2025 年 1 月 20 日

「マイナンバー制度の問題点と解決策」に関する提言の補足 2(システム移行編)

付録 1 【本人確認定義の見直し案】

一般社団法人　情報システム学会　マイナンバー制度研究会

【目次】

1．はじめに

2024 年 11 月に公表した「『マイナンバー制度の問題点と解決策』に関する提言の補足 2(システム移行編)」の 3.1 節 1）において、以下の提案をした。

---以下、3.1 節 1）からの抜粋

・今のマイナンバー制度の中で使用している「本人確認」という言葉の使用を止め、身元確認、当人確認（認証)、真正性確認＋属性情報確認に分離し、現在の「本人確認」という曖昧な言葉を使用している法令、ガイドラインを全て洗いだして見直し・改正する。

・例えば、「本人確認ガイドライン改定方針 令和 5 年度中間とりまとめ」、「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」などである。どちらのガイドラインにおいても、見直しの重要なポイントは「身元確認と当人確認（認証）の定義を混在させず、分離した定義をする」ことである。

---以上

そして、3.1 節 1)の中では、「本人確認ガイドライン改定方針 令和 5 年度中間とりまとめ」、「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」における、身元確認と当人確認（認証）の改正案の骨格のみを提案した。補足 2 の提言の中では骨格のみの提案にとどめたが、本付録では改正案について、さらに具体的な内容をまとめたので、ご覧いただきたい。

なお、本付録の提言は、「米国立標準技術研究所（NIST）の Digital Identity Guidelines 第 3 版（NIST SP 800-63-3)」(以降は、「NIST SP 800-63-3」と表示）を参考にしているが、「NIST SP 800-63-3」では定義されていない点にも言及している。そのため、提言の中では、随所で「NIST SP 800-63-3」の内容を参考にした点、異なる点について言及している。

2．本人確認

2.1.「本人確認」という用語の曖昧な使用を止めることの必要性

現在のマイナンバー制度の中では、「本人確認」という用語は、2023 年 10 月公表の「『マイナンバー制度の問題点と解決策』に関する提言」で触れたように曖昧に使用されており、そのことが今のマイナンバー制度の混乱や設計不良を誘発する根本原因の一つになっている。そのため、「本人確認」という用語を、曖昧な定義のままで使用することは中止する必要がある。

そこで、本付録では「本人確認」の定義について、具体的に提案する。

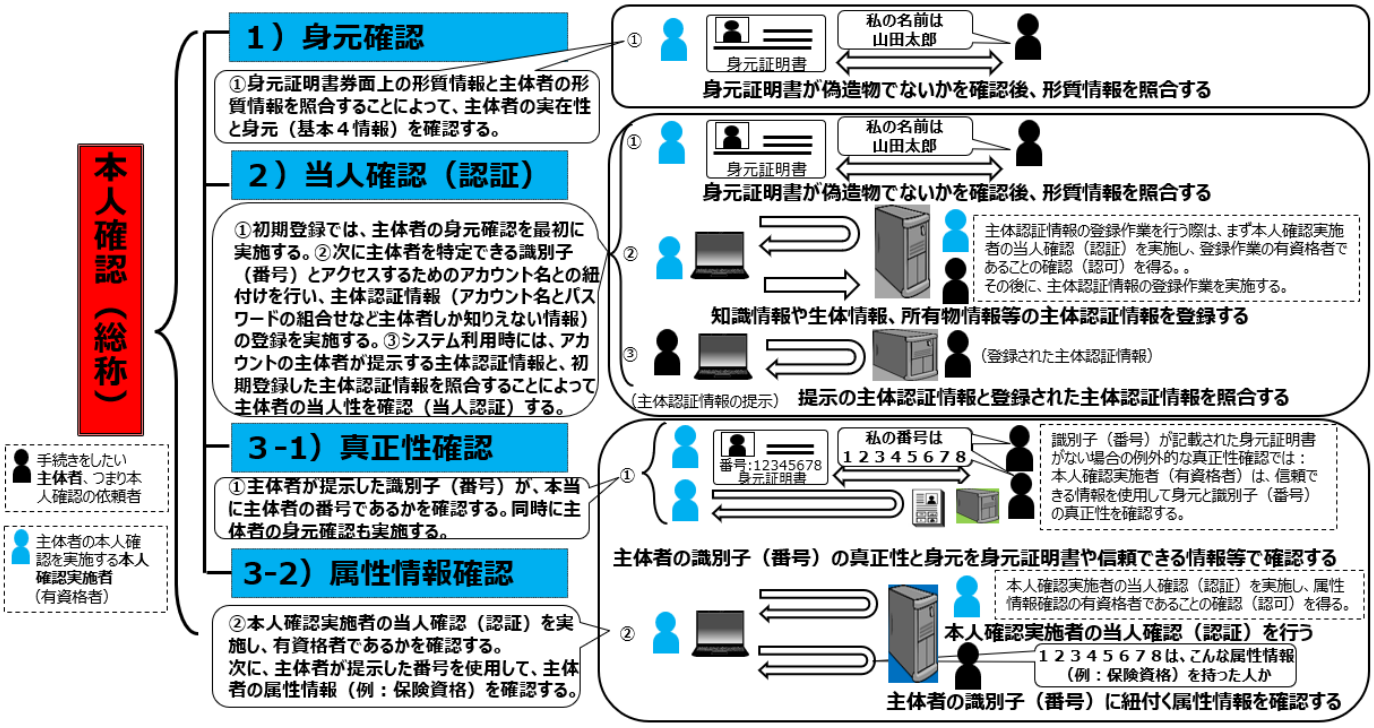
2.2.「本人確認」の用語の定義

本節では、「本人確認」を以下のように定義することを提案する。

「本人確認とは、なんらかの手続きを行いたい主体者の本人性を確認するプロセスの総称であり、『身元確認』『当人確認（認証）』『真正性確認と属性情報確認』の３つの確認プロセスから構成される。つまり、主体者の本人性の確認が必要な手続きは、これらの３つの確認プロセスを適切に組み合わせることによって確認作業を実施することになる。そして、これらの確認プロセスの実施者は、本人確認を依頼する『主体者』と、主体者の本人確認を実施する『本人確認実施者』から構成される。」

- 『主体者』：本人確認を依頼する者
- 『本人確認実施者』：主体者の本人確認を実施する者

本人確認を構成する３つの確認プロセスの詳細な定義と厳密度（保証レベル）については、次章以降に提案しているので、ご覧いただきたい。本節では、簡略化した定義の説明を以下に記し、３つの本人確認プロセスを図式化したものを、図１に示す。



【図１】「本人確認」とは、３つの本人性を確認するプロセスの総称

１）身元確認【リアル環境とオンライン環境での確認プロセスを対象とする】

「本人確認実施者が、主体者の形質情報（顔写真など）と身元証明書上の形質情報（顔写真など）を照合することによって、主体者の身元情報（基本４情報）と主体者の実在性を確認する」こと。

（注）「NIST SP 800-63-3」では、上記の確認（身元情報（基本４情報）の確認は含まれていない）プロセスのことを「Identity Proofing」と呼んでおり、一般的には「身元確認」と翻訳され、上記の身元情報（基本４情報）の違いを除けば本付録での「身元確認」の定義と同義である。

２）当人確認（認証）【基本的にオンライン環境のみでの確認プロセスを対象とするが、身元確認プロセスはリアル環境とオンライン環境を対象とする】

「まず、本人確認実施者が、オンラインサイトを利用したい主体者の身元確認を行う。次に、本人確認実施者が主体者の主体認証情報の登録を行う。なお、本人確認実施者は主体認証情報を登録するための情報システムにアクセスする権利の有資格者である必要がある。そのため、本人確認実施者は登録作業を実施する前に、自分の当人確認（認証）を行い有資格者であることの確認（認可）を得る必要がある。そして、オンラインサイトを実際に利用する際には、主体者が提示する主体認証情報と事前に登録された主体認証情報を照合することによって、主体者の当人性を確認する」こと。この照合作業は本人確認実施者が行う作業であるが、主体者が情報システムを使用して人手を介さずに電子的に照合が行われるのが一般的である。

（注）「NIST SP 800-63-3」では、主体認証情報の登録のことを「Enrollment」と呼んでおり、一般的には「登録」と翻訳されている。オンラインサイトを実際に利用する際に行う当人性の確認のことは「Authentication」と呼んでおり、一般的には「当人認証」と翻訳されている。つまり、本付録が提案している「当人確認（認証）」と、「当人認証」とは用語は似ているが、意味が異なる。本付録の「当人確認（認証）」の定義においては、「NIST SP 800-63-3」の「Authentication（当人認証）」プロセスは一要素でしかない。本付録では、主体者の身元確認（Identity Proofing）と主体認証情報の登録（Enrollment）、当人性の確認（Authentication）、の３つのプロセスを含めて「当人確認（認証）」として定義している（図２参照）。

つまり、本付録における「当人確認（認証）」は「NIST SP 800-63-3」の全体の目的として書かれている「Electronic Authentication」（一般的な翻訳は、「電子的な認証」）に該当すると理解していただきたい（図４参照）。

３-１）真正性確認【リアル環境のみを対象とする】

「本人確認実施者が、主体者の形質情報と身元証明書上の形質情報を照合して身元を確認し、その身元証明書に記載された識別子（番号）の真正性（その識別子（番号）が主体者に

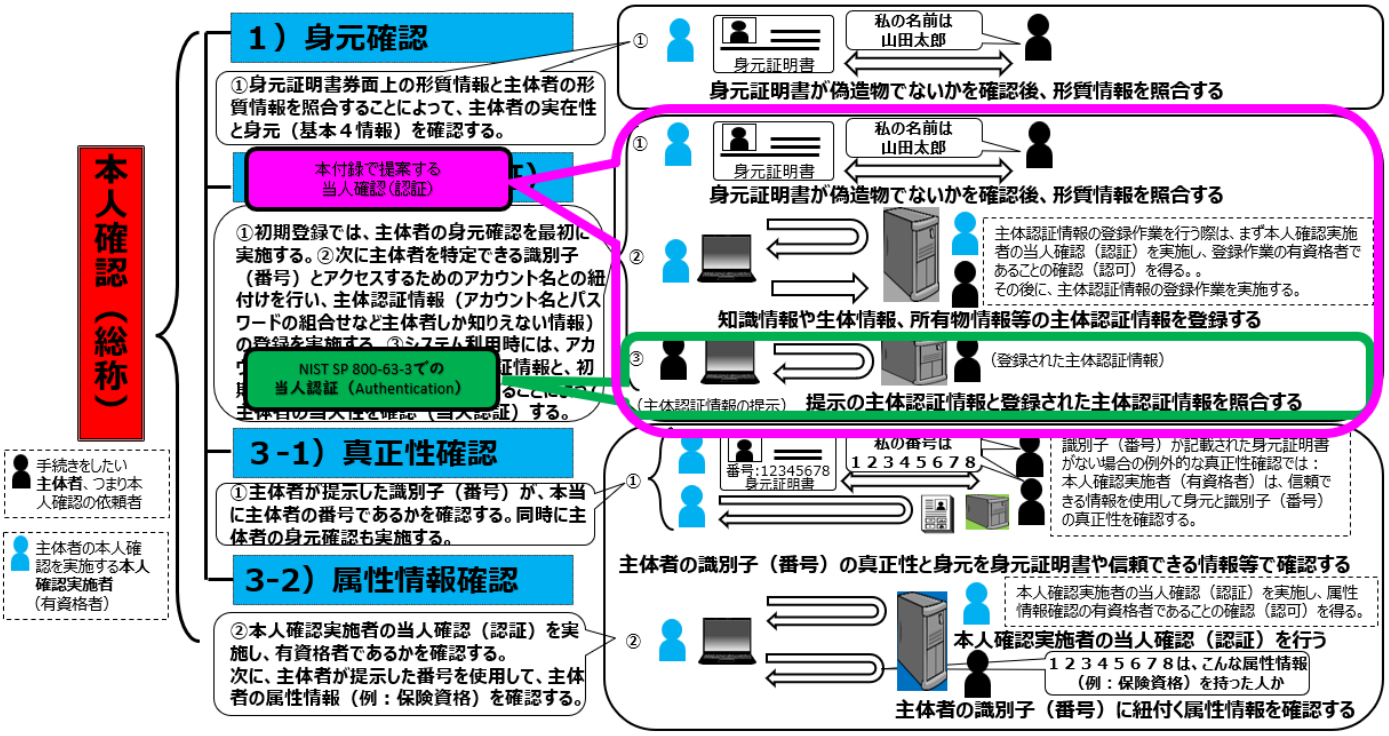
付番された識別子（番号）であること）を確認する」こと。識別子（番号）が記載された身元証明書がない場合の真正性確認手段については、５章で後述する。

（注）「NIST SP 800-63-3」では、関連する定義はない。

３-2）属性情報確認【オンライン環境を対象とする】

「本人確認実施者が、真正性確認された識別子（番号）を検索キーとして、情報システムを使用して主体者の属性情報（保険資格、住所、氏名、性別、生年月日など）を確認する」こと。なお、本人確認実施者は主体者の属性情報確認を実施するための情報システムにアクセスする権利の有資格者である必要がある。そのため、本人確認実施者は属性情報確認を実施する前に、自分の当人確認（認証）を行い有資格者であることの確認（認可）を得る必要がある。

（注）「NIST SP 800-63-3」では、関連する定義はない。



【図２】本付録提案の「当人確認（認証）」と「NIST SP 800-63-3」の当人認証の違い

2.3. 現在のマイナンバー制度における「本人確認」の定義

現在のマイナンバー制度では、「本人確認」という用語が明確に定義されないまま、多様な意味合いで使用されている。以下に例を示す。

・「犯罪収益移転防止法施行規則第６条第１項第１号ワ方式」での「本人確認」は、署名用電子証明書と６桁暗証番号を使用した照合による「身元確認」の意味で使用されている。「本人確認書類」は具体的な書類の例をあげているが、「本人確認」という用語の明確な定義はされていない。

・マイナ保険証を使用した「本人確認」は、「マイナ保険証を使用して当人確認（認証）を実施し、その後保険資格などの属性情報確認を行う」の意味で使用されている。しかし、マイナ保

険証を利用する際に必要な「本人確認」は本来「身元確認」である。今のマイナンバー制度では、マイナンバーカードの利用者証明用電子証明書と４桁暗証番号を使用して当人確認（認証）を行い、その裏側で利用者証明用電子証明書のペアとして登録されている署名用電子証明書を照合することにより「身元確認」を実施したとみなすイレギュラーな仕組みが構築されている。今のマイナ保険証の「本人確認」は、署名用電子証明書と６桁暗証番号を使用した照合をしていないケースがあるため、厳密にいうと「身元確認」はできていない、と言える。

・マイナンバーカードを使用したマイナンバーの「本人確認」は、マイナンバーの「真正性確認」の意味で使用されている。現在のマイナンバー制度におけるマイナンバーカード導入のそもそもの目的は、このマイナンバーの「真正性確認」であるため、このことをマイナンバーの「本人確認」と呼んでいる。

・「本人確認ガイドライン改定方針 令和５年度中間とりまとめ」の中では明確な「本人確認」の定義はないが、「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」の中では、「本人確認」を以下のように定義している。

「手続を行う人が実在する本人であるかを確認すること。代理人が本人に代わって手続を行う場合には、本人から正当な代理権が付与されていることを確認することも含む。」

本付録で提案している「身元確認」のことを意味しており、非常に曖昧な定義がされていると言わざるを得ない。

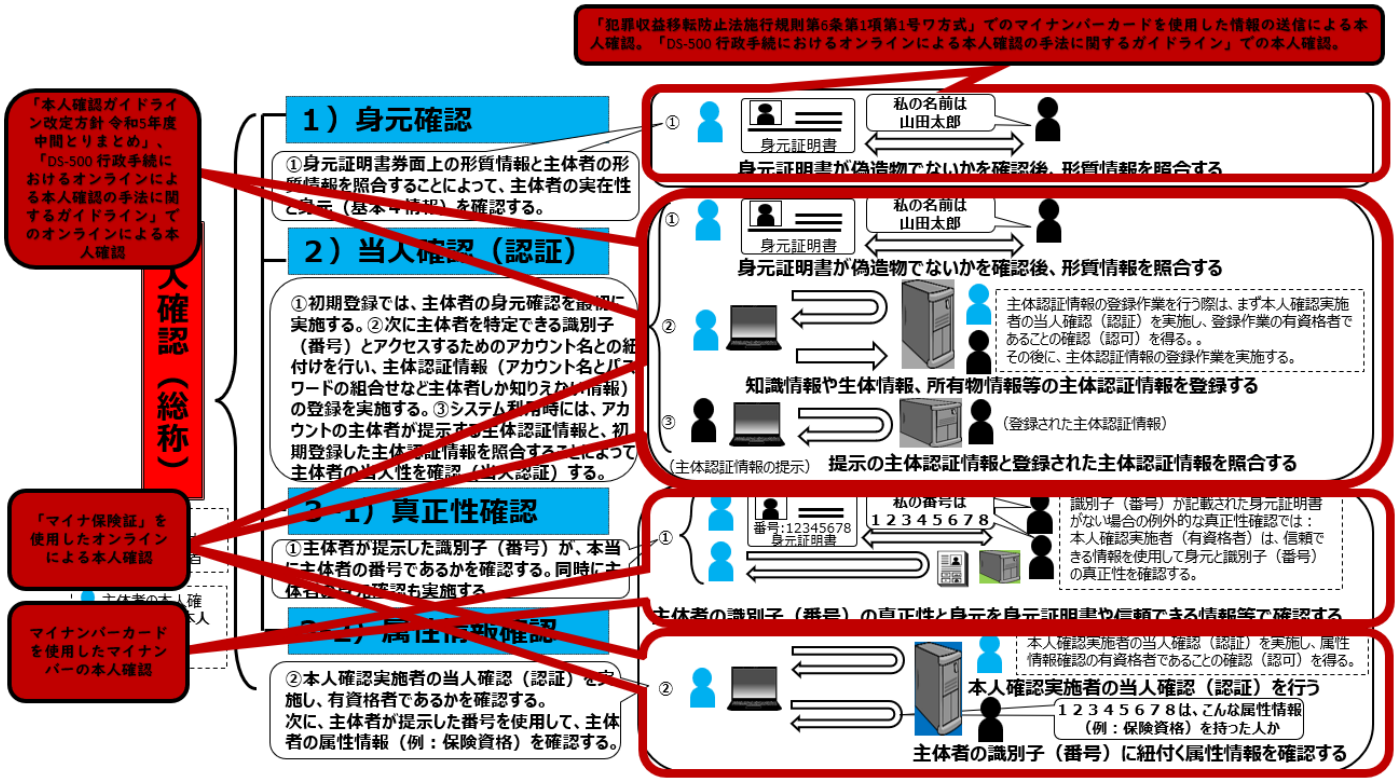
・「DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン」の中では、「オンラインによる本人確認」を以下のように定義している。

「オンラインにおける本人確認の手法の総称のこと。本人確認並びに非改ざん性の確保及び事実否認の防止をするために行う行為を含む。具体的には本人による電子署名、主体認証による直接的な確認方法だけではなく、アクセスログ、電子メール送付等のプロセスの記録を活用し間接的に本人確認を行う確認方法を含む。さらに、電子文書上の氏名等が記名された文書の保存であっても、そのプロセスにより本人確認が可能なものも含む。」このように曖昧な定義がされているが、本付録で提案している「当人確認（認証）」の意味である。つまり、「当人確認（認証）」における「『身元確認』＋『登録』＋『当人性の確認（当人認証）』」の意味で使用されている。

現在のマイナンバー制度における「本人確認」の定義および使用状況を、本付録の定義にマッピングしたものを図３に示す。現在のマイナンバー制度においては、「本人確認」という用語が曖昧に定義され、多様に使用されていることが見て取れる。おそらく「NIST SP 800-63-3」のガイドライン全体を「本人確認」と拡大解釈してしまい、日本特有の「本人確認」という概念を曖昧な定義のまま創作してしまったことに起因していると思われる。「NIST SP 800-63-3」は、あくまでも本付録でいうところの「当人確認（認証）」のガイドラインでしかない（図４参照）。

なお、「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」では「本人確認」の定義をオンラインに限定しているが、「本人確認ガイドライン改定方針

令和５年度中間とりまとめ」では、「オンラインだけでなく対面等での本人確認も『オンラインによる本人確認』の適用対象に含める」と書かれている。



【図３】現在のマイナンバー制度における「本人確認」の図Ｉへのマッピング

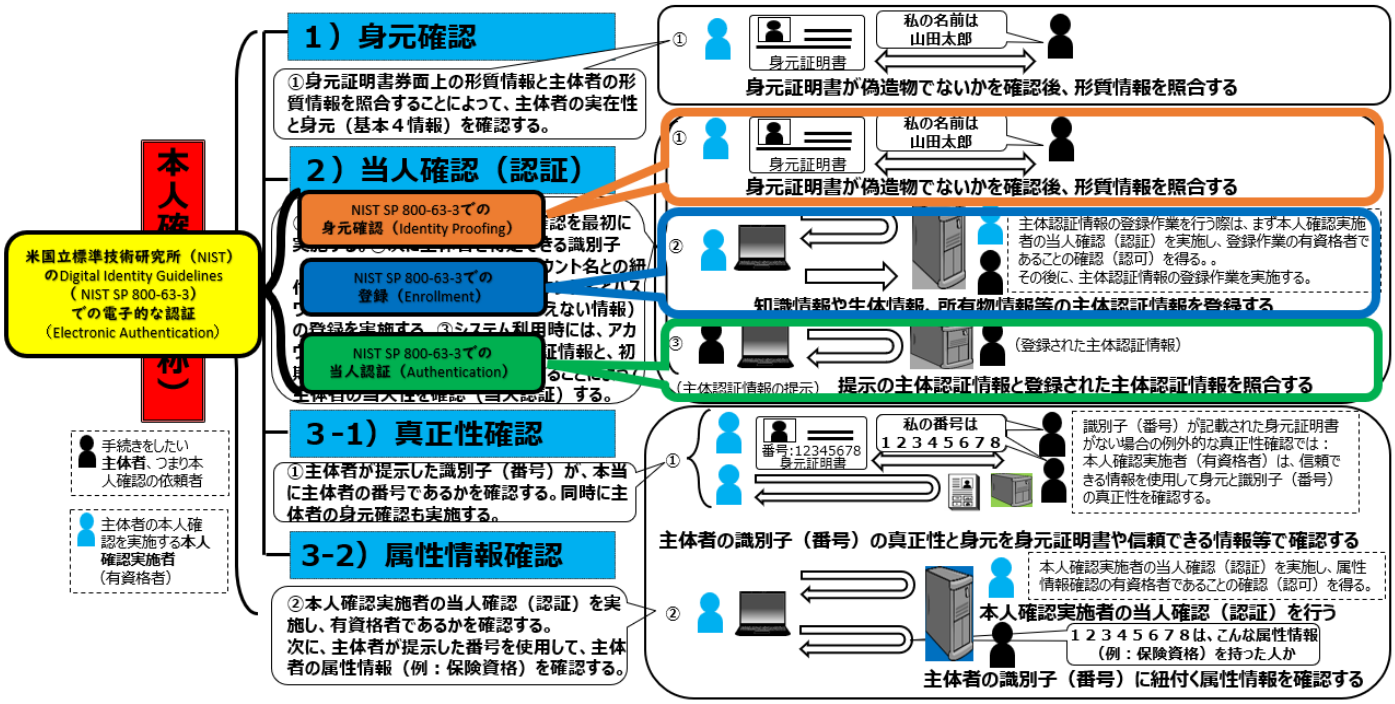
2.4.「NIST SP 800-63-3」における「本人確認」の定義

「米国立標準技術研究所（NIST）の Digital Identity Guidelines 第３版（NIST SP 800-63-3)」）においては、「本人確認」の明確な定義はされていない。そして、このガイドラインの目的としては、「政府機関に対して『Digital Authentication（電子的な認証)』の実装に際した技術的なガイドラインを提示する」と書かれている。

「Digital Authentication（電子的な認証)」のことを「電子的な本人確認」と翻訳されるケースが散見されるが、誤解を発生させる原因となるので止めることを提案する。前述したように、本付録における「当人確認（認証)」は「NIST SP 800-63-3」の全体の目的として書かれている「Electronic Authentication」（一般的な翻訳は、「電子的な認証」）に該当する。

なお、「NIST SP 800-63-4（ドラフト版)」では、「ID 連携（Federation)」についても言及しているが、本付録では対象外とする。

図４に「NIST SP 800-63-3」の機能を本付録の提言内容にマッピングしたものを示す。



【図４】「NIST SP 800-63-3」機能の図Ⅰへのマッピング

3．身元確認

3.1.「身元確認」の定義

本節では、「身元確認」を以下のように定義することを提案する。

「本人確認実施者が、なんらかの手続きを行いたい主体者の身元を確認することである。手続きやサービスの主体者を一意に識別するため、厳密な手順で作成された身元証明書の真正性（偽造品でないか）の確認、主体者と身元証明書の紐付けの検証等を行うことで、次のような事項を確認するプロセスから構成される。

・主体者が身元証明書に記載された人物と同一の人物であること
・主体者が現実に存在している人物であること（架空の人物でないこと）
・主体者が生存している人物であること（実在性確認）
・当該手続き/サービスにおいて同一人物が既に登録されていないこと
・主体者の身元情報（基本４情報）を確認すること　等」

（注）「NIST SP 800-63-3」では、上記の「主体者の身元情報（基本４情報）を確認すること」の違いを除いた上記の確認を「Identity Proofing」と呼び、一般的には「身元確認」と翻訳されている。

なお、主体者がなんらかの理由（大規模災害など）により身元証明書を所有しない場合は、例外的な身元確認を実施する仕組みも用意する必要がある。例えば、主体者から主体者以外が知るのが難しい属性情報（基本４情報、家族情報、勤務先情報など）を複数提示してもらい、信頼できる情報源（情報システムや紙の台帳など）が持つ属性情報と照合することにより身元確認を実施する仕組みの用意である。

3.2.「身元確認」の厳密度（保証レベル）の定義

「身元確認」は、手続きやサービスに要求される「身元確認」の厳密度（保証レベル）に合った確認方法を実施することによって、確認の信頼性を保証することになる。過去の提言書でも触れたように、１枚の身元証明書を常時携行して、全ての手続きやサービスにおいて１枚の身元証明書を使用することは、逆にセキュリティリスクが高まることに繋がるからである。

以下の表に、「身元確認」の保証レベル（IAL（Identity Assurance Level））の定義を提案する。

なお、本付録で提案する「身元確認」は、「NIST SP 800-63-3」の「身元確認（Identity Proofing)」とほぼ同義であるため、その保証レベルの考え方を参考にしている。

「身元確認」の保証レベル：IAL	レベルの定義
レベル３（IAL3）	対面で厳密な身元確認を実施している。法令で定められた身元証明書の真正性の確認（偽造物ではないことの確認）をした上で、対面で主体者と身元証明書上の記載人物との同一性が確認されている。必要に応じて、追加で本人しか知りえない情報（暗証番号や属性情報）の確認をしている。 （注）ここで使用している真正性の確認は、身元証明書の真正性（偽造物でないこと）を確認することである。本付録で提案している「真正性確認」は、識別子（番号）が本人に対して付番されたものであることを確認することである。
レベル２（IAL2）	対面もしくは遠隔で多少厳密性の低い身元確認を実施している。身元証明書の真正性の確認（偽造物ではないことの確認）か主体者と身元証明書上の記載人物との同一性確認に曖昧性がある。 主体者から身元証明書の提示がない場合、主体者から主体者以外が知ることが難しい属性情報（基本４情報、家族情報、勤務先情報など）をできるだけ多く提示してもらい、信頼できる情報源（情報システムや紙の台帳など）が持つ属性情報と照合を行い身元の確認を行う。
レベル１（IAL1）	厳密な身元確認を実施していない。自己申告も可。

4．当人確認（認証）

4.1.「当人確認（認証）」の定義

本節では、「当人確認（認証）」を以下のように定義することを提案する。

「まず、本人確認実施者が、オンラインサイトを利用したい主体者の身元確認を行う。次に、主体認証情報の登録資格を有する本人確認実施者が、主体認証情報の登録を行う。そして、オンラインサイトを実際に利用する際には、主体者が提示する主体認証情報と事前に登録された主体認証情報を照合することによって、主体者の当人性を確認することである。なお、この照合作業は本人確認実施者が行う作業であるが、主体者が情報システムを使用して人手を介さずに電子的に照合が行われるのが一般的である。

以下のような脅威への対策として、認証の３要素である知識・所有物・生体の１つ又は複数を組み合わせた主体認証情報を用いる。

・主体認証情報の推測・盗聴・分析
・中間者攻撃・リプレイ攻撃
・フィッシング/ファーミング
・リアルタイム型フィッシング
・多要素認証疲労攻撃　等」

（注）この「当人確認（認証）」のプロセスは、「NIST SP 800-63-3」での「Digital Authentication」に該当し、一般的には「電子的な認証」と翻訳されている。なお、「NIST SP 800-63-3」の表紙には、「Digital Identity Guidelines」と記載されている。この翻訳として、一部において「電子的な本人確認ガイドライン」と訳されているため、「NIST SP 800-63-3」のことを「本人確認ガイドライン」と誤解してしまうケースが発生している。「NIST SP 800-63-3」では、本人確認という用語は定義されておらず、このガイドラインの目的には「Digital Authentication（電子的な認証）の実装のための技術的ガイドライン」としか記載されていないことを認識していただきたい。

つまり、「当人確認（認証）」は以下の３つのプロセスから構成される。

１）主体者の身元確認のプロセス

まず、「本人確認実施者が、オンラインサイトを利用したい主体者を識別するための身元確認を実施する」

（注）「NIST SP 800-63-3」の「Identity Proofing」に該当し、一般的には「身元確認」と翻訳されている。

２）主体認証情報を登録するプロセス

次に、「本人確認実施者が、当人性を確認するために必要な主体認証情報（アカウント名と

パスワードなどの本人しか知りえない知識情報や、本人しか持ち得ない生体情報、所有物情報）を登録する」なお、本人確認実施者は、主体認証情報を登録できる有資格者である必要があるため、登録作業前に本人確認実施者の当人確認（認証）を実施し、登録権限の確認（認可）を得る必要がある。

加えて、主体認証情報は主体者を一意に特定するための識別子（番号）と紐付いている必要がある。現在のマイナンバー制度では識別子（番号）として電子証明書のシリアル番号を使用しているが、提言書補足２で提案したように、その使用は止めて「名寄せ用番号」を使用するべきである。

（注）「NIST SP 800-63-3」の「Enrollment」に該当し、一般的には「登録」と翻訳されている。

３）当人性の確認をするプロセス

そして、「主体者がオンラインサイトを実際に利用する際には、登録した主体認証情報と主体者が提示した主体認証情報を照合することによって、主体者が主体認証情報を登録した者と同一人物であること（当人性）を確認する」この照合作業は本人確認実施者が行う作業であるが、主体者が情報システムを使用して人手を介さずに電子的に照合が行われるのが一般的である。

（注）「NIST SP 800-63-3」の「Authentication」に該当し、一般的には「当人認証」と翻訳されている。

4.2.「当人確認（認証）」の厳密度（保証レベル）の定義

「当人確認（認証）」は、オンラインサイトの利用の際に要求される厳密度（保証レベル）に合った確認方法を実施することによって、確認の信頼性を保証することになる。提言書補足２で提案したように、１つの「当人確認（認証）」方法で全てのオンラインサイトを利用可能にすることは止めた方がよい、１つの方法が突破されてしまうと全てのオンラインサイトが利用可能となってしまいセキュリティリスクが高まることに繋がるからである。以下に、「当人確認（認証）」の保証レベル（TAAL（Total Authentication Assurance Level））の定義を提案する。

「当人確認（認証）」のプロセスは、4.1 節で述べた３つのプロセスから構成されるため、まずその３つのプロセスの厳密度（保証レベル）を定義する必要がある。そして、その３つの厳密度（保証レベル）の掛け合わせによって、「当人確認（認証）」の厳密度（保証レベル）を定義することを提案する。

１)主体者の身元確認プロセスの厳密度（保証レベル）：IAL の定義

3.2 節で提案した「身元確認」の厳密度（保証レベル）の定義をそのまま使用することを提案する。

「身元確認」の保証レベル：IAL	レベルの定義
レベル３（IAL3）	対面で厳密な身元確認を実施している。法令で定められた身元証明書の真正性の確認（偽造物ではないことの確認）をした上で、対面で主体者と身元証明書上の記載人物との同一性が確認されている。必要に応じて、追加で本人しか知りえない情報（暗証番号や属性情報）の確認をしている。 （注）ここで使用している真正性の確認は、身元証明書の真正性（偽造物でないこと）を確認することである。本付録で提案している「真正性確認」は、識別子（番号）が本人に対して付番されたものであることを確認することである。
レベル２（IAL2）	対面もしくは遠隔で多少厳密性の低い身元確認を実施している。身元証明書の真正性の確認（偽造物ではないことの確認）か主体者と身元証明書上の記載人物との同一性確認に曖昧性がある。 主体者から身元証明書の提示がない場合、主体者から主体者以外が知ることが難しい属性情報（基本４情報、家族情報、勤務先情報など）をできるだけ多く提示してもらい、信頼できる情報源（情報システムや紙の台帳など）が持つ属性情報と照合を行い身元の確認を行う。
レベル１（IAL1）	厳密な身元確認を実施していない。自己申告も可。

２）主体認証情報を登録するプロセスの厳密度（保証レベル）:EAL の定義

まず、本人確認実施者は、主体認証情報を登録できる有資格者である必要があるため、登録前に本人確認実施者の「当人確認（認証）」を実施し、登録権限を認可される必要がある。つまり、主体認証情報を登録するプロセスの厳密度を高めるためには、登録を行う情報システムにおいて、本人確認実施者に対して高い厳密度での「当人確認（認証）」の実施と、厳密な登録権限の認可を行う必要がある。

本人確認実施者が主体認証情報を登録するプロセスの厳密度（本付録では、簡略化して「登録」の保証レベルと呼ぶ）：EAL（Enrollment Assurance Lebel）の定義を、以下の表に提案する。

「登録」の保証レベル：EAL	レベルの定義
レベル３（EAL3）	TAAL３レベルで本人確認実施者の当人確認（認証）を行い、本人確認実施者が登録作業の有資格者であることが確認（認可）されている。その状

	況下で、本人確認実施者が、厳密な手順で主体認証情報の登録作業を実施している。
レベル２（EAL2）	TAAL2 レベルで本人確認実施者の当人確認（認証）を行い、登録作業の有資格者であることが確認（認可）されている。もしくは、その後の主体認証情報の登録作業が、多少厳密性の低い手順で実施されている。
レベル１（EAL1）	TAAL1 レベルで本人確認実施者の当人確認（認証）が行われているか、厳密性の低い主体認証情報の登録作業が行われている。自己登録も可。

３）当人性の確認の厳密度（保証レベル）:AAL の定義

登録した主体認証情報と主体者が提示した主体認証情報を照合することによって、主体者が主体認証情報を登録した者と同一人物であること（当人性）を確認する厳密度（保証レベル）: AAL（Authentication Assurance Level）の定義を以下に提案する。この照合作業は本人確認実施者が行う作業であるが、主体者が情報システムを使用して人手を介さずに電子的に照合が行われるのが一般的である。

なお、本付録で提案する当人性の確認は、「NIST SP 800-63-3」の当人認証（Authentication）とほぼ同義であるため、その保証レベルの考え方を参考にしている。

「当人性の確認」の保証レベル：AAL	レベルの定義
レベル３（AAL3）	耐タンパー性ハードウェアを含む２要素（知識情報、生体情報、所有物情報から２要素）以上の認証で当人性の確認が行われている。
レベル２（AAL2）	２要素以上の認証で当人性の確認が行われている。
レベル１（AAL1）	単要素の認証で当人性の確認が行われている。

４）「当人確認（認証）」の厳密度（保証レベル）:TAAL の定義

本節では、「当人確認（認証）」の厳密度（保証レベル）の定義を「TAAL（Total Authentication Assurance Level）」と呼び、以下の定義を提案する。

「当人確認（認証）」の保証レベル：TAAL	レベルの定義
レベル３（TAAL3）	手続きやサービス利用時に厳密度の高い当人性の確認がされている。加えて、主体認証情報登録時には、主体者の厳密な身元確認がされている。主体認証情報の登録作業は、本人確認実施

	者に対して厳密な登録作業の有資格者であることの確認がされた状況下で、厳密な手順で実施されている。
レベル２（TAAL2）	手続きやサービス利用時に多少厳密度の低い当人性の確認がされている。もしくは、主体認証情報登録時に、主体者の身元確認および主体認証情報の登録作業のいずれかの厳密度が低くなっている。
レベル１（TAAL1）	当人確認（認証）プロセスの厳密な作業が行われていない。

TAALの厳密度（保証レベル）は、上記１）～３）の３つの厳密度（保証レベル）の掛け合わせで決定されるが、３つの厳密度（保証レベル）の掛け合わせの中で１番低い厳密度（保証レベル）が、TAALの厳密度（保証レベル）となる。例えば、IALがレベル３・EALがレベル３・AALがレベル１の場合には、「当人確認（認証）」を構成するプロセスの中で１番保証レベルが低いAALがレベル１であるため、TAALの保証レベルはレベル１となる。つまり、TAALの厳密度（保証レベル）がレベル３となるのは、IAL、EAL、AALの全ての厳密度（保証レベル）がレベル３の時だけである。

「当人確認（認証）」の保証レベル：TAAL		「身元確認」の保証レベル:IAL	「登録」の保証レベル：EAL	「当人性の確認」の保証レベル：AAL
レベル３（TAAL3）	＝	レベル３（IAL3）	レベル３（EAL3）	レベル３（AAL3）
レベル２（TAAL2）	＝	レベル２（IAL2）以上	レベル２（EAL2）以上	レベル２（AAL2）以上
レベル１（TAAL1）	＝	レベル１（IAL1）以上	レベル１（EAL1）以上	レベル１（AAL1）以上

4.3.「当人確認（認証）」プロセスのリアル世界（銀行印の使用例）での検証

本付録での「当人確認（認証）」の定義は、あくまでもオンラインサイトを利用する際の定義に限定している。参考までに、「銀行での口座開設と入出金」の当人確認を例にして、オンラインが普及していなかった時代に行われていたリアル世界の「当人確認~~（認証）~~」と、ネット時代のデジタル世界の「当人確認（認証）」の仕組みを比較して、違いを検証してみる。ちなみに、リアル世界では認証という概念はないので、本付録で定義している「当人確認（認証）」は「当人確認~~（認証）~~」と表現している。

（注）「NIST SP 800-63-3」においては、目的に「Digital Authentication（電子的な認証）」の実装と書かれているように、デジタル世界での定義に限定されている。

１）リアル世界での「当人確認~~（認証）~~」の例

①主体者の身元確認のプロセス

・対面で、銀行口座開設（預金通帳発行）申請時に、身元証明書を使用して主体者の身元確認を実施する。

②主体認証情報を登録するプロセス

・対面で、主体者の個人情報を確認し登録する。

・対面で、銀行印（デジタル世界の主体認証情報に該当）を登録する。

・対面で、預金通帳を発行する。

③当人性の確認をするプロセス

・対面で、提示された「預金通帳＋銀行印」の「銀行印」を照合して入出金を行う。

２）デジタル世界での「当人確認（認証)」(預金通帳を発行しないケース）の例

①主体者の身元確認のプロセス

・対面もしくは遠隔で、銀行口座開設申請時に、身元証明書を使用して主体者の身元確認を実施する。

②主体認証情報を登録するプロセス

・対面もしくは遠隔で、主体者の個人情報を確認し登録する。

・対面もしくは遠隔で、暗証番号などの主体認証情報を登録する。

③当人性の確認をするプロセス

・遠隔で、主体認証情報を電子的に照合して入出金を行う。

5．真正性確認と属性情報確認

5.1.「真正性確認と属性情報確認」の定義

本節では、「真正性確認と属性情報確認」を以下のように定義することを提案する。なお、「真正性確認」と「属性情報確認」はペアで実施されることを基本とするため、２つ合わせて１つの本人確認プロセスとして定義する。

「まず、本人確認実施者は、なんらかの手続きを行いたい主体者が提示する識別子（番号）が主体者に対して付番された正しい番号であることを確認（真正性確認）する。
そして、本人確認実施者が、真正性確認された識別子（番号）を検索キーとして、情報システムを使用して主体者の属性情報（保険資格、住所、氏名、性別、生年月日など）確認をすることである。なお、本人確認実施者は属性情報確認を実施することができる有資格者である必要があるため、属性情報確認作業前に本人確認実施者の当人確認（認証）を実施し、属性情報確認権限の確認（認可）を得る必要がある。」

上記のように、「真正性確認と属性情報確認」は、以下の２つのプロセスから構成される。

１）識別子（番号）の真正性確認のプロセス

まず、「本人確認実施者は、主体者の識別子（番号）が主体者に対して付番された正しい番号であることを確認（真正性確認）する」。本人確認実施者は、主体者が提示する識別子（番号）が記載された身元証明書を使用して、主体者の身元確認を実施すると同時に識別子（番号）の真正性確認を実施する」

なお、主体者がなんらかの理由（大規模災害など）により識別子（番号）が記載された身元証明書を所有しない場合は、例外的な真正性確認を実施する仕組みも用意する。例えば、主体者から主体者以外が知るのが難しい属性情報（基本４情報、家族情報、勤務先情報など）を複数提示してもらい、信頼できる情報源（情報システムや紙の台帳など）が持つ属性情報と照合することにより真正性確認を実施する仕組みの用意である。

２）属性情報確認のプロセス

そして、「本人確認実施者は、真正性確認された識別子（番号）を検索キーとして、情報システムを使用して主体者の属性情報（保険資格、住所、氏名、性別、生年月日など）を確認する」なお、属性情報確認では、本人確認実施者は情報システムを使用して主体者の様々な個人情報を参照し使用することになるため、本人確認実施者は主体者の属性情報を参照・使用できる有資格者である必要がある。そのため、属性情報確認前に本人確認実施者の当人確認（認証）を実施し、属性情報確認権限の確認（認可）を得る必要がある。

5.2.「真正性確認と属性情報確認」の厳密度（保証レベル）の定義

「真正性確認と属性情報確認」の保証レベル（IAAAL（Identifier Authenticity Attribute Assurance Level）の定義を以下に提案する。

「真正性確認と属性情報確認」のプロセスは、5.1 節で述べた２つのプロセスから構成されるため、まずその２つのプロセスの厳密度（保証レベル）を定義する必要がある。そして、その２つの厳密度（保証レベル）の掛け合わせによって、「真正性確認と属性情報確認」の厳密度（保証レベル）を定義することを提案する。

１)識別子（番号）の真正性確認のプロセスの厳密度（保証レベル）：IAAL の定義

識別子（番号）の「真正性確認」は、手続きやサービスに要求される「真正性確認」の厳密度（保証レベル）に合った確認方法を実施することによって、確認の信頼性を保証することになる。

以下の表に、「真正性確認」の保証レベル（IAAL（Identifier Authenticity Assurance Level)）の定義を提案する。

「真正性確認」の保証レベル：IAAL	レベルの定義
レベル３（IAAL3）	IAL3 レベルでの身元確認を実施し、提示された信頼できる身元証明書に記載された識別子（番号）を確認している。必要に応じて、追加で本人しか知りえない情報（暗証番号や属性情報）の確認をしている。
レベル２（IAAL2）	IAL２レベルで対面もしくは遠隔で多少厳密性の低い身元確認を実施し、提示された身元証明書に記載された識別子（番号）を確認している。 なお、大規模災害などにより識別子（番号）が記載された身元証明書を所有しない場合は、主体者から主体者しか知りえない属性情報を複数提示してもらい、信頼できる情報源（情報システムや紙の台帳など）が持つ属性情報と照合することにより真正性確認を実施する。
レベル１（IAAL1）	識別子（番号）は自己申告レベルであり、真正性確認がとれていない。

２）属性情報確認のプロセスの厳密度（保証レベル）:AIAL の定義

属性情報確認では、主体者の様々な個人情報について、本人確認実施者が情報システムを使用して参照し使用することになる。そのため、属性情報確認を実施するためには、事前に本人確認実施者の「当人確認（認証)」を実施し、本人確認実施者が属性情報確認作業の有資格者であることの確認（認可）を得る必要がある。つまり、属性情報確認プロセスの厳密度を高める

ためには、属性情報確認を行う情報システムにおいて、本人確認実施者に対して高い厳密度での「当人確認（認証）」の実施と、厳密な属性情報確認権限の認可を行う必要がある。

「属性情報確認」の保証レベル（Attribute Information Assurance Level）の定義を、以下の表に提案する。

「属性情報確認」の保証レベル：AIAL	レベルの定義
レベル３（AIAL3）	TAAL３レベルで本人確認実施者の当人確認（認証）を行い、本人確認実施者が属性情報確認作業の有資格者であることの確認（認可）が厳密にされている。その状況下で、本人確認実施者が厳密な手順で属性情報確認作業を実施している。
レベル２（AIAL2）	TAAL2 レベルで本人確認実施者の当人確認（認証）を行い、本人確認実施者が属性情報確認作業の有資格者であることの確認（認可）の厳密性が少し低い。もしくは、その後の属性情報確認作業が、多少厳密性の低い手順で実施されている。
レベル１（AIAL1）	TAAL1 レベルで本人確認実施者の当人確認（認証）が行われ、本人確認実施者が属性情報確認作業の有資格者であることの確認（認可）が行われていない。属性情報確認作業の手順も厳密ではない。

３）「真正性確認と属性情報確認」の厳密度（保証レベル）:IAAAL の定義

本節では、「真正性確認と属性情報確認」の厳密度（保証レベル）の定義を「IAAAL（Identifier Authenticity Attribute Assurance Level)」と呼び、以下の内容を提案する。

「真正性確認と属性情報確認」の保証レベル：IAAAL	レベルの定義
レベル３（IAAAL3）	厳密度の高い番号の真正性確認が実施され、本人確認実施者が主体者の属性情報確認作業の有資格者であることの確認が厳密に実施された状況下で、厳密な手順で属性情報確認作業が実施されている。
レベル２（IAAAL2）	厳密度の低い番号の真正性確認の実施、あるいは本人確認実施者が主体者の属性情報

	確認の有資格者であることの確認が低い厳密度で実施された状況下で、厳密度の低い手順で属性情報確認作業が実施されている。
レベル１（IAAAL1）	識別子（番号）の真正性確認が行われていない、あるいは本人確認実施者が主体者の属性情報確認の有資格者であることの確認が実施されていない。

IAAAL の厳密度（保証レベル）は、上記１）～2）の２つの厳密度（保証レベル）の掛け合わせで決定されるが、２つの厳密度（保証レベル）の掛け合わせの中で低い方の厳密度（保証レベル）が、IAAAL の厳密度（保証レベル）となる。例えば、IAAL がレベル３・AIAL がレベル１の場合には、低い保証レベルが AIAL のレベル１であるため、IAAAL の保証レベルはレベル１となる。つまり、IAAL の厳密度（保証レベル）がレベル３となるのは、IAAL、AIAL の両方の厳密度（保証レベル）がレベル３の時だけである。

「真正性確認と属性情報確認」の保証レベル：IAAAL		「真正性確認」の保証レベル：IAAL		「属性情報確認」の保証レベル：AIAL
レベル３（IAAAL3）	＝	レベル３（IAAL3）	○	レベル３（AIAL3）
レベル２（IAAAL2）	＝	レベル２（IAAL2）以上	×	レベル２（AIAL2）以上
レベル１（IAAAL1）	＝	レベル１（IAAL1）以上	×	レベル１（AIAL1）以上

参考として、上記の表をより分かり易く書き換えた表を以下に記す。

属性情報確認 / 真正性確認	AIAL1	AIAL2	AIAL3
IAAL3	IAAAL1	IAAAL2	IAAAL3
IAAL2	IAAAL1	IAAAL2	IAAAL2
IAAL1	IAAAL1	IAAAL1	IAAAL1

6. まとめと事例検証

6.1. まとめ

本付録では、「本人確認」は、「身元確認」「当人確認（認証）」「真正性確認と属性情報確認」の３つから構成され、手続きやサービスから要求される厳密度（保証レベル）に合わせて、３つの確認プロセスを組み合わせて実施されるべきであることを提案した。以下に、保証レベルの概要をまとめる。

１）「身元確認」の厳密度（保証レベル）：IAL（Identity Assurance Level）

「身元確認」の保証レベル：IAL	レベルの定義
レベル３（IAL3） （事例検証） 6.2 3)①預金口座開設 6.2 3)②携帯電話契約	対面で厳密な身元確認を実施している。法令で定められた身元証明書の真正性の確認（偽造物ではないことの確認）をした上で、対面で主体者と身元証明書上の記載人物との同一性が確認されている。必要に応じて、追加で本人しか知りえない情報（暗証番号や属性情報）の確認をしている。 （注）ここで使用している真正性の確認は、身元証明書の真正性（偽造物でないこと）を確認することである。本付録で提案している「真正性確認」は、識別子（番号）が主体者本人に対して付番されたものであることを確認することである。
レベル２（IAL2） （事例検証） 6.2 3)④図書館カード作成	対面もしくは遠隔で多少厳密性の低い身元確認を実施している。身元証明書の真正性の確認（偽造物ではないことの確認）か主体者と身元証明書上の記載人物との同一性確認に曖昧性がある。 主体者から身元証明書の提示がない場合、主体者から主体者以外が知ることが難しい属性情報（基本４情報、家族情報、勤務先情報など）をできるだけ多く提示してもらい、信頼できる情報源（情報システムや紙の台帳など）が持つ属性情報と照合を行い身元の確認を行う。
レベル１（IAL1） （事例検証） 6.2 3)③ポイントカード作成	厳密な身元確認を実施していない。自己申告も可。

２）「当人確認（認証）」の厳密度（保証レベル）：TAAL（Total Authentication Assurance Level）

「当人確認（認証）」の保証レベル：TAAL	レベルの定義
レベル３（TAAL3） （事例検証） 6.2 2)④国家的機密情報へのアクセス、医療機関での要配慮個人情報へのアクセス	手続きやサービス利用時に厳密度の高い当人性の確認がされている。加えて、主体認証情報登録時には、主体者の厳密な身元確認がされている。主体認証情報の登録作業は、本人確認実施者に対して厳密な登録作業の有資格者であることの確認がされた状況下で、厳密な手順で実施されている。
レベル２（TAAL2） （事例検証） 6.2 2)①オンラインでの確定申告 6.2 2)②大学での教員の成績入力 6.2 2)③オンラインバンキングでの入出金 6.2 2)⑥マイナポータルへのアクセス	手続きやサービス利用時に多少厳密度の低い当人性の確認がされている。もしくは、主体認証情報登録時に、主体者の身元確認および主体認証情報の登録作業のいずれかの厳密度が低くなっている。
レベル１（TAAL1） 6.2 2)⑤フリー電子メールへのアクセス	当人確認（認証）プロセスの厳密な作業が行われていない。

３）「真正性確認と属性情報確認」の厳密度（保証レベル）：IAAAL（Identifier Authenticity Attribute Assurance Level）

「真正性確認と属性情報確認」の保証レベル：IAAAL	レベルの定義
レベル３（IAAAL3） （事例検証） 6.2 1)①医療機関での保険資格情報等の確認 6.2 1)②役所窓口での住所や氏名の変更	厳密度の高い番号の真正性確認が実施され、本人確認実施者が主体者の属性情報確認作業の有資格者であることの確認が厳密に実施された状況下で、厳密な手順で属性情報確認作業が実施されている。
レベル２（IAAAL2） （事例検証） 6.2 1)③大学での学生の成績の確認	厳密度の低い番号の真正性確認の実施、あるいは本人確認実施者が主体者の属性情報確認の有資格者であることの確認が低い厳密度で実施された状況下で、厳密度の低い手順で属性情報確認作業が実施されている。

レベルⅠ（IAAALⅠ） （事例検証） 6.2 Ⅰ)④現在、実際の事例としては数多く存在するが、本来はこういった仕組みは構築してはいけない	識別子（番号）の真正性確認が行われていない、あるいは本人確認実施者が主体者の属性情報確認の有資格者であることの確認が実施されていない。

4）本付録での「本人確認」に関する厳密度（保証レベル）の整理

略称	正式名	内容
IAL	Identity Assurance Level	「身元確認」の保証レベル （注）「NIST SP 800-63-3」で使用されている「Identity Proofing（身元確認）」の内容とほぼ同義
EAL	Enrollment Assurance Lebel	「当人確認（認証）」の中での主体認証情報の「登録」の保証レベル （注）本付録独自の提案
AAL	Authentication Assurance Level	「当人確認（認証）」の中での「当人性の確認」の保証レベル （注）「NIST SP 800-63-3」で使用されている「Authentication（当人認証）」の内容とほぼ同義
TAAL	Total Authentication Assurance Level	「当人確認（認証）」全体の保証レベル。IAL、EAL、AAL の掛け合わせで保証レベルが決まる。 （注）本付録独自の提案
IAAL	Identifier Authenticity Assurance Level	「真正性確認」の保証レベル。 （注）本付録独自の提案
AIAL	Attribute Information Assurance Level	「属性情報確認」の保証レベル。 （注）本付録独自の提案
IAAAL	Identifier Authenticity Attribute Assurance Level	「真正性確認と属性情報確認」全体の保証レベル。IAAL と AIAL の掛け合わせで保証レベルが決まる。 （注）本付録独自の提案

6.2. 事例検証

本節では、実際の業務が、本付録で提案した「身元確認」「当人確認（認証）」「真正性確認と属性情報確認」のどれに該当するかの検証結果を以下に示す。

1）「真正性確認と属性情報確認」の事例検証

①医療機関での保険資格・過去の診療情報確認のケース

・「真正性確認と属性情報確認」に該当

医療機関で、「顔写真付きの新保険証カード」を使用して記号番号・保険者番号の真正性確認を実施する（必要な保証レベル IAAL3）。次に、本人確認実施者である担当者（窓口事務員、医師）の有資格確認を実施後、担当者（窓口事務員、医師）は記号番号・保険者番号を検索キーとして使用して属性情報確認（保険資格や過去の診療情報など）を行う（必要な保証レベル AIAL3）。

・必要な厳密度（保証レベル）：IAAAL3

（注）現在の医療機関での保険資格・過去の診療情報確認のケースでは、まず真正性確認が不十分な状態にある。例えば、紙の健康保険証や資格確認書では身元確認ができていないし（保証レベル IAAL2or1 に相当）、マイナンバーカードを使用したケース（俗称はマイナ保険証）においても前述したように身元確認としては不十分である（保証レベル IAAL2 に相当）。そもそもマイナ保険証を使用した身元確認機能は、提言書（補足２）で指摘したように、別の情報セキュリティの問題が発生してしまうので設計を見直す必要がある。さらに、本人確認実施者である担当者（窓口事務員、医師）が属性情報確認（保険資格や過去の診療情報など）の有資格者であることの確認（認可）も不十分な状態にある（保証レベル AIAL2or1 に相当）。つまり、現在の医療機関での保険資格・過去の診療情報確認の保証レベルは、IAAAL1 もしくは IAAAL２のレベルである。本付録の提言に従って、保証レベルを IAAAL3 にあげる仕組みを構築することが望まれる。

その実現のためには、まず IAAL のレベル３を確保する必要があり、そのためには提言書（補足１）で提案したサブの身元証明書である「顔写真付きの新保険証カード」の導入が有効である。さらに、本人確認実施者である担当者（窓口事務員、医師）が属性情報確認（保険資格や過去の診療情報など）の有資格者であることの確認（認可）を厳密に行う必要があり、AIAL のレベル３を確保しなければならない。そのためには、提言書（補足２）で提案した耐タンパー性の「利用者証明用の IC カード（エストニア政府発行の eID カードに相当）」を発行して本人確認実施者である担当者（窓口事務員、医師）に貸与し、公的個人認証の仕組みを使用することが有効である。

②役所窓口での住所や氏名の変更のケース

・「真正性確認と属性情報確認」に該当

役所で、「新身元証明書カード」を使用して「名寄せ用番号」の真正性確認を実施する（必要な保証レベル IAAL3）。次に、本人確認実施者である担当者（役所職員）の有資格確認を実施後、担当者（役所職員）は、「名寄せ用番号」を検索キーとして使用して属性情報確認（住所や氏名）を行う（必要な保証レベル AIAL3）。

・必要な厳密度（保証レベル）：IAAAL3

（注）現在の役所窓口での住所や氏名の変更のケースでは、まず真正性確認は高い厳密度（保証レベル IAAL３に相当）で実施されている。しかし、現在実施されている本人確認実施者である担当者（役所職員）の有資格確認については厳密度に疑問が残る（保証レベル AIAL2orl に相当）。あらためて、本付録の提言に従って、IAAAL3 にあげる仕組みを構築することが望まれる。

その実現のためには、本人確認実施者である担当者（役所職員）が属性情報確認（住所や氏名）の有資格者であることの確認（認可）を厳密に行う必要があり、AIAL のレベル３を確保しなければならない。そのためには、提言書（補足２）で提案した耐タンパー性の「利用者証明用の IC カード（エストニア政府発行の eID カードに相当）」を発行して本人確認実施者である担当者（役所職員）に貸与し、公的個人認証の仕組みを使用することが有効である。

③大学で学生から教員へ成績の問合せがあったケース

・「真正性確認と属性情報確認」に該当

担当者（教員）は、「学生証」を使用して「学籍番号」の真正性確認を実施する（必要な保証レベル IAAL2）。次に、本人確認実施者である担当者（教員）の有資格確認を実施後、担当者（教員）は「学籍番号」を検索キーとして使用して属性情報確認（学生の成績）を行う（必要な保証レベル AIAL2）。

・必要な厳密度（保証レベル）：IAAAL2

（注）現在の大学教員が大学提供の情報システムを使用して学生の成績を確認するケースの当人性の確認では、単要素認証つまり保証レベルは AALl で行われている事が多く、現在の仕組みは IAAALl に該当する。将来的には、当人性の確認の保証レベルを AAL2 に変更して、「真正性確認と属性情報確認」の保証レベルを IAAAL2 にあげることが望まれる.

④IAAALl レベルの「真正性確認と属性情報確認」のケース

・「真正性確認」が行われていない（IAALl に相当）、もしくは本人確認実施者の「属性情報確認」の権限確認（認可）が厳密に実施されていないケースに該当（AIALl に相当）。

・必要な厳密度（保証レベル）：IAAALl

（注）IAAALl レベルの「真正性確認と属性情報確認」で確認した属性情報には信憑性がないため、実際にはこういった仕組みを構築してはいけない。しかし、上記①～③で事例検証したように現実には IAAALl レベルの「真正性確認と属性情報確認」が行われているのが実

態である。全ての「真正性確認と属性情報確認」は、IAAAL2 以上のレベルで実施されることが望まれる。

２)「当人確認（認証)」の事例検証

①オンラインでの確定申告（税務署発行の利用者識別番号を使用）のケース

・「当人確認（認証)」に該当

税務署で、「新身元証明書カード」を使用して主体者（オンラインで確定申告したい利用者）の身元確認を実施後（必要な保証レベル IAL3)、本人確認実施者（税務署で登録の資格を有する担当者）は主体認証情報（利用者識別番号と暗証番号）を登録する（必要な保証レベル EAL3)。国税庁提供の情報システム（e-Tax）を使用してオンラインで確定申告をする際には、主体者は情報システム（e-Tax）に主体認証情報を使用してログインして確定申告を行う（必要な保証レベル AAL2)。

・必要な厳密度（保証レベル)：TAAL2

（注）現在のオンラインでの確定申告（税務署発行の利用者識別番号を使用）の当人性の確認は、単要素認証つまり保証レベルは AAL1 で行われているため、現在の仕組みは TAAL1 に該当する。将来的には、当人性の確認の保証レベルを AAL2 に変更して、「当人確認（認証)」の保証レベルを TAAL2 にあげることが望まれる。その場合には、「利用者識別番号＋暗証番号」ではなく、提言書（補足２）で提案した「スマートフォンの利用者証明用電子証明書の格納情報（エストニア政府発行の Smart-ID に相当）＋暗証番号」の公的個人認証の仕組みを使用することが有効である。

②大学教員が大学提供の情報システムで学生の成績を入力するケース

・「当人確認（認証)」に該当

大学事務所で、「新身元証明書カード」を使用して主体者（大学教員）の身元確認を実施後（必要な保証レベル IAL3)、本人確認実施者（大学事務所で登録の資格を有する担当者）は主体認証情報（アカウント名と暗証番号）を登録する（必要な保証レベル EAL3)。成績入力を行う際には、主体者（大学教員）は大学提供の情報システムに主体認証情報を使用してログインして成績入力を行う（必要な保証レベル AAL2)。

・必要な厳密度（保証レベル)：TAAL2

（注）現在の大学教員が大学提供の情報システムで学生の成績を入力するケースの当人性の確認では、単要素認証つまり保証レベルは AAL1 で行われている事が多く、現在の仕組みは TAAL1 に該当する。将来的には、当人性の確認の保証レベルを AAL2 に変更して、「当人確認（認証)」の保証レベルを TAAL2 にあげることが望まれる。

③銀行でのオンラインバンキング利用手続きのケース

・「当人確認（認証)」に該当

銀行で、「新身元証明書カード」を使用して主体者（オンラインバンキングを使用したい人）の身元確認を実施後（必要な保証レベル IAL3）、本人確認実施者（銀行で登録の資格を有する担当者）は主体認証情報（アカウント名と暗証番号）を登録する（必要な保証レベル EAL3）。入出金や振り込みをする際には、主体者（オンラインバンキングを使用したい人）はオンラインバンキングの情報システムに主体認証情報を使用してログインして入出金や振り込みを行う（必要な保証レベル AAL2）。

・必要な厳密度（保証レベル）：TAAL2

（注）以前の銀行のオンラインバンキングの当人性の確認では、単要素認証つまり保証レベルは AAL1 で行われている事例が多くみられた。現在では AAL2 に変更して「当人確認（認証）」の保証レベルを TAAL2 にあげているケースが増えているが、全ての銀行において当人性の確認の保証レベルを AAL2 に変更して「当人確認（認証）」の保証レベルを TAAL2 にあげることが望まれる。

④国家的な機密性の高い情報にアクセスするケース

・「当人確認（認証）」に該当

担当部署で、「新身元証明書カード」を使用して主体者（国家的機密情報にアクセスしたい人）の身元確認を実施後（必要な保証レベル IAL3）、本人確認実施者（担当部署で登録の資格を有する担当者）は、提言書（補足２）で提案した耐タンパー性の「利用者証明用の IC カード（エストニア政府の eID カードに相当）」を発行し、必要な主体認証情報（「利用者証明用の IC カード」の電子証明書と暗証番号など）を登録する（必要な保証レベル EAL3）。国家的機密情報にアクセスする際には、主体者（国家的機密情報にアクセスしたい人）は情報システムに主体認証情報（「利用者証明用の IC カード」の電子証明書と暗証番号など）を使用してログインして機密性の高い情報にアクセスする（必要な保証レベル AAL3）。つまり、提言書（補足２）で提案した「利用者証明用の IC カード（エストニア政府発行の eID カードに相当）」を貸与し、公的個人認証の仕組みを使用することが有効である。

・必要な厳密度（保証レベル）：TAAL3

（注）医療機関などにおいて、医師や医療事務担当者が患者の要配慮個人情報（診療履歴や病歴など）にアクセスする場合も、国家的機密情報にアクセスするケースと同様に TAAL3 の保証レベルが必要であり、「利用者証明用の IC カード（エストニア政府発行の eID カードに相当）」を貸与し、公的個人認証の仕組みを使用することが有効である。

⑤フリーの電子メールサイトでメールアドレスを作成して利用するケース

・「当人確認（認証）」に該当

電子メールサイトで、主体者（電子メールを利用したい人）の身元確認を実施せずに（必要な保証レベル IAL1）、主体認証情報（アカウント名と暗証番号）の登録も主体者が自ら

実施する（必要な保証レベル EAL1）。電子メールを利用する際には、主体者（電子メールを利用したい人）は電子メールサイトに主体認証情報を使用してログインして電子メールを利用する（必要な保証レベル AAL1）。

・必要な厳密度（保証レベル）：TAAL 1

⑥マイナポータルへアクセスするケース

・「当人確認（認証）」に該当

担当部署で、「新身元証明書カード」を使用して主体者（マイナポータルにアクセスしたい人）の身元確認を実施後（必要な保証レベル IAL3）、本人確認実施者（担当部署で登録の資格を有する担当者）は、主体認証情報（提言書（補足２）で提案した「スマートフォンの利用者証明用電子証明書の格納情報（エストニア政府発行の Smart-ID に相当）＋暗証番号」）を登録する（必要な保証レベル EAL3）。マイナポータルにアクセスする際には、主体者（マイナポータルにアクセスしたい人）はマイナポータルに主体認証情報（「スマートフォンの利用者証明用電子証明書の格納情報（エストニア政府発行の Smart-ID に相当）＋暗証番号」）を使用してログインして、情報の参照や公的な手続きを行う（必要な保証レベル AAL2）。

・必要な厳密度（保証レベル）：TAAL2

（注）現在、マイナンバーカードと４桁暗証番号を使用してアクセスする仕組みが構築されている。マイナンバーカードは耐タンパー性のカードであり、カード中に格納されている利用者証明用電子証明書と４桁暗証番号の組合せを確認することにより、高い厳密度での本人確認（正しくは、当人確認（認証））が実施されているということになっている。しかし、提言書（補足２）で指摘したように高齢者施設でのマイナンバーカードと４桁暗証番号の運用には問題があり、今の保証レベルは TAAL1 である。前述したように、マイナポータルへのアクセスには、提言書（補足２）で提案した「スマートフォンの利用者証明用電子証明書の格納情報（エストニア政府発行の Smart-ID に相当）＋暗証番号」の公的個人認証の仕組みを構築し、TAAL2 の保証レベルを確保することを提案する。

３）「身元確認」の事例検証

①銀行窓口での預金口座開設のケース

・「身元確認」に該当

銀行窓口で、本人確認実施者である窓口の担当者は主体者（預金口座を開設したい人）が提示する「新身元証明書カード」と専用機器を使用して身元確認を実施後（必要な保証レベル IAL3）、必要な主体者（預金口座を開設したい人）の身元情報を確認して預金口座開設の手続きを行う。

・必要な厳密度（保証レベル）：IAL3

（注）現在の銀行窓口での預金口座開設のケースでは、「身元確認」の保証レベルはIAL３に近いレベルで実施されている。しかし、提言書（補足２）で述べたように、犯罪収益移転防止法施行規則第６条第１項第１号ワ方式では、遠隔での「身元確認」による銀行口座開設を認めている。身元証明書として提言書（補足１）で提案した「新身元証明書」を使用したとしても、犯罪収益移転防止法施行規則第６条第１項第１号ワ方式での「身元確認」は厳密性が低いため、IAL２でしかない。提言書（補足１）で提言したように、預金口座開設のケースにおける遠隔での「身元確認」を認める際には、本人受取限定郵便を組み合わせた仕組みを必須とし、IAL3の保証レベルを確保することが望まれる。ちなみに、「NIST SP 800-63-3」における遠隔での「Identity Proofing（身元確認）」の保証レベルの定義の中でも、「身元確認」の実施は、「訓練を受けた本人確認実施者が厳密に監視し、対面と同レベルの厳密性で「身元確認」を実施しない場合は、保証レベルはIAL2である」と定義されている。

さらにいうと、犯罪収益移転防止法施行規則第６条第１項第１号ワ方式で現在のマイナンバーカードを「身元確認」に使用した場合は、提言書（補足２）で指摘したように高齢者施設でのカード運用に問題があり、保証レベルはIAL１でしかないため、マネーロンダリングの温床となる可能性がある。現在のマイナンバー制度の制度設計を根本から見直し、遠隔での銀行預金口座開設における「身元確認」は、IAL3に近い保証レベルの仕組みを構築することが望まれる。今のマイナンバーカードさえ使用していれば「本人確認の保証レベルは３」であるといった曖昧な考え方は、根本から考え直す必要がある。

②携帯電話契約のケース

・「身元確認」に該当

携帯電話会社店舗で、本人確認実施者である店舗の担当者は主体者（携帯電話の契約をしたい人）が提示する「新身元証明書カード」と専用機器を使用して身元確認を実施後（必要な保証レベルIAL3）、必要な主体者（携帯電話の契約をしたい人）の身元情報を確認して携帯電話契約の手続きを行う。

・必要な厳密度（保証レベル）：IAL3

（注）現在の携帯電話契約のケースでは、提言書（補足１）で示したような厳密な「身元確認」は実施されていないため、なりすまし犯罪の温床となる可能性がある。そのため、携帯電話契約の「身元確認」においても、銀行預金口座開設と同様にIAL3に近い保証レベルの仕組みを構築することが望まれる。

③小売り店舗でのポイントカードを作成するケース

・「身元確認」に該当

小売店舗で、身元確認を実施せずに、ポイントカードを作成する。

・必要な厳密度（保証レベル）：IAL１

（注）このケースでは、身元確認は不要である。

④図書館貸出カードを作成するケース

・「身元確認」に該当

図書館で、本人確認実施者である図書館職員は主体者が提示するサブの身元証明書（「顔写真付き新保険証」か「新運転免許証」）を使用した身元確認を、身元証明書チェック（偽造品でないことのチェック）の専用機器を使用せずに目視のみで実施後（必要な保証レベルIAL2）、必要な主体者の身元情報を確認して図書館貸出カードを作成する。

・必要な厳密度（保証レベル）：IAL２

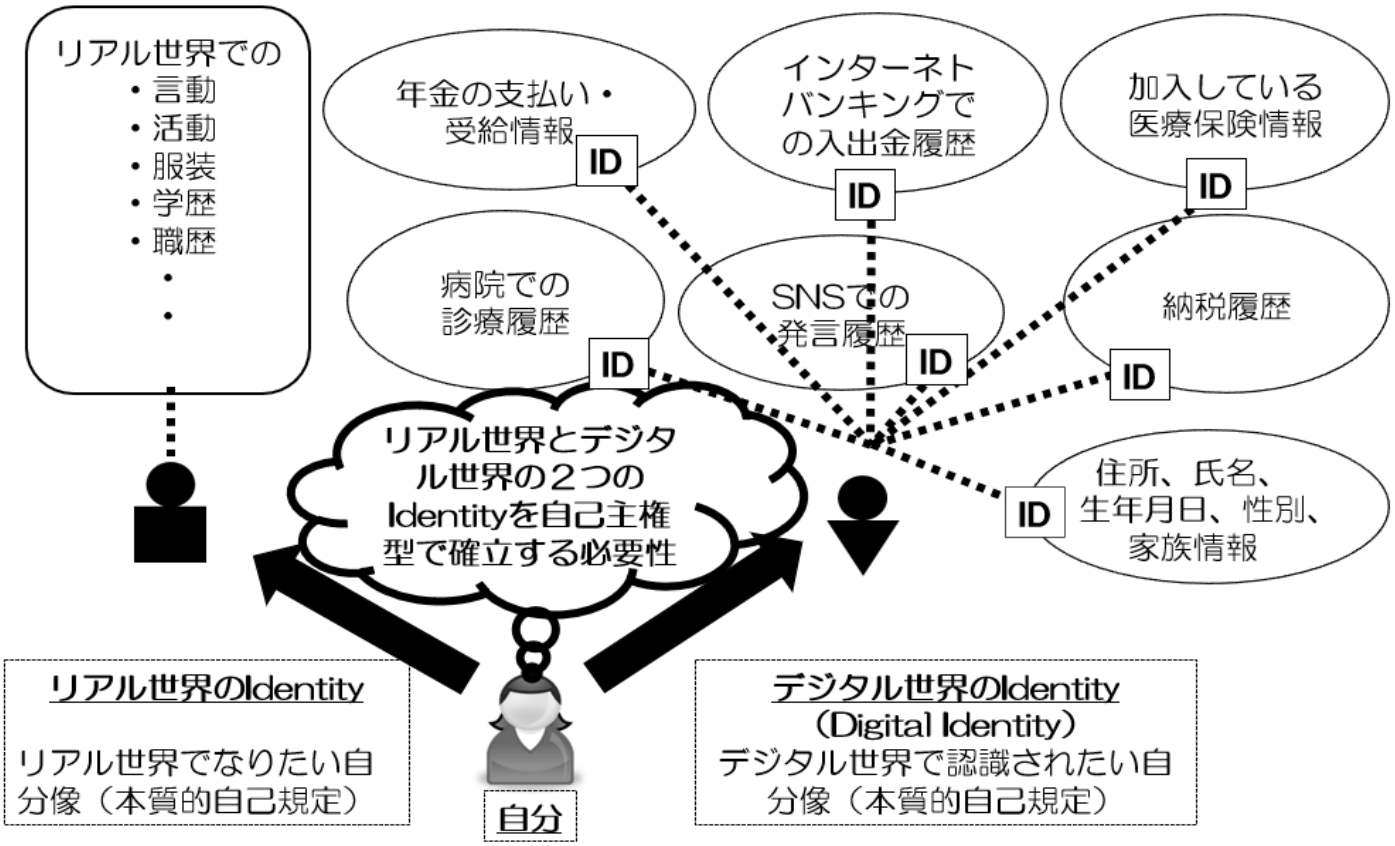
（注）このケースでは、IAL３レベルでの厳密な身元確認は必要ない。提言書（補足２）で提案したサブの身元証明書（「顔写真付き新保険証」か「新運転免許証」）を使用したIAL2レベルの身元確認を実施し、図書館貸出カードを作成することが望まれる。

7．おわりに

本付録では、「本人確認」に関する定義を以下のように提案した。

「本人確認とは、なんらかの手続きを行いたい主体者の本人性を確認するプロセスの総称であり、『身元確認』『当人確認（認証）』『真正性確認と属性情報確認』の３つの確認プロセスから構成される。つまり、主体者の本人性の確認が必要な手続きは、これらの３つの確認プロセスを適切に組み合わせることによって確認作業を実施することになる。そして、これらの確認プロセスの実施者は、本人確認を依頼する『主体者』と、主体者の本人確認を実施する『本人確認実施者』から構成される。」

本付録の内容は、「米国立標準技術研究所（NIST）の Digital Identity Guidelines 第３版（NIST SP 800-63-3)」を参考にして、過去の情報システム学会からの提言内容と日本社会の現状を踏まえた提案として検討した結果である。Digital Identity を「デジタル本人確認」などと翻訳するケースをみかけるが、Digital Identity を敢えて翻訳するとしたら「デジタル世界の本質的自己規定」とすることを提案したい（図５参照)。そして、「デジタル世界の本質的自己規定」は自己主権型で確立する必要があり、その実現のためには高い厳密度（保証レベル）で主体者の本人性を確認（本人確認）することが最も大切な要素になる、ということである。そのために必要なプロセスが本人確認であり、『身元確認』『当人確認（認証)』『真正性確認と属性情報確認』の３つの確認プロセスから構成される、ということである。



【図５】Digital Identity（デジタル世界の本質的自己規定）の自己主権型での確立

情報システム学会の過去の提言と合わせて読んでいただき、今後の「本人確認ガイドライン改定方針 令和５年度中間とりまとめ（デジタル庁)」の改定の参考になれば幸いである。

以上