デジタル社会推進標準ガイドライン 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（案）

- 本資料は、「本人確認ガイドラインの改定に向けた有識者会議」での議論を反映・とりまとめることを目的として作成した改定案です。
- 本資料の内容はドラフト段階のものであり、何ら決定・確定されたものではありません。

2025 年（令和 7 年）XX 月 XX 日

デジタル庁

〔ドキュメントの位置付け〕

Normative：政府情報システムの整備及び管理に関するルールとして順守する内容を定めたドキュメント

〔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

〔概要〕

国の行政機関が行政手続等において申請者の本人確認を行う際のデジタルアイデンティティに関する枠組み、対策基準、リスクの評価手順、本人確認手法の選定方法等を示した標準ガイドライン附属文書。

検討にあたる基本的な考え方

リスクに応じた「適切な保証レベル」の選択

本ガイドラインで定義する「保証レベル」とは、本人確認の確からしさを段階的なレベルとして表現する概念である。

これまでの行政手続では、「保証レベルはなるべく高い方がよい」といった考え方により、必要以上に厳格な保証レベルの手法が採用され、結果として利用者にとっては使いにくいサービスとなってしまうことが少なくなかった。

今回の改定では、対象手続のリスクに応じた「適切な保証レベル」を選択できるようにすることを念頭におき、そのための基本的な考え方として「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」及び「セキュリティ」の５つの観点を定義した。

本ガイドラインに基づく検討では、これら 5 つの観点を念頭におきつつ、リスクに応じた「適切な保証レベル」の本人確認手法を選択することが重要であるとご認識いただきたい。

改定履歴

改定年月日	改定箇所	改定内容
2025年x月xx日	全般	・ 「DS-500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」を全面改定。トラスト関連ガイドライン群の文書体系の見直しに伴い、文書番号をDS-500からDS-511に変更。 ・ 表題を「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」に変更。

目次

1　はじめに

1.1　背景と目的

1)　本人確認とデジタルアイデンティティを取り巻く環境

本ガイドラインの前身となる「DS-500 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」(2019 年（平成 31 年）2 月 25 日各府省情報化統括責任者（ＣＩＯ）連絡会議決定）は、各府省が行政手続をデジタル化する際に必要となる本人確認に関する基準、手法例、リスク評価の手順等をとりまとめた文書として策定されたものである。

同ガイドラインの策定以降、我が国ではいわゆるデジタル手続法の施行、マイナンバーカードの普及・利活用の推進などが進められ、本人確認においてデジタルアイデンティティ[1]を取り扱う機会が急速に拡大した。同時に、本人確認書類の偽造、オンラインサービスにおけるフィッシング攻撃、生成 AI を悪用したディープフェイクによるなりすましなど、本人確認に対する脅威も高度化の一途を辿っており、本人確認とデジタルアイデンティティを取り巻く環境は大きく変化している。

2)　デジタルアイデンティティに関する諸外国の動向

諸外国においても、デジタルアイデンティティに関するガイドライン等の見直しや新規制定が活発に進められている。米国標準技術研究所（NIST）では、米国連邦政府向けのデジタルアイデンティティガイドラインである SP 800-63 の改定作業が進められており、フィッシング対策の強化、プライバシーや公平性への配慮の強化、運転免許証をスマートフォンに格納して利用できる仕組みである「モバイル運転免許証（mDL)」への対応などが盛り込まれる見込みである。また、欧州においては「欧州デジタルアイデンティティ規則（The European Digital Identity Regulation)」と称される規則が 2024 年 5 月に施行され、様々なデジタル資格情報をスマートフォンに格納して利用するための「EU Digital Identity Wallet」の導入に向けた検討が欧州各国で進められている。

3)　本ガイドラインの目的

本ガイドラインは、前述のような環境の変化を踏まえ、我が国の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を最新の脅威・

[1] ある主体をデジタル空間において表現するための属性の集合のこと。

技術等に適応させるべく、「DS-500 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」を全面改定する形で制定したものである。

本ガイドラインにより、国の行政手続等における本人確認が、それぞれのリスクに応じた適切な手法によって実施され、ひいては安全・安心で、公平かつ利便性の高い行政サービスの実現に資することを目的とする。

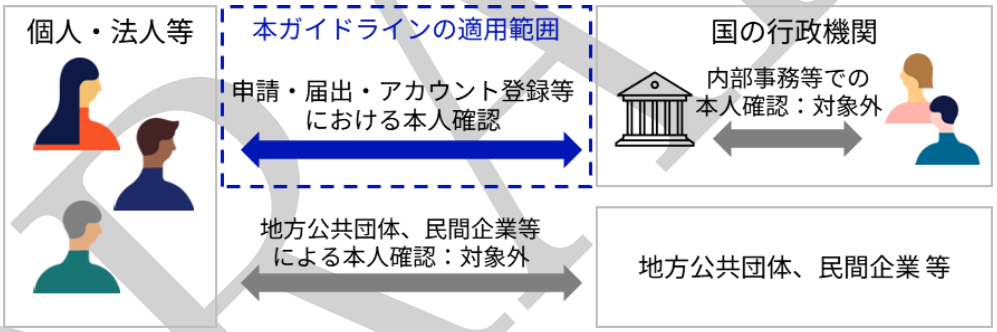
１．２　適用対象

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。

また、法人等の手続における身元確認については、個人に対する身元確認とは異なる考え方や手法が必要となるため、その考え方、プロセス、手法例を「別紙２　法人等の手続における身元確認の考え方について」で示す。

なお、委任や代理人等の条件については対象手続に関係する法令等に従うものとし、本ガイドラインの対象外とする。

図　1-1　本ガイドラインの適用対象の範囲



１．３　位置付け

本文書は、デジタル社会推進標準ガイドラインにおける「標準ガイドライン（Normative）：政府情報システムの整備及び管理に関するルールとして順守する内容を定めたドキュメント」として位置付ける。

１．４　用語

本ガイドラインにおいて使用する用語は、標準ガイドライン群用語集及び表1-1 のとおりとする。ただし、標準ガイドライン群用語集と異なる定義をするときは、標準ガイドライン群用語集と異なる定義であることが明確となるように記載するものとする。なお、参照しやすいよう文中の注記等にて用語集と同様の定義を記載する場合がある。

標準ガイドライン群用語集及び標準ガイドライン群各文書中に用語の定義をしていないものは、一般的な用語の意義を用いるものとする。その他専門的な用語については、民間の用語定義を参照されたい。

なお、国の行政機関における本人確認やデジタルアイデンティティにおいては、諸外国との国際的な相互運用性が求められる場面が想定されるため、用語の対応関係を明確にすることを目的として、一部の用語には対応する英語表記を併記する。

表 1-1 本人確認に係る用語の定義

用語	意味
本ガイドライン全般に係る用語	
本人確認	申請者の実在性や当人性を確認する行為のこと。 本ガイドラインでは、本人確認を「身元確認」、「当人認証」及び「フェデレーション」の 3 つの要素によって定義する。 なお、本人確認という言葉は多義的に用いられる言葉であるため、本ガイドラインでの定義と対象手続の根拠法等での定義が異なる場合があることに留意すること。
デジタルアイデンティティ (Digital Identity)	ある主体をデジタル空間において表現するための属性の集合のこと。
身元確認 (Identity Proofing)	申請者を一意に識別するとともに、実在性を確認すること。 具体的には、申請者の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。
当人認証 (Authentication)	申請者の当人性を確認すること。 具体的には、対象手続を利用しようとする者が、身元確認時に登録された者と同一の人物であることを、申請者と紐づけて登録した認証器を用いて確認する。
フェデレーション (Federation)	身元確認や当人認証を、他者に依拠して実現すること。

用語	意味
	具体的には、信頼できる ID プロバイダと連携し、ID プロバイダによって行われた身元確認や当人認証の結果に関する情報を入手することで、対象手続における本人確認を実現する。
申請者 （Applicant/ Claimant）	対象手続において、申請・届出・アカウント登録・ログイン等を行おうとする個人又は法人等の担当者のこと。 申請者は必ずしも対象手続の正当な利用者とは限らないため、「身元確認」や「当人認証」によって検証する必要がある。
法人等	国税庁長官により法人番号の指定を受けた法人。 ・　設立登記法人・国の機関・地方公共団体。 ・　法人税・消費税の申告納税義務又は給与等に係る所得税の源泉徴収義務を有することとなる設立登記のない法人及び人格のない社団等 ・　上記以外の団体であって、一定の要件に該当するもののうち、国税庁長官に法人番号の指定を受けるための届出書を提出したもの
保証レベル	本人確認の確からしさを段階的なレベルとして表現するカテゴリー。本ガイドラインでは「身元確認保証レベル」と「当人認証保証レベル」の 2 種類の保証レベルを定義する。
対策基準	対象手続の本人確認において実施すべき対策の基準を定めたもの。
身元確認（Identity Proofing）に係る用語	
属性情報（Attributes）	ある主体が備えている性質や特徴に関する情報。例えば、氏名、生年月日、住所など。
本人確認書類 （Identity Evidence）	身元確認において、申請者が主張する属性情報の証拠として用いる書類。マイナンバーカードや運転免許証などの物理的な本人確認書類のほか、スマートフォンに格納されたデジタル証明書なども本人確認書類になり得る。
真正性	情報、データ、文書などが本物であり、偽造や改ざんがされていないこと。本ガイドラインでは本人確認書類の真正性について扱う。

用語	意味
デジタル署名 （Digital Signature）	公開鍵暗号を用いた電子的な署名情報のこと。情報の正当性を保証する。
信頼できる情報源 （Authoritative Source）	本人確認書類の記載情報を保持している権威ある組織やシステム等。本人確認書類の検証において、記載情報を照会することで正確性や非改ざん性を確認する際に用いられる。
当人認証（Authentication）に係る用語	
認証の 3 要素	当人認証に用いる「知識」、「所有」及び「生体」の 3 つの要素の総称。 ただし、昨今は必ずしもこの 3 要素で区分できない技術や仕組みも登場している。
知識認証	パスワードや暗証番号等、利用者本人のみが知り得る情報によって当人認証を行う方式。
所有物認証	秘密鍵を格納した IC カードやスマートフォン、ワンタイムパスワード生成器、乱数表など、利用者本人のみが所持する所有物によって当人認証を行う方式。
生体認証	顔、指紋、光彩、静脈等、本人のみがもつ生体的特徴によって当人認証を行う方式。
単要素認証 （Single-Factor Authentication）	認証の 3 要素のうち、単一の要素のみを用いて当人認証を行う方式。
多要素認証 （Multi-Factor Authentication）	認証の 3 要素のうち、複数の要素を組み合わせて当人認証を行う方式。
認証器 （Authenticator）	当人認証に用いるために申請者が所持し管理する情報、機器、ソフトウェア等の総称。具体例として、パスワード、ワンタイムパスワード生成器、公開鍵暗号を格納したデバイスなどが認証器に該当する。「トークン」と呼ばれることもある。
フィッシング攻撃 （Phishing Attack）	利用者を偽のサイトに誘導し、入力されたパスワードや個人情報等を窃取する攻撃。 昨今では、入力された認証情報を正規のサイトに中継することで、ワンタイムパスワード認証等を突破して不正アクセスを行う「リアルタイム中継

用語	意味
	型」の手法も登場している。
SIM スワップ（SIM Swap）	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等の攻撃を行い、利用者の携帯電話番号を乗っ取る攻撃。
サイドチャネル攻撃	IC カード等のハードウェアを物理的に観測することで得られる情報（消費電力、電磁場、処理時間等）をもとに、内部の秘匿された秘密鍵等の情報を復元する攻撃。
耐タンパ性	暗号鍵を格納する機器等において、内部に格納された情報の不正な読み出し、改ざんなどの攻撃（物理的な解析攻撃やサイドチャネル攻撃等）への耐性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。
フェデレーション（Federation）に係る用語	
ID プロバイダ（Identity Provider）	フェデレーションによる連携を行うモデル（連携モデル）において、申請者に対する身元確認や当人認証を行い、その結果に関する情報を依拠当事者へと連携する主体のこと。
依拠当事者（Relying Party）	連携モデルにおいて、身元確認や当人認証を ID プロバイダに依拠する主体のこと。
アサーション（Assertion）	連携モデルにおいて、身元確認や当人認証の結果に関する情報を連携するために、ID プロバイダから依拠当事者へと発行される情報のこと。
アサーションインジェクション攻撃（Assertion Injection Attack）	偽造・改ざん・再利用などによる不正なアサーションを依拠当事者に提示することで、不正アクセス等を行う攻撃。
共有シグナル（Shared Signaling）	ID プロバイダと依拠当事者の間で、利用者アカウントの停止、侵害の疑い、属性情報の変更などを共有するために用いられる情報のこと。

１.５　基本的な考え方

本人確認は、単に高いセキュリティを確保すればよいというものではなく、事業目的の遂行、公平性、プライバシーなど様々な観点を考慮した検討が必要

となる。本ガイドラインに基づく検討は、以下に示す 5 つの観点を念頭において実施するものとする。

1) 事業目的の遂行

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。

例えば、国民に対して緊急性の高い給付金を支給する手続において、必要以上に厳格な本人確認手法を求めた場合、それが申請の妨げとなり「給付金を迅速に支給する」という本来の事業目的を阻害してしまう恐れがある。

採用しようとする本人確認手法において事業目的の遂行を阻害する懸念がある場合には、代替の手段や例外措置をあわせて検討する必要がある。

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のみを前提とする当人認証手法は、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。

採用しようとする本人確認手法によって公平性の懸念が生じる場合には、代替の手段や例外措置をあわせて検討する必要がある。

3) プライバシー

本人確認においては個人に関する情報を取り扱うため、プライバシー保護についての留意が必要である。

例えば、身元確認において申請者の情報入力を求める場合には、個人情報の収集目的を明示する、目的外の利用を行わないようにする、取り扱うデータを必要最小限に留めるなどといった、プライバシー保護の観点で必要な措置を検討する必要がある。

4) ユーザビリティ及びアクセシビリティ

本人確認におけるユーザビリティやアクセシビリティが十分に考慮されていないと、申請者が誤った操作や入力をしてしまったり、手続を途中で断念してしまったりする原因にもなり、最終的には事業目的の遂行や公平性などにも影響を与えることになる。

したがって、対象手続の利用者の特性や制約などを考慮したうえで、利用者が正しい操作を行いやすく、誤った操作は行いにくく、誤った操作を簡単に修正できるようなユーザビリティ及びアクセシビリティの確保が必要であ

る。

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、ユーザビリティ及びアクセシビリティの観点ではデメリットを抱えている場合がある。したがって、セキュリティ面のリスクの影響度を考慮しつつ、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踏まえた適切な手法の選択が必要である。

2　本人確認の基本的枠組み

2.1　本人確認の構成要素

本ガイドラインでは、本人確認を構成する要素として「身元確認」と「当人認証」を定義する。さらに、身元確認や当人認証を他者（信頼できるIDプロバイダ）に依拠して実現する要素として「フェデレーション」を定義する。

それぞれの構成要素の定義を表 2-1 に改めて示す。また、各要素による本人確認の概念図を図 2-1 及び図 2-2 に示す。

表 2-1　本人確認を構成する要素の定義

構成要素	定義
身元確認 (Identity Proofing)	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こと。 具体的には、申請者の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。
当人認証 (Authentication)	申請者の当人性を確認すること。 具体的には、対象手続を利用しようとする者が、身元確認時に登録された者と同一の人物であることを、申請者と紐づけて登録した認証情報を用いて確認する。
フェデレーション (Federation)	身元確認や当人認証を、他者に依拠して実現すること。 具体的には、信頼できるIDプロバイダと連携し、IDプロバイダによって行われた身元確認や当人認証の結果に関する情報を入手することで、対象手続における本人確認を実現する。

図　2-1　身元確認と当人認証の概念図

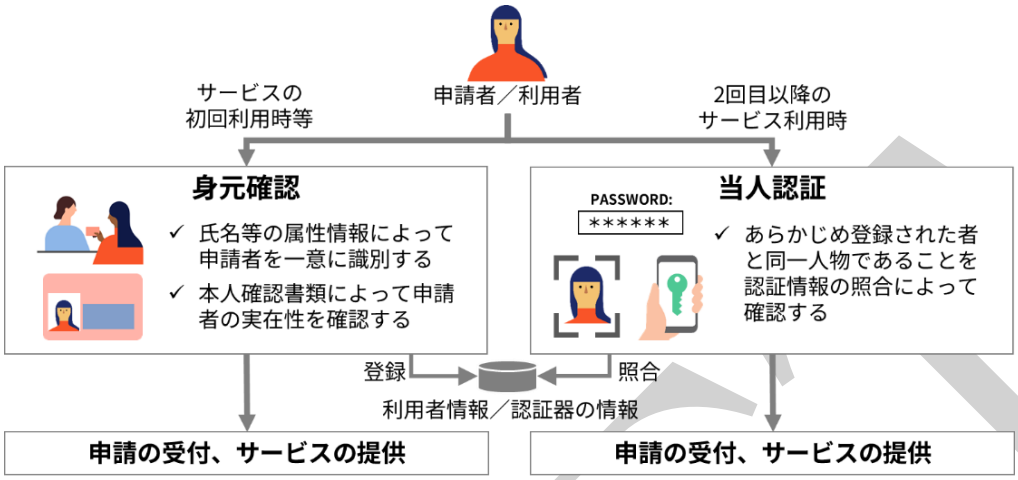
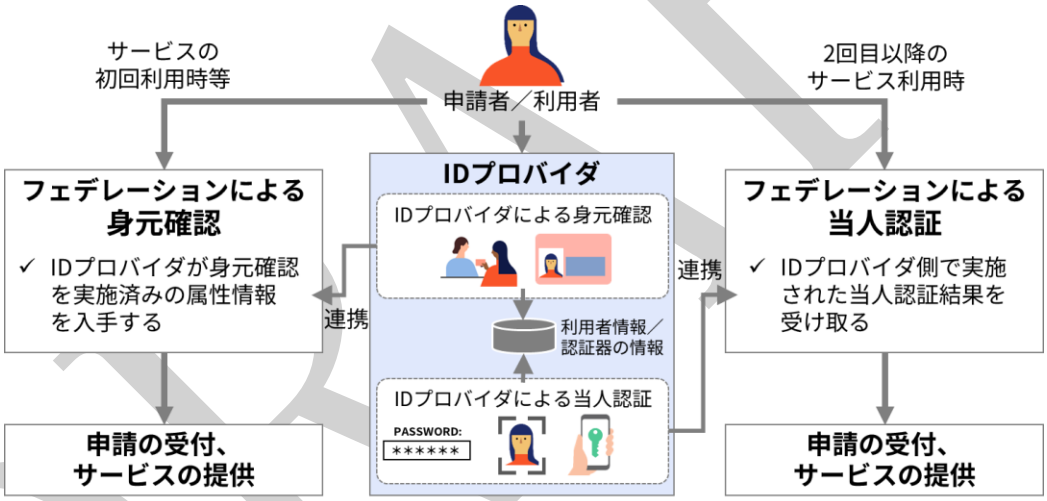


図　2-2　フェデレーションによる本人確認の概念図



２．２　本人確認の実装モデル

情報システムにおいて本人確認を実装するためのモデルとして、前述のフェデレーションによる本人確認を行う「連携モデル（Federated Model)」と、フェデレーションを行わない「非連携モデル（Non-Federated Model)」の２つのモデルを定義する。

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。

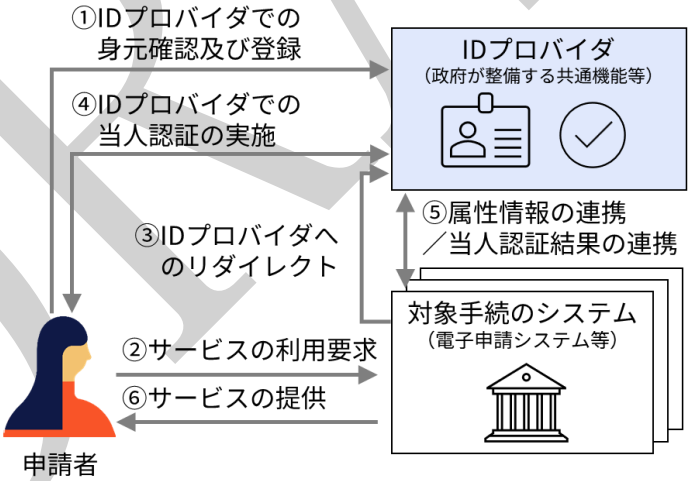
「非連携モデル」については、適切なIDプロバイダが存在しないなど「連携モデル」を採用し難い制約がある場合のみ、採用を検討するものとする。

1)　連携モデル（Federated Model）

連携モデルは、ID プロバイダとのフェデレーションによって、身元確認や当人認証に関する情報の連携を行うモデルである。

ID プロバイダを共通機能として複数のシステムが共同利用することで、本人確認に必要な機能を対象手続それぞれが重複して開発・運用することを回避できる。利用者にとっても複数のサービスにおける身元確認が一度で済むなど利便性の向上が期待できる。

図　2-3　連携モデルの概要図



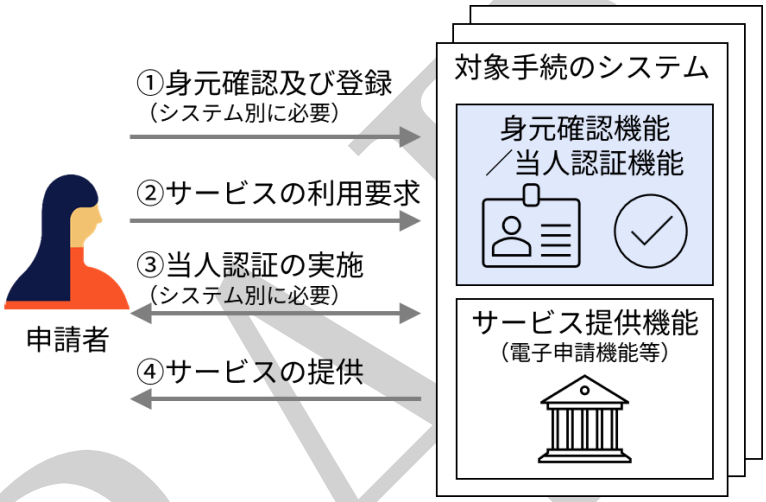
なお、連携モデルの採用においては、対象手続が必要としている保証レベルを満たすIDプロバイダが存在していることが前提となる点や、フェデレーションに関する脅威への対策が必要となる点に留意が必要である。詳細については「３．３　フェデレーション（Federation)」を参照すること。

2)　非連携モデル（Non-Federated Model）

フェデレーションを行わず、サービス提供機能と本人確認機能を自システムのみで構築するモデルである。

自システム専用の本人確認機能を独自に構築できるが、連携モデルのような共同利用のメリットは得られず、利用者にとってもシステムごとに身元確認や当人認証を行う必要が生じるなど、連携モデルと比べて利便性が低下する点に留意が必要である。

図　2-4　非連携モデル概要図



3)　連携モデルと非連携モデルの組み合わせ

前述の連携モデルと非連携モデルは、組み合わせて活用することも可能である。実装モデルを組み合わせる場合の一例を以下に示す。

- 身元確認は対象手続における独自の要件を満たすため「非連携モデル」として実装しつつ、当人認証は「連携モデル」により ID プロバイダと連携して実現する
- 公平性の観点から、「連携モデル」による当人認証手法と「非連携モデル」による当人認証手法をいずれも提供し、利用者が手法を選択できるようにする
- 「連携モデル」によって ID プロバイダから取得した属性情報と、「非連携モデル」によって対象手続自らが入手・検証した属性情報とを組み合わせることで、申請者の身元確認を行う

3　本人確認における脅威と対策

3.1　身元確認（Identity Proofing）

身元確認の目的は、申請者の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ことである。

本節では、身元確認において想定される脅威、実施すべきプロセスと手法例を解説し、身元確認における保証レベルと対策基準を定義する。

1)　身元確認における脅威と対策

身元確認においては、以下に示すような脅威が想定される。これらの脅威を検知又は防止するため、「対策プロセス」に記載した各プロセスを経て身元確認を実施することが必要である。

表　3-1　身元確認における主な脅威と対策プロセス

No.	主な脅威	脅威の概要	対策プロセス
1	重複登録	申請情報の不足や誤り等によって、同一の申請者による重複申請を検知できずに受け付けてしまう	属性情報の収集
2	別人との誤紐づけ	申請情報の不足や誤り等によって、申請者と別の人物とを区別できなくなり、誤った人物の情報と紐づけてしまう	
3	本人確認書類の偽造・改ざん	偽造又は改ざんされた本人確認書類によって、実在する別の人物や架空の人物になりすまされる	本人確認書類の検証
4	本人確認書類の複製	電子的又は物理的に複製された本人確認書類によって、実在する別の人物になりすまされる	
5	本人確認書類の盗用	盗まれた本人確認書類によって、実在する別の人物になりすまされる	申請者の検証
6	本人確認書類の貸し借り	貸し借りされた本人確認書類によって、実在する別の人物になりすまされる	

2)　身元確認のプロセス

身元確認は、「属性情報の収集」、「本人確認書類の検証」及び「申請者の検証」の３つのプロセスによって実施する。また、身元確認の完了後には、利用者の属性情報や認証情報等を登録する「登録」プロセスを行う。関連するプロセスの全体像を以下に示す。

図　3-1　身元確認プロセスの全体像

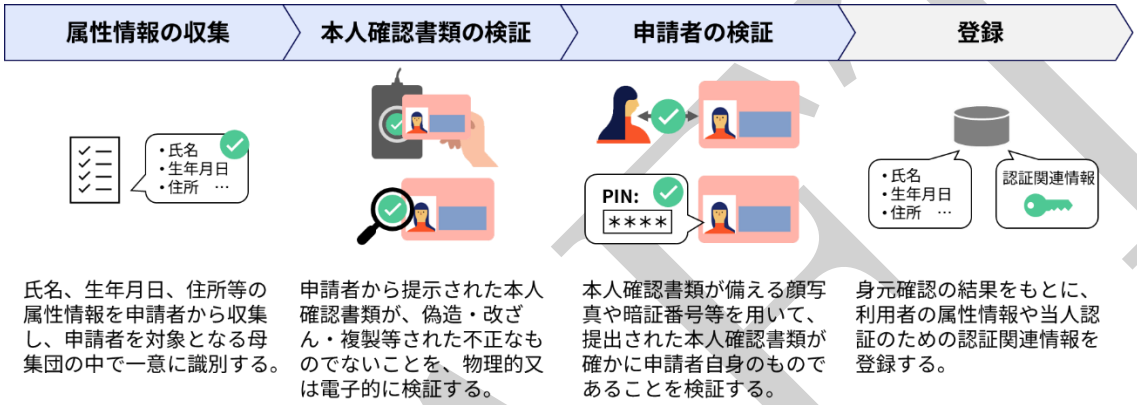


表　3-2　身元確認プロセス及び登録プロセスの概要

No.	プロセス		概要
1	身元確認	属性情報の収集	氏名、生年月日、住所等の属性情報を申請者から収集し、対象となる母集団の中で申請者を一意に識別する。これにより、重複登録や別人との誤紐づけを検知・防止可能とする。
2		本人確認書類の検証	申請者から提示された本人確認書類の真正性を物理的又は電子的に検証する。これにより、本人確認書類の偽造・改ざん・複製等によって別の人物や架空の人物になりすまそうとする攻撃を検知する。
3		申請者の検証	本人確認書類が備える顔写真や暗証番号等を用いて、提出された本人確認書類が確かに申請者自身のものであることを検証する。これにより、本人確認書類が盗難や貸し借りされたものでないことを検証する。
4	登録		身元確認の結果をもとに、利用者の属性情報や当人認証の際に利用する認証情報等を登録する。

3) 身元確認の手法

身元確認の各プロセスにおける主な手法を示す。なお、ここで示す手法は主な例であり、他の手法の採用を妨げるものではない。

ア 属性情報の収集手法

このプロセスでは、申請者の氏名等の属性情報を収集することで、申請者を一意に識別する。収集対象とする属性情報は、氏名、生年月日、住所、個人識別符号（対象手続で利用可能である場合）等が一般的であるが、対象手続の業務特性等により異なる。

属性情報を正確に収集できないと、申請者を一意に識別できず重複登録や別人との誤紐づけの原因となる。そのため、誤記や表記揺れのほか、改姓や改名、住所変更、通称、外国語の表記法、文字コード、異体字や外字の取扱いなど、一意な識別を妨げる様々な要素を考慮しなければならない。

属性情報の収集における主な手法は以下のとおりである。

a) 電子的な読取り

本人確認書類に搭載された IC チップ等から、属性情報を電子データとして読み取る手法。手書き・手入力に伴う誤記や表記揺れ等を防ぎ、属性情報を正確に収集できるが、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となる。

後述する本人確認書類の検証手法において「デジタル署名の検証」を行うことが前提となる。

b) 物理的な読取り

OCR（Optical Character Recognition：光学式文字認識）装置等を用いて、本人確認書類の券面から属性情報を機械的に読み取る手法。手書きや手入力に起因する誤記等のリスク低減が期待できるが、読み取り精度を考慮した確認作業は必要である。

c) 申請者自身による記入・入力

申請様式や申請フォームを用意し、申請者自身による記入・入力を求める方式。誤記や表記揺れなどのリスクが存在する。また、紙への記入を求める方式については、申請を受け付けた側でのデータ入力時の入力ミスや読み間違いのリスクについても考慮が必要となる。

d) IDプロバイダからの情報取得

ID プロバイダに身元確認を依拠する連携モデルの場合、ID プロバイダが実施した身元確認の結果を取り寄せることで、対象手続側で必要とする申請者の属性情報を取得することができる。この場合、後述する「本人確認書類の検証」や「申請者の検証」は ID プロバイダによって実施済みのものとして扱うことができる。

ここで取得した属性情報の正確性や保証レベルは、ID プロバイダが実施した身元確認の手法（身元確認の具体的手法、提示された本人確認書類の種類等）に依存する点や、ID プロバイダが身元確認を実施した時点から属性情報が変更されている可能性がある点に留意すること。

正確性や保証レベルが対象手続において受け入れ可能なものであるかについては、ID プロバイダとの「信頼関係の確立」プロセスにおいてあらかじめ確認・合意することが必要である。詳細については「３．３　フェデレーション（Federation)」を参照すること。

参考：属性情報の収集手法の具体例

参考情報として、対面及び非対面における各手法の具体例を以下に示す。

手法例	対面での具体例	非対面での具体例
a) 電子的な読取り	スマートフォン又は IC カードリーダーを用いて、マイナンバーカードの IC チップから基本 4 情報を読み取る	（対面と同じ）
b) 物理的な読取り	OCR 装置を用いて、本人確認書類の券面の記載情報を光学的に読み取る	OCR 機能付きのスマートフォンアプリを用いて、券面の記載情報を光学的に読み取る
c) 申請者自身による記入・入力	紙の申請書を用意し、申請者自身による記入を求める	申請サイトの Web フォームに申請者自身による入力を求める
d) IDプロバイダからの情報取得	（対面での実施は想定されない）	IDプロバイダと連携し、必要な属性情報を ID プロバイダから取得する

イ　本人確認書類の検証手法

このプロセスでは、身元確認におけるなりすまし等の不正を防ぐため、申請者から提示された本人確認書類に対して、それが偽造・改ざんされたものでないことを検証する。

主な手法は以下のとおりである。手法により利用可能な本人確認書類と検証強度が異なるため、対象手続の利用者特性、取り扱う本人確認書類、想定されるリスク等を踏まえながら、採用する手法を検討する必要がある。

a)　デジタル署名の検証

本人確認書類に格納された電子データに発行元のデジタル署名が付与されている場合、デジタル署名を検証することで、データの発行元と、データが発行後に改ざんされていないことを検証できる。デジタル署名のもつ暗号学的な性質に基づき、厳密な検証が可能である。

b)　信頼できる情報源への照会

信頼できる情報源（本人確認書類の発行元など、本人確認書類の記載情報を正確に保持している、権威ある組織やシステム）に対して、一意な参照番号や QR コード等を用いて情報を照会することで、本人確認書類に記載された内容の真正性を確認する手法。発行元等の情報を直接取得できるため厳密な検証が可能であるが、参照に用いる参照番号や QR コード等の真正性については別の手法で検証する必要がある。

c)　券面の物理的検査（対面）

対面において、本人確認書類の券面を物理的（視覚的・触覚的）に検査することで、偽造・改ざんがされていないことを検証する。

検証の強度は、検査を行う環境（照明の明るさ等)、検査に利用できる道具、本人確認書類が備える偽造対策技術（ホログラムやパールインキ等の印刷技術)、検査担当者の経験・技能、訓練やマニュアルの有無など、様々な要因によって左右される。

d)　券面の物理的検査（非対面）

カメラによる画像・動画の撮影、複合機等による複写・スキャン等によって、本人確認書類の券面を非対面で検証する手法。

手法により強度の差はあるが、この手法による精巧な偽造・改ざんの検知は難しく、対面の場合と比べて検証の強度は低くなる。

参考：本人確認書類の検証手法の具体例

参考情報として、対面及び非対面における各手法の具体例を以下に示す。

手法例	対面での具体例	非対面での具体例
a) デジタル署名の検証	マイナンバーカードの IC チップから読み取った電子データに付与されているデジタル署名を検証し、電子データの偽造や改ざんが行われていないことを確認する	（対面と同じ）
b) 信頼できる情報源への照会	本人確認書類の QR コードを読み取るなどして発行元のサイトにアクセスし、表示された情報と本人確認書類の記載内容が一致していることを確認する	本人確認書類の券面の画像や複写物の提出を求め、そこに記載された QR コードを読み取るなどして発行元のサイトにアクセスし、表示された情報と本人確認書類の記載内容が一致していることを確認する
c) 券面の物理的検査（対面）	本人確認書類の券面を担当者が視覚的・触覚的に検査することで、券面の偽造や改ざんが行われていないことを確認する	―
	本人限定受取郵便（特定事項伝達型）など、対面で本人確認書類の確認を行う郵送サービスを利用する	
d) 券面の物理的検査（非対面）	―	本人確認書類の券面の画像や複写物の提出を求め、それを担当者が視覚的に確認することで、券面の偽造や改ざんが行われていないことを確認する

ウ　申請者の検証手法

「本人確認書類の検証」によって本人確認書類が真正かつ有効であることを確認できた場合でも、窃盗や貸し借りによって正規の本人確認書類が悪用されている可能性がある。そのため、このプロセスでは本人確認書類が確かに申請者自身のものであることを検証する。

主な手法は以下のとおりである。手法によって利用可能な本人確認書類と検証強度が異なるため、対象手続の利用者特性、取り扱う本人確認書類、想定されるリスク等を踏まえながら、採用する手法を検討する必要がある。

a)　対面での容貌確認

対面において、本人確認書類に含まれる顔写真と申請者の容貌とを見比べ、本人確認書類が確かに申請者自身のものであることを検証する手法。

この検証の強度は、検証を行う環境（照明の明るさ等）、検証時の条件（帽子やマスク等の着脱等）、本人確認書類の顔写真の品質や媒体（券面に印刷されたものか、IC チップに格納された電子データか）、検証を担当する者の経験・技能、マニュアルや訓練の有無など、様々な要因によって左右される。

b)　非対面での容貌確認

オンラインでの手続において、カメラで撮影された映像・画像等を観察することで、本人確認書類に含まれる顔写真と申請者の容貌とを見比べ、本人確認書類が確かに申請者自身のものであることを検証する手法。

この検証の強度は、カメラでの撮影を行う環境（照明の明るさ等）、カメラの解像度、本人確認書類の顔写真の精度、検査を担当する者の経験・技能、マニュアルや訓練の有無など、様々な要因によって左右される。顔照合技術等を用いて検査担当者を介さずに行う場合は、当該技術の精度によっても左右される。

また、カメラに対して偽の映像・画像を提示する攻撃（プレゼンテーション攻撃）や、カメラで撮影されたデータを偽の映像・画像に差し替える攻撃（インジェクション攻撃）など、この手法における特有の攻撃への対策も必要となる。

c)　暗証番号等による検証

IC チップを備える本人確認書類やスマートフォンに搭載された本人確認書類等において、それらが備える暗証番号や生体認証等の認証機能を利用することで、本人確認書類が確かに申請者自身のものであることを検証す

る手法。

この検証の強度は、認証に用いる要素、認証機能の精度や仕様（暗証番号の桁数、生体認証の本人拒否率や他人受入率等）等に左右されるが、検証の環境や担当者の技能等に左右されにくく、一定の強度が期待できる。ただし、暗証番号を用いる場合、本人確認書類とともに暗証番号が攻撃者に共有され得るため、本人確認書類の貸し借りは検知できない。

d) 確認コードの送付による検証

本人確認書類に記載された住所等の連絡先に対して「確認コード（6 桁の番号等）」を送付し、申請者がそのコードを入力できることをもって申請者と本人確認書類との紐づきを検証する手法。顔写真を含まない本人確認書類にも適用できる特徴がある。

この検証の強度は、検証の環境や担当者の技能等に左右されにくく、対面・オンラインのいずれにおいても一定の強度が期待できる。ただし、送達中の確認コードが攻撃者に不正取得されるリスクが存在する点などへの留意が必要である。また、確認コードが攻撃者に共有され得るため、本人確認書類の貸し借りは検知できない。

なお、本人確認書類に紐づかない連絡先（電話番号、電子メールアドレス等）に確認コードを送付しても、本プロセスが目的とする「申請者と本人確認書類の紐づきの検証」はできない点に留意が必要である。

参考：申請者の検証手法の具体例

参考情報として、対面及び非対面における各手法の具体例を以下に示す。

手法例	対面での具体例	非対面での具体例
a) 対面での容貌確認	窓口等において、申請者の容貌と本人確認書類の顔写真とを見比べ、同一の人物であることを確認する	―
	本人限定受取郵便（特定事項伝達型）など、対面での容貌確認を行う郵送サービスを利用する	
b) 非対面での容貌確認	―	申請者の容貌と本人確認書類の券面をスマートフォンで撮影することを求め、提出された映像・画像を見比べることで、同一の人物であることを確認する
c) 暗証番号等による検証	マイナンバーカードをスマートフォンやICカードリーダーで読み込む際の暗証番号による認証成功をもって、当該マイナンバーカードが申請者自身のものであることを確認する	（対面と同じ）
d) 確認コードの送付による検証	提出された住民票の写しに記載された住所に6桁の確認コードを郵送し、Webサイト上でコードが入力されたことを確認することで、提出された住民票の写しが申請者自身のものであることを確認する	（対面と同じ）

4) 身元確認保証レベルと対策基準

ア 身元確認保証レベルの位置づけ

身元確認の保証レベルは、表 3-3 に示す 3 段階で定義する。

なお、対象手続におけるリスクの影響度の判断基準については本ガイドラインの 4 章を参照すること。

表 3-3 身元確認保証レベルの位置づけ

身元確認保証レベル	保証レベルの位置づけ
レベル 3	身元確認に関するリスクの影響度が「高位」となる対象手続が該当する保証レベル。 デジタル署名の検証によって本人確認書類の検証を行うことを必須とし、本人確認書類の偽造・改ざん及び複製の脅威に対して厳格な耐性を確保する。
レベル 2	身元確認に関するリスクの影響度が「中位」となる対象手続が該当する保証レベル。 デジタル署名の検証、信頼できる情報源への照会又は対面による券面の物理的検査のいずれかにより本人確認書類の検証を行うことを必須とし、本人確認書類の偽造・改ざんの脅威に対して標準的な耐性を確保する。
レベル 1	身元確認に関するリスクの影響度が「低位」となる対象手続が該当する保証レベル。 本人確認書類の検証は、レベル 2 までの手法に加えて非対面での券面の検査を行うことを許容し、本人確認書類の偽造・改ざんの脅威に対して簡易的な耐性を確保する。

イ　身元確認の対策基準

身元確認における各保証レベルの対策基準は下表のとおりとする。

なお、対策基準はあくまで基準である。同等の脅威耐性を確保できる場合は他の手法等により代替してもよい。

表 3-4　身元確認保証レベルの対策基準

身元確認保証レベル	対策基準
レベル 3	属性情報の収集手法は、以下のいずれかとすること。 ・　電子的な読取り ・　ID プロバイダからの情報取得
	本人確認書類の検証手法は、電子的な複製が困難な本人確認書類を用いた「デジタル署名の検証」とすること。
	申請者の検証手法は、以下のいずれかとすること。 ・　対面での容貌の確認又は非対面での容貌確認 ・　暗証番号等による検証
レベル 2	属性情報の収集手法は任意とする。
	本人確認書類の検証手法は、以下のいずれかとすること。 ・　デジタル署名の検証 ・　信頼できる情報源への照会 ・　券面の物理的検査（対面）
	申請者の検証手法は、以下のいずれかとすること。 ・　対面での容貌の確認又は非対面での容貌確認 ・　暗証番号等による検証
レベル 1	属性情報の収集手法は任意とする。
	本人確認書類の検証手法は、以下のいずれかとすること。 ・　デジタル署名の検証 ・　信頼できる情報源への照会 ・　券面の物理的検査（対面） ・　券面の物理的検査（非対面）
	申請者の検証手法は、以下のいずれかとすること。 ・　容貌の確認（対面）又は容貌の確認（非対面） ・　暗証番号等による検証 ・　確認コードの送付による検証

5)　身元確認に関する個別検討事項

以下の事項については、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て個別の検討を行うものとする。

ア　身元確認において収集する属性情報

身元確認において申請者からどのような属性情報を収集する必要があるかについては、対象手続の事業目的、対象とする利用者層、マイナンバーの利用可否などによって異なる。プライバシーの観点からは、収集する情報は必要最小限の範囲とする必要もある。

これらの点を考慮しつつ、対象手続の身元確認において申請者から収集すべき属性情報を検討すること。

イ　身元確認で利用可能とする本人確認書類

対象手続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、対象手続の目的、根拠法、利用者層、身元確認保証レベル、採用する身元確認手法など、様々な条件や制約を考慮して決定する必要がある。したがって、利用可能とする本人確認書類の種類や条件、複数の本人確認書類の組み合わせの可否等については、対象手続において個別に検討すること。

検討の参考として、採用する身元確認手法に基づく本人確認書類の条件の考え方を以下に示す。

表 3-5　利用可能とする本人確認書類の考え方

身元確認手法	利用可能とする本人確認書類の条件
共通	・　公的機関等の信頼できる機関によって、適切な身元確認を経たうえで発行された本人確認書類であること ・　本人確認書類に一意な参照番号が付与されており、不正の発覚時等に発行元への照会が可能であること
デジタル署名の検証	・　発行元によるデジタル署名が付与されており、発行元の検証及び真正性の検証が可能であること ・　電子データの不正な取り出しや複製が困難な仕組み（耐タンパ性を有する IC チップや、それに類する技術的対策等）を備えていること
券面の物理的検査	・　券面の偽造や改ざんを防止するための技術（ホログラム、パールインキ、顔写真のシェーディング等）が備えられていること
容貌確認	・　適切な品質の顔写真を券面に含むこと

身元確認手法	利用可能とする本人確認書類の条件
	・　適切な品質の顔写真を電子データに含むこと
暗証番号等による検証	・　暗証番号等による認証機能を備えること
確認コードの送付による検証	・　確認コードの送付先として利用できる住所等の情報を含むこと

ウ　本人確認書類の貸し借りへの対策

申請者の検証手法のなかには、「本人確認書類の貸し借り」への耐性を備えない手法もある。対象手続において本人確認書類の貸し借りが行われた場合のリスクを評価し、これを受容できない場合は貸し借りへの耐性を有する手法の採用を検討すること。

エ　身元確認の実施担当者に対する訓練等

身元確認手法のなかには、実施手順や実施する担当者の技能等によって検証強度が大きく左右されるものがある。そのような手法を採用する場合は、適切な検証を実施するためのマニュアル等を整備し、身元確認の実施担当者に対して適切な教育や訓練を行うこと。

実施担当者に対する訓練を必要とする手法例：

- 本人確認書類の検証手法の「券面の物理的検査（対面）」
- 本人確認書類の検証手法の「券面の物理的検査（非対面）」
- 申請者の検証手法の「対面での容貌確認」
- 申請者の検証手法の「非対面での容貌確認」

オ　カメラに対する攻撃への対策

非対面の身元確認においてカメラの映像・画像を用いる場合、カメラに偽の映像・画像を流し込む、通信途中にデータを差し替える、AI 技術等を用いて映像をリアルタイムに加工するなど、この手法に対する特有の攻撃（プレゼンテーション攻撃、ビデオインジェクション攻撃）が想定される。有効な対策は採用しようとする手法や端末環境によって異なるため、必要な対策を個別に検討し講じること。

対策の例：

- 攻撃を検知するための技術（ライブネスチェック等）の採用

・　攻撃が技術的に困難な仕組みを備えるOSや端末の指定
・　専用端末が備えられたブースなど、第三者による攻撃が困難な環境での身元確認の実施

カ　「基本的な考え方」に基づく考慮事項

「１．５　基本的な考え方」に基づき、以下の点を考慮すること。

a)　事業目的の遂行、公平性への影響

身元確認に利用できる本人確認書類が限られることによって、事業目的の遂行や公平性への影響が生じないか留意すること。例えば、本人確認書類に対して「デジタル署名による検証」を必須とする場合、デジタル署名に対応した本人確認書類を有していない利用者の存在を考慮した対応の要否を検討すべきである。

b)　プライバシーに関する考慮事項

身元確認では個人情報を収集するため、収集した情報の取扱いに係るプライバシー面のリスクを識別・評価し、必要な対策を検討すること。

例えば、収集した情報の不適切な利用、名寄せ、第三者への提供、改ざん、漏洩などのリスクが想定される。対策の例としては、収集する情報の最小化、必要のなくなったデータの破棄、目的外利用が行われないための適切な管理や教育などが考えられる。

c)　セキュリティに関する考慮事項

それぞれの手法による検証の強度は、運用方法によっても大きく左右されることに留意すること。特に、担当者が目視で行う「券面の検査」や「容貌の確認」といった手法では、検証の環境、本人確認書類の種別、機材の有無、検証に費やせる時間、マニュアルや訓練の有無など、様々な要因によって検証の強度が変わる。これらの手法を採用する場合には、これらの要素について具体的な運用設計を行うこと。

３．２　当人認証（Authentication）

当人認証の目的は、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一の人物であること（当人性）を確認することである。

本節では、当人認証において想定される脅威、プロセス、手法例等を解説し、当人認証における保証レベルと対策基準を定義する。

1)　当人認証における脅威と対策

当人認証における主な脅威と対策を以下に示す。

表 3-6　当人認証における主な脅威と対策例

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

2)　当人認証のプロセス

当人認証は、認証器のライフサイクルに沿って、「認証器の登録」、「当人認証の実施」、「盗難・紛失等への対応」及び「アカウントの回復」のプロセスを考慮する必要がある。以下に関連するプロセスの全体像を示す。

図　3-2　当人認証プロセスの全体像

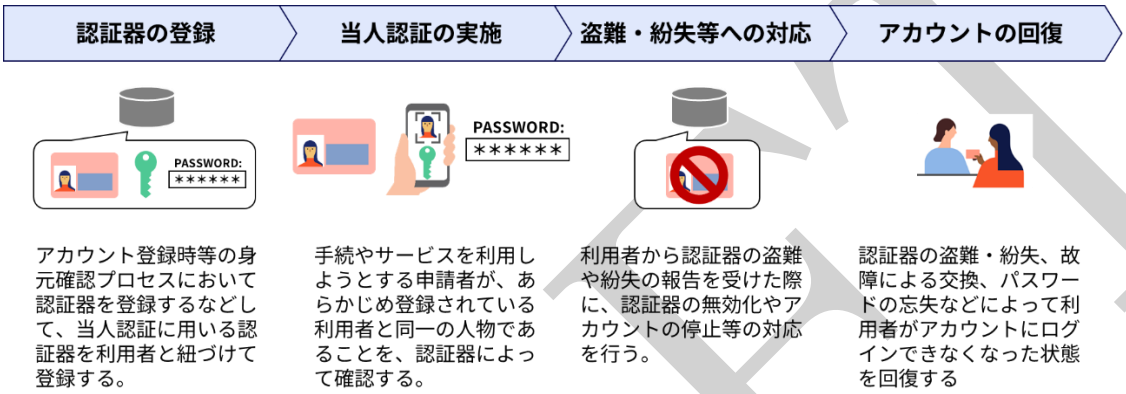


表　3-7　当人認証に関連するプロセスの概要

No.	プロセス	概要
1	認証器の登録	アカウント登録時等の身元確認プロセスにおいて認証器を登録するなどして、当人認証に用いる認証器を利用者と紐づけて登録する。
2	当人認証の実施	手続やサービス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利用者と同一の人物であることを、認証器によって確認する。
3	認証器の盗難・紛失時の対応	利用者から認証器の盗難や紛失の報告を受けた際に、認証器の無効化やアカウントの停止等の対応を行う。
4	アカウントの回復	認証器の盗難・紛失、故障による交換、パスワードの忘失などによって利用者がアカウントにログインできなくなった状態を回復する。

3)　当人認証の手法例

当人認証の手法は、一般に「認証の 3 要素」と呼ばれる「知識認証」、「所有物認証」及び「生体認証」に区分される。これらのうち、1 つの要素を用いるものを「単要素認証」、複数の要素を組み合わせて用いるものを「多要素認証」という。代表的な当人認証の手法例を以下に示す。

表 3-8　代表的な当人認証手法の例

No.	区分	手法例の分類	具体例
1	単要素認証	パスワード認証	―
2		ワンタイムパスワード認証	・ SMS や電子メールアドレスへの認証コード送信
3		公開鍵認証（単要素のもの）	・ IC カード ・ USB セキュリティキー
4	多要素認証	パスワード認証＋ワンタイムパスワード認証	・ スマートフォン用のワンタイムパスワード生成アプリ
6		公開鍵認証（多要素のもの）	・ 暗証番号付き IC カード ・ 生体認証付き USB セキュリティキー ・ パスキー

ア　パスワード認証

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。オンラインサービスにおいて最も普及している当人認証手法の一つである。

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洩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る。また、利用者を偽のサイトに誘導してパスワードを窃取するフィッシング攻撃に対して脆弱である。こうしたリスクは利用者の行動や判断にも依存するため、サービス提供側での根本的な対策が難しい。

イ　ワンタイムパスワード認証

一回限りのパスワードを生成して認証する方式。パスワードの生成や伝達方法によって様々な種類があり、スマートフォン用の 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電子メールや SMS 等によって送信する方式などが代表的である。ワンタイムパスワードは「二段階認証」と

呼ばれる方式でパスワードとともに用いられることがあるが、リアルタイム中継型のフィッシング攻撃への耐性を有さないことに留意が必要である。

SMS 等を用いてワンタイムパスワードを送信する方式は、SIM スワッピング攻撃により利用者が携帯電話番号を不正に奪取されるリスク、第三者によってSMS等の認証代行が行われるリスク、携帯電話番号の再割り当てが行われることで別人に届いてしまうリスク等がある。採用に当たってはこれらのリスクを受容できるか個別のリスク評価が必要である。

電子メールアドレスに対してワンタイムパスワードを送信する方式は、電子メールへのアクセスがパスワードに依存している場合が多く、パスワードと同時に侵害される可能性があることや、メールの送信経路中で傍受されるリスクがある。採用に当たってはこれらのリスクを受容できるか個別のリスク評価が必要である。

ウ　公開鍵認証

IC カード、スマートフォン、USB セキュリティキー等のデバイスに秘密鍵を格納し、公開鍵暗号に基づく認証を行う方式。通常、秘密鍵はデバイスの外部に取り出すことはできない仕組みとなっているが、複数のデバイス間で秘密鍵を同期できる技術も存在する。

a)　単要素の認証器

公開鍵認証のうち、暗証番号や生体認証を必要とせずに利用できる認証器を用いる場合、「所有物認証」による単要素認証となる。

b)　多要素の認証器

公開鍵認証のうち、暗証番号や生体認証によるアクティベーション機能を有する認証器を用いる場合、多要素認証となる。

4)　当人認証保証レベルと対策基準

ア　当人認証保証レベルの位置づけ

当人認証の保証レベルは、以下の 3 段階で定義する。

なお、対象手続におけるリスクの影響度の判断基準については本ガイドラインの 4 章を参照すること。

表 3-9　当人認証保証レベルの定義

当人認証 保証レベル	保証レベルの位置づけ
レベル 3	当人認証に関するリスクの影響度が「高位」となる対象手続が該当する保証レベル。 多要素認証を必須とし、さらにフィッシング耐性をもつ認証手法を全ての利用者が利用することを必須とすることで、厳格な耐性を確保する。
レベル 2	当人認証に関するリスクの影響度が「中位」となる対象手続が該当する保証レベル。 多要素認証を必須とし、さらにフィッシング耐性をもつ認証手法を希望する利用者が選択的に利用できるようにすることで、標準的な耐性を確保する。
レベル 1	当人認証に関するリスクの影響度が「低位」となる対象手続が該当する保証レベル。 単要素認証により、簡易的な耐性を確保する。

イ　当人認証保証レベルの対策基準

当人認証における各保証レベルの対策基準は下表のとおりとする。

なお、対策基準はあくまで基準であり、同等の脅威耐性を確保できる場合は他の手法等により代替してもよい。

表 3-10　当人認証保証レベルの対策基準

当人認証 保証レベル	対策基準
レベル 3	多要素認証であること。 うち一要素は「公開鍵認証」であること。
	以下の全ての脅威耐性を備えること。 ・　フィッシング攻撃への耐性（全ての利用者） ・　レベル 2 で求められる脅威耐性
レベル 2	多要素認証であること。
	以下の全ての脅威耐性を備えること。 ・　フィッシング攻撃への耐性（希望する利用者（※）） ・　暗号鍵の不正な取り出し・複製への耐性 （公開鍵認証を用いる場合） ・　レベル 1 で求められる脅威への耐性
レベル 1	単要素認証又は多要素認証であること。
	以下の全ての脅威耐性を備えること。 ・　オンライン上でのパスワードの推測への耐性 ・　盗聴・リプレイ攻撃への耐性

※ 希望する利用者が、フィッシング耐性をもつ認証手法を選択的に利用できることを指す。

5)　当人認証に関する個別検討事項

以下の事項については、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て個別の検討を行うものとする。

ア　認証器の登録方法

認証器を利用者と紐づけて登録するための登録方法を定めること。

身元確認プロセスの一環として登録することが一般的であるが、アカウント回復のための追加の認証器の登録、認証器の盗難・紛失や故障による交換時の再登録についても考慮が必要である。

イ　認証器の盗難・紛失時の対応

認証器の盗難や紛失を想定した対応をあらかじめ定めること。具体的には、利用者からの報告に応じて当該認証器の登録を解除する、アカウントを一時停止するなどの対応が考えられる。

なお、利用者からの報告を受け付ける際には、第三者のなりすましによる攻撃を想定し、当該利用者に対する本人確認を行う必要がある。後述する「アカウントの回復」とあわせて、報告者に対する本人確認手法を検討すること。

ウ　アカウントの回復

利用者がパスワードを忘れた場合や認証器を紛失した場合に備え、アカウントの回復手段を検討すること。代表的な手段としては以下のような手法例が考えられる。

なお、アカウント回復手段を攻撃の起点とされることを防ぐため、アカウント回復の手段は、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。

表　3-11　代表的なアカウント回復手段例

手法例	概要と留意点
身元確認の再実施	初回登録時と同様の身元確認を再度実施する方式。 身元確認を再実施する負担が生じるが、アカウント回復に起因する脆弱性を生みにくい。
予備の認証器の登録	認証器の紛失等に備え、複数の認証器をあらかじめ登録しておく方式。利用者が複数の認証器を利用できることが前提となる。
リカバリーコードの	アカウントの登録時にリカバリー専用のコードを発行

手法例	概要と留意点
事前発行	しておき、アカウント回復が必要となった際にリカバリーコードの入力を求める方式。 リカバリーコードは登録時に一度だけ発行されるため、攻撃者が能動的に不正入手できる機会が少ないが、利用者はリカバリーコードを適切に保管する必要がある
リカバリーコードの必要時発行	利用者の求めに応じて、利用者の連絡先（住所、電子メール、携帯電話番号等）に対してリカバリーコードを送信し、入力を求める方式。 利用者はリカバリーコードを保管する必要がないが、攻撃者が連絡先を乗っ取り、リカバリーコードを不正に発行・窃取する攻撃への考慮が必要である。

エ　利用者の死亡時の対応

対象手続の特性、根拠法、想定されるリスク等に基づき、利用者が死亡した場合のアカウントの取扱いについて必要な対応を定めること。

オ　「基本的な考え方」に基づく考慮事項

a)　事業目的の遂行や公平性への考慮事項

採用する当人認証手法によって、事業目的の遂行や公平性への影響が生じないか留意すること。例えば、スマートフォンの所有を前提とする手法を採用する場合、スマートフォンを有していない利用者の存在を考慮した対応の要否を検討すべきである。

b)　プライバシーに関する考慮事項

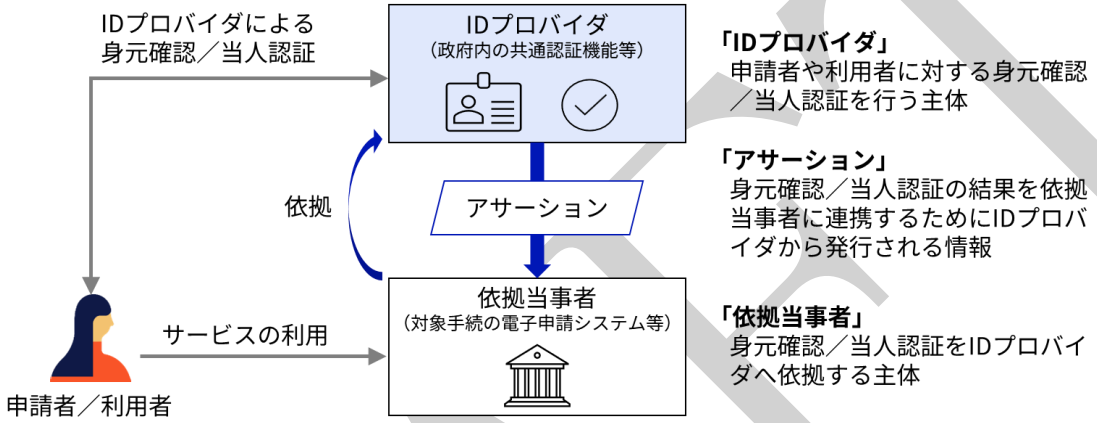
なりすまし等によって不正アクセスを受けた際にアクセス可能となる情報の範囲等を踏まえ、利用者に生じるプライバシー面のリスクを考慮して当人認証手法を検討すること。

さらに、認証器に含まれる情報によって利用者の意図しない名寄せが行われるリスクなど、当人認証手法によって引き起こされるリスクについても考慮すること。

３.３　フェデレーション（Federation）

フェデレーションでは、対象手続における身元確認や当人認証を、信頼できる他者に依拠して実現する。このとき、依拠元となる対象手続を「依拠当事者」、依拠先を「ID プロバイダ」といい、連携のために ID プロバイダから発行される情報を「アサーション」という。概念図を以下に示す。

図　3-3　フェデレーションの概念図



1)　フェデレーションにおける脅威と対策

フェデレーションにおける主な脅威は以下のとおりである。

表　3-12　フェデレーションにおける主な脅威と対策

No.	主な脅威	脅威の概要	対策例
1	保証レベルの齟齬	ID プロバイダが実施する身元確認・当人認証の保証レベルと依拠当事者が必要とする保証レベルに齟齬が生じることで、本来必要とする強度の身元確認・当人認証が行われず、なりすまし等の攻撃を受ける	・ ID プロバイダとの信頼関係の確立
2	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を攻撃者に盗聴・窃取されたり、偽造・改ざん・再利用されたりすることで、情報の窃取やなりすまし等の攻撃を受ける	・ 安全な連携のための設定・登録・鍵管理 ・ 適切な対策を講じたアサーションによる連携

2)　フェデレーションのプロセス

フェデレーションによる安全な連携を実現するためには、ID プロバイダと依拠当事者間で事前調整により信頼関係を確立したうえで、システム面の設定・登録及び鍵管理や、連携されたアサーションの検証等が必要となる。

フェデレーションのプロセスの全体像を以下に示す。

図　3-4　フェデレーションのプロセスの全体像

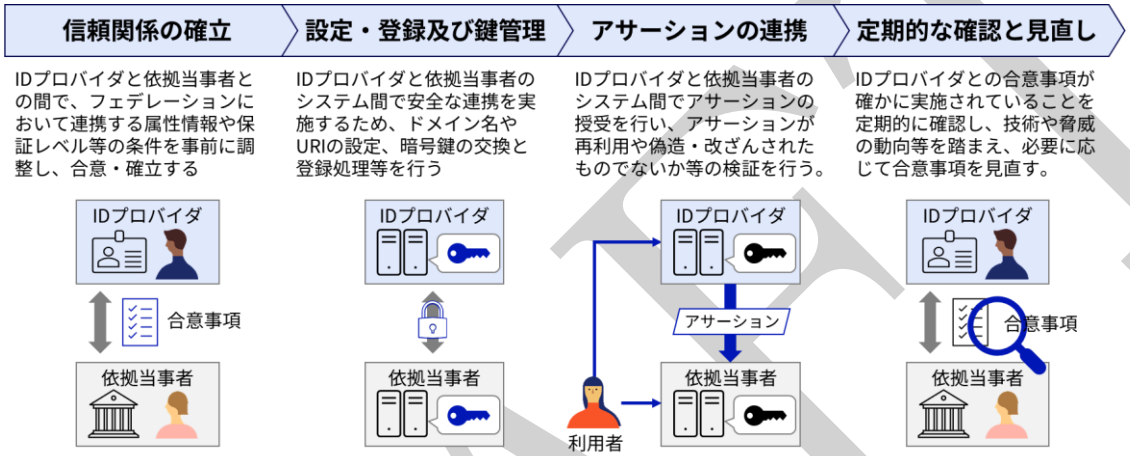


表　3-13　フェデレーションのプロセスの概要

No.	プロセス	概要
1	信頼関係の確立	ID プロバイダと依拠当事者との間で、フェデレーションにおいて連携する属性情報や保証レベル等の条件を事前に調整し、合意・確立する。
2	設定・登録及び鍵管理	ID プロバイダと依拠当事者のシステム間で安全な連携を実施するため、識別子の設定、暗号鍵の登録とその後の鍵管理を行う。
3	アサーションの授受と検証	ID プロバイダと依拠当事者のシステム間でアサーションの授受を行い、アサーションが再利用や偽造・改ざんされたものでないか等の検証を行う。
4	定期的な確認と見直し	「信頼関係の確立」プロセスにおいて合意した事項が確かに実施されていることを定期的に確認する。 また、技術や脅威の動向等を踏まえ、必要に応じて合意事項を見直す。

3)　フェデレーションに関する対策基準

フェデレーションの各プロセスにおいて、依拠当事者となる対象手続が満たすべき対策基準を本項に示す。

なお、本ガイドラインではフェデレーションに関する保証レベルは定義せず、一律の対策基準を定義する。

ア　信頼関係の確立

依拠当事者は、フェデレーションにおいて必要な条件等について ID プロバイダと調整・合意することで、ID プロバイダとの信頼関係を事前に確立するものとする。このプロセスにおいて最低限合意すべき事項を以下に示す。なお、合意事項は文書化して管理するものとする。

表 3-14　信頼関係の確立において合意すべき事項

No.	大項目	合意すべき事項
1	連携対象とする属性情報	・　属性情報名、属性情報の概要 ・　連携する情報の利用目的、利用範囲
2	ID プロバイダが実施する本人確認の保証レベル	・　ID プロバイダが実施する身元確認の保証レベル及び具体的手法 ・　ID プロバイダが実施する当人認証の保証レベル及び具体的手法
3	依拠当事者が必要とする本人確認の保証レベル	・　依拠当事者が必要とする身元確認の保証レベル ・　依拠当事者が必要とする当人認証の保証レベル
4	設定・登録・鍵管理等の方法	・　連携に使用するプロトコル、プロファイル ・　ID プロバイダと依拠当事者との間で安全な連携を確立するために必要となる設定・登録事項（ID プロバイダ及び依拠当事者の識別子、暗号鍵等） ・　暗号鍵の更新期間、更新方法、管理方法、動的な設定や登録を行う場合の技術方式 等
5	共有シグナルの活用方針	・　ID プロバイダと依拠当事者との間でアカウントに関する情報を連携する「共有シグナル」の利用の有無 ・　共有シグナルの送信契機とするイベント（アカウントの停止、アカウントの侵害の疑い、アカウントの属性情報の変更等） ・　共有シグナルに含める情報

No.	大項目	合意すべき事項
6	その他	・　運用面の合意事項（ID プロバイダの SLA、インシデント発生時の連絡経路、対応方針　等）

イ　設定・登録及び鍵管理

「信頼関係の確立」プロセスにおいて合意した内容に基づき、ID プロバイダとの安全な連携に必要となる各種設定・登録（お互いの識別子の設定、暗号鍵の交換・登録等）を行う。暗号鍵については、定期的な更新などの鍵管理を行う。

設定・登録及び鍵管理は手動で行うことを基本として想定するが、必要時に自動的に行うための技術を採用してもよい。

ウ　アサーションの授受と検証

依拠当事者は、ID プロバイダから発行されるアサーションを受け取ることで連携を行う。このアサーションには利用者の個人情報や認証に係る情報が含まれるため、攻撃者によるアサーションの盗聴、窃取、偽造・改ざん、再利用などの脅威を想定し、適切な対策を講じる必要がある。

アサーションに関して最低限満たすべき対策基準は以下のとおりとする。ただし、詳細は ID プロバイダとの連携方式、連携に用いるネットワーク、採用するプロトコルの仕様等によっても異なるため、システムの構築段階において想定される脅威とリスクを分析し、必要な具体的対策を講じること。

表 3-15　アサーションに関する対策基準

No.	分類	対策基準
1	基本事項	・　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。
2	アサーションの検証	アサーションに関する攻撃を想定し、ID プロバイダから受け取ったアサーションに対して依拠当事者は以下の

No.	分類	対策基準
		検証を行うこと。 ・ 想定する ID プロバイダから発行されたものであること ・ 第三者により偽造・改ざんされたものでないこと ・ 自身が要求したリクエストに対して発行されたものであること ・ 自身に向けて発行されたものであること ・ 再利用されたものでないこと ・ 有効期限内であること
3	保証レベル等の情報連携	ID プロバイダ側が複数の認証方式に対応している場合は、必要に応じて、以下の情報をアサーションに含めて依拠当事者へ連携すること。 ・ ID プロバイダ側で実施された身元確認/当人認証の保証レベル ・ 連携時に ID プロバイダ側の当人認証に用いられた認証器の種類
4	その他の脅威への対策	ID プロバイダとの連携方式、連携に用いるネットワーク、採用するプロトコルの仕様等に応じて、対象手続において想定される脅威とリスクを分析し、必要な対策を講じること。

エ　定期的な確認と見直し

依拠当事者は、「信頼関係の確立」プロセスにおいて合意した事項が ID プロバイダにおいて確かに実施されていることを定期的に確認すること。また、技術や脅威の動向等を踏まえ、必要に応じて合意事項を見直すこと。

4　本人確認手法の検討方法

本人確認手法の検討は、表 4-1 のプロセスに従って行うものとする。各プロセスの検討結果は文書化して管理し、継続的な評価と改善に活用すること。

表 4-1　本人確認手法の検討プロセスの全体像

No.	検討プロセス		概要
1	対象手続の保証レベルの判定	リスクの特定	対象手続の機能やサービス等を踏まえつつ、本人確認のリスクを特定する。
2		リスクの影響度の評価	特定したリスクが顕在化した場合の影響度の大きさを 3 段階で評価する。
3		保証レベルの判定	影響度の評価結果に基づき、対象手続に求められる保証レベルを判定する。
4	本人確認手法の評価と決定	本人確認手法の評価	採用候補とする本人確認手法を選定し、事業目的の遂行、公平性、プライバシー等の観点での影響を評価する。
5		補完的対策等の検討	手法の評価結果を踏まえ、懸念される影響を軽減するための補完的対策を検討する。また、必要に応じて対象手続における保証レベルを見直す。
6		例外措置の検討	本人確認における例外ケースを想定し、必要な例外措置を検討する
7	継続的な評価と改善	評価のための情報収集	本人確認手法の評価と改善に必要となる情報を検討し、運用期間中における情報収集を行う。
8		評価と改善の実施	収集した情報をもとに本人確認手法の評価を行い、必要に応じて改善措置を講じる。

４．１　対象手続の保証レベルの判定

このプロセスでは、対象手続における本人確認のリスクを特定し、当該リスクが顕在化した場合の影響度を評価することで、対象手続に求められる保証レベルを判定する。

1)　リスクの特定

対象手続が提供する機能やサービス、取り扱う情報資産、手続によって得られる権益等を踏まえつつ、対象手続の身元確認や当人認証において想定されるリスクを特定する。具体的には、身元確認及び当人認証における脅威をもとに対象手続におけるリスクケース（脅威によって悪影響が引き起こされる典型的なケース）を定義し、当該ケースにおいて利用者や関係者に生じる悪影響の内容を明確化する。

代表的なリスクケースの例を以下に示す。ただし、想定すべきリスクケースは対象手続によって異なることに留意すること。

表　4-2　代表的なリスクケース例

プロセス	リスクケース例	リスク特定の考え方
身元確認	実在する人物になりすました申請や登録	本人確認書類の偽造・改ざん、盗用等によって、攻撃者が実在する人物になりすまして申請やアカウント登録を行った場合に、なりすまされた人物、自組織、その他の関係者にどのような悪影響が生じるか。
	実在しない架空の人物になりすました申請や登録	本人確認書類の偽造・改ざん等によって、攻撃者が実在しない架空の人物になりすまして申請やアカウント登録を行った場合に、自組織やその他の関係者にどのような悪影響が生じるか。
当人認証	登録済みの利用者に対する不正アクセス	パスワードの推測や認証器の盗用等によって、攻撃者が他の利用者アカウントに不正にログインした場合に、不正アクセスを受けた利用者、自組織、その他の関係者にどのような悪影響が生じるか。
	フィッシングサイトに対する認証情報や個人情報の入力	利用者がフィッシングサイトに誘導され、認証情報や個人情報が攻撃者に詐取された場合に、利用者、自組織、その他の関係者にどのような悪影響が生じるか

2) リスクの影響度の評価

特定したそれぞれのリスクに対して、リスクが顕在化した際の影響度を「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」として判定する。リスクの影響度の評価基準を下表に示す。

なお、対象手続によっては身元確認と当人認証でリスクの影響度が異なる場合も想定される。そのような場合は、身元確認と当人認証のリスクの影響度をそれぞれ個別に判定すること。

表 4-3 リスクの影響度の評価基準

観点	評価の基準	影響度	想定例
対象手続等によって得られる権利権益等の侵害	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	高位	なりすましの被害者が長期間にわたって行政サービスを受けられなくなり、遡及等の原状回復にも時間を有する
	特定の利用者や関係者が、本来有する権利利益を一時的に行使又は享受できなくなるが、短期間での回復や復旧ができる	中位	なりすましの被害者が本来有する資格を一時的に行使できなくなるが、短期間で復旧できる
	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	低位	なりすましの被害者はアカウント再発行が必要となり一時的な不便を被る
プライバシーの侵害	特定の利用者や関係者に関する要配慮個人情報が侵害されるなど、容易には回復できないプライバシー面の影響を受ける	高位	不正アクセスによって利用者の要配慮個人情報等を攻撃者に閲覧・窃取される
犯罪や攻撃への悪用	対象手続におけるなりすましや不正アクセスの結果が、犯罪や他の行政サービス・民間サービスへの攻撃に悪用される	高位	攻撃者に対して対象手続から証明書が発行され、民間サービスに対するなりすましに悪用される

3) 保証レベルの判定

影響度の評価結果を基に、対象手続に求められる保証レベルを以下の基準に基づき判定する。

なお、身元確認と当人認証のリスクの影響度が異なる場合には、身元確認保証レベルと当人認証レベルも異なるレベルとなる。

表 4-4 影響度と保証レベルの対応関係

影響度	身元確認 保証レベル	当人認証 保証レベル
高位	レベル 3	レベル 3
中位	レベル 2	レベル 2
低位	レベル 1	レベル 1

補足：本ガイドラインが想定するリスクの影響度の範囲について

本ガイドラインは、対象手続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しているため、本人確認に関するリスクの影響範囲は、攻撃や侵害を受けた特定の利用者やアカウント等に限定されることを前提としている。

したがって、リスクの影響範囲が多数の利用者又は関係者に及ぶ場合には、その影響度は本ガイドラインが定義する「高位」よりも更に高次のものとして扱う必要があり、必要な対策についても「保証レベル 3」より高次の対策が求められるため、対象手続において個別のリスク分析と追加対策の検討を行うこと。

４．２　本人確認手法の評価と決定

本人確認手法には様々な種類や方式が存在し、対象手続の目的、根拠法、想定利用者などによって適する手法は異なる。

このプロセスでは、対象手続の保証レベルに基づき採用候補とする本人確認手法を評価することで、補完的対策の検討、保証レベルの見直し、例外措置の検討を行い、対象手続で採用する本人確認手法を決定する。

1)　本人確認手法の評価

保証レベルの判定結果を基に、採用候補とする本人確認手法を選定し、「1.5 基本的な考え方」で示す５つの観点に基づき手法の評価を行う。

表　4-5　本人確認手法の評価観点

評価の観点	評価の観点の具体内容
事業目的の遂行	事業目的の遂行に適した手法であるか。 具体的には、対象手続の目的、根拠法、緊急性、本人確認を行う環境、想定される利用者層などに対して適した手法であり、事業目的の遂行を阻害する懸念がないか。
公平性	当該手法によって公平性が損なわれないか。 具体的には、想定される利用者の一部にとって障壁となる懸念がなく、当該事業が対象とする利用者全員に対して、公平な利用機会を提供できる手法であるか。
プライバシー	当該手法によるプライバシー面の懸念がないか。 例えば、対象手続のサービス提供に必要な範囲以上の個人情報を収集してしまうなど、プライバシーの原則に抵触するような制約がないか。
ユーザビリティ及びアクセシビリティ	ユーザビリティについては、想定する利用者にとって理解しやすく、間違いにくく、効率的な手続ができるユーザビリティを提供できる手法であるか。アクセシビリティについては、利用者の怪我、障害、視力や聴力の低下など、利用者の様々な条件や制約を考慮したうえで十分なアクセシビリティを確保可能であるか。
セキュリティ	対象手続が求める保証レベルに該当する手法であり、必要以上の強度を有する過剰な手法となっていないか。 また、耐性を有さない脅威によるリスクは受容可能であるか。

2) 補完的対策等の検討

前項の評価の結果、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、セキュリティの観点での懸念やリスクが想定される場合には、対象手続で求められる要求事項とのギャップを補完するための補完的対策を検討する。補完的対策の例を以下に示す。

表 4-6 補完的対策の例

補完的対策	概要
複数の本人確認手法の併用	採用しようとする手法の制約によって事業目的の遂行や公平性の阻害が懸念される場合には、複数の本人確認手法を併用することで制約を緩和することが検討できる。
追加の対策	採用しようとする本人確認手法だけではプライバシーやセキュリティの要求事項を満たせない場合には、追加的な対策を講じることでリスクを軽減することが検討できる。
より高い保証レベルの本人確認手法の採用	採用しようとする本人確認手法にセキュリティ面の懸念がある場合などには、対象手続に求められる保証レベルよりも高いレベルの本人確認手法を採用することも検討できる。ただし、それによって事業目的の遂行や公平性など他の観点へ与える影響を考慮する必要がある。
より低い保証レベルの本人確認手法の採用	事業目的の遂行、公平性、ユーザビリティ及びアクセシビリティ等の観点から、対象手続に求められる保証レベルよりも低いレベルの本人確認手法を採用することも検討できる。この場合、本来必要とされる保証レベルとの差によるセキュリティ面のリスクを「追加の対策」によって補完するか、リスクを受容する判断が必要となる。

3) 例外措置の検討

本人確認を行う手続においては、申請者の本人確認書類の紛失、利用者の当人認証用デバイスの故障など、様々な例外ケースが想定される。対象手続の事業目的や緊急性によっては、こうした例外ケースにおいても申請等を受け付けなければならない場合も想定されるため、採用する本人確認手法とともに、対象手続における例外措置の要否と内容を検討・決定する。

なお、本来の手法と例外措置に保証レベルに差があると、なりすまし等の攻撃の起点に悪用される恐れがある点に留意が必要である。また、攻撃の起点とされることを防ぐため、例外措置の詳細については非公開とすることに

ついても検討すべきである。

４．３　継続的な評価と改善

1)　評価のための情報収集

対象手続において採用した本人確認手法について、評価に必要となる情報を定義し、それらの情報を収集・蓄積すること。

評価に必要な情報には、対象手続における利用者からの問合せ履歴、セキュリティ監視によって検知したイベントやインシデントの履歴、本人確認に関する脅威やインシデントの動向など様々なものが考えられる。

これらの情報収集には、システムの運用・監視等の仕組みの構築が必要となるものも含まれるため、情報システムの要件定義時点から、このような情報収集を見据えた要件定義を行うことが必要である。

2)　評価と改善の実施

収集した情報をもとに本人確認手法の評価を行い、必要に応じて手法の見直し、追加対策の導入、本人確認担当者に対する教育・訓練等の改善措置を講じること。

別紙１　附則

附則（令和７年X月XX日デジタル社会推進会議幹事会決定）

１　施行期日

本ガイドラインは、決定の日から施行する。

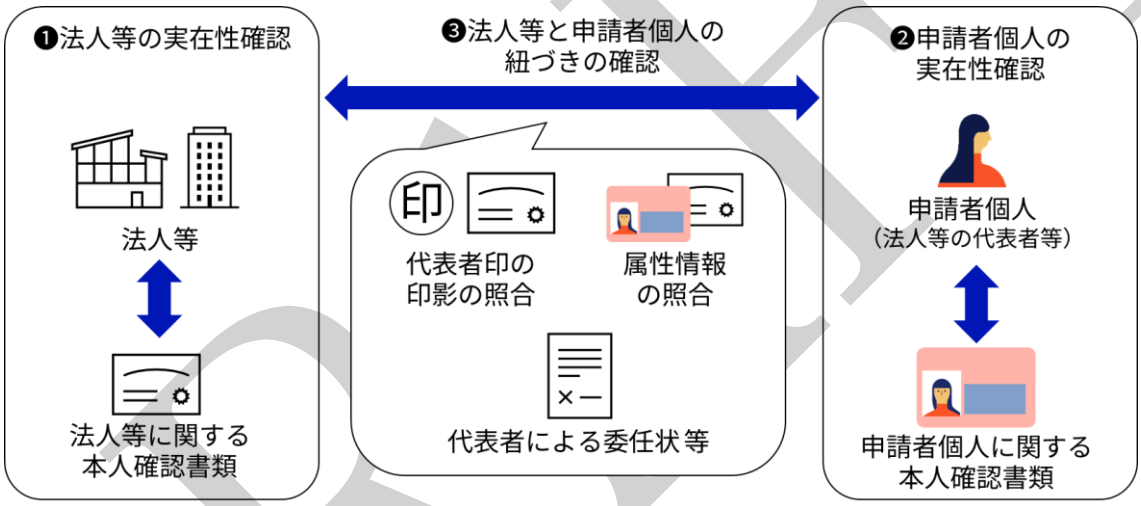
別紙２　法人等の手続における身元確認の考え方について

法人等の手続における身元確認では、個人に対する身元確認とは異なる考え方や手法が必要となる。本別紙において、その考え方や手法例を示す。

１　基本的な考え方

法人等の手続における身元確認では、❶法人等の実在性確認、❷申請等の手続を行う代表者等の個人（以下「申請者個人」という）の実在性確認を行ったうえで、❸法人等と申請者個人との紐づきの確認を行う必要がある。概念図を以下に示す。

図　1-1　法人等の手続における身元確認の概念図



２　法人等の手続における身元確認のプロセスと手法例

前述の考え方に基づき、法人等の手続における身元確認のプロセスと手法例を以下に示す。

２．１　法人等の実在性確認

法人等の実在性確認は、「属性情報の収集」及び「本人確認書類の検証」のプロセスによって実施する。

1)　属性情報の収集

申請等の主体となる法人等を一意に識別するための属性情報を収集する。収集対象とする属性情報は、「法人等の基本３情報」と呼ばれる「法人番号」、「称号又は名称」及び「本店又は主たる事務所の所在地」を基本とすること

が考えられる。

加えて、法人等と申請者個人との紐づきを確認するための情報についても収集が必要となる。具体的には、代表者印による紐づきを行う場合は代表者印の印影の収集、代表者の属性情報による紐づきを確認する場合は「代表者氏名」及び「代表者住所」の収集などが考えられる。

2)　本人確認書類の検証

法人等の本人確認書類の提出を求め、その真正性をそれぞれ検証する。

法人等の本人確認書類に該当する書類としては、法人番号が記載された公的な証明書を扱うことが考えられる。具体例としては、法人番号指定通知書、登記事項証明書、印鑑（登録）証明書などが想定される。

本人確認書類の検証手法は、基本3情報については「国税庁法人番号公表サイト」による「信頼できる情報源への照会」を基本とすることが考えられる。その他の本人確認書類については、券面の物理的な検査や発行元の照会等による検証が考えられる。

２.２　申請者個人の実在性確認

申請者個人に関する本人確認書類により、申請者個人の実在性確認を行う。このプロセスや手法については本ガイドラインの本編を参照すること。

２.３　法人等と申請者個人の紐づきの確認

法人等の実在性確認、申請者個人の実在性確認を行ったうえで、法人等と申請者個人の紐づきの確認を行う。

1)　申請者個人が法人等の代表者の場合

申請者個人が法人等の代表者である場合は、代表者印の印影と印鑑（登録）証明書の印影を照合することで、当該申請者個人が確かに法人等の代表者であることを検証できる。

法人等の本人確認書類と申請者個人の本人確認書類のそれぞれに記載された属性情報（代表者氏名、代表者住所 等）の一致をもって、紐づきを確認することも考えられる。

2)　申請者個人が法人等の代表者以外の場合

申請者個人が代表者以外の場合は、上記の手法により法人等と代表者との紐づきを検証したうえで、更に委任状の提出を求めることで、法人等との紐づきを確認することが考えられる。

３　留意事項

本別紙の内容は、法人等の実在性確認、申請者個人の実在性確認及び法人等と申請者個人の紐づきの確認のみを対象としたものである。その他の観点（例えば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）は含まない点に留意されたい。