公的個人認証サービス利用のための
民間事業者向けガイドライン

－第 1.1 版－

総務省

平成 27 年 9 月

修正箇所・内容一覧

版	発出	主な修正箇所・内容	修正の内容
1.0	７月	―	―
1.1	９月	・１８頁を修正 ・２０頁を削除	・強固な認証について記載を簡明化した。

― 目次 ―

1　本ガイドラインの背景と目的

(1) 本ガイドラインの背景（公的個人認証法の一部改正）

住民の利便性の向上及び行政運営の簡素・合理化を図るため、国や地方公共団体の行政手続等のオンライン化、いわゆる電子政府・電子自治体の実現に向けた取組みが進められてきている。行政手続等においては一般に、手続きを行う住民の本人確認を厳格に行うことが求められるが、一方でインターネットに代表されるデジタル社会では、なりすまし、改ざんなどの課題が指摘されている。こうしたデジタル社会の課題を解決しつつ、電子政府・電子自治体を実現するためには、確かな本人確認ができる個人認証サービスを全国どこに住んでいる人に対しても安い費用で提供することが必要なことから、「電子署名に係る地方公共団体の認証業務に関する法律」（以下、公的個人認証法という。）に基づく公的個人認証サービス制度が創設され、平成 16 年 1 月 29 日よりサービスが開始されている。

現行の公的個人認証法では、電子証明書の有効性を確認できる者（署名検証者等）の範囲については、行政機関、裁判所、行政手続の代理者、民間の認定認証事業者等に限定されている。この点を緩和し、より多くの者が公的個人認証サービスを使えるようにすることで、サービスの利用促進、ひいては国民・民間企業の利便性向上につながると考えられることから、公的個人認証法の一部改正が行われ、行政機関等に限られていた署名検証者等の範囲を総務大臣が認める民間事業者にも拡大することとなった。

(2) 想定対象者

公的個人認証サービスの活用を検討する民間事業者を想定対象者とする。

(3) 本ガイドラインの目的

民間事業者における公的個人認証サービスの利用検討を支援し、当該サービスの普及を促進するべく、以下について説明する。

① 公的個人認証サービスの概要
② 公的個人認証サービスのメリット
③ 公的個人認証サービス利用の手引き（案）
- 民間事業者側に必要となる情報システム設備
- 総務大臣による認定基準・手続
- 失効情報提供手数料

これらを簡明に示すことで、民間企業の利用検討を円滑にすることを目的とする。

２　公的個人認証サービスの概要

本章では、公的個人認証サービスの概要として、次の 4 点について記述する。

(1) 公的個人認証サービスとは
(2) 現在の公的個人認証サービスの利用ケース
(3) 公的個人認証サービスの改正のポイント
(4) 公的個人認証サービス利用の流れ

(1) 公的個人認証サービスとは

公的個人認証サービスとは、インターネット上での申請や届出を行う際に、第三者によるなりすましやデータの改ざんを防ぐために用いられる、本人確認手段を提供するサービスである。本人確認は、電子証明書と呼ばれる電子的な身分証明書を用いて行う。電子証明書は、外部から読み取られるおそれのない IC カード※1 に記録し、保持する。インターネット上での申請や届出を行う際に、IC カードから電子証明書を読み取り、これを利用して電子署名やユーザ認証を行うことができる※2。

公的個人認証サービスの利用の流れについては、本章の 「(4) 公的個人認証サービス利用の流れ」にて記述する。

※1 住民基本台帳カード又は個人番号カード（平成 28 年 1 月以降）を指す。
※2 現行の公的個人認証サービスでは、行政サービスのオンライン上での申請手続における、電子署名の機能のみが提供されている。なお、電子署名は紙での手続きにおける署名や押印に相当する。平成 28 年 1 月以降は、ユーザー認証の機能も追加的に提供される（(3)ウ「利用者証明用電子証明書の新設」を参照。）。

(2) 現在の公的個人認証サービスの利用ケース

現在、公的個人認証サービスを活用して利用できる主な行政サービスとして、以下が挙げられる。

・e-Tax（国税電子申告・納税システム）
・自動車保有関係手続
・住民票の写し等の交付請求等（一部市区町村のみ）

上記の中でも、「e-Tax（国税電子申告・納税システム）」は、平成 24 年度の利用件数が約 1,730 万件、e-Tax が利用可能な国税申告・納税においては 50%超が e-Tax を利用して行われている（いずれも国税庁ホームページより）ように、幅広く利用されている電子申請サービスである。利用者は、パソコンとインターネットの環境があれば、税務署に赴くことなく、国税に関する申告や納税を行うことができる。確定申告期については、24 時間の受付を実施しており、税務署の開庁時間帯以外でも申請を行うことができる。

e-Tax の概要は、図 2-1 のとおりである。図中の⑤で送信されるデータには電子署名及び電子証明書が添付され、データが適正に本人によって作成されたものであることが保証される仕組みになっている。

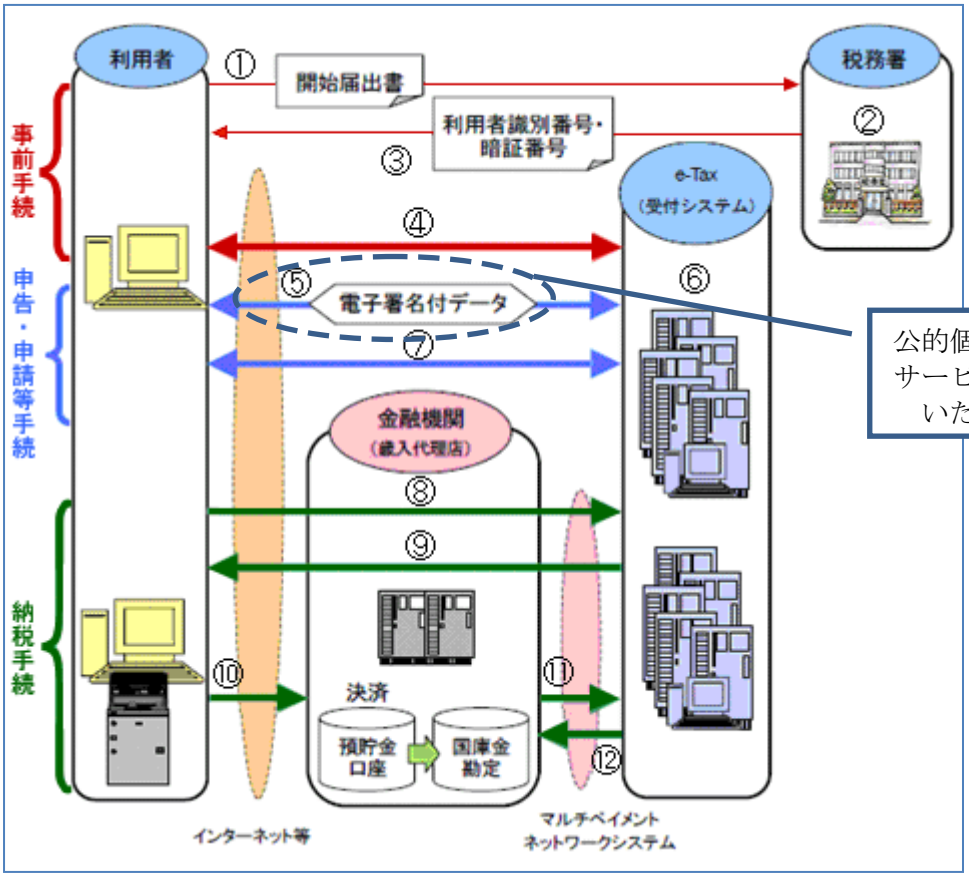


図 2-1 e-Tax の概要（出所 ： 国税庁ホームページ）

図 2-1 における①～⑫の詳細は、次のとおりである。

① 開始届出書の提出
② 審査登録
③ 利用者識別番号・暗証番号の取得
④ 暗証番号の変更、電子証明書等の登録／変更・登録した旨のメッセージ
⑤ 申告・申請等データ（電子署名付）の送信／データを受信した旨の通知
⑥ 受信データのチェック等／データのメッセージボックスへの格納
⑦ 送信データの確認等
⑧ 収納機関番号、利用者識別番号、納税用確認番号及び納付区分番号を送信
⑨ 納税者氏名、税目、課税期間及び納付金額等を通知
⑩ 納付指図
⑪ 領収済データの連絡
⑫ 領収済データ受信の通知

(3) 公的個人認証サービスの改正のポイント

平成 25 年 5 月 31 日に公布された社会保障・税番号制度関連四法によって、公的個人認証法の一部が改正された。改正法の施行日については政令にて別途定められるが、現時点では、平成 28 年 1 月からの施行が見込まれている。

公的個人認証サービスに関する主な改正のポイント 4 点を以下に記述する。

ア 公的個人認証サービスの対象を民間事業者へ拡大

現行制度では、公的個人認証サービスの利用は行政機関等に制限されているが、本改正に伴い、公的個人認証サービスの対象が民間事業者へ拡大される。ただし、民間事業者は、公

的個人認証サービスの利用に際し、総務大臣による認定を受ける必要がある。総務大臣による認定の基準については、本ガイドラインの第 4 章にて記述する。

イ 電子証明書格納媒体の変更

平成 25 年 5 月 31 日に公布された社会保障・税番号制度関連四法のうち、「行政手続における特定の個人を識別するための番号の利用等に関する法律」により、全国民に個人番号が付番されることとなる。市町村長は、当該市町村長が備える住民基本台帳に記録されている者に対し、その者の申請により、個人番号カードを交付する（平成 28 年 1 月開始）。個人番号カードの交付開始に伴い、住民基本台帳カードの発行が終了する。

上記の理由から、公的個人認証法の現行制度では、公的個人認証サービスで利用する電子証明書の格納媒体を住民基本台帳カードとしているが、個人番号カード交付開始後は、その格納媒体が個人番号カードに変更される。

なお、個人番号カード交付開始後においても、既に住民基本台帳カードに記録されている電子証明書の有効期間が切れるまでは、当該電子証明書を引き続き利用可能である。

ウ 利用者証明用電子証明書の新設

本改正に伴い、公的個人認証サービスで利用する電子証明書として、現行制度において既に提供されている署名用電子証明書に加え、利用者証明用電子証明書が新設される。

署名用電子証明書は、電子署名を行うことを利用目的とした電子証明書である。それに対して、利用者証明用電子証明書は、インターネット上で提供される各種 Web システムへのログイン認証等を利用目的とした電子証明書である。

署名用電子証明書と利用者証明用電子証明書では、その用途が異なるため、保持する情報に差異がある。主な差異は、電子証明書内に基本 4 情報を保持するか否かである。基本 4 情報とは、各個人の氏名、住所、性別及び生年月日を指す。署名用電子証明書は、行政手続の申請時等に電子署名用途で利用されるものであるが、その用途から、申請者の正確な住所等の確認に資する情報が求められるため、電子証明書内に基本 4 情報を保持する必要がある。一方、インターネット上のログイン認証等の用途で利用される利用者証明用電子証明書は、本人であることを確認できればよいため、基本 4 情報を保持する必要がない。これらを踏まえ、公的個人認証サービスで使用される電子証明書は、用途に応じて、必要以上の情報を保持しないように設計されている。

エ 電子証明書の発行者を地方公共団体情報システム機構に変更

現行制度では公的個人認証サービスで利用する電子証明書は、都道府県知事により発行されている。本改正に伴い、電子証明書の発行者が地方公共団体情報システム機構（以下、機構という。）に変更される。

(4) 公的個人認証サービス利用の流れ

公的個人認証法の改正後、公的個人認証サービスは、図 2-2 の流れで利用されることとなる。

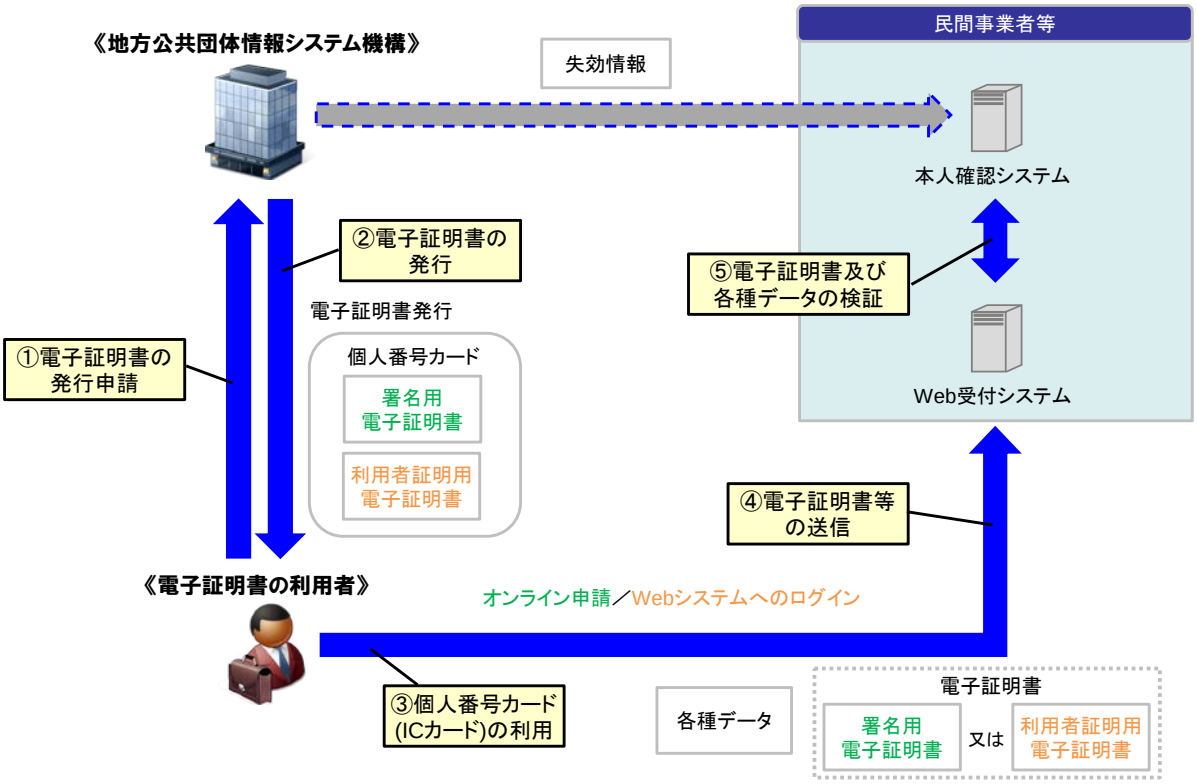


図 2-2 公的個人認証サービスの利用フロー

図 2-2 における①～⑤の詳細は、次のとおりである。

① サービスの利用を希望する者は、機構に対し電子証明書の発行申請を行う。
② 機構は、申請者に対して電子証明書を発行する。申請者は、各市町村窓口（市役所等）にて、発行された電子証明書を利用するためのパスワードを設定し、個人番号カードに記録された形で電子証明書を受領する。
③ 発行を受けた者は、オンライン申請、Web システムのログイン時等に、個人番号カード(IC カード)を IC カードリーダライタにセットし、電子証明書を利用するためのパスワードを入力する。
④ 発行を受けた者は、電子証明書、申請書等のデータを民間事業者等に送信する。
⑤ 民間事業者等は、機構から提供される電子証明書の失効情報等を用いて、電子証明書及び受領したデータの有効性の検証を行う。

上述のとおり、電子証明書の有効性を検証するに当たり、電子証明書の失効情報が必要となる。失効情報とは、電子証明書が失効状態にあるか否かを判定するための情報である。民間事業者は、機構へ失効情報提供手数料※3 を支払い、失効情報を入手して電子証明書が失効状態にあるかを判定する。また、電子証明書には有効期間が定められており、有効期間が過ぎたものは使用不可となって失効する。さらには、個人番号カードの紛失・盗難、婚姻による氏名変更、引越しによる住所変更等によって、たとえ有効期間内であっても電子証明書が失効する場合もある。

なお、利用者が個人番号カードを紛失した場合、電子証明書の失効及び再発行、並びに個人番号カードの一時停止及び再発行は公的機関で行われるので、民間事業者での対応は不要となる。利用者が個人番号カードを紛失し、電子証明書の失効及び再発行、並びに個人番号カードの一時停止及び再発行を行う場合の対応は、以下のように行われる。

Ⅰ．個人番号カードを紛失した利用者が、公的機関が運営するコールセンターへ連絡する。
Ⅱ．連絡を受けたコールセンターは、下記対応を行う。
　① 個人番号カードを利用できない状態（一時停止）とする。
　② 電子証明書を利用できない状態（失効状態）に変更する。

電子証明書の変更内容は、システム上で必要な処理が行われ、失効情報として民間事業者等に提供される。

Ⅲ. 個人番号カード及び電子証明書の再発行を希望する利用者は、市町村窓口にて個人番号カード及び電子証明書の再発行※4 の申請を行う。

Ⅳ. 再発行を申請した者は、再発行された個人番号カード及び電子証明書を市町村窓口にて受け取る。

※3 失効情報提供手数料については、第 4 章にて説明する。
※4 個人番号カードは市町村長によって、電子証明書は機構によって発行される。

(5) 公的個人認証サービスを利用した口座開設申込・取引の流れ

公的個人認証法の改正後、利用が可能となった民間事業者においては、多くの場合、初回に署名用電子証明書による口座等の開設申込を受け、２回目以降は利用者証明用電子証明書によるログインを受けるという活用方法になると想定される。その流れのイメージを図 2-3 に示す。

すなわち、初回、口座開設等の申込を受けるシーンでは、署名用電子証明書・電子署名を受け、申込者の実在性、氏名・住所等を正確・確実に把握し、かつ、申込書を安心して（改ざんや送信否認のおそれがないものとして）受け取ることができる（図 2-4 中、１）。次回以降のシーンでは、ログインしてきた者が、申込者本人であることを確認できれば十分であり、利用者証明用電子証明書・利用者証明を受ける（図 2-4 中、２）※5。

※5 次回以降のシーンで、必ず利用者証明を受けなければならないことはない。初回登録時に ID・パスワードを発行し、単なるログインの際には ID・パスワードにより認証を行い、送金などの取引の場面において、改めて利用者証明を受けるといったように、認証レベルは民間事業者が自由に定めることができる。

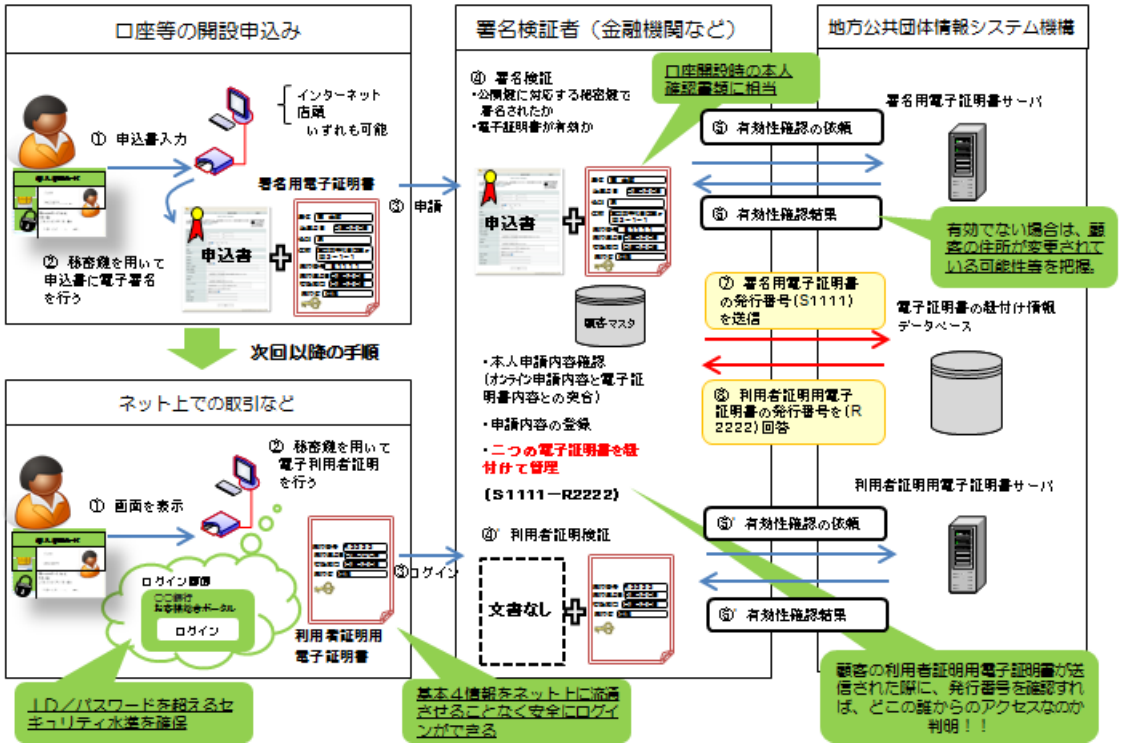


図 2-3 新しい公的個人認証サービス（署名と利用者証明）利用フロー（イメージ）

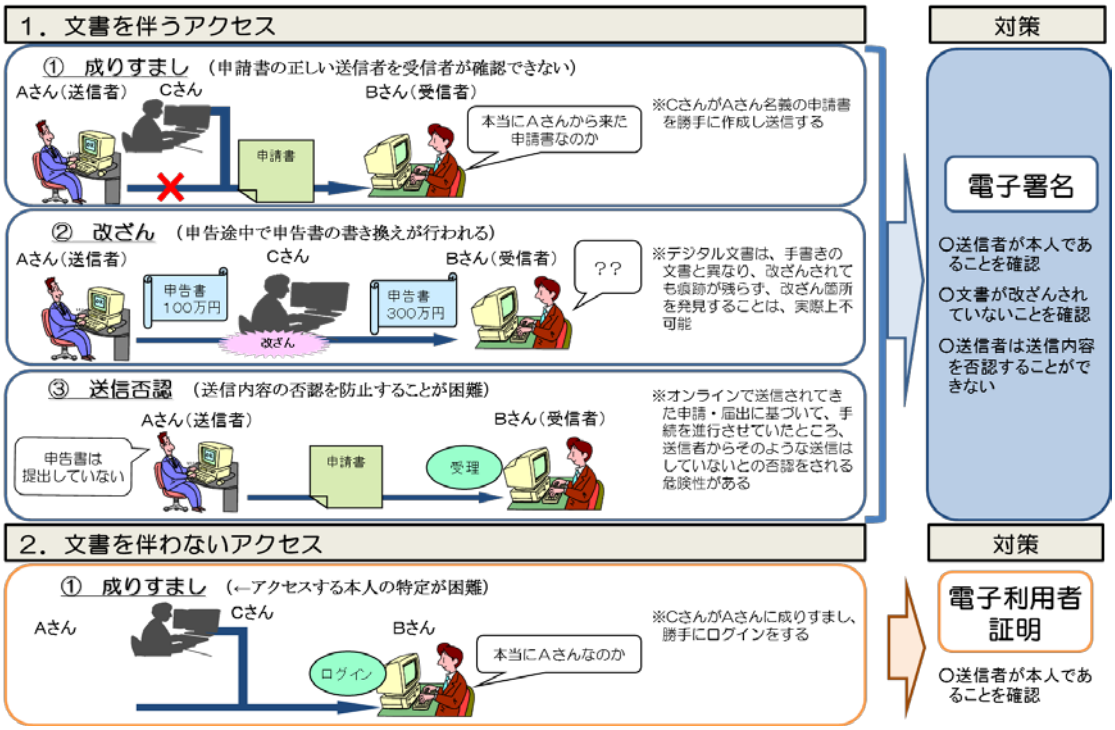


図 **2-4** 安全、安心な認証サービスの提供（電子署名と電子利用者証明）

3　公的個人認証サービスのメリット

本章では、民間事業者が第 2 章で説明した公的個人認証サービスを利用することによって得られるメリットについて記述する。

(1) 公的個人認証サービスのメリット

本項では、民間事業者が公的個人認証サービスを利用することによって得られるメリットとして、下記 2 点を記述する。

① 公的個人認証サービスの電子証明書活用のメリット
② 同等サービスを民間事業者が自前で構築する場合と比較した際のメリット

ア 公的個人認証サービスの電子証明書活用のメリット

(ｱ) 署名用電子証明書活用のメリット

署名用電子証明書を利用することで、個人が民間事業者へ提出する電子文書（各種申請書等）に対して、電子署名を付することが可能になる。

電子署名を付することによって、民間事業者では表 3-1 に示す内容が実施可能となる。

表 3-1 電子署名により実現可能となること

項番	実施可能となること	詳細
1	なりすましの防止	受領した電子文書が、提出者本人の作成に係るものであることを確認できる。
2	改ざんの防止	受領した電子文書が、第三者による改変が行われていないことを確認できる。

電子署名が可能になることによって、これまで対面での本人確認（運転免許証の確認等）を要していた業務が、インターネット経由によるオンラインで実施可能となる。これにより、民間事業者には、たとえば、表 3-2 に示すようなメリットが期待される。

表 3-2 署名用電子証明書活用による民間事業者のメリット

項番	メリット	詳細
1	費用削減	郵送費や人件費等の費用削減 （例） 本人確認資料の郵送費、店頭の人件費、書類の保管経費が削減可能となる。
2	利用者満足度の向上	申請手続の受付時間拡大 （例） 対面での本人確認が不要になることによって、平日昼間以外でも申請手続が可能となる。
3		オンラインでの手続完結 （例） 対面での本人確認や、本人確認資料の郵送が不要になる。それに伴い、民間事業者が提供する各種サービスの利用開始をオンラインで申し込んだ後、即時に利用開始できる。

(ｲ) 利用者証明用電子証明書活用のメリット

利用者証明用電子証明書を利用することで、オンラインで利用者本人であることを証明すること（電子利用者証明）が可能となる。

一般的に、本人認証の方法は、表 3-3 に示す 3 種類の方法に大別できる。

表 3-3 本人認証方法

項番	認証方法	詳細
1	知識認証	本人しか知りえない知識を提示できるかにより、本人か否かを判断する。 （例）ID・パスワードによる認証
2	所有物認証	本人しか持っていない所有物を提示できるかにより、本人か否かを判断する。 （例）IC カードによる認証、USB トークンによる認証
3	生体認証	指紋や静脈、虹彩など、本人の身体的な特徴を照合することにより、本人か否かを判断する。 （例）指紋認証、静脈認証、虹彩認証

公的個人認証サービスの電子利用者証明では、個人番号カードを所有していることによる認証（所有物認証）に加え、IC チップ内の電子証明書等にアクセスするためのパスワードによる認証（知識認証）を併用可能である。これは、2 種類の異なる方法を組み合わせた認証（多要素認証）であり、1 種類だけを使う場合よりも高いセキュリティが確保される。

民間事業者は、利用者証明用電子証明書を利用することによって、自社が個人向けに提供しているインターネットサービスにおいて、ID・パスワードによる認証よりもセキュリティの高いログイン認証が利用可能となる。これにより、民間事業者には、たとえば、表 3-4 に示すようなメリットが期待される。

表 3-4 利用者証明用電子証明書活用による民間事業者のメリット

項番	メリット	詳細
1	セキュリティの向上	インターネットサービスにおけるセキュリティの高いログイン認証
2	費用削減	インターネットサービスにおけるパスワードを利用者が失念した際の対策費用削減 ➢ 対策を必要とする対象が減少 個人番号カードによる認証の利用者増加に伴い、パスワードによるログイン認証利用者が減少する。 ➢ 利用者が個人番号カードのパスワードを失念した際の対策は不要 個人番号カードのパスワード失念に関する問い合わせは、機構が対応する。
3	利用者満足度の向上	インターネットサービスにおけるパスワード多重管理の負担削減 ➢ 個人番号カードのパスワードのみの管理 インターネットサービスごとに利用者はパスワードを管理していたが、公的個人認証サービスの利用により、個人番号カードのパスワードの管理のみとなる。

イ 同等サービスを民間事業者が自前で構築する場合と比較した際のメリット

民間事業者が電子証明書を利用するに当たっては、公的個人認証サービスを利用する方法以外に、民間事業者各社が独自で認証局を構築して電子証明書を発行する方法も考えられる。

公的個人認証サービスの利用は、民間事業者が独自で認証局を構築・運用する場合と比較し、品質（Quality）・費用（Cost）・時間（Delivery）の面でメリットがあると想定される。

(ｱ) 品質面のメリット

公的個人認証サービスでは、信頼度の高い住民基本台帳で管理される基本 4 情報（氏名、住所、性別及び生年月日）を基に、機構から発行された電子証明書及び最新の電子証明書の失効情報によって認証が行われる。最新の住民基本台帳の情報を基にした失効情報を管理するため、利用者の最新の状況を踏まえた認証が可能となる。これに対し、民間事業者が独自で認証局を構築・運用する場合は、住民基本台帳で管理される基本 4 情報は利用できないため、利用者からの申告がない限り、最新の状況を踏まえた認証を行うことができない。したがって、公的個人認証サービスを利用することによって、民間事業者が独自で認証局を構築・運用する場合と比較し、信頼度の高い本人確認が可能となる。

(ｲ) 費用面のメリット

認証局は、電子証明書発行申込の受付、申込者の本人確認、電子証明書の発行、紛失時における電子証明書の失効等を行う。これらを行うためにはシステムの導入が必須であるため、認証局を構築・運営する上では、業務担当者の人件費に加えて、相応のシステム関連費用が必要となる。

民間事業者が独自で認証局を構築・運営する場合は、前述の費用を民間事業者が単独で負担する必要があるため、負担額は大きなものとなる。それに対し、機構が提供する公的個人認証サービスを利用する場合は、民間事業者は認証局システム構築費用を負担せずに済むとともに、サービスを利用する上で民間事業者が継続的に機構へ支払う費用についても、民間事業者が独自で認証局を運営する場合の運営費用より少なくなることが想定される。したがって、公的個人認証サービスの利用によって、民間事業者は、独自で認証局を構築・運営する場合と比較し、安価な費用で電子証明書を利用することが可能となる。

(ｳ) 時間面のメリット

(ｲ)で述べたとおり、認証局の運営にはシステムの導入が必須であるため、民間事業者が独自で認証局を構築し、運営を開始するためには多くの時間を要する。

公的個人認証サービスを利用する場合、民間事業者による認証局の構築は不要であり、公的個人認証サービス利用に向けたシステム対応のみを検討すればよい。また、民間事業者が提供するサービスの利用者側に関しても、民間事業者から電子証明書の発行を受ける必要がないため、サービスの利用開始までに要する時間が短縮される。したがって、公的個人認証サービスの利用によって、民間事業者が独自で認証局を構築する場合と比較し、サービス利用開始までの時間を大幅に短縮することが可能となる。

表 3-5 民間事業者における公的個人認証サービス利用のメリット

項番	観点	公的個人認証サービス	独自構築
1	品質面 (Quality)	基本 4 情報を利用した電子証明書及び最新の失効情報による本人確認が可能。	基本 4 情報を利用した電子証明書及び最新の失効情報による本人確認ができない。
2	費用面 (Cost)	認証局の初期構築費用及び運用費用が発生しない。※1	認証局の初期構築費用及び運用費用が発生する。
3	時間面 (Delivery)	認証局を構築する時間が不要。 システム対応の検討時間が必要。	認証局を構築する時間が必要。 システム対応の検討時間が必要。

※1 ただし、公的個人認証サービスの利用料（失効情報提供手数料）は発生する。

(2) 民間事業者の公的個人認証サービス利用によるメリット

本項では、民間事業者の公的個人認証サービス利用によるメリットをより具体的に分析して記述する。

ア ４つのメリット

民間事業者の公的個人認証サービス利用によるメリットは、図 3-1 に記載する４つであると整理できる。以下、４つのメリットについて、それぞれ順に、イ以下で説明する。

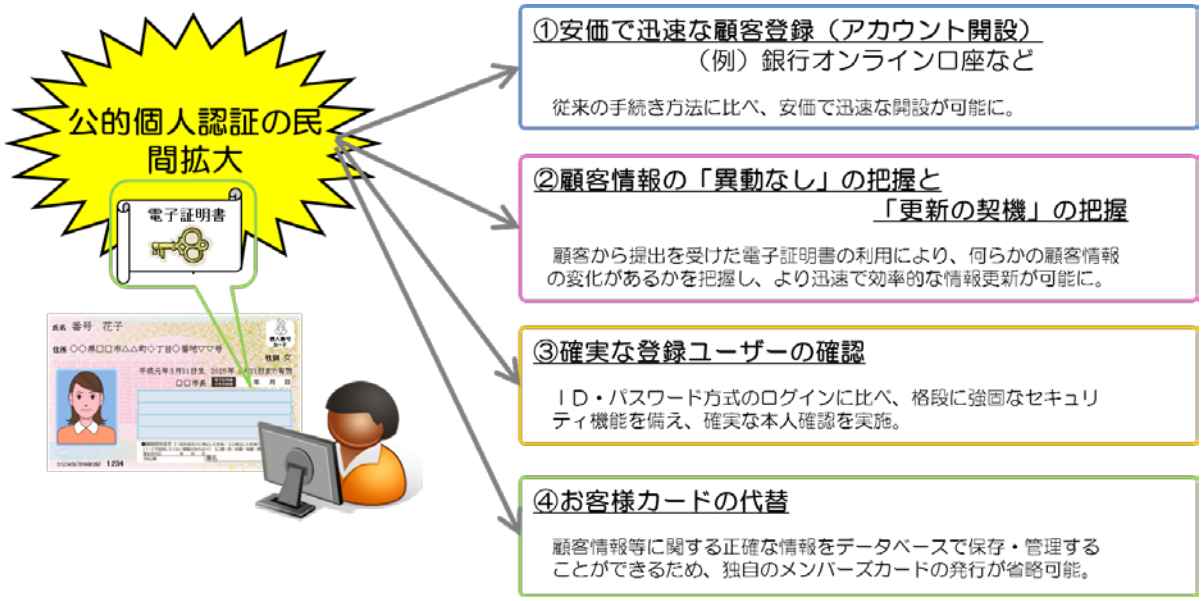


図 3-1 民間事業者の公的個人認証サービス利用による４つのメリット

イ メリット①：正確・迅速・安価な顧客登録が可能に

(ｱ) 現在、運転免許証等のコピーの郵送を受けている事業者について

民間事業者の公的個人認証サービス利用のメリットの第１として、「正確・迅速・安価な顧客登録（アカウント開設）が可能に」なる点が挙げられる。

従来の方法は（図 3-2 上段)、申込者の実在性、氏名・住所等の確認のため、運転免許証等のコピーを郵送してもらう必要があり、例えば、銀行の場合、利用申込から開始まで数週間が必要であり、コストも１回の手続につき 500～1,000 円程度発生する。

この点、民間事業者が公的個人認証サービスを利用し、署名用電子証明書・電子署名を受け、利用申込を受ける場合には、申込者の実在性、氏名・住所等を確実に確認できるので、別途、郵送等による本人確認書類の提出を求める必要はない※2。申込者は申込後、直ちに利用が可能であり、コストも大幅に削減できる（図 3-2 下段)。なりすまし等による被害がないという安心感もあり、申込拡大も期待できると考えられる。

※2 銀行等の口座開設や携帯電話の販売など、法令により本人確認が義務づけられている様々なものがあるが、概ね電子署名がその方法の一つとして位置づけられる見込みである。

(ｲ) ア以外の事業者について

現在、特に身分証明書の郵送を求めず、申込者の申告する氏名・住所等を登録している事業者においても、新たに公的個人認証サービスを利用し、正確な顧客情報を把握するメリットは大きいと考えられる。

例えば、現在、多くのオンラインショッピングでは、不払いをおそれ、支払確認の後に、商品を発送していると思われる。

この点、公的個人認証サービスを利用する（利用登録シーンで、署名用電子証明書・電子署名を受け、申込者の実在性、正確な氏名・住所等を確認し、販売シーンで、利用者証明を受け、本人の同一性を確認する）こととすれば、販売後直ちに、商品を発送することも可能になると考えられる。

また、（２）で述べる顧客情報の「異動の有無」の把握を行い、継続的に正確な顧客情報を把握すれば、継続的に顧客にセール情報等の提供を行うことができる。

あるいは、結婚紹介、SNS、インターネット調査をはじめ、事業の特性から、利用者の実在性、氏名・住所等が正確に把握できれば、大きな発展が期待できるインターネット等サービスは多々あるのではないかと思われる。

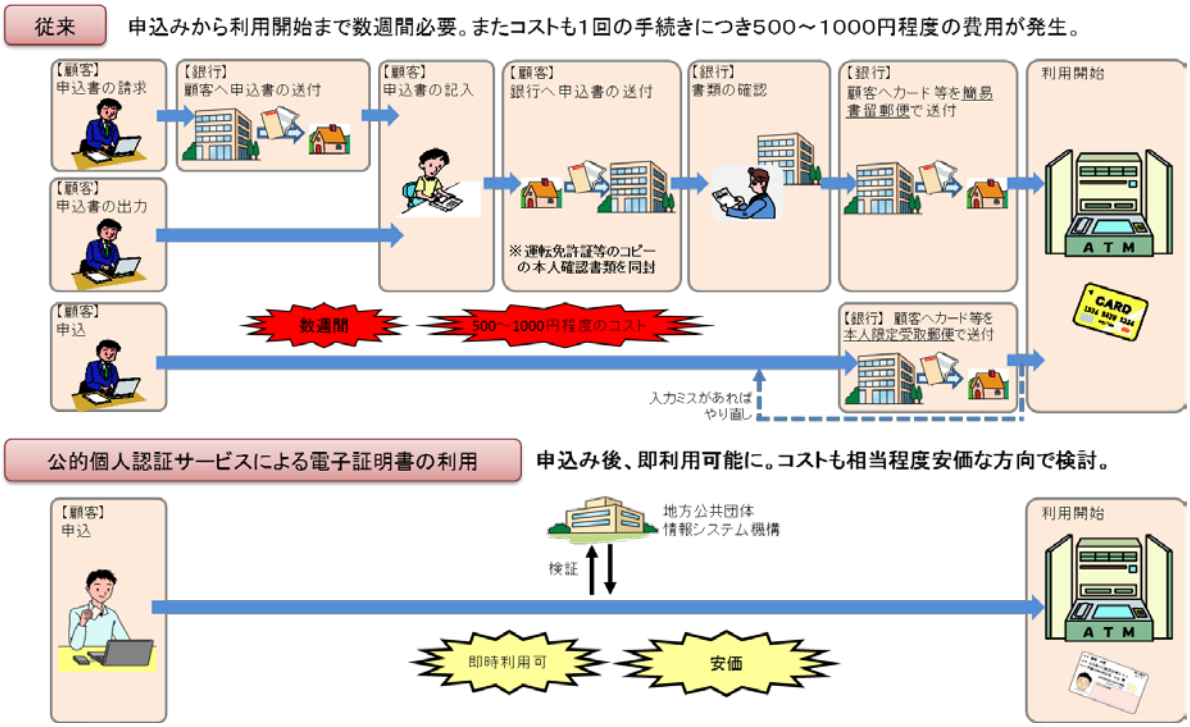


図 3-2 顧客登録のビフォー・アフター

ウ メリット②：顧客情報の「異動の有無」の把握が可能に

(ｱ) 現在、一定期間ごとに郵便で現況確認等を行っている事業者について

民間事業者の公的個人認証サービス利用のメリットの第２として、『顧客情報の「異動の有無」の把握が可能に』なる点が挙げられる。

従来の方法は（図 3-3 左欄）、例えば、ユーザー登録の一年経過時などに、全てのユーザーに郵便で現況確認を行い、これにより現況確認ができない場合には実地調査を行い、異動の有無を把握し、登録情報を更新するというものであり、現況確認のための郵便料金等や実地調査のための人件費など、相当のコストを要する。

この点、民間事業者が公的個人認証サービスを利用し、顧客の同意を得て、一定期間ごとに電子証明書の失効の有無を確認すれば、顧客情報の異動の有無をある程度の理由も含め把握することができ（図 3-4）、これまで生じていたコストカットが可能である※3。

※3 なお、異動後の住所・氏名等の把握は、顧客情報変更届を更新後の署名用電子証明書・電子署名とともに送信してもらう方法や、個人番号カードの入力補助アプリケーションに記録された情報を送信してもらう方法により、正確・迅速な取得が可能である。

(ｲ) アのうち、生命保険会社について

『顧客情報の「異動の有無」の把握』が可能になるという公的個人認証サービス利用のメリットは、例えば、生命保険会社において大いに活かせると考えられる（図 3-5）。まず、死亡保険であれば、定期的に電子証明書の失効の有無を確認することで、未払いリスクを回避できる。また、年金保険であれば、支払いの都度、電子証明書の失効の有無を確認することで、死亡等の事実がないことを確認して支払うことができるため、現在、大きなコストとなっている過誤払金を無くすことができる。

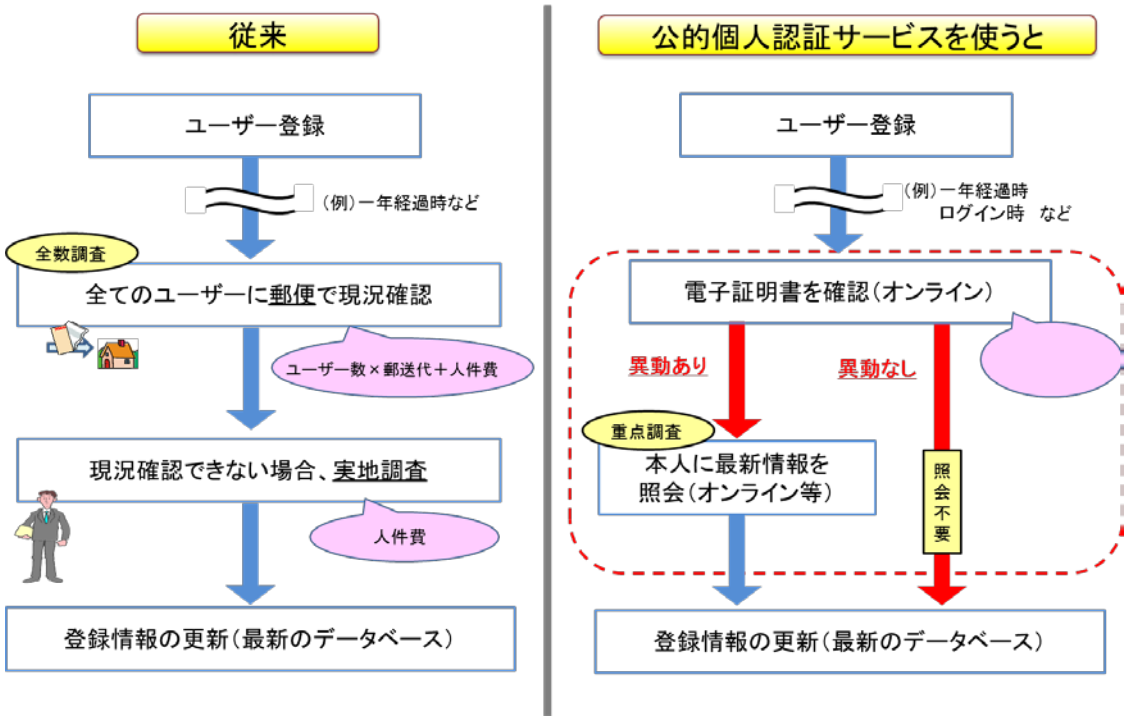


図 3-3 顧客情報の異動の把握ビフォー・アフター

	署名用電子証明書	利用者証明用電子証明書
①	氏名、住所等の変更 ※住民票の基本4情報（氏名、生年月日、性別及び住所）の記載が修正された場合に失効	（失効しない）
②	本人の死亡等 ※住民票が消除される場合に失効 →死亡、国外転出、住基法適用外（外国人が在留資格を喪失した場合等）となったとき　等	同左
③	本人の申出 （ア）個人番号カードの失効に伴う利用停止の届出 →カードの紛失・盗難、カードの有効期限到来、個人番号の変更　等 （イ）電子証明書の利用停止、秘密鍵の漏えい等	同左
④	電子証明書の有効期限到来 ※有効期間は原則5年 →5年以内に個人番号カードの有効期限が到来する場合は、個人番号カードの有効期限まで →利用者証明用電子証明書の有効期限と一致	同左

※未成年者、被成年後見人は、利用者証明用電子証明書のみ取得。
それ以外の場合でも、2種類の電子証明書のどちらか一方のみ取得する場合あり（ただしレアケース）。
※上記のほか、電子証明書に記録誤り又は記録漏れがあった場合等に失効。

署名用　：×失効
利用者証明用　：○有効
↓
住所・氏名等の確認手続へ
→①更新後の署名用電子証明書を送信してもらう
②個人番号カードの入力補助アプリの記録情報を送信してもらう

署名用　：×失効
利用者証明用　：×失効
↓

電子証明書の失効理由	分かること
affliationChanged	「死亡」又は「海外転出」
cessationOfOperation	「カード紛失」又は「海外転出」
Superseded	「証明書更新」
certificateHold	「カード紛失」

各事業者の登録時情報（電子証明書）でチェックが可能

図 3-4 電子証明書が失効する場合とそれぞれの場合に応じた採るべき対応

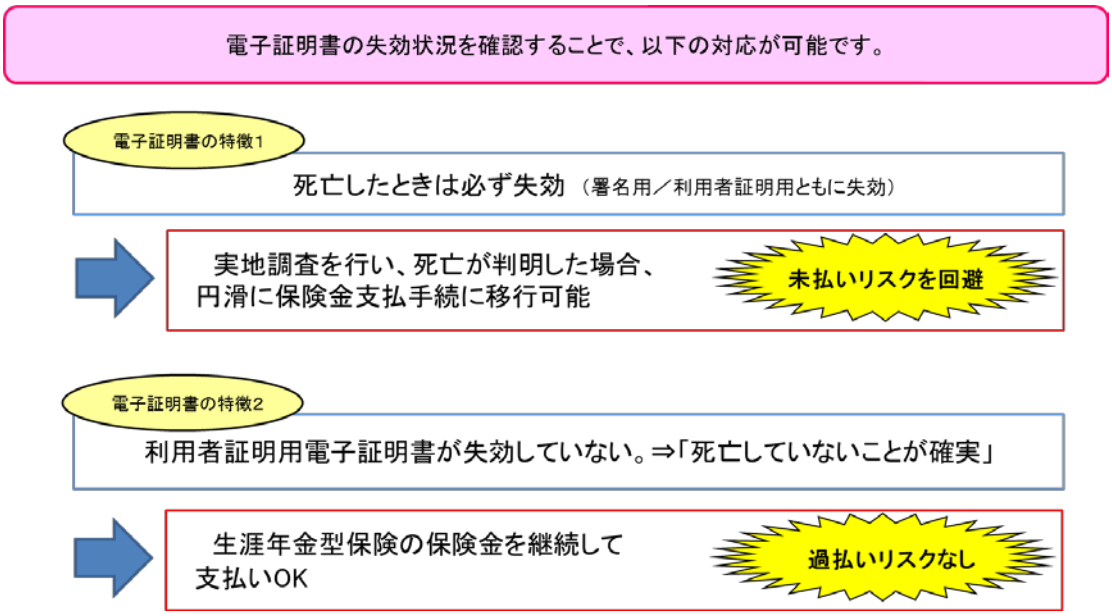


図 3-5 生命保険会社におけるメリット

(ｳ) ア・イ以外の事業者について

ア・イ以外の事業者（定期的な現況確認をそもそも行っていない事業者）は、正確な顧客情報の継続的な把握が困難なため、顧客の転居等を契機に、顧客を失ってしまう場合も多かったと考えられる。

この点、公的個人認証サービスを利用する（一度、署名用電子証明書を受け、定期的に、変更確認を行う）こととすれば、本人の同意の下で、継続的に、正確な住所へのダイレクトメールの送信等が可能になり、再度の購買につなげる等が期待できると考えられる。

(ｴ) 対面取引でも、既存の登録者でも、サービスの利用が可能

こうしたメリットは、インターネット等取引や、新規の登録者に限るものではない。例えば、イで述べた生命保険など、既存の登録者に対し、公的個人認証サービスによる変更確認同意書を、署名用電子証明書・電子署名とともに、生保営業担当者がタブレットをもって回り、対面営業により求めることが考えられる。公的個人認証サービスを利用して変更確認を行うことにより、登録者の負担が減るばかりではなく、事業コストが削減できるので、保険料の削減という形で還元することも可能だと思われる。利用者の満足度が向上し、事業の発展に寄与すると考えられる。

エ メリット③：確実な登録ユーザーの確認が可能に

(ｱ) 従来の方式（ＩＤ・パスワード方式）より、はるかに強固

民間事業者の公的個人認証サービス利用のメリットの第３として、「確実な登録ユーザーの確認」が可能になる点が挙げられる。

従来の方法（図 3-6 上段）は、悪意のある第三者に ID・パスワードが詐取され、なりすましが行われる危険がある（例えば、犯罪者が、他人のオンラインバンキングの ID・パスワードを詐取し、その口座から犯罪者の口座に不正送金を行うといったものであり、近年、こうした事件の急増が報告されている。）。

この点、公的個人認証サービスの場合、電子署名又は電子利用者証明に必要となる秘密鍵は、個人番号カードの IC チップに記録され、その外へは決して出ない（電子署名又は電子利用者証明も IC チップの中で行われる）ので、盗まれることはない。

万が一パスワードが探知されても、カードを所持していなければ、決してなりすましできないので、はるかに強固な認証手段であるといえる（図 3-7）※4。

※4 カードを所持しなければ決して利用できないとしても、カード盗取や遺失を考えると、類推されにくパスワードを設定し、適切に管理することが重要である。なお、仮に遺失等の場合には、２４時間３６５日のコールセンターに連絡すれば、電子証明書の利用を停止し、第三者の悪用を防止できる。

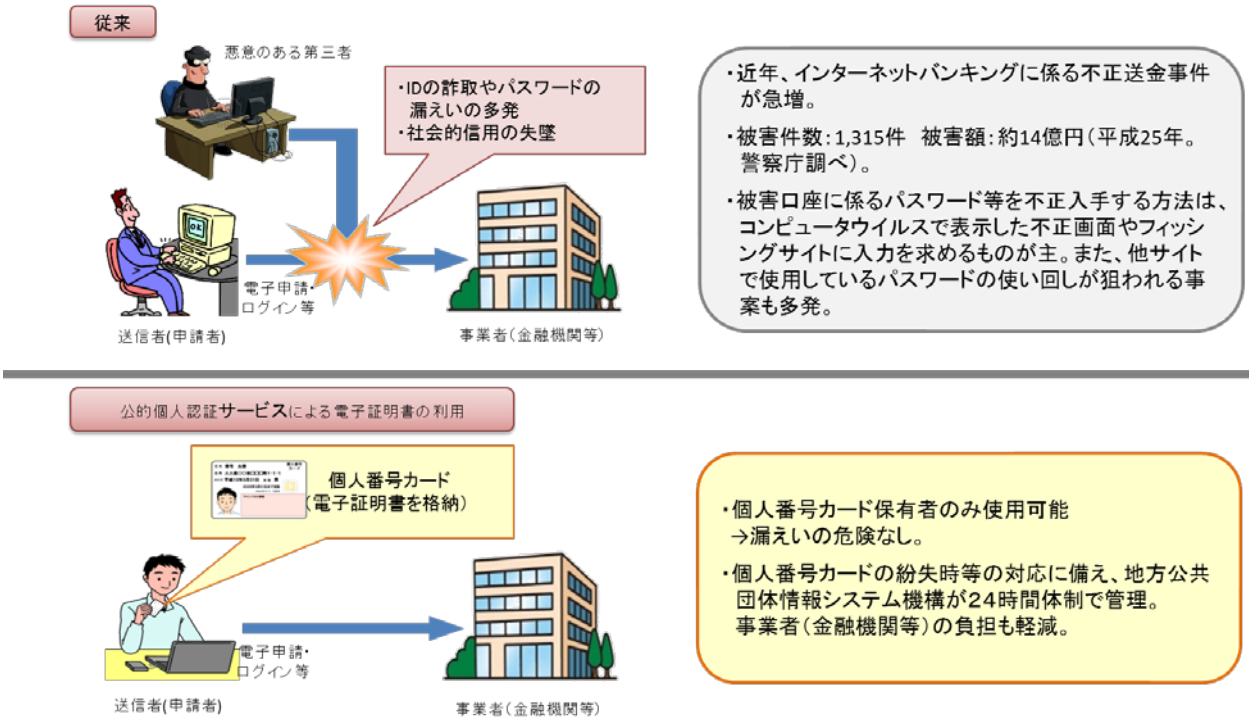


図 3-6 登録ユーザーの確認ビフォー・アフター

	ＩＤ・パスワード	公的個人認証サービス	
		利用者証明用電子証明書	署名用電子証明書
方法	○利用者がＩＤ・パスワードをキーボードで入力。通常、数文字程度の英数字。	○　個人番号カードに電子証明書と秘密鍵を記録。	
		○パスワード（４桁の数字）を入力した上で、乱数を利用者証明用の秘密鍵で暗号化。	○パスワード（６～１６桁の英数字）を入力した上で、確定申告書等の文書を署名用の秘密鍵で暗号化。
危険性	○スパイウェア、フィッシングの蔓延等により、ＩＤ・パスワードが抜き取られる恐れあり。 ○生年月日や電話番号などからの類推、無作為入力によるヒットのおそれあり。 ○利用するシステムが増えるほど管理が甘くなる可能性が高まる（例：パスワードをメモ）。	左のような危険性はない。 ○秘密鍵は、個人番号カードのＩＣチップに記録。秘密鍵は、一度記録すると絶対に外に取り出せないため（耐タンパ性）、第三者が取り出して使うことは不可能。 ※盗用するためには、①本人の個人番号カードを所持した上で、②本人の設定した暗証番号を入力する必要あり。 ○異なるシステムでも同一の電子証明書を安全に使用可能。	
その他	－	－	○電子署名法に基づき、電子署名により、電子文書が真正に成立したとの法律上の推定効が発生。

図 3-7 ID パスワードと公的個人認証サービスの違いについて

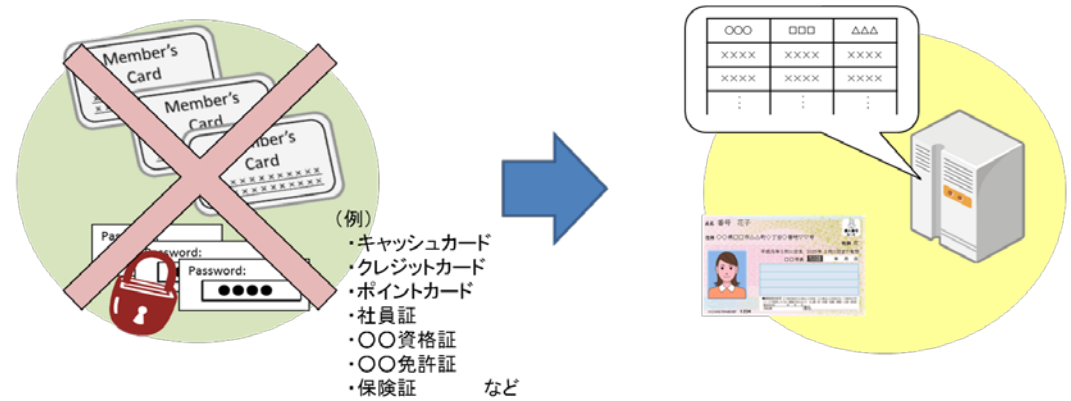
オ メリット④：お客様カードの発行が不要に

民間事業者の公的個人認証サービス利用のメリットの第４として、「お客様カードの発行が不要に」なる点が挙げられる（図 3-8）。

従来は民間事業者自らがお客様カードを発行し、遺失時の一時停止を含め、その運用を管理する必要があり、相当のコストを要していたところである。

この点、公的個人認証サービスを活用する場合には、お客様カードは不要となり、相当のコストを削減することが可能となる。万が一、落としたお客様は、２４時間３６５日のコールセンターに電話すれば、１５分以内[※5] というスピーディな一時停止が可能ですが、この運用コストも、民間事業者が特段の負担を求められるものではない。

※5 OCSP 方式により失効情報の提供を受ける場合。OCSP 方式により提供される失効情報は、１５分単位で更新される。一方、CRL 方式により提供される失効情報は、一日単位で更新される。



・公的個人認証サービスによる電子証明書の提出を受ける事業者は、顧客情報とともに電子証明書の有効性に関する正確な情報をデータベースで保存・管理することが可能。

・また顧客も電子証明書が格納された個人番号カードを持っていればよいため、お客様カードを発行する必要がなく、コストの削減が可能。

・事業者自らがパスワードを管理する必要がなく、コストの削減が可能。

図 3-8 お客様カードが不要に ビフォー・アフター

カ 民間事業者のための公的個人認証サービスの付加サービス

(ｱ) 利用者証明用電子証明書の新旧シリアル番号の紐付けサービス（平成 29 年１月提供開始予定）（図 3-9）

民間事業者の要望を踏まえたサービスである。利用者証明用電子証明書を更新する場合、そのシリアル番号（発行番号）が変わるため、更新前後の同一性を民間事業者においては判断できず、再度、利用者登録からやり直す必要が生じるという課題があった。

この点、利用者の同意を前提として、民間事業者が不知のシリアル番号のログインがあった場合に、その一代前のシリアル番号を民間事業者が J-LIS に問い合わせ、J-LIS がこれを回答し、民間事業者が利用者の同一性を把握できるサービスを提供する予定である。

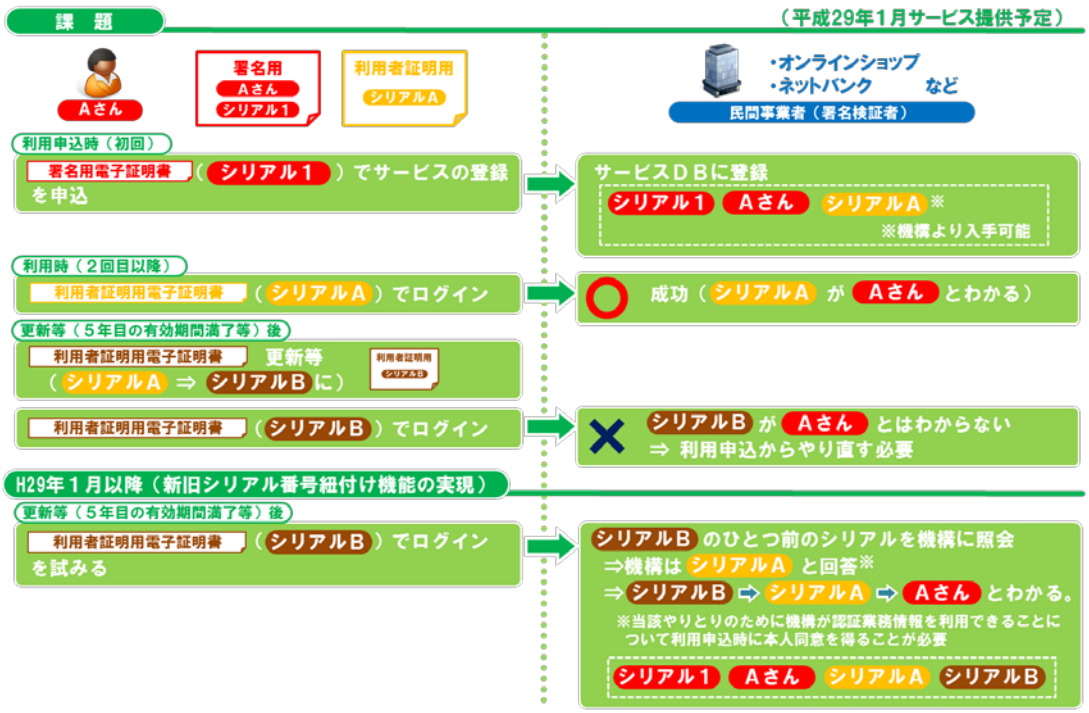


図 3-9 利用者証明用電子証明書の新旧シリアル番号の紐付け実現について（イメージ）

(ｲ) 年齢判定サービス※6（平成 29 年１月提供開始予定）（図 3-10）

民間事業者においては、酒やたばこなどの販売や、高齢者割引・子供料金など、利用者の年齢の判定を必要とする様々な事業があると考えられる。公的個人認証サービスでは、利用者の同意を前提として、「○歳以上か否か」について「Ｙｅｓ/Ｎｏ」を回答するサービスを提供する予定である。

※6 図 3-12 は自動販売機・券売機などのイメージであるが、インターネットサイト等の非対面や、対面についても、同様に可能である。

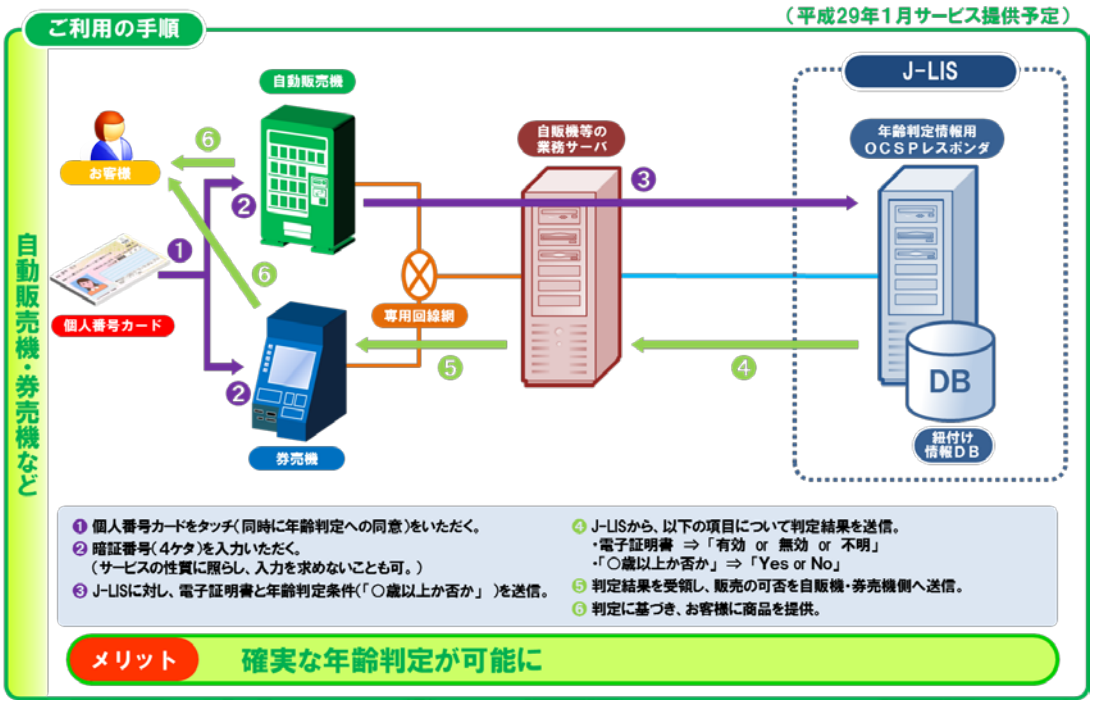


図 3-10 年齢判定機能について

4　公的個人認証サービス利用の手引き（案）

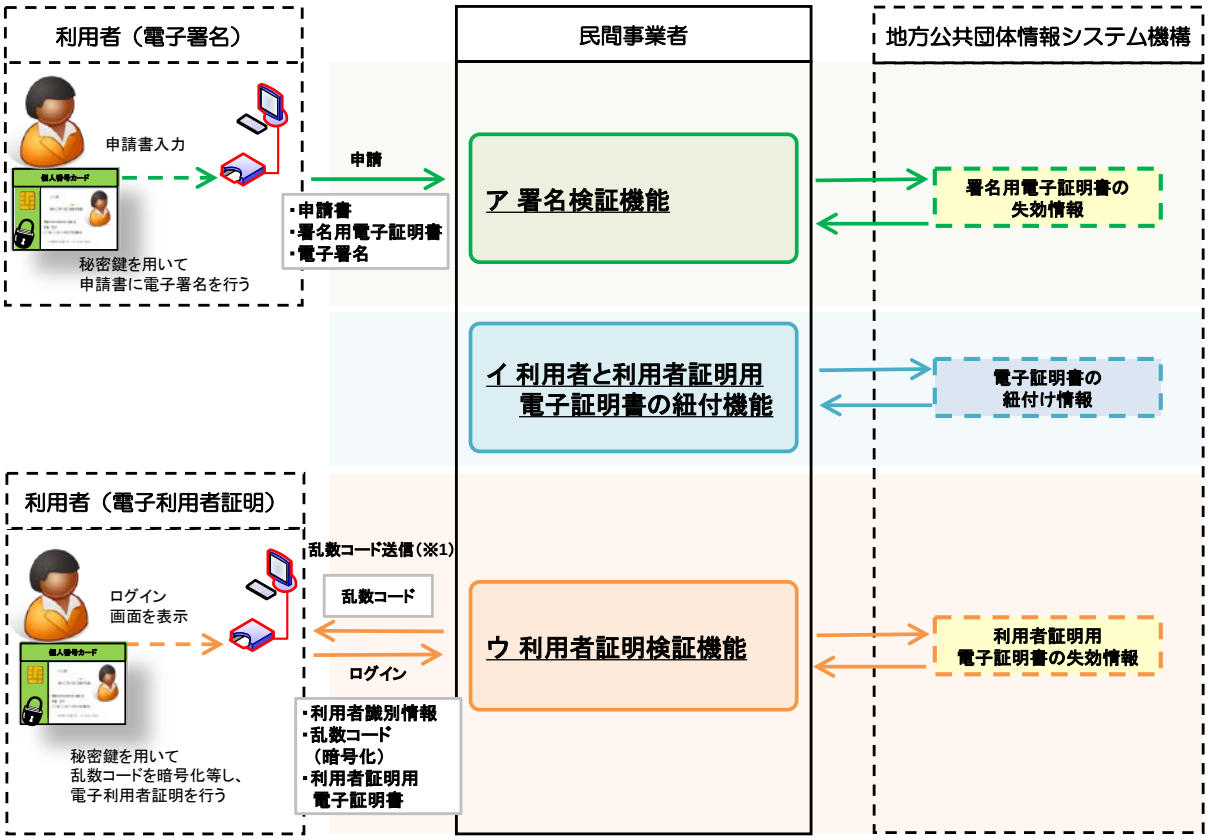
本章では、民間事業者が公的個人認証サービスを利用するための手引き（現時点の案）として、次の 3 点について記述する。

(1) 民間事業者側システム要件
(2) 総務大臣による認定
(3) 失効情報提供手数料

(1) 民間事業者側システム要件

本項では、公的個人認証サービスを利用するに当たって、民間事業者が準備するシステムについて説明する。

公的個人認証サービスのシステム全体の流れを図 4-1 に示す。



※1 「【APPENDIX ②】利用者証明機能の技術解説」の(ウ)参照

図 4-1 公的個人認証サービスのシステム全体の流れ

民間事業者側システムに必要となる機能は、公的個人認証サービスの利用目的により異なる。

■ 「電子署名」を利用する場合に必要となる機能
　ア　署名検証機能

■ 「電子利用者証明」を利用する場合に必要となる機能
　ア　署名検証機能
　イ　利用者と利用者証明用電子証明書の紐付機能
　ウ　利用者証明検証機能

なお、電子利用者証明を利用する場合において、「ア 署名検証機能」は必須ではないが、「イ 利用者と利用者証明用電子証明書の紐付機能」の効果的な実装を行う上で、署名検証機能が必要となる。効果的な実装の詳細は「4.(1).イ 利用者と利用者証明用電子証明書の紐付機能」を参照のこと。

前述のア～ウの機能について以下に記述する。

ア 署名検証機能

利用者から受信した署名用電子証明書及び電子署名を検証するための機能である。電子署名の流れを図 4-2 に示す。

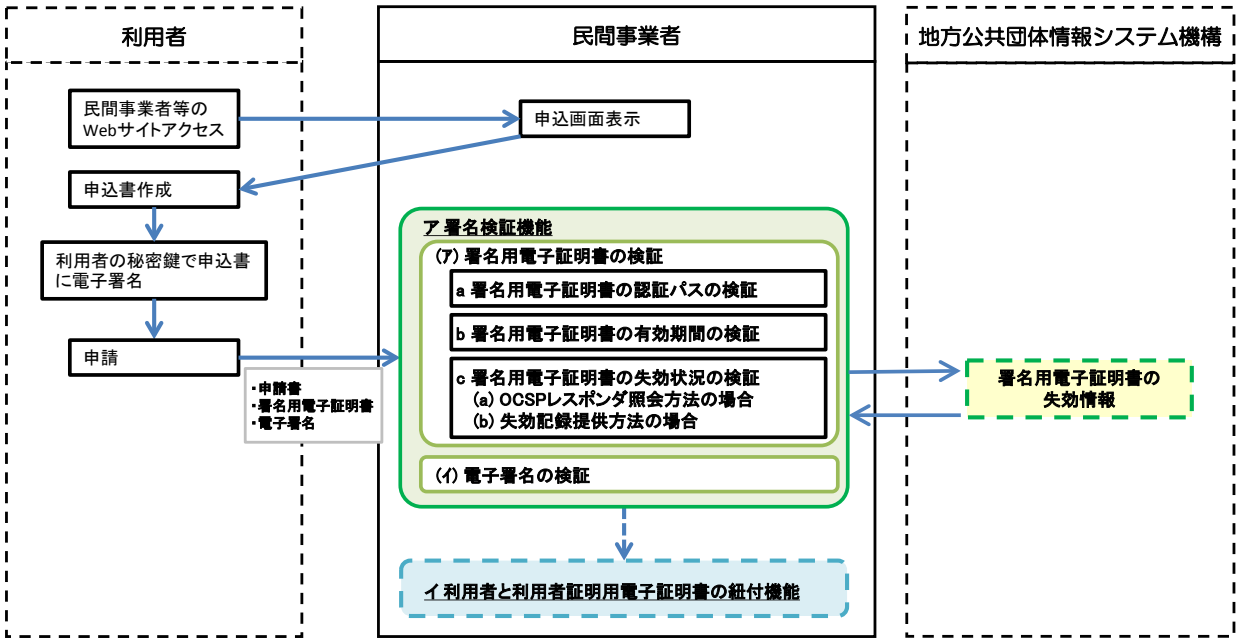


図 4-2 電子署名の流れ

図 4-2 で示したとおり、民間事業者では、署名検証を行うに当たり、以下の検証を行う必要がある。

(ア) 署名用電子証明書の検証
(イ) 電子署名の検証

(ア)及び(イ)の処理は、公的個人認証サービスに特化した方式ではないため、電子証明書に関して一般に普及している仕組みを用いて実現可能である。

(ア)及び(イ)の内容については、「【APPENDIX ①】署名検証機能の技術解説」を参照のこと。

イ 利用者と利用者証明用電子証明書の紐付機能

民間事業者側で、利用者識別情報（会員 ID、口座番号等）と利用者証明用電子証明書を紐付ける機能である。

利用者証明用電子証明書には基本 4 情報が格納されていないため、利用者証明用電子証明書単体では、その電子証明書が誰に紐付くものであるかを判別できない。そこで、電子利用者証明を利用するに当たっては、民間事業者側の事前準備として、利用者ごとに発行された利用者識別情報と利用者証明用電子証明書を紐付けておく必要がある。そのための方法として、署名用電子証明書の発行番号を基に利用者証明用電子証明書の発行番号を機構に照会する方法が有効と考えられる。この場合の紐付け方法のイメージを図 4-3 に示す。

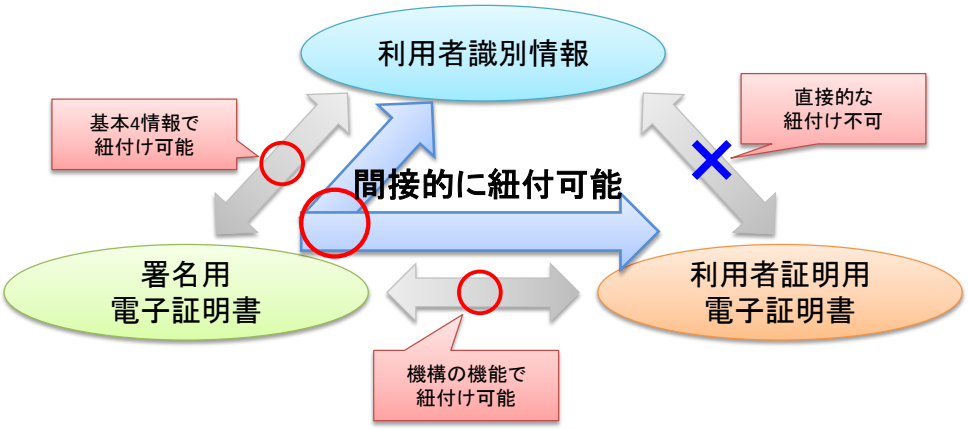


図 4-3 利用者識別情報と利用者証明用電子証明書紐付けのイメージ

署名用電子証明書には基本 4 情報が格納されているため、基本 4 情報を基に、利用者識別情報と署名用電子証明書を紐付けることは可能である。そこで、民間事業者は、署名用電子証明書の発行番号を基に、同一個人宛てに発行された利用者証明用電子証明書の発行番号を取得することで、利用者識別情報と利用者証明用電子証明書を紐付けることが可能となる。機構は署名用電子証明書の発行番号を基に利用者証明用電子証明書の発行番号を応答する機能を保有しているため、民間事業者は、署名検証機能にて取得した署名用電子証明書の発行番号を機構に送信することで、利用者証明用電子証明書の発行番号の取得が可能となる。

本機能を使用した紐付け処理の流れを図 4-4 に示す。

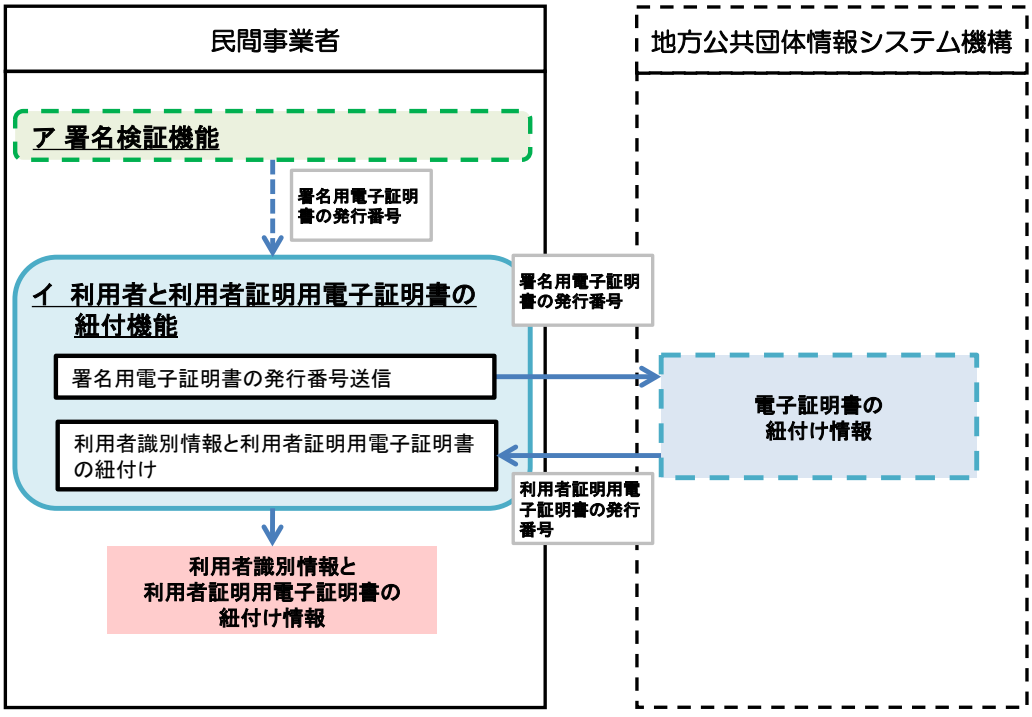


図 4-4 利用者識別情報と利用者証明用電子証明書の紐付けの流れ

ウ 利用者証明検証機能

利用者証明用電子証明書による利用者証明を検証するための機能である。利用者が民間事業者の Web サービスのログイン時等に利用者証明を使用した場合の流れを図 4-5 に示す。

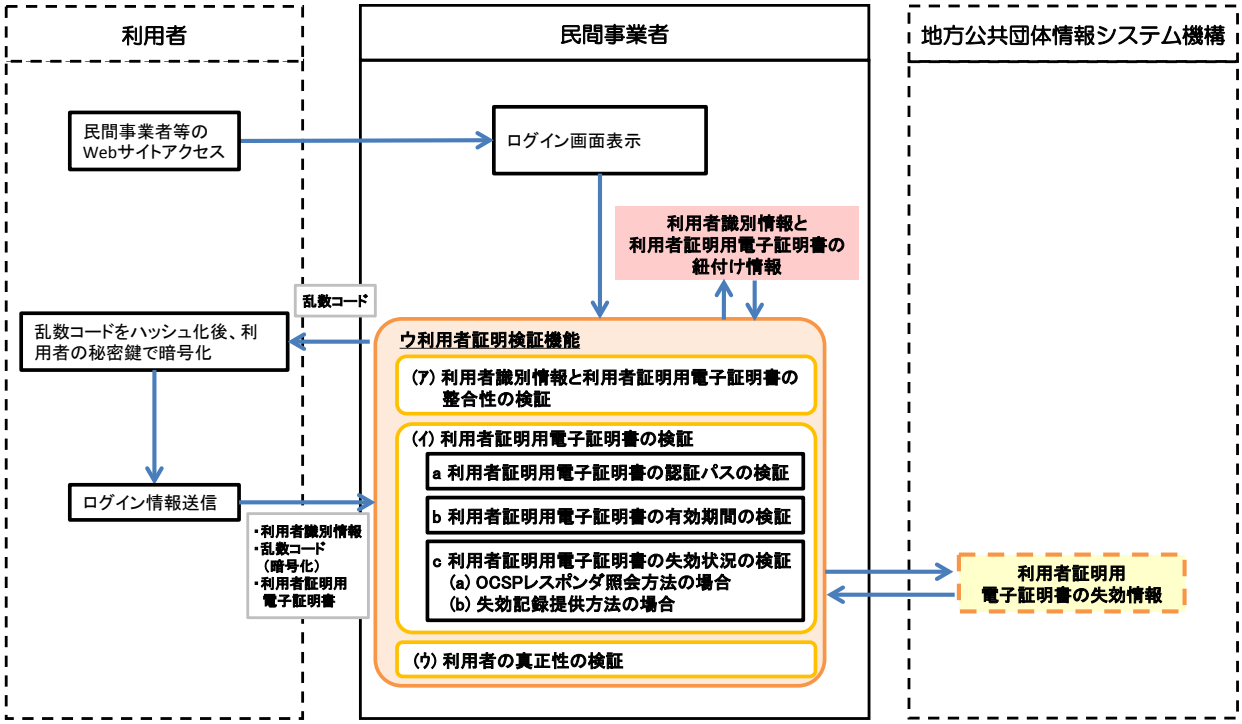


図 4-5 利用者証明の流れ

図 4-5 に示したとおり、民間事業者では、利用者証明を検証するに当たり、以下の検証を行う必要がある。

(ｱ) 利用者識別情報と利用者証明用電子証明書の整合性の検証
(ｲ) 利用者証明用電子証明書の検証
(ｳ) 利用者の真正性の検証

(ｱ)～(ｳ)の処理は、公的個人認証サービスに特化した方式ではないため、電子証明書に関して一般に普及している仕組みを用いて実現可能である。
(ｱ)～(ｳ)の内容については、「【APPENDIX ②】利用者証明機能の技術解説」を参照のこと。

(2) 総務大臣による認定

署名検証又は利用者証明検証を行うためには、電子証明書の失効情報が必要である。また、民間事業者が失効情報を入手するためには、改正後の公的個人認証法第 17 条第 1 項第 6 号の定めに従い、総務大臣による認定を受ける必要がある。

認定を受けた民間事業者は、機構に対して届出を行うことで失効情報を入手できるようになり、公的個人認証サービスの利用が可能となる。民間事業者は、認定を受けた後、使用する失効情報の機構への届出を、署名用電子証明書と利用者証明用電子証明書で個別に行うことになる※1。概要を図 4-6 に示す。

※1 法的には個別の届出となるが、事実上は一本の届出とする予定。

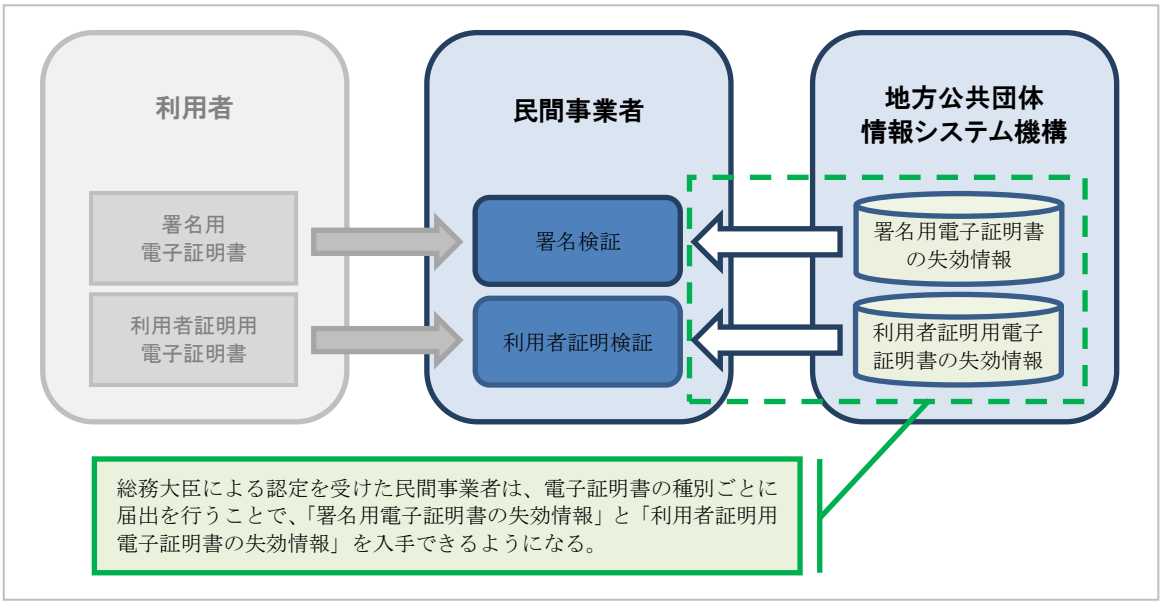


図 4-6 失効情報の入手と総務大臣による認定の関係

本項では、まず始めに「認定の概要」を解説する。その後、「認定基準」及び「認定手続」として、民間事業者が認定を受ける上で必要となる具体的内容を記述する。

ア 認定の概要

公的個人認証サービスは今回の法改正によって民間事業者による利用も認められるようになるが、不適切な利用を防止するためには一定の制限が必要である。公的個人認証サービスを利用する上では電子証明書の失効情報が必須であることから、失効情報の提供範囲を総務大臣が認定した民間事業者だけに制限することで、不適切な利用の抑止が可能となる。

総務大臣は、民間事業者側のシステム、組織体制、運用規程の整備状況等を総合的に評価し、主にセキュリティの観点から、公的個人認証サービスを適切に利用できる民間事業者を認定する。認定基準及び認定手続については後述するが、その内容を正しく理解するための準備として、まずは以下の内容について解説する。

(ｱ) 民間事業者側システムにおける評価対象範囲
(ｲ) 認定の単位

(ｱ) 民間事業者側システムにおける評価対象範囲

前述の「(1) 民間事業者側システム要件」の項で示したとおり、民間事業者は、公的個人認証サービスを利用するに当たり、電子証明書を取り扱うためのシステムを用意する必要がある。民間事業者側のシステムは、利用者からの電子証明書等の受領、電子証明書を用いた本人確認、本人確認結果の業務への活用等、複数の要素から構成される。

改正後の公的個人認証法において、署名検証者等には、表 4-1 に示す情報に関して、目的外利用の禁止及び漏えい等からの保護が法的に義務付けられる。

表 4-1　公的個人認証法において署名検証者等に対し保護が求められている情報

項番	情報名	説明	関連条文	目的
1	署名利用者検証符号	署名用電子証明書内に格納されている、利用者の公開鍵	第 19 条第 2 項	目的外利用の禁止
2	利用者証明利用者検証符号	利用者証明用電子証明書内に格納されている、利用者の公開鍵	第 38 条第 2 項	目的外利用の禁止
3	失効情報	署名用電子証明書及び利用者証明用電子証明書の失効状態を確認するための情報	第 50 条第 1,2 項 第 51 条第 1,2 項	適切な管理義務
			第 52 条第 1,2 項 第 53 条第 1 項	目的外利用の禁止
4	失効情報リスト	複数の失効情報がとりまとめられ、CRL[※2]形式になったもの	第 54 条第 1,2 項 第 55 条第 1,2 項	秘密保持義務
5	対応証明書の発行の番号	署名用電子証明書及び利用者証明用電子証明書に関する、個々の電子証明書を識別するための番号（電子証明書のシリアル番号）	第 56 条第 1 項 第 57 条第 1 項	（受託者）目的外利用の禁止・秘密保持義務

※2　CRL については、「【APPENDIX ①】署名検証機能の技術解説」の(ｱ).c を参照。

そのため、民間事業者側が用意するシステムの構成要素のうち、上記情報を取り扱う部分を認定審査を行う際の評価対象範囲とする。

民間事業者側システムにおける評価対象範囲の例を図 4-7 に示す。この例では、利用者から電子証明書等を受領する部分（Web 受付システム）と、電子証明書を用いた本人確認等を行う部分（本人確認システム）が評価対象範囲になる。本人確認結果を業務へ活用する部分（各種業務システム）については、前述の表 4-1 に示した情報を直接取り扱わない限り、評価対象範囲には含まれない。

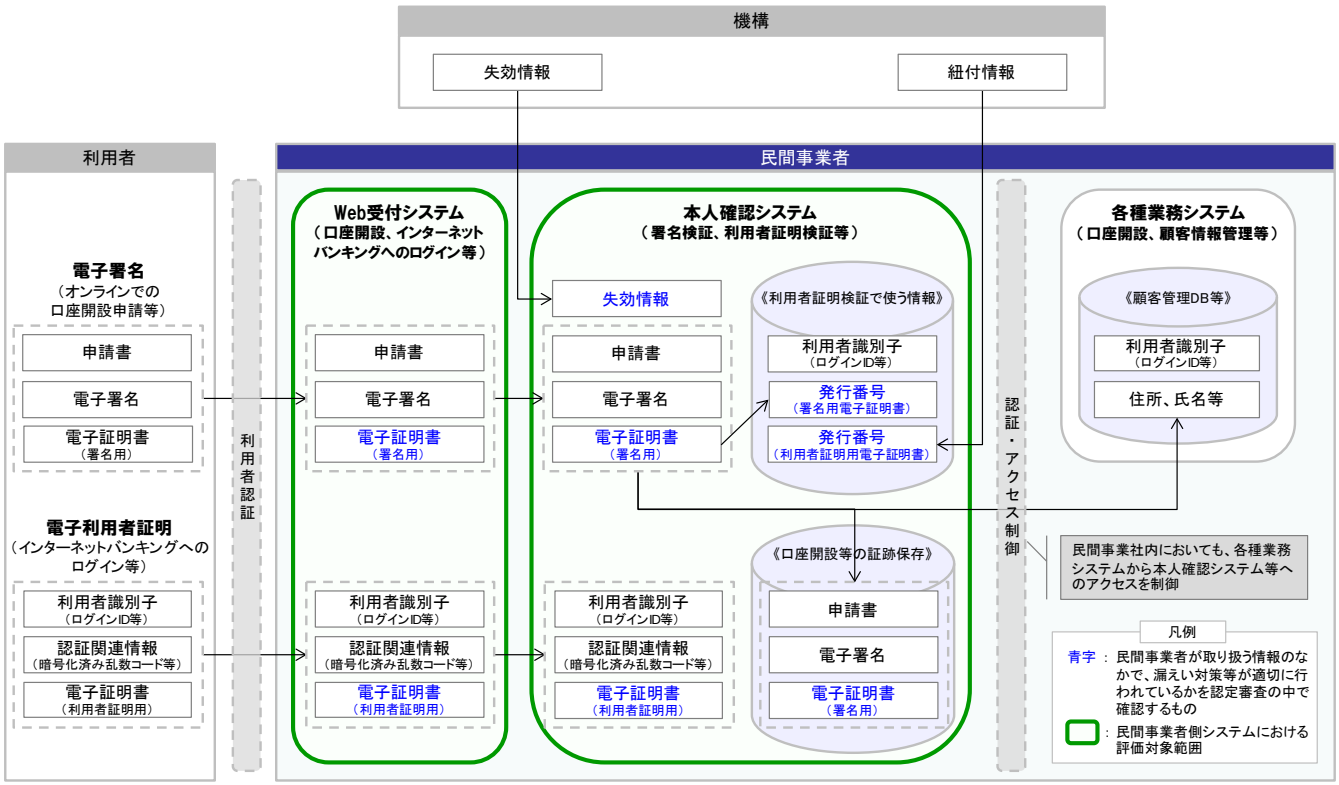


図 4-7 民間事業者側システムにおける評価対象範囲（例）

(イ) 認定の単位

失効情報の入手に際しては、公的個人認証サービスを利用する民間事業者ごとに認定を受けることが基本となる**【例 1】**。ただし、システムの管理を外部委託する場合等においては、複数の民間事業者が連携した形での申請・認定となる場合がある**【例 2】**。

考え方としては、評価対象システムの管理の責任を負う者が複数の民間事業者に亘る場合に、該当するすべての事業者が連携して申請・認定を受ける必要がある。

【例 1】単独で認定を受ける場合

失効情報を利用した業務を行う者が、自ら全ての評価対象システムの管理を行う場合は、単独での認定となる。

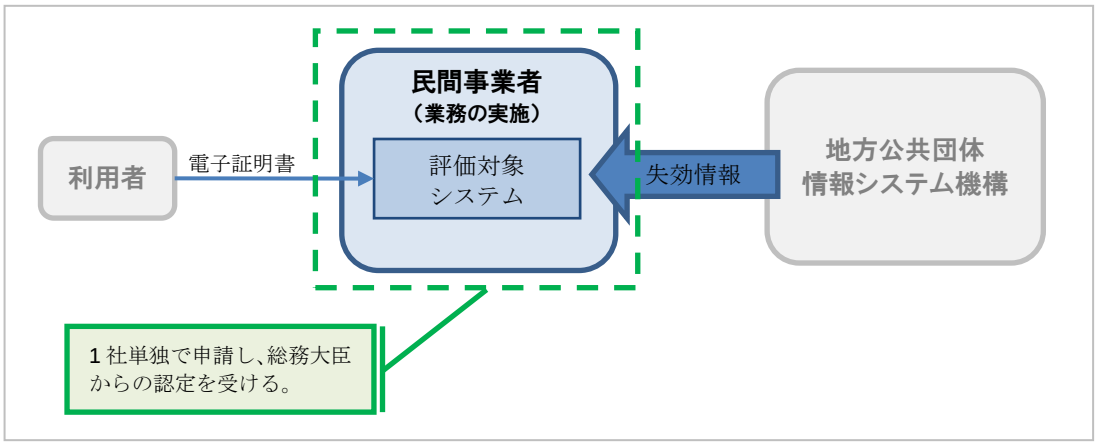


図 4-8 単独で認定を受ける場合

【例 2】システム管理を外部委託する場合

評価対象システムの管理を外部へ委託している場合は、委託元が委託先にシステム管理を委託する旨を明示した上で、総務大臣からの認定を受けることが予定されてい

る。実際の申請・認定審査に際しては委託元・委託先が連携して対応することとなる。

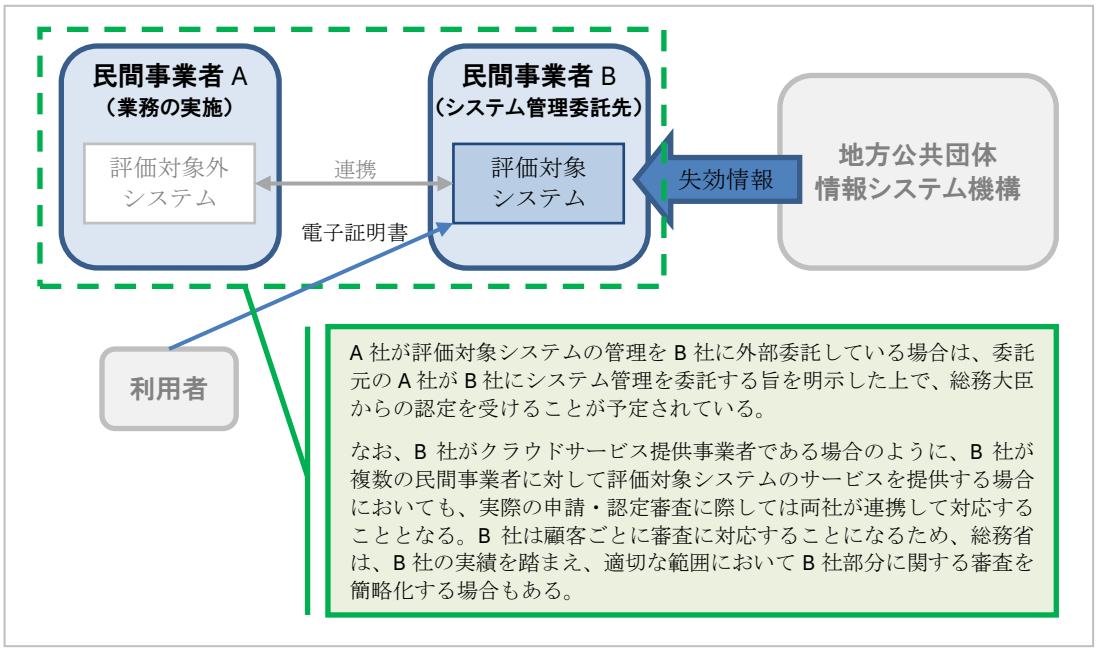


図 4-9 システム管理を外部委託する場合

(ｳ) プラットフォーム事業者の特例

公的個人認証サービスの利用については、失効情報を利用した業務を行う者が、複数で、特定の者に、評価対象システムの設置及び管理の全部を委託する場合が考えられる。このような場合を想定し、次のような趣旨の特例を設ける予定である。

① 受託する者（民間事業者 B）が、委託する者（民間事業者 A1～A6）に代わり、総務大臣の認定（法第 17 条第 1 項第 6 号）を受ける。
⇒委託する者（民間事業者 A1～A6）における、総務大臣の認定を受ける負担を解消。

② 委託する者（民間事業者 A1～A6）は、受託する者（民間事業者 B）に対し、機構への届出（法第 17 条第 1 項）を委託することができる。
⇒委託する者（民間事業者 A1～A6）における、機構への届出の負担を解消。

この特例により、いわゆるプラットフォーム事業者が、評価対象システムの設置及び管理の負担のみならず、総務大臣の認定、機構への届出などの法手続上の負担についても、公的個人認証サービスを利用する者（失効情報を利用した業務を行う者＝署名検証者）に代わって担うことを可能とし、もって、公的個人認証サービス利用者の負担を軽減することにより、その利用拡大を図る予定である。

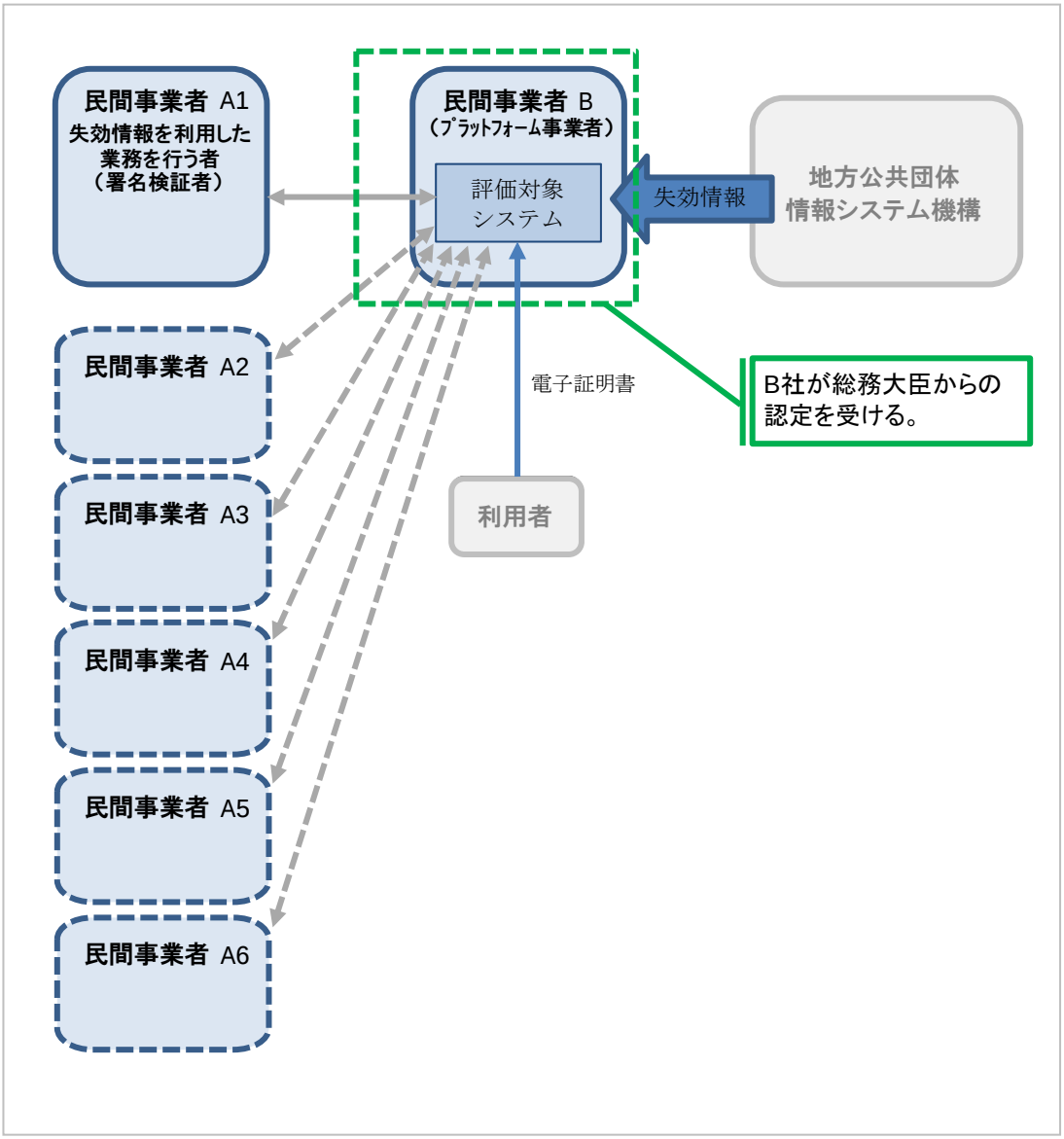


図 4-10 プラットフォーム事業者の場合

イ 認定基準

民間事業者は、総務大臣による認定を受けるために、8 個の評価項目から成る認定基準を満たす必要がある。審査方法は書類審査を基本とし、特段の事情がある場合には、必要に応じて実地審査が行われる。

現時点で想定される認定基準の全体像を表 4-2 に、また、各項目の具体的内容を図 4-11 から図 4-18 に示す。

なお、認定基準に関する正式な内容は、政令又は省令にて別途規定される予定である。

表 4-2　認定基準の全体像

項番	評価項目名	概要	評価項目としての必要性
1	規程類の整備	署名検証等を実施するに当たって必要な事項（業務手順、業務従事者の責任・権限、監査等）が、民間事業者内で規定されているかを評価する。	従業員を統制し、電子証明書及び失効情報を適切な形で継続的に取り扱うためには、組織として規程類の整備が必要である。
2	電気通信回線を通じた不正アクセスの防止	主にインターネットを通じた社外からの攻撃に対して、ネットワーク面でのセキュリティ対策が講じられているかを評価する。	公的個人認証サービスの仕組み上、電気通信回線を通じた通信が必須になる。そのため、ファイアウォール設置等のネットワーク面でのセキュリティ対策が必要である。
3	正当な権限を有しない者による操作の防止	担当者以外がシステムを操作できないように、必要な措置（ID・アクセス権の管理等）が講じられているかを評価する。	悪意を持った従業員による不正（失効情報の漏洩等）を防止するための対策が必要である。
4	動作を記録する機能	監査を実施するためには、監査に必要なログ（システムの動作記録）を取得しておくことが必要となる。必要なログが取得される措置が講じられているかを評価する。	監査の前提として、ログの取得に関する措置が必要である。
5	入退場管理に必要な措置	民間事業者側の設備に関して、評価対象システムが設置される場所（失効情報を取り扱うサーバの設置場所等）への入退場管理について、必要な措置が講じられているかを評価する。	失効情報等が格納された機器（サーバ内のハードディスク等）の物理的な盗難の防止が必要である。
6	外部組織との連携に係る措置	総務大臣の認定を受けようとする民間事業者が社外の資源を利用する場合（外部の事業者が提供するシステムやサービスを利用する場合等）に、秘密保持契約等の必要な措置が講じられているかを評価する。	前述「(イ) 認定の単位」の記載のとおり、複数事業者が連携した形での申請・認定となる場合がある。そのため、民間事業者単体を評価するだけでは不十分であることから、委託元の民間事業者が委託先のサービスを適切に利用しているかの評価が必要である。
7	情報セキュリティに係る組織体制	署名検証等に係る民間事業者側の情報セキュリティ管理体制（責任者、業務実施担当者等）が整備されているかを評価する。	セキュリティ事故の防止、及び万が一発生した場合の適切な対応のために、責任者を明確にした組織体制が必要である。
8	役員等の要件	役員及び業務統括責任者において、公的個人認証法及び暴力団員による不当な行為の防止等に関する法律等に違反する等により、罰金の刑以上の刑に処せられた者等がないかを評価する。	公的個人認証サービスは、法令を遵守した業務において利用されるべきものであり、業務を担う役員等において一定の要件を求めることが必要がある。

【項番 1】規程類の整備

概要

署名検証等を実施するに当たって必要な事項（業務手順、業務従事者の責任・権限、監査等）が、民間事業者内で規定されているかを評価する。

要求事項

署名検証等に係る次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。

① 業務の手順
② 業務に従事する者の責任及び権限並びに指揮命令系統
③ 業務の一部を他に委託する場合においては、委託を行う業務の範囲及び内容並びに受託者による当該業務の実施の状況を管理する方法その他の当該業務の適切な実施を確保するための方法
④ 業務の監査に関する事項
⑤ 署名利用者検証符号、利用者証明利用者検証符号、失効情報、失効情報リスト及び電子証明書の発行の番号に係る、目的外利用の禁止及び漏えいの防止のために必要な措置

解説、適合例

ここでいう業務とは、公的個人認証サービスが提供する電子証明書や失効情報等を用いて電子署名や電子利用者証明による本人確認等を行うこと、及びそのためのシステムを運用・管理することを指す。対象システムの範囲については、「図 4-7 民間事業者側システムにおける評価対象範囲（例）」を参照のこと。
なお、署名検証等が人手を介さずにコンピュータで自動的に行われる場合には、システムを運用・管理する部分のみが本項の対象業務となる。

規程類の整備に当たっては、要求事項に記載された内容を漏れなく規定し、文書化した上で、経営陣又は署名検証等の業務に係る責任者の承認を得ることが必要である。

■要求事項の語句解説

- 署名利用者検証符号 ： 署名用電子証明書内に格納されている、利用者の公開鍵
- 利用者証明利用者検証符号 ： 利用者証明用電子証明書内に格納されている、利用者の公開鍵
- 失効情報 ： 署名用電子証明書及び利用者証明用電子証明書の失効状態を確認するための情報
- 失効情報リスト ： 複数の失効情報がとりまとめられ、CRL 形式になったもの
- 電子証明書の発行の番号 ： 署名用電子証明書及び利用者証明用電子証明書に関する、個々の電子証明書を識別するための番号（電子証明書のシリアル番号）

書類審査

本要求事項に係る必要事項が全て記載され、適切な権限を有した者による承認済みの書類を総務省へ提出することにより、本項目への充足を証明する。
書類の様式については任意とする。

■提出書類の例

- 業務手順書（業務概要の説明、業務フロー図、操作手順書、目的外利用禁止の説明等）
- 業務実施体制図
- 業務委託管理規程
- 監査規程
- 情報管理規程（失効情報等を漏洩してはならない旨を業務従事者に通知）

図 4-11 【評価項目】規程類の整備について

【項番 2】電気通信回線を通じた不正アクセスの防止

概要

主にインターネットを通じた社外からの攻撃に対して、ネットワーク面でのセキュリティ対策が講じられているかを評価する。

要求事項

電気通信回線を通じた不正なアクセス等を防止するために必要な措置として、以下の対策を講じること。

① 評価対象システムに対する電気通信回線を通じた不正なアクセスを防御するためファイアウォール等のシステムを備えること。

② 評価対象システムが二以上の部分から構成され、かつ、署名利用者検証符号、利用者証明利用者検証符号、失効情報、失効情報リスト及び電子証明書の発行の番号のいずれかが電気通信回線を介して複数の建物間で送受信される場合においては、一の部分から他の部分への通信に関し、送信をした設備の誤認並びに通信内容の盗聴及び改変を防止する仕組みを備えること。

解説、適合例

① インターネットを通じた社外からの攻撃によって失効情報が漏えいすることが無いように、失効情報を取り扱うシステムとインターネットへの接続部の間にファイアウォールを設置する。また、不正なアクセス等を検知するシステムとして、侵入検知システム（IDS：Intrusion Detection System）又は侵入防御システム（IPS：Intrusion Prevention System）を設置することが望ましい。設置に当たっては、ファイアウォールと IDS／IPS の機能を併せ持った統合脅威管理（UTM：Unified Threat Management）の機器を採用しても良い。
なお、IDS／IPS を使わずに別の手法で不正なアクセスを検知する場合には、検知の仕組み及び検知可能な内容を総務省に説明する。

② 民間事業者側のシステムが複数拠点に分散して配置され（外部委託によって一部システムが委託先のデータセンターに設置される場合を含む）、かつ、要求事項②に示された情報が拠点間を跨いで通信される場合には、拠点間の通信回線に専用線を用いるか、又は VPN（Virtual Private Network）によってサーバ間の相互認証及び通信の暗号化の対策を講じる。
なお、要求事項②に示された情報に関して拠点間を跨いだ通信が発生しない場合には、本項目は非該当となる。また、民間事業者と機構との通信に関しては、機構側で通信方法を別途規定するため、本項目内では考慮対象外として良い。

書類審査

要求事項を充足するようにシステムを設計した上で、システムの設計書（ネットワーク構成図等）を審査書類として総務省に提出する。
設計書の様式は任意とするが、以下の内容をわかりやすく記載すること。

- ✓ 評価対象システムがどの拠点に設置されるか
- ✓ 評価対象システムとインターネットの間にファイアウォールが設置され、適切な通信制御がなされているか
- ✓ 不正なアクセス等を検知するシステムが設置されているか
- ✓ 要求事項②に該当するか否か（建物間を跨いだ通信が発生するか）
- ✓ 要求事項②に該当する場合は、該当する通信経路はどこか
- ✓ 要求事項②に該当する場合は、どのような仕組みで設備の誤認並びに通信内容の盗聴及び改変を防止するか

図 4-12 【評価項目】電気通信回線を通じた不正アクセスの防止について

【項番 3】正当な権限を有しない者による操作の防止

概要

担当者以外がシステムを操作できないように、必要な措置（ID・アクセス権の管理等）が講じられているかを評価する。

要求事項

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として、以下の対策を講じること。

① 評価対象システムを操作者によって作動させる場合においては、各操作者に対する権限の設定並びに当該操作者及びその権限が確認できること。

② システム管理者に係る識別符号については、特に厳重な管理が行われていること。

解説、適合例

① 署名検証等の業務に従事する正規の担当者以外がシステムを操作できないように、システムへのログイン認証の仕組みを用意する。アカウント（ID）や操作権限については、最小限の範囲で払い出し、申請・承認などの管理ルールを定めた上で、責任者の下で適切に管理する。

② 特権アカウント（root、administrator 等）とは別に、通常業務で使用するアカウント（必要最小限の権限だけを付与したアカウント）を用意する。

書類審査

要求事項の充足が証明可能な資料を用意し、審査書類として総務省に提出する。
書類の様式については任意とする。

■提出書類の例
- 業務手順書（ログイン認証が必要であることの説明等）
- システム設計書（ログイン認証機能が具備されていること等）
- アカウント管理規程（申請・承認などの管理ルール、特権アカウントと通常アカウントの区別等）

審査軽減措置

評価対象システムの管理責任を負う組織が ISO/IEC 27001（JIS Q 27001）で規定されている情報セキュリティ管理システム（以下、ISMS という。）の認定を取得している場合は、ISMS の認定における登録範囲に公的個人認証サービスに関する内容が含まれる場合のみ、ISMS の認定証の提示を以って、本項目に係る書類審査の代替とすることが可能である。

図 4-13 【評価項目】正当な権限を有しない者による操作の防止について

【項番 4】動作を記録する機能

概要

監査を実施するためには、監査に必要なログ（システムの動作記録）を取得しておくことが必要となる。必要なログが取得され、改ざん等から保護するために必要な措置が講じられているかを評価する。

要求事項

動作を記録する機能として、署名検証等を行う機器は、各動作の要求者名（操作者によって作動させる場合に限る。）、内容、発生日時、結果等を履歴として記録し、取得した記録を改ざん等から保護する機能を備えること。

解説、適合例

監査の実施やセキュリティ事故発生時の原因調査等に必要なログを取得する。また、ログを改ざん等から保護するために、外部記憶媒体（テープなど）への定期的なバックアップの仕組み等を用意する。

書類審査

要求事項の充足が証明可能な資料を用意し、審査書類として総務省に提出する。
書類の様式については任意とする。

■提出書類の例
・システム設計書（ログ取得機能、ログの改ざん防止対策等）
・運用設計書（ログのバックアップ運用等）

審査軽減措置

評価対象システムの管理責任を負う組織が ISMS の認定を取得している場合は、ISMS の認定における登録範囲に公的個人認証サービスに関する内容が含まれる場合のみ、ISMS の認定証の提示を以って、本項目に係る書類審査の代替とすることが可能である。

図 4-14 【評価項目】動作を記録する機能について

【項番 5】入退場管理に必要な措置

概要

民間事業者側の設備に関して、評価対象システムが設置される場所（失効情報を取り扱うサーバの設置場所等）への入退場管理について、必要な措置が講じられているかを評価する。

要求事項

署名検証等に係る業務に従事する者以外が、署名検証等を行う機器の設置場所へ入場し、当該機器に触れることができないようにするための施錠等の措置を講じること。

解説、適合例

評価対象システムは、ID カード等による入退場管理が可能な部屋に設置する。
なお、民間事業者が保有する他システム（公的個人認証サービスとは関連のないシステム）と同じ部屋に設置する場合は、搭載するサーバラックを分けた上で施錠管理（サーバラックに対する施錠）する等の手段により、署名検証等の業務従事者以外が評価対象システムに触れることができないようにする。

書類審査

要求事項の充足が証明可能な資料を用意し、審査書類として総務省に提出する。
書類の様式については任意とする。

■提出書類の例
- ファシリティ設計書（サーバー室の入退場管理等）
- サーバ室レイアウト図
- サーバラック搭載図

審査軽減措置

評価対象システムの管理責任を負う組織が ISMS の認定を取得している場合は、ISMS の認定における登録範囲に公的個人認証サービスに関する内容が含まれる場合のみ、ISMS の認定証の提示を以って、本項目に係る書類審査の代替とすることが可能である。

図 4-15 【評価項目】入退室管理に必要な措置について

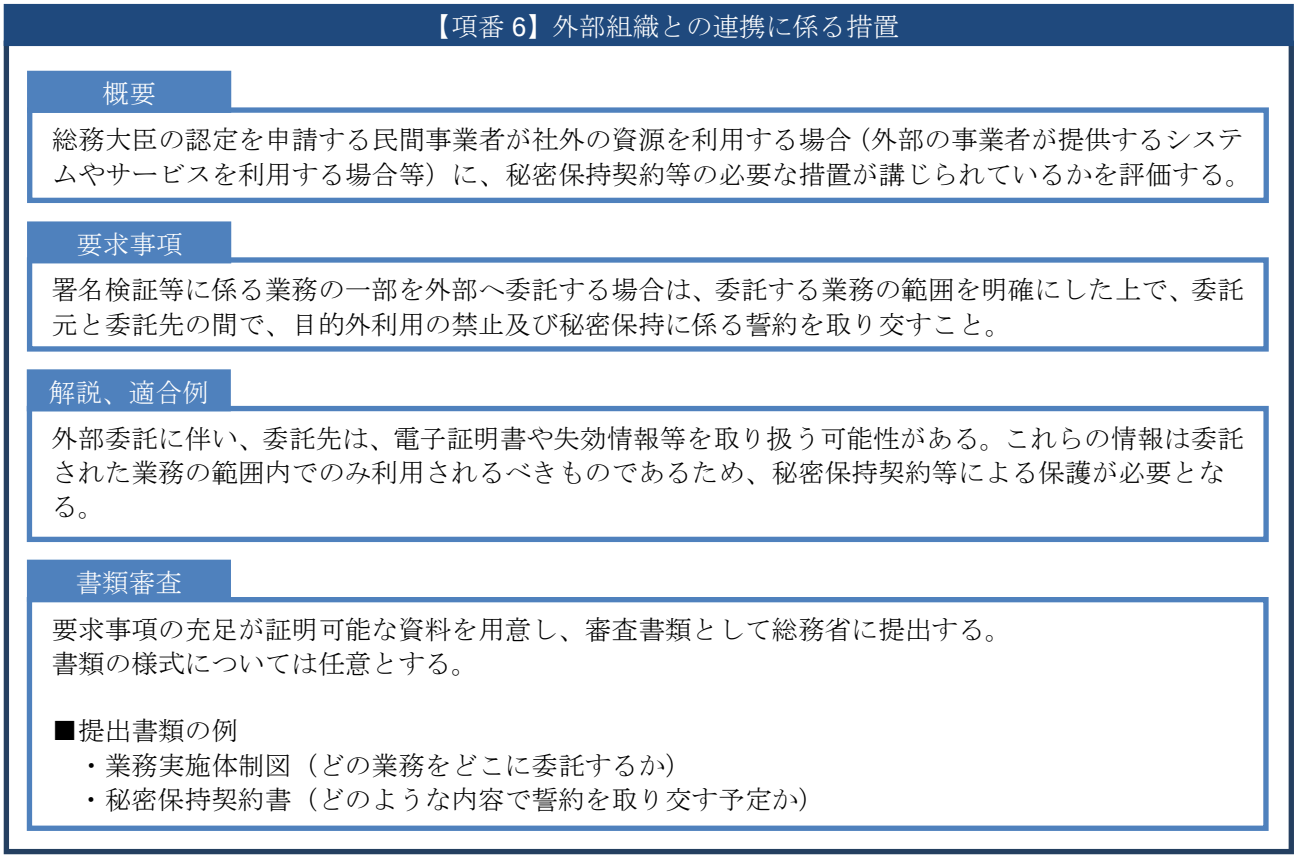


図 4-16 【評価項目】外部組織との連携に係る措置について

【項番 7】情報セキュリティに係る組織体制

概要

署名検証等に係る民間事業者側の情報セキュリティ管理体制（責任者、業務実施担当者等）が整備されているかを評価する。

要求事項

署名検証等に係る業務の情報セキュリティ管理体制について、以下の対応を行うこと。
① 役割、責任及び権限を定め、文書化し、かつ、署名検証等に係る業務の全従事者に周知すること。
② セキュリティ事故が発生した場合に、総務省への報告が迅速に行われるように、連絡経路を明確に定めること。

解説、適合例

① 署名検証等を行う上で、セキュリティ事故の発生を防止するためには、組織的なセキュリティ管理が必要である。組織的な管理を行うための前提として、署名検証等に係るセキュリティ管理体制を定めて文書化する。
なお、外部委託を行う場合には、委託元だけでなく、委託先も含めた管理体制を明確化すること。

② 署名検証等においてセキュリティ事故が発生した場合、民間事業者は事故の発生を総務省へ報告する。迅速な報告が可能となるように、連絡経路（エスカレーションのルート）をあらかじめ定めておく。

書類審査

要求事項の充足が証明可能な資料を用意し、審査書類として総務省に提出する。
書類の様式については任意とする。

■提出書類の例
・情報セキュリティ管理体制図
・緊急時連絡ルール

なお、管理体制に係る内容を文書化する上では、個人名まで明記する方法と、組織名や役職名のみを明記する方法がある。基本的にはどちらの方法を採用しても構わないが、情報セキュリティに係る責任者及び総務省との窓口担当者については特に重要であるため、個人名を明記すること。

図 4-17 【評価項目】情報セキュリティに係る組織体制について

【項番 8】役員等の要件

概要

役員及び業務統括責任者において、公的個人認証法及び暴力団員による不当な行為の防止等に関する法律等に違反する等により、罰金の刑以上の刑に処せられた者等がないかを評価する。

要求事項

役員及び業務統括責任者において、以下の者（①かつ②）がないこと。

① 公的個人認証法若しくは暴力団員による不当な行為の防止等に関する法律若しくはこれに相当する外国の法令の規定に違反し、
又は刑法若しくは暴力行為等処罰に関する法律の罪を犯し、

② 罰金の刑に処せられ、
その刑の執行を終わり、
又はその刑の執行を受けることがなくなった日
から５年を経過しない者

解説、適合例

業務統括責任者とは、部長、次長、課長その他いかなる名称を有する者であるかを問わず、業務を統括する者の権限を有する地位にある者をいう。

書類審査

役員及び業務統括責任者（就任が予定されている者を含む）の名簿及びそれらの者に要求事項に該当する者がないことを誓約する書類を総務省に提示する。
書類の様式については任意とする。

■提出書類の例
・役員及び業務統括責任者（予定者）名簿
・役員及び業務統括責任者に要求事項に該当する者がないことの誓約書

図 4-18 【評価項目】役員等の要件

ウ 認定手続

民間事業者が公的個人認証サービスの利用を開始するまでの流れを図 4-19 に示す。図中の緑色の破線で囲まれた部分が、総務大臣による認定を受けるための手続きに該当する。

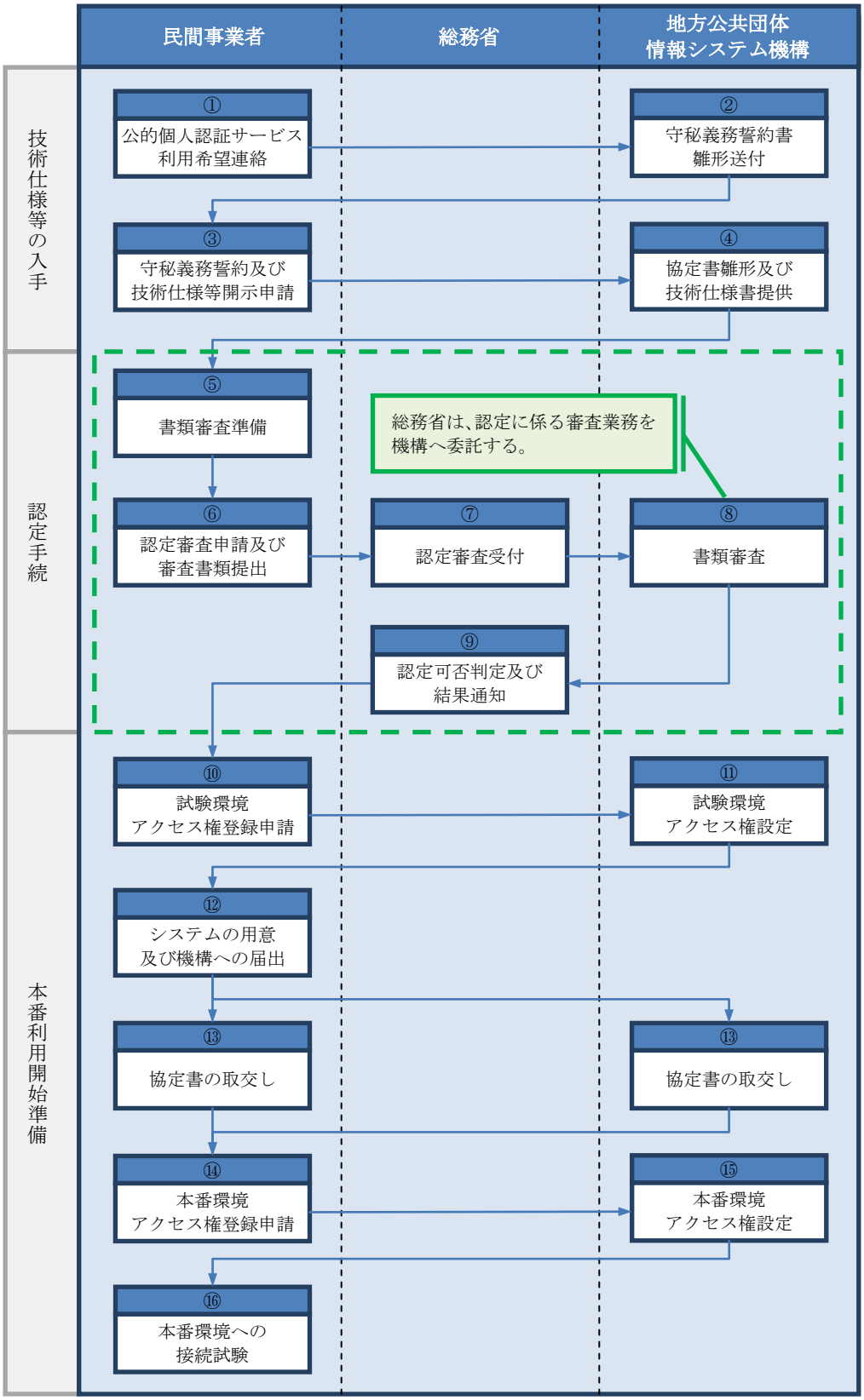


図 4-19 公的個人認証サービス利用開始までの流れ

図 4-19 における①～⑯の詳細は、次のとおりである。

【step１】 技術仕様等の入手

① 民間事業者は、公的個人認証サービスを利用したい旨を、電話又はメールで機構へ連絡する。
② 機構は、守秘義務誓約書の雛形を民間事業者宛てに送付する。
③ 民間事業者は、守秘義務に関する誓約を機構との間で取り交わした上で、公的個人認証サービスに係る技術仕様等の開示を申請する。
④ 機構は、民間事業者が公的個人認証サービスを利用開始する際に取り交すことになる協定書の雛形及び公的個人認証サービスに係る技術仕様書を民間事業者へ提供する。

【step２】 認定手続

⑤ 民間事業者は、認定基準に示されている要求事項への対応を行い、要求事項を満たすことの証明に資する書類を作成する。なお、本段階では、設備やシステム等の実環境の準備や、業務の一部を外部へ委託する場合の委託契約締結までは必須としない。
⑥ 民間事業者は、総務省に認定審査を申請するとともに、⑤で作成した審査書類を提出する。なお、外部委託によって複数事業者が連携した形での申請・認定となる場合は、委託元が主体となって認定審査を申請すること。
⑦ 総務省は、民間事業者からの審査申請を受け付けた上で、書類審査の実施を機構へ依頼する。
⑧ 機構は、民間事業者が認定基準を満たしているかを確認し、確認結果を総務省へ報告する。
⑨ 総務省は、機構による確認結果を踏まえて認定可否を判定し、結果を民間事業者へ通知する。

【step３】 本番利用開始準備

⑩ 審査に合格して総務大臣による認定を受けた民間事業者は、公的個人認証サービスの試験環境に接続するための申請を行う。
⑪ 機構は、試験環境に接続するための設定を行い、接続に必要な情報を民間事業者へ通知する。
⑫ 民間事業者は、署名検証等を行うために必要なシステム環境を用意し、⑪で接続可能になった試験環境を使って動作確認を行う。動作に問題が無いことを確認した後、機構から失効情報の提供を受けるための届出を行う。
⑬ 民間事業者は、機構との間で協定書を取り交わす（改正後の公的個人認証法第 17 条第 4 項及び第 36 条第 2 項で規定されている「取決めの締結」に相当）。
⑭ 民間事業者は、公的個人認証サービスの本番環境に接続するための申請を行う。
⑮ 機構は、本番環境に接続するための設定を行い、接続に必要な情報を民間事業者へ通知する。
⑯ 民間事業者は、公的個人認証サービスの本番環境に接続するための準備を行い、機構と連携して本番環境への接続試験を行う。

総務大臣による認定に関して、公的個人認証サービス利用開始後の留意事項 2 点を以下に示す。

■認定の有効期間

総務大臣による認定には有効期間があることから、認定を受けた民間事業者が継続して公的個人認証サービスを利用するためには、有効期間が満了する前に認定の更新手続を

行う必要がある。具体的な有効期間については政令で規定される予定であるが、認定の有効期間は、1 年間である（政令第 10 条）。

認定の更新では、更新時点においても要求事項がすべて充足されていることを確認する必要がある。更新審査の迅速化のため、総務省から求めがあった場合、更新を受けようとする民間事業者は、要求事項の充足を証明するための審査書類一式に加え、初回審査時に提出した審査書類からの変更箇所を簡潔に示した資料を追加で提出することが望まれる。

■認定審査時の内容からの変更

民間事業者は、認定基準の評価項目である「【項番 6】外部組織との連携に係る措置」又は「【項番 7】情報セキュリティに係る組織体制」をはじめ、書類審査時に記載した内容の主要な要素について変更しようとする場合は、変更予定内容を総務省に遅滞なく連絡する必要がある。総務省は、変更内容を確認し、必要に応じて再審査等を行う。

(3) 失効情報提供手数料

本項では、失効情報手数料について記述する。失効情報提供手数料に関する 2015 年 7 月時点の案は次のとおりである。最終的には 10 月・11 月を目途に、機構にて定められ、総務大臣の認可がなされる予定である。

ア 基本的な考え方（案）

① 低廉性：インターネット取引等の基盤として、多様な業種の多数の事業者に利用頂けるよう、十分に低廉な料金設定とする。

② 公平性：多様な業種の多数の事業者の利用を想定し、サービス利用に応じた料金設定とする。

③ 持続性：サービスが持続可能となるよう、サービスの利用が拡大する将来においては、利用者の負担（電子証明書発行手数料（国民）及び情報提供手数料（府省等・民間事業者）並びに地方の利用相当負担）で、サービスの費用を賄うことが見込める料金設定とする※4。

※4 サービスの費用は、これまで利用者に代わりほぼ地方が負担。今後、これに加え、当面、国が、番号法施行に伴う費用増加及び個人番号カード普及促進の観点から、電子証明書発行手数料相当額を負担。

イ 情報提供手数料（案）

① 当面は、利用促進を図るため、民間事業者から見たサービス利用のメリットを分析し、「低廉性」を重視した単価とする※5。

② 「公平性」等の観点から、利用に応じた料金（従量制）を基本としつつ※6、多様な業種・事業者に適切に対応するため、「大口割引」等を可能にするための規定も設ける。

③ 当該単価等は、当面のものであり、利用の拡大等に応じ、柔軟かつ適切に見直しを行う。特に、単価の低減が図れるよう、利用の拡大に積極的に取り組む※7。

【手数料（案）】

- ◆ 署名用電子証明書の有効性確認を行った件数　×　２０円
- ◆ 利用者証明用電子証明書の有効性確認を行った件数　×　２円
  - ◇ 大口の利用、利用事務・事業の公益性その他の事情にかんがみ、手数料の単価又は総額の減額を行う場合がある。

※5 手数料（案）の単価では、当面（５年程度）は、利用者の負担のみで費用を賄うことは難しいと考えられる（地方及び国の負担が継続する）が、将来的に、サービスの利用が拡大・定着すれば、利用者の負担のみで費用を賄うことが期待できる単価であり、「持続性」にも配慮している。

※6 「定額制」では、「利用の少ない者」の利用が進まず、「利用が多い者」の利用に応じた負担がなされない（すなわち、「公平性」及び「持続性」の観点から、課題がある。）。このため、「署名等検証者からの問い合わせに対して失効情報の集合物を提供する方法」又は「即時に応答する方法」の別を問わず、有効性確認を行った件数に応じた「従量制」を基本とする。

※7 情報提供手数料を含めた利用者の負担が、サービス全体の経費を超えないことは当然。よって、将来的に、利用が拡大していけば、単価を低減させることが可能。 そのような状況になることをめざし、利用の拡大に向けて取り組む。

【民間事業者から見たサービス利用のメリット分析】

○ 署名用を利用することによる主なメリットは、次のとおりであり、これらを総合的に勘案し、２０円と設定した。

① 「住民票記載の正確な氏名・住所等の４情報＋有効／無効」が取得できる。

② 申請等の否認・改ざん、なりすましを防止できる（法的な真正成立推定効も得られる。）（ネットバンキングの不正送金被害約１４億円（２５年））。

③ 銀行等において、口座開設時に必要となる本人確認書類の郵送の負担（郵便代８２円等）が不要となる。

④ 利用者証明用とあわせ利用することで、氏名・住所の異動を把握できる（確認葉書郵送の負担（郵便代５２円等）がなくなる。）。

○ また、利用者証明用を利用することによる主なメリットは、次のとおりであり、これらを総合的に勘案し、また、住基ネット手数料の大口料金（３円）等を参照して、署名用の１０分の１である２円と設定した。

① なりすましログインを防止できる（不正送金等の被害を防止できる。）（安心感の増大から取引拡大も期待できる。）。

② 署名用とあわせ利用することで、氏名・住所の異動を把握できる（確認葉書郵送の負担（郵便代５２円等）がなくなる。）。

【APPENDIX ①】署名検証機能の技術解説

電子署名の流れを図 APPENDIX①-1 に示す。

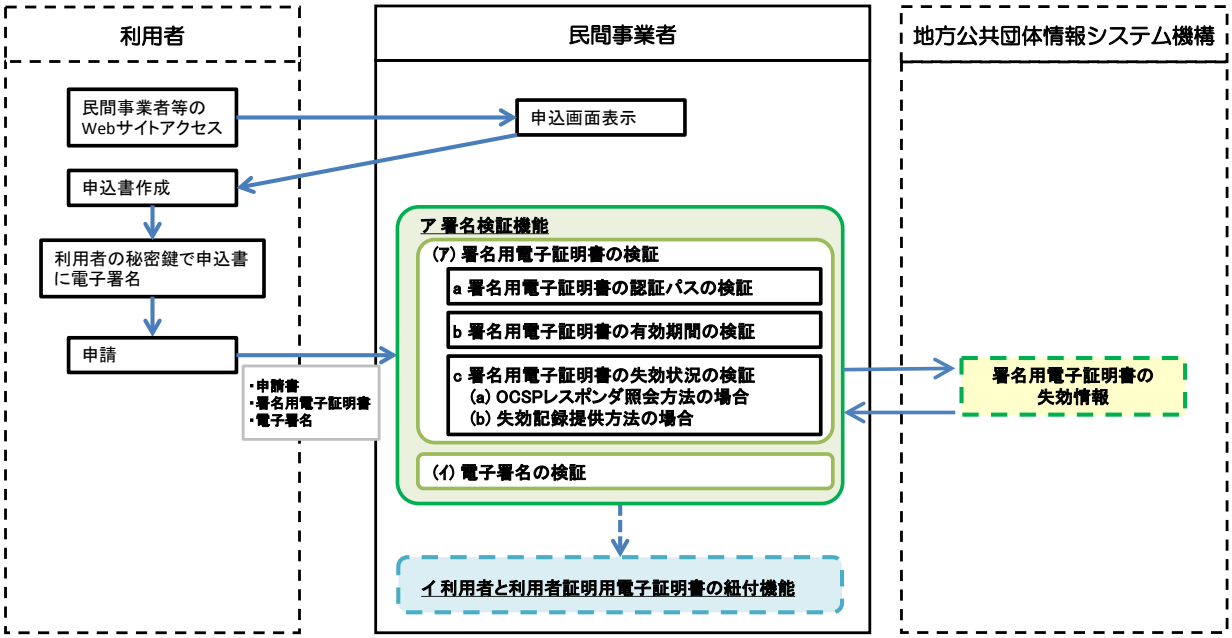


図 APPENDIX①-1 電子署名の流れ

図中の(ア)及び(イ)の概要について、それぞれ以下に記述する。

なお、より詳細な技術的内容については、RFC 5280「インターネット X.509 PKI： 証明書と CRL のプロファイル」を参照のこと。

(ア) 署名用電子証明書の検証

電子署名の検証を行うに当たり、利用者から受領した署名用電子証明書が有効であることを確認する必要がある。検証内容について以下に記述する。

a 署名用電子証明書の認証パスの検証

電子署名の検証では、利用者から受領した署名用電子証明書が機構から発行されているものであり、改ざんされていないかを確認する必要がある。署名用電子証明書の認証パスの検証の概要を図 APPENDIX①-2 に示す。

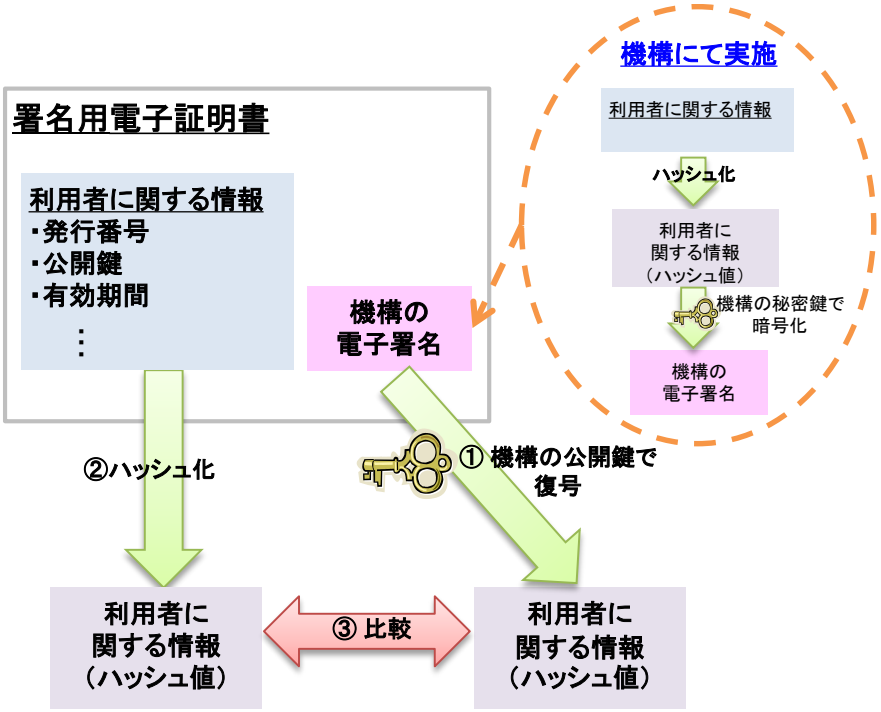


図 APPENDIX①-2 署名用電子証明書の認証パスの検証の流れ

図 APPENDIX①-2 で示したとおり、署名用電子証明書の認証パスの検証は以下の流れで行う。

① 民間事業者があらかじめ保持している機構の公開鍵※1 で、署名用電子証明書内に格納されている、機構の電子署名※2 を復号する。
② 署名用電子証明書内の利用者に関する情報をハッシュ化する。
③ ①、②の結果を比較し、同一であることを確認することで、署名用電子証明書が機構から発行されたものであり、改ざんされていないことを確認したことになる。

※1 機構の自己署名証明書に格納されている。機構の自己署名証明書が失効しているかどうかは、機構から提供される認証局（機構）の証明書失効リスト(ARL : Authority Revocation List)にて確認する。
※2 署名用電子証明書内の利用者に関する情報をハッシュ化し、機構の秘密鍵で暗号化したものである。

b 署名用電子証明書の有効期間の検証

署名用電子証明書の中に格納されている署名用電子証明書の有効期間が超過していないかを確認する。有効期間を超過している電子証明書については失効情報が提供されないため、民間事業者にて必ず有効期間の検証を行う必要がある。

c 署名用電子証明書の失効状況の検証

署名用電子証明書の失効状況の検証は、以下に示す機構からの失効情報の提供方法に応じて、計 2 パターン存在する。それぞれの場合について以下に記述する。

(a) OCSP レスポンダ照会方法の場合

「OCSP（Online Certificate Status Protocol）レスポンダ照会方法」の場合、民間事業者は、民間事業者側システムに失効情報を保持せず、失効情報の照会が必要な都度、機構に問い合わせる必要がある。具体的には、利用者から署名用電子証明書を受領した際に、機構が保持する OCSP レスポンダに対して当該電子証明書の発行番号※3 を送信し、機構から当該電子証明書の失効状況の照会結果を受領する。失効状況の検証イメージを図 APPENDIX①-3 に示す。

※3　利用者証明用電子証明書と署名用電子証明書には、それぞれ一意の発行番号が割り振られている。発行番号は電子証明書の中に格納されている。

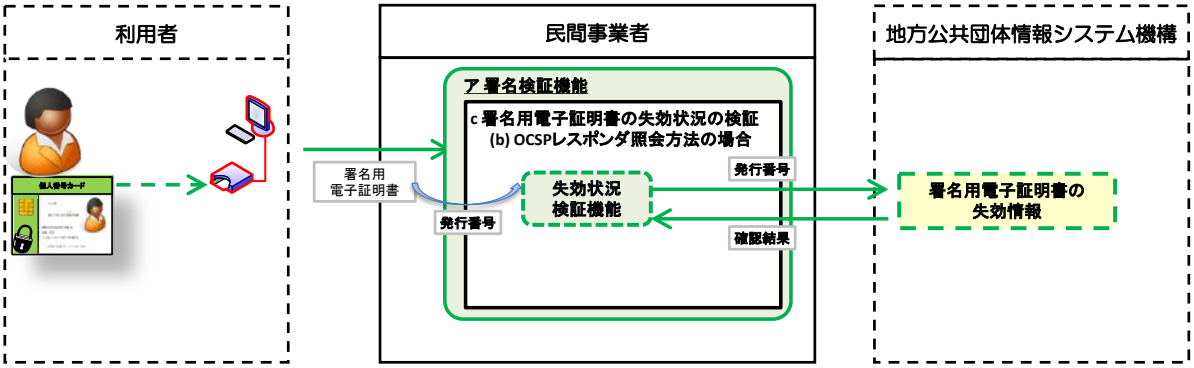


図 APPENDIX①-3　「OCSP レスポンダ照会方法」の場合の失効状況検証イメージ

機構から送信されてくる確認結果の情報には、それ自体がなりすましや改ざんされたものでないことを保証するために、機構の秘密鍵による電子署名が付与されている。そのため、民間事業者は、機構の自己署名証明書に格納されている公開鍵を使って電子署名の検証を行い、なりすましや改ざんされたものでないこと確認した上で、機構から送信されてくる確認結果を使用する必要がある。電子署名の検証方法については、後述の「(イ) 電子署名の検証」を参照※4 のこと。

※4　後述の「(イ) 電子署名の検証」の記載内容と同じ処理の流れで、機構から送信されてくる確認結果に付与された電子署名の検証を行うことができる。ただし、利用者の公開鍵ではなく、機構の自己署名証明書に格納されている公開鍵を使用する点が異なる。

(b) 失効記録提供方法の場合

「失効記録提供方法」では、機構は、最新の失効情報を基に日次で電子証明書失効リスト（CRL：Certificate Revocation List）を作成し、民間事業者の要求に応じてこれを提供する。このため、民間事業者では、機構に対して日次で CRL の送信を要求し、受領した CRL を民間事業者側システム内に失効情報として保持する機能（CRL 取得機能）が必要となる。取得した失効情報を参照し、失効状況の検証を行う。具体的には、利用者から受領した署名用電子証明書の発行番号を基にシステム内に保持された失効情報を照会し、電子証明書の失効状況を検証する。失効状況の検証イメージを図 APPENDIX①-4 に示す。

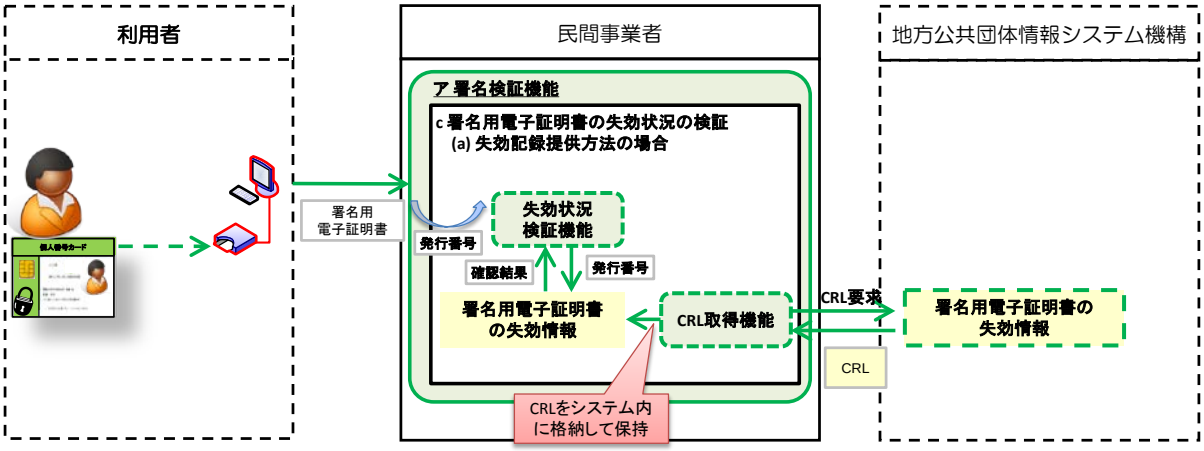


図 APPENDIX①-4　「失効記録提供方法」の場合の失効状況検証イメージ

なお、機構から提供される CRL には、それ自体がなりすましや改ざんされたものでないことを保証するために、OCSP レスポンダ照会方法の場合と同様に機構の秘密鍵による電子署名が付与されている。そのため、民間事業者は、機構の自己署名証明書に格納されている公開鍵を使って電子署名の検証を行い、なりすましや改ざんされたものでないこと確認した上で CRL を使用する必要がある。

(ｲ) 電子署名の検証

利用者から受信した電子署名を検証する。利用者から受信した電子署名は、申請書等の情報をハッシュ化し、利用者の秘密鍵にて暗号化されたものである。電子署名の検証の流れを図 APPENDIX①-5 に示す。

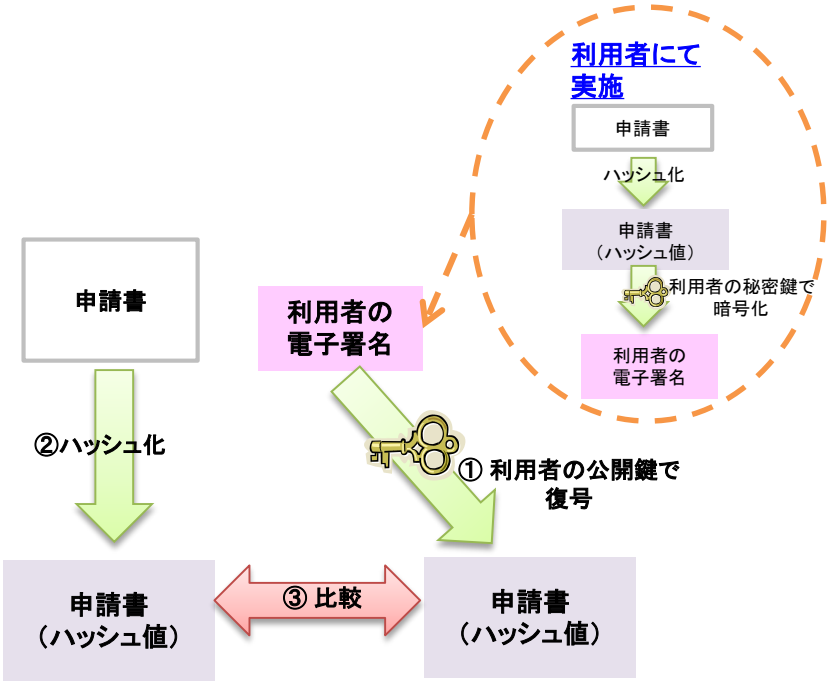


図 APPENDIX①-5 電子署名の検証の流れ

図 APPENDIX①-5 で示したとおり、電子署名の検証は以下の流れで行う。

① 電子署名を利用者の公開鍵で復号する。
② 申請書等の情報をハッシュ化する。
③ ①、②の結果を比較し、同一のものであることを確認することで、利用者による申請等が利用者本人によって行われたものであり、改ざんされていないことを確認したことになる。

【APPENDIX ②】利用者証明検証機能の技術解説

利用者が民間事業者の Web サービスのログイン時等に利用者証明を使用した場合の流れを図 APPENDIX②-1 に示す。

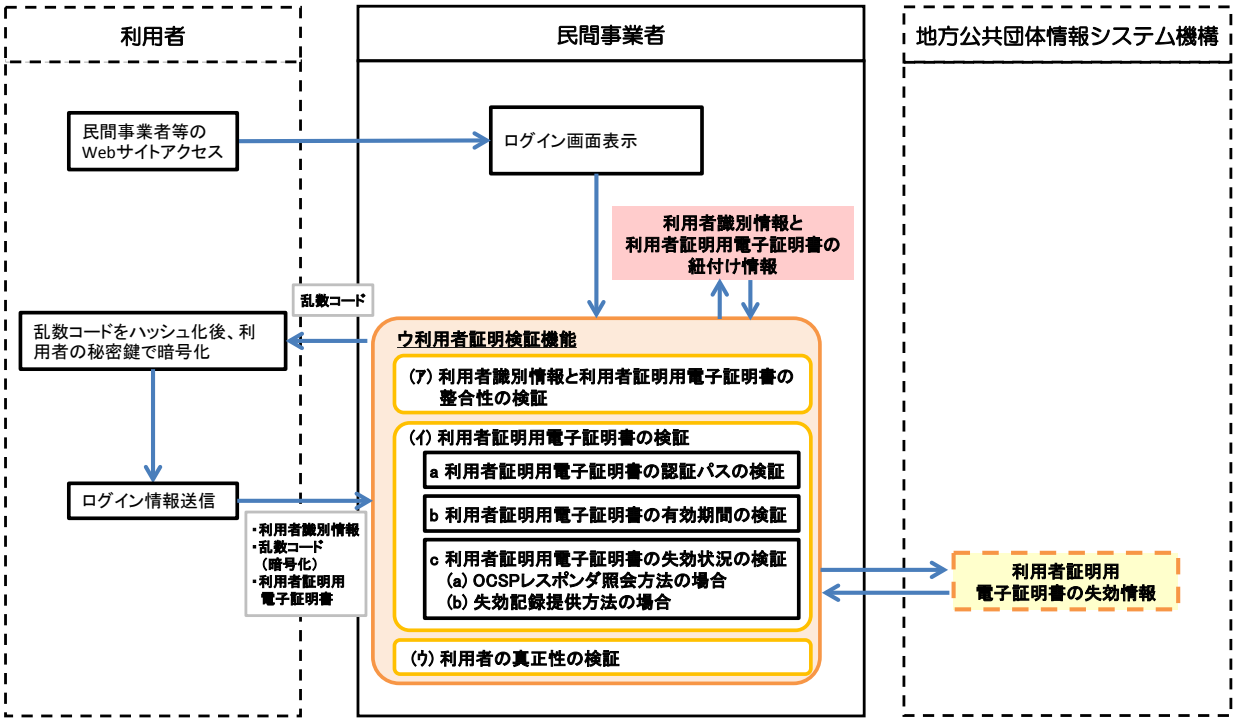


図 APPENDIX②-1 利用者証明の流れ

図中の(ｱ)～(ｳ)の概要について、それぞれ以下に記述する。

(ｱ) 利用者識別情報と利用者証明用電子証明書の整合性の検証

利用者から受領した情報（利用者識別情報と利用者証明用電子証明書）と、民間事業者側システムにあらかじめ格納していた利用者識別情報及び利用者証明用電子証明書の紐付情報が一致することを確認する。これにより、利用者識別情報と利用者証明用電子証明書の整合性が確認可能である。

(ｲ) 利用者証明用電子証明書の検証

利用者証明の検証を行うに当たり、利用者証明に使用する利用者証明用電子証明書が有効であることを確認する必要がある。検証内容について以下に記述する。

a 利用者証明用電子証明書の認証パスの検証

利用者証明用電子証明書が機構から発行されているものであり、改ざんされていないかを確認する。検証方法については、「【APPENDIX ①】(ｱ).a 署名用電子証明書の認証パスの検証」と同等であり、検証の対象が利用者証明用証明書となるだけである。検証方法の詳細については、「【APPENDIX ①】(ｱ).a 署名用電子証明書の認証パスの検証」を参照のこと。

b 利用者証明用電子証明書の有効期間の検証

利用者証明用電子証明書の中に格納されている利用者証明用電子証明書の有効期間が超過していないかを確認する。有効期間を超過している電子証明書については失効情報が提供されないため、民間事業者にて必ず有効期間の検証を行う必要がある。

c 利用者証明用電子証明書の失効状況の検証

利用者証明用電子証明書の発行番号を基に、失効情報を照会し、利用者証明用電子証明書が失効状態にないかを確認する。検証方法については、「【APPENDIX ①】(ｱ).c 署名用電子証明書の失効状況の検証」と同等であり、検証の対象が利用者証明用証明書となるだけである。検証方法の詳細については、「【APPENDIX ①】(ｱ).c 署名用電子証明書の失効状況の検証」を参照のこと。

(ｳ) 利用者の真正性の検証

Web サービスへのログイン等に当たり、利用者証明を行おうとしている者が利用者本人であることを確認する。利用者本人であることの確認は、利用者本人しか持ちえない利用者証明用電子証明書の秘密鍵を用いることで確認が可能である。秘密鍵を利用した確認として、乱数コードを利用した方法が有効であると考えられる。乱数コードを利用することにより、ログインする都度インターネット上を流れる通信データが変わるため、通信データ盗聴及び再利用によるなりすましの不正利用の防止に有効である。

民間事業者は、利用者が利用者証明を行おうとする際に乱数コードを発行し、利用者に送信する。利用者は、乱数コードをハッシュ化して利用者の秘密鍵にて暗号化したものを、利用者用電子証明書等とともに民間事業者に送信する。民間事業者内における乱数コードの検証の流れを図 APPENDIX②-2 に示す。

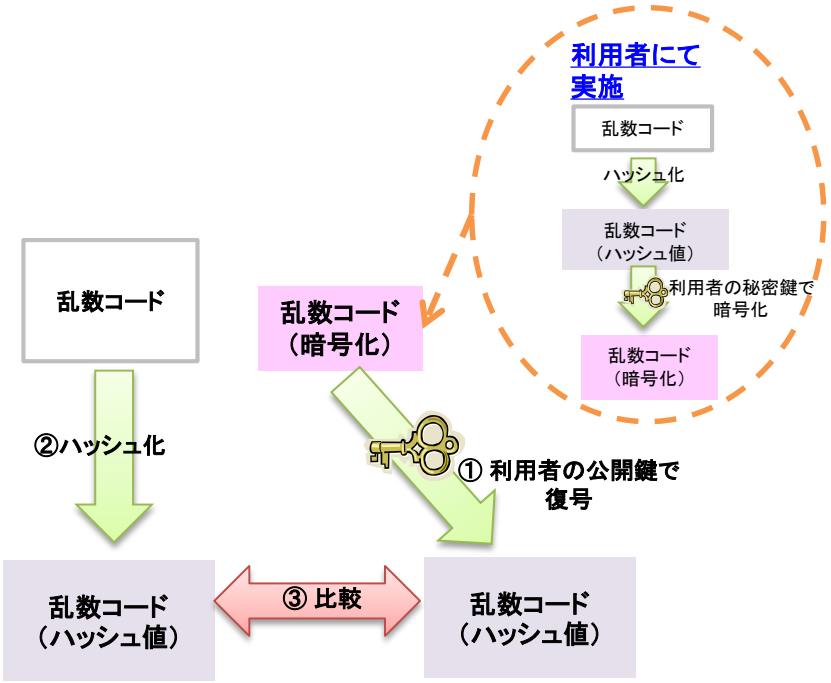


図 APPENDIX②-2 乱数コードの検証の流れ

図 APPENDIX②-2 で示したとおり、民間事業者において、乱数コードの検証は以下の流れで行う。

① 利用者が乱数コードをハッシュ化して利用者の秘密鍵にて暗号化したものを利用者の公開鍵で復号する。
② 乱数コードをハッシュ化する。
③ ①、②の結果を比較し、同一のものであることを確認することで、利用者証明が利用者本人によるものであることを確認したことになる。

【APPENDIX ③】FAQ（よくある質問とその回答）

分類	項番	質問内容
個人番号カード発行	1	個人番号カードは、国民全員に配布されるのでしょうか。それとも、個人番号カード発行に当たり、利用希望者による申込みが必要となるのでしょうか。
	2	電子証明書が格納される個人番号カードの受け取り方法について教えてください。
	3	個人番号カードの発行には、手数料が発生するのでしょうか。
電子証明書について	4	オンラインで各種申請手続を行う際の、署名用電子証明書の役割について教えてください。
	5	電子証明書に有効期間は設定されるのでしょうか。
	6	住所変更等が行われた場合、個人番号カード内の電子証明書の情報は自動的に更新されるのでしょうか。
紛失・盗難時の対応	7	紛失や盗難等によって、不正に入手された個人番号カードを用いて本人確認が行われた場合、後日紛失したと思われる日時以降に公的個人認証サービスで認証した民間企業やサービスに対して通知を行うなどの措置は用意される予定でしょうか。
情報セキュリティ対策について	8	個人番号カードの紛失・盗難時を想定したセキュリティ対策を教えてください。
IC カードリーダー装置について	9	個人番号カードを読み込むための IC カードリーダー装置は、利用者が準備する必要があるのでしょうか。
公的個人認証サービスの利用方法	10	利用者の最新住所を確認することは可能でしょうか。
	11	民間事業者が契約者の生死情報を確認する場合に利用することは可能でしょうか。
利用者及び民間事業者負担費用	12	公的個人認証サービス利用に伴う、利用者及び民間事業者で負担する必要がある費用はどのようなものがあるのでしょうか。

Q.1　個人番号カードは、国民全員に配布されるのでしょうか。それとも、個人番号カード発行に当たり、利用希望者による申込みが必要となるのでしょうか。

A.1　申込みが必要となります。
番号制度施行時に、全国民に通知カードによる個人番号の通知が行われますが、この通知とともに個人番号カードの申込書が同封される予定です。
利用者の顔写真と申込書を返送していただければ、申込みとなります。

Q.2　電子証明書が格納される個人番号カードの受け取り方法について教えてください。

A.2　「A.1」の申込み後、市町村窓口で本人確認を行ったうえで、個人番号カードが交付されます。

Q.3　個人番号カードの発行には、手数料が発生するのでしょうか。

A.3　無料です。但し、再発行については、原則として手数料が発生します。

Q.4　オンラインで各種申請手続を行う際の、署名用電子証明書の役割について教えてください。

A.4　署名用電子証明書は、書面で申請する場合の「印鑑登録証明書」に相当するものとお考えください。
電子署名を使ってオンラインで申請する場合と、実印を使って書面で申請する場合を対比して整理すると、図 APPENDIX①-1 のようになります。

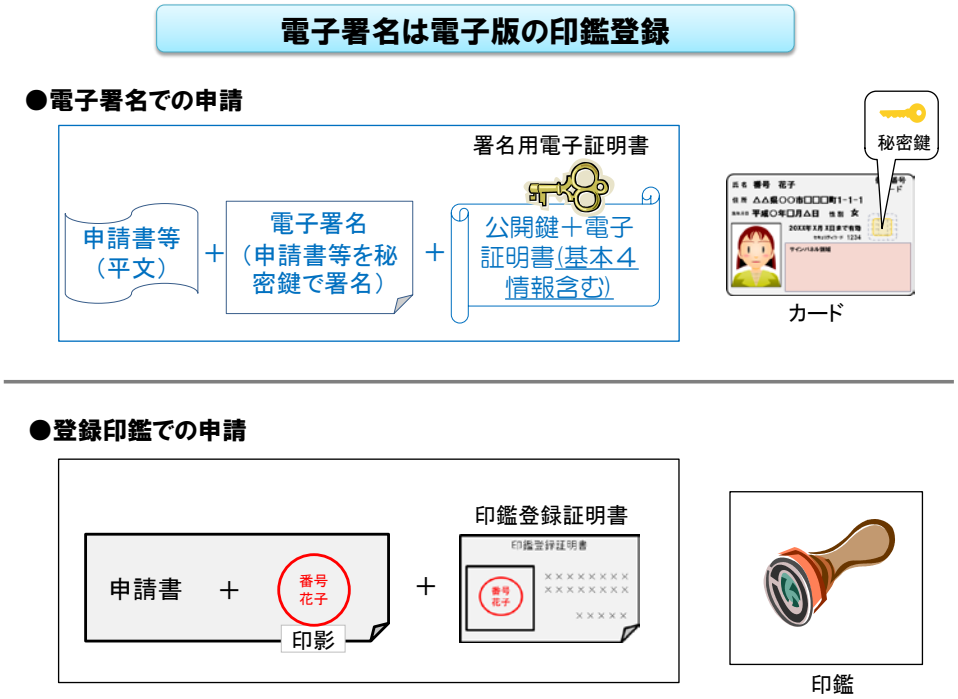


図 APPENDIX③-1 署名用電子証明書の役割

Q.5　電子証明書に有効期間は設定されるのでしょうか。

A.5　設定されます。
基本的には電子証明書の有効期間は、証明書発行から申請者の 5 回目の誕生日までとなります。ただし、電子証明書の有効期間が切れる前であっても、氏名・住所の変更等により、電子証明書が失効する場合があります。

Q.6　住所変更等が行われた場合、個人番号カード内の電子証明書の情報は自動的に更新されるのでしょうか。

A.6　市町村窓口にて住所変更等の行政手続を行うとともに電子証明書の再発行の申請を行うことで電子証明書の更新が可能となります。

Q.7　紛失や盗難等によって、不正に入手された個人番号カードを用いて本人確認が行われた場合、後日紛失したと思われる日時以降に公的個人認証サービスで認証した民間企業やサービスに対して通知を行うなどの措置は用意される予定でしょうか。

A.7　公的個人認証サービス側から特段の通知を行うことはありません。
公的個人認証サービスは、電子証明書の失効情報の提供のみを行います。

Q.8　個人番号カードの紛失・盗難時を想定したセキュリティ対策を教えてください。

A.8　個人番号カードの紛失又は盗難時は、電子証明書の発行を受けた本人が、公的機関が運営するコールセンターへ連絡することによって、電子証明書を利用できない状態にすることが可能です。
紛失又は盗難が発生してからコールセンターへ連絡するまでの期間については、「パスワードによる保護※1」によって、一定のセキュリティが確保されます。
なお、電子証明書を再び利用するためには、本人による市町村窓口での手続きが必要となります。

※1 パスワードによる保護
公的個人認証サービスの電子証明書等は、個人番号カード上の IC チップ内に格納されます。電子証明書等を利用するためには、IC チップ内のデータにアクセスする必要があり、その際は基本的には個人ごとに設定されたパスワードの入力が必要になります。

Q.9　個人番号カードを読み込むための IC カードリーダー装置は、利用者が準備する必要があるのでしょうか。

A.9　個人番号カードを読み込むためには、公的個人認証サービスに適合している IC カードリーダー装置を利用者に用意してもらう必要があります。
また、NFC 機能を有したスマートフォンをパソコンに接続して IC カードリーダー装置として使用すること、さらには、パソコンを使わずに携帯電話端末及び個人番号カード（IC カード）だけで認証を行えるようにすることについて検討を進めております。

Q.10　利用者の最新住所を確認することは可能でしょうか。

A.10　最新住所を確認するタイミングで、利用者による電子署名が行われることで確認可能です。
署名用電子証明書には最新の基本 4 情報（氏名、住所、生年月日、性別）が含まれているため、電子署名時に署名用電子証明書を受領し、その電子証明書が失効していないことを確認することで、電子証明書に記載されている住所が最新の情報であることを確認できます。

Q.11　民間事業者が契約者の生死情報を確認する場合に利用することは可能でしょうか。

A.11　電子証明書の所有者が死亡すると、死亡に伴い住民票が消除されたタイミングで、電子証明書が失効します。
そのため、本人同意を得た上で、電子証明書が失効していないことを定期的に確認することで、死亡等の事実があったことをすることが可能です（詳細は 16 ページをご覧ください）。

Q.12　公的個人認証サービス利用に伴う、利用者及び民間事業者で負担する必要がある費用はどのようなものがあるのでしょうか。

A.12　主な費用として、下記の費用が発生すると想定されます。

■利用者
- PC 等のインターネット接続環境及び IC カードリーダー装置をご用意していただく必要があります。

■民間事業者
- 公的個人認証サービス利用に伴う民間事業者側システムの構築費用
- 失効情報提供に伴う手数料