

本人確認実務の課題・事例・手法とそのガイドラインに関する有識者会議（第1回）

身元確認手法の具体例について

令和7年9月 デジタル庁 トラストタスクフォース

はじめに

本資料の位置づけ

本人確認ガイドラインの改定にあわせ、具体的な手法例等を取りまとめた「解説書」を準備中。

本資料は「[解説書](#)」に掲載予定の**主要な本人確認手法**に関して、その概要、脅威耐性、考慮事項、その他の関連する[コラム](#)の案を、有識者会議での協議用資料として取りまとめたものである。

本人確認ガイドライン 本編
(改定版の発行に向け現在手続中)

位置づけ：Normative

(遵守する内容)

本人確認の概念、基本的な枠組み、検討のプロセスなど、原則的・普遍的で陳腐化しにくい情報をとりまとめる

読み手の負担を軽減するため、本編はできる限りシンプルな内容に留めてページ数を抑え、参考情報は「解説書」に移動する

比較的長期間の改定サイクルを想定

デジタル社会推進標準ガイドライン DS-511

行政手続等での本人確認における
デジタルアイデンティティの取扱い
に関するガイドライン

2025年(令和7年)XX月XX日

デジタル庁

【ドキュメントの位置付け】

Normative: 政府情報システムの整備及び管理に関するルールとして遵守する内容を定めたドキュメント

【キーワード】

本人確認、デジタルアイデンティティ、身元確認、本人認証、フェデレーション、対象手続のデジタル化、マイナンバーカード、公的個人認証

【概要】

国の行政機関が行政手続等において申請者の本人確認を行う際のデジタルアイデンティティに関する枠組み、対策基準、リスクの評価手順、本人確認手法の選定方法等を示した標準ガイドライン附属文書。

本人確認ガイドライン 解説書 (仮称)
(2025年度内の発行に向け執筆中)

位置づけ：Informative

(参考情報)

本人確認ガイドライン本編の参考資料として、

- ・採用候補となる**具体的手法**
- ・実際の事例、留意点
- ・検討用ワークシート

などの情報をとりまとめる

技術や脅威の動向等を踏まえつつ、比較的短期間のサイクルでの継続的な改定を行う運用を想定

デジタル社会推進実践ガイドブック DS-512

行政手続等での本人確認における
デジタルアイデンティティの取扱い
に関するガイドライン
解説書

2025年(令和x年)XX月XX日

デジタル庁

【ドキュメントの位置付け】

Informative
参考とするドキュメント

【キーワード】

本人確認、デジタルアイデンティティ、身元確認、本人認証、フェデレーション、行政手続のデジタル化、マイナンバーカード、公的個人認証

【概要】

「DS-511 行政手続等における本人確認及びデジタルアイデンティティに関するガイドライン」に基づく本人確認手法の検討にあたる解説や補足を記載した参考文書。

はじめに

解説書に記載予定の具体手法一覧（身元確認手法）

本人確認ガイドライン解説書では、以下に示す身元確認手法を具体例として掲載することを予定している。

掲載予定の身元確認手法

- 1) 実物のマイナンバーカード（券面事項入力補助AP）
- 2) 実物のマイナンバーカード（署名用電子証明書）
- 3) 実物のマイナンバーカード（利用者証明用電子証明書）
- 4) 実物のマイナンバーカード（対面確認アプリ）
- 5) スマートフォンのマイナンバーカード（属性証明機能）
- 6) スマートフォンのマイナンバーカード（電子証明書機能）
- 7) スマートフォンのマイナンバーカード（対面確認アプリ）
- 8) 写真付き本人確認書類の対面確認
- 9) 本人確認書類の撮影＋申請者の容貌の撮影
- 10) 本人確認書類の郵送＋住所への到達確認

身元確認に関連するコラム

- コラム1) 身元確認の実施担当者に対する訓練等について
- コラム2) 電子メールでの手続における身元確認について
- コラム3) 郵便を使った身元確認について
- コラム4) スマートフォンに搭載された本人確認書類について

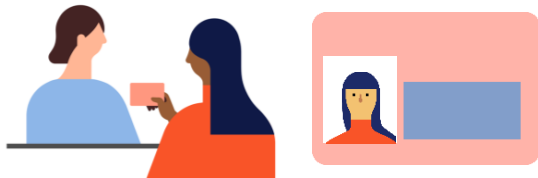
身元確認の概要

（「本人確認ガイドライン改定方針 令和6年度とりまとめ」より一部抜粋・編集）

本人確認の基本的要素

本人確認ガイドライン改定案では、本人確認の構成要素を「身元確認」、「当人認証」及び「フェデレーション」とし、それぞれを以下のように定義。

身元確認 (Identity Proofing)



申請者を一意に識別するとともに、その実在性を確認すること。

具体的には、申請者の属性情報を収集することで、申請者を一意に識別するとともに、収集した属性情報が真正かつ申請者自身のものであることを本人確認書類により検証することで、申請者が実在かつ生存する人物であることを確認する。

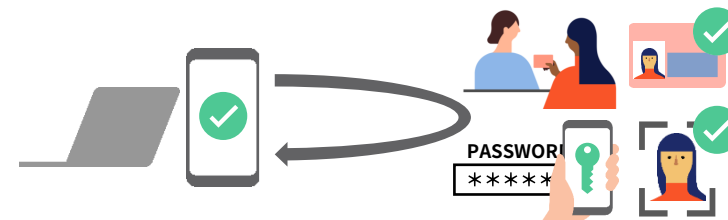
当人認証 (Authentication)



申請者の当人性を確認すること。

具体的には、対象手続を利用しようとする者が、身元確認時に登録された者と同じの人物であることを、申請者と紐づけて登録した認証器を用いて確認する。

フェデレーション (Federation)

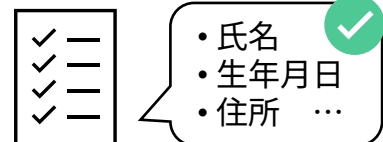
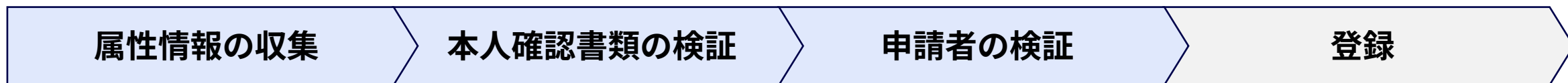


身元確認や当人認証を、他者に依拠して実現すること。

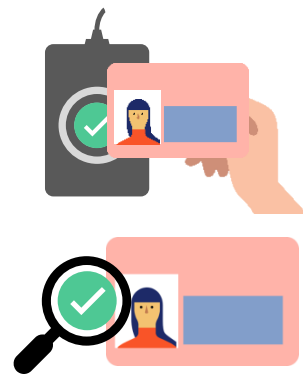
具体的には、信頼できるIDプロバイダと連携し、IDプロバイダによって行われた身元確認や当人認証の結果に関する情報を入手することで、対象手続における本人確認を実現する。

身元確認のプロセスの定義

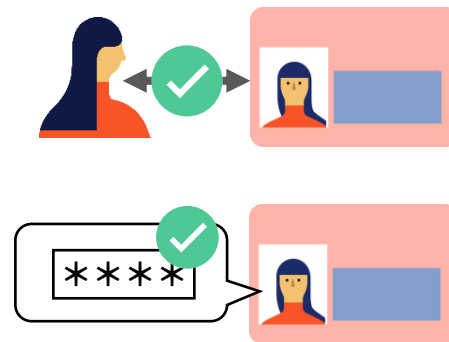
身元確認は、「属性情報の収集」「本人確認書類の検証」「申請者の検証」の3つのプロセスによって定義。また、身元確認完了後の「登録」についても明記した。



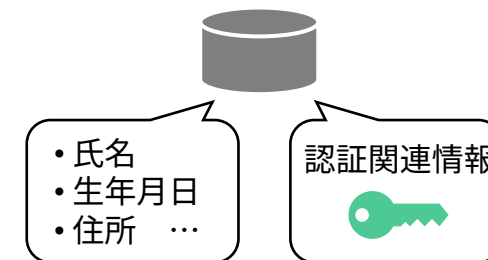
氏名、生年月日、住所等の属性情報を申請者から収集し、申請者を対象とする母集団の中で一意に識別する。



申請者から提示された本人確認書類が、偽造・改ざん・複製等された不正なものでないことを、物理的又は電子的に検証する。



本人確認書類が備える顔写真や暗証番号等を用いて、提出された本人確認書類が確かに申請者自身のものであることを検証する。



身元確認の結果をもとに、利用者の属性情報や本人認証のための認証関連情報を登録する。

身元確認における脅威

身元確認における主な脅威を、以下のように身元確認の各プロセスと紐づけて整理した。

No.	主な脅威	脅威の概要	対策プロセス
1	重複登録	申請情報の不足や誤り等によって、同一の申請者による重複申請を検知できずに受け付けてしまう	属性情報の収集
2	別人との誤紐づけ	申請情報の不足や誤り等によって、申請者と別の人物とを区別できなくなり、誤った人物の情報と紐づけてしまう	
3	本人確認書類の偽造・改ざん	偽造又は改ざんされた本人確認書類によって、実在する別の人物や架空の人物になりすまされる	本人確認書類の検証
4	本人確認書類の複製	電子的又は物理的に複製された本人確認書類によって、実在する別の人物になりすまされる	
5	本人確認書類の盗用	盗まれた本人確認書類によって、実在する別の人物になりすまされる	申請者の検証
6	本人確認書類の貸し借り	貸し借りされた本人確認書類によって、実在する別の人物になりすまされる	

身元確認の手法の体系化

身元確認のための手法は、以下のとおり体系化して整理。

また、それぞれに該当する具体的な手法名（例えば「マイナンバーカードの署名用電子証明書」など）については本編には詳細を記載せず、「解説書」において技術仕様や留意点等を解説する方針とした。

属性情報の収集手法例

a) 電子的な読取り

- ・ スマートフォンやICカードリーダーを用いて、本人確認書類のICチップから電子データを読み取る

b) 物理的な読取り

- ・ OCR等を用いて本人確認書類の券面の記載情報を物理的に読み取る

c) 申請者自身による記入・入力

- ・ 紙の申請書やWebフォームに申請者自身による記入や入力を求める

d) IDプロバイダからの情報取得

- ・ IDプロバイダとの連携により身元確認済みの属性情報を取得する

本人確認書類の検証手法例

a) デジタル署名の検証

- ・ 本人確認書類から読み取った電子データのデジタル署名を検証する

b) 信頼できる情報源への照会

- ・ 参照番号やQRコードなどにより発行元等に情報を照会する

c) 対面での物理的検査

- ・ 本人確認書類の券面を、対面にて目視・触覚等で検査する

d) 非対面での物理的検査

- ・ 本人確認書類の券面を、カメラ映像や複写物等によって検査する

申請者の検証手法例

a) 対面での容貌確認

- ・ 本人確認書類の顔写真と申請者の容貌を目視にて比較する

b) 非対面での容貌確認

- ・ 本人確認書類の顔写真と申請者の容貌をカメラ映像等で比較する

c) 暗証番号等による検証

- ・ 本人確認書類が備える暗証番号等の認証機能によって、申請者が本人確認書類の持ち主であることを確認する

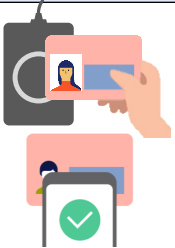


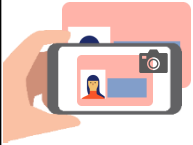

d) 住所への到達確認による検証

- ・ 本人確認書類に記載された住所に確認コードを郵送するなどして申請者へと到達できることを確認することで、申請者が本人確認書類の持ち主であることを確認する

身元確認保証レベル — 全体概要

昨今の脅威動向を踏まえ、身元確認保証レベルは「ICチップ等によるデジタル的な検証の有無」を、保証レベルの差として表現できるように改定。また低リスクの手続・サービス向けの保証レベルとして「レベル1」を定義*。

(※改定前のガイドラインの「レベル1」は「身元確認なし」の位置づけであったが、今回の改定で簡易的な身元確認を行うレベルとして再定義する。)

保証レベル	保証レベルの位置づけ	
	本人確認書類の検証手法	申請者の検証手法
身元確認保証レベル3	 <ul style="list-style-type: none"> ICチップ等によるデジタル的な検証を必須とし、偽造や改ざんに対する厳格な耐性を確保するレベルとする。 (「デジタル的な検証」：発行者によって付与されたデジタル署名等による暗号学的な検証を行うこと。) 	 <ul style="list-style-type: none"> 本人確認書類の盗用に対し、対面での容貌確認、非対面での容貌確認又は暗証番号による検証を必須とする。
身元確認保証レベル2	 <ul style="list-style-type: none"> 本人確認書類の対面での物理的検査等も許容する。ただし検証強度を考慮しカメラ越しや複写物による検査（非対面での物理的検査）は不可とし、一定の耐性を確保する。 	<p>暗証番号: ****</p> <ul style="list-style-type: none"> 本人確認書類の貸し借りに対しては、<u>対象手続のリスクに応じた個別検討*</u>を行うこととする。 <p>※ 暗証番号のみでは本人確認書類の貸し借りを検知できないため、貸し借りのリスクを許容できない場合は「容貌の確認」の追加実施等を検討する。</p>
身元確認保証レベル1	 <ul style="list-style-type: none"> 保証レベル2までの手法に加えて、非対面での物理的検査（カメラでの撮影、複写物の郵送等）も許容する。偽造・改ざんへの簡易的な耐性をもつレベルとして位置付ける。 	 <ul style="list-style-type: none"> 保証レベル2までの手法に加えて、住所への到達確認による検証も許容する。 (本人確認書類に記載されている住所に居住していることの確認をもって、本人確認書類との紐づきを検証する手法)

身元確認保証レベル — 各レベルの対策基準

前述の「位置づけ」に基づき、各レベルの対策基準は以下のとおりとした。

※対策基準はあくまで基準であり、同等の脅威耐性を確保できる場合は他の手法等を用いてもよいものとして位置づけ。

保証レベル	対策基準 (青字：上位レベルとの差分)		
	属性情報の収集 	本人確認書類の検証 	申請者の検証 
身元確認保証レベル3	電子的な読取り	デジタル署名の検証	以下のいずれか <ul style="list-style-type: none"> 対面での容貌確認 非対面での容貌確認 暗証番号等による検証
身元確認保証レベル2	(収集手法は任意とする)	以下のいずれか <ul style="list-style-type: none"> デジタル署名の検証 信頼できる情報源への照会 対面での物理的検査 	以下のいずれか <ul style="list-style-type: none"> 対面での容貌確認 非対面での容貌確認 暗証番号等による検証
身元確認保証レベル1	(収集手法は任意とする)	以下のいずれか <ul style="list-style-type: none"> デジタル署名の検証 信頼できる情報源への照会 対面での物理的検査 非対面での物理的検査 	以下のいずれか <ul style="list-style-type: none"> 対面での容貌確認 非対面での容貌確認 暗証番号等による検証 住所への到達確認による検証

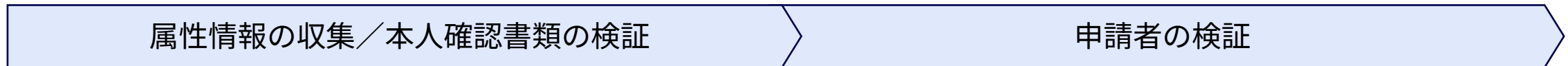
1. 身元確認手法の具体例

- 1) 実物のマイナンバーカード（券面事項入力補助AP）
- 2) 実物のマイナンバーカード（署名用電子証明書）
- 3) 実物のマイナンバーカード（利用者証明用電子証明書）
- 4) 実物のマイナンバーカード（対面確認アプリ）
- 5) スマートフォンのマイナンバーカード（属性証明機能）
- 6) スマートフォンのマイナンバーカード（電子証明書機能）
- 7) スマートフォンのマイナンバーカード（対面確認アプリ）
- 8) 写真付き本人確認書類の対面確認
- 9) 本人確認書類の撮影＋申請者の容貌の撮影
- 10) 本人確認書類の郵送＋住所への到達確認

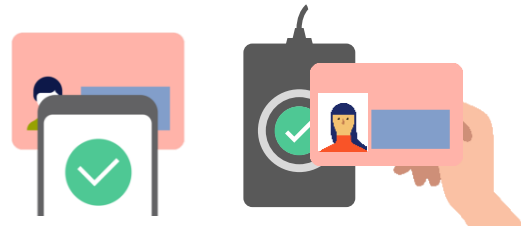
実物のマイナンバーカード（券面事項入力補助AP） — 概要

マイナンバーカードの「券面事項入力補助AP」は、カードの券面に記載されている事項（マイナンバー及び基本4情報）を電子データとして読み取ることができる機能である。

これを適切に用いることで、[身元確認保証レベル3](#)の身元確認を実現できる。



マイナンバーカードの読み取り
（券面事項入力補助AP）



- マイナンバーカードのICチップを読み取り、券面事項入力補助APから基本4情報やマイナンバーを電子的に読み取る
- データに付与されたデジタル署名を検証することで、本人確認書類が偽造・改ざんされたものでないことを検証する

券面事項入力補助用暗証番号
（数字4桁）

+

容貌確認
（必要に応じて実施）



- 券面事項入力補助APを利用する際の暗証番号入力により、本人確認書類が確かに申請者自身のものであることを検証する
- 貸し借りへの対策が必要な場合は、追加の容貌確認（対面又は非対面）を実施する

1) 実物のマイナンバーカード（券面事項入力補助AP）

脅威耐性と考慮事項

主な脅威	脅威への耐性
重複登録	<ul style="list-style-type: none"> 属性情報を電子データとして読み取ることで、誤記や表記揺れ等を防ぎ、属性情報を正確に収集できる。ただし、取り扱うシステムにおける文字コードや異体字・外字の整合等についての留意が必要。 個人番号取扱事務においては、マイナンバーによる正確な識別と紐づけが可能。
別人との誤紐づけ	
本人確認書類の偽造・改ざん	<ul style="list-style-type: none"> 券面事項入力補助APから取得したデータに付与されたデジタル署名を検証することで、それが偽造・改ざんされたものでないことを暗号的な強度で検証できる。
本人確認書類の複製	<ul style="list-style-type: none"> マイナンバーカードのICチップが有する耐タンパ性により、電子的な複製への耐性を備える。
本人確認書類の盗用	<ul style="list-style-type: none"> 券面事項入力補助用暗証番号（数字4桁）の入力をもって、本人確認書類が盗用されたものではなく、確かに申請者自身のものであることを検証できる。
本人確認書類の貸し借り	<ul style="list-style-type: none"> 暗証番号とともにマイナンバーカードの貸し借りが行われた場合は検知できない。貸し借りの検知が必要な場合は、対面又は非対面による容貌確認を追加実施する必要がある。

観点	考慮事項
事業目的の遂行	<ul style="list-style-type: none"> マイナンバーカードを保有していない方、暗証番号を覚えていない方、紛失中の方などの存在を考慮し、事業目的や公平性の観点から必要と判断される場合には、他の手法との併用や例外措置を検討する必要がある。
公平性	
プライバシー	<ul style="list-style-type: none"> 特筆すべき考慮事項はない。
アクセシビリティ及びユーザビリティ	<ul style="list-style-type: none"> マイナンバーカードの他の機能と併用する場合、カードの読み取りや暗証番号入力が複数回発生することに留意する必要がある。
セキュリティ	<ul style="list-style-type: none"> 左記のとおり、暗証番号のみでは貸し借りへの耐性を有さない。
その他	<ul style="list-style-type: none"> 券面事項入力補助APの利用に照合番号A／照合番号Bを用いた場合は「申請者の検証」としての機能を果たさないことに留意が必要。

1. 身元確認手法の具体例

- 1) 実物のマイナンバーカード（券面事項入力補助AP）
- 2) 実物のマイナンバーカード（署名用電子証明書）
- 3) 実物のマイナンバーカード（利用者証明用電子証明書）
- 4) 実物のマイナンバーカード（対面確認アプリ）
- 5) スマートフォンのマイナンバーカード（属性証明機能）
- 6) スマートフォンのマイナンバーカード（電子証明書機能）
- 7) スマートフォンのマイナンバーカード（対面確認アプリ）
- 8) 写真付き本人確認書類の対面確認
- 9) 本人確認書類の撮影＋申請者の容貌の撮影
- 10) 本人確認書類の郵送＋住所への到達確認

2) 実物のマイナンバーカード（署名用電子証明書）

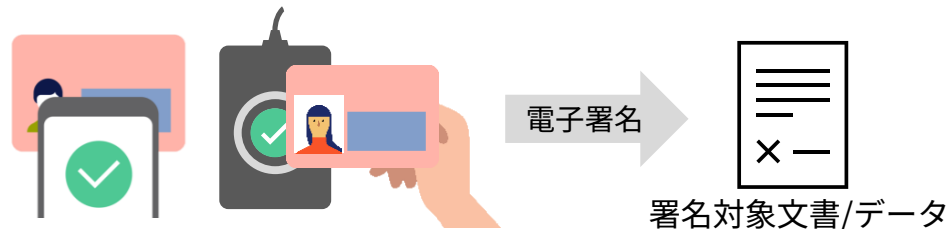
実物のマイナンバーカード（署名用電子証明書） — 概要

マイナンバーカードの公的個人認証APによって電子署名を行う場合、署名用電子証明書内の基本4情報をデータとして電子的に読み取ることができる。

これを適切に用いることで、[身元確認保証レベル3](#)の身元確認を実現できる。



マイナンバーカードの読み取りによる電子署名
(公的個人認証AP)



署名用パスワード
(英数字6～16桁)

+

容貌確認
(必要に応じて実施)



- マイナンバーカードのICチップを読み取り、公的個人認証APの署名用電子証明書から基本4情報を電子的に読み取る
- データに付与されたデジタル署名を検証することで、本人確認書類が偽造・改ざんされたものでないことを検証する

- 公的個人認証APにより電子署名を行う際の署名用パスワードの入力により、本人確認書類が確かに申請者自身のものであることを検証する
- 貸し借りへの対策が必要な場合は、追加の容貌確認（対面又は非対面）を実施する

2) 実物のマイナンバーカード（署名用電子証明書）

脅威耐性と考慮事項

主な脅威	脅威への耐性
重複登録	<ul style="list-style-type: none"> 属性情報を電子データとして読み取ることで、誤記や表記揺れ等を防ぎ、属性情報を正確に収集できる。ただし、取り扱うシステムにおける文字コードや異体字・外字の整合等についての留意が必要。 署名用電子証明書は転出等により失効するため、身元確認の直前に行われた転居等を検知できる。
別人との誤紐づけ	
本人確認書類の偽造・改ざん	<ul style="list-style-type: none"> 署名用電子証明書に付与された発行元のデジタル署名を検証することで、それが偽造・改ざんされたものではないことを暗号的な強度で検証できる。
本人確認書類の複製	<ul style="list-style-type: none"> マイナンバーカードのICチップが有する耐タンパ性により、電子的な複製への耐性を備える。
本人確認書類の盗用	<ul style="list-style-type: none"> 署名用パスワードの入力をもって、本人確認書類が盗用されたものではなく、確かに申請者自身のものであることを検証できる。
本人確認書類の貸し借り	<ul style="list-style-type: none"> 署名用パスワードとともにマイナンバーカードの貸し借りが行われた場合は検知できない。貸し借りの検知が必要な場合は、対面又は非対面による容貌確認を追加実施する必要がある。

観点	考慮事項
事業目的の遂行	<ul style="list-style-type: none"> マイナンバーカードを保有していない方、署名用パスワードを覚えていない方、紛失中の方に加えて、転居直後やその他の理由で電子証明書を失効中の方などの存在を考慮し、事業目的や公平性の観点から必要と判断される場合には、他の手法との併用や例外措置を検討する必要がある。
公平性	
プライバシー	<ul style="list-style-type: none"> 特筆すべき考慮事項はない。
アクセシビリティ及びユーザビリティ	<ul style="list-style-type: none"> マイナンバーカードの他の機能と併用する場合、カードの読み取りや暗証番号入力回数が増えることに留意する必要がある。
セキュリティ	<ul style="list-style-type: none"> 左記のとおり、署名用パスワードのみでは貸し借りへの耐性を有さない。
その他	<ul style="list-style-type: none"> 手続が電子署名を必要としない場合は、券面事項入力補助APなど、他の機能の利用を検討すべきである。 この機能の取扱いは、公的個人認証法に基づく必要がある。

1. 身元確認手法の具体例

- 1) 実物のマイナンバーカード（券面事項入力補助AP）
- 2) 実物のマイナンバーカード（署名用電子証明書）
- 3) **実物のマイナンバーカード（利用者証明用電子証明書）**
- 4) 実物のマイナンバーカード（対面確認アプリ）
- 5) スマートフォンのマイナンバーカード（属性証明機能）
- 6) スマートフォンのマイナンバーカード（電子証明書機能）
- 7) スマートフォンのマイナンバーカード（対面確認アプリ）
- 8) 写真付き本人確認書類の対面確認
- 9) 本人確認書類の撮影＋申請者の容貌の撮影
- 10) 本人確認書類の郵送＋住所への到達確認

3) 実物のマイナンバーカード（利用者証明用電子証明書）

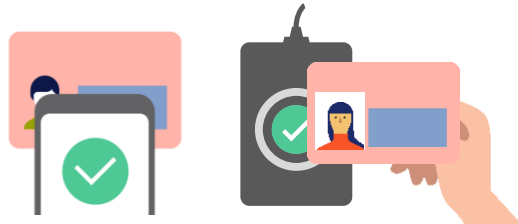
実物のマイナンバーカード（利用者証明用電子証明書） — 概要

マイナンバーカードの公的個人認証APの利用者証明用電子証明書を使って身元確認を行うことも可能である。証明書のシリアル番号による重複登録の検知などが可能となる。ただし、利用者証明用電子証明書には基本4情報等は含まれていないため、必要な場合は「券面事項入力補助AP」など他の手法を併用する必要がある。これを適切に用いることで、[身元確認保証レベル3](#)の身元確認を実現できる。

属性情報の収集／本人確認書類の検証

申請者の検証

マイナンバーカードの読み取り
(公的個人認証AP：利用者証明用電子証明書)



利用者証明用暗証番号
(数字4桁)

+

容貌確認
(必要に応じて実施)



- マイナンバーカードのICチップを読み取り、公的個人認証APの利用者証明用電子証明書から、証明書のシリアル番号を電子的に読み取る
※基本4情報等は「券面事項入力補助AP」など他の手法を併用して収集する。
- データに付与されたデジタル署名を検証することで、本人確認書類が偽造・改ざんされたものでないことを検証する

- 公的個人認証APを利用する際の暗証番号の入力により、本人確認書類が確かに申請者自身のものであることを検証する
- 貸し借りへの対策が必要な場合は、追加の容貌確認（対面又は非対面）を実施する

3) 実物のマイナンバーカード（利用者証明用電子証明書）

脅威耐性と考慮事項

主な脅威	脅威への耐性
重複登録	<ul style="list-style-type: none"> 利用者証明用電子証明書のシリアル番号を収集できるため、重複登録や別人との誤紐づけを確実に防ぐことが可能。
別人との誤紐づけ	
本人確認書類の偽造・改ざん	<ul style="list-style-type: none"> 利用者証明用電子証明書に付与された発行元のデジタル署名を検証することで、それが偽造・改ざんされたものでないことを暗号学的な強度で検証できる。
本人確認書類の複製	<ul style="list-style-type: none"> マイナンバーカードのICチップが有する耐タンパ性により、電子的な複製への耐性を備える。
本人確認書類の盗用	<ul style="list-style-type: none"> 暗証番号の入力をもって、本人確認書類が盗用されたものではなく、確かに申請者自身のものであることを検証できる。
本人確認書類の貸し借り	<ul style="list-style-type: none"> 暗証番号とともにマイナンバーカードの貸し借りが行われた場合は検知できない。貸し借りの検知が必要な場合は、対面又は非対面による容貌確認を追加実施する必要がある。

観点	考慮事項
事業目的の遂行	<ul style="list-style-type: none"> マイナンバーカードを保有していない方、暗証番号を覚えていない方、紛失中の方などの存在を考慮し、事業目的や公平性の観点から必要と判断される場合には、他の手法との併用や例外措置を検討する必要がある。
公平性	
プライバシー	<ul style="list-style-type: none"> 特筆すべき考慮事項はない。
アクセシビリティ及びユーザビリティ	<ul style="list-style-type: none"> 多くの場合、基本4情報等の属性情報を収集するためにマイナンバーカードの他の機能と併用する必要があり、カードの読み取りや暗証番号入力が複数回発生する。
セキュリティ	<ul style="list-style-type: none"> 左記のとおり、暗証番号のみでは貸し借りへの耐性を有さない。
その他	<ul style="list-style-type: none"> この機能の取扱いは、公的個人認証法に基づく必要がある。

1. 身元確認手法の具体例

- 1) 実物のマイナンバーカード（券面事項入力補助AP）
- 2) 実物のマイナンバーカード（署名用電子証明書）
- 3) 実物のマイナンバーカード（利用者証明用電子証明書）
- 4) **実物のマイナンバーカード（対面確認アプリ）**
- 5) スマートフォンのマイナンバーカード（属性証明機能）
- 6) スマートフォンのマイナンバーカード（電子証明書機能）
- 7) スマートフォンのマイナンバーカード（対面確認アプリ）
- 8) 写真付き本人確認書類の対面確認
- 9) 本人確認書類の撮影＋申請者の容貌の撮影
- 10) 本人確認書類の郵送＋住所への到達確認

4) 実物のマイナンバーカード（対面確認アプリ）

マイナンバーカード対面確認アプリによる身元確認 — 概要

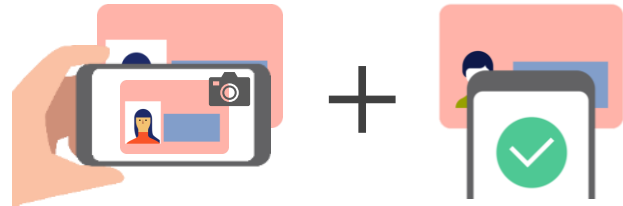
マイナンバーカード対面確認アプリでは、マイナンバーカードの券面事項入力補助APを利用して、ICチップに格納された基本4情報などをアプリ上で確認することができる。

これを適切に用いることで、[身元確認保証レベル3](#)の身元確認を実現できる。

属性情報の収集／本人確認書類の検証

申請者の検証

マイナンバーカードの撮影と読み取り



容貌確認（対面）



- マイナンバーカードの券面を撮影し、照合番号BをOCRによる読み取り又は手入力によって入力する。その後マイナンバーカードのICチップを読み取り、基本4情報、顔写真等を電子的に読み取る
- データに付与されたデジタル署名を検証することで、本人確認書類が偽造・改ざんされたものでないことを検証する

- マイナンバーカードのICチップから読み取った顔写真及びマイナンバーカードの券面の顔写真により対面での容貌確認を行うことで、本人確認書類の盗用や貸し借りが行われていないことを検証する

4) 実物のマイナンバーカード（対面確認アプリ）

脅威耐性と考慮事項

主な脅威	脅威への耐性
重複登録	<ul style="list-style-type: none"> 属性情報を電子データとして読み取ることで、属性情報を正確に収集できる。ただし、個人情報の取り扱いの観点からデータの転送は行わない仕組みのため、他のシステムへのデータ入力を行う場合は入力ミス等への留意が必要となる。 個人番号取扱事務においては、マイナンバーによる正確な識別と紐づけが可能。
別人との誤紐づけ	
本人確認書類の偽造・改ざん	<ul style="list-style-type: none"> 券面事項入力補助APから取得したデータに付与されたデジタル署名を検証することで、それが偽造・改ざんされたものでないことを暗号学的な強度で検証できる。
本人確認書類の複製	<ul style="list-style-type: none"> マイナンバーカードのICチップが有する耐タンパ性により、電子的な複製への耐性を備える。
本人確認書類の盗用	<ul style="list-style-type: none"> 顔写真を用いて対面での容貌確認を行うことで、マイナンバーカードや盗用や貸し借りされたものであることを検証できる。
本人確認書類の貸し借り	

観点	考慮事項
事業目的の遂行	<ul style="list-style-type: none"> マイナンバーカードを保有していない方、紛失中の方などの存在を考慮し、事業目的や公平性の観点から必要と判断される場合には、他の手法との併用や例外措置を検討する必要がある。
公平性	
プライバシー	<ul style="list-style-type: none"> スマートフォンの画面キャプチャを行っても個人情報記録されず、情報が盗用されない仕組みが実装されている。
アクセシビリティ及びユーザビリティ	<ul style="list-style-type: none"> 本手法は、マイナンバーカードの暗証番号を覚えていない場合でも利用できる。
セキュリティ	<ul style="list-style-type: none"> 容貌確認においては、その精度を高めるため、対面確認アプリでICチップから読み取った顔写真データ（白黒）を用いて実物のマイナンバーカードの券面に印刷された顔写真の偽造・改ざんがないことを確認したうえで、その後マイナンバーカードの券面に印刷された顔写真による容貌確認を行うことが望ましい。
その他	<ul style="list-style-type: none"> 対面確認アプリで読み取った属性情報は、個人情報の取り扱いの観点からデータの転送は行わない仕組みのため、他のシステムへのデータ入力を行う場合は入力ミス等を防ぐための対策を講じること。

1. 身元確認手法の具体例

- 1) 実物のマイナンバーカード（券面事項入力補助AP）
- 2) 実物のマイナンバーカード（署名用電子証明書）
- 3) 実物のマイナンバーカード（利用者証明用電子証明書）
- 4) 実物のマイナンバーカード（対面確認アプリ）
- 5) スマートフォンのマイナンバーカード（属性証明機能）
- 6) スマートフォンのマイナンバーカード（電子証明書機能）
- 7) スマートフォンのマイナンバーカード（対面確認アプリ）
- 8) 写真付き本人確認書類の対面確認
- 9) 本人確認書類の撮影＋申請者の容貌の撮影
- 10) 本人確認書類の郵送＋住所への到達確認

5) スマートフォンのマイナンバーカード（属性証明機能）

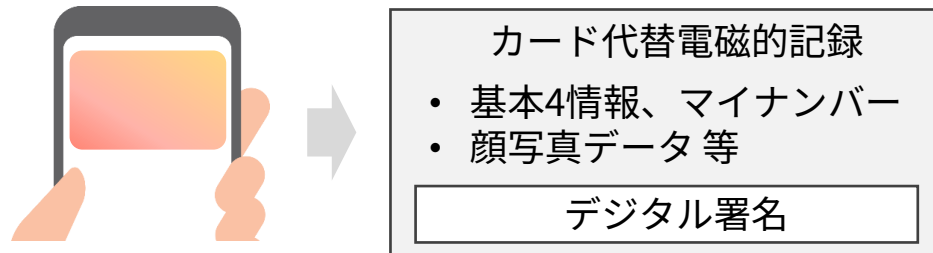
スマートフォンのマイナンバーカード（属性証明機能） — 概要

スマートフォンに搭載されたマイナンバーカード機能のうち「属性証明機能」は、実物のマイナンバーカードの券面に記載された基本4情報、マイナンバー、顔写真等を電子的に提出できる機能である。

実物のマイナンバーカードにおける「券面事項入力補助AP」を用いた身元確認に相当し、[身元確認保証レベル3に該当する手法](#)である。

属性情報の収集／本人確認書類の検証

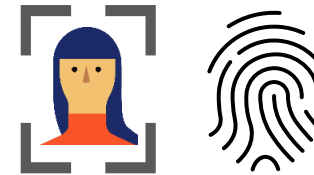
属性証明機能からのデータの読み取り



- スマートフォンのマイナンバーカードの属性証明機能から、基本4情報や顔写真等が含まれたデータ（カード代替電磁的記録）を電子的に読み取る
- カード代替電磁的記録のデジタル署名等を検証し、本人確認書類が偽造・改ざんされたものでないことを検証する

申請者の検証

スマートフォンで実行される当人認証 (顔認証、指紋認証等)



容貌確認 (必要に応じて実施)



- 属性証明機能を利用する際にスマートフォンの実行される当人認証*により、本人確認書類が確かに申請者自身のものであることを検証する
* 顔認証、指紋認証等
- 貸し借りへの対策が必要な場合、追加の容貌確認を実施する

5) スマートフォンのマイナンバーカード（属性証明機能）

脅威耐性と考慮事項

主な脅威	脅威への耐性
重複登録	<ul style="list-style-type: none"> 属性情報を電子データとして読み取ることで、誤記や表記揺れ等を防ぎ、属性情報を正確に収集できる。ただし、取り扱うシステムにおける文字コードや異体字・外字の整合等についての留意が必要。 個人番号取扱事務においては、マイナンバーによる正確な識別と紐づけが可能。
別人との誤紐づけ	
本人確認書類の偽造・改ざん	<ul style="list-style-type: none"> カード代替電磁的記録に付与されたデジタル署名を検証することで、それが偽造・改ざんされたものでないことを暗号学的な強度で検証できる。
本人確認書類の複製	<ul style="list-style-type: none"> カード代替電磁的記録はスマートフォンの安全な領域に格納され、電子的な複製攻撃への耐性を備える。 カード代替電磁的記録は、1枚の実物のマイナンバーカードに対して1台のスマートフォンにしか登録できないよう、重複登録を防止する措置が講じられている。
本人確認書類の盗用	<ul style="list-style-type: none"> スマートフォンで実行される本人認証によって、当該スマートフォンが盗用されたものではなく、確かに申請者自身のものであることを検証できる。
本人確認書類の貸し借り	<ul style="list-style-type: none"> 暗証番号とともにスマートフォンの貸し借りが行われた場合は検知できない。貸し借りの検知が必要な場合は、対面又は非対面による容貌確認を追加実施する必要がある。

観点	考慮事項
事業目的の遂行	<ul style="list-style-type: none"> マイナンバーカードやスマートフォンを保有していない方、暗証番号を覚えていない方、紛失中の方などの存在を考慮し、事業目的や公平性の観点から必要と判断される場合には、他の手法との併用や例外措置を検討する必要がある。
公平性	
プライバシー	<ul style="list-style-type: none"> カード代替電磁的記録には基本4情報、マイナンバー、顔写真等が含まれるが、取得する情報は身元確認に必要な最小限の範囲とすべきである。
アクセシビリティ及びユーザビリティ	<ul style="list-style-type: none"> 実物のマイナンバーカードと比べ、カードの読み取りや暗証番号入力が必要ない。 スマートフォンの操作に慣れていない方などへの配慮が必要。
セキュリティ	<ul style="list-style-type: none"> 意図的に他人のスマートフォンに対してカード代替電磁的記録を発行された場合を想定した考慮が必要である。 追加の容貌確認を実施する場合、カード代替電磁的記録に含まれる顔写真データの仕様（グレースケール等）に留意する必要がある。
その他	<ul style="list-style-type: none"> カード代替電磁的記録の取扱いは、マイナンバー法に基づく必要がある。

1. 身元確認手法の具体例

- 1) 実物のマイナンバーカード（券面事項入力補助AP）
- 2) 実物のマイナンバーカード（署名用電子証明書）
- 3) 実物のマイナンバーカード（利用者証明用電子証明書）
- 4) 実物のマイナンバーカード（対面確認アプリ）
- 5) スマートフォンのマイナンバーカード（属性証明機能）
- 6) スマートフォンのマイナンバーカード（電子証明書機能）
- 7) スマートフォンのマイナンバーカード（対面確認アプリ）
- 8) 写真付き本人確認書類の対面確認
- 9) 本人確認書類の撮影＋申請者の容貌の撮影
- 10) 本人確認書類の郵送＋住所への到達確認

6) スマートフォンのマイナンバーカード（電子証明書機能）

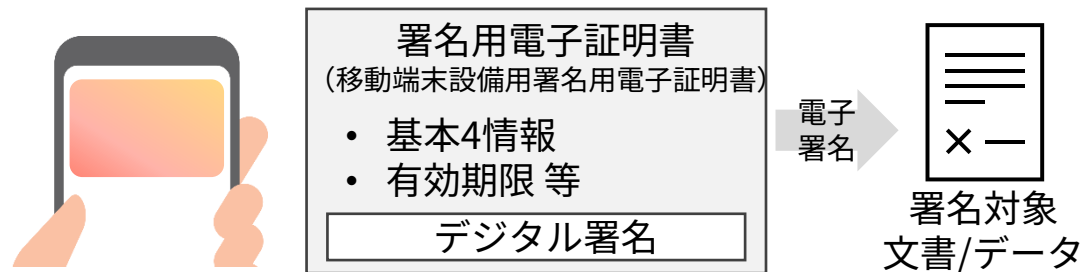
スマートフォンのマイナンバーカード（電子証明書機能） — 概要

スマートフォンに搭載されたマイナンバーカード機能のうち「電子証明書機能」は、公的個人認証の電子証明書をスマートフォンに格納して利用できる機能であり、これを用いて身元確認を行うことができる。

実物のマイナンバーカードにおける「署名用電子証明書」を利用した身元確認に相当し、[身元確認保証レベル3に該当する手法](#)である。



スマートフォンの電子証明書機能による電子署名



- スマートフォンに搭載された署名用電子証明書から、基本4情報等を電子的に取り出す
- 署名用電子証明書のデジタル署名を検証することで、本人確認書類が偽造・改ざんされたものでないことを検証する

署名用パスワード
(英数字6～16桁)

+



- 署名用電子証明書を利用する際の署名用パスワードにより、利用されているスマートフォンが確かに申請者自身のものであることを検証する
- 貸し借りへの対策が必要な場合、追加の容貌確認を実施する

6) スマートフォンのマイナンバーカード（電子証明書機能）

脅威耐性と考慮事項

主な脅威	脅威への耐性
重複登録	<ul style="list-style-type: none"> 属性情報を電子データとして読み取ることで、誤記や表記揺れ等を防ぎ、属性情報を正確に収集できる。ただし、取り扱うシステムにおける文字コードや異体字・外字の整合等についての留意が必要。 署名用電子証明書は転出等により失効するため、身元確認の直前に行われた転居等を検知できる。
別人との誤紐づけ	
本人確認書類の偽造・改ざん	<ul style="list-style-type: none"> 署名用電子証明書に付与された発行元のデジタル署名を検証することで、それが偽造・改ざんされたものではないことを暗号的な強度で検証できる。
本人確認書類の複製	<ul style="list-style-type: none"> 署名用電子証明書はスマートフォンの安全な領域に格納され、電子的な複製攻撃への耐性を備える。 署名用電子証明書は、1枚の実物のマイナンバーカードに対して1台のスマートフォンにしか登録できないよう、重複登録を防止する措置が講じられている。
本人確認書類の盗用	<ul style="list-style-type: none"> スマートフォンで実行される本人認証によって、当該スマートフォンが盗用されたものではなく、確かに申請者自身のものであることを検証できる。
本人確認書類の貸し借り	<ul style="list-style-type: none"> 署名用パスワードとともにスマートフォンの貸し借りが行われた場合は検知できない。貸し借りの検知が必要な場合は、対面又は非対面による容貌確認を追加実施する必要がある。

観点	考慮事項
事業目的の遂行	<ul style="list-style-type: none"> マイナンバーカードやスマートフォンを保有していない方、署名用パスワードを覚えていない方、紛失中の方に加えて、転居直後やその他の理由で電子証明書を失効中の方などの存在を考慮し、事業目的や公平性の観点から必要と判断される場合には、他の手法との併用や例外措置を検討する必要がある。
公平性	
プライバシー	<ul style="list-style-type: none"> 特筆すべき考慮事項はない。
アクセシビリティ及びユーザビリティ	<ul style="list-style-type: none"> 実物のマイナンバーカードと比べ、カードの読み取りが必要ない。ただし、署名用パスワードは生体認証等では代替できない。 スマートフォンの操作に慣れていない方などへの配慮が必要。
セキュリティ	<ul style="list-style-type: none"> 署名用パスワードとともにスマートフォンの貸し借りが行われた場合や、意図的に他人のスマートフォンに対して電子証明書を発行された場合を想定した考慮が必要である。 追加の容貌確認を実施する場合、署名用電子証明書には顔写真データが含まれていないため、別の方法で顔写真を取得する必要がある。
その他	<ul style="list-style-type: none"> 手続が電子署名を必要としない場合は、券面事項入力補助APなど、他の機能の利用を検討すべきである。 この機能の取扱いは、公的個人認証法に基づく必要がある。

1. 身元確認手法の具体例

- 1) 実物のマイナンバーカード（券面事項入力補助AP）
- 2) 実物のマイナンバーカード（署名用電子証明書）
- 3) 実物のマイナンバーカード（利用者証明用電子証明書）
- 4) 実物のマイナンバーカード（対面確認アプリ）
- 5) スマートフォンのマイナンバーカード（属性証明機能）
- 6) スマートフォンのマイナンバーカード（電子証明書機能）
- 7) スマートフォンのマイナンバーカード（対面確認アプリ）
- 8) 写真付き本人確認書類の対面確認
- 9) 本人確認書類の撮影＋申請者の容貌の撮影
- 10) 本人確認書類の郵送＋住所への到達確認

7) スマートフォンのマイナンバーカード（対面確認アプリ）

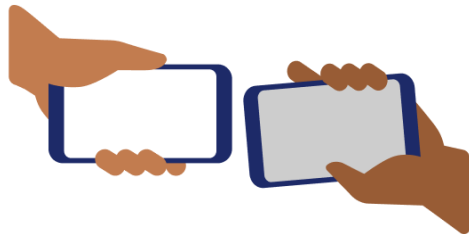
スマートフォンのマイナンバーカード（対面確認アプリ） — 概要

マイナンバーカード対面確認アプリは、実物のマイナンバーカードのほか、スマートフォンのマイナンバーカード（属性証明機能）を検証することもできる。

実物のマイナンバーカードを読み取る場合と同様、[身元確認保証レベル3](#)の身元確認を実現できる。

属性情報の収集／本人確認書類の検証

スマートフォンのマイナンバーカードの
属性証明機能の読み取り



- マイナンバーカードのスマートフォン（属性証明機能）を、別のスマートフォンの対面確認アプリで読み取り、カード代替電磁的記録から基本4情報、顔写真等を電子的に読み取る
- データに付与されたデジタル署名を検証することで、本人確認書類が偽造・改ざんされたものでないことを検証する

申請者の検証

スマートフォンで実行される当人認証
(顔認証、指紋認証、暗証番号等)



+

容貌確認
(必要に応じて実施)



- スマートフォン側で実行される当人認証によって、スマートフォンの盗用が行われていないことを検証する
- 貸し借りへの対策が必要な場合、スマートフォンのマイナンバーカードから読み取った顔写真を用いて追加の容貌確認を実施する

7) スマートフォンのマイナンバーカード（対面確認アプリ）

脅威耐性と考慮事項

主な脅威	脅威への耐性
重複登録	<ul style="list-style-type: none"> 属性情報を電子データとして読み取ることで、属性情報を正確に収集できる。ただし、個人情報の取り扱いの観点からデータの転送は行わない仕組みのため、他のシステムへのデータ入力を行う場合は入力ミス等への留意が必要となる。 個人番号取扱事務においては、マイナンバーによる正確な識別と紐づけが可能。
別人との誤紐づけ	
本人確認書類の偽造・改ざん	<ul style="list-style-type: none"> カード代替電磁的記録に付与された発行元によるデジタル署名を検証することで、それが偽造・改ざんされたものでないことを暗号的な強度で検証できる。
本人確認書類の複製	<ul style="list-style-type: none"> カード代替電磁的記録はスマートフォンの安全な領域に格納され、電子的な複製攻撃への耐性を備える。 カード代替電磁的記録は、1枚の実物のマイナンバーカードに対して1台のスマートフォンにしか登録できないよう、重複登録を防止する措置が講じられている。
本人確認書類の盗用	<ul style="list-style-type: none"> スマートフォンで実行される本人認証によって、当該スマートフォンが盗用されたものではなく、確かに申請者自身のものであることを検証できる。
本人確認書類の貸し借り	<ul style="list-style-type: none"> 暗証番号とともにスマートフォンの貸し借りが行われた場合は検知できない。貸し借りの検知が必要な場合は、対面による容貌確認を追加実施する必要がある。

観点	考慮事項
事業目的の遂行	<ul style="list-style-type: none"> マイナンバーカードやスマートフォンを保有していない方、暗証番号を覚えていない方、紛失中の方などの存在を考慮し、事業目的や公平性の観点から必要と判断される場合には、他の手法との併用や例外措置を検討する必要がある。
公平性	
プライバシー	<ul style="list-style-type: none"> スマートフォンのマイナンバーカードを利用する場合、対面確認アプリにおいて、取得する情報を限定することができる。身元確認に必要な最小限の情報のみを選択して取得すべきである。
アクセシビリティ及びユーザビリティ	<ul style="list-style-type: none"> 実物のマイナンバーカードを利用する場合と比べ、カードの撮影や読み取りが必要ない。 スマートフォンの操作に慣れていない方などへの配慮が必要である。
セキュリティ	<ul style="list-style-type: none"> 追加の容貌確認を行う場合、この手法において利用できる顔写真は、対面確認アプリで読み取った顔写真データ（グレースケース）のみとなる点に留意が必要である。
その他	<ul style="list-style-type: none"> 対面確認アプリで読み取った属性情報は、個人情報の取り扱いの観点からデータの転送は行わない仕組みのため、他のシステムへのデータ入力を行う場合は入力ミス等を防ぐための対策を講じること。

1. 身元確認手法の具体例

- 1) 実物のマイナンバーカード（券面事項入力補助AP）
- 2) 実物のマイナンバーカード（署名用電子証明書）
- 3) 実物のマイナンバーカード（利用者証明用電子証明書）
- 4) 実物のマイナンバーカード（対面確認アプリ）
- 5) スマートフォンのマイナンバーカード（属性証明機能）
- 6) スマートフォンのマイナンバーカード（電子証明書機能）
- 7) スマートフォンのマイナンバーカード（対面確認アプリ）
- 8) 写真付き本人確認書類の対面確認
- 9) 本人確認書類の撮影＋申請者の容貌の撮影
- 10) 本人確認書類の郵送＋住所への到達確認

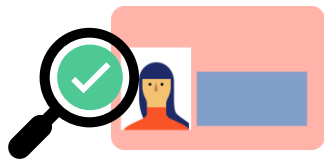
写真付き本人確認書類の対面確認 — 概要

窓口等の対面において本人確認書類の提示を求める手法のうち、顔写真付き本人確認書類を物理的検査したうえで記載事項を読み取る方法は、[身元確認保証レベル2に該当する](#)。

なお、この手法では、申請者の検証を行うために顔写真付き本人確認書類が必要となる。

属性情報の収集／本人確認書類の検証

本人確認書類の
物理的検査・読み取り



- 本人確認書類の券面等が偽造・改ざんされていないことを、視覚、触覚などにより物理的に検証する
- 本人確認書類の券面等に印字された情報から、身元確認に必要な属性情報（氏名、住所等）を視覚的に読み取る

申請者の検証

顔写真による
容貌確認



- 本人確認書類の券面等に印刷された顔写真と申請者の容貌とを比較することで、本人確認書類が確かに申請者自身のものであることを検証する

8) 写真付き本人確認書類の対面確認

脅威耐性と考慮事項

主な脅威	脅威への耐性
重複登録	<ul style="list-style-type: none"> 属性情報を物理的に読み取ることになるため、誤記、表記揺れ、データ入力ミスなどが発生する可能性の考慮が必要である。
別人との誤紐づけ	
本人確認書類の偽造・改ざん	<ul style="list-style-type: none"> 本人確認書類の検証強度は、検査を行う環境や道具、本人確認書類が備える偽造対策技術、検査担当者の経験・技能、訓練やマニュアルの有無など、様々な要因によって左右される。 精巧な偽造・改ざんについては人手での検知が難しい場合もある。
本人確認書類の複製	
本人確認書類の盗用	<ul style="list-style-type: none"> 顔写真を用いて対面での容貌確認を行うことで、本人確認書類が盗用や貸し借りされたものであることを検証できる。
本人確認書類の貸し借り	

観点	考慮事項
事業目的の遂行	<ul style="list-style-type: none"> 顔写真付き本人確認書類を保有していない方、紛失中の方などの存在を考慮し、事業目的や公平性の観点から必要と判断される場合には、他の手法との併用や例外措置を検討する必要がある。
公平性	
プライバシー	<ul style="list-style-type: none"> 本人確認書類を撮影又はスキャンした情報を身元確認の証跡として保管する場合、当該情報が必要なくなった時点で削除を行うなど、プライバシー面を考慮した運用設計が必要である。
アクセシビリティ及びユーザビリティ	<ul style="list-style-type: none"> 特筆すべき考慮事項なし
セキュリティ	<ul style="list-style-type: none"> 偽造・改ざんのリスクに応じて、本人確認書類の物理的検査を行うための環境、道具、利用可能とする本人確認書類の種類、検査担当者に対する訓練やマニュアル整備などを検討する必要がある。 容貌確認に用いる顔写真は、本人確認書類によって撮影条件、解像度、撮影されてからの期間等の条件が異なることに留意が必要である。
その他	<ul style="list-style-type: none"> 特になし

1. 身元確認手法の具体例

- 1) 実物のマイナンバーカード（券面事項入力補助AP）
- 2) 実物のマイナンバーカード（署名用電子証明書）
- 3) 実物のマイナンバーカード（利用者証明用電子証明書）
- 4) 実物のマイナンバーカード（対面確認アプリ）
- 5) スマートフォンのマイナンバーカード（属性証明機能）
- 6) スマートフォンのマイナンバーカード（電子証明書機能）
- 7) スマートフォンのマイナンバーカード（対面確認アプリ）
- 8) 写真付き本人確認書類の対面確認
- 9) **本人確認書類の撮影＋申請者の容貌の撮影**
- 10) 本人確認書類の郵送＋住所への到達確認

8) 本人確認書類の撮影+申請者の容貌の撮影

本人確認書類の撮影+申請者の容貌の撮影 — 概要

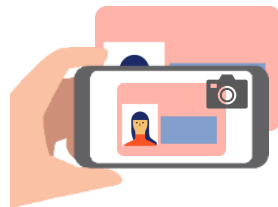
スマートフォンのカメラ等を用いて本人確認書類と申請者の容貌をそれぞれ撮影することで、非対面での身元確認を実現する手法である。[身元確認保証レベル1に該当する](#)。

撮影の条件、枚数、動画の併用、画像処理による自動検証の有無、人手による検証の有無、インジェクション攻撃やプレゼンテーション攻撃への対策の有無などによって、細かな脅威耐性が異なる。

属性情報の収集／本人確認書類の検証

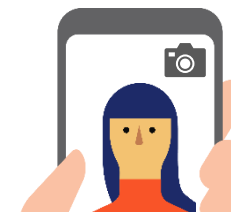
申請者の検証

本人確認書類の撮影



- 本人確認書類の券面等の撮影を求め、撮影された画像から身元確認に必要な属性情報（氏名、住所等）を視覚的に読み取る
- 本人確認書類の券面等が偽造・改ざんされていないことを、撮影された画像により物理的に検証する

申請者の容貌の撮影
(非対面での容貌確認)



- 申請者の容貌の撮影を求め、本人確認書類を撮影した画像の顔写真との比較により、本人確認書類が確かに申請者自身のものであることを検証する

8) 本人確認書類の撮影+申請者の容貌の撮影

脅威耐性と考慮事項

主な脅威	脅威への耐性
重複登録	<ul style="list-style-type: none"> 属性情報を物理的に読み取ることになるため、誤記、表記揺れ、データ入力ミスなどが発生する可能性の考慮が必要である。
別人との誤紐づけ	
本人確認書類の偽造・改ざん	<ul style="list-style-type: none"> 画像や映像を介した本人確認書類の検証では、検証強度に限界があり、精巧な偽造・改ざんを検知することは難しい。
本人確認書類の複製	
本人確認書類の盗用	<ul style="list-style-type: none"> 顔写真を用いて対面での容貌確認を行うことで、本人確認書類が盗用や貸し借りされたものであることを検証できる。 ただし、画像や映像の差し替えや改ざん等の攻撃（インジェクション攻撃、プレゼンテーション攻撃に対する対策は、個別検討が必要となる。
本人確認書類の貸し借り	

観点	考慮事項
事業目的の遂行	<ul style="list-style-type: none"> 顔写真付き本人確認書類を保有していない方、紛失中の方などの存在を考慮し、事業目的や公平性の観点から必要と判断される場合には、他の手法との併用や例外措置を検討する必要がある。
公平性	
プライバシー	<ul style="list-style-type: none"> 画像や映像を身元確認の証跡として保管する場合、当該情報が必要なくなった時点で削除を行うなど、プライバシー面を考慮した運用設計が必要である。
アクセシビリティ及びユーザビリティ	<ul style="list-style-type: none"> 特筆すべき考慮事項はない。
セキュリティ	<ul style="list-style-type: none"> 画像や映像を介した本人確認書類の検証強度には限界があるため、偽造・改ざんによるリスクを考慮のうえで、補完的対策の必要性を検討することが望まれる。 画像や映像の差し替えや改ざん等の攻撃（インジェクション攻撃、プレゼンテーション攻撃）を想定し、利用可能なデバイスやアプリケーションを制限する、ライブネスチェック等の対策を導入するなどの検討が必要である。
その他	<ul style="list-style-type: none"> 特になし

1. 身元確認手法の具体例

- 1) 実物のマイナンバーカード（券面事項入力補助AP）
- 2) 実物のマイナンバーカード（署名用電子証明書）
- 3) 実物のマイナンバーカード（利用者証明用電子証明書）
- 4) 実物のマイナンバーカード（対面確認アプリ）
- 5) スマートフォンのマイナンバーカード（属性証明機能）
- 6) スマートフォンのマイナンバーカード（電子証明書機能）
- 7) スマートフォンのマイナンバーカード（対面確認アプリ）
- 8) 写真付き本人確認書類の対面確認
- 9) 本人確認書類の撮影＋申請者の容貌の撮影
- 10) 本人確認書類の郵送＋住所への到達確認

本人確認書類の郵送 ＋ 住所への到達確認 — 概要

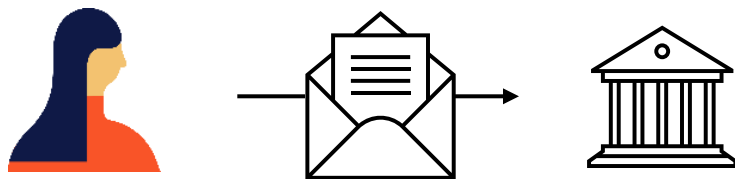
住民票の写し等の本人確認書類を郵送することによる身元確認手法は、「住所への到達確認」による申請者の検証を行うことで[身元確認保証レベル1に該当する](#)。

なお、本人確認書類の郵送提出のみを求め、その後の「申請者の検証」のプロセスを行わない場合は、本人確認書類の盗用等の検知ができず、身元確認保証レベルは1に満たない手法となることに留意すること。

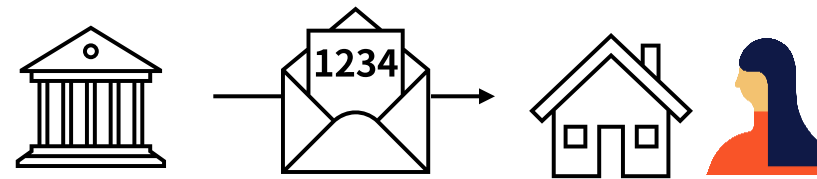
属性情報の収集／本人確認書類の検証

申請者の検証

本人確認書類（原本又は写し）の郵送



住所への到達確認
(確認コード等による検証)



- 本人確認書類の郵送による提出を求め、提出された住民票の写しの記載事項から身元確認に必要な情報を収集する。
- 物理的検査、信頼できる情報源への照会等により、提出された本人確認書類が偽造・改ざんされたものでないことを検証する。

- 本人確認書類に記載された住所に対して確認コード（6桁の番号等）を送付し申請者に確認コードの入力を求めるなどして、本人確認書類が確かに申請者自身のものであることを検証する

10) 本人確認書類の郵送+住所への到達確認

脅威耐性と考慮事項

主な脅威	脅威への耐性
重複登録	<ul style="list-style-type: none"> 属性情報を物理的に読み取ることになるため、誤記、表記揺れ、データ入力ミスなどが発生する可能性の考慮が必要である。
別人との誤紐づけ	
本人確認書類の偽造・改ざん	<ul style="list-style-type: none"> 住民票の写しや戸籍謄本/抄本など、行政機関が発行した証明書そのものを提出させる場合は、物理的検査により一定程度の検証が可能である。 マイナンバーカードや運転免許証などの券面のコピーを郵送させる場合は、コピーを介した検証強度には限界があり、偽造・改ざんを厳密に検査することは難しい。
本人確認書類の複製	
本人確認書類の盗用	<ul style="list-style-type: none"> 住所への到達確認を行うことにより、本人確認書類の盗用を検知できる。ただし、券面のコピーを提出させる場合は本人確認書類の偽造・改ざんの厳密な検査が難しいため、住所が偽造され得る可能性には留意が必要である。
本人確認書類の貸し借り	<ul style="list-style-type: none"> 本人確認書類とともに確認コードも共有された場合には、貸し借りは検知できない。

観点	考慮事項
事業目的の遂行	<ul style="list-style-type: none"> 利用可能な本人確認書類を広く確保することが可能な手法であるため、事業目的の遂行や公平性の確保の観点から、他の手法を補完する位置づけでの採用が考えられる。
公平性	
プライバシー	<ul style="list-style-type: none"> 住民票の写しや戸籍謄本/抄本の提出を求める場合、身元確認には必要のない情報が多く含まれることに留意し、収集・記録する属性の限定、提出を受けた書類の保管等の扱いについて考慮すべきである。
アクセシビリティ及びユーザビリティ	<ul style="list-style-type: none"> デジタルに不慣れな方でも利用しやすい方法と言える。
セキュリティ	<ul style="list-style-type: none"> 本人確認書類の種類によって検証強度が異なる。一部の本人確認書類については、偽造・改ざんの検知が現実的に困難となることに留意が必要である。 確認コードは配送中に不正取得されるリスクがあることに留意が必要である。
その他	<ul style="list-style-type: none"> 特になし

2. 身元確認手法に関するその他の解説（コラム）

コラム1) 身元確認の実施担当者に対する訓練等について

コラム2) 電子メールでの手続における身元確認について



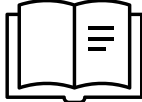
コラム3) 郵便を使った身元確認について

コラム4) スマートフォンに搭載された本人確認書類の扱いについて

コラム案：身元確認の実施担当者に対する訓練等について

「本人確認書類の物理的検証」や「容貌確認」を行う場合、その身元確認の強度は、身元確認を行う環境、利用できる道具、実施手順、実施担当者の訓練の有無などによって大きく左右される。

そのような手法を採用する場合は、**その実施条件について事前に検討を行い、マニュアルの整備、担当者の訓練などの対策を講じる**ことが必要である。

考慮事項	検証強度に影響する主な事項
<p>身元確認の実施環境</p> 	<ul style="list-style-type: none"> 身元確認を行う場所は屋内か、屋外か 十分な明るさを確保できるか、照明は利用できるか 検証にはどのような道具を利用できるか (例：ルーペ、真贋判定機、偽造対策インキを確認するためのブラックライト等) 1人あたりの身元確認に費やせる時間はどれくらいか
<p>身元確認の実施条件</p> 	<ul style="list-style-type: none"> 利用可能な本人確認書類は何とするか (本人確認書類によって、検証に利用できる券面の偽造対策技術等が異なることを考慮した検討が必要) 身元確認書類を一時的に預かることが可能かどうか 申請者にマスクの着脱の指示を行うかどうか 申請者の容貌の撮影を行うかどうか
<p>マニュアル・訓練等</p> 	<ul style="list-style-type: none"> マニュアルの整備や周知は行われているか 担当者に対する訓練は行われているか

2. 身元確認手法に関するその他の解説（コラム）

コラム1) 身元確認の実施担当者に対する訓練等について

コラム2) 電子メールでの手続における身元確認について

コラム3) 郵便を使った身元確認について

コラム4) スマートフォンに搭載された本人確認書類の扱いについて

コラム案：電子メールでの手続における身元確認について

電子メールで受け付ける手続において身元確認を実施する場合でも身元確認のプロセスや考え方は同様であるが、**申請用のWebサイトを構築する場合と比べて採用できる手法は限定され、検証強度が低くなる場合もある。**

対象手続において不正申請やなりすましが行われた場合の影響を踏まえ、リスクを受容可能であるか判断する必要がある。必要な場合は、補完的対策を講じることが望まれる。

No.	電子メールでの手続で採用可能な主な手法		考慮事項	身元確認 保証レベル
	本人確認書類の検証	申請者の検証		
1	顔写真付き本人確認書類を撮影又はスキャンした画像のメール添付を求める	申請者の容貌を撮影した写真のメール添付を求める	<ul style="list-style-type: none"> カメラ越しに精巧な偽造を検知することは難しい 画像を偽造・改ざんされるリスクがある 	レベル1
2		オンライン会議などにより申請者の容貌を確認する	<ul style="list-style-type: none"> カメラ越しに精巧な偽造を検知することは難しい オンライン会議の映像がリアルタイムに偽造・改ざんされるリスクがある 	レベル1
3	住民票の写しを撮影又はスキャンした画像のメール添付を求める	記載された住所に確認コードを郵送するなどして、到達性を検証する	<ul style="list-style-type: none"> カメラ越しに本人確認書類の精巧な偽造を検知することは難しい 画像ファイルを直接編集されることでの偽造・改ざんが行われるリスクがある 	レベル1
4	マイナンバーカードによって電子署名を行った申請書のメール添付を求める	電子署名時の署名用パスワードの入力をもって本人確認書類と申請者の紐づきを検証する	<ul style="list-style-type: none"> 提出された申請書の電子署名を検証できる環境が必要となる（公的個人認証法に基づく検証を行う必要がある） 	レベル3

コラム案：電子メールでの手続における身元確認について（参考情報）

電子メールでの利用においては、「行政手続のオンライン化に当たっての本人確認の考え方」（令和2年11月16日 内閣府規制改革推進室、内閣官房 IT 総合戦略室、内閣官房行政改革推進本部事務局）における[行政手続における電子メールの利用に関する本人確認の補完の考え方](#)についても参考とされたい。

4. 行政手続における電子メールの利用

行政手続において電子メールを利用する場合、当該手続の性質等に照らし、必要に応じて、例えば、他の手続における既存の本人確認、面談・電話等による従前からの継続的なやり取り又は事後のやり取り、現地調査等により本人確認が補完されると考えられる³。

なお、インターネットを経由した電子メールは、申請等受付機能を有する Web システムではエラーという反応が起こるのに比べ、電子メールプロトコルの特徴から、何の反応もなく送受信が完了しない可能性があり、また、セキュリティ製品が電子メールの添付ファイル等を検査し、マルウェアやスパムメールと判断した場合には、電子メールは隔離又は受信拒否される可能性がある。このため、行政手続において電子メールを利用する場合には、当該手続の性質等も勘案しつつ、必要に応じ、電話等により相手方に所要の確認を行うべきである。

2. 身元確認手法に関するその他の解説（コラム）

コラム1) 身元確認の実施担当者に対する訓練等について

コラム2) 電子メールでの手続における身元確認について

コラム3) 郵便を使った身元確認について

コラム4) スマートフォンに搭載された本人確認書類の扱いについて

コラム：郵便を使った身元確認について

「本人限定受取郵便（特定事項伝達型）」は、配達担当者が受取人に対する身元確認を行い、その結果を差出人が確認できる仕組みである。これを用いる場合の身元確認レベルの解釈は以下のとおりである。

なお、本人確認書類から収集した情報が差出人に伝達されない種別のサービスは「属性情報の収集」を行うことができないため、身元確認に用いることはできない。

身元確認プロセス	該当する手法	考慮事項
属性情報の収集	「申請者自身による記入・入力」に相当 ※実際には配達担当者による記入・入力が行われるが、申請者自身による記入・入力と同等程度の強度とみなせる。	<ul style="list-style-type: none"> 「申請者自身による記入・入力」と同様、誤記、誤入力、異体字の扱いなどについての考慮が必要
本人確認書類の検証	「物理的検査（対面）」に該当	<ul style="list-style-type: none"> 検証は玄関先などで行われ、検証に用いることのできる時間や道具には制約がある。 担当者の訓練等の条件は指定できないため、差出人は検証強度を統制できない。
申請者の検証	「容貌確認（対面）」に該当	

2. 身元確認手法に関するその他の解説（コラム）

コラム1) 身元確認の実施担当者に対する訓練等について

コラム2) 電子メールでの手続における身元確認について

コラム3) 郵便を使った身元確認について

コラム4) スマートフォンに搭載された本人確認書類の扱いについて

コラム：スマートフォンに搭載された本人確認書類の扱いについて

昨今、属性情報や資格情報などをスマートフォンに格納して利用するための技術の利活用が始まりつつある。今後は「スマートフォンのマイナンバーカード」のように、様々な本人確認書類がスマートフォンに搭載され、身元確認においても利用可能になると想定される。

スマートフォンに搭載された本人確認書類を受け入れる場合も基本的な考え方は大きく変わらないが、以下のような特有の事項への考慮が必要である。

No.	身元確認プロセス	項目	考慮事項
1	本人確認書類の検証	スマートフォンに搭載できる本人確認書類は1枚に制限されているか	<ul style="list-style-type: none"> 本人確認書類を複数のスマートフォンに搭載できる仕様の場合、不正な発行や貸し借り等のリスクが生じる点に留意する必要がある。
2		電子的な複製への対策が講じられているか	<ul style="list-style-type: none"> 対策が講じられていない場合、悪意を持ったものによる不正な複製が行われるリスクの考慮が必要となる。
3		本来の発行元とは異なる機関から発行されたものでないか	<ul style="list-style-type: none"> スマートフォンに搭載された本人確認書類が、本来の本人確認書類の発行元とは異なる組織・機関から発行されたものである場合、失効管理などが適切になされないおそれがあるため、そのような本人確認書類を身元確認において受け入れ可能とすべきか検討が必要である。
4	申請者の検証	本人確認書類の提示時に、適切な認証が実行されるか	<ul style="list-style-type: none"> 本人確認書類を提示する際に、スマートフォン側で生体認証や暗証番号入力などによる適切な認証が行われない場合は、スマートフォンの盗用等のリスクに対して別の手段による「申請者の検証」を実施する必要がある。

デジタル庁

Digital Agency