

社会基盤としての電子認証の調査研究

—電子自治体の構築をめざして—

平成 14 年 5 月 1 日

兵庫ニューメディア推進協議会

X M L ・ 電子認証研究会

代表 力宗幸男（神戸商科大学教授）

目次

1 . はじめに	1
2 . 認証の意義	2
(1) 認証とは何か	
(2) 電子認証の意義	
(3) 電子認証の必要性	
(4) I D やパスワードによる認証	
(5) 公開鍵暗号方式 (P K I) による電子認証	
3 . 認証の仕組み	4
(1) 認証の対象	
(2) 認証を支える技術	
4 . 電子署名・電子認証制度	8
(1) 電子化に対応した法制度	
(2) 電子署名法	
(3) 商業登記に基礎を置く電子認証制度	
(4) 公証制度に基礎を置く電子公証制度	
(5) 地方公共団体による公的個人認証サービス	
(6) 行政機関における組織認証制度	
5 . 電子認証の普及のための課題と提言	16
(1) 利用者の視点にたった電子認証の普及	
(2) 利便性の高い電子申請システムの構築	
(参考)	20
(1) 参考条文	
(2) 電子認証サービス一覧	
(3) 用語集	
(4) 参考文献	

1. はじめに

1998年12月に内閣総理大臣決定として発表された、「ミレニアム・プロジェクト(新しい千年紀プロジェクト)」の中で述べられた「2003年度までに、民間から政府、政府から民間への行政手続きをインターネットを利用しペーパーレスで行える電子政府の基盤を構築する。」が、電子署名及び認証業務に関する法律(電子署名・認証法:平成12年5月成立)が2001年4月1日に試行されるに至り、いよいよ現実のものとなってきている。

一方、兵庫ニューメディア推進協議会の「電子行政とXML」自主研究グループは、2000年度、1997年度から続けてきた兵庫ニューメディア推進協議会「地域情報化策専門部会」「行政の情報化分科会」の研究を引き続き、「電子県庁」を実現するための要素技術としてのXML(eXtensible Markup Language)に焦点を当て、「XMLとは何か」、「XMLの行政手続きへの応用」、「XMLのWeb表示とアプリケーションとの連携」、「電子県庁のデータベースとしてのXMLデータベース」等の研究を行なった。

2001年度は、これらの成果をさらに発展させるべく、「電子政府」、「電子県庁」実現の為に必要となる「電子手続きにおける認証」というテーマに焦点を当て、「PKIの概要と基礎、将来における問題点」、「電子自治体と認証関連技術」、「電子認証による社会の変化」、「XMLデータベースと電子署名」、「Web/XML/電子フォームで実現する電子自治体へのアプローチ」、「行政手続オンライン化の法整備」、「経済産業省における汎用電子申請システム」等について研究を行ってきた。

その結果、「電子県庁」、「電子政府」等の為の「電子認証」技術は、細かな点を除けば既に殆んど完成していると言えるが、問題は、「電子認証の認知度の低さ」、「電子認証導入の費用対効果」、「電子認証導入の為の法律の改正」、「既存のワークフローの単なる電子化」等の点にあることが明らかになった。従って、今後、「電子認証に対する普及啓発」、「ワークフローを見直すことによる費用の削減」、「利用者にとって利用し易く信頼性の高いシステム構築」、「これらを実現するための法律の改正」等を積極的に推進して行く必要がある。

アクセンチュア社の電子政府化ランキング(2002年4月26日)では、日本は先進23カ国中17位で、やっと「出遅れ組み」から「新興勢力」になったに過ぎない。その遅れは、技術の問題ではなく、「制度」、「やる気」、「国民の意識」等が問題であることが明らかである。この遅れを取り戻し「革新的リーダー」となるために、さらに研究、議論の必要性がある。この研究成果が、そのための1つの足がかりとなることを祈念してやまない。

2. 認証の意義

(1) 認証とは何か

私たちは、モノやサービスを生産し、消費するために取引を行ったり、役所の窓口で住民票やパスポートの発行、税の申告などさまざまな手続を行っている。これらの取引や手続が有効に成立するためには、当事者が互いに本人の意思によって行われたものであることを確認できる「本人の確認」が必要である。こうした本人を確認する仕組みが「認証」と呼ばれるものである。認証は取引の安全や行政手続の信頼性を保証し、私たちの社会経済活動に欠くことのできない役割を担っている。

それでは、ネットワークを利用した電子商取引や電子申請を行う場合は、どのように相手の確認を行えばいいのだろうか。この場合、契約書や申請書は電子文書となるため、認証も電子的な手段で行う必要がある。これを「電子認証」というが、利用者はどのような方法で利用できるのか、相手の確認や電子文書の内容に争いが起きたときにも、安心できる仕組みになっているのだろうか。

インターネットの普及に伴って、企業間での電子商取引が急速に進展し、行政機関では行政手続の電子化が推進されつつあるなか、電子認証には大きな期待が寄せられている。電子認証が、生活や産業、行政の情報化の基盤として、どのような役割を担い、ネットワーク社会の基盤として普及していくための課題は何か。ここでは、電子認証の仕組みや役割を制度面、技術面、運用面から調査検討し、今後の電子認証のあり方について考えていきたい。

(2) 電子認証の必要性

総務省の情報通信白書によると、平成12年末のインターネットの利用者は4,708万人で対前年比74%増、世帯普及率は34%、従業員300人以上の企業では96%の普及率となり、急速に普及が進んでいる。

こうしたインターネットの普及に伴って、電子商取引も著しく拡大している。平成12年末の市場規模は、企業間の取引(B to B)では約34兆円(対前年比60%増)、オンラインショッピングなど企業対消費者(B to C)では約1兆5千億円(対前年比80%増)、電子調達・入札など企業対行政(B to G)では約60億円の規模になっている(経済産業省「平成13年度電子商取引市場規模調査」)。

今後、インターネットを利用した電子商取引や行政機関での電子申請、電子調達のシステムが構築されていくが、利用者が安心して取引や手続が行えるようにするためには電子認証は欠くことのできない役割を担っている。

特に、行政手続は、住民の権利・義務や給付など生活に重要な影響を及ぼすものも多く、システムの構築や運用に当たっては、簡便な操作に加えて、個人情報保護やセキュリティなどの信頼性や安定性の確保は最も重要な課題となる。

今後、地方公共団体においても、電子自治体の実現に向けて、電子申請システムの基盤となる住民の個人認証基盤や行政の組織認証基盤の整備を進める必要がある。電子認証についての理解を一層深め、各種のシステムを構築することが求められる。

(3) 電子認証に求められる機能

書面で取引や手続を行う場合、当事者は契約書に署名、押印することによって、互いに相手を確認でき、信頼して取引を行うことができる。仮に、相手が契約の成立について争いになった場合でも、本人の署名や押印(実印)と印鑑登録証明書が添付されていれば、相手に契約の履行を求めることができるのである。

これに対して、電子商取引や電子申請では、紙を媒体とするのではなく、電子文書の交換を行うため、文書を容易にコピーしたり、他人が改ざんしてもその痕跡がつか

めないという問題がある。また、インターネットは誰もが接続できるオープンなネットワークであり、文書の送受信者を相互に確認できず、通信の途中で他人に「盗聴」されたり、本人になりすましてデータが送信される恐れがあり、安心して取引や手続が行えないという危険性を抱えている。

こうした電子化の特性に対応した信頼性の高い電子認証の仕組みを作ることが求められる。

(4) ID・パスワードによる認証

ネットワーク上での電子認証の方法として、IDやパスワードが利用されてきた。これは、あらかじめ本人から発行の申込みを受け、本人確認を行った上で、システムにアクセスする権限を与えるIDと本人しか知り得ないパスワードを発行することにより、利用者の確認を行うもので施設利用案内・予約システムなどに利用されている。

このID・パスワード方式は、高度な技術は要さず、低廉な経費で運用できるというメリットがあり、また、後述するVPN、SSLやSSH等により暗号化した通信手順を併用すれば、安全性を高めることは可能であるが、前述したとおり、ID・パスワードを不正に入手した「本人へになりすまし」や文書の改ざんの可能性があるほか、送信者が後日、そのような電子文書を送信した事実はないという否認も防止することができない。

さらに、国や地方公共団体がさまざまなシステムを構築する場合、利用者はそれぞれの機関のシステムごとにIDとパスワードを用意しなければならず、非効率で利便性の低いサービスになるという問題もある(表1参照)。

ID・パスワード方式を利用する場合には、どの程度まで安全性、信頼性が求められる手続なのか、万一「盗聴」などの問題が生じても大きな被害にはならないのかどうかなどを検討する必要がある。

(5) 公開鍵暗号方式(PKI)による電子認証

こうしたID・パスワード方式の限界を踏まえて、現在では暗号技術に基づく公開鍵暗号方式(PKI:Public Key Infrastructure)が実用化されている。

これは、電子文書の作成者が、本人しか知り得ない「秘密鍵」と呼ばれる暗号化のプログラムによって文書を暗号化し、受信者は秘密鍵とペアとなる「公開鍵」によって解読するものである。受信者が解読できた場合は、送信された文書は秘密鍵で作成された文書であることから、確かに作成者本人の文書に間違いがないことが確認できたということになる。この秘密鍵で文書の暗号化を行うことを「電子署名」といい、書面の場合における実印に相当するものである。

なお、本人が電子署名を行っても、使用した秘密鍵は盗用された可能性もあり、必ずしも本人のものとは限らない。そこで、印鑑登録証明書と同様に、本人でしか知り得ない秘密鍵によって電子署名が行われたことを第三者が証明する必要がある。

民間では既にこの証明を行う認証事業が実施されている。認証事業者は、認証局を設置し、秘密鍵及び公開鍵を作成した本人に対して、当該公開鍵は本人のものに間違いがないことを証明する電子証明書を発行し、本人から証明書を受け取った受信者に対して、その証明書が失効していないか否かを確認できるサービスを提供している。

以下、この公開鍵暗号方式を中心に電子認証のあり方について考える。

表1 認証方法の対比

	認 証		通信の暗号化	非改ざん性	否認防止
	本人の同一性	文書の同一性			
署名・押印			-		
ID・パスワード		×	(SSL等の活用)	×	×
PKI					

非改ざん性：送信した情報内容が伝送途中で改変されていないことの保証

否認防止：送信者が自ら作成した文書でないと事後に否定することの防止

3. 認証の仕組み

(1) 認証の対象

公開鍵暗号方式による認証の対象として、個人の認証、企業・法人の認証及び行政機関の認証について述べる。

個人の認証

個人の認証については、民間の認証事業者でも認証サービスを行っているが、今後、電子申請が全国のどこでも、誰もが安価な費用で利用できるよう、平成15年度から地方公共団体による公的個人認証サービスの運用が開始される予定である。総務省では、平成14年2月に「地方公共団体による公的個人認証サービスのあり方検討委員会」の報告書を公表し、「電子署名に係る地方公共団体の認証業務に関する法律案（仮称）」を制定するとともに、14年度に実証実験を行い、具体的な運用の準備を行うこととしている。

本制度は、市町村が認証登録局となり、窓口で本人確認を行い、都道府県知事名で個人を認証する電子証明書を発行するもので、住民は住民票の交付申請など電子申請を行う場合、他人になりすまして申請していないか等、申請者としての正当性の確認が可能となる。

なお、この公的個人認証は、住民基本台帳に記載された住民を対象とするもので、住民基本台帳をもとに本人が当該住所地に居住しているか、死亡していないかなど本人の実在性の確認を行うものである。

企業・法人の認証

企業・法人の認証については、平成13年10月に「商業登記簿法等の一部を改正する法律」が施行され、「商業登記に基礎を置く電子認証制度」が運用されている。

これは、インターネットを用いた電子的な取引社会における取引の安全と円滑を図るために、従来の法人代表者の「印鑑証明書」や「資格証明書」に代わる電子的な証明として、法務局が「電子証明書」を発行するものである。これにより、インターネット上の企業間取引及び行政機関への各種電子申請や電子入札などに際して、当該企業が確かに正当に手続を行ったものであるとの信頼性が付与されることになる。

なお、「商業登記に基礎を置く電子認証制度」における認証対象は法人の代表者に

限定されており、実際の企業活動においては実務者の署名で取引されることも多いので、その場合には別の認証基盤が必要となる。例えば、国土交通省の建設 CALS における電子入札では電子入札用の認証局を使うようになっている。現在、帝国データバンクの電子入札用認証局が認証サービスを行っている。

また、アイデントラス社では、国際的な取引を行う基盤として金融機関が取引先の法人を認証するサービスを提供しており、より信頼性の高い認証サービスの普及をめざしている。

行政機関の認証

行政機関では、国民から申請・届出等手続に対して、許可通知等を書面で作成し、公印の押印を行っているが、インターネットを介してオンラインで実施することに伴い、申請者から当該通知が確かに行政機関から送信されたものであり、内容が改ざんされていないことを確認できる仕組みが必要となる。

このため、政府では府省の大臣等の官職を証明する政府認証基盤（GPKI）の構築を進めており、総務省、経済産業省及び国土交通省は先導的に府省認証局を、総務省においてはこれらを相互に接続するブリッジ認証局を構築した。その他府省認証局についても平成 14 年度までに全て整備されることになる。

また、地方公共団体についても、組織認証基盤の整備が進められており、平成 15 年度までには市町村まで整備完了することが求められている。

（２）認証を支える技術

認証技術の重要性

まずは、近年のサイバー社会の進展により、認証に関わる技術の重要性が益々高まっている点に触れる。

国内外のセキュリティ侵害状況を例に示すと、米国 CERT（コンピュータ緊急対策センター）や日本国内の JP/CERT に対するセキュリティ侵害（ホームページ改ざん、不正アクセス等）に関する届出が近年急激な伸びを示している。

また、一般的に、情報の電子化及びネットワーク化により、利便性は向上するが、一方で様々な脅威に対するより高度なセキュリティ対策が必要となる。例えば、紙ベースで個別に（スタンドアロンで）管理されている情報が、電子化され、更にはネットワーク上でインターネット等を介して流通するようになると、様々な脅威（盗聴、破壊、消滅、ウイルス攻撃、ハッキング、なりすまし、改ざん等）にさらされることになる。認証技術は、有効なセキュリティ対策の一つとして、特にこの中でもファイヤーウォールやアクセス監視等の物理的な対策で対応できない「改ざん」や「なりすまし」等の脅威への対処として重要である。

認証技術の内容

次に認証に関する技術の内容について述べる。

実の世界で、文書を本人が作成したことを示すために「記名+捺印(またはサイン)」を付す。文書が変更(改ざん)されていないことは、紙質の相違、修正跡の有無を見て判断される。これに対して、電子的な文書では、コピーや変更(改ざん)が容易であり、また改ざんされたことを証明することは難しい(印影やサインを電子的な形で文書に添付しても、コピーが可能のため、文書作成者の本人性は確認できない)。

このため、電子的な文書で、本人性を確認するため、暗号技術を使用した「デジタル署名」により、文書作成者の本人性確認、文書の真正性確認が可能にする。電子的な方法で、本人かどうかを確認する方法として、通信アクセスしている相手、文書やデ

ータを作成した者を確認することを対象とする。一般に公開鍵暗号を基本とする電子認証が用いられる。デジタル署名を検証する公開鍵について、その所有者を証明する「公開鍵証明書」を、認証局（CA）が発行する。

一般的に、主な認証方法として、（１）IDカードを用いた認証（IDカードから読み出したIDと事前に登録しているIDの一致検証を行う）、（２）ID/パスワードによる認証、（３）ワンタイムパスワードを用いた認証、（４）認証局（CA）を利用した電子認証がある。

本人性の確認は、上記のいずれの方法でも確認できる。ところが、送られてきた文書の真正性を確認できるのは（４）認証局（CA）を利用した電子認証のみである。一般的な生活では、本人性の確認のみで良い場合が多いので、（１）～（３）の方法を状況によって使い分けることで対応すればよい。但し、重要な文書や書面が関係する場合は、文書の真正性を確認する方法が不可欠である。この場合には、認証局（CA）を利用した電子認証が必要である。

また、ID/パスワード方式に比べ、公開鍵暗号方式による本人性の確認のメリットとして、管理の問題がある。ID/パスワード方式ではセンターでIDとパスワードを保存しておかなくてはならず、それが漏洩しないように厳重な管理をしなければならないが、公開鍵暗号方式では秘密鍵の管理は本人のみの責任に委ねられ、センターは秘密鍵を保管する必要がない。この点は公開鍵暗号方式の良い点である。更に、ID/パスワード方式では、予め登録しておくことが必要であるが、PKI（公開鍵暗号方式＋CA）では始めて通信する相手であっても本人確認ができるという利点がある。

PKI（公開鍵暗号方式＋CA）を利用した本人性の確認の仕組の例を図1に示す。

次に公開鍵暗号方式を利用した暗号通信について述べる。SSLは公開鍵暗号方式を使ったサーバとクライアント間の暗号通信の方式である。サーバ、及びクライアントはそれぞれ相手の公開鍵証明書を交換し、相手の公開鍵が何かを知り、それによって通信データを暗号化して送る方式である。公開鍵で暗号化されたデータは対応する秘密鍵でしか復号化することができないので、通信路上で傍受されたとしても中身を相手以外に知ることはできない。

また、悪意のある者がサーバになりすまし、サーバの公開鍵証明書をクライアントに送るなどというようなことをしても、公開鍵に対応する秘密鍵は、公開鍵証明書に書かれた本人しか知り得ないので、なりすました者は受信したデータを復号化することはできない。

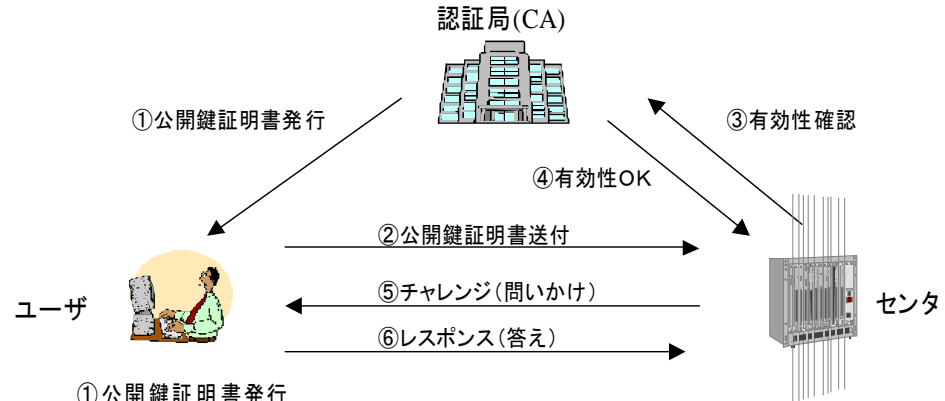
このように、SSLは始めて通信する人との間でも暗号通信を行うことができるものである。

なお、公開鍵による暗号/復号は、プロセッサに与える負荷が大きいので、実際には、まず、今回の通信で使う共通鍵を公開鍵暗号方式で暗号化して相手に送り、実際のデータはこの共通鍵で暗号化して送ると言う方法が取られている。

図1

本人性確認の仕組み（例）

通信に先だって、以下の仕組みで本人性の確認が行われる。



- ① 公開鍵証明書発行
公開鍵が誰のものを証明するもので、認証局の署名がされている。
- ② 公開鍵送付
ICカードに格納された公開鍵証明書を送付する。
- ③ 有効性確認
公開鍵が有効かどうか、認証局に問い合わせる。
失効リストを入手して調べる方法と、その都度オンラインで問い合わせる方法がある。
- ④ 有効性OK
認証局は、鍵が失効しているかどうかを答える。
- ⑤ チャレンジ(問いかけ)
センタは乱数を使ってランダムなデータ(チャレンジ)を作成し、ユーザの公開鍵で暗号化しユーザに送る。
- ⑥ レスポンス(答え)
ユーザは受信したチャレンジを秘密鍵で復号化し、レスポンスとしてセンタに返す。センタはレスポンスとチャレンジが一致することを確認する。公開鍵で暗号化したデータを正しく復号化できるのは、公開鍵に対応した秘密鍵のみであり、それを知り得るのは公開鍵証明書に書かれた本人のみであるため、上記の方法で通信相手の本人性確認を行うことができる。

4 . 電子署名・電子認証制度

(1) 電子化に対応した法制度

電子署名の法的効果

書面による取引で契約の成立について争いが生じた場合、民事訴訟法では、「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。」と規定されており、署名又は押印は文書の成立を事実上推定する効果を持っている。

インターネットを利用した電子商取引の場合についても、電子署名は書面による署名又は押印と同様、本人が確かに作成した文書であることを推定する効力を持たせる必要がある。

このため、平成13年4月1日に「電子署名及び認証業務に関する法律」(以下「電子署名法」という。)が施行され、一定の要件を満たす電子署名が行われた電子文書については、書面の場合と同様、本人が作成した文書であることを推定する規定が設けられている。

認証業務と法的根拠

電子署名法では一定の認証業務を対象に主務大臣による認定制度が導入されているが、認証業務そのものの実施については許可や免許などの規制はなく、民間事業者は自由に参入できる。

行政機関においても、従来、書面で行ってきた認証が電子的にも行えるよう法律改正や新たな法整備を進めている。法務省では、登記所が発行している法人の代表者の印鑑証明書や資格証明書を電子的にも行えるよう、商業登記法の一部改正を行い、法人代表者の認証業務を実施している。また、公証制度に基づく電子公証サービスも実施されている。

総務省では、すべての行政手続は書面に加えて、電子的にも可能とする法制度を整備するため、「行政手続のオンライン化法案」や平成15年度に地方公共団体による公的個人認証サービスを実施するため、「電子署名に係る地方公共団体の認証業務に関する法律案(仮称)」を平成14年通常国会に提出する予定である。

行政の組織認証基盤の法的根拠

行政機関においても、住民や企業が受け取った公文書が、大臣や知事等からの文書であることが確認できるよう、当該官職について電子証明書を作成し、添付することが必要となる。こうした行政機関において一定の権限を持つ官職の認証を行う仕組みは組織認証基盤と呼ばれている。

各府省や地方公共団体では、それぞれ認証局を設置し、当該官職の電子証明書の発行を行っている。なお、この電子証明書を発行するための法令は必要とはされていない。

表2 印鑑登録証明書と電子証明書との比較

	印鑑登録証明書	電子証明書
発行主体	・市町村	・民間、行政
証明機能 (文書成立の推定)	<ul style="list-style-type: none"> ・本人の印鑑であること (印鑑登録証明書を添付) ・本人が押印したこと (押印した印影と印鑑登録証明書の印影が同一) 	<ul style="list-style-type: none"> ・電子署名で使用された秘密鍵は本人のものであること (証明書の対象は秘密鍵に1対1で対応する公開鍵) ・本人による電子署名であること
発行形態	・紙	・電磁的記録
有効期間	・証明書を必要とする都度、 交付を申請	・有効期限があり、その期限を超えると失効
発行の根拠	・市町村の条例	・電子署名法等

表3 認証サービスの概要

サービス提供者	サービスの利用者(証明書の交付を受ける者)	
	企業・個人	行政機関
民間事業者	<ul style="list-style-type: none"> ・電子署名法に基づく特定認証業務 ・一般認証業務 	
行政機関	<ul style="list-style-type: none"> ・商業登記に基づく電子認証サービス(法務省) ・公証制度に基づく電子公証サービス(日本公証人連合会) ・公的個人認証サービス(地方公共団体) 	<ul style="list-style-type: none"> ・政府組織認証基盤(大臣等の官職証明書) ・地方公共団体組織認証基盤(首長等の官職証明書)

(2) 電子署名法

電子署名法では、本人による一定の要件を充たす電子署名が行われた電子文書は、手書きの署名や押印と同様、本人の意思に基づき真正に作成されたものという推定効果があることを明らかにしている。また、一定の水準を充たす認証業務については、国の認定を受けることができるようにした。主務省庁は総務省、経済産業省及び法務省の3省で、平成13年4月1日に施行されている。

電子署名法の意義

ア 電子署名の定義

電子署名はこの法律で初めて定義され、「電磁的記録に記録することができる情報について行われる措置」であって、「その情報は本人が作成したものであること」、かつ「情報が改変されていないこと」を確認することができるものである、とされている（第2条）。

イ 電磁的記録の真正な成立の推定

民事訴訟法第228条第4項では、「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。電子文書についても、この手書きでの署名や押印と同じく、本人でしかなしえない方式で電子署名が行われている場合には、真正に成立したものと推定される（第3条）。

ウ 特定認証業務に関する認定制度の導入

認証業務のうち、一定の基準を充たす特定認証業務を行う事業者は主務大臣の認定を受けることができる（第4条）。認定の対象は、事業者自身ではなく、事業者が提供する一定の認証業務とされている。

この認定は、上記の電子文書の成立を推定する効果の発生要件とはされていない。したがって、特定認証業務でなくても、電子署名に基づく電子文書の成立の推定効果は生じるが、一方で、次のような実体上の効果を持つ。

- ・ 特定認証業務は信頼できるサービスであるという評価が受けやすくなること。
- ・ 特定認証業務での認証局と政府認証基盤（ブリッジ認証局）との相互認証が認められること。

国に電子申請を行う場合、申請者は、当該認定認証事業者から電子証明書の交付を受けて当該府省に申請し、府省からの結果通知を受ける際、当該認定認証事業者の認証局を通じて発信者（大臣等の官職）の電子署名の確認を行うことができる。これにより、国への電子申請が実質的に保証される。

- ・ 特定認証業務に係る本人確認に公的個人認証サービスが活用できること。

特定認証業務の概要

平成14年3月末現在、電子署名法に基づいて、6つの認証サービスが特定認証業務として認定されている（表4参照）。

これらのサービスを提供する事業者は、法人や個人が作成した公開鍵が本人のものであることを認証する電子証明書の発行及び当該公開鍵の有効性の確認に係る照会・回答等の業務を行っている。

表4 特定認証業務の認定状況

特定認証業務	認定認証事業者	認定年月日
Accredited Sign パブリックサービス ・電子証明書の発行 ・9,000円 / 証明書1枚	日本認証サービス(株)	H13.7.13
電子入札用電子認証サービス ・国土交通省が行う電子入札に参加するための認証サービス ・45,000円 / 新規1枚目	(株)帝国データバンク	H13.9.6
Accredited Sign パブリックサービス2 ・行政への電子申請に要する電子証明書の発行 ・9,000円 / 証明書1枚	日本認証サービス(株)	H13.10.19
(株)日本電子公証機構認証サービス iPROVE ・電子メール送信者の本人性及び電子メール電文の非改ざん性を第三者機関の立場から証明するサービス ・年間利用料 7,000円 / 1証明書	(株)日本電子公証機構	H13.12.14
日本行政書士会連合会認証サービス	日本行政書士会連合会	H14.3.1
C E C S I G N 認証サービス ・建設業における工事請負契約の電子化に必要な発注者、受注者への電子証明書の発行 ・利用料金 個別対応	(株)コンストラクション・イ ーシー・ドットコム	H14.3.26

(3) 商業登記に基礎を置く電子認証制度

企業間の取引では、相手方の企業の存在や代表権限の有無を確認するために、法務局の登記所が発行する法人代表者の印鑑証明書や資格証明書が利用されてきた。

商業登記に基礎を置く電子認証制度とは、これらの証明書に代わって、法人の登記情報に基づいて電子証明書を発行し、インターネットを利用した企業間の商取引や電子申請を円滑に実現するものである。

法務省では、「商業登記法」の一部改正を行い、平成12年10月10日から電子認証サービスの運用を開始している。

認証サービスの内容

管轄の法務局が電子証明書の発行申請の受付、申請者の本人確認を行い、電子認証登記所として指定された東京法務局の登記官が申請者に電子証明書を発行する。

会社の代表者の公開鍵を証明するほか、登記簿の情報に基づいて、一定の登記事項(会社の代表者であれば、商号、本店、代表者の資格、氏名)についても証明する。

利用条件

ア 利用者

商業登記法による企業の代表者、支配人、商号使用者及び他の法令により商業登記法の関係規定（第12条の2）が準用される法人（民法法人、特殊法人、協同組合等）の代表者で登記所に印鑑を提出した者

但し、代表権や代理権の範囲又は制限に関する登記がなされている者、民事再生法、会社更生法による管財人・保全管理人等は除く。

イ ソフトウェア

利用については、専用のソフトウェアを使用する必要がある。

ウ 手数料

電子証明書の証明期間3か月当たり 24,000円
（証明期間が1年の場合は96,000円）

（4）公証制度に基礎を置く電子公証制度

公証人役場では、契約や遺言などの文書の成立についての争いを防止するために、第三者である公証人が当事者の立ち会いのもとに、日付、氏名を記載し、職印を押印することにより、文書の成立の確定日付の付与や文書内容の確認等を行ってきた。こうした仕組みは公証制度と呼ばれている。

電子公証制度とは、従来の書面と同様、公証人が行っている証明（公証）を、電子文書についても利用できるようにすることであり、日本公証人連合会が平成14年1月15日から運用を開始している。

電子公証サービスの内容

公証人が紙の文書について行っている確定日付の付与や私文書の認証を、指定公証人が電子文書についても行うものである。

ア 電子確定日付の付与

公証役場には、確定日付印が備え付けられており、公証人が私人の署名又は記名押印のある文書（私署証書）にこの確定日付印を押印すると、その私署証書がその日付の日に存在したということが証明される。

電子確定日付の付与とは、インターネットを通じて企業が作成した電子文書（電子私署証書）に対しても、指定公証人が確定日付を付与したうえ、電子署名を行い、電子証明書を発行するものである。

イ 電子私署証書の認証

当事者が公証人の面前で文書に署名又は押印した場合やその署名、押印は自分が行ったものであると認めた場合、公証人はその文書（私署証書）は確かに本人が作成したものであるという認証を行っている。

電子私署証書の認証とは、電子文書に対しても同様の公証を行うものである。法人の代表者等は電子署名を行った電子文書（電子私署証書）を送信し、指定公証人はその電子文書を審査し、電子署名を行ったうえ、電子証明書を本人に発行する。

利用条件

ア 利用者

法人登記された企業であって、あらかじめ、法務省の「商業登記制度に基礎を置く電子認証制度」に基づいた電子証明書を取得している者。

イ ソフトウェア

利用については、専用のソフトウェアを使用する必要がある。

ウ 手数料

電子確定日付の付与は1件当たり700円、電子私署証書の認証は、1件当たり11,000円(原則)で、いずれも紙文書の場合と同額。

電子公証の動向

電子公証制度は、信頼できる第三者機関(TTP:Trusted Third Party)に電子文書の内容を保管し、後日、紛争が生じた場合に、文書の存在や内容を確認、証明できるようにすることにより、紛争の解決に役立てることを目的としている。指定公証人が行う公証サービスは、私署証書の認証や確定日付の付与であり、公正証書自体の電子化は検討課題となっている。

(参考) 公証人と公証業務

- 1 公証人とは、法務大臣が任命する公務員で、全国の法務局・地方法務局に所属し、管轄区域内の公証役場で執務している。
- 2 公証人は次のような公証事務を行っている。
 - 公正証書の作成
 - ・金銭や不動産の賃貸借契約、遺言などの内容を、公証人が当事者の面前で確認し、公文書として作成する。
 - ・金銭の貸借で債務者が支払いを怠った場合に、直ちに強制執行に服する旨の記載がされていれば、裁判に訴えなくても強制執行することが可能。
 - 確定日付の付与
 - ・文書が作成された日付を認証する
 - 認証
 - ・定款の認証
 - 会社の設立に際して作成する定款を公証人が審査し、認証を行うこと。
 - 公証人の認証を受けなければ定款は効力を持たない。
 - ・私署証書の認証
 - 個人や企業が署名又は押印した文書を、本人によって作成されたものであることを証明すること。

(5) 地方公共団体による公的個人認証サービス

住民が国や自治体に電子申請を行う場合に必要な電子証明書が、全国どこの地域にあっても低廉な費用で利用できるようにするため、市町村が申請者の本人確認を行い、都道府県が申請者の公開鍵に係る電子証明書を発行する公的個人認証制度が平成15年度に導入される予定である。

このため、総務省では、「電子署名に係る地方公共団体の認証業務に関する法律案(仮称)」を整備することとしている。

また、民間認証事業者が行う特定認証業務にかかる本人確認の手段としても活用し、電子商取引の活性化にも役立てることをめざしている。

利用者

- ・住民基本台帳に記録されている住民を対象とする。
- ・住民は、市町村の窓口を設置されたパソコンにより、公開鍵と秘密鍵を生成し、電子証明書の発行申請を提出する。
- ・市町村の窓口で、県知事から電子証明書の交付を受け、ICカード等に格納する。

市町村長

- ・住民からの電子証明書の発行申請を受け付ける。
- ・申請者の「氏名、出生の年月日、男女の別、住所」を住民基本台帳ネットワークシステム等により、本人の実在を確認する。
- ・電子証明書の発行申請と公開鍵を総合行政ネットワークを通じて県あてに送信する。
- ・県から受信した電子証明書を申請者に交付する。

都道府県知事

- ・市町村長から総合行政ネットワークを通じて、電子証明書の発行申請を受け付ける。
- ・市町村長あてに総合行政ネットワークを通じて、電子証明書の発行を行う。
- ・電子証明書の失効情報の管理を行い、署名検証者からの照会に対応する。

署名検証者(住民から電子証明書を受け、本人確認を行う機関)

- ・国・地方公共団体
住民から電子申請を受け付ける際、申請者の電子証明書の有効性を確認する。
- ・特定認証業務を行う認定認証事業者
特定認証業務を利用する個人が、当該認定認証事業者から電子証明書の発行申請を行う場合、認証事業者は申請者の本人確認を行うため、申請者から送信される知事の電子証明書の有効性を確認する。

(6) 行政機関における組織認証制度

行政手続の電子化については、申請者の本人確認ができる仕組みと同時に、行政機関においても、大臣や知事など一定の権限を有する官職から発信されたものであることが確認できる仕組みが必要となる。

こうした行政機関側の官職を証明する仕組みが政府認証基盤(GPKI:Government Public Key Infrastructure)あるいは地方公共団体認証基盤(LGPKI:Local Government Public Key Infrastructure)と呼ばれるものである。

組織認証基盤の機能

国の各府省や地方公共団体がインターネットを介して、申請者に公文書を送信する場合、従来の書面での大臣や知事等の公印を押印することに代えて、大臣や知事等の秘密鍵で電子署名を行い、その官職を証明する電子証明書を添付して申請者に送信する。

申請者は、電子証明書により行政機関からの通知であることを検証し、電子申請が確実に行えるのである。

組織認証基盤の法的根拠

電子署名を行った電子文書の成立の推定効果を認める電子署名法3条の規定は、私文書が対象であり、公務員が職務上作成した公文書は除かれている。行政機関の電子署名は、法律ではなく、規則で規定されている。

ア 公文書の成立の推定

一般に公文書は私文書と比較して、文書の成立・内容ともに真正であるとの強い推定が働き、相手方が虚偽だという立証をしない限り、この推定は破れない。

民事訴訟法では公文書の成立について、「文書は、その方式及び趣旨により公務員が職務上作成したものと認めるべきときは、真正に成立した公文書と推定する。（第228条第2項）」と規定されているように、私文書の場合に必要とされる署名又は押印は必ずしも必要とはされていないのである。

イ 公印と電子署名規定

通常、公文書には公印が使用されているが、一方で「公印省略」の公文書も数多く発出されている。公印自体は公文書の成立要件や効果発生要件ではなく、その成立について争いが生じた場合に有力な証拠となるものである。

したがって、公印の根拠は法律ではなく規則で定められている（例：「国の行政機関において使用する公印の形式、寸法等に関する規則」）。ただ、行政機関の意思を明確にするためには、電子的な公文書については電子署名を行うことを規則で定めることが望ましい。総務省や経済産業省では、自らの組織の官職証明書を発行する認証局の設置とあわせて、電子的な公印となる電子署名の根拠規定を置いている。

認証局の設置

ア 各府省の認証局

各府省では大臣等の官職の秘密鍵や公開鍵を生成し、その公開鍵が真に大臣等のものに間違いのないことを証明する電子証明書を発行するため、認証局を設置している。平成13年度は、総務省、経済産業省、国土交通省の3省で設置されている。

イ ブリッジ認証局

国民が各府省からの電子文書に付される電子証明書の有効性を確認するため、総務省が各府省の認証局を相互に結ぶブリッジ認証局を設置している。

ウ 地方公共団体認証局

地方公共団体の組織認証基盤については、総合行政ネットワークの整備の一環として、各団体ごとの認証局が設置される。

認証局の運用管理については、各団体で規則・規定を整備する。

5. 電子認証の普及のための課題と提言

(1) 利用者の視点にたった電子認証の普及

電子認証が電子商取引や行政手続の電子化に不可欠な役割を担う社会インフラとして普及するためには、多くの課題がある。ここでは、技術面ではなく、実際に電子認証を利用する利用者に視点にたって、今後の電子認証の普及に求められる課題と提言を取りまとめた。

電子認証について理解を深めるための普及啓発

公開鍵暗号方式を用いた電子認証の仕組みや電子署名法などの制度は、複雑であり、専門家でなければ理解することは難しい。今後、電子署名や電子認証が電子商取引や電子申請の基盤として、社会に普及し、利用されるためには、電子認証というものがどういうもので、どのような処理を行い、どのようなサービスをするものかを、インターネットを利用する人にはもちろん、インターネットに興味のない人、また仕事の上で認証を使わなければならない人に対して、十分に理解してもらえような周知啓発を進める必要がある。

総務省や経済産業省、法務省などのホームページには、電子署名・電子認証の情報は提供されており、電子署名法に基づく調査機関である（財）日本品質保証機構では普及啓発セミナーの開催も行われているが、広範なPRはされておらず、企業や自治体に認知されていないのではないかとと思われる。

このため、地域の情報化推進団体である兵庫ニューメディア推進協議会や電子自治体の構築をめざして県と県内市町で設立された兵庫県電子自治体推進協議会で、電子署名・電子認証についてわかりやすく理解できるような普及啓発事業に積極的に取り組むことが求められる。

電子認証の利用実態調査と情報の開示

電子認証は電子商取引の実現に必要な基盤ではあるが、はたして現実の電子商取引で認証事業者の電子認証サービスは利用されているのだろうか。

研究会では、民間事業者の認証サービスや商業登記に基づく法務省の認証サービスは、企業にはほとんど利用されていないのではないかという講演や意見が大半であった。民間分野で電子認証が利用されていなければ、平成15年度に導入が予定されている公的個人認証サービスも仕組みはできても使う人がいないということになりかねない。

電子認証が普及していないのが実態なら、その理由は何か。利用するニーズが現時点では少ないのか、電子認証を組み込んだ電子申請などのシステムが構築されていないからか。あるいはコストが高いからなのか。今回の研究会では十分な分析はできなかったが、今後、電子認証の普及のためには、現在の利用実態を明らかにする調査の実施と情報の開示が不可欠である。

総務省では、平成14年4月に「電子認証ビジネス市場規模調査」の結果をインターネットで公表している。それによると、平成13年度の電子認証ビジネスの市場規模は約63億円であり、平成18年度には約420億円にまで拡大すると予測している。特に、電子政府の取り組みは電子認証ビジネスの市場拡大に大きく貢献し、電子政府の要因を考慮しない場合に比べて、その効果は約2.5倍になると推測している。

私たちが知りたいのは、また、今後の電子認証を考えるうえで重要なことは、将来予測ではなく、普及のためにネックになっているは何なのかを明らかにすることである。総務省では、企業のヒアリングも行っているが、その内容は公表扱いにはなっていない。

いない。

電子認証が今後の情報社会のあり方に大きなインパクトを持つことを推測するのであれば、より綿密な課題調査と情報の開示を行い、認証サービスを提供する認証事業者や国の行政機関とサービスの利用者である住民、企業、地方公共団体との情報の共有化を行い、広く議論できる場を持つことが求められる。

利便性の高い電子認証サービス

電子認証は、インターネットで取引を行っている者や今後取引しようとする人にとって必要となる仕組みであり、取引上のトラブルが解消されることも期待されるであろう。

しかし、利用するにあたって、細かな制限や条件があれば、今まででは考えられないトラブルが発生することも考えられるのではないか。安価な費用で、利用しやすく、かつ、仕組み自体が簡易で、全体が見渡せるような明瞭なものでないと、利用も進まずに、普及促進につまずくことにもなる。

特に、公的個人認証サービスを考える場合、高齢者や障害者にとっても使いやすいサービスを提供する必要がある。行政はそれに対してどのような対応を実施していくのか、制度ができた後に推進体制を整えるのではなく、国の各府省、自治体や各種団体とで十分な情報交換を行い、事前に具体的な対応を検討する必要がある。

また、現在、一般的な身分証明として使われている運転免許証や官公庁が発行する写真入りの各種許可証などの取り扱いも今後変えていくのか、認証システムとあわせて検討すべき課題の一つだろう。

技術先行で電子認証の器ができて終わりでは、「仏作って魂入らず」になりかねない。行政側だけの達成感に終始してしまわないことに留意すべきである。

低廉な利用料

利用のしやすさとも関連するが、電子認証という仕組みを利用するに当たっては、低廉な利用料でないと普及しない。

現在のように年間数万円も必要な認証サービスを果たして利用するだろうか。公開鍵暗号方式は高度なセキュリティが伴い、制度の運営や維持には高額な費用を要するとしても、利用者に高額な負担を求めると、普及はしないだろう。

例えば、「高速道路における料金自動精算システム（ETC）」は、実用開始1年間の状況で普及が2%と利用が進んでいない原因として、自動車側に設置する機器（価格は約3～5万円）を利用者の負担にしていることがあげられている。同様のシステムが米国では、リースでの対応で機器を返還すると費用も還付され、利用率は7割を超える道路もあるといわれている。

このような事例から考えてみても、認証における利用者の負担が普及率に大いに関わってくるのではないか。現在の経済事情では、利用者の負担が安価でないと、普及促進を図ることは難しい。利用者が負担すべき利用料については、現行の印鑑登録証明書等の手数料等を基準に考えていく必要があるだろう。

総務省では、平成14年度に公的個人認証サービスの実証実験を行う予定であり、制度の構築に必要な運用費の試算や利用料の検討も進められているが、自治体や利用者側が納得できるよう検討内容の情報を公開し、できるだけ利用者の負担が軽減されるような制度化を行うことが求められる。

セキュリティの確保

電子認証システムの運営に当たっては、住民や企業の権利・義務、財産に関わる情報を取り扱うことから、運用管理者には万全のセキュリティ対策を講じることが求められる。

また、利用者についても、秘密鍵や公開鍵証明書等についての管理意識をいかに高めていくのが重要な課題となる。これについては、容易なように思われて、かなり難しい問題ではないかと思われる。認証サービスが十分に普及しておらず、利用者も使い慣れない状況では、秘密鍵を格納するICカード等の紛失や再発行などの事例が多発するのではないか。

特に、公的個人認証サービスの普及には、住民に対するきめ細かな普及啓発を十分に行う必要がある。その際、サービスの利用方法だけでなく、個人情報保護や住民基本台帳ネットワークシステムとの関係など、利用者の信頼が得られるような制度の構築と普及啓発を進めることが必要である。

(2) 利便性の高い電子申請システムの構築

研究会では、電子認証を基盤とするアプリケーションシステムとして、さまざまな電子申請システムの事例を調査したが、必ずしも効率的なソリューションが実現されているとは言えない。書面からネットワークへの単なる置き換えだけでなく、申請手続の簡略化や効率化を進める必要がある。

利用者の視点にたった電子申請システムについての課題と提言を取りまとめた。

手続の標準化

同じ行政手続でも、自治体によって申請様式や審査の運用基準、添付書類、実印の要・不要など取り扱いが異なる場合が多いと思われる。実務面で具体的にどのように取り扱いが違うのか、どの手続で自治体間の取り扱いが異なるのか、十分な実態調査が不足している。研究会で行われたプレゼンテーションでも、具体的な自治体の事例をもとに、どのようにシステムの標準化をしていくべきか方向性は明らかではなかった。

例えば、電子申請システムの構築に当たっては、利用者の利便性を高めるために、少なくとも個人データに関連する項目のタグの名称は行政機関の間で統一しなければいけないが、従来の様式における項目名称と電子申請でのタグ名称が異なった場合、混同から間違いが生じる可能性がある。

システム化の目的は、こうしたつまらない事故を未然に防ぐためのものであり、より細かな調査と対策の検討が望まれる。また、こうした事実をソフト開発企業に早急に公開するべきである。

利用者への対応・サポートセンターの設置

電子申請は現行の書面による手続と併用されるが、各手続における電子申請の手順やトラブルなど、役所の担当窓口への問い合わせはかなり多いと予想される。

電子申請の利用方法だけでなく、パソコンやネットワークのトラブルの問い合わせも想定されるが、行政機関はどう対応していくのか。窓口担当者の対応が問われるが、パソコンやネットワークの基礎知識を始めとして、基本的な問い合わせへの対応やそれに伴う職員の研修も行う必要がある。

こうした対応を行うため、電子申請に伴うサポートセンターを各地区に設置して対応していく必要があるのではないか。あわせて、ホームページに住民からの質問に対する回答(FAQの設定)や電子申請の利用案内機能の充実が必要となる。

代理申請の利用

手続の標準化がされ、利用しやすい電子申請システムが実現しても、パソコンなどの情報機器になじめない人もおり、誰もが利用できるシステムは難しい。

こうした場合、簡単に申請代行を依頼できる窓口があれば利用者にとって利用しやすいものとなる。例えば、全国行政書士会などで、さまざまな手続きについて各地区の行政書士が相互に連絡しながら手続きを完了できるような仕組みができれば、システムの普及が進むのではないか。電子申請システムの画面上で代行者の欄を設け、そこにIDとパスワードを入力すれば、本人代行で申請ができる仕組みである。

電子申請を誰もが利用できるような仕組みを作ることは今後の重要な課題である。

XMLを活用した事務処理システム

総務省では、汎用電子申請システムの標準仕様で、申請書をホームページに提供する際に用いる技術として、記載漏れのチェックやデータ相互の突合が容易に可能なXML (eXtensible Markup Language) を推奨している。

今後、行政機関が利便性の高い電子申請システムを構築するうえで、XMLがより安価なコストで利用できるよう民間事業者の努力が求められるとともに、行政内部での事務処理を効率的に進めるため、ワークフローに基づいた事務処理システムにも活用を進めることが求められる。

(参考)

(1) 参考条文

民事訴訟法(平成八年六月二十六日法律第九号)

(文書の成立)

第二百二十八条 文書は、その成立が真正であることを証明しなければならない。

2 文書は、その方式及び趣旨により公務員が職務上作成したものと認めるべきときは、真正に成立した公文書と推定する。

3 公文書の成立の真否について疑いがあるときは、裁判所は、職権で、当該官庁又は公署に照会をすることができる。

4 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。

5 第二項及び第三項の規定は、外国の官庁又は公署の作成に係るものと認めるべき文書について準用する。

電子署名及び認証業務に関する法律(平成十二年五月三十一日法律百二号)(抄)

(定義)

第二条 この法律において「電子署名」とは、電磁的記録(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であつて、電子計算機による情報処理の用に供されるものをいう。以下同じ。)に記録することができる情報について行われる措置であつて、次の要件のいずれにも該当するものをいう。

- 一 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
- 二 当該情報について改変が行われていないかどうかを確認することができるものであること。

(電磁的記録の真正な成立の推定)

第三条 電磁的記録であつ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、当該電磁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及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。

商業登記法(昭和三十八年法律第二百五号)(抄)

(印鑑証明)

第十二条 第二十条の規定により印鑑を登記所に提出した者、支配人又は民事再生法(平成十一年法律第二百五号)若しくは会社更生法(昭和二十七年法律第七十二号)による管財人若しくは保佐管理人でその印鑑を登記所に提出した者は、手数料を納付して、その印鑑の証明書の交付を請求することができる。

2 (略)

(電磁的記録の作成者を示す措置の確認に必要な事項等の証明)

第十二条の二 前条第一項に規定する者(以下この条において「印鑑提出者」という。)は、印鑑を提出した登記所が法務大臣の指定するものであるときは、この条に規定するところにより次の事項(第二号の期間については、法務省令で定めるものに限る。)の証明を請求することができる。ただし、代表権の制限その他の事項でこの項の規定による証明に適しないものとして法務省令で定めるものがあるときは、この限りでない。

- 一 電磁的記録(電子的方式、磁気的方式その他人の知覚によつては認識することができない方式で作られる記録であつて、電子計算機による情報処理の用に供されるものをいう。)に記録することができる情報が印鑑提出者の作成に係るものであることを示すために講ずる措置であつて、当該情報が他の情報に改変されているかどうかを確認することができる等印鑑提

出者の作成に係るものであることを確実に示すことができるものとして法務省令で定めるものについて、当該印鑑提出者が当該措置を講じたものであることを確認するために必要な事項

- 二 この項及び第三項の規定により証明した事項について、第八項の規定による証明の請求をすることができる期間
- 2 略
- 3 第一項の規定により証明を請求した印鑑提出者は、併せて、自己に係る登記事項であつて法務省令で定めるものの証明を請求することができる。
- 4 略
- 5 第一項及び第三項の規定による証明は、法務大臣の指定する登記所の登記官がする。ただし、これらの規定による証明の請求は、第一項の登記所を経由してしなければならない。
- 6 略
- 7 第一項の規定により証明を請求した印鑑提出者は、同項第二号の期間中において同項第一号の事項が当該印鑑提出者が同号の措置を講じたものであることを確認するために必要な事項でなくなつたときは、第五項本文の登記所に対し、第一項の登記所を経由して、その旨を届け出ることができる。
- 8 何人でも、第五項本文の登記所に対し、次の事項の証明を請求することができる。
 - 一 第一項及び第三項の規定により証明した事項の変更（法務省令で定める軽微な変更を除く。）の有無
 - 二 第一項第二号の期間の経過の有無
 - 三 前項の届出の有無及び届出があつたときはその年月日
 - 四 前三号に準ずる事項として法務省令で定めるもの
- 9 第一項及び第三項の規定による証明並びに前項の規定による証明及び証明の請求は、法務省令で定めるところにより、登記官が使用する電子計算機と請求をする者が使用する電子計算機とを接続する電気通信回線を通じて送信する方法その他の方法によつて行うものとする。

公証人法（明治四十一年四月十四日法律第五十三号）（抄）

- 第一条 公証人ハ当事者其ノ他ノ關係人ノ囑託ニ因リ左ノ事務ヲ行フ権限ヲ有ス
 - 一 法律行為其ノ他私権ニ関スル事実ニ付公正証書ヲ作成スルコト
 - 二 私署証書ニ認証ヲ与フルコト
 - 三 商法第百六十七条及其ノ準用規定ニ依リ定款ニ認証ヲ与フルコト
 - 四 電磁的記録（電子的方式、磁気的方式其ノ他人ノ知覚ヲ以テ認識スルコト能ハザル方式（以下電磁的方式ト称ス）ニ依リ作ラルル記録ニシテ電子計算機ニ依ル情報処理ノ用ニ供セララルルモノヲ謂フ以下之ニ同ジ）ニ認証ヲ与フルコト但シ公務員ガ職務上作成シタル電磁的記録以外ノモノニ与フル場合ニ限ル

- 第七条ノ二 本法及他ノ法令ニ依リ公証人ガ行フコトトセラレタル電磁的記録ニ関スル事務ハ法務大臣ノ指定シタル公証人（以下指定公証人ト称ス）之ヲ取扱フ
 - 2 前項ノ指定ハ告示シテ之ヲ為ス
 - 3 第六章ノ規定ハ本法及他ノ法令ノ定ムルトコロニ依リ指定公証人ガ行フ電磁的記録ニ関スル事務ニ付テハ之ヲ適用セズ
 - 4 本法ニ規定スルモノノ外指定公証人ガ行フ電磁的記録ニ関スル事務ニ付テハ法務省令ヲ以テ之ヲ定ム

(2) 電子認証サービス一覧

区 分	実施主体	利用者	認証サービスの概要	備 考
電子認証サービス (電子署名法による 特定認証業務等)	民間認証事業者	企業、個人	<ul style="list-style-type: none"> 日本認証サービス株式会社の「AccreditedSignパブリックサービスタイプ2」などが特定認証業務として認定されている。 国の各府省や自治体に電子申請等を行う個人に対して本人確認のための電子証明書を発行する。 	<ul style="list-style-type: none"> 電子署名法により特定認証業務の認定が行われており、政府認証基盤と相互認証が認められている。 手数料 証明書1枚 7,000円～45,000円
商業登記に基礎を 置く電子認証制度	法務局	法人登記した企業	<ul style="list-style-type: none"> 電子認証登記所として指定された法務局の登記官が、従来の法人代表者の「印鑑証明書」や「資格証明書」に代わる「電子証明書」を発行する。 	<ul style="list-style-type: none"> H12.10.10から運用開始 手数料 証明書3ヶ月当たり 24,000円
公証制度に基礎を 置く電子公証制度	日本公証人連合会	商業登記に基づく電子認証のサービスを利用する企業 (個人は対象外)	<ul style="list-style-type: none"> 現行の公証制度に基礎を置き、指定公証人がインターネットを通じて電子文書(契約書等)に対する電子確定日付の付与、電子私署証書の認証等の公証サービスを提供する。 公正証書の電子化は、今後の検討課題 	<ul style="list-style-type: none"> H14.1.15から運用開始 手数料(紙文書と同額) 電子確定日付の付与 700円/件 電子私署証書の認証 11,000円/件
公的個人認証サービス	地方公共団体 市町村:本人確認機関 都道府県:証明書発行	住民基本台帳に登録された住民	<ul style="list-style-type: none"> 行政機関に対する電子申請を行う個人に対して、本人確認に必要な電子証明書を発行する。 認定認証事業者の特定認証業務を利用する個人に対して、当該申請に係る本人確認に必要な電子証明書を発行する。 	<ul style="list-style-type: none"> H15に運用開始予定 証明書の有効期間は3年間(予定) 利用者の負担は実費相当額(予定) 署名検証者(行政機関、特定認証業務を行う民間認証事業者)には適切な受益者負担(予定)
政府認証基盤 (GPKI)	各府省	各府省の大臣等の官職	<ul style="list-style-type: none"> 国の各府省に電子申請等を行う個人が、府省からの結果通知の発出者を確認できるよう府省の大臣等の官職を証明する。 	<ul style="list-style-type: none"> H13に総務省、経済産業省、国土交通省が認証局を設置
地方公共団体認証 基盤(LGPKI)	都道府県、市町村	都道府県、市町村の首長等の官職	<ul style="list-style-type: none"> 自治体に電子申請等を行う個人が、自治体からの結果通知の発出者を確認できるよう自治体の首長等の官職を証明する。 	<ul style="list-style-type: none"> H13に都道府県、政令市の認証局を設置 H15までに全自治体の認証局を設置 総合行政ネットワークの整備の一環として整備

(3) 用語集

- ・建設 CALS

公共工事実施に際して、業務上必要な情報を標準化・電子化して共同利用することにより工程短縮、コスト軽減及び品質の向上を実現することを目的として、設計、入札、契約、施行及び維持管理において IT を活用すること。

- ・ファイヤーウォール

インターネットからの不正な侵入を防ぐための機能を持つ製品。社内ネットワークと外部（インターネット）との間に設置する。サーバー搭載型のソフト製品のほか、ハード一体型製品など様々な種類の製品がある。

- ・デジタル署名

電子文書を代表するデータを特定のアルゴリズムと特定の鍵により変換すること。デジタル署名のデータを検証することにより、変換した時の鍵を特定することができる。またデジタル署名のデータ作成後、電子文書が改ざんされていないことを確認できる。

- ・ワンタイムパスワード

携帯型専用装置等で生成した 1 回限り有効なパスワードを指す。

- ・PKI

公開鍵暗号基盤(Public Key Infrastructure)を指し、公開鍵暗号方式を用いた電子証明書を活用したセキュリティ基盤である。PKI という場合には、単に公開鍵暗号方式の暗号システムを指すのではなく、電子証明書、認証局、リポジトリなどの技術要素を含める。

- ・SSL

Secure Sockets Layer の略。Web ブラウザと Web サーバが完全にデータをやりとりするための機能。米ネットスケープコミュニケーションズが開発。ブラウザの身元を確認する公開鍵暗号方式とデータを暗号化する秘密鍵暗号方式を使う。

- ・ハッシュ関数

デジタル署名を行う際の署名処理の効率化を行うために、署名対象データの圧縮に使用するものである。任意の長さのデータを固定の長さのデータに変換するものであり、変換された値はハッシュ値またはメッセージダイジェストと呼ばれる。また一方向性関数とも呼ばれ、ハッシュ値からメッセージへ逆算するのが困難である。

(4) 参考文献

・「電子認証が日本を変える」生産性出版
日本総合研究所編、宮脇訓晴、加藤研也著
ネットワーク社会における電子認証のあり方、電子認証を基盤としたビジネスモデルの構築を提唱している。

・「電子政府・電子自治体入門」発行：ぎょうせい
NEC電子行政推進新プロジェクト編集
電子政府・電子自治体の背景・課題、システムの動向などを簡潔にまとめている。

・「電子行政の法務知識」発行：ぎょうせい
NTTデータ情報化法制度研究会編集
電子申請に伴う法制度面の課題をまとめている。

・「PKI 公開鍵インフラストラクチャの概念、標準、展開」
発行：ピアソンエデュケーション
著者：カーライル・アダムズ/スティーブ・ロイド
訳：鈴木優一

・電子署名法の URL
<http://www.meti.go.jp/policy/netsecurity/digitalsign.htm>

・商業登記に基礎を置く電子認証制度
・公証制度に基礎を置く電子公証制度
<http://www.moj.go.jp/>

・政府認証基盤
<http://www.gpki.go.jp/>

・公的個人認証サービス
http://www.soumu.go.jp/s-news/2002/020228_3.html

・電子署名・認証ハンドブック
<http://www.jqa.or.jp/j/esaec/esaec.html>

(財)日本品質保証機構は、電子署名法に基づく指定調査機関として、特定認証業務の認定に伴う調査を実施するほか、電子署名・認証に関する技術調査や普及啓発事業を行っている。