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

〔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。

改定履歴

改定年月日	改定箇所	改定内容
2019年2月25日	―	・初版決定

目次

目次 i
１ はじめに 1
　１．１ 背景と目的 1
　１．２ 適用対象 1
　１．３ 位置付け 2
　１．４ 用語 2
２ 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（個人の場合） 8
　２．１ デジタル化を念頭に入れた対象手続の業務改革（BPR） 8
　２．２ オンラインによる本人確認に必要な保証レベルの判定 8
　２．３ 選択したレベルに対応する本人確認の手法例の選択 10
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） .. 12
　３．１ デジタル化を念頭に入れた対象手続の業務改革（BPR） 12
　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 13
　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 14
４ 中長期計画への組込み等 16
　４．１　中長期計画への組込み 16
　４．２　中長期計画の改定及び検討の継続 16
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 . 16

別紙１　附則 17
１ 施行期日 17
２ 関連する指針等の廃止 17
別紙２　オンラインにおける本人確認の手法例の対応表（個人に係る行政手続） 18
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） .. 19

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 20
１ リスク評価の対象外となるケース 21
２ リスク評価の前提条件 21
３ オンライン手続に関わる脅威 22
４ リスクの影響度の定義 23
５ リスクの種類 24
６ リスク評価による保証レベルの導出 24
７ 各リスクの種類による影響度の導出 25

８ 身元確認保証レベル（IAL（Identity Assurance Level））の選択 28
９ 当人認証保証レベル（AAL（Authentication Assurance Level））の選択 29
１０ 総合的リスク評価の導出方法 30
１１ 評価の実施に当たっての留意点 30
１２ リスク評価に基づく認証方式の選択等の実施 30

付録B　認証方式の保証レベルに係る対策基準 35
１ 保証レベル 35
２ 認証方式の基本概念実施 38
　２．１　電子署名と認証 38
　２．２　適用対象電子署名と認証の使い分けの考え方 38
３ 認証に係る対策基準 40
　３．１　認証フレームワーク 40
　３．２　登録 41
　３．３　発行・管理 43
　３．４　トークン 46
　３．５　認証プロセス 51
４ 署名等に係る対策基準 54
　４．１　署名等フレームワーク 54
　４．２　署名等プロセス 56
５ 基準実現のための配慮事項 58
　５．１　対策基準の適用の考え方 58
　５．２　標準仕様の採用 59
　５．３　利用者への配慮 59
　５．４　異なる保証レベルの認証方式間の連携 59
　５．５　証跡管理 60
　５．６　客観的評価による安全性の確認 61

付録C　保証レベルに応じた対策基準の概要 62

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」

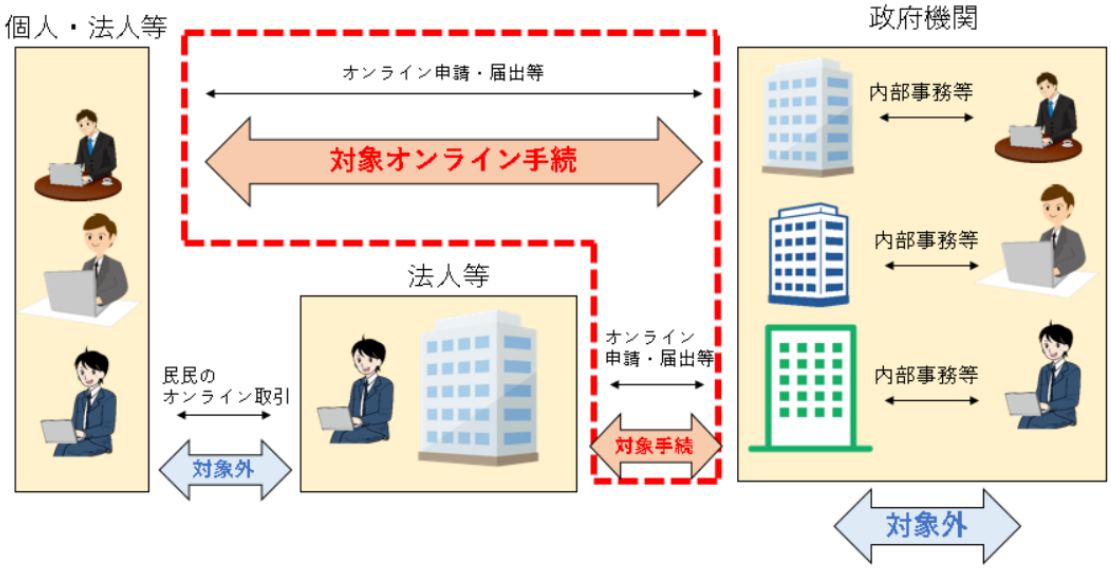
以上を活用することによって、オンライン手続における脅威に対するリスクの影響度を踏まえた合理的な行政手続におけるオンラインによる本人確認の手法について、検討を可能とすることを本ガイドラインの目的とする。

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。

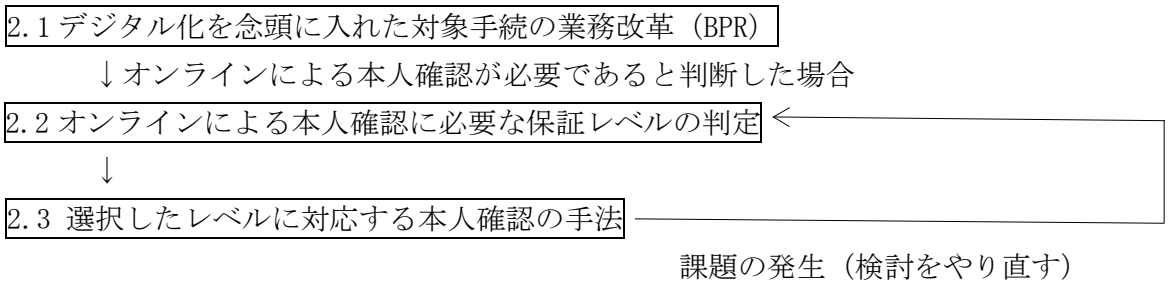
用語	意味
トークン（Token）	認証要求者が所持し管理する何かであり、認証情報等の認証に用いる情報を格納又は出力するハードウェアやソフトウェア（IC カード、ワンタイムパスワード生成機器等）、あるいは知識等の認証情報そのもの（パスワード等）等がある。
トークンの活性化	トークンの一部又は全部の機能を有効化すること。
なりすまし	自身ではない他人のふりをして何らかの行為を行うこと。
パスワード	装置やシステム等の利用時に当たり、正当な利用者であることを示すために利用者が入力すべき秘密情報のこと。英数字や記号によって構成される文字列を用いる場合が多い。
ハードウェア	回路や周辺機器等による物理的な集合体（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。

２　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（個人の場合）

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。

２．１　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、法令等に基づく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（以下「業務改革（BPR）」という。）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、個人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。

２．２　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２．１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特定する。

具体的には、個人の当該本人についての氏名、住所、資格、連絡先等の属性情報を特定する。また、個人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。例えば、本人又はその代理人からマイナンバーの提供を受ける際は、本ガイドラインではなく、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（平成 25 年法律第 27 号）第 16 条に基づく本人確認措置を行うことが義務付けられていることに留意すること。

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」までの内容に基づいて行う。

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　2-1 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　2-2 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。

２．３　選択したレベルに対応する本人確認の手法例の選択

２．２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 2-4 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をする。

表　2-3 保証レベルと手法例の対応付け[2]（個人）

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
該当しない	該当しない	レベル D

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。

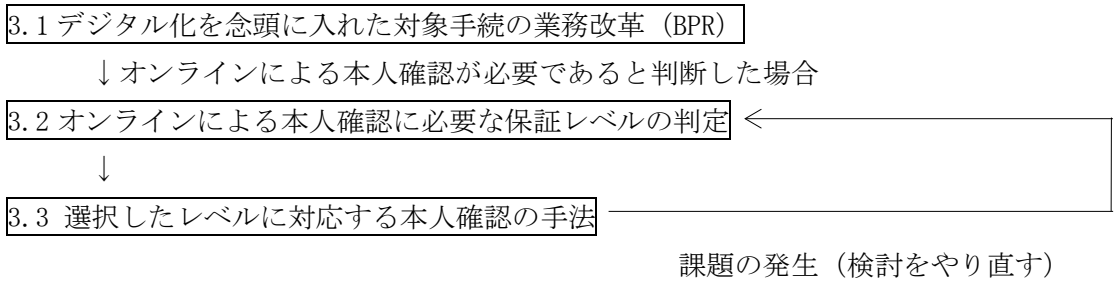
表 2-4 手法例と実現できること・特徴の対応表（個人）

	オンラインによる手法例	実現できること・特徴
レベルA	・マイナンバーカード（公的個人認証：署名用電子証明書）による身元確認でアカウントを作成し、アカウント作成後はマイナンバーカード（公的個人認証：利用者証明用電子証明書）の耐タンパ性ハードウェアトークンによる当人認証を実施。 ・申請データに対するマイナンバーカード（公的個人認証：署名用電子証明書）による電子署名を付与。 ※耐タンパ性ハードウェアトークン例： －PIN＋IC カード（マイナンバーカード）	・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、個人の基本4情報を毎回確認している。 ・マイナンバーカード（公的個人認証：署名用電子証明書）の機能により付与された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、耐タンパ性を有した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	・マイナンバーカード（公的個人認証：署名用電子証明書）等による身元確認でアカウント作成し、アカウント作成後はマイナンバーカード（公的個人認証：利用者証明用電子証明書）若しくはこれによることができない場合、その他の多要素認証による当人認証を実施。 ・マイナンバーカードによるオンラインでの身元確認が行えない場合、対面での身分証明書等の確認や郵送した申請書（捺印付）、印鑑証明書、公的証明書（住民票等）等の確認によりアカウントを作成。 ・法人番号を付与された法人等の法人等代表者及び事業を行う個人を認証する主体認証機能を複数の電子申請システムに提供する情報システム（以下「法人共通認証基盤」という。）における多要素認証の機能を利用する場合等、事業を行う個人について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： －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	・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、登録時に個人の基本4情報を確認し、認証プロセス時には、登録時の個人と同一の個人であることを確認している。 ・登録時に相当程度の信用度のある「身元確認」を行い、マイナンバーカード（公的個人認証：利用者証明用電子証明書）等の多要素認証を用いることにより相当程度の信用度で「当人認証」を行っている。 ・特に法人共通認証基盤においては、登録時に事業を行う個人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	・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。 ・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： －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、個人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。
レベルD	・身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後もアカウントを入力するだけ（当人認証を行わない。）。	・本人に関する情報は不要。

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２　オンラインにおける本人確認の手法例の対応表（個人に係る行政手続）

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	・マイナンバーカード（公的個人認証：署名用電子証明書）による身元確認でアカウントを作成し、アカウント作成後はマイナンバーカード（公的個人認証：利用者証明用電子証明書）の耐タンパ性ハードウェアトークンによる当人認証を実施。 ・申請データに対するマイナンバーカード(公的個人認証：署名用電子証明書)による電子署名を付与。 ※耐タンパ性ハードウェアトークンの例： －PIN＋IC カード（マイナンバーカード）	・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、個人の基本４情報を毎回確認している。 ・マイナンバーカード(公的個人認証：署名用電子証明書)の機能により付与された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、耐タンパ性を有した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	・マイナンバーカード（公的個人認証：署名用電子証明書）等による身元確認でアカウントを作成し、アカウント作成後はマイナンバーカード（公的個人認証：利用者証明用電子証明書）若しくはこれによることができない場合、その他の多要素認証による当人認証を実施。 ・マイナンバーカードによるオンラインでの身元確認が行えない場合、対面での身分証明書等の確認や郵送した申込書（捺印付）、印鑑証明書、公的証明書（住民票等）等の確認によりアカウントを作成。 ・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、事業を行う個人について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： －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	・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、登録時に個人の基本 4 情報を確認し、認証プロセス時には、同一の個人であることを確認している。 ・登録時に相当程度の信用度のある「身元確認」を行い、マイナンバーカード(公的個人認証：利用者証明用証明書）等の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。 ・特に法人共通認証基盤においては、登録時に事業を行う個人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	・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。 ・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： －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、個人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。
該当しない	該当しない	レベル D	・身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後もアカウントを入力するだけ（当人認証を行わない。）。	本人に関する情報は不要

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： －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： －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： －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。

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

「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」（平成 30 年 7 月 25 日サイバーセキュリティ戦略本部決定）では、情報システムのセキュリティ機能のうち主体認証機能の導入に当たって、以下の遵守事項が定められている。

6.1 情報システムのセキュリティ機能
6.1.1 主体認証機能

遵守事項

（１）主体認証機能の導入

(a) 情報システムセキュリティ責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の **識別** 及び **主体認証** を行う機能を設けること。

(b) 情報システムセキュリティ責任者は、国民・企業と機関等との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合は、**オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定すること**。

(c) 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び **不正な主体認証の試行に対抗するための措置** を講ずること。

出所）「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」

この付録では、遵守事項の「オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定すること」を実施するためのリスク評価手法を示す。

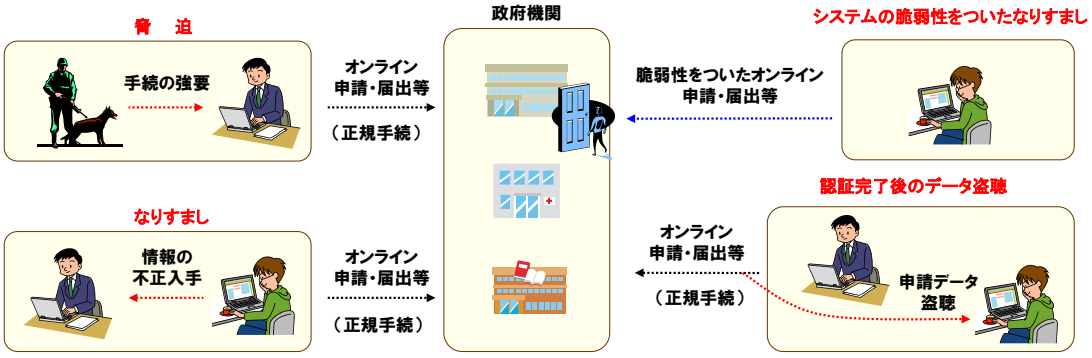
リスク評価手法の策定に当たっては、米国政府の電子政府における認証の必要性や適切な認証方式の選択に関する各政府機関の意思決定を支援することを目的として策定された「連邦政府機関向け電子認証にかかわるガイダンス（OMB M-04-04）」及び同ガイダンスを基に検討された経済産業省の「電子政府認証ガイドライン検討報告書」及び米国政府の情報システムにおけるリスク管理の一般的な方法論を規定している「IT システムのためのリスクマネジメントガイド（NIST Special Publication 800-30）」を参考としている。

1　リスク評価の対象外となるケース

本ガイドラインのリスク評価手法では、電子政府システムに対するセキュリティ確保策として認証方式を適用する場合に、想定される脅威に対して、認証方式の有効性を確認するために行うことから、認証方式の有効性とは関連性がない脅威については、リスク評価の対象外となる。

例えば、悪意のある第三者が申請者本人を脅迫しての手続の強要、あるいは、何らかの方法により申請者本人から手続に必要な情報を入手し、申請者本人になりすますなどして正規の手続により、申請を行い、不正に情報等を入手するようなケースが考えられる。また、認証が完了した後の処理手続を盗聴するケースやシステム上の脆弱性を突いてなりすまし等の攻撃を行うなど認証方式の適用の有無に関係なく、通常ではシステムの堅牢化や通信路の暗号化といった他の方法でセキュリティを確保すべきケースについては、本ガイドラインの対象外となる。

図　A-1 リスク評価の対象外となるケース



2　リスク評価の前提条件

現状適用された、あるいは適用される予定の認証方式が、リスクに見合う有効なものかどうかを確認するために、リスク評価が実施される。その際、リスクの潜在的な影響度を把握することが重要となることから、リスク評価の実施に当たっては、電子署名や認証が全て機能していない状態を前提にするものとする。

3　オンライン手続に関わる脅威

「IT システムのためのリスクマネジメントガイド（NIST Special Publication 800-30)」では、人為的脅威を脅威源ごとに分類している。このうち、コンピュータ犯罪者による不法な情報開示や金銭取得を目的とした詐欺行為（なりすまし、傍受、リプレイ攻撃等）については、本ガイドラインが対象としているオンライン手続（個人・法人等と政府の間の申請・届出等のオンライン手続）に対しても同様に脅威として該当すると判断できる。

表　A-2 人為的脅威

脅威源	動機	脅威行動
ハッカー、 クラッカー	挑戦、 自己顕示、 反抗	ハッキング、ソーシャルエンジニアリング、システム侵入・侵害、不正なシステムアクセス
コンピュータ 犯罪者	情報破壊、 不法な情報開示、 金銭取得、 不当なデータ改ざん	コンピュータ犯罪（例えば、サイバーストーキングなど)、詐欺行為（例えば、なりすまし、傍受、リプレイ攻撃など)、情報の贈収賄、スプーフィング、システム侵入
テロリスト	脅迫、破壊、 攻略、復讐	爆弾／テロリズム、情報戦争、システム攻撃（例えば、DDoS など)、システム侵入、システム改ざん
産業スパイ （企業、外国政府、その他の政府関連）	競争優位性、 経済的スパイ行為	経済的攻略、情報窃盗、個人プライバシー侵害、ソーシャルエンジニアリング、システム侵入、不当なシステムアクセス
インサイダー （訓練の不足した ／不満を持つ ／悪意のある ／不注意な ／解雇された 従業員）	好奇心、自己満足、 自己顕示、 金銭取得、復讐、 不作為の誤り及び怠慢 （例えば、データ入力ミス、プログラミングミスなど）	従業員に対する攻撃、脅迫状、知財情報の参照、コンピュータの不正使用、詐欺・窃盗、情報の贈収賄、偽造・変造されたデータの入力、傍受、悪意のコード（例えば、ウイルス、論理爆弾、トロイの木馬など)、個人情報販売、システムのバグ、システム侵入、システム損傷、不正なシステムアクセス

出所)「IT システムのためのリスクマネジメントガイド（Special Publication 800-30)」

4　リスクの影響度の定義

対象オンライン手続に関わる脅威に対するリスクについては、ケースによって与える影響が異なることから、与える影響を分析しレベル分けを実施する必要がある。そのレベルを「影響度」という尺度で 3 つのレベルに分類する。

このレベル分けに当たっては、米国政府が定めた基準である「連邦政府の情報および情報システムに対するセキュリティ分類規格（連邦情報処理規格　FIPS 199)」を参考とし、以下のとおりリスクの影響度を定義した。

表　A-3 リスクの影響度の定義

影響度	定義
高位	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に致命的又は壊滅的な悪影響を及ぼすと予想される
中位	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に重大な悪影響を及ぼすと予想される
低位	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に限定的な悪影響を及ぼすと予想される

出所）「連邦政府の情報および情報システムに対するセキュリティ分類規格（連邦情報処理規格 FIPS 199)」

５　リスクの種類

「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」では、オンライン手続において想定されるリスクを以下のとおり分類している。

オンライン手続において想定されるリスクとしては、主に以下の 6 種類に分類することができる。 ①　オンライン手続サービスの利用において国民等の利用者に不便、苦痛を与える、又はオンライン手続サービスを所管する機関等が信頼を失う ②　国民等の利用者に金銭的被害を与える、機関等に賠償責任が生じるなど、財務上の影響を与える ③　機関等の活動計画や公共の利益に対して影響を与える ④　国民等の利用者の個人情報等の機微な情報が漏えいする ⑤　国民等の利用者の身の安全に影響を与える ⑥　法律に違反する なお、認証方式の選択に当たっては、上記①～⑥のリスクを検討し、適切なセキュリティ確保と普及を妨げない利便性とを両立させることが重要である。その際は、特定のリスクのみに着目せず、様々な観点でリスクを評価した上で認証方式を決定する必要がある。

出所）「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」

６　リスク評価による保証レベルの導出

リスク評価については、多くの手法がある。ここでは、「デジタルアイデンティティガイドライン（NIST SP800-63-3）」を基に示す。このガイドラインでは、始めに、オンライン手続の中で、各リスクの種類による影響度を導出する。次に、各リスクの種類の影響度から身元情報の確認プロセスの保証レベルである身元確認保証レベル（IAL(Identity Assurance Level)と認証プロセスの保証レベルである当人認証保証レベル（AAL(Authentication Assurance Level)）を導出する。

なお、以下の表 A-4 以降の図表の和訳は、一般財団法人日本情報経済社会推進協会による和訳された NIST SP800-63-3 及び独立行政法人情報処理推進機構による和訳された OMB-04-04 を基に作成した。

7　各リスクの種類による影響度の導出

前述の「①オンライン手続サービスの利用において国民等の利用者に不便、苦痛を与える、又はオンライン手続サービスを所管する機関等が信頼を失う」「②国民等の利用者に金銭的被害を与える、機関等に賠償責任が生じるなど、財務上の影響を与える」「③機関等の活動計画や公共の利益に対して影響を与える」「④国民等の利用者の個人情報等の機微な情報が漏えいする」「⑤国民等の利用者の身の安全に影響を与える」「⑥法律に違反する」のそれぞれに関して、影響度を以下の表に従って導出する。

表 A-4 「①オンライン手続サービスの利用において国民等の利用者に不便、苦痛を与える、又はオンライン手続サービスを所管する機関等が信頼を失う」リスクの影響度

レベル	内容
低位	限定的かつ短期間の不便や苦痛又は、利用者や機関等が当惑する。
中位	深刻かつ短期間又は限定的かつ長期間の不便や苦痛又は、利用者や機関等の地位や評判に対する影響がある。
高位	深刻又は長期間の不便や苦痛又は、利用者や機関等の地位や評判に対する影響がある。この影響は、特に深刻な影響や多くの利用者に影響する状況をいう。

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

表 A-5 「②国民等の利用者に金銭的被害を与える、機関等に賠償責任が生じるなど、財務上の影響を与える」リスクの影響度

レベル	内容
低位	利用者や機関等の軽微又は若干の財務上の損失、若しくは機関等の軽微又は若干の賠償責任が生じる。
中位	利用者や機関等の深刻な財務上の損失、若しくは機関等の深刻な賠償責任が生じる。
高位	利用者や機関等の壊滅的な財務上の損失、若しくは機関の深刻又は壊滅的な賠償責任が生じる。

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

表 A-6 「③機関等の活動計画や公共の利益に対して影響を与える」リスクの影響度

レベル	内容
低位	機関等の運営又は資産、若しくは公共の利益に対する限定的な悪影響がある。限定的な悪影響の例としては以下が考えられる。（i）機関等の主要な機能が「著しく」低下した状態が継続し、業務能力の劣化が生じている。（ii）機関等の資産や公共の利益の軽微な損害が生じる。
中位	機関等の運営又は資産、若しくは公共の利益に対する深刻な悪影響がある。深刻な悪影響の例としては以下が考えられる。（i）機関等の主要な機能が「大幅に」低下した状態が継続し、業務能力の大幅な劣化が生じている。（ii）機関等の資産や公共の利益の重大な損害が生じる。
高位	機関等の運営又は資産、若しくは公共の利益に対する重大又は壊滅的な悪影響がある。重大又は壊滅的な悪影響の例としては以下が考えられる。（i）機関等の主要な機能の 1 つ以上が実施できない状態が継続し、業務能力の激しい劣化又は喪失が生じている。（ii）機関等の資産又は公共の利益の際立った損害が生じている。

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

表 A-7 「④国民等の利用者の個人情報等の機微な情報が漏えいする」リスクの影響度

レベル	内容
低位	公開許可のない個人情報、政府の機密情報又は企業秘密の限定的な公開により、機関等の活動や資産、又は利用者に機密性喪失の限定的な悪影響をもたらすことが予測される。
中位	公開許可のない個人情報、政府の機密情報又は企業秘密の公開により、機関等の活動や資産、又は利用者に機密性損失の重大な悪影響をもたらすことが予測される。
高位	公開許可のない個人情報、政府の機密情報又は企業秘密の公開により、機関等の活動や資産、又は利用者に致命的又は壊滅的な機密性損失の悪影響をもたらすことが予測される。

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

表 A-8 「⑤国民等の利用者の身の安全に影響を与える」リスクの影響度

レベル	内容
低位	医療措置を必要としない軽症の影響を与える。
中位	軽症が生じる中程度のリスク又は医療措置を必要とする負傷が生じる限定的な影響を与える。
高位	深刻な負傷又は死亡の影響を与える。

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

表 A-9 「⑥法律に違反する」の潜在的影響

レベル	内容
低位	法執行の対象とならないような性質の民事上又は刑事上の法律違反のリスクがある。
中位	法執行の対象となる可能性のある民事上又は刑事上の法律違反のリスクがある。
高位	法執行の計画で、特に重要とされている民事上又は刑事上の法律違反のリスクがある。

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

8　身元確認保証レベル（IAL（Identity Assurance Level））の選択

各リスクの種類の影響度を評価し、次の選択概念図に当てはめて、身元確認保証レベル（IAL）を選択する。以下は、選択概念図と身元確認保証レベル IAL の概要である。

図　A-10 NIST SP800-63-3 の IAL の選択概要図

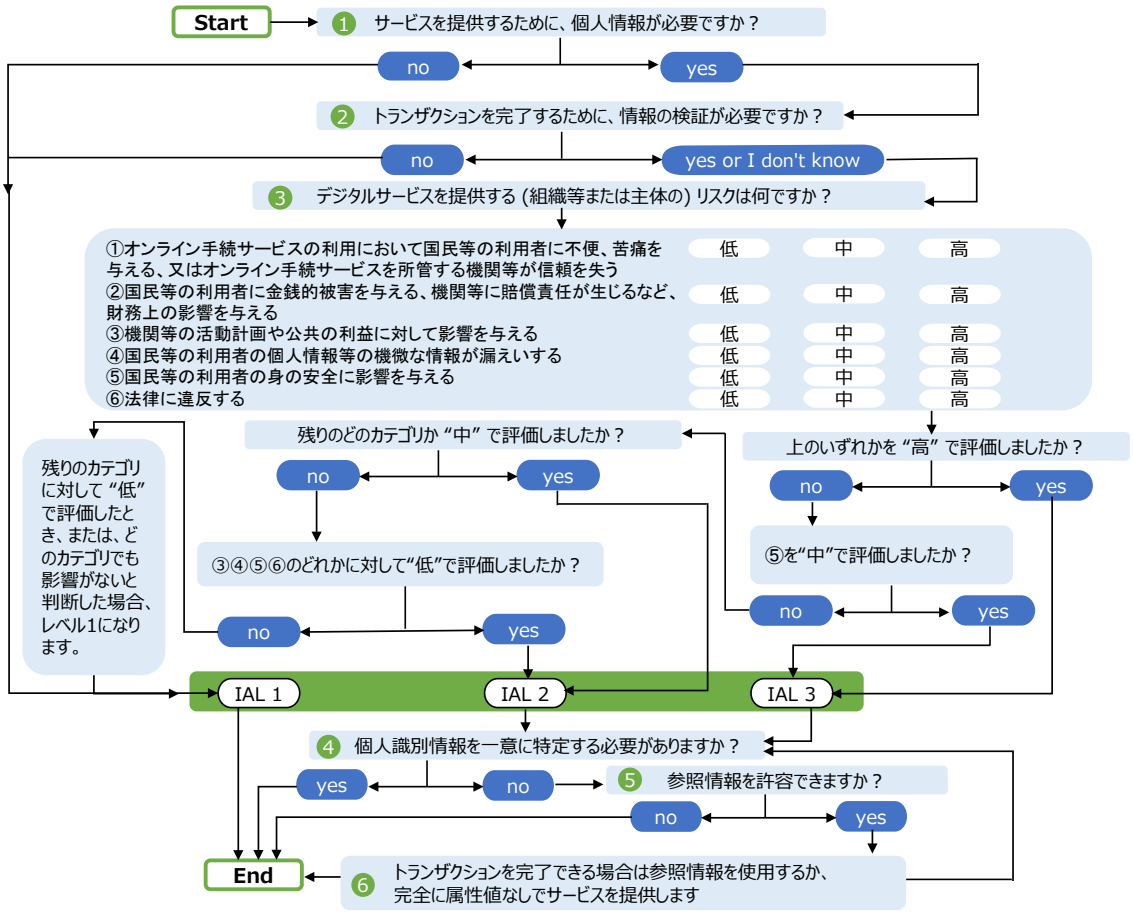


表　A-11 身元確認保証レベル（IAL）の概要

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（NIST SP800-63-3）」より作成

９　当人認証保証レベル（AAL（Authentication Assurance Level））の選択

各リスクの種類の影響度を評価し、次の選択概念図に当てはめて、当人認証保証レベル（AAL）を選択する。以下は、選択概念図と当人認証保証レベル AAL の概要である。

図　A-12 NIST SP800-63-3 の AAL の選択概要図

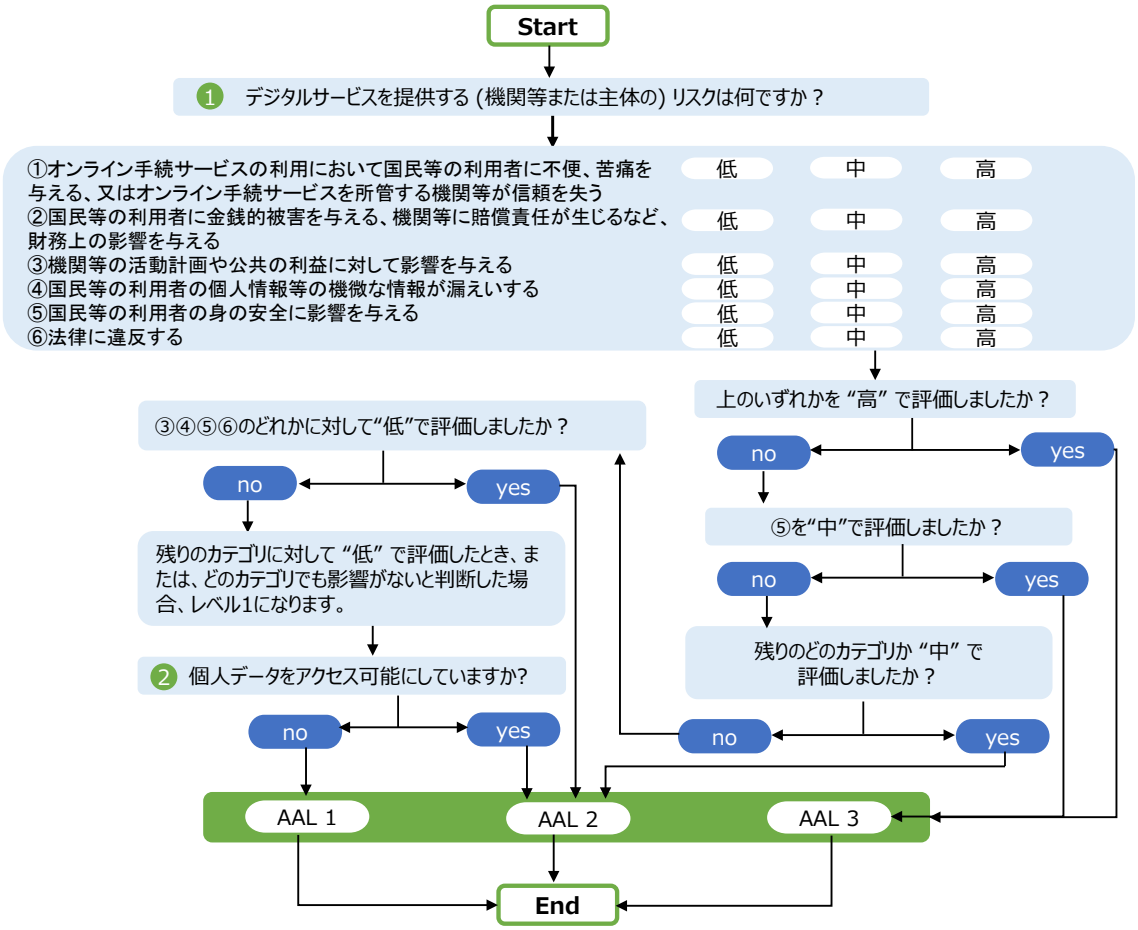


表　A-13 当人認証保証レベル（AAL）の概要

当人認証保証レベル	内容
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（NIST SP800-63-3）」より作成

１０　総合的リスク評価の導出方法

「身元確認保証レベル」及び「当人認証保証レベル」の選択に当たっては、手続固有の特性を踏まえて、各リスクの種類について考慮すべき全ての要素を対象としつつ、総合的なリスクの影響度を導出する。

総合的なリスク評価に考慮する可能性があるものとしては、本人になりすまして公的証明書を不正に取得し、それを悪用して詐欺行為を行うなど二次的被害につながる可能性が高い場合、給付される額が小額であり、被害の絶対規模が小さくても、当該申請者にとって、給付が受け取れないことによるダメージが大きいと考えられる場合、手続の不備に対して罰則を課す、あるいは、詳細な調査、検証を事後調査により課すなど、不正に対する抑止効果がありリスク低減を図っていると考えられる場合などが考えられる。

また、申請者等の特性を考慮する必要がある場合も考えられる。例えば、代理人が手続を行う場合で、この代理人になりすまして複数あるいは多数の手続を行い、結果としてリスクが積み上がって影響度が高まる場合などである。この場合は、リスクの影響を勘案し、同一の手続であっても、申請者等の特性を区分して、本人が手続を行う場合と代理人が行う場合で、リスク評価の導出結果が異なることになる。

以上のように、考慮すべき全ての要素を加味した上で、相応した総合的なリスクの影響度の導出を行う。

１１　評価の実施に当たっての留意点

電子政府の行政サービス向上を図っていく中で、今後、電子政府の新たな進展において、ワンストップサービスやバックオフィス連携などにより、公的証明書等を含め提出書類が削減されていく、あるいは、各主体が保有するデータの連携により確認作業が簡便になっていくなど、申請等に係る厳格さの程度を考慮する上で、現在の手続の方法の性格が変容していく可能性がある。

こうした状況を踏まえ、各府省が行うリスク評価の実態に即して、本ガイドライン運用にフィードバックしながら、必要が生じれば、別の評価指標など新たなノウハウを取り入れていくなど、リスク評価手法全般について、継続して、研究・検討を進めていく必要がある。

１２　リスク評価に基づく認証方式の選択等の実施

本ガイドラインに基づくリスク評価は、当該オンライン手続を所掌する各府省が必要に応じて実施する。

リスク評価の実施時期については、各府省が当該オンライン手続に係る電子政府システムの新規構築又は改修を行う際の計画策定や要件定義等の企画段階などで

セキュリティ確保策として電子署名・認証の適用を検討する際を想定する。リスク評価を実施し、得られた評価結果である「身元確認保証レベル」及び「当人認証保証レベル」を導出する。これにより、当該手続に関わる脅威に対するリスクの影響度に見合った合理的な認証方式の選択が可能となる。

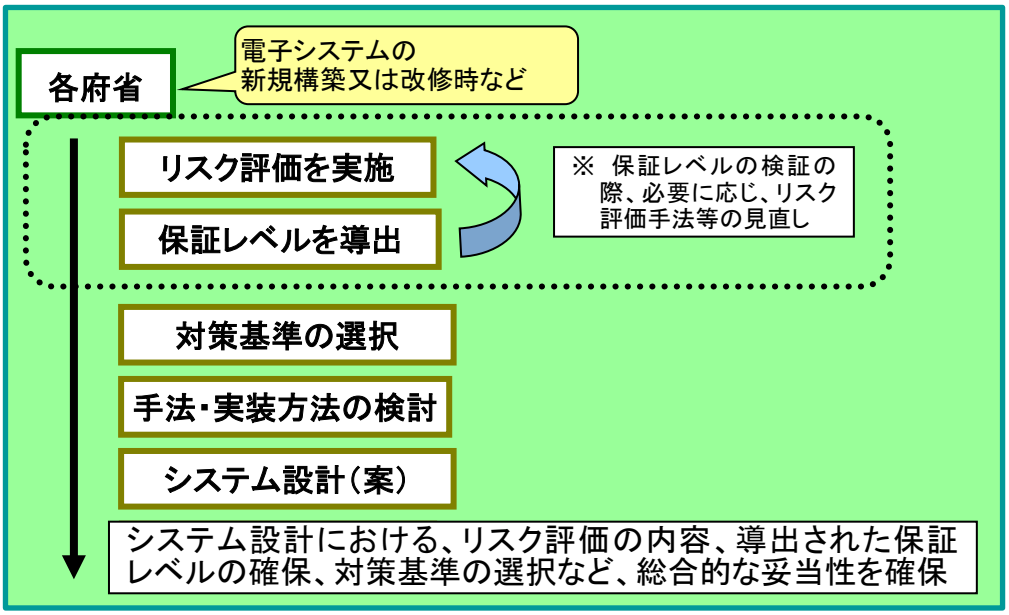
表　A-14 保証レベルと対策基準の対応付け

対応する保証レベル	対策基準
レベル３	*各保証レベルの対策基準は、本ガイドラインの付録Ｂを参照*
レベル２	
レベル１	

保証レベルに応じた対策基準については、「付録Ｂ．認証方式の保証レベルに係る対策基準」を参照し、システム設計に当たっては、リスク評価の内容、導出された保証レベルの確保、対策基準の選択など、総合的な妥当性を確保するため、各府省は、それらの適切さを確保するため、専門的知見を有する者からの助言等を受けるものとする。

また、導出された保証レベルを確保するため、その妥当性を継続的に確認することとし、必要があれば、リスク評価結果等の見直しを行うこととする。

図　A-15　リスク評価に基づく認証方式の選択等の実施フロー



参考：『各保証レベルの適用が想定されるサービスの例』

各保証レベルを適切に使い分けるためには、その位置付けを正しく理解する必要がある。そこで、本ガイドラインがベースとした基準の１つである「OMB M-04-04」から、各保証レベルの想定サービスの例を紹介する。

「OMB M-04-04」では、レベル１を本人の身元を識別することはせず、あえて匿名によるサービス提供を想定する場合に相応しい保証レベルとしている。
また、レベル２とレベル３については、いずれも個人及び法人等の民間との幅広い業務が例示されており、特に、レベル３はより高い信頼性が求められる場合に適する保証レベルとされている。例えば、特許手続、政府調達、等のように、不正利用が競争相手を競争上優位に立たせる、あるいは財務上の大きな損失を発生させる可能性があるサービス等がレベル３の適用対象として例示されている。
最後に、レベル４については、非常に高い信頼性が求められる場合、例えば、「司法当局による犯罪歴データベースアクセス」、「規制医薬品の調剤に係る業務」等といった「政府機関内における極めて機密性の高い業務」が例示されている。

このような「OMB M-04-04」の例示を踏まえれば、本ガイドラインが適用範囲とする「個人・法人等と政府の間の申請・届出等のオンライン手続」に対しては主にレベル２又はレベル３の適用が想定される。一方、レベル４は、政府機関内において極めて重要性の高い業務を担う情報システムへの適用が想定される高い安全性を備えた保証レベルであることが分かる。また、必然的に、レベル４の対策基準の内容は極めて厳格なものとなる。

表　各保証レベルの適用が想定されるサービスの例（「OMB M-04-04」の場合）

保証レベル	サービスの例
レベル１	Web サイトにおけるオンラインディスカッション、等
レベル２	社会保障サービスに関する住所変更手続、等
レベル３	特許弁理士による特許手続、大規模な政府調達、等
レベル４	司法当局による犯罪歴データベースアクセス、規制医薬品の調剤、等

本参考例は２００３年１２月に公開された「OMB M-04-04」内に記載されている例に基づいて記述した。「OMB M-04-04」は保証レベルが４段階で整理されている。なお、２０１７年６月に公開された「デジタルアイデンティティガイドライン（NIST SP800-63-3)」において保証レベルは３段階に再整理されている。

『追加的対策を実施することでリスク軽減が可能なサービスの検討例』

オンライン手続における各保証レベルを適切に評価においては、申請時の認証のみならずその後の確認行為等の追加的対策を実施することでリスクを軽減することが可能な場合があるが、ここでは事業主が行う社会保険手続を具体例にとり、追加的対策を検討した結果を示す。

社会保険手続（事業主実施分）

１．リスク評価の実施

社会保険手続に関し、事業主が行うオンライン手続について、本ガイドラインに示す手法により、各手続に関する脅威を行政機関への申請行為のみに着目して分析した結果[1]、対象手続については以下 A～G の７種に分類されるとともに、各リスクの種類による影響度については、②「国民等の利用者に金銭的被害を与える、機関等に賠償責任が生じるなど、財務上の影響を与える」、④「国民等の利用者の個人情報等の機微な情報が漏えいする」のうち、１つ又は２つが高位相当又は中位以下相当との断定が困難との評価可能との分析が行われた。[2]

表 A-15-1 事業主が行う社会保険手続[3]とリスク評価（申請行為のみに着目した場合）

分類	リスク②	リスク④
A：保険の適用日・喪失日を申請内容に含む手続	○	○
B：保険料又は給付額算定の根拠となる報酬等を申請内容に含む手続	○	○
C：雇用継続給付申請に関する手続	○	○
D：口座振替等の登録・変更を申請内容に含む手続	○	○
E：郵送通知物の宛先となる住所の登録・変更を申請内容に含む手続		○
F：公的証明書の発行に関する手続	○	○
G：上記 A～F のいずれにも該当しない手続		○

２．追加的対策によるリスク軽減

上記の申請行為のみに着目する分析に加え、以下の追加的対策を実施した場合にリスクを軽減することが可能か検討した結果、下記の表に示す対策を講じることで、一定のリスク軽減が可能との分析が行われた。

1 本ガイドラインに従い、認証方式の有効性とは関係のない脅威については、リスク評価の対象外とするとともに、リスクの評価の実施に当たっては、電子署名や認証がすべて機能しない状態を前提にリスク評価を行っている。

2 IAL,AAL について実施。分析に当たり、幅広い申請者が多数の申請を行う社会保険手続固有の特性も考慮した。

3 2018 年末時点における手続について分析を行った。

表 A-15-2 追加的対策とその効果の例

分類	リスク	追加的対策	効果
A,B,C	第三者による修正申請等による給与額等や適用喪失日の改ざん、なりすまし申告により金銭的被害を受ける。[4]	・申請ごとの通知等[5] ・金銭的被害への補償措置[6] ・J-LIS との情報連携（C)[7]	・第三者による申請の探知 ・金銭的被害の抑制
A,B,C,D,F,G	個人情報を含む申請情報が、第三者からの行政機関への情報照会によって流出する。[8]	・情報照会時における本人確認の厳格化又は開示情報の限定[9]	・個人情報を含む申請情報の流出防止

３．認証方式の選択

当該追加的対策により軽減されたリスクを評価すると、分類 A,B,C 及び G の手続については、身元確認及び当人認証の保証レベル２に対応し、ログイン履歴の管理機能や未登録端末からのログイン検出機能等を有する法人共通認証基盤が提供する ID・パスワード（多要素認証）の認証方式の選択が可能と考えられる。(※1)（※2）[10]

(※1)上記については、幅広い事業主が多数の申請等を行う社会保険手続固有の特性も考慮しており、そのまま他の手続に援用できるものではない点に留意する。

(※2)現在、当該条件を満たす認証方式として法人共通認証基盤が提供する ID・パスワード（多要素認証）が該当するが、これと同等の認証方式が新たに整備された場合は、内閣官房情報通信技術(IT)総合戦略室に協議し適用を判断するものとする。

---

4 分類Dについては、多額の保険料を納付する場合の口座登録・修正を厳格に実施する必要があること等、分類Fについてはなりすましによる証明書発行により、二次的な被害が生じるリスク等を考慮する必要がある。

5 具体的には、事前登録されたアカウント・メールアドレスに対して、申請の都度、申請があった旨のメッセージを送付する等が考えられる。

6 具体的には、第三者による修正申請等により改ざんが生じた場合には、申請者が事実に即した申請情報に基づき一定期間内に届け出ることで、行政機関側が金銭被害への補償措置を講じること等が考えられる。

7 具体的には、雇用継続給付申請に係るリスク低減のため、氏名変更手続の際に J-LIS との情報連携を行い確認を実施する等が考えられる。

8 分類Eについては、情報照会行為がない場合であっても、郵送通知物の宛先変更を実施することで機微な情報漏えいが生じる場合があることを考慮する必要がある。

9 具体的には以下の方法が考えられる。
(ア)保証レベル3に対応する方式による情報照会しか認めない。
(イ)情報照会の際は、対面での本人確認を実施する、又は、保証レベル2に対応する方式で照会申請は受け付けるが、機微情報自体は本人限定受取郵便(基本型)により送付する。
(ウ)情報照会の際は、申請における機微情報は情報照会に応じない又は一切の情報照会に応じない。

10 配偶者からの暴力の被害者等、特殊な事情により、オンラインにおける情報照会に応じることが適切でない場合については、情報照会に応じない等の対応をとる必要があることに留意する。

付録Ｂ　認証方式の保証レベルに係る対策基準

１　保証レベル

本ガイドラインにおける「保証レベル」とは、認証方式の強度の違いを表す抽象的な指標である。保証レベルは、身元確認に関する「身元確認保証レベル」及び「当人認証保証レベル」に分けられる。表 Ｂ-1 に示すとおり、身元確認保証レベルは、例えば電子署名の検証、あるいはアクセス元に対する認証によって特定される（電子署名の生成者あるいはアクセス元の）身元識別情報の「信用度」を表す概念である。また、表 Ｂ-2 に示すとおり、当人認証保証レベルは、例えば電子署名の暗号鍵のトークン、あるいは認証に用いるトークンによって特定される当人認証の「信用度」を表す概念である。

本ガイドラインでは、認証方式における脅威に対する対策基準を、図 Ｂ-3 のようにそれぞれ４種類の評価軸（例えば、認証は「登録」「発行・管理」「トークン」「認証プロセス」）ごとに定めている。したがって、認証方式の保証レベルの評価に当たっては、評価軸ごとの保証レベルが異なる場合が想定され、そのような場合には、評価軸ごとの保証レベルの評価結果のうち最も低い保証レベルが当該認証方式の保証レベルとなる。

なお、本ガイドラインが採用するこのような認証方式の強度のレベル分けの考え方及びレベルの導出方法の考え方は、諸外国においても広く類似した考え方が採用されており、本ガイドラインでは主に以下を参考としている。

・ 米国の「連邦政府機関向けの電子認証に関わるガイダンス（OMB M-04-04）」、「電子認証に関するガイドライン（NIST Special Publication 800-63-3）」

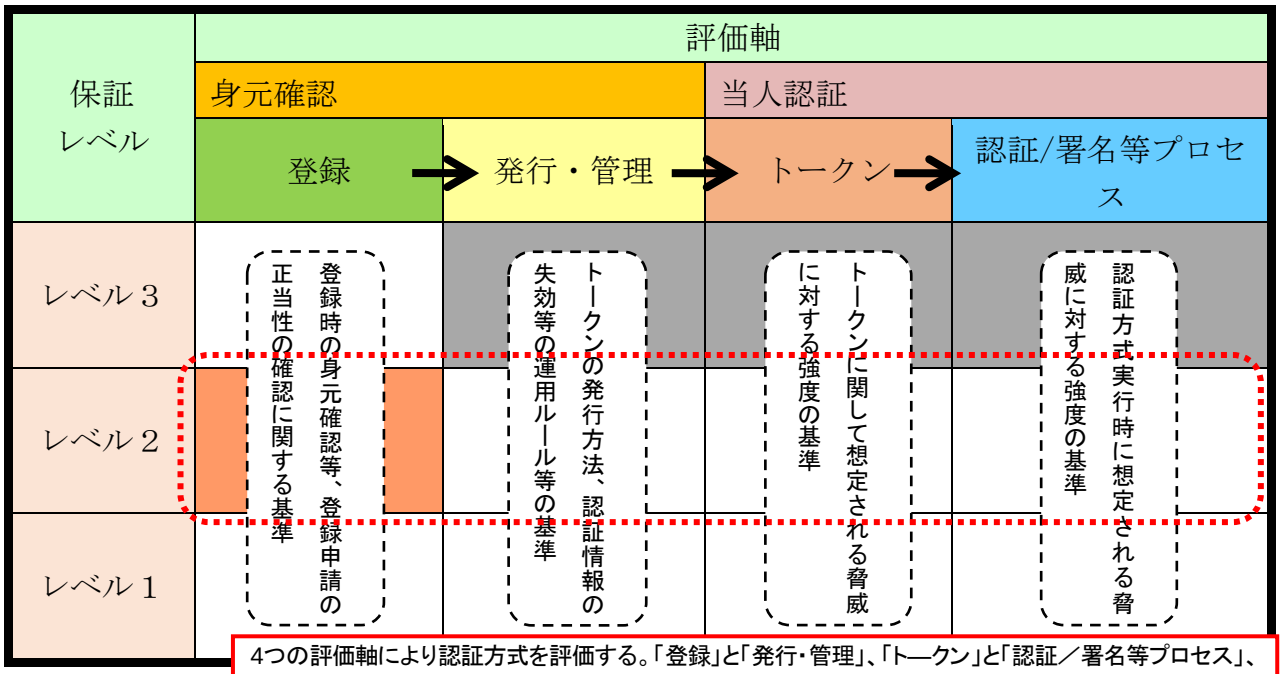
表 B-1 身元確認保証レベル

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。

表 B-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。

図 B-3 保証レベルの評価軸



4つの評価軸により認証方式を評価する。「登録」と「発行・管理」、「トークン」と「認証／署名等プロセス」、それぞれの評価軸の組み合わせにおいて、レベルが異なる場合には、より低いレベルが上位の評価軸である「身元確認」、「当人認証」それぞれの保証レベルとなる。（上記の場合は「身元確認」、「当人認証」ともにレベル２ ）

2　認証方式の基本概念実施

2.1　電子署名と認証

電子政府のオンライン手続における「申請者の特定」等のように、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を、本ガイドラインでは「認証」と呼び、特に認証の実行方法を「認証方式」と呼ぶ。

一般には、アクセス主体に対する認証は単に「認証」と呼ばれる場合が多いため、本ガイドラインにおいても、「認証」を同様の意味の用語として用いるものとする。一方、電子文書（電子データ、メッセージ等）の作成主体（生成主体）の認証については、当該電子文書に対して作成者によって付与された「電子署名」を検証する方法が用いられる。

2.2　適用対象電子署名と認証の使い分けの考え方

ここでは、オンライン手続における代表的な以下の 3 種類の脅威を考える。

- 他人になりすまして申請される（なりすまし）
- 申請後に申請内容を改ざんされる（改ざん）
- 実際には申請済みであるにもかかわらず、その事実を否認される（事実否認）

電子署名と認証をそれぞれ個別の技術として捉える場合、一般的には、電子署名が上記のいずれの脅威に対しても有効に働き、認証は「なりすまし」を対象とした対策に位置付けられる。[1]

一方、情報システムの設計に当たっては、脅威に対する有効性に加え、利用・運用コスト、性能等を含む総合的な観点から対策を合理的に選択することが求められる。表 B-4 は、認証に証跡を組み合わせることによって、改ざん、及び事実否認の脅威に対しては一定の対策効果を得ることが可能である点に着目し、脅威と対策の関係を例示したものである。

1　オンライン手続を例に電子署名の働きを整理すると、電子署名の検証は、署名生成者（申請者）の認証に加え、署名対象（申請内容）の完全性、及び署名対象（申請内容）に対する署名生成者の意思（申請の意思）を確認することと捉えることができる。

また、現状の実装技術においては、電子署名は認証と比較して技術単体にて対処可能な脅威の幅が広い反面、高度な利用環境や運用が必要となりコストが高まる傾向がある。また、認証に証跡を組み合わせる方法は、利用者側の負担を抑え利便性を確保し易い一方で、証跡の記録保管を担うシステムや運用者の信頼性の確保策が重要となる。認証方式の合理的な選択、設計のためには、各技術の特性と適用対象となるシステムの要件を踏まえた慎重な検討が求められる。

表 B-4 認証と電子署名による対策例の比較

脅威	認証を主に用いた対策例	電子署名を用いた対策例
なりすまし	（認証） 認証によって、申請元（アクセス元）の身元識別情報を特定する	（電子署名） 申請情報に付与された電子署名の検証によって身元識別情報を特定する
改ざん	（認証＋証跡） 申請元（アクセス元）を認証した上で、当該申請者の申請内容を証跡として保管する （※送受信中の改ざんに対しては暗号通信により対処）	（電子署名） 申請情報に付与された電子署名の検証によって改ざんの有無を検出する
事実否認	（認証＋証跡） 申請元（アクセス元）を認証した上で、当該申請者の申請記録（操作記録）を証跡として保管する	（電子署名） 申請情報に付与された電子署名の検証によって身元識別情報が表す主体による申請事実を確認

３　認証に係る対策基準

３．１　認証フレームワーク

表　B-5 に示すように、認証の実行のために必要な構成要素は、「登録」「発行・管理」「トークン」「認証プロセス」である。

登録による身元確認の結果、認証の対象者はシステムの「加入者」となる。加入者に対しては、身元識別情報（あるいは、システムにおいて加入者を一意に識別可能ななんらかの属性情報等）に関連付けられた認証情報、及び当該認証情報を格納するトークンが発行される。

認証プロセスでは、加入者が認証の要求者として身元識別情報をシステムに主張するとともに、認証情報を当該要求者が保持していることをシステムが検証する。この検証によって、当該要求者と身元識別情報との同一性、すなわち当該要求者が加入者であることを判定することが可能となる。

表 B-5 認証フレームワークの構成要素

	構成要素	説明
身元確認	登録	認証の対象者の身元確認を行うプロセスであり、機能的には RA が担う。
	発行・管理	登録による身元確認の結果（身元の保証）に基づいて、認証情報、トークンの発行、及び管理を行うプロセスであり、機能的には CSP が担う。
当人認証	トークン	認証要求者が所持し管理する何かであり、認証情報等の認証に用いる情報を格納又は出力するハードウェアやソフトウェア（IC カード、ワンタイムパスワード生成機器等）、あるいは知識等の認証情報そのもの（パスワード等）等がある。
	認証プロセス	認証要求者の身元識別情報を特定し、認証情報を保持していることを検証することによって、当該対象者が主張する身元識別情報との同一性を検証するプロセスである。

３．２　登録

認証を希望する者（例えば、認証を要するサービスの加入希望者）は、「申請者」として登録申請を行う。登録申請に当たっては、申請者が 1 つ又は複数の本人確認書類を提示することによって、RA による身元確認が行われる。

表 B-6 は登録申請における脅威と対策の例であり、表 B-7 は対面により登録申請を実施する場合、表 B-8 は遠隔（郵送やオンライン等）により登録申請を実施する場合の各保証レベルの対策基準である。表 B-8 に記載のとおり、レベル３の保証レベルでは遠隔による登録申請が認められない。

高い保証レベルほど、身元確認のために用いられる本人確認書類及び当該本人確認書類の提示プロセスに求められる信頼性は厳しいものとなる。また、レベル１の保証レベルでは、申請者の身元確認は特に必要ではなく、申請者が名前等の情報を提示した場合、そのまま受け入れる。そのため、レベル１において登録された名前などは全て仮名として扱われる。

表 B-6 登録における脅威と対策の例

脅威／攻撃	説明	脅威の例	対策の例
存在性の詐称	現実には存在しない架空の人物へのなりすまし	偽造パスポートの提示	発行元への問い合わせ等による偽造パスポートの検証
生存性の詐称	過去に存在していたが、現在は生存していない人物へのなりすまし	死亡した人物の本人確認書類の提示	生存していなければ提示困難な本人確認書類の提示を求め矛盾点を検出
当人性の詐称	実在する他の人物へのなりすまし	他人の本人確認書類の提示	顔写真付きの本人確認書類によりなりすましの検出
唯一性の詐称	同一人物による不正な重複登録	個人情報を一部変更する等して登録を申請	過去の記録と照合し類似の申請事実を検出
登録の否認	登録事実の否認	トークン受領後に登録事実を否認	登録申請書への署名

表 B-7 登録の保証レベル（対面の場合）

対策基準	身元確認保証レベル（※1）		
	1	2	3
電子メールアドレスが申請された場合、有効性（到達性）を確認する。	◎	○	○
申請者は、公的な写真付きの身分証明書（マイナンバーカード、運転免許証、パスポート等）を 1 種類、又は、その他の身分証明書を 2 種類提示する。		◎	◎（※2）
申請者の氏名や住所等の公的な台帳との照合、又は申請書に添付された公的証明書（住民票等）によりチェックする。		◎	◎（※3）
重複登録ではないことを確認する。			◎

※1　「◎」は各保証レベルへの準拠に当たり必須の対策基準、「○」は任意の対策基準であることを示す。

※2　公的な写真付きの身分証明書を必須とする

※3　公的な台帳との照合を必須とする

表 B-8 登録の保証レベル（遠隔の場合）

対策基準	身元確認保証レベル（※1）		
	1	2	3
電子メールアドレスが申請された場合、有効性（到達性）を確認する。	◎	○	
申請者の氏名と住所等及び身元確認に有効な他機関の登録情報（クレジットカード番号等　※2）が記載された申請書により申請する。		○	
申請者の氏名や住所等の公的な台帳との照合、又は申請書に添付された公的証明書（住民票等）によりチェックする。		◎	
申請者の氏名と住所等が記載された申請書に本人の電子署名（郵送の場合は署名又は捺印）を付与して申請する。		◎（※3）	

※1　「◎」は各保証レベルへの準拠に当たり必須の対策基準、「○」は任意の対策基準であることを示す。

※2　登録申請に当たってクレジットカードによる決済行為を伴う場合には、結果として他機関であるクレジットカード会社の登録情報に基づく対象者の存在確認の効果が得られると考えられる。

※3　電子署名は対象の保証レベルと同等の基準を満たすものの利用が望ましい。

３．３　発行・管理

発行・管理業務では、登録業務の結果を受けて、認証要求者に対し、認証情報とトークンの発行を行う。簡易な発行業務では、登録業務の一環として、認証要求者がトークン（例えば、パスワード）の登録を行うことも含まれる。利用期限切れ、又は失効した認証情報やトークンに対して、再発行や回収も行う。

表 B-9 は、発行・管理業務における脅威と対策の例であり、表 B-10 は各保証レベルの対策基準である。

表 B-9 発行・管理における脅威と対策の例

脅威	脅威例	対策例
暴露（漏えい）	パスワードが、CSP から利用者に送付される過程、あるいは CSP の装置内の残留によって、攻撃者に流出する。	・ 本人に直接トークンを手渡す。 ・ 本人の確認済み住所に郵送する。 ・ 高い機密性を持つプロトコルを用いてオンラインにて発行する。 ・ CSP の設備を隔離された部屋に設置する等して保護する。
改ざん	利用者によるパスワードの変更の過程で（例えば、利用者から CSP にパスワードを送信中に）、攻撃者によってパスワードが不正に変更される。	・ 本人の確認済み住所に郵送する。 ・ 高い機密性を持つプロトコルを用いてオンラインにて発行する。 ・ 認証によって CSP の正当性を確認する。
権利を持たない者への発行	利用者であると主張する不正な利用者に、正規利用者に発行されるべき認証情報（パスワード等）が発行される。	・ トークンを受領する者が登録手続を行った者と同一であることを確認する。

表 B-10 発行・管理の保証レベル

保証レベル	対策基準
レベル１	〔発行〕 ・認証情報及びトークンが、本人の電子メールアドレスに対して送付される。又は、オンラインでの登録手続の過程で、本人が認証情報及びトークンをダウンロードする。 〔管理〕 ・検証者が使用する秘密情報（アカウント管理情報等）はアクセス制御によって保護され、パスワードのような秘密情報を平文のままで含まない。
レベル２	〔発行〕 ・認証情報及びトークンが、以下のいずれかの方法により本人に配付される。（１）窓口にて直接手渡される、（２）本人住所に書留郵便又は本人限定受取郵便にて送付される、（３）本人住所に書留郵便又は本人限定受取郵便にてパスワードが送付され、本人が当該パスワードによる認証の上で、認証情報及びトークンをダウンロードする、（４）申請者が電子署名を付与した申請を行い、それが検証された後で、認証情報及びトークンをダウンロードする。（５）申請者が携帯電話の電話番号の申請を行い、その携帯電話の電話番号が検証された後で、認証情報及びトークンをダウンロードする。 〔管理〕 ・レベル１と同等以上の対策基準とする。 〔更新／再発行〕 ・認証情報及びトークンの更新、再発行に関する運用ポリシー（認証情報や登録情報等の更新の必要性や手続方法等）が策定され、周知されている。 ・特にオンラインによる手続の場合には、既存の認証情報及びトークンを用いた認証の上で、通信を暗号化して行う。 〔失効〕 ・認証情報及びトークンが有効ではなくなった、又は危殆化されたことを通知された時から、認証情報及びトークンを遅滞なく失効する。 〔記録保管〕 ・認証情報及びトークンの発行、管理に関する記録を、当該認証情報の有効期限又は失効時期の遅い方の時期から一定期間保管する。 ・記録を定期的に分析、評価する。

保証レベル	対策基準
レベル３	〔発行〕 ・認証情報及びトークンが窓口にて直接手渡される。（本人限定受取郵便基本型、及び同サービスと同等の手段による身元確認は対面として扱う） 〔管理〕 ・レベル２と同等以上の対策基準とする。 〔更新／再発行〕 ・レベル２と同等以上の対策基準とする。 〔失効〕 ・レベル２と同等以上の対策基準とする。 〔記録保管〕 ・レベル２と同等以上の対策基準とする。

３．４　トークン

トークンとは、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。

トークンは、認証の 3 要素（知っているもの、持っているもの、生体情報）のうち、一つ以上のものを利用し、認証プロトコルに対する入力となる認証情報を出力する。表 B-11 に、代表的なトークンの種類を示す。

トークンを奪った攻撃者は、トークンの所有者になりすますことができる可能性がある。トークンに対する脅威は、トークンを構成する認証要素の種類別の攻撃で分類することができる。

- 「持っているもの」が盗まれて、攻撃者によって複製された場合。(例えば、銀行のキャッシュカード等の磁気カードの磁気情報が盗まれて、カードを複製される場合)
- 「知っているもの」が攻撃者に開示されてしまった場合。(例えば、入力されたキー情報を盗み出すプログラムによって、パスワードが盗まれる場合)
- 「生体情報」がコピーされてしまった場合。(例えば、指紋が盗まれて不正な指紋認証を実行可能な人工的な指を作られた場合)

なお、本文書では、利用者が攻撃者と共謀して検証者を騙すような攻撃は、検討の範囲外とする。このことを前提として、脅威を表 B-12 にまとめた。また、これらの脅威を踏まえ策定した各保証レベルの対策基準は表 B-13 であり、対策基準の実現例は表 B-14 である。

表 B-11 トークンの種類

種類	定義
ハードウェアトークン	保護された暗号鍵を備えているハードウェアデバイス。この鍵を利用して認証情報を出力することで認証を達成させる。暗号鍵の保護機構はハードウェアにより実装され、ハードウェアトークンからは暗号鍵を取り出すことができないものとする。また、トークンを活性化させるためにパスワードの入力を利用者に求める機能を有する場合がある。
ソフトウェアトークン	ハードディスクなどの媒体に暗号鍵を格納し、この鍵を利用して認証情報を出力することで認証を達成させる。暗号鍵の保護機構はソフトウェアにより実装されるため、柔軟な運用が可能である一方で、一般的にハードウェアトークンよりも暗号鍵の複製に対する耐性を確保しづらい。また、トークンを活性化させるためにパスワードの入力を利用者に求める機能を有する場合がある。
ワンタイムパスワードトークン （OTP トークン）	認証に使用する「ワンタイム（一回限り）」のパスワードを生成する機能を有するトークンであり、装置や紙等のハードウェア、あるいはソフトウェアといった様々な実装方法が有り得る。また、トークンを活性化させるためにパスワードの入力を利用者に求める機能を有する場合がある。
パスワードトークン	利用者が記憶している秘密情報のみを利用して認証を行う。

表 B-12 トークンにおける脅威と対策の例

脅威	説明	脅威例	対策例
盗難	トークンが奪取される。	・ハードウェアトークン、OTP トークン、携帯電話等の盗難	・PIN 認証や生体認証によって、正当な持ち主のみがトークンの活性化可能とする。
複製	トークンの複製が作られる。	・紙に手書き又は印字されたパスワードの盗み見 ・電子ファイルに格納されたパスワードのコピー ・ソフトウェアトークンの盗難による複製	・ハードウェアトークンのような複製が技術的に困難なトークンを使用する。

脅威	説明	脅威例	対策例
盗聴	トークンや認証情報を使用する過程で攻撃者に盗聴される。	・肩越しからのパスワードの覗き見 ・キーボードの入力ログからパスワード等を不正に取得 ・認証時の入力機器を通じてPIN や指紋情報等を不正に取得	・ワンタイムパスワードトークンを使用する。
オンライン上での推測	オンラインにて認証要求を行う方法によって認証情報を推測する。	・辞書に掲載された単語を元にする等して、考え得る認証情報をオンラインにて認証に使用し、正しいものを推測	・エントロピーの高い十分な複雑性を備えた認証情報を格納あるいは生成するトークンを使用する。
オフライン分析	トークンが不正に解析される。	・盗まれたハードウェアトークンに対する物理的な解析 ・ソフトウェアトークンに対する PIN の推測による特定	・耐タンパ性が立証されたハードウェアトークンを使用する。 ・PIN 認証の失敗が一定回数繰り返された場合に以降の PIN 認証を禁止し、使用不能となるトークンを使用する。
フィッシング／ファーミング	サービス提供者へのなりすまし等によりトークンや認証情報が盗まれる。	・不正なサービス提供者（銀行等）を装った偽のメールにより、不正な Web サイトに利用者を誘導し、パスワードを不正収集 ・DNS の登録情報の改ざんにより不正なWebサイトに誘導し、パスワードを不正収集	・ワンタイムパスワードトークンを使用する。
ハードウェア危殆化	技術革新等により安全性が低下する。	・技術革新等により、ハードウェアの耐タンパ性や暗号機能が危殆化する。	・ハードウェアを交換する。 ・ハードウェアのファームウェアを更新する。

表 B-13 トークンの保証レベル

対策基準	当人認証保証レベル（※1）		
	1	2	3
［単一又は複数による認証］ 記憶された秘密、認証デバイスの所有、生体の特徴のいずれか１つ以上の認証要素を利用すること。	◎	○	○
［複数要素認証又は複数トークンによる認証］ 複数の認証要素を利用すること。		◎	◎
［所有による認証かつ複製に対する強い耐性を有する認証］ 耐タンパ性（Common Criteria による EAL4+、又は JCMVP のセキュリティ評価に基づく耐タンパ性等）が確保されたハードウェアトークンを利用し、トークン・認証情報の複製に対し強い耐性を有すること。			◎

※　1　「◎」は各保証レベルへの準拠に当たり必須の対策基準、「○」は任意の対策基準であることを示す。

表 B-14 トークンの対策基準の実現例

当人認証保証レベル	実現例
レベル１	（パスワード[12]、認証デバイス、生体認証） ・事前登録したパスワード等の記憶された秘密 ・パスワードなしのソフトウェアワンタイムパスワードトークン ・指紋認証等の生体認証
レベル２	（ソフトウェアトークンとパスワードなどの複数のトークンの組み合わせ） ・パスワード付きソフトウェアワンタイムパスワードトークン ・パスワード付きソフトウェアトークン ・パスワード付きハードウェアワンタイムパスワードトークン
レベル３	（耐タンパ性を有する IC カードや USB トークンなど）（※１） ・ 耐タンパ性を有するパスワード付きハードウェアトークン

※１　法律に基づき設置された団体等が、申請者の身元情報や資格を確認した上で発行する電子証明書に関するパスワード付きソフトウェアトークンについては、当該資格を所管する省庁によって有資格者本人に対する通知を行うことが可能であること等を踏まえた追加的対策によりリスク軽減がなされたと評価される場合には、所管省庁の判断において、保証レベル２に対応する認証方式の選択も可能と考えられる。

1 パスワードの設定に当たっては、政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）6.1 情報システムのセキュリティ機能を参考とされたい。

2 パスワードの実現例としては、以下のようなものが挙げられる
- 94 種類の文字（アルファベット、数字、記号）による 6 桁以上の無作為（ランダム）のパスワード、かつ 3 回連続失敗時は 1 日間パスワード入力不可、かつ有効期限 10 年以内
- 94 種類の文字（アルファベット、数字、記号）による 8 桁以上のユーザ選択によるパスワード、かつアルファベット・数字・記号の全てを用い、かつ辞書に掲載された単語ではない、かつ 3 回連続失敗時は 1 日間パスワード入力不可、かつ有効期限 10 年以内
- 数字による 6 桁以上の無作為（ランダム）のパスワード、かつ 3 回連続失敗時は 1 日間パスワード入力不可、かつ有効期限 10 年以内

３．５　認証プロセス

認証プロセスは、認証要求者が認証情報を保持していることを確認することによって、認証要求者と、認証要求者が主張する身元識別情報の同一性を検証するプロセスである。認証要求者は、認証情報をトークンに格納した上で保持するため、認証プロセスにおいては、認証要求者が正当なトークンの保持者であることの検証も行われる。

また、認証プロセスにおいては、認証要求者の認証情報の検証を行う者を　検証者と呼ぶ。検証者とサービス提供者が同一である場合と異なる場合が想定　されるが、本ガイドラインでは、同一である場合のみを前提とする。なお、異なる場合には、サービス提供者が検証者から検証結果を受理するプロセスに係る脅威を分析し、対策を講ずる必要性が生じる場合があることに注意が必要である。

表 B-15 は、認証プロセスの実行過程において想定される主な脅威と対策の例である。これらを踏まえ、表 B-16 に、認証プロセスに関する各保証レベルの対策基準を示す。

表 B-15 認証プロセスにおける脅威と対策の例

脅威	説明	脅威例	対策例
オンライン上での推測	攻撃者が、繰り返しログインを試行するなどして、認証情報（パスワード等）を推測する。	攻撃者がWebページにアクセスし、加入者のID と一般的な文字列等を元にして推測したパスワードを入力して、ログインを試みる。	・一定期間内に実行可能な認証の回数を制限する。 ・パスワードによる認証と CAPTCHA を組み合わせる。
フィッシング	利用者を欺いて、不正なサイトに誘い出し、情報を不正に取得する。	不正な電子メールによる不正な Web サイトに利用者を誘導し、ユーザ名やパスワード等の情報を入力させる。	・正当なサービス提供者に接続したことを認証プロトコル（EV-SSL 証明書を用いた TLS 等）によって確認する。 ・データを傍受されても、当該データを悪用できないように正しい相手との間で通信内容に暗号化を施す。
ファーミング	利用者を、強制的に不正なサイトにアクセスさせ、情報を不正に取得する。	DNS の登録情報の改ざんにより偽のWebサイトに利用者を導き、ユーザ名やパスワード等の情報を入力させる。	

脅威	説明	脅威例	対策例
盗聴	通信を盗聴し、情報を不正に取得する。	利用者がサービス提供サイトにアクセスする際の通信内容を傍受し、パスワード等の認証情報を取得する。	・通信内容を暗号化する。
リプレイ攻撃	認証に関する通信を盗聴し、同じ内容を再度送信してなりすましを行う。	利用者とサービス提供サイトの間の通信を盗聴することによって、認証プロトコルの一部又は全部を傍受し、再度送信する。	・認証要求ごとにランダムなデータを生成し、これを認証プロトコルにて交換される情報に含めることによって、攻撃者が同じデータを使用して認証要求を行っても、認証に成功しないようにする。
セッション・ハイジャック	認証プロトコルが完了した後に、利用者とサービス提供者の接続を奪うことによって、正当な利用者に代わってサービスを利用する。	HTTP プロトコル等により交換されるセッション情報（クッキー等）を盗聴又は推測することによって、接続を乗っ取る。	・端末に対して、ウイルス、トロイの木馬などの不正検知等のための総合的なセキュリティ対策（ウイルスチェックソフトの導入等）を実施する。
中間者攻撃	利用者とサービス提供者の通信を中継する形で横取りし、改ざん等の不正を行う。	ルータに侵入する等して、サービス提供者と利用者の間の通信に割り込み、両者が暗号通信のための鍵を交換する際、代わりに攻撃者の鍵をそれぞれに送信することによって、攻撃者の存在を気づかせることなく、以後の暗号化された通信内容を傍受する。	・正当なサービス提供者に接続したことを認証プロトコルによって確認する。

表 B-16 認証プロセスの保証レベル

対策基準（対策を講ずるべき脅威）	当人認証保証レベル（※1）		
	1	2	3
オンライン上の推測	◎	◎	◎
リプレイ攻撃	◎	◎	◎
盗聴	◎	◎	◎
セッション・ハイジャック	◎	◎	◎
中間者攻撃	△	△	◎
フィッシング／ファーミング		◎	◎

※1　「◎」は各保証レベルへの準拠に当たり必須の対策基準、「△」は対策の強度に制約を設けて良いことを示す。

４　署名等に係る対策基準

４．１　署名等フレームワーク

「２　認証方式の基本概念実施」にて述べたとおり、電子署名は、「改ざん」「事実否認」の脅威に対する有力な対策技術である。

一方、「２　認証方式の基本概念実施」にて述べた認証は「なりすまし」に対する対策技術であると同時に、必要十分な信頼性を備えた証跡管理技術を組み合わせることによって、改ざん、及び事実否認の脅威に対しても一定の対策効果を得ることが可能である。例えば、電子政府のオンライン手続において、申請者の認証を行った上で、認証結果、及び当該申請者の申請内容と申請事実を証跡として記録・保管することを考える。この証跡に対して、セキュリティ技術（タイムスタンプ等）、あるいはセキュリティ基準に基づく厳格な運用によって、サービス提供に当たり必要十分な信頼性を確保することを想定すれば、認証を用いる場合でも、申請内容の改ざん、申請事実の否認といった脅威を軽減することが可能となる。

なお、技術的視点から見れば、電子署名による「改ざん」「事実否認」の対策効果と、認証と証跡の組み合わせによる対策効果は必ずしも等価ではない。したがって、これらの技術をサービスに適用するに当たっては、当該サービスにおいて想定される各脅威の対処方針（どの脅威に対処し、どの脅威は許容するか）を慎重に検討する必要がある。

以降、本ガイドラインでは、以上のような申請内容の完全性及び申請事実の非否認性を確保するための措置を「署名等」と総称する。

表 B-17 に示すように、署名等フレームワークと表 B-5 に示した認証フレームワークの差異となる要素は「署名等プロセス」であると捉えると分かりやすい。そこで、「登録」「発行・管理」「トークン」の対策基準については、「３　認証に係る対策基準」の「認証」の対策基準に準ずることとし、ここでは「署名等プロセス」の対策基準に関して述べる。

表 B-17 署名等フレームワークの構成要素

構成要素	説明
登録	認証の対象者の身元確認を行うプロセスであり、機能的には RA が担う。
発行・管理	登録による身元確認の結果（身元の保証）に基づいて、認証情報、トークンの発行、及び管理を行うプロセスであり、機能的には CSP が担う。
トークン	認証の対象者が認証情報を保持するための格納媒体である。
署名等プロセス	認証要求者に対する認証、及び当該認証要求者の意思（本ガイドラインでは、例えば、申請事実及び申請内容を想定）の確認を行うプロセスである。以下の 2 種類の実現方式が考えられる。 〔電子署名を用いる場合〕 ・ 認証要求者が電子文書（本ガイドラインでは、例えば申請書等）に対して生成した電子署名を検証することによって、電子署名の生成者の身元識別情報の特定及び当該身元識別情報と電子署名の生成者の同一性を検証するとともに、当該電子文書の内容の完全性と当該認証要求者の意思を確認する。 〔認証及び証跡管理技術を用いる場合〕 ・ 認証フレームワークにおける「認証プロセス」による対象者の認証を行った上で、当該対象者による操作に基づいてその意思を確認する。加えて、当該対象者の操作（本ガイドラインでは、例えば、申請に係る一連の操作、申請内容、意思確認、等）を記録、保管した情報を証跡として用いることによって、事後の申請内容の改ざん、申請事実の否認に対処する。

４．２　署名等プロセス

署名等プロセスにおいて、想定される主な脅威と対策の例を表 B-18 に示す。

表 B-19、表 B-20 は、署名等プロセスにおける保証レベルごとの対策基準と実現例である。一般に、署名等が特に有効に働く脅威（例えば、申請内容の改ざん、申請事実の否認）を扱うシステムは、求める保証レベルが高位のものとなると想定されるため、本ガイドラインでは保証レベル２及び保証レベル３に絞って対策基準を定める。

表 B-18 署名等プロセスにおける脅威と対策の例

脅威	説明	脅威例	対策例
中間者攻撃	署名等プロセスに介入し、意図せぬ署名を生成させる。	・利用者が使用する機器やソフトウェアの脆弱性等を利用して、署名対象の改ざん、差し替え等を行い、利用者が意図しない対象に署名させる。	・利用者が、機器やソフトウェアの正当性を検証可能とする機能を搭載する。
アルゴリズム危殆化攻撃	危殆化した暗号アルゴリズムを用いるように誘導し、安全性の低い電子署名を行わせる。	・複数の暗号アルゴリズムを併用可能なシステムにて、危殆化した暗号アルゴリズムを用いるように利用者を誘導し、安全性の低い電子署名を行わせた後、改ざんを行う。	・危殆化した暗号アルゴリズムに関する機能をシステムから削除し、安全な暗号アルゴリズムのみが動作するようにする。
フィッシング	利用者を欺いて、不正なサイトに誘い出し、利用者が意図せぬ対象に電子署名を行わせる。	・不正なサイトに誘い出し、認証と見せかける、あるいは不正なデータを送付する等して、利用者が意図せぬ対象に電子署名をさせる。	・証明書等のトークンや認証情報を認証用と電子署名用とに分離、使い分ける。 ・認証用と電子署名用のトークンを活性化させるPINを分け、利用者が使い分けを意識しやすくする。

表 B-19 署名等プロセスの保証レベル

対策基準（※1）	当人認証保証レベル（※2）		
	1	2	3
電子政府推奨暗号リストに記載された公開鍵暗号による署名方式を用いること。		◎	◎
「表 B-13 トークンの保証レベル」の保証レベル２と同等の対策基準を満たすトークンを用いて署名等プロセスを実行すること。		◎	
電子署名用の証明書の用途を電子署名のみに限定すること。			◎
「表 B-13 トークンの保証レベル」の保証レベル３と同等の対策基準を満たすトークンを用いて署名等プロセスを実行すること。			◎

※１ 上記は、電子署名を用いる場合の対策基準である。本ガイドラインでは、認証及び証跡管理技術を用いる場合の対策基準について特に規定せず、別途検討すべき課題として位置付けるとともに、関連事項について「５．５ 証跡管理」にて述べる。
※２ 「◎」は各保証レベルへの準拠に当たり必須の対策基準であることを示す。

表 B-20 署名等プロセスの対策基準の実現例

保証レベル	実現例
レベル２	ソフトウェアトークン（PINあり）又はハードウェアトークン（PINあり）による電子署名
レベル３	耐タンパ性を備えたICカード（PINあり）やUSBトークン（PINあり）等による電子署名

５　基準実現のための配慮事項

本ガイドラインで定義された保証レベルを実現するためには、様々な配慮を行わなければならない。本章では、保証レベルを対策基準へ適用するに当たり考慮が望まれる事項について述べる。また、電子政府において、実装する際の複数の満たすべき要件について述べる。一方、各基準を実現したのち、実際にそれぞれのフェーズにおける実行のされ方を確認するために証跡管理を確実に行う必要性がある。そこで、証跡管理を正しく行うための目安について述べる。

５．１　対策基準の適用の考え方

対策基準を適用する際には、一律にそれぞれの保証レベルを実現する必要性がない場合がある。上位基準を適用するに当たっては、認証方式の強度とコスト及び利便性が一般的にトレードオフの関係にあるため、むやみに上位レベルの対策基準を採用するのではなく、コストや利便性等の多様な観点による総合的な判断が求められる。そこで、対策基準を適用する際には、安全側の発想に立って、与えられた保証レベルの上位レベルの対策基準を満たす方式を採用してもよい。これにより、与えられた保証レベルが２であっても、レベル３の対策基準を満たす方式を採用することが可能である。ただし、セキュリティ上の理由でむやみに上位レベルの対策基準を採用することは適切ではない。

また、本ガイドラインの対策基準は絶対的なものではなく、同等の代替基準であれば他の対応策による代替が許容されるものとする。そこで、各手続の事情により、対策基準の一部を満たさなくても同等のセキュリティが確保されると判断される場合には、対策基準の該当部分を見直しても差し支えない（例えば、十分な信頼性が確保された「自動交付機」を通じてトークンを発行する方法が将来的に確立された場合には、そのような方法を窓口にて手渡しによりトークンを配付する方法と同等とみなす等が考えられる。また、申請者が法人等に所属する者である場合には、登録申請時に身分証明書として社員証を確認する方法、社員番号や所属等の情報を申請する方法等が代替の運用として考えられる。）。

一方、複数の手続が一つにまとまっているサービスにおいて、それぞれの手続ごとに導出される保証レベルが異なる場合には、利用者から見える手続の姿や手続の利用状況等を十分考慮して、適切な対策基準を採用することが適当である。

５．２　標準仕様の採用

認証方式の実装に当たっては、標準化仕様を採用してインタオペラビリティを確保することが、認証方式の利用促進やシステム間連携の拡大等に有効である。標準仕様の採用によって、システムの構築時には想定していなかったシステムとの連携の可能性が生まれる場合もある。また、標準化、実用化された技術仕様の採用によって、既存の製品やサービスの活用が容易となるため、システムに対する認証方式の実装コストの低減を図る。

５．３　利用者への配慮

利用者に新たな機器の購入やソフトウェアのダウンロードを利用することは、利用者がその認証手段を利用する際の大きなハードルとなる可能性を持つ。セキュリティについて十分に配慮しなければならない場合以外の利用は、利用に際し、十分検討し総合的な判断が必要となる。また、電子政府ユーザビリティガイドラインによるユーザビリティテストを認証部分についても利用し、利用者の利便性を向上させることが求められる。

例えば、高齢者・障害者に使いにくい機能については、代替手段を提供するなどの配慮を検討しなければならない。これは、各種の認証・署名等の手段は、健常者には利用しやすくても障害者には非常に使いにくいものになる可能性がある。たとえば、視覚的 CAPTCHA は、視覚障害者には使用不能である。したがって、そのようなものを提供する場合には、聴覚的 CAPTCHA も同時に提供するなど、代替手段を提供するようにしなければならない。

５．４　異なる保証レベルの認証方式間の連携

サービスごとに保証レベルが異なる場合、サービスごとに異なる認証方式が設けられる可能性がある。この場合、一方のサービスの利用者は、保証レベルが異なる他方のサービスを利用することができず、また、利用者が複数のサービスを利用する場合には、保証レベルごとに複数の認証方式を使い分けなければならないなど、利用者の利便性を損ねる可能性がある。

ところで、認証方式を脅威の軽減技術としてのみ見る場合、上位の保証レベルの認証方式はより下位の保証レベルを求めるサービスの認証方式として代替的に用いることが可能な関係にある。一方、下位の保証レベルの認証方式は、追加的な認証処理を一時的に行うことによって、より上位の保証レベルを求めるサービスの認証方式として用いることが可能な関係にある。

このような保証レベルの関係に着目すると、複数のサービス間で共用する認証連携基盤の導入が、上記のような利用者の利便性を損ねる問題の解消に有効である可能性がある。すなわち、利用者は当該認証連携基盤を介してサービスを利用することによって、高々1 つの認証方式を利用しさえすれば、基盤を共用するすべてのサービスを利用することが可能となる。

５.５　証跡管理

証跡（ログ）管理は、本ガイドラインで定めた電子認証及び電子署名においてプロセスがどのように行われたかについての証拠を残すための手段として利用される。特に認証においては、署名以上に、証跡を電子文書として正しく取得管理することによって、完全性及び非否認性を証明することにつながる。

このような電子文書の管理を行うための目安が、総務省行政管理局 共通課題研究会によってまとめられた「インターネットによる行政手続の実現のために第５章　電子文書の原本性」（平成 12 年３月）において以下のように整理されている。（以下抜粋）

> *電子文書の保存・管理上の問題点をふまえ、電子文書の原本性を確保するために充足すべき要件としては、次の３つに整理することができる。*
>
> *ア　完全性の確保*
>
> *電子文書が作成された際、電子文書に対する改変履歴を記録すること等により、電子文書の改ざん等を未然に防止し、かつ、改ざん等の事実有無が検証できるような形態で、保存・管理されること。*
>
> *イ　機密性の確保*
>
> *電子文書へのアクセスを制限すること、アクセス履歴を記録すること等により、アクセスを許されない者からの電子文書へのアクセスを防止し、電子文書の盗難、漏洩、盗み見等を未然に防止する形態で、保存・管理されること。*
>
> *ウ　見読性の確保*
>
> *電子文書の内容が必要に応じ電子計算機その他の機器を用いて直ちに表示できるよう措置されること。*

また、この中では、要件担保のための措置の内容が示されており、アクセス管理の在り方や保管場所の決定その他の電子文書の管理に関するルールを整備することが必要であると述べられている。一方、このような証跡や署名を施した文書は、長期間の利用／保存が見込まれる場合がある。この場合、アルゴリズムの危殆化などの別の脅威が生じる可能性を持つ。そこで、長期保存した文書の

完全性及び非否認性を示すためには、タイムスタンプ署名を定期的に施すなどの処置をすべきである。

５．６　客観的評価による安全性の確認

電子署名及び認証に係る機能を情報システムに導入するに当たっては、当該技術の実行を構成する各要素（例えば、トークン、検証装置、証跡管理装置、等）について、認定基準に基づく第三者評価（Common Criteria、JCMVP によるセキュリティ評価等)、あるいは自己点検結果の公表、等により、安全性の客観的確認が可能であることが望ましい。

付録Ｃ　保証レベルに応じた対策基準の概要

■　各保証レベルに求められる具体的な対応基準を４つの評価軸ごとに規定
■　対策基準の適用の考え方（※１、※２）など、基準実現のための配慮事項についても規定

保証レベル	身元確認		当人認証		
	登録（※３）	発行・管理（※４）	トークン	認証プロセス	署名等プロセス（※３）
レベル３	（対面の場合） ・公的な写真付き身分証明書１種の提示 ・申請情報の公的な台帳照合 ・重複登録ではないことの確認	・手渡しによるトークン発行 ※本人限定受取郵便基本型及びこれと同等の手段は対面として扱う	・レベル２の基準に加え、耐タンパ性が確保されたハードウェアトークンを利用すること（※５）	・レベル２と同等の基準	・電子政府推奨暗号リストに記載の電子署名 ・電子署名用の証明書の用途は電子署名限定
レベル２	（対面の場合） ・公的な写真付き身分証明１種（又は他２種）の提示 ・申請情報の台帳（又は公的証明書）照合 （郵送又はオンラインの場合） ・申請書に対する電子署名（郵送の場合は署名又は捺印） ・申請情報の台帳（又は添付の公的証明書）照合	・レベル３の方法に加え、書留郵便、書留郵便＋ダウンロード、電子署名＋ダウンロード、携帯電話の番号検証＋ダウンロードによるトークン発行	・記憶された秘密、認証デバイス、生体認証の中から複数の認証要素を利用すること	・レベル１と同等の基準に加え、フィッシングの脅威に対する耐性	・電子政府推奨暗号リストに記載の電子署名
レベル１	（対面、郵送又はオンラインの場合） ・メールアドレスの到達確認 ※身元確認は不要	・レベル２の発行方法に加え、電子メールによる送付、ダウンロードによるトークン発行	・記憶された秘密、認証デバイス、生体認証の中から単一又は複数の認証要素を利用すること	・オンライン上の推測、リプレイ攻撃、盗聴、セッション・ハイジャック、中間者攻撃の脅威に対する耐性	－

※１　上位基準の採用：認証方式の強度とコスト及び利便性は一般的にトレードオフの関係にあり、コストや利便性等の多様な観点による総合的な判断が必要となる。
※２　代替基準の採用：ガイドラインの対策基準は絶対的なものではなく、同等の代替基準であれば他の対応策による代替が許容される。
※３　各レベルで掲載事項のうち該当するものを全て満たす必要がある。
※４　各レベルで掲載事項のいずれかを満たす必要がある。
※５　法律に基づき設置された団体等が、申請者の身元情報や資格を確認した上で発行する電子証明書に関するパスワード付きソフトウェアトークンについては、当該資格を所管する省庁によって有資格者本人に対する通知を行うことが可能であること等を踏まえた追加的対策によりリスク軽減がなされたと評価される場合には、所管省庁の判断において、保証レベル２に対応する認証方式の選択も可能と考えられる。