資料７－２

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

各府省情報化統括責任者（CIO）連絡会議決定

目次

図の目次

表の目次

1. ガイドラインの概要

1.1. 背景

「オンライン利用拡大行動計画（平成 20 年９月 12 日、IT 戦略本部決定）」は、これまでの国の行政手続におけるオンライン利用促進の取組を抜本的に見直し、対象を国民に広く利用されている手続に重点化し、新たな目標を設定して、オンラインのメリット拡大、使い勝手の向上等の措置を集中的に講ずることを目的として、2009 年度（平成 21 年度）から 2011 年度（平成 23 年度）までの間に講ずる措置を定めた政府全体としての行動計画として策定された。

同計画では、国民が広く利用するオンライン化された手続のうち、国民や企業による利用頻度が高い年間申請等件数が 100 万件以上の手続及び 100 万件未満であっても主として企業等が反復的又は継続的に利用する手続等を「重点手続」と分類し、オンライン利用率の大幅な向上を図るための重点的な取組対象としている。また、重点手続以外の利用促進対象手続についても、同計画に示すオンライン利用拡大方策を踏まえつつ、手続所管府省において計画的に取組を進めることとしている。

同計画には、目標の達成に向けた重点的取組が示されており、その１つに、電子政府の手続に応じたセキュリティ確保策、ユーザビリティ向上方策について政府横断的な統一ガイドラインを策定するための取組が掲げられている。これに沿って「電子政府ガイドライン作成検討会」が設置され、さらにその下部組織として、電子政府の手続に応じたセキュリティに関する検討を目的とした「セキュリティ分科会」、及び電子政府の手続利用シナリオに応じたユーザビリティに関する検討を目的とした「ユーザビリティ分科会」が設置された。

本ガイドラインは、電子政府の手続に応じたセキュリティ確保策の方向性等に関する「セキュリティ分科会」における議論内容を踏まえ、「電子政府ガイドライン作成検討会」において策定されたものである。

1.2. 目的･位置づけ

本ガイドラインは、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」の導入を検討するにあたり活用可能な対策基準を提供することを目的としている。本ガイドラインの主な規定範囲は、下記の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認証方式の検討を可能とすることを本ガイドラインの目的とする。

1.3. 対象とする手続

本ガイドラインにおいて対象とする手続は、オンライン手続のうち、「オンライン利用拡大行動計画」にて対象とされている国民・企業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。

なお、同計画が対象としていない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、国民と企業間で行われる民間のオンラインサービス等は、本ガイドラインの対象外としている。

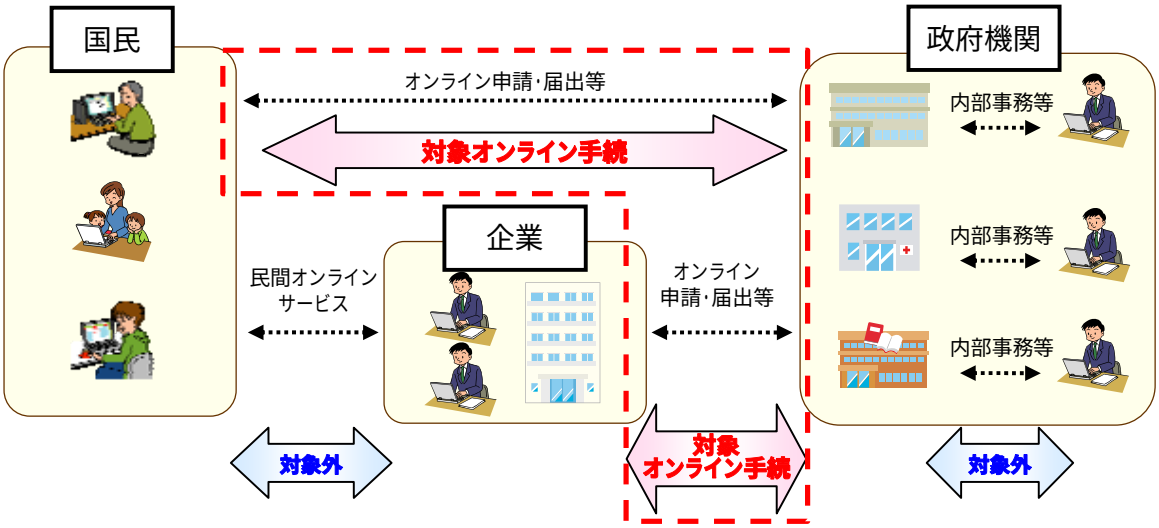

図 1-1 対象とする手続

2. 用語定義

表 2-1 用語

用語	語義
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。
IP スプーフィング	偽の IP アドレスを送信元アドレスに設定したパケットを作成して送信すること。DoS 攻撃 (サービス妨害攻撃) 等に利用される。
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、復号鍵 (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。
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。
オフライン	機器等が相互に接続されていない状態、あるいは機器等がネットワークに接続されていない状態のこと。
クレデンシャルサービスプロバイダ (Credentials Service Provider、CSP)	加入者のトークン及び認証情報を発行する機関のこと。
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。
真正性	ある情報の記載内容が、挙証者の主張する特定人の思想の表現であり、かつ改変されていないこと。

用語	語義
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なう手法のこと。
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」「対タンパ性がある」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。
DoS 攻撃	ネットワークに接続されたコンピュータに過剰な負荷をかけて、サービスの提供を不能に陥れる攻撃のこと。
DDoS 攻撃 （Distributed Denial of Service：分散サービス妨害）	標的に対して、複数のコンピュータ等を利用して DoS 攻撃を行うこと。攻撃元のコンピュータは、攻撃者自身のものとは限らず、ウイルスへの感染により意図せず攻撃者のコンピュータとなる場合もある。
電子署名 （Electronic Signature）	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。
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また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。

用語	語義
トークンの活性化	トークンの一部また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。
認証 (Authentication)	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 (およ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。
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。
パスワード	装置やシステム等の利用時にあたり、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であり、数文字の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。
本人確認	手続を行う人が実在し、本人であるかを確認すること。
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。
身元確認 (Identity proofing)	個人、企業、組織等を対象として、本人であること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、住所、氏名、生年月日、本籍、

用語	語義
	所属、資格、等について、当該情報を証明する書類の提示を求めることにより実施される。
身元識別情報 (Identity)	個人を一意に識別する情報。個人の法的な名前は必ずしも一意とは限らないため、個人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 (たとえば、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。

3.　認証方式の合理的な選択を目的としたリスク評価手法

リスク評価手法の策定にあたっては、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。

3.1.　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。

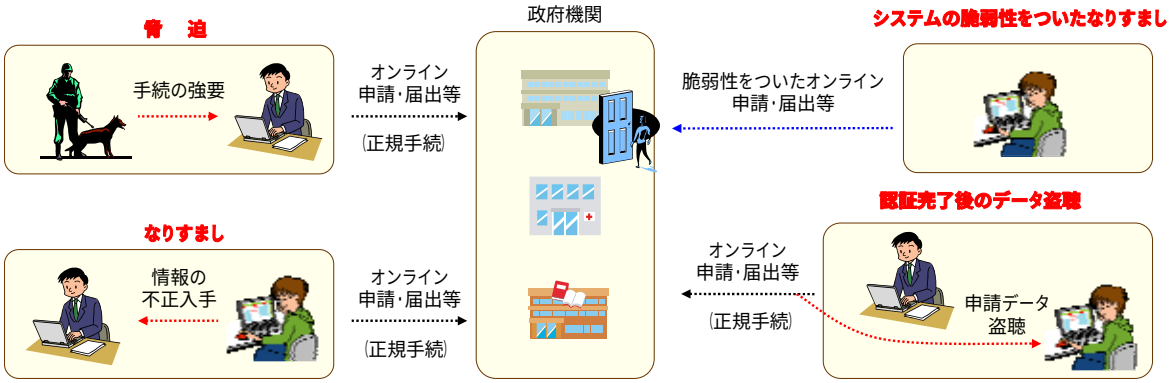

図 3-1 リスク評価の対象外となるケース

3.2. 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（国民・企業と政府の間の申請・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 3-1 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）」

3.3. 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。今回、そのレベルを「影響度」という尺度で４つのレベルに分類した。

このレベル分けにあたっては、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、以下の通りリスクの影響度を定義した。

表 3-2 リスクの影響度の定義

影響度	定義
特高	当該リスクの影響による損失が、組織の運営、組織の資産、または個人に致命的または壊滅的な悪影響を及ぼすと予想される
高	当該リスクの影響による損失が、組織の運営、組織の資産、または個人に重大な悪影響を及ぼすと予想される
中	当該リスクの影響による損失が、組織の運営、組織の資産、または個人に限定的な悪影響を及ぼすと予想される
低	当該リスクの影響が、測定可能な結果をもたらさない

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)」より作成

3.4. リスクの種類

経済産業省の「電子政府認証ガイドライン検討報告書」では、オンライン手続に関わる脅威に対するリスクについて、「身体の安全への被害」、「違反行為の実施」、「機微情報の漏えい」、「サービスの継続への被害」、「金銭的損害」及び「不便さ、苦痛又は地位や評判の毀損」の６つのリスクを想定している。

このうち、本ガイドラインが対象とするオンライン手続に関わる脅威として、3.2 節にて述べた詐欺行為がもたらすリスクを考慮すると、不正に情報を搾取されることによる「機微情報の漏えい」、不正な申請によってもらされる「金銭的被害」の２つが主に該当することが考えられる。そのため、本ガイドラインでは主たるリスクとして「機微情報の漏えい」、「金銭的被害」の２つのリスクについて考慮した。

表 3-3 リスクの種類

リスクの種類	オンライン申請との関係	重点 47 手続との関係
身体の安全への被害	該当する可能性がある	対象なし
違反行為の実施	該当する可能性が低い	対象なし
機微情報の漏えい	該当する	対象あり
サービスの継続への被害	該当する可能性がある	対象なし
金銭的損害	該当する	対象あり
不便さ、苦痛又は地位や評判の毀損	該当する可能性が低い	対象なし

3.5. 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が、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あたっては、電子署名や認証がすべて機能していない状態を前提にするものとする。

リスクの影響度の導出にあたっては、「金銭的損害」、「機微情報の漏えい」、「身体の安全への被害」、「違反行為の実施」、「サービスの継続への被害」及び「不便さ、苦痛又は地位や評判の毀損」等を含むあらゆるリスクを考慮し、総合的にリスクの影響度を勘案する。

他方、3.4 節にて示した通り、対象オンライン手続においては、電子署名を要する 47 の重点手続を対象として調査を行ったところ、「金銭的損害」と「機微情報の漏えい」の２つが主たるリスクとして発生する可能性が確認された。

そのため、電子政府におけるオンライン申請等の手続について、リスク評価方法を検討するにあたっては、電子署名を要する 47 の重点手続を対象として、上記の２つのリスクの影響度の評価に関する定量的評価方法や 47 の重点手続以外の手続への当該方法の適用可能性、二次的被害のリスク等の手続固有の特性やその他のリスク等の反映方法について検討し、それらの内容をリスクの影響度を導出する方法として取りまとめた。

3.5.1. 金銭的損害に係るリスク評価方法（基礎的評価方法）

オンライン手続には、申請や届出、報告、閲覧など様々な目的を持った手続が存在するが、それらの手続に関わる脅威に対するリスクの影響度を導出するにあたっては、それらの手続を横串しで比較できるような共通的に発生する可能性があるリスクを評価軸として位置付けることが重要となる。このような位置付けを持つリスクとしては、「金銭的損害」が適当であると考えられる。

また、こうした意味において、金銭的損害に係るリスクの影響度は、各手続相互のリスク評価結果を比較する上で、共通の「ものさし」となることから、あらゆる手続の基礎的評価として導出されることを原則とする。

金銭的損害に係るリスクの影響度の導出にあたっては、「事案がもたらす被害規模」と「申請等に係る厳格さ」の２つの評価軸を設定する。

２つの評価軸のうち、「事案がもたらす被害規模」については、個人や企業等が所有する財産・資産の損失額として認識できる場合が多いことから、その金額の多寡でもって、影響の度合いを推量できるものとする。

また、「申請等に係る厳格さ」については、なりすましなどの不正な行為によって受ける影響が高くなるほど、本人確認や申請書等の真正性確保において求められる確認の厳格さが高くなると認識できる場合が多いことから、基礎的なデータベースとの突合や公的証明書等による確認の実施状況をもって、影響の度合いを推量できるものとする。

各要素について「低、中、高、特高」の４段階のレベルを設定し、基礎的なリスクの影響度を導出する。

3.5.1.1. 事案がもたらす被害規模

事案がもたらす被害規模については、損失額という直接的な被害のみを取り扱い、補償や補填、システム復旧に係るコスト等の間接的な被害によるものについては、対象外とするものとする。

また、被害規模については、当該手続の申請等１件当たりの平均金額の値を用いるものとする。よって、毎月所定の金額の給付金等が申請者等に支払われるような手続については、申請を繰り返すことよって期間内に支払われた給付金等の総額ではなく、あくまで申請１件当たりの平均支払金額を用いるものとする。

被害規模は、「低、中、高、特高」の４段階にレベル分けし、以下の通り定義するものとする。

表 3-4 被害規模のレベル

レベル	金銭的損害の程度
特高	1,000 万円以上の金銭的損害
高	100 万円以上、1,000 万円未満の金銭的損害
中	100 万円未満の金銭的損害
低	金銭的損害なし

なお、定期的な給付を継続して受ける場合への考慮や、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く、十分な配慮が必要な場合については、後述する「3.5.4 総合的リスク評価の導出方法」における、総合的リスクの評価の導出時に、反映させるものとする。

3.5.1.2. 申請等に係る厳格さ

申請等に係る厳格さについては、当該手続を所管する主体が本人確認や申請書等の真正性確保のために実施する、基礎的なデータベース（自ら保有するデータベース、他の主体が保有するデータベースの両方を含む）との突合や公的証明書等による確認状況をもとに、「低、中、高、特高」の４段階にレベル分けし、以下の通り定義するものとする。

表 3-5 申請等に係る厳格さ

レベル	申請等に係る厳格さの程度
特高	当該手続の申請等にあたり、本人確認又は申請書等の真正性確保のため、当該手続を所管する主体が保有するデータベースに加え、主体以外が保有するデータベースとの照合を実施している、もしくは厳格な公的証明書等[注]による確認を実施している
高	当該手続の申請等にあたり、本人確認又は申請書等の真正性確保のため、当該手続を所管する主体が保有するデータベースとの照合、もしくは公的証明書等による確認を実施している
中	当該手続の申請等にあたり、本人確認又は申請書等の真正性確保のため、上記の方法ほどの厳格さはないが、何らかの確認を実施している
低	当該手続の申請等にあたり、特に確認を実施していない。

注）「厳格な公的証明書等」とは、「行政手続等における本人確認に関する調査結果に基づく通知」（平成 20 年 9 月、総務省行政評価局）において、行政手続により発行された証書等が本人確認書類として二次利用される際の信頼性で述べている「申請者等の実在性の担保」と「申請者等の同一性の担保」の 2 つの指標について、Aa 以上の評価（前者で「（A）最も高いと認められる」、かつ、後者で「（a）高いと認められる」との評価以上）の証書等、もしくは同等と認められる証明書を指す。

3.5.1.3. 導出方法

「事案がもたらす被害規模」と「申請等に係る厳格さ」の２軸を用いたマトリクス表に基づき、金銭的損害に係るリスクの影響度を導出するものとする。

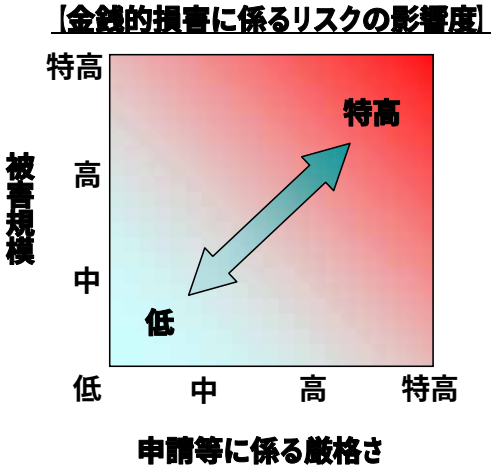

図 3-2 金銭的損害に係るリスクの影響度の導出方法

3.5.2. 機微情報の漏えいに係るリスク評価方法

電子政府におけるオンライン申請等の手続においては、個人が行うオンライン手続には、申請内容に、「氏名」、「性別」、「住所」、「生年月日」等の個人情報のほか、本籍や障害に関する情報のように、機微（センシティブ）な情報が含まれる場合がある。他方、企業が行う手続にも、「技術情報」や「非公開情報」等の営業秘密に関わる機微（センシティブ）な情報が含まれる場合がある。

このような情報が漏えいした場合、情報の種類や重要度によってはプライバシー侵害が生じて、個人が精神的苦痛を受けることや企業が不利益を被ることが予想される。

機微情報の漏えい係るリスク評価手法では、それぞれの手続において情報が漏えいした場合の影響度合いを定量的に判断することができる、「情報の重要度」という評価軸を設定してリスク評価を実施する。

3.5.2.1. 情報の重要度

「情報の重要度」については、情報に含まれる機微（センシティブ）の度合いごとに「低、中、高、特高」の４段階にレベル分けを実施し、以下の通り定義するものとする。

表 3-6 情報の重要度のレベル

レベル	情報に含まれる機微（センシティブ）の度合い
特高	生命の危険または差別や名誉毀損等の社会的不利益につながるもののうち、回復が困難なもの（「個人情報保護マネジメントシステム－要求事項（JIS Q 15001）」で収集禁止の個人情報として定義されているものなど）
高	特高と中の中間に位置するもの
中	公知のもの
低	機微情報ではないもの

3.5.2.2. 導出方法

「情報の重要度」の１軸を用いて、機微情報の漏えいに係るリスクの影響度を導出するものとする。

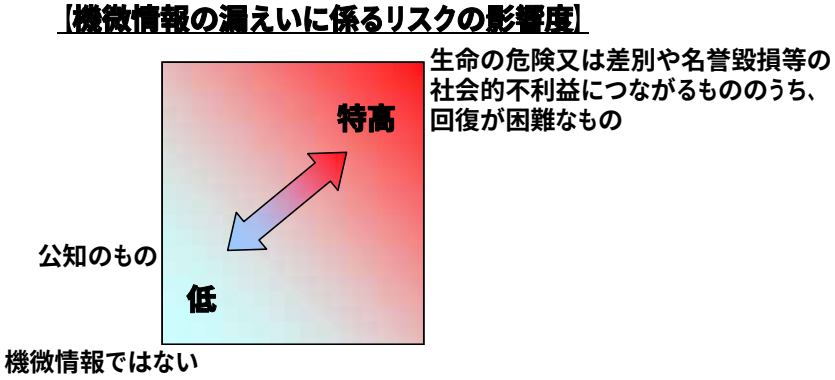

図 3-3 機微情報の漏えいに係るリスクの影響度の導出方法

3.5.3. 評価の実施にあたっての留意点

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。

3.5.4. 総合的リスク評価の導出方法

総合的なリスクの影響度の導出においては、手続固有の特性を踏まえて、考慮すべき全ての要素を対象としつつ、評価の手順としては、基礎的評価として「金銭的損害に係るリスク」の影響度を導出した後、「機微情報の漏えいに係るリスク」の影響度の導出を行い、総合的なリスクの影響度を導出することを基本とする。両リスクの影響度に差があるようであれば、リスクの回復可能性について考慮した上で、２つのリスクにおける総合的なリスクの影響度を導出する。

表 3-7 総合的リスク評価の導出方法

金銭的損害に係るリスクの影響度	機微情報の漏えいに係るリスクの影響度	総合的なリスクの影響度
高	中	変更について検討（中 or 高）
高	高	高
高	特高	変更について検討（高 or 特高）

「金銭的損害に係るリスク」と、「機微情報の漏えいに係るリスク」の他に、3.4 節で述べた「身体の安全への被害」、「違反行為の実施」、「サービスの継続への被害」及び「不便さ、苦痛又は地位や評判の毀損」、その他のリスクについても発生の可能性が確認されれば、リスク影響度の判断材料として対象に含め、回復可能性などを考慮しつつ、総合的なリスク評価を導出するものとする。

その他、総合的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。

4. 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かか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「総合的なリスクの影響度」から、**表 4-1** に基づいて「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 4-1 総合的なリスクの影響度と保証レベルの対応付け

総合的なリスクの影響度	対応する保証レベル	対策基準
特高	レベル4	***各保証レベルの対策基準は、本ガイドラインの付録を参照***
高	レベル3	
中	レベル2	
小	レベル1	

保証レベルに応じた対策基準については、「付録 A　認証方式の保証レベルに係る対策基準」を参照し、システム設計にあたっては、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、情報セキュリティ対策推進会議等の場において、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とともに、業務・システム最適化に係るものは、計画への反映状況について、CIO 連絡会議等に報告するものとする。ここで、最適化計画への反映については、各々の業務・システム最適化計画の改定のタイミングとする。また、電子政府評価の一環として、必要に応じ各府省に対して本ガイドラインに基づく取組の報告を求め、評価等を行うものとする。

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。

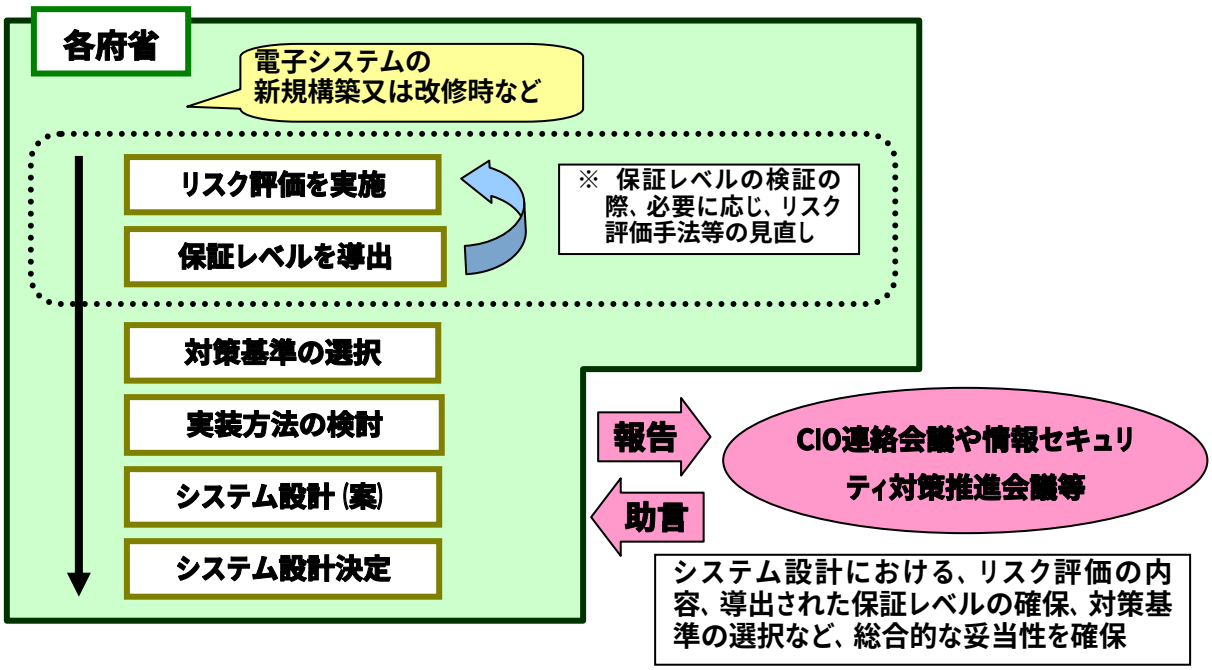

図 4-1 リスク評価に基づく認証方式の選択等の実施フロー

付録A. 認証方式の保証レベルに係る対策基準

A.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。表 A.1-1 に示す通り、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）識別情報の「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 A.1-1 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あたっては、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下記を参考としている。

- 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）」
- EU の「IDABC - Documentation on IDA Authentication Policy」、「STORK project」
- ニュージーランドの「New Zealand Authentication Standards」

表 A.1-1 保証レベル

保証レベル	レベルの定義
レベル 1（低い保証）	特定される身元識別情報の信用度がほとんどない
レベル 2（中程度の保証）	特定される身元識別情報の信用度がある程度ある
レベル 3（高い保証）	特定される身元識別情報の信用度が相当程度ある
レベル 4（かなり高い保証）	特定される身元識別情報の信用度が非常に高い

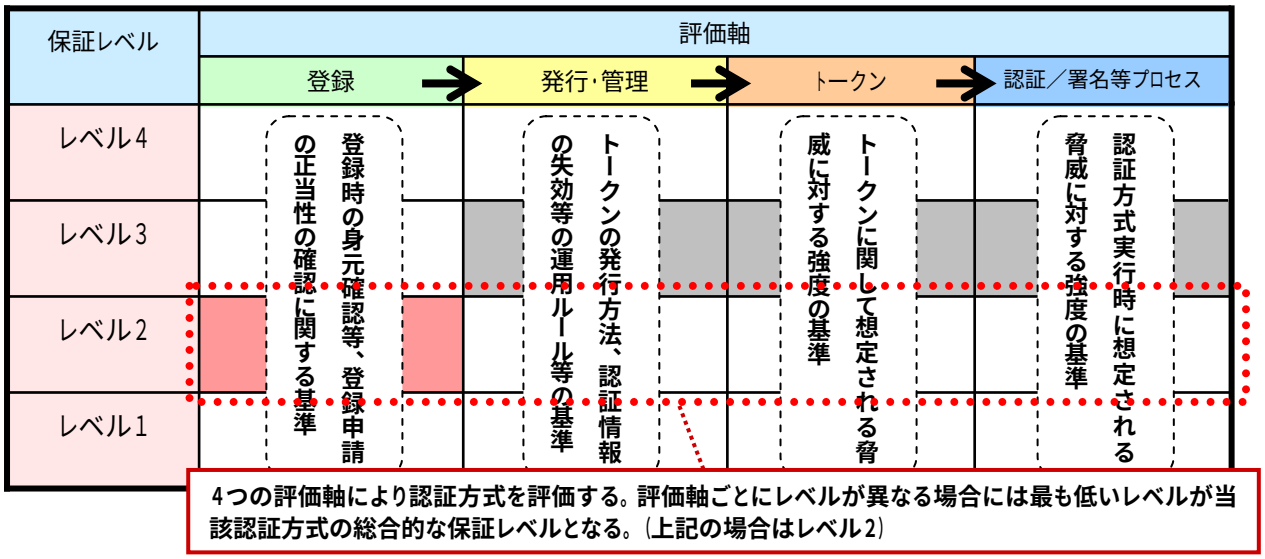

図 A.1-1 保証レベルの評価軸

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、いずれも国民及び企業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「国民・企業と政府の間の申請・届出等のオンライン手続」に対しては主にレベル２またはレベル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

A.2. 認証方式の基本概念

A.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。

A.2.2. 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下記の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づけられる。[1]

一方、情報システムの設計にあたっては、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 A.2-1 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

[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。

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。

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 A.2-1 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

A.3. 認証に係る対策基準

A.3.1. 認証フレームワーク

表 A.3-1 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 A.3-1 認証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なうプロセスであり、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、及び管理を行なうプロセスであり、機能的には CSP が担う。
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また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。

A.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なう。登録申請にあたっては、申請者が１つまた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なわれる。

表 A.3-2 は登録申請における脅威と対策の例であり、表 A.3-3 は対面により登録申請を実施する場合、表 A.3-4 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 A.3-4 に記載の通り、レベル４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すべて仮名として扱われる。

表 A.3-2 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 A.3-3 登録の保証レベル（対面の場合）

対策基準	保証レベル（※1）			
	1	2	3	4
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、公的な写真つきの身分証明書（運転免許証、パスポート等）を1種類、または、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、また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あ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　公的な写真つ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 A.3-4 登録の保証レベル（遠隔の場合）

対策基準	保証レベル（※1）			
	1	2	3	4
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、また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あ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　登録申請にあ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。

A.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、また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 A.3-5 は、発行・管理業務における脅威と対策の例であり、表 A.3-6 は各保証レベルの対策基準である。

表 A.3-5 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 A.3-6 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。または、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） 2つに分割され（例えば、IDとパスワード等）、少なくともその1つが本人住所に普通郵便により送付される、（3） 本人の電子メールアドレスに対して入手サイト先の情報とパスワードが通知され、本人が当該パスワードによる認証の上で、当該サイトからダウンロードする。 〔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。 〔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または失効時期の遅い方の時期から一定期間保管する。
レベル3	〔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また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また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。 〔管理〕 ・ レベル2と同等以上の対策基準とする。 〔更新／再発行〕

保証レベル	対策基準
	・ レベル2と同等以上の対策基準に加え、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なう。 〔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〕 ・ レベル2と同等以上の対策基準に加えて、記録を定期的に分析、評価する。
レベル4	〔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3と同等以上の対策基準とする。 〔更新／再発行〕 ・ レベル3と同等以上の対策基準とする。 〔失効〕 ・ レベル3と同等以上の対策基準とする。 〔記録保管〕 ・ レベル3と同等以上の対策基準とする。

A.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また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、属性情報）の内、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 A.3-7 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）
- 「属性情報」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 A.3-8 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 A.3-9 であり、対策基準の実現例は表 A.3-10 である。

表 A.3-7 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と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さまざま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 A.3-8 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。	・ 紙に手書きまた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な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、考えう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	技術革新等に安全性が低下する危うくなる。	・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 A.3-9 トークンの保証レベル

対策基準	保証レベル(※1)			
	1	2	3	4
[記憶された秘密など] 攻撃者が有効な認証情報を推測できる確率(※2)は、トークンの有効期間を通じて2^{-10}(1024 分の1)未満とすること。	◎	○	○	○
[記憶された秘密など] 攻撃者が有効な認証情報を推測できる確率は、2^{-14}(16384 分の1)未満とすること。		◎	◎	◎
[複数要素認証また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あ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 確率とは、攻撃者が有効期間内に不正に認証を繰り返して正しい認証情報を推測できる度合いであり、例えばパスワードの場合、パスワードに用いる文字の種類、パスワードの長さ、有効期間、認証を規定回数失敗した際のロックが解除されるまでの時間、等によって推測できる確率は変動する。(このようなパスワード強度の考え方については「電子認証に関するガイドライン(NIST Special Publication 800-63)」の付録 A が参考になる)

表 A.3-10 トークンの対策基準の実現例

保証レベル	実現例
レベル1	(パスワード、事前登録知識の確認など) ・ 94 種類の文字 (アルファベット、数字、記号) による 4 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 7 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・記号のすべてを用い、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 8 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 ・ 数字による 8 桁以上のユーザ選択によるパスワード、かつ 5 回連続失敗時はパスワード変更を強制
レベル2	(パスワード、事前登録知識の確認など) ・ 94 種類の文字 (アルファベット、数字、記号) による 5 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・記号のすべてを用い、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 9 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 ・ 数字による 12 桁以上のユーザ選択によるパスワード、かつ 5 回連続失敗時はパスワード変更を強制
レベル3	(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4	(耐タンパ性を有する IC カードや USB トークンなど) ・ 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

A.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なわれる。

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な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 A.3-11 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 A.3-12 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 A.3-11 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または全部を傍受し、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なっても、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）を盗聴また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なう。	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 A.3-12 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）	保証レベル（※1）			
	1	2	3	4
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あ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。

A.4. 署名等に係る対策基準

A.4.1. 署名等フレームワーク

A.2 章にて述べた通り、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、A.3 章にて述べた認証は「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、申請者の認証を行なった上で、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、サービス提供にあ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あたっては、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 A.4-1 に示すように、署名等フレームワークと表 A.3-1 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、A.3 章の「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 A.4-1 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なうプロセスであり、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、及び管理を行なうプロセスであり、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なった上で、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。

A.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 A.4-2 に示す。

表 A.4-3、表 A.4-4 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３、及び保証レベル４に絞って対策基準を定める。

表 A.4-2 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、改ざんを行なう。	・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 A.4-3 署名等プロセスの保証レベル

対策基準(※1)	保証レベル(※2)			
	1	2	3	4
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 A.3-9 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。			◎	
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 A.3-9 トークンの保証レベル」の保証レベル4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づけるとともに、関連事項について A.5.5 節にて述べる。
※2　「◎」は各保証レベルへの準拠にあたり必須の対策基準であることを示す。

表 A.4-4 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3	ソフトウェアトークン（PINあり）またはハードウェアトークン（PINあり）による電子署名
レベル4	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

A.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あ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。

A.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あたっては、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、レベル４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よい。（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、申請者が企業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。

A.5.2. 標準仕様の採用

認証方式の実装にあたっては、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。

A.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。

A.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なうことによって、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。

A.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）において下記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、改ざん等の一時角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、アクセス管理のあ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。

A.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あたっては、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。