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 1.2 版－

デジタル庁
総務省

平成 27 年 9 月
令和５年５月 改正

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	平成 27 年 ７月	―	―
1.1	平成 27 年 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。
1.2	令和５ 年 ５月	・特定署名用電子証明書記録情報の提供機能の追加による改正 ・スマートフォン用電子証明書の提供開始に伴う改正	・特定署名用電子証明書記録情報の提供機能を追加 ・スマートフォン用電子証明書に関する対応等を追加

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

住民の利便性の向上及び行政運営の簡素化・効率化を図るため、国や地方公共団体の行政手続のオンライン化を初め、社会全体のデジタル化に向けた取組みが進められてきている。他方で、特に行政手続では、手続を行う住民の厳格な本人確認が求められるが、インターネットに代表されるデジタル社会においては、なりすまし、改ざんなどの課題が指摘されている。こうした課題を解決しつつ、社会全体のデジタル化を実現するためには、厳格な本人確認ができるオンラインサービスを、全国いずれに住んでいる人に対しても安く提供することが必要であることから、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成 14 年法律第 153 号。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、以下の者について公的個人認証サービスを利用し、オンライン手続の申請者について厳格な本人確認ができることとしている。

・行政機関等、裁判所、主務大臣（内閣総理大臣及び総務大臣をいう。以下同じ。）が認定した民間事業者等のうち、地方公共団体情報システム機構（以下「機構」という。）に公的個人認証法第 17 条第 1 項の届出をした者（以下「署名検証者」という。）
・上記の「署名検証者」に委託する「みなし署名検証者／サービスプロバイダ事業者」

以上のような公的個人認証サービスの民間活用を一層促すために、本ガイドラインを策定するものである。

(2) 本ガイドラインの想定対象者

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円滑にするため、以下について説明し当該サービスの普及を促進する。

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
- 民間事業者側に必要となる情報システム設備
- 主務大臣による認定基準・手続
- 失効情報提供手数料　　等

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３点について記述する。

(1) 公的個人認証サービスとは
(2) 公的個人認証サービス利用の流れ
(3) 現在の公的個人認証サービスの利用事例

(1)公的個人認証サービスとは

ア 公的個人認証サービスの仕組み

公的個人認証サービスとは、インターネット上で本人確認手段を提供するサービスである。インターネット上で申請や届出を行う際に、本サービスを用いることで、第三者によるなりすましやデータの改ざんを防ぐことが可能となる。

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、マイナンバーカード又はスマートフォン(*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は、マイナンバーカード又はスマートフォンから電子証明書を読み取り、これを利用することで電子署名やユーザ認証を行うことができる。

公的個人認証サービスの利用の流れについては、本章の「(2) 公的個人認証サービス利用の流れ」にて記述する。

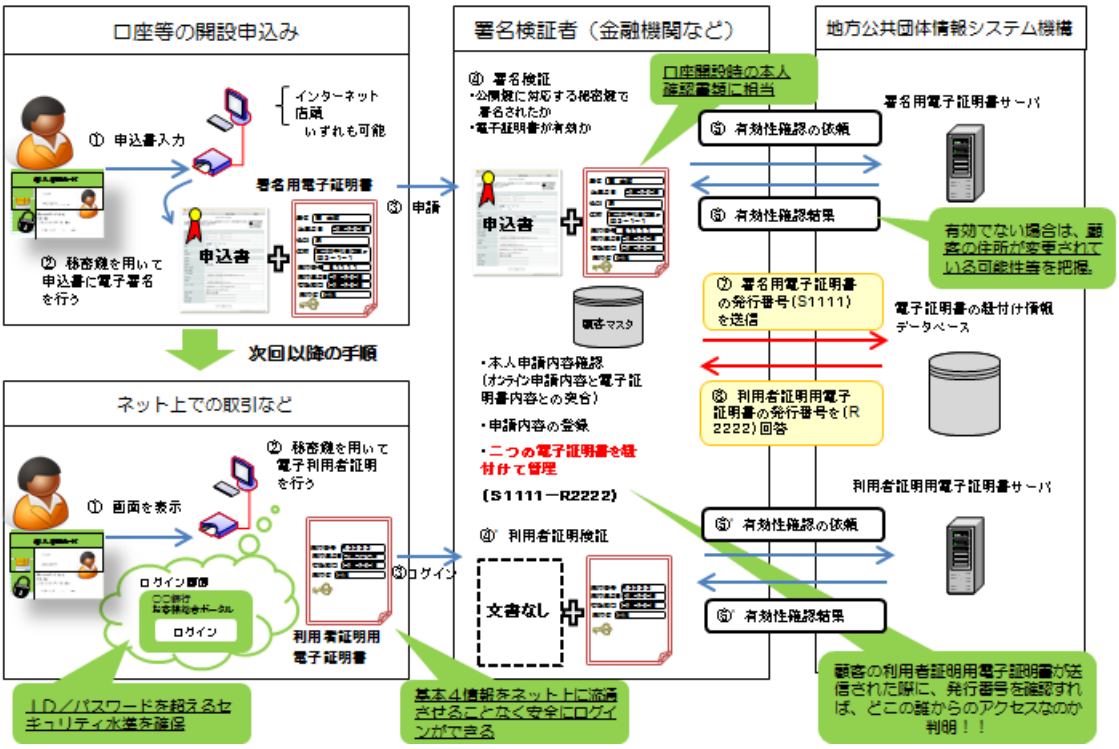
（*１）　一定の基準を満たしたチップを搭載したスマートフォンに限定される。

イ 署名検証者とは

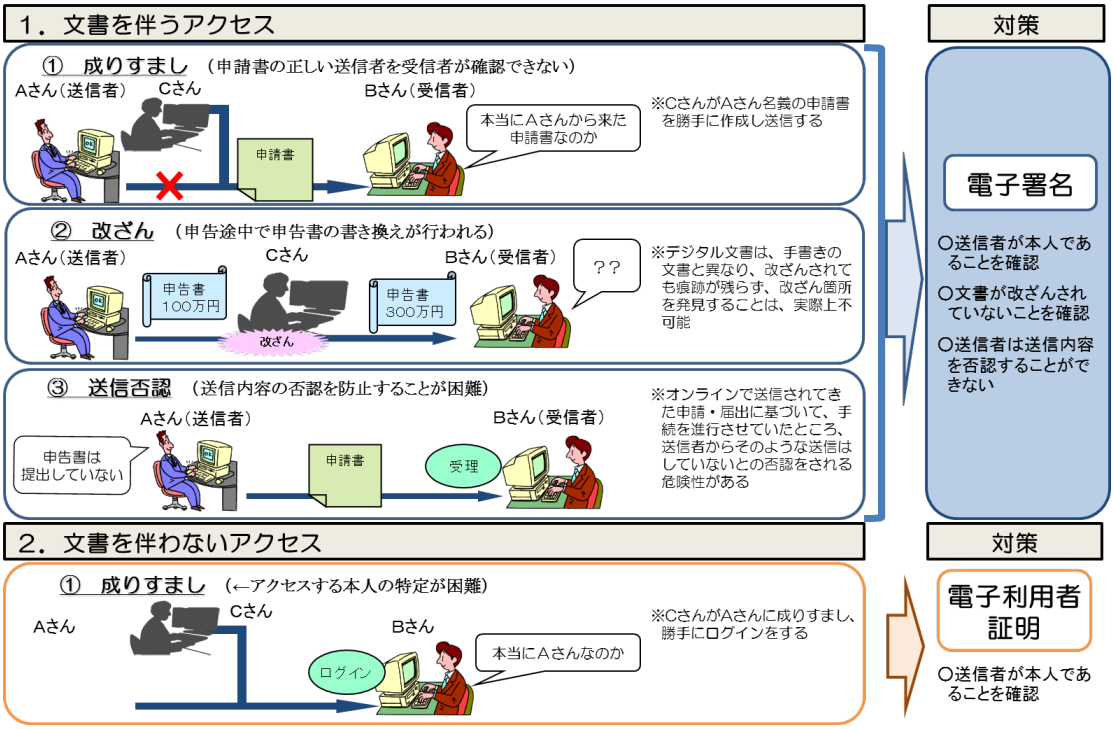
署名検証者とは、行政機関等、裁判所、主務大臣が認定した民間事業者等のうち、機構に公的個人認証法第 17 条第１項の届出をした者をいう。

公的個人認証法では、「署名検証者」について公的個人認証サービスを利用し、オンライン手続の申請者について厳格な本人確認ができることとしている。

＜図 2-1 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 2-2 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）＞



(2) 公的個人認証サービス利用の流れ

ア 電子証明書の発行

公的個人認証サービスの利用の流れは、図 2-3 のとおり。

＜図 2-3 公的個人認証サービスの利用フロー＞

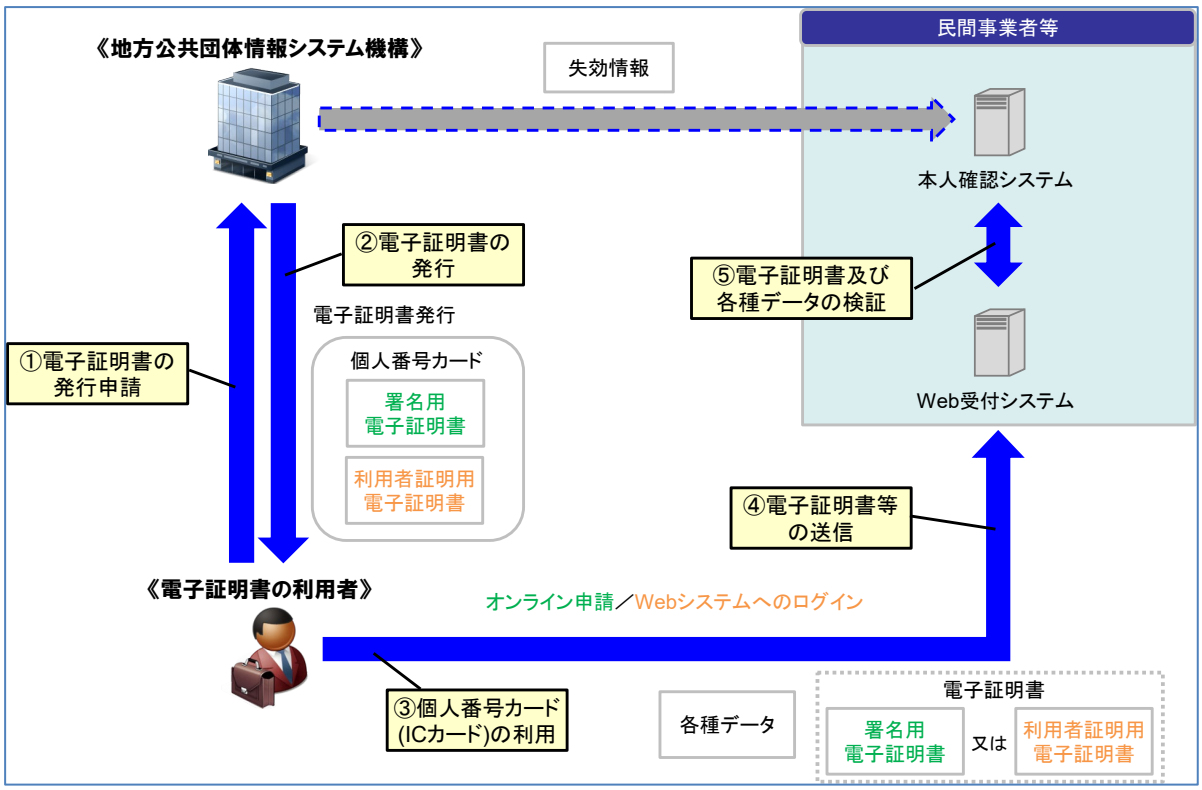


図 2-3 における①～⑤の詳細は、次のとおりである。

【マイナンバーカード用の電子証明書の場合】

① サービスの利用を希望する者(*2)は、各市区町村窓口を経由して、機構に対し電子証明書の発行申請を行う。

② 申請を受け付けた機構は電子証明書を発行し、各市町村窓口に通知する。申請者(*2)は、各市区町村窓口にて、発行された電子証明書を利用するための暗証番号を設定し、電子証明書が記録されたマイナンバーカードを受領する。

③ 電子証明書の発行を受けた者(*2)は、オンライン申請、Web システムのログイン時等に、マイナンバーカードをカードリーダライタ等にセットし、電子証明書を利用するための暗証番号を入力する。

④ 電子証明書発行を受けた者(*2)は、電子証明書、申請書等のデータを署名検証者(*3)に送信する。

⑤ 署名検証者(*3)は、機構から提供される電子証明書の失効情報を用いて、電子証明書の有効性を確認する。

（*2）図 2-3 内では≪電子証明書の利用者≫を指します。
（*3）図 2-3 内では「民間事業者等」を指します。

【スマートフォン用の電子証明書の場合】

① サービスの利用を希望する者(*2)は、各市区町村窓口において、マイナンバーカード用の電子証明書の発行を受ける。

② サービスの利用を希望する者(*2)は、スマートフォンでマイナポータルアプリにおいて、

マイナンバーカード用の署名用電子証明書を用いて、機構に対し電子証明書の発行申請を行う。

③ 機構はスマートフォン用の電子証明書を発行し、申請者(*2)に通知する。通知を受けた申請者(*2)は、電子証明書を利用するための暗証番号を設定の上、当該電子証明書をスマートフォンに格納する。

④ 電子証明書の発行を受けた者(*2)は、オンライン申請、Web システムのログイン時等に、電子証明書を利用するための暗証番号を入力する。

⑤ 電子証明書の発行を受けた者(*2)は、電子証明書、申請書等のデータを署名検証者(*3)に送信する。

⑥ 署名検証者(*3)は、機構から提供される電子証明書の失効情報を用いて、電子証明書の有効性を確認する。

(*2) 図 2-3 内では≪電子証明書の利用者≫を指します。
(*3) 図 2-3 内では「民間事業者等」を指します。

イ　電子証明書の検証

署名検証者は、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。署名検証者は、機構へ失効情報提供手数料(*4)を支払い、失効情報を入手することで電子証明書が有効であるかを判定する。

電子証明書は以下の場合に失効する。

・電子証明書の有効期間の満了
・マイナンバーカード又はスマートフォンの紛失・盗難・故障等
・(署名用電子証明書のみ) 婚姻による氏名変更、引越しによる住所変更等　　等

上記２つ目の「マイナンバーカード又はスマートフォンの紛失・盗難・故障等」については、後述「ウ　電子証明書の一時利用停止等」を参照されたい。

(*4)　失効情報提供手数料については、第４章にて説明する。

ウ　電子証明書の一時利用停止等

利用者がマイナンバーカードを紛失した場合は、市区町村窓口に届け出るほか、機構が運営するコールセンターへ電話することで、マイナンバーカードの利用を止めることができる。コールセンターに電話することで、電子証明書についても一時利用停止され、不正な利用を防止することができる。一時利用停止を解除するためには、利用者が市区町村窓口において手続をする必要がある。

また、電子証明書を格納したスマートフォンを紛失した場合においても、機構が運営するコールセンターに電話することで、電子証明書を一時利用停止することができる。

なお、電子証明書を格納したスマートフォンを下取りに出す等の場合には、利用者が自らスマートフォンを操作して、失効申請をする必要がある。

これらの手続が実施されることで、機構が署名検証者に提供する失効情報に反映され、一時利用停止解除や再発行には利用者自らが市区町村窓口又はスマートフォンにおいて手続をする必要があるため、署名検証者における対応は不要である。具体的な流れは、それぞれ以下のとおり。

【マイナンバーカードの場合】

Ⅰ．マイナンバーカードを紛失・盗難された利用者が、機構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、以下の対応を行う。

① マイナンバーカードを利用できない状態（一時利用停止）とする。

② 電子証明書を利用できない状態（失効／一時利用停止）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、失効情報として署名検証者に提供される。

Ⅲ．マイナンバーカード及び電子証明書の一時利用停止解除又は再発行を希望する利用者は、市区町村窓口にて手続を行う。

Ⅳ．再発行を申請した者は、電子証明書が格納されたマイナンバーカードを市区町村窓口にて受け取る。

【スマートフォンの場合】

スマートフォンの場合、紛失・盗難・故障等のケースに応じて、次の①②いずれかの対応が必要となる。

①スマートフォンを故障等により修理、下取りに出す等（利用者の任意）：失効手続

②スマートフォンの紛失・盗難：一時利用停止

①失効手続

Ⅰ．マイナポータルアプリにおいて失効を選択する。

Ⅱ．スマートフォンに格納された署名用電子証明書を用いて、失効申請を行う。
（端末操作ができない場合は、下記②同様にコールセンターへ連絡する。）

Ⅲ．新たにスマートフォン用電子証明書を申請する場合は、マイナポータルアプリから電子証明書の再発行を行う。

②一時利用停止

Ⅰ．スマートフォンの利用者が、機構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、電子証明書を利用できない状態（一時利用停止）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、失効情報として署名検証者に提供される。

Ⅲ．スマートフォンが手元に戻ってきた場合は、マイナポータルアプリから電子証明書の一時利用停止解除又は再発行を行う。

(3) 公的個人認証サービスの利用事例

ア　行政手続

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

上記の「e-Tax（国税電子申告・納税システム）」においては、利用者は、マイナンバーカードの読み取りが可能な端末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。

また、電子署名及び電子証明書が添付されることにより、申告等の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を保証している。

イ　民間サービス

公的個人認証サービスの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開設等の申込を受け、２回目以降はマイページへのログイン等、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が想定される。

すなわち、初回、口座開設等の申込を受けるシーンでは、申請書等に対して、署名用電子証明

書・電子署名を行った上で送付することで、申込者の実在性、氏名・住所等を正確・確実に把握し、かつ、改ざんや送信否認のおそれがないものとして申請書等を安心して受け取ることができる。

２回目以降のシーンでは、開設したマイページ等のログインの際に、利用者証明用電子証明書・電子利用者証明を送付してもらうことにより、ログインしてきた者が申請者本人であることを確認できる

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のメリットについて記述する。

(1) 公的個人認証サービスの高度なセキュリティ

マイナンバーカードは、公的な本人確認書類として用いることができるほか、以下①から③までの仕組みにより、マイナンバーカードの電子証明書は「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（平成 31 年２月 25 日各府省情報化統括責任者（ＣＩＯ）連絡会議決定）(*1) に規定されている最高位の本人確認レベルも満たしている。また、いわゆる公開鍵基盤（Public Key Infrastructure）の仕組みを用いているため、秘密鍵を用いて暗号化された情報は、なりすましを防ぎ、改ざんを検知することができる。これらにより、マイナンバーカードは対面でもオンラインでも安全・確実に本人確認ができるデジタル社会の基盤となっている。

①市区町村窓口において対面による厳格な身元確認のもと発行する。
②耐タンパー性 (*2) を有するハードウェアである。
③電子証明書の利用時には、上記①②に加え、カード本体と利用者自らが設定した暗証番号を利用する必要がある。

また、スマートフォンに搭載された電子証明書についても、以下のことからマイナンバーカードに係る電子証明書と同等に、最高レベルの本人確認を実現している。

①マイナンバーカードに係る署名用電子証明書を用いてセキュアな通信回線で発行される。
②耐タンパー性を有する等の一定基準を満たしたチップが搭載されたスマートフォンに限り利用可能。
③電子証明書の利用時には、上記①②に加え、スマートフォン本体と利用者自らが設定した暗証番号を利用する必要 (*3) である。

（*１）日本国内において、各種行政手続をデジタル化する際に必要となる、オンラインでの本人確認に対する考え方及び手法をまとめたもの。
（*２）耐タンパー性とは、IC チップ自身が有する偽造目的の不正防止策のことをいう（無理に情報を読み取ろうとするとメモリの内容が消去される等）。
（*３）利用者証明用電子証明書については、生体認証も可能。

(2) 公的個人認証サービスのメリット

本項では、署名検証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。

ア　電子証明書活用によるメリット
イ　認証局を民間事業者自ら構築する場合と比較した際の費用面でのメリット

ア マイナンバーカードに係る電子証明書の活用

以下では、署名用電子証明書及び利用者証明用電子証明書のメリットについて説明する。

(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、個人が署名検証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、署名検証者では表 3-1 に示す内容が実現可能となる。

＜表 3-1 電子署名により実現可能となること＞

項番	実現可能となること	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	改ざんの検知	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、署名検証者には、表 3-2 に示すようなメリット（例）が期待される。

＜表 3-2 署名用電子証明書活用による署名検証者のメリット（例）＞

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することにより、本人か否かを判断する。 （例）ID・パスワードによる認証
2	所持認証	本人しか持っていない所有物を提示することにより、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、マイナンバーカード又は電子証明書が搭載されたスマートフォンを所有していることによる認証（所持認証）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種類だけを用いる場合よりも高いセキュリティが確保される。なお、スマートフォンの場合には、４桁の暗証番号に代わり、スマートフォンで設定している指紋認証等の生体認証機能の利用が可能である（署名用電子証明書は対象外）。

署名検証者は、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（例）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（例）＞

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 ID・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 マイナンバーカード用又はスマートフォン用の電子証明書による認証の利用者増加に伴い、ID・パスワードによるログイン認証利用者が減少する。 ➢ 利用者が電子証明書の暗証番号を失念した際の対策は不要 電子証明書の暗証番号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 ➢ 電子証明書の暗証番号のみの管理 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、電子証明書の暗証番号の管理のみとなる。

イ 認証局を民間事業者自ら構築する場合と比較した際の費用面

民間事業者が電子証明書を利用する場合、公的個人認証サービス以外に、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、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）をトラストアンカーとして、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。失効情報は、最新の住民基本台帳の情報を基に管理されているため、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情報を利用できないため、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で、より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必要があるため、認証局を構築・運営するには、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、単独での負担額は大きなものとなる。それに対し、公的個人認証サービスを利用する場合は、認証局を機構が担うことになるため、民間事業者は認証局システム構築費用の負担がない。公的個人認証サービスを利用する場合、民間事業者が失効情報手数料等、継続的に機構へ支払う費用が発生するが、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負担額が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を利用する場合は、より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、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（例）＞

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。(*4)	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。

（*４） 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。詳細については「第４章（３）失効情報提供手数料」を参照されたい。

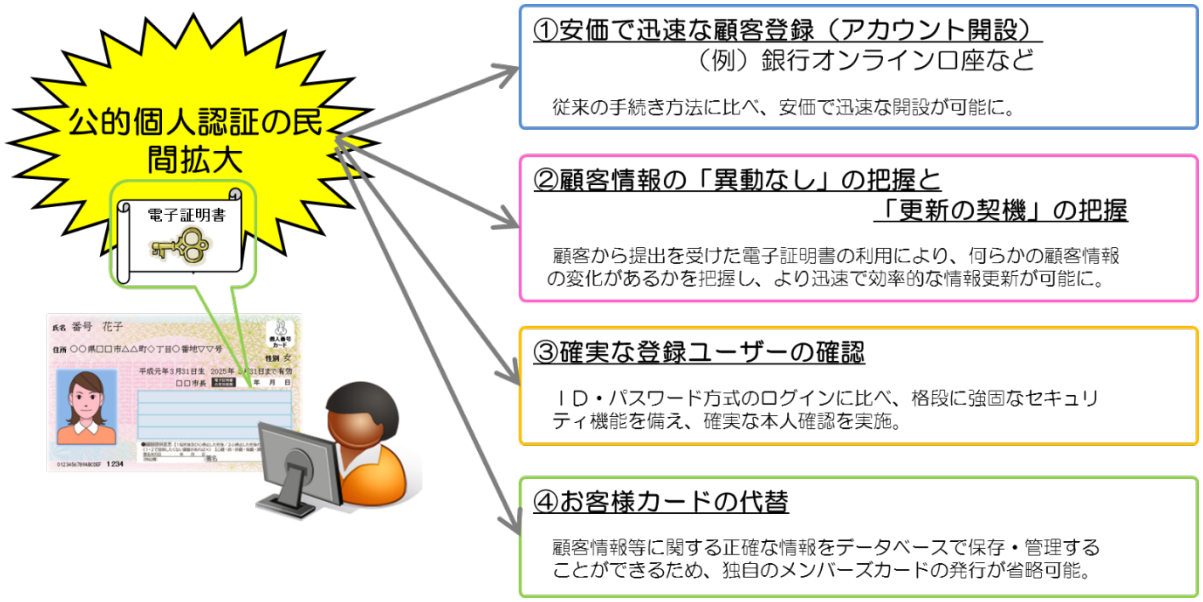
(3) 民間事業者の公的個人認証サービス利用によるメリットと具体的な事例

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な事例と合わせて分析して記述する。

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、具体的には図 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＞



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

民間事業者は、公的個人認証サービスを利用することにより、「正確・迅速・安価な顧客登録（アカウント開設）が可能に」なる。

従来は（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が必要があり、時間も費用もかかっていた(*5)。

しかし、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ため、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(*6)。また、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。

（*５）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。

（*６） 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ている。

(ｲ) (ｱ)以外の事業者について

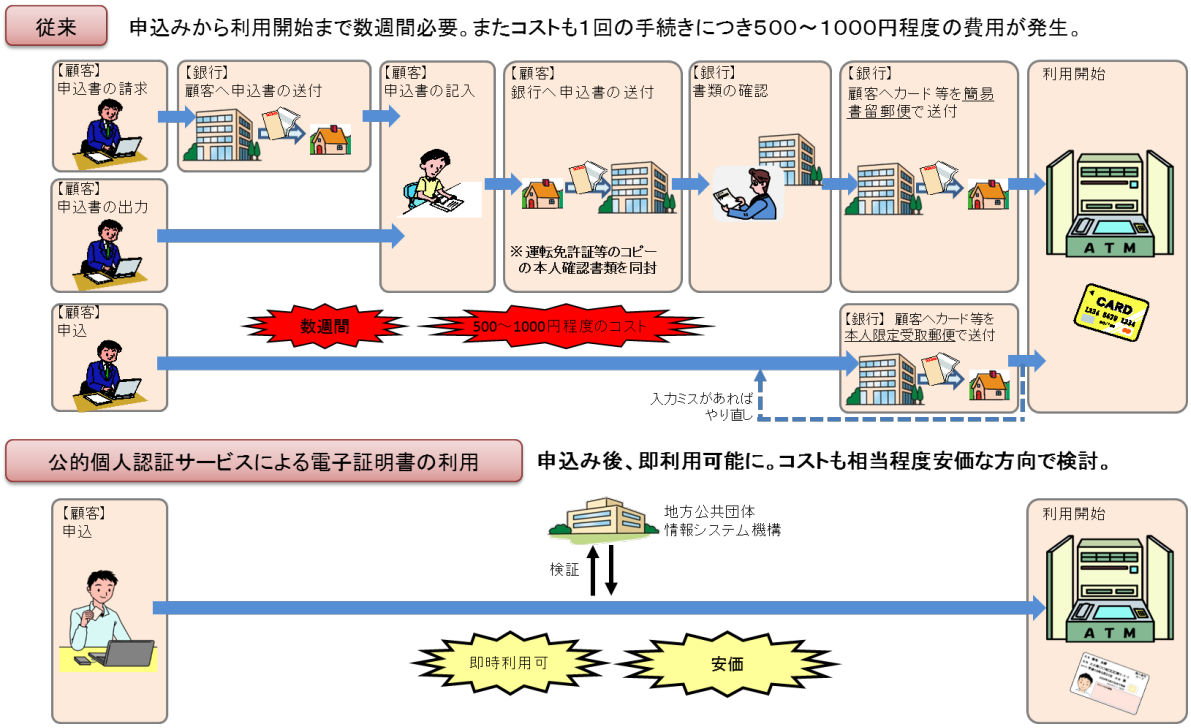
現在、特に身分証明書の郵送を求めず、申込者の申告する氏名・住所等を登録している事業者においても、新たに公的個人認証サービスを利用し、正確な顧客情報を把握するメリットは大きいと考えられる。

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(*7)ことで、契約締結後直ちに、商品を発送することも可能になると考えられる。

また、メリット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、例え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。

（*７）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、利用者証明用電子証明書・電子利用者証明を受け、本人の同一性を確認する。

＜図 3-2 顧客登録のビフォー・アフター＞



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

民間事業者は、公的個人認証サービスを利用することにより『顧客情報の「異動の有無」の把握が可能に』なる。

従来の方法は（図 3-3 左欄）、例えば、ユーザー登録の１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必要があった。このため、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、相当の費用を要していた。

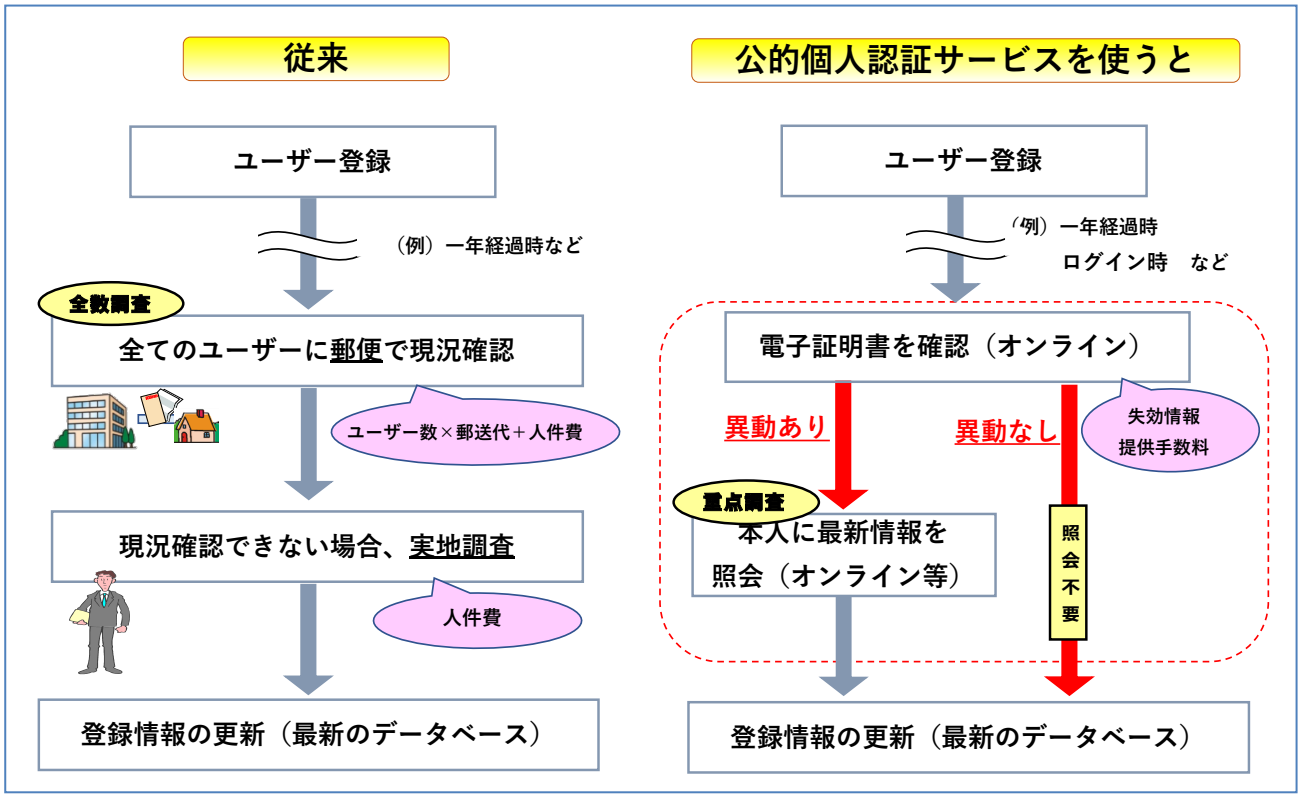
しかし、民間事業者が公的個人認証サービスを利用し、顧客の同意を得て、一定期間ごとに電子証明書の失効の有無を確認することで、顧客の異動等を把握することができ（図 3-4）、これまで生じていた費用削減が可能である（*8）。

（*8） なお、令和５年５月より、あらかじめ本人の同意を得ておくことで、失効している場合でも機構から最新の基本４情報を提供することができる仕組みが開始される。詳細は「５.本人同意に基づく最新の利用者情報（基本４情報）提供サービスの概要」にて記述する。

(ｲ) (ｱ)のうち、生命保険会社について

公的個人認証サービスを利用することで『顧客情報の「異動の有無」の把握』が可能になるというメリットは、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、保険金の未払いリスクを回避できる。また、年金保険であれば、年金支払いの都度、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年金を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大幅に減らすことができる。

＜図 3-3 顧客情報の異動の把握ビフォー・アフター＞



＜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とるべき対応＞

	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。

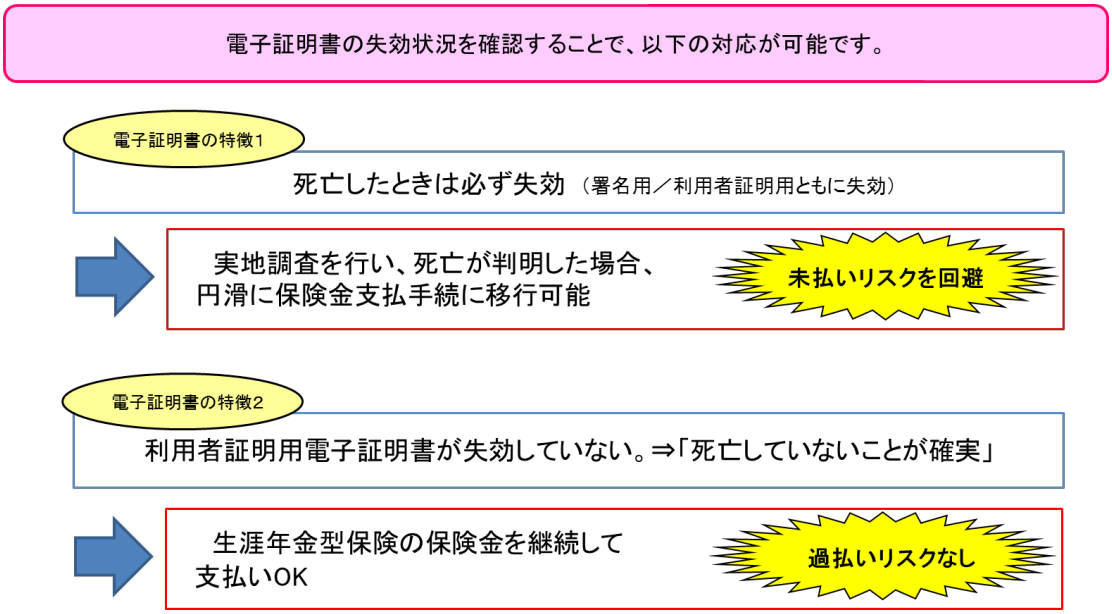
署名用　：×失効
利用者証明用　：○有効
↓
住所・氏名等の確認手続へ
→①更新後の署名用電子証明書を送信してもらう
②個人番号カードの入力補助アプリの記録情報を送信してもらう

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 3-5 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。

しかし、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）ことで、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。

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

民間事業者は公的個人認証サービスを利用することにより、「確実な登録ユーザーの確認」が可能になる。

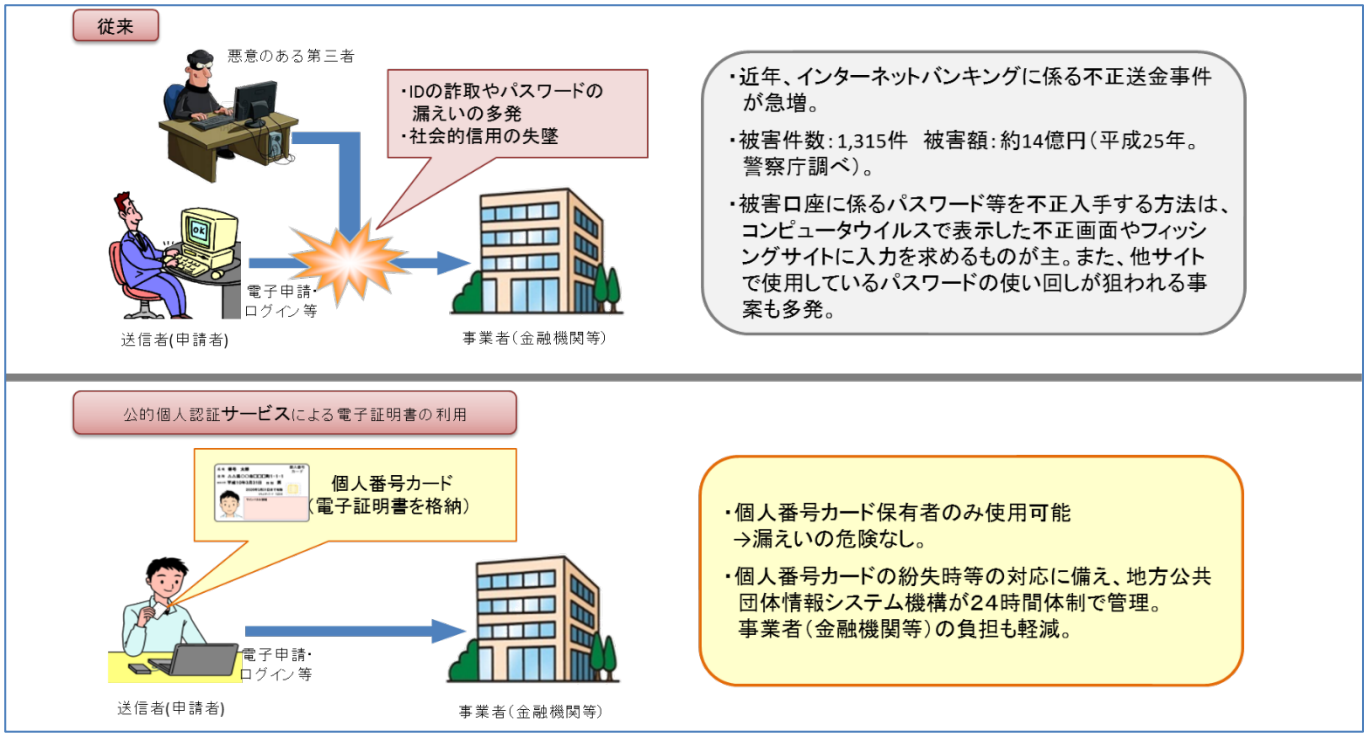
従来の方法（図 3-6 上段）は、悪意のある第三者に ID・パスワードが詐取され、なりすましが行われる危険がある。

しかし、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、マイナンバーカード又はスマートフォンの 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）ため、盗まれることはない。

万が一パスワードが探知されても、本人の電子証明書が格納されたマイナンバーカード又はスマートフォンを所持していなければ、決してなりすましできないため、従来の ID・パスワードによるものに比較し、はるかに強固な認証手段といえる（図 3-7）(*9)。

（*9） マイナンバーカード又はスマートフォン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、類推されにくい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＞



＜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＞

	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。

メリット④：お客様カードの発行が不要に

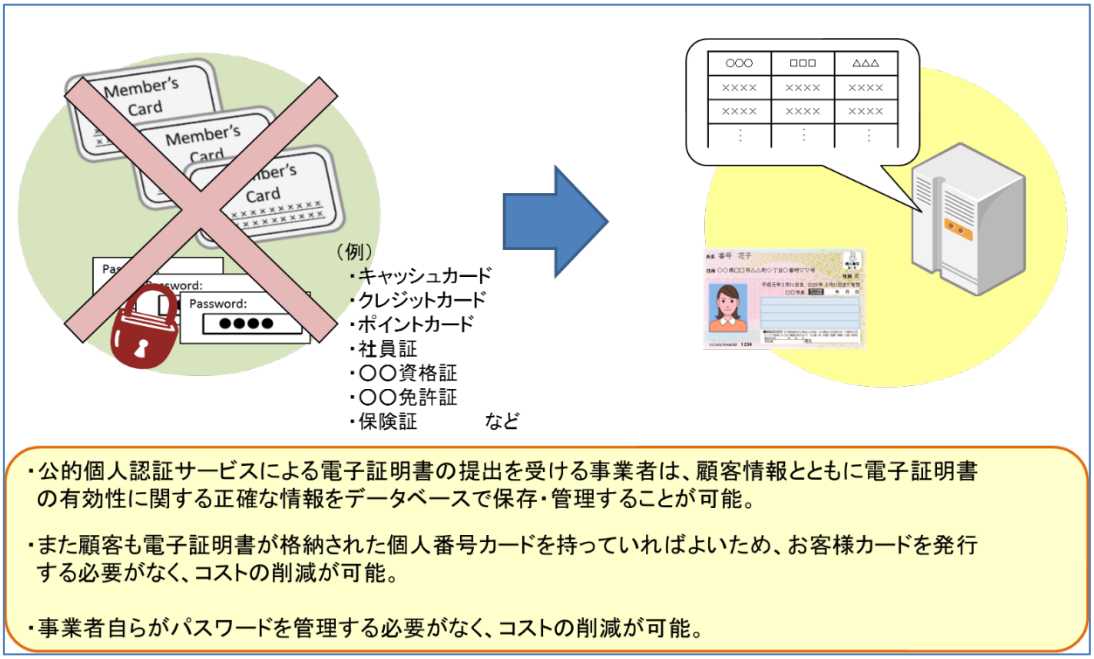
民間事業者は、公的個人認証サービスを利用することにより、「お客様カードの発行が不要に」なる（図 3-8）。

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、相当の費用を要していた。

しかし、公的個人認証サービスを利用する場合には、お客様カードは不要となり、相当の費用削減が可能となる。万が一、マイナンバーカード又は電子証明書が搭載されたスマートフォンを紛失した利用者は、24 時間 365 日のコールセンターに電話すれば、15 分以内 (*10) というスピーディな一時利用停止が可能だが、この運用費用も、民間事業者が特段の負担を求められるものではない。

（*10） 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。

＜図 3-8 お客様カードが不要に ビフォー・アフター＞



イ　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) 電子証明書の新旧シリアル番号 (*11) の紐付けサービス（図 3-9）

利用者が、署名用電子証明書又は利用者証明用電子証明書を更新した場合、電子証明書のシリアル番号が変わることになる。

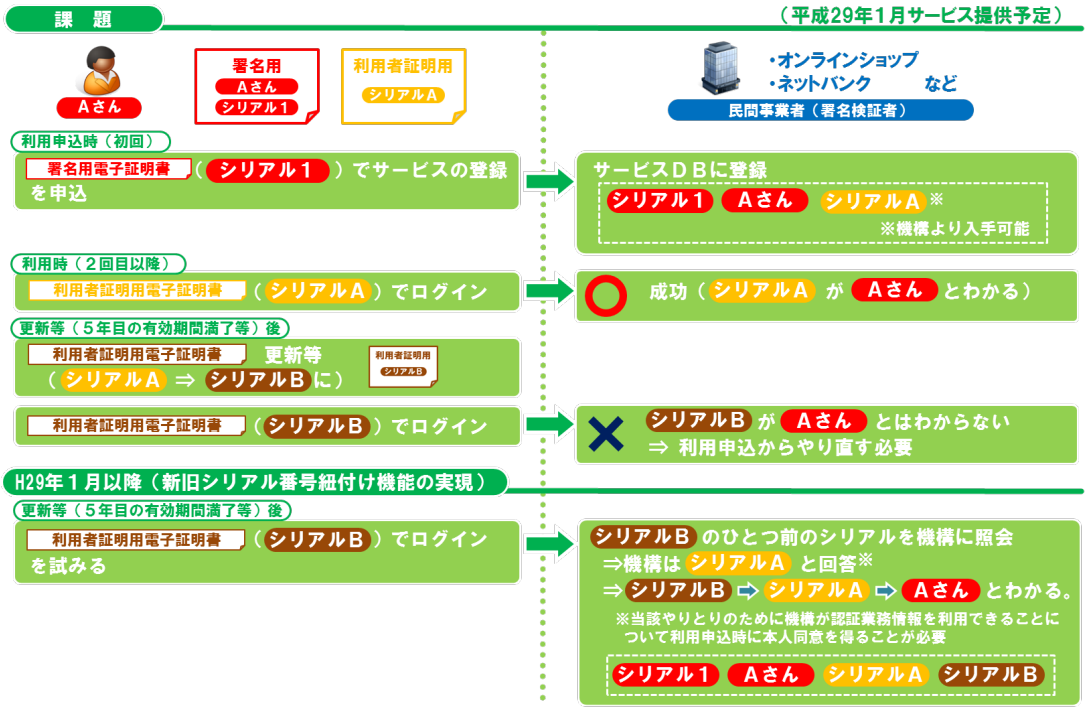
この場合、民間事業者はこの「更新前後の電子証明書の同一性」を把握できないため、再度、利用者登録をする必要性が生じ得る。

しかし、民間事業者も利用者の同意を前提に、機構が提供する電子証明書の新旧シリアル番号の紐付けサービスにより「更新前後の電子証明書の同一性」を把握することが可能となる。

具体的には、署名用電子証明書又は利用者証明用電子証明書の新しいシリアル番号を利用者から受け付けた場合、当該シリアル番号の一世代前のシリアル番号を機構に問い合わせることで取得が可能となる。

（*11）「発行番号」のことをいう。以下同様。

＜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）＞



4　公的個人認証サービス利用の手引き

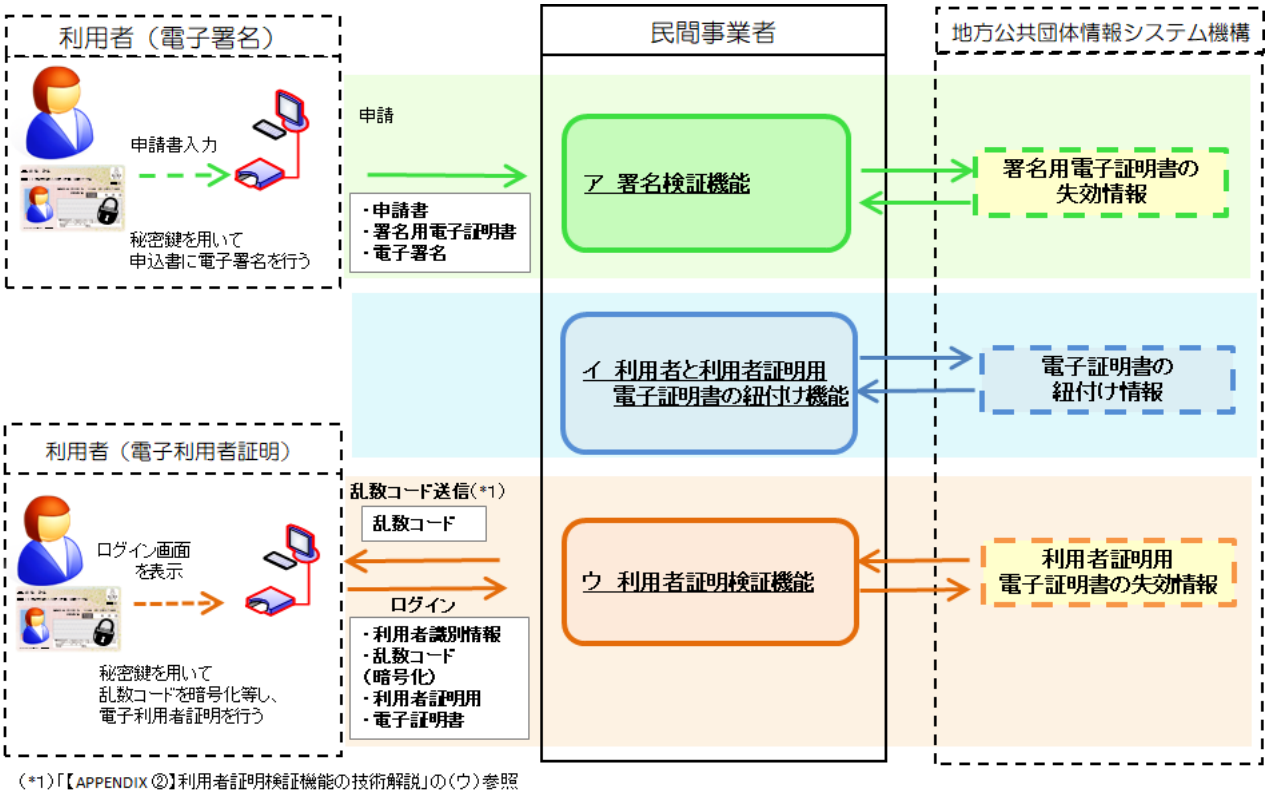
本章では、民間事業者が公的個人認証サービスを利用するための手引きとして、次の３点について記述する。

(1) 民間事業者側システム要件
(2) 主務大臣による認定
(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は図 4-1 のとおり。

＜図 4-1 公的個人認証サービスのシステム全体の流れ＞



(*1)「【APPENDIX ②】利用者証明検証機能の技術解説」の(ウ)参照

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後述の「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＞

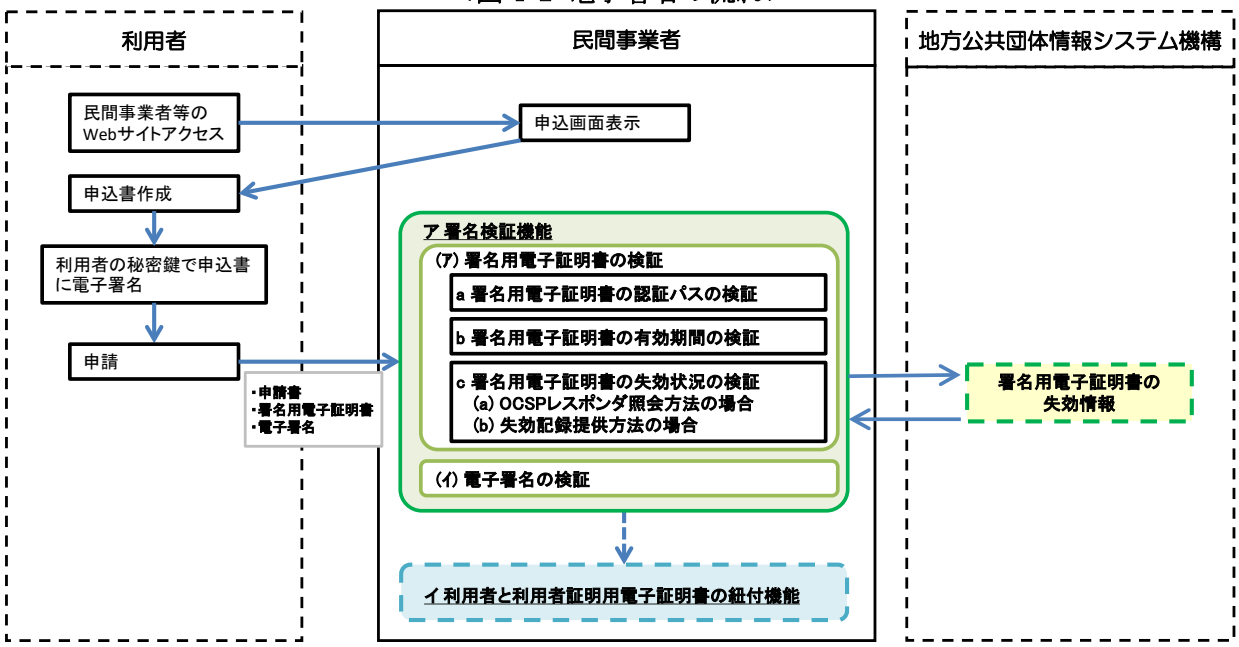


図 4-2 で示したとおり、民間事業者では、署名検証を行うに当たり、以下の検証を行う必要がある。

(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情報が記録されていないため、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することができない。そこで、民間事業者が利用者証明用電子証明書を利用する場合には、利用者ごとの「利用者識別情報」と「利用者証明用電子証明書」を紐付ける必要がある。そのための方法として、同一個人宛てに発行された「署名用電子証明書の発行番号（「シリアル番号」のことをいう。以下同様。）」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。

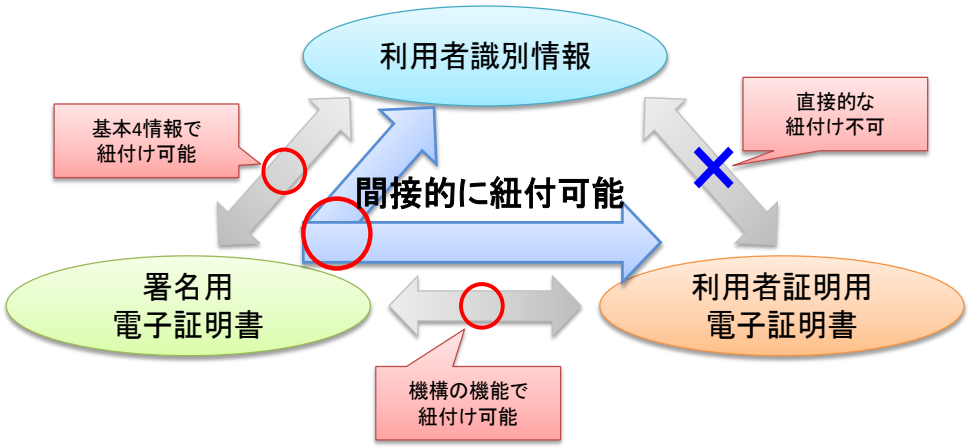
「署名用電子証明書」には基本４情報が記録されているため、それを基に、「利用者識別情報と署名用電子証明書を紐付ける」ことが可能である。また機構は、署名用電子証明書の発行番

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。

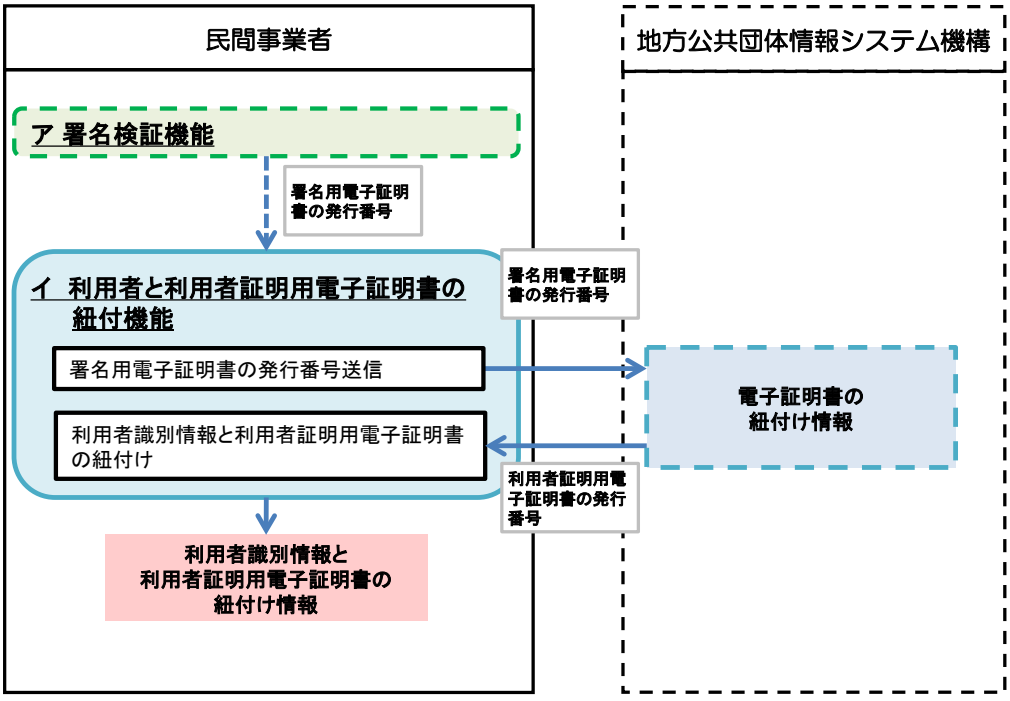
この場合の紐付け方法の全体イメージを図 4-3 に、民間事業者と機構における本機能を使用した紐付け処理の流れを図 4-4 に示す。

なお、署名用電子証明書及び利用者証明用電子証明書の発行番号については、電子署名等確認業務以外の業務において、個人を識別し管理するための符号として直接に使用してはならず、また、外部に提供してはならない。

＜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＞



＜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＞

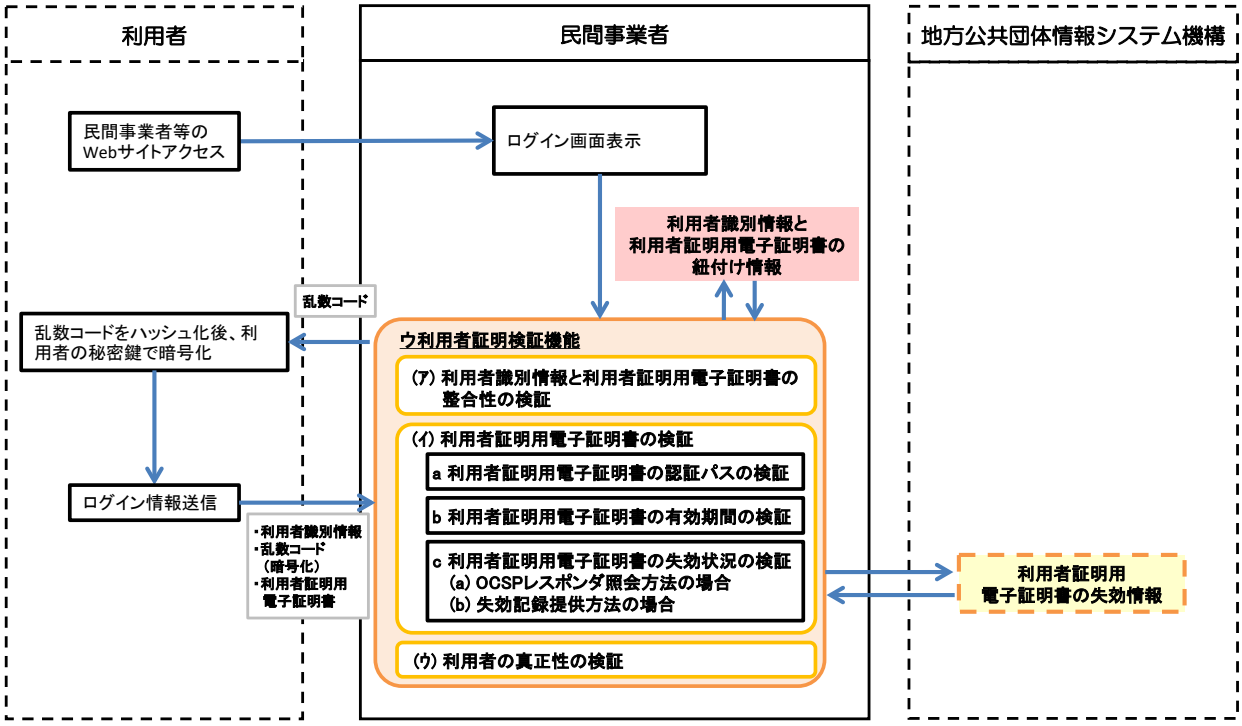


図 4-5 に示したとおり、民間事業者では、利用者証明を検証するに当たり、以下の検証を行う必要がある。

(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

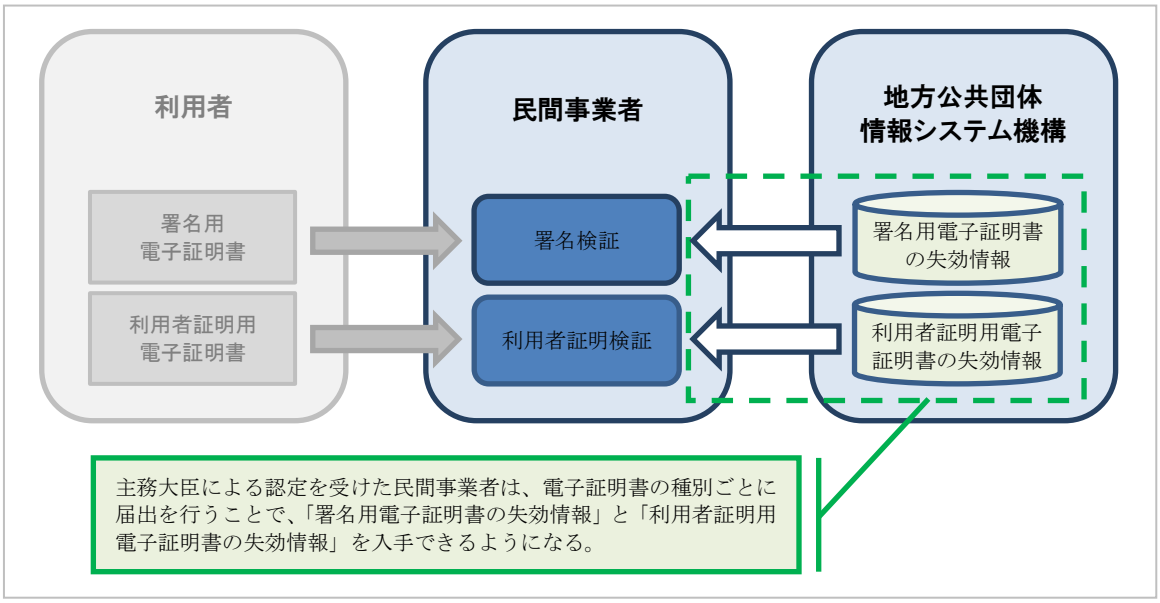
(ア)から(ウ)までの処理は、公的個人認証サービスに特化した方式ではないため、電子証明書に関して一般に普及している仕組みを用いて実現可能である。
(ア)から(ウ)までの内容については、「【APPENDIX ②】利用者証明機能の技術解説」を参照のこと。

(2) 主務大臣による認定

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、公的個人認証法第 17 条第１項第６号の規定により、主務大臣による認定を受ける必要がある。（同号に規定する認定のほか、民間事業者は、同項第４号及び第５号の規定により、署名検証及び利用者証明検証を行うことができるが、以下では、同項第６号の規定による認定に限り、解説することとする。）

主務大臣の認定を受けた民間事業者は、機構に対して失効情報を求めることによりそれを入手することができ、公的個人認証サービスの利用が可能となる。なお、機構に対する失効情報の提供依頼は、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。概要を図 4-6 に示す。

＜図 4-6 失効情報の入手と主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、不適切な利用を防止するために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際には電子証明書の失効情報が必須であるが、失効情報の提供範囲を主務大臣が認定した民間事業者に限定することで、不適切な利用の抑止を行っている。

主務大臣は、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、まずは以下の２点について解説する。

(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。

公的個人認証法において、署名検証者には、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＞

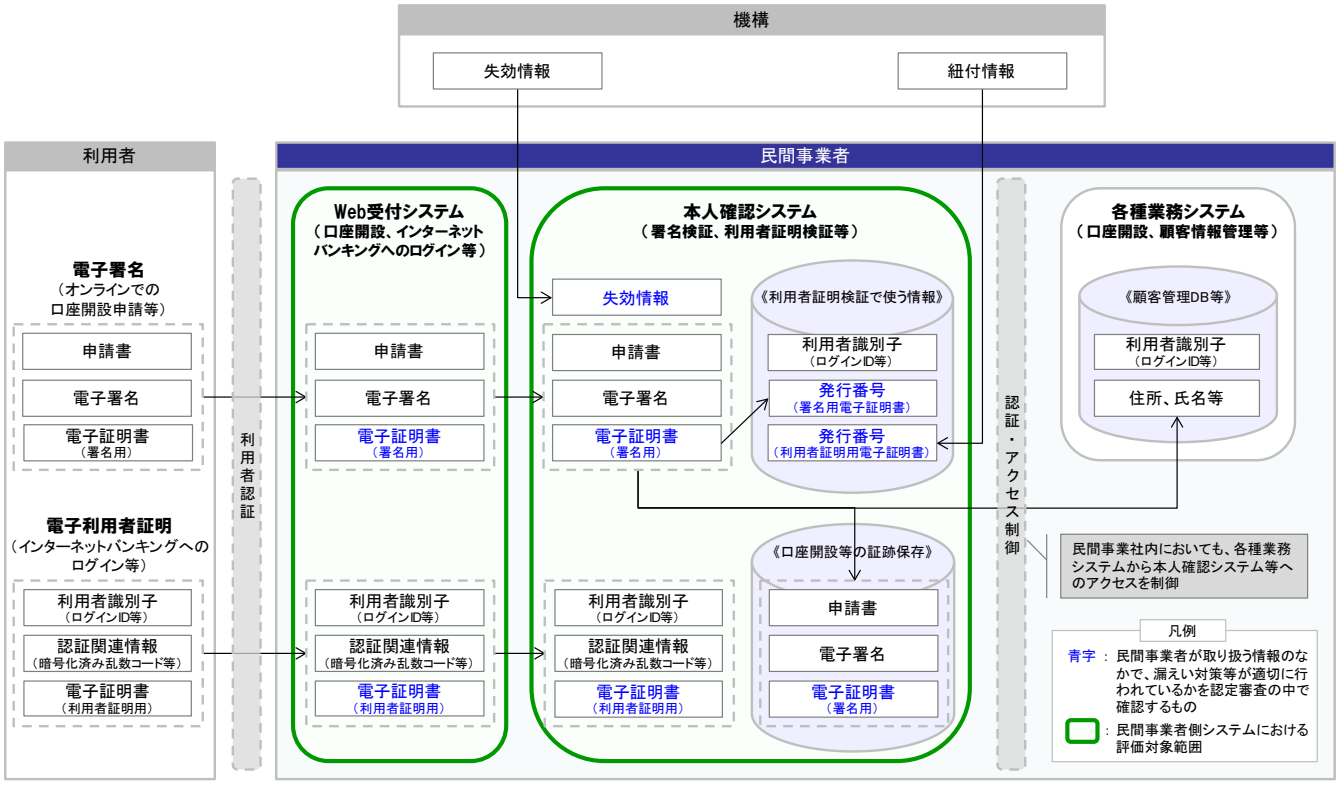
項番	情報名	説明	関連条文	目的
1	署名利用者検証符号	署名用電子証明書内に格納されている、利用者の公開鍵	第 19 条第３項	目的外利用の禁止
2	利用者証明利用者検証符号	利用者証明用電子証明書内に格納されている、利用者の公開鍵	第 38 条第３項	目的外利用の禁止
3	失効情報	署名用電子証明書及び利用者証明用電子証明書の失効状況を確認するための情報	第 50 条第１項及び第２項 第 51 条第１項及び第２項	適切な管理義務
			第 52 条第１項及び第２項 第 53 条第１項及び第２項	目的外利用の禁止
4	失効情報リスト	複数の失効情報がとりまとめられ、CRL (*2) 形式になったもの	第 54 条第１項及び第２項 第 55 条第１項及び第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している図 4-7 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

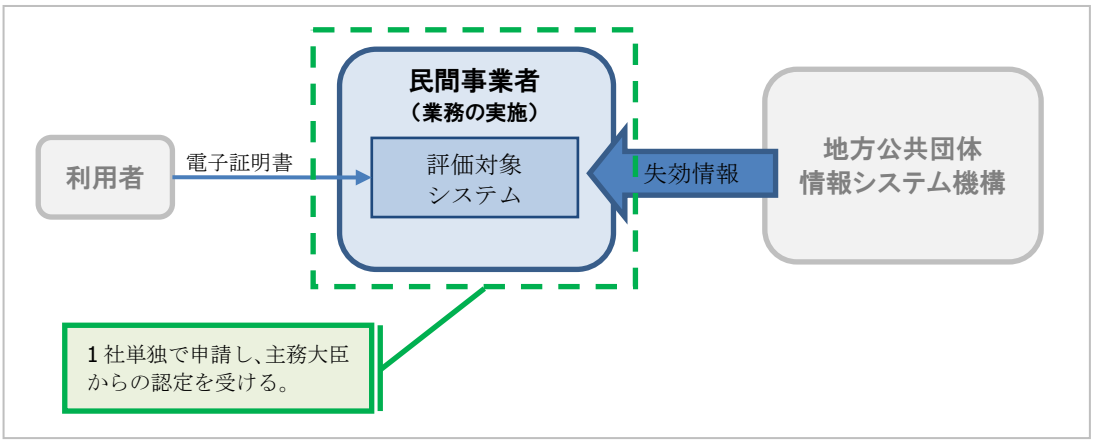
失効情報の入手に際しては、公的個人認証サービスを利用する民間事業者ごとに認定を受けることが基本となる【例 1】。ただし、システムの管理を外部委託する場合等においては、複数の民間事業者が連携した形での申請・認定となる場合がある【例 2】。

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、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。

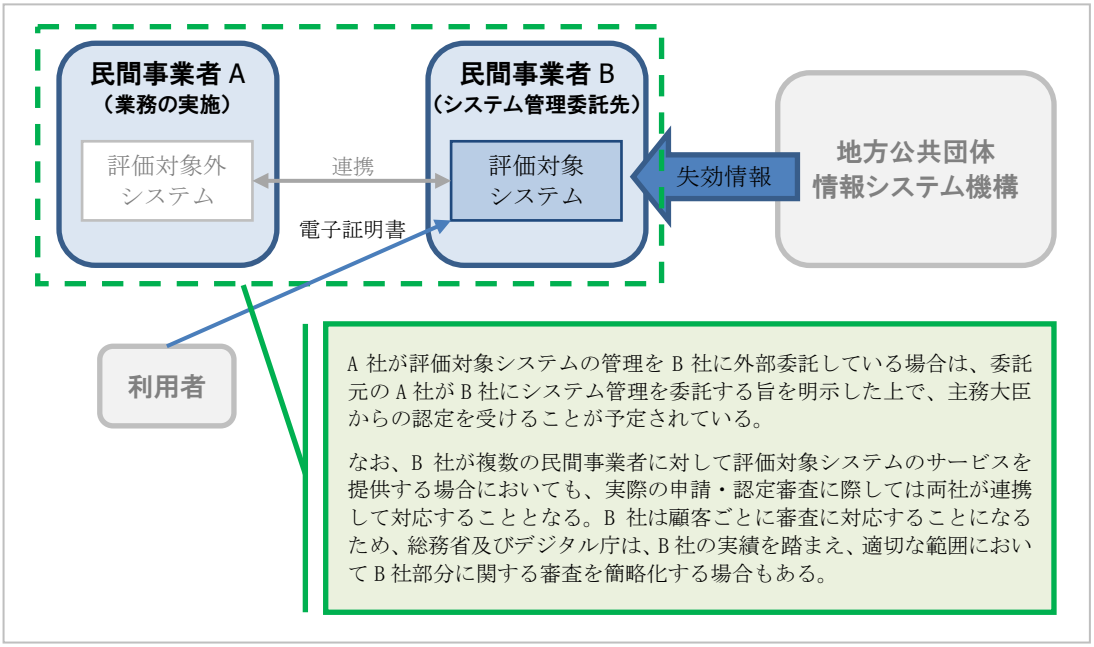
＜図 4-8 単独で認定を受ける場合＞



【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、主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、「電子証明書の受付・有効性確認等のためのシステム」を、各民間事業者が個別に整備・運用するのではなく、特定の事業者（いわゆる「プラットフォーム事業者」）が整備し、これを、各民間事業者が委託し利用することで、いわゆる「割り勘効果」により、各民間事業者の導入・利用費用を大きく削減することが期待できる。

このような場合を想定し、次のような趣旨の特例を設けられている。

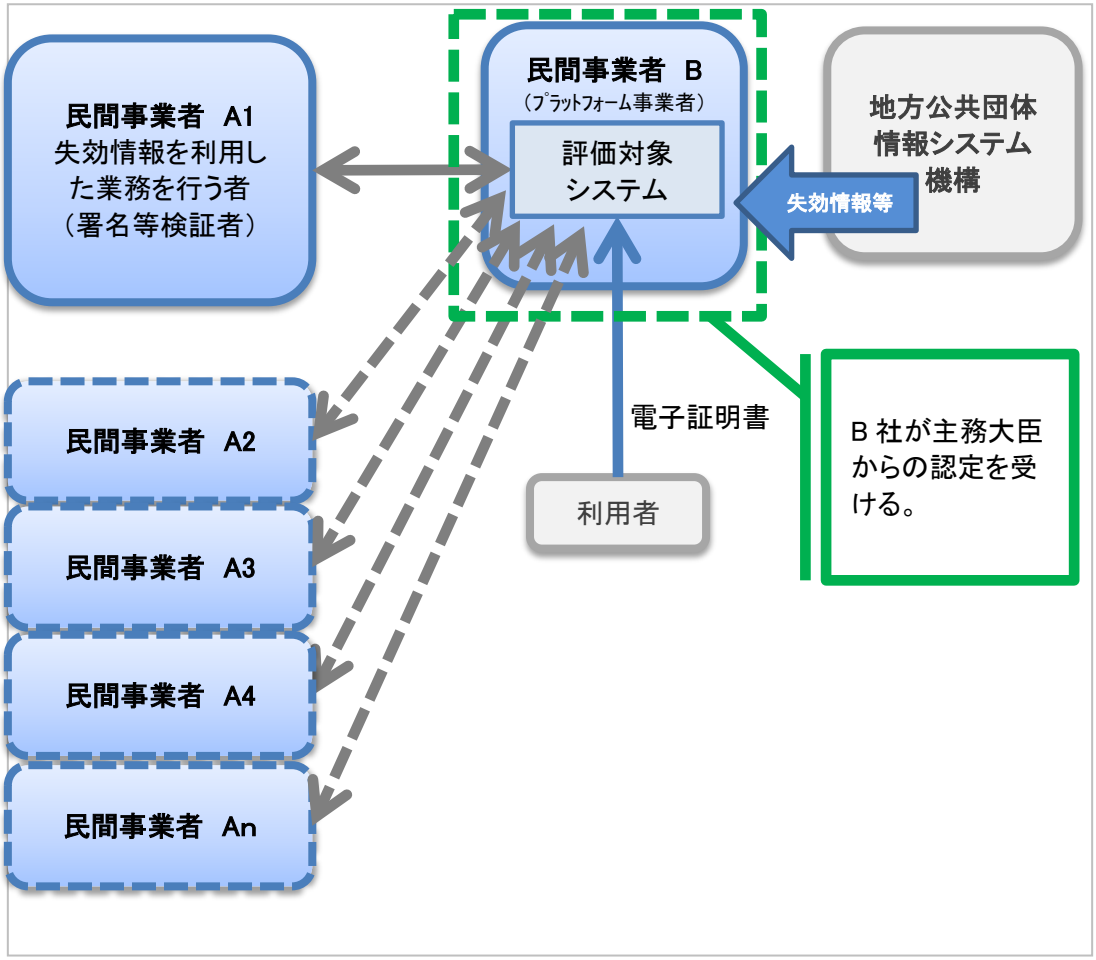
下記、図 4-10 の例では、法第 17 条第 1 項第 6 号に規定する者を挙げているが、同項第 4 号及び第 5 号に規定する者についても、令和 3 年 2 月より、本特例が適用されることとなった。なお、法第 17 条第 1 項第 1 号から第 3 号までに規定する行政機関等の者については、本特例を適用されず、機構へ届け出ることで自ら署名検証者になる必要がある。

① 「受託する者（民間事業者 B）」が、委託する者（民間事業者 A1～An）に代わり、主務大臣の認定（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～An）は、主務大臣の認定が不要。

② 「委託する者（民間事業者 A1～An）」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～An）は、機構への届出が不要。

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、主務大臣の認定、機構への届出などの法定の手続も、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。サービスプロバイダ事業者）に代わって担うことを可能とし、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こととしている。

＜図 4-10 プラットフォーム事業者の場合＞



(エ) サービスプロバイダ事業者が行ってはならない業務

プラットフォーム事業者の特例では、公的個人認証サービスの民間活用を促すために、公的個人認証法施行規則第 29 条にみなし規定を設けることで、サービスプロバイダ事業者が主務大臣認定を取得しなくとも署名検証者と同等の地位を得られるものとして創設された。しかしながら、サービスプロバイダ事業者は以下の業務を禁じられているため注意が必要である。

① 本人から提出された電子証明書を保持してはならない。
② 電子証明書の発行番号を取得・保持してはならない。

イ 認定基準

民間事業者は、主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及び現地調査を基本として行われる。

現時点の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、令和２年５月に、認可を受けた利用者証明検証者は、利用者証明利用者本人が電子利用者証明を行ったことの確認を、暗証番号ではなく下記①②いずれかの方法で行うことができるとされたが、それらの認可基準については、本項では省略する。

①マイナンバーカードの写真と利用者が同一者であることを目視により確認する方法
②マイナンバーカードの写真と利用者が同一者であることを機器を用いて確認する方法

また、電子証明書を扱うシステムについては、令和３年２月より、クラウドを活用することも認められたが、以下ではオンプレミスを前提として記載する。

＜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	主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。

＜図 4-11 【評価項目】規程類の整備について＞

【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 ： 署名用電子証明書に記録されている、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に記録されている、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及びデジタル庁へ提出することにより、本項目への充足を証明する。なお、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 4-12 【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 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及びデジタル庁に説明する。

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及びデジタル庁に提出する。
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 4-13 【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 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及びデジタル庁に提出する。
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。（ただし、必要に応じて、調査票等に概要の記載等を求めることがある。以下同じ。）

＜図 4-14 【評価項目】動作を記録する機能について＞

【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及びデジタル庁に提出する。
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 の認定証の提示をもって、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＞

【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、端末の盗難や不正持ち出し、署名検証等の業務従事者以外が端末に触れることができないよう、棚や机等に施錠保管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及びデジタル庁に提出する。
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 4-16 【評価項目】外部組織との連携に係る措置について＞

【項番 6】外部組織との連携に係る措置

概要

主務大臣の認定を申請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。

要求事項

署名検証等に係る業務の一部を外部へ委託する場合は、委託する業務の範囲を明確にした上で、委託元と委託先の間で、目的外利用の禁止及び秘密保持に係る誓約を取り交すこと。

解説、適合例

外部委託に伴い、委託先は、電子証明書や失効情報等を取り扱う可能性がある。これらの情報は委託された業務の範囲内でのみ利用されるべきものであるため、秘密保持契約等による保護が必要となる。

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及びデジタル庁に提出する。
書類の様式については任意とする。

■提出書類の例
・業務実施体制図（どの業務をどこに委託するか）
・秘密保持契約書（どのような内容で誓約を取り交す予定か）

＜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 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、総務省及びデジタル庁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及びデジタル庁へ報告する。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及びデジタル庁に提出する。
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、デジタル庁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 4-18 【評価項目】役員等の要件＞

【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及びデジタル庁に提示する。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

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、主務大臣による認定を受けるための手続に該当する。

＜図 4-19 公的個人認証サービス利用開始までの流れ＞

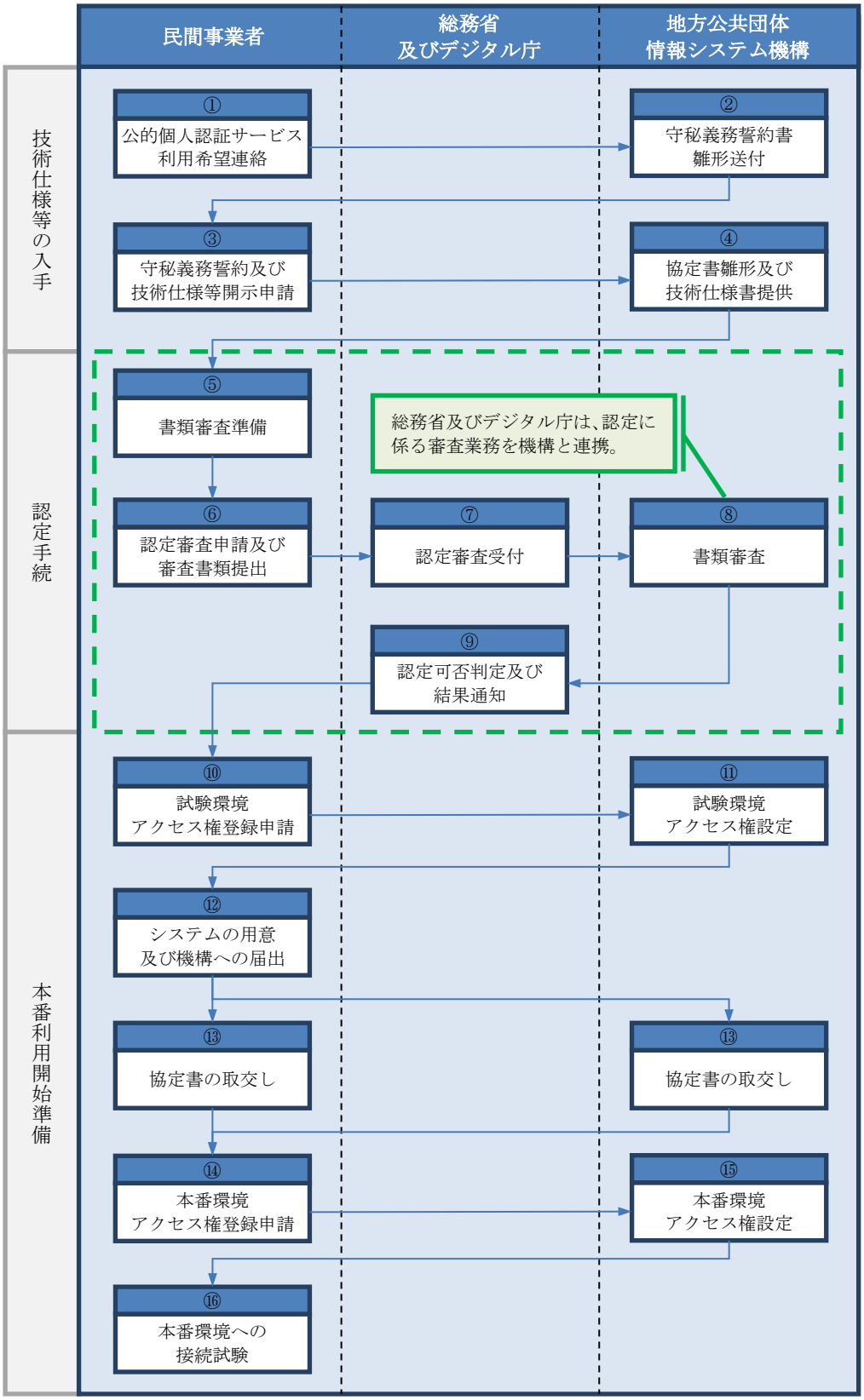


図 4-19 における①～⑯の詳細は、次のとおりである。

【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、総務省及びデジタル庁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 総務省及びデジタル庁は、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、確認結果を総務省及びデジタル庁へ報告する。書類審査後、総務省、デジタル庁及び機構において、現地調査を実施する。
⑨ 総務省及びデジタル庁は、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 審査に合格して主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（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」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。

主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。

■認定に要する時間

民間事業者が公的個人認証サービス利用の申請を行ってから、主務大臣による認定に可否判定及び結果通知が行われるまでに要する時間は、当該事業者が審査事項をどの程度満たしているかにも拠るため一概にはいえないが、目安としては、新規事業者の場合おおよそ５～10ヶ月程度、更新の場合３ヶ月程度である。

■認定の有効期間

主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において１年間と規定している。

認定の更新のおいては、更新時点で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、総務省及びデジタル庁から求めがあった場合、更新を希望する民間事業者は、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必要がある。

■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及びデジタル庁に遅滞なく連絡する必要がある。総務省及びデジタル庁は、変更内容を確認し、必要に応じて再審査等を行う。

なお、これまでマイナンバーカード用の電子証明書のみを扱ってきた署名検証者が、新たにスマートフォン用の電子証明書を扱う場合、例えば電子証明書を読み取る際の動線等の変更により、電子署名等の確認の用に供する設備の概要又は確認の実施の方法に変更が生じる場合には、変更の認定が必要となるため、留意されたい。

■失効情報の提供の求めの終了

署名検証者は、いつでも失効情報の提供の求めを終了することができる。この場合、機構に対し、必要な事項を届け出なければならない。また、当該届出を行った場合、受領した失効情報等は消去しなければならず、併せて総務省及びデジタル庁に対して電子証明書の発行番号の削除報告書の提出も必要となる。取得した認定の効力については、認定の更新手続をしないことで失われる。

なお、失効情報の提供の求めを終了するに当たっては、以下についても留意されたい。

・事前に総務省及びデジタル庁に連絡すること。
・失効情報の提供の求めを終了する理由や意見等求める場合があること。

(3) 失効情報提供手数料

本項では、機構が徴収する失効情報手数料について記述する。

ア 基本的な考え方

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が利用できるよう、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（署名検証者））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。

イ 情報提供手数料

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。

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(*3)、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(*4)。

【手数料】

◆ 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。

（*３） 「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。

（*４） 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である。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、利用の一層の拡大に向けて取り組む。

◆手数料の観点から見た民間事業者にとってのメリット分析

◇ 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・住所等の基本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 11 億円（令和２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 84 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 63 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 63 円等）がなくなる。）。

※2023 年１月より、手数料の取扱いは以下の運用となっている。

失効情報提供方法(*5)	手数料	期間
CRL 方式	無料	恒久
OCSP 方式	無料	2025 年 12 月 31 日まで

（*５） 失効情報提供方法の各方式については、後述【APPENDIX①】署名検証機能の技術解説 ア c を参照。

５　本人同意に基づく最新の利用者情報（基本４情報）提供サービスの概要

本章では、公的個人認証サービスにおける本人同意に基づく最新の利用者情報（基本４情報）提供サービス（以下「最新の基本４情報提供」という。）の概要として、次の６点について記述する。

（1）本人同意に基づく最新の基本４情報提供とは
（2）本人同意に基づく最新の基本４情報提供の仕組み
（3）本人同意の取得
（4）本人同意の取消し
（5）利用者クライアントソフトを用いた本人同意の状況照会・取消し
（6）本人同意に基づく「最新の基本４情報提供サービス」における留意事項

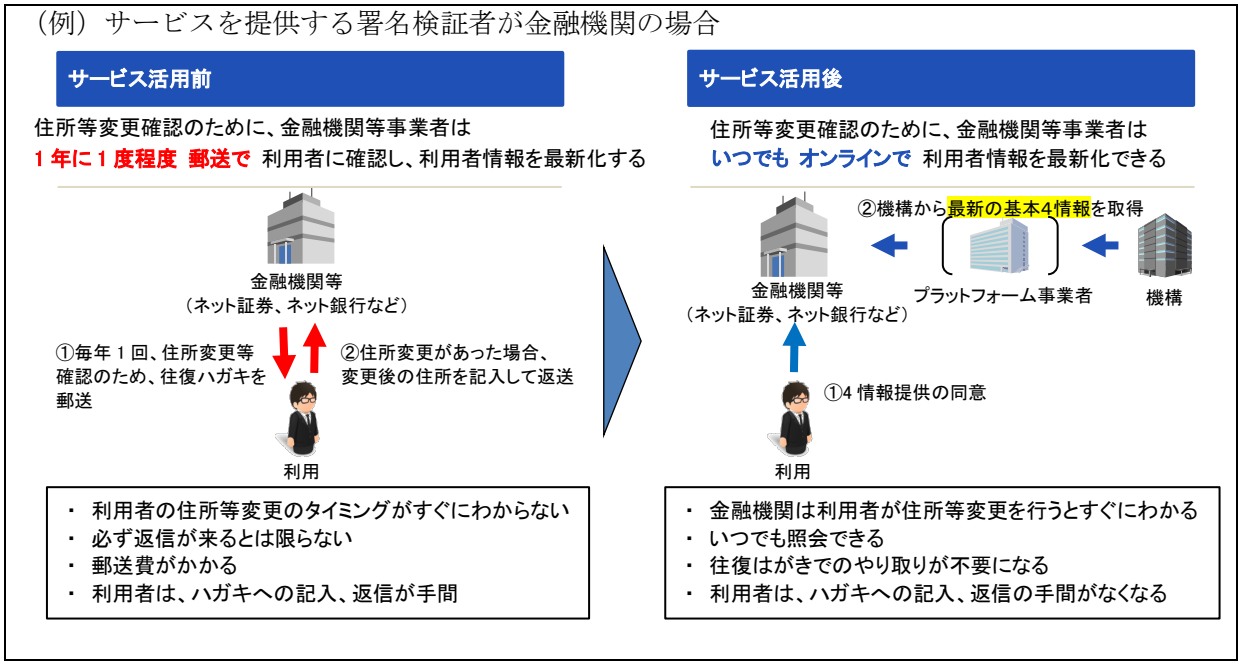
(1)本人同意に基づく最新の基本４情報提供とは

署名用電子証明書を利用する署名検証者(*1)は、公的個人認証サービスを利用して署名用電子証明書の有効性を機構に確認するだけでなく、住所や氏名の変更等により署名用電子証明書が再発行された利用者について、本人の同意に基づき、再発行された署名用電子証明書に記録された最新の基本４情報（住所、氏名、生年月日、性別の４情報。）を機構より提供を受けることができる（情報提供に伴う手数料は後述（２）(*２)参照。）。具体的には、プラットフォーム事業者が機構より直接最新の基本４情報を受け、サービスプロバイダ事業者はプラットフォーム事業者を経由して間接的に提供を受けることとなる。

これにより、署名検証者とサービスプロバイダ事業者においては、利用者の最新の基本４情報を把握できるため、郵送物等の不着削減が可能となるほか、利用者においても署名検証者もしくはサービスプロバイダ事業者に対し住所変更手続等を不要とすることができる。なお、取得した４情報は、機構と署名検証者ならびにサービスプロバイダ事業者にて保管・管理されるが、プラットフォーム事業者においては保管・管理せず、サービスプロバイダ事業者へ提供後、廃棄する。本人同意に基づく最新の基本４情報提供の仕組みについては、本章の「(2) 本人同意に基づく最新の基本４情報提供の仕組み」にて記述する。

（*１）　本章では、「プラットフォーム事業者」及び「サービスプロバイダ事業者」の位置付けを前提に記述している。みなし署名検証者を傘下に持たない「署名検証者」の場合は「プラットフォーム事業者」及び「サービスプロバイダ事業者」の役割を兼ねているとみなし、以降の記述について参照されたい。

＜図 5-1 本人同意に基づく最新の基本４情報提供の概要＞



(2)本人同意に基づく最新の基本４情報提供の仕組み

本人同意に基づく最新の基本４情報提供サービスは、図 5-2 の仕組みで利用される。

＜図 5-2 本人同意に基づく最新の基本４情報提供の仕組＞

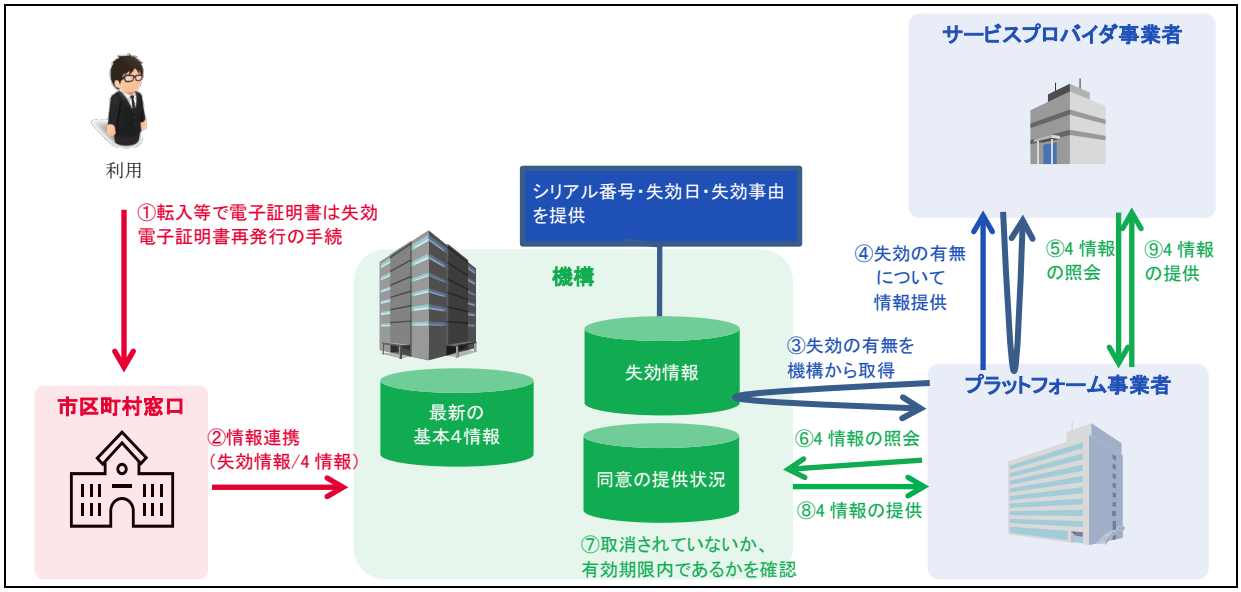


図 5-2 で示したとおり、本人同意に基づく最新の基本４情報提供は以下の流れで行う。

① 利用者は、引越しや改姓等により市区町村窓口においてマイナンバーカードの更新手続を行う。更新前の署名用電子証明書は失効し、引越しや改姓後の基本４情報が記録された署名用電子証明書が再発行される。

② プラットフォーム事業者は、サービスプロバイダ事業者の求めに応じて、事前に利用者から取得していた更新前の署名用電子証明書の失効情報を機構から取得する。

③ プラットフォーム事業者は、サービスプロバイダ事業者と取り決めた任意の期間ごとに、機構から取得した署名用電子証明書の有効性について情報提供する。

④ サービスプロバイダ事業者は、更新前の署名用電子証明書が失効していることを確認した場合、プラットフォーム事業者に対し、更新後の署名用電子証明書の最新の基本４情報の提供を求める。

⑤ プラットフォーム事業者は、機構に対し最新の基本４情報の提供を求める（*2）。

⑥ 機構は、予め利用者から取得している同意が有効期限内にあるか、同意の取消しがされていないか、同意の対象項目が何かを確認する。

⑦ 機構は、⑥の状況を確認したうえで、プラットフォーム事業者に対し、同意している対象項目について最新の基本４情報の提供を行う。

⑧ プラットフォーム事業者は、サービスプロバイダ事業者に対し最新の基本４情報の提供を行う。サービスプロバイダ事業者は、最新の基本４情報を取得することが可能となる。

（*2）プラットフォーム事業者が J-LIS より最新の基本４情報を取得する際の手数料は、1 件あたり 20 円となる。ただし、最新情報がない場合は手数料は発生しない。

(3)本人同意の取得

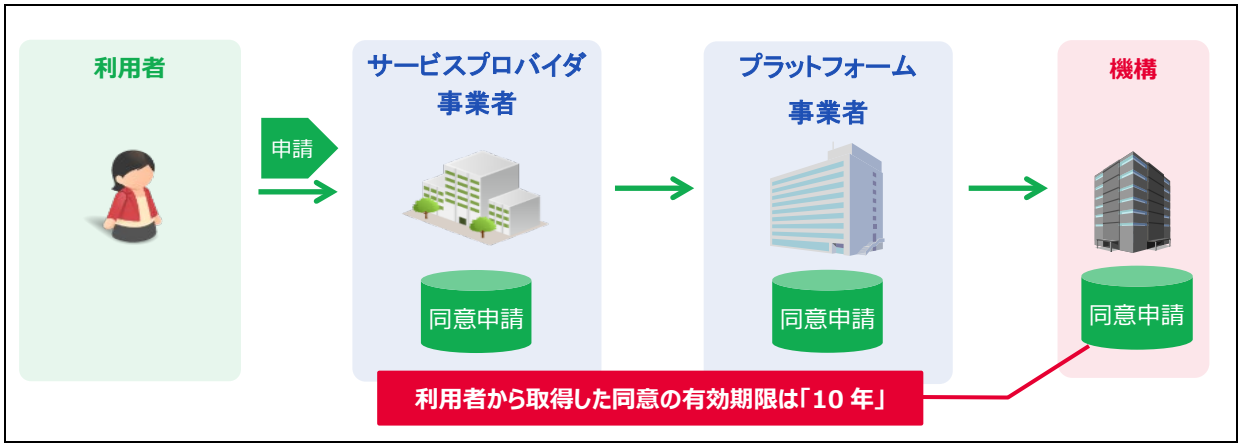
図 5-2 の流れで利用される最新の基本４情報提供においては、事前に利用者本人から同意を取得することが前提となる。同意の対象となる項目は、住所・氏名・生年月日・性別の基本４情報である。なお、最新の基本４情報を提供する上では、機構から最新の発行番号（シリアル番号）がプラットフォーム事業者に提供されるが、発行番号（シリアル番号）はサービスプロバイダ事業者へ提供する内容には含まれず、同意の対象とはならない。

利用者本人は、機構がプラットフォーム事業者を経由しサービスプロバイダ事業者へ最新の基

本４情報を提供することについて、基本４情報の各項目に対し同意するか否かの選択をすることができる。また、機構は利用者が同意した項目に限り、最新の基本４情報を提供することとなる。

本人同意の取得については以下の流れで行う。
※サービスプロバイダ事業者が行ってはならない業務については、前述の「４(2)ア(ｴ)サービスプロバイダ事業者が行ってはならない業務」を参照のこと。

＜図 5-3 最新の基本４情報提供の同意申請＞



① 同意を取得する主体・情報管理

利用者からの「同意」は、原則として、実務上利用者と接点を持つサービスプロバイダ事業者が受け付ける。取得した同意情報は、サービスプロバイダ事業者からプラットフォーム事業者を経由し機構に送信する。各事業者及び機構は、それぞれ同意情報に関するデータベース等を構築し、保存・管理をする。

② 同意の取得方法

同意は、電子的に取得することとし、紙での取得は認めない。
また、同意は、本人の意思に基づくものであることを確実に示すため、マイナンバーカード用の署名用電子証明書を用いる（スマートフォン用の署名用電子証明書も可）。
署名用電子証明書を用いた同意は、サービスプロバイダ事業者とプラットフォーム事業者を経由したうえで、機構に提供される。なお、同意の取得単位は、サービスプロバイダ事業者のサービスごととする。

③ 同意の取得タイミング

利用者から同意を取得するタイミングは、サービスプロバイダ事業者の任意のサービス提供時とする。具体的には、署名用電子証明書を活用したサービスの申し込み時や、サービスプロバイダ事業者が提供するマイページ等を通じて利用者向けの案内をする時等、オンライン上の手続時が考えられる。同意の取得期限については、機構に対し最新の基本４情報の提供を求める前までとする。

④ 同意の一括取得

サービスごとに署名用電子証明書を付与する利用者の負担を軽減するため、ホールディングスカンパニー傘下の企業群が提供するサービス等について、同意を一括取得したい場合は、その旨を利用者に提示した上で、各サービスに対する利用者の同意を明示的に取得することを前提として、一括での同意を認める。

⑤ 同意の有効期間

利用者から取得した同意の有効期間は、サービスプロバイダ事業者が利用者から同意を受

付した翌日を起算日として 10 年となる。なお、有効期間内に署名用電子証明書が何度失効した場合であっても、有効期間中の同意については引き続き有効となる。

また、10 年の有効期間が経過した、もしくは経過する前に、署名検証者から利用者に対し、同意の更新を促す必要がある。

【例】

サービスプロバイダ事業者が利用者から同意を受付した日時:2023 年 5 月 18 日　10:00:00
同意の有効期間開始日時：2023 年 5 月 19 日　00:00:00
同意の有効期間終了日時：2033 年 5 月 18 日　23:59:59

⑥ 同意の状況照会

利用者は、自身が同意をした内容「同意をした事業者・サービス・同意の対象となる項目・同意の有効期限等」について照会をすることができる。実務上は、サービスプロバイダ事業者が、事業者窓口や事業者が提供するマイページ等を通じて、利用者からの照会を受け付けることを原則とする。

利用者が至急で同意の状況照会する必要がある場合は、機構が提供するアプリ「利用者クライアントソフト」においても照会をすることができる。利用者クライアントソフトを用いた同意の状況照会については、後述の「(5)利用者クライアントソフトを用いた本人同意の状況照会・取消し」を参照のこと。

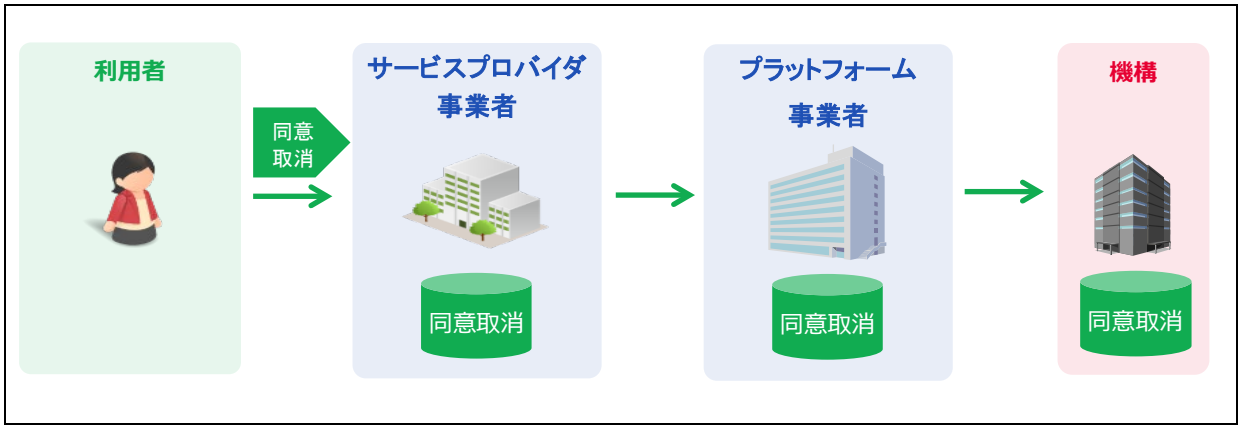
⑦ 同意する項目の選択

利用者が、同意の対象である 4 項目「住所・氏名・生年月日・性別」のうち、一部の項目しか同意しない場合は、サービス提供事業者の判断により、「最新の基本 4 情報の提供をするサービス」自体を不可とすることを認める。なお、本サービスについて利用者が同意しない場合、事業者が提供するサービスが受けられない等、利用者が不利益を被ることのないようにされたい。

(4)本人同意の取消し

利用者が一旦同意をした後、利用者本人の意向変更等により、同意を取り消すことを可能とする。利用者による同意の取消し申請後、機構にて申請を受信次第、即時に、機構からサービスプロバイダ事業者への最新の基本 4 情報提供を停止することができる。本人同意の取消しは以下の流れで行う。

＜図 5-4 本人同意の取消し＞



① 同意の取消しを受け付ける主体

利用者からの「同意の取消し」は、原則として、実務上利用者と接点を持つサービスプロバイダ事業者が受け付ける。ただし、同意を取り消したい時機が以下のような場合には、機構が提供するアプリ「利用者クライアントソフト」においても受け付けることとする。

・署名検証者やサービスプロバイダ事業者の営業時間外の場合
・複数事業者のサービスを一括して同意を取り消したい場合
・緊急で同意を取消したい場合　等

利用者クライアントソフトを用いた同意の取消しについては、後述の「(5)利用者クライアントソフトを用いた本人同意の状況照会・取消」を参照のこと。

② 同意の取消し方法

同意の取消しは、本人の意思に基づくものであることを確実に示すため、同意の申請時と同様、署名用電子証明書を用いる。

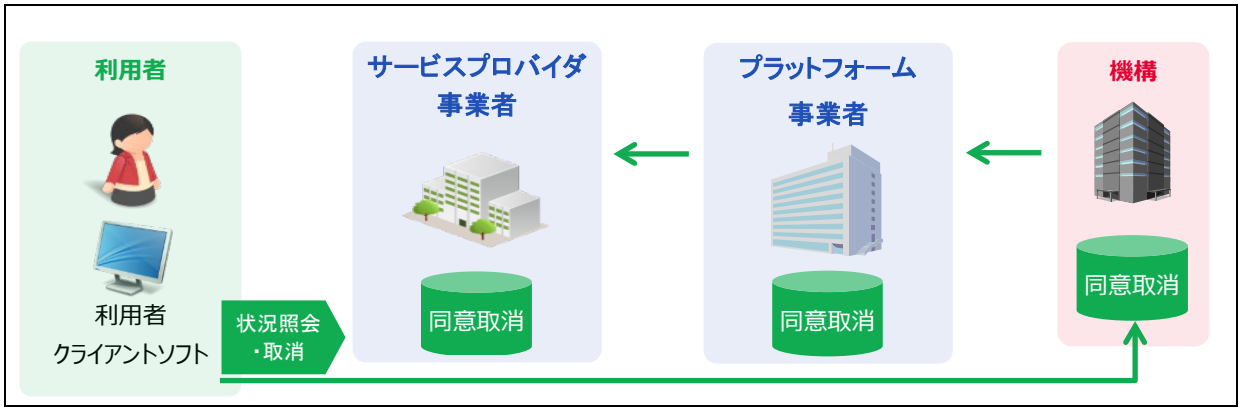
(5)利用者クライアントソフトを用いた本人同意の状況照会・取消し

本人の同意については、原則として、同意を取得した署名検証者において管理されるべきであるが、以下のような場合に備えて、利用者が機構に対し、直接同意の状況照会や同意の取消し申請を行う方法がある。

・最新の基本４情報提供に係る同意について、利用者が同意の照会や取消しをしたい時機が、署名検証者やサービスプロバイダ事業者の営業時間外の場合
・複数事業者のサービスを一括して同意を取消ししたい場合
・緊急的な同意の取消しをしたい場合　等

上記のような場合には、機構が提供するアプリ「利用者クライアントソフト（Windows 版・Android 版・Mac 版・iOS 版）」を用いることで、同意の状況照会や取消しを行うことができる。

＜図 5-5 利用者クライアントソフトを用いた本人同意の状況照会・取消＞



① 利用者クライアントソフトを用いた同意の状況照会

同意の状況照会については本人であることを確認するため利用者証明用電子証明書を用いる。

② 利用者クライアントソフトを用いた同意の取消し

同意の取消しは、本人の意思に基づくものであることを確実に示すため、署名用電子証明書を用いる。

③ 利用者クライアントソフトを用いた同意取消しの情報連携

利用者が利用者クライアントソフトを用いた同意の取消しを行うと、機構に対し同意取消しの情報が連携される。利用者が同意を取消しした事実は、機構から自動的に通知されるわけではないため、署名検証者も速やかに把握できるよう、プラットフォーム事業者は機構に

対し、サービスプロバイダ事業者ごとに割り振られた ID を用いて、利用者の同意取消しの情報を取得することができる。
また、サービスプロバイダ事業者は、プラットフォーム事業者を経由して、同意取消しの状況を照会し、結果を把握する。

④ 利用者クライアントソフトを用いた同意取消し後の再同意

上記②で利用者クライアントソフトを用いた同意の取消しを行った後、再度、同意をする場合には、利用者はサービスプロバイダ事業者に確認のうえ手続を行う。
（利用者クライアントソフトでの再同意はできない。）

（6）本人同意に基づく「最新の基本４情報提供サービス」における留意事項

ア　同意

①（事業者が提供するサイト上での手続について）

サービスプロバイダ事業者は、利用者からの同意の申請、同意の状況照会、同意の取消しを事業者の事業所窓口において対面で受け付ける場合、利用者の端末等を用いながら実施することに加え、事業者が提供するマイページ等の画面開発を行う等により、非対面でのオンライン上の手続においても対応可能となるよう備える。

②（開示請求）

サービスプロバイダ事業者は、利用者からの求めにより、最新の基本４情報を取得した日時、取得した情報等の開示請求があれば回答できるように備えること。開示請求がある場合は、請求者が本人であることを確認のうえ、各事業者所定の書式に記入いただいた上で回答する。

開示請求に係る手続については、各事業者が設置する問い合わせ窓口をプライバシーポリシー等で案内するほか、利用規約等で明らかにした上で同意を取得することが望ましい。

③（最新の基本４情報提供における任意性の確保及び利用者が同意しなかった場合の取引）

最新の基本４情報提供のサービスについて、利用者が同意をするか否かは、利用者の任意となる。ただし、取得する最新の基本４情報の全部又はその一部が、サービスプロバイダ事業者のサービス提供において必要な情報であって、利用者が当該情報の提供に同意しない場合等は、事業者の判断により最新の基本４情報のサービス提供自体を取りやめることも可能である。ただし、最新の基本４情報のサービス提供に関して同意をしない場合は、サービスプロバイダ事業者が提供するサービスの提供が受けられない等の不利益が生じることのないようにする。

④（利用者に対する同意状況の情報提供について）

サービスプロバイダ事業者は利用者から同意を取得し、一定の時間が経過した後、利用者に対し同意項目の再確認や変更有無の確認を促すことを目的に、少なくとも１年に１回程度、利用者にリマインドメールを発信する等、同意状況の情報提供を実施する。

イ　最新の基本４情報

①（事業者が提供するサービス停止による最新の基本４情報提供の停止）

サービスプロバイダ事業者が提供するサービスを停止する場合は、プラットフォーム事業者を経由して、機構に対し、事前にサービス停止日の情報を連携する。この手続に基づき、サービス停止日の同意をもって、機構からプラットフォーム事業者及びサービスプロバイダ事業者への最新の基本４情報提供を停止する。

ただし、この場合、署名用電子証明書に基づく利用者からの申請が行われないため、機構ではシステム上同意の取消しを反映させることができない。このため、利用者が利用者クライアントソフトを用いて状況照会を行った場合、サービスが停止されているにもかかわらず「基本４情報提供の同意」は有効期間中である限り有効の状態となっている。これをシステム上も停止させたい場合には、利用者から電子証明書を用いた同意取消しを行う必要がある。署名検証者は、利用者に対しこの点についてもあらかじめ案内しておくことを推奨する。

②（利用者の同意取消しの申請及び事業者が提供するサービス停止による最新の基本４情報提供データの取扱い）

利用者の同意取消しの申請、及びサービスプロバイダ事業者が提供するサービスの停止により、機構から最新の基本４情報提供が停止した場合には、不要となった（機構より取得した）すべてのお客様の最新の基本４情報を事業者にて廃棄する。

③（署名検証者が認定を取り消された場合における基本４情報提供データの取扱い）

署名検証者が、主務大臣認定を取り消された場合や署名検証業務を終了する場合等には、機構より取得したシリアル番号を事業者にて廃棄する。

６　公的個人認証サービス利用に当たっての留意事項

本章では、署名検証者が公的個人認証サービスを実際に利用するために当たって、留意すべき事項について解説する。なお、本章に記載される事項は、新規に認定を取得する事業者にかかわらず、既存の署名検証者についても留意すべき事項として記載する。

(1) 電子署名の対象について

署名検証者が署名用電子証明書及び電子署名を活用して、電子申請を受け付ける場合、署名用電子証明書に係る電子署名を行う対象や、何のために署名用電子証明書に係る暗証番号（６桁～16 桁の英数字）を入力しているのかが利用者にとって明らかではない事例が見受けられる。

このため、署名検証者（サービスプロバイダ事業者を含む）は利用者に対して、以下の対応を行う必要がある。

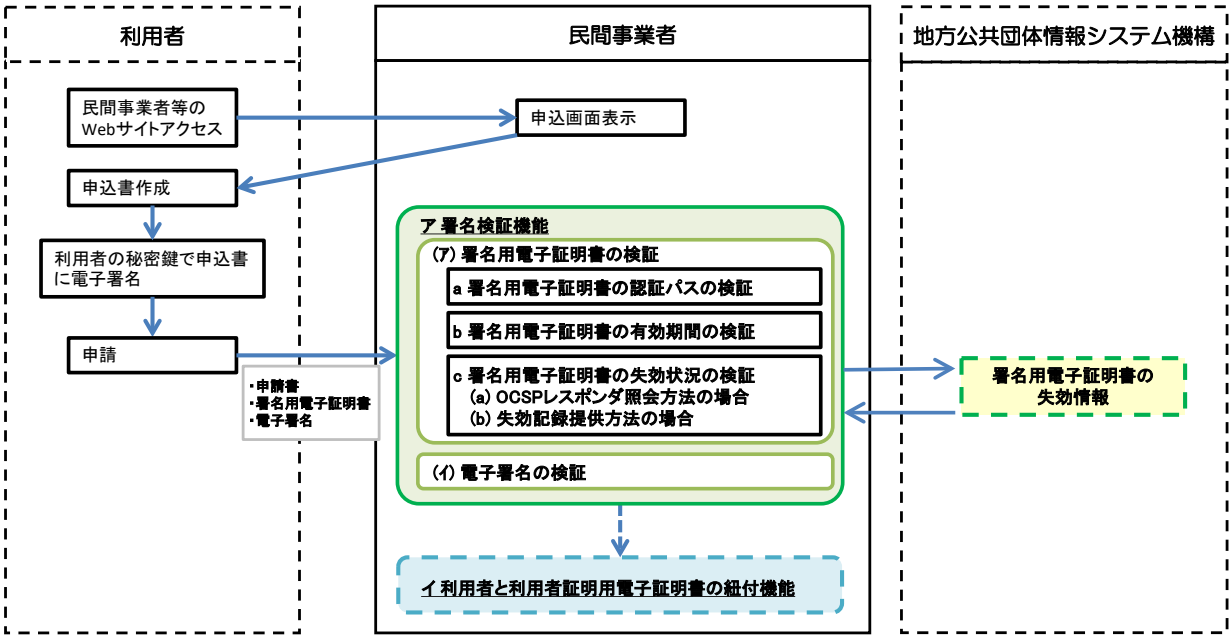
・利用者が、署名用電子証明書に係る暗証番号の入力による電子署名を行う前に、どのような情報に対して当該電子署名を行うのかを明らかにする。
・暗証番号の入力により電子署名が行われること自体やその意義について明らかにする。

なお、プラットフォーム事業者は、サービスプロバイダ事業者において上記の措置がとられていることを確認、担保させ、適切な措置がとられていない場合は、指導等を行うこと。

【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＞

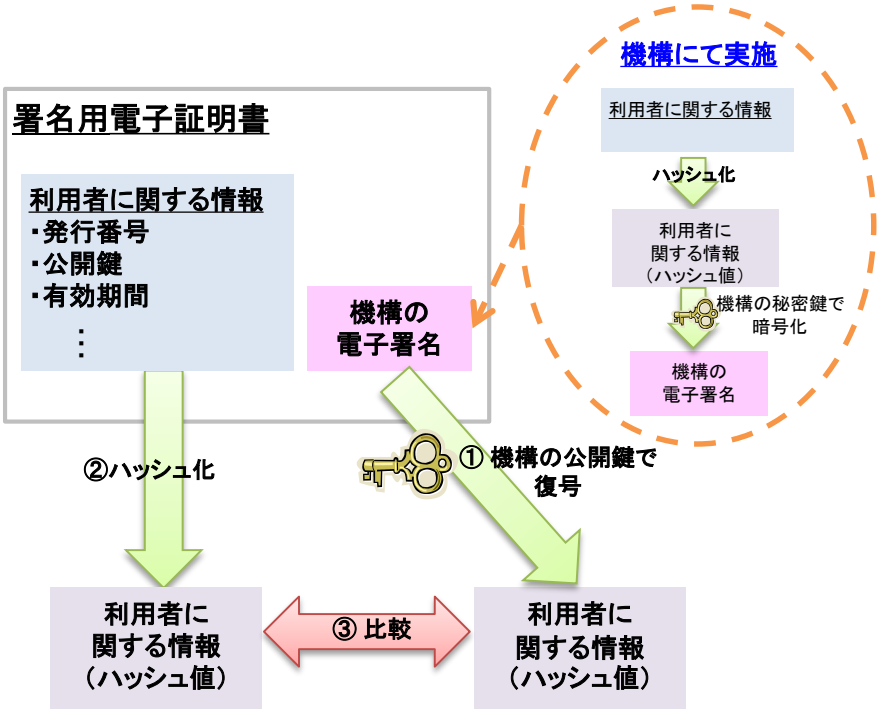


図 APPENDIX①-2 で示したとおり、署名用電子証明書の認証パスの検証は以下の流れで行う。

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。

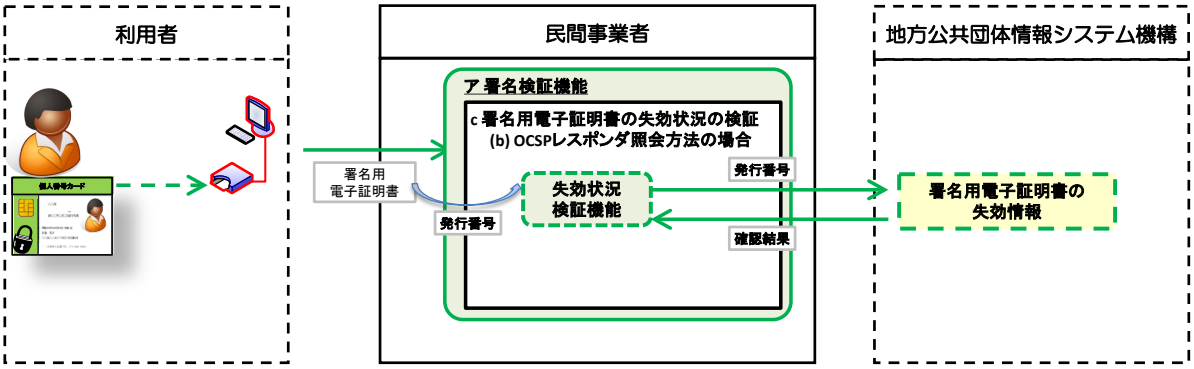
(a) OCSP レスポンダ照会方法の場合

「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の番号 (*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＞



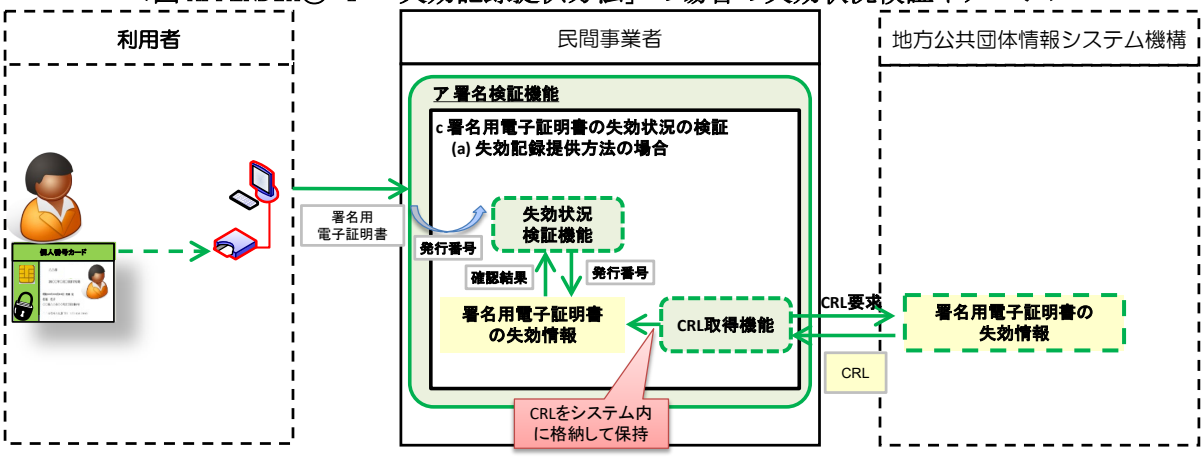
機構から送信されてくる確認結果の情報には、それ自体がなりすましや改ざんされたものでないことを保証するために、機構の秘密鍵による電子署名が付与されている。そのため、民間事業者は、機構の自己署名証明書に格納されている公開鍵を使って電子署名の検証を行い、なりすましや改ざんされたものでないこと確認した上で、機構から送信されてくる確認結果を使用する必要がある。電子署名の検証方法については、後述の「(イ) 電子署名の検証」を参照（*4）のこと。

（*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＞

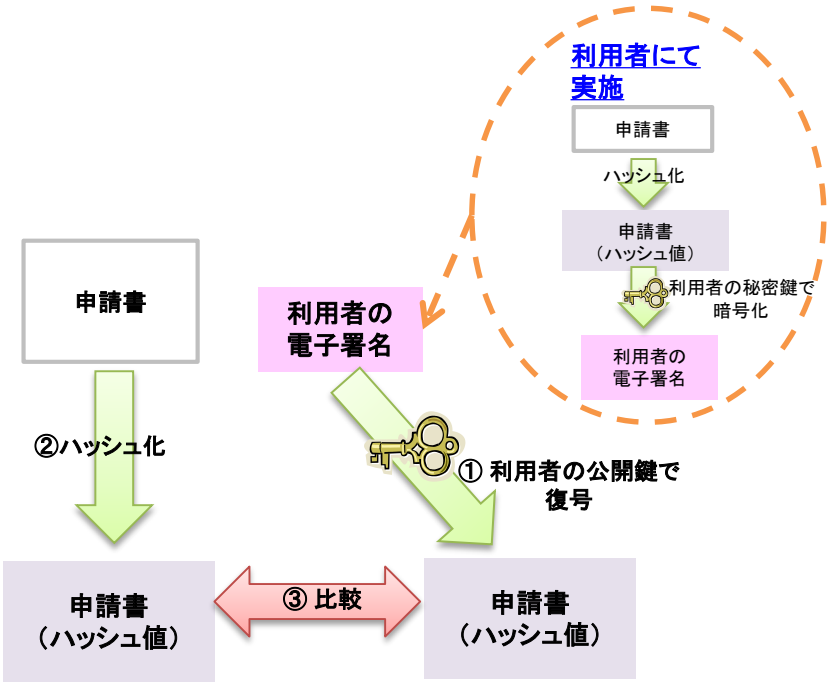


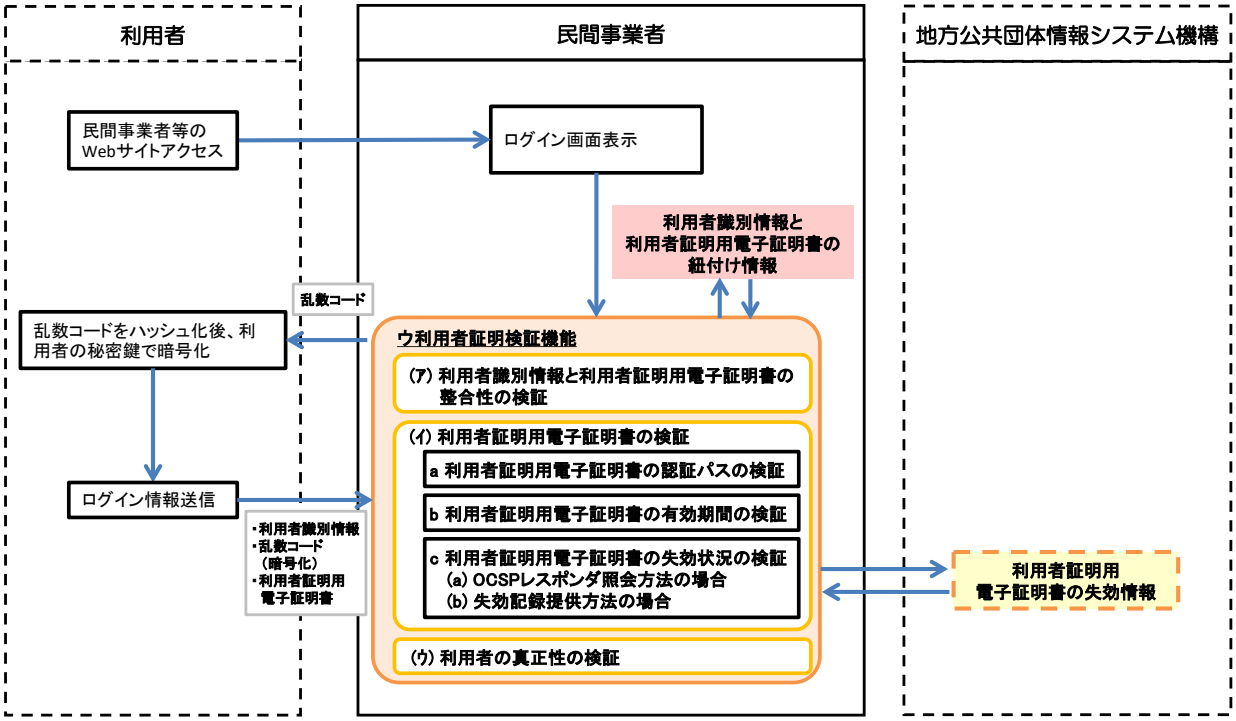
図 APPENDIX①-5 で示したとおり、電子署名の検証は以下の流れで行う。

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の番号を基に、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、電子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、利用者証明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＞

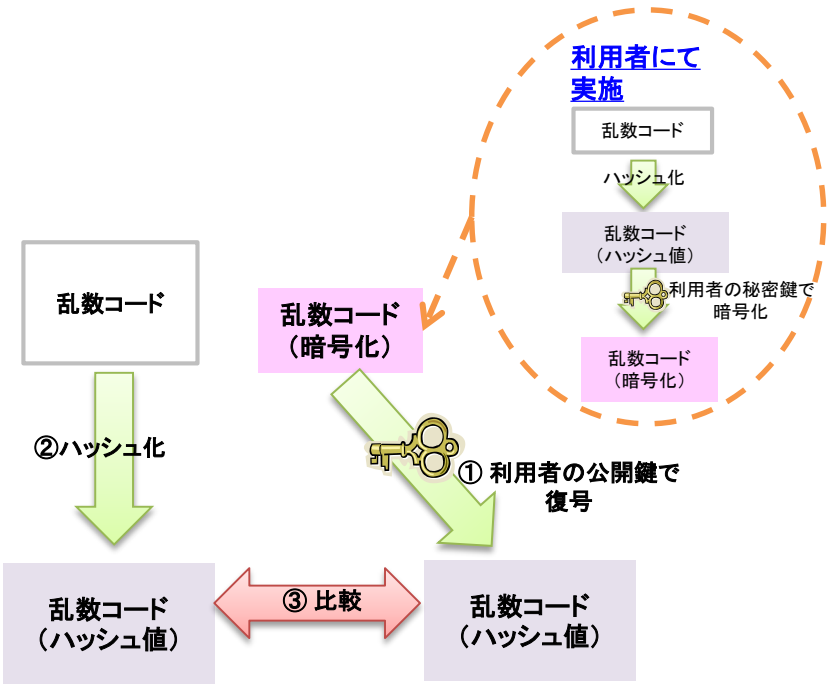


図 APPENDIX②-2 で示したとおり、民間事業者において、乱数コードの検証は以下の流れで行う。

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
マイナンバーカード発行	1	マイナンバーカードは、国民全員に配布されるのでしょうか。それとも、マイナンバー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マイナンバーカードの受け取り方法について教えてください。
	3	マイナンバーカードの発行には、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限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、マイナンバー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、不正に入手されたマイナンバー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	マイナンバーカードの紛失・盗難時を想定したセキュリティ対策を教えてください。
公的個人認証サービスの利用方法	9	利用者の最新住所を確認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	10	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　マイナンバーカードは、国民全員に配布されるのでしょうか。それとも、マイナンバー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。
市区町村から送付された交付申請書の二次元バーコードからの申込みや、市区町村の窓口でにおいて申し込むことができます。

Q.2　電子証明書が格納されるマイナンバー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、市区町村窓口で本人確認を行ったうえで、マイナンバーカードが交付されます。

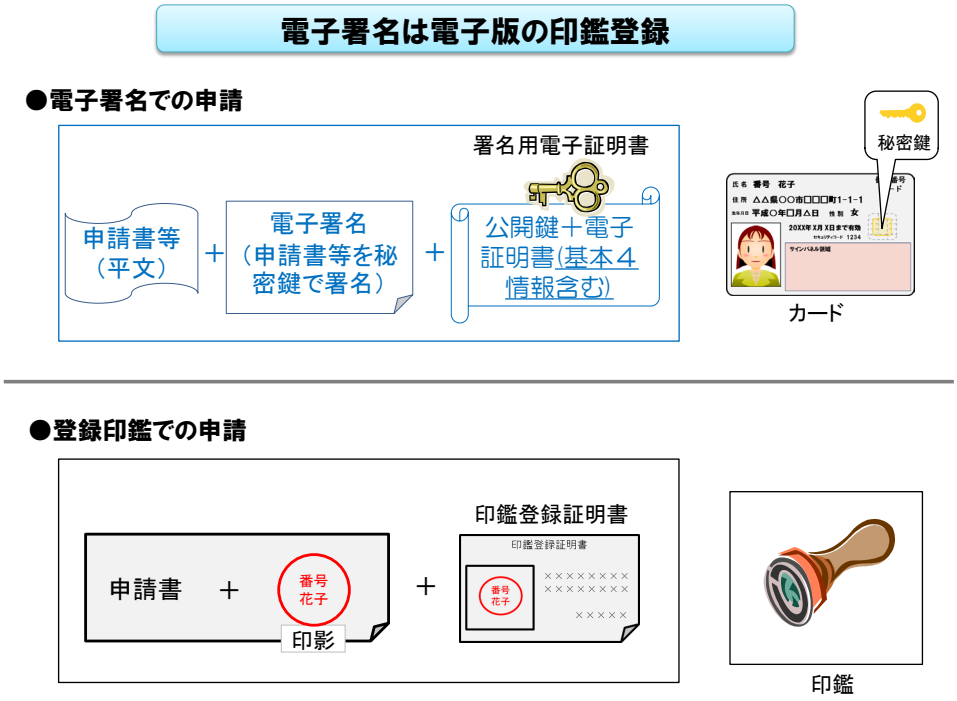
Q.3　マイナンバーカードの発行には、手数料が発生するのでしょうか。

A.3　無料です。ただし、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限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、マイナンバー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　市区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、不正に入手されたマイナンバー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　マイナンバーカードの紛失・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　マイナンバー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、機構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、「暗証番号による保護(*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、本人による市区町村窓口での手続が必要となります。

（*1）暗証番号による保護
公的個人認証サービスの電子証明書等は、マイナンバーカード又はスマートフォンの 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した暗証番号の入力が必要になります。

Q.9　利用者の最新の住所を確認することは可能でしょうか。

A.9　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。
また、「第５章 本人同意に基づく最新の利用者情報（基本４情報）提供サービスの概要」のとおり、本人同意を前提として、最新の住所を機構から取得することが可能です。

Q.10　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.10　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
・ スマートフォンや PC 等のインターネット接続環境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