基般

1. マイナンバーと電子署名・電子認証

手塚　悟（東京工科大学）

マイナンバーとは

2013 年 5 月 24 日, 第 183 回通常国会で成立した「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（以下「マイナンバー法」）」および関連法により導入されるのが，社会保障･税番号制度（以下「マイナンバー制度」）である．このマイナンバー制度とは，複数の機関に存在している個人や企業の情報を，同一人や同一企業の情報であることを特定し連携するための基盤であり，国民一人ひとりには 12 桁の個人番号，企業等には 13 桁の法人番号が割り当てられる．

そのねらいは，社会保障・税・災害対策の各分野において，効率性・透明性を高め，国民にとって利便性の高い公平・公正な社会を実現することにある．

これまでは，このような基盤がなかったため，所得を十分に捕捉することができず，不当に負担を免れたり，給付を不正に受け取ったりする人がいても特定が困難であった．今後は所得の正確な捕捉が可能となり細やかで公平な社会保障制度の運用が可能になる．さらにまた，社会保障・税にかかわる行政手続の添付書類の削減や，行政からのプッシュ型サービス，大災害時における被災者に対する積極的な支援など，国民の利便性向上と行政機関の業務効率化も実現できる．

マイナンバーの生成および通知は，2014 年 4 月に設立された地方公共団体情報システム機構が担う．2015 年 10 月から，個人番号が記載された「通知カード」が世帯単位に簡易書留で郵送される．電子署名・電子認証に用いることができる IC カード「個人番号カード」は，同封される申請書で申し込めば無料で交付される．

マイナンバーは原則として生涯不変であり，各人はマイナンバーを大切に管理する必要がある．マイナンバーの利用が始まると，税の納付や健康保険，年金保険，介護保険などの手続きの際に，マイナンバーの記入が求められる．マイナンバーは，マイナンバー法によって利用できる事務が規定されており，法律の定める事務以外での利用，さらにはマイナンバーの提供を求める行為は罰則付きで禁止されている．ただし自治体は，マイナンバーの利用事務を条例により独自に定めることもできる．

マイナンバー法では，マイナンバーに関連付けられた個人情報を「特定個人情報」と呼んでいる．マイナンバー制度の大きな特徴は，行政機関などが保有する特定個人情報を組織間で電子的に取得する仕組みが整備されることである．つまり，複数の機関にまたがった特定個人情報が紐付けられるようになる．

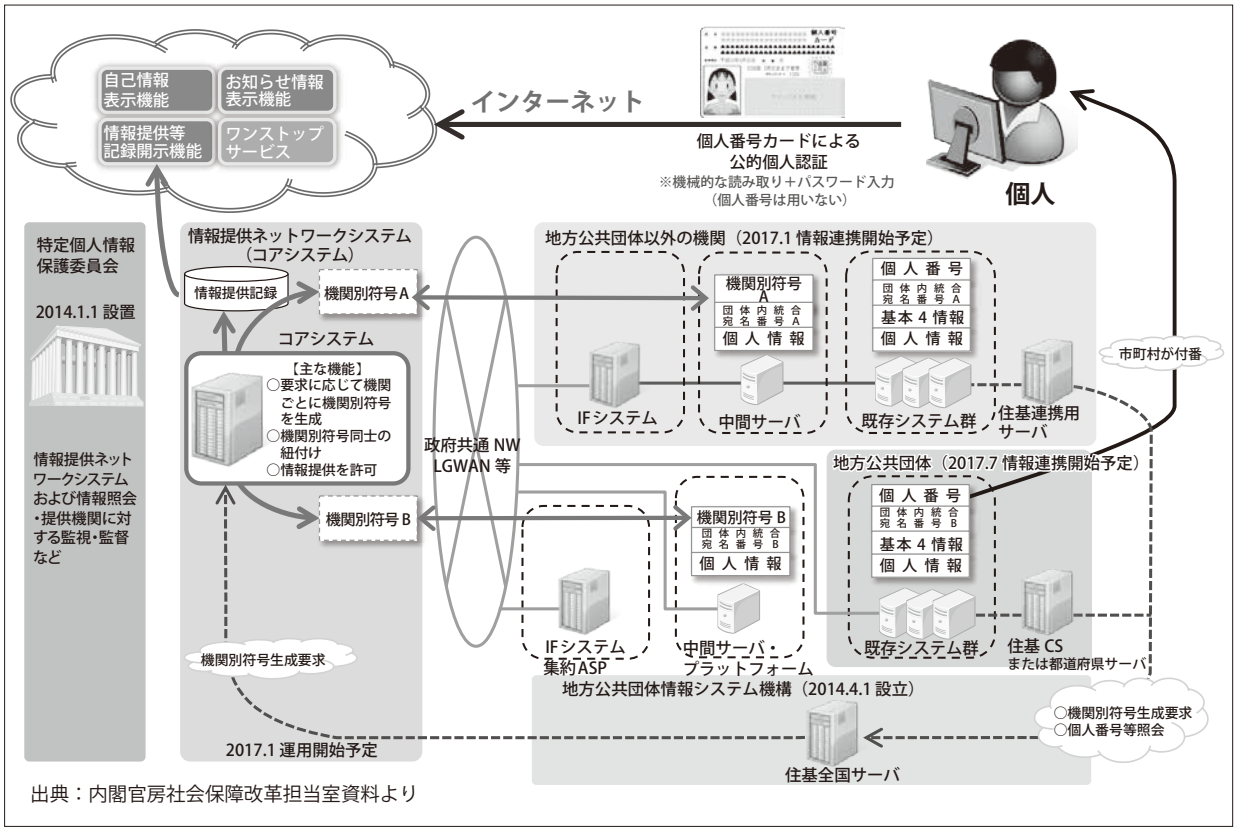
図 -1 は，マイナンバー制度における情報連携の概要を示したものである．異なる機関が保有する特定個人情報を連携させる際には，情報連携のための専用システムである「情報提供ネットワークシステム」を利用する．

同システムで情報を連携させるときは，マイナンバーを直接利用するのではなく，情報連携のための個人識別子である「機関別符号」を用いる．この機関別符号は，同じ個人に対しても，情報保有機関が異なれば異なる値が割り当てられている．つまり，同一人物の場合，マイナンバーはどこの機関でも同じだが，機関別符号はその名称の通り機関によって異なっている．各機関で使われる機関別符号は，情報提供ネットワークシステムが住民票コードを基に生成する．技術的な詳細は省略するが，複数の機関にまたがって個人情報を紐付けられるのは，情報提供ネットワークシステムだけである．

電子署名・電子認証とは

電子署名と電子認証の違い

我が国において一般的に使われている電子署名の制



出典：内閣官房社会保障改革担当室資料より

図 -1　マイナンバー制度における情報連携の概要

度は，民間分野では「電子署名法」，公的分野では「公的個人認証法」がある．

「電子署名法」は，正式には「電子署名及び認証業務に関する法律」と呼ばれ，2001 年 4 月 1 日に施行された．電子署名法の概要は，電磁的記録の真正な成立の推定と特定認証業務の認定である．

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

特定認証業務の認定とは，電子署名法第二条三項で，「『特定認証業務』とは，電子署名のうち，その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう」と規定された特定認証業務に対して，第四条で，「特定認証業務を行おうとする者は，主務大臣の認定を受けることができる」と規定されている．

一方，「公的個人認証法」は，2004 年 1 月 29 日に開始され，「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」）に基づくものである．

第一章第一条に，「この法律は，電子署名に係る地方公共団体の認証業務に関する制度その他必要な事項を定めることにより，電磁的方式による申請，届出その他の手続における電子署名の円滑な利用の促進を図り，もって住民の利便性の向上並びに国及び地方公共団体の行政運営の簡素化及び効率化に資することを目的とする」と目的が書かれており，いわゆる電子政府，電子自治体等において，電子申請，電子申告等を行うときに使用するものである．

上記の「電子署名法」と「公的個人認証法」は，いずれも電子署名に関する法律で，技術的には，PKI（Public Key Infrastructure）システムを構築し実現している．「公的個人認証法」では「署名」ではなく「認証」という言葉が使われているが，ここでの「認証」とは何のことなのか，それを明確に理解することが必要で

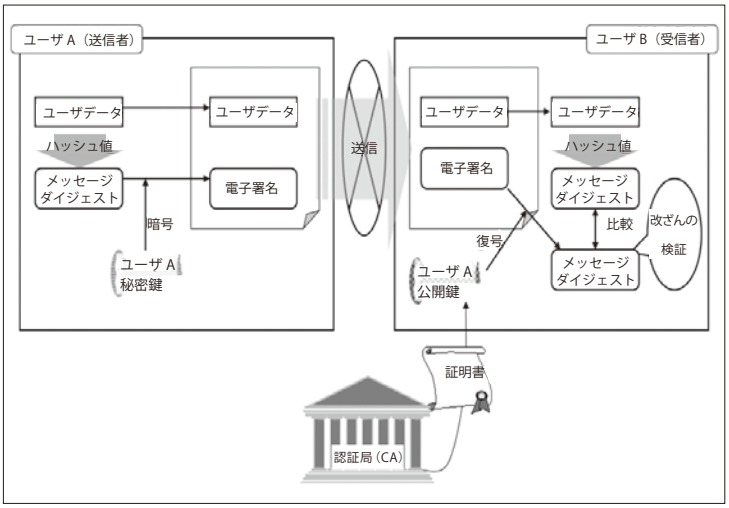


図 -2　電子署名技術のメカニズム

ある.

日本語の「認証」にあたる言葉は，英語では「Certification」と「Authentication」がある.「公的個人認証法」の「認証」はどちらであるかというと,「Certification」である. つまり, PKI システムにおいて，本人の公開鍵に対して,「公的個人認証法」が「お墨付きを与える(Certify)」ことを,「認証」と呼んでいるのである.「電子署名法」においても, PKI システムで，本人の公開鍵に「お墨付きを与える (Certify)」機関を「認証局」と呼び，英語では「Certificate Authority (CA)」と記述する.

では「Authentication」とは何であるかというと，End Entity である人が正当な本人であるかどうかの確認をする方法のことで，この場合も日本語では「認証」と呼ぶ. 英語でいう「Electronic Authentication」は，電子的に本人確認を行う方法で，日本語でいう「電子認証」に対応するものである.

つまり,「Certification」は，認証局のような Trusted Third Party (TTP) が本人であることの「お墨付きを与える(Certify)」ことである.「Authentication」は，そのお墨付きを与えられた本人が，その後ある電子商取引のシステムにアクセスする場合，本当にお墨付きを与えられた本人であるかをシステムが確認することである. それによって，確かにお墨付きを与えられた本人であるならば，アクセスを許可することになる. このように,「Certification」と「Authentication」の概念とその違いをしっかりと理解することは大変重要で，それにより日本語の「認証」という言葉の曖昧さを払拭することができるのである.

今年 (2015 年) 成立した「マイナンバー法」においては，国民一人ひとりが自分の「マイナポータル (従来の「マイ･ポータル」から改称)」へアクセスするために,「電子認証」を採用した. 従来の「公的個人認証法」は「電子署名」のみを制度化していたが，今回は「公的個人認証法」の一部を改正し,「電子認証」も新たに制度化された.

一方,「電子署名法」においては,「電子認証」の概念をどう捉えればよいのかを考えてみると，まず「署名」の概念は「自然人」が行う行為であると考えられているので,「認証」の概念をどのように入れるかについては，議論の余地がある. 1 つの方法としては,「公的個人認証法」の一部改正と同様に電子署名法の一部改正を行うやり方がある. また別の方法としては，銀行口座開設や携帯電話購入時における本人確認方法を基にして，その拡張としての電子的本人確認方法を制度化することで,「電子認証」を実現するやり方が考えられる. いずれにしても，今後の検討が望まれるところである.

電子署名技術

2001 年に「電子署名および認証業務に関する法律(以下「電子署名法」)」が成立し，電子署名に対して手書き署名や実印等と同等の法的効力が保証されるようになった.

ここでは，電子署名技術とはどのようなものであるかを簡単に解説する. **図 -2** は，電子署名技術のメカニズムを示したものである. 送信者から受信者にメールの文章を転送するときに，そのメールの文書に電子署名を付して送り，その電子署名の検証により本当にその人から送られてきたものかということと，その送られてきたメールの文章が間違いないかということを検証する仕掛けを示したものである.

そのメカニズムは次のとおりである. まずユーザ A(送信者) がユーザ B (受信者) にユーザデータを送る場合，ユーザ A は，送ろうとしたユーザデータが確かに自分

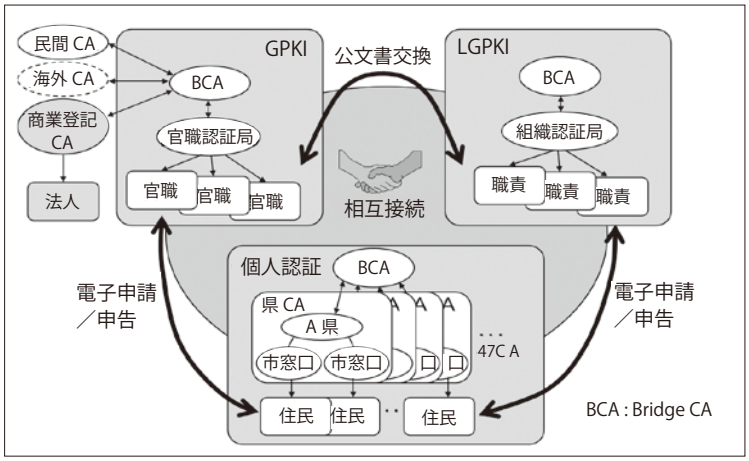


図 -3　電子政府における電子認証基盤の概要

認証基盤名	発行者		利用者		法律	用途
GPKI	官	各府省	官	政府官職		G / G, B, C
LGPKI		都道府県認定局		地方官職		G / G, B, C
法務省商業登記		法務省	民	法人代表者	○	B / G, B, C
公的個人認証サービス (JPKI)		都道府県知事		住民	○	C / G
HPKI		厚生労働省から認定を受けた HPKI 認証局		医療従事者		B / B, C
特定認証局	民	民間事業者		自然人	○	C / G, B, C
その他の認証局		民間事業者等		人，物，アドレス　ほか		B, C / B, C

G : 公共機関　B : 民間企業　C : 国民

表 -1　我が国における電子認証基盤

の書いたものであるという保証をするために電子署名を付す.

それによって，ユーザ B 側では確かにそれがユーザ A の送ってきたユーザデータであるということと，そのユーザデータの中身が確かにユーザ A の書いたものに相違ないということを検証できる.

具体的には，まずユーザ A 側では，ユーザデータにハッシュ関数を使ってハッシュ値を出し（これをメッセージダイジェストと呼ぶ），これをユーザ A の秘密鍵で暗号化する．この部分が電子署名に相当し，これをユーザデータとペアにしてユーザ B に送り届ける.

一方ユーザ B は，受け取ったユーザデータと電子署名に対して次のことを行う．まずユーザデータについてはユーザ A の側で行った処理とまったく同じ処理を行い，ユーザデータからハッシュ関数によりメッセージダイジェストを導き出す．一方，電子署名の部分に対しては，ユーザ A の公開鍵で復号し，メッセージダイジェストを取り出す.

この 2 つのメッセージダイジェストを比較することによって，改ざんとなりすましの 2 つの点についてチェックができる.

それらが一致していれば，送信者のなりすましがないこと，そして送信者のユーザデータに対する改ざんが行われていないことが保証できる.

電子認証基盤とは

我が国における電子認証基盤

我が国において，電子署名・電子認証技術を使った安心安全な基盤を構築するための電子認証基盤の現状に関して解説する.

図 -3, **表 -1** は，電子政府の電子認証基盤の概要と我が国における電子認証基盤を示したものである．この基盤は，2000 年ごろの電子政府・電子自治体を始めた時期に整備されたものである．マイナンバー制度でもこの電子認証基盤を活用する.

以下では，それぞれの電子認証基盤を解説する.

(1) 政府認証基盤 (GPKI)

政府認証基盤 (GPKI：Government Public Key Infrastructure) は，行政機関側の認証局である「ブリッジ認証局」と「官職認証局」で構成される.

GPKI と地方公共団体組織認証基盤 (LGPKI：Local Government Public Key Infrastructure)，公的個人認証サービス共通基盤 (JPKI：Japanese Public Key Infrastructure) などの電子認証基盤が相互認証を行うことで，行政機関の処分権者と申請者間の各種手続きをインターネット上で行える仕組みが実現する.

(2) 地方公共団体組織認証基盤 (LGPKI)

地方公共団体組織認証基盤 (LGPKI：Local Government Public Key Infrastructure) は，「組織認証局」「アプリケーション認証局」「ブリッジ認証局」で構成される．これによって，地方公共団体が住民・企業などの各種申請や届け出等の手続きや地方公共団体間の文書のやりとりにおいて，盗聴や改ざん，なり

すまし，否認を防止し，送受信される電子文書の真正性を担保する.

⑶ 公的個人認証サービス共通基盤（JPKI）

公的個人認証サービス共通基盤（JPKI：Japanese Public Key Infrastructure）は，「都道府県認証局」と「ブリッジ認証局」で構成される.

⑷ 保健医療福祉分野の公開鍵基盤（HPKI）

保険医療福祉分野の公開鍵基盤（HPKI：Healthcare Public Key Infrastructure）とは，医療従事者が，保険医療福祉分野の国家資格（医師・看護師・薬剤師など）の所持情報を格納した電子証明書を用いて，インターネットで各医療機関の医療情報システムにアクセスすることを可能とするための仕組みである.

⑸ 商業登記に基づく電子認証

商業登記に基づく電子認証とは，会社の代表者の電子証明書を用いて署名と認証を行う仕組みである．電子証明書を利用した身分の公的な証明は，国民や政府職員といった自然人だけでなく，企業の取締役を対象にしている.

⑹ 認定認証事業者（認定認証局）

数ある認証局の中で，電子署名法の主務三省から特定認証業務の認定を受けている民間企業は，「認定認証事業者」といい，一般的には「認定認証局」と呼ばれている．認定認証局は特定認証業務，つまり電子証明書の発行と管理を行う.

欧州における電子認証基盤

2014 年 8 月, EU（欧州連合）で「eIDAS 規則」が発効した. eIDAS は「electronic IDentification and Authentication Signature services」の略で，日本語に訳すと「電子識別・認証・署名サービス」となる．一言で表現すると，市民や企業が紙媒体での環境と同じように，オンライン上で経済活動に取り組めたり，行政サービスを受けられたりするように，安心・安全にかかわる保証を与える法律である.

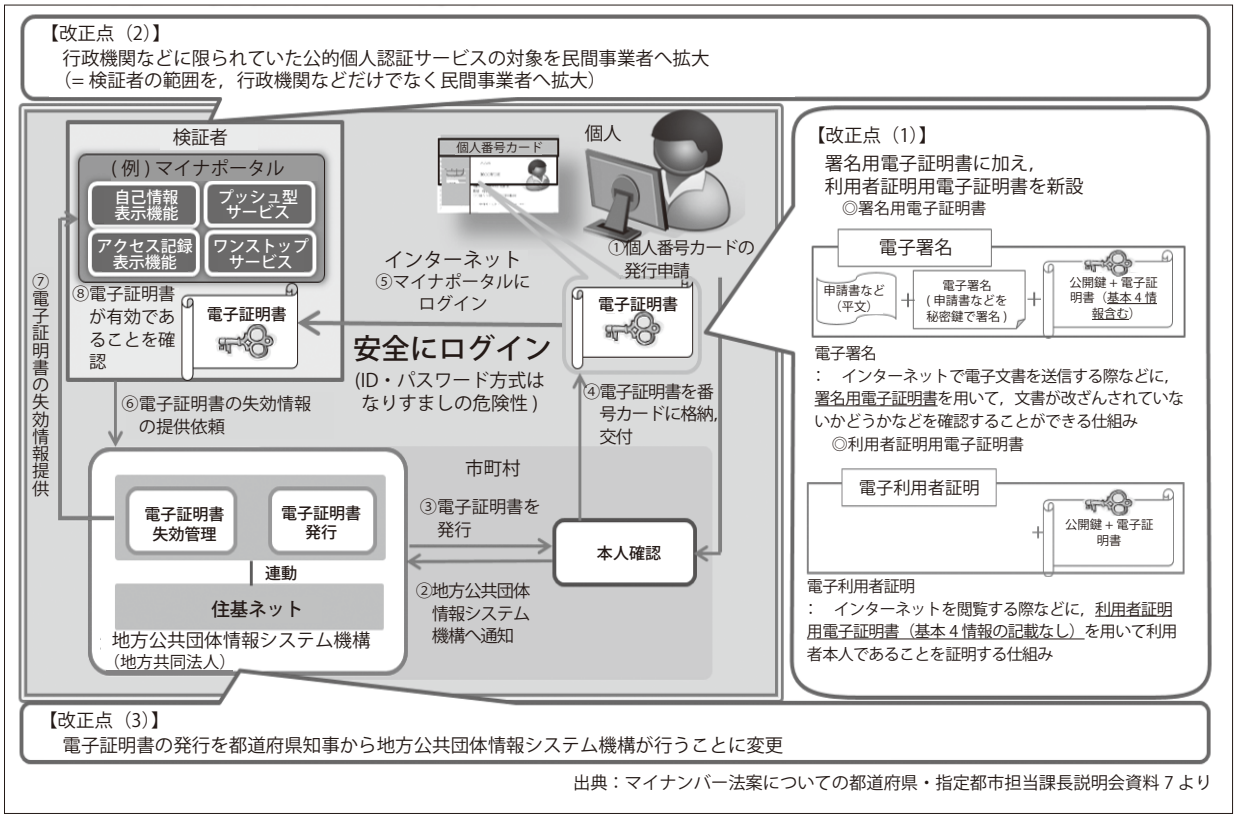
eIDAS 規則は, 1999 年に EU 域内のセキュアな電子取引の促進を目的に発効された「電子署名指令」に代わるものであり, EU 加盟各国の電子署名法を上書きするものである.

電子署名指令と eIDAS 規則では，その法形態の違いによって法的効力に大きな差がある.「指令」とは，ある特定の目的の達成のために，加盟国が国内法を整備するものであり，これまでは電子署名指令に沿った国内法が加盟国で定義されていた．しかし，今回の eIDAS 規則では，より強制力の強い「規則」という法形態をとっており，すべての加盟国に EU 全体の新しい法律として適用される．また，電子署名指令では言及されていなかった「タイムスタンプ」や「e- シール」といった電子署名以外のトラストサービス（安心と信頼を強化するサービス）が新たに定義された点も同指令との違いである．さらに, eID（オンラインで本人確認を実現できる ID）のオンライン認証結果の加盟国間の相互承認までを含んでいる．これらによって，電子署名指令では実現しきれなかった, EU 域内での電子署名の相互運用および，その他のトラストサービスの相互運用を実現し，電子取引を活性化するとともに，国境を越えて市民の権利の保証を促すことがねらいである.

電子署名やタイムスタンプなどのトラストサービスは，オンライン上での電子取引に対して，紙の文書による取引と同等の信頼性を確立するのに必要不可欠である. eIDAS 規則に基づいて EU 域内で共通のトラストサービスに関する法的枠組みが整備されることによって，従来よりも円滑な電子取引が促進されることになる．日本でも 2015 年 10 月からマイナンバー法が施行され，国民一人ひとりが識別番号を持つ時代を迎えるが，EU ではすでに多くの加盟国が国民 ID カードを発行しており，その ID カードの eID 機能を使ったオンライン個人認証まで実用化が進んでいる．このオンライン個人認証結果を EU 域内で相互に受け入れることにより，市民（学生等）はたとえば，他加盟国の大学への入学申請をオンラインで容易に処理できるようになる.

マイナンバー制度における電子認証技術の活用

個人番号カードが，これまでの住基カードと大きく異なる点が 3 点ある. **図 -4** は，電子認証技術を活用したマイナポータルへのログイン認証を示したものである.



出典：マイナンバー法案についての都道府県・指定都市担当課長説明会資料７より

図 -4　電子認証技術を活用したマイナポータルへのログイン認証

1 点目は，公的個人認証法の一部改正により，これまでの「署名用電子証明書」に加えて，マイナポータルへのログイン認証のために使用する「利用者証明用電子証明書」が新たに搭載されることである．これまでの「署名用電子証明書」は，e-Tax などの電子署名として利用されていた．電子証明書には個人の基本 4 情報が含まれている．一方，今回新設された「利用者証明用電子証明書」は，マイナポータルのログインなど本人確認のための電子認証の手段として利用される．電子証明書には，個人情報である基本 4 情報は含まれていない．

2 点目は，これまで行政機関に限定されていた電子署名の検証者が民間事業者にも拡大されたことである．公的個人認証法の一部改正によって，2017 年 1 月からは民間事業者も総務大臣の認可を受けることで，個人番号カードに格納された電子証明書によって作成された署名の検証者となることができる．

「署名の検証者」は，署名用電子証明書による電子署名だけでなく，新たに利用可能となる利用者証明用電子証明書による電子利用者証明についても検証を行うことができる．署名用電子証明書および利用者証明用電子証明書の有効性は，地方公共団体情報システム機構に問い合わせて確認する．総務大臣の認可を受ければ，民間事業者も個人番号カードの電子証明書を利用して，オンラインでの本人認証サービスを提供できるようになる．たとえば，インターネットバンキングやネット通販の利用者認証に利用できる．民間事業者のメリットとしては，これまでの ID ／パスワード方式に代わって，より強固な本人確認が行えるようになることが挙げられる．

3 点目は，冒頭に述べたマイナンバー法と共に成立した「地方公共団体システム機構法」により，従来は都道府県知事が行っていた電子証明書の発行を，地方 公共団体情報システム機構が行うことに変更したことである．

以上により，マイナンバー制度の安心・安全を確保することができる．

（2015 年 8 月 13 日受付）

手塚　悟（正会員）■ tezuka@stf.teu.ac.jp

東京工科大学教授．1984 年慶應義塾大学工学部数理工学科卒業．同年日立製作所入社．2009 年から現職．情報ネットワーク法学会理事長．特定個人情報保護委員会委員．博士（工学）．