デジタル署名の長期的な利用とその安全性について

松本 勉（まつもと つとむ）／岩下直行（いわしたなおゆき）

要　旨

インターネットの急速な発達と高性能なパーソナル・コンピュータの普及に伴い、さまざまな産業分野、行政手続の分野において、紙の文書をデジタル化された文書（電子文書）に置き換える動きが加速している。紙の文書から電子文書への移行により、効率性や利便性が向上する一方、電子文書は、何も工夫をしなければ、痕跡を残すことなく内容を変更したり、全く同じものを複製したりすることが極めて容易にできるため、偽造や改ざんといったセキュリティ侵害のリスクが高まることも懸念されている。その対策として、本人認証、完全性確保、否認防止の効力を持つデジタル署名を利用することが有効と考えられている。

ところが、通常のデジタル署名が付与された電子文書を長期保管した場合、デジタル署名の効力が維持できないという問題が発生してしまう。この問題に対処するためには、ヒステリシス署名など、署名生成機能の危殆化対策の施されたデジタル署名方式を利用したり、デジタル署名に加えてデジタル・タイムスタンプを併用したり、原本性保証装置を利用したりするなどの対策を検討する必要がある。

本稿では、デジタル署名を付与した電子文書を、署名・捺印のある紙の文書の代替物として実務に利用するために解決されなければならない課題として、デジタル署名の長期的な利用の問題を取り上げ、問題の所在を明らかにするとともに、今後の改善の方向性について検討する。

キーワード：デジタル署名、電子署名法、デジタル証拠性、電子政府、電子文書、長期保管

本稿は、2003年3月7日に日本銀行で開催された「第5回情報セキュリティ・シンポジウム」への提出論文に加筆・修正を施したものである。なお、本稿に示されている内容および意見は筆者たち個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではない。

松本　勉　横浜国立大学大学院環境情報研究院（E-mail: tsutomu@mlab.jks.ynu.ac.jp）
岩下直行　日本銀行金融研究所研究第2課（E-mail: iwashita@imes.boj.or.jp）

１．はじめに

インターネットの急速な発達と高性能なパーソナル・コンピュータの普及に伴い、さまざまな産業分野において、デジタル化された文書（電子文書）の利用が拡大している。また、2003年度までに電子政府[1]を実現するという政府の方針は、行政手続の分野において、紙の文書から電子文書への移行という大きな流れを一段と加速している。電子文書は、コンピュータ・システムを用いて迅速かつ正確な処理が可能なことや、コンピュータ・ネットワーク経由で遠隔地との間の送受信が可能であることなどから、さまざまな産業や行政手続における業務の効率性を高め、利用者の利便性を向上させることが期待されている。その一方で、電子文書は、何も工夫をしなければ、痕跡を残すことなく内容を変更したり、全く同じものを複製したりすることが極めて容易にできるため、紙の文書を電子文書に置き換えていくことによって、偽造や改ざんといったセキュリティ侵害が発生するリスクが高まってしまうことも懸念されている。

こうした問題に対しては、電子文書にデジタル署名を付与することが有効な対策と考えられている。デジタル署名技術は、適切に利用すれば、ある程度の期間にわたって、電子文書の作成者を特定し、作成された文書の完全性を確保し、作成者による事後的な否認を防止することが可能な技術である。例えば、電子商取引においては、取引の過程で送受信された電子文書にデジタル署名を付与して保管しておけば、その文書の偽造を防止し、取引の証拠として利用することができる。2001年4月に施行された「電子署名及び認証業務に関する法律」（電子署名法）は、デジタル署名技術が電子文書の作成者を特定し、完全性を確保し、否認を防止する機能を持つことに着目して、一定の基準を満たすデジタル署名が本人により付与された電子文書について、本人の署名・捺印の付された紙の文書と同等に、その文書が「真正に成立した（本人が作成した）ものと推定する」という効力を認めた。これによって、デジタル署名技術を用いて電子文書の持つセキュリティ侵害の懸念に対処しつつ、さまざまな取引の電子化を進めていくための基盤が整備されたといえる。

現時点では、電子文書にデジタル署名を付与することによって、「真正な成立の推定」の効果を得ようとするシステムはあまり多くはない[2]。セキュリティに対す

1 高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）［2001］では、電子政府を、「行政内部や行政と国民・事業者との間で書類ベース、対面ベースで行われている業務をオンライン化し、情報ネットワークを通じて省庁横断的、国・地方一体的に情報を瞬時に共有・活用する新たな行政を実現するもの」と位置付けている。

2 デジタル署名は、紙の文書への署名・捺印に相当するものとして電子文書に付与する以外にも、インターネットで配信されるコンピュータ・プログラムの改ざんを防止し、作成者を確認するために、広く利用されている。デジタル署名のこのような用途は、システムのセキュリティを守るうえで重要なものであるが、本稿は紙の文書を電子文書へ置き換えるうえでのデジタル署名の役割を中心に検討しているため、このような用途については捨象することとする。

る要請が比較的高い電子金融取引や電子商取引のシステムにおいて、暗号技術や電子認証技術が利用されることはあるものの、その利用目的は主として遠隔地からのシステムへのアクセスにおける利用者認証と、通信経路上での改ざん防止のような、「取引の瞬間」に短期的に利用されるものにとどまっている[3]。電子文書を保管する場合、そのセキュリティはシステム管理者によるアクセス管理によって確保される仕組みがほとんどであり、デジタル署名を付与した電子文書が長期間にわたって保管され、かつ、デジタル署名技術によってその完全性が保証されるようなシステムの事例は、ほとんどみられないのが実情である。署名・捺印のある紙の文書が、取引の瞬間における作成者の意思の確認という役割に加えて、事後的に確認可能な証拠という役割をも果たしていることを考えると、現時点では、デジタル署名の付与された電子文書が、署名・捺印のある紙の文書の代替物になっているとはいえない状態にある。

そこで、本稿では、デジタル署名の付与された電子文書が、署名・捺印のある紙の文書の代替物として実務に利用されていくために解決しなければならない課題として、デジタル署名の長期的な利用の問題を取り上げ、問題の所在を明らかにするとともに、今後の改善の方向性について検討することとしたい。

2．電子文書の利用拡大の実態

まず、現在、どのような書面が紙の文書から電子文書に切り替えられているのか、それらのなかで、デジタル署名技術が利用されている例があるかという点について、民間の商取引において利用される書面と、行政手続において利用される書面とに分けてみてみよう。

(1) 民間の商取引において利用される書面

民間企業同士、あるいは、民間企業対個人の商取引においては、従来から、当事者間の合意により、紙の文書の作成を省略し、電子文書のみが用いられることが少なくなかった。例えば、一般の企業間取引では、見積書、注文書、請求書等を電子化して情報ネットワーク経由で送受信するEDI[4]が普及している。金融機関や機関投資家を対象とする大口の金融・証券取引においては、注文、約定、決済等の取引を全てネットワーク上で完結させる仕組みが整備されているが、これも、紙の文書に

3 松本・岩下［2002］を参照。

4 EDI（electronic data interchange）：企業間取引において商品の受発注などを行う際に、企業のコンピュータ同士を通信回線で接続し、標準化されたフォーマットを用いて、電子的に商取引データを交換する仕組みのこと。

代えて電子文書が利用されている例といえる。しかし、こうした取引に利用される電子文書にデジタル署名が付与されている事例はあまりない。これらの取引は、元々、長期継続的な取引を前提として、特定の企業間、特定の業界内の閉域の通信ネットワーク内で送受信される仕組みとして発達してきたため、デジタル署名技術のような特別な情報セキュリティ技術を利用しなくても、取引の安全性に問題はないと考えられてきたからである[5]。

民間の商取引で利用されている書面のうち、法律等により交付が義務付けられているものの場合、従来は紙の文書を用いる必要があると考えられていたが、2001年4月に施行された「書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律」（IT書面一括法）によって、証券取引などに利用される多くの書面について、顧客の承諾があれば、電子メールやウェブサイト等を用いた電子文書の形式での交付（電子交付）が認められるようになった。この結果、例えば証券業界では、インターネット取引を扱う証券会社を中心に、顧客に交付する目論見書や取引報告書を、紙の文書から電子文書に切り替える動きが活発化している[6]。また、最近では、インターネット・バンキングを提供している銀行においても、取引内容を電子メールやウェブサイトを用いた電子文書によって預金者に通知する先が増えつつある。インターネット証券取引やインターネット・バンキングにおける顧客との事務連絡の場合、機密性のない情報については通常の電子メールで送信し、顧客のプライバシー等の機密性のある情報については、パスワード認証と暗号通信機能を備えたウェブサイトから提供されることが多い。これらの電子文書は、主として、証券会社や金融機関が、顧客の行った取引の内容・条件を書面で通知することにより、顧客に当該取引の内容・条件等を事後的に確認させるという役割を果たすものであり、電子文書自体が取引が行われたことの証拠として送付されているわけではないことから、顧客の同意を得た場合には、書面の交付を要しないものとしたものである[7]。また、書面の内容についての完全性確保や否認防止に対する要請がないため、デジタル署名が付与されることもない。

（2）行政手続において利用される書面

従来、行政手続の分野では、もっぱら紙の文書が利用されており、電子文書の利用による事務の効率化が進んでいなかった。しかし、2001年1月に高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）が決定した「e-Japan戦略」において、

5 EDIや金融取引については、従来の専用線を用いた閉域の通信ネットワークを利用したシステムから、インターネットのようなオープンなネットワークを利用するシステムに移行しつつあり、オープンなネットワークにおけるセキュリティを確保する観点から、暗号技術やデジタル署名技術を利用しようとする動きも出始めているが、そうした動きは現時点ではまだ一般的ではない。

6 大和総研の調査によれば、2002年10月末時点で、目論見書や取引報告書の電子交付に対応している証券会社は19社に達する（石田・久原［2003］）。

7 金融サービスの電子取引等と監督行政に関する研究会［2000］を参照。

「2003年までに、電子情報と紙情報とを同等に扱う電子政府を実現する」との目標が掲げられたことを受け、政府全体として電子政府の実現に向けたさまざまな取組みが進められることとなった。法制面では、2003年2月に施行された「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」（行政手続オンライン化法）により、(1) 書面で行う行政手続は原則としてすべてコンピュータ・システムを利用して行うことができ、(2) この方法で行われた行政手続も書面により行われたものとみなすことが規定された。一方、技術面では、官民双方におけるPKI（public key infrastructure）構築などの技術基盤の整備が進められるとともに、各府省において、申請・届出・入札・納付等の電子化を実現するための電子政府システムの構築が進められている。

行政手続のうち申請・届出等に利用される書面については、その電子化に際して、デジタル署名が積極的に利用されている。デジタル署名により、当該行政手続が真にその名義人によってなされたものであるかどうか（他人によるなりすましがないかどうか）、電子文書の内容が改ざんされていないかどうか等について確認できる仕組みを導入することにより、従来、署名・捺印された紙の文書が果たしていた機能を電子文書により代替することが企図されている。

3．問題の所在 ――電子文書を長期保管した場合のデジタル署名の有効性

デジタル署名方式は、(1) その署名を生成したのが誰であるかを検証可能とする、(2) 電子文書の完全性をある程度の期間にわたって保証する、(3) 署名生成者による事後的な否認を防止するといった効力を持つ技術である。このため、取引の過程で送受信された電子文書にデジタル署名を付与して、長期的に保管・管理する仕組みとすれば、電子文書の偽造を防止し、取引の証拠としての効力（デジタル証拠性）を確保することができるように思える。しかし、実際には、電子文書の長期保管において、その完全性、真正性確保のためにデジタル署名方式が利用されることは、これまではほとんどなかった。それは、現在利用されている通常のデジタル署名方式を用いただけでは、上記のようなデジタル署名の効力を長期間維持することが難しいからである。

一般に、デジタル署名は、生成されてから時間が経つほど、安全性が低下する。現在最も広く利用されているRSA署名方式の場合、その安全性の基礎となっているのは素因数分解問題の困難性であるが、時間が経つほど、効率的に素因数分解を行うための技術革新が進み、計算に用いるコンピュータのコスト・パフォーマンスも改善することから、従来、計算量的に困難であった大きな合成数の素因数分解ができる確率が高まるという意味で、安全性が低下すると考えられている。また、署名生成のための秘密鍵の漏洩についても、同一の管理方法を前提とすれば、秘密鍵を管理する期間が長ければ長いほど危険性が高くなる。

さらに、デジタル署名が付与された電子文書を長期保管した後で検証する場合には、公開鍵証明書の有効期間の問題も考慮しなければならない。公開鍵証明書は、デジタル署名の生成・検証に利用される鍵ペアとその持ち主を結び付けるために認証機関が発行するものであり、認証機関のデジタル署名が付与されている。認証機関は、各公開鍵の所有者に対して、秘密鍵が第三者への漏洩等によって危殆化した場合に、認証機関に直ちに証明書の失効を請求するよう要請している。認証機関は、秘密鍵が危殆化したとの通知を受けた場合、その証明書を失効させ、関連するデジタル署名が安全ではないことを検証者に知らせる仕組みとなっている[8]。デジタル署名の検証者は、公開鍵証明書を用いて署名生成者を確認するとともに、秘密鍵の危殆化等の問題がないことを確認したうえで検証を行う必要がある。ところが、公開鍵証明書に付与された認証機関のデジタル署名も、時間が経てばその安全性が低下してしまうため、公開鍵証明書には有効期間が設けられており、秘密鍵の危殆化に関する情報の周知は、有効期間内にしか行われない。このため、公開鍵証明書の有効期間外の時期に、検証者がデジタル署名の有効性を確認しようとしても、その署名にかかる秘密鍵の漏洩等がなかったことが確認できないため、当該デジタル署名を信用することができなくなる。したがって、長期保管のために特別な対策が講じられていない通常のデジタル署名方式の場合、その効力が維持され、内容を信頼することができる期間は、たかだか公開鍵証明書の有効期間内と考えるべきである[9]。

電子署名法には、公開鍵証明書の有効期間と電子署名の効力との関係について、明確な規定は置かれていない。他方、電子署名法施行規則における特定認証業務に関する規定には、認証機関の発行する公開鍵証明書（法令上の用語は「電子証明書」）については、有効期間を5年以内とすること（第6条4号）、その有効期間内において、認証機関が、証明書の失効処理（第6条10号）および失効情報の周知（第6条11号）を行うことが定められている。こうしたことから、通常のデジタル署名が付与された電子文書の場合、5年を超えて保管すると、デジタル署名用の公開鍵証明書の有効期間を超過してしまう結果、電子署名法第3条の前提となる「本人による電子署名」と認められるかどうかが不透明となり、「当該文書が真正に成立したものと推定する」という法的効果を受けられなくなるおそれがあるのではないかと考えられ

8 秘密鍵が危殆化した場合、認証機関は、公開鍵証明書失効リスト（CRL：certificate revocation list）を配布したり、OCSP（online certification status protocol）と呼ばれるプロトコルを利用したりして、検証者に情報を伝える。具体的な通知手順については、宇根［2002］を参照。

9 公開鍵証明書の有効期間経過後に秘密鍵が漏洩した場合、その秘密鍵を用いて虚偽の署名生成時刻を示すデジタル署名を生成することが可能となる。このため、公開鍵証明書の有効期間経過後には、ある電子文書にデジタル署名が付与され、その文書が「公開鍵証明書の有効期間内に署名が生成されていた」ことを示していたとしても、署名生成時刻を証明する別の証拠がない限り、その表示を信頼することはできない。このため、特別な対策が講じられない限り、公開鍵証明書の有効期間後においては、当該公開鍵証明書に対応する秘密鍵で生成された全てのデジタル署名付き電子文書が信頼できなくなってしまう（電子商取引推進協議会（ECOM）認証・公証ワーキンググループ［2001, 2002］）。

る[10]。実際には、公開鍵証明書の有効期間は1年程度とされることが多く、公開鍵証明書が発行されてからデジタル署名が生成されるまでのタイムラグも存在するので、デジタル署名付きの電子文書を上記のような懸念を生じることなく保管・管理できる期間はさらに短くなると考えられる。

4．電子文書の長期保管の必要性

デジタル署名を付与した電子文書を長期保管した場合、デジタル署名の効力が維持できなくなることは、デジタル署名の利用者にとって、どの程度切実な問題なのであろうか。署名・捺印のある紙の文書にも、ごく短期的にしか利用しないものと、長期間の保管を前提とするものがある。電子文書も同じであり、その電子文書がどのような局面でどのような役割を担うものとして設計されているかによって、長期保管の必要性も異なってくる。

紙の文書と電子文書とを比べると、紙の文書は紀元前からの長い歴史を持つ技術である一方、電子文書はたかだかここ50年程度の歴史しかない技術である。紙の文書から電子文書への移行が進んでいるとはいっても、契約書をはじめとした長期保存が必要な重要な書面は、現在でも紙の文書で作成されることが多い。これに対して、電子文書への移行が進んでいるのは、商取引の過程で一時的に利用されるが、長期保存の必要のない書面が中心であった。このため、従来であれば、電子文書を長期保管するニーズはあまりなく、長期保管によるデジタル署名の効力の低下が問題とされることはあまりなかったと思われる。

しかし、紙の文書から電子文書への移行が進むと、徐々に、「電子化しやすい書面」のみならず、「電子化しにくい書面」にまで、その対象は広がってきた。法律により交付が義務付けられている書面とか、政府の行政手続で利用される書面が電子化されようとしていることが、そうした動きを象徴しているといえよう。そのように電子文書としては後発であるほど、業務上の要求事項は紙の文書に近く、デジタル署名を付与したり、それを長期保管したりするニーズが、他の一般的な電子文書よりも高くなる傾向にある。この結果、特に最近になって、「デジタル署名付き電子文書の長期保管」の問題が注目され始めたという面もある。

10　この点、電子署名法第3条は、裁判上の争いが生じた場合、デジタル署名とこれに対応する公開鍵証明書が提出されれば、公開鍵証明書の有効期間経過後であっても、当該署名について「本人によるもの」との事実上の推定がなされるという運用を想定しているとの見方もありうる。本稿の立場は、デジタル署名が依存している情報セキュリティ技術の内容やデジタル署名に関するシステムの運行・管理等からみると、上記のような見方をしてよいかどうか不透明ではないかというものである。

５．デジタル署名の効力低下への対応策

デジタル署名を付与した電子文書を長期保管することによって、デジタル署名の効力が失われてしまうとは、具体的にどういう状況で、それに対してどのような対応策があるのか、次のような仮設事例で検討しよう。

個人Aと個人Bが、一定期間経過後にBがAに対して商品を引き渡す旨の契約を結んだ。この際、Aは、Bからデジタル署名付きの「電子契約書」を受領し、これを契約の証拠として保管していた。契約を結んだ当初は、Bのデジタル署名は、公開鍵証明書を用いて検証可能であり、秘密鍵も漏洩しておらず、失効リスト（CRL）にも掲載されていないなど、電子署名法第3条が適用される条件を満たしていた。ところが、商品の引渡期日を迎える前に、公開鍵証明書の有効期間が過ぎてしまった。Aは、商品の引渡期日に、Bに対し、「電子契約書」を提示して引渡しを求めたが、Bはこれを拒んだ。Bによれば、公開鍵証明書の有効期間を過ぎた後、Bの秘密鍵が漏洩してしまったため、秘密鍵を知っていれば誰でもデジタル署名付きの「電子契約書」を偽造できるという。Aが提示した「電子契約書」も、そのようにして偽造したものではないかというのだ。

現実の世界においては、「電子契約書」だけが証拠という状況は考えにくいが、このような設定のもとで、個人Aがどのような対応策をとれば、この「電子契約書」が真正に成立した契約書と認められるだろうか。

まず考えられる方法は、個人Aが「電子契約書」を受領した時点で、そのデジタル署名が有効であったこと、すなわち、公開鍵証明書の有効期間内であって、問題なく署名検証が実施できたことを、手元の記録等に基づいて立証するという方法である**（対応策1）**。ただし、この方法は、特に保管期間が長ければ長いほど立証が難しく、立証に失敗するリスクも高まるという問題点がある。

また別の方法として、個人Aが、電子契約書を受領した時点で、外部機関からデジタル・タイムスタンプを発行してもらい、電子文書を受信した時刻の証明[11]を得ておくことも考えられる**（対応策2）**。常に、デジタル署名付き電子文書を受領したタイミングでタイムスタンプを取得するようにできれば、長期保存したデジタル署名の有効性が大幅に向上すると思われる。

この事例とは合わないが、公開鍵証明書の有効期間が切れる都度、新たな「電子契約書」を個人Aが個人 Bから受領するようにしていれば、こうした問題は防ぐこ

11 電子文書の送受信証明については、宇根［2001］を参照。

とができたはずである**（対応策3）**。あるいは、個人Bが作成したデジタル署名が、通常のデジタル署名ではなく、署名生成機能の危殆化対策が講じられた署名方式[12]であったならば、「電子契約書」に付与されていたものが正当な署名であったことを立証することができたと思われる**（対応策4）**。

上で述べた対応策について整理すれば、表1のとおりである。

表1　デジタル署名の効力低下への対応策

対応策 1	**デジタル署名の長期保管者が、署名を検証のうえ、変更を加えずに保管していたことを立証。**
対応策 2	**デジタル・タイムスタンプにより、電子文書の受信証明を取得。**
対応策 3	**定期的に更新されたデジタル署名付き電子文書を受領。**
対応策 4	**署名生成機能の危殆化対策が講じられた署名方式を利用。**

6．電子政府における検討――電子文書の原本性を巡る議論

通常のデジタル署名方式を用いるだけでは、電子文書を長期保管した場合にデジタル署名の効力が維持できないことは、行政手続の電子化の検討においても、重要な論点となった。電子政府においては、電子文書にデジタル署名を付与することを前提に、「電子情報と紙情報とを同等に扱う」ことが標榜されているが、長期保管した場合の署名の効力という観点からは、電子文書は紙の文書と同程度のセキュリティを確保できないことになると考えられるからである。

旧総務庁・行政管理局が1999年から2000年にかけて開催した共通課題研究会は、電子政府における電子文書の長期的な利用について先駆的な検討を行い、報告書『インターネットによる行政手続の実現のために』（2000年3月）を取りまとめた。共通課題研究会では、デジタル署名の長期保管の問題について直接検討したわけではないが、「電子文書の原本性確保」という問題を取り上げ、その解決策について検討している。

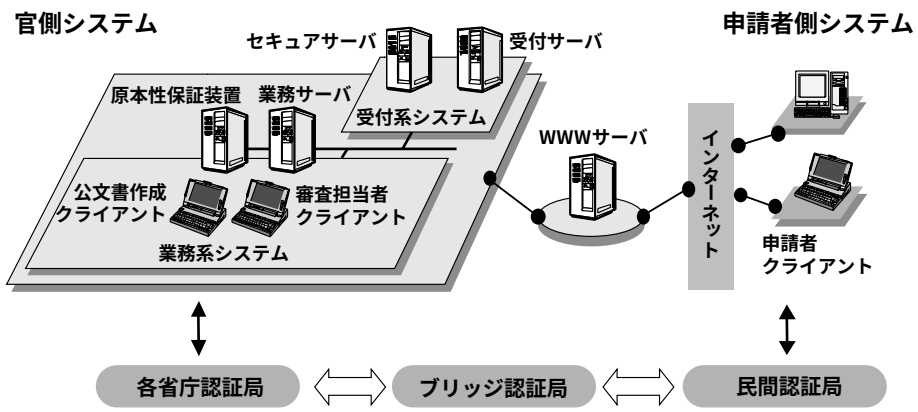
同報告書では、電子文書の原本性を、「電子文書について、紙文書と比較した場合の保存・管理上の問題点が解決された状態にあるようにしておくこと」と定義し、その要件として、(1) 完全性の確保（電子文書の改ざん等を未然に防止し、かつ、改ざん等の事実の有無が検証できるような形態で、保存・管理されること）、(2) 機密性の確保（電子文書の盗難、漏洩、盗み見等を未然に防止する形態で、保存・管理されること）、(3) 見読性の確保（電子文書の内容が必要に応じ直ちに表示で

12　秘密鍵漏洩時の対策が講じられたデジタル署名方式としては、フォワード・セキュア署名（Bellare and Miner［1999］）、ヒステリシス署名（松本他［2000］、洲崎・松本［2002］）、実行ハードウエア確認タグ付きデジタル署名（松本・田中［2000］、宇根・松本［2002］）、MAC付きデジタル署名（小森・松浦・須藤［2002］）などがある。これらについて整理した文献として、宇根［2003］がある。

きるよう措置されること）の3点を挙げている。そして、この原本性を確保する手段として、(a)管理組織体制、(b)データ管理方法、(c)システム運用管理に関する注意事項を定めた。

こうした報告書を踏まえ、現在、構築が進められている各府省の電子申請・届出システムでは、デジタル署名が付与された申請書類などの電子文書をシステム内で長期保管するにあたり、原本性を確保するための装置（原本性保証装置）を組み込む仕組みとなっている（図1参照）。この装置は、(1)ID、パスワード等によってアクセス制御されたハードウエアであり、(2)電子文書の更新履歴（削除した内容、追加入力した内容等）を確実に記録する機能を持っている。申請者から送付された申請書類や官庁が作成した公文書をこの装置に格納することによって、電子文書の改ざんを防止するほか、デジタル署名の長期保管が可能となる。各府省では、申請者から送付された電子文書のデジタル署名を検証しておき、原本性保証装置に保存することによって、デジタル署名にかかる公開鍵証明書の有効期間後であっても、デジタル署名の証明力を維持することが可能と考えている。いわば、5節における「対応策1」を、システム的に実現していることになる。

図1　経済産業省・汎用電子申請システムの全体構成図



資料：ニューメディア開発協会［2002］

7．電子文書の長期保管における安全対策の選択

このように、電子政府システムは、長期保管する電子文書のセキュリティを確保する手段として、原本性保証装置により、適切なアクセス管理、履歴管理を実施するというコンセプトに基づいて構築が進められている。こうした安全対策は、金融機関の勘定系システムのように高度な安全性が求められるシステムにおいて従来から実施されてきたセキュリティ対策の延長線上にあるものと位置付けることができる。現時点で利用可能な通常のデジタル署名技術だけでは、長期的な電子文書のセキュリティを確保することが難しい以上、電子文書を格納した専用システムへのアクセス管理や履歴管理に重点を置いた安全対策としたことは、早期に行政手続の電子化を進めるうえで、現実的な対応であったと考えられる。

しかし、そのような対応にはいくつかの問題点が存在しているのも事実である。電子文書を専用システムに格納し、アクセス管理、履歴管理によってセキュリティを確保する場合、万一、その防御機構の一角が破られ、一部の電子文書についてセキュリティが損なわれると、当該システムが格納している全ての電子文書について信頼を失うリスクがある。システム提供者が信頼を失い、システムに保管されている電子文書が改ざんされているかもしれないという疑いをかけられた場合、電子文書を作成して送信した利用者が作成の事実を否認する余地を与えることとなり、そのシステムに格納された電子文書が証拠として機能しなくなるおそれもある。

また、「国民と政府」や「預金者と金融機関」といった関係の行政手続や取引が行われた場合に、アクセス管理、履歴管理といった対策によって電子文書の安全性を長期にわたって保証することができるのは、センター管理型のシステムを提供している政府や金融機関の側に限られるという点も問題として指摘できよう。例えば、電子政府システムの場合、国民が政府に提出した電子文書は、政府のシステムで適切に管理されることによって長期間の安全性が保証されるが、政府から国民に交付された電子文書は、国民の側に原本性保証装置等がない以上、長期的には安全性が保証されない[13]。このため、政府との取引で国民が提出した電子文書に対するデジタル署名付きの「電子受領証」とか、金融機関との取引で預金者が指示した資金移動に対するデジタル署名付きの「電子領収書」といった仕組みが実現しにくい。こうした電子文書は、いったん利用者に交付されてしまうと、長期的に安全に検証することが難しくなってしまうからである。

13 現在の電子政府システムの一部では、こうした問題に対処するため、政府機関側のデジタル署名が付加された電子文書を電子政府システム内に格納し、これを国民から検証させることにより、その安全性を長期的に保証しようとしている。この方式は安全対策としては有効と考えられるが、個別文書の検証を、毎回、政府におけるセンター型のシステムで実施することに伴う効率性の問題や、サービス拒否攻撃を受けるリスクが存在すること等から、そうした形態で安全性を確保することには限界があると考えられる。

こうした問題の存在を踏まえると、今後、電子文書の長期保管における安全対策を考えていくうえでは、システム提供者によるアクセス管理、履歴管理によって、「電子文書が保管されているシステム全体」を防御するという現在の対応に加えて、「デジタル署名が付加された電子文書単体」に対する長期的な安全性を向上させるための対策を講じることが望ましいと考えられる。それを実現する技術として、ヒステリシス署名に代表される「署名生成機能の危殆化対策が講じられた署名方式」の研究が進められているほか、デジタル署名の作成や送受信にかかる時刻を認証し、秘密鍵の漏洩などに伴う被害を限定すること等を目的としたデジタル・タイムスタンプ技術の実証研究も進められている。

8．おわりに

今後、紙の文書から電子文書への移行がいっそう進んでいくことを考えると、デジタル署名方式を長期的に安全に利用できるよう、環境を整備していく必要があると思われる。既に、電子政府の電子申請・届出システムにおいて、原本性保証装置を組み入れたシステムの構築が進められている。同様に、署名生成機能の危殆化対策が講じられたデジタル署名方式や、デジタル・タイムスタンプなどの新しい技術についても、さまざまな研究開発が行われ、一部で商用サービスが開始されている。現段階では、こうした新しい技術は、その効果を見極めるために、更なる分析が必要な段階と考えられるが、電子政府や電子商取引の安定性、安全性を向上させるためには、これらの新技術の採用について、積極的に検討していくことが重要と考えられる。

もとより、従来の紙の文書に基づくさまざまな商取引、行政手続の安定性、安全性は、その手段である署名･捺印そのものによって支えられてきたわけではない。署名・捺印のある紙の文書が、極めて精巧に偽造や変造ができたとしても、長年の経験により確立され、法律などの制度によっても支えられた「実務の枠組み」によって、取引の安定性が維持されていると考えるべきである。

インターネットを利用した電子商取引、電子政府における情報セキュリティの問題点とは、そのような「実務の枠組み」を崩すことに伴う不安や取引の不安定化を、技術のみによっては完全には支えきれないことにあるといえる。対面取引における紙による偽造防止、署名・捺印による認証といった手段は、基礎となる技術も素朴なものであり、人手が介在するだけに完璧を期すことは難しいが、長年の利用によるノウハウの蓄積、前例や裁判例の積重ねがあるため、問題が発生する確率を予測可能であり、万一問題が生じてもその被害の範囲が想定できるという意味で、利用者に安心感を与えてくれる。しかし、電子文書を介して行われる取引には、現段階ではそのような実績の積重ねがない。電子文書の利用を拡大し、そのメリットを最大限に活かしていくためにも、デジタル署名の長期的安全性について、今後さらに検討を深めていくことが必要であろう。

参考文献

石田隆夫・久原美香、「産業界における電子書面交付の現状」、『大和レビュー』2003年新春号No. 9、大和総研、2003年1月、94～107頁

宇根正志、「電子文書の送受信証明を行うためのプロトコルの研究動向と安全性評価」、『金融研究』第20巻別冊第1号、日本銀行金融研究所、2001年4月、79～124頁

――――、「金融分野におけるPKI：技術的課題と研究・標準化動向」、『金融研究』第21巻別冊第1号、日本銀行金融研究所、2002年6月、227～283頁

――――、「デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策」、『金融研究』第22巻別冊第1号、日本銀行金融研究所、2003年6月、15～50頁（本号所収）

――――・松本 勉、「実行ハードウェア確認タグ付きディジタル署名方式」、『情報処理学会研究報告』2002-CSEC-18、情報処理学会、2002年7月、245～252頁

金融サービスの電子取引等と監督行政に関する研究会、『金融サービスの電子取引の進展と監督行政』、2000年4月

高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）、『e-Japan戦略』、2001年1月

小森 旭・松浦幹太・須藤 修、「電子商取引における紛争解決のための電子証拠物に関する分析」、『2002年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2002年2月、627～632頁

洲崎誠一・松本 勉、「電子署名アリバイ実現機構―ヒステリシス署名と履歴交差」、『情報処理学会論文誌』第43巻 第8号、情報処理学会、2002年8月、2381～2393頁

総務庁・共通課題研究会、『インターネットによる行政手続の実現のために』、2000年3月

電子商取引推進協議会（ECOM）認証・公証ワーキンググループ、『電子署名文書長期保存に関する中間報告』H12－認証・公証－3、2001年3月

――――、『電子署名文書長期保存に関するガイドライン』H13－認証・公証－3、2002年3月

ニューメディア開発協会、『研究成果レポート』第7号、2002年7月

松本 勉・岩下直行、「インターネットを利用した金融サービスの安全性について」、『金融研究』第21巻別冊第1号、日本銀行金融研究所、2002年6月、207～225頁

――――・岩村 充・佐々木良一・松木 武、「暗号ブレイク対応電子署名アリバイ実現機構（その1）―コンセプトと概要―」、『情報処理学会研究報告』2000-CSEC-8、情報処理学会、2000年3月、13～17頁

――――・田中直樹、「計算の実行ハードウエアを確認する方法」、『コンピュータセキュリティシンポジウム2000論文集』情報処理学会シンポジウムシリーズVol. 2000、No. 12、情報処理学会、2000年10月、199～204頁

Bellare, Mihir, and Sara K. Miner, “A Forward-Secure Digital Signature Scheme,” *Proceedings of CRYPTO ’99*, LNCS 1666, Springer-Verlag, August, 1999, pp. 431-448.