

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

2026年（令和8年）2月24日

デジタル庁

【ドキュメントの位置付け】

Informative：参考とするドキュメント

【キーワード】

本人確認、デジタルアイデンティティ、身元確認、当人認証、フェデレーション、マイナンバーカード、公的個人認証、カード代替電磁的記録

【概要】

「DS-511 行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン」に関する解説や補足情報等を記載した参考文書。

改定履歴

改定年月日	改定箇所	改定内容
2026年2月24日	—	・ 初版決定

目次

改定履歴	i
目次	ii
1 はじめに	1
1.1 本解説書について	1
1.2 適用対象	1
1.3 位置付け	1
1.4 用語	1
2 ガイドライン本編の全体概要	2
2.1 本人確認に関する直近の動向（2026年初頭）	2
2.2 ガイドライン本編の全体構成	5
2.3 ガイドライン本編の適用対象について	7
2.4 「基本的な考え方」について	8
2.5 「本人確認の実装モデル」について	12
3 本人確認の構成要素と対策基準（本編3章の解説）	14
3.1 身元確認（Identity Proofing）に関する解説	14
3.2 当人認証（Authentication）に関する解説	19
3.3 フェデレーション（Federation）に関する解説	28
4 本人確認手法の検討方法（本編4章の解説）	30
4.1 業務分析と前提情報の整理	30
4.2 対象手続の保証レベルの判定（本編4.1）	32
4.3 身元確認手法の選定の考え方（本編4.2関連）	35
4.4 当人認証手法の選定の考え方（本編4.2関連）	42
4.5 継続的な評価と改善（本編4.3関連）	45
5 その他の参考情報	47
別紙1 身元確認手法の具体例	51
1 主要な身元確認手法の解説	51
1.1 マイナンバーカードによる身元確認手法	51
1.2 マイナンバーカード以外による身元確認手法	62
2 主要な本人確認書類の具体例	72
2.1 区分A：デジタル署名を備える本人確認書類	72
2.2 区分B：顔写真を備える本人確認書類	74
2.3 区分C：その他の本人確認書類	75
2.4 スマートフォンに搭載された本人確認書類等の扱いについて	76

別紙2 本人認証手法の具体例	77
1 主要な本人認証手法の解説	77
1.1 フィッシング耐性を有する本人認証手法	77
1.2 その他の本人認証手法	83
別紙3 参考資料一覧	90
1 本人確認及びデジタルアイデンティティに関する参考資料	90
2 プライバシーに関する参考資料	91
3 アクセシビリティに関する参考資料	92

1 はじめに

1.1 本解説書について

本解説書は、「DS-511 行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン」（以下「ガイドライン本編」又は単に「本編」といいます。）の解説や補足を目的とした文書です。ガイドライン本編の読者が、国の行政機関が提供する行政手続又は行政サービス（以下「対象手続」といいます。）において採用すべき本人確認手法を本編に沿って検討する際の参考情報となるよう、本人確認に関する最新動向、ガイドライン本編の記載内容の解説、具体的な検討の手順、検討にあたる留意点、採用候補となる手法の具体例等をまとめたものです。

1.2 適用対象

本解説書の適用対象は、ガイドライン本編と同様とします。

なお、ガイドライン本編の適用対象に関する解説は「2.3 ガイドライン本編の適用対象について」を参照してください。

1.3 位置付け

本解説書は、デジタル社会推進標準ガイドラインにおける「実践ガイドブック（Informative）：参考とするドキュメント」として位置付けます。

（参考情報）ガイドライン本編と解説書の役割・位置づけについて

ガイドライン本編は、その記載内容への順守が求められる「Normative」に位置づけられるガイドラインであり、長期にわたり適用されることを前提として、原則的な情報を取りまとめた内容となっています。

一方、本解説書の位置づけは参考情報である「Informative」とし、比較的頻繁に改定を行うことを前提として、世の中の技術動向や脅威動向、手法の具体例等についても解説を行う位置づけとしています¹。

1.4 用語

本解説書において使用する用語は、ガイドライン本編と同様とします。また、補足や解説が必要と考えられる技術用語については、文中や脚注にて解説します。

¹ 本解説書は、ガイドライン本編とあわせてお読みいただく想定で作成しています。

2 ガイドライン本編の全体概要

本章では、ガイドライン本編の全体概要の理解を助けることを目的として、本人確認に関する最新動向と本編の全体概要を解説します。

また、本編の「1 はじめに」及び「2 本人確認の基本的枠組み」に関して、本編の記載内容の理解を助ける解説・補足・参考情報を記します。

2.1 本人確認に関する直近の動向（2026年初頭）

ここでは、本人確認の検討にあたって特に把握いただきたい動向について説明します。令和7年9月のガイドライン本編の全面改定では、これらの動向を踏まえた保証レベルや対策基準の見直しを行いました。

1) 脅威の動向

ア 本人確認書類の偽造・改ざんの高度化

本人確認書類の偽造・改ざん技術は、近年ますます高度化・巧妙化しています。組織的な犯罪集団によって大量の偽造カード・偽造書類が作成され、攻撃に利用されているようなケースも摘発されています。

精巧に偽造された本人確認書類を目視で見破ることは容易ではなく、検査に必要な道具や環境が用意され、十分に訓練された検査員がいない環境においては、偽造・改ざんの検出は困難となりつつあります。ビデオベースのオンライン身元確認手法²によって偽造を検証することは更に困難です。

このような動向により、本人確認書類の偽造・改ざんを厳密に検知するためには、ICチップを具備した本人確認書類等によるデジタル署名を用いた電子的な検証が必要となりつつあります。

イ リアルタイムフィッシング

利用者を偽サイトに誘導し、偽サイト上で入力させることで窃取したパスワード等を正規サイトにリアルタイムに中継することで不正アクセスを行う「リアルタイムフィッシング」と呼ばれる攻撃手法が急増しています。

リアルタイムフィッシングでは、ID/パスワードだけでなくワンタイムパスワード³も窃取・中継されてしまうため、パスワードとワンタイムパスワードを組み合わせた多要素認証であっても不正アクセスを防ぐことができませ

² ビデオベースの身元確認手法：本人確認書類の券面や申請者の容貌を、動画や写真で撮影し送信することで、オンラインでの身元確認を行う手法のこと。

³ ワンタイムパスワードには、SMSで送信や電子メール等で送信する方式、スマートフォンの認証アプリで生成する方式などがあるが、いずれの方式であっても窃取・中継され得る。

ん。リアルタイムフィッシングを防ぐためには、後述するパスキーや PKI（公開鍵基盤）をベースとした認証のような「フィッシング耐性」をもつ本人認証手法が必要です。

ウ SIM スワップ

SIM スワップは、偽造した本人確認書類を用いたり、携帯電話会社の契約手続 Web サイトに不正にログインしたりして携帯電話会社の SIM カードの再発行手続等に対してなりすまし攻撃を行うことで、利用者の SIM カード（携帯電話番号）を乗っ取る攻撃です。攻撃者は、乗っ取った SIM カードを悪用し、SMS で届いた認証コードを窃取して様々なサービスへの不正アクセスを行ったり、SIM カードを糸口としたさらなる攻撃を行ったりする事例が報告されています。

こうした攻撃に対し、我が国では携帯電話事業者における SIM カード再発行時の本人確認手続の強化、携帯電話不正利用防止法に基づく本人確認手法の見直し（同法施行規則の改正）等が行われています⁴。

エ 生成 AI を悪用したディープフェイク

生成 AI 技術の発展により、実在する人物の顔や声を高度に模倣した「ディープフェイク」と呼ばれるコンテンツの作成が容易となり、ビデオベースの身元確認を行う場合の新たな脅威となっています。

特にビデオベースのオンライン身元確認手法において、申請者の容貌を撮影した映像をリアルタイムに改ざんされた場合、あらかじめ録画された映像の検知を主眼としていた従来型のライブネスチェック⁵では検知が難しくなることが懸念されています。

本件については、本解説書の以下で更に詳細を解説しています。

- ・ 「3. 1 身元確認 (Identity Proofing) に関する解説」
「3) ビデオベースの身元確認手法における脅威」

⁴ 参考：「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について」

(https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf)

⁵ ライブネスチェック：ビデオベースの身元確認手法において、カメラに写っている人物が本物の人間であることを確認するための技術の総称。まばたき・光の反射・手ブレ・顔の動きの検知、「右を向いてください」といった指示に従うことの確認等、様々な手法が存在する。従来型のライブネスチェックには「あらかじめ録画された映像の検知」を主眼としているものもあり、そのような対策はリアルタイムのディープフェイクを検知できない場合がある。

2) 技術や対策の動向

ア マイナンバーカードの普及状況と最新動向

マイナンバーカードは対面及びオンラインでの本人確認に利用できる様々な機能を有しており、我が国における本人確認の重要な社会インフラです。2025年12月には、マイナンバーカードの保有枚数が1億枚を突破し、人口に対する保有率は80%超となりました。

また、公的個人認証（JPKI）に基づく電子証明書やカード代替電磁的記録（属性証明機能）等、実物のマイナンバーカードが有する各種機能をスマートフォンで利用可能とするための機能も順次拡大されており、カードの読み取りが不要となり暗証番号入力を生体認証で代替できるなど、利便性の向上も進められています。

（用語解説）カード代替電磁的記録とは

カード代替電磁的記録とは、マイナンバーカードに記録された氏名、住所、生年月日等の情報と、その情報が真正であり、かつ送信者本人のものであることを証明するための情報とを一体的に構成したデータのことを指します。カード代替電磁的記録はスマートフォンに格納され、その情報を相手に送信することで、スマートフォンのみで本人の属性を証明することができます。

詳しくは、デジタル庁のカード代替電磁的記録（属性証明機能）についてのWebサイトをご参照ください。

イ 本人確認書類のスマートフォン搭載

昨今、様々な本人確認書類や証明書をスマートフォンに電子的に格納し、対面やオンラインにおいて電子的に提示・提出できるようにする技術が登場しています。米国では運転免許証をスマートフォンに格納して利用できる「モバイル運転免許証（mDL）」が導入されつつあるほか、EUや英国においても活発な検討が進められています。

今後は、本人確認書類をはじめとする様々な証明書等がスマートフォンに格納され、本人確認で利用されるようになる想定されます。

ウ パスキー

パスキーは、フィッシング耐性を有する新たな認証技術です。利用者のスマートフォンやパソコン等に保存した「鍵」を使って認証を行う仕組みであ

り、利用者の所持する「鍵」を利用する際には原則として指紋認証、顔認証、PIN 等での端末のロック解除が求められるため、多要素認証として機能します。

パスキーについての詳細な解説は、本解説書の以下の記載についても参考としてください。

- ・ 「3. 2 当人認証 (Authentication) に関する解説」
- ・ 「別紙2 当人認証手法の具体例」

2.2 ガイドライン本編の全体構成

ガイドライン本編は、以下の4章により構成されています。

図 2-1 ガイドライン本編の全体構成

DS-511 本人確認ガイドラインの全体構成	各章の記載内容のポイント
<p>1 はじめに 1.1 背景と目的/1.2 適用対象/1.3 位置づけ/1.4 用語/1.5 基本的な考え方</p>	<ul style="list-style-type: none"> ・ 本人確認ガイドラインの改定の背景 ・ 検討にあたる「基本的な考え方」
<p>2 本人確認の基本的枠組み 2.1 本人確認の構成要素 2.2 本人確認の実装モデル</p>	<ul style="list-style-type: none"> ・ 本人確認を構成する3つの要素 (身元確認、当人認証、フェデレーション) ・ システムでの実装モデルのパターン
<p>3 本人確認における脅威と対策 3.1 身元確認 (Identity Proofing) 3.2 当人認証 (Authentication) 3.3 フェデレーション (Federation)</p>	<ul style="list-style-type: none"> ・ 身元確認、当人認証、フェデレーションのそれぞれで想定されるリスクと対策 ・ 3段階の保証レベルと対策基準の定義 ・ 検討すべき「個別検討事項」
<p>4 本人確認手法の検討方法 4.1 対象手続の保証レベルの判定 4.2 本人確認手法の評価と決定 4.3 継続的な評価と改善</p>	<ul style="list-style-type: none"> ・ リスク評価による保証レベルの判定手順 ・ 「基本的な考え方」の5つの観点を踏まえた本人確認手法の選定手順

各章の概要は以下のとおりです。

1) 「1 はじめに」

ガイドライン本編の第1章では、令和7年9月の全面改定にあたっての背景と目的、適用対象、デジタル社会推進標準ガイドラインとしての位置づけ、用語、基本的な考え方を示しています。

このうち「基本的な考え方」は、令和7年9月の改定において新たに追加した考え方です。ガイドライン本編に基づく検討を、「事業目的の遂行」、「公平性」、「プライバシー」、「アクセシビリティ及びユーザビリティ」、「セキュリティ」の5つの観点を念頭において実施することを求めています。

2) 「2 本人確認の基本的枠組み」

ガイドライン本編の第2章では、本人確認を構成する要素として「身元確認」及び「当人認証」並びに「フェデレーション」を定義しています。「フェデレーション」は、令和7年9月の改定において新たに追加した概念です。

また、情報システムにおいて本人確認を実装する際のモデルとして連携モデル (Federated Model)・非連携モデル (Non-Federated Model)・連携モデルと非連携モデルの組み合わせを示しています。

(参考情報)「フェデレーション」という用語について

令和7年9月のガイドライン本編の改定では、身元確認や当人認証を、他者に依拠して実現することを表す概念である「フェデレーション (Federation)」という用語を追加しました。

参考としている NIST SP 800-63-4 においては、フェデレーションを実現するための代表的な技術として OpenID Connect、あるいは SAML (Security Assertion Markup Language) が言及されています。我が国においては、フェデレーション及びこれを用いて当事者間のアイデンティティ情報が結びつく概念を示すフェデレーテッドアイデンティティ (Federated Identity) ※を単純に翻訳しただけの「連合 (連合アイデンティティ)」、あるいは、一般的にフェデレーションの過程で行われる当人認証をイメージした「認証連携」という言葉が用いられがちです。

しかしながら、フェデレーションはユーザの識別子や属性情報、その他のメタデータ等も含めた情報を「アサーション」と呼ばれる保護されたデータとして流通させるものであり、「連合」はその概念の理解を助ける訳語とは言いがたく、また「認証を連携する」ものではありません。

これを踏まえ、ガイドライン本編では「連合」や「認証連携」といった用語は用いずに、Federation を片仮名で表記した「フェデレーション」という用語を用いることとしました。本解説書もこの表現に沿っております。

※文書によっては「ID連携」と記載しているものも同様の概念です。

3) 「3 本人確認における脅威と対策」

ガイドライン本編の第3章では、身元確認、当人認証、フェデレーションのそれぞれにおける脅威と対策、実施プロセス、主な手法等を体系的に整理して示しています。

その上で、身元確認と当人認証については3段階の「保証レベル」を定義し、

それぞれの保証レベルに求める「対策基準」を定義しています。対象手続は、自身の保証レベルに応じた対策基準を満たすように本人確認を実施することが必要です。

また、身元確認と当人認証では、保証レベルや対策基準によらず対象手続の特性等を踏まえた個別の検討が必要な事項を「個別検討事項」として示しています。

4) 「4 本人確認手法の検討手法」

ガイドライン本編の第4章では、リスク評価を実施することで対象手続に求められる保証レベルを判定し、保証レベルに応じた本人確認手法を選定するための手順を示しています。本人確認手法の選定の際には、前述の「基本的な考え方」で示す5つの観点から、その手法の採用是非や、手法の採用とあわせて講じるべき「補完的対策」を検討するプロセスを今回の改定で追加しました。

また、本人確認手法を選定した後には、その手法について継続的な評価を行い、必要に応じて改善を行うプロセスについても明確化しました。

2.3 ガイドライン本編の適用対象について

本節では、ガイドライン本編の適用対象についての補足や留意点を解説します。なお、本解説書の適用対象もガイドライン本編と同一としています。

1) 適用対象となる「本人確認」の範囲について

ガイドライン本編の対象範囲は以下のとおりです。ここで対象となる「本人確認」には、オンラインによる本人確認だけでなく対面や郵送によって行われる本人確認も含まれる⁶点に留意してください。

本ガイドラインは、国の行政機関が提供する行政手続又は行政サービス（以下「対象手続」という。）において、個人又は法人等が申請・届出・アカウント登録・ログイン等を行う際の本人確認を対象とする。

⁶ 令和7年9月の全面改定前のガイドラインである「DS-500-1 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」では、オンラインによる本人確認のみを対象としていましたが、本人確認書類の偽造・改ざん等の脅威の高度化の動向や、デジタル技術を活用した本人確認手法（ICチップの読み取り等）が対面の手続においても広く利用可能となっている現状を鑑みて、適用対象の見直しを行いました。

参考：「本人確認ガイドライン改定方針 令和6年度とりまとめ」(https://www.digital.go.jp/resources/standard_guidelines#ds511)

2) 政府職員等に対する本人確認について

ガイドライン本編の適用対象には、行政機関の内部事務等を担当する政府職員や派遣職員、委託事業者の作業員等（以下「政府職員等」といいます。）に対する本人確認は含まれないことに注意してください。

これは、政府職員等は業務上多数の個人情報や要機密情報にアクセスし得る場合があります、なりすましや不正アクセスが行われた場合の影響が、ガイドライン本編が想定する適用対象よりも大きくなり得るためです。政府職員等の内部事務に携わる者に対する本人確認については、ガイドライン本編が示す対策基準よりも更に厳格な基準⁷を適用することが必要です。

(参考情報) 管理者アカウントにおける本人確認について

ガイドライン本編の適用対象は上記のとおり「個人又は法人等が申請・届出・アカウント登録・ログイン等を行う際の本人確認」としており、なりすましや不正アクセスが発生した場合の影響範囲も基本的に単一のユーザーアカウントの範囲に限定されることを想定しています。

他方、一般のシステムでは「管理者アカウント」などと呼ばれる、複数のアカウントの管理、設定、情報閲覧等が可能な権限のアカウントが設けられる場合があります。そのようなアカウントにおいてなりすましや不正アクセスが発生した場合の影響は複数のユーザーアカウントに及ぶことが想定されますので、想定されるリスクの大きさに応じて、ガイドライン本編が示す対策基準よりも更に厳格な基準を適用することについても検討を行ってください。

2.4 「基本的な考え方」について

本人確認は、単にセキュリティが高ければよいというものではありません。例えば行政手続における身元確認や当人認証の手順が煩雑・難解であった場合、申請者が途中で申請を諦めてしまい、その行政手続が本来達成したい目的を阻

⁷ この点は、ガイドライン本編が参考としている米国の NIST SP 800-63-4 とは異なる点です。NIST SP 800-63-4 は政府職員等に対する本人確認についても適用対象としているため、要求事項や保証レベルが想定している影響の大きさも本ガイドラインとは異なります。

害してしまう恐れがあります。また、本人確認手法を利用できる条件等によって、申請者に不公平が生じてしまうことも懸念されます。

ガイドライン本編では、こういった様々な観点から本人確認手法が検討されるよう、「基本的な考え方」として以下の5つの観点を定めています。

図 2-2 5つの観点による「基本的な考え方」

1) 事業目的の遂行	• 本人確認が障壁となって行政手続が達成しようとする事業目的が阻害されてはならない。採用しようとする本人確認手法に事業目的の遂行を阻害する懸念がある場合には、代替手段や例外措置を検討する。
2) 公平性	• 本人確認手法によって対象手続の公平性が損なわれてはならない。例えば、スマートフォンの所持を前提とする本人認証手法は、その採用によって対象手続の申請や利用における公平性が損なわれないか、慎重な検討が必要である。
3) プライバシー	• 利用者のプライバシーを毀損しない本人確認が必要である。収集目的を明示する、目的外の利用を行わない、取り扱うデータを必要最小限に留めるなどプライバシー保護の観点で必要な措置を検討し講じることが必要である。
4) アクセシビリティ及びユーザビリティ	• アクセシビリティやユーザビリティが悪いと、利用者が手続きを断念したり、誤操作したりする原因になるため、事業目的の遂行や公平性などにも影響を与える重要な要素である。
5) セキュリティ	• 単にセキュリティレベルの高い手法を選べばよい訳ではない。事業目的の遂行、公平性、プライバシー、ユーザビリティ及びアクセシビリティへの影響も考慮しながら、リスクに応じたレベルの本人確認手法を選択することが必要である。

それぞれの観点の理解の助けとなる参考情報を以下に示します。

1) 事業目的の遂行

「事業目的の遂行」は、本人確認が障壁となって、対象手続が達成しようとする事業目的が阻害されてはならないとする考え方です。例として、以下のようなケースが考えられます。

- 災害時の避難者を支援するための手続において、マイナンバーカードによる厳格な身元確認や本人認証を必須とってしまうことで、マイナンバーカードを持たずに避難してきた方が迅速に申請できなくなる(マイナンバーカードがあれば迅速に、そうでない方を例外として丁寧に対応する等)。
- 住所不定の方からの申請が想定される手続において、本人確認に利用できる本人確認書類を必要以上に厳格に制限してしまうことで、申請条件を満たす本人確認書類を提示できない方が申請できなくなる。

事業目的を阻害するおそれがある場合には、複数の手法を併用したり、例外措置を設けたりするなどの検討が必要です。

2) 公平性

「公平性」は、本人確認手法によって、対象手続が想定する様々な利用者

が、公平に申請やサービスの享受を受けられるようにするという考え方です。公平性の懸念が生じる例として、以下のようなケースが考えられます。

- オンラインサービスの本人認証を、スマートフォンの所持を前提とする手法しか選択できない仕様とすることで、スマートフォンを所持していない方が利用できなくなる。
- 対面での身元確認を必須とする手続において、対応窓口が都市部にしかなく、遠隔地に在住する方の申請が困難となる。

公平性に懸念がある場合には、窓口、郵送、オンライン等複数の申請手法を設けたり、例外措置を設けたりするなどの検討が必要です。

3) プライバシー

個人に関する情報を取り扱う本人確認においては、プライバシーの保護について十分に考慮した上で、手法の選択や情報の取扱いを検討しなければならないという考え方です。本人確認がプライバシー侵害につながる懸念がある具体例として、身元確認の名目で、本来は身元確認に不必要な情報までも申請者から収集し、その情報が漏えいしたり、不適切に二次利用されたりする等が考えられます。

本人確認を実施する上では、我が国の個人情報保護法を順守し、書面（電磁的記録を含む。）により本人から直接個人情報を取得する際の利用目的の明示や、利用目的の達成に必要な範囲に限定した保有および厳格な安全管理措置を実施する必要があります。また、本人確認ではステークホルダーが多岐にわたることが想定されるため、対象手続をデジタル化する際のサービス・業務企画の初期段階で、事前に個人情報を含むデータの取得・利用・提供・保有等に関する整理とリスク分析・評価を実施することなど、プライバシー影響評価やプライバシー・バイ・デザインの取組を導入する必要があります。

4) アクセシビリティ及びユーザビリティ

提供する本人確認手法は障害の有無にかかわらず利用できるもの（アクセシビリティ）であり、利用者にとって使いやすいもの（ユーザビリティ）でなくてはならないという考え方です。アクセシビリティやユーザビリティに懸念がある例として、以下のようなケースが考えられます。

- ワンタイムパスワード入力制限時間が短すぎると、視覚障害や上肢障害などにより入力に時間のかかる利用者が本人確認を完遂できない。
（アクセシビリティ）
- 特殊な操作を求める手法を用いることによって、ブラウザや OS が備え

る入力支援や読み上げ等のアクセシビリティ機能を利用できなくなり、本人確認を完遂できなくなる。(アクセシビリティ)

- PIN の最終桁を入力すると同時に送信されるつくりになっていると、入力した内容を余裕をもって確認できないため、誤入力後の再入力でも再び誤入力する可能性が高まる。回数制限がある場合に特に懸念される。(ユーザビリティ)

(用語解説) アクセシビリティとユーザビリティ

アクセシビリティとは、製品やサービスが障害の有無に関わらずあらゆる人々が利用できるように設計・開発されていることをいいます。デジタルにおけるアクセシビリティは「ウェブアクセシビリティ」ともいい、WCAG 2.2 という国際的なガイドラインも定められています。WCAG 2.2 は ISO/IEC 40500:2025 として国際標準規格になっており、日本産業規格 JIS X 8341-3:2016 についても一致規格としての改正作業が進められています。ウェブアクセシビリティの対象はウェブサイトだけではなく、スマートフォンのアプリ等も含まれており、iOS アプリや Android OS アプリのガイドラインも WCAG を参照して作られています。

ユーザビリティとは、製品やサービスを利用する際における使いやすさの効果・効率・満足度、そして利用目的を達成できる度合いのことで、ISO 9241-11:2018 (日本産業規格では JIS Z 8521:2020) で定義されています。アクセシビリティが確保されていないと、特定の利用者層以外には使いにくくなってしまうことから、アクセシビリティを確保した上でユーザビリティを考慮した設計・開発を行うことが、望ましい製品やサービスの在り方であると言えます。

5) セキュリティ

セキュリティ強度の高い本人確認手法は、前述の事業目的の遂行、公平性、プライバシー、アクセシビリティ及びユーザビリティの観点ではデメリットを抱えている場合があります。そのため、必要なセキュリティレベルを確保すればよいという考え方ではなく、セキュリティレベルを満たした上で、その他の観点も踏まえた総合的な見地から採用すべき手法を選択することが必要であるという考え方です。

参考情報：セキュリティとユーザビリティの関係性について

これまで「セキュリティとユーザビリティはトレードオフの関係にある」との認識のもと、「高いセキュリティを確保するためにはユーザビリティの低下もやむなし」と判断され、ユーザビリティが軽視されることがありました。しかしながら、そうして構築されたオンラインサービスは利用率が伸び悩み、結果としてデジタル化全体を足踏みさせてしまうことも少なくありませんでした。

昨今では、セキュリティとユーザビリティを両立できる技術⁸も登場しており、「セキュリティとユーザビリティはトレードオフ」という関係は、必ずしも成り立たなくなっています。

事業目的の遂行という観点では、ユーザビリティは非常に重要な要素です。ガイドライン本編に基づく検討では、どちらかを重視するのではなく、セキュリティとユーザビリティとを両立させることを目指した検討を心掛けてください。

2.5 「本人確認の実装モデル」について

ガイドライン本編に基づく政府情報システムの検討においては、「連携モデル」の採用を第一候補として検討する方針としています。

本ガイドラインに基づく政府情報システムの検討においては、共通機能の活用による開発の効率化や費用負担の軽減等を目的として、まずは「連携モデル」の採用を第一候補として検討するものとする。

(ガイドライン本編「2.2 本人確認の実装モデル」より)

これは、連携モデルには、表2-1に記載されるように、一般に利用者の利便性向上、セキュリティ強化、コスト削減等のメリットが期待できるためです。ただし、対象手続に適するIDプロバイダが存在しない場合も想定されます。この場合には、非連携モデルによる実装を選択してください。

なお、本解説書の4章で後述するとおり、身元確認手法や当人認証手法は複数の手法を併用する場合も想定されます。そのような場合には、「連携モデルと非連携モデルの組み合わせモデル」を選択することを検討してください。

⁸ セキュリティとユーザビリティを両立できる手法の例としては「パスキー」や「スマートフォンのマイナンバーカード」が挙げられます。各手法の詳細については「別紙1 身元確認手法の具体例」及び「別紙2 当人認証手法の具体例」を参照してください。

表 2-1 連携モデルと非連携モデルの主な特徴

項目	連携モデル	非連携モデル
利用者の 利便性	利用者は、ID プロバイダ側で一度実施した身元確認結果を他の連携サービスでも利用できるようになる。	利用者は、サービスごとに身元確認を実施することが前提となる。
	利用者は、パスワード等の認証器をIDプロバイダに登録すればよく、サービスごとに管理しなくてよい。	利用者は、パスワード等の認証器をサービスごとに管理する必要がある。
可用性	ID プロバイダの可用性に依存する。ID プロバイダが障害やメンテナンスによってサービスを停止している間は、身元確認や当人認証が行えなくなる。	自システムの可用性に依存する。メンテナンス等による計画停止については自システム側でコントロールできる。
セキュリティ	セキュリティ面の適切な実装や運用において、自システム側の責任範囲を小さくすることができる。	セキュリティ面の適切な実装や運用を自システム側で負うこととなる。 新規開発部分が多くなることで、一般に脆弱性が作り込まれやすい。
実装の自由度	ID プロバイダの実装に依存するため、自由度は低い。	サービス提供側は、身元確認機能を自ら実装できるため、機能や仕様の自由度が高い。
コスト	本人確認機能を自ら実装・運用せずに済むが、ID プロバイダとの連携機能の実装や調整コストが必要となる。 総コストは非連携モデルと比較して一般に低い。	本人確認機能を独自に実装・運用する必要があり、連携モデルと比較して一般に高コスト。

3 本人確認の構成要素と対策基準（本編3章の解説）

本章では、ガイドライン本編の第3章「本人確認における脅威と対策」に関する解説、補足、参考情報を示します。

なお、政府情報システムにおいて主要な選択肢となる本人確認手法の具体例については「別紙1 身元確認手法の具体例」及び「別紙2 当人認証手法の具体例」をご覧ください。

3.1 身元確認（Identity Proofing）に関する解説

身元確認は、申請者から属性情報を収集することで申請者を一意に識別するとともに、収集した属性情報が真正かつ申請者自身のものであることを本人確認書類により検証することで、申請者が実在かつ生存する人物であることを確認するプロセスです。

ここでは、ガイドライン本編の記載内容のうち、実際の検討において特に留意いただきたい事項について解説します。

1) 身元確認において収集する属性情報の考え方

身元確認において申請者から収集すべき属性情報は、以下の3つの条件を満たす必要があります。

- ・ 第一に、その対象手続が扱う母集団の中で申請者を一意に識別できること。これには複数の属性を組み合わせる場合もあります。
- ・ 第二に、その対象手続や行政サービスを提供するために必要な属性が全て含まれていること。申請者の一意な識別には必要のない情報であっても、サービス提供に必要な情報は身元確認で収集する必要があります。
- ・ 第三に、必要最小限であること。プライバシー保護や個人情報保護の観点からは、申請者から収集する属性情報は必要最小限としなければなりません⁹。

図 3-1 身元確認において収集する属性情報が満たすべき基本条件



⁹ 収集情報の最小化は、万が一の情報漏えい等が発生した場合の影響範囲を小さくすることができるため、サービス提供側にとってもメリットのある考え方です。

2) 身元確認において利用可能とする本人確認書類の考え方

対象手続の身元確認においてどのような本人確認書類を利用可能とすべきかについては、次のような多角的な観点から検討することが望まれます。検討の際には、「別紙1 身元確認手法の具体例」の第2章も参考としてください。

- ・ **対象手続の利用者層**：申請者や利用者の様々な属性によって、本人確認書類の取得可否や所持率・普及率が異なります。対象手続が想定している申請者層・利用者層を踏まえた検討が必要です。
- ・ **必要な属性情報**：本人確認書類によって収集できる属性情報が異なるため、「身元確認において収集する属性情報」の検討結果を踏まえ、その属性情報を収集可能な本人確認書類を選択する必要があります。
- ・ **求められる保証レベル**：本人確認書類が備える機能によって、実現可能な身元確認保証レベルが異なるため、対象手続に求められる保証レベルを満たすことのできる本人確認書類を選択する必要があります。
- ・ **信頼可能な発行元**：対象手続にとって、本人確認書類の発行元は信頼可能な組織である必要があります。「公的機関により発行されたもの」を条件とする場合が多いですが、公的機関以外が発行した本人確認書類についても、その発行元が信頼できると判断できる場合には、受け入れ可能とするケースもあります。
- ・ **対象手続の根拠法令等**：行政手続の場合、利用可能な本人確認書類の条件が根拠法令等によって定められている場合があります。

なお、「4.3 身元確認手法の選定の考え方（本編4.2 関連）」で示すように、多くの手続・サービスにおいては、マイナンバーカードを基本としつつ、マイナンバーカード以外の代替手法についても併用を検討することになると想定されます。

3) ビデオベースの身元確認手法における脅威

ビデオベースの身元確認手法では、「プレゼンテーション攻撃」や「ビデオインジェクション攻撃」と呼ばれる、この手法で特有の脅威の考慮が必要です。これらの攻撃への対策は、身元確認に利用する端末やアプリケーションの仕様によって異なるほか、日々進歩する生成 AI が攻撃の高度化に関係しているため、本解説書の執筆時点（2026年2月時点）では一律の対策基準を示すことが難しい状況です。

そのため、ビデオベースの身元確認手法の採用を検討する際には、その時

点の最新の脅威と対策技術の動向を確認し、必要な対策を判断してください。

ア プレゼンテーション攻撃とは

印刷した写真、タブレット端末に映した映像等を身元確認時にカメラに映すことで、攻撃者が自身の容貌を偽装する攻撃のことを指します。カメラ等のセンサに偽造物等を提示（プレゼンテーション）する攻撃であるため、プレゼンテーション攻撃と呼ばれます。静止画や事前に撮影された動画だけでなく、AI 技術を活用しリアルタイムに顔を入れ替えられた映像が用いられる場合もあります。また、攻撃者が精巧に作られた 3D マスクを被ってカメラ越しの身元確認を突破しようとする攻撃例もあります。

プレゼンテーション攻撃は攻撃方法が単純であり、偽装された映像には不自然な点が比較的生じやすい攻撃と言えます。その一方で、身元確認を行うデバイスを侵害せずに攻撃が行われるため、デバイス側のセキュリティ機能による防止・検知が難しいという特徴があります。

イ ビデオインジェクション攻撃とは

攻撃者がカメラや映像処理の途中で偽の映像データを注入することで、本来撮影した映像ではない別の映像データを送信する攻撃です。プレゼンテーション攻撃と同じく、AI 技術を活用しリアルタイムに顔を入れ替えられた映像が用いられる場合もあります。

プレゼンテーション攻撃と異なり、デバイス側を侵害して偽のデータを注入する必要があるため、デバイス側のセキュリティ機能による防御や検知による対策を検討することができます。一方、映像の不自然さによる検知はプレゼンテーション攻撃よりも一般に難しくなります。

4) 身元確認におけるプライバシー面の考慮事項

行政機関等における身元確認では、2. 4 3)で示したとおり所掌事務又は業務に必要な場合に限り、利用目的が特定された形で、必要最小限の個人情報を取得することとなります¹⁰。連携モデル、非連携モデルのどちらの場合であっても、民間事業者が委託先としてステークホルダーに加わる場合があるため、「誰が」「どのような利用目的」で身元確認のために個人情報を取得するのかを、サービス・業務企画のできるだけ早い段階でのプライバシー影響評価（PIA）等により把握し、リスクを整理することが大切です。

(解説) 身元確認におけるプライバシー侵害の可能性

必要以上の取得について

個人情報保護法や根拠法令等に従って個人情報を取得する上では、利用目的を達成する上で必要最小限の取得が求められますが、「念のため」と必要以上に身元確認情報を求めることは、利用者にも無用な不信感を与える可能性があります。

不適切な長期保存について

行政機関等の場合は、公文書管理の観点から適切に保存期間を決定し保存する必要がありますが、不必要に保有することは情報漏えい時のリスクが高まります。民間事業者の事例では、サービス退会者の本人確認書類（運転免許証等の画像）が漏えいして問題となったものもあります。

目的外利用について

例えば、身元確認のためと明示して電話番号やメールアドレスを取得した場合、その電話番号やメールアドレスを使って身元確認とは関係のないお知らせやマーケティングを行ってしまうと、利用者の想定とは異なり目的外の利用となるためプライバシーの侵害にあたる可能性があります。

委託の範囲外での個人情報等の利用について

連携モデル、非連携モデルを問わず、外部民間事業者が行政機関等からの委託を受け、身元確認を実施する場合があります。外部民間事業者は行政機関等からの個別契約等によって、当該行政機関等の身元確認に係る委託の範囲での個人情報等の取扱いとすることが必要となります。

¹⁰ 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事務対応ガイド（行政機関等向け）」4-1 保有に関する制限。

上記とは別に、身元確認を行う外部民間事業者が、利用者から直接的に当該外部民間事業者の利用規約やプライバシーポリシーに記載された利用目的によって各種個人情報等を取得し、行政機関等へは身元確認の結果のみを伝える場合、身元確認の過程において収集された個人情報等は当該外部民間事業者の利用目的の範囲で取り扱われることとなるため、行政機関等はPIA等を実施し当該外部民間事業者のリスク分析・評価を十分に実施することが望まれます。

3.2 当人認証 (Authentication) に関する解説

当人認証は、対象手続を利用しようとする申請者が、あらかじめ登録されている者と同じの人物であること（当人性）を確認することです。

ここでは、ガイドライン本編の記載内容のうち、実際の検討において特に留意いただきたい事項について解説します。

1) リアルタイムフィッシングについて

「2.1 本人確認に関する直近の動向」でも述べたとおり、昨今は「リアルタイムフィッシング」と呼ばれる攻撃手法が増加しています。

従来の（リアルタイムでない）フィッシングは、利用者を偽サイト上に誘導することによるパスワード等の窃取と、窃取したパスワード等を悪用して実際に不正アクセスを試みる攻撃が独立して非同期的に（ばらばらに）行われることが一般的でした。このような攻撃に対しては、有効期限の短いワンタイムパスワード認証を組み合わせることで、事後的に不正アクセスを試みられた場合でもワンタイムパスワードは期限切れ（又は時間経過による不一致）となるため、不正アクセスを防ぐ対策として機能していました。

しかしながら、リアルタイムフィッシングでは、利用者が偽サイトに入力したパスワード等を、攻撃者がリアルタイムに正規サイトに中継して不正アクセスを試みます。このため、有効期限の短いワンタイムパスワードであっても、利用者の入力と攻撃者の不正利用のタイミングが一致してしまうことで、不正アクセスを防ぐことが困難です。こうした高度な攻撃手法に対抗するためには、フィッシング耐性のある認証方式の導入が重要となります。

参考情報：フィッシングの進化と被害事例

金融取引や行政手続がオンラインで完結する現代において、最も基本的かつ深刻な脅威の一つとして拡大し続けているのがフィッシングです。フィッシングとは、実在する銀行、クレジットカード会社、EC サイト、あるいは公的機関を装ってメールやSMSを送信し、本物そっくりで作られた「偽の Web サイト（フィッシングサイト）」へ誘導する手口です。その目的は、ID/パスワード等の認証情報、クレジットカード番号、銀行口座情報等を入力させ、盗み出すことにあります。

リアルタイムフィッシング

フィッシングは進化しており、「中継サーバ」を用いたリアルタイムフィッシングにより、従来安全とされてきた「多要素認証」すらも突破されてしまいます。攻撃者は、利用者と正規サイトの間に「中継サーバ」として

割り込み、利用者が偽サイトに入力した ID やパスワード、ワンタイムパスワード (OTP) をリアルタイムで正規サイトに転送することで、認証を突破してしまいます。

「攻撃の流れ」



この手法により、利用者は「正しい手順をしている」と思い込んだまま、攻撃者によって不正にログインされてしまいます。攻撃者は不正ログイン後に、利用者に対して認証失敗画面を表示することで、利用者は攻撃に気づきにくくなります。

被害事例

フィッシングの脅威は、認証情報の窃取にとどまらず、個人の預金等の資産そのものを狙う段階へと深刻化しています。ここでは、日本国内で発生した被害事例を紹介します。

「インターネットバンキングの不正送金被害」

一つ目は、銀行口座から預金が不正に送金される被害です。警察庁の発表によると、2023年から2024年にかけてインターネットバンキングに係る不正送金被害が過去最悪のペースで急増しました。銀行を装い、「取引制限のお知らせ」などのメールで偽サイトへ誘導し、認証情報を盗み取る手口が横行しています。特筆すべきは、個人だけでなく法人口座も標的になり始めている点です。法人口座は送金限度額が高く設定されていることが多いため、一件あたりの被害額が数百万～数千万円にのぼるケースもあり、企業の存続に関わる重大なリスクとなっています。

「ネット証券を標的とした資産収奪」

二つ目は、ネット証券会社を装った攻撃です。攻撃により、認証情報だけでなく、出金に必要な「取引パスワード」までもが盗まれています。さらに、株式や投資信託を勝手に大量に購入することで、短時間のうちに株価を釣り上げ、攻撃者が利益を得る事例が発生しました。本被害における補償についても話題に上がり、近年で大きく取り上げられた事例となりました。

2) 「フィッシング耐性」を実現できる手段について

当人認証がフィッシングへの耐性を備えることを「フィッシング耐性」と呼びます。本解説書の執筆時点（2026年2月時点）で厳密なフィッシング耐性を有する当人認証手法は、「パスキー」と「PKI（公開鍵基盤）をベースとした認証」の2つが現実的な選択肢です。

ア 「パスキー」について

パスキーは、Web サイトから利用者の Web ブラウザ等に送られてくるデータ等に、利用者側の鍵（秘密鍵）でデジタル署名を行い、Web サイト側にあらかじめ登録されている対となる鍵（公開鍵）によってデジタル署名の検証を行うことで、利用者側が本物の鍵を持っていることを確認する仕組みです。

パスキーは、そのドメインに紐づけられたものしか使うことができないように Web ブラウザ等によって制御されます。そのため、たとえ利用者がフィッシングメールに騙されて偽サイトにアクセスしてしまっても、偽サイトのドメインでは正規のパスキーを使うことはできません。これにより、パスキーはフィッシングへの耐性をもつ方式とされています。

参考情報：パスワードと比較したパスキーの真の価値

昨今のフィッシングと被害の増加を受けて、フィッシングへの耐性が高いと言われているパスキーへの注目が世界的に高まっています。

パスキーは Web サイトのドメインと紐づけて管理され、異なるドメインでは使うことができないよう制御されます。これによって利用者が偽サイトに誘導されてしまった場合でもログインに必要な情報の窃取を防ぎ、フィッシングを防ぐことができる仕組みとなっています。

Web サイトのドメインを用いて判定するという仕組みについては、一般的な「パスワードマネージャー」でも同じではないかと考える方もいらっしゃるかもしれませんが、確かにパスキーでなくパスワードを用いて、ブラウザがドメインで正規のサイトかを判定し、正規のサイトであればパスワードを自動で入力するのであれば、フィッシングへの耐性はパスキー同様にあると捉えられます。

しかしながら、パスワードマネージャーのパスワードはパスキーと比べて幾つかの難点があります。そもそも、Web サイト側からは利用者がパスワードをパスワードマネージャーに保管させて使うことを確認することも強制することもできません。また、同じパスワードを複数の Web サイトで用いている場合は、たとえパスワードマネージャーに保管して入

力を任せていたとしても、Web サイト側が攻撃者に侵害された場合にパスワードを盗み取られる可能性があります。攻撃者が ID とパスワードの組合せを盗み取って、様々な Web サイトに当該の ID とパスワードを入力してログインを試行するパスワードリスト攻撃によって、既に多くの被害が生じています。パスキーは、Web サイトごとに異なる鍵を使うだけでなく、さらには利用者側と Web サイト側では異なる鍵をそれぞれ持ち合わせるため、Web サイト側が攻撃者に侵害されて盗まれた鍵を不正ログインに使うことはできません。

また、パスワードマネージャーは通常パスワードと Web サイトのドメインを紐づけて管理しますが、利用者が手動のコピー&ペーストをすれば、紐づけられていないドメインの Web サイトにもパスワードを入力できてしまうため、フィッシングサイトにもパスワードを入力できてしまいます。パスキーでは、登録している Web サイト以外にはパスキーを使えないように制御されるため、フィッシングサイトによる情報窃取を防ぐことができます。

他方で、パスキーを使えない利用者側の環境もあることや、Web サイト側の改修が必要となるためパスキーの導入が進まないという場合もあります。とはいえ、総合的に見てもセキュリティと、利便性の向上という観点でもパスワードに比べてパスキーに優位性があります。

イ 「PKI（公開鍵基盤）をベースとした認証」について

PKI をベースとした認証では、利用者に紐づくクライアント証明書を用いた mTLS (Mutual TLS、相互 TLS) を行うことで、フィッシング耐性を備えた本人認証を実現できることが知られています。mTLS では、サーバ側だけでなくクライアント側（利用者側）にも証明書を発行し、通信の際に双方が互いの証明書を検証することで認証を行う仕組みです。クライアント側とサーバ側の双方で証明書を保持することから、mTLS と呼ばれます。利用者が正規の証明書を保持していない限り認証が成立せず、偽サイトが中継しようとした場合でもフィッシングを防ぐことができます。

ただし、クライアント証明書と鍵ペアを格納した IC カードや USB キー等をあらかじめ利用者側に配付する必要があります。

3) アカウムの回復手法について

本人認証の検討においては、利用者が認証に用いるデバイス等を紛失した場合や、サービスへの不正アクセスを検知した場合等に備えて、アカウントの停止（ロック）と、停止状態からの回復手段を設けておく必要があります。

このとき、採用している本人認証手法よりも強度の低いアカウント回復手

段を設けてしまうと、そこを不正アクセス攻撃の起点とされる懸念があるため、アカウント回復手段については十分な注意を払った検討が必要です。

例えば、フィッシング耐性のある「パスキー」を当人認証手法として採用していたとしても、利用者側の操作ミス等によってパスキーを喪失した際のアカウント回復手段が「パスワード認証+ワンタイムパスワード認証」であった場合、利用者に対して「パスキーを再設定してください」といったフィッシングメールが送られ、騙された利用者が偽サイト上でパスワードとワンタイムパスワードを入力してしまうと、リアルタイムフィッシングによって攻撃者にアカウントを乗っ取られてしまう可能性があります。

したがって、ガイドライン本編ではアカウント回復手段の検討においては、「採用している当人認証手法と同等以上の強度の手法を選択すること」を求めており、具体的な手法の例として以下を示しています。万能な手法は存在せず、いずれの手法も一長一短であるため、対象手続の特性や求められる保証レベルに応じた検討が求められます。

ア 身元確認の再実施

アカウント回復が必要となった場合に、身元確認の再実施を求める方法です。十分な保証レベルの身元確認を行うことで、前述するアカウントの乗っ取りのような脅威を防ぐことができます。ただし、身元確認の再実施は運用負担増やコスト増につながる場合があるほか、利便性への影響についても考慮が必要です。

主な特徴と考慮事項は次のとおりです。

- ・ アカウント回復に起因する脆弱性を生みにくく、リカバリ用の仕組みを別途構築する必要がない。
- ・ 一方、身元確認は一般的にサービス提供側の負担の高い作業であるため、アカウント回復のための身元確認の再実施が大量に必要となるとシステムの運用負担やコスト増の原因となる。
- ・ 身元確認の再実施は、一般に利用者側にとっても時間や手間がかかる作業であり、利便性が高い方法とは言えない場合もあるため、サービスからの離脱を招く（紙・郵送による申請の方が面倒がないと判断され、オンライン手続を諦めてしまう）きっかけになってしまう可能性も懸念される。

参考情報：マイナンバーカードを活用した身元確認の再実施について

従来の「対面による身元確認」や「ビデオベースの身元確認」といった

手法では、身元確認の再実施はサービス提供側・利用者側の双方にとって負担の高いプロセスでしたが、マイナンバーカードによる身元確認を行う場合については、従来よりも簡便に身元確認を再実施できる可能性があります。

例として「実物のマイナンバーカードの券面事項入力補助 AP」を用いる場合（かつ、容貌確認が不要な場合）であれば、利用者側は実物のマイナンバーカードと暗証番号さえあれば、身元確認の再実施をオンラインで即座に実施することができます。

イ 予備の認証器の登録

アカウント回復が必要となったときに備えて、複数の認証器（予備の認証器）をあらかじめ登録しておく方法です。

主な特徴と考慮事項は次のとおりです。

- ・ サービス提供側は複数の認証器の登録に対応する必要があるが、「ア 身元確認の再実施」よりは低コストで済む可能性がある。また、利用者側にとっても、「ア 身元確認の再実施」よりは利便性が高い。
- ・ 認証器の追加登録や変更が行われた際には、登録されている利用者の連絡先に対してその旨を通知するとともに、変更が有効となるまで一定の時間を設けることで、攻撃が行われた場合でも正規の利用者が検知しサービス側に連絡する猶予が生まれ、アカウントの乗っ取り攻撃のリスクを低減することができる。
- ・ ただし、①同程度の認証強度をもち、②同時に紛失するリスクが低く、③多くの利用者が利用できる、という条件を満たす複数の認証器の組み合わせは限られる¹¹。
- ・ 複数の認証器の登録を強制すると利用者の利便性の低下につながり、登録を任意とすると別のアカウント回復手段も必要となる。また、利用者が全ての認証器を喪失した場合のアカウント回復方法は別途用意する必要がある。

ウ リカバリーコードの事前発行

アカウントの登録時に、アカウント回復用のリカバリーコードを発行しておき、アカウント回復が必要となった際にはリカバリーコードの入力を求める方法です。運用の負担や制約が比較的少ない方法と考えられますが、フィ

¹¹ 一例として、「パスキー」と「マイナンバーカードの利用者証明用電子証明書」は、この条件に該当する組み合わせとして利用できる場合がある。

ッシングに脆弱な点には考慮が必要です。

主な特徴と考慮事項は次のとおりです。

- ・ リカバリーコードは登録時に一度だけ発行される仕組みであるため、後述する「リカバリーコードの必要時発行」と比べると、攻撃者が能動的に不正入手できる手段が比較的少ない。
- ・ 「イ 予備の認証器の登録」と異なり、基本的にはどのような利用者に対しても適用できる。
- ・ 利用者はリカバリーコードを適切に保管しておかなければならないが、アカウント回復の作業は「ア 身元確認の再実施」よりは簡易で済む。
- ・ 利用者がリカバリーコードを紛失した場合のアカウント回復方法は別途用意する必要がある。
- ・ リカバリーコード入力フィッシングには脆弱であり、「あなたのアカウントが停止されました。以下のリンクからリカバリーコードを入力してください。」といったフィッシングメールによって窃取されてしまう懸念がある。

エ リカバリーコードの必要時発行

アカウント回復が必要となったタイミングで、利用者の求めに応じて登録されている連絡先（住所、電子メールアドレス、携帯電話番号等）に対してリカバリーコードを送信し、その入力を求める方法です。「ウ リカバリーコードの事前発行」よりも利便性が高い方法ですが、連絡先が乗っ取られた場合のリスクの考慮が必要です。

主な特徴と考慮事項は次のとおりです。

- ・ 「ウ リカバリーコードの事前発行」と比べて、利用者はリカバリーコードを保管する必要がないという利点がある。
- ・ リカバリーコードの連絡先となる電子メールアドレスや携帯電話番号が攻撃者に乗っ取られた場合、リカバリーコードも不正に入手され、アカウントが連鎖的に乗っ取られるリスクがある。
- ・ 「ウ リカバリーコードの事前発行」と同様に、フィッシングには脆弱である。

4) パスワード認証に関する留意事項

パスワード認証は「当人認証保証レベル 1」に該当する手法です。現時点で多くの行政情報システムで使用されている当人認証手法ですが、「パスワードの使い回し」というサービス提供側でのコントロールが難しい脅威があり、フィッシングに対しても脆弱です。このため、満たすべき当人認証保証レベ

ルが2以上であるシステムの場合、パスワードはもはや採用を検討すべき手法ではありません¹²。

民間サービスでは、パスキーへの転換が進む等、パスワードレス化の流れが加速しています。また、米国 NIST SP 800-63B-4 ではパスワード認証に関する要求事項が更に厳格化されており、仮に採用する場合でも、その実装に当たっては十分な検討が求められます。

参考情報：パスワード認証に関する米国 NIST の要求事項

2025 年 8 月に改定第 4 版が発行された米国 NIST SP 800-63B-4 では、パスワード認証の実装に関して以下のような要求事項が求められています。

政府情報システムにおいてパスワード認証の仕様や実装を検討する際にも、これらの要求事項を参考とすることが望まれます。

- ・ パスワードの長さは、単要素認証として利用する場合は 15 文字以上、多要素認証の一要素として利用する場合は 8 文字以上としなければならない。また、設定可能なパスワードの最大長は少なくとも 64 文字とすべきである。
- ・ パスワード設定時に異なる文字種を混在させることを強制してはならない¹³。
- ・ 利用者に対して、定期的なパスワードの変更を求めてはならない¹⁴。ただし、パスワードが侵害された証拠がある場合には、パスワードの変更を求めなければならない。
- ・ パスワードを思い出すための「ヒント」や「秘密の質問」は実装してはならない¹⁵。
- ・ パスワードマネージャーや自動入力機能（オートフィル機能）を利用できるようにしなければならない。パスワードの「貼り付け」についても、自動入力ができない場合を考慮して許可すべきである。

(NIST SP 800-63B-4 「3.1.1. Passwords」より抜粋・要約)

¹² パスワード認証の安易な採用は、様々なセキュリティ面の対処が必要となり、結果として将来的なコスト増の要因となることも懸念されます。

¹³ 異なる文字種の混在を強制させることは、攻撃者が予測しやすいパスワードの設定を誘導してしまう弊害があると言われてしています。

¹⁴ 定期的な変更も、利用者が覚えやすいパスワードを設定しやすくなり、攻撃者が予測しやすいパスワードの設定を誘導してしまう弊害があると言われてしています。ただし、複数人で共有するアカウントの場合については、パスワードの定期変更が有効に機能する場合があります。

¹⁵ 「ヒント」や「秘密の質問」は、パスワードが本来もつ空間を狭めることで攻撃者の予測可能性を高めてしまったり、本来は秘密情報ではない情報（例：母親の旧姓等）を設定することで、認証に必要な情報を別の手段で調査・推測されてしまったりする懸念があります。

5) 当人認証におけるプライバシー面の考慮事項

なりすまし等によって不正アクセスを受けた場合、登録されているアカウント情報や身元確認情報が漏えいしたときの影響を、事前にPIA等を実施してリスク分析・評価し、適切に当人認証保証レベルを決定することが大切です。

また、当人認証に係る利用目的の範囲とならないような利用や、認証器に含まれる情報によって利用者を不適切に名寄せ・分析することがないようにするなど、当人認証の利用目的についても事前にリスク分析・評価が実施されることが推奨されます。

当人認証におけるプライバシー侵害の可能性

個人情報漏えいの影響について

例えば、登録されているアカウント情報や身元確認情報に生体認証情報や要配慮個人情報（病気、障害の有無等）のような機微性の高い情報が存在する場合、漏えいが起こった際に容易には回復できないプライバシー面への影響が懸念されるため、適切な当人認証手法を検討する必要があります。

目的外利用や不適正な利用について

例えば、どのような行政手続や行政サービスを利用しているか等、認証器の情報から不必要な名寄せや追跡を行うことは、利用者のプライバシーへの影響が懸念され、目的外利用や不適正な利用とみなされる可能性があります。

委託の範囲外での個人情報等の利用について

連携モデル、非連携モデルを問わず、外部民間事業者が行政機関等からの委託を受け、当人認証を実施する場合があります。外部民間事業者は行政機関等からの個別契約等によって、当該行政機関等の当人認証に係る委託の範囲での個人情報等の取扱いとすることが必要となります。

上記とは別に、当人認証を行う外部民間事業者が、利用者から直接的に当該外部民間事業者の利用規約やプライバシーポリシーに記載された利用目的によって各種個人情報等を取得し、行政機関等へは当人認証の成功・失敗の結果（およびその理由）のみを伝える場合、当人認証の過程において収集された個人情報等は当該外部民間事業者の利用目的の範囲で取り扱われることとなるため、行政機関等はPIA等を実施し当該外部民間事業者のリスク分析・評価を十分に実施することが望まれます。

3.3 フェデレーション (Federation) に関する解説

1) フェデレーションにおける主な脅威の解説

前述のとおり、フェデレーションを使った連携モデルには多くのメリットがあります。他方、フェデレーションには特有の脅威や考慮事項もあり、適切な実装・運用がなされなかった場合にはリスクにつながります。

ガイドライン本編では、主な脅威として「保証レベルの齟齬」と「アサーションに関する攻撃」を示しています。これらの脅威を理解した上で、フェデレーションの適切な実装や運用を行うことが必要です。

ア 保証レベルの齟齬

フェデレーションにおいて、対象手続（依拠当事者¹⁶）が本来必要とする保証レベルと、ID プロバイダで実際に実施されている本人確認手法が満たす保証レベルとの間に不一致が生じることを指します。

ID プロバイダが提供する本人確認手法の仕様や保証レベルを依拠当事者側が十分に把握できていなかったり、フェデレーションによる運用開始後に ID プロバイダ側の本人確認手法の仕様や運用が変更されたりすることで、齟齬が生じる可能性があります。保証レベルの齟齬が生じた場合、依拠当事者側が本来検知しなければならない攻撃を検知できず、攻撃の起点として悪用されるリスクがあります。

このような保証レベルの齟齬を防ぐためには、依拠当事者側が要求する保証レベルと ID プロバイダによって提供される保証レベルの一致を「信頼関係の確立」プロセスによって確認・合意することが必要です。また、合意事項が認識なく変更されることを防ぐため、本人確認に関する機能、仕様、運用等に変更が生じる場合は ID プロバイダから依拠当事者に事前共有することを定めたり、合意事項が実際に実装されていることを定期的に検査したりするなどの対策も考えられます。

イ アサーションに関する攻撃

ID プロバイダから依拠当事者に対して発行されるアサーションが、盗聴・窃取・偽造・改ざん・再利用されることで、アサーションに含まれる利用者

¹⁶ 依拠当事者：連携モデルにおいて、身元確認や本人認証を ID プロバイダに依拠する主体のことを指します。

の個人情報を窃取されたり、アサーションを使って依拠当事者に対するなりすまし等の攻撃が行われたりする懸念があります。

アサーションに関する攻撃への対策は、ID プロバイダと依拠当事者との間で安全な連携のための設定を行った上で、詳細についてはフェデレーションプロトコルの技術標準に則って実装することが一般的です。

2) フェデレーションに関する主要な技術標準

フェデレーションを実現するための主要な技術標準として、OpenID Connect と SAML (Security Assertion Markup Language) があります。これらの標準を適切に活用することで、フェデレーションの安全性と利便性を高めることが可能となります。

なお、どちらの標準を採用するかは ID プロバイダ側の対応状況等に依存しますが、後述するフェデレーションのトランザクションの開始に関する対策基準を満たすためには、OpenID Connect を候補とすることが推奨されます。

ア SAML を利用する際の留意事項について

ガイドライン本編では、アサーションに関する攻撃への基本的な耐性を確保するため、フェデレーションのトランザクションは依拠当事者側から開始することを原則としています。

フェデレーションによる連携は、ID プロバイダが依拠当事者に対してアサーションを発行することによって行うこと。

アサーションに関する攻撃への基本的な耐性を確保するため、フェデレーションのトランザクションは原則として依拠当事者側から開始すること。ただし、連携が閉域網内で行われる場合など第三者による攻撃のリスクが低いとみなせる場合には、ID プロバイダ側からトランザクションを開始する方式としてもよい。

(ガイドライン本編「表 3-15 アサーションに関する対策基準」より)

しかしながら、SAML ではフェデレーショントランザクションを依拠当事者側ではなく ID プロバイダ側から開始する方式での実装も少なくありません。

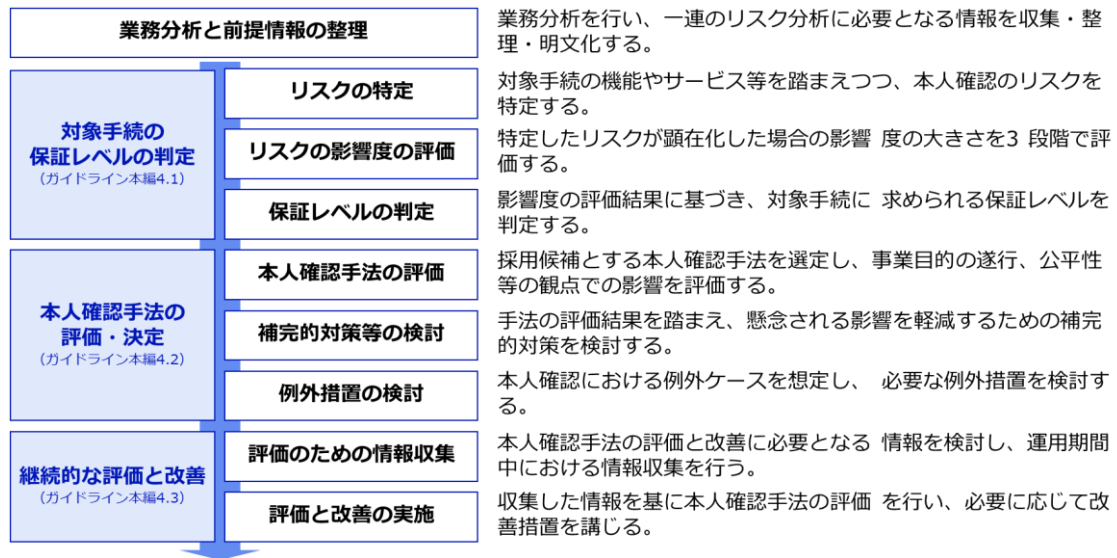
SAML を利用する場合には、上記の対策基準を満たすために依拠当事者側からフェデレーショントランザクションを開始する方式での実装とするか、閉域網内で連携を行う等攻撃リスクが低いとみなせる環境において ID プロバイダと連携する必要がある点に留意してください。

4 本人確認手法の検討方法（本編4章の解説）

本章では、ガイドライン本編の4章における各検討プロセスについて、検討にあたる基本的な考え方や、検討の参考となる情報を解説します。

本人確認手法の検討プロセスの全体像は以下のとおりです。

図 4-1 本人確認手法の検討プロセスの全体像



4.1 業務分析と前提情報の整理¹⁷

本人確認に関するリスクとその影響は、対象手続が提供する機能、サービス、取り扱う情報資産、手続によって得られる権益等によって様々です。したがって、対象手続におけるリスクを正確に特定するためには、対象手続に関する業務分析を行い、リスク分析に必要となる前提情報を収集・整理し、明文化することが必要です。

整理すべき前提情報としては、以下のような項目が考えられます。

¹⁷ 業務分析は本人確認の検討において特有のプロセスではなく、業務改革（BPR）や情報システムの整備・更改等を検討する際に求められる共通的なプロセスであるため、ガイドライン本編においては具体的なプロセスとして定義していません。本解説書でも業務分析自体の具体的な実施方法は割愛し、本人確認手法の検討のために業務分析によって整理しておくべき情報に限って解説します。

表 4-1 リスク分析にあたって整理すべき前提情報（例）

分類	項目	整理すべき情報
基本情報	名称・目的	対象手続の名称と目的 (誰に対して、どのような効果や権利権益を与え、どのような結果を目指すものか)
	根拠法令等	対象手続の根拠法令、関係する準拠文書やガイドライン等
業務概要	対象手続の申請者・利用者	対象手続(行政手続、行政サービス等)の申請者や利用者は誰であるか/個人か法人か/どのような属性をもつ者か
	業務の関係者	対象手続を提供するための業務に、どのような者が関係するか(申請の受付担当者、審査担当者、関係業務の委託事業者、システム運用事業者等)
	業務フロー	対象手続における各業務が、どのような関係者によって、どのようなフローで実施されるか
	サービス提供に必要な申請者の情報	対象手続を提供するために、申請者からどのような属性情報を収集し、把握する必要があるのか
	取り扱う情報	各業務を実施する際に、誰が・どのような情報を取り扱うのか
システム概要	機能一覧	対象手続の業務を遂行しサービスを提供するために、どのような情報システムの機能が必要となるか
	システム利用者とアクセス権限	対象手続を提供するためのシステムの利用者にはどのような者がおり、どのような機能やデータに対するアクセス権限を有するか
	他システムとの連携の概要	対象手続を提供するために、他システムとどのような情報を連携するのか
その他	根拠法令等による制約	根拠法令等によって求められている本人確認に関する制約等はあるか (申請時の電子署名の可否等、受入可能としない本人確認書類の種類、採用可能な本人確認手法の指定等)

4.2 対象手続の保証レベルの判定（本編4. 1）

このプロセスでは、対象手続におけるリスクの特定と評価を行うことで、対象手続に求められる保証レベルを判定します。

1) リスクの特定

このプロセスでは、前述の「業務分析と前提情報の整理」の結果を踏まえつつ、対象手続における本人確認が適切に行われなかったり、不正アクセスが行われたりする場合はリスクケースとして特定し、そのリスクケースが顕在化したときに「誰に対して」、「どのような悪影響が及ぶのか」を整理し、文書化します。

ガイドライン本編では、代表的なリスクケースとして4つの例を挙げています。検討の実務においては、この代表的なリスクケースを基本として考えつつ、対象手続において実際に想定されるリスクケースにあわせた追加・削除を行いながら、具体的な影響内容を特定してください。

参考として、架空の対象手続における検討結果の例を以下に示します。

表 4-2 リスクケースと顕在化時の影響の特定（例）

プロセス	リスクケース	顕在化時の悪影響の特定結果（例）
身元確認	実在する人物になりすました申請や登録	なりすましを検知できなかった場合、攻撃者に対して給付金が不正に支給される可能性があり、組織は金銭的な被害を受ける。攻撃者になりすまされた個人がその後に申請を行った場合は二重申請として検知されるが、なりすまされた個人に対する給付金の支給が最大●●か月程度遅延する可能性がある。
	実在しない架空の人物になりすました申請や登録	なりすましを検知できなかった場合、攻撃者に対して給付金が不正に支給される可能性があり、組織は金銭的な被害を受ける。個人に対する影響は想定されない。
当人認証	登録済みの利用者に対する不正アクセス	申請システムへの不正アクセスが行われた場合、システム上に表示される氏名や申請受理状況が攻撃者に漏えいする。ただし、システム上に表示される情報や当該申請の有無は、要配慮個人情報等の機微な情報には該当しない。

プロセス	リスクケース	顕在化時の悪影響の特定結果（例）
		また、不正アクセスが行われた場合でも、申請の変更や取り消し等を行うことはできないため、申請そのものへの影響はない。
	フィッシングサイトに対する情報入力	電子申請システムの登録者のメールアドレスやパスワードが攻撃者に漏えいし、不正アクセスに繋がる。

※斜体は検討結果の「例」です。実際の検討結果は対象手続の特性やシステムの実装等によって異なることに注意してください。

2) リスクの影響度の評価

このプロセスでは、「リスクの特定」プロセスにおいて整理したリスク顕在化時の悪影響の内容を踏まえ、その影響度を「高位」、「中位」、「低位」の3段階で評価し、最も高い影響度を「対象手続における総合的な影響度」として判定します。

リスクの影響度の「高位」、「中位」、「低位」の評価は、ガイドライン本編の「表 4-3 リスクの影響度の評価基準」を基準として評価を行います。

参考として、架空の対象手続における検討結果の例を以下に示します。

表 4-3 リスク顕在化時における影響度の判定（例）

顕在化時の悪影響の特定（例） （「リスクの特定」の結果より抜粋）	影響度の判定結果と 判断根拠（例）
なりすましを検知できなかった場合、攻撃者に対して給付金が不正に支給される可能性があり、組織は金銭的な被害を受ける。 攻撃者になりすまされた個人がその後申請を行った場合は二重申請として検知されるが、なりすまされた個人に対する給付金の支給が最大● ●か月程度遅延する可能性がある。	【高位】 なりすまされた個人に対する給付金の支給遅延は長期間にわたるおそれがあり、高位の基準の一つである「 <u>特定の利用者や関係者が、本来有する権利権益を長期間にわたって行使又は享受できなくなるなど、深刻かつ長期的な影響を受ける。</u> 」に該当すると判断。
申請システムへの不正アクセスが行われた場合、システム上に表示される氏名や申請受理状況が攻撃者に漏えいする。要配慮個人情報等の機微な情報は含まれない。	【低位】 不正アクセスが発生した場合でも漏えいする情報は限定的であり、プライバシーの重大な侵害につながる情報も含まれていない。また、申請手

顕在化時の悪影響の特定（例） （「リスクの特定」の結果より抜粋）	影響度の判定結果と 判断根拠（例）
不正アクセスが行われた場合でも、申請の変更や取り消し等を行うことはできないため、申請そのものへの影響はない。	<p>続への影響も生じず、利用者に生じる影響はパスワードの変更等によるアカウント回復の手続程度と想定されるため、低位の基準である「<u>特定の利用者や関係者の権利権益は侵害しないが、一時的な不便等の影響を与える。</u>」に該当すると判断。</p>

※斜体は検討結果の「例」です。実際の検討結果は対象手続の特性やシステムの実装等によって異なることに注意してください。

3) 保証レベルの判定

リスクの影響度の評価結果をもとに、対象手続に求められる保証レベルを判定します。

保証レベルは、「高位」が一つでも含まれれば「レベル 3」、「高位」が一つもなく、かつ「中位」が一つでも含まれれば「レベル 2」といったように、最も高い影響度に合わせて決定します。

参考情報：身元確認保証レベルと本人認証保証レベルが異なる例

ガイドライン本編に記載のあるとおり、対象手続によっては、身元確認保証レベルと本人認証保証レベルが異なる保証レベルとなる場合もあり得ます。

保証レベルが異なるケースの一例として、複数の手続等で共通的に利用する電子申請システムにおいて、申請を行う際にはその都度、身元確認の実施を求め、ログインだけでは申請状況等のステータス情報しか確認できないようなケースが考えられます。このようなシステムでは、身元確認を突破された場合の影響は「他人になりすました不正な申請」につながる一方、本人認証を突破された場合の影響は「申請ステータス等の不正な閲覧」等に限られるため、身元確認保証レベルと本人認証保証レベルの検討結果は異なるレベルとなる可能性があります。

逆に考えると、身元確認と本人認証によって、利用者が実施できる手続や、閲覧できる情報に差異がない場合には、なりすまし等による影響度も同等であり、保証レベルも同じレベルとなると考えられます。

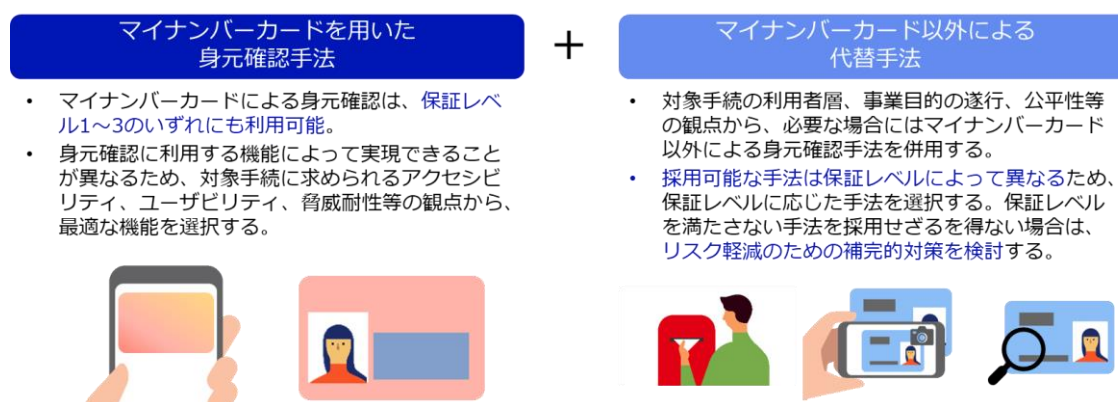
4.3 身元確認手法の選定の考え方（本編4.2関連）

本節では、身元確認手法の選定に当たって多くのケースに共通すると考えられる検討の流れと考え方を示します。

身元確認に利用可能な本人確認書類としての普及率や対応可能な保証レベルを考えると、多くのケースにおいて、まずはマイナンバーカードの活用を検討することが基本となると考えられます。

しかしながら、マイナンバーカードのみでは事業目的の遂行や公平性等の観点での懸念や支障が生じる場合も想定されます。そのような場合には、対象手続に求められる保証レベルに応じて、マイナンバーカード以外による代替手法を併用することでの対応を検討します。

図 4-2 身元確認手法の基本的な考え方



ただし、上記は多くのケースに共通する考え方を示すものであり、ここで示す手法の採用を必須とするものではありません。例えば、外国人観光客向けの行政サービスにおいてはマイナンバーカードによる手法は適しておらず、代替手法を中心とした手法の検討が必要であると考えられます。

1) マイナンバーカードを用いた身元確認手法の検討事項

マイナンバーカードを用いた身元確認手法には複数の手法が存在するため、対象手続の特徴、要求、根拠法等を踏まえ、適切な手法を選択することが求められます。

具体的には、「電子署名の要否」、「スマートフォンのマイナンバーカードの利用」、「複数機能の併用の回避」、「容貌確認の要否」等が主な検討事項となります。

ア 電子署名の要否の検討

マイナンバーカードによる身元確認手法は、大きく「電子署名を行うもの」と「券面情報の電子データ¹⁸によるもの」に大別できます。電子署名は実印に相当するものと位置付けられており、本人の意思表示としての法的効力を有することから、電子署名については真に必要な場合に限り利用し、電子署名の必要がない場合は「券面情報の電子データによる身元確認」を採用するという考え方が望まれます。

なお、スマートフォンで採用されている顔又は指紋による生体認証では署名用パスワードの認証強度を担保できないため、署名用パスワードを生体認証に代えることはできず、電子署名の要否によって身元確認の利便性は大きく左右されます。また、マイナンバーカードによる電子署名が可能なのは15歳以上に限られるという制約にも考慮が必要です。

電子署名の要否を判断するためには、次のような観点での確認や検討が必要です。この時、従前に公印を押印していたり電子署名を用いていた場合であっても、改めて確認・検討することが推奨されます。

- ・ 電子署名の対象文書が存在するか¹⁹
- ・ 対象手続において、電子署名による厳格な否認防止や電子署名法に基づく法的効力が必要かどうか（対象手続が否認された場合のリスクの大きさから判断）
- ・ 対象手続の根拠法等において、電子署名が求められているかどうか

イ スマートフォンのマイナンバーカードの活用方針の検討

スマートフォンのマイナンバーカードは、「利用のたびに実物のマイナンバーカードを読み取る必要がない」、「暗証番号の入力を生体認証で代替できる」等の様々なメリットがあるため、実物のマイナンバーカードによる身元確認手法を採用する場合には、スマートフォンのマイナンバーカードについても利用可能とすることが推奨されます。

¹⁸ ここでの「券面情報の電子データ」とは、実物のマイナンバーカードの「券面情報入力補助AP」や、スマートフォンのマイナンバーカードによる属性証明機能（カード代替電磁的記録）によって電子的に取得した、デジタル署名による検証が可能なデータのことを指します。

¹⁹ 署名対象文書が存在しないにもかかわらず、署名用電子証明書に含まれる基本4情報等を取得することを目的として電子署名を求める行為は、本来の電子署名の趣旨から逸脱しており適切ではありません。

参考情報：スマートフォンのマイナンバーカードの機能について

本解説書の執筆時点（2026年2月時点）では、Android端末では「Androidスマホ用電子証明書搭載サービス」が、iPhoneでは「iPhoneのマイナンバーカード」が利用可能であり、それぞれ対応している機能が異なります。

スマートフォンのマイナンバーカードで利用可能なサービスは順次拡大予定とされているため、検討の際には最新の情報を確認してください。

	属性証明機能	電子証明書機能
機能の概要	属性証明機能では、マイナンバー法 ²⁰ に基づく「カード代替電磁的記録」をスマートフォンに搭載して利用できる。 カード代替電磁的記録には基本4情報、個人番号、顔写真等が含まれており、これらを電子データとして提示・提出することができる。	公的個人認証法に基づく署名用電子証明書及び利用者証明用電子証明書をスマートフォンに搭載して利用できる。 実物のマイナンバーカードの署名用電子証明書及び利用者証明用電子証明書と同様に、電子文書に対する電子署名や、電子証明書を用いた本人認証に利用できる。
Androidの対応状況	2026年秋頃に提供開始予定 ²¹	対応
iPhoneの対応状況	対応	対応

ウ 複数機能の併用の回避

マイナンバーカードには前述のとおり、電子署名や券面情報入力補助AP等、身元確認に利用できる複数の機能が備えられています。

しかしながら、複数の機能を併用した場合、暗証番号・パスワード入力や

²⁰ マイナンバー法：行政手続における特定の個人を識別するための番号の利用等に関する法律 (<https://laws.e-gov.go.jp/law/425AC0000000027/>)

²¹ デジタル庁 Web サイト「2026年秋頃に「Androidのマイナンバーカード」へ刷新します」 (<https://services.digital.go.jp/mynumbercard-android/news/0cfe138d7fb5927e4dc6d/>)

カードの読み取りが複数回必要となってしまう、ユーザビリティが大きく損なわれてしまいます。

このため、マイナンバーカードにおける身元確認では、単一の機能で十分な保証レベルが確保できる場合は複数機能の併用はできる限り避け、単一の機能による身元確認の実施を検討することが推奨されます。

エ 容貌確認の要否の検討

マイナンバーカードの貸し借りが行われた場合、暗証番号や署名用パスワードも攻撃者に共有され得るため、貸し借りの検知ができません。対象手続におけるリスク評価の結果、マイナンバーカードの貸し借りを検知しなければならない場合には、貸し借りを検知するための容貌確認²²を組み合わせる必要があります。

身元確認を対面で行う場合は、券面の顔写真の偽造可能性にも留意が必要です。特に身元確認保証レベル 3 が求められる場合は、顔写真の偽造・改ざんが行われていないことをデジタル署名の検証によって確認する必要があります。

身元確認をオンラインで行う場合は、ビデオベースの容貌確認を行うことになるため、プレゼンテーション攻撃やインジェクション攻撃といった特有の脅威への対策も検討が必要です。これらの攻撃の詳細については「3. 1 身元確認 (Identity Proofing) に関する解説」の該当項を参照してください。

²² 非対面の場合は、マイナンバーカードによる非対面の身元確認（暗証番号等による検証）を実施した上で、さらにビデオベースの身元確認手法を組み合わせることによって容貌確認を実施する手順が考えられます。

2) マイナンバーカード以外による手法の検討

マイナンバーカード以外の手法の検討では、マイナンバーカードを用いた手法における留意事項²³を検討の上で、事業目的の遂行や公平性等の観点から代替手法の要否を検討します。代替手法が必要と判断される場合には、対象手続の保証レベルに応じた手法と補完的対策の採用を検討します。

ア マイナンバーカード以外による手法の要否の検討

対象手続の事業目的、想定される利用者層、申請等を行う環境条件、申請等の緊急性、マイナンバーカードの交付対象、普及状況、未取得者が新規交付にかかる期間等を考慮した上で、ガイドライン本編の「基本的な考え方」として示す5つの観点²⁴を踏まえつつ、身元確認においてマイナンバーカード以外による手法を受け付ける必要があるかどうかを判断します。

イ 採用する代替手法と補完的対策の検討

マイナンバーカード以外による身元確認手法（代替手法）が必要と判断した場合、対象手続に求められる身元確認保証レベルや利用可能とする本人確認書類を踏まえつつ、採用可能な代替手法を検討します。

一例として、ICチップを有する主要な本人確認書類にはマイナンバーカード以外にも以下のものがあり、身元確認保証レベル3が求められる手続において、これらを用いた代替手法の採用を検討できる場合があります。

- ・ 運転免許証
- ・ パスポート（旅券）
- ・ 在留カード
- ・ 特別永住者証明書

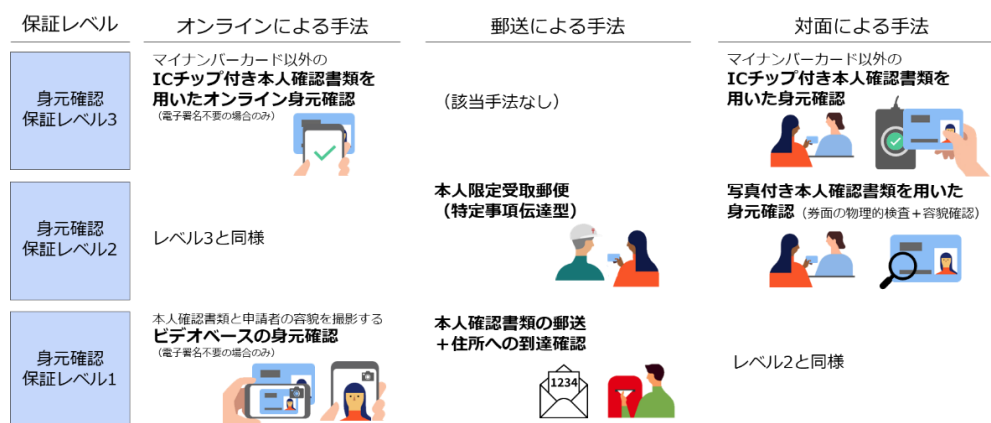
なお、対象手続に求められる保証レベルを満たさない代替手法を採用せざるを得ない場合には、当該手法によって想定されるリスクを特定し、当該リスクを低減するための補完的対策を併せて検討する必要がある点に留意してください。

身元確認保証レベル別の主要な代替手法の例を以下の図に示します。代替手法において利用可能な本人確認書類については、「別紙1 身元確認手法の具体例」の「2 主要な本人確認書類の具体例」を参考としてください。

²³ マイナンバーカードを用いた身元確認手法における留意事項については「別紙1 身元確認手法の具体例」を参考としてください。

²⁴ 「基本的な考え方」に関する解説は、本解説書の「2.4 「基本的な考え方」について」も参考としてください。

図 4-3 身元確認保証レベル別の主要な代替手法



※上記は代表的な手法の一例である。これら以外の手法であっても各保証レベルの対策基準を満たす手法であれば採用可能。

3) 実装モデルと実現手段の検討

前述までの検討結果を踏まえ、マイナンバーカードによる手法、マイナンバーカード以外による手法のそれぞれについて、情報システムの実装モデル及びその他の実現手段を検討します。

ア システムの実装モデルの検討

実装モデルは、ガイドライン本編に記載のあるとおり「連携モデル」を第一候補として検討します。採用しようとする手法に対応した適切なIDプロバイダが政府内や自省庁内に存在するかどうかを確認し、該当するIDプロバイダが存在する場合には、その利用是非を検討してください。

また、単独では条件を満たすIDプロバイダがない場合でも、「連携モデル」と「非連携モデル」を組み合わせることでの実現可能性を検討してください。例えば、IDプロバイダから入手できる情報では身元確認のための情報が不足する場合でも、「非連携モデル」によって独自に属性を追加収集するといった構成は、部分的ではあるものの「連携モデル」のメリットを享受できるため、採用の検討余地があります。

なお、適切なIDプロバイダが全くなく、全ての身元確認プロセスを「非連携モデル」として実装する場合においては、独自開発はコスト面で不利となるだけでなく脆弱性を生むリスクも高まるため原則として避け、既存の製品、サービス、OSS等の活用を検討してください。

イ その他の実現手段の検討

身元確認を実現するために必要となる、システム以外の構成要素についての実現手段を検討します。例えば、対面での身元確認を行う場合、身元確認

に必要な環境、機器、設備等（例えば窓口の端末やICカードリーダー等）についても検討が必要です。

また、「本人確認書類の物理的検査」等、人手による検証手法を採用する場合には、身元確認を適切に実施するための環境整備、身元確認担当者に対する訓練、マニュアルの整備等についても検討が必要となる点に留意してください。

参考情報：身元確認の環境整備や担当者への訓練等について

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

上記のような身元確認手法を採用する場合は、その実施条件について事前に検討を行うことが必要です。参考情報として、主な考慮事項を以下に示します。

身元確認の実施環境：

- ・ 身元確認を行う場所は、屋内か、屋外か
- ・ 本人確認書類の目視検査や申請者の容貌確認を行うために、十分な明るさを確保できる環境であるか
- ・ 本人確認書類の検証には、どのような道具を利用できるか
（例：ルーペ、偽造対策インキを確認するためのブラックライト、比較のための見本、機械的な検証を行うための真贋判定機 等）
- ・ 申請者1人あたりの身元確認に費やせる時間はどれくらいか

身元確認の実施条件：

- ・ どのような本人確認書類を利用可能とするか（本人確認書類によって、検証に利用できる券面の偽造対策技術等が異なる）
- ・ 本人確認書類を申請者から一時的に預かって検査することができるか、それとも申請者が手に保持した状態で検査しなければならないか
- ・ 容貌確認において、申請者にマスクや帽子、サングラス等の着脱の指示を行うことができるか

訓練やマニュアルの整備等：

- ・ 身元確認の実施担当者に対する訓練は行われているか
- ・ 身元確認に関するマニュアルの整備や周知は行われているか

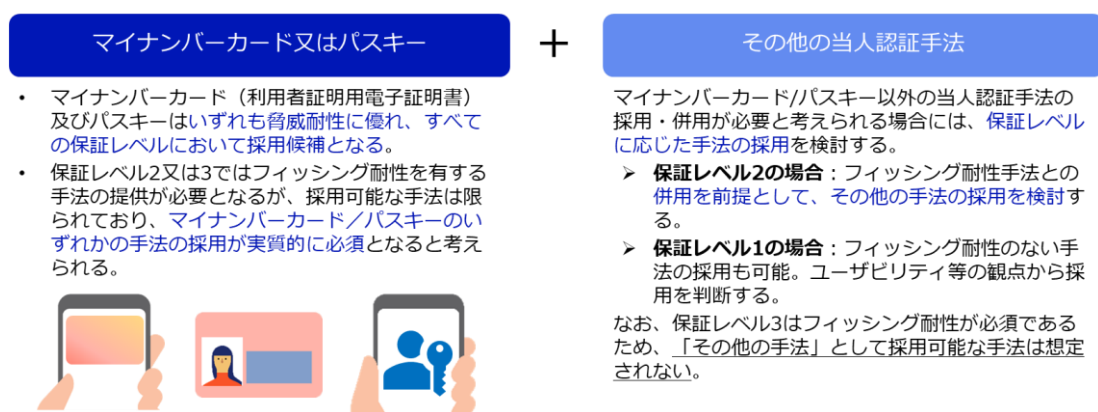
4.4 当人認証手法の選定の考え方（本編4.2関連）

本節では、当人認証手法の選定に当たって多くのケースに共通すると考えられる検討の流れと考え方を示します。

当人認証に関する昨今の技術動向や脅威動向、利用者側に必要となる環境（PC やスマートフォン等）の普及率等を踏まえると、まずはマイナンバーカード又はパスキーのいずれかの採用を検討することが、多くのケースにおいて基本的な流れとなると考えられます。

その上で、対象手続の事業目的の遂行や公平性等の観点からマイナンバーカード又はパスキー以外の当人認証手段が必要と判断される場合には、対象手続に求められる保証レベルに応じたその他の手法の併用を検討します。

図 4-4 当人認証手法の基本的な考え方



1) マイナンバーカード又はパスキーの採用検討

マイナンバーカード（利用者証明用電子証明書）及びパスキーは、いずれも脅威耐性に優れる方式であり、すべての保証レベルにおいて採用の候補として検討することができます。

なお、特に当人認証保証レベル2以上においてはフィッシング耐性を有する手法の提供が必要となりますが、本解説書の執筆時点（2026年2月時点）においてフィッシング耐性を有する手法は限られており、マイナンバーカード又はパスキーのいずれかの採用は実質的に必須となると想定されます。

ア マイナンバーカード（利用者証明用電子証明書）の採用検討

マイナンバーカードの利用者証明用電子証明書は、適切に実装することでフィッシングを含む幅広い脅威への耐性をもつ当人認証を実現できます。

また、スマートフォン用の利用者証明用電子証明書（移動端末設備用利用

者証明用電子証明書) を利用可能とすることができればユーザビリティも確保できるため、いずれの保証レベルにおいても採用候補として検討できます。

マイナンバーカード(利用者証明用電子証明書)の詳細については、「別紙2 当人認証手法の具体例」を参照してください。

イ パスキーの採用検討

パスキーは、フィッシングを含む幅広い脅威への耐性をもち、ユーザビリティについても従来手法より優位とされる手法であるため、いずれの保証レベルでも採用候補として検討できます。

対応するスマートフォン等のデバイスを所持していれば、マイナンバーカードを保有していない方でも利用できるため、対象手続が想定する利用者層に依りて採用を検討することが望まれます。また、マイナンバーカードとの併用についてもアカウント回復の観点で検討余地があります。

パスキーの詳細については、「別紙2 当人認証手法の具体例」を参照してください。

2) その他の当人認証手法の採用検討

マイナンバーカード又はパスキーの採用検討結果と採用に当たる留意事項²⁵を踏まえつつ、対象手続における事業目的の遂行や公平性等の観点から、その他の当人認証手法の要否を検討します。その他の当人認証手法の採用又は併用が必要と考えられる場合には、対象手続に求められる当人認証保証レベルに応じた手法の採用を検討します。

ア 当人認証保証レベル3の場合

当人認証保証レベル3の場合では、全ての利用者がフィッシング耐性を有する手法を用いることが対策基準として求められます。したがって、フィッシング耐性を有さない「その他の手法」を採用することはできません。

イ 当人認証保証レベル2の場合

パスワード認証+ワンタイムパスワード認証の組み合わせによる多要素認証が候補として考えられます。

ただし、当人認証保証レベル2においては、少なくとも一つのフィッシング耐性を有する手法を提供することが必要となるため、マイナンバーカード又はパスキーが手法として採用されていることが前提となります。パスワー

²⁵ マイナンバーカード又はパスキーを用いた当人認証手法における留意事項については、「別紙2 当人認証手法の具体例」を参考としてください。

ド認証+ワンタイムパスワード認証の組み合わせのような、フィッシング耐性を有さない手法だけを利用可能としても、当人認証保証レベル 2 の対策基準は満たせないことに留意が必要です。

ウ 当人認証保証レベル 1 の場合

ワンタイムパスワードを電子メールによって送信する手法等が候補として考えられます。

当人認証保証レベル 1 の場合はマイナンバーカード又はパスキーを採用せず、フィッシング耐性のない手法のみを提供することも可能です。

3) 実装モデルと実現手段の検討

前述までの検討結果を踏まえ、採用する当人認証手法を実現するための情報システムの実装モデル及びその他の実現手段を検討します。

ア システムの実装モデルの検討

前述までの検討結果を踏まえ、当人認証手法の実装モデルを検討します。実装モデルは、ガイドライン本編に記載のあるとおり「連携モデル」を第一候補として検討します。採用しようとする手法に対応した適切な ID プロバイダが政府内や自省庁内に存在するかどうかを確認し、該当する ID プロバイダが存在する場合には、その利用是非を検討してください²⁶。

適切な ID プロバイダがなく「非連携モデル」によって当人認証機能を実装する場合においても、独自開発はコスト面で不利となるだけでなく脆弱性を生むリスクも高まるため原則として避け、既存の製品、サービス、OSS 等の活用を検討してください。

イ その他の実現手段の検討

当人認証を実現するために必要となる、システム以外の構成要素についての実現手段を検討します。例えば、TOTP 方式のワンタイムパスワードを採用する場合には、利用可能とするワンタイムパスワード生成用アプリ等が利用者側の環境に必要となります。

また、対面での当人認証を行う場合は、当人認証に必要な環境、機器、設備等（例えば窓口の端末、IC カードリーダー等）についても検討します。

²⁶ 当人認証への利用を検討できる ID プロバイダの一例として、デジタル庁が提供する「デジタル認証アプリ」があります。詳しくは以下の Web サイトを確認してください。
デジタル認証アプリ Web サイト: <https://services.digital.go.jp/auth-and-sign/>

4.5 継続的な評価と改善（本編4.3関連）

前述までの手順によって検討し、採用した本人確認手法が意図どおりに機能しているかどうかは、実際の利用状況を測定しないと確認できません。また、本人確認に関する脅威は日々進歩しているため、採用時には大きな懸念のなかった手法であっても、運用期間中の脅威動向の変化によって脆弱性が浮き彫りとなる場合もあります。したがって、採用した本人確認手法については継続的な評価を行い、必要に応じて改善を行うことが求められます。

継続的な評価と改善において重要な点の一つが、「本人確認手法を評価するために、どのような情報を収集・蓄積し、評価指標とすべきなのか」という点です。これは、採用する本人確認手法や、身元確認において利用可能とする本人確認書類によっても異なります。

評価指標の具体例としては、例えば次のような情報が考えられます。これらの情報は、情報システムの設計に組み込まないと収集が難しいものも多いため、継続的な評価と改善のための手段については、要件定義時点において検討・明確化した上でシステムを調達・構築することが必要です。

なお、これらの情報を継続的に収集し、適切な評価を行うための実装には相応の専門性が求められます。こうした観点からも、できる限り「連携モデル」を採用し、専門的な評価と改善の運用についてもIDプロバイダとの連携によって実施することが望まれます。

表 4-4 身元確認に関する評価指標の例

No.	評価指標の例	概要
1	身元確認の完了率 身元確認の失敗発生率 身元確認の離脱率	<ul style="list-style-type: none">申請者が身元確認プロセスを開始してから最後まで完了できた割合身元確認プロセスにおいて検証の失敗が発生した割合身元確認プロセスを最後まで完了できず申請者が途中離脱した割合
2	身元確認の失敗原因	<ul style="list-style-type: none">身元確認が失敗したプロセス、失敗の原因等の記録
3	身元確認完了までの時間	<ul style="list-style-type: none">身元確認プロセスの平均完了時間
4	本人確認書類の利用率	<ul style="list-style-type: none">複数の本人確認書類を利用可能な場合、申請者がどの本人確認書類を用いて身元

		確認を行ったかの割合
5	身元確認手法の利用率	・ 複数の身元確認手法を併用する場合、申請者がどの手法によって身元確認を行ったかの割合
6	身元確認に関する問い合わせ履歴	・ 身元確認に関する問い合わせ件数、その内容、対応結果等

表 4-5 当人認証に関する評価指標の例

No.	評価指標の例	概要
1	当人認証の成功率 当人認証の失敗率	・ 利用者が当人認証に成功した割合 ・ 利用者が当人認証に失敗した（認証エラーとなった）割合
2	当人認証手法の登録率／利用率	・ 複数の当人認証手法を併用する場合、利用者がどの手法を登録しており、実際にどの手法を用いて当人認証を行ったかの割合
3	当人認証に関する問い合わせ履歴	・ 当人認証に関する問い合わせ件数、その内容、対応結果等

5 その他の参考情報

ガイドライン本編に関連するその他の参考情報を本章に掲載します。

参考情報：段階的な身元確認について

ガイドライン本編では、本人確認を次の三つの要素で構成すると定義しています。一つ目は「身元確認」です。これは申請者を一意に識別するとともに、その実在性を確認するプロセスで、申請者の属性情報を収集し、その真正性を本人確認書類により検証することで実現され、同時にシステムを利用するうえで必要な利用者の属性を収集します。二つ目は「本人認証」です。身元確認済みの本人が再度システムにアクセスする際に、本当にその人であることを確認するプロセスで、申請者と紐づけて登録した認証器（パスワードやパスキー、スマートフォンアプリ等）を用いて実現されます。三つ目は「フェデレーション」で、身元確認や本人認証を信頼できる ID プロバイダと連携して実現する仕組みです。

標準的な流れは、まず公的証明書などを利用して（フェデレーションを利用する、併用することも可能です）必要な属性をすべて収集し、それを確認することで身元確認を実施し、確認が完了したらその人に ID を発行、同時にパスワード、パスキーなどの認証関連情報を登録するというものです。この方法は、すべての ID の身元確認保証レベルが統一されているため、システムの構築が容易であるという利点があります。

一方、コンシューマ向けサービスでは、「段階的な身元確認（Credential first flow 等と呼ばれます）」という方法が広く採用されています。この方式では、例えば、まずメールアドレスを入力し、その到達確認が完了した時点で ID と認証器を発行し、サービス利用を開始します。この時点では申請者が当該メールアドレスへのアクセスが可能であるということを確認しているのみであり、身元確認はほとんど行われていません。そして必要に応じて、段階的に詳細な身元確認を実施していくのです。例えば、補助金申請サイトで現在有効な補助金の一覧を検索するだけなら詳細な身元確認は不要ですが、実際に補助金を申請する際には追加の身元確認を求めるといった使い方です。

この方式には2つのメリットがあります。一つ目は、利用者が煩雑な身元確認の手続なしにすぐサービスを使い始められることです。例えば、簡易な身元確認により、自分が利用可能な補助金が存在するのかが確認でき、利用可能な補助金が存在しない場合はそこでシステム利用を取りやめることができます。補助金申請が必要になって初めて、より正確な身元確

認を行うこととなります。二つ目がセキュリティの向上です。一般的な会員登録の流れではサービス提供に必要な身元確認とシンプルな認証器（典型例：パスワード）を先に登録します。つまり、多要素認証に必要な強力な認証器の登録は後から追加で実施するため、それまでの間にアカウントの乗っ取りのリスクが相対的に高い状態のままとなってしまいます。一方、身元確認の手間を減らす代わりに最初に「強力な」認証器を登録してもらうことで、アカウント乗っ取りのリスクを減じた状態でサービスを利用できるわけです。

ただし、段階的な身元確認アプローチには重要な注意点があります。それは各 ID について、どのレベルの身元確認が完了しているかを記録し、そのレベルに応じて「できること/利用できるサービス」を制限する必要があるということです。例えば、身元確認がほとんど行われていない段階の利用者には利用可能な手続の閲覧、検索のみを許可し、IAL2 相当の利用者には手続の申請を許可するといった形です。この制御が適切に行われないと、アクセス制御の不備に起因する業務上の問題となりえます。

段階的な身元確認は、ログインした利用者の身元確認レベルが異なるため、身元確認レベルに応じた適切なアクセス制御が必要である代わりに、利用者の利便性を高め、アカウント乗っ取りに対する強力なセキュリティ対策になります。サービスの性質によっては採用を検討してみても良いでしょう。

参考情報：法人に対する本人確認について

ガイドライン本編別紙2では法人に対する本人確認方法を例示しています。その範囲は①法人等の実在性確認、②申請等の手続を行う代表者等の個人としての身元確認、③法人等と申請者個人との紐づきの確認、の3つです。一方、留意事項として「法人の事業内容の確認、事業実態の確認、実質的支配者の確認、コンプライアンス面の確認」などを含んでいない旨を記載しています。これは法人の本人確認はその意味するところ、範囲が目的に応じて多岐にわたるものであり、画一的な記載が難しいためです。

自然人の本人確認と比べて法人の本人確認が根本的に異なる点は、確認すべき対象が二層構造になっている点です。まず、取引相手となる「法人」という法人格を持つ組織体そのものを確認する必要があります。これは登記簿謄本などの公的証明書による法的実在性の確認が基本です。しかし、法人は自ら行動することができず、実際には代表者、従業員、業務委託先の社員といった立場の自然人が法人を代表・代理して行動します。これらの自然人と法人との関係性（在籍確認、権限確認）と、自然人そのものの本人確認の両方が必要となります。

さらに、法人という組織の確認についても、目的によって確認すべき内容が大きく異なります。具体的には、例示した法人登記の有無と内容、代表者といった法的実在性の確認に加え、反社会的勢力との関係性チェック（反社チェック）、制裁リスト該当性の確認、マネーロンダリング・テロ資金供与リスクの評価といったコンプライアンス関連の確認も存在します。さらに、実際に事業活動を行っているか、事業所が実在するか等の事業実態の確認、そして財務状況、支払能力といった経営の健全性・安全性の確認も含まれることがあります。

これら多様な観点での確認が求められる背景は二つに分類されます。一つは法令による要求で、犯罪収益移転防止法や各種業法での規制などがあります。法令要求の場合、確認すべき項目や方法が明確に定められています。もう一つは行政上のリスク管理で、補助金交付における政策効果の判断、許認可における事業遂行能力の確認、入札参加資格審査などがこれに該当します。この場合、各行政機関は法令の範囲内において、透明性・公平性・説明責任を確保したうえで、政策目的や事案の性質に応じて確認の内容・深さを決定します。

また、自然人と法人の関係についても、ガイドライン本編で例示した自然人が法人の代表権を持つか否かの確認以外に、自然人が法人に雇用され

ているか、自然人が法人において特定の業務、手続などを実行する権限を保有するか、法人と契約する別の自然人がその契約においてどの範囲で法人の業務を代理して実施するか等その確認は広範囲にわたります。

このように法人の本人確認は、自然人の本人確認に比べて本質的に複雑です。法人そのものと法人に紐づく自然人の両方を確認する二層構造であること、法的実在性、コンプライアンス、事業実態確認、事業遂行能力など確認内容が目的によって異なることについて理解することが重要です。

別紙1 身元確認手法の具体例

本別紙では、身元確認手法の選定時の参考情報として、主要な身元確認手法の概要、脅威耐性、採用時の留意事項について解説します。

また、身元確認において重要な要素となる本人確認書類についても、主要な本人確認書類の概要や留意点を解説します。

1 主要な身元確認手法の解説

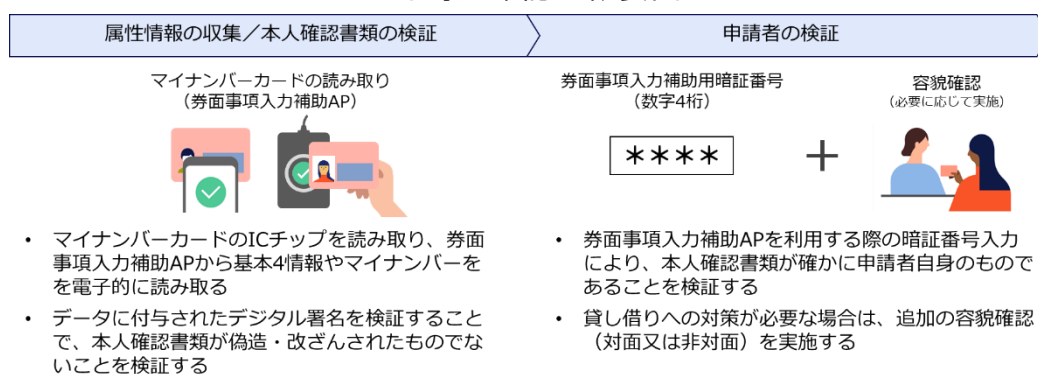
1.1 マイナンバーカードによる身元確認手法

1) 実物のマイナンバーカード（券面事項入力補助 AP）

ア 手法の概要

マイナンバーカードの「券面事項入力補助 AP」は、カードの券面に記載されている事項（マイナンバー及び基本4情報）を電子データとして読み取ることができる機能です。これを適切に用いることで、身元確認保証レベル3の身元確認を実現することができます。

図 1-1 実物のマイナンバーカード（券面事項入力補助 AP）による身元確認の概要図



イ 脅威耐性と留意事項

a) 重複登録／別人との誤紐づけ

- ・ 属性情報を電子データとして読み取ることで、誤記や表記揺れ等を防ぎ、属性情報を正確に収集できます。ただし、取り扱うシステムにおける文字コードや異体字・外字の整合等についての留意が必要です。

- ・ 個人番号取扱事務においては、マイナンバーを取得して利用することが可能です。
- b) **本人確認書類の偽造・改ざん**
 - ・ 券面事項入力補助 AP から取得したデータに付与されたデジタル署名を検証することで、それが偽造・改ざんされたものでないことを暗号学的な強度で検証することが可能です。
- c) **本人確認書類の複製**
 - ・ マイナンバーカードの IC チップが有する耐タンパ性により、電子的な複製への耐性を備えます。
- d) **本人確認書類の盗用**
 - ・ 券面事項入力補助用暗証番号（数字 4 桁）の入力をもって、本人確認書類が盗用されたものではなく、確かに申請者自身のものであることを検証できます。
 - ・ ただし、照合番号 A や照合番号 B は券面から読み取れる番号であり「申請者の検証」としては機能しないため、容貌確認等の別の手法を組み合わせる必要がある点に留意してください。
- e) **本人確認書類の貸し借り**
 - ・ 暗証番号とともにマイナンバーカードの貸し借りが行われた場合は検知できません。貸し借りの検知が必要な場合は、対面又は非対面による容貌確認を追加実施する必要があります。

ウ 採用に当たる考慮事項

- a) **事業目的の遂行／公平性に関する考慮事項**
 - ・ 採用に当たっては、マイナンバーカードを保有していない方、暗証番号を覚えていない方、紛失中の方等の存在の考慮が必要です。

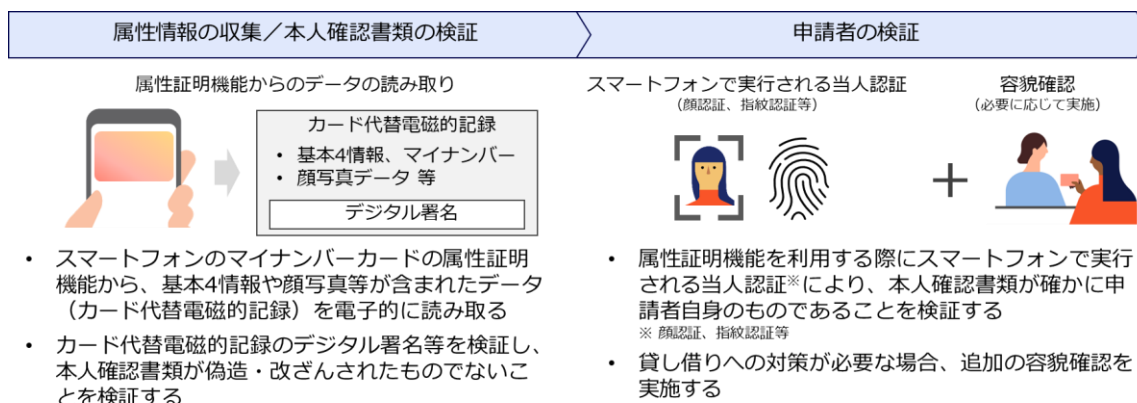
2) スマートフォンのマイナンバーカード（属性証明機能）

ア 手法の概要

スマートフォンに搭載されたマイナンバーカード機能のうち「属性証明機能」は、実物のマイナンバーカードの券面に記載された基本4情報、マイナンバー、顔写真等を「カード代替電磁的記録」としてスマートフォンに格納し、申請等において電子的に提出できる機能です。

実物のマイナンバーカードにおける「券面事項入力補助 AP」に相当し、これを適切に用いることで、身元確認保証レベル3の身元確認を実現できます。

図 1-2 スマートフォンのマイナンバーカード（属性証明機能）による身元確認の概要図



イ 脅威耐性と留意事項

a) 重複登録/別人との誤紐づけ

- 属性情報を電子データとして読み取ることで、誤記や表記揺れ等を防ぎ、属性情報を正確に収集できます。ただし、取り扱うシステムにおける文字コードや異体字・外字の整合等についての留意が必要です。
- 個人番号取扱事務においては、マイナンバーを取得して利用することが可能です。

b) 本人確認書類の偽造・改ざん

- カード代替電磁的記録に付与されたデジタル署名を検証することで、それが偽造・改ざんされたものでないことを暗号的な強度で検証することが可能です。

c) **本人確認書類の複製**

- ・ カード代替電磁的記録はスマートフォンの安全な領域に格納され、電子的な複製攻撃への耐性を備えます。
- ・ カード代替電磁的記録は、1枚の実物のマイナンバーカードに対して1台のスマートフォンにしか登録できないよう、重複登録を防止する措置が講じられています。

d) **本人確認書類の盗用**

- ・ カード代替電磁的記録の利用時には、スマートフォン側において生体認証等による本人認証が実行されることで、当該スマートフォンが盗用されたものではなく申請者自身のものであることを検証します。

e) **本人確認書類の貸し借り**

- ・ 他人のスマートフォンに対して意図的にカード代替電磁的記録を不正発行するような行為が行われる可能性についての考慮が必要です。

ウ **その他の考慮事項**

a) **事業目的の遂行／公平性に関する考慮事項**

- ・ 採用に当たっては、マイナンバーカードやスマートフォンを保有していない方、紛失中の方等の存在の考慮が必要です。
- ・ カード代替電磁的記録を搭載可能なスマートフォン²⁷を有していることが前提となるため、これらを有していない方への考慮が必要です。

b) **プライバシーに関する考慮事項**

- ・ 属性証明機能は、カード代替電磁的記録に含まれる属性情報のうち一部の属性のみを選択的に提示する機能を備えます。この機能を活用し、対象手続に必要な属性のみを収集することを検討してください。

²⁷ 属性証明機能に対応したスマートフォンについては、検討時点の最新情報を確認してください。なお、2026年2月時点において属性証明機能はiPhoneのみ対応しており、Androidについては「2026年秋頃」の提供開始を予定しています（参考1）。また、iPhoneの具体的な対応端末は「iPhone XS以降でiOS 18.5以上を搭載した端末」（参考2）となっています。

- ・ 参考1：デジタル庁Webサイト「2026年秋頃に「Androidのマイナンバーカード」へ刷新します」（<https://services.digital.go.jp/mynumbercard-android/news/0cfe138d7fb5927e4dc6d/>）

- ・ 参考2：マイナポータル よくあるご質問「使用しているiPhoneがiPhoneのマイナンバーカードに対応しているかわかりません。どうしたらよいですか。」（<https://faq.myna.go.jp/faq/show/11995>）

c) **アクセシビリティ及びユーザビリティに関する考慮事項**

- ・ 実物のマイナンバーカードの券面事項入力補助 AP と比較すると、カードの読み取りが必要ない点、暗証番号の入力を生体認証等で代替できる点において優位な手法となります。例えば、実物のマイナンバーカードでは、カードの表裏・上下の判別やスマホを重ねる位置の確認を非視覚的に行うことが難しかったり、上肢に障害があると困難だったりすることがありますが、カードの読み取りが必要なくなることで、こうした点を解消できる場合があります。

d) **セキュリティに関する考慮事項**

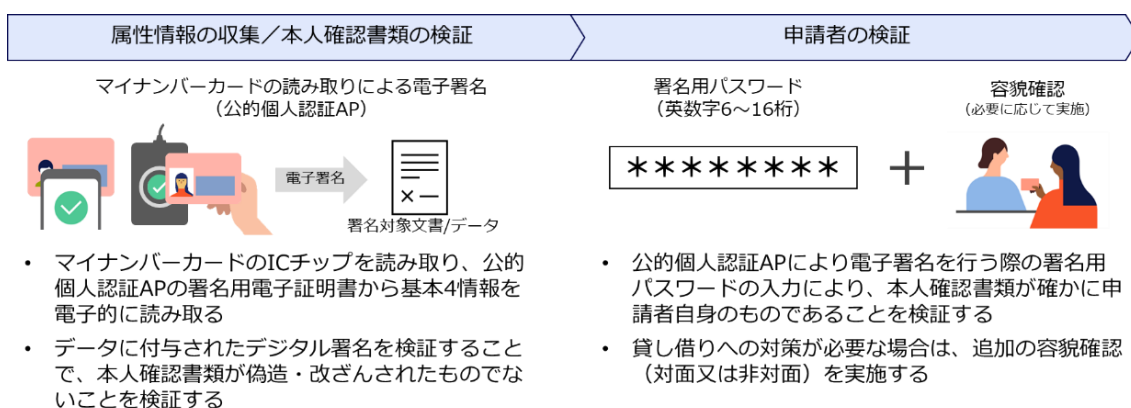
- ・ カード代替電磁的記録に含まれる顔写真データを用いて容貌確認を実施しようとする場合、当該顔写真データの仕様（解像度やグレースケールであること等）が必要な水準を満たしているかどうかを留意してください。

3) 実物のマイナンバーカード（署名用電子証明書）

ア 手法の概要

マイナンバーカードの公的個人認証APによって電子署名を行う場合、署名用電子証明書内の基本4情報をデータとして電子的に読み取ることができます。これを適切に用いることで、身元確認保証レベル3の身元確認を実現することができます。

図 1-3 実物のマイナンバーカード（署名用電子証明書）による身元確認の概要図



イ 脅威耐性と留意事項

a) 重複登録/別人との誤紐づけ

- 属性情報を電子データとして読み取ることで、誤記や表記揺れ等を防ぎ、属性情報を正確に収集できます。ただし、取り扱うシステムにおける文字コードや異体字・外字の整合等についての留意が必要です。
- 署名用電子証明書は転出等により失効するため、身元確認の直前に行われた転居等を検知できます。

b) 本人確認書類の偽造・改ざん

- 署名用電子証明書に付与された発行元のデジタル署名を検証することで、それが偽造・改ざんされたものでないことを暗号的な強度で検証できます。

c) 本人確認書類の複製

- マイナンバーカードのICチップが有する耐タンパ性により、電子的な

複製への耐性を備えます。

d) 本人確認書類の盗用

- ・ 署名用パスワードの入力をもって、本人確認書類が盗用されたものではなく、確かに申請者自身のものであることを検証できます。
- ・ マイナンバーカードの紛失の届け出がマイナンバー総合フリーダイヤルにされた場合は、署名用電子証明書の失効がなされるため、仮に署名用パスワードと一緒にマイナンバーカードが盗用されても紛失の届け出が即座に行われれば署名用電子証明書の失効確認で盗用を検知することができます。

e) 本人確認書類の貸し借り

- ・ 署名用パスワードとともにマイナンバーカードの貸し借りが行われた場合は検知できません。貸し借りの検知が必要な場合は、対面又は非対面による容貌確認を追加実施する必要があります。

ウ その他の考慮事項

a) 事業目的の遂行／公平性に関する考慮事項

- ・ 採用に当たっては、マイナンバーカードを保有していない方、暗証番号を覚えていない方、マイナンバーカードに電子証明書を搭載されていない方²⁸、紛失中の方等の存在の考慮が必要です。
- ・ 署名用電子証明書は転出等により失効するため、転出直後の方はこの手法を一時的に利用できなくなる点に留意が必要です。

b) その他の考慮事項

- ・ この機能の取扱いは、公的個人認証法に基づく必要があります。
- ・ 電子署名を行う際には、以下のような点に留意が必要です。
 - － 利用者が電子署名を行う前に、どのような情報に対して当該電子署名を行うのかを明らかにする。
 - － 署名用パスワードの入力によって電子署名が行われること自体やその意義について明らかにする。
- ・ この機能は電子署名を目的とした機能であるため、対象手続が電子署

²⁸ マイナンバーカードの電子証明書は、15歳未満の方には原則として発行されません。また、マイナンバーカードの交付申請時に「電子証明書を不要」として申請を行った場合にも、電子証明書は搭載されません。

名を必要としない場合においては、券面事項入力補助 AP 等他の機能の利用を検討すべきです。

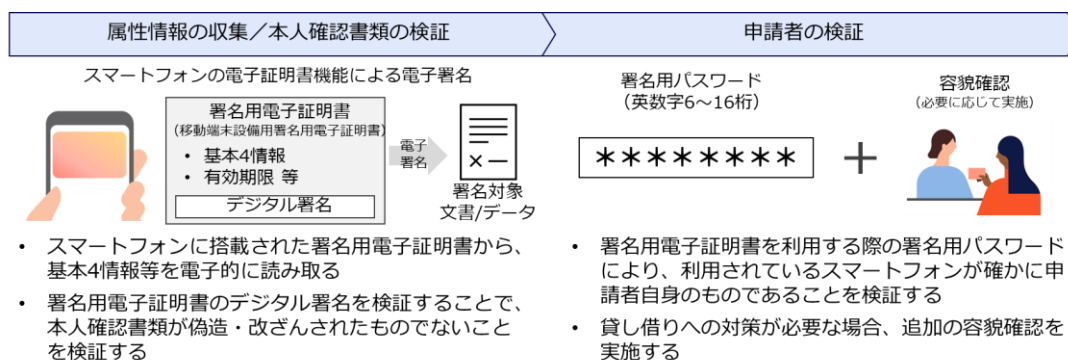
4) スマートフォンのマイナンバーカード（署名用電子証明書）

ア 手法の概要

スマートフォンに搭載されたマイナンバーカード機能のうち「電子証明書機能」では、スマートフォン用の署名用電子証明書（移動端末設備用署名用電子証明書）をスマートフォンに格納し、電子署名を行うことができます。

実物のマイナンバーカードにおける「署名用電子証明書」に相当し、これを適切に用いることで、身元確認保証レベル3の身元確認を実現できます。

図 1-4 スマートフォンのマイナンバーカード（署名用電子証明書）による身元確認の概要図



イ 脅威耐性と留意事項

a) 重複登録／別人との誤紐づけ

- 属性情報を電子データとして読み取ることで、誤記や表記揺れ等を防ぎ、属性情報を正確に収集できます。ただし、取り扱うシステムにおける文字コードや異体字・外字の整合等についての留意が必要です。
- 署名用電子証明書は転出等により失効するため、身元確認の直前に行われた転居等を検知できます。

b) 本人確認書類の偽造・改ざん

- 移動端末設備用署名用電子証明書に付与された発行元のデジタル署名を検証することで、それが偽造・改ざんされたものでないことを暗号的な強度で検証できます。

c) 本人確認書類の複製

- 移動端末設備用署名用電子証明書はスマートフォンの安全な領域に格

納され、電子的な複製攻撃への耐性を備えます。

- ・ 移動端末設備用署名用電子証明書は、1枚の実物のマイナンバーカードに対して1台のスマートフォンにしか登録できないよう、重複登録を防止する措置が講じられています。

d) 本人確認書類の盗用

- ・ 移動端末設備用署名用電子証明書の利用時には署名用パスワードによる本人認証を行うことで、当該スマートフォンが盗用されたものではなく申請者自身のものであることを検証します。

e) 本人確認書類の貸し借り

- ・ 署名用パスワードとともにスマートフォンの貸し借りが行われた場合は検知できません。貸し借りの検知が必要な場合は、対面又は非対面による容貌確認を追加実施する必要があります。
- ・ 他人のスマートフォンに対して意図的に移動端末設備用署名用電子証明書を不正発行するような行為が行われる可能性についての考慮が必要です。

ウ その他の考慮事項

a) 事業目的の遂行／公平性に関する考慮事項

- ・ 採用に当たっては、マイナンバーカードを保有していない方、暗証番号を覚えていない方、マイナンバーカードに電子証明書を搭載されていない方²⁹、紛失中の方等の存在の考慮が必要です。
- ・ 移動端末設備用署名用電子証明書は転出等により失効するため、転出直後の方はこの手法を一時的に利用できなくなる点に留意が必要です。
- ・ 移動端末設備用署名用電子証明書を搭載可能なスマートフォンを有していることが前提となるため、これらを有していない方への考慮が必要です。

b) その他の考慮事項

- ・ この機能の取扱いは、公的個人認証法に基づく必要があります。
- ・ 電子署名を行う際には、以下のような点に留意が必要です。

²⁹ マイナンバーカードの電子証明書は、15歳未満の方には原則として発行されません。また、マイナンバーカードの交付申請時に「電子証明書を不要」として申請を行った場合にも、電子証明書は搭載されません。

- 利用者が電子署名を行う前に、どのような情報に対して当該電子署名を行うのかを明らかにする。
- 署名用パスワードの入力によって電子署名が行われること自体やその意義について明らかにする。
- ・ この機能は電子署名を目的とした機能であるため、対象手続が電子署名を必要としない場合においては、属性証明機能等他の機能の利用を検討すべきです。

1.2 マイナンバーカード以外による身元確認手法

1) IC チップ付き本人確認書類を用いた身元確認

ア 手法の概要

マイナンバーカード以外にも、①IC チップを備えており、②本人確認書類の券面の記載事項を電子データとして読み取ることができ、③デジタル署名による発行元と偽造・改ざんの検証ができる、という条件を満たす本人確認書類については、これを適切に用いることで、身元確認保証レベル 3 の身元確認を実現することができます。

上記の条件に該当する主要な本人確認書類は、本解説書の執筆時点（2026年2月時点）において以下のとおりです。

- ・ 運転免許証
- ・ パスポート（旅券）
- ・ 在留カード
- ・ 特別永住者証明書

イ 脅威耐性と留意事項

以下は、IC チップを備える本人確認書類を用いた場合の一般的な脅威耐性と留意事項です。本人確認書類の仕様によっては詳細な耐性や制約が異なる場合がある点に留意してください。

a) 重複登録／別人との誤紐づけ

- ・ 属性情報を電子データとして読み取ることで、誤記や表記揺れ等を防ぎ、属性情報を正確に収集できます。ただし、取り扱うシステムにおける文字コードや異体字・外字の整合等についての留意が必要です。

b) 本人確認書類の偽造・改ざん

- ・ 本人確認書類の IC チップから取得したデータに付与されたデジタル署名を検証することで、それが偽造・改ざんされたものでないことを暗号的な強度で検証することが可能です。なお、運転免許証については、IC チップからのデータの取得には暗証番号の入力が必要です。

c) 本人確認書類の複製

- ・ IC チップが有する耐タンパ性により、電子的な複製への耐性を備えません。

d) 本人確認書類の盗用

- ・ 顔写真を用いて対面又は非対面による容貌確認を行うことで、本人確認書類が盗用されたものではなく、確かに申請者自身のものであることを検証できます。
- ・ 運転免許証の場合は、IC チップからデータを取得する際に必要となる暗証番号等の入力によって申請者の検証を行うこともできます。

e) 本人確認書類の貸し借り

- ・ 貸し借りの検知が必要な場合は、対面又は非対面による容貌確認を実施する必要があります。

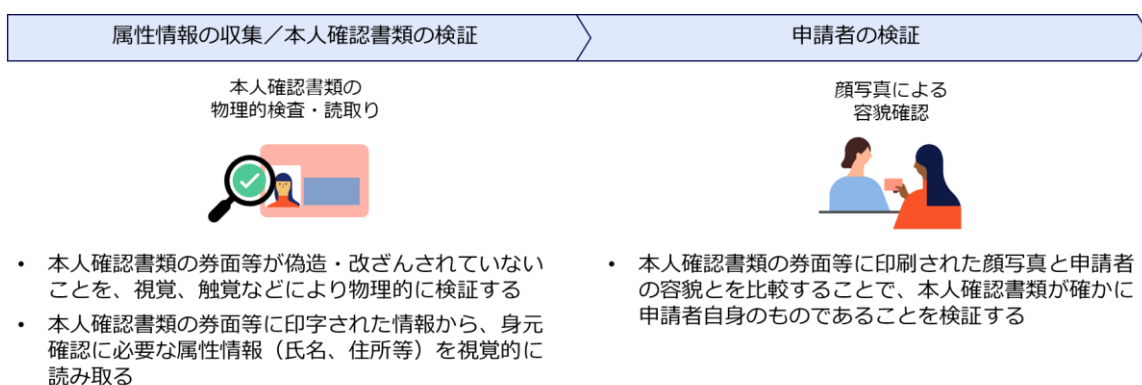
2) 顔写真付き本人確認書類を用いた身元確認（対面）

ア 手法の概要

顔写真が券面に印刷された本人確認書類は、これを適切に用いることで、身元確認保証レベル2の身元確認を実現することができます。

なお、身元確認保証レベル2を満たすためには本人確認書類が偽造・改ざんされたものでないことを物理的に検査する必要があるため、窓口等の対面環境において身元確認を行うことが前提となります。

図 1-5 顔写真付き本人確認書類による身元確認（対面）の概要図



イ 脅威耐性と留意事項

a) 重複登録／別人との誤紐づけ

- 本人確認書類に記載された属性情報を物理的に読み取る必要があるため、誤記、表記揺れ、データ入力ミス等が発生する可能性の考慮が必要です。

b) 本人確認書類の偽造・改ざん／本人確認書類の複製

- 本人確認書類の検証強度は、検査を行う環境や道具、本人確認書類が備える偽造対策技術、検査担当者の経験・技能、訓練やマニュアルの有無等、様々な要因によって左右されます。また、精巧な偽造・改ざんについては、人手での検知が難しい場合も想定されます。

c) 本人確認書類の盗用／本人確認書類の貸し借り

- 顔写真を用いて対面での容貌確認を行うことで、本人確認書類が盗用や貸し借りされたものでないことを検証できます。

ウ その他の考慮事項

a) プライバシーに関する考慮事項

- ・ 身元確認のなかで本人確認書類を撮影したりスキャンしたりする場合、当該情報が必要なくなった時点で削除を行う等、プライバシー面を考慮した運用設計を行う必要があります。

b) セキュリティに関する考慮事項

- ・ 本人確認書類の物理的検査については、偽造・改ざんリスクに応じて、検査を行うための環境、道具、利用可能とする本人確認書類の種類、検査担当者に対する訓練やマニュアル整備等を検討する必要があります。
- ・ 容貌確認についても同様に、申請者の顔と顔写真とを目視比較するポイントや、帽子・スカーフ・サングラス・マスク等の着脱指示の基準等を検討し、検査担当者に対する訓練やマニュアル整備等を検討する必要があります。なお、容貌確認に用いる顔写真は、本人確認書類によって撮影条件、解像度、撮影されてからの期間等が異なることについても留意が必要です。

参考情報：本人限定受取郵便（特定事項伝達型）による身元確認について

日本郵便が提供する「本人限定受取郵便（特定事項伝達型）」は、配達担当者が受取人に対する身元確認を行い、その結果を差出人が確認できるサービスです。

このサービス（又はこれに類するサービス）を用いた身元確認は「顔写真付き本人確認書類を用いた身元確認（対面）」の一種であると考えられますが、以下のような点についても留意が必要です。

- ・ **属性情報の収集**：配送担当者による読み取り・記入・入力が行われるため、強度としては「申請者自身による記入・入力」に相当するとみなせる。誤記入、誤入力、異体字の扱いなどについての考慮が必要。
- ・ **本人確認書類の検証**：「物理的検査（対面）」に相当するとみなせる。ただし、検証は一般に玄関先等などで行われ、検証に用いることのできる時間や道具には制約がある。また、担当者の訓練等についてもサービス側に依存するため、検証の強度を対象手続側でコントロールすることができない。

- ・ **申請者の検証**：「容貌確認（対面）」に相当するとみなせる。ただし、容貌確認の際の環境（明るさ）や実施手順（マスクの着脱を求める等）を指定することはできず、担当者の訓練等についてもサービス側に依存するため、検証の強度を対象手続側でコントロールすることができない。

なお、上記は本人確認書類から収集した情報を、差出人が確認できることを前提としています。「属性情報の収集」ができない場合は身元確認の要件を満たさず、身元確認として用いることはできない点に留意してください。

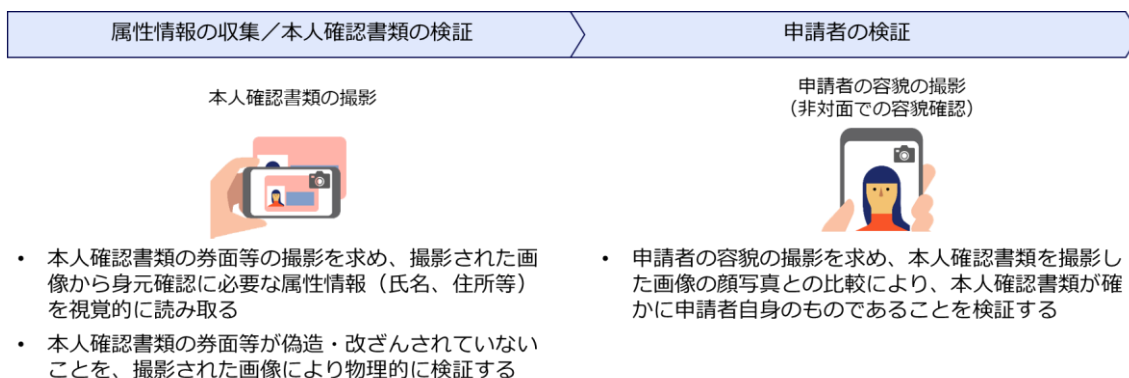
3) 顔写真付き本人確認書類を用いたビデオベースの身元確認

ア 手法の概要

スマートフォンのカメラ等を用いて、顔写真付き本人確認書類と申請者の容貌を撮影することで、非対面での身元確認を実現する手法です。身元確認保証レベル1に該当します。

ここでは一般的な手法について解説しますが、脅威耐性の詳細については、撮影の条件や枚数、動画の併用有無、画像処理による自動検証の有無、人手による検証の有無、インジェクション攻撃やプレゼンテーション攻撃への対策の有無等、様々な条件や仕様によって異なります。

図 1-6 顔写真付き本人確認書類を用いたビデオベースの身元確認の概要図



イ 脅威耐性と留意事項

a) 重複登録／別人との誤紐づけ

- 本人確認書類に記載された属性情報を物理的に読み取る必要があるため、誤記、表記揺れ、データ入力ミス等が発生する可能性の考慮が必要です。

b) 本人確認書類の偽造・改ざん／本人確認書類の複製

- 画像や映像を介した本人確認書類の検査では、精巧な偽造・改ざん・複製の検知は難しいと考えられます。
- 本人確認書類が備える偽造対策技術（特殊な印刷技術等）の多くは対面での検査を想定したものであり、画像や映像を介した場合には利用できない点にも留意が必要です。

c) **本人確認書類の盗用／本人確認書類の貸し借り**

- ・ 顔写真を用いて対面での容貌確認を行うことで、本人確認書類が盗用や貸し借りされたものでないことを検証できます。ただし、顔写真そのものが偽造・改ざんされ得る点については留意が必要です。

ウ **その他の考慮事項**

a) **プライバシーに関する考慮事項**

- ・ 身元確認のなかで本人確認書類を撮影したりスキャンしたりする場合、当該情報が必要なくなった時点で削除を行う等、プライバシー面を考慮した運用設計を行う必要があります。

b) **セキュリティに関する考慮事項**

- ・ 本人確認書類の非対面での物理的検査には限界があるため、偽造・改ざんによるリスクを考慮の上で、必要に応じて補完的対策を検討することが望まれます。
- ・ 容貌確認については、画像や映像の差し替えや改ざん等を行うインジェクション攻撃やプレゼンテーション攻撃への対策について、個別の検討が必要です。

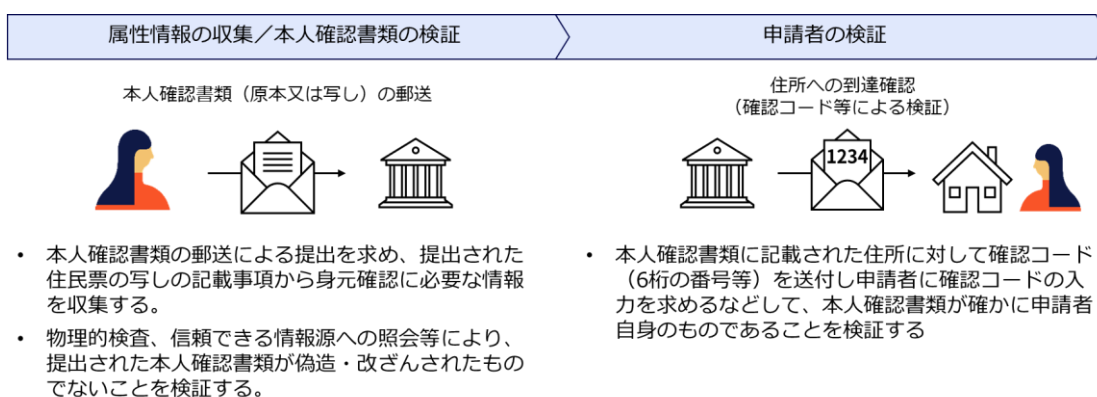
4) 本人確認書類の郵送＋住所への到達確認

ア 手法の概要

住民票の写し等の本人確認書類を郵送することによる身元確認手法は、「住所への到達確認」による申請者の検証を行うことで、身元確認保証レベル1の身元確認を実施することが可能です。

本人確認書類の郵送による提出のみでは「申請者の検証」に相当するプロセスがなく、本人確認書類の盗用や貸し借りの検知ができないため身元確認保証レベル1にも満たない点に十分留意してください。

図 1-7 本人確認書類の郵送＋住所への到達確認による身元確認の概要図



なお、上図では「属性情報の収集／本人確認書類の検証」を「申請者の検証」よりも先に実施する手順を図示していますが、申請対象者の住所等をあらかじめ把握している場合には、申請案内等を郵送するタイミングで住所への到達確認による「申請者の検証」を行い、その後に本人確認書類の郵送を受けることで「属性情報の収集／本人確認書類の検証」を実施する手順とすることも可能です。

イ 脅威耐性と留意事項

a) 重複登録／別人との誤紐づけ

- 本人確認書類に記載された属性情報を物理的に読み取る必要があるため、誤記、表記揺れ、データ入力ミス等が発生する可能性の考慮が必要です。

b) 本人確認書類の偽造・改ざん／本人確認書類の複製

- ・ 住民票の写しや戸籍謄本/抄本等、行政機関が発行した証明書そのものを提出させる場合は、対面で物理的検査を行う手法に相当する検査が可能であり、一定程度の検証が可能です。
- ・ 本人確認書類の複写物（複合機等でコピーしたもの）を郵送させる場合は、精巧な偽造・改ざん・複製の検知は難しいと考えられます。

c) 本人確認書類の盗用

- ・ 住所への到達確認を行うことにより、本人確認書類の盗用を検知できます。ただし、本人確認書類の複写物を提出させる場合には、本人確認書類に記載された住所が偽造・改ざんされる可能性に留意が必要です。

d) 本人確認書類の貸し借り

- ・ 郵送する本人確認書類が意図的に他人に譲渡・売却された場合、「住所への到達確認」を行うための確認用コード等についても同様に共有され得ると想定されるため、貸し借りは検知できません。

ウ その他の考慮事項

a) 事業目的の遂行／公平性の考慮事項

- ・ 他の手法と比較して、利用可能な本人確認書類を広く確保することが可能な手法です。

b) プライバシーに関する考慮事項

- ・ 住民票の写しや戸籍謄本/抄本の提出を求める場合、身元確認には必要のない情報が多く含まれることに留意が必要です。身元確認として収集・記録する属性の範囲を限定したり、提出を受けた書類の保管等の扱いをあらかじめ定めたりするなどの考慮が必要です。

c) セキュリティに関する考慮事項

- ・ 脅威耐性は郵送を求める本人確認書類によっても異なりますが、一般に検証強度が高い手法とは言えません。様々なリスクを考慮の上で、必要に応じて補完的対策を検討することが望まれます。

d) **その他の考慮事項**

- ・ 郵送を伴うため、身元確認の完了までには一定の日数を要します。また、申請の不備等が生じた場合には、返戻や再提出のために更に日数を要することになります。

2 主要な本人確認書類の具体例

身元確認を検討する際の参考情報として、我が国において広く流通している主要な本人確認書類の具体例を解説します。

なお、ここでは主な特徴や留意点のみを示します。各本人確認書類の記載事項や技術的仕様等の詳細については、個別に確認を行ってください。

2.1 区分A：デジタル署名を備える本人確認書類

氏名や住所等の記載事項を、デジタル署名付きのデジタルデータとして読み取ることができる本人確認書類です。身元確認に必要な情報をデータとして電子的に読み取ることができるため、目視による誤入力等を防ぐことができ、デジタル署名の検証によって偽造・改ざんに対して厳密な検証が可能です。

身元確認保証レベル3では、この区分Aの本人確認書類が必須となります。

表 2-1 区分Aに該当する主要な本人確認書類の概要

No.	名称・種別	身元確認に関連する特徴・留意事項
1	実物のマイナンバーカード	<ul style="list-style-type: none"> ・ 券面の記載事項、顔写真、公的個人認証の電子証明書等をデータとして取得可能。 ・ 暗証番号や署名用パスワードにより「申請者の検証」を同時に実施することができる。 ・ 照合番号 A 及び照合番号 B は券面から読み取れる情報であるため「申請者の検証」としては機能しない。容貌確認等を別途行う必要がある点に留意が必要。 ・ 詳細については本別紙の1章を参照。
2	スマートフォンのマイナンバーカード	<ul style="list-style-type: none"> ・ 券面の記載事項、顔写真、公的個人認証の電子証明書等をデータとして取得可能。 ・ 生体認証や署名用パスワードにより「申請者の検証」を同時に実施することができる。 ・ 詳細については本別紙の1章を参照。
3	運転免許証	<ul style="list-style-type: none"> ・ 券面の記載事項、顔写真、本籍情報（券面には記載されない）等をデータとして取得可能。 ・ 暗証番号により「申請者の検証」を同時に実施することができる。暗証番号は取得対象データに応じて2種類が存在する。
4	パスポート（旅券）	<ul style="list-style-type: none"> ・ 券面の記載事項、顔写真等をデータとして取得可能。ただし、住所は含まれない点に留意。また、

No.	名称・種別	身元確認に関連する特徴・留意事項
		<p>氏名はローマ字表記であり、漢字表記の氏名は含まれない点にも留意が必要。</p> <ul style="list-style-type: none"> データ取得に暗証番号は必要ないため、「申請者の検証」は別途実施する必要がある。
5	在留カード・特別永住者証明書	<ul style="list-style-type: none"> 券面の記載事項、顔写真等をデータとして取得可能。 データ取得に暗証番号は必要ないため、「申請者の検証」は別途実施する必要がある。 在留カード・特別永住者証明書が真正なものであることを認証するとともに、ICチップ内の情報を読み取り表示するための「在留カード等読取アプリケーション」が出入国在留管理庁により提供されている。(URL：https://www.moj.go.jp/isa/applications/procedures/rcc-support.html)

2.2 区分B：顔写真を備える本人確認書類

IC チップやデジタル署名は備えず、券面に顔写真を備える本人確認書類です。記載事項、発行プロセス、有効期限、偽造・改ざん対策等は、本人確認書類の種別や発行元によって様々である点に留意が必要です。身元確認保証レベル 2 では、この区分B又は前述の区分Aのいずれかの本人確認書類が必要です。

身元確認の際には券面の物理的検査によって偽造・改ざんの有無を検証する必要があるため、蛍光インクやホログラム印刷など、偽造・改ざんの検知に役立つ印刷技術が用いられているものを用いることが推奨されます。

表 2-2 区分Bに該当する主要な本人確認書類の概要

No.	名称・種別	身元確認に関連する特徴・留意事項
1	運転経歴証明書	<ul style="list-style-type: none"> ・ 運転免許証とは異なり、IC チップを搭載していない。 ・ 有効期限はなく生涯有効。
2	顔写真付きのその他の国家資格証（小型船舶操縦免許証 等）	<ul style="list-style-type: none"> ・ 記載事項、発行プロセス、有効期限、券面の偽造・改ざん対策の有無等は資格証の種別によって異なる。 ・ ホログラム印刷等の偽造対策を備えるものもあるが、紙の資格証にラミネート加工を施しただけの簡易なものも存在するため、身元確認における利用可否の判断は資格証の種別ごとに個別検討が必要。
3	顔写真付きの福祉手帳（身体障害者手帳、精神障害者保健福祉手帳、療育手帳）	<ul style="list-style-type: none"> ・ 記載事項、発行プロセス、有効期限、券面の偽造・改ざん対策の有無等は、福祉手帳の種別や発行元となる地方公共団体によって異なる。 ・ 顔写真の有無は発行元となる地方公共団体によって異なる。利用者が写真の有無を選択できる場合も多い。 ・ 形状は、手帳型のもの、PVC カード型のものが存在するほか、スマートフォンのアプリで表示可能としている団体も存在する。

2.3 区分C：その他の本人確認書類

区分A、区分Bのいずれにも該当しない本人確認書類又はそれに類する書類です。身元確認保証レベル1の対象手続において利用可能な場合がありますが、実際に利用可能であるかどうかは、必要な属性情報や受容可能なリスクによっても異なる点に留意が必要です。

区分A、区分Bのいずれも保有していない申請者を考慮しなければならない場合において、例外措置としての利用を検討できる場合があります。

表 2-3 区分Cに該当する主要な本人確認書類の概要

No.	名称・種別	身元確認に関連する特徴・留意事項
1	住民票の写し	<ul style="list-style-type: none">・ コンビニ交付されたものについては、けん制文字、スクランブル画像、偽造防止検出画像などの偽造・改ざん・複写等への対策が講じられている³⁰。・ コンビニ交付以外の場合は、発行元の地方公共団体によって偽造等への対策が異なる。
2	顔写真なしの福祉手帳 (身体障害者手帳、精神障害者保健福祉手帳、療育手帳)	<ul style="list-style-type: none">・ 記載事項、発行プロセス、有効期限、券面の偽造・改ざん対策の有無等は、福祉手帳の種別や発行元となる地方公共団体によって異なる。・ 形状は、手帳型のもの、PVC カード型のものが存在するほか、スマートフォンのアプリで表示可能としている団体も存在する。

³⁰ 参考：地方公共団体情報システム機構「コンビニエンスストア等における証明書等の自動交付【コンビニ交付】 | 受け取った証明書の確認」(<https://www.lg-waps.go.jp/02-01.html>)

2.4 スマートフォンに搭載された本人確認書類等の扱いについて

昨今、属性情報や資格情報などをスマートフォンに格納して利用するための技術の利活用が始まりつつあり、今後は様々な本人確認書類や証明書がスマートフォンに搭載され、身元確認においても利用可能になると想定される。

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

1) 「属性情報の収集」における考慮事項

- ・ スマートフォンに搭載された本人確認書類等から、属性情報を電子的に取得可能であるかどうか。属性情報を画面に表示するだけの場合、情報を手入力したり書き写したりする必要が生じるほか、表示内容の偽造・改ざんの検証が実施できない場合も想定される。

2) 「本人確認書類の検証」における考慮事項

- ・ スマートフォンに搭載できる本人確認書類の発行状況が管理されているかどうか。例えばスマートフォンへの発行枚数が管理・制御されていない場合、証明書を意図的に他人のスマートフォンに発行するような脅威についても考慮する必要がある。
- ・ 電子的な複製やタンパリング攻撃等への対策が講じられているか。対策が講じられていない場合、悪意を持った者による不正な複製や取出しが行われるリスクの考慮が必要となる。
- ・ スマートフォンに搭載された本人確認書類が、本来の証明書の発行元とは異なる機関から二次的に発行されたものでないか。本来の本人確認書類の発行元とは異なる組織・機関から二次的に発行されたものである場合、その証明書が法的に有効なものであるか、二次的な発行元は信頼できる組織・機関であるのか等を踏まえ、そのような本人確認書類を受け入れ可能とすべきかどうかの判断が必要である。

3) 「申請者の検証」における考慮事項

- ・ 本人確認書類の提示時に、生体認証や暗証番号入力などによる適切な本人認証が実行されているか。提示時の本人認証が行われない場合は、スマートフォンの盗用等のリスクに対して別の手段による「申請者の検証」を実施する必要がある。

別紙2 当人認証手法の具体例

本別紙では、当人認証手法の選定時の参考情報として、主要な当人認証手法の概要、脅威耐性、採用時の留意事項について解説します。

1 主要な当人認証手法の解説

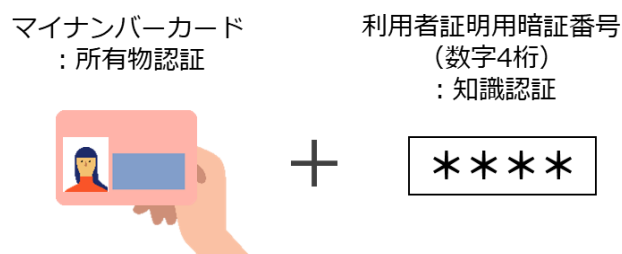
1.1 フィッシング耐性を有する当人認証手法

1) 実物のマイナンバーカード（利用者証明用電子証明書）

ア 手法の概要

マイナンバーカードの「利用者証明用電子証明書」は、Web サイト等へのログイン時において、公開鍵認証による当人認証を行うことができる機能です。実装において適切なフィッシング対策を講じることで³¹、当人認証保証レベル3の当人認証を実現できます³²。

図 1-1 実物のマイナンバーカード（利用者証明用電子証明書）による当人認証の概要図



イ 脅威耐性と留意事項

a) オンライン上でのパスワードの推測

- ・ 暗証番号による当人認証はローカルで処理されるため、オンライン上での推測攻撃を受けません。

³¹ 利用者証明用電子証明書を利用すれば無条件にフィッシング耐性をもつという訳ではありません。フィッシング耐性を確保するためには、mTLSによる相互認証やアクセス先ドメインの制限等の適切な実装が必要です。

³² マイナンバーカードの利用者証明用電子証明書には、対面等の特定の条件下において暗証番号の入力を2回目以降不要とする「かざし利用」と呼ばれる利用方法があります。この場合は単要素の所有物認証となり、当人認証保証レベル1に該当します。

- b) **盗聴・リプレイ攻撃**
 - ・ 通信の暗号化やチャレンジレスポンス等による対策が可能です。
- c) **パスワードや認証器の盗用**
 - ・ 多要素認証であるため、単一の認証要素を盗まれた場合にも耐性を有します。
 - ・ マイナンバーカードと暗証番号が同時に盗まれた場合の耐性は有しません。
- d) **フィッシング**
 - ・ mTLS による相互認証や、スマホアプリ等によるアクセス先ドメインの制限等による対策が可能です。
- e) **暗号鍵の不正な取り出し・複製**
 - ・ マイナンバーカードの IC チップが備える耐タンパ性による耐性を有します。

ウ その他の考慮事項

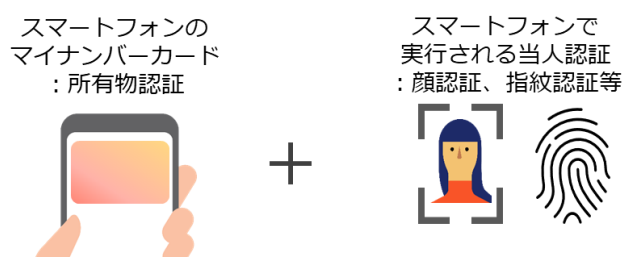
- a) **事業目的の遂行／公平性の考慮**
 - ・ 採用に当たっては、マイナンバーカードを保有していない方、暗証番号を覚えていない方、紛失中の方等の存在の考慮が必要です。
- b) **アクセシビリティ及びユーザビリティに関する考慮事項**
 - ・ ログイン時には、実物のマイナンバーカードの読み取りが必要となりますが、スマートフォンでの読み取り時にはマイナンバーカードの表裏・上下の判別やスマートフォンを重ねる位置の確認を非視覚的に行うことが難しかったり、上肢に障害があると困難だったりすることがあります。また、暗証番号を覚えていない方はログインができなくなる点についても留意が必要です。
- c) **その他の考慮事項**
 - ・ この機能の取扱いは、公的個人認証法に基づく必要があります。

2) スマートフォンのマイナンバーカード（利用者証明用電子証明書）

ア 手法の概要

スマートフォンに搭載されたマイナンバーカード機能のうち、スマートフォン用の利用者証明用電子証明書（移動端末設備用利用者証明用電子証明書）を用いることで、実物のマイナンバーカードと同じく、公開鍵認証による当人認証を行うことができます。実装において適切なフィッシング対策を講じることで、当人認証保証レベル3の当人認証を実現できます。

図 1-2 スマートフォンのマイナンバーカード（利用者証明用電子証明書）による当人認証の概要図



イ 脅威耐性と留意事項

a) オンライン上でのパスワードの推測

- ・ 暗証番号による当人認証はローカルで処理されるため、オンライン上での推測攻撃を受けません。

b) 盗聴・リプレイ攻撃

- ・ 通信の暗号化やチャレンジレスポンス等による対策が可能です。

c) パスワードや認証器の盗用

- ・ 多要素認証であるため、単一の認証要素を盗まれた場合にも耐性を有します。

d) フィッシング

- ・ mTLS による相互認証や、スマホアプリ等によるアクセス先ドメインの制限等による対策が可能です。

e) **暗号鍵の不正な取り出し・複製**

- ・ 移動端末設備用利用者証明用電子証明書はスマートフォンの安全な領域に格納され、不正な取り出しや電子的な複製攻撃への耐性を備えます。

ウ **その他の考慮事項**

a) **事業目的の遂行／公平性の考慮**

- ・ 採用に当たっては、マイナンバーカードを保有していない方、暗証番号を覚えていない方、マイナンバーカードに電子証明書を搭載されていない方³³、紛失中の方等の存在の考慮が必要です。
- ・ 移動端末設備用利用者証明用電子証明書を搭載可能なスマートフォンを有していない方への考慮も必要です。

b) **アクセシビリティ及びユーザビリティに関する考慮事項**

- ・ 実物のマイナンバーカードと比べ、カードの読み取りが必要なく、暗証番号入力についても生体認証等で代替できる点で、アクセシビリティ及びユーザビリティに優れる手法です。

c) **その他の考慮事項**

- ・ この機能の取扱いは、公的個人認証法に基づく必要があります。

³³ マイナンバーカードの電子証明書は、15歳未満の方には原則として発行されません。また、マイナンバーカードの交付申請時に「電子証明書を不要」として申請を行った場合にも、電子証明書は搭載されません。実物のマイナンバーカードに電子証明書を搭載していない場合、スマートフォン用の利用者証明用電子証明書を発行することができません。

3) パスキー

ア 手法の概要

パスキーは、FIDO 標準に基づきパスワードに代わる認証方式として普及が進められている手法です。パスキーはフィッシング耐性を有しており、かつ多要素認証として機能するため、当人認証保証レベル 3 の当人認証を実現できます。

なお、デバイス間で同期できる方式は「同期パスキー」、特定のデバイスから取り出せない方式のものは「デバイス固定パスキー」と呼ばれます。

イ 脅威耐性と留意事項

a) オンライン上でのパスワードの推測

- ・ オンライン上で推測・試行され得るパスワードのような認証要素を利用しないため、攻撃を受けません。

b) 盗聴・リプレイ攻撃

- ・ 通信の暗号化やチャレンジレスポンス等による対策が可能です。

c) パスワードや認証器の盗用

- ・ 多要素認証であるため、パスキーを格納したデバイスが盗まれた場合にも耐性を有します。
- ・ デバイスとアクティベーションに用いる暗証番号等が同時に盗まれた場合の耐性は有しません。
- ・ 同期パスキーの場合、何らかの手段によって同期に用いるアカウントを攻撃者に奪われた場合の耐性は有しません。

d) フィッシング

- ・ パスキーはドメイン名と紐付けられる仕組みとなっており、紐づけられたドメイン名以外では使用できないため、フィッシング耐性を有します。

e) 暗号鍵の不正な取り出し・複製

- ・ 詳細については利用者が用いるデバイスや同期用クラウドサービス等の実装に依存します。多くの場合、パスキーはデバイス内の安全な領域に格納されます。また、同期パスキーがデバイス間で同期するとき

には、エンドツーエンドでの暗号化により保護されます。

ウ その他の考慮事項

a) 事業目的の遂行／公平性に関する考慮事項

- ・ パスキーを利用可能なデバイスには対応条件があり、対応したデバイスの所持が前提となる点に考慮が必要です。

b) アクセシビリティ及びユーザビリティに関する考慮事項

- ・ 他の当人認証手法と比べて比較的新しい手法であるため、利用者の認知度や理解度についての考慮が求められます。

c) セキュリティに関する考慮事項

- ・ パスキー自体はフィッシング耐性を有していますが、パスキーの登録・再設定時の本人確認が不十分であった場合、そこが脆弱性となつてなりすまし攻撃による不正アクセスやアカウント奪取等につながるおそれがある点に留意が必要です³⁴。パスキーの登録・再設定等のプロセスが脆弱性とならないよう、適切な設計が必要です。
- ・ 同期パスキーの場合、同期に利用するクラウドサービスのアカウントが乗っ取られた場合のリスクの考慮が必要です。
- ・ 利用者側のデバイスや OS、同期に利用するクラウドサービスによって、実装の差異が生じる点に留意が必要です。例えば、デバイス内に保存される秘密鍵の保護方法、パスキー利用時の当人認証（ローカルユーザー検証）の挙動、同期パスキーのバックアップ方法、エクスポートの可否、リカバリ方法等は、利用者側の環境等に依存します。

³⁴ 認証器の登録や再設定プロセスが攻撃の起点として悪用されるリスクはパスキー特有のものではありませんが、パスキーの導入時には特に留意いただきたい点であるため、本項目に記載しています。

1.2 その他の当人認証手法

1) パスワード認証+ワンタイムパスワード認証

ア 手法の概要

ワンタイムパスワードは、一回限りのパスワードを生成して認証する方式です。ワンタイムパスワードの生成・伝達方法によって複数の方式があり、利用者側のスマートフォンの TOTP (Time-based One-Time Password) アプリでワンタイムパスワードを生成する方式や、サーバ側で生成したワンタイムパスワードを「認証コード」として SMS や電子メール等によって送信する方式等が代表的です。

いずれの方式においても、ワンタイムパスワードは所有物認証としてみなすことができ、知識認証であるパスワード認証と組み合わせることで当人認証保証レベル 2 に該当する多要素認証として機能します。ただし、ワンタイムパスワードはフィッシングへの耐性を有さない点には留意が必要です。また、ワンタイムパスワードの生成又は送信方法によって脅威や留意事項が異なります。

イ 脅威耐性と留意事項

a) オンライン上でのパスワードの推測

- ・ ワンタイムパスワードは通常ランダムに生成されるため、オンライン上での推測攻撃に耐性を有します。

b) 盗聴・リプレイ攻撃

- ・ 盗聴に対しては通信の暗号化等により対策します。ワンタイムパスワードのリプレイ攻撃に対しては、ワンタイムパスワードの有効期限が短期間であること、ワンタイムパスワードによる認証回数を 1 回きりに制限することによって耐性を有します。

c) パスワードや認証器の盗用

- ・ 多要素認証であるため、単一の認証要素を盗まれた場合にも耐性を有します。
- ・ パスワードとワンタイムパスワードを生成又は受信する環境が同時に盗まれた場合の耐性は有しません。

d) **フィッシング**

- ・ 利用者が偽サイトに誘導され入力したワンタイムパスワードを攻撃者が正規サイトに中継することでの不正アクセスが可能であるため、フィッシングへの耐性を有しません。

e) **暗号鍵の不正な取り出し・複製**

- ・ TOTP 方式の場合、ワンタイムパスワードの生成に使用する暗号鍵（シード値）が漏えいするとワンタイムパスワードを推測可能となるため、安全に管理する必要があります。
- ・ SMS や電子メール等によってワンタイムパスワードを送信する方式の場合は、該当する脅威はありません。

参考情報：「誤ログイン」を防ぐ副次的効果について

昨今、ログイン時の ID にはメールアドレスを用いることが一般的ですが、大量のユーザを抱えるサービスにおいては、一文字しか違いのないような似たようなメールアドレスが ID として用いられることとなります。

このような状況で安直なパスワードが用いられていた場合、ユーザが ID を誤って入力してしまい、さらにパスワードも偶然一致して他者のアカウントに意図せずログインしてしまう「誤ログイン」が発生するケースがありますが、ワンタイムパスワードを組み合わせた認証においては、このような誤ログインの発生を防ぐことができる副次的効果が期待できるとされています。

ウ その他の考慮事項

a) **事業目的の遂行／公平性に関する考慮事項**

- ・ それぞれの方式において、ワンタイムパスワードの生成又は受信のための環境の所持が前提となる点に考慮が必要です。具体的には、TOTP 方式の場合はスマートフォンの Authenticator アプリ、SMS で送信する方式の場合は SMS を受信できる携帯電話番号、電子メールで送信する場合は電子メールアドレスの所持が前提となります。

b) **アクセシビリティ及びユーザビリティに関する考慮事項**

- ・ パスワード認証＋ワンタイムパスワード認証をログインのたびに求めることは、ユーザビリティの面では好ましくありません。ワンタイム

パスワード認証に短い時間制限がある場合は、アクセシビリティ観点での懸念も生じます。利用者側の OS やブラウザが備えるワンタイムパスワードの自動入力機能を利用可能としたり、ログインは単要素認証のみで可能としつつ、高リスクの操作を行う場合にのみワンタイムパスワードを組み合わせた多要素認証を求めたりするといった検討が望まれます。

c) セキュリティに関する考慮事項

- ・ フィッシングへの耐性を有していない点に十分な留意が必要です。
- ・ ワンタイムパスワードを生成又は伝達する方式によって、下表のように考慮すべき脅威が異なります。

表 1-1 ワンタイムパスワードの方式別の主な脅威

No.	方式	考慮すべき脅威
1	利用者側のデバイスで TOTP を生成	<ul style="list-style-type: none"> ・ ワンタイムパスワードの生成に係るシード値が漏えいし、攻撃者側の環境でワンタイムパスワードを生成される ・ TOTP 生成アプリに紐づくアカウントが乗っ取られ、攻撃者にワンタイムパスワードが窃取される
2	SMS 等で認証コードを送信	<ul style="list-style-type: none"> ・ SIM スワップにより、利用者が携帯電話番号を不正に奪取される ・ 第三者によって SMS 等の認証代行が行われる ・ 通信が暗号化されておらず、経由する通信網に脆弱なプロトコルが用いられていた場合に SMS が盗聴される
3	電子メールで認証コードを送信	<ul style="list-style-type: none"> ・ 電子メールアカウントが乗っ取られ、認証コードが奪取される ・ 電子メールの中継中の盗聴により認証コードを奪取される ・ メールの自動転送やメールアカウントの共有等が不適切に行われ、本来の利用者以外に認証コードが伝送される ・ ワンタイムパスワードを伝達するための電子メールを標的型攻撃の起点として悪用される

2) パスワード認証

ア 手法の概要

パスワード認証は、あらかじめ登録した文字列によって利用者を認証する方式です。オンラインサービスにおいて最も普及している本人認証手法の1つです。

しかしながら、利用者側が複数のサービスで同じパスワードを使い回すことが少なくなく、他のサービスから漏えいしたパスワードによって不正アクセスを受けるリスクが大きな問題となっています。また、フィッシングに対しても耐性がなく脆弱です。これらのリスクは、利用者側の運用や注意に依存する部分が多分にあり、サービス提供側での根本的な対策が難しいのが実情です。

加えて、利用者側にとっても複数のサービスのパスワードを覚える必要があるなど利便性が良いとは言えない方式であるため、昨今はパスワード認証を用いない「パスワードレス」な認証方式を採用することが、民間サービスでの一つの潮流となっています。

イ 脅威耐性と留意事項

a) オンライン上でのパスワードの推測

- ・ パスワードの複雑性の確保、一定時間当たりの認証試行回数の制限等により対策を講じる必要があります。

b) 盗聴・リプレイ攻撃

- ・ 通信の暗号化等により対策します。

c) パスワードや認証器の盗用

- ・ 耐性を有しません。

d) フィッシング

- ・ 耐性を有しません。

e) 暗号鍵の不正な取り出し・複製

- ・ 利用者側で暗号鍵は管理しないため、該当する脅威はありません。

ウ その他の考慮事項

a) アクセシビリティ及びユーザビリティに関する考慮事項

- ・ パスワードの設定画面や入力画面は、利用者がパスワードマネージャーを円滑に利用できる実装とすべきです。パスワードマネージャーの利用を禁止又は阻害するような実装は、ユーザビリティを低下させるだけでなくフィッシングに対しても脆弱となるため、推奨されません。なお、「パスワードマネージャーの利用を禁止又は阻害するような実装」とは、以下のような実装が該当します。
 - 利用可能な特殊文字やパスワード長が、一般的なパスワードマネージャーの仕様に対応しておらず、パスワードマネージャーが生成したパスワードがエラーとなり登録できない
 - ID やパスワードの入力欄において、オートフィル機能に向けた適切な属性が設定されていない又は明示的にオートフィル機能を無効化されていることで、パスワードマネージャーが円滑に起動できない
 - ID の入力欄が複数に分割されているなど、一般的なパスワードマネージャーの入力に対応していない
 - パスワード設定時のドメイン名とログイン時のドメイン名が異なるなどして、ログイン時にドメイン名に紐づくパスワードをパスワードマネージャーが自動選択できず、利用者が手動で選択しなければならない
 - ID やパスワードの入力欄において、コピー&ペーストが無効に設定されている

b) セキュリティに関する考慮事項

- ・ フィッシングへの耐性を有していない点に十分な留意が必要です。
- ・ 利用者側が複数のサービスで同じパスワードを使い回すことが少なくなく、他のサービスから漏えいしたパスワードによって不正アクセスを受けるリスクがあります。利用者側のパスワードの使い回しが原因である場合であっても、サービス提供側に不正アクセスについて一定の責任が問われるケースもあります。
- ・ パスワード認証に関する詳細な要求事項（パスワード長の要求事項、複雑性等）については、NIST SP 800-63B-4 についても参考とすることが望まれます。

参考情報：パスワードについてのコラム

コンピュータの黎明期から半世紀以上にわたり、Identity and Access Management (IAM) の世界においてパスワードは最も一般的な認証手段です。人間の脳内に保存でき、キーボードさえあれば提示できる「柔軟性」は、サービス提供者・利用者の双方に、利便性を提供してきました。

本論に入る前に、言葉の定義を明確にしておきましょう。ここで話題にする「パスワード」とは、インターネットなどの通信路を通じてリモートのサービス（パスワードの検証者）に送信・提示される文字列を指します。スマートフォンや PC のロック解除に用いる、デバイス内（ローカル）で完結するもの（しばしば PIN と呼ばれる）とは明確に区別します。

この「リモートに送るパスワード」が今、デジタル社会における大きなリスク要因となっています。

認知能力の限界という「人間の脆弱性」

現代において、個人のプライバシー、資産、信用は少なくない範囲でデジタルデータとして管理されています。しかし、それを守るドアの鍵が「人間の記憶」に依存している点に、技術的な対策だけで解決が難しい構造的な問題が生じています。人間の認知能力には限界があり、記憶できるパスワードの数は限られます。忘却はログイン手段の喪失を意味するため、利用者は無意識のうちにパスワードの「使い回し」や「安易なパターン化」という行動をとるといわれています。これは利用者個人の怠慢ではなく、生物学的な限界、すなわち「人間そのものに存在する脆弱性」とも言えるものです。

たとえば、パスワードの使いまわしによって、あるサイトで漏えいした ID とパスワードで別のサイトへなりすましログインされてしまうリスト型アカウントハッキングや、「緊急」「アカウント停止」といった言葉で利用者を焦らせ、人の判断力を鈍らせ、本物そっくりの偽サイトでパスワードを入力させるフィッシングは、人間の認知能力の限界からくる典型的な攻撃として知られています。

攻撃の経済合理性と防御のアンバランス

攻撃者にとって、パスワードで保護されたサービスに対する攻撃は「コストパフォーマンスの良い」攻撃方法になりえます。インターネットを介して自動化されたツールを利用し、短期間に膨大な回数、大量の利用者を対象とした試行が可能です。成功率がわずかでも、試行回数が膨大なので

十分に元が取れる、つまり攻撃者側に明確な合理性が生じうるということを意味します。

これに対し、サービス提供者がパスワードを使い続けたまま、例えば「リスクベース認証」などの発見的な対策を組み合わせて利用者を保護しようとしても期待した効果を得るのは簡単ではありません。つまり、パスワードだけの保護という不安定な土台の上に、発見的な防御策を講じるのはアンバランスであり、まずは多要素認証あるいはフィッシング耐性のある認証手段を採用したうえで追加の対策を組み合わせる方が理にかなっています。

パスワードマネージャーは理想的な解になるか？

現在、多くのセキュリティ専門家がパスワードマネージャーの利用を推奨しています。パスワードマネージャーには強度の高いパスワードの生成・管理や、URL を機械的に比較した自動入力機能等の機能があり、人間の認知能力への依存度を下げるため有用です。一方、パスワードという形態である以上、最終的に「人間が介在する余地」が残ります。例えば、マネージャーが動かない場面で利用者が手動入力を試みたり、巧妙なフィッシングサイトに誘導されたりした場合、すなわち人間が介在した瞬間にシステムは脆弱になります。パスワードマネージャーは優れた解決策ではあるものの、利用者が選択的に利用するものである限り、根本的な解決策にはならない点に留意しておくのが良いでしょう。

「利用者の責任」から「システムの責任」へ

従来からセキュリティの世界では「強いパスワードを考え、管理するのは利用者の責任」とされてきました。一方、昨今は「パスワードは漏えいし、攻撃されるものである」という前提に立つ必要があります。

利用者にパスワード認証だけを提供し、なりすまし被害のリスクを利用者に転嫁することはサービス提供者としての責任を果たしているとは言えない状況になりつつあります。これからは、利用者の記憶 (Something you know) に依存せず、所持 (Something you have) や生体 (Something you are) を組み合わせること、そして「フィッシング耐性」を有する方式を採用することが重要です。

「パスワードだけで利用者を保護するのは技術的に困難」な時代において、適切な認証手段を採用するための取り組みが求められています。

別紙3 参考資料一覧

本別紙では、ガイドライン本編に基づく検討や、本人確認に関連するシステム整備等の実務において参考となる外部資料とその概要を示します。

なお、各文書の概要や URL については本解説書の執筆時点（2026年2月時点）のものであるため、参照される際には改版の有無を確認の上で、最新版を参照してください。

1 本人確認及びデジタルアイデンティティに関する参考資料

1) NIST SP 800-63 Digital Identity Guidelines

米国国立標準技術研究所（NIST）が策定したデジタルアイデンティティガイドラインです。米国政府のオンラインサービスにおける身元確認、本人認証、フェデレーションの要求事項や推奨事項を定めており、リスクに応じた要求事項や、身元確認、本人認証、フェデレーションのそれぞれに対応する保証レベル（IAL: Identity Assurance Level、AAL: Authentication Assurance Level、FAL: Federation Assurance Level）等が体系的に示されています。

本ガイドラインの対象はあくまで米国政府のサービスですが、実装レベルの要求事項も多く記載されているため、政府情報システムにおける認証機能等の要件定義や実装の際の参考情報として活用することができます。

- ・ 発行元：米国国立標準技術研究所（NIST）
- ・ URL：<https://pages.nist.gov/800-63-4/>

2) ENISA Remote ID Proofing – Good practices

欧州ネットワーク情報セキュリティ庁（ENISA）が発行した、リモートでの身元確認に関するベストプラクティス集です。オンラインでの身元確認プロセスにおけるセキュリティやプライバシー保護のための推奨事項や、リスク低減のための手法等が体系的にまとめられています。

インジェクション攻撃、プレゼンテーション攻撃、ライブネスチェックといったリモート身元確認で特有の脅威と技術の解説が充実しており、ビデオベースの身元確認手法の採用を検討する際の参考情報となります。

- ・ 発行元：欧州ネットワーク情報セキュリティ庁（ENISA）
- ・ URL：<https://www.enisa.europa.eu/publications/remote-id-proofing-good-practices>

3) 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

デジタル庁・総務省が発行した、公的個人認証サービスの適切な運用を確保しながら民間事業者における公的個人認証サービスの利用検討を支援し円滑にするため、公的個人認証サービスの概要、メリット、利用の手引き等を説明したガイドラインです。

民間事業者向けのガイドラインですが、身元確認や本人認証においてマイナンバーカードの公的個人認証の利用を検討する際の参考情報となります。

- ・ 発行元：デジタル庁・総務省

- ・ URL:

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/1f2fb150-febe-4bee-b691-f02f68c4e8d4/3d68c090/20251010_policies_mynumber_private-business_outline_01.pdf

4) パスキー・セントラル (Passkey Central)

パスキー・セントラル (Passkey Central) は、FIDO アライアンスが提供するパスキー導入支援の情報サイトです。概要説明から導入手順、使いやすさの工夫、運用時の確認ポイント、社内向け資料までをまとめ、パスワードに頼らないログインへの移行を支援するためのコンテンツが掲載されています。

本人認証手法としてパスキーを検討する際の参考情報となります。

- ・ URL: <https://www.passkeycentral.org/ja/home/>

2 プライバシーに関する参考資料

1) OECD Privacy Principles (OECD プライバシー原則)

OECD Privacy Principles は、プライバシーに関する国際的な基本指針です。8つの原則が定められており、本人確認手法の採用検討等においてプライバシー面の考慮事項やリスクを検討する際の参考情報となります。

- ・ OECD 公式 Web サイト URL:

<https://www.oecd.org/en/topics/privacy-principles.html>

2) 個人情報保護法等 (個人情報保護委員会 Web サイト)

個人情報保護法に関する法令・ガイドライン・Q&A 等の情報がまとめられたページです。

身元確認において収集する属性情報の検討や、収集した情報の行政機関で

の取扱いにおける個人情報保護法等での要求事項を確認・把握する際の参考となります。

- ・ URL: <https://www.ppc.go.jp/personalinfo/>

3 アクセシビリティに関する参考資料

1) Web Content Accessibility Guidelines (WCAG) 2.2

World Wide Web Consortium (W3C)が2024年12月に勧告した、ウェブアクセシビリティに関するガイドラインで、2025年10月21日よりISO/IEC 40500:2025として国際標準規格にもなっています。我が国のアクセシビリティ規格はJIS X 8341-3:2016 (WCAG 2.0の内容)も一致規格として改正されます。

WCAG 2.2には、解説書やテクニック集もあわせて用意されており、また、これらは情報通信アクセス協議会 ウェブアクセシビリティ基盤委員会 (WAIC)によって日本語化もされています。

また、WCAGが実態としてコンテンツを超える幅広い範囲を網羅するガイドラインになっていることから、策定中の後続バージョン3.0から「W3C アクセシビリティ・ガイドライン (WCAG)」に改称されます。

- ・ 発行元: ウェブアクセシビリティ基盤委員会 (WAIC)
- ・ WCAG 2.2 URL: <https://waic.jp/translations/WCAG22/>
- ・ 解説書 URL: <https://waic.jp/translations/WCAG22/Understanding/>
- ・ テクニック集 URL: <https://waic.jp/translations/WCAG22/Techniques/>