第３部 電子署名・電子認証に関する法制度整備の在り方

2000 年 9 月 23 日

暗号通信の在り方に関する研究会

第１章　電子署名技術・電子認証サービスの現状と法制度モデル

我が国における電子署名・電子商取引の法制度の在り方を検討するに当たっては、現在の電子署名技術や電子認証サービスの実態に則した上で、どのような法制度モデルが適切なのかを分析することが不可欠である。

第１章においては、電子署名技術の発展動向や電子認証ビジネスの現状を把握するとともに、法制度モデルを分析し、諸外国の法制度の概要を整理する。

第１節　電子署名技術・電子認証サービスの動向

１．暗号技術の発展による電子署名技術の多様化

情報通信分野の急速な技術革新に伴い、暗号技術も大きな発展を遂げている。また、冷戦構造の終結により、これまで主に軍事用に用いられていたものと比較しても、安全面で遜色のないような高度な暗号技術が民間部門でも用いられるようになっている。

このような状況を背景に、高度な暗号技術を用いた多様な電子署名技術が開発されている。また、1990 年代のインターネットの商用化により、ネットワークにおけるセキュリティ確保の重要性が認識されるようになり、高度な暗号技術の応用が進み始めた。

(1)　デジタル署名

多様な電子署名技術の中でも、現在主流となりつつあり、今後も当面は中心的な位置を占めると考えられているのが、公開鍵暗号方式に基づいたデジタル署名である。（p.18、図―９参照）

デジタル署名においては、署名作成者がその通信内容となる電子文書を署名者固有の署名鍵（秘密鍵）により暗号化し、署名付き電子文書の受信者がその署名鍵に対応する署名作成者の検証鍵（公開鍵）によりそのデジタル署名が本当に送信者の署名であるのかどうかを検証することができるという仕組みになっている。

したがって、デジタル署名は、通信内容を暗号化したものを署名とするという技術的な特性から、署名そのものと通信内容である電子文書自体との結合性が強く、もし通信内容が通信途上で改ざんされれば、署名の検証過程によって、改ざんされたという事実も検証することができるという利点がある。一方で、デジタル署名が本人のものであることを確認することが必要であり、第三者とし

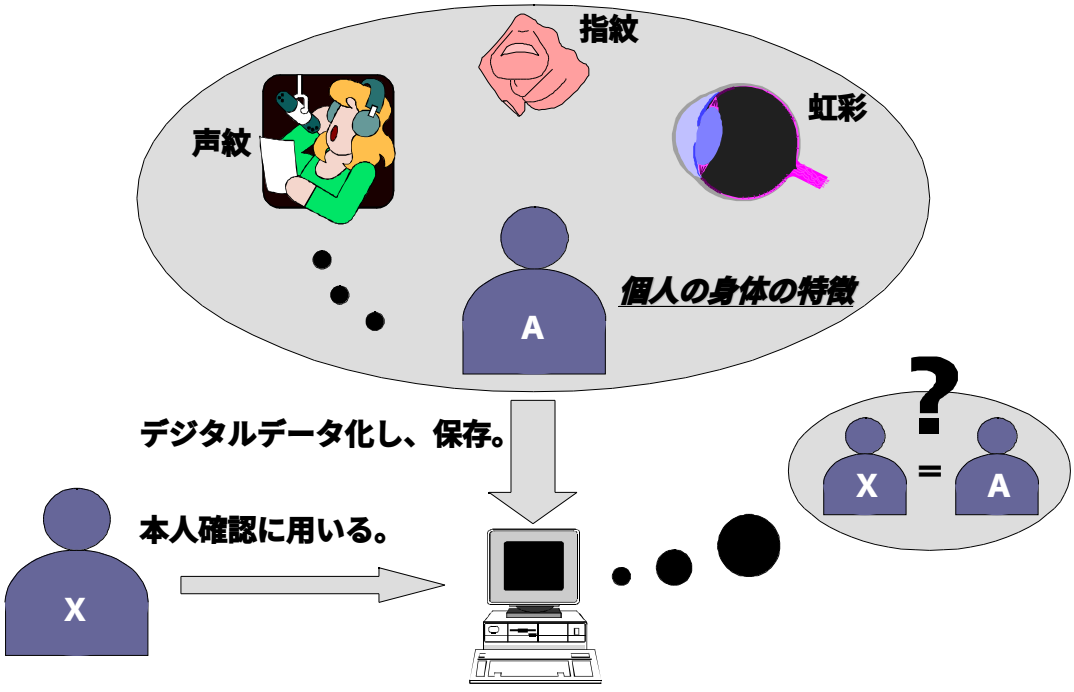
て、デジタル署名に使用された署名鍵と検証鍵の鍵ペアが本人のものであることを証明する認証機関の存在が必要となる。

デジタル署名が電子署名技術の主流となっていることから、各国の法制度においても、「デジタル署名」技術に限定した法制度を整備する例が多く見られ、またカナダ、オーストラリアのように、政府主導で、デジタル署名の有効性を実現するため、公開鍵暗号方式に基づいた PKI（Public Key Infrastructure：公開鍵インフラ）を整備し、認証機関を体系化しているところもある。

(2) バイオメトリクス（図―１６参照）

また、指紋や声紋、虹彩といった個人の特徴に基づいて本人性を確認する技術の開発も進んでいる。身体的な特徴に基づいているため、最も強力な本人認証手段であるが、その反面、指紋等の個人情報を電子データ化することに対する懸念がある。また、デジタル署名が有しているような通信内容との結合性についても別途確保する必要があるため、当面は、デジタル署名の署名鍵を使用する際の本人確認手段として、デジタル署名技術との併用が有望視されている。

［図―１６　バイオメトリクスの仕組み］

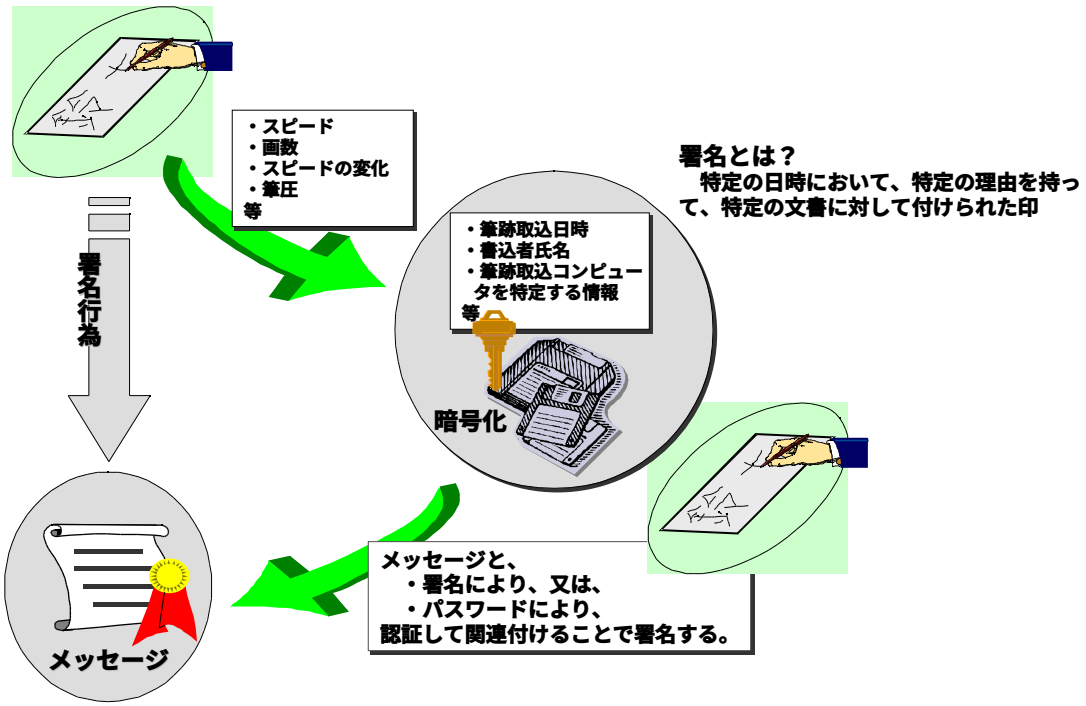


(3)　Signature Dynamics（図―１７参照）

他方、Signature Dynamics と呼ばれる、手書きの署名を、筆跡や筆圧、要する時間といった様々な要素を数値化することにより、電子データに変換し、そのままの形で電子文書に結合させるという技術も開発されている。デジタル署名技術に比べると、通信内容である電子文書本体との結合性は弱いが、署名者の本人性を確認する手段としては有効であり、署名鍵使用時における本人確認などデジタル署名技術との併用が考えられる。

また、実際にパッドの上などで手書きの署名を行うという儀式的なプロセスを伴うことから、簡単なパソコン操作だけで署名が付されてしまう他の電子署名技術に比較して、手書き署名や押印と同様に、利用者が署名を行うという行為の意義を認識しやすいという長所もある。

［図―１７　Signature　Dynamics の仕組み］



２．電子認証サービスの現状と認証機関の分類

(1)　認証機関（CA:Certification Authority）の分類

電子署名に関する電子証明書を発行する認証機関（CA:Certification Authority）は、主に以下のように分類できる。

① 登録機関（RA:Registration Authority）と発行機関（IA:Issuing Authority）

電子認証サービスを提供するに当たっては、電子証明書発行の申請者の本人確認を行う「登録業務」と電子証明書の作成・発行を行う「発行業務」が必要となる。電子認証サービスの提供形態によっては、これら二つの業務を別々の主体が行うケースがあり、「登録業務」を行う主体を「登録機関（RA：Registration Authority）」、「発行業務」を行う主体を「発行機関（IA：Issuing Authority）」と称すことがある。

② 「パブリックな認証機関（パブリック CA）」と「プライベートな認証機関（プライベート CA）」

あらゆる社会経済活動のデジタル化に伴い、企業内における電子メールのやり取りから巨額の商取引・決済まで、様々な目的で電子署名や電子認証が利用されるようになりつつあり、それぞれの目的に応じて、求められる認証（本人確認）のレベルも多様化している。また、情報通信技術の発展に伴い、電子認証を行うために必要なシステムパッケージが比較的低廉な価格で販売されるようになり、個人でも認証機関を構築することが可能となっている。

この結果として、認証機関の提供する電子認証サービスのレベルも分化する傾向にあり、認証機関は、大きく分けて、広く一般の顧客に対して電子認証サービスを提供する「パブリックな認証機関（パブリック CA）」と企業内の個人認証を行うような「プライベートな認証機関（プライベート CA）」とに分類できる。

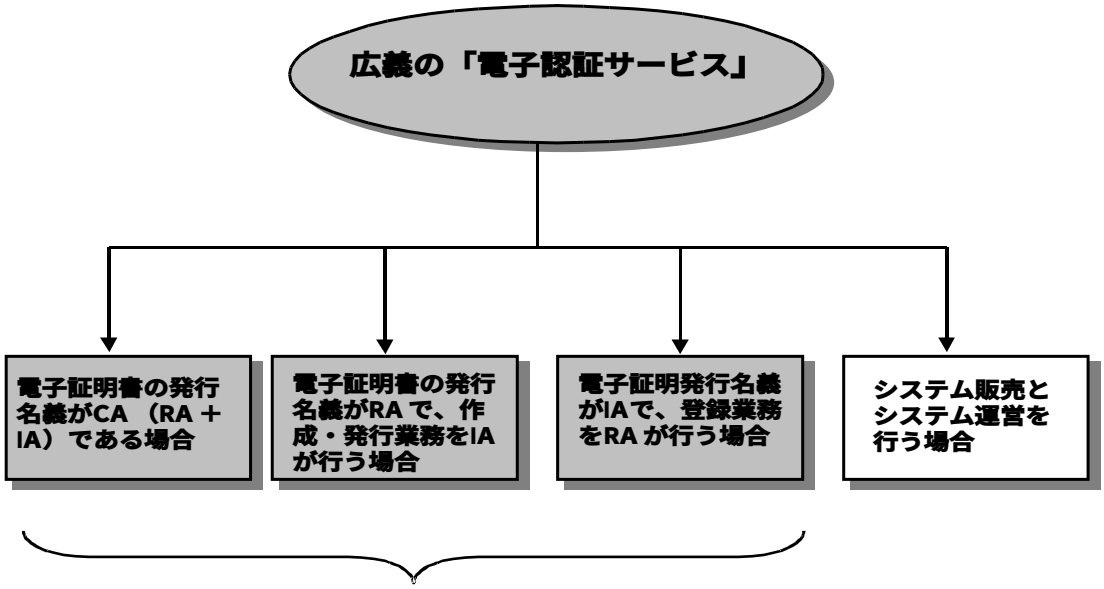
(2) 電子認証サービスの形態と市場規模

現在開始されている広義の電子認証サービスは、大きく分けて、①「電子証明書の発行名義が CA（RA＋IA）である場合」、②「電子証明書の発行名義が RA であり、作成・発行業務を IA が行う場合」、③「電子証明書の発行名義が IA であり、登録業務を RA が行う場合」、④「電子証明書の発行に必要なシステムを販売するとともに、システム運営サービスを提供する場合」の４つに分類できる（図―１８参照）。

①は、認証機関が顧客からの申請を受けて認証機関名義で電子証明書を発行するサービス形態、②は、金融機関などが、電子証明書の発行業務を別の企業に委託して、委託元の名義で電子証明書を発行するサービス形態、③は、電子証明書を発行するに当たり、登録業務のみを別の企業に委託し、委託元の名義で電子証明書を発行するサービス形態、④は、システムの販売を行うとともに、システムの運営を行うサービス形態であり、狭義の電子認証サービスということで言えば、電子証

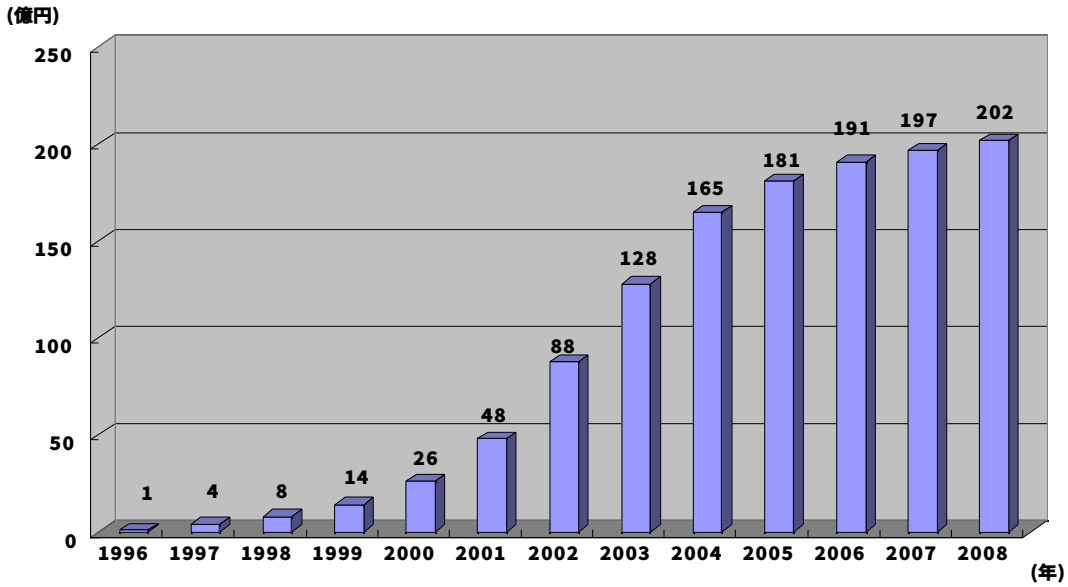
明書の発行を伴うという意味で、①、②、③のサービス形態を指すことが多い。

[図－１８　電子認証サービスの分類]



我が国を始め、世界各国において、電子商取引の普及に従って、このような電子認証サービスが開始されているところであり、その市場規模は将来的に大きな成長が見込まれている。（狭義の電子認証サービスの市場規模について、米国では1998年で、すでに約100億円、我が国においても、1998年現在で約８億円、2008年には200億円を突破するとの推計もある。図－１９参照）

[図－１９　日本における電子認証サービスの市場規模予測]



出典：日本能率協会総合研究所「市場予測」（NTTデータ経営研究所作成資料より作成）

(3)　認証機関の体系（図－２０参照）

認証機関は、電子署名に使用された鍵が名義人のものであることを証明する地位にあるが、認証

機関が行う認証の信頼性を担保するためには、認証機関自身が認証 されることが求められる。したがって、電子認証に対する利用者の信頼を確実なものとしていく観点から、認証機関の信頼性の連鎖の枠組みを構築することが必要となり、現在様々なモデルが考えられている。主なものとしては、以下の３つが挙げられるが、電子認証サービスはまだ始まったばかりの産業分野であり、今後どのようなモデルが主流となっていくかについては、現在の段階で予測することは困難である。

① 階層型モデル

下位の認証機関を上位の認証機関が認証し、その上位認証機関を、さらに上位の認証機関が認証していくというモデルである。最上位の認証機関は、ルート認証機関（ルート CA）と呼ばれる。VISA MASTER を中心とするクレジット業界で用いられている SET（Secure Electronic Transaction）プロトコルに基づく電子認証モデル（SET-PKI）が代表例として挙げられる。このモデルでは、各階層の一つの認証機関に複数の下位認証機関を属させることができることから、一つのルート CA を設けることで、膨大な認証機関を包含する認証機関の信頼性体系を構築することができるが、他方、ルート CA の信頼性をどのように担保するのかという問題がある。

② メッシュ型（水平型）モデル

各認証機関が上位・下位の階層を形成せず、独立して存在するというモデルである。各認証機関は、自分の発行する電子証明書の信頼性を自ら担保するという意味で、すべての認証機関はルート CA であるということができる。信頼性の連鎖については、各認証機関間で、「相互認証」（お互いに相手方の認証機関の信頼性を保証すること）を行うことにより構築される。米国の自動車業界の電子認証モデル（ANX-PKI）が、代表例として挙げられる。ルート CA の信頼性の担保に関する問題を回避できるというメリットがある一方、パブリック CA とプライベート CA に見られるように、各認証機関で採用するセキュリティ技術のレベル、業務運営方針（ポリシー）に大きな相違があることが多いことから、相互認証を行うに当たり、これらの相違をいかに克服するかが問題となる。また、相互認証については、相手方の認証機関の負う法的責任の一部を負担することになる可能性があることが、その推進の障害となり得る。

③ 階層型・メッシュ型混合モデル

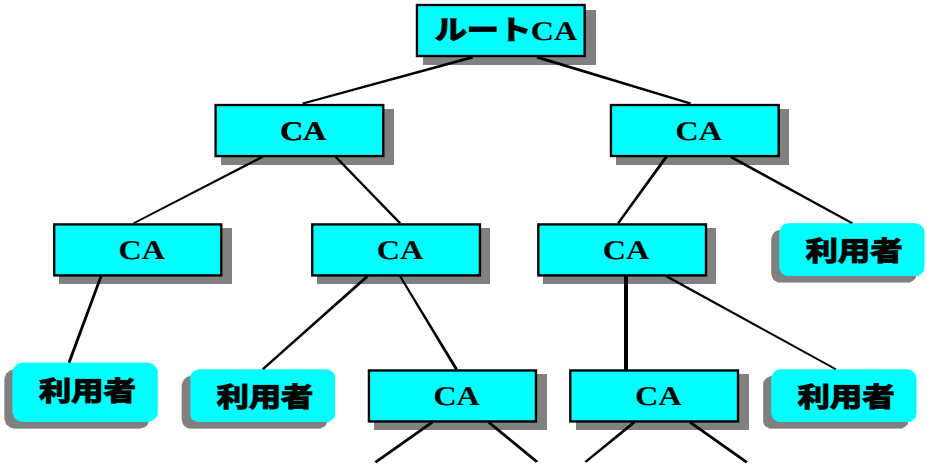
階層型とメッシュ型を混合したモデルで、階層型モデルを採用する認証機関体系とメッシュ型モデルを採用する認証機関体系が複数存在する枠組みを前提として、各体系をブリッジする（仲介する）ブリッジ認証機関（「ブリッジ CA」又は「ハブ CA」と呼称される。）を設け、すべての認証機

ここでいう「認証」とは、「認証機関に対して信用を付与する行為」を意味するものであり、認証機関が電子証明書を発行することで顧客の本人性を確認するという一般的な認証とは異なるものである。

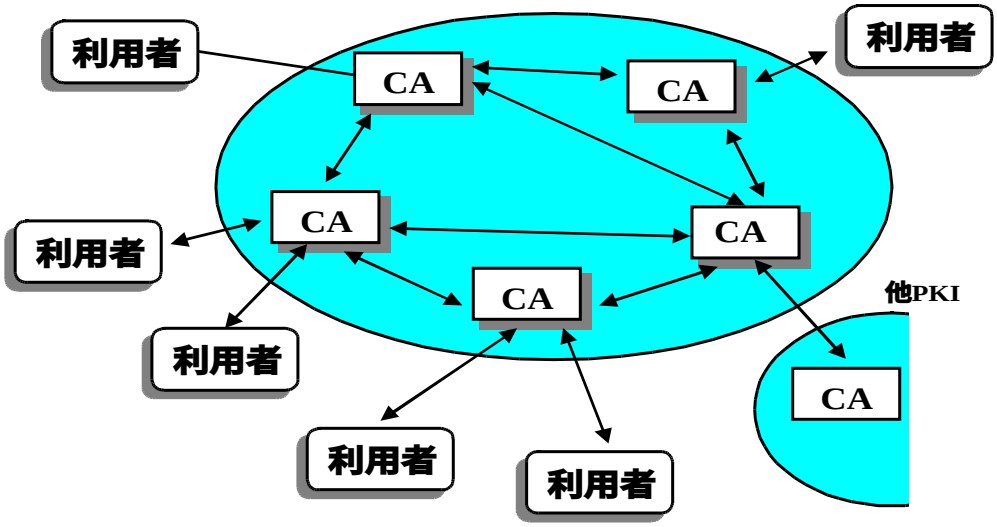
関間の信頼性連鎖の体系を構築するという考え方である。ブリッジ CA は、ブリッジに接続する CA を相互認証して、信頼性の連鎖を拡張する。米国政府の認証モデル（FPKI）がこのモデルを採用している。複数の認証機関体系の存在を許容し、各体系に階層型・水平型のいずれを採用するかの自由が与えられるというメリットがある一方、階層型構造におけるルート CA と同様、ブリッジ CA に対する信頼性を担保するスキームが問題となる。

［図－２０　認証機関の体系のモデル］

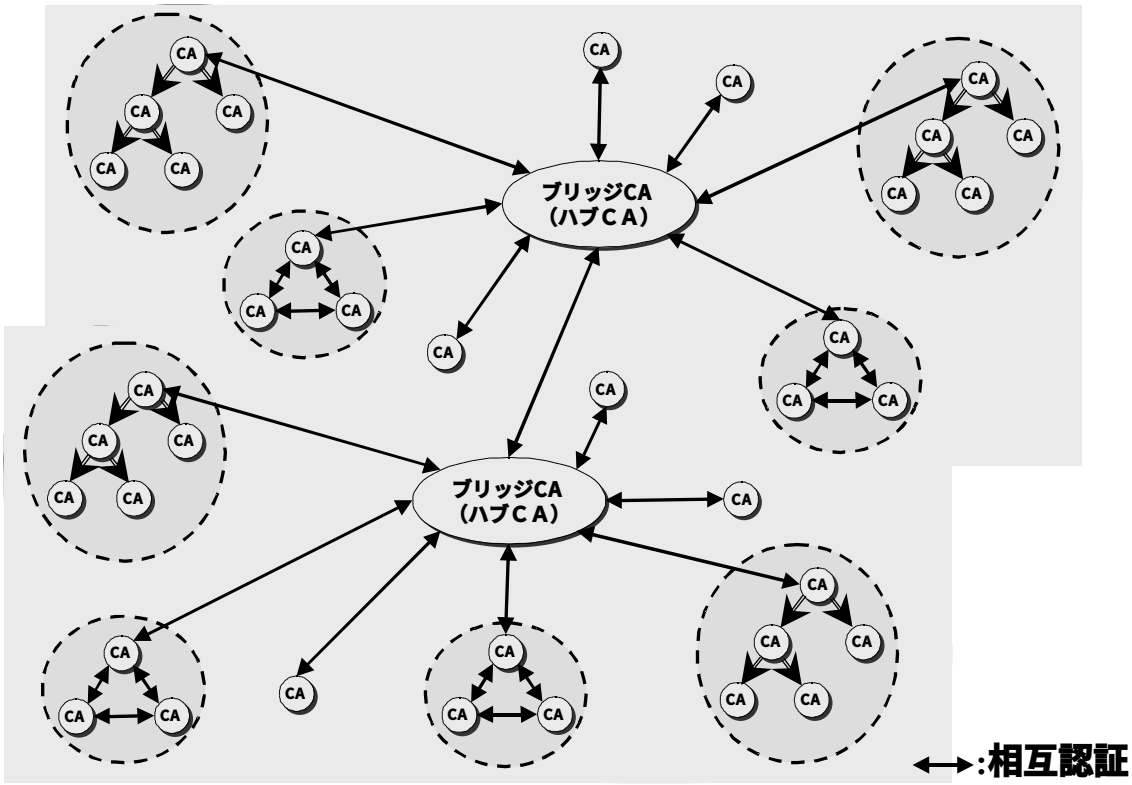
（階層型モデル）



（メッシュ型モデル）



（階層型・メッシュ型混合モデル）



３．電子署名・電子認証に関する主な課題

(1)　最上位認証機関等（ルート CA、ブリッジ CA）の信頼性を担保するスキーム

認証機関の信頼性連鎖の体系としてどのようなモデルを採用するにせよ、認証機関を認証機関が認証するという仕組みを採用する以上、その最上位に位置する認証機関の信頼性をどのようなスキームで担保していくかということが問題となる。

①　国による権威づけ（authorization）

国による権威づけにより、最上位認証機関の信頼性を擬制するという考え方であり、究極的には、マレーシアやイタリアにおける法制度のように、認証機関に対して義務的な免許制度を導入することにより、国自身が国内の認証機関のルート CA となるという方法も考えられる。また、義務的な免許制でなくとも、任意的な資格認定制度を導入することにより、国が少なくとも資格認定を受けた認証機関に対するルート CA の機能を果たすというアプローチを採用する例も見られる。

この方法によれば、ルート CA に対する信頼性を擬制することは容易であるが、義務的な免許制など過度の規制の導入は、民間部門の自由なビジネス展開を阻害する危険性がある。

② 認証機関間の相互認証の推進

典型的なメッシュ型構造に見られるように、特定の最上位認証機関を設けず、各認証機関間の相互認証を促進することにより、各認証機関の最終的な信頼性を担保する方法も考えられる。

この考え方によれば、国による規制的なアプローチを用いる必要がないことから、民間の認証機関の自由なビジネス展開は確保されるが、提供するサービスレベル、業務運営方針（ポリシー）が著しく異なる認証機関間の相互認証をいかに進めるか、また、相互認証の枠組みから漏れた認証機関の信頼性をどのように確保するのかが問題となる。

(2) 認証の有効性の証明

認証機関が発行する電子証明書は、電子署名に用いられた鍵が名義人のものであることを証明するものであるが、認証の有効性を確実なものとする観点から、電子証明書の有効期間は、通常、一定期間に制限されている。したがって、電子証明書の受信者は、電子証明書に記載された有効期間内であるかどうかを確認することによって、受け取った電子署名が有効に認証された鍵によって行われたものであるかどうかを検証することができるようになっている。

しかしながら、電子証明書の有効期間内であっても、電子署名の名義人が署名鍵を紛失したり、あるいは盗難にあったということが考えられるため、電子署名に対する電子証明書の効力を失わせる仕組みを設ける必要がある。

この場合、実際の電子認証サービスにおいては、電子証明書失効リスト（CRL:Certificate Revocation List）を作成して、認証機関の発行する電子証明書が有効かどうかを判定できる仕組みを導入しているが、この電子証明書失効リスト自体の有効性、すなわち失効した電子証明書が電子証明書失効リストにリアルタイムで掲載されているかどうかが問題となる。とりわけ、金融機関間の決済業務のように、リアルタイムでの電子証明書の有効性が問われるようなケースにおいては、この電子証明書失効リスト自体が有効なのかどうかが、取引の安全・信頼性を確保する上で重要な要素となる。

電子認証サービスは、まだ揺籃期にあることから、電子証明書失効リストのリアルタイムでの有効性をどのように確保していくかについては、検討が行われている段階であり、その具体化にはさらに時間を要すると考えられるが、現在考えられている方向性としては、①電子証明書失効リストの即時性を高めていくアプローチ、②ユーザである受信者側において有効性を判断させる仕組みを導入するアプローチ、③認証機関とは別に電子証明書失効リスト証明機関（VA: Validation Authority）を設け、VA が電子証明書失効リストの有効性を証明するアプローチという３つが挙げ

られる。

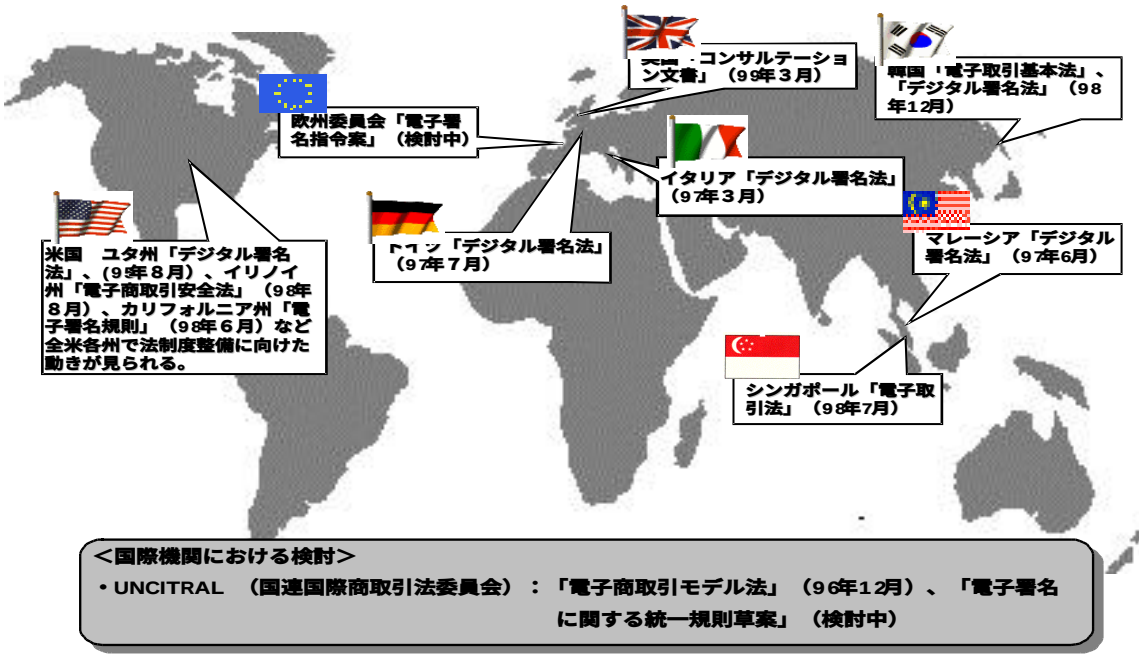
このように、これらの問題については、技術的な進歩やビジネスの発展等に応じて今後、さらに検討を進め、解決を図っていく必要があるものであり、過度に規制的な制度的基盤の構築により、電子署名・電子認証分野の技術革新やビジネス活動を阻害することとならないよう十分配慮する必要がある。

第２節　電子署名・電子認証に関する法制度モデルと諸外国の動向

１．法制度モデルの類型

電子商取引における安全・信頼性を高める観点から、欧米を中心とする諸外国や国連などの国際機関においても、電子署名・電子認証に関する法制度整備が進められている（図―２１参照）。

[図―２１　世界の電子署名・電子認証の法制化に関する動向]



国によって、取引の商慣行や電子署名・電子認証法制のベースとなる民事基本法制の体系が大きく異なることから、その法制の構造も多様化しているが、大まかに以下のような観点から分類することが可能である。

(1)　　対象とする電子署名技術による分類

①　公開鍵暗号方式に基づくデジタル署名技術のみを対象とするモデル

電子署名技術として主流となりつつある公開鍵暗号方式に基づくデジタル署名技術のみを対象と

するモデルである。デジタル署名という特定の技術を対象としているため、具体的な規定を設けやすいという利点はあるが、デジタル署名以外の電子署名技術の発展が阻害される可能性がある。また、電子署名・電子認証分野の急速な技術革新により、将来的にデジタル署名以外の技術が主流となった場合に法制度そのものが意味をなさなくなるという危険性を孕んでいる。

② デジタル署名に限定せず、すべての電子署名技術を対象とするモデル

デジタル署名などの特定の電子署名技術を対象とすることなく、すべての電子署名技術を対象とするモデルである。利用者の自由な電子署名技術の選択を可能とし、電子署名・電子認証分野における急速な技術革新に対する柔軟性も確保できるが、すべての電子署名技術を対象とするため、それぞれの電子署名技術の特性に応じた具体的な規定を設けることが難しくなるという法技術的な困難さがある。

(2) 認証機関に対する規律の方法による分類

① 認証機関に義務的な免許制度を導入するモデル

電子認証サービスを提供するすべての認証機関に一定の要件を定め、その要件に基づいて、免許の取得を義務付けるというモデルである。認証機関の安全・信頼性を確保するという意味では、有効であるが、民間部門の自由な経済活動を阻害し、利用者の選択の幅を狭めてしまう危険性がある。

② 認証機関に任意的な資格認定制度を導入するモデル

電子認証サービスを提供する認証機関に関して、一定の要件を定め、その要件に基づいて、安全・信頼性の高い認証機関に対して資格認定を行う一方で、資格認定を受けない認証機関の自由な活動を許容するというモデルである。資格認定基準の設定の仕方によって、規制的な制度にも非規制的な制度にもなり得るので、モデルの幅は広いが、いずれにしても、民間部門の自由な活動は保証される。

③ 認証機関に対する免許制や資格認定制度を導入せず、電子署名に関する基準のみを規定するモデル

認証機関に対する規定は設けず、一定の要件を充たす安全性の高い電子署名（「セキュアな電子署

名」と称されることもある）について、法的な効力を付与するというモデルである。認証機関の自由な活動が保証されるが、安全性の高い電子署名に関する具体的な規定を設けることの法技術的な困難さがある。

２．諸外国の法制度整備の動向（図―２２、２３参照）

(1)　　米国

米国においては、連邦政府のレベルでは、議会への法案提出は行われているものの、電子署名・電子認証に関する法制度は確立されていない。他方、各州の州法のレベルでは、全米 50 州のうち、すでに 35 の州で何らかの電子署名・電子認証に関する法制度が確立されている（1999 年 4 月現在)。そのうち、主なものとして以下の３つが挙げられる。

①　ユタ州「デジタル署名法」（1995 年 5 月成立）

世界で最初に成立した電子署名・電子認証に関する法制度であり、公開鍵暗号方式に基づくデジタル署名技術のみを対象としている。財務基盤、セキュリティ要件などを充たす認証機関に対して、任意的な資格認定制度を導入し、資格認定を受けた認証機関の認証する電子署名に関して、a）名義人のものであること、b）名義人は、その電子文書に署名を行う意図を持って署名を行ったことなどについて、裁判上の推定が与えられている。

ユタ州においては、この制度に基づき、すでに３つの民間の認証機関が州政府より資格認定を受け、電子認証サービスを提供している。（1999 年 5 月現在）

②　イリノイ州「電子商取引安全法」（1998 年 8 月成立）

認証機関に対する義務的な免許制度や任意的な資格認定制度は導入せず、一定のセキュリティ手続を経て作成された電子署名を「セキュアな電子署名」として定義している。「セキュアな電子署名」については、a）名義人のものであること、b）「セキュアな電子署名」が付された「セキュアな電子文書」は、電子署名が付されて以降、改ざんが行われていないことなどについて、裁判上の推定が与えられている。

③　カリフォルニア州「電子署名規則」（1998 年 6 月成立）

州の行政機関の使用する電子署名及び認証機関に関する規則を定めたもので、対象とする電子署名技術について、州政府の認定した電子署名技術に限定するとともに、州政府の使用する電子署名を認証する認証機関に関して義務的な免許制を導入している。他方、政府以外の一般利用者に対し

て認証機関が提供する電子認証サービスに関する法制度は今のところ存在しない。

現在の規則では、デジタル署名及び Signature Dynamics が州政府の使用する電子署名技術として認定されており、さらに認定電子署名技術の追加手続も定められている。

(2) 欧州委員会「電子署名指令案」（1999 年 4 月、検討中）

欧州においては、イタリア、ドイツを始めとして各国のレベルでの法制化も進められているが、欧州委員会においても加盟国域内の電子認証市場の発展に向けた統一的な基準作りの観点から、「電子署名指令」の策定が進められている。

現在、検討中の「電子署名指令案」においては、各国において認証機関に対して義務的な免許制を導入することは禁止しているが、任意的な資格認定制度の導入は許容している。資格認定を受けた認証機関の電子証明書により認証された電子署名に関して、署名を行うことの要件を充足するものであるとするとともに、裁判などの法手続において、証拠として採用できるという効力を認めている。

(3) ドイツ「デジタル署名法」（1997 年 7 月成立）

対象となる電子署名技術をデジタル署名に限定し、認証機関に対する任意的な資格認定制度を導入している。他方で、電子署名や資格認定を受けた認証機関の行う認証の法的効力に関する規定は設けられておらず、安全・信頼性の高い認証機関の評価基準としての機能を果たしている。また、資格認定に際しては、認定自体は、国（郵電規制庁）が行うことする一方で、その認定基準の一つである認証機関のセキュリティ評価については、国が直接行わず、国から指定を受けた民間の機関が行うこととしている。

ドイツにおいては、この制度に基づいて、すでに 8 社が資格認定を受けて、電子認証サービスを提供しているほか、数社の認証機関が資格認定に対する申請を行っている。（1999 年 5 月現在）

(4) イタリア「デジタル署名法」（1997 年 3 月成立）

対象とする電子署名技術をデジタル署名技術に限定するとともに、認証機関に対して義務的な免許制を導入している。今後、認証機関に対する義務的な免許制度の導入を禁止する「欧州電子署名指令」が発効した場合、その抵触関係が問題となる可能性がある。

(5) 英国「電子商取引における信頼性の構築：コンサルテーション文書」（1999 年 3 月公表）

英国においては、現在開会中の議会において電子署名・電子認証に関する「電子商取引法案」の提出が検討されているところであり、その骨格となる政府の考え方をまとめた「電子商取引における信頼性の構築：コンサルテーション文書」が本年３月に公表され、コメントの招請が行われた。

「コンサルテーション文書」においては、一定の要件を充足する電子署名を「高度な電子署名（Advanced Electronic Signature)」と定義した上で、a）電子署名が名義人のものであること、b）電子署名が付された電子文書が署名添付後改ざんされていないことについて推定を与えるべきであるとの考え方が示されており、また、認証機関に関しても、「暗号サービス事業者」を「電子認証サービス提供事業者（＝認証機関)」と通信内容の秘密化を行う「秘匿通信サービス事業者」に分類した上で、そのいずれにも任意の資格認定制度を導入する方向性が示されている。

(6)　　マレーシア「デジタル署名法」（1997 年 6 月成立）

対象とする電子署名技術をデジタル署名に限定し、認証機関に対しては義務的な免許制度を導入しており、違反した場合には罰則規定を設けている。また、認証機関により認証されたデジタル署名については、a）名義人のものであること、b）名義人は、その電子文書に署名を行う意図を持って署名を行ったことなどについて、裁判上の推定が与えられている。

マレーシアにおいては、すでに二つの認証機関が免許を取得しており、そのうち１社がすでに電子認証サービスの提供を開始している。（1999 年 5 月現在）

(7)　　シンガポール「電子取引法」（1998 年 7 月成立）

対象とする電子署名技術については、すべての電子署名技術を対象としつつも、認証機関の取扱う電子署名技術については、デジタル署名技術に限定するというアプローチを採用している。

一定の要件を充たす電子署名を「セキュアな電子署名」と定め、a）名義人のものであること、b）名義人の意思により作成されたものであることについて、裁判上の推定を与えている。また、認証機関に対して、任意的な資格認定制度を導入し、資格認定を受けた認証機関の認証するデジタル署名については、「セキュアな電子署名」であるとみなしている。さらに、資格認定を受けた認証機関に対しては、規定違反に対する罰則規定を設けるとともに、認証行為から発生した損害に対する認証機関の賠償限度額（「推奨信頼限度」）を定めることを義務づけている。

(8)　　韓国「電子取引基本法」、「デジタル署名法」（1998 年 12 月成立）

韓国においては、昨年 12 月に二法が成立し、現在、本年 7 月の施行に向けて、規則等を検討し

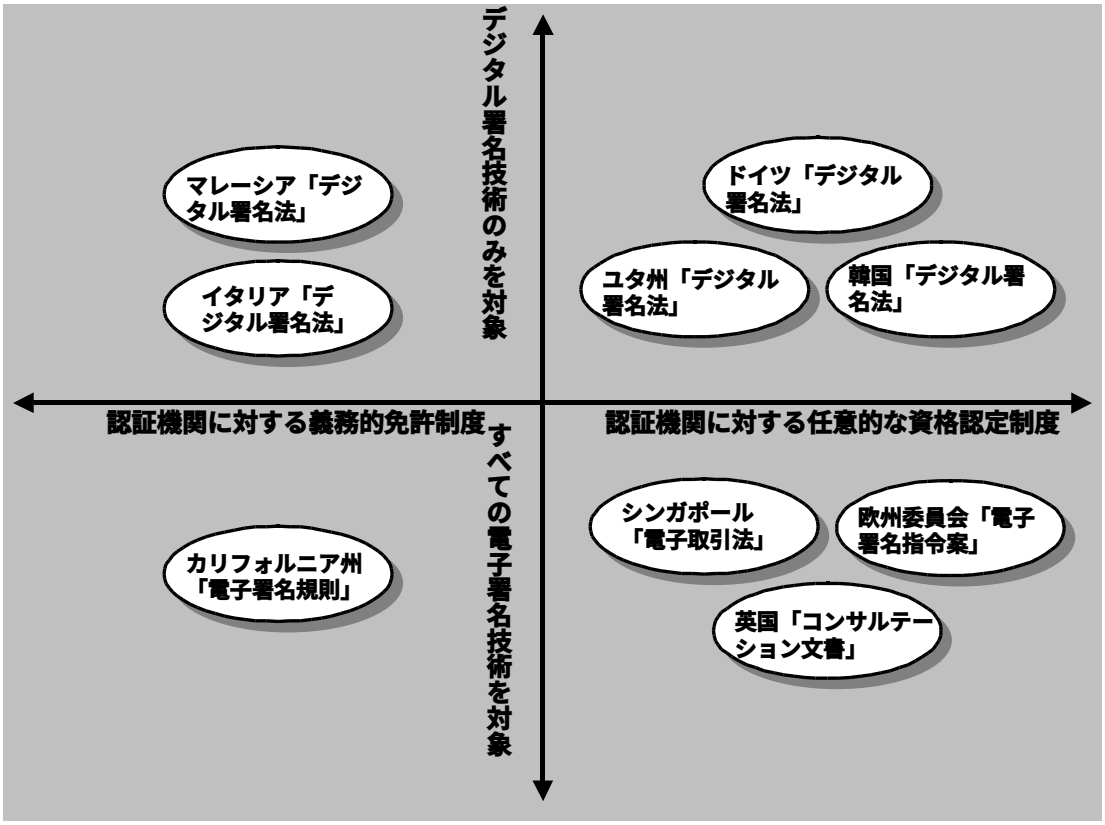
ている。

対象とする電子署名技術をデジタル署名に限定し、認証機関に対して、任意の資格認定制度を導入している。他方で、ドイツと同様に、資格認定を受けた認証機関の電子証明書に対する法的効力を定めておらず、安全・信頼性の高い認証機関の評価基準としての機能を果たしている。

(9)　国連国際商取引法委員会（UNCITRAL）「電子商取引モデル法」（1996 年 12 月)、「電子署名に関する統一規則草案」（検討中）

「電子商取引モデル法」において、電子署名や電子文書が手書きの署名や文書と同等に扱われる旨を規定するとともに、電子署名に関する法制度の具体化を行うという観点から、「電子署名に関する統一規則草案」について検討を行っている。しかし、各国の法制度整備の進展に伴い、考え方の対立が生じており、今後の方向性は不透明である。

[図－２２　法制度モデルによる各国の法制度の分類]



[図－２３　各国の法制度の概要]

	ユタ州	イリノイ州	ドイツ	イタリア	マレーシア	シンガポール	韓国
対象とする電子署名	デジタル署名	すべての電子署名	デジタル署名	デジタル署名	デジタル署名	すべての電子署名(認証機関に関してはデジタル署名)	デジタル署名
電子署名の法的効力	・署名要件の充足 ・資格認定を受けた認証機関の認証するデジタル署名に関して、名義人のものであることなどを裁判上推定	・署名要件の充足 ・secure な電子署名に関して、名義人のものであることを裁判上推定	規定なし	手書き署名と同じ効力	・署名要件の充足 ・認証機関の認証するデジタル署名に関して、名義人のものであることなどを裁判上推定	・署名要件の充足 ・secure な電子署名に関して、名義人のものであることなどを裁判上推定（資格認定を受けた認証機関の認証するデジタル署名については secure な電子署名とみなす）	署名要件の充足
認証機関の法的位置付け	任意的な資格認定制度	免許制・資格認定制を導入せず	任意的な資格認定制度	義務的な免許制度	義務的な免許制度	任意的な資格認定制度	任意的な資格認定制度
免許・資格認定機関	商務庁	―	郵電規制庁	情報技術庁	エネルギー・通信・マルチメディア省	国家コンピュータ委員会	情報通信部
認証機関固有の罰則規定	なし	なし	なし	なし	あり	あり	あり

国際相互認証	**言及あり**	**言及なし**	**言及あり**	**言及あり**	**言及あり**	**言及あり**	**言及あり**

第２章　我が国における法制度整備の在り方

第１節　電子署名・電子認証に関する法制度整備における基本的理念

我が国における法制度整備を進めるに当たっての基本的な理念としては、このような電子署名技術、電子認証ビジネスの現状及び諸外国の法制度整備の動向を踏まえて、以下のような要素が重要であると考えられる。

１．電気通信の安全・信頼性の確保、プライバシー・通信の秘密の保護

あらゆる社会経済活動をネットワーク上で行う「デジタル社会」への移行期において、従来の音声通信に加えて、データ伝送のニーズが大幅に増加するという、ネットワーク上を流通する情報の性質の変化が見られる。また、電話に代表されるような集中管理型のネットワークから、インターネットに代表されるように単一の管理者が存在しない分散型のネットワークへという、ネットワーク構造の変化も生じている。

電話などの音声通信においては、音声で相手方の本人性や通信内容を確認することによりネットワークの信頼性を確保することが可能であったが、データ伝送においては、同様の手段を採ることはできない。電子署名や電子認証は、データ伝送において、電子データを送信した相手方の本人性や通信内容の確認を行う手段であり、その法制度を検討するに当たっては、電気通信の安全・信頼性を確保するという観点から検討を行うことが求められる。

また、電子認証においては、従来の音声通信と異なり、通信当事者に加えて、認証機関という第三者が介在し、当事者のプライバシーや個人情報を収集し得る立場にあるため、電子認証サービスの利用者のプライバシーや通信の秘密をいかに保護するかという視点が必要である。

２．電子商取引における法的予見可能性の確保

通常の商取引においては、問題が生じた際の法律的な拠り所としての民法や商法、民事訴訟法といった民事基本法制が存在しているほか、商慣行等に基づく経験則が確立されており、商取引の当事者、利害関係者にとっては、どのような行為がどのような法的結果をもたらすのかについてある程度明確に予測することができる環境が整備されている。

他方、これらの民事基本法制や商慣行は、最近急速な発展を遂げている電子商取引のような、容易に国境を越え、かつ当事者同士が対面しないという取引形態を想定していないものが多いため、電子商取引を行う当事者、利害関係者にとっては、通常の商取引において用いられている法律や商慣行が、そのまま電子商取引においても適用されるのか否かが不明確となっている。この点が利用

者の電子商取引の安全・信頼性に対する懸念の原因となっている。

とりわけ、電子商取引の安全・信頼性を確保するためのインフラストラクチャである電子署名や電子認証については、社会において、果たして暗号化された電子データに過ぎない電子署名を通常の取引における手書きの署名や押印と同じように受け入れられるのか、あるいは民間の認証機関が行う認証が印鑑証明と同じように扱われるのかが不明確である。

我が国における電子商取引の発展を促進する観点からは、どのような電子署名や電子認証であれば、安心して利用することができるのかという客観的な基準作り、すなわち、どのような電子署名・電子認証がどのように扱われるのかといった点について、利用者と利害関係者のすべてが予測可能となるような枠組み作りを行うことが重要である。

したがって、我が国の電子署名・電子認証に関する法制度を検討するに当たっては、抽象的な規定にとどまるのではなく、利用者が容易に結果を予測できるような具体的なものとなるよう配慮することが求められる。

３．電子署名技術に関する技術的中立性の確保と過度の規制の排除

(1)　電子署名技術に関する技術的中立性の確保

情報通信技術の急速な発展に伴い、デジタル署名技術だけでなく、新たな電子署名技術が次々と開発されており、今後もさらにこの傾向は続いていくものと想定されている。

現在のところ、通信メッセージとの結合性が強いという技術的特性から、署名の本人確認だけでなく、通信メッセージが通信の途中で改ざんされていないことまで検証することができるという利点があるデジタル署名技術が電子署名技術の主流となりつつあり、当面はデジタル署名技術の優位は揺らがないと考えられる。

しかしながら、デジタル署名技術のみに立脚した法制度を導入することは、産業界に対しては、新しい電子署名技術の研究開発に対するインセンティブを減退させ、利用者に対しては、使用する電子署名技術の自由な選択の機会を奪い、政府自身にとっても、デジタル署名技術に替わる新しい技術が電子署名技術の主流となった時に、法制度が意味をなさなくなるという危険性を孕んでいるなど、大きな問題があるものと考えられる。

他方、具体的な署名技術を想定せず、すべての電子署名技術を包含するような法規定を設けることは、法技術的な困難を伴うものであり、法規定が抽象化せざるを得ない。その結果として、電子署名・電子認証に関する法制度の導入の最大の目的である電子商取引における法的予見可能性の明確化が損なわれる可能性もある。

したがって、我が国における法制度を導入するに当たっては、これらのバランスを勘案することが必要であり、具体的には、ある程度技術的中立性に配慮して、すべての電子署名技術を包含するような概念を設けた上で、当面主流となると想定されるデジタル署名を念頭においた具体的な規定を設けるというアプローチが適切であると考えられる。

(2)　　過度の規制の排除

政府による過度の規制は、民間部門の自由な経済活動を拘束するものであり、また電子署名・電子認証分野の急速な技術革新に柔軟に対応していくことができなくなるという危険性も孕んでいる。したがって、電子署名・電子認証のように揺籃期にある産業分野については、民間部門主導の柔軟で自由な経済活動によりその発展を図っていくという視点が不可欠であり、この点については国際的なコンセンサス が形成されている。

このような観点から、我が国において、電子署名・電子認証に関する法制度を検討するに当たっては、新たな電子署名技術の開発や認証機関のビジネス展開を阻害するものとならないよう十分に配慮する必要がある。

４．国際的な制度の整合性の確保

従来の物理的な空間での商取引においては、相手方の本人性や内容を確認する手段として、例えば我が国においては印鑑、欧米においては署名といったように、各国においてそれぞれ異なる方法が用いられてきた。これは、従来の物理的な空間における一般的な商取引は、基本的に国内のみで

電子商取引に関する日米共同声明（　1998 年 5 月 15 日）
Ⅰ．一般原則
電子商取引の発展及び商慣行の確立は民間部門が主導すべきである。

完結するものが多く、むしろ国境を越える商取引は希であったという背景によるものである。

他方、インターネットのような国際的にオープンに接続されたネットワークを通じて行われる電子商取引は、本質的にグローバルな性質を持っている。したがって、今後、電子商取引が発展するに伴って、本人性や通信内容を確認する手段として、電子署名は世界共通に用いられるようになると想定され、認証機関が、国境を越えて行われる電子商取引において用いられる電子署名に使用される鍵を認証するようなケースがますます増加していくものと考えられる。

このような状況においては、我が国の認証機関の認証が、果たして外国においても有効となるのか、また、外国の認証機関の認証が我が国においても有効となるのか否かが問題となる。このような問題をスムーズに解決するには、二国間あるいは多国間で、国際相互認証に関する法制度的な枠組みを構築していくことが、不可欠である。

このため、我が国において電子署名・電子認証の法制度を検討するに当たっては、諸外国において採用されている法制度のアプローチとの整合性に配慮することが求められる。

第２節　望まれる法制度の姿（図―２４参照）

１．「電子署名」と「電子認証」の定義

一般的には、「電子署名」とは、通常の商取引において用いられている手書の署名や押印と同様に、個人を識別するために用いられる電子的な情報であり、「電子認証」とは、電子証明書の発行などによって、電子署名に用いられる鍵が名義人のものであることを電子的に証明する行為であり、ひいては電子署名の有効性を担保するものであると捉えられている。

「電子署名」の定義に関しては、原則として幅広く捉えられるべきであると考えられるが、電子文書との結合性をどこまで求めるか、あるいは、作成者が電子文書の内容を承認し、これに拘束される旨の意思が表示されていることが必要かといったことも含めて、今後さらに検討を行うことが必要である。

２．電子署名と電子認証の法的効力

(1)　　我が国の現行法制における手書き署名・押印の訴訟上の取扱い

我が国においては、契約法の分野においては、書面を交わさなくとも、口頭の意思表示による合意

によっても契約が成立するという諾成主義が基本的に採用されていると一般的に認識されている 。また、手続法の分野においては、裁判官の判断基準として、証拠として採用できるものを、書面で作成されたものや手書き署名や押印が施されたものといったように限定した上で、その証拠に基づいて判断するというアプローチではなく、口頭弁論や証拠調べの結果に基づいて裁判官の自由な心証により判断を行うというアプローチ（自由心証主義 ）が採用されている。

自由心証主義における証拠の証明力の評価に関して、我が国においては、通常の取引において用いられている手書き署名や押印の訴訟における取扱いについて、民事訴訟法第 228 条第４項において「私文書は、本人又はその他の代理人の署名又は押印があるときは、真正に成立したものと推定する。」との規定が設けられている。これは、契約書などの私文書に署名や押印が行われている場合、その署名や押印が名義人によって行われたものであることが証明されれば、私文書全体がその名義人によって作成されたことが、推定されるという効力を与えるものである。

さらに、署名や押印が名義人よって行われたことの証明については、手書き署名については筆跡により、名義人のものであるかどうかを検証することが可能である。また、押印については、印鑑登録証明制度により印鑑登録証明書の印影と押印された印影を比較することにより容易に検証することが可能であるため、印鑑は安易に他人に使用させることはないという我が国の慣行に基づいて、本人によって押印されたとの「事実上の推定」（法律上の明文の規定はないが、裁判所において真実であると判定される蓋然性が非常に高い。）が認められており、その結果として、民事訴訟法第 228 条第４項の推定の前提となっている「名義人により行われたものであること」という条件を充たし、印鑑登録の行われた押印のある文書の成立の真正に関する推定が認められることとなる。

(2)　電子署名・電子認証の訴訟上の取扱いの在り方

「諾成主義」と「要式主義」

契約の成立に関して、意思表示を書面で行うなどの方式を必要とせず、口頭の意思表示の合致によっても契約が成立するという考え方が「諾成主義」であり、一定額以上の契約の成立等に関して、書面で行うことなどの方式を要件とするという考え方が「要式主義」である。諾成主義においては、契約手続における煩雑さがないことから、経済活動の円滑化が図れるという利点があるが、他方、争いが生じた場合に、物理的な証拠が残らないことから、裁判所における判定が困難となるという欠点がある。他方、要式主義は、詐欺などを防止する観点から、当事者の意思表示行為における慎重さを促すために採用されているものであるが、契約手続が煩雑となることから経済活動の円滑化が阻害される可能性があるという問題点がある。

我が国については、契約法制上、様式を求められていないので、諾成主義を採用していると一般的に認識されているが、実務においては、重要度の高い文書については、定型的な様式が多く用いられており、必ずしも諾成主義ではないのではないかと指摘もある。

「自由心証主義」と「証拠法定主義」

裁判官が判断を行うに当たって、口頭弁論に表れた一切の資料や証拠調べの結果に基づいて、裁判官の自由な心証によって判断を行うというのが「自由心証主義」であり、反対に、証拠として提出できるものを限定して、その範囲内で提出された証拠の内容に基づいて裁判官が判断を行うという考え方が「証拠法定主義」である。

証拠法定主義は、陪審制度などを導入している英米法系の国において採用されている例が多い。他方、日本を始めとする大陸法系の国においては、自由心証主義を採用する例が多く見られる。いずれのアプローチを採用しているかによって、電子署名や認証機関の発行する電子証明書の法的な位置付けに対する考え方は大きく異なってくるところであり、今後国際的にどちらのアプローチが主流となっていくかについて注意深く見守る必要がある。

現在の法制度においては、「電子署名」が「署名・押印」の中に含まれる概念なのか明らかでなく、また認証機関の発行する電子証明書の法的な位置付けについても明らかでない。このため、電子署名・電子認証の訴訟における取扱いを明確にし、電子商取引における法的予見可能性を確立するべきであるという観点から、電子署名や認証機関の発行する電子証明書に関して、法的な位置づけを与えることが必要である。

これらの取扱いの在り方を検討するに当たっては、主に以下の論点が挙げられる。

① 電子署名と電子署名が付された電子文書の結合性

電子署名については、電子的であるということの特性から、署名が付された電子文書との結合性が問題となる。すなわち、手書き署名や押印については、一旦手書き署名や押印が付された文書を改ざんすることは相当困難であるという前提があるが、電子署名においてもこの前提が成立するのかという問題である。

この点については、デジタル署名のように、その技術的な特性から電子文書との強い結びつきがあり、文書が改ざんされていないことが検証できるようなものについては、むしろ手書き署名や押印以上に強い電子文書との結合性があるものと考えられる。

② 認証機関の電子証明書と印鑑登録証明書の関係

認証機関の発行する電子証明書の訴訟上の取扱いに関して、印鑑登録証明制度の印鑑登録証明書とのバランスをどのようにするのかについては、ⅰ）明文の規定を設けず、印鑑登録証明書と同様の扱いにとどめるべきであるという考え方と、ⅱ）電子署名の技術的な特性に鑑みて、一定の認証機関の電子証明書に係る電子署名の付された電子文書の成立について法律に明文の規定を設けるべきであるという考え方がある。

ⅰ）法律上、明文の規定は設けないという考え方

この考え方のベースとなっているのは、公的機関が発行する印鑑登録証明書でさえ、「事実上の推定」しか認められていないにも関わらず、免許制度や資格認定制度を導入するにせよ、民間の認証機関が発行する電子証明書に対して、それ以上の強い効力を与えてよいのかという問題である。

印鑑登録証明書に関しては、例えば、住民登録や会社その他の商人の印鑑を登録する商業登記制度においては、虚偽の登記申請を行った者に対しては制裁が課されている。また、商業登記における登記官や地方公共団体の担当官の故意又は過失により発行された虚偽の印鑑登録証明書により損害が生じた場合には、損害を受けた者は、国家賠償法の規定に従い、損害賠償請求を行うことができる。ま

た、民間の認証機関が電子証明書を発行する際に行う本人確認手続は、パスポートや運転免許証などの公的証明書によることが多いと考えられる。したがって、この民間の認証機関の発行する電子証明書の法的効力を検討するに当たっては、印鑑登録証明制度とのバランスを考慮するべきであるという考え方もある。

ii）法律上、明文の規定を設けるべきであるという考え方

他方、本人との結びつきが厳格に確認された電子署名については、署名が本人のものであることについて、押印よりも高い信頼性があると考えることもできる。したがって、厳格な本人確認やセキュリティ手続を経て作成された民間の認証機関の電子証明書が付された電子署名に対しては、印鑑登録証明書とは異なり、明文の規定を設けるべきであるという考え方もある。

また、印鑑登録証明制度は日本に独特な制度であり、電子認証に関する国際的な制度との整合性を考慮すれば、我が国において、印鑑登録証明制度とのバランスのみを理由として、安全・信頼性の高い認証機関の発行する電子証明書についてまで、明文の規定を設けないのは、必ずしも適切ではないという視点もある。

電子署名・電子認証には、手書きの署名・押印や印鑑登録証明制度のようなこれまでの歴史の積み重ねがないため、裁判において「事実上の推定」が認められるようになるには、さらに相当な年月を要するのではないかという指摘もある。このような立場からは、電子商取引の急速な進展に対応し、その健全な発展を促進するため、商慣行や判例の積み重ねを待つのではなく、法律上、明文で規定するべきであるとも主張される。

このように、認証機関の発行する電子証明書の訴訟上の取扱いについては、様々な観点から、今後さらに検討を行っていくことが必要である。

③　受信者保護と送信者 保護のバランス

電子署名や認証機関の電子証明書の法的効力については、受信者保護の観点からは、受信した内容の確実性を担保するため、強い法的効力を認めるべきであるとの意見がある。しかしながら、他方、どのようなセキュリティシステムを用いても、署名鍵を紛失したり、通信の途中で改ざんされる可能性を全く否定することはできないことから、送信者保護の観点からは、電子署名や電子認証にあまり強い効力を認めることは適当でないと考えられ、また、電子署名の名義人が負担を強いられることへの懸念から、電子署名や電子認証の利用が進まないという可能性もある。

したがって、これらの受信者保護と送信者保護のバランスに配慮した上で、法的効力の範囲を検討していくことが求められる。

３．認証機関に対する任意的な資格認定制度の導入の検討

---

* 送信者
ここでいう「送信者」とは、単に電子メッセージを送信した者ではなく、電子署名や電子文書の帰属先となる者を意味するものである。UNCITRAL の電子商取引モデル法(1996 年)等では、“ originator ”と表記されている。

(1)　　任意的な資格認定制度導入の必要性と意義

①　多様な電子認証サービスの安全・信頼性の目安としての基準作り

すでに第１部でも見たように、認証機関の提供するサービスのレベルは相当に多様化している。したがって、他の方法で信頼関係が確立していない当事者間で、より確実な認証を必要とするやり取りを行う場合には、電子認証サービスの利用者側から見れば、自分が利用する認証機関が信頼できるものなのかどうかを判断することが難しい。

また、認証機関の発行する電子証明書の法的効力の観点からも、認証機関がセキュリティレベルなど、認証機関の安全・信頼性が多様であることに鑑みれば、すべての認証機関の発行する電子証明書を、公的機関が発行する印鑑登録証明書と同様に取扱うのは適切ではなく、一定の基準を設ける必要がある。

このような観点から、資格認定制度を導入することは、認証機関の安全・信頼性の目安に関する基準作りとして、電子商取引分野における法的予見可能性を確立するためにも意義があるものと考えられる。

また、諸外国においては、認証機関に対する免許制や資格認定制度の導入が進んでおり、諸外国の法制度との国際的な整合性を確保し、国際相互認証の枠組み作りを推進していくという観点からも、我が国において資格認定制度の導入を検討すべきである。

②　任意的なものとすることの必要性

電子署名・電子認証は、サイバースペースにおける社会経済活動のインフラストラクチャであり、その用いられる用途に応じて、求められる認証のレベルも様々である。例えば、企業内での社員の個人認証など、資格認定を受けるレベルの認証機関のサービスでなくても十分なものもある。

したがって、資格認定を受けない認証機関の多様なレベルのサービス提供が阻害されるべきではなく、また利用者の自由な選択を確保する観点からも、義務的な免許制度による認証機関に対する規制を導入することは適切ではない。

(2)　　資格認定を受ける認証機関に求められる要素

資格認定制度の導入を検討するに当たり、認証機関が資格認定を受けるために必要とされる要素としては、以下のものが考えられる。

① セキュリティ技術

認証機関の安全・信頼性の最大の基準は、どのようなセキュリティシステムを用いているかという点である。資格認定を受ける認証機関に対しては、認証システムへの不正アクセス対策など、相当程度のセキュリティ技術に基づいた運営が求められるべきである。

また、認証機関に関しては、とりわけ運用面のセキュリティの確保が求められるところであり、認証機関への資格認定制度を導入するに当たっては、認証機関に関するこれらのセキュリティ評価基準の在り方について検討を行うことが必要である。

② 厳格な本人確認手続

認証機関において、どのように厳格なセキュリティ手続を用いられていても、顧客登録時の本人確認が十分なものでなければ、なりすまし等の危険性を排除することができない。

したがって、安全・信頼性の高い認証機関として資格認定を受けるに当たっては、厳正な本人確認手続を採用することが求められる。

③ 財務基盤の安定性

資格認定を受ける認証機関は、安全・信頼性の高い認証機関として認知されるものであり、継続的な事業運営が求められることから、安定的な財務基盤を確保することが求められる。

④ 人的信頼性の確保

認証機関は、個人情報を収集し得る立場にあることから、業務の適正な運営が求められる。また、業務運営に当たっては、暗号技術や情報通信システムに関する高度な専門性が要求されることから、関連の部門にこれらの技術に関する専門性を備えた職員を適切に配置することが求められる。

(3) 資格認定制度のスキーム

① 資格認定の対象となる認証機関

認証機関のサービス提供については、CA が自らの名義で電子証明書を発行する形態もあれば、金融機関などの登録機関（RA）が発行機関（IA）に電子証明書発行業務を委託して、登録機関（RA）名義の電子証明書を発行する形態もある。

登録機関（RA）と発行機関（IA）のいずれが資格認定を受ける主体となるべきかについては議論があるところであるが、利用者との間で直接法律関係を有する機関を資格認定対象とし、登録機関（RA）と発行機関（IA）の関係については、両者の契約関係に基づいて処理するというアプローチが、資格認定に伴う責任関係を明確にする観点からも、適当であると考えられる。

② 資格認定主体

資格認定により、認証機関の行う認証に一定の法的効力が発生することを前提にすれば、国を資格認定主体とすることが適当である。

ただし、資格認定に際して民間部門のビジネスの現状を反映していく観点から、資格認定のための要件を充たしているかどうかの審査に関しては、国から委託を受けた複数の民間の指定団体が行うことも考えられる。また、ドイツの立法例に見られるように、技術革新が急速で、審査に当たって高度な専門性が要求されるセキュリティ技術要件の部分についてのみ、複数の民間の指定団体で行うという方法も一案である。

③ 資格認定による効果

資格認定制度の導入の目的が、認証機関の安全・信頼性の目安に関する基準を設定し、電子商取引における法的予見可能性を確立することであることから、資格認定を受けた安全・信頼性の高い認証機関の発行する電子証明書については、公的機関の発行する印鑑登録証明書と同様に、電子署名が名義人の意思に基づいて作成されたことに関する「事実上の推定」が認められるべきである。

印鑑登録証明書以上の強い効力、例えば、電子署名が名義人の意思に基づいて作成されたことに関する推定に関する明文規定を設けるべきか否かについては、電子認証ビジネスの現状等を考慮しながらさらに検討を行うことが必要である。

これらの訴訟上の取扱いは、資格認定を受けた認証機関の発行する電子証明書について認められるものであるが、資格認定を受けない認証機関の認証する電子署名についても、裁判において十分な安全・信頼性があることが証明されれば、同様の扱いとされることが否定されるべきではない。

④ 資格認定による認証機関の義務

ｉ）　認証機関一般にかかる義務

ア）　顧客の個人情報保護

認証機関は、顧客の個人情報を収集し、保管する立場にあることから、収集した顧客の個人情報を適正に管理する義務がある。

イ）　顧客の署名鍵保管の原則禁止

電子署名や電子認証が、通常の取引における手書き署名や押印と少なくとも同等に扱われることの前提は、個人の署名鍵が本人によって適正に保管されていることである。顧客の署名鍵が適正に保管されていないと、容易にコピーができるという電子的データの特性から、重大な結果を引き起こしかねない。

したがって、このようなリスクを軽減するという観点から、認証機関は、顧客からの明示的な依頼のない限り、顧客の署名鍵を保管するべきではないと考えられる。

ⅱ）　資格認定を受けた認証機関にかかる義務

ア）　監査

資格認定を受けた認証機関の安全・信頼性を担保していく観点から、業務運営が適正に行われているかどうかについて、定期的に監査を受けることが求められる。

イ）　情報開示

資格認定を受けた認証機関は、その安全・信頼性を広く利用者に対して周知するべきであると考えられる。したがって、資格認定を受けた認証機関は、安全対策について、監査人に適正に開示するとともに、その監査結果を広く周知するべきである。また、一般利用者に対しても、電子証明書の発行条件や使用条件に関する運用規則、財務内容等について、開示することが求められる。

⑤　資格認定を受けた認証機関の法的責任

資格認定を受けた認証機関の発行した電子証明書を利用したことにより損害が生じた場合、どこまで認証機関が責任を負うべきかについては議論がある。認証機関は、自身が行った認証がどのような規模の取引に用いられるのかを把握するのは、困難であることから、電子認証ビジネスの発展を促進する観点から、認証機関に対する損害賠償請求に対する推奨信頼限度（ここまでは保証するという一定の限度額）を設定することも考えられる。しかしながら、推奨信頼限度を設定するに当たっては、一認証当たりの限度額を定める方法と一個人当たりの限度額を定める方法のいずれをとるにせよ、求償権者の特定や分配方法等に問題が残る。したがって、推奨信頼限度を設けることの適否については、国際動向も踏まえ、今後さらに認証機関と電子認証サービス利用者のコンセンサスの醸成に向けて、検討を行っていく必要がある。

いずれにせよ、認証機関が負うべき責任の範囲については、無制限とされるべきではなく、認証機関に課される注意義務に対する違反と「相当因果関係」がある範囲に限定されるべきである。したがって、法的責任の範囲は、認証機関に課される注意義務をどのような内容とするかによって変わってくることから、認証機関に求められる登録、電子証明書発行等の役割とこれを信頼して行動する者の利益を考慮し、被害者救済と社会インフラの一翼を担う認証機関の円滑な事業継続との均衡をはかりながら、今後とも検討する必要がある。

また、損害賠償請求における立証責任においても、資格認定を受けた認証機関については、認証機関以外の者が認証機関の運営に瑕疵があったことを立証することは非常に困難なことから、裁判における立証責任の転換を図り、資格認定を受けた認証機関に立証責任を負わせることも検討すべきである。

⑥　資格認定の更新

電子署名・電子認証分野の技術革新は急速であり、資格認定において最も重要な基準であるセキュリティ技術がいつまでも十分なものであると言えるとはは限らない。また、一度資格認定を受ければ、業務を廃止するまで有効であるとすると、一種のモラルハザードが生じかねず、業務の適正な運営が損なわれる可能性もある。

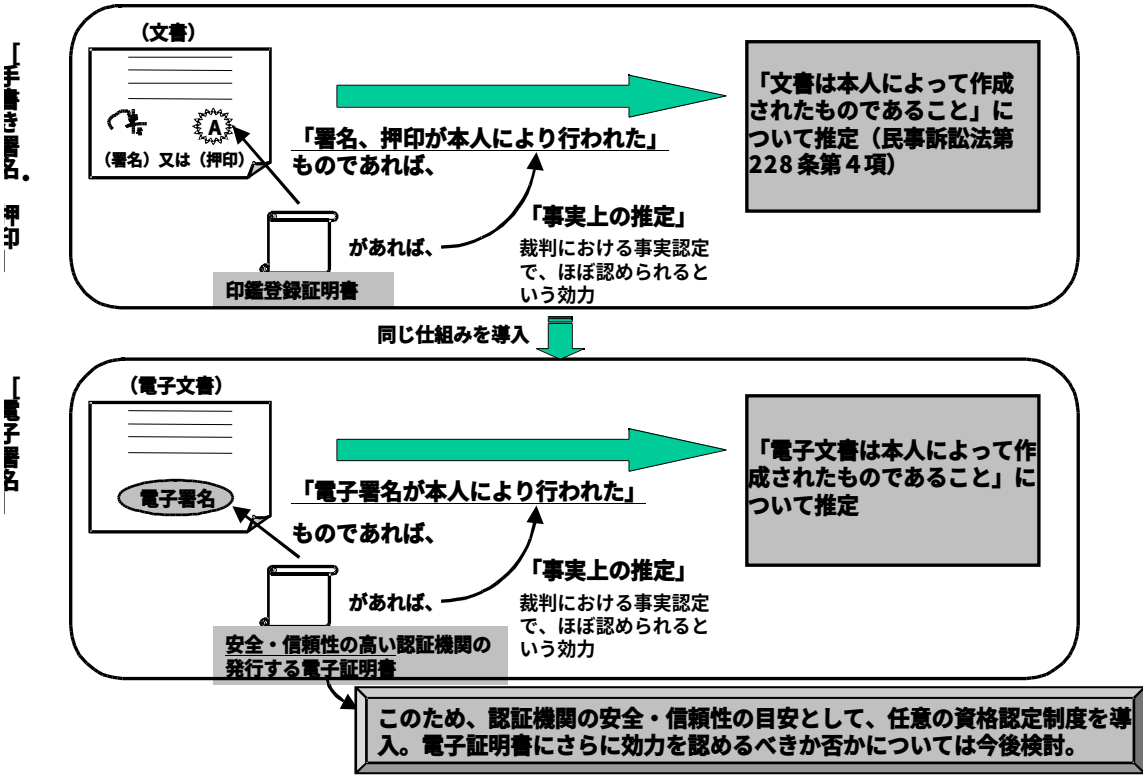
このような観点から、諸外国の立法例にも見られるように、資格認定の有効期間については、一定の期間に限定するべきであり、更新手続を導入することが適切であると考えられる。

４．外国の認証機関の取扱い

電子商取引はグローバルな性質を持っており、電子認証ビジネスについてもグローバルなビジネス展開を行うことが求められていることから、外国の認証機関に対しても差別的な取扱いを行うべきではない。

外国に所在する認証機関に対して、資格認定を行うべきかどうかという問題については、法的管轄の問題も含め、検討を行っていくことが必要である。

［図―２４　我が国において想定される法体系のイメージ］



第３節　電子署名・電子認証に関するその他の課題

１．国際相互認証の枠組み

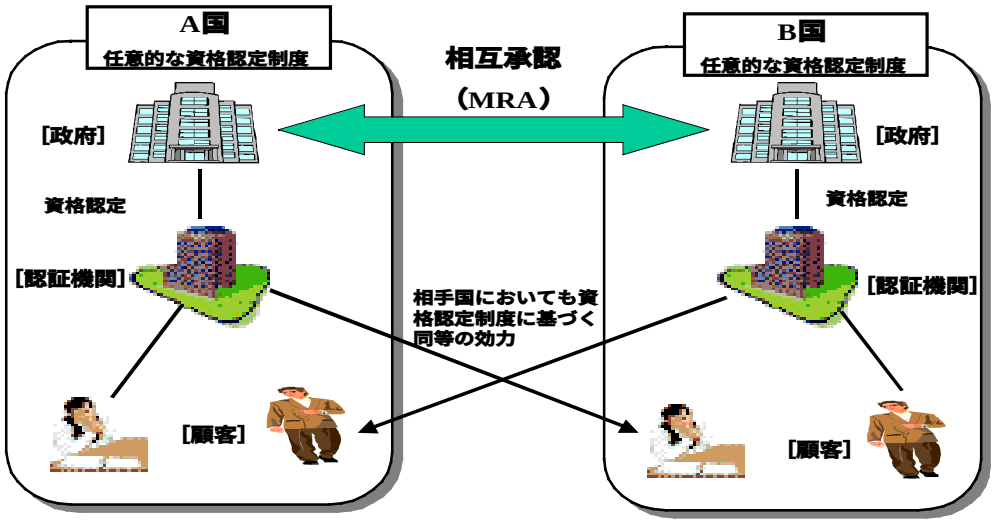
認証機関の体系について、世界中のすべての認証機関を一つの最上位認証機関（ルート CA）を頂点とする階層型のツリー構造の下に構成するということが困難である以上、認証機関の信頼性の連鎖の体系を構築していくためには、何らかのレベルで認証機関間で相互認証を推進することが必要となる。

各国で整備が進められている電子署名・電子認証に関する法制度は、各国の民事基本法制、商慣行の違いから、とりわけ、認証機関の法的な位置付け、対象とする電子署名技術の範囲について、大きな差異が見られる。

一般的には、義務的な免許制度や任意の資格認定制度を導入している法制度においても、外国の認証機関に対しても、相手国内で同等の基準や要件に従って免許や資格認定を受けた認証機関については自国内で免許や資格認定を受けた認証機関と同等に扱う旨の規定を設けている例（ドイツ、マレーシアなど）が多い。

さらに認証機関のグローバルなビジネス展開を促進する観点から、法制度的な互換性があることを事前に明示的に認知できるようにすることが有効であることから、二国間あるいは多国間の政府間レベルで、法制度に関する相互承認（MRA）を促進していくことが求められる（図―２５参照）。

［図―２５　国際相互認証］



※政府間で相互承認を行うにあたっては、両国間の認証機関の法的位置付けに関するアプローチが重要な要素となる。

２．電子文書に関する証明制度

社会経済活動において、「認証」によって確認される「相手が誰であるか」ということに加えて、さらに「いつ、何を行ったのか」を確認することが求められるケースがある。物理的な現実の世界において、公証人役場が行っているいわゆる公証業務がこの概念に当てはまる。

社会経済のデジタル化に伴い、経済活動を中心とする人間の活動をサイバースペースの中で実現することができるようになるに連れて、相手方を確認する電子認証サービスにとどまらず、到達証明、否認の防止、記録の保存、証拠の生成といった電子的な証明サービスに対するニーズも高まってくるものと思われる。

法務省において公証人役場の公証サービスの電子化が検討されているほか、技術的にも民間部門においてシステム開発が行われている。電子認証と同様に、今後、民間部門が行うこの種の証明サービスを法的にどのように位置づけるのかについて、検討を行っていく必要がある。

３．電子署名・電子認証に関するユーザリテラシーの向上

一般の商取引行為において署名を行うあるいは印鑑を押すという行為が一定の法的な意味を持つということについては、ほとんどの利用者が認知しているため、署名を行ったり、印鑑を押すことについては、それなりの慎重な注意が払われていると考えることができる。

他方、電子商取引が十分に普及していない現段階においては、一般の電子商取引の利用者は、電子文書に電子署名を付す行為に慣れ親しんでおらず、また、簡単なパソコン操作で、手書の署名や押印と同じ効力を持つ電子署名を行うことが可能であるため、行為の重大性を認識せずに、電子署名を行ってしまうという危険性がある。

また、電子署名・電子認証の仕組みの根幹である「署名鍵の適正な管理」の重要性についても、現段階では、十分な理解が浸透していないと考えられる。

このような現状を踏まえ、我が国において電子署名・電子認証に関する法制度整備を行うに当たっては、電子商取引における電子署名・電子認証の意義に関する普及啓発活動を行うことが必要であると考えられる。また、電子署名を用いる習慣が根付くまでの過渡期においては、Signature Dynamics のように「署名を行う」という一種の儀式的な行為を伴うユーザインターフェースを用いることも有用であると考えられる。

４．消費者保護

立証における「個人」と「法人」の能力の差異から、電子署名・電子認証に関する法制度においても、その法的効力の範囲や立証責任について、「個人」と「法人」を同列に扱ってよいかという議論がある。

消費者保護を徹底するべきであるという立場からは、電子署名の名義人が「個人」である場合には、法律の中に特則を設けるべきであるとの考え方もあるが、個人名義で行われた法人の代表者としての署名をどのように扱うのかなど、「個人」と「法人」の境界は不透明であり、電子署名・電子認証に関する法制度の中に「個人」と「法人」の峻別を導入することは、却って電子商取引における法的予見可能性に曖昧さをもたらす危険性があり、適当ではない。

５．モデルユーザとしての政府の役割

電子商取引のインフラストラクチャである電子署名・電子認証の普及を促進していくためには、暗号の標準化の推進方策と同様に、最大規模のユーザである政府機関が率先して、政府調達手続、電子申請などにおいて、電子署名・電子認証を利用していくことが求められる。

「暗号通信の在り方に関する研究会」構成員名簿

（五十音順・敬称略）

座長	辻井（つじい）　重男（しげお）	中央大学理工学部教授
座長代理	多賀谷（たがや）　一照（かずてる）	千葉大学法経学部教授
	稲村（いなむら）　雄（ゆう）	日本ベリサイン（株）マーケティング部テクノロジーマネージャ
	大谷（おおたに）　和子（かずこ）	（株）日本総合研究所法務部長
	岡本（おかもと）　龍明（たつあき）	日本電信電話（株）ＮＴＴ持株会社移行本部 情報流通プラットフォーム研究所特別研究員
	川島（かわしま）　昭彦（あきひこ）	サイバートラスト（株）代表取締役社長
	神田（かんだ）　秀樹（ひでき）	東京大学法学部教授
	小林（こばやし）　善和（よしかず）	日本アイ・ビー・エム（株）通信渉外副部長
	白井（しらい）　力（ちから）	三井物産（株）ソリューション事業部コンピュータシステム営業部 Ｉ＆Ｃチームセキュリティコンサルタント
	鈴木（すずき）　優一（ゆういち）	エントラストジャパン（株）取締役
	道垣内（どうがうち）　正人（まさと）	東京大学法学部教授
	長迫（ながさこ）　忠良（ただよし）	日本認証サービス（株）取締役管理担当
	奈良（なら）　隆司（たかし）	（財）金融情報システムセンター業務調査部長
	林（はやし）　誠一郎（せいいちろう）	（株）エヌ・ティ・ティ・データ技術開発本部 マルチメディア技術センタ部長
	東田（ひがしだ）　正信（まさのぶ）	サイバービジネス協議会インターネットキャッシュ推進部会長
	松本（まつもと）　勉（つとむ）	横浜国立大学大学院工学研究科助教授
	室町（むろまち）　正実（まさみ）	弁護士
	森山（もりやま）　由縁（ゆかり）	日本電気（株）技術企画部標準化推進部主任
	山田（やまだ）　慎一郎（しんいちろう）	（株）エクスウエイ代表取締