マイナンバーカードの普及・利用に関する
お役立ち情報をお届け

マイナンバーカード・インフォ
（民間事業者向け）
vol.12

○民間事業者の取組紹介

TRUSTDOCK「民間事業者向けデジタル本人確認ガイドライン概要」について

デジタル庁国民向けサービスＧ
マイナンバーカード担当
令和５年６月 16 日

○ **民間事業者の取組紹介**

・TRUSTDOCK「民間事業者向けデジタル本人確認ガイドライン概要」について

TRUSTDOCK が提供※する「民間事業者向けデジタル本人確認ガイドライン概要」についてご紹介します。詳細につきましては、次ページ以降の別添をご覧いただきますようお願いいたします。

※本年 3 月に OpenID ファウンデーション・ジャパンが公表した「民間事業者向けデジタル本人確認ガイドライン」から抜粋し、TRUSTDOCK が再構成した資料となります。

□　別添 1　【TRUSTDOCK】民間事業者向けデジタル本人確認ガイドライン概要

マイナンバーカード･インフォでは､国の施策や民間事業者の事例紹介など､マイナンバーカードの利用促進に関するお役立ち情報をお届けしております。

デジタル庁のマイナンバーカード制度ページで紹介しておりますので､是非､マイナンバーカードの利用検討にお役立てください。

□　マイナンバー（個人番号）制度　民間事業者向けお役立ち情報ページ

https://www.digital.go.jp/policies/mynumber/private-business/?mnci=pr12-1

以　上

別添1

J-Startup

民間事業者向け
デジタル本人確認ガイドライン
概要

2023年3月20日

株式会社TRUSTDOCK
Public Affairs室

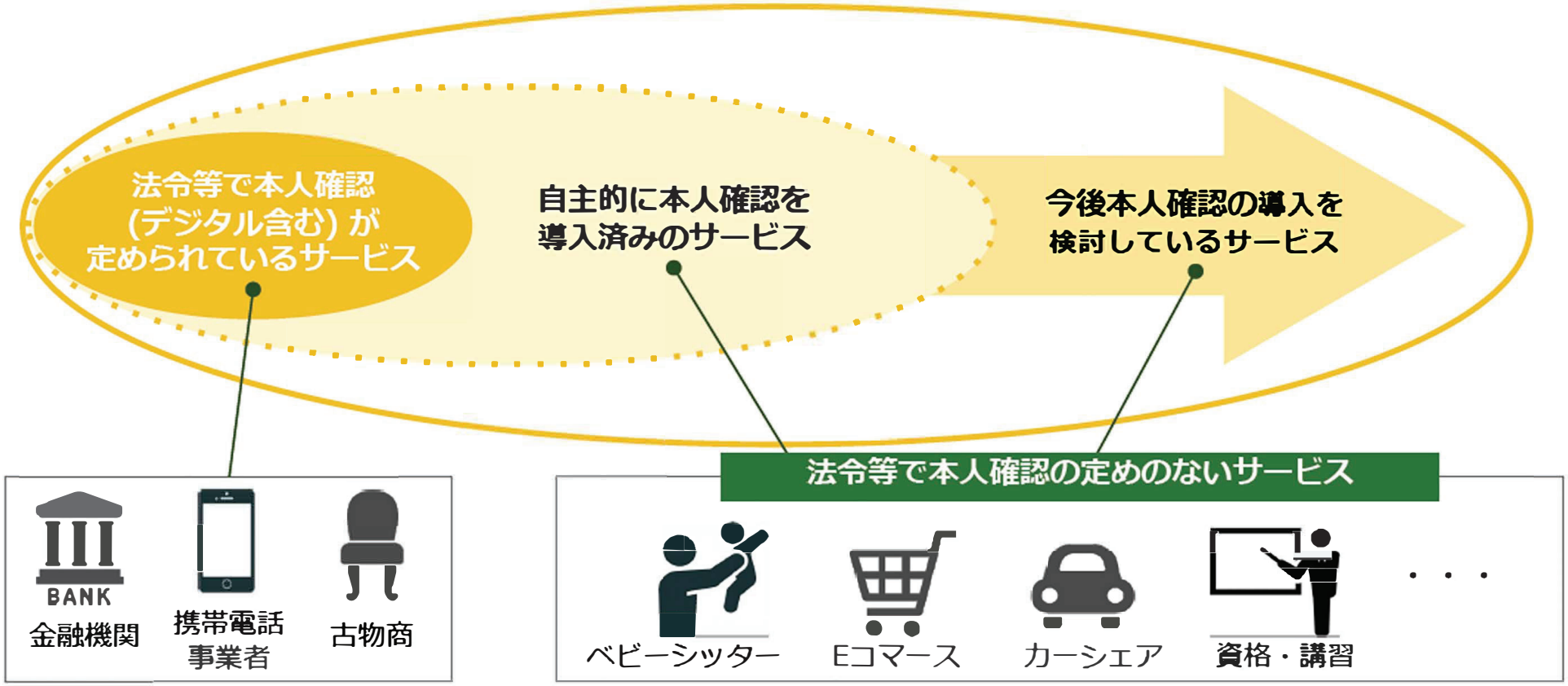
本概要は、OpenIDファウンデーション・ジャパン
「民間事業者向けデジタル本人確認ガイドライン」から
抜粋し、株式会社TRUSTDOCKが再構成したものです

目次

TRUSTDOCK

近年、オンラインサービスの普及により、法令等で本人確認が定められていない幅広いサービスにおいて、デジタル技術を活用した本人確認が自主的に導入されています。

法令等で本人確認が定められていないサービスにおける本人確認の拡大（イメージ）



TRUSTDOCK

法令等で本人確認の定めのないサービスを提供している事業者は、対応すべき本人確認手法が明確ではないため、リスクと比較して厳格な本人確認手法を選択する等の過剰対応や、本人確認の導入を断念することによる不正リスク増大の懸念があります。

本人確認の指針の不在による懸念点

行政機関

デジタル手続法等
の法令

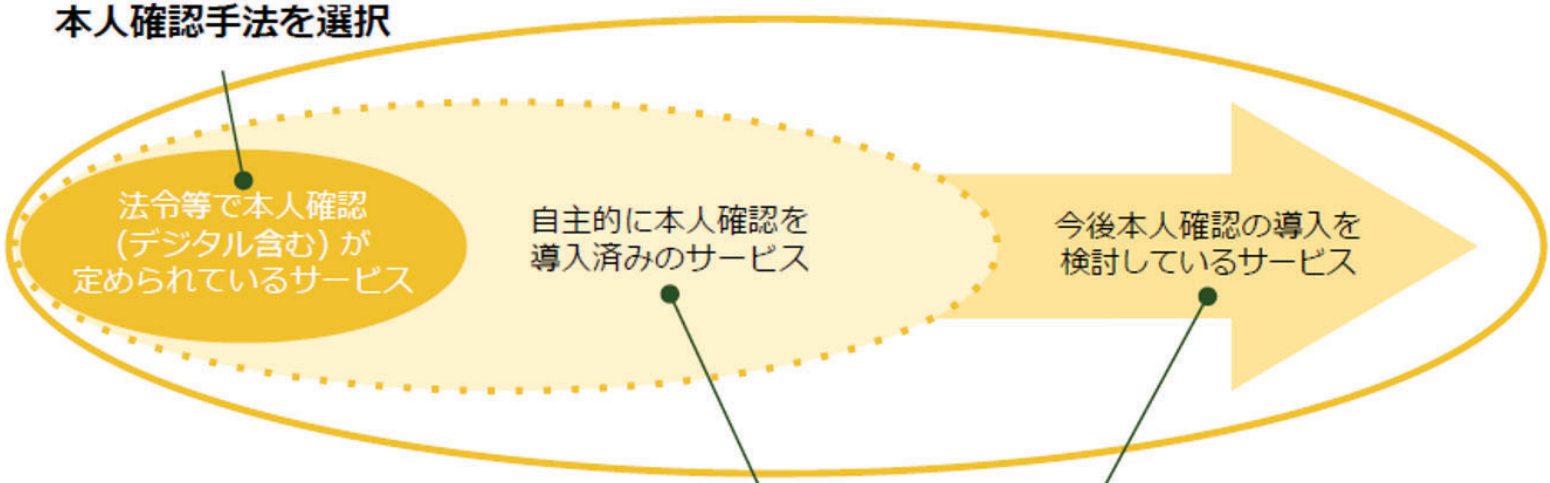
＋

行政手続における
オンラインによる
本人確認の手法に関する
ガイドライン

本人確認について
一定の指針が存在

民間事業者

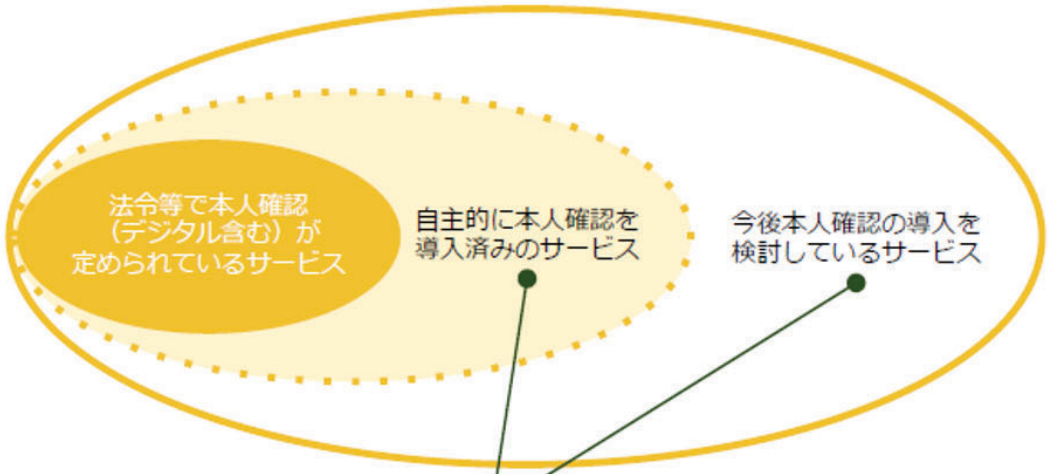
法令等で義務付けられた
本人確認手法を選択



本人確認に関する指針がないため、自社サービスに適した本人確認手法がわからない
①金融機関等と同等の本人確認手法を導入（＝過剰対応）
②本人確認の導入を断念（＝不正リスク増大）

本ガイドラインは、法令等で本人確認の定めのないサービスを提供している事業者が、自社サービスに応じた本人確認（手法）を選択するために活用することを主な目的としています。

対象*



**法令等で本人確認の定めのない
サービス提供事業者を対象**

内容及び目的

OpenID

民間事業者向けデジタル本人確認ガイドラインの主な内容

- 本人確認の導入・選択に必要な基礎知識のまとめ
- 本人確認手法の特徴の整理
- マイナンバーカードや本人確認を巡る最新動向の紹介

**自社サービスに応じた本人確認（手法）を
選択するためのガイドブックとしての活用を想定**

本ガイドラインは何らかの規制を設けるものではありません

注釈：行政機関（地方公共団体を含む）においても、行政分野の各種法令やガイドラインにおいて網羅されていない内容の補完的な文献として役立てるために活用されることが期待されます。

OpenIDファウンデーション・ジャパン　本人確認ガイドラインタスクフォース　メンバー

リーダー	株式会社TRUSTDOCK
サブリーダー	株式会社NTTドコモ
構成員（50音順）	伊藤忠テクノソリューションズ株式会社 KDDI株式会社 株式会社ジェーシービー セコム株式会社 ソフトバンク株式会社 デロイト トーマツ サイバー合同会社 トッパン・フォームズ株式会社 株式会社Liquid
オブザーバー（50音順）	渥美坂井法律事務所・外国法共同事業 プロトタイプ政策研究所 　落合孝文弁護士 一般社団法人OpenIDファウンデーション・ジャパン デジタル庁（吉田泰己、林達也、山田達司、前川沙美）

OpenIDファウンデーション・ジャパンでは、安心・安全なデジタル社会の実現を目指しており、
その取組みの一環として本ガイドラインを策定しました

目次

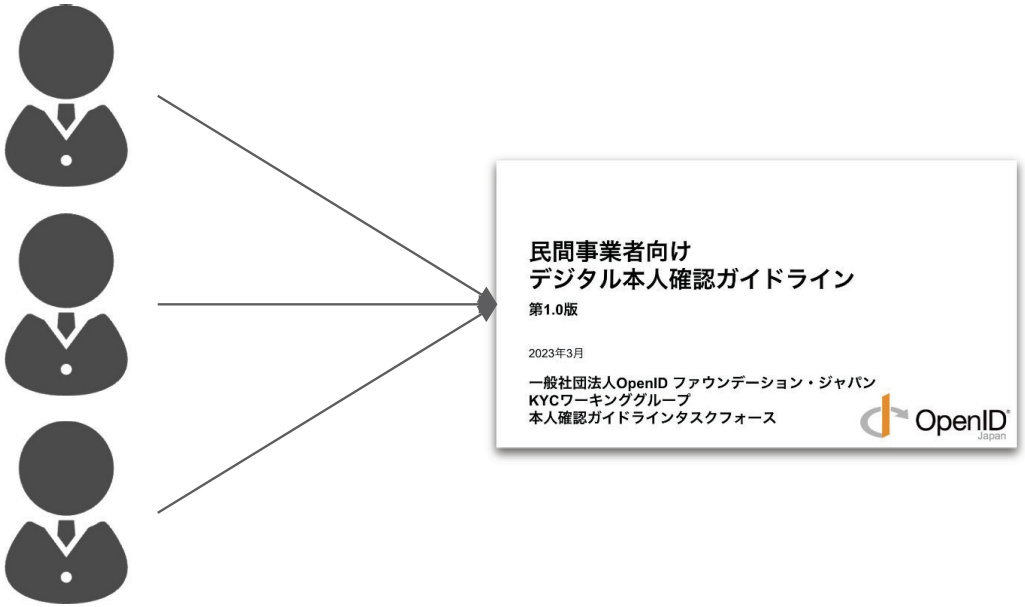
民間事業者向けデジタル本人確認ガイドラインの主な利用シーン

TRUSTDOCK

本ガイドラインは、①本人確認の導入を検討する際に事業者が直接参照する、②事業者団体等が本人確認に関わる規程（ガイドライン）等を整備する際に参考にする、の2つの利用シーンを想定して作成しています。

本ガイドラインの利用イメージ

①個々の事業者として直接参照するケース



自社で本人確認を導入する際に、具体的な本人確認の手法や特徴・留意点などを参照する

②団体として参考にするケース

事業者団体等が本人確認に関わる規程等を整備する際に、保証レベルの考え方や手法例等を参考にする

一般社団法人日本フランチャイズチェーン協会（JFA）のガイドライン策定

一般社団法人日本フランチャイズチェーン協会は、コンビニエンスストアの酒・たばこ販売時のデジタル年齢確認を推進するため、本ガイドラインを参考にした「デジタル技術を活用した酒類・たばこ年齢確認ガイドライン*」を公表しました（2023年1月）。

一般社団法人日本フランチャイズチェーン協会（JFA）ガイドラインの特徴と期待される効果

1. 求められる保証レベルが明確
2. 保証レベルに対応する手法が明確
3. 業界特有の慣習や規制を考慮

コンビニエンスストアの実体にフィットした確認手法を選択

デジタル臨時行政調査会における検討から実現したもので、今後関係省庁とも連携し、他の業界団体等で同様のガイドライン策定が広がっていくことが期待されています。

注釈：詳細は本編「【コラム】一般社団法人日本フランチャイズチェーン協会「デジタル技術を活用した酒類・たばこ年齢確認ガイドライン」の取組みについて」のこと。

TRUSTDOCK

本ガイドラインの内容も踏まえ、事業者団体等におけるガイドラインの検討・策定を支援いたします。

業界団体等における本ガイドラインの活用イメージ

一般社団法人日本フランチャイズチェーン協会
（酒類・たばこ販売時の年齢確認）

業界ガイドライン*の策定作業を支援済み

その他の業界団体等

今後ガイドライン等の検討・策定を支援

OpenIDファウンデーション・ジャパン
「民間事業者向けデジタル本人確認ガイドライン」

注釈：詳細は本編「【コラム】一般社団法人日本フランチャイズチェーン協会「デジタル技術を活用した酒類・たばこ年齢確認ガイドライン」の取組みについて」のこと。

目次

本ガイドラインの全体像

		主な内容
ガイドラインの位置付け	1. 対象・目的 11. 行政分野における本ガイドラインの活用 12. 事業者団体等における本ガイドラインの活用	● 法令等に本人確認の定めの無い事業者を対象とし、本人確認の導入を検討したい民間事業者が利用することを目的に作成。 ● また、手法の特徴等は行政分野や事業者団体等での参考となることも想定。
本人確認の基礎知識	2. 本人確認とは 3. 本人確認に関わる法令等 4. 本人確認書類	● 身元確認・当人認証の概念やそれぞれの保証レベルを中心に整理。 ● 本人確認について定められている法令について整理。 ● 公的身分証を中心とした本人確認書類の特徴について整理。
事業者が留意すべき内容	5. 事業者として留意すべきこと 6. 個人情報の取扱い	● 身元確認の導入において失敗しないための主なポイントを整理。 ● 本人確認において取扱う個人情報の留意点について整理。
本人確認手法の選択	7. ホ方式の自動化 8. 身元確認結果の活用（いわゆる“依拠”） 9. 主な身元確認手法 10. 主な当人認証手法	● 具体的な本人確認手法を選択できるよう、各手法の特徴を整理。 ● 身元確認について、安全性と利便性を兼ね備えた「中間的な手法」について紹介。
本人確認に関するトピックス	マイナンバーカードの機能のスマートフォン搭載 コラム	● マイナンバーカードの機能のスマートフォン搭載に関する政府の動向や、NIST SP 800-63-4(draft)やパスキーなど、本人確認に関するトピックスを紹介。
その他	13. 本ガイドラインの今後の更新等について 附録	● 本ガイドラインの今後の更新の考え方について記載。 ● 附録として、法令等の詳細、事業者ヒアリングの結果、保証レベルマッピング、参考文献一覧、主な用語集、執筆者一覧等を記載。

本人確認の目的の1つには、不正防止があります。具体的には、①不正の未然防止、②不正の牽制、③不正時の対応等、とサービスの各段階で不正を防止・牽制することができます。

本人確認による不正防止のポイント

本人確認を行うことで不正を防止する効果があります

不正の未然防止	不正の牽制	不正時の対応
不正行為を目的とした利用者のサービス登録・利用を防ぐ	なりすましを防止することで、不正行為を牽制する	本人確認記録を参照することで、不正者の特定や賠償請求等が可能

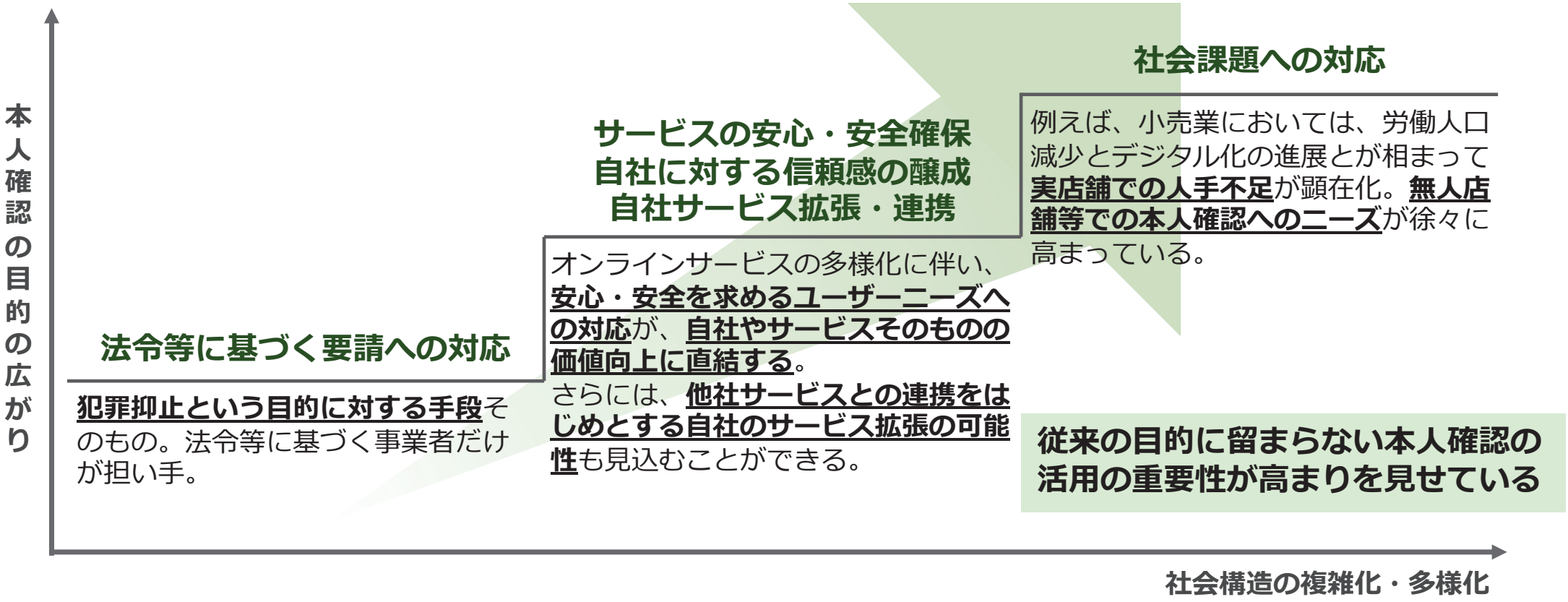
サービスの各段階での不正を防止・牽制でき、サービス全体の安全・安心に繋がる

注釈：主な不正事案は「【コラム】個人情報の漏えい事例とその要因」を参照。

TRUSTDOCK

社会の変化に伴い、 単に法令上の義務を履行するための手段に留まらず、自社やサービスのプレゼンス向上や社会課題解決のために本人確認を導入する動きが拡大しています。

社会変化と本人確認の広がりのイメージ



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*1。

「身元確認」は、本人確認書類を確認する等により、「実在性*2」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生体情報等と手続を行う際に入力されたパスワードや生体情報等を照合する等により、「当人性」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。

本人確認と身元確認・当人認証と主な特徴

本人確認

	身元確認	当人認証
確認の内容の例	● 提示された本人確認書類が偽造されていないことを確認 ● 提示された本人確認書類と申告内容を照合し、申請者に関するものであることを確認	● 取得されたパスワードや生体情報を、あらかじめ登録されているものと照合し、同一人物であることを確認
確認できること	実在性*2	当人性
実施シーンの事例	● ユーザー登録*3 ● 銀行口座の開設 ● 携帯電話の契約 ● クレジットカードの申込み	● ログイン ● スマートフォンのロック解除 ● サービス問い合わせ時の電話等での本人確認

注釈1：この整理は経済産業省「オンラインサービスにおける身元確認に関する研究会」において整理されたものであり、本ガイドラインにおいても当該整理を参照。
注釈2：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「（参考）身元確認のプロセス」を参照。）
注釈3：登録後に、取引や手続によっては改めて身元確認を求めることもある。

身元確認と当人認証の保証レベルの考え方

TRUSTDOCK

身元確認手法、当人認証手法のそれぞれに保証レベルが定義されます。また、本人確認全体の強度は、身元確認と当人認証の両者の保証レベルを踏まえることが重要です。

身元確認と当人認証の保証レベル

身元確認の保証レベル*1, 2
Identity Assurance Level（IAL）

- IAL3：対面での身元確認
- IAL2：遠隔又は対面での身元確認
- IAL1：身元確認のない自己表明

当人認証の保証レベル*1, 2
Authenticator Assurance Level（AAL）

- AAL3：複数の認証要素に加え耐タンパ性が確保されたハードウェアトークン*3
- AAL2：複数の認証要素
- AAL1：単一又は複数の認証要素

ただし、保証レベルだけでなく、具体的な脅威の特定とその脅威に対応できているかといった視点が重要

注釈1：ここでの「保証レベル」はNIST SP 800-63-3 Digital Identity Guidelinesにおいて定義されている保証レベルを参考に、各府省情報化統括責任者（CIO）連絡会議が2019年に策定した「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（以下、「行政手続ガイドライン」という。）の保証レベルを採用。「IAL」、「AAL」と表記されているものは特別な言及がない限り、この行政手続ガイドラインの保証レベルを示す。

注釈2：保証レベルを考慮する際には、身元確認の方法や当人認証の要素数だけに着目することは推奨されない。本来的には、保証レベルとして「当該保証レベルを満たすことで対応できる脅威は何か」を示すことで定義されることが望ましい。しかしながら、本ガイドラインの策定にあたっては、現時点では脅威に着目した具体的な保証レベルの整理を深めきれておらず、今後、さらなる検討が必要と考えられる。

注釈3：ここでの「耐タンパ性が確保されたハードウェアトークン」とは、暗号化・復号・署名生成のための鍵をはじめとする秘密情報や秘密情報の処理メカニズムを外部から不当に観測・改変することや秘密情報を処理するメカニズムを不当に改変することが極めて困難であるように意図して作られたハードウェアトークンのこと。

出所：内閣官房 情報通信技術（IT）総合戦略室 (2019)「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」より。

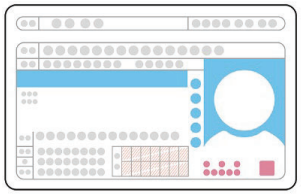
政府がデジタル社会のパスポートと位置づけているマイナンバーカードの普及が急速に進み、他の本人確認書類の機能をマイナンバーカードへ一体化する検討も進められています。

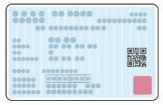
これまでは、幅広い本人確認書類が選択・使用され、中でも運転免許証が本人確認書類としての役割を中心的に担ってきました。近年、政府の推進により**健康保険証、運転免許証、在留カードの機能をマイナンバーカードへ一体化する検討も進められています。**

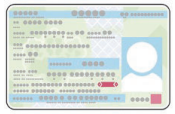
本人確認書類の変化（イメージ）

これまで

パスポート

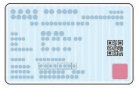

運転免許証

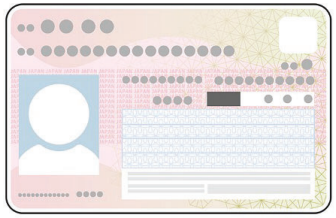

健康保険証

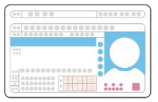

在留カード


マイナンバーカード

これから


廃止の方向





マイナンバーカードへの一体化を検討中

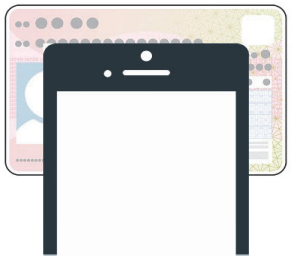
デジタル本人確認が拡大する中、スマートフォンを活用することで、本人確認書類の撮影や読み取りが不要な手法が登場してきています。

これまでのデジタル本人確認では、本人確認に必要な情報を送信するために、常に本人確認書類を所持し、その場でスマートフォン等で撮影や読み取りを行う必要がありました。本ガイドラインでは、よりユーザーの負荷が低い、スマートフォンを活用した手法もご紹介します。

これまでのデジタル本人確認とこれからのデジタル本人確認

これまでの本人確認

本人確認書類を撮影したり、かざして読み取る

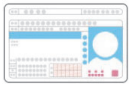


これからの本人確認

スマートフォンだけで本人確認が完結できる

顔写真付き本人確認書類は、記載事項のほか、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っており、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	 在留カード	 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*1	中長期間在留する外国人*2	日本国籍を有する者
	発行数*	約8,058万枚（2023.3.5時点累計交付枚数）	約8,190万枚（2021）	約143万枚（2021）	約2,440万枚（2021）
	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
	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
	ICチップ読取の暗証番号	4.4マイナンバーカードの概要①を参照	4桁数字①下記以外の券面 4桁数字②本籍、顔写真	在留カード番号	4.6. パスポートを参照
	マイナンバーカードとの関係	-	2024年度末までの一体化予定の前倒しを検討中	2025年度末までの一体化交付を目指す	-

***1 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チップも搭載されず。

***2 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。

注釈：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。

身元確認の導入（手法の変更も含む）に当たって必要な対応事項は、主として以下の5点が挙げられます。一部は、必要に応じて外部の事業者に委託することもでき、委託の要否も含めてリスクや全体的なコスト等を踏まえて検討することが効果的です。

主要な対応事項

	主な対応事項	主な検討の視点
導入前	1. 必要な属性の検討・身元確認手法の選択・ユーザーエクスペリエンスの設計	● 自社サービスが抱えるリスクを踏まえた手法か？ ● 当該手法が対応可能な本人確認書類の種類や提出方法等はユーザーに対して十分な選択肢を提供できているか？
導入前	2. システムの構築・改修	● システムの構築・改修のスケジュール・コスト等を踏まえ、自社開発・委託・API連携等から適切なシステム構築方法を選択したか？
導入前	3. ユーザーへの事前周知	● 身元確認の導入について、ユーザーへの周知は十分か？ ● 個人情報の取扱い等について、ユーザーに対して不安を感じさせないための施策を講じているか？
導入後	4. システム運用・セキュリティ体制の整備	● 個人情報を取り扱う上で十分な体制を整備・運用できているか？ ● 委託・API連携の場合には、委託先事業者やAPI提供事業者と連携の上、必要な体制を確保できているか？
導入後	5. 問い合わせ対応の体制整備	● セキュリティや身元確認に関する問い合わせに対し、迅速・的確に対応可能な体制を整備できているか？

外部事業者へ委託可能（API連携を含む*）

注釈：API連携の場合であっても、自社のシステムの改修、連携等については、自社で対応する必要がある。

TRUSTDOCK

中間的な手法とは、保証レベルとユーザーや事業者の負担のバランスを取った手法です。様々な手法が考えられますが、本ガイドラインでは「ホ方式の自動化」と「身元確認結果の活用」の2つを紹介しています。

中間的な手法のイメージ

中間的な手法

適度に簡易で信頼性のある手法

ホ方式の自動化

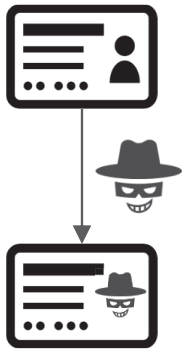
AIの活用で目視審査を省略

身元確認結果の活用

情報連携技術で本人確認書類を省略

本人確認書類の画像を送信する方式（アップロード）

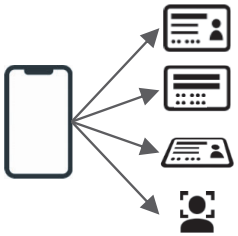
簡便だが、保証レベルは低い



画像の加工が容易

本人確認書類の表・裏・厚みと容貌を撮影する方式（犯収法ホ方式）

保証レベルは高いが、負担が大きい



撮影が多くユーザーが大変

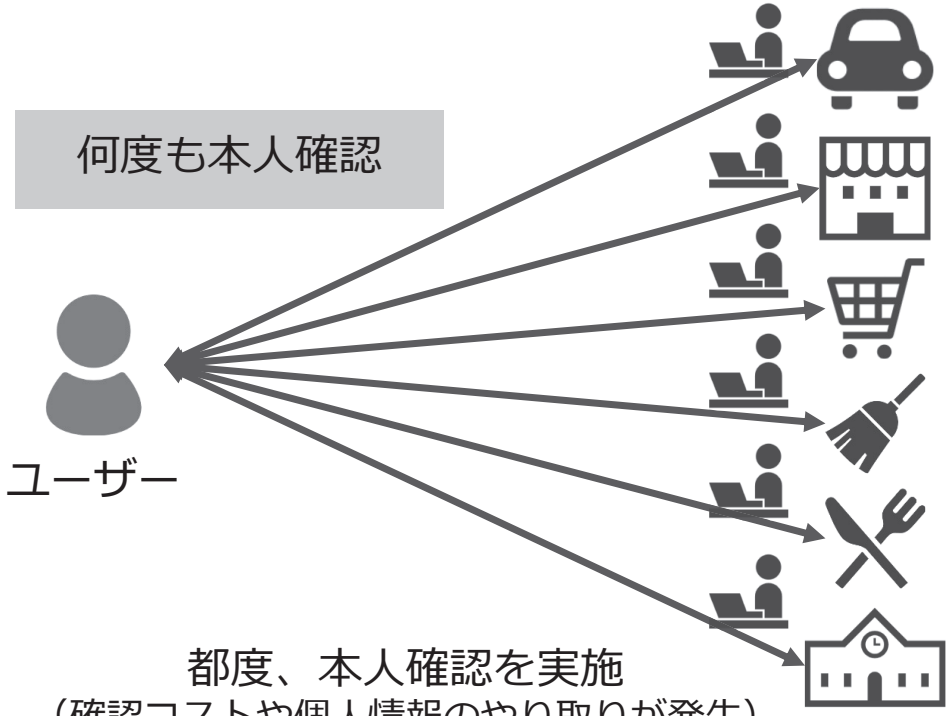
審査体制の構築・維持が大変

例えば、他社のサービス利用時に行った身元確認結果を活用することで、何度も本人確認を行う手間を省くことや必要最小限な個人情報の提供が可能になります。

デジタル社会の新しい本人確認

現状

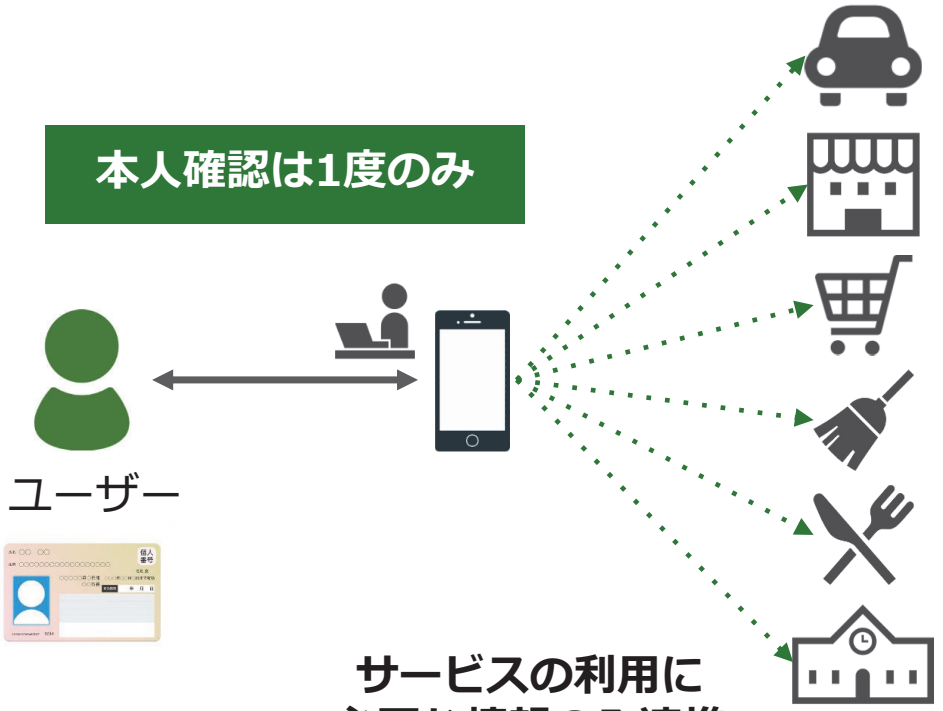
何度も本人確認



都度、本人確認を実施
（確認コストや個人情報のやり取りが発生）

新しい本人確認

本人確認は1度のみ



サービスの利用に
必要な情報のみ連携

主な身元確認手法とその特徴

TRUSTDOCK

		自己申告	アップロード	犯収法ホ方式	犯収法ヘ方式	公的個人認証 (署名用電子証明書)
手法の概要		本人確認書類に基づかない、自己申告	本人確認書類の券面画像のアップロード	顔写真付き本人確認書類の券面(裏・表・厚みその他)と容貌のリアルタイム撮影	顔写真付き本人確認書類のICチップ読み取りによる券面画像の取得と容貌のリアルタイム撮影	マイナンバーカードの署名用電子証明書により最新の氏名・住所等を取得(券面画像の取得は不要)
手法の特徴	保証レベル IAL*	IAL 1	IAL 2	IAL 2	IAL 2	IAL 3
	保証レベル DADC IAL	DADC IAL 0	DADC IAL 1	DADC IAL 3	DADC IAL 3	DADC IAL 4
	利用可能な本人確認書類	-	本人確認書類全般 (健康保険証や場合によっては学生証等も含む)	顔写真付き本人確認書類 (運転免許証、マイナンバーカード、パスポート、在留カード等が主流)	顔写真付き本人確認書類 (運転免許証、在留カードが主流)	マイナンバーカード
	暗証番号	-	不要	不要	必要	必要
	ユーザーの所要時間(目安)	-	約30秒 (本人確認書類画像を選択し、アップロードする時間)	約60秒 (本人確認書類と容貌の撮影時間)	約40秒 (暗証番号の入力・ICチップ読み取りと容貌の撮影時間)	約20秒 (暗証番号の入力とICチップ読み取り時間)
	事業者の審査時間	-	数時間～数日 (目視確認を行う場合)	数時間～数日 (法令に基づいた目視確認を行う場合)	数時間～数日 (法令に基づいた目視確認を行う場合)	即時
ユースケースの事例		ウェブサイトへのアカウント登録	ウェブサイト等での身元確認等、法令等に定めの無い身元確認	銀行口座の開設、携帯電話の登録等、法令に定めのある身元確認	銀行口座の開設、携帯電話の登録等、法令に定めのある身元確認	行政文書等の電子申請や電子申告等

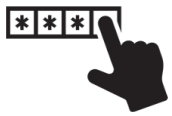
注釈：IALは「行政手続におけるオンラインによる本人確認の手法 に関するガイドライン」における保証レベル。

公的個人認証（署名用電子証明書）（＝犯収法ワ方式）

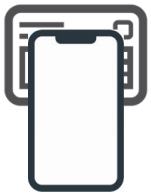
マイナンバーカードの署名用電子証明書を取得する手法。対象書類がマイナンバーカードに限られますが、ユーザーの操作時間が短い上に、偽造耐性が極めて高い特徴があります。また、電子証明書の失効情報を取得することで、最新の情報かどうかを確認することができます。

公的個人認証（署名用電子証明書）の概要

手順



署名用電子証明書暗証番号(英数字6文字以上16文字以下)を入力



マイナンバーカードをかざす

基本情報

保証レベル	• IAL 3 • DADC IAL 4
本人確認書類	マイナンバーカード

主な特徴

1. 身元確認の保証レベルが最も高い。
2. 暗証番号を入力し、カードをかざすだけで身元確認が可能となり、ユーザーの所要時間が少ない。
3. 目視確認が不要のため、本人確認のリードタイムが短い。

メリット・デメリット

メリット

- 対面相当の最高の保証レベルの身元確認が可能。
- 住基台帳に基づく氏名、住所、生年月日、性別を取得できる。
- 電子証明書の失効情報を取得できる。
- 操作に慣れれば簡便な手法。

デメリット

- マイナンバーカードを所持し、署名用電子証明書暗証番号を記憶している必要がある。
- ICチップを読み取ることができるスマートフォンやアプリ等が必要であり、NFCアンテナの位置を理解している必要がある。
- 署名検証を行うことができる事業者が限定される。

主な当人認証手法とその特徴

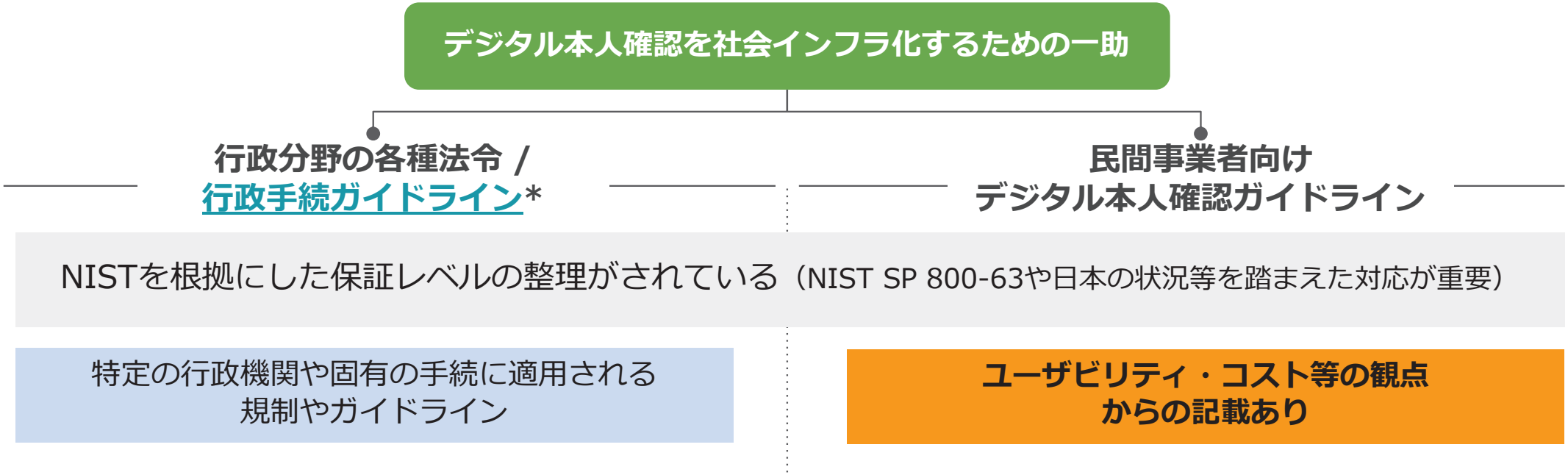
		パスワード	パスワード+OTP	パスワードレス 生体認証(FIDO認証)	セキュリティキー 認証(FIDO認証)	公的個人認証 (利用者用電子証明書)
手法の概要		パスワードの入力	パスワードの入力に加え、ワンタイムパスワードの入力又はアプリのプッシュ認証	スマートフォンアプリやブラウザを利用した生体認証(FIDO認証)	セキュリティキーに生体やパスワードなどの第2要素を組み合わせた認証(FIDO認証)	マイナンバーカードの読み取り及び利用者用証明書暗証番号 (4桁)の入力による認証
手法の特徴	認証要素	記憶	記憶 + 所持	生体*2 + 所持	生体*2+ 所持 (耐タンパ端末)	記憶 + 所持 (耐タンパ端末)
	保証レベル*1	AAL1	AAL 2	AAL2	AAL 3	AAL 3
	ユーザーの利便性	一般的なログイン手法であり、なじみがある	金融機関やSNSへのログイン等で一定程度普及しており、認知度が高い	生体認証を行うだけで、強度の高い認証が可能 (ただし、事前にアプリやブラウザによる登録が必要)	セキュリティキーと第2要素の併用で最高レベルの強度の認証が可能	マイナンバーカード1枚で強固なログインが可能 (ただし、事前に会員登録を行っている必要がある)
	脅威耐性 リスト型攻撃	×	○	○	○	○
	脅威耐性 フィッシング	×	×	○	○	○
	留意事項	パスワードの桁数や内容によって強度が変動	OTPをフィッシングサイトに入力してしまうリスクがある	プロダクトにより、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	利用するセキュリティキー等がAAL3の要件を満たしている必要がある	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
ユースケースの事例		IDとパスワードを入力しての認証	金融機関へのログイン等の2要素認証	パスワードレス認証、パスキー	YubiKey 5 FIPSシリーズを利用した認証	マイナポータルへのログイン、住民票や印鑑証明書の写しのコンビニ交付等

注釈1：保証レベルは「行政手続におけるオンラインによる本人確認の手法 に関するガイドライン」における保証レベル。
注釈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。

行政分野には行政手続ガイドライン等、各種法令・指針が整備されています。本ガイドラインはこれらに相当するものではありませんが、行政分野の指針等に網羅されていないユーザビリティ・コストの記載等も含まれています。

官民一体となったデータ・技術の活用や抜本的な構造改革が社会課題として謳われる中、民間分野においても、行政手続ガイドライン等から、行政手続固有の考え方を学ぶことも有用です。デジタル本人確認がデジタル社会における社会インフラとしての歩みを着実に進める上で、両ガイドラインがその一助となることを期待します。

行政分野における本ガイドラインの位置づけ



注釈：「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」のこと。

END

本資料は、TRUSTDOCKが信頼できると判断した情報をもとにTRUSTDOCKが細心の注意を払って作成・表示したものですが、TRUSTDOCKは本資料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。
本資料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。

本資料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、TRUSTDOCKは一切の責任を負いません。
本資料に記載された内容は、本資料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。
ただし、TRUSTDOCKは本資料を更新する義務を負うものではありません。

TRUSTDOCKは、本資料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、TRUSTDOCKは、本資料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。