電子公証制度の現状と問題点

木　村　哲　也*

公証制度を研究するにあたっては、従来からの紙ベースの公証制度とは別に、あらたに導入された電子公証についても目を向けなければならない。とはいえ、電子公証についての法的問題点の考察は、法律家の共通認識になっている部分が少なく、制度・システムの内容さえ理解しづらい部分が多い。あらたに導入された公的電子公証制度の基本的な内容を紹介したうえで、現時点で想定できる法的問題のありかを呈示する。

第１　公的電子公証制度の創設

平成12年４月11日、商業登記法等の一部を改正する法律が成立し、同年４月19日に公布された（平成12年法律第40号）。具体的には、商業登記法、公証人法、民法施行法の一部改正が行われ、「商業登記制度に基礎を置く電子認証」及び「公証人制度に基礎を置く電子公証」等の制度が創設された。上記の改正法のうち、公証人制度の一内容となる「公証人制度に基礎をよる電子公証制度」を概観する。

１　公証人による電子公証制度の概要

１）現在、実際に稼働している電子公証サービスの具体的内容は、①定款の認証、②電子私署証書の認証、③電子確定日付の付与、④同一性の証明・同一情報の取得である。いずれについても、制度がスタートした当初は、法人だけしか利用することができないものであったが、2004年（平成16年）３月１日からは、個人でも利用することが可能となった。

①　定款の認証

会社設立の際に作成を要求される定款を、紙ベースではなく、電子文書として作成し、これに公証人が認証を与えるというものである。印紙税の納付が不要となり、少なくともこの点において電子化のメリットが認められる。

②　電子私署証書の認証

従来の紙ベースで作成される私署証書の認証と同様に、電子化した文書にも公証人の認証を施すというものである。二通りの作成方法があり、ａ　指定公証人（後述）に対し、電子

編集部注*　関西大学法務研究科教授（法学研究所公証制度研究班研究員）本稿は、2005年７月23日開催法学研究所第45回総合研究会の報告原稿に加筆修正したものである。

署名をしたことを自認した場合と、b 指定公証人の面前で、電磁的記録に記録された情報に、電子署名をした場合である（公証人法第62条の６）

③ 電子確定日付の付与

従来の確定日付の付与の制度を電子文書にも施すというものである。指定公証人が、電磁的記録として記録された情報に日付情報を電子的に付する。この措置を施せば確定日付のある証書とみなされる（民法施行法第５条２項）。

④ 情報の保存及び内容の証明

認証を受けた私署証書または日付情報が付せられた電磁的記録の a 同一性の証明を行い、さらに、b 電磁的記録の保存・複製情報の提供を受けることができる（公証人法第62条の７）。

2） 取り扱っているサービスは上記のものに限定され、従来の公証人によるサービスのすべてが電子化されたわけではない。

従来から紙ベースで公証人が作成してきた金銭消費貸借公正証書や公正証書遺言等の証書の電子版とでもいうべき、電子公正証書については、いまだ制度化されていない。その理由は、次のように説明されている。① 公正証書の作成過程において、当事者の意思決定が慎重に行われなければならないが、電子的方法では当事者の意思確認が容易にはできない。② 仮に公正証書だけ執行証書を電子的に作成できたとしても、民事執行手続において、これが電子的に利用できなければ意味がない。③ 現時点での需要が見込めない[1)]。

確かに、制度として存在しないからであるともいえるが、特にそのようなものをどうしても作成したいという要望をあまり聞かない。近年ようやく、一般の人々の間に遺言を作成しておくのがよいという意識が浸透し、公正証書遺言の作成件数が飛躍的に伸びていているようではあるが、これを電子化することの必要性を感じている人は、皆無といっていいのではないかと思われる。作成の段階、保存、執行という局面ごとに分析してみる必要があるが、現時点で電子化するメリットは何かと問われても、紙ベースで保存することによるスペースの節約といった程度のことしか考えられない。印紙税の節約はまさに徴税側の政策によって決まることであり、そのメリットは確実に保障されたものとはいえない。執行の段階では、電子化と結びつける制度はないし、作成の段階においても、紙ではなくデジタル情報として記録することが作成者の意思確認をより確実にする手段であるともいえない。従来の公証人の仕事がそっくり電子化され、これがために、従来と比較してサービスの効率化や確実性、安全性が確保されるといえるようになるのは、まだまだ遠い先のことのように思われる。

2 運営主体・技術的基盤

1）運営体制

上記サービスは、全国の公証人会及び公証人をもって組織する日本公証人連合会が運営主体

1）小川秀樹「電子公証制度の創設について」自由と正義2000年８月号 日弁連発行 52頁注(4)

となっているが、運用技術については、民間に業務委託するという形態になっている[2)]。なお、全国すべての公証人ではなく、「指定公証人」として、法務大臣から指定された公証人だけが携わることになっているが、年々その数が増え、現時点では、全国55役場、85名が指定公証人になっている[3)]。

2）技術的基盤

従来、ワープロやパソコンは、紙に印字して使用する文書を作成する道具であり、印字前の状態は文書作成の途中経過でしかなかった。その状態のまま文書として通用するとは考えられなかった。それは、印字前のワープロやパソコンの文書、正確にはテキストファイルやワープロ文書ファイルは、いつでも容易に痕跡なく改変でき、固定化できるものではなかったからである。紙ベースの文書は、インクで書かれ、容易に消すことはできず、もし、訂正するのであれば、作成名義下に押印するのと同じ印を訂正箇所に押印するなどの一定の形式を踏むことになっている。内容が改変されていないという点では、電子情報よりも紙ベースの文書の方がはるかに信頼できるものであった。この情報の固定化と同一性の確認が紙の文書と同じように信頼できる技術なくして、電子文書の公証サービスはなしえないことだったのである。この問題を乗り越えることができたのは、意外にも暗号技術であった。この点については、さらに、次の「電子署名・電子認証」ところで述べることとする。

第2　電子署名・電子認証

公証人による電子公証制度は、それ以前から民間においてサービスが提供されている電子認証制度の技術的基盤や平成12年に制定された「電子署名及び認証業務に関する法律」（電子署名法）の規定の適用を受ける電子署名をもとにシステムが構築されている。電子公証を考察するには、電子署名の仕組みと電子署名法の理解が前提となるので、以下必要な範囲で概要を説明する。

1　電子署名の仕組み

電子公証の前提となる電子署名の仕組みは、暗号技術がもとになっている。本来の暗号は、一般人が読んで理解できるメッセージを、秘密のルールにしたがって一般人には読めないように改変して伝達し、秘密のルールを知っている者だけが元のメッセージの内容を知ることができるという技術である。暗号技術は、通信の秘密を保持するために発明され、発展してきた。今でもその役割は非常に大きい。電子取引において、クレジット番号や口座番号などの決済に関する重要な情報の伝達に利用されている。

ところで、デジタル情報に暗号を施す方法には、現在、二通りの方法があるとされる。ひとつは「共通鍵暗号システム」と呼ばれる方式であり、もうひとつは「公開鍵暗号方式」よばれる方

2）日本認証サービス株式会社の電子署名に関する電子証明書等を利用することになっている。

3）日本公証人連合会ホームページ「電子公証制度のご案内」http://www.koshonin.gr.jp/de.html

式である。

前者は、暗号化と復号に共通の内容の鍵を用いるシステム（あたかも、複数人が同じ形の部屋の鍵をコピーして持っているのと同じ）であり、この原理は、デジタルデータというものが世に出現する以前から行われていた暗号方式である。例えば､暗号化される元のメッセージを平文(ひらぶん）というが、仮に「あすこい」という平文のメッセージを伝えたいときに、これを「うそしえ」という文字の並びに変換する。これを受け取った者が、事前に暗号化のルールを知らされていれば、元の平文のメッセージに複合することができる。この場合の暗号化のルールは、「平文の各文字を50音順で２文字後ろにずらして暗号にする」ということがすぐにわかる。2001年宇宙の旅に登場するＨＡＬ9000というコンピュータの名称は、コンピュータメーカーＩＢＭのアルファベットの順番を一つずつ前にずらしたのではないかという話と同じ発想である。この場合は、暗号化のルールは、同時に復号のルールでもあり、共通鍵暗号方式であると理解される。このルールを複雑化すれば、一定程度の秘密保持の機能が得られるのである。

ただし、この方式だと、インターネットの世界でこれを利用できる場合がおのずから限定される。もし、ＡがＢに暗号をかけたメッセージを送信したいときに、暗号化した鍵もインターネットを通じて送信すると、暗号化したメッセージと鍵の両方を他人に盗られる可能性がある（実際にはこっそりコピーされるだけで盗られたことがわからない)。そうすると、すぐに他人に解読されてしまう。それを防ぐためには、鍵だけは別の方法で送るしかないが、そもそも別の方法で鍵を送れるのだったら、本文もインターネットを使わずに別の方法で送ればよいということになる。あらかじめ鍵を別の方法で送っておき、あとはインターネットを通じて頻繁にメッセージをやりとりするというような者の間でしか機能しない。１回きりのメールのやりとりに使うという場合には、ほとんど意味がないことになる。

そこで開発されたのが「公開鍵暗号方式」である。これは、高等数学を応用したもので、比喩的にいうならば、相関する一対の鍵（暗号化する鍵と復号する鍵は別の形をしており、片方の鍵を見ても、対になっているもう片方の鍵の形はわからない）を作り、片方を秘密にし、もう片方を公開する（ことさらに公開するという意味ではなく、誰に知られてもさしつかえないというくらいの意味）システムである。この方式だと、インターネットの世界において、次のようにして使うことができる。Ｂは、Ａから暗号化したメッセージを送りたいという申し出を受けると、Ｂの手元で一対の鍵を作成し、暗号化する鍵（公開鍵）をインターネットを通じてＡに送りつける。Ａは、Ｂに送信したいメッセージをＢから受け取った鍵を使って暗号化し、インターネットを通じて発信する。Ａからのメッセージを受け取ったＢは、自分の手元に残しておいた秘密鍵である復号鍵を使って解読する。もし、第三者が、ＢからＡに発信した鍵を手に入れたうえで（こっそりコピーをするのでＡＢにはそのことがわからない)、Ａから発信したメッセージを手に入れても、手に入れた鍵は暗号化する鍵であって、復号する鍵の形はわからないのであるから復号はできないということになる。

ここまでは、暗号を使って秘密を保持するという説明であるが、この公開鍵暗号方式を応用すれば、認証システムに利用することができる。秘密保持のやり方を逆に利用するのである。Ａが

手元で一対の鍵を作成し、復号する鍵をＢ宛に送信する。そして、手元に残しておく秘密鍵を使ってメッセージを暗号化し、そのメッセージをＢに発信する。Ｂにおいて、届いたメッセージがＡから送られてきた鍵（公開鍵）を使って復号できるとすれば、まさしくＡ作成によるメッセージであり、他人がＡになりすまして送りつけてきたものではないと信頼できる。第三者で信頼できる認証機関がＡの委託を受けてＡの公開鍵を預かり、Ａの公開鍵であることを証明するシステムにすれば、Ｂの信頼はさらに厚くなる。紙ベースにおける印鑑証明のシステムと同様のものとなる。このようにして、誰の作成によるものであるかということの確認が、上記の暗号技術の応用によって可能となるのである。

さらに、デジタル情報の内容が、後に変更されたものではないということが確認される必要がある。電子署名（デジタル署名）の技術も暗号技術が応用されたものである。通常は、いつでもすぐに痕跡なく改変できるテキストデータを、ハッシュ関数（データを圧縮する関数であるが、圧縮されたデータを復元することが極めて困難な関数。一方向性ないし不可逆性を有する。）を使って圧縮し、元のテキストデータとあわせて保管する。もし、あるテキストデータがオリジナルか否かについての疑いが生じたときには、当該テキストデータを同じハッシュ関数を使って圧縮し、当初に作成された本来のテキストデータの圧縮データと比較すれば、改ざんの有無を発見することができる。二つのデータが同じであれば改ざんがなく、異なる場合には改ざんがあったことになる。紙媒体ではなく、コンピュータによって処理されるデジタル情報であるがゆえになしうる技である。

暗号技術を基盤とした電子署名、電子公証の基本的なシステムを、単純化した概念で説明したが、実務では、これらの暗号技術を組み合わせて、秘密保持、認証、同一性確認の機能を同時に果たすようにし、かつ、ユーザーが意識しないうちに自動的に実行されるように仕組んでいる。

2　電子署名法と認証機関

電子署名を法律の側面から考察する場合、電子署名法の基本的理解が不可欠である。

第１条には、同法の目的が規定されている。

電子署名に関し、

１　電子署名の効力としての電磁的記録の真正な成立の推定、

２　特定認証業務に関する認定の制度、

３　その他必要事項

を定めることにより、

電子署名の円滑な利用の確保による

イ、情報の電磁的方式による流通

ロ、情報処理の促進

を図り、もって、国民生活の向上及び国民経済の健全な発展に寄与することであるとしている。

条文から明らかなように、電子署名法の究極の目的は、「国民生活の向上及び国民経済の健全な発展」にある。その目的達成のために、電子署名の円滑な利用の確保による、イ 情報の電磁

的方式による流通、ロ 情報処理の促進を図るのであるが、電子署名法は、その手段として、1 電子署名の効力としての電磁的記録の真正な成立の推定、2 特定認証業務に関する認定の制度、3 その他必要事項を定めるというのである。

第2条では、1 電子署名、2 認証業務、3 特定認証業務が定義されている。

「電子署名」は、次の二つの要件を備える電磁的記録に施される「措置」であるとされる。電子署名にあたるか否かは、次の二つの目的、機能を有する措置であるか否かによって決せられる。一つめは、当該電磁的記録を作成した者を特定するものであること、二つめは、当該措置（つまり、電子署名）を行った後は、その電磁的記録が書き換えられていないかどうかを判別することできるということである。電子署名は、暗号技術を利用して行われるが、情報内容を他に漏れないようにするだけであれば、以上のいずれの措置にも該当しないから電子署名ではないことになる。なお、現時点において実際に利用されている電子署名は、先に述べた公開鍵暗号方式によるものであるが、法律上は、技術的基盤を必ずしも公開鍵暗号方式に限定していない。技術的中立性に配慮し、将来、公開鍵暗号方式に代わる有力な方式が考え出されたときには、それも本法にいう電子署名にあたると考えられる。機能を基準として電子署名か否かを区別するのである。

「認証業務」とは、前項の「電子署名」が誰によってなされたものであるかを確定し、対外的にそれを証明する業務である。あたかも区役所や市役所で印鑑証明の交付を受けるがごとく、ある電子署名が誰のものであるかを証明する。公開鍵暗号方式においては、「復号化する公開鍵が、誰の暗号化の秘密鍵に対応したものであるか」を証明することが認証業務となる。

「特定認証業務」とは、上記の「認証業務」のうち、電子署名法に基づいて認定されるものを意味する。認定を受けるためには、一般的な信用と一定の技術的信頼性を有するものでなければならない。設備基準や本人確認に関する基準、業務方法一般についての基準などが電子署名法第6条に規定されている。この「特定認証業務」として認定を受けなければ認証業務を行えないというわけではないが、認定を受けることにより、下記のとおり、電子文書についての成立の真正の推定がより強くはたらくということになる。

本人による電子署名が行われると、その電子署名が施された電磁的記録は、真正に成立したものと推定されるという効力が生じる（法第3条）。民事訴訟法228条4項には、「私文書は、本人又はその代理人の署名又は押印があるときは真正に成立したものと推定する。」と規定されている。これは、本来の私文書についての規定であるが、電磁的記録の情報についても同様の推定をはたらかせるというのがその趣旨である。反証がない限り、本人が作成した電磁的記録たる情報であると取り扱われる。ただし、民事訴訟法228条4項は、署名、押印が本人・代理人の意思に基づき真正に成立したものであれば、それが記されている書面全体が本人の意思に基づき作成された真正なものと推定されるという趣旨の規定である。その印影が本人あるいは代理人の印影であるというだけで、ただちに文書全体の成立の真正を推定する規定ではない。したがって、同条の解釈も同様に、単に当該電子署名が本人が日頃使っている電子署名だと証明されただけでは、電磁的記録全体の真正な成立が推定されるものではない。条文に「本人による電子署名」とあるところからも、本人の意思によって施された電子署名があると証明された場合にはじめて電磁的

記録全体の真正な成立についての推定がはたらくと解釈される。もっとも、通常の文書について、判例[4]は、文書中の印影が本人または代理人の印章によって顕出された場合には、反証がない限り、当該印影は、本人または代理人の意思に基づいて成立したものとの事実上の推定がはたらくとしており、電子署名についても、ある人の電子署名が施されているときには、それが本人によって施されたものと事実上推定されると解釈すべきである。

第３　電子署名・電子認証制度の脆弱性

以上のように述べると、電子署名や電子署名は、確固たるシステムであると見えるかもしれない。しかし、次に述べるように、技術的な面において脆弱性を有しているうえに、法的問題が生じる可能性をはらんでいる。そもそも、あまり問題点についての考察が進んでいるとはいえない状況にある。

１　技術的脆弱性

暗号は必ず破られるといわれる。数式の処理によって成り立つ暗号である以上、絶対に破られないということはない。どれくらいの時間破られないかがその信頼性を見極める重要な基準となる。そう考えると、電子認証を得た後の一定の時間内であれば、なりすましがないことを信頼できるが、ある時点で電子署名されたものが、以後何年経っても改ざんがないことを証明する力を有していると考えることはできない。コンピュータのハードウェアの向上により、計算能力が飛躍的に高まれば、現時点では相当期間大丈夫だと信じられているシステムが、意外に早く弱体化することも考えられるのである。この点をよく理解し、将来のシステムの更新時期を見誤らないことが重要である。

なお、現時点の公的電子公証の運用上は、オフラインにおいて行われている。つまり、フロッピィディスクに格納した電磁的記録を公証人役場へ持参するという方法によるのである。オンラインで扱うにはまだまだ信頼性が確固たるものではないと評価されているのである。

２　法的脆弱性

今回の改正は、あらたな運用の内容を定めるだけの改正である。新制度の運用に伴って生じるであろう異常事態に対処するための特別な手立てはないに等しい状況にある。この問題に関心をもっている法律家が少ないという点も問題であろう。

４）最判昭和39年５月12日民集18巻４号597頁

第４　法的課題

１　公証（認証）機関の責任

電子公証だけでなく、電子署名の認証も同様の問題があるので便宜上一緒に考察する。

公証（認証）に誤りがあった場合の認証機関の責任が問題となるだろう。ある特定の電子署名がＡのものであるという電子証明書の呈示を受け、これを信じた第三者が、Ａと取引をしたところ、実はＢがＡになりすましていたような場合である。第三者と認証機関との間には契約関係はないと一応考えられるから、第三者が認証機関に対して、契約違反（債務不履行）を理由に損害賠償を求めることは困難であると考えられる。不法行為に基づく損害賠償請求をすることは可能であろう[5)]。第三者が認証機関に依頼して証明書の交付を受けるシステムであれば、当然のことながら契約関係があるといえる。

不法行為と構成する場合、認証機関の過失を証明しなければならない。本人を特定する資料が不十分なままで認証したり、資料を見誤って認証した場合などには、認証機関に過失があるといえるだろう。公の証明書を偽造するなど、手口が巧妙で誰であっても誤認したであろうといえる場合には微妙である。具体的事例の積み重ねがない状況では予測が難しい問題である。利用者においても一定のリスクを覚悟しておかなければならない。

免責条項の効力も問題となる。問題を認証機関の側からみると、損害賠償額がとてつもなく大きくなるのであれば、業務を行うことを躊躇する。利用者に対して、あらかじめ損害賠償責任を限定する旨（一切責任を負わないとか､一定の金額までしか責任を負わないとかを）予告する（直接の契約者に対しては契約や約款、一般第三者に対しては広告して）ことを考えることになる。確かに、損害賠償額の限定に一定の効果があると考えられるが、故意や重過失があるときにでも責任を免れるとは解されない。また、むやみにそのような予告をすることは、自社の認証の信頼性を低下させることになるので、おのずから一定の調和が保たれるのかもしれない。

２　電子公証（認証）とプライバシー

電子公証（認証）は、特定の電子署名が誰のものであるかを特定して証明するものであるから、認証機関が、個人を特定する情報を入手することを前提としている。公証（認証）機関が、利用者の依頼を受けて電子認証を引き受ける際に、本人特定のための個人情報をどの程度要求するのか、どのような証明書を要求するのかは、基本的には各認証機関の判断による。その目的から考えて、利用者の氏名、住所、性別、生年月日などが必要最低限度の情報となろう。本人を特定するに必要十分な資料の提供を要求すべきは当然である。しかし、本人の同一性の確認とは無関係な、例えば、資産状態や健康状態、趣味などといった情報は不必要である。役所や企業から個人情報が漏れたり、目的外使用されるという事例が後を絶たないという現状からみて、不必要な個人情報の提供は、プライバシーへの脅威となる。本人が十分特定しうるにもかかわらず、不必要

5）福岡高裁判決平成元年３月15日・大阪高裁判決平成元年３月29日判決等

な個人情報をむやみに提供させることのないように配慮しなければならない。また、認証機関が発行する電子証明書には、個人を特定する一定の情報を記載することが予定されている（そうでないと証明書を見る第三者からみて、「誰」についての認証であるかがわからない）ので、個人情報が多数の人々の目にさらされるだけでなく、利潤を追求する企業や名簿業者などによる情報収集を許すことになる（個人情報保護法による規制はあるが）。このように、個人情報のコントロールという点では、従来の印鑑証明書発行による認証システムに比較して、プライバシー侵害の可能性はより大きい。そこで、認証機関が認証できるか否かを判断するのに利用する資料の範囲と電子証明書に記載される本人特定情報の内容の両方について、明確な基準が定められなければならない。

認証機関は、多数の人々の個人情報を知り得る立場にあるから、このような情報を目的外に利用しないようにする義務を負っている。認定認証事業者についてはその旨の規定があり（法第12条）、これに違反したときには認定を取り消されることになるが（第16条１項３号）、罰則はない。もっとも、個人情報保護法においては、認定を受けていない業者も同様に、「個人情報取扱事業者」として、取得した個人情報の第三者への無断提供や目的外利用の制限等の義務規定の適用を受けることになる。実効性があるかどうかの検証はこれからである。

第５　電子公証制度のこれから

１　技術の進歩は必ずしも安全を保証しない。

上記のとおり、現時点では公開鍵暗号方式がデジタル情報に署名を施す最良の方法と考えられているが、暗号技術がその基盤であるがゆえに、解析する技術の進歩によってあっさり無力化される危険を孕んでいる。コンピュータ技術の進歩を振り返ってみると、10年前に10年後を予測した技術内容と現在のそれとでは、現実の方がはるかに進んでいるといわれる。10年後に新たに施される電子署名は、その時点での一定の信頼性を有するものと思われるが、現在施される電子署名が果たして数年も持ちこたえられるかという不安がないではない。公開鍵暗号方式だけにとらわれない新たな認証技術の開発が絶対に必要となろう。

２　技術の進歩にあわせた柔軟な法制

上記のとおり、この領域において生じる法的問題に対しても、基本的には従来からの法体系によって対応できることが多いと考えられるが、今後さらに技術の進歩が果てしなく続けば、例えば、認証機関の責任を問うにしても、電子署名を作出する技術的な部分がブラックボックス化し、製造物責任法が制定されていないときの製造物責任を追及する場面と同様に、認証機関側の故意過失の立証が極めて困難であるといった不都合が生じてくるであろう。もちろん、電子署名、電子公証の過誤に製造物責任法を適用するのは無理である。例えとしてあげた問題点は、ほんの思いつきにすぎず、もっと予想をはるかに超えた法的問題が出現するかもしれない。技術の進歩にあわせた柔軟な法制を検討していかなればならない。