

# 本人確認手法の公的個人認証 一本化と金融機関の課題

## 最短で25年度から施行、 支店窓口事務に影響する可能性も

2023年、政府は遠隔での本人確認手法をマイナンバーカードによる公的個人認証サービス「JPKI=Japanese Public Key Infrastructure」へ一本化する方針を公表した。その背景には、偽造本人確認書類による犯罪の増加がある。本稿では、電子的な本人確認（eKYC）を取り巻く環境や、JPKIによる認証方法について概観するとともに、今後金融機関に求められる対応について整理する。

### 犯罪抑制のため JPKIに統一

政府は2023年6月9日、「デジタル社会の実現に向けた重点計画」を閣議決定した。この計画は、デジタル社会の実現に向けた政府の重点施策であり、その中の「マイナンバーカード

の機能拡充と安心安全対策」において、犯罪収益移転防止法施行規則に基づく本人確認手法を「マイナンバーカードによる公的個人認証サービス」（JPKI）へ一本化する方針が明記された。JPKIは、マイナンバーカードのICチップ内に格納された電子証明書を用い、本人

しか作成できない電子署名の真正性を、電子的かつ専用の認証機関により検証する手法である。計画では、24年度中のJPKI一本化方針の確定、25年度から「十分な準備期間」を確保した上での施行という工程が示されており、金融機関には最短で25年度からの一本化に向けた取

SocioFuture  
ソリューション企画本部

課長 佐野祥吾



グループリーダー

金山優也



り組みが求められる。

政府がJPKI一本化を急ピッチで進める目的には、事務効率化のほか、本人確認の厳正化による犯罪抑制がある。近年、金融業界では本人確認書類の偽造による犯罪が多発している。全国銀行協会「口座不正利用に伴う口座の利用停止・強制解約等の件数の推移」によると、口座不正利用に伴う口座の利用停止・強制解約件数は20～22年度に約3万件（増加率165%）増えている。これは、偽造技術の向上などによって「本人確認書類を目視で確認する真贋判定には限界がある」ことを物語っている。

## 「チェックを 活用したJPKI」

JPKIは極めてセキュリティ強度が高い認証である。その手法について解説する。なお、混同されがちだが、12桁の個人番号「マイナンバー」は法令で定められた事務手続きに使われるもので、本稿で対象とする「マイナンバーカード」はその12桁の個人番号などが記載され

たICカード身分証である。JPKIは、マイナンバーカードに搭載されたICを活用した本人確認手法である。

マイナンバーカードが持つ情報は、①券面記載事項と②IC内アプレット（AP）の2種類に分けられる。

①券面記載事項について、表側には顔写真と基本4情報（氏名・生年月日・住所・性別）等が、裏側にはマイナンバー等が記載されており、券面のみでも本人確認書類としての利用が可能である。しかし、券面記載事項の目視確認のみでは真贋判定は難しく、実際、議員を標的としたスマートフォン乗っ取りによる犯罪に悪用された。そのため、マイナンバーカードの信頼性に疑義を示す意見もあるが、政府の求めているJPKIは次の②を活用した手法である。

②IC内APによる本人確認は、電子証明書を用いた公開鍵認証基盤（PKI = Public Infrastructure）の仕組みに基づき行われる。ここでは、公開鍵暗号方式（PKI = Public Key Cryptography）という手

法が使われる。これは、本人のみが保有し他者へ開示しない、巨大な乱数である「秘密鍵」と、その秘密鍵とペアになる、検証者へ開示する「公開鍵」を組み合わせた手法である。秘密鍵で生成された電子署名は、ペアとなる公開鍵を用いることで、その真正性を暗号的に検証することができる。

さらに、権威ある第三者認証局が、秘密鍵の持ち主を確認した上で、公開鍵を電子証明書というかたちで発行する。そうすることで、電子署名と電子証明書を受け取った検証者は、その署名が秘密鍵の持ち主によって生成されたことと、その秘密鍵の持ち主が誰なのかを検証することができる。この方法は、極めてセキュリティ強度の高い手法と見なされており、電子メールの送付や、ウェブサイトでデータの交換といった場面で利用されている。

この秘密鍵を耐タンパー性（無理にデータを取り出そうとすると自壊する機構）のあるICカード内で生成し、本人によるパスワードの入力を必須とす

る。その上で電子証明書の有効性を国自身（地方公共団体情報システム機構J-LIS）が認証する。この一連の手法をJPKIと呼んでいる。

## JPKIの安全性は 最高の「レベル3」

わが国では「デジタルで本人を確認することについて、各府省情報統括責任者（CIO）連絡会議でガイドラインとして定義される。そして、国際的な基準（米国家标准800-63-3等）を参考に、その真正性を二つの要素で評価している（図表1）。

一つ目の判定基準は「身元確認保証レベル（IAL = Identity Assurance Level）」である。「身元確認」とは、ある個人が初回到事業者サービスへアクセスした際、その人物の本人特定事項（身元情報、氏名や住所等）を確認し、当該人物が実在する一意の自然人であることを確認して事業者の台帳に登録するプロセスのこと。IALとは、身元確認における信頼性の度合いを示すものである。

〔図表1〕

本人確認の真正性の二要素評価

レベル	身元確認保証レベル (IAL)		本人認証保証レベル (AAL)		オンラインによる手法例
	概要	詳細	概要	詳細	
レベル3	対面での身元確認	身元確認された本人の信用が高い	耐タンパー性が確保された電子	請求者からの3要素のうち、複数の要素を含むことにより信用度が非常に高い	<ul style="list-style-type: none"> <li>マイナンバーカード（公的個人認証＝署名用電子証明書）による身元確認、アカウント作成後のマイナンバーカード（公的個人認証＝利用者証明用電子証明書）の耐タンパー性ハードウェアトークンによる本人認証を実施。</li> <li>申請データに対するマイナンバーカード（公的個人認証＝署名用電子証明書）による電子署名を付与。</li> <li>※耐タンパー性ハードウェアトークンの例＝PIN+ICカード（マイナンバーカード）</li> </ul>
レベル2	遠隔または対面での身元確認	身元確認された本人の信用が相当	複数の認証要素	請求者からの3要素のうち、複数の要素を使用することにより信用度が相当	<ul style="list-style-type: none"> <li>マイナンバーカード（公的個人認証＝署名用電子証明書）等による身元確認、アカウント作成後のマイナンバーカード（公的個人認証＝利用者証明用電子証明書）もしくはこれによることができない場合、その他の多要素認証による本人認証を実施。</li> <li>マイナンバーカードによるオンラインでの身元確認が行えない場合、対面での身分証明書等の確認や郵送した申込書（押印付き）、印鑑証明書、公的証明書（住民票等）等の確認によりアカウントを作成。</li> </ul>
レベル1	身元確認の自己表明	身元確認された本人の信用が自己表明に相当	単一または複数の認証要素	請求者からの3要素のうち、単一の要素を使用することにより信用度が相当程度	身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後は単一要素認証で本人認証を実施

〔出所〕 各府省情報化統括責任者（CIO）連絡会議決定「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日付。

二つ目の判断基準は「本人認証保証レベル（AAL）＝Authenticator Assurance Level」である。これは、台帳登録済みの個人がサービスにアクセスした際に、その個人が、事業者が想定する当人であるかを検証する際の信頼性の度合いを示すものである。IALとAALとも、3段階での基準が示され、マイナンバーカードは居住自治体窓口による対面での本人確認と住民基本台帳を元に発行しているため、IALは最高の「レベル3」であり、対タンパー性のあるマイナンバーカードIC内の署名用電子証明書をを用いた電子認証もAALで「レベル3」と評価される。

を用いた手法は、ガイドラインにおける最高水準の真正性を持つ、保証レベル3の本人確認である。

**容貌確認の限界が露呈し JPKI早期導入へ**

JPKIへの一化が特に強く求められるのが、金融機関を含む、犯刑法における特定事業者（金融、不動産、電話、士業等）である。金融機関としては口座開設や大口現金取引といった特定取引での利用が求められる。特に遠隔での口座開設時の本人確認方法（eKYC）においてJPKI一化が求められる。

現状、犯刑法に即した手法（犯刑法施行規則6-1-1、図表2）のうち、最も採用されているものは「本人確認書類＋容貌確認のホ方式」である（当社調べ）。これは、免許証等の本人確認書類の券面や厚みをスマホ等で撮影・アップロードし、書類の顔写真と本人の容貌写真に相違がないかの確認を行う手法である。真贋判定を行うシステムの導入や目視で判定できる「職人」の育成により、各金融

〔図表2〕

銀行における一般的なeKYC手法例

改竄防止策	容貌		電子証明書		
方法	写真付き本人確認書類（画像）+ 容貌画像	写真付き本人確認書類（ICチップ情報）+ 容貌画像	民間認定認証事業者が発行する電子証明書による認証	マイナンバーカードの公的個人認証による認証	PF事業者が発行する電子証明書による認証
犯収法施行規則	ホ	ヘ	ヲ	ワ	カ
携帯法施行規則	ハ	ニ	チ	チ	チ
携帯法施行規則見直し方針案	廃止	存置	存置	存置	存置

（出所） 金融庁資料、犯収法施行規則、携帯法施行規則見直し案から筆者作成。

機関は偽造書類の申請を排除しているものの、前述の犯罪被害のニュースからも分かるように書類の偽造技術は日々向上しており、いずれ認証判断の信頼度にも限界が来ると考えられる。加えて、ディープフェイクで画像認証を突破した事例など最新技術の犯罪利用も予想され、恒久的にこの手法で本人確認を続けるのは難しい。

現在では「十分な準備期間」を確保した上でのJPKIへの移行が政府から宣言されている段階である。とはいえ、近年の金融犯罪の活発化によって、早期でのJPKI（犯収法施行規則での「ワ」方式）への一本化が強く求められると考えられる。

### JPKI導入には 検証事業者選定が重要

検討が必要な要素は事務規程の見直しとパートナー企業の設定である。

事務規程の見直しは金融機関で完結するが、JPKIの利用に際してはプラットフォーム（PF）事業者のパートナー選定が必要となる。

JPKIでJ-LISに照会を行うことができるのは、主務大臣（総務大臣、デジタル大臣）に認定されたPF事業者に限られる。PF事業者は利用者の電子証明書を安全な認定設備内に保管することが義務付けられており、厳しい審査基準を通過する必要がある。

JPKIを本人確認業務に活用したい事業者は、JPKIの署名検証業務の全部をPF事業者に委託することで、厳しい設備基準を満たすことなく、簡易的な手続きで主務大臣の認定を得ることが可能。このような事業者はサービスピロバイダー（SP）事業者（みなし認定事業者）と呼ばれる。

特に、SP事業者についてはデジタルIDを包括的に提供するなど、付加価値を持つ事業者も存在する。そのため、金融機関がJPKIを利用する際には、関係各社から情報収集し、どのような仕組みが自社の環境に則しているか検討する必要がある。

### 厳正化が求められる 携帯電話事業者

本人確認の厳正化を特に求められるのが、携帯電話事業者である。匿名や偽名で発行された携帯電話が犯罪に利用される事例が多く、早急な携帯電話不正利用防止法（以下、携帯法）施行規則の見直し対応が求められている。その対策の一環として、24年5月15日に総務省の「ICTサービスの利用環境の整備に関する研究会」内で、「不適正利用対策に関するワーキンググループ（第4回）」が開催された。

この研究会における当面の検討課題は「特殊詐欺等のICTサービスの不適正利用への対処」であり、第4回会合においては、携帯法に基づく本人確認方法の見直し（JPKIへの一本化）について、関係者から意見が募られた。その中で、一本化の方向性には賛同するものの、対面での不正リスク拡大懸念から、対面についても同時期にJPKIへ一本化してほしいとの要望が関係者意見の中で寄せられた。

これは遠隔ではJPKIによる厳格な本人確認を行ったとし

業態と根拠法令、所管省庁

業態	根拠法令	所管省庁
金融機関	犯罪収益移転防止法	警察庁
携帯電話事業者	携帯電話不正利用防止法	総務省・警察庁

(出所) 各種資料から筆者作成。

## 完全には防げない マイナカード貸与

JPKIによる安全性については前述したが、遠隔での不正利用を完全に排除することは難

でも、対面でも、対面での券面の目視確認による手続きが可能なた態が継続すると、対面での抜け穴を目的とした不正利用者が窓口に入流する懸念があるからである。根拠法令や所管省庁が異なる(図表3)ものの、

電子証明書をを用いない手法と比してのJPKIの安全性は極めて高いが、それは「マイナンバーカードも電子証明書を利用するためのパスワードも他者に貸与・開示されない」という前提での考え方である。前述のように、さまざまな契約が可能となる媒体・情報の貸与は本来起り得るものではないが、可能性を完全には排除できない。デジタル庁「本人確認ガイドラインの改定に向けた有識者会議」第5回会議(24年2月27日)での「本人確認ガイドライン改定方針令和5年度中間とりまとめ(案)協議用資料」においても、脅威耐性に係る考慮事項として次のように記載されている。「マイナンバーカードによる本人確認手法でも暗証番号のみでの確認では、容貌照合を行わないため、カードの貸し借りは検知できない点に留意する必要がある」。

こうした懸念から、法令的な基準はJPKI利用のみで達成できるものの、「念のため」や将来的な犯罪対策での利用を想定し、申請者の容貌確認・保存

を追加要件として考慮したいとの意見を持つ金融機関は複数存在する。「法令準拠の本人認証」と「実務的に完全な本人認証」との間にはなお差異があり、金融業界としてどこまで対応すべきか議論を尽くす必要がある。

\* \* \*

24年7月現在、マイナンバーカードの交付枚数(累計)は約1億枚となり、人口に占める割合は率は約80%となった。

運転免許証の普及率は66%(21年時点)、パスポートは17%(同)である。両者の重複保有を考慮すれば、本人確認書類としてマイナンバーカードの方が普及したとも言える。健康保険証と運転免許証、在留カードとの一体化方針を踏まえると、今後、日本国内において、マイナンバーカードが唯一の本人確認書類として取り扱われていくだろう。官民問わず利用者認証においては、マイナンバーカード利用が前提となる。

特に金融機関においては、JPKIを利用した最新の利用者情報(4情報)提供サービス

(利用者の同意を得て変更後住所等をJ-LISから取得可能)など政府主導での機能拡充もされている。前述の特定取引時のJPKI対応にとどまらず、マイナンバーカードを核とした業務設計が求められる。

個別案件ごとのパートナー選定も短期的には重要であるが、各金融機関には既存の業務にどのようにマイナンバーカードを融合させていくか、あるべき姿を描いていくことが肝要である。

さのしように

11年明治大学商学部卒。日本ATM(現SocioFuture)入社。金融機関のリテール戦略立案支援や関連知識に基づく論文、書籍を執筆。22年から現職。デジタルID、マイナンバーカード関連の企画立案を検討。

かなやま ゆうや

18年東洋大学国際地域学部卒。日本ATM(現SocioFuture)入社。流通系金融機関や系統系金融機関の営業等に従事。22年から現職。デジタルID、マイナンバーカード関連の企画立案を検討。