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

（抜粋）

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

〔標準ガイドライン群ＩＤ〕

1004

〔キーワード〕

本人確認、身元確認、当人認証、非改ざん性の確保、事実否認の防止、行政手続におけるオンラインによる本人確認、電子署名、認証

〔概要〕

各種行政手続をデジタル化する際に必要となるオンラインによる本人確認の手法を示した標準ガイドライン附属文書。

目次

１　はじめに

１．１　背景と目的

政府は、行政の在り方そのものをデジタル前提で見直すデジタル・ガバメントを実現するため、平成 30 年 7 月 20 日に「デジタル・ガバメント実行計画」（デジタル・ガバメント閣僚会議決定）を策定した。その計画において「電子的な本人確認の手段についても、行政手続における本人確認等の手法として広く用いられているマイナンバーカード等を用いた電子署名に加え、情報システムの取り扱う情報や行政サービスの性質等を勘案し、電子署名以外の電子認証等の適切な技術選択を行うことが重要である。また、電子認証に関しては、近年技術標準の検討も進んでおり、国際的な標準化（米国 NIST SP800-63-3 等）とも整合性を持った取組を推進する必要がある。」とされたところである。

本ガイドラインは、デジタル・ガバメント実行計画に基づき、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」（平成 22 年 8 月 31 日 CIO 連絡会議決定）を見直し、各種行政手続をデジタル化する際に必要となるオンラインでの本人確認に対する考え方及び手法をまとめたものである。

主な規定範囲は、次の 3 点である。

(1) オンライン手続に関わる脅威と、脅威から生じる「リスクの影響度」を導出する手法
(2) 上記の手法により導出されるリスクの影響度を踏まえ、オンライン手続に求められる認証方式の「保証レベル」を導出する手法
(3) 上記の手法により導出される認証方式の各保証レベルにて求められる「対策基準」

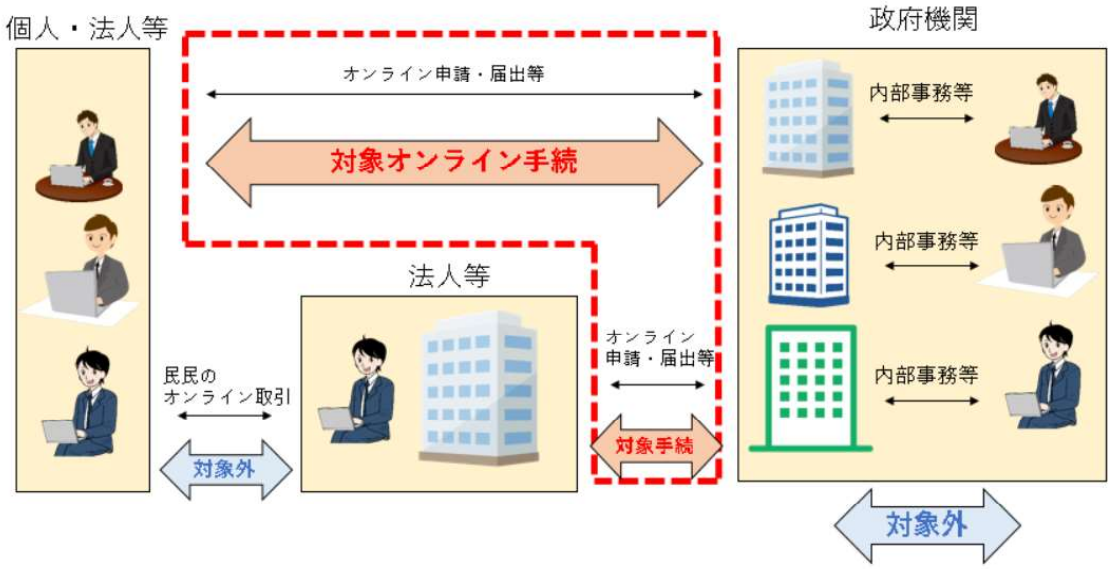
以上を活用することによって、オンライン手続における脅威に対するリスクの影響度を踏まえた合理的な行政手続におけるオンラインによる本人確認の手法について、検討を可能とすることを本ガイドラインの目的とする。

１．２　適用対象

各府省が法令等に基づき行う行政手続をデジタル化する際に、個人又は法人等のオンラインによる本人確認が必要であると見込まれる行政手続を対象とするものであり、そのうち、個人・法人等と政府との間の申請・届出等のオンライン手続の全て（以下「対象オンライン手続」という。）とする。代理人による申請について、代理権の付与の確認は手続ごとの要件に従い、利用者として代理人が申請する場合の本人確認については本ガイドラインを参考にできるため利用されたい。

なお、政府機関内部のイントラネットにおいて内部事務等のために各府省の職員が行う手続、民民のオンラインサービスは、本ガイドラインの対象外としている。

図　1-1 対象とする手続



１．３　位置付け

本ガイドラインは、標準ガイドライン群の一つである。

１．４　用語

本ガイドラインにおいて使用する用語は、表　1-2 及び本ガイドラインに特別の定めがある場合を除くほか、標準ガイドライン群用語集の例による。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。

表 1-2 用語の定義

用語	意味
申請者・ 届出者等	行政手続等を行うために情報システムを利用しようとする者。例えば、申請者、届出者のほか、請求者、申込者、依頼者等が含まれる。
本人確認	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。
オンラインによる本人確認	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。
身元確認	手続の利用者の氏名等を確認するプロセスのこと。 この確認プロセスは、一般的には、個人の場合、氏名、住所、生年月日、性別、法人等の場合、商号又は名称、本店又は主たる事務所の所在地、法人番号等について、当該情報を証明する書類の提示を求めるなどにより実施される。
当人認証	ある行為の「実行主体」と、当該主体が主張する「身元識別情報」との同一性を検証することによって、「実行主体」が身元識別情報にあらかじめ関連付けられた人物（あるいは装置）であることの信用を確立するプロセスのこと。認証情報の確認方法により、以下の二つに大別する。 (1) 単要素認証 単一の認証情報によって、利用者本人であることを確認する当人認証方法。 ※例えば、ID と紐付けて、パスワード（≒本人だけが記憶している情報）、所有物、指紋、虹彩といった生体情報等のいずれかを用いる方法がある。

用語	意味
	(2) 多要素認証 記憶、所有物、生体情報の各要素のうち、複数の認証情報を組み合わせることで、利用者本人であることを確認する当人認証方法。 ※例えば、パスワード（≒本人だけが記憶している情報）とワンタイムパスワード（ワンタイムパスワードを発行できるスマートフォンを所有していることを確認する。）を組み合わせる方法がある。
非改ざん性	ある情報の記載内容が、改変されていないこと。
完全性	申請データなどが改ざんされたり破壊されたりせず、整合性を保ち一貫性を持つこと。
事実否認	利用者から、実際には申請済であるにも関わらずその事実又は内容を否認されること。
電子署名	電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。 ・当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。 ・当該情報について改変が行われていないかどうかを確認することができるものであること。
主体認証	本人しか知り得ない情報（パスワード等）、本人のみが所有する機器等（IC カード等）、本人の生体的な特徴（指紋等）により当人認証を行う手法の総称。
IC カード	集積回路（IC）を組み込んだ情報の記録や演算を行うことができるカードのこと。
暗号、 暗号アルゴリズム	情報を第三者に知られることがないように、情報に何らかの変換処理を施すこと。また、この変換処理の方式を暗号アルゴリズムと呼ぶ。
暗号鍵、秘密鍵 (Cryptographic key)	暗号化、復号、署名生成、署名検証等の暗号処理に使用する値のこと。
ウイルス、トロイの木馬	コンピュータ上で利用者の意図しないような悪意のある動作を行うことができるプログラムのこと。

用語	意味
エントロピー （Entropy）	情報の不確実性や無秩序性の度合いを表し、例えば、攻撃者が秘密の情報を特定する場合に直面する不確実性の度合いを測るものさしのようなもののこと。通常、エントロピーはビットで表現される。
検証者 （Verifier）	認証要求者がトークンを所持していることを、認証プロトコルを使用して確認することにより、認証要求者の身元識別情報を検証する者のこと。この目的のために、検証者はトークンと身元識別情報を関連付ける認証情報の有効性を検証するとともに、それらの状態を確認しなければならないこともある。
公開鍵暗号	対となる 2 つの鍵をそれぞれ暗号化と復号のための鍵として用い、暗号化に用いる鍵を公開可能とする暗号方式のこと。
主体 （Subject）	情報システムに対するアクセス等のなんらかの行為を実行する者のこと。主体は人間以外に、装置、システム、等の場合もある。
ソーシャル エンジニアリング	人間の心理的な隙につけ込む等して、非技術的・社会的な手段を用いて何らかの攻撃を行う手法のこと。
ソフトウェア	ハードウェア（コンピュータ）の動作を制御する一連の手順や命令をハードウェアが解釈可能な形式にてまとめた情報のことであり、プログラムとも呼ばれる。
属性、 属性情報	ある主体が備えている性質、特徴のことであり、そのような情報を属性情報と呼ぶ。例えば、性別、住所等のような個人情報は属性情報の一種である。
耐タンパ性	内部の情報に対する不正な読み出し、改ざんなどの攻撃が困難であることを示す度合いのこと。一般に、「耐タンパ性を備えている」「耐タンパ性がある」と表現する場合、そのような攻撃が極めて困難であることを意味することが多い。
中間者攻撃 (Man-in-the-Middle attack、MitM)	認証要求者と検証者（例えばサービス提供サイト等）の間に介入し、両者がやりとりするデータを改ざんする等して、両者に気づかれることなく不正を働くこと。
データベース	何らかの目的をもって集められたデータを保持する情報システムのこと。

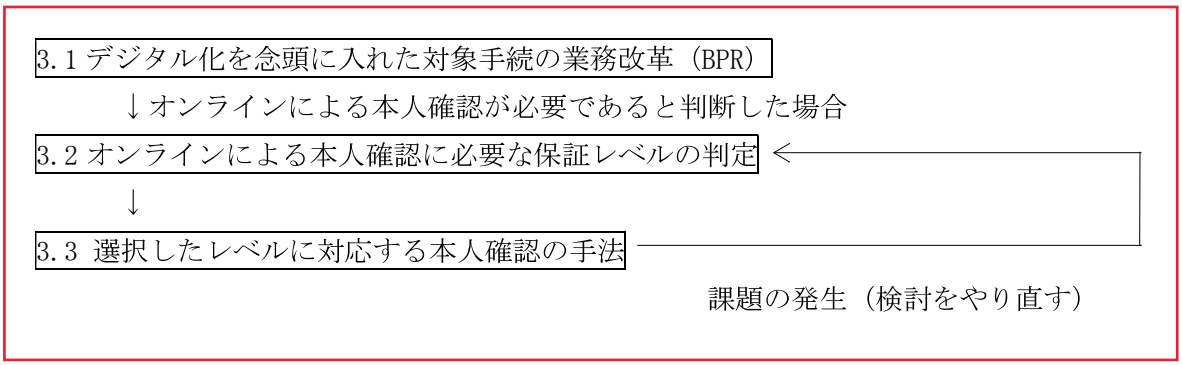
用語	意味
トークン（Token）	認証要求者が所持し管理する何かであり、認証情報等の認証に用いる情報を格納又は出力するハードウェアやソフトウェア（IC カード、ワンタイムパスワード生成機器等）、あるいは知識等の認証情報そのもの（パスワード等）等がある。
トークンの活性化	トークンの一部又は全部の機能を有効化すること。
なりすまし	自身ではない他人のふりをして何らかの行為を行うこと。
パスワード	装置やシステム等の利用時に当たり、正当な利用者であることを示すために利用者が入力すべき秘密情報のこと。英数字や記号によって構成される文字列を用いる場合が多い。
ハードウェア	回路や周辺機器等による物理的な集合体（装置、システム等）のこと。
PIN （Personal Identification Number）	本人確認のために用いる本人のみが知り得る番号等のこと。例えば、銀行のキャッシュカードの 4 桁程度の暗証番号は PIN の一種である。
プロトコル	コンピュータ間の通信方法に関する規約のこと。
本人限定受取郵便	郵便局員によって本人を確認し、本人以外が受け取ることができない郵便サービスのこと。
身元識別情報（Identity）	個人等を一意に識別する情報のこと。個人等の法的な名前は必ずしも一意とは限らないため、個人等の身元識別情報には全体が一意となるように十分な補足情報（例えば、住所、あるいは従業員番号や口座番号といった識別子など）を含める必要がある。
リプレイ攻撃	「なりすまし」による攻撃の一種。盗聴などにより認証データを不正に入手し、これを認証サーバに送信し、不正にログインを行う。
ワンタイムパスワード	利用可能回数が 1 回限りのパスワードのこと。
認証情報（Credential）	個人等の主体が身元識別情報やそのほかの属性の持ち主であることを立証するための情報のこと。例えば、書面による一般的な認証情報には、旅券、出生証明書、運転免許証、社員証などがある。電子的な認証情報は、身元識別情報（及び場合によってはそのほかの属性）と、特定の人物が所持し管理しているトークンとを結び付ける情報であり、例えば、X.509 公開鍵証明書と秘密鍵、あるいはデータベース中に記録されたユーザ名と暗号化されたパスワードの組み合わせのような形で存在する場合がある。

用語	意味
認証プロトコル（Authentication protocol）	認証要求者をリモートで認証するためにトークンの所持を確認する、厳密に規定されたメッセージ交換プロセスのこと。認証プロトコルによっては暗号鍵を生成するものもある。暗号鍵はセッション全体を保護するのに使用され、セッション中に転送されるデータが暗号による手段で保護される。
認証要求者（Claimant）	身元識別情報が関連付けられた対象であり、認証情報を用い身元識別情報との同一性（持ち主であること）を主張する者のこと。
認証の 3 要素	知っているもの、持っているもの及び身体に係る属性情報のこと。
法人等	国税庁による法人番号の指定対象法人 ・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。

３　オンラインによる本人確認の手法を決定するための進め方（法人等の場合）

オンラインによる本人確認の手法を決定するに当たっては、以下のフローに従い、判断を行うものとする。

なお、判断を行うに当たっては、技術的な知見が不可欠であることから、検討段階の当初から、府省 CIO 補佐官に協力を求め、必要な支援を得るものとする。



フロー上の各項目については、以下の具体的な内容に沿って進める。

３．１　デジタル化を念頭に入れた対象手続の業務改革（BPR）

各府省は、法令等に基づき行政手続をデジタル化する場合には、当該手続の事務フローを作成するものとし、デジタル化を念頭に入れて当該手続の事務フローを抜本的に見直すものとする。

なお、業務改革（BPR）の方法については、デジタル・ガバメント実行計画に基づき、利用者のニーズ、利用状況及び現場の業務を詳細に把握・分析した上で、手続のあるべきプロセスを法令・体制・手法を含めて一から検討する。

この検討の過程において、そもそも本人確認の前提として、法人等に申請行為等を求めることが必要かどうか、バックオフィスで連携する等の代替手段がないかどうか、業務フローの見直し等によるリスクの低減が可能であるかどうか等を検討するものとする。

３．２　オンラインによる本人確認に必要な保証レベルの判定

上記の業務改革（BPR）を行っても、なお、オンラインによる本人確認が必要であると判断した場合には、オンラインによる本人確認に求められる要件を整理するものとする。

まずは、申請者・届出者等の本人確認を行うため、①身元確認及び②当人認証について検討を行う。

そのための手順は以下のとおりである。

1)　オンラインによる本人確認が必要であると判断した場合、当該本人の何を確認することを目的としているかを特定する。

具体的には、法人等代表者の氏名、住所、資格、連絡先等や法人等の商号、所在地、法人番号等の属性情報を特定する。また、法人の代理人や法人等代表者の代理人が利用者として本人に代わって申請する場合には、正当な代理権が付与されていることを確認する必要がある。なお、個人情報の取り扱いには法令等も踏まえ配慮すること。

2)　対象となるオンライン手続で想定される脅威についてリスク評価を行う。具体的なリスク評価は、「付録Ａ．認証方式の合理的な選択を目的としたリスク評価手法」の「７ 各リスクの種類による影響度の導出」に基づいて行う。

3)　対象となるオンライン手続の認証強度として求められるレベル（保証レベル）を判定する。保証レベルは上記 2)の結果を用いて「身元確認保証レベル」と「当人認証保証レベル」とをそれぞれ判定する。具体的な判定は、「付録Ａ．認証方式の合理的な選択を目的としたリスク評価方法」の「８ 身元確認保証レベル（IAL（Identity Assurance Level））の選択」以降に基づいて行う。

表　３-1 身元確認保証レベル

身元確認保証レベル	レベルの定義
レベル１ （IAL1）	身元識別情報が確認される必要がなく、身元確認の信用度がほとんどない。身元識別情報は、自己表明若しくは自己表明相当である。
レベル２ （IAL2）	身元識別情報が遠隔又は対面で確認され、身元確認の信用度が相当程度ある。
レベル３ （IAL3）	身元識別情報が特定された担当者の対面で確認され、身元確認の信用度が非常に高い。

出典）「デジタルアイデンティティガイドライン（SP800-63-3）」より作成

表　3-2　当人認証保証レベル

当人認証保証レベル	レベルの定義
レベル１ （AAL1）	認証要求者が身元識別情報と紐付けられており、認証情報の3 要素のうち、単要素若しくは複数要素を使うことにより、当人認証の信用度がある程度ある。
レベル２ （AAL2）	認証要求者が身元識別情報と紐付けられており、認証情報の3 要素のうち、複数要素を使うことにより、当人認証の信用度が相当程度ある。
レベル３ （AAL3）	認証要求者が身元識別情報と紐付けられており、認証情報の3 要素のうち、耐タンパ性を有するハードウェアを含む複数要素を使うことにより、当人認証の信用度が非常に高い。

出典）「デジタルアイデンティティガイドライン（SP800-63-3）」より作成

4)　具体の認証方式の実装においては、上記 3)で判定した保証レベルに準拠するよう、対策を講じる。なお、「身元確認保証レベル」に準拠するための対策と、「当人認証保証レベル」に準拠するための対策を、いずれも講じる。準拠するための対策は、「付録Ｂ．認証方式の保証レベルに係る対策基準」[1]に基づいて行うこととし、その概要は、付録Ｃを参照されたい。

３．３　選択したレベルに対応する本人確認の手法例の選択

３．２により選択した保証レベルに対応する本人確認の手法例は、以下の表 3-4 のとおりとなる。当該手法により実現できることやその特徴も併せて確認する。

表　3-3 保証レベルと手法例の対応付け[2]（法人等）

必要な保証レベル		オンラインによる手法例
身元確認保証レベル	当人認証保証レベル	
レベル３ 対面での身元確認	レベル３ 耐タンパ性が確保されたハードウェアトークン	レベル A
レベル２ 遠隔又は対面での身元確認	レベル２ 複数の認証要素	レベル B
レベル１ 身元確認のない自己表明	レベル１ 単一又は複数の認証要素	レベル C

1　「5.1 対策基準の適用の考え方」において示す考え方も考慮して対策基準の適用を検討されたい。

2　「身元確認保証レベル」及び「当人認証保証レベル」の組み合わせは、それぞれの保証レベルが異なる場合がある。それぞれの保証レベルが異なる場合には、「付録 B　認証方式の保証レベルに係る対策基準」及び「付録 C 保証レベルに応じた対策基準の概要」に基づいて、オンラインにおける手法を検討すること。

表 3-4 手法例と実現できること・特徴の対応表（法人等）

	オンラインによる手法例	実現できること・特徴
レベル A	・法人等代表者を対面によって確認の上、アカウントを作成し、アカウント作成後は耐タンパ性ハードウェアトークンによる当人確認を実施。 ※耐タンパ性ハードウェアトークン例： －PIN＋IC カード ・申請データに対して、対面によって法人等代表者へ発行された電子証明書(IC カード)を用いて、電子署名を付与。	・行政手続の対象者や行政手続を実施している者について、法人等の基本 3 情報を毎回確認している。 ・電子署名を検証することにより、非常に高い信用度で「身元確認」を行っている。また、耐タンパ性を有するハードウェアトークンにより、非常に高い信用度で「当人認証」を行っている。
レベル B	・法人共通認証基盤における多要素認証の機能を利用する場合等、法人等については、国税庁法人番号公表サイトで商号、所在地及び法人番号を確認し、法人等代表者の押印及び印鑑証明書等の郵送による身元確認で、アカウントを作成し、アカウント作成後は多要素認証による当人認証の実施。 ※多要素認証例： －ID・パスワード＋二経路認証アプリ －ID・パスワード+ワンタイムパスワード生成アプリ －ID・パスワード＋生体認証 ・申請データに対して、法人等代表者へ発行された電子証明書を用いて、電子署名を付与。	・行政手続の対象者や行政手続を実施している者について、登録時に法人等の基本 3 情報を確認し、認証プロセス時には、登録時の法人等と同一の法人等であることを確認している。 ・特に法人共通認証基盤においては、登録時に法人等を相当程度の信用度で「身元確認」を行い、多要素認証の機能を用いることで相当程度の信用度で「当人認証」を行っている。
レベル C	・法人共通認証基盤における単要素認証の機能を利用する場合等、身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後は単要素認証で当人認証を実施。 ※単要素認証例 －ID・パスワードのみ －認証デバイスのみ －生体認証のみ	・行政手続の対象者や行政手続を実施している者について、法人等を正確に確認する必要がない場合で、単に毎回のアクセスが、同一の者により行われていることを確認しており、「当人認証」における信用度はある程度ある。

４　中長期計画への組込み等

４．１　中長期計画への組込み

各府省は、所管する法令に係る手続について、前述の「オンラインによる本人確認の手法を決定するための進め方」に基づき、本人確認の手法の見直し等を実施し、中長期計画にその検討状況を組み込むものとする。

ただし、即時に見直し等が可能な手続については、速やかに実施するものとする。

４．２　中長期計画の改定及び検討の継続

中長期計画の策定後も、引き続き検討を実施し、中長期計画の改定等のタイミングを捉え、検討の結果（先行実施分も含む。）を中長期計画に反映するものとする。

５　独立行政法人等が個人及び法人等に対し求めている本人確認の手法の見直しの指導

各府省は、所管する総務省設置法（平成 11 年法律第 91 号）第 4 条第 7 号から第 9 号までに掲げる法人（本ガイドラインにおいて「独立行政法人等」という。）に対し、当該法人が個人及び法人等に対し求めている本人確認の手法についても、本ガイドラインの考え方を踏まえて、検討を推進するよう指導するものとする。

別紙１　附則

１　施行期日

本ガイドラインは、決定の日から施行する。

なお、当該ガイドラインの適用は、施行後新たに定められる中長期計画に組み込みつつ、当該中長期計画の中で反映するものとする。

２　関連する指針等の廃止

「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」（2010 年（平成 22 年）8 月 31 日 CIO 連絡会議決定）は、廃止する。

別紙３　オンラインにおける本人確認の手法例の対応表（法人等に係る行政手続）

①必要な保証レベル		②オンラインによる手法例		③実現できること・特徴
身元確認保証レベル	当人認証保証レベル			
レベル３ 対面での身元確認	レベル３ 耐タンパ性が確保されたハードウェアトークン	レベル A	・法人等代表者を対面によって確認の上、アカウントを作成し、アカウント作成後は耐タンパ性ハードウェアトークンによる当人確認を実施。 ※耐タンパ性ハードウェアトークンの例： ーPIN＋IC カード ・申請データに対して、対面によって法人等代表者へ発行された電子証明書(IC カード)を用いて、電子署名を付与。	・行政手続の対象者や行政手続を実施している者について、法人等の基本 3 情報を毎回確認している。 ・電子署名を検証することにより、非常に高い信用度で「身元確認」を行っている。また、耐タンパ性を有するハードウェアトークンにより、非常に高い信用度で「当人認証」を行っている。
レベル２ 遠隔又は対面での身元確認	レベル２ 複数の認証要素	レベル B	・法人共通認証基盤における多要素認証の機能を利用する場合等、法人等については、国税庁法人番号公表サイトで商号、所在地及び法人番号を確認し、法人等代表者の押印及び印鑑証明書等の郵送による身元確認で、アカウントを作成し、アカウント作成後は多要素認証による当人認証の実施。 ※多要素認証の例： ーID・パスワード＋二経路認証アプリ ーID・パスワード＋ワンタイムパスワード生成アプリ ーID・パスワード＋生体認証 ・申請データに対して、法人等代表者へ発行された電子証明書を用いて、電子署名を付与。	・行政手続の対象者や行政手続を実施している者について、登録時に法人等の基本 3 情報を確認し、認証プロセス時には、登録時の法人等と同一の法人等であることを確認している。 ・特に法人共通認証基盤においては、登録時に法人等を相当程度の信用度で「身元確認」を行い、多要素認証の機能を用いることで、相当程度の信用度で「当人認証」を行っている。
レベル１ 身元確認のない自己表明	レベル１ 単一又は複数の認証要素	レベル C	・法人共通認証基盤における単要素認証の機能を利用する場合等、身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後は単要素認証で当人認証を実施。 ※単要素認証の例： ーID・パスワードのみ ー認証デバイスのみ ー生体認証のみ	・行政手続の対象者や行政手続を実施している者について、法人等を正確に確認する必要がない場合で、単に毎回のアクセスが、同一の者により行われていることを確認しており、「当人認証」における信用度はある程度ある。