解説

電子署名法の概要

(財) 日本情報処理開発協会, (財) 日本データ通信協会
電子署名・認証センター

萩原　隆
hagiwara@ac.jipdec.or.jp

■電子署名法の背景と電子署名・電子認証

▌インターネット上の電子商取引の拡大

近年におけるインターネット利用者の増大は著しい. 我が国のインターネット利用者数は, 1999年末には2,706万人だったが, 2005年末には7,670万人になると予測されている[1]. こうしたインターネット利用者数の増加とともに, 電子商取引が一般消費者にとっても急激に身近なものとなりつつある. インターネット利用者増加による通信コスト面での大きなメリット, 暗号技術やネットワークセキュリティ技術の進展によるセキュアな通信技術の確保等が理由である.

現在においては, インターネット上の電子商取引は, 教育, 医療, 金融等, 多くの業界に及んでいる. 平成8年に国内最初のサービスとして大和証券が開始したオンライン証券取引, 自動車販売のオートバイテルや書籍販売のAmazon.com, 文具販売のアスクルなどに代表されるオンライン販売, その他にもインターネットバンキングやオンラインオークション等々, 一般消費者においても, ネットワークを用いて国内外より日常生活に必要なさまざまな商品を入手することができるようになった.

今後, インターネットの利用コストが低下し, また, 高速アクセス回線の普及や通信の安全性が向上するにともない, ますますインターネットによる電子商取引の範囲は拡大していくであろう.

▌電子商取引と法制度

従来の法律や制度は, こうしたインターネットを基盤として成立しているディジタル社会を前提とせず, 紙と対面文化に立脚した取引の世界を前提として成立していた. このため, 従来の社会のルールでは, 新しいインターネット化, ディジタル化の時代に向けた, 新たなルール整備がここ数年行われてきた.

ディジタル化された知的製造物の複製の製造・流通に関する不正競争防止法の改正や, ネットワークを経由したコンピュータへの不正アクセスを防止するための不正アクセス防止法の成立, 商業登記に基礎を置く電子認証制度の開始, そして本稿の中心的話題である電子文書の真正な成立に推定効を与える電子署名法(正式名称：電子署名及び認証業務に関する法律)の成立へと続いた. さらには, 昨年夏, 通商産業省(現, 経済産業省)が, インターネットでの取引の妨げとなる法律を一括改正するため, 書面や対面販売を義務付けた法律の改訂法案を昨年秋の臨時国会に提出すると発表し, 内閣内政審議室を中心に各省庁でも同様な動きが開始された. そして, 民間における電子商取引の促進を図るため, 書面の交付等に代えて書面に記載すべき事項をネットワーク技術を利用する方法により提供し, かつ組合等における議決権の行使等を電子文書により行うことができる等の関係法律の規定を改正するための, 「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」が平成12年の秋の臨時国会で成立し, 平成13年4月に施行される.

▌電子署名と電子認証

インターネットを利用したビジネス, ショッピングなどの電子商取引における消費者は, 取引している相手の顔が見えないため本当に意図している人間なのか, また送信した情報のセキュリティは大丈夫なのか等々の不安を常に抱えている[2]. このような問題を解決する技術の1つが, 暗号技術を応用した電子認証技術と呼ばれるもので, その代表的なものとして, 公開鍵暗号方式によるディジタル署名を中心とした電子署名が注目されている. 公開鍵暗号方式による認証の仕組みについては解説のための数々の文献が存在しており, ここでは簡単に述べるにとどめる.

自分の作成した電子文書（法律では電磁的記録と呼んでいる）にハッシュ関数で数学的処理を行い固有の数値データを作る．これはメッセージダイジェストと呼ばれるものである．さらに，メッセージダイジェストに自分の秘密鍵を使って暗号化する．この暗号化されたデータがディジタル署名と呼ばれる電子署名である．

ディジタル署名は，発信者本人しか使えない暗号化処理を電子文書に施すことにより，その電子文書が発信者のものであり，通信路の途中で改ざんされていないことを証明する．しかし，発信者本人を特定するためには，秘密鍵と対をなす公開鍵でディジタル署名を復号でき，かつその公開鍵が発信者本人のものであることを第三者が証明しなければならない．この信頼される第三者が，認証機関と呼ばれる機関であり，認証機関を中心として公開鍵証明書を発行する認証システムの整備がなされ，電子認証システムが構築される．このような公開鍵暗号方式に則った公開鍵証明書を利用するシステムをPKI（Public Key Infrastructure）と呼ぶ．

▌電子署名法

日本においては，すでに民間の認証事業者が存在しており，一部では電子署名が，本人確認の手段として利用されていた．しかし，その法的位置付けがはっきりしておらず，消費者は電子署名や電子認証を利用した場合でも安心した電子商取引を行うことはできなかった．

そこで，政府（所管省庁は，総務省・経済産業省・法務省である）は，2000年5月の第147回国会で成立した電子署名法（正式名称：電子署名及び認証業務に関する法律）において，電子署名や電子認証を行う業務に一定のルールを課し，手書きの署名や押印と同様な法的位置付けを行った．

■ 諸外国にみる電子署名・認証の法制度

ここ数年，電子署名法またはディジタル署名法が諸外国で成立している．

▌米国

米国では，ほとんどの州で電子署名・電子文書の法的効果を否定しない法律があるが，代表的なものに1995年5月に成立したユタ州のディジタル署名法がある．この法律は世界で最初に成立した電子署名法として有名で，多くの米国の州や他国で参考にされた．法律の対象となる電子署名は公開鍵暗号方式を用いたディジタル署名技術のみとしている．地理的要件や財政的基盤，認証業務への専門知識，セキュリティ要件を充足した認証機関が認証する電子署名について，利用者が電子文書に署名を行う意思を持って署名を行った場合について，法的な推定が与えられた．

現在では，電子文書に署名をする意思を持つ人が実行した電子署名であることが立証できれば，どのような電子署名でもその有効性を認めることができるとした，1999年7月に作られた統一電子取引法（UETA）が各州のモデル法として位置付けられている．UETAでは，本人への帰属性は，電子署名で用いられた技術のセキュリティレベル等を参考にしている．2000年6月には，米国政府により電子署名法が制定され，同年10月に施行した．技術中立の立場から，電子署名を構成する技術については，法律では定めていない．採用する技術は，契約にかかわる当事者間の合意に基づいて決められるとしている．

▌イタリア

イタリアでは，1997年3月にディジタル署名法が成立し，先進国の中で唯一認証機関に対して義務的な免許制度を設けている．

▌ドイツ

ドイツでは，ディジタル署名に限定された電子署名を規定した法律として，1997年7月マルチメディア法の一部として「ディジタル署名法」が成立した．認証機関に対する認定制度は任意的なものとなっており，認証機関への評価基準は，厳格な本人確認やディジタル署名のセキュリティに関する情報開示，個人データ保護等の高い安全性，信頼性を求めている．しかし電子署名の法的効果は規定されていない．現在同法は，2000年1月に公布されたEU電子署名指令も考慮に入れた見直し作業を進めており，電子署名の要件の確立や，一定の要件を満たした他の電子署名に関する取り扱いを正当な電子署名としてみなすとする記述，および安全性を高めた認証機関に対する任意の認定制の要件についての記述などが追加される模様である．

▌英国

英国で電子署名法に相当する法律は，2000年5月に成立した電子通信法である．本法の中で，一定の形態の電子署名については，その証拠力を認める規定がなされている．また認証機関の任意の認定制度も設けられている．この法律は，2005年に英国政府のすべてのサービスを電子的手段で提供するための制度的基盤となるものである．さらに，この法律の成立を契機として，企業

が年次報告書および会計報告書の株主への送付を電子的に行うことができる会社法（1985年）の改訂や，電子的手段による不動産譲渡を可能にする不動産法（1925年），土地登記法（1925年）の改訂等の多くの既存の法律の見直しが進められている．

■フランス

フランスでは，2000年3月に電子署名法が成立し，一定の基準を満たす電子署名は，手書き署名と同等の署名行為の真正性を推定し法的効果を認めるフランス民法の改正について規定された．

■EU（欧州連合）

欧州では，各国ですでに法制度整備がなされているが，EUの欧州委員会において加盟国内の電子商取引市場を発展するための統一的な基準を示すため，電子署名指令（Directive）が検討され，2000年1月に公布された[7]．ちなみに指令が公布されると，各国は指令に沿って国内法や行政規則等を改正する義務が生ずる．指令では電子署名を技術中立的にとらえ，ディジタル署名に限定せず，電子署名一般について規定している．また，認証機関への義務的免許制度は禁止され任意的認定制度のみが認められている．

■アジア

アジアでも多くの国で法制度整備が進んでいる．シンガポールでは，電子取引法が1998年7月に成立しており，認証機関が政府の認定の有無にかかわらず，すべての認証機関に認証実施規定を定めている点は他国との違いをみることができる．さらに，マレーシアのディジタル署名法（1997年6月成立）や韓国の電子取引基本法／電子署名法（1999年2月成立），香港の電子商取引法（2000年1月成立），インドの情報技術法（2000年5月成立），フィリピンの電子商取引法（2000年6月成立）等の中で電子署名や電子文書の法的な取り扱いについて，それぞれ規定されている．

■ 日本の電子署名法

我が国の電子署名法には，3つのポイントがある．

■電子文書（電磁的記録）の真正な成立の推定

電子署名法第3条には「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．」とある．

「真正に成立した」とは，その電子文書が本人の意思に基づいて作成されたものであることを意味している．つまりこの法律では，本人による電子署名が付与された電子文書は，本人の意思に基づいて作成されたと判断している．また，ここで述べた「本人による電子署名」とは，電子署名法第2条の定義によると，公開鍵暗号方式における秘密鍵による等の電子署名を行った本人のものであることを表すもの，電子署名の対象となった電子文書が，電子署名の後に，他の情報に置き換えられたり，一部が書き換えられたりしているかどうかを確認することができるものである．また，推定機能が働きやすくするために，技術的信頼性のある電子署名について現在主務官庁で定めようとしている．平成12年11月20日にパブリックコメントを求めるために公開された原案（以降，パブリックコメント案という）によれば，電子署名の信頼性を保証するための目安として，1）ほぼ同じ大きさの2素数の積である1,024ビットの整数の素因数分解等による「解読の困難性」と，2）署名鍵を解読せずに署名文を偽造できない等とする「安全性機能を規定」し，3）暗号がRSA方式であって，鍵長が1,024ビット以上のものとする「技術的基準」の3点についてクリアされたものを技術的信頼性のある電子署名とするのではないかと思われる．本稿が印刷された頃には，省令として公表されていることと推定されるため興味のある方はぜひ確認していただきたい．

法律では特定の電子署名技術を述べていないが，パブリックコメント案を見る限りディジタル署名が対象となっているようである．しかし，パブリックコメント案で規定されたディジタル署名と，同等の安全性が確認できた電子署名は，主務大臣が定めることが可能となっている．これは技術を中立にとらえ，特定のメーカの規格による電子署名技術のみを，法的に位置付けるものでないためである（パブリックコメント案に規定されていても，最終的に変更になる規定部分もあるため，注意されたい）．

■特定認証業務に関する任意の認定制度

電子署名法では，より安心して電子署名を利用できるように，電子証明書を発行する事業者の特定の業務について，国が認定をするように定めている．しかしこの認定制度は，義務的な免許制ではない．したがって，認定を受けていない認証機関も，ビジネスの遂行に問

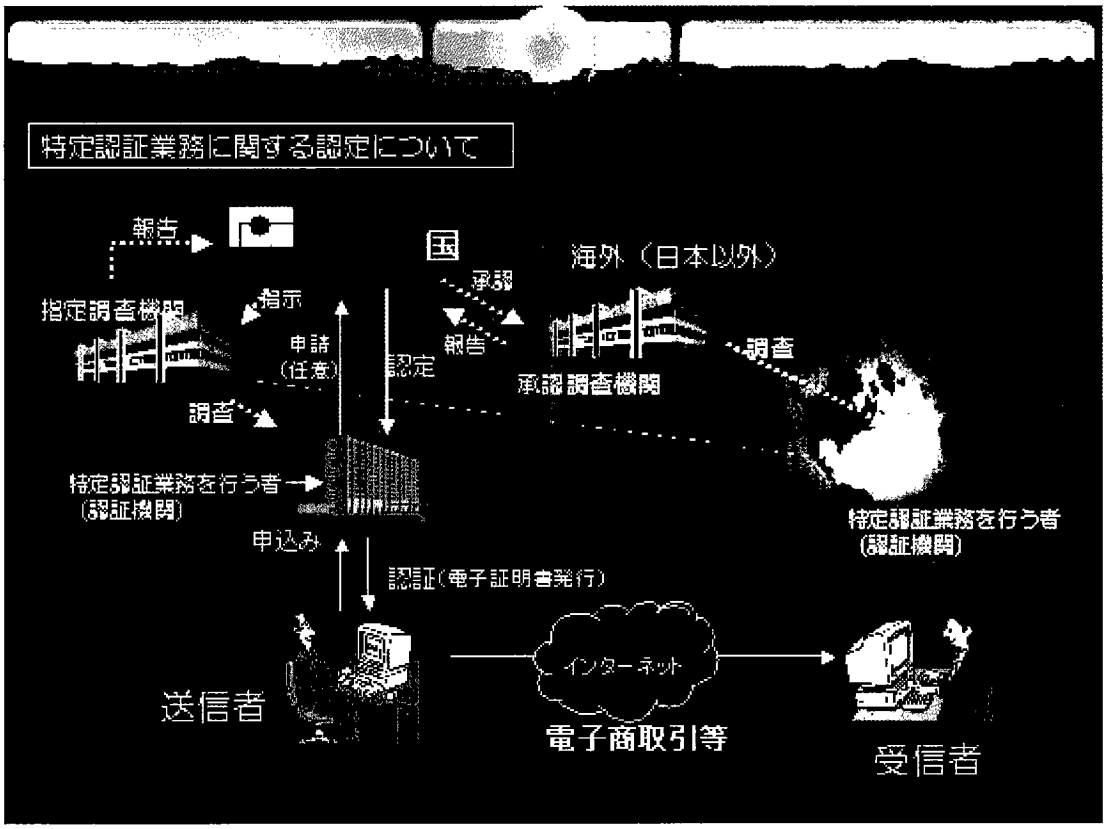

図-1　特定認証業務に関する認定について

題はなく，特に規制もない．

認定を受けた認証機関は，認定対象の認証業務の中で発行している電子証明書が付いた電子署名の安全性や，電子証明書の発行に際しての利用者の本人確認の適切性などについて，電子署名法に基づいて，認定を受けることが想定される．こうした認定制度により，利用者に対する信頼性の目安を提供するという意図を持っている．認証機関がこの認定を受けるためには，さまざまな基準や条件をクリアする必要があり，詳細な内容は，政省令で明らかになるが，パブリックコメント案によれば，対面および郵送等による電子証明書取得のための日本国旅券，運転免許証等の写真付き官公庁発行の証明書の提示による本人確認方法等を含む，「利用者の真偽の確認の方法」や，証明（認証）の実施方法，認証業務規定の作成や公開について，認証業務を適切に実施するための組織体制やセキュリティ要件等について規定されており，これらの規定をクリアしていれば認定される．

また，電子署名法では，信頼できる認証事業者や認証機関を認定するために，調査業務規定等に基づく一定の基準により調査する機関を，指定調査機関と承認調査機関として定めている．認定を受けようと申請してきた認証機関（認証事業者）の認定対象となる特定の認証業務の実施体制について，実地の調査等を国の代理として指定を受けた調査機関と承認を受けた調査機関が行うというものである（図-1）．

指定調査機関と承認調査機関の違いは，前者は主に日本国内，後者は日本国外を管轄すると考えると理解しやすい．

指定調査機関は，具体的には，認証機関（認証事業者）の事業場に立入り，認証機関の設備等について主務省令で定めた基準への適合確認を行うこととしている．この調査をする指定機関は，非常に高い専門的・先進的技術を要求されることと，民間機関の能力を積極的に活用する目的で，秘密保持義務等の規定を設けたうえで，民間の機関に国の事務を代行させるように定められている．

承認調査機関に関しては，日本の国外にある外国の認証機関が，日本の電子署名法の中の認定を受けるとき，外国の事務所に実地調査をする調査機関について，

国が承認することができるとしており，その承認された機関が承認調査機関といわれる．外国の認証機関が，日本国内の指定調査機関の調査を受ける負担は大きいと想定されるため，外国の認証機関の負担軽減の観点から，外国において実地の調査を行う調査機関がある場合に，電子署名法を管轄する総務省，経済産業省，法務省の3省の主務大臣が承認し，その調査結果に基づいて認定のための審査を行うという，外国の認証事業者の利便性を考えたものとなっている．承認認証機関への申請は，その調査を行う調査機関からの申請に基づくものと決められている．

インターネット上の取引等は，国境を越えてグローバルに進められるため，電子署名法では，諸外国の法制度との国際整合性を図りつつ，外国の認証事業者の取り扱いについても考慮されている．

▌その他（特定認証業務に対する援助，教育・広報，国家公安委員会の役割等）

電子署名法第33条には「主務大臣は，特定認証業務に関する認定の制度の円滑な実施を図るため，電子署名及び認証業務に係る技術の評価に関する調査及び研究を行うとともに，特定認証業務を行う者及びその利用者に対し必要な情報の提供，助言その他の援助を行うよう努めなければならない．」と定められている．電子署名および電子認証の根幹を成す暗号技術は，CPUの処理能力の進展や攻撃技術の研究等により，長期間にわたり安全性を維持することは困難になっている．さらに，他の関連技術の開発も重要となる．電子署名法においては，これらの情報について，主務大臣が，認定を受けた認証事業者やその利用者に，安全面・信頼面の判断できる材料を客観的に提供していくことが重要だとしている．

また，パソコン上で電子署名をする行為は非常に簡単に行うことができる．たとえば，電子署名の法的な位置付けを認識せず，安易に電子署名を行ったり，秘密鍵の管理が不十分な場合も考えられる．したがって，この法律では，電子署名および認証業務を円滑に普及させるため，国が意識の啓発や知識の普及に努めなければならないと定めている．また主務大臣は，さまざまな情報に基づいて判断しながら，認定に不適合な場合は，認定を取り消すことができる．さらに国会公安委員会は，不正な事実があった場合は，主務大臣に必要な措置をとることを要請できるとしている．

■ 電子署名法施行に伴う今後の課題

日本政府は平成12年7月7日の閣議決定において内閣総理大臣を本部長とする情報通信技術（IT）戦略本部を設置した．その中での検討課題の1つに，電子商取引を促進するための規制改革等諸制度の総点検，新たなルール作りがあり，ネット上の取引・事業を制約する制度等の早急な見直しや，電子政府の実現に向けた手続きの電子化に伴う手続き法制の整備が上げられており，法改正作業が進んでいる．電子署名法の整備が最も先行している米国においてもビジネスに大きく影響する電子署名・認証の利用が本格化するのはこれからである．

ここでは，こうした現状を認識し，電子署名法が電子商取引の促進を目的としたものであることを念頭に置き，電子署名法に基づく電子署名・認証制度が，広く我が国に浸透し，長く利用されるための課題について述べる．

▌技術的な課題

郵政省（現，総務省）は，2000年7月4日に，「暗号通信の普及・高度化に関する研究会」報告書を発表した[3]．この中で電子署名にかかわる技術課題についても触れている．この報告書を参考に，技術的な課題を述べる．

第一に，エンドエンティティにおける技術を挙げることが可能である．エンドエンティティにおける技術は，セキュリティとユーザインタフェースに分けられる．エンドエンティティにおけるセキュリティとは，主として秘密鍵のセキュアな保管と端末における暗号機能の実装を目的とした技術であり，安全なICカードリーダの開発や耐タンパソフトウェア技術の確立が望まれている．エンドエンティティにおけるユーザインタフェースとは，ユーザが秘密鍵へのアクセスを安全かつ容易に行うことができると位置付けられ，エンドエンティティにおける個人認証手段についてバイオメトリクスを利用することも検討されている．

第二に，相互認証にかかわる技術を挙げる．証明書のフォーマットは，ITU-TのX.509等において標準化がなされている．しかし，異なる認証機関の間での，証明書の流通のためには，証明書のフォーマット詳細のみならず検証プロトコルについても標準化が必要であり，今後の課題である．

第三に，暗号技術の高度化を挙げることができる．メッセージ認証アルゴリズム，ハッシュ関数に関しては，主として高速性に対するニーズが高い．ディジタル署名の技術的基盤となる公開鍵暗号に関しては，暗号の

強度評価技術により評価を行いつつ，整数論的な問題（素因数分解，離散対数問題，楕円離散対数問題等）の改良拡張に努めるだけではなく，将来の量子計算機の登場時にも安全なアルゴリズムの開発が望まれる．

■普及啓発にかかわる課題

電子署名法は，刑法等とは異なり，電子商取引の活性化のために電子署名の利用を促進する法律である．特に，企業間のクローズドな取引のみならず，一般消費者も含むオープンな場での電子署名の利用に向けた，普及啓発が肝要と考えられている．こうした前提のもとに，電子署名法および電子署名の普及に向けた課題とポイントを挙げる．

第一に，キラーアプリケーションの登場を挙げることができる．電子署名法は，電子文書および民間の認証機関にかかわる法律であるが，電子署名が広く世間に認知されるためには，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，その他行政手続のオンライン化により，電子政府・電子自治体の整備がなされることが重要であり，こうした行政の電子化の動きが，電子署名普及の大きな推進力となると考えられる．

第二に，エンドエンティティにおける個人認証環境の整備である．現状のパソコンでは，個人認証環境が整っておらず，実質的にだれでも使える状態となっている．こうした状況下で，秘密鍵の管理を行うことは困難であり，ICカードリーダのパソコンへの標準装備，（個人確認がなされている）携帯電話の利用等がなされる必要がある．

第三に，利用者の不安感に対する適切なケアが必要となる．先に述べたように，インターネット上でのショッピングに対する不安感を相当数の利用者が抱いており，官公庁，認証業者，取引業者，モール業者，消費者団体等が連携し，情報提供や苦情受付を行うための体制を整備することなどにより，対応することが重要である．

第四に，第一～第三を通して，利用者が利便性を感じるサービスを提供するにいたることである．利便性とは，システムや制度のコスト面を含めた使いやすさであり，電子署名の利用により，安全で便利な取引が可能であるという雰囲気の醸成が育つことを目的としたい．

■法律面における課題

電子署名法に関する法律面に関する議論は，以前より多くなされてきた[4)～6)]．これらを基に，我が国の電子署名法の法律的側面から見た課題について述べる．

第一に，文献4）で内田先生が指摘している文書の非改竄性に関する推定効の問題を挙げることができる．一般に，電子署名が付与された電子文書の非改竄性は，割印を押印した紙ベースの文書よりも強く担保されると考えられる．しかし，電子署名法では，電子署名付き電子文書の非改竄性にかかわる推定効が明記されておらず，今後の裁判官の判断に委ねられている．

第二に，文献4）および文献6）で取り上げられている国際相互認証の問題がある．我が国の電子署名法が強く意識しているとされるEU電子署名指令[6)]においては，EU内の認証機関がギャランティを与えれば，証明書の効力が認められるという規定があるが，我が国の電子署名法にはそのような条文はなく，今後調整が必要となる．また，インターネットによって，国際的な電子商取引が増加した場合の問題ともなる．

その他に，誤操作による発信，電子的にとり交わされた契約等の成立時期，電子的な文書の原本性，電子的な契約にかかわる印税，国際間取引における準拠法および課税等の問題が存在する．しかし，これらは電子署名法のみにかかわる問題ではなく，電子商取引全般にかかわる問題であり，電子契約法等による法体系の整備が望まれる．

■電子署名・認証センター

電子署名・認証センターは，（財）日本情報処理開発協会と（財）日本データ通信協会が共同で運営する，電子署名・認証についての調査研究と普及啓発を主業務とする組織である．電子署名法の主務官庁である総務省，経済産業省，法務省と連携をとりながら，活動しており，説明会等を行っている．以下のURLを参照いただき，読者の中で，当センターの活動内容に興味のある方はぜひ参加していただきたい．

http://www.jipdec.or.jp/esac/esac.htm

参考文献
1) 平成12年版 通信白書 (2000).
2) MIN第5回アンケート「購買行動とインターネット・ショッピングに関するアンケート」: 情報通信総合研究所, http://www.commerce.or.jp/ (1999).
3) 郵政省:「暗号通信の普及・高度化に関する研究会」報告書, http://www.mpt.go.jp/pressrelease/japanese/denki/000704j602.html (2000).
4) 稲垣他: ≪座談会≫電子取引法制度整備の課題, ジュリスト, No.1183, pp.2-34, 有斐閣 (2000).
5) 信森毅広: 認証と電子署名に関する法的問題, 日本銀行金融研究所ディスカッションペーパー, http://www.imes.boj.or.jp/jdps98/98-J-06.pdf (1998).
6) 夏井高人: 電子署名に関する訴訟対応, インターネット訴訟2000 pp.381-395, ソフトバンク(2000).
7) DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCI of 13 December 1999 on a Community Framework for Electronic Signatures, http://europa.eu.int/comm/internal_market/en/media/sign/Dir99-93-ecEN.pdf (1999).

（平成13年2月7日受付）