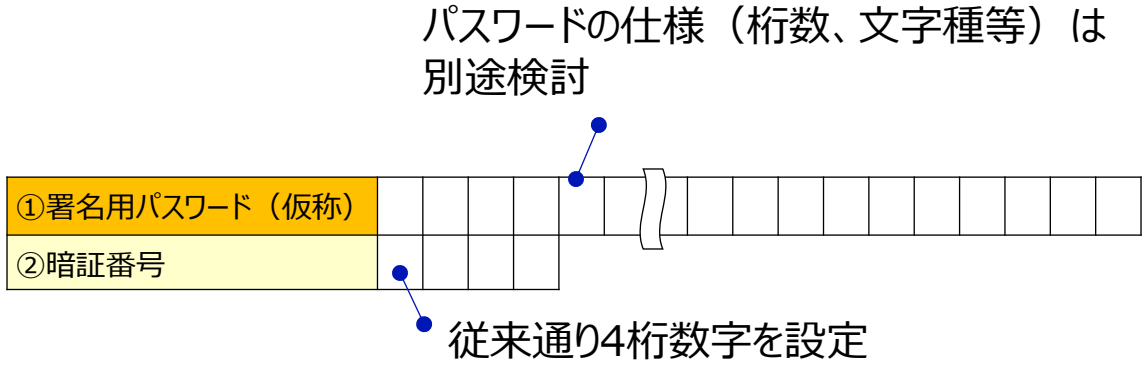
○ 上記の対応に伴い、カード内APの在り方の検討や、現行のマイナンバーカード読み取り端末（例　マイナンバーカード健康保険証用顔認証付カードリーダ等）の影響について留意する必要がある。これらの点についても、技術検討WGにおいて十分な検討を求める。

【次期カード】



①署名用パスワード(仮称)の照合が必要

①署名用パスワード(仮称)または②暗証番号の照合が必要



(2)カード等に用いる技術　③J-LISマイナンバー関係システムの刷新（1/3）

更改内容、スケジュールはどうなるか。

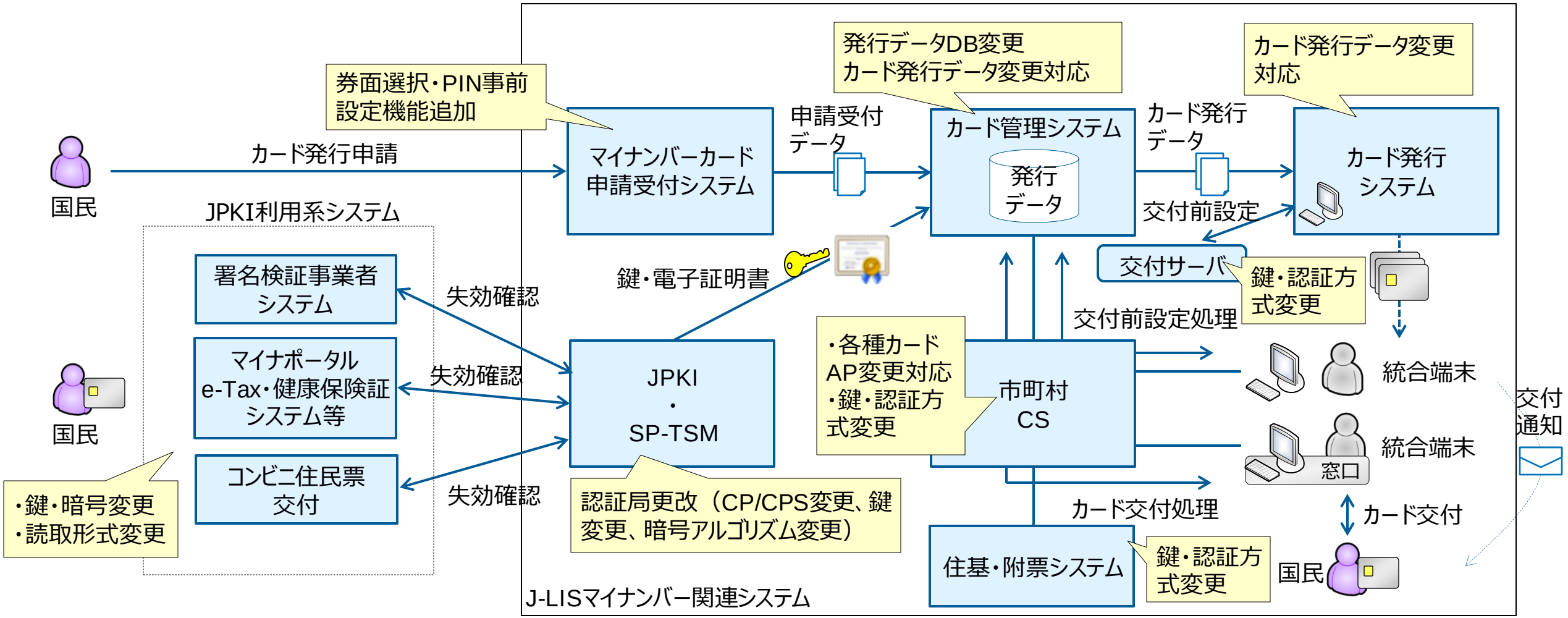
1. 現行のカード仕様及び運用

○ 現行のマイナンバーカードの発行や利用に係るシステムは以下の通りであり、本タスクフォースにて取り扱う次期カード仕様の取り込みにあたってはシステム改修が生じる見込みである。

No.	関係システム	マイナンバーカードとの関わり
1	マイナンバーカード申請受付システム	マイナンバーカードの申請受付、申請受付データの生成
2	カード管理システム	カード発行データの生成、マイナンバーカードの発行状態、発行データの管理
3	カード発行システム	マイナンバーカードの発行、カード発行データの書き込み、市町村への送付
4	市町村CS・統合端末	マイナンバーカードの交付前設定、交付
5	住基・附票システム	マイナンバーカードの認証に関する処理
6	JPKI・SP-TSM	マイナンバーカード内のJPKI　APへの電子証明書の発行等 スマートフォンのGPSE内のJPKI　APへの電子証明書の発行等
7	署名検証事業者システム	マイナンバーカード（電子証明書）による本人確認
8	マイナポータル・e-Tax・健康保険証システム等	マイナンバーカード（電子証明書）による本人確認
9	コンビニ住民票交付システム	マイナンバーカード（電子証明書）による本人確認

(2)カード等に用いる技術　③J-LISマイナンバー関係システムの刷新（2/3）

○　前頁の各システムの関係とシステム改修内容を以下に示す。



(2)カード等に用いる技術　③J-LISマイナンバー関係システムの刷新 (3/3)

2. 課題・論点

○ 次期マイナンバーカードへの対応にあたり、改修等の対応を行う対象となる関連システムが多く、これら関連システムにおける改修内容や改修スケジュールの整合確保が必要である。

○ カード発行時間の短縮を見据え、カード発行におけるバッチプログラムのオンライン化等、次期マイナンバーカードの対応を機にアーキテクチャの見直し、刷新が必要である。

○ これらの論点についても、技術検討WGにおける検討を求める。

(3)カード発行体制　①カードの速やかな発行体制(1/4)

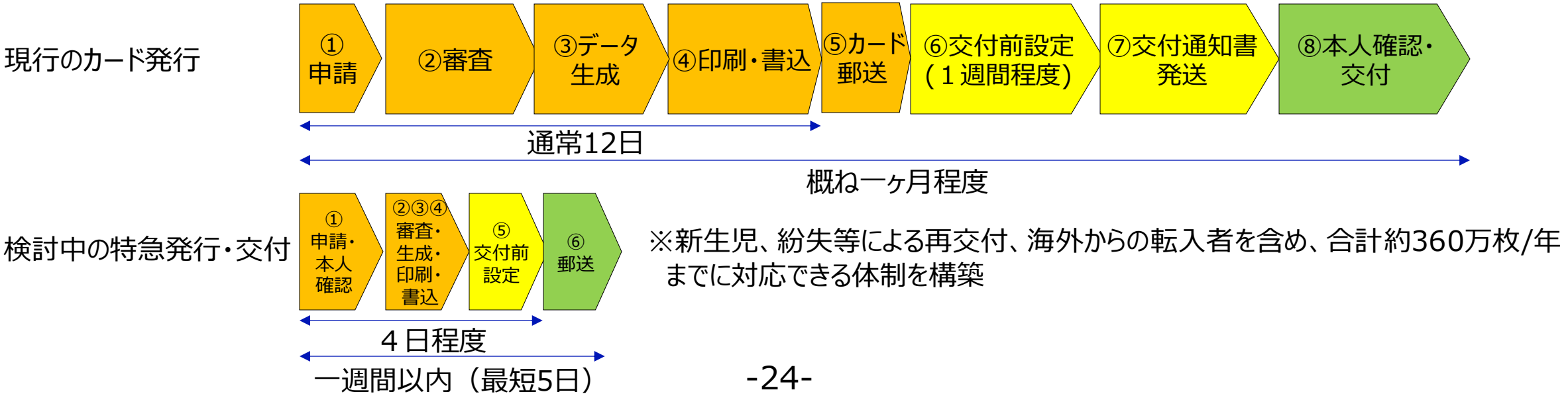
次期カードに求められる製造技術等を踏まえつつ、早期発行・交付体制の構築のためどのような方策があるか。

1. 現行のカード仕様及び運用

○ マイナンバーカードは、J-LISにおける②審査、③カード管理システムにおけるカード発行データ生成、④印刷・データ書き込み、⑤市町村へのカード郵送、⑥市町村職員による交付前設定、⑦交付通知書発送、⑧市町村窓口の交付の作業を経て交付される。これよりカード発行から交付までに要する期間は概ね１ヶ月程度を要しており、カード発行・交付期間の短縮が求められる。

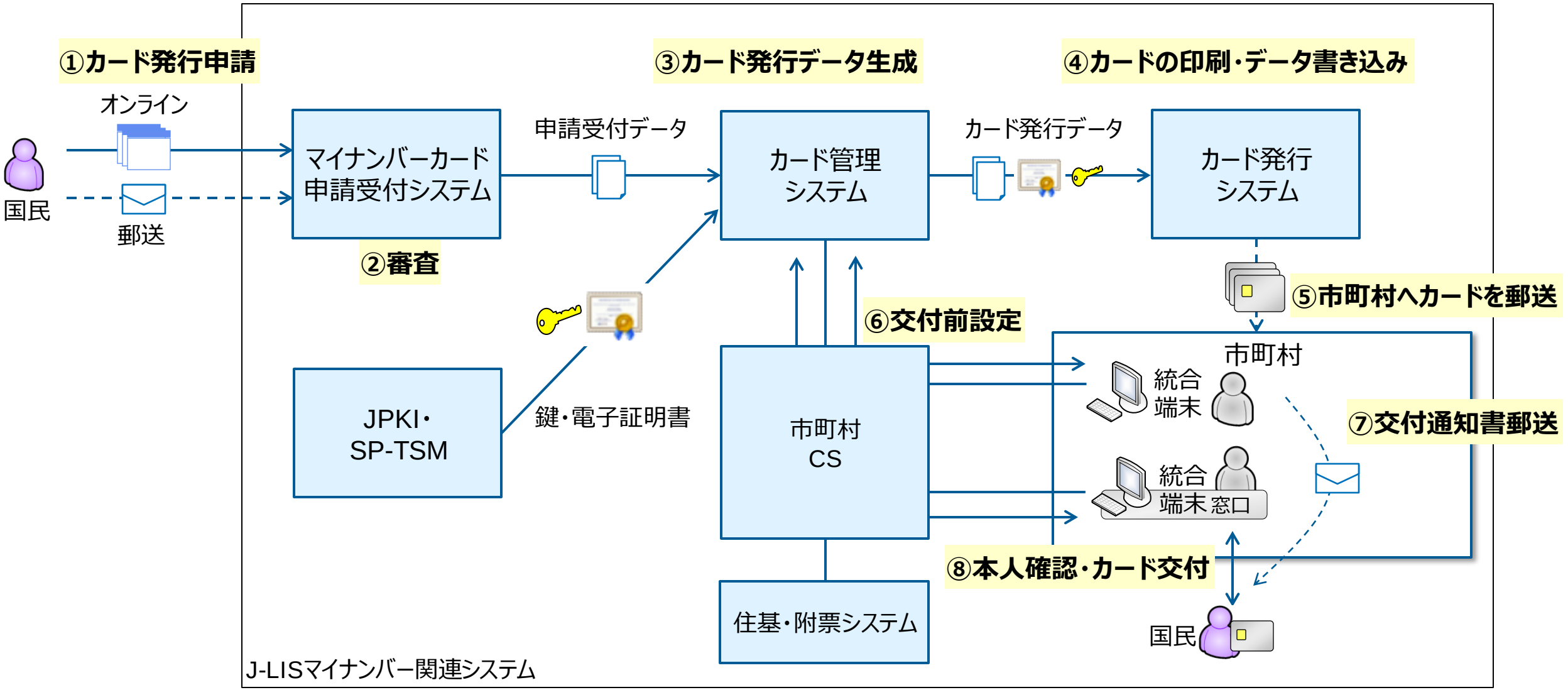
○ 上記にて、②はデータ取り込みや顔写真の審査を人手で行っていること、⑥は職員が手作業で設定を行っていること等により申請が集中した際に時間がかかる、⑤⑦と2回の郵送がある等の課題がある。

○ これより、カード紛失時の再交付等、速やかにカードを取得する必要がある場合を対象に、J-LISにおいて②の専用審査、⑤交付前設定を集約、⑥直接住民へカードを郵送することにより、カード発行・交付期間を最短5日に短縮した特急発行・交付の運用(令和６年秋までに開始予定)を予定している。



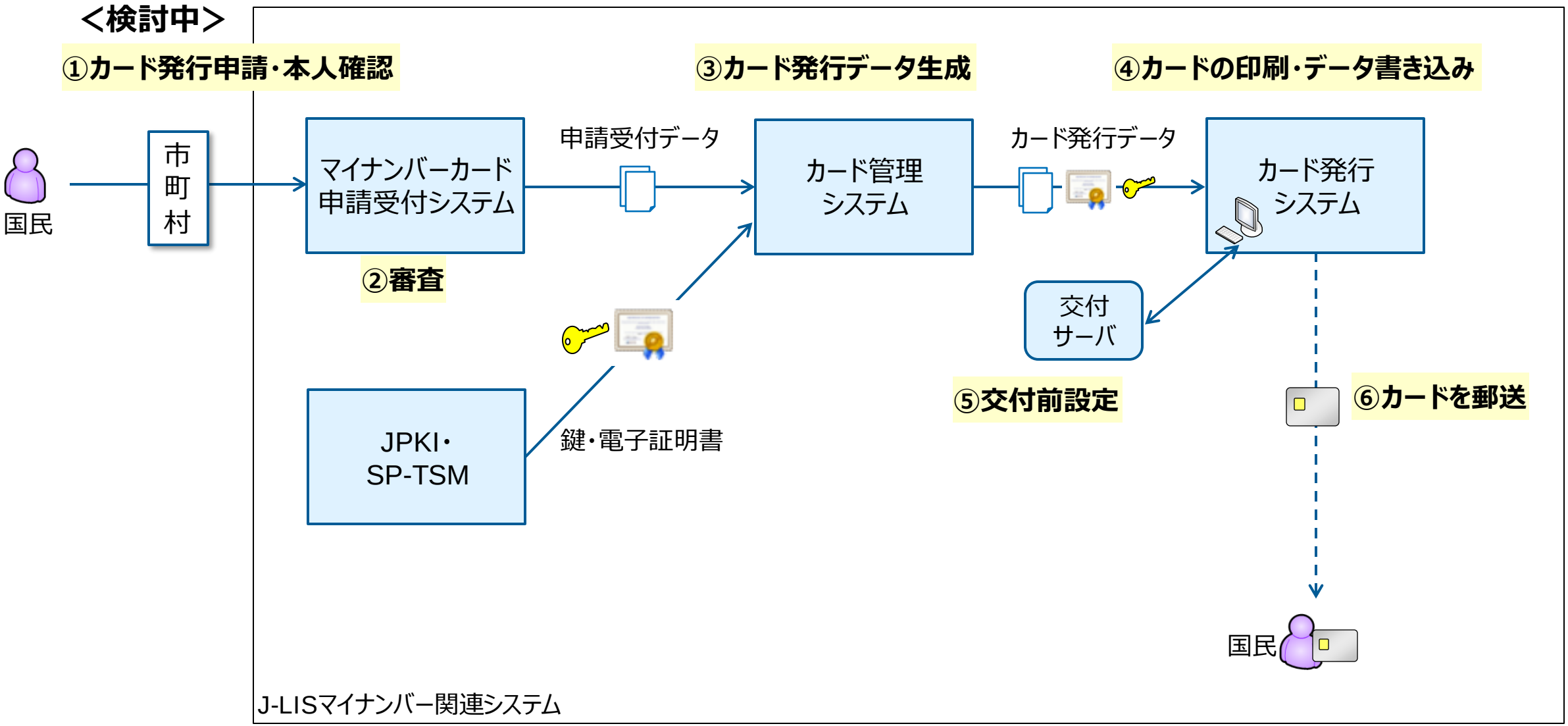
(3)カード発行体制　①カードの速やかな発行体制(2/4)

○ マイナンバーカード発行におけるシステム間連携及び作業の流れを以下に示す。



(3)カード発行体制　①カードの速やかな発行体制(3/4)

○ 特急発行・交付による発行マイナンバーカード発行におけるシステム間連携及び作業の流れ（検討中）を以下に示す。



(3)カード発行体制　①カードの速やかな発行体制(4/4)

2. 課題・論点

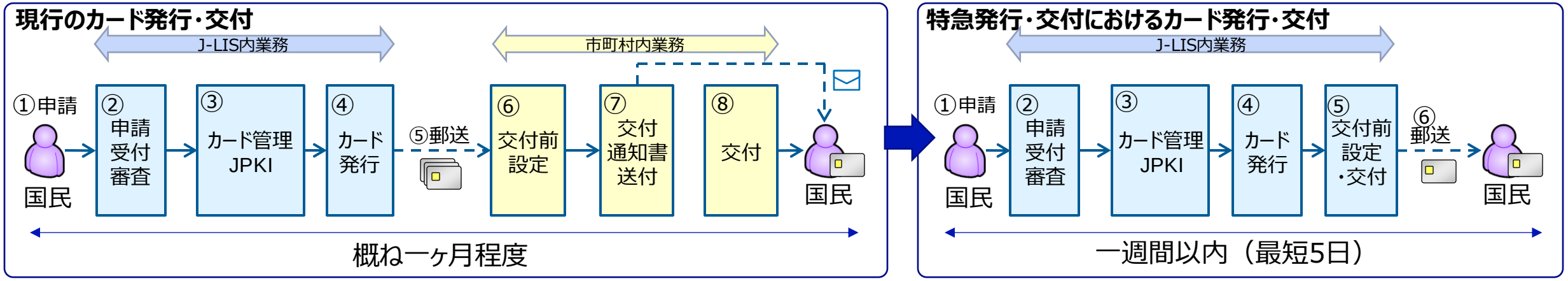
○ 特急発行・交付の対象拡大や、カードのオンライン更新(次頁)も含め、カードの速やかな発行・交付体制の強化・整備が考えられないか。

○ 特急発行・交付はカード紛失時の再交付等、速やかにカードを取得する必要がある場合に限定されており、通常のカード発行時にも適用するためには②における作業体制の強化、④におけるカード発行レーンの投資・増加、⑥における交付前設定作業の体制強化が必要である。

○ 特に②においては、申請書(紙)のデータ化や、顔写真の加工・補正、身分証としての顔写真の適切さの審査、審査が不可となった場合の連絡等を行っている。申請書(紙)のデータ化に伴う付帯作業や、申請内容の不備等への例外対応、顔写真審査においては顔検出・補正の自動化ではカバーしきれない問題への例外対応が発生する為、一定の体制が必要な状況である。

○ また②にて、申請受付システムからカード管理システムへのカード発行データの送信はバッチプログラムで行っており、バッチ起動時間に間に合わなかった申請は翌日の送信となるため、改善が必要である。

○ これらの論点についても、技術検討WGにおける検討を求める。



(3)カード発行体制　②オンライン更新の在り方(1/3)

役所に赴かずに更新できないか。この場合において、マイナンバーカードに要求される身元保証レベル等について維持することが必要と考えられるが、どう整理するか。

1. 現行のカード仕様及び運用

○ マイナンバーカードの有効期間は10年であり、発行から10回目の誕生日の3か月前から更新が可能である。

○ 上記において有効期限切れを迎える住民に対し、J-LISより有効期限切れの2～3か月前を目途に有効期限通知書を送付し、有効期限通知書に記載の申請書IDをもとに、新規発行と同様の手続きによりカード更新申請を行う。

○ これまでのマイナンバーカードの年間交付枚数は以下の通りである。

年度	交付枚数	年度	交付枚数
2015年度	228万枚	2019年度	376万枚
2016年度	876万枚	2020年度	1,558万枚
2017年度	293万枚	2021年度	1,894万枚
2018年度	260 万枚	2022年度	2,957万枚

(3)カード発行体制　②オンライン更新の在り方(2/3)

○「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（2019年2月25日、各府省情報化統括官(CIO)連絡会議決定）では、身分証における身元保証レベル(IAL、Identity Assurance Level)として以下を定義しており、マイナンバーカードは自治体職員が対面で身元確認を実施した上でカードを交付しているため、IAL3となっている。

身元保証レベル	定義
レベル1(IAL1)	身元識別情報が確認される必要がなく、身元確認の信用度がほとんどない。身元識別情報は、自己表明若しくは自己表明相当である。
レベル2(IAL2)	身元識別情報が遠隔又は対面で確認され、身元確認の信用度が相当程度ある。
レベル3(IAL3)	身元識別情報が特定された担当者の対面で確認され、身元確認の信用度が非常に高い。

(3)カード発行体制　②オンライン更新の在り方(3/3)

2. 課題・論点

○ マイナンバーカードは累計9千万枚以上発行されており、このうち4千8百万枚以上の発行が、2021年～2022年に集中したことから2031年～2032年にはカードの更新がピークとなり、これまでと同様に市町村窓口への集中、混雑が予想される。

○ 役所に赴かずに更新できないか。この場合においても、マイナンバーカードに要求される身元保証レベル等について維持することが必要であるが、どう整理するか。どのような方策があるか。

○ 特に、現在カードの交付時等において対面で必ず厳格な本人確認を行っているが、オンライン更新を行うこととした場合、本人性の確認（申請をしている者が本人であることの確認）についてどのように行うのか。また、マイナンバーカードの顔写真について、申請者本人のものであることの確認をどのように行うか。

３．現行カードにおける電子証明書のオンライン更新

○ 現行では、カード自体の有効期間が10年であるのに対し、電子証明書は有効期間が５年であるため、2021年～2022年にかけてマイナンバーカードの発行が集中したことから、2026年～2027年には電子証明書の更新がピークとなり、市町村窓口の負担の増加が予想される。

○ 電子証明書については、市町村窓口に行くことなく更新を行うことを可能とするニーズが高いと考えられることから、現行カードにおいても、身元保証レベルの維持や秘密鍵・電子証明書を扱う端末・回線のセキュリティ等を踏まえつつ、検討を進める。

(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か。

1. 現行のカード仕様及び運用

○ 現行のマイナンバーカードは、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、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。

2. 課題・論点

○ 他国の国民IDカードでも国名が記載されることが通例であることから、国の保証の元に発行されていることを明確化するために、カード発行者として以下２案のいずれか、若しくはその組合せを記載してはどうか。

- 案1：総務大臣及び市町村長名の連名
- 案2：「日本国　JAPAN」の記載等

検討事項各論

１．カードの機能向上に向けた重点的対策項目

２．その他重要論点

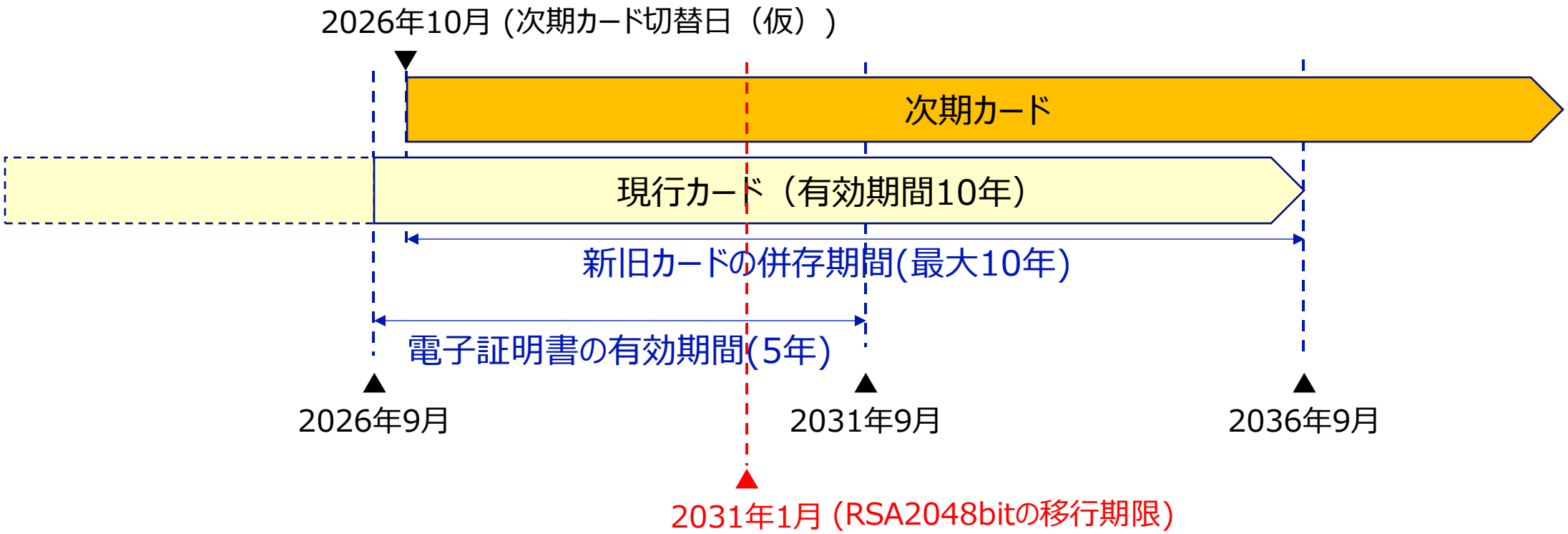
(1)次期カード発行直前に発行されるカードの電子証明書の扱い(1/3)

現在、電子証明書で採用している暗号（RSA2048）の適格性（2030年末まで）について、猶予期間が設けられないか。

1. 現行のカード仕様及び運用

○ 次期マイナンバーカードの切り替え後も、直前で発行した現行のマイナンバーカードを10年利用可能であることから、現行のカードを積極的に回収し次期カードに切り替えない限り、最大10年間新旧の2種類のカードが併存することとなる。

○ 上記において次期カード切替直前に発行された現行カードの電子証明書の有効期間は5年であることから、例えば以下のケースでは、2031年9月まで電子証明書の利用が可能となる。



(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(2/3)

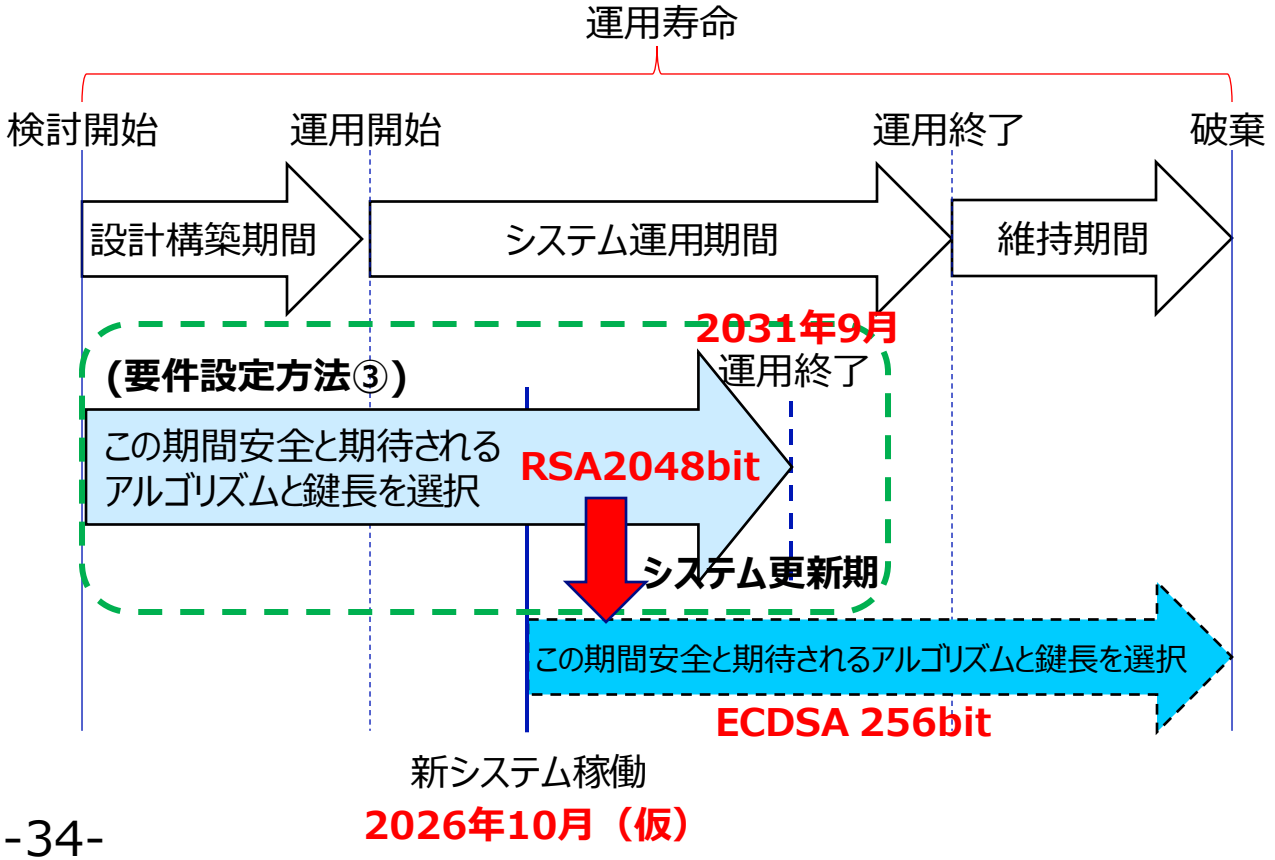
2. 課題・論点

○ 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(RSA2048bit)は2031年1月1日以降利用してはならないとされているが、前頁の例では次期カード切替直前に発行された現行カードの電子証明書の有効期限は2031年9月となり、移行期限である2030年12月31日から約9か月程度経過してしまう等の課題がある。

○ 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（初版：2022年（令和4年）3月、CRYPTREC LS-0003-2022R1）[P. 13]にて、運用寿命とセキュリティ強度要件の関係として以下を示している。

3.1 電子政府システムに求められる運用寿命とセキュリティ強度要件の関係

【要件設定方法③】
対象となる電子政府システムにおいて、運用寿命が決まっていない（明確ではない）場合には、システム更新期を明確化したスケジュールを立案することを条件としたうえで、その更新期まで安全に運用するために必要なセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズム及び鍵長をサポート（実装）しなければならない。なお、そのスケジュールにおいて、新システムの稼働開始予定時期及び新旧システムの併用運用想定期間を示しておくことが望ましい



(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(3/3)

○ マイナンバーカードにおいては、新暗号に対応した次期カードへの移行時期を明確にする予定であり、万が一旧暗号のセキュリティ強度が想定よりも著しく低下することとなった場合次期カードへの切り替え手段を確保していることや、移行期限からの超過期間が短期であることから、当該期間における旧暗号による電子証明書の利用を許容できないか。

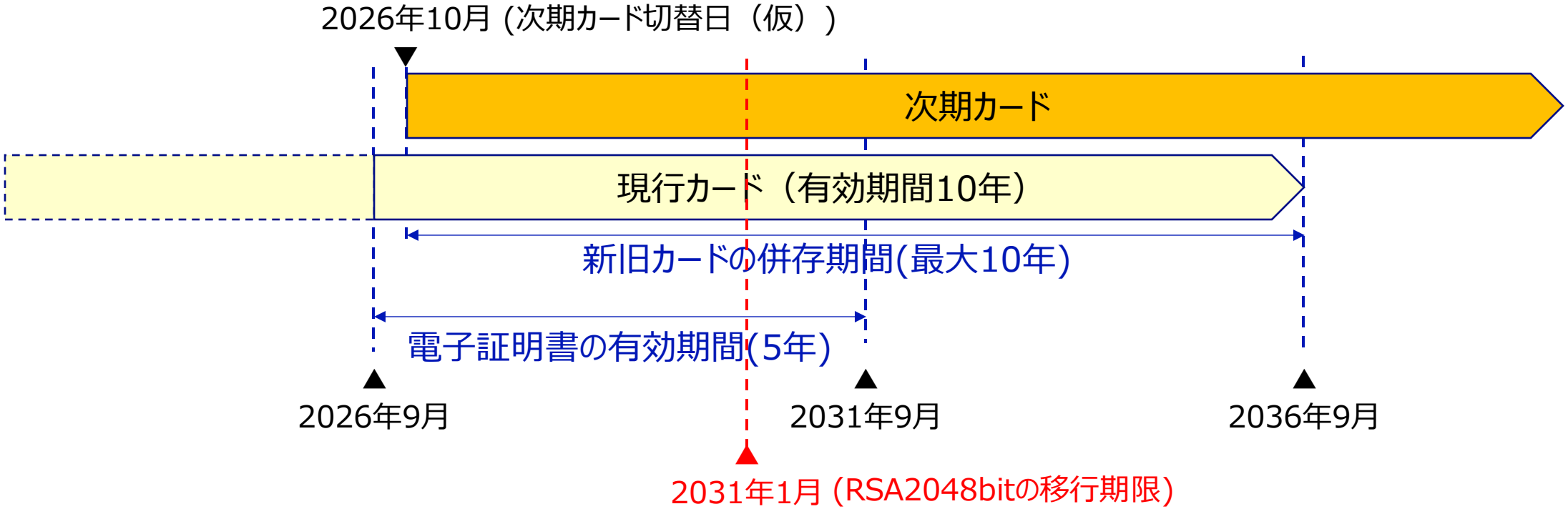
(2)新旧カードの切り替えに伴うカード利用機関等への影響(1/3)

次期カードにおいて、新暗号のみならず、旧暗号も処理できることとして、カード利用機関における二重の対応を不要にすることができるか。

1. 現行のカード仕様及び運用

○ 前頁論点に示す通り、次期マイナンバーカードの切り替え後も、直前で発行した現行のマイナンバーカードを10年利用可能であることから、現行のカードを積極的に回収し次期カードに切り替えない限り、最大10年間新旧の2種類のカードが併存することとなる。

○ 同様に、次期カード切替直前に発行された現行カードの電子証明書の有効期間は5年であることから、例えば以下のケースでは、2031年9月まで電子証明書の利用が可能となる。



(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(2/3)

○ 現行のカードでは、以下に示す暗号が使用されており、2031年1月1日以降の利用が推奨されないRSA 2,048bitが含まれている。その他の暗号アルゴリズムは2050年まで利用可能である。

No.	項目	暗号使用箇所	暗号アルゴリズム	CRYPTREC上の分類			
				通信時及び鍵共有の暗号化	保管時の暗号化	署名・メッセージ認証	エンティティ認証
1	ICカードOS	内部認証、外部認証	AES128bit, RSA2048bit, SHA256				○
2	ICカードOS	通信路暗号化	AES128bit(CBC), RSA2048bit	○			
3	カードAP(共通)	内部認証、外部認証	AES128bit, RSA2048bit, SHA256				○
4	カードAP(共通)	通信路暗号化	AES128bit(CBC), RSA2048bit	○			
5	券面事項確認AP	カードAP内データの署名	RSA2048bit, SHA256			○	
6	JPKI AP	署名	RSA2048bit, SHA256			○	

(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(3/3)

2. 課題・論点

○ これよりカード利用機関における新暗号への対応を考慮し、次期カードには新旧暗号を扱えるようにすることで次期カード切替時の負担を軽減するとしてはどうか。

○ 但し、前述に示す暗号強度の問題を考慮し、以下に示すカード利用機関における利用シーン毎に、次期カード切替日以降の現行カードを利用可能とする期間や、カード利用機関における新暗号への対応期限を検討する。

①署名利用（署名検証者等）
前頁の表No.6(JPKI AP)に該当するが、前頁論点に示す通り移行期限である2030年12月31日から約9か月程度の経過となり、これが許容できるかという問題に帰着する。

②カードAP利用（端末等）
前頁の表No.5(券面事項確認AP)においては、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」では、署名検証の用途では2040年まで許容されており、新旧カード併用期間において旧暗号を用いても問題ないと考えられる。
前頁の表No.3、4において次期カード切替日以降の現行カードを利用可能とする期間や、カード利用機関における新暗号への対応期限を検討が必要である。

③空き領域利用（条例利用AP等）
空き領域への条例利用APダウンロード等においては、前頁の表No.1、No.2に該当し、同様に次期カード切替日以降の現行カードを利用可能とする期間や、カード利用機関における新暗号への対応期限を検討が必要である。

(3) ICチップの空き容量

必要性やコスト等を勘案した場合、ICチップ容量や空き容量をいかにすべきか。

1. 現行のカード仕様及び運用

○ 現行のマイナンバーカードのカード仕様書では、ICチップの空き容量を以下としている。

現状（本書作成時点である平成25 年11 月）において、空き容量を具体的に定義することは困難であるため、概ね次の考え方に基づくこととする。

- 読み書き可能な領域（メモリ）のうちの、「ISD、SSD、カードAP 等」のために使用可能な領域の総量を10 割とした場合に、現状想定される「券面事項入力補助AP、住基AP、本人確認業務用領域、券面事項確認AP、公的個人認証AP、条例利用領域および複数の条例利用AP」を搭載した上で、将来利用のための予約領域として、4 割～5 割程度の空き容量を確保すること。
- 実装方法としてEEPROM（不揮発性メモリの一種で、電気の操作によってデータの消去や書換えが可能となっている半導体記憶装置）を採用する場合で例示すると、64 キロバイトのメモリ容量では、上記の要件を満たせない可能性が高いことから、128 キロバイト以上のメモリ容量を確保することが考えられる。

2. 課題・論点

○ 令和6年度に実現するIC運転免許証との一体化や、他在留カードとの一体化を考えると、上記のメモリ容量の目安では足りなくなる可能性がある。

○ IC運転免許証や在留カード他、将来的に他のカードAPの搭載を想定した場合に必要とするICチップの空き容量をどのぐらいとするか、ICチップの単価も考慮し検討を進める。

(4) ISO認証（現在、ISO15408のCC認証を取得）

次期カードにおいて、満たすべきセキュリティ要件をどのように規定し、その内容を担保すべきか。

1. 現行のカード仕様及び運用

○ ICカード等のセキュリティ製品は内部がブラックボックスであり調達者が製品の内部にセキュリティホール等の脆弱性が包含されていないか検査することができない為、その製品に対し、第三者のセキュリティ評価機関によるセキュリティ評価※が不可欠である。
※ISO/IEC 15408に基づくセキュリティ評価・認証、Common Criteria認証とも言う。

○ 現行のマイナンバーカードにおいては、4カードAP(JPKI、住基、券面事項確認、券面入力補助)を搭載した状態でICチップ・ICカードOSと合わせた認証（コンポジット認証）を取得しており、セキュリティ評価(EAL 4+)を獲得している。

○ 一方では、ICチップやICカードOS単体で取得するケースもあり、欧州ではICチップ単体でEAL5を取得した市販製品を利用した例もある。（コンポジット認証は評価対象が広いため認証取得に時間を要することが一般的である。）

2. 課題・論点

○ 次期カードにおいて、満たすべきセキュリティ要件をどのように規定し、その内容を担保すべきか。

○ 求められる発行時期との整合をどうとるべきか。

○ その他、考慮すべき脅威や留意事項はあるか。

(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）

カラー化・容量増化（解像度アップ）を行うか。

1. 現行のカード仕様及び運用

○ 現行のマイナンバーカードでは、券面（表面）に顔写真がカラー印刷されている。ICチップでは券面事項確認AP内に顔写真データを格納している。

○ なお、IC旅券には顔認証用の顔写真が格納されており、画像形式はJPEG、24bitカラー、縦540Pixel×横420Pixel、最大24kBとなっている。

2. 課題・論点

○ 顔写真のカラー化・高精細化を行うことが必要か。（顔認証を行うニーズに対応）

○ 顔写真のカラー化・高精細化を行うことで顔写真データの容量が増大する場合には、ICチップの格納容量の肥大化、ICからの読み出しに時間がかかる等の課題が発生するところ、実用に耐えうるものとなるよう、画像の解像度や圧縮率等を考慮するか。

(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）

磁気ストライプの搭載を継続するか。廃止するか。（現在の印鑑登録証等の利用や将来のクレジットカード利用等に留意）

1. 現行のカード仕様及び運用

○ 現在、JIS規格の磁気ストライプが実装されている。

○ 市町村は、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。

○ 一方で、それほど活用されているものではなく、また、磁気ストライプはそもそもセキュリティ強度は高くない。また、券面において相当の領域を占有している。

2. 課題・論点

○ 次期カードで、磁気ストライプを継続するか。廃止するか。
※なお、仮に、将来的に、マイナンバー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。現在の全銀協仕様で、磁気ストライプをまず読む仕様となっている。

(7)PUK（PIN UNLOCK KEY）の発行（海外で採用例が多い）

市町村窓口への往訪を不要とするためにPUKを採用するか。（盗難・紛失等のセキュリティリスクについて確認）

1. 現行のカード仕様及び運用

○ 現行のマイナンバーカードは、各カードAP毎に暗証番号が設定され、暗証番号を規定回数誤るとカードAPがロックされ、使用不能となる。ロックの解除には市町村窓口に赴き、職員に対応してもらう必要がある。

※なお、署名用電子証明書がロックされた場合に、コンビニ端末で解除する方法が導入されているが、コンビニへの移動や一定の手順が必要である。（利用者証明用電子証明書についても現在検討が行われている。）

○ 諸外国のeIDカードにおいては、認証時の暗証番号誤りによるロック解除の手段としてPUK(PIN UNLOCK KEY)を配布し、ユーザ自身でPUKを用いてロック解除する等の運用が多く見られる。

No.	項目	クロアチアeID	エストニアeID	ノルウェーeID	ベルギーeID	スロバキアeID
1	PUK桁数	8桁	8桁	8桁	8桁	8桁
2	PUK初期値	通知書に記載	通知書に記載	通知書に記載	通知書に記載	通知書に記載
3	PUKの値を変更する者	所有者	所有者	所有者	（不可）	所有者
4	PUK試行回数許容値	6回	3回	8回	3回	10回
5	PUKをロックした場合の対応	警察署でロック解除	警察署で通知書発行申請	カスタマーサポートへ連絡または他IDで認証し解除	市町村役場にてPUK再発行	警察署にて電子証明書再発行

2. 課題・論点

○ 諸外国のeIDカードの運用を参考にPUKを導入すべきか。

○ PUK通知書と一緒にマイナンバーカードが盗難にあった場合に備えた、PUKの通知方法（カードと別にして郵送等）や通知書の管理方法を考慮すべきか。また、PUKを忘れた場合、国によってはコールセンター問い合わせを認める事例があるが、どうするか。

(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

カード本体の真贋性判定をオンラインで行える機能の追加が必要か。（米国PIVカードの例も参考に検討）

1. 現行のカード仕様及び運用

○ 現行カードでは、カードAP単位で真贋判定機能を実装しているが、カード本体の真贋判定機能を有していない。米国の職員カード(PIV)では、カード本体の真贋性を確認する証明書が格納されており、オンラインで行える確認する機能を実装している。

2. 課題・論点

○ カード本体の真贋性判定をオンラインで行える機能の追加が必要か。（米国PIVカードの例も参考に検討）

JPKIアプリにも、他の3つのアプリと同様にアプリの真贋性を判定する機能を実装するか。

1. 現行のカード仕様及び運用

○ 住民基本台帳AP、券面事項確認AP、券面事項入力補助APにはそれぞれAPの真贋判定機能(内部認証)が備わっており、公開鍵証明書を用いた内部認証が可能となっている。

○ JPKI APの真正性については、利用者証明用電子証明書または署名用証明書による署名への検証をもって確認できるため、真贋判定機能が搭載されていない。しかし、先の通常国会で署名を行わず電子証明書のみを利用する規定が承認されたことから、JPKI APにおける真贋性判定機能が求められることとなった。

2. 課題・論点

○ JPKI APにも、他の3つのカードAPと同様にAPの真贋性を判定する機能を実装してはどうか。

(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ができないか。

1. 現行のカード仕様及び運用

○ 電子証明書の失効理由「affiliationChanged」には、死亡や海外転出、職権消除が含まれており、失効理由から死亡だけを特定することができない。このため、affiliationChangedが指定された利用者証明用電子証明書の失効件数の内訳を特別に調べていたところ、内訳は以下のとおり。(令和４年)

①死亡：約157万件　②海外転出：約12万件　③その他職権消除（国籍喪失等）：約12万件

※証明書失効リスト(CRL)に当該電子証明書の情報（シリアル番号、失効年月日、失効事由）が記載される。JPKIではRFC5280※※の規定に従い失効事由には以下のコードを使用。

No.	失効事由に指定されるコード	定義
1	unspecified(0)	証明書を交付前に破棄した
2	keyCompromise(1)	証明書利用者の秘密鍵が危殆化（漏洩）した
3	cACompromise(2)	認証局の秘密鍵が危殆化（漏洩）した
4	**affiliationChanged(3)**	**証明書の記載内容に変更が生じた**
5	superseded(4)	証明書を取り替えた
6	cessationOfOperation(5)	証明書の必要性がなくなった（使用しなくなった）
7	certificateHold(6)	秘密鍵の安全性に被疑が生じたため、証明書を一時的に保留する

※※Internet X.509 Public Key Infrastructure Certificate and CertificateRevocation List (CRL) Profile

2. 課題・論点

○ 死亡による失効だけを特定できるようにすべきとの要望があることから、「死亡」の細分を設けることができないか

(11)個人番号カードの呼称の変更／(12)インターフェイス仕様の公開

次期個人番号カードの導入に合わせ、「マイナンバーカード」以外の新たな呼称を採用するか。また、その場合、いかなる呼称が適当か。

1. 現行のカード仕様及び運用

○ 法制上の名称は「個人番号カード」だが、従来より、「マイナンバーカード」という呼称を統一的に用いている。

2. 課題・論点

○ マイナンバーカードを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、こうしたケースでも、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ために、「マイナンバーカード」の名称を変える必要があるとの意見もあるがどう取り扱うか。仮に、変えるとするならば、いかなる呼称が考えられるか。

カードの利用を促進するために、カードのインターフェイス仕様(APDU仕様書)を公開できないか。

1. 現行のカード仕様及び運用

○ マイナンバーカードの利用者において必要とする技術仕様は非公開となっている。

2. 課題・論点

○ アプリの開発やカードの利用の促進にとって、公開されることが望ましいため、カードAP仕様書・インターフェイス仕様書を公開すべきではないか。

(13)（長期的論点）将来的な物理カードの必要性

スマートフォンのマイナンバーカード機能の搭載が実現され、普及した後には、物理的なカードはそもそも不要とならないか。

1. 現行のカード仕様及び運用

○ 令和5年5月にスマートフォンへのマイナンバーカードの電子証明書機能の搭載を開始し、電子証明書機能以外のマイナンバーカード機能についても、スマートフォンへの搭載を進めている。

○ 本サービスは、マイナンバーカード保有者のうち希望する者にスマホ搭載の電子証明書機能サービスを提供するものである。マイナンバーカード自体の保有を条件としている理由は、以下のとおり。

- スマートフォンを保有していない国民はまだ多く、マイナンバーカードをなくしスマートフォンをメインとすることは難しい。
- スマートフォンのライフサイクルは概ね5年程度と短く、スマートフォンをメインとすると逆に頻繁な更新手続きが必要となる。
- マイナンバーカードによる本人確認がバックアップとして使えれば、ユーザが希望する任意のスマホにカード機能の搭載を行うことができる。普段はカードを持ち歩く必要がない一方、スマホの紛失・不具合などの場合は、必要な新たなスマホへの再発行を自ら行うことができる。

※ＥＵにおいても、スマートフォンへの国民IDの搭載（EU DI Wallet）の検討が進められているが、その発行等には、日本と同様に、国民IDカードによる本人確認が必要であり、国民IDカードの存続が前提となっている。

2. 課題・論点

○ スマートフォンでマイナンバーカードの機能を果たすことができるようになれば、マイナンバーカードの発行は不要ではないか、との意見があるが、上記理由により、カード自体の発行を不要とする必要はないのではないか。

○ ただし、スマホ搭載が進めば、スマートフォン上の認証機能（顔認証、指紋認証）等を積極的に活用することができ利便性が高いと考えられるため、スマホ搭載の普及を更に積極的に進めるべきではないか。

○ 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べきか。