電子署名及び認証業務に関する制度分析
電子インフラストラクチャーにおける市場と政府の役割*

Law and Economics Analysis of Digital Certification Policy:
How Government and Market Act in Support of Digital Infrastructures*

岡田　仁志**

Hitoshi OKADA**

Abstract

The Ministry of Posts and Telecommunications (MPT), the Ministry of International Trade and Industry (MITI), and the Ministry of Justice (MOJ) passed the bill of Digital Authentication and Digital Signature, in order to promote digital authentication business and to make a legal framework for digital signatures in Japan. On the other hand, the MOJ passed the bill of Digital Public Certificates, using the system of Commercial Registration. This paper analyzes these two laws, and discusses how the government should work in support of market mechanisms in order to promote digital infrastructure in cyber space.

キーワード：電子認証、電子署名、電子インフラストラクチャー、市場と政府の役割

keywords：Digital Certification, Digital Signature, Cyber Infrastructures, Government and Market

---

* 本稿は2000年２月に開催された OSIPP 寄附講座研究集会「個人金融サービスに関する政策分析」における報告を、関連２法案の国会通過など爾後の環境変化を受けて新たに加筆・修正したものである。

**大阪大学大学院国際公共政策研究科 個人金融サービス寄附講座 助手

1. 電子商取引を巡る立法の現状

1997年7月にアメリカ合衆国政府が「世界的商取引の枠組み」を発表して以来、アメリカにおけるインターネット利用者の数は急増した。今やアメリカ経済の実質成長に占める情報技術業種の割合は1/3強に相当し、電子商取引は事実上全ての経済セクターでの生産性向上に寄与している[1)]。アメリカ合衆国は、情報革命における先導力を維持し「新経済」の急成長を持続させるために、国際的に合意形成しておくべき論点として9項目の政策課題を指摘し、それぞれアメリカ合衆国政府の立場を明らかにしている（図表1）。本稿では第5の論点である契約条件の国際合意に関する立法の状況を概観し、その政策学的意味を論じることとする。

2. 電子署名及び認証業務に関する法制度

2.1 法制化の必要性

ＥＵ地域や日本でもインターネット利用者数は着実に増加しており、その応用範囲はあらゆる分野にわたっている。インターネットにおける電子商取引においては、クレジットカード番号をＳＥＴ方式やＳＳＬ方式のプロトコルによって安全に送信する手段がとられることが多い。しかし、インターネットは不特定多数人が参加できるオープンなネットワークであるため、専用回線を通じたデータ交換とは異なり、相手方が確実に本人であることを証明する本人性の認証（authentication）と、情報内容が途中で改ざんされていないことを証明する非改ざん性の認証（certification）が必要である。

2.2 法制化の現状

2.2.1 電子署名及び認証業務に関する法律

郵政省、通商産業省、法務省の電子商取引関連3省庁は1999年11月19日に「電子署名・認証に関する法制度の整備について」と題するプレスリリースを共同発表した[2)]。

そこでは「インターネット上の電子商取引をはじめとするネットワークを通じた社会経済活動においても、手書き署名・押印及び印鑑登録証明と同様の機能を果たす、電子署名及び民間認証機関による電子認証が利用されはじめている。しかしながら、我が国では電子署名・認証の法的な取り扱いについては明確なルールが存在しないため、仮に紛争が起きた場合に

1) アメリカ合衆国における電子商取引の動向については電子商取引実証推進協議会国際課［1999］に詳しい。
2) 共同プレスリリース本文は郵政省・通商産業省・法務省［1999］に公表された。

図表１　グローバルＥＣ政策のフレームワーク

	政策課題	各地域の政策現況		
		アメリカ政府	EU 政府	日本政府
Ⅰ	プライバシーの保護	民間主導でプライバシー保護策を実現するが、EU指令の保護要求についてはFTCによる準司法的救済を充実することでクリアした。	1995年のEU指令で加盟国に個人情報保護法の制定を義務付けた。保護レベルの不充分な第三国へのデータ移転を制限。	個人情報保護基本法制の整備に向けて大綱案をまとめ、既に業界向けヒアリング実施やパブリックコメント募集段階にある。
Ⅱ	情報コンテンツ制限	政府による検閲ではなくレイティングやフィルタリングなどで対応するのを原則としていたが、特定の領域には法律を制定している。	ドイツの 1997 年マルチメディア法はコンテンツ制限に関する法律をインターネットに適用する条項を置いている。	特定の領域においてはリアル社会よりも厳格な法律を整備する。通信傍受法の施行により内容審査が合法となる場面もある。
Ⅲ	標準的な技術の選定	政府間合意ではなく、市場原理に基づいて選別する。電子技術の標準化作業を行うことは賢明ではなく、不必要であると主張する。	ITU による政府間調整的な標準化作業のほか、ISO における通信プロトコルや IC カードの標準化作業が重要性を増している。	GBDe などの国際民間コンソーシアムの場で、民間企業が政府に代替して国際標準化に積極的に参加している。
Ⅳ	知的所有権の保護策	インターネットで流通する著作権、商標、特許の保護を重要視する。WIPO 条約を電子商取引に適した形に変更するよう提案していく。	データベースの法的保護に関する欧州議会及び理事会の指令が EU 委員会から 1996 年に発令されている。	著作権法、意匠法、実用新案法をデジタルコンテンツに対応して改正したほか、ビジネスモデル特許に関する運用指針を策定。
Ⅴ	契約条件の国際合意	デジタル署名や認証の有効性に関する合意を形成する。電子署名に手書き署名同様の効力を与える電子署名法が2000年秋に施行される。	認証機関についての任意的認定制度を導入することに決定した。電子署名には手書き署名と同様の法的効力を与える。	電子署名及び認証業務に関する法律が成立し、2000年4月から施行される。認証機関には任意的認定制度を適用する。
Ⅵ	商取引の障壁を撤廃	インターネットはシームレスなグローバルマーケットであるとの立場から、文化的な理由による障壁も撤廃すべきであると主張する。	EU としてのアイデンティティを守るため、自国言語尊重などの文化的な理由による障壁は認めるべきであると主張する。	九州・沖縄サミットや日米交渉の議題となるが、IT 担当省が存在しないため電子商取引全般に対する基本姿勢は明らかではない。
Ⅶ	電子決済の規制政策	市場に登場する電子決済システムを、政府規制ではなく市場原理によって自律的に選別するのが好ましい。消費者保護には別途配慮する。	電子決済手段の発行体を金融機関に限るべきか等の規制課題について、OECD や EU 委員会などが提案を出している。	新たに電子マネー法を制定する動きもあったが中断しており、電子認証法や銀行業務免許等の組み合わせで対処している。
Ⅷ	セキュリティの確保	確実な電送を保証するため、高度な暗号技術を用いて安全にデータを取引できるネットワーク環境を構築する必要性を強調する。	OECD の暗号政策ガイドラインなどが安全なネットワーク実現のための具体的施策を提言している。	不正アクセス防止法の施行により、パスワードの盗用等による不正なサーバ侵入などを処罰できるようになった。
Ⅸ	インターネット課税	インターネットを介して取引されるサービスやインターネットを構築していくための製品は無関税とする。ネット新税の創設にも反対する。	越境インターネット取引への課税ルールを取りまとめ、具体的な納税方式についても提案していく態度を表明している。	EU と同様の徴税ルールを採用する見こみ。ネット徴税機会の逸失を防ぐ目的においてEU と政策方針が一致している。

参考資料：岡村法律事務所ホームページ　(http://www.law.co.jp/cyberlaw1.asp)
夏井高人研究室ホームページ (http://www.isc.meiji.ac.jp/~sumwel_h/)

どれだけ証拠として評価を受けるのかが必ずしもはっきりとしていない」との現状認識が示されている。

そこで、法律を制定することによって電子署名に民事訴訟法上の証拠力を付与し、認証機関には任意的な認定制度を導入しようというのが立法の趣旨である。電子署名及び認証業務に関する法律が存在しない状況では、既存の印鑑の押印による印影と電子認証局の発行した認証を基礎とする電子署名とを同視してよいかなど多数の論点に関して、具体的な紛争が提起されてから裁判所において解釈を確定していかなければならない。このことが企業による電子商取引分野への本格的参入を慎重にさせ、ともすればユーザの利便性よりも紛争発生時の免責を企図した使い勝手の良くない電子商取引システムを構築させる遠因となっていた。多くの電子モールでは、消費者側に過分な責任を負担させる旨の約款を提示しており、いわゆるシュリンクラップ条項と同様に、「同意する」ボタンをクリックしたことをもって、約款の内容を十分に理解して契約関係を締結したと擬制していた。しかし、このような一方的約款は、その効力が裁判において否定される可能性もあるため、電子モール運営事業者としては、法的に不安定な立場に立たされていた。

このように、消費者・電子モール運営者ともに法的な予測可能性の不十分な状態で契約関係に入っている現状を改善する意味で、電子署名及び認証業務に関する法律を制定することは、電子商取引を普及させるための前提条件の整備を意味する。同法は第147回通常国会で可決成立し、2001年4月から施行される。

電子署名及び認証業務に関する法律では、「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が行われているときは、真正に成立したものと推定する」旨の規定が置かれている（同法第3条）。この条項により、紛争発生時に要する労力を大幅に節約できると同時に、契約に参加する段階で紛争発生時の司法判断を高度に予測することが可能となる。

2.2.2 商業登記法等の一部を改正する法律

電子署名及び認証業務に関する法律と並行して法整備が進められたのが、商業登記制度を基盤とした認証業務等を導入する「商業登記法等の一部を改正する法律」である[3)]。同法は、(1)登記情報に基づく電子認証制度として、法務大臣の指定する登記所に印鑑を提出した者が登記官に対し、(a)その者が用いる電子署名の公開鍵、(b)法人の商号、代表者の氏名・資格等の登記事項、(c)証明の有効期間の3項目に関して電子証明書の発行を求めることができると規定する（同法第1条によって加条される商業登記法第12条の2）。暗号処理には256桁の公開鍵方式を採用し、電子取引において会社の実在性を公的に証明する。同法はまた公証人法

3) 法務省［2000］参照。

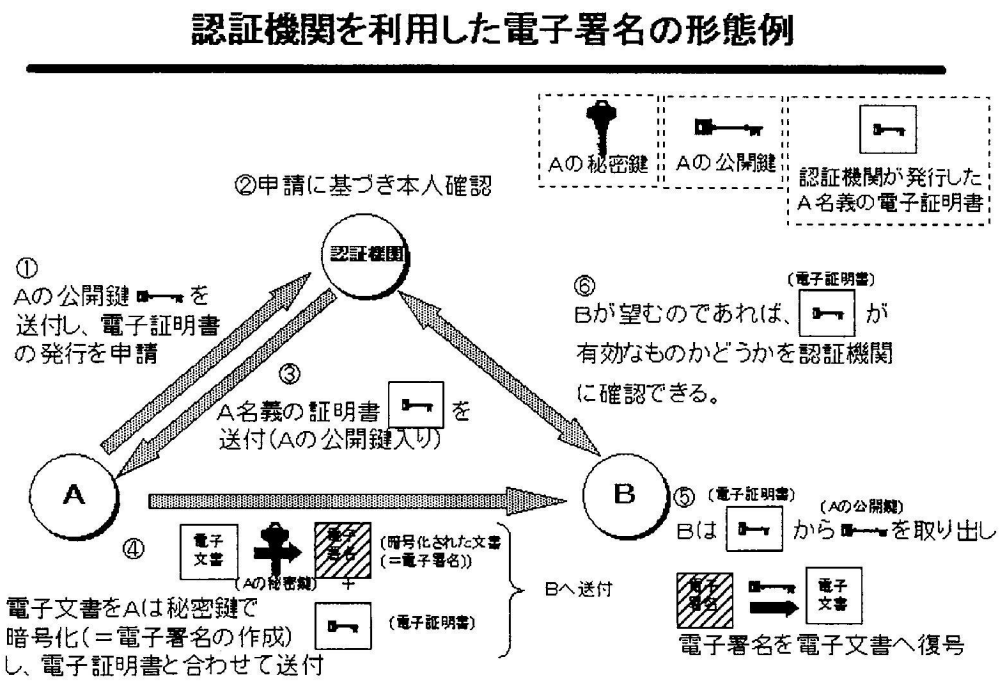
の一部を改正し、公証人がコンピュータを用いて電子的な方法により確定日付の付与等の事務を行う電子公証制度を創設した（同法第２条によって改正される公証人法第２条）。同法は第147回通常国会で可決成立し、2001年４月より施行される。

3.　電子署名及び認証業務の仕組み

3.1　認証機関を利用した電子署名の形態例

実際のインターネット上における電子商取引において、認証機関を利用した電子署名及び認証に関する業務は、典型的には図表２に説明されるような形態で行われる[4]。

図表２　法律が想定する取引形態



3.2　法律が予定する技術形態

電子署名及び認証業務に関する法律が想定する技術形態は、図表２に見られるように、一対の公開鍵と秘密鍵を利用して、本人の同一性の認証と、文書の真正性の認証を実現する方式である。この仕組みにおいて、認証機関は鍵の管理と電子証明書の発行を担当する。ここ

4）郵政省・通商産業省・法務省［1999］付属資料「認証機関を利用した電子署名の形態例（図）」を抜粋。

では、共通の鍵を当事者双方が保管する共通鍵方式の利用は念頭に置かれていない。同法は例示するプロトコル以外の技術方式を排除するものではないが、公開鍵暗号方式を強く意識する内容となっている。

3.2.1 ＳＳＬ方式プロトコル

公開鍵方式の暗号送信プロトコルとしては、ＳＳＬ方式とＳＥＴ方式の２つが競争している。ＳＳＬ方式はネットスケープやインターネットエクスプローラーなどのブラウザにプレインストールされており、消費者側では特に手続きをする必要もなく簡単に利用できる。ブラウザのヘルプ項目やバージョン情報を見ると、例えばインターネットエクスプローラーなら暗号強度 40bit と、ＳＳＬ送信プロトコルで利用できる暗号のレベルが書かれている。ＳＳＬプロトコルの仕組みは比較的簡単で、ネット上で購入したい商品を見つけた消費者Ａが、クレジットカードの番号をそのまま送信する代わりに、商店Ｂがネット上に公開しているＳＳＬ公開鍵で顧客のクレジットカード番号情報に鍵をかけて、暗号化してから送信する。この鍵を開けて元の文章に戻すためには公開鍵とペアになった秘密鍵が必要なのだが、これは商店Ｂのサーバの中に厳重に格納してあるので、ネット上を流れる情報を誰かが拾得しても、暗号を解読することに成功しない限りは、内容を了知することはできない。ＳＳＬ方式を利用するためには、商店Ｂが認証機関に公開鍵を登録しておく必要があるが、顧客Ａは事前に公開鍵の登録などの手続きを経ていなくても利用できる。この場合、商店Ｂの同一性は認証されるが、顧客Ａの同一性は認証されないため、この部分は商店Ｂがリスクを負うことになる。

ＳＳＬプロトコルをより安全に利用するためには、商店Ｂが予め認証機関から顧客人数分の認証書発行権を購入し、顧客Ａ等に登録用ソフトを配布する。顧客Ａはこれを実行して認証機関にアクセスし、一対の公開鍵と秘密鍵の発行を受ける。これによって、以降はログイン時に本人認証が行われるため、他人によるなりすましによって自己の財産が侵害される危険性が低くなる。現在、顧客にＳＳＬ認証書を発行するのは、多額の資産を管理するオンライン・トレーディングなどによく見られる。

3.2.2 ＳＥＴ方式プロトコル

ＳＳＬ方式に比較して、ＳＥＴ方式は手続きが複雑である。ＳＥＴ方式では、顧客Ａのクレジットカード番号に暗号をかけて商店Ｂに送信するのではなく、予め認証機関にクレジットカード番号を登録して、クレジットカード番号に代わるＳＥＴ取引用の会員番号の発行を受ける。これを暗号化して商店Ｂに送信するのだが、商店ＢはＳＥＴ取引用の会員番号を復号しても顧客Ａを認識できないので、さらに認証機関に転送する。認証機関はこれを復号し

てＳＥＴ取引用の会員番号を読み取り、予め登録されたクレジットカードと照合して認証が完了する。最初に顧客Ａが認証書を取得することが不可欠であるため、顧客と加盟店の双方が認証機関と契約しなければ成立し得ないのがＳＥＴ方式の特徴である。

ＳＥＴ方式は顧客Ａに必ず事前登録を要求する点で取引の準備コストが高い。それに加えて、消費者Ａのパソコンにセット用のウォレットソフトをインストールするのが大変な作業であるため、これがＳＥＴ普及の妨げになると指摘されている。また、商店側のサーバにも受け側のソフトをインストールしなければならず、これは中小の事業者にとっては電子商取引への参入を断念するほどの金銭的かつ手続的負担となりうる[5]。

3.3 法律の技術中立性

3.3.1 電子署名及び認証業務に関する法律の技術中立性

電子署名及び認証業務に関する法律が標準として想定する認証プロトコルは、一対の公開鍵と秘密鍵を利用して、本人の同一性の認証と、文書の真正性の認証を実現する方式である。この仕組みにおいて、認証機関は鍵の管理と電子証明書の発行を担当する。ここでは、共通の鍵を当事者双方が保管する共通鍵方式の利用は、少なくとも明示的には念頭に置かれていない[6]。

認証機関と不可分一体で運営されるＳＥＴ方式は、電子署名及び認証業務に関する法律の成立を契機として普及する前提条件が整う。しかし、第一にＳＥＴ方式はパソコンのシステムリソースへの負担が重いなど、家庭用のパソコンにインストールして広く利用されるまでには解決すべき課題が多い。第二に、認証機関の発行する電子証明書の証拠力が高まるのであれば、ＳＳＬ方式で顧客Ａが認証機関に事前登録する形でも十分な法的安定性が実現できる。このように考えると、同法の成立によってＳＳＬ方式よりもＳＥＴ方式が有利になるとは限らず、寧ろＳＳＬ方式に有利に働く事態も考えられる。

ＳＳＬ方式を使ったオンライン・トレーディングなどは広く利用されている。解読が困難とされる鍵長の大きい公開鍵暗号は、軍事技術としてアメリカ合衆国から他国への輸出が規制されていた。しかし、アメリカ合衆国内の民間セクターからの強い要望を受けてアメリカ政府も態度を軟化し、企業毎にアメリカ商務省の許可を得ることを条件に 128bit のＳＳＬ暗号が輸出解禁された。これを受けて、日本のトップクラスのオンライン・トレーディングなどでは、128bit のＳＳＬ暗号を利用している。ここでは、顧客側でも認証機関に登録して鍵の発行や電子証明書発行のサービスを受ける安全な仕組みがとられる。128bit のＳＳＬ方式

5) ＳＥＴ認証技術とＳＳＬ認証技術に関する詳細な技術解説として、電子商取引実証推進協議会認証局検討WG８・相互接続検討ＳＷＧ［1997］などがある。
6) 共通鍵方式と公開鍵方式の相違など暗号技術全般に関しては、辻井［1998］に詳しい。

は現段階でも強度が高く、制度インフラとしての法律が成立することにより、ＳＳＬ方式による電子商取引はさらに普及のための条件が揃うことになる。

3.3.2 商業登記法等改正の技術中立性

これに対して、商業登記制度を基盤とした電子認証業務においては、法務省の指定する方式が唯一の方式となる意味において技術中立的ではなく、制度導入時において信頼性が高いと判断された方式が採用されることになる。また、公的な主体による認証業務の提供という性格から、異なるプロトコルへの移行において柔軟性を欠くことが予測される。しかし、公的機関の選択した認証プロトコルであることから利用者側の信頼が得やすく、また商業登記というリアルの世界において浸透した制度と一体で運用されるプロトコルであること、さらに利用者が個人よりも判断力の高いと思われる企業であることなどから、安全な電子商取引を推進する法的インフラとして早くから評価を得やすい立場にある[7]。

4. 規制手法の比較分析

4.1 規制方式と干渉の度合い

一般に、技術革新ペースの速い電子商取引の分野においては、事前に明確な認可基準を開示することは困難である。このため、代替的な手段として、より緩やかな基準を設定して、これを満たすことを要求するなど、規制手法を工夫する必要がある[8]。

このような分野における規制手法として、Ogus [1994] は事前承認、各種基準による認可、情報措置を挙げる。Ogus [1994] によると、基準の性質と干渉の度合いは図表3のような関係にあり[9]、この中では事前承認が最も干渉の度合いが高く、これより緩やかな基準として指定基準、行動基準、目標基準の3つがあり、最も干渉度の低い手法として情報措置がある。Ogus [1994] の原表にはないが、事前承認よりもさらに介入の度合いが高い手法として事後解釈を図表の右側に加える。これは、介入の態様が事前に予測できない裁量型の行政手法や、立法段階や行政指導によって明らかとなっていない規制ルールが事後的に裁判の場で始めて明らかとなる場合が最も私的自治への介入度合いが高いとの判断に基づく分類である。以下、それぞれの手法について詳細に検討を加える。

---

7) 原田・早貸 [1998] は、商業登記制度を基盤とした制度の利点として、登記官が誤った職務執行を行ったときには国家賠償法の適用があることなどをあげる。
8) 電子商取引に関する規制手法全般については、岡田 [1998a]、岡田 [1998b] で論じた。
9) 以下の分析は Ogus [1994], pp. 150-179 の提案する規制の枠組みを電子認証機関の規制政策手法の分野にあてはめて論じたものである。

図表３　規制方式と干渉の度合い

政府干渉度					
← 低い					高い →
情報措置	任意認定制度			義務認定制度 事前承認	事後解釈 行政指導
	目標基準	行動基準	指定基準		
			EU 電子署名法	ドイツ 電子署名法	
			マレーシア、シンガポール、韓国 電子署名法		
			日本 電子署名及び認証業務に関する法律		自由心証主義 暗号技術審査
NPO レイティング	アメリカ 電子署名法				

パブリック・コメント結果		
	①典型的な規制要件を設定すべき	任意制に反対
	②明確にして恣意的運用を避けるべき	
	③規制要件は必要最小限にすべき	

図注：任意認定制度枠内における各国政策の位置づけは、目標基準、行動基準、指定基準の３分類と厳密に対応するものではない。

4.1.1 事前承認

事前承認を適用すると、認証機関を営業しようとする者は事前に監督官庁の認可を受けなければならない。この手法は認可主体の裁量が広くなりやすい点で干渉の度合いが高い[10]。事前承認を必要とすると、技術改革の頻繁な電子商取引分野では、優れた新しい技術が開発されても監督官庁の許可が滞ることによって実用化が遅れるなどの事態につながりやすいという欠点が生じる。電子署名及び認証業務に関する法律の制定過程では、パブリック・コメントなどで義務的免許制を求める意見も少数ながら存在したが、最終的には事前承認制度は採用されなかった。認証業務に関する法制度の方針を近時まで明らかにしていなかったＥＵ政府は、義務的免許制を導入しないことを消極的に明確化し、最終的には任意認定制度を導入することを積極的に明らかにした。ところが、ＥＵ加盟国であるドイツの電子署名法は、Artikel 4 (1) において「認証機関の業務をするためには、所管官庁の認可を要する。これは、申請によってなされる」と規定しており、これにより認証業務に関して義務的免許制が採用されているため、今後ＥＵ指令を受けて規制緩和に向けた調整が必要となるか注目されるところである。

4.1.2 任意認定制度

4.1.2.1 指定基準

事前承認の次に干渉の度合いが強い指定基準には、積極的基準と消極的基準の二種類がある。積極的基準を適用すると、一定の技術を使用する義務が設定される。例えばＳＳＬ暗号は 128bit 以上の長さを利用しなければならないなどの基準がこれにあたる。消極的基準を適用すると、一定の技術を利用することが禁止される。例えば、解読歴のある暗号方式を提供してはならないなどの基準がこれにあたる。しかし、現在の電子商取引で通常利用されている暗号方式は、鍵長によって解読の容易さは異なるものの、解読歴のない暗号方式を想定することは現実的ではない。むしろ、取引の金額規模などに応じて利用する暗号方式をコスト・ベネフィットの観点から選択し、解読リスクは解読容易性からリスク額を算出して、損害保険などの制度によって担保することの方が現実的である。

電子署名及び認証業務に関する法律では、認証業務を行おうとする事業者がいかなる認証技術を利用すべきかについて、具体的には何ら規定していない。従って、指定調査機関あるいは承認調査機関による調査の過程を通じて、適正な方式を協調的規制方式によって指導することになる。このように見ると、電子署名及び認証業務に関する法律が想定する規制方式

10) 西垣［1996］は、暗号や認証のシステムは一種の「両刃の剣」的な性格を持っていると指摘する。もし、暗号や認証の悪用による不正送金などの犯罪行為を防止するために、公共の第三者に暗号キーを寄託するキーエスクローなどの対策を徹底するならば、認証機関は少なくとも事前承認を受けることになろう。

は、協調的手法による指定基準を前提とする任意的認定制度であると評することもできそうである。しかし、具体的な基準を消極的にも積極的にも明確には規定せず、認証機関として必要と思われる安全レベルを達するよう指導するという面からは、むしろ次の行動基準に該当すると判断するのが妥当であろう。

4.1.2.2 行動基準

行動基準を適用する場合には、一定の条件をみたすように義務づけるのみで、達成するための方法は問わない。例えば、年間に発生する誤認証事故の件数あるいは被害金額に上限を設定し、これを達成するために利用する技術は問わないという基準がこれに該当する。電子署名及び認証業務に関する法律では、特に明確な基準を設定するわけではないので、直ちに行動基準を採用したとは認められないが、指定調査機関または承認調査機関による調査の手法によっては、結果的に行動基準を採用した場合と同様の効果が得られよう。こうしたことから、日本の法律は運用において行動基準を導入する可能性が高いと思われる。こうした形態での行動基準は、紛争発生時における裁判所での判断において、自由心証主義の司法制度と親和性が高いという利点がある。

4.1.2.3 目標基準

目標基準を適用する場合には、特定の基準は設定しない。ただし、発生した被害については刑事または民事上の責任を課すなど、故意・過失を要件としない結果責任を問う。これは、命令的規制を前提としながら事業者の裁量範囲を広く認める方式としては優れているが、協調的規制を前提とする場合においては、事故発生の蓋然性が高い方式を採用している業者には予め改善を申し入れるのが通常である。従って、指定調査機関または承認調査機関による協調的な規制を導入する電子署名及び認証業務に関する法律の運用においては、目標基準の設定による規制手法は採られないものと考えられる。

4.1.3 情報措置

より制限的でない政策手法として、事業者が認証機関をどの程度の安全性で運営しているか、公的な機関などが情報を提供する方法がある。この方法は、一定の基準を満たさない認証機関を排除するわけではないため、事業者は公的機関から高いレイティングを取得できるよう、情報措置を積極的に活用する戦略をとるか、または高いレイティングの取得を目指すことなく独自の方式で運営する戦略を取るか、自主的に選択することができる。

他方、消費者の側では、認証機関がどのレイティングに属するか情報を得ることができ、どのレベルの認証機関を利用するか、安全性と費用などを勘案しながら判断することができ

る。このため、セキュリティレベルの高低に関わらず、最適なタイプの認証機関が市場原理によって選択されることになる。

情報措置の消極的な要素として、企業と消費者の間の非対称性があげられる[11]。例えば、電子商取引が高度に発展して消費者が不可避的に利用している場合であって、しかもある種のサービスにネットワーク外部性が働いて、サービスを提供する業者がごく少数に限られているような場合にあっては、消費者は主体的な選択をする立場にあるとはいえない。このように市場原理が機能していないような場面においては、情報施策が実効性を確保することは困難となる。

アメリカの電子署名法は認証機関の資格要件などに関する規定を置いていないため、義務的にも任意的にも政府の承認を経ることなく認証業務を営業することができる[12]。このため、補完的な消費者保護手法として情報措置を導入することが検討されるところであるが、今のところ政府として情報措置を実施するとの発表はない。しかし、アメリカではプライバシー保護の分野においてＢＢＢオンラインなどのＮＰＯ組織が実施するレイティングが国民の信頼を得ており、これらの組織が認証機関のレイティングに関しても積極的に発言することが考えられる[13]。さらに、政府系の消費者保護推進機関としてＦＴＣが存在しており、ＥＵ政府からもその活動が信頼されていることから、何らかの面で不適切な認証機関が存在すると認められる場合には、ＦＴＣが準司法的機関として勧告を発するなどの行動を取ることが期待される。このように、アメリカでは電子署名法に認証機関の地位に関する規定が置かれていなくても、少なくともＮＰＯなどによる情報措置が提供され、ＦＴＣによる勧告などの措置が取られる可能性もあるものと考えられる。

4.1.4 事後解釈

4.1.4.1 行政による要件明確化

上記の各規制手法とやや異質なのが事後解釈の手法である。これには、行政が事後的に具体的解釈をフォローする手法と、司法府が具体的争訟の解決を通じて解釈を明らかにする方法とがある。もとより、立法の段階で要件を可及的に明確化し、恣意的な解釈の余地をなるべく狭くすることが予見可能性を高める理想的な規制手法である。しかし、電子商取引の分野における技術革新の速さに鑑みると、ある特定の技術を前提として詳細な要件を規定しておくことは、必ずしも現実的な手法であるとはいえない。また、技術標準の中立性という観

11) Cooter and Ulen [1997], pp. 226-229 は、完全契約のモデルにおける契約費用に関する4仮定の1つとして、完全情報保有の仮定を挙げる。
12) アメリカにおける電子署名法の立法過程については Smedinghoff and Bro [2000] に詳しい。アメリカ大統領の電子署名によってスピード成立した最終案には内容が事業者寄りとの批判もある。
13) プライバシー政策をめぐるＥＵ政府とアメリカ政府間の調整については岡田 [1999] で論じた。

点からも好ましくない。そこで、法律の要件がある程度は抽象的になることはやむを得ない側面もある。

認証業務に関しては、任意的認定を受けようとする認証機関が利用すべき暗号通信プロトコルの具体的種類などに関しては特に規定が置かれていない。そこで、法律施行後の任意認定機関への検査実施などにあたって、どのような暗号通信プロトコルを利用していれば安全基準を充たしたと評することができるか、任意認定を付与する行政機関が基準を作成する必要がある。ところが、暗号通信プロトコルは極めて専門性の高い技術分野に属するため、当該領域の専門機関ではない所轄官庁において適切な評価基準を作成しうべき能力に欠ける。そこで、暗号通信プロトコルの強度評価を実施する研究プロジェクトを行政主導で組織し、この組織において専門性の高い暗号通信プロトコルの強度評価を実施することとなった。このような手法は、従来型の裁量幅に制約のない窓口指導に比べて、公表された技術評価のあてはめによる一義的な行政指導であるため、事後の要件明確化であるが比較的行政の介入度合いは低いものと評することができる。

4.1.4.2 司法による規範明確化

行政による対応と比較して、予測可能性を欠くのが司法による事後的解釈に依存する手法である。司法による救済システムは具体的争訟の発生を受けてから発動されるため、裁判開始前には判断を予測することが難しい。具体的事件の解決を通じて明らかとなった裁判規範が内容的に妥当であったとしても、事前に予測可能性が全くない点と、司法による立法作業の度合いが高いという点において、国民の権利は法律によってのみ制限され得るという憲法の理念に合致しているとは言い難い。

これを解決する方法としては、行政が事前に詳細なコンメンタールを公表して司法判断の材料を提供する手法が考えられるが、裁判所側としても積極的に判断指針の作成に参画して、例えば最高裁判所調査官から構成される研究会が関連省庁と共同で司法判断の指針を作成するという案も考えられよう。こうした司法による積極的関与は、司法判断の対象が行政にも及ぶとしている三権分立の趣旨に反する面もあろうが、全くの事前予告なしに裁判所が司法判断を下す現状よりは予測可能性を高める効果があると思われる[14]。

4.2 政策形成過程

これらの規制方式の中からいずれの手法を選択するかの判断にあたって、認証機関の自由な参入による電子商取引ビジネスの発展という効率性の観点を重視するならば、費用効果分析によって最適な手法を決することになる。これに対して、効率性の観点をある程度制限し

14) 電子署名に関する裁判上の論点を法律家の視点から指摘した論文として夏井［2000］がある。

ても情報弱者に被害が発生することを防ぐという公正の観点を重視すると、費用効果分析から導き出される解とは別の規制方式が選ばれるかもしれない。効率性と公正のバランスに関する判断を最終的に下すのは主権者である国民であり、行政としては政策立案過程において国民に判断材料を提供するよう説明する義務がある。従来は困難であった政策形成過程における民意の反映を容易にしたのがインターネットである。

電子署名・認証に関する法制度の整備にあたっては、郵政省・通商産業省・法務省の3省庁がパブリック・コメントを募集し、その結果を公表している[15]。それによると、総論として電子署名・認証に関する早期の法制度整備に賛成するのが32件であったのに対し、反対は3件であった。また、法制度整備にあたっては、過度な規制を避け認証業務の自由な提供を確保することが重要であると指摘する意見が18件であった。

各論においては、国による任意的認定制度の導入に賛成する意見が25件であったのに対し、反対が3件であった。そして、最も意見の分かれた認証機関の認定要件に関しては、「必要最小限にすべき」との意見が8件、「明確にして恣意的運用を避けるべき」との意見が5件、「セキュリティ技術の保有、運営の適格性、財産基盤の安定性、人的信頼性、本人確認方法等を要件とすべき」との意見が6件、「本人確認の具体的方法等は認証機関に任せ、一律に法定すべきではない」との意見が8件であった。

4.3 パブリック・コメントの結果

パブリック・コメントに現れた意見は、国による任意的認定制度を導入することには圧倒的に賛成であった。任意的認定制度は、免許制や、厳格な意味での認可制などとは異なり、国による認定を受けるか否かは事業者の任意判断に委ねられる。認定を受けた事業者は国民に対して、認定事業者としての信用を得ることができるが、国民の側で認定を受けていない事業者を選択する自由も残される。このような意味で、任意的認定制度は、Ogus [1994] の分類でいうところの情報措置に該当する。

情報措置の一形態と解される任意的認定制度の採用を前提として、その認定要件を論じるものとして各意見を見ると、「セキュリティ技術の保有、運営の適格性、財産基盤の安定性、人的信頼性、本人確認方法等を要件とすべき」という規制法規において典型的な要件を設定する意見は6件と少ない。これに対して、「必要最小限にすべき」との意見と「明確にして恣意的運用を避けるべき」との意見が合計で13件ある。ここでは、任意的認定制度の導入に賛成しつつも、認定する業者は極めて安全性の高い業者に絞って消費者が被害を受けないようにするという公正の観点よりも、参入障壁を低くして中小事業者でも認証業務に参入しやすい環境を作るという効率性の観点にウェイトを置いた判断傾向が現れている。

15) パブリック・コメントの結果全文は、郵政省・通商産業省・法務省 [2000a] に公開されている。

今回のパブリック・コメントは回答数が少ないうえ、インターネットで自己の側から情報を発信する能力を有する情報強者に属する人の意見であるから、ここから国民の意見構成を推定することはできない。しかし、少なくとも意見情報を発信した国民の大勢としては、やや効率性に重きを置いた、自由競争指向の意見が強かったと評することができよう。

5. 法制度相互の補完的関係

5.1 電子署名及び認証業務に関する法律の位置付け

電子署名及び認証業務に関する法律は、国による任意的認定制度を導入することになった。この方式は、多種多様な事業者による認証ビジネスへの参入を促し、電子商取引の基盤整備を活性化する効果をもたらす。その反面で、国による任意的認定を受けない認証業者を情報弱者が不用意に利用するようなことがあれば、リアルの社会における被害とは質的に異なるサイバー社会特有の現象として、ごく軽微な不注意から大規模な損害が生じるといった事態を招くおそれがある。従って、任意的規制手法を適用する際には、消費者に対する不断の啓発活動などを併せて実施することが不可欠である[16)]。

例えば、本格的にインターネット上で電子商取引を行う前に、安全に疑似体験できる場を整備して、少なくとも被害を避けようと努力する消費者に対しては訓練の機会を提供することなどが考えられる。または、全ての国民に対して情報リテラシーを高めるための根本的な対策として、初等教育段階においてマネーや商取引に親しむ授業を実施し、中等教育段階においてはインターネットを通じた取引のルールを学ぶ機会を設けるなどのカリキュラムが有益かもしれない。こうした商取引感覚を身につけるためのリテラシー教育に関しては、日本でも具体的な組織化の動きがあると伝えられる。

こうしたリテラシー教育を十分に実施することによって、認証ビジネスへの自由な参入という効率性を重視する観点と、情報弱者が被害を受けることを防ぐという公正さの観点とをバランスよく両立させる施策を実現することが可能となる。

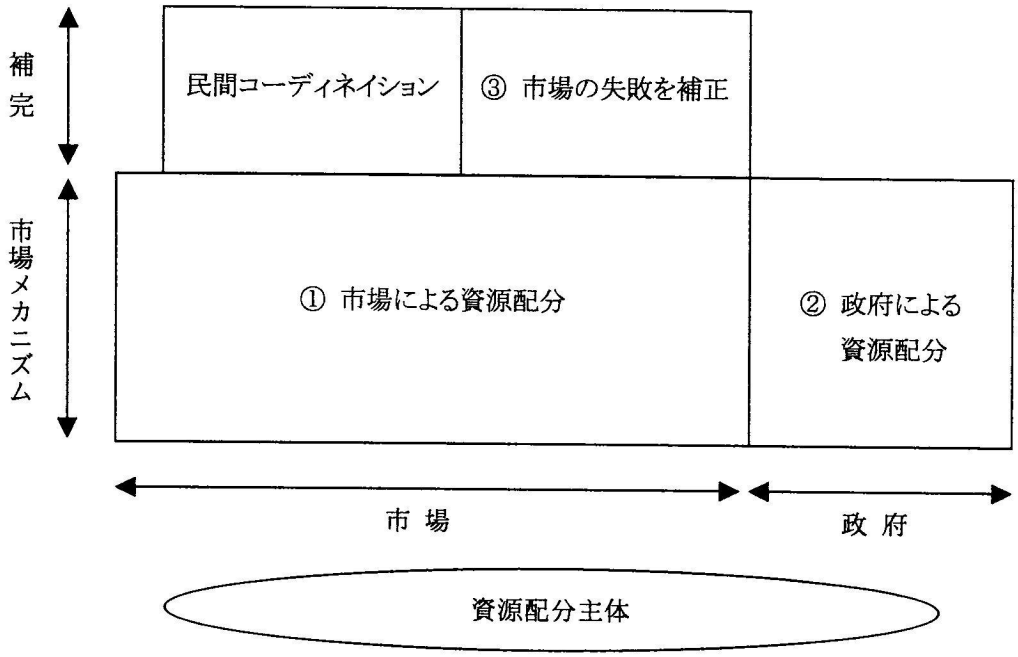
5.2 商業登記法等改正法の位置付け

これに対して、商業登記法等の改正によって導入される、登記情報に基づく電子認証制度にあっては、電子証明書の発行主体が登記官であることから、利用者保護の観点において主体の適格性に問題が生じることはない。

16) 田中 [1997]、pp. 58-65 は規制遵守コストや機会損失の発生しない費用効果の観点から優れた手法として、消費者への啓発活動が有効であると指摘する。

図表4 市場・民間コーディネイションと政府の役割

(一柳・細谷 [1999]、p. 110 による)



しかしながら、商業登記であるため個人として登録することができないこと、民間事業者のように絶え間なく技術革新を継続するインセンティブが存在しないこと、市場メカニズムに基づかないため適正なコストに見合った価格設定が難しいこと、などの問題点がある。現に、商業登記制度を応用した認証サービスは予定される価格設定が民間相場と比べてかなり割高であることを指摘する意見が散見される。確かに、政府が主体となって提供する場合であるから、原価に基づく価格設定という観点によらないことは当然であるともいえる。では、そもそも政府が認証サービスを提供することは、市場との役割分担の観点からみてどのように評価すべきであろうか。この点をさらに詳論する。

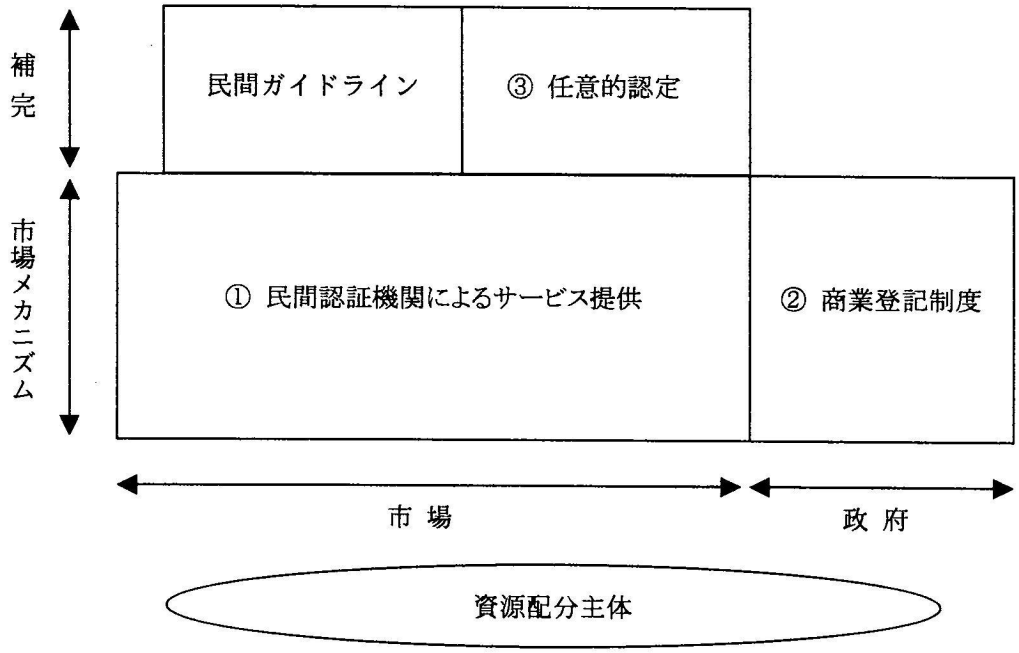
5.3 市場と政府の補完関係

電子署名及び認証業務に関する法律と、商業登記法等の一部を改正する法律は、企業に対する電子証明書の発行という業務において競合する。電子認証に関しては、民間主導によるルール作りを提言する日米財界人会議の声明にみられるように、政府による規制を牽制する意見が多数存在する。他方、消費者保護などの公共政策的側面から、何らかの規制があった方がよいとする意見もある[17]。一般に市場の役割と国家の役割を対立や代替だけでとらえる

17) 例えば、大谷 [1999] は「公的機関でなければならない積極的理由に乏しい」と指摘する。

図表5　電子認証における市場と政府の役割

（一柳・細谷［1999］、p. 110 を参考に作図）



ことは適切ではなく、歴史的経路依存性を背景として存在する経済社会システムのもとで、選択肢の中から限定的ではあるが合理的な選択をすることになる[18]。

市場と政府が相互に関係しあいながら経済活動が行われる混合経済のもとでは、資源の配分は市場と政府の役割分担によって実現される。その態様は、①市場による資源配分、②政府による代替的な資源配分（公共財の提供）、③政府が市場の失敗を補完する部分、の3方式に分類される[19]。ここで、②「政府による資源配分」は価格メカニズムの機能する部分であり、③「政府による補完」は価格メカニズムの機能不全を補完する部分である。

電子署名及び認証業務における政府と市場の役割分担のあり方を考えると、電子認証インフラストラクチャーの構築は、インターネットを通じた安全な商取引を可能にする。これは、『安全な取引環境の提供』という公共財の提供としての側面を有する。なぜなら、電子認証インフラストラクチャーが構築されると、具体的に認証書を取得して電子商取引に参加していない消費者であっても、潜在的には何時でもインターネットを通じた安全な商取引に参加することが可能となるからである。

そこで、市場と政府の役割分担に関する分析枠組みを電子署名及び認証業務にあてはめる

18）以下の分析は一柳・細谷［1999］、pp. 105-145 で論じられるフレームワークに依拠している。
19）一柳・細谷［1999］、p. 110、図4－1『市場・民間コーディネーションと政府の役割』による。

ならば、①民間の事業者が電子証明書を発行し且つこれを認証する業務を提供するのは、市場による『電子認証インフラストラクチャー』という資源の配分であり、②商業登記制度に基づいて登記官が電子証明書を発行し且つこれを認証するのは、政府による『法的信頼性の高い電子認証インフラストラクチャー』という資源の代替的な提供であり、③政府が（①の）民間事業者を任意認定することは、政府が市場の失敗を補完する行為であると位置付けることができよう。

電子署名及び認証業務に関しては、義務的免許制を主張する意見から、任意的認定制度が適切であるとする意見、さらには何らかの情報措置で足りるとする意見までが存在した。これらはいずれも民間によるサービス提供を念頭に置いているが、認証インフラストラクチャーの構築が公共財としての性格を強く有するのであれば、もはや民間によるサービスとしては事業の成立が難しい。これに対し、民間による提供の潜在的可能性が存しながら、民間事業者の独力では認証インフラストラクチャーの構築に至るほどの参加者を集めることが難しいなどの市場の失敗が起こるのであれば、これを補完すべく政府が義務的認定制度ないし任意認定制度を導入することによって、市場の失敗の程度に応じた補完をすることができる。

果たして電子署名及び認証業務は、政府による代替的な公共財の供給が必要な場面であるのか、または、政府が市場の失敗を補完することが適当な場面であるのか。もし市場の失敗を補完する必要があるとすれば、どの程度の介入が最適であるのか。任意的認定事業者と政府による公共財の提供が並存する形となった日本の法制度の下では、安全性レベルと価格レベルとを比較考量した利用者による選択を通じて、任意認定事業者と政府のいずれによるサービスが優れているかが、いわば市場メカニズムに基づいて選択される。また、任意認定事業者と認定を受けない事業者のいずれが適当であるかに関しても、安全性レベルと価格レベルを勘案した利用者が、取引の規模や態様ごとに判断を下すことになる。

サイバースペースにおいては、市場と政府の最適な役割分担の関係が市場メカニズムによって選択形成されていく。制度デザインにあたっては市場による政策選択の可能性を残しておくことが大切であり、電子署名及び認証業務における法律が任意認定制度を採用したことは、市場メカニズムによる緩やかな選択の幅を可能にしている面で優れている。将来的には国内のみならず国外の政策をも任意的に選択することを認め、制度間における国際自由競争の状態を現出することによって、サイバースペースにおける市場と政府の関係は最適な状態に到達する。

グローバルＥＣ政策のフレームワークは、国際的に整合的であることよりも、競争選択的であることが好ましい。市民にとって政策手法が選択可能な状態にあることが、変化の激しいＥＣ政策のフレームワークを緩やかに淘汰し、サイバースペースに持続的な進化をもたらすといえよう。

参考文献

Cooter, Robert D. and Ulen, Thomas S. [1997], "Law and Economics (2nd ed.)" (Addison-Wesley Educational Publishiers Inc.); 太田勝造訳『新版 法と経済学』(商事法務研究会).

電子商取引実証推進協議会国際課 [1999]、『電子商取引に関する米国視察団報告書』(電子商取引実証推進協議会).

電子商取引実証推進協議会認証局検討WG 8 ・相互接続検討SWG [1997]、『相互認証技術解説及び基本仕様案』(電子商取引実証推進協議会).

原田晃治・早貸淳子 [1998]、「商業登記情報を活用した電子認証制度の整備について」『ジュリスト』No. 1138 (有斐閣).

法務省 [2000]、『商業登記法等の一部を改正する法律案』
(http://www.moj.go.jp/HOUAN/S_TOUKI/refer02.htm)

一柳良雄・細谷祐二 [1999]、「市場と政府の補完的関係—市場機能拡張的政策の必要性」青木昌彦・奥野正寛・岡崎哲二編著『市場の役割・国家の役割』(東洋経済新報社).

夏井高人 [2000]、「電子署名に関する訴訟対応」岡村久道編著『インターネット訴訟2000』(ソフトバンクパブリッシング).

西垣通 [1999]、「電子マネーは「究極の貨幣」か」NTTデータシステム科学研究所編『電子貨幣論』(NTT出版).

Ogus, Anthony. I. [1994], "Regulation" (Clarendon Press, Oxford).

岡田仁志 [1998a]、「高度情報通信社会における電子決済の法政策学的分析—決済手段の電子化と決済方法の電子化—」『テレコム社会科学学生賞入賞論文集』vol. 7 (電気通信普及財団).

岡田仁志 [1998b]、「電子的決済手段の公共政策的分析」『国際公共政策研究第3巻第1号』(大阪大学大学院国際公共政策研究科).

岡田仁志 [1999]、「サイバー社会のプライバシー：EU型と米国型の調和はありうるか」『国際公共政策研究第3巻第2号』(大阪大学大学院国際公共政策研究科).

大谷和子 [1999]、「電子商取引の法律問題」高橋和之・松井茂記編『インターネットと法』(有斐閣).

Smedinghoff, T. J. and Bro, R. H. [2000]、「電子署名—アメリカ」指宿信 (編集代表)『サイバースペース法：新たな法的空間の出現とその衝撃』(日本評論社).

田中秀樹 [1997]、「ストアード・バリュー・プロダクツに対するEFT法の適用に関する議会へのレポート」『金融情報システム』(金融情報システムセンター).

辻井重男 [1998]、『暗号と情報社会』(文藝春秋).

郵政省・通商産業省・法務省 [1999]、『電子署名・認証に関する法制度の整備について』
(http://www.mpt.go.jp/top/ninshou-law/index.html)

郵政省・通商産業省・法務省 [2000a]、『パブリック・コメント募集結果』
(http://www.mpt.go.jp/pressrelease/japanese/denki/000131j601.html)

郵政省・通商産業省・法務省 [2000b]、『電子署名及び認証業務に関する法律案骨子』

(http://www.mpt.go.jp/top/ninshou-law/law-point.html)