民間事業者向け
デジタル本人確認ガイドライン

第1.0版

2023年3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タスクフォース

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

注釈：身元確認と当人認証については、「2.本人確認とは」を参照。

附録目次

コラム目次

はじめに

はじめに

本人確認は、変化しています。
10年ほど前まで、本人確認は、行政や金融などの一部のサービスにおいてのみ行われていましたが、今ではあらゆるサービスに導入され、対象となるサービスは拡大し続けています。

本人確認の目的も変容しています。
KYC（Know Your Customer）の言葉に代表されるように、かつては、犯罪を防ぐためにサービス利用者の身元を知ることが主目的でしたが、今では、サービスの信頼性向上、また、担い手不足などの社会課題を解決するために導入する事業者が増加しているなど、目的が多様化しています。

さらに、本人確認は、デジタル化が急速に進んでいます。
行政手続、金融などの一部のサービスについては、国が法令やガイドラインを定め、ルールに沿った「デジタル本人確認」が着実に浸透してきました。
また、「デジタル社会のパスポート」と銘打たれた本人確認書類であるマイナンバーカードの普及が進み、デジタル本人確認の利便性を高める環境が技術的にも整備されています。

しかし、民間事業者には、デジタル本人確認を検討・判断するに当たっての横断的な指針がありません。

そこで、OpenIDファウンデーション・ジャパンでは、有志の民間事業者によりタスクフォースを設置し、デジタル庁の協力も得て、民間事業者向けのデジタル本人確認ガイドラインを策定しました。

このガイドラインは、ガイドブックと指針の2つの性格を持ち合わせています。民間事業者の目的、ニーズに合わせてご利用いただき、デジタル本人確認を導入する際の拠りどころにしていただけることを願います。

本ガイドラインにより、デジタル本人確認の理解・普及が拡大し、安心・安全なデジタル社会が実現されることを期待します。

注釈：本ガイドラインの利用上の留意点等は、最終ページ「本ガイドラインの使い方と参照時の留意事項」を参照。

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）

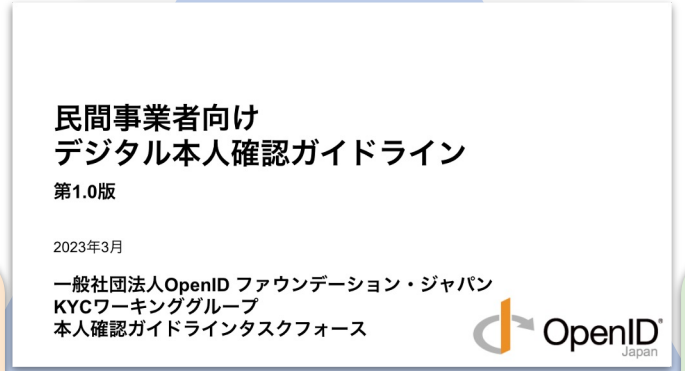
OpenIDファウンデーション・ジャパンでは、安心・安全なデジタル社会の実現を目指しており、
その取組みの一環として本ガイドラインを策定しました

To Be：本ガイドラインが目指す社会

本ガイドラインにより、デジタル本人確認の理解・普及が拡大し、以下の3点を推進することで、安心・安全なデジタル社会が実現することを目指します。

安心・安全なサービス

- 業界横断的なデジタル本人確認ガイドライン
- 個人情報の取扱いやユーザビリティを重視した内容と構成



誰一人取り残されない

- 選択可能な複数の本人確認手法を提示
- デジタル技術、本人確認の活用による課題解決策を提示

インターオペラビリティ

- グローバルな標準仕様であるOpenID Connectに基づく手法（身元確認結果の活用）を紹介
- NISTやニュージーランド基準など海外動向も参照

Ⅰ　総則

Ⅰ　総則

1. 対象・目的
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

本章では、本ガイドラインの対象や目的について説明します。

本章のポイント

- 本人確認が導入されるサービスは、「法令等で本人確認について定めのあるサービス」と「法令等で本人確認について定めのないサービス」に分類できます。
- 「法令等で本人確認について定めのあるサービス」は、本人確認の対象となる取引や講じなければならない手法、利用できる本人確認書類などが定められ、各所管官庁において、細かな解釈が示されていることが一般的です。
- 一方、「法令等で本人確認について定めのないサービス」については、一般的な本人確認のルールがなく、拠りどころとなる横断的な指針も存在しません。
- 「法令等で本人確認について定めのないサービス」を提供している事業者は、①金融機関等と同等の本人確認手法を導入（＝過剰対応）、又は、②本人確認の導入を断念（＝不正リスクの増大）する傾向があり、サービスの特性に応じた適切な本人確認手法の選択が難しい状況にあります。
- そこで、本ガイドラインは、①本人確認の導入・選択に必要な基礎知識のまとめ、②本人確認手法の特徴の整理、③マイナンバーカードや本人確認を巡る最新動向等を紹介しつつ、自社サービスの特徴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しています。
- さらに、本ガイドラインでは、安全性と利便性を兼ね備えた手法（中間的な手法）の特徴を整理・紹介し、本人確認手法の選択肢の拡大を図ります。

1.1. 背景①

多くのサービスや取引は、法令等*1で本人確認が求められていません。また、法令等で本人確認について定めがあるサービスにおいても、本人確認の対象となる取引は一部に限定されていることが一般的です*2。

法令等で本人確認（デジタル含む）が定められているサービスのイメージ

	本人確認の実施主体例	本人確認の対象となる取引例
犯罪収益移転防止法	特定事業者 (銀行、クレジットカード事業者、宅地建物取引業者、士業者等)	特定取引 (マネー・ロンダリング等のおそれの高い一定の類型の取引)
携帯電話不正利用防止法	携帯電話事業者	音声契約の契約締結、譲渡、貸与業者の貸与時
古物営業法	古物商	古物の買受け、交換、売却、交換の委託時

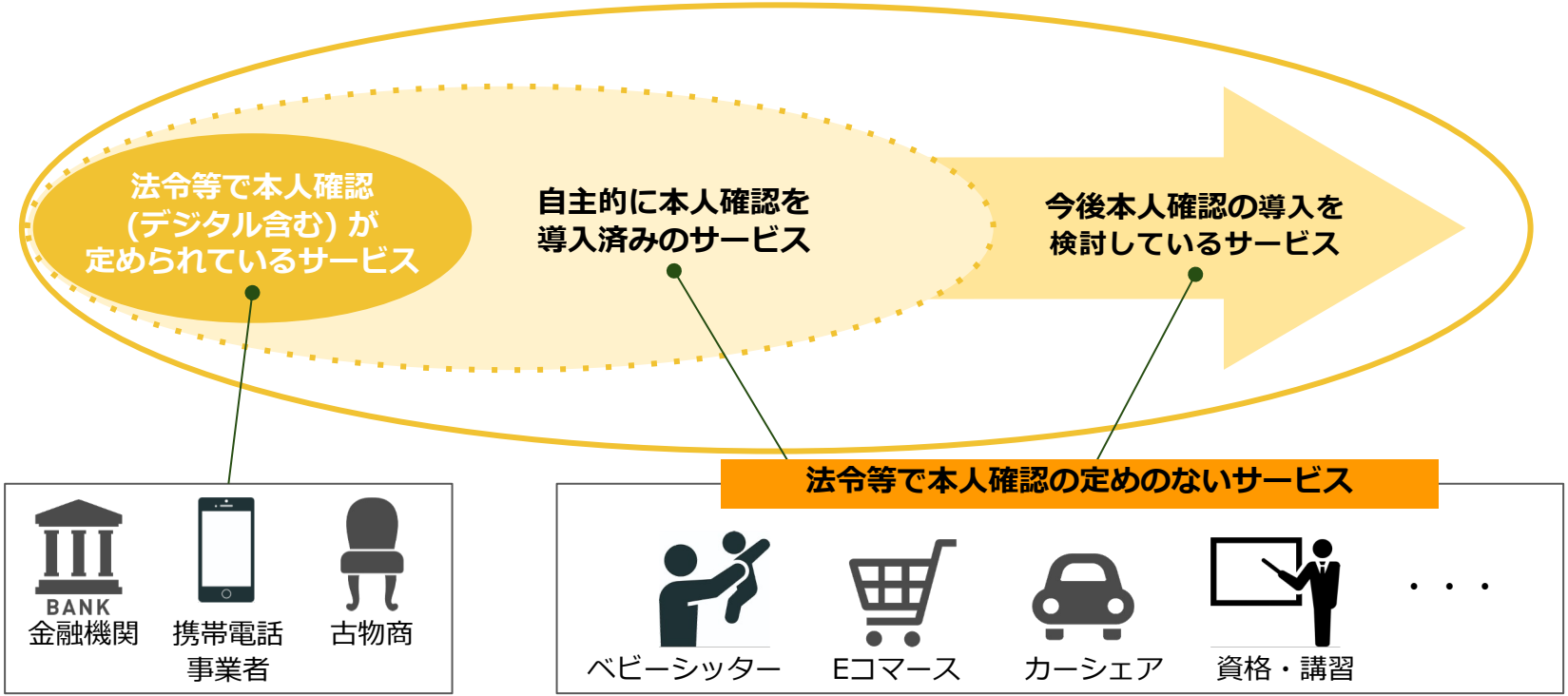
・
・

注釈1：「法令等」には、法律、政令、省令に加え、告示や通達、各種ガイドライン等を含む。
注釈2：例えば、「犯罪による収益の移転防止に関する法律」においては、金融機関の取引のうち、預貯金契約、現金送金（10万円超）等が本人確認の対象となっている。
（詳細は、「犯罪による収益の移転防止に関する法律」を参照）

1.2. 背景②

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）



1.3. 課題

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

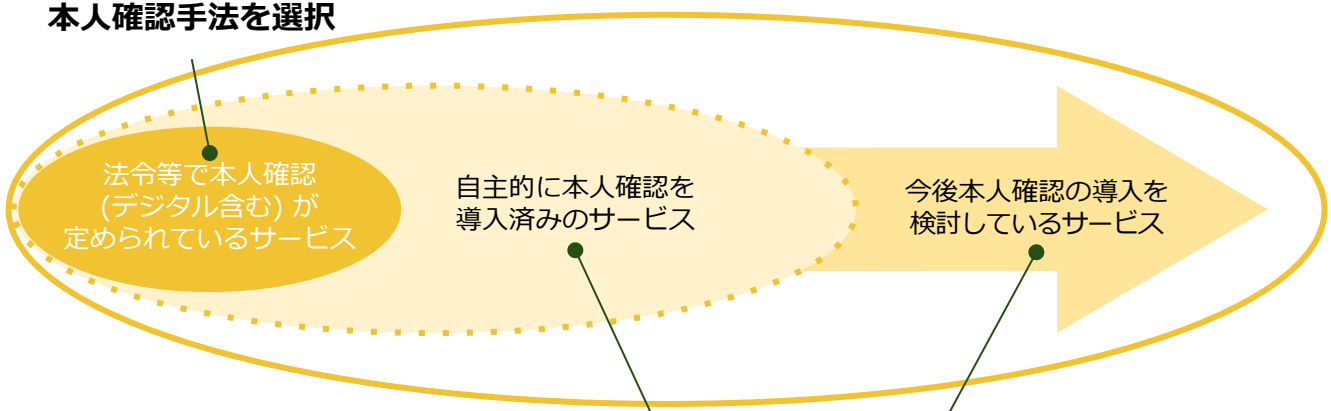
＋

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

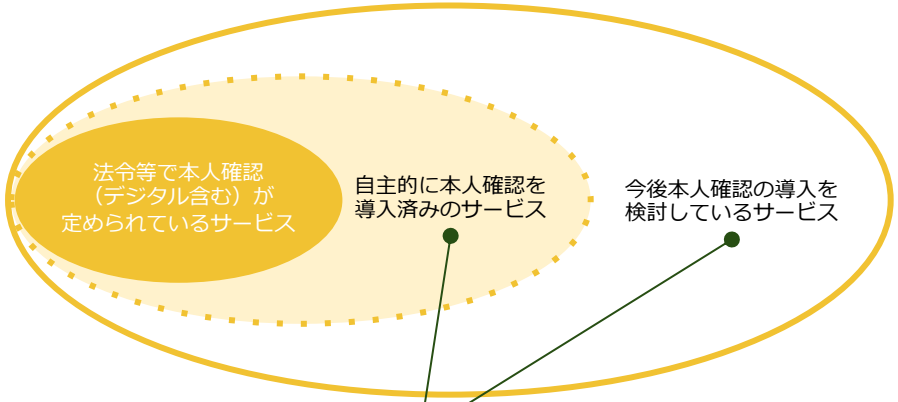
①金融機関等と同等の本人確認手法を導入（＝過剰対応）

②本人確認の導入を断念（＝不正リスク増大）

1.4. 対象・目的

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 Japan

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。

1.5. サービスに応じた本人確認手法の選択肢拡大

近年、デジタル技術の活用により、安全性と利便性を兼ね備えた手法 (中間的な手法)が実装されはじめています。本ガイドラインでは、中間的な手法を含めた各手法の特徴を整理し、本人確認手法の選択肢の拡大を図ります。

デジタル本人確認手法は、既に実装されているものだけでも複数存在します。法令等に定められている手法には、安全性が高いものの厳格な手続や要件を求めるものが多いのに対し、法令等に定められていない手法は、手続が簡易でも安全性が懸念される傾向があります。そこで、本ガイドラインでは、安全性と利便性を兼ね備えた中間的な手法を提案します。

本ガイドラインにおける中間的な手法の位置づけ

法令等に定められていない手法

例：
本人確認書類の
アップロード手法等

特徴：
手続は簡易だが、
安全性は低い

中間的な手法*1

デジタル技術を活用し
安全性と利便性を
兼ね備えた新しい手法

法令等に定められている手法

例：
犯収法*2等に定められた
デジタル本人確認手法等

特徴：
安全性は高いが、
手続や要件が厳格

**サービスに応じた
本人確認手法の選択肢拡大**

注釈1：手法の詳細は、「中間的な手法」を参照。
注釈2：「犯罪による収益の移転防止に関する法律」のこと。以降「犯収法」は同様。

1.6. 官民連携したガイドラインの策定

本ガイドラインは、経済産業省における研究会を皮切りに官民で議論・検討を重ね、2022年5月以降はOpenIDファウンデーション・ジャパンにタスクフォースを設置し、デジタル庁とも連携して策定しました。

2021年6月の政府の成長戦略に「eKYC等を用いた本人確認手法の普及」が盛り込まれて以降、同様の文言がデジタル社会の実現に向けた重点計画等に盛り込まれており、デジタル本人確認の普及促進は、政府の重点施策に位置づけられ続けています。

民間事業者向けデジタル本人確認ガイドラインの検討経過

経済産業省 Ministry of Economy, Trade and Industry

オンラインサービスにおける身元確認に関する研究会
- 身元確認、当人認証の整理
- 中間的な手法の必要性

IPA Digital Architecture Design Center

デジタルアーキテクチャ・デザインセンター インキュベーションラボ
- 保証レベルの整理、アーキテクチャの検討
- 事業者、団体へのヒアリング

デジタル庁

トラストを確保したDX推進サブワーキンググループ報告書（本人確認関係部分）
- DADC*の検討も踏まえた保証レベルの検討
- 「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」の議論への活用

OpenID Japan

民間事業者向けデジタル本人確認ガイドライン

注釈：デジタルアーキテクチャ・デザインセンターのこと。以降「DADC」は同様。

1.7. 本ガイドラインに残されている主な論点

本ガイドラインは今後も適宜改訂していきます。改訂にあたっては、最新情勢を踏まえつつ、以下の論点も踏まえながら検討することとします。

- **NIST SP 800-63-4の視点を取り入れた改正**
  - 特に、ミッションの達成度や公平性（コミュニティへの影響も含む。）の観点等を想定。
- **ガイドラインの全体構成の精緻化**
  - 本ガイドラインを活用し、一義的には、本人確認に関する認知の拡大や基本的な知識の理解醸成を図った上で、ガイドライン全体の構成について精緻化を進めていくことが重要。
  - 例えば、①本人確認の論理的ステップ、②本人確認で対応できる脅威やリスクの整理、③整理した脅威やリスクに対する管理策（脅威に対して複数オプションがあって良い）を明確化し、④管理策を検討、採用したプロセスの文書化等の推奨事項についても整理し、明示することを想定。
- **本ガイドラインの規範性の整理**
  - 本ガイドラインの記載のうち、遵守すべき項目、遵守することが望ましい項目、単なる情報提供等、規範性の度合いを明確化する。
- **身元確認や当人認証の保証レベルの再整理**
  - 脅威に対応した保証レベルの再定義等を想定。
- **当人認証に関する情報の追加**
  - 主な手法の拡充。
  - 当人認証手法の選択に資する追加情報（手法選択のフレームワーク等）。
- **フェデレーションに関する情報の追加**

注釈：本ガイドラインの見直しについては、2023年度中に改正の論点・方向性をまとめる予定。

Ⅰ　総則

1. 対象・目的
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

2. 本人確認とは

本章では、本人確認に関する基礎知識を説明します。

本章のポイント

- 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」では、「本人確認」を「身元確認」と「当人認証」の2つの要素に分解し、それぞれの概念を整理しています。
- アメリカ国立標準技術研究所（以下「NIST」という。）のSpecial Publication（以下「SP」という。） 800-63 Digital Identity Guidelinesでは、身元確認と当人認証のそれぞれに保証レベル（≒本人確認の確からしさの強度）を定めています。日本国政府が定めた「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」もこのNISTの考え方をベースに策定されています。
- 本人確認全体の強度は、身元確認保証レベル（Identity Assurance Level, IAL）と当認認証保証レベル（Authenticator Assurance Level, AAL）の両方を考慮することが重要です。そのため、一方の保証レベルが高い場合でも、もう一方の保証レベルが低いと、本人確認全体の強度は低いものとなります。
- 一方で、多くの身元確認手法がIAL2に位置づけられるため、各手法の強度を細分化して表現することを目的に経済産業省の情報処理推進機構（IPA）に設立されたデジタルアーキテクチャ・デザインセンター（DADC）においてDADC IALが作成されました。
- 本ガイドラインでは、身元確認の保証レベルとしてIAL及びDADC IAL、当人認証の保証レベルとしてAALをそれぞれ参照するとともに、保証レベル以外の特徴として、ユーザビリティやコスト等にも触れながら、具体的な手法を紹介します。

2.1. 本人確認の目的①

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

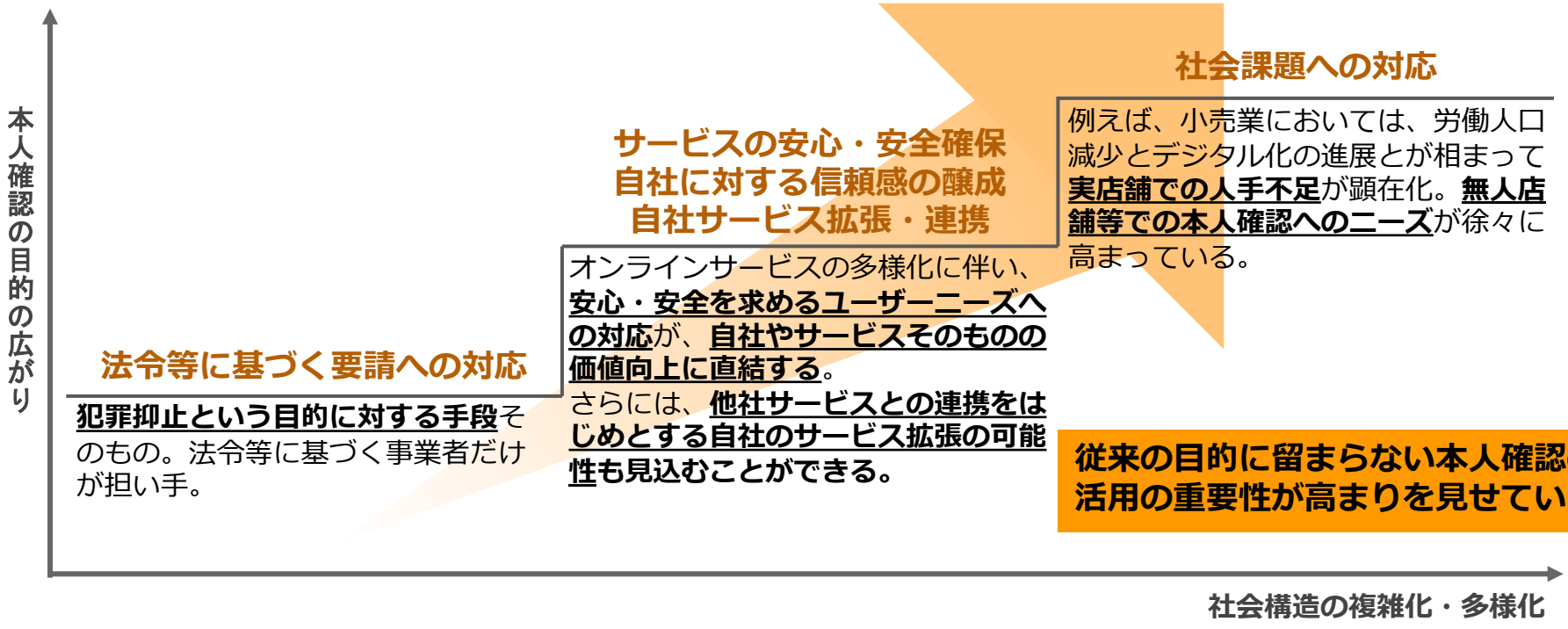
サービスの各段階での不正を防止・牽制でき、サービス全体の安全・安心に繋がる

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。

2.2. 本人確認の目的②

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



2.3. 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*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

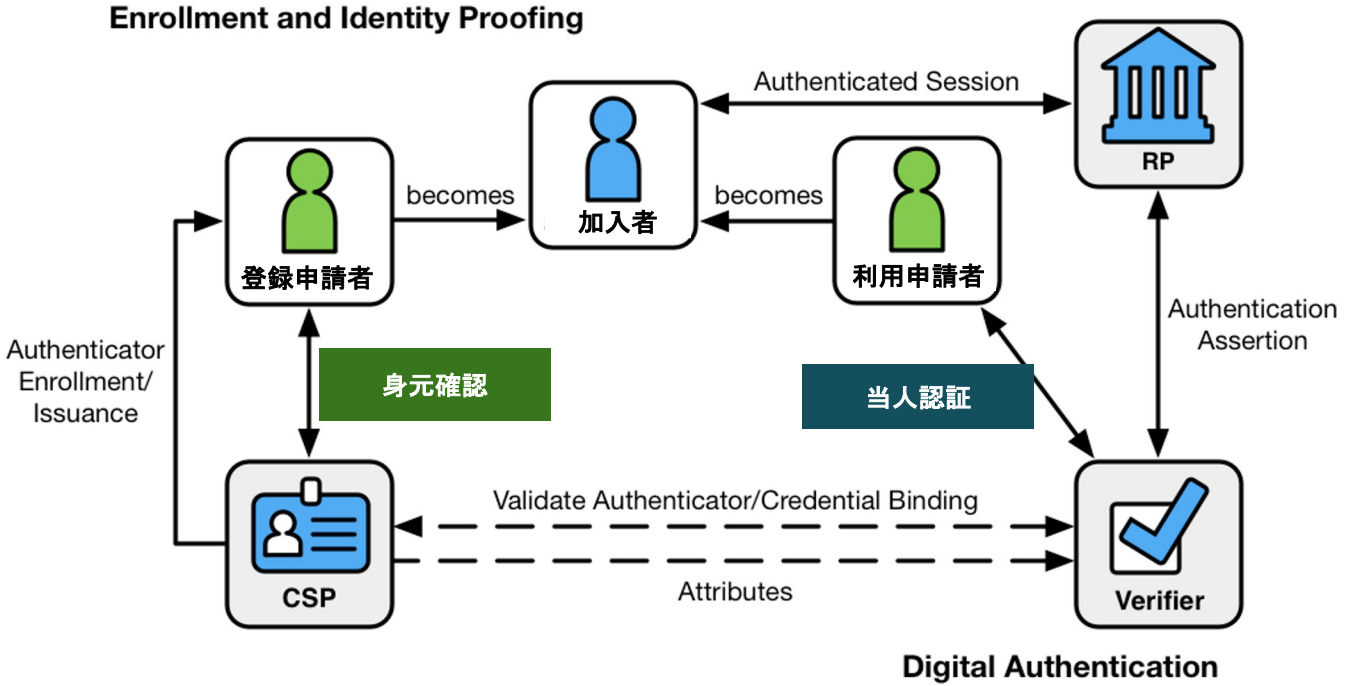
	身元確認	当人認証
確認の内容の例	● 提示された本人確認書類が偽造されていないことを確認 ● 提示された本人確認書類と申告内容を照合し、申請者に関するものであることを確認	● 取得されたパスワードや生体情報を、あらかじめ登録されているものと照合し、同一人物であることを確認
確認できること	実在性*2	当人性
実施シーンの事例	● ユーザー登録*3 ● 銀行口座の開設 ● 携帯電話の契約 ● クレジットカードの申込み	● ログイン ● スマートフォンのロック解除 ● サービス問い合わせ時の電話等での本人確認

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。

（参考）身元確認と当人認証の関係性

身元確認（Identity Proofing）に基づき「登録申請者」を「加入者」とし、「利用申請者」が「加入者」かどうかを当人認証（Authentication）で確認します。

デジタルアイデンティティモデル

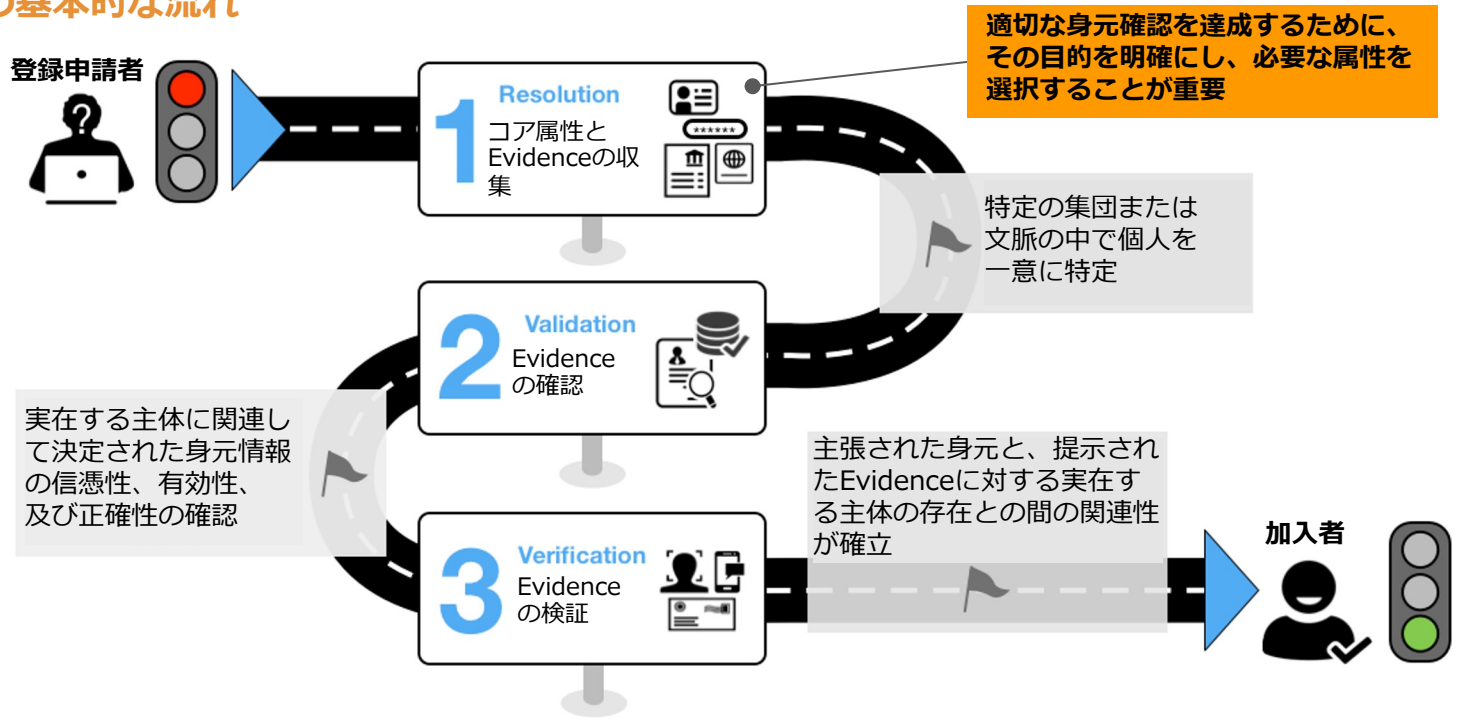


出所：NIST (2017)「Special Publication 800-63-3 Digital Identity Guidelines」より.

（参考）身元確認のプロセス

身元確認では、登録申請者について、①一意に特定（=Resolution）、②本人確認書類の有効性や正確性等を確認（=Validation）、③主張された身元と提示された本人確認書類の関連性を確立（=Verification）の3つのステップを経ます。

身元確認の基本的な流れ



出所：NIST (2017)「Special Publication 800-63-3 Digital Identity Guidelines」より.

2.4. 身元確認と当人認証の保証レベルの考え方

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）	当人認証の保証レベル*1, 2 Authenticator Assurance Level（AAL）
IAL3：対面での身元確認	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
IAL2：遠隔又は対面での身元確認	AAL2：複数の認証要素
IAL1：身元確認のない自己表明	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。

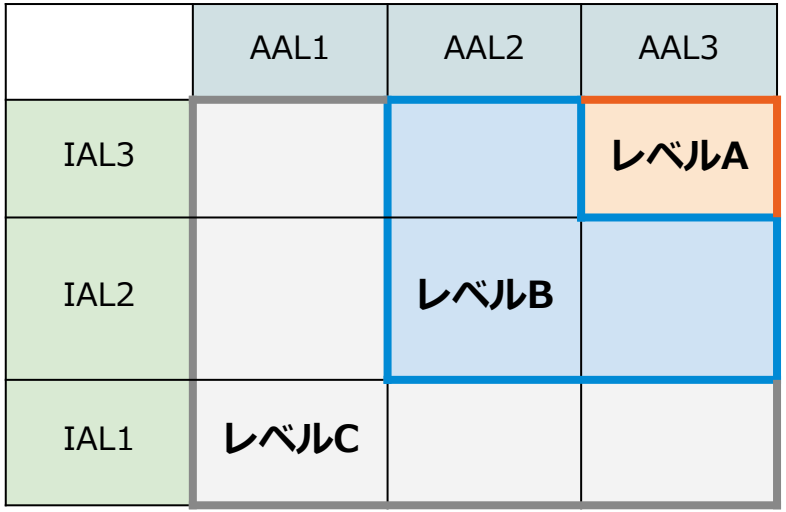
2.5. 身元確認と当人認証の保証レベルの考え方

行政手続ガイドラインでは、身元確認、当人認証のいずれかのレベルが低い場合は、全体として強度の低い本人確認となることを示しています。

行政手続ガイドラインにおける本人確認全体の保証レベルの考え方

IAL	AAL
IAL3 対面での身元確認	**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
IAL2 遠隔又は対面での身元確認	**AAL2** 複数の認証要素
IAL1 身元確認のない自己表明	**AAL1** 単一又は 複数の認証要素

本人確認全体の保証レベル
（行政手続ガイドラインの整理）*



本人確認全体の保証レベルを意識した上で、手法を選択することが肝要です。

注釈：ただし、IALとAALを掛け合わせ、本人確認全体の保証レベルをA～Cに定義することには議論がある。
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。

2.6. 身元確認と当人認証の保証レベルの考え方

一般的には、本人確認の強化を身元確認の強化と捉えがちですが、実際には、当人認証の保証レベルも意識した、本人確認全体としての検討が重要です。

例えば、①銀行における口座の開設・利用と②家事代行サービスの登録・利用を比較すると、ともにIAL2以上の身元確認を行っているものの、組み合わせている当人認証の保証レベルが異なるため、本人確認全体の保証レベルにも差が生じている。

銀行と家事代行サービスにおける本人確認の保証レベル*1の事例

		身元確認	当人認証	本人確認全体の保証レベル*2（行政手続ガイドラインの整理）
銀行	手続例	口座開設	オンラインバンキングへのログイン	**レベルB** (IAL2 or IAL3 × AAL2)
	保証レベル	• IAL2 (オンライン) • IAL3 (対面)	• AAL2 2要素(知識:パスワード + 所持:SMS-OTP)	
家事代行	手続例	ユーザー登録	マイページへのログイン	**レベルC** (IAL2 × AAL1)
	保証レベル	• IAL2 (オンライン)	• AAL1 1要素(知識:パスワード)	

注釈1：ここでの保証レベルは「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：ただし、IALとAALを掛け合わせ、本人確認全体の保証レベルをA～Cに定義することには議論がある。

2.7. DADC IALの概要

行政手続ガイドラインのIALについて、IAL2に強度の異なる複数手法が混在している現状を受け、デジタルアーキテクチャ・デザインセンターにおいてIALを細分化（DADC IAL）し、手法別の保証レベルが明確化されました。

DADCにおけるIAL細分化の検討の結果

IALの現状と問題意識

IAL2の定義　郵送・リモートでの確認

同定義に基づくと、券面偽造を防ぐことが困難な本人確認書類のアップロードと、マネー・ロンダリング対策等のために金融機関等で用いられている犯収法に規定された手法が同レベルに位置づいてしまう。

IALの要素を細分化し、行政手続ガイドラインでIAL2に位置づけられる複数手法の差異の明確化を試みた

DADC IAL検討の視点

ニュージーランドの本人確認規格を参考に身元確認を2つの観点に細分化し、身元確認手法を再評価

身元確認 IAL

- **Information Assurance**（情報のアシュアランス）：**本人確認書類情報の正確性**
- **Binding Assurance**（紐付けのアシュアランス）：**本人確認書類と身元確認主体の紐付けの確実性**

DADC IAL（結果概要）

手法	DADC IAL	IAL
公的個人認証(署名用電子証明書)	4	3
犯収法ヘ方式	3	2
犯収法ホ方式	3	2
銀行口座情報のAPI連携	3	2
携帯契約情報のAPI連携	3	2
リアルタイム撮影	2	2
アップロード	1	2
自己申告	0	1

出所：デジタルアーキテクチャ・デザインセンター（2022）「第2回インキュベーションラボ　テーマ２：サービスに応じたデジタル本人確認ガイドラインの検討　活動成果報告(詳細版)」より作成.

2.8. 本ガイドラインにおける保証レベルのまとめ

本ガイドラインでは、行政手続ガイドラインのIAL及びAALに加え、身元確認ではDADC IALも一部参照します。また、保証レベル以外にも、ユーザビリティやコスト等の特徴にも触れながら、具体的な手法を紹介します。

本ガイドラインにおける保証レベル参照の考え方

本人確認の導入検討

手法候補の選定

手法の決定

ガイドラインの活用範囲

個別対応

身元確認の導入検討

当人認証の導入検討

リスク対応

IAL
DADC IAL

AAL

リスク対応以外の重要な特徴

ユーザビリティ

コスト等

ガイドラインを参照し、自社サービスの特徴やサービスが抱えているリスク等を踏まえ、デジタル本人確認手法を選択する際の参考とする

本人確認サービス提供事業者等の具体的なプロダクトを比較検討し、コストや導入スケジュール等を踏まえて適切なデジタル本人確認手法を決定し、導入する

2.9. オンライン完結型本人確認以外の本人確認

本人確認手法には対面での確認及び郵送での確認もありますが、本ガイドラインではデジタル技術を活用した本人確認を対象とします。

対面・郵送による本人確認の概要

	対面での本人確認	郵送による本人確認
主なメリット	● 対面に基づくため、なりすましが困難。IALやDADC IAL等においても最高の保証レベルに位置づけられている。 ● なりすましの心理的ハードルが高く、非対面と比較して不正が行われにくい。	● デジタル技術の活用が難しいユーザーでも利用可能。 ● 本人限定受取郵便物等*を用いることで、対面での本人確認を導入することができる。 ● 住所地の確認が可能。
主なデメリット	● 本人確認の場所や時間が限定され、ユーザーの負荷が大きい。 ● 本人確認を行う窓口や人員の確保が必要であり、事業者の負荷が大きい。	● 本人確認が完了するまでに期間を要する。 ● 本人限定郵便の場合、本人確認が可能な時間が限定される。 ● 本人確認書類のコピーを添付する方法では、偽造リスクが存在する。

注釈：「本人限定受取郵便物等」とは、郵便物の受取り時に本人確認書類を提示することで本人に限り郵便物を受け取ることができるサービスのこと。日本郵政の本人限定受取郵便物等をはじめ、民間事業者で複数サービスが存在。

2.10. これからの本人確認

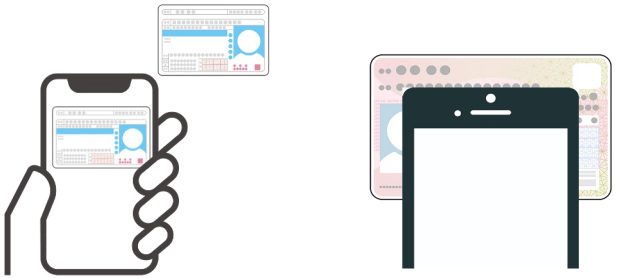
デジタル本人確認が拡大する中、スマートフォンを活用することで、本人確認書類の撮影や読み取りが不要な手法が登場してきています。

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

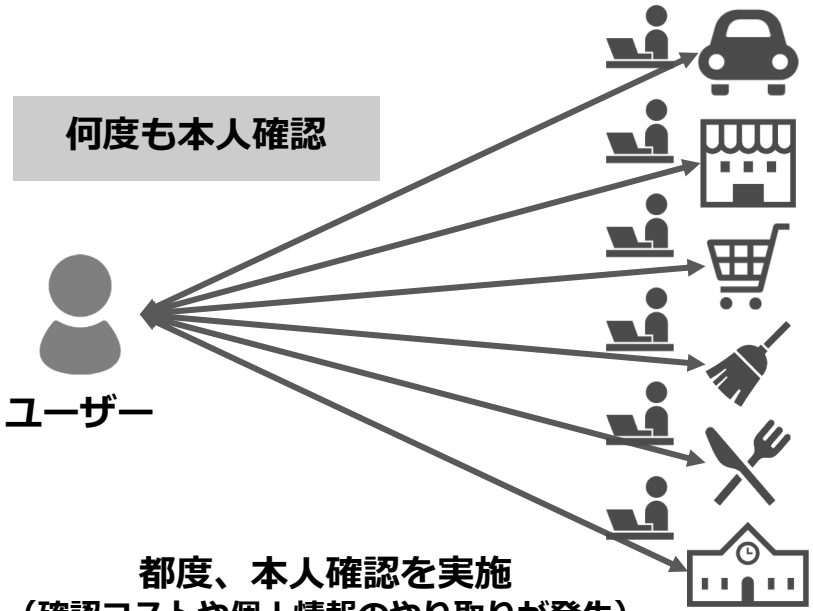
2.11. これからの本人確認（身元確認結果の活用の例）

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

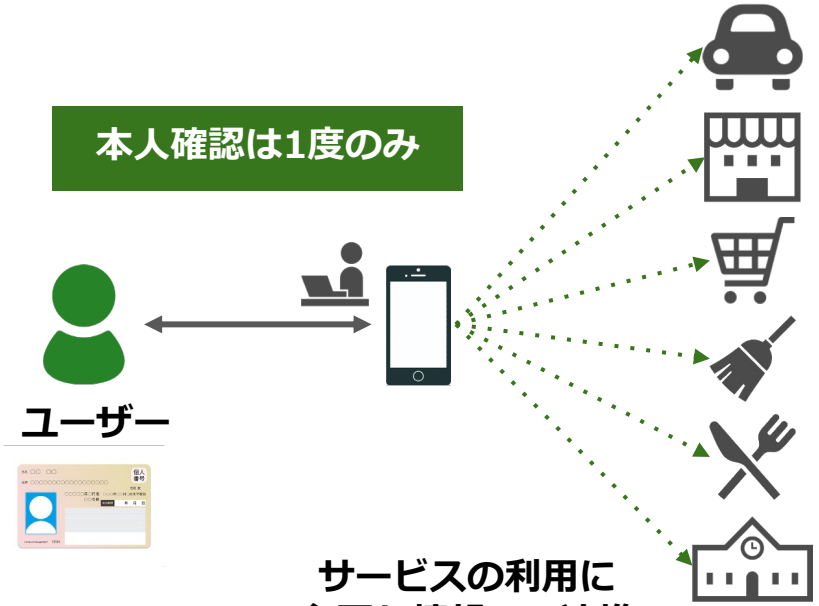
何度も本人確認



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

Ⅰ　総則

1. 対象・目的
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

3. 本人確認に関わる法令等

本章では、本人確認に関し一定のルールを定めている法令等の概要について紹介します。

本章のポイント

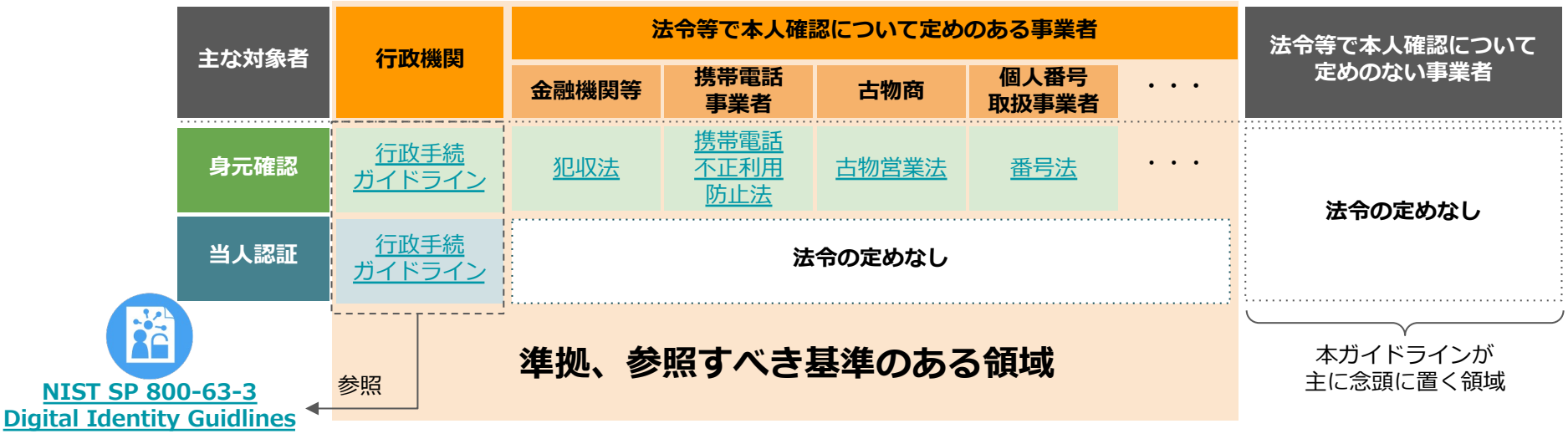
- 社会には様々なサービスが存在します。それらのサービスの中には、例えば、金融業における不正な送金など本来意図されていなかった者にサービス提供がなされてしまった場合に社会に及ぼす悪影響が大きいものがあります。こうしたサービスについては、法令等で本人確認の実施が義務付けられている場合があります。
- 本人確認のうち、身元確認に関しては、講ずべき具体的な手法まで個別の法令で規定されているものがあります。しかしながら、それら手法や対象は必ずしも一様ではなく、個々の法令の趣旨や目的によって異なっています。
- 当人認証に関しては、身元確認のように、個別の手法を詳細に規定するものはありません。ただし、IDやパスワード入力等での認証に関する規定を置く法令も一部に存在しています。
- また、法令以外にも、「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」のように、オンラインでの本人確認を行う際の考え方や手法例を、その保証レベルとともに示すものもあります。

3.1. 本人確認に関する規制

「身元確認」については、一定の業態について、具体的な手法まで個別の法令で規制されているものがあります。一方で、「当人認証」に関しては、一部を除いて、法令等で明確な規制はありません。

例えば、犯収法では、なりすまし等に起因する犯罪（マネー・ロンダリング等）を防止するため、金融機関等には、顧客である金融サービスの利用者が、実在する特定の人物であることを所定の身元確認手法で確認することなどが厳しく求められています。（個別法令の例は巻末附録の「本人確認に関わる法令等（詳細）」を参照）

本人確認を巡る基準や規制の全体像（イメージ）



注釈：例えば、古物営業法では、同法が定める身元確認手法により既に身元確認済みの顧客について、2回目以降はID・パスワードの入力等による確認を行う場合には、身元確認を行わずとも足りるとされているなど、一部において、当人認証の考え方を採用する法律の例はあります。

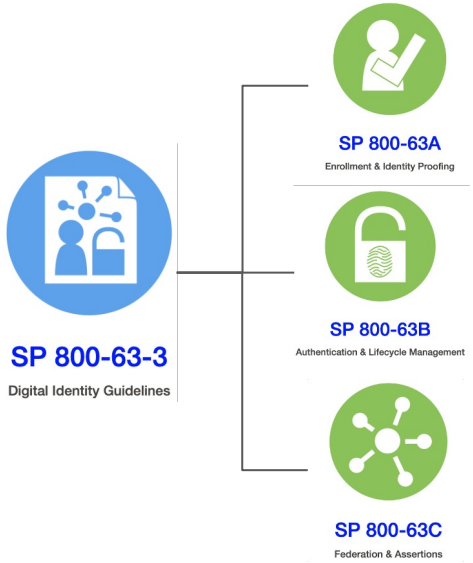
出所：NIST (2017)「Special Publication 800-63-3 Digital Identity Guidelines」より.

3.2. NIST SP 800-63-3

NIST SP 800-63-3は、NIST（米国立標準技術研究所）が電子的な本人確認に関し、主に米国政府機関向けに策定したガイドラインですが、その考え方は非常に有用であり、国際的な技術標準として様々な業界で参照されています。

Digital Identity Modelの各フェーズについて、IAL（身元確認の保証レベル）、AAL（当人認証の保証レベル）、FAL（認証連携の保証レベル）の3つの保証レベルが示されています。各保証レベルの詳細はサブドキュメント化されており、各フェーズの保証レベルを実際のサービス内容に合わせて活用可能となっています。

NISTガイドラインの構造と保証レベル



名　称	内　容	詳　細	
IAL (Identity Assurance Level)	ユーザーが申請者として新規登録する際に行われる身元確認プロセスの厳密さ、強度を示す	IAL3	**対面**での身元確認が必要であり、本人確認書類の**検証を有資格者が実施**
		IAL2	本人確認書類での**確認をリモートまたは、対面**で実施
		IAL1	実在性の確認や検証は行わず、**自己申告を許容**
AAL (Authenticator Assurance Level)	登録済のユーザーがログインする際の当人認証プロセスの厳密さ、強度を示す	AAL3	**2要素認証以上**（**暗号鍵の所持証明要素、ハードウェアの関与**が必要）
		AAL2	**2要素認証以上**（2要素目の認証手段は**ソフトウェアによるもので可**）
		AAL1	**単要素認証**で良い
FAL (Federation Assurance Level)	IDトークンなど認証結果データのフォーマットや連携手法の厳密さ、強度を示す	FAL3	認証結果データへの**署名・暗号化**、これと紐付く**秘密鍵の本人所有**を証明できる連携
		FAL2	アカウント発行元の**署名・暗号化**された認証結果データによる連携
		FAL1	アカウント発行元の**署名**付き認証結果データによる連携

出所：NIST (2017)「Special Publication 800-63-3 Digital Identity Guidelines」より.

3.3. 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

「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」は、行政手続に関して、オンラインでの本人確認を行う際の考え方や手法例を示したものあり、NIST SP800-63-3を参考に、身元確認・当人認証の保証レベルが示されています。

行政手続（個人）に係る本人確認手法例と保証レベル

必要な保証レベル		オンラインによる手法例	
IAL 身元確認保証レベル	**AAL** 当人認証保証レベル		
レベル3 対面での 身元確認	**レベル3** 耐タンパ性が 確保された ハードウェア トークン	レベルA	• **マイナンバーカード(公的個人認証:署名用電子証明書)による身元確認**でアカウントを作成し、アカウント作成後はマイナンバーカード(公的個人認証:利用者証明用電子証明書)の耐タンパ性ハードウェアトークンによる当人認証を実施。 • 申請データに対するマイナンバーカード (公的個人認証:署名用電子証明書)による電子署名を付与。 ※耐タンパ性ハードウェアトークン例: PIN+IC カード(マイナンバーカード)
レベル2 遠隔又は対面での 身元確認	**レベル2** 複数の 認証要素	レベルB	• マイナンバーカード(公的個人認証:署名用 電子証明書)**等**による身元確認でアカウント作成し、アカウント作成後はマイナンバーカード (公的個人認証:利用者証明用電子証明書) 若しくはこれによることができない場合、 その他の多要素認証による当人認証を実施。 ※多要素認証の例:ID・パスワード+二経路認証アプリ、ID・パスワード+ワンタイムパスワード生成アプリ、ID・パスワード+生体認証
レベル1 身元確認のない自己表明	**レベル1** 単一又は複数の認証要素	レベルC	• 身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後は単要素認証で当人認証を実施。 ※単要素認証の例:ID・パスワードのみ、認証デバイスのみ、生体認証のみ
該当しない	該当しない	レベルD	• 身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後もアカウントを入力するだけ(当人認証を行わない)。

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。

Ⅰ　総則

1. 対象・目的
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**

4. 本人確認書類について

本章では、「本人確認書類」について説明します。本人確認手法を選択する際に本人確認書類は重要な要素であり、マイナンバーカード等の本人確認書類の特徴をまとめ、説明します。

本章のポイント

- 本人確認書類には様々なものがあり、顔写真があるものとしては、マイナンバーカード、運転免許証、パスポートなど、顔写真が無いものとしては被保険者証、住民票の写しなどが挙げられます。
- これまで、本人確認書類としては運転免許証の利用が中心でしたが、近年はマイナンバーカードの普及が急速に広がり、他の本人確認書類の機能をマイナンバーカードへ一本化する検討も進められています。
- 本人確認書類は、記載事項のほか、ICチップに格納されている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、身元確認でどの本人確認書類を利用するかを選択することが重要です。
    - マイナンバーカードは、マイナンバーが記載されたICチップ付き本人確認書類であり、電子証明書の機能を活用することで、身元確認以外にも、様々なサービスを利用できます。
    - パスポートは、政府による厳格な確認の上で発行されたものであり、本人確認書類としても様々な場面で活用されています。
- ICチップを搭載した本人確認書類であっても、券面の撮影による本人確認手法を選択できます。そのため、具体的な身元確認手法は、サービスや手続のリスク・ユーザーのニーズ等を踏まえて選択することが求められます。（詳細は「5. 事業者として留意すべきこと」や「9. 主な身元確認手法」を参照）

4.1. 本人確認書類の種類

本人確認書類は、顔写真の有無で大別でき、以下のような様々なものがあります。

例：犯収法施行規則に定める自然人の本人確認書類

顔写真あり	運転免許証、運転経歴証明書、在留カード、特別永住者証明書、マイナンバーカード、 旅券（パスポート）、乗員手帳、船舶観光上陸許可書（パスポートの写しが添付）、身体障害者手帳、 精神障害者保健福祉手帳、療育手帳、戦傷病者手帳　等 （本人の氏名、住居及び生年月日の記載があるもの）
	上記のほか、官公庁から発行され、又は発給された書類その他これに類するもの （本人の氏名、住居及び生年月日の記載、顔写真のあるもの）
顔写真なし	被保険者証（国民健康保険、健康保険、船員保険、後期高齢者医療、介護保険）、 健康保険日雇特例被保険者手帳、組合員証（国家公務員共済組合、地方公務員共済組合）、 私立学校教職員共済制度の加入者証、児童扶養手当証書、特別児童扶養手当証書、母子健康手帳　等 （本人の氏名、住居及び生年月日の記載があるもの）
	印鑑登録証明書 戸籍附票の写し 住民票の写し又は住民票の記載事項証明書

注釈：上記の本人確認書類の補完書類として、その他、納税証証明書、社会保険・公共料金の領収証により確認を行うこともある追加的確認を行うこともある（例：2020.2.4以降発行のパスポートには「住居」記載欄がないなど、追加的な確認が必要な場合あり）。

4.2. 本人確認書類の変化

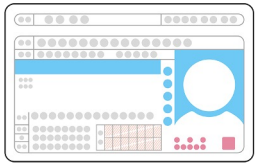
政府がデジタル社会のパスポートと位置づけているマイナンバーカードの普及が急速に進み、他の本人確認書類の機能をマイナンバーカードへ一体化する検討も進められています。

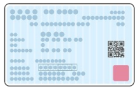
これまでは、幅広い本人確認書類が選択・使用され、中でも運転免許証が本人確認書類としての役割を中心的に担ってきました。近年、政府の推進により**健康保険証、運転免許証、在留カードの機能をマイナンバーカードへ一体化する検討も進められています。**

本人確認書類の変化（イメージ）

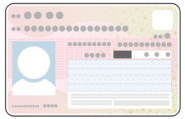
これまで

パスポート

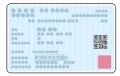

運転免許証

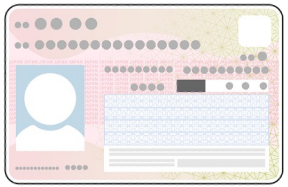

健康保険証

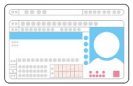

在留カード


マイナンバーカード

これから


廃止の方向



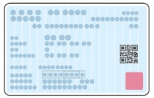
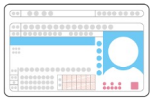
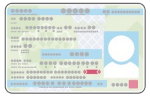


マイナンバーカードへの一体化を検討中

（参考）マイナンバーカードとの一体化のスケジュール

複数の本人確認書類については、マイナンバーカードとの一体化に向けた検討が行われており、特に、健康保険証は当初の予定を早め原則廃止を目指す見込みとされています。

マイナンバーカードとの一体化に向けた検討等に関するスケジュール

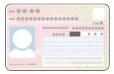
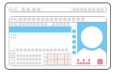
	2022年度	2023年度	2024年度	2025年度
 健康保険証	2024年の秋までに原則廃止を目指す			保険証は原則廃止の見込み
 運転免許証	2024年度末までの一体化の前倒しを検討		2024年度から更新時のオンライン講習対象拡大（4道県から）	運転免許証は存続予定
 在留カード	2025年度までに一体化カードの交付を目指す			在留カードの存続は不明

出所：健康保険証及び運転免許証の一体化については、河野デジタル大臣記者会見（2022年10月13日）より。在留カードの一体化については、「デジタル・ガバメント実行計画（2020年12月25日閣議決定）」より.

4.3. 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、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。

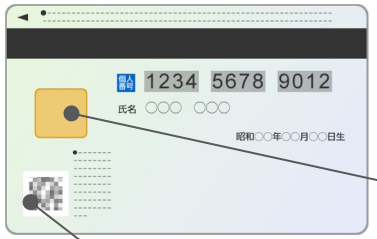
***2 特別永住者証明書**
特別永住者の法的地位等を証明するものとして交付されるもので、氏名、生年月日、性別、国籍・地域、住居地、有効期間の満了日などの情報が記載（16歳以上には顔写真が表示）
ICチップを搭載。

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。

4.4. マイナンバーカードの概要①

マイナンバーカードは、マイナンバーが唯一記載された顔写真付き本人確認書類です。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* **（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、氏名、住所、 生年月日、性別は4桁の数字* **（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。

注釈：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。
出所：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」より作成.

4.5. マイナンバーカードの概要②

マイナンバーカードの電子証明書には役割の異なる2種類の証明書があります。オンラインによる本人確認において利用が広がっており、政府では、電子証明書機能をスマートフォンに搭載するための検討が行われています。

マイナンバーカードに格納されている2種類の電子証明書

署名用電子証明書

申請書等 ＋ 電子署名（秘密鍵で署名） ＋ 公開鍵＋電子証明書（氏名、住所、生年月日、性別を記録）

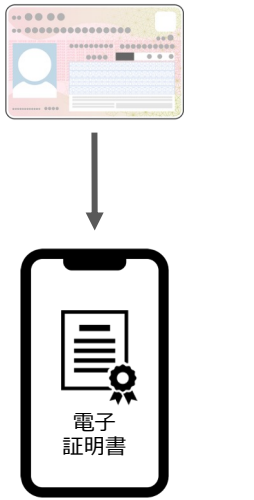
e-Taxなどの電子申請等のほか、電子署名機能を利用して身元確認にも利用される

利用者証明用電子証明書

公開鍵＋電子証明書（氏名等の記録なし）

マイナポータルのログインやコンビニエンスストア等における証明書等の自動交付等に利用される

2023年5月から電子証明書機能のスマートフォン搭載（Android）が開始される予定

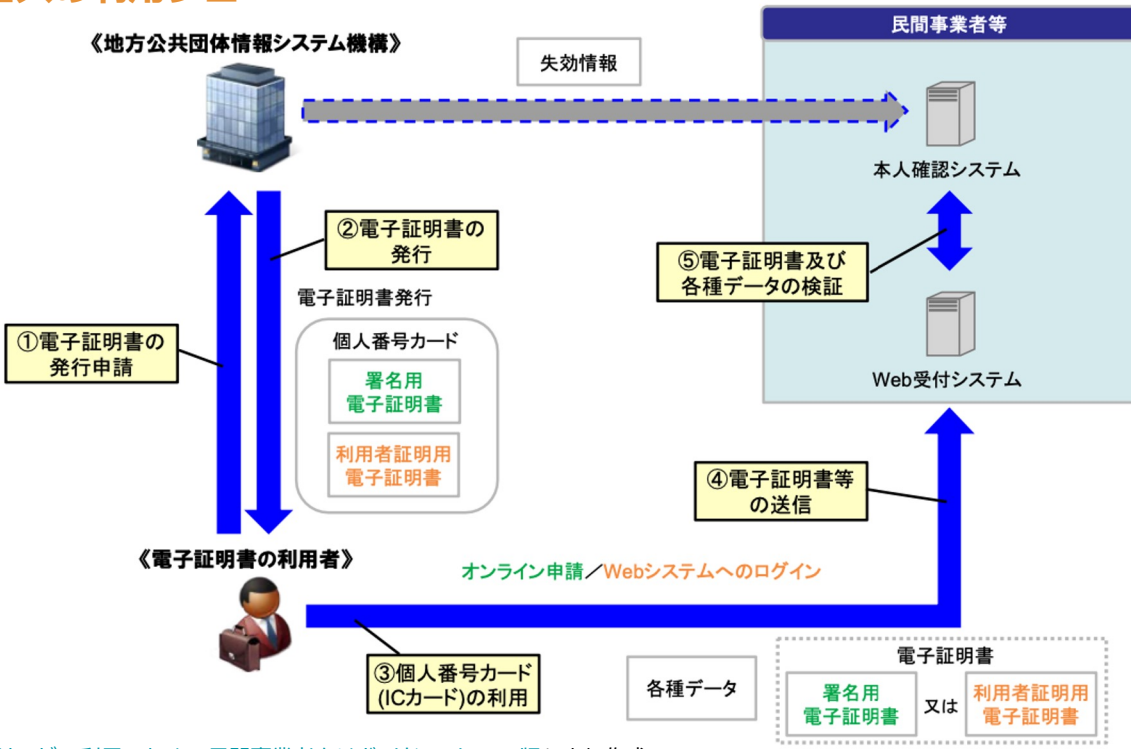


詳細は、「マイナンバーカードの機能のスマートフォン搭載（検討状況の整理）」を参照

（参考）公的個人認証サービスの概要

公的個人認証サービスとは、インターネット上での申請や届出を行う際に、第三者によるなりすましやデータの改ざんを防ぐために用いられる、本人確認手段を提供するサービスです。本人確認は、マイナンバーカードに格納された電子証明書を用いて行われます。

公的個人認証サービスの利用フロー

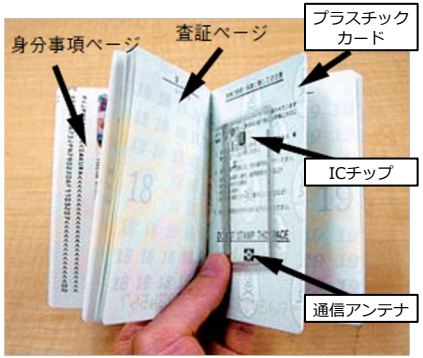


出所：総務省(2015)「公的個人認証サービス利用のための民間事業者向けガイドライン1.1版」より作成.

4.6. パスポート

パスポートは、政府が外国に渡航する自国民の国籍・身分を証明し、渡航先の外国政府に保護を依頼するための公文書としての性格を持ちます。このため、政府による厳格な確認の上で発行されており、本人確認書類としても様々な場面で活用されています。

本人確認書類としてのパスポート



券面（身分事項ページ）

- ○ 旅券番号
- ○ 国籍
- ○ 有効期限
- ○ 氏名
- ○ 生年月日
- ✕ 住居
- ○ 顔写真

ICチップ（ICページ）

- **身分事項ページ記載事項**
- **顔写真データ**

ICチップ情報へのアクセスは、PIN入力ではなく、券面情報（旅券番号・生年月日・有効期限）をキーとするアクセスコントロールの手法が採用されている。

「本人確認書類」として利用の際の留意点

● 新型パスポート（2020年2月4日**以降**発行）	● 旧型パスポート（2020年2月4日**以前**発行）
➡「住居」の記載欄廃止	➡「住居」の記載欄あり
住居の確認ができない点に留意が必要	**単独で本人確認書類になるが、自己申告の住所であることに留意が必要**

犯収法の本人確認など、住居の情報を含めた確認が法令上求められている場合、新型パスポートに加え、住居の記載のある別の本人確認書類や補完書類での確認が必要になる。

出所：上画像：外務省ウェブサイト「パスポート（旅券）」、下画像：外務省「平成18年度外交青書」より.

（参考）外国人向けの本人確認書類

海外在住者へのサービス提供や外国人訪日客の増加など、日本人や日本在留の外国人以外の方々に対する本人確認が必要となり得るケースも想定されます。本人確認の相手方の国籍に着目した本人確認書類には、下記の例が挙げられます。

犯罪収益移転防止法の例

日本に在留する外国人

日本国籍を有する個人と同じ本人確認書類（4.1. 本人確認書類の種類を参照）

マイナンバーカード　パスポート　運転免許証　住民票の写し　etc.

外国籍であることに着目した本人確認書類

在留カード　**特別永住者証明書**

日本に在留していない外国人*1,2

- **パスポート**（日本政府の承認した外国政府発行のもの）
- **国際機関発行の旅券**（国連通行証など）
- **旅券に代わる証明書**（渡航証明書、再入国許可証など）

上記は氏名・住所・生年月日が確認できる必要がある

特例

短期滞在者（訪日観光客など）*3

外貨両替、宝石・貴金属売買（現金決済）等の場合

氏名・生年月日・国籍・番号の記載のある**旅券**
- 旅券（パスポート）の**住居の記載は不要**
- 他の確認書類による**住居の確認も不要**

注釈1：本人確認の際、国外に所在しており、日本に住居を有していない外国人。
注釈2：法律は、利用できる本人確認書類を日本在留資格の有無や国籍によって区分する規定とはなっていないが、日本に在留していない外国人が現実的に所持・提示可能な本人確認書類は、上記図のパスポート等の旅券類に限定される。
注釈3：日本に住居を有していない外国人で、短期（90日以内）の日本滞在者。

4.7. 本人確認書類から見た身元確認手法選択の考え方

ICチップ搭載の本人確認書類であっても、ICチップを利用せず、券面を撮影した画像を送信する手法（アップロード手法等）で対応する事業者が多い現状があります。自社サービスや手続のリスクとユーザーエクスペリエンス等を踏まえた身元確認手法の選択が求められます。

マッチングサービスにおける本人確認において利用できる本人確認書類の事例

	マイナンバーカード	運転免許証	パスポート	在留カード	健康保険証	年金手帳	障がい者手帳
A社	○	○	○	○	○	-	-
B社	○	○	○	○	-	-	-
C社	○	○	○	○	○	○	○
D社	○	○	○	-	○	-	-
E社	○	○	○	○	○	○	○

ICチップを搭載した本人確認書類だが、
券面撮影（≠ICチップ読み取り）で本人確認書類を提出する

複数の本人確認書類と身元確認手法を組み合わせ、身元確認の実施完了率を向上させることが可能
（詳細は、5.3. 身元確認手法の選択・ユーザーエクスペリエンスの設計を参照）

出所：各社ウェブサイト等から作成。

Ⅱ　デジタル本人確認の導入、手法の選択時に留意すべきこと

5. 事業者として留意すべきこと
6. 個人情報の取扱い

5. 事業者として留意すべきこと

本章では、デジタル本人確認導入の際の留意事項として、主に身元確認導入時の検討項目について説明します。

本章のポイント

- 身元確認は、サービス提供者事業者が実施主体であり、責任を持って適切な実施を確保する必要があります。
  - 身元確認を他者に委託して実施する場合も、信頼に足る委託先を選定することが重要です。
- 身元確認の導入にあたっては、主に、①身元確認手法の選択・ユーザーエクスペリエンスの設計、②システムの改修、③ユーザーへの事前周知、④システム運用・セキュリティ体制の整備、⑤問い合わせ対応の体制の整備、の5つについて対応が必要です。
  - 身元確認を導入することで、一定数の顧客離脱が発生します。一方で、複数の本人確認書類や身元確認手法を組み合わせることで、機会損失を低減させることが可能です。
  - 身元確認の導入のためには、システムの構築・改修が必要になります。また、最近では身元確認サービスをAPIとして提供している事業者もおり、こうした事業者とのAPI連携も導入負荷軽減に効果的だと考えられます。
  - 身元確認の導入は事業者だけでなく、ユーザーにも影響があります。ユーザーに対して、身元確認導入の必要性やメリットなどを丁寧に伝えることで、離脱を防ぐだけでなく、サービスの信頼性向上を訴求することに繋がると考えられます。
  - 身元確認では、個人情報を取得するため、システムやセキュリティ体制の整備が不可欠です。
  - 身元確認を適切に運営するためには、円滑な運営体制の整備が重要です。その際、身元確認に関する専門的な内容に迅速に対応する必要があり、外部事業者への委託も含め、事前の体制整備が求められます。
- 時間や場所を選ばないオンラインでの身元確認はユーザビリティが優れている点が効果的です。
  - 特に、身元確認手続が完了するまでの所要時間はデジタル化により格段に短縮されています。

5.1. 身元確認の主体と責任

身元確認は、サービス提供者事業者が実施主体であり、責任を持って適切な実施を確保する必要があります。また、身元確認を委託する場合でも、信頼に足る委託先の選定が重要です。

身元確認を委託する際の留意事項等

身元確認はサービス提供事業者が自らの責任と判断で導入するもの

身元確認の責任の主体

- 身元確認を適切に実施できなかった場合の法的責任は、委託先ではなく委託元の事業者が負う。
- 法令に本人確認の定めのないサービスについては、別途委託契約書等で責任分担を規定する等し、双方が一定の責任を負う。

信頼に足る委託先の選定

- 提供している身元確認手法の強度
- 各種の法令遵守状況（個人情報保護法等）
- セキュリティ（個人情報の取扱い、第三者認証の取得状況等）

継続的かつ適切な委託先管理*

- 各種法令遵守状況の継続的な確認
- セキュリティ対策の実施状況の継続的な確認

利便性やコストだけでなく、上記の留意事項を踏まえた委託先の選定・管理が重要

注釈：個人情報保護法上、個人データの取扱いを委託する場合、委託元には、委託先が安全管理措置を適切に講じているか監督する義務が課されている。

5.2. 身元確認導入時の対応事項

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*）

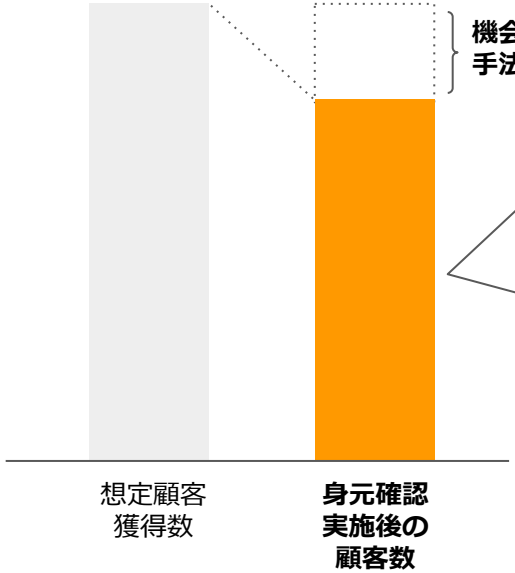
注釈：API連携の場合であっても、自社のシステムの改修、連携等については、自社で対応する必要がある。

5.3. 身元確認手法の選択・ユーザーエクスペリエンスの設計

身元確認手法を選択する際は、手法が対応できる本人確認書類のカバー率、本人確認書類提出完了率、身元確認承認率を踏まえて手法を選択することが重要です。

本人確認手法の選択と顧客獲得時の機会損失

顧客獲得数イメージ



機会損失をゼロにすることはできないが、
手法の工夫により最低限に抑えることができる。

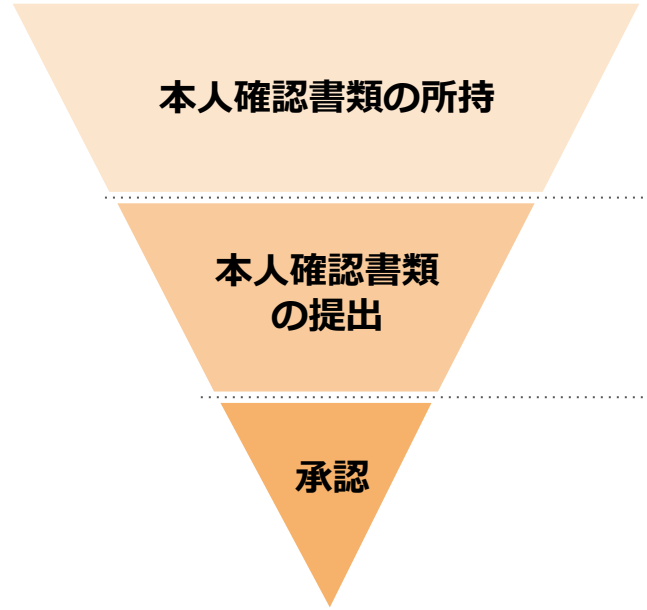
身元確認の実施完了率	=	本人確認書類のカバー率	×	本人確認書類提出完了率	×	身元確認承認率*
完了率を上げるための工夫		• 広く利用される本人確認書類を利用できる手法を選択する • 複数の本人確認書類を利用できる手法を選択する		• 提出完了率が高い手法を選択する • 提出手法のFAQを提示する		• 不備が起こらないユーザーインターフェースを工夫する • 身元確認基準を調整する

注釈：身元確認承認率とは、本人確認書類の提出が完了した手続のうち、身元確認の承認に至る手続き数のこと。本人確認書類と入力情報の不一致のほか、本人確認書類の画像の提出を求める手法においては、券面画像のぼやけや切れ等により一定の差し戻しが発生する。

5.4. 身元確認手法の留意点

身元確認の過程にはユーザーの離脱のポイントが複数あり、手法ごとに影響の大きさが異なります。身元確認の導入にあたっては、必要に応じて複数手法を組み合わせることでユーザー離脱の影響を防ぐことができます。

身元確認における離脱の傾向と手法の特徴例



ユーザーの主な離脱ポイント	（身元確認手法別の特徴例） 犯収法ホ方式	公的個人認証	身元確認結果の活用
本人確認書類の所持	複数種類の顔写真付き本人確認書類を利用可能	マイナンバーカードだけしか利用できない（申請枚数は運転免許証を超えている）	本人確認書類の所持は不要（情報提供元事業者を選択する負担感がある）
本人確認書類の提出	撮影ステップが多く、途中離脱が発生（撮影行為は多くのユーザーが対応できる）	暗証番号の入力間違いによる途中離脱が発生（暗証番号を覚えていないなどのケースも存在）	通常利用しているアカウントの当人認証を用いて提出が可能
承認	写真のぼやけや切れ等による差し戻しが発生(審査に時間を要するため、否認の決定が遅れるケースもありうる)	提出が完了すれば即時に承認可能（署名用電子証明書の有効期限切れによる否認が起こりうる）	提出が完了すれば即時に承認可能

5.5. システム構築・改修

**デジタル技術を活用した身元確認手法の導入にはシステムの構築・改修が欠かせません。
また、最近では身元確認サービスをAPIとして提供している事業者もおり、こうした事業者とのAPI連携も効果的な選択の1つです。**

システム改修・構築の視点

自社に適切なシステム導入方法を選択（例）

	開発コスト	柔軟性	スケジュール
自社開発	大	大	遅
API連携	小	中	早

API連携のメリットと留意点

API連携のメリット

- コスト・時間の削減、機能の追加も用意
- セキュリティや個人情報の取扱いに対応
- 入力の自動化等のUI/UXが優れている

実装までの留意点

- API仕様の理解、変更、停止時の対応
- トラブル時の対応フロー（テストを実施）

APIを導入した場合でも、身元確認の責任の主体は導入事業者です。そのため、APIの提供元任せにせず、APIに関する理解を深めることが重要です。

注釈：APIとは「Application Programming Interface（アプリケーション・プログラミング・インタフェース）」の略であり、プロダクトやソフトウェアをつなぐインタフェースのことを指す。APIを利用して、プロダクトやソフトウェアを接続することを「API連携」という。

5.6. ユーザーへの周知

身元確認の導入は、事業者だけでなく、ユーザーにも大きく影響します。そのため、導入の必要性やメリットなどを丁寧に伝えることで、ユーザーの離脱を防ぐだけでなく、サービスの信頼性を訴求することに繋がると考えられます。

他方で、ユーザーへの説明や透明性が不十分な場合には、個人情報を提供するユーザーが困惑や不安を感じ、サービスの利用を控えるおそれもあります。

ユーザーへの周知内容（例）

	主な周知内容の項目例
1 **導入の目的**	● なぜ、このサービスに身元確認を導入する必要があるのか。 ● 身元確認を導入することで、ユーザーにどのようなメリットがあるのか。
2 **身元確認手法の説明**	● 身元確認の具体的な手続フロー（動画または画面の遷移があると良い）。 ● 特に、必要とされる本人確認書類と身元確認の所要時間はユーザーの関心が高いため、ウェブサイトのFAQ等で発信することが望ましい。
3 **個人情報の取扱い**	● プライバシーポリシーへの利用目的等の記載は必須。 ● 第三者提供の有無や保存期間なども明示することが望ましい。

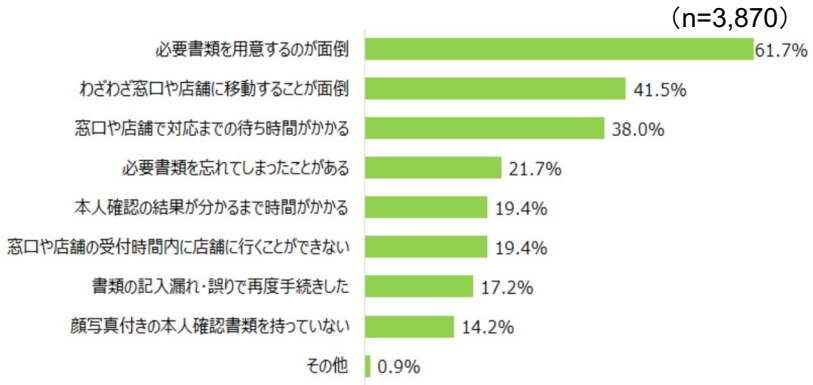
透明性のある説明を行うことが、自社や自社サービスの信頼構築に繋がります。そのため、中・長期的なサービス拡大を目的とし、身元確認を導入する事業者も存在しています。

（参考）本人確認に対するユーザーの意識

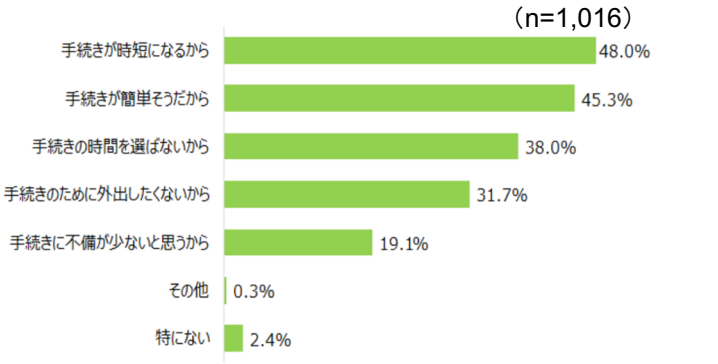
対面や郵送などの本人確認はユーザーが不便を感じる傾向にありますが、デジタル本人確認であれば、ユーザーの不便を解消することが可能です。近年、ユーザーからの要望を踏まえ、デジタル本人確認を導入する事業者も増加しています。

対面での本人確認の課題とデジタル本人確認に感じるメリット

対面での本人確認手続の課題



デジタル本人確認を利用したいと思う理由



デジタル本人確認を活用することで、
ユーザーの利便性と信頼の双方を確保することが可能

出所：TRUSTDOCK, MMD研究所 (2021)「オンライン本人確認（eKYC）に関する利用動向調査」より作成.

（参考）身元確認手続の所要時間の手法別比較

身元確認手続が完了するまでの所要時間は、デジタル化によって短縮されています。

身元確認手法によっては、偽造やなりすましといった不正を防ぐために目視による照合作業などが求められ、身元確認手続の完了までに数時間から数日かかる場合もあります。近年では、デジタル技術の更なる活用により、ユーザーや事業者の所要時間を短縮する手法が検討・導入されています。

デジタル化された身元確認手法における手続完了までに要する所要時間の目安

	アップロード	顔写真付き本人確認書類の表面・裏面・厚みのリアルタイム撮影＋容貌の撮影（ホ方式）	顔写真付き本人確認書類のICチップ読み取り＋容貌の撮影（ヘ方式）	公的個人認証（署名用電子証明書）
ユーザーの情報送信	約30秒	約60秒	約40秒	約20秒
入力情報との一致確認	通常：数分 要確認：数時間	通常：数分 要確認：数時間	通常：数分 要確認：数時間	通常：数分 要確認：数時間
不正等防止のためのチェック	通常：数分 要確認：数時間～数日	通常：数分 要確認：数時間～数日	即時	即時

AIを活用することで、入力情報との一致確認や不正等防止のためのチェックを即時で完了する方式も登場（ホ方式の自動化）

注釈：身元確認手法の詳細は、「9. 主な身元確認手法」以降を参照。

5.7. システム運用・セキュリティ体制の整備

身元確認の導入においては、アプリ等のデジタルツールを用いて大量の個人情報を取得するため、デジタル本人確認に関係するシステムやツールの運用、個人情報の取扱いに対応できる専門的な体制の整備が求められます。

身元確認は、サービスの登録・利用の際の表玄関を担うとともに、サービスの信頼を向上させる役割を果たします。身元確認のトラブルは、サービスの継続に大きな影響を与えてしまうため、適切な体制の構築や、専門事業者への委託等が重要です。

システム運用やセキュリティ担当の主な業務

システムの不具合対応、バージョンアップ対応	● 身元確認のためのシステムに不具合が生じた場合に、迅速かつ適切に対応する。 ● システムのバージョンアップが生じた際に適切に対応する。
システムのデザインや案内画面等の改修	● 身元確認のためのシステムのデザインや案内画面等を定期的に見直し、ユーザーに迷いを生じさせず、希望者が適切に身元確認を完了できるデザインとする。 ● 法令改正等に基づく、利用規約やプライバシーポリシー等の改訂を適切に反映させる。
不正アクセス等の予防	● 不正アクセス等を未然に防止し、個人情報の漏えいを予防する。 ● 社内においても、適切なアクセス権限を付与する等し、不必要な個人情報へのアクセスを防止する。
インシデント（個人データの漏えいを含む）への対応	● 個人情報の漏えい等のインシデント時に、法令等に基づき、迅速かつ適切に対応する。 ● インシデントの影響があるユーザー等に対して、適切に通知等を行う。

注釈：個人情報の取扱いについては、個人情報保護法等の法令に基づく対応が必要（個人情報の取扱いに関する留意点は、「6. 個人情報の取扱い」を参照）。

5.8. 問い合わせ対応の体制整備

身元確認を適切に運営するためには、不正防止・ユーザビリティの双方の観点から、身元確認を円滑に運営できる体制が重要となります。

セキュリティや本人確認に関する専門的な内容に、迅速かつ的確に対応する必要があるため、外部事業者への委託も含め、事前に体制を整備することが求められます。

問い合わせ対応の体制のパターンと主な問い合わせ内容

体制のパターン

パターン1

自社で対応

パターン2

本人確認サービス事業者への委託で対応

パターン3

問い合わせサービス事業者への委託で対応

主な問い合わせ内容の事例

- 本人確認手法が分かりにくい。途中で失敗した。
- 確認審査に通過できなかった理由。
- 確認審査が完了するまでの所要時間、手続の進捗。
- 本人確認書類が改ざんされている可能性がある。
- 不正と思われるIDから申請が届いている。
- 本人確認技術に関する質問。
- 個人情報の取扱いへの懸念。
- サービス全般への意見や会社への意見。

注釈：「主な問い合わせ内容の事例」は、事業者・ユーザー双方からの問い合わせについて、本人確認専門事業者の経験則に基づき、問い合わせの多いものを上に記載。

5. 事業者として留意すべきこと
6. 個人情報の取扱い

6. 個人情報の取扱い

本章では、本人確認において留意する必要がある個人情報の取扱いについて、個人情報保護法の条文を参照しながら概略を説明します。

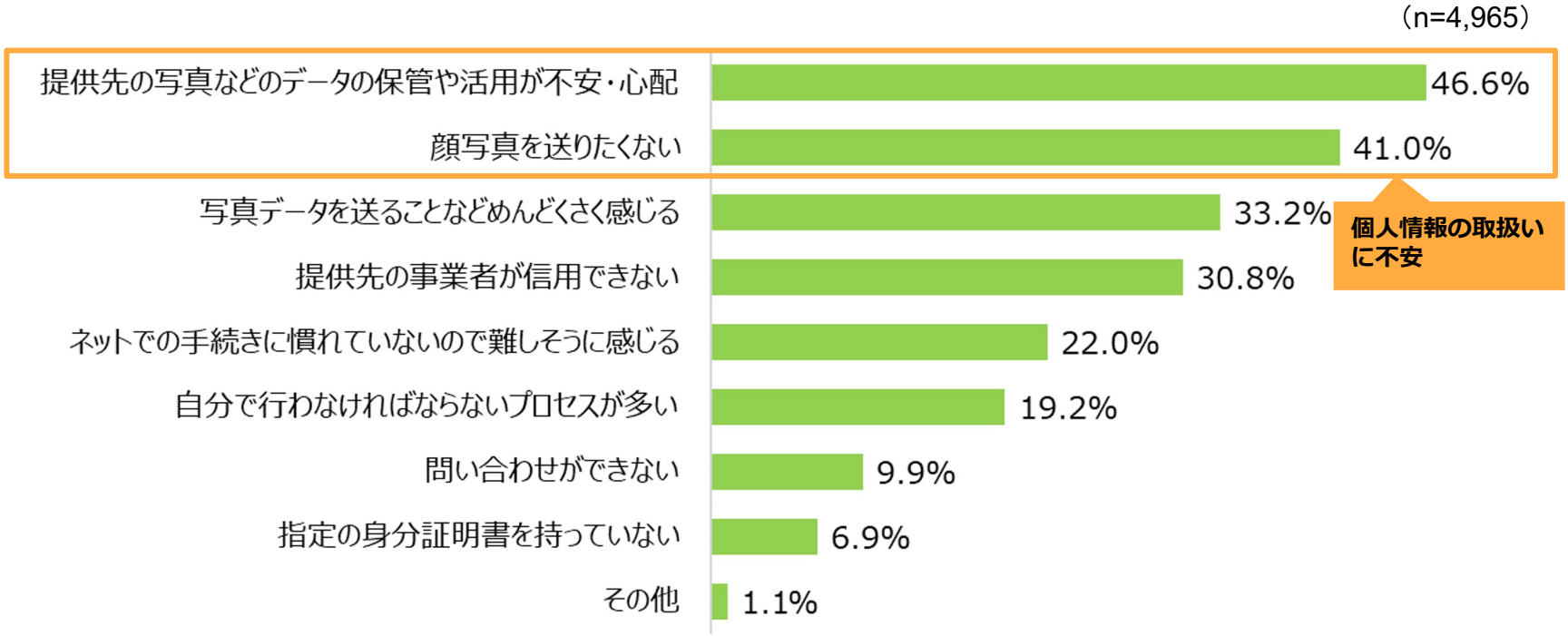
本章のポイント

- オンライン本人確認の未利用者の多くは、個人情報の取扱いに対して懸念を抱いています。本人確認では個人情報を取り扱う必要があることから、デジタル本人確認の導入には、個人情報の取扱いに留意が必要です。
- 個人情報は、情報のライフサイクルや個人情報保護法令等を踏まえ、適切に取り扱うことが重要です。
- 本人確認のために個人情報を取得・利用する場合には、利用目的を特定し、本人が予測・想定できるようにする必要があり、あらかじめ定めた利用目的以外の用途に用いることはできません。
- 個人データの漏えい、滅失又は毀損を防止するために安全管理措置を講じる必要があります。
- 不要となった個人データは速やかに消去する努力義務があるほか、保有し続けることによる漏えいなどのリスクもあります。
- 保有個人データについては、開示、内容の訂正・追加又は削除、利用の停止又は消去への対応が必要です。
- 個人情報の取扱いは、従業員が行うか委託をするかに関わらず、監督責任は各事業者が有しています。

6.1. 個人情報の取扱いに関するユーザーの意識

オンライン本人確認（eKYC）に対する懸念として「個人情報の取扱い」が最も多く、本人確認の導入時には個人情報の取扱いに留意する必要があります。

オンライン本人確認（eKYC）未利用者が持つeKYCに対する懸念等



出所：TRUSTDOCK, MMD研究所 (2021)「オンライン本人確認（eKYC）に関する利用動向調査」より.

（参考）本人確認で取り扱う個人情報

本人確認では、特定の個人に関する情報を収集・検証します。そのため、身元確認・当人認証ともに、取扱情報は個人データに該当し、個人情報保護法に従った管理が必要です。

本人確認において取り扱う個人情報

	主な取扱情報
身元確認	氏名、住所、生年月日、顔写真等、**特定の個人の身元を表す情報**
当人認証	**特定の個人と紐付いた**認証情報（パスワードや電子署名等）

該当

個人情報

生存する個人に関する情報であって、「当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」または「個人識別符号が含まれるもの」

個人データ

個人情報データベース等を構成する個人情報

保有個人データ

個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの以外のもの。

出所：「個人情報の保護に関する法律（平成15年法律第57号）（令和4年10月1日施行）」より.

6.2. 個人情報を取り扱う際に留意すべきこと

個人情報を取り扱う際には、情報のライフサイクルや個人情報保護法令等を踏まえ、適切に取り扱うことが重要です。

情報のライフサイクルと個人情報保護法の対応関係

取得	利用	提供	公表等	消去
● 利用目的の特定（法17条） ● 適正な取得（法20条） ● 取得に際しての利用目的の通知等（21条） ● 第三者提供を受ける際の確認等（法30条）	● 利用目的による制限（法18条） ● 不適正な利用の禁止（法19条）	● 第三者提供の制限（法27条） ● 外国にある第三者への提供の制限（法28条） ● 第三者提供に係る記録の作成等（法29条）	● 保有個人データに関する事項の公表等（法32条） ● 開示（法33条） ● 訂正等（法34条）	● 利用停止等（法35条）

- 理由の説明（法36条）
- 開示等の請求等に応じる手続（法37条）
- 手数料（法38条）

- データ内容の正確性の確保等（法22条）
- 安全管理措置（法23条）
- 従業者の監督（法24条）
- 委託先の監督（法25条）
- 漏えい等の報告等（法26条）
- 苦情の処理（法40条）

注釈：ここでの「法」は「個人情報の保護に関する法律」のこと。

（参考）OECD8原則

OECDが1980年に採択した「OECD8原則」は、世界の個人情報保護法制の規範となっており、個人情報を適切に取り扱うために意識する必要がある原則です。

OECD8原則の内容

目的明確化の原則	収集目的を明確にし、データ利用は収集目的に合致するべき
利用制限の原則	データ主体の同意がある場合、法律の規定による場合以外は、目的以外に利用使用してはならない
収集制限の原則	適法・公正な手段により、かつ、情報主体に通知又は同意を得て収集されるべき
データ内容の原則	利用目的に沿ったもので、かつ、正確、完全、最新であるべき
安全保護の原則	合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護するべき
公開の原則	データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき
個人参加の原則	自己に関するデータの所在及び内容を確認させ、又は異議申立てを保障するべき
責任の原則	管理者は諸原則実施の責任を有する

出所：日本情報経済社会推進協会（JIPEC）「OECD8原則」より.

6.3. 個人情報の取得及び利用時の主な留意事項

本人確認のために個人情報を取得・利用する際には、利用目的を特定し、本人が予測・想定できるようにしつつ、あらかじめ定めた利用目的以外の用途に用いることはできません。

個人情報保護法における利用目的の特定及び利用目的による制限

法第17条

個人情報取扱事業者は、個人情報を取り扱うに当たっては、**その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない**。

法第18条

個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された**利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない**。

法第21条

個人情報取扱事業者は、**個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない**。

本人確認のために個人情報を利用する際には、プライバシーポリシー等で利用目的を示すか、本人に通知等する必要がある

出所：「個人情報の保護に関する法律（平成15年法律第57号）（令和4年10月1日施行）」より.

6.4. 個人データ取扱い時の主な留意事項①

個人データの漏えい、滅失又は毀損を防止するために安全管理措置を講じる必要があります。

個人情報保護法による安全管理措置の概要

法第23条

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の**個人データの安全管理のために必要かつ適切な措置を講じなければならない**。

具体的内容		**基本方針の策定**	事業者の名称、関係法令・ガイドライン等の遵守、安全管理措置に関する事項、質問及び苦情処理の窓口　等
	規律の整備	**組織的安全管理措置**	組織体制の整備、個人データの取扱いに係る規律に従った運用、個人データの取扱状況を確認する手段の整備、漏えい等事案に対応する体制の整備、取扱状況の把握及び安全管理措置の見直し
		人的安全管理措置	従業員の教育
		物理的安全管理措置	個人データを取り扱う区画の管理、機器及び電子媒体等の盗難等の防止、電子媒体等を持ち運ぶ場合の漏えい等の防止、個人データの削除及び機器、電子媒体等の破棄
		技術的安全管理措置	アクセス制御、アクセス者の識別と認証、外部からの不正アクセス等の防止、情報システムの使用に伴う漏えい等の防止
	外的環境の把握		外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等の把握及び個人データの安全管理のために必要かつ適切な措置

出所：「個人情報の保護に関する法律（平成15年法律第57号）（令和4年10月1日施行）」、個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）（令和4年9月一部改正）」より.

6.5. 個人データ取扱い時の主な留意事項②

個人データのメンテナンスの必要性や前項の安全管理措置等を踏まえると、本条にあるように、不要となった個人データは速やかに消去する努力義務があるほか、保有し続けることによる漏えいなどのリスクもあります。

個人データの更新・消去

法第22条

個人情報取扱事業者は、利用目的の達成に必要な範囲内において、**個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない**。

本人確認のために一時的に取得した個人データについては、本人確認完了後*には速やかに削除等する努力義務がある

【参考】GDPRにおけるデータの最小化の原則

GDPRでは、個人データの取扱いの基本原則として「その個人データが取扱われる目的との関係において、十分であり、関連性があり、かつ、必要のあるものに限定されなければならない」と規定されています。このような**不必要な個人情報を保持しないという考え方は、安全管理措置の面からも望ましいといえます。**

注釈：法令等で本人確認に関わる個人情報の保存が定められている場合には、保存年限中は安全管理措置を講じた上で、適切に保存する必要がある。また、本人確認を専門事業者等に委託する場合には、委託先が個人データの収集・保管を行うこととなるが、本条における適切な個人データの消去も含め、委託元が委託先に対する必要かつ適切な監督を行う必要がある。

出所：「個人情報の保護に関する法律（平成15年法律第57号）（令和4年10月1日施行）」、個人情報保護委員会「一般データ保護規則（GDPR）の条文」より.

6.6. 個人データ取扱い時の主な留意事項③

個人データの漏えい等の発生時には、顧客対応だけでなく、個人情報保護委員会への報告等が必要な場合もあることから、不必要な個人情報の保有はリスクであると考えられます。

漏えい等の報告等

法第26条

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって**個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるもの**が生じたときは、個人情報保護委員会規則で定めるところにより、**当該事態が生じた旨を個人情報保護委員会に報告しなければならない**。（略）

2　前項に規定する場合には、個人情報取扱事業者（同項ただし書の規定による通知をした者を除く。）は、**本人に対し、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を通知しなければならない**。（略）

個人の権利利益を害する恐れが大きいもの（個人情報の保護に関する法律施行規則第7条）

- **要配慮個人情報**が含まれる漏えい等
- **財産的被害**が生じるおそれがある漏えい等
- **不正の目的**をもって行われた漏えい等
- **1,000人を超える**漏えい等

- **個人情報保護委員会に報告**
- **本人に対して速やかに通知**

出所：「個人情報の保護に関する法律（平成15年法律第57号）（令和4年10月1日施行）」、「個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号）（令和4年10月1日施行）」より.

6.7. 保有個人データ取扱い時の主な留意事項

保有個人データについては、開示、内容の訂正・追加又は削除、利用の停止又は消去（以上を総称して「開示等」という。）への対応が必要であり、本人確認目的で取得した個人データについても開示等への対応が必要になります。

保有個人データの開示等の請求等

法第33条

本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの電磁的記録の提供による方法その他の個人情報保護委員会規則で定める方法による**開示を請求することができる**。

法第34条

本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの内容が事実でないときは、当該保有個人データの**内容の訂正、追加又は削除（以下この条において「訂正等」という。）を請求することができる**。

法第35条

本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データが第十八条若しくは第十九条の規定に違反して取り扱われているとき、又は第二十条の規定に違反して取得されたものであるときは、当該保有個人データの**利用の停止又は消去（以下この条において「利用停止等」という。）を請求することができる**。

出所：「個人情報の保護に関する法律（平成15年法律第57号）（令和4年10月1日施行）」より.

6.8. 個人データの取扱いにおける責任主体

個人データの取扱いは、従業者が行うか委託をするかに関わらず、監督責任は各事業者が有しています。

従業者及び委託先の監督

法第25条

個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、**当該従業者に対する必要かつ適切な監督を行わなければならない**。

法第26条

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、**委託を受けた者に対する必要かつ適切な監督を行わなければならない**。

自社で本人確認を行う際の従業者に対する監督責任はもちろん、本人確認を委託した場合であっても、監督責任がある。

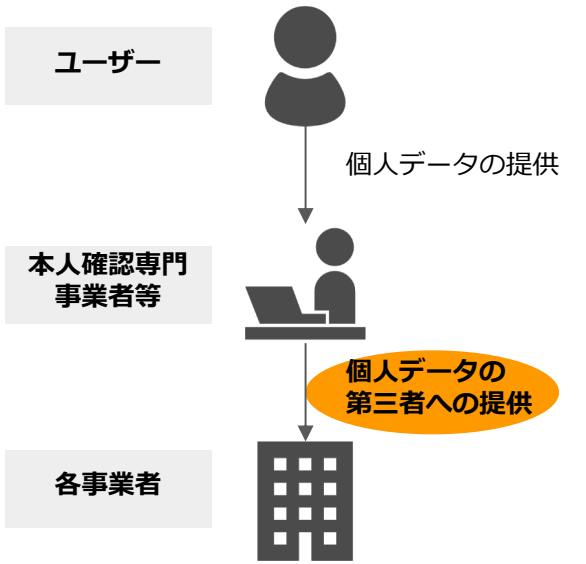
出所：「個人情報の保護に関する法律（平成15年法律第57号）（令和4年10月1日施行）」より.

（参考）個人データの第三者提供

取得した個人データを第三者に提供する場合、原則、事前の同意取得やオプトアウト機会の提供が必要です。また、委託や共同利用等による方法もありますが、いずれにしてもユーザーにとって自身のデータがどこに提供されるかが分かるよう、透明性を持った取扱いが重要です。

個人データを第三者に提供する方法（法第27条関連）

本人確認における個人データの第三者提供のイメージ



個人データを第三者に提供する際の法令での規定

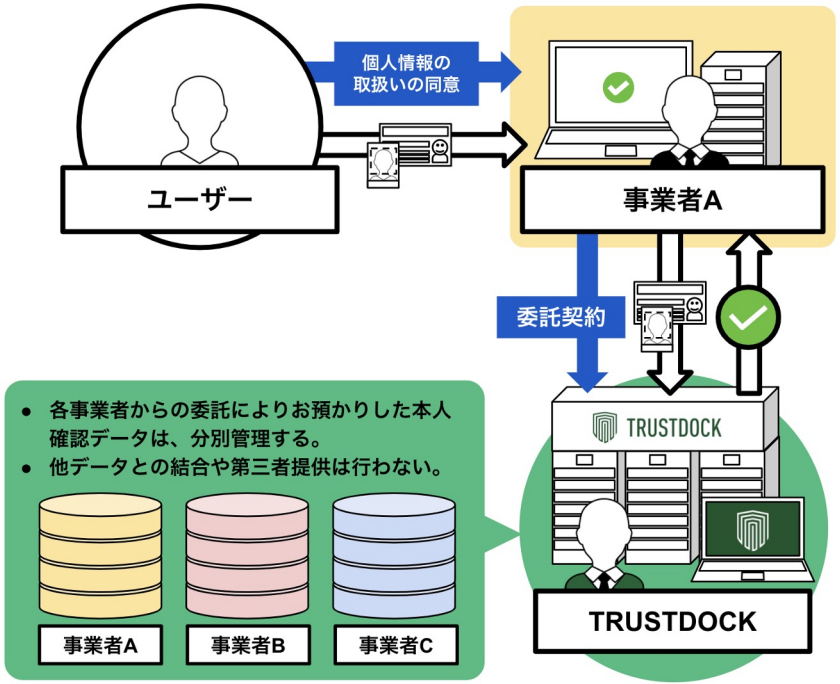
個人データの第三者提供（本人同意に基づく）	あらかじめ本人の同意を得る必要がある。
個人データの第三者提供（オプトアウト）	本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出る必要がある。
委託	利用目的の達成に必要な範囲での委託に限られる。
共同利用	グループ企業等で個人データを利用する場合に限られる。

出所：「個人情報の保護に関する法律（平成15年法律第57号）（令和4年10月1日施行）」より.

（参考）本人確認専門事業者における委託での個人情報の取扱いの事例

本人確認専門事業者は委託により本人確認を行うことが一般的です。その際には、事業者ごとに個人データを分別管理するとともに、他のデータとの結合や委託により取得した個人データの第三者提供等は行いません。

TRUSTDOCKにおける個人情報取扱いの事例



出所：TRUSTDOCK (2021)「アドバイザリーボードからの提言（個人情報の取扱いについて）」より.

Ⅲ　事業者、ユーザーの負担を軽減する中間的な手法

事業者、ユーザーの負担を軽減する中間的な手法

次の2章では、既存の身元確認手法の課題に対応する身元確認手法として、保証レベルとユーザビリティを兼ね備えた「中間的な手法」を2つ紹介します。

7、8章のポイント

- 既存の身元確認手法の中には、目視による照合等が含まれており手続に時間がかかったり、本人確認書類の撮影やICチップ読み取りが上手くできずに、身元確認を完了できないユーザーが一定数存在するという課題があります。
- 法令等で本人確認の定めのない事業者やサービスは、自由に身元確認手法を選択することができ、上述の既存の身元確認手法の課題を解決しうる「中間的な手法」を活用できます。
- 「ホ方式の自動化」については、ユーザーの操作は犯収法ホ方式と変わらないものの、事業者による目視確認をAIで実施することにより、審査完了までのリードタイムを最大10分の1程度まで削減することが可能です。
- 「身元確認結果の活用」は、携帯電話事業者や銀行等の身元確認済みのユーザー情報を活用することで、ユーザーは日頃利用しているアカウントでの当人認証により身元確認を行うことが可能です。

既存の身元確認手法の課題と中間的な手法の考え方

既存の身元確認手法の課題を解決し、事業者・ユーザーの負担を軽減しつつも、リスクへの対応として中間的な強度の手法が登場しています。

中間的な手法の考え方

既存手法の課題

目視による照合等により手続完了まで時間がかかる

本人確認書類等の画像を何度も撮影・送信しなければいけない

事業者・ユーザー負担を軽減する、中間的な手法

AI技術により、犯収法ホ方式[*1]の照合作業を自動化する手法

OpenID Connet[*2]等のID連携技術により、第三者の身元確認結果を利用する手法

OpenID Japan

法令等で本人確認の定めのない事業者は全手続で利用可能

注釈1：「犯収法ホ方式」については、後述の「9. 主な身元確認手法」を参照。
注釈2：OpenID Connectについては、「【コラム】OpenID Connectとは」を参照。

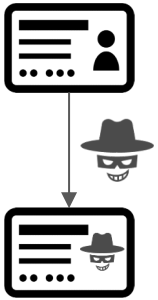
中間的な手法の概要

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

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

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

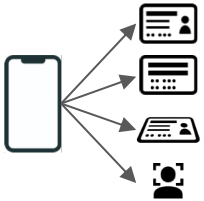
AIの活用で目視審査を省略

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

中間的な手法の特徴

既存の身元確認手法の課題に対応する新たな身元確認手法として、
①AIを活用したホ方式の自動化、②身元確認結果の活用を整理します。

既存の身元確認手法の課題に対応した中間的な手法のメリット

	アップロード リアルタイム撮影	ホ方式の自動化	身元確認結果の活用	犯収法ホ方式
リスク	主な課題 券面偽造やなりすましのリスクが高い	犯収法ホ方式と同様の情報に基づき、券面情報の論理チェックや画像解析等により**一定の精度で券面偽造を見抜くことが可能**	携帯電話事業者や銀行等の身元確認手法の保証レベルに応じた、**正確な氏名・住所・生年月日等の情報を記録できる**	法令に定められている強固な手法
ユーザビリティ	券面画像をアップロード又はその場で撮影するだけでシンプル	ユーザーにとっては**犯収法ホ方式と同様の操作であり、迷いが生じない**	OpenID Connect*等のID連携技術を利用することで、**日常で利用しているアカウントでの当人認証に基づき、簡単に身元確認が可能**	主な課題 券面及び容貌を複数回撮影する必要がある
コスト等	複雑な実装は不要で、コストは安価	バックオフィスにおける目視確認が省略でき、**リードタイムの削減や体制整備等のコスト削減につながる**	**複数回の身元確認を行う必要があるシーンではコスト面での優位性**が生じる	主な課題 自社での体制整備又は専門事業者への委託等のコストが生じる

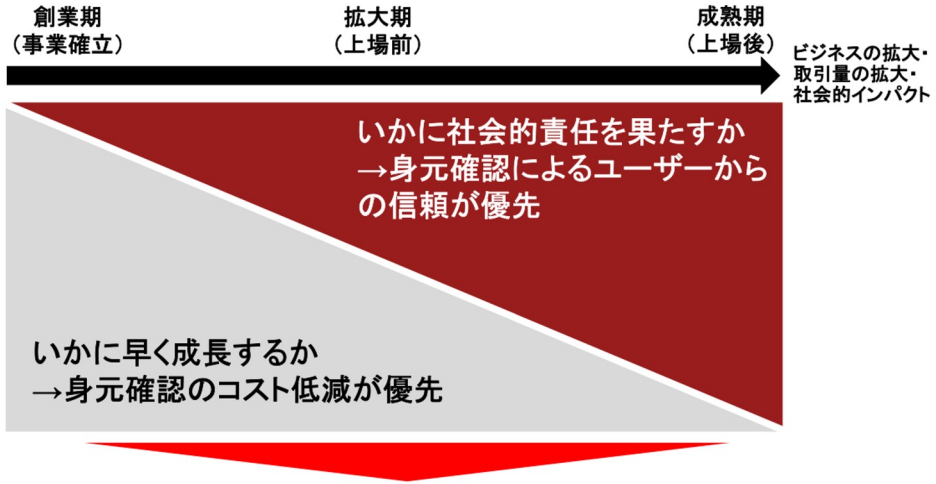
リスクへの強度や情報の最新性は「アップロード」や「リアルタイム撮影」以上、
「犯収法ホ方式」未満と考えられるため、「中間的な手法」と呼称

注釈：OpenID Connectについては、「【コラム】OpenID Connectとは」を参照。

（参考）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」のまとめ

経済産業省の「オンラインサービスにおける身元確認に関する研究会」では、「適度に簡易で信頼性のある」中間強度の手法（≒中間的な手法）の有用性が指摘されています。

中間強度の身元確認手法の活用場面



「簡易で低コストな中間強度の身元確認の手法が普及」することは、全てのステージの事業者にとってメリット

- 簡易で低コストな中間強度の身元確認の手法があれば、創業間もない成長を優先する事業者や、成熟期にあるコストをかけてでも信頼性を優先する事業者など、全ての事業者にとって有用な身元確認手法を提示できる

出所：経済産業省（2020）「オンラインサービスにおける身元確認手法の整理に関する検討報告書」より.

Ⅲ　事業者、ユーザーの負担を軽減する中間的な手法

7．ホ方式の自動化

8．身元確認結果の活用（いわゆる“依拠”）

7.1.「ホ方式の自動化」の背景

ホ方式の自動化手法は、「目視作業を自動化することで本人確認手続を迅速化したい」というニーズに対応できます。

犯収法施行規則6条1項1号ホの要件を満たすためには、以下の照合作業等について目視で対応することとされており、特に事業者にとって審査体制構築等のコストが課題となっている。ホ方式の自動化では、**現時点では犯収法の要件を満たすことはできないが、審査体制構築等のコスト削減が可能**になる。

犯収法ホ方式の概要と目視確認項目

目視で対応されている照合作業等

① 「厚みその他の特徴」の確認

② 顔写真付き本人確認書類の写真と容貌写真の照合

出所：金融庁「参考資料（犯罪収益移転防止法におけるオンラインで完結可能な本人確認方法の概要）」より.

7.2. 「ホ方式の自動化」のメリット

目視確認を省略し機械判定とすることで、審査完了までのリードタイムを最大10分の1程度まで削減することが可能です。

犯収法ホ方式は、導入事業者のオペレーター（BPO含む）による「目視確認（真正性の確認）」が必須。他方で、法令に本人確認の定めの無い身元確認の場合は、導入事業者のリスク許容（セキュリティレベルの判断）に応じて、機械判定のみの自動化が可能。

ホ方式の自動化によるリードタイム削減のイメージ

出所：Liquid社提供資料

7.3. 「ホ方式の自動化」での自動化のポイント

犯収法ホ方式の各ステップの確認をOCR読み取りとAI等による機械判定に基づき確認。
自動化の範囲は各サービスや手続のリスクに応じて適切な範囲で設計可能です。

ホ方式の自動化による自動化のポイント

犯収法ホ方式における人手の審査項目			自動化ポイント
本人確認書類	おもて面・裏面	真正性	撮影画像の券面情報における論理矛盾や、規定デザイン等の形状矛盾を判定する
		有効期限	券面記載の有効期限をOCRにより抽出して判定する
		書類番号	券面記載の書類番号をOCRにより抽出し、規定ロジックに従った番号かどうかを判定する
	斜め面	真正性（厚み部分）	斜めで撮影された書類の厚みを判定する
		おもて面との一致	おもて面と同一の書類かどうかを判定する
本人容貌	本人確認書類「顔写真」との一致		本人確認書類「顔写真」と自撮りの容貌画像が同一かどうかを判定する
livenessチェック時の本人容貌	「正面自撮りの本人容貌」との一致		事前に撮影されたものでないことの確認におけるlivenessチェック時の本人容貌が、自撮りの容貌画像と同一かどうかを判定する
身元情報	氏名・生年月日・住所等の一致		券面記載情報をOCRにより抽出して、自己申告身元情報と一致しているかどうかを判定する。氏名、生年月日等、どこまでの身元情報を参照するかはユースケースによって異なる
センシティブ情報のマスキング			本人確認書類の券面情報に含まれるセンシティブ情報を自動で黒塗りする

出所：Liquid社提供資料

Ⅲ　事業者、ユーザーの負担を軽減する中間的な手法

7. ホ方式の自動化

8. 身元確認結果の活用（いわゆる“依拠”）

8.1. 身元確認結果の活用の背景

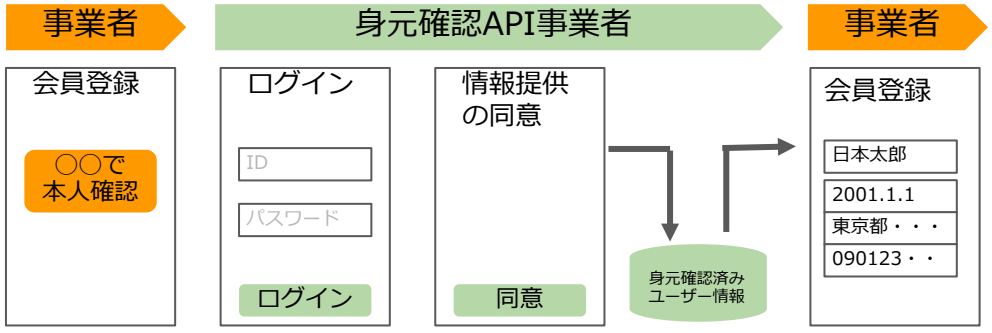
「身元確認結果の活用」は、「携帯電話事業者や銀行等の身元確認済みのユーザー情報を活用して、本人確認を省略したい」というニーズに対応できます。

本人確認書類を用いた身元確認を都度求めることは、ユーザー・事業者の双方にとって負担であり、身元確認導入の阻害要因となっています。身元確認結果の活用では、OpenID Connect*1等のID連携技術を用いて身元確認を行うことができ、本人確認書類の都度の提示は不要となります。

身元確認結果の活用のイメージとメリット

利用イメージ(会員登録)

API事業者とのID連携で取得した身元確認済み情報により身元確認を即時に完了



携帯電話事業者*2	NTTドコモ、KDDI、ソフトバンク
銀行*2	みずほ銀行、三菱UFJ銀行、三井住友銀行、横浜銀行、 十六銀行、福岡銀行、十八親和銀行、肥後銀行、熊本銀行

主なメリット

① ユーザーの操作が簡単
携帯電話事業者や銀行等のID・パスワード、回線認証・暗証番号のみで身元確認が可能

② オンラインで即時に身元確認が可能
本人確認書類の目視確認が不要

③ 本人確認以外の情報も取得
氏名・生年月日・住所に加え携帯電話番号や銀行口座等の情報も取得できる

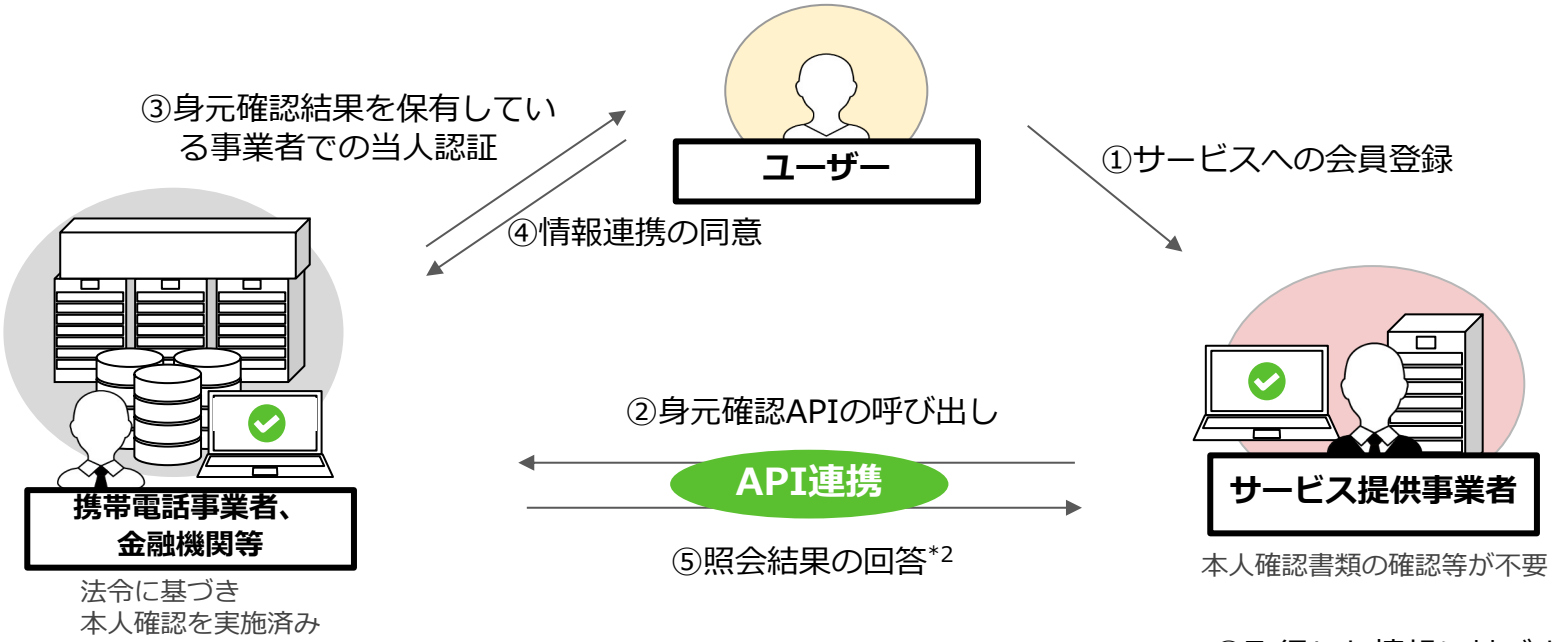
④ ユーザーカバレッジが高い
携帯電話事業者や銀行等が提供している

注釈1：OpenID Connectについては、「【コラム】OpenID Connectとは」を参照。
注釈2：事業者名は2023年2月現在、サービスを提供（又は提供を予定している企業を含む）している事業者の例。

8.2. 身元確認結果の活用の概念図

「身元確認結果の活用」は、OpenID Connect*1等のAPI連携により、ユーザー同意に基づき、自身の過去の身元確認結果を連携する手法です。ユーザーは本人確認書類の撮影等が不要となります。

身元確認結果の活用のイメージ



注釈1：OpenID Connectについては、「【コラム】OpenID Connectとは」を参照。
注釈2：個人情報保護法においては、「個人データの第三者提供」に該当。

8.3. 「身元確認結果の活用」（いわゆる"依拠"）の有用性①

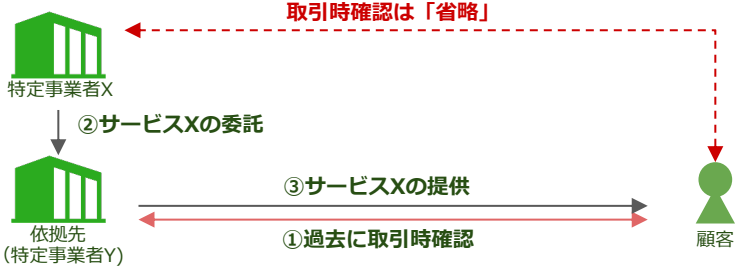
「身元確認結果の活用」の有効性は、厳格な対応が求められる法令でも認識されています。例えば、犯収法は、特定事業者に取引時確認（身元確認）を義務付けていますが、一定の場合に、この義務を軽減することを認める枠組みが設けられています。

犯罪収益移転防止法の例

	通常の取引時確認	他の特定事業者の取引時確認への依拠	
	原則	例外（政令13条）	特例（規則13条）
特定事業者自身（委託含む）での実施	**必要**	**省略**	**簡素化**[*1]
対象となる取引	特定取引**全般**	**金融関係**の特定取引 （口座開設、送金、貸付け、有価証券売買等）	**口座引落・クレカ決済**で決済される一定の特定取引[*2]
依拠先	―	**他の特定事業者** （金融関係の特定取引を扱う事業者）	**他の特定事業者** （銀行、クレジットカード会社）

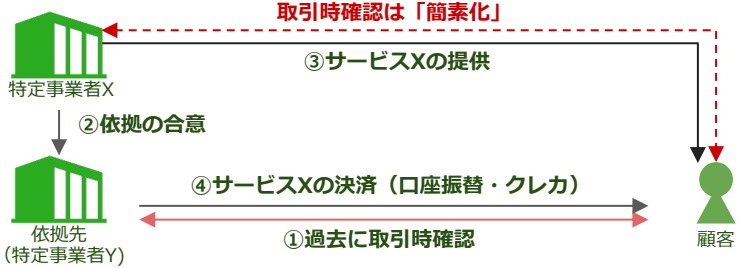
例外

自らのサービス（金融関係取引）の委託先（依拠先）で、過去に別の取引で顧客を取引時確認・記録済の場合



特例

自らのサービスに係る決済（口座振替等）を行う銀行等（依拠先）で、過去に取引時確認・記録済、かつ、依拠することの合意がある場合



注釈1：「特例」は、あくまで取引時確認の方法として、他者の確認結果の活用を認めるもので、義務そのものが免除されるわけではない点に留意。例えば、依拠先の特定事業者が行った本人確認により得られた情報を確認することが必要。また、確認記録の作成義務は免除されない。

注釈2：口座振替等で決済されるものであっても、全ての特定取引ではない点に留意（詳細は法令で列挙）。例えば、特定事業者でも宅建事業者、貴金属売買業者の扱う業務に関する取引などは対象外。

8.4. 「身元確認結果の活用」（いわゆる"依拠"）の有用性②

「依拠」の考え方については、犯収法のベースでもあるFATF勧告の考え方が1つの参考になります。このコンセプトは、法令に定めのない事業者の場合が、「身元確認結果の活用」の安全かつ効果的な実施を検討する際の1つの道標としても有用と考えられます。

FATF勧告の依拠の考え方 （最終的な責任は依拠元の事業者にあることを前提に以下を満たすこと）	法令に定めのない事業者が依拠を検討する場合の考え方の例 （依拠先の本人確認の結果が自社に悪影響を及ぼすことのないよう以下を確保）	
依拠元の事業者が取引時確認（本人確認）情報を速やかに取得する	依拠先からの**本人確認情報のタイムリーな連携**	例）依拠先との間でタイムリーな情報連携の体制は整っているか？（OpenID Connect*やOpenID Connect for Identity Assuranceの実装など）
要請に応じ本人確認書類等の写しを第三者から遅滞なく入手できる	依拠先における**本人確認記録の適切な管理**	例）情報セキュリティの規定等がきちんと整備されているか？
第三者が適切に規制・監督され、取引時確認・記録保存等の義務遵守のための適切な措置を講じることが確保されている	**依拠先の信頼性**（本人確認を適切に実施できるだけの技術・ノウハウ）	例）信頼の置ける実績はあるか？身元確認や当人認証の保証レベルは適切か？

（参考）FATF勧告の考え方を前提とすれば、現在の犯収法の規定（政令13条：金融関係の取引に限定（リース・宅建取引等は対象外）、規則13条（決済方法が口座・カード引落（銀行・クレカ会社）に限定）はやや要件が厳しい面がある。

注釈：OpenID Connectについては、「【コラム】OpenID Connectとは」を参照。
出所：FATF勧告17より.

（参考）犯罪収益移転防止法施行規則ト との違い

身元確認結果を活用する手法として、犯収法施行規則6条1項1号トがありますが、ユーザーが本人確認書類の撮影や読み取りを行う必要がある点等が異なります。

犯収法施行規則ト(1)の概要

本人確認書類情報に記載されている顧客が、他の特定事業者で身元確認済の顧客と同一であることを確認（③）

犯収法施行規則ト(2)の概要

本人確認書類に記載されている顧客の銀行口座が有効（＝他の特定事業者で本人確認済）であることを確認（③, ④）

出所：金融庁「参考資料（犯罪収益移転防止法におけるオンラインで完結可能な本人確認方法の概要）」より.

Ⅳ　サービスに応じた本人確認手法を探す

9、10章では、具体的な本人確認手法を選択するための情報として、「主な身元確認手法」と「主な当人認証手法」のそれぞれ具体的な手法の特徴をまとめています。

その他、附録では、各手法の保証レベルを一覧化し、各保証レベルの具体的な手法を参照しやすいものとした「本人確認手法の保証レベルマッピング」と、シェアリングエコノミー事業者を事例に、現在導入されている身元確認手法・当人認証手法を整理した「サービス別の保証レベルマッピング（事例）」をそれぞれまとめています。

9、10章のポイント

- 身元確認手法の特徴と身元確認手法を選択時の考え方のフレームワークを整理しました。身元確認手法は、自社のサービス・手続等が抱えるリスクを評価し、必要十分な保証レベルの手法の中から、ユーザビリティやコストを踏まえて選択することが重要です。
    - さらに、身元確認を独立して検討するのではなく、サービス・手続の全体と身元確認手続を一体として捉え、適切な手法を選択することが重要です。
- 身元確認手法と比較して、当人認証手法はさらにバリエーションに富んでいますが、その中でも特に主要となる手法の特徴について整理しました。本人確認全体のレベルを向上させるためには、身元確認だけでなく当人認証の保証レベルも意識することが重要です。

Ⅳ　サービスに応じた本人確認手法を探す

9．主な身元確認手法

10. 主な当人認証手法

本章で紹介する身元確認手法の一覧

- 自己申告
- 本人確認書類のアップロード
- 本人確認書類のリアルタイム撮影
- 顔写真付き本人確認書類の表裏のリアルタイム撮影+容貌の撮影
- 犯収法ホ方式
- 犯収法ヘ方式
- 犯収法ト方式
- 公的個人認証（署名用電子証明書）（＝犯収法ワ方式）
- ホ方式の自動化
- 身元確認結果の活用

9.1. 主な身元確認手法とその特徴

		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。

9.2. 自己申告

本人確認書類の確認等を行わずに、ユーザー自身に情報を入力してもらう方式。手軽な反面、虚偽登録も可能であり、正確な個人情報に基づくサービス提供はできません。

自己申告の概要

手順

氏名、住所、生年月日等の必要な情報を自己申告で入力

基本情報

保証レベル	• IAL 1 • DADC IAL 0
本人確認書類	-

主な特徴

1. ウェブサイトでのユーザー登録等、一般的に用いられている。
2. 事業者側の確認作業等のリードタイムが発生しない。

メリット・デメリット

メリット

- ユーザーは、身元確認のためだけの手続が不要であり、負担が軽い。
- 事業者は、身元確認のためだけに自社サービスの提供に不必要な個人情報を取り扱う必要がない。

デメリット

- 登録情報の真偽を確認できないため、正確な情報に基づくサービス提供はできない。
- なりすましを防止することができない。
- 不正等が発生した際に、不正行為を行った本人を特定することが困難。

9.3. 本人確認書類のアップロード

本人確認書類を撮影し、画像としてアップロードする方式。本人確認書類の情報を確認できるものの、偽造やなりすましを防ぐことが困難です。

アップロードの概要

手順

本人確認書類の表面の写真を撮影・アップロード

（必要に応じて）
本人確認書類の裏面の写真を撮影・アップロード

基本情報

保証レベル	• IAL　2 • DADC IAL　1
本人確認書類	マイナンバーカード（表面）、 運転免許証、パスポート、 住民基本台帳カード、在留カード、 特別永住者証明書、 運転経歴証明書、健康保険証　等

主な特徴

1. 様々な種類の本人確認書類 (場合によっては公的身分証以外も含む。) を利用可能。
2. 本人確認書類を所持していれば、暗証番号等を記憶しなくとも利用可能。
3. 事業者側の確認内容によっては、本人確認書類を目視で確認するリードタイムが発生する。

メリット・デメリット

メリット

- 本人確認書類の写真をアップロードするだけであり、ユーザー・事業者ともに本人確認書類を確認する手法の中では最も簡易な手法。
- システム構築等のコストも他の手法と比較して安価。

デメリット

- 本人確認書類画像を加工した後にアップロードが可能なため、偽造リスクが高い。
- 他人の本人確認書類がアップロードされた場合、なりすましを防ぐことができない。

9.4. 本人確認書類のリアルタイム撮影

本人確認書類をリアルタイムで撮影する方式。本人確認書類を確認することができ、画像の加工ができないため一定の偽造対策ができますが、なりすましを防ぐことは困難です。

リアルタイム撮影の概要

手順

本人確認書類の表面の写真を撮影

（必要に応じて）
本人確認書類の裏面の写真を撮影

基本情報

保証レベル	• IAL 2 • DADC IAL 2
本人確認書類	マイナンバーカード（表面）、 運転免許証、パスポート、 住民基本台帳カード、在留カード、 特別永住者証明書、 運転経歴証明書、健康保険証　等

主な特徴

1. 様々な種類の本人確認書類 (場合によっては公的身分証以外も含む。)を利用可能。
2. 本人確認書類と撮影用スマートフォン又はWebカメラ等を所有している必要がある。
3. 事業者側の確認内容によっては、本人確認書類を目視で確認するリードタイムが発生する。

メリット・デメリット

メリット

- ユーザーは本人確認書類を撮影するだけでよく、負担は軽い。
- アップロードと比較して、本人確認書類の撮影画像の加工ができないため、偽造リスクに一定の対応が可能。

デメリット

- 画像の加工を防ぐことができるが、券面偽造のリスクは高い。
- 他人の本人確認書類を撮影する等の、なりすましを見分けられない。
- 撮影用スマートフォンアプリ等の導入が必要。

9.5. 顔写真付き本人確認書類の表裏のリアルタイム撮影+容貌の撮影

顔写真付き本人確認書類の表面・裏面を撮影した後、撮影者の容貌を撮影する方式。券面の偽造やなりすましへの耐性があるものの、厚み撮影*を行わない分、偽造リスクは残ります。

顔写真付き本人確認書類の裏表のリアルタイム撮影＋容貌の撮影の概要

手順

顔写真付き本人確認書類の表面の写真を撮影

顔写真付き本人確認書類の裏面の写真を撮影
（マイナンバーカードは除く）

顔写真の撮影

基本情報

保証レベル	• IAL　2 • DADC IAL　2
本人確認書類	マイナンバーカード、運転免許証、パスポート、住民基本台帳カード、在留カード、特別永住者証明書、運転経歴証明書　等

主な特徴

1. 顔写真付き本人確認書類であれば利用できる(場合によっては公的身分証以外も含む)。
2. 顔写真付き本人確認書類と撮影用スマートフォン又はWebカメラ等を所有している必要がある。
3. 券面画像や顔写真等の確認を目視で行う場合には、ユーザーが申請後、審査期間(通常数時間～数日)を要する。

メリット・デメリット

メリット

- リアルタイム撮影と比較して、券面画像と容貌の画像を突合することが可能であり、身元確認時のなりすましへの耐性が一定ある。
- 犯収法ホ方式と比較して、厚み*撮影が不要であり、ユーザーの撮影の手間を軽減できる。

デメリット

- リアルタイム撮影と比較して、撮影ステップが多く、撮影環境によっては、不鮮明な画像等による否認が発生する。
- 犯収法ホ方式と比較して、厚み*撮影を行わないため、券面の偽造リスクは残る。

注釈：犯収法ホ方式における厚み撮影は、法令の規定では「厚みその他の特徴」から書類の真正性の確認を求めるものであり、必ずしも「厚みの撮影」に限定するものではない。

9.6. 犯収法ホ方式

顔写真付き本人確認書類の表面・裏面・厚み及び撮影者の容貌を撮影する方式。複数回の撮影を経ることで偽造リスクやなりすましへの対応が可能です。一方で、撮影ステップが多いためユーザーの負荷が高く、また、券面の精巧な偽造を見抜くことには限界があります。

犯収法ホ方式の概要

手順

顔写真付き本人確認書類の表面の写真を撮影

顔写真付き本人確認書類の裏面の写真を撮影
（マイナンバーカードは除く）

顔写真付き本人確認書類の厚み*の写真を撮影

顔写真の撮影

基本情報

保証レベル	• IAL　2 • DADC IAL　3
本人確認書類	マイナンバーカード、運転免許証、パスポート、住民基本台帳カード、在留カード、特別永住者証明書、運転経歴証明書　等

主な特徴

1. 犯罪収益移転防止法施行規則に規定されている手法であり、導入事例は多い。
2. 顔写真付き本人確認書類であれば利用可能。
3. 券面画像や顔写真等の確認を目視で行うため、ユーザーが申請後、審査期間 (通常数時間～数日)を要する。

メリット・デメリット

メリット

- 法令に定められている強固な手法。金融機関等でも導入が進んでおり、利用経験のあるユーザーが増加。
- 券面画像と容貌の突合を行うことで、身元確認時の当人性を確認できる。
- 複数の本人確認書類が利用可能であり、本人確認書類を所持していないことによる機会損失が起こりにくい。

デメリット

- 撮影回数が多く、ユーザーへの負担が大きい。
- システムの開発・導入コストやオペレーションコスト等、より簡素な手法と比較してコストがかかる。
- 一定の偽造耐性を有するが、極めて精緻な偽造は見抜くことができないリスクが残る。

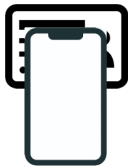
注釈：法令の規定は「厚みその他の特徴」から書類の真正性の確認を求めるものであり、必ずしも「厚みの撮影」に限定するものではない。

9.7. 犯収法ホ方式

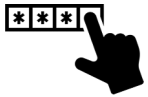
顔写真付き本人確認書類のICチップを読み取り、本人の容貌を撮影。本人確認書類の偽造対策としては最も強固な手法ですが、ユーザーが暗証番号を記憶している必要があります。

犯収法ホ方式の概要

手順



顔写真付き本人確認書類のICチップを読み取る



暗証番号の入力*

顔写真の撮影

基本情報

保証レベル	• IAL 2 • DADC IAL 3
本人確認書類	マイナンバーカード、運転免許証、在留カード、パスポート　等

主な特徴

1. 犯罪収益移転防止法施行規則に規定されている手法。
2. 券面の撮影が不要であり、犯収法ホ方式と比較してユーザーの所要時間が短い。
3. 本人確認書類や顔写真等の確認を目視で行う場合には、ユーザーが申請後、審査期間（通常数時間～数日）を要する。

メリット・デメリット

メリット

- 法令に定められている強固な手法。券面偽造のリスクが極めて低い。
- 券面画像と容貌の突合を行うことで、身元確認時の当人性を確認できる。
- 犯収法ホ方式よりステップが少なく、鮮明な画像を取得できるため、画像の不鮮明等により否認が起こりにくい。

デメリット

- ユーザーがICチップの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。
- 利用できる顔写真付き本人確認書類の種類が少ない。

注釈：マイナンバーカードの場合には、券面に記載の生年月日・有効期限・セキュリティコードを入力。

9.8. 犯収法ト方式

銀行やクレジットカード会社等の他の特定事業者において身元確認を実施済みであることを確認する手法。容貌の撮影が不要ですが、対応サービスが限られます。

犯収法ト方式の概要

手順

事前

あらかじめ銀行口座やクレジットカードを作成

身元確認時

本人確認書類の画像の撮影又はICチップを読み取る

銀行やクレジットカード会社のサイトにログイン

銀行やクレジットカード会社に対し、身元確認済の顧客であることを確認

※ユーザーは意識しない

基本情報

保証レベル	• IAL 2 • DADC IAL 3
本人確認書類	マイナンバーカード、運転免許証、パスポート、住民基本台帳カード、在留カード、特別永住者証明書、運転経歴証明書　等

主な特徴

1. 銀行口座やクレジットカード会社等の他の特定事業者での身元確認に準拠した複数の本人確認書類が利用可能。
2. 銀行やクレジットカード会社のサイトへのログインにより身元確認を行うことができるため、ユーザーの所要時間は短い。
3. 券面画像と連携情報を目視で比較する場合には、事業者のリードタイムが発生する。

メリット・デメリット

メリット

- 法令に定められている強固な手法。
- ユーザーは、銀行口座やクレジットカードで日頃利用しているアカウント情報を利用することで、本人確認書類の撮影等を行わずとも身元確認を行うことができる。

デメリット

- ユーザーがあらかじめ対応している銀行口座やクレジットカードを保有している必要があり、また、対応している事業者が限定されるため、本方式に対応可能な利用者が限定される。

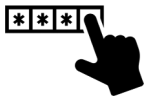
注釈：その他犯罪収益移転防止法施行規則6条1項1号トには、本人確認書類の画像又はICチップ読み取りと顧客名義口座への振込みを組み合わせた方法が規定されている。

9.9. 公的個人認証（署名用電子証明書）（＝犯収法ワ方式）

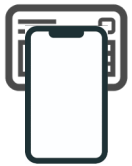
マイナンバーカードの署名用電子証明書を取得する手法。対象書類がマイナンバーカードに限られますが、ユーザーの操作時間が短い上に、偽造耐性が極めて高い特徴があります。また、電子証明書の失効情報を取得することで、最新の情報かどうかを確認することができます。

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。

9.10. ホ方式の自動化

ユーザー体験は犯収法ホ方式と同様ですが、AIを活用することで券面画像や顔写真の目視確認が不要となり、事業者のリードタイムを短縮できます。一方で、撮影環境によっては、犯収法ホ方式と比較して偽造やなりすましの判定精度が下がる場合もあります。

AIを活用したホ方式の自動化の概要

手順

顔写真付き本人確認書類の表面の写真を撮影

顔写真付き本人確認書類の裏面の写真を撮影
（マイナンバーカードは除く）

顔写真付き本人確認書類の厚みの写真を撮影

顔写真の撮影

基本情報

保証レベル	• IAL 2 • DADC IAL 3
本人確認書類	マイナンバーカード、運転免許証、パスポート、住民基本台帳カード、在留カード、特別永住者証明書、運転経歴証明書

主な特徴

1. 券面情報やデザインの矛盾を自動判定するとともに、券面画像と容貌画像との一致を確認することで、一定の不正対策が可能。
2. ユーザーの操作は犯収法ホ方式と同じ。
3. 確認結果は即時に返却されるため、事業者のリードタイムが発生しない。

メリット・デメリット

メリット

- AIを活用することで、券面偽造やなりすましの一定程度の確認が可能。
- 犯収法ホ方式と同様のUIであり、経験あるユーザーの操作に迷いが生じにくい。
- 審査完了までのリードタイムや、目視確認を行うオペレーションコストを大幅に削減できる。

デメリット

- 撮影環境によっては、犯収法ホ方式（目視確認）と比較して偽造やなりすましの判定精度が下がる。
- ユーザー体験は犯収法ホ方式と同じであり、撮影回数が多い等、ユーザー負担は簡素な方式と比較して大きい。

9.11. 身元確認結果の活用

携帯電話事業者や銀行の契約時等の身元確認結果を利用した身元確認が可能です。本人確認書類の撮影や読み取りが不要であり、ユーザにとっては簡単に身元確認を完了できます。

身元確認結果の活用の概要

手順

事前

携帯電話事業者や銀行の口座開設時等に身元確認を行う

身元確認時

身元確認をしたいサイトにアクセス

携帯電話会社や銀行等のサイトにログイン

携帯電話会社や銀行等の身元確認済情報を取得

※ユーザーは意識しない

基本情報

保証レベル	● IAL　2以上 ● DADC IAL　3以上 *携帯電話事業者や銀行等の身元確認レベルに準じる
本人確認書類	マイナンバーカード、運転免許証、パスポート、住民基本台帳カード、在留カード、特別永住者証明書、運転経歴証明書　等

主な特徴

1. 携帯電話事業者や銀行等の身元確認に依拠した手法。
2. 携帯電話事業者や銀行等のアカウント認証に基づく身元確認が可能であり、所要時間が短い。
3. 画像等の目視確認が不要であり、事業者のリードタイムが発生しない。

メリット・デメリット

メリット

- 日常利用しているアカウントの当人認証に基づき、手軽な身元確認が可能。
- 身元確認以外の属性情報も取得可能。
- OpenID Connect等のグローバルな標準技術に基づく方式であれば、拡張性がある。

デメリット

- 転居や結婚等によりユーザーの情報が変更となった場合、ユーザーは再度本人確認書類を用いた身元確認を行う必要がある。
- 比較的新しい手法であり、サービスやプロダクトを提供可能な企業が限られる。

9.12. 身元確認手法候補を選択するための参考フレームワーク

START

法令等で身元確認に関する規定がない
- No → 法令等に基づく身元確認手法を導入
- Yes ↓

サービスの提供に個人情報が必要
- No → 身元確認を行わない
- Yes ↓

本人確認書類に基づいた個人情報が必要
- No → IAL1 (DADC IAL 0)
- Yes ↓

下記のようなリスクを評価

- 人の生命や安全への影響
- 物的損害の多寡
- 金銭的損害の多寡
- 自社の信頼や評判への影響
- 個人情報の漏えい　等

リスクを踏まえ必要な保証レベルを選択

- IAL1 (DADC IAL 0) → 自己申告
- IAL2 (DADC IAL 1,2,3)
- IAL3 (DADC IAL 4)

（参考）本人確認書類の提出方法

- ICチップ読み取り → 犯収法ヘ方式
- 券面の撮影 → 犯収法ホ方式 / ホ方式の自動化 / 券面の裏表＋容貌の撮影 / リアルタイム撮影 / アップロード
- 日頃利用しているアカウントを活用 → 身元確認結果の活用

IAL3 (DADC IAL 4) → 公的個人認証(署名用電子証明書) / マイナンバーカードの機能のスマートフォン搭載(予定)

上記のリスクはあくまで例示であり、業界・業種、企業規模等の実態を踏まえてリスクの分析・評価を行うことが重要です。

また、金銭的損害等については、保険で補償する等の代替手段もあり、身元確認以外の対策も一体として検討することが重要です。

他方で、「人の生命や安全へ影響があるリスク」、「想定被害額が大きいかつ頻度が高いリスク」、「要配慮個人情報を含む個人情報の漏えいリスク」等については、高い保証レベルの身元確認を導入することが望ましいと考えられます。

（参考）身元確認手法候補を選択するための参考フレームワークの考え方

前提

- 前ページの「身元確認手法候補を選択するための参考フレームワーク」は、身元確認手法の候補を選択するための基本的な考え方を示したものであり、このフレームワークを機械的に当てはめ、保証レベルを選択することは望ましくありません。
- IALは高ければ高いほど良いというものではありません。特に、不必要な個人情報を取り扱わないという観点から、自社のサービスや具体的な手続に身元確認が必要かどうかも含め、検討することが重要です。
- 身元確認手法にはそれぞれ保証レベル以外にも、ユーザビリティやコスト等の特徴があります。こうした特徴を踏まえつつ、必要に応じて複数の身元確認手法を導入するなどして、ユーザーが適切に自社サービスにアクセスできるようにすることも重要です。

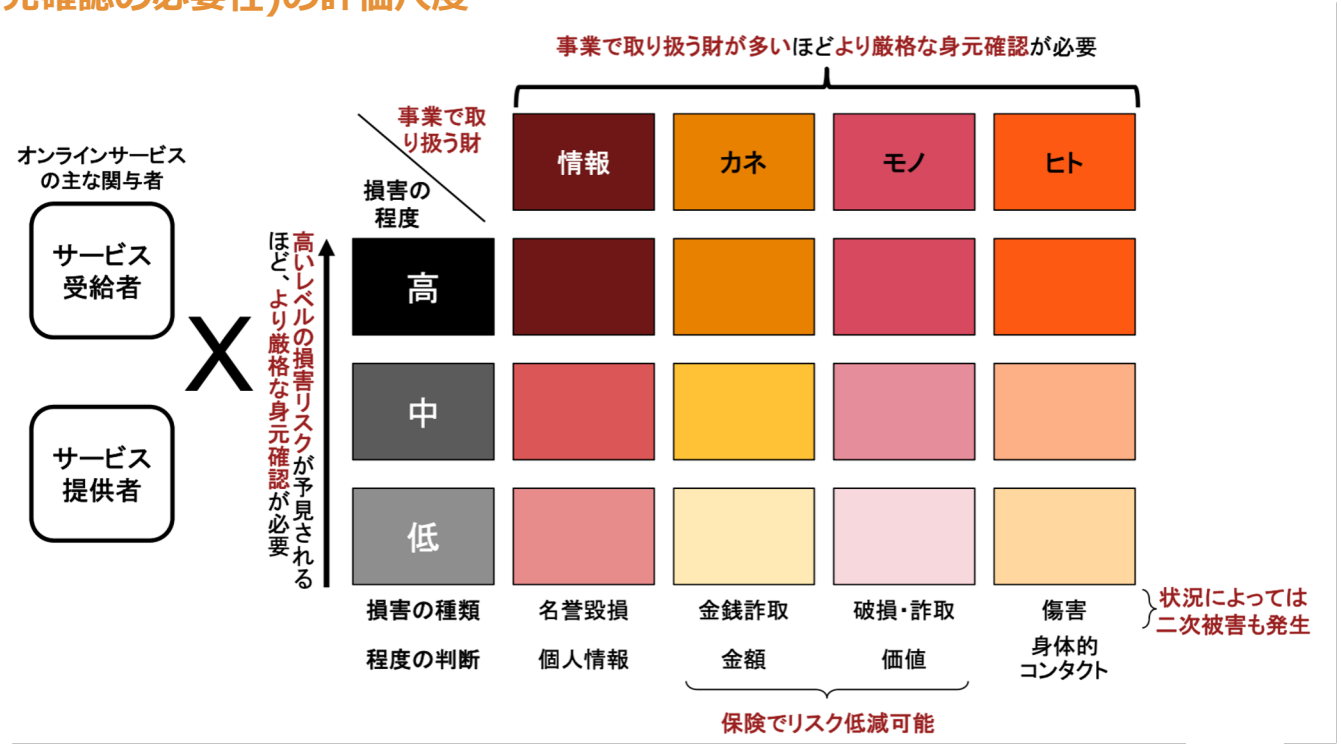
リスクについて

- リスクへの対応を検討する際には、単にIALだけを考慮するのではなく、対象とする脅威に対して適切に対応できていることを確認することが重要です。また、リスクの変化に対応するため、身元確認手法は一度選択した後にも、継続的に見直しを行うことが重要です。
- リスクの分析・評価は一様に行うことができるものではなく、それぞれの事業者が、自社の業界・業種や企業規模等を踏まえ、適切に実施する必要があります。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」では、事業者の自己チェック用に、取引する財に応じてサービス受給者・提供者が被る損害リスクをベースに、身元確認の必要性を評価する尺度を作成しています。
- こうしたリスクの分析・評価については、各業界団体等が当該業界に一般的なリスクについて分析・評価することも有効と考えられます。また、さらに、本フレームワークを各業界に特化したものに改変することで、各事業者が自社の業界特性を踏まえた身元確認手法を簡易かつ適切に選択できることが可能になります。

（参考）事業リスクの判断指標

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」では、事業者の自己チェック用に、取引する財に応じてサービス受給者・提供者が被る損害リスクをベースに、身元確認の必要性を評価する尺度を作成しています。

事業リスク(身元確認の必要性)の評価尺度

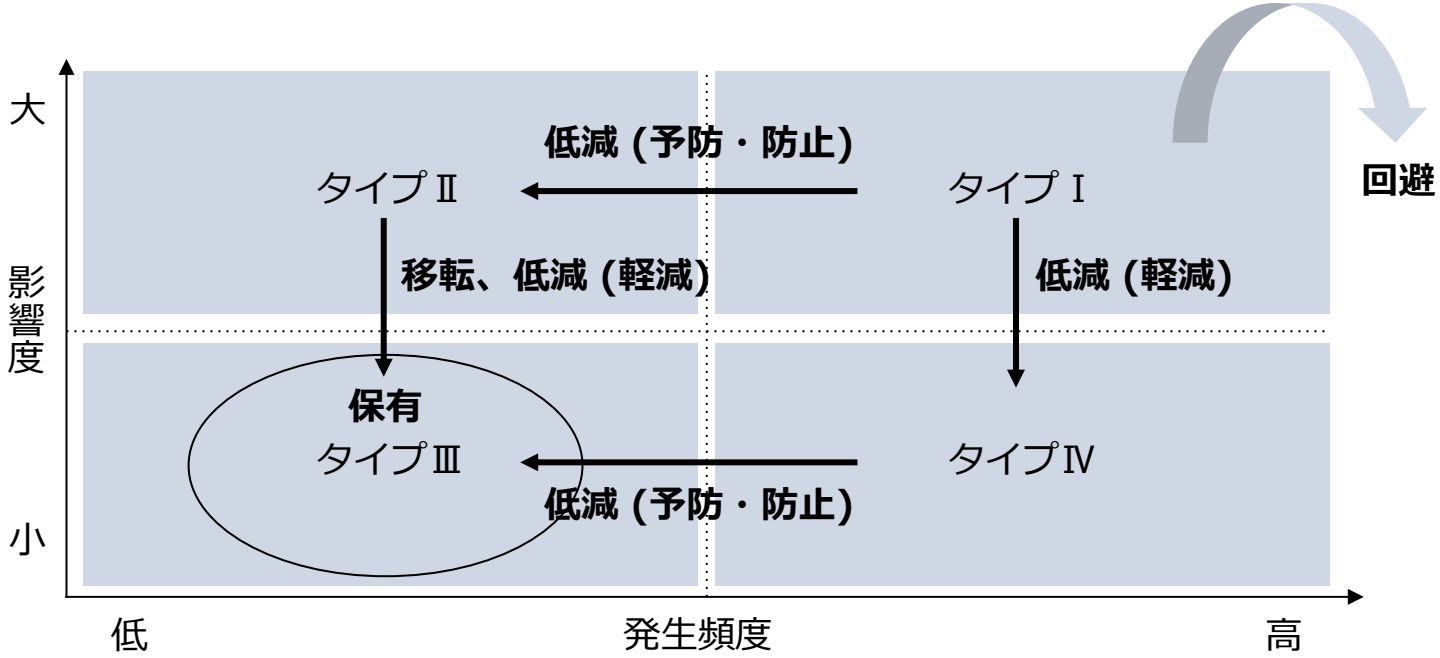


出所：経済産業省（2020）「オンラインサービスにおける身元確認手法の整理に関する検討報告書」より.

（参考）リスクマネジメントにおけるリスク評価の基本的考え方

一般的にリスクマネジメントでは、各リスクを影響度と発生頻度のリスクマップ上にプロットし、各社が優先順位をつけて適切なリスク戦略を選択する必要があります。

リスク戦略の基本的パターン



リスク戦略の例

- 移転:
  損害保険
- 低減(予防・防止):
  本人確認
- 低減(軽減):
  サービスごとに立案
- 回避:
  事業撤退

原出所：経済産業省 (2005)「先進企業から学ぶ事業リスクマネジメント実践テキスト－ 企業価値の向上を目指して －」より
出所：デジタルアーキテクチャ・デザインセンター「第2回インキュベーションラボ　テーマ２：サービスに応じたデジタル本人確認ガイドラインの検討　活動成果報告(詳細版)」より.

（参考）サービスや手続全体を考慮した身元確認手法の選択

ユーザビリティ等を高めるためには、身元確認を独立して検討するのではなく、サービス・手続の全体と身元確認手続を一体として捉え、適切な手法を選択することが重要です。

カーシェアリングにおける身元確認導入の考え方の一例と主なメリット

身元確認手法選択（例）

リスクの判断

- 主要リスクは、車の盗難や破損。金額も大きいため、必要な保証レベルは、IAL2以上。
- 特に、運転免許証が身元確認を行う本人のものであることは、しっかりと確認したい。

ユーザー属性等の特徴の検討

- ユーザーは運転免許を所持していることが前提。
- 運転免許の種類等の情報が必要。
- ユーザーの年齢層は幅広い。

手法候補の選択とネクストアクション

- 運転免許証を利用した、「犯収法ホ方式」又は「ホ方式の自動化」が有力な候補。
- 自社開発かAPI連携化を判断するために、実際のプロダクトの情報を収集する。

主なメリット

ユーザー

- 身元確認を完了できないユーザーを最小化できる。
- 身元確認を通して、必要な運転免許証情報を提出できる。

事業者

- 最低限の手続とすることで、身元確認の導入による機会損失を最小化できる。
- 身元確認を通して必要十分な情報を取得できる。

注釈：以上はイメージであり、本ガイドラインとしてカーシェアリングにおいて特定の身元確認手法を推奨しているわけではありません。

本章で紹介する当人認証手法の一覧

- パスワード
- パスワード及びワンタイムパスワード
- 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（利用者証明用電子証明書）

10.1. 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、事前に身元確認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。

10.2. パスワード

IDに対応するパスワードを入力する方式。パスワードの文字数や内容、使い回し等により リスクへの対応強度が変わります。リスト型攻撃やフィッシングに対応できません。

パスワードの概要

手順

事前登録時

パスワードを登録

認証時

パスワードを入力

基本情報

保証レベル		AAL1
認証要素		記憶
脅威への耐性	リスト型攻撃	×
	フィッシング	×

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一般的。
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。

10.3. パスワード及びワンタイムパスワード

パスワードに加え、別に取得したワンタイムパスワードを入力する方式。不正への強度は高まりますが、フィッシングには対応できないケースもあります。

パスワード及びワンタイムパスワードの概要

手順

事前登録時

パスワードを登録

電話番号やメールアドレス等を登録（送達確認を行う）

認証時

パスワードを入力

SMSやEメール等で受信したワンタイムパスワードを入力

基本情報

保証レベル		AAL2
認証要素		記憶 + 所持
脅威への耐性	リスト型攻撃	○
	フィッシング	×

主な特徴

1. 2要素認証の中ではよく使われており、金融機関へのログイン等でも一般的。
2. ワンタイムパスワードを受信できる環境が必要。
3. リスト型攻撃には対応できるが、フィッシングには対応できないケースがある。

メリット・デメリット

メリット

- 携帯電話番号やメールアドレスを所持していれば利用可能であり、特別な機器等は不要。
- 既存のパスワードに追加で導入可能であり、他の2要素認証手法と比較して導入が手軽。

デメリット

- パスワードと比較して入力回数が多いため、ユーザーの負担は増える。
- パスワードを記憶しており、かつ、ワンタイムパスワードを受信できる環境でしか利用できない。
- ワンタイムパスワードの送信方法により、なりすましリスクに差がある*。

注釈：例えば、自己申告で取得可能なフリーメールアドレスと身元確認が行われたSMSでは、なりすましリスクに差があると考えられる。

10.4. パスワードレス生体認証（FIDO認証）

端末の生体認証を用いた方式。ユーザー体感は生体認証ですが、2要素認証です。
ただし、事前に生体情報の登録作業が必要なほか、端末の変更時の再登録等が必要です。

パスワードレス生体認証（FIDO認証）の概要

手順

事前登録時

生体情報を登録
（生体情報は端末内に保管）

秘密鍵・公開鍵を生成し、
認証用サーバーに保存

※ユーザーは意識しない

認証時

生体認証

生体

秘密鍵による署名データを
公開鍵を用いて検証

所持

※ユーザーは意識しない

基本情報

保証レベル		AAL2[*1]
認証要素		生体[*2] + 所持
脅威への耐性	リスト型攻撃	○
	フィッシング	○

主な特徴

1. パスワード等を記憶する必要がなく、あらかじめ登録したスマートフォンアプリまたはブラウザがあれば認証可能。
2. 秘密鍵の管理場所等により保証レベルが変動するが、一般的にAAL2以上。
3. リスト型攻撃・フィッシングに対応可能。

メリット・デメリット

メリット

- 脅威への耐性とユーザーの利便性を兼ね備えている。
- リスト型攻撃及びフィッシングという当人認証の主要な脅威に対応できる。
- 近年では、パスキー等の利便性を向上させた仕組みが登場している。

デメリット

- 秘密鍵を厳格に管理する必要があり、端末紛失時等のアカウントリカバリが課題となる。
- パスワードレス生体認証が成功しない場合のフローを定める必要がある。
- 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。

注釈1：ここでの保証レベルは代表的な例であり、実際の保証レベルはプロダクトや実装の方法により異なる。
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。

10.5. セキュリティキー認証（FIDO認証）

セキュリティキーに生体情報やパスワードなどの第2要素を組み合わせた方式。物理デバイスを併用し高い保証レベルを担保できます。一方、ユーザーは事前にセキュリティキーを入手する必要があります。

セキュリティキー認証（FIDO認証）の概要

手順

事前登録時

- セキュリティーキーを登録
- 生体情報やパスワードを登録
- 秘密鍵・公開鍵を生成し、認証用サーバーに保存

※ユーザーは意識しない

認証時

- 生体情報やパスワード認証
- セキュリティーキーで認証
- 秘密鍵による署名データを公開鍵を用いて検証

※ユーザーは意識しない

基本情報

保証レベル		AAL3*1
認証要素		生体*2 + 所持(耐タンパ)
脅威への耐性	リスト型攻撃	○
	フィッシング	○

主な特徴

1. セキュリティキーを含む2要素認証で、最高レベルの保証レベルの認証が可能
2. AAL3を達成するためには、AAL3の要件を満たしたセキュリティキーを使用する必要がある。
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。
- 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。

注釈1：ここでの保証レベルは代表的な例であり、実際の保証レベルはプロダクトや実装の方法により異なる。
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。

10.6. 公的個人認証（利用者証明用電子証明書）

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。最高の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。

公的個人認証（利用者証明用電子証明書）の概要

手順

事前登録時

マイナンバーカードを発行
(同時に電子証明書も発行)

認証時

利用者証明用電子証明書
暗証番号(数字4文字)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		AAL3
認証要素		知識 ＋ 所持(耐タンパ)
脅威への耐性	リスト型攻撃	○
	フィッシング	○

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最高の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

- 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。
- 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。また、利用者証明用電子証明書パスワードを記憶している必要がある。
- 署名検証者が限られており、システム連携が必要。

注釈：利用者証明用電子証明書を当人確認に利用する場合は、別途身元確認を行い利用者証明用電子証明書とユーザー情報を紐づけておく必要がある。

V　おわりに

V　おわりに

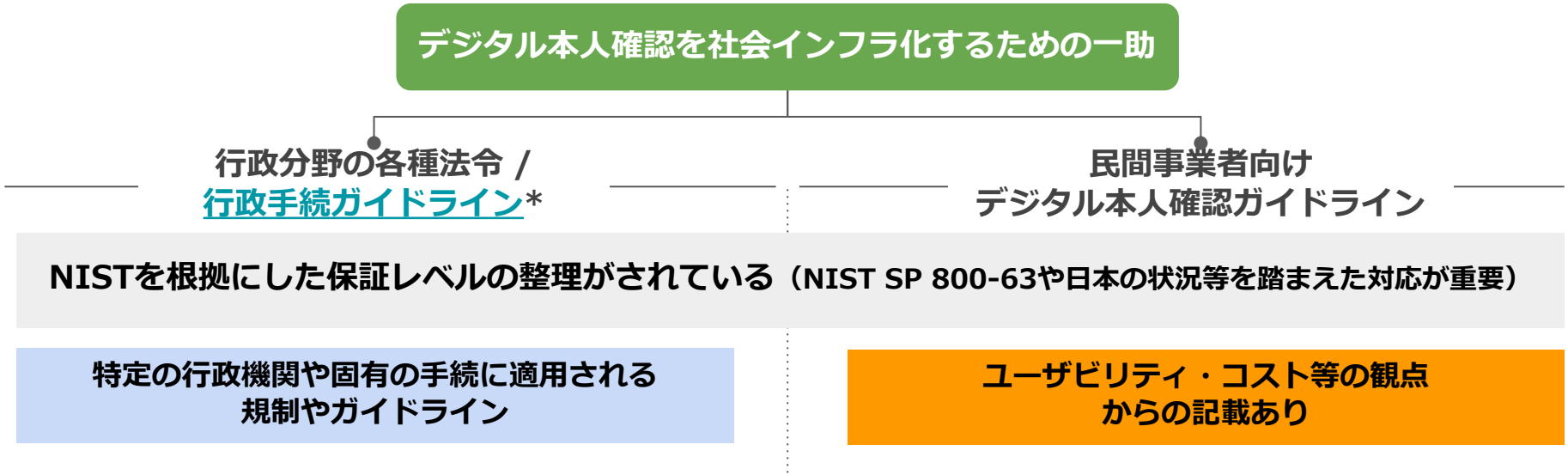
11. 行政分野における本ガイドラインの活用
12. 事業者団体等における本ガイドラインの活用
13. 本ガイドラインの今後の更新等について

11. 行政機関における本ガイドラインの活用について

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。

V　おわりに

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
13. 本ガイドラインの今後の更新等について

12.1. 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「【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。

12.2. 事業者団体等における本ガイドラインの活用

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「【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。

V　おわりに

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
13. 本ガイドラインの今後の更新等について

13. 本ガイドラインの更新等について

現在、NIST SP 800-63-4の改訂が検討されており、本ガイドラインも当該改訂に対応した更新を予定しております。

その他テクノロジー、社会情勢の変化や皆様からのご意見等も踏まえ適宜更新を重ねてまいります。

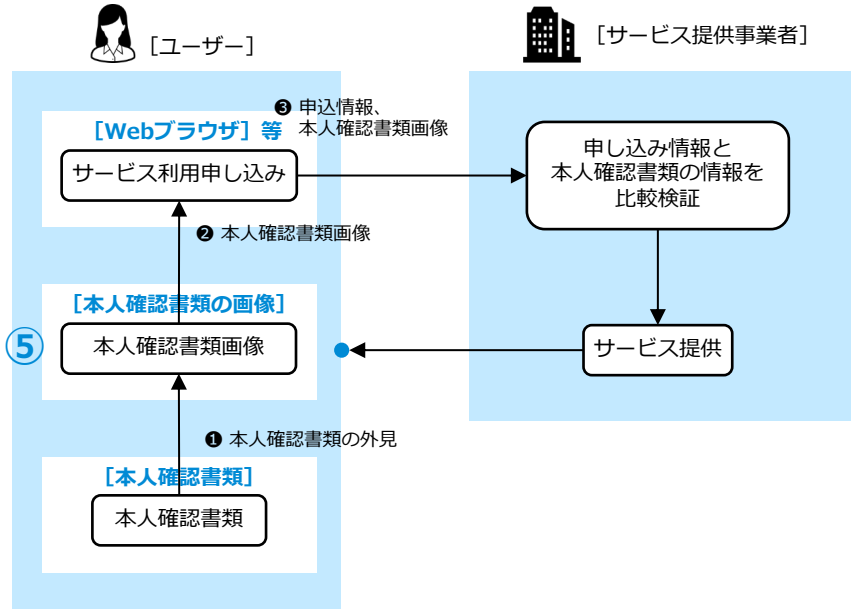
附録目次

DADC IALの詳細

DADC IALのレベル間の外形的な違い　①DADC IAL1

偽造やなりすましのリスクはありますが、本人確認書類に基づいた身元確認を行うことができます。

アップロードの事例



<凡例>
：機能　：プロセス、情報の流れ　（白色青字オブジェクト含む）：責任範囲

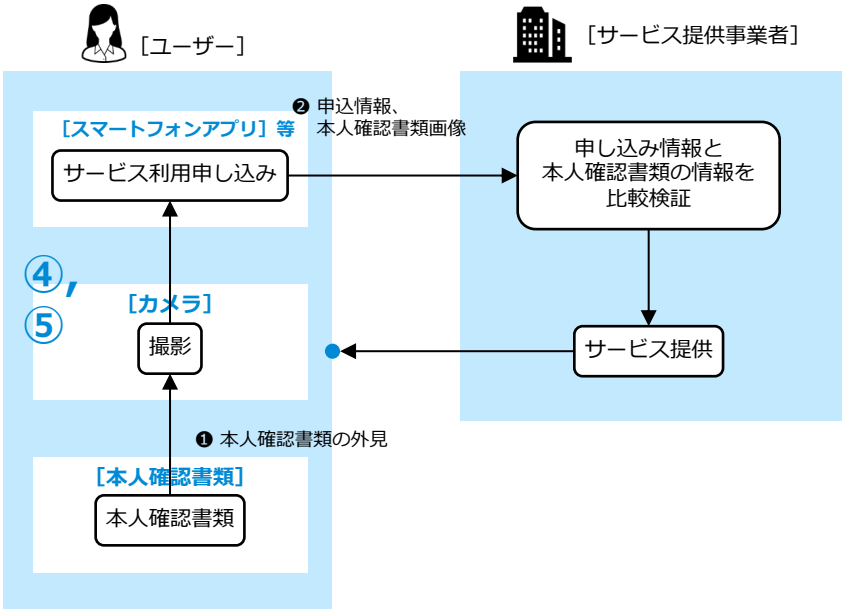
今回の整理におけるIAL間の外形的な差異項目	有／無	有無の理由等、備考	DADC IAL
① 現況確認	無		DADC IAL4
② エビデンス確認対象	無		-
③ 偽造不正対策	無	罫線位置等、本人確認書類の外見的特徴を検査することにより、対策を実施している場合もあり。	DADC IAL3
④ 本人確認書類の所持確認	無		DADC IAL2
⑤ 本人確認書類	有	本人確認書類の画像データで確認。	**DADC IAL1**

出所：デジタルアーキテクチャ・デザインセンター（2022）「第2回インキュベーションラボ　テーマ２：サービスに応じたデジタル本人確認ガイドラインの検討　活動成果報告(詳細版)」より作成.

DADC IALのレベル間の外形的な違い　②DADC IAL2

偽造やなりすましのリスクはありますが、身元確認時に当該本人確認書類を所持していることを確認できます。

リアルタイム撮影の事例



<凡例>
：機能　：プロセス、情報の流れ　（白色青字オブジェクト含む）：責任範囲

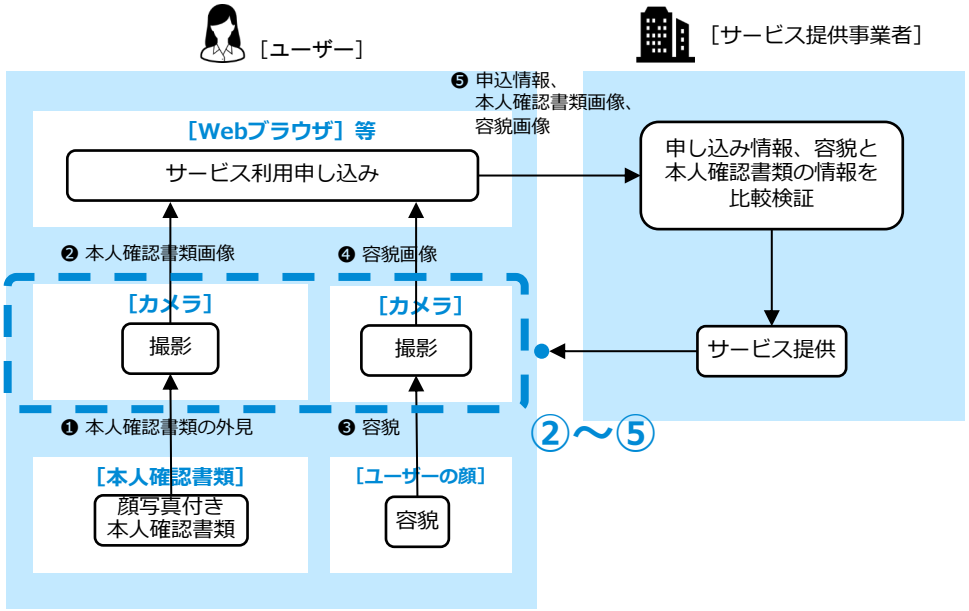
今回の整理におけるIAL間の外形的な差異項目	有/無	有無の理由等、備考	DADC IAL
① 現況確認	無		DADC IAL4
② エビデンス確認対象	無		-
③ 偽造不正対策	無	罫線位置等、本人確認書類の外見的特徴を検査することにより、対策を実施している場合もあり。	DADC IAL3
④ 本人確認書類の所持確認	有	リアルタイム撮影により、ユーザーが身元確認時に本人確認書類を所持していることを確認。	**DADC IAL2**
⑤ 本人確認書類	有	本人確認書類の画像データで確認。	DADC IAL1

出所：デジタルアーキテクチャ・デザインセンター（2022）「第2回インキュベーションラボ　テーマ２：サービスに応じたデジタル本人確認ガイドラインの検討　活動成果報告(詳細版)」より作成.

DADC IALのレベル間の外形的な違い　③DADC IAL3

犯収法要件に準拠する等により、本人確認書類が偽造されていないことを確認できます。

犯収法ホ方式の事例



<凡例>
：機能　：プロセス、情報の流れ　（白色青字オブジェクト含む）：責任範囲

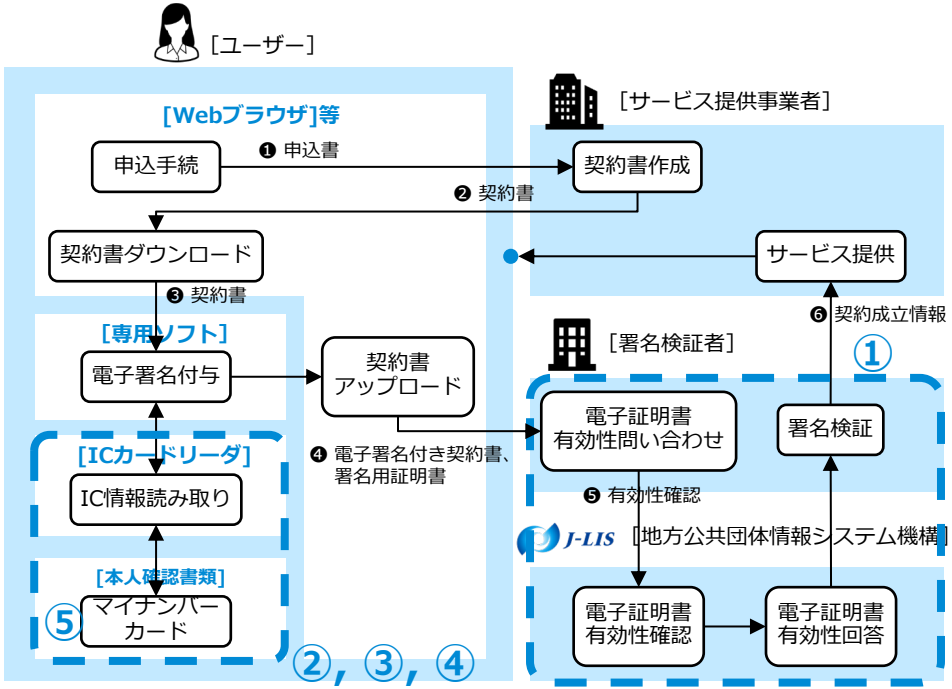
今回の整理におけるIAL間の外形的な差異項目	有/無	有無の理由等、備考	DADC IAL
① 現況確認	無		DADC IAL4
② エビデンス確認対象	有	本人確認書類と容貌画像を比較検証することで、顔写真付き本人確認書類とユーザーの紐づけを確認。	-
③ 偽造不正対策	有	顔写真付き本人確認書類の表、裏、厚み確認等、犯収法要件に準拠し対策。	**DADC IAL3**
④ 本人確認書類の所持確認	有	リアルタイム撮影により、ユーザーが身元確認時に本人確認書類を所持していることを確認。	DADC IAL2
⑤ 本人確認書類	有	顔写真付き本人確認書類の画像データで確認。	DADC IAL1

出所：デジタルアーキテクチャ・デザインセンター（2022）「第2回インキュベーションラボ　テーマ２：サービスに応じたデジタル本人確認ガイドラインの検討　活動成果報告(詳細版)」より作成.

DADC IALのレベル間の外形的な違い　④DADC IAL4の間

電子証明書の失効確認により、最新の氏名・住所・生年月日等であること（≒現況確認）が確認できます。

公的個人認証（署名用電子証明書）+電子署名付契約書の事例



<凡例>
：機能　：プロセス、情報の流れ　（白色青字オブジェクト含む）：責任範囲

今回の整理におけるIAL間の外形的な差異項目	有/無	有無の理由等、備考	DADC IAL
① 現況確認	有	総務省認定事業者経由でJ-LISへ電子証明書の有効性を確認。	**DADC IAL4**
② エビデンス確認対象	有	署名用パスワードの入力により、マイナンバーカードとユーザーの紐付けを確認	-
③ 偽造不正対策	有	マイナンバーカードのICチップに耐タンパ性あり。	DADC IAL3
④ 本人確認書類の所持確認	有	ICチップ読み取りにより、ユーザーが身元確認時にマイナンバーカードを所持していることを確認。	DADC IAL2
⑤ 本人確認書類	有	マイナンバーカードの署名用電子証明書で確認。	DADC IAL1

出所：デジタルアーキテクチャ・デザインセンター（2022）「第2回インキュベーションラボ　テーマ２：サービスに応じたデジタル本人確認ガイドラインの検討　活動成果報告(詳細版)」より作成.

本人確認に関わる法令等（詳細）

本人確認の法令での義務付けは、国際的なマネー・ロンダリング対策を契機とした金融機関への要請が端緒。その後、様々な領域で重要性が認識され、今日では、実施を義務付ける法律が複数存在するに至っています。

本人確認の法令での義務化の主な経緯

FATF「40の勧告」	**1989年、マネロン対策の国際協力のための会議体、FATF（金融活動作業部会）が発足。** **1990年、FATFが、各国が実施すべき対策の基準「40の勧告」を策定。** - 必要な国内法制の整備、金融機関による顧客の本人確認、疑わしい取引報告等を要請
大蔵省通達	**1990年、大蔵省（当時）が、金融機関に対し本人確認の実施を要請する通達を発出。** - あくまで行政指導として本人確認を求めるもの（根拠となる法令は未整備）
FATF「特別勧告」	**2001年、米国同時多発テロ事件を受け、FATF「特別勧告」が策定。** - 組織的犯罪に加え、テロ資金供与もマネロン対策の対象に。
本人確認法	**2003年、「本人確認法」が施行*。** - 通達により行われていた金融機関の本人確認が「法律上の義務」として位置づけられる - 外為法も改正され、海外送金等の際の本人確認が同法でも義務化
FATF勧告改訂	**2003年、マネロン犯罪傾向の変化等を踏まえ、FATF勧告を改訂** - 本人確認等の措置を講ずべき事業者の範囲を非金融業者・職業専門家にも拡大
犯罪収益移転防止法	**2008年、本人確認法と組織犯罪処罰法の一部を母体として制定された「犯罪収益移転防止法」が施行。** - FATF勧告改訂に合わせ本人確認義務の対象となる事業者が拡大 - 複数の法律でまたがって課されていた義務が同法に一元化

注釈：正式名称は「金融機関等による顧客等の本人確認等に関する法律」

本人確認を取り巻く規制面の動向

犯収法など国内ルールは、FATFを中心とする国際的議論の動向等を踏まえ、見直しが検討・実施される流れが一般的です。近年、マネロン対策の高度化を求める議論が高まりを見せており、これに伴い、本人確認に関連する国内の規制も年々厳格化する傾向にあります。

本人確認を含む法令等の厳格化の潮流

FATF等における背景

FATFの国際議論

- テロ情勢等を背景とする金融制裁措置（犯罪リスク増加）
- 暗号資産等の違法活動への利用懸念（ランサムウェア等）
- 各国の基準遵守レベルの底上げの必要性　等

FATF第4次対日相互審査

- 当局の監督強化・事業者の取組の高度化
- 新技術（暗号資産等）への対応
- マネロン等対策強化のため必要な法改正　等

国内の金融機関等を取り巻く状況

- 決済手段の多様化
- 非対面取引の拡大
- 疑わしい取引の届出の増加　等

本人確認にも関係する規制動向の例

取引時確認義務の対象拡大	**法令に基づく本人確認が必要な場面の増加** ● これまで、カジノ事業*1、暗号資産交換業*2、いわゆるステーブルコイン、高額電子移転可能型前払式支払手段の取扱い*3などが新たに犯収法の対象に追加
継続的顧客管理*4の徹底	**随時・定期的な本人確認の必要性** ● 当局による期限（2024年3月末）までの実施態勢整備の慫慂など

注釈1：改正犯罪収益移転防止法によりカジノ事業者が特定事業者に追加（令和3年7月施行）
注釈2：改正犯罪収益移転防止法により暗号資産交換業者が特定事業者に追加（平成29年4月施行、令和元年5月改正で、仮想通貨交換業者から暗号資産交換業者に名称変更）
注釈3：令和4年資金決済法等改正により、電子決済手段等取引業者、高額電子移転可能型前払式支払手段の届出事業者が特定事業者に追加（公布日（令和4年6月10日）から1年以内施行予定）
注釈4：金融庁「マネロン・テロ資金供与対策ガイドライン」において、契約時のみならず、各顧客のリスクが高まったと想定される具体的な事象が発生した場合等の機動的な顧客情報の確認、及び、定期的な顧客情報について、確認の頻度を顧客のリスクに応じ異にして実施することが求められている（必要な実施態勢の整備について、2024年3月末までの期限が設けられている）。

犯罪による収益の移転防止に関する法律

犯罪収益移転防止法は、マネー・ロンダリング等の防止の観点から、金融機関等の一定の事業者に対し、マネー・ロンダリング等のおそれの高い一定の類型の取引について、顧客の本人確認義務を課しています。

本人確認の枠組み

〈主体〉	〈フェーズ〉	〈確認事項〉
特定事業者	**特定取引**	**本人特定事項の確認** （氏名、住所、生年月日）
・金融関連事業者 ・ファイナンスリース業者 ・クレジットカード事業者 ・宅地建物取引業者 ・貴金属等取扱事業者 ・電話転送サービス業者 ・士業者 ・カジノ事業者　等	・預貯金契約 ・現金送金（10万円超） ・保険契約 ・証券取引 ・クレジットカード契約 ・宅地建物の売買 ・宝石・貴金属売買（200万円超） ・カジノのチップの販売換金　等	犯収法の本人確認は「取引時確認」と呼ばれ、 ● 本人特定事項の確認に加え、 ● 取引目的、職業、（高リスク取引の場合は）資産・収入の状況等の確認も必要

利用できるオンライン完結の本人確認手法

容貌＋本人確認書類（写真付）の画像
（犯収法ホ）

容貌＋本人確認書類（写真付）のICチップ情報
（犯収法ヘ）

本人確認書類の画像/ ICチップ＋銀行・クレカ情報照合/ 口座振込み
（犯収法ト）

公的個人認証
（犯収法ワ）

民間事業者発行の電子証明書*1
（犯収法ヲ・カ）

注釈1：電子署名法の認定認証事業者、公的個人認証法の認定を受けた署名検証者が発行する電子証明書が規定されている。
注釈2：上記の手法は、本人確認の相手方が個人である場合の手法を掲載。

携帯電話不正利用防止法は、携帯電話が振り込め詐欺等の犯罪に利用されることを防止するため、携帯電話事業者に対し、契約者の本人確認義務を課しています。

本人確認の枠組み

〈主体〉

- **携帯電話事業者**（MVNO含む）
- **契約（販売）代理店**[*1]
- **レンタル携帯電話事業者**

▶

〈フェーズ〉

役務提供契約の締結時
（譲渡（名義変更）時も含む）

▶

〈確認事項〉

本人特定事項の確認
（氏名、住所、生年月日）

利用できるオンライン完結の本人確認手法

容貌＋本人確認書類（写真付）の画像
規則[*2]3条1項1号ハ
（犯収法ホの手法に類似）

容貌＋本人確認書類（写真付）のICチップ情報の送付
規則3条1項1号二
（犯収法への手法に類似）

電子証明書（公的個人認証・民間事業者発行）[*3]
規則3条1項1号チ
（犯収法ワ・ヲの手法に類似）

注釈1：携帯電話通信事業者は代理店に本人確認を行わせることが可能だが、代理店に関して監督責任を負う。
注釈2：上記の図の「規則」は、「携帯電話不正利用防止法施行規則」を指す。
注釈3：公的個人認証サービスの署名用電子証明書に加え、民間事業者（電子署名法の認定認証事業者）が発行する電子証明書が規定されている。
注釈4：手法は本人確認の相手方が個人である場合の手法を掲載。

古物営業法

古物営業法は、盗品等の売買の未然防止等のため、古物[*1]の売買を取り扱う事業者に対し、取引相手の本人確認義務を課しています。

本人確認の枠組み

〈主体〉	〈フェーズ〉	〈確認事項〉
古物商	**取引金額が1万円以上[*2]の古物取扱い** ・古物を買い受ける場合 ・古物の交換を行う場合 ・古物の売却・交換の委託を受ける場合	**本人特定事項の確認** （住所、氏名、職業、年齢）

利用できるオンライン完結の本人確認手法

容貌＋本人確認書類（写真付）の画像
規則[*3]15条3項8号
（犯収法ホの手法に類似）

容貌＋本人確認書類（写真付）のICチップ情報
規則15条3項9号
（犯収法への手法に類似）

公的個人認証
規則15条3項11号
（犯収法ワの手法に類似）

民間事業者発行の電子証明書[*4]
規則15条3項12号
（犯収法力の手法に類似）

他の法定手法による身元確認を経て発行したID・PW（2回目以降）
規則15条3項13号

注釈1：古物営業法は、美術品類、衣類、時計・宝飾品類、自動車、自動二輪車・原動機付自転車、自転車類、写真機類、事務機器類、機械工具類、道具類、皮革・ゴム製品類、書籍、金券類の13種の品目について、一度使用された物品、未使用でも使用のために取引された物品、これらを補修・修理をした物品を「古物」として定義している。
注釈2：1万円未満の場合であっても、家庭用ゲームソフト、自動二輪（部品含む）、原動機付自動車（部品含む）、書籍、CD等については金額に関わらず本人確認が必要となる。
注釈3：上記の図の「規則」は、「古物営業法施行規則」を指す。
注釈4：公的個人認証法の認定を受けた署名検証者が発行する電子証明書が規定されている。
注釈5：上記の手法は、本人確認の相手方が個人である場合の手法を掲載。

外国為替及び外国貿易法

外為法は、犯罪収益移転防止法の取引時確認と同様のマネー・ロンダリング対策、加えて、資産凍結等の経済制裁措置の実効性を確保するため、海外送金等を扱う銀行等に対し、顧客の本人確認義務を課しています。

本人確認の枠組み

〈主体〉

- **銀行等**
- **資金移動業者**
- **暗号資産交換業者**

▶

〈フェーズ〉

一定の為替取引

・外国送金（10万円超）
・外貨両替（200万円超）など

▶

〈確認事項〉

本人特定事項の確認
（氏名、住所、生年月日）

【犯罪収益移転防止法との差異】

- 外為法の本人確認は、本人特定事項の確認のみ。
- 犯収法の取引時確認は、本人特定事項の確認に加え、取引目的・職業や事業内容、実質的支配者の確認等も必要。

利用できるオンライン完結の本人確認手法

容貌＋本人確認書類（写真付）の画像
省令8条1項1号ホ
（犯収法ホの手法と同様）

容貌＋本人確認書類（写真付）のICチップ情報
省令8条1項1号ヘ
（犯収法ヘの手法と同様）

本人確認書類の画像/ ICチップ＋銀行・クレカ情報照合/ 口座振込み
省令8条1項1号ト
（犯収法トの手法と同様）

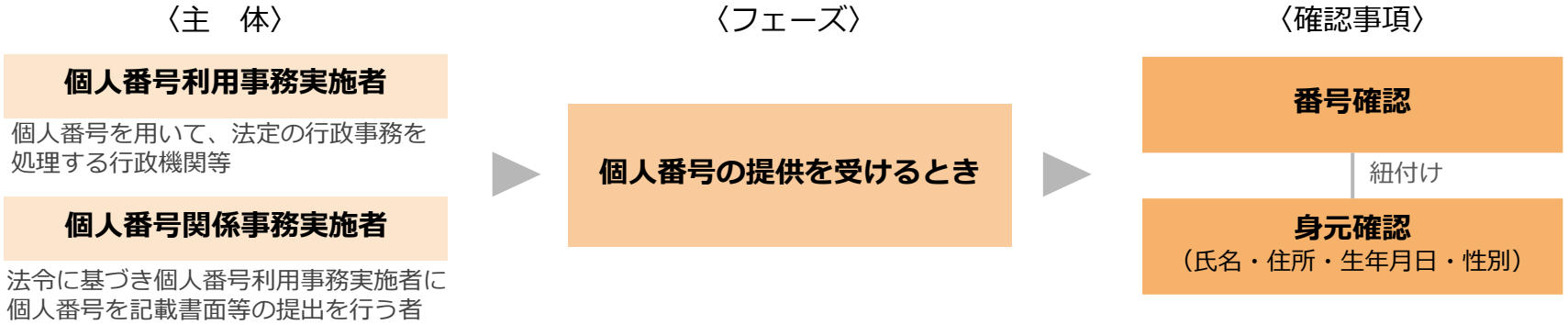
公的個人認証
省令8条1項1号ワ
（犯収法ワの手法と同様）

民間事業者発行の電子証明書
省令8条1項1号ヲ・カ
（犯収法ヲ・カの手法と同様）

注釈1：上記の図の「省令」は、「外国為替に関する省令」を指す。
注釈2：上記の手法は、本人確認の相手方が個人である場合の手法を掲載。

番号法は、事業者等が番号法で規定された分野に関する業務手続のために、個人番号の提供を受ける際に身元確認と個人番号の確認を義務付けています。具体的な手法としては、マイナンバーカードや住民票の写しの提示のほか、オンラインでの確認手法も許容されています。

本人確認の枠組み



利用できるオンライン完結の本人確認手法

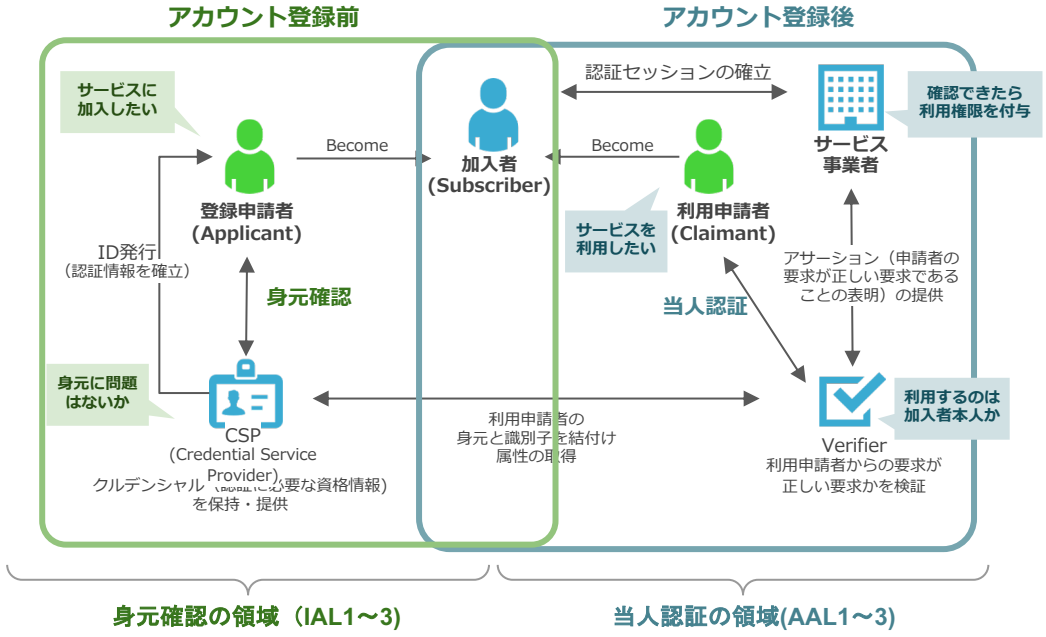
番号確認	身元確認
• マイナンバーカードのICチップ読み取り • 過去に本人確認の上作成しているファイルの確認 • マイナンバーカード等の画像データの電子的送信 • 地方公共団体情報システム機構への確認	• マイナンバーカードのICチップ読み取り • 公的個人認証による電子署名 • マイナンバーカードや運転免許証等の画像データの電子的送信 • 民間発行の電子署名 • 事業者が本人確認済で発行したID/PW

注釈：上記の手法は、本人確認の相手方が個人である場合の手法を掲載。

NIST SP 800-63-3のDigital Identity Model

NISTガイドラインは、オンラインサービスの申請から利用に至る一連のプロセス*に関与する主体と相互作用をモデル化しています。このモデルは、身元確認・当人認証が、どのような場面で、どのように機能するものなのかを理解する上でも幅広く参照されています。

NISTのDigital Identity Modelのイメージ



身元確認・当人認証の主要な概念

身元確認
(Identity Proofing)

3つの段階

収集 (Resolution)	検証 (Validation)	確認 (Verification)
氏名・住所・生年月日等の情報の収集、エビデンス確保（本人確認書類の券面撮影等）	提供された情報の内容の検証（本人確認書類発行元への確認、識別番号等のデータ照合等）	提出情報に紐付く本人との一致確認（申請者の容貌と本人確認書類画像との一致確認等）

当人認証
(Authentication)

3つの要素

知識 (you know)	所持 (you have)	生体 (you are)
記憶シークレット（PW,PIN,パスフレーズ等）	帯域外デバイス（スマートフォン等） OTPソフトウェア/デバイス（Google Authenticator等） 暗号化ソフトウェア（USBトークン、暗号鍵紐付き証明書等）	バイオメトリクス（指紋、顔写真、静脈等）

注釈：サービスの登録申請に際しての他者との「識別(Identification)」から、利用申請に際しての当人性の「認証（Authentication)」、実際のサービス利用のための「認可（Authorization）」に至たるための関係当事者が有する機能の相互連携プロセス。
出所：NIST (2017)「Special Publication 800-63-3 Digital Identity Guidelines」を参考に作成。

マイナンバーカードの機能のスマートフォン搭載（検討状況の整理）

2023年5月にAndroidスマートフォンへの搭載に向けて政府が検討している「マイナンバーカードの機能のスマートフォン搭載」の検討状況について、2022年4月15日に公表された「第2次とりまとめ」を参照しながら整理します。

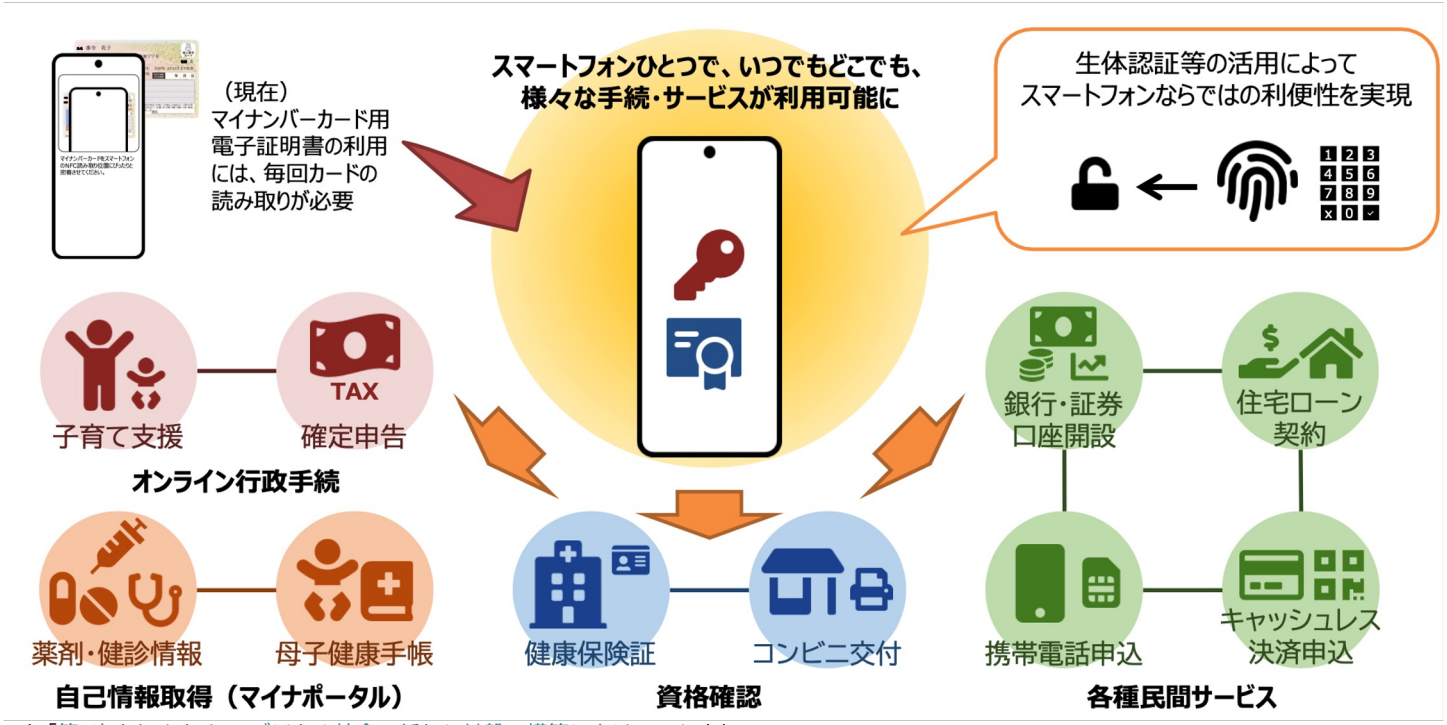
ポイント

- 「マイナンバーカードの機能のスマートフォン搭載」では、公的個人認証サービスの電子証明書の機能をスマートフォンに搭載することによって、スマートフォンひとつで、いつでもどこでもオンライン行政手続等を行うことができる環境構築が目指されています。
- 「マイナンバーカードの機能のスマートフォン搭載」は、2023年5月にAndroidで対応予定です。
- 「マイナンバーカードの機能のスマートフォン搭載」には署名用電子証明書と利用者用電子証明書の2種類の電子証明書が搭載されます。そのうち、利用者証明用電子証明書については、画面ロック解除機能（生体認証等）での認証が可能です。
- スマートフォン用電子証明書の新規発行は、マイナポータルアプリを利用し、オンラインで手続が完結する方針です。また、機種変更時には新端末での電子証明書の発行と、旧端末の電子証明書の失効・削除をシームレスに行えます。
- スマートフォン用電子証明書は、マイナンバーカードと同等の本人確認保証レベル（IAL3・AAL3）を確保する方向で検討されています。
- 「マイナンバーカードの機能のスマートフォン搭載」の主要なユースケースの1つが本人確認です。
- 他サービスのアプリ・ブラウザとの連携にあたっては、①マイナポータルアプリのみを介してアクセス可能、②一定水準のセキュリティ対策が講じられた事業者のアプリ・ブラウザにアクセスを限定し、ホワイトリストで管理する、等の重層的な対策が検討されています。

「マイナンバーカードの機能のスマートフォン搭載」が目指す姿

「マイナンバーカードの機能のスマートフォン搭載」では、公的個人認証サービスの電子証明書の機能をスマートフォンに搭載することによって、スマートフォンひとつで、いつでもどこでもオンライン行政手続等を行うことができる環境構築が目指されています。

マイナンバーカードの機能のスマートフォン搭載の目指す姿

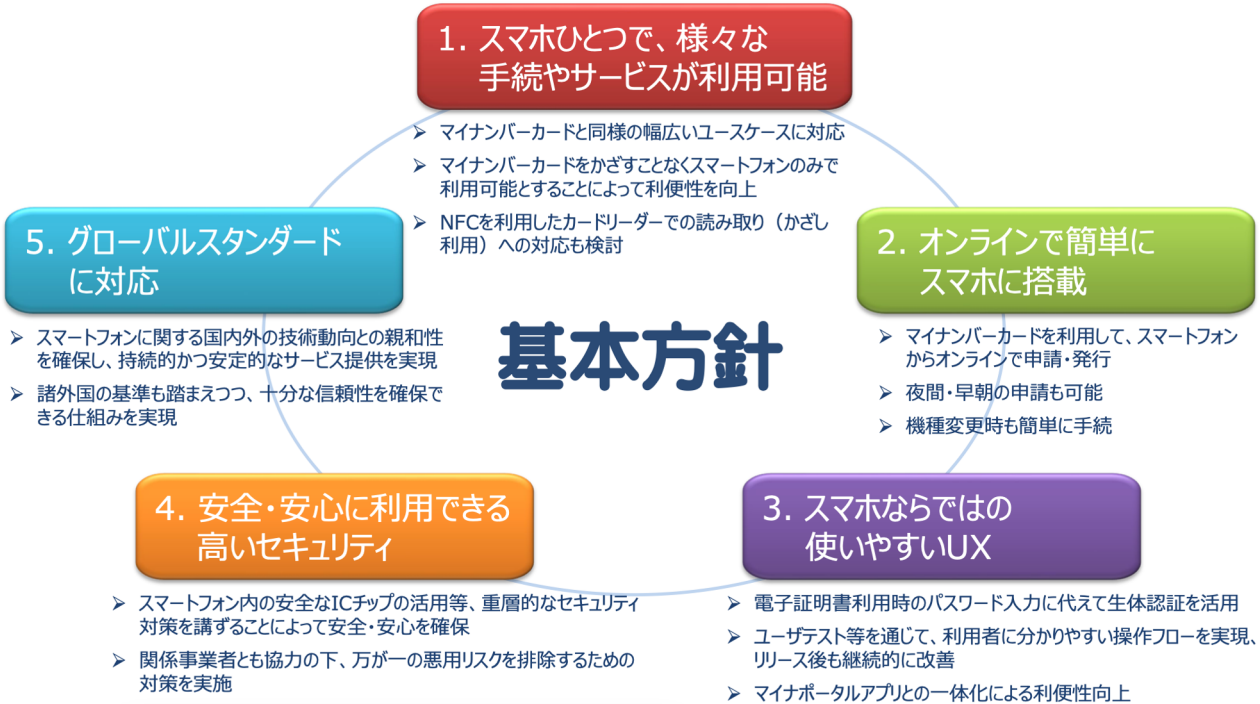


出所：総務省 (2022)「第2次とりまとめ ～デジタル社会の新たな基盤の構築に向けて～」より.

「マイナンバーカードの機能のスマートフォン搭載」の基本方針

「マイナンバーカードの機能のスマートフォン搭載」は、ユーザビリティとセキュリティを両立しつつ、グローバルスタンダードに対応することを基本に検討されています。

マイナンバーカードの機能のスマートフォン搭載の基本方針

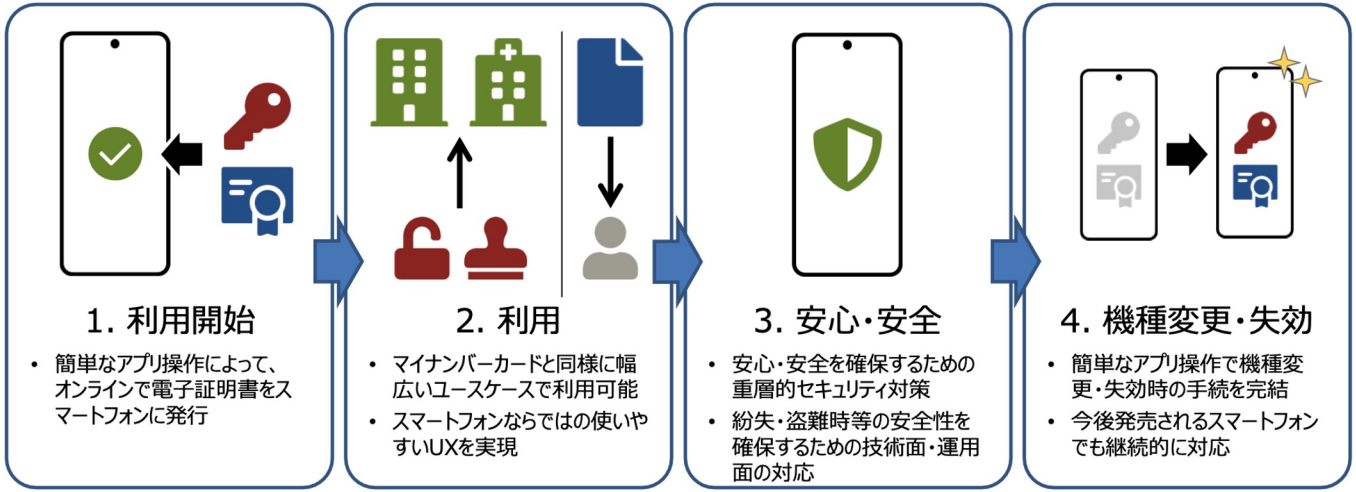


出所：総務省 (2022)「第2次とりまとめ ～デジタル社会の新たな基盤の構築に向けて～」より.

「マイナンバーカードの機能のスマートフォン搭載」の全体像

「マイナンバーカードの機能のスマートフォン搭載」は、2023年5月にAndroidで対応予定です。簡単なアプリ操作によってオンラインで電子証明書をスマートフォン内に発行・管理し、幅広いユースケースで利用可能となる方向で検討されています。

電子証明書のライフサイクル（イメージ）



2023年5月にAndroidスマートフォンに搭載予定

iPhoneについては早期実現を目指して検討・調整中

J-LIS、**スマートフォン製造事業者**、**OS事業者**、**携帯電話事業者**、**中古端末取扱事業者**等との協力を通じて安定的なサービス提供を図る。

※対応端末は順次公表予定

出所：総務省 (2022)「第2次とりまとめ ～デジタル社会の新たな基盤の構築に向けて～」より.

「マイナンバーカードの機能のスマートフォン搭載」の利用イメージ

「マイナンバーカードの機能のスマートフォン搭載」には署名用電子証明書と利用者証明用電子証明書の2種類の電子証明書が搭載されます。そのうち、利用者証明用電子証明書については、画面ロック解除機能（生体認証等）での認証が可能です。

スマートフォン用電子証明書で可能な認証手段と認証操作フロー（イメージ）

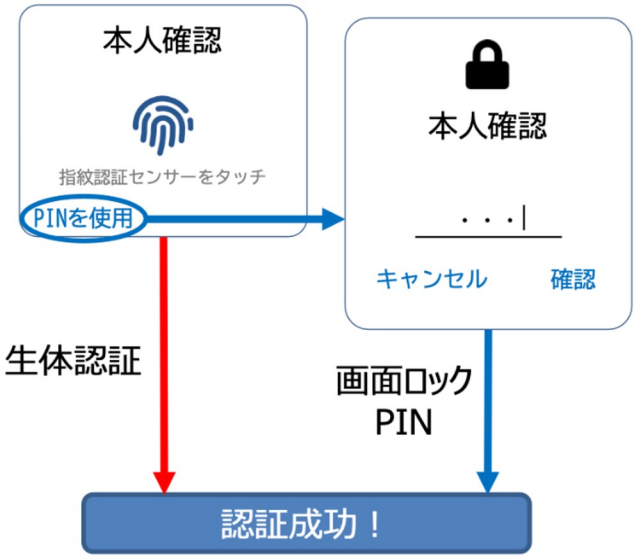
スマートフォン用電子証明書で利用可能な認証手段

	GP-SEに設定されたパスワード	Androidスマートフォンの画面ロック解除機能
署名用電子証明書	○ （6～16桁の英大文字・数字の組合せ）	×
利用者証明用電子証明書	○ （4桁の数字）	○ （※）

※利用者証明用電子証明書のパスワードを代替可能な画面ロック解除機能は、Android CDDに沿って、以下の要件を満たすものとする。

	要件
プライマリ認証	画面ロック解除用のPIN・パターン・パスワード
セカンダリ認証	Class 3（Android 10以前：強）の生体認証 • FAR（他人受入率）：0.002%（5万人に1人）以下 • SAR（スプーフィング攻撃への耐性）：7%以下 • IAR（なりすまし攻撃への耐性）：7%以下 • 少なくとも72時間に一度はプライマリ認証が求められる

認証操作フロー（イメージ）

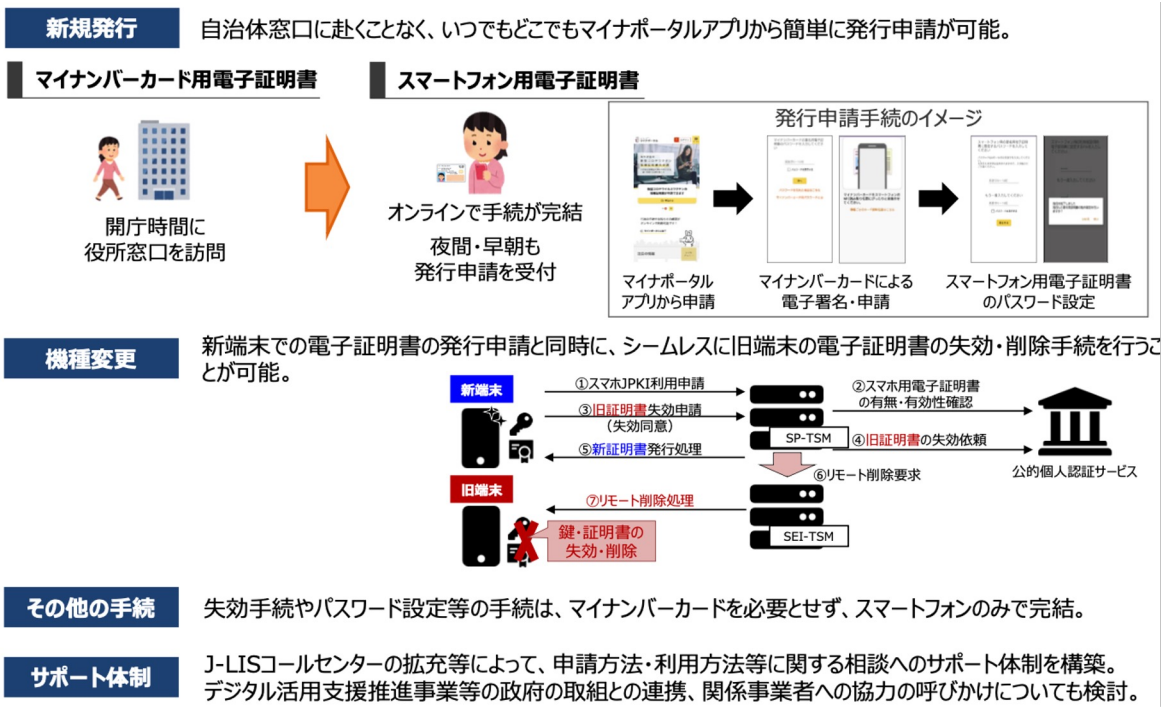


出所：総務省 (2022)「第2次とりまとめ ～デジタル社会の新たな基盤の構築に向けて～」より.

スマートフォン用電子証明書の利用手続

スマートフォン用電子証明書の新規発行は、マイナポータルアプリを利用し、オンラインで手続が完結する方針です。また、機種変更時には新端末での電子証明書の発行と、旧端末での電子証明書の失効・削除手続をシームレスに行うことができます。

スマートフォン用電子証明書の利用手続（イメージ）



出所：総務省 (2022)「第2次とりまとめ ～デジタル社会の新たな基盤の構築に向けて～」より.

スマートフォン用電子証明書の本人確認保証レベル等

スマートフォン用電子証明書は、マイナンバーカードと同等の本人確認保証レベル（IAL3・AAL3）を確保する方向で検討されています。

マイナンバーカード用電子証明書とスマートフォン用電子証明書保証レベルの比較

保証レベル	マイナンバーカード用電子証明書	スマートフォン用電子証明書
IAL（身元確認） 【レベル３の要件】 対面での身元確認	レベル３ ○自治体窓口等での対面による交付	レベル３相当 ○対面交付されたマイナンバーカードによる電子署名に基づき発行
AAL（当人認証） 【レベル３の要件】 耐タンパ性が確保されたハードウェアを含む複数の認証要素による認証	レベル３ ○所持（耐タンパ性を有するマイナンバーカードのICチップ） ○知識（パスワード）	レベル３相当 ○所持（スマホに搭載された耐タンパ性を有するGP-SE） ○知識（パスワード）又は 生体（指紋・顔）

○マイナンバーカードを用いたスマートフォン内のローカル環境（GP-SE内のアプレット）での鍵ペア生成

○高セキュリティな秘匿通信の環境下で公開鍵をJPKI側に登録して電子証明書を発行

→一連のスキームにおいて、マイナンバーカード交付時の本人確認の強度が引き継がれており、特にスマホとJPKIとの間に第三者が関与する余地がない

○マイナンバーカードのICチップとGP-SE（アプレットを含む）はいずれもCC認証を取得し、耐タンパ性を保証

米国NISTデジタルアイデンティティガイドライン（SP 800-63-3）参照

出所：総務省 (2022)「第2次とりまとめ ～デジタル社会の新たな基盤の構築に向けて～」より.

「マイナンバーカードの機能のスマートフォン搭載」の主なユースケース

「マイナンバーカードの機能のスマートフォン搭載」では、マイナンバーカードと同等のセキュリティを確保し、マイナンバーカードの電子証明書を使って利用できる手続・サービスをスマートフォン1つで完結できるようになります。

政府が想定している主なユースケース

主なユースケース	概要	スマートフォン対応予定時期	備考
マイナポータル	毎回マイナンバーカードをかざす必要がなく、生体認証等によって簡単にログインすることができ、いつでもどこでも、マイナポータルのサービスを利用できるようになる。	令和５年５月	マイナポータルでは、 ・子育て関係等の行政サービスの検索・電子申請 ・自己情報の確認・提供（税・年金・薬剤情報・特定検診情報等） ・確定申告の簡便化 等の様々なサービスを利用可能。
各種行政手続のオンライン申請	スマートフォン用電子証明書を使用した電子署名等によって、いつでもどこでも、各種行政手続のオンライン申請が可能になる。	令和５年５月以降順次	
コンビニ交付サービス	スマートフォンを携行していれば、全国のコンビニ等において、住民票の写しや印鑑登録証明等の証明書の取得が可能になる。	令和５年度	コンビニ交付サービスシステム、コンビニのマルチコピー機又は一部のスマートフォンで要システム対応。また、コンビニ事業者と調整中。
健康保険証	健康保険証やマイナンバーカードを携行することなく、医療機関の受診等が可能になる。	令和６年４月	厚生労働省において、オンライン資格確認システムの改修等の対応を予定。
各種民間サービスのオンライン手続等	スマートフォン用電子証明書を使用した電子署名等によって、いつでもどこでも、証券口座の開設や住宅ローン契約等のオンライン手続が可能になる。	令和５年５月以降順次	民間事業者173社が公的個人認証サービスを活用（令和５年１月1日時点）。 民間事業者においてスマートフォン対応のためのシステム改修等が必要。令和4年10月にAPI（β版）を公開。

出所：デジタル庁提供資料より.

「マイナンバーカードの機能のスマートフォン搭載」の利用イメージ

「マイナンバーカードの機能のスマートフォン搭載」では、マイナポータルへのログイン（利用者証明用電子証明書の利用）が生体認証等を使って可能になります。また、行政手続についても、電子証明書を使ってオンラインで手続が可能です。

マイナポータルにおける利用イメージ

これまで

マイナポータルへのログイン時には毎回マイナンバーカードの読み取りが必要

スマートフォン用電子証明書を利用

マイナンバーカードを読み取る必要がなく、生体認証等を使って簡単にログインが可能

→通勤中でも、外出先でも、いつでもどこでもサービスを利用可能

マイナポータルで利用できる主なサービス	
行政手続の検索・電子申請	自治体の各種手続の検索及び電子申請が可能。対象手続拡大中。 【例】保育施設利用申込み、給付金申請、児童手当申請
自己情報の確認・提供	行政機関等が保有する自分の情報を確認したり、第三者に提供することが可能。 【例】税・所得情報（金融機関や自治体における手続等に利用） 予防接種履歴・薬剤情報（民間の健康管理アプリ・お薬手帳アプリ等と連携が可能）
お知らせ	行政機関等から情報配信を受けることが可能。 【例】税金の納付依頼、児童手当の手続等の利用者の状況に応じた行政手続の案内

これまで（役所窓口）

書類作成、役所訪問・提出 → 本人確認・申請完了

スマートフォン用電子証明書を利用（電子申請）

マイナポータルで手続を検索・申込内容を入力 → 電子証明書を使って電子署名・電子申請

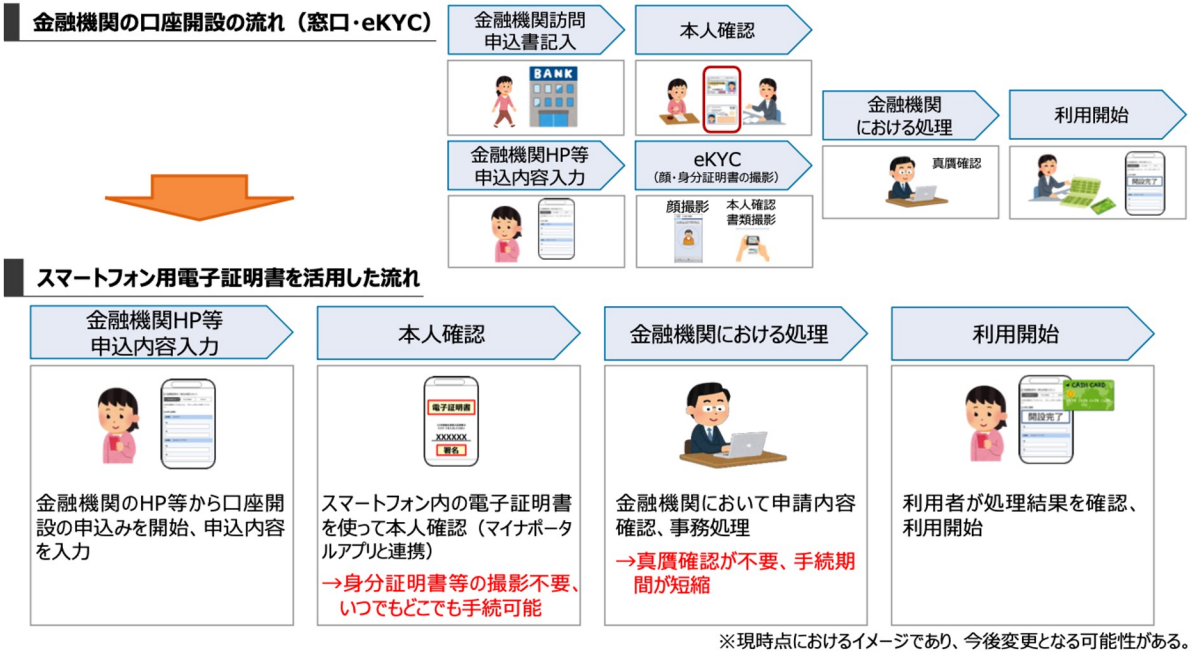
- 入力支援機能を使って、氏名・住所や過去の申請情報等を簡単に入力
- 役所窓口に出向くことなく、いつでもどこでも、スマートフォンひとつで手続可能

出所：総務省 (2022)「第2次とりまとめ ～デジタル社会の新たな基盤の構築に向けて～」より.

「マイナンバーカードの機能のスマートフォン搭載」の民間サービスでの利用イメージ

「マイナンバーカードの機能のスマートフォン搭載」の主要なユースケースの1つが本人確認です。スマートフォン内の電子証明書を利用することで、身分証明書等の撮影を伴わず手続を行うことができるようになります。

金融機関における本人確認での利用シーン



※現時点におけるイメージであり、今後変更となる可能性がある。

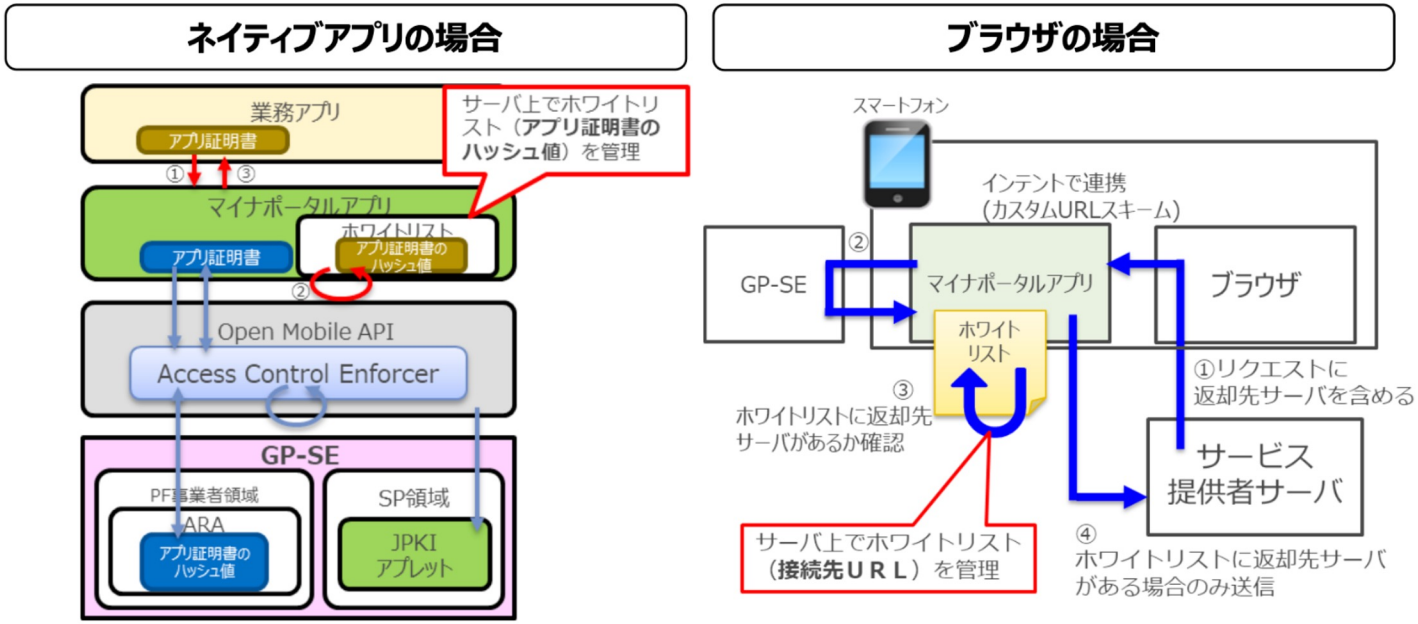
※遅くとも令和4年9月には民間サービス等との連携に必要なAPI情報を公開予定。また、民間サービスにおける更なる利用拡大を促進する観点から、海外事例（シンガポール等）も参考としつつ、開発者目線の利便性向上にも取り組む。

出所：総務省 (2022)「第2次とりまとめ ～デジタル社会の新たな基盤の構築に向けて～」より.

他サービスのアプリ・ブラウザとの連携

他サービスのアプリ・ブラウザとの連携にあたっては、①マイナポータルアプリのみを介して利用可能、②一定水準のセキュリティ対策が講じられた事業者のアプリ・ブラウザにアクセスを限定し、ホワイトリストで管理する、等の重層的な対策が検討されています。

他サービスのアプリ・ブラウザとの連携のイメージ



- セキュリティ対策を1つのアプリに集中して行うことが可能
- 利用者が行う生体認証の登録・変更設定はマイナポータルアプリのみとなるため利便性に優れ、GP-SEの容量も圧迫しない
  （複数アプリからGP-SEにアクセスする場合、アプリ毎に設定が必要）

出所：総務省 (2022)「第2次とりまとめ ～デジタル社会の新たな基盤の構築に向けて～」より.

事業者ヒアリングの概要

事業者ヒアリングの概要

11の民間事業者・団体等に対して身元確認の導入実態に係るヒアリング調査を行い、本ガイドラインにおける身元確認手法の選択等を整理する上での参考事例を収集しました。

ヒアリング調査の概要

目的	● 身元確認の導入事例を通して、①導入にあたって検討したこと、②導入にあたっての課題、③中間的な手法に対する感想等を事例ベースで収集・整理し、本ガイドラインの内容がより参照しやすいものとする ● その他、本ガイドライン全般に係る意見を収集する
方法	● ビデオ会議システムによるリモート調査 ● 平均的に1社当たり約60分実施
期間	● 2022年8～10月
対象	● 全11事業者・団体等を対象に実施 ● 事業者の業界・業種は、チケット販売、エネルギー、インフラ、遠隔医療、小売、金融、食品製造、業界団体等 ● 法令等で本人確認が求められていないサービスを展開している事業者を中心に、タスクフォース参加各社が選定
質問事項	● 導入している身元確認手法と導入の目的 ● 身元確認手法の選択理由と主な課題 ● 身元確認手法の選択時に重視するポイント ● 「ホ方式の自動化」、「身元確認結果の活用」に対する意見・感想 ● その他

導入している身元確認手法と導入の目的

ヒアリング対象者が導入している身元確認手法は、「アップロード」、「犯収法ホ方式」、「ホ方式の自動化」でした。また、身元確認の主な導入目的は不正の未然防止のほか、「正確なユーザー情報の取得」や「業界規制等で必要」等でした。

ヒアリング対象企業における身元確認の導入状況と導入の目的

	導入している身元確認手法	身元確認導入の目的
D社	登録時：アップロード 利用サービスの拡大時：ホ方式の自動化	● 不正取引を防ぐため。特に、利用サービス範囲を広げる際には、不正が行われないよう、より厳格な手法を採用
E社	（アップロード）	● ただし、身元確認目的ではなく、資格確認のため
F社	アップロード→現在では廃止 （その他、郵送、店舗でのタブレットを使った加入手続きも実施）	● 売掛で売買している代金を確実に回収するため ● 正確なユーザー情報を取得するため（特に住所情報は、宅配やその他手続時に重要）
G社	犯収法ホ方式	● 連携先からの要望を満たすため ● サービスの一部が犯罪収益移転防止法の対象となるため
I社	犯収法ホ方式→現在では、ホ方式の自動化	● 対面サービスにおいても身元確認を行っており、オンラインサービスでもある程度厳格な身元確認を行いたいため
J社	対面確認	● 本人同意を確実に得たうえで、取引を行うため
K社	アップロード	● 業界規制により、年齢確認を行う必要があるため

注釈：以下、本ヒアリングのまとめでは、ヒアリング対象の11事業者・団体をA～K社として表記。

身元確認手法の選択理由と主な課題

アップロードは「手軽な身元確認手法」、犯収法ホ方式は「犯収法の手法のうち最も一般的な手法」、ホ方式の自動化では「ホ方式と比べた負担軽減」が主な選択理由でした。また、課題としては、「なりすましリスク」や「撮影不備」、「審査体制の整備」が主なものでした。

ヒアリング対象企業における身元確認手法の選択理由と主な課題

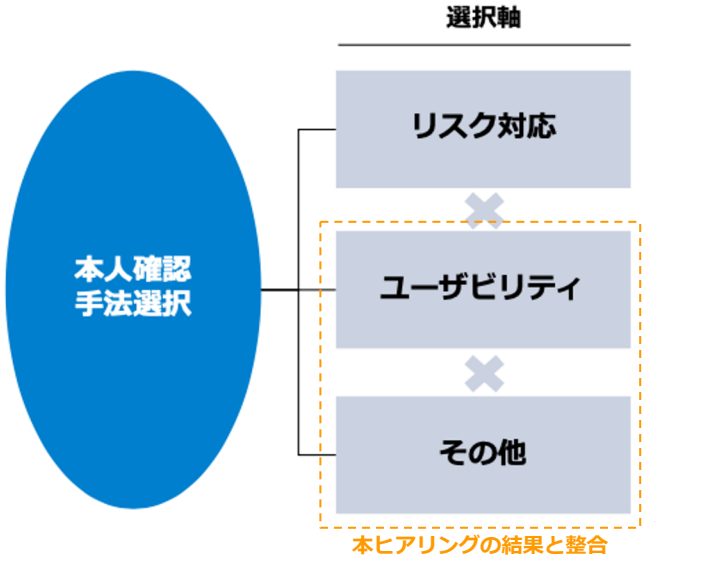
	選択理由	主な課題
アップロード（D、E、F、K社）	● 一般的に用いられている手法であるため ● ユーザーにとって負担が少ない手法であるため（リスクを踏まえて十分な強度を有していると判断） ● 自社開発が容易な手法であったため ● 氏名、住所、生年月日が確認できれば良いため	● なりすましによる不正取引が時々発生する ● 途中離脱と撮影不備（券面情報と登録情報の不一致、券面写真が不鮮明、誤った写真のアップロード等） ● 撮影不備の際の目視確認コスト ● 複数の本人確認書類への対応
犯収法ホ方式（G、I社）	● 犯収法の要件として最も一般的な手法であったため（ベンチマークとしての位置づけ） ● ICチップを読み取る等の障壁がなく、ユーザーが利用しやすい手法であるため ● ICチップ読み取りと比較し、開発が容易	● 身元確認を完了できないユーザーからのクレーム ● ICチップ読み取りと比較して、券面偽造への耐性が劣る ● 審査体制の整備（人員配置）
ホ方式の自動化（D、I社）	● セルフィーが含まれている手法の中で、開発や運用コストを抑えることができるため ● 写真付き本人確認書類と容貌の一致を確認できるため	後述

リスクへの対応以外に事業者が身元確認手法に重視しているポイントは、ユーザビリティとコストに関するものでした。

ヒアリング対象企業における身元確認手法で重視するポイント（リスク対策を除く）

	身元確認手法の選択時に重視するポイント
D社	● ユーザーの負担を軽減し、いかに身元確認時の離脱を減らすか ● 導入時の負担（開発コスト等）が低いこと
E社	● 対面サービスと比較し、必要以上に厳格な身元確認にならないこと
F社	● ユーザーの利便性とコスト ● 宅配サービスを行うため、正確な住所情報を取得できること
G社	● 基本的にはリスクベースで手法を選択しており、リスク対策が重要
J社	● 高齢のユーザーも利用できる、シンプルなユーザーインターフェース（ユーザビリティ）

（参考）DADCでの検討において整理した本人確認手法の選択軸



出所：デジタルアーキテクチャ・デザインセンター（2022）「第2回インキュベーションラボ　テーマ２：サービスに応じたデジタル本人確認ガイドラインの検討　活動成果報告(詳細版)」より.

ホ方式の自動化に対する意見・感想

ホ方式の自動化に対するポジティブな感想として「ユーザーからの問い合わせや離脱が少ない」、「業務負荷を軽減できた」というものがありました。他方で、「OCRの読み取り精度等の判断」や「負担軽減の効果」等が懸念としてあげられました。

ヒアリングにおけるホ方式の自動化に対する意見・感想

ポジティブな意見・感想


D社

想定よりユーザーの離脱や問い合わせが少ない。
SDKが提供されており、比較的スムーズに導入できた。


G社

法令に準拠する必要がない身元確認においては検討の余地がある手法


I社

目視の業務負荷を大幅に軽減できた。現在は、住所不一致等の限られたものだけを目視で確認すれば良い（身元確認全体の8%程度）

ネガティブな意見・感想


D社

開発メンバーが仕様の全体を把握するのに多少時間がかかった。また、エラーパターンが多く、テストが多かった。


I社

旧字体の読み取り時にエラーが発生する。
顔認証ではエラーが無いが、本当に顔画像と容貌の一致を判定できているかが不安。


J社

100%自動化が可能ではなく、一定程度目視確認が含まれるため、工数をどれだけ削減できるか懸念。
また、OCRの読み取り精度が向上すると良い。


K社

ユーザーの負担は犯収法ホ方式と大きく変わらず、最低限の身元確認を行いたい場合には導入は難しい

身元確認結果の活用に対する感想

身元確認結果の活用については導入済みの事業者はなかったものの、関心は高く、ポジティブな感想として「ユーザーの負担軽減」「個人情報の取扱い」「本人確認書類が不要」等がありました。他方で、「手法の認知度」や「導入・運用コスト」等が懸念としてあげられました。

ヒアリングにおける身元確認結果の活用に対する感想

ポジティブな意見・感想

E・H社	本人確認書類を使わない点が手軽で良い
F社	個人情報の取扱いの観点から、本人同意のもとで情報がやり取りされる点は良い。入力補助としての付加価値にもメリットを感じる
H社	外部サービスとの連携で、新規ビジネスに繋がる。定期的に利用するアカウントを利用できるため、ユーザーが迷わず身元確認を行える
K社	ユーザーの負担軽減に繋がる点は良い

ネガティブな意見・感想

I社	金融機関の身元確認結果を活用する場合、事業者側に一定の心理的ハードルが存在するよう。また、利用者にメリットを訴求することが難しい
J社	ソーシャルログインのように、サービスごとに動線が複数に分岐するとなると、開発や運用の負担が大きくなることが懸念
K社	まずはこの手法が広がることが課題（認知度）
G・H・K社	システム開発コストが低いと良い

マイナンバーカードに対する期待・懸念や、個人情報の取扱い、ガイドラインに対する要望等がありました。本ガイドラインに対しては、法令等で本人確認の定めのない業界にとっての指針として評価いただくとともに、ガイドラインの横展開についても言及されました。

ヒアリングにおけるその他の意見等

マイナンバーカードについて

D社

マイナンバーカードは普及率が拡大しており、今後暗証番号を覚えているユーザーが増えてくると良い。ただし、高齢の方が公的個人認証を利用できるかが懸念

E社

マイナンバーカードは暗証番号を覚えれば比較的簡単な手法であり、将来的な導入も検討しうる

G社

今後マイナンバーカードがどれだけ使われるかに注目している

個人情報の取扱いについて

G社

個人情報については丁寧な説明が必要。その際、ユーザーにとって煩わしくならず、一方でユーザーの同意をきちんと取得するというバランスが難しい

本ガイドラインについて

D社

本人確認手法は変化していくと思われ、リアルタイムに最適な手法を選択できるようなガイドラインがあるとありがたい

E社

対面では厳格な本人確認を求められていないにも関わらず、オンラインになると急に厳格な手法を求めるような規制にならないようにすべき

G社

各サービスにはグラデーションがあり、適する本人確認手法も異なる。こうした実態から乖離しない、使い勝手のよいガイドラインにしていただきたい

J社

法令等に定めのない業界向けのガイドラインはありがたい。また、横展開として、他の省庁や団体等からもガイドラインが出されるとありがたい

本人確認手法の保証レベルマッピング

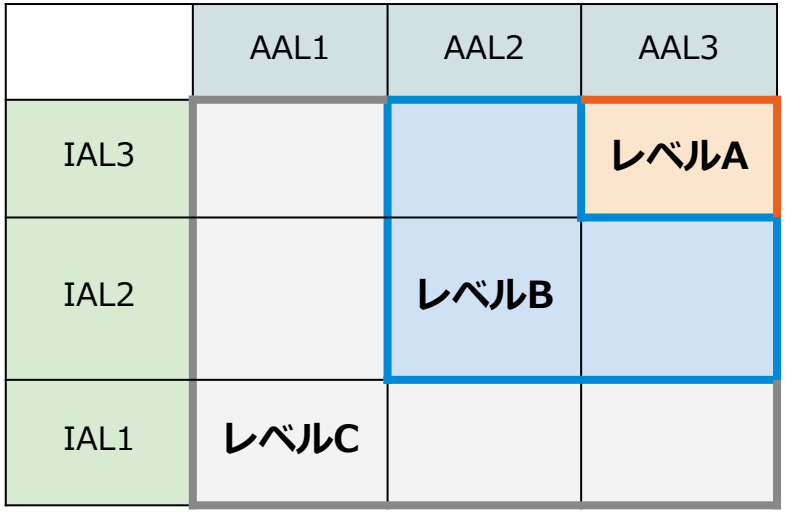
本人確認手法の保証レベルマッピングの概要

本人確認全体の強度を考える上では、身元確認の保証レベルはもちろん、当人認証の保証レベルについても意識することが重要です。

本人確認全体の保証レベルの考え方【再掲】

IAL	AAL
レベル3 対面での身元確認	**レベル3** 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
レベル2 遠隔又は対面での身元確認	**レベル2** 複数の認証要素
レベル1 身元確認のない自己表明	**レベル1** 単一又は 複数の認証要素

本人確認全体の保証レベル*
（行政手続ガイドラインの整理）



注釈：ただし、IALとAALを掛け合わせ、本人確認全体の保証レベルをA～Cに定義することには議論がある。
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。

保証レベル別の身元確認手法マッピング

IAL	DADC IAL	主な手法例*	行政手続ガイドラインの定義
IAL3	DADC IAL4	• マイナンバーカードの公的個人認証（署名用電子証明書） • マイナンバーカードの機能のスマートフォン搭載の署名用電子証明書（予定）	身元識別情報が特定された担当者の対面で確認され、身元確認の信用度が非常に高い。
IAL2	DADC IAL3	• 犯収法ホ方式 • 犯収法ヘ方式 • 犯収法ト方式 • ホ方式の自動化 • 身元確認結果の活用	身元識別情報が遠隔又は対面で確認され、身元確認の信用度が相当程度ある。
	DADC IAL2	• リアルタイム撮影 • 顔写真付き本人確認書類の裏表のリアルタイム撮影＋容貌の撮影	身元識別情報が確認される必要がなく、身元確認の信用度がほとんどない。身元識別情報は、自己表明若しくは自己表明相当である。
	DADC IAL1	• アップロード	
IAL1	DADC IAL0	• 自己申告	

注釈 ：掲載した手法例は一部であり、今後皆様からのご意見等を踏まえて継続的にアップデートしていきます。
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」を参照。

保証レベル別の当人認証手法マッピング

AAL	主な手法例*1	行政手続ガイドラインの定義
AAL3	• マイナンバーカードの公的個人認証（利用者証明用電子証明書） • セキュリティキー認証（FIDO認証）*2	認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、耐タンパ性を有するハードウェアを含む複数要素を使うことにより、当人認証の信用度が非常に高い。
AAL2	• パスワード及びワンタイムパスワード • パスワードレス生体認証（FIDO認証）*2	認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、複数要素を使うことにより、当人認証の信用度が相当程度ある。
AAL1	• パスワード	認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、単要素若しくは複数要素を使うことにより、当人認証の信用度がある程度ある。

注釈1 ：掲載した手法例は一部であり、今後皆様からのご意見等を踏まえて継続的にアップデートしていきます。
注釈2：FIDO認証の保証レベルは製品やプロダクトにより異なるため、ここでは代表的な整理を記載。
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」を参照。

サービス別の保証レベルマッピング（事例）

サービス別本人確認手法マッピングの考え方

本人確認手法導入検討時の参考資料として、実際に導入されている本人確認手法について、身元確認手法と当人認証手法の組み合わせを調査し、可視化しました。

サービス別本人確認手法マッピングの概要と参照方法

サービスマッピングの概要

前提	実サービスとして導入されているデジタル本人確認手法について、登録時を中心とした身元確認手法及びログイン時を中心とした当人認証手法のそれぞれを事例ベースで調査・整理したもの
方法	各サービスのWebサイト等を調査し、事例を記録（一部ヒアリングによる聞き取り情報を含む）
対象	シェアリングエコノミーサービスを実施している企業（約200企業）
主な留意点	既存の本人確認手法を調査したものであり、必ずしもサービスに応じた本人確認手法となっていない場合がある。さらに、各サービスで本人確認の導入シーンは様々であり、本マッピングはサービス登録時とログイン時の組み合わせを整理した一事例であるため、実際の本人確認手法は自社サービスの特性等を踏まえて検討する必要がある

サービスマッピングの参照方法

実際に各サービスで導入されている本人確認手法について「身元確認手法 / 当人認証手法」の組み合わせで記載

IAL	DADC IAL	AAL 1	AAL 2
3	4	公的個人認証 / パスワード	
2	3	犯収法ホ方式 / パスワード 犯収法ホ方式 / OTP	
	2	リアルタイム撮影 / パスワード リアルタイム撮影+IDセルフィ / パスワード 顔写真付き身分証の表裏のリアルタイム撮影+容貌の撮影 / パスワード	リアルタイム撮影+IDセルフィ / パスワード +OTP
	1	アップロード / パスワード アップロード / OTP アップロード / OTP+生年月日入力 アップロード+IDセルフィ / パスワード	アップロ アップロ +OTP
1	0	自己申告 / パスワード 自己申告 / OTP	自己申告 / パスワード+OTP

各手法の保証レベルは、身元確認手法はIAL及びDADC IAL、当人認証手法はAALと定義

本調査の範囲で、事例数が多い保証レベルの組み合わせを濃淡で表現

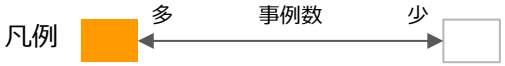
サービス別本人確認手法マッピング　シェアリングエコノミー（全体）

シェアリングエコノミーサービス全体では、様々なレベルの身元確認手法が導入されています。一方、当人認証についてはパスワード（AAL1）が中心でした。

シェアリングサービス全体の本人確認手法マッピング

（n=190）

IAL	DADC IAL	AAL		
		1	2	3
3	4	公的個人認証 / パスワード		
2	3	犯収法ホ方式 / パスワード 犯収法ホ方式 / OTP		
	2	リアルタイム撮影 / パスワード リアルタイム撮影+IDセルフィ / パスワード 顔写真付き本人確認書類の表裏のリアルタイム撮影+容貌の撮影 / パスワード	リアルタイム撮影+IDセルフィ / パスワード+OTP	
	1	アップロード / パスワード アップロード / OTP アップロード / OTP+生年月日入力 アップロード+IDセルフィ / パスワード	アップロード / パスワード+OTP アップロード+容貌の撮影 / パスワード+OTP	
1	0	自己申告 / パスワード 自己申告 / OTP	自己申告 / パスワード+OTP	



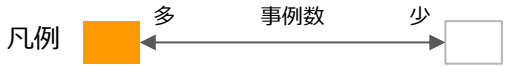
注釈1：本マッピングは聴き取り及びウェブリサーチにより作成しており、参照時点では手法等が変更になっている可能性があります。
注釈2：上記には、サービスの利用範囲を拡大する際に身元確認が求められる場合も含まれています。
注釈3：C to Cサービスの場合、サービスを提供する側・サービスを利用する側の手法が含まれています。

スキルシェアサービスでは、特に対面サービスを中心に、利用者の安全・安心を確保する観点から本人確認書類に基づく身元確認を導入している傾向がありました。

スキルシェアリングサービスの本人確認手法マッピング

（n=86）

IAL	DADC IAL	AAL 1	AAL 2	AAL 3
3	4			
2	3	犯収法ホ方式 / パスワード 犯収法ホ方式 / OTP		
	2	顔写真付き本人確認書類の表裏のリアルタイム撮影+容貌の撮影 / パスワード		
	1	アップロード / パスワード アップロード / OTP アップロード / OTP+生年月日入力 アップロード+IDセルフィ / パスワード		
1	0	自己申告 / パスワード 自己申告 / OTP	自己申告 / パスワード+OTP	



注釈1：本マッピングは聴き取り及びウェブリサーチにより作成しており、参照時点では手法等が変更になっている可能性があります。
注釈2：上記には、サービスの利用範囲を拡大する際に身元確認が求められる場合も含まれています。
注釈3：C to Cサービスの場合、サービスを提供する側・サービスを利用する側の手法が含まれています。

サービス別本人確認手法マッピング　シェアリングエコノミー（空間）

空間シェアサービスでは、現地における対面での身元確認が行われているケースも多く、オンライン完結での身元確認事例は少ない傾向がありました。

空間シェアリングサービスの本人確認手法マッピング

（n=46）

IAL	DADC IAL	AAL 1	AAL 2	AAL 3
3	4	公的個人認証 / パスワード		
2	3			
	2			
	1	アップロード / パスワード アップロード+IDセルフィ / パスワード	アップロード / パスワード+OTP	
1	0	自己申告 / パスワード		

凡例　多 ← 事例数 → 少

注釈1：本マッピングは聴き取り及びウェブリサーチにより作成しており、参照時点では手法等が変更になっている可能性があります。
注釈2：上記には、サービスの利用範囲を拡大する際に身元確認が求められる場合も含まれています。
注釈3：C to Cサービスの場合、サービスを提供する側・サービスを利用する側の手法が含まれています。

サービス別本人確認手法マッピング　シェアリングエコノミー（モノ）

モノのシェアリングサービスでは、非対面サービスが中心、かつ、破損等を損害保険で担保するのが一般的であるため、事前の身元確認の導入は少ない傾向でした。

モノのシェアリングサービスの本人確認手法マッピング

（n=30）

NIST IAL	DADC IAL	AAL 1	AAL 2	AAL 3
3	4			
2	3			
	2	リアルタイム撮影 / パスワード		
	1	アップロード / パスワード		
1	0	自己申告 / パスワード	自己申告 / パスワード+OTP	

凡例　多 ← 事例数 → 少

注釈1：本マッピングは聴き取り及びウェブリサーチにより作成しており、参照時点では手法等が変更になっている可能性があります。
注釈2：上記には、サービスの利用範囲を拡大する際に身元確認が求められる場合も含まれています。
注釈3：C to Cサービスの場合、サービスを提供する側・サービスを利用する側の手法が含まれています。

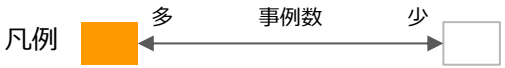
サービス別本人確認手法マッピング　シェアリングエコノミー（移動）

移動のシェアリングサービスでは、カーシェアを中心に利用者が運転免許証を所持しているケースが多く、運転免許証に基づく身元確認が中心となっています。

移動のシェアリングサービスの本人確認手法マッピング

（n=17）

NIST IAL	DADC IAL	AAL 1	AAL 2	AAL 3
3	4			
2	3			
	2	リアルタイム撮影+IDセルフィ / パスワード	リアルタイム撮影+IDセルフィ / パスワード+OTP	
	1	アップロード / パスワード アップロード+IDセルフィ / パスワード	アップロード+容貌の撮影 / パスワード+OTP	
1	0	自己申告 / パスワード 自己申告 / OTP	自己申告 / パスワード+OTP	



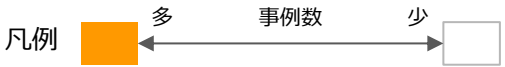
注釈1：本マッピングは聴き取り及びウェブリサーチにより作成しており、参照時点では手法等が変更になっている可能性があります。
注釈2：上記には、サービスの利用範囲を拡大する際に身元確認が求められる場合も含まれています。
注釈3：C to Cサービスの場合、サービスを提供する側・サービスを利用する側の手法が含まれています。

お金のシェアリングサービスでは、法令等による本人確認の定めの有無により、導入されている手法のIALが二分しています。

お金のシェアリングサービスの本人確認手法マッピング

（n=10）

NIST IAL	DADC IAL	AAL		
		1	2	3
3	4	公的個人認証 / パスワード		
2	3	犯収法ホ方式 / パスワード 犯収法ホ方式 / OTP		
	2			
	1	アップロード / パスワード		
1	0	自己申告 / パスワード		



注釈1：本マッピングは聴き取り及びウェブリサーチにより作成しており、参照時点では手法等が変更になっている可能性があります。
注釈2：上記には、サービスの利用範囲を拡大する際に身元確認が求められる場合も含まれています。
注釈3：C to Cサービスの場合、サービスを提供する側・サービスを利用する側の手法が含まれています。

参考文献一覧

主な参考文献一覧

- OpenID Foundation (2023)「OpenID for Verifiable Credential Issuance」
- OpenID Foundation (2023)「OpenID for Verifiable Presentations」
- クレジット取引セキュリティ対策協議会 (2023)「EMV 3-Dセキュア導入ガイド1.2版」及び「EMV 3-Dセキュア導入ガイド1.2版サマリー版」
- 一般社団法人日本フランチャイズチェーン協会 (2023)「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」
- NIST (2022)「Special Publication 800-63-4(Draft) Digital Identity Guidelines」
- OpenID Foundation (2022)「OpenID Connect for Identity Assurance 1.0」
- W3C (2022)「Verifiable Credentials Data Model v1.1」
- W3C (2022)「Decentralized Identifiers (DIDs) v1.0」
- 総務省 (2022)「第2次とりまとめ ～デジタル社会の新たな基盤の構築に向けて～」
- デジタルアーキテクチャ・デザインセンター (2022)「第2回インキュベーションラボ　テーマ 2：サービスに応じたデジタル本人確認ガイドラインの検討　活動成果報告(詳細版)」
- フィッシング対策協議会 (2022)「フィッシング対策ガイドライン（2022年度版）」
- OpenIDファウンデーション・ジャパン (2021)「サービス事業者のための、 継続的顧客確認（オンゴーイングKYC）に関する調査レポート」
- TRUSTDOCK (2021)「アドバイザリーボードからの提言（個人情報の取扱いについて）」
- TRUSTDOCK, MMD研究所 (2021)「オンライン本人確認（eKYC）に関する利用動向調査」
- OpenIDファウンデーション・ジャパン (2020)「サービス事業者のための本人確認手続き（KYC）に関する調査レポート」
- 経済産業省（2020）「オンラインサービスにおける身元確認手法の整理に関する検討報告書」
- 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」
- NIST (2017)「Special Publication 800-63-3 Digital Identity Guidelines」
- 総務省(2015)「公的個人認証サービス利用のための民間事業者向けガイドライン1.1版」
- OpenID Foundation (2014)「OpenID Connect Core 1.0」
- OpenID Foundation (2014)「OpenID Connect Core 1.0（日本語版）」
- IETF (2012)「The OAuth 2.0 Authorization Framework」

注釈：上記は本ガイドラインで参考にした主要文献を整理したもの。具体的な参考箇所については、各頁の出所に記載。

主な用語の定義

主な用語の定義（1/5）

#	用語	定義	参照先
1	AAL （当人認証保証レベル）	当人認証保証レベル（Authenticator Assurance Level）。アメリカ国立標準技術研究所（NIST）が定義する、当人認証プロセスの強度を示す。本ガイドラインでは、NISTが定義したAALを参考に作成された「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」のAALを参照している。	OpenIDファウンデーション・ジャパン (2021)「サービス事業者のための、継続的顧客確認（オンゴーイングKYC）に関する調査レポート」
2	API	システムやソフトウェアが公開している機能を外部から利用するためのプログラム上の規約	デジタル庁「デジタル社会の実現に向けた重点計画用語集」
3	eKYC	electronic Know Your Customerの略。 本ガイドラインでは、電子的=オンラインでの身元確認を指す。	OpenIDファウンデーション・ジャパン (2020)「サービス事業者のための本人確認手続き（KYC）に関する調査レポート」
4	FATF	The Financial Action Task Force (金融活動作業部会)の略。マネーローンダリング・テロ資金供与対策の国際基準（FATF勧告）を策定し、その履行状況について相互審査を行う多国間の枠組み。1989年のアルシュ・サミット経済宣言を受けて設立された。現在、G7を含む37カ国・2地域機関が加盟しており、その他9つのFATF型地域体を加えると、FATF勧告は、世界205の国・地域に適用されている。	金融庁ウェブサイト「FATF（金融活動作業部会）による第4次対日相互審査報告書の公表について」（2023年2月取得）
5	FIDO	Fast IDentity Onlineの略称で、FIDOアライアンスが提唱するオンライン認証方式のモデルとそれに基づく仕様群。	NTTドコモ（2020）「FIDOアライアンスにおけるオンライン認証の標準化動向とドコモの貢献」
6	IAL （身元確認保証レベル）	身元確認保証レベル(Identity Assurance Level)。アメリカ国立標準技術研究所(NIST)が定義する、身元確認の厳密さや 強度を示す。本ガイドラインでは、NISTが定義したIALを参考に作成された「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」のIALを参照している。	OpenIDファウンデーション・ジャパン (2021)「サービス事業者のための、継続的顧客確認（オンゴーイングKYC）に関する調査レポート」

主な用語の定義（2/5）

#	用語	定義	参照先
7	KYC	顧客確認、Know Your Customerの略称。 本ガイドラインでは身元確認と同義語と定義する（対面・オンラインを問わない。）。	OpenIDファウンデーション・ジャパン (2020)「サービス事業者のための本人確認手続き（KYC）に関する調査レポート」を参考に作成
8	シェアリングエコノミー	個人等が保有する活用可能な資産等（スキルや時間等の無形のものを含む。）をインターネット上のマッチングプラットフォームを介して他の個人等も利用可能とする経済活性化活動。	デジタル庁「デジタル社会の実現に向けた重点計画用語集」
9	耐タンパ性	内部の情報に対する不正な読み出し、改ざんなどの攻撃が困難であることを示す度合いのこと。一般に、「耐タンパ性を備えている」「耐タンパ性がある」と表現する場合、そのような攻撃が極めて困難であることを意味することが多い。	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」
10	中間的な手法	本ガイドラインにおいて中間的な手法とは、「適度に簡易で信頼性のある」身元確認手法のこと。具体例として「ホ方式の自動化」と「身元確認結果の活用」を指す。	
11	デジタル本人確認	本ガイドラインにおいてデジタル本人確認とは、デジタル技術を活用して、本人に係る情報を電子データとして取得・連携し、当該本人の実在性又は当人性を確認すること。	
12	電子証明書	公開鍵証明書ともいい、ある公開鍵を、記載された者が保有することを証明する電子的文書。認証局が記載内容を確認した上、電子署名を行うことで、その公開鍵の正当性を保証する。電子証明書には、発行者名、利用者名、電子証明書の有効期間、利用者の公開鍵などが記載されている。	JIPDEC「JIPDEC用語集」（2023年2月取得）

主な用語の定義（3/5）

#	用語	定義	参照先
13	電子署名	電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。 ・当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。 ・当該情報について改変が行われていないかどうかを確認することができるものであること。	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」
14	当人認証	ある行為の「実行主体」と、当該主体が主張する「身元識別情報」との同一性を検証することによって、「実行主体」が身元識別情報にあらかじめ関連付けられた人物（あるいは装置）であることの信用を確立するプロセスのこと。認証情報の確認方法により、以下の二つに大別する。 (1) 単要素認証 単一の認証情報によって、利用者本人であることを確認する当人認証方法。 ※例えば、ID と紐付けて、パスワード（≒本人だけが記憶している情報）、所有物、指紋、虹彩といった生体情報等のいずれかを用いる方法がある。 (2) 多要素認証 記憶、所有物、生体情報の各要素のうち、複数の認証情報を組み合わせることで、利用者本人であることを確認する当人認証方法。 ※例えば、パスワード（≒本人だけが記憶している情報）とワンタイムパスワード（ワンタイムパスワードを発行できるスマートフォンを所有していることを確認する。）を組み合わせる方法がある。	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」

主な用語の定義（4/5）

#	用語	定義	参照先
15	トークン	認証要求者が所持し管理する何かであり、認証情報等の認証に用いる情報を格納又は出力するハードウェアやソフトウェア（ICカード、ワンタイムパスワード生成機器等）、あるいは知識等の認証情報そのもの（パスワード等）等がある。	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」
16	フィッシング	実在する組織を騙って、ユーザーネーム、パスワード、アカウントID、ATMの暗証番号、クレジットカード番号といった個人情報を詐取すること。	フィッシング対策協議会 (2022)「フィッシング対策ガイドライン（2022年度版）」
17	マイナポータル	子育てや介護などの行政手続の検索、オンラインでの申請など、ワンストップのサービスを提供するウェブサイト。行政機関等が保有する自身の情報を確認することや、行政機関等からのお知らせ内容を確認することができる。なお、一部の機能の利用にはマイナンバーカードが必要。また、様々なサービスを提供する民間企業の方とは、社会保険や税などの手続のため、システム間での連携（API連携）も可能である。	デジタル庁ウェブサイト「マイナポータル」（2023年2月取得）
18	マスキング処理	本ガイドラインにおいてマスキング処理とは、第三者への提供に制限のある情報や機微な情報の漏えいを回避するため、本人確認書類の撮影前に無地の紙・付箋紙やマスキングテープ等で覆すこと、または、撮影後に画像編集アプリやソフトウェアで塗りつぶすこと。	
19	身元確認	手続の利用者の氏名等を確認するプロセスのこと。この確認プロセスは、一般的には、個人の場合、氏名、住所、生年月日、性別、法人等の場合、商号又は名称、本店又は主たる事務所の所在地、法人番号等について、当該情報を証明する書類の提示を求めるなどにより実施される。	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」

主な用語の定義（5/5）

#	用語	定義	参照先
20	ユーザーインターフェース（UI）	画面や音声入出力、キーボードなど、システムにおいて、ユーザーに対する情報提供や操作手段に関係する要素のこと。	デジタル庁「デジタル社会の実現に向けた重点計画用語集」
21	ユーザーエクスペリエンス（UX）	あるサービス（システム）を使う過程で起きるユーザーの知覚および反応。（ニーズが適切に満たされることで）達成感を感じたり、システムを快適に利用できる。	デジタル庁「デジタル社会の実現に向けた重点計画用語集」
22	ユーザビリティ	機能やサービスの使いやすさのこと。十分な機能が備わっており、効率的で、ユーザーが満足できる度合い。	デジタル庁「デジタル社会の実現に向けた重点計画用語集」
23	リスト型攻撃	何らかの手段により不正に入手した他者のID・パスワードをリストのように用いて様々なサイトにログインを試みることで、個人情報の閲覧等を行うサイバー攻撃	総務省「リスト型アカウントハッキングによる不正ログインへの対応方策について（サイト管理者などインターネットサービス提供事業者向け対策集）」の公表」（2023年2月取得）
24	ワンタイムパスワード（OTP）	利用可能回数が1回限りのパスワードのこと。	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」

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（50音順）	氏名（敬称略）
伊藤忠テクノソリューションズ株式会社	岡本　俊一
株式会社NTTドコモ	栗山　盛行
株式会社NTTドコモ	松岡　洋平
株式会社NTTドコモ	佐藤　拓実
株式会社NTTドコモ	加藤　周
KDDI株式会社	小岩井　航介
株式会社ジェーシービー	南井　享
セコム株式会社	佐藤　雅史
ソフトバンク株式会社	作田　宗臣
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	柏井　茂達
デロイト トーマツ サイバー合同会社	宮崎　貴暉
トッパン・フォームズ株式会社	本多　英明
トッパン・フォームズ株式会社	後藤　聡
トッパン・フォームズ株式会社	田村　康子
トッパン・フォームズ株式会社	福田　智洋
株式会社TRUSTDOCK	菊池　梓
株式会社TRUSTDOCK	神谷　英亮
株式会社TRUSTDOCK	笠原　基和
株式会社TRUSTDOCK	中村　竜人
株式会社Liquid	保科　秀之
株式会社Liquid	近藤　潤也
株式会社Liquid	池田　雄一郎

オブザーバー

所属（50音順）	氏名（敬称略）
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
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
デジタル庁	吉田　泰己
デジタル庁	林　達也
デジタル庁	山田　達司
デジタル庁	前川　沙美
デジタル庁（元）	天達　泰章
デジタル庁	鈴木　智明

アドバイザー

所属（50音順）	氏名（敬称略）
OpenID Foundation	崎村　夏彦

スペシャルサンクス

所属（50音順）	氏名（敬称略）
トッパン・フォームズ株式会社	水口　慎也

その他ご協力いただいた皆様

所属（50音順）	氏名（敬称略）
株式会社TRUSTDOCK	肥後　彰秀
株式会社TRUSTDOCK（元）	杉　眞里子
株式会社TRUSTDOCK（元）	升方　治佳
株式会社TRUSTDOCK	渡辺　良光
株式会社TRUSTDOCK	竹位　和也

*網掛けは事務局メンバー

コラム目次

【コラム】OpenID Connect とは

【コラム】OpenID Connect とは

1. OpenID Connect とは?
2. OpenID Connect と OAuth 2.0の違い
3. OpenID Connect for Identity Assurance とは？

参照関連仕様

- The OAuth 2.0 Authorization Framework
- OpenID Connect Core 1.0
- OpenID Connect Core 1.0（日本語訳）
- OpenID Connect for Identity Assurance 1.0

1. OpenID Connect (OIDC)とは？

「ソーシャルログイン」とも呼ばれ、SNSアカウントなどを利用して、各種サービスにログインを行うためのプロトコルです。

技術的には、API「認可」フレームワークである OAuth2.0 を拡張し、「認証イベント」を連携できるようにしたもので、**「パスワード」を直接受け渡すことが無いため、安全にログインを行うことができます**。

OIDCの利用シーンの例

SNSアカウントや銀行アカウントを利用したログインの例

ソーシャルログイン画面の例

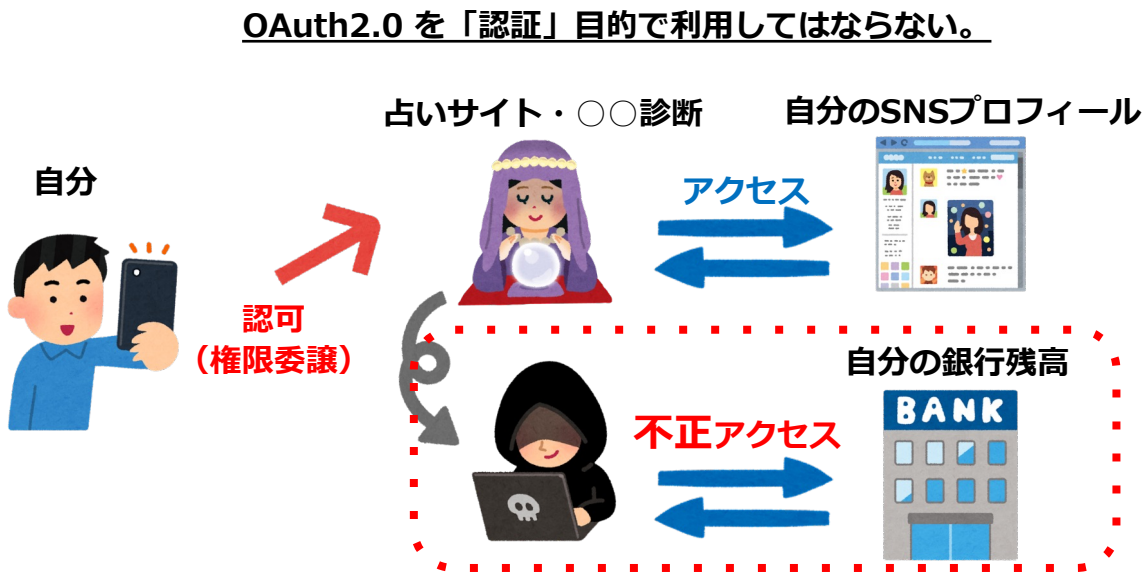
出所：（右画像）KDDIトビラ（https://time-space.kddi.com/ict-keywords/20191204/2794）

2. OpenID Connect と OAuth 2.0の違い

OpenID Connect では、「特定の人物が、特定のサービスにログインするため、特定の認証方法を用いてこの時間に認証した」という情報を「IDトークン」という形で、ログイン元からログイン先に提供します。

OAuth2.0で得られるのは、特定のAPIを使う権限「認可」であり、本人であることの証明ではないため、OAuth2.0を「認証」目的で利用すると危険です。

OpenIDとOAuth2.0の比較



OAuth2.0 で提供されるのは「認可」＝権限委譲されたことを示す「アクセストークン」である。悪意のある第三者が「アクセストークン」を取得し、他サービスへ送信することで、本人になりすましてログインを行えてしまう可能性がある。

一方、OpenID Connect で提供される「IDトークン」には、「認証先サービス」「認証時間」などの情報が含まれているため、ユーザが意図した以外のサービス事業者が不正に「IDトークン」を奪取したとしても、それを再利用することはできない。

3. OpenID Connect for Identity Assurance とは？

OpenID Connect for Identity Assurance は、各種個人情報に対してメタデータを付与できるOpenID Connectの拡張仕様です。

OpenID Connect for Identity Assuranceの概要

- OpenID Connectを利用すると、「氏名」、「メールアドレス」、「生年月日」など、様々な個人情報を連携できますが、情報の確度は連携元ごとに異なります。
    - 例えば、SNSで20歳以上と記載があっても、それを根拠にお酒を売ることはできません。
- そこで、オンラインでの情報連携による身元確認のニーズに対応するため、OpenID Connect仕様を拡張し、各種個人情報に対して、「誰が」「どのように」「いつ」「何を元に」確認したか等を、メタデータとして付与できる仕様 OpenID Connect for Identity Assurance が開発されています。
- OpenID Connect for Identity Assuranceにより、あらゆる事業者の身元確認結果を活用しやすくなることが期待されています。

注釈：OpenID Connectで連携される属性情報は、”claim”（クレーム）と呼ばれます。一方、OpenID Connect for Identity Assurance で連携される身元確認済みの属性情報のセットは、“Verified Claims” と呼ばれます。

【コラム】個人情報の漏えい事例とその要因

主な不正事案について

本人確認の一義的な目的は、取引や契約に際して生じるリスクを回避することであり、なりすましや偽造などの不正を防ぐために、サービスに応じた対策が求められます。

ここでは、実際に起きた主な不正事案のうち、事案の概要と再発防止のためにとられた対策、又は有効と考えられる対策を紹介します。

1. スマホ決済アプリの不正利用
2. モバイルウォレット経由の口座不正出金
3. フィッシング詐欺
4. フィッシング対策について

また、API経由で事業者のデータベースに不正アクセスを受け、事業者が保有する本人確認に用いた個人情報が大量に漏えいした事案について、概要を紹介します。

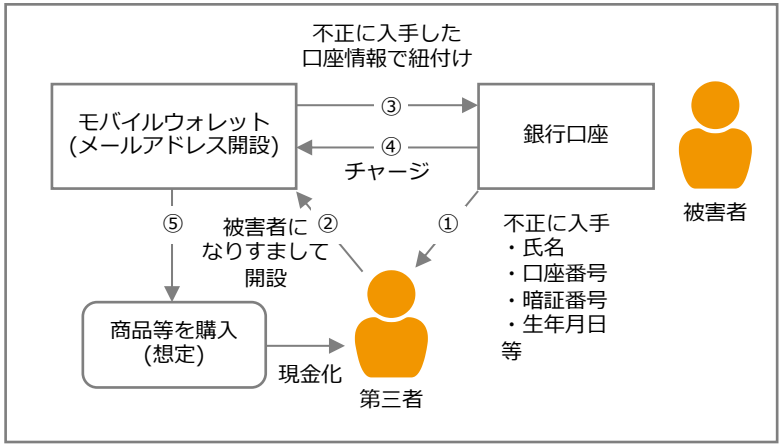
5. 本人確認に用いた個人情報が大量に漏えいした事案

1. スマホ決済アプリの不正利用

- 第三者が利用者のIDやパスワードを不正に入手、アプリに登録されていたクレジットカード等からチャージ後、店舗で商品を購入したもので、被害者らのIDには海外からの不正アクセスが集中していた。
- 外部で入手したIDとパスワードを使って不正にログインする「リスト型アカウントハッキング」の可能性が高いと発表されており、攻撃を受けた要因として「**複数端末からのログインに対する対策**」や「**二要素認証等の追加認証の検討**」が十分でなかったとされている。
- 「複数端末からのログインに対する対策」としては、**二重でログインした場合は利用者に通知が届く仕組み**を設けたり、**ログインできる端末を限定**する。また、国内のサービスであれば**海外からのIPアドレスを制限する**ことも有効。
- 「二要素認証等の追加認証の検討」については、**ソフトトークンによるワンタイムパスワードを使ったログイン**やパスワードを必要としない生体認証を用いた**FIDO（Fast Identity Online）認証**導入などのセキュリティ対策がある。

2. モバイルウォレット経由の口座不正出金

- モバイルウォレットを経由して提携銀行に口座を保有する人の預金が不正出金される被害が多発した。被害者の銀行口座が他人の作ったモバイルウォレットと、いつの間にか紐付けされ、知らぬ間に預金を引き出された。
- **メールアドレスだけで開設でき、本人確認が不十分であった**ことが原因の一つである。モバイルウォレット開設後、そこに銀行口座を登録すると「本人確認」と見なし、銀行口座からのチャージ（引き出し）ができてしまう。第三者はこの仕組みを利用して、不正に入手した氏名、口座番号、生年月日、暗証番号等の情報を用いて被害者の口座を紐付け、不正出金した。
- 事業者は、**SMSによる2要素認証、および、銀行口座登録前にeKYC等による身元確認を実施。**また、銀行側においても、資金移動業者のアカウントと銀行口座を紐付けて口座振替を行う際は、**複数要素認証を導入する**などのセキュリティ強化が必要となった。



3. フィッシング詐欺

フィッシング（Phishing）とは、「魚を釣る（Fishing）」フィッシングのことではなく、人をだまして情報を盗み、最終的に金銭的な利益を得ようとする不正行為のことを意味する。フィッシングにより、例えば、あなたのクレジットカード情報やインターネットバンク、ショッピングサイトの登録情報（ID、パスワード）が盗まれ、勝手にお金が引き出されたり、物品を購入されたりする恐れがある。フィッシングはphishingというつづりで、釣りのfishingを、昔のハッカーが「f」を「ph」にするのを好んでいたことから作られた造語といわれている。

フィッシングの報告件数は2020年から毎年倍増しており、2022年の年間累計は96万8,832件*となった。悪用されるブランド件数も増加しており、EC系が最も多く、クレジット・信販系、オンラインサービス系、交通系、金融系、省庁などをかたるフィッシング詐欺が発生した。

クレジットカード情報の詐取を目的としたフィッシング詐欺報告件数が最も多く、金融以外のブランドのフィッシングもクレジットカード情報の詐取に悪用されている。

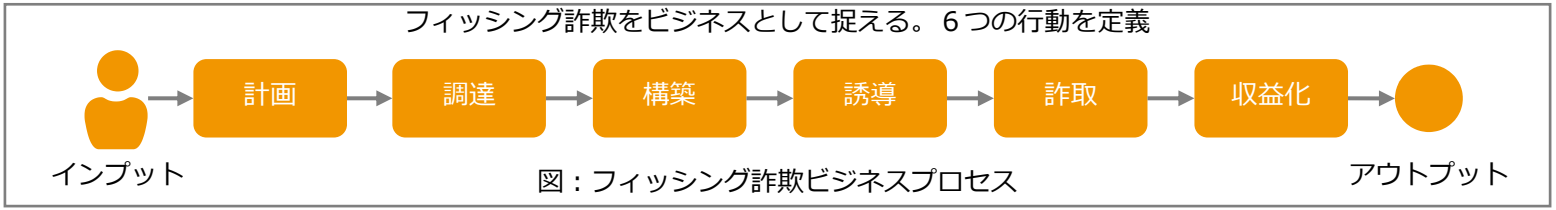
SMSによるフィッシング詐欺はスミッシングと呼ばれている。宅配便関連の不在通知やApple、アマゾン、auなどのスミッシングが発生している。事業者は、安全なSMS 送信を行うことが重要となる。スミッシングには国際網を経由した SMSの利用が多いため、 **国内の携帯電話事業者に直接接続している SMSを利用する**か、**SMSの次世代版であるRCS(Rich Communication Service) に準拠した「+メッセージ」を利用する**ことも有効である。また、メールであれば、**なりすましメール対策技術 (DMARC) への対応や BIMIに対応してブランドアイコンを表示**、正規メールの視認性向上も対策の一つとなる。

詳細は、フィッシング対策ガイドラインも参照。

注釈：2022年の年間累計は、フィッシング対策協議会「フィッシング報告件数」の2022年報告の合計値。
出所：フィッシング対策協議会ウェブサイトより

4. フィッシング対策について

- フィッシング対策は、事業者、利用者の両者で対応が必要となる。
- フィッシング詐欺は、計画→調達→構築→誘導→詐取→収益化の6つの行動によって行われることから行動に沿って対策することがポイントとなる。



図：フィッシング詐欺ビジネスプロセス

- 「誘導」： **送信ドメイン認証「 DMARC 」＋ポリシー =reject 指定による対策**を導入する。
- 経済産業省、警察庁及び総務省は、クレジットカード番号等の不正利用の原因となるフィッシング被害が増加していることに鑑み、クレジットカード会社等に対し、**送信ドメイン認証技術（DMARC）の導入**をはじめとするフィッシング対策の強化を要請した。（2023年2月1日）
- 「収益化」： SMS 認証、ワンタイムパスワードなど **複数要素認証を要求する**。経済産業省では、クレジット決済の本人確認、複数認証の義務付けを検討（認証規格「EMV3-Dセキュア*」）（2022年10月11日）
- 利用者へフィッシング対策に関する情報を提供し、**フィッシングに遭ってしまったときの対処をアドバイス**していくことも信頼継続のために必要。

詳細は、フィッシング対策ガイドラインも参照。

注釈：EMV3-Dセキュアについては、「【コラム】3-Dセキュアとは」を参照。
出所：フィッシング対策協議会ウェブサイトより

5. 本人確認に用いた個人情報が大量に漏えいした事案

（概要）

- APIを経由で事業者のクラウドサーバーに不正アクセスが行われ、保存されていた170万人分を超えるユーザーの本人確認書類画像が不正取得された。
- 不正取得されたのは、運転免許証、健康保険証、パスポート、マイナンバーカード（表面）等の画像で、画像は、ユーザーの顔写真、氏名、住所などが確認できる状態とされていた。

（対策）

- 外部ネットワークからのアクセスやリクエスト制限の厳格化、本人確認書類画像データの保管場所の移動と暗号化、サーバーへのログイン認証の厳格化と監査証跡の強化などの対策を講じるとともに、外部のeKYCサービスを導入した。
- 「個人情報管理のルール」及び「情報セキュリティに関するルール」を見直し、ユーザー情報の保存期間をそれまでの「退会後10年間」から、本人確認書類の画像は「事業者への提出後72時間」、個人情報データは「退会後90日間」に変更した。

【コラム】NIST SP 800-63-4(Draft)について

NIST SP 800-63 は米国政府機関における自然人向けのデジタルアイデンティティのガイドラインである。

NIST SP 800-63-4(Draft)


NIST Special Publication
NIST SP 800-63-4 ipd
Digital Identity Guidelines
Initial Public Draft
David Temoshok
Ryan Galluzzo
Connie LaSalle
Naomi Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory
Yee-Yin Choong
Information Access Division
Information Technology Laboratory
Diana Proud-Madruga
Sarbari Gupta
Electrosoft
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-4.ipd
December 2022
U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

- 2017年6月に第3版(SP 800-63-3)が発行された後、2020年6月～8月の第4版草稿前コメント募集の期間を経て、寄せられたコメント内容をはじめ最新の技術動向や脅威環境を反映した第4版草稿(SP 800-63-4(Draft))が2022年12月16日に発行された。
- NIST SP 800-63は国内外で広く参照されているガイドラインであり、本ガイドラインも第3版を参考に作成している。
- 更新された第4版(Draft)の内容も引き続き参考にし、今後の本ガイドラインの更新において、必要に応じて内容を反映していきたいと考えている。
- 構成は第3版から変更なく、Base Volume、63A、63B、63Cの4部構成となっており、それぞれ内容は下記の通りである。

SP 800-63-4 - Digital Identity Guidelines
全てのVolumeから参照される基本的な内容およびリスク評価

SP 800-63A - Enrollment & Identity Proofing
申請者の身元確認と登録に関する要件とガイダンス

SP 800-63B - Authentication & Lifecycle Management
当人認証とライフサイクル管理に関する要件とガイダンス

SP 800-63C - Federation & Assertions
フェデレーションにおける要件とガイダンス

出所：SP 800-63-4 (Draft), Digital Identity Guidelines | CSRC (nist.gov)

2. 主な変更点

第3版からの主な変更点（本ガイドラインに関連すると思われる事項の抜粋）

SP 800-63-4
Digital Identity Guidelines

- 「非フェデレーションモデル」に加えて、「フェデレーションモデル」の追加
- xAL選択のフローチャートの、リスク管理プロセス詳述文章への置き換え

SP 800-63A
Enrollment & Identity Proofing

- IALの再定義

第3版	第4版草稿	概要
IAL1	IAL0	検証なし
IAL2	IAL1	検証あり
IAL2	IAL2	生体情報での検証あり
IAL3	IAL3	対面での検証あり

- Digital Evidenceの要件明記
- 受け入れ可能なEvidenceの拡張

SP 800-63B
Authentication & Lifecycle Management

- フィッシング耐性オーセンティケーターの定義追加、要件の更新
- 生体認証の性能要件追加
- アクティベーションシークレットの要件追加
- NFCやBluetoothなどワイヤレス技術で接続されるオーセンティケーターの要件追加

SP 800-63C
Federation & Assertions

- FALの全体的な見直し
- フェデレーションプロセスに新しいステップが追加
- FALの定義から暗号化要件撤廃
- FAL2にてインジェクション保護要件の追加
- FAL3 におけるbound authenticatorの追加

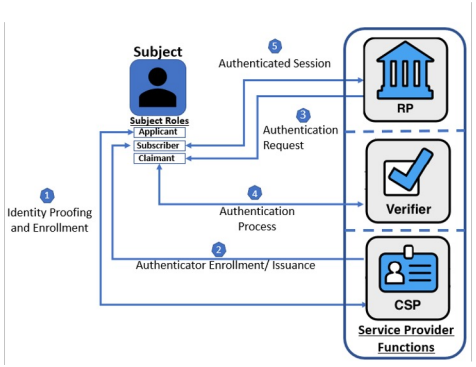
3. NIST SP 800-63-4(Draft)（Base Volume） の概要

SP 800-63-4
Digital Identity Guidelines

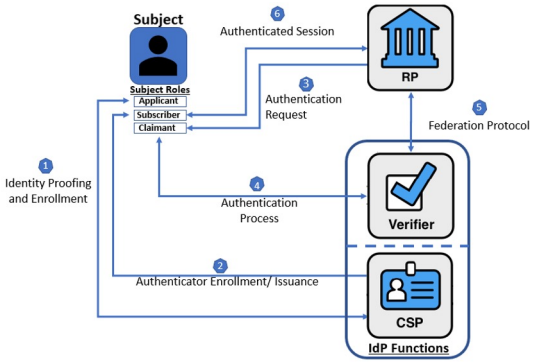
SP 800-63-4(Draft) 概要
：全てのVolumeから参照される基本的な内容およびリスク評価

Base Volumeに記載されている主な内容は下記の通り。

- デジタルアイデンティティの基本
  基本的な概念や、デジタルアイデンティティモデル



非フェデレーションモデル



フェデレーションモデル

- デジタルアイデンティティのリスク評価
  身元確認、当人認証、フェデレーションの保証レベルを選択する際のリスク評価の方法やプロセス、判断基準

影響カテゴリー	個人への害	組織への害	（その他の害）	総合的な影響レベル
Mission Deliveryへの損害	低 / 中 / 高	低 / 中 / 高	低 / 中 / 高	
信頼や評判の損害	低 / 中 / 高	低 / 中 / 高	低 / 中 / 高	
機密情報の喪失	低 / 中 / 高	低 / 中 / 高	低 / 中 / 高	
経済安定性の損害、喪失	低 / 中 / 高	低 / 中 / 高	低 / 中 / 高	
人命の喪失、安全や健康、環境の安定性の損害	低 / 中 / 高	低 / 中 / 高	低 / 中 / 高	
法律、規制、契約上の義務の不遵守	低 / 中 / 高	低 / 中 / 高	低 / 中 / 高	

適切なxALを選択

- 用語定義、略語
  関連する用語定義や略語についての説明

4. NIST SP 800-63A-4(Dtaft) の概要

SP 800-63A
Enrollment & Identity Proofing

SP 800-63A-4(Draft) 概要
：申請者の身元確認と登録に関する要件とガイダンス

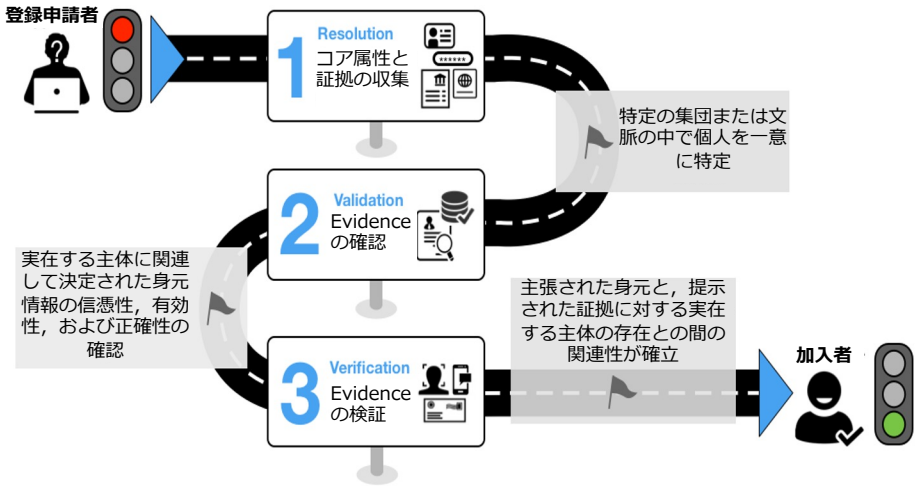
63A に記載されている主な内容は下記の通り。

- 身元確認におけるプロセスとその要件

プロセス	要件
Resolution	• 身元確認に必要な証拠とコア属性の収集を行うプロセス • 必要な証拠についての要件
Validation	• 収集した証拠やコア属性の真正性を確認するプロセス • 確認方法についての要件
Verification	• 確認した証拠やコア属性が間違いなく申請者に紐づくものであることを検証するプロセス • 検証方法についての要件

- 身元確認保証レベルの概要と各レベルの詳細要件

レベル	概要
IAL0	• 身元確認なし • 提示された属性情報は何の確認も検証もされない
IAL1	• 規定された情報源にてコア属性の確認および検証を行わなければならない
IAL2	• 生体情報での検証を行わなければならない
IAL3	• 対面あるいは監視付きのリモートにて物理的な本人確認資料を確認することにより、検証されなければならない



身元確認におけるプロセス

5. NIST SP 800-63B-4(Draft) の概要

SP 800-63B
Authentication & Lifecycle Management

SP 800-63B-4(Draft) 概要
：当人認証とライフサイクル管理に関する要件とガイダンス

63B に記載されている主な内容は下記の通り。

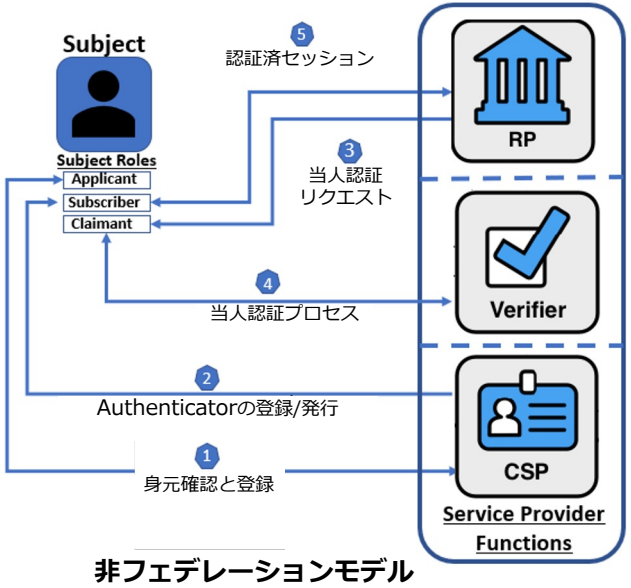
- 当人認証におけるプロセスとその要件

プロセス	要件
Authenticatorの発行/登録	• Authenticatorを発行し登録するプロセス • 発行と登録（対象者とのバインディング）についての要件
Authenticatorの有効性確認	• 対象者が、当人認証に使用されるAuthenticatorを制御していることを確認するプロセス • Authenticatorについての要件 　• 種類とそれぞれの詳細 　• ライフサイクル（紛失、盗難、複製、失効） • 生体認証についての要件
認証済セッション管理	• 当人認証の結果、認証済セッションを発行/管理するプロセス • セッション管理について（セッションの長さや再認証の要件など）の要件

※プロセスについてはBase Volumeを参考に記載。63Bの本文では表中のプロセスの言及はない。

- 当人認証保証レベルの概要と各レベルの詳細要件

レベル	概要
AAL1	• 単一認証要素
AAL2	• 多要素認証 • 承認された暗号技術
AAL3	• ハードウェアベースの暗号多要素認証 • フィッシング耐性 • 承認された暗号技術



非フェデレーションモデル

6. NIST SP 800-63C-4(Draft) の概要

SP 800-63C
Federation & Assertions

SP 800-63C-4(Draft) 概要
：フェデレーションにおける要件とガイダンス（フェデレーション：ネットワーク化されたシステム間での認証情報と属性情報の伝達）

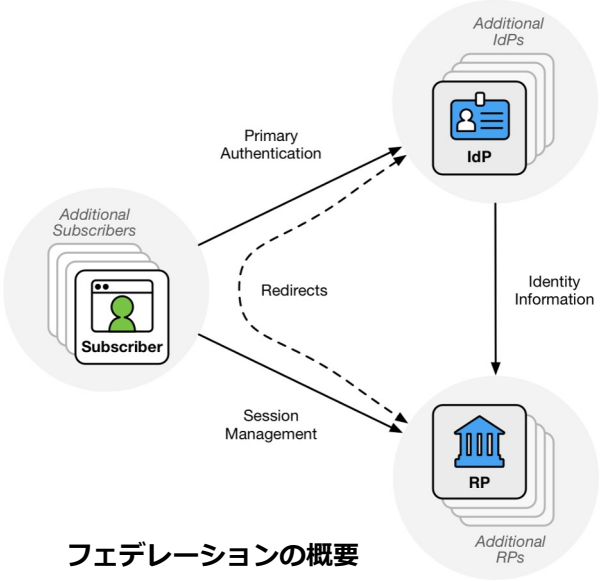
63C に記載されている主な内容は下記の通り。※フェデレーションは、身元確認や当人認証と異なり、フェデレーションモデルを採用する場合にのみ発生

- フェデレーションにおけるプロセスとその要件

プロセス	要件
信頼の合意形成	• RPとIdPが接続するための最初のプロセス • お互いのポリシーや要求、属性提供の責任の所在を明らかにするなど
登録	• プロトコルレベルで接続ができるようにするプロセス • RPを表す識別子やクレデンシャルの発行、その他プロトコルに必要な情報を交換して登録するなど
認証と属性の開示	• 当該トランザクションでやりとりする内容を決め、ユーザーに対して認証を行い、決定した内容を含むAssertionを提示するプロセス • Assertionに含む属性やAssertionの提示についての要件など

- フェデレーション保証レベルの概要と各レベルの詳細要件

レベル	概要	対応する既存のプロトコル例	
FAL1	• IdPにより署名されたAssertionを使うなどの基本的な要件を満たす	OIDC	• Implicitクライアントプロファイル • ハイブリッドクライアントプロファイル
		SAML	• Rediret Binding • POST Binding
FAL2	• バックチャネルでのやりとりなど、Assertionのインジェクション保護の要件を満たす	OIDC	• Basic Client プロファイル
		SAML	• Artifact Binding • SOAP Binding
FAL3	• RP側での認証も併用し、Assertionの盗難/偽造に対する保護の要件を満たす	いずれのプロトコルを利用した場合でも、Assertionのみでなく、bound authenticatorを利用したRP側での認証の併用が必須	



フェデレーションの概要

【コラム】海外動向に関して

近年に発表されている主な本人確認基準は、いずれもNISTとは異なり4段階以上の区分で保証レベルを設定している

近年発行された本人確認基準の比較

国名	発行組織	規定名	発行年月	区分数
アメリカ合衆国	NIST	SP800-63-3-A	2017/06	3段階
イギリス	Cabinet Office & Government Digital Service	Guidance – How to prove and verify someone's identity	2021/02	4段階
ドイツ連邦	BSI	TR-03147-1 v1.0.6[Technical Guideline]	2021/12	4段階
カナダ	DIACC	Pan-Canadian Trust Framework: Verified Person	2022/03	4段階
ニュージーランド	DIA (NZ Gov.)	Identification Management Standards	2022/06	4段階
オーストラリア	Australian Government	The Trusted Identity Framework (TDIF) Ver 4.7 – Identity proofing levels	2022/06	6段階
タイ	ETDA	Digital Identity Ver2.0	2022/09	5段階
アメリカ合衆国	NIST	SP800-63-4-A(Draft)	2022/12	3段階*

注釈：従来(SP800-63-3)ではIAL1として扱われていたレベルがIAL0(保証なし)として扱われているため、実質的な4段階の分類とみなすことも可能

【コラム】新しい当人認証方式 パスキー (Passkeys)

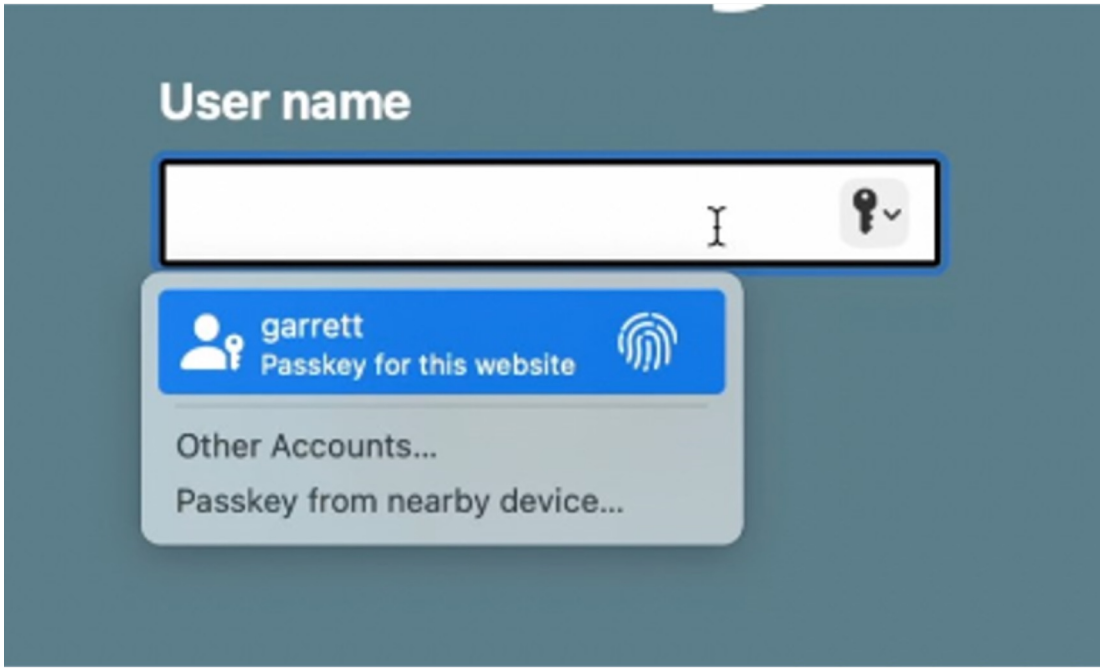
1. パスキーの特徴

パスキーの概要

- FIDO(ファイド)、Web Authntication(Web認証) とも呼ばれる。
- ユーザ端末内で、 Webサイト別に管理され、保存されている**秘密鍵**を使った**公開鍵暗号方式**による認証を行う。パスワードのような、使い回しによる被害や、フィッシングによる被害を防げる。
- ログインのために秘密鍵を利用する際、ユーザ端末上で、生体認証やパスコードによる認証が求められるため、**ユーザ目線では、生体認証**を行っているように見える。
- 秘密鍵は、Apple ID、Google ID、Microsoft IDに紐付けて各OSの提供するクラウド等にバックアップされ、端末紛失・故障時にも復旧が可能な場合もある。
    - 一方、 クラウドのIDが盗まれると、紐付く秘密鍵も利用されるリスクがある

2. パスキーのログインイメージ

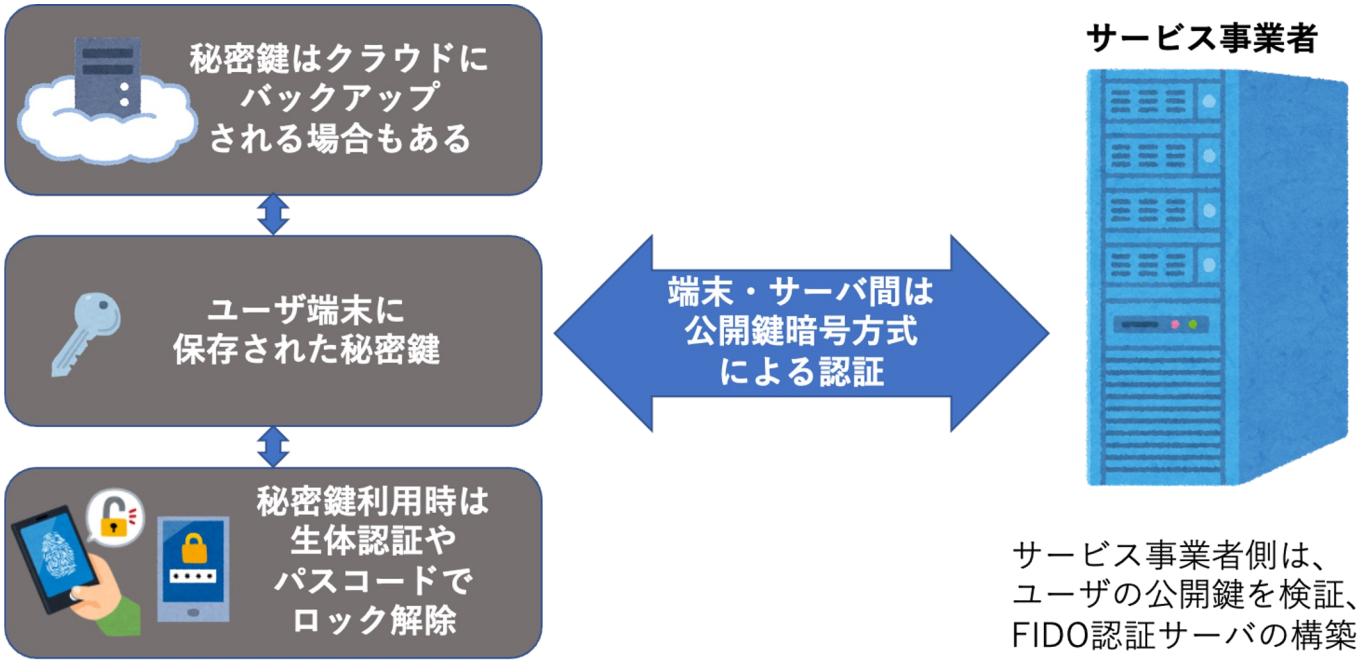
パスキーによるログイン画面の例



出所：Apple社ウェブサイトより

3. パスキーのシステム構成

パスキーによるログイン画面の例



サービス事業者側は、
ユーザの公開鍵を検証、管理するための
FIDO認証サーバの構築が必要

出所：FIDO Allianceウェブサイトより

【コラム】3-Dセキュア* とは

*本コラムはクレジット取引セキュリティ対策協議会
「EMV 3-Dセキュア導入ガイド 1.2版」
「EMV 3-Dセキュア導入ガイド 1.2版 サマリー版」
を基に作成しております。
詳細は同ガイドをご参照ください。

【コラム】3-Dセキュアとは

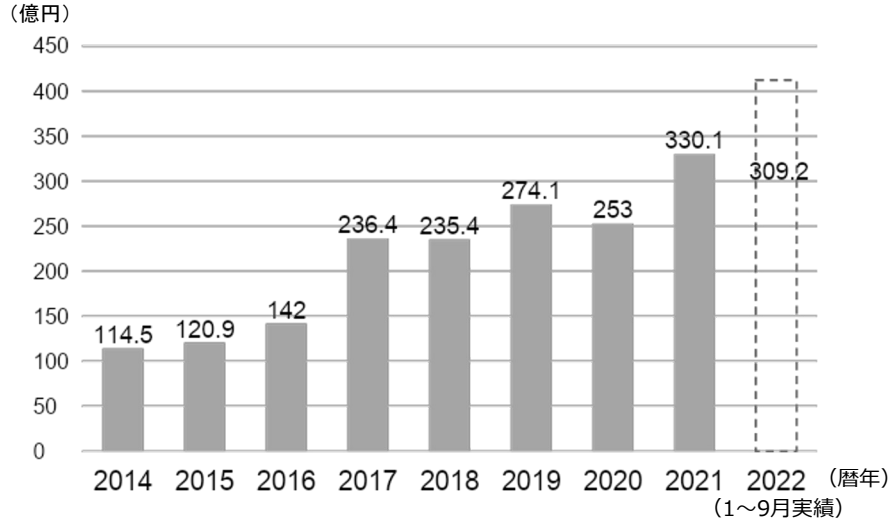
1. クレジットカード利用における不正利用の状況
2. 3-D セキュアとは?

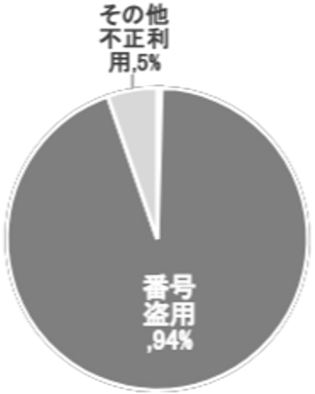
1. クレジットカード利用における不正利用の状況①

オンラインショッピング・非対面取引でのクレジットカード利用は拡大していますが、一方で不正利用も増加しています。2021年統計では不正利用被害額は330億円にのぼっており、2022年は被害額の更新が予想されます。

不正利用の大部分が「番号盗用（主に非対面取引でのクレジットカード番号等のなりすましによる不正利用）」です。

クレジットカードにおける不正利用被害の発生状況と被害額内訳





注釈：2022年は1月～9月の実績。破線は12ヶ月換算での予測（イメージ）。
出所：日本クレジット協会「クレジットカード不正利用被害の集計結果について（2022年12月28日）」より作成

2. EMV3-Dセキュアとは？①

「EMV3-Dセキュア」とは、オンラインショッピング時にクレジットカード番号等の情報の盗用による不正利用を防ぎ、 安全にクレジットカード決済を行うために国際ブランドが推奨する本人認証サービスです。

EMV3-Dセキュアの導入イメージ

EMV3-Dセキュア導入前

- クレジットカードそのものを盗難された場合、オンラインではカード利用者が本当にカード保有者かどうかが確認できなかった。

EMV3-Dセキュア導入後

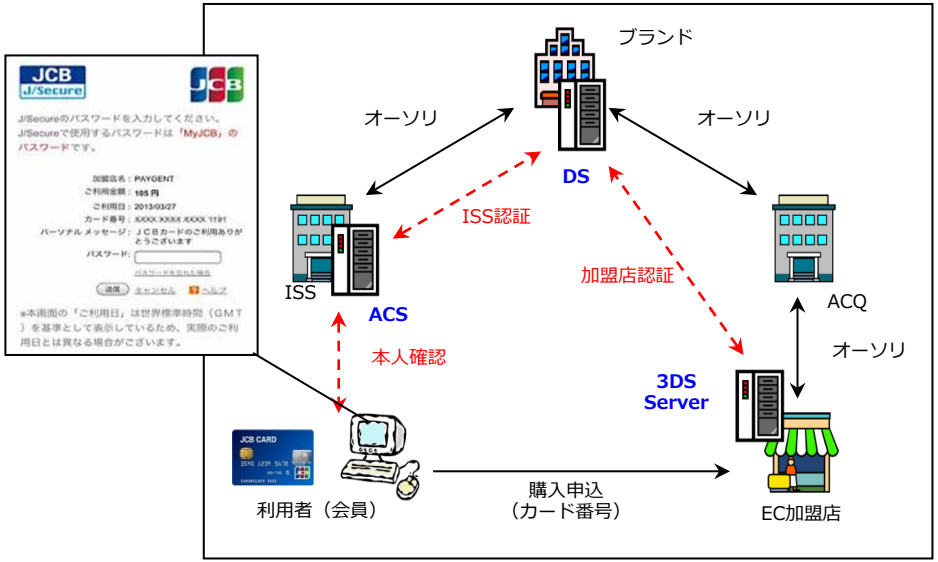
- EMV3-Dセキュアを用いることで、オンラインでのカード利用者が本当にカード保有者かどうかを確認できるようになった。
(仕組みは後述)

2. EMV3-Dセキュアとは？②

EMV3-DセキュアとはEC加盟店における不正利用防止のための本人認証手法の一つです。

近年では加盟店やPSP（決済代行会社）から決済に使用されたデバイスの設定情報や購入パターンに関する情報等がイシュアーへ送信され、イシュアーにて当該取引の不正度合いをリスク判定する「リスクベース認証」の機能が実装されており、リスクの低い取引ではパスワード等による認証を行わずに決済等が完了するようになっています。（後述）

EMV3-Dセキュアのフロー（イメージ図）



DS (Directory Server)	• 各カードブランドが運営するサーバー • カード番号に紐付く ACSを判別し、3DS サーバーと ACS間の電文の仕向け中継を行う
3DS Server (3D Secure Server)	• DSとEC加盟店とのデータ通信を取り持つ認証サーバー • 3Dセキュアの認証要求を行なう加盟店やPSP（決済代行会社）とDS間の機能的インタフェースを提供
ACS (Access Control Server)	• イシュアー側の認証サーバー • カード番号が3Dセキュア認証の対象であるかを検証し、対象である場合、認証要求に対するリスク判定や個別のトランザクションの認証を実行する

出所：クレジット取引セキュリティ対策協議会「EMV 3-Dセキュア導入ガイド1.2版」を参考にOpenIDファウンデーション・ジャパンにて作成.

2. EMV3-Dセキュアとは？③

「EMV3-Dセキュア」では、これまでの「3Dセキュア1.0（2022年10月サービス終了）」で課題となっていた「かご落ち」の増加を防ぐため、あらゆる取引においてID・パスワードの入力を求める形を改め、パスワード入力負荷の軽減やユーザビリティの改善を行っています。

「EMV3-D セキュア」の改善点

旧3Dセキュア（2022年10月サービス終了）	EMV 3-Dセキュア			
	特長	内容	メリット	
			会員	加盟店
全取引にパスワードを毎回入力	パスワード入力負荷を低減	・原則リスクベース認証のみとなり、会員へのパスワード要求が不要（フリクションレス）※	入力負荷軽減	取引離脱（カゴ落ちの減少）
固定パスワードで一律認証	ワンタイムパスワードによる本人認証	・中リスク判定時のみワンタイムパスワードなどによる追加認証を実施	パスワード漏洩による不正リスクの軽減	会員のパスワード忘れによる機会損失の軽減
ブラウザ取引のみ	スマホアプリへの対応	・ブラウザに加え、スマートフォンやタブレットのアプリ内決済に対応	利便性向上	認証強化

※「カゴ落ち」：ECサイトでカートに商品を入れたものの、購入まで至らず離脱してしまうこと

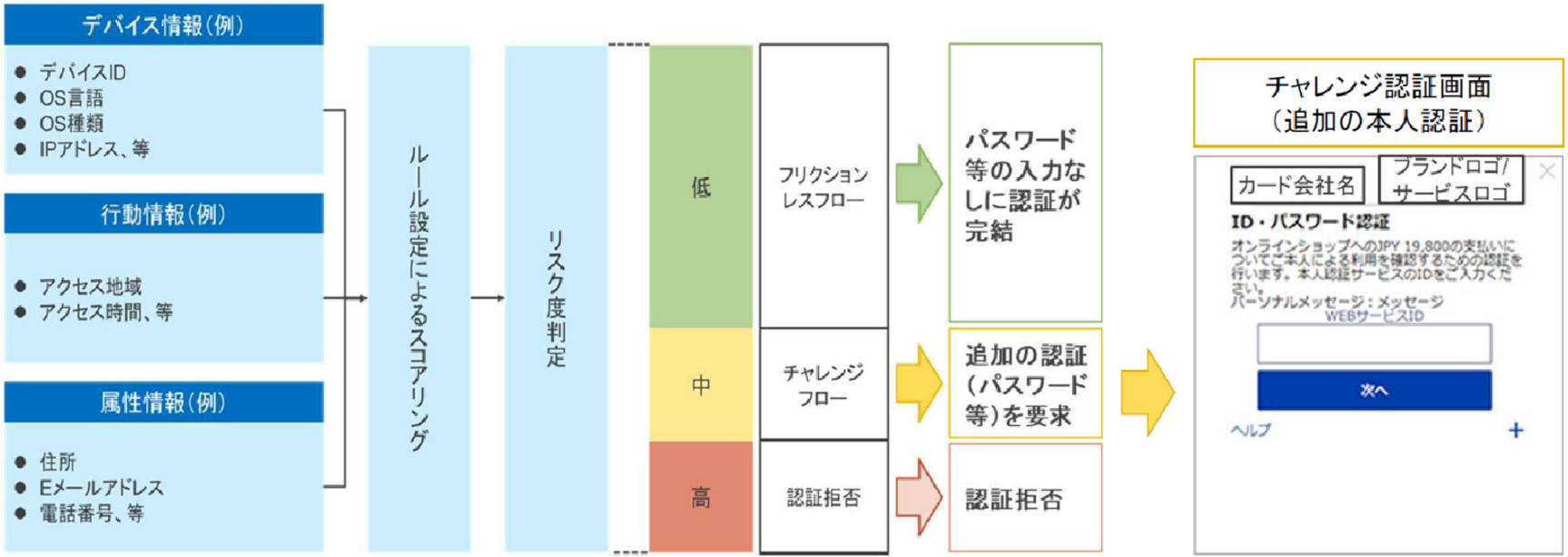
※「リスクベース認証」：後述

出所：クレジット取引セキュリティ対策協議会「EMV 3-Dセキュア導入ガイド 1.2版 サマリー版」より.

2. EMV3-Dセキュアとは？④

リスクベース認証とは、ECで使用されるパソコンやスマートフォンにおける機器やネットワークの情報から不正利用を判定する手法で、スコアリングによるリスク度判定によって、認証処理が異なります。

EMV3-Dセキュアにおける「リスクベース認証」のイメージ



出所：クレジット取引セキュリティ対策協議会「EMV 3-Dセキュア導入ガイド 1.2版 サマリー版」より.

2. EMV3-Dセキュアとは？⑤

EMV3-Dセキュアを実装した取引のうち、「認証成功」または「イシュアーがEMV3-Dセキュアに未対応」及び「会員がEMV3-Dセキュアに未参加*」の取引において不正利用が発生した場合、リスク負担は原則イシュアーとなります。（=ライアビリティシフト）

EMV3-Dセキュアにおける不正リスク分担（表）

	ステータス	リスク負担
1	EMV 3-Dセキュア認証成功	加盟店は免責対象※1
2	会員のカード発行会社 または会員がEMV 3-Dセキュア未参加	
3	EMV 3-Dセキュア認証取引外	加盟店※2は免責対象外

「かご落ち」が発生する可能性を考慮しても、EC加盟店が3-Dセキュアを導入するのは、カードの不正利用によるチャージバックが発生した場合に、カード発行会社が売上代金を補償する形となるため。

※1 カード登録時にEMV 3-Dセキュア認証していても、以降の取引時にもEMV 3-Dセキュア認証しない限りは免責対象外となる。
※2 契約のカード会社（アクワイアラー）との契約内容による。

注釈：「会員がEMV3-Dセキュアに未参加」とは、EMV3-Dセキュアを利用可能な状態にしていないこと。
出所：クレジット取引セキュリティ対策協議会「EMV 3-Dセキュア導入ガイド 1.2版 サマリー版」より.

【コラム】VC (Verifiable Credential)について

【コラム】VC（Verifiable Credential）について

1. VC（Verifiable Credential）とは?
2. VCのもたらす世界観（可能性）について
3. 本人確認手法としてのVC／DIDの活用可能性について

参照関連仕様

- Verifiable Credentials Data Model v1.1, W3C Recommendation 03 March 2022
- Decentralized Identifiers (DIDs) v1.0, W3C Recommendation 19 July 2022
- OpenID for Verifiable Credential Issuance / OpenID for Verifiable Presentations

1. VC（Verifiable Credential）とは①

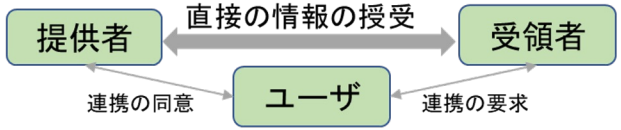
デジタル署名が施され「発行者から正しく発行された情報である事（情報の真正性）を検証可能」な属性情報のデータモデルで、ワクチン接種証明書などで活用が始まっています。

DID（※）と組み合わせることにより、受領者と発行者の間に直接的なシステム間接続関係を構築しなくても、受領者は情報の真正性を検証可能となります。

従来の情報連携方式とVCを使った情報連携方式の比較

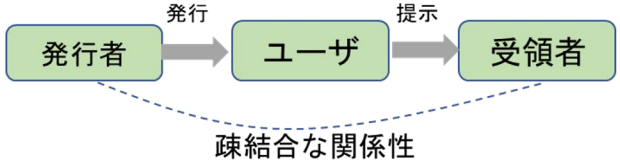
従来の情報連携方式

従来の情報連携方式では、事前に情報提供者と情報受領者の間で、システム間接続条件等の合意などが必要でした。そのため、受領者として利用できる提供元の制約が多かったり、ユーザが情報を提示した先が提供元に見えてしまうなどの課題がありました。



Verifiable Credentialを使った情報連携方式

DIDと併せてVCを使うことで、VC単体での情報の真正性検証が可能になります。発行者と受領者の間は疎結合な関係性となり、ユーザが情報を提示した先が発行者に見えなくなる為、発行者に過度な行動情報の把握をされる事を軽減出来る等の利点が期待されます。

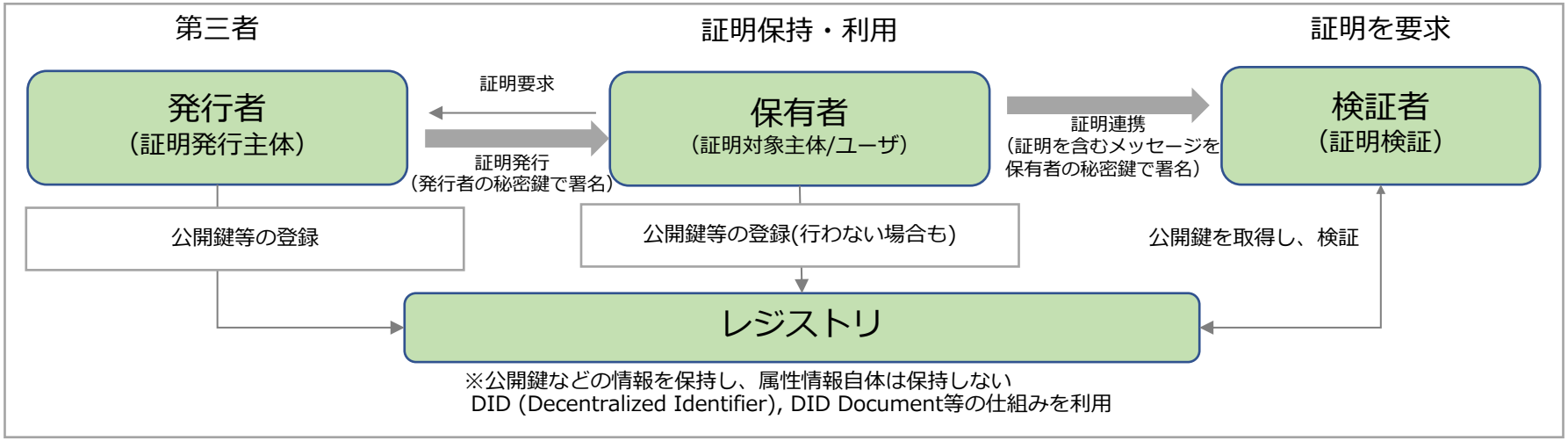


注：ここで言うDIDとはW3Cの定義する分散型識別子を指します。
Decentralized Identifiers (DIDs) v1.0, W3C Recommendation 19 July 2022　https://www.w3.org/TR/did-core/

1. VC（Verifiable Credential）とは②

Verifiable Credentialのアーキテクチャは、下図に示す発行者、保有者、検証者、そしてレジストリで構成されます。

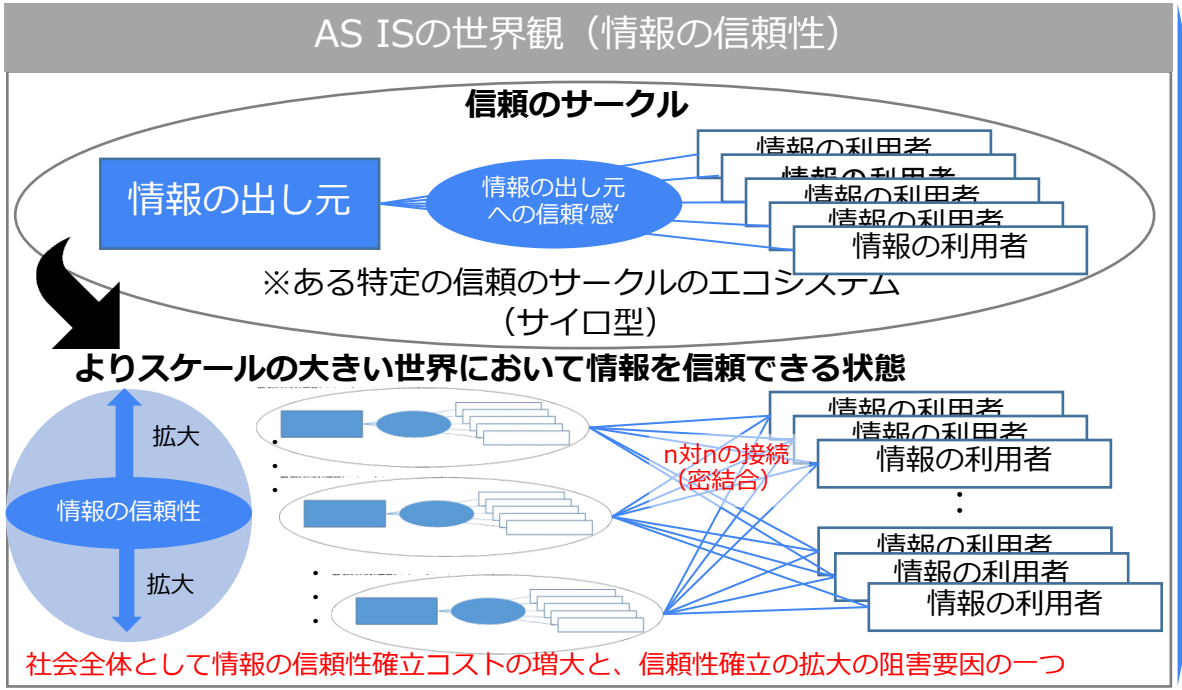
VCのアーキテクチャ



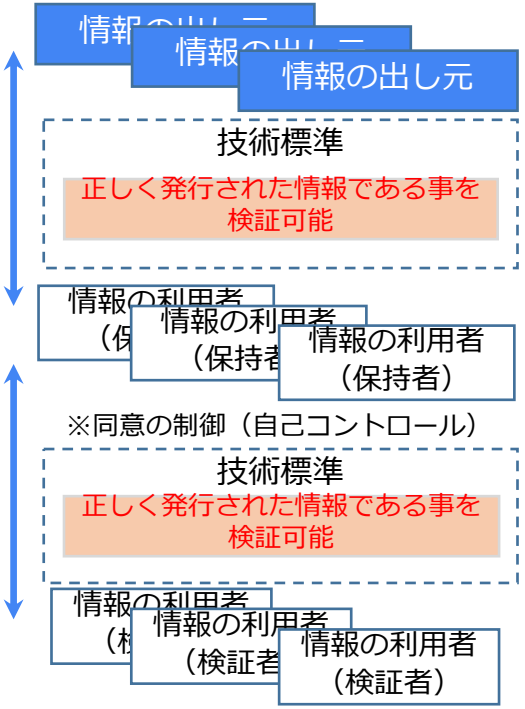
発行者とは証明書（VC）を発行する主体で、教育機関（卒業証明書の発行）や、公安委員会（運転免許証の発行）などが考えられます。
保有者とは発行された証明書（VC）を保有する主体で、利用するユーザ等が考えられます。
検証者とは受け取った証明書（VC）を検証する主体で、お店・企業等が考えられます。
レジストリとは証明書（VC）の署名検証に利用する公開鍵情報を保有する主体で、分散台帳等が考えられます。

2. VCのもたらす世界観（可能性）について

情報の出し元への「信頼“感”」を軸にしたサイロ型の「信頼のサークル」の現状の世界観から、**疎結合な関係性においても情報の真正性を検証可能**とする**技術標準と同意の制御の手法の拡大**により、**相互接続コスト軽減と検証可能な情報の拡大**の両立を背景にした、**相手を信頼しながら行動可能な範囲が拡大した世界観**につながる可能性があります。



疎結合な相互接続性の拡大によるコスト軽減



3. 本人確認手法としてのVC／DIDの活用可能性について

VCの仕組みを、本人確認等に活用できる可能性が期待されます。

- 保有者（ユーザ）が手元保持した、信頼できる第三者（Isuuer）が発行した「**当人確認済情報**」や「**資格情報**」を活用して、**身元確認**と同時に**様々な資格情報を基にした確認や認証・認可等も可能**になる事が期待されます。
- また、身元確認において、**他事業者の身元確認結果の活用が普及することが期待**されます。

＜背景＞

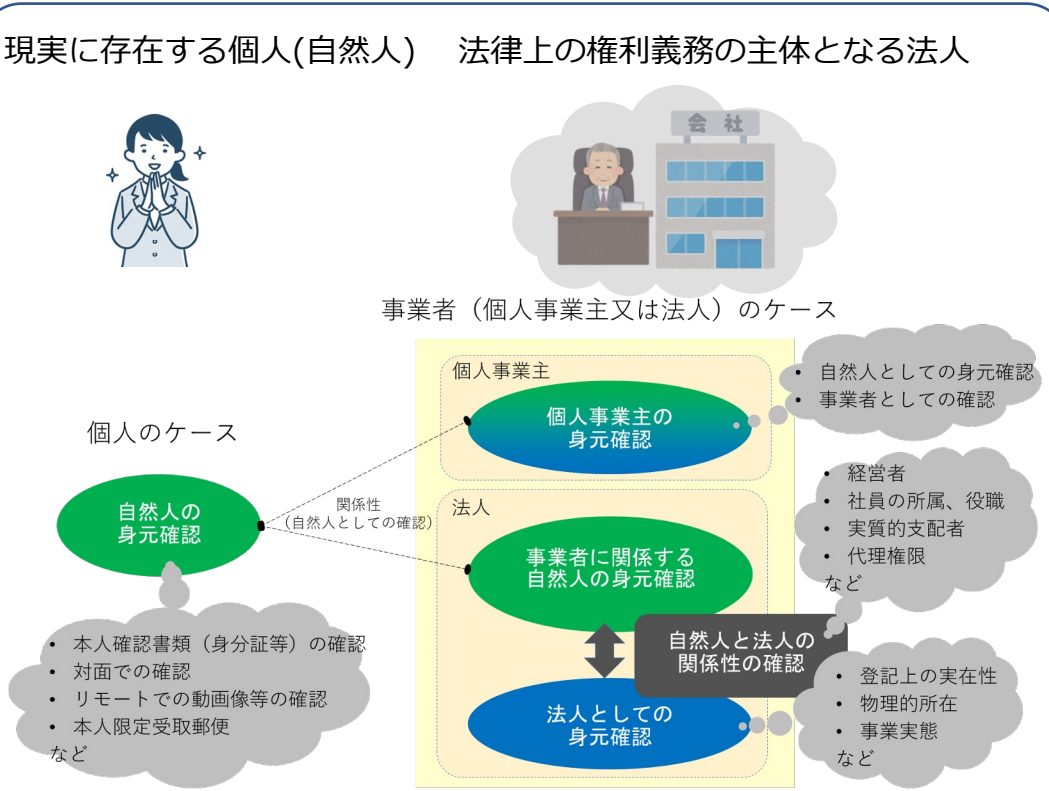
- Webで使用される各種技術の標準化団体であるW3C（World Wide Web Consortium）にて、2014年から検討開始され、2021年に標準仕様　第１版が公開されたVC／DID(Verifiable Credentials／Decentralized Identifiers)について、近年注目されており、政府においてもDFFT(Data Free Flow with Trust：自由で信頼あるデータ流通)を背景に、 Trusted Web推進協議会での検討や実証プロジェクトなども存在します。
- W3Cの標準に基づき、様々な団体等で実装仕様策定が推進されており、OpenID Foundationにおいても、OpenID for Verifiable Credentials Issuance/OpenID for Verifiable Presentationsとして推進されています。

【コラム】事業者KYCについて

1. 事業者KYC議論の特徴①（要素の複雑さ）

事業者KYCには、以下のような複数の視点が存在する為、自然人の本人確認と比較して議論が難しいと考えられます。

- 法人とは、例えば株式会社や学校法人といったように、法律上において自然人と同様に権利義務の主体となるものです。
- 現実世界に実在する自然人とは異なり、法人は代表者や職員など複数の人間の関係により成り立っており、その実在性の把握は自然人の場合よりも分かりにくいものとなります。
- 例えば、登記されている法人の場合は、登記簿と照合したり、本社所在地に存在することを確認することで法人としての実在性を確認することができます。
- さらに、実際に法人との取引等に応じるのは、法人の意思を示す代表者や、代理権限を与えられた者になるため、その者の自然人としての実在性を確認したうえで、法人との関係性を確認することも求められる可能性があります。
- このように、法人の身元確認は関係者に対する自然人としての身元確認の要素を内容しつつ、法人としての実在性の確認や自然人と法人の関係性の確認に関係する多岐にわたる要素が含まれるため、自然人よりも複雑になりえます。

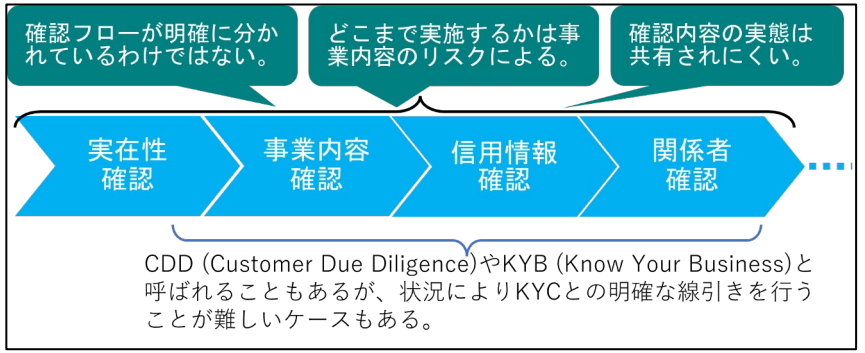


2. 事業者KYC議論の特徴②（整理の難しさ）

事業者KYCとは、「事業者の当該行為等のリスク判断や責務（ライアビリティ）に基づき必要となる確認要素について、経済合理性の範囲で、必要な情報収集と信頼性の確認を執り行う行為」とも考えられ、どこまでの範囲を確認すれば当該業務目的を達することができるかに明確な基準を設けることが難しいと考えられます。

事業者の身元確認には複数の要素が関係するが、どの要素について確認するかは身元確認を求める事業内容によって異なります。

例えば、サービス提供先への連絡手段など必要最小限の情報のみを必要とし、取引リスクがそれほど大きくないケースでは、いくつかの要素を確認するだけで十分であるのに対し、取引が犯罪組織やテロ組織への利益供与になりえるものは、事業者に関する多くの要素をより厳格に確認することが求められます。



身元確認を行う事業者がその目的に照らし合わせて、取引相手の事業者の存在をどこまで確認することでリスクを許容できるかということになります。その目的によっては、相手の実在性に留まらず事業内容や実態についても確認することもあり、いわゆるCDD (Customer Due Diligence)やKYB (Know Your Business)として考えられる要素が入り込むことも考えられます。さらに、身元確認を行う事業者としては相手の事業者の実在性確認、事業内容合確認、信用調査といった各項目について明確にフローを分けているわけではなく、一連の取引プロセスの中でそれらの要素が混在していることが多いと考えられます。このように、事業者に関しては、自然人の場合よりも、身元確認や信用情報などの項目を明確に線引きしにくい傾向があり、これが事業者KYCの議論を難しくする要因にもなっています。

さらに、議論を難しくするもう一つの要因として、情報共有の難しさがあります。自然人の身元確認の議論に比べ、事業者に対する身元確認の具体的な方法は公にされることは少なく、比較整理することが難しいです。そのため、共通要素の洗い出しや標準化の議論が進みにくい傾向があります。

3. 事業者確認事項の要素

自然人の身元確認の議論と同様に、事業者身元確認の議論を促進するには、現状の事業者身元確認の要素を整理することが不可欠です。

右表は、例として、犯罪収益移転防止法が求める確認要素や、他のいくつかのケースにおける確認事項を調査したものです。身元確認を行う事業者は目的や事業内容に応じて、必要な要素を確認することとなります。

(注) 本整理や以降に続く考察は犯罪収益移転防止法等の法令に対する準拠や妥当性を議論する意図ではなく、一般的な民間事業者における身元確認に対する考察が主な対象である点に留意。

分類	要素	補足説明
1.1 事業者の身元確認 (事業者の実在性確認)	法的実在性確認	法令に従った登記情報等に当該事業者や組織が存在することを確認。 例：商業登記や法人登記されていることを確認
	物理的実在性確認	当該事業者や組織の所在を確認。 例：商談プロセス等における対面確認、郵送やり取りなどにおける非対面確認
	法人等に属する内部属性の実在性確認	部門や事業所等を確認
1.2 事業者の身元確認（事業者に関係する自然人）	所属確認（代表者、従業員、代理人等）	法人格と事業者に関連する自然人の「関係性」の確認。 例：代表者、従業員、代理人等、所属組織
	取引の任に当たっている事の確認（権限確認）	適切な権限や資格をもって、当該行為を執り行っているかどうかの確認。
	事業者に関連する自然人(代表者等)の「個人」としての本人確認	Identity Document等の確認をもって、当該本人自身である事の確認（本人特定事項の確認）。
2. 意思の確認	法人格の当該行為自体に関わる意思の確認（内容確認をしている事の確認含む）	申請代表者等取引の任に当たっている自然人の行為を介しての、法人としての当該行為に対する意思の確認。 例：契約書や申請書等の代表者等の押印の確認、印鑑登録証明書の照合 例：電話等や、電子証明書による電子署名の確認など非対面確認
3. 顧客管理	事業の内容の確認	一般事業者間の取引行為等においては、各事業者の取引判断等に際し、当該取引先事業者との取引開始または継続的取引について、どのようなリスクが存在するのか、取引リスクに見合った価値があるのか等、主に各事業者の社内基準に基づき、適切かつ相応な注意や努力を払って調査を執り行う事などが含まれる
	事業活動の実態有無の確認（当該事業者や組織の運営状態を確認）	
	実質的支配者（BO）の確認	
	反社確認	
	資産及び収入の状況の確認	
	信用情報確認	

4. 事業者確認における確認手法の例

確認事項の各要素には特徴の異なる様々な手法が考えられます。

求める確認内容の厳密さに応じて適切な確認手段を選ぶ必要があります。また、確認手法の例の中にはアナログ的な手法も多く含まれ、現状のままでは全てがデジタル化可能か明らかではありません。自然人とは異なりeKYCの議論が進みにくい理由にもなっています。

アナログ	デジタル
商業登記の登記事項証明書（対面or書留等）	商業登記電子証明書（電子認証登記所発行の電子証明書）を用いた電子署名を用いた電子申請や取引に関わる情報
商業登記事項証明書（対面or書留等）	登記情報提供サービス
	法人番号公表サイトやgBizINFOの照会等
法人登記の登記事項証明書（対面or書留等）	登記情報提供サービス
	法人番号公表サイトやgBizINFOの照会等
TBDやTSRの企業情報調査書	TBDやTSRの企業情報照会サービス
公証役場または商業登記所でのBO情報確認	
取引の任に当たる代表者または担当者の自然人の本人特定事項の確認書類	公的個人認証他
取引の任に当たっている事の確認の為の委任状または本店や事業所などへの架電など	電子委任状
契約書面、請求書面など	電子証明書を用いた電子署名を用いた取引に関わる情報
	EDI等を介した取引に関わる情報
印鑑証明書（対面or書留等）	
対面での名刺やり取りや事業所での打ち合わせや書類の郵送や架電やり取りやメールアドレスなどを通じての所属確認など	
ホームページ等公開情報の確認など	法人番号公表サイトやgBizINFOの照会等

デジタル社会における事業者KYCの課題に関する議論は今後も深掘りすることが必要です。

事業者の身元確認(Identity Proofing)の確認事項やプロセスをデジタル化するためには様々な課題があり、今後も各要素を深堀した議論が求められます。その一方で、民間の事業者において、本業ビジネスに付帯して得られた身元確認にも鮮度の高い有益な情報が含まれており、それらのデータを相互に連携することで、より確度の高い情報に基づいた判断が可能となることに期待できます。この考え方は、事業者に対するProofingを行うというよりも、いかに確度の高い情報に基づいて、その事業者を信頼するかというTrustの概念に近いと考えられます。事業者のTrustをより高めるための基盤の1つとして、事業者情報を集約する事業者KYCアグリゲートの考え方があります。事業者KYCアグリゲートを実現するためには、事業者KYCに関するガイドラインや標準化が求められますが、そのためには、事業者KYCの共通的事項や技術的課題についてさらに考察を深堀りしていく必要があり、今後の議論の活性化が期待されます。

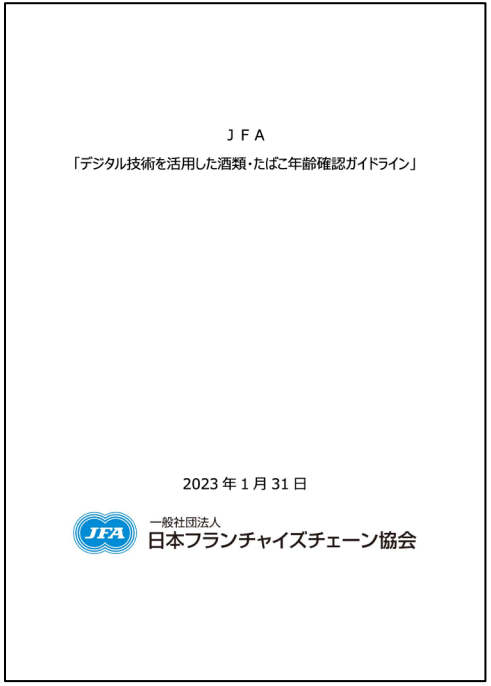
【コラム】一般社団法人日本フランチャイズチェーン協会「デジタル技術を活用した酒類・たばこ年齢確認ガイドライン」の取組みについて

*本コラムは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」
「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（デジタル臨時行政調査会作業部会（第16回）提出資料）」
を基に作成しております。
詳細は同ガイドラインをご参照ください。

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策定について

一般社団法人日本フランチャイズチェーン協会は、協会加盟のコンビニエンスストア4社（セブン-イレブン、ファミリーマート、ミニストップ、ローソン）が検討して策定した、「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。

「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」の検討経過



検討の経過

- 「令和2年度流通・物流の効率化・付加価値創出に係る基盤構築事業（省力化店舗実現可能性検討事業）」では、酒・たばこの販売に係る関係法令やプライバシー・消費者保護の課題を踏まえつつ、デジタル技術を活用した成人認証について検討が行われた。
- 同報告書を受け、一般社団法人日本フランチャイズチェーン協会はCVS部会の下に「酒類・たばこの年齢確認に関するデジタル認証検討会」を設置し、「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（以下「JFA年齢確認ガイドライン」という。）」の検討を行った。
- JFA年齢確認ガイドラインは、2022年11月30日のデジタル庁デジタル臨時行政調査会作業部会において案が示され、妥当で合理的との評価を受け、公表された。
- JFA年齢確認ガイドラインの検討においては、本ガイドラインと連携し、OpenIDファウンデーション・ジャパンからは年齢確認手法の保証レベルや具体的手法について助言を行った。

出所：一般社団法人日本フランチャイズチェーン協会 (2023)「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」及び同ガイドラインプレスリリース、
経済産業省「令和2年度流通・物流の効率化・付加価値創出に係る基盤構築事業（省力化店舗実現可能性検討事業）」より作成

コンビニエンスストア業界の課題

コンビニエンスストア業界ではデジタル技術を活用した省人化施策が進められていますが、酒類・たばこのセルフレジ等での販売時のデジタル技術を活用した年齢確認方法について、関係省庁が発行するようなルールは存在していませんでした。

コンビニエンスストア業界における酒類・たばこ販売時の年齢確認に関するルール

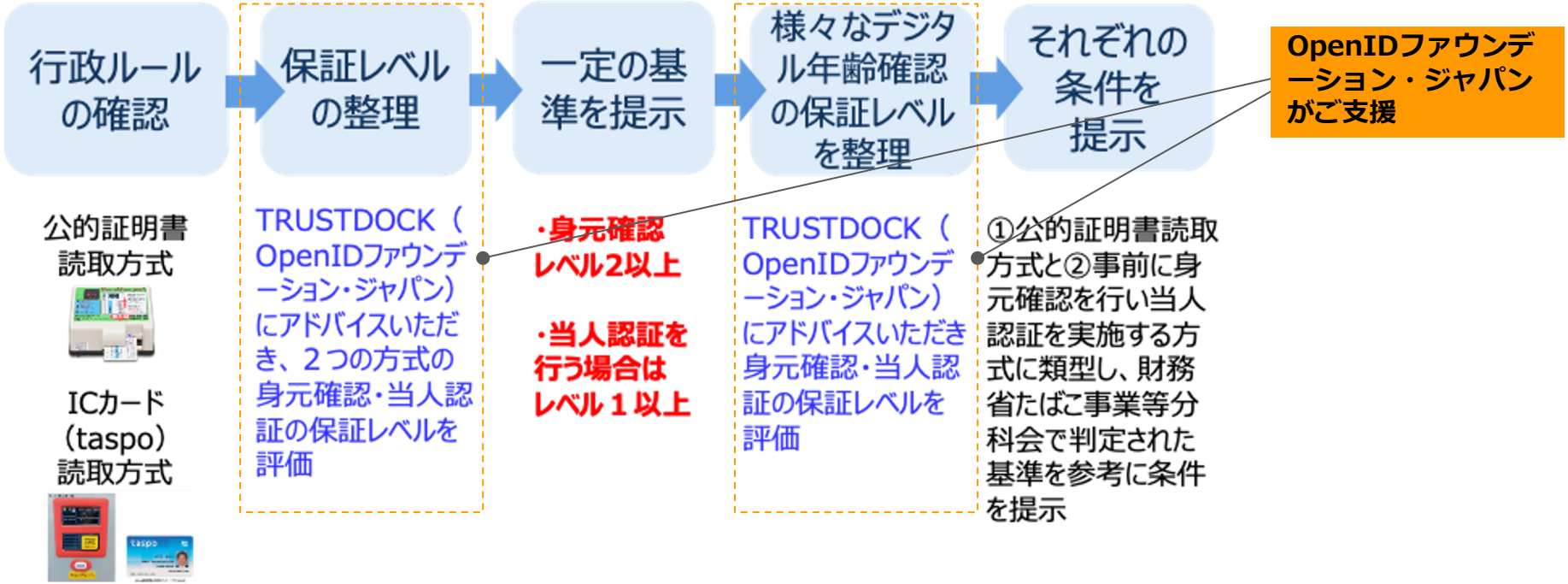
	酒類	たばこ
法律	20歳未満の者の飲酒の禁止に関する法律 ・販売者への罰則が規定されており、当該20歳未満の者が自用に供することを販売者が知っていたこと、が構成要件 ・販売をする際の年齢確認等が求められている	20歳未満の者の喫煙の禁止に関する法律
通常のレジ（対面販売）	20歳未満の者に販売しないよう年齢確認を徹底 20歳未満に販売しないよう、20歳代と思われるお客様には年齢確認証の提示を実施 **⇒年齢確認は従業員にとって負担**	
自動販売機	運転免許証等により年齢確認が可能な改良型酒類自動販売機は許可がされている 	財務省のたばこ事業分科会において、許可の条件が設定され、対象機種を認定した上で公表 
セルフレジ（店内には従業員がいる）	 有人の通常レジへ誘導するか、セルフレジから従業員を呼び出して年齢確認を行う等の方法で対応 **⇒省人化の足かせに** **規制改革ホットラインの回答** 年齢確認の方法については、**販売対象者が確実に20歳以上であることが確認できるものであれば、**対面販売のみに限定するものではありません。	

出所：一般社団法人日本フランチャイズチェーン協会 (2022)「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（デジタル臨時行政調査会作業部会（第16回）提出資料）」より.

一般社団法人日本フランチャイズチェーン協会における年齢確認ガイドライン作成の流れ

一般社団法人日本フランチャイズチェーン協会は、OpenIDファウンデーション・ジャパンが作成している本ガイドラインと連携しながら、デジタル年齢確認の保証レベルや具体的な手法を整理した「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」を策定しました。

一般社団法人日本フランチャイズチェーン協会における年齢確認ガイドライン作成の流れ

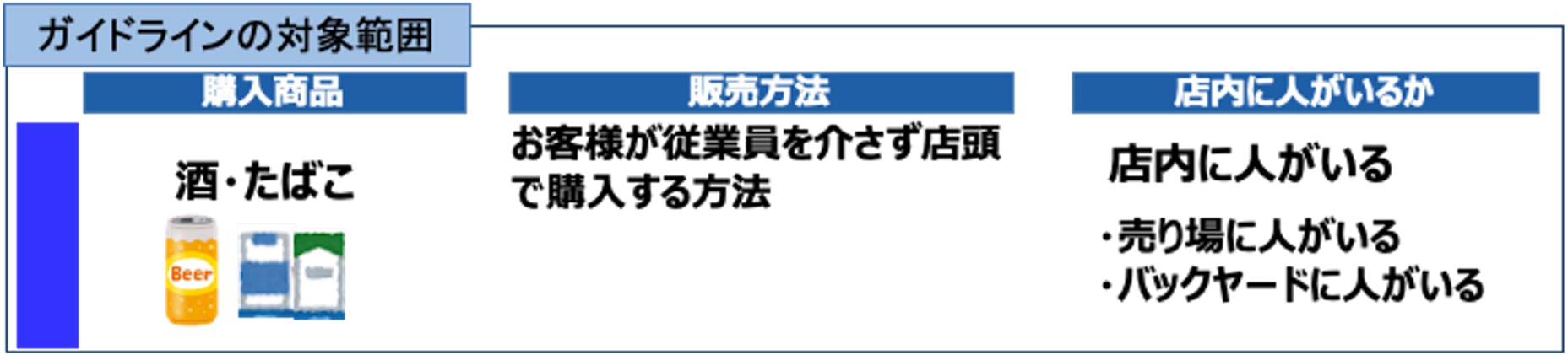


出所：一般社団法人日本フランチャイズチェーン協会 (2022) 「デジタル技術を活用した 酒類・たばこ年齢確認ガイドライン（デジタル臨時行政調査会作業部会（第16回）提出資料）」より.

JFA年齢確認ガイドラインの対象範囲

JFA年齢確認ガイドラインは、「酒類・たばこ」を対象に、お客様が従業員を介さず、店頭で購入できる方法（「セルフレジ」、「Amazon Goに類似するケース」、「スマホレジ」での販売）を対象としています。また、店内に従業員がいるケースが想定されています。

JFA年齢確認ガイドラインの対象範囲と留意点



【留意点】

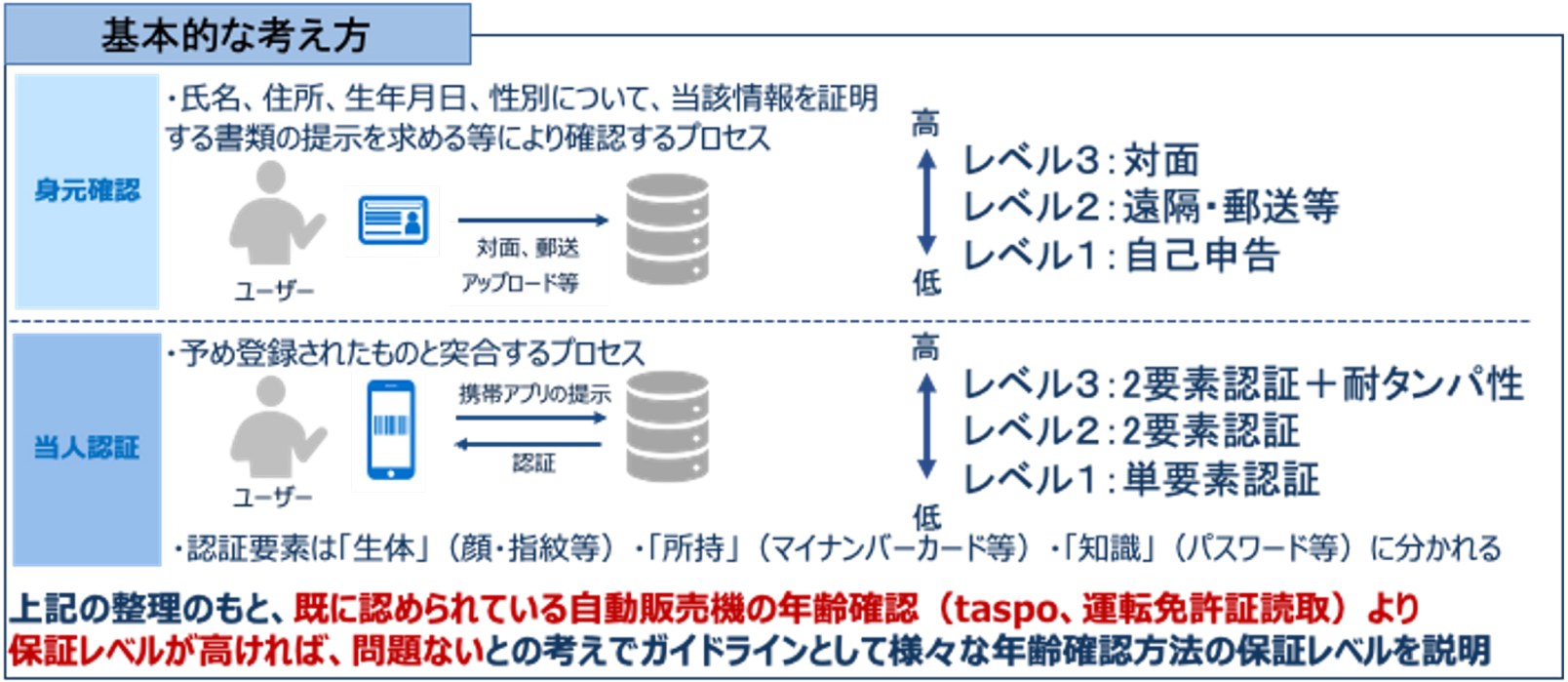
- 購入商品：toto 等のくじや成人向け雑誌は対象としない。
- 販売方法：自動販売機による販売及びインターネット販売については、既存のルールが存在するため対象としない。
- 店内の従業員の有無：完全無人店舗は対象としない。

出所：一般社団法人日本フランチャイズチェーン協会 (2022)「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（デジタル臨時行政調査会作業部会（第16回）提出資料）」、
一般社団法人日本フランチャイズチェーン協会 (2023)「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」より.

JFA年齢確認ガイドラインの基本的な考え方

JFA年齢確認ガイドラインでは、身元確認・当人認証それぞれについて整理を行っています。ここでは、既に認められている自動販売機での年齢確認の保証レベル（IAL2・AAL1）以上であれば問題ないとの考え方が整理されています。

JFA年齢確認ガイドラインにおける保証レベルの整理

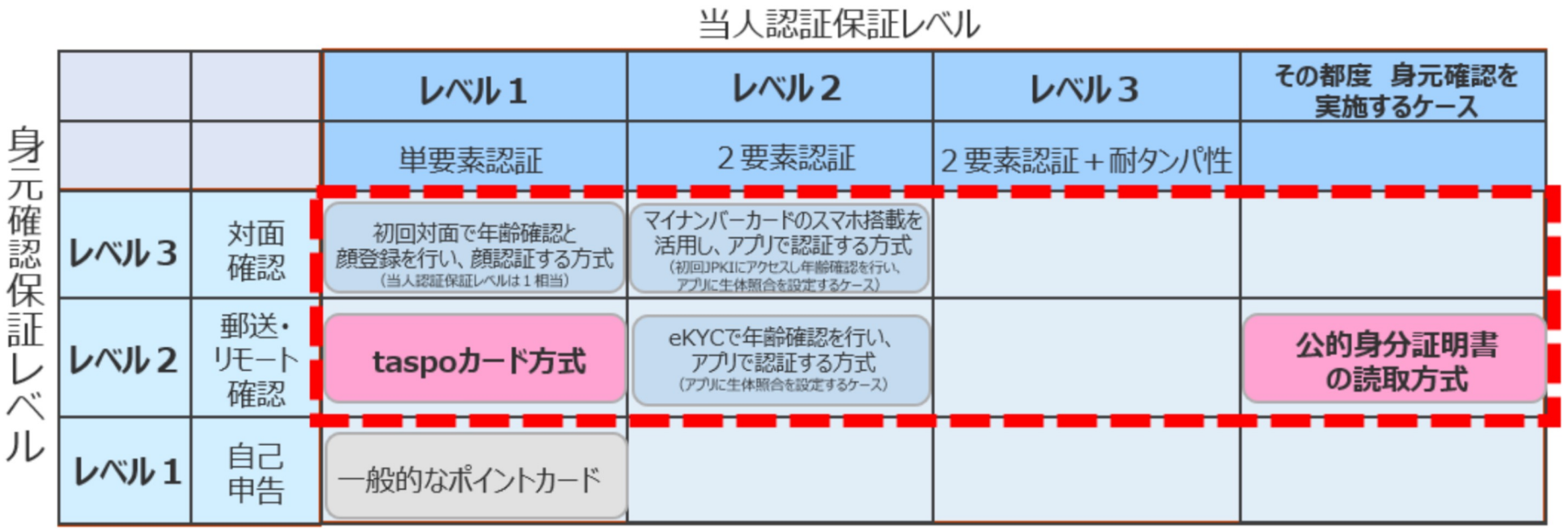


出所：一般社団法人日本フランチャイズチェーン協会 (2022)「デジタル技術を活用した 酒類・たばこ年齢確認ガイドライン（デジタル臨時行政調査会作業部会（第16回）提出資料）」より.

JFA年齢確認ガイドラインで紹介されている年齢確認手法①

JFA年齢確認ガイドラインでは、身元確認保証レベルと当人認証保証レベルのマトリックスを作成し、そのマトリックスに具体的な手法を位置づけて紹介しています。

JFA年齢確認ガイドラインにおける年齢確認手法



※「行政手続きにおけるオンラインによる本人確認の手法に関するガイドライン」（2019年2月CIO連絡会議決定）の定義・レベル区分をもとに、民間事業者の本人ガイドラインを参考に、JFAにて図式化したもの

出所：一般社団法人日本フランチャイズチェーン協会 (2022)「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（デジタル臨時行政調査会作業部会（第16回）提出資料）」より.

JFA年齢確認ガイドラインで紹介されている年齢確認手法②

JFA年齢確認ガイドラインでは、年齢確認手法の保証レベルを整理するだけでなく、具体的な手法を提示しています。

JFA年齢確認ガイドラインにおける年齢確認手法の具体例

赤字：身元確認レベル　青字：当人認証レベル

	taspoカード方式	初回対面で年齢確認と顔登録を行い、顔認証する方式	eKYCで年齢確認を行い、アプリで認証する方式 （アプリに生体認証を設定するケース）	マイナンバーカードのスマホ搭載を活用し、アプリで認証する方式 （初回JPKIにアクセスし年齢確認を行い、アプリに生体照合を設定するケース）	公的身分証明書読取方式
利用イメージ					

中間的な手法（身元確認結果の活用）に該当

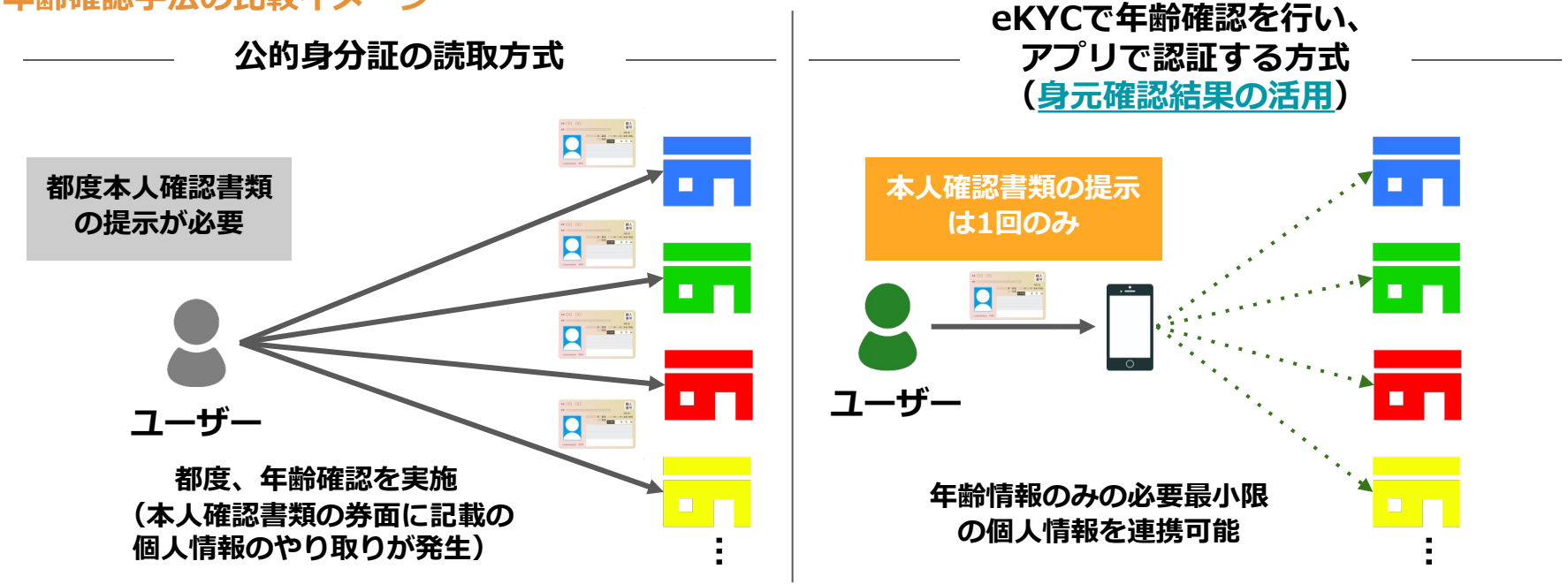
出所：一般社団法人日本フランチャイズチェーン協会 (2022)「デジタル技術を活用した 酒類・たばこ年齢確認ガイドライン（デジタル臨時行政調査会作業部会（第16回）提出資料）」より.

（参考）年齢確認における身元確認結果の活用について

JFA年齢確認ガイドラインで紹介されている年齢確認手法のうち、「eKYCで年齢確認を行い、アプリで認証する方式」は、本ガイドラインにおける「身元確認結果の活用」に該当すると考えられます。

「公的身分証の読取方式」では、本人確認書類を持ち歩き、かつ、当該本人確認書類を使った年齢確認を購入の都度行う必要があります。他方で、「身元確認結果の活用」では本人確認書類を用いた身元確認を1度行うだけでよく、また、年齢確認の際にも必要最小限の個人情報を連携することが可能であり、プライバシー面においてもメリットがあります。

年齢確認手法の比較イメージ



本ガイドラインの使い方と参照時の留意事項

本ガイドラインの使い方

本ガイドラインは、デジタル本人確認の手法を選択する際に参考となる様々な情報を取りまとめたものです。そのため、何らかの新しい規制を設けたものではなく、民間事業者の目的やニーズに合致する箇所のみを参照いただくこともできます。また、「個人情報の取扱い」など一部法令等に関わる内容についても記載がありますが、そうした内容については、本ガイドラインのみを遵守すればよいわけではありません。そのため、個別具体的な内容については、本ガイドラインに記載のないものも含め、関係法令等に適切に遵守頂く必要があります。

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・ジャパン本人確認ガイドラインタスクフォース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。

END