

電子商取引における電子署名 (1)

—グローバル化と国内法の関係—

大 仲 末 雄

目 次

第1章 まえがき

第2章 電子署名

第3章 各国の電子署名法

第1節 国際連合

第2節 アメリカ

第3節 ヨーロッパ

第4節 アジア・オセアニア

第4章 電子商取引における電子署名の機能

第1節 電子署名の法制度上の扱い

第2節 電子署名の実務上の扱い

第5章 むすび

(以上 本号に掲載)

(資料)

1. 国際連合 電子署名に関する UNCITRAL モデル法
2. アメリカ合衆国 連邦電子署名法
3. ヨーロッパ EU 電子署名指令

第1章 ま え が き

電子技術の急速な進歩、特に、電子計算機の普及が、製造業における自動化、効率化をもたらし、さらに、事務の効率化を果たした。また、

インターネットの普及にともない、1980年代後半より商取引の分野にもコンピュータが取り入れられるようになり、電子商取引（eコマースということもある）の時代が到来した。電子商取引は、基本的に、国境を越えた商行為が可能であり、従来の国単位の法体制では対処しきれなくなりつつある。わが国では、高度情報通信ネットワーク社会形成基本法が2000年12月6日に公布され、政府は、電子商取引を普及させるための法整備を進める一方で、電子政府を急速に整備しようとしている。

既存の商取引で確立している契約形態における契約の締結が、紙の媒体などによる知覚可能な意思表示、すなわち、口頭または文書もしくは書面（知覚可能な形態のデータ）による契約申込の意思表示、およびその申込に対する相手方による承諾の意思表示（当事者双方の意思表示）の一致により行われている。これに対し、電子商取引においては、申込およびその承諾の意思表示の対象である情報をコンピュータに入力して処理し、それによって得られる、直接には知覚することができないデータ（データ・メッセージということもある）を、電流、電波、光波などの媒体を用いて伝送する。こうして処理または伝送された電子、磁気、光などの知覚不能なものに量子化されたデータを保存するために、電子または磁気媒体に記録する、いわゆる電磁的記録（これを電子文書または電子書面ということがある）が用いられる。電子商取引を推進するための法整備は、この、従来存在しなかった新しい意思表示手段、情報媒体への記録手段に対して、法的効力を付与することである。すなわち、既存の法規で、契約成立の要件として、文書または書面に対して認めている法的効力を、電子文書または電子書面に対しても付与する必要がある。このための法律がいわゆる電子商取引法である。

ところで、電子商取引による取引として、主に、金融／決済および物の売買の2つがある。このうちの、金融／決済については、銀行業務が大幅に電子化され、最近では、コンビニエンスストアでのバンキングのみならず、自宅から送金するホームバンキングも可能になっている。こ

電子商取引における電子署名（1）

の金融／決済の電子化については、いわゆる電子資金移動（EFT=Electronic Fund Transfer）として、クレジットカード、デビットカード、プリペイドカードなどの電子マネーが整備されつつある。また、電子商取引の安全を担保するために、アメリカ、イギリス、カナダ、シンガポール、オーストラリアなど、英米法系の諸国において、不動産取引に際して利用されているエスクロー決済方式⁽¹⁾の応用が提案されている。この決済方式は、取引の安全を図るための条件付第三者委託で、有効な契約を締結した当事者の合意に基づいて、譲渡人、諾約者（約束者）または債務者が、捺印証書、債券、株券、その他の文書または金銭を中立の第三者（これをエスクロー・エージェントという）に預託するものである。エスクロー・エージェントは、契約の定める条件が成就するまで、当事者双方から預託された証書類または金銭を保管し、条件成就時に譲受人、要約者（受約者）または債権者に引渡すことにより、両当事者間の債権・債務を決済する。

また、物品の売買契約の締結に際して用いられる文書または書面には、いわゆる署名（わが国の記名・押印もこれに含まれる）を添付することが多い。それは、その署名に用いる紙媒体上のインクによる筆跡または朱肉による印影が比較的改ざんが困難であり、さらに印鑑の偽造については刑法上の規制もあるからである。したがって、署名があれば、その文書または書面は、真正であると推定することができるとともに、これを添付した文書または書面が改ざんされてなく、それと署名との関連付けおよび署名者の本人性（身元）を証明することができれば、当該文書または書面の完全性を証明することができる。しかし、電子文書または電子書面およびこれに添付する電子署名は、特殊な技術的対策を施さないかぎ

(1) 堀裕，六川浩明，藤池智則「インターネット・エスクロー決済の法的構成案の検討」，(NBL 707号 (2001年) 29頁)，本田正樹「インターネット取引の決済について(上)(下)」，(金融法務事情1608号 (2001年) 30頁，同1609号36頁)。

り、複製および改ざんが極めて容易であり、しかも、その複製・改ざんを検証または識別することが困難である。そこで、ある一定の法的要件を具備する法規を制定し、その要件を技術的に満たす電子署名に対して、紙媒体上の署名と同等の法的効力を付与する必要がある。このための法律が電子署名法である。すなわち、電子商取引には、電子商取引法と電子署名法とを制定する必要がある。電子商取引における消費者保護の問題、電子決済の問題を含めて、電子商取引法については、別途検討することとし、ここでは、主として、電子署名法について考察する。

電子商取引に用いる電子署名についての現時点での課題は、①セキュリティの確保、②社会制度面の整備などが考えられる。⁽²⁾その主なものとして、米国の暗号化技術輸出規制の緩和、デジタル・キャッシュと通貨制度の見直し、電子商慣習、特に電子署名技術と現行民商法との整合性⁽²⁾の見直し、国境を越えた商取引における契約の成立(準拠国の法律との衝突)要件の見直しなどがあり、早期に法律を整備する必要がある。電子商取引の法制度の問題、特に、セキュリティの問題を考えるにあたって、ネットワーク、すなわち、通信の側面から取り上げたものと、取引すなわち契約締結の側面から見たものがありうる。前者は、通信法などの公法ないしは行政法の観点からの議論になり、後者は、私法、主に民商法の観点からの議論になる。

これまででは、対面による口頭または書面(紙に書いた)による意思表示の一致によりなされることをベースにし、隔地者間では郵便等による契約の申込の意思表示と相手方の承諾の意思表示との一致を、知覚可能な媒体を通して行うことにより、契約が成立するものとされている。それに対して、電子商取引では、知覚可能な媒体(紙媒体にプリントアウトしたもの)以外の、ソフトウェアやデジタル化されたデータ・メッセージなどの知覚することができない情報をも取引の対象とする。そして、原則

(2) 桜井伝治『エレクトロニック・コマースの課題』NTT出版編『電子商取引のすべて』26頁(NTT出版、1996)。

電子商取引における電子署名（1）

として、ネットワークを経由して、隔地者間で、ときには国境を越えて、契約の締結が書面によらない電子媒体（わが国の法律では、これを電磁的記録という）によってなされる。ときには、コンピュータとコンピュータとの間の自動処理により売買（注文と納入）が行われる。

したがって、情報の秘匿あるいは本人確認や情報の信憑性確認の手段と法による保護が不可欠である。そのために、わが国をはじめ、各国で電子署名法が制定され、従来の紙の上に署名する場合の効力と同等の法的効力を、一定の要件を満たす電子署名に対して付与している。

第2章 電 子 署 名

電子商取引の安全を法的に確保するための最も重要な要素のひとつとして、電子署名をあげることができる。電子媒体におけるメッセージに添付する署名を電子署名という。

電子署名には、いわゆるデジタル署名が、現時点では一般的である。しかし、それ以外にも、指紋、声紋、会話記録（いわゆる録音）、筆跡などのバイオメトリックスの応用が考えられ、近い将来、これを用いた電子署名の実用化が期待される。

電子署名が署名としての法的効力を認められる（署名された文書または書面が、真正に成立したことを推定されるか、または証拠力を付与される）には、一定の要件が必要である（電子署名認証法2条および3条）。メッセージが、署名者自身が作成し署名したことを確認しうること、および、そのメッセージが署名後に改ざん（⁽³⁾ 改変）されていないことを証明しうる⁽³⁾ことがその要件である。

電子署名に法的効力を認める電子署名法の性格については、各国の電子署名法の規定で、必ず明確に述べているというわけではない。しかし、UNCITRAL モデル法および EU 指令が電子商取引の関連法規として、

(3) 電子署名法では、電子署名者の身元確認＝本人認証が要件になっていない。

すなわち私法として位置付け、アメリカ連邦法および日本法では、公法として位置付けているように思われる。⁽⁴⁾

電子署名のうち、現時点で、上の要件を満たしているデジタル署名は、つぎのようにして実行される。

① 発信人(署名者)は、メッセージを、ハッシュ関数という特殊かつ署名者固有の関数で、一定の長さに切り刻んで重ねたり折り畳んだりすること(ハッシュ)により、一定の長さの短いメッセージにする。この短いメッセージをハッシュ結果といい、一般的にメッセージ・ダイジェストという(意味のある文章ではなく、単なる数字の羅列である)。ハッシュ関数のうち、メッセージ・ダイジェストから、もとのメッセージをうることができないようにするハッシュ関数を、一方向性(または片道)ハッシュ関数という。

② 発信人は、このメッセージ・ダイジェストを、個人秘密鍵を用いて暗号化する。これがデジタル署名である。

このデジタル署名に用いる暗号方式を公開鍵暗号方式といい、平文を暗号文にする暗号化と、暗号文を平文に戻す復号化では異なるけれども、数学的に関連を有する一対の鍵(鍵対という)を用いる。暗号化は個人秘密鍵を用いて行ってもよく、公開鍵によって行ってもよい。しかし、復号化には、鍵対のうちの暗号化に用いたものでない方の鍵を用いなければならない。通常、デジタル署名のためには、署名者(発信者)を特定することができる必要があるので、署名者の個人秘密鍵を用いて暗号化する。これに対し、メッセージ(契約文など)の暗号化には、名宛人(依存者、受信者)だけがそのメッセージを読むことができ

(4) UNCITRAL および EU のものは、電子商取引法と一体であることを規定で、または公式の注釈で述べている。アメリカ合衆国の連邦電子署名法は、法律の番号付けが public law としてなされている。また、日本の電子署名認証法は、三省堂発行の模範六法(2001年版)では、憲法編の裁判所法の部に含まれている。

電子商取引における電子署名（1）

るようにする必要があるので、名宛人の公開鍵を用いて暗号化し、名宛人が自らの個人秘密鍵で復号化する。

これに対して、シーザーの時代から暗号が用いられているが、これらは、共通鍵暗号方式といわれるもので、暗号化と復号化のいずれに対しても同じ鍵（これを共通鍵または秘密鍵という）を用いる。この共通鍵暗号方式では、鍵を秘密裏に相手方に引渡す必要があり、両当事者が鍵の保管に十分な注意をし、必要に応じて鍵を変更する必要がある。この方式は、署名には使用することができない。

- ③ 発信人は、メッセージとデジタル署名とを同時にまたは別々に、通信ネットワークを通して名宛人（依存者）に送信する（電磁記録媒体に記録して郵送してもよい）。この場合には、メッセージを暗号化してもよい。この暗号化には、デジタル署名に用いる暗号方式を用いてもよい。しかしながら、デジタル署名に用いる公開鍵暗号は、暗号化および復号化に必要な計算量が多いので、長文のメッセージに使用するには不適當である。そこで、発信人は、共通鍵暗号方式で共通鍵を用いてメッセージを暗号化する。そして、この共通鍵を別の秘密チャンネルまたは郵便で送るか、または名宛人（相手方、受信者）の公開鍵を用いて暗号化し、署名者自身のデジタル署名と一緒に送信する。
- ④ 受信者（依存者・検証者ということもある）は、デジタル署名を、署名者の公開鍵を用いて復号化してメッセージダイジェスト（ハッシュ結果）を作成する。
- ⑤ 受信者は、平文のメッセージを、暗号化されている場合には、暗号文をこの共通鍵によって復号化した平文のメッセージを用いて、①と同じハッシュ関数でメッセージ・ダイジェストを作成する。このハッシュ関数は、署名者から直接または認証局を經由して署名者の公開鍵（および証明書）と共に入手することができる。なお、共通鍵が暗号化されて送られてきた場合には、受信者の個人秘密鍵を用いて復号化して、共通鍵を取り出す。

⑥ 上の④と⑤で得られた2つのメッセージ・ダイジェストを比較する。これを検証という。この2つが一致すれば、受信したデジタル署名は、署名者自身が署名したものであり、受信したメッセージは、署名後に改ざん（改変）されていないと判断することができる。

⑦ 署名用の公開鍵暗号としては、RSA 暗号が多く用いられる。また、電子署名とは直接には関係ないけれども、メッセージの暗号化には、アメリカ合衆国の NIST（国立標準技術研究所＝The National Institute of Standards and Technology）が標準規格に採用している DES（20世紀末まで）、AES（21世紀初頭より）が多く用いられている。

なお、AES として、NIST は2000年8月に、ベルギーの若い技術者 Dr. Joan Daemen と Dr. Vincent Rijmen が提案した方式（Rijndael）⁽⁵⁾を採用した。

⑧ 電子署名を用いた取引の安全を確保するために、上記の署名技術とそれに用いた暗号解読の困難さなどの技術的要素だけでなく、暗号化に用いる鍵の管理およびハッシュ関数および暗号化のための鍵対についての公的な認証を行う認証局、認証局の発行する証明書および公開鍵の配布、証明書の失効リストを発行するなど、電子署名の信頼性を保証する必要がある。そのような一連のシステムを、PKI（Public Key Infrastructure＝公開鍵インフラストラクチャー、公開鍵基盤または公開鍵認証基盤）という。

(5) NIST “Commerce Department Announces Winner of Global Information Security Competition”, Oct. 2, 2000 (<http://www.ta.nist.gov>) より。なお、NIST の標準規格により、アメリカの暗号についての規制が、実質的に緩和されている。

(6) 暗号文を正規の鍵を用いて、平文に戻すことを暗号文の復号化または復号といい、正規の鍵を所持せずに、試行錯誤などの方法によりその適合する鍵を作成して、平文に戻すことを暗号文の解読という。

第3章 各国の電子署名法

このような法整備に関して、アメリカ合衆国では、NCCUSL (NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS=統一州法委員会全国会議) は、UCC 2 (売買) を改正する議論において、2 B (ライセンス) を制定する方向で準備した。しかし、結局、UCITA (Uniform Computer Information Transaction Act=統一コンピュータ情報取引法) および UETA (Uniform Electronic Transaction Act=統一電子取引法) の2つの独立法を制定することになった。⁽⁷⁾

一方、ユタ州が先行してデジタル署名法を制定し (1995年)、続いて、カリフォルニア州が、デジタル署名法を制定した (1995年)。この動きに対して、ABA (American Bar Association=アメリカ法律家協会) がデジタル署名法ガイドラインを発表した (1995年、1996年に改正) のを端緒として、各州で、署名の電子化の法整備がなされた。しかし、法律の内容は、ユタ州のものが詳細に規定しており、ほぼ ABA のものと同じであるのに対して、カリフォルニア州のものは、デジタル署名に従来の署名と同等の法的効力を認めるだけの簡単なものである。その後、バイオメトリックスなどを活用したデジタル署名以外の電子署名に対しても、同様に効力を認める、いわゆる、媒体中立の法律を作ろうという動きがあり、フロリダ州 (1996年) およびイリノイ州 (1998年) がその主旨に沿った電子署名法を制定した。⁽⁸⁾ 連邦政府は、このような各州の統一性のなきが各

(7) この経緯については、信森毅博「米国における電子取引法の検討状況 (1)~(4)」(NBL No. 663, 16頁, No. 665, 40頁, No. 669, 46頁, No. 675, 32頁 (1999)), およびペンシルバニア大学法学部のホームページ (http://www.law.upenn.edu/bll/ulc/ulc_frame.htm) に詳細に述べられている。

(8) この間の事情については、内田貴「電子認証・電子署名をめぐる法制度整備のあり方(上)(下)」(NBL No. 675, 6頁, No. 676, 28頁 (1999)) に詳しく紹介されている。また、それぞれの条文は、各州政府のホームページ、および ABA のホームページから入手することができる。

州間の電子商取引を阻害するようになることを恐れて、全世界および国内商取引における電子署名法 (Electronic Signature in Global and National Commerce Act=連邦電子署名法とも呼ばれている) を2000年6月に⁽⁹⁾制定した。

国際的には、EUが電子署名に関する指令(1999年)⁽¹⁰⁾と共に、電子商取引に関する指令(2000年)⁽¹¹⁾を制定し、各国に対してこれを遵守する法律の整備を促している。国連は、1996年に、電子商取引に関するUNCITRALモデル法およびその手引書を採択し発表した。しかし、署名に関しては、当初は、電子署名についてもこの電子商取引に関するモデル法と同時に制定するつもりであったが、アメリカでの州法制定の変遷の影響を受け、その制定が大幅に遅れ、2000年9月に条文が、2001年6月に手引書が採⁽¹²⁾択された。

(9) United States Code Title 15§7001 to 7006, 7021, 7031. この法律の試訳を、資料2として添付してある。

(10) 399L0093 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (Official Journal L 013, 19/01/2000 p. 0012-0020)。なお、この条文の試訳を資料3として添付してある。また、K.F.レンツ教授による訳文(レンツ、K-F「EU電子署名指令の翻訳」青山法学論集43巻1号(2001年)154頁)がある。

(11) 300L0031 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (Official Journal L 178, 17/07/2000 p. 0001-0016)。これについては、K.F.レンツ教授による訳文(レンツ、K-F「EU電子署名指令の翻訳」青山法学論集42巻1号(2000年)98頁)、および米丸教授による論説(米丸恒治「EU情報社会サービス基盤法制とその課題—その一、電子商取引指令の検討—」立命館法学2001年第2号、1頁)がある。

(12) United Nations Commission on International Trade Law [Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures] UN Document A/CN.9/493. (17 May 2001)。これに対する

電子商取引における電子署名（1）

これらの国際機関の動きに呼応して、ヨーロッパ各国が EU 指令に基づいて電子商取引法を作成しているほか、カナダ、オーストラリア、シンガポール、フィリピン、マレーシア、インド、韓国などが相次いで電子商取引法と電子署名法（両方または片方だけ）を制定した⁽¹³⁾。特に、アジア各国およびオーストラリア、カナダは、電子商取引に関する UNCTRAL モデル法を参考にした法律を制定している⁽¹⁴⁾。

わが国は、電子署名及び認証業務に関する法律を2000年5月に公布し、2001年4月に施行した。それに関連して、商業登記法も改正されたほか、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によって、書面要件のある法律のうちの50の法律を、電磁的記録の授受（コンピュータとネットワークによる通信による情報の伝達）を書面の代わりに用いることを認めることとして、一括改正した（これを IT 書面一括法ということがある）。また、電子消費者契約および電子承諾通知に関する民法の特例に関する法律（電子消費者契約民法特例法または電子消費者契約法）が、2001年6月に公布された。

電子商取引は、必然的にグローバルなものとなるため、各国間の法制度の整合性が重要になる。もちろん、電子署名についても同様である。以下、各国政府のホームページなどにより入手した、電子署名およびその認証についての法律の概要を紹介する。

多くの国において電子署名に関する法制度整備が進んでいる。そのほ

試訳を、資料1として添付してある。

(13) 各国の法律は、各国政府のホームページで公開されており、比較表として、ASEAN ELECTRONIC COMMERCE LEGISLATION COMPARISON TABLE (version dated 1 Dec 2000) がある。韓国の条文は、近藤佐保子訳 夏井高人 監修「韓国の『1999年電子商取引基本法』(仮訳)」(<http://www.meiji.ac.jp/>の夏井教授ホームページ)があり、また英訳は、<http://www.consumersinternational.org/>から入手することができる。

(14) カナダ：Electronic Commerce Act, 2000, およびオーストラリア：ELECTRONIC TRANSACTIONS ACT 2000 という名称の法律がある。

とんどもは、電子署名に手書きの署名と同等の法的効力を認めることを目的とし、電子的な認証を法制度において手当てすることにより、電子的情報処理を用いた効率的な情報交換を目的としている。

電子署名、電子認証に関する法整備については、その法制度の対象は、各国で開きが大きく、公開鍵暗号システムを用いる PKI による狭義の電子署名いわゆるデジタル署名から、一般的な電子認証やデジタル署名以外の電子署名を含む広義の電子署名までである。ILPF (Internet Law and Policy Forum) の調査報告では、電子署名認証法におけるアプローチには、(1)規範的 (prescriptive)、(2)二段階 (Two Tier)、(3)最小限主義 (Minimalist) の3つがあるという。(1)は、デジタル署名とその認証を対象とするもので、法律を制定した国として、アルゼンチン、ドイツ、イタリア、マレーシアがあり、ガイドラインとして、日本の電子商取引実証推進協議会 (ECOM) の提案をあげている。なお、米国 ABA のガイドライン、ユタ州のデジタル署名法がこれにあたる。(2)は、技術的中立を考慮するが、現時点での安全な電子署名をも法律に盛り込む二重の規定を設けるもので、EU の指令および UNCITRAL が当初統一ルールとして起草したもの、シンガポールの法律などがこれに該当する。(3)は、技術の急速な進歩による法律の陳腐化を恐れて、技術的中立を重視し、規定を必要最小限に抑えるもので、報告では、オーストラリアの法律をあげている。現在では、日本、アメリカ合衆国を始め多くの国が採用している。また、⁽¹⁵⁾ UNCITRAL モデル法もこれに該当する。

各国が立法化に当って、どのように考えているかについて、その概要を以下に示す。⁽¹⁶⁾

(15) Survey of International Electronic and Digital Signature Initiatives (Internet Law and Policy Forum Home Page, <http://www.ilpf.org/intsurvey>, Last updated: September 24, 1999)。

(16) この項目の選定にあたって、ECOM：認証局検討 WG『認証に関わる諸外国の法制度・調査報告』4頁、ECOM (1998年) に準拠した。

電子商取引における電子署名（1）

紹介項目は、(1)名称、(2)法律の状態・分類、(3)法規の適用範囲、(4)署名の定義（技術特性）、(5)認証局の責任、(6)電子署名・デジタル署名の有効性・証拠力、(7)義務・要件、(8)相互認証、(9)料金の考え方（刑事・民事の罰則を含む）、(10)その他、とする。

第1節 国際連合

現在、電子署名および認証局に関連する法的事項について、電子署名に関する UNCITRAL モデル法が制定され、その手引書と共に発表されている⁽¹⁷⁾。これは、1997年12月にほぼまとまっていた、PKI によるデジタル署名をベースにした、電子署名一般ルール（案）の面影をほとんど残していない（比較のため、両方とも記述する）。

(ア) 電子署名統一ルール（案）（1997年12月現在）⁽¹⁸⁾

- (1) 名称 電子署名統一ルール（案）
- (2) 法律の状態 草案段階→電子署名に関する UNCITRAL モデル法に引き継がれた。
- (3) 適用範囲 国際統一ルールとし、私法の側面に限定する。公的政策、行政法、消費者法、刑法の側面を扱わない。
- (4) 署名の定義（技術特性） 第I節. 安全な電子署名として、1条で、技術中立性を念頭において、つぎのように定義している。「(b)『電子署名』は、電子形式の、またはデータ・メッセージに添付された、または論理的に関連し、そして、その者を識別し、かつ、データ・メッセージの内容を、その者が承認したことを示すことを意図する者によって、使用された署名データを意味する。」と定義している。

(17) 国連文書 A/CN.9/493, (17 May 2001), <http://www.un.or.at/>より検索（2000年）。

(18) 同 A/CN.9/WG.IV/WP.73 (12 December1997), <http://www.un.or.at/>より検索（2000年）。この草案は、結局採用されず、つぎの(i)が採用された。

その上で、「(c)『安全な電子署名』を、(i)4条、5条の要件を満たすデジタル署名。または(ii)つぎによりその作成時の特定の人の署名であることを検証することができること。①その使用者に、唯一リンクされていること、②即座に、客観的かつ自動的にその人を確認することができること、③その使用者だけの管理下にある手段を使用して作成されていること、④メッセージの改ざんがあれば、電子署名を無効にする方法で、データ・メッセージにリンクしていること。または(iii)そのビジネスの通常の過程で、その生成、……にかかわった当事者によって事前に合意し、適切に適用された状況下で、商業的に妥当な電子署名である。」と定義している。第II節、デジタル署名として、4条に、代替案A、Bを規定している。要約すると、「デジタル署名」は、データ・メッセージ(平文)と署名者の公開鍵を所持する者が、つぎのことを正確に決定することができる非対称暗号システムを使用するデータ・メッセージ(暗号文)からなる、電子署名のひとつのタイプを意味する。①暗号化が、署名者の公開鍵に対応する署名者の個人秘密鍵を使用して作成されたか否か、および、②署名前のデータ・メッセージが署名後に改ざんされたか否か。

- (5) 認証局の責任 11条で、契約責任として、①認証局と利用者間の契約で決定すること、②認証局は、契約があるかまたは技術的に不可避な場合には、責任を免除または制限することができること、しかし、それがはなはだしく不公平なときは、免除または制限条項の実施をしなくてもよく、③悪意または不注意でなした場合は、認証局の責任は有限ではない、と規定している。また、12条で、証明書への依存者に対して、①認証書記載内容を誤り、②失効手続をせず、③認証局運用規程(CPS=Certificate Practice Statement)準用法規を無視したことに対して責任を負う。そのうえで、免責のための要件を規定している。

電子商取引における電子署名（1）

- (6) 電子署名・デジタル署名の有効性・証拠力 2条にて、①安全な電子署名によって認証されたデータ・メッセージは、a. 署名の後に改ざんされていない、b. 本人の署名である、c. メッセージに署名する意思で署名した、と推定している。②安全な電子署名以外の電子署名により認証されたデータ・メッセージについては、データ・メッセージまたは電子署名の完全性に対する推定効がなく、立証が必要である。5条において、①データ・メッセージに一定の要件を満たすデジタル署名がなされた場合に、そのデジタル署名は安全な電子署名とみなされ、②データ・メッセージに①の要件を一部満たしていないデジタル署名がなされた場合に、認証局の証明書の本人と公開鍵とを正確に関連付けるための十分な立証がなされたときは、デジタル署名は、安全な電子署名とみなされる。このように、本人性（身元）についての推定効には触れていないが、非改ざんについての推定効をも付与している。
- (7) 義務・要件 16条で、依存者の求めに応じて、証明書記載の利用者を確認するために必要な情報、認証局の責任限界に関する情報の提供などの義務を規定している。また、条文ではないが、7条の注釈48に、①独立性、②損失リスクに耐える財政的基盤、③暗号技術に対する専門的識見、④継続性、⑤ハードウェア、ソフトウェアの承認、⑥監査結果の維持および独立主体者による外部監査、⑦非常事態対応計画、⑧信頼できる人選、⑨認証局自身の個人秘密鍵に対する保管体制、⑩内部セキュリティ、⑪ユーザへの通知を含む業務停止に対する措置、⑫補償とその表示、⑬責任の範囲、⑭保険、⑮他の認証局との相互運用、⑯鍵喪失または不正使用時の鍵失効手続、⑰認証局内での認証機能の独立性を信頼性評価要素としてあげている。
- (8) 相互認証 17条では、この規則の下でサービスを提供する外国認証局について、18条では、国内認証局による外国証明書の保証につ

いて、19条では、外国証明書の認定について規定している。

(9) 料金の考え方 (刑事・民事の罰則を含む) 規定なし

(イ) 電子署名に関する UNCITRAL モデル法 (2001年7月)

(1) 名称 電子署名に関する UNCITRAL モデル法

(2) 法律の状態 制定済

(3) 法規の適用範囲 1条は、適用範囲として、「本法は、電子署名が商業的活動の文脈で使用される場合に適用する。ただし、消費者の保護を意図する法の規定を変更するものではない。」と規定し、商取引すなわち私法の範囲に限定し、その上、国内法による消費者保護を優先している。

(4) 署名の定義 (技術特性) 2条の定義は、「本法の目的に対して、つぎの各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。(a)「電子署名」とは、データ・メッセージに添付または論理的に組み入れられた電子書式のデータを意味する。それは、データ・メッセージに関連する署名者を識別するため、およびデータ・メッセージに包含される情報を署名者が承認するために使用することができる。」としている。このように、名称を「電子署名」とし、技術的中立性を重視している。また、審議の中間段階(上記(ア)(4)参照)には定義が存在していた「安全な電子署名」、「デジタル署名」については、その定義がなくなっている。

(5) 認証局の責任 9条は、認証サービス提供者の行為として、①表示に従うこと、②合理的な注意義務、③依存者に対して自己の本人性、証明書の真正性、証明書の有効性、アクセス可能性、電子署名(鍵)の安全性、失効の措置とその通知などの責任を規定している。

(6) 電子署名・デジタル署名の有効性・証拠力 効力について、明文の規定はない。しかし、3条は、「本法においては、第6条第(1)項で規定した要件または準拠法の要件を満たす電子署名を生成する手法の法的効力を排除、制限、または剥奪をするために適用してはなら

電子商取引における電子署名（1）

ない。ただし、第5条（合意による変更）はこの限りではない。」とあり、6条(1)項で、「法が人の署名を要求する場合、関連合意を含むすべての事情に照らして、データ・メッセージが作成され、かつ、通信された目的に対して適切な電子署名と、同程度に信頼することができる電子署名が用いられたときは、その要件は、データ・メッセージとの関連において満たされる。」としている。また、(3)項で、「つぎの各号に掲げる要件を満たすときは、電子署名は、第(1)項に規定した要件を満たす目的に対して、信頼することができるものとみなされる。(a)署名生成データは、それが使用された文脈の範囲において、他の者ではないその署名者にリンクされること。(b)署名生成データは、署名時点で、他の者ではないその署名者の管理下にあったこと。(c)署名時点より後になされた電子署名に対する変更を検出可能であること。(d)署名に関する法律要件の目的が、それが関係する情報の完全性に関する保証を提供するためである場合には、署名後に、その情報に対してなされた変更を検出可能であること。」と規定している。したがって、この要件を満たしたときは、紙ベースの署名と同様の効力が認められる。また、データ・メッセージの真正な成立の推定効が付与されることになる。しかし、完全性については、立証責任があり、推定効はない。

- (7) 義務・要件 義務については明確な規定はないが、8条、9条、11条で、署名者、認証サービス・プロバイダ、依存者のそれぞれの行為を規定している。署名者には、無権限使用を回避するための注意および署名生成データが危険にさらされていることを通知する行為を、認証サービス・プロバイダには、一般的な注意のほか、依存者が有効性確認のためにアクセス可能なことを保証し、署名生成データが危険にさらされたことに対しては、その旨の通知と失効サービスの提供および信頼できるシステムならびに財政基盤および人材を維持する行為を、依存者には、信頼性の検証、失効の有無および

制限の確認などの行為をする義務が課される。特に、9条は、認証サービス・プロバイダの行為について、「(1)認証サービス・プロバイダが、署名としての法的な効力に対して使用することができる電子署名をサポートするためのサービスを提供するときは、その認証サービス・プロバイダは、つぎの各号に掲げるところによるものとする。(a)認証サービス・プロバイダの方針と実務に関して、認証サービス・プロバイダが行った表示に従って行為すること。(b)その有効期間を通して、常に証明書に関連しているかまたは証明書に含まれる認証サービス・プロバイダが行なった、すべての重要な表示の正確さと完全性を保証するために、合理的な注意をすること。(c)証明書からつぎに掲げる事項を、依存者が確かめることを可能にする合理的にアクセス可能な方法を提供すること。(i)認証サービス・プロバイダの本人性、(ii)証明書で確認された署名者が、証明書が発行された時点で、署名生成データを管理していたこと、(iii)署名生成データは、証明書が発行された時以前には、有効であったこと。(d)関連を有するときは、証明書その他から、つぎに掲げる事項を依存者が確認しうるようにする合理的にアクセス可能な方法を提供すること。(i)署名者を確認するために使用する手法、(ii)署名生成データまたは証明書を使用する可能性がある目的または価値に関する何らかの制限、(iii)署名生成データが有効、かつ、危険にさらされていないこと、(iv)認証サービス・プロバイダが規定した責任の範囲に関する制限、(v)第8条(1)項(b)号に従って署名者に通知する方法が存在するか否か、(vi)適時に失効サービスが提供されたか否か。(e)本条(1)項(d)号(v)の下でサービスが提供される場合には、署名者が第8条(1)項(b)号に従って通知する方法を提供すること。また、(d)号(vi)の下でサービスが提供される場合には、適時に失効サービスが得られることを保証すること。(f)そのサービスの遂行において、信頼できるシステム、信頼できる手続および信頼できる人材を利用

電子商取引における電子署名（1）

すること。(2)認証サービス・プロバイダは、第(1)項の要件を満たしえなかったときは、その責任を負うものとする。」と規定している。さらに、上の(1)(f)の信頼性については、10条で、資産や人材など、財政的基盤の確保のほかにも詳細に規定している。また、要件については、上述のように、6条につきの事項の規定がある。①信頼できる電子署名の使用、②信頼できるシステムの使用と管理、③改変の検出が可能、④信頼度確保の方法の確立および非信頼性の立証責任。また、モデル法の手引書の61に、前述(ア)のルール案の注釈の48と同様の記述がある。⁽¹²⁾

- (8) 相互認証 12条に規定がある。「(1)証明書または電子署名が法的に有効か否かの決定、またはその範囲の決定において、つぎの各号に掲げる事項は無関係とする。(a)証明書が発行されたか、または電子署名が生成または使用された地理的な場所。(b)発行人または署名者の営業所の地理的な場所。(2) [制定国] 外で発行された証明書は、それが実質的に同等な信頼性のレベルを提供するときは、[制定国] 内で発行された証明書として、同じ法的効力を、[制定国] において有するものとする。(3) [制定国] の外で生成または使用された電子署名は、実質的に同等な信頼性レベルを提供するときは、[制定国] 内で生成または使用された電子署名として、[制定国] において同じ法的効力を有するものとする。(4)証明書または電子署名が、第(2)項または第(3)項の目的に対して、実質的に同等な信頼性レベルを提供するか否かの決定において、認定された国際標準規格その他の関連要素にも関係の有するものとする。(5)本条第(2)項、第(3)項および第(4)項にもかかわらず、電子署名または証明書の使用する種類について、当事者間で合意した場合には、その合意は、国内法の下で無効でない限り、国境を越えた認定の目的に対しては、十分として認定されるものとする。」と規定している。

- (9) 料金の考え方（刑事・民事の罰則を含む） 規定なし

第2節 アメリカ

合衆国は、アメリカ法律家協会（ABA）が「デジタル署名法ガイドライン」⁽¹⁹⁾を公表してから、州法として各州でデジタル署名法、電子署名法が制定されている（ほとんどすべての州）。連邦としての電子署名法⁽²⁰⁾が2000年6月30日に制定され、クリントン大統領が電子署名方式で署名した。

各州の電子署名法の多くは、認証機関等に関する規定である。しかし、これとは別に、広く電子的署名を認める規制緩和の動きがある。FDA（連邦食品医薬品局）は、電子記録・電子認証に関する規則を策定し、1997年8月に施行した。それは、一定要件のもとで、暗号による電子署名や、広くバイオメトリックスによる認証手段を認めている。従来の署名のほかに、電子的に処理するための要件を与えて拡大したことになる。UCITA（統一コンピュータ情報取引法）と UETA（統一電子取引法）⁽²¹⁾では電子的な署名の法的効力について規定している。また、1年の有限立法として1997年に制定した電子金融サービス法は、電子署名の法律上の効力を認めていた。⁽²²⁾

(19) Information Security Committee Electronic Commerce and Information Technology Division Section of Science and Technology American Bar Association “Digital Signature Guidelines-Legal Infrastructure for Certification Authorities and Secure Electronic Commerce August 1, 1996” <http://www.abanet.org/scitec/ec/isc/dsgfree.html> (1999年)

(20) <http://thomas.loc.gov/cgi-bin/bdquery/>: より検索(2000年)。法律の略称は、Electronic Signature in Global and National Commerce Actである。この法律の条文は、資料2として添付してある。ただし、それは、合衆国法典(USC) (<http://www4.law.cornell.edu/uscode/15/>) に拠ったので、条項番号が制定時のものとは異なる。

(21) UCITA（統一コンピュータ情報取引法）は、当初、UCC2B編として、コンピュータ関係のライセンス契約を対象に検討されたが、現在は、このような独立法になった。また、これとは別に UETA（電子取引法）を、電子商取引一般の制度として制定している。

(22) ECOM：認証局検討WG『認証に関わる諸外国の法制度・調査報告』

電子商取引における電子署名（1）

これらを統一する意味で制定されたものが、連邦電子署名法である。この法律は、各州間および国際間の電子商取引を促進するために、商取引における電子署名に対して、手書き署名と同様に、一定の法的効力を付与することを狙ったものである。すなわち、この法律の主な目的は、(1)各州間および国際貿易の電子商取引を促進すること、(2)そのための障害になる各州の電子署名法の相違点を除去すること、(3)国際的な電子商取引を促進することである。

なお、連邦電子署名法は、各州内では州法が優先適用されることになっており、連邦法は任意規定である。

この他に、カナダが統一電子商取引法を制定している。⁽²³⁾カナダはコンウェルスの自治領であり、その上、各州の法律が優先するため、ここに掲げたものは、モデル法としての機能を持つことになる。この国は、独立の電子署名法を制定していない。

(ア) アメリカ合衆国 連邦電子署名法

- (1) 名称 全世界および国内商取引における電子署名法 (USC, Title 15, Chapter 96, Subchapter I)
- (2) 法律の状態 Act (公法 No. 106-229. USC は、Title 15, Chapter 96, Subchapter I として収録)
- (3) 適用範囲 全て、ただし、連邦法優先に対する免除 (7002条) および特定の例外がある (7003条)。特に、7003条において、①遺言、遺言補足書または遺言信託、②養子、離婚、その他家族法の問題、③各州で有効な統一商事法典に規定する事項を除外している。
- (4) 署名の定義 (技術特性) 7006条(5)項で、「用語『電子署名』とは、電子的方法で生成、作成、送信、通信、受信、または保存された契約その他の記録を意味する」とし、デジタル署名という用語を用いていない。また、(2)項は、「用語『電子的』とは、電気的、デジタル、

5 頁 ECOM (1998年)。

(23) <http://www.law.ualberta.ca/alri/ulc/index.htm>

磁氣的，無線，光學的，電磁的その他同様な能力を有する技術に関連することを意味する。」と規定している。このように，技術的中立性を考慮した規定になっている。

- (5) 認証局の責任 規定なし
- (6) 電子署名・デジタル署名の有効性・証拠力 7001条(a)項（総則）で、「州際通商または海外貿易においてまたは影響がある取引に関して，制定法，規則その他の法の原則（本章および本章の第II節以外の）にかかわらず，つぎの各号に掲げるところによるものとする。(1)そのような取引に関連する署名，契約その他の記録は，それが電子書式であることを唯一の理由として，法的効力，有効性，または執行力を否認することはできない。(2)そのような取引に関連する契約は，電子署名または電子記録が，その成立において使用されたことを唯一の理由として，その法的効力，有効性，または執行力を否定することはできない。」とし，電子書式，電子署名を理由とした法的効力の否定・否認を禁止している。この規定からは，電子文書の推定効は，紙の文書の場合と同様に扱われ，個別に判断されることになる。
- (7) 義務・要件 認証に対する規定は存在しない。しかし，記録の保存が要求される。
- (8) 相互認証 認証と同様に規定がない。
- (9) 料金の考え方（刑事・民事の罰則を含む） 規定なし
- (10) その他，消費者保護について7001条で詳細に規定している。詳細は，添付の資料2 [アメリカ合衆国 連邦電子署名法] 7001条(c)消費者開示(1)電子記録への同意を参照されたい。

（備考） この法律は，各州法の矛盾を解消するためのもので（対象として州際通商と海外貿易を対象とすることを，明白に規定している），認証等の私法的事項については，個別の各州法に委ねているので，あまり詳しい規定をしていない。

電子商取引における電子署名（１）

(イ) 合衆国の主な州

(i) ユタ州デジタル署名法およびデジタル署名実施規則⁽²⁴⁾

ユタ州は、合衆国で最初にデジタル署名法を制定した州で、基本的には PKI によるデジタル署名方式で規定している。デジタル署名法についての ABA ガイドラインは、これを参考にしてしている事項が多い。

(1) 名称 ユタ州デジタル署名法およびデジタル署名実施規則

(2) 法律の状態 Act および Rule

(3) 法規の適用範囲 一般

(4) 署名の定義（技術特性） Act 103 条で、「『デジタル署名』は、初期のメッセージを作成し、かつ、署名者の公開鍵を保持している人が、正確につきのことに決定することができる、非対称の暗号システムを使用しているメッセージの変換を意味する。その変換が署名者の公開鍵に対応している個人秘密鍵を使用して作成されたか否か、そして、変換がなされた後に、メッセージが改ざんされたか否か」と規定し、明らかに公開鍵暗号システム (PKI) の使用を要求している。そして、「個人秘密鍵」、「公開鍵」、「個人秘密鍵の正当な保持」、「デジタル署名の検証」などの定義を行っている。

(5) 認証局の責任 Act 309 条は、推奨依存限度と責任、推奨依存限度の重要性、証明書に対する推奨依存限度を規定することにより、発行認証局および未承諾加入者は、全リスクの大きさが推奨依存限度を超えない範囲に対してのみ、その証明書に依存することを勧告する。すなわち、認可認証局に対する填補限度は、認可認証局が本項の適用を放棄しない限り、認可認証局は、以下のようにするものとする。過誤または偽造のデジタル署名に関して、認証局が本章のす

(24) 『Commentary to the Utah Digital Signature Act Utah Code Annotated Title 46, Chapter 3 (1996)』 <http://www.rules.state.ut.us/> より (2000年), および ECOM: 認証局検討 WG『認証に関わる諸外国の法制度・調査報告』6頁, ECOM (1998年)。 <http://www.ecom.or.jp/> (1999年)。

すべての重要な要件に従っているならば、加入者の過誤または偽造のデジタル署名への依存によって生ずる損失に対しては、責任を負わないものとする。以下のいずれかに対して、推奨依存限度として証明書に指定された額を超える責任を有しない。①認可認証局が確認する必要がある事実の証明書での虚偽表示への依存によって生じた損失、または、証明書を発行する際に302条に従うための過失、②証明書への依存による損失を回復する行為における直接的、填補損害賠償に対してのみ責任を有する。ただし、以下の直接填補損害賠償は含まない。①懲罰的または懲戒的損害賠償、②逸失利益、貯蓄、または機会損失に対する損害賠償、③肉体的および精神的苦痛に対する損害賠償、④310条は、適正な保証契約に基づく取立、⑤原告の取立権。それとは反対に、適当な保証契約における規定にかかわらず、適当な保証契約が保証証券業務ならば、人は保証証券に指定された主体に対する支払いへの適切な権利の全額、または保証証券の支払期間内に1つ以上このような適切な権利があるときは、保証証券の額に等しい担保の最大の負債合計までの比例配分で取り立てることができる。また、適当な保証契約が信用状であれば、人は、信用状で指定された顧客への支払いに対する制限付権利の全額を、または信用状の支払期間内に1つ以上、このような制限付権利を有するときは、信用状の額に等しい発行人の最大の全負債合計までの、比例配分額までを発行金融機関から取り立てることができる。要求者は、その期間内に支払いの制限付権利の原因となる、すべての人々に対する適当な保証契約に関して、負債合計が適正な保証契約の額を超えるべきではない、と規定され、同じ適正な保証契約に関して、引き続いて回復することができる。弁護士報酬については、支払いに対する制限付権利の金額を回復することに加えて、要求者は、制限付権利を生じさせているか、またはその期間内の弁護士報酬を回復しているすべての人に対する適正な保証契約上の負債合計が、適

電子商取引における電子署名（1）

当な保証契約の額を超えるべきではないと規定した要求を集めるに際して、要求者によって被らされた合理的な金額の弁護士報酬、および法廷訴訟費用を、それが使い果たされるまで、保証契約の収益から回復することができる。請求手続としては、適当な保証契約の担保または発行人への支払いに対する適切な権利を回復するために、要求者は、以下のようにするものとする。要求者の名前とアドレスを、請求額および支払いの制限付権利の根拠、および担当部署の原則によって必要とするその他の情報を記述している担当部署に対して、請求の書面通知を提出すること。そして、制限付権利に基づく判断の認証謄本を通知に添付すること。原告が本項に実質的に従わない限り、適当な保証契約の収益からの支払に対する制限付権利の回復は排除されるものとする。請求手続の時間的制限としては、上の請求手続において必要な請求の通知が、請求に対する根拠である本章の違反が発生した後2・3年以内に提出されない限り、適当な保証契約の収益からの支払に対する制限付権利の回復は永久に排除されるものとする。というように、責任限度を設けてその範囲で損害を補償することになっている。

- (6) 電子署名・デジタル署名の有効性・証拠力 Act の401条は、『総則』：法の原則が署名を要求するか、または署名がないときにある結果を生じることを規定している場合には、つぎのときには、その原則が満たされる。①そのデジタル署名は、認可認証局が発行した有効な証明書に示された公開鍵に対する参照で検証されるとき、②メッセージに署名する意図で、そのデジタル署名を署名者が添付したとき、③受け手は、署名者がつぎのいずれかであることを知らず、通知も受けていないとき、a. 加入者としての義務に違反したこと、b. またはデジタル署名用の個人秘密鍵を正当に保持していないこと。ただし、本章においては、他の準拠法の下で、署名として有効なシンボルを排除するものではない。』と規定している。また、

402条の「低信頼性デジタル署名」は、「法または契約による別段の規定がないかぎり、デジタル署名に対する依存がその状況下で合理的でないときは、デジタル署名の受け手は、デジタル署名が偽造であるというリスクを当然のこととする。本条に従って、受け手が、デジタル署名によらないことを決定したときは、受け手は、即座に署名者に対して、デジタル署名によらないことを決定したことおよびその根拠を通知するものとする。」と規定する。そして、403条で、「その全体についてデジタル署名している。そして、そのデジタル署名が認可認証局によって発行され、デジタル署名が生成された当時有効であった公開鍵によって、検証することができるものであったときは、紙に書いた文書と同様に、メッセージは有効であり、執行可能であり、効力を有する」としている。さらに、404条は、「署名者が唯一の正本であるべき、デジタル署名付のメッセージの場合を指定したことが明白でない限り、その事実が有効、かつ、執行可能なメッセージを構成する場合にのみ、デジタル署名付メッセージのコピーは、メッセージの原本として有効かつ執行可能である」としている。ただし、201条で、「当事者間での契約で、別段の規定をしない限り、本条の認可要件は、デジタル署名の有効性、執行力、または妥当性に影響しない。ただし、本章のパート4が認可認証局によって発行された証明書によって検証することができないデジタル署名に関連して適用されないものとしたものを除く。なお、309条の責任限度額の規定は、無免許の認証局には適用されない。」とし、無免許認証局の発行した認証書にも法的効力を認めている。認可された認証局の発行した公開鍵で検証しうる、いわゆる、安全なデジタル署名を添付した電子文書には、執行力が付与されている。したがって、完全性の推定効を付与していることになる。

- (7) 義務・要件 a. (Act) 認証局に対する規定は、301条～303条にわたっている。詳細は省略するが、この条項は、パート3に含まれ

電子商取引における電子署名（1）

ている。パート3. 認証局および加入者の任務要約は、「このパートは、認可された認証局の運用を支配する原則、特に、認証局によって確認された人、法人、または事業主体に対するデジタル署名鍵対にリンクする、証明書、記録の発行の一時停止、失効に対する原則を規定する。このパートは、証明書における虚偽表示を禁じ、加入者に対して個人秘密鍵の秘密を保持することを要求する。さらに、それは重要な証明書にて指定または勧告された依存基準限界に対して認証局の責任を制限する。」と規定している。301条. 認証局に対する一般要件：信頼できるシステム、問合せに関する開示など、302条. 証明書の発行：証明書の発行に対する前提条件、発行済証明書の承諾の刊行、許容されるより厳しい要件、不完全な発行に対する認証局による一時停止または失効、命令による一時停止または失効など、303条. 証明書の発行に関して加入者への認証局の保証と義務：加入者に対する保証、加入者に対する進行中の義務、発行に関する表示、刊行での表示などの項目よりなる。その要件などは、201条～204条よりなる、パート2に含まれている。パート2, 認証局のライセンスと規則要約は、「このパートは、デジタル署名の信頼性に重要な、それらのサービスにおける品質の基本的なレベルを保証するために、担当部署に認証局を認可しかつ規制する権限を与える。」と規定している。201条. 認証局のライセンスと認定：認定、ライセンスの発行、限定ライセンス、ライセンスの一時停止または失効、他のライセンスの認定、認可の欠如の効果など、202条. 履行監査：年に一度の履行監査、遵法度の分類と判明事項の刊行、履行監査要件の免除など、203条. 認定認証局のための要件の執行：担当部署の監督能力、ライセンスの限定性、一時失効、または失効、民事罰、監視部門の訴訟費用、手続きと裁定、第204条. 認証局による危険な活動の禁止：商業的に不合理なリスクがないこと、忠告告示の刊行、命令と禁止命令などの項目よりなる。

b. (Rule) 当局への登録料金 (年間500ドル), 保証金 (75000ドル), 開示情報項目 (住所, URL 等), 最低資本金 (5000ドル以上), 認証書の項目, 認証局運用規程の形式, 保管記録の条件, 認証業務停止時期の義務, 監査人の要件, 規則の見直しについて, 規定している。

(8) 相互認証 規定なし

(9) 料金の考え方 (刑事・民事の罰則を含む) 規定あり (Act 203 条に民事罰の規定がある: 5000ドルまたは与信額の90%のいずれかより少ない額), また, Rule に, 上記の登録料金の規定がある。

(ii) カリフォルニア州デジタル署名法およびデジタル署名規則⁽²⁵⁾

カリフォルニア州の署名法は, 法律が十数行の極めて簡単なもので, 規則でそれを補い詳細に規定している⁽²⁶⁾。

(1) 名称 カリフォルニア州政府法典16.5 (名称なし) および規則「デジタル署名」

(2) 法律の状態 制定法 Code 16.5 および Regulations Title2 Administration Division7 Secretary of State Chapter 10

(3) 適用範囲 公的機関

(4) 署名の定義 (技術特性) Code 16.5 (a)は, 「……取引に対して要求するかまたは使用することを意思表示する当事者は, 本条の要件を満たすデジタル署名の使用によって署名を書き添えることができる。……」とし, デジタル署名を規定している。そして, 規則22000条は, 「『デジタル署名された意思表示』は, メッセージに署名した個人にメッセージを関連付ける方法で, コンピュータによって処理

(25) カリフォルニア州ホームページ <http://ss.ca.gov/>より検索(2000年), および ECOM: 認証局検討 WG, 『認証に関わる諸外国の法制度・調査報告』7, 8頁(1998年), <http://www.ecom.or.jp/> (1999年)。

(26) 内田教授は, ABA やユタ州のタイプを「デジタル署名 PKI アプローチ」, カリフォルニア州のタイプを「障害除去アプローチ」といつている: 内田貴「電子認証・電子署名をめぐる法制度整備のあり方(上)」NBL 675号9頁(1999年)。

電子商取引における電子署名（1）

されたメッセージである」と定義しており、必ずしも非対称暗号システムによるデジタル署名を要求していない。しかし、22003条で「デジタル署名が第22003(a)(1)–(5)条での規定と一致している状態で作成されるならば、公開鍵暗号として知られている技術はカリフォルニアの公共の法主体による使用に対して許容することができる技術である。……」とし、非対称暗号システムを明確に想定した規定になっている。

- (5) 認証局の責任 規定なし
- (6) 電子署名・デジタル署名の有効性・証拠力 Code 16.5 は、「(a)……それが以下の属性のすべてを具体化するならば、かつ、そのときのみ、デジタル署名の使用は、手書きの署名の使用と同じ効力を有するものとする。(1)使用している人に対して固有であること、(2)確認可能であること、(3)それを使用している人のみの管理下にあること、(4)データが変更されたときは、デジタル署名が無効にされる程度に、データにリンクしていること、(5)州務長官によって採用された規則に従うこと。」としてデジタル署名の要件を規定し、かつ、手書きの署名と同一の効力を付与している。また、Code 16.5 は、「(b)デジタル署名の使用または承認は、当事者のオプションとするものとする。本条において、デジタル署名の使用または使用許可をするために、公法人を要求しないものとする。(c)略。(d)『デジタル署名』は、それを使用している当事者により手書きの署名の使用と同じ効力を持たせることを意図された、コンピュータによって作成された、電子確認者を意味する。」とあり、その使用について、当事者の意思を重視している。そして、電子署名の推定効についての明文規定は、Code および Regulation の何れにも見出せなかった。
- (7) 義務・要件 州当局の信用審査を受ける（規則で制定）
- (8) 相互認証 規定なし
- (9) 料金の考え方（刑事・民事の罰則を含む） 規定なし

(iii) その他

そのほかに、フロリダ州、イリノイ州、ミネソタ州、ミシシッピ州、ニューハンプシャー州、ニューメキシコ州、ニューヨーク州、オレゴン州、テキサス州、バーモント州、ワシントン州などほぼ全州で法律が制定された。これらの内容は、イリノイ州法に代表されるもので、ユタ州法とカリフォルニア州法との中間的なものであるが、どちらかというユタ州法に近い。さらに、フロリダ州法は、カリフォルニア州法よりもさらに形式を重視しており、電子署名に署名要件を充たすための手続法的性格が強い。イリノイ州法は、電子書面署名法という略称を用い、フロリダ州法は、統一電子署名法という略称を用いている。このイリノイ州法およびフロリダ州法が初期のデジタル署名法から最近の電子署名法への制度整備の流れの端緒になり、UNCITRAL モデル法、合衆国連邦電子署名法、あるいは日本の電子署名認証法の名称および内容に影響している⁽²⁷⁾と考えることができる。

(v) カナダ

- (1) 名称 統一電子商取引法
- (2) 法律の状態 制定法
- (3) 適用範囲 電子署名法ではないので必ずしも適切ではないが、あえて掲げておく。2条(適用範囲)で、「(1)本条を条件として、本法は、[制定法域]に関して適用される。(2)[適切な権限付与]は、[法定の証書]によって、本法を適用しないことに関して [制定法域]の法の下での規定または要件を指定することができる。(3)本法は、以下に関しては、適用しない。(a)遺言書およびその補足書、(b)遺言によって生成された信託または遺言に対する補足書、(c)弁護士の権限、ただし、個人の財務または人権保護に関する範囲に対してとす

(27) 同上 NBL 675号 9頁, 10頁 (1999年), および <http://www.acsp.uic.edu/>, <http://www.mbc.com/or> <http://www.logis.state.il.us/>より検索 (2000年)。

電子商取引における電子署名（1）

る、(d)土地に対する利害関係を生成または譲渡する書類および第三者への対抗力であるべき登録を要求する書類。(4)3章（物品の輸送）を除いて、本法は、流通性のある権原証券を含む流通証券に関しては適用されない。以下略

- (4) 署名の定義（技術特性） 1条(b)号において、「『電子署名』とは、人が文書に調印するために生成または採用し、そして文書に添付または組み込まれた電子書式での情報を意味する。」と規定しているだけで、要件および技術特性について、規定していない。
- (5) 認証局の責任 認証局についての規定はない。
- (6) 電子署名・デジタル署名の有効性・証拠力 10条は、「(1)人の署名に対する〔制定法域〕の法の下での要件は、電子書式の署名によって満たされる。(2)(1)項の目的に対して、〔その要件に対して責任を負うべき当局〕は、つぎの規則を作成することができる。(a)電子署名は、関連合意および電子文書の作成時を含む、すべての情況に照らして、その人の身元証明の目的に対して信頼できるものでなければならない。(b)関連電子書類と電子署名との組合せは、電子書類を作成した目的に対して、すべての情況に照らして、関連合意および電子署名を作成した時を含めて、信頼できなければならない。(3)(1)項の目的に対して、署名または署名付きの文書が、政府に提供されるべきである場合には、その要件は、以下ならば、電子署名のみで満たされる。(a)情報が提供されるべき政府または政府の一部が、電子署名を受け付けることに同意した、(b)場合によっては、政府または政府の一部によって確立された、署名の手法に関しておよび信頼性に関して、電子文書は、情報技術標準規格および要件を満たす。」としている。これだけからは、電子署名の法的効力を検討することはできない。なお、EU 指令および英国ならびにフランスの法律をベースにした、電子署名に関する法律が制定されるものと思われる。
- (7) 義務・要件 認証に対する規定は存在しない。

- (8) 相互認証 認証と同様に規定がない。
- (9) 料金の考え方 (刑事・民事の罰則を含む) 料金の規定はない。

第3節 ヨーロッパ

(ア) EU 電子署名指令⁽²⁸⁾

ヨーロッパ各国で、デジタル署名の法律が制定されたが、国境を越えて取引が行われるようになり、電子商取引の分野でも法制度の統一を図る必要が生じた。そこで、EU はそれに対処するために、電子商取引に対する指令とともに電子署名に対する指令を作成した。各国は、これに合わせて、自国のデジタル署名法または電子署名法を見直すことになる。電子署名に対する指令の概要はつぎのとおりである。

- (1) 名称 電子署名に対する共同体の枠組みに関する欧州議会および評議会指令 1999/93/EC
- (2) 法律の状態 欧州議会および評議会の指令で、これに基づいて、各国が法律を制定する。なお、本指令は、各国に対して、これを遵守した法律を制定することを、期限付きで要求している (13条)。
- (3) 適用範囲 1条は、「本指令の目的は、電子署名の使用を容易にし、その法的承認に貢献することである。本指令は、内部市場の適切な機能を実質的にするために、電子署名および信頼できる証明サービスに対する法的枠組を確立する。本指令は、国または共同体法によって規定された形式に関する要求がある場合、契約その他の法的義務の結論および効力に関する側面をカバーしていない。また、文書の使用を規律している国または共同体の法に含まれる規定と制限に対

(28) DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures “Official Journal of the European Communities”, 19.1.2000 L 13/12, EU. HP: <http://www.europa.eu.int/celex/> (2000年)。また、添付資料2を参照されたい。

電子商取引における電子署名（1）

して、本指令は、影響を与えるものではない。」とし、契約その他の法律を優先している。

- (4) 署名の定義（技術特性） 2条1項は、「『電子署名』とは、他の電子データに付属するかまたは論理的にリンクしており、かつ、認証の手段として有用な電子書式のデータを意味する」とし、2項で「『高度な電子署名』とは、つぎの各号に掲げる要件を満たす電子署名を意味する。(a)それが署名者にユニークにリンクしていること、(b)それが署名者を確認することができること、(c)署名者が自己の単独の管理下で保持することができる方法を使用して、それが生成されていること、(d)データのその後の変更が検出可能な方法で、関係しているデータに、それがリンクしていること。」と定義され、デジタル署名としていない。しかし、6項では「『安全な署名生成デバイス』は、付録IIIで定める要件を満たす、署名生成デバイスを意味する。」とし、付録IIIは、「1. 安全な署名作成デバイスは、適切な技術上および手続上の手段によって、少なくとも、つぎの各号に掲げる事項が保障されなければならない。(a)署名作成のために使用される署名生成データは、実用上、一度だけ出現可能であり、そして、それらの秘密性が合理的に保証されること、(b)合理的な保証を伴って、署名作成に使用される署名作成データを抽出することができず、そして、当該署名は、現時点で利用可能な技術を使用する偽造に対して、保護されること、(c)署名作成に使用される署名生成データは、他の者の使用に対して、正当な署名者によって、確実に保護することができること。2. 安全な署名作成デバイスは、署名プロセスの前に、署名されるべきデータを変更してはならない。また、安全な署名作成デバイスは、署名プロセスの前に、署名者に対してそのようなデータが提示されることを妨げてはならない。」として、詳細に要件を規定している。

- (5) 認証局の責任 証明サービス・プロバイダは、証明書によって依

存者に対してもたらされる損害を保証し、その免責には、挙証責任がある。6条に認証サービス提供者の責任を「1. 公衆に対して、認定証明書として証明書を交付すること、または公衆に対して、そのような証明書を保証することによって、つぎの各号に掲げる証明書に、合理的に依存する権利主体、法人または自然人にもたらされる損害に対して、証明サービス・プロバイダが責任を有することを、最小限、加盟国は保証しなければならない。ただし、証明サービス・プロバイダが、過失がなかったことを自ら立証した場合はこの限りではない。(a)認定証明書に含まれた全情報の発行時点での正確さに関して、および認定証明書に対して規定されたすべての詳細を含んでいる事実に関しての証明書、(b)証明書の交付時点で、認定証明書で特定される署名者が、証明書で付与または特定された署名検証データに対応する署名生成データを保持していたことを保証する証明書、(c)認証サービス・プロバイダが署名生成データおよび署名検証データの両方を作成する場合に、その両方のデータを補足的な方法で使用することができることを保証する証明書。2. 公衆に対する認定証明書として証明書を交付した証明サービス・プロバイダは、証明書の失効を登録しなかったために、証明書に正当に依存する権利主体、法人または自然人が被る損害に対して責任を負うことを、最低限、加盟国は保証しなければならない。ただし、認証サービス・プロバイダが、自身が過失行為をしなかったことを立証しなるときは、この限りではない。3. 制限が第三者に対して承認されうることを規定した、その証明書の使用に関する制限を、証明サービス・プロバイダが認定証明書に示すことができることを、加盟国は保証しなければならない。証明サービス・プロバイダは、それに設けた制限を超える認定証明書を使用することによって生じる損害に対しては、責任を有しないものとする。4. 証明サービス・プロバイダが、証明書を使用することができ、限界が第三者により承認され得

電子商取引における電子署名（1）

ることを規定した取引額に関して、限界を認定証明書において示すことができることを、加盟国は保証しなければならない。証明サービス・プロバイダは、この限界値を超過したことから生じる損害に対しては、責任を有しないものとする。5. 第1項から第4項までの規定は、消費者契約の不公平な条項に関する1993年4月5日の評議会指令 93/13/EEC に対して、不利益をもたらしてはならない。」と規定している。

- (6) 電子署名・デジタル署名の有効性・証拠力 5条は、「1. 認定証明書に基づき、および次の各号に掲げる安全な署名生成デバイスによって作成された高度な電子署名であることを、加盟国は保証しなければならない。(a)紙ベースのデータに関連して、手書きの署名がその要件を満たすことと同じ手法で、電子書式のデータに関連した署名の法律要件を満たしていること、(b)訴訟手続における証拠として証拠能力を有すること。2. 単に、つぎに掲げることを根拠にして、電子署名が、訴訟手続における法的効力および証拠力を否定されないということを、加盟国は保証しなければならない。①電子的書式であること、②認定証明書に基づいていないこと、③認定証明サービス・プロバイダによって交付された認定証明書に基づいていないこと、④安全な署名生成デバイスによって生成されていないこと。」とし、高度な電子署名に対しては、紙ベースでの手書き署名と同じ署名としての法的効力を付与し、訴訟手続における証拠力を付与するように、各国がしなければならないとしている。これは、この要件を満たす電子署名に対して、訴訟手続における証拠力を付与し、したがって、完全性の推定効を付与していることになる。
- (7) 義務・要件 2条10項に、「『認定証明書』とは、付録Iに規定する要件を満たし、かつ、付録IIに規定する要件を満たす認証サービス・プロバイダによって提供される証明書を意味する」とあり、また、付録I. 認定証明書の要件で、(a)認定証明書として交付されたとい

う表示, (b)認証サービス・プロバイダおよびそれが設立されている国の特定, (c)署名者の名前または仮名, (d)関係があれば, 証明書が意図する目的によって含まれるべき署名者の特定の属性に関する規定, (e)署名者の管理下にある署名作成データに対応する署名検証データ, (f)証明書の有効期間の開始と終了の指示, (g)証明書の識別符号 (ID ナンバー), (h)証明書を交付する認証サービス・プロバイダの高度な電子署名, (i)適切なときは, 証明書の使用範囲に関する制限, (j)適切なときは, 証明書を使用することができる取引限度額, を規定している。付録II. 認定証明書を交付する認証サービス・プロバイダに対する要件で, つぎの事項が義務付けられている。(a)証明サービスを提供するために必要な信頼度を立証すること, (b)迅速かつ安全な登録者名簿の運用と即時の失効のサービスを請合うこと, (c)証明書が交付されたかまたは失効にされた日時を正確に決定することができることを保証すること, (d)証明書の交付を受ける者の身元(本人性)を, そして適用可能ならば, その特定の属性を国内法に従った適切な方法によって検証すること, その他にも, (e)適切な専門知識技能の保持者による運用, (f)信頼できるシステムおよびセキュリティを保証することができるシステムの使用, 秘密の保証, (g)損害賠償の危険に耐える財源の確保, (h)記録の維持, (i)署名生成データのコピーの禁止, (j)検証できる形式での証明書の保存に必要な信頼できるシステムの使用, (k)一方向性, 一過性署名生成デバイスの使用, (l)証明時点の技術による偽造が不可能なこと, (m)安全な署名検証が可能なことなど。

(8) 相互認証 (1)第三国にて確立された認証局による証明書は, 自国の認証局による証明書と同等とする, (2)問題が発生したときは, 評議会に解決策を提案し, 評議会は, 条件付多数決で議決する, としている。

(9) 料金の考え方 (刑事・民事の罰則を含む) 特に規定なし

電子商取引における電子署名（1）

イ) ドイツ

ECOM の報告書によると、ドイツは、単独法ではなく、マルチメディア法第3条として、デジタル署名を規定している。⁽²⁹⁾

基本的には、非対称暗号による PKI デジタル署名方式で、認証局の責任、電子署名の有効性・証拠力については、私法上の一般原則によるとして、なんら規定していない。認証局の義務・要件については、提出する計画書の記載事項を規定している。また、認証局の許可は、政府機関と民間の両方が取得可能で、許可取得には要件があり、許可認証局には規制がある。

しかし、弥永助教授によると、その後、EU 電子署名指令に合致させるために、これを改正し、法律名を「電子署名の基本的枠組みに関する法律」とする内容の討議草案が公表されている。それは、対象が電子署名一般に拡大され、定義、用語などを EU 指令の定義に適合させ、認証機関については任意の認証制度であることを示す規定を新設して、監督に関する規定を改正した。さらに、法的効力について電子文書を法的に受入れるために民法典その他の法律を変更する法律草案を作成している。⁽³⁰⁾ 2001年5月22日に電子署名法が1997年のデジタル署名法を改正して施行された。⁽³¹⁾

ウ) イギリス

TTP（信頼される第三者）の規制および認可に関する法制化への提案が⁽³²⁾ 1997年3月に発表された。

しかし、EU 指令を反映するために、1999年11月に電子通信法案が議会

(29) ECOM：認証局検討 WG「認証に関わる諸外国の法制度・調査報告」13頁、20頁 ECOM（1998年）。

(30) 弥永真生「電子取引と EU 諸国の取組み」ジュリスト1183号140頁（2000年）。

(31) FindLaw Digital Signature Law Survey: Germany（2002年7月4日 <http://www.findlaw.gov> より入手）。

(32) 上掲29)20頁。

に提出され、2000年5月に電子通信法として成立した。これは、第I部(第1条~第6条)で、暗号サービス提供者を国務大臣が認定する為の要件、手続等の規定をし、第II部(第7条~第10条)で、電子商取引、データ蓄積の容易化すなわち電子署名や認証ならびに法的効力などについて規定し、電子署名に証拠力を付与している。⁽³³⁾ また2002年3月8日に電子署名規則が施行され、電子通信法2000第7条により、電子署名の証拠能力を付与するEU指令の規定は、実行された。⁽³⁴⁾

(エ) イタリア

イタリアでは、デジタル署名法が1997年3月に発効した。内容は、ほぼ、合衆国ユタ州の規定と同じである。ただ、認証機関の法的位置付けについては、ユタ州の規定では認定制度であるのに対して、イタリアの規定では、義務的な免許制度である。⁽³⁵⁾ しかし、EU指令では、認証サービスの提供をEU加盟国が事前認可にかからしめることを禁じており(EU指令第3条1項)、いずれ改定されよう。現時点では、電子署名法は未制定で、1997年のデジタル署名法および規則が有効である。しかし、2001年に最高裁で、デジタル署名のない文書に対して証拠力を認め、実効的にEU指令を承認した。⁽³⁶⁾

(オ) その他

フランスは、暗号の利用を原則として禁止していた。しかし、1998年に、一定の範囲での暗号の利用が認められるようになり、2000年2月に

(33) 上掲30)ジュリスト1183号141頁参照、また、法律原文は、<http://www.legislation.hmso.gov.uk/acts/acts2000/20000007.htm> または <http://www.mbc.com/ecommerce/legis/uk.html> (2000年)より入手可能。

(34) FindLaw Digital Signature Law Survey: United Kingdom (2002年7月4日 <http://www.findlaw.gov> より入手)。

(35) 法務省 HP: <http://www.moj.go.jp/PUBIC/MINJI02/pub-minji02-03.htm> (1999年)。

(36) FindLaw Digital Signature Law Survey: Italy (2002年7月4日 <http://www.findlaw.gov> より入手)。

電子商取引における電子署名（１）

「情報技術による証拠法および電子署名に関する法を導入する法律案」が可決され、民法典の一部が改正された。これによると、一定の要件を満たす限り、電子的形式の文書、電子媒体の文書は、紙媒体の文書と同一の証拠能力を有することになった。^(37・38)

これ以外のいくつかの国も、EU 電子署名指令を受けた法律を制定している。⁽³⁹⁾

第４節 アジア・オセアニア

アジアでは、電子商取引に関する法制度の整備が進められている。そのうちで、独立した電子署名に関する法律を制定しているのは、日本、韓国、マレーシアである。シンガポール、フィリピン、タイ等は、電子商取引法または電子取引法の中で、電子署名に触れているに過ぎない。

わが国は、電子商取引の法制度について、現時点では、電子商取引を一般的に規定した法律を制定している法律がなく、既存の法律を一部修正して、電子商取引を可能にしている。すなわち電子消費者契約および電子承諾通知に関する民法の特例に関する法律、IT 関連法（「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」で、50の法律を改正するもの）などにより、コンピュータおよび通信ネットワークを利用して、情報を交換すること（EDI）に対して法的効力を付与している。したがって、個別の規定であり、EDI をすべての法律行為に利用することができるというものではない。

この他に、オーストラリア⁽⁴⁰⁾、ニュージーランド⁽⁴¹⁾が統一電子商取引法を

(37) 上掲30)140頁。

(38) FindLaw Digital Signature Law Survey: France (2002年7月4日 <http://www.findlaw.gov> より入手)。

(39) 上掲30)141頁。

(40) “Electronic Transactions Act 2001” [http://scaleplus.law.gov.au/html/numord/3/1937/rtf/2001 No10.rtf](http://scaleplus.law.gov.au/html/numord/3/1937/rtf/2001%20No10.rtf) [Notified in ACT Gazette No 10: 8 March 2001]

制定または起草している。いずれもコモンウェルスの自治領で、電子商取引が多くなっている。この国では、各州の法律が優先するため、ここに掲げたものは、モデル法としての機能を持つことになる。いずれも、独立の電子署名法を制定していない。

1 日本

(1) 名称 電子署名及び認証業務に関する法律

(2) 法律の状態 単独の制定法

(3) 適用範囲 特別の条文がない。しかし、1条では、「この法律は、電子署名に関し、電磁的記録の真正な成立の推定、特定認証業務に関する認定の制度その他必要な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情報の電磁的方式による流通及び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を目的とする。」とあり、特に制限していない。したがって、別の法律で特に規定されないかぎり、商取引に対してのみならず、すべて法律行為に適用される。

(4) 署名の定義（技術特性） 2条1項は、「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って、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って、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。」となっており、技術中立性を保持している。しかし、EU 規定にあるような、安全な電子署名の定義は

(41) FindLaw Digital Signature Law Survey: New Zealand (2002年7月4日 <http://www.findlaw.gov> より入手)

電子商取引における電子署名（1）

ない。

- (5) 認証局の責任 特に規定した条文が見当たらない。しかし、2条2項は、「この法律において『認証業務』とは、自らが行う電子署名についてその業務を利用する者（以下『利用者』という。）その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務をいう。」とし、3項は、「この法律において『特定認証業務』とは、電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。」と定義しており、電子署名の署名者の身元を証明する責任がある。しかし、責任の程度、すなわち利用者に損害が発生したときの、損害賠償責任などの規定がない。これは、既存の印鑑証明と類似している。
- (6) 電子署名・デジタル署名の有効性・証拠力 2章「電磁的記録の真正な成立の推定」との標題が付された、3条は、「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。」と、規定している。この規定は極めて抽象的な規定であるが、2条の要件を満たす電子署名をしている電子書類（電磁的記録）は、紙に書いた署名された書類と同等の効力を推定していること、すなわち、電子署名を添付した電子書式の文書に真正な成立の推定効を与えていることになる。しかし、非改ざんを推定する、いわゆる完全性の推定効を付与していない。したがって、証拠力を付与していない。
- (7) 義務・要件 わが国の法律では、特定認証業務を行う、いわゆる認定認証局と、そうではない認証局が存在することになる。認定認

証局については認定のための要件が規定されている。しかし非認定認証局の要件については規定がない。したがって、非認定認証局の証明があっても、証明のない電子署名の効力との間に差異がないことになる。これは、紙の書類に押す印鑑の銀行印と認印の場合と同様の効力と見ることができよう。それに対して、認定認証局の証明書があれば、印鑑証明のある実印と同様な効力を推定されることになる。認定の要件は、4条(認定)「特定認証業務を行おうとする者は、主務大臣の認定を受けることができる。2 前項の認定を受けようとする者は、主務省令で定めるところにより、次の事項を記載した申請書その他主務省令で定める書類を主務大臣に提出しなければならない。一 氏名又は名称及び住所並びに法人にあっては、その代表者の氏名 二 申請に係る業務の用に供する設備の概要 三 申請に係る業務の実施の方法」と規定し、5条に欠格条項を設けている。そして、認定基準として、6条は、「1 主務大臣は、第四条第一項の認定の申請が次の各号のいずれにも適合していると認めるときでなければ、その認定をしてはならない。一 申請に係る業務の用に供する設備が主務省令で定める基準に適合するものであること。二 申請に係る業務における利用者の真偽の確認が主務省令で定める方法により行われるものであること。三 前号に掲げるもののほか、申請に係る業務が主務省令で定める基準に適合する方法により行われるものであること。2 主務大臣は、第四条第一項の認定のための審査に当たっては、主務省令で定めるところにより、申請に係る業務の実施に係る体制について実地の調査を行うものとする。」としている。義務については、11条(業務に関する帳簿書類)で、「認定認証事業者は、主務省令で定めるところにより、その認定に係る業務に関する帳簿書類を作成し、これを保存しなければならない。」とし、12条(利用者の真偽の確認に関する情報の適正な使用)で、「認定認証事業者は、その認定に係る業務の利用者の真偽の確認に

電子商取引における電子署名（1）

際して知り得た情報を認定に係る業務の用に供する目的以外に使用してはならない。」とし、13条（表示）で、「1 認定認証事業者は、認定に係る業務の用に供する電子証明書等（利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明するために作成する電磁的記録その他の認証業務の用に供するものとして主務省令で定めるものをいう。次項において同じ。）に、主務省令で定めるところにより、当該業務が認定を受けている旨の表示を付することができる。2 何人も、前項に規定する場合を除くほか、電子証明書等に、同項の表示又はこれと紛らわしい表示を付してはならない。」と規定している。しかし、これらの義務は、証明書の失効または一時停止もしくは失効などの利用者への通知または公告義務等の積極的行為義務ではない。

- (8) 相互認証 3章2節 外国における特定認証業務の認定との標題の下に、15条（認定）は、「1 外国にある事務所により特定認証業務を行おうとする者は、主務大臣の認定を受けることができる。2 第四条第二項及び第三項並びに第五条から第七条までの規定は前項の認定に、第八条から第十三条までの規定は同項の認定を受けた者（以下「認定外国認証事業者」という。）に準用する。この場合において、同条第二項中「何人も」とあるのは、「認定外国認証事業者は」と読み替えるものとする。3 主務大臣は、第一項の認定若しくはその更新又は前項において準用する第九条第一項の変更の認定を受けようとする者が外国の法令に基づく認証業務に関する制度で第四条第一項の認定の制度に類するものに基づいて当該外国にある事務所により認証業務を行う者である場合であって、我が国が当該外国と締結した条約その他の国際約束を誠実に履行するために必要があると認めるときは、それらの者に対して、前項において準用する第六条第二項（前項において準用する第七条第二項及び第九条第三項において準用する場合を含む。）の規定による調査に代えて、主務省令で定

める事項を記載した書類の提出をさせることができる。4 前項の場合において、これらの者から当該書類の提出があったときは、主務大臣は当該書類を考慮して第一項の認定若しくはその更新又は第二項において準用する第九条第一項の変更の認定のための審査を行わなければならない。」と規定し、外国の認証業局を認定することができるようになってきている。しかし、わが国の認定認証局と同等のレベルで信頼できる外国の認証局が発行した証明書であっても、わが国の認定を受けていない場合には、その効力は非認定認証局のものと同じ扱いになる。ただし、3項および4項により、書類審査のみで認定されることになろう。

- (9) 料金の考え方（刑事・民事の罰則を含む） 認証に関しては、規定なし。認証局の認定に関しては、政令で定めることになっている。

2 アジア・オセアニア

電子商取引や、電子署名に関する法律は、アジア諸国でもすでに制定されている。マレーシアは、1997年6月にデジタル署名法を制定し、電子署名の定義で非改ざん性を要件としている。本法に対する改正案が、2001年3月、議会に提出された（内容未調査⁽⁴²⁾）。韓国は、1997年6月に電子取引基本法／電子署名法を制定し、電子署名が検証されたときには、メッセージは、改変されていないと推定している（これを完全性の推定ともいう⁽⁴³⁾）。現在、国際法との整合性に配慮した改正を検討している。また、シンガポールは、1998年7月に電子取引法を制定し、同様の推定をしている。フィリピンは電子商取引法を2000年6月に制定し、同様の推定⁽⁴⁴⁾については直接規定していないけれども、完全性の要件を定めている。

(42) FindLaw Digital Signature Law Survey: Malaysia (2002年7月4日 <http://www.findlaw.gov> より入手)。

(43) FindLaw Digital Signature Law Survey: South Korea (2002年7月4日 <http://www.findlaw.gov> より入手)。

(44) 法務省 HP: <http://www.moj.go.jp/PUBIC/MINJI02/pub-minji02-03.htm> (1999年)。および <http://www.miti.go.jp/> より検索 (2000年)。

電子商取引における電子署名（1）

また、施行規則も制定され、最高裁により、電子文書の証拠能力が承認された。⁽⁴⁵⁾ブルネイは、シンガポールの法律とほとんど同じ規定を持つ電子取引命令書を2000年に制定した。タイは、電子取引法案を発表している。そのなかで、電子署名を定義している。デジタル署名ではない。また、認証局は、政府機関によることを原則とし、認定認証局をも認め、⁽⁴⁶⁾外国の証明書もこれに準じている。さらに、改定案を審議中である。中国では電子商取引・電子認証センターが、深鋤（Shenzhen）に設立されたようである（その根拠となる法律については不明）。⁽⁴⁷⁾台湾では、2001年10月31日に電子署名法が通過し、⁽⁴⁸⁾香港は、2000年1月7日に電子商取引条例を制定した。⁽⁴⁹⁾インドでは、2000年10月に情報技術法が施行され、2001年に情報技術省が認証局の認可に関する規則を制定した。⁽⁵⁰⁾

いずれも、UNCITRALの統一規則草案を念頭においたものとなっている。

ア) マレーシア

さらに、フィリピンの法律については、http://www.chanrobles.com/publicactno_8792.htm “Republic Act No. 8792-Electronic Commerce Act of 2000”. シンガポールについては、<http://www.cca.gov.sg> より、韓国については、前掲13)により入手することができる。また、各国の法律は、当該国のホームページのリンクを用いて検索することができる。

(45) FindLaw Digital Signature Law Survey: Philippines (2002年7月4日 <http://www.findlaw.gov> より入手)。

(46) FindLaw Digital Signature Law Survey: Thailand (2002年7月4日 <http://www.findlaw.gov> より入手)。

(47) FindLaw Digital Signature Law Survey: China (2002年7月4日 <http://www.findlaw.gov> より入手)。

(48) FindLaw Digital Signature Law Survey: Taiwan (2002年7月4日 <http://www.findlaw.gov> より入手)。

(49) FindLaw Digital Signature Law Survey: Honkong (2002年7月4日 <http://www.findlaw.gov> より入手)。

(50) FindLaw Digital Signature Law Survey: India (2002年7月4日 <http://www.findlaw.gov> より入手)。

マレーシアの電子署名法の概要はつぎのとおりである。

- (1) 名称 デジタル署名法 (1997)
- (2) 法律の状態 単独の制定法
- (3) 適用範囲 特別の条文がなく、62条および64条など法律の規定から、範囲は明白に制限されない。法律は、黙示によって、すべてのクラスの取引に適用される。
- (4) 署名の定義 (技術特性) 2条 (デジタル署名) は、「最初の署名を持っている人、および署名者の公開鍵により、つぎのことを正確に決定することができる非対称の暗号システムを使用しているメッセージの変換を意味する。
 - (a) その変換が、署名者の公開鍵に対応している個人秘密鍵で生成されたか否か。そして
 - (b) 変換がなされた以後に、そのメッセージが変更されたか否か。電子署名の定義はない。
- (5) 認証局の責任 61条において、「認定認証局が本条の適用を放棄しない限り、認定認証局は、以下による。(a)錯誤または偽造のデジタル署名に関して、認定認証局が本法の要件に従っているならば、加入者の錯誤または偽造のデジタル署名に関して、依存者によって惹起される如何なる損失に対しても責任を負わないものとする。(b)認証局は、つぎの何れに対しても、その推定依存基準限度として証明書で指定された額を超える責任を負わないものとする。(i)認定認証局が確認する必要がある事実の証明書における虚偽表示に関する依存によって惹起される損失。または、(ii)証明書を発行する際に、29条および30条に従わなかったことによる損失。および(c)以下に対して責任を負わないものとする。(i)懲罰的損害賠償。または(ii)身体的または精神的苦痛に対する損害賠償。」と規定している。
- (6) 電子署名・デジタル署名の有効性・証拠力 67条で、デジタル署名に関する推定事項として規定している。すなわち、「デジタル署名

電子商取引における電子署名（1）

にかかわる紛争に対して判決を下す際に、裁判所は、つぎのように推定するものとする。(a)認証局がデジタル署名した証明書が、当該認証局が発行し、かつ、加入者がつぎの事項を承認していること、(i) 認定レポジトリにおいて発行されたこと、または(ii) 発行認証局または証明書に示している加入者によって利用可能にされたこと、(b) 有効な証明書に示した情報および証明書を発行する認定認証局によって確認された情報は正確であること、(c) デジタル署名が認定認証局によって発行された有効な証明書に示された公開鍵によって検証された場合には、つぎのように推定する。(i) 当該デジタル署名は、その証明書に示された加入者のデジタル署名であり、(ii) 当該デジタル署名は、メッセージに署名する意図を有するその加入者によって添付されたものであり、そして(iii) 当該デジタル署名を受取った者は、つぎに掲げることを知らなかったことおよび通知を受けなかったものとする。(ア) 加入者としての義務に違反したこと、または(イ) デジタル署名を添付するために使用した個人秘密鍵を正当に保持していないこと。また、裁判所は、当該デジタル署名が、信頼できるシステムを利用した認定済みの日時付与サービスによってスタンプされる前に生成されたものと推定する。」と規定し、署名が署名者によって真正に作成されたこと、電子文書の改ざん等の加入者としての義務違反のないこと、加入者がその個人秘密鍵を危険にさらすことなく正当に管理していること、すなわち、電子署名の完全性を推定している。その結果、当該電子文書は、裁判手続きにおける証拠力を付与される。

- (7) 義務・要件 これについては、明文規定がない。
- (8) 相互認証 第19条につぎの規定がある。「(1) 管理者は、官報によって発表された命令によって、マレーシア以外の政府機関による免許認証局または認定認証局を認定することができる。(2) 政府機関による免許その他の認可が(1)項のもとで認定された場合には、つぎのと

おりとする。(a)政府機関による免許認証局その他の認定認証局によって発行された証明書で指定された推奨依存基準限界値は、もしあれば、マレーシアの認定認証局が発行した証明書で指定された推奨依存基準限界値と同じように効力を有するものとする。そして(b)政府機関によって免許その他の認可がなされた認証局によって発行された証明書に適用するものとする。」

(9) 料金の考え方 (刑事・民事の罰則を含む)

(イ) 韓国

(1) 名称 1999年電子署名法

(2) 法律の状態 制定法

(3) 適用範囲 特に規定していない。しかし、3条第1項は、「認定認証局が第15条の規定によって提供した証明書に含まれる公開鍵に合致する個人秘密鍵で生成された電子署名は、法令が定めた署名または記名捺印とみなす。」と規定しており、認定認証局による認証が効力要件となる。

(4) 署名の定義 (技術特性) 2条 (定義) の2号で「『電子署名』とは、電子文書を作成した者の身元と電子文書の変更の可否を確認できるよう、非対称暗号化方式を利用して個人秘密鍵として生成した情報であり、当該電子文書に固有なものをいう。」と規定している。このように、デジタル署名に限定した規定になっている。

(5) 認証局の責任 26条 (賠償責任) で、「認定認証局は、認証業務の遂行に関連して加入者または証明書を信頼した利用者に損害を負わせたときは、その損害を賠償しなければならない。但し、その損害が不可抗力または利用者の故意または過失で発生した場合には、その賠償責任を軽減または免除することができる。」と規定し、認証局の責任を明確にしている。さらに、7条 (認証役務) は、「第1項、認定認証局は、正当な事由なく認証役務の提供を拒否してはならない。第2項、公認認証機関は、加入者または認証役務の利用者を不

電子商取引における電子署名（1）

当に差別してはならない。」とし、8条（認定認証局の業務遂行）は、
「第1項、認定認証局は、認証業務を開始する前に、情報化促進基本法第14条の2の規定に基づく韓国情報保護センター（以下「保護センター」という。）から、公開鍵の認証を受けなければならない。第2項、認定認証局は、第1項の規定によって認証を受けた公開鍵に対応する個人秘密鍵を利用して認証業務を遂行しなければならない。」と規定し、認証局の行為義務を定めている。

- (6) 電子署名・デジタル署名の有効性・証拠力 3条（電子署名の効力）で、「第1項、認定認証局が第15条の規定によって提供した認証書に含まれる公開鍵に対応する個人秘密鍵で生成された電子署名は、法令が定めた署名または記名押印とみなす。第2項、第1項の規定による電子署名がある場合には、当該電子署名は当該電子文書の名義人の署名または記名押印であり、当該電子文書が電子署名された後その内容が変更されていないものと推定される。」と規定し、紙媒体での署名と同等の効力をみなし規定で認め、本人性および非改ざんすなわち完全性の推定効を付与し、法廷手続きにおける証拠力を付与している。非否認に関する明示規定はないが、上記1項、2項から非否認を含意すると見ることができる。つぎに、20条（電子文書の時点の確認）は、「認定認証局は、加入者または認証書の利用者の申請があった場合、電子文書が当該公認認証機関に提示された時点を、電子署名で確認することができる。」と規定し、認証局に公証機能の一部であるタイムスタンプの付与権を与えている。これも、証拠力付与の要件のひとつと見ることができる。

- (7) 義務・要件 4条（認定認証局の指定）で、「第1項、情報通信部長官は、認証業務を安全かつ信頼性をもって遂行し得る能力があると認められる者を認定認証局として指定することができる。第2項、認定認証局として指定を受けられる者は、国家機関・地方自治体または法人に限る。第3項、認定認証局として指定を受けようとする

者は、大統領令が定める技術能力・資金力・施設及び装備その他の必要な事項を備えなければならない。第4項、認定認証局の指定手続きその他必要な事項は、大統領令で定める」としてその要件を定めている。その上で、7条（認証役務）は、「第1項、認定認証局は、正当な事由なく認証役務の提供を拒否してはならない。第2項、認定認証局は、加入者または認証役務の利用者を不当に差別してはならない。」とし、8条（公認認証機関の業務遂行）は、「第1項、認定認証局は、認証業務を開始する前に、情報化促進基本法第14条の2の規定に基づく韓国情報保護センター（以下「保護センター」という）から、公開鍵の認証を受けなければならない。第2項、認定認証局は、第1項の規定によって認証を受けた公開鍵に対応する個人秘密鍵を利用して認証業務を遂行しなければならない。」と認定認証局の義務を規定している。

また、19条（認証管理システムの運営）が、「認定認証局は、自己の発給した証明書が有効であるか否かを、誰でも情報通信網を通じて常に確認できるように、認証管理システムを安全に運営しなければならない。」とし、認証局の義務を規定している。さらに、21条（電子署名生成鍵の管理）は、「第1項、加入者は、自己の電子署名生成鍵を安全に保管・管理しなければならず、紛失または毀損したときは、公認認証機関に通知しなければならない。第2項、認定認証局は、加入者の申請がない限り、加入者の個人秘密鍵を保管してはならず、加入者の申請によって加入者の個人秘密鍵を保管する場合においても、当該加入者の承諾なくこれを利用したり流用してはならない。第3項、認定認証局は、自己の利用する個人秘密鍵を安全に保管・管理しなければならず、当該個人秘密鍵が紛失・毀損または盗難・流用されたときは、保護センターに遅滞なく通知して、認証業務の安全性と信頼性を確保し得る対策を講じなければならない。第4項、保護センターは、第3項の規定による通知を受けたときは、当該認

電子商取引における電子署名（1）

定認証局に発給した証明書を失効させ、認証管理システムによって誰でもその事実を常に確認しうよう、遅滞なく必要な措置をとらなければならない。この場合、失効した証明書は、失効した時からその効力が消滅する。第5項、保護センターは、第3項の規定によって認定認証局が認証業務の安全性と信頼性を確保し得る対策を講じたときは、当該認定認証局の申請によって新しい証明書を発行しなければならない。」とし、22条（認証業務に関する記録の管理）は、「第1項、認定認証局は、加入者の証明書と認証業務に関する記録を安全に保管・管理しなければならない。第2項、認定認証局は、加入者認証書等を、当該証明書が失効した日から10年間、保管しなければならない。」と、認証局と加入者の義務を規定している。さらに、23条（電子署名生成鍵の保護など）で、「第1項、何人も他人の個人秘密鍵を盗用または漏示してはならない。第2項、何人も他人の名義で証明書の提供を受け、または、その発給を受けることができるようにしてはならない。」とし、24条（個人情報の保護）では、「第1項、認定認証局は、認証業務の遂行のために必要な個人情報の収集は、最低限のもののみにならなければならない。かつ、本人の同意なく個人情報を収集してはならない。第2項、認定認証局は、収集した個人情報を認証業務以外の目的で利用し、または、流用してはならない。但し、他の法律に特別な規定がある場合または本人の同意がある場合には、この限りでない。第3項、認定認証局は、加入者が自己の個人情報に対して閲覧を申請し、または、当該個人情報の誤謬に対して訂正を要求したときは、遅滞なく必要な措置をとらなければならない。第4項、認証業務に従事する者及び従事していた者は、職務上知り得た他人の個人情報を漏示し、または、これを他人に提供してはならない。」と規定している。さらに、25条（電子署名認証管理業務）第1項は、「保護センターは、電子署名を安全かつ信頼性をもって利用しうように環境を形成し、公認認証機関を効率

的に管理するために認定認証局の公開鍵に対する認証，電子署名認証技術の開発及び普及その他電子署名認証に関連した業務を遂行する」とし，第2項は，「第3条，第6条，第7条，第15条から第19条まで，第22条ならびに第28条の規定は，第1項の規定に基づく認定認証局の公開鍵に対する認証に関してこれを準用する。この場合，『認定認証局』は『保護センター』と，『加入者』は『認定認証局』と読み換える。」とあり，認証局の上部機関である保護センターの義務を規定している。

(8) 相互認証 27条（相互認定）で，「第1項，政府は，電子署名の相互認定のために外国政府と協定を締結することができる。第2項，第1項の規定によって協定を締結する場合は，外国の認証局または外国の認証局の発行した証明書に対して，本法による認定認証局または認定認証局が発行した証明書と同一の法的地位と法的効力を付与することを協定の内容として定めることができる。第3項，情報通信部長官は，第1項の規定によって外国政府と電子署名の相互認証に関する協定を締結したときは，その内容を告示しなければならない。」と規定している。

(9) 料金の考え方（刑事・民事の罰則を含む） 28条（料金の賦課）として，「認定認証局は，証明書の交付申請者または認証役務の提供を受ける者に対して，手数料など必要な料金を賦課することができる。」と規定している。

(ウ) シンガポール

(1) 名称 電子取引法（電子署名法ではなく，取引法の一部として電子署名を規定している—I章 序，II章 電子記録と電子署名通則，IV章 電子契約，V章 安全な電子記録と署名—）

(2) 法律の状態 制定法

(3) 適用範囲 全て，ただし，a. 遺言の作成または発行，b. 流通証券，c. 擬制信託および復帰信託を除いた齒形捺印証書，信託宣

電子商取引における電子署名（1）

言あるいは委任状の生成，履行または実施，d. 不動産の販売その他の譲渡処分または，資産での利害に対する契約，e. 不動産権の譲渡または不動産における権利の移動，f. 権利証書を除く（4条(1)項）。

(4) 署名の定義（技術特性） 2条において、「……『電子署名』とは，電子記録に添付，またはそれと論理的に関連し，そして，電子記録を認証または承認する目的で実行または採用されるデジタル形式での表音文字，表意文字，数その他のシンボルを意味する。」とし，また，「……『デジタル署名』とは，最初の変換されていない電子記録および署名者の公開鍵を保持している人がつぎのことを正確に決定することができる，非対称暗号システムおよびハッシュ関数を使用して，電子記録の変換をする電子署名を意味する。a. その変換が，その署名者の公開鍵に対応している個人秘密鍵を使用して生成されたか否か。およびb. その変換がなされてから後に，最初の電子記録が変更されたか否か。」と規定し，技術的中立性について特に規定せずに，デジタル署名に重点をおいて規定している。

(5) 認証局の責任 特に規定がない。むしろ，免責とも取れる規定がある。すなわち，44条（推奨依存基準限度）は，「(1)認定認証局は，加入者に証明書を発行する際に，証明書における推奨依存基準限度を指定しなければならない。(2)適合性を考慮して，認定認証局は，証明書毎に異なった基準限度の値を指定することができる。」とし，45条（認定認証局に対する責任限度）は，「認定認証局が本条の適用を放棄しない限り，認定認証局は以下でなければならない。a. 錯誤または偽造のデジタル署名に関して，認定認証局が本法の要件を充たしているならば，加入者の錯誤または偽造のデジタル署名への依存によって惹起される損害に対して責任を課すべきではない。b. つぎのいずれかに対して，推奨依存基準限界として証明書で指定された額を超えて責任を課すべきではない。i. 認定認証局が確認する

必要がある事実の、証明書における虚偽表示に関しての依存によって惹起された損害。または、ii. 証明書を発行する際に、29条と30条に従わなかったこと。」と規定している。

- (6) 電子署名・デジタル署名の有効性・証拠力 II章電子記録と署名通則として、6条(電子記録の法的な認定)が、「疑問の回避のために、それが電子記録の形式であるという唯一の根拠に基づいて、情報が法的効力、有効性、あるいは執行力を否定されるべきでないことが宣言される。」とし、7条(書面要件)は、「法のルールが書面で書くべき、書面で提示されるべき情報を要求しているか、または、それがなければ、ある結果に対して規定する場合には、そこに含まれた情報が、その後の参照のために使用可能になるようにアクセス可能であるならば、電子記録は、法のそのルールを充たす。」と規定し、さらに、8条(電子署名)で、「(1)法のルールが、署名を要求するか、またはある帰結になることを規定している場合には、文書が署名付きでなくても、電子署名は、法のそのルールを満たす。(2)電子署名は、取引をより一層推進するために、それがある当事者に対して必要な手続きが存在したこと、電子記録がそのような当事者のものであることを検証する目的で、シンボルまたは安全性手続きの実行の表示を含めて、何らかの方法で立証することができる。」と規定している。

つぎに、V章(安全な電子記録と署名)として、安全な電子署名について、17条(安全な電子署名)は、「かかわった当事者が合意した、規定のまたは商業的に妥当な安全性手続の適用を通して、それを作成した時点で、電子署名がつぎの通りであることを確かめることができる。a. それを使用している人にユニークである、b. その人を確認することができる、c. それを使用している人の単なる管理下での方法でまたは方法を使用して生成された、そして、d. その記録が変更されたときは、電子署名が無効になるような方法で関係

電子商取引における電子署名（1）

する電子記録にリンクされているならば、そのような署名は、安全な電子署名として取扱われなければならない。」とし、18条（安全な電子記録および署名に関する推定）は、「(1)安全な電子記録にかかわる手続に際して反証が提出されないかぎり、安全な状態が関係する特定の時点以降、安全な電子記録は、変更されていないことが推定されなければならない、(2)安全な電子署名にかかわる手続において、反証が提出されない限り、つぎのことが推定されなければならない、
a. 安全な電子署名は、それが関連する人の署名であること、そして、
b. 安全な電子的な署名が、電子記録に調印または承諾することを意図して、その人によって添付されたこと、(3)安全な電子記録か安全な電子署名がない場合には、本章は、電子記録または電子署名の信憑性と完全性に関連する推定を作成してはならない。(4)本条の目的に対する用語の定義……『安全な電子署名』とは、17条または20条の理由で、安全な電子署名として扱われた電子署名を意味する。」としている。

VI章デジタル署名の効力として、19条（デジタル署名付安全な電子記録）は、「デジタル署名で調印された電子記録の部分は、デジタル署名が第20条に基づく安全な電子署名ならば、安全な電子記録として取扱われなければならない。」とし、第20条（安全なデジタル署名）は、「電子記録のある部分がデジタル署名で調印されたときに、つぎの如くならば、そのデジタル署名は、記録のその部分に関しては、安全な電子署名として取扱われなければならない。a. デジタル署名が証明書の有効期間内に生成され、その証明書に示された公開鍵との照合で検証されていること。そして、b. 証明書が人の身元（本人性）に対して、公開鍵が正確に関連付けられることについて、つぎの理由で、証明書が信頼できると考えられる。①証明書が、42条の下で作成された規則に従って運用している認定認証局によって発行されたものであること、②43条の下で作成された規則に従う管理者

により、この目的のために認定されたシンガポール外の認証局によってその証明書が発行されたこと。③証明書が、大臣が規則によって課すかまたは指定することができる、そのような条件に基づき認証局として行動することを、大臣が承認した政府の部または省、州の機関あるいは法定の法人によって発行されたこと。または、④当事者は、安全性手続としてデジタル署名を使用するために、自分たち（送り手と受け手）の間で明白に合意し、かつ、そのデジタル署名が送り手の公開鍵に対する照合により適切に確かめられたこと。」とし、さらに、21条（証明書に関する推定）は、「反証が提出されないかぎり、証明書が加入者によって受入れられたならば、認定認証局が発行した証明書に示されている情報（確かめられなかった加入者情報などの識別情報を除く）は、真正であると推定されるべきである。」として、その完全性（非改ざん性、真正性）が推定される。ただし、依存者のリスクについて、22条（低信頼のデジタル署名）は、「法または契約による別段の規定がない限り、デジタル署名に関する信頼が、つぎの要素に関係を有する事情の下で合理的でないならば、デジタル署名付きの電子記録への依存者は、デジタル署名が署名またはデジタル署名付きの電子記録として無効であるというリスクを負っている。a. 証明書に示したか参照で組み込まれた事実を含めて、デジタル署名付きの電子記録に依存者が知っているかまたは通知を受けた事実、b. 既知ならば、デジタル署名された電子記録の値または重要性、c. デジタル署名された電子記録への依存者と加入者の間での取扱過程およびデジタル署名以外の信頼性または非信頼性の利用可能な徴候、そして、d. 通商、特に、信頼できるシステムその他の電子手法によって行われる通商の用法。」と規定している。このように、安全なデジタル署名に対しては、本人性および非改ざん性すなわち完全性を推定し、執行力すなわち法定手続上の証拠力を付与されている。

電子商取引における電子署名（1）

- (7) 義務・要件 VIII章認証局の義務として、27条で信頼できるシステムの利用、28条で、a. その認証局によって使用された個人秘密鍵に対応する公開鍵を含む証明書、b. 関連する認証局運用規程、c. その認証局証明書の失効か一時停止の通知、d. 認証局が発行した証明書の信頼度、またはそのサービスを履行する認証局の能力の何れかに、重大な、かつ、悪影響を及ぼすその他の事実の開示、およびその認証局運用規程で指定した、そのような事件の発生を支配する手続きに従って行為すべき義務を規定している。さらに29条で証明書の発行について詳細に規定し、30条で証明書の発行に関する表示について規定している。さらに、31条は、証明書の一時停止を、32条は、証明書の失効を、33条は、加入者の同意のない失効を、34条は、一時停止の通知を、そして、35条は、失効の通知を認証局の行為義務として規定している。この他に、加入者（署名者）の行為義務の規定もある。さらに、Ⅷ章、総則で、48条（守秘義務）として、
「(1)本法の目的に対して、または成文法の下でのオフENSE（軽犯罪）に対する起訴、または通信文、情報、文書その他の資料にアクセスした人は、電子記録、本、レジスター、通信文、情報、文書その他の資料を他人に開示してはならない。(2)(1)項に違反した者は、オフENSE（軽犯罪）に該当し、1万ドル以下の罰金または12ヵ月以下の投獄もしくはその両方の刑に処せられるべきである。」としている。
- (8) 相互認証 規定がない。
- (9) 料金の考え方（刑事・民事の罰則を含む） 規定なし
- (E) フィリピン
- (1) 名称 電子商取引法
- (2) 法律の状態 制定法
- (3) 適用範囲 4条（適用範囲）で、「この法律は、地域内のおよび国際的な取引、整理、合意、契約および情報の交換ならびに保管を合

む、商業活動および非商用活動の文脈で使用した、ある種の電子データ・メッセージおよび電子文書に適用されるものとする。」と、電子署名について明示の規定をしていない。しかし、電子商取引のすべてに適用すると考えることができる。

- (4) 署名の定義(技術特性) 5条(e)号に「用語『電子署名』は、人の身元(本人性)を表わし、かつ、電子データ・メッセージに添付または論理的に組み込まれた電子書式の、特有のマーク、特性および／または音、あるいは電子文書を認証または承認する意図で、その者によって使用または採用され、かつ、そのような人によって実行または採用された方法または諸手続を示す。」とし、デジタル署名という用語を用いていない。また、(c)号は、「用語『電子データ・メッセージ』は、電子的、光学的その他同様の方法によって作成、送信、受信、または保存された情報を示す。」と規定している。このように、技術的中立性を考慮した規定になっている。
- (5) 認証局の責任 認証局についての規定はない。しかし、30条で、サービス・プロバイダの責任の範囲について、「本条に別段の規定がない限り、人または当事者は、そのような責任が、以下に基づくならば、第5条に定義されるサービス提供者として行動する人または当事者が、アクセスを単に提供する電子データ・メッセージまたは電子文書に関して、民事または刑事上の責任を条件とされないものとする。a 電子データ・メッセージまたは電子文書の下における当事者の義務と責任、b そのような資料に存在しているかまたはそのような資料に関連して、権利の可能な侵害を含めて、そのような資料またはそのような資料のなかで行った陳述の作成、刊行、散布、配布。その資料には、以下のことが規定される、①サービス・プロバイダが実際の知識を持っていないか、または、そのような資料の作成、刊行、散布、または配布が、そのような資料に、存在または関連して、不法または権利侵害であることが明らかである事実また

電子商取引における電子署名（1）

は状況に気が付いていない、②サービス・プロバイダは、不法なまたは侵害の活動に直接起因する財政的な利益を故意に受領しない、そして、③サービス・プロバイダは、侵害その他の不法行為に直接コミットせず、また別の人または相手方が侵害その他の不法行為にコミットすることを誘発または惹起せず、そして／または別の人または相手方の侵害行為または不法行為からの財政上の利益を得ることはない。さらに、本条においては、何ら、以下に影響しないものとするということを、規定した、a. 契約を根拠とした義務、b. 成文法の下で確立された認可その他の規制管理体制の下におけるなど、サービス・プロバイダの義務、または、c. 成文法の下でも課される義務、d. そのような責任が差止命令に対する基礎を形成する範囲に対する当事者の民事責任は、サービス・プロバイダが、資料に対するアクセスを除去し、妨げ、または拒絶するか、あるいは、法の違反の証拠を保存するために、必要な行為を取得するか、または差し控えることを要求している法の下で、法廷によって発行される。」と規定し、むしろ当事者自治の規定となっている。

- (6) 電子署名・デジタル署名の有効性・証拠力 8条（電子署名の法的な認定）で、「署名が電子署名であり、規定された手続が、以下の下で存在した、電子文書に関係する当事者によって変更することができないことを示すことによって立証されるならば、電子文書上の電子署名は、書かれた文書上の人の署名と同等とする。(a)電子署名を通して、締結されようとする当事者を確認するために、および、その当事者の同意または承認に対して必要な電子文書への自身のアクセスを示すために、ある方法が使用される、(b)関連合意を含めて、すべての事情に照らして、電子文書が作成されたか、または通信された目的のために、その方法が確かで適切である、(c)電子署名を実行または提供することが、取引をさらに続けるために締結されようとする当事者にとって必要である、そして、(d)相手方は、電子署名

を確証すること、および、同じ方法によって認証された取引を継続することを、決定することが認可され、そして可能になる。」とし、9条（電子署名に関連する推定）は、「電子署名にかかわる手続に際して、つぎのことが推定されるものとする。(a)電子署名は、それが関連する人の署名である、そして、(b)電子的に署名された電子データ・メッセージまたは電子文書に依存している人が、署名あるいは信用が欠如していることまたはそれが信頼できないこと、あるいは、その状況の下で電子署名への依存が妥当でないことを知っているか、あるいはその通知を受けているかでない限り、電子署名は、電子データ・メッセージまたは電子文書に調印することまたはそれを承諾することを意図してその人によって添付された。」と規定し、手書き署名と同等の効力を付与し、妥当性を推定している。ただし、この規定からは、電子文書成立真正についての推定効を付与されるに過ぎず、完全性の推定にはならない。もちろん法廷手続における証拠力もない。

また、6条（電子データ・メッセージの法的な認定）で、「情報は、それがそのような法的な効力をもたらしていると称している電子データ・メッセージの形式であること、あるいは、その電子データ・メッセージに、参照によって組み入れられていること、という根拠のみで、有効性または執行力を否定されないものとする。」とし、さらに、7条（電子文書の法的な認定）で、「電子文書は、他の文書または法的な書面として、法的な効力、有効性または執行力を有するものとする。(a)法が書面であるべき文書を要求する場合に、前述の電子文書がその完全性、信頼性を維持し、以下において、その後の参照に使用可能になるなどの、権限を付与することができるならば、その要件は電子文書によって満たされる、(i)電子文書が、記載の追加および認可された変更、あるいは通信、保存および表示の通常の過程で生じる変化を除いて、完全に改ざんされずに残っていた、

電子商取引における電子署名（1）

そして、(ii)電子文書はそれが作成された目的に照らして、かつ、すべての関連情況に照らして確かである。(b)(a)項は、その原本の形式で提示または保有されない文書に対して、そこでの要件が義務の形式であるか否か、または、法が単なる結果を規定するか否かに関係なく適用される。(c)法が、文書がオリジナルの形式で提示されるか、または保有されることを要求する場合には、以下のときは、その要件は、電子文書によって満たされる、(i)それがその最終的な形式で最初に作成された時から、文書の完全性に関して確かな保証が存在する、そして、(ii)その文書は、それが提示されるべき人に対して表示することができる。この法律の規定は、それらの妥当性に対して文書の実行の際に要求した様式性に関する既存法の何らかの、およびすべての要件を変えるために、適用されないものとする、と規定される。証拠を構成する目的に対して、電子文書は、既存の法の下で書かれた文書と、機能的に同等とする。この法律は、認証および最良の証拠に関連する原則を除いて、電子データ・メッセージまたは電子文書の許容性に関連する法定の原則を変更しない。」としている。このことは、完全性を立証することを要求しており、電子署名にその推定効および証拠力を認めていない。

(7) 義務・要件 認証に対する規定は存在しない。しかし、32条（秘密性の義務）で、「この法律の下で認可された目的を除いて、電子鍵、電子データ・メッセージ、または電子文書、本、登録、通信、情報、またはこの法律の下で授与された権限に従う他の資料を利用する権利を得た者は、他人に譲渡せず、他人と共有しないものとする。」として、関係者に機密の保持義務を負わせている。

(8) 相互認証 認証と同様に規定がない。

(9) 料金の考え方（刑事・民事の罰則を含む） 料金の規定はない、また、刑罰規定があるが、電子署名に関するものではない。

(オ) ブルネイ

シンガポールの規定とほぼ同じであるので省略。

(カ) タイ

電子取引法案が、ようやく議会の承認、国王の署名が得られた(2002年2月)。以下は、草案の内容によった。

- (1) 名称 電子取引法案
- (2) 法律の状態 法案段階
- (3) 適用範囲 3条. この法律は、データ・メッセージによって行われる民間商行為に適用されるものとし、国王判例で規定されるような、その適用を認めない法的な性質の取引はこの限りではない。法の下で、州行政機関と何らかの行為の申請、許可、登録、行政命令または実行は、国王判例による規定および手順によるデータ・メッセージの形式で作成されたときは、本法の適用を受ける。そして、特定の事項に関する法による規定および手順に従った法律の実行と同じ法的効力を有するものと見なさなければならない。また、この目的に対して、国王判例は、ある事件における詳細を規定する規則を発行することを州行政機関に要求することができる。
- (4) 署名の定義(技術特性) 4条(電子署名)は、「署名者を確認し、その人が、そのようなデータ・メッセージに拘束されることを承認し、合意したことを示す目的でデータ・メッセージとある特定の人との結びつきを確立するために、電子的方法で生成してデータ・メッセージに添付された証書、文字、数、音響その他のシンボル」とし、33条は、「以下の電子署名は、安全な電子署名であるとみなされるべきである。24条の下で、国王判例に規定された電子署名。」と規定している(注:この規定からは、この電子署名を「特定 PKI」と限定することはできない)。
- (5) 認証局の責任 規定がない。
- (6) 電子署名・デジタル署名の有効性・証拠力 7条が、「法の規定が、情報が書面で提示されることを要求するか、そうでなければ、ある

電子商取引における電子署名（1）

結果について規定している場合には、そこに含まれた情報がその後の参照に対して使用可能になるようにアクセス可能であるならば、電子記録は、その法の規定を満たす。」と規定している。しかし、電子署名法ではないので、証拠力については規定がない。

(7) 義務・要件 規定が存在しない。

(8) 相互認証 38条。外国証明書は、外国証明書の発行に際して、本法の下での信頼できるシステムと同等に信頼でき得るシステムが発行し、かつ、その発行が委員会で規定した規則および手順に従っているならば、本法の下で発行された証明書に与えられるものと同一効力を有するものとみなされなければならない。39条。38条の下で生成された外国証明書によって生成ならびにサポートされる電子署名は、本法の下での証明書によってサポートされる電子署名に与えられているそれと同じ効力を有しているとみなされなければならない。

(9) 料金の考え方（刑事・民事の罰則を含む） 料金の規定はない。

(※) オーストラリア

電子署名に関する法律は見当たらない。1999年から2000年に、各州が電子取引法を制定している。⁽⁵¹⁾イギリスがEU指令に準拠した電子署名法を制定した後に、制定するものと考えられる。

(1) 名称 電子取引法2001

(2) 法律の状態 制定法

(3) 適用範囲 本法が電子取引法であって、電子署名法ではないので、その適用範囲が同じであるわけではない。また、適用範囲の明確な規定はない。

(4) 署名の定義（技術特性） 規定なし。

(5) 認証局の責任 認証局についての規定はない。

(51) FindLaw Digital Signature Law Survey: Australia (2002年7月4日 <http://www.findlaw.gov> より入手)。

- (6) 電子署名・デジタル署名の有効性・証拠力 9条1項は、「この法域の法の下において、人の署名が必要であるときは、つぎの各号に掲げる場合には、その要件は、電子通信に対して満たされたものとみなされる。(a)手法が人を特定しかつ伝えられた情報のその人の承認を示すために使用された場合、(b)その手法が使用されたときすべての関連状況に関係を考慮したならば、その手法が、情報が知らされた目的に対して適切であったのと同様に信頼できた場合、(c)要件が(a)号で述べた手法の使用を通して満たされるということに、署名を付与する必要がある人が、同意する場合。」として電子署名を署名とみなしている。

ただし、電子署名法ではないので、証拠力については規定がない。

- (7) 義務・要件 認証に対する規定は存在しない。
(8) 相互認証 認証と同様に規定がない。
(9) 料金の考え方 (刑事・民事の罰則を含む) 料金の規定はない。

第4章 電子商取引における電子署名の機能

第1節 電子署名の法制度上の扱い

電子署名は、世界中で使用されている手書きの署名やシール、あるいはわが国で日常的に使用されている記名・押印と同様に、必ずしも、商取引の場合に限って用いるというものではない。それは、アメリカの連邦法では、電子署名法を公法の範疇に入れ、わが国でも、電子署名及び認証業務に関する法律(電子署名認証法)を公法として分類していることでも認められよう。

しかし、電子署名に関する UNCITRAL モデル法は、その手引書で、この法律を、電子商取引に関する UNCITRAL モデル法に対する追加として考えるといっている。⁽⁵²⁾ また、電子商取引法と電子署名法とを別々に

(52) UNCITRAL Draft Guide to Enhancement of the UNCITRAL Model Law on Electronic Signatures, UN. Document A/CN.9/493 of

電子商取引における電子署名（1）

制定している国がある一方で、電子署名法の機能を含めた電子商取引法だけを制定し、電子署名法を制定していない国がある。そこで、電子商取引法に電子署名法の機能を含めて規定している国を混乱させないように配慮した上で、電子商取引に関する UNCITRAL モデル法を改正するという手法によらず、電子署名に関する UNCITRAL モデル法を独立に⁽⁵³⁾制定する、という表現が UNCITRAL モデル法の手引書に見られる。

電子署名に関する UNCITRAL モデル法が採択されたことで、今後、電子署名法を制定する国が多くなると思われるが、現時点で電子商取引法とは別に、独立の電子署名法を制定しているのは、アメリカと日本の他、EU 諸国、韓国、マレーシアなど僅かの国にとどまっている。EU は、両者を独立の指令として制定している。EU 各国は、これに従って自国の法律を独立の法律として制定または改正することになる。

わが国は、電子署名認証法を制定したほかに、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）として、50の法律の書面による手続を相手方の同意を前提に、電磁的記録（一般的には電子媒体といわれている磁気テープ、ハードディスク、フロッピーディスクなどの磁気記録、または CD、DVD または MO などの光記録、コンパクトディスク、スマートメディアなどのフラッシュメモリ・IC メモリを用いる電子記録などがある）で代替することを認めた法律を制定した。ただし、この法律は、事業者に対する規制のために書面を要求している場合に、この書面を電磁的記録によって代替することを許容するものであって、民法に規定された書面をすべて電磁的記録で代替することを想定していない。また、電子消費者契約および電子承諾通知に関する民法の特例に関する法律（略称：電子消費者契約民法特例法または消費者契約法）が制定された。この法律には、電子消費者契約の要素に錯誤があった場合の契約の成立要件について、民法の規定を修正する重要な規定があ

4, 65, 66, 67, 68, 86など。

(53) 同上 65

り、また、電子承諾通知の場合には、契約の申込に対する承諾の発信主義の規定（民法526条1項および527条）を適用しないとしている。ただし、この法律は、事業者が個人の消費者との間で契約を締結する場合を想定したもので、それ以外の、個人と個人の間の契約、公共機関の関与する契約などについては適用対象になっていない。このように、わが国の電子商取引への対応は、独立の電子署名法を制定しているほかは、ばらばらに現行法を修正する方法をとっている。このことは、当事者間で合意すれば、電磁的記録によって契約上の書面と同様な効力を推定されると見ることができる。

わが国の電子署名認証法は、一定の要件を満たした電子署名に対して、法的効力を認めている。しかし、電子署名をされた文書について、その効力は、第2条に示す電子署名の要件を満たし、さらに、第3条に示す電子署名デバイスについて適正な管理をしている場合に、それによって作成された電磁的記録が真正に成立したことを推定するに過ぎない。すなわち、「現実には電子署名といわれる技術（現状では、デジタル署名）によって実現できている効果を、法的にも認めることが必ずしも十分ではない⁽⁵⁴⁾」、 「……本人性の推定効とか非改ざん性の推定効なども認めるべきではないかという議論もしていました。……リアルの世界でも実印に認められていない本人性の推定効はともかくとして、……正面から非改ざん性の推定効という形にはなっていません。」⁽⁵⁵⁾ というように、いわゆる完全性に対する推定効がない。今後の運用すなわち判例に委ねられることになる。

前述のように、電子署名認証法は、公法として取扱われ、電子商取引に対してのみ適用されるものではないけれども、関連する法律の改正ま

(54) 稲垣史則＝岩間芳仁＝神田秀樹＝横山経通＝内田貴（司会）「〈座談会〉電子取引 法制度整備の課題」ジュリスト、1183号15頁（2000年）（内田発言）。

(55) 同上、（稲垣発言）。

電子商取引における電子署名（1）

たは特別法の制定状況、あるいは、UNCITRAL モデル法に見られるように、電子商取引と密接に結びついていることは疑う余地がない。カナダ電子商取引法2条(3)項は、遺言とそれによる信託、弁護士の権限、土地の利害関係の生成、譲渡に関する登記を含む文書に対して電子取引法を適用しないとしており、シンガポールの法律も、4条(1)項に同様の規定がある。カナダの法律は、さらに2条(2)項で、各法域で適用範囲を制限してもよいとしている。アメリカ合衆国連邦電子署名法は、これと同様のもののほかに、養子縁組、離婚などの家族法に関する問題、訴訟関係文書、公益事業サービスの解除または終了の通知、個人住宅に関連する事項の通知、健康保険または生命保険給付の解除または終了の通知、健康または安全を危うくする危険がある製品の回収または欠陥に関する通知、および危険な材料、殺菌剤その他有毒なまたは危険な材料の輸送に必要な文書については適用除外としている。このように、電子文書、これに添付する電子署名は、電子商取引に限定されると見てよいであろう。

国際的商取引（貿易）は、これまで、特定の商社を代理店として、特定の当事者間で実行されてきた。しかし、インターネットを用いる電子商取引では、一般消費者が直接取引に参加することができ、しかも、だれでも世界中のどこでも取引することができる国際性をもつことになり、個人による貿易が可能になった。もちろん、在来の当事者間での貿易が電子化され、これに電子署名が用いられることもありうる。また、インターネットなどのオープンなネットワークではなく、両当事者間で閉じた通信回線、ネットワークを使用することもある。

また、わが国では、高度情報通信ネットワーク社会形成基本法に見られるように、政府は、通信ネットワークを利用した電子情報社会の構築を推進しようとしており、これは、電子商取引のみならず、電子政府、すなわち行政の電子化をも推進するものである。この電子政府は、2003年を目標に行政手続きの完全電子化を目指すもので、これにより、従来

からある提出書類を電子化することが期待される。個人情報漏洩の恐れがあるなどの問題を持ったままではあるが、住民基本台帳ネットワークの1次稼動が2002年8月5日から始まった。しかし、電子政府が実現した場合でも、電子化される範囲からは、不動産所有権の取得および移動の登記、出生届、パスポートの交付申請、公開鍵とハッシュ関数よりなる電子署名認証の届出、印鑑登録などのように、身元確認を必要とする事項や重要な取引に関連する事項について、多くの例外が生じると思われる。

この適用範囲の限定の方法には、上述のIT書面一括法のように、個別に電子化するものを規定する方法と、合衆国の連邦法やカナダ法のように、電子化しないものを列挙する方法とがある。電子化の推進には後者が望ましい。今後わが国でも電子化を許容する範囲がさらに増加すると思われるが、各省庁からどのような提案がなされるかが注目される。また、電子化可能なものの中で、現在でも、実印ではなく認印が用いられており、それほど高い信頼度を要求しないものが多いと思われる。これらについては、デジタル署名における当事者間の自己認証のみで認証局の証明書(認証書)を必要としない、いわゆる低信頼のデジタル署名、認定認証局による認証書のないデジタル署名(例えば、PGPのようにネットワーク以外の郵送などの通信系で公開鍵の受け渡しをする電子署名)、またはデジタル署名以外の簡易な電子署名(電子印鑑や電子指紋など電子署名の要件を満たすもの)を認め、その法的効力については、判断を裁判所に委ねるという方法がある。わが国やUNCITRALは、この手法をとっている。それに対して、EU指令に基づくヨーロッパ各国は、国が相当に詳細な規定を設けたPKIを構築するという手法を採っている。これについては、国家が民事に対して可能な限り介入しないことが望ましく、しかも、わが国には、記名押印により署名と同等の効力を認めるということが慣習として認められているため、前者の方法でよいと考える。

第2節 電子署名の実務上の扱い

以上のように、各国において電子署名法が制定され、わが国においても2000年5月24日に電子署名認証法が成立し、2001年4月19日に施行された。これにより、記名押印、特に、印鑑証明を要する取引についても、電子商取引の方式で実行することが可能になった。また、電子署名認証法の施行後、現在（2002年8月）までに、総務省、経済産業省および法務省は、2001年7月13日に、電子署名及び認証法4条1項に基づき、日本認証サービス株式会社が⁽⁵⁶⁾行う特定認証業務「Accredited Sign パブリックサービス」を認定した。その他にも、2002年7月4日現在で、帝国データバンク、株式会社日本電子公証機構、日本行政書士会連合会、株式会社コンストラクション・イー・シー・ドットコム、およびセコムトラストネット株式会社が認定されている。さらに、認定とは別に、日本ベリサイン株式会社は、認証、保証を含むセキュリティ業務を総合的に行っている。署名とは直接関係がないが、日本商工会議所は、電子商取引の安全性を確保するために、オンラインマークを制定し、電子商取引を行う業者について認定している。今後、多くの業者がこの認定を受けるものと思われる。これとは別に、法務省は、2000年4月1日に公布された改正商業登記法に基づく、商業登記に基礎を置く電子認証制度が、2000年10月10日より運用され、法務省管轄の電子認証登記所として、「全国を一として、電子証明書の発行やその有効性に関する証明等を、インターネットを通じて行う登記所として東京法務局を指定」⁽⁵⁷⁾した。また、全国の地方自治体が、印鑑証明と並行して、認証業務を実施しようとしてい⁽⁵⁸⁾る。

このように、電子署名・認証法の施行に伴う民間の認証業者と、法務省の運用する電子登記所が存在することになる。もっとも、法務省が運

(56) 法務省ホームページ (<http://www.moj.go.jp>) より。

(57) 法務省ホームページ (同上) より。

(58) 総務省ホームページ (<http://www.somu.go.jp>) より。

用する電子登記所の機能は、法人が登記簿に記載されているか否かの証明、および、その代表権を有する者が誰であるかの証明に限定されるので、国内向けの制度に過ぎず、国際的な広がりをもつ電子商取引に対してはそれほど重要な機能を果たすとは考えがたい。また、現時点では存在しないが、電子政府が整備され、それが高度化されれば、地方自治体の印鑑証明に対応する、電子署名の認証を各市町村長が行うようになると思われる。この制度は、従来、紙媒体による文書に記名・押印する際に印鑑証明書を添付するわが国の慣習に照らして、新しい電子文書に添付する電子署名に対して認証局の電子証明書と同等の機能を持つことになるかと予想される。このような、民間の認証局による証明と国や地方自治体による証明との二階建ての制度が、国際的にオープンな電子商取引に馴染むかどうかは、大いに疑問が残る。電子署名、電子認証の制度は、各種届出書面の電子化など行政のIT化、すなわち、中央省庁、各地方自治体をはじめとする行政機関でのIT化にも使用される公的性格の強い制度ではある。しかしながら、電子認証を必要とする電子署名は、電子商取引での使用が重要な地位を占め、かつ、国際性があるので、電子商取引の推進に与える影響を含めて、諸外国の制度と、必要があれば法律を含めて、比較しながらこの制度を見直す必要がある。

電子商取引などの私的なものに対して、電子署名を必要とする場合であっても、書籍など低額商品の注文では、暗証番号（ID）での身元確認のデータ交換だけでよく、より高額な取引または継続的取引のときは、電子印鑑などの簡易電子署名を用いる。そして、特定のグループ内での取引のときは、PGPなど、第三者（認証局）認証を要しない電子署名を用い、さらに、高額な取引または重要な取引の場合には、認定認証局の認証を要する電子署名を使用する、というように使い分けることができる。もちろん、電子商取引によることができない、上述のカナダ法に列挙されているようなもの、または、生命や人権にかかわる契約などに対しては、電子署名で代替することができないものもありうる。

電子商取引における電子署名（1）

このように、民対民の法律行為のうち、政府による規制の対象になっている特定のものについては、上述の一括法に掲げたものの書面の電子化が可能になり、しかも、現時点では、特別法で書面を必要とするものうち、電子化が認められるのは、上述の一括法で列挙したものに限られる。しかし、特別法による規制のないものについては、法律で、手書きの署名、押印をした紙の文書を特に要求（強行規定として）されない限り、私的自治の原則に則り、合意によって電子署名をした電子文書による代替が認められる。ただし、法律の規定が、強行規定であるか、任意規定であるかの解釈については、電子文書の出現という、従来の法文化の枠を越えた新しい法文化として、再構築をする必要がある。例えば、現民法の典型契約においては、原則として、その法律行為は、不要式行為である。したがって、契約において交わされる書面は、単に、紛争の際の証拠としての効力を有するに過ぎない。書面によらない贈与契約は、撤回することができるが、撤回を制約する書面については従来から議論がある。この書面の電子化については、民法549条および550条が要式行為を要求していない以上、当事者の合意によって、電磁的記録（電子文書）にて代替することができる。しかし、従来の議論とは異なる観点から、検討する必要がある。すなわち、改ざんの容易な電子文書については、従来の書面に対する解釈とは異なり、真正に成立したものか否か（偽造・改ざんの有無を含めて）の視点で解釈されるべきであって、単に書面（メモなどの様式を含む）であるか電子文書であるかによって、その効力および証拠力ならびに立証責任の帰属を判断すべきものではない。

当事者間の合意により、書面を電子文書で代替することができるといっても、セレモニーの性格を持つ文書（調印式を行う契約文書、表彰状、卒業証書など）の交換、授受などは電子文書に馴染まず、電子署名を使用することにはならないであろう。しかし、事務の合理化、文書保存庫の圧縮などの必要から、調印文書をデジタル化した電子文書にする必要がある場合には、相手方との合意により、電子署名をした電子文書にする

ことは可能であり、電子署名認証法に規定する署名要件を満たした電子署名が添付されていれば、その電子文書が正当に成立したものと推定される。また、従来、板切れへのメモであっても書面としての効力を認められていたが、これに相当する低信頼の電子文書については、簡易な電子署名を添付することで、書面に代替するようになるであろう。この場合、紛争になれば、立証責任は、電子署名作成者にある。また、情報化社会での契約締結には、仮に調印式等のセレモニーが行われる場合でも、紙に手書き署名および押印をした文書に並行して電子文書を交換しておくことが、事後の作業の効率化および火災等の被害を防止するためにも望ましい。

短期的には、デジタル署名であれば署名に使用したハッシュ関数および個人秘密鍵を解読することが不可能であるから、技術的に改ざんの可能性が小さく、この両者に矛盾が生じるとは考え難いけれども、長期的には、技術の進歩により、特に、コンピュータの処理速度が大幅に向上し、改ざんすることができるようになる可能性があり、この両者に矛盾が生じることがありうる。したがって、この両者に矛盾があった場合、その法的効力の優劣が問題になる可能性がある。すなわち、電子技術の進歩に伴い古い電子文書および電子署名の信頼性が低下するため、電子署名の信頼性と、筆跡鑑定などの一応評価基準が確立されている従来の署名手法による判断の信頼性との比較の問題として、議論になるであろう。しかも、電子署名については、今後も技術が進歩しつづけるので、ある時点で行われた裁判による判例が時間の経過とともに、暗号鍵の強度が弱体化するなどの問題が生じ、急速に陳腐化する。したがって、判例の見直しを頻繁に行わなければ、電子文書が真正に成立し、それが維持されているか否かについての判断を、陳腐化した判例を引用して行うことになり、誤った判決を下すおそれがある。そのように、判例の意味付けが、署名の日付、引用判例の日付、当該事件の判決日付との関連で議論しなければならないことを意味する。

電子商取引における電子署名（1）

また、私法上の問題ではないけれども、上述の電子政府の推進政策にもかかわらず、電子署名認証法3条では、「電磁的記録であって情報をあらわ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。）……」と規定している。この括弧書きによって、電子記録情報のうち、公務員が職務上作成したものを除外しているため、公務員は、公文書を電子書式で作成して電子署名を添付しても、当該文書が真正に成立したと推定することができないことになり、法的に有効な電子書式の公文書は存在しえないことになる。

このことは、商業登記所が運用する認証局が、法人の代表者の個人秘密鍵に対応する公開鍵の電子証明書を発行するけれども、この行為の法的効力および電子証明書の有効性についての証明情報の法的効力については、どのように考えればよいのかという疑問を生むことになる。すなわち、商業登記所が発行する電子証明書は、フロッピーディスクなどに証明情報および登記官の電子署名を記録することになっている。

しかし、そのフロッピーディスクは電子書式であって、法的効力に疑問があるので、登記官が押印し、かつ、同一の内容を記述した紙の書面に添付して、交付する必要があることになる。然るに、平成12年9月28日付の法務省民事局の、「『商業登記に基礎を置く電子認証制度』の運用開始について」によると、たとえば、会社代表者の電子証明書発行の申請は、会社代表の印鑑を押した電子証明書発行申請書に自己の公開鍵等の必要事項を記録したフロッピーディスクを添付して管轄の登記所において行う。電子認証登記所は、申請を受けた管轄登記所からの通知を受けて、電子証明書発行の処理を行う。電子証明書の発行がなされると、電子証明書の発行申請書を提出した管轄登記所の窓口において、その電子証明書の番号（シリアル番号）が告知される。管轄登記所の窓口において電子証明書の発行申請の手続を終えた後、申請人は、告知された電子証明書の番号と自己の公開鍵を指定して、いつでもインターネットを通じて、電子認証登記所から電子証明書を取得することができる。この取

得には、対応のソフトウェアが必要である。なお、一度取得した電子証明書は、コピーして何度でも使用することができる。電子証明書を添付した署名文書を受信した者は、その添付された電子証明書について、電子認証登記所に対して、インターネットを通じてその有効性についての証明を請求することができることになっている。当然、それに対する応答は電子書式による書面（電子文書）になり、この証明書には発行者である電子認証登記所の登記官による電子署名が付され、その登記官の電子証明書が添付される。⁽⁵⁹⁾この2つの電子証明書に添付された登記官の電子署名の法的効力については、登記官という公務員がその職務に対して実施するものであるから、上述のように問題がある。もっとも、登記官に対しては、国家公務員法1条による制約があり、また、民訴法228条2項による推定があり、その電子証明書を信用してもよいという考えもある。そうだとすれば、電子署名認証法3条の括弧書き除外規定が、本法の適用範囲を私文書に限定する目的を持つ（夏井教授は、文書が真正に成立したことを推定する、民事訴訟法228条の規定のうち、2項の公文書に対しては、署名または押印を要求していないので、電子署名認証法を適用する必要がなく、4項の私文書に対しては、それを要求しているので、電子署名認証法が適用されるという⁽⁶⁰⁾）。それでもなお、その意義については、上述の疑問が残る（私見としては、確かに、公文書に対しては、民事訴訟法228条3項によって、裁判所は職権で、その成立の真否を当該官庁または公署に紹介することができることになっているけれども、紙媒体の公文書には、所定の記名・押印があり、上記の2項は、それを前提とした規定であると解することができるので、電子署名に関して、私文書と公文書とを差別扱いする必要性が少なく考える）。

また、電子政府が稼働をはじめた後には、ネットワークを通して、本人の保持するカードを用いて、管轄外の自治体窓口において、本人の戸

(59) 法務省ホームページ (<http://www.moj.go.jp>) より。

(60) このことについて、夏井高人『電子署名法』、リックテレコム（2001年）304頁以下に詳細に述べられている。

電子商取引における電子署名（１）

籍簿・住民基本台帳等を管轄する自治体から、戸籍抄本・住民票等を入力することができるようになる。これには、管轄自治体首長の電子署名（信頼度レベルの如何にかかわらず）が添付されることになる（仮に、戸籍抄本に押印された首長の印鑑であったとしても、電子伝送されたものは電磁的記録と同様に、デジタル化され、必要に応じて暗号化・復号化されているなど、電子書式の文書—電子文書—としての性質を持っている）。したがって、この正本の有効性と、上述の、電子署名認証法３条の括弧書きの意味付けとの関係については、問題がある。

さらに、夏井教授によると、本法３条にいう本人は自然人に限られ、法人はこれに含まれず、法人には３条が適用されないと解釈すべきである⁽⁶¹⁾という。そうだとすれば、電子署名を必要とする電子文書で、３条により真正な成立を推定され、法的効力を認められるものは極めて限られることになり、現在の商取引の多くが法人によって行われていることを考えると、この法律（および施行規則）は、法人の作成する文書に記名・押印が添付されるわが国では、時代に逆行するものであり、IT化推進、電子商取引の推進の流れを阻害することになる。夏井教授は、商業登記法を改正して整備した電子認証登記所の発行する商業登記についての電子証明書は、単に、証明書に記載された事項が商業登記簿に記載されていることを電子的に証明しているだけのことであるという。そうだとすれば、この電子証明書が、主に、法人代表者の電子署名に対するものであり、法人の作成する電子文書の真正性がこの代表者の電子署名によっ

(61) 夏井教授は、本法の施行規則５条が、本法３条の本人が法人を含むと解釈する道を絶っているといっている。すなわち、「……、電子署名施行規則５条は、このような解釈を前提として、電子署名法６条に基づき特定認証事業者が利用者の審議確認のために提出させべきものを、①住民票の写し、②戸籍の謄本若しくは抄本、③外国人登録原票記載事項証明書、または、④これらに準ずるものに限定しています。つまり、自然人について本人であることを確認するために用いられる書類に限定しているのです。……」という。同上、311～315頁。

ても推定されないことになり、立法の趣旨に反する。また、法人が電子文書を作成した場合は、法人の代表者が、民法53条によるその代表権に基づいて作成した電子文書とみなすことができるので、電子署名法2条1項の要件を満たす法人の電子署名が添付されている当該法人の電子文書は、真正に成立したものと推定することができる。すなわち、電子署名法3条の本人は、自然人、および自然人である代表者を通しての法人を含むと解すべきである。また、夏井教授が根拠としている電子署名認証法施行規則5条1項には、「……。ただし、認証業務の利用の申込又は第三号の規定する申込の事実の有無を照会する文書の受取を代理人が行うことを認めた認証業務を実施する場合においては、当該代理人に対し、その権限を証する利用申込者本人の署名および押印（押印した印鑑に係る印鑑証明書が添付されている場合に限り）がある委任状（利用申込者本人が国外に居住する場合においては、これに準ずるもの）の提出を求め、かつ、当該代理人について次の各号に掲げる方法のうちのいずれかの一以上のものにより、真偽の確認を行うものとする。（一～三省略）。四 前3号に掲げるものと同等なものとして主務大臣が認めるもの……」とあり、この1項ただし書きから、自然人である代表者（代理人）を通して署名した本人には、法人を含むものと解釈することが可能であり、そのような取扱をすることを可能にするために、4項の規定を設けたと解することもできる。このように、電子署名法の本人には、自然人のみならず法人をも含む、と解釈するのが妥当である。

また、わが国の電子署名認証法は、UNCITRALモデル法を考慮して立案されていると考えられるから、次に述べる、UNCITRALモデル法をはじめ、EU指令および合衆国連邦電子署名法などの規定と同様に、法人に対しても適用されるものと解釈すべきである。

すなわち、UNCITRALモデル法2条(d)項において、署名者の定義として、その人自身またはその人を代表する者のために署名する者とし、また、UNCITRALモデル法の手引書で、「人」を、自然人、会社その他

電子商取引における電子署名（1）

の法人を含むすべてのタイプの権利主体者を包含する、と理解すべきであるとしている。また、EU 指令2条3項にも同様の規定がある。さらに、アメリカ合衆国連邦電子署名法7006条(8)項でも、「人」を、個人、会社、……その他の法人または商業上の権利主体者……としている。

このように、わが国の電子署名認証法の適用範囲は、自然人のみならず、法人をも包含していると考えるのが妥当である。仮に、夏井教授の解釈に沿った判決がなされ、それが確定したときは、立法府において、直ちに法律を改正する必要があると考える。

第5章 む す び

本稿において、各国の電子署名の法的取扱について比較検討し、わが国の電子署名認証法の問題点を指摘した。わが電子署名認証法の問題について、内田教授が先に指摘したもののほかにも、夏井教授は、「……世界標準を意識した新たな立法や法改正を速やかに行うことが妥当……」⁽⁶²⁾と述べている。あえて私見を述べれば、21世紀は、情報化社会になるといわれており、経済活動の国際化が一層進み、現時点でも、為替市場や証券市場などで見られるように、リアルな物品（ハードウェア）やバーチャルな情報（ソフトウェア）などの売買市場についても、世界がひとつの市場とみなされるようになると思われる。わが国としては、UNCITRALモデル法の内容をすべて取り入れ、かつ、各国の法律との間で整合性のある国内法に改正するか、または新たに法律を制定すべきであると考え

以上

次号において、資料として、電子署名に関する UNCITRAL モデル法、電子署名に対する EU 指令およびアメリカ合衆国の連邦電子署名法を

(62) 上掲41, 夏井高人『電子署名法』, 265頁。

手引書または注釈付で紹介する。ただし、手引書および注釈については、前述の内容と重複する部分および条文の規定に直接関係のない部分、例えば審議経過などについては、省略してある。