電子認証サービスの現状と課題

Digital Certificate Service in Japan

椿　　康和
Yasukazu Tsubaki

要　約

電子商取引の広がりと電子政府化の進展により，ネット上の取引や届出・回答の当事者が本人であることの証明と，電子化書類の真正性の保証を行う電子認証の普及が大きな課題となっている。技術面では公開鍵暗号方式による認証基盤（PKI）が一般的な方法として確立してきており，それを基礎とした電子認証サービスについては，民間事業者に対する認定制度，法務局の登記所や公証人によるサービスの開始，政府の認証局の設置などが相次ぐなど，制度整備も進展している。電子認証サービスの市場規模はまだ小さいものの，今後，企業間取引の電子化と電子政府化の進展により，法人・団体向けについては，市場の拡大と付加的なサービスを含めた種々の認証ビジネスの展開が進むことが推測される。これに対し，個人向けの認証サービスの普及にあたっては，現状ではいくつかの課題がある。

1．はじめに

コンピュータベースでのサービス利用に関する本人認証は，主としてIDとパスワードが用いられてきた。ネットワークのオープン化や電子商取引の広がり，官公庁への届出とそれに対する結果通知を電子化する電子政府化の進展などにより，ネットワーク上で行われる取引や届出・回答の当事者が主張されているような本人であることを証明する本人認証と，電子化された書類の真正性を保証する，信頼性の高い電子認証技術の普及が大きな課題となってきた。

それまで少数の民間企業によるビジネスとして行われてきた電子認証サービスは，政府のe-Japan政策の一環として，法的な制度整備が急速に進展し，平成13年度からは民間事業者に対する認定制度の新設に加え，法務局の登記所や公証人によるサービスも開始された。また，政府職員の真正性を保証するための政府自身の認証局の設置も開始されている。さらには，平成14年6月には，地方公共団体による公的な個人認証サービス制度の創設を目的とした法案が国会に提出された。

電子認証サービスを事業としてとらえたときの市場規模は，わが国全体でまだ30億円強にすぎないが，今後の企業間取引の電子化や中央省庁の電子政府化により，企業向けの電子認証サービスに対する需要は拡大し，認証をベースにした付加的なサービスへと広がることが期待されている。しかし，その一方で，特に個人の利用における電子認証サービスの必要性の度合いや，認証局や認証システムの信頼性などの運用に係る問題も多い。本稿では，電子認証に関する制度や事業展開の現状とその課題について検討する。

2．電子認証のしくみ

2.1．認証

商取引を始めとする社会的なサービスは，店舗での現金による購入のように，利用資格に何ら制限を設けないものと，会員制サービスのように，何らかの制限を設けるものとに大別される。後者の場合，会員証などの手段によって，正当な利用者であることを確認するプロセスが伴う。サービスの受益だけでなく，各種の業務遂行にあたっても同様に，資格の有無を問われる場合とそうでない場合がある。

正当な利用者や業務遂行者であることを何らかの形で証明する行為を認証という。認証には，利用資格の有無だけを確認するものから個人を厳密に特定化するものまで，精度において種々のレベ

ルがある。個人を特定化する認証では，通常，本人が事前に登録あるいは届出しておいた情報と，認証時に提示された情報とを照合して，対象者が登録や届出を行った本人であることを確認する手順をとる。これを本人認証という。

コンピュータによるサービス提供にあたっては，人間同士の直接の対面的環境ではなく，ネットワークを介して人と機械がやりとりする非対面的環境の下で認証が行われる。そこにおける認証機能は，マン＝マシンシステムにおける基本的なインターフェース構成の一部として組み込まれることになるが，高度なサービスを安全に提供するために，確実で精度の高い本人認証のシステムが必要とされている。

2.2. 本人認証の目的と手段

本人認証は，サービス提供の前提条件の確認に行われるものであり，それ自身が目的ではない。アプリケーションを提供するサービスの視点で，本人認証の主な目的を示すと，次の3つが挙げられる。

(1) アクセス権や利用権の管理

各種サーバの利用，機密情報や私的情報を収めたファイルの閲覧，銀行口座へのアクセス，特定の場所への立ち入りなど，情報や場所へ対するアクセス権を管理する。

(2) トラッキング

商品やサービスの購入，サーバ上で行った作業，通信，部屋への出入りなど，「誰が，どこで，何をしたか」をその都度記録し，必要に応じて後で確認できるようにする。これにより，従来，押印やサインで行ってきた，取引や作業者の責任を明確にすることが可能となる。

(3) 使用者認識

共用の端末機器の使用やデータベースへのアクセス時において，予め登録された利用者の個々の属性（プロファイル）に応じた環境を提供するためのカスタマイズを行う。イントラネットにおける組織内ポータルの運営などにも適用できる。

このうち，(1)，(2)は主としてセキュリティの維持を目的とし，(3)はサービス内容の差別化・高度化を狙いとするものである。

本人認証に用いられる主な手段には次のようなものがあり，必要とされるセキュリティの水準に応じて，単独あるいは複数の組み合わせで用いられる。

(1) 知識による認証

知識による認証は，「何を知っているか」という情報を手段として，予め登録された情報と提示された情報との照合で行われる。これには，パスワードや暗証番号のような基本的に本人しか知り得ない「秘密」の情報を用いる。利用されるネットワーク環境が専用線による閉じたものから，インターネットなどのオープンな環境に移行するにつれて，通常のパスワードでは盗聴に対して無力になってきた。このため，暗号化されたパスワードや，使う度に捨て去る方式のパスワード（ワンタイム・パスワード）が用いられるようになっている。

(2) 所有物による認証

パスポートや身分証明書，クレジットカードや会員証など，所有物による本人認証はコンピュータ以前から広く利用されてきた。この方式では，本人であることを証明する「もの」－これにはその中に記録された情報を含む－を，認証主体や第三者が発行し，それを所持する者を本人とみなしている。しかし，知識による認証に比べ，盗難や遺失，偽造によって他人に成りすまされるリスクが大きくなる。このため，パスポートやICカードのように媒体そのものを複製や偽造が困難にする，身分証明書のように顔写真のような補完的情報を追加する，暗証番号のように知識による認証と併用する，などの対策が講じられている。

(3) 生体情報による認証

生体情報による認証は，人間の外見的な特徴である，指紋，虹彩，掌紋などで個人を識別する。これらの特徴は，人により必ず異なっていることについて科学的な裏づけが必要とされ，また，それが示すパターンが基本的に変化し難いものであることも要求される。音声や署名も広い意味での生体情報に分類されるが，恣意的に変化させることが可能であり，それによる成りすましを排除する必要がある。

生体情報による認証は，他の手段に比べ本人情報の偽造が困難であり，何も覚えずに，また持たずに認証できるというメリットがあるが，識別に用いられる装置の普及が遅れていることもあり，現時点では，特に厳重なアクセス制限を課す必要

があるところなどに使用範囲が限られている。

2.3. 公開鍵基盤

ネットワークを介した電子的な取引では，上述の本人認証とともに，送信されてきたデータ（電子文書）の内容が，途中で改ざんされたものではない原本そのものであることも，合わせて確認する必要がある。

紙媒体の文書の場合，その真正性を保証する手段として自筆の署名が用いられるが，電子文書の場合には，署名も電子的に行われる。この電子署名とは，署名者（送信者）だけが行いうる処理をメッセージに対して行い，受信者側でそれを検証することである[1)]。

電子署名を行う一般的な手段として，公開鍵暗号方式（public key cryptosystem）が用いられる[2)]。公開鍵暗号方式では，送信者は誰でも利用できる受信者の公開鍵を用いて暗号化し，それを受信者宛てに送る。受信者は自身しか知らない秘密鍵で暗号文を復号する。電子署名は，この暗号方式における公開鍵と秘密鍵の役割を逆にする。すなわち，送信者は自分の秘密鍵を用いて送信メッセージを暗号化し，それを電子署名として送る。受信側は電子署名を送信者の公開鍵で復号する。送信者の公開鍵以外では復号できないので本人認証が可能である。

実際には，送信メッセージ全体を暗号化すると処理コストが高くなるため，メッセージからダイジェストと呼ばれる小さなサイズの電子情報を生成し，これを暗号化して送信する[3)]。受信側は受け取ったメッセージからダイジェストを生成し，復号したものと照合する。両者が一致すれば，署名者によって署名され，かつ通信途中の改ざんが行われなかったことが証明され，内容の正当性が確認される。

電子署名の主な機能をまとめると，以下のようになる。

(1) 保　証

ネットワークを経由した利用者が本人であることを，第三者機関が他の利用者に対して保証する。

(2) 完全性

改ざんを検出することができるため，送信されたデータが改ざんされていないことを保証する。

(3) 秘　匿

送付先の公開鍵で暗号化された情報は，本人の秘密鍵のみで復号可能なため，特定の相手にのみ内容を読み取ることを認める。

(4) 否認防止

注文を実際にしておきながら，後でそれを否定することを否認という。電子署名を施した電子文書では，本人の秘密鍵が漏洩していない限り，送信者が本人であることの証明が容易であり，否認の防止に効果がある。

2.4. 認証局

電子署名だけでは本人認証を完全には行いえない。使用されている公開鍵が，本当に送信者本人のものであるとの確認が別途必要である。

例えば，不正利用者Bが利用者Aになりすまして，公開鍵BをAの公開鍵として開示し，さらに，その公開鍵に対応した秘密鍵Bで電子署名を行って第三者へ送付したとしよう。この場合，受け取った側が，開示された公開鍵Bを利用者Aの公開鍵として認識して使用すると，不正利用者Bを利用者Aと認証してしまうことになる。

このように，公開鍵とその所有者との対応関係は自動的に信頼できるものではない。このため，印鑑証明制度と同様に，送信者と送信者の公開鍵との関係を証明する第三者機関が必要となる。これを認証局（Certification Authority, CA）という。

認証局は，申請者本人を確認した上で認証データベースに登録し，申請に応じて公開鍵とその所有者との対応関係を証明する電子証明書（公開鍵

1）電子署名と類似の用語にデジタル署名（digital signature）があるが，ここでは同義として扱う。

2）暗号方式は鍵の種類により秘密鍵方式と公開鍵方式に大別される。秘密鍵方式は，送信者と受信者とで共通の鍵を用いて暗号化と復号を行うもので，共通鍵，あるいは対称鍵暗号とも言われる。古くから使用されてきたこの方式は，通信相手ごとに複数の鍵を管理する必要があり，不特定多数との取引にあたり，その内容を暗号化するには適していない。これに対し公開鍵方式は，非対称鍵暗号とも呼ばれ，一般に公開した公開鍵（public key）と本人自身しか知らない秘密鍵（private key）のペアを使って暗号化と復号を行うため，鍵の管理が容易である。公開鍵から秘密鍵を導出することは非常に困難であることが数学的に証明されており，これによって初めて実現可能となった。

3）この変換は，ダイジェストから元のメッセージを復元できない一方向関数を用いて行う。

証明書）を発行する[4]。公開鍵証明書には認証局の電子署名が付されており，送信者は，データに自分の電子署名とこの電子証明書を付けて送る。受信者は受け取った電子署名の検証にあたり，認証局に対して，発行した電子証明書の有効性を確認する。

認証局はさまざまな組織が運営することが可能である。私企業が有料で証明書を発行する場合もあれば，政府機関や企業が業務遂行のために，その職員を認証する，印鑑証明のように自治体が住民を対象として発行する，企業が顧客サービスの一環として行うなど，それぞれの目的に応じた運営がありうる。また，利用する側も目的に応じた認証局を利用することが考えられる。

このような，本人認証や文書の真正性の証明など，電子取引や電子文書の利用に係るセキュリティを維持する仕組みを認証基盤と総称する。その中でも，現在最も一般的で広く採用されているのが，上述の公開鍵暗号方式を用いたもので，公開鍵基盤（PKI, Public Key Infrastructure）といわれる。

3．電子認証制度

3.1．電子署名法と認定認証事業者

電子署名された電子データに対して，本人によるものと推定し，それに捺印や署名と同等の法的根拠を与えることを規定した，「電子署名及び認証業務に関する法律（電子署名法）」が，平成12年5月に成立し，平成13年4月から施行された。この法律の目的は，電子商取引などでの電子文書による情報の流通を円滑に行わせることである。電子署名法では，電子署名や認証の具体的な方式までは規定されておらず，公開鍵暗号方式やPKIだけを対象とするものではないが，現時点での実用性並びに普及状況から見て，他に代わる方式はない[5]。

電子署名に証拠能力を与える方法として，電子署名法では認定認証事業者制度を導入した。これは，国として一定の基準を満たす認証局を認定し，それが発行した公開鍵証明書にもとづいて本人を特定できる電子署名について，手書きの署名や紙への押印と同じ法的効力を認めようとするものである。ここで保証される電子署名は，従来の制度で言えば個人の実印に相当する。

認定認証事業者として認定される基準は主務政省令で提示されている。それには，①公開鍵の強度，②利用者の審議の確認方法，③証明の実施方法，④証明書の内容と有効期限，⑤認証設備のセキュリティ，などが規定されており，表1に示す事業者が認定を受けている[6]。

なお，認定を受けていない認証局であっても従来どおりサービスを提供可能である。しかしながら，その利用者側には，認証局の証拠能力が問題となった場合に，認定を受けた認証局と同等の能力があるとの立証責任を負わされることになる。また，後述の政府認証基盤との相互認証の対象とされているのは，特定認証業務として認定されている事業者のみであるため，認定認証事業者の優位性は否定できない。

電子署名法は個人を対象とした認証制度である。法人を対象とした制度は，平成12年4月の商業登記法改正により，「商業登記に基礎を置く電子認証制度」として，平成12年10月から運用を開始した。実際には，東京法務局が管理する電子認証登記所が認証局として，法人代表者に対して公開鍵証明を発行するものであり，保証レベルは法人印に相当する。

3.2．その他の電子認証制度

これらの制度に加え，現在，公証人による認証制度と政府認証基盤が機能している。

(1) 公証人による認証

上記の商業登記法改正により，従来の公証制度に基礎を置く電子公証制度が創設され，実際の公証人が運用する電子公証制度は平成14年1月から開始された。電子公証制度は，現行の公証制度に基礎を置き，一定の環境を整えた指定公証人によって，現在紙ベースで提供されている「確定日付の

4）電子証明書の標準仕様はITU（国際電気通信連合電気通信標準化部門）によって定められており，公開鍵，その所有者に関する情報，発行認証局に関する情報，認証局の署名などを記した上で，認証局の公開鍵で暗号化されている。

5）電子署名法では，電子署名について，「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」であり，「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」，と規定している（同法第二条）。

6）http://www.meti.go.jp/policy/netsecurity/digisign_ninteiitiran.htm（平成14年11月20日現在）

表1　特定認証業務の認定事業者

認定に係る特定認証業務の名称	業務を行う者の名称
Accredited Signパブリックサービス	日本認証サービス株式会社
電子入札用電子認証サービス	株式会社帝国データバンク
Accredited Signパブリックサービス2	日本認証サービス株式会社
株式会社日本電子公証機構認証サービスiPROVE	株式会社日本電子公証機構
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
CECSIGN認証サービス	株式会社コンストラクション・イーシー・ドットコム
セコムパスポート for G-ID	セコムトラストネット株式会社
AOSignサービス	日本電子認証株式会社
e-ProbatioPSサービス	エヌ・ティ・ティ・メディアサプライ株式会社

付与」及び「私署証書の認証」などの公証サービスを，ネットワークを介した電子文書についても利用できるようにしたものである。なお，現在のところ，このサービスの対象は法人のみである[7]。

(2) 政府認証基盤

電子政府化の一環として，民間からの各種電子申請に対する結果の通知を電子化するにあたり，それらの作成者が処分権者であること，並びに結果の通知等の内容が改ざんされていないことを証明する必要が生じる。このため，従来の大臣公印などの役割を果たす電子的な証明書を発行するために，各府省がそれぞれの認証局を運用し，職員を被認証者として公開鍵証明書を発行することとした。

政府認証基盤は，総務省の運用するブリッジ認証局と各府省認証局から構成される。申請者（民間）と行政機関との間での申請や届出と結果通知の相互のやりとりを電子化するには，双方の証明内容を相互に信頼するという相互認証が前提となるが，各府省の認証局と民間認証局等とが個別に相互認証すると煩雑になるため，総務省の運営するブリッジ認証局で一本化して相互認証を行う仕組みをとっている。平成14年8月現在，府省で運用されている認証局は，平成13年4月に設立された，総務省，経済産業省，国土交通省の3局であり，今後，平成14年度中に各府省の認証局が順次開設されていく予定となっている。

政府認証基盤は，自治体の電子政府化が進むとともに，地方公共団体の職員に対する公開鍵認証の実施へと拡大するのが必然であり，地方公共団体がその職員の真正性を証するための認証局の設置が求められてく。しかしながら，現時点ではその具体的な計画はまだ明らかにされていない。

4．電子認証サービス

4.1．電子認証ビジネス市場

平成13年秋から14年にかけて，総務省の行った調査によれば，平成13年度の電子認証ビジネスの市場規模は約63億円と推計されている（図1）[8]。この調査では，電子認証ビジネスの市場を，登録業務代行，証明書発行業務代行などの電子証明書関連サービス（個人及び法人向け），認証業務に必要とされる認証事業者のシステム構築及び利用者向けのPKI対応ソフトウェア販売などから構成されるものとして定義している。

平成13年度の推計の内訳は，個人向けの電子証明書関連サービスが0.5億円，法人・団体向けの同サービスが30億円，ソフトウェア市場が33億円弱となっている。

すなわち，個人向けの電子証明書サービスに対する需要が現時点ではほとんど皆無に近い状態であることが分る。さらに，楽観的な見通しの下での5年後の値も，1.6億円程度という無視しうる程度の規模にとどまっている。

これに対し，法人・団体向けの市場は順調に拡大する見込みで，今後5年間で6～8倍に拡大するものと予想されている。また，平成15年度に開始予定の電子政府がビジネス市場の拡大に大きな役割を果たすことが指摘できる。

7）http://www.koshonin.gr.jp/TOPICS/topics11.htm

8）総務省・アクセンチュアによる「電子認証ビジネス市場規模調査」から（平成14年度情報通信白書）。

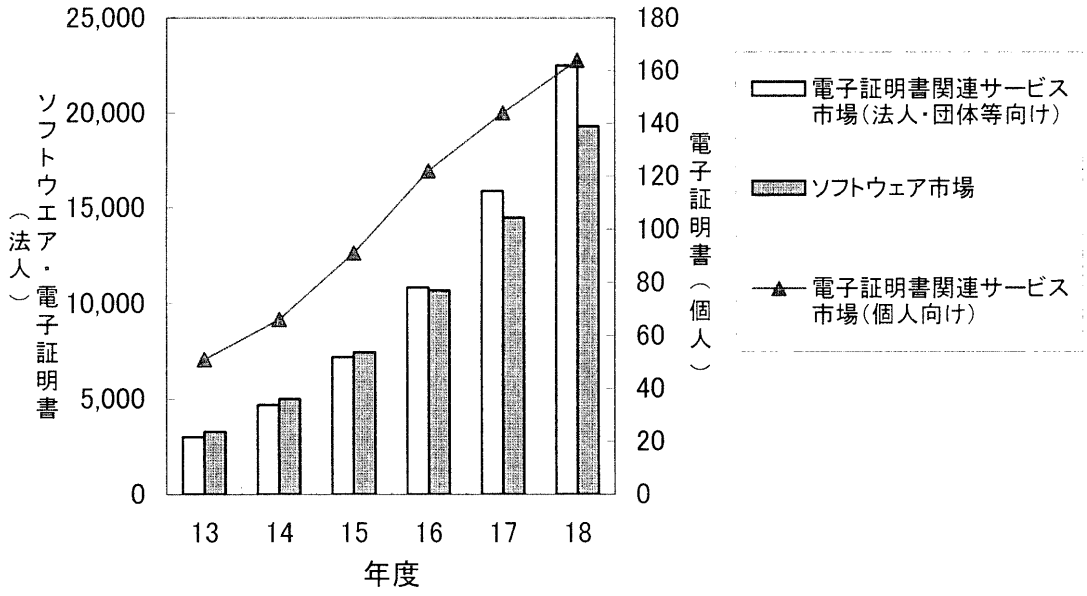

図1　電子認証ビジネス市場の推計

4.2. 企業向け電子認証サービス

上述のように，企業向けの電子認証サービスへのニーズは，企業間電子商取引（B-to-B）に対する安全性の保証へのニーズの高まりを電子政府化の進展が後押しする形で，急速に高まっていくことが予想される。制度的にも，電子署名法に加えて，従来紙で交付することが義務付けられていた書面を電子的手段で代替することを認めたIT書面法（「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」，平成13年4月施行）や，電子的手段を介して契約を行った時の成立時期を従来の通知の発信時から到達時に変更する電子契約法（「電子消費者契約及び電子承諾通知に関する民法の特例に関する法律」，平成13年12月施行）など，ネットワーク上での取引の増大に呼応した法律の整備が進められている。

企業向け電子認証サービスが扱う企業の認証といっても種々あり，Webサイトの真正性の認証から，登記情報などの存在証明，資格証明などがあるが，いずれにせよ，例えばeマーケットプレイスでは，運営会社および市場参加者（購入者，販売者）のすべてに電子証明書が義務付けられるなど，電子証明書を持たない企業はビジネスへの参加が困難になるであろう。

今後は，株主総会等での議決権の行使における電子署名，ネットワーク上での証券取引やオークションにおけるタイムスタンプの証明，さらに，本人そのものの認証から取引能力や与信情報などまで含めた認証へと，サービス内容が広がって行くことが予想される。

民間事業者による認証サービスは，不特定多数の顧客を対象にしたビジネス展開だけではない。金融分野では決裁機能を提供する銀行を中心とした認証サービスが広がりつつある。それは，1999年に欧米の有力金融機関によって設立されたアイデントラス（Identrus）である。アイデントラスは，インターネット上での企業間電子商取引において，金融機関が各企業に対し，そのメッセージの有効性を保証し，ICカード認証書を利用したPKIシステムによって秘密通信を行う国際的なインフラを提供するシステムである。既に世界130カ国で事業を展開する50以上の有力な金融機関が参加しており，国際的な電子認証サービスのデファクトスタンダードとなりつつある。わが国でも，みずほグループや東京三菱，三井住友などの有力金融グループがアイデントラスベースの電子認証で連携して対応し，認証書発行手順，電子認証書の形式などの共通化を進めている。

アイデントラスの認証の仕組みは4-Corner Model（4者間モデル）と呼ばれ，図2のような流れで認証が行われている。

買い手企業が売り手企業にインターネットで物品購入の発注する場合，買い手側はその取引銀行から発行された電子証明書を同時に売り手側に送る。売り手企業は，その証明書が正しいものであ

るかを自分の取引銀行に照会し，取引銀行は相手企業の取引銀行に問い合わせを行って証明書の有効性を確認する。それぞれの銀行に関する証明書の有効性については，その都度アイデントラス社のルート認証局が確認する。これらの確認はインターネットを経由してリアルタイムで行われ，同じ証明書がアイデントラスが関与するすべての電子商取引において使用できる。

この認証システムは，金融機関が信頼できる第三者として，取引相手の本人性，支払能力，業務能力などを保証する枠組みを提供するものであり，企業にとっては，従来行ってきた取引上の各種リスクに対する処置を大幅に軽減できる。さらに，この証明書の有効性確認に加え，決裁機能や保険サービスなど，金融機関の特徴を生かした付加サービスの展開も計画されている。

このような認証サービスを電子社会のインフラとして普及させて行くためには，PKIの技術面での安全性の向上はもとより，行政と民間の認証局の相互運用性の向上，海外の認証局との国際的な相互運用性の向上など，より一層の環境整備が求められている。

4.3. 個人向け電子認証サービス

4.1で示したように，個人向けの電子認証サービス市場の規模拡大はあまり期待できないのが実情である。その理由としては，

①電子証明書の取得手続きや関連のアプリケーションの操作方法が標準化されていないなど，利用者にとってはまだ使いづらい
②現実の電子商取引で使用されている種々の個人認証手段が定着している
③本当に必要とされている状況が限られている

ことなどが挙げられる。

①については事業者側の努力で改善されていくであろうが，②および③については，電子証明書に関する本質的な問題に関連している。

例えば，個人の行う電子商取引の典型であるオンラインショッピングでは，買い物という行為そのものに本人確認は必要ではなく，支払い又は支払い能力の確認さえ伴えば良い。そこに必要なセキュリティには，Webサーバとブラウザ間での相互認証と暗号化された通信を保証する，SSL（Secure Sockets Layer）という通信プロトコルで十分対応が可能であり，現在，クレジットカード番号などによる支払いに広く用いられている。また，座席や宿泊等の予約における本人確認は，住所，氏名，電話番号と電子メールアドレスで行われており，SSLを用いるまでもない。また，株式取引のように一定の本人認証を求める場合でも，プロバイダによる利用者認証で代行させているケースも見られる。

購入希望者に対して認証局による真正性の証明を求めることは，オンラインショッピングサイトが，成りすましによるリスクを防止するための，

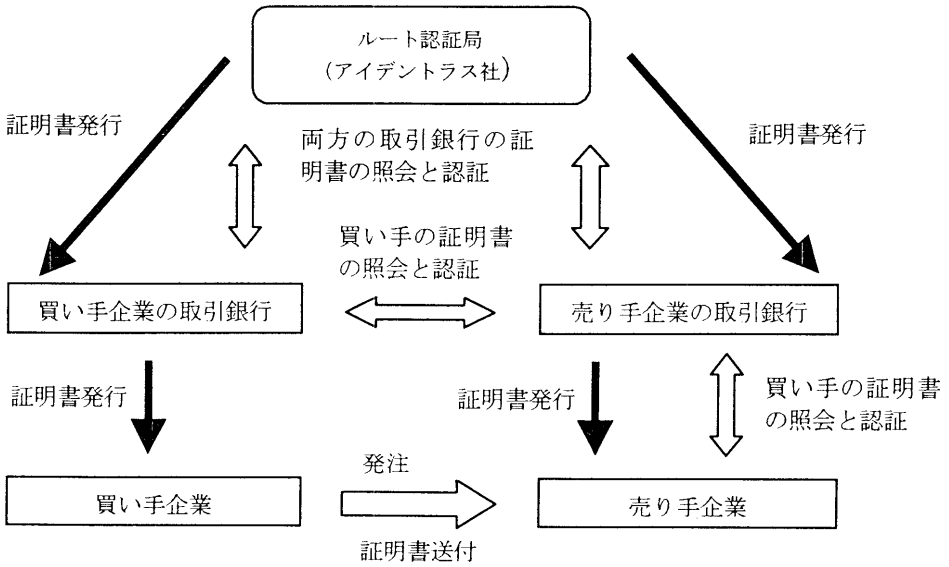

図2　アイデントラスの4者間モデル

機器や専用ソフトの購入と設置，証明の取得などにかかるコストの負担を購入者に求めることに他ならず，それを主張できるサイトは現実にはごく少数に限られている。

認証局による個人認証は印鑑証明と同等のレベルであると先述したが，我々が日常生活の中で実印と印鑑証明を必要としているのは公的な事項に関する登記や届出など，相当程度限定されている。これらを考慮すると，個人における電子証明書の利用度は，現実には，あまり高くないものと考えられる。

このような状況にあって，平成15年度からの地方公共団体による公的な個人認証サービス制度の創設するための「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」が平成14年6月に国会に提出された[9]。上述のように，認証局による個人向け電子認証サービスへの需要がまだ低いこと，サービスの提供主体である地方公共団体が，既存の認証局と同程度の技術水準を達成できるか疑問であること，さらには電子認証サービスの利用については，民間事業者のサービスがネットワークを通じてどこからでも申込が可能であり[10]，自治体による住民限定のサービスとして行う必要性が低いこと，などの理由から，現時点におけるこの制度の創設については疑問を呈せざるを得ない[11]。

認証サービスの個人レベルでの利用を普及させるには，自治体による住民を対象とした一律の認証制度や，実証実験の結果，使用頻度が非常に低いことが明らかになった本人確認専用のICカードの導入などの施策は得策ではない。むしろ，現在用いられている種々の本人認証システムを考慮しつつ，新たな電子認証システムを必要とする利用者にとって分りやすく，低コストで使やすいシステムの開発などへの取り組みが求められている。

5．むすび

電子署名に法的な効力を持たせる電子認証制度の創設と認証基盤としてのPKI技術の普及により，電子認証サービスの利用環境は整いつつある。企業・団体向けは順調な拡大が見込めるが，個人向けサービスの普及には課題が多い。また，PKIについては，認証局の安全性の確保や運用コストなどの運用体制がこれからの課題として指摘できる。（本稿は，平成12年度前期広島大学研究支援金 文理ジョイントプロジェクトによる研究成果の一部である。）

参考文献

青木隆一・稲田　龍，「PKIと電子社会のセキュリティ」，共立出版，2001年

インターネットビジネス研究会，「インターネットビジネス白書2002」，ソフトバンクパブリッシング，2001年

C. カウフマン，R. パールマン，M. スペシナー著，石橋他訳「ネットワークセキュリティ」，プレンティスホール出版，1997年

丸山誠二，「電子認証技術に関する動向調査」，郵政研究所月報，2001年4月，pp.19-33

9）この法案は平成14年12月現在，継続審議中である。

10）たとえば http://www2.jcsinc.co.jp/service/e-Japan.html（日本認証サービス(株)）など。

11）認証事業者とインターネット接続事業者との提携による電子証明書発行サービスも開始されている。