暗号政策と電子署名

石﨑　靖敏

1. はじめに

暗号技術は，ネットワーク社会において不可欠の情報セキュリティ確保の基本技術である．暗号の機能は，秘匿と認証に大別される．

暗号の秘匿機能は，暗号の古くからの機能であり，ギリシャ・ローマの時代から軍事または外交の分野で使用されてきた．暗号は，1980年代前半までは主として，軍事，外交，民間では金融機関にその利用がほぼ限られていたが，1990年代，いわゆる「情報スーパーハイウェイ」，「情報社会」，「電子商取引」等が提唱されるようになると，民間でも，企業情報の保管，交信，身近な例ではクレジットカード番号やパスワードのネットワークを通しての送信など，情報の秘匿の必要性が生じてきた．情報の電子的な扱いへの信頼の醸成は，情報ネットワーク社会の進展の基礎であり，国際競争力に大きく寄与する．他方，多くの国で，国家安全保障および犯罪捜査のための国の機関による通信傍受[1]が法律で規定されているが，政府機関は，民間での強度の高い暗号の使用が政府機関による従来からの通信傍受を実質的に無効にしてしまうという懸念を持っている．国際的にも，G7リヨン・サミットは，テロリズム対策に最大の優先順位を与えることを決定した．それを受けて，1996年7月のG7閣僚会議は，「合法的な通信のプライバシィを守りながら，テロリズムの行動の防止または捜査の目的でのデータまたは通信への政府の合法的なアクセスを可能とする暗号[2]の使用に関して，国際フォーラムにおける協議を促進することを全ての国に要求する決議」を採択した．

秘匿目的での暗号使用の問題点は，経済発展に寄与する情報社会におけるプライバシィの保護やセキュリティの確保と国家安全保障，対外政策または法執行の目的のための政府機関の通信内容へのアクセス権限の間のバランスをどのようにとるかという点である．

情報社会では，電子商取引や電子政府のように，文書を書面でなく電子的記録で扱うことが増加する．電子的記録は，作成者の成りすまし，記録自体の改竄，記録作成の否認が容易であるという問題点を持っている．これらを解決するのが電子署名である．

G8サミットではテロ対策が論じられると共に，情報社会の進展のための協力も論じられている．ネットワークで結ばれた情報社会では，各国それぞれに構築されてきた制度や文化を背景としながら，制度の調和が必要とされるが，暗号政策や電子署名の制度もその一つであろう．以下，2章において各国の暗号政策およびそれに関する国際機関の動きを，3章において各国の電子署名および国際機関の動きを紹介する．

2. 暗号政策

暗号政策には，暗号の使用の規制と，暗号製品および技術の輸出の規制の2つの側面がある．

政府機関による通信傍受と民間における強度の高い暗号の使用の両立を図るため，鍵寄託（key escrow），鍵回復（key recovery），トラステッド・サード・パーティ（TTP: Trusted Third Party）[3]などと呼ばれる方式が提案されてきた．これらは，政府機関が，通信当事者に知られずに，第三者機関から暗号鍵の入手または平文にアクセスすることを可能にす

いしざき　やすとし
情報通信アナリスト
中央大学研究開発機構客員研究員
〒162-0473 新宿区市谷本村町42-8

[1] 1999年10月から12月に発表された欧州議会資料では，米国，英国，カナダ，オーストラリア，ニュージーランドによる冷戦時代の通信傍受網Echelonが経済情報の収集に使われているとの懸念が示されている

[2] わかりにくい表現であるが，後述のKMIを指していると考えられる．

[3] TTPは，ISO CD 10181-1においてセキュリティ機能において他の組織から信頼されるセキュリティ・オーソリティとして定義され，ISOにおいて標準化作業が行われている．セキュリティ機能としては，公開鍵証明，タイムスタンプ，公証，情報の保管等が含まれている．国によって鍵寄託機能を併せ持つ提案も行われた．

る．暗号を使用する際に，このような方式の利用を強制するか否かが，暗号政策問題の一つの焦点である．

暗号の輸出に関しては，暗号製品および暗号技術は，Wassenaar協約において，軍用および商用両用技術として加盟国が輸出規制を行うべき対象になっている．

以下においては，秘匿目的での暗号の使用と暗号製品および技術の輸出に関する暗号政策について，米国を中心として，各国およびOECDなどの国際機関の暗号政策を概観する．米国はインターネットなどの情報ソフトウェアの高いシェアを占め，事実上の標準を作り出して情報社会をアプリケーションおよび技術の両面でリードしている

2.1 米国の暗号政策

2.1.1 米国暗号政策の前提

暗号政策の前提である政府機関による通信傍受は，犯罪捜査については，合衆国法律集（USC）第18篇—犯罪と刑事訴訟の第119節，第121節，第206節に，国家安全保障および対外政策については，第50篇—戦争と国防の第36節[4]に規定されている．

2.1.2 クリントン政府の暗号政策の経緯

クリントン政府は，国家情報インフラ（NII: National Information Infrastructure）を提唱した1993年，Clipperと通称される暗号イニシアティブを発表した．これは，政府機関が設計した非公開の暗号アルゴリズムSKIPJACK，それを実現する半導体チップClipper Chip，鍵寄託システムを要素とするものであった．鍵寄託技術は1992年にMITのMicali教授が提案してはいたが，このイニシアティブは，鍵寄託に関する多くの論議の発端となった．この提案は，Clipper Chipによる暗号以外の暗号の使用を禁止し，Clipper Chipは暗号鍵を自動的に政府機関に寄託するというものであった．これは，アルゴリズムが非公開[5]で正規の手順でなく政府機関が暗号を復号する裏口が存在するのではないかの懸念，鍵の寄託機関が政府機関であること，暗号アルゴリズムとその実現が市場競争に基づいていないことなど多くの批判をあびた．

これらの批判に対して，クリントン政府は，1995年9月，1996年5月と緩和した提案を行ない，1996年7月には，評判の悪い鍵寄託に代る鍵回復暗号システム（key recovery encryption）を提唱し，全世界的規模での鍵管理インフラ（KMI: Key Management Infrastructure）の構築を提唱した．暗号の使用者にとっても，暗号鍵の紛失などの不測の事態に備えるために暗号鍵の管理は必要であり，鍵回復は，その目的と政府の犯罪捜査，国家安全保障の目的の両方の目的を兼ねたシステムにしようという提案であった．1996年10月には，国際的なKMIを推進する「鍵回復」イニシアティブを発表した．これに呼応し，IBMを中心とする11社の企業は，鍵回復技術の開発のアライアンスを発表し，1997年5月には，60社を超える国際的アライアンスに発展した．

暗号製品および暗号技術の輸出に関しては，米国政府は，国務省の管轄する「米国武器リスト（US Munitions List）」によって，その輸出を統制してきた．米国産業界は競争力が高いと自負する暗号製品の輸出規制緩和を強く希望し[6]，クリントン政府は，1996年11月には，暗号の輸出統制の管轄を国務省管轄の「武器リスト」から商務省管轄の「商業統制リスト（CCL: Commercial Control List）」による統制に移管すると共に，鍵回復を条件に56ビットDESまでの強度の輸出を可とする決定を行った．1998年9月には，この鍵回復の条件の撤廃，更に1999年9月には，小売りの暗号コモディティまたはソフトウェアを中心に，鍵長の制限を撤廃する方針を発表し，新しい規制が2000年1月に商務省から告示された．

2.1.3 議会をめぐる動き

このような政策に影響を及ぼしたと考えられるのは，議会の要請に基づく米国研究評議会（National Research Council）の1996年5月の報告「情報社会の安全確保における暗号の役割（Cryptography's Role in Securing the Information Society (CRISIS)）」である．これは，米国内での暗号の自由な使用，輸出規制の緩和などを勧告している．

米国議会では，第104（1995-1996），105（1997-1998），106（1999-2000）議会と暗号の国内での使用および輸出管理の扱いに関する法案が提出され，審議

---

[4] FISA（Foreign Intelligence Surveillance Act）として有名である．

[5] 暗号アルゴリズムは，それ以前のDES暗号において公開されていた．アルゴリズム公開の場合には「鍵」だけが秘密であり，それを知っているのは使用者のみであるのに対し，アルゴリズム非公開の場合には，「鍵」は暗号使用者の秘密であり，「アルゴリズム」は暗号設計者の秘密となる．したがって，秘密の漏洩元も2箇所になり，危険が増える．第2の問題として，第三者によるアルゴリズムの検証が行われないという問題がある．SKIPJACKも世界一の暗号組織といわれる国家安全保障局（NSA）の設計といわれたが，アルゴリズム公開後すぐに解読された．

[6] 米国の暗号製品輸出規制を回避するために，米国以外の国に開発拠点を設けた米国企業もある．

されてきた．現106議会においては，下院で，H. R. 850 Security and Freedom Through Encryption (SAFE) Act および H. R. 2616 Encryption for the National Interest Act，上院で，S. 798 Promote Reliable Online Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999 および S. 854 E-RIGHTS などの法案が審議されている．

米国議会に提出された暗号関連の法案の多くは，暗号の使用および輸出に対する政府による規制を排除または制限する内容のものであり，行政府の政策とは対立するものが多かった．これまで立法に至ったものはないが，米国政府が国内での鍵寄託の実施を行わず，輸出においても KMI の条件を撤廃する方向にあるので，政府機関のための鍵寄託，鍵回復の論議も決着の方向にあると見られる．

2.1.4 米国における暗号をめぐる裁判

暗号ソフトウェアの輸出管理が，米国憲法修正第1条（言論，出版の自由）に違反しているか否かという点について裁判で争われた．これまで，(1)英語などの自然言語だけでなく，C言語などのコンピュータ言語で書かれたプログラムも言論，出版の自由の対象になり，その輸出の制限は憲法違反である；(2)紙に書かれたソース・プログラムは輸出管理の対象でないが，フロッピーディスク上のソース・プログラムは輸出管理の対象であるという判決が出ている．

ソースコードが紙に書かれているかフロッピーディスクに書かれているかによって輸出管理の対象か否かが変わることを揶揄して，印刷されたソースコードを OCR で読み取っている写真が掲載されたりもした．

これらの裁判は，プライバシィ保護の基と考えられている憲法修正第1条に関連してではなく，言論，出版の自由の基である憲法修正第4条に関連して争われている．これは，米国では，暗号の使用は自由であって，輸出規制のみが実施されていることに起因する．

2.1.5 鍵回復インフラへの暗号専門家の批判

Hal Abelson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller 及び Bruce Schneier の9人の暗号専門家は，1997年5月，「キーリカバリ，キーエスクロウ，及びトラステッド・サード・パーティ暗号の危険性」という文書を発表した．この批判の論点は概略下記のような点である：

(i) 暗号は，システムとしては送信者と受信者の間だけで使用される単純なものである．政府提案の全世界的な鍵管理インフラ (KMI) は複雑なシステムであり，単純な暗号には存在しない情報漏洩経路を作り出す．例えば，暗号文に回復機関の ID 等を添付する方式は，回復機関が攻撃目標になり易く，回復機関の秘密鍵等の流出の影響が広範囲に及ぶ危険がある．

(ii) 鍵回復は暗号利用者にとっても鍵の紛失などの不測の事態に備えるために有用であるという政府の主張に対して，政府のアクセスのための鍵回復システムとユーザ自身の利便のための鍵回復システムとでは多くの点で要求条件が異なる．

(iii) コスト負担の問題が未検討である．

2.2 OECD 暗号政策ガイドライン

上記のように米国で暗号政策が大きな問題となった1995年から1996年にかけて OECD は暗号政策ガイドラインの作成を進めてきたが，1997年3月，OECD 理事会はガイドラインを採択した．OECD 暗号政策ガイドラインは，下記の8原則からなる．

(1) 暗号手法に対する信頼
(2) 暗号手法の選択
(3) 市場主導による暗号手法の開発
(4) 暗号手法の諸標準
(5) プライバシィと個人データの保護
(6) 合法的アクセス
(7) 責任
(8) 国際協力

この中で，(5)項では，「通信の秘密および個人のデータの保護を含むプライバシィに関する個人の基本的権利は，各国の暗号政策の策定や暗号手法の開発・利用にあたって尊重されるべきである」としている．

(6)項は，各国の通信傍受に関する法の違いが基で，このガイドラインの作成作業の中で最ももめた点といわれている．結局は，「各国の暗号政策は，暗号化されたデータの平文または暗号鍵への合法的アクセスを許可することができる．これらの政策は，本ガイドラインの他の諸原則を最大限尊重しなければならない」という表現で合意に達した．

2.3 ヨーロッパ諸国および欧州連合の暗号政策

2.3.1 英国の暗号政策

英国における通信傍受の規定としては，「1985年通信傍受法」があった．

英国貿易産業省は，1996年6月および1997年3月に TTP に関する提案文書を発表した．これは，ユーザに TTP の利用を強制するものではないが，公衆に

暗号サービスを提供するTTPは免許制とし，政府機関が令状によってそこに寄託された鍵等にアクセスすることを可能にするものであった．

しかし，保守党から労働党への政権交替の後，1999年3月の貿易産業省の諮問文書では，強い暗号の使用の法執行への影響に懸念を示しながらも，TTPサービスの提供に鍵寄託を強制することは電子商取引の成長を阻害するとして，方針の変更を行った．また，1999年5月の内閣府の報告書も「鍵寄託は国際的に広く採用されて初めて効果があるが，その可能性はなく，強制的鍵寄託の実施は英国が電子取引で世界のリーダになることを阻害する」として，鍵寄託を否定した．

2000年5月に制定された「2000年電子通信法」は，その第14節で鍵寄託を禁止した．また，2000年7月に制定された「2000年捜査権規制法」は，第III部「暗号等によって保護された電子データの捜査」で，鍵の保有者に鍵の開示要求を行うことを認め，保有者がその要求を拒否できないことを規定している．暗号の使用者は，暗号鍵の寄託を義務づけられていない．

2.3.2 フランスの暗号政策

フランスは，暗号の使用に最も厳しい制限を課していた国であった．1996年7月に制定した「1996年電気通信法規制法」の第17条は，暗号の使用，暗号機器の輸出入に関する従来の規定を改訂した．この改定によって，若干の緩和が行われたが，秘匿目的の暗号の使用および輸出入には首相の許可を必要とし，鍵回復をサービスとする機関には政府機関の要求に応じて鍵の提出または復号を行うことを義務づけるなど厳しい規定となっていた．しかし，1999年1月，Jospin首相は，強制的鍵寄託を廃止すると発表した．

2.3.3 ドイツの暗号政策

ドイツは，憲法に相当するドイツ連邦基本法第10条に通信の秘密に関する規定が存在する点が日本と似ているが，NATO加盟の時点で通信の秘密の例外規定を設けた．その規定が通信傍受の根拠となっている．

ドイツ連邦議会は，1996年6月，通信の秘密の憲法上の権利の範囲で，利用者が効果的な暗号手法を自由に選択できるという決議をおこなった．1996年10月に発足した暗号政策の省庁間タスクフォースは，暗号の自由な選択と犯罪者の暗号の悪用の間のトレードオフを求めている．

2.3.4 欧州連合

欧州連合加盟各国の間の暗号政策の相違は，域内の情報の流通を阻害し，欧州における情報社会の発展を遅らせるとの観点から，欧州連合は，域内の暗号政策の調和を図ってきた．欧州委員会文書「電子通信におけるセキュリティと信頼の保証」(COM (97) 503) (1997年10月) は，2.1.5項で述べた暗号学者の論文を参照し，鍵寄託/鍵回復のサービスを提供するTTPが攻撃の目標になる懸念と犯罪者が鍵寄託/鍵回復を容易に回避できることからその効果への懸念を述べている．

2.4 日本の暗号政策

日本は，憲法に通信傍受の規定がある点でドイツに似ている．この憲法21条2項の規定のためか，最近まで通信傍受に関する法律が存在しなかったが，1999年8月通信傍受法が成立した[7]．

鍵寄託，鍵回復に関しては，警察庁の依頼による財団法人社会安全研究財団の情報セキュリティ調査研究委員会の情報セキュリティ調査研究報告書（1996年9月）および情報セキュリティビジョン策定委員会報告書（1998年3月）に検討内容が述べられている．鍵回復機関を仮定した場合に，現行刑事訴訟法では法執行機関が容疑者などの公開鍵暗号の秘密鍵を鍵回復機関から押収することになり，令状等に指定された通信文の範囲に限定することが困難であるので，法執行機関が鍵回復機関にセッション鍵を提出させることを可能にする法律が必要であると論じている．

2.5 暗号政策の流れ

米国では，クリントン政府は鍵寄託の提案を行ったが，結局国内での暗号の使用は制限されていない．暗号製品および技術の輸出規制緩和も行ってきた．各国の暗号政策も，この米国の動向に対応して，同様の自由化の方向を示している．この流れの底には，暗号機器を含む情報システムの輸出，電子商取引を含む情報社会の進展において遅れてはならないという考えがあると見られる．しかし，G8での主要議題の一つは国際犯罪への対処であり，法執行機関は通信傍受がその重要な手段であると主張しているので，今後も両者の間のバランスを巡る政策論争は続くであろう．

3. 電子署名の法制度

電子商取引や電子政府では，文書を書面でなく電子的に扱うが，電子文書（あるいは電子的記録）は，その作成者の成りすまし，記録自体の改竄，記録作成の

[7] ドイツが基本法の改訂を行ったのに対し，日本はいつものように憲法の解釈で対応している．

否認が容易であるという問題点を持っている．これらを解決するための手段が電子署名である．

3.1 電子署名とデジタル署名

電子文書に対して，署名の持つ機能である(1)署名者の特定と(2)署名が添付された文書の内容を署名者が承認したことを示すという機能面だけを扱い，その実現技術に触れないことによって技術中立性を保ち，将来起こり得る技術の進歩にも影響を受けない規定を作りたい場合がある．電子文書に対するこのような署名機能だけを扱う場合，それを電子署名という．

電子署名の実現技術としては，現在，公開鍵暗号方式を使用する方法が主流である．公開鍵暗号方式を使った電子署名は，デジタル署名と呼ばれている．デジタル署名として規定する方が具体的な方法で明確に規定ができる．

3.2 電子署名法の論点

肉筆による署名と異なり，電子署名はあくまでデータであるために，鍵と署名者の間の結びつきを証明する手段が必要となる．この機能が証明業務[8]である．この点では，電子署名は，署名よりも印鑑に似ていて，証明業務を行う証明局は，印鑑登録と同様に本人確認を行なって公開鍵登録を行い，印鑑証明と同様に公開鍵証明を発行する．

したがって，電子署名には(i)署名の保有者，(ii)署名に依存する人（署名の受領者），(iii)証明局という3つの人または組織が関係する．

契約などの成立の要件として，文書が必要か，また署名または押印が必要かということは，国毎に異なる．電子署名法は，その点は扱わず，電子署名が手書きの署名と同じ効力を持つために満たすべき条件を扱う．また，上記の三者の義務，責任を規定する．即ち，電子署名法は，これらの間に紛争が生じた場合に，署名の証拠性の推定を行なう基準や立証責任の帰属を規定していることが多い．

電子署名の基礎は，検証に使用する公開鍵が真に署名者のものかという点とコピーの不在（あるいはコピーが使用されていない保証）にある．

第1の点に関しては，証明局の信頼性の保証は，電子署名法の重要な部分である．認証局を免許制とするか認定制とするか等，各国の電子署名法で異なる．第2の点の責任は署名保有者にあるが，デジタル署名における実際問題として，署名用の秘密鍵の生成をどのように行なうのかも問題であろう．自宅のコンピュータで生成する場合には，鍵生成プログラムの質の保証をどうするかが問題になり，認証局が生成する場合には，認証局からの漏洩[9]がないことの保証が問題になる．欧州連合で検討されているTTPの機能仕様には，鍵の生成・管理が含まれている．証明局やTTPの倒産や廃業の場合の漏洩も考慮する必要があろう．

電子署名が署名または押印と異なる点の一つは，署名者が直接ではなくコンピュータ等のハードウェアおよびソフトウェアを使って署名を行なうことである．このように使われる機器を電子署名エージェントとか署名デバイスと呼んでいる．このハードウェア，ソフトウェアの信頼性はきわめて重要である．このような電子署名エージェントを使って，自動的に電子署名を行なうことも可能である．そのような場合でも署名保有者の管理下にある署名エージェントによる署名の責任は署名保有者に帰属するというのが原則である．

3.3 電子署名法制定の動向

3.3.1 米国

米国では，州内の商取引は州の管轄であり，電子署名法も州法として制定されている．

1995年5月に制定された「ユタ州デジタル署名法[10]」は，最初のデジタル署名法として有名である．この法律は，公開鍵暗号の使用と署名後の文書の変更の検出可能性をデジタル署名の条件としている．証明局に関しては免許制を導入し，法律が署名を要求している場合に，免許を受けた証明局の発行した証明に掲載された公開鍵で検証されたデジタル署名はその要求を満たすと規定している．証明局の免許には限度額を設定し，その証明局の証明による署名は限度額を超える契約には使えないという規定を設けてある．

米国全体を見れば，各州の立法状況は様々で，殆どの州で電子署名またはデジタル署名に関して立法を行っているが，立法を行っていない州もある．

米国統一州法委員会全国会議（NCCUSL）は，各州の電子署名法が最小限満たすべきものとして「統一

[8] 通常は，この業務を認証業務と呼び，それを行なう機関を認証局と呼ぶ．日本の法律でも，認証業務，認証事業者と呼んでいる．これに対する英語は，certificationおよびcertification authorityであり，証明および証明局という訳のほうがふさわしいように思える．

[9] 週刊文春2000年7月13日号は，この懸念を問題にしている．また，類似の問題として，自動車販売店からの鍵情報の漏洩による自動車盗難の例が報告されている．

[10] ユタ州法第46篇「文書の公証と認証およびデジタル署名」第3章「ユタ州デジタル署名法」

電子取引法」をまとめ，現在，各州で州法をこれに整合させる動きがある．これは，電子取引にだけ適用するものであり，遺言関連の署名は範囲外としている．また，電子的な手段で取引することに合意した当事者間にのみ適用するとしている．電子エージェントを使う自動取引についての規定がある点が注目される．

今年6月には「全世界および米国商取引における電子署名法」が連邦法として成立した．この法律は，州際および国際取引における電子署名および電子記録の法的効力を確立するものであるが，一方で，消費者との取引において書面で提供されなければならないことが法律で規定されている場合に，電子記録でその書面に代替するには，消費者の合意が必要という消費者保護の観点からの例外を規定している．更に，この法律は，商務長官に国際的な電子署名の促進の義務を課している．

3.3.2 ヨーロッパ

ヨーロッパでは，1997年3月にイタリアで，法律1997年3月15日第59号第15条2項「電子形態の証書，文書および契約」に関する規制法（通称：イタリアデジタル署名法）が制定された．更に同年11月にはそれを補足する大統領布告513号が出されている．この法律は，公開鍵暗号を使用したデジタル署名を規定している．公開鍵の10年間の保管義務やデジタル署名の使用の結果他人に損害を与えた場合の損害賠償責任などを規定している．このように署名用秘密鍵の保有者の責任を規定しているので，秘密鍵の預託に関しても媒体に入れて封をすることを規定するなど署名の唯一性の確保に慎重である．証明局は秘密鍵を預かることを禁止されている．

7月にはドイツで，「情報通信サービスの一般条件を設定する連邦法—情報通信サービス法　第3条　デジタル署名に関する法律」が制定された．この法律は，主に証明局について規定している．証明局は免許制である．

欧州委員会は，1997年10月，「電子通信におけるセキュリティと信頼の保証　電子通信におけるディジタル署名および暗号化に対するヨーロッパの枠組みに向けて」(COM(97)503) を発表し，イタリアおよびドイツのデジタル署名法の制定の動きを歓迎しながらも，欧州域内市場の観点から，共同体レベルの枠組みが緊急に必要であるとの見解を述べた．1998年5月には「電子署名の共通枠組みに関する欧州委員会の提案」が出され，ヨーロッパ共同体内の整合性を目的として，欧州議会および評議会は1999年12月に「電子署名に対する共同体の枠組みに関する指令」を発布した．この指令では，署名者が電子署名を作るときに使うハードウェアおよびソフトウェアを署名作成デバイスと定義し，抽象的ではあるが，セキュアな署名作成デバイスの条件を定義している．また，署名作成データ（デジタル署名の秘密鍵）の保存およびコピーは電子署名の法的な有効性への脅威であるとして，証明サービス提供者（証明局）が署名作成データを保存またはコピーすることを禁止している．

3.3.3 アジア

アジアでは，1997年にマレーシアがデジタル署名法を制定した．

日本は，本年5月24日に「電子署名及び認証業務に関する法律」が成立し，2001年4月1日から施行されることになった．内容は証明業務に関する規定が主である．

3.3.4 国連

このような背景の中で，国連国際商取引委員会(UNCITRAL) は，1996年，デジタル署名と認証局の問題を検討することを決定し，「電子署名に関する統一規則」を作成中である．現在2000年2月の作業部会案が審議されている．ここでも，欧州連合の署名作成デバイスと類似の署名デバイスについての規定がある点が注目される．

3.4 電子署名の課題

現在20を超える国で，電子署名法またはデジタル署名法が立法化されているが，その内容は様々である．勿論各国のこれまでの制度によって多様化することは当然ではあるが，現状は，むしろ未経験の世界であることに起因する多様化のように見える．米国内での統一電子取引法，欧州議会および評議会指令，国連国際商取引委員会の統一規則案などを基に，ある程度の調和が図られていくであろう．

しかし，電子商取引といっても，予めある期間の取引を前提とした契約を結んだ企業間のB2B取引では，このようなパブリックな電子署名制度は不要という意見もある．電子署名制度が経済発展に実質的にどれだけ寄与するかは未だ分からない．また，電子署名制度自体も変化していくのであろう．