民間事業者向け
デジタル本人確認ガイドライン

第1.2版　本人確認手法編

2026年2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

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　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、25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2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」等を参照することを推奨します。

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

本人確認ガイドライン 本編

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する

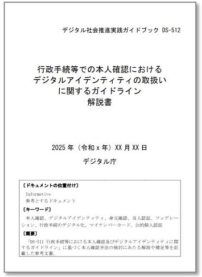
本人確認ガイドライン 解説書

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

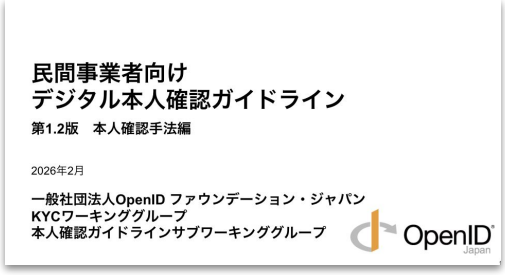
などの情報をとりまとめる

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する



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。

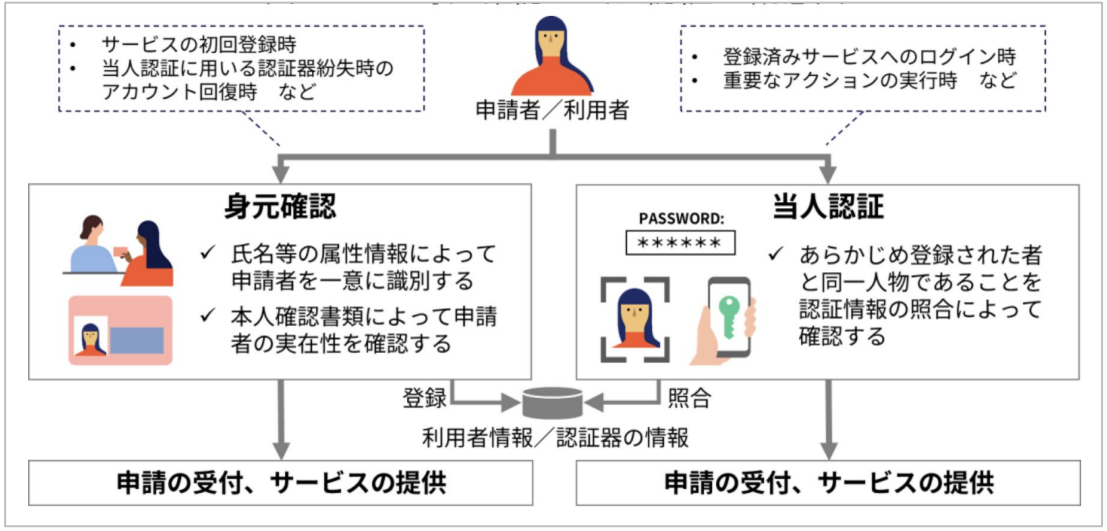
身元確認 当人認証

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

注釈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	×	申請者の検証
		ICチップの読み取り		ICチップ読み取り時のパスワード・暗証番号
		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
		書類コピーの送付（電子・物理）		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
		スマホ内に格納されたデータの取得		銀行口座情報にアクセスできることの確認
		目視確認		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
		自己申告（書類なし）		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

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）
書類そのものの提示・提出	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

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月予定
容貌確認方式（ICチップ型）	ヘ	ヘ	**ホ（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）	**ヘ(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）	**ヘ(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）**	**ヲ（変更）**	チ	チ	**ト（変更）**
民間電子証明書方式※2	ヲ	**ワ（変更）**	**ル（変更）**	チ	チ	**ト（変更）**
カード代替電磁的記録方式※3	-	**ル（新規）**	**リ（変更）**	-	**リ（新規）**	**チ（変更）**
転送不要郵便方式（ICチップ型）	チ	チ	ト	-	-	**ニ（新規）**
転送不要郵便方式（原本送付型）	チ	チ	ト	ホ	ホ	ホ
転送不要郵便方式（写し送付型）	リ	リ	**廃止**	ヘ	ヘ	**廃止**※4
特定事項伝達型本人限定郵便方式	ル	**ヲ（変更）**	**ヌ（変更）**	ト	ト	ヘ

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1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 携帯電話不正利用防止法 26年4月改正のリ方式（旧ヘ方式）は非居住者等にしか適用できないため廃止と表現した

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）

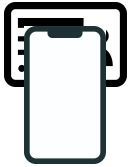
ICチップの読み取り

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、もしくはカードの撮影によりカードに記載された番号を取得 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
1. 在留カード、特別永住者証明書
   カード番号（11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
1. パスポート
   パスポート番号
   ※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月に非対面での身元確認には今後利用できなくなります。

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（※要確認）

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

- 犯収法・携帯電話不正利用防止等を満たした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/OCRによる自動化は進んでいる。しかし、犯収法・携帯電話不正利用防止法等を満たす場合は目視確認が必要で、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月に非対面での身元確認には今後利用できなくなります。

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）マイナポータルアプリが立ち上がり、スマホ用電子証明書の読み取り
3）パスワードの入力

ユーザ体験

- マイナポータルアプリで「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

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

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

書類の種類

スマートフォンのマイナンバーカード

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

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

申請者の検証手法の解説

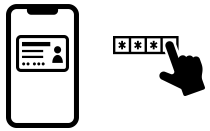
- ICチップ読み取り時のパスワード・暗証番号
- 書類の顔画像と申請者の顔写真の比較
- スマホ内のデータ取得時のパスワード、暗証番号や生体認証
- 銀行口座情報にアクセスできることの確認
- 銀行口座（オンラインバンキング）にログインできることの確認
- 配達員の目視
- 郵送
- チェックなし

ICチップ読み取り時のパスワード・暗証番号

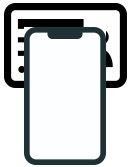
本人確認書類のICチップを読み取る際に、ユーザにパスワードや暗証番号といった、ユーザ本人しか知り得ない情報を入力することで、書類に記載の当人であることを確認します。

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（8桁）

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
2）店員による券面の顔画像の目視確認

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/OCRによる自動化は進んでいる。しかし、犯収法・携帯電話不正利用防止法等を満たす場合は目視確認が必要で、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
- 店員の目視誤り: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

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住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

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

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

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

書類の種類

銀行口座

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

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

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

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	要注意※	要注意※
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ヶ月程度要する

注釈1：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URLを送信し、受信した端末でそのURLを開くと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※	所持※	所持※
	フィッシング耐性	なし	なし	なし	一定程度あり	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

注釈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
注釈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。
登録したドメイン以外での利用はブラウザが拒否するため、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。
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

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、マイナンバーカードを所持していないと利用できません。

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
- QRコードによるログインを許容している場合、フィッシング攻撃のリスクがある
- 紛失時の再発行に1ヶ月程度要する

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、事前の登録をしていないと利用できません。

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
- QRコードによるログインを許容している場合、フィッシング攻撃のリスクがある
- 実物のマイナカード紛失時に同時に失効し、再発行に1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
- 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

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	×
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
1. フィッシングには対応できない
1. ワンタイムコードなのでリプレイ攻撃に耐性がある
1. 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
- 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
- メールアカウントの流出はそのままワンタイムパスワードの流出を意味する
- 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。送信コストがかからない認証方式で、フィッシング攻撃にも一定の耐性があるため、多くの場面で利用されています。

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
- 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
- メールアカウントの流出はそのままワンタイムパスワードの流出を意味する
- 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	×
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

- 事前にアプリのインストールや設定を行う必要がある
- 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

執筆者等一覧

本ガイドラインの執筆者一覧

執筆メンバー

所属（KYC WG参加登録順）	氏名（敬称略）
有限会社ラング・エッジ	宮地 直人
一般財団法人日本情報経済社会推進協会	東條 雅史
一般財団法人日本情報経済社会推進協会	曾我部 倭玄
ソフトバンク株式会社	作田 宗臣
TOPPANエッジ株式会社	後藤 聡
TOPPANエッジ株式会社	本多 英明
伊藤忠テクノソリューションズ株式会社	岡本 俊一
伊藤忠テクノソリューションズ株式会社	貞弘 崇行
株式会社オプティム	菊池 佑
株式会社ジェーシービー	南井 亨
デロイトトーマツサイバー合同会社	櫻田 仁詩
デロイトトーマツサイバー合同会社	小林 真弘
デロイトトーマツサイバー合同会社	宮崎 貴暉
KDDI株式会社	小岩井 航介
KDDI株式会社	小畑 雅人
株式会社メルカリ	狩野 達也
株式会社NTTドコモ	栗山 盛行
株式会社NTTドコモ	菊池 裕次郎
株式会社NTTドコモ	佐藤 拓実
Okta Japan株式会社	板倉 景子
ポケットサイン株式会社	関 響
デジタル庁	山田 達司

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

END