電子政府ガイドライン作成検討会
セキュリティ分科会報告書

平成 22 年 2 月

電子政府ガイドライン作成検討会　セキュリティ分科会

はじめに

電子政府ガイドライン作成検討会は、平成 20 年 10 月、「使いやすく安全な電子政府」を目指して設置された。私が主査を務めた「セキュリティ分科会」においては、ユーザアンケートなどで問題点として指摘されることが多い、電子申請時における電子署名等の本人確認方法について、セキュリティと利便性、コストといった通常トレードオフの関係にあるとされているものの最適解を探るという難しいタスクを担当することとなった。本報告書及びガイドラインのとりまとめにご尽力いただいた、佐々木良一主査代理をはじめとする分科会構成員各位、須藤座長をはじめとした検討会構成員ほか検討に参画いただいた関係各位に深く感謝する。

この困難なタスクへの回答として、本分科会では現状の我が国の電子政府が抱える課題や諸外国及び国際標準機関で検討されている認証ガイドラインを精査した上で、セキュリティ設計における「ものさし」を策定することとした。我が国における本人確認手続きについては、個人情報保護に対する意識の高まりや犯罪防止の観点等から、近年になって重要視されてきたものであり、標準的な手法・基準が確立しているとはいえない状況にある。本分科会が策定した「ものさし」が、オンライン手続きにおける本人確認手法の判断基準として、また官民共通の基準として、関係方面で活用して頂ければ幸いである。

さて、電子政府は、国民の生活基盤であるに止まらず、官民連携の上に構築される産業基盤としても将来の日本の発展を左右する重要分野であるにも拘らず、目に見えない情報の世界であるが故に理解され難く、その緊急性が広く認識されていない。それもあってか、電子行政の全体最適化が遅々として進展しないのは誠に憂うるべきことである。

例えば、国民一人一人が年金、税金、医療、介護、福祉などに関する個人情報を、プライバシー保護の保障の下で、常に把握できるような環境の構築は生活の安心安全の面からも、また国民の知る権利という意味でも不可欠である。そのためには、各省庁・自治体のバックオフィスを連携して各種のデータベースを疎結合した上でポータルを設けることが必要であろう。また、本分科会の担当である署名・認証に関しては、現在、電子申請（署名）に用途が限定されていること等もあって、より一層の普及拡大の必要性が指摘されている公的個人認証システムの用途を拡大して、認証（本人確認・実在性確認）にも、官・産・民で広く利用できるようなシステムを官民連携して構築することが急がれる。

上にも述べたように、安全性と利便性・効率性は、ある時点での利用環境を固定して考えればトレードオフの関係にあると言えるが、今後、適切な法制度とその運用、及び市場メカニズムの活用などにより電子行政の全体最適化を進める過程で、ユーザビリティとセキュリティのより高

いレベルでのダイナミックなバランスを達成することも可能となろう。
こうしたことが広く理解されるよう、政策決定者を含む各層で深い議論を盛り上げ、また周知活動を展開することも緊急の課題である。

本分科会で検討した署名・認証は電子政府の入り口に過ぎないが、クラウドに代表される情報技術・利用の新潮流を契機として、国民に対する透明性の高い安心できるサービスの効率的な提供基盤としての、ひいては我が国の活力ある発展基盤としての電子政府の本格的構築に向けて、本報告書及びガイドラインが、その一助となることを期待している。

電子政府ガイドライン作成検討会　セキュリティ分科会主査

辻井　重男

目次

図の目次

表の目次

第1章　検討の背景

第１章では、電子政府ガイドライン作成検討会セキュリティ分科会報告書（以下、「本報告書」）および別冊のガイドラインを検討・作成するにあたっての背景となる、オンライン利用拡大行動計画、第２次情報セキュリティ基本計画及び電子政府ガイドライン作成検討会セキュリティ分科会の設置の経緯、同分科会の役割と検討方針について述べる。

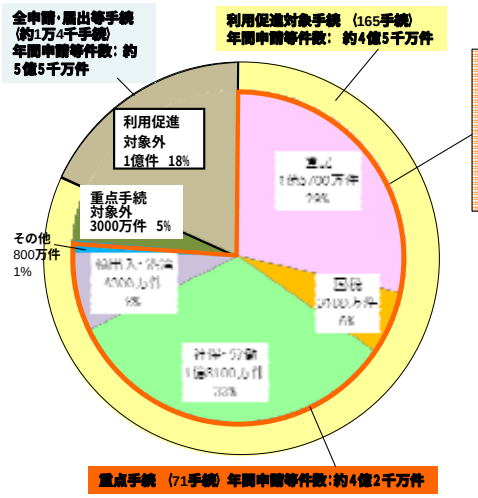
1.1.　オンライン利用拡大行動計画

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、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、平成 20 年９月 12 日に「オンライン利用拡大行動計画」が IT 戦略本部によって決定された。

オンライン利用拡大行動計画は、オンライン利用促進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、2009年度から2011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ている。具体的には、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100万件以上のもの及び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、このような重点手続全体で2013年度末までにオンライン利用率72%以上の実現を目指すという目標が掲げられている。

■ オンライン利用の拡大に向けた基本方針

1. 平成21年度から3年間に集中的に取り組む行動計画を政府全体として策定
2. 重点手続を絞り込み
   - ◆ 165手続　→　71手続（全申請件数の76.5%をカバー）
   - ◆ 重点手続分野ごとに取組方針と目標値を設定



＜重点手続選定の考え方＞

- ◆ 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
- ◆ 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

重点手続分野ごとの手続数

登記	国税	社会保険・労働保険	輸出入・港湾	産業財産権出願関連	自動車登録	その他
5	15	21	20	1	1	8

図　1.1　「オンライン利用拡大行動計画」と重点手続

上記の目標の達成に向けて、同行動計画では、各手続の所管府省における利用拡大の取組を推進するとともに、所管府省のみの改善努力では解決が困難である課題や複数の行政手続にまたがる共通の課題への対応として、以下に示すような９つの重点的取組が示されている。

ここで、「オンライン利用に係るガイドラインの策定」については、内閣官房（IT担当室及び情報セキュリティセンター）において、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ことに向け、有識者を含めた検討の場を速やかに立ち上げ、一定の方向性を取りまとめることとされている。

他方、セキュリティの観点から対応が求められる「認証基盤の抜本的な普及拡大策」については、電子政府推進の基礎となる認証基盤の普及拡大に向けて、本人確認方法の見直しに関する方策や、商業登記に基づく認証や公的個人認証など各種認証サービスの使い勝手の向上について、各運用主体により検討されることとなっている。

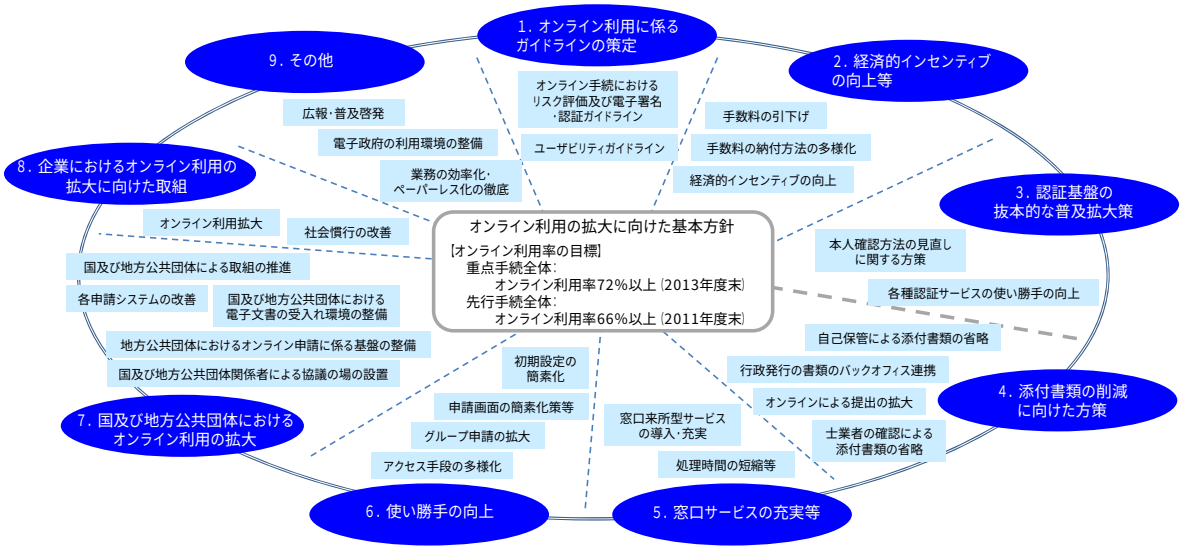


図 1.2 オンライン利用拡大行動計画の重点的取組

1.2. 第２次情報セキュリティ基本計画

「事故前提社会」のコンセプトを提唱した、情報セキュリティ政策における我が国の全体設計図である「第２次情報セキュリティ基本計画」（平成 21 年 2 月 3 日情報セキュリティ政策会議決定）においても、政府機関の取組として、電子政府の利便性向上と適切なセキュリティレベルの確保を目指すべく明記されており、平成21年から平成23年の3年間での実現が求められている。

第２次情報セキュリティ基本計画（一部抜粋）

第3章 今後3年間に取り組む重点政策
第1節 対策実施4領域における取組みの推進と政策目的の着実な実現
(1) 対策実施4領域
① 政府機関･地方公共団体
(ウ) 電子政府の利便性･セキュリティレベルの向上
行政サービスの利便性向上と行政運営の効率化･高度化を推進するとともにセキュリティレベルの向上を図る観点から、電子政府に係るシステムのセキュリティ機能の在り方について検討することとし、特に利用者とのインターフェースに係るものについては、利用者の利便性を向上し、かつ安全を確保できるものとなるよう、費用対効果を勘案した上で、実装方法を含めて検討を行う。

1.3. 電子政府ガイドライン作成検討会セキュリティ分科会

オンライン利用拡大行動計画の中で重点的取組の一つとして示されている「オンライン利用に係るガイドラインの策定」を具現化し、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し、一定の方向性を取りまとめることを目的として、「電子政府ガイドライン作成検討会」が平成 20 年 10 月に設置された。

電子政府ガイドライン作成検討会

座長 ： 須藤 修 東京大学大学院情報学環教授
座長代理 ： 辻井 重男 中央大学研究開発機構教授
構成員 ： 井堀 幹夫 市川市情報政策監（CIO）
： 遠藤 紘一 （社）日本経済団体連合会電子行政推進委員会電子行政推進部会長
： 大山 永昭 東京工業大学大学院理工学研究科教授

セキュリティ分科会

主査 ： 辻井 重男 中央大学研究開発機構教授
主査代理 ： 佐々木良一 東京電機大学未来科学部教授

ユーザビリティ分科会

主査 ： 山田 肇 東洋大学経済学部教授
主査代理 ： 黒須 正明 放送大学 ICT 活用･遠隔教育センター教授

庶務 ： 内閣官房IT担当室（電子政府ガイドライン作成検討会およびユーザビリティ分科会の主担当）
内閣官房情報セキュリティセンター（セキュリティ分科会の主担当）

同検討会では、（１）電子政府の手続に応じたセキュリティ、及び（２）電子政府の手続利用シナリオに応じたユーザビリティ、の２点について検討が進められることとなったことから、そ

の下部組織として「セキュリティ分科会」及び「ユーザビリティ分科会」[1]を設置し、それぞれの分科会にてガイドライン策定に向けて議論されることとなった。

こうしたことから、セキュリティ分科会においては、オンライン利用拡大行動計画における「重点手続」のセキュリティ確保策として、適切な認証と電子署名を選択するための考え方について整理を行い、オンライン手続のリスクに応じた認証方式を合理的に選択することによって認証方式の適切な利用を促進するための考え方を取りまとめたガイドラインを作成することとする。また、その際には、第２次情報セキュリティ基本計画に明記されたように、利用者の利便性を向上し、かつ安全を確保できるものとなるよう、費用対効果及び行政事務の効率化を勘案した上で検討を行うものとする。

セキュリティ分科会の開催経緯と構成員について以下に示す。

[1] ユーザビリティ分科会においては既に「電子政府ユーザビリティガイドライン」が取りまとめられており、2009 年 7 月 1 日に各府省情報化統括責任者（CIO）連絡会議にて決定されている。

表 1.1 セキュリティ分科会の開催経緯

会合	開催日	審議事項
第１回	平成20年10月17日（金）	・認証に関する現状について ・検討課題及び今後の進め方について
第２回	平成20年11月21日（金）	・セキュリティ分科会の進め方の見直しについて（案） ・eGovの動向と次世代電子行政サービス構想 ・「電子政府認証ガイドライン検討報告書」について ・オンライン利用拡大行動計画における重点手続の再点検について（案）
第３回	平成20年12月12日（金）	・電子署名の運用状況 ・電子署名及び認証業務に関する法律における「推定効」について ・ユーザインタフェースに関する技術動向
第４回	平成21年1月26日（月）	・電子自治体（電子府庁）推進の現状 ・電子私書箱（仮称）で想定されるオンライン認証が必要となる利用シーンについて ・オンライン利用拡大行動計画における重点手続の再点検について（中間報告） ・海外の電子政府における認証・署名のガイドラインについて
第５回	平成21年2月27日（金）	・検討スケジュール等の見直しについて ・保証レベルとリスク評価の考え方 ・ガイドラインの内容案について
第６回	平成21年3月23日（月）	・リバティ・アライアンスの取り組みについて ・セキュリティ分科会中間報告案について
第７回	平成21年5月18日（月）	・バイオメトリクス認証について ・認証に関する検討事項について
第８回	平成21年7月15日（水）	・多要素認証 ・モバイル認証 ・重点手続のリスク評価手法について①
第９回	平成21年8月31日（月）	・重点手続のリスク評価手法について② ・分科会の成果物について（案） ・認証技術及び利用動向について
第10回	平成21年10月5日（月）	・電子文書の証明力について ・報告書及びガイドライン（骨子案）について
第11回	平成21年11月18日（水）	・報告書及びガイドライン（案）について

構成員等名簿

	荒木　慶司	（財）自治体衛星通信機構理事長
	岩下　直行	日本銀行金融研究所情報技術研究センター長 （任期：2009 年 6 月迄）
	宇賀　克也	東京大学大学院法学政治学研究科教授
	國井　秀子	リコーIT ソリューションズ（株）取締役会長　執行役員
	小松　文子	（独）情報処理推進機構 情報セキュリティ分析ラボラトリー室長
主査代理	佐々木良一	東京電機大学未来科学部教授
	猿渡　知之	京都府副知事（任期：2009 年 3 月迄）
主査	辻井　重男	中央大学研究開発機構教授
	中尾　康二	（独）情報通信研究機構 インシデント対策グループリーダー
	満塩　尚史	各府省情報化統括責任者（CIO）補佐官等連絡会議情報セキュリティワーキンググループリーダー （環境省 CIO 補佐官）

電子政府ガイドライン作成検討会構成員

井堀　幹夫	市川市情報政策監（CIO）
遠藤　紘一	（社）日本経済団体連合会電子行政推進委員会 電子行政推進部会長
大山　永昭	東京工業大学大学院理工学研究科教授
須藤　修	東京大学大学院情報学環教授

オブザーバー

洲崎　誠一	安心・安全インターネット推進協議会／（株）日立製作所システム開発研究所
松本　泰	（株）セコム IS 研究所

総務省行政管理局行政情報システム企画課長

総務省自治行政局地域政策課長

総務省自治行政局地域情報政策室長

総務省自治行政局市町村課長

総務省情報流通行政局情報流通振興課情報セキュリティ対策室長

法務省民事局民事第二課長

法務省民事局商事課長

国税庁長官官房企画課長

厚生労働省大臣官房統計情報部企画課情報企画室長

厚生労働省労働基準局労働保険徴収課長

厚生労働省職業安定局雇用保険課長

社会保険庁総務部総務課情報企画調整室長

経済産業省商務情報政策局情報経済課情報セキュリティ政策室長

【参考】電子署名と認証の考え方

本報告書及びガイドラインでは、電子署名及び認証の定義を以下の表のように定義している。（付録１参照）

用語	語義
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。
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。

そもそも、電子政府のオンライン手続は、既存の紙手続をそのまま電子化したという背景がある。そのために、オンライン手続においては、図のとおり、申請、受付、保存・管理等の一連の流れにおいて紙手続と同一であり、その各場面における対策として電子署名・認証技術等が複合的に利用されている。以下では、その基本的な考え方についてここで整理をしておく。

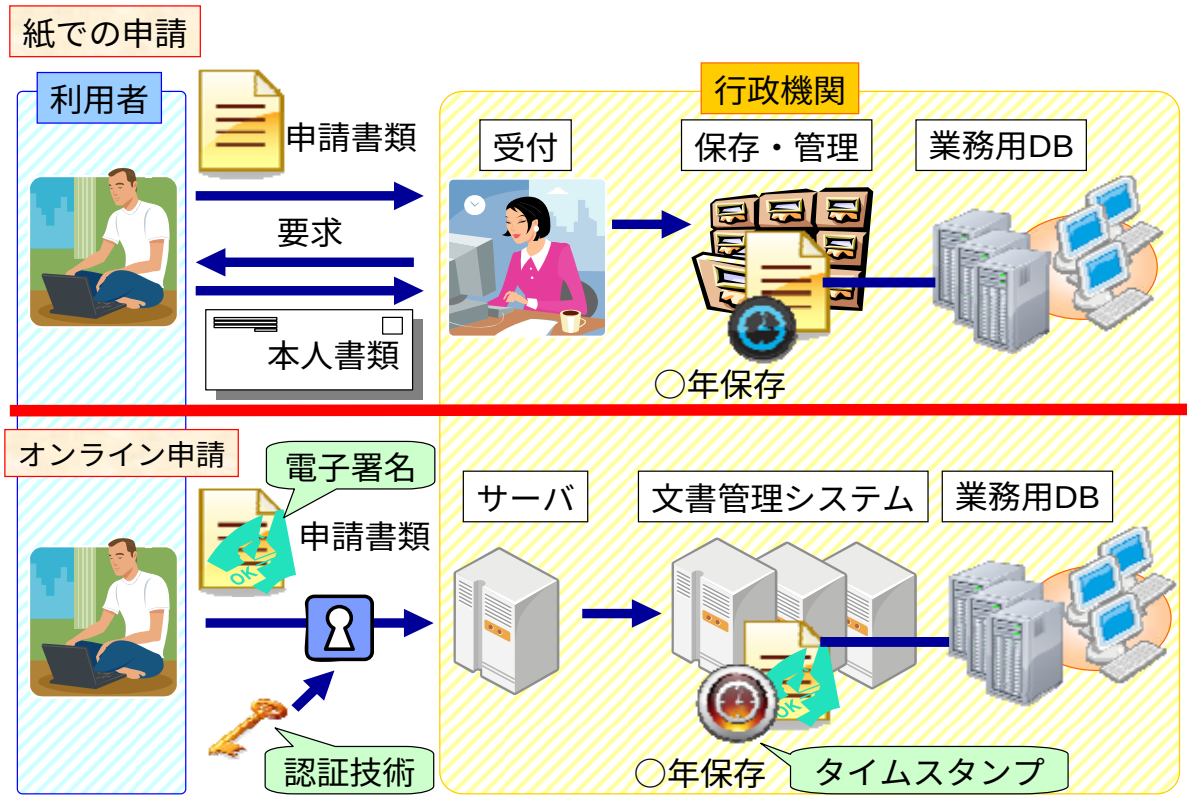


図 1.3 紙申請とオンライン申請の手続の比較

まず、電子署名とは、①（オンライン申請の際に提出される）電磁的記録が電子署名を付与した本人の作成に係るものであることを示すために行われるものであり、かつ、②電子署名の対象となった情報が改変されていないということを確認することができるものである。この電子署名は、紙申請では押印に相当するものであり、利用者（申請者）側からの行為ということになる。

一方、認証とは、申請者が本当に当該申請を行う本人であるかを検証する本人確認の手段である。これは、本人か否かを検証する必要がある主体、つまりサービス提供者側からの行為である。

電子署名と認証において、このような厳然とした違いは存在するものの、類似点も同時に存在する。まず、双方ともに同一の技術（PKI：公開鍵基盤）に立脚して実現している点、そして、海外電子政府において 1990 年代の電子署名制度と 2000 年代の認証ガイドラインの策定という潮流が存在している点（第３章参照）、電子署名と認証はともに対象手続に関わる脅威に対する保証レベルという共通軸を有している点（第５章・ガイドライン参照）、さらに、双方において登録、発行・管理における手続が共通である点（第５章・ガイドライン参照）等である。また、利用者（国民等）にとって、電子署名と認証の違いを必要以上に意識させることがないような配慮も望まれる。こうしたことから、本報告書及びガイドラインにおいて、「電子署名・認証」という形で併記して記載している場合がある。

第2章　電子政府の現状

第２章では、電子政府のオンライン利用の現状を整理し、その利用拡大の阻害要因を抽出することで、拡大に向けた課題を把握することとする。また、現在検討が進められている電子政府の将来像を実現するための取組の方向性を概説し、電子政府における認証方式の普及拡大による基盤化にあたって解決が求められる課題を整理する。

2.1. オンライン利用の現状

オンライン利用の現状については、内閣官房、総務省をはじめとする各種行政機関が様々な観点から調査を行っており、それらを整理することで概観を把握することができる。

ここから、電子政府のオンライン利用の現状整理と、その利用拡大の阻害要因及び拡大に向けた取組及びそれに対する課題の把握を行うこととする。

2.1.1. オンライン手続の実態

オンライン手続の利用状況については、総務省によって、行政手続等における情報通信の技術の利用に関する法律に基づき、行政機関等が公表した国民や企業がオンライン等で行うことができる行政手続の状況が取りまとめられ、毎年度、公表されている。

一方、内閣官房情報セキュリティセンターでは、オンライン手続の実態を把握するため、オンライン利用拡大行動計画における以下の記載に基づき、重点手続の再点検を行った。

以上の資料等をもとに、電子政府のオンライン利用の現状整理を行うこととする。

オンライン利用拡大行動計画（一部抜粋）

Ⅰ　オンライン利用の拡大に向けた基本方針
Ⅰ－2　目標達成のための重点的取組
3. 認証基盤の抜本的な普及拡大策
(1)本人確認方法の見直しに関する方策
①本人確認方法の再点検
　電子署名を要する手続について、セキュリティの確保に留意しつつ、本人確認手法の再点検を行う。特に、次に該当する手続については、重点的に見直すものとする。
・ 紙の申請時に署名や押印を要しない手続
・ 法令上、署名や押印を必要としていない手続
・ 既にID･パスワード化を実施している手続と同種の手続
・ なりすましにより不当に利益を得ることが想定できない手続

2.1.1.1. オンライン利用状況

国の機関が扱う申請・届出等手続のオンライン利用率については、オンライン利用拡大行動計画に基づき、重点手続を対象として目標利用率を設定し、利用率向上に取り組んでいる。

総務省が公表した「平成 20 年度における行政手続オンライン化等の状況」[2]によると、平成 20 年度の重点手続（全申請・届出等件数の 76.5%をカバー）におけるオンライン利用率は 50.6%（平成 19 年度は 43%）となっており、平成 20 年度計画値（45.4%）を上回る結果となった。

（注）オンライン利用拡大行動計画においては、窓口等で磁気媒体等を用いてデータ形式で提出される申請等も、行政内部における事務処理が電子的に行われることにより行政の効率化や国民の利便性の向上に資するとの趣旨で、オンライン利用件数に含めることとしたため、この方針に従って集計。なお、磁気媒体等を含まないオンライン利用率は 36.9%。

国の機関が扱う申請・届出等手続のオンライン利用にあたっての認証基盤は、ID・パスワードによるものと、電子署名を用いるものとに二極化しているが、重点手続を、ID・パスワードのみを用いるもの、電子署名のみを用いるもの、電子署名と ID・パスワードを併用するもの、の３つに区分した。その上で、この３つの区分（カテゴリー）ごとに、分類された手続の利用率の総和を手続数で割った平均値を求め、相互に比較を行った。

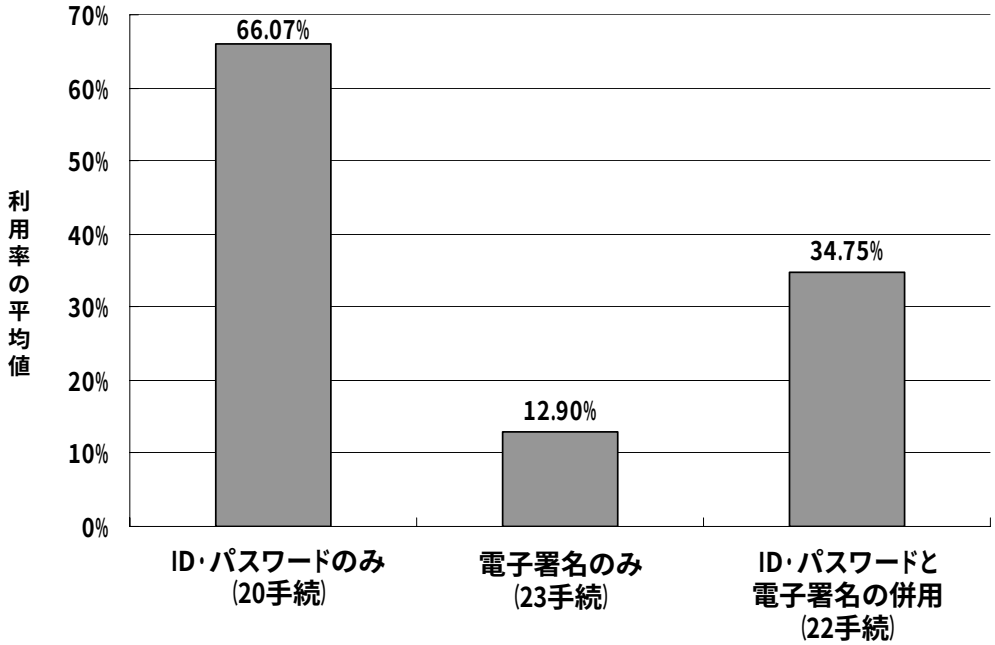
[2] 「平成 20 年度における行政手続オンライン化等の状況」
（http://www.soumu.go.jp/main_content/000031924.pdf）

表 2.1 「オンライン利用拡大行動計画」で定められた 71 重点手続

年度	年間申請等件数	オンライン利用件数	オンライン利用率		
			実績値	計画値	25 年度目標値
20 年度	417,578,403	211,196,651	50.6%	45.4%	72%

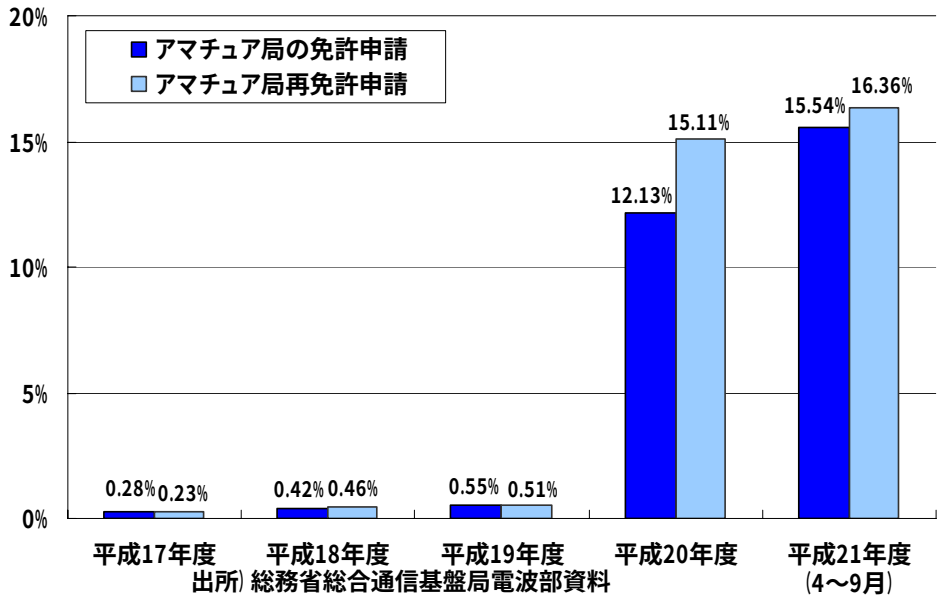
その結果、ID・パスワードのみを用いる手続（20 手続）の利用率の平均値が 66.07%であるのに対し、電子署名のみを用いる手続（23 手続）の利用率の平均値は 12.90%であり、５倍程度の開きがあることが判明した。この傾向は、無線局（アマチュア局）の免許申請や再免許申請に係るオンライン手続の推移でも見られる。これら手続においては、平成 20 年度から ID・パスワードを発行すれば電子署名不要で申請できるようにしたところ、それぞれの申請の利用率が、平成 19 年度には僅か 0.55%、0.51%であったが、平成 20 年度には 12.13%、15.11%にまで飛躍的に向上している。

このように、重点手続の各手続によってオンライン利用率の高低にばらつきがあるのが現状であり、オンライン利用拡大を着実に推進するにあたり、署名・認証方式の適切な選択が重要な要素となっていることが分かる。



注1) 重点手続71のうち、本人申請がない手続や利用率が見当たらない手続の6手続を除いて集計
注2) 利用率の平均値は、各カテゴリーにおいて分類された手続の利用率の総和を手続数で割った値として示している
出所)「平成 20 年度における行政手続オンライン化等の状況」等を基に作成

図 2.1 重点手続におけるカテゴリー別（電子署名、ID･パスワード、併用）の利用率の平均値



出所) 総務省総合通信基盤局電波部資料

図 2.2 無線局 (アマチュア局) の免許申請・再免許申請のオンライン利用率

2.1.1.2. 重点手続の再点検結果

オンライン利用拡大行動計画を受けて、内閣官房情報セキュリティセンターにて行った重点手続の再点検の概要を以下に示す。ここでは、オンライン手続の実態を把握するために、重点手続のうち電子署名を要する 47 手続を調査対象としてアンケート調査を実施した。

以下、再点検結果より判明した電子政府のオンライン利用の現状を示す。

表 2.2 アンケート調査の概要

調査対象	47 手続の所管省庁に対して調査を依頼
調査方法	書面によるアンケート調査を実施し、必要に応じて内容補足のためのヒアリング調査等を実施
調査時期	平成 20 年 12 月上旬から平成 21 年 1 月中旬までの約 1 ヶ月間。
調査内容	紙手続での申請・届出の状況、オンライン申請の状況、その他手続全般に関する事項

(1) 本人確認の状況

紙手続での申請・届出が併用されている重点手続において、窓口で申請書等を受領している手続が 45 手続あり、そのうち、申請者本人が来訪した際に、申請書等の作成者と同一であることを

確認している手続は、20 手続のみであった。一方、残りの 25 手続では、このような本人確認が制度として特に求められていない。

この 20 手続では、そのすべてにおいて、本人確認の際に、自動車免許証等の身分証明書の提示やその写しの提出を要求している。加えて、16 手続では、申請者の顔と身分証明書に貼付された顔写真との照合を実施している。

ここから、紙手続とオンライン手続とで本人確認の有無（や方法）に違いが生じており、オンライン手続においては紙手続よりも厳しい本人確認を求める傾向にあることが分かる。

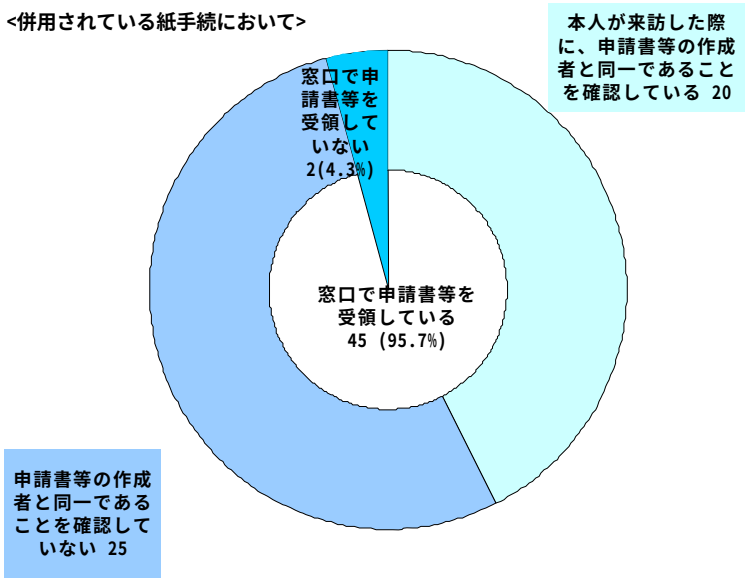


図 2.3 窓口における申請書等の作成者の本人確認の有無

(2) 否認防止対策･改ざん防止対策の状況

重点手続では、否認防止対策・改ざん防止対策として、電子署名が用いられているが、同じ手続において併用されている紙手続についてみると、押印が実印である必要がある手続は僅か 3 手続であり、残りの手続では、認印など実印以外による押印が認められているかそもそも押印を必要としていない。

また、紙手続では、47 手続中 39 手続において、否認防止対策・改ざん防止対策として、申請者に受領印が付された提出書類の写しが配布されている。そのうち申請者全員に写しが配布されている手続は僅か 7 手続である。残りの 32 手続は希望者のみに写しが配布されている。

このように、実印以外による押印を認めている、もしくは、そもそも押印を必要としない紙手続であっても、オンライン手続になれば電子署名を求めるという実情が判明した。また、受領印

が付された提出書類の写しが配布されていない、もしくは、希望者のみに写しが配布されている紙手続であっても、オンライン手続になれば否認防止対策・改ざん防止対策として有効な電子署名を求めていることが明らかとなった。

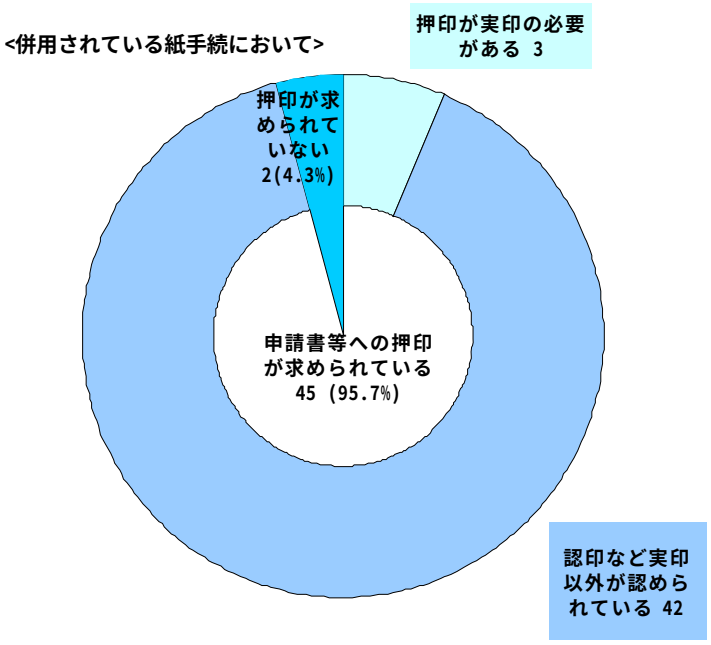


図 2.4 申請書等への押印の要求有無

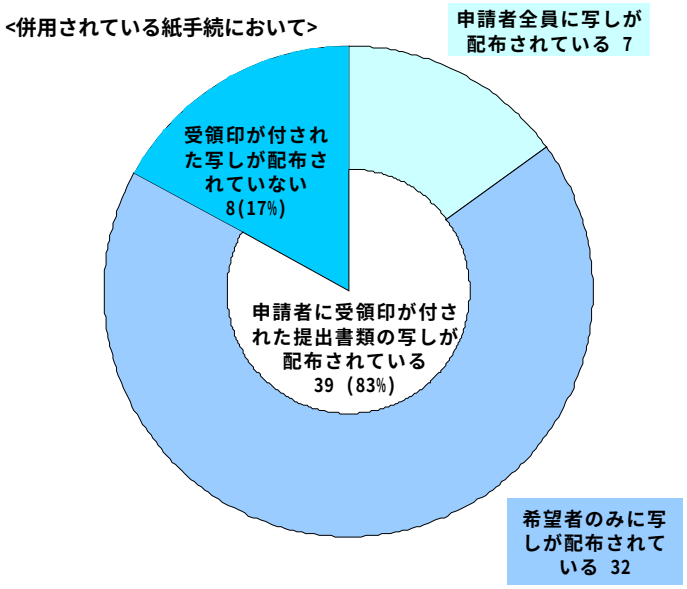


図 2.5 受領印が付された提出書類の写しの配布有無

2.1.2. オンライン手続の利用阻害要因

内閣官房が公表した「個別手続における認知度・利用度・満足度等の調査」[3]では、個人、企業、士業それぞれに対し、オンライン申請を利用しなくなった理由・断念した理由を尋ねている。アンケート調査の概要とその結果を以下に示す。

表 2.3 アンケート調査の概要

調査対象者	登記、国税、社会保険・労働保険関係手続を調査対象手続とし、当該手続の想定利用者である個人、企業、士業（税理士、司法書士、社会保険労務士）に対して調査を実施
調査方法	個人：会員制サイト等を利用して Web アンケートを実施 企業：郵送法によるアンケートを実施 士業：各士業団体への協力のもと、郵送法によるアンケートを実施
調査時期	個人：平成 21 年 1 月 23 日から平成 21 年 1 月 28 日までの 6 日間 企業：平成 21 年 1 月 16 日から平成 21 年 1 月 30 日までの 15 日間 士業（税理士、社会保険労務士）： 平成 21 年 1 月 16 日から平成 21 年 1 月 30 日までの 15 日間 士業（司法書士）： 平成 21 年 1 月 20 日から平成 21 年 1 月 30 日までの 11 日間
調査内容	各手続の認知度・利用意欲度・利用度・満足度等に関する事項

[3] 「電子政府評価委員会 平成２０年度報告書」の参考６として添付されている。（http://www.kantei.go.jp/jp/singi/it2/ithyouka/houkoku/2008/den_huzoku2.pdf）

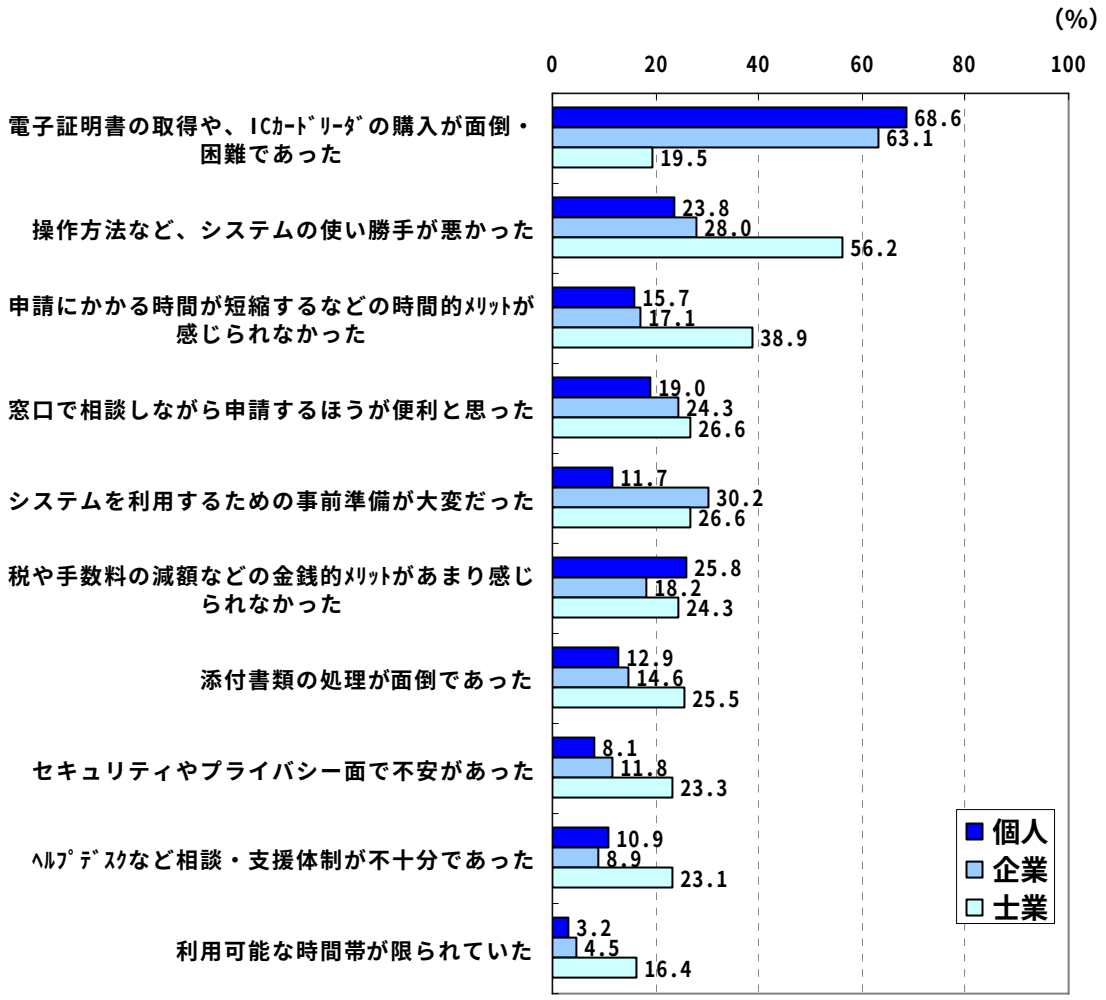


図 2.6 利用を中断･断念した理由 (利用中断･断念者)

個人がオンライン申請の利用を中断･断念した理由として最も高いのは､「電子証明書の取得や、IC カードリーダの購入が面倒・困難であった」であり、回答者の 68.6%を占める。次いで、「税や手数料の減額などの金銭的メリットがあまり感じられなかった（25.8%)」､「操作方法など、システムの使い勝手が悪かった（23.8%)」の順となっている。このように、個人においては、利用者がパソコンに向き合う前に行う事前準備に手間がかかる点が、中断・断念した理由として突出しており、オンライン申請の利用の阻害要因となっていることがわかる。

一方、企業に関しても、個人と同様､「電子証明書の取得や、IC カードリーダの購入が面倒・困難であった」と回答するものの割合が 63.1%を占め、最も高い。次いで､「システムを利用するための事前準備が大変であった（30.2%)」､「操作方法など、システムの使い勝手が悪かった（28.0%)」の順となっている。企業においては、利用者が、パソコンに向き合う前に行う事前準備のみならず、パソコンへのソフトウェアのインストールなども含め、一連の準備に手間がかか

っているといった状況が見て取れる。

さらに、士業がオンライン申請の利用を中断・断念した理由として最も高いのは、「操作方法など、システムの使い勝手が悪かった」であり、回答者の 56.2%を占める。次いで、「申請にかかる時間が短縮するなどの時間的メリットが感じられなかった（38.9%）」、「窓口で相談しながら申請する方が便利と思った（26.6%）」、「システムを利用するための事前準備が大変だった（26.6%）」の順となっている。士業によるオンライン申請の利用においては、システムの使い勝手が悪いという状況や、システムを使いこなせないという状況に直面する場合が多い。

このように、現在のオンライン申請においては、利用者がパソコンに向き合う前に行う事前準備やパソコンへのソフトウェアのインストールなど一連の準備に手間がかかっていることが明らかとなった。また、士業においては、申請頻度が比較的高いことから、その後の操作方法などに対する問題点への指摘が多いことが判明した。

2.1.3. オンライン利用拡大に向けた課題

2.1.1 及び 2.1.2 から、電子政府におけるオンライン利用拡大においては、以下のような課題が明確となった。

（1）重点手続の各手続によってオンライン利用率の高低にばらつきがあるのが現状であり、オンライン利用拡大を着実に推進するにあたり、署名・認証方式の適切な選択が重要な要素となっている。

（2）現実は、同一の手続であっても、紙手続とオンライン手続とで厳格性に違いが生じており、オンライン手続においては紙手続よりも本人確認や押印、否認防止対策・改ざん防止対策が厳格に求められている傾向にある。

（3）現在のオンライン申請においては、利用者がパソコンに向き合う前に行う事前準備、パソコンへのソフトウェアのインストールなど一連の準備の手間、操作方法の困難性等において支障が生じている。

以上を踏まえ、以下ではより具体的に拡大に向けた課題を把握することとする。

2.1.3.1. 電子署名・認証方式の適切な選択にあたっての課題

インターネット等の拡大によって、遠隔による情報のやりとりが可能となったことで、電子商取引等においてなりすましや改ざん、事実否認等の脅威に対応する必要性が生じてきたことから、平成 13 年 4 月から「電子署名及び認証業務に関する法律」（以下、「電子署名法」という。）が施行されている。本法に基づく認定認証局が発行する電子証明書は主として電子申請・電子入札等

で活用されているが、平成 20 年度末現在の累積発行枚数は約 57 万枚（有効枚数約 27 万枚）に留まっている。

認定認証局以外にも、携帯電話事業者が発行する携帯電話に内蔵されるタイプの証明書や、web サービス事業者が利用するサーバ証明書など、電子証明書の裾野は広がりを見せている。

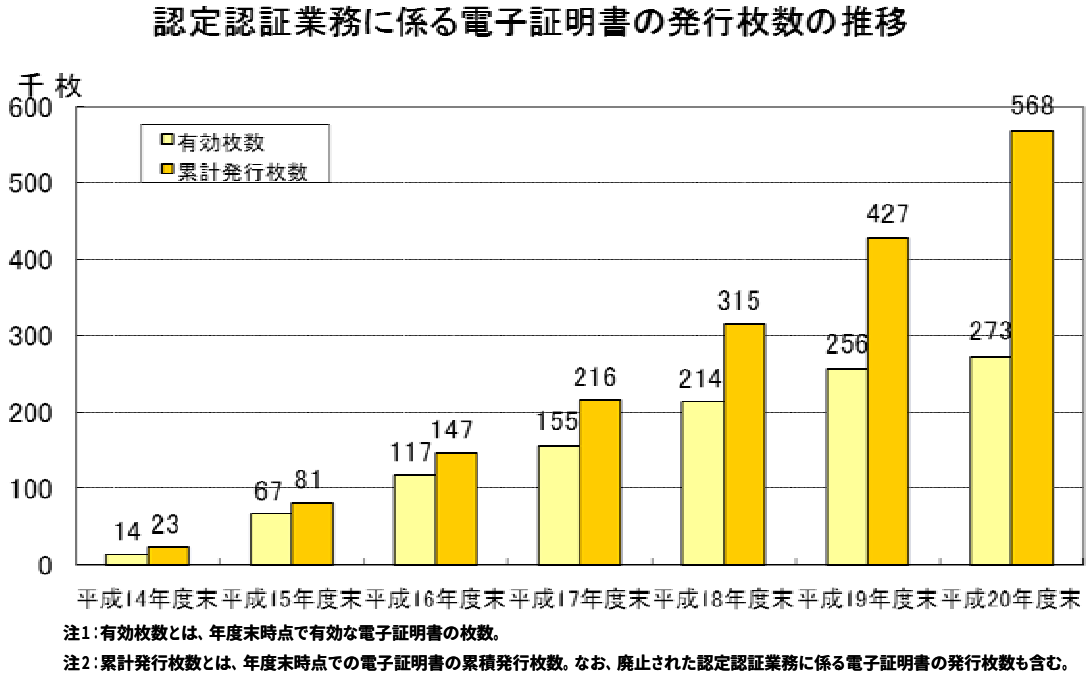


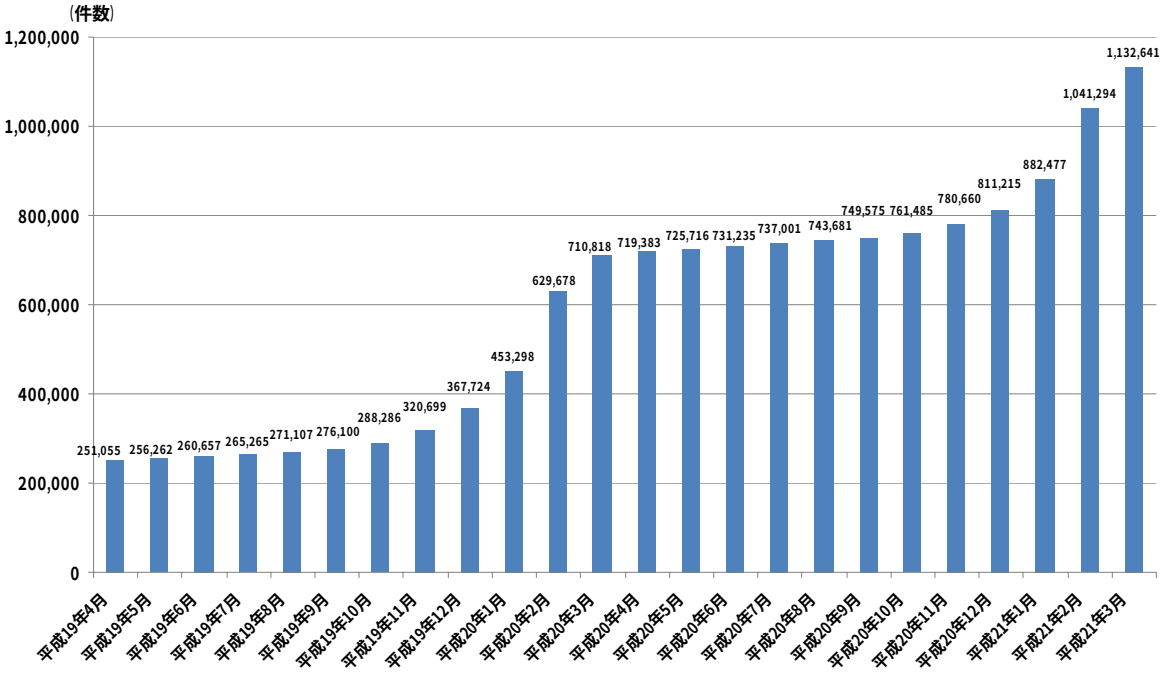
図 2.7 認定認証業務に係る電子証明書の発行枚数の推移

また、電子政府・電子自治体を実現するために、確かな本人確認ができる個人認証サービスを全国民に安価で提供することを目的として、平成１６年１月 29 日より公的個人認証サービスの提供が開始され、国や地方公共団体の手続の本人確認手段として活用されている。平成 19 年度から始まったオンライン確定申告に伴うインセンティブの付与を契機に、公的個人認証サービスの電子証明書の発行枚数（発行累計）は、平成 21 年 3 月末現在、約 113 万枚[4]（有効枚数約 94 万枚）まで増加したが、我が国全国民の 1%程度にしか普及していないのが現状である。

公的個人認証サービスは、現在、多くのオンライン手続で採用されている一方、①利用者（住民）は、３年毎に、市町村窓口に出向いて電子証明書を更新（失効及び発行）する必要があること、②技術的基準を満たす電子証明書の記録媒体が住民基本台帳カードのみとなっていること、などが利用者におけるサービス利用の足かせとなっている。このような点を踏まえ、利用サービスの拡大、利便性の向上、行政分野における更なる利用促進等のための具体的方策について総合

[4] 平成 19 年度の 2、3 月、平成 20 年度の 2、3 月のように、電子証明書の発行枚数が著しく増加する時期がみられるが、これは、平成 19 年度の税制改正の効果によるものである。平成 19 年分と平成 20 年分の所得税について電子申告で行った場合に、最高で 5 千円の税額控除が受けられるようになっている。

的な検討を行うことを目的として、総務省において平成 21 年 4 月に「公的個人認証サービス普及拡大検討会」[5]が開始され、目下検討が進められているところである。



出所) 財団法人自治体衛星通信機構資料

図 2.8 公的個人認証サービスの電子証明書の発行枚数 (発行累計) の推移

一方、既存の認証方式としては、ID・パスワードが広く一般に利用されているものの、野村総合研究所が公表した「個人情報に関するアンケート調査」（以下に概要を示す）によると、インターネット利用者の約55%が、記憶可能なID・パスワードの数を「２～３組」と回答しており、ID・パスワードの忘却リスクが存在していることに注意しなければならない。結果として、異なるサービスにおいて､同一もしくは類似のID･パスワードを利用する傾向にあるのが実情である。

このように、現在利用されている電子署名・認証方式は、構築までの経緯や普及状況、利便性等の面でそれぞれに特徴を有しており、オンライン利用の拡大に向けては、電子署名・認証方式の適切な選択が求められる。しかしながら、オンライン申請ごとの適切な署名・認証方式の選択方法についての統一的な考え方は存在しておらず、その作成が求められている。また、総務省が平成 20 年９月に発表した「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」においても、本人確認の手順・方法等については、各機関が「不正発生リスク」と「申請者の利便／負担」の関係を斟酌して判断している現状であると指摘されている。

また、「行政手続等における情報通信の技術の利用に関する法律」第４条第３項において、オン

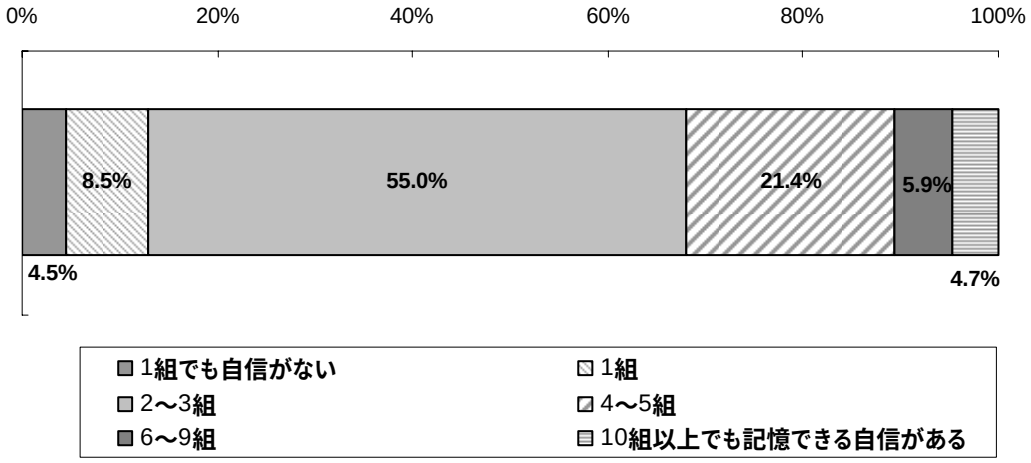
[5]公的個人認証サービス普及拡大検討会
（http://www.soumu.go.jp/main_sosiki/kenkyu/kojin_kakudai/index.html）

ライン利用時の署名、押印に換わる措置を主務省令で定めることができる旨規定されている。

表 2.4 野村総合研究所「個人情報に関するアンケート調査」の概要

調査対象	全国 15 歳以上の男女のインターネット利用者を対象に調査
調査方法	Web アンケート調査を実施
調査時期	平成 21 年 3 月 13 日から平成 21 年 3 月 17 日までの約 5 日間
調査内容	個人情報の管理状況、ID・パスワードの管理状況、それらに関わる課題全般に関する事項

〔Q．あなたは、ID やパスワードを管理する際、何組までなら確実に記憶することができると思いますか〕



出所〕野村総合研究所

図 2.9 野村総合研究所「個人情報に関するアンケート調査」の結果

2.1.3.2. 電子政府の各サービスの認証方式に見受けられる課題

前述のとおり、紙の手続とオンライン手続を併用している同一の手続であっても、本人確認の手順・方法の厳格性の内容に違いがあった。同様に、オンライン手続の中でも、行政機関によって、本人確認の手順・方法の運用に差異がある状況が見受けられる。

このように、電子政府のオンライン手続では、架空名義や他人へのなりすましによる不正な申請等を防止するために、申請者等が本人であることの確認が行われているが、その厳格性や手順・方法の運用については、各行政機関に委ねられており、標準的な手順・方法が確立されていないのが現状である。

このような差異については、当該手続に責任を有するそれぞれの機関が、手続の公平公正の観

点から、こうした差異が不合理なものとならないようにする必要がある。また、申請者等の手続利用に混乱をきたし、オンライン利用促進の足かせにならないようにする必要がある。

このため、今後、電子政府における認証方式を設計するにあたり、各手続に関わる脅威に対するリスクの影響度を導出して、手続ごとに本人確認等の標準的な手順・方法を確立していく必要がある。

2.1.3.3. 電子的な証跡の法的解釈における課題

申請等の行為についてなりすまし、改ざん、事実否認などが発生し、争いとなった場合には、訴訟の場において決着を図ることになる。この場合に、裁判所が申請書等の書証について、要証事実を証明する証拠力を認定するかどうかは、裁判官の自由心証に任されている。

このような証拠力については、形式的証拠力（真正な成立）と実質的証拠力の２つ[6]があり、申請書等が「真正に成立したもの」と推定されるためには、形式的証拠力が認定されなければならない。申請書等の形式的証拠力を認定するかどうかについては、

①作成名義者の印鑑の印影があれば、その押印が同人の意思に基づいて行われたと推定する（最高裁判決 S39.5.12）

②作成名義者の署名または押印があれば、文書の真正な成立が推定される（民訴法第 228 条 4 項）

という二段の推定でもって、判断されることになる。

[6]形式的証拠力（真正な成立）とは、文書の記載内容が、挙証者の主張する特定人の思想の表現であると認められること。文書に関しては、真正な成立の証明が必要である（民訴法第 228 条 1 項)。一方、実質的証拠力とは、形式的証拠力が肯定されたことを前提として、その文書の記載内容が、要証事実の証明に役立つ効果を示すものである。

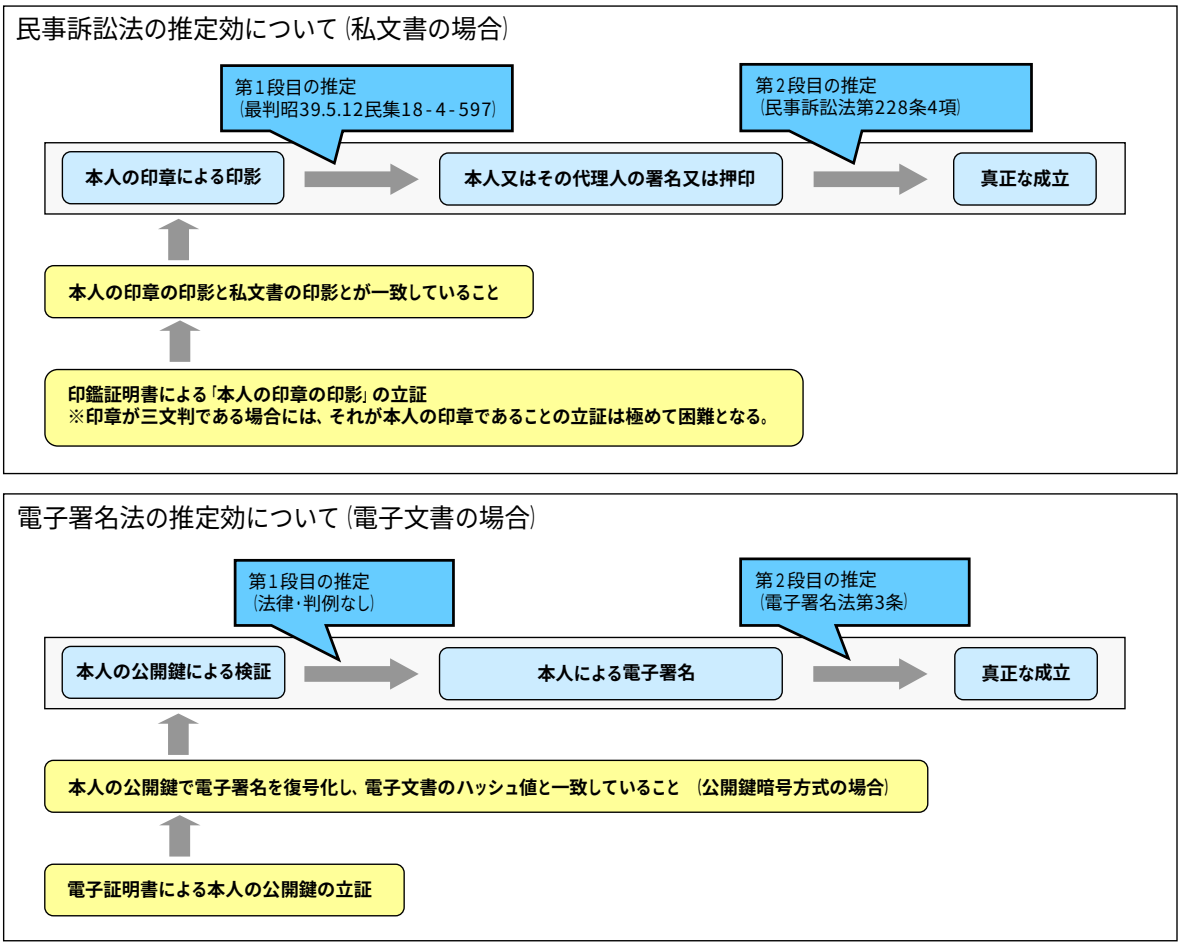


図 2.10 二段の推定の考え方について

オンライン申請等の申請データの真正な成立の立証についても、申請書と同様、上記の考え方が適用されるが、ここで特筆すべき点は、このような二段の推定が、「事実上の推定」に該当していることである。そもそも「推定」は、前提事実が証明されても、推定事実について反証できるものであり、前提事実が証明されたら、推定事実を覆すことができない「みなす」とは性質が大きく異なる。さらに、「事実上の推定」は、推定事実を疑わせる程度の立証で推定を覆せるものである。

電子署名法第 2 条及び第 3 条では、電子証明書に係る電子署名があれば、申請データの真正な成立が推定されるとされている。しかしながら、この推定も「事実上の推定」であり、真正な成立を疑わせる程度の事実が示されれば、推定は破られてしまい、成立を立証する必要が生じることに注意しなければならない。

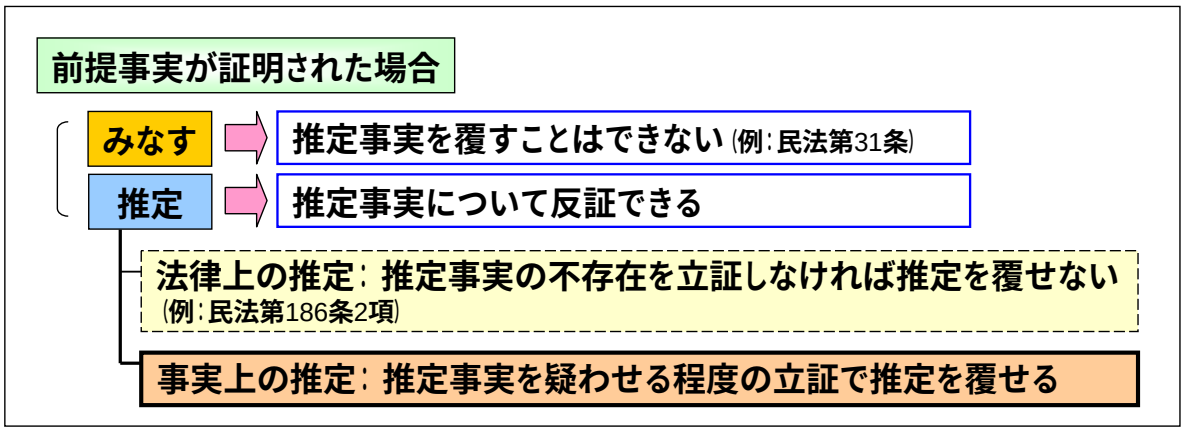


図 2.11 法律における「推定」と「事実上の推定」について

一方、申請データの真正な成立の立証のためには、原本の存在と原本の成立[7]を証明しなければならない。この具体的な方策としては、アクセス記録、タイムスタンプ等により申請データの完全性を確保し、認証やアクセス制御により原本の成立を推認させた上で、これらの処理の正しさを運用体制により確保することが挙げられると考えられる。国際的には、国連国際商取引法委員会（UNCITAL）電子取引モデルにおいて電子メッセージの許容性と証明力が規定されており、わが国でも電子帳簿保存法において電子的な保存のシステム要件が規定されているが、わが国における統一的な基準は未だ存在していないのが現状である。

【参考】電子署名法における電子署名の定義及び推定効

電子署名の定義については、平成１３年４月１日に施行された電子署名法の第二条一項において、以下のとおり規定されている。

（定義）
第二条　この法律において「電子署名」とは、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。以下同じ。）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。
一　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。
二　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。

[7] 原本の存在とは、その文書が作成されたときの文書との同一性（電子データの完全性）のことであり、原本の成立とは、作成名義人がその文書を作成したことを示すことである。

また、申請書データの真正な成立の推定については、第三条において、以下のとおり規定されている。

第三条　電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

2.2. 次世代電子行政サービスの検討状況

電子政府の将来像についての検討としては、平成 20 年 6 月に「次世代電子行政サービス（e ワンストップサービス）の実現に向けたグランドデザイン（次世代電子行政サービス基盤等検討プロジェクトチーム）」[8]が取り纏められ、その後、当該構想の具現化のため、標準モデル構築に向けた技術的方策の検討が進められている。

この検討の中で、次世代電子行政サービス基盤は、情報爆発時代において IT を利活用することにより、日本社会を知識創造の社会へ導き、社会インフラの刷新を伴うイノベーションの連鎖を関係する機関などが情報や知識を共有化し、力を発揮できる環境として組織化されるものとされている。こうした観点を具体化した「利用者視点でのサービス提供」、「行政事務の最適化の推進」、「民間企業活動の活性化」、「国民と行政の信頼強化」の４つの目標を実現することにより、国民本位の究極の電子社会の実現が目指されている。

[8] 「次世代電子行政サービス（e ワンストップサービス）の実現に向けたグランドデザイン（次世代電子行政サービス基盤等検討プロジェクトチーム）」
（http://www.kantei.go.jp/jp/singi/it2/nextg/pdf/grandhonbun.pdf）

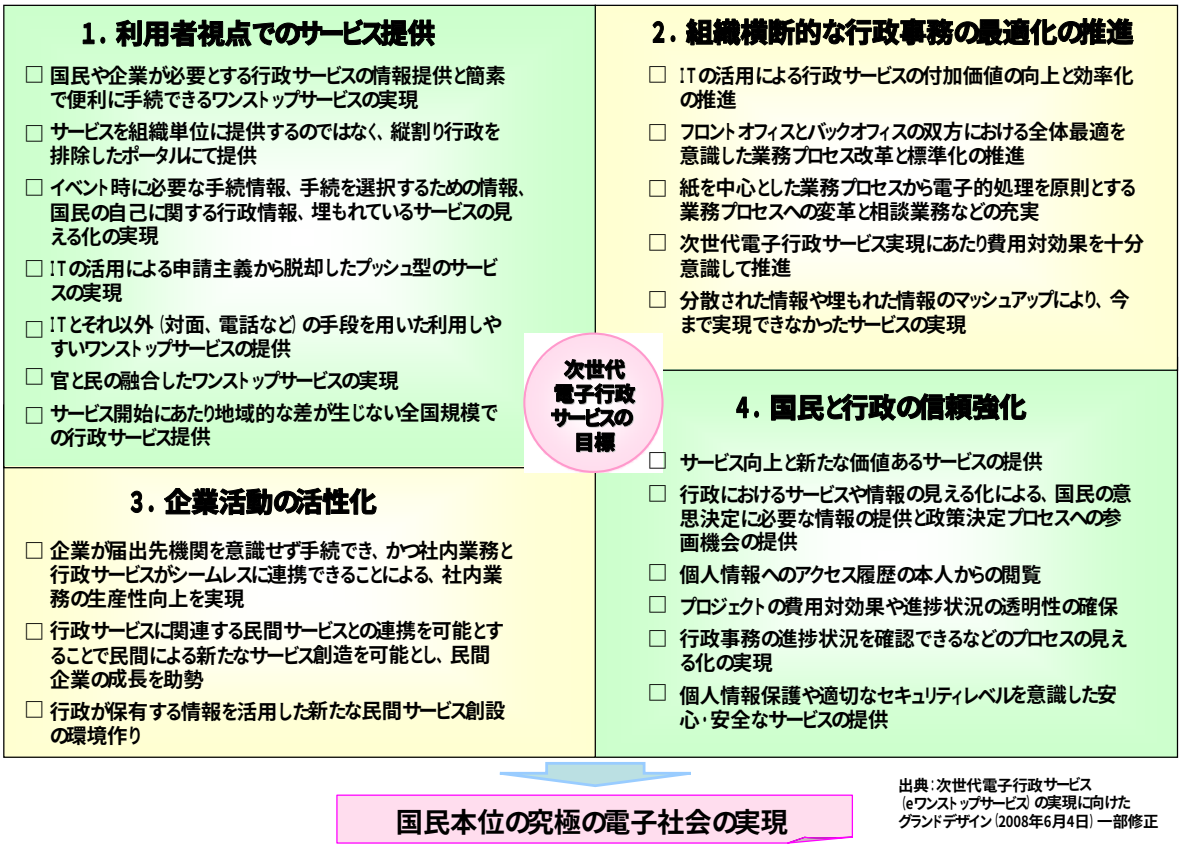


図 2.12 次世代電子行政サービスの目標

ここでは、上記の目標について述べた上で、それに対応する次世代電子行政サービス基盤（以下の図は全体像）の特徴について概説する。なお、このような目標や特徴は、電子政府の認証方式の検討にも敷衍できる可能性があることに留意されたい。

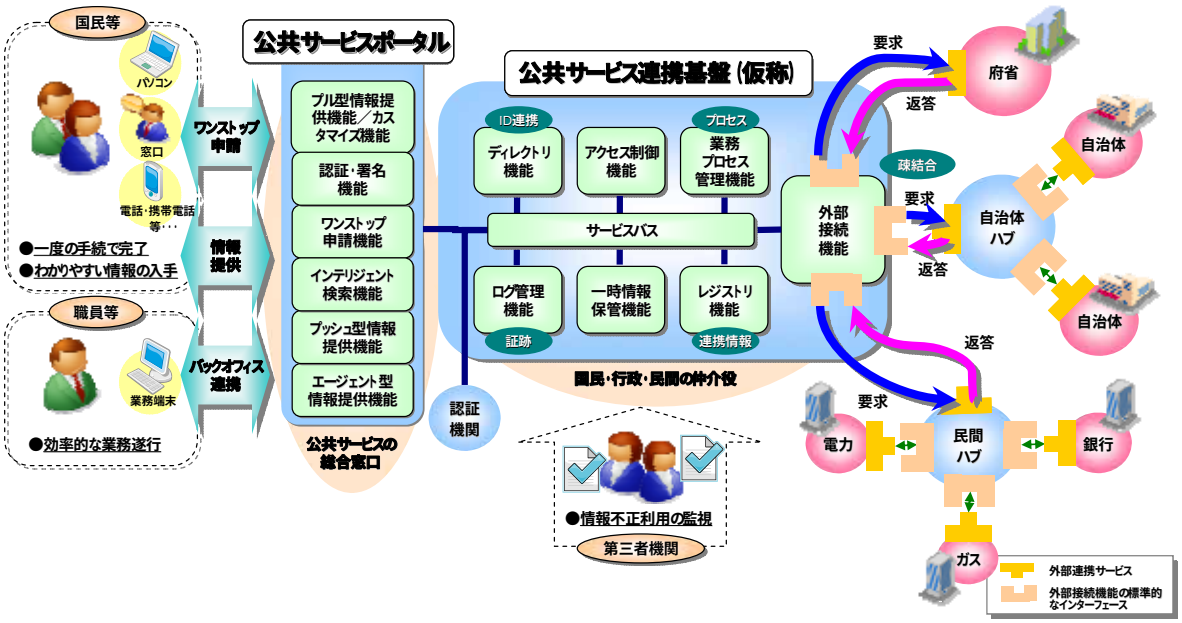


図 2.13 次世代電子行政サービス基盤の全体像

⑴ 利用者視点でのサービス提供

従来の行政サービスは、申請を受ける各行政機関の業務遂行に主眼をおいて組み立てられている。次世代電子行政サービスでは、国民や企業などの利用者の目線で簡素で便利な行政サービスの提供を掲げ、例えば、添付書類の煩雑な準備や複数機関・複数回の訪問要請などといった利用者が直面している問題の解消を目指している。

こうした状況を踏まえ、次世代電子行政サービスでは「公共サービスポータル」の導入を提案しており、利用者の使い勝手の向上や構築・運用に対する費用対効果の改善に資する観点から、複数の関連する手続を一括で行うサービスとしてのワンストップサービスの具現化を目指すものとしている。

⑵ 組織横断的な行政事務の最適化の推進

現在の行政事務は、紙を前提とした業務内・組織内での最適化が図られており、IT を活用した業務の最適化や行政全体の最適化が達成されているとは言い難い状況である。今後、IT の活用をさらに進めることで、電子的処理を前提とし、行政の全体最適を目指した業務プロセスに変革していくことが求められる。

そこで、次世代電子行政サービスでは、各行政機関により分散管理されている行政情報のメタデータ（行政情報の所在、保有している機関、およびアクセス方法等やデータの形式に関するデータ）を管理する「公共サービス連携基盤（仮称）」を構築し、行政機関側でバックオフィス業務の電子的処理を実現させることを目指している。これによって、入力作業の手間が省かれるとともにそこからの人為的ミスが低減され、行政サービス全体としての業務の高効率化が図られるものと期待できる。

⑶ 民間企業活動の活性化

現在の電子政府においては、民間企業等との連携を想定していないために、独自の基盤を構築している。これでは、国・地方の連携や官・民の連携などを通じた情報や知識を共有化、それによる社会的なコラボレーションの実現を期待することはできない。

次世代電子行政サービスの基盤である「公共サービス連携基盤（仮称）」には標準インターフェースを用意し、地方公共団体や民間企業を含む各機関において現在稼働している業務システムとの連携を目指すこととしている。また、各機関の保有する既存システムには、様々なプラットフォームが存在することから、標準インターフェースのプロトコルは、複数の国際標準的なプロトコルをサポートすることとしている。

⑷ 国民と行政の信頼強化

行政においては、そのサービスにかかる業務プロセスや事業進捗などの見える化を図り、その透明性確保に努めることで、国民との信頼強化を深めることが重要である。それと同時に、行政における個人情報のアクセス履歴等の適切な管理等も信頼強化の上で重要である。

そこで、次世代電子行政サービスの基盤では、行政情報等の共有による利用者の不安を解消するために、利用者が希望した場合のみ情報連携することを前提としたサービスの制御を行い、また、個人情報についての本人が意図しない連携や目的外の利用を抑制・防止するために、第三者機関等によるログ記録等の監視が必要であるとしている。

第3章　各分野における電子署名・認証の動向

本章では、電子政府にて用いられる署名・認証方式において求められる要件や、ガイドラインの作成に関する検討にあたって、参考になると考えられる海外の電子政府における事例やそれに関連する標準化の動向、民間における認証方式の利用動向、認証方式の技術的動向について整理する。

3.1.　海外電子政府における認証方式の利用動向

海外電子政府における認証方式の利用動向として、1990 年代の電子署名に関する法制化から、2000 年代の認証ガイドライン策定への経緯について解説するとともに、標準化の動向も含めた海外電子政府の認証ガイドラインの特徴、基盤整備の特徴について概説する。

3.1.1.　海外電子政府における認証方式の時代的背景とその傾向

⑴ 海外電子政府における認証方式の時代的背景

海外電子政府においては、我が国より以前から電子署名及び認証のガイドラインを策定してきた。その時代的背景には、以下のような流れを見て取ることができる。

欧州では、1999年に12月にEUの電子署名指令が成立し、同指令により、構成国に対して、2001年7月までに国内法上必要な措置を講ずることが求められたため、それに対応する形で、多くの国が電子署名法やデジタル署名法の法制化に踏み切った。同指令では、適格電子証明書（Qualified Certificate）以外の証明書（非適格電子証明書）を利用したアドバンスド電子署名(Advanced Signature)や、適格証明書を利用した適格電子署名(Qualified Signature)の要件（表3.1）が規定されており、このような要件に基づいて、欧州標準化委員会（CEN：European Committee for Standardization）と欧州電気通信標準化機構（ETSI：European Telecommunications Standard Institute）において電子署名に関する標準が作成されてきた。

さらに、電子署名の検証等に係るEU域内での相互運用性の確保の観点から、2008年11月には、「単一市場における国境を越える公共サービスの提供を促進するための電子署名とeIDに関する行動計画」が採択されており、2009年第3四半期を目標に適格証明書をベースとした電子署名の相互運用性確保に係るガイドラインを、2010年にはアドバンスド電子署名の国境を越える利用促

進に関する報告を、2012年までには国境を越えるeIDの利用方策についてSTORKのパイロットプロジェクトのなかで取り組むこととされている。

表 3.1 EU 電子署名指令における電子署名等の区分

電子署名の区分	特徴
適格電子署名 Qualified Signature（QS）	**適格証明書に基づき、かつ、安全署名作成装置（SSCD; Secure Signature Creation Device;耐タンパ性を有するハードウェアトークン)により作成されたアドバンスド電子署名。手書き署名と同等の法的効果を有する。**
適格電子証明書 Qualified Certificate（QC）	**電子証明書のうち、付属書Ⅰの要件（署名者の氏名や有効期限等、当該証明書が含むべき事項）を満たし、付属書Ⅱの要件（信頼性の確保に係る運用基準）を満たす認証サービスプロバイダにより発行されたもの。**
アドバンスド電子署名 Advanced Signature（AS）	**電子署名のうち、以下の要件を満たすもの。①署名者にユニークに帰属し、②署名者の同一性確認ができ、③署名者だけが管理できる手段で生成され、④データの改ざんが発見できること。**
シンプル電子署名 Simple Signature（SS）	**電子署名（別の電子データに付加もしくはリンクされ、真正性確認の方法として使われる電子データ）のうち、上記に該当しないもの。（ID/PWなど。）**

大陸法の国では、EU電子署名指令を受け、電子署名の法的効果等について、国内法の整備を行い、電子政府分野においても署名重視のアプローチを採用している。一方、英米法の国では、市場的なアプローチとして広義の電子署名[9]を採用しており、結果として（狭義の）電子署名ではなく認証が幅広く使われるに至っている。電子政府が提供する認証サービスにおいても、英国では認証の保証レベルを定めることを目的として、2002年9月に「Registration and Authentication」が作成された。その後も、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）」やニュージーランドの「Authentication for e-government Best Practice Framework」、豪州の「Australian Government e-Authentication Framework (AGAF)」が策定されている。

大陸法の国においても、インターネット、特にwebサービスの普及に伴い、電子政府の目的が電子申請に代表される「行政の効率化」に加え、「行政の透明化・見える化」が重要なサービスとなってきており、認証が重視されるようになっている。このため、欧州のIDABC[10]の一環で作成

9 例えば、米国1998年ペーパーワーク削減法に基づき、パブコメを踏まえてOMBが決定した行政府における電子署名としては、暗号を用いないID認証（PIN、スマートカード、デジタル化した手書き署名、バイオメトリクス）、暗号を用いるもの（共通鍵、公開鍵）から各省がコスト、リスク、利便性を判断して適切なものを採択することとされている。
http://www.whitehouse.gov/omb/fedreg_gpea2/

10 Interoperable Delivery of pan-European eGovernment Services to Public Administrations,

された「Authentication Policy」に代表されるように、電子政府を推進する多くの国・地域において、「電子政府認証ガイドライン（類するものを含む）」が策定されている。これらのガイドラインでは、認証の保証レベル（LoA（Levels of Assurance））（類するものを含む）が定義されて、各手続・サービスのリスク評価の結果から求められる認証の保証レベルに従って、適切な認証方式が選択できるようになっている。

さらに、2007 年 6 月に、OECD が電子認証は電子商取引や電子政府に不可欠なトラスト及びアイデンティティ保護のためのツールであるとして「電子認証に関する勧告及びガイダンス」を採択した他、ITU-T や ISO などにおける国際標準化の場においても「電子認証ガイドライン」が検討されている。

このような電子署名と認証のガイドライン策定の流れは、我が国も追随していると言える。我が国においては、前述のとおり、2001 年（平成 13 年）4 月に電子署名法を施行しており、2007 年に経済産業省及び財団法人日本情報処理開発協会が「電子政府認証ガイドライン検討報告書」を作成し、各府省における電子行政サービスの主体認証方式を決定する際の考え方、技術的な論点等を提示している。また、第２章で紹介した「次世代電子行政サービスの実現に向けたグランドデザイン」においても、国民と行政の信頼強化が柱の１つして掲げられている。

Businesses and Citizens：　2004 年 4 月に EU で設置が決定された域内における電子政府構築プログラム。i2010 戦略に基づく共通の関心事と水平展開が必要なものを扱う。

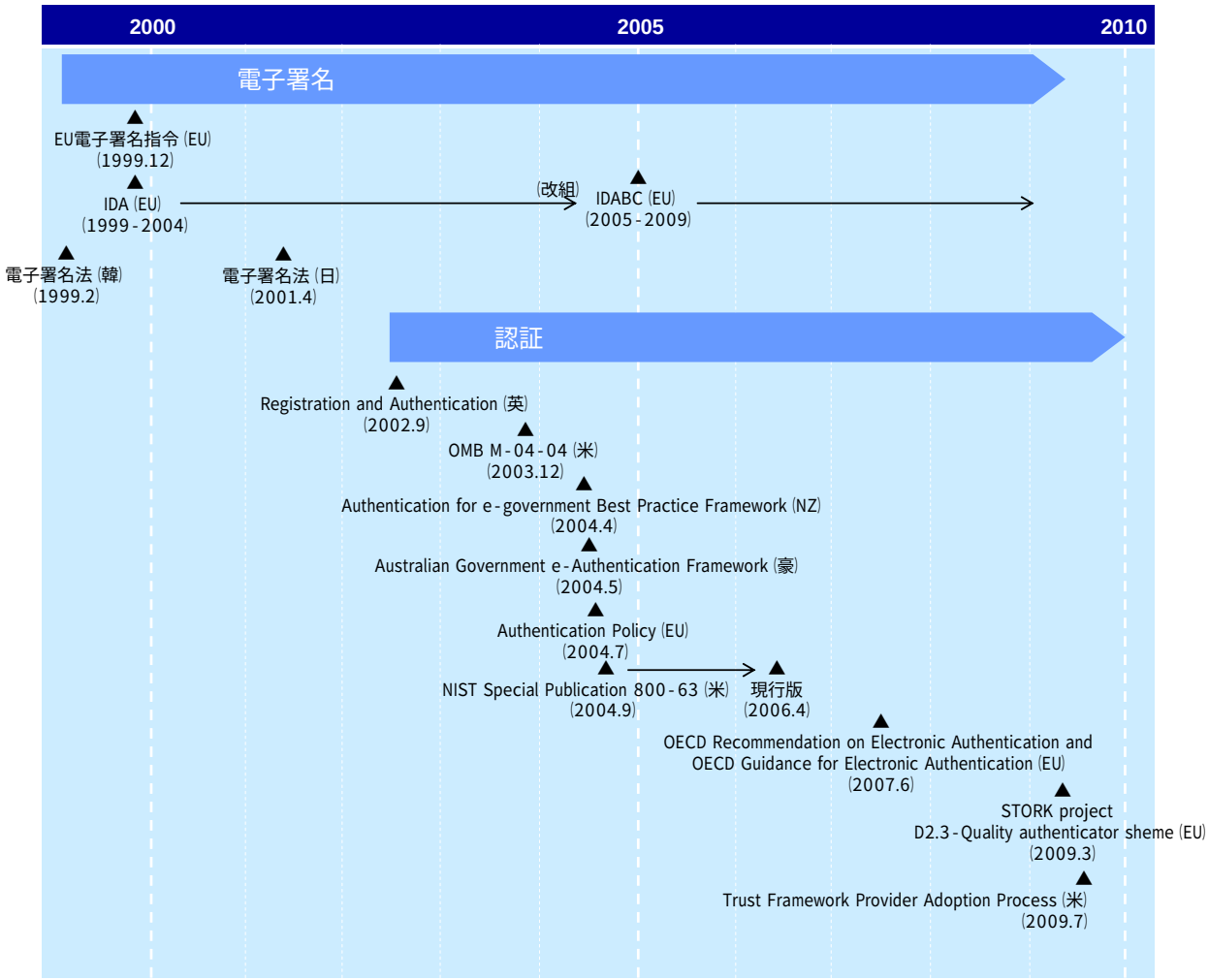


図 3.1 海外における電子署名、認証ガイドラインの検討状況

なお、このような海外電子政府における電子署名・認証基盤の動向と、IT アーキテクチャからの観点における電子文書のやりとりの変化には深い関連があるものと推察される。電子文書のやりとりは、1990 年代後半にはインターネットを利用した電子メール等の利用が中心であったが、2000 年代に入ってサーバ上でプログラムを実行し、端末側では画面表示や入力などの限定された機能のみを行うサーバベースドコンピューティングの活用も大きな割合を占めつつある。その結果、電子メールでのやりとりを主として前提とし、データの改ざんや事実否認に対する不安から電子署名の利用を想定していたが、電子メールの交換を前提としないサーバ側での電子文書の作成・保存においては、利用者側のなりすましに対する不安が高まるため、電子署名に加え、電子署名の一部の効果を実現するためにユーザ認証の重要性が増してきたものと考えられる。

表 3.2 特徴的な電子政府認証ガイドライン

ガイドライン名	Registration and Authentication	Authentication Policy	OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication	STORK project D2.3-Quality authenticator sheme	OMB M-04-04	NIST Special Publication 800-63	Trust Framework Provider Adoption Process	Australian Government e-Authentication Framework	Authentication for e-government Best Practice Framework
発行国･地域	英国	欧州	欧州	欧州	米国	米国	米国	オーストラリア	ニュージーランド
発行機関	電子特命庁	Interchange of Data between Administrations (IDA)	OECD	EU	大統領府行政管理予算局 (OMB)	米国国立標準技術研究所 (NIST)	The Identity, Credential and Access Management (ICAM)	財務管理省情報管理局	行政サービス委員会
発行年月	2002年9月	2004年7月	2007年6月	2009年3月	2003年12月	2004年9月 ※現行版は2006年４月	2009年7月	2004年5月	2004年4月
目的	電子政府サービスへのアクセスを要求する利用者の登録と認証に関するフレームワークのポリシーとガイドラインを提示する。	EU加盟国政府や欧州の公共機関を対象とし、部門ネットワークや横断的なセキュリティ関連プロジェクトにおいて、適切な認証メカニズムを規定するための認証ポリシーの策定に寄与する。	国を超えた電子取引を容易にするための電子認証のガイドラインを提示する。	国を超えたID管理、認証の保証レベルの整合といった制度面も含めた相互運用性の課題を解決する。	電子政府における認証の必要性や適切な認証の選択に関する各政府機関の意思決定を支援する。	認証に関する4つの保証レベルを規定している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) の内容を補完する。	既存の標準化団体や連携認証オペレータを信頼フレームワーク提供団体として認定することで、それらの団体に加盟する企業や組織が政府機関へ認証サービスを提供できる制度を確立する。	政府機関や、政府機関のオンライン取引に関わる民間企業に対して、一貫性のある認証を実践するアプローチを提供する。	各政府機関が認証のプラクティスにおいて一貫性を保持できるように支援する。
特徴	主として、登録と認証の保証レベルについて、4つのレベルを定義。	認証の保証レベルとして、4つのレベルを定義。	認証の保証レベルとして、3つのレベルを定義。	認証の保証レベルとして、4つのレベルを定義。	認証の保証レベルという考え方（4つのレベルの定義等）やリスクアセスメント手法を詳しく解説。	保証レベル毎の申請者の身元識別情報検証やトークン、トークンと身元識別情報の管理メカニズム、認証メカニズムをサポートするために用いられるプロトコル、アサーションのメカニズムの要求事項を詳しく解説。	民間組織を信頼フレームワーク提供団体 (Trust Framework Providers) として認定し、認証プロバイダーの認定プロセスの運用を団体に委譲するプロセスを定義。	政府機関のオンライン取引に関わるリスクに対応した保証レベルとして、4つのレベルを定義。	電子政府のサービスにおいて想定されるリスクの潜在的な影響度を、「身分証明」、「認証」、「処理（トランザクション）」の3つの軸を用いて評価。

(2) 海外電子政府における認証方式の傾向

電子政府で利用される認証方式は、一定水準のセキュリティを確保しつつ、基盤として成立するために普及させなければならない。認証方式は、普及して初めて基盤と言える。

海外の電子政府においては、概ね、認証方式の普及を図り真の基盤とすることを目指している。実際いくつかの国においては、認証方式の普及に成功しており、名目どおりに電子政府における基盤が成立しつつある。たとえば、韓国では、電子政府利用における料金割引等のインセンティブの導入や金融取引で必要となること等を背景として、我が国よりもはるかに多くの電子証明書が利用されている。

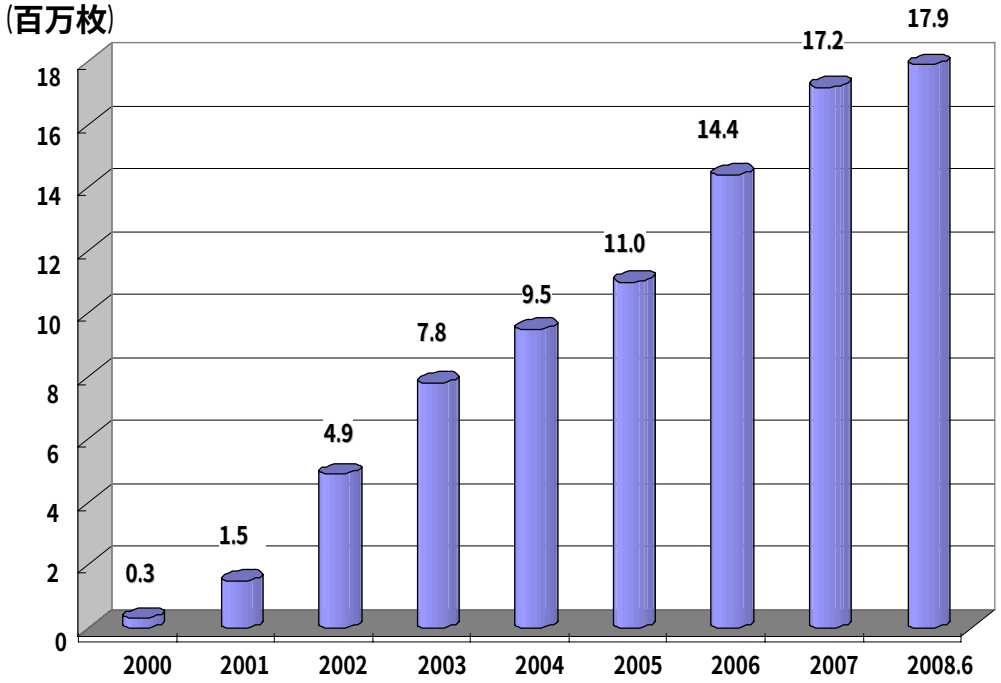


図 3.2 韓国における公認認証書発行数 (韓国行政安全部「情報化に関する年次報告」)

ここで、海外電子政府における認証方式とその基盤の整備の取組に関する特徴を概観するに、普及策には２通りのパターンがあるように見受けられる。

１つは、強制力を持って普及させるパターンである。欧州のベルギーやエストニア等では、セキュリティレベルの高い IC カードを身分証明書としての国民 ID カードとしての強制力を持って普及させている。こうした国々では、強制力を持って普及させるためのコストに見合った様々な利活用を行っている。たとえば、エストニアにおいては、国民 ID カードを使ったインターネット投票を世界で初めて国政選挙に取り入れている。

もう１つの流れとしては、韓国やデンマークに見られるように電子証明書の取得が簡易にできることで普及をはかっている事例がある。デンマークでは、窓口での配布は普及を阻害するという判断から、オンラインで電子証明書を無料で取得でき、その電子証明書を使って、さまざまな電子政府サービスを受けることができる。

一方、すべての国がこのように電子政府において認証方式の普及を実現できているわけではない。例えば、フィンランドにおいては、1999 年にセキュリティレベルの高い IC カードを採用するも、有料かつ任意取得とし、カードリーダ等の機器購入についても国民負担としたために、幅広い普及には至っていない。現在では、銀行が発行するワンタイムパスワード（OTP）トークン（TUPAS トークン）が広く普及したため、電子政府においてもこのトークンが広く利用されている。この OTP トークンは、EU の電子署名指令に合致しないものの、国内においては電子署名としても利用されている。この他、スウェーデンでも銀行が発行するソフトウェアトークンが広く官民で使われている。

我が国と同程度もしくはそれ以上の人口を有する国においては、ハードウェアトークンを導入したばかり、ないしは導入予定及び未定としている国がほとんどであり、現時点でとりあげるべき事例は見あたらない。

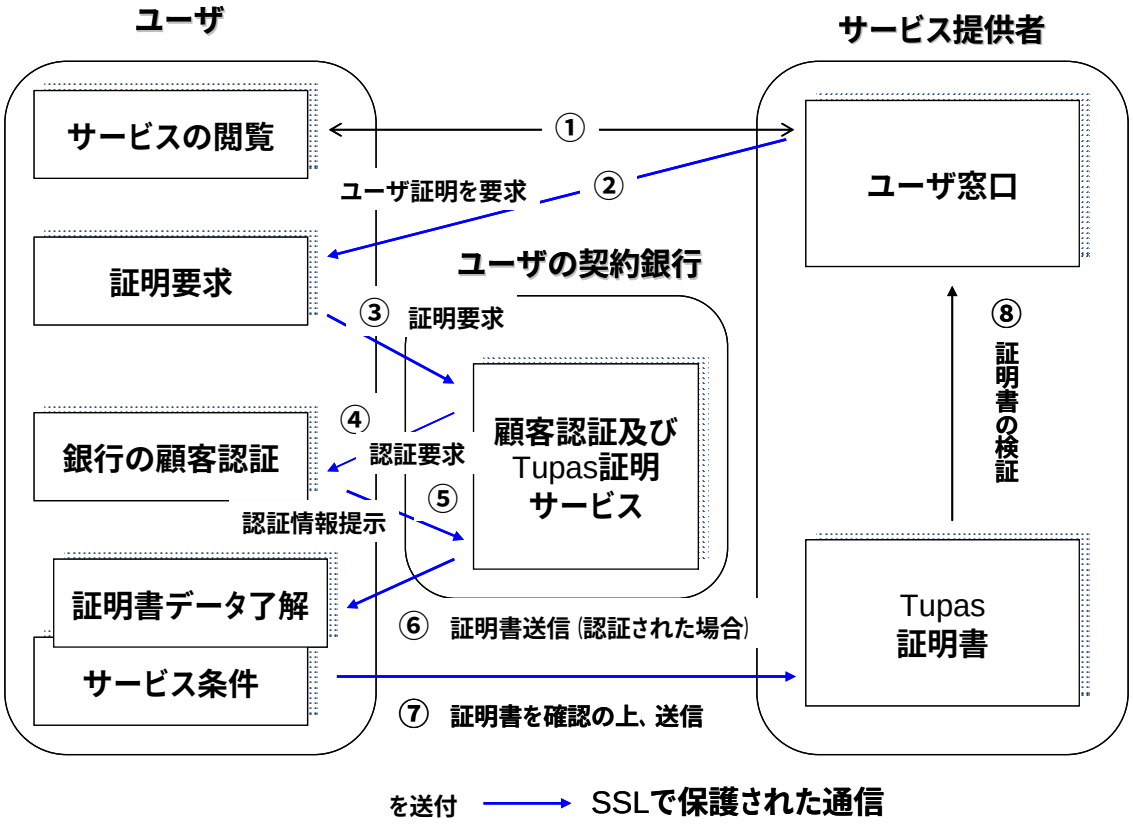


図 3.3 フィンランドの TUPAS を用いた認証方式[11]

[11] TUPAS certification service, Service description and guidelines Version 2.2 https://myacc.tut.fi/tupas/docs/TUPAS_V22_eng.pdf

表 3.3 各国の認証、電子署名制度 (出典：IDABC; Study on Mutual Recognition of eSignatures 他)

	エストニア	ベルギー	韓国	オーストリア	デンマーク	スウェーデン	フィンランド
人口（万人）	約 134 万人	約 1,058 万人	約 4846 万人	約 823 万人	約 551 万人	約 918 万人	約 532 万人
UN e-Gov08	13 位	24 位	6位	16 位	2位	1位	15 位
認証方式	IC カード	IC カード	ﾊｰﾄﾞ・ｿﾌﾄ証明書	ハード証明書	ソフト証明書	ﾊｰﾄﾞ・ｿﾌﾄ証明書	IC カード
導入年	2002 年	2003 年	1999 年	2004 年	2003 年	2002 年	1999 年
取得	義務	義務 (12 歳以上)	任意	任意	任意	任意	任意
発行枚数（年）	105 万枚 (09)	約 850 万枚 (08)	約 1790 万枚(08)	約 10 万枚 (07)	134 万枚 (09)	約 230 万枚 (09)	約 24 万枚 (09)
（人口比）	約 80%	約 80%	約 37%	約 1%	約 24%	約 26%	約 5%
価格	€ 10 (初回限)	概ね€10～15	無料 (用途限定)	eCard は無料	無料	無料	€ 48
携帯対応	対応	なし	対応	対応	予定	2010 年予定	現在中止
発行時対面	必要	必要	必要	必要	不要	ﾊｰﾄﾞの場合必要	必要
電子証明書	署名･認証各1枚	署名･認証各1枚	署名･認証兼用	署名用 2 枚	署名･認証兼用	署名･認証各1枚	署名･認証各1枚
ID	住民コード (ユニーク ID)	住民コード (民間利用に制限あり)	住民登録番号 (ユニーク ID)	住民コードを暗号化した sourcePIN を利用。	住民コードを変換したユニーク番号	住民コード (ユニーク番号)	SSN を変換したユニーク番号
その他	公共交通 (割引あり) や電子投票にも利用。	住民コードの用途制限から認証用途の証明書について、ID 部分の暗号化が議論されている。	一定規模の金融取引で必須。 発行枚数は公認認証書のみ。 銀行窓口でも申請可能。 ﾈｯﾄ用の ID として i-PIN を導入。	銀行カード、全国民が保有する健康保険カード (eCard)、連邦職員証、携帯、USB 等から任意の媒体に格納。	対面発行が妨げるとの配慮からソフト証明書を選択。 2010 年から OTP 導入予定。	BankID 等 3 者を認証提供者として調達。納税申告の場合、税務署作成の申告書に同意する場合は、同封のｾｷｭﾘﾃｨｺｰﾄﾞ送信で手続可。	1990 年代から銀行が始めた OTP トークン (TUPAS) が官民で広く使われている。300 万超 ID を発行。

3.1.2. 海外における電子政府認証ガイドラインの事例

電子政府における認証方式に関する代表的な仕様として、海外の電子政府にてベースとして幅広く活用されている欧州の STORK project や米国政府の基準、及び国際標準化機関における検討状況などを解説する。

3.1.2.1. 欧州の STORK[12] QAA

欧州では、国を超えた ID 管理、認証の保証レベル（LoA（Levels of Assurance））の整合といった制度面も含めた相互運用性の課題を解決するために、STORK プロジェクトが実施されており、そのなかで国境をまたがる認証プラットフォームや EU 域内での引越手続の電子化、安全なドキュメント送信などのパイロット実験が取り組まれているところである。

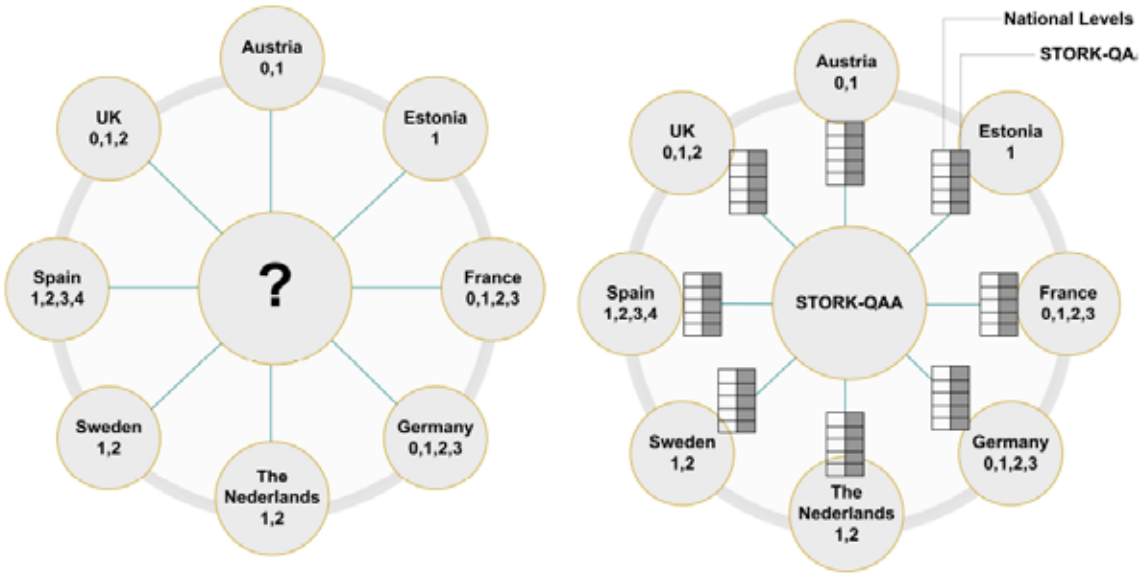


図 3.4 QAA の設定による各国保証レベルの対応づけ概念図[13]

---

[12] Secure idenTity acrOss boRders linKed: EU が出資するプロジェクトで、EU の電子政府の行動計画（i2010）における eID 管理の重要さに鑑み、2010 年までに域内におけるセキュアで利便性が高く、相互運用性のある、市民、企業が政府サービスに使える eID を確立しようとするもの。各国政府機関、研究機関、NPO、企業からなる 29 者が参画している。

[13] STORK D2.3 Quality authenticator scheme
http://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

STORK プロジェクトが、2009 年 3 月にとりまとめた Quality authenticator scheme では、各国の認証方式の相互運用性を確保するための仲介装置として、EU 電子署名指令の適格証明書の概念を包含した形で STORK QAA（Quality Authentication Assurance）を設定している（図 3.4）。

STORK QAA では４段階の保証レベルを設定し、登録、発行、管理、クレデンシャル、認証メカニズムの段階毎の各保証レベルが達成すべき基準を示している。

表 3.4 STORK QAA レベル

STORK QAA レベル	保障レベル
1	ない、もしくは最低限の保障レベル
2	低い保障レベル
3	ある程度の保障レベル
4	高い保障レベル

表 3.5 STORK QAA 対策基準の一例（クレデンシャル）

対策基準	対応するｸﾚﾃﾞﾝｼｬﾙﾚﾍﾞﾙ			
	Lv1	Lv2	Lv3	Lv4
認証要求者が選ぶ、もしくは、自動的に生成されるパスワードもしくは PIN のうち、強いパスワード、PIN のガイドラインを満たさないため（パスワード長や文字種、再利用等）で、推測、辞書攻撃に脆弱なもの。	○			
認証要求者が選ぶ、もしくは、自動的に生成されるパスワードもしくは PIN のうち、強いパスワード、PIN のガイドラインを満たすもの。	○	○		
ソフトウェア証明書もしくはワンタイムパスワードトークン	○	○	○	
EU 電子署名指令付属書Ⅰを満たすソフトウェア適格証明書	○	○	○	
ハードウェア証明書	○	○	○	
EU 電子署名指令付属書Ⅰを満たすハードウェア適格証明書	○	○	○	○

なお、STORK QAA ではサービス提供者が行うリスク分析は、IDABC が 2007 年 12 月にまとめた”Proposal for a multi-level authentication mechanism”[14]や米国 NIST（後述）を参考に

[14]金銭的損失、身体への危険、機密性・可用性・完全性の損失の5軸について、5段階の発生確率及び5段階の規模のスケールでリスク評価を行い、最終的にレベル１～４の保証レベルを決定することとしている。http://ec.europa.eu/idabc/servlets/Doc?id=29622

判断することとされている。EU 域内には、セキュリティレベルの高いハードウェアトークンのみが流通しておりそれ以外の保証レベルを考慮していない国もあるが、他国からの利用者を失わないために、自国ではレベル４利用者しかいない場合であっても、STORK QAA に基づいた保証レベルを決定することを推奨している。

表 3.6 STORK QAA と各国基準の対照

	QAA レベル１	QAA レベル２	QAA レベル３	QAA レベル４
オーストリア				レベル１
ベルギー	レベル１	レベル２	レベル３	レベル４
エストニア		レベル１（利用者名と複数パスワード）	レベル１（OTP トークン）	レベル１（ID カードもしくは携帯 ID）
フランス			レベル１	レベル２、３
ドイツ	レベル０	レベル１	レベル２	レベル３
アイスランド	レベル１	レベル２	レベル３	レベル４
イタリア		レベル１（PIN、パスワード）		レベル１（IC カードに入った電子証明書）
ルクセンブルグ				レベル１、２
オランダ		レベル１	レベル２	
ポルトガル		レベル１	レベル２	レベル３
スロベニア	レベル１		レベル２	レベル３
スペイン	レベル１	レベル１	レベル２	レベル３
スウェーデン			レベル１	レベル２
英国	レベル０	レベル１	レベル２	

3.1.2.2. 米国の OMB M-04-04 と NIST SP800-63

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）は、電子政府における認証の必要性や適切な認証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、2003 年 12 月に大統領府行政管理予算局（OMB）により発行されており、認証の保証レベル（LoA（Levels of Assurance））という考え方やリスクアセスメント手法を詳しく解説している点に

大きな特徴がある。

認証の保証レベルに関しては、以下に示す４つの保証レベルを定めている。

レベル１：利用者が主張する身元識別情報（クレデンシャル）の有効性について、ほぼ、あるいは全く信頼性がない。
レベル２：利用者が主張する身元識別情報（クレデンシャル）の有効性について、ある程度の信頼性がある。
レベル３：利用者が主張する身元識別情報（クレデンシャル）の有効性について、高い信頼性がある。
レベル４：利用者が主張する身元識別情報（クレデンシャル）の有効性について、きわめて高い信頼性がある。

このような保証レベルは、以下に示す手順に従い決定される。

①電子政府のサービスのリスクアクセスメントを実施する。
②上記①で明らかにされたリスクを、適用可能な保証レベルに割り当てる。
③電子認証の技術ガイダンスに基づいて必要な技術的手段を選択する。
④技術的手段を実装したサービスが、要求されている保証レベルを達成していることを検証する。
⑤技術的手段の更新の必要性を判断するために、サービスを定期的に再評価する。

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）では、主として、上記①及び②に関する手法が解説されており、上記③については、電子認証の技術ガイダンスとして、電子認証に関するガイドライン（NIST Special Publication 800-63）の利用が想定されている。

リスクアセスメント手法としては、想定されるリスクの種類を以下に示す６つに分類している。

①不便、苦痛もしくは地位または評判に対する打撃
②財務上の損失または政府機関の賠償責任
③政府機関の活動計画または公共の利益に対する害
④機密情報の無許可の公開
⑤身の安全
⑥民事上または刑事上の法律違反

OMB M-04-04 においては、電子政府内における職員認証を含めた電子政府のサービス提供時における認証を対象として、それぞれの分類について、低位、中位、高位の３つのレベルで潜在的な影響を評価し、最終的にこれらを総合的に勘案してサービスで要求される保証レベルを決定することとしている。

一方、電子認証に関するガイドライン（NIST Special Publication 800-63-1）は、認証に関する４つの保証レベルを規定している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）の内容を補完することを目的として、2004 年 9 月に米国国立標準技術研究所（NIST）により発行されたものである。以下に示す各段階において４つの保証レベルが満たすべき対策基準について、詳しく解説している点に大きな特徴がある。

①申請者の身元識別情報（クレデンシャル）の検証と登録
②トークン（身元を証明するもの（通常は暗号鍵またはパスワード））
③トークンと身元識別情報（クレデンシャル）を獲得・維持管理するために用いられるトークンと身元識別情報（クレデンシャル）管理のメカニズム
④認証要求者と検証者との間の認証メカニズムをサポートするために用いられるプロトコル
⑤リモート検証の結果を他者に送る場合に、これらを通信するために用いられるアサーションのメカニズム

この他、米国においては、民間認証機関のさらなる活用、連携を図り認証に係るコストを削減する観点から、2009 年 7 月に CIO カウンシルの下に設置された ICAM が Trust Framework Provider Adoption Process（TFPAP）を取りまとめた。これは連携認証オペレータや標準化団体等（Kantara Initiative、OpenID Foundation、InfoCard Foundation、InCommon Federation 等を予定）を認定し、電子政府アクセスに係る認証プロバイダの認定プロセスを委ねるためのプロセスを定義している。

3.1.2.3. ITU-T　X.eaa Entity Authentication Assurance 及び ISO/IEC 29115

認証ガイドラインに関する国際標準としては、ISO（国際標準化機構）、ITU（国際電気通信連合）が現在、2010 年の勧告案凍結を目標に ISO/IEC 29115 Information Technology-Security techniques-Entity authentication assurance /ITU-T 勧告 X.eaa Entity Authentication Assurance の策定に向けた合同起草作業を行っているところである。

X.eaa は、電子政府に限られたものではないが、NIST の SP800-63 等をベースラインドキュメントとした４レベルの保証レベルの考え方の下、国際的な認証連携を促進するという観点から、各保証レベルの脅威に対する対策基準の標準化を図ろうというものである。勧告案はまだ十分議

論されているとはいえない段階であるが、現時点においては、登録、認証情報（クレデンシャル）の発行・管理、認証プロセスの３段階における、４レベルの対策基準が検討されている。

3.2. 民間における認証方式の利用事例

電子政府における認証方式の普及と基盤化にあたって、民間における認証方式の導入の考え方を把握し、今後の官民における共通理解となりうるような「ものさし」を策定することは、将来的な官民連携を考える際にも重要である。そこで、ここでは民間サービスにおけるユーザ認証、金融機関のセキュリティ対策について解説する。

3.2.1. 民間サービスにおけるユーザ認証

民間におけるオンラインサービスにおいては、既存の紙と押印による手続を電子的に置き換えた電子行政サービスとは対照的に、元々紙文書を前提とせず発展してきた傾向が強い。そのため、民間サービスでは電子署名よりも認証が利用されている。

この民間サービス分野においても、我が国の行政サービスと同じく、認証のセキュリティ基準となりうる統一的な「ものさし」は存在しておらず、事故の発生を前提として、必要な安全性を確保するための情報セキュリティ対策が講じられている。具体的に、認証方式を選定するに際しては、以下に示す「利便性」、「適用性」、「経済合理性」の３つの観点と安全性のバランスを考慮して、許容できるレベルの事故発生を前提としつつ、適切かつ合理的な手段が選択されている。

また、事故の発生を前提とした場合の対応としては、サービス約款での利用者と事業者の責任分担の事前合意や保険によるリスクファイナンス、事実否認への対処としてのログ保存等が重要となっている。

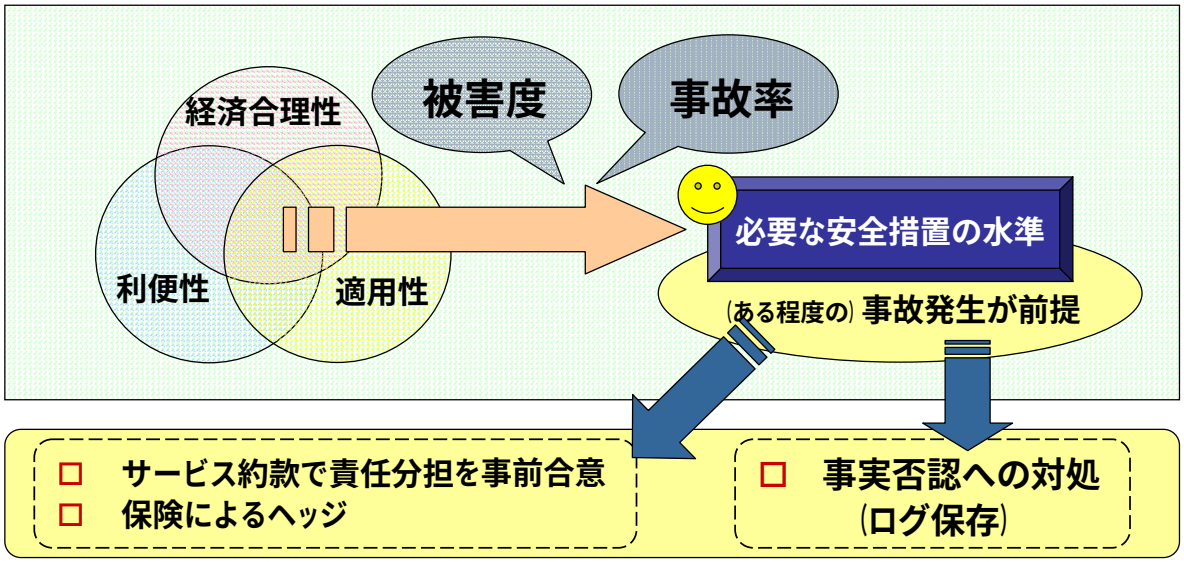


図 3.5 民間サービスにおけるユーザ認証のあり方

(1) 利便性

民間サービスにとって、顧客である利用者に負担を与えるような認証方式は避けなければならない。専用機器や専用ソフトウェア、複数パスワードの利用は、利用者の負担を増し、サービス利用の敬遠につながるおそれがあることから、PC サイトでは、単一パスワードを用いた認証、携帯サイトでは、端末 ID（個体識別情報）を用いた認証が主流になっている。

利用者が複数のパスワードを利用した場合、セキュリティ確保策としては有効であるが、それらの忘却リスクが高まるとともに、利用者の利便性が低下するものと考えられている。

(2) 適用性

民間サービスにとって、多様な端末環境にて広く利用可能な認証方式であることは顧客獲得の上で重要である。PC、携帯電話、スマートフォン、ゲーム機、デジタルテレビなど端末環境が多様化する中で、特定の端末環境や状況に利用が限定される認証方式は採用しにくいと考えられている。

(3) 経済合理性

民間サービスにとって、提供するサービスに見合うコストで認証方式を実現できるか否か判断することは利益を追求する上で重要である。事故の発生率いかんによっては、高価なトークンによるワンタイム（OTP）パスワードのように、認証方式にコストをかけるよりも、被害を被った

利用者への補償にコストをかけた方が安く済む場合が多いと考えられている。

3.2.2. 金融機関のセキュリティ対策

金融機関においては、インターネットバンキングが今や重要なチャネルとして認識されている。同時に、インターネット専業銀行も定着しつつあり、電子商取引における決済サービス機能を提供するなど、重要性を増しつつある。

こうしたインターネット上での取引に対し、金融機関においては、本人認証の強化やサイト認証などを含めた総合的な対策が展開されている。

金融機関のセキュリティ対策

（1）セキュリティ対策の強化
・本人認証等の強化
・メールやサイトの正当性を確認するための手段の提供
・不正取引監視、前回ログイン時刻の表示、取引結果のメール通知
（2）利用者の啓発
・各金融機関のホームページ上等での注意喚起
（3）リスクに応じた利便性、セキュリティ、サービスのバランス確保
・振込み限度額の引き下げ
・事前登録先による振込先の限定
（4）各業界の関係者との連携
・フィッシングサイトの早期発見、閉鎖、情報共有

このうち本人認証においては、利便性に配慮した上で、リスクに応じた複数の認証方式を組み合わせて用いる多要素認証等の導入が進められている。例えば、ID・パスワードに追加して、乱数表やワンタイムパスワード（OTP）等を利用する形態が挙げられる。同時に、リスクに応じた利便性、セキュリティ、サービスのバランス確保の観点から、認証方式のセキュリティレベルや被害発生時の補償範囲に応じた利用限度額の設定が行われており、一定の効果を上げている。また、サイト認証については、紛らわしいドメインを取得した上で SSL 証明書を用意する不正なサイトも出現していることから、EVSSL 証明書[15]の導入がその対策として普及している。

[15] EVSSL 証明書とは、SSL 証明書の一種であるが、法人登記など実在証明にかかる審査基準を厳しくすることで、発行に際して厳密な存在確認を行うことを要件としている。

一方、米国では、米国連邦機関検査協議会（FFIEC）が 2005 年 10 月にインターネットバンキングにおける認証に関する指針（Authentication in an Internet Banking Environment）を改訂し、2006 年末までに二要素認証を導入するよう奨励している。このような二要素認証の範囲については、一般的な認証方式のみならず、利用者のブラウザ環境の設定情報を取得したものなども含まれている。

3.3. オンライン手続における認証方式の技術動向

電子政府のオンライン手続においては、下図のとおり、申請、受付、保存・管理等の一連の場面において、電子署名・認証技術等が複合的に利用されている。ここでは、具体的な電子署名・認証技術の紹介として、このような電子署名・認証技術を採り上げ、その特徴を解説する。

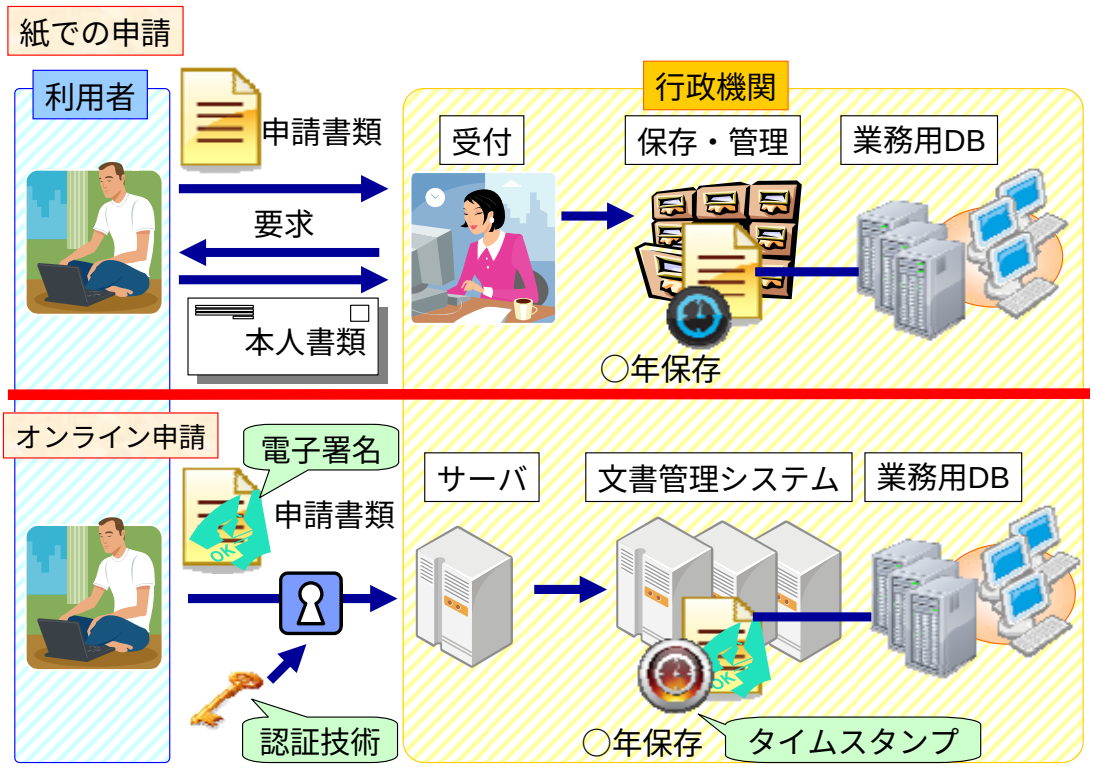


図 3.6 紙申請とオンライン申請の手続の違い

3.3.1. 認証技術について

3.3.1.1. 生体認証

生体認証（バイオメトリクス認証）とは、個人の「身体的特徴」や「行動的特徴」を利用する認証技術である。生体認証では、本人が、本人自身の身体を用いなければ示すことが困難な情報をシステムや装置に対して提示することによって、本人であることを確認する。

生体認証によって利用される主な身体的特徴には、指紋、虹彩、血管パターン、掌形、顔形等があり、行動的特徴には、手書き署名、キー・ストローク、声紋等がある。なお、身体的特徴であっても、本人の身体から分離し、他人によって提示することが容易な身体的特徴は、生体認証に利用することはできない点に注意が必要である。（例えば、DNA は本人が知らぬ間に取得された髪の毛から取得する等が可能である）

生体認証は、ID・パスワードや IC カード等による認証方式と比較して、本人による記憶や所持といった負担が生じないことから、携帯電話、パソコン、USB トークン、入退管理システム、CD／ATM、パスポート等の用途に普及が拡大している。

生体認証における認証の精度を表す代表的な尺度として、誤受入率や誤拒否率が利用されてい

る。誤受入率は、全試行回数に占める誤受入回数の割合で表わされ、攻撃者が自分の生体情報を提示してなりすましを試みるゼロ・エフォート攻撃に対する認証の精度を評価する尺度として用いられている。また，誤拒否率は、自分の生体情報がどの程度の割合で他人のものであると判断されるかを示したものである。

その一方で、人工指等の人工構造物を用いた攻撃や、センサーの不正な設定操作による攻撃等、それらの脆弱性を厳格に確認するための手段や方法が確立されていないだけでなく、ウルフと呼ばれる複数の他人の参照データと高い確率で誤一致を引き起こす特殊なサンプルが存在することが指摘されていること等、従来の尺度だけではははかることのできない攻撃方法が様々問題提起されている。このような状況から、前述の尺度では、生体認証システムへのセキュリティの評価は困難となっている。特に、オンライン認証については、入国管理における目視による確認や銀行 ATM のように防犯カメラによって監視することができないこと等から、人工物等の新しい攻撃がより見破られにくい環境ということができる。

そこで、このような攻撃への耐性に関する評価尺度の確立と、それらのプロセスの標準化を図ることが有用であり、具体的な検討が必要となっている。また、個々の生体認証システムのセキュリティ評価についても、ベンダーが独自に行うものが主流となっていることから、現状の誤受入率・誤拒否率といった用語の統一だけでなく、セキュリティの評価尺度の確立、そして、同一基準でのセキュリティの測定・評価の実現に向けた検討が必要となっている。

3.3.1.2. **ワンタイムパスワード**

ワンタイムパスワード（OTP）は、万が一固定のパスワードが悪意のある第三者に渡ってしまった際にそれを再利用されるリスクを軽減する手段として認知されている。一般的には、OTP 生成機を用いて一度しか使えないパスワードをランダムに発生させて認証情報として利用する。

OTP 技術は、生成機が発生させた OTP の他にも、活性化させるための PIN 番号入力（記憶）や、ハードウェアトークンの場合には OTP 生成器を持っていること（所持）自体が追加の認証要素となるため、多要素認証技術として機能する。

OTP を発生させる方式としては、時間同期アルゴリズムを用いて OTP 生成機側と認証サーバ側の OTP 生成を同期させる方式が一般的であるが、他にも様々な実装手段が考案されている。

これまで、OTP 生成機は専用のハードウェアトークンとして利用者に配られることが多かったが、最近では携帯電話を OTP 生成機として利用することにより、利用者の利便性を向上する配布形態も取られるようになっている。

3.3.1.3. **画像認証**

画像認証は、本人の記憶に基づく認証技術の一種であり、画像を認証のパスワードとして用い、本人の記憶を確認することによって認証を行なう技術である。画像認証は主に下記の方式に大別される。

- 複数の画像から、本人のみが知る正しい画像を選択（Cognometric 方式）
- 画像内の本人のみが知る特定箇所をマウス操作等により指定（Locimetric 方式）
- 本人が画像を描画し、事前に登録済みの描画パターンと照合（Drawmetric 方式）

画像認証の利便性は、利用者に対して記憶の負担を与える点でパスワード認証等と類似しているが、人間は文字情報に対して画像情報の認識・処理能力が高いため、パスワードよりも画像のほうが覚えやすいという利点がある。特に人間の画像再認能力は顕著であり、利用者の画像が表示される Cognometric 方式や Locimetric 方式においては、利用者の記憶負荷が大きく抑えられると考えられている。利用者にとって関係の深い画像ほど覚えやすい、類似した画像に対しては記憶の混同が起こるなどの側面があるため、利用者が記憶しやすい画像や操作（描画パターン）を用いるための工夫が望まれる。また、画像認証は視覚に依存せざるを得ないことから、視覚障害者に対しては代替手段を提供する必要がある点にも配慮が必要である。

安全性に関しては、画像認証が記憶による認証技術であることから、論理的にはパスワード等による認証技術と同等の安全性を確保することが可能である。しかしながら、利用者の利便性を優先し、画像の選択肢、描画のバリエーションが十分に確保されない場合、十分な安全性が確保されない可能性がある点に注意が必要である。特に、一般的なディスプレイに一度に表示できる画像の枚数は高々数十枚であることから、複数の囮画像の中から正しい画像を選ぶという認証形態となる Cognometric 方式においては、総当り数の確保が課題となる。また、画像という視覚情報を認証情報として使う以上、覗き見対策が必須となる。

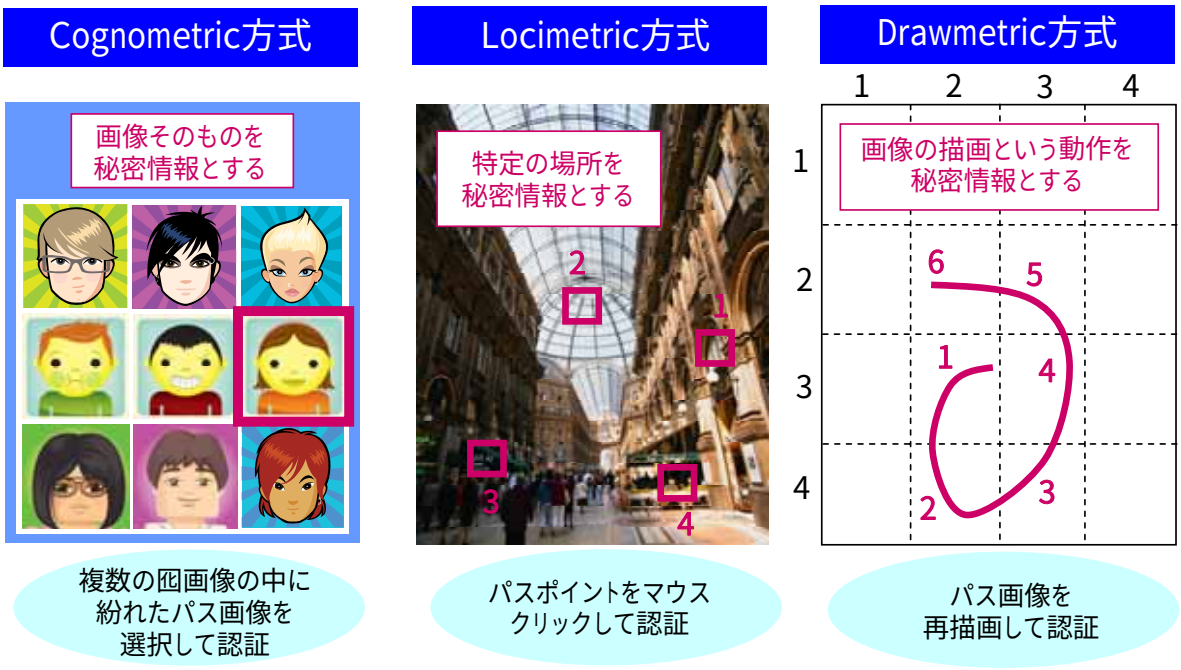


図 3.7 画像認証の種類

3.3.2. 電子署名技術

3.3.2.1. デジタル署名

デジタル署名は、電子化されたメッセージや文書の真正性を証明するために付与される電子署名を、暗号技術を用いて計算するスキームである。デジタル署名により、メッセージや文書の受け手は、その送り手が誰か（真正性）とその情報が改ざんされていないこと（完全性）を確認することができる。

デジタル署名が提供する別の機能として、電子化された契約文書等に対する否認防止がある。デジタル署名による否認防止機能は、タイムスタンプの技術と組み合わせることにより、電子証明書が失効しても、また、万が一、署名に利用した暗号化アルゴリズムが危殆化、あるいは秘密鍵が盗まれてしまったケースにおいても、その効力を維持することができるようになる。

現在最も流通しているデジタル署名では、そのアルゴリズムとして公開鍵暗号方式を採用している。公開鍵暗号方式でもっと著名なものは RSA アルゴリズムである。

また、仕様の具体例としては、主に XML で書かれた文書にデジタル署名を付与するために利用され、特に XML を用いて実装されている SAML（Security Assertion Markup Language）、Web Service -*のような認証プロトコルにおいて安全性を高める手段として採用されている XML デジタル署名（XML DSig, XML-DSig, XML-Sig）や、EU 電子署名指令 1999/93/EC において長

期間に渡る証明の有効性、より強度な非否認性という要件に基づいてプロファイル化した XAdES（XML Advanced Electronic Signature）などがある。

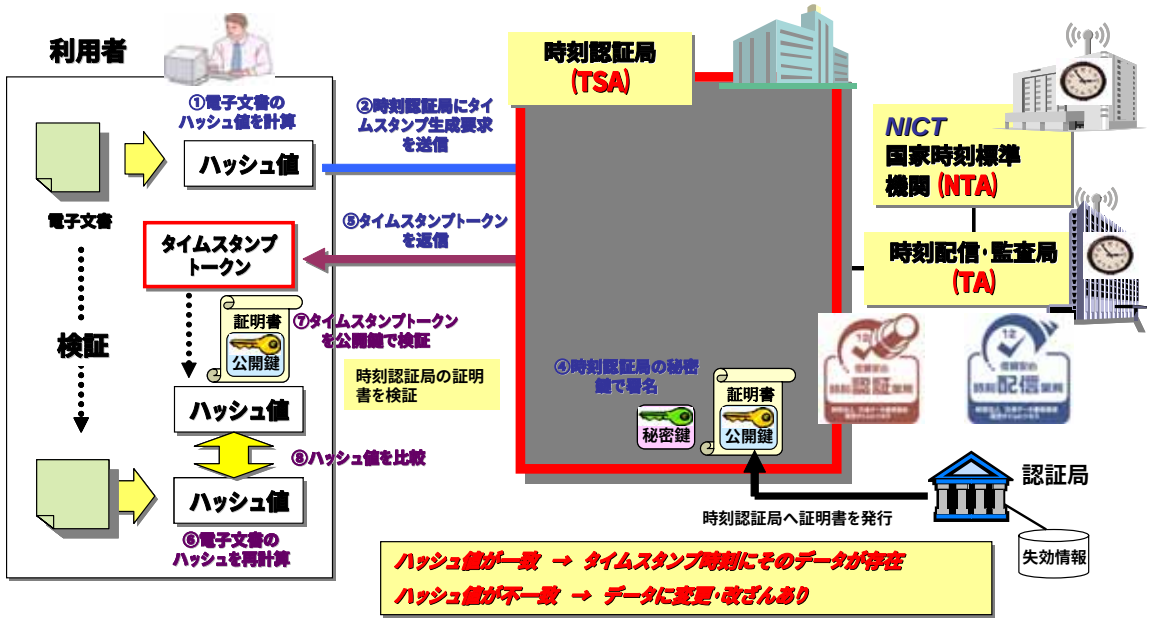
3.3.2.2. タイムスタンプ

信頼できる時刻を利用して、電子文書の証拠性を確保するタイムスタンプは、電子文書に関して、スタンプ時刻以前に存在していたこと、スタンプ時刻以降に改ざんされていないことを証明することができる。

電子文書の長期保存には、以下に示す要件が求められるが、電子署名が付された電子文書にタイムスタンプを付与することにより、そのタイムスタンプの有効期間内において、いつでも電子署名の有効性が検証できるようになるため、有用である。

真正性：電子文書の作成の責任と所在が明確で改ざんがないこと。 見読性：必要に応じて内容を肉眼で読み取ることを可能とすること。 保存性：真正性と見読性を法定保存期間にわたって確保できること。

既に標準化が完了していることや、e-文書法の要件にあがっていることなどから、普及のフェーズに入っており、電子契約における契約書等の原本製保証や、図面・文書管理、知的財産保護などの民間の用途に幅広く活用されている。



出所）財団法人　日本データ通信協会タイムビジネス協議会（TBF）

図 3.8 タイムスタンプの仕組み（例：電子署名方式）

3.3.3. シングルサインオン

シングルサインオン（SSO）については、諸外国の電子政府においても、利用者の利便性向上やサービス利用の促進の観点から、導入や検討が進められている。標準化動向としては、OpenID Foundation が推奨する OpenID や、Liberty Alliance Project が推奨する SAML、The Information Card Foundation が推奨する InformationCard といった業界標準仕様が制定されている。

さらに、このようなシングルサインオンの各仕様間の相互運用性を確保するための技術の開発や課題検討が、Kantara Initiative の下、コンコーディア・ディスカッショングループにおいて推進されている。

設立の背景には、過去に認証プロトコルの主導権争いがベンダー間で長年行われてきたため、複数のプロトコルが並立してきた経緯がある。ユーザ企業ではそれらの優位性を比較しなければならず、技術や製品の選択肢の多さが逆に負担になることも多い。また、これまで競争関係にあったため、プロトコル間での相互運用や協力は進められてこなかった。こうした状況が認証方式そのもの普及の妨げになっていた一面もある。

プロジェクト・コンコーディアではこうした過去を教訓として捉え、全ての認証プロトコルを内包した連携認証実現のために、SAML、WS-*、OpenID の推進者が一堂に集うコミュニティを形成している。

第4章　電子政府に求められる認証基盤の要件とあり方

第３章では、海外電子政府における認証方式の動向として、1990 年代は欧州中心に電子署名に関する法制化が進んだが、その後 2000 年代に入り、電子政府を推進する多くの諸外国において見える化の必要性が高まり、認証が重視されるようになったことを受けて、「電子政府認証ガイドライン」が策定されるようになったことを述べた。

こうした認証重視の風潮は、我が国においては電子政府よりも民間分野において顕著になっている。民間においては、オンラインによる閲覧系サービス等における本人認証においてだけでなく、電子署名の利用が想定されていた電子商取引分野においても認証が広く利用されており、電子署名の利用シーンは、電子入札、納税申告等、官提供サービスに偏っている。民間企業が認証方式を選定するに際しては、利便性、適用性、経済合理性と安全性のバランスを考慮して、許容できるレベルのリスクを取りつつ、適切かつ合理的な手段が選択されている。このような考え方を前提としていることから、民間においては多種多様な認証方式が用いられるとともに、様々な用途への利用拡大が着実に進んでいるのであろう。

このような風潮の中で、我が国電子政府についても、今後、さらなる見える化、透明化が求められることが予想され、その対応策として適切な認証方式を考えていく必要が出てきている。さらに、第２章で述べたように、我が国電子政府における認証方式は、利便性や適用性などにおいてまだまだ改善すべき問題を内包しており、次世代電子政府の実現に向けた認証方式のあり方について整理を行う必要がある。

以上から、本章では、第２章、第３章において整理した電子政府の現状と各分野における電子署名・認証の動向より問題点を再度洗い出し、電子政府に求められる認証方式の要件を整理するとともに、認証方式の普及拡大によって実現される基盤[16]のあり方を導出する。

[16] 本章では、電子署名を含む認証方式の普及拡大によって実現される基盤を「認証基盤」と呼ぶことにする。

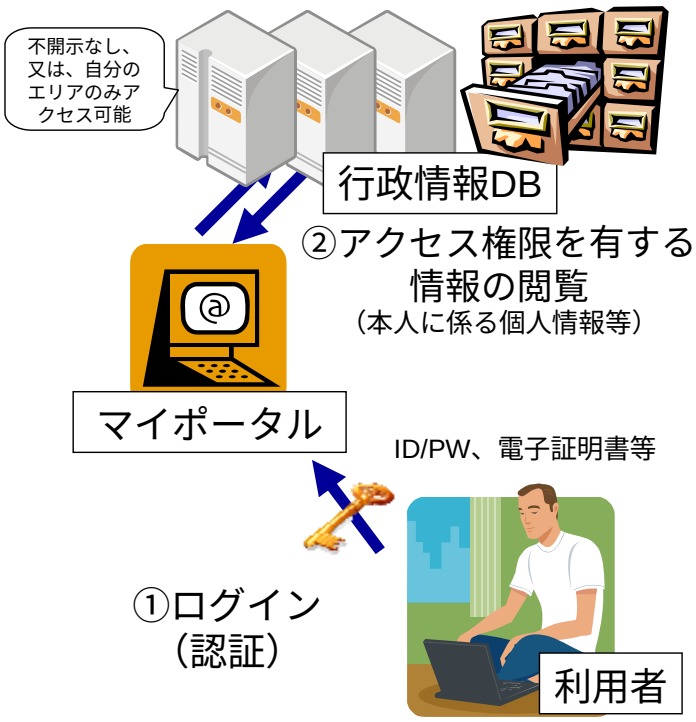


図 4.1 電子政府の見える化、透明化の概念例

4.1. 電子政府の認証に見られる問題点

ここでは、第２章、第３章から判明した我が国電子政府の認証に見られる問題点を再度整理することにする。

第２章では、オンライン利用率が手続によってばらつきがあり、電子署名と認証方式の適切な選択がその拡大にとって重要な１つの要素であることを述べた。また、現在の電子政府における課題として、認証方式における利用性の問題（例えば、利用者がパソコンに向き合う前に行う事前準備、ソフトウェアのインストールなど一連の準備の手間、ID・パスワードの乱立による忘却）や同一手続における方式の違い、改ざん・事実否認等に対する対策の必要性を指摘した。さらに、電子政府の将来像として紹介した次世代電子行政サービスにおいては、利用者視点、行政事務の最適化、民間企業との連携などの目標が設定されている。

一方、第３章では、先行している海外の電子政府や民間サービスにおける認証においては、複数の認証方式や媒体の選択が可能であること、万人に対する利便性や経済合理性を追求した上で許容できるレベルでの事故前提社会に立脚した運用を行っていることなど、我が国の電子政府とは異なった視点が存在している。

このような背景から、現在の電子政府の認証に見られる問題点を整理すると、以下の６点に集

約することができる。

（１）利用者に対する負担の強制

（２）利用できる認証方式の制限

（３）同一手続における本人確認方式の違い

（４）改ざん・事実否認等に対する対策の必要性

（５）行政サービス内における連携不足（業務独自の認証局の構築）

（６）官民での連携のなさ（官独自の認証方式の導入）

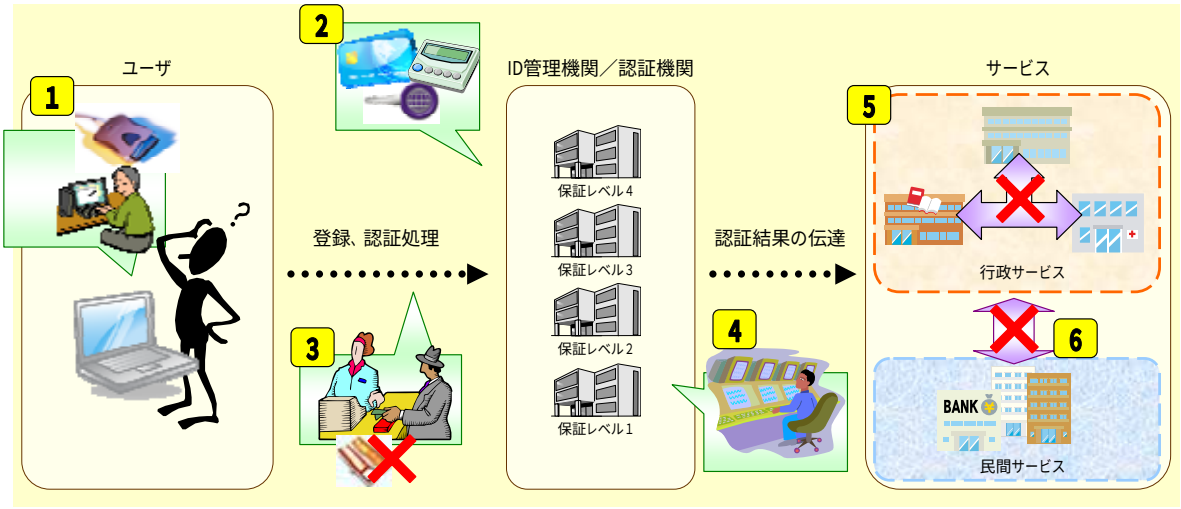


図 4.2 電子政府の認証に見られる問題点

4.2. 電子政府の認証基盤において求められるシステム要件

前節で述べた電子政府の認証に見られる問題点を踏まえると、電子政府における認証方式の導入にあたり求められるシステム側の要件としては以下の７点を考えることができる。次項以降、この具体的内容について説明を行うことにする。

表 4.1 電子政府の認証方式の導入あたり求められるシステム側の要件

(1) 利用者数や利用率に応じた適切なシステムのスケーラビリティ
・利用者数や利用率に応じてシステム規模が拡張可能な設計とすること。
(2) 標準化、実用化された技術の採用による相互運用性
・認証方式の普及展開と方式間の連携のため、標準化、実用化された技術を採用して相互運用性を確保すること
(3) ユーザビリティ
・利用者に新たな機器の購入やソフトウェアダウンロードをできる限り強制しないこと。 **・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[17]を認証部分についても実施すること。**
(4) アクセシビリティ
・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こと。
(5) 客観的評価による安全性の確認
・認定基準に基づく第三者評価、自己点検結果の公表、等により、安全性を客観的に確認できること。(証跡管理、トークンの強度など)
(6) 費用対効果に見合う適切な構築・運用コスト
・費用対効果に見合う構築・運用コストであること。例えば、申請・閲覧1回あたりのシステム構築・運用・監査費用を指標とする。
(7) 電子政府全体としての最適化
・認証方式のプラットフォーム化等により、電子政府全体としての最適化を図ること。(ユーザビリティの観点からもプラットフォーム化は有効。)

4.2.1. 利用者数や利用率に応じた適切なシステムのスケーラビリティ

民間のシステムでは、システムの運用開始後に設計時に想定した以上のトランザクションが発生し、システム基盤の性能不足に陥ることがある。一方、電子政府システムの中には、オンライン利用率の低迷等を背景に実質的にほとんど利用されていないものもあり、システム基盤の過剰性能が問題視される場合がある。

電子政府の認証方式においては、このような過剰性能を適正化していく上で、利用者数や利用率に応じてシステム規模を拡張可能な設計・構成とすることが重要となる。

---

[17] ユーザビリティテスト：「電子政府ユーザビリティガイドライン」（平成 21 年 7 月 1 日）3.4 節及び付属文書 6 の 7 章に記載。（http://www.kantei.go.jp/jp/singi/it2/guide/index.html）

4.2.2. 標準化、実用化された技術の採用による相互運用性

電子政府における認証方式の共通化や認証方式間の官民連携のため、相互運用性や拡張性、信頼性の面で優れている標準化、実用化された技術を活用することが、前述した電子政府の問題点を解決にあたり有効であると考えられる。さらに、標準化、実用化された技術での認証基盤の構築は、開発コストの低減にも資するものである。

4.2.3. ユーザビリティ

認証方式の利用者に情報リテラシーが必ずしも十分にあるとは限らないことを考慮すると、利用者の使い勝手の良さを求めることは必要不可欠である。新たな機器の購入やソフトウェアのダウンロードなど、利用者への負担を強制するような認証方式は避けるべきである。

また、利用者の負担にならないように、下位レベルの認証方式に追加的な要素を付加すれば、上位レベルの認証方式として利用可能になる（例えば、オンラインバンクにおいて、口座残額照会では ID・パスワード、さらに振り込み等ではワンタイムパスワードを利用）など、双方で互換性のある選択肢が提供されることが重要である。

さらに、第３者視点による評価はユーザビリティ向上にとって重要であることから、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実施することが求められる。

4.2.4. アクセシビリティ

電子政府の手続で用いられる認証方式においては、高齢者・障害者等に配慮して、容易に操作できるように設計・構築されることが求められる。例えば、入力や情報表示、ヘルプ等の必要機能については、障害の種類・程度と操作上の障壁との関係を十分勘案して、できる限り多様な代替手段が提供されることが重要である。

4.2.5. 客観的評価による安全性の確認

電子政府における認証基盤の普及展開や基盤間の連携を促進していく上で、当該認証基盤の強度の指標等が明確化される必要がある。このため、認定基準に基づく第三者評価や自己点検結果の公表などにより、機能面、及び証跡管理を含む運用面等から、認証方式の安全性を客観的に評価・確認するための仕組みが構築されることが重要である。

4.2.6. 費用対効果に見合う適切な構築・運用コスト

無謬性を追求して信頼性や安全性の高いシステムを構築することは重要であるが、その結果として利用者に使われないシステムになるようでは意味がないものになるばかりか、費用対効果も十分とは言えないものとなる。

このため、利用者への普及見込みや障害・リスクへの対処可能性等を十分勘案しつつ、費用対効果の観点からみてコスト負担が過重なものにならないよう構築・運用コストを適正化していくことが重要となる。

4.2.7. 電子政府全体としての最適化

ID・パスワードをはじめとした認証方式が数多く存在する中、電子政府の認証方式の一元化を図ることは、利用者にとって利便性及び安全性の観点から有効である。つまり、利用するサービスに応じた認証方式の合理的な選択や、利用者における認証方式の使い分けに伴う負担感の改善などによって、利用者の安全性及び利便性の向上に資するものである。この電子政府の認証方式の一元化に当たっては、その根幹となる ID 管理についても検討していくことが重要である。

また、こうした最適化は、本人確認や認証の発行・管理等の重複する業務の集約による行政サービスの効率化を実現し、電子政府全体としての最適化を達成することを可能とする点でも重要である。

4.3. 電子政府の認証基盤において利用者から求められる要件

前節では、電子政府の認証方式の導入にあたり求められるシステム側の要件を７点に整理して述べた。一方、利用者にとって使いやすい認証方式を提供するという観点から、利用者視点での要件を整理し、それぞれの特徴を解説する。

4.3.1. 保証レベルに対する実装の考え方

電子署名や ID・パスワードなどの認証方式は、それぞれ脅威に対する強度（保証レベル）を有している。このため、保証レベル[18]ごとに異なった認証方式を利用することが予想されるが、利便性の観点から、利用者にとって実際に使い分ける認証方式は、できるだけ少ない方が良いと考えられる。

しかしながら、例えば、身分証明書としても使われている健康保険証は窓口で他人に預ける可能性があるが、実印は大切に保管すべきであり、他人には預けることは想定されていないといった常識も存在していることから、日常的に用いる認証方式と、利用頻度は低いものの重要な用途に用いるため大切に保管すべき認証方式は分ける方が妥当である。

さらに、実際の認証の場において、複数の認証方式が必要な場合でも、それぞれの操作方法に互換性を持たせる、もしくは分かり易く整理する等の措置を講じることが重要である。

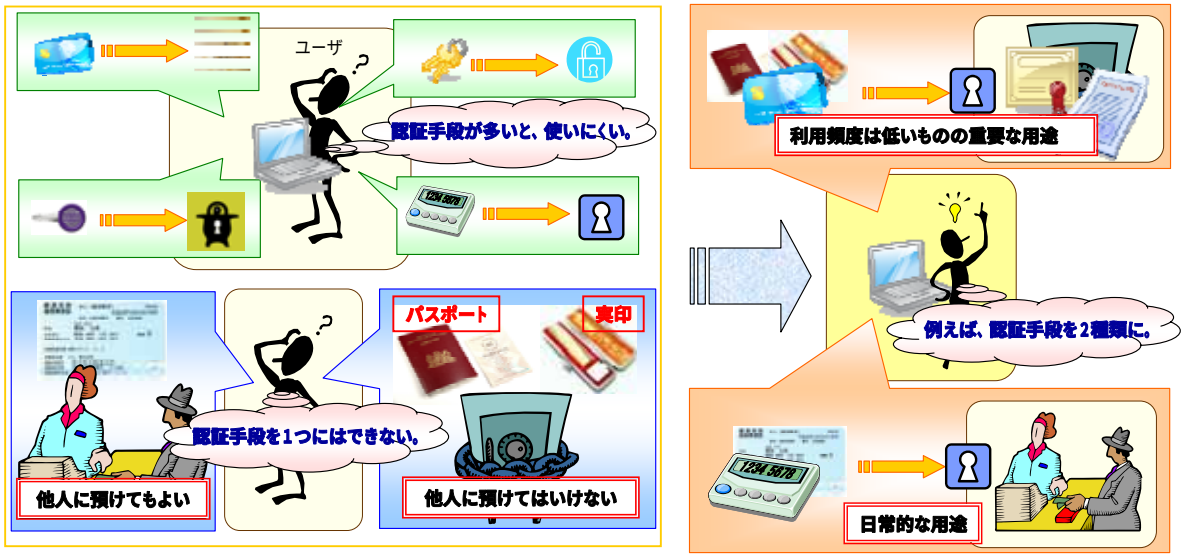


図 4.3 保証レベルに対する実装の考え方

4.3.2. 国民の負担感に対する配慮

現在の電子政府の認証方式における問題点や求められる要件にて繰り返し記載しているとおり、特別な周辺機器の購入やソフトウェア等の導入の強制は利便性の低下を招き、認証方式の普及の阻害要因となるため、できる限り強制しないことが望ましい。

---

18 保証レベルとは、電子署名・認証の各方式の強度の違いを示す抽象的な指標である。

また、高齢者や障害者等に配慮した認証方式の設計・構築を行い、適切な代替手段等を用意することが求められる。一方、国民に代わって行政手続を行う代行業（いわゆる士業）は、依頼人の個人情報を取り扱うことなどから有資格者（プロフェッショナル）と整理されており、資格確認をオンライン上で行う必要性があることから、電子政府の認証方式においても国民と同等以上のセキュリティ上の扱いが妥当であると考える。

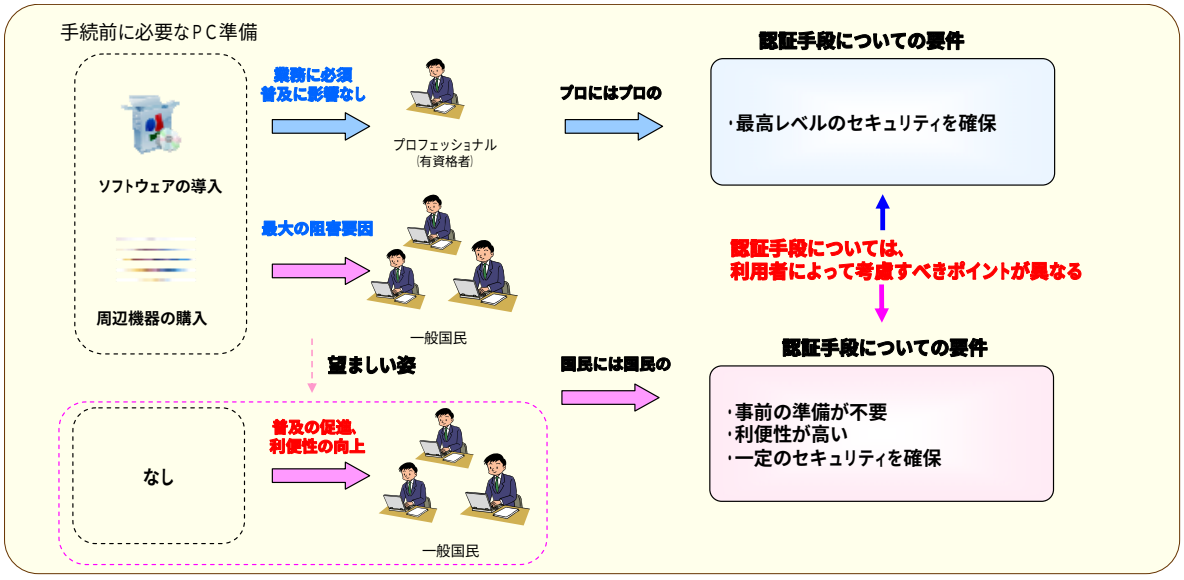


図 4.4 国民の負担感に対する配慮

4.3.3. 認証方式の合理的な選択

一般にセキュリティと利便性、コストは相互にトレードオフの関係にあるが、電子政府の現状や民間サービスにおける認証の動向から、利便性を追及しなければ利用者である国民には広く利用してもらえないのが現実であると言える。ついては、具体的な行政手続に関わる脅威に対するリスクの影響を導出し、それに対応する保証レベルを見極めることで、適切なセキュリティ確保と普及を妨げない利便性、経済性とを両立させることが重要である。

このセキュリティ確保の際には、万一、改ざんや事実否認などが発生し、係争となった場合に備えた自由心証主義の下での対応策も勘案する必要がある。

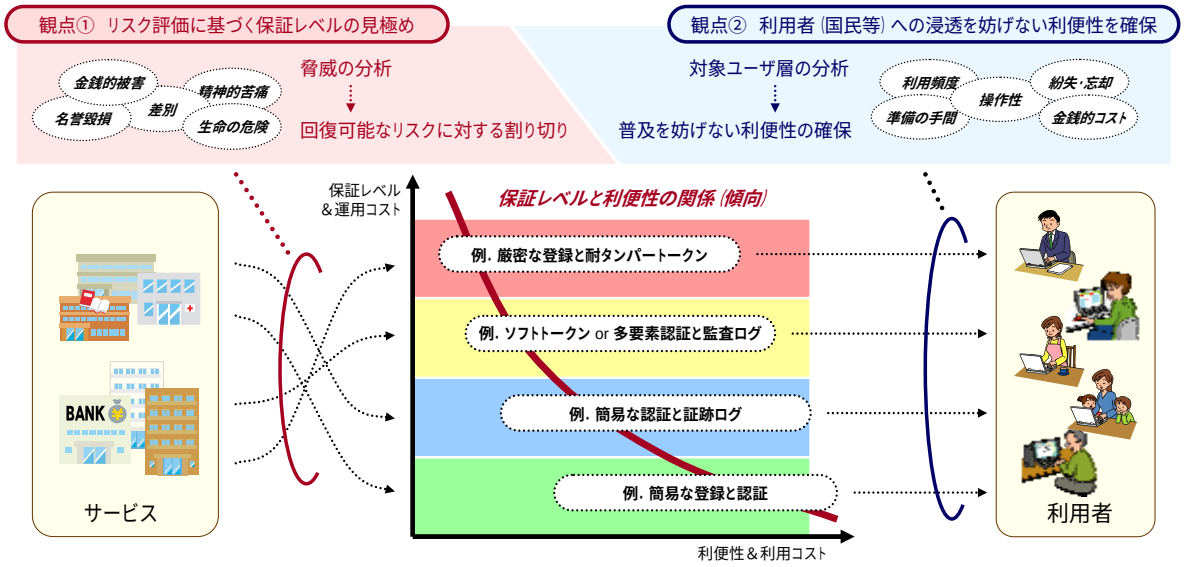


図 4.5 認証方式の合理的な選択

4.4. 電子政府における ID 管理と認証のための望ましい基盤

電子政府において認証方式の普及拡大を図り、基盤化するにあたっては、前述のシステム側の６つの視点と、利用者側の３つの視点を踏まえた要件への対応が必要であり、図 4.6 はこのことを示す概念図である。この双方の要件をともに満たす基盤の構築が、電子政府における ID 管理と認証において必要となっていると考える。

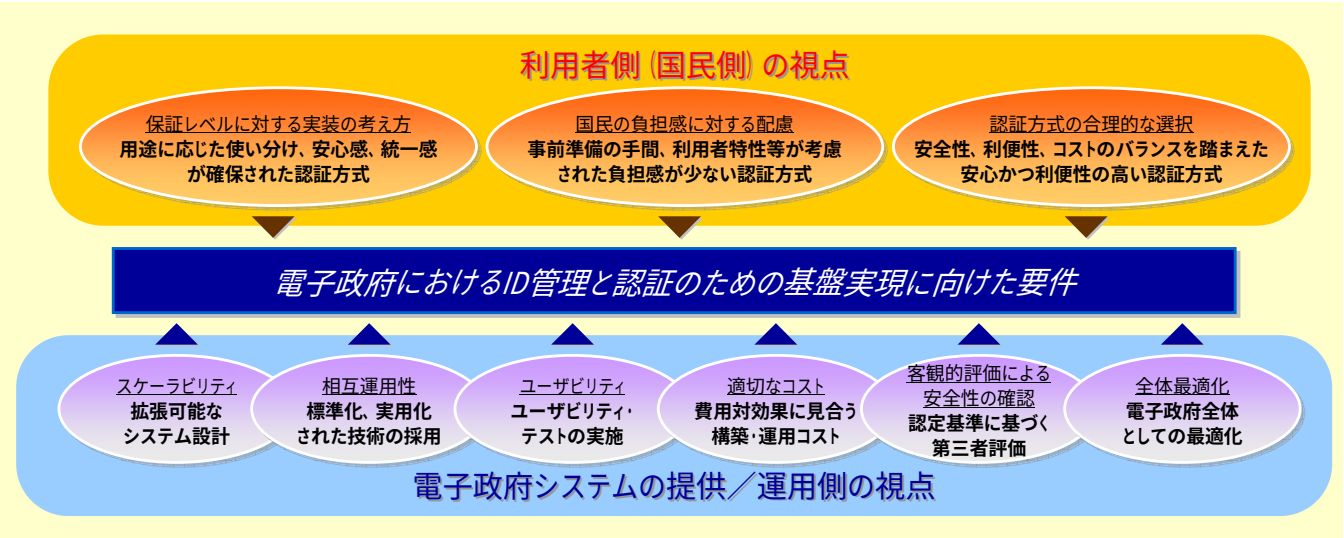


図 4.6 電子政府における認証方式の普及拡大と基盤化にあたり考慮が求められる要件

これらの要件を実現するにあたって考えられる ID 管理と認証の基盤を、具体的な形で示したものが、以下の図である。

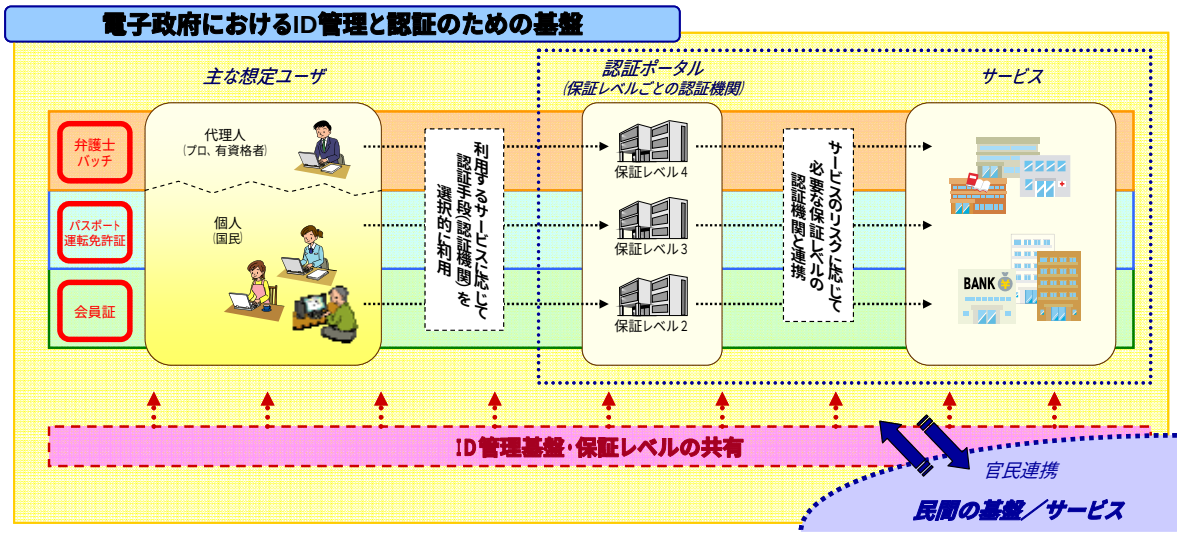


図 4.7 電子政府における ID 管理と認証のための基盤

認証の基盤を確立するためには、認証の対象となる利用者の身元確認のための情報管理、及び、認証の結果、特定される利用者をシステム上で一意に識別するための識別情報としての ID の体系が必要であり、これらの役割を包括的に担う基盤として ID 管理基盤の整備が求められる。

このように電子政府においては、より多くの利用者（国民等）に利用されるために、利便性と安全性、そして経済性の最適なバランスの上に立った ID 管理及び認証方式のための基盤を構築することが不可欠である。そのために、行政手続におけるリスクの影響度に応じた適切な保証レベルの認証方式を「必要十分」かつ「柔軟」に選択できるように認証基盤を構築していくことが求められる。

その一方で、利用者の負担を考慮すると、利用する認証方式はできるだけ少ない方がよいとの考えるのが自然である。しかしながら、窓口で他人に預ける可能性がある健康保険証とそうでない実印が存在することから、日常的に用いる認証方式と、利用頻度は低いものの重要な用途に用いるため大切に保管すべき認証方式を分ける方が妥当である。

また、利用者特性に対する配慮として、政府への申請手続を業とする者とほとんど行わない者の違い、他人の個人情報を取り扱う有資格者・代理人に係る資格確認の必要性について配慮して、認証方式を決定するべきである。

さらに、利便性向上の観点から、ID 管理基盤の導入や保証レベルの共有を目指す。これによって、行政サービスにおける業務効率向上や官民連携によるサービス範囲の拡大、認証方式の乱立防止を期待することができる。

第5章　ガイドラインの概要と活用方法

本章では、諸外国のガイドラインや国際標準における考え方をベースに、我が国の電子政府における認証方式の設計にあたり活用可能な「ものさし」を確立することを目的とした策定した「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」（以下、「ガイドライン」）について、その位置づけ、概要、活用方法を解説する。

5.1. ガイドラインの位置づけ

5.1.1. 対象

ガイドラインは、電子政府システムに対する確保策として電子署名や認証の適用を検討する場合に当該システムを企画する政府職員を想定読者としている。ガイドラインで対象としているオンライン手続は、「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であり、「オンライン利用拡大行動計画」で対象とされていないクローズな環境である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などは対象外としている。

5.1.2. 全体的な枠組み

電子政府のオンライン手続において、リスクに応じた適切な認証方式を選択し、必要となるシステム基盤を設計・構築するためには、まず、対象となるオンライン手続に関わる脅威を特定し、それに対するリスクの影響度を判断した上で、所要となる保証レベル（セキュリティ対策に関する尺度）を決定する必要がある。このための手法をまとめたものが、本ガイドラインである。

所要の保証レベルが決定された後には、それに対応する対策を選択するフェーズに移る。このフェーズにおいては、ガイドラインの付録にまとめた保証レベル毎の対策基準を参照し、前章でとりあげた全体最適化や利用者の利便性等について考慮した上で、最終的な対策を選択する（図 5.1、図 5.2）。

これらは業務・システムの最適化工程においては、いずれも企画段階で行う作業にあたり、シ

ステムのライフサイクルに合わせて妥当性検証を合わせて行うべき性格のものである（図 5.3）。

なお、認証結果をサービス側に提供するプロセスについては、SAML や OpenID 等として標準化が行われているため、本分科会ではそのためのガイドラインを策定しない。

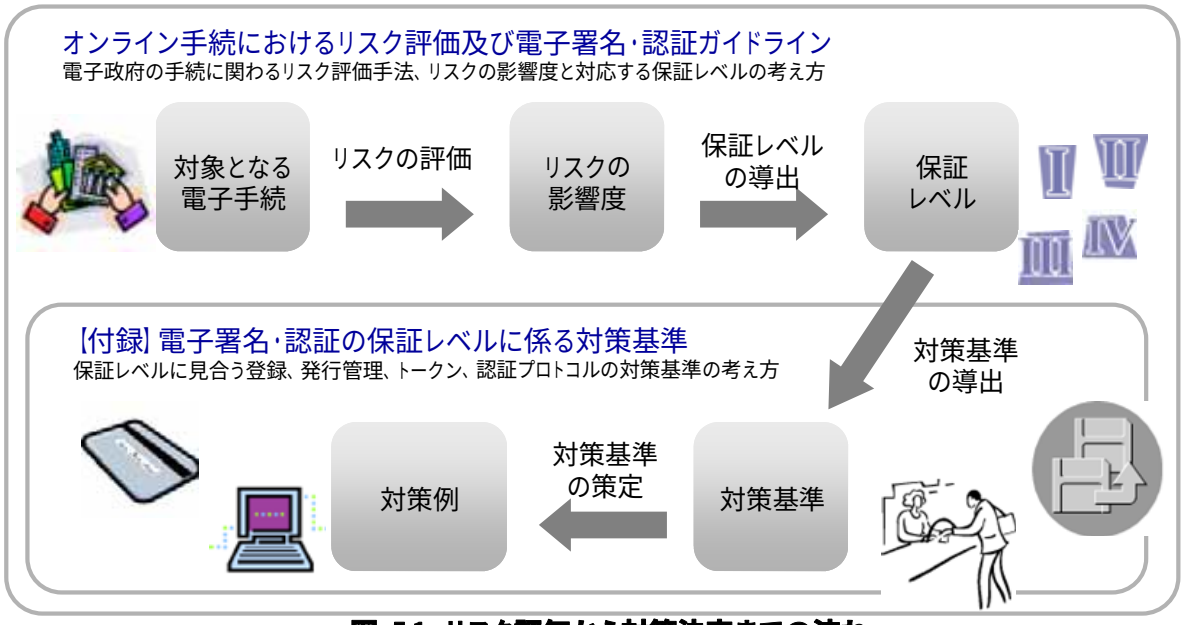


図 5.1 リスク評価から対策決定までの流れ

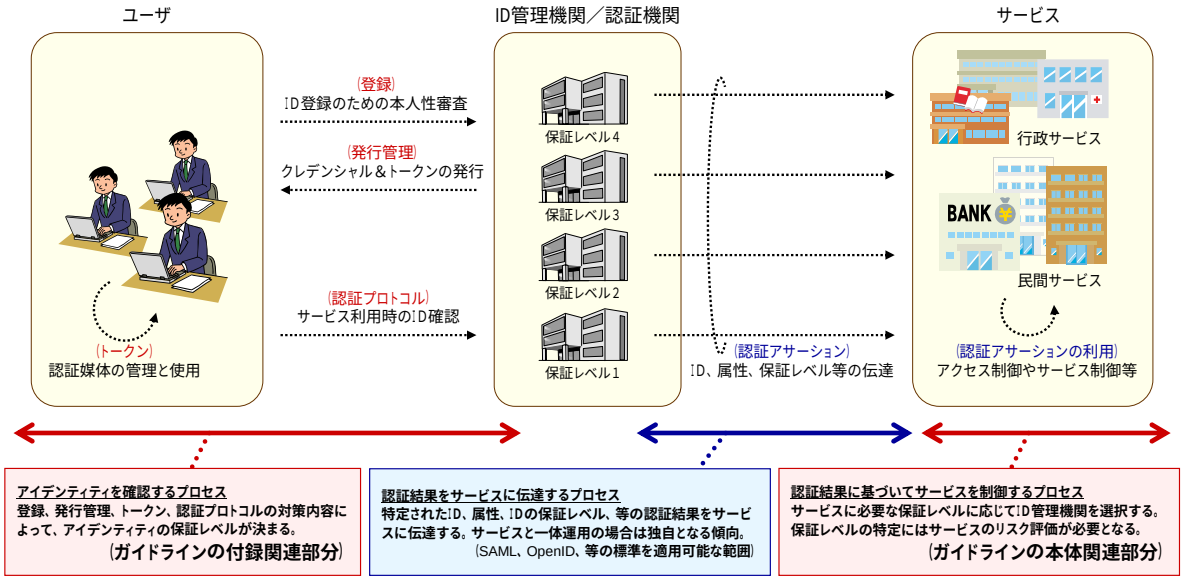


図 5.2 ガイドラインの役割

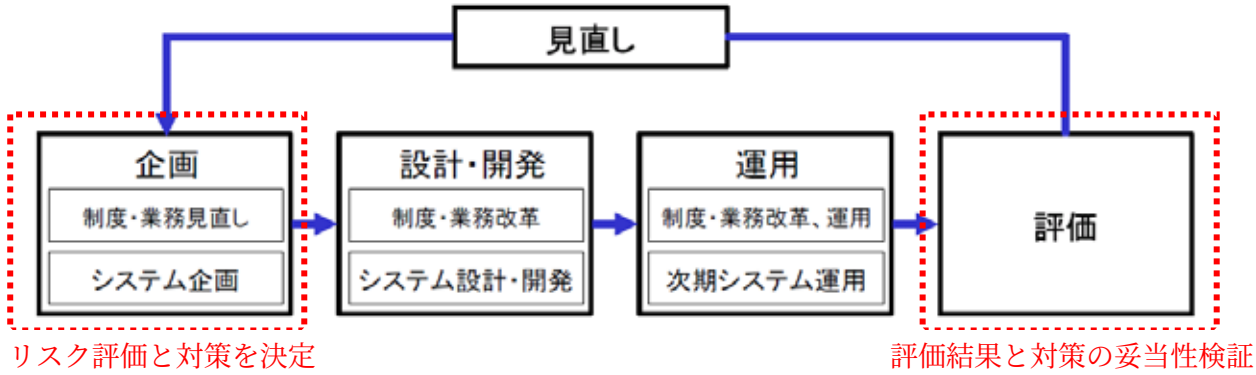


図 5.3 業務・システム最適化工程における位置づけ

5.2. ガイドラインを用いたリスク評価

本節では、ガイドラインの概要としてオンライン手続に関わる脅威、リスクの影響度の定義、リスクの種類、リスクの影響度を導出する手法を示した上で、リスクの影響度に関連付けられた保証レベルの導出までの手法を述べる。

5.2.1. リスク評価手法

本ガイドラインにおいては、米国政府で採用されている FIPS199「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」を参考とした「リスクの影響度」を、対象オンライン手続に関わる主たるリスクとして考えられる「金銭的被害」及び「機微情報の漏えい」の観点から評価する手法を提供する。

なお、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。

表 5.1 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）連邦情報処理規格（FIPS）199「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」より作成

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、考慮すべき全てのリスクを踏まえて行うことを踏まえつつ、総合的なリスク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 5.2 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）

なお、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「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。

5.2.2. リスク評価結果と保証レベル

保証レベルとは、電子署名・認証の各方式における認証情報が確かに本人に関連付けられていることの保証の度合いであり、本ガイドラインにおいては、国際標準機関や多くの海外電子政府で採用されている４段階の保証レベルを採用する（表 5.3）。

表 5.3 保証レベル

レベル	レベルの説明
レベル1（最低限の保証）	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（低い保証）	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（中程度の保証）	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（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

総合的なリスクの影響度と保証レベルの対応付けについては、リスクの影響度の高いものから高い保証レベルが必要とすることから表 5.4 のような対応付けとなる。

なお、ガイドラインの付録においては、保証レベルと対策基準との対応関係が示されるが、保証レベルをマッチングキーとして、ガイドライン本体と付録で示された対応関係を組み合わせて用いることとなる

表 5.4 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	
高	レベル3	
中	レベル2	
低	レベル1	

5.3. ガイドラインを用いた電子署名・認証の対策基準の選定

本節では、電子署名、認証の使い分けの考え方、及び、ガイドラインを用いた対策基準選定の概要について述べる。

5.3.1. 電子署名と認証の使い分け

オンライン手続のうち、書類の送信を伴う申請系サービスにおいては、なりすまし、改ざん、事実否認の大きく３つのリスクについて対策が求められる。この３つのリスクにすべて対応した技術が電子署名であるが、高度な保証レベルが求められる場合を除き、認証と SSL/TLS による回線暗号化、タイムスタンプ付与、証跡保存、及び、適切な運用体制との組み合わせにより、一定の効果が得られる（表 5.6）。このため、電子署名以外に、認証及び証跡保存等による対策も認められるが、これに関する対策基準は別途検討すべき課題とする。

一方、オンライン手続のうち、書類の送信を伴わない閲覧系サービスにおいては、なりすましが主要なリスクとなるため、対策としては保証レベルに応じた認証と監査のための証跡保存が要求される。

表 5.5 認証と電子署名による対策例の比較

	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

5.3.2. 電子署名・認証の対策基準の概要

ガイドライン付録にある電子署名・認証の保証レベルに係る対策基準は、国際標準化機関や各国で採用されている認証ガイドラインをベースに策定されたものである。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、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・署名等プロセス」）ごとに定めている。評価軸のうち、認証・署名等プロセス以外の 3 軸は共通であることから、これらについては共通の対策とする（図 5.4）。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。

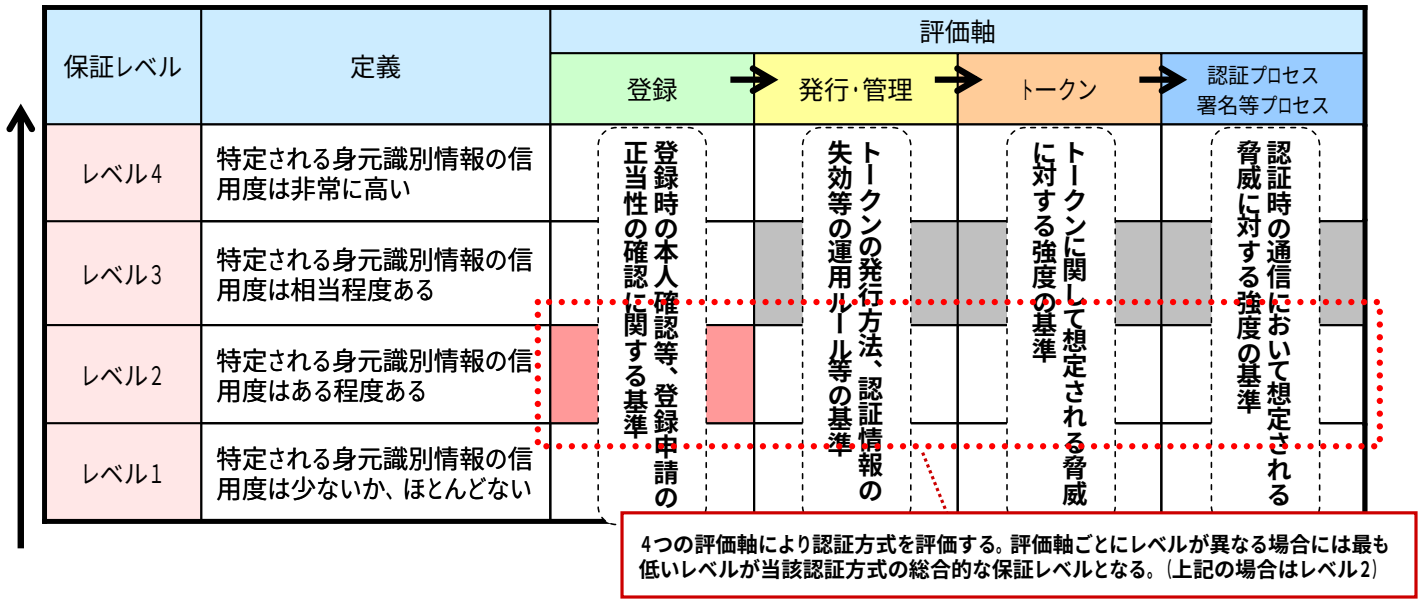


図 5.4 電子署名・認証の保証レベルの考え方

(1) 登録の保証レベル

対面の場合:

対策基準	保証レベル			
	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。		◎	◎	◎ (※1)
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。			◎	◎ (※2)
重複登録ではないことを確認する。				◎

※1　公的な写真つきの身分証明書を必須とする

※2　公的な台帳との照合を必須とする

遠隔 (郵送やオンライン等による登録申請) の場合:

対策基準	保証レベル			
	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) 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。			◎	

（2）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が通知され、本人が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手続及びその必要性等）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〕 ・ 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暗号通信路を介して行なう。 〔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

保証レベル	対策基準
	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とする。
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、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。

（3）トークンの保証レベル

対策基準	保証レベル			
	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。				◎

(4) 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	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			◎	◎

※「◎」の対策基準は各保証レベルへの準拠にあたり必須の基準、「△」の項目は準拠にあたり一部制約を設けて良い基準である。

(5) 署名等プロセスの保証レベル

対策基準	保証レベル			
	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。			◎	◎
「(3) 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。				◎
「(3) 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。				◎

※ 上記は、電子署名を用いる場合の対策基準である。

5.4. ガイドラインの活用方法

このガイドラインを使って認証方式を決定するプロセスを図 5.5 に示す。

「リスク評価を実施」、「保証レベルを導出」のプロセスにおいては、個別手続毎の保証レベル、対策基準の検討を行うが、最終的には「対策基準の選択」のプロセスにおいて、その他のリスク削減方策（インターネットと電話又は郵便などとの複数経路化等）の採用や、保証レベルが異なる複数の手続によって構成されるサービスの場合における利用者の利便性、サービス提供者側と利用者側を合わせたライフサイクルコストの観点等から見て、総合的に判断して対策を決定する

ことが望ましい。

求められる対策基準と遜色がないレベルや範囲において、代替手段を採用してもよい。上位レベルの対策基準を採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、セキュリティ上の理由のみでむやみに上位レベルの対策基準を採用するべきではなく、利用者の利便性やコスト等の観点からも検討することが適切である。なお、選択された対策やリスク評価について、各府省は、それらの適切さを確保するために情報セキュリティ対策推進会議等の場において専門的知見を有する者からの助言等を受け、決定するとともに、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、当該計画の改訂のタイミングとする。また、ユーザビリティガイドラインと同様に、電子政府評価委員会は、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、両ガイドライン自体も、技術やインフラの進展に合わせて、適時に見直されるべきである。

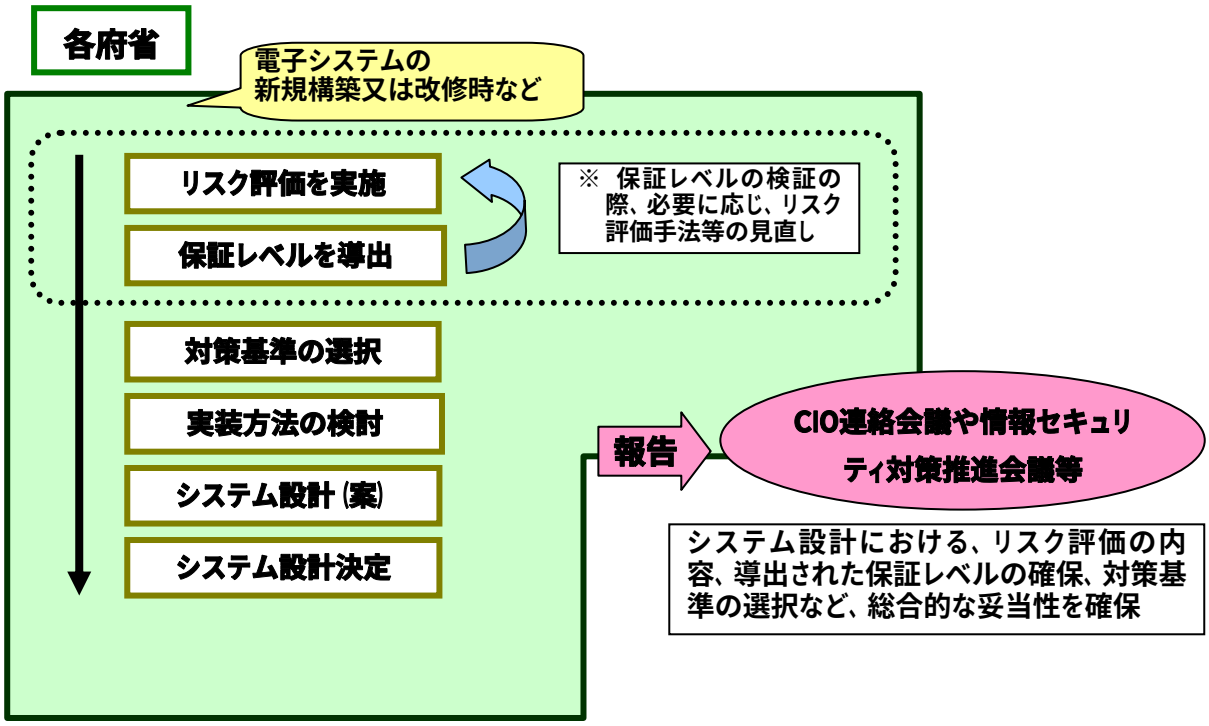


図 5.5 リスク評価に基づく認証方式に係る対策基準の選択等の実施フロー

第6章　今後の検討課題

本章では、本分科会における検討過程において明らかになった、次世代電子政府における認証方式の実現に向けた検討課題について述べる。

6.1. 技術的な課題

（1） 証跡管理

電子署名、認証のいずれを用いる場合においても、信頼性確保及びサービス品質向上の観点から、

① 適切な処理がされたことをサービス提供側、サービス利用者側の双方が確認でき、

② 利用者のプライバシーを保護した上で、サービス品質向上に寄与できるデータを取得

するための証跡管理が不可欠であるが、十分な学術的な検討がされているとはいえない状況にある。今後、関係機関において技術面、制度的からの検討を進め、次世代電子政府の検討に資するとともに、成果を今後のガイドライン改訂に反映することが望まれる。

（2） 認証方式間の連携

次世代電子政府においては、認証用途や複数の保証レベルに対応した官民の認証基盤間の連携が必要となることから、これらを実現するための仕組みとして、次世代電子政府における認証基盤間の相互接続を行うための技術／運用基準に係る検討の中で、保証レベルの技術的要件の担保方策や、X.509 電子証明書における key usage 等のプロファイル規定等を検討することが必要である。

6.2. 制度的な課題

（1）本人確認に関する横断的な制度設計

2003 年（平成 15 年）、CIO 連絡会議において決定された「電子政府構築計画」[19]のなかで IT 化に対応した業務改革が提唱され、業務・システムの最適化への取組が始まったものの、依然として我が国の制度は、情報通信技術の利活用を前提としたものとはなっておらず、本格的な EA（Enterprise Architecture）は取り組まれていないのが現状である。

このため、2009 年（平成 21 年）8 月から IT 戦略本部の下に「デジタル利活用のための重点点検専門調査会」が設置され、デジタル技術・情報の利活用を阻むような規制・制度・慣行、サービスの仕組みそのものの在り方や運用などを国民にとって利益となる形で抜本的に見直すための点検が行われているところである。

本人確認については、今回、ガイドラインによりオンライン手続におけるリスク評価手法及び対策基準を規定したところであるが、制度的には個別手続毎にそれぞれの機関がリスクと利便性を斟酌して判断している状況にあり、国民 ID や個人情報の取り扱いと合わせて、横断的な制度設計に着手することが望まれる。（例えばエストニアにおいては、個人情報保護法により、機密性に応じて個人情報を３段階に分類している。）

（２）代理人の扱い

紙申請の場合において、代理人が申請する場合の本人確認手法については、委任状により行っているが、オンライン手続における委任の確認手法について検討されることが必要である。家族による代理申請など、代理申請は頻繁に行われていることから、オンラインにおいても紙と同等な簡便さで代理申請ができるよう、委任されたことの確認が可能となるようなシステム設計をするべきである。

（３）認証の法的位置づけ

電子署名については、電子署名法によりその法的効力が規定されているものの、認証については、各主体のリスク判断により運用されているところである。今後、より信頼できるネットワーク社会の構築に向けた環境整備の一環として、「誰が」の保証について、どのような制度的裏付けが適切であるのか、関係者間による検討が望まれる。

（４）CC 認証の取得促進に向けた環境整備

IC カードのセキュリティ評価については、世界的に ISO/IEC15408（コモンクライテリア）に基づくセキュリティ評価・認証を取得することが、一般的である。このため、現在国内に IC カード等のシステム LSI のセキュリティ評価･認証体制の整備に向けた取組が行われてい

[19] 2003 年（平成 15 年）7 月 17 日、各府省情報化統括責任者（CIO）連絡会議決定、2004 年（平成 16 年）6 月 14 日一部改定

るところである。今後、このような取組がより一層促進されることが望まれる。

（5）術語

我が国の既存法令等においては「認証」が Certification(証明、検定)の意味で使われており、Authentication（認証）に充てる適切な術語がなく、認証方式に関する議論を難しくしている。このため、さらなる制度検討にあたっては、認証に関する分かりやすい術語について、検討することが望まれる。

6.3. 基盤整備に係る課題

（1） 電子政府における認証方式のための基盤整備

現在、電子政府の入口は e-Gov に集約されつつあるものの、各機関による ID・パスワードの払い出しなど、個別な取組が散見されており、利用者側から ID・パスワードの統一的運用が望まれているところである。このため、次世代電子政府の構築にあたっては、SSO（シングルサインオン）を組み込んだ形で、認証に係る利用者の負担が低減する方向での、認証機関間の連携体制を構築することが望まれる。

（2） ID 管理基盤の整備

次世代電子政府構想におけるバックオフィス連携や透明性の高い電子政府を実現するためには、ID 管理基盤の整備が不可欠である。我が国においては、デジタル社会に対する漠然とした不安感から国民的な懸念がなかなか払底できないところであるが、電子政府システム全体としてセキュリティやプライバシー対策と利便性とのバランスを考慮した形で検討し、国民的なコンセンサスを形成していくことが望まれる。

【付録1】 用語集

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	情報や通信の内容を第三者に知られることがないように、情報や通信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)	なんらかの意思を持ち、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	ある情報を改ざんされていないこと。
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。

用語	語義
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。
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

用語	語義
	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利用者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、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。

【付録2】 重点手続の再点検アンケートの内容

アンケート調査の概要

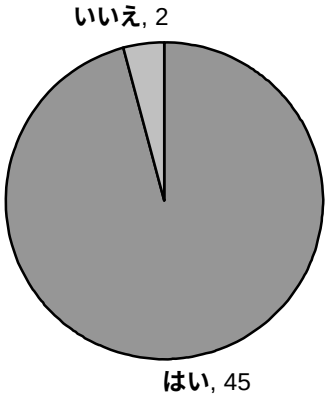
調査対象	47 手続の所管省庁に対して調査を依頼
調査方法	書面によるアンケート調査を実施し、必要に応じて内容補足のためのヒアリング調査等を実施
調査時期	平成 20 年 12 月上旬から平成 21 年 1 月中旬までの約 1 ヶ月間。
調査内容	紙手続での申請・届出の状況、オンライン申請の状況、その他手続全般に関する事項

調査項目の分類		調査項目の概要
1 紙		
	1-1 押印	･主に実印の要否とそれぞれの詳細。
	1-2 署名	･署名の要否、必要な場合の詳細。
	1-3 窓口申請	･窓口申請における本人確認の詳細。
	1-4 郵送申請	･郵送申請における利用している特殊取扱郵便の種類や本人確認方法。
	1-6 実在性確認	･外国人等を申請の対象にしている場合の本人確認方法等。
	1-7 否認防止対策･改ざん防止対策	･申請書等の提出書類の写しの取扱。
	1-8 申請書等の保管	･申請書の原本、添付書類の保管状況。
	1-10 代理申請	･申請者本人の意思の表示の状況、代理申請者の本人確認方法。
2 オンライン申請		
	2-1 ID･パスワード	･利用者への ID･パスワード発行における取得情報や本人通知方法等。
	2-2 申請書データの管理	･申請書データの管理に際し、識別コードの付与の状況等。
	2-3 本人性確認	･申請書等の作成者の本人確認方法。
	2-4 否認防止対策･改ざん防止対策	･電子署名以外の技術的な対策の実施状況。
	2-5 代理申請	･代理申請における申請者本人の電子署名が不要な理由。
	2-6 法令等の改正	･オンライン申請の導入やオンライン利用率拡大のための法令等の改正の状況。
	2-7 その他	･オンライン申請に係る上記以外の事項。
3 その他		**･上記以外の手続全般に関する事項**

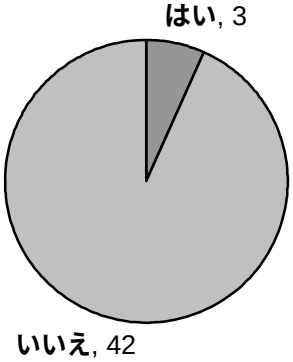
1－1　押印の状況（紙）

申請書等に、「押印」が必要な手続きは 47 件中 45 件と大半を占めているが、その中で「実印」が必要な手続きは 45 件中 3 件にとどまった。また申請書等の真正性を確かめる手続きを行っているのは 42 件中 36 件と多く見られた。

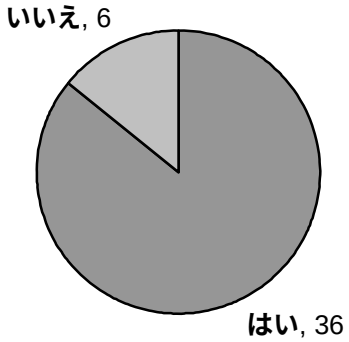
No. 1-1-1 申請書等に、「押印」は必要ですか？
(N=47)



No. 1-1-2「実印」である必要がありますか？
※実印は印鑑登録されているものとします
(N=45)



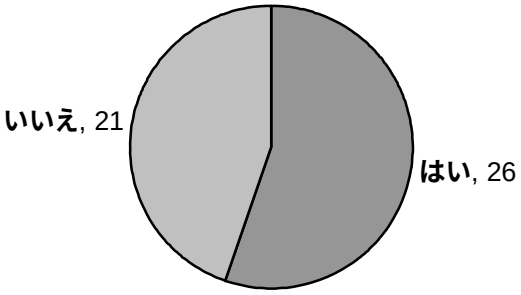
No. 1-1-11 申請書等の真正性を確保するための措置を取っていますか？
(N=42)



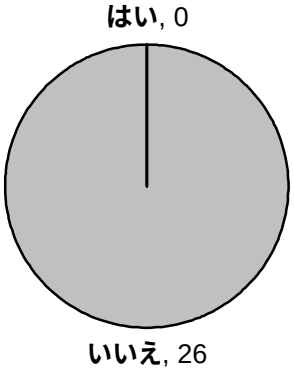
1－2　署名の状況（紙）

申請書等に、「署名」が必要な手続きは 47 件中 26 件と過半にのぼるが、そのうち署名証明書の添付が必要な手続きは 0 件であった。

No. 1-2-1 申請書等に、「署名」が必要ですか？
(N=47)



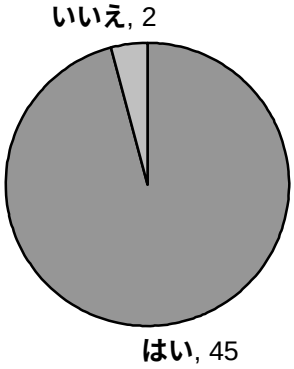
No. 1-2-2 署名証明書の添付を求めていますか？
(N=26)



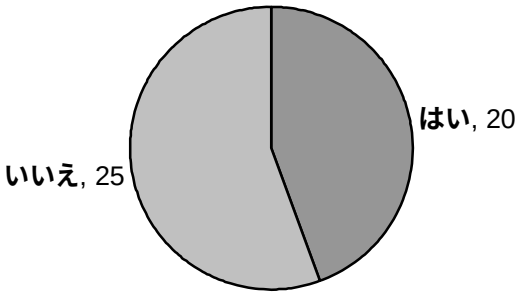
1－3　窓口申請の状況（紙）

窓口で申請番号を受領する手続きは、47 件中 45 件と大半を占めたが、そのうち、申請者本人が来訪した場合に申請書の作成者と同一であることを確認する手続きは 20 件と半分以下にとどまった。また来訪時の本人確認方法が法令で定められる手続きは 20 件中 3 件にとどまり、本人確認の際に自動車免許書等の身分証明書の提示を求めている手続きは 0 件であった。

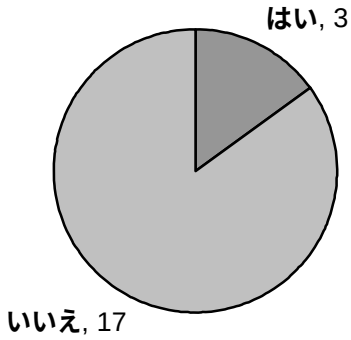
No. 1-3-1 窓口で申請番号を受領する手続きですか？
(N=47)



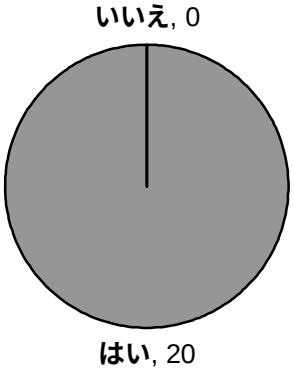
No. 1-3-2 申請者本人が来訪した場合、申請書の作成者と同一であることを確認していますか？
(N=45)



No. 1-3-3 申請者本人が来訪した場合における、本人確認方法は法令等で定められていますか？
(N=20)



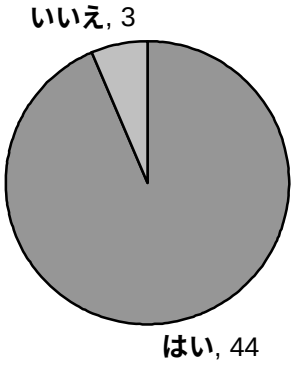
No. 1-3-5 本人確認の際に、自動車免許証等の身分証明書の提示やその写しの提出を求めているか？
(N=20)



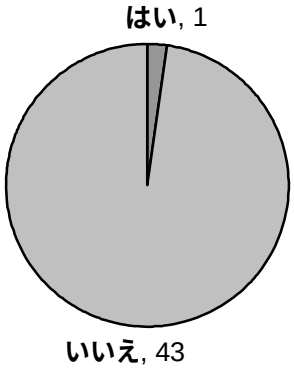
1－4　郵送申請の状況（紙）

郵送で申請書等を受領する手続きは 47 件中 44 件にのぼったが、そのうち内容証明郵便等、郵便法で定められている特殊取扱を利用している手続きは 1 件にとどまった。また郵便申請において申請者の本人確認を行っている手続きは半分程度であった。

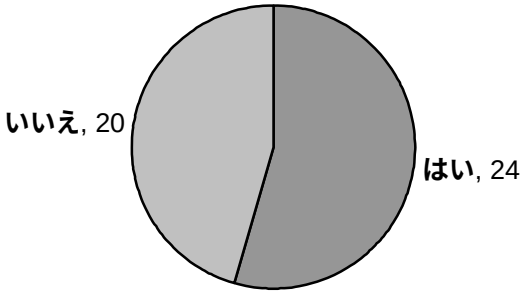
No. 1-4-1 郵送で申請書等を受領する手続ですか？
(N=47)



No. 1-4-2 内容証明郵便等、郵便法で定められている特殊取扱を利用していますか？
(N=44)



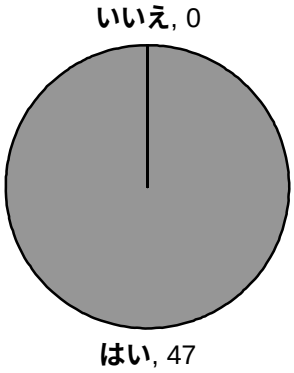
No. 1-4-4 郵送申請における申請者（申請書の作成者）の本人確認を行っていますか？
(N=44)



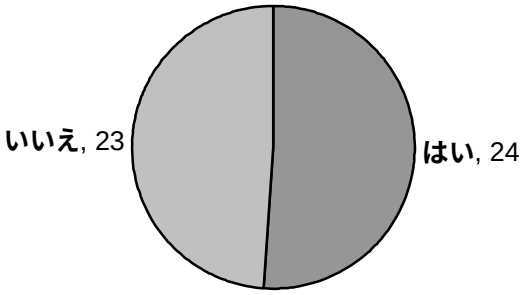
1－6　実在性確認の状況（紙）

申請者に外国人や在留邦人が含まれる手続きは、47 件中 47 件全てが該当した。本人確認のための書類の提示を求める手続き、本人確認のための基礎データと突合を行う手続きはそれぞれ半数程度であった。

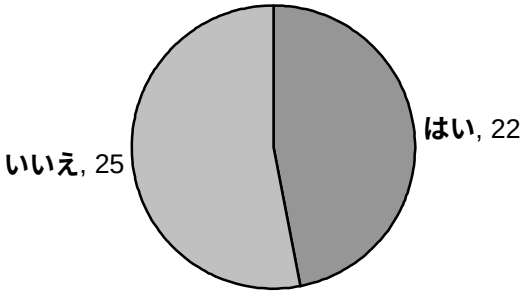
No. 1-6-1 申請者には外国人や在留邦人が含まれていますか？
(N=47)



No. 1-6-2 本人確認のために書類の提示等を求めていますか？
(N=47)



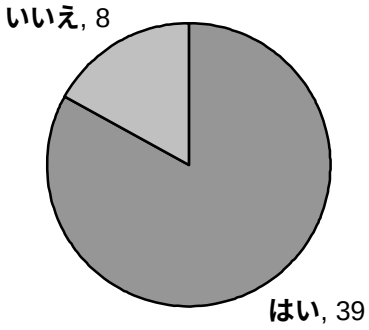
No. 1-6-4 本人確認のために、基礎的なデータとの突合を行っていますか？
(N=47)



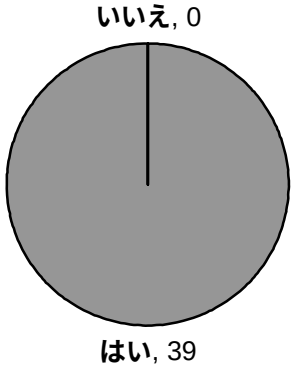
1－7　否認防止対策･改ざん防止対策の状況（紙）

申請書等の提出書類の写しを申請者に渡している手続きは、47 件中 39 件にのぼり、多くの手続きで行われている。しかしその中で提出書類の写しに受領印をつけて渡す手続きは 0 件であった。

No. 1-7-1 申請書等の提出書類の写しを申請者に渡していますか？
※雇用保険被保険者資格取得確認通知書（事業主通知用）、雇用保険被保険者資格取得確認通知書（被保険者通知用）、雇用保険被保険者証を渡している
(N=47)



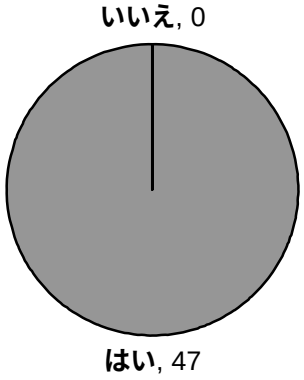
No. 1-7-3 提出書類の写しには受領印をつけて渡していますか？
(N=39)



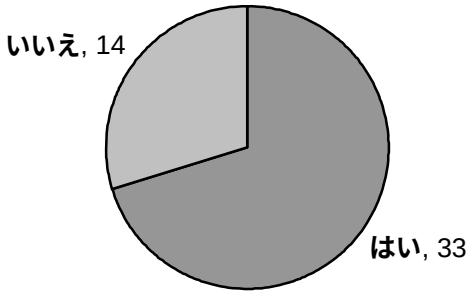
1－8　申請書等の保管の状況（紙）

申請書等の原本を保管している手続きは 47 件中 47 件全てであったが、申請書に添付される書類を保管している手続きは 33 件であった。

No. 1-8-1 申請書等の原本を保管していますか？
(N=47)



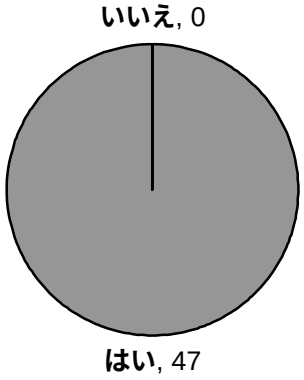
No. 1-8-4 申請書に添付される書類を保管していますか？
(N=47)



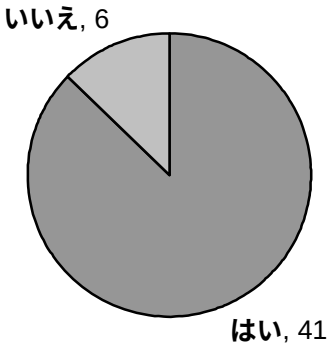
1－10　代理申請の状況（紙）

士業等による代理申請を認めている手続きは、47 件中 47 件全てであった。その中で、申請者本人の署名もしくは実印が必要となる手続きは 41 件と大半を占めたが、申請者の委任状を求める手続きは 25 件と半数程度であった。

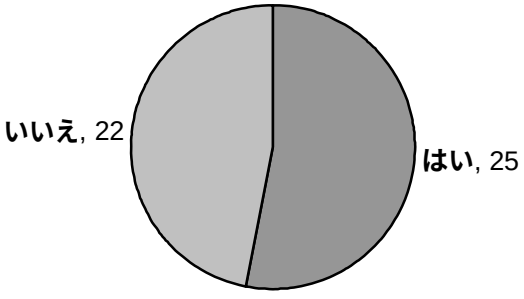
No. 1-10-1 士業等による代理申請を認めていますか？
(N=47)



No. 1-10-2 申請者本人の署名もしくは実印を必要としていますか？
(N=47)



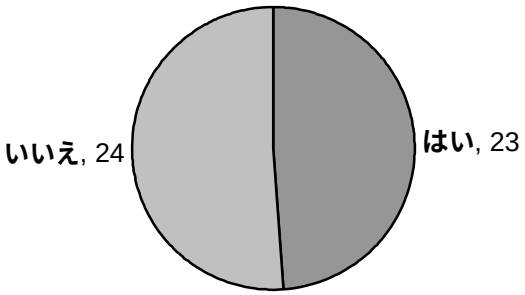
No. 1-10-4 申請者の委任状の提出を求めていますか？
(N=47)



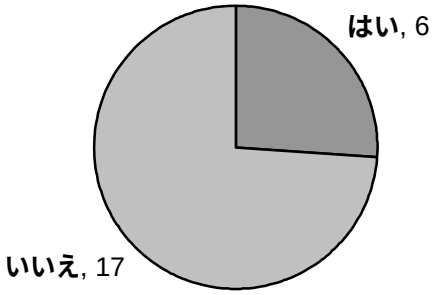
2－1　ID･パスワード（オンライン）

オンライン手続きにおいて、利用者に ID･パスワードを発行している手続きは 47 件中 23 件と半数程度であった。その中で ID･パスワードを発行する際に、本人に確実に ID･パスワードを渡す措置を取っている手続きは 6 件にとどまった。

No. 2-1-1 利用者にID･パスワードを発行していますか？
(N=47)

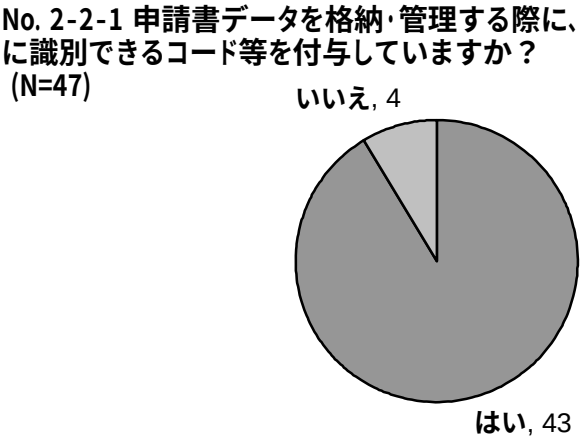


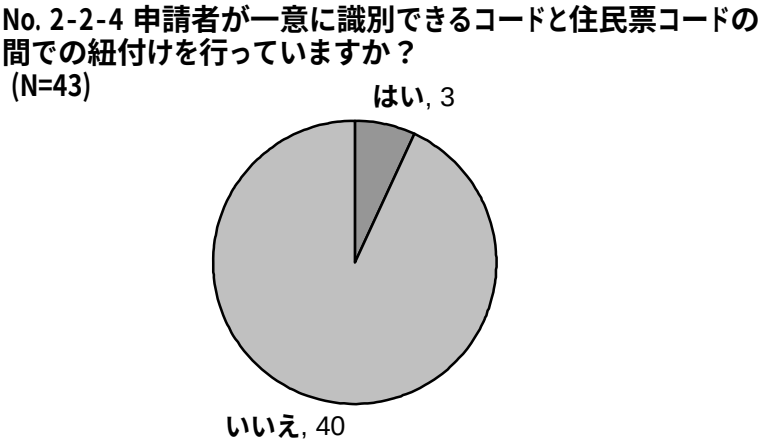
No. 2-1-3 ID･パスワードを発行する際に、本人に確実に渡すための措置を取っていますか？
(N=23)



2－2　申請書データの管理（オンライン）

申請書データを格納･管理する際に、申請者が一意に識別できるコード等を付与している手続きは 47 件中 43 件と大半を占めた。しかし、そのうち申請者が一意に識別できるコードと住民票コードの紐付けを行っている手続きは 3 件にとどまった。

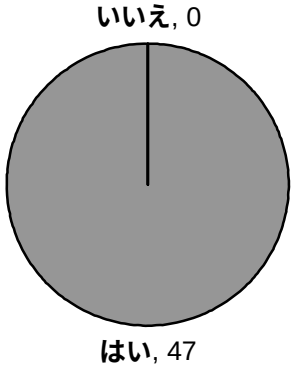




2－3　本人性確認の状況（オンライン）

申請書等の作成者の本人確認を行っている手続きは 47 件中 47 件全てであった。

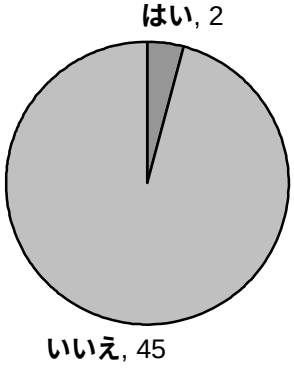
No. 2-3-1 申請書等の作成者の本人確認を行っていますか？
(N=47)



2－4　否認防止対策･改ざん防止対策の状況（オンライン）

否認防止対策･改ざん防止対策を目的として、電子署名の他に技術的な対策をとっている手続きは 47 件中 2 件にとどまった。

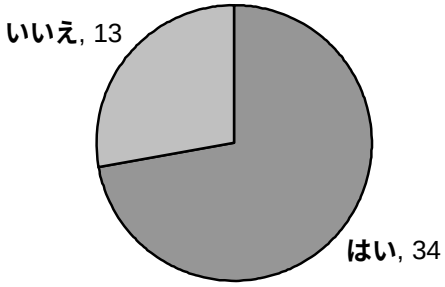
No. 2-4-1 否認防止対策･改ざん防止対策を目的として、電子署名の他に、電子署名以外の技術的な対策を取っていますか？
(N=47)



2－5 代理申請の状況（オンライン）

代理申請において申請者本人の電子署名を不要としている手続きは、47 件中 34 件と過半である。

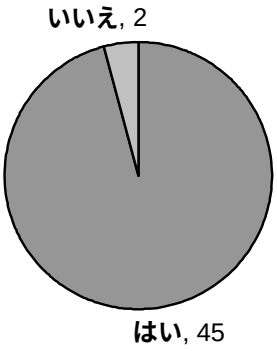
No. 2-5-1 代理申請において申請者本人の電子署名を不要としていますか？
(N=47)



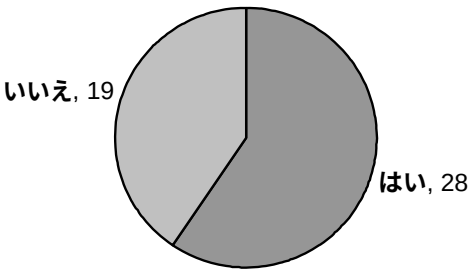
2－6 法令等の改正の状況（オンライン）

オンライン申請の導入に伴い、法令等の改正を行った手続きは 47 件中 45 件と大半を占めた。またオンライン申請の利用率の拡大のために、法令等の改正を行った手続きは 47 件中 28 件であった。

No. 2-6-1 オンライン申請の導入に伴い、法令等の改正を行いましたか？
(N=47)



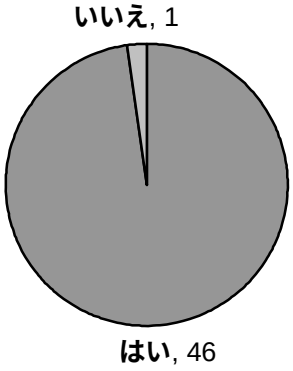
No. 2-6-3 オンライン申請の利用率の拡大のために、法令等の改正を行いましたか？
(N=47)



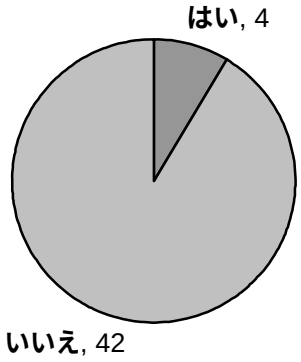
2－7　その他（オンライン）

オンライン申請と紙の申請を併用している手続きは 47 件中 46 件と大半を占めた。また、そのうち将来的に紙による申請をやめることが可能と回答があった手続きは 2 件にとどまった。

No. 2-7-1 紙による申請と併用していますか？
(N=47)



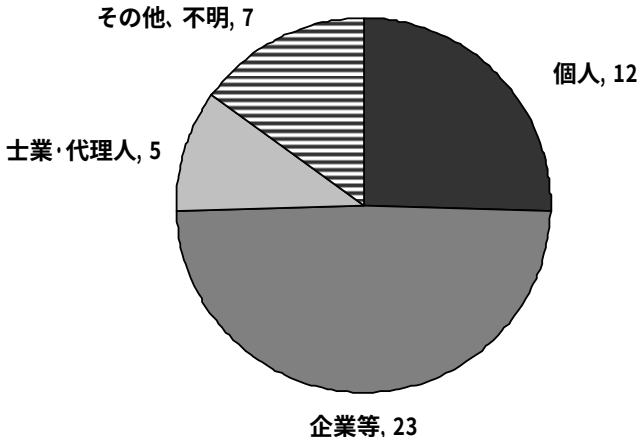
No. 2-7-2 紙による申請を将来的にやめることは可能ですか？
(N=46)



3 その他

手続きの申請者の属性を、「個人」、「企業等」、「士業・代理人」の3つに分類した場合に、「個人」が主な申請者となっている手続きは 47 件中 12 件にとどまった。また、約半数が「企業等」が主な申請者となっている手続きであった。

No.3-1 申請者の属性を、「個人」「企業等」「士業・代理人」の3つに分類した場合に最も多いものはどれですか？（N=47）



次に、利用者が手続きを利用する頻度についてみると、利用頻度が1年に1回以下（「一生に1回」と「数年に1回」と「1年に1回」を合計した値）となっている手続きは 47 件中 22 件と全体の半数近くを占めた。

No.3-2 利用者が当該手続を利用する頻度を記載ください。（N=47）