# 公的個人認証サービスにおける署名検証者の範囲の在り方に関する研究会

# 報告書

平成１６年１２月

＜目次＞

## １　公的個人認証サービスの現状

### （１）制度創設の背景

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、成りすまし、改ざん、送信否認などの課題が指摘されている[1]。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」に基づく公的個人認証サービス制度を創設することとされ、サービスの提供が平成１６年１月２９日から開始されたところである。

### （２）公的個人認証サービスの全体像[2]

公的個人認証サービスでは、電子証明書の発行や失効情報の管理など認証局としての役割を都道府県知事が、電子証明書の発行時などにおける本人確認機関としての役割を市町村長が、それぞれ担うこととされている。ただし、各都道府県知事がそれぞれ認証局としての業務を行うのは必ずしも効率的でないことから、電子計算機処理等の事務を総務大臣が指定する指定認証機関に委任することができることとされており、現在、唯一この指定を受けている財団法人自治体衛星通信機構に全都道府県知事が事務を委任しているところである。

公的個人認証サービスを利用して電子申請等を行おうとする住民はこれに先立ち、まず電子証明書の発行を受ける必要がある。電子証明書の発行は住民が住民基本台帳に記録されている市町村の窓口で行われる。担当者が住民の実在性・本人性を確認した後、窓口に設置された鍵ペア生成装置を用いて住民自身が公開鍵・秘密鍵の鍵ペアを生成する。基本４情報（氏名、生年月日、男女の別及び住所）と公開鍵を含む電子証明書及び秘密鍵は一定の基準を満たしたＩＣカードに格納される。なお、現在該当するＩＣカードは住民基本台帳カードのみである[3]。

電子証明書の発行を受けた住民は、これを用いて行政機関等に対し、インターネット経由で電子申請等を行うことが可能となる。公的個人認証サービスで

---

[1] 資料３－１（デジタル社会における課題）参照。
[2] 資料３－２（公的個人認証サービス）参照。

は、他の認証局全般と同様に公開鍵暗号方式を採用している。発信者である住民の側では、平文と呼ばれる申請書等をハッシュ関数により圧縮した後、自身の秘密鍵により暗号化し電子署名を得る。住民から平文、電子署名及び電子証明書の送信を受けた受信者（行政機関等）の側では、平文を発信者と同様にハッシュ関数により圧縮するとともに、電子署名を発信者の公開鍵により復号し、得られた両者の結果を照合することにより、本人性及び文書内容の真正性を確認することが可能となる（＝電子署名の検証）。[4]

申請書等（平文）、電子署名及び電子証明書による電子申請等を受信した行政機関等は、電子証明書の有効性確認及び電子署名の検証を行うことが義務づけられており、電子証明書の有効性確認に関し、具体的には都道府県知事（指定認証機関）が備える失効リストへの問い合わせを行うこととなる。この失効リストの作成に当たっては、住民基本台帳ネットワークシステムと連携し、住所・氏名の変更や死亡等の異動等が発生した場合、民間の認証局に比べて的確に失効情報を作成して署名検証者に提供し、その有効性確認に対応することが可能となっている[5]。

（３）公的個人認証サービスの利用状況

電子証明書の発行を受けた利用者が実際に公的個人認証サービスによる電子署名を行って電子申請等を行えるようになるためには、行政機関等がそれぞれの受付システムを整備した上で公的個人認証サービスに対応する必要がある。平成１６年１１月末現在で、公的個人認証サービスの対象手続となっているのは、国では５省庁、地方公共団体では１７県及び一部市町村の手続である[6]。これまでのところ、利用の多く見込まれる手続が必ずしも対象となるに至っていないが、今後、国の機関の他手続・各地方公共団体の手続等が順次追加される見込みであり、これに伴ってサービスの利用も増えていくものと考えられる。

---

[3] 資料３－３（電子証明書の発行等の手続イメージ）参照。
[4] 資料３－４（電子署名（デジタル署名）の概要）参照。
[5] 資料３－５（公的個人認証サービスと住民基本台帳ネットワークシステムの関係）参照。
[6] 資料３－６（公的個人認証サービスの対象手続）参照。

## ２　代理申請等における現制度の課題

### （１）署名検証者の限定

公的個人認証サービスが行政手続等のオンライン化における確かな本人確認手段の提供を主な目的とした制度であること、また、既に民間の認証局がサービスを提供しており[7]、官民の適切な棲み分けを確保する必要があることなどから、現在の公的個人認証サービスにおいては法律の規定により、住民の電子証明書に関する失効情報等の提供を受け、その有効性確認を行える署名検証者の範囲が行政機関等、裁判所及び一定の条件を満たした民間認証事業者に限定されている[8]（裁判所については法施行当時、署名検証者の範囲に含まれていなかったが、第１６１回国会において「民事関係手続の改善のための民事訴訟法等の一部を改正する法律」が成立し、追加する旨の改正が行われたところである）。

行政機関等については、行政手続等における情報通信の技術の利用に関する法律第２条第２号に規定する行政機関等の定義が引用されており、国の各府省や地方公共団体のほか、独立行政法人、地方独立行政法人、いわゆる特殊法人等のうち政令で定めるもの、指定法人などが対象となっている。なお、全国社会保険労務士会連合会、日本行政書士会連合会、日本司法書士会連合会、日本税理士会連合会、日本土地家屋調査士会連合会などのいわゆる士業連合会は、行政手続等における情報通信の技術の利用に関する法律施行令第１条の規定により、署名検証者の範囲に含まれている。

### （２）代理申請等における課題

代理申請等の場合、申請等の代理を業とすることができる、いわゆる士業個人等は現制度上、署名検証者の範囲に含まれていないため顧客の電子証明書に関する失効情報等の提供を受けられない。したがって、仮に顧客の電子証明書が失効していた場合、いったん行政機関等に提出した申請書等一式が有効と扱われず手続をやり直すことになる。これは士業個人等にとって顧客等との関係で大きなリスクであり、結果として士業個人等が代理申請等の方法としてオンラインを選択することが困難であるとの問題が指摘されている。

特に、不動産取引に伴う登記申請など関係者が多数に及ぶ場合や資金決済が連動する場合には、複数当事者間ですべての手続が適正に完了することを前提として申請等が行われるものである。仮に一つの電子証明書が失効していたと

---

[7] 資料４－１（電子認証サービスの提供主体など）参照。
[8] 資料４－２（署名検証者の範囲）参照。

すると、当該申請等のみならず、関連する全ての手続に波及するおそれがあり、そのリスクは甚大である。

　オンラインとオフラインの間の選択に関しては、オフラインの場合の厳格な本人確認に使用される印鑑登録証明書との比較が問題となる。印鑑登録証明書は手続ごとに必要となる都度発行され、その発行期日が記載されているが、発行時点以降の有効性を保証するものではない。行政機関等では一般に、添付される印鑑登録証明書の要件として、発行後一定期間内（通例は３か月が多い）のものに限ることとしており、逆に当該期間内に発行された印鑑登録証明書であれば、申請等時点における本人確認書類として有効なものとして取り扱っている。したがって、士業個人等にとっては、印鑑登録証明書が一定期間内に発行されたものであることが確認できれば、行政機関等に申請等を行った段階で当該印鑑登録証明書が本人確認書類として有効と扱われることが担保されることとなる。

　一方、公的個人認証サービスの電子証明書は印鑑登録証明書と異なり、いったん発行されたものが異なる手続に共通して使用されるものであるとともに、申請等の時点における有効性確認の仕組み（失効情報の提供）が提供されており、行政機関等の側では申請等の時点において電子証明書が有効であることを手続上の要件としている。したがって、士業個人等としては、何らかの形で顧客の電子証明書の有効性を確認できなければ、行政機関等に申請等を行った段階で本人確認情報として有効と扱われることが担保されないものである。

## ３　必要な方策

### （１）基本的な考え方

１（１）に示したとおり公的個人認証サービスは行政手続等のオンライン化を主な目的とした制度であり、官民の適切な棲み分けを確保する観点から、署名検証者の範囲を拡大することについては、一定の制限が課されるべきものと考えられる。一部には、民間認証局と同様に署名検証者の範囲に制限を課す必要はないとの意見もあるところではあるが、本研究会においては、行政手続等における代理申請等の課題を解決するとの観点を中心として、署名検証者の範囲に関する問題を検討することとされたところである。

検討の過程においては４に後述するとおり、署名検証者の範囲を行政機関等、裁判所及び民間認証事業者に限定した現制度の枠内で代理申請等の課題に対処する可能性の分析も試みたところである。しかしながら、いずれの対処策もシステム面・実務面等の問題を含むことが判明したことから、代理申請等の課題を解決するためには行政手続等における申請等の代理等を業とすることができる、いわゆる士業個人等が顧客の電子証明書の有効性確認を実質的に行えるような制度とすることが必要であるとの基本的な考え方を採るに至った[9]。

### （２）具体的な制度の要件

#### ①　都道府県知事（指定認証機関）が失効情報等を提供する相手

２（１）で示したとおり、公的個人認証サービスでは署名検証者の範囲が限定されているが、この制度の実効性を確保するため、失効情報を提供する都道府県知事（指定認証機関）ではＩＰアドレス[10]によるアクセス管理を行っている。こうしたアクセス管理は、今回の代理申請等における課題を解決するに当たっても、制度全体として署名検証者を限定した現制度の趣旨を維持する以上、引き続き必要である。

仮に士業個人等に直接、失効情報を提供するとした場合、各業態を合わせて数万人から数十万人の単位に達すると考えられる士業個人等のアクセス管理を個々に行うのは物理的に不可能である。各業態においては、士業個人等を会員とし、その指導及び連絡に関する事務を行うこととされている連合会等が設置

---

[9] 本報告書の内容に基づいて提供される制度を各関係機関が実際に利用するかどうかは、必要となる情報システムの開発や義務の履行などにかかる負担などを考慮し、各関係機関で判断されるべきものである。

[10] Internet Protocol Address。インターネットやイントラネットなどのＩＰネットワークに接続されたコンピュータ１台１台に割り振られた識別番号。

されているところであり、都道府県知事（指定認証機関）から失効情報等を提供する相手はこの士業連合会等とすることとし、士業個人等へはそれぞれの士業個人等が実質的に有効性確認を行うのに必要な限度において、士業連合会等を通じて回答する仕組みとすることが適当である。

② 回答された情報の用途

士業連合会等から士業個人等に回答された情報の利用は、公的個人認証サービスが行政手続等のオンライン化を主な目的とした制度であること、また官民の適切な棲み分けを確保する必要があることに鑑み、行政機関等に対する代理申請等を行うのに必要な場合に限定する制度とすべきである。

③ 士業個人等と士業連合会等の役割分担

士業個人等と士業連合会等の役割について、顧客との関係やシステム整備の負担などの要素を考慮した場合、具体的な分担の方法として、Ａ案（士業連合会等が失効情報等の提供を受けるとともに、顧客からの受付機能も提供）及びＢ案（士業連合会等が失効情報等の提供を受けるが、顧客からの受付は士業個人等が行う）の２案が想定されたところである。[11]

Ａ案はシステム整備にかかる士業個人等の負担をできるだけ軽くしようという考え方に基づくもの、Ｂ案は顧客と士業個人等の関係を重視しようという考え方に基づくものである。研究会での検討においては、ア）現在の業務の実態を考えれば、顧客に対し、顧客と直接の関係がない士業連合会等に情報を送信するよう依頼することは現実的でなく、顧客と士業個人等の関係を重視すべきであること、また、イ）オフラインの場合に士業連合会等が特段の役割を担っていないことに鑑み、オンラインの場合に士業連合会等が持つ機能が大きくなるのは適当ではないこと、ウ）一方、Ａ案では士業連合会等に顧客の個人情報が集約されるため、士業連合会等にＢ案に比べて過重な個人情報保護上の負担が生ずることなどから、Ａ案は不適当でありＢ案が適当との意見が出されたところであり、Ｂ案の考え方に基づく制度とすることが適当である。

[11] 資料４－３（ＡＢ両案及び現状のスキーム図）参照。

なお、この場合、士業個人等が顧客との関係における直接の相手方となり、顧客の電子証明書等必要な情報の提供を受けることとなることから、士業個人等が必ず顧客の電子署名を検証しなければならないこととすることが適当である。[12]

④　士業連合会等の条件

現制度において、署名検証者は法律の規定により、受領した失効情報等の安全確保、利用・提供の制限、秘密保持等の義務を負うこととされている。[13]

本章の方策に基づく制度において士業連合会等は、都道府県知事（指定認証機関）から失効情報等の提供を受ける点において、現制度の署名検証者と同様の立場に立つものであり、現制度における署名検証者の義務を同様に適用することとすることが適当である。これらの義務は定性的に規定されており、士業連合会等が提供する機能が仮に現制度における署名検証者より量的に小さいとしても、同様の規定が適用されるべきものと考えられる。

なお、現制度における署名検証者については想定されていない、士業個人等に対して有効性確認の結果に関する回答を行う機能が生ずることからは、この機能に関し、更に一定のチェックが可能な制度が必要である[14]。

---

[12] 後述⑥のとおり、士業個人等から士業連合会等に顧客の電子証明書が送信されることもあり得るものであり、その場合には士業連合会等が顧客の電子署名を検証することも可能となる。しかしながら、士業個人等が顧客の電子署名を検証しなくてもよいこととすると、検証が行われるかどうかが不安定となるため、士業個人等が一義的に検証する制度とする必要がある。

[13] 資料４－４（署名検証者の義務）参照。

[14] 具体的な手法としては、現制度で民間認証事業者を対象としている認定（法第１７条第１項＝資料４－５（総務大臣認定の基準）参照）や都道府県知事と署名検証者の取決め（法第１７条第４項及び同項に基づく電子署名に係る地方公共団体の認証業務に関する法律施行規則第２８条）の中で規定、都道府県知事の報告徴収権（法第５６条第１項）などが想定されるが、現制度との均衡等の面での検討が必要である。

⑤　士業個人等の義務

士業個人等についても士業連合会等と同様、量的な違いこそあれ、失効情報等と同種の情報の提供を受けることとなるものである。したがって、現制度における署名検証者に準じ、署名検証者の義務と同様の規定に基づく義務を適用することとすることが適当である[15]。

⑥　士業個人等から士業連合会等に送信される情報の範囲

（ア）申請書、委任状等の本体文書

顧客名義の申請書、委任状等のいわゆる本体文書には、申請や委任の内容等に関する顧客の重要な個人情報が含まれているところ、個人情報保護の観点からは、士業連合会等が顧客の個人情報を必要以上に取得すべきではない。士業連合会等が顧客の電子署名の検証を行わない場合には本体文書を士業連合会等に送信する必要がないことはもちろんのこと、士業連合会等が顧客の電子署名の検証を行う場合であっても、本体文書のように重要な個人情報を含まない別の文書[16]を士業連合会等に送信することとすることが望ましい。

（イ）電子証明書

士業連合会等が顧客の電子署名の検証を行わない場合であっても、その顧客の電子証明書の有効性確認を行うためには、対象となる電子証明書を特定するために必要な情報が士業連合会等に送信される必要がある。この場合、（ア）と同様に個人情報保護の観点からは、電子証明書そのものを送信する方法ではなく、電子証明書のシリアル番号及び発行都道府県知事者名に関する情報のみを送信する方法を採ることが望ましい。[17]

なお、この方法については、（ａ）士業個人等が都道府県知事の自己署名証明書を入手する必要がある、（ｂ）仮に悪意ある士業個人等が存在した場合に技術面のみの対処では限界がある、（ｃ）士業個人等と士業連合会等の間の厳格な本人確認が必要であるなどの課題が指摘されたところである。これらの課

---

[15] 署名検証者は法第２５条第１項の規定により、失効情報等の適切な管理のために必要な措置を講じなければならないこととされている。士業個人等について、これに準じることとなれば、例えば、士業個人等が使用するクライアントソフト等について、その管理義務が一義的には士業個人等に生ずることとなるものである。ただし、実態上は個々の士業個人等が管理するのは効率的でないことから、士業連合会等や民間企業等に委託されることになるものと想定される。なお、脚注２１参照。

[16] 例えば、単に顧客の電子証明書の有効性確認を請求する旨のみを記載した有効性確認請求書などが想定される。

[17] ２つの方法におけるシステム開発・運用の費用等については、財団法人自治体衛星通信機構より一定の条件下で両者を比較した試算が示されたが、両者の間に大きな相違は

題に対しては、（ａ）士業連合会等が一括して都道府県知事の自己署名証明書を士業個人等に送付する、（ｂ）悪意ある士業個人等に対しては④⑤に示した制度上の措置による抑止を図る、（ｃ）士業連合会等自身やその他の認証局が士業個人等に発行する電子証明書を活用するなどの方策を採るといった解決策が可能である。[18]

ただし今後、技術的な条件等が変動する等の可能性もあるため、制度上は電子証明書のシリアル番号及び発行都道府県知事者名に関する情報のみを送信する方法だけでなく、電子証明書そのものを送信する方法を士業連合会等が選択することを可能とすることもあり得る。

⑦　士業連合会等から士業個人等に行われる回答の範囲

現制度において署名検証者に対する失効情報の提供方法としては、ア）ＣＲＬ方式（提供時点で失効しているすべての電子証明書に関する失効情報を一覧にしたＣＲＬ[19]を提供）と、イ）ＯＣＳＰレスポンダ方式（特定の電子証明書についてのオンラインでの照会に対し、その電子証明書に関する失効情報のみをＯＣＳＰレスポンダ[20]から回答）の２つがある。

ＣＲＬ方式では、提供されたＣＲＬと該当の電子証明書の間の照合を署名検証者自身で行わなければならないものの、多くの電子証明書の有効性確認を効率的に行えるのに対し、ＯＣＳＰレスポンダ方式では比較的少ない数の電子証明書であれば、その電子証明書に関する失効情報を直ちに回答として得られるものである。個人情報を厳格に保護する観点からは、士業個人等に提供される失効情報の範囲は、それぞれの士業個人等が実質的に有効性確認を行うのに必要な限度に限定されるべきところ、士業個人等が現制度における署名検証者と同様に大量の電子証明書を扱うこととなることはまず想定されないことから、士業個人等に対する有効性確認の結果に関する回答はＯＣＳＰレスポンダ方式と同様の方式のみによることとし、回答の範囲をそれぞれの士業個人等が実質的に有効性確認を行うのに必要な電子証明書に関するものに確実に限定できるようにすることが必要である。

なお、更に個人情報を厳格に保護すべきとの観点からは、現在のＯＣＳＰレスポンダ方式により提供される失効事由（リーズンコード＝紛失等利用者の秘密鍵危殆化時／認証局秘密鍵危殆化時／異動等による失効時／証明書更新に伴

---

見られなかった。

[18] 資料５（シリアル番号通知による電子証明書有効性確認の検討（財団法人自治体衛星通信機構資料））参照。

[19] Certificate Revocation List。

[20] Online Certificate Status Protocol Responder。

う失効時／利用者からの希望による失効時の５種類）を士業個人等に行う回答の範囲に含めないこととする考え方もありうるところである。しかし、これらの事由が士業個人等に提供されることについては、提供の方式がＯＣＳＰレスポンダ方式と同様の方式に限定されるのであれば個人情報保護の観点から問題とはならないと考えられるとの意見で一致したところであり、こうした考え方を採るものではない。[2122]

[21] なお、この整理により、士業個人等に行われる個々の電子証明書に関する回答については、その範囲・内容と一般の署名検証者に提供される個々の電子証明書に関する失効情報の範囲・内容が同様となることから、⑤で士業個人等に対し、現制度における署名検証者に準じ、署名検証者の義務と同様の規定に基づく義務を適用することが必要となるものである。

[22] 一方、不動産登記に関し、死亡や氏名変更、住所変更等の事実があった場合に登記名義人変更登記の必要があることから、失効情報の中にこれらの事実を示す情報を追加すべきだとの意見も出されたところである。しかしながら、これらの情報については電子証明書の記載事項を定めた国際標準との関係で追加することができないこと、また現制度においても個人情報保護の観点から含めておらず、公的個人認証サービス側（都道府県知事（指定認証機関））で当該情報を保持していないものであることなどから、追加は困難である。

## ４　現制度における対処可能性の分析

検討の過程においては、３（１）で示したとおり、署名検証者の範囲を行政機関等、裁判所及び民間認証事業者に限定した現制度の枠内で代理申請等の課題に対処する可能性の分析も試みたところである。その対処策及び問題点は次のとおりである。

### （１）顧客の電子署名の必要性の精査

#### ①　対処策

代理申請等において、行政機関等としては士業個人等の本人確認さえ厳格に行えば、顧客の本人確認を士業個人等に一定程度委ねることが可能ではないかとの観点から、代理申請等における顧客の電子署名の必要性を精査することによる対処もあり得るところである。これにより顧客の電子署名が不要となれば、士業個人等が顧客の電子証明書の有効性確認を行う必要はなくなるものである。

#### ②　問題点

顧客の電子署名の要否は、顧客の本人確認を行う各行政機関等の判断によるものとされており、一概に要不要を論ずることはできない問題である。申請等の内容にもよるが、一般には、送信される情報の作成者及びその内容の改ざんがされていないことを確認する必要性があるが、これは代理申請等における顧客についても同様に当てはまるものであり、[23]この手段として電子署名が必要となるものである。

### （２）行政機関等による速やかな「受理証明」の提示

#### ①　対処策

士業個人等から行政機関等に代理申請等が行われる際、行政機関等から電子証明書の有効性確認の結果が例えば「受理証明」といった形で速やかに示されれば、失効していた場合でもその時点から申請等をやり直せば足り、士業個人等が顧客の電子証明書の有効性確認を行う必要はなくなるとも考えられるところである。

#### ②　問題点

そもそも今回の代理申請等における課題に関しては、２（２）で示したとおり、いったん行った手続をやり直すことに伴うリスクがオンライン化の障害に

---

[23] 電子申請等を受け付けている国の各府省及び地方公共団体を対象に、代理申請等の現状を調査したところ、代理人による申請等を受け付けている６機関（国の４省及び２県）のうち、３機関がすべての手続について、残りの３機関も大部分の手続について、それぞれ本人（顧客）の電子署名を要することとしているとの結果が得られた。

なるとの指摘がなされているものであり、特に関係者が多数に及ぶ場合や資金決済が連動する場合など、申請前に有効性確認を行えるようにすることが求められているものである。

なお、国の機関においては、申請者が自らの申請等が受付システムに到達したかどうかを確認できるよう、申請者に「到達確認通知」を行うこととされている。しかしながら、これが電子証明書の有効性確認を行った上で行われるかどうかは各行政機関等の判断によるものであり、すべての行政機関等における対応を前提に制度を設計するのは適当でない。

### （３）自己の電子証明書の有効性確認の応用

#### ①　対処策

（ア）結果に関する顧客本人からの自己申告

顧客はオンライン窓口[24]により自己の電子証明書の有効性確認を行えるので、顧客本人から士業個人等に自己申告すれば足りるとの対処も考えられるところである。

（イ）士業個人等の事務所における顧客本人の確認

顧客が士業個人等の事務所に出向いて自己の電子証明書の有効性確認を行えば足りるとの対処も考えられるところである。

（ウ）都道府県知事（指定認証機関）から士業個人等への結果の同報

顧客が行う自己の電子証明書の有効性確認の結果が都道府県知事（指定認証機関）から、顧客本人だけでなく士業個人等にも同時に伝えられれば足りるとの対処も考えられるところである。

#### ②　問題点

（ア）オンライン窓口による自己の電子証明書の有効性確認の結果は、単に顧客のパソコンの画面に表示されるだけであり、士業個人等がその結果を正当なものとして確認できる手段がない（署名検証者に提供される失効情報のように都道府県知事の電子署名による正当性の確認ができない。また、そもそも顧客本人が真実を申告しているかどうかについても確認する方法がない）。したがって、申告を受けた士業個人等にとっては申告の結果についての正当性が証明されるものではなく、十分とは言えない。

（イ）代理・委任関係における顧客と士業個人等の間の本人確認をオフラインで行うことと、代理申請等の要件として顧客本人の有効な電子証明書が必要とされていることは区別して考える必要がある。また、代理申請等の実態上、

---

[24] 利用者が自宅や会社等のパソコンから、自らの電子証明書の有効性確認や失効申請を行えるシステム。

**すべての手続に顧客と士業個人等の間で対面によるやりとりがあるわけではなく、不動産取引など当事者が多数に及ぶ場合があることを考えれば、オンラインによる代理申請等の場合に士業個人等の事務所に出向くことを必須とするのは現実的でない。また、オンライン申請等において、オフラインによるやりとりを経なければならないこととするのは手法として不適当である。**

**（ウ）署名検証者を限定している制度の趣旨からは、有効性確認の結果を回答する相手方（この場合は士業個人等）に対してアクセス管理を施す必要がある。しかしながら、３（２）①でも示したとおり、これは都道府県知事（指定認証機関）・士業個人等の両者にとって、手数・費用等の面で現実的とは言えない。**

## ５　その他

以上に示した代理申請等における課題に関する検討のほか研究会では、医療機関等による公的個人認証サービスの利用についても検討すべきではないかとの意見が出されたところである。

現制度において、国公立の医療機関等は署名検証者の範囲に含まれているが、私立の機関等は対象となっていない。しかしながら、医療機関等が提供しているサービス等の内容を考えれば、その機関が国公立か私立かという違いは、特にサービスを受ける利用者にとってそれほど意識されるものではないと考えられる。

医療機関等による利用は、代理申請等における課題を検討する本研究会で直接検討すべき課題ではないが、本研究会を契機に提示された課題であることから、事務局において厚生労働省等の関係機関等と調整したところであり、その結果を以下に示す。

医療機関等には、患者等の個人が行政手続等を行う際に必要となる情報をその個人に提供する役割[25]を担っているという特徴がある。これらの情報が不可欠な申請等をオンラインで行おうとした場合、将来的には申請書等の本体文書だけでなく、医療機関等から提供される情報についても電子化されることが望ましい。

これらの情報は患者等本人の高度に保護されるべき個人情報を含むものであることから、医療機関等が本人に提供する際に本人確認を厳格に行う必要があり、その場合には公的個人認証サービスにより発行された本人の電子証明書及びそれによる電子署名を用いることが有効である。

しかしながら、現制度においては署名検証者の範囲に私立の医療機関等が含まれていないことから、これら私立の医療機関等は患者等に対して診断書等の情報をオンラインで提供することは現実的に不可能である。

申請等を行う患者等個人の側としては、医療機関等が国公立であるか私立であるかの違いによって、診断書等の電子的な発行を含めた医療サービスの提供範囲が異なるとすれば社会通念上、妥当な制度とは言い難いものと考えられる。こうした行政手続等に必要な情報を提供する医療機関等に関しては、私立機関等についても、その必要な範囲に限って、公的個人認証サービスによる患者等個人の電子証明書に関する有効性確認を実質的に行えるような制度とすることが適当である。

---

[25] 例えば、患者に対する診断書の提供などが想定される。

**　なお、医療機関等については、士業個人等と同様に数量的なアクセス管理上の問題があることから、関係団体等を通じて各医師等に必要な回答を行うこととすることが必要である。**

資料１

# 「公的個人認証サービスにおける署名検証者の範囲の在り方に関する研究会」開催要綱

## １　目的

電子政府・電子自治体の実現のため、行政手続等のオンライン化における確かな本人確認サービスとして、平成１６年１月２９日より公的個人認証サービスが開始された。同サービスにおいては、電子証明書の有効性確認を行える署名検証者が行政機関等及び民間認証事業者に限定されているところである。これについては、行政手続等の代理が行われる場合、即ち、いわゆる「士業」等が顧客の行政手続等を代理する場合、顧客の電子証明書の有効性確認を行えないことが行政手続等のオンライン化を進める上での課題となっている。

したがって、署名検証者の範囲の在り方に関し、いわゆる士業等の資格を有する個人による公的個人認証サービスの電子証明書の有効性確認について、その実施及び手法等を検討し、総務省等における制度設計の参考とする。

## ２　名称

本研究会は、「公的個人認証サービスにおける署名検証者の範囲の在り方に関する研究会」（以下「研究会」という。）と称する。

## ３　検討課題

（１）現制度における問題点の明確化
（２）対策の実施及び手法等
（３）その他付随して生ずる課題への解決策

## ４　運営

（１）研究会の構成員は、別紙「構成員名簿」のとおりとする。
（２）研究会には座長を１名置く。

## ５　開催期間

平成１６年９月から１２月まで、合計３回程度開催する。

## ６　庶務

総務省自治行政局自治政策課が行う。

（附則）この要綱は、平成１６年９月２８日から施行する。

別　紙

「公的個人認証サービスにおける署名検証者の範囲の在り方に関する研究会」
構成員名簿

（５０音順、敬称略）

| | |
|---|---|
| 宇賀　克也 | 東京大学教授 |
| 大谷　義雄 | 全国社会保険労務士会連合会理事 |
| 大山　永昭 | 東京工業大学教授 |
| 栗原　達雄 | 日本認証サービス株式会社代表取締役社長 |
| 佐々木　浩 | 岐阜県知事公室長 |
| 佐藤　純通 | 日本司法書士会連合会副会長 |
| 田中　一志 | 日本税理士会連合会情報システム委員会委員長常務理事 |
| 辻井　重男 | 情報セキュリティ大学院大学学長（座長） |
| 中井川　禎彦 | 総務省行政管理局行政情報システム企画課情報システム企画官 |
| 中西　豊 | 日本行政書士会連合会高度情報通信社会対策本部委員 |
| 藤原　宏髙 | 日本弁護士連合会コンピュータ委員会委員長 |
| 牧野　二郎 | 弁護士 |
| 馬渕　良一 | 日本土地家屋調査士会連合会副会長 |
| 吉崎　賢介 | 財団法人自治体衛星通信機構公的個人認証サービスセンターセンター長 |
| 米倉　昭利 | 財団法人日本情報処理開発協会電子署名・認証センターセンター長 |
| 渡部　正和 | 日本公証人連合会電子公証委員長 |

資料２

# 「公的個人認証サービスにおける署名検証者の範囲の在り方に関する研究会」開催状況

○　第１回会合：平成１６年９月２８日（火）

- 座長選出
- 公的個人認証サービスの現状
- 代理申請における課題

○　第２回会合：平成１６年１０月２８日（木）

- 第１回の論点整理
- 本研究会の論点整理（報告書骨子）

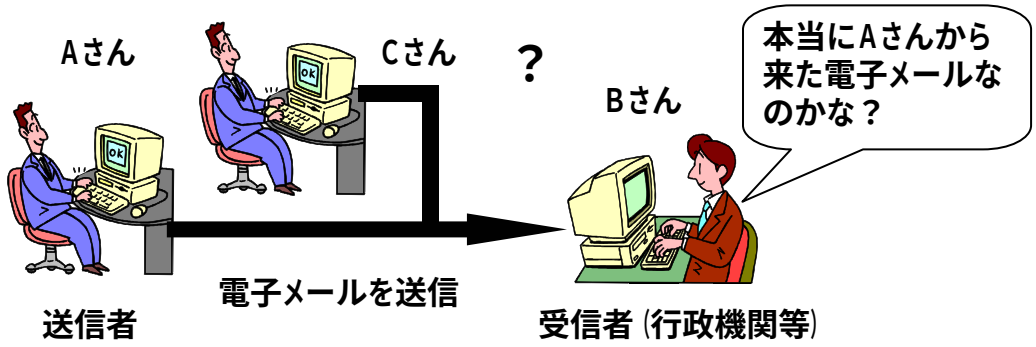
○　第３回会合：平成１６年１２月９日（木）

- 報告書取りまとめ

# デジタル社会における課題

資料３－１

## ① 成りすまし （←インターネット上におけるデジタル文書については、文書作成者の特定が困難）




※例えば、suzuki@jichiseisaku.co.jp というメールアドレスで、自治政策株式会社鈴木という名義で文書が送られてきたとしても‥

・「自治政策株式会社」が実在しないかもしれない。

・「鈴木」さんが実在しないかもしれない。

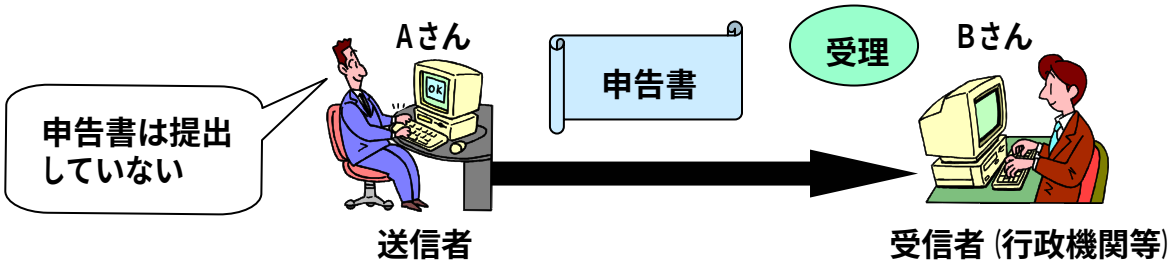
・第三者が実在する「自治政策株式会社」の「鈴木」さんのメールアドレスを乱用しているかもしれない。

という疑いが解消できない。

## ② 改ざん （←送信途上でメッセージを書き換えることが容易）


※デジタル文書は、手書きの文書と異なり、改ざんされても痕跡が残らず、改ざん箇所を発見することは、実際上不可能。

## ③ 送信否認 （←送信内容の否認を防止することが困難）



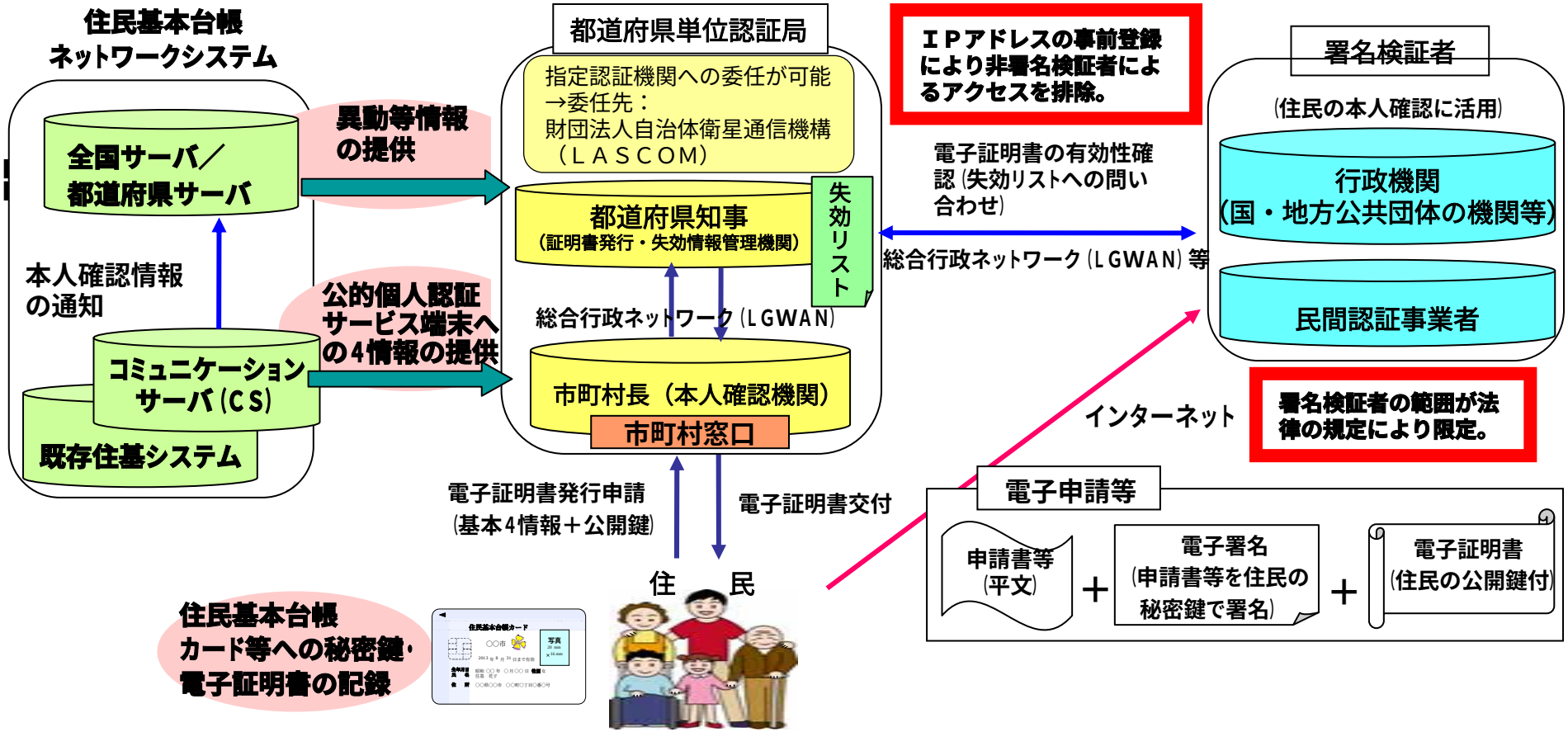

※オンラインで送信されてきた申請･届出に基づいて、手続を進行させていたところ、送信者からそのような送信はしていないとの否認をされる危険性がある。

# 公的個人認証サービス

資料３－２

○　成りすまし、改ざん、送信否認などの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。

→　平成１６年１月２９日、公的個人認証サービスの提供を開始。
（電子証明書の有効期間３年間、発行手数料５００円）

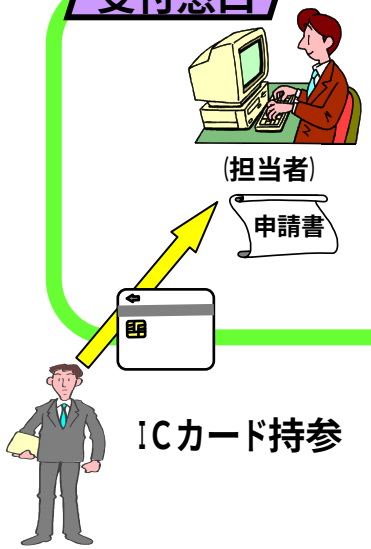


# 電子証明書の発行等の手続イメージ

資料３－３

## １．市町村役場へ行く

受付窓口



（担当者）

申請書

ICカード持参

## ２．受付手続
（申請書提出）

**公的個人認証サービス**
**電子証明書発行申請書**

平成　年　月　日

| | |
|---|---|
| 申請者氏名 | 総務　　太郎 |
| ふりがな | そうむ　たろう |
| 生年月日 | 昭和３７年　６月１７日 |
| 男女の別 | 男 |
| 住所 | 霞が関２丁目１番地２号 |

※1　氏名、住所の記載表記は、住民票に記載されている漢字を 用いてください。
※2　パソコン等で、住民票に記載されている漢字が表記できない場合、申請者が日常パソコン等で使用している代替文字を記載してください。

| | |
|---|---|
| 代替文字 | 有　・　(無) |
| 指定代替文字 | |

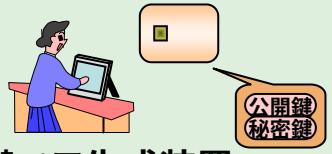
## ３．本人確認

・実在していること
（住民基本台帳データと突合）
・本人であること
（写真付住基カード、運転免許証etc.）

（担当者）

## ４．本人確認後、住民自身による鍵生成

ICｶｰﾄﾞへの暗号鍵ﾍﾟｱ書込（パスワード設定）




鍵ペア生成装置
（市町村窓口に設置）

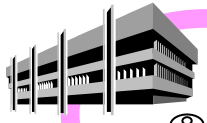
## ５．公開鍵提出

公開鍵提出

（担当者）

## ６．証明書発行手続

都道府県知事が発行




CD－ROM（利用者クライアントソフト）
利用のご案内ほかを併せて配付

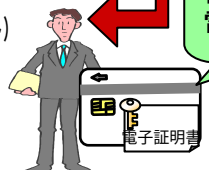
## ７．証明書の交付

受渡窓口

ICカードへの
電子証明書の
書き込み

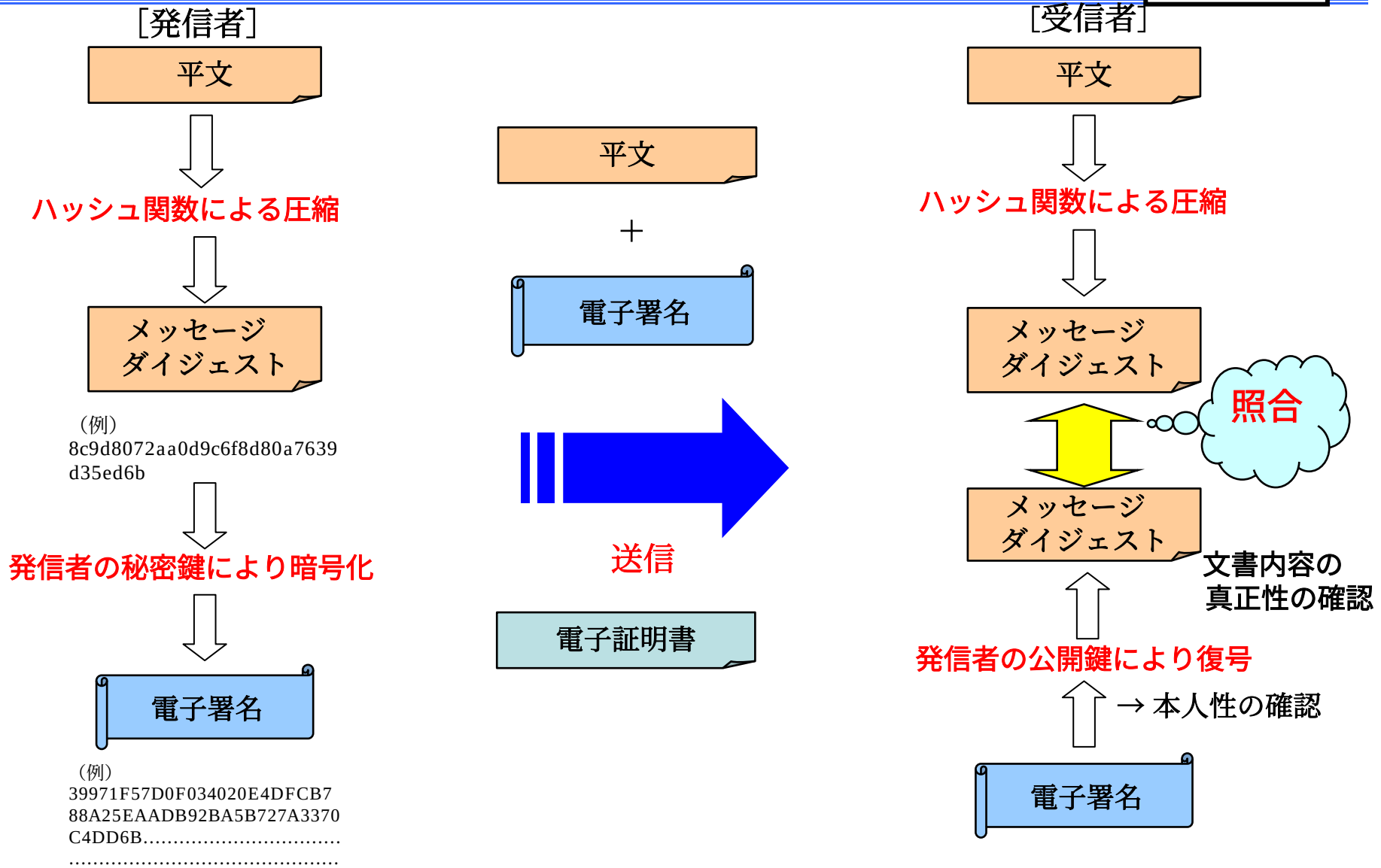
（担当者）

住民の秘密鍵
電子証明書



# 電子署名(デジタル署名)の概要

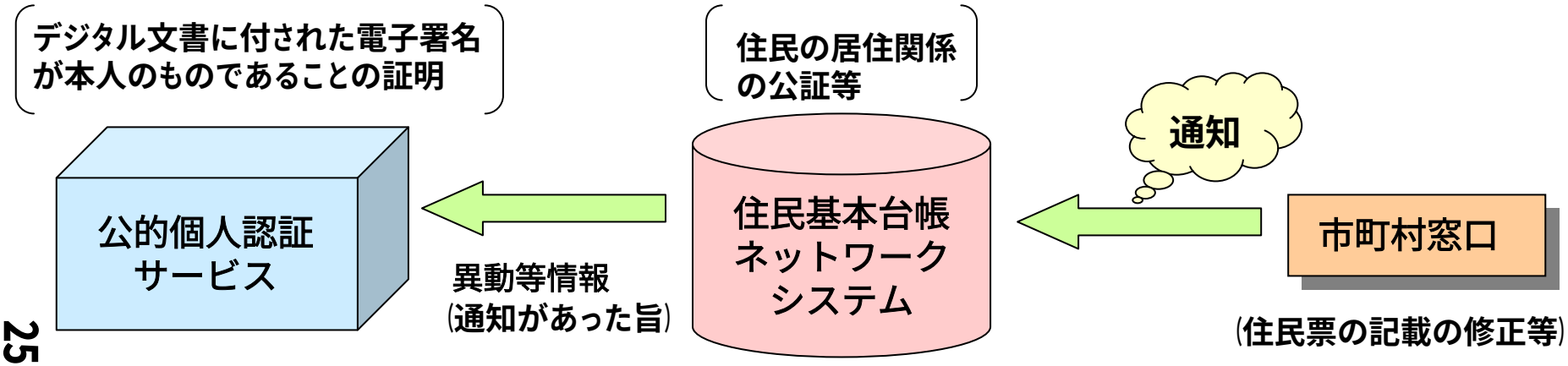
資料３－４




※（注）１　この他、文書内容の秘匿性を確保するための暗号化に鍵ペアが使用されることもある。
２　ハッシュ関数：y=f(x)において、x（平文）からy（メッセージ・ダイジェスト）を求めるのは簡単であるが、yからxを求めるのは事実上困難であり、かつ異なるxから同一のyを生成するのが計算上不可能であるような関数をいう。

資料３－５

# 公的個人認証サービスと住民基本台帳ネットワークシステムの関係




・住所の変更
・氏名の変更
・死亡の事実

※　異動等情報とは、住民基本台帳法の規定による本人確認情報について、住所・氏名の変更又は死亡の事実が生じた場合における当該異動等の事実のみをいい、異動等の内容（新しい住所又は氏名等）及び住民票コードを含まない。

なお、この情報の提供を住民基本台帳ネットワークシステムから受けることにより、

① 公的個人認証サービスのシステム側で、住所異動等に係る個人情報の収集をせずに適確な失効情報を作成すること、
② 住所等電子証明書記載事項の変更があった場合に、利用者及び市町村の担当者は、公的個人認証サービス側には申告を行う必要がなく、利用者の利便性の向上・市町村都道府県の事務の省力化に資すること、
③ 失効情報作成の正確性が向上すること、

等が可能となる。

# 公的個人認証サービスの対象手続

資料３－６

## 国

（件数は紙も含めた過去の全国における年間実績）

| | | |
|---|---|---|
| ・２月２日～ | 電子申告・納税（国税庁）【東海４県先行,6/1～全国展開】 | :約 2,000万件/年 |
| ・２月１６日～ | 恩給関連申請の一部（総務省） | :約 19万件/年 |
| ・３月２９日～ | 社会保険関係手続（厚生労働省） | :約 4,900万件/年 |
| 〃 | 無線従事者免許関係手続（総務省） | :約 6万件/年 |
| 〃 | 旅券申請（外務省） 【岡山県ほか順次】 | :約 270万件/年 |
| ・７月１日～ | 年金関係手続（国家公務員共済組合連合会） | :約 23万件/年 |
| ・９月２日～ | 航空従事者技能証明の申請（国土交通省） | :約 1.5万件/年 |
| ・１１月２２日～ | 商業・法人登記申請(法務省)※登記事項証明書等の交付請求を除く | :約 200万件/年 |

## 地方公共団体

（手続の例：住民票の写しの交付請求、納税証明書の交付申請など）

| | |
|---|---|
| ・３月２９日～ | 岡山県 |
| ・４月１日～ | 岐阜県 |
| ・４月１９日～ | 岐阜県内の一部市町 |
| ・４月２１日～ | 山梨県・山梨県全市町村 |
| ・５月２５日～ | 茨城県 |
| ・７月１日～ | 石川県 |
| ・７月９日～ | 富山県 |
| ・７月１２日～ | 茨城県内の一部市町村 |
| ・７月２０日～ | 愛知県 |
| 〃 | 兵庫県 |
| ・７月２８日～ | 香川県 |
| ・８月２日～ | 埼玉県 |
| ・９月１３日～ | 福岡県 |
| ・１０月１日～ | 島根県内の一部市町 |
| 〃 | 滋賀県 |
| 〃 | 大分県・大分県内の一部市町村 |
| 〃 | 鹿児島県 |
| ・１１月１日～ | 山口県 |
| ・１１月１１日～ | 栃木県 |
| ・１１月２０日～ | 広島県・広島県福山市 |
| ・１１月２２日～ | 地域通貨システム(※１) |
| ・１２月１日～ | 茨城県つくば市 |
| ・１２月初旬～ | 地域安心安全情報共有システム(※２) |

（※１）千葉県市川市・福岡県北九州市・熊本県小国町で実施
（※２）北海道長沼町・青森県六戸町・栃木県岩舟町・群馬県富岡町・埼玉県草加市・埼玉県戸田市・千葉県市川市・神奈川県小田原市・神奈川県逗子市・新潟県上越市・石川県金沢市・福井県丸岡市・長野県伊那市・静岡県島田市・愛知県春日井市・大阪府豊中市・兵庫県小野市・岡山県岡山市・福岡県大牟田市・福岡県春日市で実施

**今後、国の機関の手続･各地方公共団体の手続が順次追加される見込み。**

資料４－１

# 電子認証サービスの提供主体など

| | ①個人としての存在の証明 | 組織等の一員としての本人の属性の証明 | | |
|---|---|---|---|---|
| | | ②権限･資格 | ③信用 | ④その他 |
| **公的個人認証サービス**<br>（公的電子認証法） | ･**全国の市町村の役場･支所において、住民基本台帳データを基礎に本人確認（氏名･住所･生年月日･性別）** | | | |
| 民間認証機関によるサービス<br>（電子署名法） | ･住民票の写し等の活用により、自社において本人確認<br>･**公的個人認証サービスの活用によりオンラインで本人確認** | 業務の必要に応じて様々なサービスの提供 | | |
| 商業登記に基礎を置く電子認証制度<br>（商業登記法） | ･登記官への登記申請により、本人の氏名、法人の存在（商号、本店）、代表権限の存在を確認 | | | |

資料４－２

# 署名検証者の範囲（１）

## ○電子署名に係る地方公共団体の認証業務に関する法律第１７条第１項

行政手続等における情報通信の技術の利用に関する法律第二条第二号に規定する行政機関等（以下「行政機関等」という。）並びに電子署名及び認証業務に関する法律第八条に規定する認定認証事業者及び同法第二条第三項に規定する特定認証業務を行う者であって政令で定める基準に適合するものとして総務大臣が認定する者（以下この項において「認定認証事業者等」という。）は、利用者から通知された電子署名が行われた情報について当該利用者が当該電子署名を行ったことを確認するため、都道府県知事に対して次条第一項の規定による同項に規定する保存期間に係る失効情報の提供及び同条第二項の規定による同項に規定する保存期間に係る失効情報ファイルの提供を求めようとする場合（認定認証事業者等にあっては、同法第二条第三項に規定する特定認証業務を行う場合に限る。）には、あらかじめ、当該都道府県知事に対し、総務省令で定めるところにより、これらの提供を求める旨の届出をしなければならない。

※裁判所については、追加する旨の改正案が第１６１回国会で成立したところ。

［抜粋］
①行政手続等における情報通信の技術の利用に関する法律第二条第二号に規定する行政機関等
②電子署名及び認証業務に関する法律第八条に規定する認定認証事業者
③同法第二条第三項に規定する特定認証業務を行う者であって政令で定める基準に適合するものとして総務大臣が認定する者

# 署名検証者の範囲（２）

## ○行政手続等における情報通信の技術の利用に関する法律第２条

この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

二　行政機関等　次に掲げるものをいう。

イ　内閣、法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関若しくは会計検査院又はこれらに置かれる機関

ロ　イに掲げる機関の職員であって法律上独立に権限を行使することを認められたもの

ハ　地方公共団体又はその機関（議会を除く。）

ニ　独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。）

ホ　地方独立行政法人（地方独立行政法人法（平成十五年法律第百十八号）第二条第一項に規定する地方独立行政法人をいう。）

ヘ　法律により直接に設立された法人、特別の法律により特別の設立行為をもって設立された法人（独立行政法人を除く。）又は特別の法律により設立され、かつ、その設立に関し行政庁の認可を要する法人（地方独立行政法人を除く。）のうち、政令で定めるもの

ト　行政庁が法律の規定に基づく試験、検査、検定、登録その他の行政上の事務について当該法律に基づきその全部又は一部を行わせる者を指定した場合におけるその指定を受けた者

チ　ニからトまでに掲げる者（トに掲げる者については、当該者が法人である場合に限る。）の長

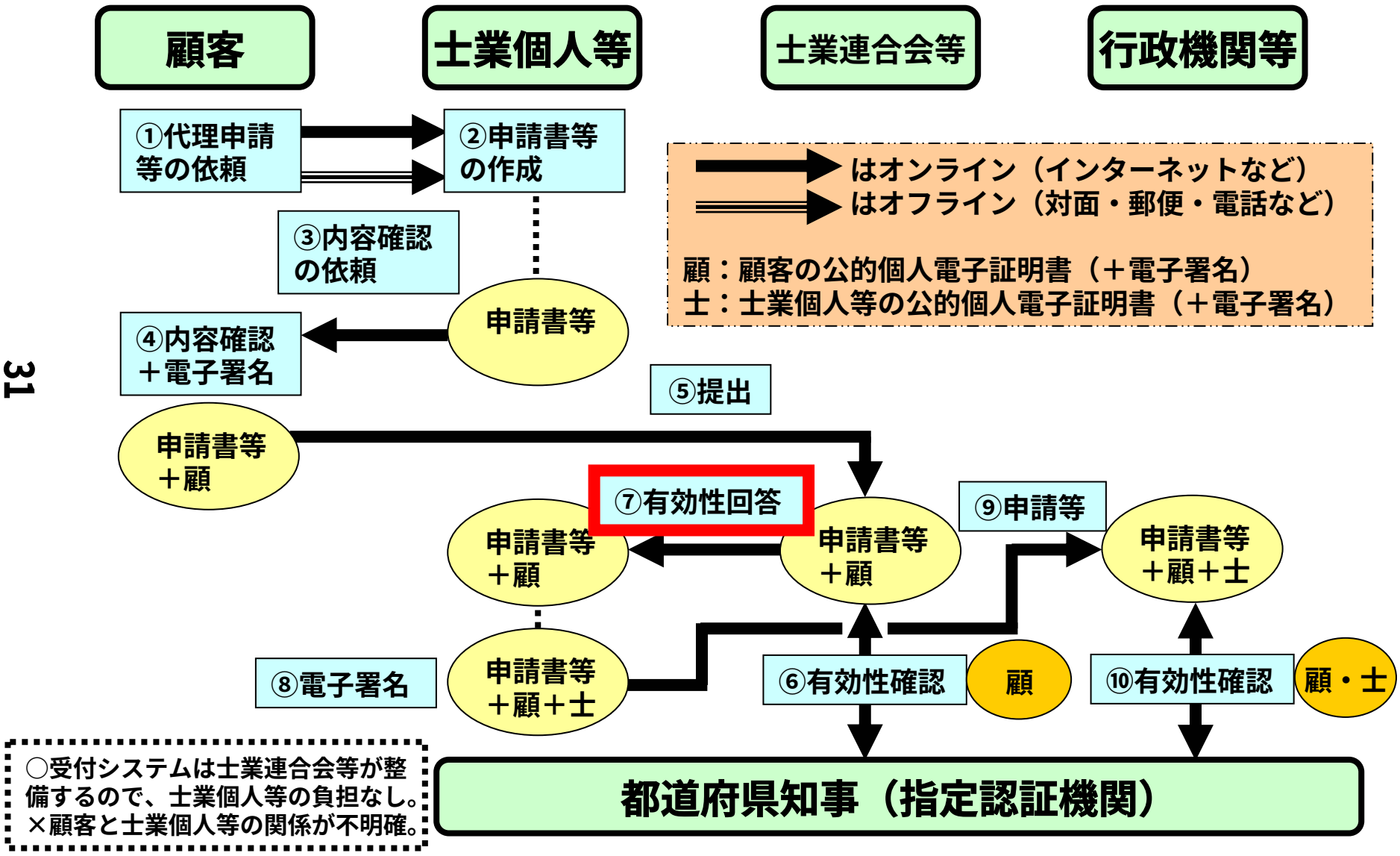
# 署名検証者の範囲（３）

## ○行政手続等における情報通信の技術の利用に関する法律施行令第１条

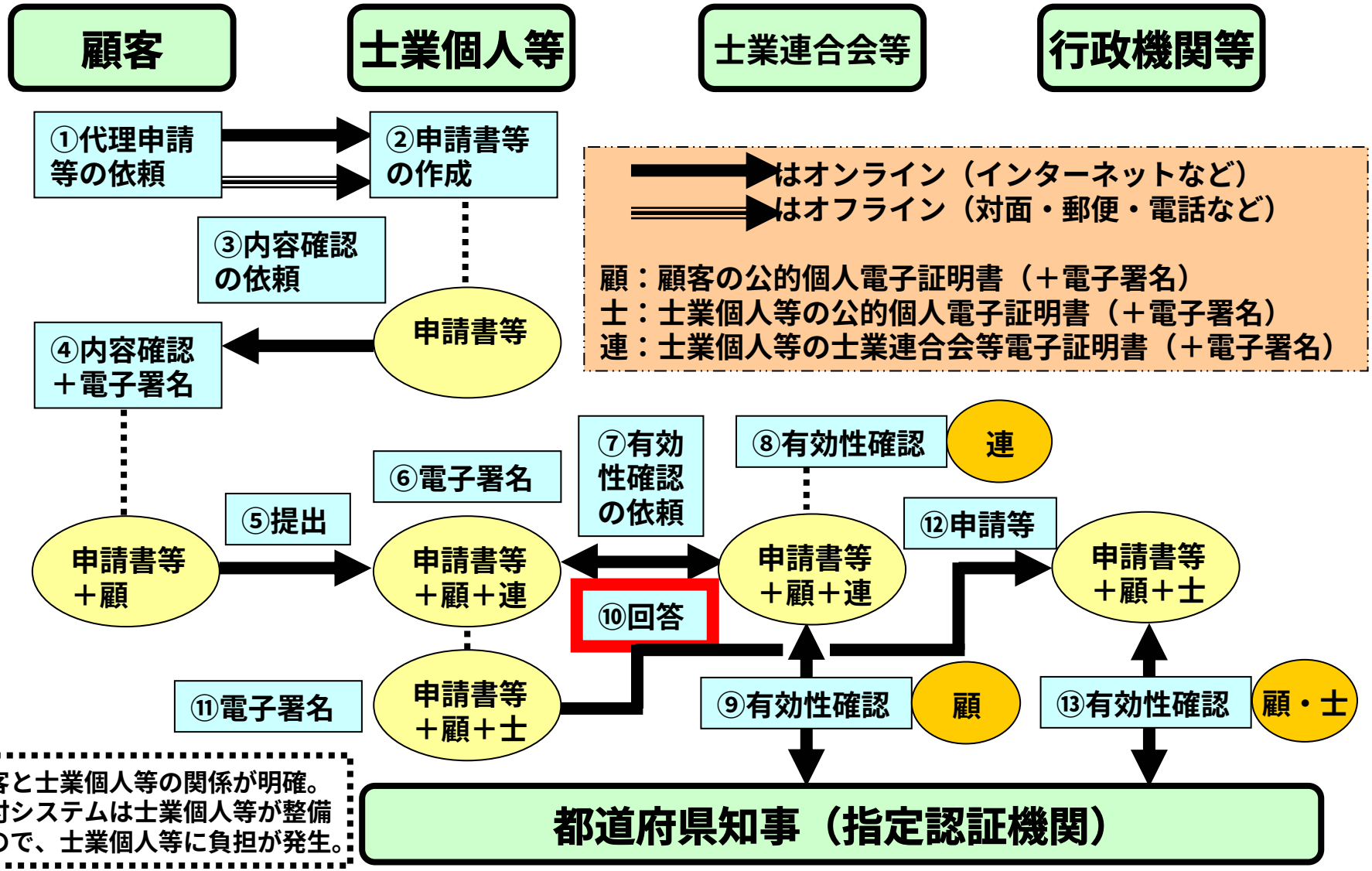
行政手続等における情報通信の技術の利用に関する法律（以下「法」という。）第二条第二号への政令で定める法人は、奄美群島振興開発基金、沖縄振興開発金融公庫、核燃料サイクル開発機構、関西国際空港株式会社、危険物保安技術協会、行政書士会、銀行等保有株式取得機構、警察共済組合、軽自動車検査協会、高圧ガス保安協会、公営企業金融公庫、厚生年金基金連合会、港務局、公立学校共済組合、小型船舶検査機構、国際協力銀行、国民生活金融公庫、国民年金基金連合会、国立大学法人、国家公務員共済組合、国家公務員共済組合連合会、産業基盤整備基金、市議会議員共済会、市町村職員共済組合、指定都市職員共済組合、自動車安全運転センター、司法書士会、社会保険診療報酬支払基金、社会保険労務士会、住宅金融公庫、首都高速道路公団、証券業協会、商工組合中央金庫、商品先物取引協会、消防団員等公務災害補償等共済基金、水害予防組合、水害予防組合連合、税理士会、石炭鉱業年金基金、石油公団、全国市町村職員共済組合連合会、全国社会保険労務士会連合会、総合研究開発機構、大学共同利用機関法人、地域振興整備公団、地方競馬全国協会、地方公務員共済組合連合会、地方公務員災害補償基金、地方住宅供給公社、地方職員共済組合、地方道路公社、中小企業金融公庫、中小企業総合事業団、町村議会議員共済会、都市基盤整備公団、都市職員共済組合、都職員共済組合、土地家屋調査士会、都道府県議会議員共済会、日本行政書士会連合会、日本銀行、日本勤労者住宅協会、日本下水道事業団、日本原子力研究所、日本公認会計士協会、日本小型自動車振興会、日本自転車振興会、日本司法書士会連合会、日本消防検定協会、日本私立学校振興・共済事業団、日本政策投資銀行、日本税理士会連合会、日本船舶振興会、日本たばこ産業株式会社、日本たばこ産業共済組合、日本中央競馬会、日本鉄道共済組合、日本電気計器検定所、日本道路公団、日本土地家屋調査士会連合会、日本弁理士会、日本放送協会、日本郵政公社、年金資金運用基金、農水産業協同組合貯金保険機構、農林漁業金融公庫、農林漁業団体職員共済組合、阪神高速道路公団、放送大学学園、本州四国連絡橋公団及び預金保険機構とする。

資料４－３

# A案（士業連合会等が署名検証者＋受付）

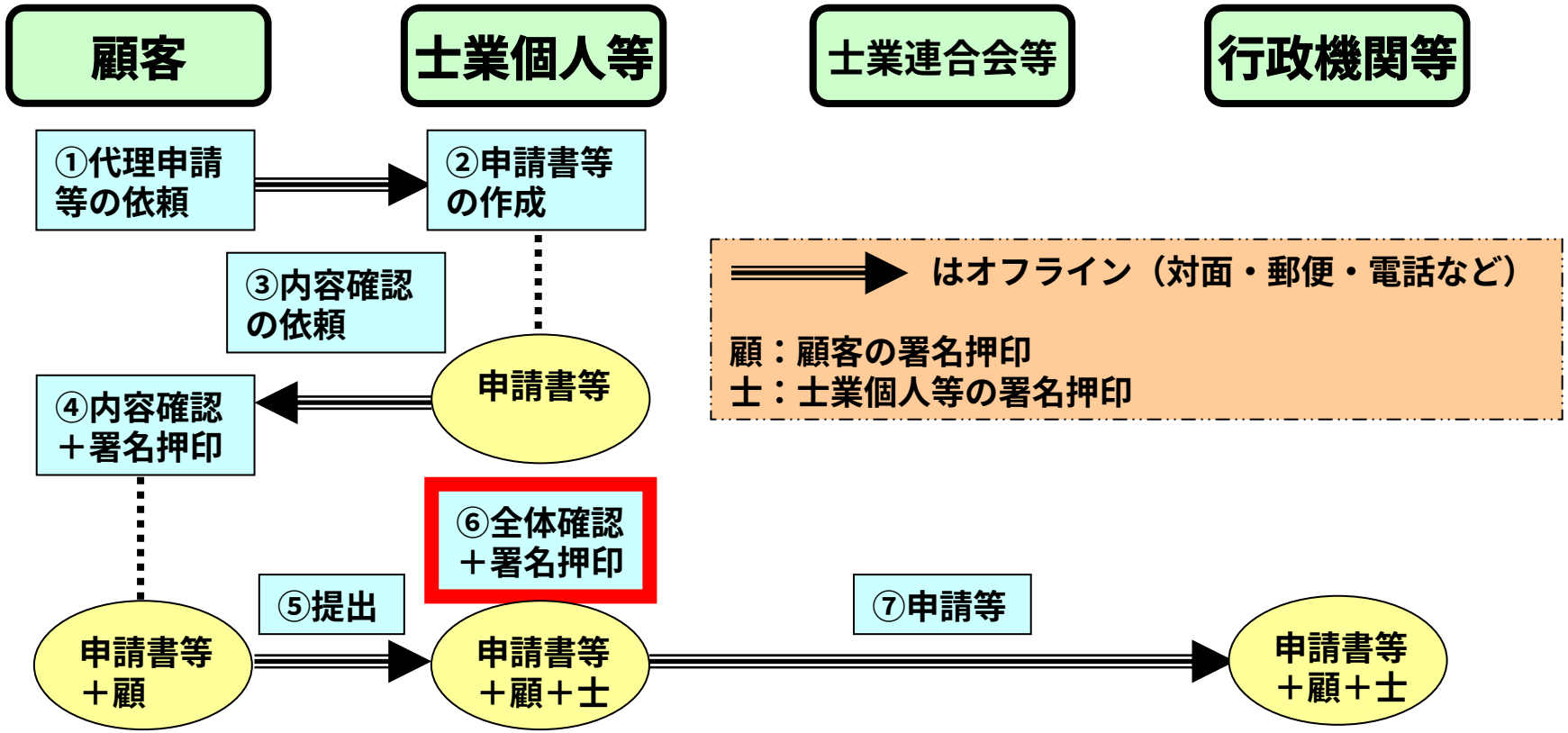


# B案（士業連合会等が署名検証者＋士業個人が受付）

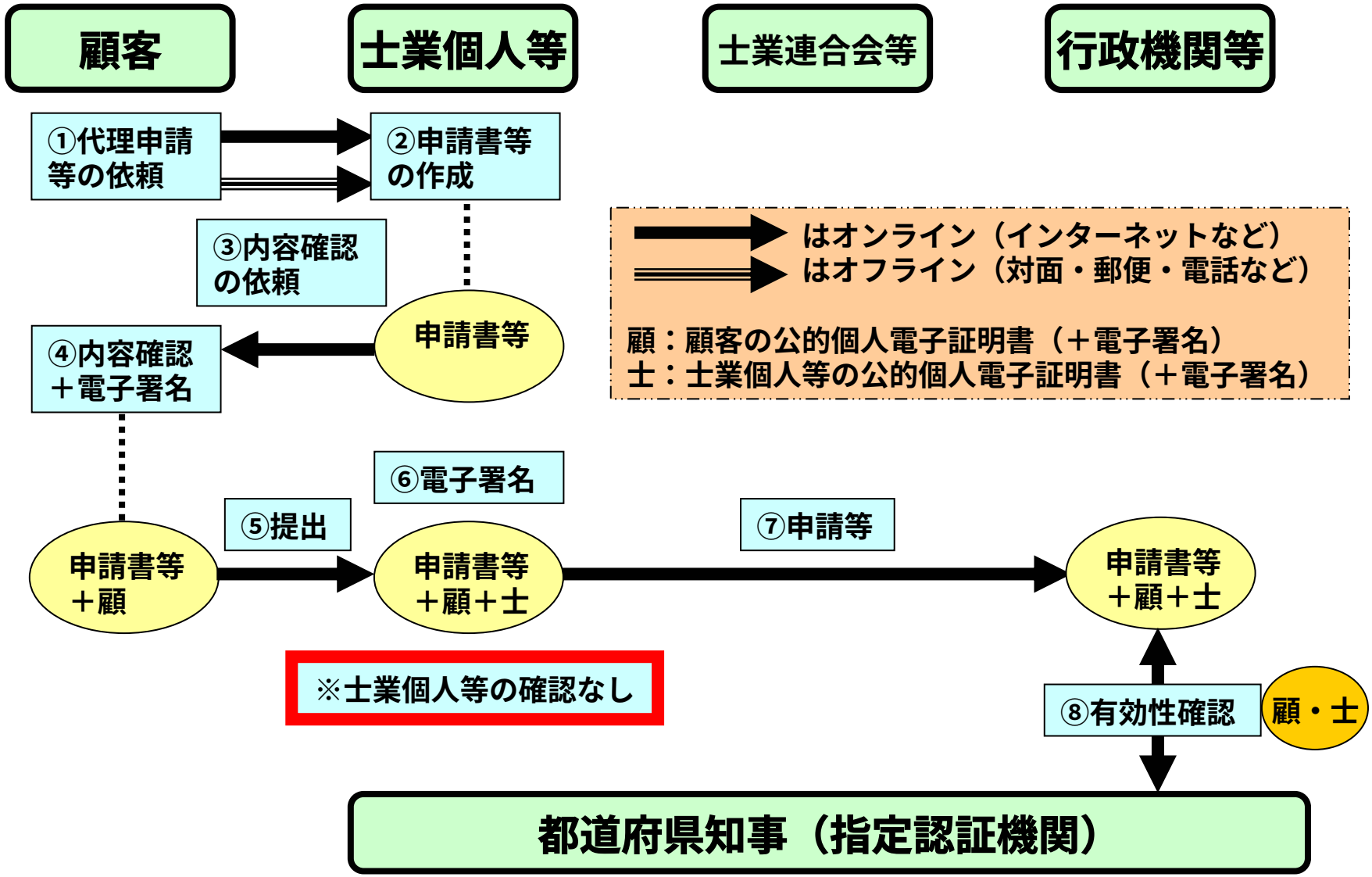



※本図は士業連合会等が士業個人等に電子証明書を発行している場合。⑥で士業個人等が付す電子証明書は「士」もありうるが、その場合、士業連合会等が当該士業個人等の資格を確認する仕組が別途必要。また、⑪で士業個人等が付す電子証明書は、行政機関等の方針によっては「連」も可。

# 現状（オフライン）


顧客
士業個人等
士業連合会等
行政機関等
①代理申請等の依頼
②申請書等の作成
③内容確認の依頼
申請書等
④内容確認＋署名押印
⑥全体確認＋署名押印
⑤提出
⑦申請等
申請書等＋顧
申請書等＋顧＋士
申請書等＋顧＋士
はオフライン（対面・郵便・電話など）
顧：顧客の署名押印
士：士業個人等の署名押印

# 現状（オンライン）


顧客
士業個人等
士業連合会等
行政機関等
①代理申請等の依頼
②申請書等の作成
③内容確認の依頼
申請書等
④内容確認＋電子署名
はオンライン（インターネットなど）
はオフライン（対面・郵便・電話など）
顧：顧客の公的個人電子証明書（＋電子署名）
士：士業個人等の公的個人電子証明書（＋電子署名）
⑥電子署名
⑤提出
⑦申請等
申請書等＋顧
申請書等＋顧＋士
申請書等＋顧＋士
※士業個人等の確認なし
⑧有効性確認
顧・士
都道府県知事（指定認証機関）

資料４－４

# 署名検証者の義務（１）

## ○電子署名に係る地方公共団体の認証業務に関する法律

（署名検証者の義務）

第十九条　署名検証者は、利用者から当該利用者に係る利用者署名符号を用いて電子署名が行われた情報及び電子証明書の通知を受理したときは、当該電子証明書が第十五条第一項の規定により効力を失っていないこと及び当該電子証明書に記録された利用者署名検証符号に対応する利用者署名符号を用いて当該電子署名が行われたことを確認しなければならない。

２　署名検証者は、利用者から通知された電子証明書を、当該電子証明書とともに通知された情報について行われている電子署名が当該電子証明書に記録された利用者署名検証符号に対応する利用者署名符号を用いて行われていることの確認以外の目的に利用してはならない。

（署名検証者による受領した失効情報等の安全確保）

第二十五条　第十八条第一項及び第二項の規定により保存期間に係る失効情報及び保存期間に係る失効情報ファイルの提供を受けた署名検証者がこれらの規定により提供を受けた保存期間に係る失効情報及び保存期間に係る失効情報ファイル（以下「受領した失効情報等」という。）の電子計算機処理等を行うに当たっては、当該署名検証者は、受領した失効情報等の漏えいの防止その他の当該受領した失効情報等の適切な管理のために必要な措置を講じなければならない。

２　前項の規定は、署名検証者から受領した失効情報等の電子計算機処理等の委託を受けた者が受託した業務を行う場合について準用する。

# 署名検証者の義務（２）

（署名検証者の受領した失効情報等の利用及び提供の制限）
第二十六条　署名検証者は、第十九条第一項の規定により電子証明書が効力を失っていないことの確認をするため必要な範囲内で、受領した失効情報等を利用するものとし、受領した失効情報等の全部又は一部を当該確認以外の目的のために利用し、又は提供してはならない。

（署名検証者の職員等の秘密保持義務）
第二十七条　受領した失効情報等の電子計算機処理等に関する事務に従事する署名検証者若しくはその役員若しくは職員又はこれらの者であった者は、その事務に関して知り得た受領した失効情報等に関する秘密又は受領した失効情報等の電子計算機処理等に関する秘密を漏らしてはならない。
２　署名検証者から、受領した失効情報等の電子計算機処理等の委託を受けた者若しくはその役員若しくは職員又はこれらの者であった者は、その委託された業務に関して知り得た受領した失効情報等に関する秘密又は受領した失効情報等の電子計算機処理等に関する秘密を漏らしてはならない。

（受領した失効情報等に係る電子計算機処理等の受託者等の義務）
第二十八条　署名検証者の委託を受けて行う受領した失効情報等の電子計算機処理等に関する事務に従事している者又は従事していた者は、その事務に関して知り得た事項をみだりに他人に知らせ、又は不当な目的に使用してはならない。

資料４－５

# 総務大臣認定の基準（１）

## ○電子署名に係る地方公共団体の認証業務に関する法律施行令

（特定認証業務を行う者に係る認定の基準）

第八条　法第十七条第一項の政令で定める基準は、特定認証業務（電子署名及び認証業務に関する法律（平成十二年法律第百二号）第二条第三項に規定する特定認証業務をいう。以下この条において同じ。）を行う者が行う特定認証業務が次の各号のいずれにも該当することとする。

一　特定認証業務の用に供する設備が総務省令で定める基準に適合するものであること。

二　特定認証業務における利用者（電子署名及び認証業務に関する法律第二条第二項に規定する利用者をいう。以下この号において同じ。）の真偽の確認が、当該利用者から通知された当該特定認証業務の利用の申込みに係る情報について行われた電子署名（法第二条第一項に規定する電子署名をいう。）が当該利用者から通知された当該利用者に係る電子証明書に記録された利用者署名検証符号（同条第二項に規定する利用者署名検証符号をいう。）に対応する利用者署名符号（同項に規定する利用者署名符号をいう。）を用いて行われたことを確認する方法により行われるものであること。

三　前号に掲げるもののほか、特定認証業務が総務省令で定める基準に適合する方法により行われるものであること。

# 総務大臣認定の基準（２）

## ○電子署名に係る地方公共団体の認証業務に関する法律施行規則

（特定認証業務の用に供する設備の基準）

第二十五条　令第八条第一号の総務省令で定める基準は、次に掲げるとおりとする。

一　法第十七条第一項の規定による総務大臣の認定を受けようとする者（以下「認定申請者」という。）が行う特定認証業務（電子署名及び認証業務に関する法律（平成十二年法律百二号）第二条第三項に規定する特定認証業務をいう。次条において同じ。）の用に供する設備のうち電子証明書（電子署名及び認証業務に関する法律施行規則（平成十三年総務省・法務省・経済産業省令第二号）第四条第一号に規定する電子証明書をいう。次条において同じ。）の作成又は管理に用いる電子計算機その他の設備（以下「認証業務用設備」という。）は、入出場を管理するために業務の重要度に応じて必要な措置が講じられている場所に設置されていること。

二　認証業務用設備は、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が講じられていること。

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

四　認証業務用設備のうち発行者署名符号（電子署名及び認証業務に関する法律施行規則第四条第四号に規定する発行者署名符号をいう。以下この号及び次条第十六号において同じ。）を作成し、又は管理する電子計算機は、当該発行者署名符号の漏えいを防止するために必要な機能を有する専用の電子計算機であること。

五　認証業務用設備及び第一号の措置を講じるために必要な装置は、停電、地震、火災及び水害その他の災害の被害を容易に受けないように業務の重要度に応じて必要な措置が講じられていること。

# 総務大臣認定の基準（３）

（特定認証業務におけるその他の業務の方法）

第二十六条　令第八条第三号の総務省令で定める基準は、次に掲げるとおりとする。

一　利用申込者（電子署名及び認証業務に関する法律施行規則第五条第一項に規定する利用申込者をいう。）に対し、書類の交付その他の適切な方法により、電子署名（電子署名及び認証業務に関する法律第二条第一項に規定する電子署名をいう。）の実施の方法及び認定申請者が行う特定認証業務の利用に関する重要な事項について説明を行うこと。

二　利用者署名符号（電子署名及び認証業務に関する法律施行規則第六条第三号に規定する利用者署名符号をいう。以下この号及び次号において同じ。）を認定申請者が作成する場合においては、当該利用者署名符号を安全かつ確実に利用者（電子署名及び認証業務に関する法律第二条第二項に規定する利用者をいう。以下この条において同じ。）に渡すことができる方法により交付し、又は送付し、かつ、当該利用者署名符号及びその複製を直ちに消去すること。

三　利用者署名符号を利用者が作成する場合において、当該利用者署名符号に対応する利用者署名検証符号（電子署名及び認証業務に関する法律施行規則第四条第一号に規定する利用者署名検証符号をいう。第五号において同じ。）を認定申請者が電気通信回線を通じて受信する方法によるときは、あらかじめ、利用者識別符号（同規則第六条第三号の二に規定する利用者識別符号をいう。）を安全かつ確実に当該利用者に渡すことができる方法により交付し、又は送付し、かつ、当該利用者の識別に用いるまでの間、当該利用者以外の者が知り得ないようにすること。

四　電子証明書の有効期間は、五年を超えないものであること。

五　電子証明書には、次の事項が記録されていること。

イ　当該電子証明書の発行者の名称及び発行番号

ロ　当該電子証明書の発行日及び有効期間の満了する日

ハ　当該電子証明書の利用者の氏名

ニ　当該電子証明書に係る利用者署名検証符号及び当該利用者署名検証符号に係るアルゴリズムの識別子

六　電子証明書には、その発行者を確認するための措置であって、電子署名及び認証業務に関する法律施行規則第二条の基準に適合するものが講じられていること。

七　認証業務に関し、利用者その他の者が認定申請者が行う特定認証業務と他の業務を誤認することを防止するための適切な措置を講じていること。

八　署名検証者（電子署名及び認証業務に関する法律施行規則第六条第九号に規定する署名検証者をいう。第十号において同じ。）が電子証明書の発行者を確認するために用いる符号その他必要な情報を容易に入手することができるようにすること。

# 総務大臣認定の基準（４）

九　電子証明書の有効期間内において、利用者から電子証明書の失効の請求があったとき又は電子証明書に記録された事項に事実と異なるものが発見されたときは、遅滞なく当該電子証明書の失効の年月日その他の失効に関する情報を電磁的方法（電子的方法、磁気的方法その他の人の知覚によっては認識することができない方法をいう。第十二号において同じ。）により記録すること。

十　電子証明書の有効期間内において、署名検証者からの求めに応じ自動的に送信する方法その他の方法により、署名検証者が前号の失効に関する情報を容易に確認することができるようにすること。

十一　第九号の規定により電子証明書の失効に関する情報を記録した場合においては、遅滞なく当該電子証明書の利用者にその旨を通知すること。

十二　認定申請者の連絡先、業務の提供条件その他の特定認証業務の実施に関する規程を適切に定め、当該規程を電磁的方法により記録し、利用者その他の者からの求めに応じ自動的に送信する方法その他の方法により、利用者その他の者が当該規程を容易に閲覧できるようにすること。

十三　電子証明書に利用者として記録されている者から、権利又は利益を侵害され、又は侵害されるおそれがあるとの申出があった場合においては、その求めに応じ、遅滞なく当該電子証明書に係る利用者に関する利用の申込みに係る情報（当該情報について行われた電子署名に係る電磁的記録を含む。）及び当該利用者から通知された当該利用者に係る電子証明書（これらに附帯する情報を含む。）を当該申出を行った者に開示すること。

十四　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。

イ　業務の手順

ロ　業務に従事する者の責任及び権限並びに指揮命令系統

ハ　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

ニ　業務の監査に関する事項

ホ　業務に係る技術に関し充分な知識及び経験を有する者の配置

ヘ　利用者の真偽の確認に際して知り得た情報の目的外利用の禁止及び業務に係る帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置

ト　危機管理に関する事項

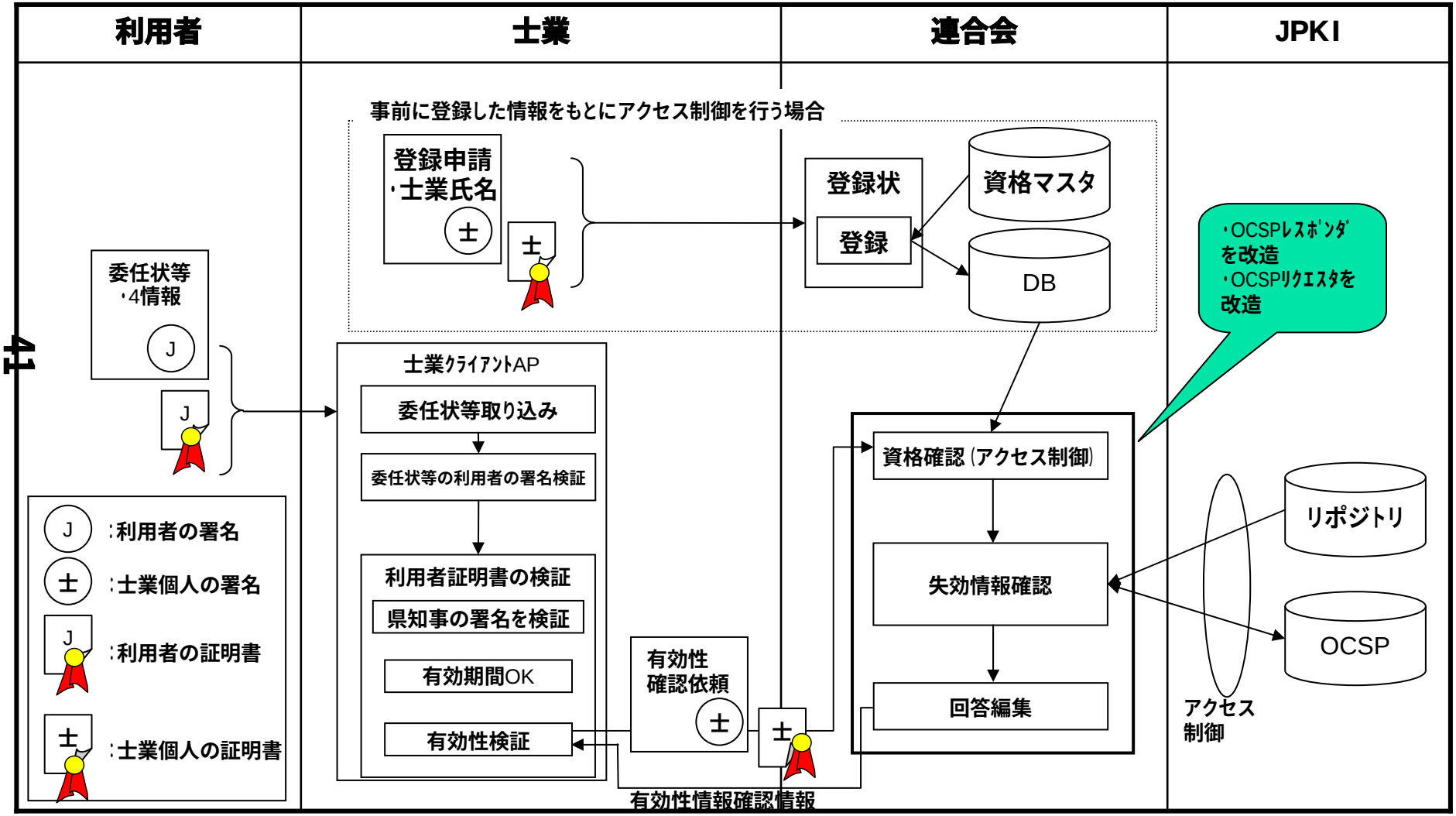
十五　認証業務用設備により行われる業務の重要度に応じて、当該認証業務用設備が設置された室への立入り及びその操作に関する許諾並びに当該許諾に係る識別符号の管理が適切に行われていること。

十六　複数の者による発行者署名符号の作成及び管理その他当該発行者署名符号の漏えいを防止するために必要な措置が講じられていること。

# シリアル番号通知による電子証明書有効性確認の検討
## (財団法人自治体衛星通信機構資料)

資料５

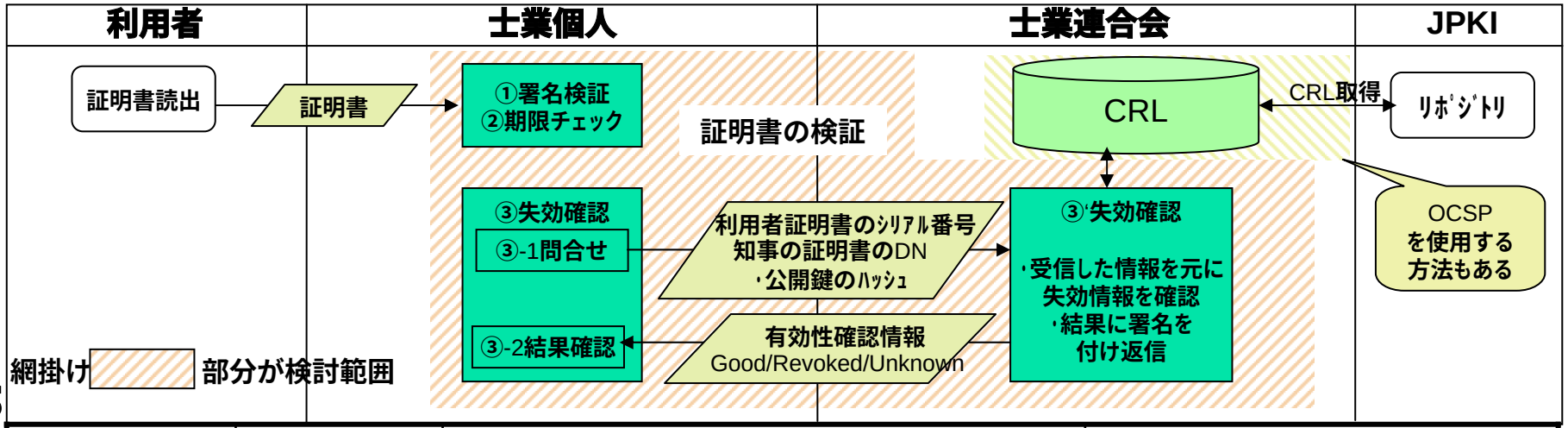
士業に対して有効性確認情報を提供する為に、士業連合会において有効性確認情報提供サービスを構築･提供する方式が考えられます。(下図)
JPKIにおいては、士業連合会を署名検証者として登録し、失効情報を提供します。



**検討の主旨：士業連合会へ個人情報を含む利用者の電子証明書を送らずに検証を行う方法はないか？**

**論点：士業連合会に対して電子証明書の有効性を確認する場合、電子証明書を通知するのではなくシリアル番号を通知するだけで問題ないのではないか？**

## 証明書検証の処理概要と要件




| 処理 | ソフトウェア | 処理内容 | 要件 |
|---|---|---|---|
| ①署名検証 | 士業ｸﾗｲｱﾝﾄAP | ・利用者からの申請書、委任状などに付与された利用者の電子署名検証<br>・利用者の証明書に付与された県知事の署名を県知事の自己署名証明書を用いて検証 | (a)県知事の自己署名証明書を入手する必要がある |
| ②期限チェック | 士業ｸﾗｲｱﾝﾄAP | 利用者の証明書に記載された有効期限の確認 | |
| ③-1問合せ | 士業ｸﾗｲｱﾝﾄAP | 適切な利用者の証明書からシリアル番号など必要項目を取り出しリクエスタ署名を付与し士業連合会へ送信 | (b)適切な利用者の証明書の判定<br>(c)必要な情報の取り出しとリクエスタ署名 |
| ③'失効確認 | OCSP相当 | ・受信した情報を元にCRLを確認<br>・結果に署名を付け返信 | (d)アクセス制御が必要<br>(e)失効事由の回答を実施しない場合は、改修要<br>(f)署名を付与するための秘密鍵が必要 |
| ③-2結果確認 | クライアントAP | ・士業連合会からの回答の検証<br>・回答の取り出し（表示） | (g)検証を行うための公開鍵が必要 |

## 要件とその課題

| 要件 | 課題 |
| --- | --- |
| (a)県知事の自己署名証明書を入手する必要がある | Ⅰ士業個人に県知事証明書の管理する負担をかけない<br>・士業個人が47都道府県知事の自己署名証明書の入手、及びその更新等の管理を行うことは負担となる。士業連合会からシステム的に送付する方式等の検討が必要 |
| (b)適切な利用者の証明書の判定 | Ⅱ任意のシリアル番号が送付できてはならない<br>・利用者証明書のｼﾘｱﾙ番号,知事の証明書のDN,公開鍵のﾊｯｼｭの組み合せは任意に作成することができるため(手元にない)不特定多数の証明書の検証が可能となる<br>Ⅲ行政手続を委任した利用者以外の証明書を送付できてはならない<br>・任意の証明書を検証することは代理申請、ひいては行政手続とは無関係な証明書の検証を許すことになる |
| (c)必要な情報の取り出しとリクエスタ署名が必要 | 技術的な検討のみ（システムの改修、開発で対応可能） |
| (d)アクセス制御が必要 | Ⅳ士業個人を識別する方策について検討が必要 |
| (e)失効事由の回答を実施しない場合は、改修要 | 士業連合会から士業個人への失効事由の提供の要否に応じた、技術的な検討のみ（システムの改修、開発で対応可能） |
| (f)署名を付与するための秘密鍵が必要 | Ⅴ士業連合会から士業個人への有効性確認情報の結果通知に正当性を担保するため、いずれかの認証局から証明書を発行してもらう必要がある。 |
| (g)検証を行うための公開鍵が必要 | 同上 |

## 課題と解決方策

- 課題Ⅰ士業個人に県知事証明書の管理する負担をかけない
  - 適切な県知事証明書を士業連合会から送付することで解決する

- 課題Ⅱ任意のシリアル番号が送付できてはならない

  **利用者証明書のｼﾘｱﾙ番号,知事の証明書のDN,公開鍵のﾊｯｼｭの組み合せは、任意に作成することができるため、この組み合せを無作為に送りつけることによって、士業個人側に有効性確認情報のDBを作成可能となる**
  - 問い合わせを行う前に利用者の証明書に付与された県知事証明書の署名検証が必須となるロジックを組むことで一定の対処が可能
    - プログラムによるガードのみのため悪意ある士業個人が存在した場合は、担保できなくなる恐れがある
    - 技術面では、一定の対処による限界があるため、制度面での抑止の検討が必要

      制度面での抑止は、法的な制限や罰則、士業連合会の規約などによる制限や罰則が想定される
- 課題III行政手続を委任した利用者以外の証明書を送付できてはならない

  **オンライン申請による行政手続等に必要な範囲に限定する必要がある**
  - 問い合わせを行う前に委任状及び申請書等に付与された利用者の署名検証が必須となるロジックを組むことで一定の対処が可能
    - プログラムによるガードのみのため悪意ある士業個人が存在した場合は、担保できなくなる恐れがある
    - 技術面では、一定の対処による限界があるため、制度面での抑止の検討が必要

      制度面での抑止は、法的な制限や罰則、士業連合会の規約などによる制限や罰則が想定される
- 課題Ⅳ士業個人を識別する方策について検討が必要
  - 士業を識別するCAが発行した証明書の検証
  - またはJPKI、民間CAが発行した証明書の情報を事前登録し突合

- 課題Ⅴ士業連合会から士業個人への有効性確認情報の結果通知に正当性を担保するため、いずれかの認証局から証明書を発行してもらう必要がある