民間事業者向け
デジタル本人確認ガイドライン

第1.3版　本人確認手法編

2026年8月

一般社団法人OpenID ファウンデーション・ジャパン
KYCワーキンググループ
本人確認ガイドラインサブワーキンググループ

改定履歴

改定年月日	版	改定内容
2023年3月20日	1.0	・公開
2023年4月14日	1.1	・改定履歴の追加 ・誤字等修正
2026年2月20日	1.2	・本人確認手法編の公開 　・身元確認手法、当人認証手法の再整理
2026年8月26日	1.3	・身元確認手法、当人認証手法の修正・追記 　・主な本人確認書類の解説 　・フィッシング耐性のある多要素認証に関する課題認識

はじめに

「民間事業者向けデジタル本人確認ガイドライン」を2023年に発行してから3年が経過し、世の中の状況は当時から大きく変化しています。マイナンバーカードの保有率は人口の80%を超えた※1だけでなく、健康保険証としての利用も開始され、運転免許証に代わって、国内では身元確認手段の主流になりつつあります。また、スマートフォンのマイナンバーカードでは、2023年5月にAndroidスマホ用電子証明書搭載サービスを開始し、2025年6月にiPhoneのマイナンバーカードを開始しています。Androidのマイナンバーカードも2026年秋頃に開始が予定※2されています。

一方で、対面、非対面を問わず、身元確認、当人認証プロセスを悪用した犯罪は後を絶たず、数千億円規模での金融犯罪を背景に、口座開設時等の非対面での身元確認においては、本人確認書類を写真撮影する方式は廃止され、取引時の当人認証手段においてはパスワードからの脱却が求められるなど、既存の本人確認方式をベースとしたサービスが大きな変革を求められる時期となっています。

当ガイドラインは、OpenID ファウンデーション・ジャパン KYC WGが2023年に発行した、「民間事業者向けデジタル本人確認ガイドライン」より、自然人の本人確認手法に関する章を抽出し、最新の状況に合わせて更新したものです。

次ページに記載の通り、デジタル庁の公開するガイドライン類と併せて利用することで、民間事業者におけるデジタルでの本人確認が一層普及し、オンライン、オフラインを問わず各種取引の安全性が向上することを期待します。

※1 出典：「マイナンバーカード交付状況について」（総務省）
※2 出典：「2026年秋頃に「Androidのマイナンバーカード」へ刷新します」（デジタル庁）

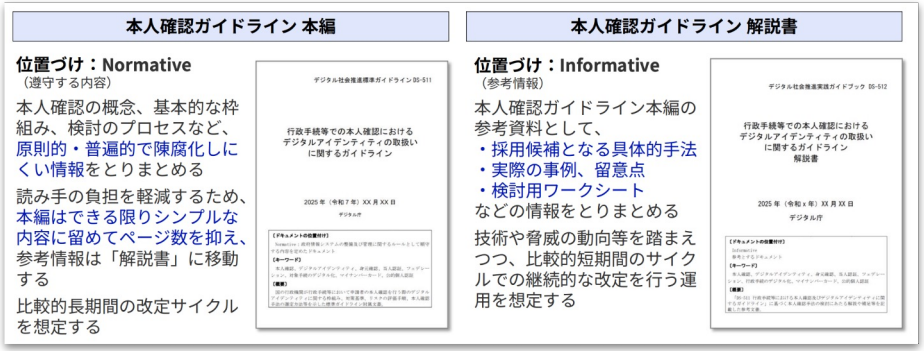
本ガイドラインの利用にあたって

当ガイドラインは、2026年8月時点において日本国内で広く普及している、もしくは今後普及が期待される自然人の本人確認手法について取りまとめたものです。

本人確認手法の概要については、デジタル庁の「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」、「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に関するガイドライン 解説書」等を参照ください。

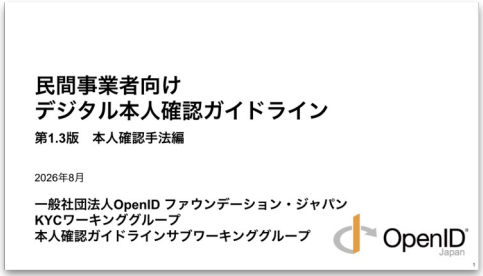
一方で、上記ガイドラインは、国の行政機関が提供する行政手続等における本人確認を対象としたものとなっていることから、民間事業者におけるデジタル本人確認手法の活用促進のため、上記ガイドラインを補完する資料として当ガイドラインが利用されることを期待します。

デジタル庁 本人確認ガイドライン



出典：「参考資料_改定に向けたとりまとめ（令和6年度（2024年度））」（デジタル庁）

OIDF-J ガイドライン（本書）



民間での活用を前提とした、主な身元確認・当人認証手法の詳細な解説

本ガイドライン参照時の留意事項

本ガイドラインは、OpenIDファウンデーション・ジャパン KYCワーキンググループ 本人確認ガイドラインサブワーキンググループが信頼できると判断した情報をもとに細心の注意を払って作成・表示したものですが、OpenIDファウンデーション・ジャパンは、本ガイドラインの内容および当該情報の正確性、完全性、的確性、信頼性等についていかなる保証をするものではありません。本ガイドラインの内容につきましては、利用者の判断に基づきご利用をお願いします。本ガイドラインの利用によって何らかの損害（直接損害・間接損害とを問いません）が発生した場合でも、OpenIDファウンデーション・ジャパン並びに執筆者は一切の責任を負いません。

本ガイドラインに記載された内容は、本ガイドライン作成時点におけるものであり、予告なく変更される場合があります。

OpenIDファウンデーション・ジャパンは、本ガイドラインが電子的に配布された場合に、利用者がコンピュータウイルスなど有害なプログラム等による損害を受けないことについて保証をするものではありません。また、OpenIDファウンデーション・ジャパンは、本ガイドラインが電子的に配布されることで生じる本資料の内容の誤り、欠落等に対する一切の責任を負いません。

本編目次

本編のスライドにおいて、記載内容が「身元確認」と「当人認証」*のどちらに該当するかの参考となるよう、スライドの右上に以下のように表示しています。

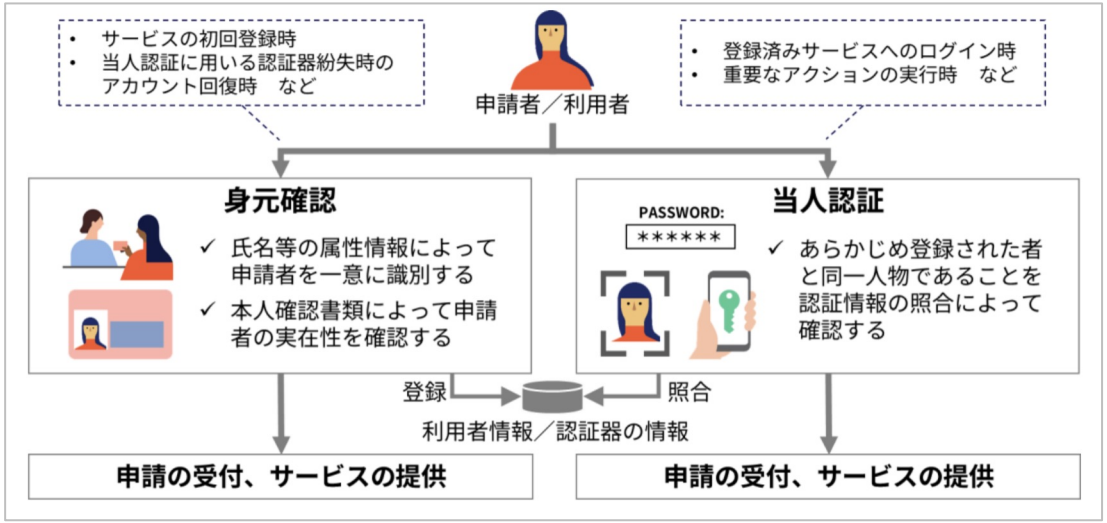
身元確認 当人認証

本人確認とは

本人確認とは

本人確認は、「身元確認」と「当人認証」の2つの要素に分かれます。

「身元確認」は、本人確認書類を確認する等により、「実在性*1」を確認することであり、一般的にはユーザー登録等が該当します。また、「当人認証」は、あらかじめ登録されているパスワードやパスキー等の認証情報と手続を行う際に入力された認証情報を照合する等により、事前に登録された者と同一人物であることを確認することであり、一般的にはログインが該当します。



出典：「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(DS-511)」（デジタル庁）

図 2-1 身元確認と当人認証の概念図

※1：ここでの実在性は、1） 集められた属性によって当該母集団の中でそれぞれの要素を区別することができ、2） 申請者が実在し、3）申請された属性の値が正しく、4） その属性が申請者に関するものであること、によって確認される。（身元確認のプロセスは1.1版26頁「（参考）身元確認のプロセス」を参照。）

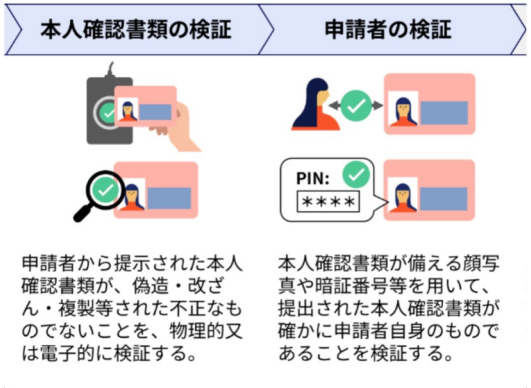
身元確認手法

身元確認の概要

身元確認は、「本人確認書類の検証」と、「申請者の検証」の2つの要素に分かれます。

身元確認には、「本人確認書類の検証」と、「申請者の検証」の２つのプロセスが必要です。
２つのプロセスそれぞれにおいて、検証すべき内容、不正を受けるリスクも異なるため、それぞれの脅威と提供するサービスが必要とする確認強度を元に、手法を選択する必要があります。

身元確認プロセスの概要



出典：「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(DS-511)」（デジタル庁）
図 3-1 身元確認プロセスの全体像より抜粋

身元確認プロセスの要素

身元確認 ＝

本人確認書類の検証
ICチップの読み取り
書類画像の撮影（厚みなど）
書類コピーの送付（電子・物理）
スマホ内に格納されたデータの取得
目視確認
自己申告（書類なし）

×

申請者の検証
ICチップ読み取り時のパスワード・暗証番号
書類の顔画像と申請者の顔写真の比較
スマホ内のデータ取得時のパスワード、暗証番号や生体認証
銀行口座情報にアクセスできることの確認
銀行口座（オンラインバンキング）にログインできることの確認
配達員の目視
郵送
チェックなし

出典：KYC WGによる作成

参考：身元確認手法の例：犯収法施行規則に規定されている身元確認手法（非対面）

主に金融機関等に遵守が求められる、犯罪による収益の移転防止に関する法律（以降「犯収法」）の施行規則に規定されている、主に非対面を想定した身元確認手法も、下記のように、本人確認の検証方法と、申請者の検証手法に要素分解できます。

本人確認書類の検証手法	申請者の検証手法	法令上の身元確認手法（名称はKYCWGによる）
ICチップの読み取り	書類の顔画像と申請者の顔写真の比較	容貌確認方式（ICチップ型）
書類画像の撮影（厚みなど）	書類の顔画像と申請者の顔写真の比較	容貌確認方式（書類画像型）
ICチップの読み取り	銀行口座（オンラインバンキング）にログインできることの確認	銀行顧客照会方式（ICチップ型）
書類画像の撮影（厚みなど）	銀行口座（オンラインバンキング）にログインできることの確認	銀行顧客照会方式（書類画像型）
ICチップの読み取り	銀行口座情報にアクセスできることの確認	銀行口座振込方式（ICチップ型）
書類画像の撮影（厚みなど）	銀行口座情報にアクセスできることの確認	銀行口座振込方式（書類画像型）
ICチップの読み取り or スマホ内に格納されたデータの取得	ICチップ読み取り時のパスワード or スマホ内のデータ取得時のパスワード	JPKI署名用電子証明書方式
ICチップの読み取り or スマホ内に格納されたデータの取得	ICチップ読み取り時のパスワード or スマホ内のデータ取得時のパスワード	民間電子証明書方式※
スマホ内に格納されたデータの取得	スマホ内のデータ取得時の暗証番号や生体認証	カード代替電磁的記録方式
ICチップの読み取り	郵送	転送不要郵便方式（ICチップ型）
書類そのものの提示・提出	郵送	転送不要郵便方式（原本送付型）
書類コピーや画像の送付	郵送	転送不要郵便方式（写し送付型）
ICチップの読み取り※1	配達員の目視	特定事項伝達型本人限定郵便方式

出典：「犯罪による収益の移転防止に関する法律施行規則」（e-Gov法令検索）を元にKYC WGが作成
※1：2027年4月施行より特定事項伝達型本人限定郵便方式でもICチップの読み取りが必須となる。

参考：本章で紹介する身元確認手法と犯収法・携帯電話不正利用防止法※1との関係

犯収法や、携帯電話不正利用防止法の施行規則に規定されている身元確認手法も、下記のように、新たな身元確認手法の普及や、脅威の変化に対応する形で変化しています。

	犯収法施行規則 第6条1項1号			携帯電話不正利用防止法施行規則 第3条1項1号		
施行規則上の身元確認手法	25年6月改正前	25年6月改正後	27年4月予定	25年6月改正前	25年6月改正後	26年4月改正後
容貌確認方式（ICチップ型）	ヘ	ヘ	**ハ（変更）**	ニ	ニ	**ハ（変更）**
容貌確認方式（書類画像型）	ホ	ホ	**廃止**	ハ	ハ	**廃止**
銀行顧客照会方式（ICチップ型）	ト（１）	ト（１）	**ニ(1)（変更）**	-	-	-
銀行顧客照会方式（書類画像型）	ト（１）	ト（１）	**廃止**	-	-	-
銀行口座振込方式（ICチップ型）	ト（２）	ト（２）	**ニ(2)（変更）**	-	-	-
銀行口座振込方式（書類画像型）	ト（２）	ト（２）	**廃止**	-	-	-
JPKI署名用電子証明書方式	ワ	**カ（変更）**	**ヌ（変更）**	チ	チ	**ト（変更）**
民間電子証明書方式※2	ヲ	**ワ（変更）**	**リ（変更）**	チ	チ	**ト（変更）**
カード代替電磁的記録方式※3	-	**ル（新規）**	**ト（変更）**	-	**リ（新規）**	**チ（変更）**
転送不要郵便方式（ICチップ型）	チ	チ	**ホ（変更）**	-	-	**ニ（新規）**
転送不要郵便方式（原本送付型）	チ	チ	**ホ（変更）**	ホ	ホ	ホ
転送不要郵便方式（写し送付型）	リ	リ	**廃止※4**	ヘ	ヘ	**廃止※4**
特定事項伝達型本人限定郵便方式	ル	**ヲ（変更）**	**チ※5（変更）**	ト	ト	**ヘ（変更）**

出典：「犯罪による収益の移転防止に関する法律施行規則」（e-Gov法令検索）並びに「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律施行規則」（e-Gov法令検索）を元にKYC WGが作成（2026年7月時点、特に将来の予定の記載は、今後の改正で変更になる可能性がある点に留意）

※1　「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律」（以降「携帯電話不正利用防止法」と略す）

※2　犯収法には民間電子証明書方式が２種類あるが、もう１種類は本書発行時点で対応している事業者が存在しないので省略した

※3　カード代替電磁的記録についての詳細は、「カード代替電磁的記録（属性証明機能）」（デジタル庁）を参照のこと

※4　犯収法 27年4月改正、携帯電話不正利用防止法 26年4月改正の転送不要郵便方式（写し送付型）は非居住者等にしか適用できないため廃止と表現した

※5　犯収法 27年4月改正の特定事項伝達型本人限定郵便方式ではICチップの読み取りが必須となる。

本人確認書類の検証手法の解説

- ICチップの読み取り
- 書類画像の撮影（厚みなど）
- 書類コピーの送付（電子・物理）
- スマホ内に格納されたデータの取得
- 目視確認
- 自己申告（書類なし）

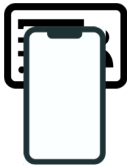
ICチップの読み取り

スマートフォンやICカードリーダにICチップ付き本人確認書類をかざし、ICチップに格納された情報を読み取ります。通常電子署名されており、本人確認書類の偽造対策としては最も強固な手法ですが、暗証番号やカードに記載された番号をユーザが入力する必要があります。

ICチップの読み取りの概要

ユーザの操作

暗証番号の手入力、もしくはカードに記載された番号の入力（券面撮影によるOCR or 手入力)



ICチップ付き本人確認書類をスマホやカードリーダにかざす

ユーザ体験

- カードを所持している必要がある
- カードを読むためのデバイスが必要（非対面の場合）
- 暗証番号8桁を覚えている必要がある（運転免許証の場合）
- 運転経歴証明書は使えない

事業者の手順

ICカードリーダ（対面の場合）やICカードを読むスマホアプリ等の用意
データの署名検証（証明書を各公共機関から入手する必要がある）
※本人確認書類の種類によってはテキストではなく画像情報でデータが格納されており、目視による確認が必要

開発・ランニングコスト

- ICカード読み取りのためのリーダデバイスの入手（対面の場合） or アプリ開発・SDKの入手
- 署名検証のための証明書の入手orSDKの入手
- JPKIを利用する場合には認定事業者との接続、利用料の支払い

書類の種類

1.マイナンバーカード
署名用電子証明書用暗証番号（6-16桁)
照合番号B（14桁）
2.運転免許証
暗証番号（４桁x２つ）
※外字情報が画像で提供されるため、OCRや目視での確認が必要
3.在留カード、特別永住者証明書
カード番号（12桁）
※多くの情報は画像として提供されるため、OCRや目視での確認が必要
4.パスポート
パスポート番号等（ICAO仕様に準拠）
※住所なし、ローマ字氏名

脅威への対応

事実上最も強固。書類の正しさを電子署名を用いて検証できるほか、書類によっては現在有効かを確認することが可能（失効確認）

書類画像の撮影（厚みなど）

スマートフォンなどで本人確認書類を撮影する方法です。書類の撮影の他に書類の厚みなどを撮影することで、一定の偽造対策が可能です。偽造書類等を防げないケースが存在し、犯収法では27年4月、携帯電話不正利用防止法では26年4月より非対面での身元確認方法として利用できません。

書類画像の撮影の概要

ユーザの操作

1）書類の表面の撮影
2）書類の厚みの撮影
3）書類の裏面の撮影
（※書類による）

事業者の手順

- 書類真正性確認: 「厚み」画像等を用いて、書類がコピーや画面の撮影ではなく、原本であるかを確認
- 再提出依頼: 画像不鮮明による差し戻し対応

書類の種類

1. マイナンバーカード
2. 運転免許証
3. 在留カード
4. 特別永住者証明書
5. 運転経歴証明書
6. パスポート

ユーザ体験

- 書類の表面・裏面の撮影で、書類不鮮明になるケースがある
- 厚み撮影の難易度が高く離脱要因となり得る

開発・ランニングコスト

- eKYCセルフィーを独自実装することは難しい。初期導入費がかかる
- 従量課金：eKYCベンダーのソリューション利用料が発生
- BPO費用：AI/OCRによる自動化は進んでいるが、最終的に人の目による確認が必要な場合、BPOコストや人的コストが必要

脅威への対応

精巧な偽造カード（プラスチック板への印刷）の場合、画像上の「厚み」確認だけでは見抜けないケースが存在

本人確認書類に記載されている機微情報のマスキング処理等が必要になる

書類コピーの送付（電子・物理）

本人確認書類をコピーした紙媒体を郵送したり、事前に本人確認書類を撮影した画像ファイルをアップロードする方法です。書類の偽造に非常に弱い方法とされ、犯収法では27年4月、携帯電話不正利用防止法では26年4月より非対面での身元確認方法として利用できません。

書類コピーの送付の概要

ユーザの操作

- 住民票などの本人確認書類の写真を撮影し、Webサイト上でアップロード
  もしくは、
- 本人確認書類の写しを郵送にて送付

事業者の手順

- 書類真正性確認: 改ざんなどの不自然な点がないかを確認
- 再提出依頼: 画像や紙媒体の印刷不鮮明による差し戻し対応

書類の種類

25年6月改正前の犯収法施行規則の例：
現在の住居の記載のある本人確認書類（2点）
または、現在の住居の記載のある本人確認書類（1点） + 現在の住居の記載のある補完書類（1点）

本人確認書類の例
- 住民票の写し
- 運転免許証
- 健康保険証

補完書類の例
- 公共料金領収書

ユーザ体験

- 高齢者などITリテラシーが低い層でも利用しやすい
- 写真撮影やコピー時に書類不鮮明になる可能性がある
- 郵送する場合、郵送コストがかかる

開発・ランニングコスト

- システム開発は基本的に不要
- 対応を行うスタッフの教育・トレーニングコストが継続的に発生（偽造防止要素の知識、確認手順、法令対応など）

脅威への対応

画像ファイルや本人確認書類のコピーであるため、書類の偽装を見抜くことが非常に難しい

スマホ内に格納されたデータの取得

スマートフォンのマイナンバーカード※1では、マイナンバーカードの機能をスマートフォンで利用できます。一度登録すれば、その後は生体認証を利用できる場合もあり、ユーザにとって利便性の高い方法です。新しい手法のため、今後の普及が期待されます。

スマホ内に格納されたデータの取得の概要

ユーザの操作

▼iPhoneのマイナンバーカード（非対面の場合）
1）事業者アプリにて「Appleウォレットで本人確認」ボタンをタップ
2）Face IDやTouch IDによる認証

▼スマホ用電子証明書（非対面の場合）
1）事業者アプリにてスマホ用電子証明書で本人確認を選択
2）マイナアプリが立ち上がり、スマホ用電子証明書用パスワードの入力

事業者の手順

- スマートフォンのマイナンバーカードに対応したスマホアプリの用意
- データの署名検証：カード代替電磁的記録※2は確認プログラムの用意、スマホ用電子証明書は認定事業者との接続が必要
- 目視確認等が不要

書類の種類

スマートフォンのマイナンバーカード

ユーザ体験

- マイナアプリで「iPhoneのマイナンバーカード」や「スマホ用電子証明書」の登録をする必要がある
- 機種変更時にスマホ用電子証明書の削除等の対応が必要
- 古い端末やメーカによって対応していない場合がある

開発・ランニングコスト

- カード代替電磁的記録、スマホ用電子証明書に対応したスマホアプリの開発
- 従量課金：採用する認定事業者やソリューションベンダーによって利用料が発生

脅威への対応

デジタル証明書が、端末のセキュアエレメント（SE / FeliCaチップ等の耐タンパー領域）に保存されるため、盗難・複製の恐れが低い

現物のICカードと同等レベルの強固な手段。書類の正しさを電子署名を用いて検証できるほか、書類によっては現在有効かどうかも確認が可能（失効確認）

※1：スマートフォンのマイナンバーカードについての詳細は、「スマートフォンのマイナンバーカード」（デジタル庁）を参照のこと。
※2：カード代替電磁的記録についての詳細は、「カード代替電磁的記録（属性証明機能）」（デジタル庁）を参照のこと。

目視確認

物理的な本人確認書類そのものを、店頭で店員が確認する方法です。対面での本人確認においては一番普及している方法ですが、偽造の検知は店員のスキルに依存し、精巧な偽造を検知することは難しい場合があります。また、店舗運営のコストがかかります。

目視確認の概要

ユーザの操作

1）本人確認書類（原本）を店舗に持参する

2）店員からの案内に従い、書類を提示する

事業者の手順

- 提示された書類の種別・有効期限・券面記載事項（氏名・住所・生年月日など）を目視確認
- 改ざん・コピー提示などの不自然な点がないかを確認（厚み、ホログラム、印刷状態など）
- 必要に応じて、券面をコピーまたはスキャンし、保管（法令・社内ルールの範囲内）

書類の種類

■顔写真付きの書類
・運転免許証/運転経歴証明書
・マイナンバーカード
・在留カード・特別永住者証明書　など

■顔写真のない書類（必要に応じて複数点の組み合わせが必要）
・健康保険証
・住民票の写し
・公共料金の領収書　など

ユーザ体験

- 店舗の営業時間内に来店する必要があり、利用時間が制限される
- 来店・待ち時間・手続き時間が発生し、オンライン完結型に比べると手間が大きい
- 手続き自体は従来から馴染みがあり、高齢者などITリテラシーが低い層でも利用しやすい

開発・ランニングコスト

- システム開発は基本的に不要
- 店舗スタッフの教育・トレーニングコストが継続的に発生（偽造防止要素の知識、確認手順、法令対応など）
- 店舗運営に伴う固定費（店舗賃料、設備費、人的コスト）が必要
- 内部監査・コンプライアンスチェックの工数が必要

脅威への対応

真偽判定は原則として「人の目」に依存するため、偽造検知の品質は店舗・担当者ごとにばらつきが生じやすい

自己申告（書類なし）

本人確認書類の提示を受けず、自己申告によって登録を受け付ける場合もあります。必要以上に個人情報を取得しないのでユーザのプライバシーを守ることができる一方で、当人認証手段の紛失時の復旧（アカウントリカバリ）や法的な連絡が必要な場合にそれが出来ないリスクもあります。

自己申告の概要

ユーザの操作

特になし

事業者の手順

特になし
（必要に応じて桁数チェックなど）

書類の種類

書類なし

ユーザ体験

手入力

開発・ランニングコスト

特になし

脅威への対応

住所・氏名については、郵送による検証を行うことで、一定レベルの確認を行うことができる

主な本人確認書類の解説

- 留意事項
- 本人確認書類の系譜
- 顔写真付き本人確認書類の特徴比較
- マイナンバーカードの概要
- 実物のマイナンバーカード
- 顔認証マイナンバーカード
- スマートフォンのマイナンバーカード
- （参考）マイナ保険証とは
- 運転免許証
- マイナ運転免許証
- 在留カード・特別永住者証明書（第２世代・特定含む）の概要
- 第２世代在留カード・第２世代特別永住者証明書
- 在留カード・特別永住者証明書（第１世代）
- 特定在留カード・特定特別永住者証明書

本章参照時の留意事項

他章と同様に、本章の記述は、OpenIDファウンデーション・ジャパン KYCワーキンググループ 本人確認ガイドラインサブワーキンググループが信頼できると判断した情報をもとに細心の注意を払って作成・表示したものですが、当団体は、本章の内容および当該情報の正確性、完全性、的確性、信頼性等についていかなる保証をするものではありません。

特に、本章の解説をご利用いただくにあたり、以下の点に十分ご留意ください。

1. 情報の性質（当局との守秘義務の遵守） 本章に記載された実運用ノウハウは、一般に公開されている情報、および当サブワーキンググループ参加メンバーの実務から得られた知見のうち、**関係当局との守秘義務（NDA等）に抵触しない範囲で一般化・抽象化されたもののみ**で構成されています。関係当局の非公開情報、個別具体的な審査基準、または公式見解を示すものではありません。

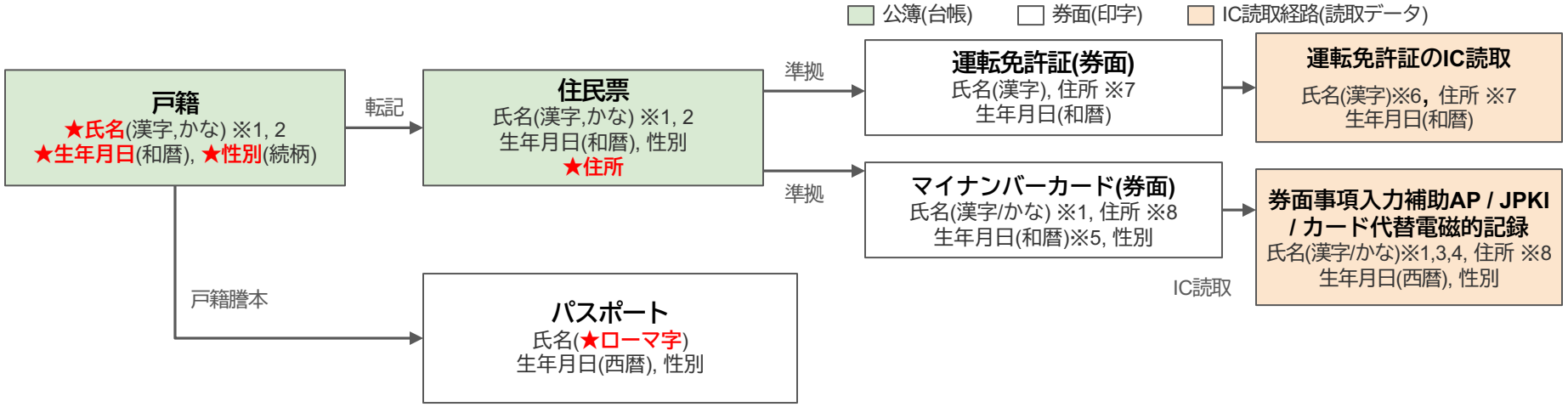
2. 法的助言の否認 本章の内容は、技術的・実務的な参考情報の共有を目的とするものであり、法的助言を提供するものではありません。特定のサービスにおける要件を法的に満たすか否かについては、利用者自身の責任において、関連法令および所管官庁の最新のガイドライン等をご確認ください。

3. 技術仕様の変動リスク ICチップの読み取りに関する技術的仕様（OSやNFC読み取りデバイスの挙動、各公的本人確認書類の仕様変更等）は継続的にアップデートされます。本章に記載された挙動や実装方法が、すべての環境で再現すること、および将来にわたって有効であることを保証するものではありません。

本章の内容につきましては、利用者の判断に基づきご利用をお願いします。本章の利用によって何らかの損害（直接損害・間接損害とを問いません）が発生した場合でも、OpenIDファウンデーション・ジャパン並びに執筆者は一切の責任を負いません。

本人確認書類の系譜 ① 日本国籍の人

「本人確認書類の系譜」は、それぞれの本人確認書類が、何を拠り所に作られているかを表したものです。
日本国籍の人の場合、戸籍を起点として、住民票への転記や、それに基づく各書類の作成を経て、本人確認書類が作られます。その過程で、氏名に使われる文字や生年月日の表記などが変換されています。そのため、同一人物でも不一致が生じる可能性があります。

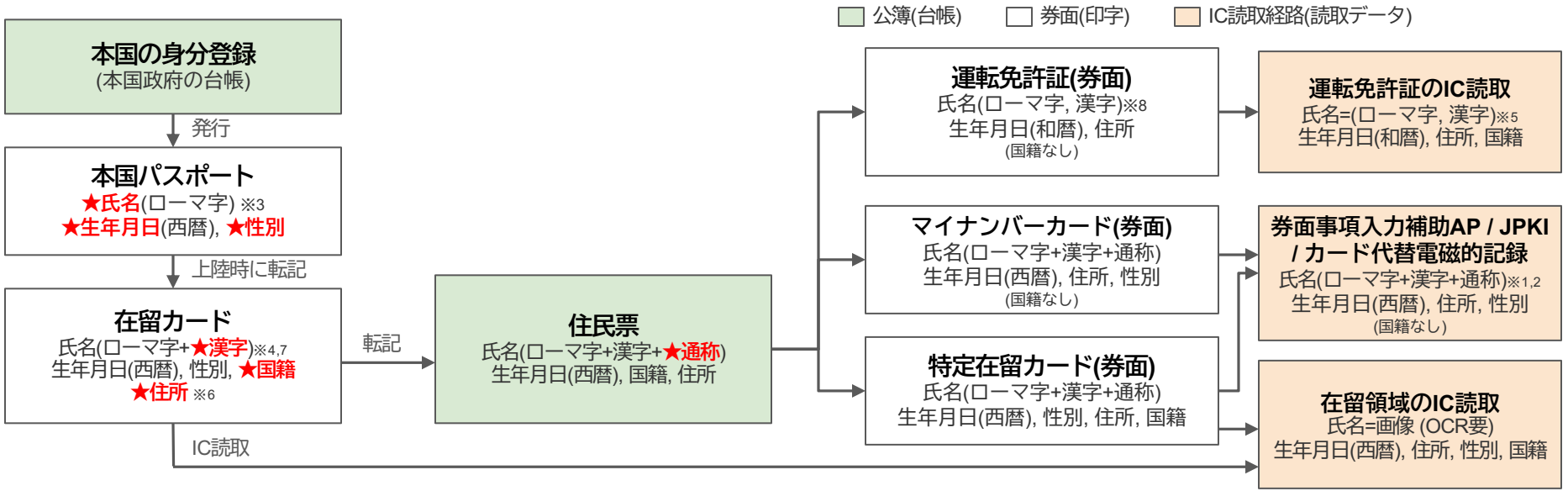


※1 かな(振り仮名)の記載開始: 戸籍=2025年5月～ / 住民票・マイナンバーカード=2026年5月～ (法務省・総務省)
※2 旧姓: 戸籍=「従前の氏」が起点。住民票=申出制の旧氏併記(2019年11月～)。戸籍・住民票・各券面では漢字氏名と旧姓は別欄 (総務省)
※3 マイナンバーカードのICテキスト経路 (券面事項入力補助AP/JPKI/カード代替電磁的記録) では、旧姓併記者は「姓［旧姓］名」の1本連結で返る (J-LIS・KYC WG調査)
※4 ICテキスト経路で使える漢字はJIS X 0208+補助漢字の範囲のみ。範囲外は代替文字に置換され、券面(原字)と文字が異なり得る (例: 髙→高、﨑→崎) (J-LIS・KYC WG調査)
※5 2026年5月26日～、申出によりマイナンバーカードの追記欄にローマ字氏名と西暦の生年月日を記載可 (券面本欄の生年月日は和暦のまま) (総務省)
※6 免許証ICの氏名はJIS X 0208の範囲で記録。外字の位置は特殊な文字コード(FFF1等)に置換され、字形データは別領域に格納される (警視庁・KYC WG調査)
※7 免許証の住所変更は届出制 (住民票の写し以外でも手続き可)。交番等での手続きではICが書き換えられない場合がある (警察庁)
※8 マイナンバーカードの住所は住民票の異動手続きの際に券面・ICとも更新。署名用電子証明書は住所変更で自動失効 (J-LIS)

上記出典をもとにKYC WGで作成

本人確認書類の系譜 ② 外国籍の人

外国籍の人の場合、本国パスポートを起点として、在留カードや住民票への転記、それに基づく作成を経て各書類が作られます。住民票から運転免許証・マイナンバーカードが作られる流れは日本国籍の人の場合と共通していますが、使われる文字の種類や、国籍・通称といった外国籍の人特有の情報が載る点に違いがあります。



※1 ICテキスト経路で使える漢字はJIS X 0208+補助漢字の範囲のみ。範囲外は代替文字に置換され、券面(原字)と文字が異なり得る (例: 髙→高、﨑→崎) (J-LIS)
※2 マイナンバーカードのICテキスト経路の氏名は「ローマ字_漢字（通称）」の1本連結で返る (KYC WGによる調査)
※3 パスポート(MRZ)では姓と名の判別可能。ミドルネームは基本的に名側に含まれるが、国ごとに扱いが異なるので、どれがミドルネームかは判別不可 (ICAO)
※4 在留カード以降は、姓と名の区切りも失われ、全体が1つの文字列として記載される (入管庁)
※5 免許証ICの氏名はJIS X 0208の範囲で記録。外字の位置は特殊な文字コード(FFF1等)に置換され、字形データは別領域に格納される (警察庁)
※6 在留カードの住居地は、入国後に市区町村へ住居地を届け出た時点で記載される。この届出が最初の住民登録となる。 (入管庁)
※7 在留カードの漢字併記は申出制。簡体字等は日本の正字に置き換えて表記される (入管庁)
※8 外国人の免許証の漢字・通称の記法は県の要領で異なる (「／」区切り、「（）」括弧書き、通称を「コト」で連結する県も) (青森県警・島根県警・KYC WG調査)

上記出典をもとにKYC WGで作成

本人確認書類の系譜 ③ 属性突合の失敗パターン

同じ人でも、本人確認に使う書類や読み取り方、読み取るタイミングによって、取得できる属性の表現・鮮度・有無が異なります。そのため、同一人物でも不一致が生じ得ます。代表的な失敗パターンを以下に整理します。

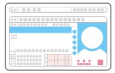
分類	失敗パターン	何が起きるか	例
氏名 (文字の変換)	代替文字	券面は原字のまま、マイナのICテキスト経路はJIS範囲内の別字に置換される	免許証券面「髙」 JPKI「高」
	正字置換	本国の簡体字等は、在留カードで日本の正字に置き換わる	本国パスポート「张」 在留カード「張」
	外字の脱落	免許証ICはJIS外の字が参照値(FFF1等)になり、テキストが欠ける	免許証IC「山［外字画像］太朗」 JPKI「山崎 太朗」
氏名 (構造の違い)	旧姓・通称の連結	券面は別欄だが、ICテキストは「姓［旧姓］名」「ローマ字＿漢字（通称）」の1本連結で返る	マイナ券面「田中 花子」 JPKI「田中［佐藤］　花子」
	姓名区切りの喪失	姓/名の区切りが分かるのはパスポート(MRZ)まで。以降は1本の文字列となり、分割が読み取り側の解釈依存になる (語順も国や発行時期で異なる可能性)	旧パスポート「HONG GIL DONG」→ 名=GIL DONG 新パスポート「HONG GILDONG」→ 名=GILDONG ローマ字声明表記の変更許容要件
	記法の差 (外国人免許証)	都道府県によりスラッシュ式・括弧式・コト式など記法が異なる	免許証「LI MING／李 明」 マイナ「ＬＩ ＭＩＮＧ＿李 明」
	文字体系の交差	ローマ字のみの書類と漢字のみの書類は、直接は比較できない	パスポート「TANAKA」 免許証「田中」
生年月日	和暦/西暦	券面は和暦、ICテキスト経路・パスポートは西暦で表記される	免許証券面「昭和55年」 JPKI「1980年」
住所	更新タイミングのズレ	免許証は住民票と自動連動しない。マイナも手続きまでは券面AP・券面事項入力補助APが旧住所のまま (署名用電子証明書は失効して取得不可)	免許証(旧住所) マイナ(新住所)
	表記ゆれ	免許証の住所はハイフン等の略記で登録されることが多い (住民票どおりの表記は申出制)。マイナは住民票の正式表記のまま乗る。 (警察庁報告書)	免許証「1-2-3」 マイナ「一丁目2番3号」
	外字 (住所)	地名の外字も氏名と同様に変換される (免許証IC=画像化、マイナICテキスト経路=代替文字)。 (警察庁報告書)	マイナ券面「﨑山町1-2-3」 JPKI「崎山町1-2-3」
	字種の揺れ (ローマ数字等)	ローマ数字「Ⅳ」等はJIS X 0208に無いため、保持できないシステムでは英字「ＩＶ」に開いて登録される (総務省も英字置換を提示)	券面OCR「メゾンⅣ」(印字どおり) ICテキスト経路「メゾンＩＶ」(英字で登録)
属性の欠損	比較対象が無い	免許証に性別なし / マイナIC経路に国籍なし / パスポートに住所なし	—

各事象の出典は「本人確認書類の系譜 ①②」の注釈を参照。上記をもとにKYC WGで作成

顔写真付き本人確認書類の特徴比較

顔写真付き本人確認書類は、記載事項のほか、普及率、ICチップの格納情報や読み出すための暗証番号の有無など特徴が異なり、これらの違いを理解した上で選択することが重要です。

主な顔写真付き本人確認書類の特徴

		 マイナンバーカード	 運転免許証※2	 在留カード・特別永住者証明書※3	 パスポート
特徴	対象	住民基本台帳に記録されている者	自動車等の運転資格を有する者	中長期間在留する外国人、特別永住者	日本国籍を有する者
	発行数※1	約1億385万枚 うち、ｽﾏｰﾄﾌｫﾝのﾏｲﾅﾝﾊﾞｰｶｰﾄﾞ保有者約854万枚 （デジタル庁ダッシュボード 2026.6時点保有枚数）	約8,150万枚※4 （令和7年版 運転免許統計）	中長期在留者：約349万人 特別永住者：約27万人 （2025年版 出入国在留管理）	約2,282万枚 （令和7年の旅券統計）
	電子証明書	①署名用電子証明書 ②利用者証明用電子証明書	-	-	-
	顔写真以外の主な券面情報	氏名、住所、生年月日、性別、個人番号等	氏名、住所、生年月日、免許証番号、免許の条件等	氏名、住所、生年月日、性別、カード番号、在留資格、国籍、在留期間・満了日、許可の種類等	氏名、生年月日、性別、旅券番号、国籍等 ※ 住所の記載なし
	ICチップの主な情報	氏名、住所、生年月日、性別、個人番号、電子証明書、顔写真等	氏名、住所、生年月日、本籍、交付年月日、有効日末日、免許の種類、番号、顔写真等	券面画像、顔画像等	旅券番号、国籍、氏名、生年月日、顔写真等

※2 運転経歴証明書
免許証を自主返納した人や更新を受けずに失効した人が交付を受けられ、氏名、住所、生年月日、免許証番号等に加え、顔写真も表示されている。有効期限は無く、ICチップも搭載されていない。

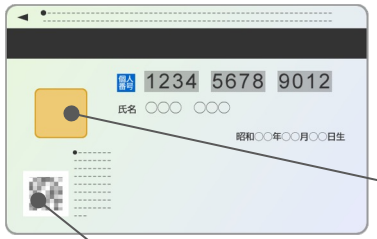
※3 特別永住者証明書
特別永住者の法的地位等を証明するものとして交付されるもので、氏名、生年月日、性別、国籍・地域、住居地、有効期間の満了日などの情報が記載（16歳以上には顔写真が表示）
ICチップを搭載。

※1：発行数は本ガイドラインの作成時点のものであり、最新の数値は各サイト等を参照。
※4：運転免許証は保有しておらず、マイナ運転免許証のみ（1枚持ち）の者も含む

マイナンバーカードの概要

マイナンバーカードは、2026年6月時点で人口に対する保有率が83%以上の本人確認書類です。ICチップに格納された電子証明書を活用し、本人確認だけでなく、様々なサービスを利用できます。

マイナンバーカードのICチップ内のアプリケーション構成



このQRコードからも
マイナンバーの読み取りが可能

搭載アプリケーション	（アクセスコントロール）	空き領域
公的個人認証（JPKI）AP 2種類の電子証明書	署名用：6桁～16桁の英数字 利用者証明用：4桁の数字 **（記憶認証）**	空き領域 地方自治体や国のアプリを搭載する領域。 一部の民間事業者も利用可能
券面AP 券面記載事項（顔写真含む）の画像データ	マイナンバー又は14桁の照合番号B※1 **（券面記載情報）**	
券面事項入力補助AP 氏名、住所、生年月日、性別やマイナンバーのテキストデータ	マイナンバー、14桁の照合番号B、もしくは4桁の暗証番号※1 **（記憶認証又は券面記載情報）**	
住基AP 住民票コードのテキストデータ	4桁の数字 **（記憶認証）**	

ICチップには、税や年金などのプライバシー性の高い情報は格納されていない。
また、パスワードを一定回数間違えるとロックされる仕組みになっているほか、不正に情報を読み出そうとする場合、ICチップが自動で壊れるようになっている。

※1：券面AP及び券面事項入力補助APのアクセスコントロールは、どの情報を取得するか（特にマイナンバーを取得するか否か）によって異なる。
出典：総務省ウェブサイト「マイナンバー制度とマイナンバーカード」、「マイナンバーカード交付状況について」より作成。

実物のマイナンバーカード

実物のマイナンバーカードから身元確認に利用する情報をデジタル的に取得する方法は、主に２つあります。

公的個人認証（JPKI）AP の「署名用電子証明書」機能を利用

- アクセスコントロール：ユーザが設定した6桁～16桁の英数字による暗証番号（パスワード）
- 取得できる情報：氏名、住所、生年月日、性別、氏名・住所の外字位置情報

券面AP・券面事項入力補助APを組み合わせて利用

- アクセスコントロール：券面記載の情報を組み合わせた14桁の照合番号B※1
- 取得できる情報：顔写真（白黒）、氏名、住所、生年月日、性別、氏名・住所の画像情報

注意事項：氏名には旧姓、ふりがな、通称などが付与される可能性があります。
15歳未満の場合には署名用電子証明書は発行できません。
申請時に1歳未満である場合は例外的に「顔写真なし」で交付されます。
生年月日には不明、年のみ、年月のみ、年および季節など様々な例外的な表記が存在します。

補足：券面AP・券面事項入力補助APを組み合わせて利用する場合に、券面事項入力補助AP用暗証番号(4桁)を用いて個人番号を含むテキスト情報を取得後、個人番号を照合番号Aとして用いて券面APの情報を取得する手段も存在するが、その場合には個人番号を一時的にでも取得・利用することとなるため、番号法に基づく事務でのみ利用可能。

※1：券面AP及び券面事項入力補助APのアクセスコントロールは、どの情報を取得するか（特にマイナンバーを取得するか否か）によって異なる。
出典：総務省ウェブサイト「マイナンバー制度とマイナンバーカード」、「公的個人認証サービス プロファイル仕様書」より作成。

顔認証マイナンバーカード

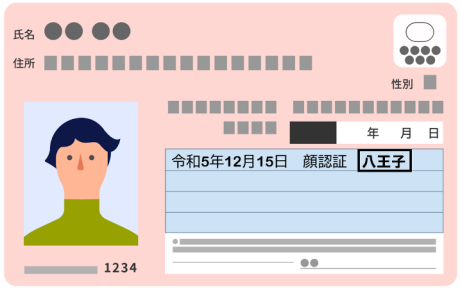
顔認証マイナンバーカードは暗証番号の設定や管理に不安がある人の負担軽減のために暗証番号を使用しないマイナンバーカードです。

実物のマイナンバーカードに対し、暗証番号等を閉塞したもの

- 署名用電子証明書を非搭載とし、利用者証明用電子証明書等の暗証番号をロックしたものです。
- 利用者証明用電子証明書の利用に係る本人確認方法を機器による顔認証又は目視による顔確認に限定します。

券面AP・券面事項入力補助APを組み合わせてICチップの情報を取得可能

- アクセスコントロール：券面記載の情報を組み合わせた14桁の照合番号B※1
- 取得できる情報：顔写真 (白黒)、氏名、住所、生年月日、性別、氏名・住所の画像情報



マイナンバーカードの追記欄に「顔認証」と記載します
出典:「暗証番号を使用しない「顔認証マイナンバーカード」について」

※1：券面AP及び券面事項入力補助APのアクセスコントロールは、どの情報を取得するか（特にマイナンバーを取得するか否か）によって異なる。

スマートフォンのマイナンバーカード

スマートフォンのマイナンバーカードはマイナンバーカードの機能をスマートフォンに追加して利用できるサービス※1で「スマホ用電子証明書」と「カード代替電磁的記録※2」があります。「カード代替電磁記録」では、暗証番号入力の代わりに登録時に設定した生体認証を使って簡単かつ安全に属性情報の確認ができます。2026年6月時点で約854万枚保有されています。

※1 スマートフォンのマイナンバーカードはマイナンバーカード用電子証明書による電子署名に基づき発行されるため、マイナンバーカードを持っていない場合、顔認証マイナンバーカードや15歳未満のマイナンバーカードといった署名用電子証明書非搭載のマイナンバーカードの場合は、利用できない。
※2 2026年7月現在、Androidの「カード代替電磁的記録」は未対応。

	スマホ用電子証明書	カード代替電磁的記録（属性証明機能）
説明	マイナンバーカード用電子証明書と同一の認証局から発行され、スマートフォンの安全な場所に格納されている電子証明書。「スマホ用署名用電子証明書」（登録時に設定した英数字6～16文字の暗証番号で利用可能）と「スマホ用利用者証明用電子証明書」（登録時に設定した数字4桁の暗証番号、あるいは、登録時に設定した生体認証で利用可能）の2種類ある。	マイナンバーカードに記録された情報をスマートフォンに搭載しスマートフォンを利用して身元確認を行うことができるデータ。 登録録時に設定した生体認証で利用可能。 ※ 2026年7月現在Androidでは未対応のため、iPhoneでの利用について記載しています。 ※ Androidにおける詳細は、対応され次第公開される情報をご確認ください。
iPhone	■ 2025年6月24日～対応（Apple Wallet）	■ 2025年6月24日～対応 ■ 氏名・住所・顔写真等をmdoc(ISO/IEC 18013-5)形式で格納
Android	■ 2023年5月～対応（Android先行開始） ■ 「Androidスマホ用電子証明書搭載サービス」と呼ばれている	■ 2026年7月現在未対応（2026年秋頃対応予定） ■ 対応後は身元確認と年齢確認ができるようになる見込み

出典：公的個人認証サービス ポータルサイト「スマホ用電子証明書の搭載について」、デジタル庁「スマートフォンのマイナンバーカード｜デジタル庁」を元にKYC WGにて作成。

マイナンバーカードデータ項目

カード代替電磁的記録のデータ項目について、実物のマイナンバーカードに格納されている情報はそのまま日本政府の名前空間に格納されます。なお、生年月日の二次的利用データは汎用名前空間に格納されます。

.JP Namespace (org.iso.23220.1.jp)

データ	説明
氏名	氏名を示す文字列（セパレート文字を使用して旧姓、通称、フリガナなどを含む）
生年月日	生年月日を示す文字列 (不明、年のみ、年月のみ、年および季節など様々な例外的な表記を含む)
現住所	現住所を示す文字列
性別	性別を示す文字列
写真	JPEG2000 形式のバイト文字（白黒）
市町村コード	全国の都道府県や市区町村に割り当てている固有の識別番号
マイナンバー	マイナンバーを示す文字列

Global namespace (org.iso.23220.1)

データ	説明
年齢確認	年齢（歳）
20 歳以上	対象年齢以上であることを示すフラグ

取得できるデータの例

名前空間	要素	サンプル値
org.iso.23220.1.jp	full_name_unicode	“日本［東京］　花子”
	birth_date_unicode	"2000年1月 23日"
	resident_address_unicode	○○県△△市□□町１−２−３
	sex_unicode	“男”
	portrait	（バイト文字）
	local_gov_code_unicode	“14109”
	individual_number_unicode	“123456789012”
org.iso.23220.1	age_in_years	23
	age_over_20	true

注意事項：取得方法によっては取得できる情報が異なる場合がある

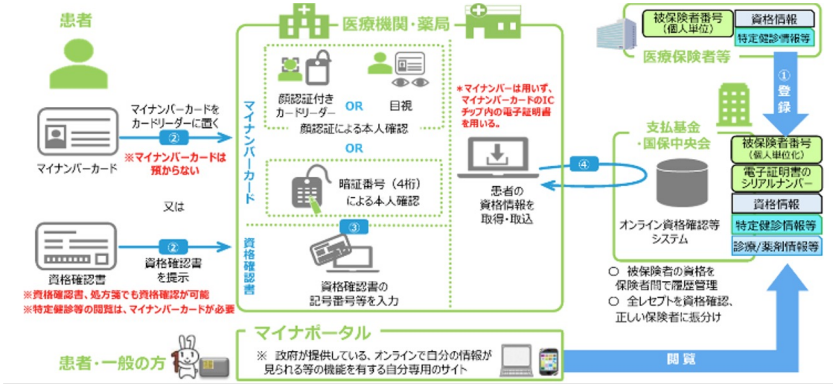
注意事項：具体的な仕様は、デジタル庁に申請をして入手する必要があります。
出典：「PKIdentityNationalIDCardDescriptor」（Apple）、「調達仕様書_マイナンバーカード機能等のスマートフォンへの搭載に係るセキュリティ規定作成業務」（デジタル庁）を元にKYC WGにて作成
灰色枠内のサンプル値の情報は、KYC WG参加者の独自調査によるもの

（参考）マイナ保険証とは

マイナンバーカードの利用者証明用電子証明書を使って、保険資格の確認ができる仕組みです。

マイナ保険証の概要

- マイナンバーカード内には情報が格納されておらず、医療機関・薬局等は、社会保険診療報酬支払基金・国民健康保険中央会が提供するオンライン資格確認システムを利用して、利用者証明用電子証明書を元に、保険者情報を確認します。
- 実物のマイナンバーカードの場合には、４桁の利用者証明用電子証明書用暗証番号、もしくは機械的な顔照合を行い、所有者本人であることを検証する。それらが利用できない場合であっても、医療機関側の目視による顔確認で利用者証明用電子証明書を利用することができる。
- 電子証明書の有効期限が切れてからも３ヶ月間は、引き続き健康保険証としての利用が可能。



補足：機械的な顔照合の場合には、券面に記載された照合番号Bをもちいてカードの**IC**チップ内に格納された顔写真を取得していると推定される。

出典：「オンライン資格確認について（医療機関・施術所等、システムベンダ向け）」（厚生労働省）
灰色枠内の情報は、KYC WG参加者の独自調査によるもの

運転免許証

運転免許証は都道府県公安委員会が運転資格を証明するために発行する公的な証明書で、氏名、住所、生年月日、顔写真等を公的に証明する本人確認書類として広く利用されています。

取得できる主なデータ

データ種類	内容	券面記載の有無	読み出しに必要な暗証番号
テキスト	免許証の番号	券面にも記載される	暗証番号1
テキスト	免許の年月日		
テキスト	交付年月日		
テキスト	有効期間の末尾		
テキスト	免許の種類（普通、大型等）		
テキスト	氏名		
テキスト	住所		
テキスト	年月日		
テキスト	免許証の色区分		
テキスト	免許の条件(AT限定、眼鏡等)		
テキスト	公安委員会名		
画像	顔写真（白黒）		暗証番号1 + 暗証番号2
テキスト	本籍	券面には記載されない	

出典：「運転免許証の暗証番号の運用に係る留意事項について」（警察庁）を元にKYC WGにて作成

券面イメージ

出典：「運転免許の更新等運転免許に関する諸手続について」（警察庁）

運転免許証

実物の運転免許証から身元確認に利用する情報をデジタル的に取得することができます。

暗証番号１を利用

- アクセスコントロール：ユーザが設定した4桁の数字による暗証番号
- 取得できる情報：氏名、住所、生年月日、氏名・住所の外字文字等

暗証番号１・２を利用

- アクセスコントロール：ユーザが設定した4桁の数字による暗証番号２つ
- 取得できる情報：上記に加え、顔写真、本籍

注意事項：運転免許証には性別は記載されない。旧氏名は、角括弧で囲い、現氏名の後ろに続けて記録する。
（例：日本　花子［東京花子］）ICチップに新住所・新氏名等が記録されている場合でも、署名の検証はできない。
外字や欠字が設定された場所は、特殊な文字コードに置き換えられるので、テキストで完全な氏名・住所を取得できない。（外字は“FFF1”～“FFF7”、欠字は“FFFA”の文字符号で表現され、外字データは記載事項とは異なる論理フォルダ階層に格納される。）
暗証番号１のみを利用した場合、署名値が検証できないので、情報の真贋の判断ができない。

その他：IC書き換え設備のない警察署等で住所変更を行った場合など、ICチップに新住所が反映していない場合がある。
検証方法：署名検証に利用する証明書は各自治体の公安委員会ごとに異なる。証明書の入手には警察庁運転免許課への問い合わせが必要。
住所欄は、自治体（公安委員会）によって、都道府県名からはじまる場合と、都道府県名が省略される場合がある。

出典：「運転免許証及び運転免許証作成システム等の仕様の改正について」（警察庁）より作成.
灰色枠内の情報は、KYC WGメンバーの独自調査による。

マイナ運転免許証

マイナ運転免許証では、マイナンバーカードのICチップ空き領域に免許に関する情報が書き込まれ、運転免許としても利用が可能です。
2025年3月24日から発行開始され、2026年6月末時点で約356万枚発行されています。

マイナ運転免許証のアプリケーション構成

搭載アプリケーション

- **公的個人認証（JPKI）AP**
  2種類の電子証明書
- **券面AP**
  券面記載事項（顔写真含む）の画像データ
- **券面事項入力補助AP**
  氏名、住所、生年月日、性別やマイナンバーのテキストデータ
- **住基AP**
  住民票コードのテキストデータ

空き領域

記録される免許情報

免許AP

- マイナ免許証の番号
- 運転免許取得年月日
- マイナ免許証の有効期間の末日
- 運転免許の種類（普通、大型など）
  免許の条件（AT限定、眼鏡など）
- 顔写真（白黒）
- 色区分（ゴールド、若草色など）

特徴

- 券面には運転免許に関する事項は記載されない。（ICチップへの記録）
- 氏名、住所は免許APに格納されておらず、券面事項入力補助APから情報を組み合わせて免許証データを生成（次頁）
- 運転免許情報はマイナ免許証読み取りアプリ、もしくはマイナポータルから参照可能
- 「マイナ免許証のみ保有」と「マイナ免許証＋運転免許の２枚保有」の選択が可能

出典：「マイナンバーカードの運転免許証利用」（デジタル庁）

参考：マイナ運転免許証の保有者数（2026年6月末時点）

保有パターン	保有者数
1. マイナ免許証のみ保有	1,001,373
2. マイナ免許証+運転免許の2枚保有	2,564,666
合計	**3,566,039**

出典；「マイナ免許証保有者数」（警察庁）

マイナ運転免許証

実物のマイナ運転免許証から属性情報をデジタル的に取得することができます。

免許AP情報の取得：マイナ免許証用暗証番号を利用

- アクセスコントロール：ユーザがマイナ運転免許交付時に任意で設定した4桁の数字による暗証番号
- 取得できる情報：免許基本情報（免許情報記録番号、色区分、有効期限、免許の条件）、
  免許の日付、免許の種類等

券面事項入力補助AP情報の取得：照合番号Bを利用

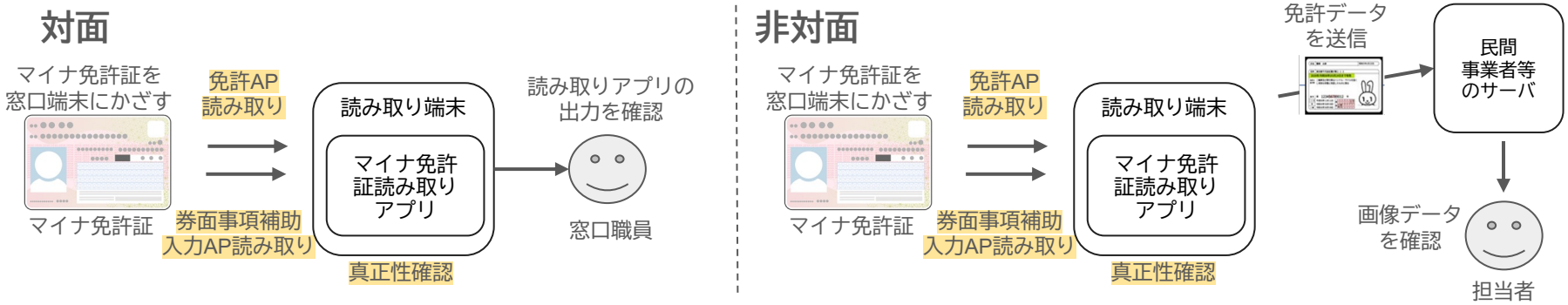
- アクセスコントロール：券面記載の情報を組み合わせた14桁の照合番号B
- 取得できる情報：氏名、住所、生年月日、性別

⇒免許APからの情報と券面事項入力補助AP の情報を組み合わせて活用可能

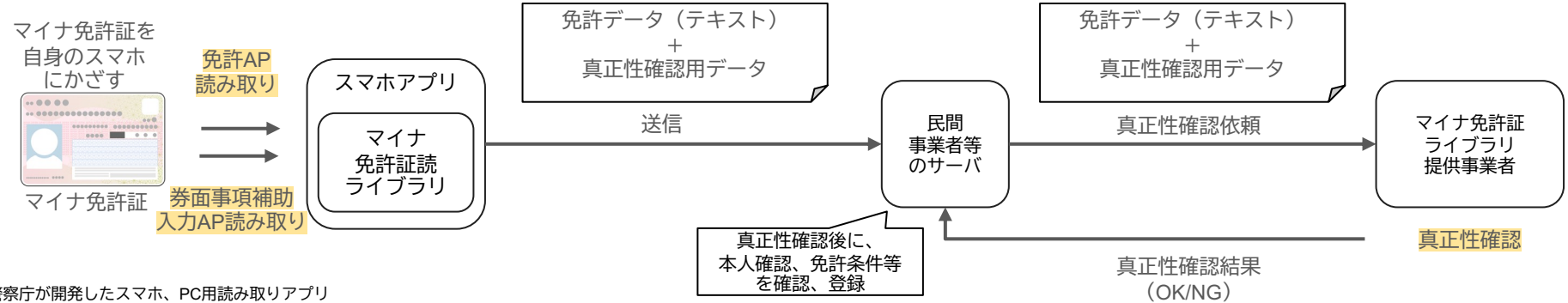
マイナ運転免許証

実物のマイナ運転免許証から情報を取得する際は、専用アプリやライブラリを用います。

マイナ免許証読み取りアプリ※1の活用



民間のマイナ免許証ライブラリ等の活用



※1：警察庁が開発したスマホ、PC用読み取りアプリ
出典：マイナンバーカード・インフォ（自治体向け）(デジタル庁)を元にKYC WGにて作成

在留カード・特別永住者証明書（第２世代・特定含む）の概要

外国籍で、日本に居住している人が保持している身分証です。いくつかの種類があります。第２世代、特定 各カードは、2026年6月14日から発行が始まったため、現時点での発行枚数は少数であると推定されます。

種類	保有者数(想定)	備考
第２世代在留カード	少数	2026年6月から発行開始。中長期間在留する外国籍の人が保有するカード。16歳以上常時携帯義務あり。
特定在留カード	少数	2026年6月から発行開始。マイナンバーカードと統合されたもの
在留カード（第１世代）	349万(2024末)	2026年6月まで発行されていた
第２世代特別永住者証明書	少数	2026年6月から発行開始。特別永住者の法的地位等を証明するものとして交付されるもの。常時携帯義務なし。
特定特別永住者証明書	少数	2026年6月から発行開始。マイナンバーカードと統合されたもの
特別永住者証明書（第１世代）	27万(2024末)	2026年6月まで発行されていた

出典：「2025年版「出入国在留管理」日本語版」（出入国管理庁）等を元にKYC WGにて作成
中長期在留者数 = 在留カード保有者数、特別永住者数 = 特別永住者証明書保有者数 とした。

注釈：上記に加えて、廃止済の外国人登録法において、平成24(2012)年7月9日時点で16歳未満だった特別永住者については、16歳の誕生日を迎えるまで外国人登録証明書が有効となっているため、現時点でも有効な外国人登録証明書がごく少数存在する可能性がある。（出典：「特別永住者・中長期在留者の方へ（お知らせ）」（出入国管理庁））

第２世代在留カード・第２世代特別永住者証明書

2026年6月14日から発行開始されました。仕様書・署名検証のための公開鍵情報が公開されており、誰でも読み取り機能を実装できます。

取得できる主なデータ（例）

データ種類	内容	備考
画像	顔	JPEG2000 カラー画像
画像	氏名	氏名は、英語名が前提だが、漢字名が併記される場合がある。
画像	住居地	署名されていない点に留意
テキスト	生年月日	
テキスト	有効期限満了日	
テキスト	国籍・地域コード	コード定義は公開されておらず、出入国在留管理庁に申請が必要
テキスト	在留資格コード	
テキスト	在留期間の満了日	特別永住者証明書は項目無し

セキュリティ；カード番号（１２桁）
試験方法；読み取り機能の開発のため、入出国管理庁の指定する場所で、テストカードの貸与を受けることができる。

出典：「第二世代在留カード等仕様書の公開について」（出入国管理庁）、
「在留カード漢字氏名表記申出」（出入国管理庁）を元にKYC WGにて作成

券面イメージ

出典：「在留カードとは？」
（出入国管理庁）

（第１世代）在留カード・（第１世代）特別永住者証明書

2026年6月13日まで発行されていました。仕様書・署名検証のための公開鍵情報が公開されており、誰でも読み取り機能を実装できます。

取得できる主なデータ（例）

データ種類	内容	備考
画像	顔	JPEG2000 カラー画像
画像	氏名	氏名は、英語名が前提だが、漢字名が併記される場合がある。 ※券面（表）イメージとして、すべて結合された１枚の画像として記録されており、OCRを行うにも範囲を指定する必要がある。
画像	住居地	
画像	生年月日	
画像	有効期限満了日	
画像	国籍・地域	
画像	在留資格	
テキスト	住居地 （裏面追記）	住所変更手続きが行われた場合 署名されていないことに留意

セキュリティ；カード番号（１２桁）
試験方法；読み取り機能の開発のため、入出国管理庁の指定する場所で、テストカードの貸与を受けることができる。

出典：「在留カード等仕様書の公開について」（出入国管理庁）、
「在留カード漢字氏名表記申出」（出入国管理庁）を元にKYC WGにて作成
灰色枠内の情報は、KYC WG参加者の独自調査によるもの

券面イメージ

出典：「在留カードとは？」
（出入国管理庁）

取得できる券面画像イメージ

出典：左記券面イメージを元にKYC WGにて加工

注意事項：氏名に漢字名が併記される場合、英語名の上に記載される。在留カードは入国時に空港で発行されるため、表面は住居地未定と記載される場合が多いが、裏面追記の住居地は、ICチップに書き込みされていないケースが非常に多いので注意。

特定在留カード・特定特別永住者証明書

2026年6月14日から発行開始されました。マイナンバーカードのICチップの空き領域に格納されます。仕様書・署名検証のための公開鍵情報が公開されており、誰でも読み取り機能を実装できます。

取得できる主なデータ（例）

データ種類	内容	備考
画像	顔	JPEG2000 カラー画像
画像	氏名	氏名は、英語名が前提だが、漢字名が併記される場合がある。
画像	住居地	署名されていない点に留意
テキスト	生年月日	
テキスト	有効期限満了日	
テキスト	国籍・地域コード	コード定義は公開されておらず、出入国在留管理庁に申請が必要
テキスト	在留資格コード	
テキスト	在留期間の満了日	特別永住者証明書は項目無し

セキュリティ：カード番号（１２桁）
試験方法：読み取り機能の開発のため、入出国管理庁の指定する場所で、テストカードの貸与を受けることができる。

出典：「第二世代在留カード等仕様書の公開について」（出入国管理庁）、
「在留カード漢字氏名表記申出」（出入国管理庁）を元にKYC WGにて作成
灰色枠内の情報は、KYC WG参加者の独自調査によるもの

券面イメージ

出典：「特定在留カード交付申請について」（出入国管理庁）

注意事項：原則マイナンバーカードとしてICを読めば、マイナンバーカードとしての情報が取得できるはずだが、特定カード未対応のICチップ読み取り機能で、マイナンバーカードより先に特定在留カード等のIC領域を先に読みにいってしまうと、未対応の券種の在留カード等としてエラーになってしまうので読み取れない場合がある。

申請者の検証手法の解説

- ICチップ読み取り時のパスワード・暗証番号
- 書類の顔画像と申請者の顔写真の比較
- スマホ内のデータ取得時のパスワード、暗証番号や生体認証
- 銀行口座情報にアクセスできることの確認
- 銀行口座（オンラインバンキング）にログインできることの確認
- 配達員の目視
- 郵送
- チェックなし

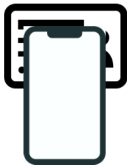
ICチップ読み取り時のパスワード・暗証番号

本人確認書類のICチップを読み取る際に、ユーザにパスワードや暗証番号といった、ユーザ本人しか知り得ない情報を入力することで、書類に記載の当人であることを確認します。

ICチップ読み取り時のパスワード・暗証番号の概要

ユーザの操作

暗証番号やパスワードの手入力



ICチップ付き本人確認書類をスマホやカードリーダにかざす

事業者の手順

- ICカードリーダ（対面の場合）やICカードを読むスマホアプリ等の用意
- データの署名検証（証明書を各公共機関から入手する必要がある）

書類の種類

1. マイナンバーカード
   署名用電子証明書用暗証番号（6-16桁）
   利用者証明用電子証明書用暗証番号（４桁）
   ※ 照合番号A、照合番号Bは券面に記載がある番号であり、申請者の検証はできない。

2. 運転免許証
   暗証番号（４桁 or ４桁 × 2）

ユーザ体験

- カードを所持している必要がある
- カードを読むためのデバイスが必要（非対面の場合）
- パスワードや暗証番号を覚えている必要がある
- 運転経歴証明書、在留カード、特別永住者証明書は使えない

開発・ランニングコスト

- ICカード読み取りのためのリーダデバイスの入手 or アプリ開発・SDKの入手
- 署名検証のための証明書の入手orSDKの入手
- JPKIを利用する場合には認定事業者との接続、利用料の支払い

脅威への対応

- パスワードや暗証番号を推測・盗み見されるリスク
- 申請者当人が共謀して他人にパスワードや暗証番号を供与した場合にはそれを防げない

書類の顔画像と申請者の顔写真の比較

本人確認書類の券面やICチップに格納された顔画像と、申請者本人の顔画像を比較し、当人であることを確認します。非対面ではカメラ経由で確認する場合もあります。顔の比較に機械を利用する場合もあります。

書類の顔画像と申請者の顔写真の比較の概要

ユーザの操作

■ 非対面の場合
1）ICチップの読み取り or 券面画像の取得
2）本人の容貌撮影（正面＋首振りや瞬きなどのLiveness判定アクション）
■ 対面の場合
1）店員への書類の提示 or ICチップ読み取り
2）店員or機械による顔画像の確認

事業者の手順

- 顔画像と容貌撮影した顔と一致確認
- 再提出依頼: 画像不鮮明による差し戻し対応

書類の種類

1. マイナンバーカード
2. 運転免許証
3. 在留カード
4. 特別永住者証明書
5. 運転経歴証明書
6. パスポート

ユーザ体験

■非対面の場合

- 容貌の正面・首振り・瞬きなどの撮影する

■対面の場合

- 書類の提示

開発・ランニングコスト

- 犯収法・携帯電話不正利用防止法等を満たしたeKYCセルフィーを独自実装することは難しい。初期導入費がかかる
- 従量課金：eKYCベンダーのソリューション利用料が発生。
- BPO費用：AIによる自動化は進んでいるが、最終的に人の目による確認が必要な場合、BPOコストや人的コストが必要

脅威への対応

- 偽造本人確認書類：精巧な偽造カードで悪意者の顔画像に貼り替えられていた場合、容貌比較が一致する
- 容貌撮影：ディープフェイク技術を悪用し、本人確認書類に写っている人物と、生成した偽の顔画像が同一人物と判定する攻撃が存在
- ICチップの顔画像の解像度：ICチップに保存されている顔画像の解像度が低く、同一人物と判定される可能性あり
- 担当者の目視誤り：偽造検知の品質は店舗・担当者ごとにばらつきが生じやすい

スマホ内のデータ取得時のパスワード、暗証番号や生体認証

スマートフォン内に格納された本人確認書類を読み取る際に、ユーザにパスワードや暗証番号の入力を求めたり、生体認証を行うことで、書類に記載の当人であることを確認します。

スマホ内のデータ取得時のパスワード、暗証番号や生体認証の概要

ユーザの操作

パスワード、暗証番号の
入力や生体認証を実施

事業者の手順

- ICカードリーダ（対面の場合）やICカードを読むスマホアプリ等の用意
- データの署名検証（証明書を各公共機関から入手する必要がある）

書類の種類

スマートフォンのマイナンバーカード

ユーザ体験

- カードを所持している必要がない
- 生体認証により、暗証番号を覚えておく必要がない場合もある

開発・ランニングコスト

- ICカード読み取りのためのリーダデバイスの入手 or アプリ開発・SDKの入手
- 署名検証のための証明書の入手orSDKの入手
- JPKIを利用する場合には認定事業者との接続、利用料の支払い

脅威への対応

- パスワード、暗証番号を推測・盗み見されるリスク
- 申請者当人が共謀して他人にパスワードを供与したり、生体認証登録を他人にさせた場合にはそれを防げない。
- 書類によっては、スマートフォンへの格納時に登録した生体情報との一致が必須な場合もある

銀行口座情報にアクセスできることによる確認

申請者名義の銀行口座に対し、少額の振込を行い、振込金額や振込明細情報を入力してもらうことで、銀行口座の残高を確認できることをもって、申請者当人であることを確認します。申請者の取引先銀行とのシステム接続が不要なことが利点です。

銀行口座情報にアクセスできることによる確認の概要

ユーザの操作

本人名義の銀行口座を申請

オンラインバンキングや通帳記帳で表示された金額や明細に記載のある情報を入力

事業者の手順

- 申請者の氏名と銀行口座の名義の一致を確認
- 銀行口座に少額の振込を実施
- ユーザが入力した情報の一致を確認

書類の種類

銀行口座

ユーザ体験

- 銀行口座を所持していれば誰でも利用可能
- オンラインバンキングへのログイン、もしくはATMで通帳記帳が必要

開発・ランニングコスト

- 銀行振込を行うための銀行とのシステム連携が必要
- 実際に少額を振り込むことになるため、その分の金額がコストになる
- 振込手数料が発生する

脅威への対応

- 銀行の本人確認プロセスに依存する（身元確認、当人認証の両方）
- 古い口座で、現行法に基づく本人確認が済んでいない銀行口座が存在する可能性がある
- 申請者当人が共謀して他人に口座を供与した場合にはそれを防げない。

銀行口座（オンラインバンキング）にログインできることの確認

申請者名義の銀行口座にログインし、ID連携を行うことで、申請者当人であることを確認します。銀行システムとのシステム連携が必要となるほか、ユーザが対応する銀行のオンラインバンキングを利用可能であることが必要です。

銀行口座（オンラインバンキング）にログインできることの確認の概要

ユーザの操作

本人名義の銀行口座を申請

オンラインバンキングにログインし、ID連携を許可する

事業者の手順

- 銀行とのID連携を実行
- 銀行から提供された情報とユーザが入力した情報の一致を確認

書類の種類

銀行口座

ユーザ体験

- オンラインバンキングを利用可能な銀行口座を所持している必要がある

開発・ランニングコスト

- 銀行とのAPI連携が必要
- API連携に対応する銀行が限られる
- 銀行から手数料を要求される可能性がある

脅威への対応

- 銀行の本人確認プロセスに依存する（身元確認、当人認証の両方）
- 古い口座で、現行法に基づく本人確認が済んでいない銀行口座が存在する可能性がある
- 申請者当人が共謀して他人に口座を供与した場合にはそれを防げない。

郵送による確認

転送不要郵便物を送付し、到着を確認することで、住所の確認を行います。郵送コストがかかります。

郵送による確認の概要

ユーザの操作

郵便物を受領する

事業者の手順

- 申請者が申請した住所に対して転送不要郵便で取引に関係する文書を送付
- 郵便物が到達したことを確認する

書類の種類

あらゆる書類

ユーザ体験

- 書留の場合、配達時に在宅している必要がある
- 身元確認の完了まで数日を要する

開発・ランニングコスト

- 郵便物を印刷・送付するためのコスト
- 到着確認を行うためのコスト

脅威への対応

- 申請者当人が共謀して他人に住所を供与した場合にはそれを防げない
- 悪意者が勝手に住所を使い、かつポストに投函された郵便物を搾取されるリスクに対応するには、書留郵便が必要

配達員による確認

郵便局や運送会社の配達員が、届け先や営業所等で本人確認書類を利用して身元確認を行います。人手での確認となるため、他の方法と比べてコストが高くなるケースが多いです。

配達員による確認の概要

ユーザの操作

配達員の来訪時、もしくは郵便局や運送会社の営業所に出向き、本人確認書類を提示する

事業者の手順

- 申請者が申請した住所に対して書留等の転送不要郵便で取引に関係する文書を送付
- 郵便物が到達したことを確認する、もしくは配達業者から本人確認記録を受領する

※ 対応する法令や本人確認方法の違いにより、複数のメニューがある（郵便局であれば、基本型・特例型・特定事項伝達型の３種類）

書類の種類

郵便局や配達会社が対応するもの
日本郵便の場合
・基本型：写真付き公的証明書1点（運転免許証、パスポート、マイナンバーカード等）
または写真の付いていない公的証明証または写真付き職員証・学生証等2点（健康保険等に係る資格確認証・職員証・学生証等）
・特例型：公的証明証1点（運転免許証、パスポート、マイナンバーカード、健康保険等に係る資格確認証）
・特定事項伝達型：写真付き公的証明書1点（運転免許証、パスポート、マイナンバーカード等）

ユーザ体験

- 郵便局や運送会社の営業所に出向いたり、配達員の来訪時に自宅にいる必要がある
- 身元確認の完了までに数日かかる

開発・ランニングコスト

- 郵便物を印刷・送付するためのコスト
- 一般書留の手数料
- 本人限定郵便の手数料

脅威への対応

- 現状、目視での確認が主体となるため、本人確認書類の偽造リスクがある

※ 犯収法施行規則 2027年4月施行より特定事項伝達型本人限定郵便方式でもICチップの読み取りが必須となる。

チェックなし

本人確認書類やそのコピーを保有していることをもって、申請者本人であることを確認します。書類の発行の難易度や、有効期限によって確認精度が異なります。

チェックなし（申請者の検証を行わない）の概要

ユーザの操作

特になし

事業者の手順

本人確認書類の検証方法に準ずる

書類の種類

あらゆる書類

ユーザ体験

本人確認書類の検証方法に準ずる

開発・ランニングコスト

とくになし

脅威への対応

- 書類のコピーや、当人に対して複数の発行ができる書類（住民票の写しなど）の原本を用いる場合には、申請者本人から悪意者が受け取ったり、盗難され、それを提示される可能性がある
- 当人に対して複数の発行ができる書類（住民票の写しなど）の原本を用いる場合には、発行から◯日以内のものと指定することで、上記のリスクを一定限軽減できる
- 一方、申請者当人が共謀して他人に書類を供与した場合にはそれを防げない

当人認証手法

当人認証の概要

当人認証は、事前に登録した人物と同一であることを確認するプロセスです。当人認証手法そのものの強度も重要ですが、当人認証方法の初期設定・リカバリ時に確実な身元確認を行うことは、それ以上に重要です。

当人認証においては、認証の３要素と呼ばれる、「記憶」・「所持」・「生体」の３つのうち２つ以上を組み合わせる「多要素認証」の概念が重要であると言われてきました。しかしながら、昨今では、発生しうる脅威を洗い出し、それらへの対策の観点で認証方法を選定する、脅威ベースの考え方が主流になりつつあります。たとえば、フィッシング耐性のない手法を複数組み合わせても、被害の軽減にはなったとしても、フィッシング攻撃から完全に防御することはできません。

次葉以降では、安全性が高く今後の普及が見込まれる手法と、現時点で広く普及しているレガシーな手法を紹介します。後者については、安全性に課題があるため留意しつつ、脅威に応じて他の手法と組み合わせて利用することを推奨します。

加えて、本人確認プロセス全体の強度は、身元確認、当人認証の両方のプロセスに依存します。どれだけ当人認証手法が安全であっても、確実な身元確認が行われていない状態で設定されたものの相対的な強度は低いものとなります。

当人認証プロセスの脅威と対策の例

No.	主な脅威	脅威の概要	対策例
1	オンライン上でのパスワードの推測	総当たりやパスワードリスト等により繰り返しログインを試行することで、なりすましを行う。	パスワードの複雑性の確保、一定時間当たりの認証回数の制限、多要素認証の採用
2	盗聴・リプレイ攻撃	通信を盗聴し、パスワード等を窃取することでなりすましを試みる、同じ内容を再送信することでなりすましを行う。	通信の暗号化、チャレンジレスポンス方式の採用、nonceの導入、ワンタイムパスワードの採用
3	パスワードや認証器の盗用	他サービスから漏えいしたパスワード、窃取したICカード等を用いてなりすましを行う。	多要素認証の採用
4	フィッシング攻撃	利用者を偽のサイトに誘導し、入力されたパスワード等を攻撃者が窃取したり、正規のサイトにリアルタイムに中継したりすることで、なりすましを行う。	フィッシング耐性を有する認証技術の採用
5	暗号鍵の不正な取り出し・複製	秘密鍵が格納されたデバイスに対し、物理的な解析やサイドチャネル攻撃等を行うことにより、秘密鍵を不正に取り出そうとする。	耐タンパ性を有するハードウェアの利用等

出典：「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(DS-511)」（デジタル庁）　表 3-6 当人認証における主な脅威と対策例

主な当人認証手法とその特徴（安全性が比較的高く、推奨される方法）

		同期パスキー	セキュリティキー（デバイス固定パスキー）	実物のマイナンバーカード利用者証明用電子証明書	スマートフォンのマイナンバーカード利用者証明用電子証明書
手法の概要		スマートフォンやPCにインストールされたパスワードマネージャーを利用した認証	セキュリティキーに生体やPINなどの第2要素を組み合わせた認証	マイナンバーカードの利用者用証明書と、暗証番号（4桁）の入力による認証	スマートフォン内に格納された利用者用証明書と、生体認証または暗証番号（4桁）の入力による認証
手法の特徴	認証要素	記憶+所持 or 生体+所持	記憶+所持 or 生体+所持	記憶+所持	記憶+所持 or 生体+所持
	フィッシング耐性	あり	あり	あり※	あり※
	ユーザーの利便性	生体認証を行うだけで、強度の高い認証が可能	生体認証を行うだけで、強度の高い認証が可能	マイナンバーカード1枚で強固なログインが可能	スマートフォン単体で強固なログインが可能
	ユーザの準備負担	自分専用のスマートフォンやPCの用意	セキュリティキーの購入	マイナンバーカードの申請手続き・NFCリーダやスマホの準備	マイナンバーカードの申請、スマートフォン用証明書の発行手続き
	複数デバイスでのログイン	パスワードマネージャによる同期、Hybrid方式による利用	セキュリティキーの差し替え	各デバイスにカードをかざす事で利用可能	設定可能なスマホは１台のみ
	ユーザに依存するリスク	弱いPINの設定、パスワードマネージャのアカウント奪取	弱いPINの設定	弱い暗証番号の設定	弱い暗証番号の設定
	留意事項	プロダクトにより、パスキー（暗号鍵）の管理方法やアカウントリカバリ等の利便性が変わる	セキュリティーキー紛失時の対応	紛失時の再発行手続きに通常1ヶ月程度要する	実物のマイナンバーカード紛失時に届出すると、スマホ用も同時に失効し、再発行手続きに通常1-1.5ヶ月程度要する

※：利用者証明用電子証明書による当人認証のフィッシング耐性は、それを行うサービスやアプリの実装により実現できる場合がある。

主な当人認証手法とその特徴（安全性に課題があるので避けるべきだが、必要に応じて組み合わせる）

		パスワード	SMS-OTP	EメールOTP	マジックリンク(Eメール)	アプリプッシュ
手法の概要		パスワードの入力	SMSで受信した4-6桁程度の数字を入力する	Eメールで受信した4-6桁程度の数字を入力する	Eメールで受信したURLを開くと、URLを開いたブラウザがログインした状態になる。	スマホアプリにプッシュ通知を行い、許可する。その際に数字の入力、選択などを求める場合もある
手法の特徴	認証要素	記憶	所持	所持※1	所持※1	所持※2
	フィッシング耐性	なし	なし	なし	一定の効果あり	なし
	ユーザーの利便性	一般的でなじみがあるが、複雑なパスワードを考えたり覚えるのが大変	認知度が高いが、ユーザが番号を入力する手間がかかる	認知度が高いが、ユーザが番号を入力する手間がかかる	メールを受信した端末のみ利用できるため、他端末でのログインに手間がかかる	専用アプリのインストール、ログインが必要
	ユーザの準備負担	なし	携帯電話	Eメールアカウント	Eメールアカウント	アプリのインストールとログイン
	複数デバイスでのログイン	制限なし	制限なし	制限なし	Eメールアカウントへのログインが必要	制限なし
	ユーザに依存するリスク	弱いパスワードの設定、使い回し、フィッシング	フィッシング	フィッシング/Eメールアカウントの認証強度が弱い	Eメールアカウントの認証強度が弱い	フィッシング、疲労攻撃
	留意事項	パスワードマネージャを利用することで一定のリスク削減が可能	SIMスワップ、番号使い回しの可能性あり	キャリアメールの場合はMNPで不通になる可能性がある	キャリアメールの場合はMNPで不通になる可能性がある	機種変更時に再登録が必要な場合がある

※1：Eメールによる認証の認証要素は、メールアカウントを所有しているという意味において「所有」と定義しているが、実際にはEメールアカウントへのアクセスの認証強度に依存する
※2：アプリプッシュによる認証の認証要素も、当該アプリをインストールし、事前にログインなどの設定を行った端末の所持という意味において「所持」と定義しているが、当該アプリでのログイン・初期設定時の認証強度に依存する

主な当人認証手法の解説

- 同期パスキー
- セキュリティキー（デバイス固定パスキー）
- マイナンバーカード利用者証明用電子証明書
- スマホ用マイナンバーカード利用者証明用電子証明書
- パスワード
- SMS-OTP
- EメールOTP
- マジックリンク（Eメール）
- アプリプッシュ

同期パスキー

スマートフォンやPCにインストールされたパスワードマネージャーを利用した認証方式。
ドメインと紐づけて登録・利用されることで強力なフィッシング耐性を持ち、
クラウド同期やバックアップが可能で、端末紛失時の復旧や機種変更時の移行が可能です。

同期パスキーの概要

ユーザーの操作

事前登録時

利用中のスマホやPCに、
生体情報やPIN等を設定

生体情報やPIN等を利用して
同期パスキーを作成

認証時

生体情報やPIN等による認証※

基本情報

パスワード リスト型攻撃	◎ 耐性あり
フィッシング	◎ 耐性あり
物理的な盗難 ・複製耐性	○ 盗難時もPINや生体が必要 鍵の共有やクラウド同期は可能
消費者側の コスト	◎ 特になし （スマホやPCの所有は前提）

主な特徴

1. リスト型攻撃やフィッシングに対応可能
2. スマホに格納したパスキーをPCでも利用可能（Hybrid方式）
3. クラウド同期やバックアップが可能で、端末紛失時の復旧や機種変更時の移行が可能
4. 比較的新しい認証手法で、ユーザの利用する端末や環境によって正常に動作しない場合がある点に留意

メリット・デメリット

メリット

- ユーザが持つ端末と第2要素の併用により、強固な認証を導入可能
- 普段利用するデバイスのロック解除用の生体認証やPIN等を利用するため、認証時のユーザーの負担は軽い
- クラウド同期やバックアップが可能で、端末紛失時の復旧や機種変更時の移行が可能

デメリット

- 事業者側が認証用サーバーを用意する必要があり、導入コストがかかる
- パスワードマネージャのアカウントへの攻撃等でパスキーが奪われるリスクがある
- ドメインの変更時には原則パスキーの再作成が必要

※ 生体認証が成功しない場合、PIN等の記憶要素を用いた認証が行われる場合がある。

セキュリティキー（デバイス固定パスキー）

セキュリティキーに生体情報やPINなどの第2要素を組み合わせた方式※1 。
同期パスキー同様、FIDO2仕様がベースになっています。
物理デバイスによる高い保証レベルを担保できる一方で、キーの入手と保有が必要です。

セキュリティキー（デバイス固定パスキー）の概要

ユーザーの操作

事前登録時

セキュリティーキーを登録

生体情報やPINを登録※1

認証時

生体情報やPIN認証※2

セキュリティーキーで認証

基本情報

パスワード リスト型攻撃	◎ 耐性あり
フィッシング	◎ 耐性あり
物理的な盗難・複製耐性	◎ 盗難時もPINや生体が必要 物理的な複製はほぼ不可能
消費者側のコスト	△ セキュリティキーのコスト

主な特徴

1. FIDO2仕様に対応した物理キーで、生体認証のためのセンサーを備える場合もある
2. 確実な所持を含む2要素認証で、最高の保証レベルの認証が可能
3. リスト型攻撃とフィッシングに対応可能

メリット・デメリット

メリット

- セキュリティキーと第2要素の併用により、強固な認証を導入可能
- セキュリティキーは、USBポートに差し込む又はNFCにかざすだけであり、認証時のユーザーの負担は軽い
- 同期パスキーと同じ仕様であり、同期パスキーがサポートされるサービスの多くはセキュリティキーも利用可能

デメリット

- 事前にセキュリティキーを入手し設定する必要があるとともに、認証時にも所持している必要がある
- 紛失時のアカウントリカバリーの対応が必要
- 事業者側が認証用サーバーを用意する必要があり、導入コストがかかる
- ドメインの変更時には原則セキュリティキーの再登録が必要

※1 生体認証やPINを登録せず、所持認証だけで利用することもある。その場合にはほかの認証方法と組み合わせることが望ましい。
※2 生体認証が成功しない場合、PIN等の記憶要素を用いた認証が行われる場合がある。

実物のマイナンバーカードの利用者証明用電子証明書

実物のマイナンバーカードの利用者証明用電子証明書を用いた方式。高い保証レベルの当人認証が可能ですが、大臣認定を受けた署名検証者とのシステム連携が必要です。

実物のマイナンバーカードの利用者証明用電子証明書の概要

ユーザーの操作

事前登録時

マイナンバーカードを発行

利用者証明用電子証明書
暗証番号(数字4桁)を入力

マイナンバーカードをかざし、
サービスに登録する

※マイナカード署名用電子証明書による身元確認を行った場合には当人認証時の事前登録操作は不要

認証時

利用者証明用電子証明書
暗証番号(数字4桁)を入力

マイナンバーカードをかざす

基本情報

パスワード リスト型攻撃	◎ 耐性あり
フィッシング	△ アプリやサービスの 実装に依存する
物理的な盗難 ・複製耐性	◎ 盗難時も暗証番号が必要 物理的な複製はほぼ不可能
消費者側の コスト	◎ 特になし

主な特徴

1. マイナンバーカードの所持と4桁の暗証番号により高い保証レベルの認証が可能
2. 事前にマイナンバーカードを取得し、利用者証明用電子証明書を発行する必要がある
3. リスト型攻撃に対応可能

メリット・デメリット

メリット

- 数字4桁の暗証番号を記憶するだけで、高い保証レベルの認証が可能
- 暗証番号がサーバに送信されないことに加え、試行回数が3回と限られているため、推測される可能性が低い
- 顔写真付き本人確認書類であるマイナンバーカードを当人認証にも用いることができ、セキュリティキー等の特別なデバイスが不要

デメリット

- マイナンバーカードを所持していないと利用できない。
- 利用者証明用電子証明書の暗証番号を記憶している必要がある
- 主務大臣の認定を受けた署名検証者とのシステム連携が必要
- マイナアプリ※1を利用の場合、QRコードによるログインはフィッシング攻撃のリスクがある
- 紛失時の再発行に1-1.5ヶ月程度要する

※1　マイナアプリとは、2026年8月25日提供開始予定の「マイナポータルアプリ」に「デジタル認証アプリ」を統合したアプリです。https://services.digital.go.jp/mynaapp/

スマートフォンのマイナンバーカードの利用者証明用電子証明書

スマートフォンに格納されたマイナンバーカードの利用者証明用電子証明書を用いた方式。
高い保証レベルの当人認証が可能ですが、事前にスマホへの登録が必要です。
また、大臣認定を受けた署名検証者とのシステム連携が必要です。

スマートフォンのマイナンバーカードの利用者証明用電子証明書の概要

ユーザーの操作

事前登録時

実物のマイナンバーカードを利用してスマホ用電子証明書を発行

発行時に登録した生体認証や暗証番号を入力し、サービスに登録する

※マイナカード署名用電子証明書による身元確認を行った場合には当人認証時の事前登録操作は不要

認証時

発行時に登録した生体認証や暗証番号を入力する

基本情報

パスワードリスト型攻撃	◎ 耐性あり
フィッシング	△ アプリやサービスの実装に依存する
物理的な盗難・複製耐性	◎ 盗難時も暗証 or 生体が必要 物理的な複製はほぼ不可能
消費者側のコスト	△ 対応するスマートフォンの所有が必要

主な特徴

1. スマートフォンに格納された電子証明書と生体認証 または 4桁の暗証番号により高い保証レベルの認証が可能
2. 事前にマイナンバーカードを取得し、利用者証明用電子証明書を発行する必要がある
3. リスト型攻撃に対応可能

メリット・デメリット

メリット

- スマートフォンのみを利用して、高い保証レベルの認証が可能
- 暗証番号の試行回数が3回と限られているため、推測される可能性が低い
- 実物のマイナンバーカードと異なり、生体認証が利用可能な場合がある

デメリット

- 事前にスマホへの登録作業を終えておく必要がある
- 対応しているスマホをユーザーが所有していない可能性がある
- 機種変更時に再登録が必要である
- 主務大臣の認定を受けた署名検証者とのシステム連携が必要
- 実物のマイナカード紛失時に同時に失効し、再発行に1-1.5ヶ月程度要する

パスワード

リスト型攻撃やフィッシング攻撃に対応できないため、特に単体としての利用は極力避けることが望まれます。

パスワードの概要

ユーザーの操作

事前登録時

パスワードを登録

認証時

パスワードを入力

脅威への耐性

パスワードリスト型攻撃	×
フィッシング	×
物理的な盗難・複製耐性	△ 紙に書かない限りは安全だが、現実的に覚えることは困難
消費者側のコスト	◎ 特になし

主な特徴

1. 一般的なログインで用いられており、当人認証としては最も普及している
2. リスト型攻撃やフィッシングには対応できない
3. 登録されているパスワードの長さや内容等によって不正への耐性が変化する

メリット・デメリット

メリット

- 一般的な当人認証手法であり、ユーザーが慣れ親しんでいる手法
- システム導入コストやオペレーションコストが比較的安い

デメリット

- ユーザーはパスワードを記憶する必要がある。単純であったり、桁数の少ないパスワードや、複数サービスで使い回ししている状態では不正ログインのリスクが高まる
- パスワードの漏えいリスクがある
- パスワード管理などの運用が利用者のリテラシーに依存し、運営側ではコントロールできない

SMS-ワンタイムパスワード(OTP)

事前に登録した電話番号に送付されるワンタイムパスワードを利用して認証する方法です。
リスト型攻撃やリプレイ攻撃に対応できますが、フィッシング耐性は低いです。

SMS-ワンタイムパスワードの概要

手順

事前登録時

電話番号を登録

認証時

SMSで受信したワンタイムパスワードを入力

脅威への耐性

パスワードリスト型攻撃	◎ 耐性あり
フィッシング	×
物理的な盗難・複製耐性	× SIMの盗難リスクあり 物理的な複製はほぼ不可能
消費者側のコスト	○ 携帯電話契約者は利用可能

主な特徴

1. クレジットカードのオンライン決済で用いられるケースが多い
2. フィッシングには対応できない
3. ワンタイムコードなのでリプレイ攻撃に耐性がある
4. デバイス由来の耐タンパ性がある
5. 悪意者が不正な本人確認書類等を利用してSIMを再発行させる攻撃が知られている
6. 解約後一定期間経過すると、他人が同じ電話番号を利用する可能性がある

メリット・デメリット

メリット

- 一般的な当人認証手法であり、パスワード認証と合わせると消費者側に高いコストのかからない2要素認証を実現できる

デメリット

- 認証画面から1度離れてSMSの画面を確認しなければならないケースも多く、操作の手間がかかる
- 基本的には携帯電話・スマートフォンを持っている状況で認証しなければならない
- SMS送信のための事業者側のコストがかかる
- 携帯電話を解約した場合にSMSが届かなくなる
- 海外滞在中や圏外などでSMSが届かない場合がある

メール-ワンタイムパスワード（OTP）

事前に登録したメールアドレスに送付されるワンタイムパスワードを利用して認証する方法です。リスト型攻撃やリプレイ攻撃に対応できますが、フィッシング耐性は低いです。

メール-ワンタイムパスワードの概要

手順

事前登録時

メールアドレスを登録

認証時

メールで受信したワンタイムパスワードを入力

脅威への耐性

パスワードリスト型攻撃	◎ 耐性あり
フィッシング	✕ リアルタイムフィッシングの耐性なし
物理的な盗難・複製耐性	△ アカウントを登録しているデバイス次第
消費者側のコスト	◎ メールアカウントの多くは無料

主な特徴

1. クレジットカードのオンライン決済で用いられるケースが多い
2. フィッシングには対応できない
3. ワンタイムコードなのでリプレイ攻撃に耐性がある
4. メールアカウントの機能によって利便性が変化する

メリット・デメリット

メリット

- 一般的な当人認証手法であり、パスワード認証と合わせると事業者側、消費者側双方に高いコストのかからない2要素認証を実現できる
- 導入コストやオペレーションコストが比較的安い

デメリット

- 認証画面から1度離れてメールの画面を確認しなければならないケースも多く、操作の手間がかかる
- フィルタリング機能によって不通のリスクがある
- メールアカウントへの攻撃等でワンタイムパスワードが奪われるリスクがある
- ユーザが携帯電話のキャリアメールを利用している場合、MNPや解約によりメールが届かなくなる場合がある

マジックリンク(Eメール)

事前に登録したメールアドレスに通知される一時的に有効なログインリンクによる認証方法です。送信コストが安価な認証方式で、フィッシング攻撃にも一定の効果があります。

マジックリンク（Eメール）の概要

手順

事前登録時

メールアドレスを登録

認証時

メールで受信した一時的に有効なURL（ログインリンク）を押下

脅威への耐性

パスワードリスト型攻撃	◎ 耐性あり
フィッシング	△　URL転送に脆弱
物理的な盗難・複製耐性	△　アカウントを登録しているデバイス次第
消費者側のコスト	◎　メールアカウントの多くは無料

主な特徴

1. クレジットカードのオンライン決済で用いられるケースが多い
2. フィッシングに一定の耐性があるが、メールを転送されたり、メールアカウントそのものへの攻撃には対応できない
3. ワンタイムコードなのでリプレイ攻撃に耐性がある
4. メールアカウントの機能によって利便性が変化する

メリット・デメリット

メリット

- 一般的な当人認証手法であり、パスワード認証と合わせると事業者側、消費者側双方に高いコストのかからない2要素認証を実現できる
- 導入コストやオペレーションコストが比較的安い

デメリット

- 認証画面から1度離れてメールを開く必要があるため、操作の手間がかかる
- フィルタリング機能によって不通のリスクがある
- メールアカウントへの攻撃等でマジックリンクが奪われるリスクがある
- ユーザが携帯電話のキャリアメールを利用している場合、MNPや解約によりメールが届かなくなる場合がある

アプリプッシュ

事前に登録したアプリケーションから通知される認証要求に応じてユーザーが応答する認証方法です。送信コストがかからない認証方式であるため、現在多くの場面で利用されています

アプリプッシュの概要

手順

事前登録時

事業者の指定するアプリをインストール

アプリ上でアカウントをセットアップ

認証時

アプリから通知される要求に応じて対応
例: 表示されている数字を入力する、表示された数字を選択する、ボタンを押し認証を許可するなど

脅威への耐性

パスワードリスト型攻撃	◎ 耐性あり
フィッシング	✕ リアルタイムフィッシングの耐性なし
物理的な盗難・複製耐性	△　アカウントを登録しているデバイス次第
消費者側のコスト	◎ 特になし（スマホの所有は前提）

主な特徴

1. アプリからの通知に応じて対応すれば良く、ユーザーが逐一アプリを立ち上げる必要がない
2. リプレイ攻撃に耐性がある
3. フィッシングには対応できない
4. アプリの通知を許可しない場合、使用できない場合がある
5. 攻撃者の認証試行により大量の通知を表示させ誤認証させる疲労攻撃のリスクがある

メリット・デメリット

メリット

- 一般的な当人認証手法であり、パスワード認証と合わせると消費者側に高いコストのかからない多要素認証を実現できる
- 意図しない認証試行を即座にユーザーが把握できる

デメリット

- スマホの所持が前提で、事前にアプリのインストールや設定を行っておく必要がある
- 通知設定をOFFにしている場合は使用できない場合がある
- 端末紛失、初期化が発生した場合に初回登録と同様の作業が必要となる

補足編

フィッシング耐性のある多要素認証に関する課題認識

NIST SP800-63-4※1やデジタル庁の「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※2」、フィッシング対策協議会の「フィッシング対策ガイドライン 2026年度版※3」、金融庁の監督指針・事務ガイドライン※4では、フィッシング耐性のある多要素認証を対応すべきリスクに応じて導入することを求められています。

防御の観点からは、フィッシング耐性のある多要素認証を全面的に導入し、必須化することが最も望ましいアプローチです。しかし、実際はユーザーが必要な対応機器を所有していないといった環境依存や、対応機器の紛失等におけるアカウントリカバリーの課題が生じます。そのため、フィッシング耐性のある多要素認証を全面的に提供するまでに、アクセシビリティの観点から「代替的な多要素認証」を併せて提供することが求められます。

「フィッシング耐性のあり・なし」の二元化ではフィッシング耐性のない代替的な多要素認証においても、「想定しうるリアルタイムフィッシング攻撃の特性に対して、それぞれの認証方式がどこまで有効か」を可視化し、代替策を検討することで、リスクを削減できる可能性があります。

本補足編では、リアルタイムフィッシングで取得されうる情報を整理し、リアルタイムフィッシングの攻撃を類型化して、各認証方式における評価をしています。

※1 NIST SP800-63-4：https://pages.nist.gov/800-63-4/
※2 デジタル庁 「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」：https://www.digital.go.jp/resources/standard_guidelines#ds511
※3 フィッシング対策協議会「フィッシング対策ガイドライン 2026年度版」：https://www.antiphishing.jp/report/guideline/antiphishing_guideline2026.html
※4 金融庁 総合的な監督指針・事務ガイドライン：https://www.fsa.go.jp/common/law/guide.html , https://www.fsa.go.jp/common/law/guide/kaisya/index.html

リアルタイムフィッシングで取得されうる情報の整理とリスク

リアルタイムフィッシングで攻撃者がリアルタイムに詐取する情報を、その「取得されうる情報」と「攻撃内容」によって大きく4つに分類しました。攻撃者は詐取した情報を１つの不正アクセスの目的だけで利用するのではなく、決済情報や個人情報を同時に取得し、継続的にかつ複合的に攻撃を行うことがあります。

	静的クレデンシャル情報	動的クレデンシャル情報	決済・クレカ情報	個人情報
取得されうる情報	ユーザーが能動的に変更しない限り、永続的に使い回せる情報 例：ID、パスワード、暗証番号（PIN）など	数分で失効する情報 例：SMSやメールに届く英数字のワンタイムパスワード（OTP）、認証アプリの6桁コードなど	不正決済をその場で完了させるための情報 例：クレジットカード番号、有効期限、CVV（セキュリティコード）、およびEMV 3-Dセキュアの OTP	偽サイト上で同時に収集される情報 例：被害者の氏名、生年月日、自宅住所、携帯電話番号など
攻撃内容	攻撃者は被害者が偽画面に入力した場合、正規サイトへのログインを試みる	攻撃者は被害者が偽画面に入力した場合、正規サイトへほぼ同時に入力を行う。既存の多要素認証が設定されているアカウントであっても、ログインを乗っ取られる	攻撃者は偽画面でカード情報を盗むと同時に、裏で本物のECサイト等に高額商品の決済を要求し、3Dセキュアの OTPをリアルタイムに偽画面へ投影してユーザーに入力させ、即時不正決済を成立させる	攻撃者は、個人情報を悪用し、「他のサービスへの不正アクセス」に流用する。また、「アカウントリカバリ（パスワード・認証器の再設定）プロセスの偽装」に悪用できる

リアルタイムフィッシングの攻撃類型（代表的なパターン）

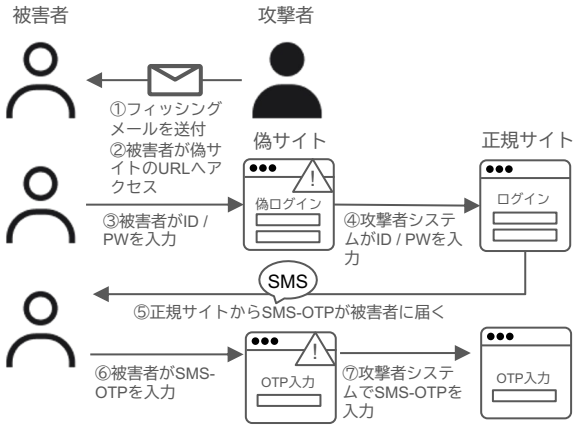
リアルタイムフィッシングの攻撃手口を、攻撃者によるシステム的・運用的な行為を軸に代表的なパターンを3つに分類しました

※各パターン図内の数字は、共通の攻撃・行動フェーズを対応させています

パターン1

入力フォームの用意

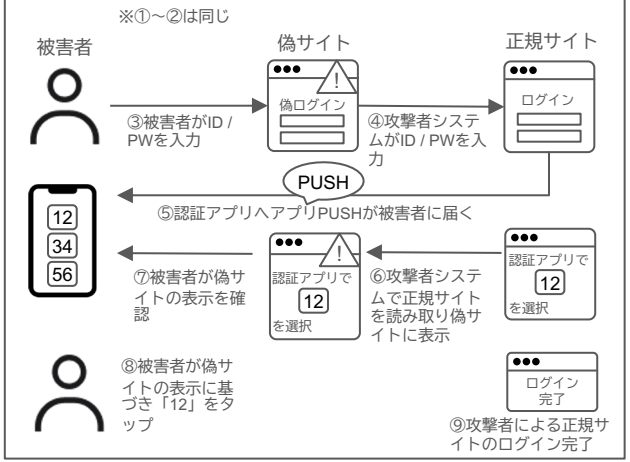
正規サイトを装った入力画面をあらかじめ用意しておき、被害者が自ら入力した情報を収集・中継する手口



パターン2

取得した情報を偽サイト上に反映

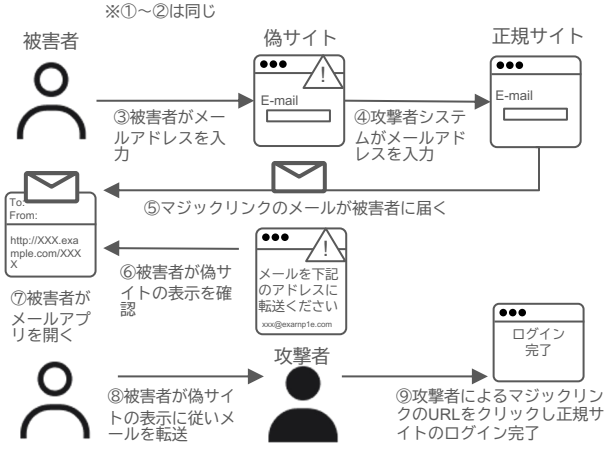
正規サイトが生成した動的クレデンシャル情報（画像、コード等）を、攻撃者が裏側（プロキシサーバ等）でリアルタイムに取得し、それを偽サイトの画面上へ表示する手口



パターン3

パターン1・2に加えて、被害者の誘導

パターン１・２に加え、被害者を一度別のサービス（メールアプリ等）へ移動させ、URLをコピーさせたり、メールを攻撃者のアドレスに転送させるなど、被害者の行動を誘導する手口



リアルタイムフィッシングの攻撃類型

［パターン1］入力フォームの表示

正規サイトを装った入力画面をあらかじめ用意しておき、被害者が自ら入力した情報を収集・中継する手口です。

1）静的クレデンシャル情報の詐取

- **概要：** IDやパスワードなど、静的クレデンシャル情報を標的とした手口
- **フロー：** 被害者を偽サイトへ誘導し、ID・パスワードを入力させます。攻撃者システムが検知し、正規サイトへのログインを試みる。後日の悪用だけでなく、アカウントロック等の先手を打つためにリアルタイムに攻撃される可能性がある。

2）動的クレデンシャル情報の詐取

- **概要：** SMS・メール・認証アプリなどに届く「英数字6桁」などのOTPを詐取する手口
- **フロー：** 被害者を偽サイトに誘導し、ID・パスワードを入力させると、攻撃者システムが検知し、正規サイトへログインを試み、正規サイトから被害者の端末にOTPを発行される。偽サイトはリアルタイムに「偽のOTP入力画面」へ切り替わり、被害者が入力したOTPを有効期限（数分）以内に正規サイトへ流し込んで突破する。

リアルタイムフィッシングの攻撃類型

［パターン2］攻撃者が取得した情報を偽サイト上に反映 (1 / 2)

正規サイトが生成した動的クレデンシャル情報（画像、コード等）を、攻撃者が裏側（プロキシサーバ等）でリアルタイムに取得し、それを偽サイトの画面上へコピーしたりミラーリングしなければ成立しない手口です。

1）SMS-OTP(絵文字)詐取

- **概要：** 「絵文字マッチング方式」などの選択式OTPを標的とし、攻撃者がプロキシサーバ等を用いて「画面の選択肢ごとリアルタイムに複製」して突破を試みる手口
- **フロー：** 攻撃者は、正規サイトが生成した「絵文字の選択肢（グリッドやボタンの配置データ）」を、偽サイト側へミラーリングして表示する。被害者が端末に通知された絵文字を偽画面上でタップすると、その「選択の座標やボタンID」が正規サイトへ中継され、キーボード入力がない認証であっても突破される。

2）アプリプッシュのナンバーマッチング攻撃

- **概要：** 認証アプリで採用されている「ブラウザに表示された2桁の数字を、スマホアプリ側でタップさせる方式」を標的にした手口
- **フロー：** 攻撃者が裏で正規サイトにログインを試みた際、正規サイトの画面に表示された「2桁の数字」を、偽サイトの画面へリアルタイムにミラーリングして表示する。被害者は自分のスマホアプリに表示された数字をタップしてしまい、攻撃者のログインを承認する

リアルタイムフィッシングの攻撃類型

［パターン2］攻撃者が取得した情報を偽サイト上に反映 （ 2 / 2)

3）動的電話番号詐取

- **概要：** 画面に表示された「特定の電話番号」へ被害者から電話をかけさせ認証する「電話発信認証」の隙を突く手口
- **フロー：** 攻撃者が裏で正規サイトにアクセスした際に画面に表示される「認証用電話番号」を、偽サイト側にそのままミラーリングする。被害者は偽画面の指示に従い、自身の登録電話番号からその番号へ発信し、結果として攻撃者のブラウザ側の認証を成立させる。

4）QRコード詐取(QRコードジャッキング)

- **概要：** PC画面のQRコードをスマホアプリでスキャンしてログインする機能を悪用し、ログイン用セッションが紐づいたQRコードをリアルタイムに横取りする手口（QRコードジャッキング）
- **フロー：** 攻撃者が手元の端末で正規サイトの「QRコードログイン画面」を開き、本物のQRコードを発行させる。そのコードは数分での失効されるので、それを防ぐために常に最新のQRコードを取得する。フィッシングメールにて被害者が偽サイトのURLをクリックすると偽サイト上にQRコードが表示される。被害者がスマホアプリでそのQRコードをスキャンした場合、攻撃者の端末側でログインが完了する。

リアルタイムフィッシングの攻撃類型

［パターン3］パターン1・2に加え被害者の誘導

パターン１・２に加え、被害者を別のサービス（メールアプリ等）へ移動させ、URLをコピーさせたり、メールを攻撃者のアドレスに転送させるなど、被害者の行動を誘導する手口です。

1）クリック元セッション移行型（マジックリンク）

- **概要：** マジックリンクのメールのURLをクリックしない限りログインできないという制約を、URLの「コピペさせること」や「メール転送させる」ことで迂回する手口
- **フロー：**攻撃者が、偽サイト内のフォームに被害者のメールアドレスを入力させる。攻撃者のサーバーが、即座に正規サイトへログイン要求を送り、被害者は正規のマジックリンク（ログインURL）を受信する。偽サイトには「大変申し訳ございません。ログインにおいて、問題が発生致しました。すぐに調査に入らせていただきますので、お客様のメールアドレスに送信されたメッセージを、こちらのメールアドレス（攻撃者のアドレス）に転送して頂きますようお願い致します」などと表示し、被害者がメールを転送する。攻撃者自身の端末ブラウザでそのURLを開くことで、被害者のアカウントでログインする。

当人認証手法別のフィッシング耐性評価マトリックス

一般的に使われる当人認証手法をリアルタイムフィッシングの攻撃類型に耐性があるのかを評価しました。
・同期パスキー・セキュリティキーは、ドメインと紐づけされ異なるドメインで認証できないため、すべてのパターンで ○としました。
・実物/スマホの利用者証明用電子証明書は、適切に実装することでフィッシングへの耐性があるため、同様にすべて ○ としました。
・パスワード、SMS-OTP(英数字)は、すべてのパターンでフィッシング耐性がないため、 ✕ としました。
・SMS-OTP(絵文字)やアプリプッシュは、パターン1は耐性があるが、パターン2はミラーリングすると攻撃可能のため、✕ としました。
・マジックリンクで、パターン1はメールに届いたURLを偽サイトにコピーさせる手法があり得るため、△ としました。
パターン2では、通知されるメールをミラーリングすることはできないため、○としました。

本表は、一般的な実装をもとに評価しており、各社の実装によってはリスクを軽減できる場合があります。

	同期 パスキー	セキュリティキー	実物マイナ 利用者証明	スマホマイナ 利用者証明	パスワード	SMS-OTP (英数字)	SMS-OTP (絵文字)	アプリ プッシュ	マジック リンク
パターン1	○	○	○	○	✕	✕	○	○	△
パターン2	○	○	○※1	○	✕	✕	✕	✕	○
パターン3	○	○	○	○	✕	✕	✕	✕	✕

※1 PCに表示されたQRコードをマイナアプリで読み取りログインに利用する場合、QRコードジャッキングにて攻撃できるリスクがあります。
マイナアプリとは、2026年8月25日提供開始予定の「マイナポータルアプリ」に「デジタル認証アプリ」を統合したアプリです。https://services.digital.go.jp/mynaapp/

出典：KYC WGグループにて作成　○：攻撃の類型に対して耐性あり　△：実装などで効果が変動　✕：耐性なし

参考）その他、留意が必要な攻撃手法

一般的なフィッシング攻撃の他にも、当人認証手法のみで防ぎきれないセキュリティ上の考慮事項があります。下記の代表的な攻撃についても対策を考慮する必要があります。

電話発信誘導（ボイスフィッシングの一種）

- 被害者がブラウザを利用中、突然「システムに重大なウイルスが検出されました」等の偽の警告やポップアップと、サポート窓口を装った電話番号が表示される。被害者が表示された番号へ直接発信し、応答したオペレーター（攻撃者）に言われるがまま遠隔操作ソフトをインストールさせられたり、認証情報を直接話したり、プリペイドカードを購入させられるなどで資産を詐取される。

正規機能（送金・決済リンク）への直接誘導

- 攻撃者が「保険料・税金の未納」等の文面と送金用リンクが添付されたメールを送信する。被害者が添付リンクをクリックすると、被害者のスマホ端末内の正規の決済アプリが直接起動し、攻撃者への個人間送金画面が正規に表示される。被害者が「保険料・税金の支払い」であると誤認したまま、自身の操作で送金・承認ボタンをタップし、被害を受ける。

マルウェアのインストールを誘導

- SMS、Eメールや、Webサイト上の広告等を経由し、不在配達の確認やセキュリティ対策のために特定のソフトのインストールを誘導され、被害者が自身のスマホ端末等にマルウェアをインストールしてしまうことで、攻撃者に資産を詐取される。

フレンドリーフラウド（本人や関係者による不正アクセス・決済）

- 被害者本人の端末を利用し正規サイトにアクセスや決済したにもかかわらず、身に覚えがないと申告がされるケース。多くの場合は、アクセスしたサイトや決済した加盟店の名称が異なっていることなどの被害者自身による「記憶違い・誤認」、家族や関係者が被害者の端末を利用した「身内の利用」、サービスの利用や商品を受けとった後に代金を支払わないで済ませようとする「意図的な詐欺」などがあげられる。

執筆者等一覧

本ガイドライン（第1.3版）の執筆者一覧

執筆メンバー

所属（KYC WG参加登録順）	氏名（敬称略）
BIPROGY 株式会社	片山 澪
株式会社 Liquid	渡邉 慶太
株式会社 Maximax	小西 優貴
株式会社 Maximax	小畑 雅人
ソフトバンク株式会社	作田 宗臣
株式会社 NTTドコモ	栗山 盛行
一般財団法人日本情報経済社会推進協会	東條 雅史
KDDI株式会社	小岩井 航介
KDDI株式会社	亀山 和真
株式会社メルカリ	狩野 達也
株式会社メルカリ	合路 健人
株式会社メルカリ	三澤 悠介
デロイトトーマツサイバー合同会社	宮崎 貴暉
伊藤忠テクノソリューションズ株式会社	岡本 俊一
FIDOアライアンス / 株式会社 NTTドコモ	森山 光一
デジタル庁	山田 達司
デジタル庁	前川 沙美
楽天グループ株式会社	中井 慎
楽天グループ株式会社	房安 央樹
PwC コンサルティング合同会社	島﨑 岳歩
PwC コンサルティング合同会社	池上 裕二
株式会社オプティム	菊池 佑
日本ヒューレット・パッカード合同会社	田中 孝明
TOPPAN株式会社	後藤 聡

オブザーバー

所属（50音順）	氏名（敬称略）
一般社団法人OpenIDファウンデーション・ジャパン	富士榮 尚寛
関原法律事務所	関原 秀行

※ 過去の版の執筆者等については、それぞれの版をご参照ください。

END