地方公共団体による公的個人認証サービス制度の創設について

「地方公共団体による公的個人認証サービスのあり方検討委員会」

報 告 書

平成１４年２月２８日

【目　　次】

第Ⅰ編　公的個人認証サービス制度創設の背景と必要性

第１章　背　景

Ⅰ－１－１　社会経済のネットワーク化の進展と新たな生活空間の出現

インターネット等の情報通信ネットワークの爆発的な普及に伴い、社会経済のあらゆる分野でネットワーク化が進展し、地理的、時間的な制約を超えた新たな生活空間である仮想空間（サイバースペース：cyber space）が出現してきており、この新たな生活空間が物理的現実世界と深く交差、融合するデジタル社会の時代が到来している。

例えば、経済分野では、インターネットを利用した企業間での電子商取引やインターネットバンキング、ネットオークション、モバイルインターネットを利用したコンテンツ配信等の企業－個人間の取引も行われている。

国民生活においても、携帯電話等を利用したメール交換、ＢＢＳ（電子掲示板）等のデジタルコミュニティが日常生活の不可欠な一部となってきている。

Ⅰ－１－２　行政手続の申請・届出等のオンライン化の推進（参考１）

経済、国民生活の分野だけでなく、行政分野でも社会経済のネットワーク化の進展によるデジタル社会の時代の到来は現実のものとなりつつある。

我が国は、電子政府を実現し、電子自治体の構築を推進するため、従来から、国及び地方公共団体の機関が扱う申請・届出等手続のオンライン化を積極的に推進してきており、電子政府・電子自治体の実現は、国民の利便性を飛躍的に向上させるとともに、行政の簡素・効率化、透明化をもたらすものと期待されている。

平成６年１２月の『行政情報化推進基本計画』（閣議決定）においては、「国民等の間の様々な行政手続等について、申請、届出等の電子化・オンライン化を業務内容に即して推進」することとされた。

その後のインターネットの急速な普及、行政の情報化を取り巻く環境の変化を踏まえ、平成９年１２月に改定された同計画では、申請・届出等手続の

電子化について、「原則として、平成 10 年度末までに可能なものから早期に電子化を行う」こととされた。

この結果、特許に関する手続等一部の手続については既にオンライン化が実現されているところである。

さらに、各行政機関が一体となって申請・届出等手続きの電子化を一層推進するため、平成１２年５月、『申請・届出等手続の電子化の推進のための基本的枠組み』が高度情報通信社会推進本部に報告され、①国民と行政との間の手続を原則として平成１５年度までに、書面による手続に加え、インターネット等を利用した手続のオンライン化を図る、②平成１５年度までの具体的なオンライン化のタイムスケジュールを示した各省庁ごとのアクションプランを策定することとなった。

これを受けて、各省庁ごとの『申請・届出等手続のオンライン化に係るアクション・プラン』がとりまとめられ、平成１２年９月にＩＴ戦略会議・情報通信技術戦略本部に報告され、約１万件の国事務に係る手続について平成１５年度までにオンライン化に取り組むこととなった。

さらに、平成１３年１月に施行された高度情報通信ネットワーク社会形成基本法（平成十二年十二月六日法律第百四十四号）に基づき、同月、高度情報通信ネットワーク社会推進戦略本部（ＩＴ戦略本部）が設置され、同本部において、『ｅ－Ｊａｐａｎ重点計画』が平成１３年３月に策定され、「国民等と行政の間の実質的にすべての申請・届出等手続を、２００３年度までのできる限り早期にインターネット等で行えるように」し、「各府省は、各個別手続のオンライン化実施時期を前倒し、簡素化等手続そのものの抜本的な見直し及び事務処理の電子化という観点から、既存のアクションプランを見直し、新たなアクションプランを２００１年度早期に策定する」こととなった。

これを受けて、国の事務についてはオンライン化の実施時期の前倒し等の見直しを行い、また、地方公共団体を相手とする手続のオンライン化の実施も新たに対象とした『申請・届出等手続のオンライン化に係る新アクション・プラン』が策定され、平成１３年６月、ＩＴ戦略本部に報告された。

同プランにおいては、国の行政機関が扱う申請・届出等手続のうち、全体の９８％に当たる約１０，９００件を、地方公共団体が扱う申請・届出等手続については、全体の９５％に当たる約４，９００件をオンライン化することが示されている。

主な行政手続としては、次のようなものが想定されている（参考２）。

①国関係

国税申告・納税、各種社会保険（健康保険、厚生年金保険、国民年金、労働保険）関係手続、自動車保有関係手続（検査・登録、車庫証明、納税等）

②地方公共団体関係

戸籍謄抄本の交付請求、戸籍関係手続（届出等）、住民票の写しの交付請求、旅券交付関係手続請求、地方税申告等、国民年金関係手続、建築確認申請、大規模小売店舗新設に係る住民からの意見の提出等

Ⅰ－１－３　デジタル社会における課題（参考３）

インターネット等のコンピュータとネットワークからなるサイバースペースは、相手方や送信された情報内容等の真偽を判別し難い空間であり、行政手続のオンライン申請、電子商取引をはじめとするネットワーク上の諸活動に当たっては、次のような課題の存在が指摘されている。

①成りすまし

ネットワークの向こうにいる人の顔は見えず、相手が本当に名乗っているとおりの本人かどうかは実感として捉えることができないため、発信者が本当に本人であるかどうか確認することが難しい。

例えば、手続を進めるに際して、電子メールアドレスやデジタル文書に記してある名義のみを信頼することで足りるかという問題がある。一般に、電子メールアドレスは、＠の前の利用者の名前と＠の後のドメイン名（組織名等）で構成される。suzuki@jichiseisaku.co.jpという電子メールアドレスで、自治政策株式会社鈴木という名義で文書が送られてきたとしても、その実在性を確認するとともに、第三者が勝手に電子メールアドレス等を取得して成りすましていないことを完全に否定することは困難である。自治政策株式会社が存在するのか、会社は存在していても鈴木という人は存在しているのか、明確でない。さらには、第三者が鈴木さんの電子メールアドレスを勝手に使っている可能性もある。

このようにネットワークを利用する場合にはなりすましの危険が大きいうえに、特に、申請・届出等を受ける行政機関側とすれば、多くの住民からのアクセスを受け付けることになるので、容易に成りすましでないことの確認ができなければならない。

②改変

デジタル文書は、手書きの文書と異なり、本物と全く同じコピーが可能であり、改変されても痕跡が残らない。このため、デジタル文書における改変箇所を発見することは、実際上不可能とされている。文書に付された名義の信頼性とともに、文書内容そのものの信頼性についても疑問が残らざるを得ないのである。

③送信否認

オンラインで送信されてきた申請･届出等に基づいて、手続を進行させたところ、本人からそのような送信はしていないと否認されるおそれがある。確かに本人が送信したことを容易に確認できることが求められる。

Ｉ－１－４　電子署名の必要性（参考４）

「Ｉ－１－３」の課題を解決するため、デジタル文書については、作成者の特定（本人により作成されたものであることの確認、送信否認の防止）や送信文書がその途中で改変されていないことを確認することが必要となる。

（１）ＩＤ・パスワードの限界

「Ｉ－１－３」の課題のうち、特に、成りすまし防止・送信否認に関して、ＩＤとパスワードで対応すればよいという考えもある。

確かに、利用者に対してＩＤを配布し、それに対応するパスワードを入力させるという方法は、コンピュータへのアクセス方法として一般的である。しかし、パスワードを他人に知られると成りすまされてしまう。しかも、パスワードは、一般的に短く、類推可能なうえに、盗まれやすいといわれている。さらに、利用者側としても、行政手続や取引ごとにＩＤを付され、それごとにパスワードを与えられるとすれば、そのパスワード管理だけでも大変である。

（２）電子署名

このような問題を解決し、ネットワーク上での安全な諸活動を確保するための技術が、高度な暗号技術を用いた電子署名の仕組みであり、中でも、非対称鍵暗号方式（公開鍵暗号方式）に基づく電子署名（デジタ

ル署名という。）が現在、広く利用されている。

非対称鍵暗号は、秘密鍵と公開鍵という一対の鍵（数値）を利用した暗号である。各個人は、秘密鍵と公開鍵のペアを生成し、秘密鍵は本人だけが秘密として厳格に保管してデジタル署名に使い、通信の相手方は公開鍵を用いて、本人のデジタル署名が真正なものであることを検証することとなる。

具体的には（パソコン上で自動的に処理されるものであるが）デジタル文書（１と０の系列）として存在する申請書本文（平文）にハッシュ（hash）という操作を加えて短い文書（メッセージダイジェスト）に圧縮する。このメッセージダイジェストと秘密鍵とを特定のアルゴリズム（algorithm：計算方法）に入力することで、デジタル署名を行う（平文の暗号化＝署名文）。署名文を受け取った相手方は、本人の公開鍵と署名文をアルゴリズムに入力し、元のメッセージダイジェストを求める（署名文の復号文）。さらに、署名文とともに送信されてきた平文をハッシュ関数に入力し、メッセージダイジェストを得て、これを復号文と比較し、同じであれば、通信途上で改変も置き換えもなされていないことが確認できる。

また、本人のものと確認できる公開鍵で復号できたことは、当該公開鍵と一対一対応関係にあり、本人のみが厳格に管理している秘密鍵で暗号化したものであることが確認できる（本人性の確認と送信否認防止）。

（３）個人認証サービス

デジタル署名を用いる場合、当該デジタル署名が行われた情報（申請書等）を受け取った相手方は、本人等から入手した公開鍵を用いて検証することとなるが、その公開鍵が本人のものであることを確認する必要がある。

このことを保証するのが、個人認証サービスであり、このサービスを提供する主体（認証局：Certification Authority）は、デジタル署名を利用する者に対して、公開鍵が本人のものであることを証明する電子証明書（digital certificates）を発行することにより行われる。

（注）電子証明書と印鑑登録証明書の類似点・相違点については、参考５を参照。

第２章　公的個人認証サービス制度の必要性（参考６）

Ⅰ－２－１　地方公共団体による公的個人認証サービス制度の必要性

（１）行政手続のオンライン申請等の手続保障に資する個人認証サービスの必要

「Ⅰ－１－２」のように、我が国は、電子政府・電子自治体の構築を推進するため、従来から積極的に、国及び地方公共団体の機関が扱う申請・届出等手続のオンライン化を推進してきているところであり、これを実現するためには、「Ⅰ－１－３」のデジタル社会における課題（成りすまし、改変、送信否認）を解決する方法として、個人認証サービスの提供が不可欠である。

ＩＴ戦略本部が、平成１３年３月に策定した『ｅ－Japan 重点計画』においては、「地方公共団体における組織認証基盤や個人認証基盤の整備を支援するとともに、申請・届出等の受付、結果通知等について、複数の手続に汎用的に利用できる汎用システムの基本仕様を２００１年度中に策定する。」とされており、これを受けて、同じくＩＴ戦略本部が、平成１３年６月に策定した『ｅ－Japan2002 プログラム』においては、「平成１５年度までに、電子政府を実現し、電子自治体の構築を推進することとされているが、そのためには、必要な基盤整備を平成１４年度中に進める必要がある。このため、申請・届出等の電子化に必要とされる地方公共団体による公的個人認証サービス等のシステムの整備等の基盤整備を着実に推進する」こととされているところである。

国及び地方公共団体の行政手続のオンライン申請・届出等の手続保障を、広く全国の住民に対して実質的に確保するためには、オンライン申請等に必要な高度な個人認証サービスを地理的条件等による格差が生じることなく、低廉な費用で提供することが必要である。

そこで、市町村が本人確認業務を、都道府県が証明書発行業務等をそれぞれ連携して担当することにより、全国サービスを低廉な費用で提供する制度（地方公共団体による公的個人認証サービス制度）を創設することが求められている。

（２）民間認証事業者が行う特定認証業務の本人確認への活用

インターネットの急速な普及に伴い、電子商取引をはじめ、様々な分

野における活動が急速にネットワーク上で行われるようになりつつあり、インターネットを利用した電子商取引等の一層の発展・活性化に向けて、その課題である成りすまし、改変、送信否認を解決する方法の提供が求められている。

このため、「電子署名及び認証業務に関する法律（平成十二年五月三十一日法律第百二号）」（以下「電子署名法」という。）が制定され、電子署名に一定の法律効果を付与するとともに、特定認証業務について認定制度の導入等が図られたところである。

（注）特定認証業務

一定の技術的信頼性を有する電子署名（鍵長が１０２４ビット以上のＲＳＡ方式によるデジタル署名等）について行われる本人確認業務（電子署名法第２条第３項参照）

さらに、民間認証事業者においては、特定認証業務の実施とともに、会社等の役員や従業員等に係る権限を証明したり、本人の資格等の属性を認証する業務の提供が行われ始めている。

例えば、インターネットバンキングの取引や電子商取引の決済のために、銀行、証券会社等の金融機関やクレジットカード会社が認証局を構築して、その顧客に対して電子証明書を発行する例があらわれてきているほか、会社や資格者の団体が、認証局を構築して、会社の従業員や資格者に電子証明書を発行していくことが想定される。

民間認証事業者が電子証明書を発行する場合、特定認証業務に係る本人確認には、対面審査や本人確認に必要な書類等の提出等の厳格な手続が期待されている。

（注）電子署名法第８条の「認定認証事業者」の場合

次のいずれかの方法により、本人確認を行わなければならない（同法施行規則第５条）とされており、申請者は、少なくとも市町村役場に出向くこと（住民票の写し、印鑑登録証明書等の取得のため）が必要なほか、方法によっては、さらに事業者の窓口又は郵便局に出向くことが必要となる。

①事業者の窓口において、住民票の写し若しくは戸籍の謄本等の提出を求めるとともに、旅券、官公庁が発行した一定の免許証、許可証、資格証明書等の提示を求める方法

②郵送等により、住民票の写し若しくは戸籍の謄本等及び申込書に押印した印鑑の印鑑登録証明書の提出を求める方法

③郵送等により住民票の写し若しくは戸籍の謄本等を提出を求めるとともに、本人限定受取郵便等により、申込みの有無を照会する文書を

送付し、これに対する返信を受領する方法

一方、地方公共団体による公的個人認証サービスにより提供される電子証明書は、市町村の窓口において、住民基本台帳データに基づく厳格な本人確認等が確保されるものであり、この電子証明書を民間認証事業者が行う特定認証業務に係る本人確認に活用できるようにすることが求められている。

その場合には、民間認証事業者は、高度な信頼性が確保された本人確認を効率的に行うことができるようになる。その上で、資格等の属性証明など様々なサービスを提供することにより、電子商取引の活性化等に大いに資することが期待される。

すなわち、電子商取引等のインフラである民間認証事業の信頼性を支える基礎的なインフラとしても、地方公共団体による公的個人認証サービスの提供が求められているのである。

Ⅰ－２－２　求められる制度の要件

２００３年度からの国又は地方公共団体の行政手続のオンライン申請・届出等の手続保障を実質的に確保するとともに、民間認証事業の信頼性を支える基礎的インフラとしての役割を果たすためには、次の要件を満たす制度を創設することが必要である。

① 全国サービスが可能であること
地理的条件等による利用機会の格差が生じないようにすること

② 厳格な本人確認が実施されること
都市部・地方に関わらず、国民・住民がどの市町村に居住していても、住所地の最寄りの市町村役場及びその支所において、対面審査による厳格な本人確認が実施されること

③ 個人情報について、厳重な保護措置を講ずること
必要最小限の個人情報により厳格な運営を行うとともに、個人情報の保護に最大限配慮したシステムによること

④ 制度の信頼性が確保されること
相当な社会的公証力を有するように、厳格なセキュリティポリシーに

より、高いセキュリティ技術及び人的信頼性等を確保した上で、システムの運用等を行うこと

⑤ 低廉な料金で提供できること
制度の信頼性を維持しつつも、本サービスに係るシステムの開発に当たっては、最大限効率的なシステムとすることにより、コストの増加を避け、できる限り少ない費用で行うことにより、低廉な料金でサービスを提供すること

第Ⅱ編　公的個人認証サービス制度試案

第１章　公的個人認証サービス制度の目的・仕組み・運営体制

Ⅱ－１－１　公的個人認証サービス制度の目的（参考７）

（１）国民・住民の利便性の向上

公的個人認証サービス（以下「本サービス」という。）の電子証明書は、市町村の窓口における厳格な本人確認手続に基づき、都道府県知事名義で発行されることから、成りすましの防止、改変の防止、送信否認の防止の効果がある高度な公証力を有する汎用的な電子証明書である。このようなサービスが、地理的条件等による格差が生じることなく低廉な費用で提供されることは、国及び地方公共団体の行政手続のオンライン申請・届出等の手続保障を確保し、国民・住民の利便性の向上に資するものと考えられる。

（２）国・地方公共団体の行政の電子化・効率化の推進

国及び地方公共団体の機関に対するオンライン申請・届出等の不可欠な本サービスの創設によって、オンライン申請・届出等が普及することにより、行政の電子化が促進されるとともに、手続の処理の迅速化等が図られ、業務の効率化も期待される。

また、本サービスを、国、都道府県、市町村の各行政機関がそれぞれが所管する申請・届出等をオンラインで行う場合に活用することにより、各行政機関等が個別にオンライン申請・届出等のための個人認証サービス制度を構築する場合に比し、行政全体としても効率的な電子政府・電子自治体の実現が図られる。

（３）電子商取引等のネットワーク上における諸活動の活性化

「Ⅱ－４－２」のとおり、認定認証事業者等の民間認証事業者が、特定認証業務の本人確認に本サービスの電子証明書を利用することにより、民間認証事業者は、高度な信頼性を確保された本人確認を効率的に行うことができるようになり、その上で、資格等の様々な属性等を証明するサービスを提供することが考えられる。

本サービスが、電子商取引等のインフラである民間認証事業の信頼性

を支える基礎的インフラとしての役割を果たすことを通じて、我が国における電子商取引等のネットワーク上の諸活動の活性化に資することが期待される。

Ⅱ－１－２　公的個人認証サービス制度の仕組み

（１）採用する電子署名の方式

諸外国の電子認証制度において一般的に採用されており、我が国においても、政府認証基盤、民間認証事業等で広く採用されている非対称鍵暗号方式による電子署名（デジタル署名）を採用することが適当である。

（２）デジタル署名を活用した公的個人認証サービス制度の仕組み（参考８）

デジタル署名を採用した場合、公的個人認証サービスの仕組みの概要としては、次のようなものが想定される。

① 電子証明書（本サービスにおいては、公開鍵証明書のことを指す。）の発行を申請する者（以下「申請者」という。）は、本人確認業務を行う機関に、必要事項を記入した申請書及び申請者の本人確認に必要な書面を提示。

② 本人確認業務を行う機関（以下「本人確認機関」という。）では、申請書を受理し、申請書記載事項と住民基本台帳に記録されている情報と照合すること等により、厳格な本人確認を実施。

③ 申請者は、本人確認機関の窓口に備え付けられた鍵ペア生成装置で、鍵ペアを生成し、ＩＣカード等の格納媒体に格納。

④ 申請者は、鍵ペアを格納した格納媒体を本人確認機関に提示し、生成した鍵ペアのうち、公開鍵を提出。

⑤ 本人確認機関は、申請者に関する情報と公開鍵を電子証明書の発行や失効情報の作成等の証明書発行・失効情報業務を行う機関（以下「証明書発行・失効情報管理機関」という。）に通知。

⑥ 証明書発行・失効情報管理機関は、提出された公開鍵は申請者本人に係るものであることを証明する電子証明書を作成し、本人確認機関に通知。

⑦ 本人確認機関は、電子証明書を格納媒体に書き込み、申請者に返却。

⑧ 電子証明書の発行を受けた者（以下「利用者」という。）は、行政機関等への申請書等について、秘密鍵を用いて電子署名を行い、電子証明書とともに行政機関等へオンラインで送信。

⑨ 行政機関等では、証明書発行・失効情報管理機関に問い合わせること等により、電子署名の検証を実施

Ⅱ－１－３　公的個人認証サービス制度の運営体制（参考９）

（１）都道府県単位認証局

都道府県知事（証明書発行・失効情報管理機関）及び当該都道府県の区域内の市町村長（本人確認機関）が、法律の定めるところによって、相互に連携・協力して、本サービスを住民に提供することが適当である。

（２）証明書ポリシー／認証実施規程（ＣＰ／ＣＰＳ）

都道府県知事は、（１）の法律の定めるところのほか、当該都道府県の区域内の市町村長と連携・協力して、本サービスの実施のための手続その他必要な事項を証明書ポリシー／認証実施規程（以下「ＣＰ／ＣＰＳ」という。）として定め、これを公表する必要がある。

なお、ＣＰ／ＣＰＳの策定に当たっては、均質で信頼性の高いサービスを全国的に確保するために、各都道府県知事は必要な連携・調整を行うことが求められる。

（３）本人確認機関（市町村長）

市町村長は、電子証明書の発行申請の受付、申請者の本人確認等の本人確認業務を行うことが適当である。

なぜなら、本人確認業務は、国民・住民に身近な行政機関であり、住民基本台帳等に基づく、厳格な本人確認を行える市町村が行うことが不可欠だからである。

（４）証明書発行・失効情報管理機関（都道府県知事：運用機関）

都道府県知事は、市町村長による本人確認に基づく電子証明書の発行、電子証明書の失効情報の作成等の証明書発行・失効情報管理業務を行うことが求められる。

証明書発行・失効情報管理業務については、電子証明書の発行の時点及び当該証明書の有効性確認の実施の時点において、公開鍵と本人との関係に係る証明を行うものである。したがって、信頼性の高い失効情報を効率的に作成できるとともに、運営経費等の経済性や均質で信頼性の高いサービスを全国的に確保できること等の観点から、都道府県知事が

行うことが適当であるからである。

この場合、都道府県が行う証明書発行・失効情報管理業務については、集中処理が可能であること等に留意し、共同処理を行う等最も合理的な方法（複数の都道府県知事から委託を受けた適切な運用機関による運用）を検討する必要がある。

この場合の運用業務は、証明書発行・失効情報管理機関としての都道府県知事の秘密鍵の管理をはじめ、極めて高いセキュリティレベル、運用ノウハウを確保することが、本サービスの円滑かつ安全な提供に不可欠であることから、当該業務を担う運用機関について、公共性・信頼性・安全性を確保しうる方法を検討すべきである。

（５）総務大臣

総務大臣は、本サービスの提供に関する業務に係る技術の評価に関する調査及び研究を行うとともに、都道府県、市町村、利用者に対し、必要な情報の提供、助言その他の援助を行うように努めることが求められる。

また、本サービスの提供に関する業務の用に供する施設、設備の管理の方法等の実施について必要な技術的基準を、総務大臣が策定することが必要である。

第２章　電子証明書の申請・発行手続（参考 10）

Ⅱ－２－１　申請

（１）電子証明書の発行を受けることができる者

住民基本台帳に記録されている者を対象とする。

なお、外国人については、出入国管理制度及び外国人登録制度との関係等を含め、別途検討する必要がある。

（２）申請

電子証明書の発行を申請する者は、その者が記録されている住民基本台帳を備える市町村の窓口に、申請者に係る住民票に記載されている事項のうち、次の事項を記載した発行申請書を提出する。

・氏名（及びそのローマ字表記）
・出生の年月日
・男女の別
・住所

Ⅱ－２－２　本人確認

発行申請書を受理した市町村長は、次のような方法により、申請者の本人確認（実在性の確認及び本人性の確認）を実施することが必要である。

（１）申請者が実在すること（実在性）の確認

申請書に記載された申請者の「氏名、出生の年月日、男女の別、住所」（以下「基本４情報」という。）と当該市町村が備える住民基本台帳に記録されている情報を照合することにより、申請者が実在すること（住民基本台帳に記録されていること）を確認する。

（２）申請者が本人であること（本人性）の確認

次の方法のいずれかのものにより、申請者と称する者が実在性の確認された申請者本人であること（住民基本台帳に記録されている者であること）を確認する。

①官公署の発行した資格証明書、運転免許証、旅券その他本人であることを証明できる書面であって、本人の写真を貼付してあるものの提示を求める方法

②本人であることを証明できる①以外の書面（各種健康保険の被保険者証、各種年金の年金手帳等（申請の受付窓口において、当該書面に係る原簿データを閲覧できるもの））の提示を求めるとともに、当該書面に係る原簿データに記録されている本人に関する事項について適宜質問し、当該データと照合して確認する方法

Ⅱ－２－３　申請者（利用者）の鍵の生成・格納・提示等

（１）鍵ペアの生成

申請者の鍵ペア（秘密鍵と公開鍵）は、暗号の強度（解読の困難性）を確保し、改変される可能性を少なくする必要等から、市町村の窓口に配備する鍵ペア生成装置を用いて、申請者自らが生成する方法に当面限定することが適当である。秘密鍵のアーカイブのシステム（秘密鍵をバックアップしておく保管システム）は採用するべきではない。

なお、鍵ペア生成装置は、生成した鍵が速やかに消去され、装置上に残らないものであることが必要である。

（２）秘密鍵の格納

秘密鍵は、外部からの不正アクセス等からの保護等の要請から、コピーを作ることが不可能で、解読が著しく困難なＩＣカード等の耐タンパ装置（住民基本台帳カード等）に格納することを原則とするべきである。

但し、当面の間は、ＩＣカード読取・書込装置の普及状況にかんがみ、フロッピーディスク等に格納することを可能とすることも検討する必要があろう。

（３）公開鍵の提示

申請者は、生成した鍵ペアのうち、公開鍵を市町村の窓口に提示する。

なお、公開鍵を窓口に提示する際には、その格納媒体を窓口に提出しするとともに、当該格納媒体を活性化するための暗証番号を入力することが必要であるが、その入力は申請者自らが行うようにすることが望まれる。

Ⅱ－２－４　電子証明書の発行・提供

（１）電子証明書の発行

市町村長は、申請者に係る基本４情報及び公開鍵を都道府県知事に通知する。

通知を受けた都道府県知事は電子証明書を発行し、当該市町村長に通知する。

この場合、市町村長と都道府県知事の間の公開鍵等の通知、電子証明書の通知等の通信はセキュリティ確保の観点から、「総合行政ネットワーク」（参考 11）を利用することが適当である。

（２）電子証明書の提供

市町村長は、電子証明書及び証明書発行・失効情報管理機関としての都道府県知事の自己署名証明書を、申請者の持参するＩＣカード等の格納媒体に格納した上で提供する必要がある。

また、電子証明書の利用規約や利用方法等を記載したガイド及び電子証明書の写し（電子証明書の記録内容を見読可能な状態にして紙に印刷したもの）を交付することが望まれる。

なお、後述のとおり、電子証明書の発行手数料は、できるだけ低廉な負担とすることから、電子証明書の複数交付は行わないものとすべきであろう。

（３）発行記録の作成

都道府県知事は、電子証明書を発行した場合には、利用者等が後日紛争が生じた場合の証拠等に利用できるよう、一定期間、発行記録（発行した電子証明書）を作成し、保存する必要がある。

Ⅱ－２－５　電子証明書の要件等

（１）電子証明書の要件

本サービスで発行する電子証明書は、次の要件を満たす電磁的記録であることが必要である。

①次の事項が記録されていること

・当該電子証明書の発行の番号、発行年月日及び有効期間の満了す

る日
・当該電子証明書に係る公開鍵及び当該鍵に係る計算方法（アルゴリズム）
・当該電子証明書の利用者の氏名等基本４情報
・本サービスに係る電子証明書の用途等に関する情報　　等
②発行した都道府県知事の電子署名が行われていること

（２）電子証明書の形式（参考 12）

電子証明書の形式は、ＩＴＵ（国際電気通信連合）の標準（Ｘ.５０９ Ver.３）に準拠し、利用者の基本４情報は、証明書の拡張領域に記録する。

（３）電子証明書の証明事項

電子証明書は、「電子証明書に記録されている公開鍵が当該利用者に係るものであること」を証明するものとする。

（４）氏名の記録方法

拡張領域に記録する氏名の表記に利用する漢字、ひらがな、カタカナは、本サービスに係るシステムが採用する文字コードに存在する漢字、ひらがな、カタカナに限定される。

住民基本台帳に記録されている氏名に、本サービスに係るシステムが採用する文字コードには存在しない漢字等がある場合には、あらかじめ定める類似の漢字等又は当該漢字等の読み仮名を表すひらがな・カタカナ（以下「代替文字」という。）を申請者が選択して使用する方法を採ることが適当である。

なお、代替文字を使用した場合には、どの文字に代替文字を使用しているかを拡張領域内に表示することが望まれる。

（５）住所の記録方法

拡張領域に記録する住所の表記に利用する漢字、ひらがな、カタカナは、本サービスに係るシステムが採用する文字コードに存在する漢字、ひらがな、カタカナに限定される。

住民基本台帳に記録されている住所に本サービスに係るシステムが採用する文字コードには存在しない漢字等がある場合は、あらかじめ代替文字を定め、その文字を使用する方法を採ることが適当である。

なお、代替文字を使用した場合には、どの文字に代替文字を使用しているかを拡張領域内に表示することが望まれる。

（６）電子証明書の有効期間

利用者の利便性及び秘密鍵・公開鍵の安全性等を勘案し、発行日から起算して３年間とすることが適当である。

Ⅱ－２－６　代理申請

申請者が疾病その他やむを得ない事由により、自ら発行申請をすることができないときは、次の申請手続により、代理人による申請を行うことができることとする必要がある。

① 代理人が申請者の署名及び実印の押印された委任状と当該実印に係る印鑑登録証明書を添えて、市町村長に発行申請書を提出

② 市町村長は、代理人の本人確認を、住民基本台帳の記録事項との照合及び官公署の発行した写真が貼付されている資格証明書等により確認

③ 代理人は、鍵ペア生成装置を用いて、鍵ペアを生成し、公開鍵を市町村長に提示

Ⅱ－２－７　更新

電子証明書の有効期間の満了時における更新の申請は市町村の窓口に出向いて行う必要がある。

この場合、既存の電子証明書を失効させるとともに、鍵ペアの変更を行うことが必要である。

なお、オンラインによる更新申請については、利用者が自宅等で鍵ペアを生成することが必要であるが、現時点では、利用者が自宅等で生成した鍵の品質を担保することが困難であるため、当面行わないこととすべきである。

第３章　電子証明書の失効

Ⅱ－３－１　失効情報の作成

（１）利用者からの失効請求による失効情報の作成

ア　本サービスの利用を取りやめるための失効

利用者は、電子証明書の有効期間内において、本サービスの利用を取りやめようとする場合には、次に掲げる方法のいずれかにより、任意に失効の請求を行うことができるようにすべきである。

①市町村の窓口に出向き、失効請求書を市町村長に提出する方法（この際、利用者の本人確認は官公署の発行した写真が貼付されている資格証明書等を提示する方法等により行う。）

※失効請求書の提出を受けた市町村長は都道府県知事に失効請求書を通知

②電子署名を行った失効請求書を都道府県知事にオンラインで送信する方法

都道府県知事は、市町村長からの失効請求書の通知又は利用者からのオンラインでの失効請求書の送信を受け、当該請求に係る電子証明書について失効情報を作成することになる。

イ　秘密鍵の危殆化等に伴う失効

利用者は、当該利用者の秘密鍵の紛失・き損・危殆化等（秘密鍵の格納媒体の紛失、き損等を含む。）が発生した場合は、速やかに、市町村の窓口に出向き、市町村長に対して、その旨の届出を行わなければならないこととすべきである。

この際、利用者の本人確認は官公署の発行した写真が貼付されている資格証明書等を提示する方法等により行う必要がある（オンラインで送信する方法は採れない。）。

都道府県知事は、市町村長からの届出の通知を受け、当該届出に係る電子証明書について失効情報を作成することになる。

（２）職権による失効情報の作成（参考 13）

ア　電子証明書に記録された事項と異なるものが発見された場合の失効

利用者の住所・氏名・男女の別・出生の年月日の変更又は死亡の事

実が生じた場合など、異動等失効情報等により、利用者の電子証明書の証明事項に関して当該電子証明書に記録されたものと異なるものが発見された場合、都道府県知事は、職権により、当該電子証明書について失効情報を作成する必要がある。

（注）「異動等失効情報」とは、住所・氏名・男女の別・出生の年月日の変更又は死亡の事実が生じた場合において、何らかの異動等の事実があった旨の情報のみをいい、異動等の区分や内容（新しい住所又は氏名等）及び住民票コードを含まないものである。

この情報の提供を住民基本台帳ネットワークシステムから受けることにより、

① 住所等電子証明書記載事項の変更があった場合に、利用者及び市町村の担当者は、公的個人認証サービス側には申告を行う必要がなく、利用者の利便性の向上・市町村都道府県の事務の省力化に資すること、

② 失効情報作成の正確性が向上すること、

③ 公的個人認証サービスのシステム側で、住所異動等に係る個人情報の収集をせずに適確な失効情報を作成すること、

等が可能となる。

イ　証明書発行・失効情報管理機関としての都道府県知事の秘密鍵の危殆化等に伴う失効

証明書発行・失効情報管理機関としての都道府県知事の秘密鍵の紛失・き損・危殆化等が発生した場合、都道府県知事は、職権で、当該秘密鍵で署名されたすべての電子証明書について失効情報を作成するとともに、Ｗｅｂ等により、その旨を公表することが望ましい。

この場合、再発行を希望する者は、無料で電子証明書の発行を受けることができることとすることが望ましい。

Ⅱ－３－２　失効情報の記録事項等

当該電子証明書に係る失効情報としては、次の事項を記録し、電子証明書の有効期間が経過するまで、保存する必要がある。

①当該電子証明書の発行番号

②失効請求、秘密鍵の危殆化等の届出、異動等失効情報の通知又は都道府県知事の秘密鍵の危殆化等、失効の理由となったいずれかの事由

③作成年月日

Ⅱ－３－３　電子証明書の失効

電子証明書は、「Ⅱ－３－１」の失効情報が作成されたとき又は有効期間が満了したときに失効する。

Ⅱ－３－４　失効情報ファイルの作成

後日、紛争が生じた場合において証拠として活用するため、いつ、どのような内容の失効情報を提供したどうかを確認できるように失効情報ファイルを作成し、一定期間保存することが必要である。

第４章　電子証明書の検証等

Ⅱ－４－１　電子証明書の有効性確認の方法

都道府県知事は、次の２つの方法により、有効期間を満了していない電子証明書について、その有効性を確認する方法を提供する必要がある。

① 応答用の電子計算機に照会する方法（ＯＣＳＰレスポンダ照会方法）
～特定の電子証明書についての問い合わせに対して、当該証明書が失効しているかどうかを個別に回答する方法

② 一定の範囲の利用者に係る失効情報を定期的（例えば、1 日１回）にまとめて提供する方法（失効リスト提供方式）

Ⅱ－４－２　署名検証者

署名検証者は、次の者のうち、電子証明書の有効性を確認する方法等の提供を希望する旨をあらかじめ都道府県知事に届け出て、アクセス権を付与された者とすることが適当である。

① 行政機関等（国の機関・地方公共団体の機関　等）

② 特定認証業務を行う民間認証事業者で一定の信頼性を有するもの

このうち、②については、「Ⅱ－１－１（３）」の目的のために、民間認証事業者を署名検証者とするものであるが、署名検証者は、本サービスの利用者から電子証明書の提供を受け、都道府県知事から、失効情報の提供を受けることとなることから、電子証明書等の適切な利用及び保護、システム全体の信頼性を確保するため、一定の信頼性を有する事業者に限定することが求められる。

具体的には、電子署名法の認定制度により、一定の信頼性を有する特定認証業務を行う事業者とされている同法第８条の認定認証事業者及びこれに準ずる事業者として一定の基準を満たす者（総務大臣が認定することが考えられる。）を対象とすることが適当である（参考 14）。

②の事業者は、特定認証業務のみを行う場合のほか、特定認証業務とあわせて本人の資格等の属性を証明する業務を行う場合も想定される（参考 15）。

Ⅱ－４－３　取決めの締結

電子証明書の有効性を確認する方法を提供するに当たっては、提供する情報の範囲及び提供方法等について、取決めを締結する必要がある。

Ⅱ－４－４　相互認証

政府認証基盤の認証局等との相互認証システムを構築し、的確に運営する必要がある（参考 16）。

Ⅱ－４－５　官職証明書の検証サービスの提供

本サービスの利用者は、オンライン申請等を行った場合、折り返し、行政機関から、当該申請等に係る許認可等の行政文書及びその電子署名を検証するために必要な電子証明書（以下「官職証明書」という。）をオンラインで受け取る場合がある。

この場合、利用者が、受け取った行政文書に行われている電子署名の検証を行うに当たっては、官職証明書の有効性を確認する必要があるため、利用者等への負荷を軽減するため、本サービスの提供に併せ、官職証明書の有効性を確認するための方法を提供することも検討されるべきである。

（注）この場合、利用者は、政府認証基盤ブリッジ認証局（当該行政機関が国の機関の場合）から当該行政機関の自己署名証明書及び官職証明書の失効情報を入手するだけでなく、都道府県単位認証局、公的個人認証サービスの相互認証システム、政府認証基盤ブリッジ認証局、当該行政機関の認証局のそれぞれの間で作成された相互認証証明書及びその失効情報等を入手しなければならない（認証パス（検証の道筋）の構築）。

第５章　関係者の義務等

Ⅱ－５－１　利用者の義務等

（１）利用者の義務

デジタル署名を採用する本サービス制度においては、利用者のみが当該利用者に係る秘密鍵を所持していることが、サービスの安全性・信頼性の根幹をなすものであることから、その担保のため、利用者に対して、法律上、次の義務を課すことが必要である。

①秘密鍵の適切な管理

②秘密鍵が紛失・き損・危殆化等が発生した場合の速やかな届出

（２）利用者の負担

本サービスは、オンライン申請等の手続保障を確保することが目的であり、利用者の負担は、実費弁償的な一定の負担にとどめるべきである。

なお、秘密鍵の紛失・き損・危殆化等の理由により、既存の電子証明書を失効し、新たな電子証明書の再発行を求める場合の発行手数料については、相当程度の追加的な負担を求めることが適当である。

Ⅱ－５－２　署名検証者の義務等

（１）署名検証者の義務

利用者の個人情報保護及び本サービス制度の安全性・信頼性を担保するため、署名検証者に対して、次の義務を法律上課すことが必要である。

① 電子署名の適格な検証（当該電子署名の検証のほか、電子証明書が有効期間内であるかどうか、当該都道府県知事から発行されたものであるかどうか、失効していないかどうか等の電子証明書の検証を行うこと）

② 利用者から受け取った電子証明書を、オンライン申請・届出等の電子署名の検証以外の目的で利用することの禁止

（２）署名検証者の負担

署名検証者に対して、適切な受益者負担を求めることが適当である。

第６章　本サービスに関する情報の公開

Ⅱ－６－１　公開する情報と公開方法

（１）法令・規程

本サービスに関する次の法令・各種規程は、本サービスの実施に当たり開設するＷｅｂ上で公開する必要がある。その場合、アクセス制限は設けない方向で検討すべきである。

・本サービスに係る根拠法令、関係法令
・ＣＰ／ＣＰＳ
・個人情報の取扱いに関する規程　等

（２）証明書等

都道府県単位認証局に関する、次の証明書等は、公的個人認証サービスの相互認証システムのリポジトリで公開する必要がある。その場合、アクセス制限は設けない方向で検討すべきである。

・自己署名証明書及びその失効情報
・相互認証証明書及びその失効情報
・リンク証明書及びその失効情報
・サーバ証明書及びその失効情報

なお、本サービスに係る利用者の電子証明書の発行記録及びその失効情報は公開せず、署名検証者に対してのみ、電子証明書の有効性を確認する方法を提供することが適当である。

Ⅱ－６－２　公開する情報の更新頻度

（１）法令・規程

「Ⅱ－６－１（１）」に掲げる公開する法令等については、変更等の都度とする。

（２）証明書等

「Ⅱ－６－１（２）」に掲げる公開する証明書等については、発行又は更新の都度とする。なお、署名検証者のみに提供する利用者の電子証明書の失効リストについては、毎日１回の更新の都度とする。

第７章　個人情報の保護

本サービス制度の運営に当たっては、取り扱う利用者の個人情報を最小限にとどめるとともに、ＯＥＣＤ８原則（『プライバシー保護と個人データの国際流通についての理事会勧告』（１９８０年）の附属文書『プライバシー保護と個人データの国際流通についてのガイドライン』のうち、第２部「国内適用における基本原則」に示された８原則）等に基づき、以下に掲げる方法等により、本サービスの運営に当たり取り扱う利用者の個人情報について、厳重かつ適切な保護を行う必要がある。

Ⅱ－７－１　収集制限

収集する個人情報は、あらかじめ特定された収集の目的を達成するため必要な限度を超えない範囲に限定すべきであり、また、個人情報を収集するに当たっては、適法かつ公正な手段により実施すべきであること。

→　本サービスにおいては、個人情報の収集手段及び収集する個人情報の種類は、次に限定するべきである。

＜個人の属性情報＞

①発行申請書、失効請求書、秘密鍵の危殆化等の届出への記載による利用者の基本４情報

②公開鍵

③本人確認を行うために提示させる（ア）官公署の発行した資格証明書、運転免許証、旅券その他本人であることを証明できる書面であって、本人の写真を貼付してあるもの又は（イ）本人であることを証明できる（ア）以外の書面、に記載される情報

④異動等失効情報

＜有効性確認等の問合せ情報＞

問合せ情報については、将来の紛争処理のために必須であるとされる情報を除き、集積しないという方向で検討する必要がある。

Ⅱ－７－２　データ内容

管理する個人情報について、利用目的に応じ正確かつ最新なものに保つように努めるとともに、利用目的に必要な範囲内で保存期間を定めることを原則とし、当該期間経過後又は利用の目的を達成した後は、遅滞なく消去すべきであること。

→　本サービスにおいては、管理する個人情報のうち、利用者の電子証明書の状態（失効情報の作成の有無）について、本人からの失効請求等により、失効情報等を作成するとともに、その他の管理する個人情報については、所定の保存期間で保存し、その期間の経過後又は利用の目的達成後は、遅滞なく消去すべきである。

Ⅱ－７－３　目的明確化

個人情報を収集するに当たっては、本サービスを提供するために必要な場合に限り、かつできる限りその目的を特定すべきであること。

→　本サービスにおいては、電子証明書の発行、発行記録、失効情報等の作成のために限り、個人情報を扱うものとすべきである。

Ⅱ－７－４　利用制限

収集された個人情報の利用又は提供は、
①本人の同意がある場合、
②法令の規定に基づく場合、
③自己の業務の遂行に必要な限度で個人情報を内部で利用する場合であって、当該個人情報を利用することについて相当な理由があるとき、
④①～③に掲げる場合のほか、本人以外の者に提供することが明らかに情報主体の利益になるとき
その他個人情報を利用し、又は提供することについて特別の理由があるとき、を除き、収集目的の達成に必要な範囲に限定すべきであること。

→　都道府県知事及び市町村長は、本サービスに係る業務の実施に際して知り得た情報について、それらの業務に用いる目的以外に使用しないこととすべきである。

　また、署名検証者については、受領した失効情報等を、電子証明書の有効性の確認や紛争が生じた場合の証拠としての活用に必要な範囲内で利用し、その目的以外のために受領した失効情報等を利用したり、提供することを禁止する必要がある。

Ⅱ－７－５　安全保護

　個人情報を管理するに当たっては、当該情報への不正なアクセス又は当該情報の紛失、破壊、改変、漏えいの防止その他の個人情報の適切な管理のために必要な措置を実施すべきであること。

→　本サービスにおいては、都道府県知事は、発行記録、失効情報等を取扱うに当たり、これらの情報の漏えい、滅失、き損の防止等適切な管理のために必要な措置を講じる必要がある。

　署名検証者についても、受領した失効情報等を取り扱うに当たり、その漏えいの防止等適切な管理のために必要な措置を講じなければならないこととすべきである。

Ⅱ－７－６　公開

　本人から自己に関する個人情報の開示の請求があった場合には、当該請求に係る個人情報について遅滞なく開示すべきであること。

→　本サービスにおいては、利用者から、当該利用者に係る発行記録、失効情報等について、都道府県知事に開示の請求があった場合には、遅滞なく、開示することが適当である。

Ⅱ－７－７　個人参加

本人から自己に関する個人情報の訂正、追加、削除等の申出があったときは、遅滞なく調査を行い、当該申出に係る個人情報に関して誤りがあること等訂正等を必要とする事由があると認めるときは、遅滞なく訂正等を実施すべきであること。

→　本サービスでは、都道府県知事は、自己に係る情報の開示を受けた利用者から、開示に係る情報について、訂正、追加、削除等を求められた場合には、遅滞なく調査を行い、その結果に基づき、当該情報の訂正等を実施することが適当である。

また、成りすましによる被害から個人を守るために、当該個人に係る情報の開示や訂正のために必要な方法等について検討する必要がある。

Ⅱ－７－８　責任

個人情報の取扱いに関する責任者を置くとともに、内部規程及び監査体制の整備等必要な個人情報保護措置を実施すべきであること。

→　本サービスにおいては、個人情報取扱責任者を置くとともに、個人情報の取扱いに関する規程の策定等を実施する必要がある。

また、本サービスに係る事務に従事する都道府県及び市町村の職員等に対して、その事務に関して知り得た秘密について、その漏えいを禁止する義務を課すとともに、署名検証者の職員についても、失効情報等の取扱いに関して知り得た秘密について、同様の義務を課すことが適当である。

第８章　帳簿書類の作成・保存

本サービス制度の運営に当たっては、業務がＣＰ／ＣＰＳ等の規程に従い、適切に運営されていることを監査等で確認するため、また、本サービスに係る紛争等が発生した場合の円滑な解決に資するため、次に掲げる帳簿書類を必要な期間、適切な方法により、保存することを検討する必要がある。

Ⅱ－８－１　作成保存する帳簿書類及び保存期間

（１）業務管理関連の帳簿書類

次の業務管理に関する帳簿書類については、作成後、１０年間程度保存することが適当である。

◯認証業務に関するポリシー等

・ＣＰ／ＣＰＳ
・セキュリティポリシー
・事務取扱要領
・上記ＣＰ／ＣＰＳ及び事務取扱要領の変更に関する書類、改訂履歴
・業務の一部を他に委託して行う場合、委託契約に関わる契約書類等
・業務に関して入手した情報の開示に関する規程
・個人情報の取扱いに関する規程

◯要員組織管理関係帳簿書類

・業務に従事する要員に関する組織、体制、主管及び指揮命令系統に関する管理情報、履歴

◯監査関連帳簿書類

・内部監査実施記録及び報告書
・外部監査実施記録及び報告書

（２）証明書発行・失効情報管理機関として都道府県知事の秘密鍵、自己署名証明書等に関する管理関連帳簿書類

次の証明書発行・失効情報管理機関としての都道府県知事の秘密鍵及び自己署名証明書等の管理に関する帳簿書類については、当該帳簿等に基づき発行された証明書の有効期間終了後、１０年間程度保存することが適当である。

◯証明書発行・失効情報管理機関としての都道府県知事の秘密鍵の管理

・鍵の生成、保存に関する記録
・鍵の状態変更に関する記録
・鍵のバックアップに関する記録
・鍵の復元に関する記録
・鍵の廃棄に関する記録

◯自己署名証明書等の管理
・自己署名証明書、相互認証証明書、リンク証明書、サーバ証明書
・上記証明書の失効情報
・上記証明書作成に関する記録

（３）電子証明書に関する管理関連帳簿書類

次の利用者の電子証明書に関する帳簿書類については、当該帳簿等に基づき発行された電子証明書の有効期間終了後、１０年間程度保存することが適当である。

◯申請関連帳簿書類
・発行申請書
・本人確認資料
・その他発行可否判断のために使用した資料

◯発行関連帳簿書類
・発行可否判断者、拒否した場合、その理由
・発行記録
・上記電子証明書作成に関する記録

◯失効関連書類
・失効請求書
・秘密鍵の危殆化等の届出
・本人確認資料
・その他失効の可否判断のために使用した資料
・失効可否判断者、拒否した場合、その理由
・失効情報ファイル
・上記ファイルの作成に関する記録

（４）運用関連帳簿書類

次の運用に関する帳簿書類については、当該記録発生期間に対する内部監査及び外部監査の双方が完了するまで保存することが適当である。

◯権限管理
・入退室及びコンピュータシステム等アクセス権限付与並びに剥奪に

関する書類並びにその履歴
・電子証明書発行担当者への業務用電子証明書及びその格納媒体等の発行管理記録

◯設備関連
・設備保守に関する記録
・入退室管理記録

◯システム関連書類
・システム変更履歴
・コンピュータシステム等へのログイン記録
・特権ユーザへの変更記録

◯障害対応
・障害記録

◯帳簿へのアクセス及び廃棄記録
・保存される帳簿に対するアクセス記録

Ⅱ－８－２　保存方法

「Ⅱ－８－１」に掲げる帳簿書類については、その保管期間内において、改変及び情報の流出を防ぐための対策を講じ、次の事項に適合する場所に安全に保管する必要がある。

・間仕切り又は壁等によって区分され、かつ防災及び防犯のための機能を備えていること。
・保存するものに応じた、防火及び防水等の対策を講じていること。
・施錠が可能な扉を備えること。

特に、磁気ディスク等の電子媒体を用いて保存する場合、データの滅失も、毀損について充分留意し、帳簿等の整合性を保つ必要がある。

電磁的記録として保存される帳簿等については、保存期間において可読性を保つ必要がある。

第９章　セキュリティの確保

Ⅱ－９－１　暗号方式

（１）採用する暗号方式等

本サービスにおいて、鍵ペアに係る暗号を作成・復号するためのアルゴリズムとしては、次の理由により、ＲＳＡ方式を採用することが適当である。

①現時点では、不特定の通信相手を認証する手段として同方式による仕組みが確立されつつあり、国内においても、政府認証基盤、民間認証事業等で同方式が採用されていること等から、同方式によることが最も合理的であると考えられること。

②海外の電子認証制度においても同方式によるものが一般的であり、国際的整合性を図る観点からも問題が少ないこと

また、鍵長については、利用者の鍵の鍵長は１，０２４ビット、証明書発行・失効情報管理機関としての都道府県知事の鍵の鍵長は２，０４８ビットとする必要がある。

（２）暗号方式に関する検証体制

暗号の方式又は強度(解読の困難性)については、定期的に検証を行い、脆弱性が検知された場合等には速やかに適切な対策を取りうる体制・仕組みをあらかじめ整備することが必要である。

また、既存の暗号方式の検証、新たな暗号方式の検討等を継続し、市町村長（本人確認機関）及び都道府県知事（証明書発行・失効情報管理機関）の業務革新をサポートできる体制を整備することも必要である。

Ⅱ－９－２　セキュリティ管理

（１）組織・運用面のセキュリティ管理

本サービスに係る組織・運営について、次のとおり、セキュリティ管理を行うことが求められる。

① 本サービスを行うに当たり、必要な電子署名技術、鍵管理技術、ネ

ットワークセキュリティ技術、システムセキュリティ技術及びセキュリティ管理に関する充分な知識を有する適切な人数の技術者を配置する。

② 本サービスを行うに当たり、ＣＰ／ＣＰＳを実現するための手順の細目を明確に定め、事務取扱要領として文書化する。また、その内容が、すべての職員に役割として理解されるようにするとともに、実施し、かつ、維持する。

③ 職員について、次に掲げる事項に関し、内部牽制を考慮したうえで、指揮命令系統、責任及び権限を明確に定め、文書化する。また、その内容がすべての職員に役割に応じて理解されるようにするとともに、実施し、かつ、維持する。

（入室権限）

異なるセキュリティ基準の境界において、アクセスが可能な職員を限定し、管理する。

・コンピュータ室（証明書発行・失効情報管理業務に供する装置を設置する場所（専ら発行指示のために用いられる装置のみを設置する場所を除く））への入室については、複数人によってなされるよう権限を管理する

・コンピュータ室へやむを得ず入室権限を有しない者を入室（設備、コンピュータのメンテナンス、監査等）させる場合には、権限を持つ者複数人が同行する

（システムアクセス制限）

証明書発行・失効情報管理業務及び本人確認業務に用いる装置等へのアクセスについては、アクセスが可能な職員を限定し、管理する。

④ システムセキュリティについては、次のとおり行う。

・システムへのアクセス管理をパスワードを用いて行う場合、適切なパスワード管理を行うこと。

・システム及びネットワーク装置について、セキュリティに関する情報を収集し、最新のセキュリティ対策モジュールを導入する等脆弱性を最小にするよう努める。

・本サービスに用いるハードウェア、ソフトウェアについて充分なセキュリティ対策を行う。

・システム、ネットワーク経由の遠隔操作が可能な設定は行わない。

⑤ 証明書発行・失効情報管理機関としての都道府県知事の秘密鍵の危殆化及び災害等による障害の発生に対する対応策及び回復手順を文書化する。また、その内容をすべての職員に役割に応じて理解されるようにする。

（２）設備等の基準

設備等については、電子署名法に基づく特定認証業務の用に供する設備等に係る水準以上のものを確保する。具体的には、次の基準に適合するものであることが求められる。

①入出場を管理するために業務の重要度に応じて必要な措置が講じられている場所に設置すること

②ネットワークを通じた不正アクセス等を防止するために必要な措置が講じられていること

③正当な権限を有しない者によって作動させられることを防止するための措置が講じられ、かつ、当該設備の動作を記録する機能を有していること

④証明書発行・失効情報管理機関としての都道府県知事の秘密鍵を生成し又は管理するコンピュータは、当該鍵の漏えいを防止するために必要な機能を有する専用のコンピュータであること

⑤停電、地震、火災及び水害その他の災害の被害を容易に受けないように業務の重要度に応じて、必要な措置が講じられていること。

（３）情報に関するセキュリティ管理

ア　情報セキュリティ

取り扱う情報について、物理的脅威、技術的脅威、人的脅威について十分なセキュリティ対策を検討し、組織・体制、情報の分類と管理（方法と責任)、物理的セキュリティ、技術的セキュリティ、運用管理等の各項目について十分な水準を確保する必要がある。

イ　機密保持

本サービスに係る公開されていないシステム、ネットワーク、詳細な手順等の機密保持に関して明確に規定し、かつ、文書化を行う。また、その内容をすべての職員が役割に応じて理解し、実施し、維持する必要がある。

（４）証明書発行・失効情報管理機関としての都道府県知事の秘密鍵の管理等

証明書発行・失効情報管理機関としての都道府県知事の秘密鍵については、次のとおり取り扱い、その安全を確保する必要がある。

ア　秘密鍵の使用範囲

証明書発行・失効情報管理機関としての都道府県知事の秘密鍵は、次の用途等限定された範囲で使用するものとする。

①本サービスに係る電子証明書及びその失効情報等への署名
②自己署名証明書及びその失効情報への署名
③相互認証証明書及びその失効情報への署名
④リンク証明書及びその失効情報への署名
⑤サーバ証明書及びその失効情報への署名

イ　秘密鍵の有効期間

証明書発行・失効情報管理機関としての都道府県知事の秘密鍵の有効期間は、１０年間とし、５年ごとに鍵更新を行うことを検討する必要がある。

ウ　秘密鍵の生成

証明書発行・失効情報管理機関としての都道府県知事の秘密鍵は、「Ⅱ－９－２（２）」の基準を満たすコンピュータ室内で、同基準を満たす暗号装置を用いて、適切な権限を有する複数人によって生成する。

エ　秘密鍵の保存

証明書発行・失効情報管理機関としての都道府県知事の秘密鍵は、コンピュータ室と同等の安全性を有する場所に設置された暗号装置内に保存する。

オ　秘密鍵のバックアップ

証明書発行・失効情報管理機関としての都道府県知事の秘密鍵をバックアップする場合は、コンピュータ室内で暗号装置自体の複製機能を使用して行う。バックアップした鍵は、コンピュータ室と同等の安全性を有する場所に保存する。

暗号装置自体の複製機能を使用しない場合は、知識分散等の手法を用

い、コンピュータ室内でバックアップ作業を行い、異なる安全な場所に分散して保存する。

カ　秘密鍵の状態変更

証明書発行・失効情報管理機関としての都道府県知事の秘密鍵を利用不可能な状態から利用可能な状態にする場合、もしくは利用可能な状態から利用不可能な状態にする状態変更は、コンピュータ室内で複数人により行う。

キ　秘密鍵の廃棄

証明書発行・失効情報管理機関としての都道府県知事の秘密鍵が有効期間の経過その他の理由により使用を終了する場合には、複数人による物理的破壊、完全な初期化、もしくはこれに準ずる手段により廃棄する。また、バックアップされた秘密鍵についても同時に廃棄する。

ク　秘密鍵の危殆化

証明書発行・失効情報管理機関としての都道府県知事の秘密鍵が盗難や解読等の危殆化等の事態にあることを認識した場合には、遅滞なく当該秘密鍵で発行された電子証明書についての失効情報を作成するとともに、その旨を利用者、署名検証者その他必要な範囲に通知する。

Ⅱ－９－３　システム監査

本サービスに係る業務が、関係法令、セキュリティポリシー、ＣＰ／ＣＰＳ等の規程に準拠して実施されていること、並びに外部からの不正及び内部の不正行為に対する措置が適切に講じられていること等の監査を定期的に実施することが必要である。

本監査は、内部で行うとともに、監査業務及び認証業務に精通した外部の専門機関に行わせることとする。

また、システム監査の結果は、公表することが必要である。

第１０章　法的措置

本サービスは、国又は地方公共団体の手続のオンライン申請・届出等の実現に不可欠であることから、平成１５年度からの運用開始を目指し、本サービス制度を創設するための所要の法制度を整備することが必要である。

第Ⅲ編　本サービスに関する実体法上の諸課題

第１章　損害賠償

Ⅲ－１－１　都道府県等の職員の故意・過失による損害

市町村の職員の不適切な本人確認、都道府県の職員の失効情報等の作成の懈怠等により、利用者、署名検証者等に損害が発生した場合、本サービスの運営は、都道府県知事及び市町村長が行うことから、都道府県、市町村は、国家賠償法第１条に基づき、利用者等に対して、損害を賠償する責めを負うこととなる（同法２条の適用については明確でない。）。

この場合、損害を負った利用者等は、その損害発生の原因となった加害公務員の故意・過失を証明することが必要となる。

Ⅲ－１－２　システムの不具合等による損害

本サービスは、電子証明書を発行するサーバ、電子証明書に証明書発行・失効情報管理機関としての都道府県知事の電子署名を行うコンピュータ、市町村窓口に設置される鍵ペア生成装置等多数のコンピュータ等のシステムにより提供されることから、これらのシステムの不具合等により、誤った内容の電子証明書が発行されたり、不実の失効情報が作成され、利用者や署名検証者に損害が発生する危険がある。

この場合、システムの不具合等により利用者又は署名検証者に発生した損害の賠償については、本サービスにおいて高いセキュリティ水準を確保するようにすることが、利用者等の側から、「過失」（国家賠償法第１条の場合）又は「瑕疵」（国家賠償法第２条の場合）の存在を証明するに際して、その実質的な負担を軽減することとなるものと思われる。

したがって、次のような事情を勘案し、十分な被害者救済に資するよう、高いセキュリティ基準を確保すべきである。

①システムの不具合等により、利用者又は署名検証者に損害が発生した場合には、電子証明書や失効情報等を信頼した署名検証者等の証明責任の負担を軽減することが被害者救済の観点から求められること。

②国家賠償法第２条は「公の営造物」の設置・管理の瑕疵から生じる損

害の賠償について、本サービスの提供の用に供するサーバ等の設備が、「公の営造物」に該当するか明確ではないものの、国家賠償法第１条適用の場合と同法第２条適用の場合とで、不均衡にならないようにすべきであること。

③本サービスは市町村、都道府県の双方の設備により提供されることから、システムの不具合により損害が発生した場合、いずれの設備の不具合によるのか不明な場合もあると考えられること。

Ⅲ－１－３　損害賠償額の上限

本サービスでは、国又は地方公共団体の機関のほか、一定の信頼性を有する特定認証業務を行う民間認証事業者についても、電子証明書の有効性を確認する方法を提供することが検討されているが、これらの者に本サービスの提供に関して損害が発生した場合には、次の理由から、あらかじめ損害賠償の上限を設定することを検討することが必要である。

① 署名検証者が、一定の信頼性を有する特定認証業務を行う民間認証事業者の場合、本サービスに係る電子証明書を本人確認に利用して、自らの民間電子証明書を発行するところ、その民間電子証明書はオンライン取引一般に利用されることから、不実の電子証明書が発行され、それに基づき発行された不実の民間電子証明書がオンライン取引等で悪用された場合、その被害は多額に及ぶことも予想されること。

② この場合、あらかじめ損害賠償額の上限を設定することにより、本サービスに係る電子証明書を利用する民間認証事業者に、それを前提としたリスク回避をなさしめ、もって、都道府県知事及び市町村長の予見可能性を確保することが制度運営上望ましいと考えられること。

第２章　本サービスに係る電子署名の実体法上の効果

III－２－１　押印が行われた私文書の証拠力

民事訴訟法（平成八年六月二十六日法律第百九号）第２２８条第１項により、文書を証拠として用いるためには、その成立の真正を証明しなければならない。

そこで、押印が行われた私文書を民事訴訟において、証拠として提出する場合には、証拠調べを請求する者は、その成立の真正を証明することが必要となる。

民事訴訟法第２２８条第４項は「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立したものと推定する」と規定しており、「本人の印鑑の押印があること」すなわち「押印に用いられた印鑑が本人のものであること」及び「本人が押印したこと」の証明が必要である。

このうち、「押印に用いられた印鑑が本人のものであること」については、通常、市町村が条例に基づき実施している実印の印影の登録制度（印鑑登録制度）が用いられており、争いになっている私文書に市町村が発行した印鑑登録証明書が添付されていれば、「押印に用いられた印鑑が本人のものであること」が事実上推定されるとされる。

また、「本人が押印したこと」については、印鑑登録証明書により本人のものとされる印鑑と同じ印影が書面上に存在していれば、「本人が押印したこと」が事実上推定される。これは、実印は本人が大切に保管するという慣習があり、実印が押されていれば、本人が押印したのだろうという経験則が働くためである。

また、文書の記載内容の改変の有無については、文書の成立の真正が証明されれば、特段の事情がない限り、文書の記載内容には改変がないことが事実上推定されるとされている。

III－２－２　電子署名が行われた電磁的記録の証拠力

民事訴訟法第２３１条で準用される同法第２２８条第１項により、電磁的記録等の準文書を証拠として用いるためには、その成立の真正を証明しなければならない。

そこで、電子署名が行われた電磁的記録についても、押印が行われた私文書と同様、民事訴訟において、証拠として提出する場合には、その成立の真正を証明することが必要となる。

この場合、本サービスに係る電子証明書により確認される電子署名のある電磁的記録について、どの程度の証拠力を認めるべきかを、押印が行われた私文書の場合と同様に、

・「電磁的記録の真正な成立」
・「電子署名に用いられた秘密鍵が本人が生成したものであること」
・「本人が電子署名を行ったこと」

それぞれの段階について、検討することが必要である。

Ⅲ－２－３　「電磁的記録の真正な成立」

民事訴訟法第２２８条第４項は、私文書について本人の署名・押印があるときは、当該私文書の成立の真正を推定していることから、本サービスに係る電子証明書により確認される電子署名のある電磁的記録についても、本人の署名・押印がある私文書と同等の証拠力を付与することが必要である。

電子署名法では、一定の電子署名がなされているときに、当該電磁的記録の真正な成立を推定する規定（同法第３条）をおいており、本サービスにおいても当該規定が適用され、本人による電子署名が行われているときは、当該電磁的記録は真正に成立したもの（特定人の意思に基づいて作成されたものであること）を推定する効果を与えるという取扱いが必要である。

Ⅲ－２－４　「電子署名に用いられた秘密鍵が本人が生成したものであること」

電子署名法において、一定の電子署名がなされているときに、当該電磁的記録の真正な成立を推定する規定（同法第３条）が適用されるためには、「電子署名に用いられた秘密鍵が本人が生成したものであること」及び「本人が署名したこと」を証明する必要がある。

本サービスの場合、次のような事情があり、サービスに係る有効な電子証明書により適格に検証された電子署名のある電磁的記録については、「電子署名に用いられた秘密鍵が本人が生成したものであること」が事実上推定される効果を有することが期待されるところである。

①原簿データを備えた市町村窓口において厳格な本人確認が行われるこ

と
②鍵ペアは、暗号の強度を確保し改変される可能性が少ない方法であって、利用者本人以外誰も関与しないもので生成されること
③同様に公的機関が発行する印鑑登録証明書よりも高い信頼性が求められていること
④大量に反復処理する必要がある行政手続等にあっては、予見可能性を確保する必要性が大きいこと
⑤電子署名については、手書きの署名・押印や印鑑登録制度のようなこれまでの歴史の積み重ねがないため、裁判において「事実上の推定」が認められるようになるには、相当な年月を要するのではないかと考えられること

Ⅲ－２－５　「本人が電子署名を行ったこと」

押印が行われた私文書の場合、「本人が押印したこと」については、これを推定する規定はおかれていないが、印鑑登録証明書により本人のものとされる印鑑と同じ印影が書面上に存在していれば、「本人が押印したこと」が事実上推定される。

一方、電子署名法においては、「本人が電子署名を行ったこと」を推定する規定はおかれておらず、また、電子署名は新しい制度であり、実印のように、「本人が大切に保管するという慣習があり、実印が押されていれば、本人が押印したのだろう」という経験則と同様の経験則がまだ確立していないことから、電子署名法による認定認証事業者が発行した電子証明書により確認される電子署名のある電磁的記録であっても、当然には、「本人が電子署名を行ったこと」は事実上の推定はなされず、本人が電子署名を行ったことに関する何らかの状況証拠が必要となると考えられる。

この場合、実印のような経験則は確立されていないものの、
◯鍵ペアは厳格な本人確認が行われた利用者本人が生成すること
◯印鑑登録制度とは異なり、利用者に対して、秘密鍵等の安全な管理・保管義務を課すこととしていること
等から、「本人が電子署名を行ったこと」は、事実上推定されることが期待される。

第３章　罰　則

本サービス制度の安全性・信頼性を担保するため、虚偽の発行申請を行い、不実の電子証明書の発行を受けた者を罰することについて、法定刑の在り方を含め、検討する必要がある。

なお、電子署名法においては、「虚偽の申込みをして、利用者について不実の証明をさせた者」に対して、「３年以下の懲役又は２００万円以下の罰金」を課す罰則を創設している。